SIMOS

Implementing Cisco Secure Mobility Solutions

Volume 2 **Student Guide**
Version 1.0

Part Number: 97-3335-01

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.

Table of Contents

Module 5

Deploying Cisco AnyConnect VPNs

When you combine the Cisco AnyConnect VPN Client with a Cisco ASA adaptive security appliance that is configured as a SSL VPN gateway, you can provide full-tunnel SSL VPN services to remote workers .The Cisco Adaptive Security Appliance also supports remote access IPsec VPNs. This module explains how to deploy both full-tunnel SSL VPNs and remote access IPsec VPNs. It also explains how to configure advanced authentication, authorization, and accounting for Cisco AnyConnect VPNs.

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

- Configure, verify, and troubleshoot a basic Cisco AnyConnect SSL VPN on a Cisco ASA security appliance
- Configure, verify, and troubleshoot advanced features of Cisco AnyConnect SSL VPNs
- Configure, verify, and troubleshoot advanced authentication and authorization in Cisco AnyConnect VPNs
- Configure, verify, and troubleshoot a Cisco AnyConnect IPsec/IKEv2 VPN on Cisco ASA security appliances

Lesson 1

Deploying Basic Cisco AnyConnect SSL VPN on Cisco ASA

A basic Cisco AnyConnect SSL VPN provides users with flexible client-based access to sensitive resources over a remote access VPN gateway, which is implemented on the Cisco Adaptive Security Appliance. A basic Cisco AnyConnect full-tunnel SSL VPN solution uses usernames and passwords to provide basic user authentication. In addition, the Cisco ASA provides IP address assignment to the full-tunnel client and uses a split tunneling policy to tunnel only traffic to specific internal networks. This lesson explains how to configure, verify, and troubleshoot a basic Cisco AnyConnect full-tunnel SSL VPN solution.

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

- Describe basic Cisco AnyConnect SSL VPN on Cisco ASA
- Describe different options to authenticate Cisco ASA when implementing basic Cisco AnyConnect SSL VPN
- Describe authentication options in basic AnyConnect SSL VPN
- Describe options for IP address assignment on AnyConnect SSL VPN clients
- Describe split tunneling on Cisco AnyConnect SSL VPN clients
- Provide configuration scenario for deploying basic Cisco AnyConnect SSL VPN on Cisco ASA
- Describe required configuration tasks for configuring basic Cisco AnyConnect SSL VPN
- Describe how to enable AnyConnect SSL VPNs
- Describe how to define an IP address pool
- Describe the configuration of identity NAT for VPN clients
- Describe the general settings configured in a group policy

Describe the split tunneling configuration in a group policy

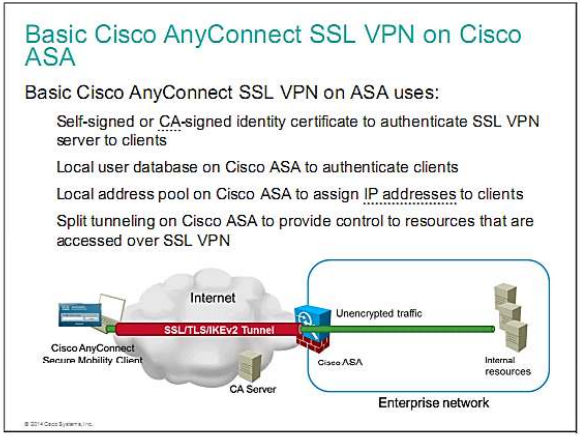
Describe the configuration of a connection profile

Describe how to monitor the AnyConnect VPN operation on the client endpoints

Describe how to monitor the AnyConnect VPN operation on the server

Basic Cisco AnyConnect SSL VPN

This topic provides an overview of basic AnyConnect SSL VPN implementation on Cisco Adaptive Security Appliance.



In a basic Cisco AnyConnect full-tunnel remote access SSL VPN solution, you use the Cisco AnyConnect Secure Mobility Client version to establish a SSL/TLS tunnel with the Cisco ASA. The basic solution uses bidirectional authentication: the client authenticates the Cisco ASA security appliance with a certificate-based authentication method and the Cisco ASA authenticates the user against its local user database, based on a username and password.

After authentication, the security appliance applies a set of authorization and accounting rules to the user session. When the Cisco ASA security appliance has established an acceptable VPN environment with the remote user, the remote user can forward raw IP traffic into the SSL/TLS tunnel. The Cisco AnyConnect client creates a virtual network interface to provide this functionality. This virtual adapter requires an IP address, and the most basic method to assign an IP address to the adapter, is to create a local pool of IP addresses on the Cisco ASA. The client can use any application to access any resource behind the Cisco ASA security appliance VPN gateway, subject to access rules and split tunneling policy, that are applied to the VPN session.

The user can use AnyConnect in the following modes:

Standalone mode - Lets the user establish an AnyConnect connection without using a web browser. If you have permanently installed AnyConnect on the user's PC, the user can run in standalone mode. In standalone mode, a user opens AnyConnect just like any other application and enters the username and password credentials into the fields of the AnyConnect GUI. Depending on how you configure the system, the user might also be required to select a group. When the connection is established, the ASA checks the version of AnyConnect on the user's PC and, if necessary, the client downloads the latest version.

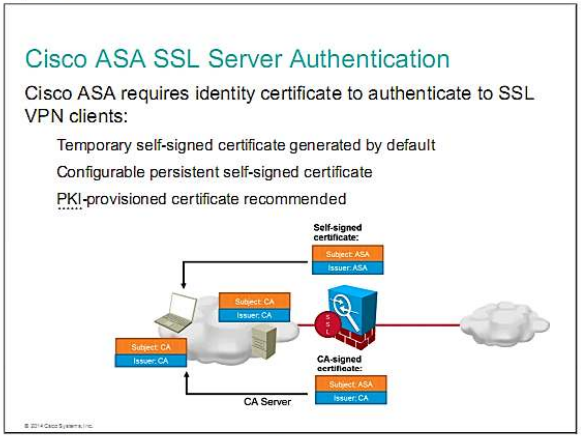
WebLaunch mode - Lets the user enter the URL of the ASA in the Address or Location field of a browser using the HTTPS protocol. The user then enters the username and password information on a Logon screen, selects the group, and clicks **Submit**. If you have specified a banner, that information appears, and the user acknowledges the banner by clicking **Continue**.

The portal window appears. To start AnyConnect, the user clicks **Start AnyConnect** on the main pane. A series of documentary windows appears. When the Connection Established dialog box appears, the connection is working, and the user can proceed with online activities.

If you configure the ASA to deploy the AnyConnect package, you ensure that the ASA is the single point of enforcement as to which versions of AnyConnect can establish a session, even if you deploy AnyConnect with an enterprise software deployment system. When you load an AnyConnect package on the ASA, you enforce a policy to which only versions as new as the one loaded on the ASA can connect. AnyConnect upgrades itself when it connects to the ASA. Alternatively, you can deploy a local policy file that specifies whether the client bypasses the client downloader, eliminating the requirement for the client package file on the ASA. However, other features such as weblaunch and automatic updates are disabled.

SSL VPN Server Authentication

This topic describes different options to authenticate Cisco Adaptive Security Appliance when implementing SSL VPN.



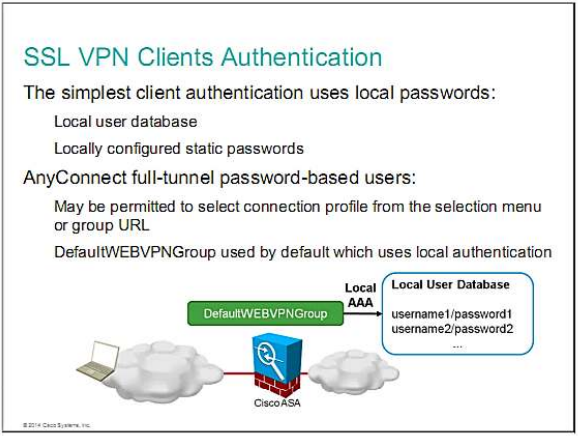
Similarly as with clientless SSL VPN, the Cisco ASA requires a server identity certificate, which the appliance sends to remote SSL VPN clients in order for remote clients to authenticate the Cisco ASA.

By default, the security appliance will create a self-signed X.509 certificate on each reboot, resulting in many client warnings when attempting SSL VPN access, as the certificate cannot be verified by any means. You can address this issue using one of the two approaches:

- By creating a permanent self-signed certificate which is persistent across reboots.
- By enrolling your Cisco ASA with an external CA.

SSL VPN Clients Authentication

This topic describes client authentication options in basic AnyConnect SSL VPN.

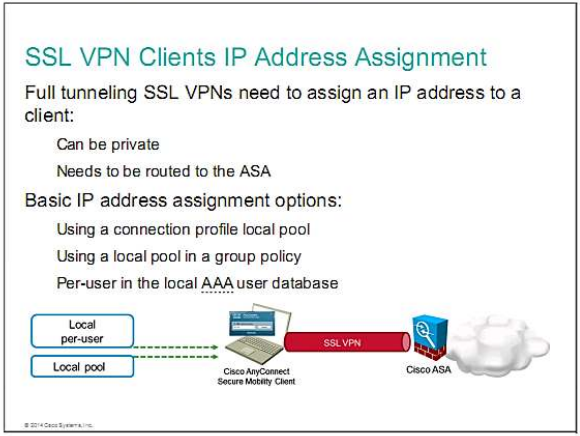


When an AnyConnect SSL VPN users connect to the Cisco Adaptive Security Appliance, the users may be permitted to select their connection profile by either choosing the desired profile from a drop-down list or connecting to the group URL. If no specific connection profile has been chosen, Cisco ASA will assign them to the DefaultWEBVPNGroup connection profile. This profile is by default configured to use user authentication using the local user database on the Cisco ASA.

When the user selects a connection profile (or uses the DefaultWEBVPNGroup connection profile), the user is required to authenticate using a method defined in the connection profile. The simplest user authentication method is using usernames and static passwords, which are stored in the local user database on the Cisco ASA. When a client enters a username and password into the login prompt, both are sent to the Cisco ASA. On the Cisco ASA, the provided username and password are compared to the locally stored username and password. If the provided and stored username and password match, the ASA establishes an SSL VPN session and applies a set of policies to the session.

SSL VPN Clients IP Address Assignment

This topic describes basic options for IP address assignment for SSL VPN clients.



When clients connect to a full-tunnel SSL VPN, the VPN gateway assigns an IP address to the virtual network interface (adapter) of the client PC. The PC uses this IP address as the source IP address to access resources beyond the VPN gateway. These IP addresses can be from the private IP address space, but they must be routed to the gateway (Cisco Adaptive Security Appliance) in the internal network.

The Cisco ASA can assign IP addresses in an SSL VPN full-tunnel solution in several different ways. The most basic ones are:

Use an IP address pool that is configured on the Cisco ASA, and assign the pool to a default or custom connection profile. Any client that uses this specific connection profile will be assigned an IP address from this pool. This is the simplest method if all users use the same connection profile and there is not need to differentiate between the users based on IP addresses.

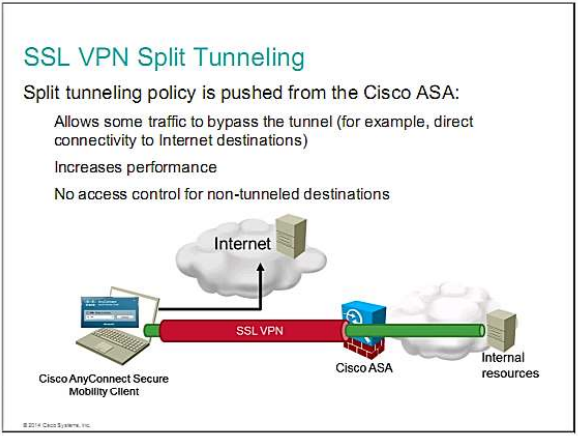
Use an IP address pool that is configured on the Cisco ASA, and assign the pool to a default or custom group policy. Any connection profiles that use this specific group policy will be assigned IP addresses from this pool. This is a good method to use if you want to differentiate between multiple groups of users on the Cisco ASA and in other parts of the protected network.

Configure the IP addresses as part of the user account in the local user database, enabling per-user IP addresses. This is a good method to use if you want to assign specific per-user policies on the Cisco ASA and in other parts of the protected network. This approach also simplifies user auditing and tracking because you can uniquely identify each user with a particular IP address when the user is connected to the VPN.

Note The ASA supports three different methods to assign an IP address back to the client: local address pool, DHCP server, and RADIUS server.

SSL VPN Split Tunneling

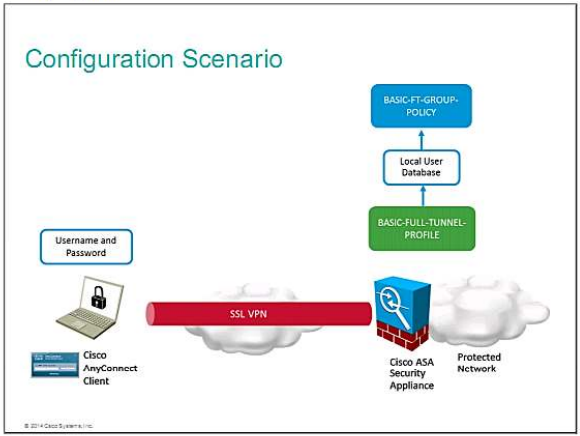
This topic describes split tunneling on Cisco AnyConnect SSL VPN clients.



By default, the Cisco Adaptive Security Appliance configures the client to forward all IP traffic over the VPN tunnel. Split tunneling allows you to tunnel only certain traffic to specific internal protected networks, while all other traffic bypasses the VPN tunnel. Split tunneling can improve the performance of applications that do not require the VPN tunnel (such as Internet access), but can increase risk because the client is not protected by central site security mechanisms when it is connecting to the other networks. Split tunneling may also increase risk because the client can be used as a relay between the external networks and the internal protected network more easily if the client is compromised by an attacker.

Configuration Scenario

This topic provides a configuration scenario for deploying basic Cisco AnyConnect SSL VPN on Cisco Adaptive Security Appliance.

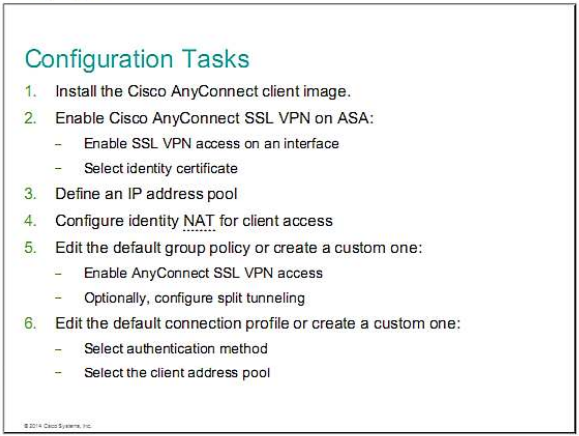


This figure presents the scenario, where you create a custom connection profile named BASIC-FULL-TUNNEL-PROFILE and a related group policy named BASIC-FT-GROUP-POLICY on Cisco Adaptive Security Appliance. Then, you will create one user named "user1" in the local user database. For simple deployments you could also customize and reuse the default connection profile and the default group policy. However, for the sake of demonstration, custom connection profile and custom group policy will be configured.

Note This configuration scenario assumes that identity server SSL/TLS certificate is provisioned to the Cisco ASA and Cisco AnyConnect client software image is loaded on the Cisco ASA.

Configuration Tasks

This topic describes required configuration tasks to configure basic Cisco AnyConnect SSL VPN on Cisco Adaptive Security Appliance.



The general deployment tasks are necessary to create a basic Cisco AnyConnect full-tunnel SSL VPN:

1. Install the Cisco AnyConnect client image, which should already be copied to the ASA's flash memory. You can also skip this step, and you will be asked to install the AnyConnect image later when enabling full-client SSL VPN access.
2. Enable Cisco AnyConnect SSL VPN on ASA:

   Enable full-client SSL VPN traffic termination on a Cisco ASA interface, which enables the security appliance SSL VPN server function. When enabling full-client SSL VPN access, you will be also asked to select and install the Cisco AnyConnect image file, if you have not done it before.

   You must assign the installed identity certificate of the Cisco ASA to the chosen VPN traffic termination interface.
3. Define an IP address pool.
4. Configure identity NAT for VPN client access.
5. Edit the default group policy or create a custom one:

   Make sure that support for Cisco AnyConnect SSL VPNs is enabled.

   Optionally, configure split tunneling, which allows you to tunnel only certain traffic to specific internal protected networks, while all other traffic bypasses the VPN tunnel.
6. Edit the default connection profile or create a custom one:

   Allow the user to choose a connection profile at login. This setting is required if you want to assign users to a specific connection profile rather than having them use the default DefaultWebVPNGroup profile.

   Select the authentication method. Default options is local AAA authentication method.

To provide IP addresses to the Cisco AnyConnect clients, create a local address pool.

Before implementing a basic Cisco AnyConnect full-tunnel SSL VPN on Cisco ASA, you must obtain and analyze several pieces of information that relate to the network and system environment:

The IP addressing plan for the VPN gateway: This information enables you to assign an appropriate IP address to the VPN-terminating interface of the Cisco ASA.

The enterprise naming plan for the VPN gateway: This information enables you to assign a correct name in the VPN gateway SSL/TLS identity certificate.

The enterprise certificate policy and certificate settings: With this information, you can enroll the Cisco ASA into a PKI (if desired) and you can include all of the relevant fields inside a PKI-provisioned certificate.

The username and password policy of the enterprise: This information enables you to correctly create the local user database on the Cisco ASA.

The IP addressing plan for remote clients: In a full-tunnel SSL VPN, the Cisco ASA must assign IP addresses to remote clients. These addresses must be unique and must be routed to the Cisco ASA for VPN connectivity to work.

Which sensitive resources remote users can access: This information enables you to configure a split tunneling policy on the Cisco ASA that will be applied to AnyConnect SSL VPN sessions.

Consider the following guidelines when deploying a basic Cisco AnyConnect full-tunnel SSL VPN solution on Cisco ASA:

Use PKI-provisioned certificates for SSL VPN identity certificate.

Use local password-based user authentication in low-risk environments where all users share the same access policy.

Strictly set the service type of local VPN user accounts to prevent these accounts from using management access.

Easily extend the basic solution with remote AAA user authentication and multiple access policies, as needed.

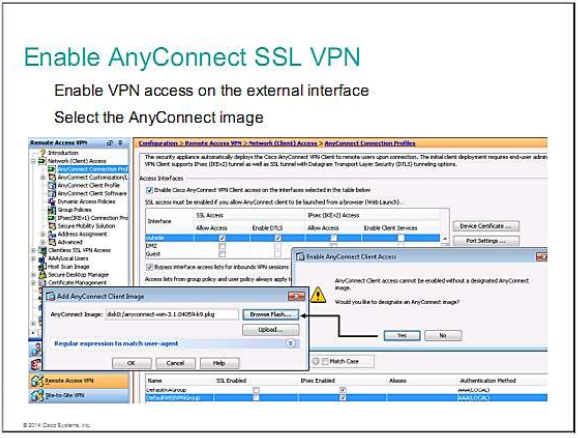
To increase authentication strength provided by static passwords, consider using client certificates or one-time passwords, at the expense of management complexity and cost.

On the the PCs that will access the VPN, you will need to complete following steps:

1. Join the PC to the Active Directory
2. Assign administrative privileges to domain users. They will need administrative privileges to install the AnyConnect client software that is pushed to them by the Cisco ASA.
3. Use the Certificate Manager console, on the Windows-based PCs, to install the user certificate for the user. The user certificate is used for certificate-based client authentication.

Enable AnyConnect SSL VPN

This topic describes how to enable AnyConnect SSL VPNs.

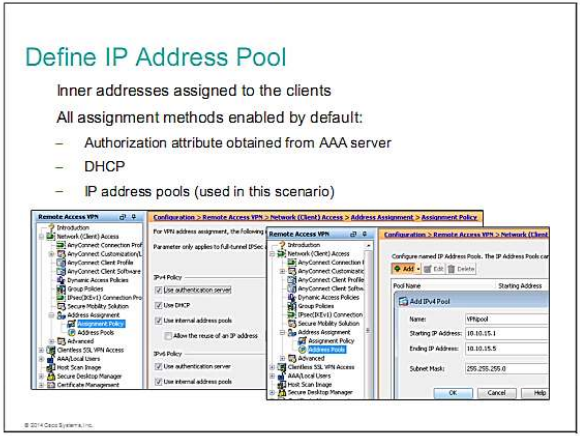


As prerequisites for an AnyConnect SSL VPN deployment you need to provision an identity server SSL/TLS certificate to the Cisco Adaptive Security Appliance and installing the Cisco AnyConnect client software image on the Cisco ASA. These tasks are not shown in this procedure.

