SIMOS

Implementing Cisco Secure Mobility Solutions

Version 1.0 **Lab Guide**

Part Number: 97-3336-01

https://t.me/learningnets



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED "AS IS" AND AS SUCH MAY INCLUDE TYPOGRAPHICAL, GRAPHICS, OR FORMATTING ERRORS. CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

© 2014 Cisco Systems, Inc.

https://t.me/learningnets

Table of Contents

Lab 2-1: Implement Site-to-Site Secure Connectivity on the Cisco ASA ***L-5***

Visual Objective L-6
Required Resources L-6
Command List L-6
Job Aids L-6
Task 1: Configuring the Cisco ASA for Site-to-Site VPN L-10
Task 2: Disabling NAT for Testing L-16
Task 3: Verifying the Site-to-Site VPN L-19

Lab 2-2: Implement Cisco IOS Static VTI Point-to-Point Tunnel ***L-25***

Visual Objective L-26
Required Resources L-26
Command List L-26
Job Aids L-27
Task 1: Configure Static VTI Point-to-Point Tunnel L-31
Task 2: Verify Static VTI Point-to-Point Tunnel L-32

Lab 2-3: Implement DMVPN ***L-39***

Visual Objective L-40
Required Resources L-40
Command List L-40
Job Aids L-42
Task 1: Configure a DMVPN Hub L-46
Task 2: Configure a DMVPN Spokes L-48
Task 3: Configure OSPF Routing in DMVPN L-50
Task 4: Verify DMVPN Hub and Spoke Operation L-51
Task 5: Configure a DMVPN Spoke to Spoke Communication L-55
Task 6: Verify DMVPN Spoke-to-Spoke Communication L-56

Lab 3-1: Implement Site-to-Site Secure Connectivity Using Cisco IOS FlexVPN ***L-63***

Visual Objective L-64
Required Resources L-64
Command List L-64
Job Aids L-65
Task 1: Implement Point-to-Point FlexVPN Using Smart Defaults And Minimal Configuration L-69
Task 2: Modify Smart Defaults to Increase Protection Strength L-77
Task 3: Implement Point-to-Point FlexVPN Without Smart Defaults L-79
Task 4: Prepare PKI L-82
Task 5: Configure One Side for Certificate-Based Authentication L-87

Lab 3-2: Implement Hub-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN ***L-95***

Visual Objective L-96

https://t.me/learningnets

Required Resources L-96
Command List L-96
Job Aids L-97
Task 1: Configure Hub and Spoke for Virtual Access Connections L-101
Task 2: Configure Certificate-Based Authentication on Spoke L-109
Task 3: Configure Locally Managed Mode Config L-111
Task 4: Add a Second Flex VPN Spoke L-115

Lab 3-3: Implement Spoke-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN L-121

Visual Objective L-122
Required Resources L-122
Command List L-122
Job Aids L-123
Task 1: Configure BGP L-127
Task 2: Configure Spoke-to-Spoke Shortcut Switching L-133

Lab 4-1: Implement ASA Basic Clientless SSL VPN L-141

Visual Objective L-142
Required Resources L-142
Command List L-142
Job Aids L-142
Task 1: Enable Clientless SSL VPN Connections L-146
Task 2: Enroll ASA in PKI L-149
Task 3: Configure a Bookmark L-159

Lab 4-2: Configure Application Access for Cisco ASA Clientless SSL VPN L-167

Visual Objective L-168
Required Resources L-168
Job Aids L-168
Task 1: Configure Application Access Using Plugins L-172
Task 2: Configure Application Access Using Smart Tunnels L-180

Lab 4-3: Implement Local and External AAA for Clientless SSL VPNs L-185

Visual Objective: Local Authorization and External AAA for Clientless SSL VPNs L-186
Required Resources L-186
Job Aids L-186
Task 1: Configure Local Authorization L-190
Task 2: Enable RADIUS-Based Authentication and Authorization L-193
Task 3: Test External Authentication and Authorization L-199

Lab 5-1: Implement ASA Basic AnyConnect SSL VPN L-203

Visual Objective L-204
Required Resources L-204
Command List L-204
Job Aids L-204

 © 2014 Cisco Systems, Inc.

https://t.me/learningnets

Task 1: Install Client Certificate on Employee-PC and Move Employee-PC to SP Subnet L-208
Task 2: Enable AnyConnect SSL VPN Connections and Create a Local VPN User L-212
Task 3: Configure VPN IP Address Pool and Identity NAT L-213
Task 4: Configure Connection Profile L-217
Task 5: Configure Group Policy: IP Pool, DNS and Split Tunneling L-218
Task 6: Test AnyConnect SSL VPNs L-220

Lab 5-2: Configure Advanced Authentication for Cisco AnyConnect SSL VPN L-227

Visual Objective L-228
Required Resources L-228
Job Aids L-228
Task 1: Join the ISE to Active Directory L-232
Task 2: Deploy Certificate-Based Client Authentication L-234
Task 3: Deploy Two-Factor Client Authentication L-237
Task 4: Deploy Local Authorization for Local VPN Users L-242
Task 5: Deploy External Authorization L-244
Task 6: Deploy AnyConnect Profile To Allow AnyConnect VPNs from Remote Desktop L-247
Task 7: Deploy Standalone AnyConnect Client on Guest-PC L-252

Lab 5-3: Implement AnyConnect IPSec/IKEv2 L-257

Visual Objective L-258
Required Resources L-258
Job Aids L-258
Task 1: Deploy AnyConnect IPsec VPN Using WebLaunch L-262
Task 2: Deploy AnyConnect IPsec VPN Using Standalone AnyConnect Mobility Client (Optional) L-272

Lab 6-1: Implement Host Scan and DAP L-277

Visual Objective L-278
Required Resources L-278
Command List L-278
Job Aids L-278
Task 1: Enable Host Scan and Examine AntiSpyware Software on Employee-PC L-282
Task 2: Deploy DAP to Evaluate Endpoint Posture Status L-285
Task 3: Deploy Automatic Endpoint Remediation L-288
Task 4: Deploy AntiVirus Posture (Optional) L-292

Lab Answer Keys L-299

Lab 2-1: Implement Site-to-Site Secure Connectivity on the Cisco ASA L-299
Lab 2-2: Implement Cisco IOS Static VTI Point-to-Point Tunnel L-299
Lab 2-3: Implement DMVPN L-301
Lab 3-1: Implement Site-to-Site Secure Connectivity Using Cisco IOS FlexVPN L-307
Lab 3-2: Implement Hub-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN L-316
Lab 3-3: Implement Spoke-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN L-322
Lab 4-1: Implement ASA Basic Clientless SSL VPN L-324

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Lab 4-2: Configure Application Access for Cisco ASA Clientless SSL VPN L-324
Lab 4-3: Implement Local and External AAA for Clientless SSL VPNs L-325
Lab 5-1: Implement ASA Basic AnyConnect SSL VPN L-325
Lab 5-2: Configure Advanced Authentication for Cisco AnyConnect SSL VPN L-325
Lab 5-3: Implement AnyConnect IPSec/IKEv2 L-325
Lab 6-1: Implement Host Scan and DAP L-326

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Lab 2-1: Implement Site-to-Site Secure Connectivity on the Cisco ASA

Activity Objective

Complete this lab activity to practice what you learned.

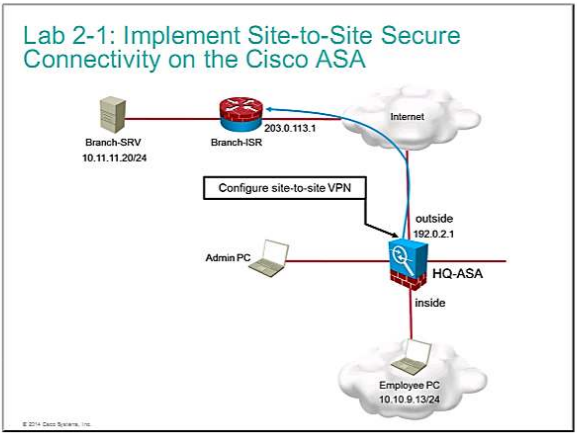
Upon completing this activity you will be able to meet these objectives:

- Implement an IPsec VPN tunnel on the Cisco ASA

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

The following equipment is required to complete this activity:

- Cisco ASA adaptive security appliance

Command List

All tasks are performed with the Cisco Adaptive Security Device Manager GUI interface. The table lists single command only. Cisco ASA command is necessary to complete verification of the lab.

Cisco ASA Command

Command	Description
show crypto ipsec sa	Verifies the status of the IPsec SAs.

Job Aids

These job aids are available to help you complete the lab activity.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

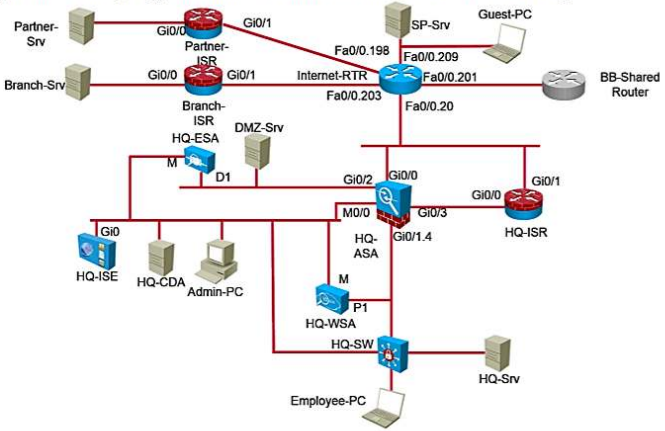
https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

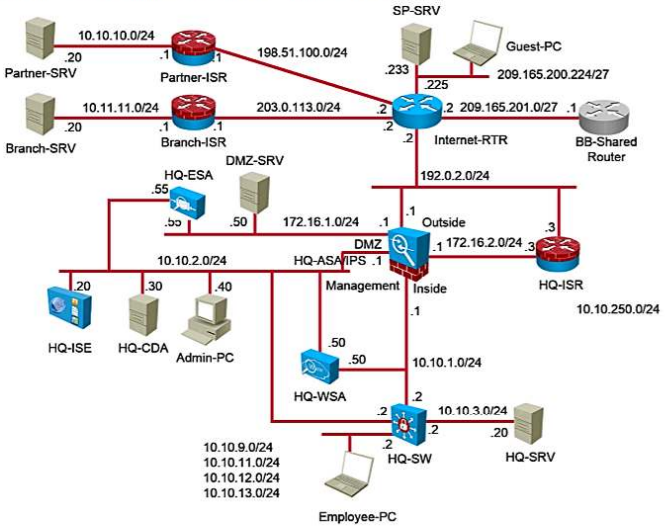
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



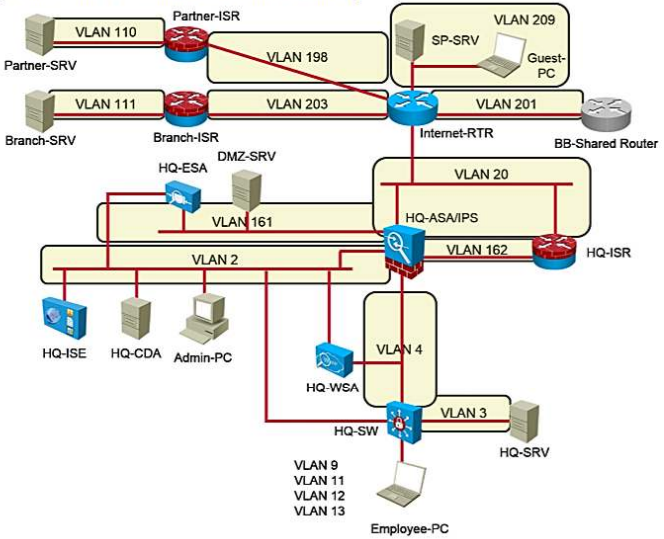
The figure shows the IP addresses that are used in this lab setup.



https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Configuring the Cisco ASA for Site-to-Site VPN

In this task, you will implement a site-to-site VPN configuration on the Cisco ASA security appliance to enable it to establish a site-to-site VPN with the **Branch-ISR** router. This will enable hosts at the branch office and hosts at headquarters to securely exchange data across the Internet. Hosts on each network will be able to access resources on the other network as if directly connected to the other private network, while benefiting from the functionality, security, and management policies of that private network.

The **Branch-ISR** router is pre-configured to support this lab exercise.

Activity Procedure

Complete the following steps:

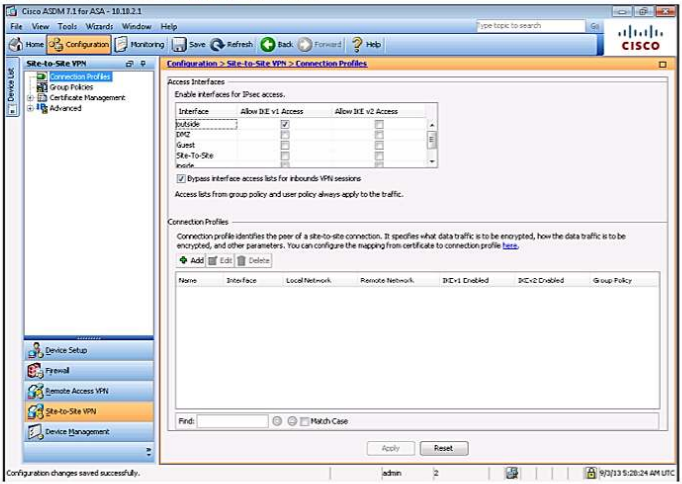
Step 1

From the Admin-PC desktop, access the Cisco ASDM on the **HQ-ASA** by double-clicking the **Cisco ASDM-IDM** Launcher icon. Log to the IP 10.10.2.1 in with the the username **admin** and the password **Ci5coAdmin**.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 2

In the Cisco ASDM, choose **Configuration > Site-to-Site VPN > Connection Profiles**. Check the **Allow IKEv1 Access** check box for the outside interface. This step ensures that IPsec is enabled on the appropriate interface of the Cisco ASA security appliance and that the desired version of IKE is used. The site-to-site VPN established in this lab uses IKEv1.



Step 3

Click the **Add** button to add a connection profile. The connection profile will identify the peer of the site-to-site connection. It will also specify what traffic is to be encrypted, how the traffic is to be encrypted, and other parameters.

Step 4

In the **Add IPsec Site-to-Site Connection Profile** window, insert the following parameters:

Peer IP Address: **203.0.113.1**

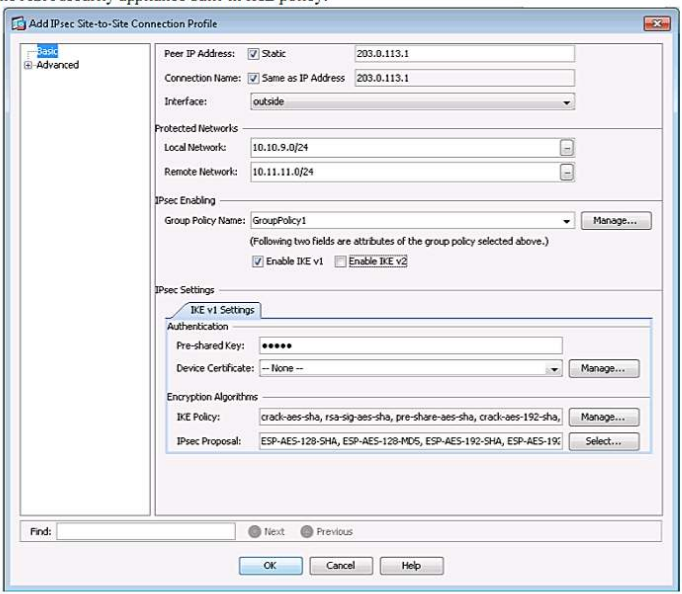
Local protected network: **10.10.9.0/24**

Remote protected network: **10.11.11.0/24**

Preshared key: **cisco**

Also uncheck the **Enable IKE v2** check box.

Use the ASA security appliance built-in IKE policy.



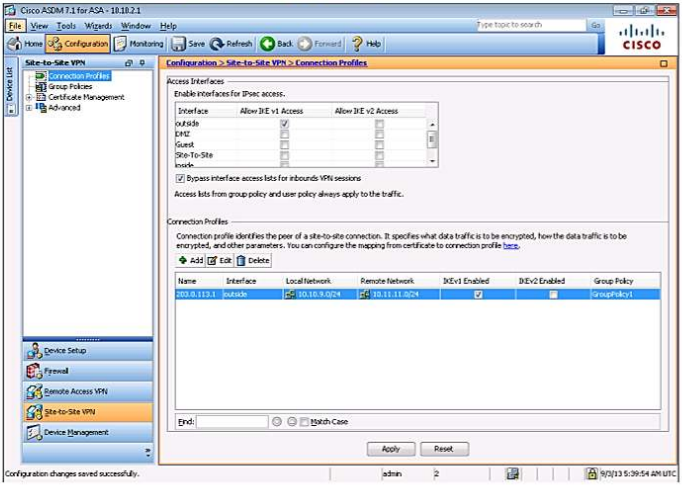
Step 5

Click **OK**. Your new connection profile should be displayed in the **Connection Profiles** area of the **Connection Profiles** pane.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 6

Click the **Apply** button to apply the changes to the **HQ-ASA**.



Step 7

Examine the commands that the Cisco ASDM will send to the **HQ-ASA** and then click the **Send** button.

```
access-list outside_cryptomap line 1 extended permit ip 10.10.9.0 255.255.255.0
10.11.11.0 255.255.255.0
group-policy GroupPolicy1 internal
group-policy GroupPolicy1 attributes
  vpn-tunnel-protocol ikev1
exit
tunnel-group 203.0.113.1 type ipsec-l2l
tunnel-group 203.0.113.1 general-attributes
  default-group-policy GroupPolicy1
tunnel-group 203.0.113.1 ipsec-attributes
  ikev1 pre-shared-key **********
  isakmp keepalive threshold 10 retry 2
crypto ikev1 policy 70
  encryption aes
  authentication crack
crypto ikev1 policy 80
  encryption aes
  authentication rsa-sig
crypto ikev1 policy 90
  encryption aes
crypto ikev1 policy 40
  encryption aes-192
  authentication crack
crypto ikev1 policy 50
  encryption aes-192
  authentication rsa-sig
crypto ikev1 policy 60
  encryption aes-192
crypto ikev1 policy 10
  encryption aes-256
  authentication crack
crypto ikev1 policy 20
  encryption aes-256
  authentication rsa-sig
crypto ikev1 policy 30
  encryption aes-256
crypto ikev1 policy 100
  authentication crack
crypto ikev1 policy 110
  authentication rsa-sig
crypto ikev1 policy 120
crypto ikev1 policy 130
  encryption des
  authentication crack
crypto ikev1 policy 140
  encryption des
  authentication rsa-sig
crypto ikev1 policy 150
  encryption des
crypto ikev1 enable  outside
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

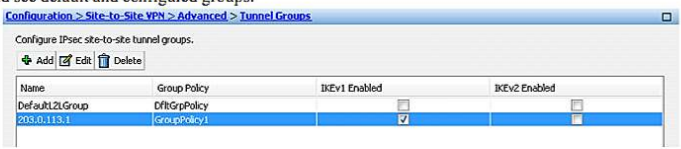
```
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS mode transport
crypto map outside_map0 1 match address outside_cryptomap
crypto map outside_map0 1 set  peer  203.0.113.1
crypto map outside_map0 1 set  ikev1 transform-set  ESP-AES-128-SHA ESP-AES-128-MD5
ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-
MD5 ESP-DES-SHA ESP-DES-MD5
crypto map outside_map0 interface  outside
```

Verification Procedure

In the activity procedure you configured PSK using **Connection profiles** in the Cisco ASDM. In this verification procedure, you will verify tunnel group setting using **Advanced** option in the Cisco ASDM:

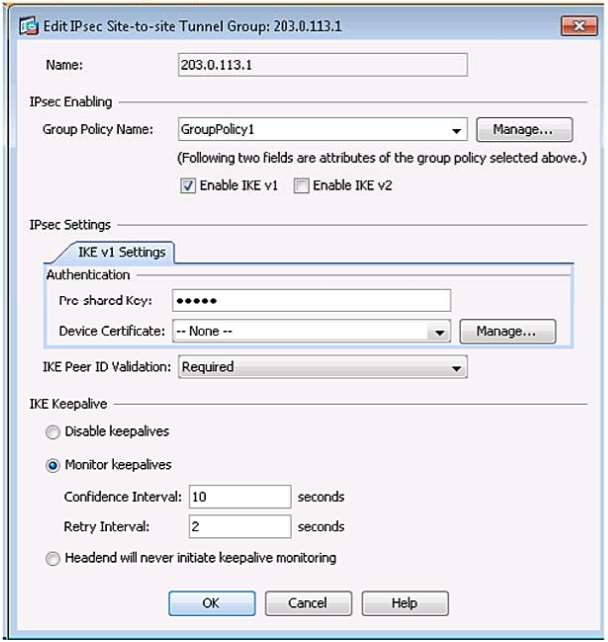
Step 1

In the Cisco ASDM, choose **Configuration > Site-to-Site VPN > Advanced > Tunnel Groups**. You should see default and configured groups.



Step 2

Select the tunnel group configured previously (**203.0.113.1**), and click the **Edit** button to see the tunnel group parameters. If the PSK is wrong, you can correct it here. Remember to click **OK** and apply changes to the HQ-ASA if you make any changes.



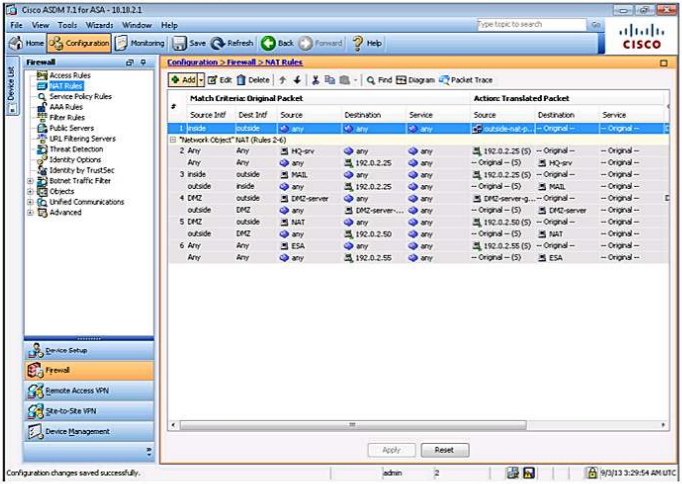
Task 2: Disabling NAT for Testing

In this task, you will disable the NAT rule on the **HQ-ASA**. This task is necessary for successful testing of the site-to-site VPN.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

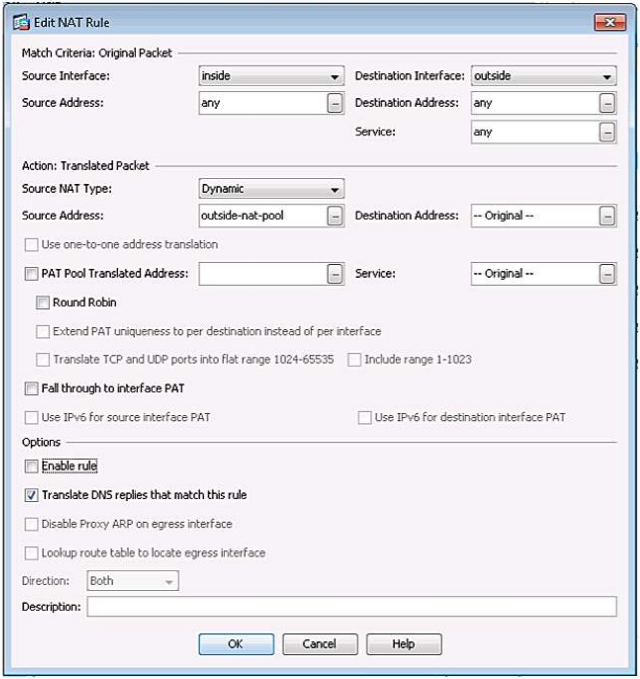
Step 1

In the Cisco ASDM, choose **Configuration > Firewall > NAT Rules**. Choose the NAT rule that uses the outside-nat-pool, and click the **Edit** button.



Step 2

In the **Edit NAT Rule** window, uncheck the **Enable rule** check box.



Step 3

Click **OK** and then click the **Apply** button to apply the changes to the **HQ-ASA**.

Step 4

Examine the commands that the Cisco ASDM will send to the **HQ-ASA** and then click the **Send** button.

```
nat (inside,outside) 1 source dynamic any outside-nat-pool dns inactive
```

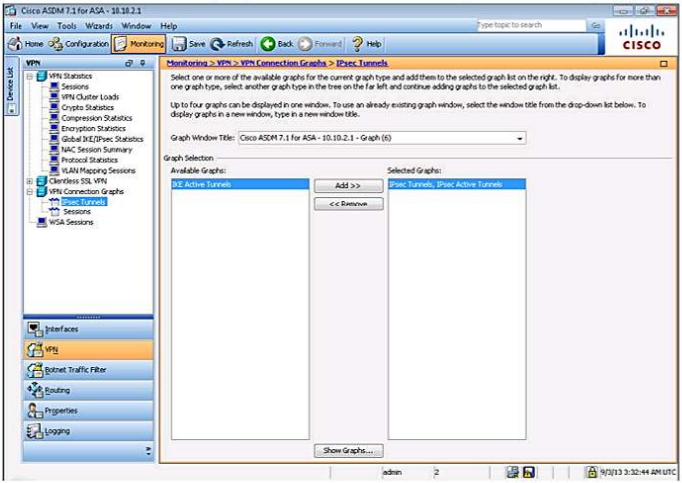

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Task 3: Verifying the Site-to-Site VPN

In this task, you will test the functionality of the VPN tunnel by verifying that the VPN tunnel has been established, by sending ICMP traffic through the tunnel, and by verifying that a host at the branch office can access a resource at headquarters via the tunnel.

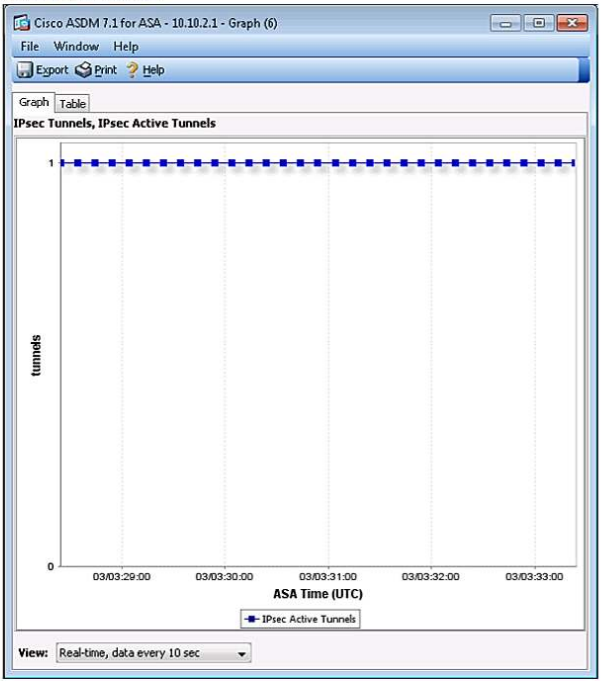
Step 1

In the Cisco ASDM opened to the **HQ-ASA**, choose **Monitoring > VPN > VPN Connection Graphs > IPsec Tunnels**. From the **Available Graphs** pane, choose **IPsec Active Tunnels**, and click the **Add >>** button to add it to the **Selected Graphs** pane. Then click the **Show Graphs...** button to display graphs.



Step 2

Verify that one tunnel is activated.

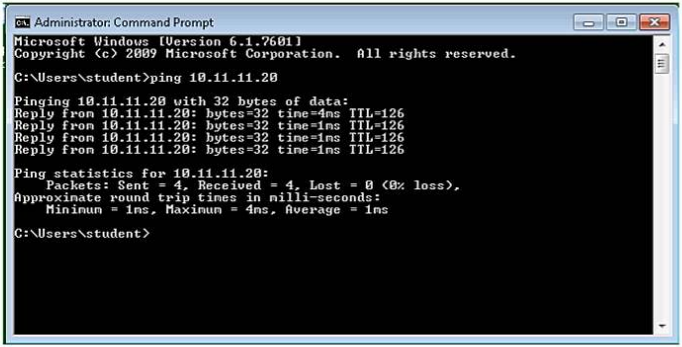


In the case tunnel is not activated, you will need to send some packets first, to trigger tunnel establishment. To trigger data via the tunnel, complete the next step first.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

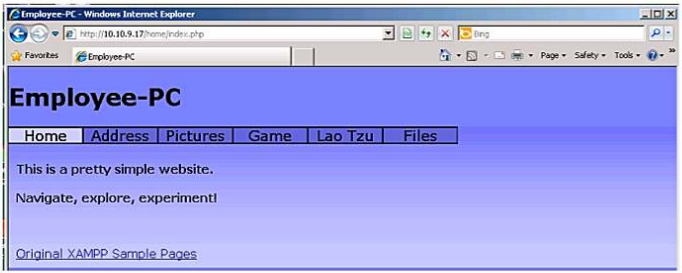
Step 3

From the Employee-PC, ping the Branch-Srv server IP address 10.11.11.20. The ping should be successful. Packets are passing through the site-to-site VPN tunnel established between the **HQ-ASA** and the **Branch-ISR** router.



Step 4

On the **Branch-Srv** server, open a web browser, and navigate to the web page at http://10.10.9.17. The attempt should be successful and you should see the web page of the **Employee-PC**. Do not close the browser.



Note If you are unable to access the web page of the **Employee-PC**, go to the **Employee-PC** and verify its IP address. Then navigate to the web page at http://<IP address of your Employee-PC>.

https://t.me/learningnets

Step 5

Access the CLI of **HQ-ASA**, and enter the **show crypto ipsec sa** command to display the IPsec SA. Note the number of encrypted and decrypted packets.

```
HQ-ASA# show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map0, seq num: 1, local addr: 192.0.2.1
      access-list outside_cryptomap extended permit ip 10.10.9.0 255.255.255.0
10.11.11.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.10.9.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.11.11.0/255.255.255.0/0/0)
      current_peer: 203.0.113.1
      #pkts encaps: 35, #pkts encrypt: 35, #pkts digest: 35
      #pkts decaps: 43, #pkts decrypt: 43, #pkts verify: 43
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 35, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 192.0.2.1/0, remote crypto endpt.: 203.0.113.1/0
      path mtu 1500, ipsec overhead 58(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 141E99CF
      current inbound spi : A9D6AC23
    inbound esp sas:
      spi: 0xA9D6AC23 (2849418275)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 12288, crypto-map: outside_map0
         sa timing: remaining key lifetime (kB/sec): (4373995/3089)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000FFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0x141E99CF (337549775)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 12288, crypto-map: outside_map0
         sa timing: remaining key lifetime (kB/sec): (4373988/3089)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

Step 6

Refresh the browser session on the **Branch-Srv** server.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 7

Return to the **HQ-ASA** CLI, and execute the **show crypto ipsec sa** command again. You should see an increased number of encrypted and decrypted packets.

```
HQ-ASA# show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map0, seq num: 1, local addr: 192.0.2.1
      access-list outside_cryptomap extended permit ip 10.10.9.0 255.255.255.0
10.11.11.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.10.9.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.11.11.0/255.255.255.0/0/0)
      current_peer: 203.0.113.1
      #pkts encaps: 45, #pkts encrypt: 45, #pkts digest: 45
      #pkts decaps: 63, #pkts decrypt: 63, #pkts verify: 63
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 45, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 192.0.2.1/0, remote crypto endpt.: 203.0.113.1/0
      path mtu 1500, ipsec overhead 58(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 141E99CF
      current inbound spi : A9D6AC23
    inbound esp sas:
      spi: 0xA9D6AC23 (2849418275)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 12288, crypto-map: outside_map0
         sa timing: remaining key lifetime (kB/sec): (4373993/2765)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0x141E99CF (337549775)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 12288, crypto-map: outside_map0
         sa timing: remaining key lifetime (kB/sec): (4373985/2765)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```


https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 2-2: Implement Cisco IOS Static VTI Point-to-Point Tunnel

Activity Objective

In the previous lab, you implemented a site-to-site VPN on the Cisco ASA security appliance. In this lab, you will implement a site-to-site VPN on a Cisco ISR router.

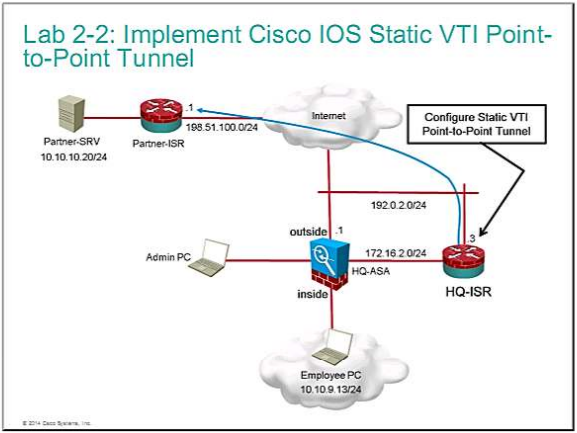
Upon completing this activity, you will be able to meet these objectives:

- Implement a Cisco IOS static VTI point-to-point tunnel
- Verify the configuration and operation of a static VTI point-to-point tunnel

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

Cisco IOS router

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Cisco IOS Commands

Command	Description
authentication pre-share	In the crypto policy configuration mode specifies authentication.
clear crypto sa counters	Resets all crypto SA counters.
crypto ipsec profile *profile-name*	Creates an IPsec profile and enters crypto profile configuration mode.
crypto ipsec transform-set *set-name* **esp-aes 128 esp-sha-hmac**	Creates an IPsec transform set for user traffic protection with AES encryption algorithm and SHA-1 hash algorithm.
crypto isakmp key key address peer-address	Creates a PSK and bind it to the IP address of the peer.
crypto isakmp policy *sequence*	Creates a new IKE policy and enters crypto policy configuration mode.
encr aes 128	In the crypto policy configuration mode specifies encryption algorithm.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Command	Description
group 14	In the crypto policy configuration mode specifies the key exchange method.
hash sha	In the crypto policy configuration mode specifies hash algorithm.
interface *Tunnel0*	Creates a new tunnel interface and enters tunnel interface configuration mode.
ip route *network mask interface*	Creates static routes to network reachable over the interface.
ip unnumbered *interface*	Assigns an IP subnet and address to the interface.
lifetime *lifetime*	In the crypto policy configuration mode specifies a lifetime.
ping *ip-destination* **source** *source-interface*	Verifies IP connectivity between local interface and remote IP destination.
set transform-set *set-name*	Configures nondefault transform set in the crypto profile.
show crypto ipsec sa	Verifies the status of the IPsec SAs.
show interface tunnel	Verifies the status of the local tunnel interface.
show ip route	Displays IP routes.
tunnel destination *IP-address*	Specifies a tunnel interface destination.
tunnel mode ipsec ipv4	Specifies the tunnel encapsulation as ipsec.
tunnel protection ipsec profile *profile-name*	Specifies the traffic protection policy by referencing the configured IPsec profile.
tunnel source *interface*	Specifies a tunnel interface source.

Job Aids

These job aids are available to help you complete the lab activity.

https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

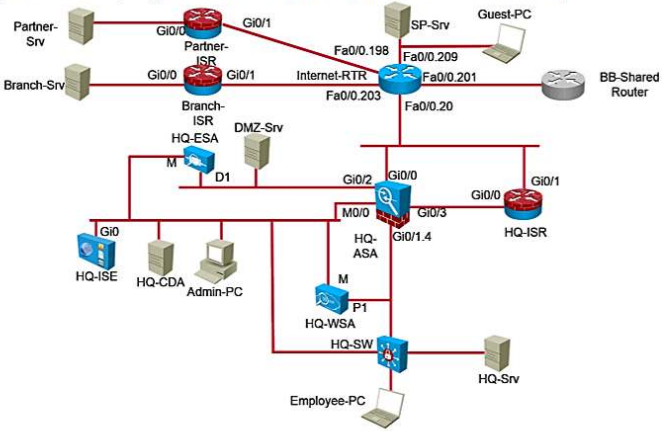
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

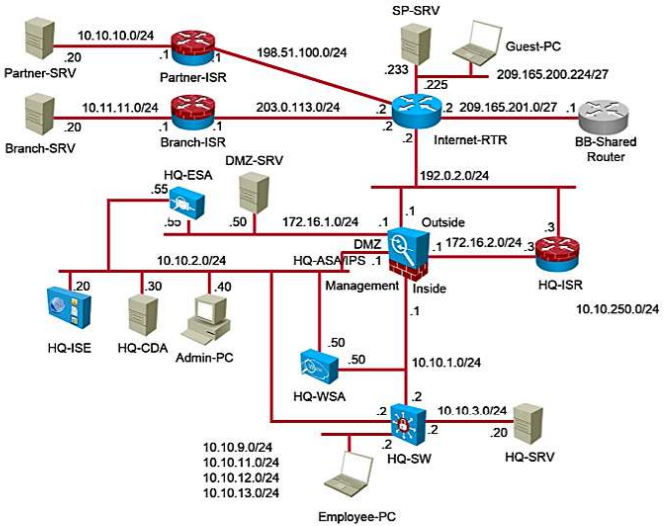
https://t.me/learningnets

Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



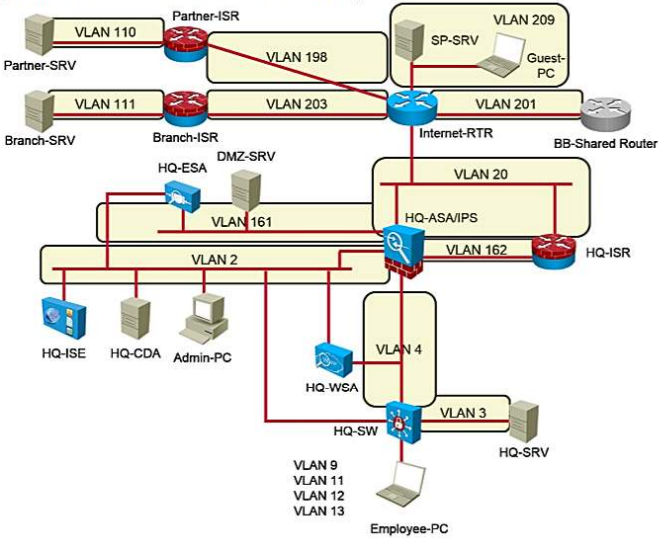
The figure shows the IP addresses that are used in this lab setup.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Configure Static VTI Point-to-Point Tunnel

In this task, you will implement a static VTI point-to-point tunnel configuration on the HQ-ISR router to enable it to establish a VTI point-to-point tunnel with the Partner-ISR router. This will enable hosts at the Partner office and hosts at Headquarters to securely exchange data across the Internet. Hosts on each network will be able to access resources on the other network as if directly connected to the other private network, while benefiting from the functionality, security, and management policies of that private network.

The Partner-ISR router is preconfigured to support this lab exercise.

Activity Procedure

Complete the following steps on the HQ-ISR router:

Step 1

Create a new IKE policy.

Specify the following parameters:

- Authentication method: **pre-shared**
- Encryption algorithm: **AES 128**
- Hash algorithm: **SHA**
- Key exchange method: **14**
- Lifetime: **1 hour**

Step 2

Create a PSK and bind it to the IP address of the Partner-ISR router (198.51.100.1).

Step 3

Create an IPsec transform set for user traffic protection. Use ESP with 128-bit AES as the encryption transform, and use ESP with SHA-1 (HMAC variant) as the authentication transform.

Step 4

Create an IPsec profile and include transform set in the profile.

Step 5

Create a new tunnel interface. Configure the interface to use the IP address and subnet of the Gi0/1 interface. Specify a tunnel source (Gi0/1) and a tunnel destination (198.51.100.1).

Step 6

Specify ipsec as the tunnel encapsulation. Specify the traffic protection policy by referencing the configured IPsec profile.

Step 7

Create a static route to the partner internal network (10.10.10.0/24) that is reachable over the tunnel.

Task 2: Verify Static VTI Point-to-Point Tunnel

In this task, you will verify the configuration and functionality of your static VTI point-to-point tunnel.

Activity Procedure

Complete the following steps:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 1

On the HQ-ISR router, verify the status of the IPsec SA. Notice that there are no packets encapsulated or de-encapsulated.

```
HQ-ISR# show crypto ipsec sa
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.0.2.3
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 198.51.100.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 192.0.2.3, remote crypto endpt.: 198.51.100.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0xBA3FBF1C(3124739868)
     PFS (Y/N): N, DH group: none
     inbound esp sas:
      spi: 0xEAAB50E1(3937095905)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: Onboard VPN:1, sibling_flags 80000040, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4210855/3471)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
      spi: 0x2F01DE5C(788651612)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000040, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4259715/3472)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x11A1D11E(295817502)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: Onboard VPN:2, sibling_flags 80000040, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4210855/3471)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
      spi: 0xBA3FBF1C(3124739868)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000040, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4259715/3472)
        IV size: 16 bytes
```


https://t.me/learningnets

```
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
    outbound ah sas:
    outbound pcp sas:
```

Step 2

On the HQ-ISR router, verify the status of the tunnel interface. The tunnel interface should be up/up.

```
HQ-ISR# show inter tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Interface is unnumbered. Using address of GigabitEthernet0/1 (192.0.2.3)
  MTU 17878 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 192.0.2.3 (GigabitEthernet0/1), destination 198.51.100.1
   Tunnel Subblocks:
      src-track:
         Tunnel0 source tracking subblock associated with GigabitEthernet0/1
          Set of tunnels with source GigabitEthernet0/1, 1 member (includes
iterators), on interface <OK>
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1438 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "MYPROFILE")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:02:24
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

On the HQ-ISR router, verify the routing table. Network 10.10.10.0/24 should be reachable via Tunnel0 interface.

```
HQ-ISR# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
Gateway of last resort is 192.0.2.2 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 192.0.2.2
      10.0.0.0/24 is subnetted, 8 subnets
O        10.10.1.0 [110/11] via 172.16.2.1, 1w6d, GigabitEthernet0/0
O        10.10.2.0 [110/12] via 172.16.2.1, 1w6d, GigabitEthernet0/0
O        10.10.3.0 [110/12] via 172.16.2.1, 1w6d, GigabitEthernet0/0
O        10.10.9.0 [110/12] via 172.16.2.1, 1w6d, GigabitEthernet0/0
S        10.10.10.0 is directly connected, Tunnel0
O        10.10.11.0 [110/12] via 172.16.2.1, 1w6d, GigabitEthernet0/0
O        10.10.12.0 [110/12] via 172.16.2.1, 1w6d, GigabitEthernet0/0
O        10.10.13.0 [110/12] via 172.16.2.1, 1w6d, GigabitEthernet0/0
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O        172.16.1.0/24 [110/11] via 172.16.2.1, 1w6d, GigabitEthernet0/0
C        172.16.2.0/24 is directly connected, GigabitEthernet0/0
L        172.16.2.3/32 is directly connected, GigabitEthernet0/0
      192.0.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.0.2.0/24 is directly connected, GigabitEthernet0/1
L        192.0.2.3/32 is directly connected, GigabitEthernet0/1
```

Step 4

From the HQ-ISR router Gi0/0 interface, ping 10.10.10.1 (Partner-ISR router internal IP). The ping should be successful.

```
HQ-ISR# ping 10.10.10.1 source GigabitEthernet 0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.2.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4
```


https://t.me/learningnets

Step 5

On the HQ-ISR router, verify the status of the IPsec SA again. Observe the packet count for encapsulated and de-encapsulated increase by five packets. The static VTI point-to-point tunnel interface is operational.

```
HQ-ISR# show crypto ipsec sa
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.0.2.3
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 198.51.100.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 192.0.2.3, remote crypto endpt.: 198.51.100.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0xC84AF165(3360354661)
     PFS (Y/N): N, DH group: none
     inbound esp sas:
      spi: 0xBD9089C8(3180366280)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: Onboard VPN:1, sibling_flags 80000040, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4153733/471)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0xC84AF165(3360354661)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: Onboard VPN:2, sibling_flags 80000040, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4153745/471)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:
     outbound pcp sas:
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 6

On the Employee-PC, open a browser and navigate to the web page at http://10.10.10.20. The attempt should be successful and you should see the web page of the Partner-SRV server.



https://t.me/learningnets

Step 7

On the HQ-ISR router, verify the status of the IPsec SA again. Notice that the packet count for encapsulated and de-encapsulated increases again.

```
HQ-ISR# show crypto ipsec sa
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.0.2.3
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 198.51.100.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 23, #pkts encrypt: 23, #pkts digest: 23
    #pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 192.0.2.3, remote crypto endpt.: 198.51.100.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0xC84AF165(3360354661)
     PFS (Y/N): N, DH group: none
     inbound esp sas:
      spi: 0xBD9089C8(3180366280)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: Onboard VPN:1, sibling_flags 80000040, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4153735/715)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0xC84AF165(3360354661)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: Onboard VPN:2, sibling_flags 80000040, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4153747/715)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:
     outbound pcp sas:
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Lab 2-3: Implement DMVPN

Complete this lab activity to practice what you learned in the related module. In this lab, you will configure a spoke-to-spoke DMVPN deployment model. The **HQ-ISR** router will serve as the DMVPN hub, and the **Partner-ISR** and **Branch-ISR** routers will function as the DMVPN spokes. The DMVPN spoke routers will dynamically peer and establish optimal routing paths.

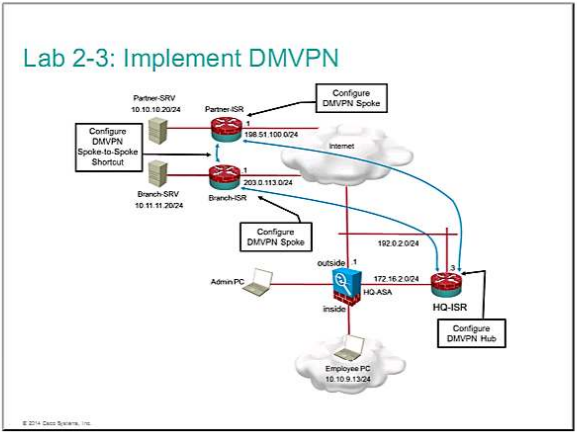
Upon completing this activity, you will be able to meet these objectives:

- Configure DMVPN hub
- Configure DMVPN spoke
- Configure OSPF routing in DMVPN
- Verify DMVPN hub and spoke operation
- Configure DMVPN spoke to spoke communication
- Verify DMVPN spoke to spoke communication

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

Cisco IOS router

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Cisco IOS Commands

Command	Description
authentication pre-share	In the crypto policy configuration mode specifies authentication.
crypto ipsec profile *profile-name*	Creates an IPsec profile and enters crypto profile configuration mode.
crypto ipsec transform-set *set-name* **esp-aes esp-sha-hmac**	Creates an IPsec transform set for user traffic protection with AES encryption algorithm and SHA-1 hash algorithm.
crypto isakmp key *key* **address** *peer-address*	Creates a PSK and bind it to the IP address of the peer.
crypto isakmp policy *sequence*	Creates a new IKE policy and enters crypto policy configuration mode.
encr aes 256	In the crypto policy configuration mode specifies encryption algorithm.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Command	Description
group 14	In the crypto policy configuration mode specifies the key exchange method.
hash sha384	In the crypto policy configuration mode specifies hash algorithm.
interface Tunnel *tunnel-id*	Creates a new tunnel interface and enters tunnel interface configuration mode.
ip address *ip-address subnet-mask*	Assigns an IP subnet and address to the interface.
ip mtu *bytes*	Sets the MTU size of IP packets that are sent on an interface.
ip nhrp authentication *string*	Configures the authentication string for an interface using the NHRP.
ip nhrp map *ip-address nbma-address*	Statically configure the IP-to- NBMA address mapping of IP destinations that are connected to an NBMA network.
ip nhrp map multicast dynamic | *nbma-address*	Configures NBMA addresses used as destinations for broadcast or multicast packets to be sent over a tunnel network
ip nhrp network-id *id-number*	Enables the NHRP on an interface.
ip nhrp nhs *nhs-address*	Specifies the address of one or more NHRP servers.
ip ospf network point-to-multipoint | broadcast	Configures OSPF network type to the interface.
ip ospf priority *priority*	Sets OSPF priority to the interface.
ip tcp adjust-mss *max-segment-size*	Adjusts the MSS value of TCP synchronize/start (SYN) packets going through a router.
mode transport	Enables IPsec in transport mode.
network *network wildcard* **area** *area*	Enables OSPF routing for the network.
ping *ip-destination*	Determines if other IP addresses are accessible.
router ospf *process-id*	Configures OSPF routing process and enters OSPF routing process configuration mode.
set transform-set *set-name*	Configures nondefault transform set in the crypto profile.
show crypto ipsec sa	Verifies the status of the IPsec SAs.
show crypto isakmp sa	Displays current IKE SAs.
show interface tunnel	Verifies the status of the local tunnel interface.
show ip ospf neighbor	Displays neighbors that are discovered by OSPF.
show ip route ospf	Displays OSPF routes in the routing table.
traceroute *ip-address*	Traces IP destination.
tunnel key *key*	Enables an ID key for a tunnel interface.
tunnel mode gre multipoint	Specifies the tunnel encapsulation as GRE multipoint.
tunnel protection ipsec profile *profile-name*	Specifies the traffic protection policy by referencing the configured IPsec profile.
tunnel source *interface*	Specifies a tunnel interface source.

https://t.me/learningnets

Job Aids

These job aids are available to help you complete the lab activity.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

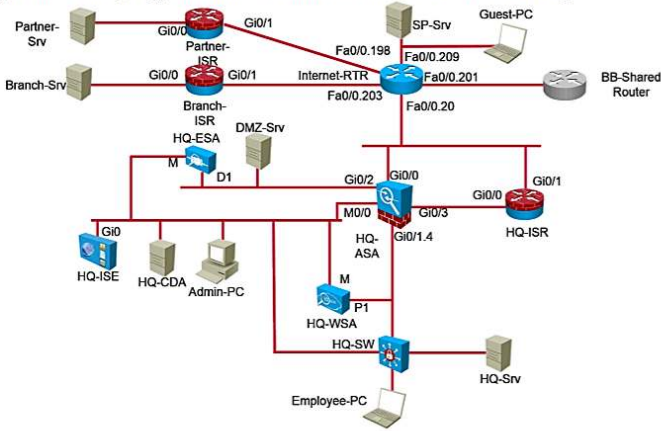
https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

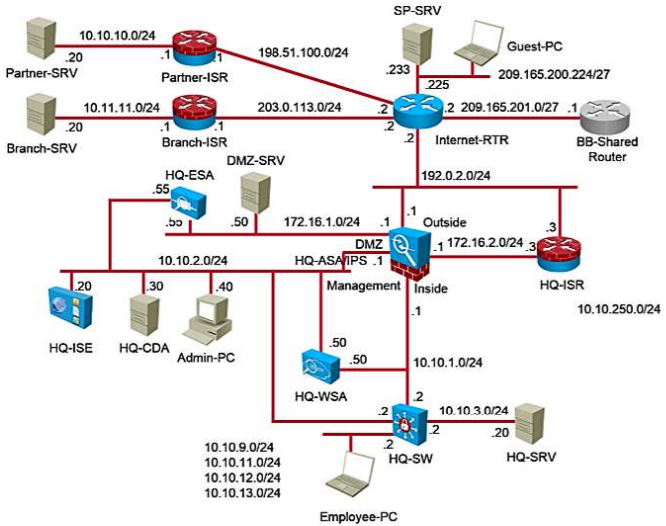
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.

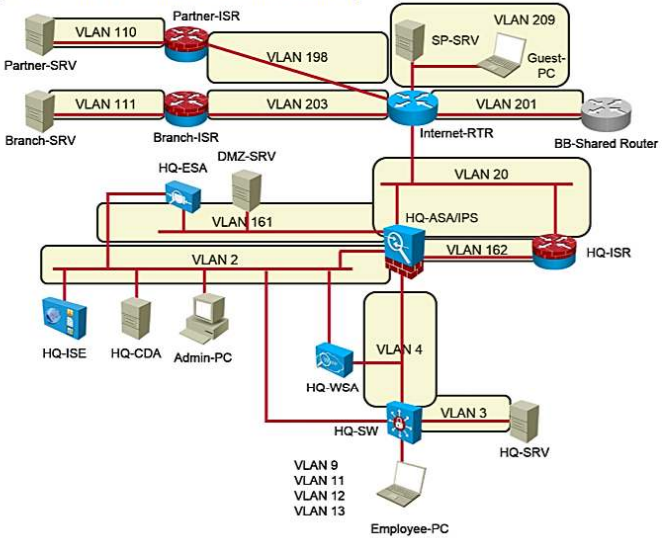


The figure shows the IP addresses that are used in this lab setup.



VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Configure a DMVPN Hub

In this task, you will configure the HQ-ISR router as the DMVPN hub router.

Activity Procedure

Complete the following steps on the HQ-ISR router:

Step 1

On the **HQ-ISR** router create a new IKE policy. Routers connecting with DMVPN will use PSK for authentication.

Use following parameters for IKE policy:

Encryption: **AES 256**

Hash algorithm: **SHA 384**

Authentication: **Pre-shared key**

Key exchange method: **14**

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 2

On the HQ-ISR router, remove the binding of the PSK **cisco** to IP address 198.51.100.1, which you configured in a previous lab.

Step 3

On the **HQ-ISR** router, create a PSK and bind it to the IP addresses of the **Branch-ISR** and **Partner-ISR** routers.

