Cisco Secure Firewall
Product Update
Session 2504
Agenda

- **Introduction**
  - Definition, history and deployment
  - Firewall technologies
- **Product Updates**
  - Cisco IOS™ Firewall
  - Cisco Secure PIX™ Firewall
  - PIX Product Family
  - PIX Roadmap
What Is a Firewall?

- A set of hardware and software enforcing security policy at a point on a network
- Perimeter security device
- Commonly capable of Virtual Private Networks (VPN)

History of Firewalls

- Originally a set of custom-configured routers and hosts
History of Firewalls

- Originally a set of custom-configured routers and hosts
- Commercial host-based products followed
- Dedicated appliance now predominant choice
The Future of Network Security

Integrated

Identity  Security Monitoring

Privacy/VPN  Policy Management  Perimeter Security

Ubiquitous  Transparent

Firewall Technologies
Basic Security Elements

- Cisco IOS security technologies provide:
  - Perimeter security and access control
  - Identification and user authentication
  - Denial of Service (DoS) protection
  - VPN
  - Auditing

Existing Cisco IOS Security Technologies

- Access control lists (ACL)
  - Reflexive access lists
  - Time-based access lists
- Network Address Translation (NAT)
- VPN technologies
  - IPsec encryption
  - Tunneling (GRE, L2F, L2TP)
- Policy-based multi-interface support
- Event logging
- TACACS+/RADIUS authentication
Firewall Technologies

- Stateful firewalling
  PIX—Adaptive Security Algorithm (ASA)
  Cisco IOS Firewall—content-based application control
  Tracks state of authorized data streams to prevent exploitation

- Application awareness
  “Fixup” protocols
  Validation of protocol syntax

Firewall Deployment

- “Pervasive Firewalling”
  Security on every network device
- Not: “Should I perform security at this network junction?”
- Rather: “Why would I not want security on this device?”
Cisco Secure PIX Firewall IPsec VPNs

- Expand corporate intranet
  Leverage the Internet for cost savings and increased connectivity

- Enable mobile users
  Increase efficiency
  Reduce response time

- DES IPsec at no cost
  3DES for nominal license fee
  Up to 90 Mbps DES
  Up to 20 Mbps 3DES in software
  Up to 70 Mbps 3DES with hardware acceleration

Product Updates
Firewall Solutions

- **Cisco IOS Firewall**
  Integrated firewall solution for Cisco IOS software which combines advanced firewalling and intrusion detection with full routing and WAN access capabilities

- **Cisco Secure PIX Firewall**
  Dedicated firewalling in a high-performance, scalable and fault-tolerant dedicated security appliance

---

**Cisco IOS Firewall**

- **Integrated solution**
  Combines firewall and routing into one platform—easy add on for existing network administrators

- **No new hardware required—**
  one device to manage
  
  Support for Cisco 800, 900, 1400, 1600, 1700, 2500, 2600, 3600, 7100, 7200 and 7500 routers and RSM for Catalyst 5000 Switch

- **Full routing functionality**
PIX Firewall Family

- **Scalability**
  - PIX 506
  - PIX 515
  - PIX 520

- **Performance**

PIX Gigabit Ethernet Card

- Designed for large enterprise, hosting services and other high-traffic environments
- Up to 387 megabits/second (full duplex) on PIX 520 systems
PIX Encryption Accelerator Card

- Designed for high-traffic VPN environments
- Up to 70 megabits/sec at 3DES

Cisco Secure PIX Firewall 506

- Small office firewall
  - 2–5 person remote office or “power user” home office
  - Two Ethernet interfaces
  - 10 Mbps throughput
  - IPsec 3DES VPN support at 4 Mbps
Cisco Secure PIX Firewall 515

- **PIX 515-R**
  Restrictions: No failover, 65,000 connections, 2 Ethernet interfaces

- **PIX 515-UR**
  125,000 connections
  Up to six Ethernet interfaces

- **High performance**
  Up to 120 Mbps throughput
  Up to 6,500 connections per second

Cisco Secure PIX Firewall 520

- **Enterprise chassis design**
  Over 250,000 simultaneous sessions
  Most flexible configuration options
  Designed for enterprise environments
Summary

Where to Put Each Firewall

**PIX Firewall**
- High-volume or sensitive network perimeters
- Dedicated device
- Multilevel security policy enforcement
- Specific application requirements
- Unique NAT applications

**Cisco IOS Firewall**
- Everywhere you have a router/switch
- Integrated solution
- Cost effective
- Highly scalable
- Home office to enterprise
- Intranet protection
- Familiar Cisco IOS configuration
Things to Remember

- Firewalls are one element in securing your network
- Defense in depth— not one device alone
- Actively audit to monitor for misuse or intrusion
- Cisco offers end-to-end network security solutions
Please Complete Your Evaluation Form

Session 2504