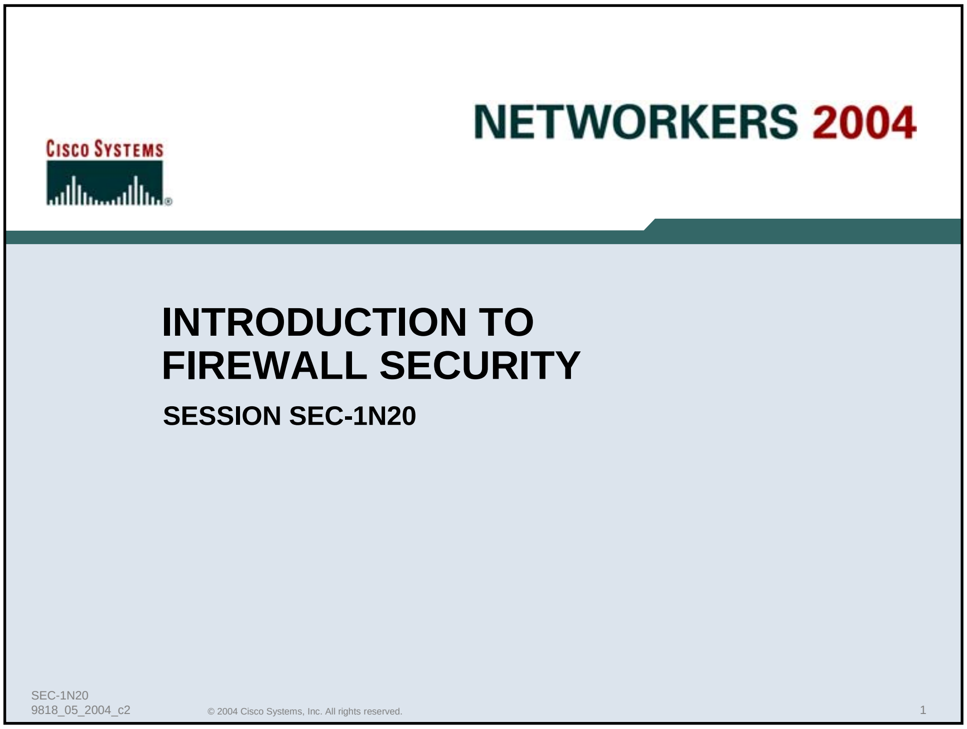
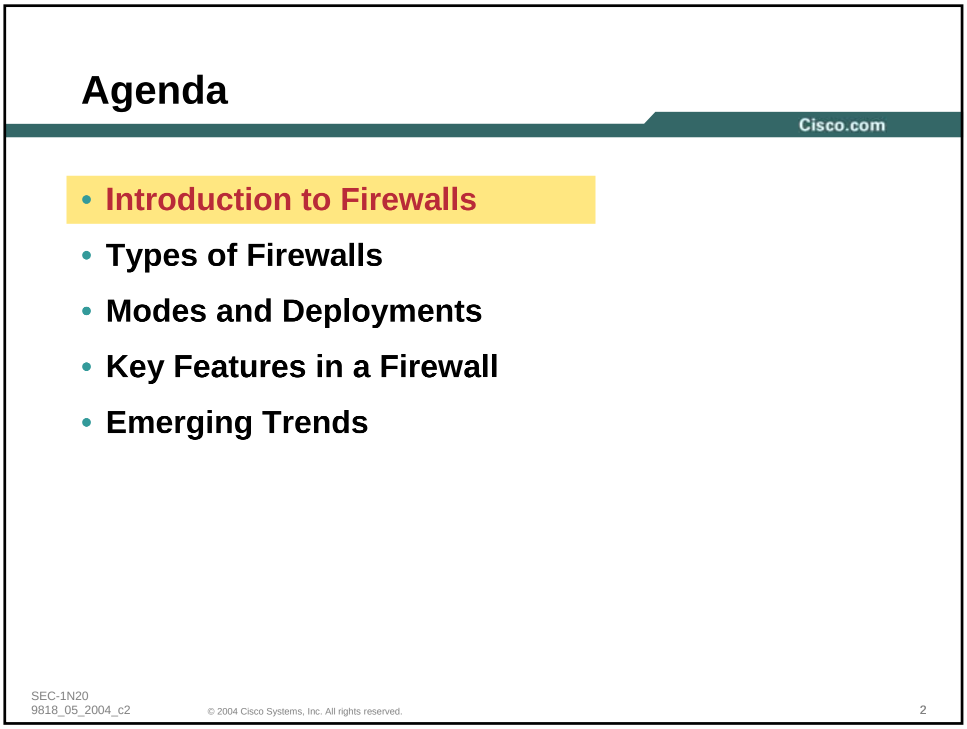


