



# PIX Firewall in Enterprise Network

How Cisco IT Uses Firewalls to  
Protect Cisco Internet Access  
Locations



## A Cisco on Cisco Case Study: Inside Cisco IT

# Overview

- Challenge

Protecting Cisco's data and network from unauthorized users

- Solution

Cisco IT deployed Cisco PIX 535 Security Appliance at six small POPs worldwide

- Results

Benefits of Cisco PIX Security Appliance

- Next Steps

Fail over to Cisco PIX security appliances counterpart in other locations

# Challenge: Protecting Cisco's data and network from unauthorized users

- Eliminating need for second set of access control lists (ACLs)

Firewall does not remember original IP address, destination port, and ID

- Improve application availability for stateful failover

Two redundant Cisco routers in every point of presence (POP)

Failing packets passing primary router is dropped, resulting in application delays for Cisco employees

# **Solution: Cisco IT deployed Cisco PIX 535 Security Appliance at six small POPs worldwide**

- Provide robust network and application security:
  - Enforcing administrator-defined access control policies
  - Perform deep packet inspections and tracking the state of all network communications
- Ensure high performance even during peak traffic times:
  - Offloading compute-intensive encryption from firewall processor
- Provide up to 70 Mbps of Triple Data Encryption Standard (3DES) VPN

# **Solution:** Cisco IT deployed Cisco PIX 535 Security Appliance at six small POPs worldwide (Contd.)

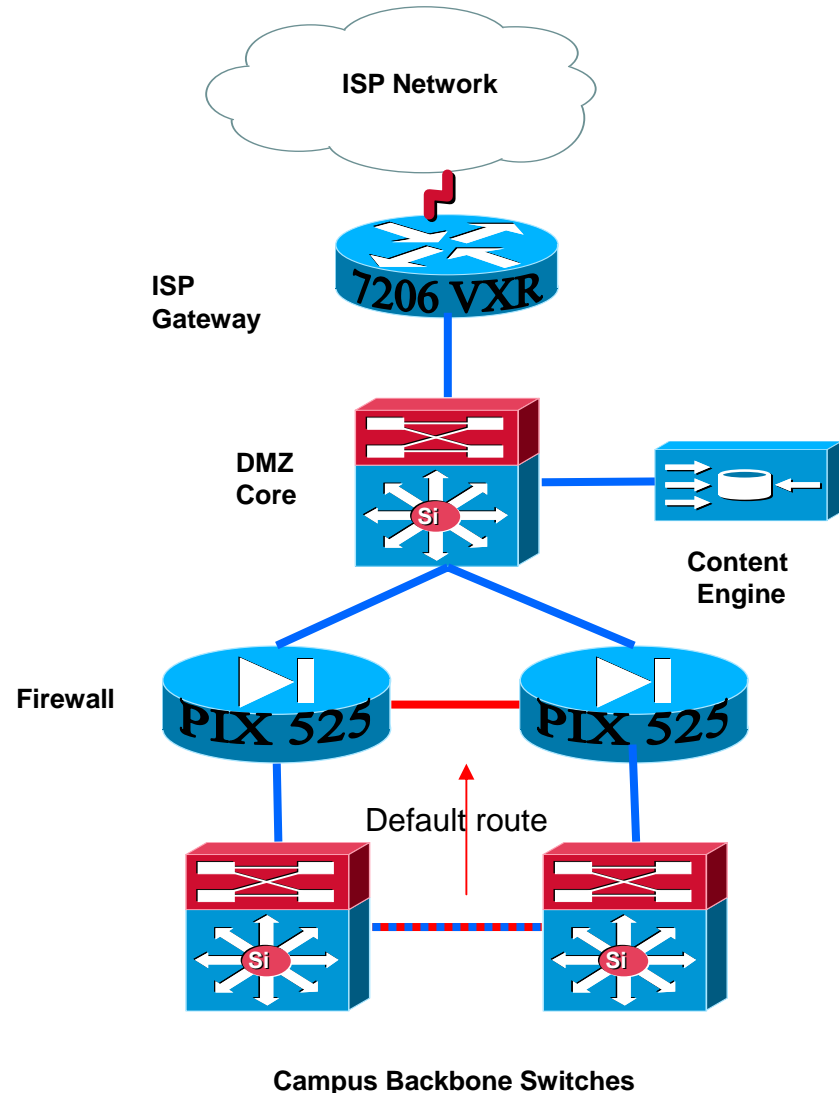
- Provide an additional layer of security

Examine packet streams at Layers 4 – 7

Network-Based Application Recognition (NBAR) is used to defend against the spreading for worms and viruses

# **Solution:** Cisco IT equipped primary & secondary redundant Cisco PIX Security Appliances

- If primary device fails, then secondary knows how many connections are currently in process and transparently takes control



# Results: Benefits of Cisco PIX Security Appliance

- Configuration Time Cut by Half

Automatically allows the return traffic for both incoming and outgoing ACLs and rules

- Increases Security

Remembers the state of TCP, UDP, or Internet Message Control Protocol (ICMP) flow

- High Availability

If primary device fails, then second device takes control to prevent lost packets

Performs Port Address Translation (PAT)

- Reduced Rack Space Requirements

# **Next Steps: Fail over to Cisco PIX security appliances counterpart in other locations**

- Cisco IT looking for different advanced BGP features
  - ISP gateways to advertise conditional routes
- With firewall services module (FWSM)
  - Same benefits will be extended to Cisco's largest sites



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](http://www.cisco.com/go/ciscoit)



**Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://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](http://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](http://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](http://www.cisco.com/go/offices).



©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0704R)