You can globally enable the SSL VPN function on the Cisco ASA and choose the interfaces on which the appliance will accept SSL VPN sessions. You can also optionally configure support for DTLS, which is automatically negotiated if the path between the client and the Cisco ASA supports it. Additionally, you can allow the user to choose a connection profile at login. This setting is required if you want to assign users to a specific connection profile rather than having them use the default DefaultWebVPNGroup profile.

Define IP Address Pool

This topic describes how to define an IP address pool.

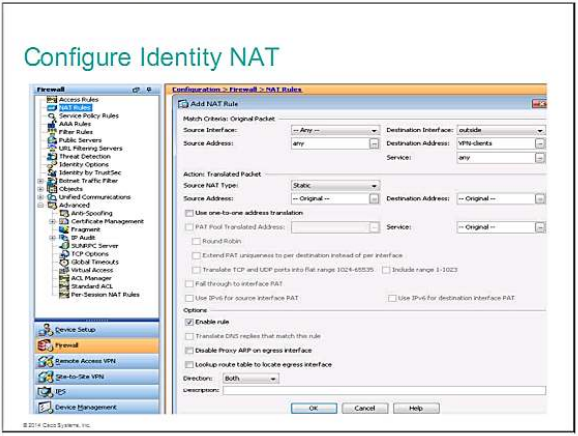


You need to configure an IP address assignment method. By default, all available methods (authorization attributes obtained from an AAA server, DHCP, and internal IP address pools) are enabled. In this scenario a local IP address pool is configured.

The IP addresses assigned to the VPN clients will be used as the inner (or internal) AnyConnect IP addresses. The inner IP address is applied to the virtual VPN adapter on the client system. The virtual VPN adapter is created during the VPN establishment phase in addition to any physical adapters on the client endpoint.

Configure Identity NAT

This topic describes the configuration of identity NAT for VPN clients.

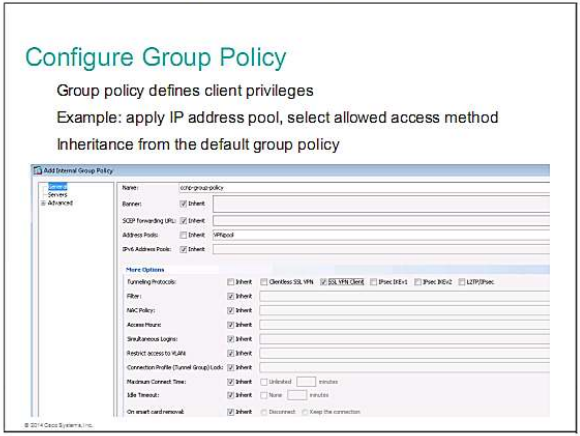


If address translation is enabled on the Cisco Adaptive Security Appliance, you will typically configure identity NAT for the VPN client access. Identity NAT causes the IP addresses of the internal resources to be unchanged in communications through the VPN tunnel. This allows the VPN clients to access the internal resources as if they were connected to the inside networks.

The destination addresses in this NAT rule refer to the address pool that is being assigned to the clients. The NAT type is static. The source and destination IP address will be retained at their original values. The direction is set for bidirectional communication.

Configure Group Policy

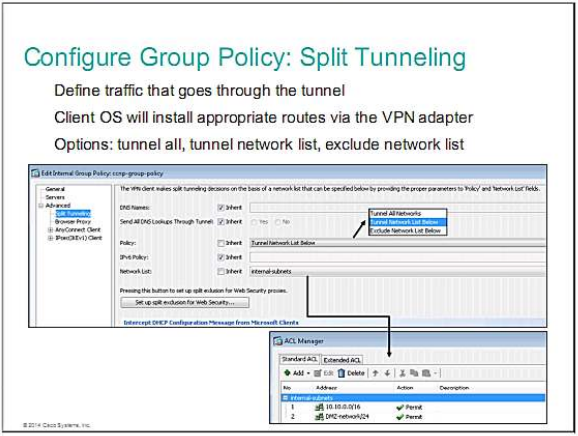
This topic describes the general settings configured in a group policy.



The group policy defines the privileges and attributes applied to the client session. You can either use the default group policy, or create a custom one. In this scenario a custom group policy is created. The custom group policy contains the selection of an IP address pool and defines the permitted VPN access methods. For SSL VPN full tunnel access, you need to enable the SSL VPN Client method.

Configure Group Policy: Split Tunneling

This topic describes the split tunneling configuration in a group policy.

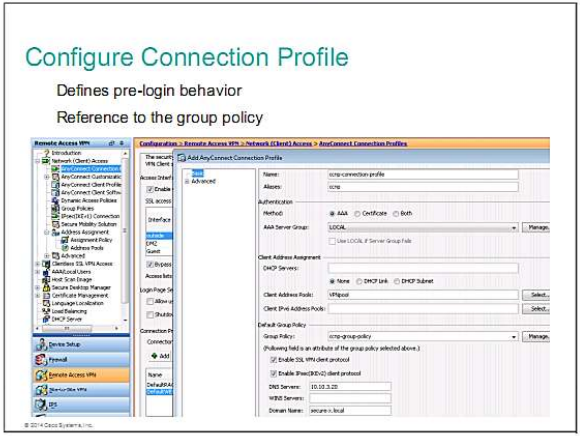


The group policy settings include the split tunneling configuration. If you do not configure split tunneling, all client traffic will go through the VPN tunnel. If you want to permit the clients direct access to external resources, you need to enable split tunneling. You can select the traffic that the clients will forward through the tunnel using one of three methods: tunnel all networks, tunnel network list, exclude network list.

This scenario uses the tunnel network list option. The internal-subnets standard ACL lists the inside and DMZ subnets that should be accessible through the tunnel. The VPN routed will be routed via the virtual VPN adapter. The client will communicate with all other destinations via the physical adapter.

Configure Connection Profile

This topic describes the configuration of a connection profile.

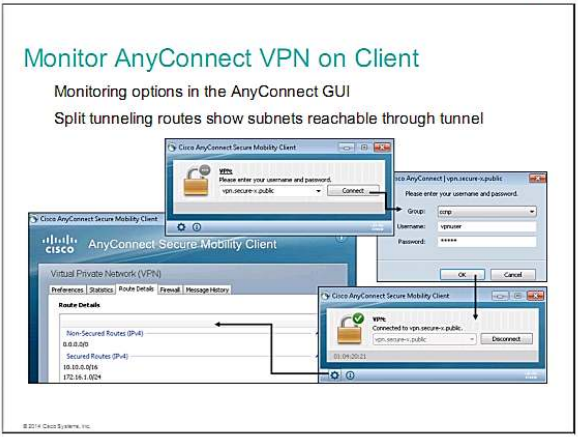


The connection profiles are used to define the pre-login behavior of the remote endpoints. They can also point to the group policy that will be applied to the clients. You can either use the default connection profile or create your custom profiles.

In this scenario a custom connection profile (ccnp-connection-profile) is created. The VPN users will be allowed to select this connection based on its alias (ccnp). The authentication will be performed against the local user database. The clients will obtain their inner IP addresses from the IP address pool (VPNpool). The connection profile refers to the custom group policy (ccnp-group-policy) that will be applied to the client session. The DNS server and domain name are also set.

Monitor AnyConnect VPN on Client

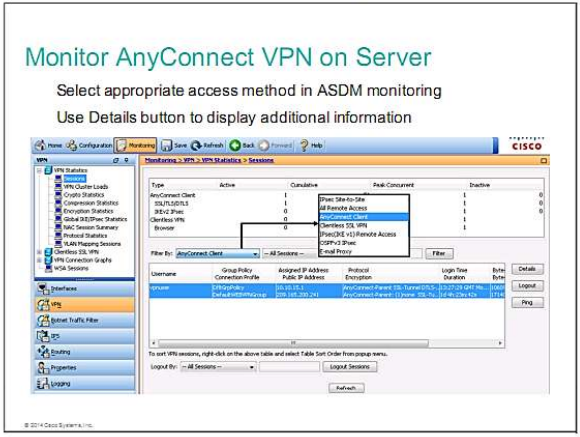
This topic describes how to monitor the AnyConnect VPN operation on the client endpoint.



Once the AnyConnect client software is installed on the endpoint, the user will connect to the VPN name or IP address. If the Cisco Adaptive Security Appliance administrator permitted the VPN users to select the connection profile, the user will choose the desired alias, provide access credentials and the tunnel will be established. When the tunnel is established, the AnyConnect user interface offers several monitoring capabilities. The Route Details tab displays the networks that are reachable through the tunnel. The network list is obtained is from the ASA as a result of the split tunneling configuration.

Monitor AnyConnect VPN on Server

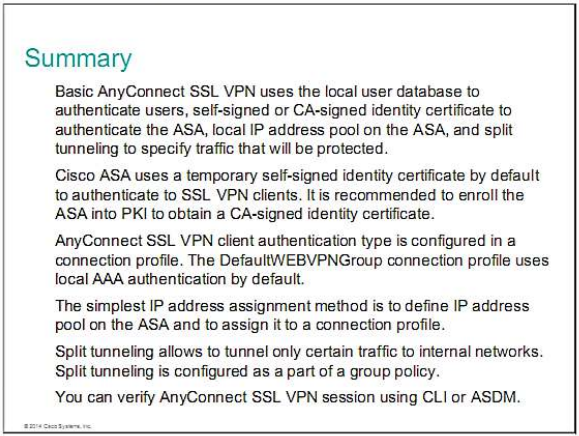
This topic describes how to monitor the AnyConnect VPN operation on the server.



You can use the Cisco Adaptive Security Appliance monitoring capabilities to view the VPN operation on the server. You can use the Cisco Adaptive Security Device Manager monitoring and various CLI commands to examine the established connections. This example illustrates how to display the VPN tunnels in the ASDM monitoring. You need to select the VPN access method that you want to examine. The ASDM provides information about the selected connection profile, the applied group policy, the transport protocol, and crypto parameters. The ASDM allows you to click the **Details** button if you want to investigate additional information. You can also disconnect a given session.

Summary

This topic summarizes the key points that were discussed in this lesson.



Lesson 2

Deploying Advanced Cisco AnyConnect SSL VPN on Cisco ASA

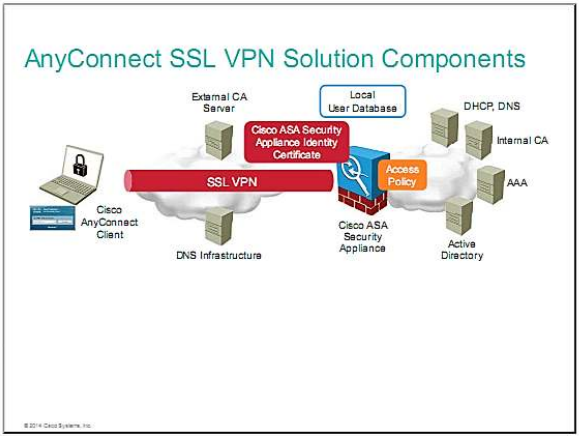
When you combine the Cisco AnyConnect VPN client with a Cisco Adaptive Security Appliance that is configured as an SSL VPN gateway, you can provide full-tunnel SSL VPN services to remote workers. This lesson describes how to deploy advanced full-tunnel SSL VPN features, such as DTLS. The lesson also describes how to manage Cisco AnyConnect client settings, lists options of integrating the Cisco AnyConnect client with the operating system, describes the Cisco AnyConnect client SBL feature and describes Cisco AnyConnect Trusted Network Detection.

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

- Describe Cisco AnyConnect SSL VPN solution components
- Describe DTLS
- Describe the parallel DTLS and TLS tunnels
- Describe DTLS configuration
- Describe how to verify DTLS
- Describe how to manage Cisco AnyConnect client settings
- Describe how to deploy Cisco AnyConnect Software management
- Describe the options of integrating the Cisco AnyConnect client with the operating system
- Describe how to configure Cisco AnyConnect Trusted Network Detection
- Describe the Cisco AnyConnect client SBL feature
- Describe how to configure Cisco AnyConnect Start Before Logon

Cisco AnyConnect SSL VPN Solution Components

This topic describes the Cisco AnyConnect SSL VPN environment.

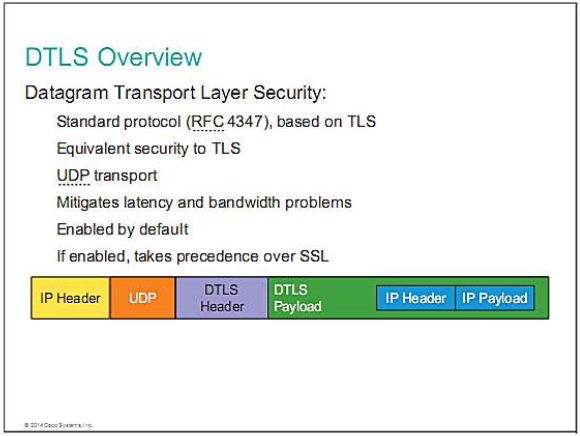


In the Cisco AnyConnect full-tunnel remote access SSL VPN solution, you use the Cisco AnyConnect Secure Mobility Client version 3.1 (Cisco AnyConnect 3.1) to establish a SSL/TLS tunnel with the Cisco Adaptive Security Appliance. The solution uses bidirectional authentication, in which the client authenticates the Cisco ASA with a certificate-based authentication method and the Cisco ASA authenticates the user using certificates and a local or external user database, or a combination.

After authentication, the security appliance applies a set of authorization and accounting rules to the user session. When the Cisco ASA has established an acceptable VPN environment with the remote user, the remote user can forward raw IP traffic into the SSL/TLS tunnel. The Cisco AnyConnect 3.1 client creates a virtual network interface to provide this functionality. The client can use any application to access any resource behind the Cisco ASA VPN gateway, subject to access rules that are applied to the VPN session.

DTLS Overview

This topic describes DTLS.



DTLS is an alternative VPN transport protocol to SSL/TLS. DTLS allows datagram-based applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. The DTLS protocol is based on the stream-oriented TLS protocol and is intended to provide similar security guarantees.

DTLS mitigates latency and bandwidth problems that are associated with some SSL-only connections, and improves the performance of real-time applications (such as voice and video applications) that are sensitive to packet delays. DTLS is a standards-based SSL protocol that provides a low-latency data path using UDP. It is defined in RFC 4347.

DTLS improves the application performance in two ways:

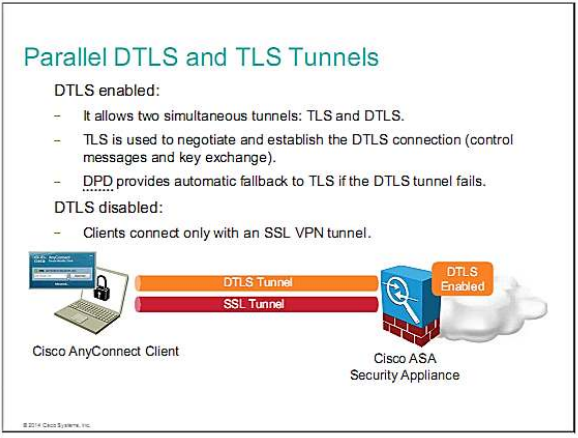
UDP transport does not stipulate any retransmissions on the VPN layer. If VPN packets are lost in transit, only the TCP stack of the application endpoints will retransmit the datagrams. In contrast, when VPN packets that are transported over an SSL session are lost, both the SSL VPN endpoint and the TCP stack of the application endpoint will retransmit the packet.

UDP is simpler than TCP, creates less overhead, and consumes fewer resources.

Note The DTLS is only capable of running in an AnyConnect SSL VPN and not in IKEv2.

Parallel DTLS and TLS Tunnels

This topic describes the parallel DTLS and TLS tunnels.



Enabling DTLS enables the Cisco AnyConnect VPN client that is establishing an SSL VPN connection to use two simultaneous tunnels—a TLS tunnel and a DTLS tunnel. The SSL/TLS tunnel is used to negotiate and establish the DTLS tunnel by exchanging a series of secured control and key exchange messages.

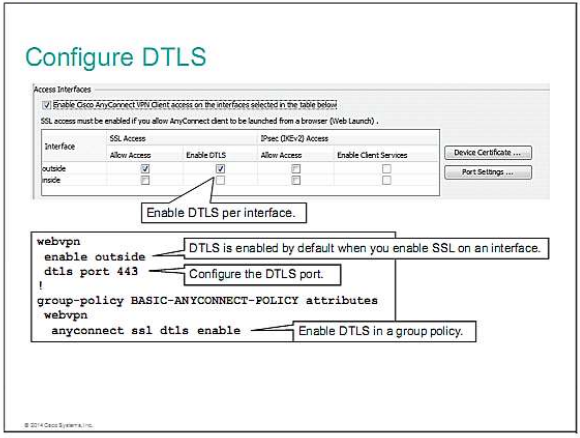
The security appliance supports an automatic fallback from DTLS to TLS if DTLS is no longer working. The DTLS-to-TLS fallback requires you to enable DPD. DPD is a keepalive feature that ensures that the remote end is still reachable. If the DTLS tunnel does not work and DPD is not enabled, connectivity is broken.

Note One more important aspect to consider is that although DPD packets can be initiated by both the Cisco Adaptive Security Appliance and AnyConnect, the client decides which tunnel (DTLS or TLS) to send packets over; the ASA just follows. The ASA will always send packets back toward the client over the tunnel it last received packets on.

The DTLS is only capable of running in an AnyConnect SSL VPN (not IKEv2). By default, DTLS is enabled globally when an interface is first enabled for SSL termination. However, if DTLS has been globally disabled, you might need to re-enable it on an interface for all AnyConnect SSL VPN users for successful delay-sensitive operation of their applications.

Configure DTLS

This topic explains how to configure DTLS.



The first step to configure DTLS, shown in the figure, is to ensure that DTLS is enabled globally. After you enable DTLS, you can activate it in a group policy or an individual user setting, but this option is not shown as a GUI screen shot.

You can configure DTLS in both a group policy and local user account in the following Cisco Adaptive Security Device Manager locations:

Group policy configuration: **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**. Choose the group policy object and click **Edit**. Then, in the Edit Internal Group Policy: name window, expand **Advanced > AnyConnect Client**.

User account configuration: **Configuration > Remote Access VPN > AAA/Local Users > Local Users**. Choose the user account from the list and click **Edit**. Then, in the Edit User Account window, expand **VPN Policy > AnyConnect Client**.

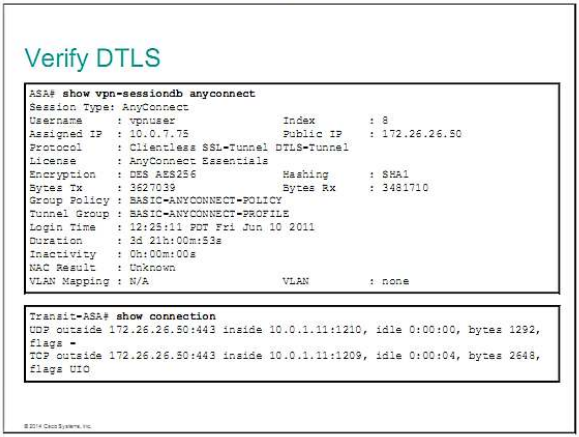
In both locations, uncheck the **Inherit** check box next to DTLS, and ensure that the **Enable** check box is checked. Enable is the default setting.

In the CLI configuration, the **enable outside** command enables SSL VPN on the outside interface. When you enable SSL VPN on an interface, DTLS is enabled by default. Use the **dtls port** command in webvpn configuration mode to set the DTLS port number. The default port is 443 and does not show in the configuration. In the example, the DTLS port is set to port 443.

To enable DTLS in a group policy, enter the webvpn configuration mode of a group policy and enter the **anyconnect ssl dtls enable** command. In the example, DTLS is enabled in the BASIC-ANYCONNECT-POLICY group policy.

Verify DTLS

This topic describes how to verify the DTLS transport.

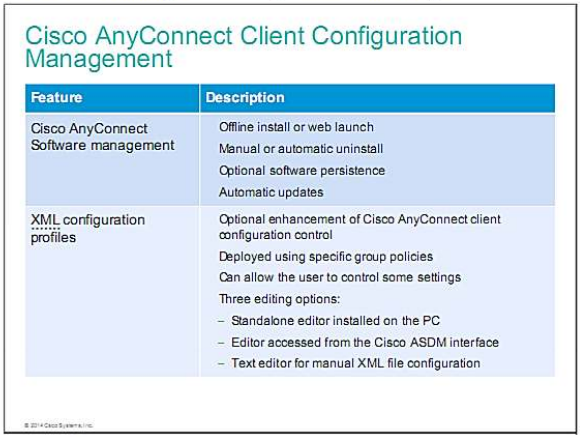


In the example, DTLS was enabled on the outside interface and the group policy (BASIC-ANYCONNECT-POLICY) that is associated with the user who logged in was configured to have DTLS enabled. You can use the **show vpn-sessiondb** command to verify the protocol in use for the connection.

The **show connection** command output in the figure is from a security appliance that resides in the VPN path. It shows an established UDP connection and an SSL session.

Cisco AnyConnect Client Configuration Management

This topic describes how to manage the Cisco AnyConnect client settings.



