Cisco ASA 5500 Series Release Notes, Version 7.0

May 2005

Contents

This document includes the following sections:

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.

Cisco Systems

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

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/cisco/software/navigator.html

New Features

Released: May 31, 2005

Table 2 lists the new features forASA and PIX Version 7.0(1).

Table 2 New Features for ASA and PIX Version 7.0(1)

Feature	Description
Platform Features	
Support for the ASA 5500 series	Support for the ASA 5500 series was introduced, including support for the following models: ASA 5510, ASA 5520, and ASA 5540.
Firewall Features	
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. We introduced the following commands: **arp-inspection, firewall, mac-address-table,** and **mac-learn**.
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 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). We introduced the following commands: **admin-context, context** (and context subcommands)**, changeto**, and **mode.**
Outbound ACLs and	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.
Time-based 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.
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.
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.

Table 2 New Features for ASA and PIX Version 7.0(1) (continued)

Feature	Description
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). We introduced the following commands: **class-map**, **policy-map**, and **service-policy**.
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.
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**.
Application Inspection Features	
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.
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 security appliance.

Table 2 New Features for ASA and PIX Version 7.0(1) (continued)

Feature	Description
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 **VRFY** (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.
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.
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. This release introduces the ability to NAT ICMP error messages. Use the **inspect icmp** and the **inspect icmp error** commands to configure the ICMP inspection engine.
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.
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.
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.
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.
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.
Configurable SIP UDP Inspection Engine	This provides a CLI-enabled solution for non-Session Information Protocol (SIP) packets to pass through the security appliance instead of being dropped when they use a SIP UDP port.

Table 2 New Features for ASA and PIX Version 7.0(1) (continued)

Feature	Description
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.
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.
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.
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.
PAT for Skinny	This feature allows Cisco IP Phones to communicate with Cisco CallManager across the security appliance when it is configured with PAT. This is particularly important in a remote access environment where Skinny IP phones behind a security appliance talk to the CallManager at the corporate site through a VPN.
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 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 security appliance. This release supports the **inspect ctiqbe 2748** command.
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 security appliance in a secure manner. See the **inspect mgcp** command.

Table 2 New Features for ASA and PIX Version 7.0(1) (continued)

Feature	Description
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.
Filtering Features	
Improved URL Filtering Performance	This feature significantly increases the number of concurrent URLs that can be processed by improving the communications channel between the 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.
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.
IPSec VPN Features	
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.
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.
OSPF Dynamic Routing over VPN	Support for OSPF has been extended to support neighbors across an IPSec VPN tunnel. This allows the 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.
Remote Management Enhancements	This feature enables administrators to remotely manage firewalls over a VPN tunnel using the inside interface IP address of the remote security appliance. In fact, administrators can define any 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.

Table 2 New Features for ASA and PIX Version 7.0(1) (continued)

Feature	Description
X.509 Certificate Support	Support for X.509 certificates has been significantly improved in the 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.
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 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 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.
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.
Easy VPN Internet Access Policy	The 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 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 security appliance can connect to the Internet regardless of the status of the VPN tunnel to the Easy VPN server.
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.
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 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.
User-Level Authentication	Support for individually authenticating clients (IP address based) on the inside network of the 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.
Secure Unit Authentication	This feature provides the ability to use dynamically generated authentication credentials to authenticate the Easy VPN remote (VPN Hardware client) device.

Table 2 New Features for ASA and PIX Version 7.0(1) (continued)

Feature	Description
Flexible Easy VPN Management Solutions	Managing the 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.
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.
VPN Client Update	To configure and change client update parameters, use the **client-update** command in tunnel-group ipsec-attributes configuration mode.
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.
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).
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.
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.
Diffie-Hellman (DH) Group 5 Support	This release supports the 1536-bit MODP Group that has been given the group 5 identifier.
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 security appliance models and hardware-accelerated AES via the new VAC+ card.
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.

Table 2 New Features for ASA and PIX Version 7.0(1) (continued)

Feature	Description
Cryptographic Engine Known Answer Test (KAT)	The function of KAT is to test the instantiation of the security appliance crypto engine. The test will be performed every time during the 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 security appliance.
Custom Backup Concentrator Timeout	This feature constitutes a configurable time out on the 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.
WebVPN 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 abroad 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.
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.
Port Forwarding	WebVPN port forwarding, also called application access, lets remote users use TCP-applications over an SSL VPN connection.
Email	WebVPN supports several ways of using email, including IMAP4S, POP3S, SMTPS, MAPI, and Web Email. • IMAP4S, POP3S, SMTPS WebVPN lets remote users use the IMAP4, POP3, and SMTP email 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 Email Web email 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.
Routing Features	
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.

