VPN Using Cisco ASA 5505

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:

- **Teleworker with Wired Ethernet Devices**—Teleworkers who need always-on, secure access to networked business services from the remote home office often require telework resources connected with wired Ethernet.

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

Scope

This guide covers the following areas of technology and products:

- Remote-site teleworking using the Cisco Adaptive Security Appliance
- Internet edge firewall and VPN termination on Cisco Adaptive Security Appliances

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 Security**—1 to 3 years installing, monitoring, and troubleshooting network devices to maintain integrity, confidentiality, and availability of data and devices

Related CVD Guides

Remote Access VPN Technology Design Guide

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

Introduction

Technology Use Case

Many organizations face increasing need to offer a telecommuter solution to their employees. Employees perceive that commuting and water-cooler chatter are time they spend at work, and renting or buying office space and fixtures, and even deploying network infrastructure to host the work force, adds up to a substantial sum of capital and operating expense.

Providing an office-like work environment at the teleworker's home requires:

- A phone that is accessible as an extension on the organization's phone system.
- An unobtrusive, quiet, low-power solution to provide multiple Ethernet connections for one or more IP-phones or other desktop collaboration resources.
- One or more Ethernet connections for computers that access the organization's network, as well as Ethernet connectivity for other network-connected devices, such as printers and IP video surveillance equipment.

Employees don't need wireless connectivity at the telework site because all of the telework resources connect with wired Ethernet.

Use Case: Teleworker with Wired Ethernet Devices

Teleworkers require always-on secure access to networked business services from the remote home office. Sometimes employees don't need wireless connectivity at the telework site because all of the telework resources connect with wired Ethernet.

This design guide enables the following network capabilities:

- Authentication for employees before they can communicate with internal resources and encryption for all information sent and received to the organization's main location
- Co-residence with the organization's Internet edge firewall or remote-access VPN setup
- Power over Ethernet (PoE) for voice endpoints at the teleworker location

Design Overview

Cisco Adaptive Security Appliance (ASA) 5505 offers a low-cost option to provide teleworker connectivity to the organization. Cisco ASA 5505 provides secure connectivity for data and collaboration endpoints in a compact, fanless form factor, minimizing noise and space requirements.

The Cisco ASA 5505 teleworker solution integrates at the organization's Internet edge. The teleworker's connection terminates at resilient Cisco ASA firewalls at the organization's Internet edge. This solution is configured on the same ASA firewalls as the remote-access virtual private network (RAVPN) solution. This configuration applies to dedicated and shared-mode RAVPN deployments. Some of the configuration re-uses portions of the RAVPN configuration, although it may be configured to be completely independent of the RAVPN resources. The addition of the head-end's support for Cisco ASA 5505 teleworker termination does not affect RAVPN connectivity, and the configuration can be applied without the imposition of a service outage.

The Cisco ASA 5505 teleworker solution provides access for endpoint devices, such as laptop and desktop computers, IP phones, printers, and other devices that connect to the network via wired Ethernet connections.

Two of the Cisco ASA 5505's ports provide Power over Ethernet (PoE) to support IP phones, IP video surveillance, and other endpoints without cluttering the teleworker's office with additional cables and wall-wart power supplies.

The Cisco ASA 5505 teleworker solution offers:

- **Low cost**–With this solution, you get a Cisco ASA 5505, a Cisco IP phone, and the necessary license on the organization's Internet edge Cisco ASAs.
- **Flexible connectivity**–The Cisco ASA 5505's integrated Ethernet switch can accommodate multiple endpoint devices, including two interfaces that can provide PoE.
- **Simple deployment**–The Cisco ASA 5505 can be configured quickly with a brief text-file configuration.
- **Security**–Deactivation of the teleworker site's credentials on the Internet-edge appliance can terminate the teleworker's connectivity.

  Ideally, the Cisco ASA 5505 teleworker device is preconfigured and sent home with the teleworker user. A newly-provisioned or existing desktop IP-phone can be taken home, as well, and registers to the Cisco Call Manager server over the VPN.

Deployment Details

Configuration of remote-access connectivity consists of two phases. In the first phase, you configure your resilient Internet-edge appliance pair to receive VPN connections from teleworkers' Cisco ASA 5505 appliances. In the second phase, you deploy configuration on the teleworkers' Cisco ASA 5505 hardware clients.

PROCESS

Configuring RAVPN Cisco ASA for Teleworker VPN

1. Configure IPsec(IKEv1) connection profile
2. Configure NAT exemption
3. Configure route advertisement

As a rule, the Cisco ASA configuration for Cisco ASA 5505 teleworker VPN is self-contained. A few aspects rely on configuration from the Internet-edge foundation, so you need to have followed the configuration steps for Cisco ASA-based Remote Access VPN in the Remote Access VPN Design Guide.

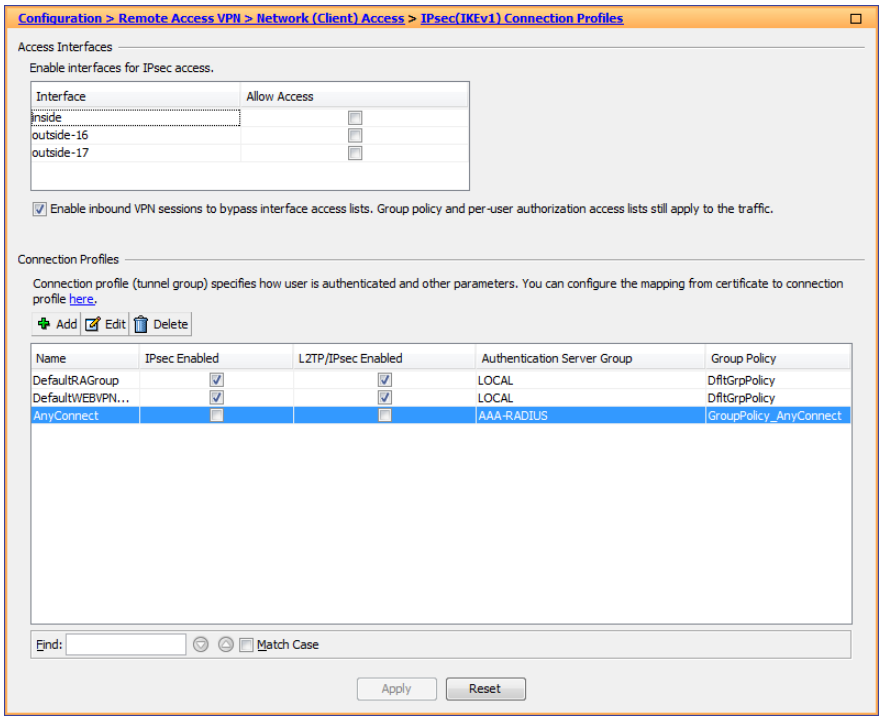
Procedure 1 Configure IPsec(IKEv1) connection profile

The IPsec connection profile carries the bulk of the configuration that sets the behavior for VPN client connections, so you must apply a number of steps in this procedure to complete the central configuration.

Step 1: Launch the Cisco ASA Security Device Manager.

Step 2: Navigate to the **Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles**.

