Remote Access VPN

TECHNOLOGY DESIGN GUIDE

August 2013

VALIDATED DESIGN

Table of Contents

Preface

Cisco Validated Designs (CVDs) provide the framework for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested and validated design and deployment details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands at a CLI or script prompt appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000 packets conform-action set-discard-class-transmit 48 exceed-action transmit
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the feedback form.

For the most recent CVD guides, see the following site:

http://www.cisco.com/go/cvd

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

Use Cases

This guide addresses the following technology use cases:

- **Highly Available, Secure Access to Internal Data Resources for Remote Users**–You use the Cisco AnyConnect Secure Mobility Client to connect remote users to a primary-site Cisco Adaptive Security Appliance (ASA) firewall. A well-designed VPN remote-access network needs to be tolerant of the most commonly observed failure types. This type of resiliency is accomplished with a single-site design that includes only a firewall pair using static default routing to the Internet.

For more information, see the "Use Cases" section in this guide.

Scope

This guide covers the following areas of technology and products:

- Cisco ASA 5500-X Series Adaptive Security Appliances for client-based remote-access VPN
- Cisco AnyConnect Secure Mobility Client for remote users who require full network connectivity
- Demilitarized zone (DMZ) and outside network LAN switching
- Management of user authentication and policy
- Integration of the above with the LAN switching infrastructure

For more information, see the "Design Overview" section in this guide.

Proficiency

This guide is for people with the following technical proficiencies–or equivalent experience:

- **CCNA Routing and Switching**–1 to 3 years installing, configuring, and maintaining routed and switched networks
- **CCNA Security**–1 to 3 years installing, monitoring, and troubleshooting network devices to maintain integrity, confidentiality, and availability of data and devices

Related CVD Guides

Firewall and IPS Technology Design Guide

Device Management Using ACS Technology Design Guide

Remote Mobile Access Technology Design Guide

To view the related CVD guides, click the titles or visit the following site: http://www.cisco.com/go/cvd

Introduction

The *Remote Access VPN Design Guide* supports the remote user with secure remote access (RA). This guide covers the deployment of RA VPN services to either the primary Internet edge firewall or to a standalone RA VPN-specific device.

Related Reading

The Firewall and IPS Design Guide focuses on the Internet edge firewall and intrusion prevention system (IPS) security services that protect your organization's gateway to the Internet.

The Remote Mobile Access Design Guide extends the remote access solution for mobile devices, such as phones and tablets, and for traditional devices, it offers expanded connection options, such as Cisco Cloud Web Security, Always-on VPN, and other features.

Technology Use Cases

Many organizations need to offer network connectivity to their data resources for users, regardless of the user's location. Employees, contractors, and partners may need to access the network when traveling or working from home or from other off-site locations. The remote-access connectivity should support:

- A wide variety of endpoint devices.
- Seamless access to networked data resources.
- Authentication and policy control that integrates with the authentication resources in use by the organization.
- Cryptographic security to prevent the exposure of sensitive data to unauthorized parties who accidentally or intentionally intercept the data.

Use Case: Highly Available, Secure Access to Internal Data Resources for Remote Users

You use the Cisco AnyConnect Secure Mobility Client to connect remote users to a primary site Cisco ASA firewall. A well designed VPN remote access network needs to be tolerant of the most commonly observed failure types. This type of resiliency is accomplished with a single-site design that includes only a firewall pair using static default routing to the Internet.

This design guide enables the following network and security capabilities:

- **User authentication**–The AnyConnect client requires all remote-access users to authenticate before negotiating a secure connection. Both centralized authentication and local authentication options are supported.
- **Differentiated access**–The remote access VPN is configured to provide different access policies depending on assigned user roles.
- **Strong encryption for data privacy**–The Advanced Encryption Standard (AES) cipher with a key length of 256 bits is used for encrypting user data. Additional ciphers are also supported.
- **Hashing for data integrity**–The Secure Hash Standard 1 (SHA-1) cryptographic hash function with a 160-bit message digest is used to ensure that data has not been modified during transit.
- **Device resiliency**–The Cisco ASA firewall supports failover between and the active and standby units of a resilient firewall pair in the event of a hardware failure.
- **Internet link resiliency**–A backup server reachable through the secondary ISP is configured in the AnyConnect client profile. This backup server is automatically used if the primary server is not reachable.

Design Overview

The Cisco ASA family supports IP Security (IPsec), web portal, full-tunnel Secure Sockets Layer (SSL) VPNs for client-based remote access, and IPsec for site-to-site VPN. This section describes the basic configuration of SSL VPNs for remote access.

The Cisco AnyConnect Secure Mobility Client is recommended for remote users who require full network connectivity. The Cisco AnyConnect client uses SSL and is designed for automated download and installation. SSL access can be more flexible and is likely to be accessible from more locations than IPsec, as few companies block HTTPS access out of their networks.

This CVD design guide offers two different remote-access VPN designs:

- **Remote-access (RA) VPN integrated with Cisco ASA Series firewall, in the integrated design model**—This integration offers lower capital investment and reduces the number of devices the network engineering staff must manage.
- **Remote-access VPN deployed on a pair of standalone Cisco ASAs, in the standalone design model**—This design offers greater operational flexibility and scalability while providing a simple migration path from an existing RA VPN installation.

This document describes the configuration for remote-access VPN via Cisco AnyConnect for SSL connections. The configuration is broken into sections for each of the various access methods, and it begins with a configuration that is common to all of the access methods. Configurations for both the integrated and standalone design models offer identical functionality and capability so that regardless of the design chosen, the user experience is unchanged from one design to the other. Unless specifically noted, the configuration described in this document is common to both the integrated and standalone designs.

Hardware applied in this design is selected based on the following performance values.

Table 1 - Hardware performance

Cisco ASA family product	Maximum SSL VPN sessions
Cisco ASA 5512-X	250
Cisco ASA 5515-X	250
Cisco ASA 5525-X	750
Cisco ASA 5545-X	2500

A different VPN group is required for each remote-access policy. This design includes three VPN groups:

- **Administrative users**—These users are authenticated by Cisco Secure Access Control System (ACS) using the RADIUS protocol and also have a local username and password fallback option. This ensures that VPN access is available when the Cisco Secure ACS or Microsoft Active Directory server is unavailable. Administrative users have full access to the entire network.
- **Employees**—These users are authenticated by Cisco Secure ACS and have open access to the entire network
- **Partners**—These users are authenticated by Cisco Secure ACS and, although they use a tunnel-all VPN policy, there is an access-list applied to the tunnels in order to restrict access to specific hosts.

Reader Tip

For more information about the baseline configuration of the appliance (including availability, routing, Internet and inside connectivity, and management or administration access), see the Firewall and IPS Design Guide.

Cisco ASA's remote-access VPN termination capabilities can be configured from the command line or from the graphical user interface Cisco Adaptive Security Device Manager (ASDM). Cisco ASDM provides a guided step-by-step approach to the configuration of RA VPN and reduces the likelihood of configuration errors.

PROCESS

Configuring Cisco Secure ACS

1. Define external groups
2. Create the device-type group
3. Create the network device
4. Create authorization profiles
5. Configure the access service
6. Create authorization rules

Authentication is the portion of the configuration that verifies that users' credentials (username and password) match those stored within the organization's database of users that are allowed to access electronic resources. This design guide uses either Cisco Secure ACS or Microsoft Active Directory for authentication of remote access VPN users. Cisco Secure ACS gives an organization enhanced ability to control the access that VPN users receive. For those organizations not interested in using Cisco Secure ACS, Microsoft Active Directory by itself will be used, and this process can be skipped.

When the Cisco ASA firewall queries the Cisco Secure ACS server (which then proxies the request to the Active Directory database) to determine whether a user's name and password is valid, Cisco Secure ACS also retrieves other Active Directory attributes, such as group membership, that Cisco Secure ACS may use when making an authorization decision. Based on the group membership, Cisco Secure ACS sends back a group policy name to the appliance, along with the success or failure of the login. Cisco ASA uses the group policy name in order to assign the user to the appropriate VPN group policy.

In this process, Active Directory is the primary directory container for user credentials and group membership. Before you begin this process, your Active Directory must have three groups defined: vpn-administrator, vpn-employee, and vpn-partner. These groups map users to the respective VPN access policies.

Procedure 1 Define external groups

Step 1: Navigate to the Cisco Secure ACS Administration Page. (Example: https://acs.cisco.local)

Step 2: In **Users and Identity Stores > External Identity Stores > Active Directory**, click the **Directory Groups** tab.

Step 3: Click **Select**.

Step 4: In the External User Groups pane, select the three vpn groups, and then click **OK**.

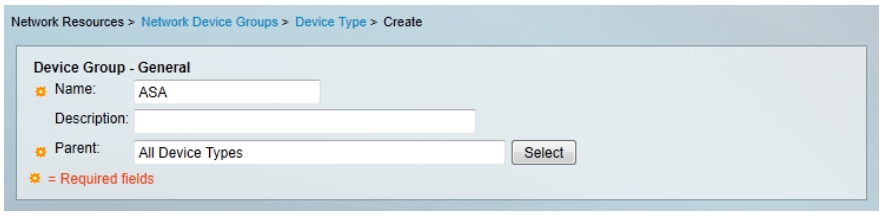
Step 5: In the Active Directory pane, click **Save Changes**.

Procedure 2 Create the device-type group

Step 1: In **Network Resources > Network Device Groups > Device Type**, click **Create**.

Step 2: In the Name box, enter a name for the group. (Example: ASA)

Step 3: In the Parent box, select **All Device Types**, and then click **Submit**.



Procedure 3 Create the network device

For the Cisco ASA firewall, create a network device entry in Cisco Secure ACS.

Step 1: In **Network Resources > Network Devices and AAA Clients**, click **Create**.

Step 2: In the Name box, enter the device hostname. (Example: IE-ASA5545X)

Step 3: In the Network Device Groups section, in the Device Type row, click on **Select**. In the Network Device Groups dialog box, select **All Device Types:ASA** then click OK.

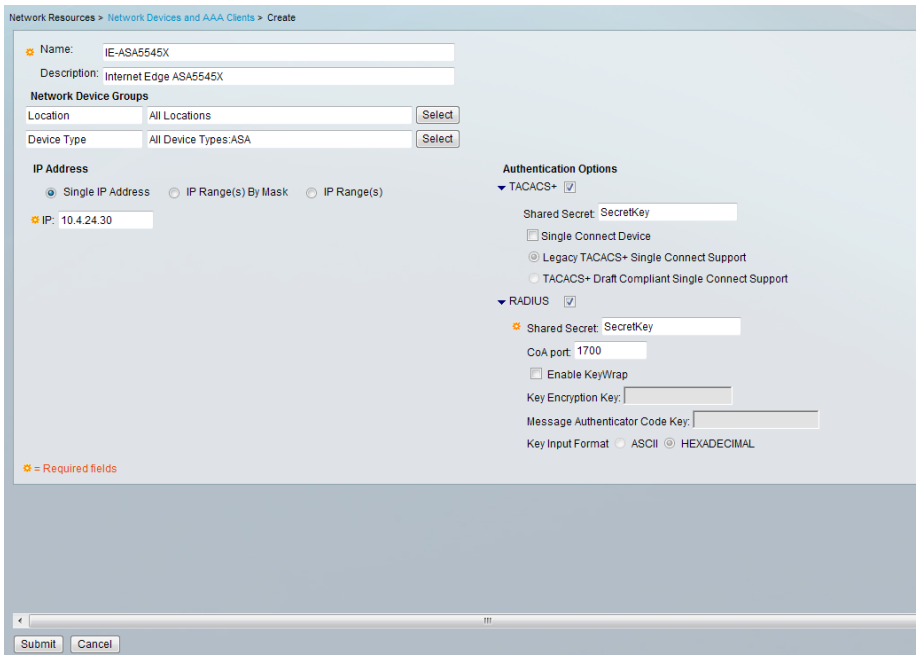
Step 4: In the IP box, enter the inside interface IP address of the Cisco ASA appliance. (Example: 10.4.24.30)

Step 5: Select **TACACS+**.

Step 6: Enter the TACACS+ shared secret key. (Example: SecretKey)

Step 7: Select **RADIUS**.

Step 8: Enter the RADIUS shared secret key, and then click **Submit**. (Example SecretKey)



Procedure 4 Create authorization profiles

Create three different authorization profiles to identify users that belong to the vpn-administrator, vpn-employee, or vpn-partner groups in Active Directory.

Step 1: In **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**, click **Create.**

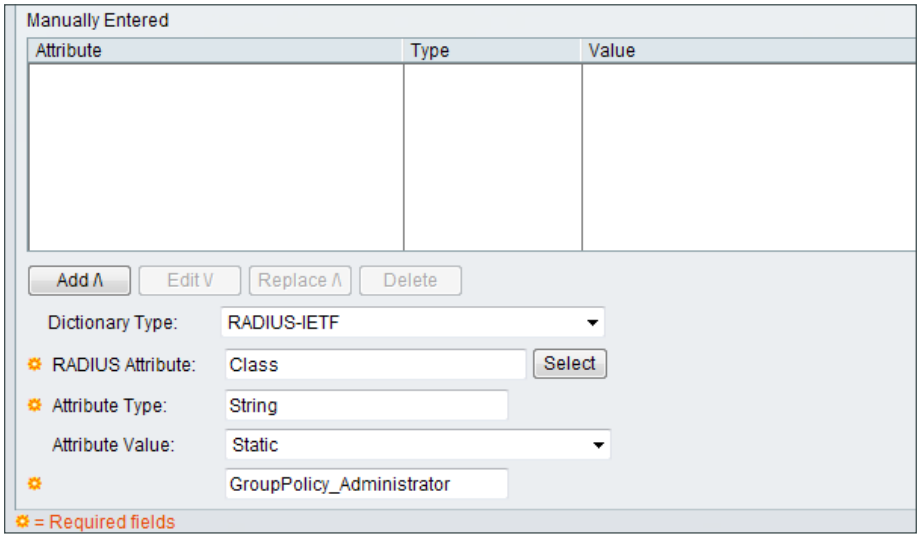
Step 2: In the Name box, enter a name for the authorization profile. (Example: VPN-Administrator)

Step 3: Click the **RADIUS Attributes** tab, and then in the RADIUS Attribute row click **Select**.

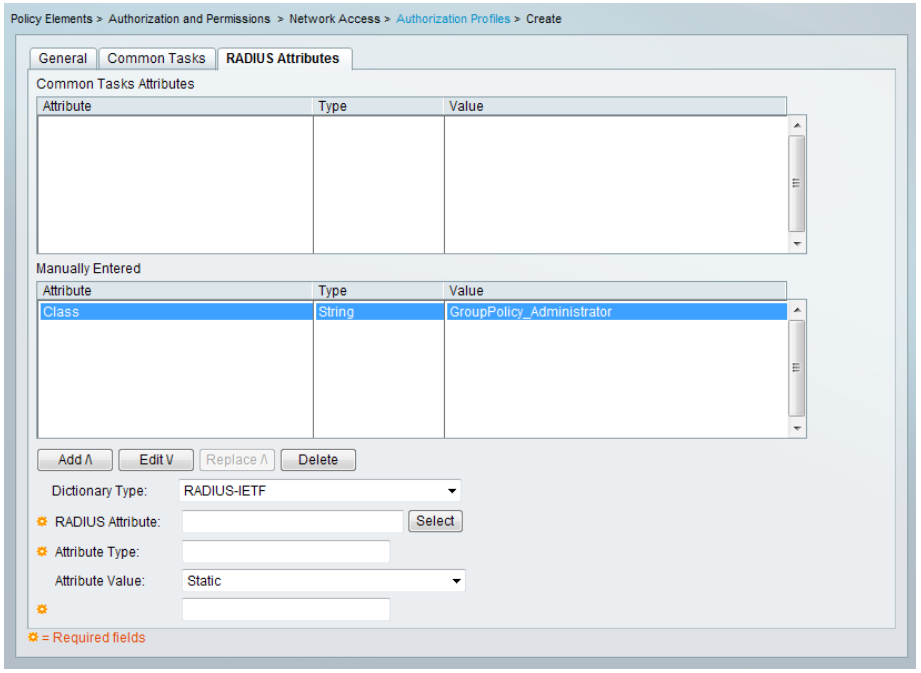
Step 4: In the RADIUS Dictionary dialog box, pane, select **Class** and then click **OK**.

Next, you must configure the attribute value to match the group policy that you will configure on the Cisco ASA appliance.

Step 5: In the Attribute Value box, enter the group policy name, and then click **Add ^**, (Example: GroupPolicy_Administrator).



Step 6: Click **Submit**.



Step 7: Repeat this procedure to build authorization profiles for vpn-employee and vpn-partner, using the group policy **GroupPolicy_Employee** and **GroupPolicy_Partner** values.

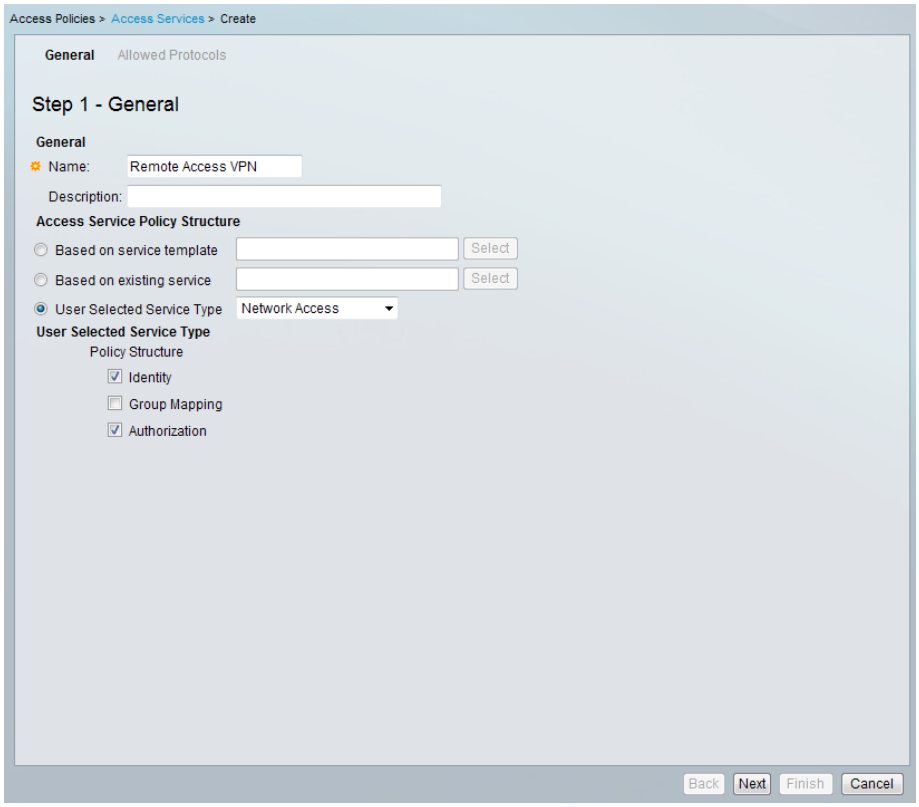
Procedure 5 Configure the access service

Create a policy to inspect for group membership in the return traffic from the Active Directory server.

Step 1: In **Access Policies > Access Services**, click **Create**.

Step 2: On the General tab, enter the name **Remote Access VPN**.

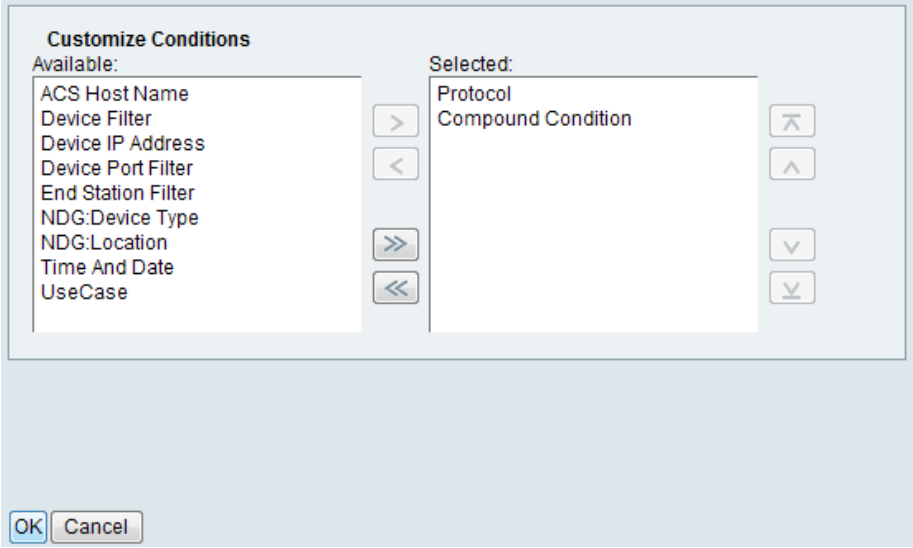
Step 3: Select **User Selected Service Type**, and then click **Next**.



