Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

SBA

Secure Remote Mobile Access Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2012 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2011 are the "August 2011 Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). 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 shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

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

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

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 forum at the bottom of one of the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

An RSS feed is available if you would like to be notified when new comments are posted.

Table of Contents

What's In This SBA Guide

About SBA

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

For more information, see the *How to Get Started with Cisco SBA* document:

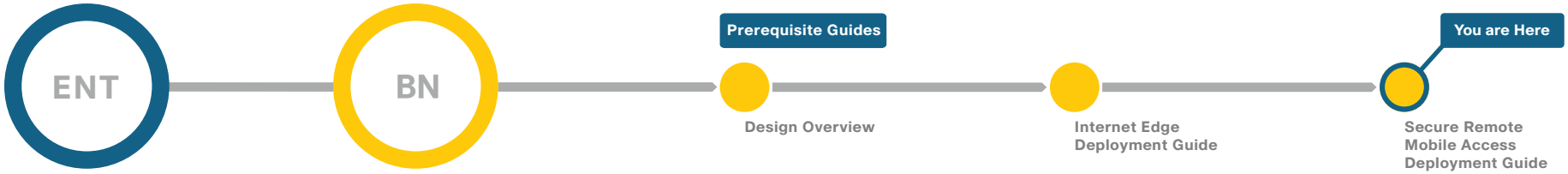
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf

About This Guide

This *additional deployment guide* includes the following sections:

- Business Overview—The challenge that your organization faces. Business decision makers can use this section to understand the relevance of the solution to their organizations' operations.
- Technology Overview—How Cisco solves the challenge. Technical decision makers can use this section to understand how the solution works.
- Deployment Details—Step-by-step instructions for implementing the solution. Systems engineers can use this section to get the solution up and running quickly and reliably.

This guide presumes that you have read the prerequisites guides, as shown on the Route to Success below.



Route to Success

To ensure your success when implementing the designs in this guide, you should read any guides that this guide depends upon—shown to the left of this guide on the route above. Any guides that depend upon this guide are shown to the right of this guide.

For customer access to all SBA guides: http://www.cisco.com/go/sba
For partner access: http://www.cisco.com/go/sbachannel

Introduction

One of the most profound advances in modern networks is the degree of mobility those networks support. Users can move around wirelessly inside the campus and enjoy the same degree of connectivity as if they were plugged in using cables in their offices. Users can leave their primary networks completely and work from a home office environment that offers the same connectivity and user experience as they would get in their offices. Users also have the option of being truly mobile and connecting from any place that offers Internet access. With smartphones and tablets, this mobility now commonly includes connecting while travelling down the highway or on a train. This guide describes business-use cases related to the truly mobile users who connect through infrastructure that is not provided by their organizations by using a laptop, smartphone, or tablet device. The guide does not cover use cases related to campus wireless access or home teleworker solutions.

Business Overview

As users move outside the boundaries of the traditional network, their requirements for access to job-related data, such as email, calendars, and more, don't change. To be productive, the network needs to allow users access wherever they are to whatever data they need to accomplish their tasks, from any device the organization allows. At the same time, the network must ensure that all access is secure and appropriate and that it follows organizational guidelines.

Mobile remote users connect using devices that can generally be broken down into two categories: laptop computers and the new group of mobile devices, such as smartphones and tablets. Networks have handled laptops for years. The newer mobile devices are being integrated currently. This integration continues to challenge network design and administration.

An organization's network must meet many requirements today that are sometimes contradictory. The network must be secure and prevent unauthorized access while being open enough to allow users to do their jobs regardless of where they are. As the mobility of users has increased, the requirements the network must meet have increased. In the past, a worker might have needed laptop connectivity while at the office or at home. Today, a worker needs access to the network from a smartphone while traveling, from a laptop while on site at a customer's or partner's office, or from both while sitting in the local coffee shop. And although providing this access is the primary requirement for the network, other requirements, such as ease of use and security, have not been relaxed.

Because these mobile users are outside the traditional perimeter (or physical border) of the network, their devices are exposed to potentially more malicious activity than a device that is located inside the protection of the network. So protection of the end device and the data being accessed and stored is critical. The mobile user's device needs to have protection from things such as malware and viruses. Ideally, this protection occurs even if the device is not connected to the headquarters' network or if such a connection isn't possible. Because many mobile devices are smaller and are used much more often than a laptop, they are also more easily lost or stolen. In today's security environment where these devices potentially carry the same information that a laptop might, there is a need to protect the data on those devices and prevent unauthorized users from retrieving it.

As a standard part of their processes and guidelines, many organizations are required to control what sites users access on the Internet while they are using organizational resources. Providing this level of control for mobile users who do not reside within the boundaries of the network is challenging. To provide a complete solution, the network enforces standard access guidelines on the device, whether the device resides inside the headquarters or is connecting from a coffee shop. The end users should have similar experiences inside or outside the traditional network perimeter. They should also receive the same protection from malware whether they are inside the network or outside.

An often overlooked component of access is ease of use. Having to check whether a secure connection is needed and enabled and having to constantly enter user credentials on a mobile device to enable a secure connection might make users look for ways to bypass the solution. Thus, a solution that is as integrated and seamless as possible means it doesn't impact users, hamper their day-to-day activities, or reduce their productivity as significantly. As part of ease of use, the solution should be automated as much as the platform allows, preventing users from either forgetting to follow the procedure or specifically trying to bypass procedures because they feel the procedures are restrictive.

As more users move outside the boundaries of the network, a corresponding increase in network load occurs on the organization's Internet connection. This can raise costs. Intelligent routing of traffic is a priority to control which traffic from a user has to go through the Internet Edge component of the organization's network and which traffic can be kept out on the Internet.

Reducing security on this traffic is not an option that is readily available. Traffic destined for the Internet that has to be brought back to the Internet Edge for security inspection increases bandwidth usage and load on the Internet Edge design while increasing latency on user connections.

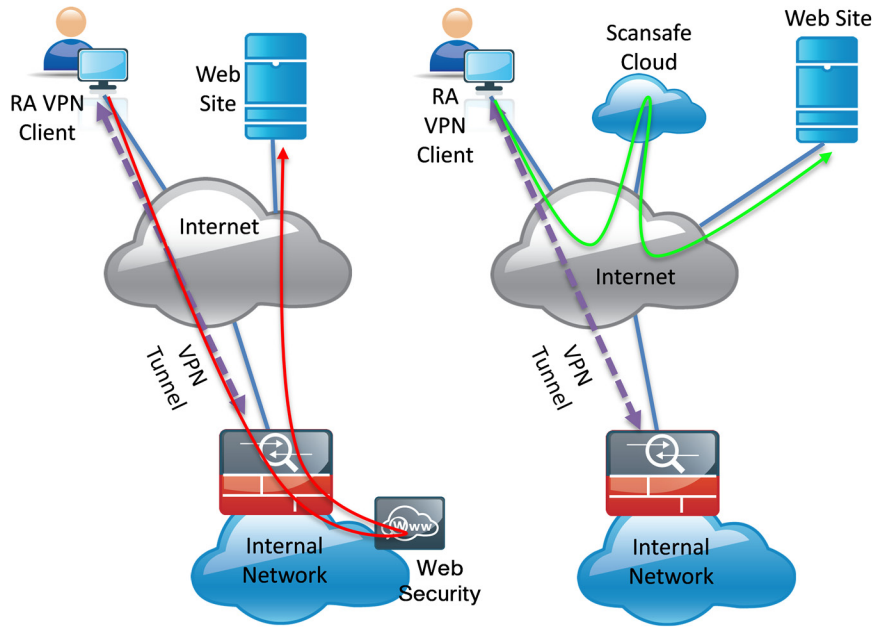
Technology Overview

The Cisco® Smart Business Architecture Enterprise Internet Edge design provides the basic framework for the enhancements and additions that will be discussed in this guide.

Mobile remote users connect to their organization's network by using devices that generally fall into two categories: laptops and mobile devices such as smartphones and tablets. Because the devices operate and are used differently, the capabilities currently available for each group differ.

The Internet Edge design for the enterprise architecture covers remote access (RA) VPN for laptops running the Cisco AnyConnect Secure Mobility Solution client (for SSL VPN or IP security [IPsec] connections). A feature built into the Cisco AnyConnect 3.0 client is the ability to interface with the Cisco ScanSafe Cloud Web Security service. This feature gives the Cisco AnyConnect client the ability to let Internet web traffic go out through a Cisco ScanSafe proxy directly to the destination without forcing it through the organization's head end. Without Cisco ScanSafe, the traffic must be routed down the VPN tunnel, inspected at the campus Internet edge, and then redirected to the original destination; this process consumes bandwidth and potentially increases user latency. With Cisco ScanSafe, the connection can be proxied through the Cisco ScanSafe cloud and never has to traverse the VPN tunnel.

Figure 1 - Traffic flow through VPN tunnel and Cisco ScanSafe Cloud



Other capabilities for the Cisco AnyConnect 3.0 client include features that allow the client to reconnect if the tunnel goes down, to disable the tunnel if the client moves onto the trusted network, or to bring up the tunnel if the client moves from a trusted to an untrusted network. These features make using the client more seamless and friendly because users don't have to manually bring up the VPN tunnel. Users are prompted for credentials when the tunnel is needed, and the tunnel is brought down when it isn't needed.

Mobile devices typically use a different deployment model in which basic services, such as mail, calendar, and contacts, are provided over Microsoft ActiveSync, which gives quick access to these commonly used services. For access to other services, including voice, video, internally hosted web servers, file shares, or other network services, a VPN tunnel is required.

Mobile devices such as the iPhone and iPad and some Android devices have access to the Cisco AnyConnect 2.5 client, which allows SSL VPN connectivity (check the app store for the device in question for availability). Using Cisco AnyConnect to connect the device to the corporate network provides full access to the internal network.

This document covers the additional configuration for remote access VPN for the Cisco AnyConnect 3.0 client that is required to activate Cisco ScanSafe Web Security, Always On, and other features. It also covers interaction with the Cisco ScanSafe Cloud management tool, ScanCenter. Last, the document covers configuration of Cisco Adaptive Security Appliance (ASA) to support mobile devices like smartphones and tablets and the configuration of the Cisco AnyConnect client for those devices that is required to let them connect to Cisco ASA.

Notes

Deployment Details

The first part of the deployment details describes how to configure the components to enable Cisco ScanSafe Cloud Web Security service for Cisco AnyConnect 3.0 users that connect with laptop devices. The second part of the deployment details describes how to configure access for mobile devices with ActiveSync. The third part describes how to configure access for mobile devices with the Cisco AnyConnect client.

Process

Configuring Access for Laptop Devices

1. Enable ScanSafe Security Configuration
2. Configure the Beacon Server on LAN
3. Configure ASA VPN Policy for Web Security
4. Configure ASA AnyConnect Group Policies
5. Test the Current Configuration
6. Test Beacon Server Functionality
7. Configure Trusted Network Detection
8. Test Trusted Network Detection
9. Install the Certificate on the Client
10. Enable Always On
11. Test the Always On Setting

Procedure 1 Enable ScanSafe Security Configuration

This guide assumes you have purchased a Cisco ScanSafe license and created a Cisco ScanSafe account that allows a user to log on and administer the account.

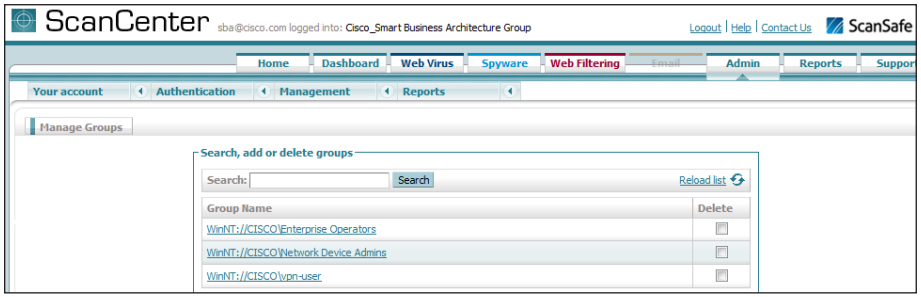
Step 1: In the Cisco ScanSafe ScanCenter Portal, after logging on with administrator rights, navigate to the following location:

https://scancenter.scansafe.com

Step 2: Navigate to **Admin** > **Management** > **Groups**.

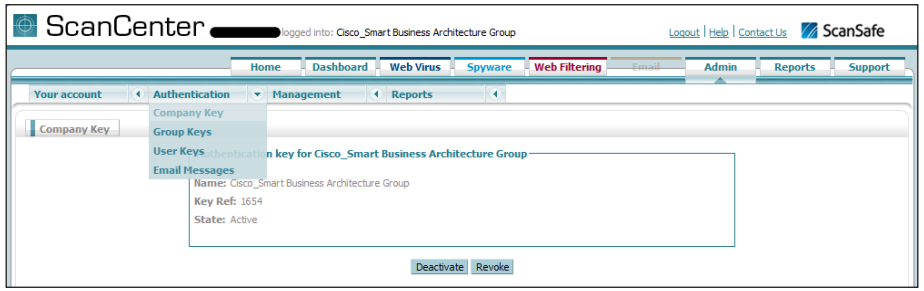
Tech Tip

Policy can differ based on organizational requirements. Windows Active Directory (AD) groups are the default method of applying policy in Cisco ScanSafe. Administrators will define one or more AD groups in the ScanCenter tool to which users belong. Policy can then be applied to one of the defined groups or the default group, which consists of users not in one of the defined groups.



A company-wide proxy authentication license key is generated for use in the Cisco ASA VPN configuration.

Step 3: Navigate to **Authentication** > **Company Key.**



Step 4: Click **Create Key**. Cisco ScanSafe generates a key that it sends to an email address of your choosing.

Write this key down because it cannot be rebuilt and can only be replaced with a new key. After it is displayed the first time (on generation) and emailed, you can no longer view it in ScanCenter. After this key is generated, the page options change to **Deactivate** or **Revoke**.

Step 5: Navigate to **Web Filtering** > **Management** > **Filters**.

Step 6: Edit the filter called **default** to reference the Pornography, Sports and Recreation, and Gambling categories, and then click **Save**.

Step 7: Create a new filter called **VPN_Users** that references the Sports and Recreation category, and then click **Save**.

Step 8: Create a filter called **Admins** that references Sports, and then click **Save**.

Step 9: **Navigate to Management** > **Policy**.

Step 10: Click **Default**, change the rule action to **Permit**, and then click **Save.**

Step 11: Create a rule called **All_Users** with a rule action of **Block**. Assign the filter **default** to this rule to block all access to porn, gambling, or sports sites.

