



Cisco ASA 5500 Series Release Notes Version 7.1(1)

February 2006

Contents

This document includes the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New Features, page 3](#)
- [Important Notes, page 12](#)
- [Open Caveats, Release 7.1\(1\), page 15](#)
- [Caveats, Release 7.0\(4\), page 16](#)
- [Related Documentation, page 18](#)
- [Obtaining Documentation and Submitting a Service Request, page 18](#)

Introduction

The Cisco ASA 5500 series security appliance are purpose-built solutions that combine best-of-breed security and VPN services with the innovative Cisco Adaptive Identification and Mitigation (AIM) architecture. Designed as a key component of the Cisco Self-Defending Network, the adaptive security appliance provides proactive threat defense that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity. The result is a powerful multifunction network adaptive security appliance family that provides the security breadth and depth for protecting small and medium-sized business and enterprise networks while reducing the overall deployment and operations costs and complexities associated with providing this new level of security. This version introduces significant enhancements to major functional areas including: new Anti-X Services, VPN services, and management/monitoring.



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

© 2006 Cisco Systems, Inc. All rights reserved.

For more information on all the new features, see [New Features, page 3](#).

Additionally, the adaptive security appliance software supports Adaptive Security Device Manager. ASDM delivers world-class security management and monitoring through an intuitive, easy-to-use Web-based management interface. Bundled with the adaptive security appliance, ASDM accelerates security appliance deployment with intelligent wizards, robust administration tools, and versatile monitoring services that complement the advanced integrated security and networking features offered by the market-leading suite of the adaptive security appliance. Its secure, web-based design enables anytime, anywhere access to adaptive security appliances.

System Requirements

The sections that follow list the system requirements for operating an adaptive security appliance. This section includes the following topics:

- [Memory Requirements, page 2](#)
- [Determining the Software Version, page 2](#)
- [Upgrading to a New Software Version, page 2](#)

Memory Requirements

[Table 1](#) lists the DRAM memory requirements for the adaptive security appliance.

Table 1 *DRAM Memory Requirements*

ASA Model	DRAM Memory
ASA 5510	256 MB
ASA 5520	512 MB
ASA 5540	1 GB

All adaptive security appliances require a minimum of 64 MB of internal CompactFlash.

Determining the Software Version

Use the **show version** command to verify the software version of your adaptive security appliance.

Upgrading to a New Software Version

If you have a Cisco.com (CDC) login, you can obtain software from the following website:

<http://www.cisco.com/kobayashi/sw-center/products.shtml>

You must upgrade or down grade from Version 7.0.(x) to 7.1(1) and vice versa because older versions of the ASA images does not recognize new ASDM images, new ASA images does not recognize old ASDM images.

You can also use command-line interface to download the image, see the “[Downloading Software or Configuration Files to Flash Memory](#)” section in the *Cisco Security Appliance Command Line Configuration Guide*.

To upgrade from Version 7.0.(x) to 7.1(1), you must perform the following steps:

-
- Step 1** Load the new 7.1(1) image from the following website: <http://www.cisco.com/cgi-bin/tablebuild.pl/asa>
 - Step 2** Reload the device so that it uses the 7.1(1) image.
 - Step 3** Load the new ASDM 5.1.1 image from the following website:
<http://www.cisco.com/cgi-bin/tablebuild.pl/asa>.
-

To downgrade from Version 7.1(1) to 7.0.(x), you must perform the following steps:

-
- Step 1** Load the 7.0.(x) image from the following website: <http://www.cisco.com/cgi-bin/tablebuild.pl/asa>
 - Step 2** Reload the device so that it uses the 7.0(x) image.
 - Step 3** Load the ASDM 5.0(x) image from the following website:
<http://www.cisco.com/cgi-bin/tablebuild.pl/asa>.
-

New Features

This section describes the new features in this version. This section includes the following topics:

