Guide

Cisco AnyConnect Deployment Guide for Cisco Jabber

October 2012

Contents

Introduction

The Cisco AnyConnect® Secure Mobility Client is the industry-leading multiservice client that provides an intelligent and optimized connection while helping ensure a secure session. The Cisco Jabber™ client enables collaboration across a multitude of devices, including laptops, smartphones, and tablets. The Jabber client also provides rich unified communications capabilities such as voice and video, instant messaging (IM), presence, visual voicemail, web conferencing, desk phone integration, and more. To meet the needs of an increasingly mobile workforce, the Jabber client requires secure access to the unified communications (UC) servers. This deployment guide discusses the various AnyConnect features[1] used to secure and improve the user experience with Jabber, offering configuration steps and best practices.

The target audience includes security and collaboration engineers and anyone seeking an understanding of what it takes to implement the Jabber and AnyConnect solution. Some prior knowledge of Cisco AnyConnect, ASA, Jabber, and Unified Communications Manager is helpful, though not required. After reading this document, the reader should have a good understanding of the components involved in the solution and will be well equipped to review other detailed collateral.

Cisco ASA 5500 Series SSL/IPsec VPN Edition[2]

The Cisco® ASA 5500 Series SSL/IPsec VPN Edition offers flexible VPN technologies for any connectivity scenario, with scalability up to 10,000 concurrent users per gateway. It provides easy-to-manage, full-tunnel network access through SSL, Datagram Transport Layer Security (DTLS), IP Security (IPsec) VPN client technologies, advanced clientless SSL VPN capabilities, and network-aware site-to-site VPN connectivity, enabling highly secure connections across public networks to mobile users, remote sites, contractors, and business partners.

Cisco AnyConnect Secure Mobility Client[3]

The Cisco AnyConnect Secure Mobility Client provides a highly secure connectivity experience across a broad set of PCs, tablets, and smartphone-based mobile devices, such as the Apple iPhone and Android. As mobile workers roam to different locations, an always-on intelligent VPN enables the AnyConnect Secure Mobility Client to automatically select the most optimal network access point and adapt its tunneling protocol to the most efficient method, including the DTLS protocol for latency-sensitive traffic such as voice over IP (VoIP) traffic or TCP-based application access.

Note: The AnyConnect client connects to the ASA head-end to terminate the VPN connection. Hence, both products are required to provide secure remote access to the Jabber client.

---

[1] Complete list of AnyConnect features:http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/vpn_anyconnect.html

[2] ASA datasheet: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd80402e3f.html

[3] AnyConnect datasheet: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/data_sheet_c78-527494.pdf

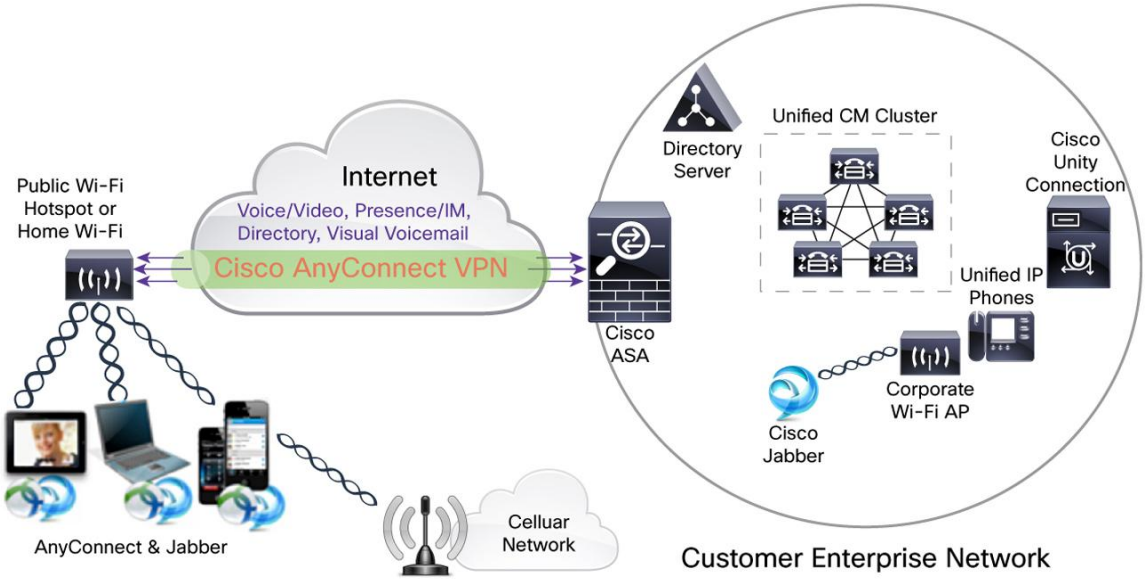
Cisco Jabber[4,5,6]

Cisco Jabber is a unified communications application that enables users to be more productive from anywhere on any device. Cisco Jabber for Windows streamlines communications and enhances productivity by securely unifying presence, instant messaging, video, voice, voice messaging, desktop sharing, and conferencing capabilities into one client on the Windows desktop. Cisco Jabber for iPhone lets users place, receive, and manage calls over their corporate Wi-Fi network. Cisco Jabber for iPhone also supports calls over any Wi-Fi hotspot using a VPN, allowing users to take further advantage of Cisco IP telephony infrastructure within the company. Cisco Jabber for iPad not only provides a complete set of unified communications capabilities but also offers deployment flexibility for administrators.

