



Cisco ASA 5500 Series Release Notes Version 7.0(2)

July 2005

Contents

This document includes the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New Features, page 3](#)
- [Important Notes, page 35](#)
- [Caveats, page 37](#)
- [Related Documentation, page 40](#)
- [Obtaining Documentation and Submitting a Service Request, page 40](#)

Introduction

The Cisco ASA 5500 series security appliance delivers unprecedented levels of defense against threats to the network with deeper web inspection and flow specific analysis, improved secure connectivity through end point security posture validation and voice and video over VPN support. It also provides enhanced support for intelligent information networks through improved network integration, resiliency, and scalability. This release introduces significant enhancements to all major functional areas, including: firewalling and inspection services, VPN services, network integration, high availability services, and management/monitoring.



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

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

Additionally, the Cisco ASA 5500 series security appliance software supports Adaptive Security Device Manager. ASDM is a browser-based, Java applet used to configure and monitor the software on the security appliances. ASDM is loaded from the security appliance, then used to configure, monitor, and manage the device.

System Requirements

The sections that follow list the system requirements for operating a Cisco ASA 5500 series security appliance. This section includes the following:

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

Memory Requirements

[Table 1](#) lists the DRAM memory requirements for the Cisco ASA 5500 series security appliance.

Table 1 *DRAM Memory Requirements*

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

All Cisco ASA 5500 series 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 Release

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

<http://www.cisco.com/public/sw-center/index.shtml>

New Features

New Features

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

- [Advanced Firewall Services, page 3](#)
- [Application-Aware Inspection Services, page 8](#)
- [Virtual Private Networking \(VPN\) Services, page 12](#)
- [WebVPN, page 18](#)
- [Network Integration, page 20](#)
- [High Availability, page 22](#)
- [Management and Monitoring, page 25](#)

Advanced Firewall Services

Transparent Firewall (Layer 2 Firewall)

This feature has the ability to deploy the security appliance in a secure bridging mode, similar to a Layer 2 device, to provide rich Layer 2 – 7 firewall security services for the protected network. This enables businesses to deploy this security appliance into existing network environments without requiring readdressing of the network. While the security appliance can be completely “invisible” to devices on both sides of a protected network, administrators can manage it via a dedicated IP address (which can be hosted on a separate interface). Administrators have the ability to specify non-IP (EtherType) ACLs, in addition to standard ACLs, for access control over Layer 2 devices and protocols.

To configure transparent firewall on the security appliance, see the “Firewall Mode Overview” and “TransparentMode Overview” sections in the *Cisco Security Appliance Command Line Configuration Guide*. The following commands are added for the transparent firewall: **arp-inspection**, **firewall**, **mac-address-table**, and **mac-learn**.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Security Contexts (Virtual Firewall)

This feature introduces the ability to create multiple security contexts (virtual firewalls) within a single appliance, with each context having its own set of security policies, logical interfaces, and administrative domain. This provides businesses a convenient way of consolidating multiple firewalls into a single physical appliance, yet retaining the ability to manage each of these virtual instances separately. These capabilities are only available on adaptive security appliance with either unrestricted (UR) or failover (FO) licenses. This is a licensed feature, with multiple tiers of supported security contexts (2, 5, 10, 20, and 50).

To configure security contexts on the security appliance, see the “Enabling Multiple Context Mode” and “Adding and Managing Security Contexts” section in the *Cisco Security Appliance Command Line Configuration Guide*. Some of the commands added for the security contexts are: **admin-context**, **context**, **changeto**, and **mode**.

**Note**

The **context** command enters the context configuration mode which has additional commands.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Downloadable Access Control Lists (ACLs)

This feature supports the download of ACLs to the adaptive security appliance from an access control server (ACS). This enables the configuration of per-user access lists on a AAA server, to provide per-user access list authorization, that are then downloadable through the ACS to the adaptive security appliance.

This feature is supported for RADIUS servers only and is not supported for TACACS+ servers.

For more information, see the “Configuring Any RADIUS Server for Downloadable ACLs” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

ACL Editing

The ACL editing feature provides users flexibility to insert or delete any access list element in an access list.

For more information, see the “Access List Overview” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Syslog by ACL Entry

This feature allows users to configure a specific ACL entry with a logging option. When such an option is configured, statistics for each flow that matches the permit or deny conditions of the ACL entry are logged.

For more information, see the “Logging Access List Activity” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Comments/Remarks in ACLs

This feature allows users to include comments in access lists to make the ACL easier to understand and scan.

For more information, see the “Adding Remarks to Access Lists” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Interface Name as Address in ACLs

Users running the DHCP client on the adaptive security appliance outside interface will no longer have to adjust their access lists every time the outside DHCP address is changed by their ISP.

For more information, see the “Inbound and Outbound Access List Overview” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Outbound ACLs and Time-based ACLs

This feature gives administrators improved flexibility for defining access control policies by adding support for outbound ACLs and time-based ACLs (building on top of our existing inbound ACL support). Using these new capabilities, administrators can now apply access controls as traffic enters an interface or exits an interface. Time-based access control lists provide administrators greater control over resource usage by defining when certain ACL entries are active. New commands allow administrators to define time ranges, and then apply these time ranges to specific ACLs.

The existing versatile **access-list** global configuration command was extended with the **time-range** command to specify a time-based policy defined using the **time-range** global configuration command. Additionally, the **access-group** global configuration command supports the **out** keyword to configure an outbound ACL. For more information, see the “Inbound and Outbound Access List Overview” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Enabling/Disabling of ACL Entries

This feature provides a convenient troubleshooting tool that allows administrators to test and fine-tune ACLs, without the need to remove and replace ACL entries.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Incomplete Crypto Map Enhancements

Every static crypto map must define an access list and an IPsec peer. If either is missing, the crypto map is considered incomplete and a warning message is printed. Traffic that has not been matched to an complete crypto map is skipped, and the next entry is tried. Failover hello packets are exempt from the incomplete crypto map check.

For more information on this feature, see the “Defining Crypto Maps” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Auto Update Support

This release supports Auto Update, a next-generation feature set for Cisco and third-party applications, that provides secure remote network management.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

EtherType Access Control

This feature includes very powerful support for performing packet filtering and logging based on the EtherType of the packets. When operating as a transparent firewall, this provides tremendous flexibility for permitting or denying non-IP protocols.

For more information, see the “Permitting or Denying Network Access” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Modular Policy Framework

This feature introduces a highly flexible and extensible next-generation modular policy framework. It enables the construction of flow-based policies that identify specific flows based on administrator-defined conditions, and then apply a set of services to that flow (such as firewall/inspection policies, VPN policies, QoS policies, and more). This provides significantly improved granular control over traffic flows, and the services performed on them. This new framework also enables inspection engines to have flow-specific settings (which were global in previous releases).

The **class-map**, **policy-map**, and **service-policy** commands were added to support this feature. For more information, see the “Using Modular Policy Framework” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

DHCP Option 66 and 150 Support

This feature enhances the DHCP server on the inside interface of the adaptive security appliance to provide TFTP address information to the served DHCP clients. The implementation responds with one TFTP server for DHCP option 66 requests and with, at most, two servers for DHCP option 150 requests.

DHCP options 66 and 150 simplify remote deployments of Cisco IP Phones and Cisco SoftPhone by providing the Cisco CallManager contact information needed to download the rest of the IP phone configuration.

For more information, see the “Configuring DHCP” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

DHCP Server Support on Multiple Interfaces

This release allows as many integrated Dynamic Host Configuration Protocol (DHCP) servers to be configured as desired, and on any interface. DHCP client and DHCP relay agent can be configured concurrently, as long as it isn't on the same interface. However, DHCP server and DHCP relay agent cannot be configured concurrently on the same adaptive security appliance, but DHCP client and DHCP relay agent can be configured concurrently. DHCP client is not allowed when the appliance is in failover mode.

