Cisco ASDM Release Notes Version 5.0

May 2005

Contents

This document contains release information for Cisco ASDM Version 5.0 on Cisco PIX 500 series and Cisco ASA 5500 series security appliances 7.0(1). It includes the following sections:

Introduction

Cisco Adaptive Security Device Manager (ASDM) delivers world-class security management and monitoring services for Cisco PIX 500 and ASA 5500 series security appliances through an intuitive, easy-to-use, web-based management interface. Bundled with supported security appliances, the device manager accelerates security appliance deployment with intelligent wizards, robust administration tools, and versatile monitoring services that complement the advanced security and networking features offered by Cisco PIX 500 and ASA 5500 series security appliance software Version 7.0(1). Its secure, web-based design enables anytime, anywhere access to security appliances.

New Features

Released: May 31, 2005

Cisco Systems

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

Table 1 lists the new features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(1).

Table 1 New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(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 1 New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(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 1 ***New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(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 1 New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(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 1 New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(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 1 New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(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 1 New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(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 1 New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(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 1 New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(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 1 New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(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 1 New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(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 1 New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(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 1 New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(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.
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.

Table 1 New Features for ASA and PIX Version 7.0(1)/ASDM Version 5.0(1) (continued)

Feature	Description
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.
ASDM Features	
Dynamic Dashboard (ASDM Home Page)	• Displays detailed device and licensing information for quick identification of system and resources available. • Displays real-time system and traffic profiling .
Real-time Log Viewer	• Displays real-time syslog messages. • Advanced filtering capabilities make it easy to focus on key events.
Improved Java Web-Based Architecture	• Accelerates the loading of ASDM with optimized applet caching capability. • Provides anytime, anywhere access to all management and monitoring features.
Downloadable ASDM Launcher (on Microsoft Windows 2000 or XP operating systems only)	• Lets you download and run ASDM locally on your PC. • Multiple instances of ASDM Launcher provide administrative access to multiple security appliances simultaneously, from the same management workstation. • Automatically updates the software based on the installed version on the appliance, enabling consistent security management throughout the network.
Multiple Language Operating System Support	Supports both the English and Japanese versions of the Microsoft Windows operating systems.

System Requirements

This section includes the following topics:

- Hardware Requirements
- Client PC Operating System and Browser Requirements

Hardware Requirements

ASDM software runs on the following platforms:

- Cisco ASA 5510 security appliance
- Cisco ASA 5520 security appliance
- Cisco ASA 5540 security appliance
- SSM-10
- SSM-20
- PIX 515/515E
- PIX 525

- PIX 535

Note ASDM is not currently supported on PIX 501, PIX 506/506E, or PIX 520 hardware.

For more information on minimum hardware requirements, see:

http://www.cisco.com/en/US/docs/security/asa/asa70/asdm50/webhelp/sysreq.html

Certain features, such as load balancing and QoS, require particular hardware platforms. Other features require licensing. For more information on feature support for each platform license, see:

http://www.cisco.com/en/US/docs/security/asa/asa70/asdm50/webhelp/gen_info_licenses.html

Client PC Operating System and Browser Requirements

Table 2 lists the supported and recommended PC operating systems and browsers for Version 5.0.

Table 2 Operating System and Browser Requirements

	Operating System	**Browser**	**Other Requirements**
Windows[1]	Windows 2000 (Service Pack 4) or Windows XP operating systems	Internet Explorer 6.0 with Sun Java[2] Plug-in 1.4.2 or 1.5.0 **Note** **HTTP 1.1**—Settings for Internet Options > Advanced > HTTP 1.1 should use HTTP 1.1 for both proxy and non-proxy connections. Netscape 7.1/7.2 with Sun Java Plug-in 1.4.2 or 1.5.0	**SSL Encryption Settings**—All available encryption options are enabled for SSL in the browser preferences.
Sun Solaris	Sun Solaris 8 or 9 running CDE window manager	Mozilla 1.7.3 with Sun Java Plug-in 1.4.2 or 1.5.0	
Linux	Red Hat Linux 9.0 or Red Hat Linux WS, Version 3 running GNOME or KDE	Mozilla 1.7.3 with Sun Java Plug-in 1.4.2	

[1] ASDM is not supported on Windows 3.1, 95, 98, ME or Windows NT4.

[2] Get Sun Java from the Java website.

Usage Notes

This section includes the following topics:

- Upgrading to a New Software Release
- Getting Started with ASDM
- Unsupported Characters
- ASDM CLI Does Not Support Intertactive User Commands
- Printing from ASDM
- Unsupported Commands

- Securing the Failover Key

Upgrading to a New Software Release

If you have a Cisco Connection Online (CCO) login, you can obtain software from the following website:

http://www.cisco.com/cisco/software/navigator.html

Refer to the *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0* for more information.

Note Before you upgrade your device manager, upgrade your platform software to Cisco PIX software Version 7.0.

To upgrade from PIX Device Manager to ASDM, perform the following steps:

Step 1 Copy the ASDM binary file (asdm-501.bin) to a TFTP or FTP server on your network.

Step 2 Log in to your security appliance using the console (or other appropriate method that you have configured).

Step 3 Ensure that you have connectivity from your security appliance to your TFTP/FTP server.