Step 3: In the right pane under **Connection Profiles**, click **Add**.



Step 4: On the Add IPsec Remote Access Connection Profile dialog box, enter the following details. This configuration affects the behavior of the Cisco ASA 5505 teleworker device, as described.

- Name–**Teleworker5505**

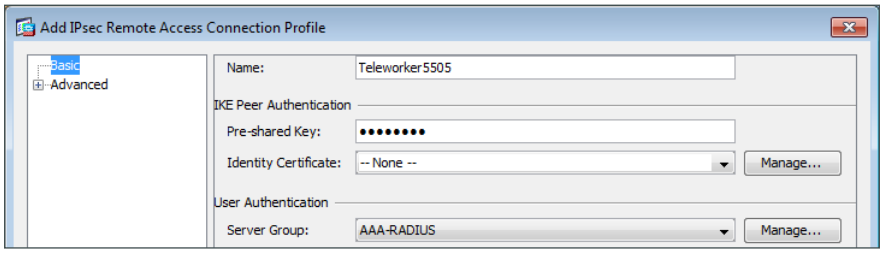
  This entry is the name of the VPN group that is reflected in the Cisco ASA 5505 Easy VPN Client configuration.

- IKE Peer Authentication Pre-Shared Key–**cisco123**

  This entry is the group key that must be duplicated in the Cisco ASA 5505 Easy VPN Client configuration.

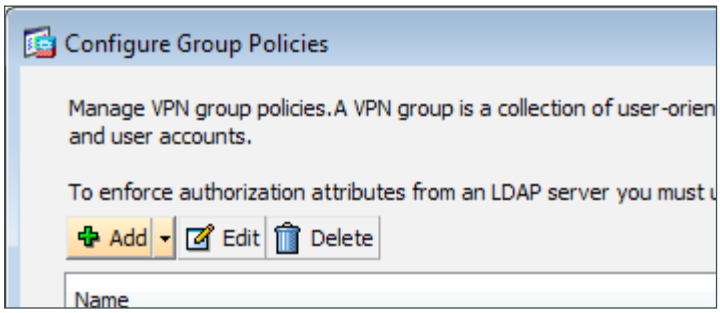
- Server Group–Select **AAA-RADIUS** or **AD**, depending on whether you are using Access Control Service (ACS) or Microsoft Active Directory for user authentication.

  This entry selects the server that authenticates user names and passwords that are presented to open the Easy VPN Client tunnel.

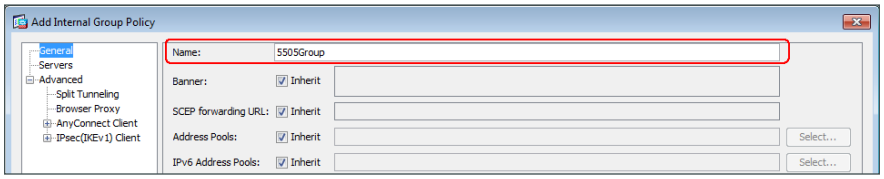


Step 5: On the right side of the **Group Policy** list, click **Manage**.

Step 6: On the Configure Group Policies dialog box, click **Add**.

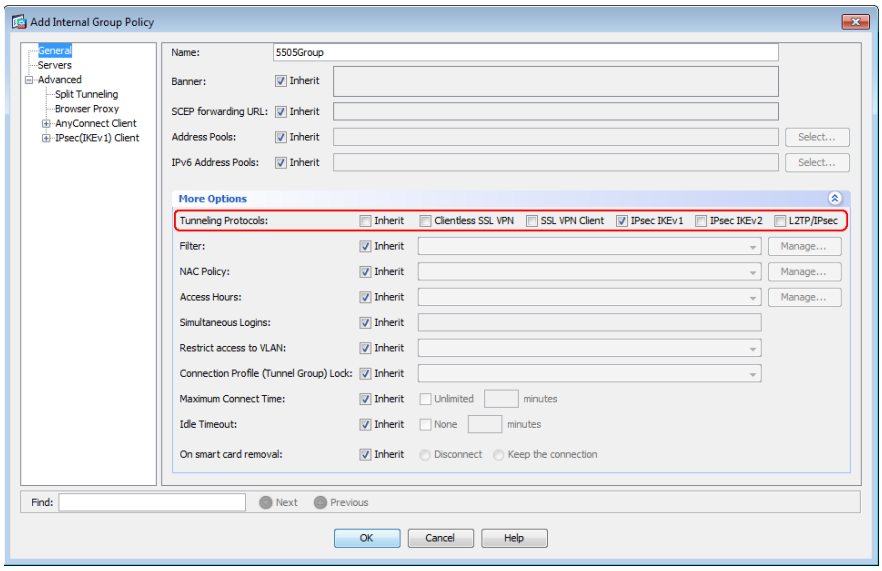


Step 7: On the Add Internal Group Policy dialog box, select **General**, and then in the **Name** box, enter **5505Group**.



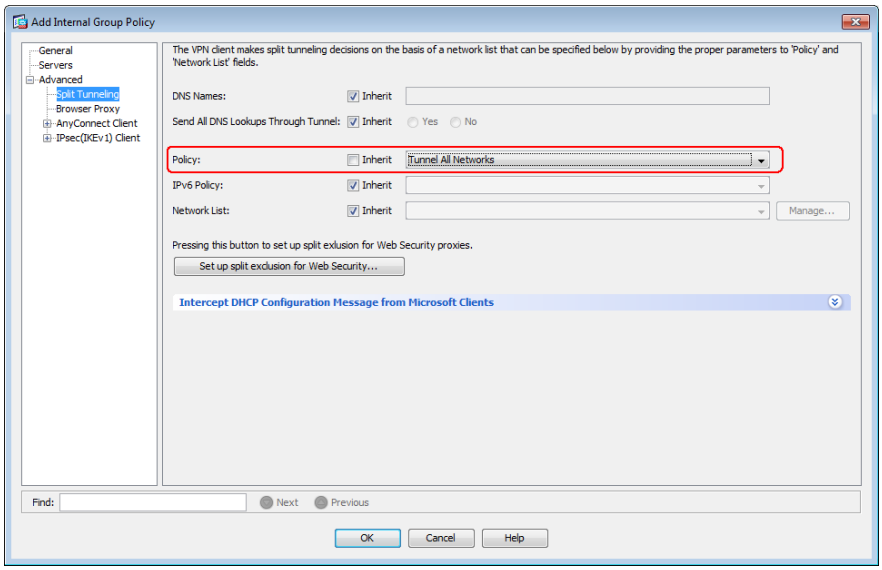
Step 8: Expand the options panel by clicking **More Options**.

Step 9: Next to **Tunneling Protocols**, clear **Inherit**, and then select **IPsec IKEv1**.



