Complete Configuration Examples With Cisco ASA Firewalls

Written By: Harris Andrea

MSc Electrical Engineering and Computer Science

Cisco Certified Network Associate (CCNA)

Cisco Certified Network Professional (CCNP)

Cisco Certified Security Professional (CCSP)

http://www.networkstraining.com

About the Author:

Harris Andrea is a Senior Network Security Engineer working for a leading Internet Service Provider in Europe. He graduated from the University of Kansas USA in 1998 with a B.S and M.S degrees in Electrical Engineering and Computer Science. Since then, he has been working in the Networking field, designing, implementing and managing large scale networking projects with Cisco products and technologies. His main focus is on Network Security based on Cisco PIX/ASA Firewalls, Firewall Service Modules (FWSM) on 6500/7600 models, VPN products, IDS/IPS products, AAA services etc. To support his knowledge and to build a strong professional standing, Harris pursued and earned several Cisco Certifications such as CCNA, CCNP, and CCSP. He is also a technology blogger owing a networking blog about Cisco technologies which you can visit for extra technical information and tutorials.

http://www.networkstraining.com

Introduction:

This is the Bonus material that comes with the book "Cisco ASA Firewall Fundamentals-3rd Edition". It contains 11 complete configuration examples that are tested to be working on Cisco ASA firewall versions 9.x and even on older versions before that (8.x etc).

In the main book of Cisco ASA Firewall Fundamentals, we have covered the most important and frequently-used features and configurations that you need to know in order to implement a Cisco ASA Firewall in the most common network scenarios.

In this Bonus document we will provide real world complete configuration examples of Cisco ASA Firewalls. These configurations will bind together many of the "pieces" we've described in the main book, in order to give you a complete picture of an ASA Configuration in different network topologies.

For any questions that you may have or clarifications about the information presented in this eBook, please contact me at: asaebook@networkstraining.com

Have fun reading my eBook. I hope it will be a valuable resource for you.

Legal Notice:

You do not have resell rights or giveaway rights to this eBook. Only customers that have purchased this material are authorized to view it.

The information services and resources provided in this eBook are based upon the current Internet environment as well as the author's experience. The techniques presented here have been proven to be successful. Because technologies are constantly changing, the configurations and examples presented in this eBook may change, cease or expand with time. We hope that the skills and knowledge acquired from this eBook will provide you with the ability to adapt to inevitable evolution of technological services. However, we cannot be held responsible for changes that may affect the applicability of these techniques. The opinions expressed in this ebook belong to the author and are not necessarily those of Cisco Systems, Inc. The author is not affiliated with Cisco Systems, Inc.

All trademarks are trademarks of their respective owners. Rather than put a trademark symbol after every occurrence of a trademarked name, we use names in an editorial fashion only, and to the benefit of the trademark owner, with no intention of infringement of the trademark. Where such designations appear in this book, they have been printed with initial caps.

All product names, logos and artwork are copyrights of their respective owners. None of the owners have sponsored or endorsed this publication. While all attempts have been made to verify information provided, the author assumes no responsibility for errors, omissions, or contrary interpretation of the subject matter herein. Any perceived slights of peoples or organizations are unintentional. The purchaser or reader of this publication assumes responsibility for the use of these materials and information. No guarantees of income are made. The author reserves the right to make changes and assumes no responsibility or liability whatsoever on behalf of any purchaser or reader of these materials.

Table of Contents:

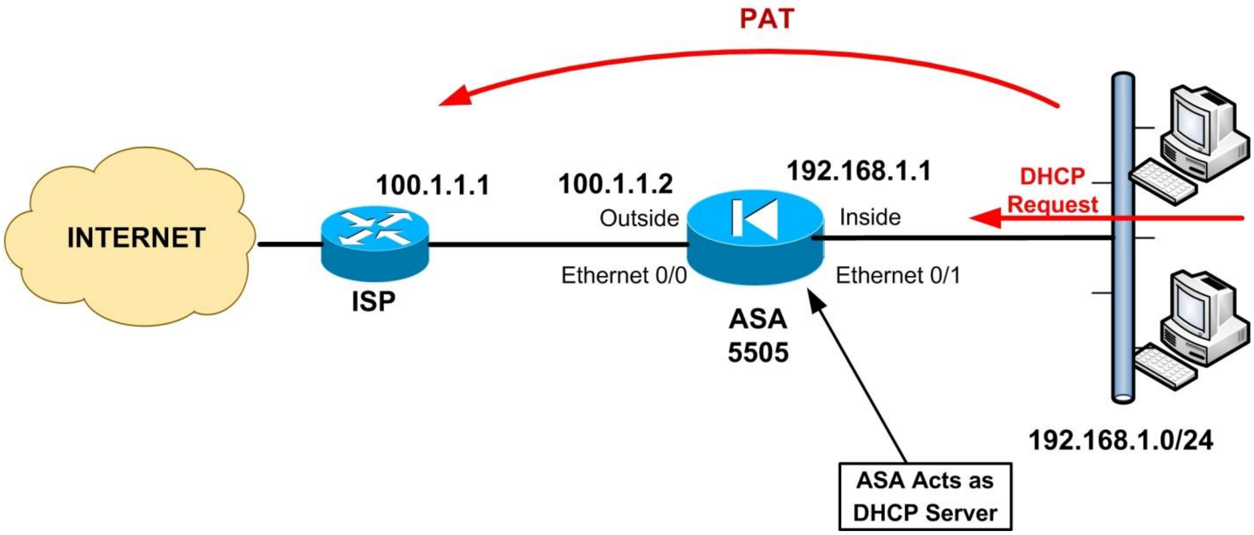
Complete Configuration Examples

1.1 ASA 5505 Configuration Examples

1.1.1 ASA 5505 Basic Internet Access with DHCP

The ASA 5505 (the smallest ASA model) is ideal for small businesses or small branch offices with approximately 50 internal users (recommended maximum). This model comes with 8 port 10/100 switch, with port Ethernet0/0 used for the Public/Outside zone and ports Ethernet0/1 up to 0/7 for the Inside zone. The difference of this model compared with the rest ASA models is that its network ports are pure Layer 2 switch ports. This means you cannot configure IP addresses directly on the physical interfaces. Instead, you have to assign the interface port in a VLAN, and then configure all Firewall Interface parameters using the **interface VLAN** command.

In this scenario the 5505 is used for basic internet access using PAT, with a static Public IP address on the outside (100.1.1.2). The Firewall will act also as a DHCP server for assigning IP addresses to inside hosts.



Let's see the complete configuration below. The commands with Bold are important.

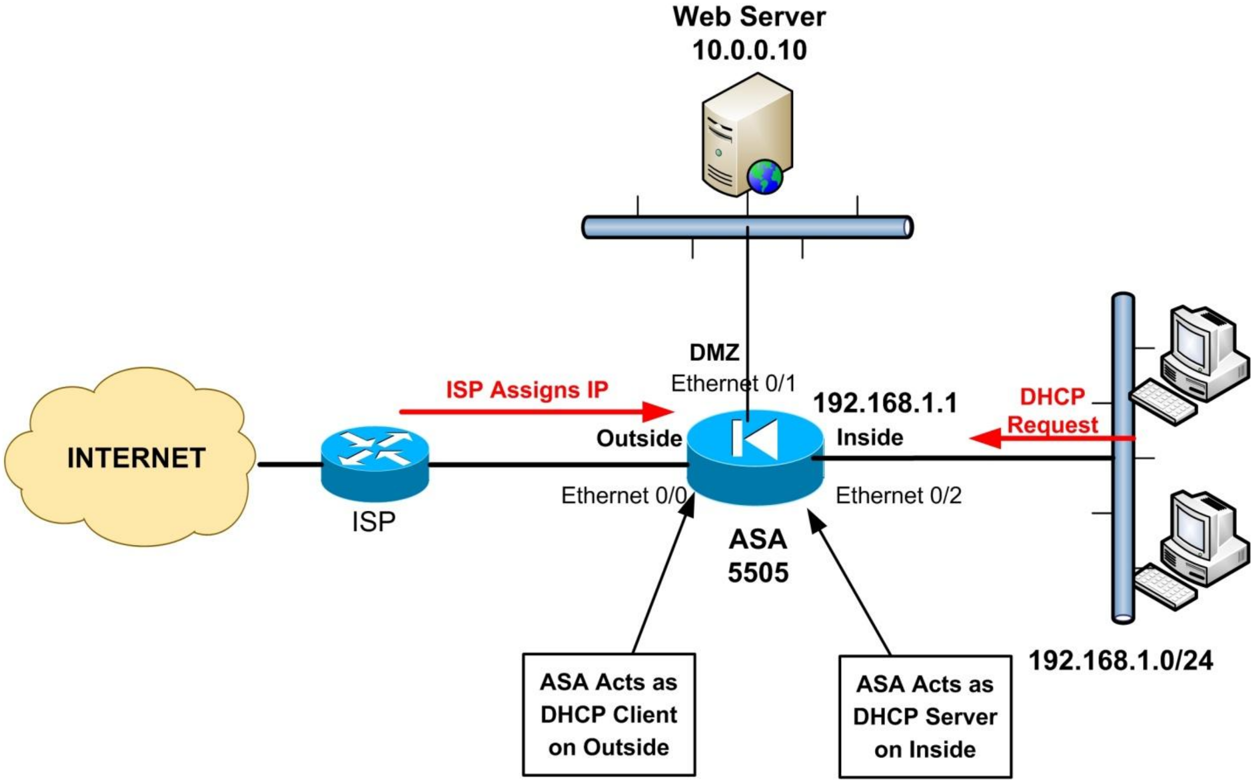
```
ASA-5505# show run
: Saved
:
!
hostname ASA-5505
domain-name test.com
enable password xxxxxxxxxxxxxxxx encrypted
names
!
! Vlan 1 is assigned by default for all ports Ethernet0/1 to 0/7 which belong to the inside zone.
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
! Vlan 2 is assigned to port Ethernet0/0 which belongs to the outside zone.
interface Vlan2
 nameif outside
 security-level 0
 ip address 100.1.1.2 255.255.255.252
!
! Assign Eth0/0 to vlan 2.
interface Ethernet0/0
 switchport access vlan 2
!
! By default, Eth0/1 to 0/7 are assigned to vlan 1. No need to change anything.
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
ftp mode passive
dns server-group DefaultDNS
 domain-name test.com

! Create an ACL on the outside that will allow only echo-reply for troubleshooting purposes. Use a
!deny all with log at the end to monitor any attacks coming from outside.
access-list outside_in extended permit icmp any any echo-reply
access-list outside_in extended deny ip any any log
pager lines 24
logging asdm informational
```

```
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
! Do PAT using the outside interface address
object network internal_lan
   subnet 192.168.1.0 255.255.255.0
   nat (inside,outside) dynamic interface

!Apply the ACL created above to the outside interface.
access-group outside_in in interface outside
route outside 0.0.0.0 0.0.0.0 100.1.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
! Configure Local authentication for firewall management (For accessing the Firewall you need to
!use the username/password configured later).
aaa authentication serial console LOCAL
aaa authentication telnet console LOCAL
aaa authentication ssh console LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
! Allow internal hosts to telnet to the device
telnet 192.168.1.0 255.255.255.0 inside
telnet timeout 5
! Allow an external management host to ssh from outside for firewall management
ssh 100.100.100.1 255.255.255.255 outside
ssh timeout 5
console timeout 0
! Assign a DNS server to internal hosts
dhcpd dns 200.200.200.1
!
! Assign IP addresses to internal hosts
dhcpd address 192.168.1.10-192.168.1.40 inside
dhcpd enable inside
!
!Create a Local username and password with administrator privileges
username admin password secretpass privilege 15

![other commands omitted]....
```

