



## Supported VPN Platforms, Cisco ASA 5500 Series, Versions 8.0(2) to 8.1(1)

---

### 11 December 2008

This document, previously titled *Adaptive Security Appliance VPN Compatibility Reference*, shows the compatibility of the ASA, clients, and Cisco Secure Desktop.

We have tested the features on the operating systems (OSs) and web browsers named in this document; however, they might work on other OSs and browsers.

For more information, go to the release notes and configuration guides for the products named in this document.



### Note

---

For AAA server compatibility information, go to “[Configuring AAA Servers and the Local Database.](#)”

---

## LAN to LAN

The ASA supports LAN-to-LAN IPsec connections with Cisco peers, and with third-party peers that comply with all relevant standards.

## ASA, ASDM, Cisco Secure Desktop, and AnyConnect (SSL) VPN Client

[Table 1](#) shows the compatibility of the latest versions.



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

**Table 1** ASA, ASDM, and Client Compatibility

ASA	ASDM	Cisco Secure Desktop	Cisco AnyConnect Client
8.1(1)	6.1(1) to 6.1(3) <sup>1</sup>	3.3.0.118+	2.2.0133+
8.0(4)	6.1(3) <sup>1</sup>	3.3.0.118+	2.2.0133+
8.0(3)	6.0(3) to 6.1(3) <sup>1</sup>	3.2.1.103 or 3.3.0.118+	2.1.0128 to 2.1.0148
8.0(2)	6.0(2) or 6.1(1) to 6.1(3) <sup>1</sup>	3.2.0.136 (subsequently referenced as “3.2”)	2.0.0343 (subsequently referenced as “2.0”)
7.1(x) - 7.2(x)	5.1(x) - 5.2(x)	3.1.1.45 (subsequently referenced as “3.1.1”)	<sup>2</sup>

1. ASDM 6.1.3 can manage ASAs running 8.0(2), 8.0(3), 8.0(4) and 8.1(1).
2. Only ASAs running 7.1(x) or 7.2(x) support the Cisco SSL VPN Client (1.1.4.176+); however Cisco Secure Desktop does not support it. See the next section for IPsec support.

## IPsec Clients

All releases of the ASA support the following IPsec clients:

- Cisco VPN Client
- Cisco ASA 5505
- Cisco PIX 501 Firewall
- Cisco VPN 3002 hardware client
- Cisco IOS 8xx Series
- Microsoft L2TP/IPsec client

## Operating Systems

The following tables show the ASA features and the OSs they support:

- [Table 2, AnyConnect and Supported OSs](#)
- [Table 3, Host Scan and Supported OSs](#)
- [Table 4, Other Cisco Secure Desktop Features and Supported OSs](#)
- [Table 5, Clientless SSL VPN Features and Supported OSs](#)

Features not shown support all of the named OSs. The tables address the following releases:

- ASA 8.0(2) to 8.1(1).
- Cisco AnyConnect VPN Client, Versions 2.0 – 2.2. AnyConnect supports Linux Kernel releases 2.4 and 2.6 on 32-bit architectures, and 64-bit architectures that support biarch (that is, that run 32-bit code). The tun module is required. All of the distributions we have tested include the tun module by default. Other [requirements](#) apply. We have tested the following distributions successfully:
  - Ubuntu 7 and 8 (32-bit only)
  - Red Hat Enterprise Linux 3 and 4
  - Fedora 4 – 9



**Note** To use Fedora 9 with the AnyConnect client, you must first install Sun Microsystems JRE, preferably JRE 6, Update 5.