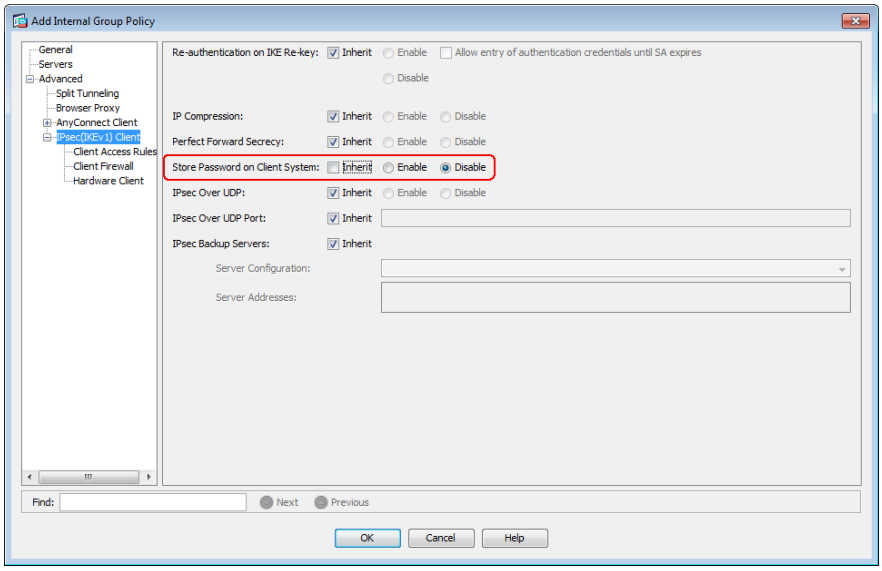
Step 10: Navigate to **Advanced > Split Tunneling**, and in the right panel, next to **Policy**, clear **Inherit.**

Step 11: Next to **Policy**, in the drop-down list, ensure that **Tunnel All Networks** is selected.



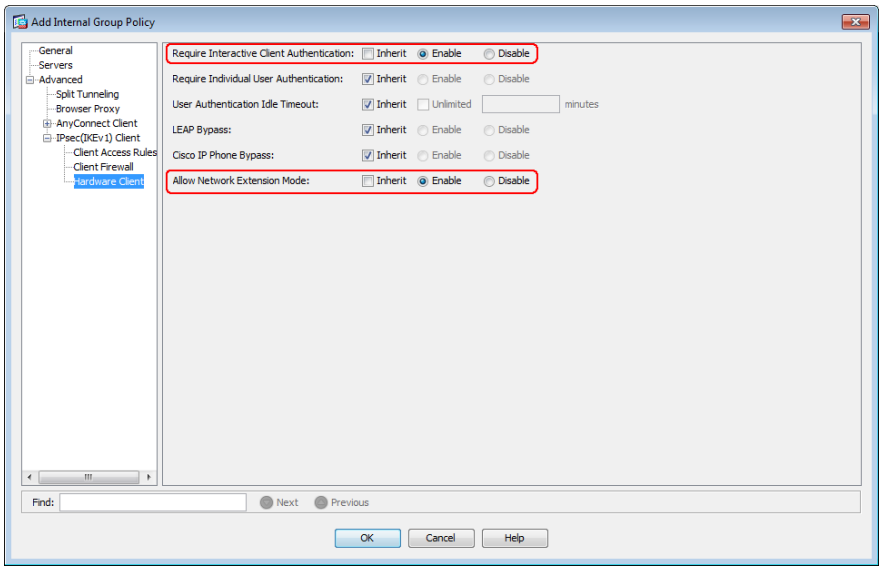
Step 12: Navigate to **Advanced > IPsec(IKEv1) Client**.

Step 13: Next to **Store Password on Client System**, clear **Inherit** and ensure that **Disable** is selected.



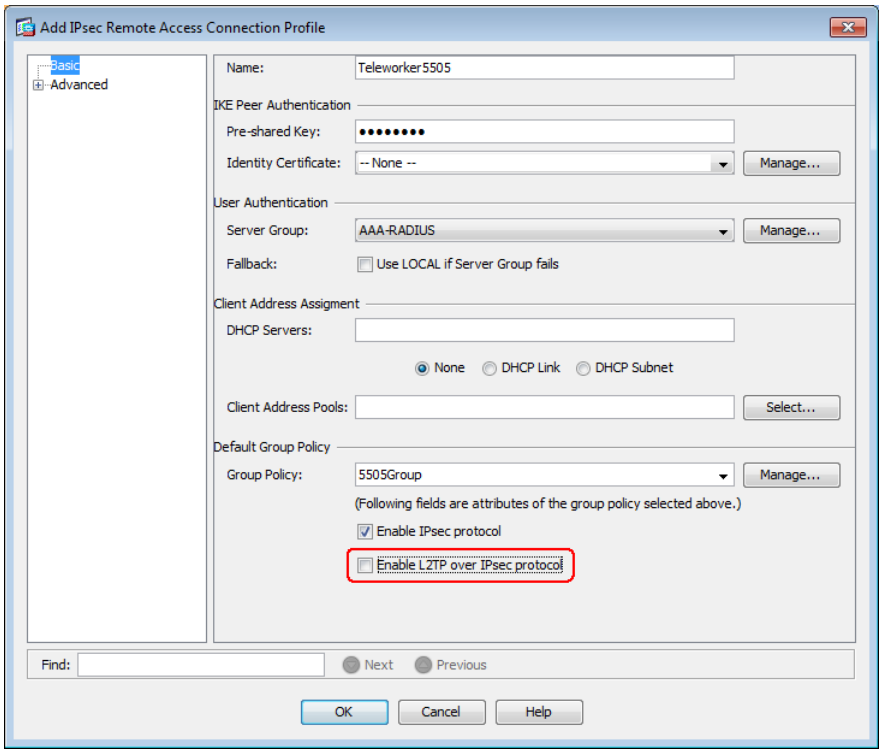
Step 14: Navigate to **Advanced > IPsec(IKEv1) Client> Hardware Client,** and do the following:

- Next to **Require Interactive Client Authentication**, clear **Inherit** and ensure that **Enable** is selected.
- Next to **Allow Network Extension Mode**, clear **Inherit** and ensure that **Enable** is selected.
- Click **OK**.



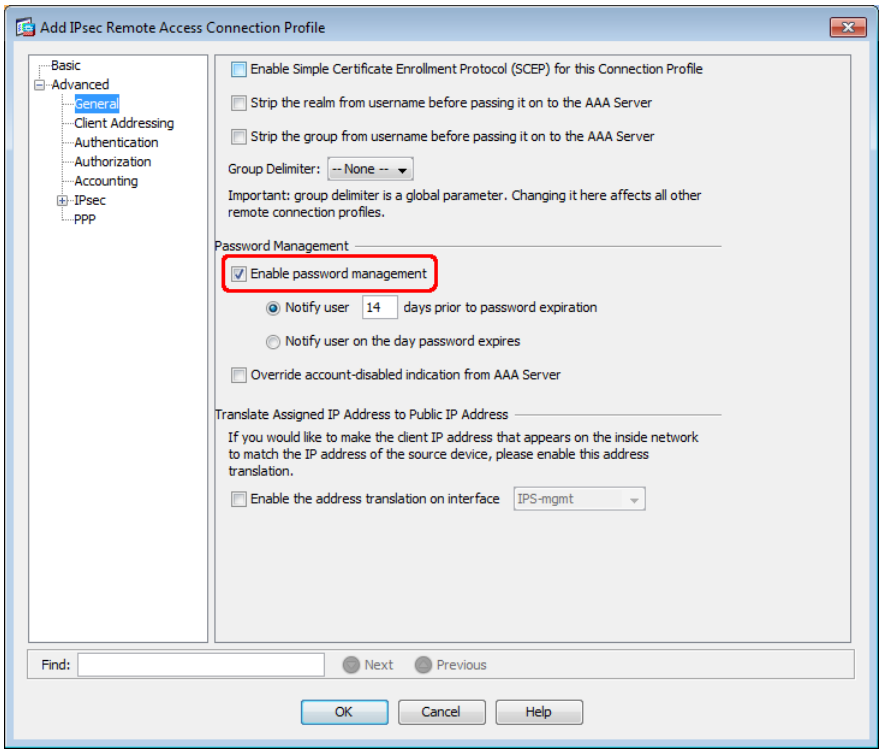
Step 15: On the Configure Group Policies dialog box, click **OK**.