1.1.2 ASA 5505 with Dynamic IP Address and DMZ Host

This is an extension scenario of the previous one. The Cisco ASA 5505 receives an outside IP address dynamically from the ISP and has three security zones (Inside, Outside, DMZ). The Inside zone network shall be able to access the Internet and DMZ, and also Internet hosts shall be able to access the DMZ Web Server. This scenario can work with both Base License and Security Plus License. However, with a Security Plus license the DMZ public server (whatever that be – FTP, Email, Web etc) will be able to initiate traffic also to the Inside network zone (with the proper configuration). Instead of having a web server on DMZ, you can use this scenario also to host a Web Camera, a DVR, or a WiFi Router in the DMZ zone.

Since we have three security zones, we must create also three VLANs. VLAN1 (Inside) will be assigned to ports Ethernet0/2 up to 0/7, VLAN2 (Outside) will be assigned to port Ethernet 0/0, and VLAN3 (DMZ) will be assigned to Ethernet 0/1.



Let’s see the complete configuration below. The commands with Bold are important.

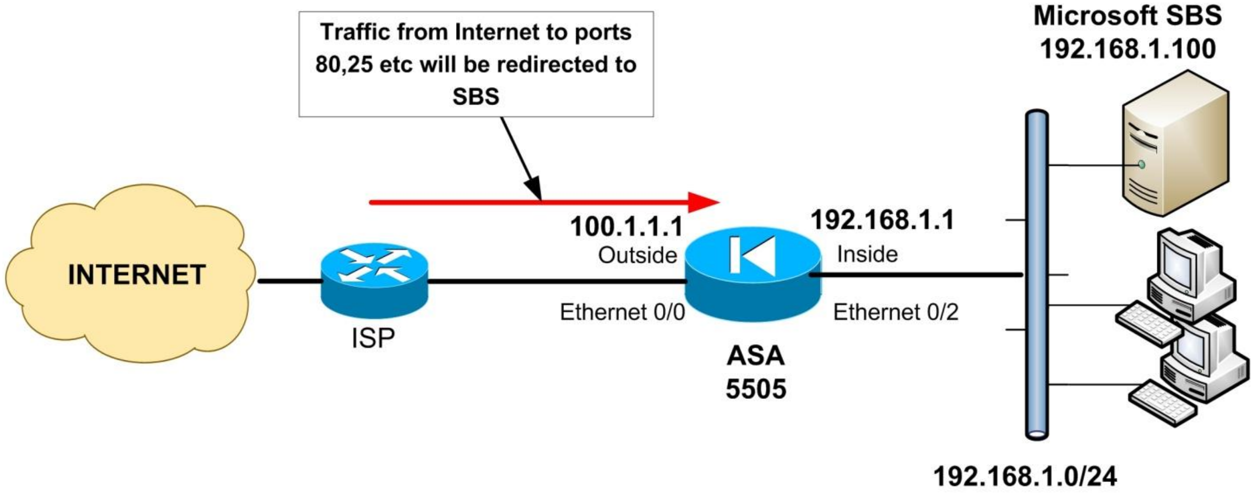
```
ASA-5505# show run
: Saved
:
!
hostname ASA-5505
domain-name test.com
enable password xxxxxxxxxxxxxxxx encrypted
names
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
! Get outside address and default gateway from ISP
 ip address dhcp setroute
!
interface Vlan3
! Use the following command ONLY if you have a BASE LICENSE
 no forward interface vlan 1
 nameif DMZ
 security-level 50
 ip address 10.0.0.1 255.255.255.0
!

! Assign Eth0/0 to vlan 2.
interface Ethernet0/0
 switchport access vlan 2
!
! Assign Eth0/1 to vlan 3.
interface Ethernet0/1
 switchport access vlan 3

! The rest are by default assigned to vlan 1. No need to change anything.
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
```

```
ftp mode passive
dns server-group DefaultDNS
 domain-name test.com

! Create an ACL on the outside that will allow access to the DMZ Web Server.
access-list outside_in extended permit tcp any host 10.0.0.10 eq 80
access-list outside_in extended deny ip any any log
pager lines 24
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu DMZ 1500
no asdm history enable
arp timeout 14400

!Do PAT on the outside and DMZ interfaces for the inside network
object network internal_lan_outside
   subnet 192.168.1.0 255.255.255.0
   nat (inside,outside) dynamic interface

object network internal_lan_dmz
   subnet 192.168.1.0 255.255.255.0
   nat (inside,DMZ) dynamic interface

! Create a static redirection for port 80 towards the DMZ web server
object network web_server_static
   host 10.0.0.10
   nat (DMZ,outside) static interface service tcp 80 80

! Do PAT on the outside for the DMZ web server. This will allow Web Server access to Internet.
object network dmz_to_outside
   subnet 10.0.0.0 255.255.255.0
   nat (DMZ,outside) dynamic interface

access-group outside_in in interface outside
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
! Configure Local authentication for firewall management (For accessing the Firewall you need to
!use the username/password configured later).
aaa authentication serial console LOCAL
aaa authentication telnet console LOCAL
aaa authentication ssh console LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
! Allow internal hosts to telnet to the device
telnet 192.168.1.0 255.255.255.0 inside
telnet timeout 5
! Allow an external management host to ssh from outside for firewall management
ssh 100.100.100.1 255.255.255.255 outside
ssh timeout 5
console timeout 0
dhcpd auto_config outside
! Assign a DNS server to internal hosts
dhcpd dns 200.200.200.1
!
! Assign IP addresses to internal hosts
dhcpd address 192.168.1.10-192.168.1.40 inside
dhcpd enable inside
!
!
! Configure here the username and password for accessing the device
username admin password secretpass privilege 15
```

1.1.3 ASA 5505 with Microsoft SBS Server on the Inside

A very common network scenario that I encounter all the time is to have a Cisco ASA 5505 working as Internet Border device and also a **Microsoft Small Business Server** (SBS) connected to the internal LAN network. This is suitable for small businesses and SOHO environments and offers an economical solution with great features. Although the best solution would be to have the SBS server isolated on a DMZ zone instead of directly connected to the internal LAN, here we assume that we have just a Basic License on ASA 5505 which does not allow DMZ configuration.

The requirement is to have all internal hosts (users' computers) to browse the Internet and also enable access from the Internet towards the SBS server. The example below will work for any SBS version (2003, 2008, 2011 etc). Depending on which services on the SBS you want to allow access from the Internet, you will need to allow the appropriate ports from the firewall. In our example below we assume that we have a single static Public IP address (100.1.1.1) configured on the outside interface of the ASA. This means that we will need to configure port redirection on the ASA in order to redirect the required traffic to the internal SBS Server (e.g traffic from internet to IP 100.1.1.1 / port 80 will be redirected to internal IP 192.168.1.100 / port 80 (SBS Server).



Let's see the complete configuration below. The commands with Bold are important.

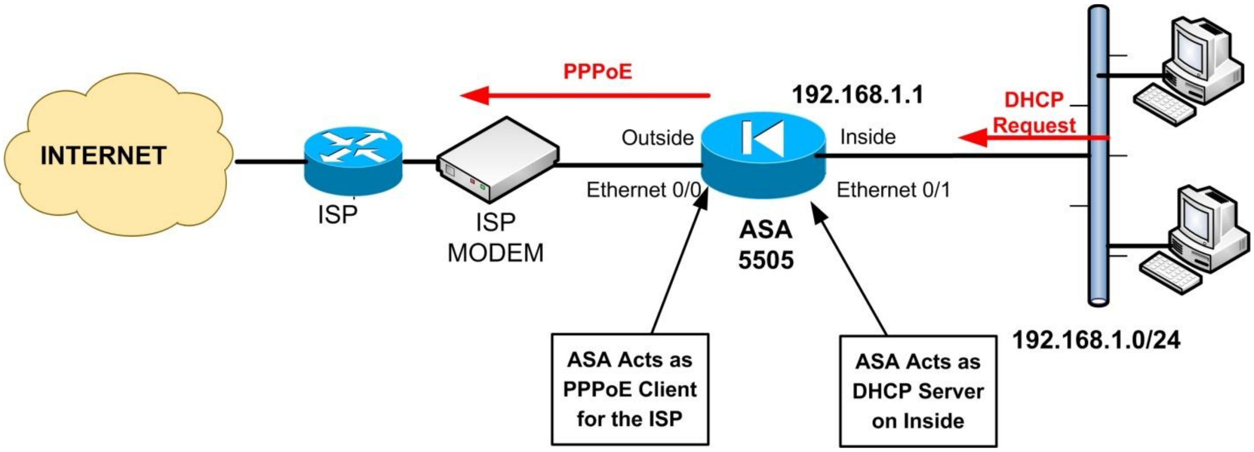
```
ASA-5505# show run
: Saved
:
!
hostname ASA-5505
domain-name test.com
enable password xxxxxxxxxxxxxxxx encrypted
names
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 100.1.1.1 255.255.255.252
!
! Assign Eth0/0 to vlan 2.
interface Ethernet0/0
 switchport access vlan 2
!
! The rest are by default assigned to vlan 1. No need to change anything.
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
ftp mode passive
dns server-group DefaultDNS
 domain-name test.com

! Create an ACL on the outside that will allow access to the SBS Server. Modify the ACL below
!according to which ports you actually need for accessing the SBS server.
access-list outside_in extended permit tcp any host 192.168.1.100 eq 80
access-list outside_in extended permit tcp any host 192.168.1.100 eq 25
access-list outside_in extended permit tcp any host 192.168.1.100 eq 443
access-list outside_in extended permit tcp any host 192.168.1.100 eq 3389
access-list outside_in extended deny ip any any log
```

```
pager lines 24
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu DMZ 1500
icmp unreachable rate-limit 1 burst-size 1
arp timeout 14400

! Do PAT on the outside interface
object network internal_lan
  subnet 192.168.1.0 255.255.255.0
  nat (inside,outside) dynamic interface

! Create static port redirections towards the internal SBS Server. Modify the commands below
!according to which ports you actually need for accessing the SBS server.
! Note that we use the keyword "interface" because the mapped IP is the one assigned on the
!outside interface.
object network sbs_server_static_80
  host 192.168.1.100
  nat (inside,outside) static interface service tcp 80 80

object network sbs_server_static_25
  host 192.168.1.100
  nat (inside,outside) static interface service tcp 25 25

object network sbs_server_static_443
  host 192.168.1.100
  nat (inside,outside) static interface service tcp 443 443

object network sbs_server_static_3389
  host 192.168.1.100
  nat (inside,outside) static interface service tcp 3389 3389

! Apply the ACL we have created above to the outside interface
access-group outside_in in interface outside

route outside 0.0.0.0 0.0.0.0 100.1.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
! Configure Local authentication for firewall management (For accessing the Firewall you need to
!use the username/password configured later).
aaa authentication serial console LOCAL
aaa authentication telnet console LOCAL
aaa authentication ssh console LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