The **[no] dhcpd address ip1[-ip2] if_name** command now allows DHCP servers to be configured as desired on any interface in the adaptive security appliance.

For more information, see the “Configuring DHCP” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

DHCP Relay

Acting as a DHCP relay agent, the adaptive security appliance can assist in dynamic configuration of IP hosts on any of its interfaces. It receives requests from hosts on a given interface and forwards them to a user-configured DHCP server on another interface. This can work in conjunction with site- to-site or Easy VPN, enabling businesses to centrally manage their IP address.

This release supports the **dhcprelay enable** command. For more information on the **dhcprelay enable** command, see the “Configuring DHCP” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

DHCP Support

The adaptive security appliance Dynamic Host Configuration Protocol (DHCP) client/server support lets the user automatically leverage the DNS, WINS, and domain name values obtained by the adaptive security appliance DHCP client for use by the hosts served by the DHCP server.

The **ip address** and **dhcpd** commands provide DHCP client/server support.

For more information, see the “Configuring DHCP” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Assignable Syslog Levels by Message

This release includes the ability to reassign the level of any syslog, allowing easy grouping of syslogs of interest.

The *level* option is added to the **login** command. For more information on this command, see the “Using System Log Messages” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Custom Logging Identifier

Allows a custom firewall identifier to be selected, such as an interface IP address, that will be included in all syslog messages to improve the centralized reporting of firewall events.

This new feature is added to the **login** command. For configuration information, see the “Using System Log Messages” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Cisco Logging Format

This feature will help users to log messages in Cisco EMBLEM format to a syslog server. The EMBLEM format is available for both messages with and without timestamp.

This new feature is added to the **login** command. For configuration information, see the “Using System Log Messages” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

clear logging Command

The **clear configure logging** command works in privileged mode.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Application-Aware Inspection Services

Advanced HTTP Inspection Engine

This feature introduces deep analysis of web traffic, enabling granular control over HTTP sessions for improved protection from a wide range of web-based attacks. In addition, this new HTTP inspection engine allows administrative control over instant messaging applications, peer-to-peer file sharing applications, and applications that attempt to tunnel over port 80 or any port used for HTTP transactions. Capabilities provided include RFC compliance enforcement, HTTP command authorization and enforcement, response validation, Multipurpose Internet Mail Extension (MIME) type validation and content control, Uniform Resource Identifier (URI) length enforcement, and more.

A user can define the advanced HTTP Inspection policy using the **http-map** global configuration command and then apply it to the **inspect http** configuration mode command that was extended to support the specification of a map name. For more information, see the “Managing HTTP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

FTP Inspection Engine

This feature includes the FTP inspection engine which provides new command filtering support. Building upon the FTP security services previously supported, such as protocol anomaly detection, protocol state tracking, NAT/PAT support, and dynamic port opening, Version 7.0 gives administrators granular control over the usage of 9 different FTP commands, enforcing operations that users/groups can perform in FTP sessions. Version 7.0 also introduces FTP server cloaking capabilities, hiding the type and version of the FTP server from those who access it through adaptive security appliance.

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

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

ESMTP Inspection Engine

This feature builds on the SMTP (RFC 821) feature with the addition of support for the SMTP (ESMTP) protocol, featuring a variety of commands defined in RFC 1869. Supported commands include **AUTH**, **DATA**, **EHLO**, **ETRN**, **HELO**, **HELP**, **MAIL**, **NOOP**, **QUIT**, **RCPT**, **RSET**, **SAML**, **SEND**, **SOML**, and **VERFY** (all other commands are automatically blocked to provide an additional level of security).

The **inspect esmtp** global configuration command provides inspection services for SMTP and ESMTP traffic. For more information, see the “Managing SMTP and Extended SMTP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

SunRPC / NIS+ Inspection Engine

The SunRPC inspection engine provides better support for NIS+ and SunRPC services. Specific enhancements include support for all three versions of the lookup service - Portmapper v2 and RPCBind v3 and v4.

Use the **inspect sunrpc** and the **sunrpc-server** global configuration commands to configure the SunRPC / NIS+ inspection Engine.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

ICMP Inspection Engine

This feature introduces an ICMP inspection engine. This engine enables secure usage of ICMP, by providing stateful tracking for ICMP connections, matching echo requests with replies. Additional controls are available for ICMP error messages, which are only permitted for established connections.

Use the **inspect icmp** and the **inspect icmp error** commands to configure the ICMP inspection engine.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

GTP Inspection Engine for Mobile Wireless Environments

This feature introduces a new inspection engine for securing 3G Mobile Wireless environments that provide packet switched data services using the GPRS Tunneling Protocol (GTP). These new advanced GTP inspection services permit mobile service providers secure interaction with roaming partners and provide mobile administrators robust filtering capabilities based on GTP specific parameters such as IMSI prefixes, APN values and more. This is a licensed feature.

The **inspect gtp** command in the policy-map configuration mode and the **gtp-map** global configuration commands are new features introduced in Version 7.0. For more information on GTP and detailed instructions for configuring your GTP inspection policy, see the “Managing GTP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*. You may need to install a GTP activation key using the **activation-key exec** command.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

H.323 Inspection Engine

The H.323 inspection engine adds support for the T.38 protocol, an ITU standard that enables the secure transmission of Fax over IP (FoIP). Both real-time and store-and-forward FAX methods are supported. The H.323 inspection engine supports Gatekeeper Routed Call Signaling (GKRCS) in addition to the Direct Call Signaling (DCS) method currently supported. GKRCS support, based on the ITU standard, now allows the security appliance to handle call signaling messages exchanged directly between H.323 Gatekeepers.

For more information, see the “Managing H.323 Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

H.323 Version 3 and 4 Support

This release supports NAT and PAT for H.323 versions 3 and 4 messages, and in particular, the H.323 v3 feature Multiple Calls on One Call Signaling Channel.

For more information on this command, see the “H.323Inspection Overview” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

SIP Inspection Engine

This feature adds support for Session Initiation Protocol (SIP)-based instant messaging clients, such as Microsoft Windows Messenger. Enhancements include support for features described by RFC 3428 and RFC 3265.

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

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Support for Instant Messaging Using SIP

Fixup SIP now supports the Instant Messaging (IM) Chat feature on Windows XP using Windows Messenger RTC client version 4.7.0105 only.

For more information, see the “SIP Inspection Overview” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Configurable SIP UDP Inspection Engine

This provides a CLI-enabled solution for non-Session Information Protocol (SIP) packets to pass through the adaptive security appliance instead of being dropped when they use a SIP UDP port.

For more information on this command, see the “SIP Inspection Overview” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

MGCP Inspection Engine

This feature includes an MGCP inspection engine that supports NAT and PAT for the MGCP protocol. This ensures seamless security integration in distributed call processing environments that include MGCP Version 0.1 or 1.0 as the VoIP protocol.

The **inspect mgcp** command in the policy-map configuration mode and the **mgcp-map** global **configuration** command enables the user to configure MGCP inspection policy. For more information, see the “Managing MGCP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

RTSP Inspection Engine

This feature introduces NAT support for the Real Time Streaming Protocol (RTSP), which allows streaming applications such as Cisco IP/TV, Apple Quicktime, and RealNetworks RealPlayer to operate transparently across NAT boundaries.

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

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

SNMP Inspection Engine

Similar to other new inspection engines, the **inspect snmp** command in policy-map configuration mode and the **snmp-map** global configuration command enables the user to configure an SNMP inspection policy. For more information, see the “Managing SNMP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

TCP Security Engine

This feature introduces several new foundational capabilities to assist in detecting protocol and application layer attacks. TCP stream reassembly helps detect attacks that are spread across a series of packets by reassembling packets into a full packet stream and performing analysis of the stream. TCP traffic normalization provides additional techniques to detect attacks including advanced flag and option checking, detection of data tampering in retransmitted packets, TCP packet checksum verification, and more.