Step 12: Create a rule called **VPN_Users** with a rule action of **WARN**.

Step 13: Under **Define Group**, select the **vpn-user** domain group.

Step 14: Under **Define Filters**, select **VPN_Users**, and then click **Create Rule.**

Step 15: Create a rule called **Admins** with a rule action of **Allow**.

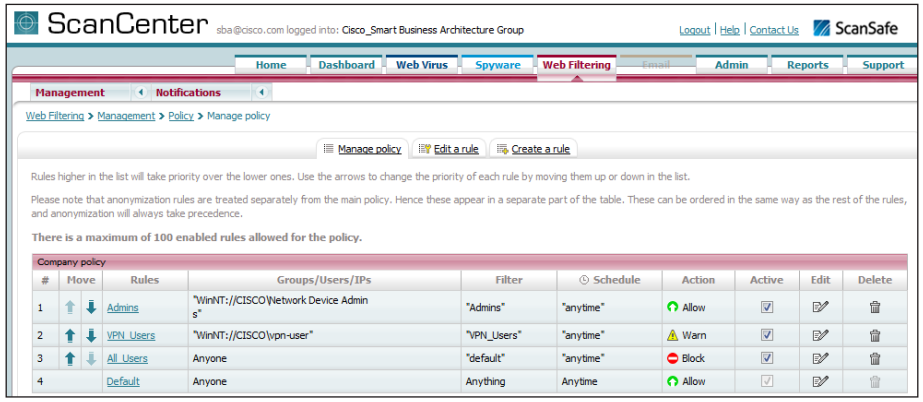
Step 16: Under **Define Group**, select the **Network Device Admin** domain group.

Step 17: Under **Define Filters**, select **Admins**, and then click **Create Rule.**

Step 18: Click **Active** on all rules, and then click **Apply Changes.**

Because all rules are evaluated on a first-hit rule, the following is the correct order for the rules in this example:

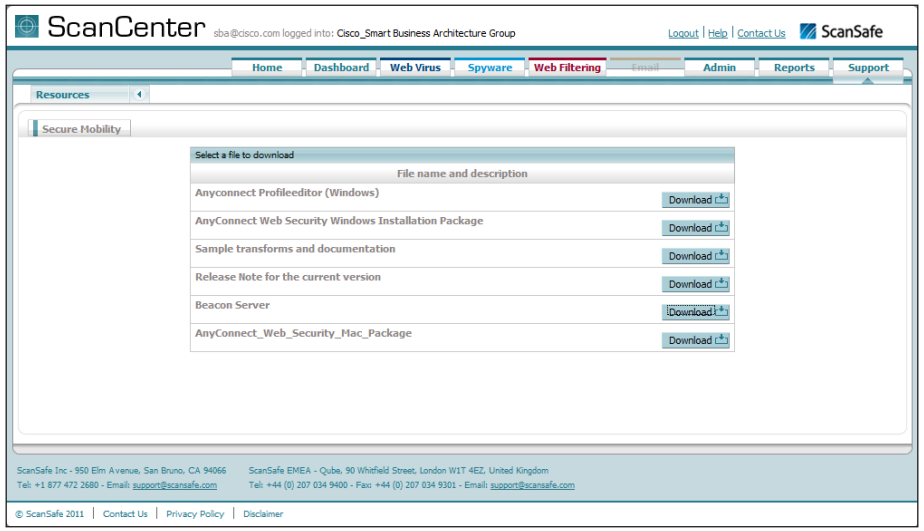
1. Admins (which allows anyone matching this rule access to sports sites)
2. VPN_Users (which allows this group access to sports sites but with a warning)
3. All_Users (which blocks sports, gambling, and pornography sites)
4. Default (which permits all other sites to all groups)



Procedure 2 Configure the Beacon Server on LAN

In this procedure, you install and configure the Beacon Server software on a server in the inside network. This server should be accessible from anywhere in the network. Access to this server will tell the Cisco AnyConnect client that it currently resides inside the network and that the Web Security module does not need to run. You will configure the Beacon server to not accept connections from hosts with specific IP addresses where you wish the Web Security module to always run (for example, when the host is connected from outside the network through RA VPN and is assigned an address from the RA VPN Pool).

Step 1: On an internal server that is reachable from anywhere in the organization, while browsing to the Cisco ScanSafe ScanCenter, navigate to **Support** > **Resources** > **Secure Mobility**.



Step 2: Select the **Beacon Server** package, and then click **Download**.

Step 3: Expand the downloaded package by using a .zip program. Inside the package, you will find OpenSSL.

Step 4: In the folder containing the openssl.exe program, from a command prompt on the Windows server, type the following:

```
openssl genrsa -out DOLprv.pem 1024
openssl rsa -in DOLprv.pem -out DOLpub.pem -outform PEM
-pubout
```

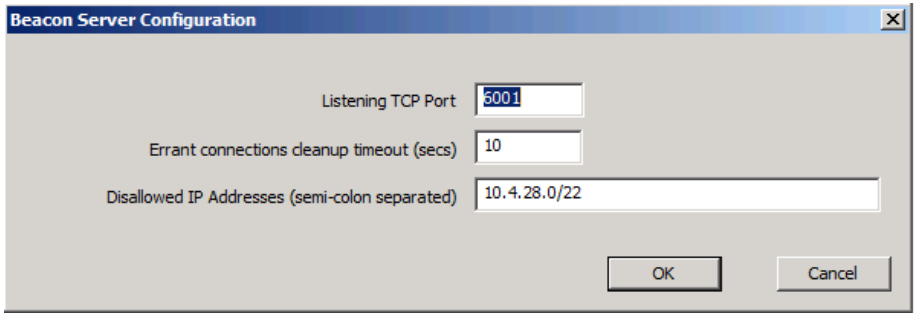
Step 5: Copy the DOLprv.pem file to the folder containing the BeaconServer.msi file.

Step 6: Copy the DOLpub.pem file to the device running Cisco Adaptive Security Device Manager (ASDM).

Step 7: In the package, in the **Beacon Server** directory, double-click the Beacon Server.msi file.

Step 8: Right-click the Windows Taskbar icon, and set preferences for Beacon Server.

Step 9: In the **Disallowed IP Addresses** box, enter the addresses used for remote access VPN.

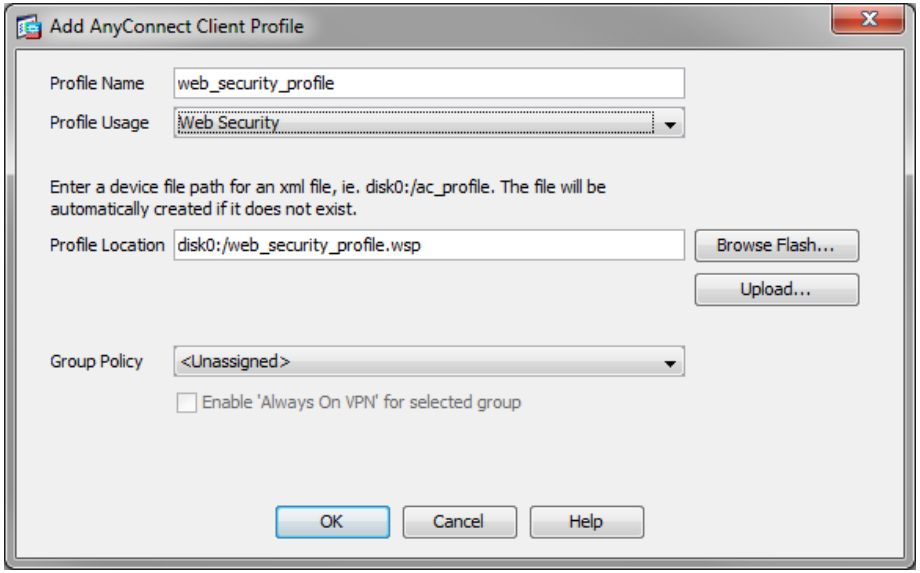


Procedure 3 Configure ASA VPN Policy for Web Security

Step 1: Open ASDM connected to the RA VPN firewall.

Step 2: In **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profiles**, select **Add**.

Step 3: In the **Add AnyConnect Client Profile** dialog box, fill in the **Profile Name** web_security_profile, select **Web Security** in the **Profile Usage** list, and then click **OK.**



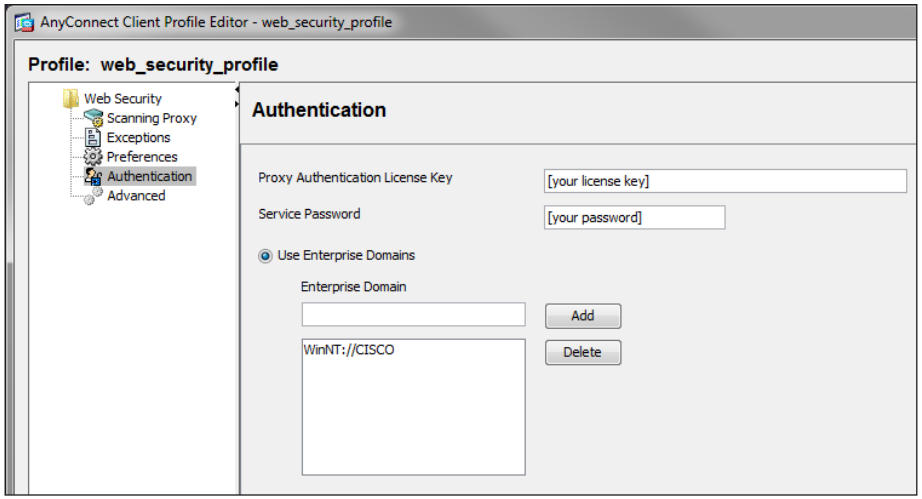
Step 4: Select the newly created web_security_profile profile, and then click **Edit**.

Step 5: In the **Scanning Proxy** section, write down the IP addresses of the different proxies. Depending on where you connect from, you can also change your **Default Scanning Proxy** selection to match your location better. This drop-down list contains numerous proxy locations that you can choose as the default.

Step 6: Under **Authentication**, in the **Proxy Authentication License Key** box, enter the key for your company-wide group.

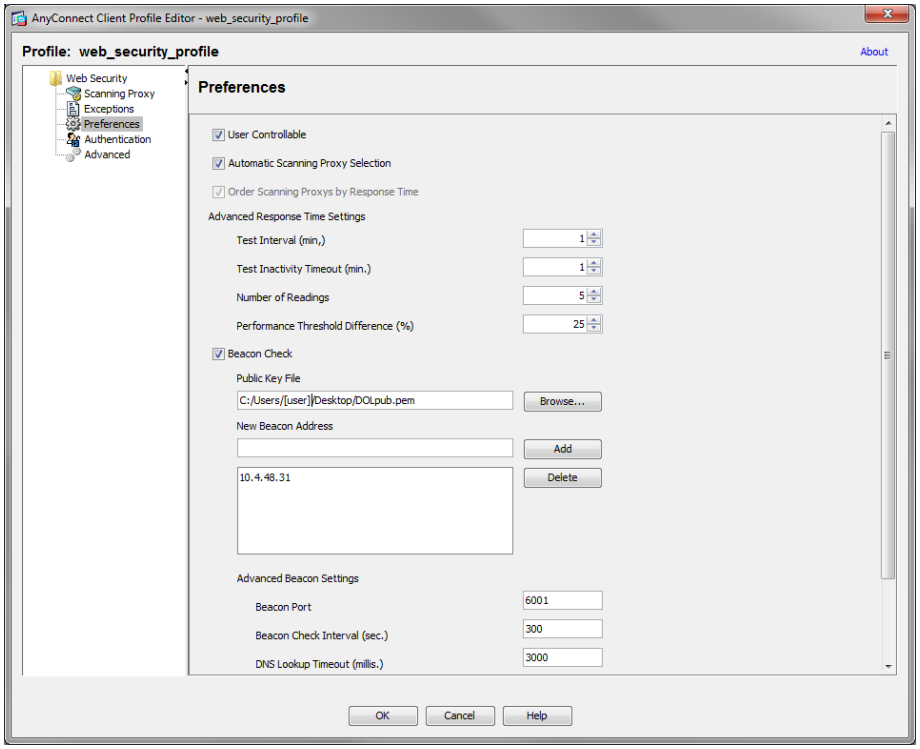
Step 7: In the **Service Password** box, enter a new password that will be associated with the web security service when the service is running on the end host.

Step 8: In the **Use Enterprise Domains box**, enter the domain information to which you wish to apply policy.



Step 9: From the **Web Security** menu, choose **Preferences**, and then do the following:

1. If your organization allows users to control use of web security functions, select **User Controllable**.
2. Select **Automatic Scanning Proxy Selection**.
3. Select **Beacon Check**.
4. Select **Browse** for the **Public Key File,** and then navigate to the public key file you copied in Procedure 2 Configure the Beacon Server on LAN above (DOLpub.pem).
5. In the **Beacon Address** field, enter the address of the server on which the Beacon software was installed.



Step 10: Click **OK,** and then apply the configuration to Cisco ASA.