You can distribute and upgrade Cisco AnyConnect on workstations using several delivery methods:

Predeployment (manual) method: This method uses an installation package that you download from http://www.cisco.com to the client PC, and a standalone installer on the client PC, such as the MSI installer for Microsoft Windows systems. This method is best suited for clients with a higher level of experience or for those users that have a slow Internet connection.

Software management tools: You can install Cisco AnyConnect to your clients using software management tools, such as Symantec Altiris or Microsoft SMS. This method is preferred for installations in large organizations that have an established infrastructure for software package deployment. Cisco AnyConnect installation is available in the MSI format for the Windows platform, the PKG format for Linux and the Mac OS X Intel platform, and the DMG format for the Mac OS platform.

Web launch (installation over the SSL VPN clientless portal): If Cisco AnyConnect is not already installed on the client PC, the remote user can use a web browser to download and install the software from a Cisco Adaptive Security Appliance. The remote user establishes an SSL connection to the security appliance that is configured to manage a web launch. When the user establishes the connection, the Cisco ASA presents a login window to the client. After the user successfully authenticates, the security appliance identifies the user as requiring the Cisco AnyConnect software. It then uploads to the remote PC the Cisco AnyConnect client that matches the operating system of the remote PC. After the software uploads, the Cisco AnyConnect client installs and configures itself and establishes a secure full-tunnel SSL connection.

The method that you choose depends on the experience level of the client and the security policy of your network. You can use several methods to uninstall the Cisco AnyConnect software:

Manually, using a computer operating system program manager

Using software management tools

Using automatic uninstall that is triggered by the security appliance after logout. If the Cisco AnyConnect software was installed over a web portal using a web launch, you can configure the software to automatically uninstall after a client logs off the security appliance.

If Cisco AnyConnect is already installed on a client, you can configure the Cisco ASA to examine the revision of the Cisco AnyConnect software when the user authenticates. The Cisco ASA can then upgrade the Cisco AnyConnect software that is on the remote computer, if necessary.

XML Configuration Profiles

You can enable Cisco AnyConnect client features in the Cisco AnyConnect profiles. Cisco AnyConnect profiles are XML files that contain configuration settings for the core client VPN functionality and for the optional Network Access Manager, posture, telemetry, and Web Security client modules. The Cisco ASA deploys the profiles during a Cisco AnyConnect installation or update. Users cannot manage or modify these profiles.

Some profile settings are stored locally on the remote computer in a user preferences file or a global preferences file. The user file has information that Cisco AnyConnect uses to display user-controllable settings on the Preferences tab of the client. The user file also has information about the last connection, such as the user, the group, and the host.

The global file has information about user-controllable settings that must be applied before login. For example, Cisco AnyConnect needs to know if SBL or AutoConnect On Start is enabled before the user logs in.

The Cisco AnyConnect client profile is an XML-formatted file that contains all of the configured Cisco AnyConnect client parameters. Standard XML format is a collection of beginning and ending tags with configuration values between them. It is recommended that you use a Cisco AnyConnect Profile Editor to initially create an XML profile, because it will correctly define the file structure. After the file is created, you can use a text editor or the Profile Editor to edit the profile.

There are two ways to create or modify the **AnyConnectProfile.xml** file:

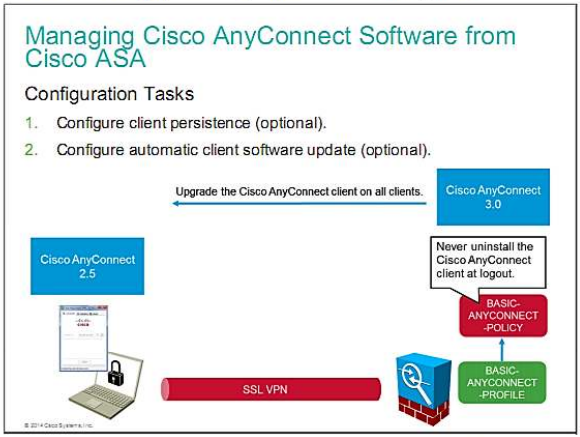
Manual Method - Using the manual method, you can create or modify the **AnyConnectProfile.xml** file by using any XML Editor such as XML Note pad or Arbortext.

Profile Editor - A better approach is to use a Cisco AnyConnect Profile Editor. This avoids syntax errors and simplifies the creation and configuration of client profiles. There is a Cisco AnyConnect Profile Editor integrated into Cisco Adaptive Security Device Manager. There are also standalone versions of the profile editors for Windows that you can use as an alternative to the profile editor integrated with ASDM. If you are predeploying the client, you can use the standalone profile editors to create profiles for the VPN service and other modules that you deploy to computers using your software management system. You can download the standalone profile editor file from http://www.cisco.com. To locate the file, search http://www.cisco.com for anyconnect-profileeditor.

You are not required to use XML profiles. You can use them only when you need to change default Cisco AnyConnect client settings or add advanced features.

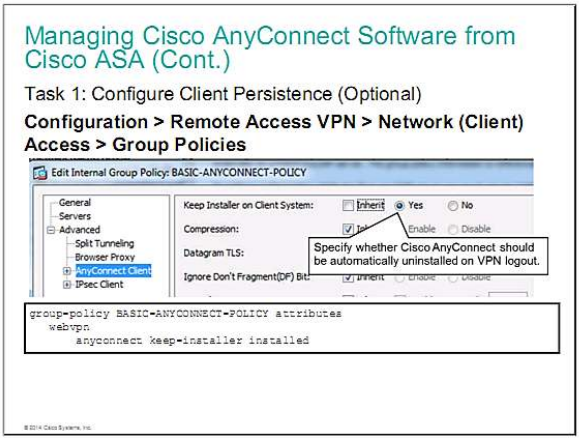
Managing Cisco AnyConnect Software from Cisco ASA

This topic describes how to deploy Cisco AnyConnect Software management.



The configuration scenario for this topic uses the Cisco Adaptive Security Appliance to upgrade a client that has Cisco AnyConnect Version 2.5 to Cisco AnyConnect Secure Mobility Client version 3.0 (Cisco AnyConnect 3.0). After Cisco AnyConnect 3.0 is installed, the software will establish an SSL tunnel to the Cisco ASA. For this scenario, after the user logs off, the security appliance will keep Cisco AnyConnect installed on the client PC.

When you upgrade to Cisco AnyConnect 3.0 from an earlier version, all of the core components of the client are upgraded but the VPN configurations are retained.

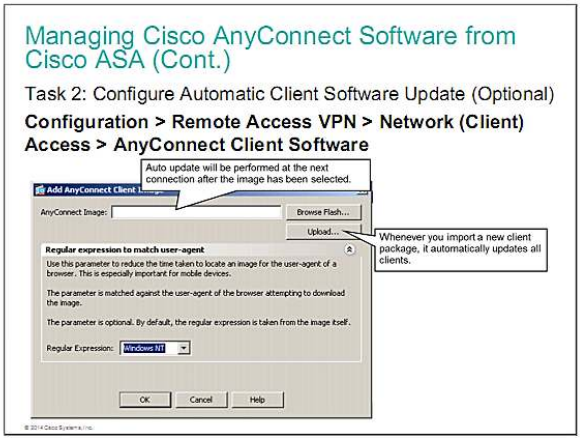


You can configure Cisco AnyConnect to remain installed on a remote computer after client logout. Follow these steps to configure this option:

1. From Cisco Adaptive Security Device Manager, choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** (not shown in the figure).
2. Select the group policy that you want to edit and click **Edit** (not shown in the figure). The Edit Internal Group Policy window appears.
3. Choose **Advanced > AnyConnect Client**.
4. Uncheck the **Inherit** check box next to the Keep Installer on Client System field. To allow a permanent Cisco AnyConnect software installation on the remote computer, click **Yes**. By clicking Yes, you disable the automatic uninstallation feature of the Cisco AnyConnect software and allow the software to remain installed on the remote computer for subsequent connections.
5. Click **OK** and click **Apply** to apply the changed policy to the security appliance.

Follow these steps to use the CLI to configure Cisco AnyConnect to remain installed on the remote computer after a client logout:

1. Enter the **group-policy** ***policy-name*** **attributes** command to enter the group-policy configuration mode.
2. To enter the configuration mode for the SSL VPN properties of the group policy, enter the **webvpn** command.
3. In webvpn configuration mode, enter the **anyconnect keep-installer installed** command to allow Cisco AnyConnect to remain installed on the remote computer.



You can also configure the Cisco ASA to upload the correct Cisco AnyConnect version to the client. To determine the correct version to upload, the security appliance matches a regular expression against a user agent string that the browser of the remote computer reports.

If you do not enter a regular expression parameter, the security appliance tries to match the operating system that the user agent of the browser reports with the operating system string that is in the Cisco AnyConnect installation filename.

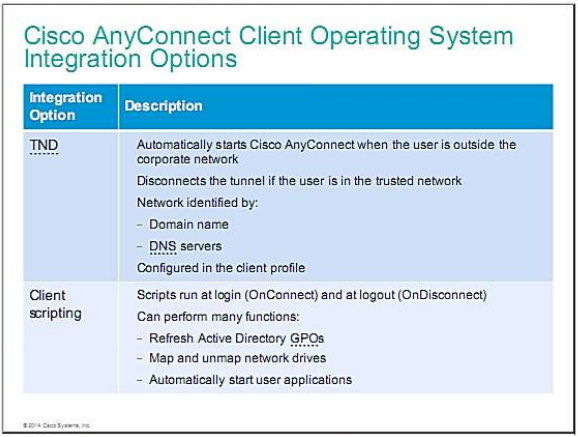
Follow these steps to configure this option:

1. Choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Software** (not shown in the figure).
2. Click **Add** to add the Cisco AnyConnect installation image from the flash memory of the Cisco ASA (not shown in the figure). The **Add AnyConnect Client Image** window appears.
3. Click **Browse Flash**. Locate the Cisco AnyConnect installation image and select it. Click **OK**. (This step is not shown in the figure.)

   If the file version that the AnyConnect Client Images window lists is higher than the file version on the remote computer, the Cisco AnyConnect software is updated on the remote computer.
4. Optionally, enter or choose a regular expression to match the user agent of a browser to reduce the time it takes for the security appliance to locate the correct image.
5. Click **OK** to close the Add AnyConnect Client Image window and click **Apply** to apply the changed policy to the security appliance.

Cisco AnyConnect Client Operating System Integration Options

This topic describes the options of integrating the Cisco AnyConnect client with the operating system.



The TND feature enables Cisco AnyConnect to automatically disconnect a VPN connection when the user is inside the corporate network (the trusted network) and start the VPN connection when the user is outside the corporate network (the untrusted network). This feature provides greater security awareness by initiating a VPN connection when the user is outside the trusted network.

If Cisco AnyConnect is also running SBL and the user moves into the trusted network, the SBL window that is displayed on the computer automatically closes.

TND does not interfere with the ability of the user to manually establish a VPN connection. It does not disconnect a VPN connection that the user starts manually in the trusted network. TND only disconnects the VPN session if the user first connects in an untrusted network and moves into a trusted network. For example, TND disconnects the VPN session if the user makes a VPN connection at home and then moves into the corporate office.

Because the TND feature controls the Cisco AnyConnect GUI and automatically initiates connections, the Cisco AnyConnect GUI should run at all times. If the user exits the GUI, TND does not automatically start the VPN connection.

Client Scripting

Cisco AnyConnect lets you download and run scripts when the following events occur:

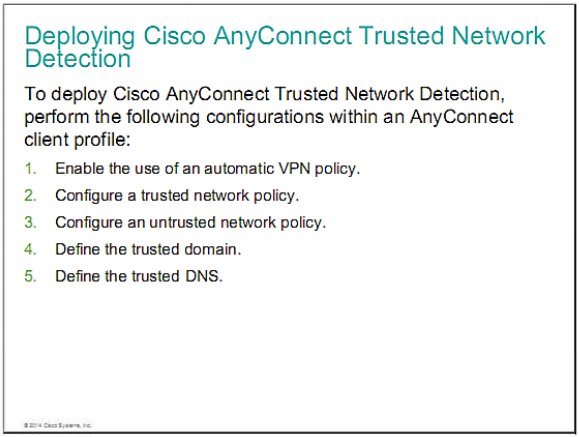
- A new client VPN session establishes with the security appliance. This method is referred to as an OnConnect script.
- A VPN session tears down. This method is referred to as an OnDisconnect script.

Client scripts can run if you are using SBL or TND, but they do not require these features to function.

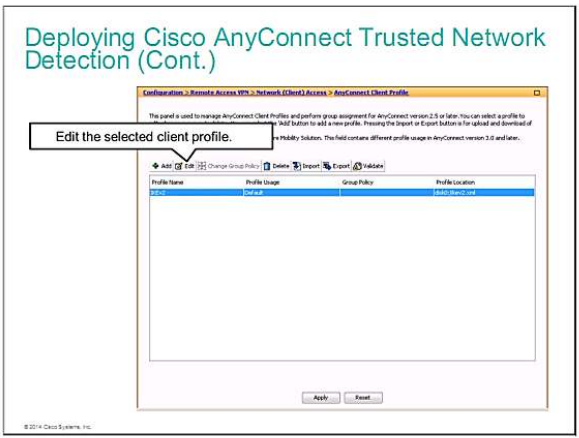
Common uses for this feature are to refresh the group policy upon VPN connection, map a network drive upon VPN connection, and unmap the network drive after disconnection. However, you can use this feature to perform any task that you can perform from a script at the command line.

Deploying Cisco AnyConnect Trusted Network Detection

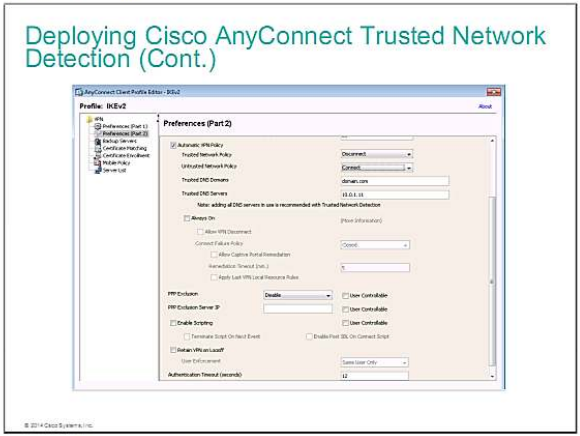
This topic describes how to configure Cisco AnyConnect Trusted Network Detection.



The figure lists the configuration tasks for deploying Cisco AnyConnect Trusted Network Detection. These tasks are performed within an AnyConnect client profile.



The figure shows the Cisco Adaptive Security Device Manager AnyConnect Client Profile panel, where you can configure client profiles. To access this panel, choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**. To configure TND within a profile, choose the client profile for which you want to configure TND and click **Edit**. The AnyConnect Client Profile Editor window for that profile is displayed.



The figure shows the AnyConnect Client Profile Editor window.

To configure TND, choose **VPN > Preferences (Part 2)** from the navigation pane. Then follow these steps:

1. Click the **Automatic VPN Policy** check box.
2. Choose a **Trusted Network Policy** from the drop-down list. Cisco AnyConnect takes this action when the user is inside the corporate network (the trusted network). There are four options:
   - **Connect:** Cisco AnyConnect initiates a VPN connection in the trusted network.
   - **Pause:** Cisco AnyConnect suspends the VPN session (instead of disconnecting it) if a user enters a network that is configured as trusted after establishing a VPN session outside the trusted network. When the user goes outside the trusted network again, Cisco AnyConnect resumes the session. This feature is for the convenience of the user because it eliminates the need to establish a new VPN session after leaving a trusted network.
   - **Disconnect:** Cisco AnyConnect terminates the VPN connection in the trusted network.
   - **Do Nothing:** Cisco AnyConnect takes no action in the trusted network. Setting both the Trusted Network Policy and Untrusted Network Policy to **Do Nothing** disables TND.
3. From the Untrusted Network Policy drop-down list, choose the action to take when an untrusted network is detected. The options are Connect and Do Nothing. The Do Nothing option disables always-on VPN.
4. In the Trusted DNS Domains field, specify the trusted DNS domains.
5. In the Trusted DNS Servers field, enter the IP addresses of the trusted DNS servers.

When you have completed your configuration, click **OK** in the AnyConnect Client Profile Editor window and then **apply** your changes.

Cisco AnyConnect Start Before Logon

This topic describes the Cisco AnyConnect client SBL feature.

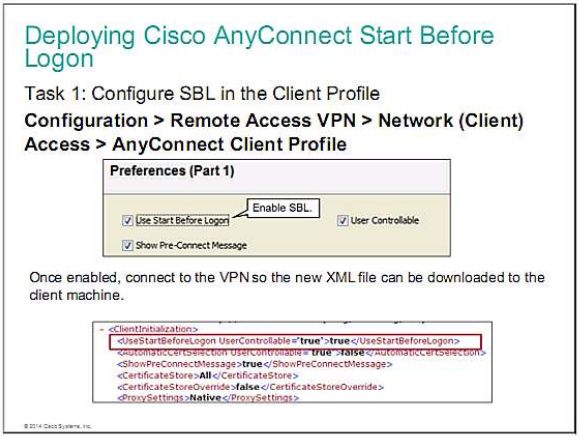
SBL starts the Cisco AnyConnect client before the Windows login dialog box appears, which forces the user to connect to the enterprise infrastructure over a VPN connection before logging into Windows. After the user authenticates to the Cisco Adaptive Security Appliance, the Windows login dialog appears and the user logs in, as usual.

SBL is only available for Windows. It lets you control the use of login scripts, password caching, mapping network drives to local drives, and more.

As part of the SBL configuration procedure, you must install the SBL components on the Windows machine. This installation package is located in the Cisco AnyConnect 3.0 ISO image that you download from http://www.cisco.com. After you install this package, it enables the PLAP capability in Windows.

Deploying Cisco AnyConnect Start Before Logon

This topic describes how to configure Cisco AnyConnect Start Before Logon.



To enable the SBL feature, you must make changes to the AnyConnect profile and enable the Cisco Adaptive Security Appliance to download an AnyConnect module for SBL.

The first task to configure SBL is to enable SBL in the Cisco AnyConnect client profile. Follow these steps to perform this task:

1. Launch the profile editor from Cisco Adaptive Security Device Manager.
2. Go to the Preferences pane and check the **Use Start Before Logon** check box.
3. To give the remote user control over using SBL, check the **User Controllable** check box. This step is optional.

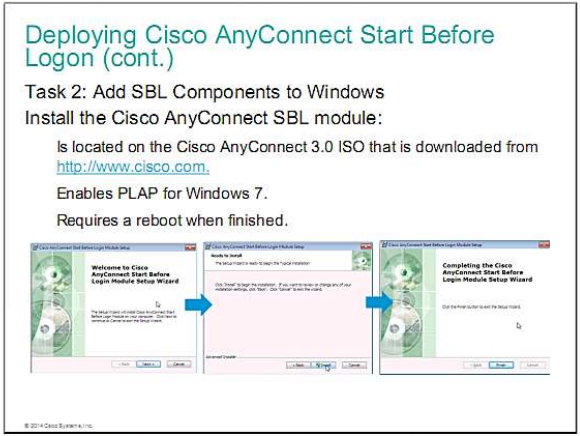
After you enable the SBL feature, the user must update the locally stored XML client profile, which means that the user must connect to the VPN again for the profile to download the update. After the user has downloaded the update and the SBL client components are installed, the SBL feature can be used.

This figure shows an updated XML profile in which the UseStartBeforeLogon feature is set to True. You can verify this by navigating to C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile directory and viewing the downloaded profile.

To minimize download time, AnyConnect requests downloads (from the ASA) only of core modules that it needs for each feature that it supports. To enable SBL, you must specify the SBL module name in group policy on the ASA. Follow this procedure:

1. Go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.
2. Select a group policy and click **Edit**.
3. Select **Advanced > AnyConnect Client** in the left navigation pane. AnyConnect Client settings display.
4. Uncheck **Inherit** for the Optional Client Module for Download setting.

5. Select the **AnyConnect SBL** module in the drop-down list.



The next task is to install the SBL components on the Windows machine. This installation package is located in the Cisco AnyConnect 3.0 ISO image that you download from http://www.cisco.com. After you install this package, it enables the PLAP capability in Windows.

The way that you enable SBL differs between systems that run Windows 7, Windows Vista, and Windows versions prior to Windows Vista. Windows versions that are prior to Windows Vista use a component called VPNGINA (which stands for virtual private network graphical identification and authentication) to implement SBL. Windows 7 and Windows Vista use PLAP to implement SBL.

PLAP is a connectable credential provider. This feature lets network administrators perform specific tasks, such as collecting credentials or connecting to network resources, prior to a user login. PLAP supports 32-bit and 64-bit versions of the operating system with vpnplap.dll and vpnplap64.dll, respectively. The PLAP function supports Windows 7 and Vista x86 and x64 versions.

Deploying Cisco AnyConnect Start Before Logon (cont.)