You can configure the extensive TCP security policy using the **set connection advanced-options** in global configuration command and **tcp-map** global configuration command.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Improved URL Filtering Performance

This feature significantly increases the number of concurrent URLs that can be processed by improving the communications channel between the adaptive security appliance and the Websense servers.

The existing **url-server** global configuration command now supports the **connections** keyword to specify the number of TCP connections in the pool that is used. For more information, see the “Applying Filtering Services” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

URL Filtering Enhancements

This release supports N2H2 URL filtering services for URLs up to 1159 bytes.

For Websense, long URL filtering is supported for URLs up to 4096 bytes in length.

Additionally, this release provides a configuration option to buffer the response from a web server if its response is faster than the response from either an N2H2 or Websense filtering service server. This prevents the web server’s response from being loaded twice.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Virtual Private Networking (VPN) Services

IPSec

Spoke-to-Spoke VPN Support

This feature improves support for spoke-to-spoke (and client-to-client) VPN communications, by providing the ability for encrypted traffic to enter and leave the same interface. Furthermore, split-tunnel remote access connections can now be terminated on the outside interface for the security appliance, allowing Internet-destined traffic from remote access user VPN tunnels to leave on the same interface as it arrived (after firewall rules have been applied).

The **same-security-traffic** command permits traffic to enter and exit the same interface when used with the **intra-interface** keyword enabling spoke-to-spoke VPN support. For more information, see the “Permitting Intra-Interface Traffic” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

OSPF Dynamic Routing over VPN

Support for OSPF has been extended to support neighbors across an IPsec VPN tunnel. This allows the adaptive security appliance to support dynamic routing updates across a VPN tunnel to other OSPF peers. OSPF hellos are unicast and encrypted for transport down the tunnel to an identified neighbor in an RFC-compliant manner.

The **ospf network point-to-point non-broadcast** command in interface configuration mode extends comprehensive OSPF dynamic routing services to support neighbors across IPsec VPN tunnels, providing improved network reliability for VPN connected networks. For more information, see the “Configuring OSPF” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

OSPF Dynamic Routing

Route propagation and greatly reduced route convergence times are two of the many benefits that arrive with Open Shortest Path First (OSPF). The adaptive security appliance implementation will support intra-area, inter-area and external routes. The distribution of static routes to OSPF processes and route redistribution between OSPF processes are also included.

To configure OSPF routing on the adaptive security appliance, see the “Configuring OSPF” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Remote Management Enhancements

This feature enables administrators to remotely manage firewalls over a VPN tunnel using the inside interface IP address of the remote adaptive security appliance. In fact, administrators can define any adaptive security appliance interface for management-access. This feature supports ASDM, SSH, Telnet, SNMP, and so on, that requires a dynamic IP address. This feature significantly benefits broadband environments.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

X.509 Certificate Support

Support for X.509 certificates has been significantly improved in the adaptive security appliance, adding support for n-tier certificate chaining (for environments with a multi-level certification authority hierarchy), manual enrollment (for environments with offline certificate authorities), and support for 4096-bit RSA keys. Version 7.0 also includes support for the new certificate authority introduced in Cisco IOS software, a lightweight X.509 certificate authority designed to simplify roll-out of PKI-enabled site-to-site VPN environments.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Easy VPN Server

This release supports Cisco Easy VPN server. Cisco Easy VPN server is designed to function seamlessly with existing VPN headend configured to support Cisco VPN client and to minimize the administrative overhead for the client by centralizing VPN configuration at the Cisco Easy VPN server. Examples of Cisco Easy VPN server products include the Cisco VPN client v3.x and greater and the Cisco VPN 3002 Hardware client.



Note

The adaptive security appliance already acts as a central site VPN device and supports the termination of remote access VPN clients.

Easy VPN Server Load Balancing Support

The ASA 5500 adaptive security appliance can participate in cluster-based concentrator load balancing. It supports VPN 3000 series concentrator load balancing with automatic redirection to the least utilized concentrator.

For more information on this command, see the “Enabling Redundancy” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Dynamic Downloading of Backup Easy VPN Server Information

Support for downloading a list of backup concentrators defined on the headend.

This feature supports the `vpngroup group_name backup-server {{ip1 [ip2... ip10]} | clear-client-cfg}` commands.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Easy VPN Internet Access Policy

The adaptive security appliance changes the behavior of a security appliance used as an Easy VPN remote device in regard to Internet access policy for users on the protected network. The new behavior occurs when split tunneling is enabled on the Easy VPN server. Split tunneling is a feature that allows users connected through the security appliance to access the Internet in a clear text session, without using a VPN tunnel.

The adaptive security appliance used as an Easy VPN remote device downloads the split tunneling policy and saves it in its local Flash memory when it first connects to the Easy VPN server. If the policy enables split tunneling, users connected to the network protected by the adaptive security appliance can connect to the Internet regardless of the status of the VPN tunnel to the Easy VPN server.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Verify Certificate Distinguished Name

This feature enables the adaptive security appliances acting as either a VPN peer for site to site, or as the Easy VPN server in remote access deployments to validate matching of a certificate to an administrator specified criteria.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Easy VPN Web Interface for Manual Tunnel Control User Authentication and Tunnel Status

With the introduction of the User-Level Authentication and Secure Unit Authentication, features the adaptive security appliance delivers the ability to enter the credentials, connect/dis-connect the tunnel and monitor the connection using new web pages served to users when attempting access to the VPN tunnel or unprotected networks through the security appliance. This is only applicable to the Easy VPN server feature.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

User-Level Authentication

Support for individually authenticating clients (IP address based) on the inside network of the adaptive security appliance. Both static and One Time Password (OTP) authentication mechanisms are supported. This is done through a web-based interface.

This feature adds support to the **vpn-group-policy** command. For more information on this command, see the “Configuring Users” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Secure Unit Authentication

This feature provides the ability to use dynamically generated authentication credentials to authenticate the Easy VPN remote (VPN Hardware client) device.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Flexible Easy VPN Management Solutions

Managing the adaptive security appliance using the outside interface will not require the traffic to flow over the VPN tunnel. You will have the flexibility to require all NMS traffic to flow over the tunnel or fine tune this policy.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

VPN Client Security Posture Enforcement

This feature introduces the ability to perform VPN client security posture checks when a VPN connection is initiated. Capabilities include enforcing usage of authorized host-based security products (such as the Cisco Security Agent) and verifying its version number, policies, and status (enabled/disabled).

To set personal firewall policies that the security appliance pushes to the VPN client during IKE tunnel negotiation, use the **client-firewall** command in group-policy configuration mode.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

VPN Client Update

To configure and change client update parameters, use the **client-update** command in tunnel-group ipsec-attributes configuration mode. For more information, see the “Configuring Group Policies” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

VPN Client Blocking by Operating System and Type

This feature adds the ability to restrict the different types of VPN clients (software client, router, VPN 3002, and PIX) that are allowed to connect based on type of client, operating system version installed, and VPN client software version. When non-compliant users attempt to connect, they can be directed to a group that specifically allows connections from non-compliant users.

To configure rules that limit the remote access client types and versions that can connect via IPsec through the security appliance, use the **client-access-rule** command in group-policy configuration mode. For more information, see the “Configuring Group Policies” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Movian VPN Client Support

This feature introduces support for handheld (PocketPC and Palm) based Movian VPN clients, securely extending access to your network to mobile employees and business partners.

New support for Diffie-Hellman Group 7 (ECC) to negotiate perfect forward secrecy was added to Version 7.0. This option is intended for use with the MovianVPN client, but can be used with other clients that support D-H Group 7 (ECC).

Bi-Directional Network Address Translation (NAT)

This feature allows Network Address Translation (NAT) of external source IP addresses for packets traveling from the outside interface to an the inside interface. All functionality available with traditional NAT such as fixups, Stateful Failover, dynamic NAT, static NAT, and PAT are available bidirectionally in this release.