Step 16: On the Add IPsec Remote Access Connection Profile dialog box, and then clear **Enable L2TP over IPsec protocol**.



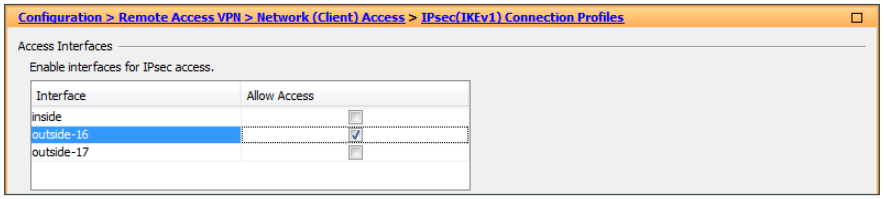
Step 17: Navigate to **Advanced > General**.

Step 18: Under **Password Management**, select **Enable password management**, and then click **OK**.



Step 19: Navigate to **Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles**.

Step 20: Under **Access Interfaces**, next to the appliance's primary outside interface, select **Allow Access**.



Step 21: Under **Connection Profiles**, verify that the new Teleworker5505 profile appears, and then click **Apply**.

The steps above apply the following configuration:

```
group-policy 5505Group internal
group-policy 5505Group attributes
  password-storage disable
  vpn-tunnel-protocol ikev1
  split-tunnel-policy   tunnelall
  secure-unit-authentication enable
  nem enable
exit
tunnel-group Teleworker5505 type remote-access
```

```
tunnel-group Teleworker5505 general-attributes
  default-group-policy 5505Group
  authentication-server-group  AAA-RADIUS
  password-management  password-expire-in-days 14
tunnel-group Teleworker5505 ipsec-attributes
  ikev1 pre-shared-key cisco123
crypto ikev1 policy 70
  encryption aes
  authentication crack
crypto ikev1 policy 80
  encryption aes
  authentication rsa-sig
crypto ikev1 policy 90
  encryption aes
crypto ikev1 policy 40
  encryption aes-192
  authentication crack
crypto ikev1 policy 50
  encryption aes-192
  authentication rsa-sig
crypto ikev1 policy 60
  encryption aes-192
crypto ikev1 policy 10
  encryption aes-256
  authentication crack
crypto ikev1 policy 20
  encryption aes-256
  authentication rsa-sig
crypto ikev1 policy 30
  encryption aes-256
crypto ikev1 policy 100
  authentication crack
crypto ikev1 policy 110
  authentication rsa-sig
crypto ikev1 policy 120
crypto ikev1 policy 130
  encryption des
  authentication crack
crypto ikev1 policy 140
  encryption des
  authentication rsa-sig
crypto ikev1 policy 150
  encryption des
crypto ikev1 enable  outside-16
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 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 map outside-16_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside-16_map interface  outside-16
```

Procedure 2 Configure NAT exemption

The Internet-edge appliances must not apply network address translation (NAT) on traffic between the organization's private network and the IP-subnet that encompasses teleworkers' remote addresses. You must configure a policy that prevents the Internet-edge appliance from applying NAT.

Configure a network object for the summary address of the internal network. The network object will be used during the security policy configuration.

Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

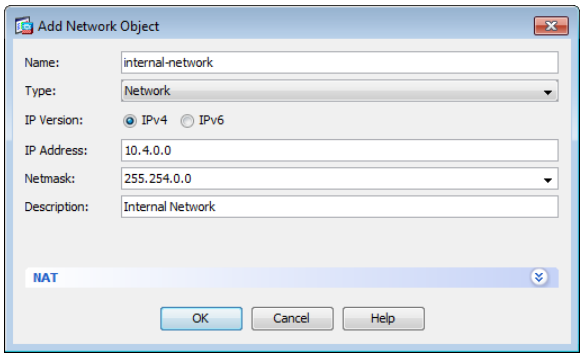
Step 2: Click **Add > Network Object**.

Step 3: On the Add Network Object dialog box, in the **Name box**, enter a description for the network summary (Example: internal-network).

Step 4: In the **Type** list, choose **Network**.

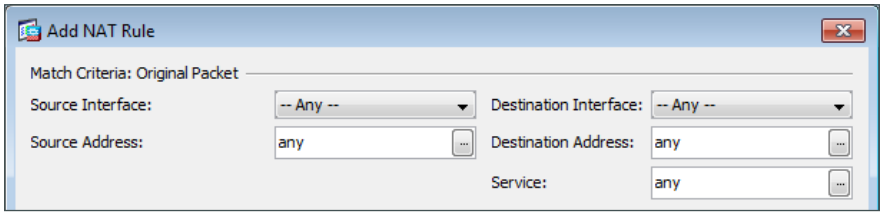
Step 5: In the **IP Address** box, enter the address that summarizes all internal networks (Example: 10.4.0.0).

Step 6: In the **Netmask** box, enter the internal network summary netmask, and then click **OK** (Example: 255.254.0.0).

