Cisco PIX 535 Security Appliance

The Cisco® PIX® 535 Security Appliance delivers a wealth of advanced security and networking services for large enterprise and service provider networks, in a high performance, purpose-built appliance. Its highly modular three-rack unit (3RU) design supports a combination of up to fourteen 10/100 Fast Ethernet interfaces or nine Gigabit Ethernet interfaces as well as redundant power supplies, making it an ideal choice for businesses requiring the highest levels of performance, port density, reliability, and investment protection.

Part of the market-leading Cisco PIX Security Appliance Series, the Cisco PIX 535 Security Appliance provides robust user and application policy enforcement, multi-vector attack protection, and secure connectivity services through a wide range of rich security and networking services, including:

- Advanced Application-Aware Firewall Services
- Market-Leading Voice-Over-IP and Multimedia Security
- Robust Site-to-Site and Remote Access IPSec VPN Connectivity
- Award-Winning Resiliency
- Intelligent Networking Services
- Flexible Management Solutions

Figure 1. Cisco PIX 535 Security Appliance

Advanced Firewall Services Deliver Strong Business Protection and Rich Application Control

Robust Stateful Inspection and Application Layer Security

Cisco PIX Security Appliances integrate a broad range of advanced firewall services to protect businesses from the constant barrage of threats on the Internet and in many business network environments. As a secure foundation, Cisco PIX Security Appliances provide rich stateful inspection firewall services, tracking the state of all network communications and preventing unauthorized network access. Building upon those services, Cisco PIX Security Appliances deliver strong application layer security through 30 intelligent, application-aware inspection engines that examine network flows at Layers 4–7. To defend networks from application layer attacks and to give businesses more control over applications and protocols used in their environment, these inspection engines incorporate extensive application and protocol knowledge and employ security enforcement technologies that include protocol anomaly detection, application and protocol state tracking, Network Address Translation (NAT) services, and attack detection and mitigation techniques such as application/protocol command filtering, content verification, and URL deobfuscation. These inspection engines also give businesses control over instant messaging, peer-to-peer file sharing, and tunneling applications, enabling businesses to enforce usage policies and protect network bandwidth for legitimate business applications.

Multi-Vector Attack Protection

Cisco PIX Security Appliances incorporate multi-vector attack protection services to further defend businesses from many popular forms of attacks, including denial-of-service (DoS) attacks, fragmented attacks, replay attacks, and malformed packet attacks. Using a wealth of advanced attack protection features, including TCP stream reassembly, traffic normalization, DNSGuard, FloodGuard, FragGuard, MailGuard, IPVerify, and TCP intercept, Cisco PIX Security Appliances identify and stop a wide range of attacks, and can provide real-time alerts to administrators.

Flexible Access Control and Powerful Flow-Based Policies

Administrators can also easily create custom security policies using the flexible access control technologies provided by Cisco PIX Security Appliances, including network and service object groups, user and group-based policies, and more than 100 predefined applications and protocols. Using the powerful Modular Policy Framework introduced in Cisco PIX Security Appliance Software v7.0, administrators can define granular flow-based and class map-based policies, which apply a set of customizable security services, such as inspection engine policies, Quality of Service (QoS) policies, connection timers, and more, to each administrator-specified traffic flow/class. By combining these flexible access control and per-flow/class security services, the powerful stateful inspection and application-aware firewall services, and the multi-vector attack protection services that Cisco PIX Security Appliances deliver, businesses can enforce comprehensive security policies to protect themselves from attack.

Market-Leading VoIP Security Services Protect Next-Generation Converged Networks

Cisco PIX Security Appliances provide market-leading protection for a wide range of voice-over-IP (VoIP) other multimedia standards. This allows businesses to securely take advantage of the many benefits that converged data, voice, and video networks provide, including improved productivity, lower operational costs, and increased competitive advantage. By combining VPN and Quality of Service (QoS) with the advanced protocol inspection services that Cisco PIX Security Appliances provide for these converged networking standards, businesses can securely extend voice and multimedia services and the benefits they deliver to remote offices, home offices, and mobile users.

Robust IPSec VPN Services Cost Effectively Connect Networks and Mobile Users

Using the new full-featured VPN capabilities of the Cisco PIX 535 Security Appliance, businesses can securely connect networks and mobile users worldwide across low-cost Internet connections. Solutions supported range from standards-based site-to-site VPN using the Internet Key Exchange (IKE) and IP Security (IPSec) VPN standards, to the innovative Cisco Easy VPN remote access capabilities found in Cisco PIX Security Appliances and other Cisco Systems security solutions, such as Cisco IOS® routers and Cisco VPN 3000 Series Concentrators. Cisco Easy VPN delivers a uniquely scalable, cost-effective, and easy-to-manage remote-access VPN architecture that eliminates the operational costs associated with maintaining the remote-device configurations that are typically required by traditional VPN solutions. Cisco Easy VPN provides feature-rich remote access VPN services, including enforcing VPN client security posture requirements and performing automated software updates of Cisco VPN Clients, to deliver secure, easy-to-manage remote access to corporate networks. Cisco PIX Security Appliances encrypt data using 56-bit Data Encryption Standard (DES), 168-bit Triple DES (3DES), or up to 256-bit Advanced Encryption Standard (AES) encryption. Certain Cisco PIX 535 Security Appliance models have integrated hardware VPN acceleration, delivering highly scalable, high-performance VPN services.