Task 3: Log into Windows Using SBL

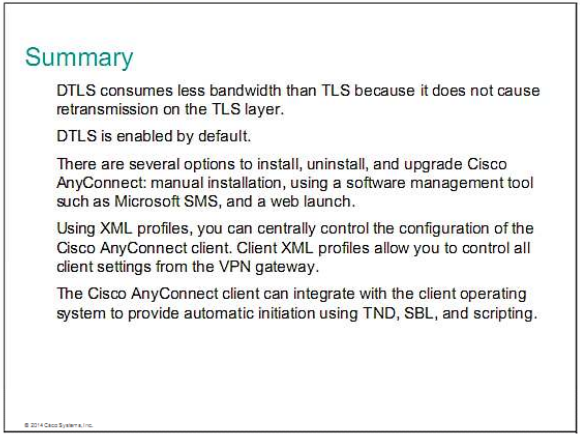
1. Click **Switch User**.
2. Click the **Network Connect** button to initiate a login.
3. Click **Connect**.
4. Enter the credentials for the VPN Connection (not shown).
5. Click the admin icon and log into Windows (not shown).

The process for SBL on Windows Vista and Windows 7 is similar. The user typically initiates the process by pressing Ctrl-Alt-Delete. With PLAP, the Ctrl-Alt-Del key combination opens a window from which the user can either click the **Switch User** button to enable PLAP or log into the system and bypass SBL. If the user clicks the **Switch User** button, the **Network Connect** button appears in the lower right corner of the screen. When the user clicks the **Network Connect** button, a Cisco AnyConnect window appears, from which the user can initiate the connection process.

Note A user still has the capability to log into the machine and bypass SBL. To bypass SBL, do not click the **Switch User** button, just log into Windows as usual. To force the use of SBL, use the Trusted Network Detection feature or an always-on configuration.

Summary

This topic summarizes the key points that were discussed in this lesson.



Lesson 3

Deploying Advanced Authentication and Authorization in Cisco AnyConnect VPNs

This lesson explains how to deploy advanced full-tunnel SSL VPN features, such as complex authentication scenarios and authorization.

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

- Describe advanced authentication scenarios in the Cisco AnyConnect SSL VPN
- Describe certificate-based server authentication options
- Describe certificate-based client authentication options
- Describe the use of the SCEP proxy in Cisco AnyConnect SSL VPNs
- Describe the PKI integration features
- Describe local authorization
- Describe the two-factor user authentication
- Describe two-factor authentication with username pre-fill
- Describe local authorization
- Describe the configuration procedure for local authorization
- Describe how to configure local authorization
- Describe how to verify local authorization
- Describe an external authorization scenario

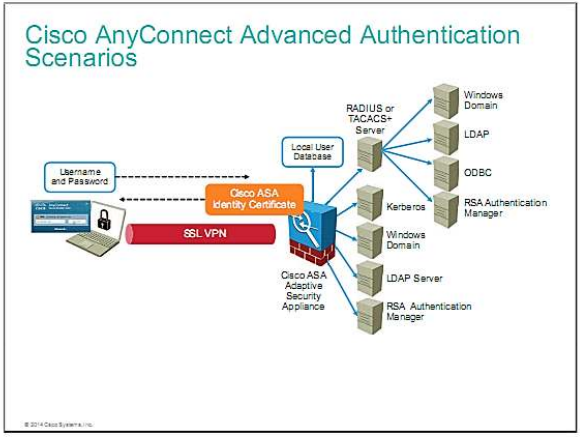
Describe the deployment of SSL VPN authorization using an external RADIUS server

Describe the monitoring of external authorization

Describe how to troubleshoot Cisco AnyConnect VPN

Cisco AnyConnect Advanced Authentication Scenarios

This topic describes advanced authentication scenarios in the Cisco AnyConnect SSL VPN.



Advanced authentication options for Cisco AnyConnect SSL VPN users include the following:

Centralized AAA authentication: You can authenticate clients with an existing external AAA database, such as a RADIUS or TACACS+ user database. Such an external database can also be integrated with other back-end databases, such as RSA SecurID or Microsoft Active Directory.

Authentication with digital certificates: You can configure the Cisco Adaptive Security Appliance to require digital certificates on clients. Before establishing a connection, the security appliance validates the certificate of a client and allows connection establishment only if the certificate can be validated using a public key that is stored on the certificate of a trusted CA.

Double and triple authentication: Starting with Cisco ASA Software Version 8.2, the SSL VPN remote-access (clientless and Cisco AnyConnect VPN Client) software supports double and triple authentication. You can combine certificate authentication with up to two AAA authentication methods that are performed sequentially. The following examples are possible combinations that can be used:

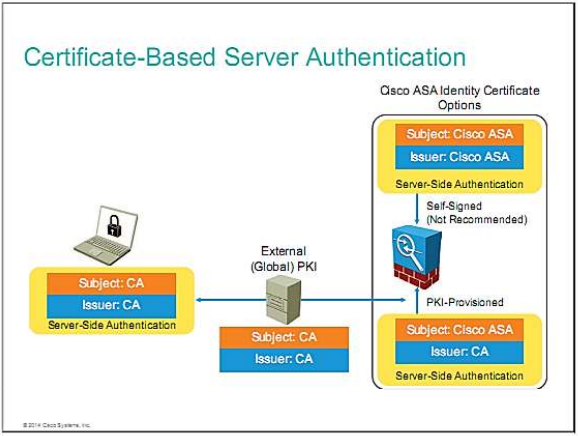
- RSA/SDI + LDAP authentication
- Certificates + RADIUS
- Certificates + RADIUS + RSA/SDI

The advanced client authentication types are deployed to enhance the manageability of users, to integrate VPN deployments with an existing user database infrastructure, or to increase strength of client authentication.

Their implementation is identical to the same methods deployed in clientless SSL VPNs.

Certificate-Based Server Authentication

This topic describes certificate-based server authentication options.



When you authenticate using digital certificates, you have different deployment options. For server authentication, you can deploy the Cisco Adaptive Security Appliance identity certificate in two ways:

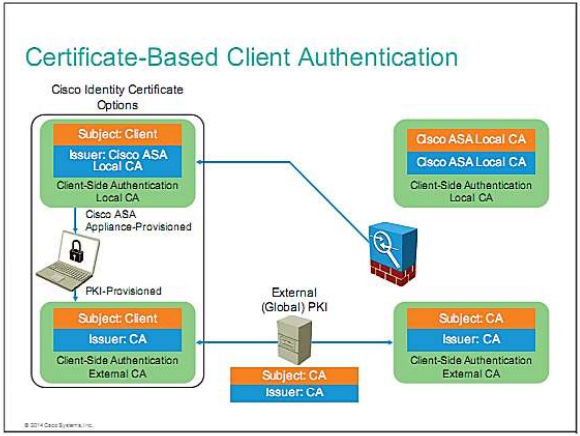
Self-signed certificate: This option is not recommended, but it is the only approach if you do not use external PKI.

PKI-obtained certificate: You can configure the Cisco ASA to obtain an identity certificate from the external PKI.

If you are using a PKI-obtained certificate, clients should have a CA certificate that is installed locally to verify the identity certificate of a server.

Certificate-Based Client Authentication

This topic describes certificate-based client authentication options.



For client-side authentication, clients can obtain their identity certificates using two different options:

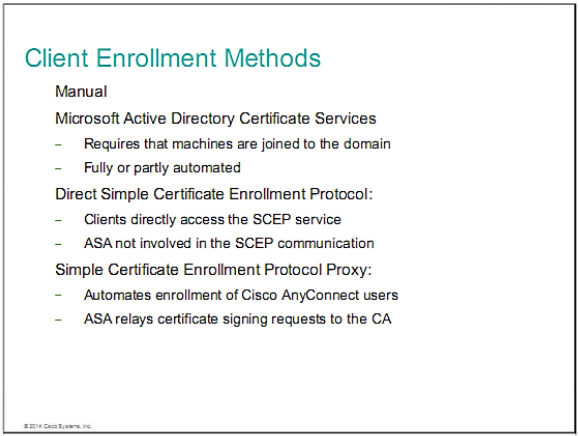
- You can enable a local CA on the Cisco Adaptive Security Appliance. In this case, the certificates of clients are issued and managed by the security appliance. The appliance still needs a self-signed or PKI-provided certificate to authenticate itself to clients.
- You can use an external PKI to issue identity certificates to the Cisco ASA and clients. In this case, certificates are managed by an external PKI system.

If you are using a PKI-obtained certificate, the server should have a CA certificate that is installed locally to verify the identity certificates of clients. If you are using a local CA on the security appliance, the appliance will create a self-signed certificate, which is used to sign certificates that are issued to clients.

Note The local CA on the Cisco ASA can be used for SSL VPNs only.

Client Enrollment Methods

This topic describes the use of the SCEP proxy in Cisco AnyConnect SSL VPNs.



Using client certificates for authentication is hindered by the difficulty of enrolling the clients with the PKI. Manual enrollment does not scale in large environments. There are multiple automated methods, such as Microsoft Active Directory Certificate Services, and SCEP.

Active Directory Certificate Services allow users and machines in a Microsoft Active Directory to receive certificates in an automated fashion. This approach is common in Active Directory environments. It is used in the CCNP Security lab environment.

The AnyConnect Secure Mobility Client can use the SCEP to provision and renew a certificate as part of client authentication. The goal of SCEP is to support the secure issuance of certificates to network devices in a scalable manner, using existing technology.

Certificate enrollment using SCEP is supported by AnyConnect IPsec and SSL VPN connections to the Cisco Adaptive Security Appliance in the following ways:

SCEP Proxy: The ASA acts as a proxy for SCEP requests and responses between the client and the CA.

- The CA must be accessible to the ASA, not the AnyConnect client, since the client does not access the CA directly.
- Enrollment is always initiated automatically by the client. No user involvement is necessary.
- SCEP Proxy is supported in AnyConnect 3.0 and higher.

Legacy SCEP: The AnyConnect client communicates with the CA directly to enroll and obtain a certificate.

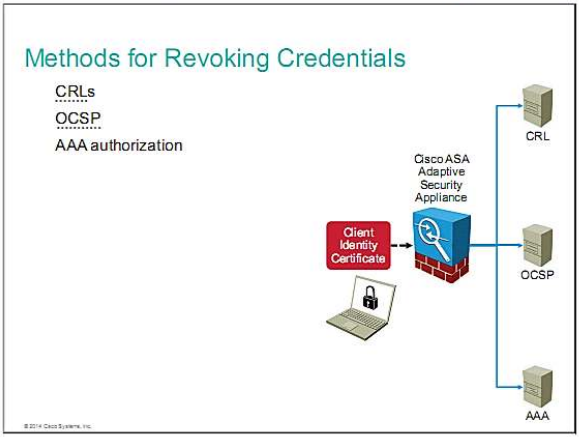
- The CA must be accessible to the AnyConnect client, not the ASA, through an established VPN tunnel or directly on the same network the client is on.

- Enrollment is initiated automatically by the client and may be initiated manually by the user if configured.
- Legacy SCEP is supported in AnyConnect 2.4 and higher.

Cisco AnyConnect Secure Mobility Client 3.x and newer supports certificate renewal. You can use a certificate threshold, which is the amount of time before a certificate expires, to initiate enrollment. If the certificate is within the specified time frame and the security appliance has SCEP configured, renewal occurs.

Methods for Revoking Credentials

This topic describes the PKI integration features available on the Cisco Adaptive Security Appliance.



For some certificate-based client authentication scenarios, you need advanced integration with an existing PKI. Advanced PKI integration includes configuring a revocation method to reduce the risk of compromised certificates. Certificates are considered to be compromised when a certificate was issued incorrectly by a CA, or a private key matching a public key on the certificate is thought to be compromised. For example, if the laptop of a user that stores a certificate, and a matching private key is lost, the certificate should be revoked. Another example would be revoking certificates that belong to users who are no longer employed at an organization.

You can implement a certificate revocation method in the following ways:

Configuring CRLs: A CRL is a list of serial numbers of certificates that have been revoked and are no longer valid. A CRL is generated and published by the CA that issues corresponding certificates and is updated periodically or immediately after a certificate has been revoked. You can configure the Cisco ASA to make CRL checks mandatory when authenticating a certificate. The Cisco ASA needs a CRL location to verify the certificates of clients. A CRL location can be found in a CDP that is specified in an identity certificate. The security appliance can download a CRL using HTTP, LDAP, or SCEP.

Configuring OCSP: OCSP is a protocol for obtaining the revocation status of digital certificates. OCSP messages are usually communicated over HTTP. You can configure the Cisco ASA to make OCSP checks mandatory when authenticating a certificate. You can configure the location of the OCSP server on the Cisco ASA as an OCSP URL that is defined in a match certificate rule. You can statically configure the location as an OCSP URL or you can specify it in the AIA field of the authenticating certificate.

Note	The OCSP server is referred to as the "OCSP responder."

Configuring AAA authorization of the certificate of a user: You can also revoke user authorization by deploying an external RADIUS server. When the Cisco ASA receives the certificate of a user, it sends a predefined field from the certificate as a username and a predefined (common to all users) password to the RADIUS server, which authorizes the user. On the RADIUS server, you must configure users with correct usernames (which match predefined fields in the user certificates) and passwords. If you want to revoke user authorization, you must delete or disable a user account that corresponds to the certificate that you want to revoke.

Enable Certificate-Based Authentication

This topic describes the certificate-based client authentication.

Certificate-based user authentication is enabled in the connection profile. When enabled, the client computer must have a certificate that can be successfully validated by the VPN server. It can be a machine or a user certificate. The AnyConnect client by default can use these both types. You can specifically control which client certificate should be used (machine or certificate) through the AnyConnect Client profiles.

In certificate-based client authentication, the client is not prompted for username and password.

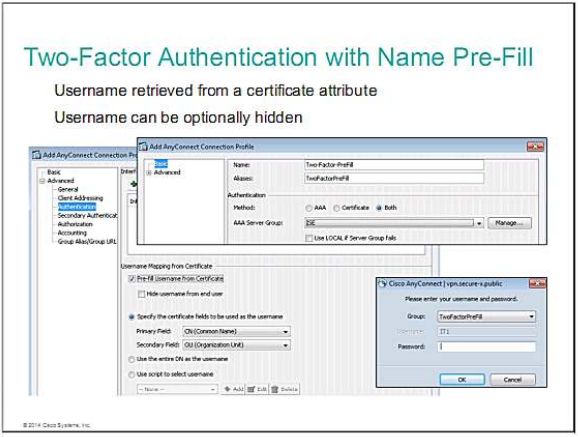
Enable Two-Factor Authentication

This topic describes the two-factor user authentication.

The two-factor client authentication is enabled by choosing the **Both** authentication option in the connection profile. The Cisco Adaptive Security Appliance first validates the client certificate and then prompts the client for username and password. The username entered by the client can be completely independent from any certificate attributes. For example, the certificate-based authentication can be performed using a machine certificate, and password-based authentication will authenticate the user.

Two-Factor Authentication with Name Pre-Fill

This topic describes the two-factor authentication with username pre-fill.



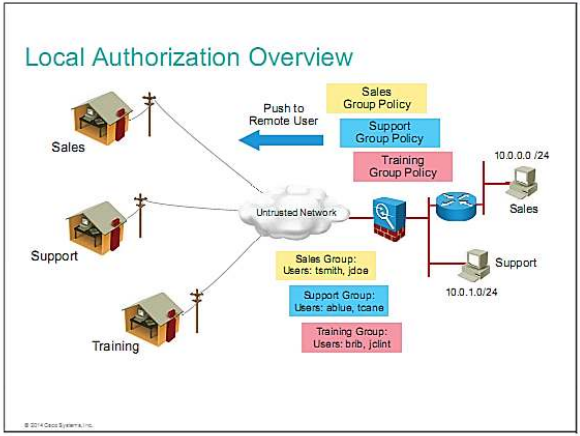
You can enhance the two-factor authentication with the username pre-fill feature. This functionality is configured in the Advanced settings of the connection profile. When enabled, the Cisco Adaptive Security Appliance will retrieve the principal username from a certificate attribute and pre-fill it for password authentication. You can specify which certificate attribute will be used as the principal username.

The username pre-fill feature is used when two credentials of the user should be validated. You cannot use it to combine machine certificate validation with user password authentication.

You can further tune the pre-fill username functionality by hiding the username from the client. In that case the client will be prompted only for a password. The username will be retrieved from the certificate but hidden from the client.

Local Authorization Overview

This topic describes the authorization performed locally on the Cisco Adaptive Security Appliance.



Within a corporation, there are varying access requirements for different personnel. Customer service engineers may require 7-day, 24-hour access; sales entry personnel need 5-day, 8-hour access; and contractors might need access from 9 a.m. to 5 p.m. (0900 to 1700), with restricted server access. The security appliance can accommodate different access and usage requirements. By using group policies, you can define different rights and privileges on a group basis. A customer service engineer, sales entry person, and contractor can be assigned to different groups. Within each group, you can configure different access hours, access protocols, idle timeouts, and server restrictions.

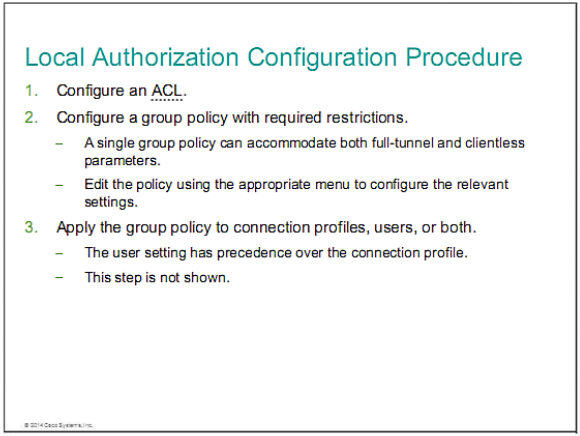
A group policy is a set of user-oriented attribute and value pairs that are stored either internally on the security appliance or externally on a RADIUS server. The connection profile refers to a group policy that sets terms for user connections after the connection is established. Group policies enable you to apply whole sets of attributes to a user or a group of users, rather than having to specify each attribute individually for each user. Each remote VPN user belongs to a specific VPN group. As users connect to the VPN server, the server identifies the group to which they belong. It then pushes the appropriate VPN group policy to the remote user.

If you decide to grant identical rights to all VPN users, you do not need to configure specific group policies; however, VPNs seldom work that way. For example, you might allow a finance group to access one part of a private network, a customer support group to access another part, and a sales group to access other parts. In addition, you might allow specific users within a sales group to access systems that other sales users cannot access. Group policies provide the flexibility to do so securely.

The security appliance includes a default group policy named DfltGrpPolicy. This group policy always exists on the security appliance, but it does not take effect unless you configure the security appliance to use it. When you configure other group policies, any attribute that you do not explicitly specify takes its value from the default group policy. You cannot delete the default group policy, but you can modify it. You can also create one or more group policies specific to your environment. You can configure internal and external group policies. Internal groups are configured on the internal database of the security appliance. External groups are configured on an external authentication server, such as RADIUS.

Local Authorization Configuration Procedure

This topic describes the configuration procedure for local authorization.



To configure local VPN authorization, perform these configuration tasks:

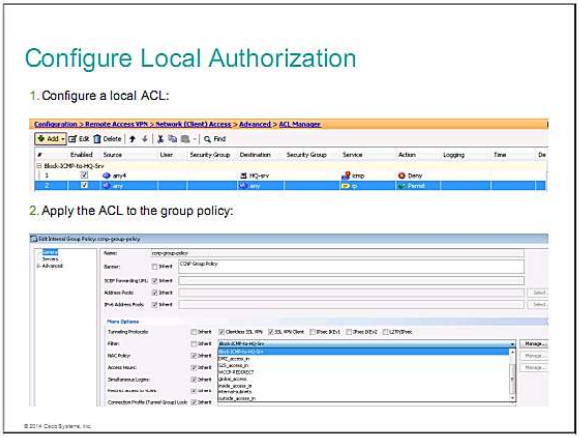
1. Configure an ACL (full-tunnel VPN).
2. Configure a group policy with required restrictions using one of two approaches:

   Define separate group policies for clientless and full-tunnel users. This approach is more difficult to manage.

   Define one group policy for a set of users with similar privileges. Enable multiple access types and configure the appropriate parameters.
3. Apply the group policy to the connection profile, users, or both. The user setting has precedence over the connection profile. This step is not shown in this configuration sequence.

Configure Local Authorization

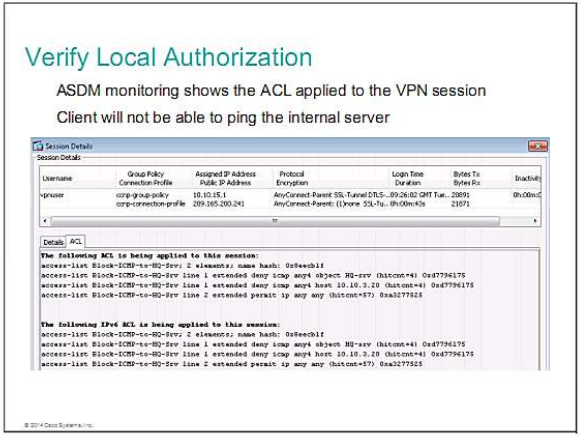
This topic describes the the configuration of local authorization.