- [Support for Content Security and Control SSM, page 4](#)
- [Cisco Secure Desktop, page 5](#)
- [Customized Access Control Based on CSD Host Checking, page 6](#)
- [SSL VPN Client, page 6](#)
- [Authentication and Authorization Enhancements, page 6](#)
- [Tunnel Group and Group Policy Enhancements, page 8](#)
- [WebVPN Functions and Performance Optimizations, page 9](#)
- [Citrix Support for WebVPN, page 9](#)
- [PDA Support for WebVPN, page 10](#)
- [WebVPN Support of Character Encoding for CIFS Files, page 10](#)
- [Compression for WebVPN and SSL VPN Client Connections, page 10](#)
- [Active/Standby Stateful Failover for WebVPN and SVC Connections, page 11](#)
- [WebVPN Customization, page 11](#)
- [ASDM Improvements, page 11](#)
- [Auto Applet Download, page 12](#)

Support for Content Security and Control SSM

This feature combines comprehensive malware protection with advanced message compliance for the multifunction adaptive security appliance. The result is a powerful solution that stops a number of Internet threats including viruses, spyware, spam, hackers, unwelcome visitors and unwanted web content while reducing the operational costs and complexity of deploying and managing multiple point solutions.

The Content Security and Control (CSC) SSM, an integral part of Cisco's Anti-X solution, delivers industry-leading threat protection and content control at the Internet edge providing comprehensive antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, URL blocking and filtering, and content filtering services. The CSC SSM services module helps businesses more effectively protect their networks, increase network availability, and increase employee productivity through the following key elements:

Table 2 **Key Features and Benefits**

Key Feature	Benefit
Antivirus	Market leading antivirus, from Trend Micro, shields your internal network resources from both known and unknown virus attacks, at the most effective point in your infrastructure, the Internet gateway. By cleaning your email and web traffic at the perimeter, it eliminates the need for resource intensive malware infection clean-ups and ensures business continuity
Anti-Spyware	Blocks spyware from entering your network through web traffic (HTTP & FTP) and email traffic. Frees-up IT support resources from costly spyware removal procedures and improves employee productivity by blocking spyware at the gateway.
Anti-Spam	Effective blocking of spam with very low false positives helps to restore the effectiveness of your email communications, so contact with customers, vendors, and partners continues uninterrupted.
Anti-Phishing	Identity theft protection guards against phishing attacks thereby preventing employees inadvertently disclosing company or personal details which could lead to financial loss.
Automatic Updates from TrendLabs	The solution is backed and supported by one of the largest teams of virus, spyware and spam experts in the industry working 24x7 to ensure that your solution is providing the most up to date protection – automatically.
Central Administration	Easy, set-and-forget administration through a remotely accessible web-console and automated updates reduces IT support costs.
Real-time protection for Web access, Mail (SMTP & POP3) and FTP (file transfer)	Even if the company mail is already protected, many employees will access their own private web-mail from their company PCs or laptops introducing yet another entry point for internet borne threats. Similarly, employees may directly download programs or files which may be similarly contaminated. Real-time protection of all web traffic at the internet gateway greatly reduces this often over-looked point of vulnerability.

Table 2 **Key Features and Benefits**

Key Feature	Benefit
Full URL filtering capability with categories, scheduling and cache	URL filtering can be used to control employee internet usage by blocking access to inappropriate or non-work related websites improving employee productivity and limiting the risk of legal action being taken by employees exposed to offensive web content.
Email Content Filtering	Email filtering minimizes legal liability due to exposure to offensive material transferred by email and enforces regulatory compliance, helping organizations meet the requirements of legislation such as GLB and the Data Protection Act

For more information, see the “Managing the CSC SSM” section in the *Cisco Security Appliance Command Line Configuration Guide*.

Cisco Secure Desktop

Cisco Secure Desktop (CSD) is an optional Windows software package you can install on the adaptive security appliance to validate the security of client computers requesting access to your SSL VPN, ensure they remain secure while they are connected, and remove all traces of the session after they disconnect.

After a remote PC running Microsoft Windows connects to the adaptive security appliance, CSD installs itself and uses the IP address and presence of specific files, registry keys, and certificates to identify the type of location from which the PC is connecting. Following user authentication, CSD uses optional criteria as conditions for granting access rights. These criteria include the operating system, antivirus software, antispyware, and personal firewall running on the PC.