- Slackware 11 and 12.1
- openSUSE 10
- SUSE 10.1
- Cisco Secure Desktop, Versions 3.1.1 to 3.3

**Table 2** AnyConnect and Supported OSs

AnyConnect Client Session Type	32-bit Microsoft Windows Vista and SP1 with <a href="#">KB952876</a>	64-bit Microsoft Windows Vista and SP1 with <a href="#">KB952876</a>	32-bit Microsoft Windows XP SP2 and SP3	64-bit Microsoft Windows XP SP2	32-bit Microsoft Windows 2000 SP4 with <a href="#">MSI 3.1</a> or later and <a href="#">MSXML 3.0</a> or later	Apple Mac OS X 10.4	Apple Mac OS X 10.5	Linux
Certificate Authentication, including DoD Common Access Card and SmartCard	✓	✓	✓	✓	✓	✓ <sup>1</sup>	✓ <sup>1</sup>	✗
Start Before Logon	✓ <sup>2</sup>	✓ <sup>2</sup>	✓ <sup>2</sup>	✗	✓ <sup>2</sup>	✗	✗	✗
Standalone or WebLaunch (Cisco Secure Desktop components not used)	✓	✓	✓	✓	✓	✓	✓ <sup>3</sup>	✓ <sup>4</sup>
Standalone with Host Scan	✓ <sup>5</sup>	✗	✓	✗	✓	✓ <sup>6</sup>	✓ <sup>6</sup>	✓ <sup>7</sup>
Standalone with Secure Desktop (Vault)	✗	✗	✓ <sup>3</sup>	✗	✓ <sup>3</sup>	✗	✗	✗
WebLaunch with Cache Cleaner	✓ <sup>3</sup>	✗	✓ <sup>3</sup>	✗	✓ <sup>3</sup>	✓ <sup>6</sup>	✓ <sup>6</sup>	✓ <sup>7</sup>
WebLaunch with Secure Desktop	✗	✗	✓ <sup>3</sup>	✗	✓ <sup>3</sup>	✗	✗	✓ <sup>7</sup>

1. With Safari keychain only.

2. Beginning with Cisco Secure Desktop 3.2.1 and AnyConnect 2.2.
3. Beginning with AnyConnect 2.1
4. [Standalone mode supports both 32-bit and biarch 64-bit.](#)
5. Beginning with Cisco Secure Desktop 3.2.1.118 and AnyConnect 2.1.
6. Beginning with AnyConnect 2.1 on 32-bit mode only.
7. Beginning with AnyConnect 2.1 on Fedora Core 4.

**Table 3** *Host Scan and Supported OSs*

Feature	32-bit Microsoft Windows Vista and SP1	32-bit Microsoft Windows XP SP2 and SP3	32-bit Microsoft Windows 2000 SP4	32-bit Apple Mac OS X 10.4 and 10.5	32-bit Linux
Clientless SSL VPN support for Host Scan	1 ✓	✓	✓	2 ✓	2 ✓
Check for Microsoft Windows service pack, or Mac OS or Linux build	✓	✓	✓	2 ✓	2 ✓
Scan for processes	✓	✓	✓	2 ✓	2 ✓
Check for listening ports (TCP only)	✓	✓	✓	1 ✓	1 ✓
Check for registry keys	✓	✓	✓	3 ✗	3 ✗

1. Beginning with Cisco Secure Desktop 3.2.1.118.
2. Beginning with Cisco Secure Desktop 3.2.1.
3. This OS does not use registry keys.

**Table 4** *Other Cisco Secure Desktop Features and Supported OSs*

Feature	32-bit Microsoft Windows Vista and SP1	32-bit Microsoft Windows XP SP2 and SP3	32-bit Microsoft Windows 2000 SP4	32-bit Apple Mac OS X 10.4 and 10.5	32-bit Linux Tested on Fedora Core 4
Cache Cleaner	✓	✓	✓	✓	✓
Certificate checks	✓	✓	✓	✗	✗
Host emulation detection	✓	✓	✓	✗	✗

**Table 4** Other Cisco Secure Desktop Features and Supported OSs

Feature	32-bit Microsoft Windows Vista and SP1	32-bit Microsoft Windows XP SP2 and SP3	32-bit Microsoft Windows 2000 SP4	32-bit Apple Mac OS X 10.4 and 10.5	32-bit Linux Tested on Fedora Core 4
Keystroke logger detection	✓	✓	✓	✗	✗
Launch cleanup upon timeout based on inactivity	✓	✓	✓	✗	✗
Launch hidden URL after installation	✓	✓	✓	✗	✗
Prelogin assessment (for rejection or policy assignment)	✓	✓	✓	✓	✓
Secure Desktop (Vault) 1	✓	✓	✓	✗	✗
Show success message at the end of successful installation	✓	✓	✓	✗	✗

1. Beginning with Cisco Secure Desktop 3.3, Secure Desktop supports Windows Vista and Vista SP1, but it does not support AnyConnect on these OS's.