```
! Allow internal hosts to telnet to the device
telnet 192.168.1.0 255.255.255.0 inside
telnet timeout 5
! Allow an external management host to ssh from outside for firewall management
ssh 100.100.100.1 255.255.255.255 outside
ssh timeout 5
console timeout 0
! Assign a DNS server to internal hosts
dhcpd dns 200.200.200.1
!
! Assign IP addresses to internal hosts
dhcpd address 192.168.1.20-192.168.1.50 inside
dhcpd enable inside
!
![some commands omitted]

! Configure here the username and password for accessing the device
username admin password secretpass privilege 15
```

1.1.4 ASA 5505 with PPPoE Internet Access

For Broadband DSL or Cable access connectivity, many ISPs provide Point to Point over Ethernet (PPPoE) access, as will be described in this example scenario. If the ISP supplies you with a username/password for internet access, this means that you need to configure your ASA as PPPoE client. Most often, in this setup the ISP provides you also with a Modem which will bridge the DSL or Cable connectivity between the Customer Premises Equipment (ASA 5505 in our case) and the ISP equipment. In the following typical environment the ISP is providing Public IP address to the ASA via PPPoE.



Let’s see the complete configuration below. The commands with Bold are important.

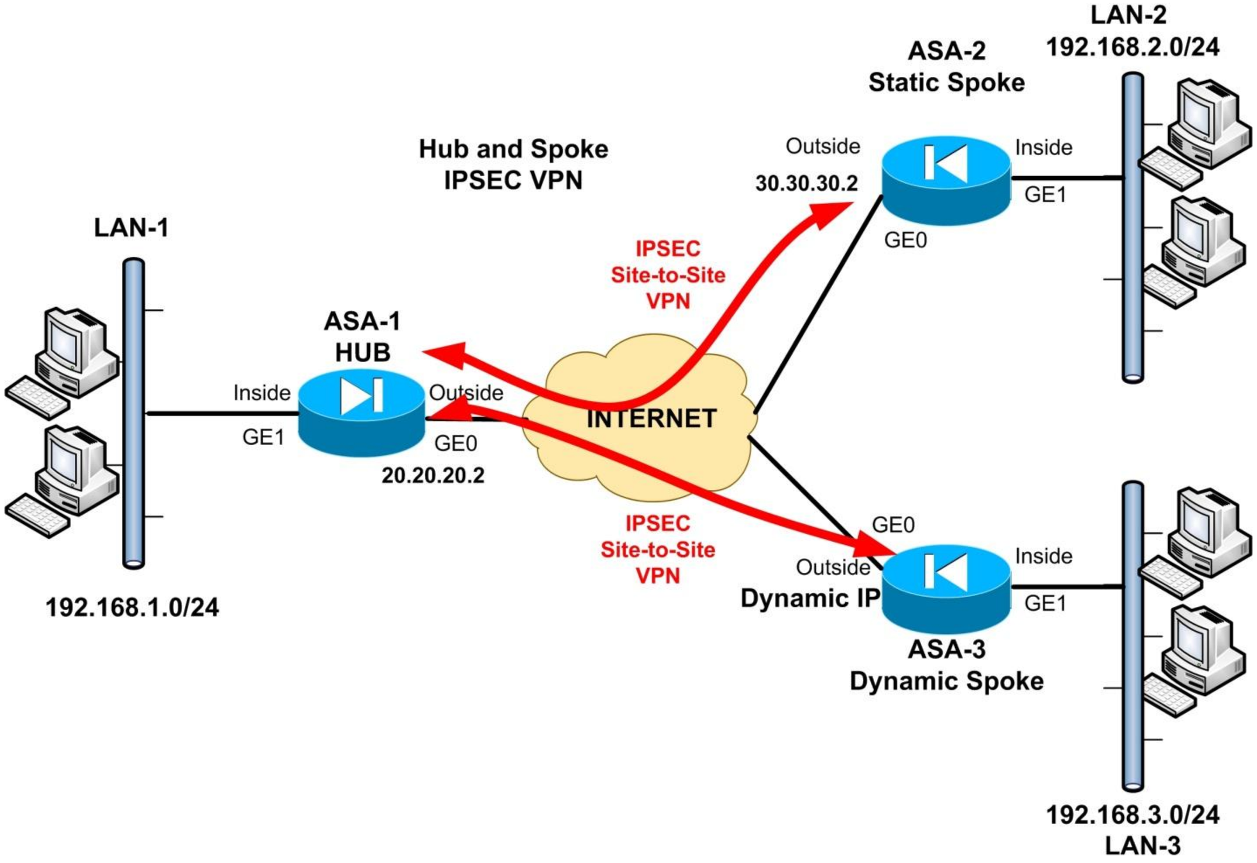
```
ASA-5505# show run
: Saved
!
hostname ASA-5505
domain-name test.com
enable password xxxxxxxxxxxxxxxx encrypted
names
!
! Vlan 1 is assigned by default to all ports Ethernet0/1 to 0/7 which belong to the inside zone.
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
! Vlan 2 is assigned to port Ethernet0/0 which belongs to the outside zone.
interface Vlan2
 nameif outside
 security-level 0
! Configure this VLAN as PPPoE Client and associate the pppoe group "ATT"
pppoe client vpdn group ATT
ip address pppoe setroute
!
! Assign Eth0/0 to vlan 2.
interface Ethernet0/0
 switchport access vlan 2
!
! By default, Eth0/1 to 0/7 are assigned to vlan 1. No need to change anything.
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
ftp mode passive
dns server-group DefaultDNS
 domain-name test.com

! Create an ACL on the outside that will allow only echo-reply for troubleshooting purposes. Use a
!deny all with log at the end to monitor any attacks coming from outside.
access-list outside_in extended permit icmp any any echo-reply
access-list outside_in extended deny ip any any log
pager lines 24
```

```
logging asdm informational
mtu inside 1500
! Configure the outside MTU as 1492 since there is an extra 8-byte overhead for PPPoE
mtu outside 1492
icmp unreachable rate-limit 1 burst-size 1
arp timeout 14400
! Do PAT using the outside interface address
object network internal_lan
   subnet 192.168.1.0 255.255.255.0
   nat (inside,outside) dynamic interface

access-group outside_in in interface outside
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
! Configure Local authentication for firewall management (For accessing the Firewall you need to
!use the username/password configured later).
aaa authentication serial console LOCAL
aaa authentication telnet console LOCAL
aaa authentication ssh console LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
! Allow internal hosts to telnet to the device
telnet 192.168.1.0 255.255.255.0 inside
telnet timeout 5
! Allow an external management host to ssh from outside for firewall management
ssh 100.100.100.1 255.255.255.255 outside
ssh timeout 5
console timeout 0

! Next create the “ATT” pppoe group with the ISP connection details
vpdn group ATT request dialout pppoe
vpdn group ATT localname [ENTER ISP USERNAME HERE]
vpdn group ATT ppp authentication chap [or PAP, depends on your ISP settings]
vpdn username [ENTER ISP USERNAME HERE] password [ENTER ISP PASSWORD HERE]

! Assign a DNS server to internal hosts
dhcpd dns 200.200.200.1
!
! Assign IP addresses to internal hosts
dhcpd address 192.168.1.10-192.168.1.40 inside
dhcpd enable inside
!
! Configure here the username and password for accessing the device
username admin password secretpass privilege 15
```

1.2 ASA VPN Configuration Examples

1.2.1 Hub-and-Spoke IPSec VPN with Dynamic IP Spoke

This is a very common and useful scenario which you can scale it to a bigger number of Spokes depending on your network topology. Many Enterprises usually have a big Central site (HUB) which shares data resources with several remote Branches (SPOKES). You can build a WAN data network between your Central and Branch sites using dedicated communication lines (very expensive) or you can use cheap Internet connectivity to build a private IPSEC Hub-and-Spoke VPN, as illustrated in the example network below. The central Hub site and one Spoke site have static IP addresses, whereas the second Spoke site has Dynamic IP address. To setup our Hub-and-Spoke VPN, we need to create two Site-to-Site IPSEC VPN tunnels between Central – Branch1 and Central – Branch2. Note that this example uses the traditional IKEv1 IPSEC.



Let’s see the complete configuration below. The commands with Bold are important.

ASA-1 (HUB)

```
hostname ASA1
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0
 nameif outside
 security-level 0
 ip address 20.20.20.2 255.255.255.0
!
interface GigabitEthernet1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
ftp mode passive

!Create objects with all local and remote LAN subnets
object network obj-local
 subnet 192.168.1.0 255.255.255.0
object network obj-remote1
 subnet 192.168.2.0 255.255.255.0
object network obj-remote2
 subnet 192.168.3.0 255.255.255.0
object network internal-lan
 subnet 192.168.1.0 255.255.255.0

access-list outside_in extended permit icmp any any echo-reply
access-list outside_in extended deny ip any any log

! Select the Interesting Traffic to be encrypted
access-list VPN-ACL1 extended permit ip 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
access-list VPN-ACL2 extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400