To configure local authorization you need to define a local ACL and apply it to the appropriate group policy. In this example, the ACL denies ICMP traffic to the HQ-Srv and permit all other traffic.

Verify Local Authorization

This topic describes how verify local authorization of AnyConnect VPNs.

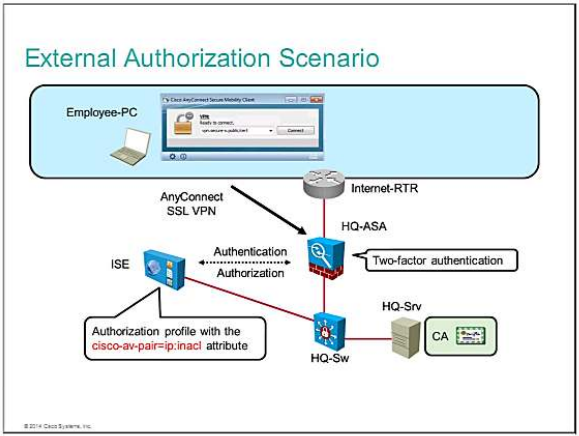


You can verify the effects of local authorization in multiple ways, including connectivity tests from the client machine. The Cisco Adaptive Security Appliance offers authorization monitoring methods both through the Cisco Adaptive Security Device Manager and in the CLI.

This figure illustrates how to monitor the authorization results in the ASDM monitoring. When you select the VPN access type, you will see all established sessions on the ASA. When you click the **Details** button for a given connection, you can select the **ACL** tab, which displays the authorization results.

External Authorization Scenario

This topic describes an external authorization scenario.

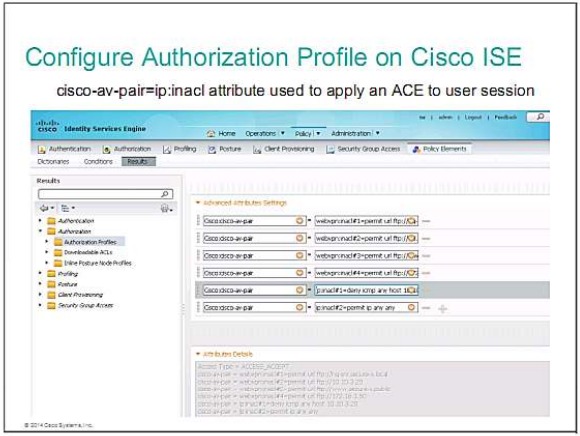


The figure presents the scenario in which you configure the Cisco Adaptive Security Appliance to authenticate and authorize clientless SSL VPN users on the external RADIUS server. Cisco Identity Services Engine acts as the RADIUS server.

The ASA is configured with a connection profile that uses AAA services, possibly in addition to the certificate-based authentication. The user will be authenticated via RADIUS on the ISE. The ISE has an authorization policy and applied an authorization profile to the user session. The authorization profile contains the **cisco-av-pair=inacl** attributes that enforce ACEs for the user traffic.

Configure Authorization Profile on Cisco ISE

This topic describes the deployment of SSL VPN authorization using an external RADIUS server.



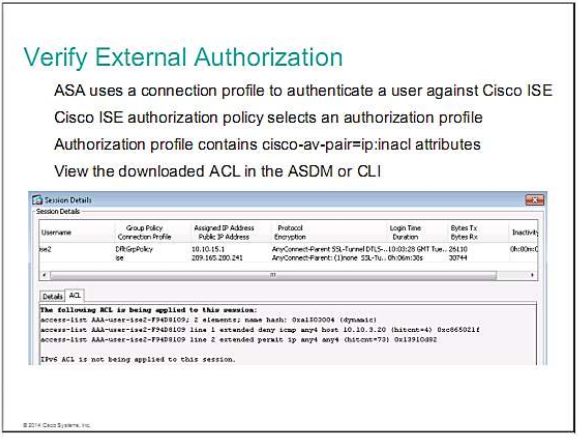
On the Cisco Adaptive Security Appliance you only need to have a connection profile that uses AAA service for client authentication. RADIUS performs authentication and authorization at the same time, so the authorization part does not need to be explicitly enabled.

The Cisco Identity Services Engine needs to have an authorization policy that applies authorization profiles to the user sessions. The authorization profile for AnyConnect VPN authorization is based on the cisco-av-pair=ip:inacl attribute.

The figure illustrates an authorization profile configured for authorization of clientless and client VPNs. The cisco-av-pair=webvpn:inacl attribute is used to push WebVPN ACEs to clientless SSL VPN sessions. The cisco-av-pair=ip:inacl attribute is used to push ACEs to full tunneling VPNs (SSL and IPsec).

Verify External Authorization

This topic describes how to monitor external authorization in AnyConnect SSL VPNs.

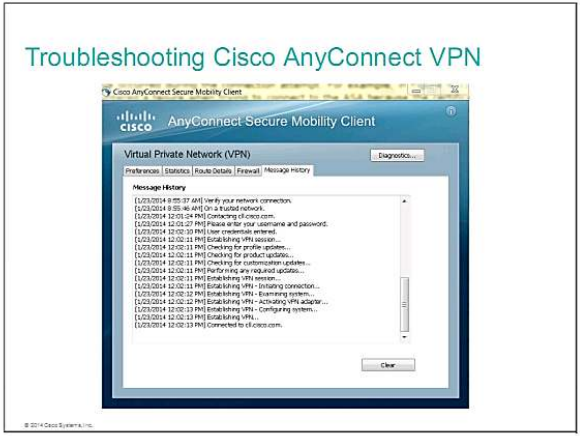


The Cisco Identity Services Engine has an authorization policy that applies authorization profiles to the user sessions. The authorization profile for AnyConnect VPN authorization uses the cisco-av-pair=ip:inacl attributes to authorize client sessions.

You can view the authorization results in the **ACL** tab in the Cisco Adaptive Security Device Manager session monitoring, as shown in the figure.

Troubleshooting Cisco AnyConnect VPN

This topic describes how to troubleshoot Cisco AnyConnect VPN.



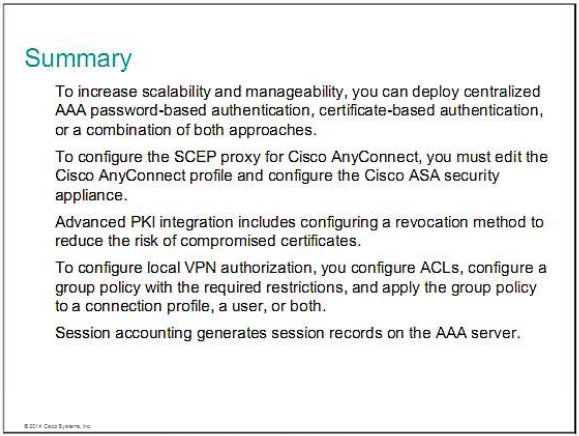
The Cisco AnyConnect client itself provides a vast amount of troubleshooting information. The Message History tab shown in the figure provides a detailed, step-by-step explanation of the current status and connection phase and any errors that may have occurred during a connection attempt. This enables you to troubleshoot any connection, from a basic connection using simple username and password authentication via the LOCAL ASA database to connections using advanced methods, such as double authentication via certificates. For example, the Message History tab might show that a user encountered a failure when trying to connect to the Cisco Adaptive Security Appliance because the certificate required for authentication was not installed.

Another way to gather information for troubleshooting is to use the DART. DART works independently of any installed AnyConnect client software or modules and is not version specific, so you can install any version of DART with any version of the Cisco AnyConnect Secure Mobility Client. DART supports Windows 7, Windows Vista, and Windows XP, Mac OS X v10.6, v10.7, and v10.8, and Red Hat Enterprise Linux 5.x (32-bit) or 6.x (64-bit). The DART wizard runs on the computer that runs AnyConnect. DART assembles the logs, status, and diagnostic information for Cisco Technical Assistance Center analysis. DART does not require administrator privileges. DART does not rely on any component of the AnyConnect software to run, though you can launch DART from AnyConnect, and DART does collect the AnyConnect log file, if it is available.

DART is currently available as a standalone installation, or you can push the application to the client computer as part of the AnyConnect dynamic download infrastructure. The DART module is integrated into the AnyConnect client package: Once installed, the end user can start the DART wizard from the Cisco folder available through the Start button.

Summary

This topic summarizes the key points that were discussed in this lesson.



Lesson 4

Deploying Cisco AnyConnect IPSec/IKEv2 VPNs

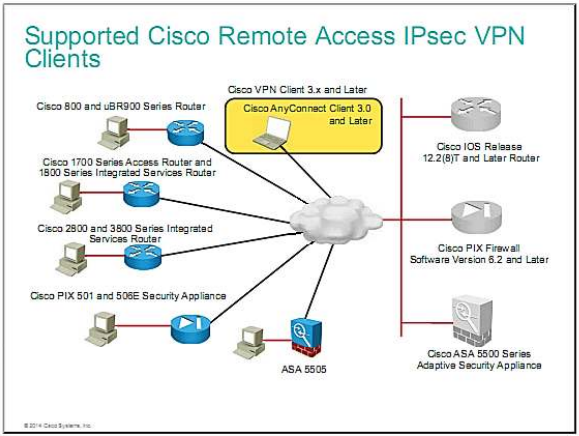
A Cisco AnyConnect remote access IPsec VPN solution provides client-based access to sensitive resources over a remote-access IPsec VPN gateway that is implemented on the Cisco Adaptive Security Appliance. Apart from password- or certificate-based authentication, the IPsec VPN solution encompasses client configuration, IP address assignment, and the provisioning of an access control policy. Cisco AnyConnect client version 3.x or newer is required for this functionality, which uses IKEv2 instead of IKEv1. This lesson enables you to describe, configure, and verify the remote access IPsec VPN solution.

Upon completing this lesson, you will be able to meet these objectvies:

- Describe supported Cisco remote access IPsec VPN clients
- Describe IKEv2 support in the Cisco AnyConnect client
- Describe the requirement to make IPsec the primary protocol for a host entry
- Describe the IKEv2 configuration procedure
- Configure Cisco AnyConnect IPsec VPN on Cisco ASA security appliances
- Verify and troubleshoot Cisco AnyConnect IPsec VPN

Supported Cisco Remote Access IPsec VPN Clients

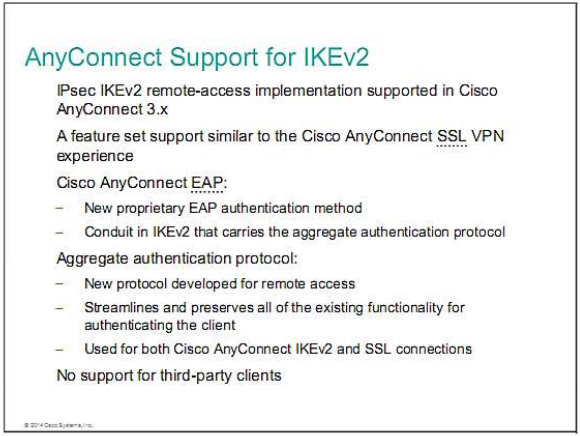
This topic lists the supported Cisco remote access IPsec VPN clients.



The Cisco Adaptive Security Appliance supports IPsec VPN in multiple ways. Multiple clients support IKEv1, and the Cisco AnyConnect Client version 3.0 and newer supports the IKEv2. This figure shows the remote-access client devices that support IPsec VPN with IKEv1 and IKEv2.

AnyConnect Support for IKEv2

This topic describes IKEv2 support in the Cisco AnyConnect client.



If you are using Cisco AnyConnect Secure Mobile Client version 3.x (Cisco AnyConnect 3.x), you can use IKEv2 with remote-access VPNs. The main goal of the implementation is to provide a user experience that is as close as possible to the current Cisco AnyConnect client experience, and to incorporate as much feature parity from both SSL and IKEv1 as possible, while providing a protocol-agnostic experience to the end user.

To meet this goal, the current IKEv2 implementation uses the core IKEv2 protocol, but it requires the addition of many extensions, including Cisco AnyConnect EAP, which is a proprietary EAP authentication method. Cisco AnyConnect EAP is the authentication method that Cisco AnyConnect 3.x and IKEv2 support. Because of this restriction, this initial offering of IKEv2 does not support other third-party clients.

Cisco AnyConnect EAP is a conduit in IKEv2 that carries the new aggregate authentication protocol that was developed for remote access. The aggregate authentication protocol streamlines and preserves all of the existing functionality for authenticating the client and is used for both Cisco AnyConnect 3.0 IKEv2 and SSL connections.

Using Cisco Adaptive Security Device Manager to configure IKEv2 support is similar to configuring a standard IPsec IKEv1 remote-access connection. However, using the CLI to configure IKEv2 remote access is very different from configuring IKEv1 remote access.

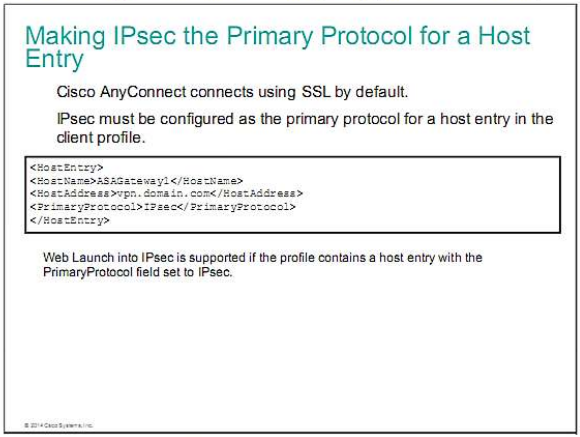
Deployment Strategies

The Cisco AnyConnect Secure Mobile Client version 3.x (Cisco AnyConnect 3.x) can support either SSL or IPsec with the introduction of IKEv2. AnyConnect exhibits the same behavior independent of the protocol in use, which allows the same policies, modules, and user mobility functions. Your choice of either protocol comes down to the security level imposed by your organization. For example, if your organization requires a very high level of protection for data incoming from a remote client, you might choose to deploy an IPsec connection using IKEv2. You must also consider the use of any current or future use of delay-sensitive applications that might require frequent use by remote users. For these, you can implement DTLS, which requires the use of SSL/TLS rather than IKEv2 (because DTLS cannot operate over IKEv2 connections).

If the remote user base requires a mix of DTLS/TLS and IPsec connections using IKEv2, you can deploy multiple connection profiles and allow users to select a connection profile either manually in the AnyConnect client or automatically if using certificate-based authentication.

Making IPsec the Primary Protocol for a Host Entry

This topic describes the requirement to make IPsec the primary protocol for a host entry.



Cisco AnyConnect 3.0 supports IKEv2. However, it connects using SSL, by default. To enable IPsec IKEv2, you must configure the IKEv2 settings on the Cisco Adaptive Security Appliance and also configure IKEv2 as the primary protocol in the client profile. The IKEv2enabled profile must be deployed to the endpoint computer, otherwise the client attempts to connect using SSL.

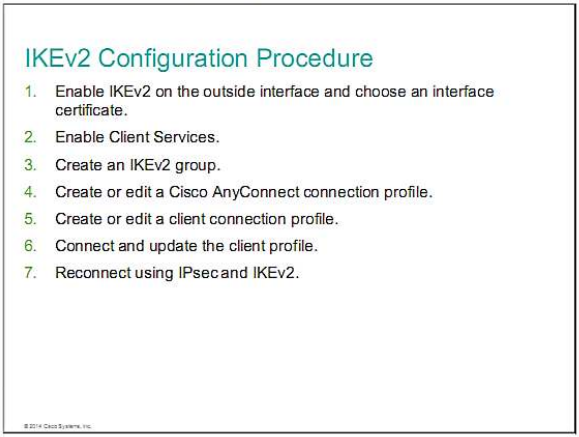
```
<HostEntry>
<HostName>ASAGateway1</HostName>
<HostAddress>vpn.domain.com</HostAddress>
<PrimaryProtocol>IPsec</PrimaryProtocol>
</HostEntry>
```

You configure this profile using Cisco Adaptive Security Device Manager in the Cisco AnyConnect Client profile.

Note	The Cisco ASA supports the Web Launch feature into IPsec if the profile contains a host entry with the PrimaryProtocol field set to IPsec.

IKEv2 Configuration Procedure

This topic describes the IKEv2 configuration procedure.

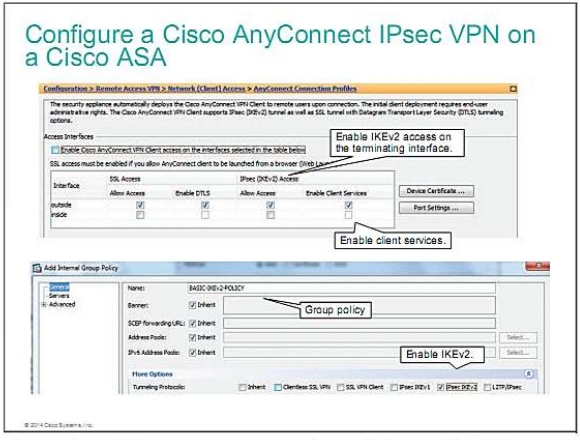


To configure an IPsec profile to support IKEv2 and Cisco AnyConnect 3.x, perform the following tasks:

1. Enable IKEv2 on the outside interface and choose an interface certificate.
2. Enable Client Services.
3. Create an IKEv2 group.
4. Create and edit a Cisco AnyConnect connection profile.
5. Create and edit a client connection profile.
6. Connect and update the client profile.
7. Reconnect using IPsec and IKEv2.

Configure a Cisco AnyConnect IPsec VPN on a Cisco ASA

This topic describes how to configure a Cisco AnyConnect IPsec VPN on a Cisco Adaptive Security Appliance.

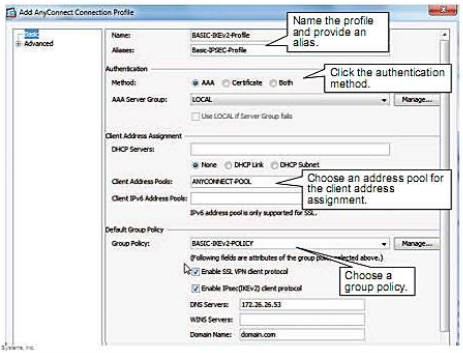


The first task to configure IKEv2 support on a connection profile is to enable IKEv2 on an interface.

The second task in configuring IKEv2 support is to enable Client Services, as shown in the upper figure. During an IPsec and IKEv1 session setup, information about client XML profiles, client updates, and client customization files must be exchanged. Because IPsec and IKEv1 were not designed to pass large amounts of data during session setup, another method is needed to exchange this data. When you enable Client Services, IKEv2 uses a separate "parallel" SSL connection to exchange this data.

In the third task, shown in the bottom figure, you configure a VPN group policy to support IKEv2.

Configure a Cisco AnyConnect IPsec VPN on a Cisco ASA (Cont.)



In the fourth task, you create or edit a Cisco AnyConnect connection profile. In the connection profile, you choose the authentication method and determine how the client will receive an IP address. In the example, the MY-POOL IP address pool is used. In the Default Group Policy section, you choose the group policy that you created in the previous task.

In the remaining tasks, not shown individually, you define a Cisco AnyConnect client profile, add the server to the server list, and make IPsec the primary connection protocol.

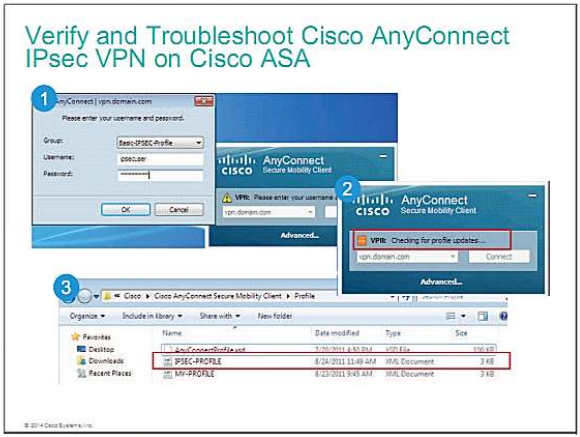
Configure a Cisco AnyConnect IPsec VPN on a Cisco ASA (Cont.)

```
webvpn
     no anyconnect enable
     webvpn
       anyconnect profiles IPSEC-PROFILE disk0:/ipsec-profile.xml
     exit
     group-policy BASIC-IKEv2-POLICY attributes
       webvpn
         anyconnect profiles value IPSEC-PROFILE type user
       exit
     exit
     group-policy BASIC-IKEv2-POLICY internal
     group-policy BASIC-IKEv2-POLICY attributes
       vpn-tunnel-protocol ssl-client ikev2
       dns-server value 10.0.1.11
       wins-server none
       default-domain value domain.com
     exit
     tunnel-group BASIC-IKEv2-Profile type remote-access
     tunnel-group BASIC-IKEv2-Profile general-attributes
       default-group-policy BASIC-IKEv2-POLICY
       address-pool  MY-POOL
```

This figure shows the CLI commands that the Cisco Adaptive Security Device Manager generates to configure the IKEv2 support.