Step 4 If you have an existing copy of the PIX Device Manager, delete it:

```
delete flash:/pdm
```

Step 5 Copy the ASDM binary onto your security appliance using the appropriate command:

- For TFTP: `copy tftp://your-server-IP/pathtofile flash:/asdm-501.bin`
- For FTP: `copy ftp://your-server-IP/pathtofile flash:/asdm-501.bin`

Note For more information on the **copy** command and its options, see the *Cisco Security Appliance Command Reference*.

Step 6 If you have more than one ASDM image, enter the following command to configure the location of the ASDM image:

```
asdm image flash:/asdm501.bin
```

Step 7 Enter the following command to enable the HTTPS server on the device:

```
http server enable
```

Step 8 Identify the systems or networks that are allowed to access ASDM by specifying one or more hosts/networks, using the following command:

```
http 10.1.1.1 255.255.255.255 inside
```

where IP address 10.1.1.1 is a host that can access ASDM and which is connected via the inside interface. Refer to *Cisco Security Appliance Command Reference* for more information on the options to the **http** command.

Step 9 Verify that ASDM is installed correctly by connecting from the client system (10.1.1.1 in the preceding example) to the security appliance, using a supported browser. For example:

```
https://10.1.1.254/admin/
```

where 10.1.1.254 is the IP address of the inside interface of the device in Step 8.

Note ASDM requires Java Plug-in software. After you install ASDM, download the latest Java Plug-in from the following site: http://www.cisco.com/cisco/software/navigator.html.

Deleting Your Old Cache

In early beta releases of ASDM and in previous releases of PDM (Versions 4.1 and earlier), the device manager stored its cache in: `<userdir>\pdmcache`. For example, `D:\Documents and Settings\jones\pdmcache`.

Now, the cache directory for ASDM is in: `<user dir>\.asdm\cache`.

The File > Clear ASDM Cache option in ASDM clears this new cache directory. It does not clear the old one. To free up space on your system, if you are no longer using your older versions of PDM or ASDM, delete your `pdmcache` directory manually.

Getting Started with ASDM

If you are using ASDM for the first time on a new security appliance, follow the instructions in this section to get started using ASDM. If you are upgrading an existing device, see Upgrading to a New Software Release, page 17.

Because ASDM uses a GUI interface, it requires that you access it from a PC using a supported web browser. For the supported browsers, see the "Client PC Operating System and Browser Requirements" section on page 16.

Before You Begin

Before using ASDM for the first time, do the following:

Step 1 Set up your security appliance.

Step 2 Connect your PC directly to the security appliance via the port Ethernet 1.

Step 3 Do one of the following:

- Either configure your PC for DHCP, or
- Make sure your PC is on the same subnet as the security appliance. (The default IP address for the security appliance is: 192.168.1.1. The default subnet mask is 255.255.255.0.)

- If you want to configure transparent firewall mode on your security appliance, enter the CLI **setup** command. Refer to the *Cisco Security Appliance Command Line Configuration Guide* for more information.

Starting ASDM

To start ASDM for the first time, perform the following steps:

Step 1 Start ASDM from a supported web browser connected to the security appliance by entering the URL: **`https://192.168.1.1/admin/`**

where 192.168.1.1 is the IP address of the security appliance.

Note Be sure to enter **`https`**, not **`http`**.

Step 2 Click **OK** or **Yes** to all prompts, including the name and password prompt. No name or password is required for a new device.

If ASDM does not start, check the device configuration. Your security appliance should be configured to accept ASDM configuration on its inside interface. (A new security appliance is configured this way by default.) If you need to modify the configuration to reestablish this default setting, use the CLI. Include configuration information similar to the following.

Note This example is of a PIX security appliance in single mode. If you are using an ASA security appliance, use the `Management0/0` interface in place of `Ethernet1`.

```
interface Ethernet1
    nameif inside
    security-level 100
    ip address 192.168.1.1 255.255.255.0
http server enable
http 0.0.0.0 0.0.0.0 inside
```

where the IP address 192.168.1.1 is on the same subnet as your security appliance and `inside` is the default name of the interface. (You might give your interface a different name, such as “management.”)

The **http server enable** command with the inside argument enables the HTTP(S) server on the security appliance interface named inside. The **http** command with the 0.0.0.0 0.0.0.0 arguments allows HTTP traffic from any and all IP addresses and subnet masks to the HTTP server through the interface named inside. For more information, see the **http** and **http server enable** commands in the *Cisco Security Appliance Command Reference*.

Note Refer to the **configure factory defaults** or **setup** command in the *Cisco Security Appliance Command Line Configuration Guide* for more information on using the CLI to reestablish factory default settings.

Using the Startup Wizard

The Startup Wizard helps you easily configure a single mode device or a context of a multiple mode device.

Use the Startup Wizard to configure the basic set-up of your security appliance:

Step 1 *If your security appliance is in multi mode,* for each new context, do the following:

a. Create a new context using the **System > Configuration > Features > Security Context** panel.

b. Be sure to allocate interfaces to the context.

c. When you apply the changes, ASDM prompts you to use the Startup Wizard.

d. Click the **Context** icon on the upper header bar and select the context name from the Context menu on the lower header bar.

e. Click **Context > Configuration > Wizards > Startup**.

f. Click **Launch Startup Wizard**.

If your security appliance is in single mode:

a. Click **Configuration > Wizards > Startup**.

b. Click **Launch Startup Wizard**.