Award-Winning Resilient Architecture Provides Maximum Business Uptime

Select models of Cisco PIX 535 Security Appliances provide award-winning stateful failover services that ensure resilient network protection for enterprise network environments. Businesses can deploy Cisco PIX Security Appliances using either an Active/Standby failover design or a more advanced Active/Active failover design, which supports complex network environments that require asymmetric routing support. Failover pairs continuously synchronize their connection state and device configuration data, thus providing an easy-to-manage high availability solution. Synchronization can optionally take place over a high-speed LAN connection, providing another layer of protection by enabling businesses to geographically separate the failover pair. In the event of a system or network failure, network sessions are automatically transitioned between appliances, with complete transparency to users.

Intelligent Networking Services Enable Simplified Deployment and Seamless Network Integration

Cisco PIX Security Appliances leverage over 20 years of Cisco Systems networking leadership and innovation to deliver a wide-range of intelligent networking services for seamless integration into today's diverse network environments. Administrators can easily integrate Cisco PIX Security Appliances into switched network environments by taking advantage of native 802.1q-based VLAN support. Cisco IP phone deployments can benefit from the "zero-touch provisioning" services provided by Cisco PIX Security Appliances, which help the phones automatically register with the appropriate Cisco CallManager and download any additional configuration information and software images. Businesses can improve their overall network resiliency by taking advantage of the robust Open Shortest Path First (OSPF) dynamic routing services provided by Cisco PIX Security Appliances, which can detect network outages within seconds and route around them. Mission-critical real-time enterprise applications, collaborative computing applications, and streaming multimedia services can be securely delivered using the comprehensive PIM-Sparse Mode v2 and Bidirectional-PIM routing support provided by Cisco PIX Security Appliances. Businesses can secure deployments of next-generation IPv6 networks using the advanced IPv6 security services provided by Cisco PIX Security Appliances, while simultaneously securing existing IPv4 environments with the same appliance during the transition period towards an IPv6 infrastructure.

Flexible Management Solutions Lower Operational Costs

The Cisco PIX 535 Security Appliance delivers a wealth of configuration, monitoring, and troubleshooting methods, giving businesses flexibility to use the methods that best meet their needs. Management solutions range from centralized, policy-based management tools to integrated, Web-based management, to support for remote-monitoring protocols such as Simple Network Management Protocol (SNMP) and syslog. Cisco PIX Security Appliances additionally provide up to 16 levels of customizable administrative roles, so that businesses can grant administrators and operations personnel the appropriate level of access to each appliance, for example: monitoring only access, read-only access to the configuration, network configuration only, firewall configuration only, and so on.

Next-Generation Centralized Management Solutions

Administrators can easily manage large numbers of Cisco PIX Security Appliances using CiscoWorks VPN/Security Management Solution (VMS). This suite consists of several integrated software modules including Management Center for Firewalls, Auto Update Server Software, and Security Monitor. This powerful combination provides a highly scalable, next-generation, three-tier management solution that includes the following features:

- Comprehensive configuration and software image management
- Device hierarchy with “Smart Rules”-based configuration inheritance
- Customizable administrative roles and access privileges
- Comprehensive enterprise change management and auditing
- Intelligent discovery and optimization of security policies and object groups
- “Touchless” software image management for remote Cisco PIX Security Appliances
- Support for dynamically addressed appliances

Attack Mitigation and Event Monitoring Solutions

Network-based attacks can be easily and accurately identified, managed, and eliminated within commercial or enterprise environments using the Cisco Security Monitoring, Analysis, and Response System (CS-MARS) product family. CS-MARS appliances analyze and correlate security events, syslog, and NetFlow data from numerous desktop, server, and network security solutions to determine actual attack paths and provide mitigation options, simplifying security incident management for environments where dedicated security analysts may not be available.

Additionally, Cisco offers the CiscoWorks Security Information Management Solution (CWSIMS), which is well suited for large enterprises and managed security services providers with dedicated security analysts who require in-depth data collection, forensic analysis, audit and compliance, and reporting for complex, multi-vendor networks.