To ensure security while a PC is connected to your network, the Secure Desktop, a CSD application that runs on Microsoft Windows XP and Windows 2000 clients, limits the operations available to the user during the session. For remote users with administrator privileges, Secure Desktop uses the 168-bit Triple Data Encryption Standard (3DES) to encrypt the data and files associated with or downloaded during an SSL VPN session. For remote users with lesser privileges, it uses the Rivest Cipher 4 (RC4) encryption algorithm. When the session closes, Secure Desktop overwrites and removes all data from the remote PC using the U.S. Department of Defense (DoD) security standard for securely deleting files. This cleanup ensures that cookies, browser history, temporary files, and downloaded content do not remain after a remote user logs out or an SSL VPN session times out. CSD also uninstalls itself from the client PC.

Cache Cleaner, which wipes out the client cache when the session ends, supports Windows XP, Windows 2000, Windows 9x, Linux, and Apple Macintosh OS X clients.

For more information about the CSD features, see the *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*.

Customized Access Control Based on CSD Host Checking

Adaptive security appliances with Cisco Secure Desktop installed can specify an alternative group policy. The adaptive security appliance uses this attribute to limit access rights to remote CSD clients as follows:

- Always use it if you set the VPN feature policy to “Use Failure Group-Policy.”
- Use it if you set the VPN feature policy to “Use Success Group-Policy, if criteria match” and the criteria then fail to match.

This attribute specifies the name of the alternative group policy to apply. Choose a group policy to differentiate access rights from those associated with the default group policy. The default value is DfltGrpPolicy.



Note

The adaptive security appliance does not use this attribute if you set the VPN feature policy to “Always use Success Group-Policy.”

For more information, see the *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administration Guide*.

SSL VPN Client

SSL VPN client is a VPN tunneling technology that gives remote users the connectivity benefits of an IPsec VPN client without the need for network administrators to install and configure IPsec VPN clients on remote computers. SVC uses the SSL encryption that is already present on the remote computer as well as the WebVPN login and authentication of the adaptive security appliance.

To establish an SVC session, the remote user enters the IP address of a WebVPN interface of the adaptive security appliance in the browser, and the browser connects to that interface and displays the WebVPN login screen. If the user satisfies the login and authentication, and the adaptive security appliance identifies the user as *requiring* the SVC, the adaptive security appliance downloads the SVC to the remote computer. If the adaptive security appliance identifies the user as having the *option* to use the SVC, the adaptive security appliance downloads the SVC to the remote computer while presenting a link on the user screen to skip the SVC installation.

After downloading, the SVC installs and configures itself. When the connection terminates, SVC either remains or uninstalls itself (depending on the configuration) from the remote computer.

You can configure SVC with ASDM or with CLI commands.

For more information, see “Configuring SSL VPN Client” in *Cisco Security Appliance Command Line Configuration Guide*.

Authentication and Authorization Enhancements

Release 7.1(1) includes the following authentication and authorization enhancements.

Override Account Disabled

You can configure the adaptive security appliance to override an account-disabled indication from a AAA server and allow the user to log on anyway.

For more information, see “Configuring IPsec Remote-Access Tunnel Group General Attributes” in *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the **override account disabled** command syntax, see the *Cisco Security Appliance Command Reference*.

LDAP Support

You can configure the security appliance to authenticate and authorize IPsec VPN users, SSL VPN clients, and WebVPN users to an LDAP directory server. During authentication, the security appliance acts as a client proxy to the LDAP server for the VPN user, and authenticates to the LDAP server in either plain text or using the Simple Authentication and Security Layer (SASL) protocol. The security appliance supports any LDAP V3 or V2 compliant directory server. It supports password management features only on the Sun Microsystems Java System Directory Server and the Microsoft Active Directory server.

For more information, see “LDAP Server Support” in *Cisco Security Appliance Command Line Configuration Guide*.

Password Management

You can configure the adaptive security appliance to warn end users when their passwords are about to expire. When you configure this feature, the adaptive security appliance notifies the remote user at login that the current password is about to expire or has expired. The adaptive security appliance then offers the user the opportunity to change the password. If the current password has not yet expired, the user can still log in using that password. This command is valid for AAA servers that support such notification; that is, RADIUS, RADIUS with an NT server, and LDAP servers. The adaptive security appliance ignores this command if RADIUS or LDAP authentication has not been configured.