**Table 5** Clientless SSL VPN Features and Supported OSs

Feature	32-bit Microsoft Windows Vista and SP1	32-bit Microsoft Windows XP SP2 and SP3	32-bit Microsoft Windows 2000 SP4	Apple Mac OS X 10.4 and 10.5	32-bit Linux
Certificate Authentication, including DoD Common Access Card and SmartCard	✓	✓	✓	1 ✓	✓
Port Forwarding (Sun Microsystems Java™ Runtime Environment (JRE) 1.4.1.x or higher must be installed. See <a href="#">Port Forwarding Restrictions</a> for other requirements.) <b>Note:</b> Recommended only for Linux	✓	✓	✓	2 ✓	3 ✓

**Table 5** Clientless SSL VPN Features and Supported OSs

Feature	32-bit Microsoft Windows Vista and SP1	32-bit Microsoft Windows XP SP2 and SP3	32-bit Microsoft Windows 2000 SP4	Apple Mac OS X 10.4 and 10.5	32-bit Linux
Smart tunnel (ASA 8.0(2) and above) <b>Note:</b> Recommended for Windows and Mac OS instead of port forwarding	4 ✓	4 ✓	4 ✓	5 ✓	✗
Web folders	✗	6 ✓	6 ✓	✗	✗

1. With Safari keychain only.
2. The most recent Safari version 2.0.4(419.3) we tested requires Java version 1.5 to use Port Forwarding.
3. Tested on Fedora Core 4.
4. Beginning with ASA 8.0(2)+. The browser must be enabled with Java, Microsoft ActiveX, or both.
5. Beginning with ASA 8.0(4)+. The browser must be enabled with Java. See [restrictions](#).
6. With [Microsoft hotfix](#) installed.

## Mobile Support

The following sections address mobile compatibility with the ASA:

- [VPN \(IPsec\) Client](#)
- [L2TP/IPsec Client](#)
- [SSL VPN Clientless](#)

### VPN (IPsec) Client

The Apple iPhone 3G ships with advanced VPN Client capabilities for Cisco IPsec connectivity already installed. Original iPhone users can upgrade to the iPhone 2.0 software to take advantage of this new capability. Features of the VPN Client include:

- The following authentication types:
  - Pre-shared keys
  - Certificates
  - Xauth
  - One-time passwords, including tokens such as RSA, Rainbow, Entrust, and SafeNet
  - RADIUS, including both one-time password tokens and other types of xauth
  - RADIUS Expiry
  - Kerberos
- VPN load balancing (clustering)
- Split tunneling control

The Cisco ASA 5500 Security Appliances and PIX Firewalls work with the Cisco VPN Client on the iPhone. We highly recommend the 8.0(x) software release or later, but you can also use the 7.2(x) software.

For Windows Mobile, the following third-party vendors offer a VPN client that works with the ASA: Antha, Apani, Bluefire, Microsoft, and NCP.DE. Cisco supports the Microsoft client; the respective vendors support the other clients.

Bluefire offers a version of the Palm Treo that has an IPsec client that works with the ASA.

[Nokia](#) provides support for Symbian on the Nokia 92xx Communicator series, Nokia 6600 and Nokia E61.

## L2TP/IPsec Client

The following mobile OS's support a built-in L2TP/IPsec client that Cisco has tested successfully with the ASA:

- Microsoft Windows Mobile 2003 for Pocket PC PDA
- Microsoft Windows Mobile 5.0 PDA and PDA Phone
- Apple iPhone

The iPhone supports MS-CHAP v2 (preferred) for PPP. It has also been tested for MS-CHAP v1 and PAP support for PPP authentication. The VPN Client on the iPhone 3G supports pre-shared keys and certificates.

Windows mobile based handheld devices support MS-CHAP v1 and v2, and pre-shared keys.