Step 4: On the Allowed Protocols tab, select **Allow MS-CHAPv2**, and then click **Finish**.

Step 5: In **Access Policies > Access Services > Service Selection Rules**, click **Customize**.

Step 6: In the Customize Conditions pane, move **Compound Condition** from **Available** to **Selected**, and then click **OK**.



Step 7: In the Service Selection Rules pane, click **Create**.

Step 8: On the dialog box, for the name of the rule, enter **Remote Access VPN**.

Step 9: Select **Protocol.**

Step 10: In the list at right, select **match**, and then in the box, enter **Radius**.

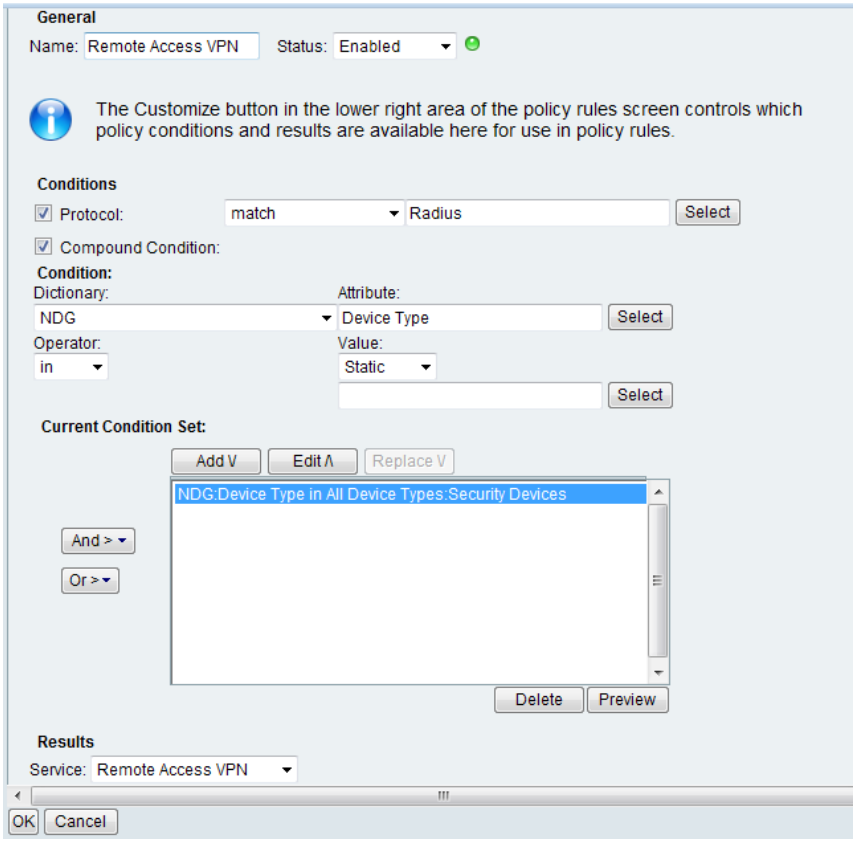
Step 11: Select **Compound Condition**, and then in the Dictionary list, choose **NDG**.

Step 12: For Attribute, select **Device Type.**

Step 13: For Value, select **All Device Types: Security Devices**.

Step 14: Under Current Condition Set, click **Add V**. The information is added to the Current Condition Set.

Step 15: In the **Results Service** list, choose **Remote Access VPN**, click **OK**, and then click **Save Changes**.

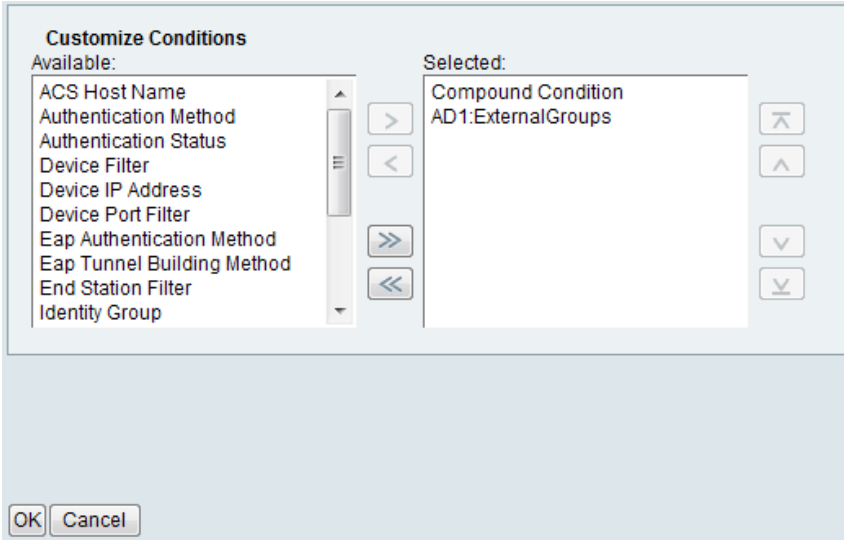


Step 16: Navigate to **Access Policies > Access Services > Remote Access VPN > Identity**.

Step 17: In the Identity Source box, select **AD1**, click **OK**, and then click **Save Changes**.

Step 18: In **Access Policies > Access Services > Remote Access VPN > Authorization**, click **Customize**.

Step 19: In the Customize Conditions pane, move **AD1:ExternalGroups** from **Available** to **Selected**, click OK, and then click **Save Changes**.



Procedure 6 Create authorization rules

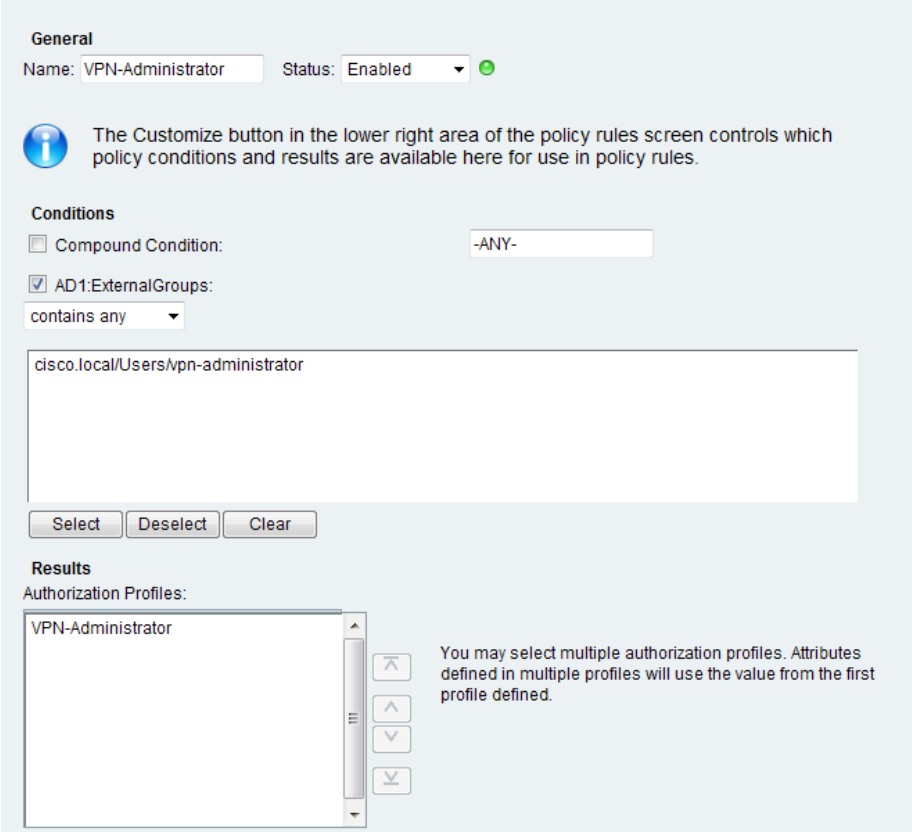
Step 1: In **Access Policies > Access Services > Remote Access VPN > Authorization**, click **Create**.

Step 2: In the **Name** box, enter a rule name. (Example: VPN-Administrator)

Step 3: Under Conditions, select **AD1:ExternalGroups**.

Step 4: In the condition definition box, select the Active Directory group. (Example: cisco.local/Users/vpn-administrator).

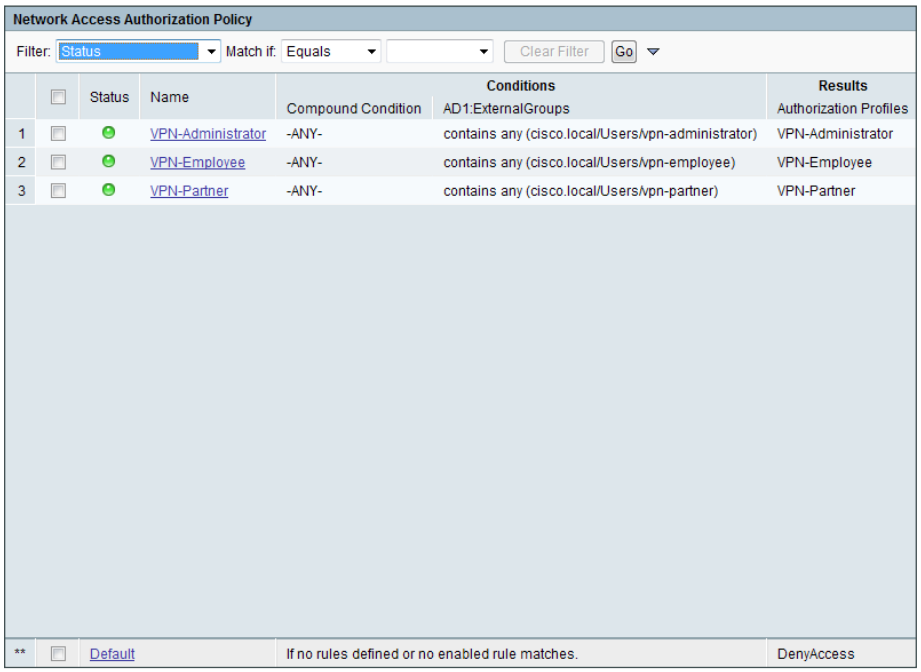
Step 5: Under Results, select the authorization profile, and then click **Select**. (Example: VPN-Administrator)



Step 6: Repeat Step 1 through Step 5 for the VPN-Employee and VPN-Partner rules.

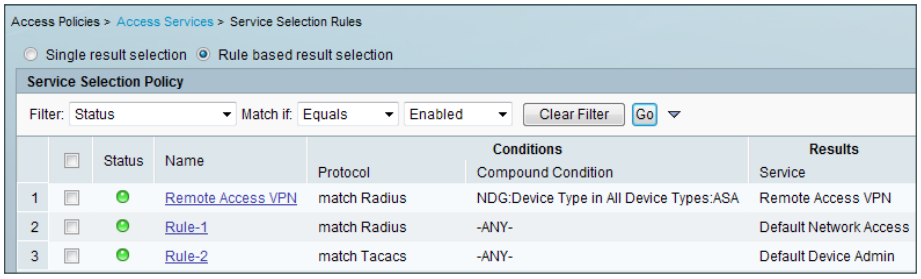
Step 7: In the Authorization pane, click the **Default** rule.

Step 8: Select **DenyAccess** as the authorization profile, clear any other selections if necessary, and then click **OK.**



Once the remote-access services have been created, you can change the order.

Step 9: In **Access Policies > Access Services > Service Selection Rules**, select the rule **Remote Access VPN**, use the up arrow button to move it above the default policies **Rule-1** and **Rule-2**, and then click **Save Changes**.



PROCESS

Configuring the Standalone RA VPN Firewall

1. Configure the LAN distribution switch
2. Apply Cisco ASA initial configuration
3. Configure internal routing
4. Configure user authentication
5. Configure NTP and logging
6. Configure device-management protocols
7. Configure HA on the primary Cisco ASA
8. Configure standby firewall for resilience
9. Configure the outside switch
10. Configure Internet interfaces
11. Configure resilient Internet routing

If you are using an integrated deployment model where RA VPN services reside on the primary set of Internet edge firewalls, this process is not needed, and you can skip to "Configuring the Remote Access VPN." If you are using standalone RA VPN devices, then continue with this process.

Procedure 1 Configure the LAN distribution switch

The LAN distribution switch is the path to the organization's internal network. A unique VLAN supports the Internet edge devices, and the routing protocol peers with the appliances across this network.

Reader Tip

This procedure assumes that the distribution switch has already been configured following the guidance in the Campus Wired LAN Design Guide. Only the procedures required to support the integration of the firewall into the deployment are included in this guide.

Step 1: Configure the interfaces that are connected to the RA VPN-specific firewalls.

```
interface GigabitEthernet1/0/23
 description VPN-ASA5525Xa Gig0/0
!
interface GigabitEthernet2/0/23
 description VPN-ASA5525Xb Gig0/0
!
interface range GigabitEthernet1/0/23, GigabitEthernet2/0/23
 switchport access vlan 300
 switchport host
 macro apply EgressQoS
 logging event link-status
 no shutdown
```

Procedure 2 Apply Cisco ASA initial configuration

This procedure configures connectivity to the appliance from the internal network in order to enable management access.

Step 1: Configure the appliance host name.

```
hostname VPN-ASA5525X
```

Step 2: Configure the appliance interface that is connected to the internal LAN distribution switch.

```
interface GigabitEthernet0/0
 no shutdown
!
interface GigabitEthernet0/0
 nameif inside
 ip address 10.4.24.24 255.255.255.224
```

Step 3: Disable the dedicated management interface.

```
interface Management0/0
 no ip address
 shutdown
```

Step 4: Configure an administrative username and password.

```
username admin password [password] privilege 15
```

Tech Tip

All passwords in this document are examples and should not be used in production configurations. Follow your company's policy, or if no policy exists, create a password using a minimum of 8 characters with a combination of uppercase, lowercase, and numbers.

Procedure 3 Configure internal routing

A dynamic routing protocol is used to easily configure reachability between networks connected to the appliance and those that are internal to the organization. Because the RA VPN Cisco ASA device is not the default route for the inside network to get to the Internet, a distribute list must be used to filter out the default route from EIGRP updates to other devices.

Caution

Default route advertisement from the RA VPN firewall will result in multiple conflicting default routes on the distribution layer switch. You must block the advertisement of the default route in order to avoid conflicting default routes.

Step 1: Create an access list to block default routes and permit all other routes.

```
access-list ALL_BUT_DEFAULT standard deny host 0.0.0.0
access-list ALL_BUT_DEFAULT standard permit any
```

Step 2: Enable Enhanced Interior Gateway Routing Protocol (EIGRP) on the appliance.

```
router eigrp 100
```

Step 3: Configure the appliance to advertise its statically defined routes including the RA VPN client address pool but not default routes and connected networks that are inside the Internet edge network range.

```
no auto-summary
network 10.4.0.0 255.254.0.0
redistribute static
distribute-list ALL_BUT_DEFAULT out
```

Step 4: Configure EIGRP to peer with neighbors across the inside interface only.

```
passive-interface default
no passive-interface inside
```

Step 5: Summarize the remote access host routes in order to keep routing tables small. A summary route matching the RA VPN client address pool is advertised after the first RA VPN client is connected to the RA VPN firewall. The summary route suppresses the advertisement of individual host routes.

```
interface GigabitEthernet0/0
 summary-address eigrp 100 10.4.28.0 255.255.252.0 5
```

Procedure 4 Configure user authentication

(Optional)

As networks scale in the number of devices to maintain, it poses an operational burden to maintain local user accounts on every device. A centralized authentication, authorization, and accounting (AAA) service reduces operational tasks per device and provides an audit log of user access for security compliance and root cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by AAA.

Reader Tip

The AAA server used in this architecture is the Cisco Secure ACS. Configuration of Cisco Secure ACS is discussed in the Device Management Using ACS Design Guide.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database was defined already to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

Step 1: Configure the TACACS+ server.

```
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (inside) host 10.4.48.15 SecretKey
```

Step 2: Configure the appliance's management authentication to use the TACACS+ server first and then the local user database if the TACACS+ server is unavailable.

```
aaa authentication enable console AAA-SERVER LOCAL
aaa authentication ssh console AAA-SERVER LOCAL
aaa authentication http console AAA-SERVER LOCAL
aaa authentication serial console AAA-SERVER LOCAL
```

Step 3: Configure the appliance to use AAA to authorize management users.

```
aaa authorization exec authentication-server
```

Tech Tip

User authorization on the Cisco ASA firewall does not automatically present the user with the enable prompt if they have a privilege level of 15, unlike Cisco IOS devices.

Procedure 5 Configure NTP and logging

Logging and monitoring are critical aspects of network security devices in order to support troubleshooting and policy-compliance auditing.

The Network Time Protocol (NTP) is designed to synchronize time across a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the organization's network.

Network devices should be programmed to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source.

There is a range of detail that can be logged on the appliance. Informational-level logging provides the ideal balance between detail and log-message volume. Lower log levels produce fewer messages, but they do not produce enough detail to effectively audit network activity. Higher log levels produce a larger volume of messages but do not add sufficient value to justify the number of messages logged.

Step 1: Configure the NTP server.

```
ntp server 10.4.48.17
```

Step 2: Configure the time zone.

```
clock timezone PST -8
clock summer-time PDT recurring
```

Step 3: Configure which logs to store on the appliance.

```
logging enable
logging buffered informational
```

Procedure 6 Configure device-management protocols

Cisco ASDM requires that the appliance's HTTPS server be available. Be sure that the configuration includes networks where administrative staff has access to the device through Cisco ASDM; the appliance can offer controlled Cisco ASDM access for a single address or management subnet (in this case, 10.4.48.0/24).

HTTPS and Secure Shell (SSH) Protocol are more secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

Use SSH and HTTPS protocols in order to more securely manage the device. Both protocols are encrypted for privacy, and the non-secure protocols, Telnet and HTTP, are turned off.

Simple Network Management Protocol (SNMP) is enabled to allow the network infrastructure devices to be managed by a Network Management System (NMS). SNMPv2c is configured for a read-only community string.

Step 1: Allow internal administrators to remotely manage the appliance over HTTPS and SSH.

```
domain-name cisco.local
http server enable
http 10.4.48.0 255.255.255.0 inside
ssh 10.4.48.0 255.255.255.0 inside
ssh version 2
```

Step 2: Specify the list of supported SSL encryption algorithms for ASDM.

```
ssl encryption aes256-sha1 aes128-sha1 3des-sha1
```

Step 3: Configure the appliance to allow SNMP polling from the NMS.

```
snmp-server host inside 10.4.48.35 community cisco
snmp-server community cisco
```

Procedure 7 Configure HA on the primary Cisco ASA

This procedure describes how to configure active/standby failover for the primary RA VPN Cisco ASA. The failover key value must match on both devices in an active/standby pair. This key is used for two purposes: to authenticate the two devices to each other, and to secure state synchronization messages between the devices, which enables the Cisco ASA pair to maintain service for existing connections in the event of a failover.