Note that this command does not change the number of days before the password expires, but rather specifies the number of days before expiration that the adaptive security appliance starts warning the user that the password is about to expire. The default value is 14 days.

For LDAP server authentication only, you can specify a specific number of days before expiration to begin warning the user about the pending expiration.

For more information, see “Managing Passwords” in *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the **password management** command syntax, see the *Cisco Security Appliance Command Reference*.

SSO

Single sign-on (SSO) support lets WebVPN users enter a username and password only once to access multiple protected services and web servers. You can choose among the following methods to configure SSO:

- Computer Associates eTrust SiteMinder SSO server (formerly Netegrity SiteMinder)—You typically would choose to implement SSO with SiteMinder if your Web site security infrastructure already incorporates SiteMinder.
- HTTP Forms—A common and standard approach to SSO authentication that can also qualify as a AAA method. You can use it with other AAA servers such as RADIUS or LDAP servers.
- SSO with Basic HTTP and NTLM Authentication—The simplest of the three SSO methods passes WebVPN login credentials for authentication through to internal servers using basic HTTP or NTLM authentication. This method does not require an external SSO server.

For more information, see “Using Single Sign-on with WebVPN” in *Cisco Security Appliance Command Line Configuration Guide*.

Tunnel Group and Group Policy Enhancements

Release 7.1(1) includes the following new tunnel group and group policy enhancements.

WebVPN Tunnel Group Type

This version adds a WebVPN tunnel group, which lets you configure a tunnel group with WebVPN-specific attributes, including the authentication method to use, the WebVPN customization to apply to the user GUI, the DNS group to use, alternative group names (aliases), group URLs, the NBNS server to use for CIFS name resolution, and an alternative group policy to apply to CSD users to limit access rights to remote CSD clients.

For more information, see “Configuring Tunnel Groups” in *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Group-Based DNS Configuration for WebVPN

You can define a list of DNS servers under a group. The list of DNS servers available to a user depends on the group that the user is assigned to. You can specify the DNS server to use for a WebVPN tunnel group. The default value is DefaultDNS.

For more information, see “Group Policies” in *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

New Login Page Option for WebVPN Users

You can optionally configure WebVPN to display a user login page that offers the user the opportunity to select the tunnel group to use for login. If you configure this option, the login page displays an additional field offering a drop-down menu of groups from which to select. The user is authenticated against the selected group.

For more information, see “Configuring User Attributes” in *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Group Alias and Group URL

You can create one or more alternate names by which the user can refer to a tunnel group by specifying one or more group aliases. The group aliases that you specify here appear in the drop-down list on the user login page. Each group can have multiple aliases or no alias. If you want the actual name of the tunnel group to appear on this list, specify it as an alias. This feature is useful when the same group is known by several common names, such as “Devtest” and “QA”.

Specifying a group URL eliminates the need for the user to select a group at login. When a user logs in, the adaptive security appliance looks for the user incoming URL in the tunnel-group-policy table. If it finds the URL and if this feature is enabled, then the adaptive security appliance automatically selects

the appropriate server and presents the user with only the username and password fields in the login window. If the URL is disabled, the dropdown list of groups also appears, and the user must make the selection.

You can configure multiple URLs (or no URLs) for a group. You can enable or disable each URL individually. You must use a separate specification (**group-url** command) for each URL. You must specify the entire URL, which can use either the HTTP or HTTPS protocol.

You cannot associate the same URL with multiple groups. The adaptive security appliance verifies the uniqueness of the URL before accepting the URL for a tunnel group.

For more information, see “Configuring Tunnel Groups” in *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

WebVPN Functions and Performance Optimizations

This version enhances WebVPN performance and functions through the following components:

- Flexible content transformation/rewriting that includes complex JavaScript, VBScript, and Java
- Server-side and browser caching
- Compression
- Proxy bypass
- Application Profile Customization Framework support
- Application keep-alive and timeout handling
- Support for logical (VLAN) interfaces

For more information, see “Optimizing WebVPN Performance” in *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Citrix Support for WebVPN

WebVPN users can now use a connection to the adaptive security appliance to access Citrix MetaFrame services. In this configuration, the adaptive security appliance functions as the Citrix secure gateway. Therefore you must configure your Citrix Web Interface software to operate in a mode that does not use the Citrix secure gateway. Install an SSL certificate onto the adaptive security appliance interface to which remote users use a fully qualified domain name (FQDN) to connect; this function does not work if you specify an IP address as the common name (CN) for the SSL certificate. The remote user attempts to use the FQDN to communicate with the adaptive security appliance. The remote PC must be able to use DNS or an entry in the System32\drivers\etc\hosts file to resolve the FQDN. Finally, use the **functions** command to enable Citrix.

