

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.



BYOD

FH

SOLUTIONS

1111111

CISCO

SBA

BYOD—Remote Mobile Access Deployment Guide

SMART BUSINESS ARCHITECTURE

August 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 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.

The Release Notes for a series provides a summary of additions and changes made in the 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 2012 are the "August 2012 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 SBA feedback form.

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

August 2012 Series

Table of Contents

What's In This SBA Guide1
Cisco SBA Solutions 1
Route to Success 1
About This Guide1
Introduction2
Business Overview2
Technology Overview
Deployment Details
Configuring Access for Laptop Devices5
Configuring Access for Mobile Devices: ActiveSync16
Configuring Access for Mobile Devices: AnyConnect Client

Appendix A: Product List	25
Appendix B: Configuration Files.	26
Appendix C: Changes	.31

What's In This SBA Guide

Cisco SBA Solutions

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.

Cisco SBA Solutions are designs for specific problems found within the most common technology trends. Often, Cisco SBA addresses more than one use case per solution because customers adopt new trends differently and deploy new technology based upon their needs.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

About This Guide

This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- Business Overview—Describes the business use case for the design. Business decision makers may find this section especially useful.
- Technology Overview—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

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

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

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



Introduction

Note

This guide is based on the *Cisco SBA—Borderless Networks* Secure Remote Mobile Access Deployment Guide. The goal of this guide is to show you how a BYOD business problem can be solved by using Cisco Smart Business Architecture. Cisco has previously developed solutions to solve issues that are similar to the various BYOD business problems. Cisco SBA uses the Cisco AnyConnect remote access solution to solve the BYOD problem of providing secure access to mobile devices at off-site locations.

There is a trend in the marketplace today that is often referred to as *Bring Your Own Device* (BYOD). BYOD is a spectrum of business problems that can be solved in various ways. These range from accessing guest wireless networks to providing device authentication and identification. The goal is to provide a common work environment, regardless of the type of device being used. This could be accomplished by providing a virtualized desktop or by allowing users to self-register devices for use on the network.

Organizations are experiencing an unprecedented transformation in the network landscape. In the past, IT typically provided network resources only to corporate-managed PCs, such as laptops and desktops. Today, employees are requiring access from both corporate managed and unmanaged devices, including mobile devices like smart phones and tablets. This rapid proliferation of mobile devices capable of supporting applications drastically increases workforce mobility and productivity, but it also presents an enormous challenge to IT organizations seeking to enforce security policies across a growing population of devices, operating systems, and connectivity profiles.

The distinction between a work device and a personal device has evolved. This evolution of mobile device usage and the introduction of mobile devices into the workplace has caused a paradigm shift in how IT views what qualifies as a network "end point device" and also what it means to "be at work." An organization needs to know not only who is accessing their wired and wireless networks, but also when the networks are accessed and from where. In addition, with the wide adoption of nontraditional devices, such as smart phones and tablets, and people bringing their own devices to access the network, organizations need to know how many of these devices are connecting. With this information, the organization can create policy to prevent connection by nontraditional devices, limit connection to approved devices, or make access to network resources easier for these non-traditional devices. This presents a challenge for IT organizations that seek to provide end-users with a consistent network access experience and the freedom to use any device, while still enforcing stringent security policies to protect corporate intellectual property. Further complicating the situation is delivering both consistent access and enforcing proper security policy based on the specific user-access scenario (wired, wireless, guest, local, branch, and remote users).

To balance the productivity gains versus the security risks, IT needs to implement a solution that allows for seamless on-boarding of users and devices, simplicity of on-going operations, and the ability to extend end-user applications to any user or any device at any time.

Other Cisco SBA Solutions guides addressing BYOD business problems include:

- BYOD—Internal Corporate Access Deployment Guide
- BYOD—Identity and Authentication Deployment Guide
- BYOD—Advanced Guest Wireless Access Deployment Guide

Business Overview

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 use a laptop, smartphone, or tablet device to connect through infrastructure that is not provided by their organizations. The guide does not cover use cases related to campus wireless access or home teleworker solutions.

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 the 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 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 (SBA) Internet edge design provides the basic framework for the enhancements and additions that will be discussed in this guide. A prerequisite for using this deployment guide is that you must have already followed the guidance in the *Remote Access VPN Deployment Guide*, which itself builds upon the *Firewall and IPS Deployment Guide*. The *Internet Edge Design Overview* describes the goals of the overall design and how the pieces interact together.

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 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 headend. 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.

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 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 in and administer the account.

It also assumes that you have different groups built in Active Directory (AD) to allow differentiation based on those groups.

Step 1: In the Cisco ScanSafe ScanCenter Portal, after logging in 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.