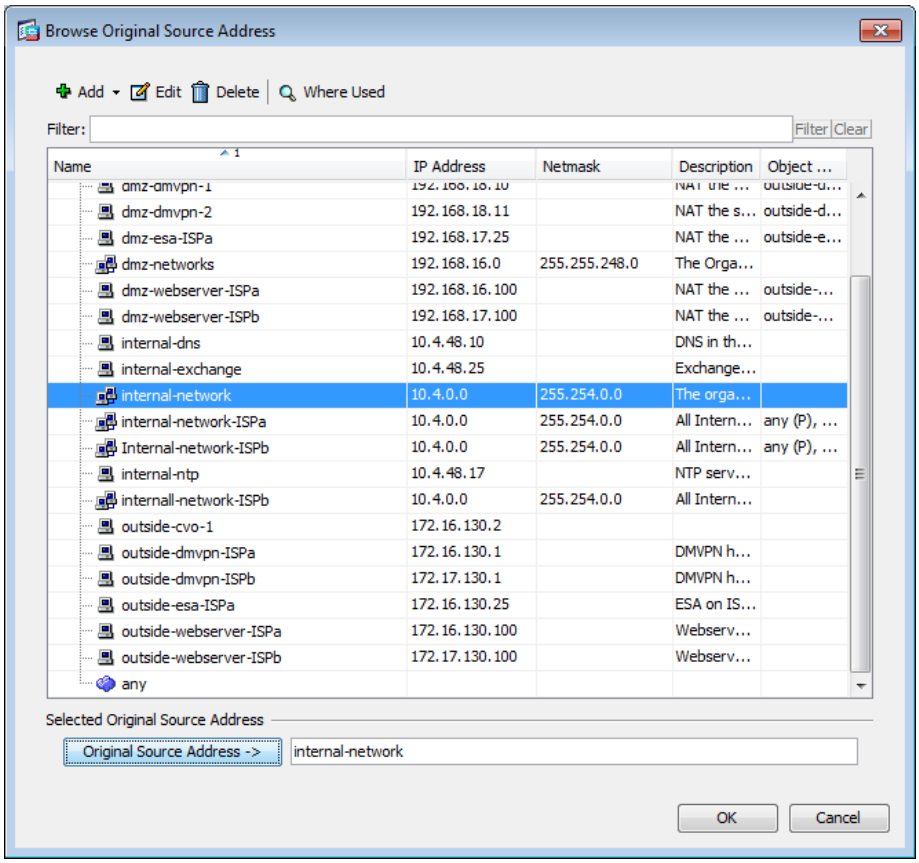


Step 7: Navigate to **Configuration > Firewall > NAT Rules**, and then click **Add**.

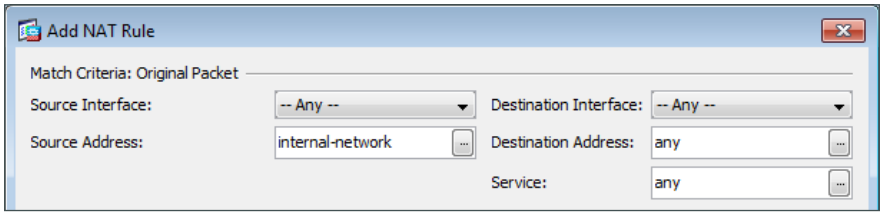
Step 8: On the Add NAT Rule dialog box, under **Match Criteria: Original Packet**, in the **Source Address** box, click the ellipsis (…).



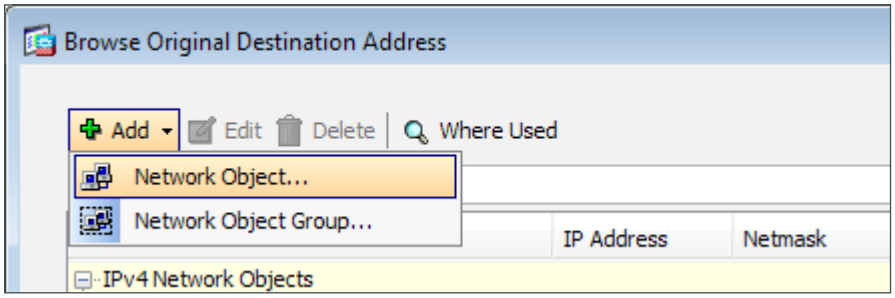
Step 9: On the Browse Original Source Address dialog box, expand the **IPv4 Network Objects** list, double-click **internal-network**, and then click **OK**.



Step 10: On the Add NAT Rule dialog box, under **Match Criteria: Original Packet**, in the **Destination Address** box, click the ellipsis (…).

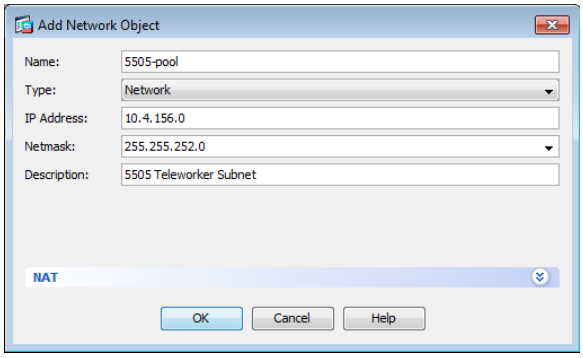


Step 11: On the Browse Original Destination Address dialog box, click **Add,** and then click **Network Object**.

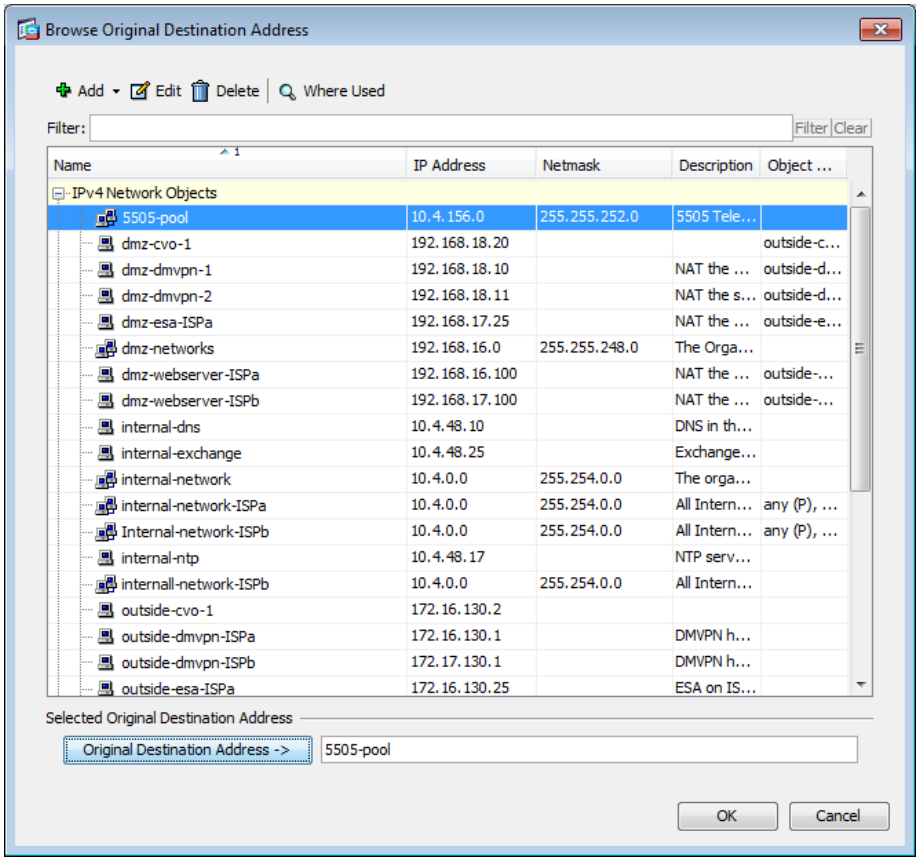


Step 12: On the Add Network Object dialog box, enter the following values, and then click **OK**.