For more information, see “Configuring Access to Citrix MetaFrame Services” in *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

PDA Support for WebVPN

You can access WebVPN from your Pocket PC 2003 or Windows Mobile X. If you are a PDA user, this makes accessing your private network more convenient. This feature requires no configuration.

For more information, see “Using WebVPN with PDAs” in *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

WebVPN Support of Character Encoding for CIFS Files

WebVPN now supports optional character encoding of portal pages to ensure proper rendering of Common Internet File System files in the intended language. The character encoding supports the character sets identified on the following Web page, including Japanese Shift-JIS characters:

<http://www.iana.org/assignments/character-sets>

Use the **character-encoding** command to specify the character set to encode in WebVPN portal pages to be delivered to remote users. By default, the encoding type set on the remote browser determines the character set for WebVPN portal pages.

The character-encoding attribute is a global setting that, by default, all WebVPN portal pages inherit. However, you can use the **file-encoding** command to specify the encoding for WebVPN portal pages from specific CIFS servers. Thus, you can use different file-encoding values for CIFS servers that require different character encodings.

The mapping of CIFS servers to their appropriate character encoding, globally with the `webvpn character-encoding` attribute, and individually with file-encoding overrides, provides for the accurate handling and display of CIFS pages when the proper rendering of file names or directory paths, as well as pages, are an issue.



Tip

The character-encoding and file-encoding values do not exclude the font family to be used by the browser. You need to complement the setting of one these values with the **page style** command in `webvpn customization` command mode to replace the font family if you are using Japanese Shift_JIS character encoding, or enter the **no page style** command in `webvpn customization` command mode to remove the font family.

For more information, see “Configuring File Access” in *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Compression for WebVPN and SSL VPN Client Connections

Compression can reduce the size of the transferring packets and increase the communication performance, especially for connections with bandwidth limitations, such as with dialup modems and handheld devices used for remote access.

Compression is enabled by default, for both WebVPN and SVC connections. You can configure compression using ASDM or CLI commands.

You can disable compression for all WebVPN or SVC connections with the **compression** command from global configuration mode.

You can disable compression for a specific group or user for WebVPN connections with the **http-comp** command, or for SVC connections with the **svc compression** command, in the group policy or username webvpn modes.

For more information, see “Using SVC Compression” in *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Active/Standby Stateful Failover for WebVPN and SVC Connections

During a failover, WebVPN and SVC connections, as well as IPSec connections, are reestablished with the secondary, standby security appliance for uninterrupted service. Active/standby failover requires a one-to-one active/standby match for each connection.

A security appliance configured for failover shares authentication information about WebVPN users with the standby security appliance. Therefore, after a failover, WebVPN users do not need to reauthenticate.

For SVC connections, after a failover, the SVC reconnects automatically with the standby security appliance.

For more information, severing SVC Sessions” in *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

WebVPN Customization

You can customize the WebVPN page that users see when they connect to the security appliance, and you can customize the WebVPN home page on a per-user, per-group, or per-tunnel group basis. Users or groups see the custom WebVPN home page after the security appliance authenticates them.

You can use ASDM or CLI commands to customize the WebVPN appearance using Cascading Style Sheet (CSS) parameters. To easily customize, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

For more information, see “Customizing WebVPN Pages” in *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

ASDM Improvements

ASDM Improvements include the following:

Management and Monitoring Support for the CSC SSM

ASDM Version 5.1 delivers an industry-first solution that blends the simplicity of Trend Micro’s HTML-based configuration panels with the ingenuity of ASDM. This helps ensure consistent policy enforcement, and simplifies the complete provisioning, configuration, and monitoring processes for the rich unified threat management functions offered by the CSC SSM. ASDM provides a complementing monitoring solution with a new CSC SSM homepage and new monitoring panels. Once a CSC SSM is installed, the main ASDM homepage is automatically updated to display a new CSC SSM panel, which provides a historic view into threats, e-mail viruses, live events, and vital module statistics such as last

installed software/signature updates, system resources, and more. Within the monitoring section of ASDM, a rich set of analysis tools provide detailed visibility into threats, software updates, resource graphs, and more. The Live Security Event Monitor is a new troubleshooting and monitoring tool that provides real-time updates regarding scanned or blocked e-mail messages, identified viruses/worms, detected attacks, and more. It gives administrators the option to filter messages using regular-expression string matching, so specific attack types and messages can be focused on and analyzed in detail.

Syslog to Access Rule Correlation

This ASDM release introduces a new Syslog to Access Rule Correlation tool that greatly enhances day-to-day security management and troubleshooting activities. With this dynamic tool, security administrators can quickly resolve common configuration issues, along with most user and network connectivity problems. Users can select a syslog message within the Real-Time Syslog Viewer panel, and by simply clicking the Create button at the top of the panel, can invoke the access-control options for that specific syslog. Intelligent defaults help ensure that the configuration process is simple, which helps improve operational efficiency and response times for business-critical functions. The Syslog to Access Rule Correlation tool also offers an intuitive view into syslog messages invoked by user-configured access rules.

Customized Syslog Coloring

ASDM allows for rapid critical system message identification and convenient syslog monitoring by allowing the colored grouping of syslog messages according to syslog level. Users can select the default coloring options, or create their own unique colored syslog profiles for ease of identification.

Auto Applet Download

To run a remote application over WebVPN, a user clicks Start Application Access on the WebVPN homepage to download and start a port-forwarding Java applet. To simplify application access and shorten start time, you can now configure WebVPN to automatically download this port-forwarding applet when the user first logs in to WebVPN.

For more information, see “Downloading the Port-Forwarding Applet Automatically” in *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Important Notes

This section lists important notes related to version 7.1(1).

SSL VPN licenses

Beginning with Version 7.1(1), SSL VPN (WebVPN) services require a license. These services are now licensed on a per-user session basis, with licensing levels at 10, 50, 100, 250, 500, 750, 1000, and 2500 user sessions. The complete SSL VPN feature functionality offered by the adaptive security appliance is included in this single SSL VPN license. No per-feature licenses are required. This SSL VPN license has a one-time fee and lasts for the lifetime of the adaptive security appliance. Upon installation of Version 7.1(1) or later, two simultaneous SSL VPN user sessions are included for evaluation.

WebVPN and Subinterfaces

You cannot enable WebVPN on a subinterface.

ActiveX and WebVPN

Many ActiveX controls are custom and require special treatment by WebVPN. Please contact Cisco TAC if your application uses ActiveX controls and you have problems with its functionality over a WebVPN connection (CSCsb85180).

CIFS Files

If a remote user accesses CIFS files using Internet Explorer, the filename in the File Download window might not display some Japanese Shift_JIS characters correctly. However, the Open and Save functions do work properly. This issue does not occur with Netscape.

Failover and WebVPN and SVC connections

To ensure that WebVPN and SVC connections reconnect quickly in the event of a failover, enable the security appliance to respond to incoming client TCP packets with the **service resetoutside** command from global configuration mode:

```
[no] service resetoutside
```

This command causes the security appliance that takes over the existing WebVPN and SVC connections to send TCP RST packets in response to incoming client TCP packets, causing client connections to reestablish quicker. If you do not enable the **service resetoutside** command, the security appliance drops TCP packets from failed-over connections and waits for each client to reestablish the TCP connection. This may take longer or result in the session being lost due to timeout.

The following example enables the security appliance to send TCP RST packets:

```
F1-asal(config)# service resetoutside
```

FIPS 140-2

The adaptive security appliances are on the FIPS 140-2 Pre-Validation List.

WebVPN ACLS and DNS Hostname

When a deny webtype URL ACL (DNS-based) is defined, but the DNS-based URL is not reachable, the browser displays “DNS Error” popup. The ACL hit counter does not increment.

If an IP address rather than a DNS name defines a deny webtype URL, then the hit counter does record the traffic flow hitting the ACL, and the browser displays a “Connection Error.”