For more information, see the “Policy NAT” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Policy NAT

Policy NAT allows you to identify both the source and destination addresses in an access list when specifying the local traffic to translate. This feature lets you use different global addresses for each source and destination pair on an interface, even if the source address is the same for each pair. Without policy NAT, you can only specify a single global address for a given source address, because the destination address is not considered. To configure policy NAT, use either the **static** or **nat** commands.

For more information, see the “Policy NAT” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Optional Address Translation Services

This feature introduces the “nat-control” configuration option, which allows NAT to be enabled incrementally.

For new security appliances or devices which have their configurations cleared, the default will be to not require a NAT policy for traffic to traverse the security appliance. For more information, see the “NAT Control” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

VPN NAT Transparency

This feature extends support for site-to-site and remote-access IPSec-based VPNs to network environments that implement NAT or PAT, such as airports, hotels, wireless hot spots, and broadband environments. Version 7.0 also adds support for Cisco TCP and User Datagram Protocol (UDP) NAT traversal methods as complementary methods to existing support for the IETF UDP wrapper mechanism for safe traversal through NAT/PAT boundaries.

See the **isakmp** global configuration command for additional options when configuring a NAT traversal policy. For more information, see the “Enabling IPSec over NAT-T” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

IKE Syslog Support

This feature introduces a small enhancement to IKE syslogging support and a limited set of IKE event tracing capabilities for scalable VPN troubleshooting. These enhancements have been added to allow for new syslog message generation and improved ISAKMP command control.

For more information on this feature, see the “Configuring ISAKMP” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Advanced Encryption Standard (AES)

This feature adds support for securing site-to-site and remote access VPN connections with the new international encryption standard. It also provides software-based AES support on all supported the adaptive security appliance models and hardware-accelerated AES via the new VAC+ card.

For more information on this feature, see the “Configuring ISAKMP” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Port Redirection

The adaptive security appliance provides static Port Address Translation (PAT) capability. This capability can be used to send multiple inbound TCP or UDP services to different internal hosts through a single global address. The global address can be a unique address, a shared outbound PAT, or shared with the external interface.

The **static** command is modified to accommodate this feature.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Port Address Translation (PAT) for H.323 and SIP Inspection Engines

This release enhances support for the existing H.323 and SIP inspection engines by adding support for Port Address Translation (PAT). Adding support for PAT with H.323 and SIP enables our customers to expand their network address space using a single global address.

For more information on this command, see the “SCCP Inspection Overview” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

PAT for Skinny

This feature allows Cisco IP Phones to communicate with Cisco CallManager across the adaptive security appliance when it is configured with PAT. This is particularly important in a remote access environment where Skinny IP phones behind a adaptive security appliance talk to the CallManager at the corporate site through a VPN.

For more information on this command, see the “SCCP Inspection Overview” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

WebVPN

WebVPN lets users establish a secure, remote-access VPN tunnel to a security appliance using a web browser. There is no need for either a software or hardware client. WebVPN provides easy access to a broad range of web resources and both web-enabled and legacy applications from any computer on the internet. WebVPN includes the following features:

Remote Access via Web Browser (WebVPN)

Version 7.0(1) supports WebVPN on ASA 5500 series security appliances in single, routed mode. WebVPN lets users establish a secure, remote-access VPN tunnel to the security appliance using a web browser. There is no need for either a software or hardware client. WebVPN provides easy access to a broad range of web resources and both web-enabled and legacy applications from almost any computer that can reach HTTPS Internet sites. WebVPN uses Secure Sockets Layer Protocol and its successor, Transport Layer Security (SSL/TLS1) to provide a secure connection between remote users and specific, supported internal resources that you configure at a central site. The security appliance recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users.

For more information on this command, see the “Using SSL to Access the Central Site” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

CIFS

WebVPN supports the Common Internet Files System, which lets remote users browse and access preconfigured NT/Active Directory file servers and shares at a central site. CIFS runs over TCP/IP and uses DNS and NetBIOS for name resolution.

For more information on this command, see the “Configuring WebVPN” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Port Forwarding

WebVPN port forwarding, also called application access, lets remote users use TCP-applications over an SSL VPN connection.

For more information on this command, see the “Creating Port Forwarding, URL, and Access Lists in Global Configuration Mode” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

E-mail

WebVPN supports several ways of using e-mail, including IMAP4S, POP3S, SMTPS, MAPI, and Web E-mail.

—IMAP4S, POP3S, SMTPS

WebVPN lets remote users use the IMAP4, POP3, and SMTP e-mail protocols over SSL connections.

—MAPI Proxy

WebVPN supports MAPI, which is remote access to e-mail via MS Outlook Exchange port forwarding. MS Outlook exchange must be installed on the remote computer.

—Web E-mail

Web e-mail is MS Outlook Web Access for Exchange 2000, Exchange 5.5, and Exchange 2003. It requires an MS Outlook Exchange Server at the central site.

For more information on this command, see the “Configuring Email” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Network Integration

Common Security-Level for Multiple Interfaces

This feature extends the security-level policy structure by enabling multiple interfaces to share a common security level. This allows for simplified policy deployments by allowing interfaces with a common security policy (for example two ports connected into the same DMZ, or multiple zones/departments within a network) to share a common security level. Communication between interfaces with the same security level is governed by the ACL on each interface.

See the **same-security-traffic** command and the **inter-interface** keyword to enable traffic between interfaces configured with the same security level. For more information, see the “Allowing Communication Between Interfaces on the Same Security Level” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

IPv6 Inspection, Access Control, and Management

This feature introduces support for IP version 6 (IPv6) inspection, access control, and management. Full stateful inspection is provided for through-the-box IPv6 traffic in both a dedicated IPv6 mode and in a dual-stack IPv4 / IPv6 mode. In addition, a security appliance can be deployed in a pure IPv6 environment, supporting IPv6 to-the-box management traffic for protocols including SSHv2, Telnet, HTTP, and ICMP. Inspection engines that support IPv6 traffic in Version 7.0 include HTTP, FTP, SMTP, UDP, TCP and ICMP.

For more information, see the “Config uring IPv6” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

fragment Command

The **fragment** command provides additional management of packet fragmentation and improves compatibility with NFS.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

HTTPS and FTP Web Request Filtering via Websense Integration

This feature extends the existing Websense-based URL filtering to HTTPS and FTP and introduces the **filter ftp** and **filter https** commands. For information on configuring this command, see the “Applying Filtering Services” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Secure HyperText Transfer Protocol (HTTPS) Authentication Proxy

This feature extends the capabilities of the adaptive security appliance to securely authenticate HTTP sessions and adds support for HTTPS Authentication Proxy. To configure secure authentication of HTTP sessions, use the **aaa authentication secure-http-client** command. To configure secure authentication of HTTPS sessions, use the **aaa authentication include https** or the **aaa authentication include tcp/0** command.

In this release configurations that include the **aaa authentication include tcp/0** command will inherit the HTTPS Authentication Proxy feature, which is enabled by default with a code upgrade to Version 6.3 or later.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Multicast Support (IGMP v2 and Stub Multicast Routing)

This release enables you to statically configure multicast routes or use an IGMP helper address for forwarding IGMP reports and leave announcements.

The following summarizes multicast support in this release:

- Access-list filters can be applied to multicast traffic to permit or deny specific protocols and ports.
- NAT and PAT can be performed on the multicast packet source addresses only.
- Multicast data packets with destination addresses in the 224.0.0.0/24 address range are not forwarded. However, everything else in the 224.0.0.0/8 address range is forwarded.
- IGMP packets for address groups within the 224.0.0.0-224.0.0.255 range are not forwarded because these addresses are reserved for protocol use.