Solution Topology

Figure 1 shows how Cisco AnyConnect and Jabber fit into the network topology.

Figure 1. Topology



VPN Initiation on iOS

1. The remote end user launches the Jabber client.
2. The Jabber client triggers the iOS On-Demand VPN feature, and the AnyConnect client establishes an SSL VPN connection with the ASA VPN gateway, using certificate-based authentication.

Note: The Apple iOS On-Demand VPN feature requires certificate-only authentication. For non-certificate authentication options, the end user has to manually initiate the AnyConnect VPN connection as needed.

[4] Cisco Jabber for iPhone: http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps7290/ps11156/data_sheet_c78-658146.html
[5] Cisco Jabber for Windows: http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps6836/ps12511/data_sheet_c78-704195.html
[6] Cisco Jabber for iPad: http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps6836/ps12430/data_sheet_c78-704194.html

VPN Initiation on Windows, Mac OS X, and Android*

1. As soon as the end user connects to noncorporate Wi-Fi or 3G cellular networks, the Trusted Network Detection feature of the AnyConnect VPN client initiates an SSL VPN connection.
2. The AnyConnect client establishes an SSL VPN connection with the ASA VPN gateway, using certificate-based authentication.

Note: The Trusted Network Detection feature is currently not available with the Android ICS (generic) version of AnyConnect. Hence, the end user has to manually initiate the VPN connection as needed. For support for other Android devices, please see the release notes.[7]

Connection Flow After Establishing VPN on All Devices

3. The Jabber client will connect to Cisco Unified Communications appliances to provide unified communications services over the VPN connection.
4. The Jabber client is then ready to place or receive voice or video calls, etc.

Recommended Licensing and Software Versions

Table 1 lists the supported platforms, required licenses, and minimum software version recommended.

Table 1. Supported Platforms

Device/Component	Licenses Required	Recommended Version
ASA[8] VPN Gateway	AnyConnect Essentials and AnyConnect Mobile[9]	ASA 8.4 or above
Adaptive Security Device Manager (ASDM)		ASDM 6.4 or above
AnyConnect for Mac OS and Windows		AnyConnect 3.0 or above
AnyConnect for iOS and Android		AnyConnect 2.5
Jabber	See Ordering Guide	See the links to datasheets on previous page.

Note: AnyConnect also offers a premium license that will be required to enforce posture assessment of the device before allowing the VPN connection. For the Jabber specific deployment covered in this guide, AnyConnect Essentials and AnyConnect Mobile licenses are sufficient.

Configuration Best Practices

This section discusses best practices to help ensure a seamless user experience when using Cisco Jabber outside the corporate network with Cisco AnyConnect. The user experience can be divided into four stages:

1. **Install:** Download and install the applications.
2. **Provision**: Provision the Jabber[10,11,12] and AnyConnect clients.
3. **Connect**: Establish a VPN connection for everyday use, including certificate enrollment.

---

[7] AnyConnect 2.5 on Android - release notes: http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect25/release/notes/rn-ac2.5-android.html

[8] ASA platforms: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_bulletin_c25-586414.html

[9] ASA licensing: http://www.cisco.com/en/US/docs/security/asa/asa84/license/license_management/license.html

[10] Jabber for iPad Administration Guide: http://www.cisco.com/en/US/products/ps12430/prod_installation_guides_list.html

[11] Jabber for Android Administration Guide: http://www.cisco.com/en/US/products/ps11678/prod_installation_guides_list.html

[12] Jabber for iPhone Administration Guide: http://www.cisco.com/en/US/products/ps11596/prod_installation_guides_list.html

4. **Session**: Enhance the connection experience after establishing the VPN.

We will discuss various administrative configuration best practices for each of the four stages.

Note: All of the ASA and AnyConnect VPN features we discuss are applicable to other applications. However, administrators who wish to manage Jabber specific VPN session parameters separately should create separate ASA connection profiles (also known as tunnel groups), group policies, and AnyConnect client profiles as needed.

Installing the Applications

iOS and Android Devices

Option 1: End users can manually download the Cisco AnyConnect and Cisco Jabber apps at no cost from the respective Apple App Store or Google Play. Administrators can also host an internal web page with links that redirect the user to the respective app stores.

Option 2: Enterprises can take advantage of the Mobile Device Manager (MDM) software to push the two applications after device registration.

Windows and Mac OS X

Option 1: Administrators can use System Center Configuration Manager (SCCM) to push the Cisco AnyConnect and Jabber applications to the laptops.

Option 2: AnyConnect can be downloaded and installed from a web portal hosted by the Cisco ASA.[13]

Note: The initial installation of AnyConnect through web download (WebLaunch) requires administrative privileges on the endpoint.