NETWORKERS 2004

INTRODUCTION TO FIREWALL SECURITY

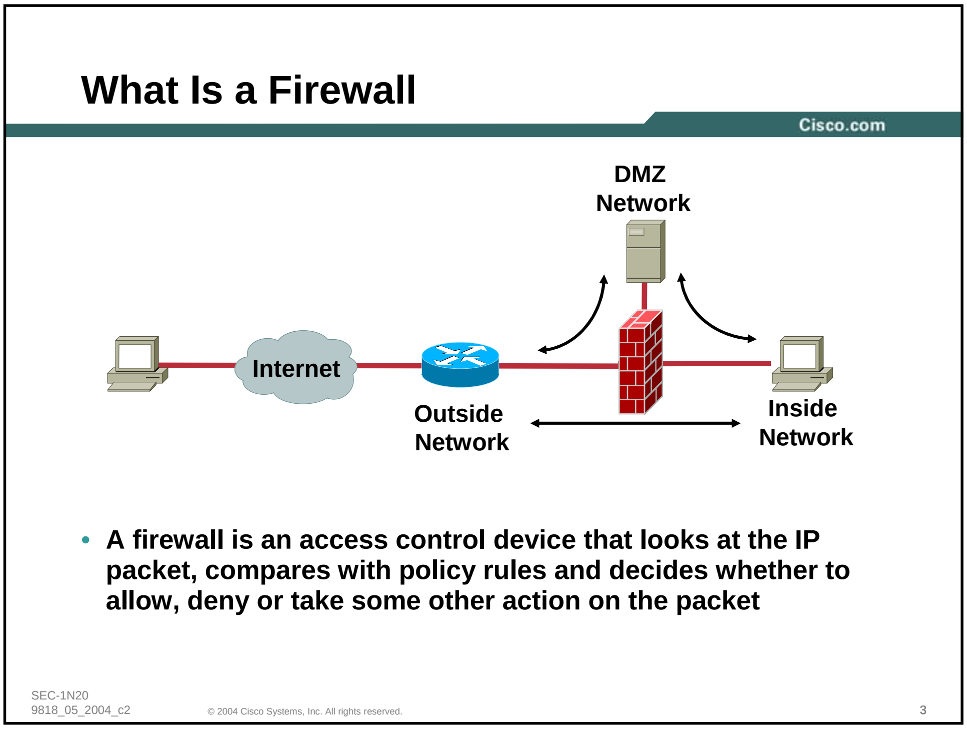
SESSION SEC-1N20



Agenda

Cisco.com

- Introduction to Firewalls
- Types of Firewalls
- Modes and Deployments
- Key Features in a Firewall
- Emerging Trends