Verify and Troubleshoot Cisco AnyConnect IPsec VPN on Cisco ASA

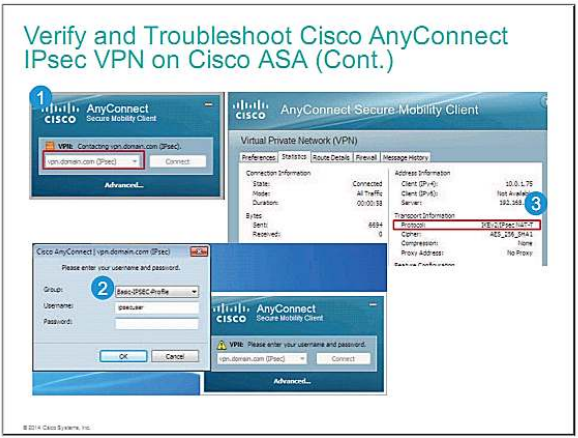
This topic describes the verification and troubleshooting of Cisco AnyConnect IPsec VPN.



When the user connects and updates the profile, the initial connection occurs over DTLS.

In the first step, the user chooses the alias from the Group drop-down list and enters a valid username and password. In the example, Basic-IPSEC-Profile is selected, which ties the user to the IPSEC-PROFILE client profile that defines all of the IPsec parameters.

In the second step, the client software checks for a profile update. The third step in the figure shows that the IPSEC-PROFILE client profile has been downloaded.



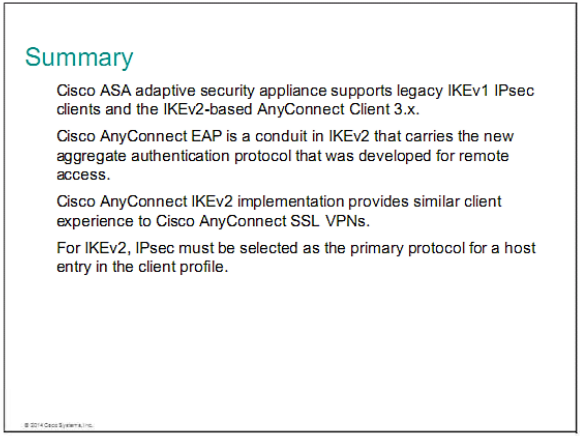
With the newly downloaded IPSEC-PROFILE, the user disconnects the connection. Now, when the user clicks the drop-down list in the initial Cisco AnyConnect connection window, there is a new entry for the IPSec connection. This new entry displays with **(IPSec)** in the entry name, as shown in the first figure.

The second figure shows the authentication window that appears when the user clicks **Connect** in the initial connection window.

The third figure shows how to confirm that the client has used IPSec/IKEv2 to connect. In the AnyConnect Secure Mobility Client window, click the **Statistics** tab and check the Transport Information: Protocol field. **IKEv2/IPsec** should appear in this field.

Summary

This topic summarizes the key points that were discussed in this lesson.



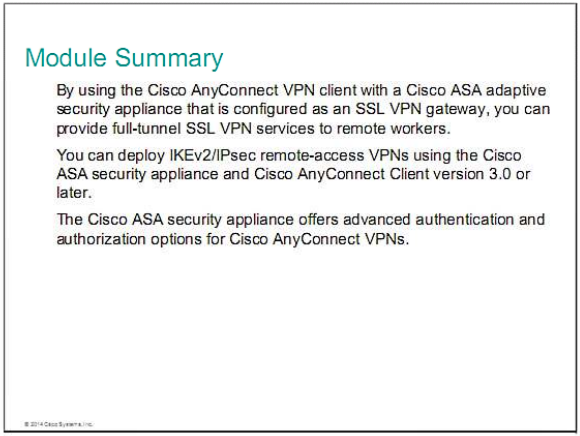
References

For additional information, refer to this reference:

Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.1. http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect31/administration/guide/ac06websecurity.html

Module Summary

This topic summarizes the key points that were discussed in this module.



References

For additional information, refer to these resources:

Cisco Systems, Inc. *Cisco AnyConnect Secure Mobility Client Administrator Guide*. http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/anyconnectadmin30.html

Module Self-Check

Questions

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

1. Which of the following are basic IP address assignment options for SSL VPN clients? (Choose two.) (Source: Deploying Basic Cisco AnyConnect SSL VPN on Cisco ASA)

   A. using a connection profile local pool
   B. using a local pool in a group policy
   C. using a connection profile remote pool
   D. using a remote pool in a group policy

2. Which of the following statements are true about using split tunneling in SSL VPN? (Choose two.) (Source: Deploying Basic Cisco AnyConnect SSL VPN on Cisco ASA)

   A. It decreases the performance of applications that do not require the VPN tunnel.
   B. It creates a separate tunnel from the SSLVPN client to each network you specify.
   C. It can increase risk because the client is not protected by central site security mechanisms when it is connecting to the other networks.
   D. It may increase risk because the client can be used as a relay between the external networks and the internal protected network more easily if the client is compromised by an attacker.
   E. It routes all traffic to the VPN gateway.
   F. It creates two separate tunnels, one for traffic that is destined for specific internal protected networks and another for all other traffic.

3. A self-signed or CA-signed identity certificate is used to authenticate the SSL VPN server to Cisco AnyConnect VPN clients. (True or false?) (Source: Deploying Basic Cisco AnyConnect SSL VPN on Cisco IOS)

   A. true
   B. false

4. Which of the following options are required for a Cisco AnyConnect IPsec/IKEv2 VPN deployment? (Source: Deploying Cisco AnyConnect IPSec/IKEv2 VPNs)

   A. configuring IKEv2 as the primary connection protocol on the Cisco ASA
   B. enabling Client Services on a Cisco ASA interface
   C. configuring IKEv2 as the primary protocol in a client profile
   D. deploying an IKEv2-enabled client profile to the endpoint computer
   E. enabling DTLS on the Cisco ASA interface to which the AnyConnect client will connect

5. Which of the following options describe DTLS? (Choose two.) (Source: Deploying Advanced Cisco AnyConnect SSL VPN on Cisco ASA)

   A. can transport only connectionless data, such as UDP
   B. prevents retransmissions from application endpoints
   C. prevents retransmissions at the VPN layer
   D. should not be used for business-critical applications
   E. used by default for delay-critical applications, such as VoIP
   F. is standards-based
   G. is Cisco proprietary

6. What of the following is the recommended method of ensuring that you edit the Cisco AnyConnect profile without errors? (Source: Deploying Advanced Cisco AnyConnect SSL VPN on Cisco ASA)

   A. manually editing the client profile XML files
   B. using the standalone profile editor that is appropriate for the client operating system
   C. using the Cisco ASA CLI
   D. using the Cisco AnyConnect Profile Editor that is integrated into Cisco ASDM

7. What should you use to enable SBL? (Source: Deploying Advanced Cisco AnyConnect SSL VPN on Cisco ASA)

   A. client scripting
   B. TND
   C. client profile
   D. predeployment
   E. authentication based on machine certificates

8. You must configure an IP address assignment in a Cisco AnyConnect IPsec VPN. (True or false?) (Source: Deploying Cisco AnyConnect IPsec VPN on Cisco ASA)

   A. true
   B. false

9. Which of the following options can be used to increase the strength of the client authentication for Cisco AnyConnect SSL VPN users? (Choose three.) (Source: Deploying Advanced Authentication, Authorization, and Accounting in Cisco AnyConnect VPNs)

   A. external RADIUS user database integrated with a back-end LDAP server database
   B. digital certificates
   C. certificate authentication combined with up to three AAA authentication methods
   D. TACACS+ user database

10. Which of the following options best describes the use of the Cisco Identity Services Engine (ISE) to enhance a Cisco AnyConnect Secure Mobility Client deployment? (Source: Deploying Advanced Authentication, Authorization, and Accounting in Cisco AnyConnect VPNs)

   A. providing authentication services
   B. providing authentication and authorization services
   C. provisioning and renewing certificates as part of client authentication.
   D. providing the ASA with the revocation status of digital certificates
   E. providing advanced web filtering services to protect AnyConnect client users from security threats

Answer Key

1. A, B
2. C, D
3. A
4. B, C, D
5. C, F
6. D
7. C
8. A
9. A, B, D
10. B

Module 6

Endpoint Security and Dynamic Access Policies

Some of the most challenging requirements of VPNs are to provide host security at the endpoint to ensure the security of hosts that connect to the trusted network and to provide high availability and high performance. Cisco HostScan enables administrators to provide a higher level of security to untrusted endpoints.

The VPN gateways operate in dynamic environments. Multiple variables can affect each VPN connection; for example, intranet configurations that frequently change, the various roles each user may inhabit within an organization, and logins from remote access sites with different configurations and levels of security. The task of authorizing users is much more complicated in a dynamic VPN environment than it is in a network with a static configuration.

Dynamic access policies (DAP) enables you to configure authorization that addresses the dynamics of VPN environments. You create a dynamic access policy by setting a collection of access control attributes that you associate with a specific user tunnel or session. These attributes address issues of multiple group membership and endpoint security.

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

- Implement Cisco HostScan for both clientless and full-tunnel SSL VPNs
- Integrate DAP with Host Scan on the Cisco ASA security appliance

Lesson 1

Implementing Host Scan

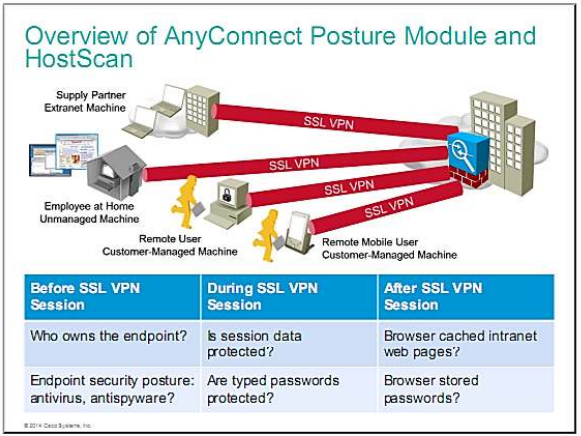
This lesson describes AnyConnect Host Scan.

Upon completing this lesson, you will be able to:

- Describe AnyConnect Posture Module and HostScan
- Describe the secure posture components
- Describe basic HostScan functionality
- Describe HostScan workflow
- Describe deployment scenarios of the AnyConnect Posture Module and HostScan
- Describe the HostScan configuration procedure
- Describe the HostScan configuration procedure
- Describe how to the configure basic HostScan and enable extensions
- Describe how to configure Advanced Endpoint Assessment

Overview of AnyConnect Posture Module and HostScan

This topic provides and overview of AnyConnect Posture Module and HostScan.



SSL VPNs provide the flexibility to deploy secure remote access to corporate resources from any location that can provide a compliant web browser that has the correct SSL support. These deployments include access for customers, partners, and employees from systems that are not necessarily corporate-managed. When you do not have direct control over the systems that are used to access corporate resources, additional security threats are introduced to your network.

Before the SSL VPN session

- Who owns the endpoint?
- Endpoint security posture: Does the system have antivirus or a personal firewall?
- Is the system already running malware?

During the SSL VPN session

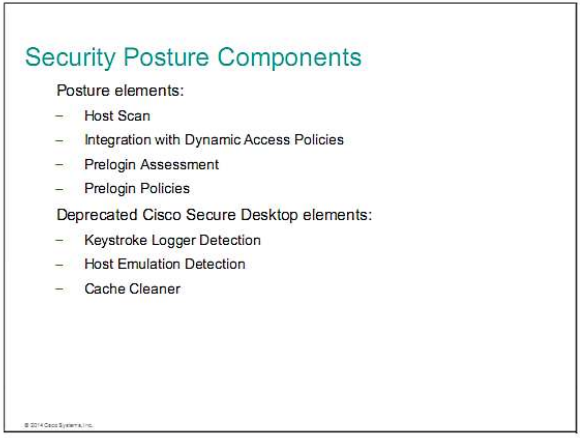
- Is the session data protected?
- Are locally typed passwords protected?
- Has malware been launched during the session?

After the SSL VPN session

- Has the browser cached intranet web pages?
- Has the browser stored any passwords?
- Are there any downloaded files left behind on the system?

Security Posture Components

This topic describes the components of the VPN security posture.



The AnyConnect Posture Module provides the AnyConnect Secure Mobility Client the ability to identify the operating system, antivirus, antispyware, and firewall software installed on the host. The HostScan application, which is among the components delivered by the posture module, is the application that gathers this information.

The components of the secure posture module include:

Host Scan: Host Scan is a package that installs on the remote device after the user connects to the Cisco Adaptive Security Appliance and before the user logs in. Host Scan consists of any combination of the Basic Host Scan module, an Endpoint Assessment module, and an Advanced Endpoint Assessment module. Host Scan runs on Microsoft Windows, Apple Mac OS X, and Linux. In order to use Host Scan features, you must have an AnyConnect Premium license installed on the ASA.

Integration with Dynamic Access Policies: The ASA integrates the HostScan features into DAPs. Depending on the configuration, the ASA uses one or more endpoint attribute values in combination with optional AAA attribute values as conditions for assigning a DAP. The HostScan features supported by the endpoint attributes of DAPs include OS detection, policies, basic HostScan results, and endpoint assessment.

Prelogin Assessment: The assessment runs after the user connects to the ASA, but before the user logs in. This assessment can check the remote device for files, digital certificates, the OS, IP address, and Microsoft Windows registry keys.

Prelogin Policies: Policies specify the remote user experience, rights, and restrictions. Depending on the results of the prelogin assessment module, a particular policy is assigned to a user session or the session is denied.

These components have been deprecated:

Keystroke Logger Detection: You can configure selected policies to scan for processes or modules that record keystrokes entered by the user, and deny VPN access if a suspected keystroke logging application is present.

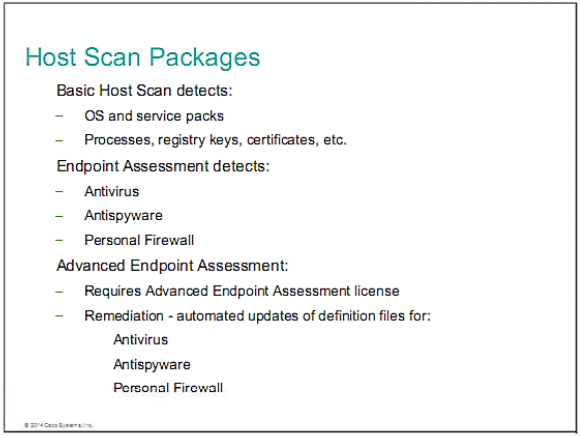
Host Emulation Detection: Host emulation detection, another feature of policies, determines whether a remote Microsoft Windows operating system is running over virtualization software.

Cache Cleaner: Cache cleaner attempts to eliminate the information from the browser cache at the end of a clientless SSL VPN session or after web-launching an AnyConnect Client session. This information includes entered passwords, auto-completed text, files cached by the browser, browser configuration changes made during the session, and cookies.

Note The Keystroke Logger Detection, Host Emulation Detection, and Cache Cleaner features have been deprecated. Cisco stopped developing them on November 20, 2012. Deprecated features, the screens used to configure these features in the Cisco Adaptive Security Device Manager, and the commands used to configure these features in the ASA command line interface will not be removed from the packages in which they are delivered until the end of engineering support to address severity 1 and severity 2 defects. After the features have been deprecated, they will continue to provide the functionality for which they were built but will eventually be incompatible with future releases of the ASA, ASDM, AnyConnect, or the operating system on which the endpoint runs.

HostScan Functionality

This topic describes basic HostScan functionality.



Host Scan can consist of any combination of three elements: Basic HostScan, an Endpoint Assessment extension, and an Advanced Endpoint Assessment extension.

Basic Host Scan

Host Scan automatically identifies operating systems and service packs on any remote device establishing a Cisco clientless SSL VPN or AnyConnect client session and when CSD or Host Scan/CSD is enabled on the Cisco Adaptive Security Appliance.

Note	Previously, the Host Scan package was one of several components available only by installing CSD. Starting with AnyConnect 3.0, the HostScan package is a shared component of the AnyConnect Secure Mobility client and CSD.

You can also configure Host Scan to inspect the endpoint for specific processes, files, registry keys, digital certificates, and IP addresses using the Secure Desktop manager. Secure Desktop manager is integrated with Cisco Adaptive Security Device Manager on the ASA. Host Scan performs all of these inspections before full tunnel establishment.

After Host Scan gathers from the endpoint the operating system and service pack information along with the processes, files, registry keys, digital certificates, and IP addresses you configured it to gather, it sends this information to the ASA where it can be used to distinguish between corporate-owned, personal, and public computers. The information can also be used in assessments.

Endpoint Assessment

Endpoint Assessment is a HostScan extension that examines the remote computer for a large collection of antivirus and antispyware applications, associated definitions updates, and firewalls. You can use this feature to combine endpoint criteria to satisfy your requirements before the ASA assigns a specific DAP to a session.

Note If HostScan was installed on the endpoint as part of a pre-deployed posture module but a HostScan package is not enabled on the ASA; when the endpoint connects to the ASA, the HostScan package on the endpoint will not perform endpoint assessment.

Advanced Endpoint Assessment

With the purchase of an Advanced Endpoint Assessment license installed on the ASA, you can use the advanced remediation features of HostScan. On Windows, Mac OS X, and Linux desktops, Advanced Endpoint Assessment can attempt to initiate remediation of various aspects of antivirus, antispyware and personal firewall protection if that software allows a separate application to initiate remediation.

Antivirus: Advanced Endpoint Assessment can attempt to remediate these components of antivirus software:

- Force File System Protection: If the antivirus software is disabled, Advanced Endpoint Assessment can enable it.
- Force Virus Definitions Update: If the antivirus definitions have not been updated in the number of days defined by the Advanced Endpoint Assessment configuration, Advanced Endpoint Assessment can attempt to initiate an update of virus definitions.

Antispyware: If the antispyware definitions have not been updated in the number of days defined by the Advanced Endpoint Assessment configuration, Advanced Endpoint Assessment can attempt to initiate an update of antispyware definitions.

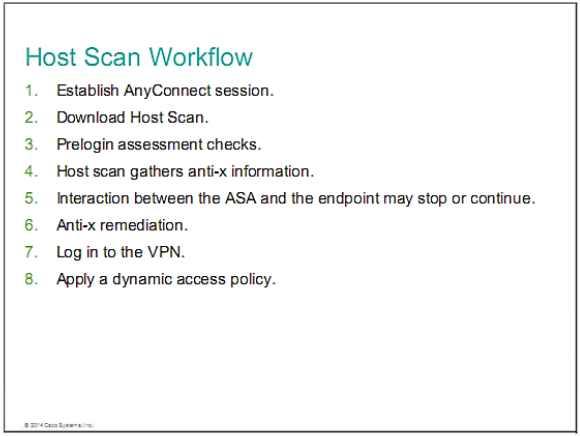
Personal Firewall: The Advanced Endpoint Assessment extension can attempt to reconfigure firewall settings and rules if they do not meet the requirements defined in the Advanced Endpoint Assessment configuration.

- The firewall can be enabled or disabled.
- Applications can be prevented from running or allowed to run.
- Ports can be blocked or opened.

Note If the end-user disables antivirus or personal firewall, after successfully establishing the VPN connection, the Advanced Endpoint Assessment feature will attempt to re-enable that application within approximately 60 seconds.

Host Scan Workflow

This topic describes HostScan workflow.



Host Scan works with the Cisco Adaptive Security Appliance to protect the corporate network as described in the workflow that follows:

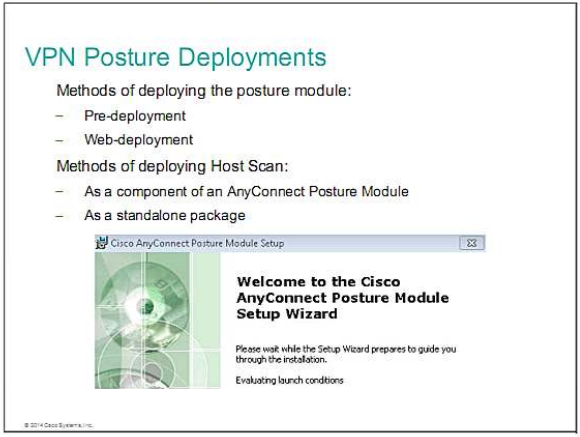
1. The remote device attempts to establish an AnyConnect Client session with the ASA.
2. The ASA downloads Host Scan to the endpoint ensuring that the ASA and the endpoint are using the same version of Host Scan. The version of Host Scan on the endpoint could either be upgraded or downgraded to match the version of Host Scan on the ASA.
3. The prelogin assessment checks for the following on the endpoint:
   - Operating system.
   - Presence or absence of any files you specify.
   - Presence or absence of any registry keys you specify. This check applies only if the computer is running Microsoft Windows.
   - Presence of any digital certificates you specify. This check also applies only if the computer is running Microsoft Windows.
   - IPv4 or IPv6 addresses within a range you specify.
4. As the endpoint undergoes the prelogin assessment, Host Scan gathers antivirus, firewall, and antispyware version information.
5. One of the following occurs, depending on the result of the prelogin assessment:
   - The endpoint attributes do not meet the requirements of the prelogin assessment and the Login Denied message appears on the endpoint. In this case, interaction between the ASA and the endpoint stops.