NAT is not performed on IGMP packets. When IGMP forwarding is configured, the adaptive security appliance forwards the IGMP packets (report and leave) with the IP address of the helper interface as the source IP address.

Multicast Support

PIM sparse mode was added to allow direct participation in the creation of a multicast tree using PIM-SM. This capability extends existing multicast support for IGMP forwarding and for Class D access control policies and ACLs. PIM-SM provides an alternative to transparent mode operation in multicast environments.

The **pim** commands and the **multicast-routing** command added support to the new functionality in addition to the **show mrib EXEC** command in this feature. For more information, see the “Configuring Multicast Routing” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Network Time Protocol (NTP) Support

The Network Time Protocol (NTP) synchronizes the times of devices operating over an IP data network.

This release supports NTP, enabling the adaptive security appliance to act as an NTP client and synchronize its time to a network time server. This enables the adaptive security appliance to maintain precise network time for logging and certificate revocation list (CRL) validation. NTP server mode is not supported because the firewall would have to allow incoming requests to open ports, which is a security risk.

This release supports Version 3 of NTP as this is currently the most common version in use and is the highest version supported by Cisco IOS software. The NTP authentication mechanism uses MD5 and is compatible with Cisco IOS software.

Optional Address Translation Services

This feature simplifies deployment of the security appliance by eliminating previous requirement for address translation policies to be in place before allowing network traffic to flow. Now, only hosts and networks that require address translation will need to have address translation policies configured. This feature introduces a new configuration option, “nat-control”, which allows NAT to be enabled incrementally.

Version 7.0 introduces the **nat-control** command and preserves the current behavior for customers upgrading from previous versions of the software. For new security appliances or devices which have their configurations cleared, the default will be to not require a NAT policy for traffic to traverse the security appliance. For more information, see the “Applying NAT” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Outbound Low Latency Queuing (LLQ) and Policing

This feature supports applications with demanding quality of service (QoS) requirements through support of Low Latency Queuing (LLQ) and Traffic Policing – supporting the ability to have an end-to-end network QoS policy. When enabled, each interface maintains two queues for outbound traffic – one for latency-sensitive traffic (such as voice or market-data), and one for latency-tolerant traffic (such as file transfers). Queue performance can be optimized through a series of configuration parameters.

The QoS functionality is managed using the following commands: **police**, **priority**, **priority-queue**, **queue-limit**, and **tx-ring-limit**. For more information, see the “Applying QoS Policies” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

High Availability

Active/Active Failover with Asymmetric Routing Support

This feature builds upon the award-winning adaptive security appliance high availability architecture, introducing support for Active/Active failover. This enables two UR licensed or one UR and one FO-AA licensed security appliance to act as a failover pair, both actively passing traffic at the same time, and

with Asymmetric Routing Support. The Active/Active failover feature leverages the security context feature of this software release – where each security appliance in a failover pair is active for one context and standby for the other, as an inverse symmetric pair. Another key customer challenge that we are addressing in Version 7.0 is Asymmetric Routing Support. This will enable customers with advanced routing topologies, where packets may enter from one ISP and exit via another ISP, to deploy the security appliance to protect those environments (leveraging the Asymmetric Routing Support introduced in Version 7.0).

To support the Active/Active feature, the **failover active** command is extended with the **group** keyword and this software release introduces the failover group configuration mode. In addition, the **asr-group** command in interface configuration mode extends the Active/Active solution to environments with Asymmetric Routing. For more information, see the “Configuring Active/Active Failover” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

VPN Stateful Failover

This feature introduces Stateful Failover for VPN connections, complementing the award-winning firewall failover services. All security association (SA) state information and key material is automatically synchronized between the failover pair members, providing a highly resilient VPN solution.

The VPN Stateful Failover is enabled implicitly when the device operates in single routed mode. In addition to the **show failover EXEC** command, which includes a detailed view of VPN Stateful Failover operations and statistics, the **show isakmp sa**, **show ipsec sa** and **show vpnd-sessiondb** commands have information about the tunnels on both the active and standby unit.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Failover Enhancements

This feature enhances failover functionality so that the standby unit in a adaptive security appliance failover pair can be configured to use a virtual MAC address. This eliminates potential “stale” ARP entry issues for devices connected to the adaptive security appliance failover pair, in the unlikely event that both adaptive security appliances in a failover pair fail at the same time and only the standby unit remains operational.

LAN-based Failover

LAN-based Failover extends the adaptive security appliance failover functionality to operate through a dedicated LAN interface, without the serial failover cable. This overcomes the distance limitation of the current serial cable. Failover configuration synchronization can now occur through the serial cable or a LAN interface. However, the adaptive security appliance failover pair must be on the same subnet, and the adaptive security appliance model remains a hot-standby model, with one unit active and the other standby.

For LAN-based Failover, use a dedicated switch or hub (or VLAN) to connect the adaptive security appliance failover pair so that the secondary unit can detect the failure of the dedicated LAN failover interface of the primary unit and become active. Crossover Ethernet cables cannot be used to connect the

LAN-based Failover interface. Additionally, we recommend that you dedicate a LAN interface for LAN-based Failover, but the interface can be shared with Stateful Failover under lightly loaded configurations.

Show Failover Command

This new feature enhances the **show failover** command to display the last occurrence of a failover.

For more information on this feature, see the “Using the Show Failover Command” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Failover Support for HTTP

This feature supports the **failover replicate http** and **show failover** commands to allow the stateful replication of HTTP sessions in a Stateful Failover environment:

When HTTP replication is enabled, the **show failover** command displays the **failover replicate http** command.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

show shun Command

The **show shun** command, when issued from an appropriately configured adaptive security appliance, provides dynamic packet filtering in response to a adaptive security appliance signature by preventing new connections from an attacking host and disallowing packets from the attacking host on any existing connection(s). When possible, the connection that caused the event is terminated.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

show interface Command

The **show interface** command has display buffer counters.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Zero-Downtime Software Upgrades

This feature introduces the ability for customers to perform software upgrades of failover pairs without impacting network uptime or connections flowing through the units. Version 7.0 introduces the ability to do inter-version state sharing between security appliance failover pairs, allowing customers to perform software upgrades to maintenance releases (for example Version 7.0(1) upgrading to 7.0(2)) without impacting traffic flowing through the pair (in active/standby failover environments or Active/Active environments where the pair is not oversubscribed – more that 50% load on each pair member).

General High Availability Enhancements

This feature includes many significant enhancements to the Failover operation and configuration to deliver faster Failover transitions, increased scalability and even further robustness in failover operation.

The release introduces the following new commands: **failover interface-policy**, **failover polltime**, and **failover reload-standby**.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Management and Monitoring

Improved SNMP Support

This feature adds support for SNMPv2c, providing new services including 64-bit counters (useful for packet counters on Gigabit Ethernet interfaces) and support for bulk MIB data transfers. Additionally, Version 7.0 includes SNMPv2 MIB (RFC 1907), and the IF-MIB (RFCs 1573 and 2233) and the Cisco IPSec Flow Monitoring MIB, giving complete visibility into VPN flow statistics including tunnel uptime, bytes/packets transferred, and more.

For more information, see the “Using SNMP” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

CPU Utilization Monitoring Through SNMP

This feature supports monitoring of the adaptive security appliance CPU usage through SNMP. CPU usage information is still available directly on the adaptive security appliance through the **show cpu [usage]** command, but SNMP provides integration with other network management software.

For more information, see the “Using SNMP” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

SNMP Enhancements

Support for the adaptive security appliance platform-specific object IDs has been added to the **SNMP mib-2.system.sysObjectID** variable. This enables CiscoView Support on the adaptive security appliance.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

DNS Inspection Engine

The **[no] fixup protocol dns [maximum-length <512-65535>]** command can be used to enable/disable the DNS fixup.

Based on this maximum-length configured by the user, the DNS fixup checks to see if the DNS packet length is within this limit. Every UDP DNS packet (request/response) undergoes the above check.