Some Windows Mobile 2003 (HP iPAQ h4150) and 5.0 (HP iPAQ hx 2495b) PDAs support enrollment with an available certificate authority server and can use certificate-based authentication.

## SSL VPN Clientless

You can access Clientless SSL VPN from your Pocket PC or other certified personal digital assistant (PDA). Neither the ASA administrator nor the Clientless SSL VPN user need do anything special to use Clientless SSL VPN with a certified mobile device. Cisco has certified the mobile devices shown in [Table 6](#):

**Table 6** *Mobile Devices Certified for SSL VPN Clientless Connections*

Device	OS	Browser
HP iPAQ h4150	Pocket PC 2003 and Windows CE 4.20.0 (Build 14053)	Pocket IE
HP iPAQ hx2495b	Windows CE 5.0 5.1.1702 (Build 14366.1.0.1)	Pocket IE
HTC p3600 PDA Phone	Windows Mobile 5.0 5.1.465 (Build 15673.3.3.1)	Pocket IE
iPhone	Software Update 1.1.3 and later	Safari

Other mobile devices (e.g., the BlackBerry) might work but are not supported.

The iPhone does not have a Java Runtime Environment (JRE) and does not support SSL, so the following SSL VPN features are not supported: application access, auto applet download, client/server plug-ins, and e-mail proxy.

Smart tunnels, plug-ins, and port forwarding do not support Microsoft Windows Mobile.

## Browsers

Cisco AnyConnect Client (when launched as a standalone client) supports any browser. [Table 7](#) shows the browsers that Clientless SSL VPN and the Cisco Secure Desktop modules support. Other browsers might also work but are not supported by Cisco.


**Note**

For ASDM operating system and browser requirements, see the [Cisco ASDM Release Notes](#).

**Table 7** *Browsers Supported by Cisco AnyConnect Client, Clientless SSL VPN, and Cisco Secure Desktop*

Browser	Microsoft Windows Vista and Vista SP1	Microsoft Windows XP SP2 and SP3	Microsoft Windows 2000 SP4	Apple Macintosh OS X 10.4 and 10.5	Linux
Internet Explorer	7.0 <sup>1</sup>	6.0 and 7.0	6.0	✘	✘
Firefox	2.0 - 3.0 <sup>2</sup>	1.5 - 3.0	1.5 - 3.0	2.0 - 3.1.1 <sup>3</sup>	1.5 - 3.0
Safari	✘	✘	✘	2.0 - 3.1.1 <sup>4</sup>	✘

1. Secure Desktop does not let Internet Explorer run on the Microsoft Vista desktop.
2. AnyConnect in standalone mode only.
3. AnyConnect on a Mac does not support the Firefox certificate store. For Host Scan with WebStart, see below.
4. Smart Tunnel requires 3.1.1.

To enable Host Scan with WebStart, the remote user must do the following:

- Step 1** Connecting to the ASA. The Opening webstart.xml window opens.
- Step 2** Click **Open With** and **Choose**.
- Step 3** Select **Applications/Utilities/Java/J2SE 5.0/Java Cache Viewer**.
- Step 4** Click **OK**.

Do not associate jnlp files with javaws or Applications/Utilities/Java/Java Web Start.

## Antivirus, Antispyware, and Firewall Packages Supported by Host Scan

Host Scan examines the remote computer connecting to the VPN for antivirus and antispyware applications, and software firewalls for compliance with configured, corporate security policies. To access the list of packages that Host Scan supports, go to the [Software Download page for Cisco Secure Desktop](#), click the PDF link above “Antivirus, Antispyware, and Firewall Packages Supported by Host Scan,” and click **Next** and **Accept** in the subsequent pages.

# E-mail Proxy

E-mail Proxy (sessions) is a legacy feature that the ASA supports for use with Microsoft Outlook 2002 (also known as Outlook XP), Outlook 2000, and Outlook Express running on the following OS's:

- Microsoft Windows Vista and SP1
- Microsoft Windows XP SP2 and SP3
- Microsoft Windows 2000 SP4

---

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0903R)

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.

© 2008 Cisco Systems, Inc. All rights reserved.