Provisioning the AnyConnect VPN Profiles

After the apps are downloaded, they have to be provisioned with the configuration profile. The AnyConnect client profile includes VPN policies such as a list of all the company ASA VPN gateways, connection protocol (IPsec or SSL), on-demand policies, etc.

Provision VPN Profiles on ASA[14] - Preferred Method

The ASDM includes a profile editor that can be used to define the VPN profile. The VPN profile will be downloaded to the AnyConnect client after the VPN connection is established for the first time. This auto-download option is the preferred method, as it can be used for all the devices and OS types and can be managed centrally on the ASA.

Note: On Windows, the VPN profile can also be deployed as part of a SCCM push of the AnyConnect client.

iOS Devices Using Apple Configuration Profiles - Alternative Method

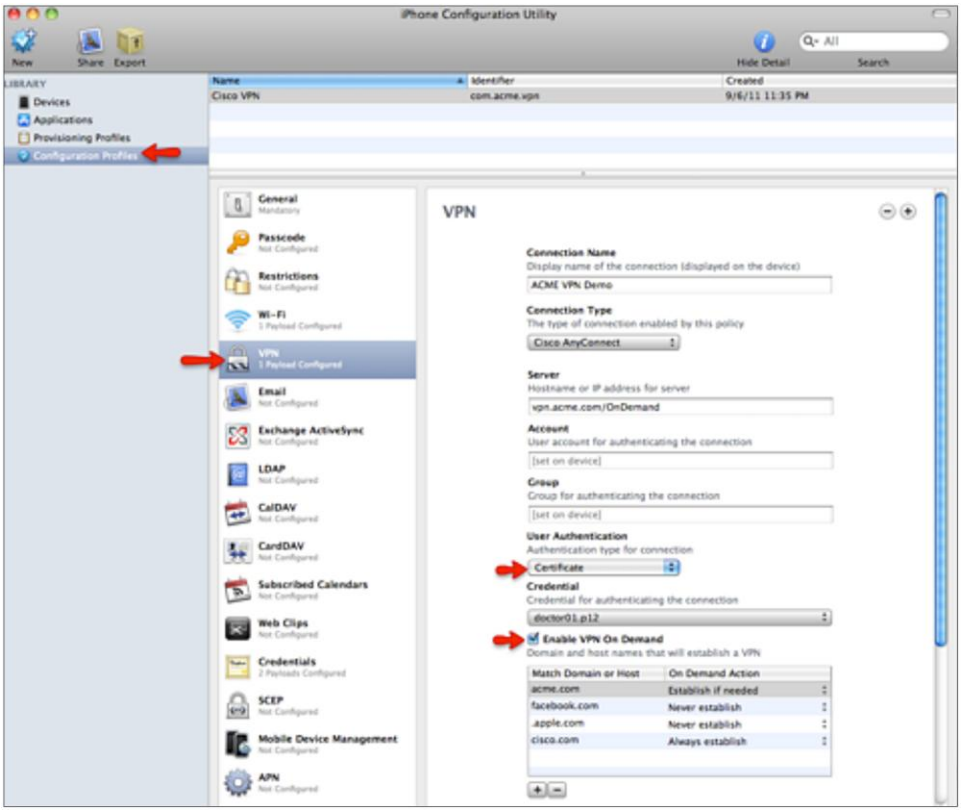
Many enterprises provisioning iOS devices would like to take advantage of the Apple configuration profiles. The Apple configuration profiles are XML files that contain device security policies, VPN configuration information, Wi-Fi settings, mail and calendar settings, etc.

---

[13] WebLaunch:
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/ac01intro.html#wp1055173

[14] AnyConnect Profile Editor:
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/ac02asaconfig.html#wp1289905

Figure 2. iPhone Configuration Utility



Option 1: An administrator can create the Apple configuration profile using the iPhone Configuration Utility (iPCU) software (Figure 2). This XML profile can be exported from the iPCU as a .mobileconfig file, which will be emailed to the end user. When the user opens the file, the AnyConnect VPN profile will be installed along with all other profile settings.

Option 2: Enterprises can use Mobile Device Management (MDM) software to define and push the Apple configuration profiles to the registered devices.

Simplifying Connection Establishment

When the user launches Jabber, the client then invokes the AnyConnect client to secure the session between the end-user device and the Cisco Unified Communications application servers. The AnyConnect client offers many features that help ensure a seamless Jabber experience.

Connect on Demand VPN[15] for iOS Devices

Apple's On-Demand VPN feature enables the Jabber client to initiate a VPN connection in the background, thus freeing the user from having to manually interact with the AnyConnect application.

[15] Connect on Demand: http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect25/iOS-user/guide/iphone-ugac-ios.html#wp179705

The Apple iOS Connect on Demand feature enables the establishment of VPN connections specified in the **domain list** without user interactions. All applications on the device, including Cisco Jabber, can take advantage of this feature. Connect on Demand supports only certificate-authenticated connections.