Step 1: On the primary Cisco ASA, enable failover.

```
failover
```

Step 2: Configure the Cisco ASA as the primary appliance of the high availability pair.

```
failover lan unit primary
```

Step 3: Configure the failover interface.

```
failover lan interface failover GigabitEthernet0/2
failover key FailoverKey
failover replication http
failover link failover GigabitEthernet0/2
```

Step 4: Tune the failover poll timers. This minimizes the downtime experienced during failover.

```
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
```

Step 5: Configure the failover interface IP address.

```
failover interface ip failover 10.4.24.97 255.255.255.248 standby 10.4.24.98
```

Step 6: Enable the failover interface.

```
interface GigabitEthernet0/2
 no shutdown
```

Step 7: Configure the standby IP address and monitoring of the inside interface.

```
interface GigabitEthernet0/0
 ip address 10.4.24.24 255.255.255.224 standby 10.4.24.23
monitor-interface inside
```

Procedure 8 Configure standby firewall for resilience

Step 1: On the secondary Cisco ASA appliance, enable failover.

```
failover
```

Step 2: Configure the appliance as the secondary appliance of the high availability pair.

```
failover lan unit secondary
```

Step 3: Configure the failover interface.

```
failover lan interface failover GigabitEthernet0/2
failover key FailoverKey
failover replication http
failover link failover GigabitEthernet0/2
```

Step 4: Tune the failover poll timers. This minimizes the downtime experienced during failover.

```
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
```

Step 5: Configure the failover interface IP address.

```
failover interface ip failover 10.4.24.97 255.255.255.248 standby 10.4.24.98
```

Step 6: Enable the failover interface.

```
interface GigabitEthernet0/2
 no shutdown
```

Step 7: If you want to verify standby synchronization between the Cisco ASA devices, on the command-line interface of the primary appliance, issue the **show failover state** command.

```
VPN-ASA525X# show failover state

               State          Last Failure Reason    Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  None

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

Procedure 9 Configure the outside switch

In this procedure, you configure the outside switch connection of the RA VPN Cisco ASA firewall. This deployment assumes a dual ISP design. It also assumes the outside switch is already configured with a base installation and that the only changes required are to allow the RA VPN devices to connect. If this is not the case, please follow the steps in the Firewall and IPS Design Guide, starting at the "Configuring the Firewall Internet Edge" process.

Step 1: Configure the interfaces that connect to the appliances.