Use following PSKs:

Bind **Branch-ISR** IP address **203.0.113.1** to the PSK: **ccnpsecDMVPN**

Bind **Partner-ISR** IP address **198.51.100.1** to the PSK: **ccnpsecDMVPN**

Step 4

On the **HQ-ISR** router, create an IPsec profile named **MYIPSECPROFILE** and a transform set named **MYSET**. Include the **MYSET** transform set in the profile.

Use following parameters for transform set:

ESP transform using AES cipher

ESP transform using HMAC-SHA authentication

Transport mode

Step 5

On the **HQ-ISR** router create a new point-to-multipoint GRE interface.

Use following parameters for GRE interface:

Tunnel interface number: **1**

Tunnel mode: **gre multipoint**

Tunnel source: **Gi0/1 interface**

Tunnel key: **12345**

Step 6

On the **HQ-ISR** router, configure NHRP server parameters in the mGRE interface.

Use following NHRP parameters:

NHRP network ID: **1**

NHRP authentication string: **NHRP**

NHRP multicast addresses: **dynamically learned**

https://t.me/learningnets

Step 7

On the **HQ-ISR** router assign the configured IPsec profile to the mGRE interface.

Step 8

On the **HQ-ISR** router enable IP processing on the Tunnel 1 interface by assigning IP address 10.1.1.1/24 to the interface.

Step 9

On the **HQ-ISR** router Tunnel 1 interface, adjust MTU and TCP MSS to avoid fragmentation of GRE and IPsec packets.

Use following parameters:

Interface MTU: **1400**

TCP MSS: **1360**

Step 10

On the **HQ-ISR** router delete Tunnel 0 interface.

Task 2: Configure a DMVPN Spokes

In this task, you will configure the **Branch-ISR** and **Partner-ISR** routers as the DMVPN spoke routers. The DMVPN spoke routers will communicate only via DMVPN hub router.

Activity Procedure

Complete the following steps on the **Branch-ISR** and **Partner-ISR** routers:

Step 1

On the **Branch-ISR** and **Partner-ISR** routers create a new IKE policy. Routers connecting with DMVPN will use PSK for authentication.

Use following parameters for IKE policy:

Encryption: **AES 256**

Hash algorithm: **SHA 384**

Authentication: **Pre-shared key**

Key exchange method: **14**

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 2

On the **Branch-ISR** router create a PSK and bind it to the IP address of the **HQ-ISR** router.

Use following PSK:

Bind **HQ-ISR** IP address **192.0.2.3** to the PSK: **ccnpsecDMVPN**

Step 3

On the Partner-ISR router, remove the binding of the PSK **cisco** to IP address 192.0.2.3.

Step 4

On the **Partner-ISR** router create a PSK and bind it to the IP address of the **HQ-ISR** router.

Use following PSK:

Bind **HQ-ISR** IP address **192.0.2.3** to the PSK: **ccnpsecDMVPN**

Step 5

On the **Branch-ISR** and **Partner-ISR** routers, create an IPsec profile named **MYIPSECPROFILE** and a transform set named **MYSET**. Include the **MYSET** transform set in the profile.

Use following parameters for transform set:

ESP transform using AES cipher

ESP transform using HMAC-SHA authentication

Transport mode

Step 6

On the **Branch-ISR** and **Partner-ISR** routers create a new point-to-multipoint GRE interface.

Use following parameters for GRE interface:

Tunnel interface number: **1**

Tunnel mode: **gre multipoint**

Tunnel source: **Gi0/1 interface**

Tunnel key: **12345**

https://t.me/learningnets

Step 7

On the **Branch-ISR** and **Partner-ISR** routers create an instance of an NHRP client.

Use following NHRP parameters:

NHRP network ID: **1**

NHRP authentication string: **NHRP**

NHRP server IP address: **10.1.1.1**

NHRP multicast map: **192.0.2.3**

Step 8

On the **Branch-ISR** and **Partner-ISR** routers assign the configured IPsec profile to the mGRE interface.

Step 9

On the **Branch-ISR** and **Partner-ISR** routers enable IP processing on the Tunnel 1 interface by assigning IP address to the interface.

Use following IP addresses:

On the **Branch-ISR** Tunnel 1 interface: **10.1.1.2/24**

On the **Partner-ISR** Tunnel 1 interface: **10.1.1.3/24**

Step 10

On the **Branch-ISR** and **Partner-ISR** routers Tunnel 1 interface adjust MTU and TCP MSS to avoid fragmentation of GRE and IPsec packets.

Use following parameters:

Interface MTU: **1400**

TCP MSS: **1360**

Step 11

On the **Branch-ISR** router remove crypto map VPN-to-ASA from Gi0/1 interface.

Step 12

On the **Partner-ISR** router, delete the Tunnel 0 interface.

Task 3: Configure OSPF Routing in DMVPN

In this task, you will configure OSPF routing between the DMVPN hub and spoke routers. The OSPF routing will be configured so that the DMVPN spoke routers will communicate via the DMVPN hub router.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Activity Procedure

Complete the following steps:

Step 1

On the **HQ-ISR** router configure the Tunnel 1 interface with a OSPF point-to-multipoint network.

Step 2

On the **HQ-ISR** router enable OSPF area 0 on the Tunnel 1 interface.

Step 3

On the **Branch-ISR** and **Partner-ISR** routers configure the Tunnel 1 interface with a OSPF point-to-multipoint network.

Step 4

On the **Branch-ISR** and **Partner-ISR** routers enable OSPF area 0 on the Tunnel 1 interface.

Step 5

On the **Partner-ISR** router enable OSPF area 2 on the Gi0/0 interface.

Task 4: Verify DMVPN Hub and Spoke Operation

In this task, you will verify DMVPN hub and spoke operation.

Activity Procedure

Complete the following steps:

Step 1

On the **HQ-ISR** router verify ISAKMP SA. You should see two active sessions.

```
HQ-ISR# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.0.2.3       203.0.113.1     QM_IDLE           1043 ACTIVE
192.0.2.3       198.51.100.1    QM_IDLE           1044 ACTIVE
IPv6 Crypto ISAKMP SA
```


https://t.me/learningnets

Step 2

On the **HQ-ISR** router verify IPSEC SA. You should see two active sessions.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

```
HQ-ISR# show crypto ipsec sa

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.0.2.3

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.0.2.3/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (198.51.100.1/255.255.255.255/47/0)
   current_peer 198.51.100.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 19, #pkts encrypt: 19, #pkts digest: 19
    #pkts decaps: 16, #pkts decrypt: 16, #pkts verify: 16
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.0.2.3, remote crypto endpt.: 198.51.100.1
     path mtu 1500, ip mtu 1500, ip mtu idb (none)
     current outbound spi: 0x6D437A92(1833138834)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x31CC2592(835462546)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2121, flow_id: Onboard VPN:121, sibling_flags 80000000,
        crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4370554/3386)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x6D437A92(1833138834)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2122, flow_id: Onboard VPN:122, sibling_flags 80000000,
        crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4370553/3386)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.0.2.3/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (203.0.113.1/255.255.255.255/47/0)
   current_peer 203.0.113.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 22, #pkts encrypt: 22, #pkts digest: 22
    #pkts decaps: 37, #pkts decrypt: 37, #pkts verify: 37
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
```

```
local crypto endpt.: 192.0.2.3, remote crypto endpt.: 203.0.113.1
path mtu 1500, ip mtu 1500, ip mtu idb (none)
current outbound spi: 0x1690DAD6(378591958)
PFS (Y/N): N, DH group: none

inbound esp sas:
 spi: 0x75F5C1F5(1979040245)
   transform: esp-aes esp-sha-hmac ,
   in use settings ={Transport, }
   conn id: 2119, flow_id: Onboard VPN:119, sibling_flags 80000000,
   crypto map: Tunnel1-head-0
   sa timing: remaining key lifetime (k/sec): (4274618/3374)
   IV size: 16 bytes
   replay detection support: Y
   Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0x1690DAD6(378591958)
   transform: esp-aes esp-sha-hmac ,
   in use settings ={Transport, }
   conn id: 2120, flow_id: Onboard VPN:120, sibling_flags 80000000,
   crypto map: Tunnel1-head-0
   sa timing: remaining key lifetime (k/sec): (4274620/3374)
   IV size: 16 bytes
   replay detection support: Y
   Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

Step 3

On the **HQ-ISR** router verify OSPF neighbors. You should see two OSPF neighbors via Tunnel1 interface.

```
HQ-ISR# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
198.51.100.1      0   FULL/  -        00:01:36    10.1.1.3        Tunnel1
203.0.113.1       0   FULL/  -        00:01:53    10.1.1.2        Tunnel1
192.0.2.1         1   FULL/DR         00:00:37    172.16.2.1      GigabitEthernet0/0
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 4

On the **Branch-ISR** router verify OSPF routes in the routing table. You should see route from partner side (10.10.10.0/24) reachable via **HQ-ISR** (10.1.1.1).

```
Branch-ISR# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
Gateway of last resort is 203.0.113.2 to network 0.0.0.0
      10.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
O        10.1.1.1/32 [110/1000] via 10.1.1.1, 00:07:20, Tunnel1
O        10.1.1.3/32 [110/2000] via 10.1.1.1, 00:06:41, Tunnel1
O        10.10.1.0/24 [110/1011] via 10.1.1.1, 00:07:20, Tunnel1
O        10.10.2.0/24 [110/1012] via 10.1.1.1, 00:07:20, Tunnel1
O        10.10.3.0/24 [110/1012] via 10.1.1.1, 00:07:20, Tunnel1
O        10.10.9.0/24 [110/1012] via 10.1.1.1, 00:07:20, Tunnel1
O IA     10.10.10.0/24 [110/2001] via 10.1.1.1, 00:06:41, Tunnel1
O        10.10.11.0/24 [110/1012] via 10.1.1.1, 00:07:20, Tunnel1
O        10.10.12.0/24 [110/1012] via 10.1.1.1, 00:07:20, Tunnel1
O        10.10.13.0/24 [110/1012] via 10.1.1.1, 00:07:20, Tunnel1
      172.16.0.0/24 is subnetted, 2 subnets
O        172.16.1.0 [110/1011] via 10.1.1.1, 00:07:20, Tunnel1
O        172.16.2.0 [110/1001] via 10.1.1.1, 00:07:20, Tunnel1
```

Step 5

On the **Branch-ISR** router trace partner side internal IP address 10.10.10.1. You should see packet is routed via **HQ-ISR** router (10.1.1.1) as expected.

```
Branch-ISR# traceroute 10.10.10.1
Type escape sequence to abort.
Tracing the route to 10.10.10.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.1 0 msec 0 msec 0 msec
  2 10.1.1.3 4 msec 0 msec *
```

Task 5: Configure a DMVPN Spoke to Spoke Communication

In this task, you will configure the DMVPN spokes to communicate directly.

Activity Procedure

Complete the following steps:

Step 1

On the **Branch-ISR** router create additional PSK and bind it to the IP address of the **Partner-ISR** router.

Use following PSK:

Bind **Partner-ISR** IP address **198.51.100.1** to the PSK: **ccnpsecDMVPN**

Step 2

On the **Partner-ISR** router create additional PSK and bind it to the IP address of the **Branch-ISR** router.

Use following PSK:

Bind **Branch-ISR** IP address **203.0.113.1** to the PSK: **ccnpsecDMVPN**

Step 3

On the **HQ-ISR**, **Branch-ISR** and **Partner-ISR** routers configure the Tunnel 1 interface with a OSPF broadcast network.

On the **Branch-ISR** and **Partner-ISR** routers configure the Tunnel 1 interface with a OSPF priority 0. This means that only **HQ-ISR** router, with default OSPF priority 1, will be able to became designated router (DR).

Task 6: Verify DMVPN Spoke-to-Spoke Communication

In this task, you will verify DMVPN spoke to spoke direct communication.

Activity Procedure

Complete the following steps:

Step 1

On the **Branch-ISR** router, verify ISAKMP SA. You should see one active session.

```
Branch-ISR# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.0.2.3       203.0.113.1     QM_IDLE           1006 ACTIVE
IPv6 Crypto ISAKMP SA
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 2

On the **Branch-ISR** router,verify IPSEC SA. You should see one active session.

```
Branch-ISR# show crypto ipsec sa
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 203.0.113.1
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (203.0.113.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.0.2.3/255.255.255.255/47/0)
   current_peer 192.0.2.3 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 245, #pkts encrypt: 245, #pkts digest: 245
    #pkts decaps: 97, #pkts decrypt: 97, #pkts verify: 97
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 203.0.113.1, remote crypto endpt.: 192.0.2.3
     path mtu 1500, ip mtu 1500, ip mtu idb (none)
     current outbound spi: 0x75F5C1F5(1979040245)
     PFS (Y/N): N, DH group: none
     inbound esp sas:
      spi: 0x1690DAD6(378591958)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2011, flow_id: Onboard VPN:11, sibling_flags 80000000, crypto map:
Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4306112/2123)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x75F5C1F5(1979040245)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2012, flow_id: Onboard VPN:12, sibling_flags 80000000, crypto map:
Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4306091/2123)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:
     outbound pcp sas:
```


https://t.me/learningnets

Step 3

On the **Branch-ISR** router, verify OSPF neighbors. You should see one OSPF neighbor via Tunnel1 interface.

```
Branch-ISR# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.0.2.3         10  FULL/DR         00:00:39    10.1.1.1        Tunnel1
```

Step 4

On the **Branch-ISR** router, verify OSPF routes in the routing table. You should see route from partner side (10.10.10.0/24) reachable directly via **Partner-ISR** (10.1.1.3).

```
Branch-ISR# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
Gateway of last resort is 203.0.113.2 to network 0.0.0.0
      10.0.0.0/8 is variably subnetted, 12 subnets, 2 masks
O        10.10.1.0/24 [110/1011] via 10.1.1.1, 00:05:28, Tunnel1
O        10.10.2.0/24 [110/1012] via 10.1.1.1, 00:05:28, Tunnel1
O        10.10.3.0/24 [110/1012] via 10.1.1.1, 00:05:28, Tunnel1
O        10.10.9.0/24 [110/1012] via 10.1.1.1, 00:05:28, Tunnel1
O IA     10.10.10.0/24 [110/1001] via 10.1.1.3, 00:05:28, Tunnel1
O        10.10.11.0/24 [110/1012] via 10.1.1.1, 00:05:28, Tunnel1
O        10.10.12.0/24 [110/1012] via 10.1.1.1, 00:05:28, Tunnel1
O        10.10.13.0/24 [110/1012] via 10.1.1.1, 00:05:28, Tunnel1
      172.16.0.0/24 is subnetted, 2 subnets
O        172.16.1.0 [110/1011] via 10.1.1.1, 00:05:28, Tunnel1
O        172.16.2.0 [110/1001] via 10.1.1.1, 00:05:28, Tunnel1
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 5

On the **Branch-ISR** router, trace partner side internal IP address 10.10.10.1.

You should see only first response from **HQ-ISR** router (10.10.10.1), but other packets are routed directly to **Partner-ISR** router (10.1.1.3). Repeat **traceroute** command several times.

```
Branch-ISR# traceroute 10.10.10.1
Type escape sequence to abort.
Tracing the route to 10.10.10.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.1 0 msec
    10.1.1.3 0 msec 0 msec
Branch-ISR#traceroute 10.10.10.1
Type escape sequence to abort.
Tracing the route to 10.10.10.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.3 0 msec 0 msec *
```

Step 6

On the **Branch-ISR** router, verify ISAKMP SA again.You should see two active sessions. The **Branch-ISR** opened ISAKMP session to the **Partner-ISR** router.

```
Branch-ISR# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.0.2.3       203.0.113.1     QM_IDLE           1006 ACTIVE
203.0.113.1     198.51.100.1    QM_IDLE           1007 ACTIVE
IPv6 Crypto ISAKMP SA
```


https://t.me/learningnets

Step 7

On the **Branch-ISR** router, verify IPSEC SA again. You should see two active sessions. The **Branch-ISR** router opened IPSEC session to the **Partner-ISR** router.

```
Branch-ISR# show crypto ipsec sa

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 203.0.113.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (203.0.113.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (198.51.100.1/255.255.255.255/47/0)
   current_peer 198.51.100.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 203.0.113.1, remote crypto endpt.: 198.51.100.1
     path mtu 1500, ip mtu 1500, ip mtu idb (none)
     current outbound spi: 0x20E49A07(551852551)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x87ECF4B7(2280453303)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2013, flow_id: Onboard VPN:13, sibling_flags 80000000,
        crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4167654/3197)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x20E49A07(551852551)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2014, flow_id: Onboard VPN:14, sibling_flags 80000000,
        crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4167654/3197)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

```
protected vrf: (none)
local  ident (addr/mask/prot/port): (203.0.113.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (192.0.2.3/255.255.255.255/47/0)
current_peer 192.0.2.3 port 500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 407, #pkts encrypt: 407, #pkts digest: 407
 #pkts decaps: 175, #pkts decrypt: 175, #pkts verify: 175
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0

  local crypto endpt.: 203.0.113.1, remote crypto endpt.: 192.0.2.3
  path mtu 1500, ip mtu 1500, ip mtu idb (none)
  current outbound spi: 0x75F5C1F5(1979040245)
  PFS (Y/N): N, DH group: none

  inbound esp sas:
   spi: 0x1690DAD6(378591958)
     transform: esp-aes esp-sha-hmac ,
     in use settings ={Transport, }
     conn id: 2011, flow_id: Onboard VPN:11, sibling_flags 80000000,
     crypto map: Tunnel1-head-0
     sa timing: remaining key lifetime (k/sec): (4306100/1447)
     IV size: 16 bytes
     replay detection support: Y
     Status: ACTIVE(ACTIVE)

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0x75F5C1F5(1979040245)
     transform: esp-aes esp-sha-hmac ,
     in use settings ={Transport, }
     conn id: 2012, flow_id: Onboard VPN:12, sibling_flags 80000000,
     crypto map: Tunnel1-head-0
     sa timing: remaining key lifetime (k/sec): (4306067/1447)
     IV size: 16 bytes
     replay detection support: Y
     Status: ACTIVE(ACTIVE)

  outbound ah sas:

  outbound pcp sas:
```


https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 3-1: Implement Site-to-Site Secure Connectivity Using Cisco IOS FlexVPN

Activity Objective

In this lab exercise, you will configure Cisco IOS point-to-point FlexVPN between the Branch-ISR and HQ-ISR. The Cisco IOS FlexVPN technology offers an enhanced range of capabilities compared to previous IPsec implementations. Initially, you will implement the point-to-point tunnel with pre-shared key authentication and extensive use of smart defaults. In this way, you will minimize the required configuration. Next, you will disable the default values and explicitly define all IKEv2 and IPsec elements. The goal of the explicit IKEv2 and IPsec configuration is traffic protection strength. In the final phase, you will deploy a Cisco IOS-based CA and deploy asymmetric FlexVPN authentication. The Branch-ISR will continue using the pre-shared key while the HQ-ISR will use certificate-based authentication. The asymmetric authentication was not supported with traditional point-to-point IPsec solutions.

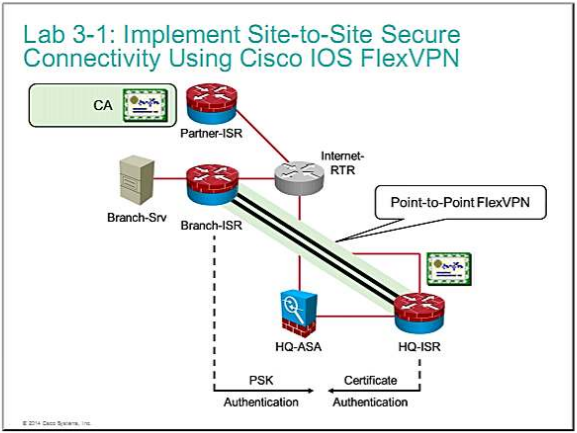
Upon completing this activity, you will be able to meet these objectives:

- Implement point-to-point FlexVPN using smart defaults and minimal configuration
- Modify smart defaults to increase protection strength
- Implement point-to-point FlexVPN without smart defaults
- Prepare the PKI for asymmetric FlexVPN authentication
- Configure one side for certificate-based authentication

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

Two Cisco IOS routers

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Commands

Command	Description
crypto pki trustpoint	Defines a PKI trustpoint that specifies how to obtain certificates
crypto ikev2 proposal	Defines an IKEv2 proposal that specifies the encryption, integrity algorithms, and DH group
[no] crypto ikev2 proposal default	Modifies (or disables) the default IKEv2 proposal
crypto ikev2 policy	Defines an IKEv2 policy that matches addresses or VRFs and chooses the IKEv2 proposal
[no] crypto ikev2 policy default	Modifies (or disables) the default IKEv2 policy
crypto ikev2 keyring	Configures an IKEv2 key ring

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile that specifies, among others, the local identity, matched remote identity, and authentication methods (local and remote)
[no] crypto ikev2 profile default	Modifies (or disables) the default IKEv2 profile
crypto ipsec transform-set	Configures an IPsec transform set
[no] crypto ipsec transform-set default	Modifies (or disables) the default IPsec transform set
crypto ipsec profile	Defines an IPsec profile that specifies the IKEv2 profile and IPsec transform set
[no] crypto ipsec profile default	Modifies (or disables) the default IPsec profile
tunnel protection ipsec profile	Applies an IPsec profile to a tunnel interface

Job Aids

These job aids are available to help you complete the lab activity.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

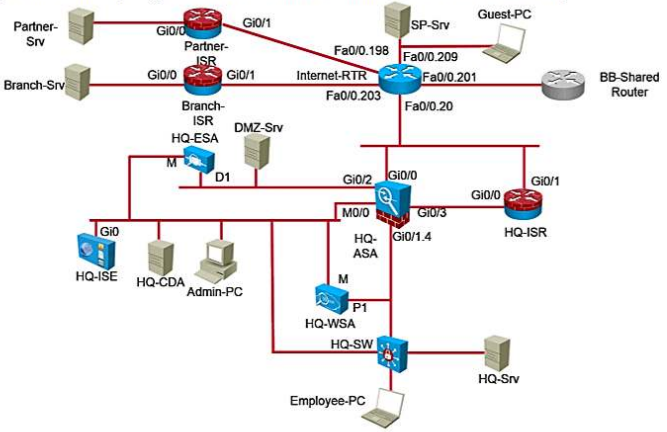
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

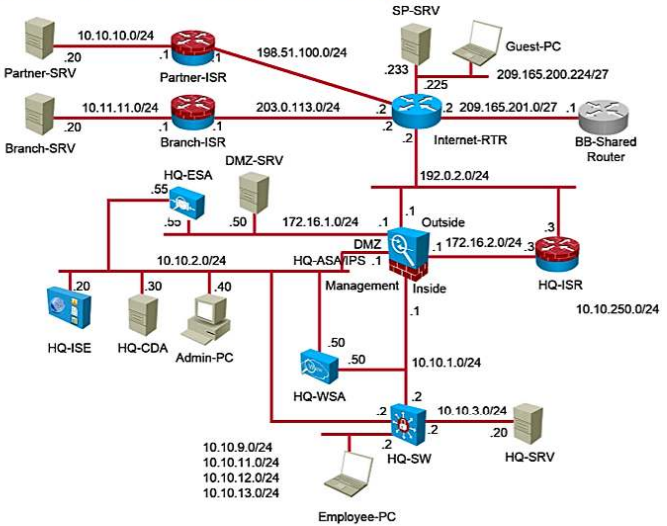
https://t.me/learningnets

Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



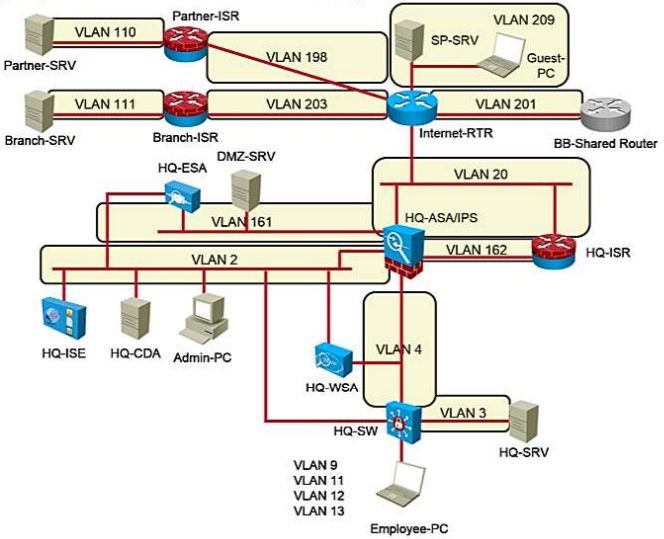
The figure shows the IP addresses that are used in this lab setup.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Implement Point-to-Point FlexVPN Using Smart Defaults And Minimal Configuration

In this task, you will configure a point-to-point IPsec FlexVPN with smart defaults and minimal pre-shared key configuration.

Note You will configure Cisco IOS point-to-point FlexVPN between the Branch-ISR and HQ-ISR. Initially, you will implement the point-to-point tunnel with pre-shared key authentication and extensive use of smart defaults. In this way, you will minimize the required configuration.

Activity Procedure

Complete the following steps:

Step 1

On Branch-ISR, configure a key ring (KR) that defines the peer (HQ-ISR):

Address: 192.0.2.3

Local and remote pre-shared key: cisco

Note	The construct names provided in parentheses (for example, KR) are examples. Using exactly the same values is not required but may help in the lab verification.

Step 2

On HQ-ISR, configure a mirrored key ring (KR) that defines the peer (Branch-ISR):

Address: 203.0.113.1

Local and remote pre-shared key: cisco

Note	In the next steps, you will configure the IKEv2 profile. The IKEv2 profile is used to define the local and remote authentication methods and the local IKEv2 identity. It is selected by matching the identity of the remote peer.

Step 3

On Branch-ISR, modify the smart default of the IKEv2 profile by setting these parameters:

Remote identity fqdn: hq-isr.secure-x.public

Local identity local fqdn: branch-isr.secure-x.public

Local and remote authentication: PSK

Keyring: KR (local)

Step 4

On HQ-ISR, modify the smart default of the IKEv2 profile in a mirrored fashion:

Remote identity fqdn: branch-isr.secure-x.public

Local identity local fqdn: hq-isr.secure-x.public

Local and remote authentication: PSK

Keyring: KR (local)

Note	In the next steps, you will configure Tunnel 0 between HQ-ISR and Branch-ISR routers and apply the default IPsec profile to the Tunnel 0 interface.

Step 5

On Branch-ISR and HQ-ISR, remove Tunnel 1 interface configured in previous lab exercise.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 6

On Branch-ISR and HQ-ISR, configure Tunnel 0 interface.

On the Branch-ISR router use following parameters:

Tunnel IP address: 10.10.100.1/24

Tunnel source IP: 203.0.113.1

Tunnel destination IP: 192.0.2.3

Tunnel mode: IPsec IPv4

On the HQ-ISR router use following parameters:

Tunnel IP address: 10.10.100.2/24

Tunnel source IP: 192.0.2.3

Tunnel destination IP: 203.0.113.1

Tunnel mode: IPsec IPv4

Step 7

On Branch-ISR and HQ-ISR, configure the Tunnel 0 interface to use the default IPsec profile.

Step 8

On Branch-ISR and HQ-ISR, configure the Tunnel 0 interface into OSPF area 0.

Note	In the next step, you will remove the remnants of the traditional VTI-based configuration. The removal has become possible after changing the tunnel protection to the default IPsec profile.

https://t.me/learningnets

Step 9

On Branch-ISR and HQ-ISR, delete the traditional crypto constructs, used for the VTI-based IPsec. They are not used in FlexVPN.

On Branch-ISR remove these elements:

crypto ipsec profile: MYIPSECPROFILE

crypto isakmp policy: 1 and 10

crypto isakmp key: cisco and ccnpsecDMVPN

crypto map: VPN-to-ASA

crypto ipsec transform-set: TSET and MYSET

Note	The order of deleting the constructs is important because they depend on each other. You should be able to delete these commands because the FlexVPN configuration is in place.

On HQ-ISR remove these elements:

crypto ipsec profile: MYIPSECPROFILE and MYPROFILE

crypto isakmp policy: 10

crypto isakmp key: ccnpsecDMVPN

crypto ipsec transform-set: MYSET

Activity Verification

You have completed this task when you attain these results:

Step 1

On Branch-ISR and HQ-ISR, verify that the IKEv2 SAs have been successfully negotiated.

```
Branch-ISR# show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA
Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         203.0.113.1/500       192.0.2.3/500         none/none            READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
      Life/Active Time: 86400/1610 sec
 IPv6 Crypto IKEv2  SA


HQ-ISR# show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA
Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.0.2.3/500         203.0.113.1/500       none/none            READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
      Life/Active Time: 86400/1698 sec
 IPv6 Crypto IKEv2  SA
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 2

On Branch-ISR and HQ-ISR, verify that the IPsec SAs have been successfully negotiated. The IKEv2 SA negotiation must be successful for the IPsec SAs to come up.

```
Branch-ISR# show crypto ipsec sa
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 203.0.113.1
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 192.0.2.3 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 214, #pkts encrypt: 214, #pkts digest: 214
    #pkts decaps: 194, #pkts decrypt: 194, #pkts verify: 194
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 203.0.113.1, remote crypto endpt.: 192.0.2.3
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0x378C47B4(931940276)
     PFS (Y/N): N, DH group: none
     inbound esp sas:
      spi: 0xE3048E6A(3808726634)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2082, flow_id: Onboard VPN:82, sibling_flags 80000040, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4266996/1763)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x378C47B4(931940276)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2081, flow_id: Onboard VPN:81, sibling_flags 80000040, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4266994/1763)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:
     outbound pcp sas:


HQ-ISR# show crypto ipsec sa
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.0.2.3
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 203.0.113.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 195, #pkts encrypt: 195, #pkts digest: 195
```


https://t.me/learningnets

```
    #pkts decaps: 215, #pkts decrypt: 215, #pkts verify: 215
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 192.0.2.3, remote crypto endpt.: 203.0.113.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0xE3048E6A(3808726634)
     PFS (Y/N): N, DH group: none
     inbound esp sas:
      spi: 0x378C47B4(931940276)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2137, flow_id: Onboard VPN:137, sibling_flags 80000040, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4251237/1754)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0xE3048E6A(3808726634)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2138, flow_id: Onboard VPN:138, sibling_flags 80000040, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4251239/1754)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:
     outbound pcp sas:
```

Step 3

On Branch-ISR and HQ-ISR, verify the OSPF adjacency established through the tunnel, and, optionally, other network connectivity. The negotiation of the IKEv2 and IPsec SAs must be successful before the tunnel can pass network traffic.

```
Branch-ISR# show ip ospf neighbor tunnel 0
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.0.2.3         0   FULL/  -        00:00:32    10.10.100.2     Tunnel0


HQ-ISR# show ip ospf neighbor tunnel 0
Neighbor ID     Pri   State           Dead Time   Address         Interface
203.0.113.1       0   FULL/  -        00:00:39    10.10.100.1     Tunnel0
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 4

On Branch-ISR and HQ-ISR, examine the smart defaults for the IPsec profile, IKEv2 profile, and IPsec transform set using appropriate **show** commands. You should see that that the default IPsec profile (applied to Tunnel 0) references the default IKEv2 profile and the default transform set.

```
Branch-ISR# show crypto ipsec profile
IPSEC profile default
        IKEV2 profile default
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                default:  { esp-aes esp-sha-hmac  } ,
        }
Branch-ISR# show crypto ikev2 profile
IKEv2 profile: default
 Ref Count: 4
 Match criteria:
  Fvrf: global
  Local address/interface: none
  Identities:
   fqdn hq-isr.secure-x.public
  Certificate maps: none
 Local identity: fqdn branch-isr.secure-x.public
 Remote identity: none
 Local authentication method: pre-share
 Remote authentication method(s): pre-share
 EAP options: none
 Keyring: KR
 Trustpoint(s): none
 Lifetime: 86400 seconds
 DPD: disabled
 NAT-keepalive: disabled
 Ivrf: none
 Virtual-template: none
 AAA EAP authentication mlist: none
 AAA Accounting: none
 AAA group authorization: none
 AAA user authorization: none

Branch-ISR# show crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },


HQ-ISR# show crypto ipsec profile
IPSEC profile default
        IKEV2 profile default
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                default:  { esp-aes esp-sha-hmac  } ,
        }
HQ-ISR# show crypto ikev2 profile
IKEv2 profile: default
 Ref Count: 4
 Match criteria:
```


https://t.me/learningnets

```
  Fvrf: global
  Local address/interface: none
  Identities:
   fqdn branch-isr.secure-x.public
  Certificate maps: none
 Local identity: fqdn hq-isr.secure-x.public
 Remote identity: none
 Local authentication method: pre-share
 Remote authentication method(s): pre-share
 EAP options: none
 Keyring: KR
 Trustpoint(s): none
 Lifetime: 86400 seconds
 DPD: disabled
 NAT-keepalive: disabled
 Ivrf: none
 Virtual-template: none
 AAA EAP authentication mlist: none
 AAA Accounting: none
 AAA group authorization: none
 AAA user authorization: none

HQ-ISR# show crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },
```

Step 5

On Branch-ISR and HQ-ISR, verify that the actual negotiated traffic protection parameters, displayed in the **show crypto ipsec sa** command, match the default transform set. The traffic protection with *esp-aes/esp-sha-hmac* can be found in the IPsec SAs in the inbound and outbound *esp* SAs.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 6

On Branch-ISR and HQ-ISR, examine the smart defaults for the IKEv2 policy and the IKEv2 proposal using appropriate **show** commands. You should see that that the default IKEv2 policy references the default IKEv2 proposal.

```
Branch-ISR# show crypto ikev2 policy
 IKEv2 policy : default
      Match fvrf : any
      Match address local : any
      Proposal    : default
Branch-ISR# show crypto ikev2 proposal
 IKEv2 proposal: default
     Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
     Integrity  : SHA512 SHA384 SHA256 SHA96 MD596
     PRF        : SHA512 SHA384 SHA256 SHA1 MD5
     DH Group   : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

```
HQ-ISR# show crypto ikev2 policy
 IKEv2 policy : default
      Match fvrf : any
      Match address local : any
      Proposal    : default
HQ-ISR# show crypto ikev2 proposal
 IKEv2 proposal: default
     Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
     Integrity  : SHA512 SHA384 SHA256 SHA96 MD596
     PRF        : SHA512 SHA384 SHA256 SHA1 MD5
     DH Group   : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

Step 7

On Branch-ISR and HQ-ISR, verify that the actual negotiated IKE protection parameters, displayed in the **show crypto ikev2 sa** command, match the first proposals in the default IKEv2 proposal.

Note	The IKEv2 policy is not referenced by any other constructs, such as IPsec or IKEv2 profile. It is used to define the proposals offered to peers when the defined criteria are met. The criteria in the default IKEv2 policy are any VRFs and any local interface addresses.

Task 2: Modify Smart Defaults to Increase Protection Strength

In this task, you will tune the FlexVPN smart defaults to achieve better protection.

Note	Having configured the FlexVPN with the smart defaults, you will now tune the smart default values to increase the traffic protection strength.

Activity Procedure

Complete the following steps:

https://t.me/learningnets

Step 1

On Branch-ISR and HQ-ISR, modify the default IKEv2 proposal to use a stronger Diffie-Hellman group, group 20. Use the following parameters:

For encryption: 256-bit CBC-mode AES

For integrity: SHA 512

For key exchange: DH group 20

Step 2

On Branch-ISR and HQ-ISR, modify the default IPsec transform set to use the Galois Counter Mode (GCM) encryption with key size of 256 bits.

Step 3

On Branch-ISR and HQ-ISR, modify the default IPsec profile to perform a Diffie-Hellman exchange with group 20 each time that the IKEv2 association times out (known as Perfect Forward Secrecy.)

Activity Verification

You have completed this task when you attain these results:

Step 1

On Branch-ISR, clear the IPsec SAs.

```
Branch-ISR# clear crypto sa
Branch-ISR#
```

Step 2

On Branch-ISR, examine the IKEv2 SAs. You should see that, in contrast to previous attributes, a stronger DH exchange (group 20) has been used to establish the SA:

```
Branch-ISR# show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA
Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         203.0.113.1/500       192.0.2.3/500         none/none            READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:20, Auth sign: PSK, Auth
verify: PSK
      Life/Active Time: 86400/128 sec
 IPv6 Crypto IKEv2  SA
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

On Branch-ISR, examine the IPsec SAs. You should see that, in contrast to previous protection, GCM is used to secure the traffic:

```
Branch-ISR# show crypto ipsec sa | include transform
        transform: esp-gcm 256 ,
        transform: esp-gcm 256 ,
```

Task 3: Implement Point-to-Point FlexVPN Without Smart Defaults

In this task, you will configure the point-to-point FlexVPN with the same protection strength, without the smart defaults. You will disable the smart default constructs.

Activity Procedure

Complete the following steps:

Step 1

On Branch-ISR, create a IKEv2 profile (**ccnp-ikev2-profile**). Configure it identically to the default IKEv2 profile.

Step 2

On HQ-ISR, create an IKEv2 profile (**ccnp-ikev2-profile**). Configure it identically to the default IKEv2 profile.

Step 3

On Branch-ISR and HQ-ISR, create an IKEv2 proposal (**ccnp-ike2-proposal**) with the strongest available encryption and integrity. Set the DH group to 20.

Step 4

On Branch-ISR and HQ-ISR, create an IKEv2 policy (**ccnp-ikev2-policy**) that references the custom proposal (**ccnp-ike2-proposal**) and matches any VRF.

Step 5

On Branch-ISR and HQ-ISR, create an IPsec transform set (**ccnp-ts**) that uses the Galois Counter Mode (GCM) with 256 bits key length.

https://t.me/learningnets

Step 6

On Branch-ISR and HQ-ISR, create an IPsec profile (**ccnp-ipsec-profile**) that uses PFS group 20, references the custom transform set (**ccnp-ts**) and the custom IKEv2 profile (**ccnp-ikev2-profile**).

Step 7

On Branch-ISR and HQ-ISR, apply the custom IPsec profile (**ccnp-ipsec-profile**) to the Tunnel 0 interface.

Step 8

On Branch-ISR and HQ-ISR, delete the smart defaults:

Default IPsec profile

Default IPsec transform set

Default IKEv2 policy

Default IKEv2 proposal

Default IKEv2 profile

Activity Verification

You have completed this task when you attain these results:

Step 1

On Branch-ISR, clear the IPsec SAs.

```
Branch-ISR# clear crypto sa
Branch-ISR#
```

Note	You will verify that the IKEv2 and IPsec SAs are successfully negotiated.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 2

On Branch-ISR, examine the existing IPsec profile and the IKEv2 profile. Validate your custom configuration.

```
Branch-ISR# show crypto ipsec profile
IPSEC profile ccnp-ipsec-profile
        IKEV2 profile ccnp-ikev2-profile
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): Y
        DH group:  group20
        Transform sets={
                ccnp-ts:  { esp-gcm 256  } ,
        }
IPSec profile default: disabled
Branch-ISR# show crypto ikev2 profile
IKEv2 profile: ccnp-ikev2-profile
 Ref Count: 4
 Match criteria:
  Fvrf: global
  Local address/interface: none
  Identities:
   fqdn hq-isr.secure-x.public
  Certificate maps: none
 Local identity: fqdn branch-isr.secure-x.public
 Remote identity: none
 Local authentication method: pre-share
 Remote authentication method(s): pre-share
 EAP options: none
 Keyring: KR
 Trustpoint(s): none
 Lifetime: 86400 seconds
 DPD: disabled
 NAT-keepalive: disabled
 Ivrf: none
 Virtual-template: none
 AAA EAP authentication mlist: none
 AAA Accounting: none
 AAA group authorization: none
 AAA user authorization: none
```

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

On Branch-ISR, examine the IKEv2 policy and the IKEv2 proposal. Validate your custom configuration.

```
Branch-ISR# show crypto ikev2 policy
 IKEv2 policy : ccnp-ikev2-policy
       Match fvrf : any
       Match address local : any
       Proposal    : ccnp-ike2-proposal
 IKEv2 policy : default Disabled
Branch-ISR# show crypto ikev2 proposal
 IKEv2 proposal: ccnp-ike2-proposal
      Encryption : AES-CBC-256
      Integrity  : SHA512
      PRF        : SHA512
      DH Group   : DH_GROUP_384_ECP/Group 20
 IKEv2 proposal: default Disabled
```

Task 4: Prepare PKI

In this task, you will prepare the PKI for asymmetric FlexVPN authentication. Branch-ISR will authenticate using pre-shared keys, and the HQ-ISR will authenticate using certificates.

Note	You will deploy a Cisco IOS-based CA and obtain appropriate certificates for the two headend routers. The Branch-ISR should continue using the pre-shared key, while the HQ-ISR should use certificate-based authentication. To serve this purpose, you will install the CA root certificate on both headend routers and obtain the identity certificate only for HQ-ISR.

Activity Procedure

Complete the following steps:

Note	In certificate-based authentication, the certificate validity period must be successfully validated. Synchronizing the system time using NTP is recommended as the best approach to ensure successful time validation.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 1

Configure NTP:

A) Synchronize the Internet-RTR via NTP to a public NTP server using the **ntp server 64.103.34.15 source FastEthernet0/0.20** command.

B) On Intemet-RTR, verify that NTP is synchronized.

```
Internet-RTR# show ntp status
Clock is synchronized, stratum 2, reference is 64.103.34.15
nominal freq is 249.5901 Hz, actual freq is 249.5866 Hz, precision is 2**18
reference time is D64B011C.469860DB (13:41:48.275 UTC Thu Dec 5 2013)
clock offset is 0.1928 msec, root delay is 171.45 msec
root dispersion is 1.75 msec, peer dispersion is 1.57 msec
```

C) On HQ-ISR, Partner-ISR, and Branch-ISR, configure the Internet-RTR as the NTP server, using the **ntp server 192.0.2.2** command.

D) On HQ-ISR, Partner-ISR, and Branch-ISR, verify that the NTP status becomes synchronized.

```
HQ-ISR# show ntp status
Clock is synchronized, stratum 3, reference is 192.0.2.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**21
ntp uptime is 6000 (1/100 of seconds), resolution is 4016
reference time is D64B01D2.2318580E (13:44:50.137 UTC Thu Dec 5 2013)
clock offset is 0.0150 msec, root delay is 173.38 msec
root dispersion is 3938.68 msec, peer dispersion is 187.57 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000003934 s/s
system poll interval is 64, last update was 55 sec ago.
```

Step 2

On Partner-ISR, start a CA:

A) Start the HTTP server.

B) Generate a RSA crypto key with the following settngs:

Modulus: 2048

Label: partner-ca.partner.public

C) Configure a PKI trustpoint (**local-ca**) with the following settings:

Rsakeypair: partner-ca.partner.public

Revocation check: none

D) Configure a PKI server (**Partner-CA**) with these settings:

Issuer name: CN=Partner-CA, O=partner.public

Database level: Minimum (default setting)

Hash method: SHA-256

Granting method: auto

E) Enable the PKI server using the **no shutdown** command. Enter a password (**cisco123**) twice to protect the private key.

https://t.me/learningnets

Note	In this lab scenario, you are using the Cisco IOS-based CA because it supports the SCEP. SCEP provides an easy-to-use method of enrolling network devices to the PKI. The Microsoft CA running on the HQ-srv does not support SCEP in the standard edition.

Step 3

On Branch-ISR, configure a PKI trustpoint (Partner-ISR) and obtain the CA root certificate from the Partner-ISR CA:

A) Enrollment URL: **http://198.51.100.1**

B) Revocation check: **none**

C) Request the CA root certificate, and confirm its fingerprint.

Note	You do not generate an RSA key pair and do not obtain a certificate for the Branch-ISR. Download the CA root certificate to be able to validate the HQ-ISR certificate.

Step 4

Enroll the HQ-ISR with the CA running on Partner-ISR.

A) Generate an RSA key pair with label hq-isr.secure-x.public and modulus 2048.

B) Configure a trustpoint (Partner-ISR) with these attributes:

- **RSA keypair: hq-isr.secure-x.public**
- **Enrollment URL: Partner-ISR IP address (http://198.51.100.1)**
- **FQDN: hq-isr.secure-x.public**
- **Subject name: CN=hq-isr,O=secure-x.public**
- **Revocation check: none**
- **No serial-number**
- **No ip-address**

C) Obtain the CA root certificate using the **crypto pki authenticate** command in the configuration mode. Accept the certificate.

D) Request the identity certificate for HQ-ISR using the **crypto pki enroll** command. Enter a challenge password (**cisco**). Confirm the request and accept the certificate, which should be granted automatically as a result of the grant auto configuration on the Partner-ISR CA.

Note	On HQ-ISR, you request two certificates from the CA (Partner-ISR): the CA root certificate, and an identity certificate for HQ-ISR. HQ-ISR will authenticate to the Branch-ISR using the identity certificate. Branch-ISR will validate the HQ-ISR identity certificate using the CA root certificate.

Activity Verification

You have completed this task when you attain these results:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 1

On Branch-ISR and HQ-ISR, view the root CA certificate:

```
Branch-ISR# show crypto pki certificates
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=Partner-CA
    o=partner.public
  Subject:
    cn=Partner-CA
    o=partner.public
  Validity Date:
    start date: 08:59:53 UTC Dec 6 2013
    end   date: 08:59:53 UTC Dec 5 2016
  Associated Trustpoints: partner-isr


HQ-ISR# show crypto pki certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 02
  Certificate Usage: General Purpose
  Issuer:
    cn=Partner-CA
    o=partner.public
  Subject:
    Name: hq-isr.secure-x.public
    hostname=hq-isr.secure-x.public
    cn=hq-isr
    o=secure-x.public
  Validity Date:
    start date: 09:07:23 UTC Dec 6 2013
    end   date: 09:07:23 UTC Dec 6 2014
  Associated Trustpoints: partner-isr
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=Partner-CA
    o=partner.public
  Subject:
    cn=Partner-CA
    o=partner.public
  Validity Date:
    start date: 08:59:53 UTC Dec 6 2013
    end   date: 08:59:53 UTC Dec 5 2016
  Associated Trustpoints: partner-isr
Router Self-Signed Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: General Purpose
  Issuer:
    cn=IOS-Self-Signed-Certificate-1158639554
  Subject:
    Name: IOS-Self-Signed-Certificate-1158639554
    cn=IOS-Self-Signed-Certificate-1158639554
```


https://t.me/learningnets

```
  Validity Date:
    start date: 11:04:34 UTC Aug 8 2013
    end   date: 00:00:00 UTC Jan 1 2020
  Associated Trustpoints: TP-self-signed-1158639554
  Storage: nvram:IOS-Self-Sig#9.cer
```

Step 2

On HQ-ISR, view the root CA certificate and the HQ-ISR identity certificate:

```
HQ-ISR# show crypto pki certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 02
  Certificate Usage: General Purpose
  Issuer:
    cn=Partner-CA
    o=partner.public
  Subject:
    Name: hq-isr.secure-x.public
    hostname=hq-isr.secure-x.public
    cn=hq-isr
    o=secure-x.public
  Validity Date:
    start date: 09:07:23 UTC Dec 6 2013
    end   date: 09:07:23 UTC Dec 6 2014
  Associated Trustpoints: partner-isr
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=Partner-CA
    o=partner.public
  Subject:
    cn=Partner-CA
    o=partner.public
  Validity Date:
    start date: 08:59:53 UTC Dec 6 2013
    end   date: 08:59:53 UTC Dec 5 2016
  Associated Trustpoints: partner-isr
Router Self-Signed Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: General Purpose
  Issuer:
    cn=IOS-Self-Signed-Certificate-1158639554
  Subject:
    Name: IOS-Self-Signed-Certificate-1158639554
    cn=IOS-Self-Signed-Certificate-1158639554
  Validity Date:
    start date: 11:04:34 UTC Aug 8 2013
    end   date: 00:00:00 UTC Jan 1 2020
  Associated Trustpoints: TP-self-signed-1158639554
  Storage: nvram:IOS-Self-Sig#9.cer
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Task 5: Configure One Side for Certificate-Based Authentication

In this task, you will implement certificate-based authentication of the HQ-ISR. The Branch-ISR will continue to authenticate to the HQ-ISR using the pre-shared key.

Note Asymmetric authentication methods, such as a mix of pre-shared keys and RSA encryption, or different pre-shared keys, are supported in FlexVPN and have not been supported in earlier methods. In this scenario, Branch-ISR will continue using the pre-shared key, while the HQ-ISR will use certificate-based authentication. If you wanted to deploy symmetric authentication, you would use mirrored copies of only one part of the configuration.

Activity Procedure

Complete the following steps:

Step 1

On Branch-ISR, modify the IKEv2 configuration to enable asymmetric authentication:

A) Delete the remote key from the key ring.

B) Configure the IKEv2 profile to use remote authentication based on certificates.

Step 2

On HQ-ISR, modify the configuration to enable asymmetric authentication:

A) Delete the local key from the key ring.

B) Configure the IKEv2 profile to use RSA signatures as the local authentication and use the trustpoint (Partner-ISR) to generate the fingerprint.

Activity Verification

You have completed this task when you attain these results:

Step 1

On Branch-ISR, clear the IPsec and IKEv2 SAs.

```
Branch-ISR# clear crypto ikev2 sa
Branch-ISR# clear crypto sa
Branch-ISR#
```


https://t.me/learningnets

Step 2

On Branch-ISR, examine the IKEv2 SAs. Notice that different types of authentications are used locally (Auth sign: PSK) and remotely (Auth verify: RSA). The Branch-ISR is using the pre-shared key, while the HQ-ISR is using certificate-based authentication.

```
Branch-ISR# show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA
Tunnel-id Local                 Remote                fvrf/ivrf             Status
1         203.0.113.1/500       192.0.2.3/500         none/none             READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:20, Auth sign: PSK, Auth
verify: RSA
      Life/Active Time: 86400/6 sec
 IPv6 Crypto IKEv2  SA
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

On Branch-ISR, examine the IPsec SAs.

```
Branch-ISR# show crypto ipsec sa
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 203.0.113.1
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 192.0.2.3 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
    #pkts decaps: 13, #pkts decrypt: 13, #pkts verify: 13
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 203.0.113.1, remote crypto endpt.: 192.0.2.3
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0x8D82CD6F(2374159727)
     PFS (Y/N): N, DH group: none
     inbound esp sas:
      spi: 0x55599CFD(1431936253)
        transform: esp-gcm 256 ,
        in use settings ={Tunnel, }
        conn id: 4352, flow_id: Onboard VPN:2352, sibling_flags 80000040, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4341601/3551)
        IV size: 8 bytes
        replay detection support: N
        Status: ACTIVE(ACTIVE)
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x8D82CD6F(2374159727)
        transform: esp-gcm 256 ,
        in use settings ={Tunnel, }
        conn id: 4351, flow_id: Onboard VPN:2351, sibling_flags 80000040, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4341601/3551)
        IV size: 8 bytes
        replay detection support: N
        Status: ACTIVE(ACTIVE)

     outbound ah sas:
     outbound pcp sas:
```


https://t.me/learningnets

Step 4

On Branch-ISR, revisit the configuration. The point-to-point FlexVPN configuration on Branch-ISR should be similar to:

```
hostname Branch-ISR
!
crypto pki trustpoint partner-isr
 enrollment url http://198.51.100.1:80
 revocation-check none
!
crypto pki certificate chain partner-isr
 certificate ca 01
 < Output omitted >
!
crypto ikev2 proposal ccnp-ike2-proposal
 encryption aes-cbc-256
 integrity sha512
 group 20
no crypto ikev2 proposal default
!
crypto ikev2 policy ccnp-ikev2-policy
 match fvrf any
 proposal ccnp-ike2-proposal
no crypto ikev2 policy default
!
crypto ikev2 keyring KR
 peer HQ-ISR
  address 192.0.2.3
  pre-shared-key local cisco123
!
crypto ikev2 profile ccnp-ikev2-profile
 match identity remote fqdn hq-isr.secure-x.public
 identity local fqdn branch-isr.secure-x.public
 authentication remote rsa-sig
 authentication local pre-share
 keyring local KR
 pki trustpoint partner-isr
!
crypto ipsec transform-set ccnp-ts esp-gcm 256
 mode tunnel
no crypto ipsec transform-set default
!
crypto ipsec profile ccnp-ipsec-profile
 set transform-set ccnp-ts
 set pfs group20
 set ikev2-profile ccnp-ikev2-profile
!
no crypto ipsec profile default
!
interface Tunnel0
 ip address 10.10.100.1 255.255.255.0
 tunnel source 203.0.113.1
 tunnel mode ipsec ipv4
 tunnel destination 192.0.2.3
 tunnel protection ipsec profile ccnp-ipsec-profile
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 5

On HQ-ISR, revisit the configuration. The point-to-point FlexVPN configuration on HQ-ISR should be similar to:

https://t.me/learningnets

```
hostname HQ-ISR
!
crypto pki trustpoint TP-self-signed-1158639554
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1158639554
 revocation-check none
 rsakeypair TP-self-signed-1158639554
!
crypto pki trustpoint partner-isr
 enrollment url http://198.51.100.1:80
 serial-number none
 fqdn hq-isr.secure-x.public
 ip-address none
 subject-name CN=hq-isr,O=secure-x.public
 revocation-check none
 rsakeypair hq-isr.secure-x.public
!
crypto pki certificate chain TP-self-signed-1158639554
 certificate self-signed 01
<output omitted>
crypto pki certificate chain partner-isr
 certificate 02
<output omitted>
 certificate ca 01
<output omitted>
!


crypto ikev2 proposal ccnp-ike2-proposal
 encryption aes-cbc-256
 integrity sha512
 group 20
no crypto ikev2 proposal default
!
crypto ikev2 policy ccnp-ikev2-policy
 match fvrf any
 proposal ccnp-ike2-proposal
no crypto ikev2 policy default
!


crypto ikev2 keyring KR
 peer Branch-ISR
  address 203.0.113.1
  pre-shared-key remote cisco123
!
crypto ikev2 profile ccnp-ikev2-profile
 match identity remote fqdn branch-isr.secure-x.public
 identity local fqdn hq-isr.secure-x.public
 authentication remote pre-share
 authentication local rsa-sig
 keyring local KR
 pki trustpoint partner-isr
!
crypto ipsec transform-set ccnp-ts esp-gcm 256
 mode tunnel
no crypto ipsec transform-set default
!
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

```
crypto ipsec profile ccnp-ipsec-profile
 set transform-set ccnp-ts
 set pfs group20
 set ikev2-profile ccnp-ikev2-profile
!
no crypto ipsec profile default
!
interface Tunnel0
 ip address 10.10.100.2 255.255.255.0
 tunnel source 192.0.2.3
 tunnel mode ipsec ipv4
 tunnel destination 203.0.113.1
 tunnel protection ipsec profile ccnp-ipsec-profile
!
ntp server 192.0.2.2
```

Step 6

On Partner-ISR, revisit the configuration. The configuration on Partner-ISR should be similar to:

```
hostname Partner-ISR
!
crypto pki server Partner-CA
 issuer-name CN=Partner-CA, O=partner.public
 grant auto
 hash sha256
!
crypto pki trustpoint local-ca
 revocation-check none
 rsakeypair partner-ca.partner.public
!
crypto pki trustpoint Partner-CA
 revocation-check crl
 rsakeypair Partner-CA
!
crypto pki certificate chain local-ca
crypto pki certificate chain Partner-CA
 certificate ca 01
 <output omitted>
!
ntp server 192.0.2.2
```


https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 3-2: Implement Hub-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN

Activity Objective

In this exercise you use an incremental approach when deploying a scalable FlexVPN hub-and-spoke environment.