ScanCenter 🖦	Bcisco.com logged into: Cisco_Smart Business Architecture Group	Logout Help Contact Us 🏼 🌌 Sca	nSafe
	Home Dashboard Web Virus Spyware Web Fi	tering Email Admin Reports	Suppor
Your account Authentication	Management Reports		
Manage Groups			
- Search,	, add or delete groups		
Search	h: Search	Reload list 😔	
Group	Name	Delete	
WinNT:	://CISCO\Enterprise Operators		
WinNT:	://CISCO\Network Device Admins		
WinNT:	://CISCO\vpn-user		

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

Step 3: Navigate to Authentication > Company Key.

ScanCenter Locout Hele Contact Lie 🜠 ScanSafe						
	Home Dashboard Web Virus Spyware Web Filtering	Admin Reports Support				
Your account	Authentication Management Reports					
Company Key	Group Keys					
	User Keys the tication key for Cisco_Smart Business Architecture Group					
	Email Messages Name: Cisco_Smart Business Architecture Group					
	Key Ref: 1654					
	State: Active					
	Deactivate Revoke					

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 sent in email, 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 Allow, 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. This blocks 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)
- 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)

15	Sc	а	nCent	Ser sba@cisco.com logged into: Cisco_Smart	Business Architecture Group		Logout He	elp Contact Us	s 💋 S	canSafe
				Home Dashboard	Web Virus Spyware	Web Filtering	nail Ad	min R	eports	Suppor
Man	ager	men	t 🔹 Noti	ifications						
eb Fil	ilterin	a > [Management > Pr	olicy > Manage policy						
				III Manage policy	z 📴 Edit a rule 🛛 🐺 Create	e a rule				
ules	highe e note	er in f	he list will take pr t anonymization r	riority over the lower ones. Use the arrows to char rules are treated separately from the main policy. I	ige the priority of each rule by r ience these appear in a separa	moving them up or down in te part of the table. Thes	n the list. e can be ordered i	n the same way	/ as the re	st of the rul
ules lease nd ar her e	highe e note nonyi re is a	er in e tha mizat a ma	he list will take pr t anonymization r ion will always tal ximum of 100	iority over the lower ones. Use the arrows to char ules are treated separately from the main policy. Is ke precedence. enabled rules allowed for the policy.	ige the priority of each rule by r	noving them up or down in te part of the table. These	n the list. e can be ordered i	n the same way	y as the re	st of the ru
tules Please Ind ar Com #	highe e note nonyi re is a pany Mo	er in f e tha mizat a ma polic ove	he list will take pr t anonymization r ion will always tal ximum of 100 y Rules	ionity over the lower ones. Use the arrows to char rules are treated separately from the main policy. I ke precedence. enabled rules allowed for the policy. Groups/Users/IPs	ige the priority of each rule by r lence these appear in a separat	moving them up or down in the part of the table. These () Schedule	n the list. e can be ordered i Action	n the same way	y as the re	st of the rul Delete
tules lease nd ar here Com # 1	highe e note nonyi re is a pany Mo	er in the mization of the miza	he list will take pi t anonymization r ion will always tal ximum of 100 y Rules Admins	ionity over the lower ones. Use the arrows to char ules are treated separately from the main polcy. I ke precedence. enabled rules allowed for the policy. Groups/Users/IPs "WinNT:/CISCO/Wetwork Device Admin s"	ge the priority of each rule by n ience these appear in a separal Filter *Admins*	© Schedule "anytime"	Action	Active	Edit	st of the rul Delete
tules fease nd ar here Com # 1 2	highe e note nonyi re is a pany Mc	er in f e tha mizat a ma polic ove	he list will take pr t anonymization r ion will always tai ximum of 100 y Rules Admins <u>VPN Users</u>	ionity over the lower ones. Use the arrows to chan ules are treated separately from the main policy. I ke precedence. Groups/Users/IPs WinNT;/CISCOWetwork Device Admin s ⁴ WinNT;/CISCOWpt-user*	ge the priority of each rule by n tence these appear in a separal Filter "Admins" "VPN_Users"	even of the table. These set of tables are set of tables are set of tables are set of tables. These set of tables are set of tables are set of tables are set of tables. These set of tables are set of tables are set of tables are set of tables. These set of tables are set of tables are set of tables are set of tables. These set of tables are set of tables are set of tables are set of tables are set of tables. These set of tables are set of tables are set of tables are set of tables. These set of tables are set of tables are set of tables are set of tables. These set of tables are se	Action Action Allow Marn	Active	Edit	St of the rul
tules lease nd ar There Com # 1 2 3	highe e note nonyr re is a pany Mo 1 1	er in 1 e tha mizat a ma polic ove i i i	t anonymization r ion will always tai ximum of 100 y Rules Admins VPN Users All Users	ionity over the lower ones. Use the arrows to chan ules are treated separately from the main policy. I ke precedence. Groups/Users/IPs WinNT:/CISCOWetwork Device Admin s ⁴ WinNT:/CISCOWetwork Device Admin s ⁴ Anyone	ge the priority of each rule by r tence these appear in a separal Filter "Admins" "VPN_Users" "default"	© Schedule anytime any	Action Action Action Allow All	Active V V V V V V V V V V V V V V V V V V V	Edit Edit E	St of the rul

Procedure 2

Configure 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 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, in the Cisco ScanSafe ScanCenter, navigate to Admin > Downloads > Secure Mobility.