```
interface GigabitEthernet1/0/20
 description VPN-ASA5525Xa Gig0/3
!
interface GigabitEthernet2/0/20
 description VPN-ASA5525Xb Gig0/3
!
interface range GigabitEthernet1/0/20, GigabitEthernet2/0/20
 switchport trunk allowed vlan 16,17
 switchport mode trunk
 spanning-tree portfast trunk
 macro apply EgressQoS
 logging event link-status
 logging event trunk-status
 no shutdown
```

Procedure 10 Configure Internet interfaces

In this procedure, you configure the outside interfaces of the RA VPN Cisco ASA firewalls. This deployment assumes a dual ISP design. If this is not the case, please follow the steps in the Firewall and IPS Design Guide, starting at the "Configuring the Firewall Internet Edge" process.

Step 1: From a client on the internal network, navigate to the firewall's inside IP address, and then launch the Cisco ASA Security Device Manager. (Example: https://10.4.24.24)

Step 2: In **Configuration > Device Setup > Interfaces**, click the interface that is connected to the outside switch. (Example: GigabitEthernet0/3)

Step 3: Click **Edit**.

Step 4: On the Edit Interface dialog box, select **Enable Interface**, and then click **OK**.

Step 5: In the Interface pane, click **Add > Interface**.

Step 6: On the Add Interface dialog box, in the **Hardware Port** list, choose the interface enabled in Step 4. (Example: GigabitEthernet0/3)

Step 7: In the **VLAN ID** box, enter the VLAN number for the primary Internet VLAN. (Example: 16)

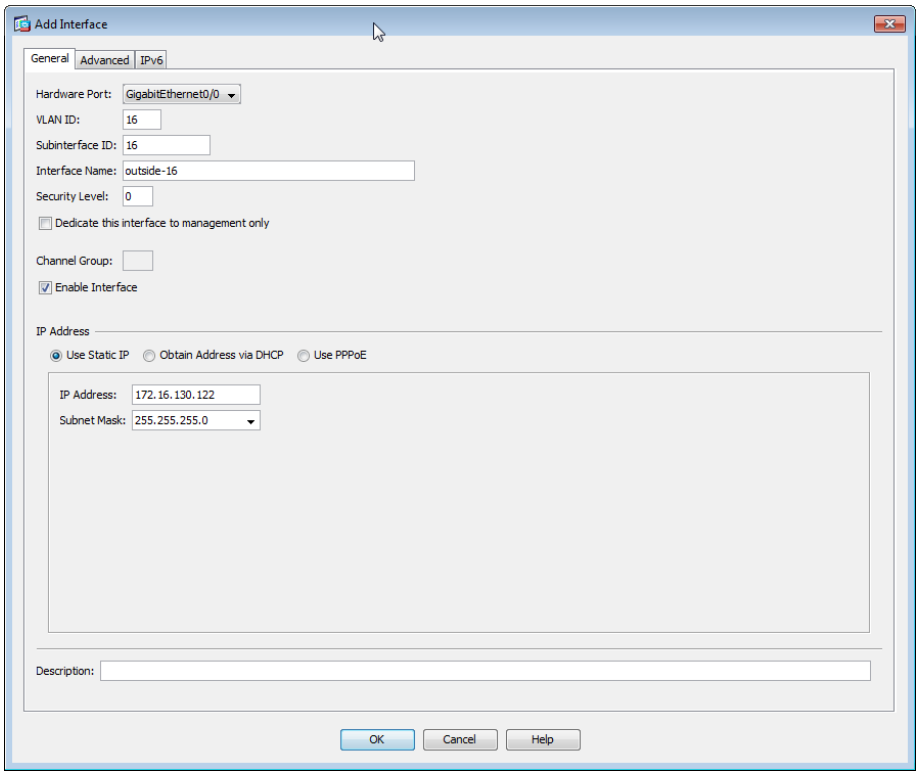
Step 8: In the **Subinterface ID** box, enter the VLAN number for the primary Internet VLAN. (Example: 16)

Step 9: Enter an **Interface Name**. (Example: outside-16)

Step 10: In the **Security Level** box, enter a value of **0**.

Step 11: Enter the interface **IP Address**. (Example: 172.16.130.122)

Step 12: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)



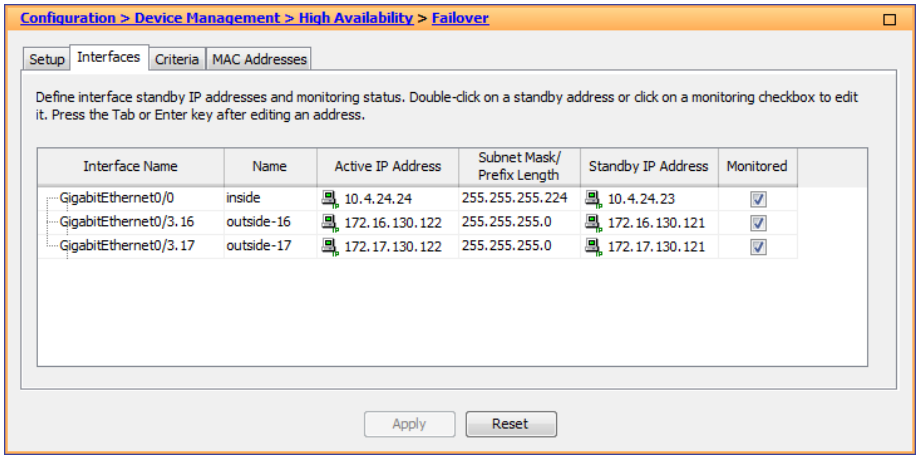
Step 13: In the Interface pane, click **Apply**.

Step 14: Repeat Step 5 through Step 13 for the resilient Internet VLAN.

Step 15: Navigate to **Configuration > Device Management > High Availability > Failover**.

Step 16: On the Interfaces tab, in the Standby IP Address column, enter the IP addresses of the standby unit for the interfaces you just created. (Example: 172.16.130.121, 172.17.130.121)

Step 17: Select **Monitored** for each, and then click **Apply**.



Procedure 11 Configure resilient Internet routing

In this procedure, you configure a pair of static default routes through the primary and secondary Internet interfaces. Each route uses a different metric.

The primary route carries a metric of 1, making the route preferred; the primary route's availability is determined by the state of the 'track 1' object that is appended to the primary route. The route-tracking configuration defines a target reachable through the primary ISP's network to which the appliance sends Internet Control Message Protocol (ICMP) probes (pings) in order to determine if the network connection is active. The target destination must be able to respond to an ICMP echo request.

The tracked object should be in the primary ISP's network. The point of tracking an object in the primary ISP's network is because if reachability to this object is available, then all connectivity to that point is working, including the appliance's connection to the customer premise router, the WAN connection, and most routing inside the ISP's network. If the tracked object is unavailable, it is likely that the path to the primary ISP is down, and the appliance should prefer the secondary ISP's route.

Step 1: In **Configuration > Device Setup > Routing > Static Routes**, click **Add**.

Step 2: On the Add Static Route dialog box, in the **Interface** list, chose the interface created in the previous procedure's Step 9. (Example: outside-16)

Step 3: In the Network box, select **any4**.

Step 4: In the Gateway IP box, enter the primary Internet CPE's IP address. (Example: 172.16.130.126)

Step 5: In the Metric box, enter **1**.

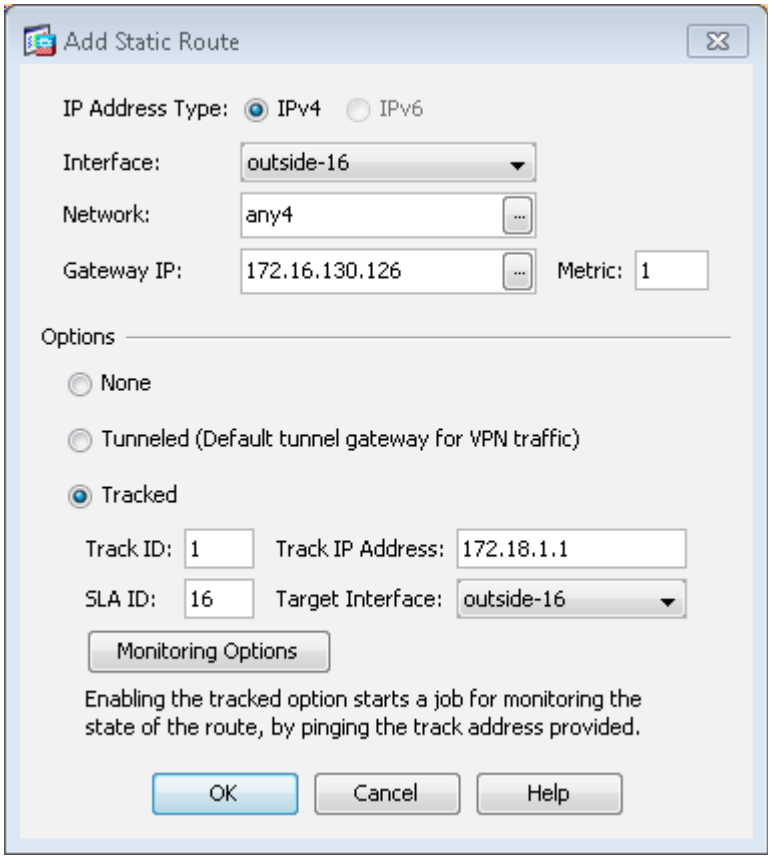
Step 6: In the Options pane, click **Tracked**.

Step 7: In the Track ID box, enter **1**.

Step 8: In the Track IP Address box, enter an IP address in the ISP's cloud. (Example: 172.18.1.1)

Step 9: In the SLA ID box, enter **16**.

Step 10: In the **Target Interface** list, choose the primary Internet connection interface, and then click **OK**. (Example: outside-16)



Next, you create the secondary default route to the resilient Internet CPE's address.

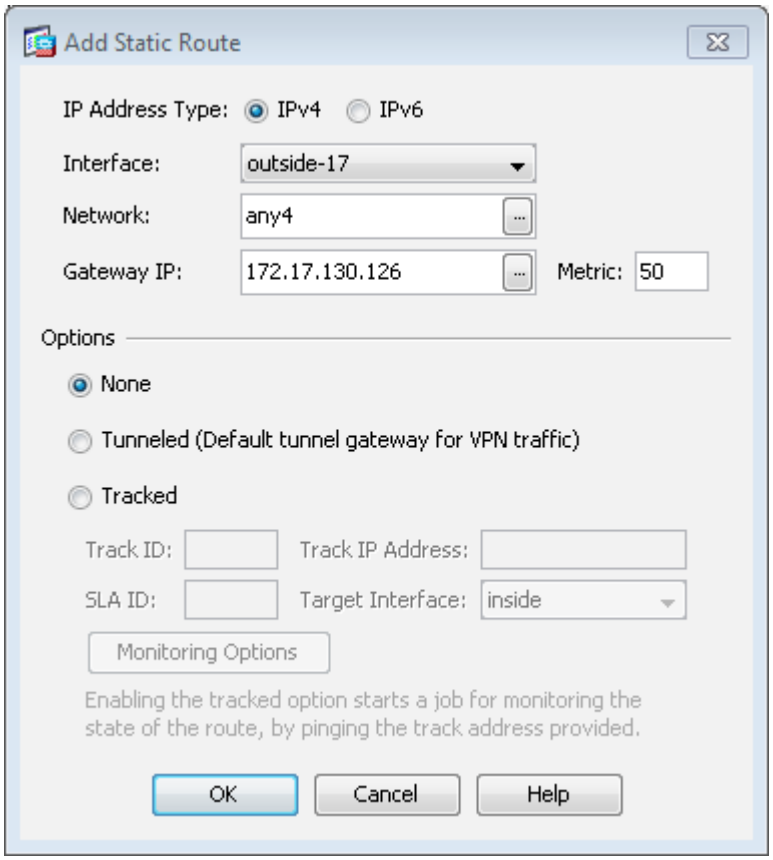
Step 11: In **Configuration > Device Setup > Routing > Static Routes**, click **Add**.

Step 12: On the Add Static Route dialog box, in the **Interface** list, choose the resilient Internet connection interface. (Example: outside-17)

Step 13: In the Network box, select **any4**.

Step 14: In the **Gateway IP** box, enter the primary Internet CPE's IP address. (Example: 172.17.130.126)

Step 15: In the Metric box, enter **50**, and then click **OK**.



Step 16: In the Static Routes pane, click **Apply**.

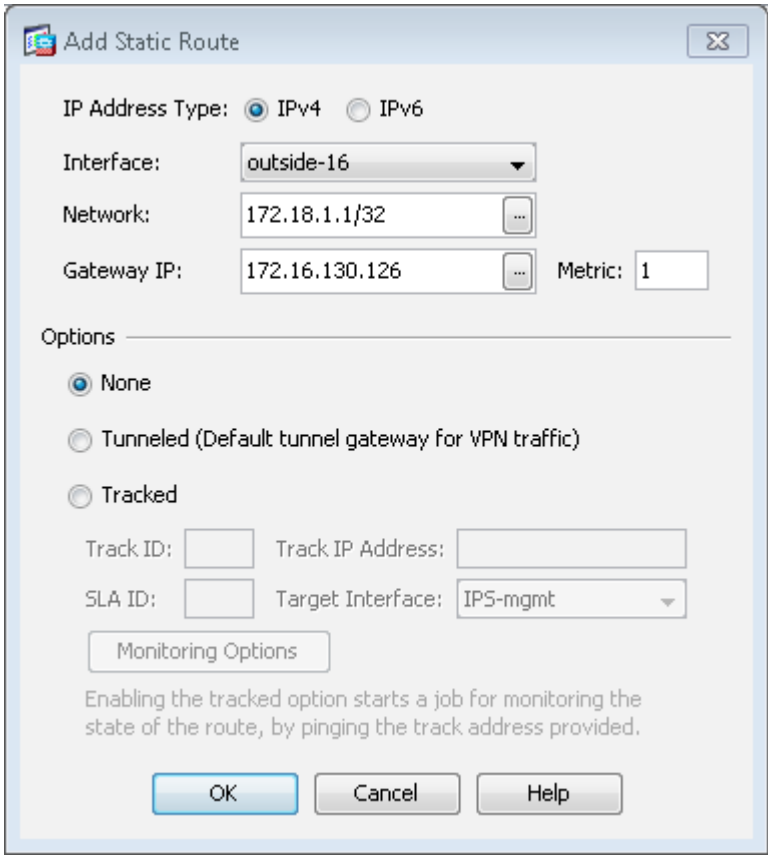
Next, you add a host route for the tracked object via the Internet-CPE-1 address. This assures that probes to the tracked object will always use the primary ISP connection.

Step 17: In **Configuration > Device Setup > Routing > Static Routes**, click **Add**.

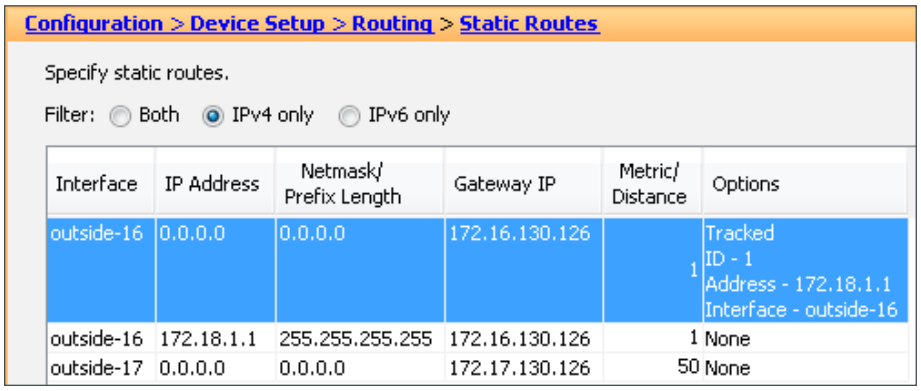
Step 18: In the Add Static Route dialog box, in the **Interface** list, choose the primary Internet connection interface. (Example: outside-16)

Step 19: In the **Network** box, enter the IP address used for tracking in the primary default route. (Example: 172.18.1.1/32)

Step 20: In the **Gateway IP** box, enter the primary Internet CPE's IP address, and then click **OK**. (Example: 172.16.130.126)



Step 21: In the Static Routes pane, click **Apply**.



PROCESS

Configuring the Remote-Access VPN

1. Load AnyConnect client images
2. Configure remote access
3. Create the AAA server group
4. Define the VPN address pool
5. Configure DNS and certificates
6. Configure default tunnel gateway
7. Configure remote access routing
8. Configure the group-URL
9. Enable SSL for additional interface
10. Configure additional NAT exemption
11. Configure the connection profile
12. Configure the employee policy
13. Configure the partner policy
14. Configure the admin policy
15. Configure Cisco AnyConnect Client Profile

The majority of the VPN configuration tasks are addressed in the Cisco AnyConnect VPN Connection Setup Wizard. Depending on requirements, additional work might need to be completed after the wizard.

Procedure 1 Load AnyConnect client images

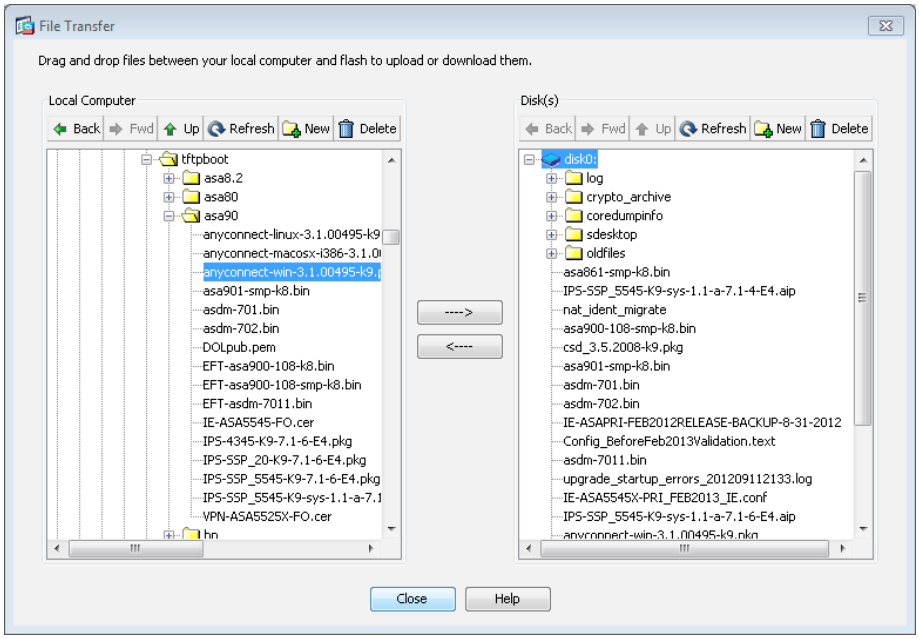
Download the Cisco AnyConnect Secure Mobility Client images from cisco.com to the computer you use to run ASDM. There are separate images for Windows, Apple OS X, and Linux; only the images that are required by your organization must be downloaded.

The images then need to be uploaded to both the primary and secondary RA VPN Cisco ASAs.

Step 1: Navigate to **Tools > File Management.**

Step 2: Click **File Transfer**, and then select **Between Local PC and Flash**.

Step 3: Browse to the location on your local file system and copy each image to the Cisco ASA flash memory by selecting the image and then clicking the right arrow.



Step 4: Repeat Step 3 for each client image. After completing the file transfers for all client images, click **Close**.

Step 5: Repeat Step 1 through Step 4 for the secondary RA VPN Cisco ASA. From a client on the internal network, navigate to the secondary RA VPN Cisco ASA's inside IP address, and then launch ASDM. (Example: https://10.4.24.23)

Tech Tip

Do not attempt to modify the firewall configuration on the standby appliance. You should make configuration changes only to the primary appliance.

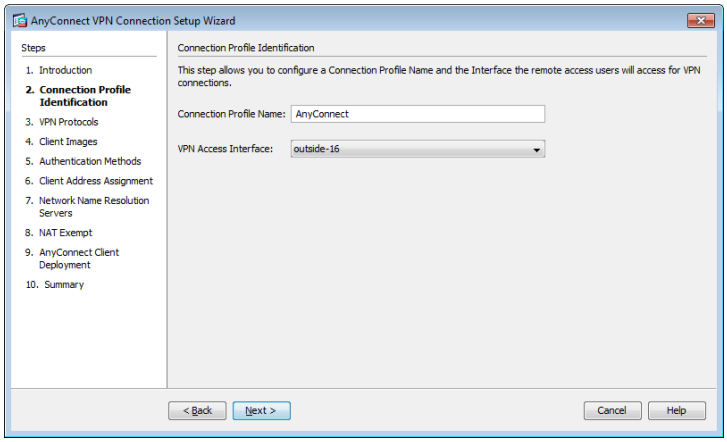
Procedure 2 Configure remote access

Step 1: Navigate to **Wizards > VPN Wizards > AnyConnect VPN Wizard.**

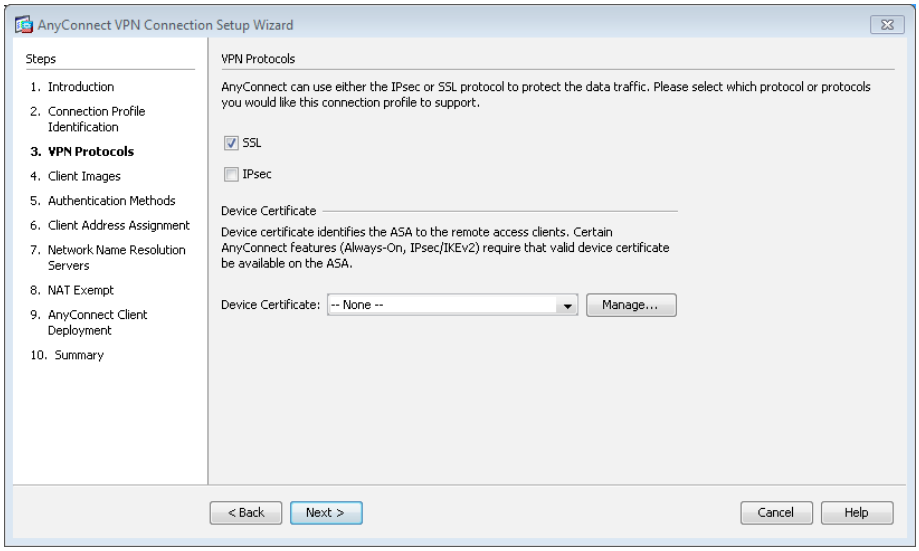
Step 2: In the AnyConnect VPN Connection Setup Wizard dialog box, click **Next**.

Step 3: In the **Connection Profile Name** box, enter a name. (Example: AnyConnect)

Step 4: In the **VPN Access Interface** list, choose the primary Internet connection, and then click **Next**. (Example: outside-16)



Step 5: Under VPN Protocols, select **SSL**, clear **IPsec**.



Next, generate a self-signed identity certificate and install it on the appliance.

Tech Tip

Because the certificate in this example is self-signed, clients generate a security warning until they accept the certificate.

Step 6: In the Device Certificate pane, click **Manage.**

Step 7: On the Manage Identity Certificates dialog box, click **Add**.

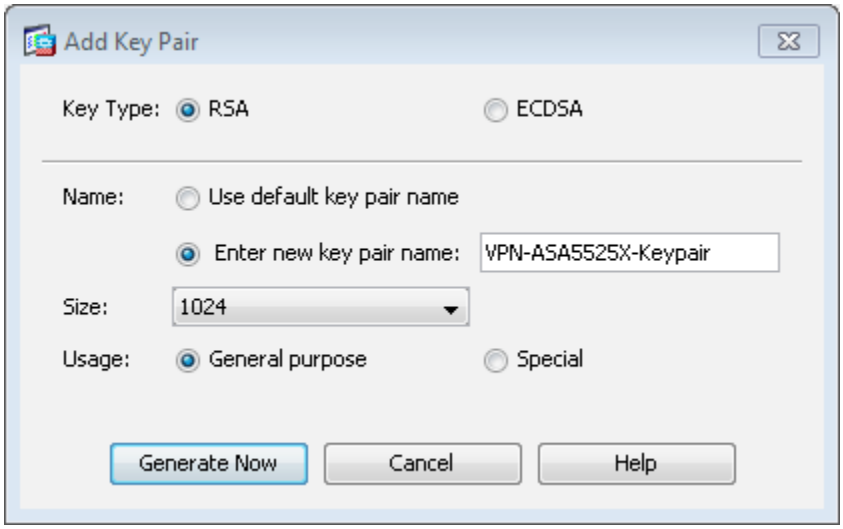
Step 8: On the Add Identity Certificate dialog box, enter a new Trustpoint Name (Example: VPN-ASA5525X-Trustpoint), and then select **Add a new identity certificate**.

> **Tech Tip**
>
> Entering a new key pair name prevents the certificate from becoming invalid if an administrator accidentally regenerates the default RSA key pair.

Step 9: For Key Pair, select **New**.

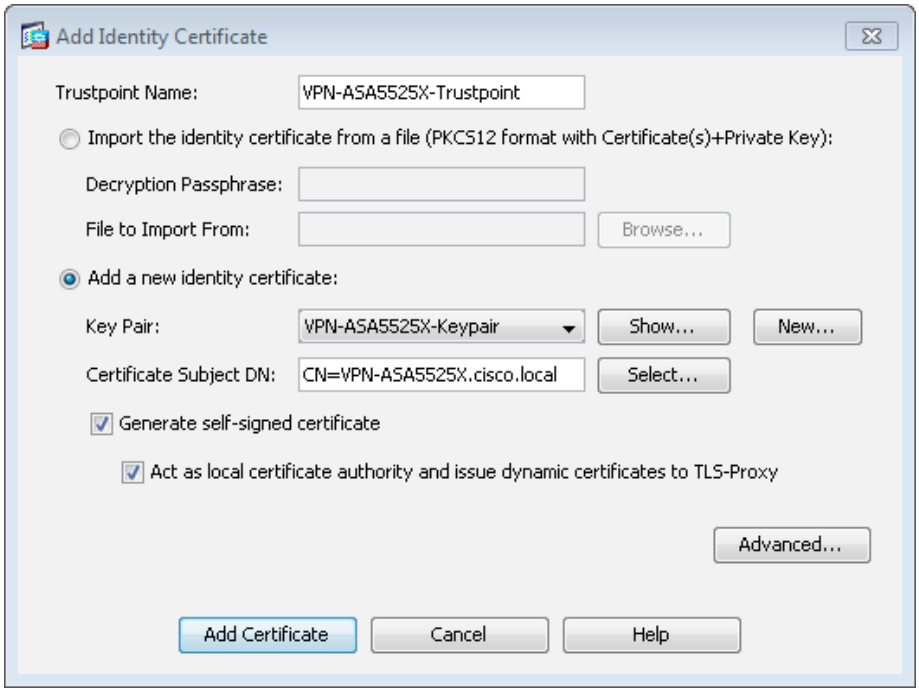
Step 10: On the Add Key Pair dialog box, select **RSA** and **Enter new key pair name**, and then in the box, enter a name. (Example: VPN-ASA5525X-Keypair)

Step 11: Click **Generate Now**.



Step 12: On the Add Identity Certificate dialog box, in Certificate Subject DN, enter the fully qualified domain name used to access the appliance on the outside interface. (Example: CN=VPN-ASA5525X.cisco.local)

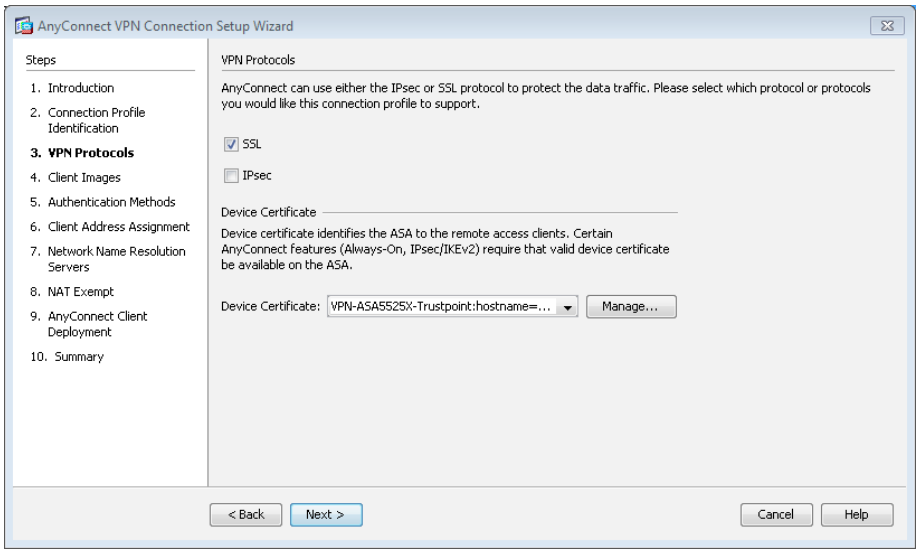
Step 13: Select **Generate self-signed certificate** and **Act as Local certificate authority and issue dynamic certificates to TLS-Proxy**, and then click **Add Certificate.**



The Enrollment Status dialog box shows that the enrollment succeeded. Click **OK**.

Step 14: In the Manage Identity Certificates dialog box, click **OK**.

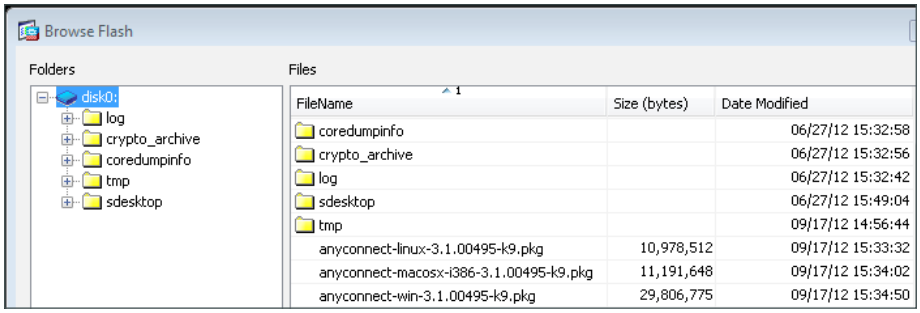
Step 15: On the VPN Protocols page, verify that the **IPsec** check box is cleared and the certificate you created is reflected in the Device Certificate box, and then click **Next**.



Step 16: On the Client Images page, click **Add**.

Step 17: On the Add AnyConnect Client Image dialog box, click **Browse Flash.**

Step 18: On the Browse Flash dialog box, select the appropriate AnyConnect client image to support your user community (linux, macosx, or win), and then click **OK**.



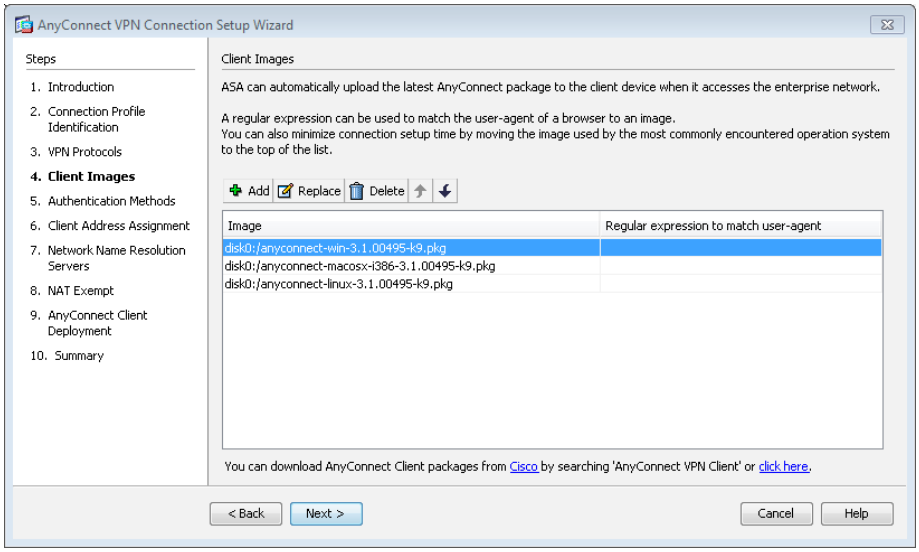