- The endpoint attributes meet the requirements of the prelogin assessment. The prelogin assessment assigns a prelogin policy name to the endpoint and reports the name of the prelogin policy to the ASA. In this case, interation between the ASA and the endpoint continues.

6. Antivirus, firewall, or antispyware remediation occurs if it is warranted and you have a license for Advanced Endpoint Assessment.
7. The user logs in.
8. The ASA typically uses the authentication data gathered in 3. along with any configured endpoint attribute criteria gathered in 4., which can include such values as the policy and HostScan results, to apply a dynamic access policy to the session.
9. Following the termination of the user session, HostScan terminates.

VPN Posture Deployments

This topic describes methods of deploying the AnyConnect Posture Module and HostScan.



There are two different methods of deploying the AnyConnect Posture Module of the Cisco AnyConnect Secure Mobility Client:

Pre-deployment method: The AnyConnect Posture Module can be installed on the endpoint using a pre-deployment package before the endpoint makes its initial connection to the Cisco Adaptive Security Appliance. Before you install the posture module, you need to install the AnyConnect Secure Mobility Client on the endpoint .The pre-deployment posture module package contains every component, library, and support chart that could be used to gather posture attributes as well as the applications that provide you with the features described earlier. If you pre-deploy to the endpoint the same version of the AnyConnect client and posture module installed on the ASA, no additional posture module files are pushed down from the ASA when the endpoint connects to the ASA.

Web-deployment method: The AnyConnect Posture Module can be deployed by the ASA to the endpoint. Using this method, when the endpoint connects to the ASA, the ASA pushes the AnyConnect client and posture module down to the endpoint. To make the download as fast and efficient as possible, the ASA only downloads the essential posture module files. When the endpoint connects again, the essential posture module files determine what other libraries or files it needs to perform an endpoint assessment and retrieves those files from the ASA. For example, the posture module may retrieve a Host Scan support chart of all Norton antivirus software because a version of Norton antivirus is running on the endpoint. After the posture module retrieves the additional files it needs, it performs the endpoint assessment and forwards the attributes to the ASA. Assuming the endpoint attributes are sufficient to satisfy a DAP rule, the ASA allows the endpoint to connect. As a result of satisfying the DAP, the ASA could be configured to push the remainder of the posture module to the endpoint or not. If you do not want the entire posture module web-deployed to the endpoint, you can perform a limited web-deployment where only one posture file is downloaded to the endpoint, and it requests only the Host Scan libraries it needs to perform endpoint assessment. In this scenario, you will have very short download times from the ASA to the endpoint, but you will lose the ability to perform Advanced Endpoint Assessment and perform such tasks as antivirus, antispyware, or firewall remediation tasks.

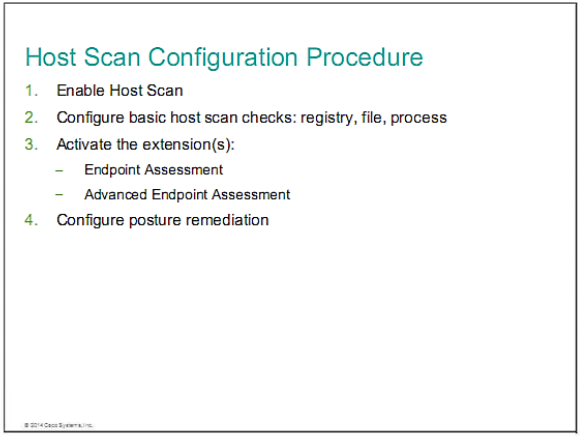
Host Scan can be installed on an endpoint as a component of a pre-deployed or web-deployed AnyConnect Posture Module, or it can be deployed as a standalone package. The standalone Host Scan package and the Host Scan package delivered with the posture module provide the same functionality. However, deploying the posture module allows Host Scan to run privileged operations even when the user on the endpoint is not an administrator, and it allows other AnyConnect modules to start using Host Scan. The advantage of the standalone Host Scan package is that it enables you to easily update the Host Scan support charts. These charts contain the product name and version information of the antivirus, antispyware, and firewall applications used to assign DAPs.

Note	To deploy Host Scan as a component of the AnyConnect Posture Module, you must first upload an AnyConnect Secure Mobility Client package (for example, anyconnect-win-version-k9.pkg) to the Cisco ASA. This package contains all the Cisco AnyConnect Secure Mobility Client features.

If you install Host Scan on an endpoint as part of a pre-deployed posture module, you must also enable the Host Scan package on the ASA; otherwise, when the endpoint connects to the ASA, the HostScan package on the endpoint will not perform endpoint assessment. To install Host Scan on the endpoint as part of a posture module web deployment, you must configure the AnyConnect Secure Mobility package as a Host Scan package and enable HostScan on the ASA.

Host Scan Configuration Procedure

This topic describes the Host Scan configuration procedure.

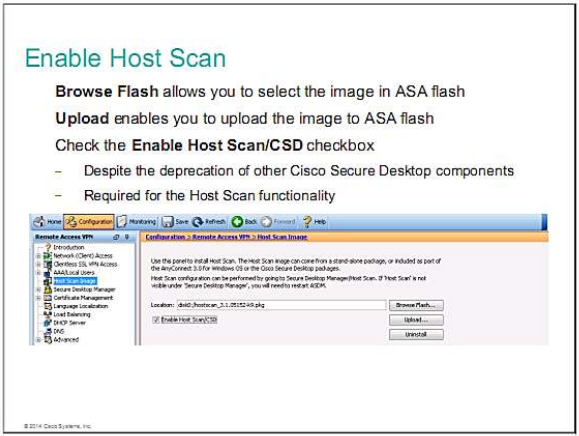


Follow this procedure to configure the Host Scan feature:

1. Enable Host Scan on the Cisco Adaptive Security Appliance.
2. Configure basic host scan checks: registry, file, process.
3. Activate the extension(s):
   - Endpoint Assessment (to detect antivirus, antispyware and personal firewall software).
   - Advanced Endpoint Assessment (to remediate antivirus, antispyware and personal firewall software).
4. Configure posture remediation, which describes the desired definition updates.

Enable Host Scan

This topic describes how to enable the HostScan feature.

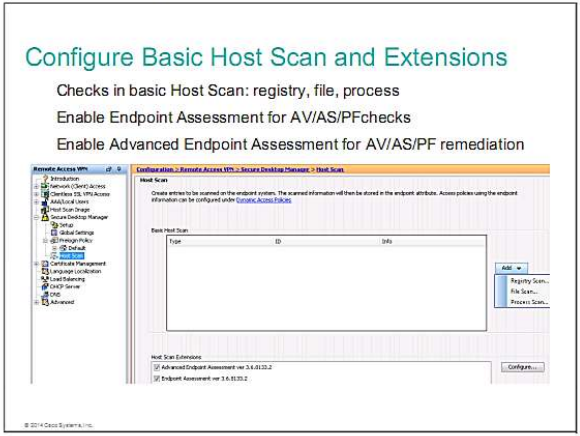


To enable the Host Scan feature for the VPN access, you need to upload a Host Scan image to the Cisco Adaptive Security Appliance flash memory. The Cisco Adaptive Security Device Manager enables you to upload the file from your management workstation. If the Host Scan image is already in the flash memory, you can browse to it and enable the Host Scan functionality.

You need to check the **Enable Host Scan/CSD** checkbox despite that fact that other CSD components have been deprecated.

Configure Basic Host Scan and Extensions

This topic describes how to configure basic HostScan and enable extensions.



You configure Host Scan operation in the **Configuration > Remote Access VPNs > Secure Desktop Manager > Host Scan** menu. Within the basic Host Scan functionality, you can define registry, file, and process checks using the appropriate menu options.

Independently of the basic Host Scan functionality, you may want to detect and remediate antivirus, antispyware, and personal firewall software installed on the VPN endpoints. To enable this functionality, you need to check the appropriate extention checkboxes: **Endpoint Assessment** for AntiVirus/ AntiSpyware/Personal Firewall checks, and **Advanced Endpoint Assessment** for AntiVirus/AntiSpyware/ Personal Firewall remediation.

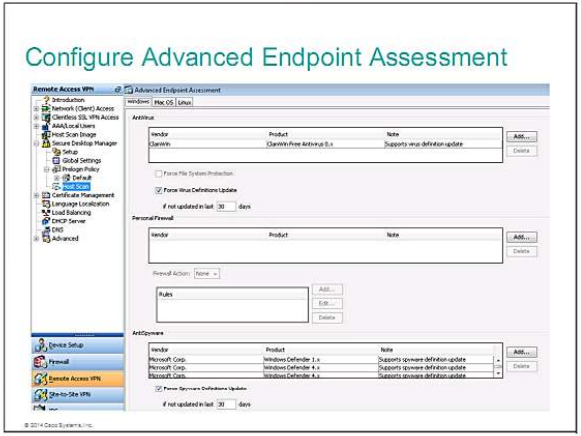
You must have the Advanced Endpoint Assessment license to be be able to activate this Host Scan extension. An example of the **show activate-key** command output on the Cisco Adaptive Security Appliance with the license enabled follows:

```
HQ-ASA# show activation-key
Serial Number:  FCH1705J941
Running Permanent Activation Key: 0xe337d553 0x3828d5fe 0xa531edc0 0xdbfce8d8
0xc723e0b4
Running Timebased Activation Key: 0x12218fca 0x95e5614b 0x39b93a43 0xec870023
0x0694bc96
The Running Activation Key feature: 7 security contexts exceed the limit on the
platform, reduced to 5 security contexts.
Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 100            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        356 days
Security Contexts                 : 5              perpetual
GTP/GPRS                          : Disabled       perpetual
```

```
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Enabled        356 days
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        356 days
Intercompany Media Engine         : Disabled       perpetual
IPS Module                        : Enabled        356 days
Cluster                           : Disabled       perpetual
This platform has an ASA 5515 Security Plus license.
The flash permanent activation key is the SAME as the running permanent key.
Active Timebased Activation Key:
0x12218fca 0x95e5614b 0x39b93a43 0xec870023 0x0694bc96
Encryption-3DES-AES               : Enabled    356 days
Security Contexts                 : 5          356 days
Advanced Endpoint Assessment      : Enabled    356 days
Botnet Traffic Filter             : Enabled    356 days
IPS Module                        : Enabled    356 days
```

Configure Advanced Endpoint Assessment

This topic describes how to configure Advanced Endpoint Assessment.

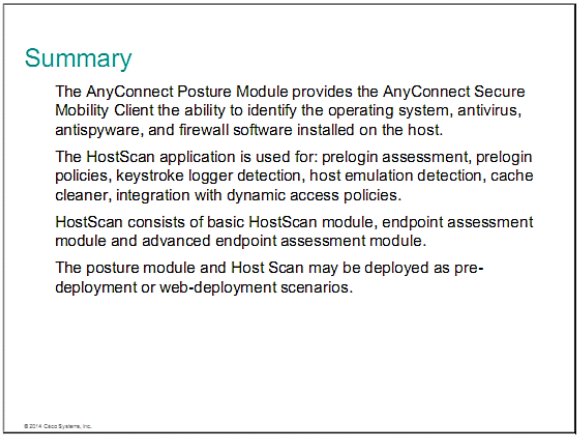


The Advanced Endpoint Assessment functionality allows you to describe the AntiVirus, Personal Firewall, and AntiSpyware software requirements for VPN endpoints running various operating systems: Windows, Mac OS, and Linux.

For each software product you specify the vendor and product name. Optionally you can enforce definitions update if the product has not been updated longer than a defined number of days.

Summary

This topic summarizes the key points that were discussed in this lesson.



Lesson 2

Implementing DAP for SSL VPNs

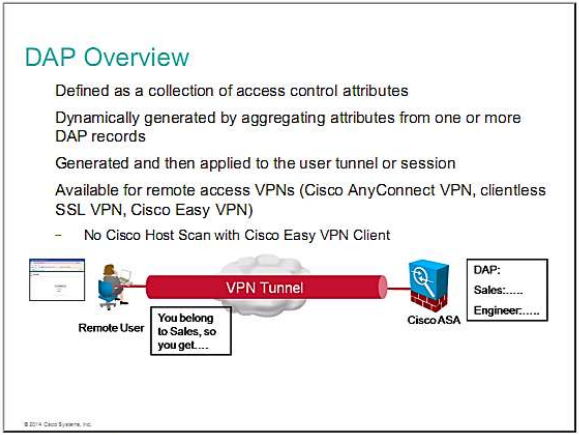
This lesson describes DAP for SSL VPNs.

Upon completing this lesson, you will be able to:

- Describe the Dynamic Access Policy (DAP) feature of the Cisco ASA security appliance
- Describe the DAP solution components
- Describe the DAP hierarchy
- Describe the DAP operations
- Describe factors affecting DAP
- Describe integration of DAP with Host Scan
- Describe a DAP with Host Scan integration scenario
- Describe how to modify the DAP with Host Scan integration scenario
- Describe how to configure the DAP to match compliant antispyware software
- Describe how to configure the DAP to match compliant antivirus software
- Describe how to verify and troubleshoot DAP

DAP Overview

This topic describes the DAP feature of the Cisco Adaptive Security Appliance.



DAP on the Cisco ASA enables you to configure authorization that addresses many variables that are found in various remote access VPNs. Setting a collection of access control attributes that are associated with a specific user tunnel or session can create a DAP. These attributes address issues of multiple group membership and endpoint security. By creating a DAP, the Cisco ASA can grant access to a particular user for a particular session, based on the configured policies. The security appliance generates a DAP at the time that the user connects by selecting or aggregating attributes from one or more DAP records. The DAP records are selected based on the endpoint security information of the remote device and the AAA information for the authenticated user. The Cisco ASA then applies the DAP record to the user tunnel or session.

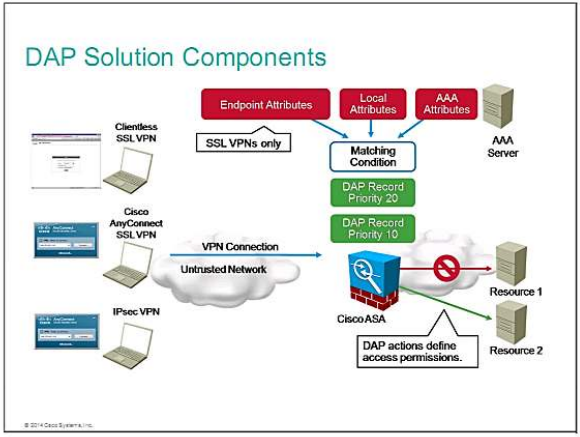
DAP selection configuration files are text files that contain criteria that the Cisco ASA uses for selecting and applying DAP records during session establishment. These files are stored on the Cisco ASA. You can use Cisco Adaptive Security Device Manager to modify and upload these files to the Cisco ASA in XML data format.

DAP selection configuration files include all of the attributes that are configured. These attributes can include AAA attributes, endpoint attributes, and access policies as configured in network and webtype ACL filter, port-forwarding, and URL lists. The DfltAccessPolicy policy is always the last entry in the DAP summary table, and it always has a priority of 0. You can configure access policy attributes for the default access policy, but it does not contain—and you cannot configure—AAA or endpoint attributes. You cannot delete the DfltAccessPolicy policy and it must be the last entry in the summary table.

DAPs apply to both IPsec and SSL VPNs. In this lesson we discuss DAPs as they apply to SSL VPN connections.

DAP Solution Components

This topic describes the DAP solution components.



There are several components of a DAP solution:

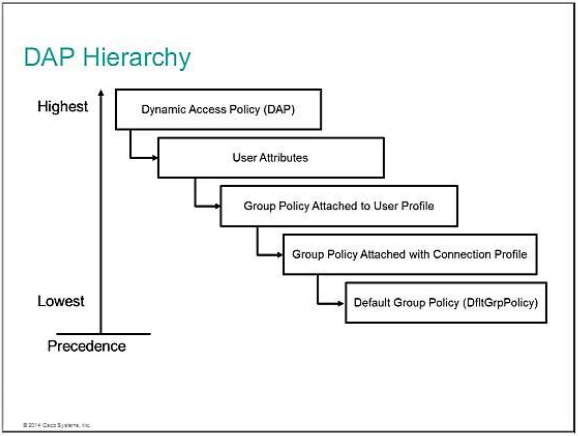
One or more DAP records: DAP records define a limited set of VPN authorization attributes that can override authorization attributes that are defined locally or provided by a AAA server. One or more DAP records are selected based on AAA attributes of a user or endpoint attributes. Authorization attributes from DAP records are then combined into a DAP policy and assigned to a VPN session. Each DAP record is identified using a name and each record has a priority. The Cisco Adaptive Security Appliance uses this value to logically sequence the access lists when it aggregates the network and webtype ACLs from multiple DAP records.

Local and AAA attributes: DAP records can be selected based on AAA information that is provided locally or by a AAA server when users authenticate to a VPN session.

Endpoint attributes of connecting VPN clients: DAP records can also be selected based on endpoint attributes of connecting clients. These endpoint attributes can be determined from the type of VPN connection or by using Cisco Host Scan.

DAP Hierarchy

This topic describes the DAP hierarchy.



The Cisco Adaptive Security Appliance supports several methods of applying user authorization attributes (also called user entitlements or permissions) to VPN connections. You can configure the ASA to obtain user attributes from any combination of:

DAP on the ASA

External RADIUS or LDAP authentication and/or authorization server

Group policy on the ASA

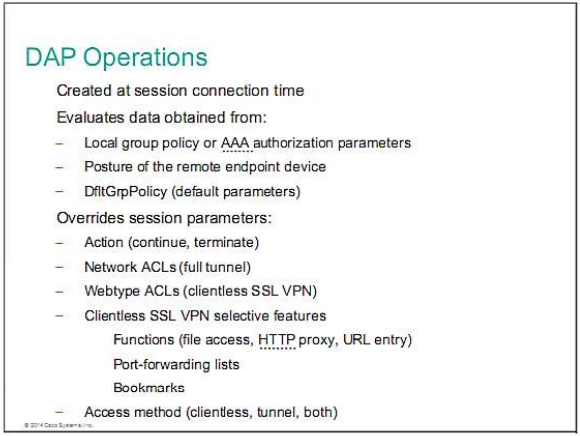
If the ASA receives attributes from all sources, the attributes are evaluated, merged, and applied to the user policy. If there are conflicts between attributes, the DAP attributes take precedence.

You can apply access control mechanisms at different levels in the VPN system. This precedence model determines effective access permissions (listed from highest to lowest precedence):

1. **DAP:** DAP rules are built at session connection time and can consider account temporary parameters, such as the endpoint security posture. The precedence among multiple DAP policies is configured using a precedence value.
2. **User profile:** Parameters that are configured at the user level are the most granular settings that are statically configured (without considering security posture).
3. **Group policy attached to the user profile:** Parameters are defined in a group policy that is attached to the individual user.
4. **Group policy attached to the connection profile:** Parameters are defined in a group policy that is attached to the connection profile to which the user connects.
5. **DfltGrpPolicy settings:** This default group policy is preconfigured on the security appliance with default parameters. You can modify it but you cannot remove it. By default, all other policy groups and users inherit the settings from the DfltGrpPolicy.

DAP Operations

This topic describes the DAP operations.



The DAP is created at session connection time, based on multiple DAP records. DAP records, which are used to create the DAP, are selected based on parameters that are obtained from a local group or from AAA authorization parameters and the posture of remote endpoint devices.

DAP overrides authorization parameters that are obtained from a local group policy or from a AAA server. A DAP can provide the following authorization parameters:

Action: There are two possible actions:

- **Continue:** Continues with session and specifies special processing to apply to specific connection.
- **Terminate:** Terminates a session.

ACLs: Specifies already-configured network ACLs to add to a DAP record. This parameter applies to full-tunnel VPN sessions.

Webtype ACLs: Specifies already-configured webtype ACLs to add to a DAP record. This parameter applies to clientless SSL VPN sessions.

Functions: Enables file server entry and browsing, HTTP proxy, and URL entry for the DAP record:

- **File Server Browsing:** Enables or disables CIFS browsing for file servers or shared features.
- **File Server Entry:** Allows or prevents a user from entering file server paths and names on the portal page. When enabled, this feature places the file server entry drawer on the portal page. Users can enter pathnames to Windows files directly. They can download, edit, delete, rename, and move files. They can also add files and folders. Shares must also be configured for user access on the applicable Windows servers. Users might have to be authenticated before accessing files, depending on network requirements.