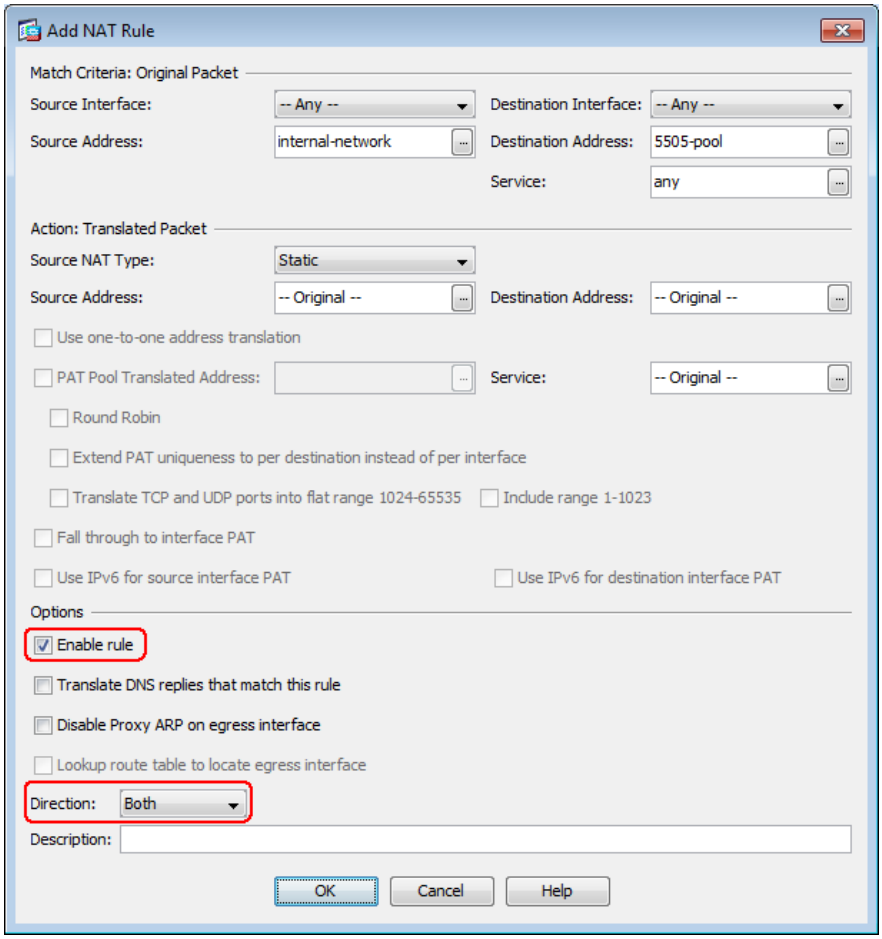
- Name—**5505-pool**
- Type—**Network**
- IP Address—**10.4.156.0**
- Netmask—**255.255.252.0**
- Description—**5505 Teleworker Subnet**



Step 13: On the Browse Original Destination Address dialog box, expand the **IPv4 Network Objects** list, double-click **5505-pool**, and then click **OK**.



Step 14: Under **Options**, ensure that **Enable Rule** is selected and that the indicated direction is **Both**, and then click **OK**.



Step 15: Review the configuration, and then click **Apply**.

Cisco Adaptive Security Device Manager (ASDM) applies the following configuration:

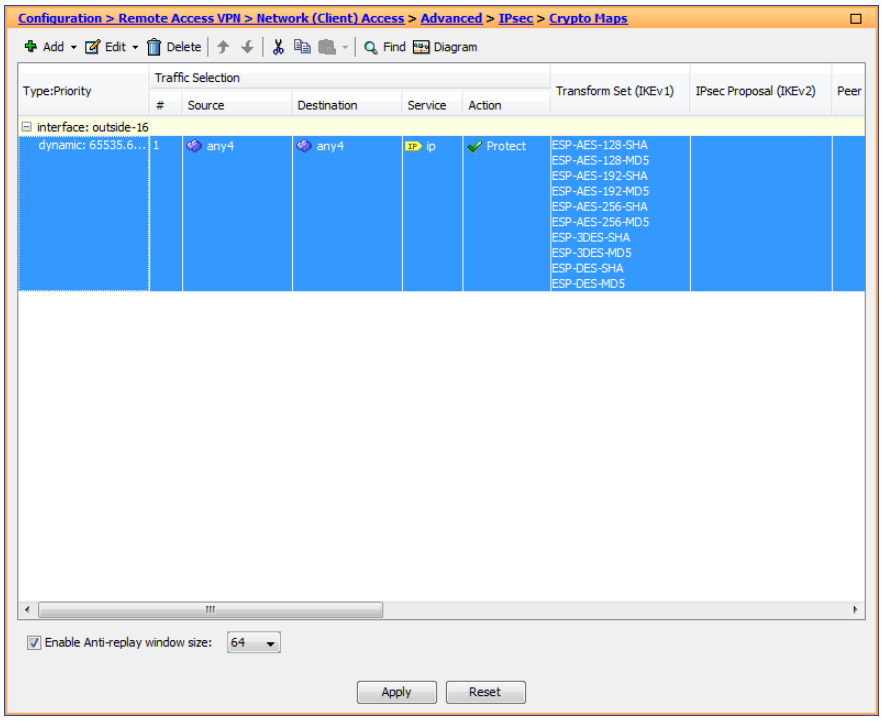
```
object network 5505-pool
  subnet 10.4.156.0 255.255.252.0
  description 5505 teleworker subnet
nat (any,any) source static internal-network internal-network destination static
5505-pool 5505-pool
```

Procedure 3 Configure route advertisement

The Internet-edge appliances must advertise the teleworker sites' networks to the internal network. RAVPN address pools are advertised as host routes by reverse route injection (RRI) and summarized by the Internet-edge appliance. Teleworker subnets are advertised by RRI, as well, but without summarization; the teleworker subnets remain intact as eight-number (/29) subnets advertised to the rest of the network.

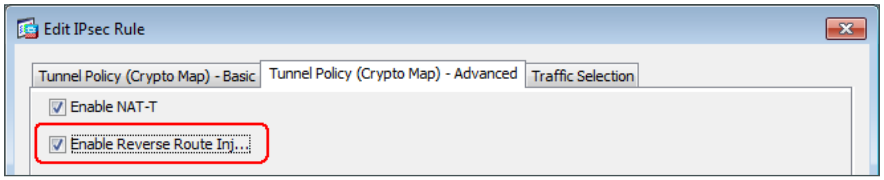
Step 1: Navigate to **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps**.

Step 2: Select the crypto map listed under the primary outside interface, and then click **Edit**.



Step 3: Click the **Tunnel Policy (Crypto Map) - Advanced** tab.

Step 4: Select **Enable Reverse Route Injection**, and then click **OK**.



Step 5: On the Crypto Maps pane, click **Apply**.

Cisco ASDM applies the following configuration:

```
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set reverse-route
```

PROCESS

Configuring Teleworker Cisco ASA 5505 Endpoints

1. Configure inside VLAN and switch ports
2. Define global device configuration
3. Configure outside VLAN and switch port
4. Configure Cisco ASA 5505 DHCP server
5. Configure Cisco ASA 5505 Easy VPN client

Each teleworker's Cisco ASA 5505 endpoint must be configured to connect to your resilient Internet-edge appliance. Because this configuration is likely to be deployed on multiple devices, the configuration is shown only in the command-line interface to streamline deployment. All Cisco ASA 5505 teleworker sites connect using Network Extension Mode, which allows teleworker-site endpoints to connect freely to the organization's LAN. Connecting in Network Extension Mode is particularly critical for endpoints, such as IP phones and video surveillance cameras, which might be susceptible to NAT's modification of data traffic.