Table 2 New Features for ASA and PIX Version 7.0(1) (continued)

Feature	Description
DHCP Option 66 and 150 Support	This feature enhances the DHCP server on the inside interface of the 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.
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 can be configured only on the outside interface, and DHCP relay agent can be configured on any interface. However, DHCP server and DHCP relay agent cannot be configured concurrently on the same security appliance, but DHCP client and DHCP relay agent can be configured concurrently. We modified the following command: **dhcpd 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.
Interface Features	
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.
show interface Command	The **show interface** command has display buffer counters.
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.
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 security appliances are configured for TBI and thus cannot support half-duplex mode, hence the half-duplex setting is removed.
VLAN-based virtual interfaces	802.1Q VLAN support provides flexibility in managing and provisioning the 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. We introduced the following command: **vlan**.
NAT Features	

Table 2 New Features for ASA and PIX Version 7.0(1) (continued)

Feature	Description
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.
High Availability Features	
Active/Active Failover with Asymmetric Routing Support	This feature builds upon the award-winning 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.
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.
Failover Enhancements	This feature enhances failover functionality so that the standby unit in a 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 security appliance failover pair, in the unlikely event that both security appliances in a failover pair fail at the same time and only the standby unit remains operational.
show failover Command	This new feature enhances the **show failover** command to display the last occurrence of a failover.
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.

Table 2 New Features for ASA and PIX Version 7.0(1) (continued)

Feature	Description
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.**
Troubleshooting and Monitoring Features	
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.
CPU Utilization Monitoring Through SNMP	This feature supports monitoring of the security appliance CPU usage through SNMP. CPU usage information is still available directly on the security appliance through the **show cpu** [**usage**] command, but SNMP provides integration with other network management software.
SNMP Enhancements	Support for the security appliance platform-specific object IDs has been added to the **SNMP mib-2.system.sysObjectID** variable. This enables CiscoView Support on the security appliance.
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.
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.
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.

Table 2 New Features for ASA and PIX Version 7.0(1) (continued)

Feature	Description
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.
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 security appliance.
Packet Capture	This release supports packet capture. The security appliance packet capture provides the ability to sniff or "see" any traffic accepted or blocked by the 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 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. 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. The 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 tech Command	This feature enhances the current **show tech** command output to include additional diagnostic information.
Management Features	
Storage of Multiple Configurations in Flash Memory	This release debuts a new Flash file system on the 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 their 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.
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.
Scheduled System Reload (Reboot)	Administrators now have the ability to schedule a reload on a 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.

Table 2 New Features for ASA and PIX Version 7.0(1) (continued)

Feature	Description
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.
Command-Line Interface (CLI) Activation Key Management	This feature lets you enter a new activation key through the security appliance command-line interface (CLI), without using the system monitor mode and having to TFTP a new image. Additionally, the security appliance CLI displays the currently running activation key when you enter the **show version** command.
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.
AAA Features	
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.
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 security appliance. The requirements and design will factor future compatibility with Cisco IOS software-like "method list" support for the security appliance, and deliver the addition of the LOCAL fallback method.
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 security appliances, as well as tracking all configuration changes that are made during an administrative session.
Secure HyperText Transfer Protocol (HTTPS) Authentication Proxy	This feature extends the capabilities of the 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.
Downloadable Access Control Lists (ACLs)	This feature supports the download of ACLs to the 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 security appliance. This feature is supported for RADIUS servers only and is not supported for TACACS+ servers.
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.

Table 2 New Features for ASA and PIX Version 7.0(1) (continued)

Feature	Description
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.
Local User Authentication Database for Network and VPN Access	This feature allows cut-through and VPN (using xauth) traffic to be authenticated using the 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.

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.

IKE DPD Now Enabled by Default

IKE DPD is now enabled by default.