- **HTTP Proxy:** Affects the forwarding of an HTTP applet proxy to the client. The proxy is useful for technologies that interfere with correct content transformation, such as Java, ActiveX, and Flash. It bypasses mangling while ensuring the continued use of the security appliance. The forwarded proxy modifies the old proxy configuration of the browser automatically, and redirects all HTTP and HTTPS requests to the new proxy configuration. It supports virtually all client-side technologies, including HTML, CSS, JavaScript, VBScript, ActiveX, and Java. The only browser that it supports is Microsoft Internet Explorer.
- **URL Entry:** Allows or prevents a user from entering HTTP and HTTPS URLs on the portal page. If this feature is enabled, users can enter web addresses in the URL entry box, and use clientless SSL VPN to access those websites.

Port Forwarding Lists: Selects port-forwarding lists for user sessions.

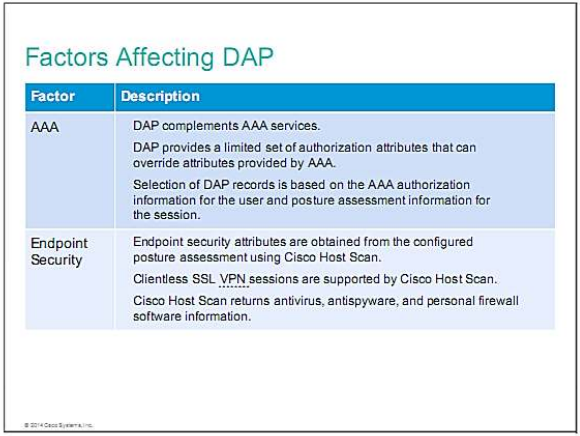
Bookmarks: Selects port-forwarding lists for user sessions.

Access Method: Configures the type of remote access that is permitted:

- **Unchanged:** Continue with the current remote access method.
- **AnyConnect Client:** Connect using the Cisco AnyConnect VPN Client.
- **Web-Portal:** Connect with clientless VPN.
- **Both-Default-Web-Portal:** Connect via either clientless or the Cisco AnyConnect VPN client, with a default of clientless.
- **Both-Default-AnyConnect Client:** Connect via either clientless or the Cisco AnyConnect client, with a default of Cisco AnyConnect.

Factors Affecting DAP

This topic describes factors that affect DAP.



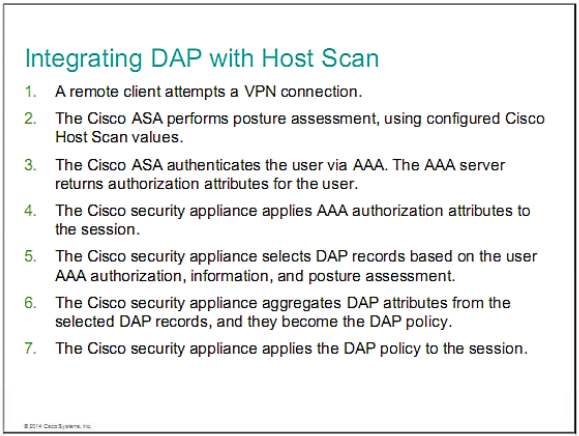
DAP complements AAA services. It provides a limited set of authorization attributes that can override the authorization attributes that AAA provides. The Cisco Adaptive Security Appliance selects DAP records based on the AAA authorization information for the user and posture assessment information for the session. Depending on this information, the security appliance can select multiple DAP records, which it then aggregates to create DAP authorization attributes.

You can specify AAA attributes from the Cisco AAA attribute hierarchy or from the full set of response attributes that the security appliance receives from a RADIUS or LDAP server.

The Cisco Adaptive Security Appliance obtains endpoint security attributes by using a posture assessment that Cisco Host Scan performs.

Integrating DAP with Host Scan

This topic describes integration of DAP with Host Scan.

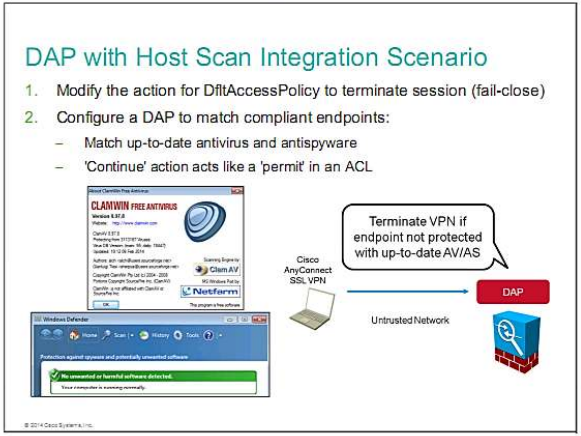


DAP is applied in the following sequence:

1. A remote client attempts a VPN connection.
2. The Cisco Adaptive Security Appliance performs posture assessment, using configured Cisco Host Scan values.
3. The Cisco ASA authenticates the user via AAA. The AAA server returns authorization attributes for the user.
4. The Cisco security appliance applies AAA authorization attributes to the session.
5. The Cisco security appliance selects DAP records based on the user AAA authorization, information, and posture assessment.
6. The Cisco security appliance aggregates DAP attributes from the selected DAP records, and they become the DAP policy.
7. The Cisco security appliance applies the DAP policy to the session.

DAP with Host Scan Integration Scenario

This topic describes a DAP with Host Scan integration scenario.

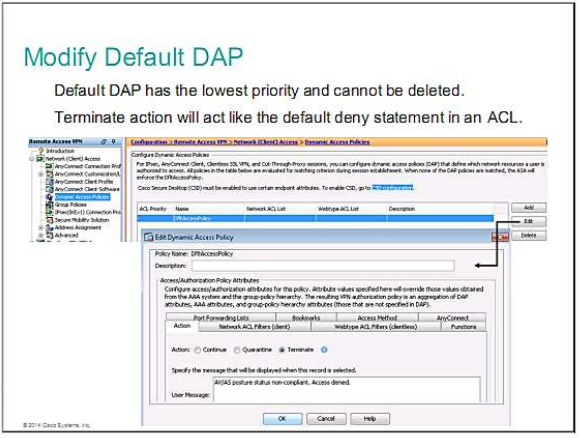


In this scenario you will implement DAP to ensure that VPN access is only permitted from compliant endpoints. The compliance status is achieved when the endpoint runs an up-to-date antispyware (Windows Defender) and antivirus software (ClamWin AntiVirus).

First you will modify the default DAP to terminate the VPN sessions. This rule will act similarly to the 'deny any any' statement at the end of an ACL. Then you will define a custom DAP that will match the compliant antivirus/antispyware software and permit access for compliant endpoints.

Modify Default DAP

This topic describes how to modify the default DAP.



When a user tries to establish a connection, DAP can analyze the posture assessment result of a remote host and apply access policies that are dynamically generated. DAP can use the AAA attributes, such as RADIUS, LDAP, and Cisco-specific, and endpoint attributes, such as host scans and prelogin locations, before an action or a series of actions can be applied to a user session. It is designed to complement the AAA services by aggregating the locally defined attributes with the received attributes from the AAA server. In the case of an authorization attribute conflict, the locally defined attribute is selected. Therefore, it is possible to generate DAP authorization attributes by aggregating multiple DAP records from the AAA server and the posture assessment information for a user session. This way, the security appliance can use the prelogin sequence, the user login credentials, and the computer scan results before a DAP can be applied to a session.

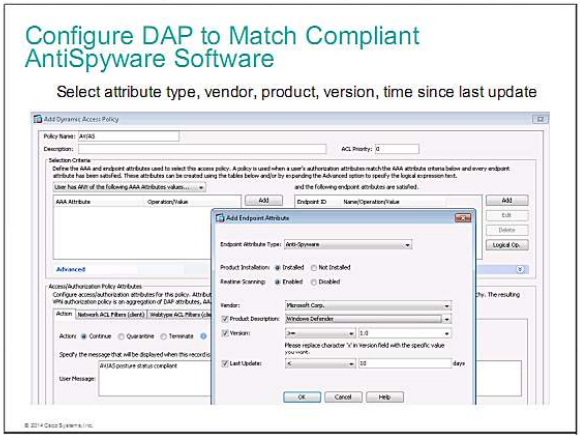
A user connection might match multiple DAP records. For example, you can have a DAP record that only scans the remote workstations for a registry key. You can have another DAP record that checks the remote computer for an active process. If a remote workstation has the registry key and the process is active as well, that workstation will match against both DAP records. In this case, the security appliance combines both records dynamically and applies an aggregated access policy to a user connection.

The security appliance has a default DAP record called DfltAccessPolicy. This DAP record cannot be deleted and can contain only access policy attributes. It does not allow you to define any AAA or endpoint selection attributes. It is applied to all sessions that do not match any configured DAP records. By default, the DfltAccessPolicy does not restrict a session and allows traffic to pass through without imposing any access policies.

In this scenario, you change the default DAP action to terminate the VPN sessions. This policy will catch and terminate all connection attempts that have not been permitted using a specific DAP. In this role it resembles a **deny any any** rule at the end of an access list.

Configure DAP to Match Compliant AntiSpyware Software

This topic describes how to configure a DAP to match compliant antispyware software.

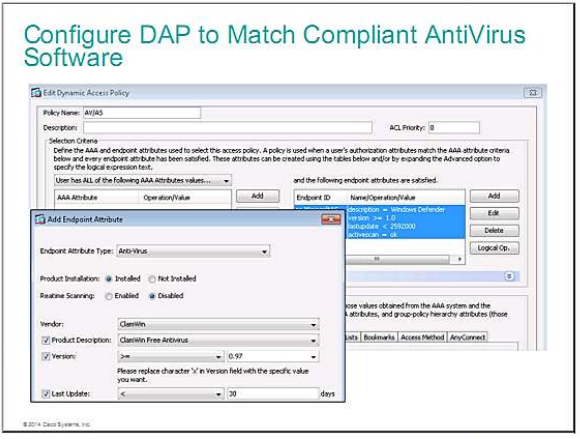


This figure illustrates how you create a custom DAP (antivirus/antispyware) and add an endpoint attribute that matches compliant antispyware software. You select the endpoint attribute type (antispyware), choose that it must be installed and actively scanning. Then you select the vendor, the specific product, the desired version, and maximum number of days since the last update.

If the endpoint matches the antispyware requirement, the action is set to continue and inform the client that the antivirus/antispyware posture status is compliant.

Configure DAP to Match Compliant AntiVirus Software

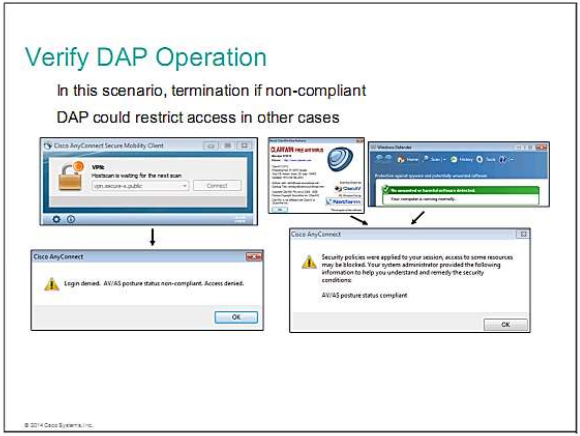
This topic describes how to configure a DAP to match compliant antivirus software.



You can add another condition to the custom DAP (antivirus/antispyware), which checks the status of the antivirus software. In this case the real-time scanning is not required. ClamWin Free Antivirus, matched in this scenario, does not support realtime scanning.

Verify DAP Operation

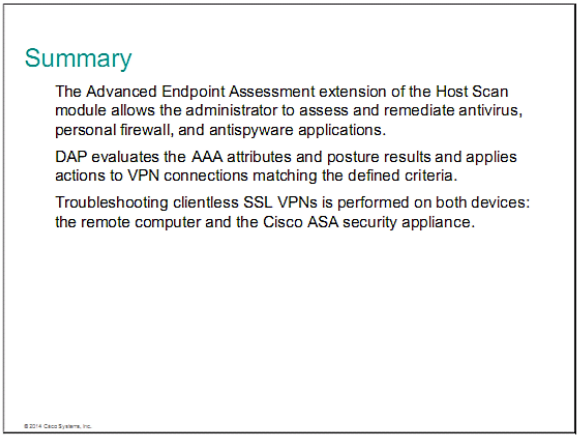
This topic describes how to verify DAP operation.



To verify DAP on the client side, log into a VPN session. The example on the left shows the notification in case of non-compliant security posture. If the antivirus/antispyware is installed and up-to-date, the client will see a notification shown on the right.

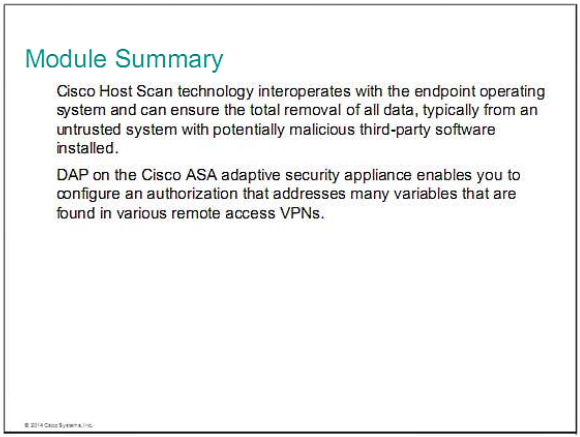
Summary

This topic summarizes the key points that were discussed in this lesson.



Module Summary

This topic summarizes the key points that were discussed in this module.



References

For additional information, refer to these resources:

Cisco Systems, Inc. *Configuring Dynamic Access Policies*. http://www.cisco.com/en/US/docs/security/asa/asa84/asdm64/configuration_guide/vpn_asdm_dap.pdf

Module Self-Check

Questions

Use the questions here to review what you learned in this module.

1. Which of the following are valid HostScan packages? (Choose two.) (Source: Implementing Host Scan)

   A. advanced endpoint assessment
   B. basic endpoint assessment
   C. basic host scan
   D. endpoint assessment

2. Which of the following is a Host Scan extension that provides remediation? (Source: Implementing Host Scan)

   A. advanced endpoint assessment
   B. basic host scan
   C. basic endpoint assessment
   D. DAP
   E. endpoint assessment
   F. NAC

3. Which of the following licenses must be installed on the Cisco ASA in order for HostScan to examine the remote computer for antivirus and antispyware applications? (Source: Implementing Host Scan)

   A. Advanced Endpoint Assessment license
   B. AnyConnect for Mobile license
   C. AnyConnect Premium license
   D. GTP/GPRS license

4. Which of the following statements is true for Cisco AnyConnect HostScan? (Source: Implementing Host Scan)

   A. It installs on the remote device after the user connects to the ASA and logs in.
   B. It is a component of the Cisco AnyConnect Posture Module.
   C. It automatically identifies operating systems and service packs on any remote device establishing a Cisco clientless SSL VPN or AnyConnect client session.
   D. It runs on Microsoft Windows, Apple Mac OS X, Chrome OS, and Linux.
   E. You can configure it to inspect the endpoint for specific files and registry keys after full tunnel establishment.

5. Which of the following options does the DAP feature apply to? (Source: Implementing DAP for SSL VPNs)

   A. AnyConnect IPsec VPNs only
   B. AnyConnect SSL VPNs only
   C. clientless SSL VPNs only
   D. AnyConnect IPsec and SSL VPNs only
   E. AnyConnect SSL VPNs and clientless SSL VPNs only
   F. AnyConnect IPsec VPNs, AnyConnect SSL VPNs, and clientless SSL VPNs

6. Which of the following statements are true for the DAP feature of the Cisco ASA adaptive security appliance? (Choose all that apply.) (Source: Implementing DAP for SSL VPNs)

   A. It evaluates AAA attributes and posture results and applies actions to VPN connections matching the defined criteria.
   B. It enables you to configure authorization that addresses many variables that are found in various remote access VPNs.
   C. Authorization parameters that are obtained from a local group policy or from a AAA server override it.
   D. It is generated by the Cisco ASA at the time that the user connects.

Answer Key

1. A, C, D
2. A
3. C
4. B, C
5. F
6. A, B, D

Glossary

Term	Definition
AAA	authentication, authorization, and accounting. Pronounced "triple a."
ACE	access control entry.
ACL	access control list. A list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).
ACL	access control list. A list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).
AIA	Authority Information Access.
CA	certification authority. Entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.
CDP	CRL distribution point.
CIFS	Common Internet File System.
CLI	command-line interface. An interface that allows the user to interact with the operating system by entering commands and optional arguments. The UNIX operating system and DOS provide CLIs.
CRL	certificate revocation list. Data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire.
CSD	Cisco Secure Desktop
CSS	Cascading Style Sheets
DAP	dynamic access policy.
DART	Diagnostic and Reporting Tool
DHCP	Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.
DMZ	demilitarized zone.
DNS	Domain Name System. System used on the Internet for translating names of network nodes into addresses.
DPD	dead peer detection.
DTLS	Datagram Transport Layer Security.
EAP	Extensible Authentication Protocol. Framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences.

Term	Definition
GPO	group policy object.
GUI	graphical user interface. A user environment that uses pictorial as well as textual representations of the input and the output of applications and the hierarchical or other data structure in which information is stored. Such conventions as buttons, icons, and windows are typical, and many actions are performed using a pointing device (such as a mouse). Microsoft Windows and the Apple Macintosh are prominent examples of platforms using a GUI.
HTTP	Hypertext Transfer Protocol. The protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.
IEEE	Institute of Electrical and Electronics Engineers. Professional organization whose activities include the development of communications and network standards. IEEE LAN standards are the predominant LAN standards today.
IKE	Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IPsec) that require keys. Before any IPsec traffic can be passed, each router, firewall, or host must verify the identity of its peer. Verification can be done by manually entering pre-shared keys into both hosts or by a CA service.
IP address	32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address. CIDR provides a new way of representing IP addresses and subnet masks. Also called an Internet address.
IPsec	IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

Term	Definition
IPv4	IP version 4. Internet Protocol version 4 is the fourth version in the development of the IP and the first version of the protocol to be widely deployed. Along with IPv6, IPv4 is at the core of standards-based internetworking methods of the Internet. IPv4 is still used to route most traffic across the Internet. IPv4 is a connectionless protocol for use on packet-switched link layer networks (for example, Ethernet). It operates on a best-effort delivery model in that it does not guarantee delivery and does not assure proper sequencing or avoidance of duplicate delivery.
IPv6	IP version 6. Replacement for the current version of IP (version 4). IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).
LDAP	Lightweight Directory Access Protocol. Protocol that provides access for management and browser applications that provide read/write interactive access to the X.500 Directory.
MSI	Microsoft Windows Installer.
NAT	Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as Network Address Translator.
OCSP	Online Certificate Status Protocol.
PKI	public-key infrastructure. System of CAs (and, optionally, RAs and other supporting servers and agents) that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography.
PLAP	Pre-Login Access Provider.
RADIUS	Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.
RFC	Request for Comments. Document series that is used as the primary means for communicating information about the Internet. Some RFCs are designated by the IAB as Internet standards. Most RFCs document protocol specifications, such as Telnet and FTP, but some RFCs are humorous or historical. RFCs are available online from numerous sources.
RSA	Acronym stands for Rivest, Shamir, and Adleman, the inventors of the technique. Public-key cryptographic system that can be used for encryption and authentication.
SBL	Start Before Logon.
SCEP	Simple Certificate Enrollment Protocol.
SDI	Security Dynamics International.

Term	Definition
SMS	Microsoft Systems Management Server.
SSL	Secure Socket Layer. Encryption technology for the Web used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.
TACACS+	Terminal Access Controller Access Control System Plus. Proprietary Cisco enhancement to TACACS. Provides additional support for authentication, authorization, and accounting.
TCP	Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.
TLS	Transport Layer Security. A future IETF protocol to replace SSL.
TND	Trusted Network Detection.
UDP	User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.
URL	uniform resource locator. Type of formatted identifier that describes the access method and the location of an information resource object on the Internet. [RFC 1738]
VBScript	Visual Basic Scripting Edition
VPN	virtual private network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunneling to encrypt all information at the IP level.
VPN	virtual private network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunneling to encrypt all information at the IP level.
XML	extensible markup language. A standard maintained by the World Wide Web Consortium (W3C). It defines a syntax that lets you create markup languages to specify information structures. Information structures define the type of information, for example, subscriber name or address, not how the information looks (bold, italic, and so on). External processes can manipulate these information structures and publish them in a variety of formats. Text markup language designed to enable the use of SGML on the World Wide Web. XML allows you to define your own customized markup language.

Term	Definition
XML	extensible markup language. A standard maintained by the World Wide Web Consortium (W3C). It defines a syntax that lets you create markup languages to specify information structures. Information structures define the type of information, for example, subscriber name or address, not how the information looks (bold, italic, and so on). External processes can manipulate these information structures and publish them in a variety of formats. Text markup language designed to enable the use of SGML on the World Wide Web. XML allows you to define your own customized markup language.