You will configure an environment consisting of a single hub and a single spoke and configure Virtual Template interface on the hub for spawning of Virtual Access interfaces. The initial scenario uses pre-shared key spoke authentication and certificate hub authentication.

In the next stage you change the spoke authentication to certificates. Further you enable the mode config feature that enables the hub to push authorization attributes to the spoke. Having established this spoke-to-hub baseline configuration, you add a second spoke using identical settings.

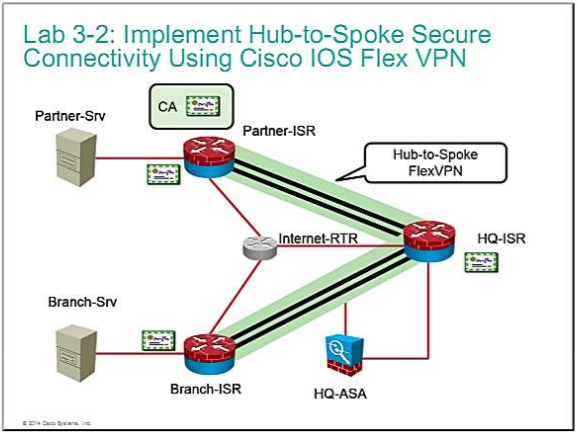
Upon completing this activity, you will be able to meet these objectives:

- Implement hub-to-spoke secure connectivity using Cisco IOS Flex VPN
- Configure Hub and Spoke for Virtual Access Connections
- Configure Locally Managed Mode Config

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

Three Cisco IOS routers

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Cisco IOS Commands

Command	Description
[no] crypto ikev2 authorization policy default	Modify (disable) the default IKEv2 authorization policy.
[no] interface Tunnel *tunnel_ID*	Creates a new tunnel interface and enters tunnel interface configuration mode. The no option will remove Tunnel interface from the device.
[no] shutdown	Enables or disables interface.
aaa new-model	Enables AAA new model.
clear crypto ikev2 sa	Clears crypto IKEv2 SAs.
clear crypto sa	Clears all crypto SAs.
crypto ikev2 authorization policy	Define an IKEv2 authorization policy (config mode).

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Command	Description
crypto ikev2 profile *profile-name*	Creates an IKEv2 profile and enters crypto profile configuration mode.
crypto pki authenticate *server-name*	Obtains the CA certificate.
crypto pki enroll *server-name*	Requests and accepts the identity certificate.
crypto pki trustpoint *server-name*	Enables PKI truspoint.
debug crypto ikev2	Enables crypto IKEv2 debugging.
enrollment url *url*	Configures enrolment URL in the trustpoint.
interface Virtual-Template *vt_ID* **type tunnel**	Configures virtual template interface with type tunnel.
ip address *ip-address subnet-mask*	Configures IP address to the interface.
ip address negotiated	Enable interface to negotiate IP address and subnet for the interface.
ip local pool *pool-name first-IP last-IP*	Creates IP pool.
ip unnumbered *interface*	Assigns an IP subnet and address to the interface.
ping *ip-destination*	Verifies IP connectivity to the remote IP destination.
pool *pool-name*	Specifies local IP address pool to be used by the IKEv2 authorization policy.
route set interface	Enable the pushing of tunnel IP address to the peer; configured in the IKEv2 authorization policy.
show crypto ikev2 sa	Displays current IKEv2 SAs.
show crypto ipsec sa	Verifies the status of the IPsec SAs.
show interface *interface*	Verifies the status of the local interface.
show ip interface brief	Display brief interface status.
show ip ospf neighbor	Displays neighbors that are discovered by OSPF.
show ip protocols	Displays IP protocol information.
show ip route	Displays IPv4 routes in the routing table.
show ntp status	Verifies NTP status.
show running-config	Displays running configuration.
tunnel mode gre ip	Specifies the tunnel encapsulation as GRE IP (default).
tunnel protection ipsec profile *profile-name*	Specifies the traffic protection policy by referencing the configured IPsec profile.
tunnel source interface *interface*	Specifies a tunnel interface source.
virtual-template	Configured in IKEv2 profile configuration mode, specifies the virtual template interface used for cloning virtual access interfaces to service tunnels on-demand.

Job Aids

These job aids are available to help you complete the lab activity.

https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

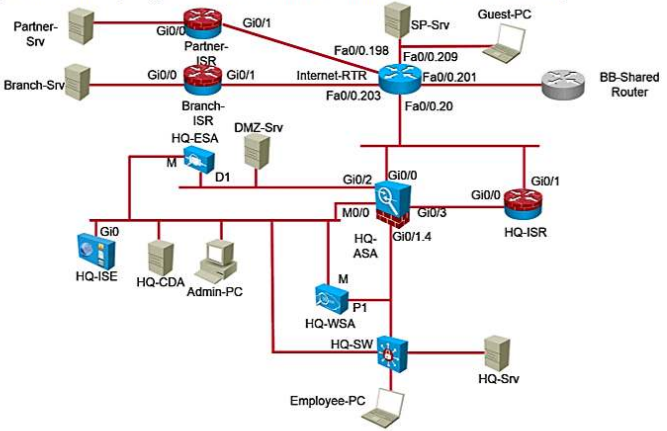
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

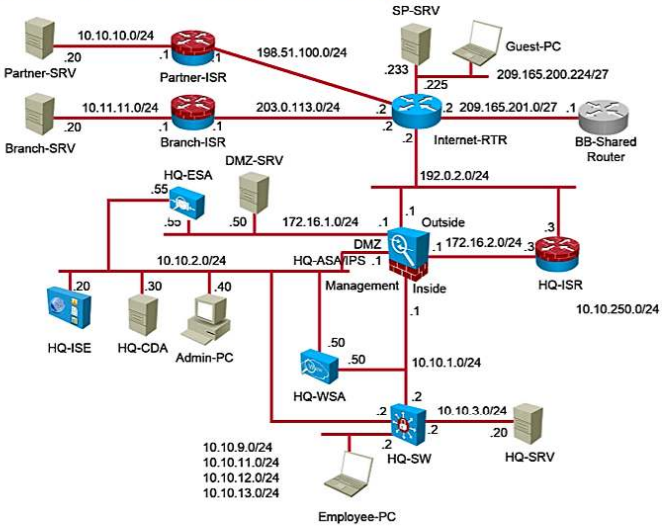
https://t.me/learningnets

Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



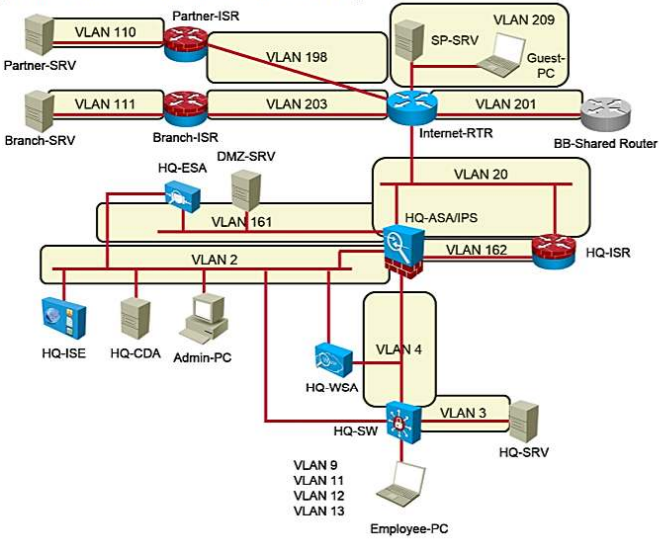
The figure shows the IP addresses that are used in this lab setup.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Configure Hub and Spoke for Virtual Access Connections

In this task you will configure the HQ-ISR to support virtual access interfaces. You will set the tunnel mode on the Branch-ISR to the default value.

Note Initially you configure an environment consisting of a single hub and a single spoke, and configure Virtual Template interface on the hub for spawning of Virtual Access interfaces. The initial scenario uses pre-shared key spoke authentication and certificate-based hub authentication.

Activity Procedure

Complete the following steps:

Step 1

Verify that the HQ-ISR and Branch-ISR routers are pre-configured for a point-to-point FlexVPN tunnel. The HQ-ISR router is configured for certificate-based authentication. The Branch-ISR is configured for pre-shared key authentication. The Partner-ISR runs the CA that issues the certificates required for the VPN.

Step 2

Make sure that the system time is synchronized on the routers in your pod. Internet-RTR should be synchronized to the public NTP server 64.103.34.15 and other routers (HQ-ISR, Branch-ISR and Partner-ISR) should be synchronized via NTP to the Internet-RTR:

```
Internet-RTR# show ntp status
Clock is synchronized, stratum 2, reference is 64.103.34.15
nominal freq is 249.5901 Hz, actual freq is 249.5900 Hz, precision is 2**18
reference time is D566CED1.15411DC6 (11:30:25.083 UTC Sat Jun 15 2013)
clock offset is 9.4739 msec, root delay is 171.30 msec
root dispersion is 10.93 msec, peer dispersion is 1.46 msec
```

Step 3

On Branch-ISR, change the tunnel mode to **GRE IP**. This is the default setting. Also, change the tunnel source to interface GigabitEthernet 0/1 instead of IP address. This will make the configuration of all spokes more similar.

Step 4

On HQ-ISR, delete the Tunnel interface and create a Loopback 0 interface . The IP address of the Loopback 0 interface will be cloned to virtual access interfaces. Set the IP address of the Loopback interface to 10.10.100.99/32.

Step 5

On HQ-ISR, create a virtual template interface (1) with these settings:

Type: **tunnel**

IP address: **Unnumbered to the Loopback 0 interface**

Tunnel mode: **tunnel mode gre ip** (default)

Protection: **your custom IPsec profile** (ccnp-ipsec-profile)

Step 6

On HQ-ISR, bind the virtual template to the custom IKEv2 profile (**ccnp-ikev2-profile**).

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Activity Verification

Step 1

Verify successful tunnel negotiation:

A) On Branch-ISR, shut down the tunnel interface.

B) On HQ-ISR, enable IKEv2 debugging and make sure that you will see it in your session.

Note	If you access the router via the console port, you should issue the **logging console** command to send the debugging output to the console line. If you access the router via Telnet, use the **terminal monitor** command.

C) On Branch-ISR, clear the IKEv2 (**clear crypto ikev2 sa**) and IPsec SAs (**clear crypto sa**) and re-enable (**no shutdown**) the tunnel interface.

D) On HQ-ISR, examine the debugging output. The SAs should be successfully negotiated. Disable the debugging.

```
HQ-ISR# debug crypto ikev2
IKEv2 default debugging is on
<Comment: the negotiation starts with an IKEv2 IKE_SA_INIT Request packet received
from the spoke. The hub finds the IKEv2 policy 'ccnp-ikev2-policy', uses Diffie-
Hellman group 20, which is not negotiated, and negotiates other parameters:>
Jun 17 16:30:36.260: IKEv2:Received Packet [From 203.0.113.1:500/To 192.0.2.3:500/VRF
i0:f0]
Initiator SPI : 0BED25BDC109EF5E - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
 SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP)
Jun 17 16:30:36.260: IKEv2:(SA ID = 1):Verify SA init message
Jun 17 16:30:36.260: IKEv2:(SA ID = 1):Insert SA
Jun 17 16:30:36.260: IKEv2:Searching Policy with fvrf 0, local address 192.0.2.3
Jun 17 16:30:36.260: IKEv2:Found Policy 'ccnp-ikev2-policy'
Jun 17 16:30:36.260: IKEv2:(SA ID = 1):Processing IKE_SA_INIT message
Jun 17 16:30:36.264: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieve configured
trustpoint(s)
Jun 17 16:30:36.264: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s):
'Trustpool4'   'Trustpool3'   'Trustpool2'   'Trustpool1'   'Trustpool'   'HQ-ISR'
Jun 17 16:30:36.264: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Get Public Key Hashes of
trustpoints
Jun 17 16:30:36.264: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of Public Key Hashes of
trustpoints PASSED
Jun 17 16:30:36.264: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Start PKI Session
Jun 17 16:30:36.264: IKEv2:(SA ID = 1):[PKI -> IKEv2] Starting of PKI Session PASSED
Jun 17 16:30:36.264: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Computing DH public
key, DH Group 20
Jun 17 16:30:36.264: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] DH key Computation
PASSED
Jun 17 16:30:36.264: IKEv2:(SA ID = 1):Request queued for computation of DH key
Jun 17 16:30:36.264: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Computing DH secret
key, DH Group 20
Jun 17 16:30:36.360: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] DH key Computation
PASSED
Jun 17 16:30:36.360: IKEv2:(SA ID = 1):Request queued for computation of DH secret
Jun 17 16:30:36.360: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Calculate SKEYSEED
and create rekeyed IKEv2 SA
Jun 17 16:30:36.360: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] SKEYSEED calculation
and creation of rekeyed IKEv2 SA PASSED
Jun 17 16:30:36.360: IKEv2:IKEv2 responder - no config data to send in IKE_SA_INIT
exch
```


https://t.me/learningnets

```
Jun 17 16:30:36.360: IKEv2:(SA ID = 1):Generating IKE_SA_INIT message
Jun 17 16:30:36.360: IKEv2:(SA ID = 1):IKE Proposal: 1, SPI size: 0 (initial
negotiation), Num. transforms: 4
   AES-CBC   SHA512   SHA512   DH_GROUP_384_ECP/Group 20
Jun 17 16:30:36.360: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieve configured
trustpoint(s)
Jun 17 16:30:36.364: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s):
'Trustpool4'   'Trustpool3'   'Trustpool2'   'Trustpool1'   'Trustpool'   'HQ-ISR'
Jun 17 16:30:36.364: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Get Public Key Hashes of
trustpoints
Jun 17 16:30:36.364: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of Public Key Hashes of
trustpoints PASSED
Jun 17 16:30:36.364: IKEv2:(SA ID = 1):Sending Packet [To 203.0.113.1:500/From
192.0.2.3:500/VRF i0:f0]
Initiator SPI : 0BED25BDC109EF5E - Responder SPI : 66CEF8AA6425A1BD Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE
Payload contents:
 SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP)
CERTREQ NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)
Jun 17 16:30:36.364: IKEv2:(SA ID = 1):Completed SA init exchange
<Comment: in the authentication exchange the hub router matches the appropriate IKEv2
profile, and finds that the peer authentication is PSK and the local authentication
is RSA-SIG:>
Jun 17 16:30:36.364: IKEv2:(SA ID = 1):Starting timer (30 sec) to wait for auth
message
Jun 17 16:30:36.464: IKEv2:(SA ID = 1):Received Packet [From 203.0.113.1:500/To
192.0.2.3:500/VRF i0:f0]
Initiator SPI : 0BED25BDC109EF5E - Responder SPI : 66CEF8AA6425A1BD Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:
 VID IDi CERTREQ NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) AUTH CFG SA TSi TSr
NOTIFY(INITIAL_CONTACT) NOTIFY(SET_WINDOW_SIZE) NOTIFY(ESP_TFC_NO_SUPPORT)
NOTIFY(NON_FIRST_FRAGS)
Jun 17 16:30:36.464: IKEv2:(SA ID = 1):Stopping timer to wait for auth message
Jun 17 16:30:36.464: IKEv2:(SA ID = 1):Checking NAT discovery
Jun 17 16:30:36.464: IKEv2:(SA ID = 1):NAT not found
Jun 17 16:30:36.464: IKEv2:(SA ID = 1):Searching policy based on peer's identity
'branch-isr.secure-x.public' of type 'FQDN'
Jun 17 16:30:36.464: IKEv2:found matching IKEv2 profile 'ccnp-ikev2-profile'
Jun 17 16:30:36.464: IKEv2:% Getting preshared key from profile keyring KR
Jun 17 16:30:36.464: IKEv2:% Matched peer block 'branch-router'
Jun 17 16:30:36.464: IKEv2:Searching Policy with fvrf 0, local address 192.0.2.3
Jun 17 16:30:36.464: IKEv2:Found Policy 'ccnp-ikev2-policy'
Jun 17 16:30:36.464: IKEv2:(SA ID = 1):Verify peer's policy
Jun 17 16:30:36.464: IKEv2:(SA ID = 1):Peer's policy verified
Jun 17 16:30:36.464: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieving trustpoint(s) from
received certificate hash(es)
Jun 17 16:30:36.464: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s):
Jun 17 16:30:36.468: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieving trustpoint(s) from
received certificate hash(es)
Jun 17 16:30:36.468: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s):
Jun 17 16:30:36.468: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieving trustpoint(s) from
received certificate hash(es)
Jun 17 16:30:36.468: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s):
Jun 17 16:30:36.468: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieving trustpoint(s) from
received certificate hash(es)
Jun 17 16:30:36.468: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s):
Jun 17 16:30:36.468: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieving trustpoint(s) from
received certificate hash(es)
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

```
Jun 17 16:30:36.468: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s): 'HQ-
ISR'
Jun 17 16:30:36.468: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Getting cert chain for the
trustpoint HQ-ISR
Jun 17 16:30:36.468: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of cert chain for the
trustpoint PASSED
<Comment: the hub first verifies the HMAC authentication data received from the
spoke. The HMAC was generated with the PSK, and the hub uses the peer's PSK to verify
the HMAC:>
Jun 17 16:30:36.468: IKEv2:(SA ID = 1):Get peer's authentication method
Jun 17 16:30:36.468: IKEv2:(SA ID = 1):Peer's authentication method is 'PSK'
Jun 17 16:30:36.472: IKEv2:(SA ID = 1):Get peer's preshared key for branch-isr.secure-
x.public
Jun 17 16:30:36.472: IKEv2:(SA ID = 1):Verify peer's authentication data
Jun 17 16:30:36.472: IKEv2:(SA ID = 1):Use preshared key for id branch-isr.secure-
x.public, key len 8
Jun 17 16:30:36.472: IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication data
Jun 17 16:30:36.472: IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data
generation PASSED
Jun 17 16:30:36.472: IKEv2:(SA ID = 1):Verification of peer's authenctication data
PASSED
Jun 17 16:30:36.472: IKEv2:(SA ID = 1):Processing INITIAL_CONTACT
Jun 17 16:30:36.472: IKEv2:(SA ID = 1):Received valid config mode data
Jun 17 16:30:36.472: IKEv2:Config data recieved:
Jun 17 16:30:36.472: Config-type: Config-request
Jun 17 16:30:36.472: Attrib type: ipv4-dns, length: 0
Jun 17 16:30:36.472: Attrib type: ipv4-dns, length: 0
Jun 17 16:30:36.472: Attrib type: ipv4-nbns, length: 0
Jun 17 16:30:36.472: Attrib type: ipv4-nbns, length: 0
Jun 17 16:30:36.472: Attrib type: ipv4-subnet, length: 0
Jun 17 16:30:36.472: Attrib type: app-version, length: 243, data: Cisco IOS Software,
C2900 Software (C2900-UNIVERSALK9-M), Version 15.3(1)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Mon 26-Nov-12 14:52 by prod_rel_team
Jun 17 16:30:36.472: Attrib type: split-dns, length: 0
Jun 17 16:30:36.472: Attrib type: banner, length: 0
Jun 17 16:30:36.472: Attrib type: config-url, length: 0
Jun 17 16:30:36.472: Attrib type: backup-gateway, length: 0
Jun 17 16:30:36.472: Attrib type: def-domain, length: 0
Jun 17 16:30:36.472: IKEv2:(SA ID = 1):Set received config mode data
Jun 17 16:30:36.472: IKEv2:(SA ID = 1):Processing IKE_AUTH message
Jun 17 16:30:36.472: IKEv2:% DVTI create request sent for profile ccnp-ikev2-profile
with PSH index 1.
Jun 17 16:30:36.472: IKEv2:(SA ID = 1):
Jun 17 16:30:36.472: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to down
Jun 17 16:30:36.480: IKEv2:% DVTI Vil created for profile ccnp-ikev2-profile with PSH
index 1.
Jun 17 16:30:36.480: IKEv2:KMI/verify policy/sending to IPSec:
        prot: 3 txfm: 20 hmac 0 flags 8177 keysize 256 IDB 0x425981CC
Jun 17 16:30:36.484: IKEv2:Error constructing config reply
<Comment: the hub will now generate the signature required for local authentication
to the peer. The signature is computed using the hub's RSA private key. The hub will
also send its identity certificate, containing the hub's public key, to the spoke.
The spoke will have to verify the hub certificate and the hub's signature using the
CA root certificate:>
Jun 17 16:30:36.484: IKEv2:(SA ID = 1):Get my authentication method
Jun 17 16:30:36.484: IKEv2:(SA ID = 1):My authentication method is 'RSA'
Jun 17 16:30:36.484: IKEv2:(SA ID = 1):Generate my authentication data
Jun 17 16:30:36.484: IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication data
Jun 17 16:30:36.484: IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data
generation PASSED
```


https://t.me/learningnets

```
Jun 17 16:30:36.484: IKEv2:(SA ID = 1):Get my authentication method
Jun 17 16:30:36.484: IKEv2:(SA ID = 1):My authentication method is 'RSA'
Jun 17 16:30:36.484: IKEv2:(SA ID = 1):Sign authentication data
Jun 17 16:30:36.484: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Getting private key
Jun 17 16:30:36.484: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of private key PASSED
Jun 17 16:30:36.484: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Sign authentication
data
Jun 17 16:30:36.780: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] Signing of
authentication data PASSED
Jun 17 16:30:36.780: IKEv2:(SA ID = 1):Authentication material has been successfully
signed
Jun 17 16:30:36.780: IKEv2:(SA ID = 1):Generating IKE_AUTH message
Jun 17 16:30:36.780: IKEv2:(SA ID = 1):Constructing IDr payload: 'hq-isr.secure-
x.public' of type 'FQDN'
<Comment: The last section describes the negotiation of the IPsec SA's:>
Jun 17 16:30:36.780: IKEv2:(SA ID = 1):ESP Proposal: 1, SPI size: 4 (IPSec
negotiation),
Num. transforms: 2
   AES-GCM    Don't use ESN
Jun 17 16:30:36.780: IKEv2:(SA ID = 1):Building packet for encryption.
Payload contents:
 VID IDr CERT AUTH SA TSi TSr NOTIFY(SET_WINDOW_SIZE) NOTIFY(ESP_TFC_NO_SUPPORT)
NOTIFY(NON_FIRST_FRAGS)
Jun 17 16:30:36.780: IKEv2:(SA ID = 1):Sending Packet [To 203.0.113.1:500/From
192.0.2.3:500/VRF i0:f0]
Initiator SPI : 0BED25BDC109EF5E - Responder SPI : 66CEF8AA6425A1BD Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
Payload contents:
 ENCR
Jun 17 16:30:36.780: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Close PKI Session
Jun 17 16:30:36.780: IKEv2:(SA ID = 1):[PKI -> IKEv2] Closing of PKI Session PASSED
Jun 17 16:30:36.780: IKEv2:(SA ID = 1):IKEV2 SA created; inserting SA into database.
SA lifetime timer (86400 sec) started
Jun 17 16:30:36.784: IKEv2:(SA ID = 1):Session with IKE ID PAIR (branch-isr.secure-
x.public, hq-isr.secure-x.public) is UP
Jun 17 16:30:36.784: IKEv2:IKEv2 MIB tunnel started, tunnel index 1
Jun 17 16:30:36.784: IKEv2:(SA ID = 1):Load IPSEC key material
Jun 17 16:30:36.784: IKEv2:(SA ID = 1):[IKEv2 -> IPsec] Create IPsec SA into IPsec
database
Jun 17 16:30:36.784: IKEv2:(SA ID = 1):Asynchronous request queued
Jun 17 16:30:36.784: IKEv2:(SA ID = 1):
Jun 17 16:30:36.784: IKEv2:(SA ID = 1):[IPsec -> IKEv2] Creation of IPsec SA into
IPsec database PASSED
Jun 17 16:30:36.784: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to up
Jun 17 16:30:36.788: IKEv2:(SA ID = 1):Checking for duplicate IKEv2 SA
Jun 17 16:30:36.788: IKEv2:(SA ID = 1):No duplicate IKEv2 SA found
Jun 17 16:30:36.788: IKEv2:(SA ID = 1):Starting timer (8 sec) to delete negotiation
context
Jun 17 16:30:36.820: %OSPF-5-ADJCHG: Process 1, Nbr 203.0.113.1 on Virtual-Access1
from LOADING to FULL, Loading Done
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 2

On HQ-ISR, verify the virtual access interface.

```
HQ-ISR# show interface virtual-access 1
Virtual-Access1 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of Loopback0 (10.10.100.99)
  MTU 17886 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  Tunnel vaccess, cloned from Virtual-Template1
  Vaccess status 0x4, loopback not set
  Keepalive not set
  Tunnel source 192.0.2.3, destination 203.0.113.1
  Tunnel protocol/transport GRE/IP
 <output omitted>
```


https://t.me/learningnets

Step 3

On HQ-ISR, verify the connectivity through the tunnel. The shown methods display the status of OSPF and IPsec SA's.

```
HQ-ISR# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "application"
  Sending updates every 0 seconds
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Maximum path: 32
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 4)
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID ...
  It is an area border router
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.2.0 0.0.0.255 area 0
    10.10.100.0 0.0.0.255 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.13.2           110      00:09:18
    203.0.113.1          110      00:03:27
    192.0.2.1            110      00:03:27
  Distance: (default is 110)
HQ-ISR# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.0.2.1         1   FULL/DR         00:00:31    172.16.2.1      GigabitEthernet0/0
203.0.113.1       0   FULL/  -        00:00:32    10.10.100.1      Virtual-Access1
HQ-ISR# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
Gateway of last resort is 192.0.2.2 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 192.0.2.2
      10.0.0.0/24 is subnetted, 9 subnets
O        10.10.1.0 [110/11] via 172.16.2.1, 00:09:36, GigabitEthernet0/0
O        10.10.2.0 [110/12] via 172.16.2.1, 00:09:36, GigabitEthernet0/0
O        10.10.3.0 [110/12] via 172.16.2.1, 00:09:36, GigabitEthernet0/0
O        10.10.9.0 [110/12] via 172.16.2.1, 00:09:36, GigabitEthernet0/0
O        10.10.10.0 [110/12] via 172.16.2.1, 00:09:36, GigabitEthernet0/0
O        10.10.11.0 [110/12] via 172.16.2.1, 00:09:36, GigabitEthernet0/0
O        10.10.12.0 [110/12] via 172.16.2.1, 00:09:36, GigabitEthernet0/0
O        10.10.13.0 [110/12] via 172.16.2.1, 00:09:36, GigabitEthernet0/0
O        10.10.100.0/24 [110/2000] via 10.10.100.1, 00:03:46, Virtual-Access1
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

```
C        10.10.100.99/32 is directly connected, Loopback0
O        10.11.11.0 [110/1001] via 10.10.100.1, 00:03:46, Virtual-Access1
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O        172.16.1.0/24 [110/11] via 172.16.2.1, 00:09:36, GigabitEthernet0/0
C        172.16.2.0/24 is directly connected, GigabitEthernet0/0
L        172.16.2.3/32 is directly connected, GigabitEthernet0/0
      192.0.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.0.2.0/24 is directly connected, GigabitEthernet0/1
L        192.0.2.3/32 is directly connected, GigabitEthernet0/1
HQ-ISR# show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA
Tunnel-id Local                 Remote                fvrf/ivrf            Status
1          192.0.2.3/500        203.0.113.1/500       none/none            READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:20, Auth sign: RSA, Auth
verify: PSK
      Life/Active Time: 86400/312 sec
 IPv6 Crypto IKEv2  SA
HQ-ISR# show crypto ipsec sa
interface: Virtual-Access1
    Crypto map tag: Virtual-Access1-head-0, local addr 192.0.2.3
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.0.2.3/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (203.0.113.1/255.255.255.255/47/0)
   current_peer 203.0.113.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 43, #pkts encrypt: 43, #pkts digest: 43
    #pkts decaps: 42, #pkts decrypt: 42, #pkts verify: 42
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 192.0.2.3, remote crypto endpt.: 203.0.113.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0x17C9553(24941907)
     PFS (Y/N): N, DH group: none
     inbound esp sas:
      spi: 0x5CC9C6FB(1556727547)
        transform: esp-gcm 256 ,
```

Task 2: Configure Certificate-Based Authentication on Spoke

In this task you will change the spoke authentication from PSK-based to certificate-based.

Note Currently the spoke authenticates using the pre-shared keys. In this phase you change the spoke authentication to RSA signatures. This is needed because the locally managed mode config feature, configured in the next task, does not support pre-shared key authentication on the clients.

Activity Procedure

Complete the following steps:

https://t.me/learningnets

Step 1

Verify the existing trustpoint configuration on Branch-ISR. It has been configured for certificate-based authentication but not yet enrolled with the PKI.

```
Branch-ISR# show running-config | section trustpoint
crypto pki trustpoint partner-isr
 enrollment url http://198.51.100.1:80
 revocation-check none
 pki trustpoint partner-isr
```

Note Branch-ISR is currently configured to verify the certificates and signatures obtained from its peers. It cannot yet perform local RSA-SIG authentication, because it does not yet have an identity certificate.

Step 2

Enroll Branch-ISR with the Partner-ISR CA.

A) Generate an RSA key pair, name it for example 'branch-keypair'. Make it 2048 bits long.

Note You can set several options when generating the RSA key pair, such as setting the length or making the private key exportable. None of these options is required in this lab scenario. You can configure any of these options.

B) Add enrollment parameters to the existing trustpoint (partner-isr):

FQDN: **branch-isr.secure-x.public**

Subject name: **CN=branch-isr,O=secure-x.public**

Serial number: **none**

IP address: **none**

RSA key: **your generated key (branch-keypair)**

Note If you do not specify the RSA keypair, a key pair will be automatically generated.

C) Request and accept the identity certificate.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

On Branch-ISR, modify the IKEv2 profile (ccnp-ikev2-profile) for local certificate authentication and acceptance of other spokes. IKEv2 profiles allow multiple authentication statements that are combined with a logical 'OR'. Be sure to remove the pre-share authentication data from the configuration. Use these settings:

A) Local authentication: **rsa-sig**

B) PKI trustpoint: **partner-isr**

C) No key ring.

D) Matching of remote peers: **FQDN domain secure-x.public**

Note	You may keep or delete the more specific match of the hq-isr.secure-x.public FQDN. The 'match identity remote' statements are combined using the OR operator.

Step 4

On HQ-ISR, modify the IKEv2 profile (ccnp-ikev2-profile) for remote certificate authentication:

A) Match remote identity: **based on domain name in FQDN (secure-x.public)**

Note	Matching remote identities based on domain name instead of the full FQDN will allow this profile to match additional spokes.

B) Remote authentication: **rsa-sig**

C) No key ring.

Activity Verification

Step 1

Verify successful tunnel negotiation:

A) On Branch-ISR, shut down the Tunnel 0 interface (**shutdown**).

B) On HQ-ISR, enable IKEv2 debugging (**debug crypto ikev2**).

C) On Branch-ISR, clear the IKEv2 (**clear crypto ikev2 sa**) and IPsec SAs (**clear crypto sa**).

D) On Branch-ISR, re-enable the tunnel interface (**no shutdown**).

E) On HQ-ISR, examine the debugging output. The SAs should be successfully negotiated. Disable the debugging (**undebug all**).

Task 3: Configure Locally Managed Mode Config

In this task you will configure locally managed mode config. The hub will apply the tunnel IP address and optionally other attributes to the spoke.

https://t.me/learningnets

Note	The mode config feature is also referred to as client authorization. It enables the hub to push authorization attributes to the spoke. In this scenario, the hub will provide an attribute (route set interface) that enables the setting of the tunnel IP address, and will assign tunnel IP addresses from a pool. Additional attributes could be used to enable IKEv2 to install static routes. The route attributes are not used in this scenario, because you will deploy BGP. BGP is the recommended routing solution due to its high scalability.

Activity Procedure

Complete the following steps:

Step 1

On Branch-ISR and HQ-ISR, enable AAA new model and enable default network authorization against the local database.

Step 2

On HQ-ISR, disable the default IKEv2 authorization policy and configure a custom IKEv2 authorization policy (ccnp-spokes), which:

A) Assigns addresses from a local address pool (ccnp-pool) with address range 10.10.100.1-10.10.100.90. Configure the local pool.

B) Sends the VPN interface IP address to the peer via IKEv2 standard config attribute INTERNAL_IP4_SUBNET (**route set interface** command).

Note	You are configuring a custom authorization policy on HQ-ISR for demonstration purposes. You will use the default policy on the spokes.

Step 3

On HQ-ISR, modify the IKEv2 profile (ccnp-ikev2-profile) for group authorization using the default list (defined as aaa authorization network default) and the custom IKEv2 authorization policy for the local user profile (ccnp-spokes).

Note	You must use the cert method, because the other side is authenticated using certificates.

Step 4

On Branch-ISR, modify the IKEv2 profile (ccnp-ikev2-profile) for group authorization using the default list (defined as aaa authorization network default) and the default IKEv2 authorization policy

Note	You must use the cert method, because the other side is authenticated using certificates.

Step 5

On Branch-ISR, allow the tunnel IP address to be obtained from the hub.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Activity Verification

Step 1

On Branch-ISR, disable and enable the Tunnel 0 interface. Verify successful tunnel re-negotiation.

```
Branch-ISR(config-if)# shutdown
Dec 10 11:40:08.025: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
Dec 10 11:40:10.025: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to down
Dec 10 11:40:10.025: %LINK-5-CHANGED: Interface Tunnel0, changed state to
administratively down
Branch-ISR(config-if)# no shutdown
Dec 10 11:40:16.013: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Dec 10 11:40:18.013: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
Dec 10 11:40:18.013: %LINK-3-UPDOWN: Interface Tunnel0, changed state to up
Dec 10 11:40:18.021: %OSPF-5-ADJCHG: Process 1, Nbr 192.0.2.3 on Tunnel0 from LOADING
to FULL, Loading Done
```

Step 2

On Branch-ISR, verify that an IP address has been applied to the Tunnel 0 interface.

```
Branch-ISR# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         10.11.11.1      YES NVRAM  up                    up
GigabitEthernet0/1         203.0.113.1     YES NVRAM  up                    up
GigabitEthernet0/0/0       unassigned      YES unset  down                  down
GigabitEthernet0/0/1       unassigned      YES unset  down                  down
GigabitEthernet0/0/2       unassigned      YES unset  down                  down
GigabitEthernet0/0/3       unassigned      YES unset  down                  down
Tunnel0                    10.10.100.1     YES manual up                    up
Vlan1                      unassigned      YES unset  down                  down
```


https://t.me/learningnets

Step 3

On HQ-ISR, view the routing table. You should see a host route to the Branch-ISR tunnel address going via the Virtual Access interface:

```
HQ-ISR# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
Gateway of last resort is 192.0.2.2 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 192.0.2.2
      10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
O        10.10.1.0/24 [110/11] via 172.16.2.1, 4d00h, GigabitEthernet0/0
O        10.10.2.0/24 [110/12] via 172.16.2.1, 4d00h, GigabitEthernet0/0
O        10.10.3.0/24 [110/12] via 172.16.2.1, 4d00h, GigabitEthernet0/0
O        10.10.9.0/24 [110/12] via 172.16.2.1, 4d00h, GigabitEthernet0/0
O        10.10.11.0/24 [110/12] via 172.16.2.1, 4d00h, GigabitEthernet0/0
O        10.10.12.0/24 [110/12] via 172.16.2.1, 4d00h, GigabitEthernet0/0
O        10.10.13.0/24 [110/12] via 172.16.2.1, 4d00h, GigabitEthernet0/0
S        10.10.100.1/32 is directly connected, Virtual-Access1
C        10.10.100.99/32 is directly connected, Loopback0
O IA     10.11.11.0/24 [110/1001] via 10.10.100.1, 00:04:35, Virtual-Access1
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O        172.16.1.0/24 [110/11] via 172.16.2.1, 4d00h, GigabitEthernet0/0
C        172.16.2.0/24 is directly connected, GigabitEthernet0/0
L        172.16.2.3/32 is directly connected, GigabitEthernet0/0
      192.0.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.0.2.0/24 is directly connected, GigabitEthernet0/1
L        192.0.2.3/32 is directly connected, GigabitEthernet0/1
```

Note Depending on the previous activity you may see a different Virtual-Access ID and/or IP address.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 4

On HQ-ISR, examine the Virtual Access interface. You should see its cloning information, source and destination address, and other details. Use the Virtual Access ID created in your router.

```
HQ-ISR# show interface virtual-access 1
Virtual-Access1 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of Loopback0 (10.10.100.99)
  MTU 17862 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  Tunnel vaccess, cloned from Virtual-Template1
  Vaccess status 0x4, loopback not set
  Keepalive not set
  Tunnel source 192.0.2.3, destination 203.0.113.1
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1422 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ccnp-ipsec-profile")
  Last input 00:00:04, output never, output hang never
  Last clearing of "show interface" counters 00:06:07
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     77 packets input, 7704 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runs, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     48 packets output, 5260 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Step 5

On HQ-ISR, ping the tunnel IP address of the spoke:

```
HQ-ISR# ping 10.10.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task 4: Add a Second Flex VPN Spoke

In this task you will configure the Partner-ISR to act as the second spoke.

https://t.me/learningnets

Note	In the previous task you have established a baseline spoke-to-hub baseline configuration. Now you are ready to replicate this baseline to additional spokes. In this scenario you add the Partner-ISR as the second spoke.

Activity Procedure

Complete the following steps:

Step 1

Enroll Partner-ISR with the CA running on the same router.

A) Configure a new trustpoint (partner-isr):

FQDN: **partner-isr.partner.public**

Subject name: **CN=partner-isr,O=partner.public**

Enrollment url: **http://198.51.100.1**

Revocation check: **none**

Serial number: **none**

IP address: **none**

Note	If you do not specify the RSA keypair, a key pair will be automatically generated.

B) Obtain the CA certificate using the **crypto pki authenticate** configuration mode command.

C) Request and accept the identity certificate using the **crypto pki enroll** configuration mode command. Enter **cisco** as the challenge password. The certificate will be granted automatically as a result of the **grant auto** configuration on the Partner-ISR CA.

Step 2

On Partner-ISR, configure the same IKEv2 and IPsec constructs as on Branch-ISR. You may copy and paste the commands. The only two differences are:

A) Identity local: **FQDN partner-isr.partner.public**

B) Remote domain match: **secure-x.public**

Step 3

On HQ-ISR, configure the IKEv2 profile (ccnp-ikev2-profile) to match remote peer domain 'partner.public' in addition to the domain 'secure-x.public'.

Step 4

On Partner-ISR, remove Tunnel 1 interface:

Activity Verification

Step 1

Verify that the VPN connection between the Partner-ISR and HQ-ISR came up automatically.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Note	If the connection does not come up, or you want to debug IKEv2 negotiation, you can disable and enable the Tunnel 0 interface on Partner-ISR.

https://t.me/learningnets

Step 2

On the HQ-ISR verify the creation of the second virtual access interface. Test IP connectivity through the tunnel. (The ping to the 10.10.100.6 address might fail because different IP address may be assigned in your POD. You will need to ping the IP address that was assigned from the pool.)

```
HQ-ISR# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
Gateway of last resort is 192.0.2.2 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 192.0.2.2
      10.0.0.0/8 is variably subnetted, 11 subnets, 2 masks
O        10.10.1.0/24 [110/11] via 172.16.2.1, 4d00h, GigabitEthernet0/0
O        10.10.2.0/24 [110/12] via 172.16.2.1, 4d00h, GigabitEthernet0/0
O        10.10.3.0/24 [110/12] via 172.16.2.1, 4d00h, GigabitEthernet0/0
O        10.10.9.0/24 [110/12] via 172.16.2.1, 4d00h, GigabitEthernet0/0
O        10.10.11.0/24 [110/12] via 172.16.2.1, 4d00h, GigabitEthernet0/0
O        10.10.12.0/24 [110/12] via 172.16.2.1, 4d00h, GigabitEthernet0/0
O        10.10.13.0/24 [110/12] via 172.16.2.1, 4d00h, GigabitEthernet0/0
S        10.10.100.1/32 is directly connected, Virtual-Access1
S        10.10.100.6/32 is directly connected, Virtual-Access2
C        10.10.100.99/32 is directly connected, Loopback0
O IA     10.11.11.0/24 [110/1001] via 10.10.100.1, 00:31:58, Virtual-Access1
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O        172.16.1.0/24 [110/11] via 172.16.2.1, 4d00h, GigabitEthernet0/0
C        172.16.2.0/24 is directly connected, GigabitEthernet0/0
L        172.16.2.3/32 is directly connected, GigabitEthernet0/0
      192.0.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.0.2.0/24 is directly connected, GigabitEthernet0/1
L        192.0.2.3/32 is directly connected, GigabitEthernet0/1
HQ-ISR# ping 10.10.100.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.100.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
HQ-ISR# show interface virtual-access 2
Virtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of Loopback0 (10.10.100.99)
  MTU 17862 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  Tunnel vaccess, cloned from Virtual-Template1
  Vaccess status 0x4, loopback not set
  Keepalive not set
  Tunnel source 192.0.2.3, destination 198.51.100.1
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1422 bytes
  Tunnel transmit bandwidth 8000 (kbps)
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

```
Tunnel receive bandwidth 8000 (kbps)
Tunnel protection via IPSec (profile "ccnp-ipsec-profile")
Last input 00:00:16, output never, output hang never
Last clearing of "show interface" counters 00:02:04
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   5 packets input, 620 bytes, 0 no buffer
   Received 0 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   19 packets output, 2020 bytes, 0 underruns
   0 output errors, 0 collisions, 0 interface resets
   0 unknown protocol drops
   0 output buffer failures, 0 output buffers swapped out
```


https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 3-3: Implement Spoke-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN

Activity Objective

In this exercise, you use an incremental approach when deploying a scalable FlexVPN hub-and-spoke environment with spoke-to-spoke shortcut switching. An environment consisting of two spokes being able to communicate with the hub is already configured. You will configure BGP and enable spoke-to-spoke shortcut switching.

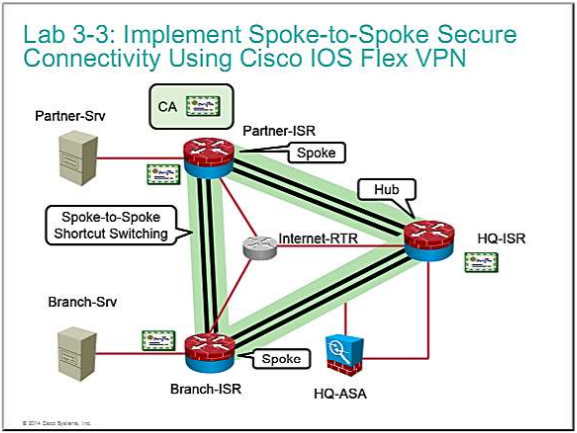
Upon completing this activity, you will be able to meet these objectives:

- Configure BGP in the Hub-and-Spoke Topology
- Configure Spoke-to-Spoke Shortcut Switching

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

Three Cisco IOS routers

Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

Cisco IOS Commands

Command	Description
[no] crypto ikev2 authorization policy default	Modify (disable) the default IKEv2 authorization policy.
[no] interface Tunnel *tunnel_ID*	Creates a new tunnel interface and enters tunnel interface configuration mode. The no option will remove Tunnel interface from the device.
[no] network *network wild-card-mask* **area** *area-ID*	Enables or disables OSPF routing for network in selected area.
[no] router ospf *process-ID*	Enables or disables OSPF routing process. Enters routing process configuration mode.
[no] shutdown	Enables or disables interface.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Command	Description
aggregate-address *IP-range*	Summarize BGP networks using a supernet; configured in BGP configuration mode.
bgp listen range *range* **peer-group** *peer-group-name*	Accept BGP sessions from the specified IP range; configured in BGP configuration mode.
crypto ikev2 authorization policy *policy-name*	Define an IKEv2 authorization policy (config mode).
crypto ikev2 profile *profile-name*	Creates an IKEv2 profile and enters crypto profile configuration mode.
debug nhrp	Enables NHRP protocol debugging.
distance *AD-distance*	When configured in OSPF routing protocol, changes administrative distance to the OSPF routes.
interface Virtual-Template *vt_ID* **type tunnel**	Configures virtual template interface with type tunnel.
ip nhrp network-id *network-id*	Enables NHRP network ID to the interface.
ip nhrp redirect	Enable NHRP redirects; configured on the hub.
ip nhrp shortcut virtual-template *VT-ID*	Enable spoke-to-spoke shortcut switching by cloning the specified virtual template interface; configured in the virtual template interface configuration mode.
ip unnumbered *interface*	Assigns an IP subnet and address to the interface.
match identity remote fqdn *fqdn-name*	Enables FQDN name matching in the crypto IKEv2 policy.
neighbor *peer-group* **peer-group | remote-as | update-source** *parameter*	Configures a BGP session using various parameters, such as a peer-group or remote AS number; configured in BGP configuration mode.
network *network* **mask** *mask*	Advertise a network in BGP; configured in BGP configuration mode.
ping *ip-destination*	Verifies IP connectivity to the remote IP destination.
pool *pool-name*	Specifies local IP address pool to be used by the IKEv2 authorization policy.
router bgp *AS-number*	Enables BGP routing process and enters routing process configuration mode.
show crypto ikev2 sa	Displays current IKEv2 SAs.
show crypto ipsec sa	Verifies the status of the IPsec SAs.
show ip bgp	Displays BGP routes.
show ip route	Displays IPv4 routes in the routing table.
tunnel protection ipsec profile *profile-name*	Enables tunnel protection to use IPsec profile.
virtual-template	Configured in IKEv2 profile configuration mode, specifies the virtual template interface used for cloning virtual access interfaces to service tunnels on-demand.

Job Aids

These job aids are available to help you complete the lab activity.

https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

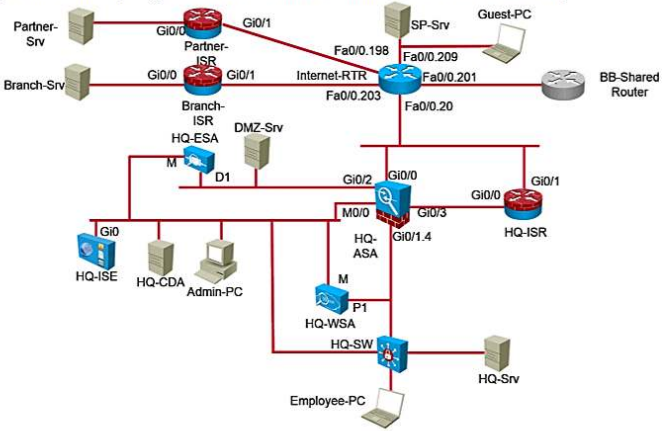
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

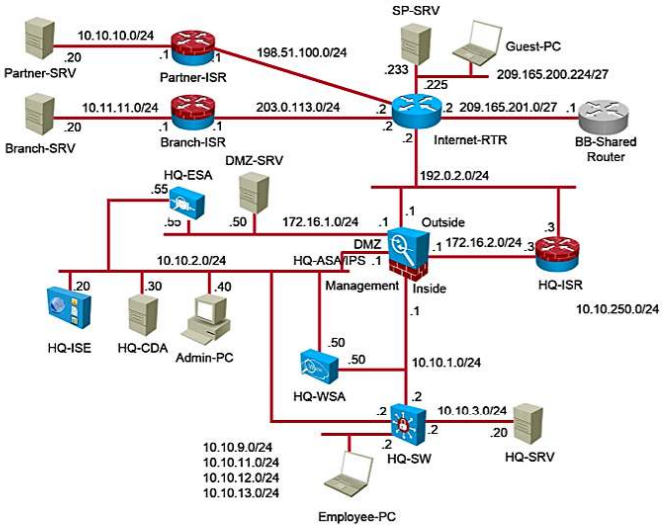
https://t.me/learningnets

Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



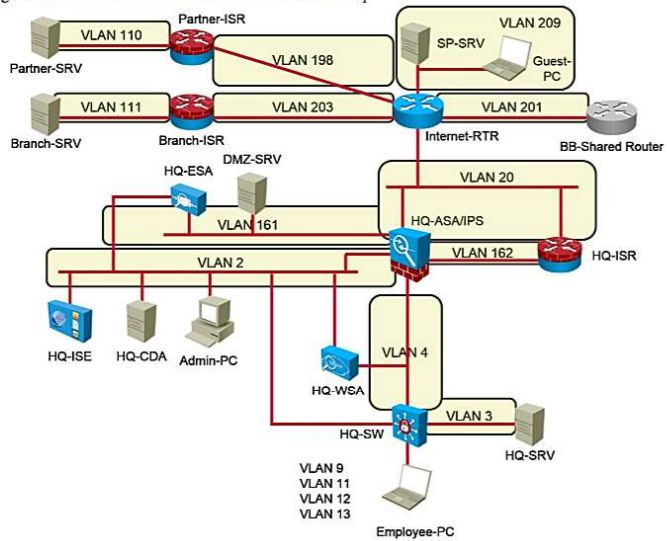
The figure shows the IP addresses that are used in this lab setup.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Configure BGP

In this task you will configure BGP routing to exchange reachability information about subnets attached to each spoke.

Note	BGP is demonstrated in this exercise because it is recommended due to its high scalability.

Activity Procedure

Complete the following steps:

Step 1

Remove the OSPF process from the Branch-ISR and disable OSPF on the tunnel subnet on HQ-ISR. In the next step, you will tune the administrative distance of OSPF to address the issue of the overlapping network 10.10.10.0/24, which is available in the partner and also in the HQ site. In this BGP scenario for spoke-to-spoke shortcut switching, you will prefer the routing information exchanged via BGP. This will effectively prevent connectivity between the Branch site and the 10.10.10.0/24 network in the HQ. Alternatively you may deploy NAT on the Branch-ISR but NAT is not typical in combination with BGP.

Step 2

Increase the OSPF administrative distance on HQ-ISR to a value that is higher (less believable) than that of internal BGP. You may use, for example, 210.

Note	The default administrative distance of internal BGP is 200.

Step 3

Configure BGP on Branch-ISR:

A) Use autonomous system (AS) ID 65001.

B) Advertise local network (10.11.11.0/24).

C) Configure IBGP session with HQ-ISR (10.10.100.99).

To configure BGP on Branch-ISR, enter these commands on Branch-ISR:

```
Branch-ISR(config)# router bgp 65001
Branch-ISR(config-router)# network 10.11.11.0 mask 255.255.255.0
Branch-ISR(config-router)# neighbor 10.10.100.99 remote-as 65001
```

Step 4

Configure BGP on Partner-ISR:

A) Use autonomous system (AS) ID 65001.

B) Advertise local network (10.10.10.0/24).

C) Configure IBGP session with HQ-ISR (10.10.100.99).