World-Class Device Management Solutions

The integrated Cisco Adaptive Security Device Manager (ASDM) provides a world-class Web-based management interface that greatly simplifies the deployment, on-going configuration, and monitoring of a single Cisco PIX Security Appliance, without requiring any software (other than a standard Web browser and Java Plug-In) to be installed on an administrator’s computer. Intelligent setup and VPN wizards provide easy integration into any network environment, while informative monitoring features, including a dashboard and real-time syslog viewer, provide vital device/network health status and event monitoring at a glance.

Alternatively, administrators can remotely configure, monitor, and troubleshoot their Cisco PIX Security Appliances using a command-line interface (CLI). Secure CLI access is available using several methods, including Secure Shell (SSHv2) Protocol, Telnet over IPSec, and out of band through a console port.

Table 1. Product Features and Benefits

Feature	Benefit
Highly Reliable and Expandable Security Appliance	
Purpose-Built Security Appliance	• Uses a proprietary, hardened operating system that eliminates the security risks associated with general-purpose operating systems • Combines Cisco product quality with no moving parts to provide a highly reliable security platform • Supports redundant AC or DC power supplies for improved platform resiliency
Fast Ethernet and Gigabit Ethernet Expansion Options	• Supports easy installation of additional network interfaces via four 66 Mhz/64-bit and five 33 MHz/32-bit PCI expansion slots • Supports expansion cards including single-port Fast Ethernet, four-port Fast Ethernet and single-port Gigabit Ethernet cards
Hardware VPN Acceleration	• Delivers high speed VPN services through the addition of either a VPN Accelerator Card (VAC) or a VPN Accelerator Card+ (VAC+)—Unrestricted (UR), Failover (FO) and Failover-Active/Active (FO-AA) models have integrated hardware VPN acceleration services
Integration with Leading Third-Party Solutions	• Supports the broad range of Cisco Technology Developer partner solutions that provide URL filtering, content filtering, virus protection, scalable remote management, and more
Industry Certifications and Evaluations	• Earned numerous leading industry certifications and evaluations, including: ◦ Common Criteria Evaluated Assurance Level 4 (EAL4) ◦ FIPS 140-2, Level 2 Validation
Advanced Firewall Services	
Stateful Inspection Firewall	• Provides wide-range of perimeter network security services to prevent unauthorized network access • Delivers robust stateful inspection firewall services which track the state of all network communications • Provides flexible access-control capabilities for more than 100 predefined applications, services, and protocols, with the ability to define custom applications and services • Supports inbound/outbound ACLs for interfaces, time-based ACLs, and per-user/per-group policies for improved control over network and application usage • Simplifies management of security policies by giving administrators the ability to create re-usable network and service object groups that can be referenced by multiple security policies, simplifying initial policy definition and ongoing policy maintenance
Advanced Application and Protocol Inspection	• Integrates 30 specialized inspection engines that provide rich application control and security services for protocols such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Extended Simple Mail Transfer Protocol (ESMTP), Domain Name System (DNS), Simple Network Management Protocol (SNMP), Internet Control Message Protocol (ICMP), SQL*Net, Network File System (NFS), H.323 Versions 1-4, Session Initiation Protocol (SIP), Cisco Skinny Client Control Protocol (SCCP), Real-Time Streaming Protocol (RTSP), GPRS Tunneling Protocol (GTP), Internet Locator Service (ILS), Sun Remote Procedure Call (RPC), and many more
Modular Policy Framework	• Provides a powerful, highly flexible framework for defining flow- or class-based policies, enabling administrators to identify a network flow or class based on a variety of conditions, and then apply a set of customizable services to each flow/class • Improves control over applications by introducing ability to have flow- or class-specific firewall/inspection policies, QoS policies, connection limits, connection timers, and more
Security Contexts	• Enables creation of multiple security contexts (virtual firewalls) within a single Cisco PIX Security Appliance, with each conxt having its own set of security policies, logical interfaces, and administrative domain • Supports four licensed levels of security contexts: 5, 10, 20, and 50 (maximum number of security contexts supported based on model of Cisco PIX Security Appliance) • Provides businesses a convenient way of consolidating multiple firewalls into a single physical appliance or failover pair, yet retaining the ability to manage each of these virtual instances separately • Enables service providers to deliver resilient multi-tenant firewall services with a pair of redundant appliances