Step 2 Click **Next** as you proceed through the Startup Wizard panels, filling in the appropriate information in each panel, such as device name, domain name, passwords, interface names, IP addresses, basic server configuration, and access permissions.

Step 3 Click **Finish** on the last panel to transmit your configuration to the security appliance. Reconnect to ASDM using the new IP address, if the IP address of your connection changes.

(Optional.) You can now enter other configuration details on the **Configuration > Features** panels.

VPN Wizard

The VPN Wizard configures basic VPN access for site-to-site or remote-client access. The VPN Wizard is available only for security appliances running in single context mode with routed (not transparent) firewall mode.

Step 1 Start ASDM.

Step 2 Click **Configuration > Wizards > VPN**. Click **Launch VPN Wizard**.

Step 3 Supply information on each wizard panel. Click **Next** to move through the VPN Wizard panels. You may use the default IPSec and IKE policies. Click the **Help** button for more information on each field.

Step 4 After you complete entering the VPN Wizard information, click **Finish** on the last panel to transmit your configuration to the security appliance.

You can now test the configuration.

Bootstrapping LAN Failover

This section describes how to implement failover on security appliances connected via a LAN.

If you are connecting two ASA security appliances for failover, you must connect them via a LAN. If you are connecting two PIX security appliances, you can connect them using either a LAN or a serial cable.

Tip If your PIX security appliances are located near each other, you might prefer connecting them with a serial cable to connecting them via the LAN. Although the serial cable is slower than a LAN connection, using a cable prevents having to use an interface or having LAN and state failover share an interface, which could affect performance. Also, using a cable enables the detection of power failure on the peer device.

As specified in the *Cisco Security Appliance Command Line Configuration Guide,* both devices must have appropriate licenses and have the same hardware configuration.

Before you begin, decide on active and standby IP addresses for the interfaces ASDM connects through on the primary and secondary devices. These IP addresses must be assigned to device interfaces with HTTPS access.

To configure LAN failover on your security applicance, perform the following steps:

Step 1 Configure the secondary device for HTTPS IP connectivity. Use the **configure factory defaults** or the **setup** CLI command to assign the standby IP address to the ASDM interface on the secondary device.

Step 2 After configuration, the secondary device, has a configuration such as the following. (If you are using an ASA security device, replace the interface `Ethernet1` with `Management0/0`.)

```
interface Ethernet1
    nameif inside
    security-level 100
    ip address 192.168.1.2 255.255.255.0
http server enable
http 0.0.0.0 0.0.0.0 inside
```

where in this example IP address 192.168.1.2 is the standby IP address of the ASDM interface on the secondary device.

Step 3 Configure the primary device for HTTPS IP connectivity using the active IP address for the ASDM interface.

Step 4 Connect the pair of devices together and to their networks in their failover LAN cable configuration.

Step 5 Start ASDM from the primary device through a supported web browser. (See the section Starting ASDM, page 19.)

Step 6 Perform one of the following steps, depending on your security context mode:

a. If your device is in multiple security context mode, click **Context**. Choose the **admin** context from the **Context** drop-down menu, and click **Configuration > Features > Properties > Failover**.

b. If your device is in single mode, click **Configuration > Features > Properties > Failover**. Click the **Interfaces** tab.

Step 7 Perform one of the following steps, depending on your firewall mode:

a. If your device is in routed mode: configure standby addresses for all routed mode interfaces.

b. If your device is in transparent mode: configure a standby management IP address.

Note Interfaces used for failover connectivity should not have names (in single mode) or be allocated to security contexts (in multiple security context mode). In multiple context mode, other security contexts may also have standby IP addresses configured.

Step 8 Perform one of the following steps, depending on your security context mode:

a. If your device is in multiple security context mode: click **System > Configuration > Features > Failover**.

b. If your device is in single mode: click **Configuration > Features > Properties > Failover**.

Step 9 On the **Setup** tab of the **Failover** panel under **LAN Failover**, select the interface that is cabled for LAN failover.

Step 10 Configure the remaining **LAN Failover** fields.

Step 11 (Optional) Provide information for other fields in all of the failover tabs. If you are configuring Active/Active failover, you must configure failover groups in multiple security context mode. If more than one failover pair of devices coexist on a LAN in Active/Active failover, provide failover-group MAC addresses for any interfaces on shared LAN networks.

Step 12 On the **Setup** tab, select the **Enable Failover** check box. If you are using the PIX 500 series security appliance, select the **Enable LAN rather than serial cable failover** check box.

Step 13 Click **Apply**, read the warning dialog that appears, and click **OK**. A dialog box about configuring the peer appears.

Step 14 Enter the IP address of the secondary device, which you configured as the standby IP address of the ASDM interface. Wait about 60 seconds. The standby peer still could become temporarily inaccessible.

Step 15 Click **OK**. Wait for configuration to be synchronized to the standby device over the failover LAN connection.

The secondary device should now enter standby failover state using the standby IP addresses. Any further configuration of the active device or an active context is replicated to the standby device or the corresponding standby context.

ASA Interface Supports Either WebVPN or ASDM Admin Session

The security appliance supports either WebVPN or an ASDM administrative session on an interface, but not both simultaneously. To use ASDM and WebVPN at the same time, configure them on different interfaces.