! Do not translate VPN Traffic
nat (inside,outside) 1 source static obj-local obj-local destination static obj-remote1 obj-remote1
nat (inside,outside) 2 source static obj-local obj-local destination static obj-remote2 obj-remote2
```

```
!
!Do PAT for the internal LAN using ASA outside interface
object network internal-lan
 nat (inside,outside) dynamic interface

access-group outside_in in interface outside
route outside 0.0.0.0 0.0.0.0 20.20.20.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart

aaa authentication ssh console LOCAL
aaa authentication serial console LOCAL
aaa authentication telnet console LOCAL

! Create a Phase 2 transform set for encryption and authentication protocols.
crypto ipsec ikev1 transform-set TRSET esp-3des esp-md5-hmac

!Create a Dynamic crypto map for the Spoke ASA with Dynamic IP address.

crypto dynamic-map DYNMAP 10 match address VPN-ACL2
crypto dynamic-map DYNMAP 10 set ikev1 transform-set TRSET

!Create a main crypto map and attach the static and dynamic crypto maps
crypto map VPNMAP 5 match address VPN-ACL1
crypto map VPNMAP 5 set peer 30.30.30.2
crypto map VPNMAP 5 set ikev1 transform-set TRSET
crypto map VPNMAP 10 ipsec-isakmp dynamic DYNMAP

!Attach the main crypto map on outside interface
crypto map VPNMAP interface outside

!Configure and enable the Phase1 isakmp policy
crypto isakmp identity address
crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
```

```
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept

!The following tunnel group (DefaultL2LGroup) is used for the Dynamic IP Spoke
tunnel-group DefaultL2LGroup ipsec-attributes
 ikev1 pre-shared-key secretkey2

!The following tunnel group (30.30.30.2) is used for the static IP Spoke
tunnel-group 30.30.30.2 type ipsec-l2l
tunnel-group 30.30.30.2 ipsec-attributes
 ikev1 pre-shared-key secretkey1
!
!
username admin password secretpass privilege 15

![other commands omitted]
```

ASA-2 (Static IP Spoke)

```
hostname ASA2
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0
 nameif outside
 security-level 0
 ip address 30.30.30.2 255.255.255.0
!
interface GigabitEthernet1
 nameif inside
 security-level 100
 ip address 192.168.2.1 255.255.255.0
!
ftp mode passive
!Create objects with all local and remote LAN subnets
object network obj-local
 subnet 192.168.2.0 255.255.255.0
object network obj-remote
 subnet 192.168.1.0 255.255.255.0
object network internal-lan
 subnet 192.168.2.0 255.255.255.0


access-list outside_in extended permit icmp any any echo-reply
access-list outside_in extended deny ip any any log
```

```
! Select the Interesting Traffic to be encrypted
access-list VPN-ACL extended permit ip 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400

! Do not translate VPN Traffic
nat (inside,outside) source static obj-local obj-local destination static obj-remote obj-remote
!
!Do PAT for the internal LAN using ASA outside interface
object network internal-lan
 nat (inside,outside) dynamic interface

access-group outside_in in interface outside
route outside 0.0.0.0 0.0.0.0 30.30.30.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
aaa authentication ssh console LOCAL
aaa authentication serial console LOCAL
aaa authentication telnet console LOCAL

! Create a Phase 2 transform set for encryption and authentication protocols.
crypto ipsec ikev1 transform-set TRSET esp-3des esp-md5-hmac

!Create a main crypto map for the tunnel with the Hub Site
crypto map VPNMAP 5 match address VPN-ACL
crypto map VPNMAP 5 set peer 20.20.20.2
crypto map VPNMAP 5 set ikev1 transform-set TRSET
crypto map VPNMAP interface outside

!Configure and enable the Phase1 isakmp policy
crypto isakmp identity address
crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept

!Tunnel group with the central Hub site
tunnel-group 20.20.20.2 type ipsec-l2l
tunnel-group 20.20.20.2 ipsec-attributes
 ikev1 pre-shared-key secretkey1
!
!
username admin password secretpass privilege 15

![other commands omitted]
```

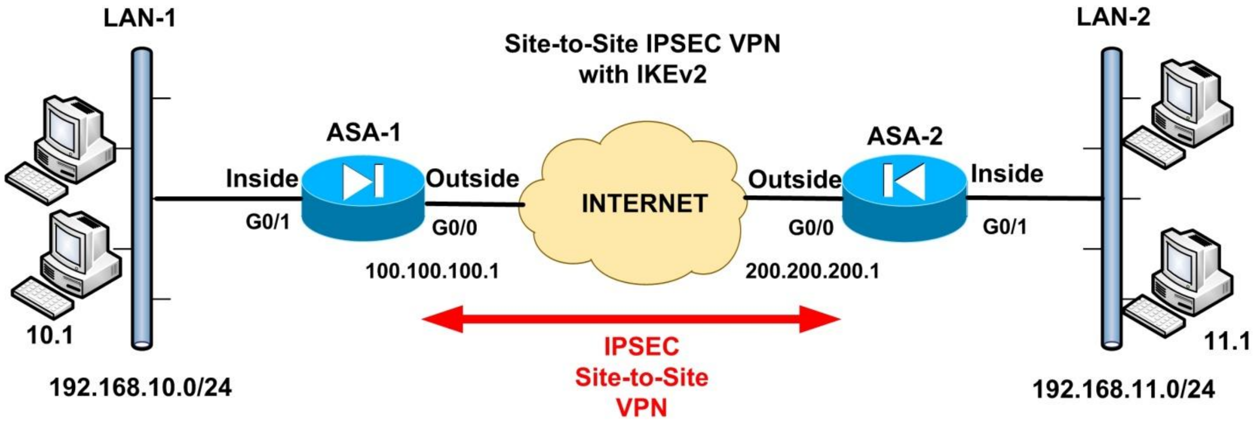
ASA-3 (Dynamic IP Spoke)

```
hostname ASA3
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
!Outside Interface receives a dynamic IP address using DHCP from the ISP
interface GigabitEthernet0
 nameif outside
 security-level 0
 ip address dhcp setroute
!
interface GigabitEthernet1
 nameif inside
 security-level 100
 ip address 192.168.3.1 255.255.255.0
!
ftp mode passive

!Create objects with all local and remote LAN subnets
object network obj-local
 subnet 192.168.3.0 255.255.255.0
object network obj-remote
 subnet 192.168.1.0 255.255.255.0
object network internal-lan
 subnet 192.168.3.0 255.255.255.0

access-list outside_in extended permit icmp any any echo-reply
access-list outside_in extended deny ip any any log
```

```
!Select VPN traffic
access-list VPN-ACL extended permit ip 192.168.3.0 255.255.255.0 192.168.1.0
255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400

! Do not translate VPN Traffic
nat (inside,outside) source static obj-local obj-local destination static obj-remote obj-remote
!
!Do PAT for the internal LAN using ASA outside interface
object network internal-lan
 nat (inside,outside) dynamic interface
access-group outside_in in interface outside
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
aaa authentication ssh console LOCAL
aaa authentication serial console LOCAL
aaa authentication telnet console LOCAL

! Create a Phase 2 transform set for encryption and authentication protocols.
crypto ipsec ikev1 transform-set TRSET esp-3des esp-md5-hmac

!Configure a main crypto map with the central Hub Site
crypto map VPNMAP 5 match address VPN-ACL
crypto map VPNMAP 5 set peer 20.20.20.2
crypto map VPNMAP 5 set ikev1 transform-set TRSET
crypto map VPNMAP interface outside

!Configure and enable the Phase1 isakmp policy
crypto isakmp identity address
crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept

!Tunnel group with the central Hub site
tunnel-group 20.20.20.2 type ipsec-l2l
tunnel-group 20.20.20.2 ipsec-attributes
 ikev1 pre-shared-key secretkey2
!
!
username admin password secretpass privilege 15

![other commands omitted]
```

1.2.2 Site-to-Site IKEv2 IPSec VPN between two ASA

The legacy IKEv1 IPSEC VPN has seen widespread implementation over the years in millions of site-to-site VPNs. Its successor, IKEv2 IPSEC, has started to take its position into the VPN networking space. Right now we are in a transitional stage where many enterprises are implementing IKEv2 VPNs while they still have legacy tunnels using IKEv1 IPSEC. In this configuration example we have two ASA firewalls with site-to-site VPN using the new IKEv2 IPSEC standard.



Let’s see the complete configuration below. The commands with Bold are important.

ASA-1

```
ASA-1# sh run

!
hostname ASA-1
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0
 nameif outside
 security-level 0
 ip address 100.100.100.1 255.255.255.0
!
interface GigabitEthernet1
 nameif inside
 security-level 100
 ip address 192.168.10.254 255.255.255.0
!
interface GigabitEthernet2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet5
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
!Create network objects for the local and remote subnets
object network obj-local
 subnet 192.168.10.0 255.255.255.0
object network obj-remote
 subnet 192.168.11.0 255.255.255.0
```

```
object network internal-lan
 subnet 192.168.10.0 255.255.255.0

access-list outside_in extended permit icmp any any echo-reply
access-list outside_in extended deny ip any any log

!Define VPN interesting traffic with an ACL
access-list VPN-ACL extended permit ip 192.168.10.0 255.255.255.0 192.168.11.0
255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400

!NAT Exemption for VPN traffic
nat (inside,outside) source static obj-local obj-local destination static obj-remote obj-remote
!
!PAT for the inside network
object network internal-lan
 nat (inside,outside) dynamic interface

access-group outside_in in interface outside
route outside 0.0.0.0 0.0.0.0 100.100.100.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart

!Create IKEv2 IPSEC Proposal
crypto ipsec ikev2 ipsec-proposal IKEv2-AES-SHA
 protocol esp encryption aes
 protocol esp integrity sha-1

!main crypto map which binds several ipsec settings together
crypto map outside_map 1 match address VPN-ACL
crypto map outside_map 1 set peer 200.200.200.1
crypto map outside_map 1 set ikev2 ipsec-proposal IKEv2-AES-SHA
crypto map outside_map interface outside
```

```
!IKEv2 policy (similar to Phase 1 in ikev1)
crypto ikev2 policy 1
 encryption aes 3des
 integrity sha md5
 group 2
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept

!Allow ikev2 as tunnel protocol
group-policy GroupPolicy1 internal
group-policy GroupPolicy1 attributes
 vpn-tunnel-protocol ikev2
tunnel-group 200.200.200.1 type ipsec-l2l
tunnel-group 200.200.200.1 general-attributes
 default-group-policy GroupPolicy1