ScanCenter sba@cisco.com logged into: Cisco_Smart Business Architecture Group						
Home Dashboard Web Virus Spyware Web Filtering	Admin Reports					
Your account C Authentication Management Audit C Downloads C						
Secure Mobility						
Select a file to download						
File name and description						
Beacon Server Download 📩						
Release Note for the current version Download						
AnyConnect Web Security Mac Installation Package Download 📩	R.					
Anyconnect Profileeditor (Windows) Download 🖆						
AnyConnect Web Security Windows Installation Package Download 📩						
Sample transforms and documentation Download 📩						
ScarSafe Inc - 590 Elm Avenue, San Bruno, CA 94065 ScarSafe EMEA - Qube, 90 Whiteled Street, London WIT 4EZ, United Kingdom Tel: +1 877 472 2680 - Email: <u>supportBramafe.com</u> Tel: +44 (0) 207 134 9400 - Fax: +44 (0) 207 034 9301 - Email: <u>supportBramafe.com</u>						
© ScanSafe 2011 Contact Us Privacy Policy Disclaimer						

Step 2: Select Beacon Server, 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.

Beacon Server Configuration			2	<
Listening TCP Port	6001			
Errant connections cleanup timeout (secs)	10			
Disallowed IP Addresses (semi-colon separated)	10.4.28.0/22			
		ОК	Cancel	
				_

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: On the Add AnyConnect Client Profile dialog box, in the Profile Name box, enter web_security_profile.

Step 4: In the Profile Usage list, choose Web Security, and then click OK.

🔂 Add AnyConne	ect Client Profile	×
Profile Name	web_security_profile	
Profile Usage	Web Security	
Enter a device f automatically cr	ile path for an xml file, ie. disk0:/ac_profile. The file will be eated if it does not exist.	
Profile Location	disk0:/web_security_profile.wsp	Browse Flash
		Upload
Group Policy	<unassigned></unassigned>	
	Enable 'Always On VPN' for selected group	
	OK Cancel Help	

Step 5: Select the newly created web_security_profile profile, and then click **Edit**.

Step 6: In the Scanning Proxy section, write down the IP addresses of the different proxies. You can also use the Default Scanning Proxy drop-down list to choose a default proxy location that best matches your location.

Step 7: Under Authentication, in the Proxy Authentication License Key box, enter the key for your company-wide group.

Step 8: 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 9: In the Use Enterprise Domains box, enter the domain information to which you wish to apply policy and click **Add**.

🚰 AnyConnect Client Profile Edito	r - web_security_profile			×
Profile: web_security_pr	ofile			About
Web Security	Authentication			
Advanced	Proxy Authentication License Key Service Password	[your license key] [your_password] Use Add Delete	Group Include List	Add Delete
	Authenticated User Authenticated User Authentication Group	Add		
	•	III		Þ
	OK Cance	el Help]	

Step 10: 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.
- Click Browse for the Public Key File, and then navigate to the public key file (DOLpub.pem) you copied in "Configure Beacon Server on LAN" earlier in this guide.
- 5. In the **New Beacon Address** field, enter the address of the server on which the Beacon Server software was installed.

veb_security_prome		
Scarning Proxy Freferences		
Arcepoins Preferences Authentication Advanced		
Automatic Scanning Proxy Selection		
✓ Order Scanning Proxies by Response Time		
Advanced Response Time Settings	1	
lest Inactivity Timeout (min.)	5.	
Beacon Check		
Public Key File	Drawer	
C./Users/[users/	browse	
New Deacon Address	Add	
10 4 48 31	Delete	
	Delet	
Advanced Beacon Settings		
Beacon Port	6001	
Beacon Check Interval (sec.)	300	
DNS Look in Timeout (millin)	3000	
	4	
Port Connection Timeout (sec.)	Line	

Step 11: Click OK, and then Apply.



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.

Step 3: Next to Policy, clear the Inherit check box, and then choose Exclude Network List Below.

Step 4: Next to Network List, clear the Inherit check box, and then click Manage.

Step 5: In **ACL Manager**, click **Add**, and then select **Add ACL**. Use Scansafe_Tower_Exclude for the ACL name.

Step 6: Select the ACL you just created, and then click Add > Add ACE.

Step 7: For the address, add each Cisco ScanSafe scanning proxy address from Step 6 of "Configure ASA VPN policy for web security" earlier in this guide 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.

Standaro	d ACL Extended ACL ▼	↓ % 🗈 💼	v	
No	Address	Action	Description	
🚊 Scan	safe_Tower_Exclude			
1	🖳 72.37.244.179	🖌 Permit	US West Coast	
2	🖳 70.39.231.107	🖌 Permit	US East Coast	=
3	🖳 69.174.58.187	🖌 Permit	US Midwest	
4	🖳 72.37.249.171	🖌 Permit	US South	
5	🖳 69.174.87.75	🖌 Permit	US Southeast	-

Step 8: On the Edit Internal Group Policy dialog box, navigate to Advanced > Split Tunneling, and then, in Network List, choose Scansafe_Tower_Exclude.