Unsupported Characters

ASDM does not support any non-English characters or any other special characters. If you enter non-English characters in any text entry field, they become unrecognizable when you submit the entry, and you cannot delete or edit them.

If you are using a non-English keyboard or usually type in language other than English, be careful not to enter non-English characters accidentally.

Workaround:

For workarounds, see CSCeh39437 under Caveats, page 26.

ASDM CLI Does Not Support Intertactive User Commands

ASDM provides a CLI tool (click **Tools > Command Line Interface**...) that allows you to enter certain CLI commands from ASDM. For a list of specific commands that are not support, see Unsupported Commands, page 24.

The ASDM CLI feature also does not support *interactive* user commands. If you enter a CLI command that requires interactive confirmation, ASDM prompts you to enter “[yes/no]” but does not recognize your input. ASDM then times out waiting for your response.

For example:

1. On the ASDM **Tools** menu, click **Command Line Interface**.
2. Enter the command: **`crypto key generate rsa`**

   ASDM generates the default 1024-bit RSA key.
3. Enter the command again: **`crypto key generate rsa`**

   Instead of regenerating the RSA keys by overwriting the previous one, ASDM displays the following error:

   ```
   Do you really want to replace them? [yes/no]:WARNING: You already have RSA
   ke0000000000000$A key
   Input line must be less than 16 characters in length.

   %Please answer 'yes' or 'no'.
   Do you really want to replace them [yes/no]:

   %ERROR: Timed out waiting for a response.
   ERROR: Failed to create new RSA keys names <Default-RSA-key>
   ```

Workaround:

- You can configure most commands that require user interaction by means of the ASDM panels.
- For CLI commands that have a noconfirm option, use the noconfirm option when entering the CLI command. For example:

  ```
  crypto key generate rsa noconfirm
  ```

Printing from ASDM

Note Printing is supported only for Microsoft Windows 2000 or XP in this release.

If you want to print from within ASDM, start ASDM in application mode. Printing is not supported in applet mode in this release.

ASDM supports printing for the following features:

- The Configuration > Features > Interfaces table
- All Configuration > Features > Security Policy tables
- All Configuration > NAT tables
- The Configuration > Features > VPN > IPSec > IPSec Rules table
- Monitoring > Features > Connection Graphs and its related table

Unsupported Commands

ASDM does not support the complete command set of the CLI. In most cases, ASDM ignores unsupported commands, and they can remain in your configuration. In the case of the **alias** command, ASDM enters into Monitor-only mode until you remove the command from your configuration.

Effects of Unsupported Commands

- If ASDM loads an existing running configuration and finds IPv6-related commands, ASDM displays a dialog box informing you that it does not support IPv6. You cannot configure any IPv6 commands in ASDM, but all other configuration is available.
- If ASDM loads an existing running configuration and finds other unsupported commands, ASDM operation is unaffected. To view the unsupported commands, see **Options > Show Commands Ignored by ASDM on Device**.
- If ASDM loads an existing running configuration and finds the **alias** command, it enters Monitor-only mode.

  Monitor-only mode allows access to the following functions:

  – The **Monitoring** area

  – The CLI tool (**Tools > Command Line Interface**), which lets you use the CLI commands

  To exit Monitor-only mode, use the CLI tool or access the security appliance console, and remove the **alias** command. You can use outside NAT instead of the **alias** command. See the *Cisco Security Appliance Command Reference* for more information.

Note You might also be in Monitor-only mode because your user account privilege level, indicated in the status bar at the bottom of the main ASDM window, was set up as less than or equal to 3 by your system administrator, which allows Monitor-only mode. For more information, see **Configuration > Device Administration > User Accounts** and **Configuration > Device Administration > AAA Access**.

Ignored and View-Only Commands

The following table lists commands that ASDM supports in the configuration when added by the CLI, but that cannot be added or edited in ASDM. If ASDM ignores the command, it does not appear in the ASDM GUI at all. If it is view-only, then the command appears in the GUI, but you cannot edit it.

Unsupported Commands	ASDM Behavior
access-list	Ignored if not used, except for use in VPN group policy screens
asr-group	Ignored
capture	Ignored
established	Ignored
failover timeout	Ignored
ipv6, any IPv6 addresses	Ignored
object-group icmp-type	View-only

Unsupported Commands	ASDM Behavior
object-group network	Nested group is view-only
object-group protocol	View-only
object-group service	Nested group cannot be added
pager	Ignored
pim accept-register route-map	Ignored. Only the **list** option can be configured using ASDM
prefix-list	Ignored if not used in an OSPF area
route-map	Ignored

service-policy global	Ignored if it uses a **match access-list** class. For example:
	`access-list myacl line 1 extended permit ip any any`
	`class-map mycm`
	`match access-list mycl`
	`policy-map mypm`
	`class mycm`
	`inspect ftp`
	`service-policy mypm global`

sysopt nodnsalias	Ignored
sysopt uauth allow-http-cache	Ignored
terminal	Ignored
virtual	Ignored

ASDM Limitations

ASDM does not support the one-time password (OTP) authentication mechanism.

Other CLI Limitations

- ASDM does not support discontinuous subnet masks such as 255.255.0.255. For example, you cannot use the following:

```
ip address inside 192.168.2.1 255.255.0.255
```

Securing the Failover Key

To prevent the failover key from being replicated to the peer unit in clear text for an existing failover configuration, disable failover on the active unit (or in the system execution space on the unit that has failover group 1 in the active state), enter the failover key on both units, and then reenable failover. When failover is reenabled, the failover communication is encrypted with the key.