Each site must use a unique inside-IP subnet. Otherwise, all configuration is identical between sites. To avoid conflicting address assignments, Cisco recommends that you maintain a spreadsheet of subnet assignments for the various users that will be issued Cisco ASA 5505 telecommuter equipment.

User name	Subnet	ASA 5505 LAN address	Hostname
Employee1	10.4.156.0/29	10.4.156.1	5505site1

Procedure 1 Configure inside VLAN and switch ports

Each Cisco ASA 5505 teleworker site needs a unique inside subnet, which you should track in a spreadsheet, as recommended in the introduction of this section.

Step 1: Configure the VLAN 1 interface for the teleworker site's LAN.

```
interface Vlan1
 no ip address
 nameif inside
 security-level 100
 ip address 10.4.156.1 255.255.255.248
```

Step 2: Associate the Cisco ASA 5505's Ethernet 0/1 through Ethernet 0/7 interfaces with VLAN 1, and instruct the teleworker to connect PoE-enabled devices to the Ethernet 0/6 and 0/7 ports.

```
interface Ethernet0/1
 switchport access vlan 1
 no shutdown
…
interface Ethernet0/7
 switchport access vlan 1
 no shutdown
```

Procedure 2 Define global device configuration

Step 1: Configure the Cisco ASA 5055's hostname and domain name.

```
hostname 5505site1
domain-name cisco.local
```

Step 2: Define a local administrative username.

```
username admin password c1sco123 privilege 15
```

Step 3: Set the enable password.

```
enable password c1sco123
```

Step 4: Define the management configuration.

```
http server enable
http 10.0.0.0 255.0.0.0 inside
ssh 10.0.0.0 255.0.0.0 inside
management-access inside
```

Step 5: If you are using centralized AAA, define authentication servers for management access.

```
aaa-server AAA-SERVERS protocol tacacs+
aaa-server AAA-SERVERS (inside) host 10.4.48.15
 key SecretKey
aaa authentication http console AAA-SERVERS LOCAL
aaa authentication ssh console AAA-SERVERS LOCAL
```

Procedure 3 Configure outside VLAN and switch port

Step 1: Configure a VLAN interface to receive an IP address via DHCP from the teleworker's Internet gateway device.

```
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp setroute
```

Step 2: Associate the Cisco ASA 5505's Ethernet 0/0 interface with VLAN 2, and instruct the teleworker to connect Ethernet 0/0 to their Internet gateway device.

```
interface Ethernet0/0
 switchport access vlan 2
 no shutdown
```

Procedure 4 Configure Cisco ASA 5505 DHCP server

The Cisco ASA 5505 must be configured to provide IP-addresses for the teleworker endpoints, such as computers, phones, printers, and video surveillance devices. Each site must use a unique subnet, which should be tracked in a spreadsheet, as recommended in the introduction of this section.

Step 1: Define the DHCP scope address range. The DHCP scope must be in the same subnet as the inside (VLAN 1) interface.

```
dhcpd address 10.4.156.2-10.4.156.6 inside
```

Step 2: Configure the DNS and domain-name values that will be distributed to clients.

```
dhcpd dns 10.4.48.10 interface inside
dhcpd domain cisco.local interface inside
```

Step 3: Define DHCP option 150 to provide the Cisco Unified Call Manager Server address for Cisco IP phones.

```
dhcpd option 150 ip 10.4.48.120
```

Step 4: Enable the DHCP scope.

```
dhcpd enable inside
```

Procedure 5 Configure Cisco ASA 5505 Easy VPN client

Cisco ASA 5505 uses Easy VPN network-extension mode to negotiate the VPN connectivity to the Internet-edge Cisco ASA Remote Access server.

Step 1: Apply the Easy VPN client configuration for the remote Cisco ASA 5505: The vpngroup and password values must match the IPsec Remote Access Connection Profile that you configured on the Internet-edge appliance.

```
vpnclient server 172.16.130.122
```

Step 2: Set network-extension mode:

```
vpnclient mode network-extension-mode
```

Step 3: Define the Easy VPN client connection attributes. The vpngroup and password values must match the IPsec Remote Access Connection Profile that you configured on the Internet-edge appliance.

```
vpnclient vpngroup Teleworker5505 password cisco123
```

Step 4: Enable the Cisco ASA 5505's Easy VPN client:

```
vpnclient enable
```

The teleworker must manually initiate their VPN connection; when the user employs a web browser to access web content on your internal network, Cisco ASA 5505 intercepts the connection and provides an interactive login prompt. The user must provide login credentials, at which point the VPN connection is negotiated with the provided username and password.

Tech Tip

The IP Phone connected to the Cisco ASA 5505 can't place or receive calls if the user's VPN connection is not active.

In the event that a teleworker's VPN access must be revoked, the authentication server should deny the teleworker's access.

Appendix A: Product List

Remote-Site

Functional Area	Product Description	Part Numbers	Software
Remote Site Appliance	Cisco ASA 5505 Firewall Edition Bundle security appliance	ASA5505-BUN-K9	ASA 9.0(1)

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)

Appendix B: Configuration Files

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 asdm-websecproxy-115-111-223-66
 host 115.111.223.66
object network asdm-websecproxy-122-50-127-66
 host 122.50.127.66
object network asdm-websecproxy-184-150-236-66
 host 184.150.236.66
```

```
object network asdm-websecproxy-196-26-220-66
 host 196.26.220.66
object network asdm-websecproxy-201-94-155-66
 host 201.94.155.66
object network asdm-websecproxy-202-167-250-90
 host 202.167.250.90
object network asdm-websecproxy-202-167-250-98
 host 202.167.250.98
object network asdm-websecproxy-202-177-218-66
 host 202.177.218.66
object network asdm-websecproxy-202-79-203-98
 host 202.79.203.98
object network asdm-websecproxy-46-255-40-58
 host 46.255.40.58
object network asdm-websecproxy-46-255-40-90
 host 46.255.40.90
object network asdm-websecproxy-46-255-40-98
 host 46.255.40.98
object network asdm-websecproxy-69-10-152-66
 host 69.10.152.66
object network asdm-websecproxy-69-174-58-179
 host 69.174.58.179
object network asdm-websecproxy-69-174-58-187
 host 69.174.58.187
object network asdm-websecproxy-69-174-87-131
 host 69.174.87.131
object network asdm-websecproxy-69-174-87-163
 host 69.174.87.163
object network asdm-websecproxy-69-174-87-171
 host 69.174.87.171
object network asdm-websecproxy-69-174-87-75
 host 69.174.87.75
object network asdm-websecproxy-70-39-176-115
 host 70.39.176.115
object network asdm-websecproxy-70-39-176-123
 host 70.39.176.123
object network asdm-websecproxy-70-39-176-131
 host 70.39.176.131
object network asdm-websecproxy-70-39-176-139
 host 70.39.176.139
object network asdm-websecproxy-70-39-176-35
 host 70.39.176.35
object network asdm-websecproxy-70-39-176-59
 host 70.39.176.59
object network asdm-websecproxy-70-39-177-35
 host 70.39.177.35
object network asdm-websecproxy-70-39-177-43
```

