# How Cisco IT Uses Firewalls to Protect Cisco Internet Access Locations

## Cisco PIX Security Appliance provides stateful firewall protection at smaller Internet gateways.

**Cisco IT Case Study / Security and VPN / PIX Firewall in Enterprise Network:** This case study describes how Cisco Systems uses Cisco PIX security appliances to protect its network assets from unauthorized access. The Cisco global network is a leading-edge enterprise environment that is one of the largest and most complex in the world. Cisco customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

"With its stateful-inspection capability, the Cisco PIX 525 Security Appliance minimizes the IT burden by reducing the number of entries in the ACLs for incoming and outgoing traffic. We've cut the previous burden in half because Cisco PIX security appliances automatically allow the return traffic for both incoming and outgoing ACLs and rules."

**— Hasan Talukdar, Cisco IT network engineer**

### CHALLENGE

Cisco Systems® gives a high priority to protecting its data and network from unauthorized users, both outside and inside the company. The accepted solution for many years has been to deploy a firewall in each of its multipeered Internet gateways worldwide. A firewall, which can be hardware- or software-based, examines network traffic and decides whether to forward packets to their destinations based on access control lists (ACLs) and inspection rules.

Recently Cisco® IT began deploying Internet gateways at data centers to better support remote-access VPN connectivity. Employees working remotely need improved access to the company intranet, to link them directly to the nearest Cisco VPN gateway instead of sending packets by circuitous routes on the Internet. From 2001 to 2004 Cisco IT raised the number of Internet access points from 5 to 11. Cisco IT selected the Cisco PIX® 535 Firewall to provide access security at these smaller gateway sites. When the Cisco PIX 525 Security Appliance became available, Cisco IT selected it to deploy in all new Internet gateways, since the 525 supported all Cisco IT needs in a smaller form facter. An important advantage available on the Cisco PIX security appliance is stateful inspection. A stateful-inspection firewall remembers the state of a network connection passing through in one direction, so that when the flow returns in the other direction, the firewall recognizes it and passes it through to its destination. Hasan Talukdar explains: "Suppose we have a TCP connection between host A and host B. The initial packet flow will have a source IP address and a destination port and ID. When the traffic returns, the nonstateful firewall won't remember it and therefore will need to look up the rules to see if it's allowed. A stateful-connection firewall, in contrast, expects to see the return traffic and forwards it without having to check the rules, improving performance and eliminating the need to maintain a second set of ACLs."

Another incentive for Cisco to deploy the Cisco PIX security appliance was the improved application availability made possible by stateful failover, a capability related to but distinct from stateful-inspection firewalling. In every point of presence (POP), Cisco had two redundant Cisco routers. If the primary router failed, the secondary automatically took control; however, packets passing through the primary router when it failed would be dropped. When that happened, Cisco employees who were using latency-dependent applications, such as H.323 and Session Initiation Protocol (SIP), experienced application delays. "Cisco routers are very reliable and have had to fail over very rarely in

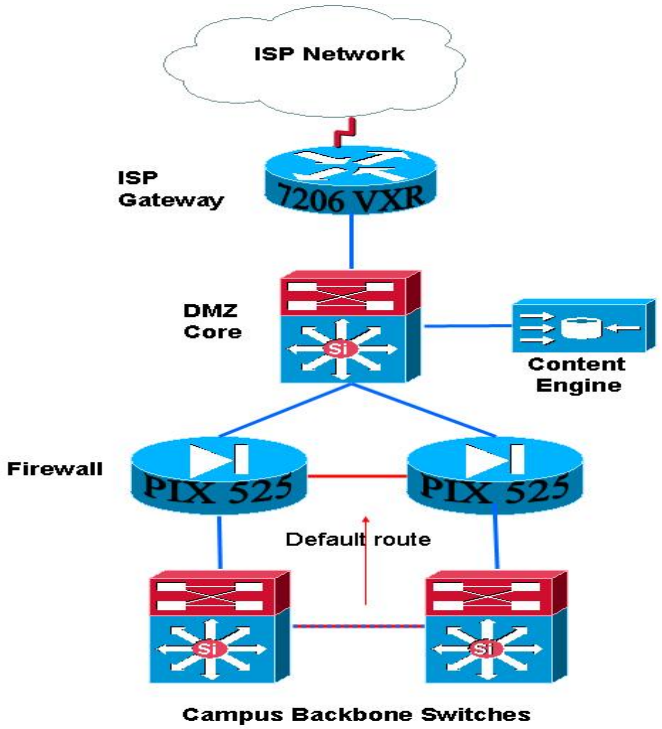
our environment," Talukdar says. "And yet, anything that Cisco IT can do to help ensure business continuity, we do. Therefore, we wanted our new stateful-inspection firewall to also provide stateful failover."