Layer 2 Transparent Firewall	• Supports deployment of a Cisco PIX Security Appliance in a secure Layer 2 bridging mode, providing rich Layer 2–7 firewall security services for the protected network while remaining "invisible" to devices on each side of it • Simplifies Cisco PIX Security Appliance deployments in existing network environments by not requiring businesses to re-address the protected networks • Supports creation of Layer 2 security perimeters by enforcing administrator defined Ethertype-based access control policies for Layer 2 network traffic
Multi-Vector Attack Protection	• Provides wealth of advanced attack protection services to defend businesses from many popular forms of attacks, including denial-of-service (DoS) attacks, fragmented attacks, replay attacks, and malformed packet attacks • Delivers advanced TCP stream reassembly and traffic normalization services to assist in detecting hidden application and protocol layer attacks • Integrates with Cisco Network Intrusion Prevention System (IPS) solutions to identify and dynamically block or shun hostile network nodes
Authentication, Authorization, and Accounting (AAA) Support	• Integrates with popular AAA services via TACACS+ and RADIUS, with support for redundant servers for increased AAA services resiliency • Provides highly flexible user and administrator authentication services, dynamic per-user/per-group policies, and administrator privilege control through tight integration with Cisco Secure Access Control Server (ACS)
Robust IPSec VPN Services	
Cisco Easy VPN Server	• Delivers feature-rich remote access VPN concentrator services for up to 2000 remote software- or hardware-based VPN clients • Pushes VPN policy dynamically to Cisco Easy VPN Remote-enabled solutions (such as the Cisco VPN Client) upon connection, helping to ensure that the latest corporate VPN security policies are used • Performs VPN client security posture checks when a VPN connection attempt is received, including enforcing usage of authorized host-based security products (such as the Cisco Security Agent) and verifying its version number and status prior to letting the remote user access the corporate network • Provides administrators precise control over what different types of VPN clients (software client, router, VPN 3002, and PIX) are allowed to connect based on type of client, operating system installed, and version of VPN client software • Supports automatic software updates of Cisco VPN Clients and Cisco 3002 Hardware VPN Clients, with the ability to trigger updates when VPN connections are established, or on-demand for currently connected VPN clients • Extends VPN reach into environments using NAT or Port Address Translation (PAT), via support of a variety of TCP and UDP-based NAT traversal methods including the Internet Engineering Task Force (IETF) draft standard
Cisco VPN Client	• Includes a free unlimited license for the highly acclaimed, industry-leading Cisco VPN Client • Available on wide-range of platforms including Microsoft Windows 98, ME, NT, 2000, XP; Sun Solaris; Intel-based Linux distributions; and Apple Macintosh OS X • Provides many innovative features including dynamic security policy downloading from Cisco Easy VPN Server-enabled products, automatic failover to backup Easy VPN Servers, administrator customizable distributions, and more • Integrates with the award-winning Cisco Security Agent (CSA) for comprehensive endpoint security
Site-to-Site VPN	• Supports IKE and IPSec VPN standards • Extends networks securely over the Internet by helping to ensure data privacy, data integrity, and strong authentication with remote networks and remote users • Improves network reliability and performance through support of OSPF dynamic routing and reverse-route injection over site-to-site VPN tunnels
Native Integration with Popular User Authentication Services	• Provides convenient method for authenticating VPN users through native integration with popular authentication services including Microsoft Active Directory, Microsoft Windows Domains, Kerberos, LDAP, and RSA SecurID (without requiring a separate RADIUS/TACACS+ server to act as an intermediary)
X.509 Certificate and CRL Support	• Supports Simple Certificate Enrollment Protocol (SCEP)-based enrollment and manual enrollment with leading X.509 solutions from Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA, and VeriSign • Interoperates with large-scale Public Key Infrastructure (PKI) deployments through n-tiered certificate hierarchy support