Follow this procedure on the active device:

Step 1 Perform one of the following steps, depending on your security context mode:

a. If your device is in single mode, navigate to **Configuration > Features > Properties > Failover > Setup**.

b. If you device is in multiple mode, navigate to **System > Configuration > Features > Failover > Setup**.

Step 2 Turn off failover. (The standby should switch to pseudo-standby mode.)

a. Clear the **Enable failover** check box.

b. Click **Apply**. (Click **OK** if CLI preview is enabled.)

Step 3 Enter the failover key in the **Shared Key** box.

Step 4 Reenable failover.

a. Select the **Enable failover** check box.

b. Click **Apply**. (Click **OK** if CLI preview is enabled.) A dialog box about configuring the peer appears.

Step 5 Enter the IP address of the peer. Wait about 60 seconds. Even though the standby peer does not have the shared failover key, the standby peer still could become inaccessible.

Step 6 Click **OK**. (Click **OK** if CLI preview is enabled.) Wait for configuration to be synchronized to the standby device over the encrypted failover LAN connection.

Caveats

The following sections describe caveats for the 5.0 release.

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/

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

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

Open Caveats - Release 5.0

- CSCeg14905

  A newly-created Access Rule might be lost if you cancel when adding a subsequent rule.

  This sequence of steps causes the error:

  1. Add a simple access rule on the **Security Policy > Access Rules** panel. Do not apply the changes.
  2. Click **Add** to add another access rule.
  3. Select the **Manage Service Groups...** button.
  4. In the Manage Service Groups dialog, add a new service group.
  5. Click **Apply**. ASDM generates the service group CLI properly.
  6. Return to the Add Access Rule dialog, click **Cancel**. Do not add a new access rule.

7. On the Access Rules panel, the rule you originally added (in Step 1) is still present. It has not yet been applied.
8. Click **Apply** to send the CLI for the originally added rule.

The "No changes were made" dialog erroneously appears.

Workaround:

– After you create a service group, avoid cancelling out of creating a rule.

– Or, create service group(s) before you create access rules.

– Or, apply the access rule when you first configure it (as in Step 2 above).

- CSCeg67083

  On Mozilla 1.7.3 on Linux with Java 1.5.0, if you convert the failover type from serial failover to LAN-based failover then click **Apply**, the ASDM panel locks up and becomes unresponsive.

  This sequence of steps produces the error:

  1. Load ASDM with serial failover enabled.
  2. Go to Configuration > Features > Properties > Failover.
  3. Enable LAN based failover as follows:

  – Click **Enable LAN** (rather than serial cable) failover.

```
LAN failover interface gigabit0
Logical name:fover
active IP:10.7.7.1
standby IP:10.7.7.2
subnet mask: 255.255.255.0
State failover interface gigabt0
```

  – Click **Apply**. Check that the CLIs sent to the security appliance match those shown above.

  The whole panel locks up.

  This problem also occurs when you click the Refresh button on the Failover panel.

  Workaround:

  – Click the **Reset** button on the ASDM panel

  – Navigate to another ASDM panel and then return to the Failover panel.

- CSCeg69476

  If you are using Mozilla 1.7.3 on SunOS 2.8/2.9 with Java 1.5.0_01, when you launch ASDM, it might not accept any keyboard input.

  Workaround:

  Remove and re-create the link to the java library twice. (The first time it may not work. The second time it usually works.)

- CSCeg85016

  On a Linux client with Mozilla 1.7.3 and JRE 1.5.0, when AAA authorization is enabled for commands, it is not possible to start ASDM. This problem also occurs if the device is using any form of authentication, including AAA Authentication or even enable password.

  When you enter a user name and password with privilege level 3, 5 or 15, ASDM does not launch. No errors display and no log is created.

  If you do not use login userid/password to log in, this error does not occur.

Note A bug has been filed with Sun Microsystems on this issue. The problem can be reproduced independently of ASDM.

Workaround:

The problem does not occur if you use JRE 1.4.2. Java 1.5.0 is not supported at this time on Linux.

- CSCeh01635

  When you invoke ASDM as an applet, the Print feature is unavailable.

  Workaround:

  Invoke ASDM using the ASDM Launcher. Printing is supported when ASDM is invoked from the Launcher.

- CSCeh06459

  On the Configuration > Features > Security Policy > Service Policy Rules panel:

  1. If you entered a correct ACL via the CLI, ASDM might mis-represent it in the GUI.
  2. If users try to create an outbound ACL for LLQ using specific addresses or networks, ASDM does not allow them to select a host/network correctly in the ACL. ASDM assumes the direction of the ACL is inbound.
  3. If you are using an ACL for traffic classification and have either a host or network as the source and/or destination, ASDM does not allow you to create the ACL in the desired direction.

  Workaround:

  Use a different traffic classification for the rule. (For example: RTP port range, any/any ACL, DSCP, IP Precedence.)

- CSCeh20409

  If interfaces are available, then a user should not be able to proceed beyond step 4, "Other Interfaces Configuration," until at least one interface has been named. Setting up address translation (NAT/PAT) or administrative access without named interfaces is subsequent step in futile.