## SOLUTION

Cisco IT decided to deploy a stateful-connection firewall solution at six small POPs worldwide. For the relatively small user populations at these locations—the largest POP served 1600 employees—Cisco selected the Cisco PIX 535 Security Appliance. This security appliance provides robust network and application security by enforcing administrator-defined access control policies while performing deep packet inspection and tracking the state of all network communications. "The Cisco PIX 535 Security Appliance provides more than 360 Mbps of firewall throughput with the ability to handle as many as 280,000 simultaneous sessions, which is important in the high-volume Cisco environment," says Talukdar. Integrated hardware VPN acceleration capabilities ensure high performance even during peak traffic times by offloading compute-intensive encryption from the firewall processor. The firewall solution provides up to 70 Mbps of Triple Data Encryption Standard (3DES) VPN and support for 2000 IP Security (IPSec) tunnels, providing the needed scalability for the tens of thousands of Cisco teleworkers, mobile workers, and partners who connect to the Cisco intranet by VPN. Cisco PIX security appliances provide an additional layer of security in the form of intelligent, application-aware security services that examine packet streams at Layers 4 through 7, using inspection engines specialized for Cisco such as Network-Based Application Recognition (NBAR), which Cisco uses to defend against the spread of worms and viruses in its popular applications.

Cisco IT equipped each POP with redundant Cisco PIX Security Appliances: a primary and a secondary (Figure 1). The secondary device continually monitors the state and number of connections of the primary device. Should the primary device fail, the secondary knows how many connections are currently in process and transparently takes control. "Even latency-sensitive applications such as H.323 and SIP can continue without interruption," says Talukdar.

**Figure 1.** Cisco PIX 525 Security Appliance Deployment in Small POPs




With its new stateful-inspection firewall, Cisco IT needs only to configure one ACL for unique incoming and outgoing flows. The Adaptive Security Algorithm (ASA), part of the Cisco PIX operating system, creates a connection table

entry for a session flow based on the source and destination addresses, randomized TCP sequence numbers, port numbers, and additional TCP flags. “When a flow comes through in one direction, the firewall remembers it and expects to see it come back,” says Talukdar. The Cisco PIX Security Appliance controls all inbound and outbound traffic by applying the security policy to these connection table entries.

### Transition Process

To transition a Cisco location from the nonstateful firewall in Cisco IOS® Software to the Cisco PIX Security Appliance, Cisco IT follows these steps:

- Build the architecture in the lab at San Jose headquarters, using the same router, core, and backbone as the site to be transitioned.
- Configure the Cisco PIX security appliances with ACLs and rules. Following are excerpts from the configuration for a Cisco site. The full rule set contains 1000 to 2000 lines. (Note that sample IP addresses have been used here.)

  interface ethernet0 100full
  interface ethernet1 100full
  interface ethernet2 100full
  interface ethernet3 auto shutdown
  nameif ethernet0 outside security0  CONNECTED TO DMZ CORE
  nameif ethernet1 inside security100 CONNECTED TO CAMPUS BACKBONE
  nameif ethernet2 stateful security15 Stateful, between 2.

  Rule sets

  ---

  access-list 111 permit ip any host 172.16.0.0 [EASILY ALLOW ACCESS TO HOST WITH A SPECIFIED PROTOCOL]
  access-list 111 permit ip any host 172.16.0.1

  Failover

  ---

  failover
  failover timeout 0:00:00
  failover poll 15
  failover ip address outside 192.168.255.255
  failover ip address inside 192.168.255.255
  failover ip address stateful 192.168.255.250
- Test the configuration. “During this phase we discover configuration issues,” says Talukdar. Configuration issues are resolved with help from Cisco Technical Assistance Center engineers.
- Test the implementation. Cisco IT tests the configuration in parallel with the solution the site is presently using—typically a Cisco 7200 Series Router. Testers use the empty port on the core switch to connect the two Cisco PIX firewalls and confirm proper connectivity and failover.
- Place the Cisco PIX firewalls in production, still in parallel with the existing infrastructure. This phase usually lasts about two weeks, or until Cisco IT is satisfied the deployment is stable.
- Migrate to the Cisco PIX Security Appliance system during a scheduled maintenance window.
- Monitor the infrastructure for a week to confirm proper operation. “Because firewalls have a lot of rules, it’s easy to miss one or two,” says Talukdar.
- For the first sites that Cisco IT migrated, proof of concept (steps 1 through 4) lasted 2 weeks, equipment

delivery took 2 weeks because of issues with shipping equipment across different countries, and the actual transition took 2 weeks, for a total of 6 weeks.

### Configuration

The Cisco PIX Security Appliance can be configured using a variety of methods: an integrated, Web-based management interface called the Cisco PIX Device Manager; centralized, policy-based management tools; and a command-line interface (CLI) accessed using Telnet, Secure Shell (SSH) Protocol, or an out-of-band console port. To avoid inadvertently leaving off a line or two of a 10,000-line configuration file during a cut-and-paste operation, Cisco enters all the rules in a file, saves it, and then uploads the configuration. “We created the rules just once; since then, loading the configuration into the firewalls for a new site takes just a few seconds,” says Talukdar.