Edit Internal Group Policy:	GroupPolicy_AnyConnect			x
General Servers	Split tunneling network lists disti appliance makes split tunneling (inquish networks tha decisions on the basi	t require traffic to go through the tunnel and those that do not require tunneling. The security s of a network list, which is an ACL that consists of list of addresses on the private network.	-
Split Tunneling	DNS Names:	🔽 Inherit		
e AnyConnect Client ⊡-IPsec Client	Send All DNS Lookups Through 1	Tunnel: 👿 Inherit	🔿 Yes 🔿 No	E
	Policy:	📄 Inherit	Exclude Network List Below 🔹	
	Network List:	🔲 Inherit	ScanSafe_Tower_Exclude	
	Intercept DHCP Configura	tion Message fror	n Microsoft Clients 🛞	
				-
Find:	Next 🔘	Previous		
		ОК	Cancel Help	

Step 9: Navigate to Advanced > AnyConnect Client. Under Optional Client Modules to Download, clear the Inherit check box, choose AnyConnect Web Security from the list, and then click OK.

Step 10: In the Always-On VPN section, clear the **Inherit** check box, and then select **Use AnyConnect Profile setting**.

Step 11: In the Client Profiles to Download section, click Add, select the **web_security_profile** for Profile Name and web security for Profile Usage, and then click OK.

General	Keep Installer on Client System:	Inherit 🔿 Yes 💿 No	
-Servers -Advanced	Compression:	🕼 Inherit 💿 Enable 💿 Disable	
Split Tunneling Browser Proxy	Datagram TLS:	🕼 Inherit 🔿 Enable 🔿 Disable	
AnyConnect Client IP-IPsec Client	Ignore Don't Fragment(DF) Bit:	🕼 Inherit 🔿 Enable 🔿 Disable	
	Keepalive Messages:	☑ Inherit Disable Interval: seconds	
	MTU:	V Inherit	
	Optional Client Modules to Download:	Inherit websecurity	• 6
	Always-On VPN:	Inherit O Disable O Use AnyConnect Profile setting	g 🔞
	Client Profiles to Download:	Inherit	
		Add 1 Delete	
		Profile Name	Profile Usage/Type
		ra profile	VPN
		web_security_profile	Web Security
Find:	Next OP	(web_security_profile	Web Searity

Step 12: Click OK, and then Apply.

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-asa5545.cisco.local

Step 2: Log in 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.

Login			
Please enter your username and password.			
GROUP:	AnyConnect -		
USERNAME:	employee1		
PASSWORD:	•••••		
Login			

Step 3: When connected, click the Cisco AnyConnect taskbar icon. This displays the client information panel.

CISCO Secure Mobility Client			
VPN: Connected to VPN-ASA5525. VPN-ASA5525 VPN-ASA5525			
Web Security: Enabled (US West Coast)			
Advanced			

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.

CISCO Secure Mobility Client VPN Connection Required			
VPN: Ready to connect. VPN-ASA5525 VPN-ASA5525			
Web Security: Enabled (US West Coast)			
Advanced			

Procedure 6

Test Beacon Server functionality

Step 1: Select a client that is connected outside the network and has the Web Security module enabled, and then move that client 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 Beacon Server. The ability to connect to 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 websites are now secured by the organization's Internet edge devices and policy.

CISCO Secure Mobility Client			
■ VPN: Ready to connect. VPN-ASA5525	Connect		
Web Security: On a trusted network.			
Advanced			

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 headend 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 end users 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.

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 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 Auto Connect On Start and Auto Reconnect, and, if policy permits, select User Controllable. In the Auto Reconnect Behavior list, ensure ReconnectAfterResume is chosen.

Step 3: In Preferences (Part 2), select Automatic VPN Policy.

Step 4: In the Trusted Network Policy list, choose **Disconnect**, and then, 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**.

🖆 AnyConnect Client Profile Editor - ra_profile				
Profile: ra_profile				About
Preferences (Part 1)	es (Part 2)			
Backup Servers	☑ Disable Automatic Certificate Selection		V User Controllable	Â
Certificate Enrolment Proxy Setting	s		Native	
Server List	al Proxy Connections			
Enable O	ptimal Gateway Selection		User Controllable	
Susper	sion Time Threshold (hours)		4	
Perfor	nance Improvement Threshol	ld (%)	20	
Automat	c VPN Policy			
Truster	Network Policy		Disconnect 👻	=
Untrus	ed Network Policy		Connect 🔹	
Truster	I DNS Domains			
Truster	DNS Servers		10.4.48.10	
Ah	rays On		(More Information)	
	Allow VPN Disconnect			
	Connect Failure Policy		Closed 👻	
	Allow Captive Porta	al Remediation		
	Remediation Timeout (n	nin.)	5	
	Apply Last VPN Loc	al Resource Rules		
PPP Exclusion		Disable 👻	User Controllable	
PPP Exclusion	Server IP		User Controllable	
Enable S	ripting		User Controllable	
	minate Corint On Next Event			-
•		m		4
	OK	Cancel Help		

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).