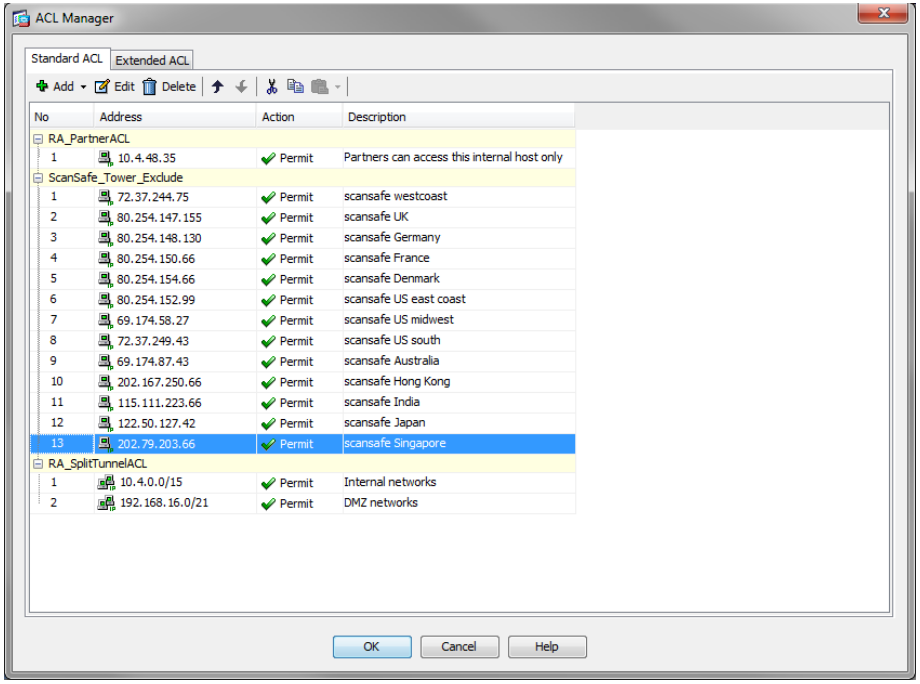
Notes

Procedure 4 Configure ASA AnyConnect Group Policies

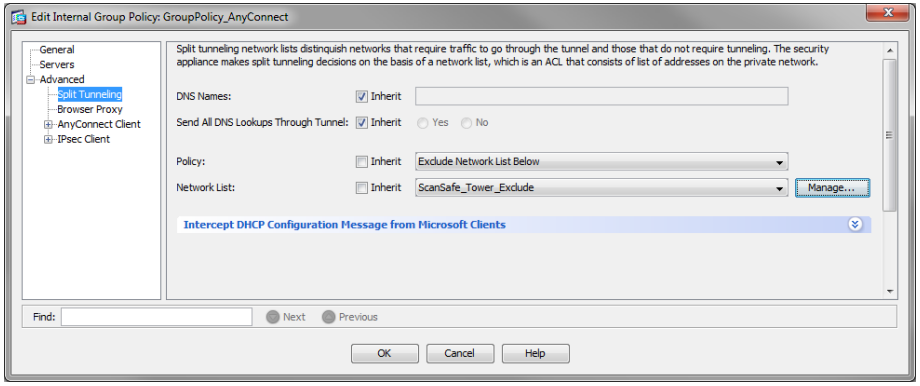
Step 1: In ASDM, navigate to **Configuration > Remote Access VPN > Network Client Access > Group Policies**, select the GroupPolicy_AnyConnect policy, and then click **Edit**.

Step 2: Under **Advanced**, select **Split Tunneling**.

1. Next to **Policy**, clear the **Inherit check box,** and then choose **Exclude Network List Below**.
2. Next to **Network List**, clear the **Inherit check box,** and then click **Manage**.
3. In **ACL Manager**, click **Add,** and then select **Add ACL**. Use Scansafe_Tower_Exclude for the ACL name.
4. Select the ACL you just created, and then click **Add > Add ACE**.
5. For the address, add in each Cisco ScanSafe Scanning Proxy address from Step 5 of Procedure 3 Configure ASA VPN Policy for Web Security above into its own Access Control Entry (ACE), and then click **OK**. This step configures the Cisco AnyConnect client to allow split tunneled traffic destined to each of the Cisco ScanSafe proxy addresses. All other traffic is sent down the VPN tunnel to the main site.



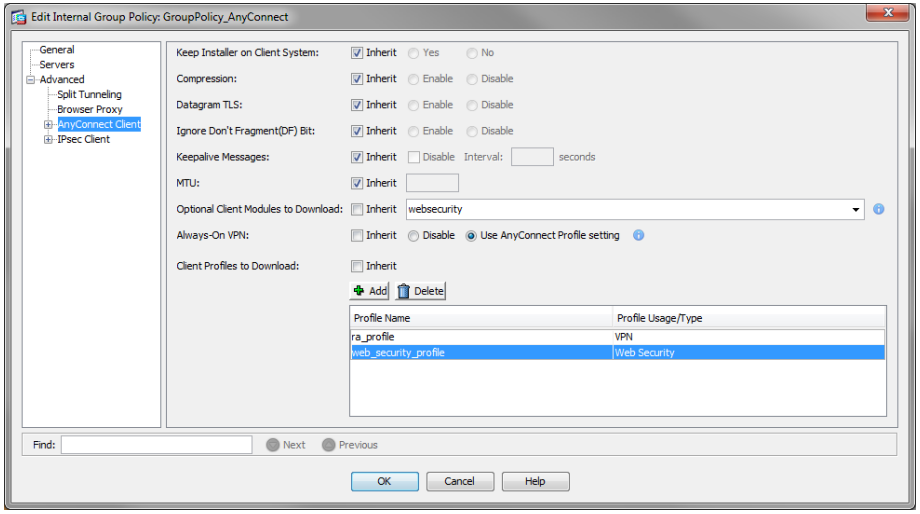
Step 3: In the **Edit Internal Group Policy** dialog box, navigate to **Advanced > Split Tunneling,** and then, in the **Network List list**, choose **Scansafe_Tower_Exclude**.



Step 4: Navigate to **Advanced** > **AnyConnect Client**. Under **Optional Client Modules to Download**, clear the **Inherit check box,** choose **websecurity** from the list, and then click **OK**.

Step 5: In the **Always on VPN** section, clear the **Inherit** check box, and then choose **Use AnyConnect Profile setting**.

Step 6: In the **Client Profiles to Download section**, click **Add**, select the **web_security_profile** profile, and then click **OK**.

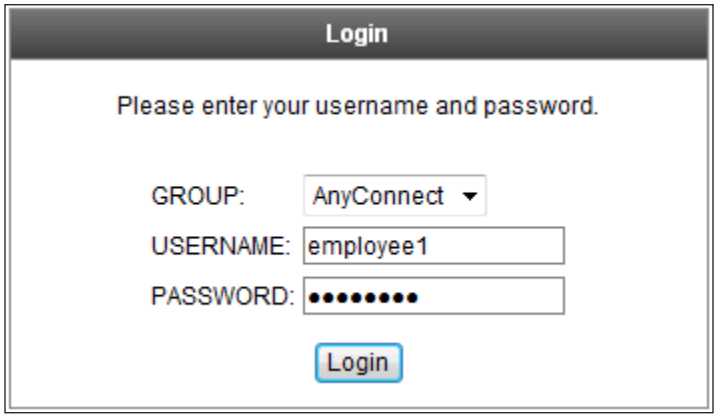


Step 7: Click **OK**, and then apply changes.

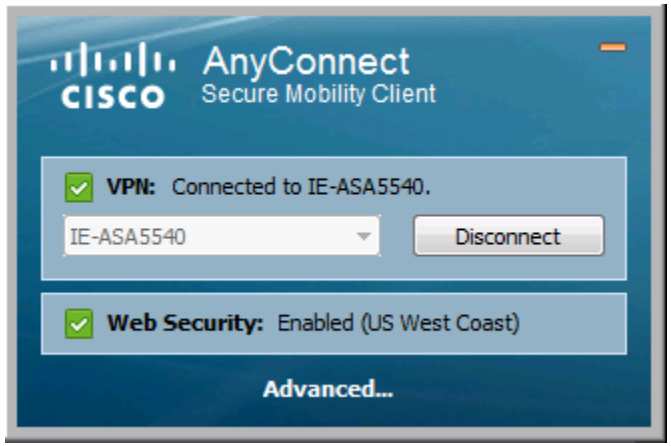
Procedure 5 Test the Current Configuration

Step 1: Open a browser on a client, and then navigate to the following outside IP address of the RA VPN ASA: https://ie-asa5540.cisco.local

Step 2: Log on using a known username and password that is part of the vpn-user group in Windows AD. If Cisco AnyConnect 3.0 is not installed, the client downloads and installs it.

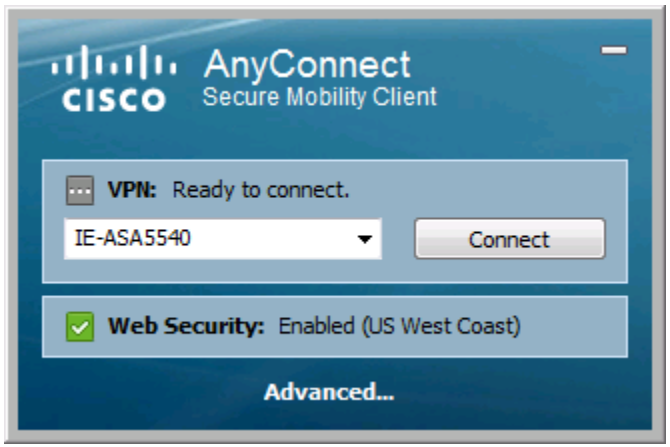


Step 3: When connected, click the Cisco AnyConnect taskbar icon to bring up the client information panel.



Step 4: Verify there is a green check box next to both VPN and Web Security.

Step 5: Click **Disconnect**, and then verify that Web Security remains enabled.



Procedure 6 Test Beacon Server Functionality

Step 1: Move a client that is connected outside the network and has the Web Security module enabled inside the network.

When the client is inside, it should be getting a DHCP address that is not part of the address space defined in the Beacon Server configuration. The client can now make a connection to the Beacon Server. The ability to connect to the Beacon Server successfully tells the Cisco AnyConnect client that the client is inside and that the Web Security Module should not be run because the client is on a trusted network. The host's web connections to external web sites are now secured by the organization's Internet Edge devices and policy.

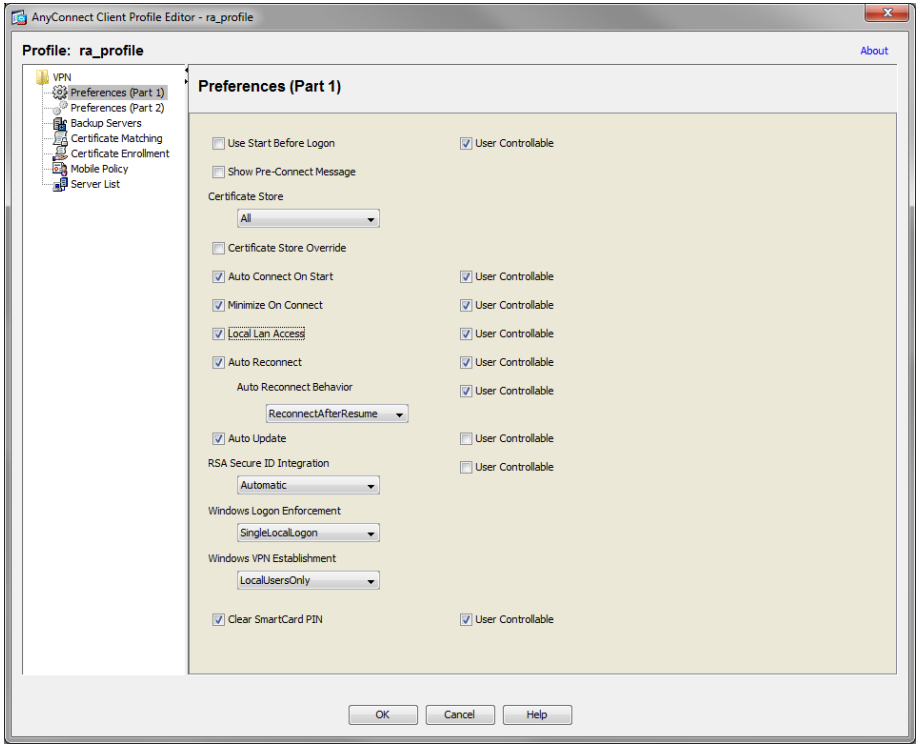
Procedure 7 Configure Trusted Network Detection

The Always On setting allows an administrator to enforce that if a laptop is outside the network and has connectivity, a VPN connection to the head end occurs and all connections go through the main site, where security policy can be applied. If the device cannot connect to the VPN, then no connections will be allowed.

If policy enforcement is not the end-use case, but instead ease of use is the end goal, then enabling the **Auto Connect on Start, Auto Reconnect**, and **Automatic VPN Policy** features that define a trusted network satisfy many requirements without applying strict enforcement that the VPN tunnel be up at all times if network access to Cisco ASA is available. Enabling these features makes access to the internal network more seamless to the end user and presents less opportunity for the end user to forget to bring up their VPN tunnel while working remotely or to attempt to bring up the VPN tunnel while on the internal network.

Step 1: Navigate to **ASDM > Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**, select **ra_profile,** and then click **Edit**.

Step 2: In **Preferences (Part 1)**, select the **Auto Connect on Start** and **Auto Reconnect check boxes**, and, if policy permits, select the **User Controllable check boxes**. In the **Auto Reconnect Behavior** list, ensure **ReconnectAfterResume** is chosen.

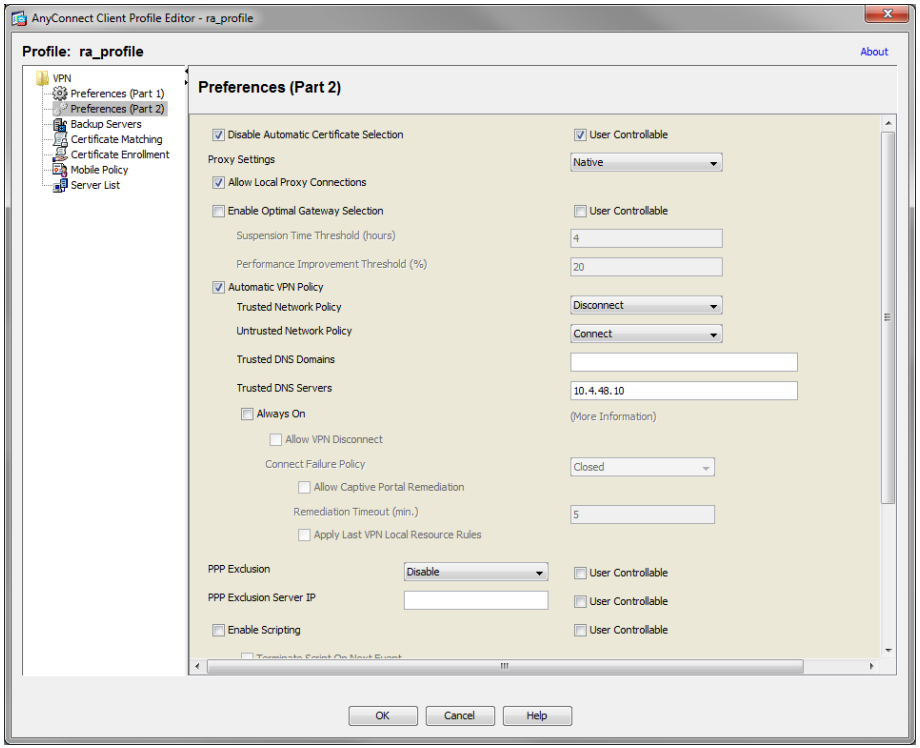


Step 3: In **Preferences (Part 2)**, select the **Automatic VPN policy check box**.

Step 4: In the **Trusted Network Policy** list, choose **Disconnect,** and, in the **Untrusted Network Policy** list, choose **Connect**.