To configure BGP on Partner-ISR, enter these commands on Partner-ISR:

```
Partner-ISR(config)# router bgp 65001
Partner-ISR(config-router)# network 10.10.10.0 mask 255.255.255.0
Partner-ISR(config-router)# neighbor 10.10.100.99 remote-as 65001
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 5

Configure BGP on HQ-ISR:

A) Use autonomous system (AS) ID 65001.

B) Accept connections from the IP range 10.10.100.0/24 (using the **bgp listen range** command) and add the peers to the peer group 'spokes'.

C) Advertise a summary address (10.0.0.0/8) of the spoke subnets using the **aggregate-address** command.

D) Define a peer group (spokes) with these characteristics:

Members of the same AS (65001)

Source packets from Loopback0 interface

To configure BGP on HQ-ISR, enter these commands on HQ-ISR:

```
HQ-ISR(config)# router bgp 65001
HQ-ISR(config-router)# bgp listen range 10.10.100.0/24 peer-group spokes
HQ-ISR(config-router)# aggregate-address 10.0.0.0 255.0.0.0
HQ-ISR(config-router)# neighbor spokes peer-group
HQ-ISR(config-router)# neighbor spokes remote-as 65001
HQ-ISR(config-router)# neighbor spokes update-source Loopback0
```


https://t.me/learningnets

Activity Verification

Step 1

Verify BGP and IP routing information on Branch-ISR:

```
Branch-ISR# show ip bgp
BGP table version is 3, local router ID is 203.0.113.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
     Network          Next Hop            Metric LocPrf Weight Path
 *>i 10.0.0.0         10.10.100.99             0    100      0 i
 *>  10.11.11.0/24    0.0.0.0                  0         32768 i
Branch-ISR# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
Gateway of last resort is 203.0.113.2 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 203.0.113.2
      10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
B        10.0.0.0/8 [200/0] via 10.10.100.99, 00:00:14
C        10.10.100.1/32 is directly connected, Tunnel0
S        10.10.100.99/32 is directly connected, Tunnel0
C        10.11.11.0/24 is directly connected, GigabitEthernet0/0
L        10.11.11.1/32 is directly connected, GigabitEthernet0/0
      203.0.113.0/24 is variably subnetted, 2 subnets, 2 masks
C        203.0.113.0/24 is directly connected, GigabitEthernet0/1
L        203.0.113.1/32 is directly connected, GigabitEthernet0/1
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 2

Verify BGP and IP routing information on Partner-ISR:

```
Partner-ISR# show ip bgp
BGP table version is 3, local router ID is 198.51.100.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
     Network          Next Hop            Metric LocPrf Weight Path
 *>i 10.0.0.0         10.10.100.99             0    100      0 i
 *>  10.10.10.0/24    0.0.0.0                  0         32768 i
Partner-ISR# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
Gateway of last resort is 198.51.100.2 to network 0.0.0.0
S*     0.0.0.0/0 [1/0] via 198.51.100.2
      10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
B        10.0.0.0/8 [200/0] via 10.10.100.99, 00:01:21
C        10.10.10.0/24 is directly connected, GigabitEthernet0/0
L        10.10.10.1/32 is directly connected, GigabitEthernet0/0
C        10.10.100.6/32 is directly connected, Tunnel0
S        10.10.100.99/32 is directly connected, Tunnel0
      198.51.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        198.51.100.0/24 is directly connected, GigabitEthernet0/1
L        198.51.100.1/32 is directly connected, GigabitEthernet0/1
```


https://t.me/learningnets

Step 3

Verify BGP and IP routing information on HQ-ISR. You should see the two spoke networks received via BGP. (The next hop addresses in the output of the **show ip bgp** command might be different from what is shown in the lab.)

```
HQ-ISR# show ip bgp
BGP table version is 4, local router ID is 10.10.100.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.0.0.0         0.0.0.0                              32768 i
 *>i 10.10.10.0/24    10.10.100.6              0    100      0 i
 *>i 10.11.11.0/24    10.10.100.1              0    100      0 i
HQ-ISR# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
Gateway of last resort is 192.0.2.2 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 192.0.2.2
      10.0.0.0/8 is variably subnetted, 13 subnets, 3 masks
B        10.0.0.0/8 [200/0] via 0.0.0.0, 00:02:26, Null0
O        10.10.1.0/24 [210/11] via 172.16.2.1, 00:09:43, GigabitEthernet0/0
O        10.10.2.0/24 [210/12] via 172.16.2.1, 00:09:43, GigabitEthernet0/0
O        10.10.3.0/24 [210/12] via 172.16.2.1, 00:09:43, GigabitEthernet0/0
O        10.10.9.0/24 [210/12] via 172.16.2.1, 00:09:43, GigabitEthernet0/0
B        10.10.10.0/24 [200/0] via 10.10.100.6, 00:02:26
O        10.10.11.0/24 [210/12] via 172.16.2.1, 00:09:43, GigabitEthernet0/0
O        10.10.12.0/24 [210/12] via 172.16.2.1, 00:09:43, GigabitEthernet0/0
O        10.10.13.0/24 [210/12] via 172.16.2.1, 00:09:43, GigabitEthernet0/0
S        10.10.100.1/32 is directly connected, Virtual-Access1
S        10.10.100.6/32 is directly connected, Virtual-Access2
C        10.10.100.99/32 is directly connected, Loopback0
B        10.11.11.0/24 [200/0] via 10.10.100.1, 00:02:26
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O        172.16.1.0/24 [210/11] via 172.16.2.1, 00:09:43, GigabitEthernet0/0
C        172.16.2.0/24 is directly connected, GigabitEthernet0/0
L        172.16.2.3/32 is directly connected, GigabitEthernet0/0
      192.0.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.0.2.0/24 is directly connected, GigabitEthernet0/1
L        192.0.2.3/32 is directly connected, GigabitEthernet0/1
```

Note If you didn't increase the OSPF distance, the network 10.10.10.0/24 network received via BGP would report a RIB failure and would not be inserted into the routing table.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Task 2: Configure Spoke-to-Spoke Shortcut Switching

In this task you will configure spoke-to-spoke shortcut switching.

Note	With two spokes being able to communicate with the hub, you will enable spoke-to-spoke shortcut switching. This scenario requires appropriate NHRP settings to be configured on the hub and the spokes.

Activity Procedure

Complete the following steps:

Step 1

Disable (shutdown) the Tunnel 0 interface on each spoke routers (Branch-ISR and Partner-ISR). This will unlock the virtual template on the hub and allow you to edit the settings.

Step 2

Configure NHRP on the hub (HQ-ISR):

A) Configure NHRP network ID (1)

B) Enable NHRP redirects.

Note	NHRP redirects will be sent from the hub to spokes to create the shortcuts.

Step 3

On Branch-ISR and Partner-ISR, configure a virtual template interface (1) that will be used for cloning the virtual access interfaces for the shortcut switching. Use these settings:

A) Type: **tunnel**

B) IP address: **unnumbered from Tunnel 0**

C) NHRP network ID: **1**

D) NHRP shortcuts: **using Virtual Template (1)**

E) Tunnel protection IPsec profile: **ccnp-ipsec-profile**

Step 4

On Branch-ISR and Partner-ISR, bind the virtual template interface (1) to the IKEv2 profile.

Step 5

On Branch-ISR and Partner-ISR, configure the Tunnel 0 interface for NHRP:

A) Use the same NHRP network ID (1).

B) Enable NHRP shortcuts by cloning the Virtual Template (1) interface

https://t.me/learningnets

Step 6

On Branch-ISR, add match statement on crypto IKEv2 profile (ccnp-ikev2-profile) to additionally match **partner.public** domain:

Step 7

Re-enable the Tunnel 0 interface on each spoke routers (Branch-ISR and Partner-ISR). The tunnels from each spoke to the hub should automatically come up.

Activity Verification

Step 1

Before you trigger spoke-to-spoke shortcuts verify that the routing tables on the spokes do not contain any entries marked with 'H'. H is used to mark NHRP entries.

```
Branch-ISR# show ip route nhrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
Gateway of last resort is 203.0.113.2 to network 0.0.0.0
```

```
Partner-ISR# show ip route nhrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
Gateway of last resort is 198.51.100.2 to network 0.0.0.0
```

Step 2

On HQ-ISR, enable NHRP protocol debugging using the **debug nhrp** command.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 3

From Partner-ISR, trigger a shortcut by pinging the Branch-srv IP address (10.11.11.20). You should see that the a shortcut virtual access interface comes up:

```
Partner-ISR# ping 10.11.11.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.11.11.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
Partner-ISR#
Dec 11 11:46:13.739: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to up
```

Step 4

Verify that a NHRP route has been added on the Partner-ISR. (The IP addresses in the NHRP route may be different in your pod from what is shown in the output.)

```
Partner-ISR# show ip route nhrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
Gateway of last resort is 198.51.100.2 to network 0.0.0.0
      10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
H        10.10.100.7/32 [250/1] via 10.10.100.7, 00:00:40, Virtual-Access1
```


https://t.me/learningnets

Step 5

From Branch-ISR, trigger a shortcut by pinging the Partner-srv (10.10.10.20). Verify that a NHRP route has been added on the Branch-ISR. (You may find different NHRP routes in your pod.)

```
Branch-ISR# ping 10.10.10.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Branch-ISR# show ip route nhrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
Gateway of last resort is 203.0.113.2 to network 0.0.0.0
      10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
H        10.10.100.8/32 [250/1] via 10.10.100.8, 00:16:38, Virtual-Access1
H        10.10.100.9/32 [250/1] via 10.10.100.9, 00:00:12, Virtual-Access1
```

Step 6

Examine the NHRP debugging output on the hub. You should see the process of providing the overlay addresses to create the shortcuts. You should also notice that the shortcuts are established in both directions (because ICMP requests and replies flow in both directions).

```
Jun 27 13:28:11.083: NHRP: Tunnels gave us remote_nbma: 198.51.100.1 for Redirect
Jun 27 13:28:11.083: NHRP: Attempting to Redirect, remote_nbma: 198.51.100.1
Jun 27 13:28:11.083: NHRP: inserting (198.51.100.1/10.11.11.20) in redirect table
Jun 27 13:28:11.083: NHRP-ATTR:  Requester Ext Len: Total ext_len  with NHRP
attribute VPE 16
Jun 27 13:28:11.083: NHRP: Attempting to send packet via DEST 10.10.10.1
Jun 27 13:28:11.083: NHRP: Send Traffic Indication via Virtual-Access2 vrf 0, packet
size: 84
Jun 27 13:28:11.083:       src: 10.10.100.99, dst: 10.10.10.1
Jun 27 13:28:11.083: NHRP: 108 bytes out Virtual-Access2
Jun 27 13:28:11.087: NHRP: Tunnels gave us remote_nbma: 203.0.113.1 for Redirect
Jun 27 13:28:11.087: NHRP: Attempting to Redirect, remote_nbma: 203.0.113.1
Jun 27 13:28:11.087: NHRP: inserting (203.0.113.1/10.10.10.1) in redirect table
Jun 27 13:28:11.087: NHRP-ATTR:  Requester Ext Len: Total ext_len  with NHRP
attribute VPE 16
Jun 27 13:28:11.087: NHRP: Attempting to send packet via DEST 10.10.100.1
Jun 27 13:28:11.087: NHRP: Send Traffic Indication via Virtual-Access1 vrf 0, packet
size: 84
Jun 27 13:28:11.087:       src: 10.10.100.99, dst: 10.10.100.1
Jun 27 13:28:11.087: NHRP: 108 bytes out Virtual-Access1
<output omitted>
```

On HQ-ISR, disable all debugging using the **undebug all** command.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 7

On the spokes, verify that direct IKEv2 sessions have been negotiated between Branch-ISR and Partner-ISR:

```
Partner-ISR# show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA
Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         198.51.100.1/500      192.0.2.3/500         none/none            READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:20, Auth sign: RSA, Auth
verify: RSA
      Life/Active Time: 86400/11456 sec
Tunnel-id Local                 Remote                fvrf/ivrf            Status
3         198.51.100.1/500      203.0.113.1/500       none/none            READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:20, Auth sign: RSA, Auth
verify: RSA
      Life/Active Time: 86400/1112 sec
 IPv6 Crypto IKEv2  SA
```


https://t.me/learningnets

Step 8

On the spokes, verify that direct IPsec SAs have been negotiated for the virtual access interface:

```
Partner-ISR# show crypto ipsec sa
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 198.51.100.1
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (198.51.100.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.0.2.3/255.255.255.255/47/0)
   current_peer 192.0.2.3 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 460, #pkts encrypt: 460, #pkts digest: 460
    #pkts decaps: 1662, #pkts decrypt: 1662, #pkts verify: 1662
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 198.51.100.1, remote crypto endpt.: 192.0.2.3
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0x372D9DA1(925736353)
     PFS (Y/N): Y, DH group: group20
     inbound esp sas:
      spi: 0xDB6C5D1F(3681312031)
        transform: esp-gcm 256 ,
        in use settings ={Tunnel, }
        conn id: 2012, flow_id: Onboard VPN:12, sibling_flags 80000040, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4340679/2390)
        IV size: 8 bytes
        replay detection support: N
        Status: ACTIVE(ACTIVE)
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x372D9DA1(925736353)
        transform: esp-gcm 256 ,
        in use settings ={Tunnel, }
        conn id: 2011, flow_id: Onboard VPN:11, sibling_flags 80000040, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4340697/2390)
        IV size: 8 bytes
        replay detection support: N
        Status: ACTIVE(ACTIVE)

     outbound ah sas:
     outbound pcp sas:
interface: Virtual-Access1
    Crypto map tag: Virtual-Access1-head-0, local addr 198.51.100.1
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (198.51.100.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (203.0.113.1/255.255.255.255/47/0)
   current_peer 203.0.113.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 23, #pkts encrypt: 23, #pkts digest: 23
    #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

```
    local crypto endpt.: 198.51.100.1, remote crypto endpt.: 203.0.113.1
    path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
    current outbound spi: 0x36431E2(56898018)
    PFS (Y/N): N, DH group: none
    inbound esp sas:
     spi: 0x9D670707(2640774919)
       transform: esp-gcm 256 ,
       in use settings ={Tunnel, }
       conn id: 2007, flow_id: Onboard VPN:7, sibling_flags 80000040, crypto map:
Virtual-Access1-head-0
       sa timing: remaining key lifetime (k/sec): (4267422/2360)
       IV size: 8 bytes
       replay detection support: N
       Status: ACTIVE(ACTIVE)
    inbound ah sas:
    inbound pcp sas:
    outbound esp sas:
     spi: 0x36431E2(56898018)
       transform: esp-gcm 256 ,
       in use settings ={Tunnel, }
       conn id: 2008, flow_id: Onboard VPN:8, sibling_flags 80000040, crypto map:
Virtual-Access1-head-0
       sa timing: remaining key lifetime (k/sec): (4267421/2360)
       IV size: 8 bytes
       replay detection support: N
       Status: ACTIVE(ACTIVE)
    outbound ah sas:
    outbound pcp sas:
```

Step 9

Verify that the spoke-to-spoke traffic takes the shortcut using the **traceroute** command. In the trace output the next hop should be the spoke tunnel IP address, and not 10.10.100.99, as before.