What Is a Firewall

Cisco.com

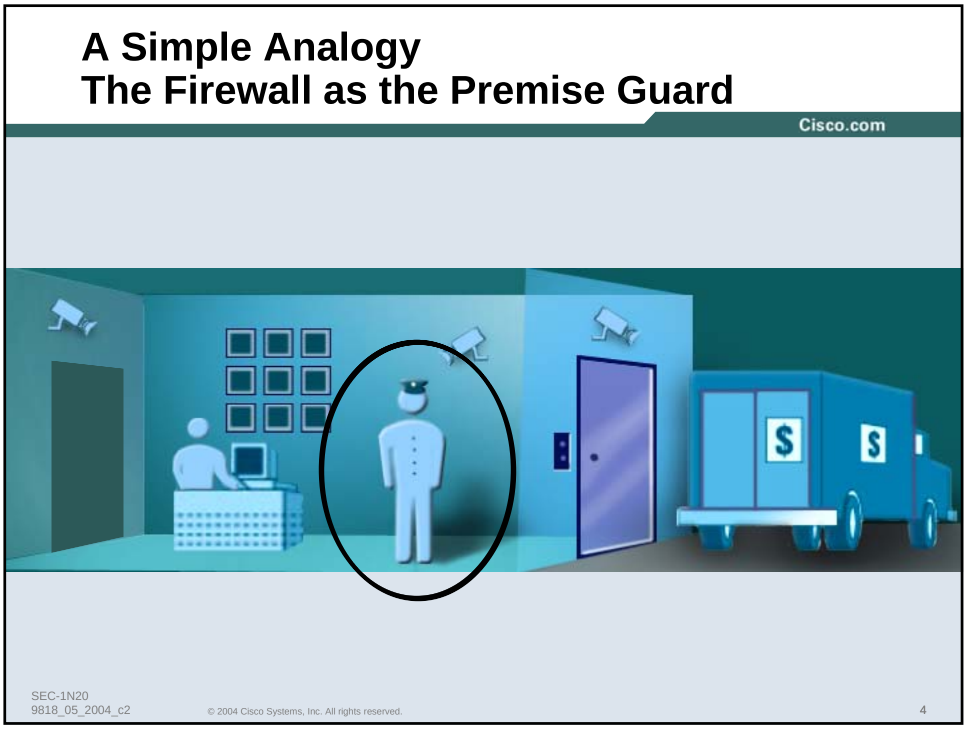
DMZ Network

Internet

Outside Network

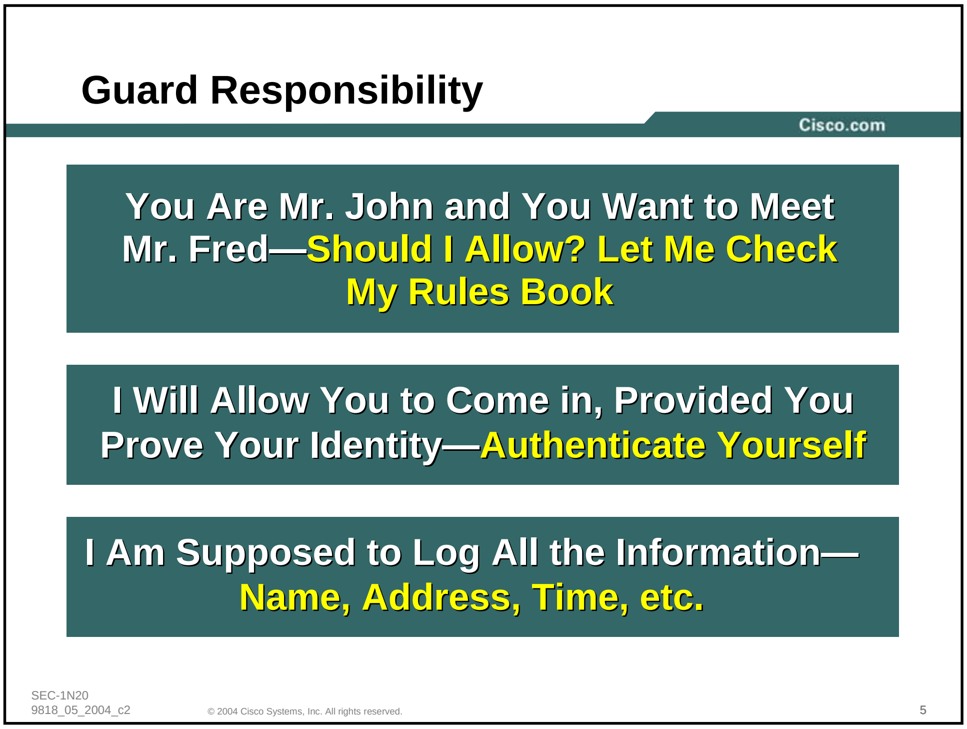
Inside Network

- A firewall is an access control device that looks at the IP packet, compares with policy rules and decides whether to allow, deny or take some other action on the packet