Step 5: In the **Trusted DNS Servers** box, enter the IP address of the internal DNS server that should be accessible from anywhere in the internal network: 10.4.48.10.

To identify whether a device is on the trusted network, before a VPN tunnel is enabled, the client checks either for a trusted DNS domain or DNS server. If a trusted DNS domain or DNS server can be reached, then the client is on the trusted domain, and no VPN tunnel is needed. If not, then the VPN tunnel is needed to access internal resources.



Step 6: Click **OK,** and then click **Apply**.

Procedure 8 Test Trusted Network Detection

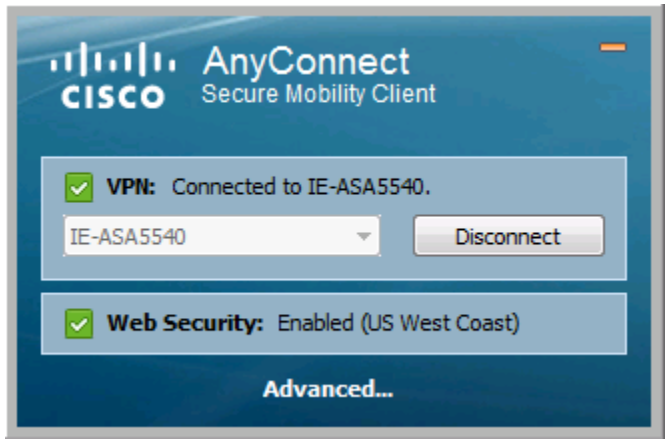
Test the configuration to ensure that trusted network detection is functional and that the VPN client attempts to start at startup if needed or when the client moves outside the network.

Step 1: On a laptop outside the network, connect the VPN to Cisco ASA.

Step 2: Move the client into the internal network, and establish a network connection again. The client should identify that it is on a trusted network and that the VPN is not required (the Web Security check box should also be disabled because the client is on the trusted network).

Step 3: Move the client back outside the network.

Step 4: At the VPN connect prompt, enter the credentials, and then verify that VPN and Web Security are enabled and the check boxes are green.



Procedure 9 Install the Certificate on the Client

In the Enterprise Internet Edge Foundation Guide, a self-signed certificate is generated and applied to Cisco ASA's outside interfaces. Because the certificate used in the lab is self-signed, all clients generate an error until the certificate is manually added to the trusted certificates. Certificates signed by a Public CA don't need to be manually added.

Because some of the features configured below involve automatic certificate checking, it isn't acceptable to have the errors show up when self-signed certificates are used. The following procedure takes care of the error problems.

Publically signed certificates do not have these issues and are in all ways superior and easier to use in practice.

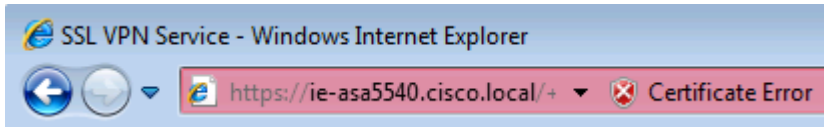
Step 1: On a client located outside the network, open a web browser (the procedure below details the process for Internet Explorer), and go to the Cisco ASA address:

https://ie-asa5540.cisco.local

The first page reports a problem with the certificate.

Step 2: Click **Continue to this website**.

Step 3: On the next page, in the URL bar, click **Certificate Error**.

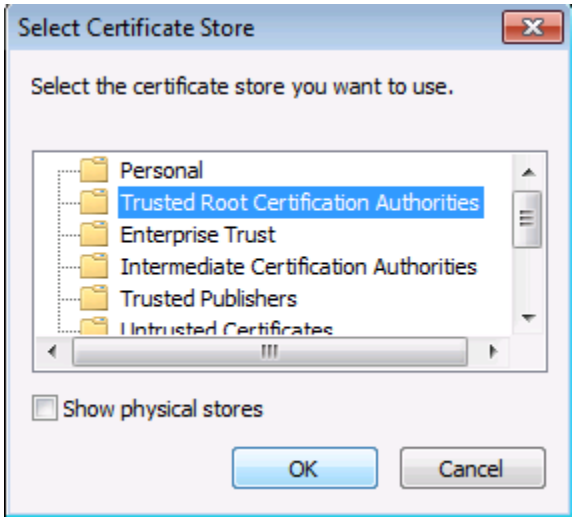


Step 4: Select **View Certificate**.

Step 5: At the bottom of the **Certificate** page, select **Install Certificate**. When the Certificate Import Wizard opens, click **Next**.

Step 6: Select **Place all Certificates in the following store,** and then click **Browse.**

Step 7: Select **Trusted Root Certification Authorities,** and then click **OK.**



Step 8: Click **Next**, and then click **Finish.**

Step 9: Accept the security warning and install the certificate.

Tech Tip

When outside a lab environment, be very careful when installing certificates; after they are installed, they are implicitly trusted by the client. Public signed certificates do not have to be manually trusted.

Step 10: In the **Certificate** window, click **OK**.

Step 11: Close and relaunch the browser, and then navigate to the following location:

https://ie-asa5540.cisco.local

The SSL VPN Service page loads without any certificate warnings or errors.

Procedure 10 Enable Always On

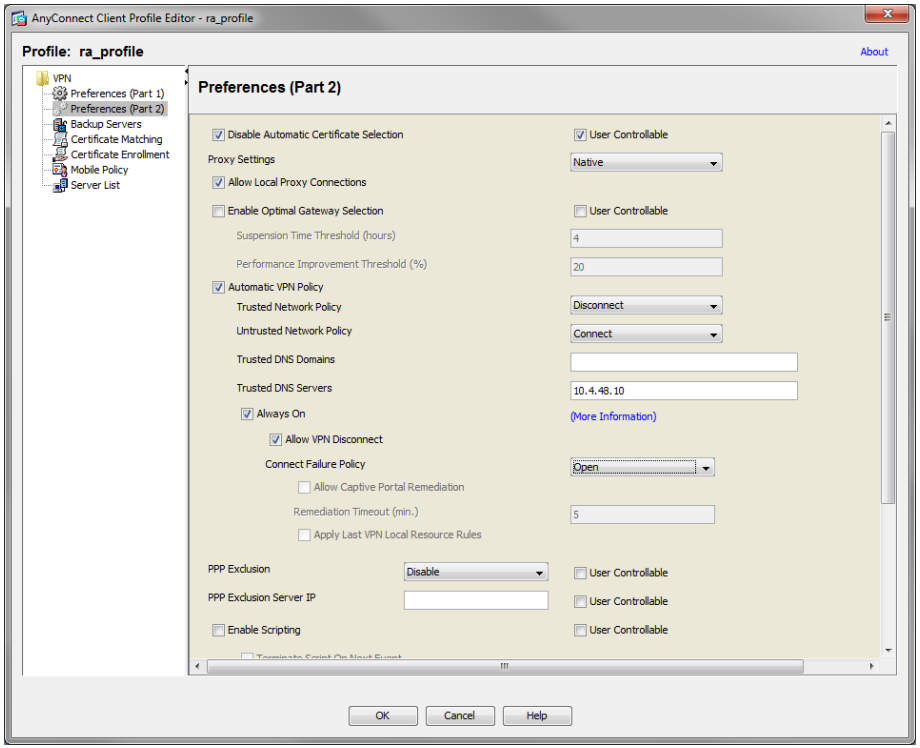
Tech Tip

If an incorrect Always On configuration is pushed to the client, it is likely that the Cisco AnyConnect software will need to be uninstalled from the client and then reinstalled after the configuration is fixed.

Step 1: In ASDM, navigate to **Configuration** > **Remote Access VPN** > **Network Client Access** > **AnyConnect Client Profile**, select ra_profile, and then click **Edit**

Step 2: In **Preferences (Part 2)**, select the **Always On** and **Allow VPN Disconnect check boxes**.

Step 3: In the **Connect Failure Policy** list, choose **Open**.

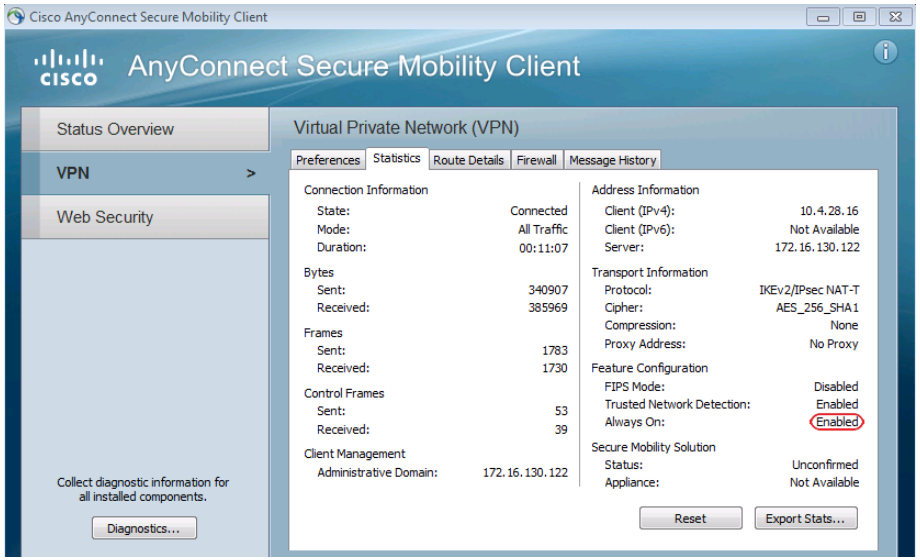


Step 4: Click **OK**, and then click **Apply**.

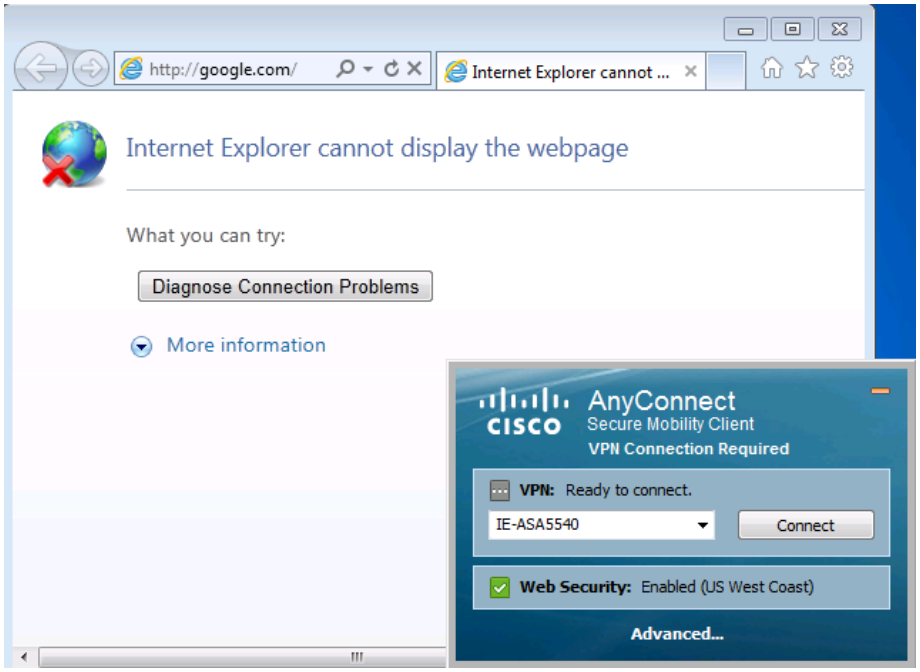
Procedure 11 Test the Always On Setting

Step 1: Connect a client, click the AnyConnect icon in the Windows taskbar, and then click **Advanced.**

Step 2: In the **VPN** > **Statistics** tab, ensure **Always On:** has a value of **Enabled**.



Step 3: With the client disconnected, check that **VPN Connection Required** appears on the Cisco AnyConnect screen. Browse to a known good website. It should fail because no access is allowed without the VPN tunnel being up.



Process

Configuring Access for Mobile Devices: ActiveSync

1. Firewall DMZ Configuration
2. Configure ActiveSync Access on Cisco ASA
3. Configure Additional Security

The first step in providing access for mobile devices like smartphones and tablets is providing email, calendar, and contacts availability. This is a basic requirement and for some users might be enough access. For those users that need or want full tunnel access or for those users connecting on more powerful devices such as tablets, full access can be achieved using SSL VPN in some cases or through the built-in IPsec client. Full access is needed for things such as internal file shares, internal web servers for employee directories, any other internally hosted web applications, or other services such as voice or video.

To this end, most administrators deploy Microsoft ActiveSync on a Microsoft ISA server in their DMZs. ActiveSync connects to the Microsoft Exchange system internally. This setup can provide access to email, calendars, and contacts from a wide variety of mobile devices including devices that run the Android, iOS, and Windows Mobile operating systems.

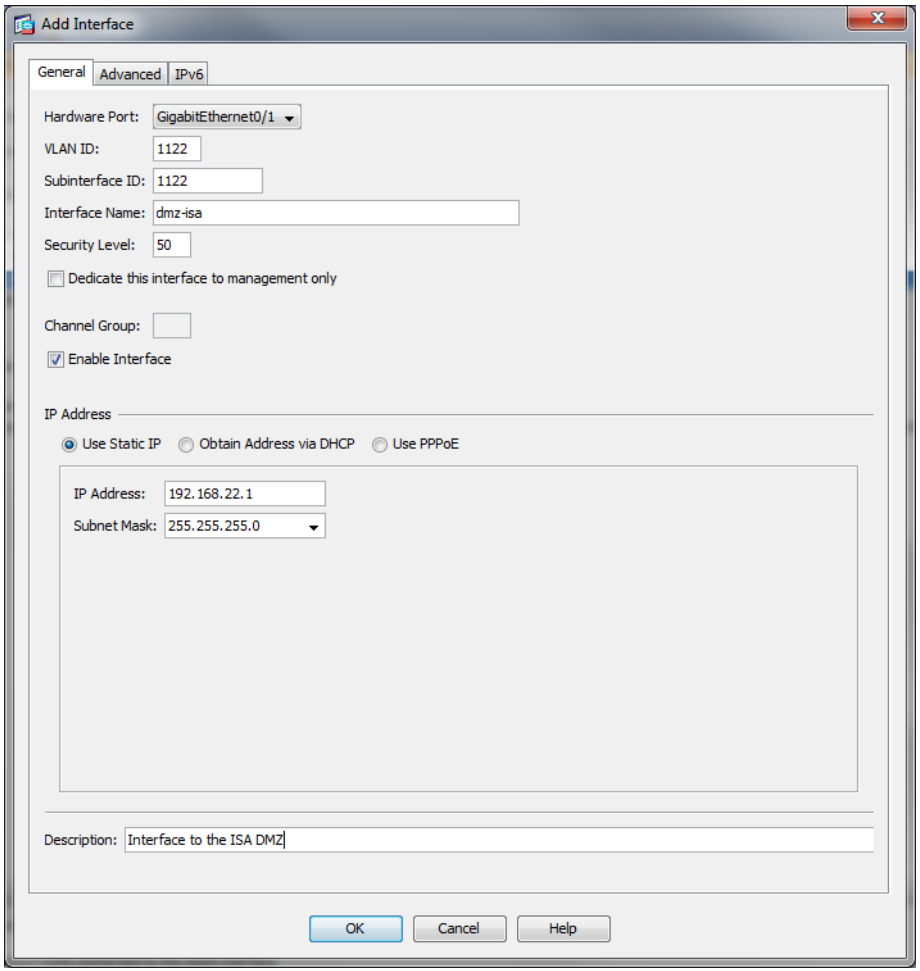
The setup and configuration of ISA, Exchange, and ActiveSync is assumed complete and functional for this document. This process discusses the configuration of Cisco ASA to support such a deployment as well as additional security steps to help improve the overall security of such a deployment.