	CISCO Secure Mobility Client			
	✓ VPN: On a trusted network. VPN-ASA5525 ✓ Connect			
I	Web Security: On a trusted network.			
Advanced				

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.

CISCO Secure Mobility Client			
VPN: Connected to VPN-ASA5525.			
Web Security: Enabled (US West Coast)			
Advanced			

Procedure 9

Install the certificate on the client

As described in the *Remote Access VPN Deployment 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 certificate authority (CA) don't need to be manually added.

Because some of the features configured later in this guide involve automatic certificate checking, it isn't acceptable to have the errors show up when self-signed certificates are used. This procedure solves the error problems.

Publicly signed certificates do not have these issues and are easier to use in practice.

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

https://vpn-asa5525.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. Publicly 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://vpn-asa5525.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 unin- stalled 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 Always On and Allow VPN Disconnect.

AnyConnect Client Profile Edi	tor - ra_profile		×
Profile: ra_profile			About
VPN	Preferences (Part 2)		
Backup Servers Certificate Matching Certificate Enrollment Mobile Policy Server List	Disable Automatic Certificate Selection Proxy Settings Allow Local Proxy Connections	V User Controllable Native	
	Enable Optimal Gateway Selection	User Controllable	
	Suspension Time Threshold (hours)	4	
	Performance Improvement Threshold (%)	20	
	Automatic VPN Policy		
	Trusted Network Policy	Disconnect	=
	Untrusted Network Policy	Connect	
	Trusted DNS Domains		
	Trusted DNS Servers	10.4.48.10	
	🕼 Always On	(More Information)	
	Allow VPN Disconnect		
	Connect Failure Policy	Open 👻	
	Allow Captive Portal Remediation		
	Apply Last VPN Local Resource Rules	5	
	PPP Exclusion Disable	User Controllable	
	PPP Exclusion Server IP	User Controllable	
	Enable Scripting	User Controllable	
	Torminato Scrint On Novt Suppt		τ •
	OK Cancel Help		

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

Cisco AnyConnect Secure Mobility Client			
AnyConnect Secure Mobility Client			
Status Overview	Virtual Private Network (VPN)		
VPN >	Preferences Statistics Route Details Firewall	Message History	
Web Security	Connection Information State: Connected Mode: All Traffic Duration: 00:11:07 Bytes Sent: 340907 Received: 385969 Frames	Address Information Client (IPv4): 10.4.28.16 Client (Pv6): Not Available Server: 172.16.130.122 Transport Information Protocol: Protocol: IKEv2/IPsec NAT-T Cipher: AS5_256_SHA1 Compression: None	
Collect diagnostic information for all installed components.	Sent: 1783 Received: 1730 Control Frames Sent: 53 Received: 39 Client Management Administrative Domain: 172.16.130.122	Proxy Address: No Proxy Peature Configuration FIPS Mode: Disabled Trusted Network Detection: Enabled Always On: Enabled Secure Mobility Solution Status: Unconfirmed Appliance: Not Available	
Diagnostics		Reset Export Stats	

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. Configure the DMZ firewall
- 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 Internet Security and Acceleration (ISA) server in their demilitarized zones (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 steps in this guide assume that the setup and configuration of ISA, Exchange, and ActiveSync is complete and functional. 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

Configure the DMZ firewall

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 server 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 then enter the required data.

🔂 Add Interface	×
General Advanced IPv6	
Hardware Port: GigabitEthernet0/1 👻	
VLAN ID: 1122	
Subinterface ID: 1122	
Interface Name: dmz-isa	
Security Level: 50	
Dedicate this interface to management only	
Channel Group:	
IP Address	
IP Address: 192 168 22 1	
Subnet Mask: 255.255.0	
Description: Interface to the ISA DMZ	
OK Cancel Help	

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 GigabitEthernet1/0/24

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 Network Address Translation (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 > Objects > Network Objects/Groups

Step 2: Click Add > Network Object.

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

付 Edit Network	Object 📃 📉	
	W.	
Name:	dmz-isa-ISPa	
Type:	Host	
IP Address:	172.16.130.55	
Description:	ISA Server outside ISP A address	
NAT	*	
	OK Cancel Help	

Step 4: Navigate to Configuration > Firewall > NAT Rules, and then click Add Network Object NAT rule. This creates 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 configuration, and then enter its actual address.

Step 6: Under NAT, select **Add Automatic Address Translation Rules**, in Type, choose **Static**, in Translated Addr, choose the ISA server network object that references the public address of the ISA server created in Step 3, and then click **OK**.