!Define both a local and remote pre-shared keys. They must be reverse on the other site
tunnel-group 200.200.200.1 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco1
 ikev2 local-authentication pre-shared-key cisco1234
!
!
[other commands omitted]
```

ASA-2

```
hostname ASA-2
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0
 nameif outside
 security-level 0
 ip address 200.200.200.1 255.255.255.0
!
interface GigabitEthernet1
 nameif inside
 security-level 100
 ip address 192.168.11.254 255.255.255.0
!
```

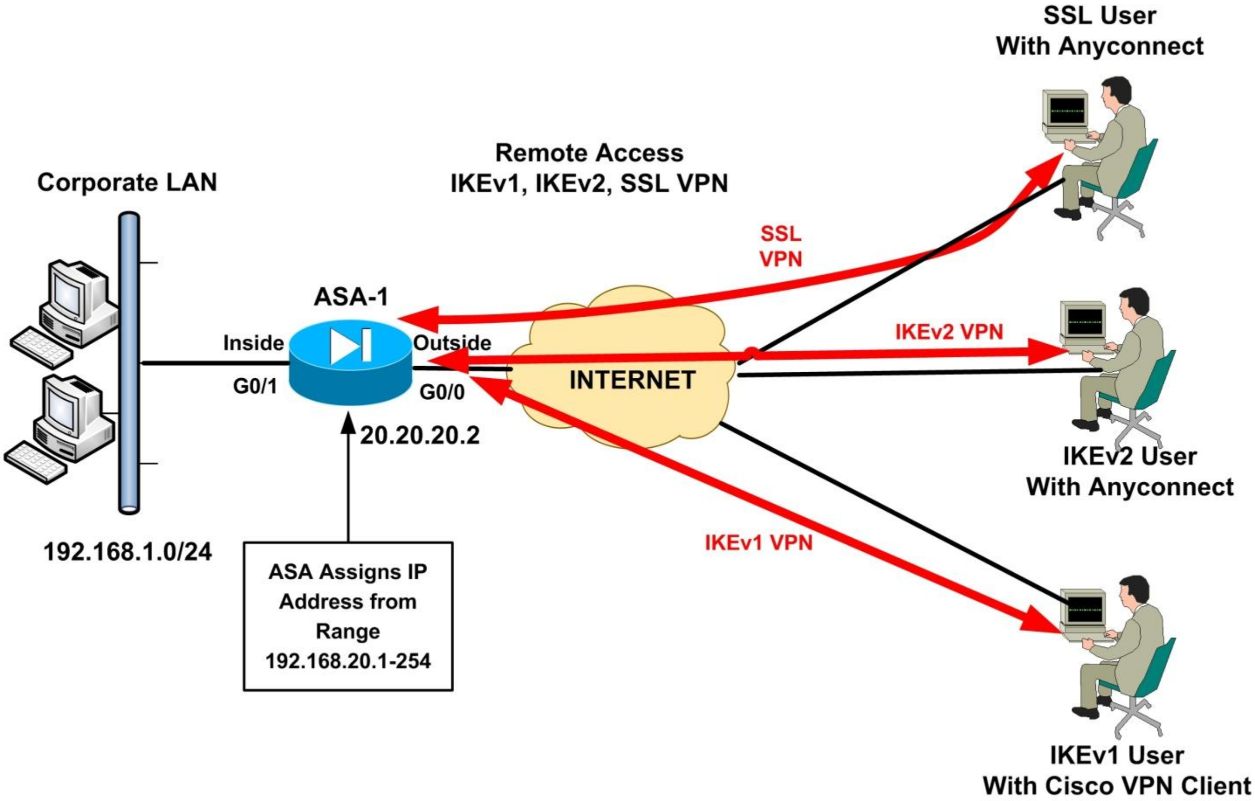
```
interface GigabitEthernet2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet5
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
!Create network objects for the local and remote subnets
object network obj-local
 subnet 192.168.11.0 255.255.255.0
object network obj-remote
 subnet 192.168.10.0 255.255.255.0
object network internal-lan
 subnet 192.168.11.0 255.255.255.0
access-list outside_in extended permit icmp any any echo-reply
access-list outside_in extended deny ip any any log

!Define VPN interesting traffic with an ACL
access-list VPN-ACL extended permit ip 192.168.11.0 255.255.255.0 192.168.10.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400

!NAT Exemption for VPN traffic
nat (inside,outside) source static obj-local obj-local destination static obj-remote obj-remote
!
```

```
!PAT for the inside network
object network internal-lan
 nat (inside,outside) dynamic interface
access-group outside_in in interface outside
route outside 0.0.0.0 0.0.0.0 200.200.200.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart

!Create IKEv2 IPSEC Proposal
crypto ipsec ikev2 ipsec-proposal IKEv2-AES-SHA
 protocol esp encryption aes
 protocol esp integrity sha-1

!main crypto map which binds several ipsec settings together
crypto map outside_map 1 match address VPN-ACL
crypto map outside_map 1 set peer 100.100.100.1
crypto map outside_map 1 set ikev2 ipsec-proposal IKEv2-AES-SHA
crypto map outside_map interface outside

!IKEv2 policy (similar to Phase 1 in ikev1)
crypto ikev2 policy 1
 encryption aes 3des
 integrity sha md5
 group 2
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
```

```
!Allow ikev2 as tunnel protocol
group-policy GroupPolicy1 internal
group-policy GroupPolicy1 attributes
 vpn-tunnel-protocol ikev2
tunnel-group 100.100.100.1 type ipsec-l2l
tunnel-group 100.100.100.1 general-attributes
 default-group-policy GroupPolicy1

!Define both a local and remote pre-shared keys. They must be reverse on the other site
tunnel-group 100.100.100.1 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco1234
 ikev2 local-authentication pre-shared-key cisco1
!
!
[other commands omitted]
```

1.2.3 Remote Access VPN with IKEv1, IKEv2 and SSL on the same ASA Device

After configuring the ASA in this scenario you will have a device that can support almost all types of remote access VPN technologies supported by Cisco ASA. Specifically, we will configure the ASA to accommodate remote access VPNs using the legacy IKEv1 IPSEC VPN, the new IKEv2 IPSEC VPN and also SSL VPNs. The first VPN type (IKEv1 IPSEC) requires the Cisco VPN client software installed on the user's computer. The other two VPN types (IKEv2 and SSL VPN) will work with the new Anyconnect Secure Mobility Client (version 3.x and above) as we have described in the main ASA book.



The following configuration has several pre-requisite settings that need to be in place in order to work. Specifically you need to create an Anyconnect XML Profile for the IKEv2 VPN as we have described in the main book. Optionally you can have also an XML Profile for the SSL VPN tunnel. These XML profiles must be created and copied to the flash of the ASA. Also, you must create RSA keys in order to generate a self-signed ASA certificate for the IKEv2 VPN (as we have described in the main ASA book). You can have also certificates signed from a third party CA instead of self-signed. Let's see the complete configuration below:

```
!Its important to configure a hostname and domain name since we will use certificates
hostname vpnasa
domain-name mycompany.com
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0
 nameif outside
 security-level 0
 ip address 20.20.20.2 255.255.255.0
!
interface GigabitEthernet1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
![some commands omitted]
!
!Its important to have correct clock settings and time-zone
clock timezone EEST 2
clock summer-time EEDT recurring last Sun Mar 3:00 last Sun Oct 4:00
dns server-group DefaultDNS
 domain-name mycompany.com

!Create network objects for the local LAN and for the VPN pool
object network obj-local
 subnet 192.168.1.0 255.255.255.0
object network obj-vpnpool
 subnet 192.168.20.0 255.255.255.0
object network FOR_PAT
 subnet 192.168.1.0 255.255.255.0

!split-tunnel ACL to enable split tunneling feature
access-list split-tunnel standard permit 192.168.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500

!IP Pool to assign addresses to remote users
ip local pool VPNpool 192.168.20.1-192.168.20.254 mask 255.255.255.0
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400

!PAT Configuration for the internal LAN
nat (inside,outside) source dynamic FOR_PAT interface
```

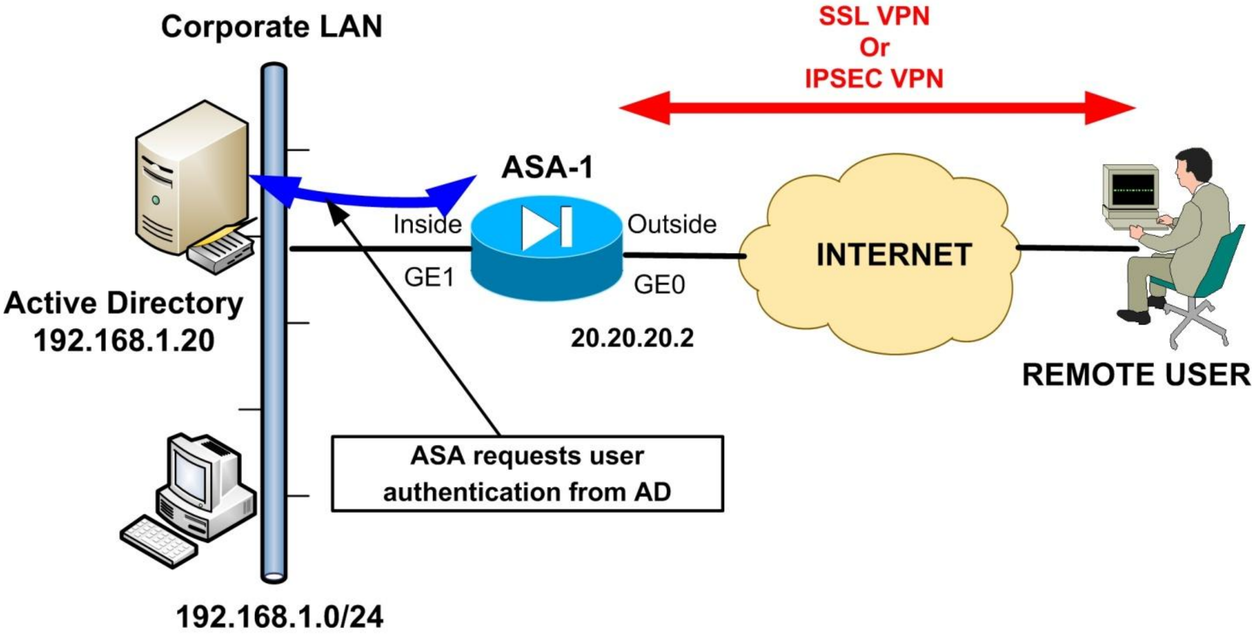
```
!NAT Exemption for the VPN traffic
nat (inside,outside) source static obj-local obj-local destination static obj-vpnpool obj-vpnpool no-proxy-arp route-lookup

route outside 0.0.0.0 0.0.0.0 20.20.20.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http redirect outside 80
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart

!Phase2 IPSEC Configuration for IKEv1
crypto ipsec ikev1 transform-set IKEv1-TS esp-3des esp-sha-hmac

!IPSEC Proposal (Phase2) Configuration for IKEv2
crypto ipsec ikev2 ipsec-proposal AES-3DES
 protocol esp encryption aes 3des
 protocol esp integrity sha-1 md5

!Create Dynamic Crypto maps for IKEv1 and IKEv2
crypto dynamic-map DYN_MAP 5 set ikev1 transform-set IKEv1-TS
crypto dynamic-map DYN_MAP 10 set ikev2 ipsec-proposal AES-3DES

!Attach the dynamic crypto map above to a static crypto map
crypto map OUTSIDE_MAP 10 ipsec-isakmp dynamic DYN_MAP
crypto map OUTSIDE_MAP interface outside

!This is the Trustpoint for the self-signed certificate
crypto ca trustpoint SELF-TP
 enrollment self
 subject-name CN=vpnasa.mycompany.com
 keypair rsakeys
 crl configure

!The following is created automatically when you generate the self-signed certificate
crypto ca certificate chain SELF-TP
 certificate 26239652
    308201ff 30820168 a0030201 02020426 23965230 0d06092a 864886f7 0d010105
    05003044 311d301b 06035504 03131476 706e6173 612e6d79 636f6d70 616e792e
    636f6d31 23302106 092a8648 86f70d01 09021614 76706e61 73612e6d 79636f6d
    70616e79 2e636f6d 301e170d 31333131 32373137 32353231 5a170d32 33313132
    35313732 3532315a 3044311d 301b0603 55040313 1476706e 6173612e 6d79636f
    6d70616e 792e636f 6d312330 2106092a 864886f7 0d010902 16147670 6e617361
    2e6d7963 6f6d7061 6e792e63 6f6d3081 9f300d06 092a8648 86f70d01 01010500
    03818d00 30818902 8181008e acca3766 bb7b5d50 1d53e073 e40f1907 313ce6d1
    6adea8a5 bd6371ff cdc68277 ca5d00a3 5c8b8ec3 385387e1 bb4ce3fe b0090129
    c79cba4d 5a72de30 df5ef8df 3e298ffd 68082aaa 6a368bc1 45251713 7bc3c756
    b73f3d1c eeef26ce 981f2a7d 25bc2dce ebff0c08 7c90c17c f537017a d7eee408
    b35528a9 1ec9598c a62c5102 03010001 300d0609 2a864886 f70d0101 05050003
    81810077 fe2dd664 da39f3b8 37bfac62 8b42c678 17fdaee3 84c61662 c665a1ff
    29557768 796336b4 f4715bbb c162bdc5 b1f5e9fb d321d445 d8cb3559 0d43b3f6
    10d7228f 245383e1 6c7132c9 6f742c4f 1fe4db48 a7020e6c 427e9000 bc334ca1
    91e04a11 c9776eb2 348f9e96 c1505349 4dab886a e4302059 be1414eb 5c76fdec 8857a9
  quit

crypto isakmp identity address

!Create ikev2 isakmp policy
crypto ikev2 policy 1
 encryption aes
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400

!Enable client-services and TrustPoint SSL authentication for IKEv2
crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint SELF-TP

crypto ikev1 enable outside

!Create ikev1 isakmp policy
crypto ikev1 policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400

telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept

ssl trust-point SELF-TP outside

!Setting for the Anyconnect VPNs (SSL and IKEv2)
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.04072-k9.pkg 1
```

```
!the following XML profiles must be copied to ASA flash (disk0)
 anyconnect profiles ikev2profile disk0:/ikev2profile.xml
 anyconnect profiles sslprofile disk0:/sslprofile.xml
 anyconnect enable
 tunnel-group-list enable

!Configure separate VPN group policies for each type of VPN users
!This is the VPN policy for SSL VPN remote access users
group-policy SSL-USERS-POLICY internal
group-policy SSL-USERS-POLICY attributes
 dns-server value 192.168.1.15
 vpn-tunnel-protocol ssl-client ssl-clientless
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split-tunnel
 webvpn
  anyconnect keep-installer installed
  anyconnect dpd-interval client 20
  anyconnect profiles value sslprofile type user
  anyconnect ask none default anyconnect

!This is the VPN policy for IKEv2 VPN remote access users
group-policy IKEv2-USERS-POLICY internal
group-policy IKEv2-USERS-POLICY attributes
 dns-server value 192.168.1.15
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split-tunnel
 webvpn
  anyconnect keep-installer installed
  anyconnect dpd-interval client 20
  anyconnect profiles value ikev2profile type user
  anyconnect ask none default anyconnect

!This is the VPN policy for legacy IKEv1 VPN remote access users
group-policy IKEv1-USERS-POLICY internal
group-policy IKEv1-USERS-POLICY attributes
 dns-server value 192.168.1.15
 vpn-tunnel-protocol ikev1
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split-tunnel

!Create local users for each type of remote access users
username ssluser password kmUcA9cVGIaUJEA6 encrypted
username ikev2user password z59Qxp4jZFQvrhoQ encrypted
username ikev1user password z59Qxp4jZFQvrhoQ encrypted

username admin password f3UhLvUj1QsXsuK7 encrypted privilege 15
```

```
!Configure separate tunnel groups for each type of VPN
!For IKEv2
tunnel-group ikev2remoteaccess type remote-access
tunnel-group ikev2remoteaccess general-attributes
 address-pool VPNpool
 default-group-policy IKEv2-USERS-POLICY

tunnel-group ikev2remoteaccess webvpn-attributes
 group-alias ikev2_users enable

!For SSL VPN
tunnel-group sslremoteaccess type remote-access
tunnel-group sslremoteaccess general-attributes
 address-pool VPNpool
 default-group-policy SSL-USERS-POLICY

tunnel-group sslremoteaccess webvpn-attributes
 group-alias sslvpn_users enable

!For IKEv1 VPN
tunnel-group ikev1remoteaccess type remote-access
tunnel-group ikev1remoteaccess general-attributes
 address-pool VPNpool
 default-group-policy IKEv1-USERS-POLICY

tunnel-group ikev1remoteaccess ipsec-attributes
 ikev1 pre-shared-key secretgroupkey
!
![other command omitted]
```

1.2.4 Anyconnect SSL VPN with Microsoft Active Directory Authentication

This is a scenario used frequently by many enterprises which have an internal Microsoft Active Directory (AD) server containing all users' credentials. Instead of configuring local usernames/passwords on the ASA device for authenticating the remote access users, you can use the existing AD to authenticate the users with their domain accounts. One important thing to keep in mind is that you must create an AD user account which has the privileges to login, search and retrieve account information from the AD. Here we used the username "**admin**" as an example. You must use a proper username which has enough privileges to be able to search/read/lookup users in the LDAP server. The ASA will use this "admin" user account to connect to the AD (whenever a remote user tries to authenticate) in order to lookup the remote user credentials and confirm the user authentication.



Let's see the configuration below based on the diagram above.

```
hostname ASA1
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0
 nameif outside
 security-level 0
 ip address 20.20.20.2 255.255.255.0
!
interface GigabitEthernet1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
![other interface commands omitted]
ftp mode passive

!network objects for the local LAN and VPN pool
object network obj-local
 subnet 192.168.1.0 255.255.255.0
object network obj-vpnpool
 subnet 192.168.5.0 255.255.255.0
object network FOR_PAT
 subnet 192.168.1.0 255.255.255.0

access-list split-tunnel standard permit 192.168.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500

ip local pool VPNpool 192.168.5.1-192.168.5.20 mask 255.255.255.0
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400

!NAT exemption for VPN traffic
nat (inside,outside) source static obj-local obj-local destination static obj-vpnpool obj-vpnpool no-proxy-arp route-lookup

nat (inside,outside) source dynamic FOR_PAT interface

route outside 0.0.0.0 0.0.0.0 20.20.20.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
```

```
dynamic-access-policy-record DfltAccessPolicy

!Configure the ASA to communicate with an internal AAA server using LDAP protocol
!(Microsoft AD uses LDAP) and the server-type will be Microsoft. The user "admin" with
!password "cisco123" must be created on the AD as we've discussed above. Also, the base DN
!tree must be obtained from the AD. Also "sAMAccountName" must be used by default

aaa-server AD-SERVER protocol ldap
aaa-server AD-SERVER (inside) host 192.168.1.20
 ldap-base-dn dc=mycompany, dc=com
 ldap-scope subtree
 ldap-naming-attribute sAMAccountName
 ldap-login-password cisco123
 ldap-login-dn cn=admin, cn=users, dc=mycompany, dc=com
 server-type microsoft

user-identity default-domain LOCAL

http redirect outside 80
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept

!Configure the SSL WebVPN
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.03103-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable

group-policy Anyconnect-Policy internal
group-policy Anyconnect-Policy attributes
 dns-server value 192.168.1.15
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split-tunnel
 webvpn
  anyconnect keep-installer installed
  anyconnect dpd-interval client 20
  anyconnect ask none default anyconnect

tunnel-group telecommuters type remote-access
```

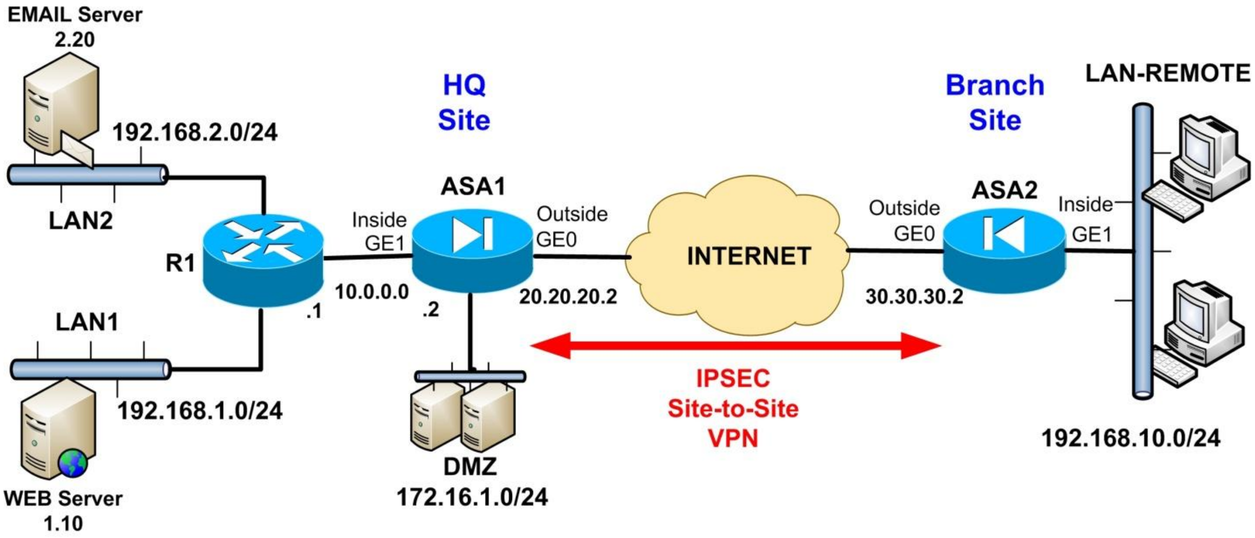
```
!Here, specify the AD-SERVER configured above as the authentication server for this tunnel
tunnel-group telecommuters general-attributes
 address-pool VPNpool
 authentication-server-group AD-SERVER
 default-group-policy Anyconnect-Policy