Resilient Architecture	
Active/Active and Active/Standby Stateful Failover	• Ensures resilient network protection for businesses through the award-winning high availability services provided by certain models of Cisco PIX 535 Security Appliances • Supports Active/Standby failover services as a cost-effective high availability solution, where one failover pair member operates in hot-standby mode acting as a complete redundant system that maintains current session state information for the active unit • Delivers advanced Active/Active failover services where both Cisco PIX Security Appliances in a failover pair actively pass network traffic simultaneously and share state information bi-directionally, enabling support for asymmetric routing environments and effectively doubling the throughput of the failover pair for bursty network traffic conditions • Supports long-distance failover enabling geographic separation of failover pair members, providing another layer of protection
VPN Stateful Failover	• Maximizes VPN connection uptime with new Active/Standby stateful failover for VPN connections • Synchronizes all security association (SA) state information and session key material between failover pair members, providing a highly resilient VPN solution **Note:** This feature is available on Unrestricted (UR), Failover (FO), and Failover-Active/Active (FO-AA) models only.
Zero-Downtime Software Upgrades	• Enables businesses to perform software maintenance release upgrades on Cisco PIX Security Appliance failover pairs without impacting network uptime or connections through the support of state-sharing between mixed Cisco PIX Security Appliance Software versions (running version 7.0(1) or higher)
Intelligent Networking Services	
VLAN-Based Virtual Interfaces	• Provides increased flexibility when defining security policies and eases overall integration into switched network environments by supporting the creation of logical interfaces based on IEEE 802.1q VLAN tags, and the creation of security policies based on these virtual interfaces • Supports multiple virtual interfaces on a single physical interface through VLAN trunking, with support for multiple VLAN trunks per Cisco PIX Security Appliance • Supports up to 150 total VLANs on Cisco PIX 535 Security Appliances
QoS Services	• Delivers per-flow, policy-based QoS services, with support for LLQ and traffic policing for prioritizing latency-sensitive network traffic and limiting bandwidth usage of administrator-specified applications • Enables businesses to have end-to-end QoS policies for their extended network
OSPF Dynamic Routing	• Provides comprehensive OSPF dynamic routing services using technology based on world-renowned Cisco IOS Software • Offers improved network reliability through fast route convergence and secure, efficient route distribution • Delivers a secure routing solution in environments using NAT through tight integration with Cisco PIX Security Appliance NAT services • Supports MD5-based OSPF authentication, in addition to plaintext OSPF authentication, to prevent route spoofing and various routing-based DoS attacks • Provides route redistribution between OSPF processes, including OSPF, static, and connected routes • Supports load balancing across equal-cost multipath routes
PIM Multicast Routing	• Streamlines the delivery of multimedia traffic in video-conferencing, collaborative computing, and mission critical real-time enterprise applications through full PIM-Sparse Mode v2 and Bidirectional-PIM routing support (based on world-class Cisco IOS multicast technology)
IPv6 Networking	• Provides access control and deep inspection firewall services for native IPv6 network environments and mixed IPv4/IPv6 network environments through dual-stack support • Delivers IPv6-enabled inspection services for HTTP, FTP, SMTP, ICMP, TCP, and UDP-based applications • Supports SSHv2, telnet, HTTP/HTTPS, and ICMP-based management over IPv6
Dynamic Host Control Protocol (DHCP) Server	• Provides DHCP server services on one or more interfaces, allowing devices to obtain IP addresses dynamically • Includes extensions for automated provisioning of Cisco IP phones and Cisco SoftPhone IP telephony solutions
DHCP Relay	• Forwards DHCP requests from internal devices to an administrator-specified DHCP server, enabling centralized distribution, tracking and maintenance of IP addresses
NAT/PAT Support	• Provides rich dynamic, static, and policy-based NAT, and PAT services

Flexible Management Solutions	
CiscoWorks VPN/Security Management Solution (VMS)	• Provides a comprehensive management suite for large scale Cisco security product deployments • Integrates policy management, software maintenance and security monitoring in a single management console
Cisco Adaptive Security Device Manager (ASDM)	• World-class Web-based GUI enables simple, secure remote management of Cisco PIX Security Appliances • Provides a wide range of informative, real-time, and historical reports which give critical insight into usage trends, performance baselines, and security events
Auto Update	• Provides "touchless" secure remote management of Cisco PIX Security Appliance configuration and software images via a unique "push/pull" management model • Next-generation secure Extensible Markup Language (XML) over HTTPS management interface can be used by Cisco and third-party management applications for remote Cisco PIX Security Appliance configuration management, inventory, software image management/deployment and monitoring • Integrates with CiscoWorks Management Center for Firewalls and Auto Update Server for robust, scalable remote management of up to 1000 Cisco PIX Security Appliances (per management server)
Cisco PIX Command Line Interface (CLI)	• Allows customers to use existing Cisco IOS Software CLI knowledge for easy installation and management without additional training • Supports improved ease-of-use with services such as command completion, context-sensitive help, and command aliasing • Accessible through variety of methods including console port, Telnet, and SSHv2
Command-Level Authorization	• Gives businesses the ability to create up to 16 customizable administrative roles/profiles for managing a Cisco PIX Security Appliance (monitoring only, read-only access to configuration, VPN administrator, firewall/NAT administrator, etc.) • Uses either the internal administrator database or outside sources via TACACS+, such as Cisco Secure ACS
SNMP and Syslog Support	• Supports Cisco IPSec Flow Monitoring SNMP MIB, providing a wealth of VPN flow statistics including tunnel uptime, bytes/packets transferred, and more

License Options

The Cisco PIX 535 Security Appliance is available in four primary models that provide different levels of interface density, failover capabilities, and VPN throughput. Optional licenses support enabling features including security contexts, GTP inspection, and various strengths of encryption technology.

Platform Licenses

Restricted Software License

The Cisco PIX 535 Restricted (PIX 535-R) model provides an excellent value for organizations looking for robust Cisco PIX Security Appliance services with gigabit firewall throughput, high interface density, maximum investment protection and moderate VPN throughput requirements. It includes 512 MB of RAM, two 10/100 Fast Ethernet interfaces, and support for up to six additional 10/100 Fast Ethernet or eight Gigabit Ethernet interfaces.

Unrestricted Software License

The Cisco PIX 535 Unrestricted (PIX 535-UR) model extends the capabilities of the security appliance with support for stateful failover, additional LAN interfaces, and increased VPN throughput via integrated hardware-based VPN acceleration. It includes an integrated VAC or VAC+ hardware VPN accelerator, 1 GB of RAM, two 10/100 Fast Ethernet interfaces, and support for up to twelve additional 10/100 Fast Ethernet or nine Gigabit Ethernet interfaces. The Cisco PIX 535-UR also adds the ability to share state information with a secondary Cisco PIX Security

Appliance (either in an Active/Active or Active/Standby deployment model) for resilient network protection.