**Note**

The adaptive security appliance drops DNS packets sent to UDP port 53 that are larger than the configured maximum length. The default value is 512 bytes.

This feature is added to the **protocol** command. For configuration information, see the “Configuring DNS Globally” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

**Note**

If DNS fixup is disabled, the Address record (A-record) is not NATed and the DNS ID is not matched in requests and responses. By disabling DNS fixup, the maximum length check on UDP DNS packets is bypassed and packets greater than the maximum length configured are permitted.

ILS Inspection Engine

This feature provides an Internet Locator Service (ILS) fixup to support NAT for ILS and Lightweight Directory Access Protocol (LDAP). Also, with the addition of this fixup, the adaptive security appliance supports H.323 session establishment by Microsoft NetMeeting. Microsoft NetMeeting, SiteServer, and Active Directory products leverage ILS, which is a directory service, to provide registration and location of endpoints. ILS supports the LDAP protocol and is LDAPv2 compliant.

Configurable RAS Inspection Engine

This feature includes an option to turn off the H.323 RAS (Registration, Admission, and Status) fixup and displays this option, when set, in the configuration. This enables customers to turn off the RAS fixup if they do not have any RAS traffic, they do not want their RAS messages to be inspected, or if they have other applications that utilize the UDP ports 1718 and 1719.

CTIQBE Inspection Engine

Known also as TAPI/JTAPI Fixup, this feature incorporates a Computer Telephony Interface Quick Buffer Encoding (CTIQBE) protocol inspection module that supports NAT, PAT, and bi-directional NAT. This enables Cisco IP SoftPhone & other Cisco TAPI/JTAPI applications to work and communicate successfully with Cisco CallManager for call setup and voice traffic across the adaptive security appliance.

This release supports the **inspect ctiqbe 2748** command. For more information on this command, see the “CTIQBE Inspection Overview” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

MGCP Inspection Engine

This release adds support for Media Gateway Control Protocol (MGCP) 1.0, enabling messages between Call Agents and VoIP media gateways to pass through the adaptive security appliance in a secure manner.

To configure the **fixup protocol mgcp** command, see the “MGCP Inspection Overview” section in the *Cisco Security Appliance Command Line Configuration Guide*.

The following commands support the following command: **debug mgcp**, **fixup protocol mgcp**. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Inspect ICMP Error

This release introduces the ability to NAT ICMP error messages.

For information on configuring this feature, see the “Adding an ICMP Type Object Group” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Object Grouping

To simplify your configuration, object grouping is supported in this release. Object grouping enables you to define groups of objects such as hosts, IP addresses, or network services. You can use these groups, for example, when you create and apply access rules. When you include an adaptive security appliance object group in an adaptive security appliance command, it is the equivalent of applying every element of the object group to the adaptive security appliance command.

Storage of Multiple Configurations in Flash Memory

This release debuts a new Flash file system on the adaptive security appliance enabling administrators to store multiple configurations on the security appliance. This provides the ability to do configuration roll-back in the event of a mis-configuration. Commands are introduced to manage files on this new file system.



Note

The new Flash file system is capable of storing not only configuration files but also multiple system images and multiple PIX images when there is adequate Flash space available.

The **boot config** global configuration command provides the ability to specify which configuration file should be used at start-up.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Stack Trace in Flash Memory

This feature enables the stack trace to be stored in non-volatile Flash Memory, so that it can be retrieved at a later time for debug/troubleshooting purposes.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Secure Asset Recovery

This feature introduces the ability to prevent the recovery of configuration data, certificates and key material if the **no service password recovery** command is in a security appliances configuration (while still allowing customers to recover the asset). This feature is useful in environments where physical security may not be ideal, and to prevent nefarious individuals gaining access to sensitive configuration data.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Scheduled System Reload (Reboot)

Administrators now have the ability to schedule a reload on a adaptive security appliance either at a specific time, or at an offset from the current time, thus making it simpler to schedule network downtimes and notify remote access VPN users of an impending reboot.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

RADIUS Support

Two new **aaa server** command options now support selection of RADIUS accounting and authentication ports.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

AAA Integration

Version 7.0(1) native integration with authentication services including Kerberos, NT Domain, and RSA SecurID (without requiring a separate RADIUS/TACACS+ server) for simplified VPN user authentication. This release also introduces the ability to generate TACACS+AAA accounting records for tracking administrative access to security appliances, as well as tracking all configuration changes that are made during an administrative session.

For more information see the “Configuring AAA Servers and the Local Database” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

AAA Fallback for Administrative Access

This feature introduces the ability to authenticate and authorize requests to fall-back to a local user database on the adaptive security appliance. The requirements and design will factor future compatibility with Cisco IOS software-like “method list” support for the adaptive security appliance, and deliver the addition of the LOCAL fallback method.

The following commands create a fallback scenario for AAA administrative access:

For more information on this feature, see the “Authentication Overview” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

AAA—Authentication, Authorization, and Accounting

The **aaa authentication** command has been modified to support HTTP authentication. The adaptive security appliance allows authentication verification of the HTTP server through the **aaa authentication http console** command before ASDM can access the adaptive security appliance.

For more information on this feature, see the “Authentication Overview” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

AAA Integration Enhancements

This feature debuts native integration with authentication services including Kerberos, LDAP, and RSA SecurID (without requiring a separate RADIUS/TACACS+ server) for simplified user and administrator authentication. This feature also introduces the ability to generate TACACS+AAA accounting records for tracking administrative access to adaptive security appliances, as well as tracking all configuration changes that are made during an administrative session.

For more information on this feature, see the “Configuring Authorization for Network Access” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

New Syslog Messaging for AAA authentication

This feature introduces a new AAA syslog message, which prompts users for their Authentication before they can use a service port.

Per-user-override

This feature allows users to specify a new keyword per-user-override to the **access-group** command. When this keyword is specified, it allows the permit/deny status from the per-user access-list (downloaded via AAA authentication) that is associated to a user to override the permit/deny status from the access-group access-list.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

AAA proxy-limit

When the **aaa proxy-limit** is set to 16, the “**aaa proxy-limit 16**” line shows up. This feature specifies the number of concurrent proxy connections allowed per user, from 1 to 128. The default value is 16.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

ICMP Ping Services

This feature introduces several additions to ping (ICMP echo) services, including support for IPv6 addresses. The **ping** command also supports extended options including data pattern, df-bit, repeat count, datagram size, interval, verbose output, and sweep range of sizes.

The existing **ping EXEC** command has been extended with various keywords and parameters to aid in troubleshooting network connectivity issues. It also provides support for an interactive mode of operation.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Command-Line Interface (CLI) Usability

This feature enhances the CLI “user experience” by incorporating many popular Cisco IOS software command-line services such as command completion, online help, and aliasing for improved ease-of-use and common user experience.

For more information, see the “Using the Command-Line Interface” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Command-Line Interface (CLI) Activation Key Management

This feature lets you enter a new activation key through the adaptive security appliance command-line interface (CLI), without using the system monitor mode and having to TFTP a new image. Additionally, the adaptive security appliance CLI displays the currently running activation key when you enter the **show version** command.

New Ability to Assign Netmasks with Address Pools

This feature introduces the ability to define a subnet mask for each address pool and pass this information onto the client.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Ability to Configure TFTP Inspection Engine

Ability to configure TFTP inspection engine inspects the TFTP protocol and dynamically creates connection and xlate, if necessary, to permit file transfer between a TFTP client and server. Specifically, the fixup inspects TFTP read request (RRQ), write request (WRQ), and error notification (ERROR).