```
Partner-ISR# traceroute 10.11.11.20
Type escape sequence to abort.
Tracing the route to 10.11.11.20
VRF info: (vrf in name/id, vrf out name/id)
  1 10.10.100.1 0 msec 0 msec 0 msec
  2 10.11.11.20 4 msec 0 msec 4 msec
```


https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 4-1: Implement ASA Basic Clientless SSL VPN

Activity Objective

In this lab activity you will deploy clientless SSL VPNs on the Cisco Adaptive Security Appliance. You will access the SSL VPN portal from the Guest-PC, which is located to the Service Provider subnet. After enabling the clientless SSL VPN connections, you will see that the client browser reports security problems with the server certificate. To resolve the problem, you will enroll the ASA with the certificate authority running on the HQ-Srv. This will enable the browser on the Guest-PC to trust the ASA certificate. Finally you will create a bookmark and test connectivity through the SSL VPN portal.

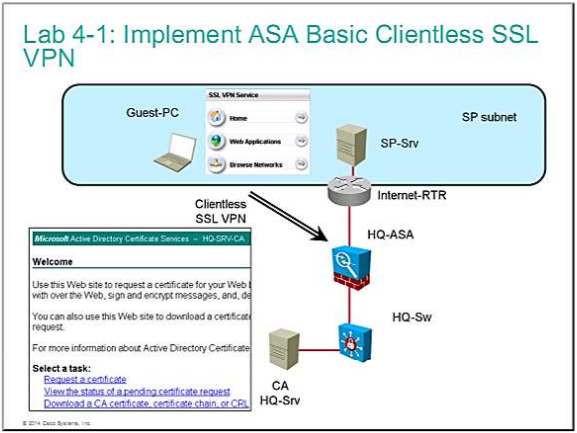
Upon completing this activity, you will be able to meet these objectives:

- Enable basic clientless SSL VPN connections on the Cisco ASA
- Enroll the ASA with the PKI
- Configure a bookmark and test connectivity through the SSL VPN portal

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

Cisco ASA adaptive security appliance

Command List

No commands are needed to complete this lab exercise. All tasks are performed with the Cisco Adaptive Security Device Manager GUI interface.

Job Aids

These job aids are available to help you complete the lab activity.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

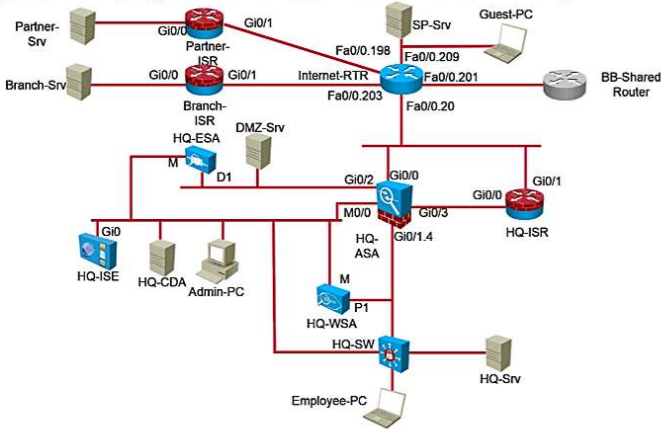
https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

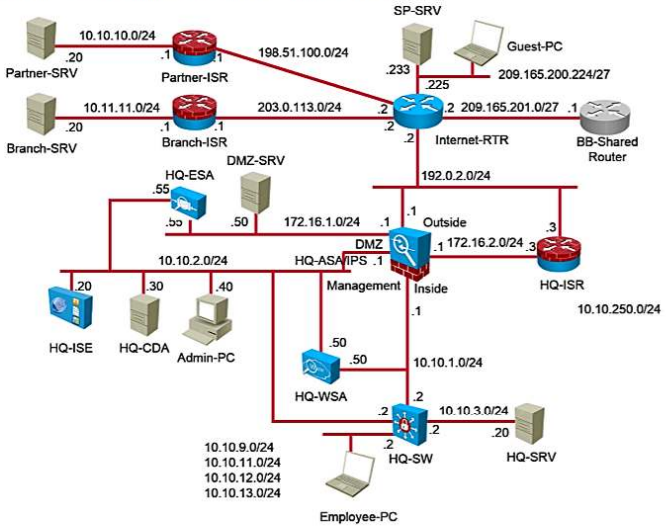
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



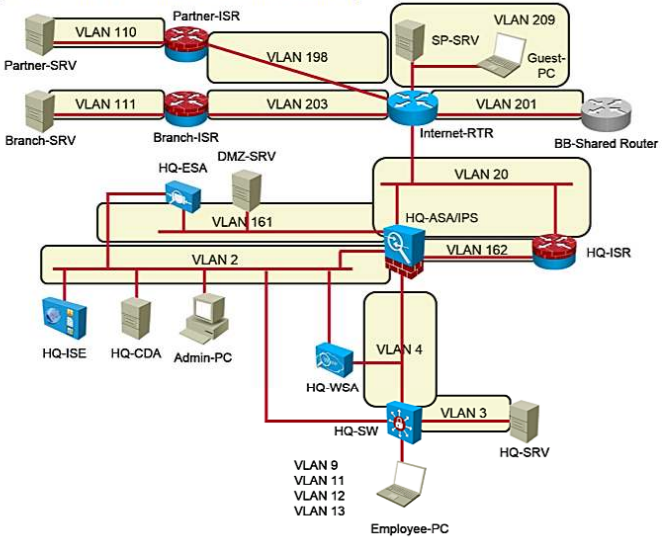
The figure shows the IP addresses that are used in this lab setup.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Enable Clientless SSL VPN Connections

In this task, you will enable clientless SSL VPN on the HQ-ASA.

Activity Procedure

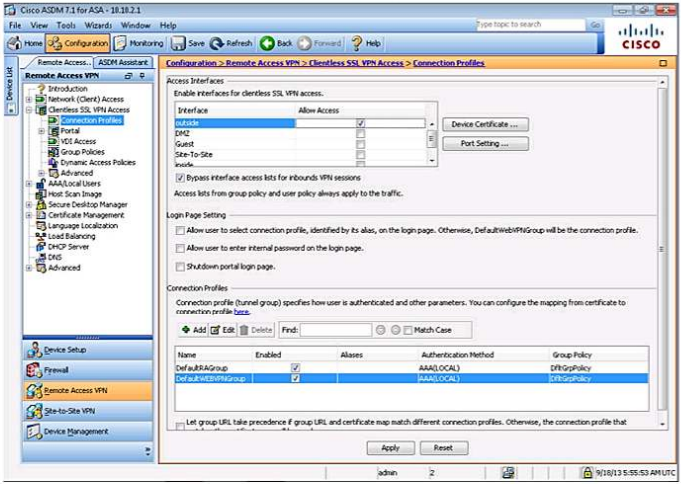
Complete the following steps:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 1

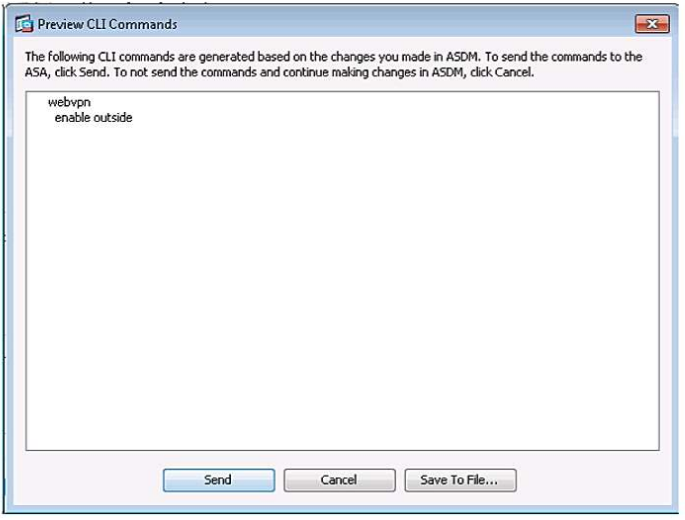
Use Cisco ASDM from Admin-PC to access the HQ-ASA at IP address 10.10.2.1.

Navigate to the **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles** and check the check box next to the outside interface.



Click the **Apply** button.

https://t.me/learningnets



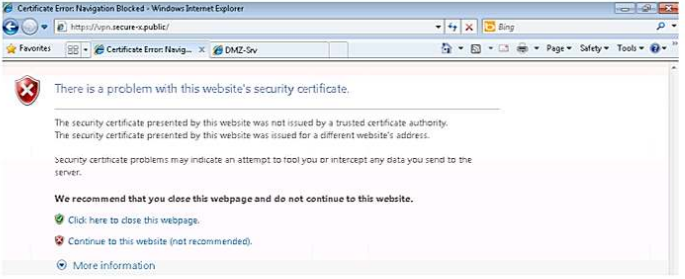
Preview the commands sent to the HQ-ASA and click the **Send** button.

Activity Verification

In the verification procedure use the Internet Explorer, because it uses a different certificate store than the Chrome and Firefox browsers. You have completed this task when you attain this result:

Step 1

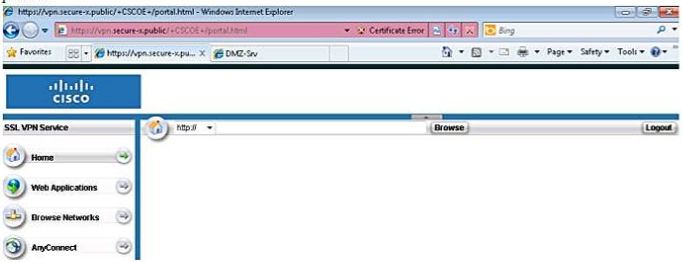
From the Guest-PC open the Internet Explorer and access **https://vpn.secure-x.public**. You will see a security warning because the Guest-PC browser cannot validate the VPN server certificate. The VPN server (HQ-ASA) has not yet been enrolled in the PKI.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

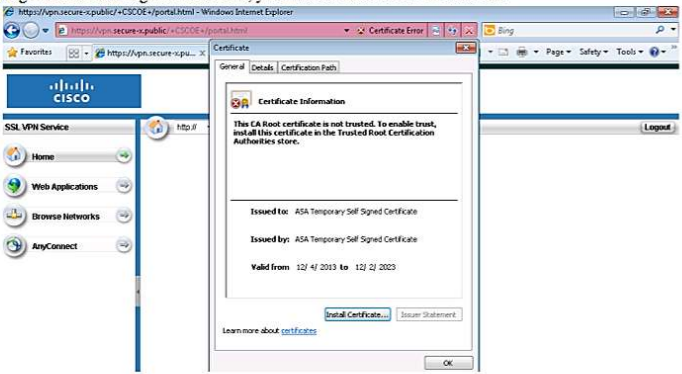
Step 2

Continue to this website and log in as user **admin** with password **Ci5coAdmin.** You will access the SSL VPN portal.



Step 3

Click the Certificate Error field in the URL window and then the View Certificates button. You will see the certificate information. The ASA temporary self-signed certificate is not trusted. Do **not** install it. Instead of installing the ASA self-signed certificate, you will enroll the ASA in the PKI.



Task 2: Enroll ASA in PKI

Having seen that the client receives a warning when connecting to the SSL VPN portal, you will now enroll the adaptive security appliance with the CA running on the HQ-Srv. To enroll the ASA with the PKI, you will install the CA root certificate on the ASA, generate a certificate signing request (CSR) on the ASA, issue the identity certificate on the HQ-Srv, and install the identity certificate on the ASA. The Guest-PC has already the HQ-Srv root certificate in its certificate store and will use it to validate the ASA certificate obtained from the HQ-Srv.

https://t.me/learningnets

Activity Procedure

Complete the following steps:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

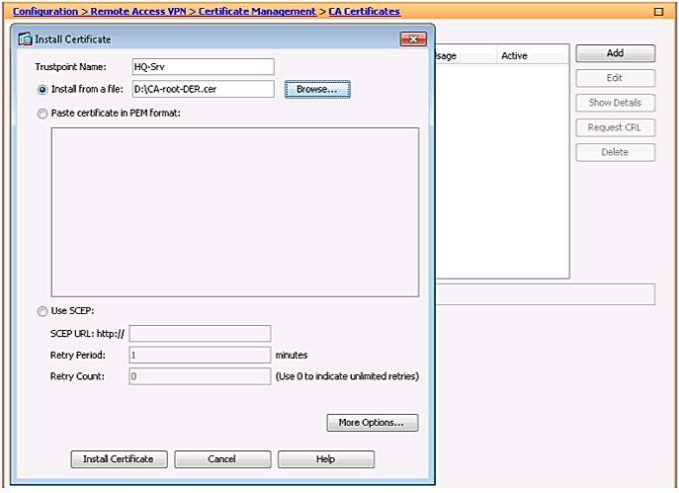
Step 1

Install the CA root certificate on the ASA:

A) In the ASDM, navigate to **Configuration > Remote Access VPN > Certificate Management > CA Certificates**. Add the CA root certificate using the trustpoint name **HQ-Srv.**

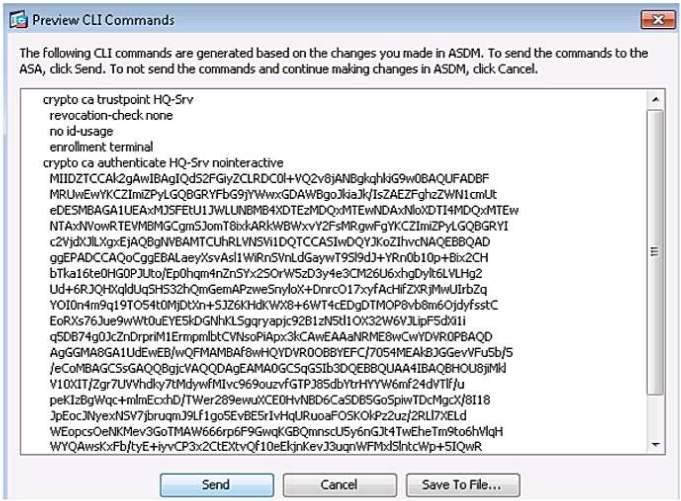
B) Choose Install from a file and select the CA root certificate file stored on the Admin-PC (D:\CA-root-DER.cer)

C) Click **Install Certificate**.



D) Preview the commands and send them to the ASA.

https://t.me/learningnets



E) Confirm the pop-up window about successful certified installation. Examine the certificate using the **Edit** and **Show Details** buttons.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 2

Generate a Certificate Signing Request (CSR) on the ASA. The CSR will contain the ASA's identity information and public RSA key. You will later submit this CSR to the CA and the CA will issue an identity certificate for the ASA.

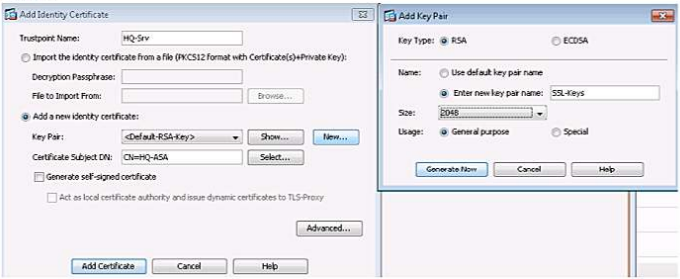
A) In the ASDM, navigate to **Configuration > Remote Access VPN > Certificate Management > Identity Certificates**

B) Click **Add**. Choose **Add a new identity certificate** radio button.

C) Set the trustpoint name to **HQ-Srv**.

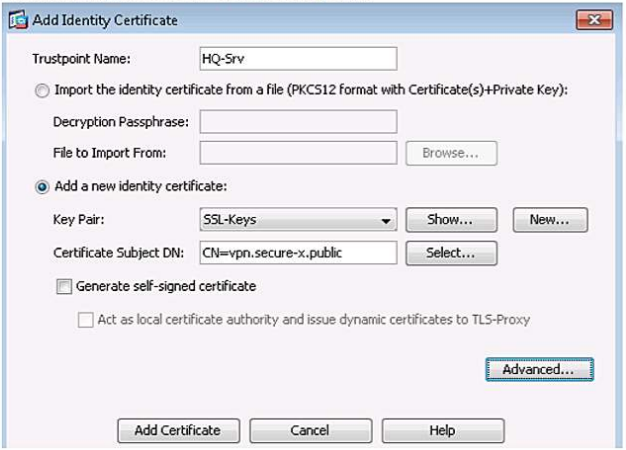


D) Click the **New** button to generate a new RSA key pair. Set its length to 2048 bits. Set the name to **SSL-Keys**. Click the **Generate Now** button. If **SSL-Keys** RSA key pair already exists, select it from **Key Pair** menu.

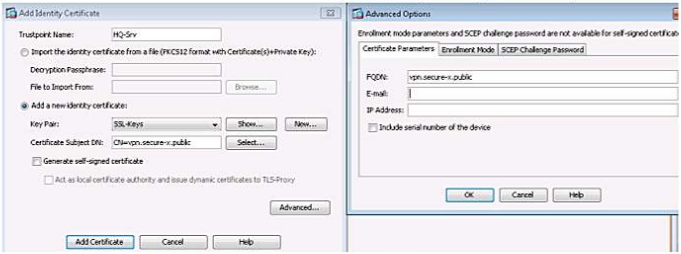


Note	2048 is the minimum size for the web server certificate template configured on the HQ-SRV CA.

E) Set the Certificate Subject DN to **CN=vpn.secure-x.public**.



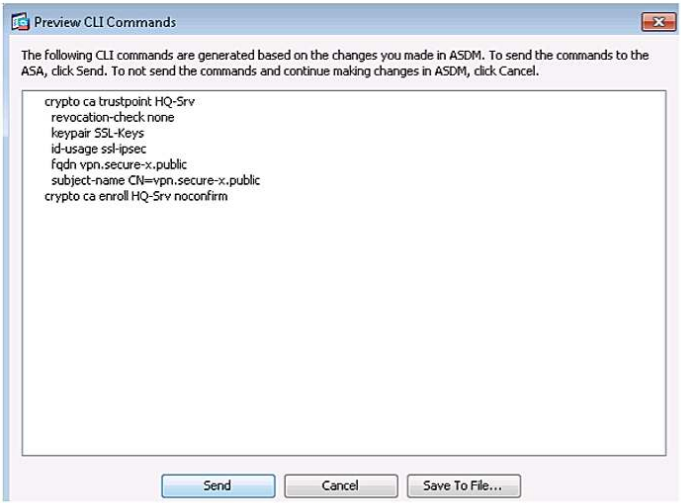
F) Click **Advanced**. In the **Certificate Parameters** tab, set the FQDN to **vpn.secure-x.public**



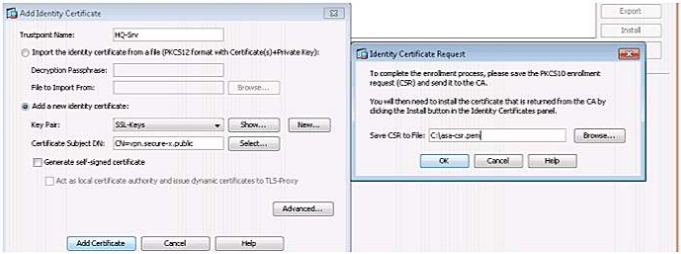
G) Examine the remaining settings (manual request) and click **OK**.

H) Click **Add Certificate**, preview and send the commands.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



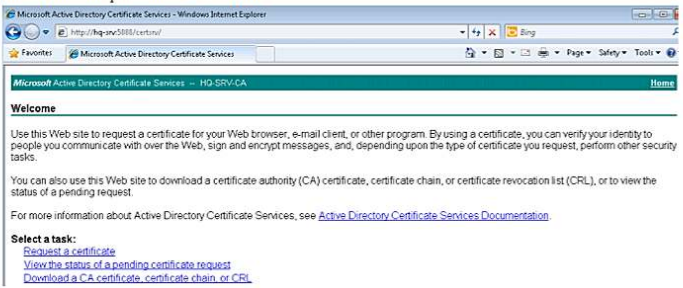
I) Save the certificate signing request as **asa-csr.pem** on disk C:\.



Step 3

Submit the CSR to the certificate authority:

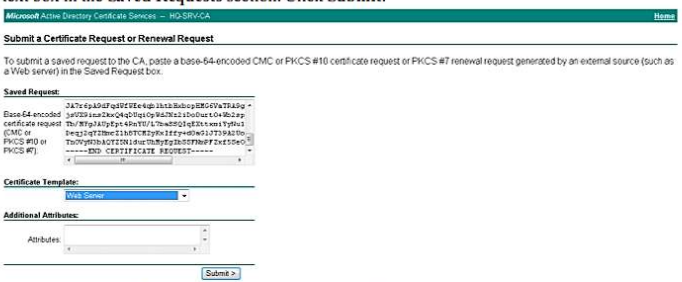
A) On the Admin-PC, open a web browser and connect to http://hq-srv:5080/certsrv. Log in as administrator with password Ci5coAdmin.



B) Click **Request a Certificate**, choose to submit an **advanced certificate request**, and then submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

C) In the **Certificate Template** drop-down list, choose **Web Server**.

D) Open WordPad, open the **C:\asa-csr.pem** file, and copy the entire contents of the CSR and paste it into the text box in the **Saved Requests** section. Click **Submit**.



E) Click **Download Certificate** and save the certificate as **C:\asa-cert.cer**.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 4

Install the obtained identity certificate on the ASA:

A) In the ASDM, return to **Configuration > Remote Access VPN > Certificate Management > Identity Certificates** and click the **Install** button for the certificate that is now in the enrollment procedure.



B) Select the **Install from a file option**, browse to select the file (**C:\asa-cert.cer**), and then click **Install Certificate**. Preview and send the commands to the ASA. Accept the popup window about the successful certificate import.

C) Examine the installed identity certificate using the **Show Details** button.

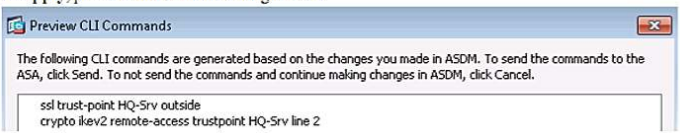
Step 5

Use the obtained identity certificate for the SSL VPN termination. The certificate used in the SSL VPNs has several consequences: a) the ASA will send this identity certificate in the initial SSL handshake with the clients, b) the clients will attempt to validate this certificate, possibly using the CA root certificate, c) the ASA will sign the VPN data using the generated ASA private key, and d) the clients will verify the signatures using the corresponding ASA public key, which is embedded in the identity certificate.

A) In the ASDM, go to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**, click the **Device Certificate** button, select the installed identity certificate.



B) Click **Apply**, preview and send the configuration.

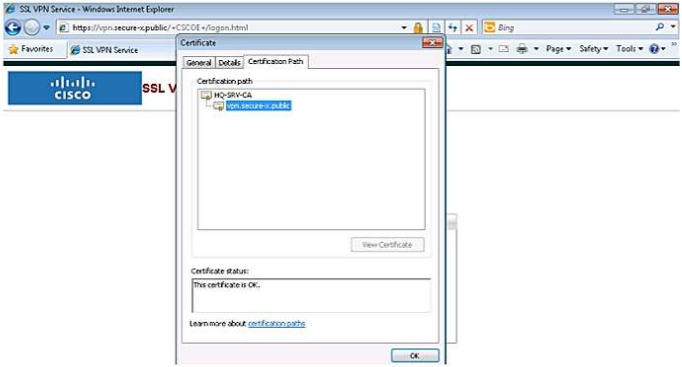


Activity Verification

In this verification procedure, you will first verify that the SS VPN client browser does not return any security warnings when connecting to the SSL VPN portal. Then you will examine the certificate store in the Guest-PC Internet Explorer and identify the CA root certificate used for validation of the ASA certificate. Finally, you will see that connections to the ASA's IP address and from other web browsers still return the security errors.

Step 1

In the Internet Explorer on the Guest-PC refresh the HTTPS session to **vpn.secure-x.public** There should be no warnings. Examine the certificate details by clicking the lock icon and the View certificates link. In the Certification Path tab, you will see that the the ASA identity certificate has been signed by the HQ-SRV-CA.

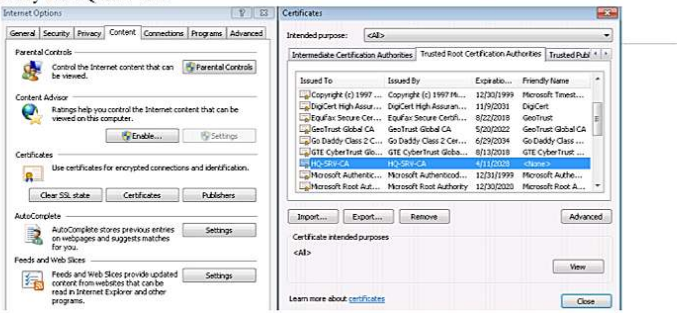


Step 2

Examine the certificate store in the Internet Explorer on the Guest-PC and identify the CA root certificate used for validation of the ASA certificate:

A) In the Internet Explorer on the Guest-PC, navigate to **Tools > Internet Options > Content > Certificates > Trusted Root Certification Authorities**.

B) Search for the HQ-SRV-CA certificate and optionally view it. This CA root certificate has been pre-installed on the Guest-PC and allows the Internet Explorer to validate the ASA identity certificate issued by the HQ-SRV-CA.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

From the Guest-PC, test other HTTPS connections to the VPN portal:

A) From the Internet Explorer, connect via HTTPS to ASA's outside IP address (192.0.2.1). You will get the security warning because the URL does not contain the FQDN embedded in the ASA identity certificate.

B) From the Mozilla Firefox browser, connect to https://vpn.secure-x.public. You will get a security warning because Firefox uses a dedicated certificate store. The Firefox's certificate store does not contain the HQ-SRV-CA root certificate and therefore cannot validate the ASA certificate.

C) From the Google Chrome browser, connect to https://vpn.secure-x.public. You will not get a security warning because Chrome uses the Microsoft certificate store.

Task 3: Configure a Bookmark

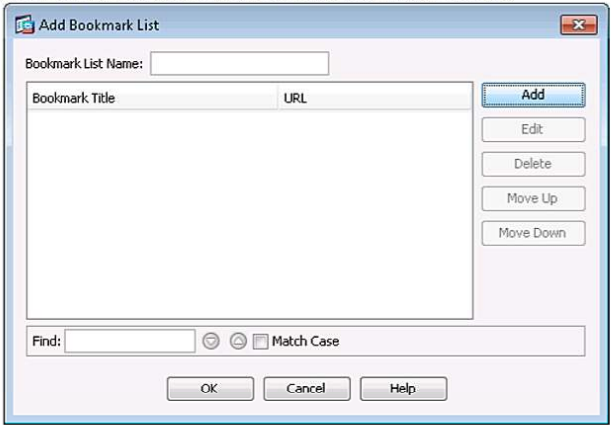
In this task, you will configure and test a bookmark.

Activity Procedure

Complete the following steps:

Step 1

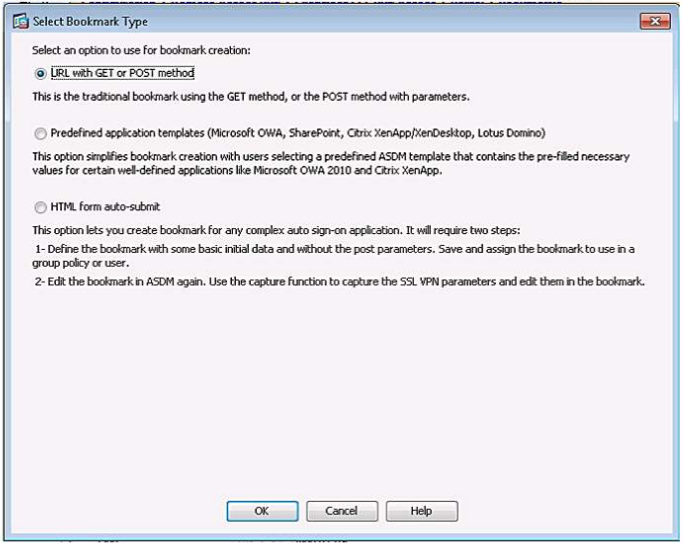
In the **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks** click the **Add** button to add new bookmark. The **Add Bookmark List** window will open.



https://t.me/learningnets

Step 2

In the **Add Bookmark List** window, click the **Add** button to add new bookmark item. The **Select Bookmark Type** window will open. Select the **URL with GET or POST method** option.

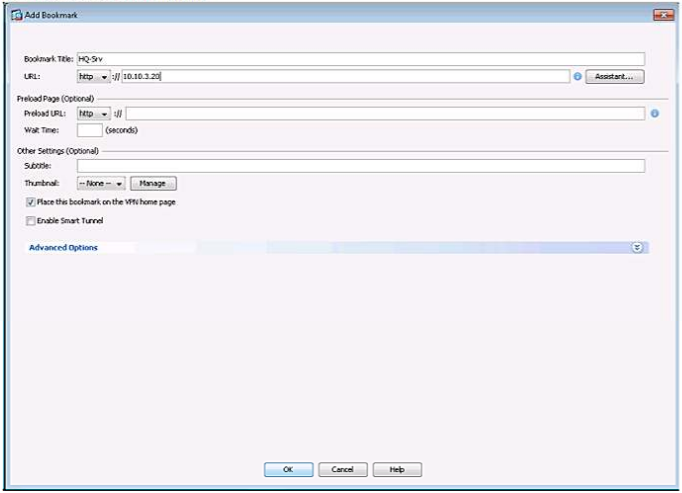


Click the **OK** button.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

In the **Add Bookmark** window, type **HQ-Srv** in the Bookmark Title field, and enter the IP address **10.10.3.20** next to the URL option.

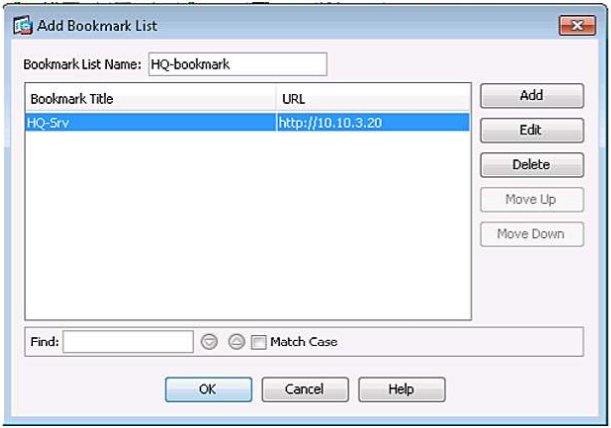


Click the **OK** button.

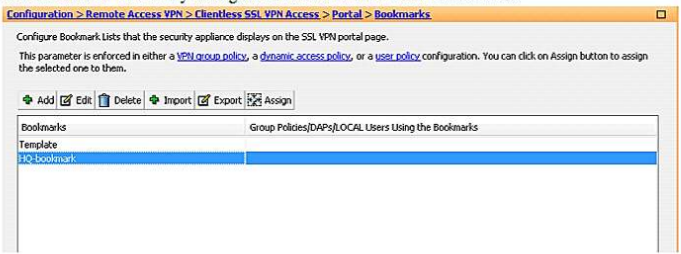
https://t.me/learningnets

Step 4

In the **Add Bookmark List** window, type **HQ-bookmark** in the **Bookmark List Name** field.



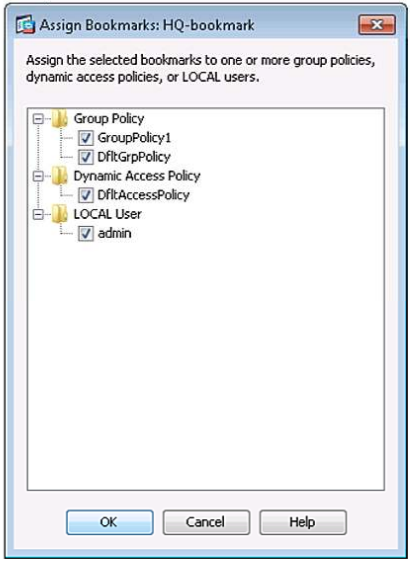
Click the **OK** button. The newly configured bookmark will be shown in the list.



https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 5

In the **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks** panel, select **HQ-bookmark** and click the **Assign** button to assign the newly created bookmark to the **Group Policy**, **Dynamic Access Policy** and **LOCAL User**.

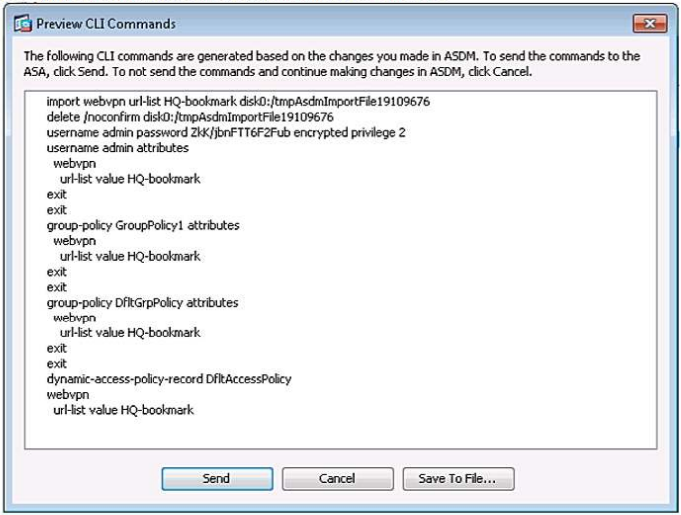


Click the **OK** button.

https://t.me/learningnets

Step 6

In the **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks** panel, click the **Apply** button. Examine the commands sent to the HQ-ASA.



Click the **Send** button.

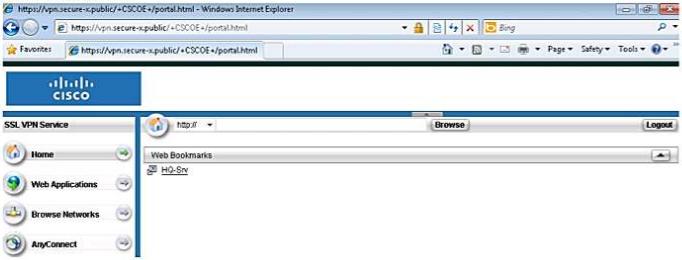
Activity Verification

You have completed this task when you attain this result:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 1

From the Internet Explorer on the Guest-PC access https://vpn.secure-x.public. Log in as **admin** with password **Ci5coAdmin.**



Step 2

Click the HQ-Srv Web Bookmark. You should see the web page of the HQ-Srv. In the upper right corner of the web page you will see the navigation pane, which allows you to move to another site, go to an address, go to the home page, or log out. Log out from the portal.



https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 4-2: Configure Application Access for Cisco ASA Clientless SSL VPN

Activity Objective

In this lab activity, you will deploy application plugins in the clientless SSL VPNs on the Cisco Adaptive Security Appliance, such as the SSH plugin to enable access to internal applications. Further, you will implement Smart Tunnels in the clientless SSL VPNs on the Cisco ASA, to enable access to TCP-based applications and enable the Smart Tunnel operation using RDP.

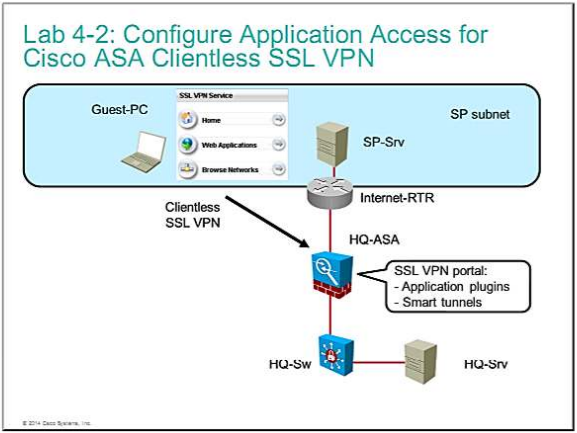
Upon completing this activity, you will be able to meet these objectives:

- Deploy application plugins in the clientless SSL VPNs
- Deploy Smart Tunnels in the clientless SSL VPNs

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

- Cisco ASA
- Client computer

Job Aids

These job aids are available to help you complete the lab activity.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

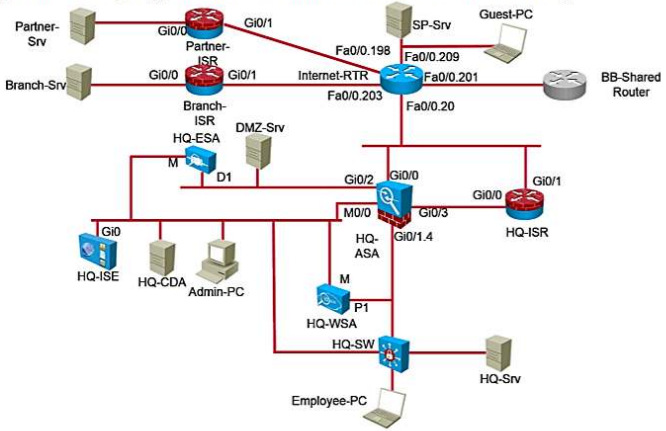
https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

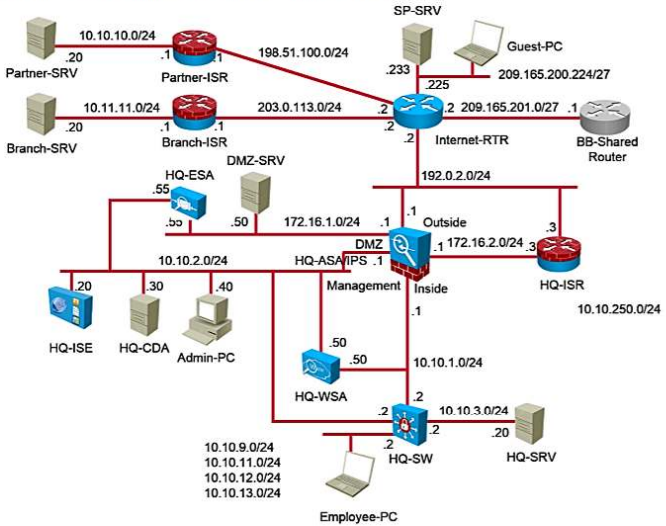
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



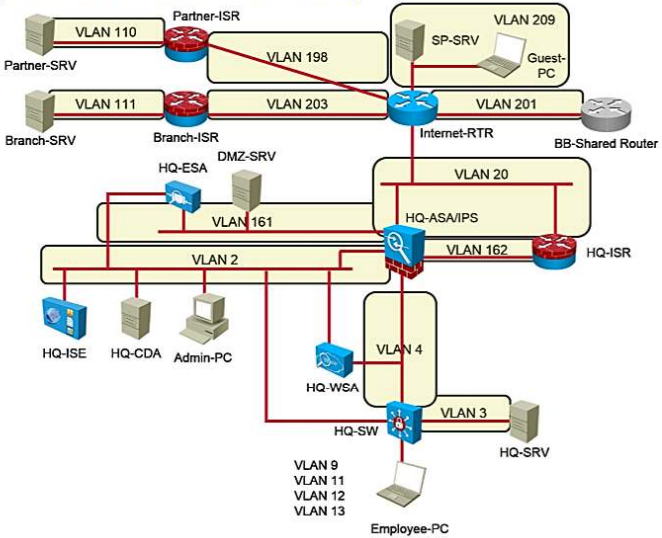
The figure shows the IP addresses that are used in this lab setup.



https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Configure Application Access Using Plugins

In this task you will configure application access using plugins. You will define custom group policy and connection profile for that purpose.

Activity Procedure

Complete the following steps:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

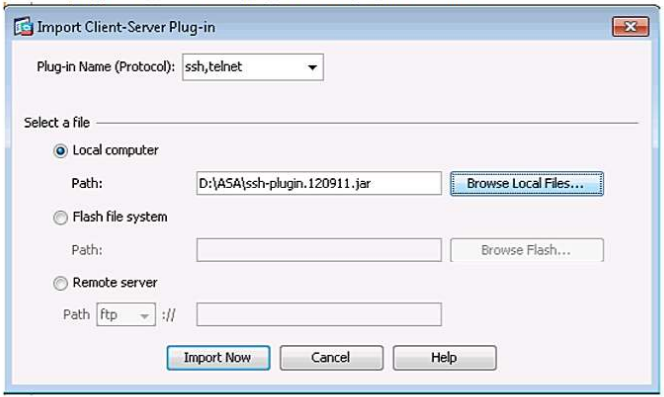
Step 1

Import the SSH/Telnet plugin to the adaptive security appliance:

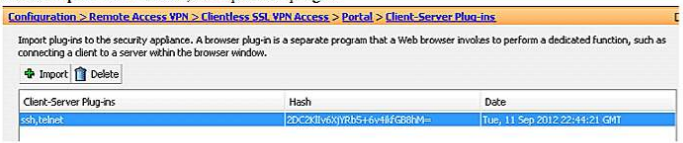
A) From the Admin-PC, log into the ASDM, and then go to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins**.

B) Click the **Import** button and choose the **ssh,telnet** protocol from the drop-down list.

C) Browse to the plugin file (**D:\ASA\ssh-plugin.120911.jar**) on the Admin PC.



Click the **Import Now** button, to import the plugin.



https://t.me/learningnets

Step 2

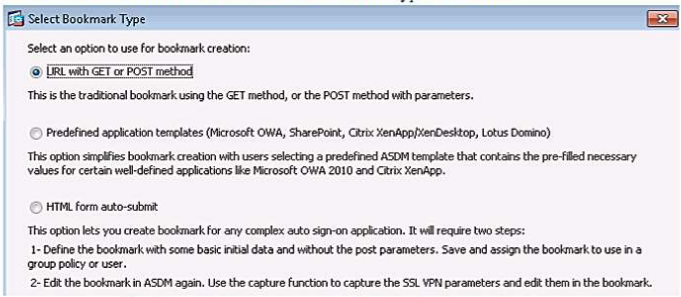
Add SSH and HTTP URLs to the existing bookmark list **HQ-bookmark.** Bookmarks provide the easiest method to define accessible resources.

A) In the ASDM, go to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks**. Select **HQ-bookmark** and click **Edit**.

B) Select bookmark **HQ-Srv** and click **Delete** button to delete existing bookmark.

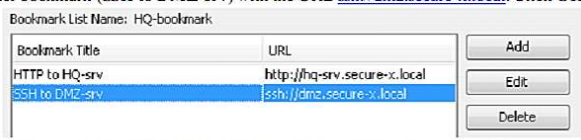
C) Click **Add** to define new bookmarks.

D) Select **URL with GET or POST method** as the bookmark type. Click **OK**.



E) Create a bookmark (**HTTP to HQ-srv**) with the URL http://hq-srv.secure-x.local. Click **OK**.

F) Add another bookmark (**SSH to DMZ-srv**) with the URL ssh://dmz.secure-x.local. Click **OK**.



G) Click the **OK** button in the **Edit Bookmark List** window and apply the configuration.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

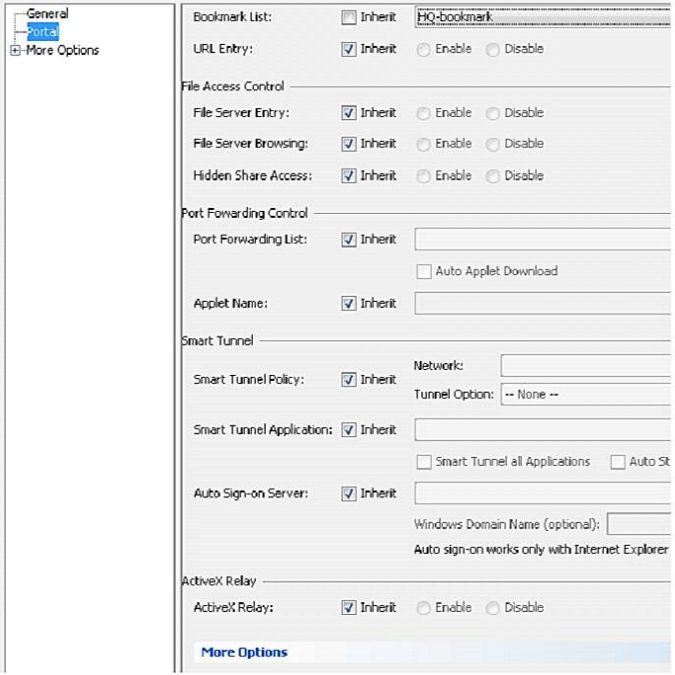
Configure a group policy to include the new bookmarks on the portal page when members of the group establish clientless SSL VPN connections to the ASA.

A) In the ASDM, go to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies**

B) Click **Add > Internal Group Policy** and create an internal group policy named **ccnp-group-policy**.

Note	This group policy will be used in this exercise instead of the default group policy. Alternatively you may tune the default group policy to achieve the same result.

C) Select the **Portal** page. Uncheck the **Inherit** checkbox near the bookmark list, and select **HQ-bookmark** from the drop-down list. Have all other attributes inherited from the default group policy.



D) Click **OK** and apply the configuration.

https://t.me/learningnets

Step 4

Configure a connection profile that points to your new group policy (ccnp-group-policy). In this step, you will also configure aliases for the custom connection profile and the default connection profile. This will enable users to select a connection profile at logon.

A) In the ASDM, go to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.

Note	This connection profile will be used in this exercise in addition to the default connection profile. Alternatively you may tune the default connection profile for similar results.

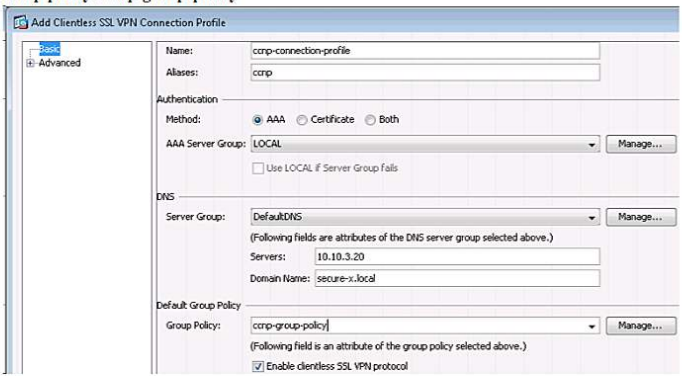
B) Click **Add** and create a connection profile (**ccnp-connection-profile**) with these attributes:

Alias: ccnp

Authentication method: AAA > LOCAL

DNS server group: Default-DNS (10.10.3.20)

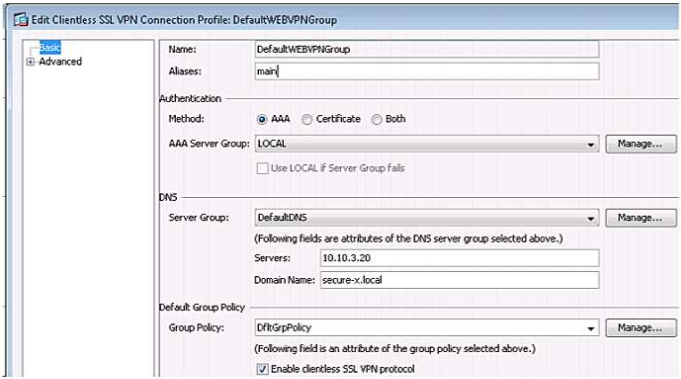
Group policy: ccnp-group-policy



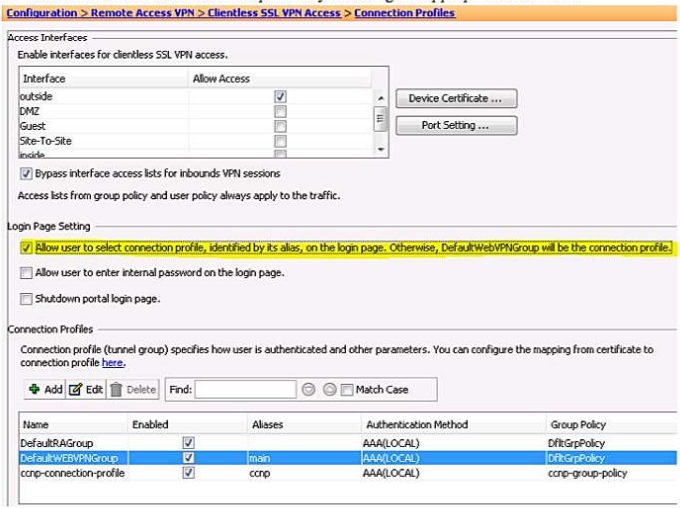
C) Click **OK**.

D) Select **DefaultWEBVPNGroup** to edit the default connection profile. Configure an alias (*main*) for the default connection profile (DefaultWEBVPNGroup) and click *OK*.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



E) Allow the users to select the connection profile by checking the appropriate checkbox.



F) **Apply** the configuration.

Activity Verification

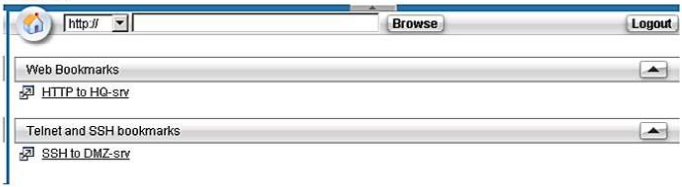
Step 1

On the Guest-PC, refresh the VPN portal page (**https://vpn.secure-x.public**) or re-connect to it. You should see two connection profiles.



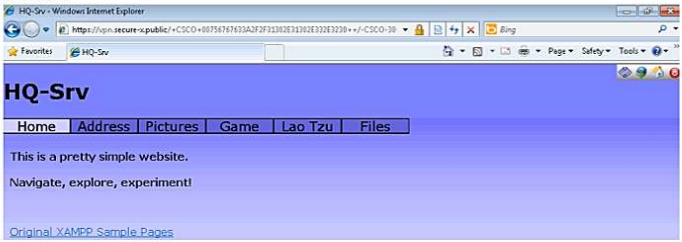
Step 2

Log in to the **ccnp** connection profile as a local user **admin** with password **Ci5coAdmin**. You should see the bookmarks.



Step 3

Click the **HTTP to HQ-srv** bookmark. You should be directed to the HQ-srv web page. If you click the **Address** tab in the HQ-Srv portal you will see the second leg of the session originates from the ASA's inside address.



Step 4

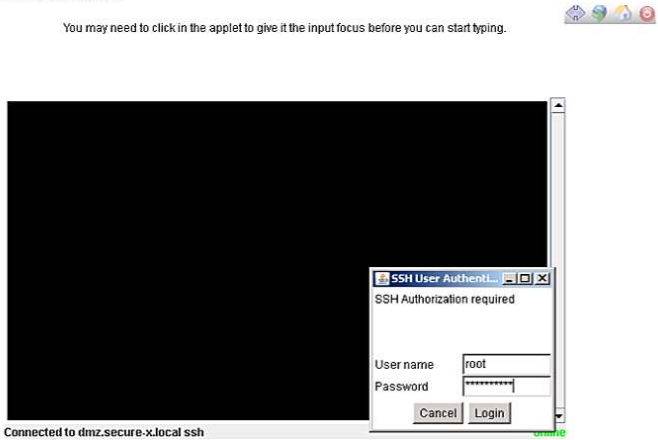
Click the **Home** icon on the floating toolbar or click the **"Go back"** icon two times.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

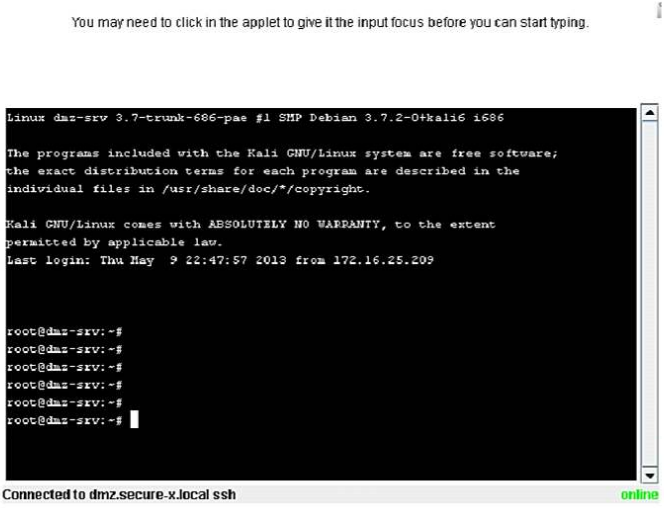
Step 5

Click the **SSH to DMZ-srv** bookmark. Depending on your browser and your certificate store configuration, you may get a warning or the plugin may not start. **Do not update Java** if prompted.

A) If you get a warning, accept it and run the application. Do not update Java. Log in as **root** with password **Ci5coAdmin**.



B) If the application does not start, try another browser (e.g. Firefox). If the application still doesn't work, lower your Java security level by going to **Start > Control Panel > Java > Security** and set the security level to **Medium**.



C) Log out from the portal.

Task 2: Configure Application Access Using Smart Tunnels

In this task you will configure application access using the SmartTunnel feature.

Activity Procedure

Complete the following steps:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 1

Configure the Smart Tunnel application list:

A) In the ASDM, go to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**.

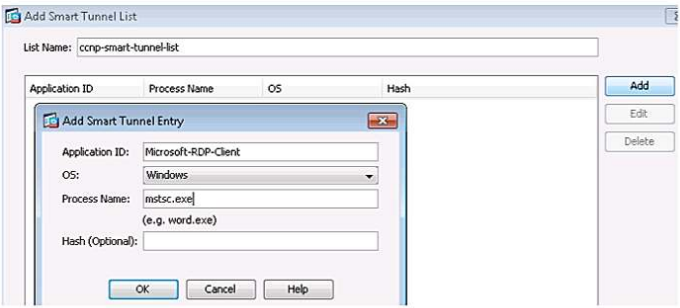
B) In the **Smart Tunnel Application List** section, click **Add** to create a list (**ccnp-smart-tunnel-list**).

C) Click **Add** to create a **Smart Tunnel** entry with these attributes:

Application ID: Microsoft-RDP-Client

OS: Windows

Process name: mstsc.exe



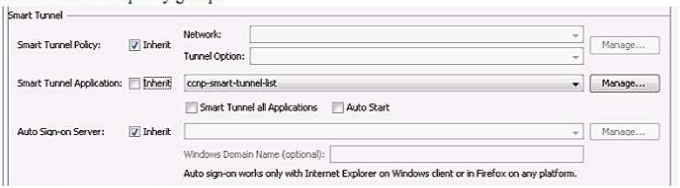
D) Click **OK** button and **Apply** button to apply the configuration.

Step 2

Apply the smart tunnel list to the group policy:

A) In the ASDM, go to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies**.

B) Edit the custom group policy (**ccnp-group-policy**). In the **Portal** page, apply the smart tunnel application list to the policy group.



C) Click **OK** button and **Apply** button to apply the configuration.

https://t.me/learningnets

Activity Verification

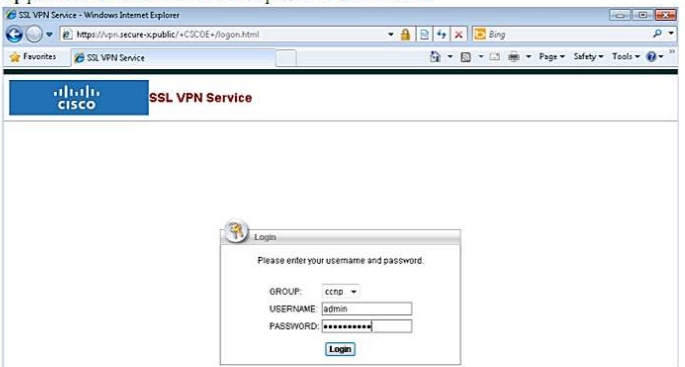
Step 1

On the Guest-PC, start the MS Terminal Services client by invoking **mstsc** from the Start menu. Verify that a connection to the HQ-srv IP address (10.10.3.20) fails. The Guest-PC is in the SP subnet, which does not have direct connectivity to the internal networks on the inside of the ASA.



Step 2

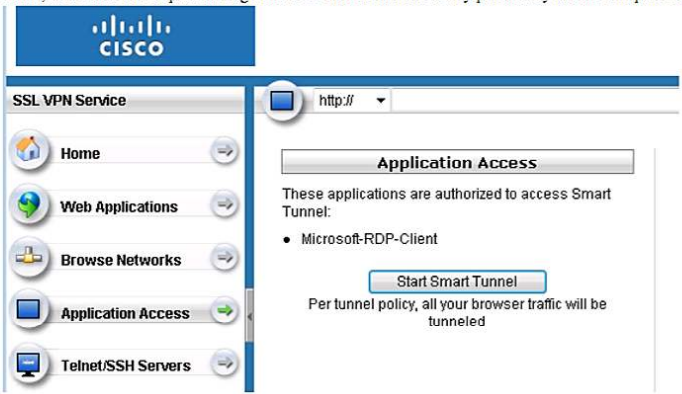
From the Internet Explorer on the Guest-PC, reconnect to the VPN portal (https://vpn.secure-x.public) using the **ccnp** profile with username **admin** and password **Ci5coAdmin**.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

Navigate to **Application Access** and click the **Start Smart Tunnel** button. Accept the prompts to run the application, allow the data to pass through the VPN and do not block any potentially unsafe components.



Step 4

Using the MS Terminal Services client, connect to the HQ-srv using its internal IP address (10.10.3.20). Accept all warnings. Log in as **administrator** with password **Ci5coAdmin**.

Step 5

Log out from the portal by clicking the **appropriate icon** in the right top corner. Notice that the RDP session has been interrupted.

https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 4-3: Implement Local and External AAA for Clientless SSL VPNs

Activity Objective

In this lab activity you will enhance the clientless SSL VPNs by local authorization and RADIUS-based authentication and authorization. You will configure a web ACL on the ASA, apply it to a local group policy and test the authorization results. You will then configure the ASA as a RADIUS client of the Cisco ISE. You will configure a connection profile for RADIUS-based authentication. You will test the external authentication and authorization.

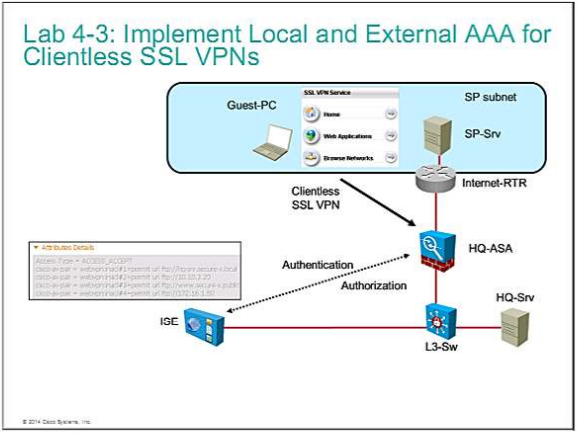
Upon completing this activity, you will be able to meet these objectives:

- Implement local authorization of clientless SSL VPNs
- Deploy RADIUS-based authentication and authorization of clientless SSL VPNs

https://t.me/learningnets

Visual Objective: Local Authorization and External AAA for Clientless SSL VPNs

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

- Cisco ASA
- Client computer

Job Aids

These job aids are available to help you complete the lab activity.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

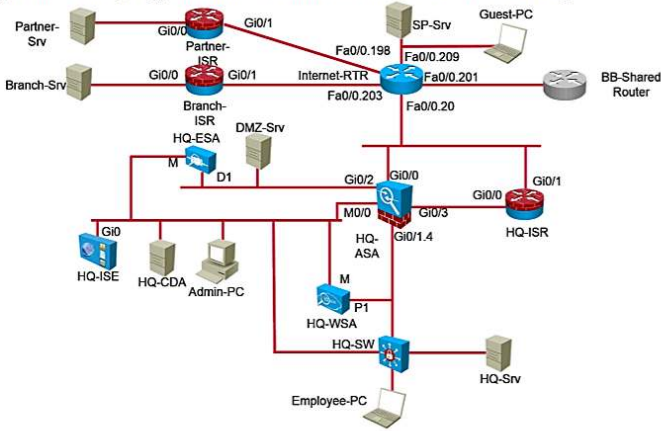
https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

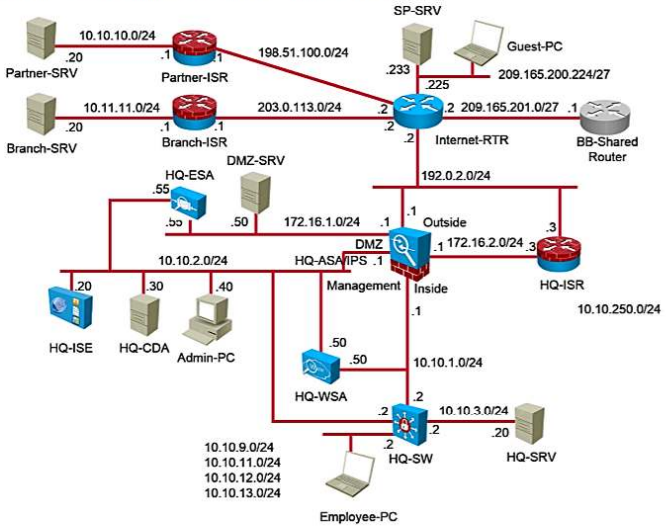
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



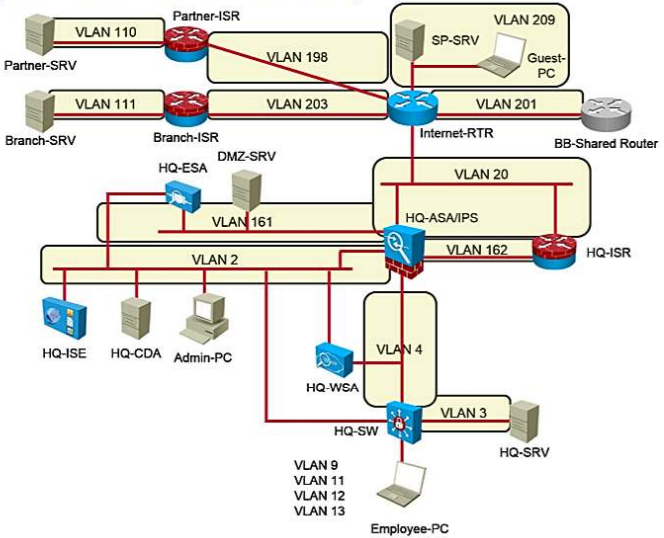
The figure shows the IP addresses that are used in this lab setup.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Configure Local Authorization

In this task you will enhance the client SSL VPN scenario with local authorization on the ASA. The local authorization is based on Web ACLs that are defined on the VPN head-end itself. You will configure a Web ACL that permits FTP to the HQ-Srv and denies other traffic. You will apply this Web ACL to your custom group policy.

Activity Procedure

Complete the following steps:

Step 1

From the Guest-PC, connect via HTTPS to the portal page (**vpn.secure-x.public**) as **admin** with password **Ci5coAdmin**. Verify that you can browse various URLs, such as the ones below. When browsing, use the URL entry field in the portal, not the main URL entry field in the browser.

A) HTTP and FTP to www.secure-x.public

B) HTTP and FTP to hq-srv.secure-x.local

C) http://cisco.com

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 2

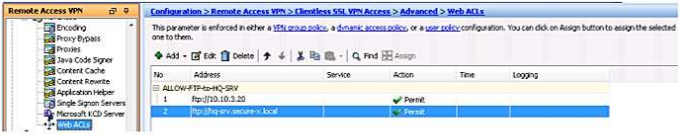
In the ASDM, configure a Web ACL that allows only FTP to the HQ-srv:

A) Go to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs**.

B) Choose **Add > Add ACL** to create a Web ACL (**ALLOW-FTP-TO-HQ-SRV**)

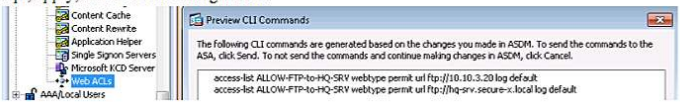
C) Click **Add > Add ACE** to configure an ACL statement that permits FTP to the HQ-srv address (**10.10.3.20**). The first entry will permit traffic based on address and service.

D) Add another ACE that permits FTP to the HQ-srv hostname (**hq-srv.secure-x.local**). This entry will permit traffic based on the URL.



Note If you configured only an address-based or a named-based ACE, you would be able to connect to the resource only by the respective notation.

E) Accept, apply, and send the configuration.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

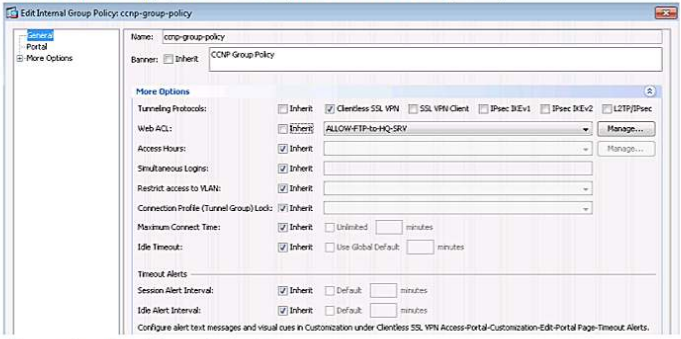
Step 3

Apply the Web ACL to the previously defined custom group policy (**ccnp-group-policy**):

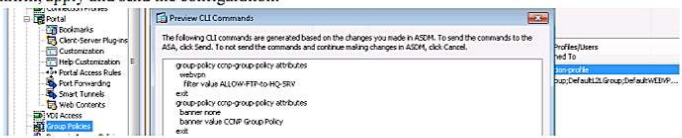
A) In the ASDM, go to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies**.

B) Edit the custom group policy (**ccnp-group-policy**). In the **General** page, set the banner to **CCNP Group Policy** for easier group identification.

C) Click **More Options**. Apply the Web ACL (**ALLOW-FTP-TO-HQ-SRV**).



D) Confirm, apply and send the configuration.



Activity Verification

Step 1

On the Guest-PC, log out and log in to the portal page (**vpn.secure-x.public**) using the ccnp profile. Click **Continue** when you see the banner about the ccnp group policy.

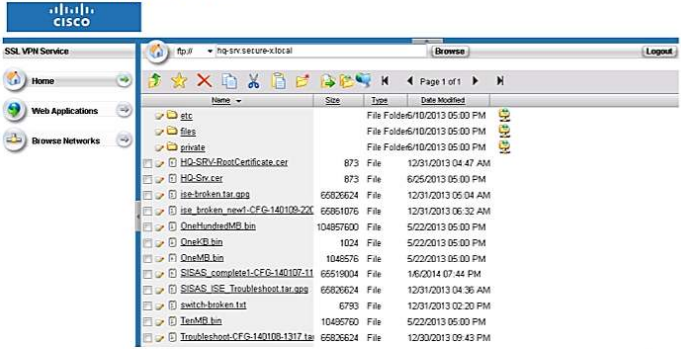
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 2

Verify the Web ACL filtering:

A) The bookmarks are inactive.

B) FTP connections to the HQ-Srv succeed, both using the DNS name and IP address. Make sure that you enter the URLs in the portal browser:



C) Connections to denied sites, such as http://dmz.secure-x.local, https://bankofamerica.com, http://cisco.com or http://hq-srv.secure-x.local fail. The access to these resources should have been denied.



Step 3

Log out from the portal by clicking the appropriate icon in the right top corner.

Note Local authorization does not scale well in large environments with multiple VPN gateways, because you must replicate the Web ACL configuration on each gateway. In the next tasks you will configure external authorization that offers more scalable access control.

Task 2: Enable RADIUS-Based Authentication and Authorization

In this task you will configure RADIUS-based authentication and authorization of the clientless SSL VPN. The Cisco ISE has been pre-configured for this scenario. The ISE has two local user accounts: ise1 and ise2. Both users have password **cisco**. The user ise1 does not have any authorization settings. The ise2 user is assigned an authorization profile that uses a Web ACL to permit FTP traffic. You will configure the ASA as an AAA client of the Cisco ISE and define a connection profile that uses the RADIUS server for authentication.

Note	Although the Cisco ISE is not covered in this course, you may connect to the ISE GUI to examine its pre-configured settings. From the Admin-PC, connect via HTTPS to ise.secure-x.local, and log in as **admin** with password **Ci5coAdmin**.

Activity Procedure

Complete the following steps:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 1

In the ASDM, configure the ASA to act as an AAA client of the Cisco ISE:

A) Go to **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups**.

B) Click **Add** in the AAA Server Groups area and create a AAA group **(ISE)** of type RADIUS.

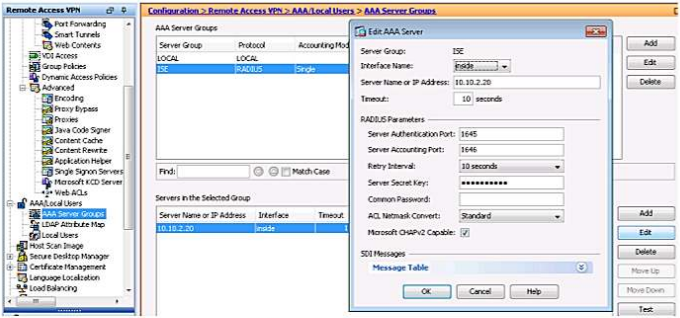
C) Click **OK**.

D) With the new AAA server group highlighted, click **Add** in the Servers in the Selected Group area to add a AAA server.

E) Add the ISE (**10.10.2.20**) as a member of the RADIUS group.

F) Use the inside interface to connect to ISE.

G) Set the server secret key to **radius-key**.



H) Click **OK**. Then apply and send the configuration.



I) Click the **Test** button and test the authentication using the preconfigured ISE user **ise1** with password **cisco**. The authentication should be successful.



Step 2

In the ASDM, configure a connection profile, named **ise**, for external authentication and authorization:

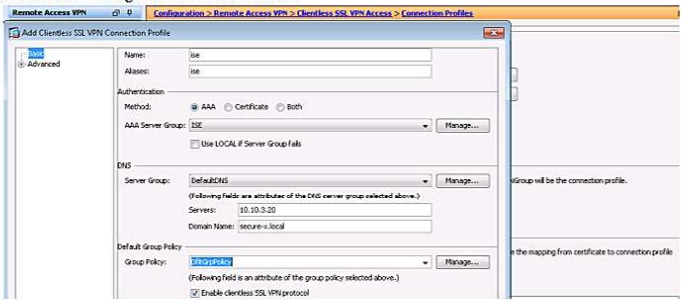
A) Go to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**

B) Name and alias: **ise**

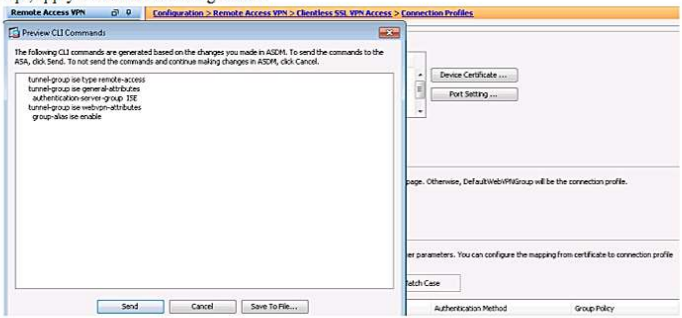
C) AAA server group (in AAA method): **ISE**

D) Group policy: **DfltGrpPolicy**

E) Leave all other settings at their default values.



F) Accept, apply and send the configuration.



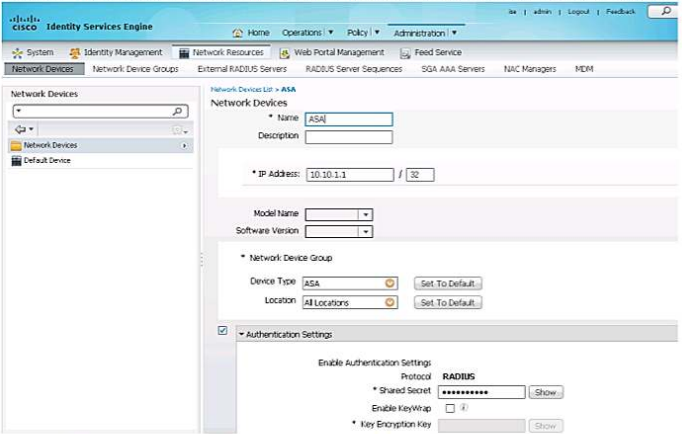
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

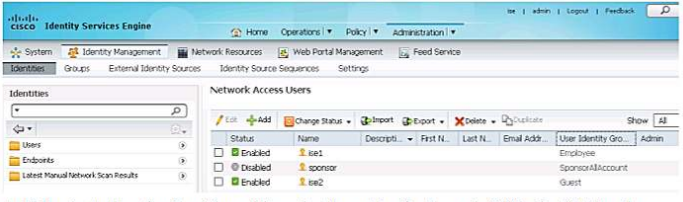
Explore the Cisco ISE settings. The ISE has been preconfigured for VPN authentication and authorization:

A) From the Admin-PC, open the Internet Explorer and connect to https://ise.secure-x.local. Log in as **admin** with password **Ci5coAdmin**.

B) Go to **Administration > Network Resources > Network Devices**. Examine the configuration of the ASA device. The network devices are defined in the ISE to allow RADIUS communication with them.

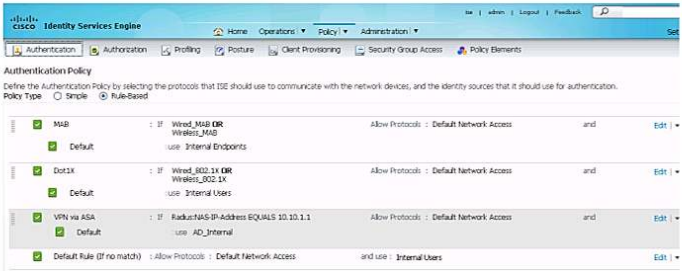


C) Go to **Administration > Identity Management > Identities > Users**. Two user accounts have been configured on the ISE: ise1 and ise2. The first belongs to the Employee group and will not be subject to ACL authorization. The second belongs to the Guest group and will be authorized using ACLs.

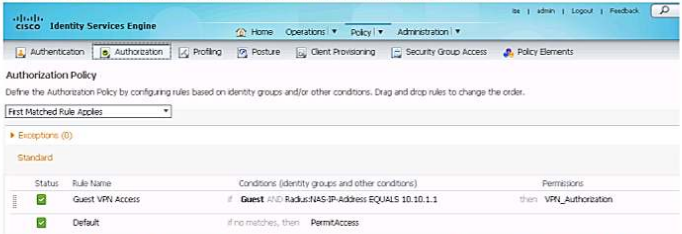


D) Go to **Policy > Authentication**. You will see that the authentication rule 'VPN via ASA' has been defined in addition to the default rules MAB, Dot1X, and Default. This rule checks all authentication requests received from the ASA (10.10.1.1) against the Active Directory, and if user is not found there, against the internal ISE database.

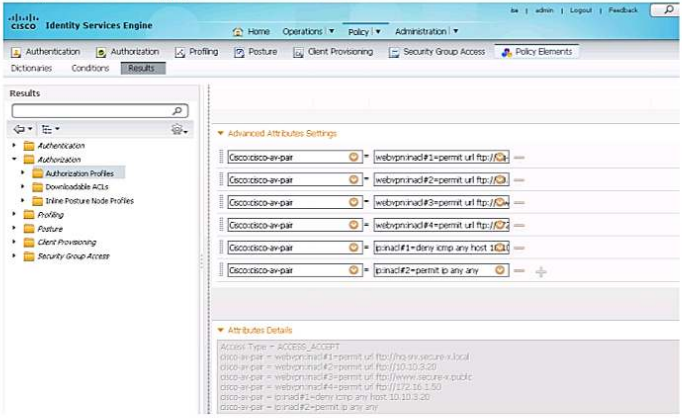
https://t.me/learningnets



E) Go to **Policy > Authorization**. The authorization rule 'Guest VPN Access' has been defined to apply the authorization profile 'VPN_Authorization' to guests accessing the VPN.



F) Go to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**. Click the authorization profile **VPN_Authorization**. Scroll down to the advanced attribute section. The first four entries (webvpn:inacl) are used to apply WebVPN ACLs to clientless sessions. The last two entries (ip:inacl) will be used to apply ACLs to client sessions.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Task 3: Test External Authentication and Authorization

In this task you will verify that ise1 can connect to the VPN portal and then access all resources, and that the user ise2 can only access the authorized FTP sites.

Activity Procedure

Complete the following steps:

Step 1

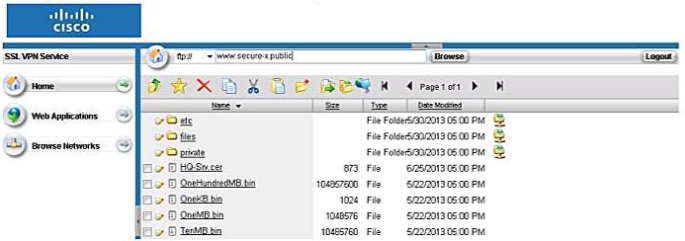
From the Guest-PC, reconnect via HTTPS to **vpn.secure-x.public**. Select the **ise** connection profile (group). Log in to the SSL VPN portal as **ise1** with password **cisco**. You should be able to access the portal.

Step 2

Test the connectivity through the portal. User **ise1** should connect to all sites:

A) HTTP to hq-srv.secure-x.local, www.secure-x.public, and cisco.com

B) FTP to hq-srv.secure-x.local and www.secure-x.public



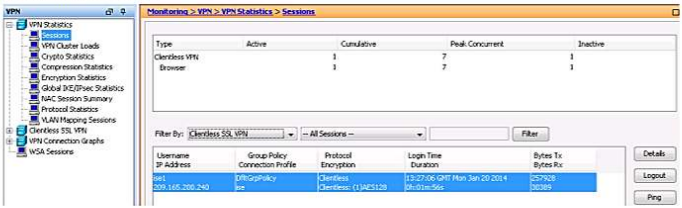
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

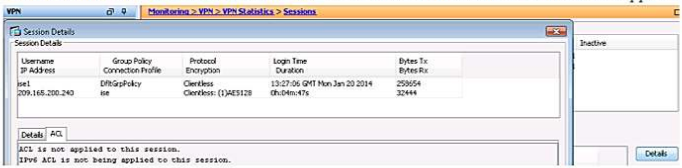
Verify the ise1 permissions through the ASDM monitoring:

A) In the ASDM, go to **Monitoring > VPN > VPN Statistics > Sessions**.

B) Choose **Clientless SSL VPN** from the **Filter By** menu. You should see that the DfltGrpPolicy has been applied to the ise1 session.



C) Click the **Details** button and select the **ACL** tab. You will see that no Web ACLs have been applied.

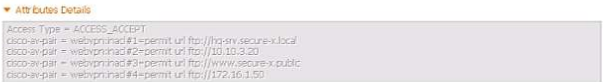


Step 4

Log out and then reconnect to the VPN portal. Select the **ise** connection profile (group). Log in to the SSL VPN portal as **ise2** with password **cisco**.

Step 5

Optionally connect to the ISE GUI (https://ise.secure-x.local) as **admin/Ci5coAdmin** and examine the authorization profile (VPN_Authorization) applied to the ise2 user in the **Policy> Policy Elements > Results > Authorization > Authorization Profiles** menu. Scroll down to the Advanced Attribute Settings and Attribute Details sections. The Cisco:cisco-av-pair webvpn:inacl attributes are used to permit FTP connections to the HQ-Srv and DMZ-srv by name and IP address. Other attributes have been configured for AnyConnect SSL VPN authorization.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 6

Test the connectivity through the portal. User **ise2** should connect only to the authorized FTP sites:

A) All HTTP browsing should be denied (hq-srv.secure-x.local, www.secure-x.public, or cisco.com)

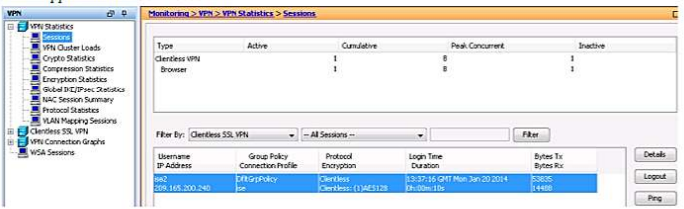
B) FTP connections to HQ-Srv and DMZ-Srv, both by IP address and DNS name, should be permitted (hq-srv.secure-x.local/10.10.3.20 and www.secure-x.public/172.16.1.50)

Step 7

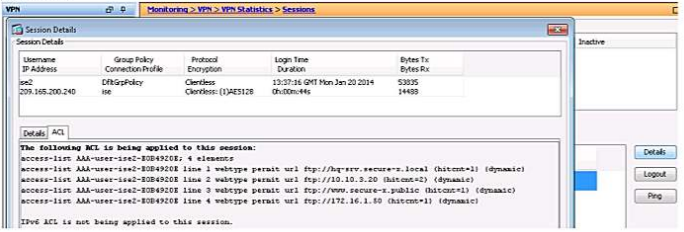
Verify the ise2 permissions through the ASDM monitoring:

A) In the ASDM, go to **Monitoring > VPN > VPN Statistics > Sessions**.

B) Choose **Clientless SSL VPN** from the **Filter By** menu. You should see that the same DfltGrpPolicy has been applied to the ise2 session.



C) Click the **Details** button and select the **ACL** tab. You will see the Web ACL that has been received from the ISE.



https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 5-1: Implement ASA Basic AnyConnect SSL VPN

Activity Objective

In this lab activity you will deploy basic AnyConnect SSL VPNs on the Cisco Adaptive Security Appliance. In the first task you will prepare the Employee-PC for a later certificate-based user authentication. You will join the Employee-PC to the Active Directory, install a user certificate in its certificate store, and then move the Employee-PC to an external location, from which the users will initiate VPN connections. You will enable AnyConnect SSL VPN connections, configure a local VPN user, create an IP address pool, configure NAT exemption, and split tunneling. When all components, including a connection profile and group policy, have been configured, you will test the VPN connectivity and access to internal resources.

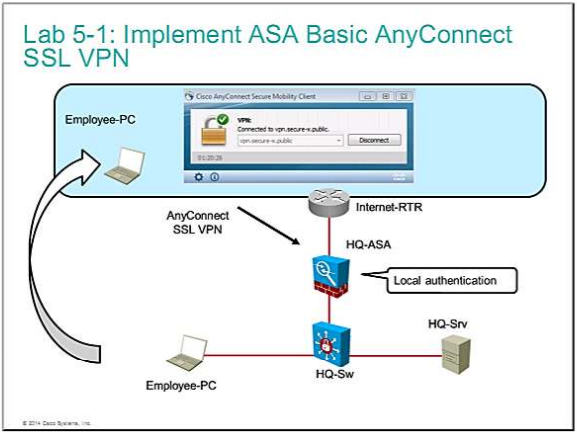
Upon completing this activity, you will be able to meet these objectives:

- Install user certificate on the client machine.
- Enable AnyConnect SSL VPN connections.
- Define a VPN user.
- Configure an IP address pool.
- Define identity NAT.
- Configure split tunneling, connection profile, and group policy.

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

- Cisco ASA adaptive security appliance

Command List

No commands are needed to complete this lab exercise. All tasks are performed with the Cisco Adaptive Security Device Manager (Cisco ASDM) GUI interface.

Job Aids

These job aids are available to help you complete the lab activity.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

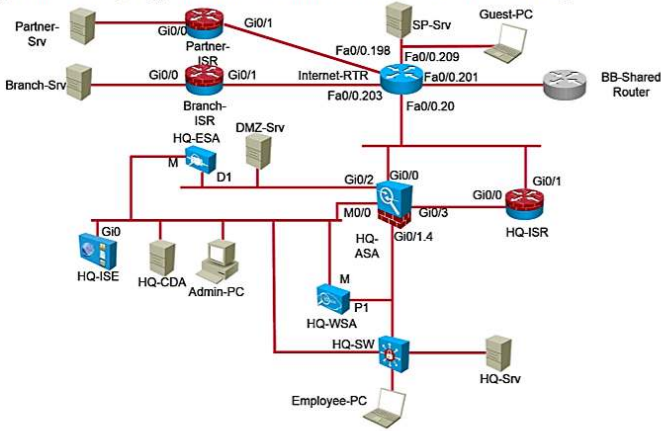
https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

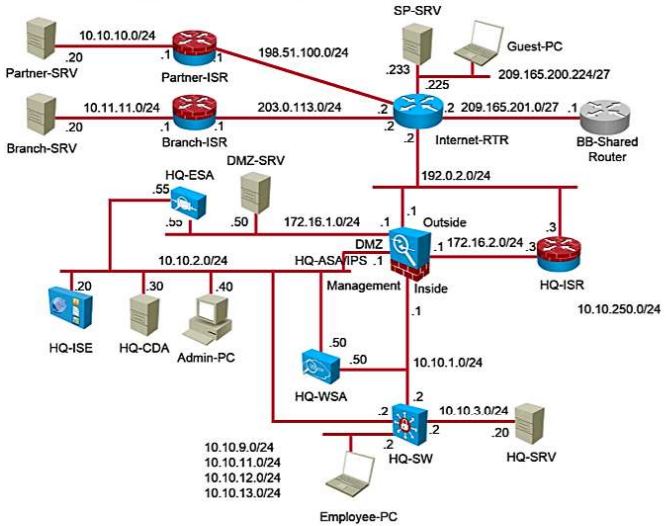
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.

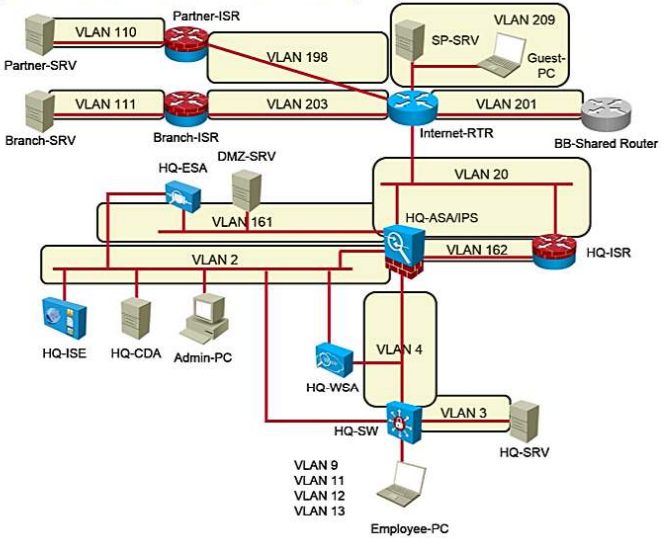


The figure shows the IP addresses that are used in this lab setup.



VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Install Client Certificate on Employee-PC and Move Employee-PC to SP Subnet

You will use certificate-based client authentication in the next exercise. To install the client certificates, the Employee-PC must be located inside the enterprise, in its initial location. In this preparatory task, you will join the Employee-PC to the domain, install the user certificate, and then move the Employee-PC to the SP subnet, from which it will initiate VPN connections.

Activity Procedure

Complete the following steps:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 1

Join the Employee-PC to the Active Directory:

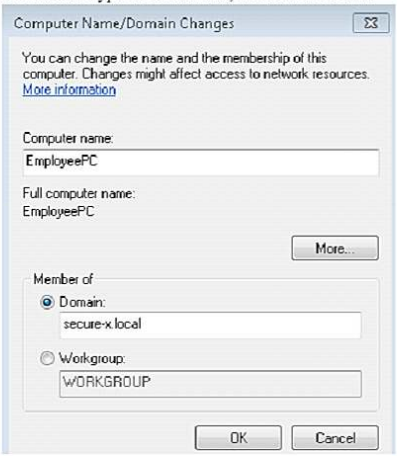
A) Access the **Employee-PC**. The local administrator credentials are student/Ci5coAdmin.

B) Click **Start**, right-click **Employee-PC**, and then click **Properties**.

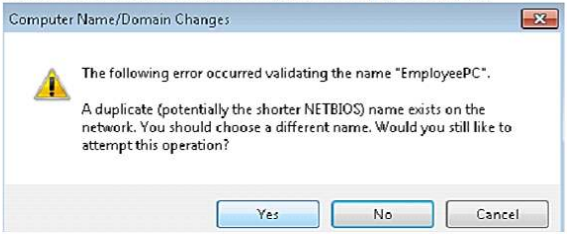
C) In the right hand pane, under **Computer Name, Domain, and Workgroup Settings**, find and click **Change Settings**.

D) Select the **Computer Name** tab and then click **Change**.

E) Under **Member of**, select **Domain**. Type **secure-x.local**, and then click **OK**.



F) You may be warned about the name conflict. Accept the warning by clicking **Yes**.



G) Authenticate as **Administrator** with the password **Ci5coAdmin** to join the domain.

H) Click **OK** on the welcome notification.

I) Once you are successfully joined to the domain, you will be prompted to restart your computer. Accept the notification and **Restart Now**.

https://t.me/learningnets

Step 2

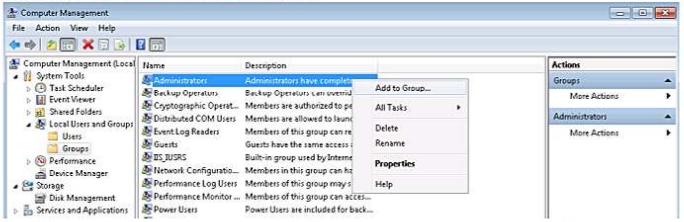
Assign administrative privileges to domain users. The domain user **it1** will need them to install the AnyConnect client software.

A) Wait until the computer restarts and log in as the domain administrator with password **Ci5coAdmin**. Enter the username **secure-x\administrator** to instruct the Employee-PC to use the domain and not the local administrator account. You will be able to log in as the domain administrator because the Employee-PC has joined the domain.

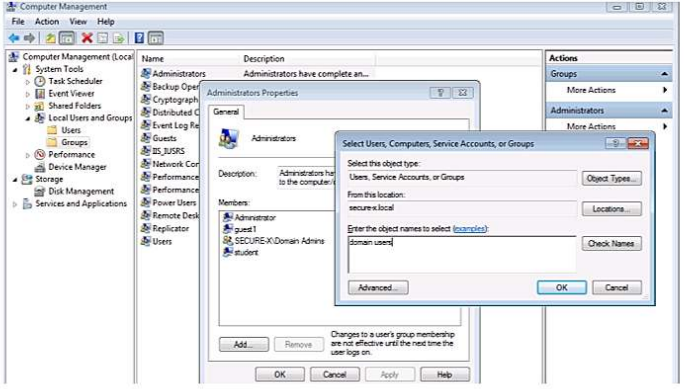
B) Go to **Start.** Right-click the **Computer** and select **Manage.**



C) Go to **Computer Management (Local) > Local Users and Groups > Groups**. Right-click the **Administrators** group and select **Add to group**.



D) Click **Add**, enter the **domain users** group. Upper/lower case notation does not matter in Windows. Click **OK**.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

Use the Certificate Manager console to install the user certificate for the user **it1**. The user certificate will be used in the next exercise, for certificate-based client authentication.

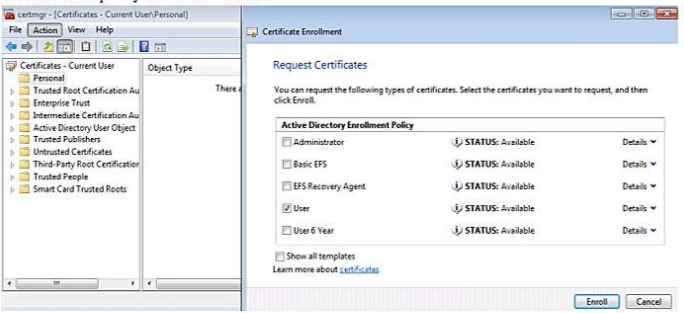
A) On the **Employee-PC**, log off the domain administrator and log in as the domain user **it1** with password **cisco**.

B) Click **Start**, and enter **certmgr.msc** into the **Search programs and files** field, then press **<Enter>**.

C) In the **certmgr**, choose **Certificates - Current User > Personal** and observe that the user has no certificate in the user certificate store.

D) Choose **Action > All Tasks > Request New Certificate**. Follow the wizard (**Next > Next**).

E) Choose the **User** policy and click **Enroll**.



F) Click **Finish**. Optionally you can double click on the certificate received for the it1 user, and examine the results. Close all open windows on the Employee-PC.

Step 4

Having obtained user certificate inside the enterprise, move the Employee-PC to the SP subnet. The employee user **it1** will at this point move to an external location and need the VPN to access internal resources.

A) Connect to the HQ-SW switch and place the Employee-PC interface in service provider VLAN (209):