Procedure 1 Firewall DMZ Configuration

A new DMZ will host the ISA server and allow incoming connections from the outside to the ISA server. It will also allow the ISA to connect to inside resources as required. Configuration of Cisco ASA and the DMZ switch must be updated.

Step 1: Open ASDM, and then navigate to **Configuration > Device Setup > Interfaces.**

Step 2: Click **Add** to create a new DMZ interface, and enter the required data.



Step 3: Click **OK,** and then click **Apply.**

Step 4: Navigate to **Configuration > Device Management > High Availability > Failover.**

Step 5: Edit the dmz-isa line to include the standby IP address for the interface: 192.168.22.2.

Step 6: On the DMZ switch, add the appropriate VLAN to the trunk ports that connect to the appliances.

Primary appliance

```
interface GigabitEthernet2/0/24
switchport trunk allowed vlan add 1122
```

Secondary appliance

```
interface GigabitEthernet2/0/24
switchport trunk allowed vlan add 1122
```

Procedure 2 Configure ActiveSync Access on Cisco ASA

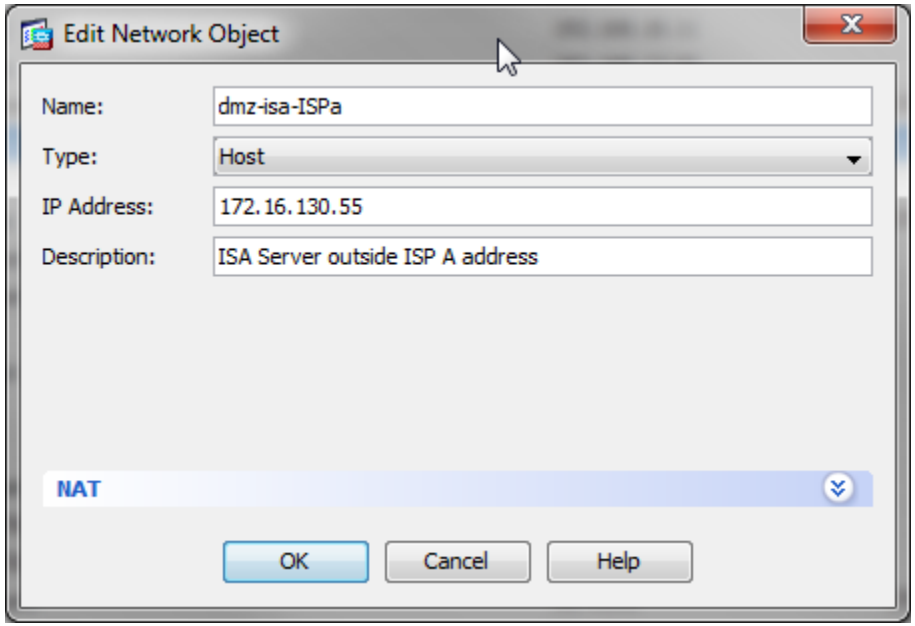
To allow ActiveSync to work through an external firewall, two things must be done. The first is building a NAT translation for the ISA server to the outside network. The second is allowing the needed connections to traverse the firewall. Allowing the connections to traverse the firewall includes outside hosts making connections to the ISA server, and also the ISA server making connections to the Exchange server.

This configuration is performed on the Cisco ASA firewall that controls access to the network and contains the DMZ where the ISA server resides.

Step 1: Open ASDM, and then navigate to **Configuration** > **Firewall** > **NAT Rules**.

Step 2: In the right-most panel, click **Add Network Object**.

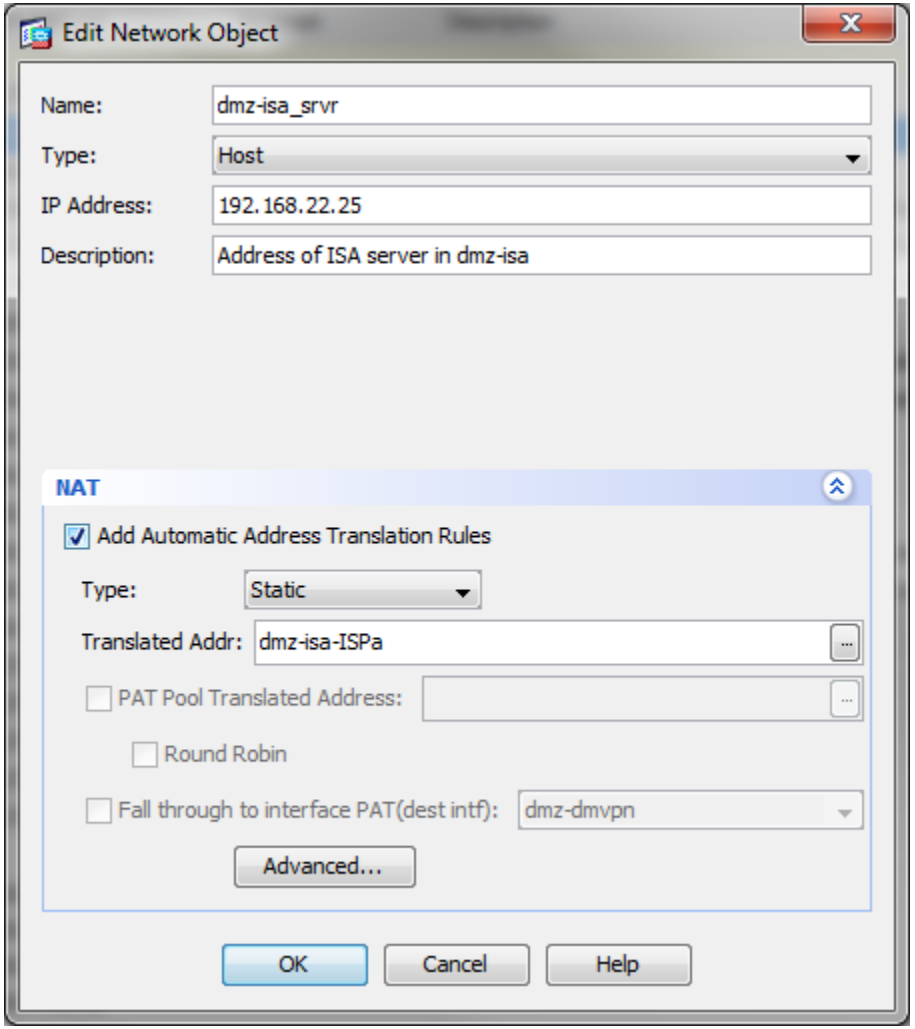
Step 3: In the **Add Network Object** dialog box, enter a name for this object for the ISA server, enter the IP address of the ISA on the outside ISP, and then click **OK**.



Step 4: Navigate to **Configuration** > **Firewall** > **NAT Rules**, click **Add Network Object NAT rule** to create the NAT object that ties the external address to the actual address of the ISA server in the DMZ.

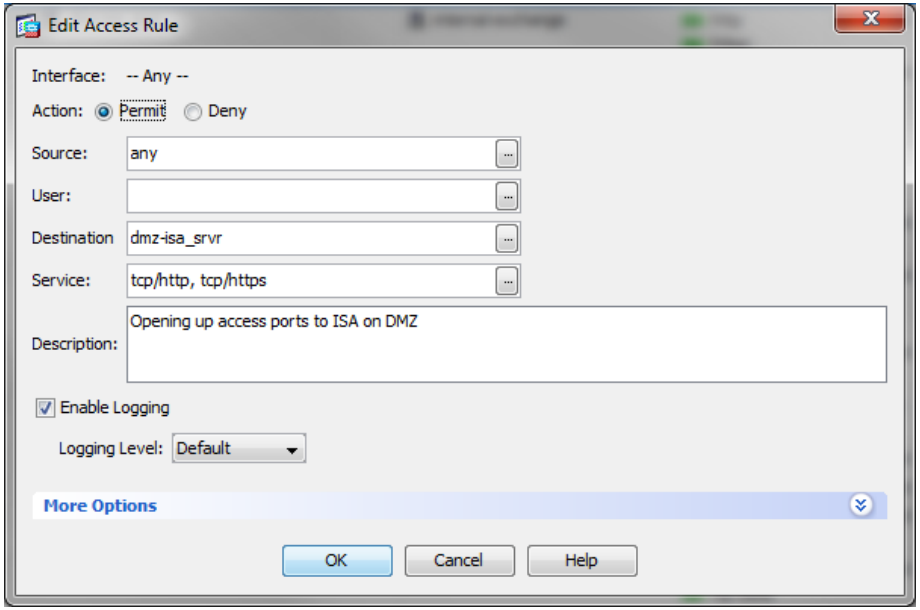
Step 5: Enter the object name to be used to reference the ISA server in the Cisco ASA config, and enter its actual address.

Step 6: Under **NAT**, select the **Add Automatic Address Translation Rules** box, in **Type**, choose **static**, in **Translated Addr**, choose the ISA server network object that references the public address of the ISA server (created above), and then click **OK.**



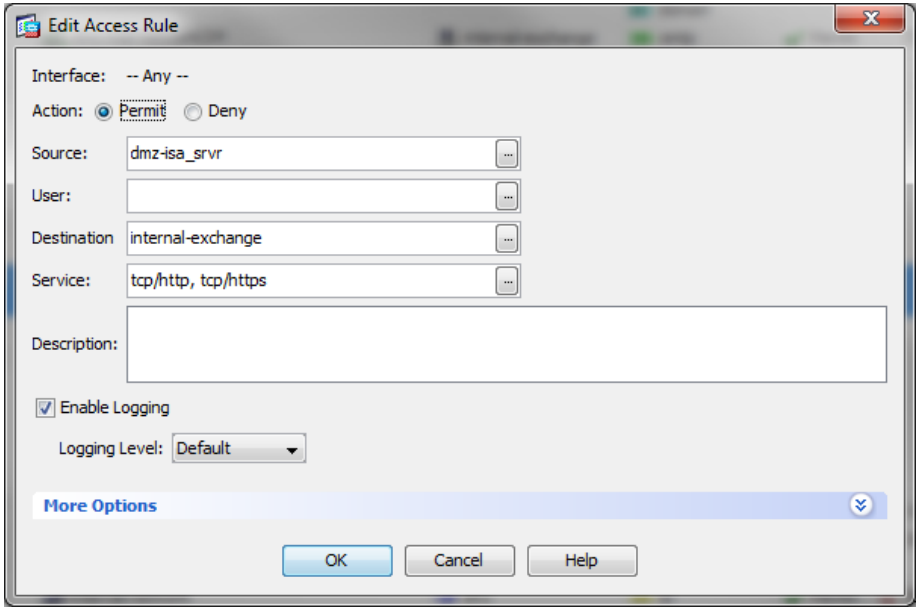
Step 7: To allow access to the ISA server running ActiveSync, navigate to **Configuration** > **Firewall** > **Access Rules**. Click **Add** > **Add Access Rule** to add a new Access Control Entry (ACE) rule to the global list of Access Rules. This allows outside hosts to make http and https connections to the ISA server.

1. For **Interface**—Any
2. For **Source**—Any
3. For **Destination**—dmz-isa_srvr
4. For **Service**—tcp/http and tcp/https



Step 8: To allow the ISA server access to the internal exchange server create another ACE.

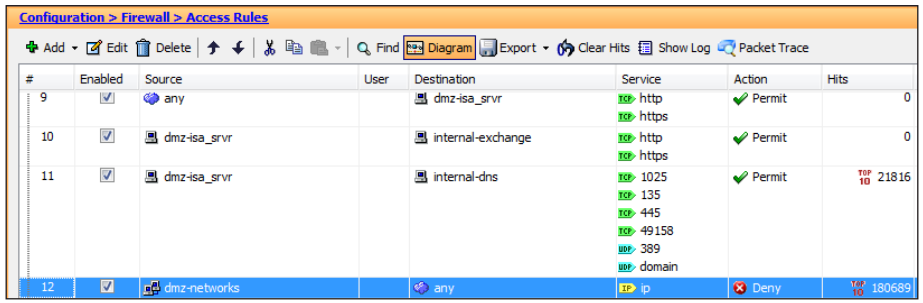
1. For **Interface**—Any
2. For **Source**—dmz-isa_srvr
3. For **Destination**—internal-exchange
4. For **Service**—tcp/http and tcp/https



Step 9: Permit access, using the examples above, from the ISA server to the Active Directory and the DNS server in the data center (in this example, the AD server is also the DNS server and is called DNS). The AD server requires ports on tcp 135, 445, 1025 and 49158 and udp 389 and the DNS server portion requires UDP 53.

Enabled	Source	User	Destination	Service	Action
☑	dmz-isa_srvr		internal-dns	TCP 1025 TCP 135 TCP 445 TCP 49158 UDP 389 UDP domain	Permit

Step 10: Move these Access Rules above any rule already configured that denies DMZ networks access to other networks.