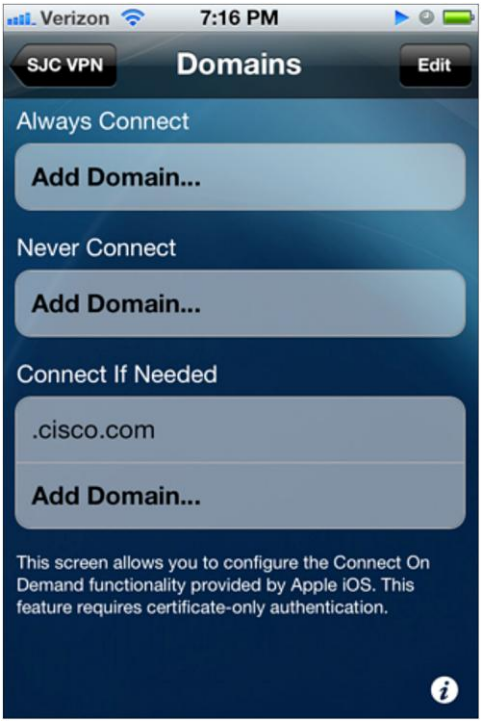
Three options are available with this feature.

Always Connect: For domains in the Always Connect list, Apple iOS will always attempt to initiate a VPN connection.

Connect If Needed: For domains in the **Connect If Needed** list, Apple iOS will attempt to initiate a VPN connection only if it could not resolve the address using DNS.

Never Connect: Apple iOS will never attempt to initiate a VPN connection to addresses in the **Never Connect** list.

Figure 3. Domain List for On-Demand VPN



Step 1. In the AnyConnect client profile, define an on-demand domain list under the **Connect If Needed** list. The domain list can include wild-card options, such as **.cisco.com** (Figure 3). As explained earlier, this profile can be created using the ASDM profile editor or iPCU or MDM software.

Step 2. Configure the On-Demand VPN URL as part of the Jabber device settings under Cisco Unified Communications Manager. For example, let's say we entered ccm-sjc-1.cisco.com as the On-Demand VPN URL (See Appendix A1).

When Jabber is launched, it will initiate a DNS query to the URL ccm-sjc-1.cisco.com. Since this URL matches the On-Demand domain list entry (.cisco.com) defined in **step 1,** the AnyConnect VPN connection will be initiated.

Note: There is a known defect (**CDETS**): The On-Demand VPN functionality does not work with Jabber on the iPad. However, It does currently function with the Apple iPhone version.

Trusted Network Detection[16] for Windows, Mac OS X, and Android

The Trusted Network Detection (TND) feature enhances the user experience by automating the VPN connection based on user location. When the user is inside the corporate network, Jabber can reach the Cisco Unified Communications infrastructure and hence does not require VPN. However, as soon as the user leaves the corporate network, the VPN will be initiated to ensure Jabber's connectivity to the Unified Communications infrastructure. The TND feature is configured in the AnyConnect client profile using ASDM.

The administrator defines the list of **trusted DNS servers** and **trusted DNS domain suffixes** that an interface may receive when the client is on a corporate network. The AnyConnect client will compare the current interface DNS servers and domain suffix with the settings in the profile.

Note: You must specify all the DNS servers for TND to work. If you configure both the trusted DNS domains and trusted DNS servers, sessions must match both settings to be considered in the trusted network.

Note: TND works for both certificate- and password-based authentication. However, certificate-based authentication provides the most seamless experience.

Certificate-Based Authentication

The AnyConnect client supports many authentication methods, including Active Directory (AD)/Lightweight Directory Access Protocol (LDAP) password, RADIUS-based one-time tokens, certificates, and more. Of all the methods, client certificate authentication enables the most seamless experience. Please see the Cisco ASA configuration guide[17] for a detailed explanation of certificates for VPN authentication.

Configuring ASA for Certificate Authentication

The Cisco ASA supports certificates issued by various standard certificate authority (CA) servers, such as Cisco IOS® CA, Microsoft Windows 2003, Windows 2008 R2, Entrust, VeriSign, RSA Keon, etc. There are five steps to enable certificate authentication on the ASA.

Step 1. Import a root certificate from the CA to the ASA.

Step 2. Generate an identity certificate for the ASA.

Step 3. Use the ASA identity certificate for SSL authentication.

Step 4. Configure the Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP).

Step 5. Configure the ASA to request client certificates for authentication.

[16] TND: http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect25/administration/guide/ac03features.html#wp1059922

[17] Certificates on ASA: http://www.cisco.com/en/US/docs/security/asa/asa84/asdm64/configuration_guide/access_certs.html#wp1637463

Distributing Client Certificates

iOS, Android, Windows, and Mac OS X:

1. The ASA supports the Simple Certificate Enrollment Protocol (SCEP) to simplify certificate distribution.

iOS Devices Specific

2. Use the iPCU software to create a .mobileconfig file and include the certificate (.pfx) file. The administrator can then forward the .mobileconfig file to the user. When the user launches the file, it will install certificates to the device.
3. The Cisco Identity Services Engine (ISE) native supplicant provisioning process can be used to distribute user certificates.
4. Enterprise MDM software can provision and publish certificates to registered devices.

Windows Specific

5. On Windows laptops that have joined the AD domain, Microsoft group policy object (GPO) policies can be used to distribute machine certificates.