Step 19: On the Add AnyConnect Client Image dialog box, click **OK**.

Step 20: Repeat Step 17 through Step 19 for all the required Cisco AnyConnect client images.

Next, if necessary, reorder the list of images so that the most commonly used image is listed first and least commonly used images are listed last.

Step 21: Click the image you want to move, and then click the up or down arrows to reorder the image.

Step 22: On the Client Images page, click **Next**.



Remaining in the wizard, you now create a new AAA server group to authenticate remote-access users. To authenticate users, the server group uses either NT LAN Manager (NTLM) to the Active Directory server or RADIUS to the Cisco Secure ACS server.

Procedure 3 Create the AAA server group

For VPN user authentication, you point Cisco ASA to either the Cisco Secure ACS you configured earlier or to the organization's Active Directory server.

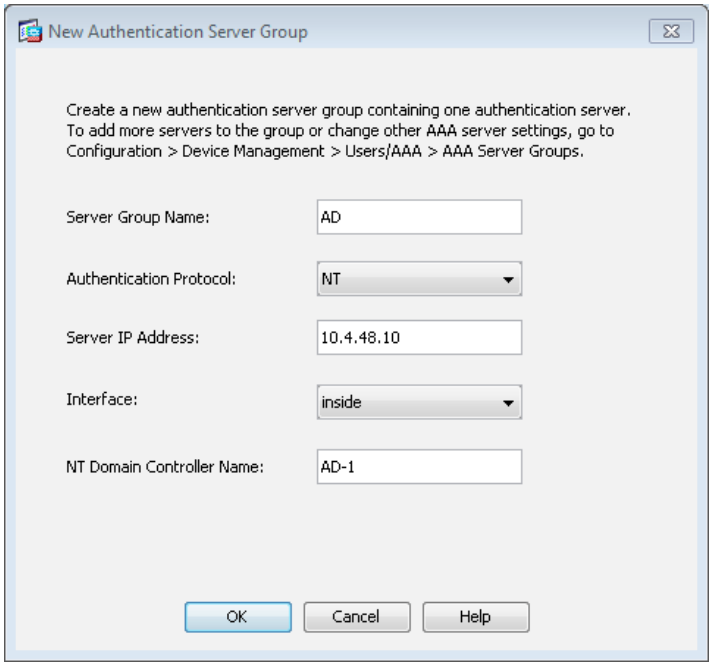
If the authentication process authenticates directly to Active Directory, complete Option 1 of this procedure. If the authentication process uses Cisco Secure ACS, complete Option 2 of this procedure.

Option 1: Use Active Directory for AAA

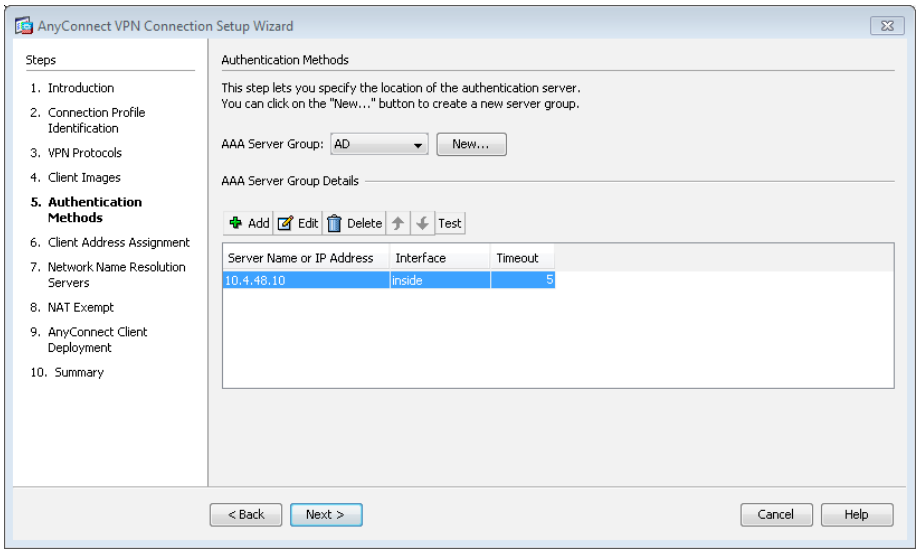
Step 1: On the Authentication Methods page, next to **AAA Server Group**, click **New**.

Step 2: On the New Authentication Server Group dialog box, enter the following values, and then click **OK**:

- Server Group Name: **AD**
- Authentication Protocol–**NT**
- Server IP Address–**10.4.48.10**
- Interface–**inside**
- NT Domain Controller Name–**AD-1**



Step 3: On the Authentication Methods page, click **Next**.

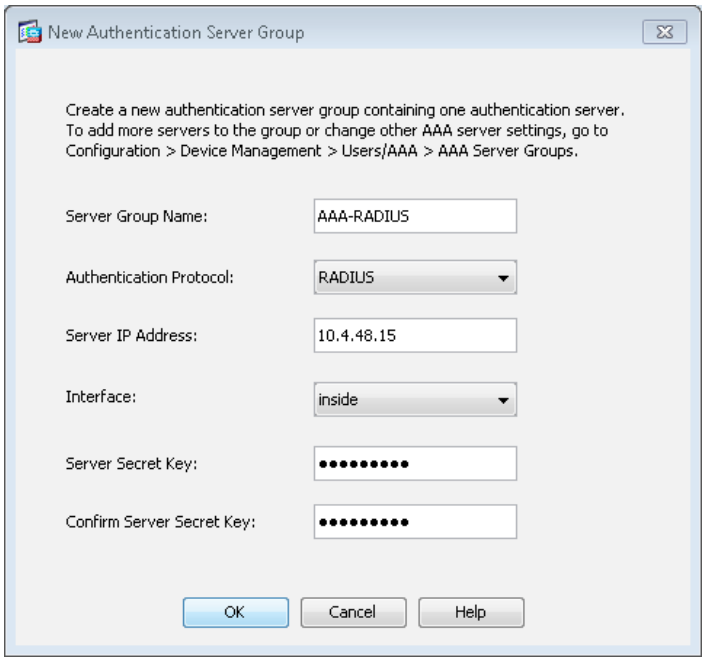


Option 2: Use Cisco Secure ACS for AAA

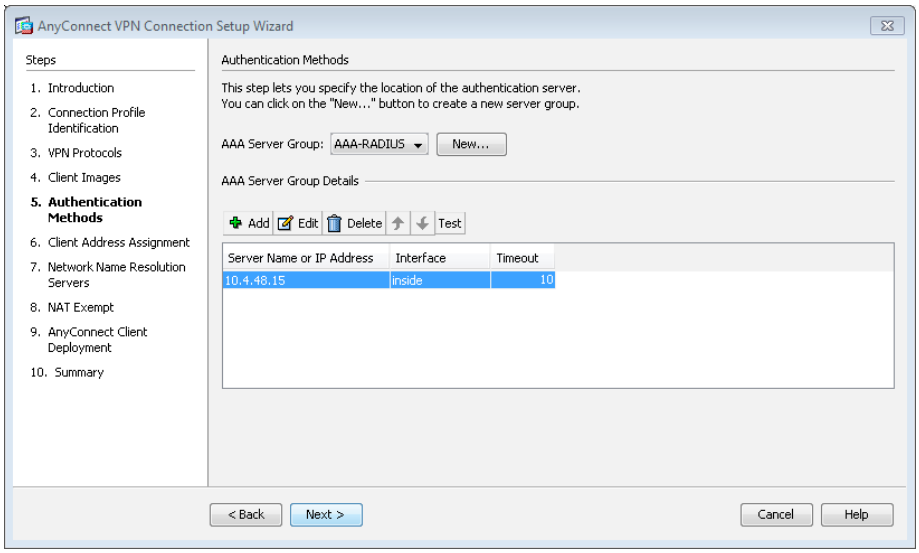
Step 1: On the Authentication Methods page, next to **AAA Server Group**, click **New**.

Step 2: On the New Authentication Server Group dialog box, enter the following values, and then click **OK**:

- Server Group Name–**AAA-RADIUS**
- Authentication Protocol–**RADIUS**
- Server IP Address–**10.4.48.15** (IP address of the Cisco Secure ACS server)
- Interface–**inside**
- Server Secret Key–**SecretKey**
- Confirm Server Secret Key–**SecretKey**



Step 3: On the Authentication Methods page, click **Next**.



Next, you define the remote-access VPN address pool that will be assigned to users when they connect to the VPN service.

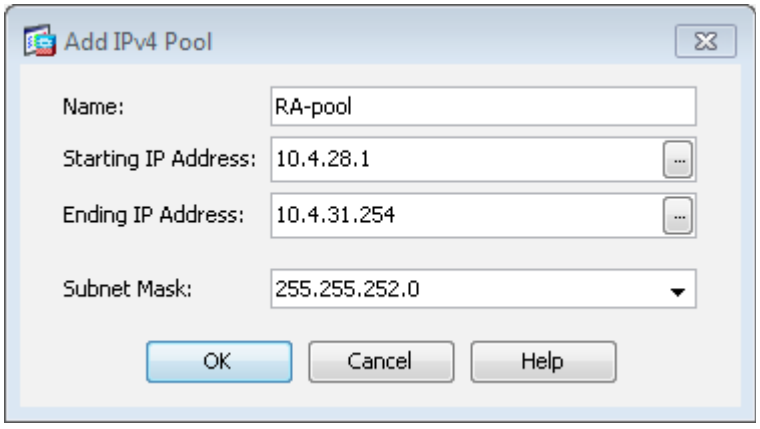
Procedure 4 Define the VPN address pool

You need to decide on an appropriate address space for your RA VPN address pool. In this example you use 4 class-C address ranges (~1000 addresses) as the pool.

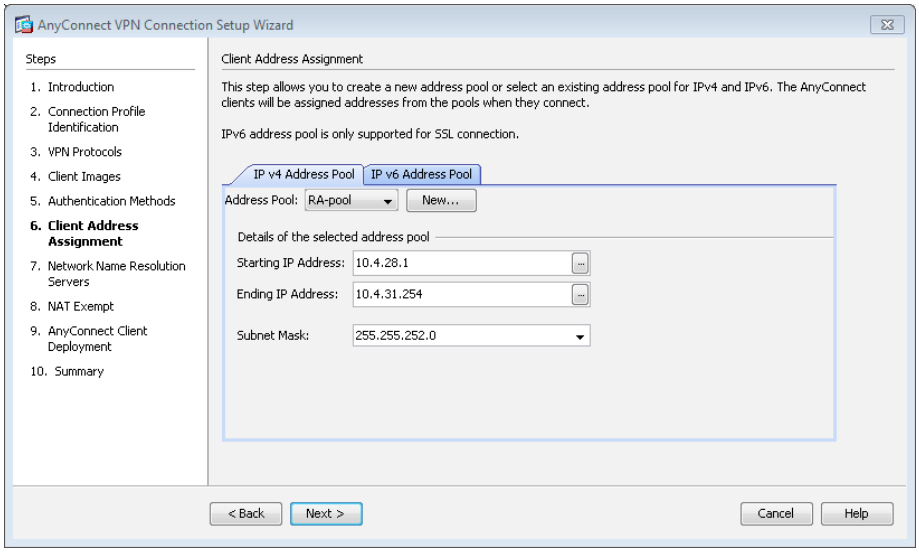
Step 1: On the Client Address Assignment page, in the IPv4 Address Pool tab, click **New**.

Step 2: On the Add IP Pool dialog box, enter the following values, and then click **OK**:

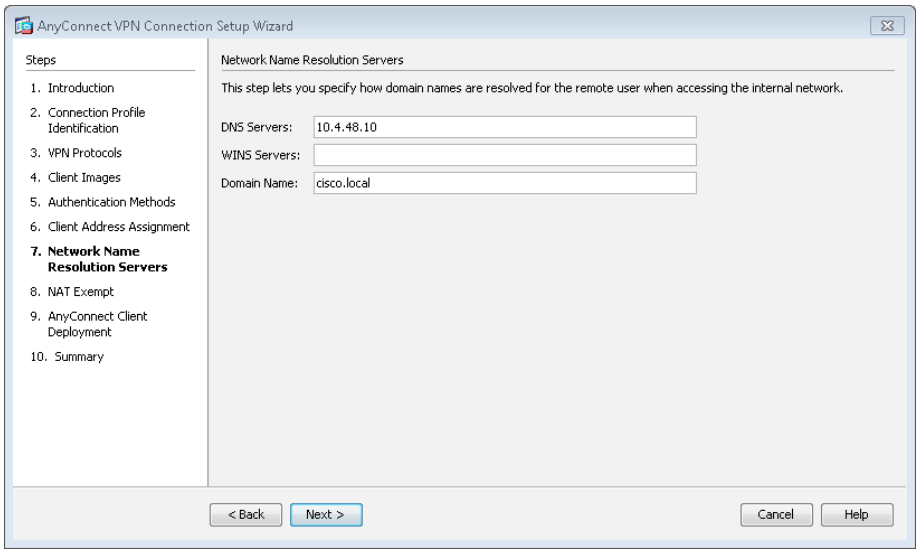
- Name—**RA-pool**
- Starting IP Address—**10.4.28.1**
- Ending IP Address—**10.4.31.254**
- Subnet Mask—**255.255.252.0**



Step 3: On the Client Address Assignment page, verify that the pool you just created is selected, and then click **Next**.



Step 4: On the Network Name Resolution Servers page, enter the organization's **DNS Servers** (Example: 10.4.48.10) and the organization's **Domain Name** (Example: cisco.local), and then click **Next**.



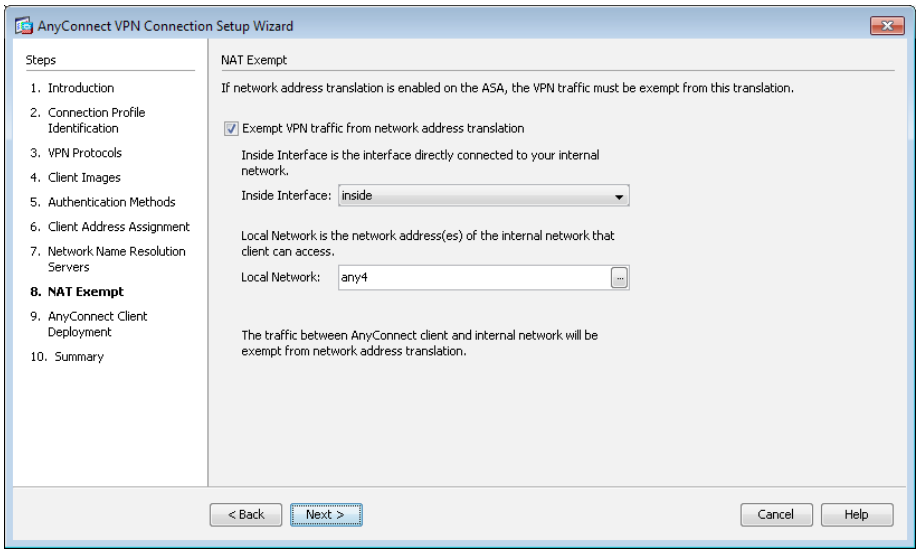
If you are using RA VPN integrated with Cisco ASA Series firewalls, NAT exemption must be configured for traffic from the LAN that is going to the remote-access clients. If this were not configured, traffic to clients would be translated, changing the source address of the traffic and making it impossible for clients to receive traffic correctly from servers with which they communicate.

Step 5: If you are implementing a standalone VPN design, skip to Step 8.

If you are implementing an integrated VPN design, in the wizard, on the NAT Exempt page, select **Exempt VPN traffic from network address translation**.

Step 6: In the **Inside Interface** list, choose **inside**.

Step 7: In the Local Network box, enter **any4**, and then click **Next**.



Step 8: On the AnyConnect Client Deployment page, click **Next.**

Step 9: On the Summary page, click **Finish**.

Procedure 5 Configure DNS and certificates

Step 1: In this procedure, you generate an additional identity certificate for the secondary outside interface of the RA VPN Cisco ASA firewall. The certificate that was generated in the AnyConnect Wizard in Step 8 of Procedure 2, "Configure remote access," is used only for the primary outside interface.

Step 2: The IP addresses assigned to each of the outside interfaces correspond to a fully qualified domain name (FQDN) that can be resolved using an external DNS server.

Table 2 - DNS names for external IP addresses

Usage	Interface name	IP address	FQDN
Primary	outside-16	172.16.130.122	VPN-ASA5525X.cisco.local
Secondary	outside-17	172.17.130.122	VPN-ASA5525X-FO.cisco.local

Step 3: Using the values in Table 2, on your DNS server create DNS records for both the primary and secondary address on the RA VPN Cisco ASA appliance.

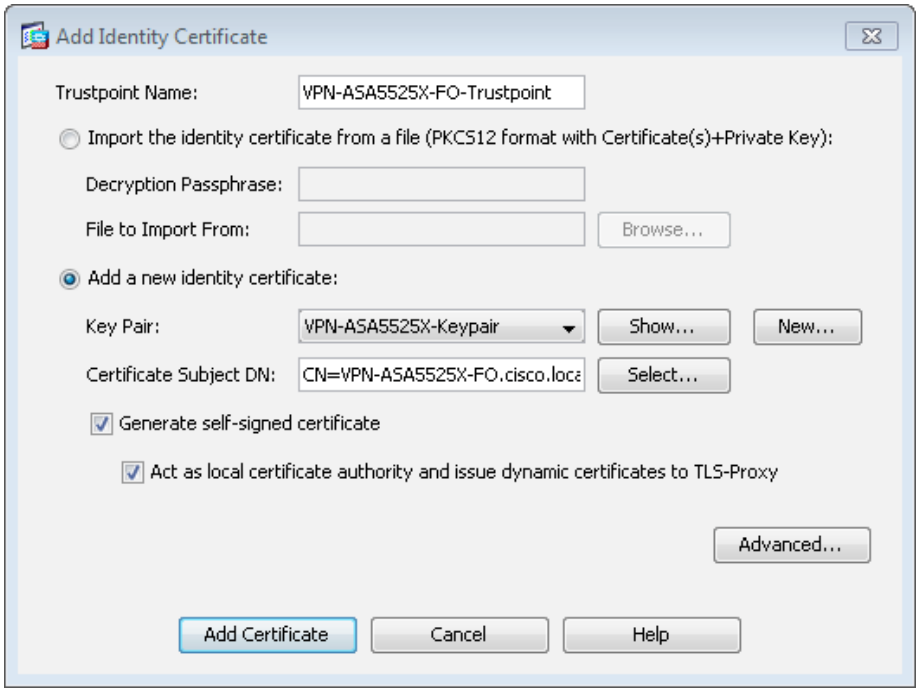
Step 4: Generate an identity certificate for the secondary interface. In **Configuration > Remote Access VPN > Certificate Management > Identity Certificates**, click **Add**.

Step 5: On the Add Identity Certificate dialog box, enter a new Trustpoint Name (example: VPN-ASA5525X-FO-Trustpoint), and then select **Add a new identity certificate**.

Step 6: For Key Pair, select the previously created key pair. (Example: VPN-ASA5525X-Keypair)

Step 7: On the Add Identity Certificate dialog box, in **Certificate Subject DN**, enter the FQDN used to access the appliance on the secondary outside interface. (Example: CN=VPN-ASA5525X-FO.cisco.local)

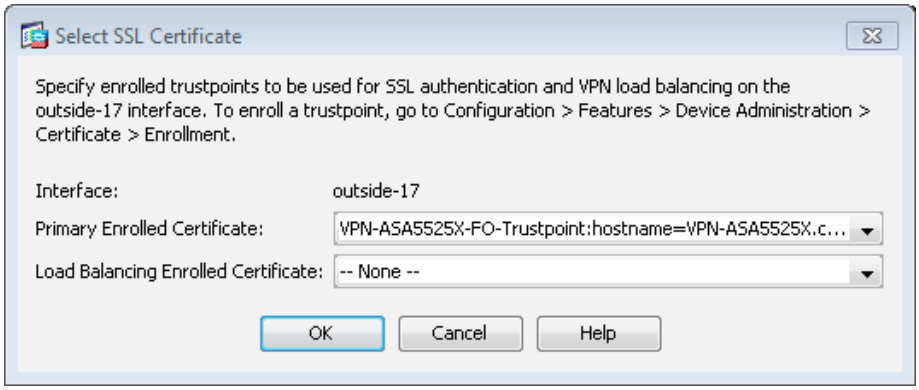
Step 8: Select the **Generate self-signed certificate** and **Act as local certificate authority and issue dynamic certificates to TLS-Proxy** check boxes, and then click **Add Certificate.**



Step 9: When the Enrollment Status dialog box that shows that the enrollment has succeeded appears, click **OK**.

Step 10: In **Configuration Management > Device Management > Advanced > SSL Settings**, in the Certificates pane, select the secondary outside interface (Example: outside-17), and then click **Edit**.

Step 11: On the Select SSL Certificate dialog box, in the **Primary Enrolled Certificate** list, choose the additional identity certificate that was created in Step 6, and then click **OK** and then click **Apply**.



Step 12: Force certificate replication to the secondary RA VPN appliance. From the command prompt, issue the **write standby** command from the primary RA VPN appliance.

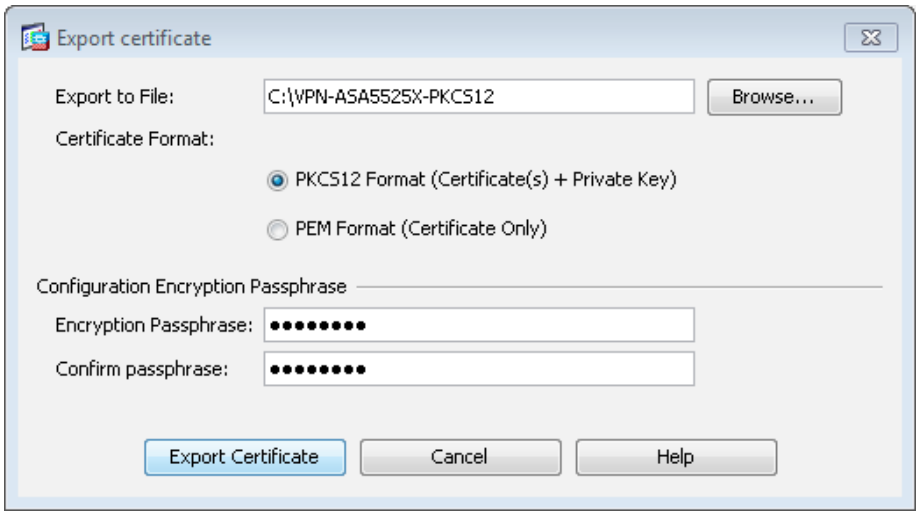
```
VPN-ASA5525X# write standby
```

Next, export the primary identity certificates for backup and distribution.

Step 13: Navigate to **Configuration > Remote Access VPN > Certificate Management > Identify Certificates**, select the certificate for backup, and then click **Export**.

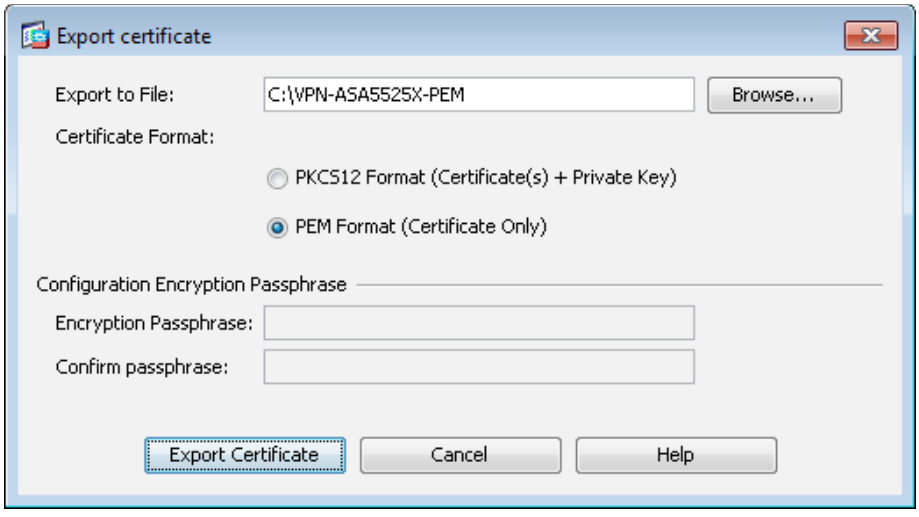
Step 14: Select the **PKCS12 format (Certificates(s) + Private Key)** certificate format. This format is used for restoring a certificate to a new device.

Step 15: Enter a secure passphrase (Example: c1sco123), and then click **Export Certificate**.



Step 16: Repeat the export in PEM format. This format is used for distribution to VPN client devices when using self-signed certificates. A secure passphrase is not used with the PEM format.

Step 17: Repeat Step 11 through Step 14 for the secondary identity certificate.



Procedure 6 Configure default tunnel gateway

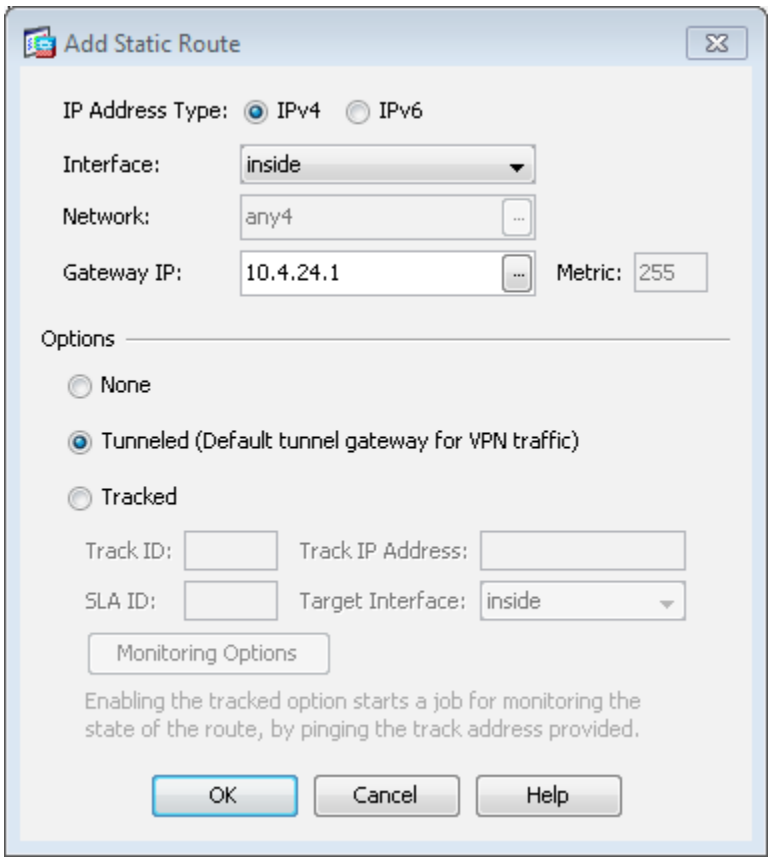
This procedure is only required when configuring a standalone RA VPN device. If you are using an integrated deployment model, skip to Procedure 7, "Configure remote access routing."

Traffic from remote-access VPN clients to and from the Internet must be inspected by the organization's firewall and IPS. To accomplish this, all traffic to and from the VPN clients must be routed toward the LAN distribution switch, regardless of the traffic's destination, so that the Cisco ASA firewall and IPS has the visibility to handle the traffic correctly.

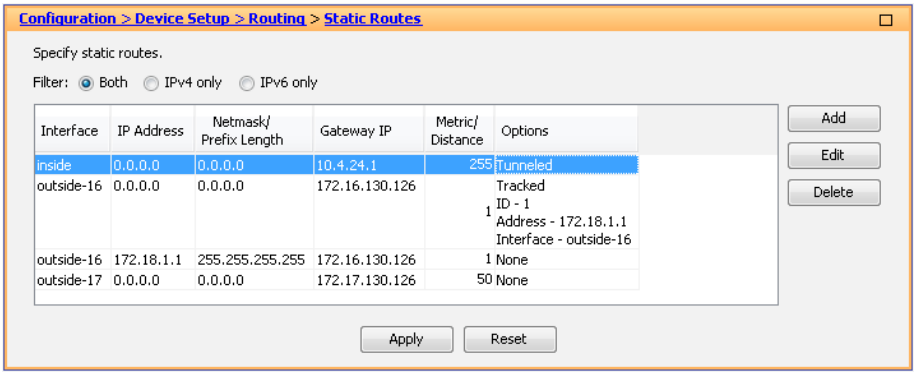
Step 1: In **Configuration > Device Setup > Routing > Static Routes**, click **Add**.

Step 2: On the Add Static Route dialog box, configure the following values, and then click **OK**.

- Interface–**inside**
- Network–any4
- Gateway IP–**10.4.24.1**
- Options–**Tunneled (Default tunnel gateway for VPN traffic)**



Step 3: Verify the configuration, and then click **Apply**.



Procedure 7 Configure remote access routing

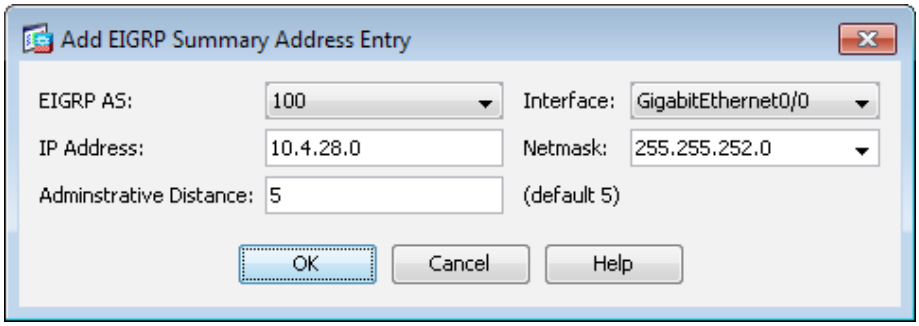
Summarize the remote access host routes in order to keep routing tables small. A summary route matching the RA VPN client address pool is advertised after the first RA VPN client is connected to the RA VPN firewall. The summary route suppresses the advertisement of individual host routes.

Summarizing the address pool also reduces the IP route table size for easier troubleshooting and faster recovery from failures.

Step 1: In **Configuration > Device Setup > Routing > EIGRP > Summary Address**, click **Add**.

Step 2: On the Add EIGRP Summary Address Entry dialog box, configure the following values, and then click **OK**.

- EIGRP AS—**100**
- Interface—**GigabitEthernet0/0**
- IP Address—**10.4.28.0** (Enter the remote-access pool's summary network address.)
- Netmask—**255.255.252.0**
- Administrative Distance—**5**

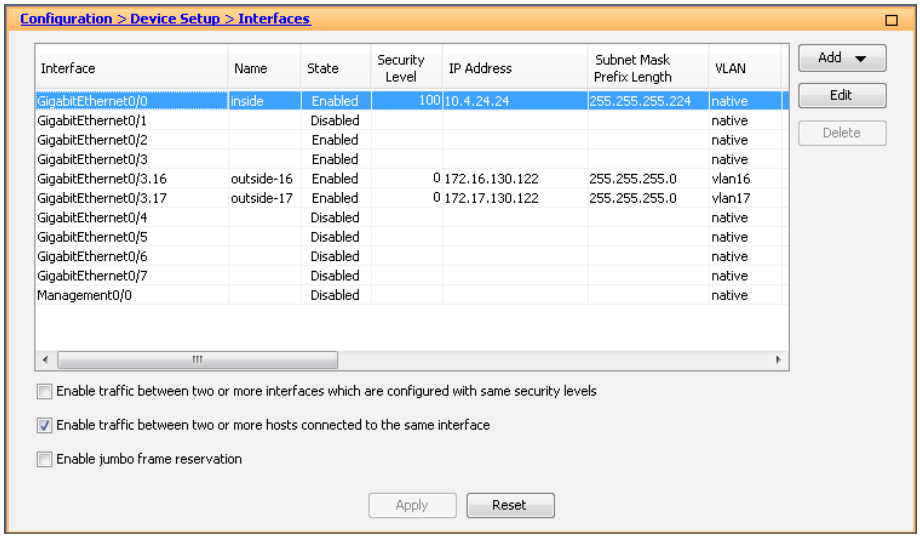


Step 3: In the Summary Address pane, click **Apply**.

Next, allow intra-interface traffic. This is critical for allowing VPN users (specifically remote workers with Cisco Unified Communications software clients) to communicate with each other.

Step 4: Navigate to **Configuration > Device Setup > Interfaces**.

Step 5: Select **Enable traffic between two or more hosts connected to the same interface**, and then click **Apply**.



Procedure 8 Configure the group-URL

The Cisco AnyConnect client's initial connection is typically launched with a web browser. After the client is installed on a user's computer, subsequent connections can be established through the web browser again or directly through the Cisco AnyConnect client, which is now installed on the user's computer. The user needs the IP address or DNS name of the appliance, a username and password, and the name of the VPN group to which they are assigned. Alternatively, the user can directly access the VPN group with the group-url, after which they need to provide their username and password.