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/pix_upgrade/upgrade/guide/pixupgrd.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 Pervious 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://tools.cisco.com/Support/BugToolKit/l

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

Table 3 Open Caveats

	Software Release 7.0	
ID Number	**Corrected**	**Caveat Title**
CSCeg10668	No	GTP: Multi-mode,no traffic for 30 mins thru PDPs,secondary reloads
CSCeg57001	No	Packet does not come to inspect after no inspect and inspect
CSCeg80301	No	sh cpu cont all doesnt show load from ctxs when conns not inspected
CSCeh04384	No	vpn failover may not succeed with 5000 tunnels and short holdtime
CSCeh07211	No	TCP intercept interop issues with older versions of linux kernel
CSCeh15557	No	Assertion in tmatch_compile_proc, all memory is not freed
CSCeh18115	No	Authentication not triggered sometimes when URL filtering enabled
CSCeh27993	No	Flows not immediately deleted after packets with IP Options dropped
CSCeh32087	No	PIM sends Register with untranslated IP when NAT pool exhausted
CSCeh34025	No	Upgrade from PIX 6.x to 7.0.1 can cause some configuration loss
CSCeh36410	No	Logging halts on the system if ssh version 2 session locks up
CSCeh37235	No	EntityMIB:entPhysicalSerialNum does not return serial number on PIX
CSCeh37241	No	Inspect:icmp, stats not available when configured on 2 class-maps
CSCeh37750	No	VPN tunnel may drop during phase 1 rekey
CSCeh39197	No	Inspect proxy should not queue dropped packet
CSCeh39325	No	Cannot switch serial to LAN failover w LAN interface configured
CSCeh40122	No	RRI:some injected routes not deleted when SA is gone
CSCeh40345	No	Traceback in IKE FSM after prolonged system testing with failover

Table 3 Open Caveats (continued)

ID Number	Software Release 7.0	
	Corrected	Caveat Title
CSCeh43321	No	Cut & paste no fail key/no fail cannot disable fover on standby
CSCeh43554	No	Device may reload if showing and removing config at the same time
CSCeh44228	No	traceback crypto_certc_pki:_crypto_certc_create_selfsigned_certifica
CSCeh45956	No	ACL:High latency with large ACL after reload or import
CSCeh46345	No	Dynamic L2L could pass clear text traffic when tunnel terminates
CSCeh49286	No	Existing nat-control cfg cmd ignored when creating new sec lvl 0 ifc
CSCeh49985	No	Address not translated when generating ICMP Unreachable message
CSCeh50620	No	traceback on standby when failing over dynamic L2L tunnel
CSCeh50715	No	show capture stalled at -more- caused failover to occur
CSCeh51288	No	MFW-T:traceback in RADIUS when authenticating large # of conns
CSCeh51949	No	Can no longer connect to ASA via WebVPN or ASDM
CSCeh52766	No	traceback in TCP normalizer with 2 IPSec/TCP tunnels and heavy rekey
CSCeh52982	No	TCP Intercept:Lowering values of mss cause applications not to work
CSCeh53428	No	Change of behavior for fixup icmp error
CSCeh53514	No	CTIQBE phones unregister during call on hold with small MTU sizes
CSCeh53519	No	Assertion in block when segmented voice pkts are processed
CSCeh54103	No	some IPSec/TCP tunnels drop during VPN failover
CSCeh54286	No	Data traffic is allowed through Failover interface
CSCeh81233	No	DHCP client: ip address dhcp setroute mission; no default route
CSCeh60673	No	Device reloads on pinhole preparation and connection limit exceeded
CSCeh81062	No	wrong ip addr on outgoing packets when PAT and static port are used
CSCeh60887	No	Device crashes due to memory corruption 7.0.1
CSCeh57035	No	named networks not working in ospf network statements
CSCeh94725	No	Embedded RTP IP not NATed in H.245 OLC Ack
CSCeh75725	No	7.0 does not support Extended ACLs (object groups) for split tunnel
CSCeh64177	No	not able to configure infinite isakmp lifetime in pix/asa 7.0

Resolved Caveats - Release 7.0

Table 4 Resolved Caveats

ID Number	Software Release 7.0	
	Corrected	Caveat Title
CSCeh81233	Yes	DHCP client: ip address dhcp setroute mission; no default route
CSCeh60673	Yes	Device reloads on pinhole preparation and connection limit exceeded

Table 4 Resolved Caveats (continued)

ID Number	Software Release 7.0	
	Corrected	Caveat Title
CSCeh81062	Yes	wrong ip addr on outgoing packets when PAT and static port are used
CSCeh60887	Yes	Device crashes due to memory corruption 7.0.1
CSCeh57035	Yes	named networks not working in ospf network statements
CSCeh94725	Yes	Embedded RTP IP not NATed in H.245 OLC Ack
CSCeh75725	Yes	7.0 does not support Extended ACLs (object groups) for split tunnel
CSCeh64177	Yes	not able to configure infinite isakmp lifetime in pix/asa 7.0

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*

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.