#	Enabled	Source	User	Destination	Service	Action	Hits
9	☑	any		dmz-isa_srvr	TCP http TCP https	Permit	0
10	☑	dmz-isa_srvr		internal-exchange	TCP http TCP https	Permit	0
11	☑	dmz-isa_srvr		internal-dns	TCP 1025 TCP 135 TCP 445 TCP 49158 UDP 389 UDP domain	Permit	TOP 10 21816
12	☑	dmz-networks		any	IP ip	Deny	TOP 10 180689

Procedure 3 Configure Additional Security

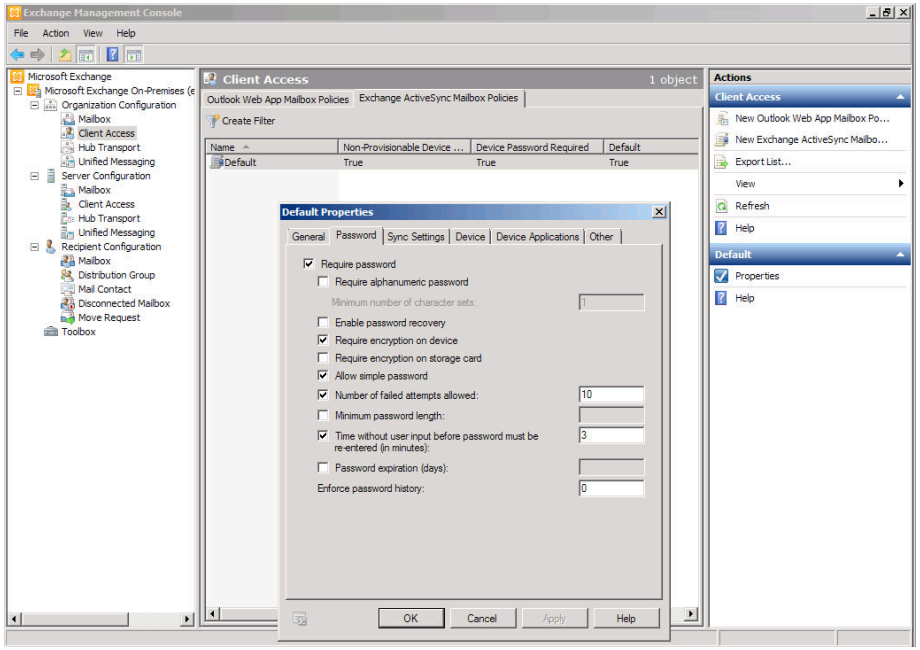
To increase the security of the deployment, ActiveSync includes some security options that administrators may deploy. These options include password requirements, inactivity timeout, device encryption, and a maximum number of failed password attempts before the data on the device is deleted. Security options vary by device. The organizational security policy should be used as a guide on how to approach the use of smartphones in the network.

Step 1: In the Exchange Management Console, navigate to **Organization Configuration** > **Client Access**.

Step 2: Click the **Exchange ActiveSync Mailbox Policies** tab, select the policy you want to view in the action pane, and then click **Properties**.

Step 3: In the **Password** tab, set password requirements for Exchange ActiveSync clients, as follows:

1. Select the **Require Password** check box.
2. Select **Allow Simple Password.** This check box allows pin-number-style simple passwords (a minimum level of security but easy to type and remember).
3. Select the **Require Encryption on Device** check box.
4. Enter a number in the **Number of Failed Attempts Allowed.** This setting limits the number of failed password attempts before all information on the device is deleted.
5. Enter a time in minutes in the **Time without user input before password must be reentered**.



Process

Configuring Access for Mobile Devices: AnyConnect Client

1. Configure Full Access using SSL VPN

Procedure 1 Configure Full Access using SSL VPN

The Cisco AnyConnect Client is available for some versions of smartphones or tablets (check the app store for your phone for availability). If available, your device can be configured to connect to Cisco ASA by using SSL VPN to provide full access to the internal network and its resources.

To better support the mobility of smartphones and tablets, a change should be made to the Cisco AnyConnect client profile that is used.

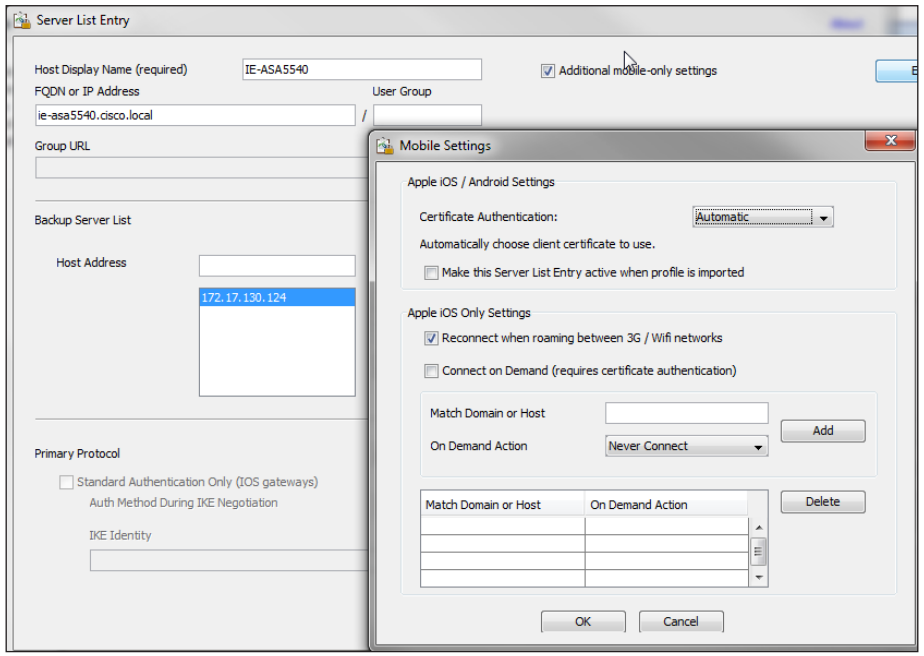
Step 1: In ASDM, navigate to **Configuration > Remote Access VPN > Network Client Access > AnyConnect Client Profile.**

Step 2: Select the profile with profile usage set to VPN that is assigned to the group policy that mobile phone users will be using (in this case, ra_profile associated with GroupPolicy_AnyConnect, GroupPolicy_Administrators and GroupPolicy_Partner), and then click **Edit.**

Step 3: In the tree, select **Server List**, highlight the server hostname (IE-ASA5540), and then click **Edit**.

Step 4: On the **Server List Entry** page, click the **Additional mobile-only settings** box, and then click **Edit**.

Step 5: Select the **Reconnect when roaming between 3G / WiFi networks** check box, and then click **OK**.



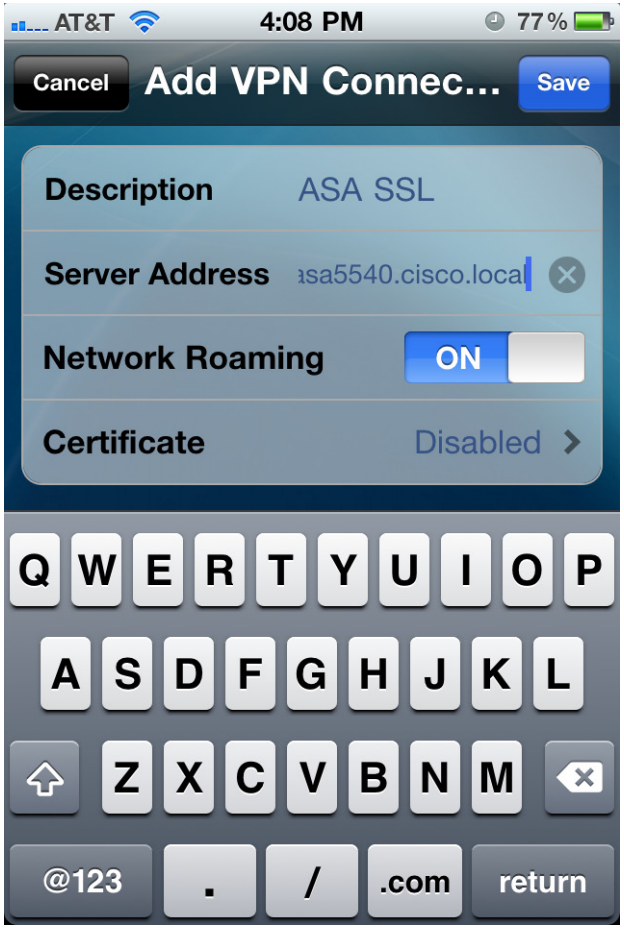
Reader Tip

The next steps are client-based and will be done on the actual phone or tablet device.

Step 6: On the device, download the AnyConnect client from the app store.

Step 7: Launch the AnyConnect application.

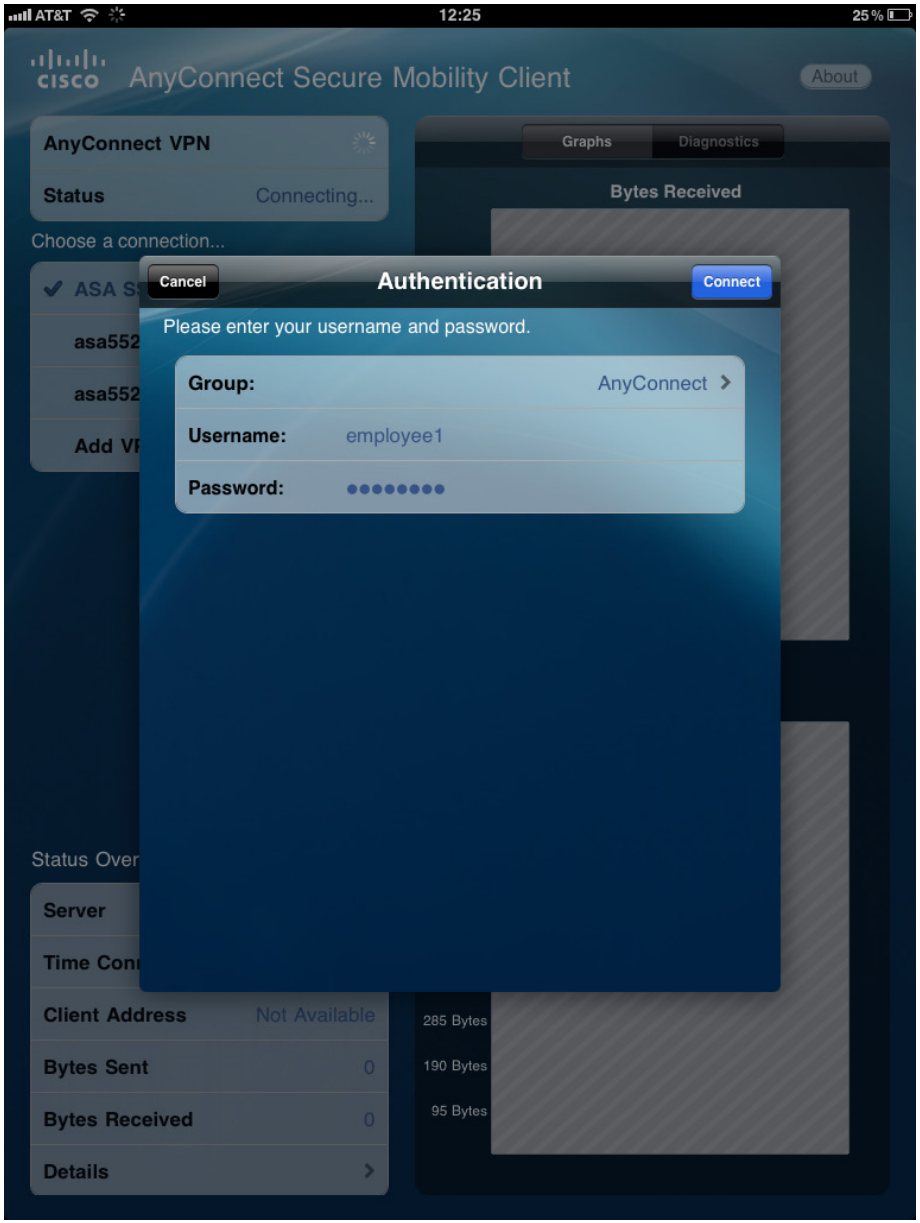
Step 8: Click **Add VPN Connection, and** enter ASA SSL in the **Description** field, enter ie-asa5540.cisco.local in the **Server Address** field, and then click **Save**.



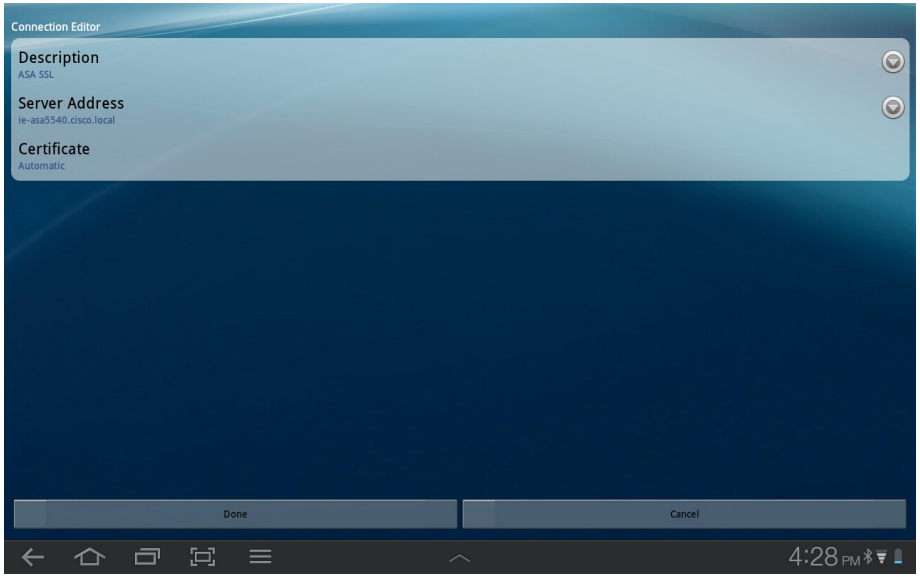
Step 9: Test the connection: select and enable the connection by moving the slider from the off to the on position. The group is AnyConnect.