Edit Network	Object	x			
Name:	dmz-isa_srvr				
Type:	Host	•			
IP Address:	192.168.22.25				
Description:	Address of ISA server in dmz-isa				
NAT		۲			
Add Automa	tic Address Translation Rules				
Type:	Static 👻				
Translated Ac	ldr: dmz-isa-ISPa				
PAT Pool	Translated Address:				
Round Robin					
Fall through to interface PAT(dest intf): dmz-dmvpn					
Advanced					
OK Cancel Help					

Step 7: Navigate to Configuration > Firewall > Access Rules, and then click Add > Add Access Rule.

Step 8: In the Edit Access Rule window, enter the following information:

- Interface—Any
- Action—Permit
- Source—Any
- Destination—dmz-isa_srvr
- Service—tcp/http and tcp/https

This adds a new access control entry (ACE) rule to the global list of access rules. The rule allows outside hosts to make HTTP and HTTPS connections to the ISA server.

Edit Acce	ss Rule
Interface:	Any
Action:	Permit O Deny
Source:	any
User:	
Destination	dmz-isa_srvr
Service:	tcp/http, tcp/https
Description:	Opening up access ports to ISA on DMZ
🔽 Enable Lo	ogging
Logging L	evel: Default 🗸
More Opt	ions 🛞
	OK Cancel Help

Next, Create another Cisco ACE. This allows the ISA server access to the internal Exchange server,

Step 9: In the Edit Access Rule window, enter the following information:

- Interface—Any
- Action—Permit
- Source—dmz-isa_srvr
- Destination—internal-exchange
- Service—tcp/http and tcp/https

📑 Edit Acce	ss Rule
Interface:	Any
Action: 🔘	Permit O Deny
Source:	dmz-isa_srvr
User:	
Destination	internal-exchange
Service:	tcp/http, tcp/https
Description:	
🔽 Enable Lo	ogging
Logging L	evel: Default 🔻
More Opt	ions 🛞
	OK Cancel Help

Step 10: Permit access, using the examples above, from the ISA server to the Active Directory server 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, 49158, and 49164 and UDP 389 and the DNS server portion requires UDP 53.

#	Enabled	Source	User	Destination	Service	Action
10		🖳 dmz-isa_srv		🚇 internal-dns	ICIII» echo ICIII» echo-reply ICIP 1025 ICIP 135 ICIP 445 ICIP 49158 ICIP 49164 ICIP 389 ICIP domain	✓ Permit

Step 11: Move these access rules above any rule already configured that denies DMZ networks access to other networks.

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: On the **Password** tab, set password requirements for Exchange ActiveSync clients, as follows:

- 1. Select Require password.
- 2. Select **Allow simple password.** This check box allows pin-numberstyle simple passwords (a minimum level of security but easy to type and remember).
- 3. Select Require encryption on device.
- 4. Enter a number for **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 for **Time without user input before password must be re-entered**.
- 6. Click OK



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 host name (VPN-ASA5525), and then click **Edit**.

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

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

Host Display Name (required) VPN-ASA5525 FQDN or IP Address vpn-asa5525.cisco.local	User Group	Additional mobile-only settings Edit
Group URL vpn-asa5525.cisco.local/AnyConnect		Mobile Settings Apple IOS / Android Settings
Backup Server List Host Address 172.17.130.122	Add Move Up Move Dowr Delete	Certificate Authentication: Automatic Clent Certificate will never be used for authentication. Make this Server List Entry active when profile is imported Apple IOS Only Settings Reconnect when roaming between 3G / Wifi networks Connect on Demand (requires certificate authentication)
Primary Protocol	SSL	On Demand Action Never Connect
Auth Method During IXE Negotation IXE Identity	IKE-RSA	Match Domain or Host On Demand Action

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, enter ASA SSL in the Description field, enter vpn-asa5525.cisco.local in the Server Address field, and then click Save.

••••• AT&T 🤝 7:	:22 AM	65 % 💻
Cancel Add VP	N Conr	IEC Save
Description	ASA SS	SL.
Server Address	.sa5525.c	isco.local 🗴
Network Roam	ing	ON
Certificate		Disabled >
QWER ASDF & ZXC	G H V B	JIOP JKL NM 💌
@123	/ .c	om return

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 username and password for authentication, and then click **Connect**. The following screens show example connection tests for the iOS and Android operating systems.