Failover Active/Standby Software License

The Cisco PIX 535 Active/Standby Failover (PIX 535-FO) model is designed for use in conjunction with a PIX 535-UR, providing a cost-effective, Active/Standby high-availability solution. It operates in hot-standby mode acting as a complete redundant system that maintains current session state information. With the same hardware configuration as the Cisco PIX 535-UR, it delivers the ultimate in high availability for a fraction of the price.

Failover Active/Active Software License

The Cisco PIX 535 Failover Active/Active (PIX 535-FO-AA) model is designed for use in conjunction with a PIX 535-UR, providing a scalable Active/Active high-availability solution. Advanced network topologies, such as those with asymmetric routing, are supported through the Active/Active architecture where both Cisco PIX Security Appliances pass network traffic and exchange bi-directional state sharing updates with one another. This license is supported by Cisco PIX Security Appliance Software v7.0 and higher. License upgrades are available for existing PIX 535-FO units to convert from Active/Standby to Active/Active failover.

Feature Licenses

Security Context Licenses

The Cisco PIX 535 Security Appliance can support up to 50 security contexts, with each context having its own separate security policies and administrative domain. Several tiers of security context licenses are available for Cisco PIX 535 Security Appliances, including 5, 10, 20, and 50 security contexts. This license is supported by Cisco PIX Security Appliance Software v7.0 and higher, and requires an Unrestricted (UR), Failover (FO), or Failover Active/Active (FO-AA) license, security contexts are not supported on Restricted (R) models.

GTP Inspection License

The Cisco PIX 535 Security Appliance can provide advanced security services for GTP/GPRS 3G Mobile Wireless environments upon installation of the GTP Inspection License. This license is supported by Cisco PIX Security Appliance Software v7.0 and higher, and requires either an Unrestricted (UR), Failover (FO), or Failover Active/Active (FO-AA) license, GTP inspection is not supported on Restricted (R) models.

Encryption License

3DES/AES and DES Encryption Licenses

The Cisco PIX 535 Security Appliance has two optional encryption licenses, one license (PIX-VPN-3DES) enables 168-bit 3DES and up to 256-bit AES encryption, the other license (PIX-VPN-DES) enables 56-bit DES encryption. Both are available either at the time of ordering the Cisco PIX 535 Security Appliance, or can be obtained subsequently through Cisco.com. Note that an encryption license must be installed to activate encryption services which are required before using certain features including VPN and secure remote management.

Performance Summary

- Cleartext throughput: Up to 1.7 Gbps
- Concurrent connections: 500,000
- 168-bit 3DES IPSec VPN throughput: Up to 425 Mbps with VAC+ or 100 Mbps with VAC

- 128-bit AES IPSec VPN throughput: Up to 495 Mbps with VAC+
- 256-bit AES IPSec VPN throughput: Up to 425 Mbps with VAC+
- Simultaneous VPN tunnels: 2000

Technical Specifications

- Processor: 1 GHz Intel Pentium III Processor
- RAM: 512 or 1 GB of SDRAM
- Flash memory: 16 MB
- Cache: 256 KB level 2 at 1GHz
- System buses: Two 64-bit, 66 MHz PCI, one 32-bit, 33 MHz PCI

Environmental Operating Ranges

Operating

- Temperature: -25 to 131ºF (-5 to 55ºC)
- Relative humidity: 5 to 95 percent noncondensing
- Altitude: 0 to 9843 ft (3000 m)
- Shock: 1.14 m/sec (45 in./sec) 1/2 sine input
- Vibration: 0.41 Grms2 (3 to 500 Hz) random input
- Acoustic noise: 65 dBa maximum

Nonoperating

- Temperature: -13 to 158ºF (-25 to 70ºC)
- Relative humidity: 5 to 95 percent noncondensing
- Altitude: 0 to 15000 ft (4570 m)
- Shock: 30 G
- Vibration: 0.41 Grms2 (3 to 500 Hz) random input

Power

Input (per power supply)

- Range line voltage: 100V to 240V AC or 48V DC
- Nominal line voltage: 100V to 240V AC or 48V DC
- Current: 4-2 A
- Frequency: 50 to 60 Hz, single phase
- Power: 220W (dual hot swap power supply capable)

Output

- Steady state: 135W
- Maximum peak: 220W
- Maximum heat dissipation: 750 BTU/hr, full power usage (220W)

Physical Specifications

Dimensions and Weight Specifications

- Form factor: 3 RU, standard 19 in. rack mountable
- Dimensions (H x W x D): 5.25 x 17.5 x 18.25 in. (13.33 x 44.45 x 46.36 cm)
- Weight (with one power supply): 32 lb (14.5 kg)