Simple Certificate Enrollment Protocol[18, 19]

The AnyConnect client uses SCEP to securely issue and renew a certificate used for client authentication. The remote user launches AnyConnect and authenticates using Active Directory or a one-time token password for the first time. After establishing the VPN, the ASA pushes a client profile that includes the SCEP request. The AnyConnect client then sends a certificate request and the CA automatically accepts or denies the request. The certificate is installed in the device native certificate store. For all subsequent connections the AnyConnect client uses the newly obtained certificate for authentication and will never prompt the user for a password.

Enhancing the Usability of the VPN Connection

After the VPN connection is established, there are many session parameters in the ASA that define the user experience of Cisco AnyConnect and Jabber. We will discuss some of the best practices for these parameters.

Datagram Transport Layer Security (DTLS)[20]

DTLS is a standards-based SSL protocol that provides a low-latency data path using UDP. DTLS allows the AnyConnect client establishing an SSL VPN connection to use two simultaneous tunnels - an SSL tunnel and a DTLS tunnel. DTLS avoids latency and bandwidth problems and improves the performance of real-time applications such as Jabber that use RTP media streams on UDP. If DTLS is configured and UDP is interrupted, the remote user's connection automatically falls back from DTLS to TLS. DTLS is enabled by default when using AnyConnect and is a valuable and essential feature to ensure the most optimal remote Jabber connection.

[18] SCEP: http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080b25dc1.shtml

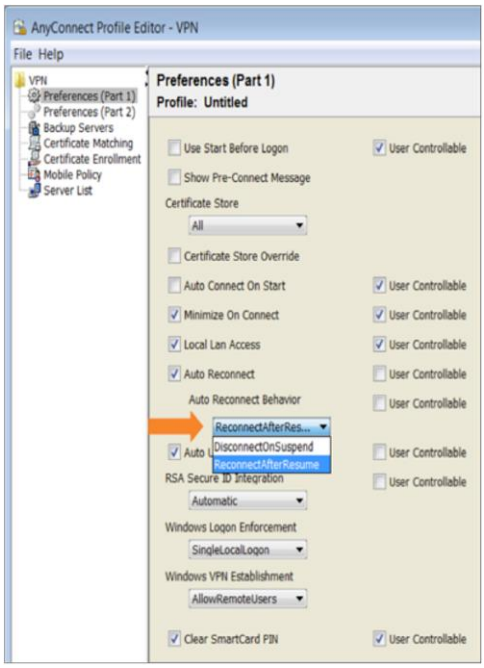
[19] SCEP-2: http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect24/administration/guide/ac03features.html#wp1073195

[20] DTLS: http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect20/administrative/guide/admin5.html#wp999810

Session Persistence (Auto-Reconnect)[21]

Session persistence in the AnyConnect client allows the VPN session to recover from service disruptions and reestablish the connection. For example, as the user roams from one Wi-Fi network to another or to a 3G cellular network, the AnyConnect client automatically resumes the VPN session.

Figure 4. Session Persistence (Auto-Reconnect)



In addition, AnyConnect should be configured to reestablish the VPN session after the device resumes from standby or from sleep or hibernation mode.

Auto-Reconnect is enabled in the VPN client profile. The parameter **Auto Reconnect Behavior** should be set to **Reconnect After Resume** (Figure 4).

Note: On iOS devices, the VPN profile includes a **Network Roaming** parameter that should also be enabled to support roaming across Wi-Fi and/or 3G cellular networks.

Idle Timeout[22]

The idle timeout (vpn-idle-timeout) is the time after which, if there is no communication activity, the Cisco ASA terminates the VPN connection. A very short idle timeout will frequently disrupt the VPN connection, requiring the user to reestablish the VPN for every call. On the other hand, a large idle timeout value results in too many concurrent sessions on the ASA. The idle timeout value can be configured per group policy. For group policies specific to Jabber clients, an idle timeout value of 30 minutes is recommended.

[21] Auto-reconnect: http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect25/administration/guide/ac03features.html#wp1113790

[22] Idle timeout: http://www.cisco.com/en/US/docs/security/asa/asa81/command/ref/uz.html#wp1563118

Dead Peer Detection (DPD)[23]

Dead peer detection (DPD) helps ensure that the ASA gateway or the AnyConnect client can quickly detect a condition where the peer is not responding and the connection has failed.

Server-side DPD should be disabled, as it prevents the device from sleeping. However, client-side DPD should be enabled, as it enables the client to determine when the tunnel is terminated due to a lack of network connectivity.