**Note**

TFTP Fixup is enabled by default. TFTP Fixup must be enabled if static PAT is used to redirect TFTP traffics.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Dedicated Out-of-Band Management Interface

The management-only configuration command has been introduced in the interface configuration mode to enable dedicated out-of-band management access to the device.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

SMTP E-mail Alerts

This feature includes the ability for administrators to be notified of system events via SMTP-based e-mail alerts. See the enhancements in the **logging** global configuration command and the **smtp-server** global configuration command to configure sending critical syslogs using SMTP. For more information, see the “SMTP E-Mail Alerts” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

System Health Monitoring and Diagnostic Services

This feature provides improved monitoring of the system operation and to help isolate potential network and security appliance issues. The **show resource** and **show counters** commands provide detailed information about resource utilization for the appliance and security contexts as well as detailed statistics. To monitor the CPU utilization you may use the new **show cpu** EXEC command as well as the **show process cpu-hog** EXEC commands. To isolate potential software flaws the software introduces the **checkheaps** command and related **show** EXEC command. Finally, to get a better understanding of the block (packet) utilization, the **show blocks** EXEC command provides extensive analytical tools on block queuing and utilization in the system.

Debug Services

The **debug** commands have been improved and many new features include to respective debug support. Furthermore, the debug output is now supported to all virtual terminals without restrictions. That is, when you enable debug output for a particular feature, you will be able to view the output without any limitations. Clearly, the output will be restricted to the session where it was enabled. Finally, the user can send debug output over syslogs if your security policy allows it and you wish to do so by leveraging the **logging** command.

Packet Capture

This release supports packet capture. The adaptive security appliance packet capture provides the ability to sniff or “see” any traffic accepted or blocked by the adaptive security appliance. Once the packet information is captured, you have the option of viewing it on the console, transferring it to a file over the network using a TFTP server, or accessing it through a web browser using Secure HTTP. However, the adaptive security appliance does not capture traffic unrelated to itself on the same network segment, and this packet capture feature does not include file system, DNS name resolution, or promiscuous mode support.

The capture Command

Users can now specify the **capture** command to store the packet capture in a circular buffer. The capture will continue writing packets to the buffer until it is stopped by the administrator.

For configuration information, see the “Capturing Packets” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Capture Support

The adaptive security appliance introduces additional support to improve the ability of the user to diagnose device operation by supporting the ability to capture ISAKMP traffic and only capture packets dropped by the new Accelerated Security Path (ASP).

The existing **capture** command has been extended with a new **type** keyword and parameters to capture ISAKMP, packet drops, and packet drops matching a specified reason string.

show version Command

The output of the **show version** command displays additional information.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

show tech Command

This feature enhances the current **show tech** command output to include additional diagnostic information.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Debug Command and Support

These commands turn off all active debugs at once, and restore the adaptive security appliance to normal operation.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

SSL Debug Support

Support for the Secure Sockets Layer (SSL) protocol is added to the **debug** command. SSL is a protocol for authenticated and encrypted communications between client and servers such as the ASDM and the adaptive security appliance.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Modification to GE Hardware Speed Settings

The Gigabit Ethernet cards can be configured by hardware in TBI or GMII mode. TBI mode does not support half duplex. GMII mode supports both half duplex and full duplex. All the i8255x controllers used in the adaptive security appliances are configured for TBI and thus cannot support half-duplex mode, hence the half-duplex setting is removed.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

The arp Command

For information on the **arp** command, see the “ARP Inspection Overview” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Show Version command

The **show version** command output now has two interface-related lines, Max Physical interfaces and Max interfaces. Max interfaces is the total physical and virtual interfaces.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Virtual LAN (VLAN)-based Virtual Interfaces

802.1Q VLAN support provides flexibility in managing and provisioning the adaptive security appliance. This feature enables the decoupling of IP interfaces from physical interfaces (hence making it possible to configure logical IP interfaces independent of the number of interface cards installed), and supplies appropriate handling for IEEE 802.1Q tags.

VLAN feature support is added to the **interface** command. For configuration information, see the “Configuring Subinterfaces” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Local User Authentication Database for Network and VPN Access

This feature allows cut-through and VPN (using xauth) traffic to be authenticated using the adaptive security appliance local username database (as an alternative in addition to the existing authenticating via an external AAA server).

The server tag variable now accepts the value LOCAL to support cut-through proxy authentication using Local Database.

For more information on this feature, see the “User Authentication Using the LOCAL Database” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Cryptographic Engine Known Answer Test (KAT)

The function of KAT is to test the instantiation of the adaptive security appliance crypto engine. The test will be performed every time during the adaptive security appliance boot up before the configuration is read from Flash memory. KAT will be run for valid crypto algorithms for the current license on the adaptive security appliance.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Media Access Control (MAC) Based Authentication

This feature allows hosts to be exempted from a broader authentication requirement, based on their MAC addresses. This is essential for devices like printers and IP phones located inside a firewall.

The **mac-list**, **aaa mac-exempt match <mac-list-id>** and **vpncient mac-exempt <mac-add_1> <mac_mask_1> [<mac_addr_2> <mac_mask_2>** commands are new commands. To configure this command on the adaptive security appliance, see the “Using MAC-Based AAA Exemption” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Custom Backup Concentrator Timeout

This feature constitutes a configurable time out on the adaptive security appliance connection attempts to a VPN headend, thereby controlling the latency involved in rolling over to the next backup concentrator on the list.

This feature supports the **vpngroup** command. For more information on this command, see the “Enabling Redundancy” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Console Connection Inactivity Timeout

This feature protects the console connection from unauthorized administrative access by automatically logging out sessions after a configurable period of inactivity.

This release supports the **console** command. For a complete description of the command syntax for this new command, see the *Cisco Security Appliance Command Reference*.

Voice Over IP Skinny Protocol Support

The **fixup protocol** command supports the Skinny Client Control Protocol (SCCP), used for IP telephony.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Custom Administrative Access Banner Messages

Users will be able to configure a message-of-the-day (motd), a login, and an exec banner that will be displayed to users who access the adaptive security appliance via the console, SSH, and Telnet.

To configure the **banner** command, see the “Configuring a Login Banner” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

show Command Output Filter

This feature provides the ability to filter or search through the full output of **show** commands.

For more information on this feature, see the “Getting Started” section in the *Cisco Security Appliance Command Line Configuration Guide*.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Important Notes

Important Notes in Release 7.0

This section lists important notes related to release 7.0(1).

Hostname and Domain Name Limitation

When using ASDM, the hostname and domain names combined should not be more than 63 characters long. If the hostname and domain names combined is more than 63 characters, you will get an error message.

WebVPN ACLs and DNS Hostname

When a deny webtype URL ACL (DNS-based) is defined, but the DNS-based URL is not reachable, a 'DNS Error' popup is displayed on the browser. The ACL hitcounter is also not incremented.

If the URL ACL is defined by an IP instead of DNS name, then the traffic flow hitting the ACL will be recorded in the hitcounter and a 'Connection Error' is displayed on the browser.

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 will display it to the client browser.

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

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 access control lists (ACLs). ACL-based configurations provide uniformity and leverage the powerful ACL feature set. ACL based configurations provide the following benefit:

- Access control element (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.

User Upgrade Guide

- For a list of deprecated features, and user upgrade information, go to the following URL:
http://www.cisco.com/en/US/docs/security/asa/asa70/vpn3000_upgrade/upgrade/guide/migr_vpn.html

Features not Supported in Version 7.0

The following features are not supported in Version 7.0 (1):

- PPPoE
- L2TP over IPSec
- PPTP

MIB Supported

For information on MIB Support, go to:

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

Downgrade to 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*.

Caveats

The following sections describe the caveats for the 7.0(1) release.