```
interface GigabitEthernet0/1
 description Employee-PC
 switchport access vlan 209
```

B) Refresh the IP address on the Employee-PC, for example using **ipconfig /release** and **ipconfig /renew** commands in the command prompt. Make sure that the Employee-PC obtains an IP address from the SP subnet (209.165.200.224/27).

C) On the Employee-PC, open the Internet Explorer and connect via HTTPS to vpn.secure-x.public. You should see the VPN portal login page. Do not log in yet.

https://t.me/learningnets

Task 2: Enable AnyConnect SSL VPN Connections and Create a Local VPN User

In this task, you will enable AnyConnect SSL VPN connections and create a local VPN user.

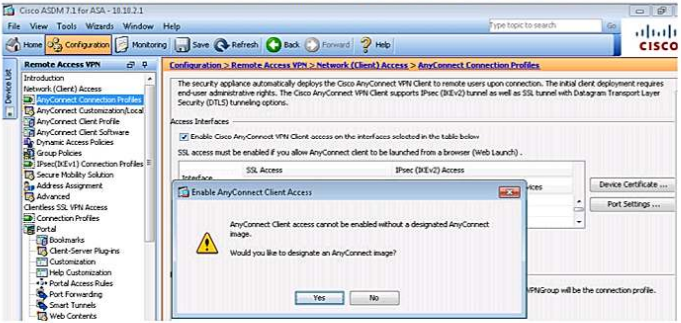
Activity Procedure

Complete the following steps:

Step 1

Use Cisco ASDM from Admin-PC to access HQ-ASA at IP address 10.10.2.1.

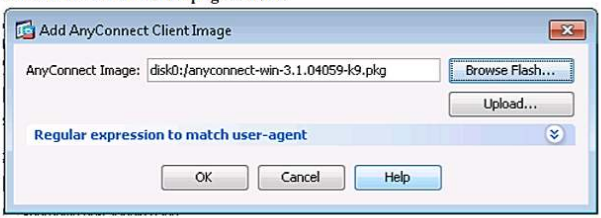
Navigate to the **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles** and enable Cisco AnyConnect VPN Client access on the outside interface.



The ASDM will ask you to designate an AnyConnect image, select **Yes** option and proceed to the next step.

Step 2

In the **Add AnyConnect Client Image** window, click **Browser Flash** and select the AnyConnect client image **anyconnect-win-3.1.04059-k9.pkg** on disk0.

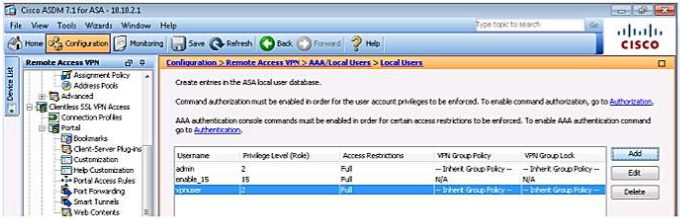


Click **OK** button and apply changes.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

In the **Configuration > Remote Access VPN > AAA/Local Users > Local Users** add a new user **vpnuser** with password **cisco**.



Apply changes to the HQ-ASA.

Task 3: Configure VPN IP Address Pool and Identity NAT

In this task, you will configure an IP address pool for the VPN clients and configure identity NAT to keep the IP addresses unchanged during communication through the VPN tunnel.

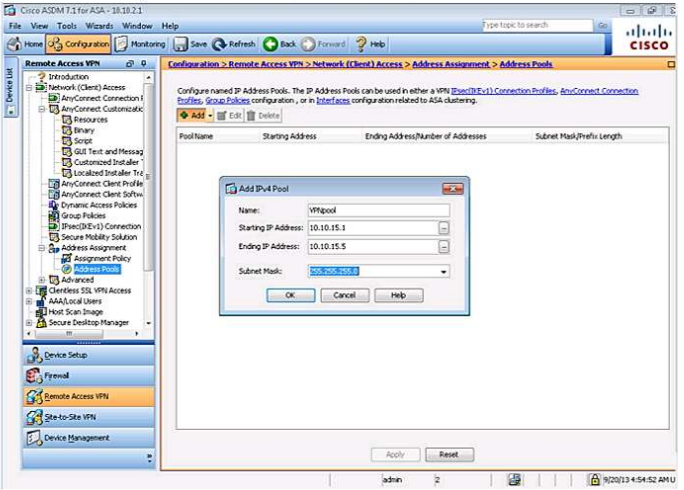
Activity Procedure

Complete the following steps:

https://t.me/learningnets

Step 1

In the ASDM, go to **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools.** Add a new address pool named **VPNpool** starting with IP **10.10.15.1** and ending with IP **10.10.15.5**, select the subnet mask **255.255.255.0**.



https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 2

Configure identity NAT for VPN clients:

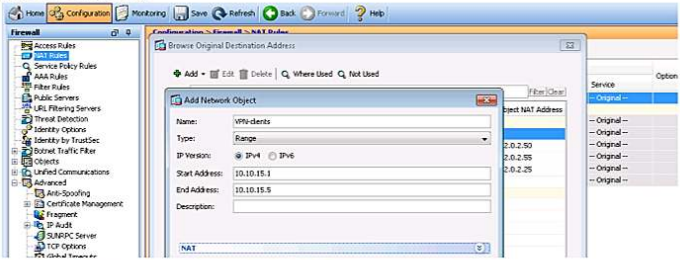
A) Go to **Configuration > Firewall > NAT Rules**.

B) Click **Add** to create a rule before "Network Object" NAT rules.



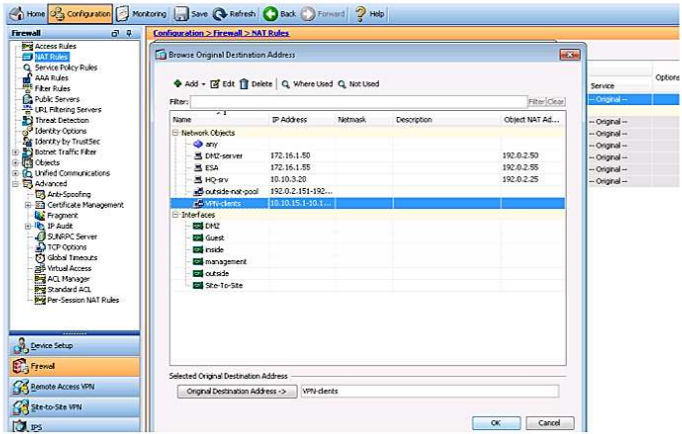
C) Choose outside as the destination interface, and click the destination address selection button. Click **Add** and create a network object.

D) Configure a network object **(VPN-clients)** that defines the VPN client address range (10.10.15.1-10.10.15.5).

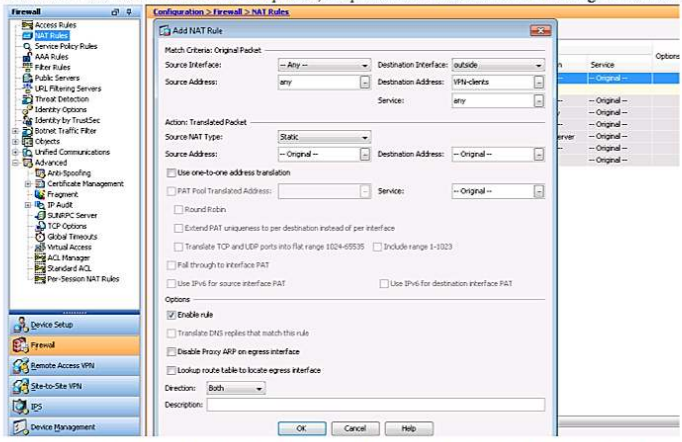


E) Click **OK**. Select the network object **(VPN-clients)** as the destination address.

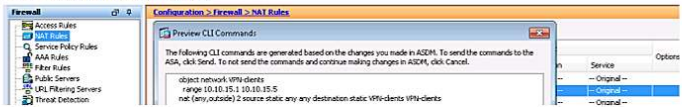
https://t.me/learningnets



F) Click **OK**. In the NAT rule configuration, verify that the network object (**VPN-clients**) is defined as the destination address. For the translated packet, keep the static translation with the original addresses.



G) Click **OK**. Accept the pop-up window about identity NAT and proxy ARP. Apply the configuration. Preview and send the commands.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Task 4: Configure Connection Profile

In this task, you will configure the connection profile for AnyConnect SSL VPNs. The connection profiles define pre-login operation. You will configure IP assignment and DNS settings for the custom connection profile (ccnp-connection-profile).

Activity Procedure

Complete the following steps:

Step 1

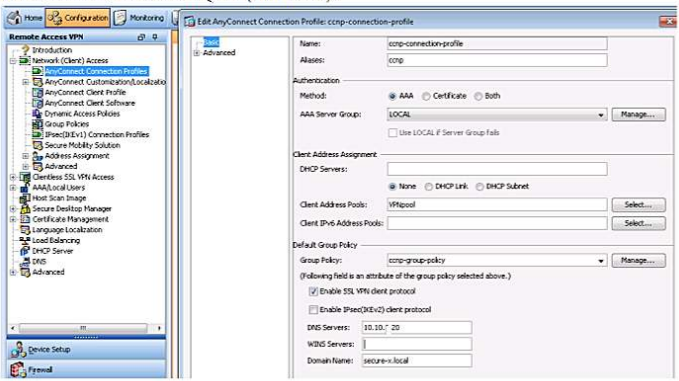
Configure the connection profile (**ccnp-connection-profile**) for DNS and IP address assignment:

A) Edit the connection profile (**ccnp-connection-profile**) from the **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles** menu. Using a custom connection profile is one of possible approaches. You could also implement the AnyConnect VPN using the default profile.

B) Configure IP address assignment based on address pool (**VPNpool**).

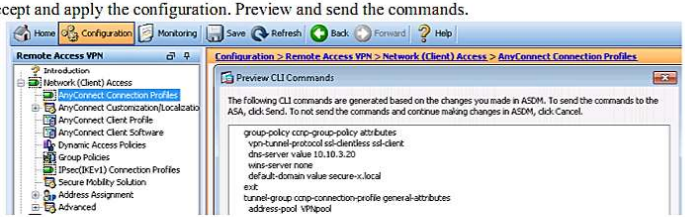
C) Enable SSL VPN client protocol. It is a setting of the group policy attached to the connection profile. You can, however, enable it in the connection profile configuration.

D) Set the DNS server address to HQ-srv (**10.10.3.20**).



E) Leave all other settings at the previously configured values.

F) Accept and apply the configuration. Preview and send the commands.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Task 5: Configure Group Policy: IP Pool, DNS and Split Tunneling

In this task, you will configure the IP pool assignment, DNS and split tunneling at the default group policy level. Split tunneling defines which traffic will be routed trough the tunnel towards the VPN head-end. In this scenario the VPN client should be able to reach internal resources through the VPN tunnel and still retain connectivity to external destinations. You will configure the DNS and split tunneling information in the default group policy. These settings will be by default automatically inherited by any custom group policies.

Activity Procedure

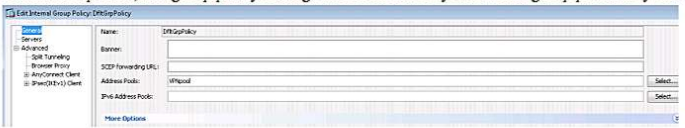
Complete the following steps:

Step 1

In the **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** edit the the default group policy (DfltGrpPolicy). Configuring global settings in the default group policy and having them inherited by the custom group policies simplifies the manageability.

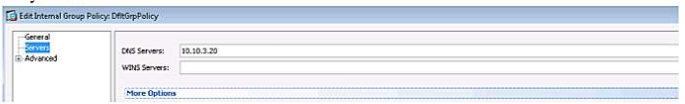
Step 2

In the General page, choose the **VPNpool** as the address pool. Although you previously set the address pool in the connection profile, this group policy setting will be inherited by all custom group policies by default.



Step 3

Select the Servers page and set the DNS server address to 10.10.3.20. Although you previously set the DNS server address in the connection profile, this group policy setting will be inherited by all custom group policies by default.



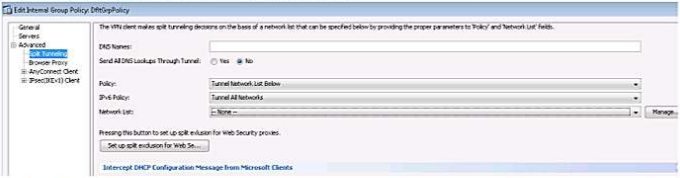
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 4

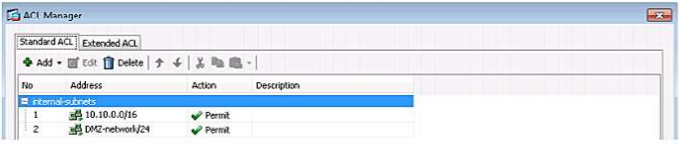
Configure split tunneling. Split tunneling defines which traffic will be routed trough the tunnel towards the VPN head-end. In this scenario you will specify the internal subnets reachable through the VPN tunnel. This will allow connectivity to external destinations.

A) Go to the **Advanced > Split Tunneling** page.

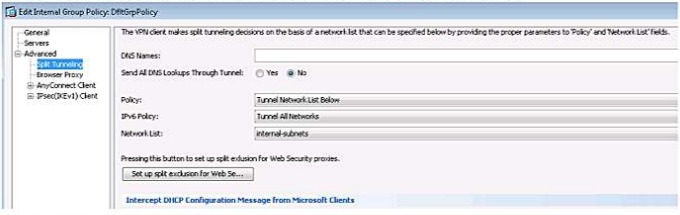
B) Set the Policy to **Tunnel Network List Below** option.



C) Click the Manage button near the Network List drop-down list. Create a standard ACL **(internal-subnets)** that permits the inside subnets **(10.10.0.0/16)** and the DMZ-network **(172.16.1.0/24)**.



D) Click **OK**. Make sure that traffic to the **internal-subnets** list will be tunneled.



E) Click **OK** and apply the configuration.

Step 5

Examine your custom group policy (ccnp-group-policy); verify that the DNS and split tunneling settings are by default configured to inherit the values from the default group policy.



Task 6: Test AnyConnect SSL VPNs

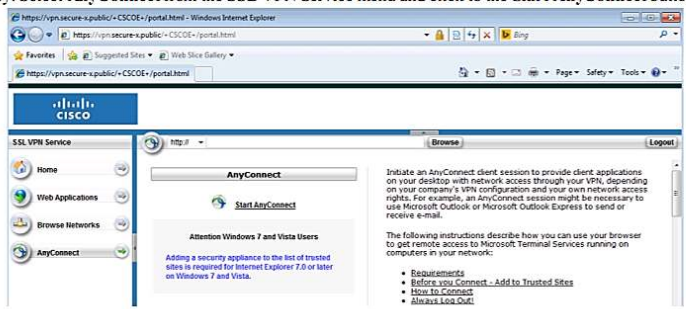
In this task, you will test the AnyConnect SSL VPN.

Activity Procedure

Complete the following steps:

Step 1

Connect to the VPN portal from the Internet Explorer on the Employee-PC (https://vpn.secure-x.public). Select **ccnp** group. Log in as **vpnuser** with password **cisco**. Accept the banner about the CCNP group policy. Select **AnyConnect** from the SSL VPN Service menu and click to the **Start AnyConnect** button.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

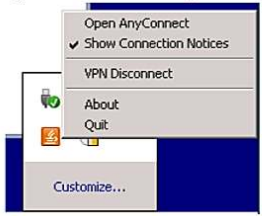
Step 2

Accept the Active-X pop-up to install the AnyConnect client. Perform the installation. The AnyConnect client will auto-install and establish the VPN connection to the ASA. You will see the AnyConnect icon in the system tray.



Step 3

Disconnect from the VPN by selecting the **VPN Disconnect** option at the AnyConnect icon.



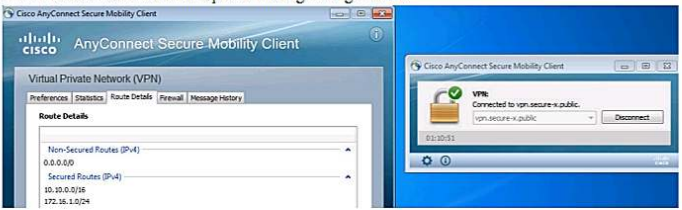
Connect back by selecting **ccnp** group (**vpnuser/cisco**) to test the connection using the AnyConnect GUI. Accept the banner about the CCNP group policy.



https://t.me/learningnets

Step 4

With the VPN connection established, click the AnyConnect icon in the system tray to open the AnyConnect GUI. Click the wheel icon in the left bottom corner of the AnyConnect GUI to open the AnyConnect Secure Mobility Client window. Choose the Route Details tab to examine the secured routes. The secured routes result from the split tunneling configuration.



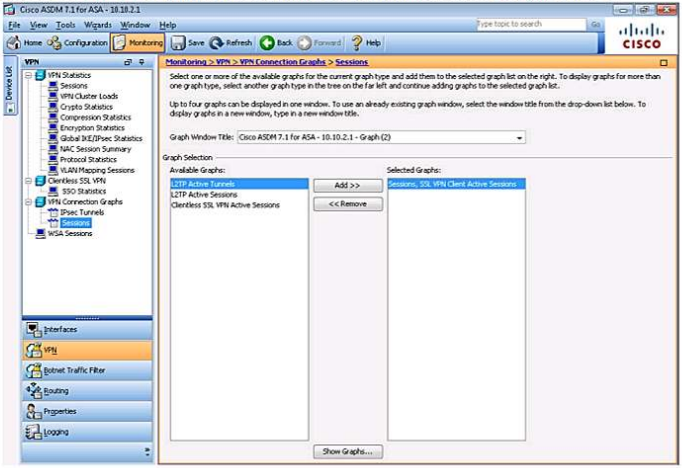
Step 5

On the Employee-PC, open a command prompt and examine the adapter configuration using the **ipconfig** command. You will see two local area connections: the physical adapter via **sp.public**, and the VPN virtual adapter via **secure-x.local**. You can also view the routing table using the **route print** command. The secured routes will point to the VPN head-end.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

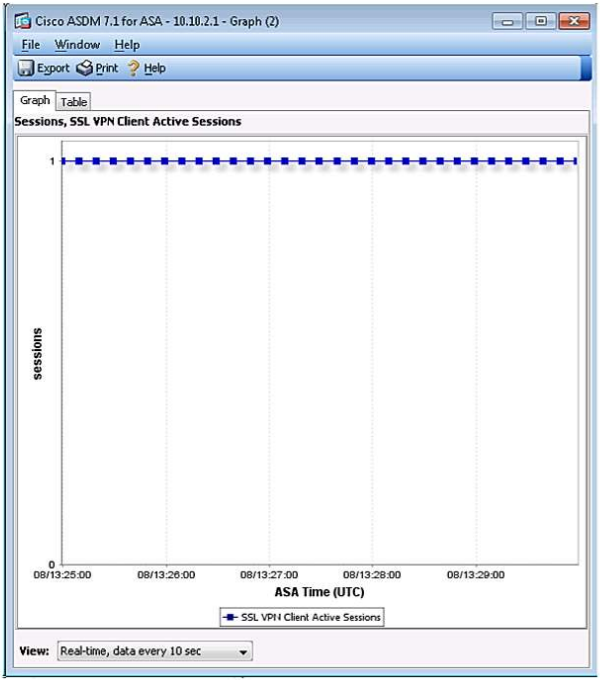
Step 6

In the ASDM on the Admin-PC navigate to the **Monitoring > VPN > VPN Connection Graphs > Sessions**. Select **SSL VPN Client Active Sessions** and add it to the Selected Graphs window.



Click **Show Graphs ...** button. You should see Sessions, SSL VPN Client Active Sessions graph showing one active session.

https://t.me/learningnets



Step 7

In a web browser on the Employee-PC, verify that you can access internal resources, such as http://hq-srv, http://hq-srv.secure-x.local, ftp://hq-srv.secure-x.local, http://dmz.secure-x.local, and ftp://dmz.secure-x.local.

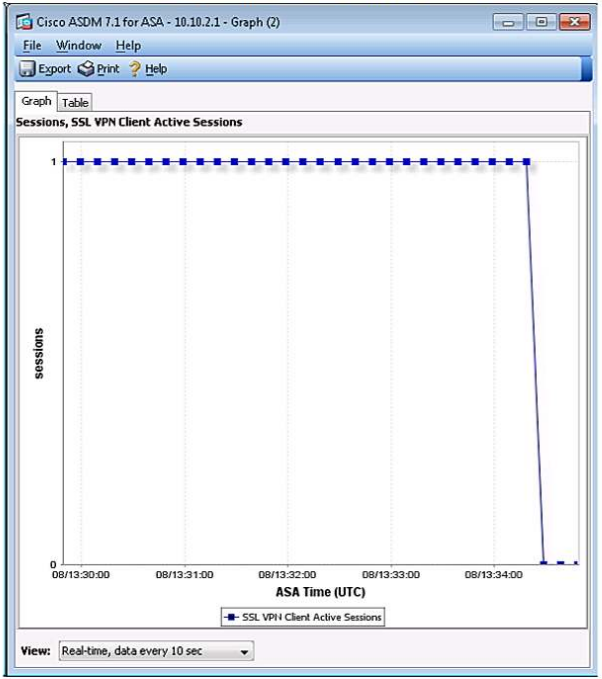
Step 8

On the Employee-PC disconnect from the VPN by selecting **VPN Disconnect** option at the AnyConnect icon. Verify that you cannot connect to the internal resources when the VPN tunnel is disconnected.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 9

In the ASDM examine **Sessions, SSL VPN Client Active Sessions** graph once again.



You should see **Sessions, SSL VPN Client Active Sessions** graph showing zero active sessions.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 5-2: Configure Advanced Authentication for Cisco AnyConnect SSL VPN

Activity Objective

In this lab activity, you will deploy Cisco AnyConnect SSL VPNs on the Cisco Adaptive Security Appliance. First, you will enable basic Cisco AnyConnect SSL VPN access with RADIUS-based user authentication. You will configure the Cisco ASA and the Cisco Identity Services Engine for RADIUS communication. You will augment the scenario by deploying two additional client authentication methods: certificate-based and two-factor (certificate and password.) Next, the Cisco AnyConnect SSL VPN scenario will be enhanced with two authorization types: local authorization with ACLs deployed on the adaptive security appliance, and RADIUS-based authorization using ACLs pushed from the RADIUS server. Finally, you will deploy the Cisco AnyConnect profile in two different ways. You will use WebLaunch to deploy a profile that allows Cisco AnyConnect sessions from remote desktops. You will use the pre-deployment method to enable Start Before Logon (SBL).

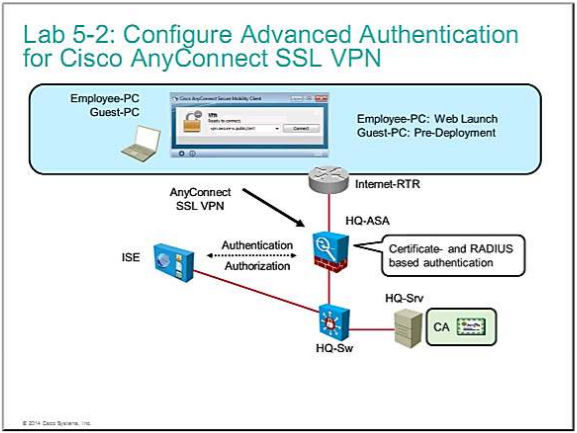
Upon completing this activity, you will be able to meet these objectives:

- Implement Cisco AnyConnect SSL VPN access with RADIUS-based user authentication.
- Deploy three client authentication types: password-based, certificate-based, and two-factor (password and certificate).
- Implement SSL VPN authorization using two methods: local authorization, and RADIUS-based authorization using ACLs downloaded from the RADIUS server.
- Deploy Cisco AnyConnect Mobility profiles using the WebLaunch and pre-deployment methods.

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources and equipment are required to complete this activity:

- Cisco ASA
- Client computer

Job Aids

These job aids are available to help you complete the lab activity.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

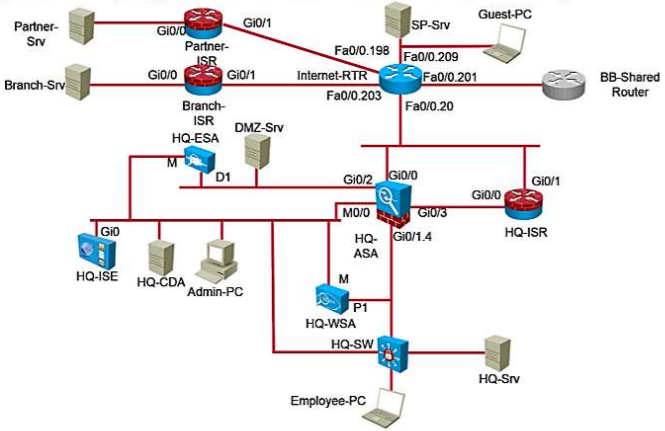
https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

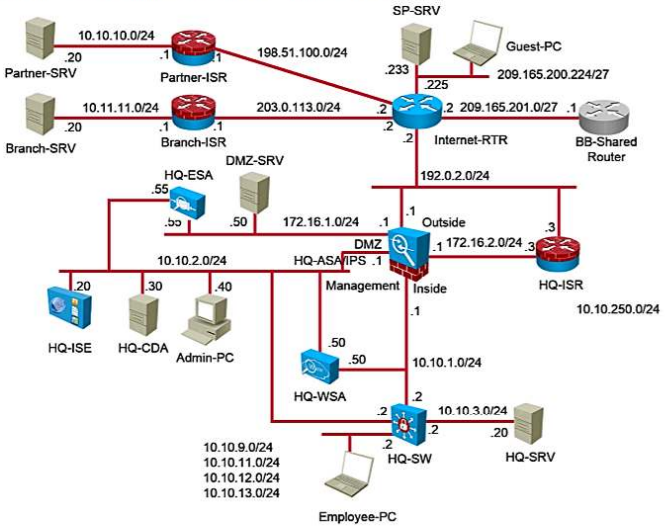
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.

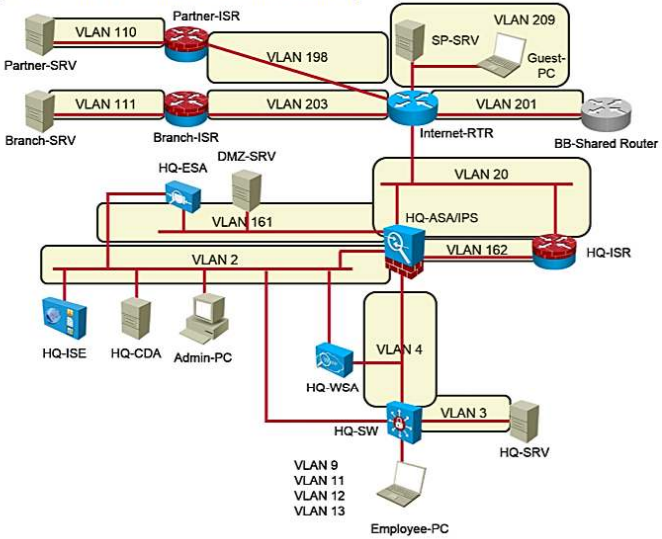


The figure shows the IP addresses that are used in this lab setup.



VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Join the ISE to Active Directory

In this task, you will join the Cisco ISE to the Active Directory. The ISE has been preconfigured for the VPN AAA, but it becomes disconnected when the lab loads.

Activity Procedure

Complete the following steps:

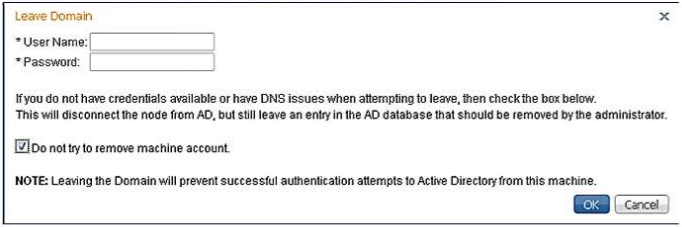
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 1

Make sure that the Cisco ISE is joined and connected to the AD server:

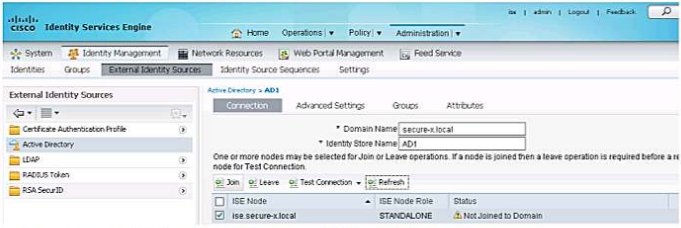
A) On the Admin-PC, open Internet Explorer and connect to the Cisco ISE management GUI (https://ise.secure-x.local). Log in as **admin** with password **Ci5coAdmin**. Go to **Administration > Identity Management > External Identity Sources > Active Directory**.

B) Choose the node and click the **Leave** button. The **Leave Doman** window will open, check the **Do not try to remove machine account** check box and then click the **OK** button.



In the **Leave Operation Status** window wait until status changes into **Completed** and click **OK** button.

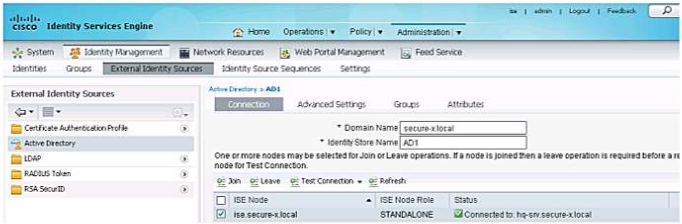
C) Choose the node and click the **Join** button:



D) Enter the username **administrator** and password **Ci5coAdmin**.



E) Verify that the Cisco ISE becomes successfully connected:



Task 2: Deploy Certificate-Based Client Authentication

In this task, you will enable certificate-based client authentication. The domain user it1 has obtained the identity certificates and installed it on the Employee-PC. The employee will use this identity certificate for authentication to the VPN headend.

Activity Procedure

Complete the following steps:

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

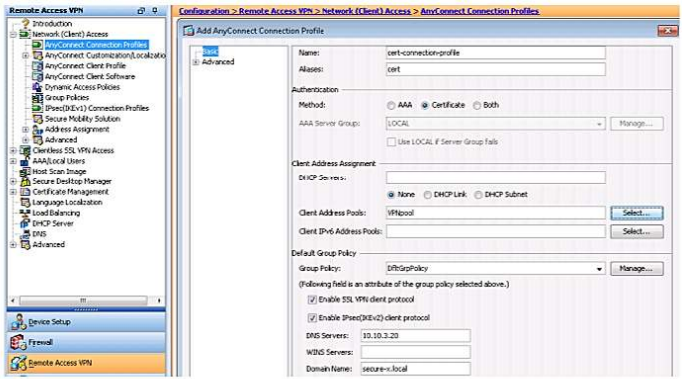
Step 1

Configure an authentication profile for certificate-based authentication:

A) In the Cisco ASDM, go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**.

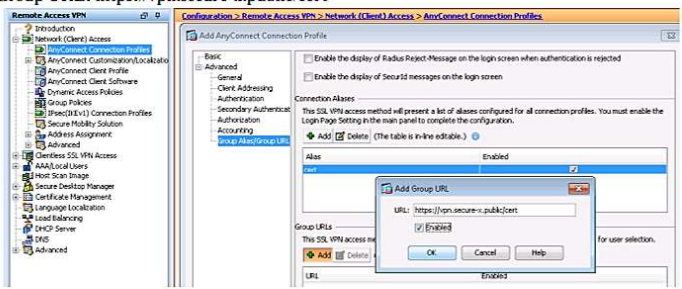
B) Create a new profile (**cert-connection-profile**) with these settings:

- **Authentication method: Certificate**
- **Client address pool: VPNpool**
- **Group policy: DfltGrpPolicy**
- **DNS: 10.10.3.20**



C) Configure a group URL (**Advanced > Group alias/Group URL**) in addition to the connection alias. The group alias and the group URL are methods of selecting a specific connection profile. You will test both methods in the subsequent steps.

- **Connection alias: cert**
- **Group URL: https://vpn.secure-x.public/cert**



D) Accept and apply the changes. Send the commands.

https://t.me/learningnets



Step 2

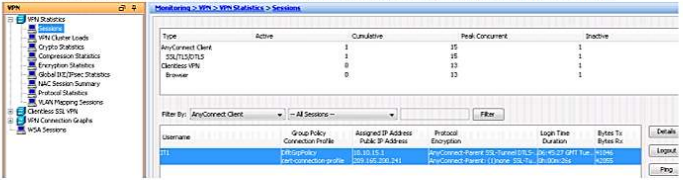
Test certificate-based authentication by accessing the connection profile alias:

A) Make sure that you are logged on to the Employee-PC as domain user it1. You have obtained a certificate for this user in a previous exercise, before moving the Employee-PC to the SP subnet.

B) Disconnect and reconnect the VPN session. Choose the **cert** alias from the **Group** drop-down list. You should see that this connection profile does not use any other entry fields, such as username or password, and that certificate will be used for authentication. Click **OK** in the **Cisco AnyConnect | vpn.secure-x.public** window.



C) In the Cisco ASDM, go to **Monitoring > VPN > VPN Statistics > Sessions** and view the established AnyConnect sessions. You should see that the it1 user has been successfully authenticated.



D) On the Admin-PC log in to the ISE GUI (https://ise.secure-x.local) and examine the authentications attempts (**Operations > Authentications**). You will not see any attempts, because the VPN server (ASA) locally validates the client certificate and does not contact the RADIUS server. The validation is successful because the ASA has been enrolled with the HQ-SRV-CA and has the CA root certificate. The public key from the CA root certificate is used to validate the signature in the client certificate.

E) Optionally, verify client connectivity to internal and DMZ resources.

F) Disconnect the session either from the VPN headend or from the client side.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

Test certificate-based authentication by connecting to the group URL:

A) Enter the **Group URL** in the **Connect** field of the AnyConnect client:



B) Click **Connect**, and test the established connection. Disconnect the session when finished.

Task 3: Deploy Two-Factor Client Authentication

Having enabled certificate-based client authentication you will augment it by an additional password authentication. The two-factor authentication is considered more secure because of its capability to verify what the users have (certificate) and what they know (password.)

Activity Procedure

Complete the following steps:

https://t.me/learningnets

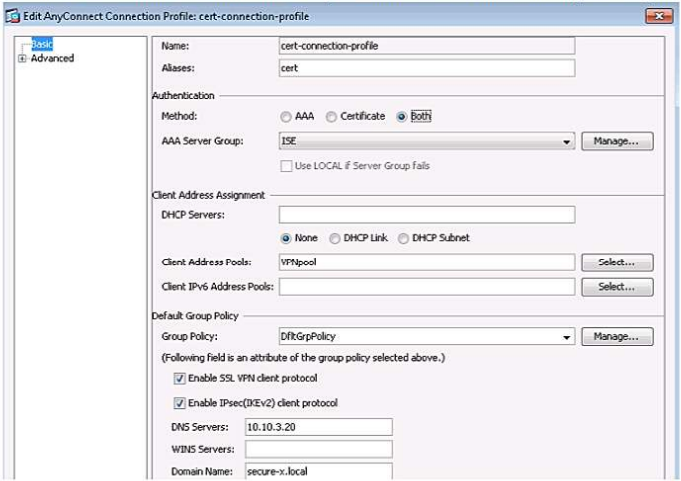
Step 1

Configure two-factor authentication based on the user certificate and user password:

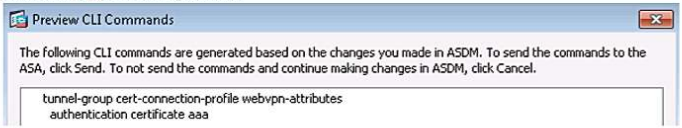
A) In the Cisco ASDM, go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**.

B) Edit the profile used for certificate-based authentication (**cert-connection-profile**).

C) Set the authentication method to **Both** and enable password-based authentication using the ISE group.



D) Confirm and apply the configuration.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 2

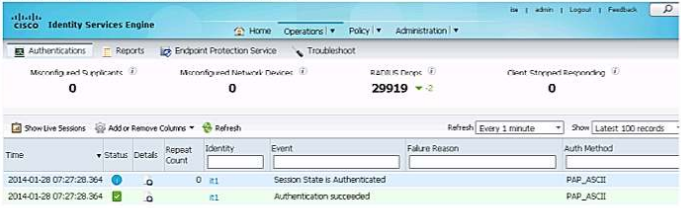
Test two-factor authentication:

A) From the Cisco AnyConnect client, connect to vpn.secure-x.public, choose the connection profile **cert** using either alias or group URL. You should be prompted for username and password. Enter the username and password (**it1**/**cisco**) and connect.



B) On the VPN headend, examine the authentication.

C) In the ISE GUI, view the successful authentication attempt of the domain user it1. The ISE has been consulted for password-based authentication,



Note If you do not see an authentication attempt on the ISE, authenticate to the VPN as another domain user, for example sales1 with password cisco. Then disconnect and re-connect as it1. This will create a fresh authentication session.

D) Disconnect the VPN session.

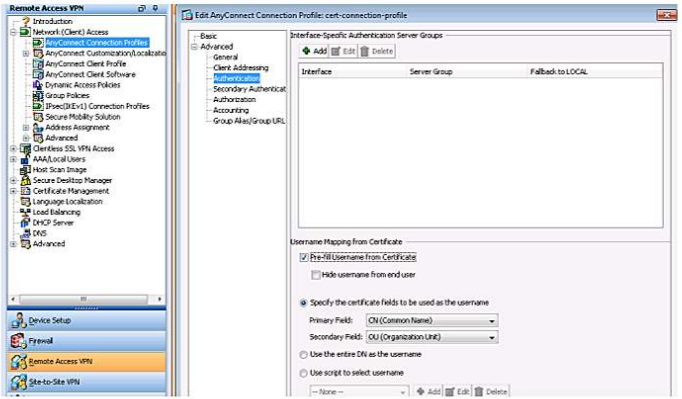
https://t.me/learningnets

Step 3

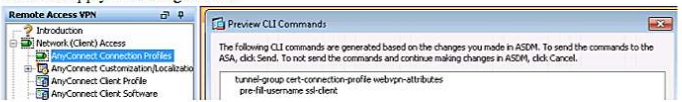
Configure username prefill in the two-factor authentication:

A) In the Cisco ASDM, edit the profile used for certificate-based authentication (**cert-connection-profile**). Go to the **Advanced > Authentication** page.

B) Check the **Pre-fill username from certificate** check box.



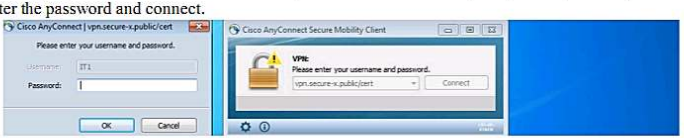
C) Confirm and apply the configuration.



Step 4

Test the username prefill feature:

Go to the Cisco AnyConnect client on Employee-PC, choose the connection profile **cert** using either alias or group URL. The username should be prefilled. You should be prompted only for the password. Enter the password and connect.



Examine the session and then disconnect.

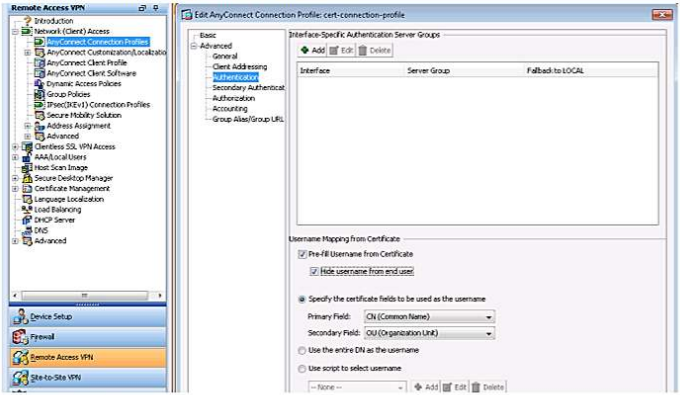
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 5

Configure username hiding in the username prefill feature:

A) In the Cisco ASDM, edit the profile used for certificate-based authentication (cert-connection-profile). Go to the **Advanced > Authentication** page.

B) Check the **Hide username from end user** check box.



C) Confirm and apply the configuration.



Step 6

Test the hidden username in the username prefill feature:

A) Go to the Cisco AnyConnect client on Employee-PC, choose the connection profile **cert** using either alias or group URL. The username should be hidden. You should be prompted for password. Enter the password and connect.



B) Examine the session on the VPN head-end and on the ISE. You will see a repeated authentication of the it1 user. Disconnect the VPN tunnel.

https://t.me/learningnets

Task 4: Deploy Local Authorization for Local VPN Users

In this task you will enhance the AnyConnect SSL VPN scenario using local authorization with ACLs deployed on the adaptive security appliance. This method is not recommended for authentication against remote user databases. In a large deployment with multiple VPN servers, the ACLs would need to be configured on every ASA.

Activity Procedure

Complete the following steps:

Step 1

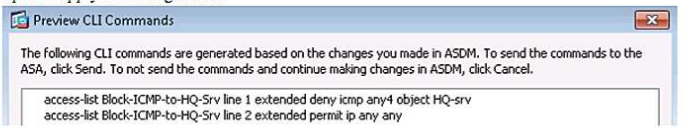
Configure an ACL that denies ICMP traffic to HQ-Srv (10.10.3.20):

A) In the ASDM, go to **Configuration > Remote Access VPN > Network (Client) Access > Advanced > ACL Manager**.

B) Configure an ACL (**Block-ICMP-to-HQ-Srv**) that denies ICMPv4 to HQ-Srv and permits all other traffic.



C) Accept and apply the configuration.



https://t.me/learningnets
© 2014 Cisco Systems, Inc.

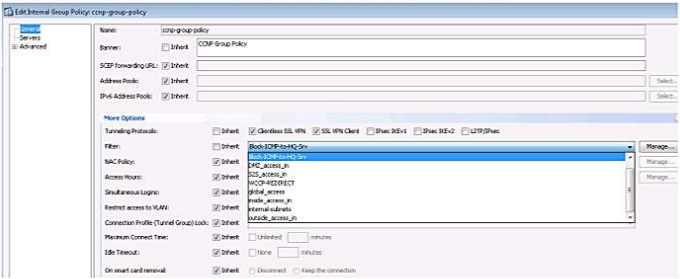
Step 2

Apply the ACL (**Block-ICMP-to-HQ-Srv**) to the ccnp-group-policy. This group policy will be applied when you connect to the VPN as vpnuser.

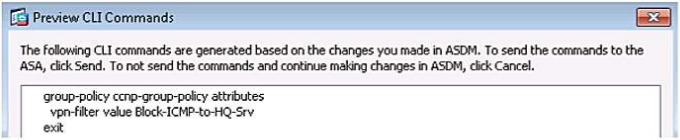
A) Go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

B) Edit the group policy **ccnp-group-policy**. In the **General page** click **More Options**.

C) Choose the ACL (**Block-ICMP-to-HQ-Srv**) from the **Filter** drop-down box.



D) Accept and apply the changes.



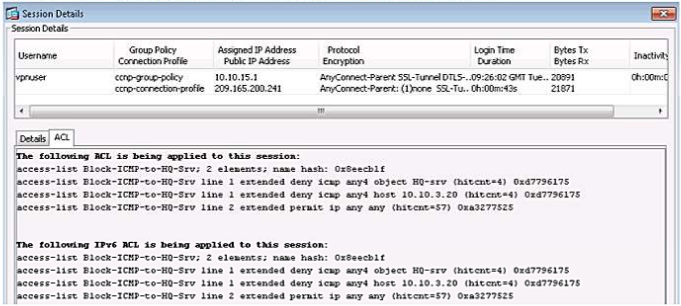
https://t.me/learningnets

Step 3

Test local authorization:

A) From the AnyConnect client, re-connect to vpn.secure-x.local. Select the **ccnp** alias. Authenticate as **vpnuser** with password **cisco**. Accept the banner.

B) In the ASDM monitoring, examine the ACL applied to the session (click **Details** and then select the **ACL tab**). You will see that the local ACL has been applied to the session.



C) On the Employee-PC, verify the connectivity:

You will ping dmz.secure-x.local

You will connect via HTTP to hq-srv.secure-x.local and dmz.secure-x.local

You cannot ping hq-srv.secure-x.local

D) Disconnect the VPN session.

Task 5: Deploy External Authorization

In this task, you will enhance the VPN scenario with RADIUS-based authorization using ACLs pushed from the RADIUS server.

Activity Procedure

Complete the following steps:

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 1

Explore the preconfigured ISE settings, which will prevent the ise2 user from communicating via ICMP with the HQ-Srv:

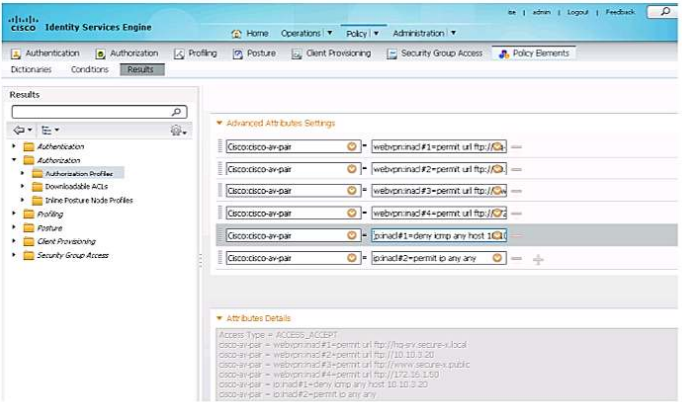
A) Log in to the ISE GUI (https://ise.secure-x.local) as **admin** with password **Ci5coAdmin**.

B) Go to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

C) Examine the advanced attribute settings of the **VPN_Authorization** profile. After the WebACL attributes you will see two ACL attributes that control the client access:

   a. cisco-av-pair = ip:inacl#1=deny icmp any host 10.10.3.20

   b. cisco-av-pair = ip:inacl#2=permit ip any any



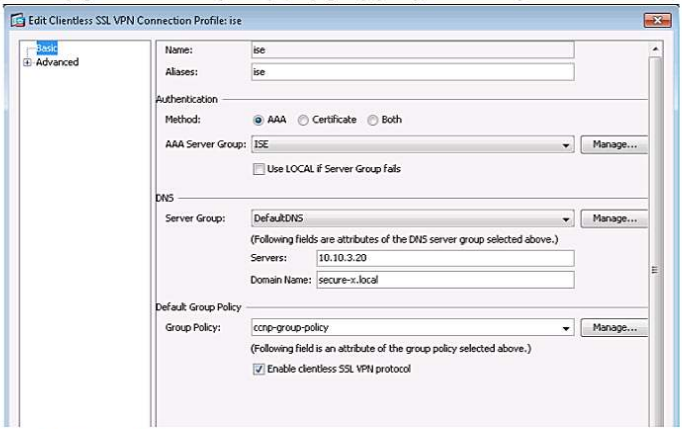
Step 2

Apply the **ccnp-group-policy** to the **ise** connection profile.

A) Go to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**

B) Edit the Connection Profile **ise**.

C) In the **Basic** page choose the Group Policy (**ccnp-group-policy**) from the drop-down menu.



D) Accept and apply the changes.

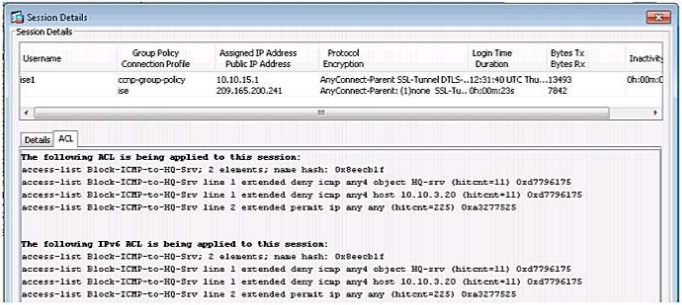
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

Test external authorization:

Establish the tunnel from the Cisco AnyConnect client and select the ise connection alias. This connection profile (**ise1/cisco**) will allow you to authenticate the users against the RADIUS database.

In the ASDM monitoring, examine the ACL applied to the session. You will see that the downloaded ACL has been applied to the session.



From the Employee-PC, verify the connectivity:

- You should connect via HTTP to **hq-srv.secure-x.local** and **dmz.secure-x.local**
- You should ping to **dmz.secure-x.local**
- You cannot ping to **hq-srv.secure-x.local**

Disconnect the session.

Task 6: Deploy AnyConnect Profile To Allow AnyConnect VPNs from Remote Desktop

Some Cisco AnyConnect settings are customized using the AnyConnect profiles. These XML files are deployed on the client machines using the WebLaunch or predeploy method. In this task, you will configure the Cisco ASA to push the Cisco AnyConnect profile using the WebLaunch method. You will use the Cisco AnyConnect profile to enable the launching of AnyConnect from remote desktop sessions.

Activity Procedure

Complete the following steps:

https://t.me/learningnets

Step 1

Verify that you cannot launch the AnyConnect from a RDP session:

A) On the Employee-PC, examine the IP address of the Employee-PC. You will connect to it via RDP. It should be similar to 209.165.200.241. Log off from the Employee-PC.

B) From the Guest-PC, connect via RDP to Employee PC (**Start > All Programs > Accessories > Remote Desktop Connection**). Log on as **employee-pc\student** with password **Ci5coAdmin**. Accept any security warnings.

C) Launch the Cisco AnyConnect client from the RDP session to the Employee-PC. Choose the **ccnp** alias. Log in as **vpnuser** with password **cisco**. The VPN connection will fail because VPN connections from remote desktops are disabled.



Step 2

Show hidden files and view the Cisco AnyConnect profile folder:

A) On the Employee-PC, open a Windows Explorer window. Go to **Organize > Folder and Search options > View tab**. Choose the **Show hidden files, folders, and drives** radio button. Apply it to all folders and click **OK**.

B) View the content of the folder **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client \Profile**. You will only see the file **AnyConnectProfile.xsd**. There are no AnyConnect profiles in this folder because you have not configured the Cisco ASA to push any profiles yet.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 3

In the ASDM, create a Cisco AnyConnect profile:

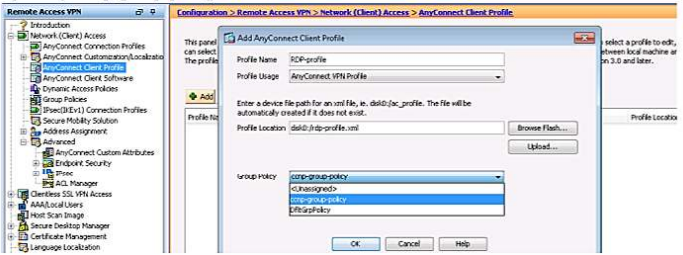
A) Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

B) Click **Add** and create a profile named **RDP-profile.**

C) Profile usage: **AnyConnect VPN Profile**

D) Profile Location: <default setting>

E) Group Policy: **ccnp-group-policy**

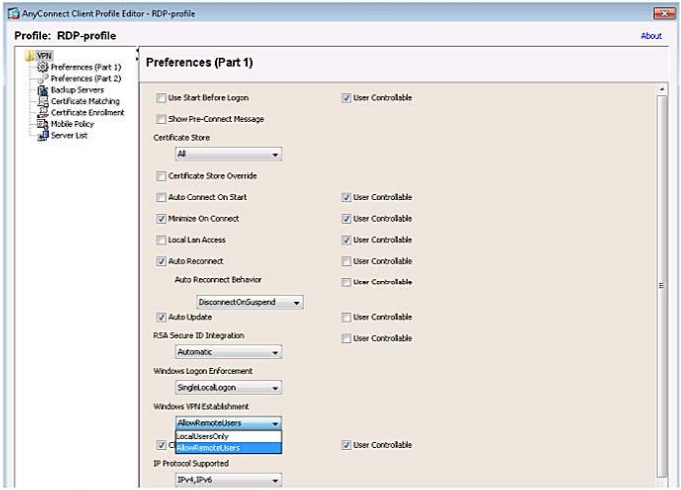


Step 4

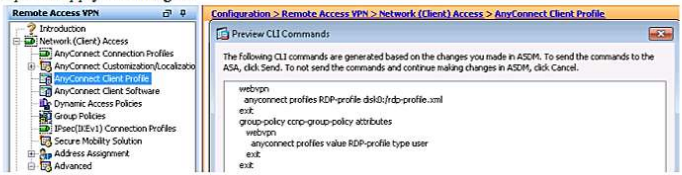
Edit the profile to allow the remote users to launch the AnyConnect sessions:

A) Click the **Edit** button.

B) Choose **AllowRemoteUsers** in the Windows VPN Establishment menu.



C) Accept and apply the changes.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 5

Connect to the Cisco ASA CLI and view the Cisco AnyConnect profile in the flash memory.