tunnel-group telecommuters webvpn-attributes
 group-alias sslgroup_users enable
!
![other commands omitted]
```

1.2.5 Special site-to-site IPSEC VPN between two ASA with Controlled VPN access

In this configuration scenario we will discuss a site-to-site IPSEC VPN implementation between two ASA devices. However, this will not be the classical simple site-to-site VPN scenario that you find everywhere but a more enhanced version of it. One of the sites will be a central headquarters (HQ) site with 2 internal network subnets (LAN1 and LAN2) and a DMZ subnet. The other site will be a remote Branch site again using Cisco ASA firewall as border Internet device (ASA2).

In a regular site-to-site VPN scenario, the two sites will have full LAN access between them over the VPN tunnel by default. In our special scenario here the remote branch site will have full network access only to the HQ DMZ subnet BUT restricted access to the two internal LAN networks of the HQ site. Specifically, the branch site will be allowed to access only a Web Server in Internal LAN1 of HQ and an Email Server in Internal LAN2 of HQ.

The above scenario will demonstrate several concepts in addition to the classical site-to-site ASA IPSEC VPN configuration. It will show how to pass multiple networks inside a VPN tunnel, how to access a DMZ via a VPN, how to restrict VPN traffic to specific hosts and ports etc.



Let's see the configuration for both ASA devices below:

ASA1 (HQ Site)

```
hostname ASA1
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0
 nameif outside
 security-level 0
 ip address 20.20.20.2 255.255.255.0
!
interface GigabitEthernet1
 nameif inside
 security-level 100
 ip address 10.0.0.2 255.255.255.0
!
interface GigabitEthernet2
 nameif dmz
 security-level 50
 ip address 172.16.1.1 255.255.255.0
!
![other interface commands omitted]
!
ftp mode passive
!Create network objects for the local and remote LANs
object network LAN1
 subnet 192.168.1.0 255.255.255.0
object network LAN2
 subnet 192.168.2.0 255.255.255.0
object network DMZ-LAN
 subnet 172.16.1.0 255.255.255.0
object network obj-remote
 subnet 192.168.10.0 255.255.255.0

!Create ACL to match the VPN traffic you want to encrypt
access-list VPN-ACL extended permit ip 192.168.1.0 255.255.255.0 192.168.10.0 255.255.255.0
access-list VPN-ACL extended permit ip 192.168.2.0 255.255.255.0 192.168.10.0 255.255.255.0
access-list VPN-ACL extended permit ip 172.16.1.0 255.255.255.0 192.168.10.0 255.255.255.0

!The outside ACL must explicitly allow IPSEC VPN protocols (ESP, AH, isakmp) and also allow
!access from remote LAN to DMZ and to Web Server and Email Server
access-list outside_in extended permit esp host 30.30.30.2 host 20.20.20.2
access-list outside_in extended permit ah host 30.30.30.2 host 20.20.20.2
access-list outside_in extended permit udp host 30.30.30.2 host 20.20.20.2 eq isakmp
access-list outside_in extended permit ip 192.168.10.0 255.255.255.0 172.16.1.0 255.255.255.0
```

```
access-list outside_in extended permit tcp 192.168.10.0 255.255.255.0 host 192.168.1.10 eq 80
access-list outside_in extended permit tcp 192.168.10.0 255.255.255.0 host 192.168.2.20 eq 25

pager lines 24
mtu outside 1500
mtu inside 1500
mtu dmz 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400

!Create the required NAT Exemptions for VPN traffic
nat (inside,outside) source static LAN1 LAN1 destination static obj-remote obj-remote
nat (inside,outside) source static LAN2 LAN2 destination static obj-remote obj-remote
nat (dmz,outside) source static DMZ-LAN DMZ-LAN destination static obj-remote obj-remote

access-group outside_in in interface outside
route outside 0.0.0.0 0.0.0.0 20.20.20.1 1
route inside 192.168.1.0 255.255.255.0 10.0.0.1 1
route inside 192.168.2.0 255.255.255.0 10.0.0.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart

!This command is important. It disables the mechanism to automatically allow all VPN traffic,
!so that you can control which VPN traffic you want to allow with the outside ACL
no sysopt connection permit-vpn

!The following commands configure IKEv1 IPSEC VPN parameters
crypto ipsec ikev1 transform-set TRSET esp-aes esp-sha-hmac

crypto map VPNMAP 10 match address VPN-ACL
crypto map VPNMAP 10 set peer 30.30.30.2
crypto map VPNMAP 10 set ikev1 transform-set TRSET

crypto map VPNMAP interface outside

crypto isakmp identity address
crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
tunnel-group 30.30.30.2 type ipsec-l2l
tunnel-group 30.30.30.2 ipsec-attributes
 ikev1 pre-shared-key secretkey1
!
!
![other commands omitted]
```

ASA2 (Branch Site)

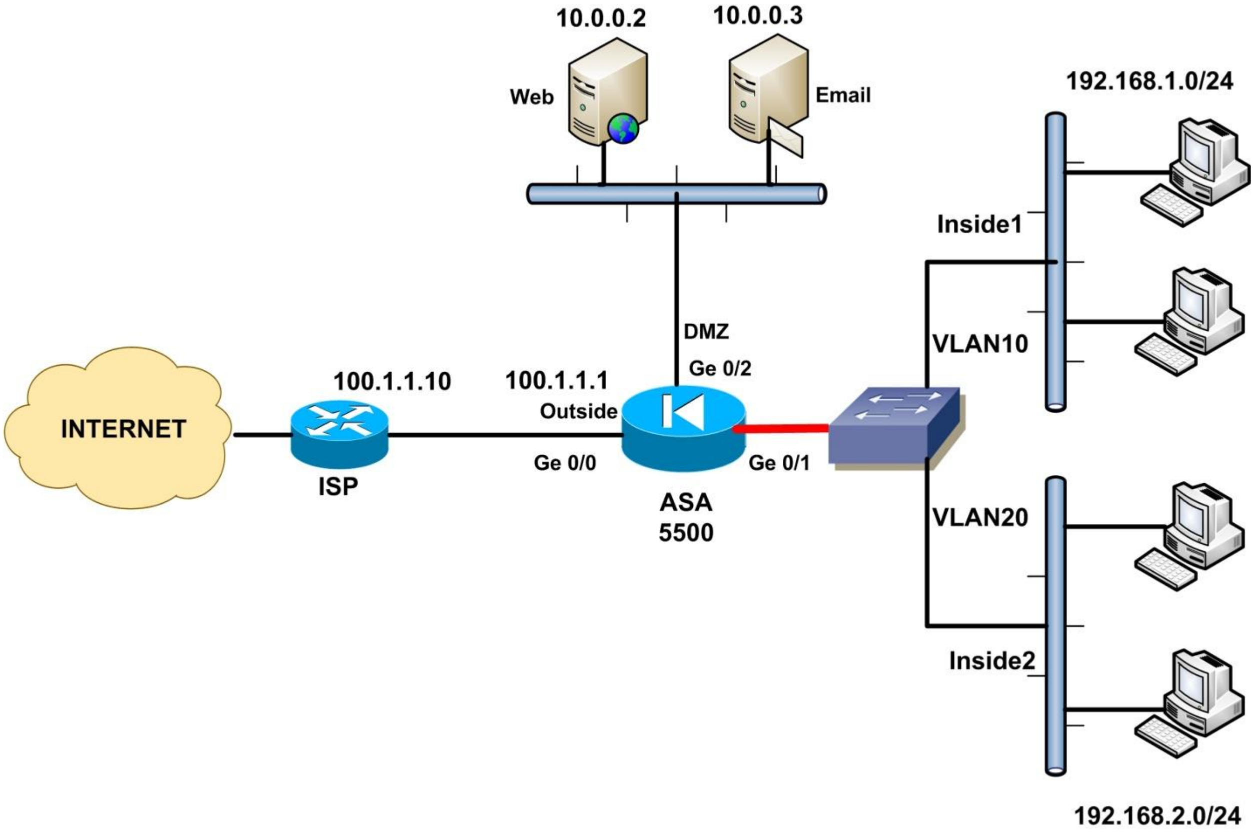
```
hostname ASA2
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0
 nameif outside
 security-level 0
 ip address 30.30.30.2 255.255.255.0
!
interface GigabitEthernet1
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
![other interface commands omitted]
!
ftp mode passive
!Create network objects for the local and remote LANs
object network LAN1
 subnet 192.168.1.0 255.255.255.0
object network LAN2
 subnet 192.168.2.0 255.255.255.0
object network DMZ-LAN
 subnet 172.16.1.0 255.255.255.0
object network obj-local
 subnet 192.168.10.0 255.255.255.0
```

```
!Create ACL to match the VPN traffic you want to encrypt
access-list VPN-ACL extended permit ip 192.168.10.0 255.255.255.0 192.168.1.0 255.255.255.0
access-list VPN-ACL extended permit ip 192.168.10.0 255.255.255.0 192.168.2.0 255.255.255.0
access-list VPN-ACL extended permit ip 192.168.10.0 255.255.255.0 172.16.1.0 255.255.255.0

pager lines 24
mtu outside 1500
mtu inside 1500
mtu dmz 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400