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 may 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/public/sw-center/index.shtml>

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(2)

Table 2 Open Caveats

ID Number	Software Release 7.0(2)	
	Corrected	Caveat Title
CSCeh60845	No	Logging queue incorrectly registers 8192 256-byte blocks
CSCeh81062	No	wrong ip addr on outgoing packets when PAT and static port are used
CSCeh90617	No	Recompiling ACLs can cause packet drops on low-end platforms
CSCeh98117	No	Tunnel-group passwords in cleartext when viewed with more
CSCei00497	No	PIX/ASA 7.0 doesn't encrypt packets if next hop is PIX interface.
CSCei20466	No	Increase in CPU utilization when OSPF is enabled
CSCei20809	No	sh access-l counters not updated when acl used in nat/nat-exempt
CSCei21362	No	PIX traceback after issuing show isakmp sa detail command.
CSCei23290	No	DHCP Relay fails when static specified
CSCei24062	No	Some hosts in the network connects to inside intf cannot be reached
CSCei38640	No	AAA: radius /w expiry does not work when using funk radius server
CSCei38651	No	NT auth for VPN clients do not work with domainuser or user@domain
CSCei38667	No	Can't differentiate between root CA certs that have been re-keyed
CSCei41326	No	AAA: fallback to LOCAL authentication does not work for SSH
CSCei50190	No	PIX/ASA not accepting 2 ISAKMP policies with different AES types

Table 2 *Open Caveats (continued)*

ID Number	Software Release 7.0(2)	
	Corrected	Caveat Title
CSCei51867	No	Usability - crypto config should be grouped together in CLI output
CSCei52413	No	PIX/ASA fails to import cert if CA issuer has 4096 bits cert
CSCsb31740	No	VPN IP local pool - detection of invalid IP OK - but fails to assign IP
CSCsb33629	No	address-pool subcommand doesn't error when list is full
CSCsb36188	No	PIX/ASA 7.0.1 - sending multiple authentication requests to ACS Server
CSCsb37531	No	Traceback after failover if TCP Intercept is triggered.
CSCsb40331	No	PIX 7.0(1)2 Assertion Violation w/Multiple Context & VOIP Configuration

Resolved Caveats - Release 7.0(2)

Table 3 *Resolved Caveats*

ID Number	Software Release 7.0(2)	
	Corrected	Caveat Title
CSCeg85121	Yes	Not able to specify url-server timeout to 5 seconds
CSCeh27584	Yes	rem-access-mon.mib fails GetNext&Bulk ops
CSCeh39197	Yes	Inspect proxy should not queue dropped packet
CSCeh50620	Yes	Traceback on standby when failing over dynamic L2L tunnel
CSCeh57035	Yes	Named networks not working in ospf network statements
CSCeh57562	Yes	Memory leak in ssh code
CSCeh59635	Yes	GTP: When the PDP CTX reached to 30000 Contexts the System Traceback
CSCeh60361	Yes	isakmp key no-config-mode - will not be converted on upgrade to 7.0
CSCeh60367	Yes	Default tunnel-groups do not appear in the output of show run all
CSCeh60673	Yes	PIX crashes on pinhole preparation and connection limit exceeded
CSCeh60887	Yes	PIX crashes due to memory corruption 7.0.1
CSCeh64177	Yes	Not able to configure infinite isakmp lifetime in pix/asa 7.0
CSCeh69389	Yes	Split-tunnel ACLs not converted to Standard ACLs on upgrade to 7.0
CSCeh71023	Yes	Broadcasts leak from High Level Sec. Intf to Low Level Sec. Intf.
CSCeh71492	Yes	xauth enabled by default on Remote Access VPN tunnels on upgrade
CSCeh72706	Yes	traceback: IKE_daemon: Unexpected cleanup of tunnel table entry
CSCeh75725	Yes	7.0 does not support Extended ACLs (object groups) for split tunnel
CSCeh79645	Yes	ASDM handler stream for blocks data is missing for 2048 size
CSCeh81233	Yes	DCHP client: ip address dhcp setroute missing: no default route
CSCeh81774	Yes	un-NATed ACK packets sent on outside interface
CSCeh89562	Yes	PIX crashes when shuns are cleared while sh shun is running

Table 3 Resolved Caveats (continued)

ID Number	Software Release 7.0(2)	
	Corrected	Caveat Title
CSCeh90902	Yes	Support for multiple crypto maps to the same peer missing
CSCeh94725	Yes	Embedded RTP IP not NATed in H.245 OLC Ack
CSCeh96708	Yes	Syslog reports erroneous transfer size in TCP Teardown 302014 syslog
CSCeh96865	Yes	H323: Media stream disconnect in the middle of H323 call
CSCeh97110	Yes	PIX should not response to reset packet outside window
CSCeh97407	Yes	RA Tunnels fail to connect after re-xauth during re-key
CSCei00227	Yes	isakmp key hostname converted to invalid tunnel-group
CSCei02443	Yes	PKI:F1 crash during crt retrieval at Crypto CA ,eip_free_pslct_108
CSCei03165	Yes	PIX reboots continuously with overlapping/redundant statics
CSCei04829	Yes	PIX 7.0 crash in IPsec message handler
CSCei08652	Yes	np70.bin reboots PIX without asking to erase the password
CSCei09266	Yes	Traceback when shuns are cleared
CSCei09829	Yes	AppsFW:HTTP-Strict when no reson string in response
CSCei12178	Yes	PIX crashes with memory corruption
CSCei12460	Yes	PIX-ASA crashes with TCP packet where dst IP is a multicast addr
CSCei12915	Yes	PIX-ASA sends Syslogs with source port other than 514
CSCei15053	Yes	IKE test suite causes multiple reboots in 7.0(1)
CSCei15215	Yes	Firewall drops IP Options packets needed for igmp and rsvp traffic
CSCei16294	Yes	ISAKMP: Port selector are in host-order on the wire
CSCei16403	Yes	TCP keepalives on H.225 (1720) blocked with inspect h323 h225
CSCei16904	Yes	Syslog adds extra space
CSCei18370	Yes	sqlnet version 1 inspection crashes the box
CSCei19528	Yes	FTP Failed if client supports EPRT but server does not
CSCei20197	Yes	Can't get acl for pim rp-address cmd
CSCei21386	Yes	SIP: CSeq No parsed incorrectly if CSeq no length is 10
CSCei21387	Yes	SIP: SIP URI Parse error happens when receiving SIP Response
CSCei24376	Yes	Interface mtu minimum value changed from 64 to 300 bytes
CSCei25213	Yes	PIX crashes with thread name SSH
CSCei27053	Yes	One byte TCP keepalives not processed correctly by normalizer
CSCei27070	Yes	Pass-through pptp with PAT stops working after a while
CSCei28815	Yes	FIN-ACK Dropped Despite Fact that Sequece Number within TCP Window
CSCei29901	Yes	Inconsistant baehvior on scanning
CSCei30474	Yes	Issue <clear con> command would hit page fault traceback
CSCei33574	Yes	GTP: box reloads on 2ndary PDP create when 1st fails

Table 3 *Resolved Caveats (continued)*

ID Number	Software Release 7.0(2)	
	Corrected	Caveat Title
CSCei34524	Yes	Deny rule in nat exempt fails xlate replication to standby
CSCei50549	Yes	License mismatch when a pix has 4-tuple key and another has 5-tuple

Related Documentation

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

- [Cisco ASA 5500 Series Hardware Installation Guide](#)
- [Cisco ASA 5500 Series Quick Start Guide](#)
- [Cisco Security Appliance Command Line Configuration Guide](#)
- [Cisco Security Appliance Command Reference](#)
- [Migrating to ASA for VPN 3000 Series Concentrator Administrators](#)

Software Configuration Tips on the Cisco TAC Home Page

The Cisco Technical Assistance Center has many helpful pages. If you have a CDC account you can visit the following websites for assistance:

TAC Troubleshooting, Sample Configurations, Hardware Info, Software Installations and more:

<http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/>

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 “[Related Documentation](#)” section.

CCSP, the Cisco Square Bridge logo, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0502R)

Copyright © 2005 Cisco Systems, Inc.
All rights reserved.