Proxy Server and ASA

If WebVPN is configured to use an HTTP(S)-proxy server to service all requests for browsing HTTP and/or HTTPS sites, the client/browser may expect the following behavior:

1. If the ASA cannot communicate with the HTTPS or HTTPS proxy server, a “connection error” is displayed on the client browser.
2. If the HTTP(S) proxy cannot resolve or reach the requested URL, it should send an appropriate error to the ASA, which in turn displays it on the client browser.

Only when the HTTP(S) proxy server notifies the ASA of the inaccessible URL, can the ASA notify the client browser about the error.

Mismatch PFS

The PFS setting on the VPN client and the security appliance must match.

Readme Document for the Conduits and Outbound List Conversion Tool 1.2

The adaptive security appliance Outbound/Conduit Conversion tool assists in converting configurations with **outbound** or **conduit** commands to similar configurations using ACLs. ACL-based configurations provide uniformity and leverage the powerful ACL feature set. ACL based configurations provide the following benefit:

- ACE Insertion capability - System configuration and management is greatly simplified by the ACE insertion capability that allows users to add, delete or modify individual ACEs.

VPN Load Balancing Requirements

VPN load balancing for the adaptive security appliance requires an ASA 5520 or ASA 5540. It also requires a 3DES-AES encryption license.

User Upgrade Guide

- For a list of deprecated features, and user upgrade information, go to the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_70/migr_vpn/index.htm

Features not Supported in Version 7.1(1)

The following features are not supported in Version 7.1(1):

- PPPoE
- L2TP over IPSec
- PPTP

MIB Support

For information on MIB Support, go to:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

Downgrading to a Previous Version

To downgrade to a previous version of the operating system software (software image), use the **downgrade** command in privileged EXEC mode. For more information and a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Open Caveats, Release 7.1(1)

The following open caveats are new in Release 7.1(1).

CSCsb85180

Terminal Services ActiveX client component is not operational via WebVPN.

Workaround: Use the SSL VPN Client (full-tunnel client) to handle this application

CSCsc27946

While using WebVPN clientless access to a Domino web access server, you cannot edit the Domino homepage layout. When you try, an Internet Explorer error occurs.

CSCsc93042

Yahoo game Java applets might fail to load through the WebVPN rewrite engine.

Workaround: Load the Java applet directly, not through WebVPN.

CSCsd00382

SVC connections have downloadable access-lists associated with them. Logging off the session (**vpn-sessiondb logoff** command) might result in the access-list remaining on the security appliance and potentially interfering with new connections with the same IP address.

CSCsd02916

When using http-proxy, users can access Citrix over a WebVPN connection, even though Citrix metafile is not configured for the group policy.

CSCsd04381

When you attempt to add a file attachment to an existing contact within Outlook Web Access 2000 or 2003 through the WebVPN rewrite engine, a blank modal window opens.

Workaround: Create a new contact and apply an attachment through the rewrite engine. A second option is to access the Outlook Web Access 2000 or 2003 servers directly, and not through WebVPN to initiate the attachment routine to an existing contact.

CSCsd08212

A Weetype ACL with a URI syntax similar to “http(s)://host address/path,” fails the ACL check routine. If this is a permit rule, users cannot access that website. However, a Weetype ACL rule with the URI similar to “http(s)://host address” works. The difference between these two ACLs is the “/path”. The “/path” might be any share within the specified website, either a file or directory.

Workaround: Define Webytype ACLS with the URI syntax http(s)://host address, for example, access-list test webytype permit url http://serverA.com).

Caveats, Release 7.0(4)

The following sections describe the caveats for the 7.0(4) version.

For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.



Note

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

<http://www.cisco.com/support/bugtools>

To become a registered cisco.com user, go to the following website:

<http://tools.cisco.com/RPF/register/register.do>

Open Caveats - Release 7.0(4)

Table 3 list the caveats that remain open from Release 7.0(4).