!Create the required NAT Exemptions for VPN traffic
nat (inside,outside) source static obj-local obj-local destination static LAN1 LAN1
nat (inside,outside) source static obj-local obj-local destination static LAN2 LAN2
nat (inside,outside) source static obj-local obj-local destination static DMZ-LAN DMZ-LAN

route outside 0.0.0.0 0.0.0.0 30.30.30.1 1

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart

!The following commands configure IKEv1 IPSEC VPN parameters
crypto ipsec ikev1 transform-set TRSET esp-aes esp-sha-hmac
crypto map VPNMAP 10 match address VPN-ACL
crypto map VPNMAP 10 set peer 20.20.20.2
crypto map VPNMAP 10 set ikev1 transform-set TRSET

crypto map VPNMAP interface outside

crypto isakmp identity address
crypto ikev1 enable outside

crypto ikev1 policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept

tunnel-group 20.20.20.2 type ipsec-l2l
tunnel-group 20.20.20.2 ipsec-attributes
 ikev1 pre-shared-key secretkey1
!
!
![other commands omitted]
```

1.3 General Configuration Examples

1.3.1 ASA Firewall with DMZ and two Internal Zones

In this scenario we will illustrate an ASA 5500 series Firewall (any model except 5505) with four security zones. One Outside, one DMZ, and two Internal Zones. The two Internal zones will be implemented on the same physical interface (Ge0/1) using two subinterfaces (Ge0/1.10 and Ge0/1.20). The DMZ zone will host a Web Server and an Email Server. We will use static NAT for the DMZ servers to translate their private IP addresses to public (Static NAT for private IP 10.0.0.2 to public IP 100.1.1.2 and Static NAT for private IP 10.0.0.3 to public IP 100.1.1.3). Also we will impose traffic restrictions to the two Internal Zones. **Inside1** users will be allowed to access only Web and Email, and **Inside2** users will have unrestricted Internet access.



Let's see the complete configuration below. The commands with Bold are important.

```
ASA-5500# show run
: Saved
:
!
hostname ASA-5500
domain-name test.com
enable password xxxxxxxxxxxxxxxxx encrypted
!
interface GigabitEthernet0/0
 description CONNECTION TO OUTSIDE INTERNET
 speed 100
 duplex full
 nameif outside
 security-level 0
 ip address 100.1.1.1 255.255.255.0
!
! Use the same Physical Interface Ge0/1 to create two internal zones using Vlans
interface GigabitEthernet0/1
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/1.10
 description CONNECTION TO INSIDE 1
 vlan 10
 nameif inside1
 security-level 80
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/1.20
 description CONNECTION TO INSIDE 2
 vlan 20
 nameif inside2
 security-level 90
 ip address 192.168.2.1 255.255.255.0
!
interface GigabitEthernet0/2
 description CONNECTION TO DMZ
 nameif DMZ
 security-level 50
 ip address 10.0.0.1 255.255.255.0
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
banner motd          ** W A R N I N G **
banner motd Unauthorized access prohibited. All access is
banner motd monitored, and trespassers shall be prosecuted
banner motd to the fullest extent of the law.
no ftp mode passive
dns server-group DefaultDNS
 domain-name test.com

!Create a service object with the Web Ports
object-group service WEB-PORTS tcp
 port-object eq 80
 port-object eq 443

! Allow access from Internet to our Web Server and Email Server. Notice that we use the private IP
access-list OUTSIDE_IN extended permit tcp any host 10.0.0.2 object-group WEB-PORTS
access-list OUTSIDE_IN extended permit tcp any host 10.0.0.3 eq 25

! Inside1 zone is only allowed to access web and email
access-list INSIDE1_IN extended permit tcp 192.168.1.0 255.255.255.0 any eq http
access-list INSIDE1_IN extended permit tcp 192.168.1.0 255.255.255.0 any eq https
access-list INSIDE1_IN extended permit tcp 192.168.1.0 255.255.255.0 any eq smtp
access-list INSIDE1_IN extended permit tcp 192.168.1.0 255.255.255.0 any eq pop3
access-list INSIDE1_IN extended permit udp 192.168.1.0 255.255.255.0 any eq dns

! Inside2 zone is allowed to access all protocols
access-list INSIDE2_IN extended permit ip 192.168.2.0 255.255.255.0 any

! Do PAT on the Outside and DMZ interfaces for internal hosts
object network internal_lan1_outside
   subnet 192.168.1.0 255.255.255.0
   nat (inside1,outside) dynamic interface

object network internal_lan1_dmz
   subnet 192.168.1.0 255.255.255.0
   nat (inside1,DMZ) dynamic interface

object network internal_lan2_outside
   subnet 192.168.2.0 255.255.255.0
   nat (inside2,outside) dynamic interface

object network internal_lan2_dmz
   subnet 192.168.2.0 255.255.255.0
   nat (inside2,DMZ) dynamic interface
```

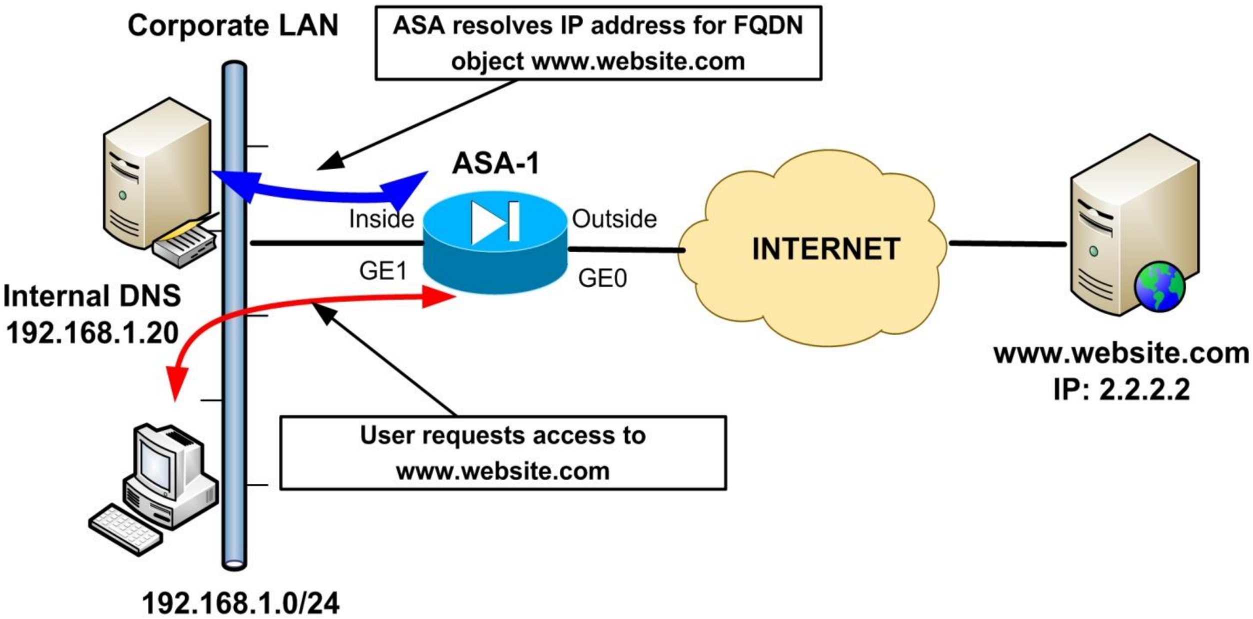
```
! Create permanent static NAT mappings for our DMZ servers.
object network web_static
   host 10.0.0.2
   nat (DMZ,outside) static 100.1.1.2

object network email_static
   host 10.0.0.3
   nat (DMZ,outside) static 100.1.1.3

!Apply ACLs on the proper interfaces
access-group OUTSIDE_IN in interface outside
access-group INSIDE1_IN in interface inside1
access-group INSIDE2_IN in interface inside2

route outside 0.0.0.0 0.0.0.0 100.1.1.10 1

!create local user for firewall administration
username admin password secretpass privilege 15

aaa authentication serial console LOCAL
aaa authentication ssh console LOCAL
aaa authentication telnet console LOCAL

!Allow ssh from zone inside1
ssh 192.168.1.0 255.255.255.0 inside1
ssh timeout 20
ssh version 2
console timeout 0
!

![other commands omitted]...
```

1.3.2 How to Block Access to specific Websites with Cisco ASA

The ASA can provide a simple solution for restricting web access to specific websites. However, it is NOT a replacement for a full-featured URL filtering solution. There are a few methods to block access to websites. These methods include regular expressions (regex) together with Modular Policy Framework (MPF), finding the IP address of the website and blocking with ACL, and using FQDN in an ACL. The first method (regex with MPF) works well with HTTP websites but it will not work at all if the website uses HTTPs. The second method (blocking the IP with ACL) will work only for simple websites which have a static IP but it will be difficult to work for dynamic websites (such as Facebook, Twitter etc) which have many different IP addresses which change all the time. The third method (using FQDN in an ACL) is the one which we will describe here.

From ASA version 8.4(2) and later, Access Control Lists (ACL) can contain an object which represents a Fully Qualified Domain Name (FQDN). So, inside an ACL you can allow or deny access to hosts using their FQDN name instead of their IP address. You can therefore deny access to website **www.facebook.com** by denying access to FQDN object "**www.facebook.com"** inside the ACL. The ASA will need to resolve all possible IP addresses of the FQDN and will dynamically insert several "deny IP" entries for these IP addresses in the ACL. Therefore you must specify what DNS server the ASA can use in order to resolve IP addresses for the FQDNs.

In our example network below, we want to restrict access to **www.website.com** which resolves to IP address 2.2.2.2. The ASA will use the internal DNS server (or any other DNS) to resolve the IP and put a "deny IP" entry in the inbound ACL applied on the "inside" interface.



ASA-1

```
hostname ASA-1
domain-name mycompany.com
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0
 nameif outside
 security-level 0
 ip address 20.20.20.2 255.255.255.0
!
interface GigabitEthernet1
 nameif inside
 security-level 100
 ip address 192.168.1.1
!
![other interface commands omitted]
!
ftp mode passive

!Specify which DNS server to use for resolving FQDN domains.
dns domain-lookup inside
dns server-group DefaultDNS
 name-server 192.168.1.20
 domain-name mycompany.com

!Create FQDN objects for website we want to block. Block both the www and non-www domains
object network obj-www.website.com
 fqdn www.website.com

object network obj-website.com
  fqdn website.com

!Add the FQDN objects above to an ACL applied inbound on the inside interface
access-list INSIDE-IN extended deny ip any object obj-www.website.com
access-list INSIDE-IN extended deny ip any object obj-website.com
access-list INSIDE-IN extended permit ip any any

!Apply the ACL above to the inside interface
access-group INSIDE-IN in interface inside

![other commands omitted]
```