Expansion

- Four 64-bit/66 MHz PCI slots
- Five 32-bit/33 MHz PCI slots
- Six 168-pin DIMM RAM slots, supporting up to 6 GB PC133 DRAM maximum

Interfaces

- Console port: RS-232, 9600 bps, RJ-45
- Failover port: RS-232, 115 Kbps, DB-15 (special Cisco PIX failover cable required)
- Two integrated 10/100 Fast Ethernet interfaces, auto-negotiate (half/full duplex), RJ-45

Regulatory and Standards Compliance

Safety

UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950, AS/NZS3260, TS001, IEC60825, EN 60825, 21CFR1040

Electromagnetic Compatibility (EMC)

FCC Part 15 (CFR 47) Class A, ICES 003 Class A with UTP, EN55022 Class A with UTP, CISPR 22 Class A with UTP, AS/NZ 3548 Class A with UTP, VCCI Class A with UTP, EN55024, EN50082-1 (1997), CE marking, EN55022 Class B with FTP, Cispr 22 Class B with FTP, AS/NZ 3548 Class B with FTP, VCCI Class B with FTP

Product Ordering Information

Table 2 lists ordering information for the Cisco PIX 535 Security Appliances and related products.

Table 2. Ordering Information

PIX-535	Cisco PIX 535 Chassis (chassis, software, two 10/100 interfaces)
PIX-535-DC	Cisco PIX 535 DC Chassis (chassis, software, two 10/100 interfaces)
PIX-535-R-BUN	Cisco PIX 535 Restricted Bundle (chassis, restricted license, software, two 10/100 interfaces, 512 MB RAM)
PIX-535-UR-BUN	Cisco PIX 535 Unrestricted Bundle (chassis, unrestricted license, software, two 10/100 interfaces, 1 GB RAM, VAC or VAC+)
PIX-535-UR-GE-BUN	Cisco PIX 535 Unrestricted Three GE + Two FE Bundle (chassis, unrestricted license, software, three Gigabit Ethernet + two 10/100 interfaces, 1 GB RAM, VAC or VAC+, dual AC power supplies)
PIX-535-FO-BUN	Cisco PIX 535 Active/Standby Failover Bundle (chassis, Active/Standby failover license, software, two 10/100 interfaces, 1 GB RAM, VAC or VAC+)
PIX-535-FO-GE-BUN	Cisco PIX 535 Active/Standby Failover Three GE + Two FE Bundle (chassis, Active/Standby failover license, software, three Gigabit Ethernet + two 10/100 interfaces, 1 GB RAM, VAC or VAC+, dual AC power supplies)
PIX-535-AA-GE-BUN	Cisco PIX 535 Failover Active/Active Bundle (chassis, failover Active/Active license, software, three Gigabit Ethernet + two 10/100 interfaces, 1 GB RAM, VAC+, dual AC power supplies)
PIX-535-HW=	Cisco PIX 535 rack mount kit, console cable, failover cable
PIX-FO=	Cisco PIX failover cable
PIX-1FE	Cisco PIX single-port 10/100 Fast Ethernet interface card, RJ-45

PIX-4FE-66	Cisco PIX 64-bit/66 MHz four-port 10/100 Fast Ethernet interface card, RJ-45
PIX-1GE-66	Cisco PIX 64-bit/66 MHz single-port Gigabit Ethernet interface card, Multimode (SX) SC
PIX-VPN-ACCEL	Cisco PIX DES/3DES VPN Accelerator Card (VAC)
PIX-VAC-PLUS	Cisco PIX DES/3DES/AES VPN Accelerator Card+ (VAC+)
PIX-SW-SC-5	Cisco PIX 5 security contexts license
PIX-SW-SC-10	Cisco PIX 10 security contexts license
PIX-SW-SC-20	Cisco PIX 20 security contexts license
PIX-SW-SC-50	Cisco PIX 50 security contexts license
PIX-SW-GTP	Cisco PIX GTP/GPRS inspection license
PIX-VPN-DES	Cisco PIX DES VPN/SSH/SSL encryption license
PIX-VPN-3DES	Cisco PIX 3DES/AES VPN/SSH/SSL encryption license

Support Services

Support services are available from Cisco and Cisco partners. Cisco SMARTnet® service augments customer support resources, providing anywhere, anytime access to technical resources (both online and by telephone), the ability to download updated system software, and hardware advance replacement.

Support Ordering Information

Table 3 lists ordering information for Cisco SMARTnet support services.