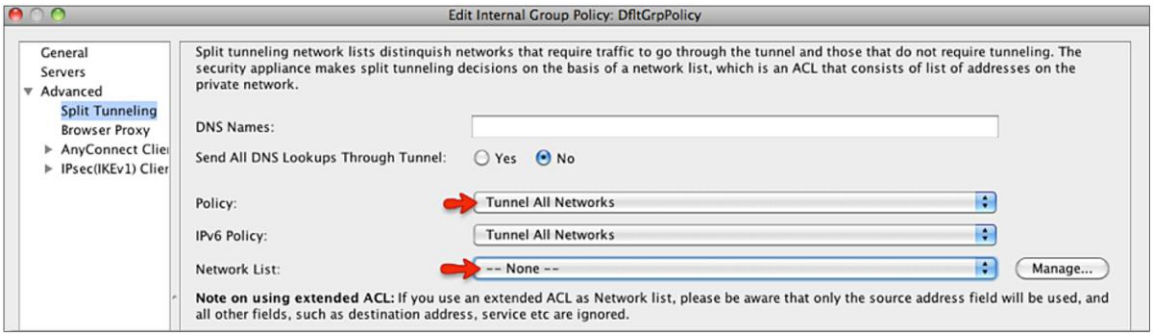
Split-Tunnel Policy

The split-tunnel feature allows administrators to specify which traffic (based on destination subnets) traverses the VPN tunnel and which goes in the clear. An associated feature, split DNS, defines which DNS traffic is eligible for resolution over the VPN tunnel and which DNS traffic should be handled by the endpoint DNS resolver.

Full-Tunnel Policy

For Jabber and AnyConnect deployments, full tunnel is the most secure option. With this feature enabled, all the traffic from all the applications on the device is sent over the VPN tunnel to the ASA gateway (Figure 5). However, it could result in latency for all the applications and drain the battery more quickly on mobile devices.

Figure 5. Full-Tunnel Policy



Administrators can optionally enable the **Local LAN Access**[24] feature to enable local printing and local network drive mapping.

Split-Include Policy with Network Access Control List (ACL)

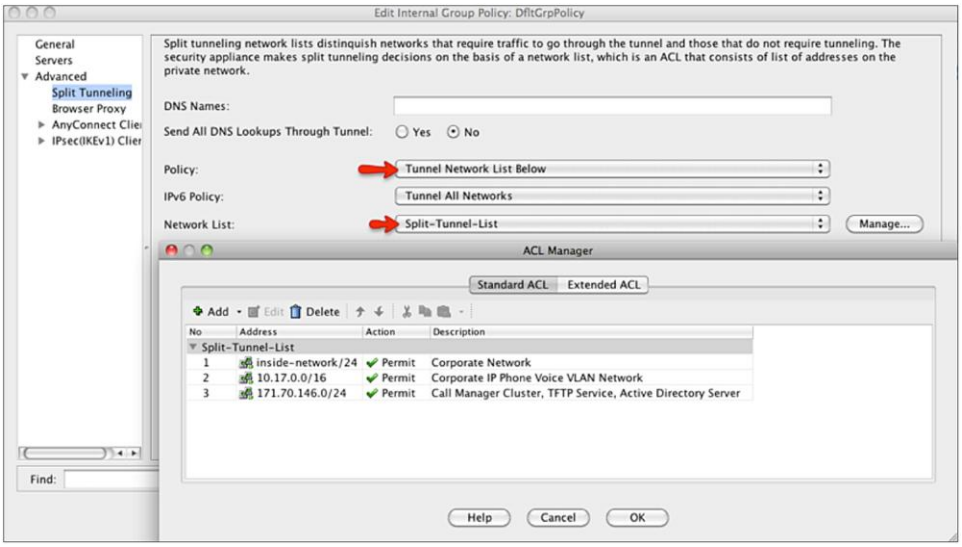
Some organizations would like to limit the traffic that is sent over the VPN tunnel due to bandwidth concerns. In addition, they would like to restrict the VPN session to the Jabber application.

The split-include policy on the Cisco ASA can be used to specify which traffic is encrypted and sent via the VPN tunnel based on the destination IP address of the traffic.

Administrators will have to include the IP subnets of the Cisco Unified Communications Manager cluster, directory server, and Trivial File Transfer Protocol (TFTP) server. The Jabber client needs peer-to-peer media connections with any IP phone or soft phone on the corporate network. Hence, the split-include policy should include the corporate network IP address range. Sometimes the IP space of a large company is not contiguous because of acquisitions and other events, so this configuration may not be applicable for all deployments.

[23] DPD: http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/svc.html#wp1090788
[24] Local LAN access: http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080702992.shtml