Example: iOS Operating System Connection

aall AT&T 🗢 🔆		12:25		25 %
cisco An	yConnect Secu	re Mobility Clie	ent	
AnyConnect	VPN		Graphs Diagnostics	
Status	Connecting		Bytes Received	
Choose a conne	ection			
✓ ASA S	Cancel	Authentication	Connect	
asa552	Please enter your userr	name and password.		
asa552	Group:		AnyConnect >	
Add Vi	Username: e	mployee1		
	Password:	•••••		
	10000			
Status Over				
Server				
Time Con				
Client Addre	ss Not Availab	le 285 Bytes		
Bytes Sent		0 190 Bytes		
Bytes Receiv	/ed	0 95 Bytes		
Details		>		
and the second				

uliatat 🗢 Ven		7:25	30%
cisco AnyConn	ect Secure N	Mobility Client	out
AnyConnect VPN	ON	Graphs Diagnostics	
Status	Connected	Bytes Received	
Choose a connection			
2500asa	۲	475 Bytes	
🖌 ASA SSL	\odot	285 Bytes	
RA VPN 1K	$\overline{\mathbf{O}}$	190 Bytes	
RA VPN ENT	$\overline{\mathbf{O}}$	95 Bytes	
VPN-ASA5525	۲	07:25:04 AM 07:25:24 AM 07:25:44 AM	n
Status Overview		Bytes Sent	
Server vpn-asa5	525.cisco.local	475 Bula	
Time Connected	00:01:03	380 Bytes	
Client Address	10.4.28.2	285 Bytes	
Bytes Sent	0	190 Bytes	
Bytes Received	1077	95 Bytes	
Details	>	07:25:24 AM 07:25:24 AM 07:25:44 AM	1

Example: Android Operating System Connection

M	🕀)) 🛜 🎢 📒 7:35 AM
Connection Editor	
Description ASA SSL	O
Server Address vpn-asa5525.cisco.local	\odot
Certificate Automatic	
Done	Cancel
۱۱۱۰۱۱۰، AnyConnect CISCO secure Mability Client	
AnyConnect VPN Connecting to ASA SSL	
Choose a connection	
Any Please enter your username and password. Group	Connect
AnyConnect	•
employee1	
Password	
Show password(s).	
OK	Cancel

× 🕋	🕀 🦃 ኛ 🏹 든 7:37 AM
CISCO Secure Mobility Client	
AnyConnect VPN Connected to ASA SSL	
Choose a connection	
ASA SSL	
SBA-A	
VPN-ASA5525	
Add New VPN Connection	

Notes	

Appendix A: Product List

Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 8.6(1)1 IPS 7.1(4) 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	6.6.114
RA VPN Firewall	Cisco ASA 5545-X Firewall Edition - security appliance	ASA5545-K9	8.6(1)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	
	Firewall Management	ASDM	6.6.114
Mobile License	AnyConnect Essentials VPN License - ASA 5545-X (2500 Users)	ASA-AC-E-5545	-
	AnyConnect Essentials VPN License - ASA 5525-X (750 Users)	ASA-AC-E-5525	
	AnyConnect Essentials VPN License - ASA 5515-X (250 Users)	ASA-AC-E-5515	
	AnyConnect Essentials VPN License - ASA 5512-X (250 Users)	ASA-AC-E-5512]
SSL Software License for ASA	ASA 5500 SSL VPN 500 Premium User License	ASA5500-SSL-500	_
	ASA 5500 SSL VPN 250 Premium User License	ASA5500-SSL-250	

VPN Client

Functional Area	Product Description	Part Numbers	Software
Mobile Device VPN Client	Cisco AnyConnect Secure Mobility Client	Cisco AnyConnect Secure Mobility Client	2.5.5130
VPN Client	Cisco AnyConnect Secure Mobility Client	Cisco AnyConnect Secure Mobility Client	3.0.07059
ScanSafe	ScanSafe	Please Contact your Cisco Scansafe Sales Representative for Part Numbers: scansafe-sales-questions@cisco.com	—

Appendix B: Configuration Files

```
RAVPN ASA5525-X
ASA Version 8.6(1)1
1
hostname VPN-ASA5525
domain-name cisco.local
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
L
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
1
interface GigabitEthernet0/1
 shutdown
 no nameif
 no security-level
no ip address
L
interface GigabitEthernet0/2
description LAN/STATE Failover Interface
L
interface GigabitEthernet0/3
 no nameif
no security-level
no ip address
1
```

interface GigabitEthernet0/3.16 description Prymary Internet connection VLAN 16 vlan 16 nameif outside-16 security-level 0 ip address 172.16.130.122 255.255.255.0 standby 172.16.130.121 Т interface GigabitEthernet0/3.17 description Resilient Internet connection on VLAN 17 vlan 17 nameif outside-17 security-level 0 ip address 172.17.130.122 255.255.255.0 standby 172.17.130.121 1 interface GigabitEthernet0/4 shutdown no nameif no security-level no ip address 1 interface GigabitEthernet0/5 shutdown no nameif no security-level no ip address 1 interface GigabitEthernet0/6 shutdown no nameif no security-level no ip address 1 interface GigabitEthernet0/7 shutdown no nameif no security-level no ip address