Table 3. Cisco SMARTnet Ordering Information

CON-SNT-PIX535	Cisco SMARTnet 8x5xNBD service for Cisco PIX 535 chassis only
CON-SNT-PIX535R	Cisco SMARTnet 8x5xNBD service for Cisco PIX 535-R bundle
CON-SNT-PIX535UR	Cisco SMARTnet 8x5xNBD service for Cisco PIX 535-UR bundle
CON-SNT-PIX535FO	Cisco SMARTnet 8x5xNBD service for Cisco PIX 535-FO bundle
CON-SNT-PIX535AA	Cisco SMARTnet 8x5xNBD service for Cisco PIX 535-AA bundle
CON-SNTE-PIX535	Cisco SMARTnet 8x5x4 service for Cisco PIX 535 chassis only
CON-SNTE-PIX535R	Cisco SMARTnet 8x5x4 service for Cisco PIX 535-R bundle
CON-SNTE-PIX535UR	Cisco SMARTnet 8x5x4 service for Cisco PIX 535-UR bundle
CON-SNTE-PIX535FO	Cisco SMARTnet 8x5x4 service for Cisco PIX 535-FO bundle
CON-SNTE-PIX535AA	Cisco SMARTnet 8x5x4 service for Cisco PIX 535-AA bundle
CON-SNTP-PIX535	Cisco SMARTnet 24x7x4 service for Cisco PIX 535 chassis only
CON-SNTP-PIX535R	Cisco SMARTnet 24x7x4 service for Cisco PIX 535-R bundle
CON-SNTP-PIX535UR	Cisco SMARTnet 24x7x4 service for Cisco PIX 535-UR bundle
CON-SNTP-PIX535FO	Cisco SMARTnet 24x7x4 service for Cisco PIX 535-FO bundle
CON-SNTP-PIX535AA	Cisco SMARTnet 24x7x4 service for Cisco PIX 535-AA bundle
CON-S2P-PIX535	Cisco SMARTnet 24x7x2 service for Cisco PIX 535-R chassis only
CON-S2P-PIX535R	Cisco SMARTnet 24x7x2 service for Cisco PIX 535-R bundle
CON-S2P-PIX535UR	Cisco SMARTnet 24x7x2 service for Cisco PIX 535-UR bundle
CON-S2P-PIX535FO	Cisco SMARTnet 24x7x2 service for Cisco PIX 535-FO bundle
CON-S2P-PIX535AA	Cisco SMARTnet 24x7x2 service for Cisco PIX 535-AA bundle
CON-OS-PIX535	Cisco SMARTnet On-Site 8x5xNBD service for Cisco PIX 535 chassis only
CON-OS-PIX535R	Cisco SMARTnet On-Site 8x5xNBD service for Cisco PIX 535-R bundle
CON-OS-PIX535UR	Cisco SMARTnet On-Site 8x5xNBD service for Cisco PIX 535-UR bundle
CON-OS-PIX535FO	Cisco SMARTnet On-Site 8x5xNBD service for Cisco PIX 535-FO bundle

CON-OS-PIX535AA	Cisco SMARTnet On-Site 8x5xNBD service for Cisco PIX 535-AA bundle
CON-OSE-PIX535	Cisco SMARTnet On-Site 8x5x4 service for Cisco PIX 535 chassis only
CON-OSE-PIX535R	Cisco SMARTnet On-Site 8x5x4 service for Cisco PIX 535-R bundle
CON-OSE-PIX535UR	Cisco SMARTnet On-Site 8x5x4 service for Cisco PIX 535-UR bundle
CON-OSE-PIX535FO	Cisco SMARTnet On-Site 8x5x4 service for Cisco PIX 535-FO bundle
CON-OSE-PIX535AA	Cisco SMARTnet On-Site 8x5x4 service for Cisco PIX 535-AA bundle
CON-OSP-PIX535	Cisco SMARTnet On-Site 24x7x4 service for Cisco PIX 535 chassis only
CON-OSP-PIX535R	Cisco SMARTnet On-Site 24x7x4 service for Cisco PIX 535-R bundle
CON-OSP-PIX535UR	Cisco SMARTnet On-Site 24x7x4 service for Cisco PIX 535-UR bundle
CON-OSP-PIX535FO	Cisco SMARTnet On-Site 24x7x4 service for Cisco PIX 535-FO bundle
CON-OSP-PIX535AA	Cisco SMARTnet On-Site 24x7x4 service for Cisco PIX 535-AA bundle

Additional Information

For more information, please visit the following links.

- Cisco PIX Security Appliance Series: http://www.cisco.com/go/pix
- Cisco Adaptive Security Device Manager: http://www.cisco.com/go/asdm
- Current list of Cisco product security certifications: http://www.cisco.com/go/securitycert
- Cisco Secure ACS: http://www.cisco.com/go/acs
- CiscoWorks VMS, Management Center for Firewalls, Auto Update Server Software and Security Monitor: http://www.cisco.com/go/vms
- CiscoWorks SIMS: http://www.cisco.com/go/sims
- SAFE Blueprint from Cisco: http://www.cisco.com/go/safe

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C78-448066-00 12/07

