

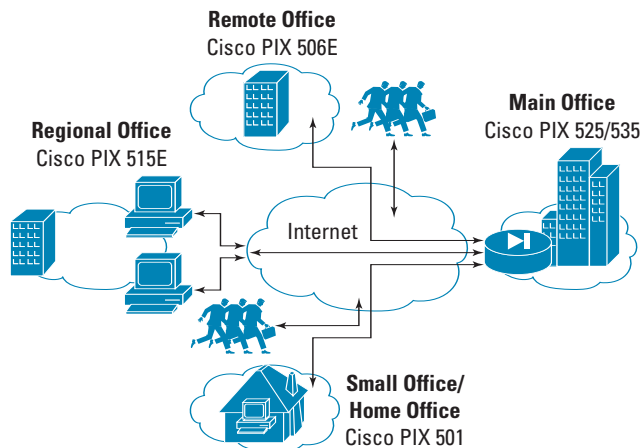
## At-A-Glance

The Cisco PIX Security Appliance Series combines market-leading, best-of-breed stateful inspection firewalling, application inspection engines, and IP Security (IPSec) VPN for the complete security solution. Cisco PIX security appliances provide robust site-to-site and remote-access VPN services, enabling businesses to create secure connections across public networks to mobile users, remote sites, and business partners. Data can be encrypted using Data Encryption Standard (DES), Triple DES (3DES), or Advanced Encryption Standard (AES). The Cisco PIX VPN Acceleration Card Plus (VAC+) delivers high-performance tunneling and hardware-based encryption services suitable for site-to-site and remote-access applications. Offloading encryption functions to the Cisco PIX VAC+ not only improves IPSec encryption processing, but also maintains high end firewall performance. An integral network component, the Cisco PIX VAC+ provides platform scalability and security while smoothly working with the services necessary for successful VPN deployments: encryption, tunneling, and firewall.

VPN connections can be authenticated using a variety of methods ranging from X.509 certificates to one-time passwords to shared secrets. Users can be authenticated against the internal user ID/password database on the appliance itself, or via an external source using TACACS+ or RADIUS. Using RADIUS and integration with Cisco Secure Access Control Server (ACS), Cisco PIX security appliances can integrate with nearly any external source of user authentication information.

This enables a network administrator to define a single policy that incorporates both security and connectivity for remote offices and workers. This single policy provides unparalleled security, while maintaining an accessible network environment. Cisco PIX security appliances provide an integrated approach to security that enables organizations to gain the connectivity and cost benefits of the Internet, without compromising the integrity of the corporate security policy (Figure 1).

Figure 1 Cisco PIX VPN Network



The integrated VPN and firewall capabilities of Cisco PIX security appliances deliver critical components of an effective VPN deployment:

### Feature-Rich for Comprehensive Network Protection

- The integrated stateful inspection capabilities of Cisco PIX security appliances protect VPN deployments against denial of service (DoS) attacks. Cisco PIX security appliances provide a secure foundation with rich stateful inspection firewall services that track the state of all network communications and prevent unauthorized network access. Building upon those services, Cisco PIX security appliances deliver strong application-layer security through 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 the applications and protocols used in their environments, these inspection engines incorporate extensive application and protocol knowledge and employ security enforcement technologies, including 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. The inspection engines also enable control over instant messaging, peer-to-peer file sharing, and tunneling applications, enabling businesses to enforce usage policies and free up network bandwidth for legitimate business applications.

### Access Control Provides Implicit User Access Control

- Detailed security policy can be applied to VPN traffic, since user access information is common to the firewall and VPN technologies. Individuals and groups of users have access to the services and resources to which they are entitled, and all VPN traffic is decrypted and inspected to ensure that only appropriate content is allowed through the device. Access to network resources can also be strongly authenticated through the Cisco PIX Security Appliance's local user database or through integration with enterprise databases, either directly using TACACS+/RADIUS or indirectly with Cisco Secure ACS. Additionally, Cisco PIX security appliances support dynamic downloading and enforcement of access control lists (ACLs) on a per-user basis, upon user authentication with the device.

### Touchless Deployment with Cisco Easy VPN Offers Ease of Management

- Cisco PIX security appliances support the innovative Cisco Easy VPN capabilities also found in other Cisco solutions such as Cisco IOS® routers and Cisco VPN 3000 Series Concentrators which deliver a uniquely scalable, cost-effective, and easy-to-manage remote-access VPN architecture. Built on the foundation of dynamic policy distribution and effortless provisioning, Cisco Easy VPN eliminates the operational costs associated with maintaining remote-device configurations typically required by traditional VPN solutions. Acting as an Easy VPN Server, Cisco PIX security appliances dynamically push the latest VPN security policy to Cisco VPN clients when they connect, simplifying management of these remote clients.

Cisco PIX security appliances also enforce VPN client security posture requirements and perform automated software updates of Cisco VPN clients to deliver secure, easy-to-manage remote access to corporate networks.