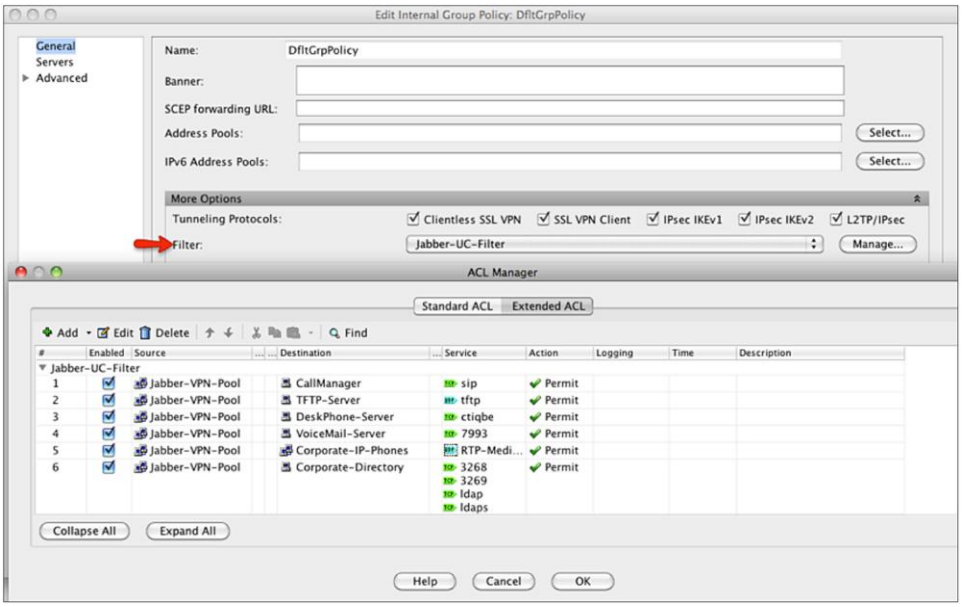
Figure 6. Split-Include Policy



The policy shown in Figure 6 will direct all internal traffic into the tunnel, but will also ensure that traffic not specified by the ACL (such as Google, Facebook, etc.) is sent in the clear, thus reducing the amount of traffic sent to the head-end ASA.

However, all applications' data that is directed to the address range specified in the split-include policy will be tunneled, so applications other than Jabber will have access to the tunnel. Hence, the administrator should apply a VPN filter (network ACL) that further restricts the available destination ports, to keep other applications from using the corporate network (Figure 7).

Figure 7. VPN Filter (Network ACL)

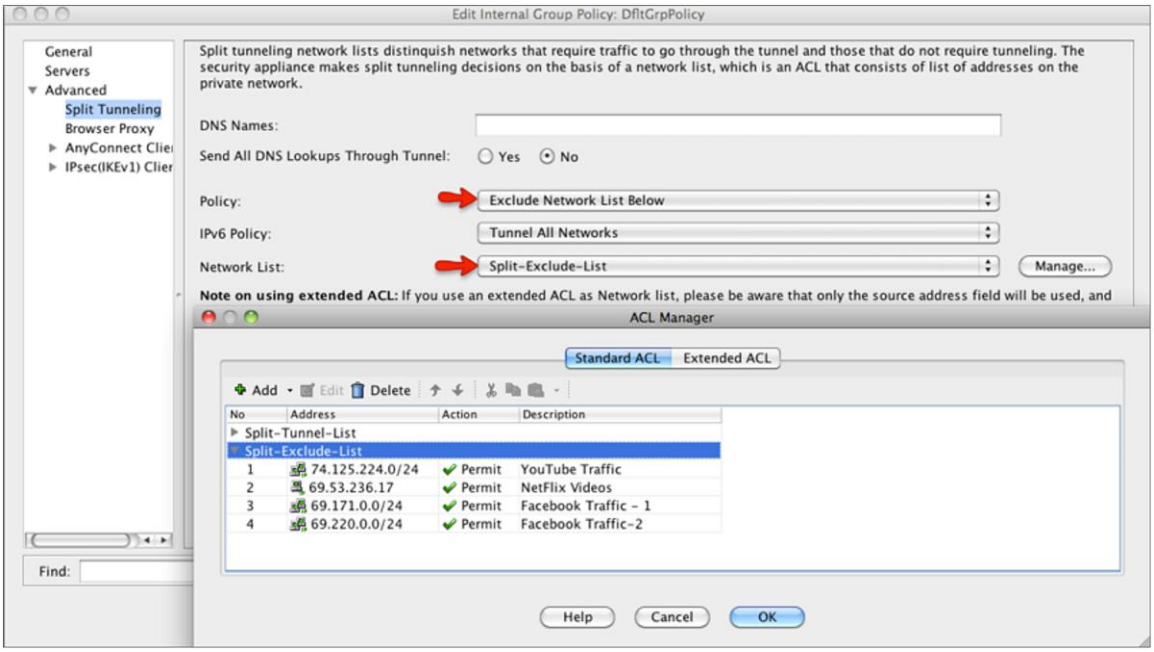


Both the split-tunnel policy and the VPN filter are configured per group policy. So the VPN administrator can apply different policies for different VPN groups.

Split-Exclude Policy

Some organizations may not find it practical to define the entire subnet required for split-include policies. However, they can use the split-exclude policy to prevent any known traffic from using the VPN tunnel. For example, an organization concerned about bandwidth could add the destination subnets for NetFlix, Hulu, YouTube, and others to their split-exclude list (Figure 8).

Figure 8. Split-Exclude Policy



Troubleshooting Common Errors

Certificate Authentication Failures

Ensure that

1. The certificate is still valid and the CA server has not revoked the certificate.
2. The correct VPN connection profile is used for authentication.
3. The **Key Usage** of the certificate is set to **TLS Web Client Authentication**.

SCEP Enrollment Failures

Ensure that

1. The CA server is configured to automatically grant the certificate.
2. The clock skew between the ASA and the CA server is less than 30 seconds.
3. The CA server enrollment URL is reachable over the VPN tunnel.

4. The **Automatic SCEP Host** value in the VPN client profile matches the **Group Alias** of the connection profile. For example, if the Group Alias is set to certenroll and the ASA address is asa.example.com, you need to set the Automatic SCEP Host to asa.example.com/certenroll.
5. The command **ssl certificate-authentication interface outside port 443** is enabled on the ASA.