The Cisco PIX Security Appliance understands Routing Information Protocol (RIP) and learns routes dynamically if companies use this protocol. Cisco, however, uses Enhanced Interior Gateway Routing Protocol (EIGRP). Therefore, to route traffic through the Cisco PIX 535, Cisco configured 5 to 10 static routes. “Static routes keep the design simple and avoid redistribution into the EIGRP routing domain,” says Jawahar Sivasankaran, Cisco IT network engineer.

## RESULTS

### Configuration Time Cut by Half

Cisco IT has achieved its goals of reducing the time to create and change firewall configurations, a primary incentive for the transition to a stateful-inspection firewall. “With its stateful-inspection capability, the Cisco PIX Security Appliance minimizes the IT burden by reducing the number of entries in the ACLs for incoming and outgoing traffic,” says Talukdar. “We’ve cut the previous burden in half because Cisco PIX security appliances automatically allow the return traffic for both incoming and outgoing ACLs and rules.”

The Cisco PIX Security Appliance also eliminates the need to configure the secondary router separately, as was required when Cisco used redundant Cisco 7500 Series routers as firewalls. Only one of the two redundant Cisco PIX firewalls has to be configured: The configuration for the primary firewall is automatically saved to the secondary over a failover cable. “Automatic copying of the configuration reduces the likelihood of errors and saves administrative overhead,” says Talukdar.

### Increased Security

The Cisco PIX Security Appliance increases the security of the Cisco network in several ways. Because it remembers the state of the TCP, UDP, or Internet Message Control Protocol (ICMP) flow, it prevents a would-be network intruder from inserting another flow. Srinivasan says, “It helps defend against denial-of-service and malformed packet attacks by using the robust Adaptive Security Algorithm, as well as built-in intrusion-protection features such as TCP Intercept, TCP SYN cookies, DNS Guard, Flood Defender, Flood Guard, Mail Guard, and Unicast Reverse Path Forwarding. It also looks for 59 different attack signatures. We can block these attacks and notify administrators about them in real time.”

### High Availability

Should the primary Cisco PIX Security Appliance fail for any reason, the secondary device takes control so that no packets are lost. Cisco users do not see application errors, and their work remains uninterrupted.

Another way the Cisco PIX Security Appliance helps ensure availability is by performing the Port Address Translation (PAT) function more efficiently than a dedicated gateway. Says Talukdar, “Since we began using the Cisco PIX Security Appliance for PAT, we haven’t had a single outage related to memory or resource issues.”

### Reduced Rack Space Requirements

Cisco has reduced its data center rack space requirements by replacing Cisco 7200 Series routers with the smaller Cisco PIX 525 Security Appliance in more recent deployments. “The Cisco PIX 525 Security Appliance is two rack units, compared to three rack units for the previous router,” says Talukdar. “That’s important in our data center, where rack space is at a premium.”

## LESSONS LEARNED

During the deployment in Tel Aviv, the Cisco team noted the following:

If there is a need to configure Border Gateway Protocol (BGP) neighbors between two routers through the Cisco PIX security appliance using Message Digest Algorithm 5 (MD5) authentication, the firewall randomizes the sequence numbers for the MD5 authentication packets. Therefore, the passwords for the neighbors do not match.

“We created a workaround by enabling static Network Address Translation (NAT) for the source IP address and using the norandomseq keyword in the static NAT command for the Cisco PIX firewall,” says Talukdar. “In addition, we denied the source IP address from being changed in the global NAT inside command.” Following is the workaround if a Cisco PIX Security Appliance is deployed between router A, with an IP address of 172.16.0.0 on the internal network, and router B, with an IP address outside the firewall:

```
 nat (inside) 0 access-list nonat

static (inside,outside)  172.16.0.0  172.16.0.0 netmask 255.255.255.255 0 0  norandomseq

access-list nonat deny ip host 172.16.0.0 any

access-list nonat permit ip any any
```

## NEXT STEPS

Long-term plans include allowing Cisco PIX security appliances to fail over to their counterparts in other Cisco locations. “If the Internet connection is down, the Cisco PIX firewall remains unaware,” says Talukdar. “Therefore, packets destined for the Internet travel all the way to the Internet gateway, only to be dropped. If a location has only one ISP connection, it presently has no alternative.” To provide a redundant route between POPs, Cisco IT is looking into different advanced BGP features that ISP gateways can use to advertise conditional routes.

“The Cisco PIX Security Appliance has helped us achieve our goals for business continuity and simplified management in the small POP environment,” says Talukdar. “With the FWSM [firewall services module], we’ll extend the same benefits to our largest sites.”

## FOR MORE INFORMATION

To read the entire case study or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

## NOTE

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

**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, Inc.
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.**