- Cisco PIX 501 and 506E Security Appliances additionally support Easy VPN Remote functionality. This enables dramatically simplified VPN rollouts to small office, teleworker, and remote/branch-office environments, allowing these devices to act as hardware VPN clients, eliminating the provisioning complexities of traditional site-to-site VPN deployments. These security appliances also support other advanced capabilities (when acting as a hardware VPN client) such as automatic tunnel re-establishment to a backup Easy VPN Server in the event of a VPN tunnel failure, support for automatic load-balancing of Cisco VPN 3000 Concentrators and IETF-based Network Address Translation (NAT) transparency.

### Resiliency Features Provide A Dependable Solution

- Cisco PIX security appliances support numerous IPSec resiliency features to help ensure maximum reliability and robustness in a VPN deployment as well as an award-winning, high-availability solution. Cisco PIX supports two methods of redundancy for IPSec connections: Cisco IKE keepalives and Dead Peer Detection (DPD). Cisco IKE keepalives are a simple, nonintrusive method to detect loss of connectivity between two IPSec peers. The Cisco PIX device sends "hello" packets to the remote peer at configurable time intervals. Once three packets are missed, the Cisco PIX device will conclude that it has lost VPN connectivity with its peer. The device will attempt to connect to the next peer in the list (if configured) to create a new security association. This will continue until a connection is made. Another redundancy method is Dead Peer Detection. The DPD is method is similar to Cisco IKE keepalives in that it also sends hello packets to an IPSec peer. However, while IKE keepalives send the hello packet at specified intervals, DPD does not send a hello packet if there is traffic from the peers that proves they are operational. DPD reduces CPU usage of sending and receiving keepalive traffic among IPSec peers.
- Cisco PIX Security Appliance select models provide award-winning, firewall stateful failover capabilities that help to ensure resilient network protection for enterprise network environments. Employing a cost-effective, active-standby, high-availability architecture, Cisco PIX security appliances that are configured as a failover pair continuously synchronize their connection state and device configuration data. Synchronization can take place over a high-speed LAN connection, providing another layer of protection through the ability to geographically separate the failover pair. In the event of a system or network failure, network sessions are automatically transitioned from the active to the standby device, with complete transparency to users.
- 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. With OSPF, Cisco PIX security appliances can detect network outages within seconds and route around them, improving network reliability for VPN-connected networks.

## At-A-Glance

### Investment Protection

- The highly modular design of Cisco PIX security appliances makes them suitable for small, medium-sized, and large enterprise. This high level of modularity provides unmatched investment protection where individual components of the solution can be upgraded as requirements grow, avoiding costly “forklift” upgrades of the entire chassis to enable new features, or increase performance levels or I/O port density. Additional Fast Ethernet or Gigabit Ethernet interfaces, VLAN-based virtual interfaces, and redundant power supplies make Cisco PIX security appliances ideal for businesses requiring the highest level of performance, port density, reliability, and investment protection.
- Certain Cisco PIX models have integrated hardware VPN acceleration capabilities. The Cisco VAC+ delivers up to 425 Mbps of DES, 3DES, or AES IPSec encryption throughput. Well beyond full-duplex OC-3 line rates, the Cisco PIX Security Appliance with Cisco VAC+ provides excellent price/performance for small to very large enterprise-class site-to-site aggregation. Moreover, it supports up to 2000 encrypted tunnels for mixed VPN environments that have both site-to-site and remote-access VPN requirements. These performance features, along with upgradeable encryption accelerators and LAN interfaces, make Cisco PIX security appliances one of the most scalable, upgradeable, and cost-effective central-site VPN and security solutions on the market. This high level of modularity provides unmatched investment protection where individual components of the solution can be upgraded as requirements grow, avoiding costly “forklift” upgrades of the entire chassis to enable new features or performance levels.

### Consolidated Management Provides A Complete Picture of Security Events

- PIX Security Appliances allow for consolidated management of security policies, particularly in networks where multiple devices are required. Security policy changes or database updates can be applied to all devices, minimizing the occurrence of configuration errors.
- An integrated security solution helps to ensure that consolidated logging and auditing for networks, users, objects, services, and administrators is available in unified log files.

### Robust Remote Management Solutions Lower Total Cost of Ownership (TCO)

- Cisco PIX security appliances deliver a wealth of remote-management methods for configuration, monitoring, and troubleshooting. Management solutions include centralized, policy-based management tools, integrated, Web-based management and 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 enterprises can grant administrators and operations personnel the appropriate level of access to each PIX device (for example, monitoring only, read-only access to the configuration, VPN configuration only, firewall configuration only, and so on). Cisco PIX security appliances also include robust Auto Update capabilities, a set of revolutionary secure remote-management services that ensure configurations and software images are kept up to date.

- Administrators can easily manage numerous remote Cisco PIX security appliances using CiscoWorks VPN/Security Management Solution (VMS) or Cisco IP Solution Center (ISC). For single device management, the integrated Cisco PIX Device Manager provides an intuitive, Web-based management interface for remotely configuring, monitoring, and troubleshooting a Cisco PIX Security Appliance without requiring any software (other than a standard Web browser) to be installed on an administrator’s computer. Alternatively, through methods that include Telnet, Secure Shell (SSH) Protocol, or out of band through a console port, administrators can remotely configure, monitor, and troubleshoot Cisco PIX security appliances using a commandline interface (CLI).