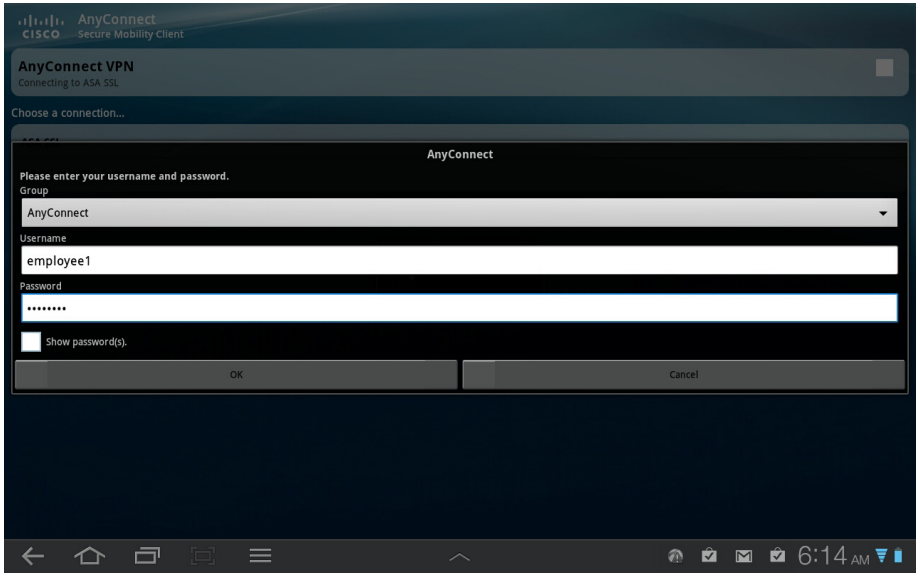
Step 10: Enter a valid user name and password for authentication, and then click **Connect**. The screens below show example connection tests for the iOS and Android operating systems.

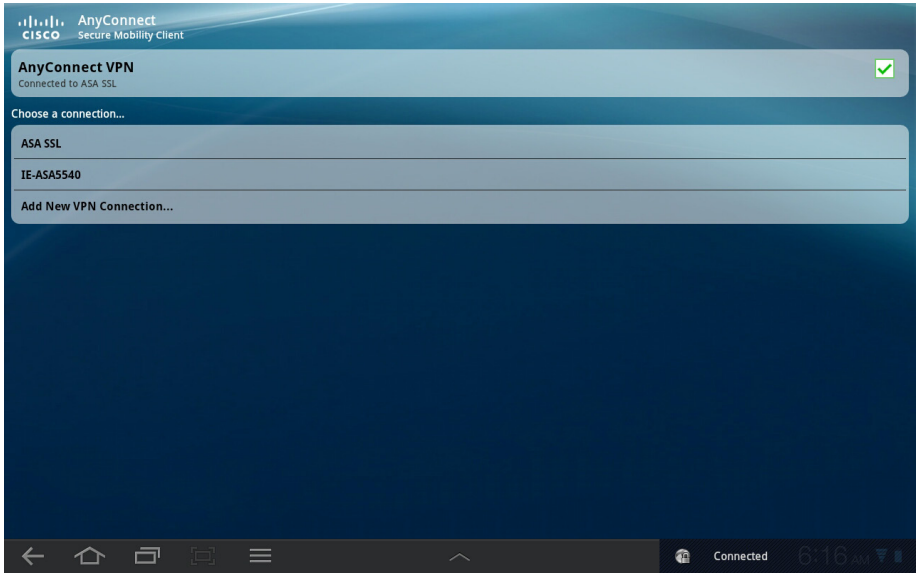
iOS Operating System Connection Example



Android Operating System Connection Example




AnyConnect
Secure Mobility Client
AnyConnect VPN
Connecting to ASA SSL
Choose a connection...
AnyConnect
Please enter your username and password.
Group
AnyConnect
Username
employee1
Password
Show password(s).
OK
Cancel
6:14 AM


AnyConnect
Secure Mobility Client
AnyConnect VPN
Connected to ASA SSL
Choose a connection...
ASA SSL
IE-ASA5540
Add New VPN Connection...
Connected

Notes

Appendix A: Product List

The following products and software versions have been validated for the Cisco Smart Business Architecture.

Functional Area	Product	Part Numbers	Software Version
Internet Edge 5K			
Firewall	ASA 5510 or ASA 5520 or ASA 5540	ASA5510-AIP10-SP-K9 ASA5520-AIP20-SP-K9 ASA5540-AIP40-SP-K9	8.4.2
RA VPN Firewall	ASA 5510 or ASA 5520 or ASA 5540	ASA5510-AIP10-SP-K9 ASA5520-AIP20-SP-K9 ASA5540-AIP40-SP-K9	8.4.2
SSL Software License for ASA	250 or 500 SSL Session Software License	L-ASA5500-SSL-250 L-ASA5500-SSL-500	* as firewall
Mobile License	Cisco AnyConnect Mobile License	L-ASA-AC-M-5520 L-ASA-AC-M-5540	
Firewall Management	ASDM	NA	6.4.5
VPN Client	Cisco AnyConnect Secure Mobility Client	NA	3.0.3054
Mobile Device VPN Client	Cisco AnyConnect VPN Client	NA	2.5.4038
ScanSafe	ScanSafe License	Please Contact your Cisco Scansafe Sales Representative for Part Numbers: scansafe-sales-questions@cisco.com	
Internet Edge 10K			
Firewall	2 x ASA 5520 or 2 x ASA 5540	2 x ASA5520-AIP20-SP-K9 2 x ASA5540-AIP40-SP-K9	8.4.2
RA VPN Firewall	ASA 5510 or ASA 5520 or ASA 5540	ASA5510-AIP10-SP-K9 ASA5520-AIP20-SP-K9 ASA5540-AIP40-SP-K9	8.4.2

Functional Area	Product	Part Numbers	Software Version
SSL Software License for ASA	250 or 500 SSL Session Software License	2 x L-ASA5520-SSL500-K9 Or 2 x L-ASA5540-SSL1000-K9	as firewall
Firewall Management	ASDM	NA	6.4.5
VPN Client	Cisco AnyConnect Secure Mobility Client	NA	3.0.3054
Mobile Device VPN Client	Cisco AnyConnect VPN Client	NA	2.5.4038
ScanSafe	ScanSafe License	Please Contact your Cisco Scansafe Sales Representative for Part Numbers: scansafe-sales-questions@cisco.com	