If using the Dual ISP design, expect to offer VPN connectivity through both ISP connections, and be sure to provide group-urls for the IP address or host names for both ISPs.

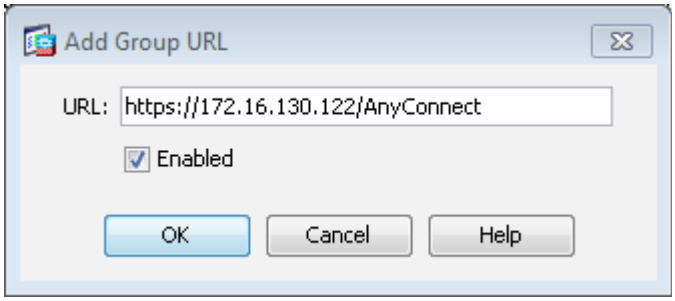
Step 1: Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**.

Step 2: In the Connection Profiles pane, select the profile created in the previous procedure (Example: AnyConnect), and then click **Edit**.

Step 3: On the Edit AnyConnect Connect Profile dialog box, navigate to **Advanced > Group Alias/Group URL**.

Step 4: In the Group URLs pane, click **Add**.

Step 5: In the URL box, enter the URL containing the firewall's primary Internet connection IP address and a user group string, click **OK**. (Example: https://172.16.130.122/AnyConnect), and then click **Save Changes**.



Step 6: If you are using the dual ISP design, which has a resilient Internet connection, repeat Step 1 through Step 5, using the firewall's resilient Internet connection IP address. (Example: https://172.17.130.122/AnyConnect)

If you are using the single ISP design, advance to the next procedure.

Procedure 9 Enable SSL for additional interface

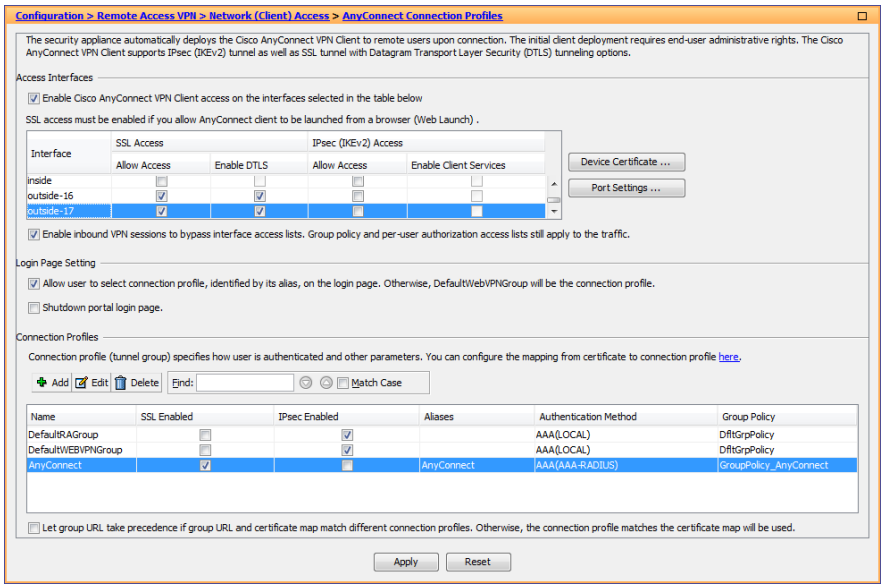
(Optional)

This procedure is required only when using the dual ISP design.

Step 1: Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**.

Step 2: In the Configuration window, in the Access Interfaces pane, select the interface attached to the resilient Internet connection. (Example: outside-17)

Step 3: Under SSL Access, select **Allow Access**, and then click **Apply**.



Procedure 10 Configure additional NAT exemption

(Optional)

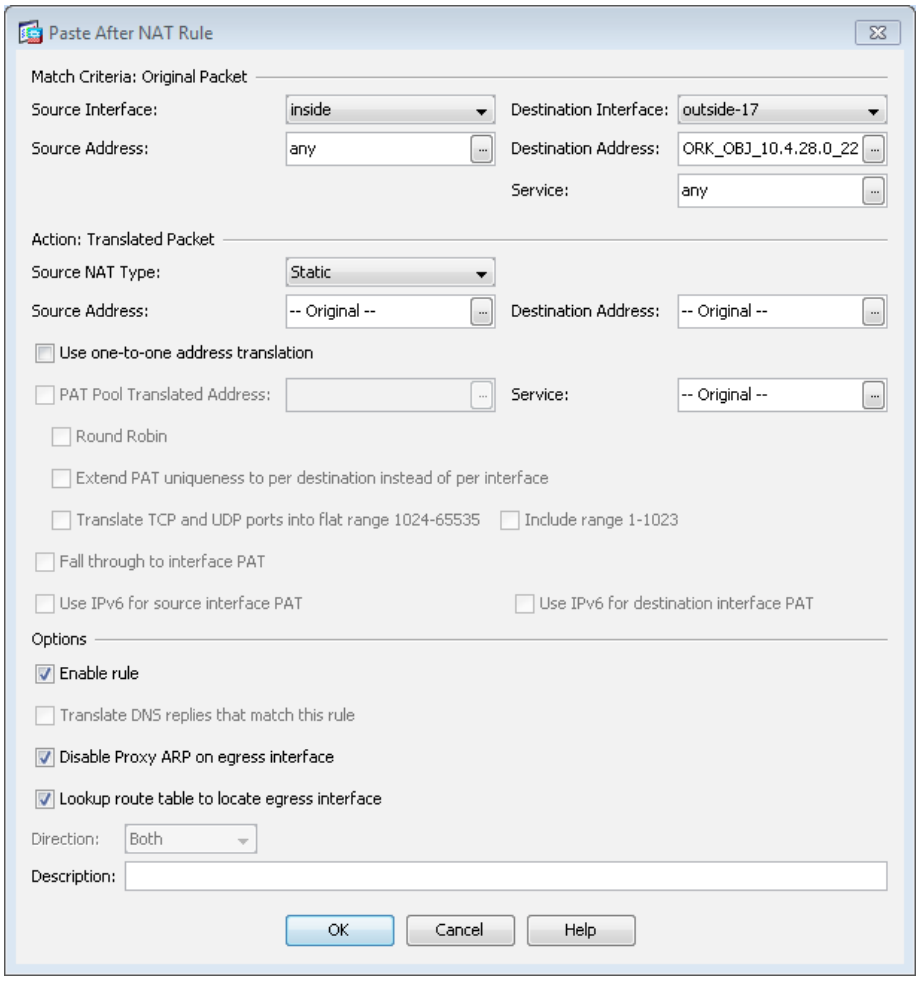
This procedure is required only when using the dual ISP design with the integrated VPN design.

Step 1: Navigate to **Configuration > Firewall > NAT Rules**. A previous NAT exemption rule already exists from an earlier procedure. (Example: Source Intf: inside, Dest Intf: outside-16, Destination: NETWORK_OBJ_10.4.28.0_22) Right-click this rule, and then click **Copy**.

Match Criteria: Original Packet					Action: Translated Packet		
Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service
inside	outside-16	any	NETWORK_OBJ_10.4.28.0_22	any	-- Original -- (S)	-- Original --	-- Original --

Step 2: Right-click after the original rule, and then click **Paste**. The new rule is opened for editing.

Step 3: Change the Destination Interface to the resilient interface (example: outside-17), and then click **OK**.

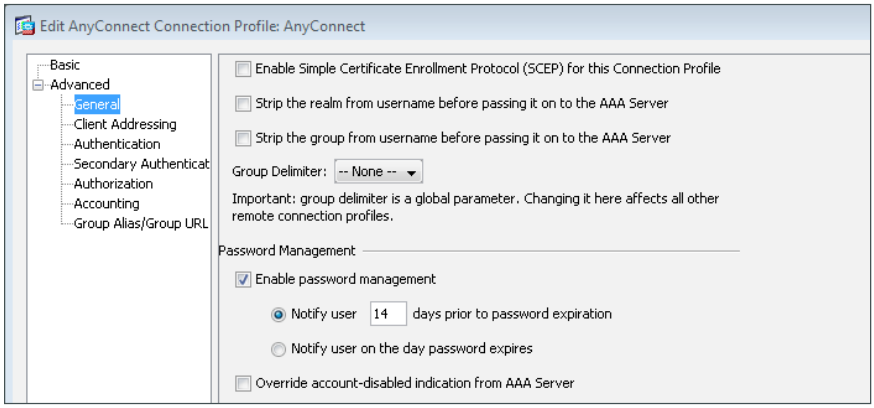


Procedure 11 Configure the connection profile

Complete this procedure when using Cisco Secure ACS as a proxy to Active Directory for authentication. The MS-CHAPv2 authentication protocol requires that password management is enabled on the RA VPN Cisco ASA appliance. This procedure is recommended but not required when using Active Directory by itself.

Step 1: Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**. In the Connection Profiles pane, select the profile that created previously using the AnyConnect VPN Wizard (Example: AnyConnect), and then click **Edit**.

Step 2: In **Advanced > General**, in the Password Management pane, select **Enable password management**, click **OK**, and then click **Save Changes**.

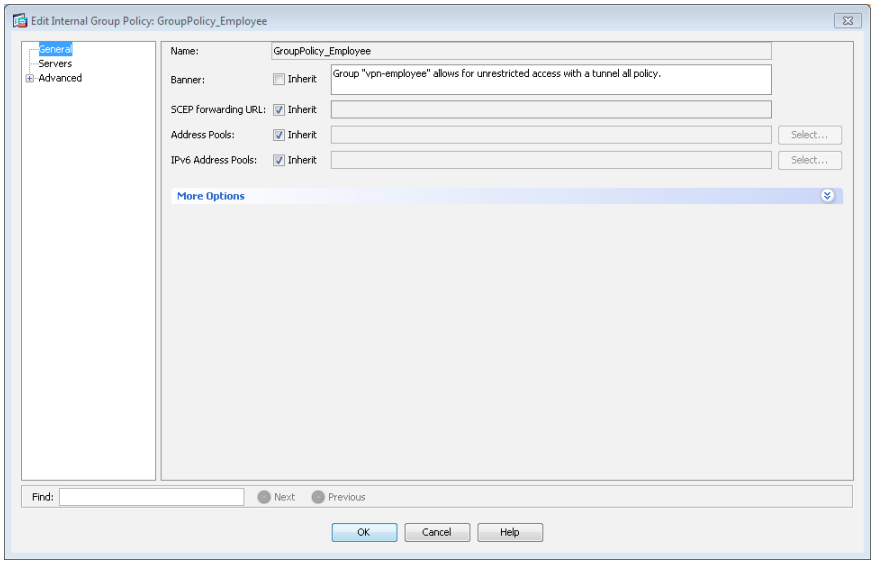


Procedure 12 Configure the employee policy

Step 1: In **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**, click **Add**.

Step 2: On the Add Internal Group Policy dialog box, enter a **Name**. (Example: GroupPolicy_Employee)

Step 3: For Banner, clear the **Inherit** check box, and then enter a banner message for the employee policy. (Example: Group “vpn-employee” allows for unrestricted access with a tunnel all policy.)

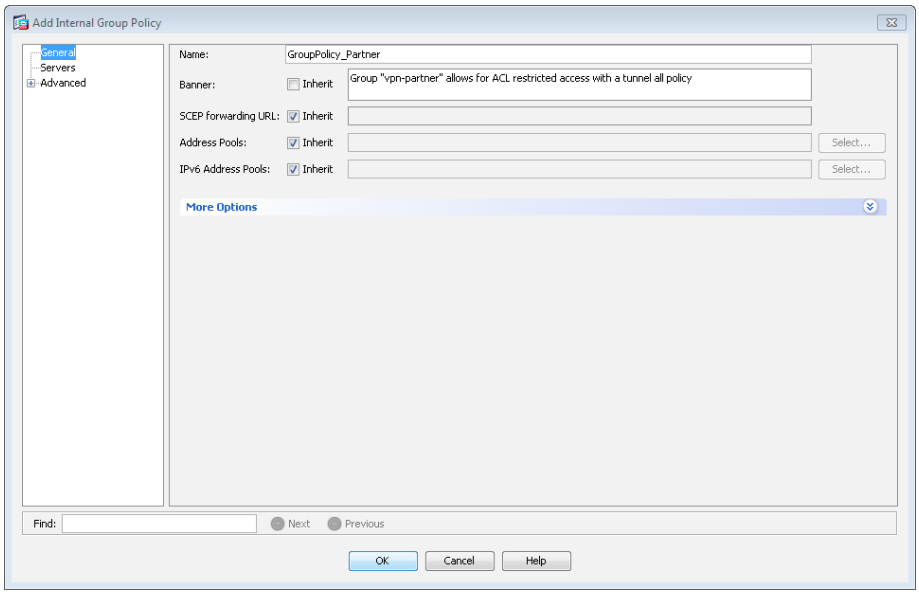


Procedure 13 Configure the partner policy

Step 1: In **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**, click **Add**.

Step 2: On the Add Internal Group Policy dialog box, enter a **Name**. (Example: GroupPolicy_Partner)

Step 3: For Banner, clear the **Inherit** check box, and then enter a banner message for the partner policy. (Example: Group "vpn-partner" allows for access control list (ACL) restricted access with a tunnel all policy.)

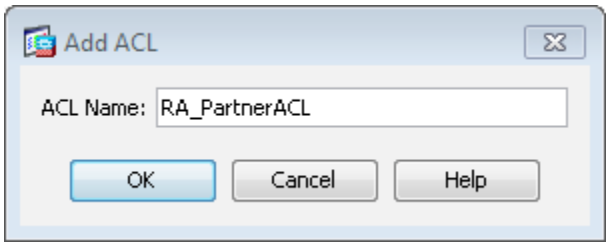


Step 4: Click the two down arrows. The More Options pane expands.

Step 5: For Filter, clear the **Inherit** check box, and then click **Manage**.

Step 6: On the ACL Manager dialog box, click the **Standard ACL** tab, then click **Add > Add ACL**.

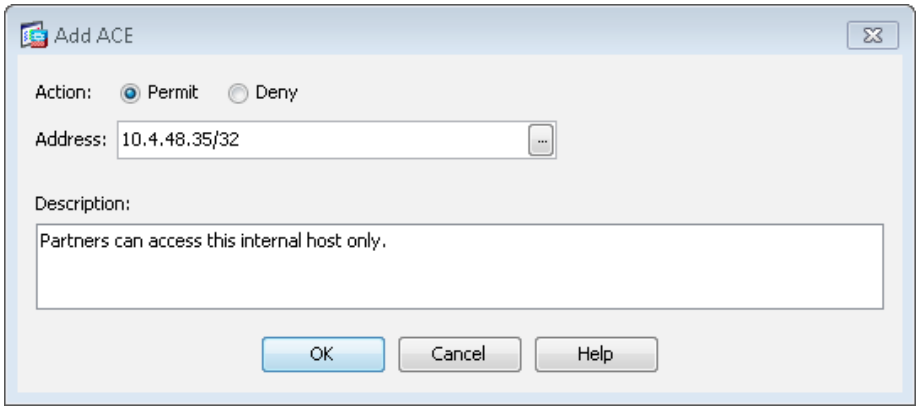
Step 7: On the Add ACL dialog box, enter an **ACL Name**, and then click **OK**. (Example RA_PartnerACL)



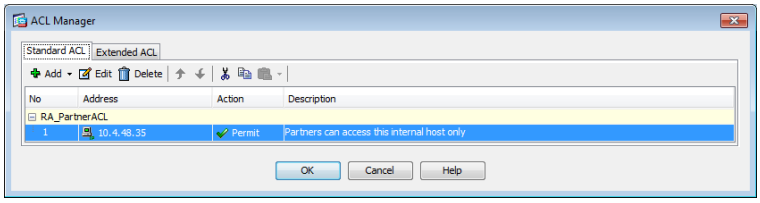
Step 8: Click **Add > Add ACE**.

Step 9: On the Add ACE dialog box, for Action, select **Permit**.

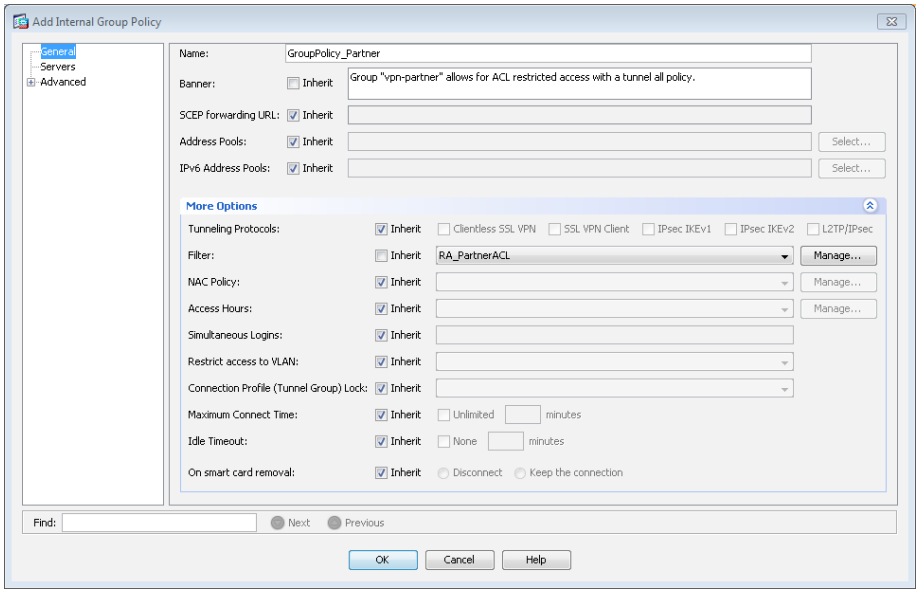
Step 10: In the Address box, enter the IP address and netmask that the partner is allowed to access, and then click **OK**. (Example: 10.4.48.35/32)



Step 11: On the ACL Manager dialog box, click **OK**.



Step 12: On the Add Internal Group Policy dialog box, click **OK**.



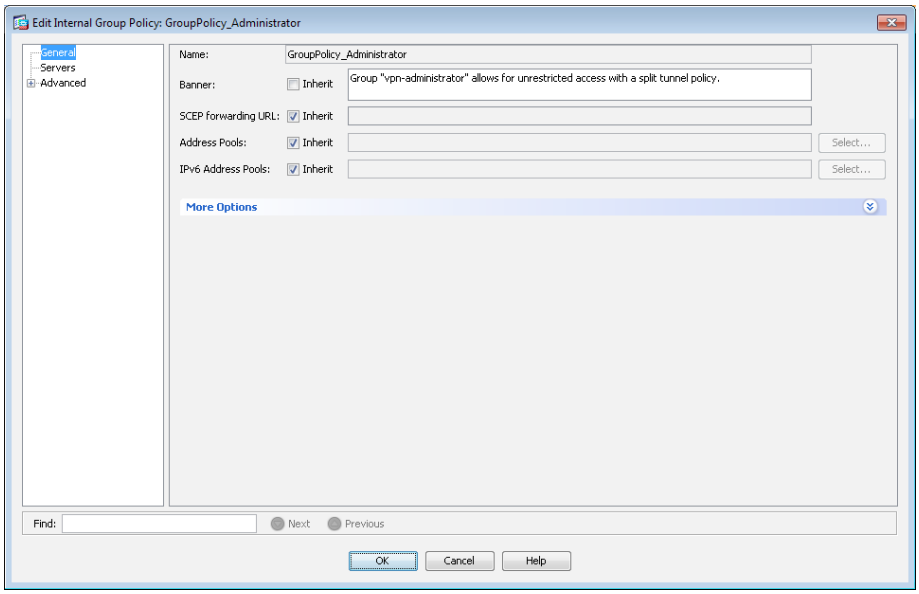
Step 13: In the Group Policies pane, click **Apply**.

Procedure 14 Configure the admin policy

Step 1: In **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**, click **Add**.

Step 2: On the Add Internal Group Policy dialog box, enter a **Name**. (Example: GroupPolicy_Administrator)

Step 3: For Banner, clear the **Inherit** check box, and then enter a banner message for the administrator policy. (Example: Group "vpn-administrator" allows for unrestricted access with a split tunnel policy.)



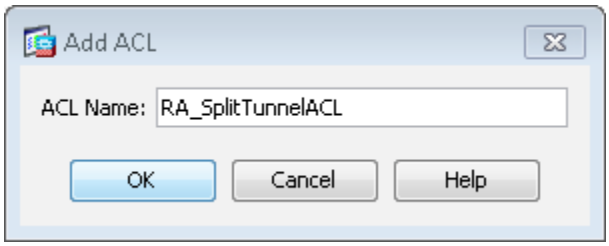
Step 4: In the navigation tree, click **Advanced > Split Tunneling**.

Step 5: For Policy, clear the **Inherit** check box, and then select **Tunnel Network List Below**.

Step 6: For Network List, clear the **Inherit** check box, and then click **Manage**.

Step 7: On the ACL Manager dialog box, click the **Standard ACL** tab, and then click **Add > Add ACL**.

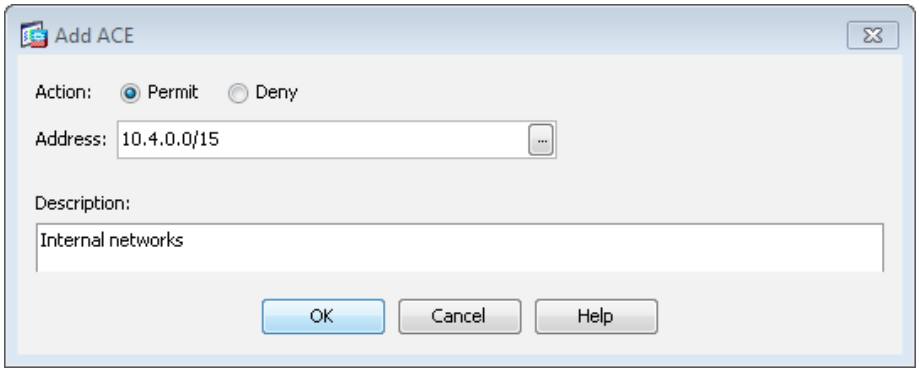
Step 8: On the Add ACL dialog box, enter an **ACL Name**, and then click **OK**. (Example RA_SplitTunnelACL)



Step 9: Click **Add > Add ACE**.

Step 10: On the Add ACE dialog box, for Action, select **Permit**.

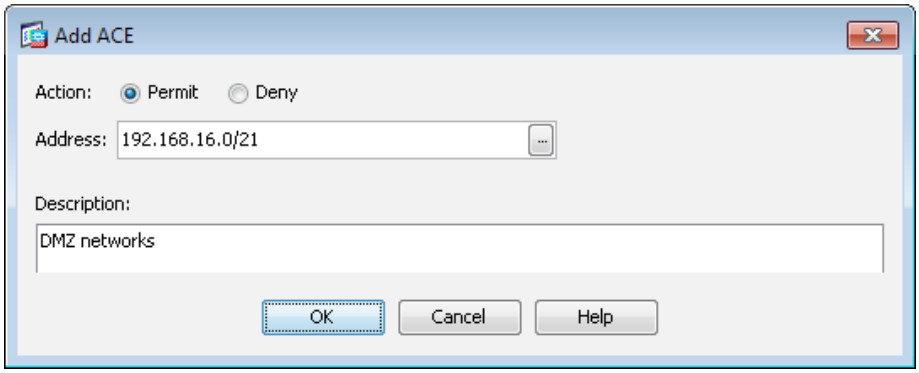
Step 11: In the Address box, enter the internal summary IP address and netmask, and then click **OK**. (Example: 10.4.0.0/15)



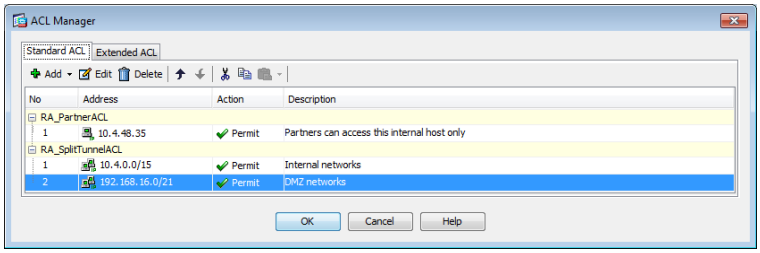
Step 12: Click **Add > Add ACE**.

Step 13: On the Add ACE dialog box, for Action, select **Permit**.

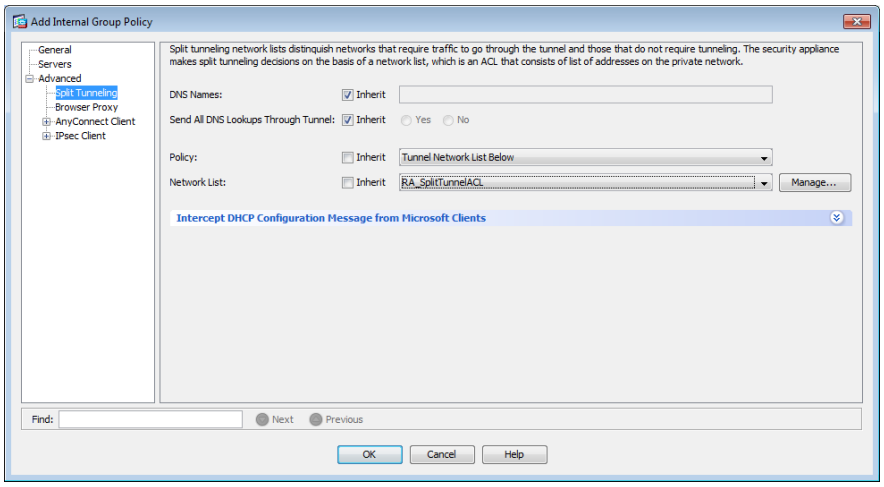
Step 14: In the Address box, enter the DMZ summary IP address and netmask, and then click **OK**. (Example: 192.168.16.0/21)



Step 15: On the ACL Manager dialog box, click **OK**.



Step 16: On the Add Internal Group Policy dialog box, click **OK**.



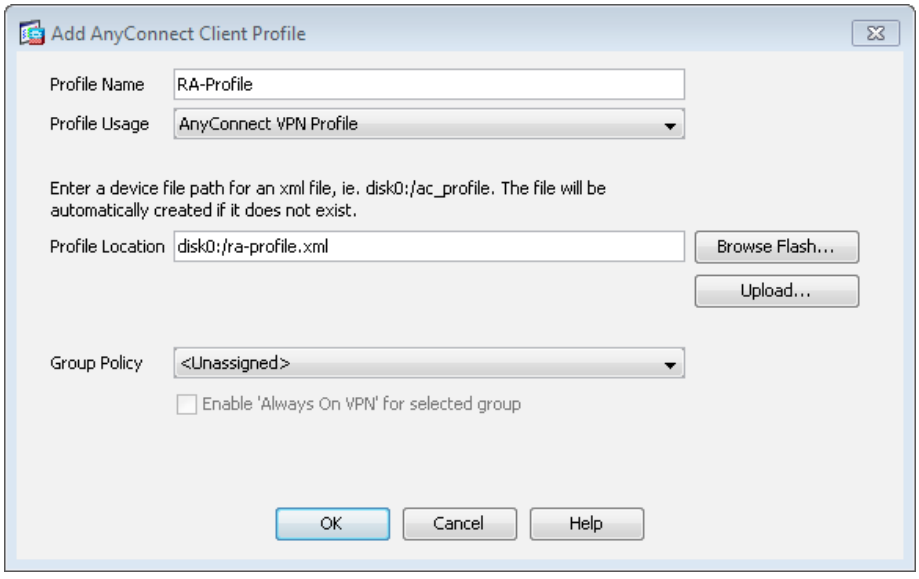
Step 17: In the Group Policies pane, click **Apply**.

Procedure 15 Configure Cisco AnyConnect Client Profile

Cisco AnyConnect Client Profile is the location where the newer configuration of the Cisco AnyConnect client is defined. Cisco AnyConnect 2.5 and later use the configuration in this section, including many of the newest features added to the Cisco AnyConnect client.

Step 1: In **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**, click **Add**.

Step 2: On the Add AnyConnect Client Profile dialog box, in the Profile Name box, enter **RA-Profile**, click **OK**, and then click **Apply**.



Step 3: In the AnyConnect Client Profile pane, select the RA-Profile you just built, and then click **Edit**. This launches the AnyConnect Client Profile Editor.

The Server List panel allows you to enter names and addresses for the appliances to which the Cisco AnyConnect Client is allowed to connect.

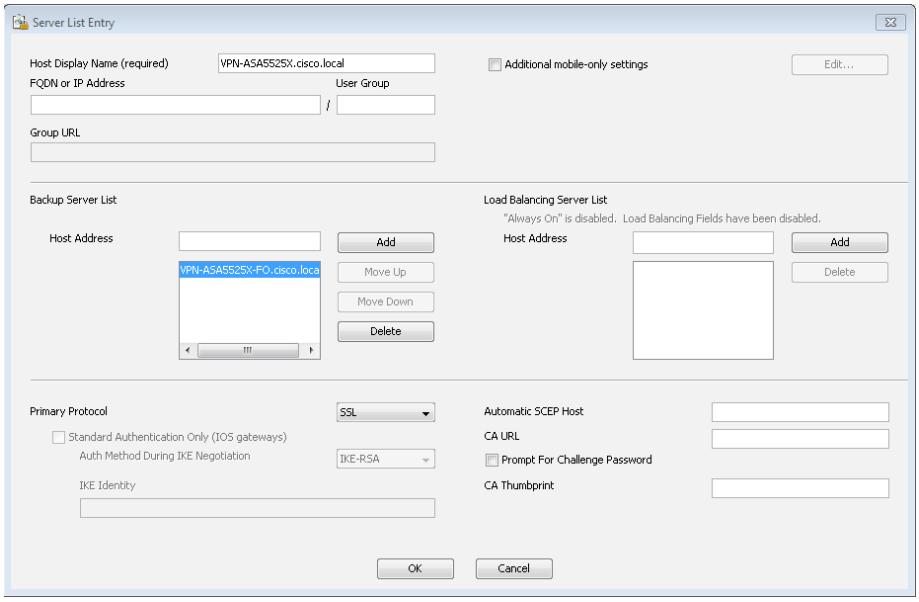
Step 4: Click **Server List**. The Server List panel opens.

Step 5: Click **Add**.

Step 6: On the Server List Entry dialog box, in the Host Display Name box, enter the primary FQDN of the remote-access firewall. (Example: VPN-ASA5525X.cisco.local)

> **Tech Tip**
>
> The entry used for the Host Display Name must be listed in your organization's DNS database. If you have not updated your DNS to include the primary and secondary FQDNs as listed in Table 2, do so now.

Step 7: In the Backup Server List pane, in the Host Address box, enter the secondary FQDN of the remote-access firewall (Example: VPN-ASA5525X-FO.cisco.local), click **Add**, and then click **OK**.



Step 8: Click **OK**. The AnyConnect Client Profile Editor closes.

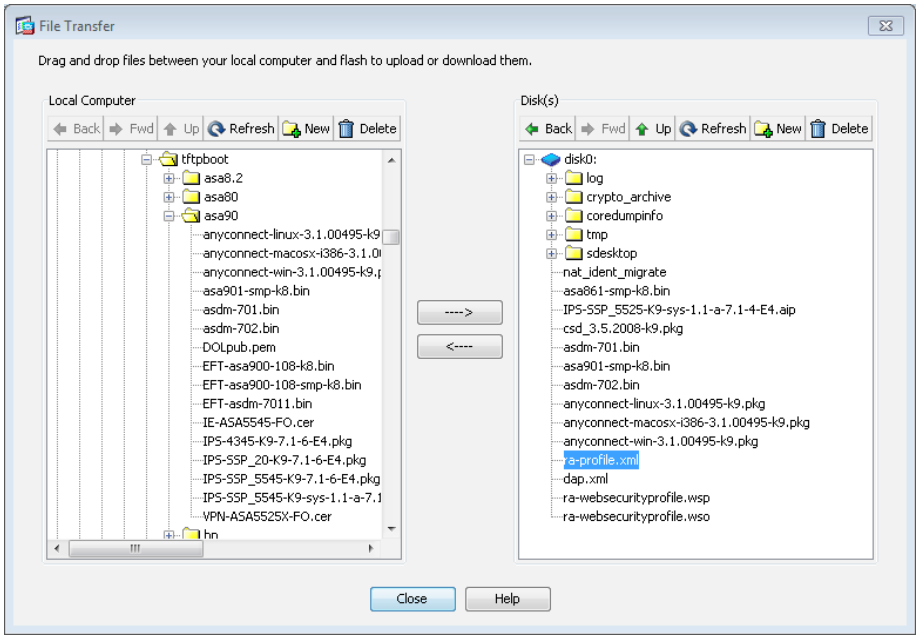
Step 9: Click **Save**. This writes the configuration changes on the Cisco ASA appliance.

When running a RA VPN Cisco ASA firewall pair, the AnyConnect client profile must be manually replicated to the secondary Cisco ASA firewall.

Step 10: Navigate to **Tools > File Management**, click **File Transfer**, and then select **Between Local PC and Flash**.

Step 11: Browse to a destination on your local file system and copy the AnyConnect client profile file from the Cisco ASA disk (Example: ra-profile.xml) by selecting the profile and then clicking the left arrow.

Step 12: After a successful file transfer, click **Close**.



Step 13: Navigate to the secondary RA VPN Cisco ASA's inside IP address, and then launch ASDM. (Example: https://10.4.24.23)

Tech Tip

Do not attempt to modify the firewall configuration on the standby appliance. You should make configuration changes only on the primary appliance.

Step 14: Navigate to **Tools > File Management.**

Step 15: Click **File Transfer**, and then select **Between Local PC and Flash**.

Step 16: Browse to a destination on your local filesystem and copy the AnyConnect client profile file from to the secondary Cisco ASA disk (Example: ra-profile.xml) by selecting the profile and then clicking on the right arrow. After a successful file transfer, click **Close**.

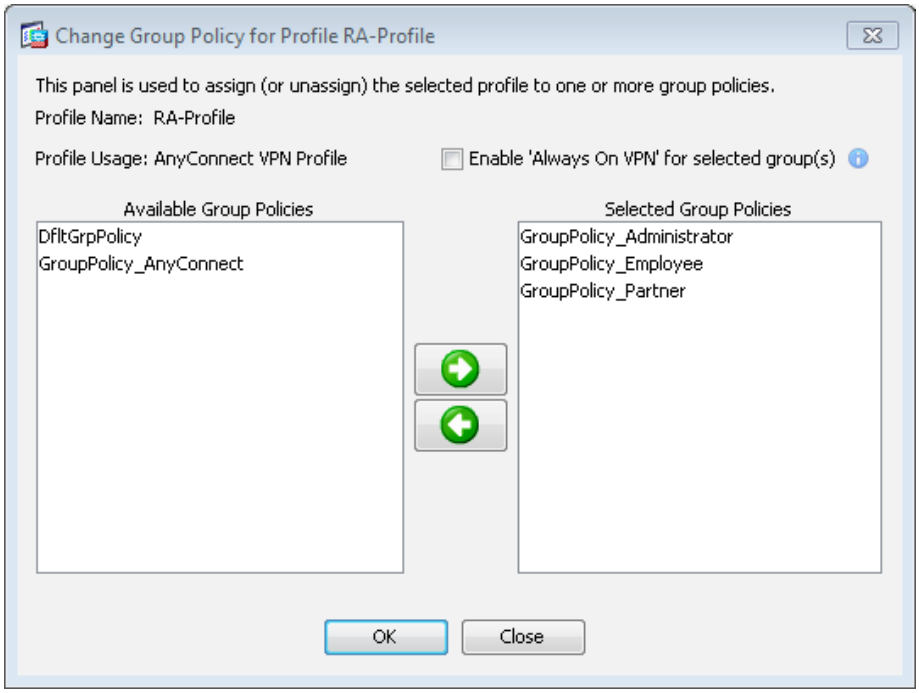
Step 17: Close ASDM on the secondary RA VPN Cisco ASA appliance.

Step 18: Once the AnyConnect client profile file has been copied to the secondary RA VPN appliance, from the command prompt, issue the **write standby** command from the primary RA VPN appliance.