```
HQ-ASA# more flash:/rdp-profile.xml
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://schemas.xmlsoap.org/
encoding/ AnyConnectProfile.xsd">
        <ClientInitialization>
                <UseStartBeforeLogon UserControllable="true">false</
UseStartBeforeLogon>
                <AutomaticCertSelection UserControllable="true">false</
AutomaticCertSelection>
                <ShowPreConnectMessage>false</ShowPreConnectMessage>
                <CertificateStore>All</CertificateStore>
                <CertificateStoreOverride>false</CertificateStoreOverride>
                <ProxySettings>Native</ProxySettings>
                <AllowLocalProxyConnections>true</AllowLocalProxyConnections>
                <AuthenticationTimeout>12</AuthenticationTimeout>
                <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
                <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
                <LocalLanAccess UserControllable="true">false</LocalLanAccess>
                <ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
                <IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
                <AutoReconnect UserControllable="false">true
                        <AutoReconnectBehavior
UserControllable="false">DisconnectOnSuspend</AutoReconnectBehavior>
                </AutoReconnect>
                <AutoUpdate UserControllable="false">true</AutoUpdate>
                <RSASecurIDIntegration UserControllable="false">Automatic</
RSASecurIDIntegration>
                <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
                <WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
                <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
                <PPPExclusion UserControllable="false">Disable
                        <PPPExclusionServerIP UserControllable="false"></
PPPExclusionServerIP>
                </PPPExclusion>
                <EnableScripting UserControllable="false">false</EnableScripting>
                <EnableAutomaticServerSelection UserControllable="false">false
                        <AutoServerSelectionImprovement>20</
AutoServerSelectionImprovement>
                        <AutoServerSelectionSuspendTime>4</
AutoServerSelectionSuspendTime>
                </EnableAutomaticServerSelection>
                <RetainVpnOnLogoff>false
                </RetainVpnOnLogoff>
        </ClientInitialization>
</AnyConnectProfile>
```

Step 6

Launch the Cisco AnyConnect client from the RDP session to the Employee-PC. Choose the **ccnp** alias. Log in as **vpnuser** with password **cisco.** Accept the banner. The connection from the remote desktop session should succeed.

https://t.me/learningnets

Step 7

View the content of the **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile** folder. You should see the **RDP-profile.xml**. Open the file using a browser and examine its content.

Task 7: Deploy Standalone AnyConnect Client on Guest-PC

In this task, you will pre-deploy the AnyConnect Mobility client and profile using the standalone installation. Stand-alone Cisco AnyConnect Mobility Client installation is also referred to as pre-deployment. In this method the users do not need to connect via clientless SSL VPN to download the client software. You will use the standalone installation to enable the SBL functionality on the Guest-PC. The SBL feature when the users need to establish the VPN tunnel before logging to the local machine.

Activity Procedure

Complete the following steps:

Step 1

Connect to the Guest-PC (**student/Ci5coAdmin**) and install the Cisco AnyConnect Mobility client using the pre-deploy package:

A) Go to **D:\AnyConnect\anyconnect-win-3.1.04059-pre-deploy-k9** folder. Launch the **anyconnect-win-3.1.04059-pre-deploy-k9.msi** installer.

B) Start the installation wizard, accept the license agreement, click **Install**. Click **Finish** when the installation completes.

Step 2

Verify the initial state with no Cisco AnyConnect profile:

A) Display hidden folders and files:

- On the Guest-PC, open a Windows Explorer window. Go to **Organize > Folder and Search options > View tab**.
- Click the **Show hidden files, folders, and drives** radio button. Apply it to all folders and click **OK**.

B) View the content of the folder **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client \Profile**. You should only see the file AnyConnectProfile.xsd.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

On the Guest-PC, install the Cisco AnyConnect Profile Editor:

A) Go to **D:\AnyConnect** folder. Launch the **anyconnect-profileeditor-win-3.1.04059-k9.exe**.

B) Start the installation wizard and choose **Custom** setup type.

C) Clear the **Network Access Manager Profile Editor** selection and choose the **VPN Profile Editor** to be installed.



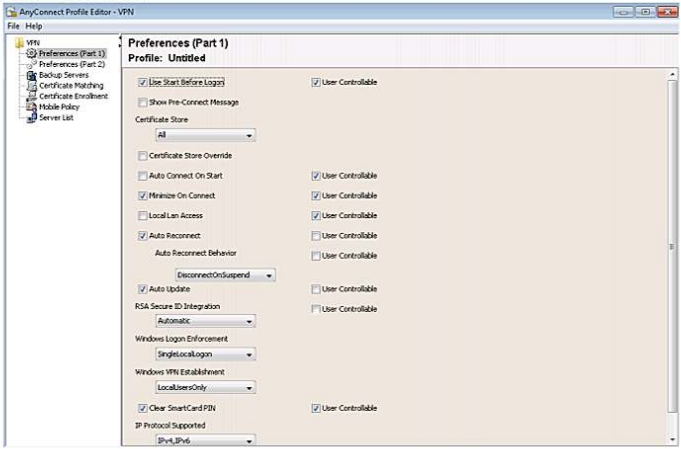
D) Click **Next**, then click **Install** to complete the installation.

https://t.me/learningnets

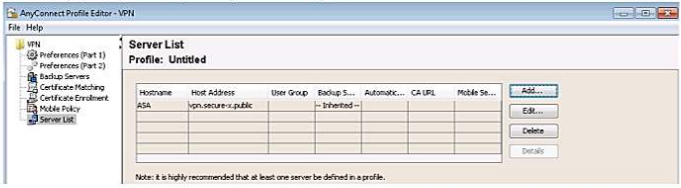
Step 4

Launch the standalone profile editor and create an AnyConnect profile with these settings:

A) Enable the SBL feature.



B) Add the entry (**ASA**) with FQDN **vpn.secure-x.public** to the server list.



C) Save the profile as **predeploy-profile.xml** in the **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile** folder.

Step 5

Launch the Cisco AnyConnect client, choose **ASA** entry from the drop-down list. Select the ise connection alias. Log in as ise1 with password cisco. The VPN tunnel will be established because the HQ-SRV-CA root certificate has been installed in the user certificate store. This trust relationship enabled also clientless SSL VPN sessions from teh Guest-PC in earlier exercises.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 6

Install the CA root certificate in the machine certificate store. The AnyConnect client uses the machine certificate store (not the user certificate store) for SBL and VPN Always On features.

A) Launch the Microsoft Management Console (**Start > mmc**).

B) Choose **File > Add/Remove Snap-in.**

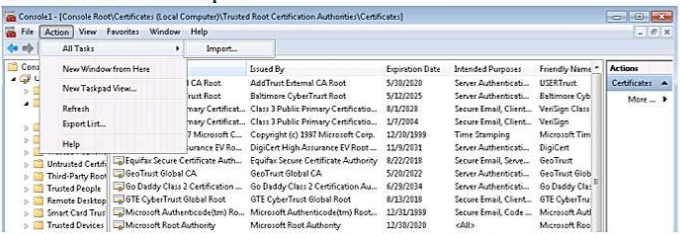
C) Choose **Certificates** from the **Available Snap-ins** list and click **Add** to move it to the **Selected Snap-ins** pane.

D) Choose **Computer account** and click **Next**.

E) Accept the **Local computer** selection and click **Finish**. Click **OK**.

F) Go to **Console Root > Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates.**

G) Choose **Action > All Tasks > Import**.



H) Follow the Certificate Import Wizard. Browse to the CA root certificate file (CA-root-DER.cer) stored on disk D:\ and import it in the **Trusted Root Certification Authorities** store.

Step 7

Install the pre-deployment version of the SBL module:

A) On the Guest-PC, run the **D:\AnyConnect\anyconnect-win-3.1.04059-pre-deploy-k9\anyconnect-gina-win-3.1.04059-pre-deploy-k9.msi** installer.

B) Follow the installation wizard. At the end of the installation, you should be prompted to reload the computer. Accept the prompt to reload.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 8

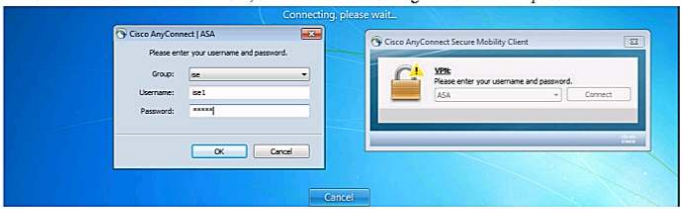
If the Guest-PC automatically boots with a user logged on to it, log off the user. Send the **Alt+Ctrl+Del** combination. You should see the SBL icon on the login screen.



Note	You will not see the SBL icon when you connect via VNC or RDP.

Step 9

Click the **SBL icon**. Connect to the ASA, select the **ise** alias. Log on as **ise1** with password **cisco**.



Step 10

When the VPN tunnel is set up, log on to the **Guest-PC** as student with password **Ci5coAdmin**.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Lab 5-3: Implement AnyConnect IPSec/IKEv2

Activity Objective

In this lab activity you will deploy AnyConnect IPsec VPNs on the Cisco Adaptive Security Appliance. You will implement two deployment methods: WebLaunch and Standalone pre-deployment. For each method, you will configure a group policy, connection profile, and an AnyConnect profile. You will observe the differences in the first VPN sessions between the two deployment methods. You will not deploy any local or external ACL-based authorization because the configuration procedure is identical to the one in AnyConnect SSL VPNs.

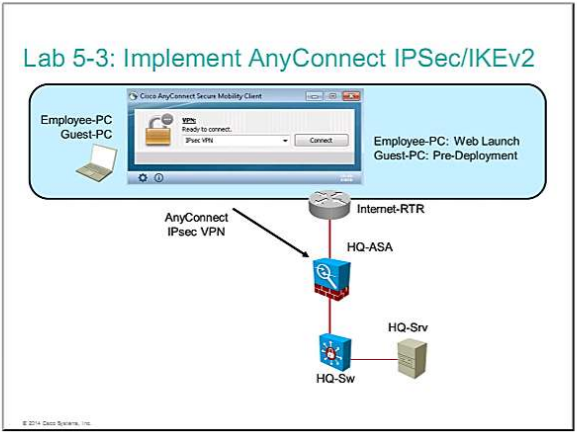
Upon completing this activity, you will be able to meet these objectives:

- Implement Cisco AnyConnect IPsec VPN using the WebLaunch method
- Implement Cisco AnyConnect IPsec VPN using the standalone pre-deployment

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

- Cisco ASA
- Two client computers.

Job Aids

These job aids are available to help you complete the lab activity.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

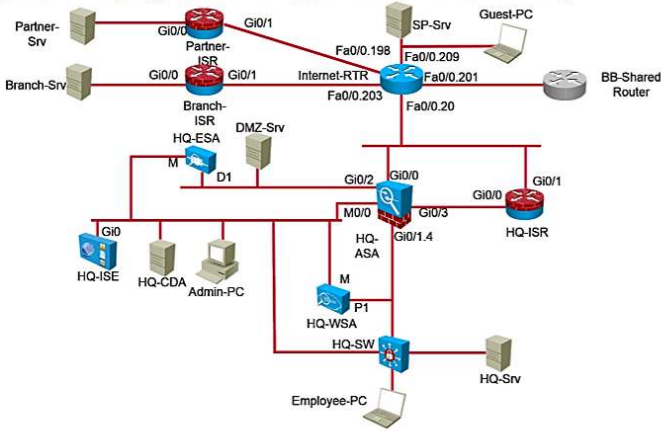
https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

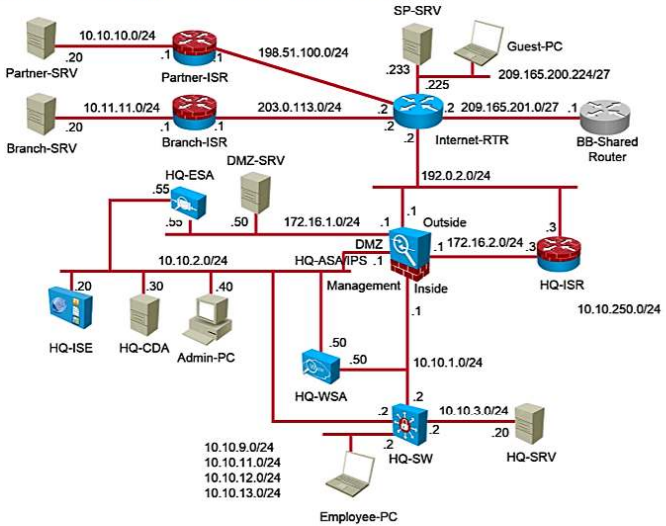
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.



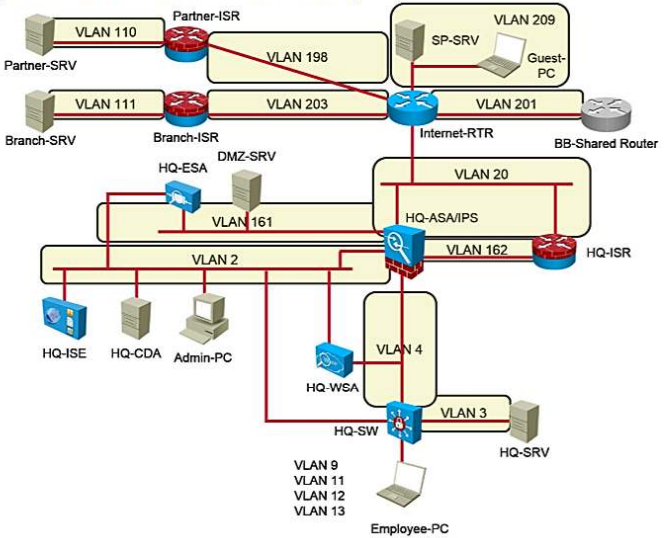
The figure shows the IP addresses that are used in this lab setup.



https://t.me/learningnets

VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Deploy AnyConnect IPsec VPN Using WebLaunch

In this task you will deploy the AnyConnect IPsec VPN on the Employee-PC using the WebLaunch method. AnyConnect IPsec VPN requires the setting of the primary protocol as IPsec in the AnyConnect profile. You will configure a new group policy (ipsec-weblaunch-policy), AnyConnect profile (IPsec) and connection profile (ipsec-weblaunch) using the ASDM. The VPN clients will download the AnyConnect profile when the appropriate connection profile is selected.

Activity Procedure

Complete the following steps:

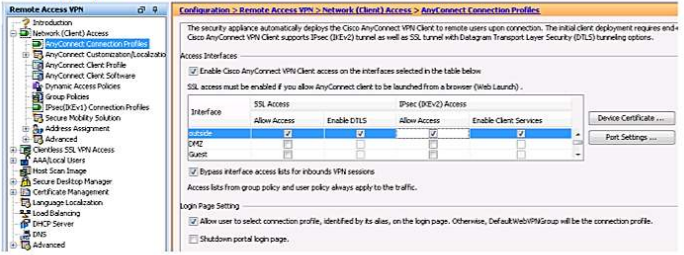
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 1

Allow IPsec VPN access via the ASA's outside interface:

A) In the ASDM on the Admin-PC, go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**.

B) Check the appropriate checkbox for IPsec/IKEv2 access via the outside interface.



C) Accept and apply the configuration.

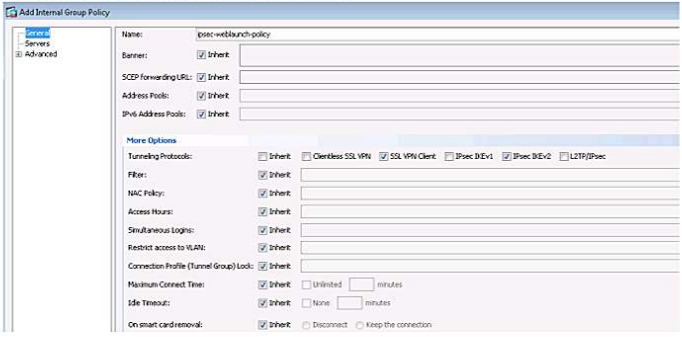
https://t.me/learningnets

Step 2

Create a custom group policy (**ipsec-weblaunch-policy**) that allows AnyConnect SSL and IPsec:

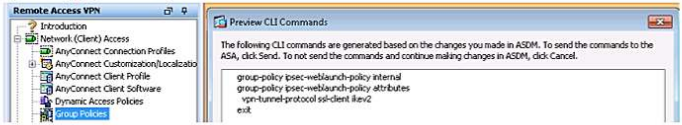
A) In the Cisco Adaptive Security Device Manager on the Admin-PC, go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

B) Add an internal group policy (**ipsec-weblaunch-policy**). Go to **General > More Options > Tunneling Protocols**. Enable SSL VPN Client and IPsec IKEv2.



Note The SSL VPN Client protocol needs to be enabled along with IPsec IKEv2 because the initial connection to the VPN server uses SSL/DTLS.

C) Accept and apply the configuration.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

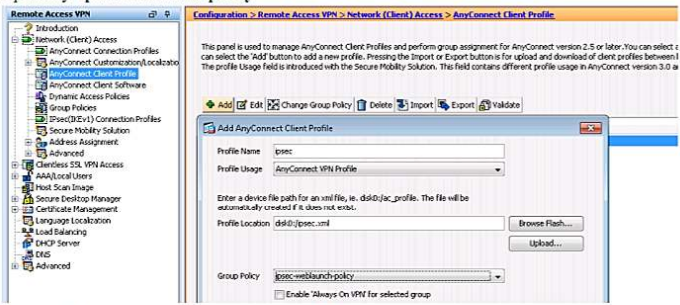
Create a new AnyConnect profile (**Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**) for IPsec access with these settings:

A) Name: **ipsec**

B) Profile Usage: AnyConnect VPN Profile (default)

C) Profile Location: disk0:/ipsec.xml (default)

D) Group Policy: **ipsec-weblaunch-policy**



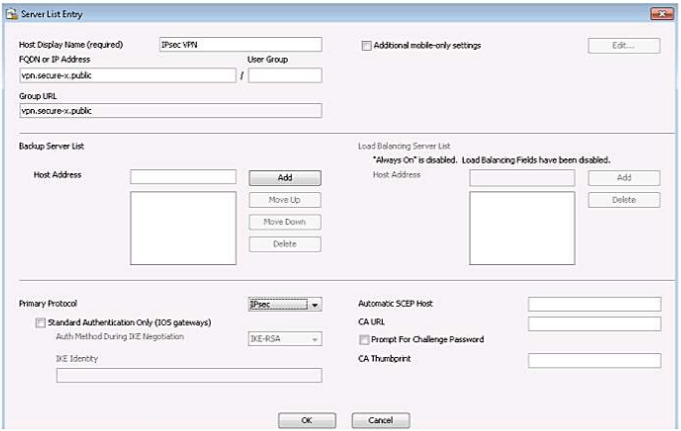
E) Click **OK** and then edit the profile using the **Edit** button. In the server list, create an entry with these attributes:

Host Display Name: IPsec VPN

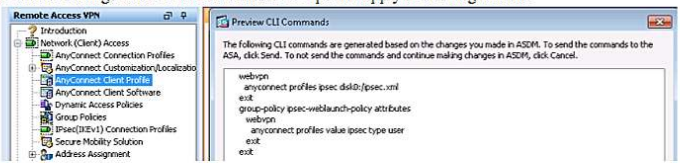
FQDN: vpn.secure-x.public

Primary protocol: IPsec

https://t.me/learningnets



F) Leave other settings at their default values. Accept and apply the configuration.



https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 4

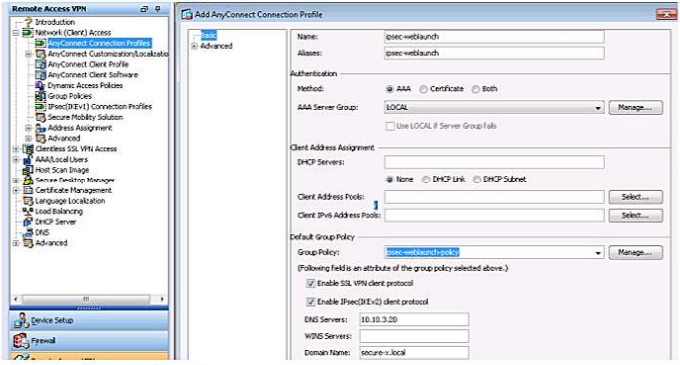
Create a new connection profile (**Configuration>Remote Access VPN>Network (Client) Access>AnyConnect Connection Profiles**) for IPsec access with these attributes:

A) **Name: ipsec-weblaunch**

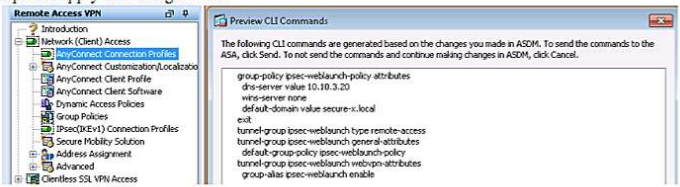
B) **Alias: ipsec-weblaunch**

C) **Group policy: ipsec-weblaunch-policy**

D) Leave other settings at their default values. The missing values, such as the address pool will be inherited from the default group policy.



E) Accept and apply the configuration.



https://t.me/learningnets

Step 5

On the Employee-PC (log on as secure-x domain user it1 with password cisco) connect the AnyConnect client to **vpn.secure-x.public**. Select the group alias **ipsec-weblaunch**. Log in as **vpnuser** with password **cisco**.

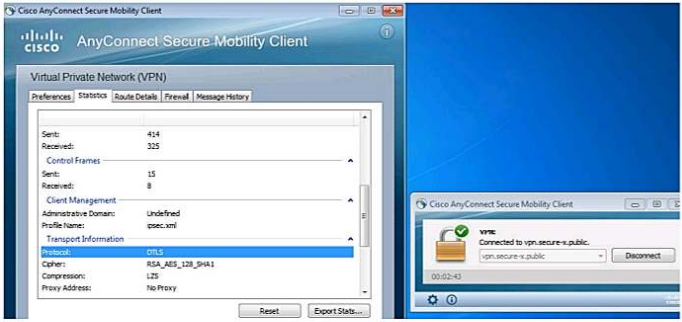


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

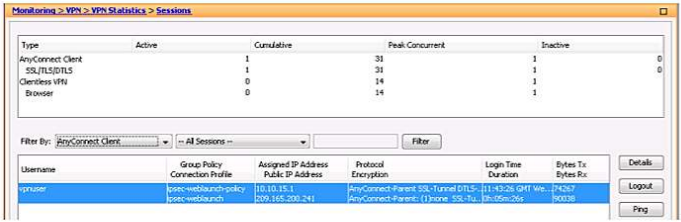
Step 6

Verify the AnyConnect status after the first connection with the connection profile and group policy configured for IPsec/IKEv2:

A) Click on the wheel symbol in the AnyConnect UI. Go to the **Statistics** tab and examine the details in the **Transport Information** section. You will see that the transport protocol for the first connection is DTLS. DTLS is used for the initial AnyConnect session, during which the AnyConnect profile is downloaded from the ASA.



B) In the ASDM, go to **Monitoring** and verify that the VPN server also reports the connection as a DTLS session.



C) On the Employee-PC, view the content of the folder **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile**. You should see that the **ipsec.xml** has been successfully downloaded from the VPN server.

Note	If the folder is hidden, go to **Organize > Folder and Search options > View tab.** Select the **Show hidden files, folders, and drives** radio button. Apply it to all folders and click **OK**.

https://t.me/learningnets

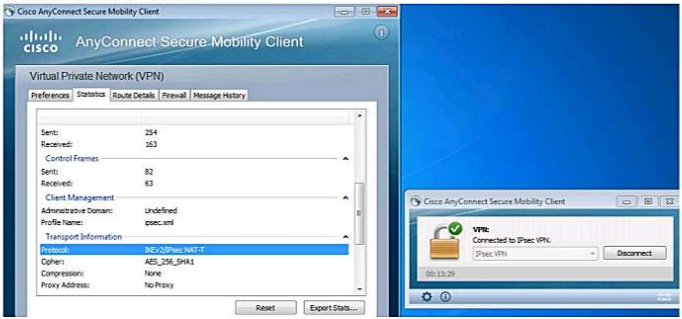
Step 7

Examine the transport of the subsequent AnyConnect connections:

A) On the Employee-PC, disconnect and re-start the AnyConnect connection. The AnyConnect UI should display **IPsec VPN**, the VPN server ID from the received AnyConnect profile. Connect using the **ipsec-weblaunch** profile. Log in as **vpnuser** with password **cisco**.



B) Click on the wheel symbol in the AnyConnect UI. Go to the **Statistics** tab and examine the details in the **Transport Information** section. You should see that the transport protocol for the subsequent connections is IKEv2/IPsec.



C) In ASDM monitoring, verify that the transport protocol of the VPN connection is IKEv2/IPsec. Disconnect the session.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

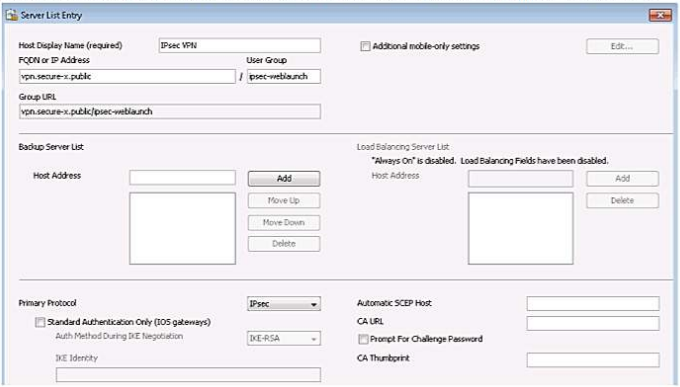
Step 8

Configure the AnyConnect profile (**ipsec**) for the automatic selection of the group alias:

A) Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

B) Edit the profile named **ipsec**

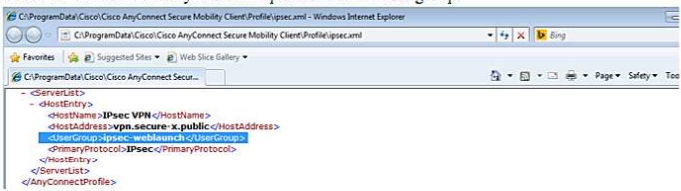
C) Edit the VPN server entry. Set the user group to the connection profile name (**ipsec-weblaunch**).



D) Click **OK** and apply the changes.

Step 9

From the Employee-PC reconnect to the IPsec VPN using the same method and then disconnect. As a result of this connection, the updated AnyConnect profile will be downloaded to the Employee-PC. Open the ipsec.xml file in the folder C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile. You should see that VPN server entry has been updated with the user group.



https://t.me/learningnets

Step 10

From the Employee-PC reconnect to the IPsec VPN using the **IPsc VPN** entry. You will not need to select the connection profile because this information has been retrieved from the downloaded AnyConnect profile. Log in as vpnuser.



Step 11

From the Employee-PC, verify that you can access internal resources. For example ping, FTP and HTTP to hq-srv.secure-x.local or dmz.secure-x.local. The group policy ipsec-policy does not any local or external authorization. You could enhance the scenario using the mechanisms demonstrated for the client access. Disconnect the session.

Task 2: Deploy AnyConnect IPsec VPN Using Standalone AnyConnect Mobility Client (Optional)

In this task you will implement the AnyConnect IPsec VPN on the Guest-PC using the pre-deployment method. In the standalone deployment you will configure the primary protocol as IPsec in the AnyConnect profile stored on the Guest-PC. You will create an appropriate group policy and connection profile in the ASDM. You will observe that the pre-deployed AnyConnect IPsec clients use the IKEv2/IPsec protection from the very first connection.

Activity Procedure

Complete the following steps:

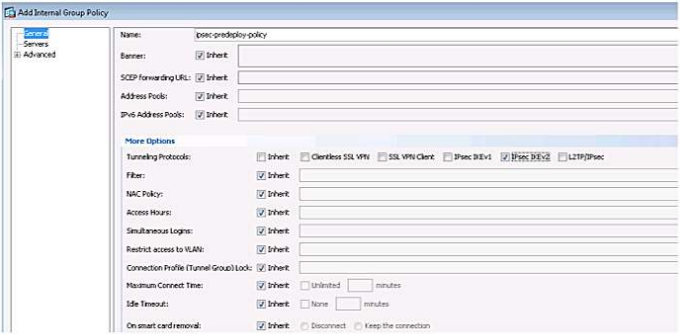
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 1

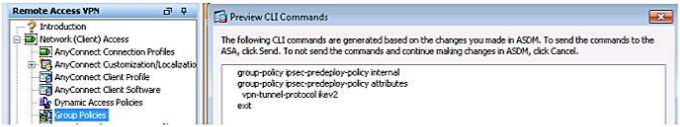
Create a custom group policy (**ipsec-predeploy-policy**) that allows only IPsec/IKEv2:

A) In the ASDM on the Admin-PC, go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

B) Add an internal group policy (**ipsec-predeploy-policy**). Go to **General > More Options > Tunneling Protocols**. Enable IPsec IKEv2.



C) **Accept** and **apply** the configuration.



Step 2

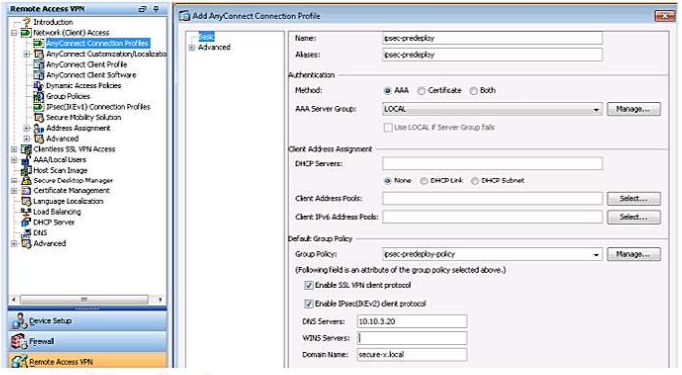
Create a new connection profile **(Configuration>Remote Access VPN>Network (Client) Access>AnyConnect Connection Profiles)** for IPsec access with these attributes:

A) **Name: ipsec-predeploy**

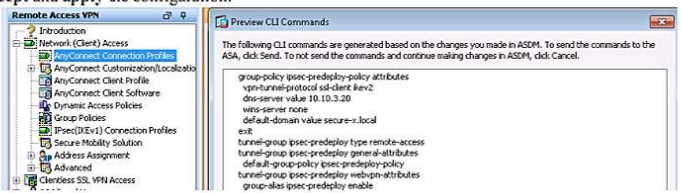
B) **Alias: ipsec-predeploy**

C) **Group policy: ipsec-predeploy-policy**

D) Leave other settings at their default values. The missing values, such as the address pool will be inherited from the default group policy.



E) **Accept** and **apply** the configuration.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

On the Guest-PC, configure an AnyConnect profile for IPsec:

A) Start the AnyConnect profile editor.

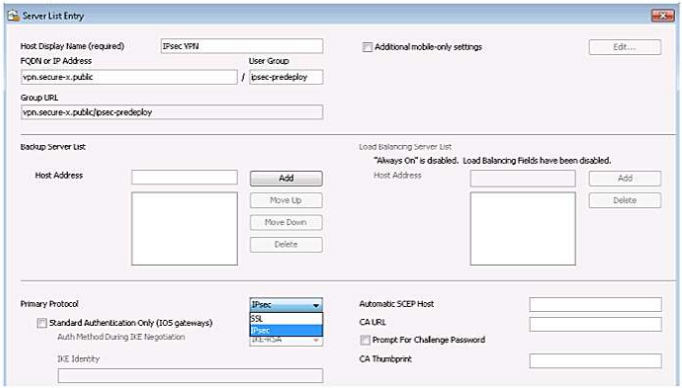
B) Configure a server in the server list with these attributes:

Host display name: IPsec VPN

FQDN: vpn.secure-x.public

User Group: ipsec-predeploy. With the connection profile alias entered in the user group you will not need to select the connection profile when connecting to the VPN.

Primary Protocol: IPsec



C) Save the profile in the the **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client \Profile** folder, for example as **ipsec-predeploy.xml**.

https://t.me/learningnets

Step 4

Verify the AnyConnect IPsec VPN session establishment with the user group configuration:

A) On the Guest-PC, from the system tray, right-click the **AnyConnect icon** and choose **Quit**. This terminates the AnyConnect client. When you restart it, the client will retrieve the profiles from the Profile folder.



B) Restart the AnyConnect client (**Start > All Programs > Cisco > Cisco AnyConnect Secure Mobility Client**). Select the connection profile alias for the IPsec VPN (**IPsec VPN**).



C) You will not see the drop-down list with the connection profile aliases because the connection profile has been specified in the AnyConnect profile user group. Log in as **vpnuser** with password **cisco**.



D) Verify that the transport protocol displayed in the AnyConnect UI and in the ASDM monitoring is IPsec/IKEv2. Verify that you can access the internal resources through the VPN tunnel. Disconnect the VPN tunnel.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Lab 6-1: Implement Host Scan and DAP

Activity Objective

In this lab activity you will use the Host Scan and Dynamic Access Policy (DAP) features to ensure that only compliant endpoints are permitted to access the AnyConnect SSL VPN. The compliance status will be met when the host scan feature detects an up-to-date anti-spyware and anti-virus software installed on the endpoint. You will use the advanced endpoint assessment capabilities to automatically update the anti-virus and anti-spyware definitions. You will build the solution in a gradual way and observe the posture results in each phase. Although the Host Scan feature is supported for all remote access VPN types, including clientless SSL VPNs, you will deploy it only for the AnyConnect access from the Employee-PC. Posture validation is most common for controlled endpoints, and less typical for uncontrolled environments, such as Internet Kiosks.

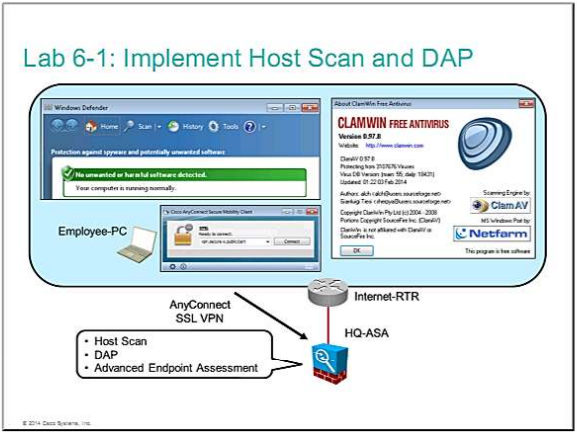
Upon completing this activity you will be able to meet these objectives:

- Deploy the ASA's Dynamic Access Policy (DAP) and evaluate endpoint attributes
- Enable the ASA's Host Scan feature
- Deploy automatic definition remediation using advanced endpoint assessment capabilities

https://t.me/learningnets

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These resources are the resources and equipment that are required to complete this activity:

Cisco ASA adaptive security appliance

Command List

No commands are needed to complete this lab exercise. All tasks are performed with the Cisco Adaptive Security Device Manager GUI interface.

Job Aids

These job aids are available to help you complete the lab activity.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

Device	Hardware	Operating System and Filenames
Partner-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Branch-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ISR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
HQ-ASA	Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module	asa911-4-smp-k8.bin IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip asa911-4-smp-k8.bin asacx-5500x-boot-9.1.1-14.img
HQ-SW	Cisco Catalyst WS-C3560X-24	c3560e-universalk9-mz.150-2.SE2.bin
Internet-RTR	Cisco 2901 ISR	c2900-universalk9-mz.SPA.153-1.T.bin
Partner-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
SP-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Branch-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
DMZ-SRV	Virtualized	Linux Ubuntu
HQ-SRV	Virtualized	Microsoft Windows Server 2008 R2 Standard
Admin PC	Virtualized	Microsoft Windows 7
Guest PC	Virtualized	Microsoft Windows 7
Employee PC	Virtualized	Microsoft Windows 7
Attacker PC	Virtualized	Linux Kali
HQ-ISE	Virtualized	Cisco ISE version 1.2
HQ-CDA	Virtualized	Cisco CDA version 1.0.0.11
HQ-ESA	Virtualized	AsyncOS version 8.0.0-550
HQ-WSA	Virtualized	AsyncOS version 7.7.5-093

The table shows the usernames and passwords that are used to access the equipment in this lab.

Device	Username	Password
HQ-ASA	**admin**	**Ci5coAdmin** Enable: **cisco**
HQ-IPS	**cisco**	**Ci5coAdmin**
Partner-SRV	**administrator**	**Ci5coAdmin**
SP-SRV	**administrator**	**Ci5coAdmin**
Branch-SRV	**administrator**	**Ci5coAdmin**
DMZ-SRV	**administrator**	**Ci5coAdmin**

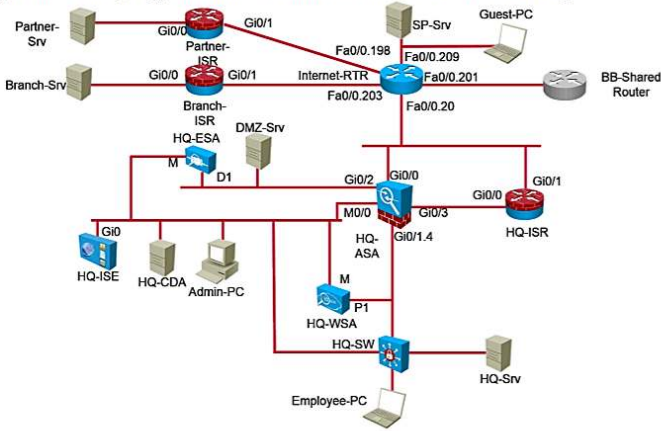
https://t.me/learningnets

Device	Username	Password
HQ-SRV	**administrator**	**Ci5coAdmin**
Admin PC	**student**	**Ci5coAdmin**
Guest PC	**student**	**Ci5coAdmin**
Employee PC	**student**	**Ci5coAdmin**
Attacker PC	**root**	**Ci5coAdmin**
HQ-ISE	**admin**	**Ci5coAdmin**
HQ-CDA	**admin**	**Ci5coAdmin**
HQ-ESA	**admin**	**Ci5coAdmin**
HQ-WSA	**admin**	**Ci5coAdmin**

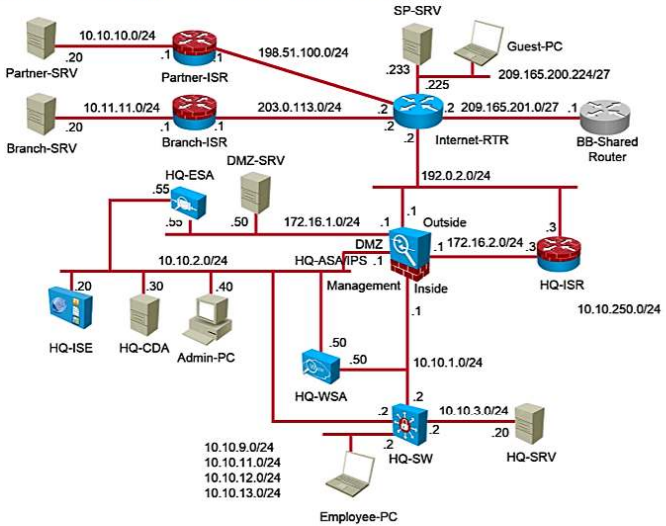
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.

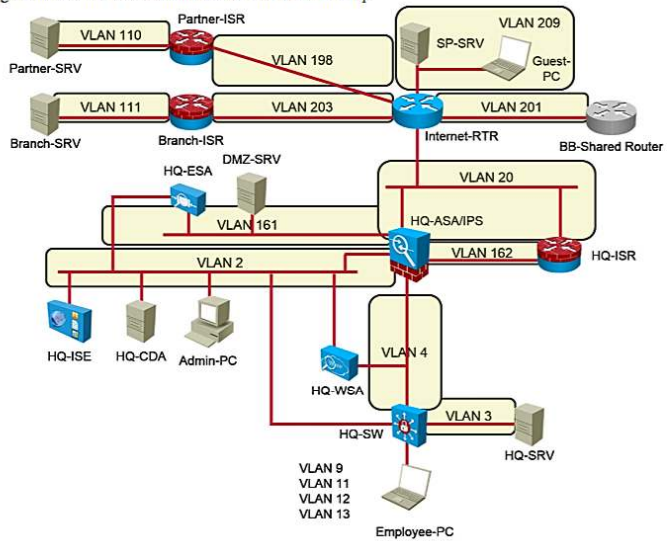


The figure shows the IP addresses that are used in this lab setup.



VLAN Setup

The figure shows the VLANs that are used in this lab setup.



Task 1: Enable Host Scan and Examine AntiSpyware Software on Employee-PC

In this task, you will enable the Host Scan feature on the ASA. You will also examine the initial security posture of the Employee-PC, before any definition remediation is performed. You will see that the Employee-PC is running an out-of-date anti-spyware software (Windows Defender).

Activity Procedure

Complete the following steps:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 1

Enable the Host Scan feature:

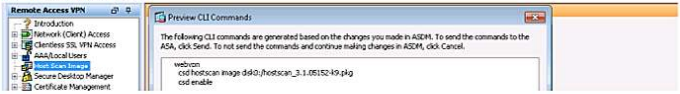
A) Access the ASDM (**admin/Ci5coAdmin**) running on the Admin-PC.

B) In the ASDM go to **Configuration > Remote Access VPN > Host Scan Image**, click **Browse Flash**.

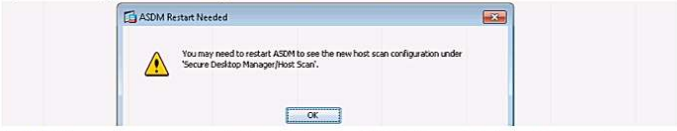
C) Select the image **hostscan_3.1.05152-k9.pkg** on **disk0**: and check the **Enable Host Scan/CSD** check box. If you cannot find the image on ASA disk0:, click **Upload**, select the file in the **D:\AnyConnect** folder, and upload it to the ASA.



D) Apply the configuration.

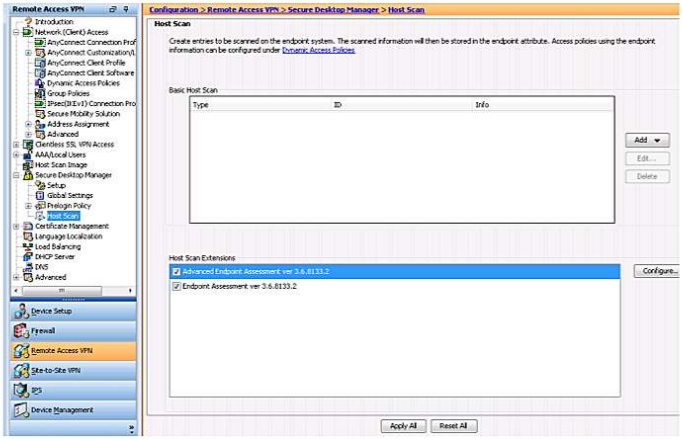


E) Accept the warning about restarting the ASDM and restart the ASDM.



F) In the ASDM, go to **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan**. Enable both extensions (**Endpoint Assessment** and **Advanced Endpoint Assessment**) and click the **Apply All** button to apply the configuration. The Endpoint Assessment needs to be enabled to scan the hosts. The Advanced Endpoint Assessment will be needed to remediate non-compliant endpoints by updating the definition databases of the anti-spyware and anti-virus products.

https://t.me/learningnets

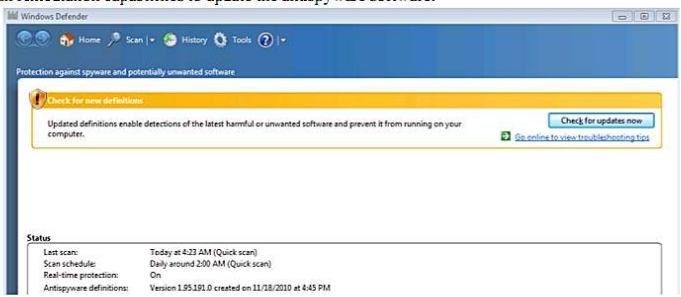


Step 2

Examine the version of the Windows Defender software initially installed on the Employee-PC:

A) Stay logged on to the Employee-PC as domain user **it1** with password **cisco**. You have previously assigned the domain users to the local administrators group. In the verification of antispyware definition remediation you may want to roll back the definition updates, which will require administrative privileges.

B) Click **Start**, and enter **defender** in the Search programs and files field. You should see that the Windows Defender software has not been updated since 2010. Do ***not*** update it. You will use the Host Scan remediation capabilities to update the antispyware software.



https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 3

On the Employee-PC, test the posture assessment initialization:

A) On the Employee-PC, connect the AnyConnect (**Start > All Programs > Cisco > Cisco AnyConnect Secure Mobility Client**) to vpn.secure-x.public. During connection establishment you will briefly see the initiation of the posture assessment.



B) Select the default connection profile (**main**). Log in as **vpnuser** with password **cisco**. Disconnect the VPN.

Task 2: Deploy DAP to Evaluate Endpoint Posture Status

In this task, you will modify the default DAP rule to terminate VPN access and create a custom DAP rule (AV/AS) that will allow access for endpoints with compliant posture status. This DAP approach resembles an ACL consisting of specific permit statements and a default deny rule at the end. When the default rule has been modified you will see that the VPN access is terminated. When the AV/AS rule has been defined, you will see that the Employee-PC can access the VPN because of the Windows Defender installation.

Activity Procedure

Complete the following steps:

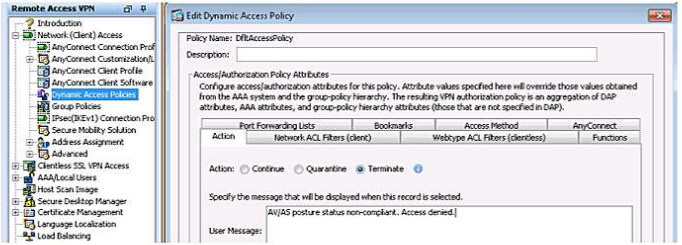
https://t.me/learningnets

Step 1

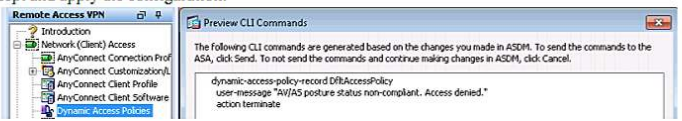
Configure the default DAP policy to terminate access. Based on this fail-close approach you will then add DAP rules to allow more access for endpoints with antivirus/antispyware software.

A) In the ASDM, go to **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies**.

B) Edit the default rule (DfltAccessPolicy). In the **Action** tab choose **Terminate**, and enter a user message such as **AV/AS posture status non-compliant. Access is denied**. Alternatively you could allow the users to connect or quarantine the VPN session with a user message, and apply an ACL to restrict their traffic.



C) Accept and apply the configuration.



Step 2

On the Employee-PC, connect the AnyConnect client to vpn.secure-x.public. Select the default connection profile (**main**). Log in as **vpnuser** with password **cisco**. The session will be terminated.

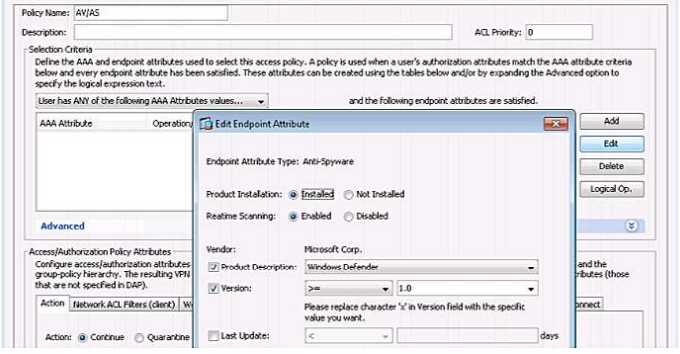


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

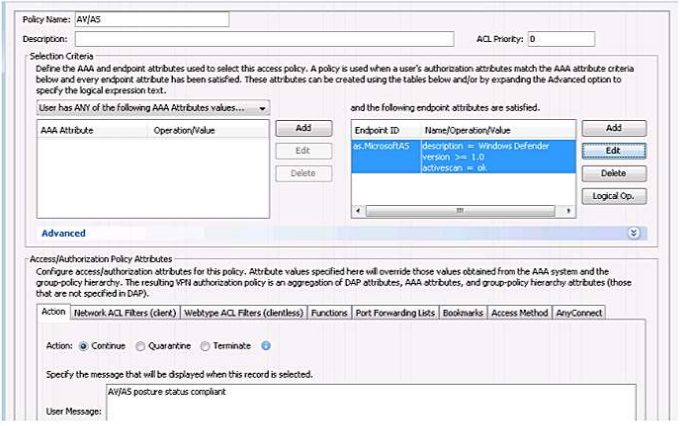
Step 3

Add a custom DAP policy (**Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies**), named **AS/AV**, with these attributes:

A) Add an endpoint attribute check in the pane on the right. Select the Windows Defender from the Microsoft Corporation with software version 1.0 or later.

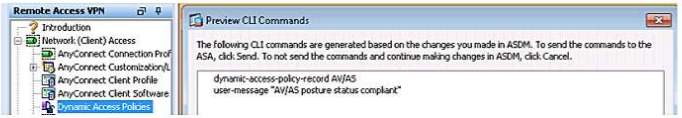


B) In the **Action** tab choose **Continue**, and enter a user message such as **AV/AS posture status compliant.**



C) Accept and apply the configuration.

https://t.me/learningnets



Step 4

Verify that the Employee-PC passes the posture compliance due to the installed AS software:

A) From the Employee-PC, reconnect the AnyConnect to vpn.secure-x.public. Select the default connection profile (**main**). Log in as **vpnuser** with password **cisco**. You should be notified that the posture status is compliant. Click **OK**.



B) Verify that you can access the internal resources, such as http://hq-srv.secure-x.local or ftp://dmz.secure-x.local. Disconnect the tunnel.

Task 3: Deploy Automatic Endpoint Remediation

In this task, you will use the ASA's Advanced Endpoint Assessment feature to automatically update the anti-spyware definition database on the Employee-PC. You will first configure the DAP to evaluate the status of the anti-spyware definitions, verify that the VPN access is denied, use the Advanced Endpoint Assessment feature to update the AS definition, and verify that the VPN access succeeds.

Activity Procedure

Complete the following steps:

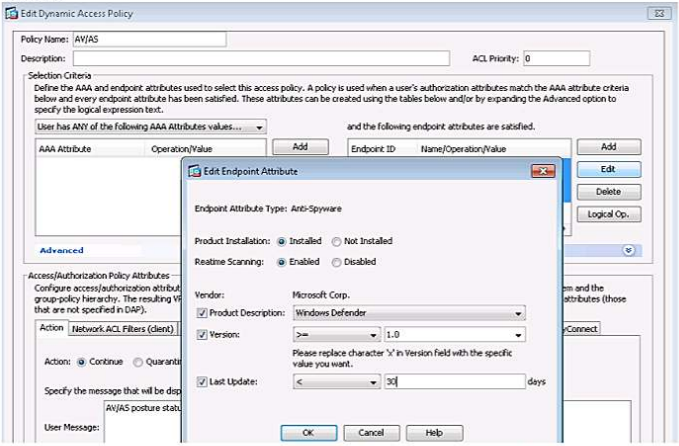
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 1

Edit the custom DAP policy (**AV/AS**), to check that the AS definition file has been updated within the last 10 days:

A) In the ASDM, go to **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies** and edit the **AV/AS** policy.

B) Edit the existing attribute definition check. Make sure that the definition files must be newer than from 30 days ago.



C) Accept and apply the configuration. Dynamic Access Policy selection file will be updated.



Step 2

Verify that the Employee-PC fails the posture compliance because of out-of-date AS software:

A) From the Employee-PC, reconnect the AnyConnect to vpn.secure-x.public. Select the default connection profile (**main**). Log in as **vpnuser** with password **cisco**.

B) You should be notified about non-compliant posture status. Click **OK** to disconnect the VPN.

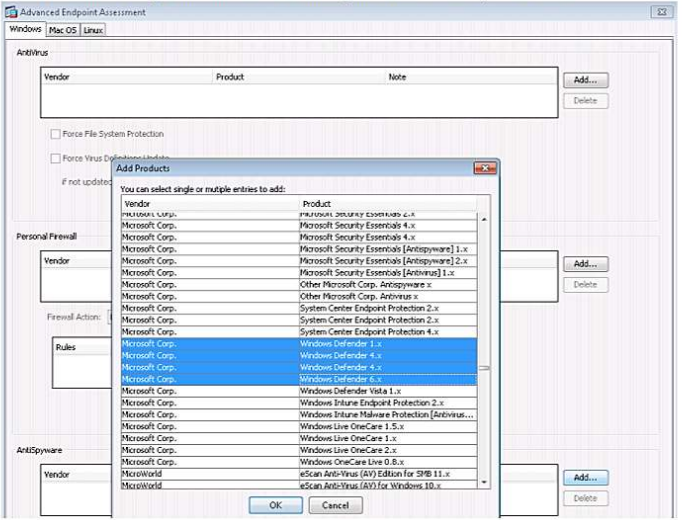
https://t.me/learningnets

Step 3

Enable automatic remediation of the anti-spyware definition files:

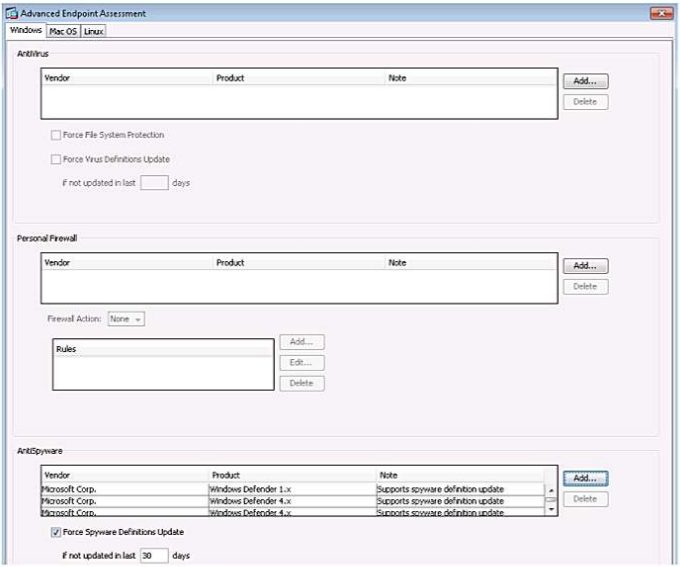
A) In the ASDM, go to **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan** and click the **Configure** button near the Host Scan extensions. If the configuration window does not open, uncheck both extensions, apply the configuration, check the extensions again, and then click the **Configure** button.

B) In the Windows tab, add a rule for AntiSpyware software. Select all four rules by Microsoft Corp., for Windows Defender, except for Windows Vista, using the Shift or Ctrl key. Click **OK**.



C) Force spyware definitions update if not updated within the last 30 days.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



D) Accept and apply the configuration.

https://t.me/learningnets

Step 4

Verify the automated AS definition remediation on the Employee-PC:

A) From the Employee-PC, reconnect the AnyConnect to vpn.secure-x.public. Select the default connection profile (**main**). Log in as **vpnuser** with password **cisco**.

B) The connection process may take up to 3 minutes longer because the Windows Defender definitions should be now automatically updated. The AnyConnect client will report posture compliance. Click **OK**.



C) On the Employee-PC, click **Start**, enter **defender** in the **Search** field, click **Enter**, and verify that the **Windows Defender** has been updated.

Note If you need to roll back the installation of the Windows Defender update, choose **Start > All Programs > Accessories**, right-click the **Command Prompt** and choose **Run as Administrator** to start an elevated command prompt. In the command prompt, run the **"C:\Program Files\Windows Defender\MpCmdRun.exe" -RemoveDefinitions** command.

Task 4: Deploy AntiVirus Posture (Optional)

In this task, you will install the ClamWin Free Antivirus software on the Employee-PC, and configure the DAP to check the status of the AV definition file. First the VPN access will be denied because the AV software will not use the latest virus definitions. When you use the Advanced Endpoint Assessment to automatically update the virus definitions, the VPN access will granted as a result of the compliant posture status.

Activity Procedure

Complete the following steps:

Step 1

On the Employee-PC, install the ClamWin Antivirus but ***do not*** update the definition files:

A) Install the ClamWin Free Antivirus using the **D:\Install\clamwin-0.97.8-setup.exe** file.

B) Follow the installation wizard using default options: accept license agreement, install for anyone who uses the computer.

C) Use the default installation path, enable the integration options with Microsoft Outlook Express and Internet Explorer, click **Next**.

D) ***Do not*** Download Virus Database Files, click **Install**, and then **Finish**.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

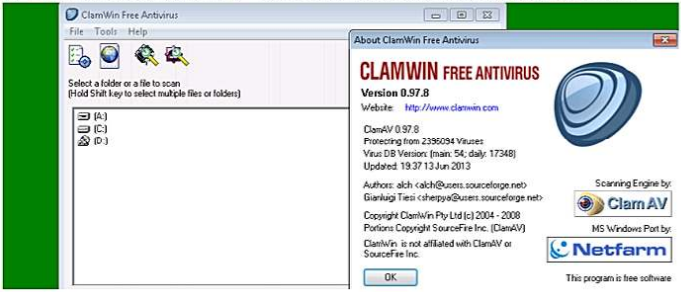
Step 2

Verify that ClamWin Free Antivirus is out-of-date:

A) On the Employee-PC, go to **Start > All Programs > ClamWin Antivirus > Virus Scanner**. You will get a notification that the signature definition file is older than 5 days. Click **No** to prevent an update at this point.



B) In the Virus Scanner GUI select **Help > About**. You will see that the last update was in 2013.



https://t.me/learningnets

Step 3

Modify the custom DAP policy (AV/AS) to check for up-to-date ClamWin AV software. In the ASDM, go to **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies** and edit your custom policy (**AV/AS**). Add an additional endpoint attribute with these parameters:

A) Endpoint attribute type: **Anti-Virus**

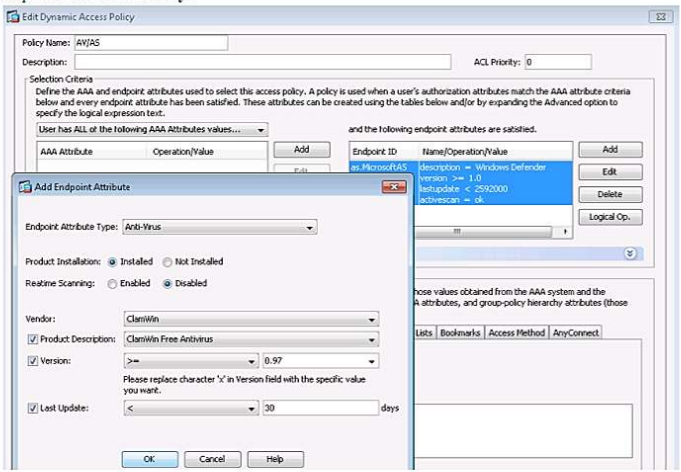
B) Realtime Scanning: **Disabled**. ClamWin Free Antivirus does not support realitime scanning.

C) Vendor: **ClamWin**

D) Product: **ClamWin Free Antivirus**

E) Version: **equal or newer than 0.97**

F) Last update: **less than 30 days**



G) Accept and apply the configuration.

Step 4

Verify that the VPN connection fails due to out-of-date anti-virus software. From the Employee-PC, reconnect to the VPN. The connection will fail.



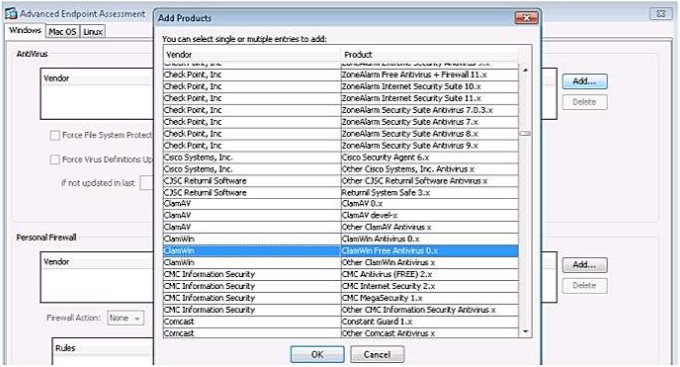
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 5

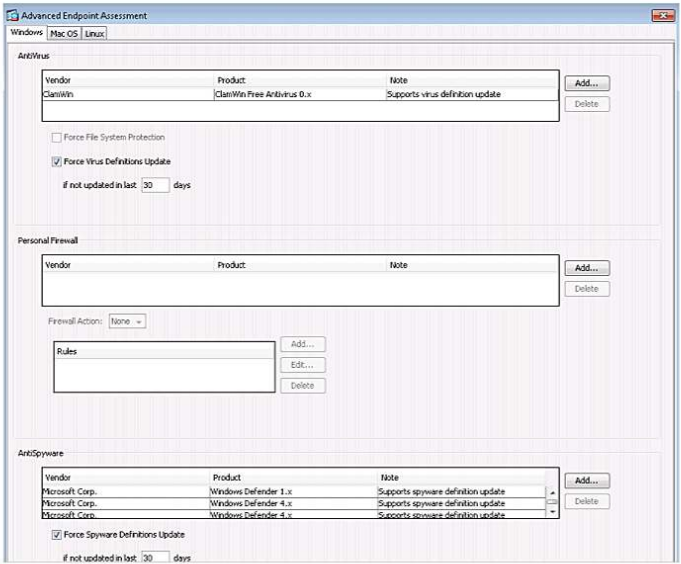
Enable automatic remediation of the anti-virus definition files:

A) In the ASDM, go to **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan** and click the **Configure** button near the Host Scan extensions. If the configuration window does not open, uncheck both extensions, apply the configuration, check the extensions again, and then click the **Configure** button.

B) In the Windows tab, add a rule for AntiVirus software. Select **ClamWin/ ClamWin Free Antivirus 0.x** and click **OK**.



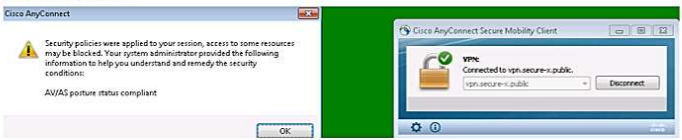
C) Force Virus definitions update if not updated within the last 30 days.



D) Accept and apply the configuration.

Step 6

Verify that the VPN tunnel can be successfully established. Select the **main** alias, log in as **vpnuser** with password **cisco.** The process of downloading the virus definitions the will take up to 5 minutes. The connection will succeed.



https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 7

Verify that ClamWin Free Antivrus has been updated:

A) On the Employee-PC, go to **Start > All Programs > ClamWin Antivirus > Virus Scanner**.

B) In the Virus Scanner GUI select **Help > About**. You will see that the software uses a current definition file instead of the previous file from 2013.

Note	Other Cisco solutions, such as the Cisco Identity Services Engine provide richer remediation capabilities. The ISE, for example, could automatically install and update anti-virus and anti-malware software.

https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab Answer Keys

Lab 2-1: Implement Site-to-Site Secure Connectivity on the Cisco ASA

Task 1: Configuring the Cisco ASA for Site-to-Site VPN

Step 1

There are no solutions for this lab.

Lab 2-2: Implement Cisco IOS Static VTI Point-to-Point Tunnel

Task 1: Configure Static VTI Point-to-Point Tunnel

Step 1

Enter these commands to the HQ-ISR router:

```
HQ-ISR(config)# crypto isakmp policy 10
HQ-ISR(config-isakmp)# authentication pre-share
HQ-ISR(config-isakmp)# hash sha
HQ-ISR(config-isakmp)# encr aes 128
HQ-ISR(config-isakmp)# group 14
HQ-ISR(config-isakmp)# lifetime 3600
```

Step 2

Enter this command on the HQ-ISR router:

https://t.me/learningnets

```
HQ-ISR(config)# crypto isakmp key cisco address 198.51.100.1
```

Step 3

Enter this command on the HQ-ISR router:

```
HQ-ISR(config)# crypto ipsec transform-set MYSET esp-aes 128 esp-sha-hmac
```

Step 4

Enter these commands to the HQ-ISR router:

```
HQ-ISR(config)# crypto ipsec profile MYPROFILE
HQ-ISR(ipsec-profile)# set transform-set MYSET
```

Step 5

Enter these commands on the HQ-ISR router:

```
HQ-ISR(config)# interface Tunnel0
HQ-ISR(config-if)# ip unnumbered GigabitEthernet0/1
HQ-ISR(config-if)# tunnel source GigabitEthernet0/1
HQ-ISR(config-if)# tunnel destination 198.51.100.1
```

Step 6

Enter these commands on the HQ-ISR router:

```
HQ-ISR(config)# interface Tunnel0
HQ-ISR(config-if)# tunnel mode ipsec ipv4
HQ-ISR(config-if)# tunnel protection ipsec profile MYPROFILE
```

Step 7

Enter this commands on the HQ-ISR router:

```
HQ-ISR(config)# ip route 10.10.10.0 255.255.255.0 Tunnel0
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 2-3: Implement DMVPN

Task 1: Configure a DMVPN Hub

Step 1

Enter these commands to the HQ-ISR router:

```
HQ-ISR(config)# crypto isakmp policy 10
HQ-ISR(config-isakmp)# encr aes 256
HQ-ISR(config-isakmp)# hash sha384
HQ-ISR(config-isakmp)# authentication pre-share
HQ-ISR(config-isakmp)# group 14
```

Step 2

Enter this command on the HQ-ISR router:

```
HQ-ISR(config)# no crypto isakmp key cisco address 198.51.100.1
```

Step 3

Enter these commands on the HQ-ISR router:

```
HQ-ISR(config)# crypto isakmp key ccnpsecDMVPN address 203.0.113.1
HQ-ISR(config)# crypto isakmp key ccnpsecDMVPN address 198.51.100.1
```

Step 4

Enter this command on the HQ-ISR router:

```
HQ-ISR(config)# crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
HQ-ISR(cfg-crypto-trans)# mode transport
HQ-ISR(cfg-crypto-trans)# exit
HQ-ISR(config)# crypto ipsec profile MYIPSECPROFILE
HQ-ISR(ipsec-profile)# set transform-set MYSET
```

Step 5

Enter these commands on the HQ-ISR router:

```
HQ-ISR(config)# interface Tunnel1
HQ-ISR(config-if)# tunnel mode gre multipoint
HQ-ISR(config-if)# tunnel source GigabitEthernet0/1
HQ-ISR(config-if)# tunnel key 12345
```


https://t.me/learningnets

Step 6

Enter these commands on the HQ-ISR router:

```
HQ-ISR(config)# interface Tunnel1
HQ-ISR(config-if)# ip nhrp network-id 1
HQ-ISR(config-if)# ip nhrp authentication NHRP
HQ-ISR(config-if)# ip nhrp map multicast dynamic
```

Step 7

Enter these commands on the HQ-ISR router:

```
HQ-ISR(config)# interface Tunnel1
HQ-ISR(config-if)# tunnel protection ipsec profile MYIPSECPROFILE
```

Step 8

Enter these commands on the HQ-ISR router:

```
HQ-ISR(config)# interface Tunnel1
HQ-ISR(config-if)# ip address 10.1.1.1 255.255.255.0
```

Step 9

Enter these commands on the HQ-ISR router:

```
HQ-ISR(config)# interface Tunnel1
HQ-ISR(config-if)# ip mtu 1400
HQ-ISR(config-if)# ip tcp adjust-mss 1360
```

Step 10

Enter these commands on the HQ-ISR router:

```
HQ-ISR(config)# no interface Tunnel0
```

Task 2: Configure a DMVPN Spokes

Step 1

Enter these commands to the **Branch-ISR** router:

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

```
Branch-ISR(config)# crypto isakmp policy 10
Branch-ISR(config-isakmp)# encr aes 256
Branch-ISR(config-isakmp)# hash sha384
Branch-ISR(config-isakmp)# authentication pre-share
Branch-ISR(config-isakmp)# group 14
```

Enter these commands to the **Partner-ISR** router:

```
Partner-ISR(config)# crypto isakmp policy 10
Partner-ISR(config-isakmp)# encr aes 256
Partner-ISR(config-isakmp)# hash sha384
Partner-ISR(config-isakmp)# authentication pre-share
Partner-ISR(config-isakmp)# group 14
```

Step 2

Enter this command on the Branch-ISR router:

```
Branch-ISR(config)# crypto isakmp key ccnpsecDMVPN address 192.0.2.3
```

Step 3

Enter this command on the Partner-ISR router:

```
Partner-ISR(config)# no crypto isakmp key cisco address 192.0.2.3
```

Step 4

Enter this command on the Partner-ISR router:

```
Partner-ISR(config)# crypto isakmp key ccnpsecDMVPN address 192.0.2.3
```

Step 5

Enter these commands on the Branch-ISR router:

```
Branch-ISR(config)# crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
Branch-ISR(cfg-crypto-trans)# mode transport
Branch-ISR(cfg-crypto-trans)# exit
Branch-ISR(config)# crypto ipsec profile MYIPSECPROFILE
Branch-ISR(ipsec-profile)# set transform-set MYSET
```

Enter these commands on the Partner-ISR router:

https://t.me/learningnets

```
Partner-ISR(config)# crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
Partner-ISR(cfg-crypto-trans)# mode transport
Partner-ISR(cfg-crypto-trans)# exit
Partner-ISR(config)# crypto ipsec profile MYIPSECPROFILE
Partner-ISR(ipsec-profile)# set transform-set MYSET
```

Step 6

Enter these commands on the Branch-ISR router:

```
Branch-ISR(config)# interface Tunnel1
Branch-ISR(config-if)# tunnel mode gre multipoint
Branch-ISR(config-if)# tunnel source GigabitEthernet0/1
Branch-ISR(config-if)# tunnel key 12345
```

Enter these commands on the Partner-ISR router:

```
Partner-ISR(config)# interface Tunnel1
Partner-ISR(config-if)# tunnel mode gre multipoint
Partner-ISR(config-if)# tunnel source GigabitEthernet0/1
Partner-ISR(config-if)# tunnel key 12345
```

Step 7

Enter these commands on the Branch-ISR router:

```
Branch-ISR(config)# interface Tunnel1
Branch-ISR(config-if)# ip nhrp network-id 1
Branch-ISR(config-if)# ip nhrp authentication NHRP
Branch-ISR(config-if)# ip nhrp nhs 10.1.1.1
Branch-ISR(config-if)# ip nhrp map multicast 192.0.2.3
Branch-ISR(config-if)# ip nhrp map 10.1.1.1 192.0.2.3
```

Enter these commands on the Partner-ISR router:

```
Partner-ISR(config)# interface Tunnel1
Partner-ISR(config-if)# ip nhrp network-id 1
Partner-ISR(config-if)# ip nhrp authentication NHRP
Partner-ISR(config-if)# ip nhrp nhs 10.1.1.1
Partner-ISR(config-if)# ip nhrp map multicast 192.0.2.3
Partner-ISR(config-if)# ip nhrp map 10.1.1.1 192.0.2.3
```

Step 8

Enter these commands on the Branch-ISR router:

```
Branch-ISR(config)# interface Tunnel1
Branch-ISR(config-if)# tunnel protection ipsec profile MYIPSECPROFILE
```

Enter these commands on the Partner-ISR router:

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

```
Partner-ISR(config)# interface Tunnel1
Partner-ISR(config-if)# tunnel protection ipsec profile MYIPSECPROFILE
```

Step 9

Enter these commands on the Branch-ISR router:

```
Branch-ISR(config)# interface Tunnel1
Branch-ISR(config-if)# ip address 10.1.1.2 255.255.255.0
```

Enter these commands on the Partner-ISR router:

```
Partner-ISR(config)# interface Tunnel1
Partner-ISR(config-if)# ip address 10.1.1.3 255.255.255.0
```

Step 10

Enter these commands on the Branch-ISR router:

```
Branch-ISR(config)# interface Tunnel1
Branch-ISR(config-if)# ip mtu 1400
Branch-ISR(config-if)# ip tcp adjust-mss 1360
```

Enter these commands on the Partner-ISR router:

```
Partner-ISR(config)# interface Tunnel1
Partner-ISR(config-if)# ip mtu 1400
Partner-ISR(config-if)# ip tcp adjust-mss 1360
```

Step 11

Enter these commands on the Branch-ISR router:

```
Branch-ISR(config)# interface GigabitEthernet0/1
Branch-ISR(config-if)# no crypto map VPN-to-ASA
```

Step 12

Enter this command on the Partner-ISR router:

```
Partner-ISR(config)# no interface Tunnel0
```


https://t.me/learningnets

Task 3: Configure OSPF Routing in DMVPN

Step 1

Enter these commands to the **HQ-ISR** router:

```
HQ-ISR(config)# interface Tunnel1
HQ-ISR(config-if)# ip ospf network point-to-multipoint
```

Step 2

Enter these commands to the **HQ-ISR** router:

```
HQ-ISR(config)# router ospf 1
HQ-ISR(config-router)# network 10.1.1.0 0.0.0.255 area 0
```

Step 3

Enter these commands to the **Branch-ISR** router:

```
Branch-ISR(config)# interface Tunnel1
Branch-ISR(config-if)# ip ospf network point-to-multipoint
```

Enter these commands to the **Partner-ISR** router:

```
Partner-ISR(config)# interface Tunnel1
Partner-ISR(config-if)# ip ospf network point-to-multipoint
```

Step 4

Enter these commands to the **Branch-ISR** router:

```
Branch-ISR(config)# router ospf 1
Branch-ISR(config-router)# network 10.1.1.0 0.0.0.255 area 0
```

Enter these commands to the **Partner-ISR** router:

```
Partner-ISR(config)# router ospf 1
Partner-ISR(config-router)# network 10.1.1.0 0.0.0.255 area 0
```

Step 5

Enter these commands to the **Partner-ISR** router:

```
Partner-ISR(config)# router ospf 1
Partner-ISR(config-router)# network 10.10.10.0 0.0.0.255 area 2
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Task 5: Configure a DMVPN Spoke to Spoke Communication

Step 1

Enter this command on the Branch-ISR router:

```
Branch-ISR(config)# crypto isakmp key ccnpsecDMVPN address 198.51.100.1
```

Step 2

Enter this command on the Partner-ISR router:

```
Partner-ISR(config)# crypto isakmp key ccnpsecDMVPN address 203.0.113.1
```

Step 3

Enter these commands to the HQ-ISR router:

```
HQ-ISR(config)# interface Tunnel1
HQ-ISR(config-if)# ip ospf network broadcast
```

Enter these commands to the Branch-ISR router:

```
Branch-ISR(config)# interface Tunnel1
Branch-ISR(config-if)# ip ospf network broadcast
Branch-ISR(config-if)# ip ospf priority 0
```

Enter these commands to the Partner-ISR router:

```
Partner-ISR(config)# interface Tunnel1
Partner-ISR(config-if)# ip ospf network broadcast
Partner-ISR(config-if)# ip ospf priority 0
```

Lab 3-1: Implement Site-to-Site Secure Connectivity Using Cisco IOS FlexVPN

Task 1: Implement Point-to-Point FlexVPN Using Smart Defaults And Minimal Configuration

Step 1

To configure the key ring, enter the following commands on the Branch-ISR:

```
Branch-ISR(config)# crypto ikev2 keyring KR
Branch-ISR(config-ikev2-keyring)# peer HQ-ISR
Branch-ISR(config-ikev2-keyring-peer)# address 192.0.2.3
Branch-ISR(config-ikev2-keyring-peer)# pre-shared-key local cisco
Branch-ISR(config-ikev2-keyring-peer)# pre-shared-key remote cisco
```

Step 2

To configure the key ring, enter the following commands on the HQ-ISR:

```
HQ-ISR(config)# crypto ikev2 keyring KR
HQ-ISR(config-ikev2-keyring)# peer Branch-ISR
HQ-ISR(config-ikev2-keyring-peer)#  address 203.0.113.1
HQ-ISR(config-ikev2-keyring-peer)#  pre-shared-key local cisco
HQ-ISR(config-ikev2-keyring-peer)#  pre-shared-key remote cisco
```

Step 3

To modify the smart default of the IKEv2 profile, enter the following commands on the Branch-ISR:

```
Branch-ISR(config)# crypto ikev2 profile default
IKEv2 profile MUST have:
   1. A local and a remote authentication method.
   2. A match identity or a match certificate statement.
Branch-ISR(config-ikev2-profile)# match identity remote fqdn hq-isr.secure-x.public
Branch-ISR(config-ikev2-profile)# identity local fqdn branch-isr.secure-x.public
Branch-ISR(config-ikev2-profile)# authentication local pre-share
Branch-ISR(config-ikev2-profile)# authentication remote pre-share
Branch-ISR(config-ikev2-profile)# keyring local KR
```

Step 4

To modify the smart default of the IKEv2 profile, enter the following commands on the HQ-ISR:

```
HQ-ISR(config)# crypto ikev2 profile default
IKEv2 profile MUST have:
   1. A local and a remote authentication method.
   2. A match identity or a match certificate statement.
HQ-ISR(config-ikev2-profile)# match identity remote fqdn branch-isr.secure-x.public
HQ-ISR(config-ikev2-profile)# identity local fqdn hq-isr.secure-x.public
HQ-ISR(config-ikev2-profile)# authentication local pre-share
HQ-ISR(config-ikev2-profile)# authentication remote pre-share
HQ-ISR(config-ikev2-profile)# keyring local KR
```

Step 5

Enter the following command on the Branch-ISR:

```
Branch-ISR(config)# no interface Tunnel1
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Enter the following command on the HQ-ISR:

```
HQ-ISR(config)# no interface Tunnel1
```

Step 6

Enter the following commands on the Branch-ISR:

```
Branch-ISR(config)# interface Tunnel0
Branch-ISR(config-if)# ip address 10.10.100.1 255.255.255.0
Branch-ISR(config-if)# tunnel source 203.0.113.1
Branch-ISR(config-if)# tunnel mode ipsec ipv4
Branch-ISR(config-if)# tunnel destination 192.0.2.3
```

Enter the following commands on the HQ-ISR:

```
HQ-ISR(config)# interface Tunnel0
HQ-ISR(config-if)# ip address 10.10.100.2 255.255.255.0
HQ-ISR(config-if)# tunnel source 192.0.2.3
HQ-ISR(config-if)# tunnel mode ipsec ipv4
HQ-ISR(config-if)# tunnel destination 203.0.113.1
```

Step 7

To configure the Tunnel 0 interface to use the default IPsec profile, enter the following commands on the Branch-ISR:

```
Branch-ISR(config)# interface Tunnel0
Branch-ISR(config-if)# tunnel protection ipsec profile default
```

To configure the Tunnel 0 interface to use the default IPsec profile, enter the following commands on the HQ-ISR:

```
HQ-ISR(config)# interface Tunnel0
HQ-ISR(config-if)# tunnel protection ipsec profile default
```

Step 8

To configure the Tunnel 0 interface into OSPF area 0, enter the following commands on the Branch-ISR:

```
Branch-ISR(config)# router ospf 1
Branch-ISR(config-router)# network 10.10.100.0 0.0.0.255 area 0
```

To configure the Tunnel 0 interface into OSPF area 0, enter the following commands on the HQ-ISR:

```
HQ-ISR(config)# router ospf 1
HQ-ISR(config-router)# network 10.10.100.0 0.0.0.255 area 0
```


https://t.me/learningnets

Step 9

To delete the unused crypto constructs, enter the following commands on the Branch-ISR:

```
Branch-ISR(config)# no crypto ipsec profile MYIPSECPROFILE
Branch-ISR(config)# no crypto isakmp policy 1
Branch-ISR(config)# no crypto isakmp policy 10
Branch-ISR(config)# no crypto isakmp key cisco address 192.0.2.1
Branch-ISR(config)# no crypto isakmp key ccnpsecDMVPN address 192.0.2.3
Branch-ISR(config)# no crypto isakmp key ccnpsecDMVPN address 198.51.100.1
Branch-ISR(config)# no crypto map VPN-to-ASA 10 ipsec-isakmp
Branch-ISR(config)# no crypto ipsec transform-set TSET
Branch-ISR(config)# no crypto ipsec transform-set MYSET
```

To delete the unused crypto constructs, enter the following commands on the HQ-ISR:

```
HQ-ISR(config)# no crypto ipsec profile MYIPSECPROFILE
HQ-ISR(config)# no crypto ipsec profile MYPROFILE
HQ-ISR(config)# no crypto isakmp policy 10
HQ-ISR(config)# no crypto isakmp key ccnpsecDMVPN address 203.0.113.1
HQ-ISR(config)# no crypto isakmp key ccnpsecDMVPN address 198.51.100.1
HQ-ISR(config)# no crypto ipsec transform-set MYSET
```

Task 2: Modify Smart Defaults to Increase Protection Strength

Step 1

To modify the IKEv2 proposal, enter the following commands on the Branch-ISR:

```
Branch-ISR(config)# crypto ikev2 proposal default
%Warning: This will Modify Default IKEv2 Proposal. Exit if you don't want
Branch-ISR(config-ikev2-proposal)# encryption aes-cbc-256
Branch-ISR(config-ikev2-proposal)# integrity sha512
Branch-ISR(config-ikev2-proposal)# group 20
```

To modify the IKEv2 proposal, enter the following commands on the HQ-ISR:

```
HQ-ISR(config)# crypto ikev2 proposal default
%Warning: This will Modify Default IKEv2 Proposal. Exit if you don't want
HQ-ISR(config-ikev2-proposal)# encryption aes-cbc-256
HQ-ISR(config-ikev2-proposal)# integrity sha512
HQ-ISR(config-ikev2-proposal)# group 20
```

Step 2

To modify the default IPsec transform set, enter the following command on the Branch-ISR:

```
Branch-ISR(config)# crypto ipsec transform-set default esp-gcm 256
%Warning: Default transform set has been modified.
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

To modify the default IPsec transform set, enter the following command on the HQ-ISR:

```
HQ-ISR(config)# crypto ipsec transform-set default esp-gcm 256
%Warning: Default transform set has been modified.
```

Step 3

To modify the default IPsec profile, enter the following commands on the Branch-ISR:

```
Branch-ISR(config)# crypto ipsec profile default
%Warning: This will Modify Default IPSec Profile.Exit if you don't want
Branch-ISR(ipsec-profile)# set pfs group20
```

To modify the default IPsec profile, enter the following commands on the HQ-ISR:

```
HQ-ISR(config)# crypto ipsec profile default
%Warning: This will Modify Default IPSec Profile.Exit if you don't want
HQ-ISR(ipsec-profile)# set pfs group20
```

Task 3: Implement Point-to-Point FlexVPN Without Smart Defaults

Step 1

To create the IKEv2 profile, enter the following commands on the Branch-ISR:

```
Branch-ISR(config)# crypto ikev2 profile ccnp-ikev2-profile
Branch-ISR(config-ikev2-profile)# match identity remote fqdn hq-isr.secure-x.public
Branch-ISR(config-ikev2-profile)# identity local fqdn branch-isr.secure-x.public
Branch-ISR(config-ikev2-profile)# authentication local pre-share
Branch-ISR(config-ikev2-profile)# authentication remote pre-share
Branch-ISR(config-ikev2-profile)# keyring local KR
```

Step 2

To create an IKEv2 profile, enter the following commands on the HQ-ISR:

```
HQ-ISR(config)# crypto ikev2 profile ccnp-ikev2-profile
HQ-ISR(config-ikev2-profile)# match identity remote fqdn branch-isr.secure-x.public
HQ-ISR(config-ikev2-profile)# identity local fqdn hq-isr.secure-x.public
HQ-ISR(config-ikev2-profile)# authentication local pre-share
HQ-ISR(config-ikev2-profile)# authentication remote pre-share
HQ-ISR(config-ikev2-profile)# keyring local KR
```

Step 3

To configure an IKEv2 proposal, enter the following commands on the Branch-ISR:

```
Branch-ISR(config)# crypto ikev2 proposal ccnp-ike2-proposal
Branch-ISR(config-ikev2-proposal)# encryption aes-cbc-256
Branch-ISR(config-ikev2-proposal)# integrity sha512
Branch-ISR(config-ikev2-proposal)# group 20
```

To configure an IKEv2 proposal, enter the following commands on the HQ-ISR:

```
HQ-ISR(config)# crypto ikev2 proposal ccnp-ike2-proposal
HQ-ISR(config-ikev2-proposal)# encryption aes-cbc-256
HQ-ISR(config-ikev2-proposal)# integrity sha512
HQ-ISR(config-ikev2-proposal)# group 20
```

Step 4

To configure an IKEv2 policy, enter the following commands on the Branch-ISR:

```
Branch-ISR(config)# crypto ikev2 policy ccnp-ikev2-policy
Branch-ISR(config-ikev2-policy)# proposal ccnp-ike2-proposal
Branch-ISR(config-ikev2-policy)# match fvrf any
```

To configure an IKEv2 policy, enter the following commands on the HQ-ISR:

```
HQ-ISR(config)# crypto ikev2 policy ccnp-ikev2-policy
HQ-ISR(config-ikev2-policy)# proposal ccnp-ike2-proposal
HQ-ISR(config-ikev2-policy)# match fvrf any
```

Step 5

To configure the transform set, enter the following command on the Branch-ISR:

```
Branch-ISR(config)# crypto ipsec transform-set ccnp-ts esp-gcm 256
```

To configure the transform set, enter the following command on the HQ-ISR:

```
HQ-ISR(config)# crypto ipsec transform-set ccnp-ts esp-gcm 256
```

Step 6

To configure the IPsec profile, enter the following commands on the Branch-ISR:

```
Branch-ISR(config)# crypto ipsec profile ccnp-ipsec-profile
Branch-ISR(ipsec-profile)# set pfs group20
Branch-ISR(ipsec-profile)# set transform-set ccnp-ts
Branch-ISR(ipsec-profile)# set ikev2-profile ccnp-ikev2-profile
```

To configure the IPsec profile, enter the following commands on the HQ-ISR:

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

```
HQ-ISR(config)# crypto ipsec profile ccnp-ipsec-profile
HQ-ISR(ipsec-profile)# set pfs group20
HQ-ISR(ipsec-profile)# set transform-set ccnp-ts
HQ-ISR(ipsec-profile)# set ikev2-profile ccnp-ikev2-profile
```

Step 7

To apply the IPsec profile, enter the following commands on the Branch-ISR:

```
Branch-ISR(config)# interface Tunnel 0
Branch-ISR(config-if)# tunnel protection ipsec profile ccnp-ipsec-profile
```

To apply the IPsec profile, enter the following commands on the HQ-ISR:

```
HQ-ISR(config)# interface Tunnel 0
HQ-ISR(config-if)# tunnel protection ipsec profile ccnp-ipsec-profile
```

Step 8

To delete the smart defaults, enter the following commands on the Branch-ISR:

```
Branch-ISR(config)# no crypto ipsec profile default
Branch-ISR(config)# no crypto ipsec transform-set default
Branch-ISR(config)# no crypto ikev2 policy default
Branch-ISR(config)# no crypto ikev2 proposal default
Branch-ISR(config)# no crypto ikev2 profile default
```

To delete the smart defaults, enter the following commands on the HQ-ISR:

```
HQ-ISR(config)# no crypto ipsec profile default
HQ-ISR(config)# no crypto ipsec transform-set default
HQ-ISR(config)# no crypto ikev2 policy default
HQ-ISR(config)# no crypto ikev2 proposal default
HQ-ISR(config)# no crypto ikev2 profile default
```

Task 4: Prepare PKI

Step 2

On Partner-ISR, enter the following commands to start a CA on Partner-ISR.

https://t.me/learningnets

```
Partner-ISR(config)# crypto key generate rsa modulus 2048 label partner-
ca.partner.public
% You already have RSA keys defined named partner-ca.partner.public.
% They will be replaced.
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 24 seconds)
Partner-ISR(config)# ip http server
Partner-ISR(config)# crypto pki trustpoint local-ca
Partner-ISR(ca-trustpoint)# rsakeypair partner-ca.partner.public
Partner-ISR(ca-trustpoint)# revocation-check none
Partner-ISR(ca-trustpoint)# exit
Partner-ISR(config)# crypto pki server Partner-CA
Partner-ISR(cs-server)# issuer-name CN=Partner-CA, O=partner.public
Partner-ISR(cs-server)# hash sha256
Partner-ISR(cs-server)# grant auto
Dec  6 08:59:37.326: %PKI-6-CS_GRANT_AUTO: All enrollment requests will be
automatically granted.
Partner-ISR(cs-server)# no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password: cisco123
Re-enter password: cisco123
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)
% Exporting Certificate Server signing certificate and keys...
% Certificate Server enabled.
```

Step 3

On Branch-ISR, enter the following commands to configure a PKI trustpoint (Partner-ISR) and obtain the CA root certificate from the Partner-ISR CA:

```
Branch-ISR(config)# crypto pki trustpoint partner-isr
Branch-ISR(ca-trustpoint)# enrollment url http://198.51.100.1
Branch-ISR(ca-trustpoint)# revocation-check none
Branch-ISR(ca-trustpoint)# exit
Branch-ISR(config)# crypto pki authenticate partner-isr
Certificate has the following attributes:
       Fingerprint MD5: 11AA7A03 60AF3688 169A1487 BD8C7E0D
     Fingerprint SHA1: 9BB21476 165D5C39 4E7DC4CA F234C939 C9807724
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

Step 4

On the HQ-ISR, enter the following commands to enroll the HQ-ISR with the CA running on Partner-ISR:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

```
HQ-ISR(config)# crypto key generate rsa modulus 2048 label hq-isr.secure-x.public
% You already have RSA keys defined named hq-isr.secure-x.public.
% They will be replaced.
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 19 seconds)
HQ-ISR(config)# crypto pki trustpoint partner-isr
HQ-ISR(ca-trustpoint)# rsakeypair hq-isr.secure-x.public
HQ-ISR(ca-trustpoint)# enrollment url http://198.51.100.1
HQ-ISR(ca-trustpoint)# fqdn hq-isr.secure-x.public
HQ-ISR(ca-trustpoint)# subject-name CN=hq-isr,O=secure-x.public
HQ-ISR(ca-trustpoint)# revocation-check none
HQ-ISR(ca-trustpoint)# serial-number none
HQ-ISR(ca-trustpoint)# ip-address none
HQ-ISR(ca-trustpoint)# exit
HQ-ISR(config)# crypto pki authenticate partner-isr
Certificate has the following attributes:
       Fingerprint MD5: 11AA7A03 60AF3688 169A1487 BD8C7E0D
      Fingerprint SHA1: 9BB21476 165D5C39 4E7DC4CA F234C939 C9807724
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
Dec  6 09:06:50.015: %CRYPTO-6-IKMP_POLICY_DEFAULT: Using ISAKMP Default policies
HQ-ISR(config)# crypto pki enroll partner-isr
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password: cisco
Re-enter password: cisco
% The subject name in the certificate will include: CN=hq-isr,O=secure-x.public
% The subject name in the certificate will include: hq-isr.secure-x.public
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose partner-isr' commandwill show the
fingerprint.
Dec  6 09:07:22.427: CRYPTO_PKI:  Certificate Request Fingerprint MD5: 826BD9D8
37E359AA 020B5676 4D0FF116
Dec  6 09:07:22.427: CRYPTO_PKI:  Certificate Request Fingerprint SHA1: 72725A1D
72886F8B 39907D2B ED04E359 69EB23B2
Dec  6 09:07:26.055: %PKI-6-CERTRET: Certificate received from Certificate Authority
```

Task 5: Configure One Side for Certificate-Based Authentication

Step 1

On Branch-ISR, modify the key ring and IKEv2 profile to obtain this configuration:

```
Branch-ISR(config)# crypto ikev2 keyring KR
Branch-ISR(config-ikev2-keyring)# peer HQ-ISR
Branch-ISR(config-ikev2-keyring-peer)#  address 192.0.2.3
Branch-ISR(config-ikev2-keyring-peer)#  pre-shared-key local cisco123
Branch-ISR(config-ikev2-keyring-peer)#  no pre-shared-key remote cisco
Branch-ISR(config-ikev2-keyring-peer)# exit
Branch-ISR(config-ikev2-keyring)# exit
Branch-ISR(config)# crypto ikev2 profile ccnp-ikev2-profile
Branch-ISR(config-ikev2-profile)# no authentication remote pre-share
Branch-ISR(config-ikev2-profile)# authentication remote rsa-sig
Branch-ISR(config-ikev2-profile)# pki trustpoint partner-isr
```

Step 2

On HQ-ISR, modify the key ring and IKEv2 profile to obtain this configuration:

```
HQ-ISR(config)# crypto ikev2 keyring KR
HQ-ISR(config-ikev2-keyring)# peer Branch-ISR
HQ-ISR(config-ikev2-keyring-peer)#  address 203.0.113.1
HQ-ISR(config-ikev2-keyring-peer)#  pre-shared-key remote cisco123
HQ-ISR(config-ikev2-keyring-peer)#  no pre-shared-key local cisco
HQ-ISR(config-ikev2-keyring-peer)# exit
HQ-ISR(config-ikev2-keyring)# exit
HQ-ISR(config)# crypto ikev2 profile ccnp-ikev2-profile
HQ-ISR(config-ikev2-profile)# no authentication local pre-share
HQ-ISR(config-ikev2-profile)# authentication local rsa-sig
HQ-ISR(config-ikev2-profile)# pki trustpoint partner-isr
```

Lab 3-2: Implement Hub-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN

Task 1: Configure Hub and Spoke for Virtual Access Connections

Step 3

To change the tunnel mode and tunnel source on Branch-ISR, enter these commands on Branch-ISR:

```
Branch-ISR(config)# interface Tunnel 0
Branch-ISR(config-if)# tunnel mode gre ip
Branch-ISR(config-if)# tunnel source GigabitEthernet 0/1
```

Step 4

To delete the tunnel interface and configure the Loopback 0 interface on HQ-ISR, use these commands:

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

```
HQ-ISR(config)# no interface Tunnel 0
HQ-ISR(config)# interface Loopback0
HQ-ISR(config-if)#  ip address 10.10.100.99 255.255.255.255
```

Step 5

To create a virtual template interface, enter the following commands on the HQ-ISR:

```
HQ-ISR(config)# interface Virtual-Template1 type tunnel
HQ-ISR(config-if)# ip unnumbered Loopback0
HQ-ISR(config-if)# tunnel protection ipsec profile ccnp-ipsec-profile
```

Step 6

To bind the virtual template to the custom IKEv2 profile, enter the following commands on the HQ-ISR:

```
HQ-ISR(config)# crypto ikev2 profile ccnp-ikev2-profile
HQ-ISR(config-ikev2-profile)# virtual-template 1
```

Task 2: Configure Certificate-Based Authentication on Spoke

Step 2

To enroll Branch-ISR with the Partner-ISR, use these commands on Branch-ISR. Enter challenge password **cisco**, when prompted.

https://t.me/learningnets

```
Branch-ISR(config)# crypto pki trustpoint partner-isr
Branch-ISR(ca-trustpoint)# fqdn branch-isr.secure-x.public
Branch-ISR(ca-trustpoint)# subject-name CN=branch-isr,O=secure-x.public
Branch-ISR(ca-trustpoint)# serial-number none
Branch-ISR(ca-trustpoint)# ip-address none
Branch-ISR(ca-trustpoint)# rsakeypair branch-keypair
Branch-ISR(ca-trustpoint)# exit
Branch-ISR(config)# crypto pki enroll partner-isr
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password: cisco
Re-enter password: cisco
% The subject name in the certificate will include: CN=branch-isr,O=secure-x.public
% The subject name in the certificate will include: branch-isr.secure-x.public
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose partner-isr' command will show the
fingerprint.
Branch-ISR(config)#
CRYPTO_PKI:  Certificate Request Fingerprint MD5: A32FFFDA 63F0D0D2 731D3D39 A4D95F37
CRYPTO_PKI:  Certificate Request Fingerprint SHA1: 7871DE0A 492E42DF 377EE012
0CA893F7 CD699367
%PKI-6-CERTRET: Certificate received from Certificate Authority
Branch-ISR(config)#
```

Step 3

On Branch-ISR, modify the IKEv2 profile (ccnp-ikev2-profile) for local certificate authentication in this way:

```
Branch-ISR(config)# crypto ikev2 profile ccnp-ikev2-profile
Branch-ISR(config-ikev2-profile)# no match identity remote fqdn hq-isr.secure-x.public
Branch-ISR(config-ikev2-profile)# match identity remote fqdn domain secure-x.public
Branch-ISR(config-ikev2-profile)# no authentication local pre-share
Branch-ISR(config-ikev2-profile)# authentication local rsa-sig
Branch-ISR(config-ikev2-profile)# no keyring local KR
```

Step 4

On HQ-ISR, modify the IKEv2 profile (ccnp-ikev2-profile) for remote certificate authentication in this way:

```
HQ-ISR(config)# crypto ikev2 profile ccnp-ikev2-profile
HQ-ISR(config-ikev2-profile)# no match identity remote fqdn branch-isr.secure-x.public
HQ-ISR(config-ikev2-profile)# match identity remote fqdn domain secure-x.public
HQ-ISR(config-ikev2-profile)# no authentication remote pre-share
HQ-ISR(config-ikev2-profile)# authentication remote rsa-sig
HQ-ISR(config-ikev2-profile)# virtual-template 1
HQ-ISR(config-ikev2-profile)# no keyring local KR
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Task 3: Configure Locally Managed Mode Config

Step 1

To enable AAA new model and enable default network authorization against the local database, enter these commands on Branch-ISR:

```
Branch-ISR(config)# aaa new-model
Branch-ISR(config)# aaa authorization network default local
```

Enter these commands on HQ-ISR:

```
HQ-ISR(config)# aaa new-model
HQ-ISR(config)# aaa authorization network default local
```

Step 2

To disable the default IKEv2 authorization policy and configure the custom IKEv2 authorization policy (ccnp-spokes), enter these commands on HQ-ISR:

```
HQ-ISR(config)# no crypto ikev2 authorization policy default
HQ-ISR(config)# ip local pool ccnp-pool 10.10.100.1 10.10.100.90
HQ-ISR(config)# crypto ikev2 authorization policy ccnp-spokes
HQ-ISR(config-ikev2-author-policy)# pool ccnp-pool
HQ-ISR(config-ikev2-author-policy)# route set interface
```

Step 3

On HQ-ISR, modify the IKEv2 profile (ccnp-ikev2-profile) for group authorization in this way:

```
HQ-ISR(config)# crypto ikev2 profile ccnp-ikev2-profile
HQ-ISR(config-ikev2-profile)# aaa authorization group cert list default ccnp-spokes
```

Step 4

On Branch-ISR, modify the IKEv2 profile (ccnp-ikev2-profile) for group authorization in this way:

```
Branch-ISR(config)# crypto ikev2 profile ccnp-ikev2-profile
Branch-ISR(config-ikev2-profile)# aaa authorization group cert list default default
```

Step 5

On Branch-ISR, enter these commands to allow the tunnel IP address to be obtained from the hub:

```
Branch-ISR(config)# interface Tunnel0
Branch-ISR(config-if)# ip address negotiated
```


https://t.me/learningnets

Task 4: Add a Second Flex VPN Spoke

Step 1

To enroll Partner-ISR with the CA running on the local system, use these commands on Partner-ISR. Enter challenge password **cisco**, when prompted.

```
Partner-ISR(config)# crypto pki trustpoint partner-isr
Partner-ISR(ca-trustpoint)# fqdn partner-isr.partner.public
Partner-ISR(ca-trustpoint)# subject-name CN=partner-isr,O=partner.public
Partner-ISR(ca-trustpoint)# enrollment url http://198.51.100.1:80
Partner-ISR(ca-trustpoint)# revocation-check none
Partner-ISR(ca-trustpoint)# serial-number none
Partner-ISR(ca-trustpoint)# ip-address none
Partner-ISR(ca-trustpoint)# exit
Partner-ISR(config)# crypto pki authenticate partner-isr
Certificate has the following attributes:
       Fingerprint MD5: 11AA7A03 60AF3688 169A1487 BD8C7E0D
     Fingerprint SHA1: 9BB21476 165D5C39 4E7DC4CA F234C939 C9807724
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
Partner-ISR(config)# crypto pki enroll partner-isr
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password: cisco
Re-enter password: cisco
% The subject name in the certificate will include: CN=partner-isr,O=partner.public
% The subject name in the certificate will include: partner-isr.partner.public
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose partner-isr' commandwill show the
fingerprint.
Dec 10 11:52:56.438: CRYPTO_PKI:  Certificate Request Fingerprint MD5: 0A9C63BD
8AD0C4B3 B6AE8F4F CEE5F590
Dec 10 11:52:56.438: CRYPTO_PKI:  Certificate Request Fingerprint SHA1: 7EE970D1
15F5343C 92F9157C 66A4AAD9 0BCDF133
Dec 10 11:52:59.398: %PKI-6-CERTRET: Certificate received from Certificate Authority
```

Step 2

To configure the same IKEv2 and IPsec constructs on Partner-ISR as on Branch-ISR, use these commands on the Partner-ISR:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

```
Partner-ISR(config)# aaa new-model
Partner-ISR(config)# aaa authorization network default local
Partner-ISR(config)# crypto ikev2 authorization policy default
Partner-ISR(config-ikev2-author-policy)# route set interface
Partner-ISR(config-ikev2-author-policy)# exit
Partner-ISR(config)# crypto ikev2 proposal ccnp-ikev2-proposal
Partner-ISR(config-ikev2-proposal)# encryption aes-cbc-256
Partner-ISR(config-ikev2-proposal)# integrity sha512
Partner-ISR(config-ikev2-proposal)# group 20
Partner-ISR(config-ikev2-proposal)# exit
Partner-ISR(config)# crypto ikev2 policy ccnp-ikev2-policy
Partner-ISR(config-ikev2-policy)# proposal ccnp-ikev2-proposal
Partner-ISR(config-ikev2-policy)# exit
Partner-ISR(config)# no crypto ikev2 policy default
Partner-ISR(config)# crypto ikev2 profile ccnp-ikev2-profile
Partner-ISR(config-ikev2-profile)# match identity remote fqdn domain secure-x.public
Partner-ISR(config-ikev2-profile)# identity local fqdn partner-isr.partner.public
Partner-ISR(config-ikev2-profile)# authentication remote rsa-sig
Partner-ISR(config-ikev2-profile)# authentication local rsa-sig
Partner-ISR(config-ikev2-profile)# pki trustpoint partner-isr
Partner-ISR(config-ikev2-profile)# aaa authorization group cert list default default
Partner-ISR(config-ikev2-profile)# exit
Partner-ISR(config)# crypto ipsec transform-set ccnp-ts esp-gcm 256
Partner-ISR(cfg-crypto-trans)# mode tunnel
Partner-ISR(cfg-crypto-trans)# exit
Partner-ISR(config)# no crypto ipsec transform-set default
Partner-ISR(config)# crypto ipsec profile ccnp-ipsec-profile
Partner-ISR(ipsec-profile)# set transform-set ccnp-ts
Partner-ISR(ipsec-profile)# set pfs group20
Partner-ISR(ipsec-profile)# set ikev2-profile ccnp-ikev2-profile
Partner-ISR(ipsec-profile)# exit
Partner-ISR(config)# no crypto ipsec profile default
Partner-ISR(config)# interface Tunnel0
Partner-ISR(config-if)# ip address negotiated
Partner-ISR(config-if)# tunnel source GigabitEthernet0/1
Partner-ISR(config-if)# tunnel destination 192.0.2.3
Partner-ISR(config-if)# tunnel protection ipsec profile ccnp-ipsec-profile
```

Step 3

To configure the IKEv2 profile to match remote peer domain partner.public in addition to the domain secure-x.public, enter these commands on the HQ-ISR:

```
HQ-ISR(config)# crypto ikev2 profile ccnp-ikev2-profile
HQ-ISR(config-ikev2-profile)# match identity remote fqdn domain partner.public
```

Step 4

Use this command on the Partner-ISR:

```
Partner-ISR(config)# no interface Tunnel1
```


https://t.me/learningnets

Lab 3-3: Implement Spoke-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN

Task 1: Configure BGP

Step 1

To remove the OSPF process from the Branch-ISR, enter this command on Branch-ISR:

```
Branch-ISR(config)# no router ospf 1
```

To disable OSPF on the tunnel subnet on HQ-ISR, enter these commands on HQ-ISR:

```
HQ-ISR(config)# router ospf 1
HQ-ISR(config-router)# no network 10.10.100.0 0.0.0.255 area 0
```

Step 2

To change the OSPF administrative distance on HQ-ISR, enter these commands on HQ-ISR:

```
HQ-ISR(config)# router ospf 1
HQ-ISR(config-router)# distance 210
```

Task 2: Configure Spoke-to-Spoke Shortcut Switching

Step 1

To disable Tunnel 0 interface on Branch-ISR, enter these commands on Branch-ISR:

```
Branch-ISR(config)# interface Tunnel 0
Branch-ISR(config-if)# shutdown
```

To disable Tunnel 0 interface on Partner-ISR, enter these commands on Partner-ISR:

```
Partner-ISR(config)# interface Tunnel 0
Partner-ISR(config-if)# shutdown
```

Step 2

To configure NHRP on the hub, enter these commands on HQ-ISR:

```
HQ-ISR(config)# interface Virtual-Template1 type tunnel
HQ-ISR(config-if)# ip nhrp network-id 1
HQ-ISR(config-if)# ip nhrp redirect
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Step 3

To configure a virtual template interface (1) that will be used for cloning the virtual access interfaces for the shortcut switching, enter these commands on Branch-ISR:

```
Branch-ISR(config)# interface Virtual-Template1 type tunnel
Branch-ISR(config-if)# ip unnumbered Tunnel0
Branch-ISR(config-if)# ip nhrp network-id 1
Branch-ISR(config-if)# ip nhrp shortcut virtual-template 1
Branch-ISR(config-if)# tunnel protection ipsec profile ccnp-ipsec-profile
```

To configure a virtual template interface (1) that will be used for cloning the virtual access interfaces for the shortcut switching, enter these commands on Partner-ISR:

```
Partner-ISR(config)# interface Virtual-Template1 type tunnel
Partner-ISR(config-if)# ip unnumbered Tunnel0
Partner-ISR(config-if)# ip nhrp network-id 1
Partner-ISR(config-if)# ip nhrp shortcut virtual-template 1
Partner-ISR(config-if)# tunnel protection ipsec profile ccnp-ipsec-profile
```

Step 4

To bind the virtual template interface (1) to the IKEv2 profile, enter these commands on Branch-ISR:

```
Branch-ISR(config)# crypto ikev2 profile ccnp-ikev2-profile
Branch-ISR(config-ikev2-profile)# virtual-template 1
```

To bind the virtual template interface (1) to the IKEv2 profile, enter these commands on Partner-ISR:

```
Partner-ISR(config)# crypto ikev2 profile ccnp-ikev2-profile
Partner-ISR(config-ikev2-profile)# virtual-template 1
```

Step 5

To configure the Tunnel 0 interface for NHRP, enter these commands on Branch-ISR:

```
Branch-ISR(config)# interface Tunnel0
Branch-ISR(config-if)# ip nhrp network-id 1
Branch-ISR(config-if)# ip nhrp shortcut virtual-template 1
```

To configure the Tunnel 0 interface for NHRP, enter these commands on Partner-ISR:

```
Partner-ISR(config)# interface Tunnel0
Partner-ISR(config-if)# ip nhrp network-id 1
Partner-ISR(config-if)# ip nhrp shortcut virtual-template 1
```


https://t.me/learningnets

Step 6

To modify crypto IKEv2 profile, enter these commands on Branch-ISR:

```
Branch-ISR(config)# crypto ikev2 profile ccnp-ikev2-profile
Branch-ISR(config-ikev2-profile)# match identity remote fqdn domain partner.public
```

Step 7

To re-enable Tunnel 0 interface on Branch-ISR, enter these commands on Branch-ISR:

```
Branch-ISR(config)# interface Tunnel 0
Branch-ISR(config-if)# no shutdown
```

To re-enable Tunnel 0 interface on Partner-ISR, enter these commands on Partner-ISR:

```
Partner-ISR(config)# interface Tunnel 0
Partner-ISR(config-if)# no shutdown
```

Lab 4-1: Implement ASA Basic Clientless SSL VPN

Task 1: Enable Clientless SSL VPN Connections

Step 1

There are no solutions for this lab.

Lab 4-2: Configure Application Access for Cisco ASA Clientless SSL VPN

Task 1: Configure Application Access Using Plugins

Step 1

There are no solutions for this lab.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lab 4-3: Implement Local and External AAA for Clientless SSL VPNs

Task 1: Configure Local Authorization

Step 1

There are no solutions for this lab.

Lab 5-1: Implement ASA Basic AnyConnect SSL VPN

Task 1: Install Client Certificate on Employee-PC and Move Employee-PC to SP Subnet

Step 1

There are no solutions for this lab.

Lab 5-2: Configure Advanced Authentication for Cisco AnyConnect SSL VPN

Task 1: Join the ISE to Active Directory

Step 1

There are no solutions for this lab.

Lab 5-3: Implement AnyConnect IPSec/IKEv2

Task 1: Deploy AnyConnect IPsec VPN Using WebLaunch

Step 1

There are no solutions for this lab.

https://t.me/learningnets

Lab 6-1: Implement Host Scan and DAP

Task 1: Enable Host Scan and Examine AntiSpyware Software on Employee-PC

Step 1

There are no solutions for this lab.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.