Appendix B: Configuration Files

This is the configuration of the ASA firewall. The new configuration for this additional deployment guide is highlighted to differentiate it from the configuration found in the foundation deployment guide.

```
ASA Version 8.4(2)
!
terminal width 511
hostname IE-ASA5540
domain-name cisco.local
enable password ******** encrypted
passwd ******** encrypted
names
 !
interface GigabitEthernet0/0
  nameif inside
  security-level 100
  ip address 10.4.24.30 255.255.255.224 standby 10.4.24.29
  summary-address eigrp 100 10.4.28.0 255.255.252.0 5
!
interface GigabitEthernet0/1
 description Trunk to DMZ-3750X GigabitEthernet X/0/24
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/1.1116
 description Web server DMZ connection on VLAN 1116
 vlan 1116
 nameif dmz-web
 security-level 50
 ip address 192.168.16.1 255.255.255.0 standby 192.168.16.2
!
interface GigabitEthernet0/1.1117
 description Email Security Appliance DMZ Connection on VLAN 1117
 vlan 1117
 nameif dmz-mail
 security-level 50
 ip address 192.168.17.1 255.255.255.0 standby 192.168.17.2
!
interface GigabitEthernet0/1.1118
 description DMVPN aggregation router connections on VLAN 1118
 vlan 1118
 nameif dmz-dmvpn
 security-level 75
 ip address 192.168.18.1 255.255.255.0 standby 192.168.18.2
!
interface GigabitEthernet0/1.1119
 vlan 1119
 nameif dmz-wlc
 security-level 50
 ip address 192.168.19.1 255.255.255.0
!
interface GigabitEthernet0/1.1122
 vlan 1122
 nameif dmz-isa
 security-level 50
 ip address 192.168.22.1 255.255.255.0 standby 192.168.22.2
!
interface GigabitEthernet0/1.1123
 description Management DMZ connection on VLAN 1123
 vlan 1123
 nameif dmz-management
 security-level 50
 ip address 192.168.23.1 255.255.255.0 standby 192.168.23.2
!
interface GigabitEthernet0/1.1128
 vlan 1128
 nameif dmz-guest
```

```
 security-level 10
 ip address 192.168.28.1 255.255.252.0
!
interface GigabitEthernet0/2
 description LAN/STATE Failover Interface
!
interface GigabitEthernet0/3
 description Trunk to OUT-2960S GigabitEthernet X/0/24
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3.16
 description Primary Internet connection on VLAN 16
 vlan 16
 nameif outside-16
 security-level 0
 ip address 172.16.130.124 255.255.255.0 standby 172.16.130.123
!
interface GigabitEthernet0/3.17
 description Resilient Internet connection on VLAN 17
 vlan 17
 nameif outside-17
 security-level 0
 ip address 172.17.130.124 255.255.255.0 standby 172.17.130.123
!
interface Management0/0
 shutdown
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
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 internal-network
 subnet 10.4.0.0 255.254.0.0
 description The organization's internal network range
object network dmz-networks
 subnet 192.168.16.0 255.255.248.0
 description The organization's DMZ network range
object network internal-network-ISPa
 subnet 10.4.0.0 255.254.0.0
 description PAT traffic from inside out the primary internet
connection
object network internal-network-ISPb
 subnet 10.4.0.0 255.254.0.0
 description PAT traffic from inside out the resilient internet
connection
object network outside-webserver-ISPa
 host 172.16.130.100
 description Webserver on ISP A
object network dmz-webserver-ISPa
 host 192.168.16.100
 description NAT the webserver in the DMZ to the outside address
on ISP A
object network dmz-webserver-ISPb
 host 192.168.16.100
 description NAT the webserver in the DMZ to the outside address
on ISP B
object network outside-webserver-ISPb
 host 172.17.130.100
 description Webserver on ISP B
object network NETWORK_OBJ_10.4.28.0_22
 subnet 10.4.28.0 255.255.252.0
object network outside-esa-ISPa
 host 172.16.130.25
 description ESA on ISP A
object network dmz-esa-ISPa
 host 192.168.17.25
```

```
 description NAT the ESA in the DMZ to the outside address on ISP
A
object network internal-dns
 host 10.4.48.10
 description DNS in the internal data center
object network internal-exchange
 host 10.4.48.25
 description Exchange server in the internal data center
object network internal-ntp
 host 10.4.48.17
 description NTP server in the internal data center
object network outside-dmvpn-ISPa
 host 172.16.130.1
 description DMVPN aggregation router on ISP A
object network dmz-dmvpn-1
 host 192.168.18.10
 description NAT the primary DMVPN aggregation router in the DMZ
to ISP A
object network dmz-web-net-v6
 subnet 2001:db8:a:1::/64
object network dmz-isa-ISPa
 host 172.16.130.55
 description ISA Server outside ISP A address
object network dmz-isa_srvr
 host 192.168.22.25
 description Address of ISA server in dmz-isa
object network dmz-dmvpn-2
 host 192.168.18.11
 description NAT the resilient DMVPN aggregation rotuer in the
DMZ to ISP B
object network outside-dmvpn-ISPb
 host 172.17.130.1
 description Resilient DMVPN aggregation router on ISP B
object network dmz-guest-network-ISPa
 subnet 192.168.28.0 255.255.252.0
object network dmz-wlc-guest-1
 host 192.168.19.10
 description Guest Anchor Wireless LAN Controller
object network internal-flex7500-1
 host 10.4.46.66
object network internal-flex7500-2
 host 10.4.46.67
object network internal-wlc-1
 host 10.4.46.64
object network internal-wlc-2
 host 10.4.46.65
object network internal-acs
 host 10.4.48.15
 description Internal ACS server
object network internal_ISE-1
 host 10.4.48.41
 description ISE 1 server
object network internal_ISE-2
 host 10.4.48.42
 description ISE 2 server
object network dmz-wlc-1
 host 192.168.19.20
 description Primary WLC to Support Office Extend APs
object network outside-wlc-1
 host 172.16.130.20
 description WLC to support Office Extend APs on ISP A
object network dmz-cvo-1
 host 192.168.18.20
 description Primary Router to Support CVO
object network outside-cvo-1
 host 172.16.130.2
 description Aggregation Router to Support CVO on ISP A
object-group service DM_INLINE_SERVICE_1
 service-object tcp destination eq ftp
 service-object tcp destination eq ftp-data
 service-object tcp destination eq tacacs
 service-object udp destination eq ntp
 service-object udp destination eq syslog
object-group service DM_INLINE_TCP_1 tcp
```

```
 port-object eq www
 port-object eq https
object-group service DM_INLINE_SERVICE_2
 service-object tcp destination eq domain
 service-object udp destination eq domain
object-group network DM_INLINE_NETWORK_1
 network-object 10.0.0.0 255.0.0.0
 network-object 172.16.0.0 255.255.0.0
 network-object 192.168.0.0 255.255.0.0
object-group service DM_INLINE_SERVICE_3
 service-object esp
 service-object udp destination eq 4500
 service-object udp destination eq isakmp
object-group icmp-type DM_INLINE_ICMP_1
 icmp-object echo
 icmp-object echo-reply
object-group service DM_INLINE_TCP_2 tcp
 port-object eq www
 port-object eq https
object-group service DM_INLINE_TCP_3 tcp
 port-object eq www
 port-object eq https
object-group service DM_INLINE_SERVICE_4
 service-object tcp destination eq 1025
 service-object tcp destination eq 135
 service-object udp destination eq 389
 service-object udp destination eq domain
 service-object tcp destination eq 445
 service-object tcp destination eq 49158
object-group service DM_INLINE_TCP_4 tcp
 port-object eq www
 port-object eq https
object-group network internal-wlcs
 description All internal wireless LAN controllers
 network-object object internal-flex7500-1
 network-object object internal-flex7500-2
 network-object object internal-wlc-1
 network-object object internal-wlc-2
object-group service DM_INLINE_SERVICE_5
 service-object tcp destination eq tacacs
 service-object udp destination eq 1812
 service-object udp destination eq 1813
object-group service DM_INLINE_SERVICE_6
 service-object 97
 service-object udp destination eq 16666
object-group service DM_INLINE_TCP_5 tcp
 port-object eq ftp
 port-object eq ftp-data
object-group network DM_INLINE_NETWORK_2
 network-object object dmz-networks
 network-object object internal-network
object-group service DM_INLINE_SERVICE_7
 service-object tcp destination eq domain
 service-object udp destination eq bootps
 service-object udp destination eq domain
object-group service DM_INLINE_TCP_6 tcp
 port-object eq www
 port-object eq https
object-group network ISE_Servers
 network-object object internal_ISE-1
 network-object object internal_ISE-2
object-group service DM_INLINE_TCP_7 tcp
 port-object eq 8080
 port-object eq 8443
object-group service DM_INLINE_SERVICE_8
 service-object tcp
 service-object tcp destination eq tacacs
 service-object udp destination eq 1812
 service-object udp destination eq 1813
object-group service DM_INLINE_UDP_1 udp
 port-object eq 5246
 port-object eq 5247
object-group service DM_INLINE_SERVICE_9
 service-object esp
```

```
 service-object tcp destination eq https
 service-object udp destination eq 4500
 service-object udp destination eq isakmp
 service-object tcp destination eq 3389
access-list global_access remark Permit management protocols from
the DMZ to the internal network
access-list global_access extended permit object-group DM_INLINE_
SERVICE_1 192.168.23.0 255.255.255.0 object internal-network
access-list global_access remark Allow anyone to access the
webserver in the DMZ
access-list global_access extended permit tcp any 192.168.16.0
255.255.255.0 object-group DM_INLINE_TCP_1
access-list global_access remark Permit the mail DMZ to sync with
the internal NTP server
access-list global_access extended permit udp 192.168.17.0
255.255.255.0 object internal-ntp eq ntp
access-list global_access remark Permit the mail DMZ to do
lookups on the internal DNS
access-list global_access extended permit object-group DM_INLINE_
SERVICE_2 192.168.17.0 255.255.255.0 object internal-dns
access-list global_access remark Permit the mail DMZ to send SMTP
to the internal exchange server
access-list global_access extended permit tcp 192.168.17.0
255.255.255.0 object internal-exchange eq smtp
access-list global_access remark Permit SMTP traffic into the
email DMZ
access-list global_access extended permit tcp any 192.168.17.0
255.255.255.0 eq smtp
access-list global_access remark Allow diagnostic traffic to the
DMVPN aggregation routers
access-list global_access extended permit icmp any 192.168.18.0
255.255.255.0 object-group DM_INLINE_ICMP_1
access-list global_access remark Allow traffic to the DMVPN
aggregation routers
access-list global_access extended permit object-group DM_INLINE_
SERVICE_3 any 192.168.18.0 255.255.255.0
access-list global_access remark Opening up access ports to ISA
on DMZ
access-list global_access extended permit tcp any object dmz-isa_
srvr object-group DM_INLINE_TCP_3
access-list global_access extended permit tcp object dmz-isa_srvr
object internal-exchange object-group DM_INLINE_TCP_4
access-list global_access extended permit object-group DM_INLINE_
SERVICE_4 object dmz-isa_srvr object internal-dns
access-list global_access extended permit tcp 192.168.28.0
255.255.252.0 192.168.16.0 255.255.255.0 object-group DM_INLINE_
TCP_6
access-list global_access extended permit object-group DM_INLINE_
SERVICE_7 192.168.28.0 255.255.252.0 object internal-dns
access-list global_access extended permit tcp 192.168.28.0
255.255.252.0 object-group ISE_Servers object-group DM_INLINE_
TCP_7
access-list global_access remark Deny traffic for the guest
network to internal and dmz resources
access-list global_access extended deny ip 192.168.28.0
255.255.252.0 object-group DM_INLINE_NETWORK_2
access-list global_access remark Allow guest traffic to the
internet
access-list global_access extended permit ip 192.168.28.0
255.255.252.0 any
access-list global_access extended permit udp 192.168.19.0
255.255.255.0 object internal-dns eq bootps
access-list global_access extended permit object-group DM_INLINE_
SERVICE_6 192.168.19.0 255.255.255.0 object-group internal-wlcs
access-list global_access remark Allow WLCs to download via FTP
from internal servers
access-list global_access extended permit tcp 192.168.19.0
255.255.255.0 object internal-network object-group DM_INLINE_
TCP_5
access-list global_access remark Allow WLCs to communicate with
the internal NTP server
access-list global_access extended permit udp 192.168.19.0
255.255.255.0 object internal-ntp eq ntp
```

```
access-list global_access remark Allow WLC to talk to ISE servers
access-list global_access extended permit object-group DM_INLINE_
SERVICE_8 192.168.19.0 255.255.255.0 object-group ISE_Servers
access-list global_access remark Allow WLCs to communicate with
the AAA server
access-list global_access extended permit object-group DM_INLINE_
SERVICE_5 192.168.19.0 255.255.255.0 object internal-acs
access-list global_access remark TEST RULE !!!!!!!!
access-list global_access extended permit icmp any any
access-list global_access remark Allow traffic to the DMZ DMVPN
aggregation routers
access-list global_access extended permit object-group DM_INLINE_
SERVICE_9 any 192.168.18.0 255.255.255.0
access-list global_access remark Deny traffic from any DMZ
network
access-list global_access extended deny ip object dmz-networks
any
access-list global_access remark Deny the use of telnet from the
internal network to external networks
access-list global_access extended deny tcp object internal-
network any eq telnet
access-list global_access remark Permit IP traffic from the
internal network to external networks
access-list global_access extended permit ip object internal-
network any log disable
access-list global_access extended permit udp any object dmz-
wlc-1 object-group DM_INLINE_UDP_1
access-list global_mpc extended permit ip any any
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 WCCP_Redirect remark Do not WCCP redirect connections
to these addresses
access-list WCCP_Redirect extended deny ip any object-group DM_
INLINE_NETWORK_1
access-list WCCP_Redirect remark WCCP redirect all other IP
addresses
access-list WCCP_Redirect extended permit ip any any
access-list ScanSafe_Tower_Exclude remark scansafe westcoast
access-list ScanSafe_Tower_Exclude standard permit host
72.37.244.75
access-list ScanSafe_Tower_Exclude remark scansafe UK
access-list ScanSafe_Tower_Exclude standard permit host
80.254.147.155
access-list ScanSafe_Tower_Exclude remark scansafe Germany
access-list ScanSafe_Tower_Exclude standard permit host
80.254.148.130
access-list ScanSafe_Tower_Exclude remark scansafe France
access-list ScanSafe_Tower_Exclude standard permit host
80.254.150.66
access-list ScanSafe_Tower_Exclude remark scansafe Denmark
access-list ScanSafe_Tower_Exclude standard permit host
80.254.154.66
access-list ScanSafe_Tower_Exclude remark scansafe US east coast
access-list ScanSafe_Tower_Exclude standard permit host
80.254.152.99
access-list ScanSafe_Tower_Exclude remark scansafe US midwest
access-list ScanSafe_Tower_Exclude standard permit host
69.174.58.27
access-list ScanSafe_Tower_Exclude remark scansafe US south
access-list ScanSafe_Tower_Exclude standard permit host
72.37.249.43
access-list ScanSafe_Tower_Exclude remark scansafe Australia
access-list ScanSafe_Tower_Exclude standard permit host
69.174.87.43
access-list ScanSafe_Tower_Exclude remark scansafe Hong Kong
access-list ScanSafe_Tower_Exclude standard permit host
202.167.250.66
```

```
access-list ScanSafe_Tower_Exclude remark scansafe India
access-list ScanSafe_Tower_Exclude standard permit host
115.111.223.66
access-list ScanSafe_Tower_Exclude remark scansafe Japan
access-list ScanSafe_Tower_Exclude standard permit host
122.50.127.42
access-list ScanSafe_Tower_Exclude remark scansafe Singapore
access-list ScanSafe_Tower_Exclude standard permit host
202.79.203.66
access-list ScanSafe_Tower_Exclude standard permit host
128.107.241.169
no pager
logging enable
logging buffered informational
logging asdm informational
mtu inside 1500
mtu dmz-web 1500
mtu dmz-mail 1500
mtu dmz-dmvpn 1500
mtu dmz-wlc 1500
mtu dmz-isa 1500
mtu dmz-management 1500
mtu dmz-guest 1500
mtu outside-16 1500
mtu outside-17 1500
mtu management 1500
ip local pool RA-pool 10.4.28.1-10.4.31.255 mask 255.255.252.0
ipv6 route outside-16 ::/0 2001:db8:a::7206
ipv6 access-list global_access_ipv6 permit tcp any object dmz-
web-net-v6 object-group DM_INLINE_TCP_2
failover
failover lan unit primary
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 10.4.24.33 255.255.255.224 standby
10.4.24.34
monitor-interface dmz-web
monitor-interface dmz-mail
monitor-interface dmz-dmvpn
monitor-interface dmz-isa
monitor-interface dmz-management
monitor-interface outside-16
monitor-interface outside-17
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
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
!
object network internal-network-ISPa
 nat (any,outside-16) dynamic interface
object network internal-network-ISPb
 nat (any,outside-17) dynamic interface
object network dmz-webserver-ISPa
 nat (any,outside-16) static outside-webserver-ISPa
object network dmz-webserver-ISPb
 nat (any,outside-17) static outside-webserver-ISPb
object network dmz-esa-ISPa
 nat (any,outside-16) static outside-esa-ISPa
object network dmz-dmvpn-1
 nat (any,outside-16) static outside-dmvpn-ISPa
object network dmz-isa_srvr
 nat (any,any) static dmz-isa-ISPa
object network dmz-dmvpn-2
 nat (any,outside-17) static outside-dmvpn-ISPb
object network dmz-guest-network-ISPa
 nat (any,outside-16) dynamic interface
object network dmz-wlc-1
 nat (any,outside-16) static outside-wlc-1
```

```
object network dmz-cvo-1
 nat (any,outside-16) static outside-cvo-1
access-group global_access global
access-group global_access_ipv6 global
!
router eigrp 100
 no auto-summary
 network 10.4.24.0 255.255.252.0
 network 192.168.16.0 255.255.248.0
 passive-interface default
 no passive-interface inside
 redistribute static
!
route outside-16 0.0.0.0 0.0.0.0 172.16.130.126 128 track 1
route outside-17 0.0.0.0 0.0.0.0 172.17.130.126 254
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 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 192.168.1.0 255.255.255.0 management
http 10.4.0.0 255.254.0.0 inside
snmp-server host inside 10.4.48.35 community ******** version 2c
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 ca trustpoint ASDM_TrustPoint0
 enrollment self
 subject-name CN=IE-ASA5540.cisco.local
 proxy-ldc-issuer
 crl configure
crypto ca certificate chain ASDM_TrustPoint0
 certificate e5035c4e
 3082026c 308201d5 a0030201 020204e5 035c4e30 0d06092a 864886f7
0d010105
 05003048 311f301d 06035504 03131649 452d4153 41353534 302e6369
73636f2e
 6c6f6361 6c312530 2306092a 864886f7 0d010902 16164945 2d415341
35353430
 2e636973 636f2e6c 6f63616c 301e170d 31313038 32393231 35313130
5a170d32
 31303832 36323135 3131305a 3048311f 301d0603 55040313 1649452d
41534135
 3534302e 63697363 6f2e6c6f 63616c31 25302306 092a8648 86f70d01
09021616
 49452d41 53413535 34302e63 6973636f 2e6c6f63 616c3081 9f300d06
092a8648
```

```
86f70d01 01010500 03818d00 30818902 818100a7 fee67ff4 14768acb
30269b24
 53e09cce 9f7691f3 17b25250 67c7e892 6362af6a 3c7fb393 83209a44
947bb7cb
 2a5b4cdb 8ccd87c4 1890f5b9 8c247e7c f2835887 a2d266fd 262804a8
6c64270f
 4f6cf5a6 248208f7 9f60bc45 0ffcb8df 4806df1f 518e4b85 2aa39e44
88455de9
 acaee96b e0f69b5b 71aa8d70 8e86a0e4 b8989b02 03010001 a3633061
300f0603
 551d1301 01ff0405 30030101 ff300e06 03551d0f 0101ff04 04030201
86301f06
 03551d23 04183016 8014fa32 2185c193 c80b6bc1 d1b24051 fd6b7044
e673301d
 0603551d 0e041604 14fa3221 85c193c8 0b6bc1d1 b24051fd 6b7044e6
73300d06
 092a8648 86f70d01 01050500 03818100 19d5cf64 3416269f 934e5601
4e36df73
 14a8f44b 14ea0c96 70fda56d de559466 4d8fafb5 65a4bad8 a65fe039
2553b96b
 44c54065 7dac21a6 7950b619 a2361fc5 c63ce35a bccc30b2 4c10cb5c
7f761f31
 9b1679ef 0f69f210 a5268f88 0a09bb37 f094859a cc66d77f e80d0df9
22c47631
 232993bc 7d0c8851 d84b7d78 076e6d07
 quit
!
track 1 rtr 16 reachability
telnet timeout 5
ssh 10.4.0.0 255.254.0.0 inside
ssh timeout 5
ssh version 2
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
!
tls-proxy maximum-session 2000
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
wccp 90 redirect-list WCCP_Redirect
wccp interface inside 90 redirect in
ntp server 10.4.48.17
ssl trust-point ASDM_TrustPoint0 outside-16
ssl trust-point ASDM_TrustPoint0 outside-17
webvpn
 enable outside-16
 enable outside-17
 anyconnect image disk0:/anyconnect-linux-64-3.0.3054-k9.pkg 1
 anyconnect image disk0:/anyconnect-macosx-i386-3.0.3054-k9.pkg 2
 anyconnect image disk0:/anyconnect-win-3.0.3054-k9.pkg 3
 anyconnect profiles ra_profile disk0:/ra_profile.xml
 anyconnect profiles web_security_profile disk0:/web_security_
profile.wsp
 anyconnect profiles web_security_profile.wso  disk0:/web_
security_profile.wso
 anyconnect enable
 tunnel-group-list enable
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
 split-tunnel-policy excludespecified
 split-tunnel-network-list value ScanSafe_Tower_Exclude
 default-domain value cisco.local
 webvpn
 anyconnect modules value websecurity
 anyconnect profiles value ra_profile type user
 anyconnect profiles value web_security_profile.wso type
websecurity
 always-on-vpn profile-setting
```

```
group-policy GroupPolicy_Administrators internal
group-policy GroupPolicy_Administrators attributes
 banner value Your access is via an unrestricted split tunnel.
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value RA_SplitTunnelACL
 webvpn
 anyconnect profiles value ra_profile type user
group-policy GroupPolicy_Partner internal
group-policy GroupPolicy_Partner attributes
 banner value Your access is restircted to the partner server
 vpn-filter value RA_PartnerACL
 webvpn
 anyconnect profiles value ra_profile type user
username admin password w2Y.6Op4j7clVDk2 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
tunnel-group AnyConnect webvpn-attributes
 group-alias AnyConnect enable
 group-url https://172.16.130.124/AnyConnect enable
 group-url https://172.17.130.124/AnyConnect enable
!
class-map global-class
 match access-list global_mpc
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 rsh
 inspect rtsp
 inspect esmtp
 inspect sqlnet
 inspect skinny
 inspect sunrpc
 inspect xdmcp
 inspect sip
 inspect netbios
 inspect tftp
 inspect ip-options
 class global-class
 ips inline fail-close
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
Cryptochecksum:86c713bf3d183a963386aad1eadd18e4
: end
```

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-0000151-1 12/11