```
VPN-ASA5525X# write standby
```

Step 19: On the primary RA VPN Cisco ASA appliance, in the AnyConnect Client Profile pane, select the AnyConnect VPN profile (Example: RA-Profile), and then click **Change Group Policy**.

Step 20: In the Change Group Policy for Profile dialog box, in the **Available Group Policies** list, choose the three group policies you just created, click the right arrow, and then click **OK**.



Step 21: In the AnyConnect Client Profile pane, click **Apply**.

Summary

This design guide is a reference design for Cisco customers and partners. It covers the Internet edge remote access VPN component, and is meant to be used in conjunction with the Firewall and IPS Design Guide.

Appendix A: Product List

Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 9.0(1) IPS 7.1(7) E4
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	
	Cisco ASA 5515-X IPS Edition - security appliance	ASA5515-IPS-K9	
	Cisco ASA 5512-X IPS Edition - security appliance	ASA5512-IPS-K9	
	Cisco ASA5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.0(2)
RA VPN Firewall	Cisco ASA 5545-X Firewall Edition - security appliance	ASA5545-K9	ASA 9.0(1)
	Cisco ASA 5525-X Firewall Edition - security appliance	ASA5525-K9	
	Cisco ASA 5515-X Firewall Edition - security appliance	ASA5515-K9	
	Cisco ASA 5512-X Firewall Edition - security appliance	ASA5512-K9	
	Cisco ASA 5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.0(2)
AnyConnect License	AnyConnect Essentials VPN License - ASA 5545-X (2500 Users)	L-ASA-AC-E-5545	
	AnyConnect Essentials VPN License - ASA 5525-X (750 Users)	L-ASA-AC-E-5525	
	AnyConnect Essentials VPN License - ASA 5515-X (250 Users)	L-ASA-AC-E-5515	
	AnyConnect Essentials VPN License - ASA 5512-X (250 Users)	L-ASA-AC-E-5512	

Internet Edge LAN

Functional Area	Product Description	Part Numbers	Software
Outside Switch	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 ports and Four GbE SFP Uplink ports	WS-C2960S-24TS-L	15.0(2)SE2 LAN Base license

VPN Client

Functional Area	Product Description	Part Numbers	Software
VPN Client	Cisco AnyConnect Secure Mobility Client (Windows)	Cisco AnyConnect Secure Mobility Client	3.1.00495
	Cisco AnyConnect Secure Mobility Client (Mac OS X)	Cisco AnyConnect Secure Mobility Client	
	Cisco AnyConnect Secure Mobility Client (Linux)	Cisco AnyConnect Secure Mobility Client	

Access Control

Functional Area	Product Description	Part Numbers	Software
Authentication Services	ACS 5.3 VMware Software and Base License	CSACS-5.3-VM-K9	5.3

LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.1(1)SY IP Services license
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module	CVR-CFP-4SFP10G	
	Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP-2T	
Modular Distribution Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.4.0.SG(15.1-2SG) Enterprise Services license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	
	Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module	WS-X4624-SFP-E	
	Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
Stackable Distribution Layer Switch	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.0(2)SE2 IP Services license
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

Appendix B: Configuration Example

RA VPN ASA5525X