  In multiple context mode, if no interfaces have been allocated to a context, the user should be warned that they cannot proceed beyond naming the context (Basic Configuration step 2) until interfaces are allocated to the context in system mode.

  If no interfaces are available currently, evoking the Startup Wizard produces an exception, java.lang.NullPointerException:

```
at com.cisco.pdm.gui.startupwiz.StartupWizModel.getOutsideIf
        (StartupWizModel.java:426)
at com.cisco.pdm.gui.startupwiz.StartupWizModel.<init>
        (StartupWizModel.java:72)
at com.cisco.pdm.gui.startupwiz.StartupWizModel.<init>
        (StartupWizModel.java:64)
at com.cisco.pdm.gui.startupwiz.StartupWizController.<init>
        (StartupWizController.java:40)
at com.cisco.pdm.gui.startupwiz.StartupWizard.<init>
        (StartupWizard.java:49)
at com.cisco.pdm.gui.startupwiz.StartupWizDialog.<init>
        (StartupWizDialog.java:36)
at com.cisco.pdm.gui.startupwiz.StartupWizDialog.<init>
        (StartupWizDialog.java:25)
at com.cisco.pdm.gui.Startup.menuItem_ActionPerformed
        (Startup.java:1853)
at com.cisco.pdm.gui.Startup.actionPerformed(Startup.java:1518)
at java.awt.MenuItem.processActionEvent(Unknown Source)
at java.awt.MenuItem.processEvent(Unknown Source)
at java.awt.MenuComponent.dispatchEventImpl(Unknown Source)
at java.awt.MenuComponent.dispatchEvent(Unknown Source)
at java.awt.EventQueue.dispatchEvent(Unknown Source)
at java.awt.EventDispatchThread.pumpOneEventForHierarchy(Unknown Source)
at java.awt.EventDispatchThread.pumpEventsForHierarchy(Unknown Source)
at java.awt.EventDispatchThread.pumpEvents(Unknown Source)
at java.awt.EventDispatchThread.pumpEvents(Unknown Source)
at java.awt.EventDispatchThread.run(Unknown Source)
```

After the java.lang.NullPointerException, the Startup Wizard may no longer be evoked from the Wizards menu nor any other menu items.

If no interface is named, a **nat () 0 0.0.0.0 0.0.0.0** command will be generated on clicking finish, which has erroneous syntax.

Workaround:

Do not attempt to finish the Startup Wizard until at least one interface has been named.

- CSCeh24609

  If you are using the CLI and you shut down and then bring up the interface through which ASDM is connected, ASDM live logging does not reconnect. It does not show a disconnection message.

  Workaround:

  Close ASDM, then restart it.

- CSCeh24529

  ASDM sometimes allows more than two traffic match criteria for a service policy rule. The CLI does not allow more than two match criteria for a service policy rule and may result an error when this configuration is delivered to the security appliance.

  As an example, the following CLIs may be generated by ASDM:

```
class-map dmz-class
match port udp eq 5060
match precedence 0 1 2 3
match tunnel-group DefaultL2LGroup
```

  But when the commands are sent to the device, the following error is received:

```
[OK] class-map dmz-class
class-map dmz-class
[OK] match port udp eq 5060
[ERR]match precedence 0 1 2 3
ERROR: multiple match commands are not supported except for the 'match tunnel-group or
default-inspect-traffic' command.
```

  The following steps cause the error to occur:

  1. Click **Configuration > Features > Security Policy > Service Policy Rules**.
  2. Select a service policy rule and click **Edit**.
  3. Change the Traffic Match criteria.
  4. For the first three to four times, the error message correctly pops up telling more than two criteria cannot be selected. But after that, you can select more than two criteria.

  For example, in this case the following three criteria were allowed after couple of attempts:

  - Tunnel Group
  - TCP or UDP Destination Port

  - IP Precedence

  Workaround:

  Only select the traffic match criteria that is required for the service policy rule.

- CSCeh33941

  ASDM port values for WebType ACLs do not match the CLI implementation.

  The following CLI help shows the ranges supported for the TCP ports when using the greater than or less than operators:

  ```
  hostname(config)# access-list 1234 webtype permit tcp any gt ?

  configure mode commands/options:
  <0-65534> Enter port number (0 - 65534)
  hostname(config)# access-list 1234 webtype permit tcp any lt ?

  configure mode commands/options:
  <2-65536> Enter port number (2 - 65536)
  ```

  ASDM, however, supports 1-65535, regardless of whether the greater than or less than operator has been specified.

  ASDM does not support:

  ```
  access-list 1234 webtype permit tcp any gt 0
  access-list 1234 webtype permit tcp any lt 65536
  ```

  ASDM does not reject the following, which are not accepted by the CLI:

  ```
  access-list 1234 webtype permit tcp any gt 65535
  access-list 1234 webtype permit tcp any lt 1
  ```

  When specifying the > or < operator for the WebTCP ACL port values, ASDM does not follow the platform implementation.