Table 3 Open Caveats

ID Number	Software Release 7.0(4)	
	Corrected	Caveat Title
CSCeg57001	No	Packet does not come to inspect after no inspect and inspect
CSCeh15557	No	Assertion in tmatch_compile_proc, all memory is not freed.
CSCeh32087	No	PIM sends Register with untranslated IP when NAT pool exhausted.
CSCeh43554	No	Device may reload if showing and removing config at the same time
CSCeh60845	No	Logging queue incorrectly registers 8192 256-byte blocks
CSCeh84006	No	Wrong http version number should not be allowed
CSCeh93834	No	RSA SecurID replica list is lost after reboot
CSCej04099	No	static xlate breaks management-access inside
CSCsb28708	No	Console traceback using show route command
CSCsb40188	No	SCEP fails if RA cert has 4096 bit key
CSCsb41742	No	P2P/IM/tunneling traffic is only dropped if strict-http action is drop

Table 3 Open Caveats (continued)

ID Number	Software Release 7.0(4)	
	Corrected	Caveat Title
CSCsb51038	No	Traceback: _snp_sp_create_flow+1937 with outbound ACL and Policy Statics
CSCsb80170	No	Address-pools needed in group-policy - missing functionality from VPN3K
CSCsb81593	No	removing sunrpc-server cli doesn't stop sunrpc traffic from getting through
CSCsb90046	No	GTP context creation might fail w/ Tunnel Limit exceeded error
CSCsb99385	No	strict-http: with a space before http ver should generate a tcp reset
CSCsc01017	No	ASA to VPN3K L2L fails rekey w/ main mode, 3des, sha, rsa, pfs-2, dh-2
CSCsc07421	No	Traceback in Dispatch Unit - decoding h323 ras message
CSCsc10617	No	GTP: memory leakage after <clear config all> at gtp_init
CSCsc11724	No	Logging: Wrong behavior if syslog is sent to a non functioning tcp server
CSCsc12094	No	AAA fallback authentication does not work with reactivation-mode timed
CSCsc16041	No	'clear local host' results in memory leak
CSCsc16607	No	fixup pptp fails with static pat server configuration
CSCsc17051	No	VPNFO: VPN Failover fails to parse P2 SA when IPCOMP is used
CSCsc18911	No	ASA does not remove OSPF route for global PAT entry after deleting

Resolved Caveats Open in Release 7.0(4)

Table 4 lists the caveats resolved since Release 7.0(4).

Table 4 Resolved Caveats

ID Number	Software Version 7.1(1)	
	Corrected	Caveat Title
CSCeh18115	Yes	Authentication not triggered sometimes when URL filtering enabled.
CSCeh46345	Yes	Dynamic L2L could pass clear text traffic when tunnel terminates
CSCeh90617	Yes	Recompiling ACLs can cause packet drops on low-end platforms
CSCei02273	Yes	1st log message is not sent by mail in transparent firewall
CSCei43588	Yes	traceback when trying to match a packet to acl with deny
CSCsc00176	Yes	clear xlate take 4.5+ mins to clear 60K PAT xlate
CSCsc02485	Yes	Session Cmd: sendind \036x\r to exit session to ssm causes Traceback
CSCsc07614	Yes	Minimum unit poll time causes trouble for failover with 4GE card
CSCsc14591	Yes	xlate and xlate perfmon print graph are all zeros
CSCsc15434	Yes	Assertion violation w/icmp traffic and icmp inspection
CSCsc16503	Yes	Transparent firewall ASR UDP out traffic got errors and inbound failed
CSCsc17409	Yes	dhcprelay: ASA blocks RELEASE packets
CSCsc17428	Yes	Tracebacks with ci/console with 'clear config all'
CSCsc18444	Yes	Tunnel-group for specific peer not created upgrading to 7.0 w/ certs

Related Documentation

For additional information on the adaptive security appliance, refer to the following documentation found on Cisco.com:

- *Cisco ASA 5500 Hardware Installation Guide*
- *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*
- *Cisco ASDM Release Notes*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Migrating to ASA for VPN 3000 Series Concentrator Administrators*
- *Release Notes for Cisco SSL VPN Client*
- *Cisco Secure Desktop Configuration Guide*
- *Release Notes for Cisco Secure Desktop*
- *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*
- *Selected ASDM VPN Configuration Procedures for the Cisco ASA 5500 Series*
- *Cisco Security Appliance Logging Configuration and System Log Messages*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.

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, CCIIP, 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.

©2006 Cisco Systems, Inc. All rights reserved.