```
ASA Version 9.0(1)
!
hostname VPN-ASA5525X
domain-name cisco.local
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
ip local pool RA-pool 10.4.28.1-10.4.31.254 mask 255.255.252.0
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.4.24.24 255.255.255.224 standby 10.4.24.23
 summary-address eigrp 100 10.4.28.0 255.255.252.0 5
!
interface GigabitEthernet0/1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/2
 description LAN/STATE Failover Interface
!
interface GigabitEthernet0/3
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3.16
 vlan 16
 nameif outside-16
 security-level 0
 ip address 172.16.130.122 255.255.255.0
!
interface GigabitEthernet0/3.17
 vlan 17
 nameif outside-17
```

```
 security-level 0
 ip address 172.17.130.122 255.255.255.0
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/7
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 shutdown
 no nameif
 no security-level
 no ip address
!
boot system disk0:/asa901-smp-k8.bin
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns server-group DefaultDNS
 domain-name cisco.local
same-security-traffic permit intra-interface
object network NETWORK_OBJ_10.4.28.0_22
 subnet 10.4.28.0 255.255.252.0
object network internal-network
 subnet 10.4.0.0 255.254.0.0
 description Internal Network
access-list ALL_BUT_DEFAULT standard deny host 0.0.0.0
```

```
access-list ALL_BUT_DEFAULT standard permit any4
access-list RA_PartnerACL remark Partners can access this internal host only!
access-list RA_PartnerACL standard permit host 10.4.48.35
access-list RA_SplitTunnelACL remark Internal Networks
access-list RA_SplitTunnelACL standard permit 10.4.0.0 255.254.0.0
access-list RA_SplitTunnelACL remark DMZ Networks
access-list RA_SplitTunnelACL standard permit 192.168.16.0 255.255.248.0
pager lines 24
logging enable
logging buffered informational
logging asdm informational
mtu inside 1500
mtu outside-16 1500
mtu outside-17 1500
failover
failover lan unit secondary
failover lan interface failover GigabitEthernet0/2
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover key FailoverKey
failover replication http
failover link failover GigabitEthernet0/2
failover interface ip failover 10.4.24.97 255.255.255.248 standby 10.4.24.98
monitor-interface outside-16
monitor-interface outside-17
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-702.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
nat (inside,outside-17) source static any any destination static NETWORK_
OBJ_10.4.28.0_22 NETWORK_OBJ_10.4.28.0_22 no-proxy-arp route-lookup
nat (inside,outside-16) source static any any destination static NETWORK_
OBJ_10.4.28.0_22 NETWORK_OBJ_10.4.28.0_22 no-proxy-arp route-lookup
!
router eigrp 100
 no auto-summary
 distribute-list ALL_BUT_DEFAULT out
 network 10.4.0.0 255.254.0.0
 passive-interface default
 no passive-interface inside
 redistribute static
!
route outside-16 0.0.0.0 0.0.0.0 172.16.130.126 1 track 1
route outside-17 0.0.0.0 0.0.0.0 172.17.130.126 50
route outside-16 172.18.1.1 255.255.255.255 172.16.130.126 1
route inside 0.0.0.0 0.0.0.0 10.4.24.1 tunneled
```

```
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (inside) host 10.4.48.15
 key SecretKey
aaa-server AAA-RADIUS protocol radius
aaa-server AAA-RADIUS (inside) host 10.4.48.15
 timeout 5
 key SecretKey
user-identity default-domain LOCAL
aaa authentication enable console AAA-SERVER LOCAL
aaa authentication ssh console AAA-SERVER LOCAL
aaa authentication http console AAA-SERVER LOCAL
aaa authentication serial console AAA-SERVER LOCAL
aaa authorization exec authentication-server
http server enable
http 10.4.48.0 255.255.255.0 inside
snmp-server host inside 10.4.48.35 community cisco
no snmp-server location
no snmp-server contact
snmp-server community cisco
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
sla monitor 16
 type echo protocol ipIcmpEcho 172.18.1.1 interface outside-16
sla monitor schedule 16 life forever start-time now
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-set ESP-AES-128-
SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5
ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set reverse-route
```

```
crypto map outside-16_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside-16_map interface outside-16
crypto ca trustpoint VPN-ASA5525X-Trustpoint
 enrollment self
 subject-name CN=VPN-ASA5525X.cisco.local
 keypair VPN-ASA5525X-Keypair
 proxy-ldc-issuer
 crl configure
crypto ca trustpoint VPN-ASA5525X-FO-Trustpoint
 enrollment self
 subject-name CN=VPN-ASA5525X-FO.cisco.local
 keypair VPN-ASA5525X-Keypair
 proxy-ldc-issuer
 crl configure
crypto ca trustpoint ASDM_TrustPoint0
 enrollment self
 subject-name CN=VPN-ASA5525X
 keypair foobar
 proxy-ldc-issuer
 crl configure
crypto ca trustpool policy
crypto ca certificate chain VPN-ASA5525X-Trustpoint
 certificate 196dbd50
    30820379 30820261 a0030201 02020419 6dbd5030 0d06092a 864886f7 0d010105
    0500304c 3121301f 06035504 03131856 504e2d41 53413535 3235582e 63697363
    6f2e6c6f 63616c31 27302506 092a8648 86f70d01 09021618 56504e2d 41534135
    35323558 2e636973 636f2e6c 6f63616c 301e170d 31323132 31373232 34353131
    5a170d32 32313231 35323234 3531315a 304c3121 301f0603 55040313 1856504e
    2d415341 35353235 582e6369 73636f2e 6c6f6361 6c312730 2506092a 864886f7
    0d010902 16185650 4e2d4153 41353532 35582e63 6973636f 2e6c6f63 616c3082
    0122300d 06092a86 4886f70d 01010105 00038201 0f003082 010a0282 010100be
    b40a3916 c07f0a5a ca49459f 1ff0fde1 18fdd1d3 1549f412 591ea3da d0fdc925
    e590bd9f ddb0a47b 488cfbcc 0a8245de 2c1bba6c b63c12d4 9378e952 c3146de5
    5cbaa719 c6cbc071 8ad5b3c1 fa3f9aaa f382b256 8518fa3b 0f4674d9 c973ec60
    b78a92a9 ccaeca0a bf55510d 1dd0e6b9 19c8d200 ae13aa37 aed1dae8 f06cd971
    9db5a13e ef9fab17 a66f1745 973ed31b 80cc10fc 27e7159b e2ada507 000d0161
    56c3c3b5 dddb1010 2db93953 7bea683e 5d15e0e0 ec616cf1 d16bd4af e744c3ec
    ca686421 21ec21aa e05121c5 6dcc6c77 68638f87 2cee1f57 015fc2a4 bd5a4f36
    ccfe7a2e 78c20b1b f0e5f5fa 01b82783 2fbf0748 1df74d18 113c52db 58a27b02
    03010001 a3633061 300f0603 551d1301 01ff0405 30030101 ff300e06 03551d0f
    0101ff04 04030201 86301f06 03551d23 04183016 80142836 731ddd16 be77e390
    7c3543cb 6fcfbeba 47d7301d 0603551d 0e041604 14283673 1ddd16be 77e3907c
    3543cb6f cfbeba47 d7300d06 092a8648 86f70d01 01050500 03820101 001f3f41
    c292da00 7b7a5435 387b60fd 169ed55d 5a8634f9 1981a26b 950e84d2 fcc1608f
    4c198baa 76c7e40a 36922ed3 ef561037 a1ed3dee 49c9e7b1 bf465d4a 31c45abc
    42da8ed6 88721355 6e10c417 71a14481 6f379edf 7052500f fbdd0142 92ec9dc2
    f82927e6 2cb3de0e 948f690b 9aa2d831 88c27c0c bbd11fa1 21a08fec 22da19d3
```

```
    ded3c076 76540ade d9e996ab 7dc26518 ea1b999c fe8d54c9 a26d455f 678030ac
    012ec360 fcab84d3 9271d88c e46e3def 45d6fa34 293d6bc6 89e014cc 740cc939
    be773a31 640b7dec 8f5b32f2 db785864 b89a68ae bb5d8bc5 33cce6b9 b16a63ca
    2d541dc2 79ed0483 3f9afc1c 3060aa60 0ecd97c5 6f1b0a1a 9af9e717 36
  quit
crypto ca certificate chain VPN-ASA5525X-FO-Trustpoint
 certificate 1a6dbd50
    3082037f 30820267 a0030201 0202041a 6dbd5030 0d06092a 864886f7 0d010105
    0500304f 31243022 06035504 03131b56 504e2d41 53413535 3235582d 464f2e63
    6973636f 2e6c6f63 616c3127 30250609 2a864886 f70d0109 02161856 504e2d41
    53413535 3235582e 63697363 6f2e6c6f 63616c30 1e170d31 32313231 37323234
    3535355a 170d3232 31323135 32323435 35355a30 4f312430 22060355 0403131b
    56504e2d 41534135 35323558 2d464f2e 63697363 6f2e6c6f 63616c31 27302506
    092a8648 86f70d01 09021618 56504e2d 41534135 35323558 2e636973 636f2e6c
    6f63616c 30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a
    02820101 00beb40a 3916c07f 0a5aca49 459f1ff0 fde118fd d1d31549 f412591e
    a3dad0fd c925e590 bd9fddb0 a47b488c fbcc0a82 45de2c1b ba6cb63c 12d49378
    e952c314 6de55cba a719c6cb c0718ad5 b3c1fa3f 9aaaf382 b2568518 fa3b0f46
    74d9c973 ec60b78a 92a9ccae ca0abf55 510d1dd0 e6b919c8 d200ae13 aa37aed1
    dae8f06c d9719db5 a13eef9f ab17a66f 1745973e d31b80cc 10fc27e7 159be2ad
    a507000d 016156c3 c3b5dddb 10102db9 39537bea 683e5d15 e0e0ec61 6cf1d16b
    d4afe744 c3ecca68 642121ec 21aae051 21c56dcc 6c776863 8f872cee 1f57015f
    c2a4bd5a 4f36ccfe 7a2e78c2 0b1bf0e5 f5fa01b8 27832fbf 07481df7 4d18113c
    52db58a2 7b020301 0001a363 3061300f 0603551d 130101ff 04053003 0101ff30
    0e060355 1d0f0101 ff040403 02018630 1f060355 1d230418 30168014 2836731d
    dd16be77 e3907c35 43cb6fcf beba47d7 301d0603 551d0e04 16041428 36731ddd
    16be77e3 907c3543 cb6fcfbe ba47d730 0d06092a 864886f7 0d010105 05000382
    0101001f 5a3e2fcc c384ca51 7519a55b 15d16c77 9a23ed00 72fba6fa ce0251dc
    274e59e8 664c0119 c42ae064 1956a610 a9f08787 3df62168 cdd9ac8a 968f69d3
    ebd48f27 c1ede1f6 63169317 bf070a22 f321d4b9 b6157593 59cb71cb bf8492fe
    ff8f8072 defb92eb 5d50b97c 24fd0c60 cd6ad778 afa18e73 b824b132 11970758
    e0a8b8f9 75b0a458 90bdefdb 324a6eb0 547a703c 0eb1d205 26f894db 02632a6d
    5b6c534b 77344868 10b4c4c3 811c073e e0193ddf bfcb3e0d 8eae3e4c 10d0a269
    6f500e65 fbf99d3b 5f06061f 241a1679 4fb0cb00 f07a01da 930a4636 959afbfd
    27e01065 d3730911 08eb3c6b c7494ff5 df273d77 adc52e75 79dd62a6 67d77785
    e88d11
  quit
crypto ikev1 enable outside-16
crypto ikev1 policy 10
 authentication crack
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 20
 authentication rsa-sig
 encryption aes-256
```

```
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 30
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 40
 authentication crack
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 50
 authentication rsa-sig
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 60
 authentication pre-share
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 70
 authentication crack
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 80
 authentication rsa-sig
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 90
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 100
 authentication crack
```

```
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 110
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 120
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 130
 authentication crack
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 140
 authentication rsa-sig
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 150
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
!
track 1 rtr 16 reachability
telnet timeout 5
ssh 10.4.48.0 255.255.255.0 inside
ssh timeout 5
ssh version 2
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 10.4.48.17
ssl encryption aes256-sha1 aes128-sha1 3des-sha1
ssl trust-point VPN-ASA5525X-FO-Trustpoint outside-17
```

```
ssl trust-point VPN-ASA5525X-Trustpoint outside-16
webvpn
 enable outside-16
 enable outside-17
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.1.00495-k9.pkg 1
 anyconnect image disk0:/anyconnect-macosx-i386-3.1.00495-k9.pkg 2
 anyconnect image disk0:/anyconnect-linux-3.1.00495-k9.pkg 3
 anyconnect profiles RA-Profile disk0:/ra-profile.xml
 anyconnect enable
 tunnel-group-list enable
group-policy GroupPolicy_Employee internal
group-policy GroupPolicy_Employee attributes
 banner value Group "vpn-employee" allows for unrestricted access with a tunnel all policy.
 vpn-filter value Block_Trusted_Host
 split-tunnel-policy excludespecified
 split-tunnel-network-list value CWS_Tower_Exclude
 webvpn
  anyconnect modules value websecurity
  anyconnect profiles value RA-Profile type user
  anyconnect profiles value RA-WebSecurityProfile.wso type websecurity
  always-on-vpn profile-setting
group-policy GroupPolicy_AnyConnect internal
group-policy GroupPolicy_AnyConnect attributes
 wins-server none
 dns-server value 10.4.48.10
 vpn-tunnel-protocol ssl-client
 default-domain value cisco.local
group-policy GroupPolicy_Partner internal
group-policy GroupPolicy_Partner attributes
 banner value Group "vpn-partner" allows for access control list (ACL) restricted access
with a tunnel all policy.
 vpn-filter value RA_PartnerACL
 webvpn
  anyconnect profiles value RA-Profile type user
group-policy GroupPolicy_Administrator internal
group-policy GroupPolicy_Administrator attributes
 banner value Group "vpn-administrator" allows for unrestricted access with a split
tunnel policy.
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value RA_SplitTunnelACL
 webvpn
  anyconnect profiles value RA-Profile type user
username admin password 7KKG/zg/Wo8c.YfN encrypted privilege 15
tunnel-group AnyConnect type remote-access
tunnel-group AnyConnect general-attributes
 address-pool RA-pool
```

```
 authentication-server-group AAA-RADIUS
 default-group-policy GroupPolicy_AnyConnect
 password-management
tunnel-group AnyConnect webvpn-attributes
 group-alias AnyConnect enable
 group-url https://172.16.130.122/AnyConnect enable
 group-url https://172.17.130.122/AnyConnect enable
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
: end
```

Feedback

Please use the feedback form to send comments and suggestions about this guide.

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.

B-0000285-1 08/13