  Workaround:

  To effect this:

  ```
  access-list 1234 webtype permit tcp any gt 0
  ```

  Use ASDM to configure this:

  ```
  access-list 1234 webtype permit tcp any eq 1
  access-list 1234 webtype permit tcp any gt 1
  ```

  To effect this:

  ```
  access-list 1234 webtype permit tcp any lt 65536
  ```

  Use ASDM to configure this:

  ```
  access-list 1234 webtype permit tcp any eq 65535
  access-list 1234 webtype permit tcp any lt 65535
  ```

  Do not use ASDM to configure:

  ```
  access-list 1234 webtype permit tcp any lt 1
  access-list 1234 webtype permit tcp any gt 65535
  ```

- CSCeh39437

  ASDM, and PIX and ASA 7.0 (1) only support English characters. Many fields in ASDM incorrectly allow you to enter non-English characters. If you enter non-English characters in any text entry field, they become unrecognizable once you submit the entry, and you cannot delete or edit them.

The unrecognizable characters also appear in the `show running-config` output.

Note that the CLI prompt does not accept non-English characters.

Note If you are using a non-English keyboard or usually type in language other than English, be careful not to enter non-English characters accidentally.

Workaround:

If you accidentally enter a non-English character in your running configuration, use one of these workarounds:

- If you have not saved the configuration since you submitted the non-English characters and you have not made any other changes since you last saved, restart your security appliance (without saving the configuration) and the problematic entries disappear.
- If you have not saved the configuration since you submitted the non-English characters, but you have made other changes since you last saved, copy the running configuration to another file as a backup. Reboot your device. Rebooting your device erases the non-English characters but also erases any other changes you have made since your last save. Re-enter the configuration changes that were erased when you rebooted your device.
- Another alternative is to remove the non-English characters with the **`clear`** CLI command. Save your configuration before trying this workaround. The clear CLI command removes all configuration for the associated command, not just the entry you are trying to remove.

  For example, to remove the network object group with a non-English character group name, enter:

  ```
  clear conf object-group network
  ```

  Unfortunately, this command also removes all network object groups, so you need to reconfigure them to restore the original configuration.

- CSCeh39531

  ASDM allows the user to attempt to create the same static NAT for different addresses.

  ```
  [OK]static (inside,outside) 21.1.1.0 1.1.1.0 netmask 255.255.255.0 tcp 0 0 udp 0
  [ERR]static (inside,outside) 21.1.1.0 2.2.2.0 netmask 255.255.255.0 tcp 0 0 udp 0
  ERROR: mapped-address conflict with existing static inside:1.1.1.0 to
  outside:21.1.1.0 netmask 255.255.255.0
  ```

  Workaround:

  Only create a translation once. No specific workaround is required. The security appliance does not accept the conflicting translation, and ASDM re-reads the configuration after the error.

- CSCeh39560

  Starting with a PIX 500 series security appliance configured for serial-cable failover, either Active/Active or Active/Standby in single mode, an attempt to switch to LAN failover with ASDM results in both devices becoming active. Thus neither device is reliably accessible via its interfaces.

  Similarly, switching from LAN to serial-based failover may leave the standby unable to communicate.

  One possible scenario starts with serial-based failover configured and operating, but no LAN failover configuration in place. ASDM enables LAN failover, supplies required LAN failover parameters, and processes the Apply button. After the commands are submitted to the primary device, which turns failover off and then back on again, a dialog requesting to configure the failover peer appears. Unfortunately, both devices are in active state since the secondary, which had failover enabled over the serial cable, does not find its active peer and switches to active itself. Previously, the "failover lan enable" command was replicated, which allowed the devices to use compatible configurations.

With LAN failover enabled and operating properly on both devices, a similar scenario results in somewhat different behavior. ASDM disables LAN failover, removes LAN failover parameters if requested, and processes the Apply button. After the commands are submitted to the primary device, which turns failover off and then back on again, a dialog requesting to configure the failover peer appears. The secondary sometimes attempts to synchronize configuration unsuccessfully at this point, eventually recognizing failure, and restarting synchronization, repeating this in a loop without the ability to disable failover because of the synchronization. Only reloading both devices recovers from the loop: the secondary reenters the loop if it alone is reloaded.

Workaround:

To switch from an operating serial-cable failover to LAN failover, ensure that failover is operating with a **show failover** command and that the primary is the active device.

1. Configure some of the LAN failover parameters with failover still on:

```
failover lan interface <IfName> <PortName>
failover lan interface ip <IfName> <IP_prime> <IP_mask> standby <IP_second>
```

2. Turn off failover on the primary with **no failover**, which replicates to the secondary to turn off failover there too.

3. Issue **failover lan enable** and **failover lan unit primary** commands on the primary.

   (ASDM can submit steps 1, 2, and 3 with a single **Apply** selection.)

4. Perform one of the following steps, depending on your context:

a. *If in multiple context mode,* replacing <Second_IP> with a standby IP address that is enabled for HTTPS in the admin context, enter the following URL in a web browser:

```
https://<Second_IP>/exec/changeto%20system/failover%20lan%20unit%20secondary/failo
ver%20lan%20enable
```

   The browser probably should request authorization.

b. *If in single context mode,* replacing <Second_IP> with a standby HTTPS enabled IP address, via a web browser visit:

```
https://<Second_IP>/exec/failover%20lan%20unit%20secondary/failover%20lan%20enable
```

   The browser probably should request authorization.

c. Or, open a SSH, telnet, or console session with the secondary device and submit:

   - **changeto system** (if in multiple context mode)

   - **configure terminal**

   - **failover lan unit secondary**

   - **failover lan enable**

5. Enable failover on the primary either through ASDM or by submitting the **failover** command, which replicates to the secondary device, beginning configuration synchronization to start LAN failover.