I. interface Management0/0 shutdown no nameif no security-level no ip address management-only ftp mode passive clock timezone PST -8 clock summer-time PDT recurring dns domain-lookup inside dns server-group DefaultDNS name-server 10.4.48.10 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 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 Scansafe Tower Exclude remark US West Coast access-list Scansafe Tower Exclude standard permit host 72.37.244.179 access-list Scansafe Tower Exclude remark US East Coast access-list Scansafe Tower Exclude standard permit host 70.39.231.107 access-list Scansafe Tower Exclude remark US Midwest access-list Scansafe Tower Exclude standard permit host 69.174.58.187 access-list Scansafe Tower Exclude remark US South

access-list Scansafe Tower Exclude standard permit host 72.37.249.171 access-list Scansafe Tower Exclude remark US Southeast access-list Scansafe Tower Exclude standard permit host 69.174.87.75 access-list DEFAULT-ONLY standard permit any access-list test extended permit ip any any pager lines 24 logging enable logging buffered informational logging asdm informational mtu inside 1500 mtu outside-16 1500 mtu outside-17 1500 ip local pool RA-pool 10.4.28.1-10.4.31.255 mask 255.255.252.0 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 10.4.24.97 255.255.258.248 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-66114.bin 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 1 router eigrp 100 no auto-summary

no default-information 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 0.0.0.0 172.16.130.126 128 track 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 sipdisconnect 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 kev ***** aaa-server AAA-RADIUS protocol radius aaa-server AAA-RADIUS (inside) host 10.4.48.15 timeout 5 kev ***** 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 ca trustpoint ASDM TrustPoint0 enrollment self subject-name CN=VPN-ASA5525.cisco.local keypair sslpair proxy-ldc-issuer crl configure crypto ca certificate chain ASDM TrustPointO certificate 3elffb4f 30820270 308201d9 a0030201 0202043e 1ffb4f30 0d06092a 864886f7 0d010105 0500304a 3120301e 06035504 03131756 504e2d41 53413535 32352e63 6973636f 2e6c6f63 616c3126 30240609 2a864886 f70d0109 02161756 504e2d41 53413535 32352e63 6973636f 2e6c6f63 616c301e 170d3132 30373039 31393034 34325a17 0d323230 37303731 39303434 325a304a 3120301e 06035504 03131756 504e2d41 53413535 32352e63 6973636f 2e6c6f63 616c3126 30240609 2a864886 f70d0109 02161756 504e2d41 53413535 32352e63 6973636f 2e6c6f63 616c3081 9f300d06 092a8648 86f70d01 01010500 03818d00 30818902 818100d6 2c54cc0b fe1cffa0 ba51f93a 7d0017b1 e17a7765 31a16ee9 f9153059 a81d6ee0 c7b98f84 09930b89 5affdb5c 7ac8cd8f 7b155d3f 9e82d041 b4979a16 df782104 f88877d7 8b22c3eb 3828b31f b2440c42 2102cf43 1ae023db 962c5224 0a6225af 11a2dc48 02e1dc72 8be4a007 42739a90 7cb16882 9815cd9f 576aa4b7 7bb4cf02 03010001 a3633061

300f0603 551d1301 01ff0405 30030101 ff300e06 03551d0f 0101ff04 04030201 86301f06 03551d23 04183016 80148d1b 53b7eff9 ebf29730 4632e70c cd0922ea 3e75301d 0603551d 0e041604 148d1b53 b7eff9eb f2973046 32e70ccd 0922ea3e 75300d06 092a8648 86f70d01 01050500 03818100 75ed2963 73550666 41e45b97 396e53d6 9b6275bc efd1ab39 31f73846 26b692b6 57579bf4 32b41d9b 02037ad1 aaa2cbec 14fc0739 59c1706f 1bf0d8aa 6bdae10a 737c2085 e8bc59a1 01f88043 b4010901 3cf81fe9 093b6dc2 cc3122e5 3086c76e 422fce7b a836736e 126c3416 f45c50a5 64e956ac e8802127 b292d041 817fd51f quit crypto ikev2 remote-access trustpoint ASDM TrustPoint0 1 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 trust-point ASDM TrustPoint0 outside-16 ssl trust-point ASDM TrustPoint0 outside-17 webvpn enable outside-16 enable outside-17 anyconnect-essentials anyconnect image disk0:/anyconnect-linux-3.0.07059-k9.pkg 1 anyconnect image disk0:/anyconnect-macosx-i386-3.0.07059-k9.pkg 2 anyconnect image disk0:/anyconnect-win-3.0.07059-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 dart, 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 acess is via unrestricted split tunnel. split-tunnel-policy tunnelall 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 restricted to the partner server vpn-filter value RA PartnerACL webvpn anyconnect profiles value ra profile type user username admin password w2Y.60p4j7clVDk2 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://172.16.130.122/AnyConnect enable
group-url https://172.17.130.122/AnyConnect enable
L
class-map inspection default
match default-inspection-traffic
L
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
I.
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 23
subscribe-to-alert-group telemetry periodic daily
```

Appendix C: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We updated the guide to reflect the changes to products and software used in the *Firewall and IPS Deployment Guide*.
- We made minor changes to improve the readability of this guide.



Feedback

Click here to provide feedback to Cisco SBA.



SMART BUSINESS ARCHITECTURE

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITH-OUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY OF USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY OF USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS ON ON CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.



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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)