Jabber Doesn't Auto-Launch the AnyConnect App on iOS Devices

Ensure that

1. The On-Demand VPN URL is configured inside the Cisco Unified Communications Manager for the device.
2. The On-Demand domain list (**Always Connect** or **Connect If Needed**) in the AnyConnect profile includes the On-Demand VPN URL.

Diagnostic AnyConnect Reporting Tool (DART)[25]

DART can be used to collect data useful for troubleshooting AnyConnect installation and connection problems. The DART wizard runs on the computer that runs the AnyConnect client. DART assembles the logs, status, and diagnostic information for analysis by the Cisco Technical Assistance Center (TAC). DART does not require administrator privileges and supports Windows and Mac OS X.

On the iOS and Android devices, AnyConnect includes the capability to collect and email the logs to the administrator.[26] Cisco Jabber also includes options to collect logs for troubleshooting purposes.[27]

Conclusion

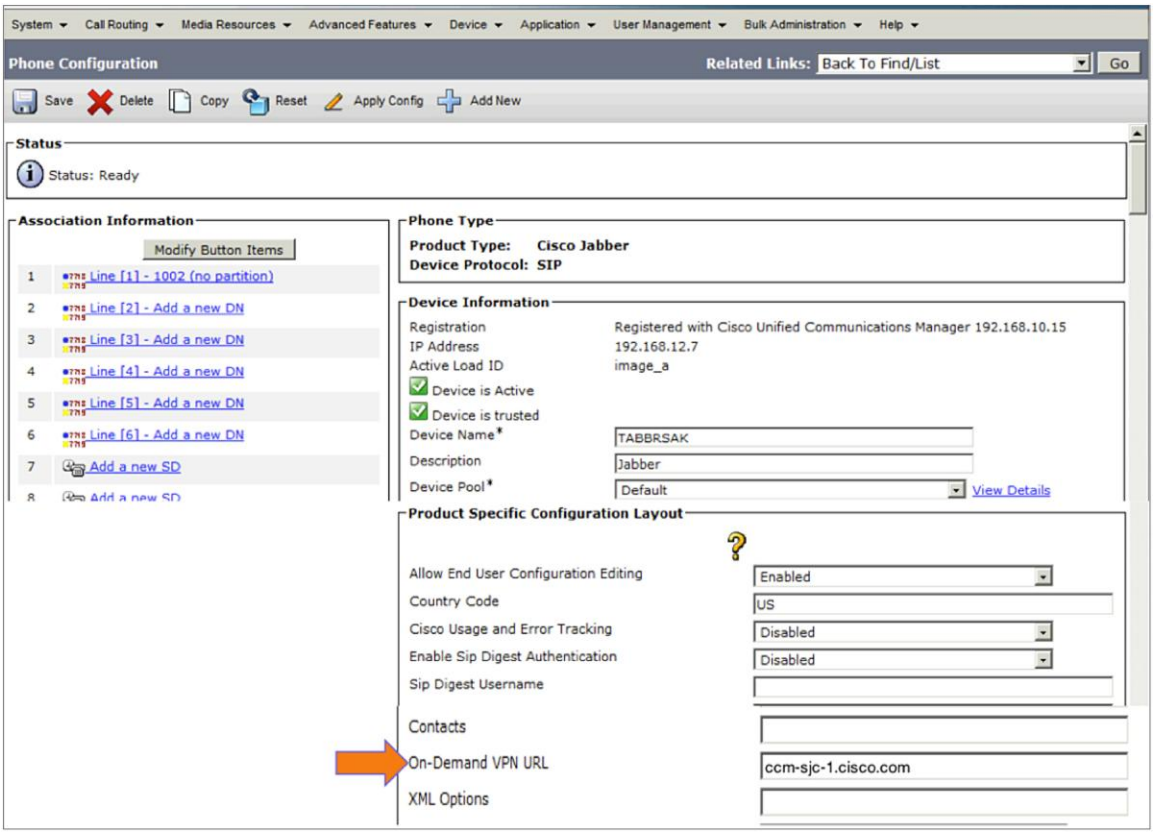
The Cisco Jabber and Cisco AnyConnect clients work seamlessly together to provide a rich collaboration experience for users, whether they are on the company network or on the go. The best practices identified, such as On-Demand VPN, certificate authentication and enrollment, VPN session timeouts, and split-tunnel policy enhance the user experience while helping ensuring security.

[25] DART: http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect24/administration/guide/ac08managemonitortbs.html#wp1055965

[26] iPhone logs: http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect24/iphone-user/guide/iphone-anyconnect-ug-24.html#wp50430

[27] Jabber logs: http://www.cisco.com/en/US/docs/voice_ip_comm/jabber/iPhone/8.6/b_Cisco_Jabber_8.6.html - reference_09FC6E4FBCA94B819D8F97E5D5B90278

Appendix A1: Configure On-Demand VPN URL in Cisco Unified Communications Manager



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.

Printed in USA C07-717020-00 10/12