To switch from LAN failover operation to serial-cable failover, ensure that failover is operating with a **show failover** command and that the primary is the active device.

1. On the primary device, submit **no failover**, **no failover lan enable**, and then any other desired commands to remove LAN failover configuration. ASDM may submit this with a single **Apply** selection.
2. Send **no failover lan...** commands to the secondary device with one of the following steps:
   a. Open a SSH, telnet, or console session with the secondary device and submit:

      - **changeto system** (if in multiple context mode)

      - **configure terminal**

      - **no failover lan enable**

      - **no failover lan unit secondary**

   b. Or to a single context mode device, replacing <Second_IP> with a standby HTTPS enabled IP address, via a web browser visit:

      ```
      https://<Second_IP>/exec/no%20failover%20lan%20unit%20secondary/failover%20lan%20e
      nable
      ```

      The browser probably should request authorization.

   c. Or to a multiple context mode device, replacing <Second_IP> with a standby HTTPS enabled IP address, via a web browser visit:

      ```
      https://<Second_IP>/exec/no%20failover%20lan%20enable/no%20failover%20lan%20unit%2
      0secondary
      ```

      The browser probably should request authorization.
3. Enable failover on the primary device, **failover**, which will replicate to the secondary device, beginning configuration synchronization to start failover over the serial cable.

- CSCeh41391

  On the Add Priority Queue screen, the upper range limit value is too high.

  Workaround:

  The upper range limit for the priority queue should be 2048 and the transmission ring limit should be 128.

- CSCeh42043

  When running on Linux with the Java 1.5 plug-in, the user is unable to select an IP Audit policy for an interface using the mouse.

  Workaround:

  Click the Choice list with the mouse to drop down the list. Then, use the keyboard arrow keys to move the cursor up and down to select the desired IP Audit policy.

- CSCeh43422

  When turning on NSSA default-information originate with metric and metric-type, the metric and metric-type are ignored. This is found in Configuration > Features > Routing > OSPF > Setup under Process Instances > Advanced. The section heading is "Default Information Originate."

  Workaround:

  Do one of the following. Either:

  - Create the new area with default-information originate, metric and metric-type specified initially.

   - Or, separately turn on default-information originate and apply the change, then edit again and change the metric and metric-type.

- CSCeh43569

  ASDM Live Logging and Log Buffer may fail to yield any output. While in this state, within your Java console you see errors such as:

  Exception in thread "AWT-EventQueue-2" java.lang.OutOfMemoryError: Java heap space

  After excessive toggling between the logging levels and viewing each log level in the Log Viewer, you may encounter an out-of-memory error.

  For example, repeating this sequence of steps produces the error.

  1. Specify the logging level for ASDM as Debugging.
  2. Go into either Live Log or Log Buffer (Monitoring > Features > Logging.)
  3. Select View.
  4. Close the view and select a different log level such as Critical.
  5. Select View and close the window.

  Workaround:

  Do not toggle excessively between the views and logging levels.

- CSCeh43624

  After editing the key value of an NTP server that was previously configured with a key value, attempting to apply the change results in a dialog saying: "No changes were made."

  Workaround:

  Delete the NTP server and add it again with the new key value.

- CSCeh49697

  On the **Monitoring > Features > VPN > VPN Connection Graphs > IPSec Tunnels** panel, IPSec/IKE Active Tunnels are not being reported correctly sometimes.

  A system with VPN sessions may, over time, show incorrect numbers of IKE and/or IPSec tunnels.

  Workaround:

  Ignore the information from the graphs and use the **Monitoring > Features > VPN > VPN**

  Statistics > Sessions panel to see the correct number of active tunnels.

- CSCeh50535

  On the Configuration -> Routing -> OSPF -> Setup -> Route Summarization panel, when there are two OSPF processes defined, you cannot edit the route summarization of the second OSPF process. After you try to edit it, clicking the OK button does nothing. An exception occurs in the Java console.

  Workaround:

  Delete the route summarization entry and create a new route summarization entry.

- CSCeh52524

  On the **Configuration > Features > Properties > Logging > Syslog Servers** panel, when you select the check box for **Allow user traffic to pass when TCP syslog server is down**, the **Apply** button is not enabled and the CLI cannot be generated.

  Workaround:

Make another change in the same panel and cancel that change, then the **Apply** button is enabled. Click **Apply** and ASDM generates the proper CLI.

- CSCeh53158

  The wrong commands are sent to the security appliance when a network-object for which a static NAT exists is added to a network object-group for which policy NAT already exists.

  For example, network object-group "A" exists and has a policy NAT present. Network "B" exists for which static NAT is configured. Network "B" is added to object-group "A". ASDM generates an invalid command.

  Workaround:

  Avoid adding network/hosts which have static NAT to an object-group which is using policy-NAT.

Related Documentation

For additional information on ASDM or its platforms, refer to the ASDM online Help or the following documentation found on Cisco.com:

- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Cisco ASA 5500 Series Quick Start Guide*
- *Cisco ASA 5500 Series Release Notes*
- *Migrating to ASA for VPN 3000 Series Concentrator Administrators*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Cisco PIX Security Appliance Release Notes*
- *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0*
- *Release Notes for Cisco Intrusion Prevention System 5.0*
- *Installing and Using Cisco Intrusion Prevention System Device Manager 5.0*

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.