```
 host 70.39.177.43
object network asdm-websecproxy-70-39-231-107
 host 70.39.231.107
object network asdm-websecproxy-70-39-231-163
 host 70.39.231.163
object network asdm-websecproxy-70-39-231-171
 host 70.39.231.171
object network asdm-websecproxy-70-39-231-180
 host 70.39.231.180
object network asdm-websecproxy-70-39-231-182
 host 70.39.231.182
object network asdm-websecproxy-70-39-231-188
 host 70.39.231.188
object network asdm-websecproxy-70-39-231-190
 host 70.39.231.190
object network asdm-websecproxy-70-39-231-91
 host 70.39.231.91
object network asdm-websecproxy-72-37-244-163
 host 72.37.244.163
object network asdm-websecproxy-72-37-244-171
 host 72.37.244.171
object network asdm-websecproxy-72-37-248-19
 host 72.37.248.19
object network asdm-websecproxy-72-37-248-27
 host 72.37.248.27
object network asdm-websecproxy-72-37-249-139
 host 72.37.249.139
object network asdm-websecproxy-72-37-249-147
 host 72.37.249.147
object network asdm-websecproxy-72-37-249-163
 host 72.37.249.163
object network asdm-websecproxy-72-37-249-171
 host 72.37.249.171
object network asdm-websecproxy-72-37-249-195
 host 72.37.249.195
object network asdm-websecproxy-72-37-249-203
 host 72.37.249.203
object network asdm-websecproxy-80-254-147-251
 host 80.254.147.251
object network asdm-websecproxy-80-254-148-194
 host 80.254.148.194
object network asdm-websecproxy-80-254-150-66
 host 80.254.150.66
object network asdm-websecproxy-80-254-154-66
 host 80.254.154.66
object network asdm-websecproxy-80-254-154-98
 host 80.254.154.98
```

```
object network asdm-websecproxy-80-254-155-66
 host 80.254.155.66
object network asdm-websecproxy-80-254-158-147
 host 80.254.158.147
object network asdm-websecproxy-80-254-158-155
 host 80.254.158.155
object network asdm-websecproxy-80-254-158-179
 host 80.254.158.179
object network asdm-websecproxy-80-254-158-187
 host 80.254.158.187
object network asdm-websecproxy-80-254-158-211
 host 80.254.158.211
object network asdm-websecproxy-80-254-158-219
 host 80.254.158.219
object network asdm-websecproxy-80-254-158-35
 host 80.254.158.35
object network 5505-pool
 subnet 10.4.156.0 255.255.252.0
 description 5505 Teleworker Subnet
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
access-list Block_Trusted_Host remark Trusted Host is 10.4.48.10:443
access-list Block_Trusted_Host extended deny tcp any4 host 10.4.48.10 eq https
access-list Block_Trusted_Host remark Permit All other traffic
access-list Block_Trusted_Host extended permit ip any4 any4
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-35
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-147-251
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-155
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-147
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
```

```
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-179
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-187
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-211
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-219
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-148-194
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-46-255-40-58
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-46-255-40-90
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-46-255-40-98
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-150-66
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-154-66
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-154-98
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-155-66
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-196-26-220-66
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-201-94-155-66
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-184-150-236-66
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-69-10-152-66
any
```

```
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-244-171
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-244-163
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-248-19
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-248-27
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-231-107
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-231-91
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-231-171
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-231-163
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-231-180
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-231-182
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-231-188
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-231-190
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-69-174-58-179
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-69-174-58-187
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-176-35
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-176-59
```

```
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-176-115
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-176-123
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-176-131
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-176-139
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-249-171
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-249-163
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-249-139
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-249-147
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-249-195
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-72-37-249-203
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-177-35
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-70-39-177-43
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-69-174-87-75
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-69-174-87-171
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-69-174-87-131
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
```

```
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-69-174-87-163
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-202-167-250-98
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-202-167-250-90
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-115-111-223-66
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-122-50-127-66
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-202-79-203-98
any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-202-177-218-66
any
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 *****
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
```

```
nat (any,any) source static internal-network internal-network destination static 5505-
pool 5505-pool
!
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 *****
aaa-server AAA-RADIUS protocol radius
aaa-server AAA-RADIUS (inside) host 10.4.48.15
 timeout 5
 key *****
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 *****
no snmp-server location
no snmp-server contact
snmp-server community *****
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 profiles RA-WebSecurityProfile disk0:/ra-websecurityprofile.wsp
 anyconnect profiles RA-WebSecurityProfile.wso disk0:/ra-websecurityprofile.wso
 anyconnect enable
 tunnel-group-list enable
group-policy 5505Group internal
group-policy 5505Group attributes
 vpn-tunnel-protocol ikev1
 password-storage disable
 split-tunnel-policy tunnelall
 secure-unit-authentication enable
 nem 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
tunnel-group Teleworker5505 type remote-access
tunnel-group Teleworker5505 general-attributes
 authentication-server-group AAA-RADIUS
 default-group-policy 5505Group
 password-management
tunnel-group Teleworker5505 ipsec-attributes
 ikev1 pre-shared-key *****
!
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
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/
DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly 5
  subscribe-to-alert-group configuration periodic monthly 5
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:7936c448b290d65f547923128c37a76c
: end
asdm image disk0:/asdm-702.bin
no asdm history enable
```

ASA-5505

```
ASA Version 9.0(1)
!
hostname 5505site2
```

```
domain-name cisco.local
enable password 2y4FIGBVVyBLau0Q encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
 shutdown
!
interface Ethernet0/3
 shutdown
!
interface Ethernet0/4
 shutdown
!
interface Ethernet0/5
 shutdown
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 10.4.157.1 255.255.255.248
!
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp setroute
!
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.local
```

```
pager lines 24
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
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-SERVERS protocol tacacs+
aaa-server AAA-SERVERS (inside) host 10.4.48.15
 key *****
user-identity default-domain LOCAL
aaa authentication http console AAA-SERVERS LOCAL
aaa authentication ssh console AAA-SERVERS LOCAL
http server enable
http 10.0.0.0 255.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
crypto ikev1 policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh 10.0.0.0 255.0.0.0 inside
ssh timeout 5
console timeout 0
management-access inside
vpnclient server 172.16.130.122
vpnclient mode network-extension-mode
vpnclient vpngroup Teleworker5505 password *****
vpnclient enable
dhcpd option 150 ip 10.4.48.120
!
dhcpd address 10.4.157.2-10.4.157.6 inside
```

```
dhcpd dns 10.4.48.10 interface inside
dhcpd domain cisco.local interface inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
username admin password w2Y.6Op4j7clVDk2 encrypted privilege 15
!
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
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/
DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
```

```
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:8ccf9a34bff8f08e83dfb2894a0e0873
: 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-0000300-1 08/13