A Simple Analogy
The Firewall as the Premise Guard

Cisco.com



Guard Responsibility

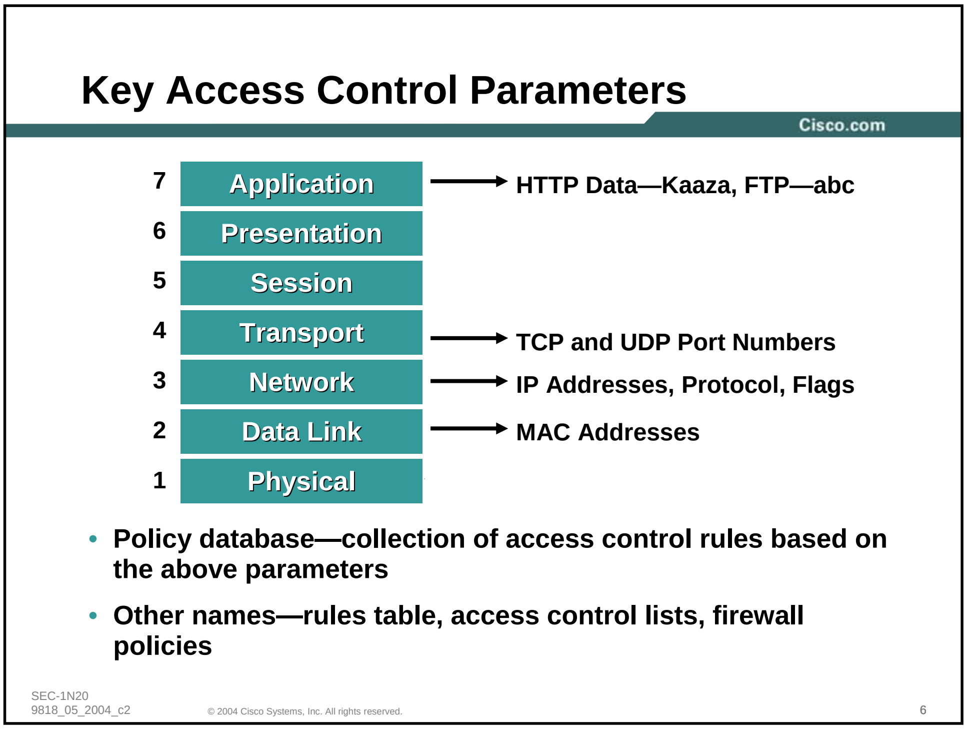
Cisco.com

You Are Mr. John and You Want to Meet Mr. Fred—**Should I Allow? Let Me Check My Rules Book**

I Will Allow You to Come in, Provided You Prove Your Identity—**Authenticate Yourself**

I Am Supposed to Log All the Information—**Name, Address, Time, etc.**

SEC-1N20
9818_05_2004_c2



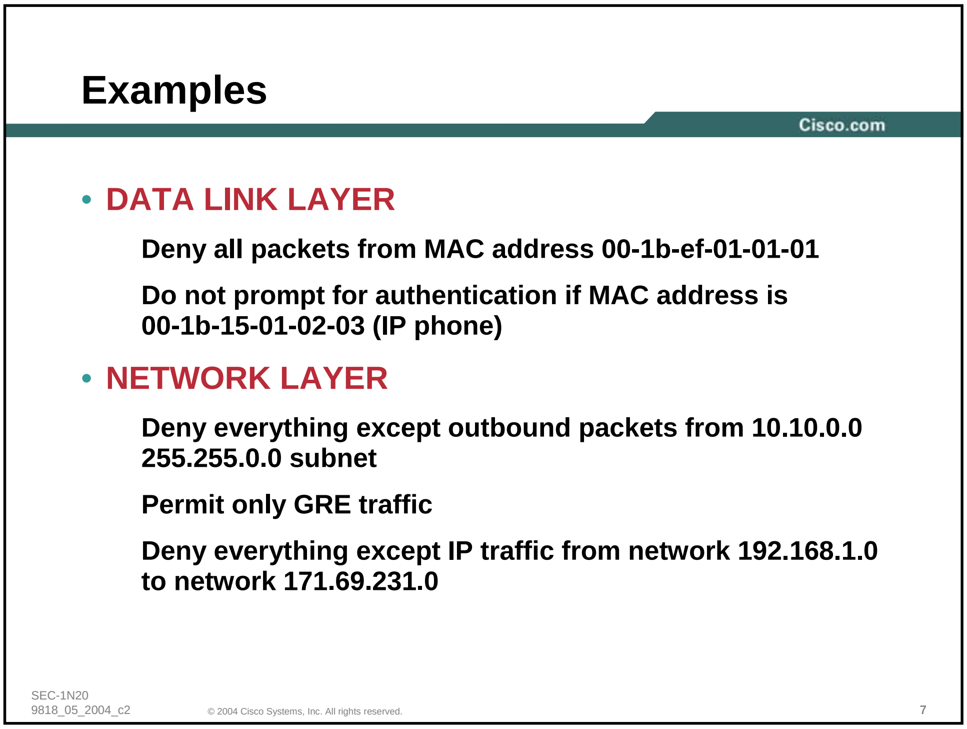
Key Access Control Parameters

Cisco.com

7	Application	→ HTTP Data—Kaaza, FTP—abc
6	Presentation	
5	Session	
4	Transport	→ TCP and UDP Port Numbers
3	Network	→ IP Addresses, Protocol, Flags
2	Data Link	→ MAC Addresses
1	Physical	

- Policy database—collection of access control rules based on the above parameters
- Other names—rules table, access control lists, firewall policies

SEC-1N20
9818_05_2004_c2



Examples

- DATA LINK LAYER

  Deny all packets from MAC address 00-1b-ef-01-01-01

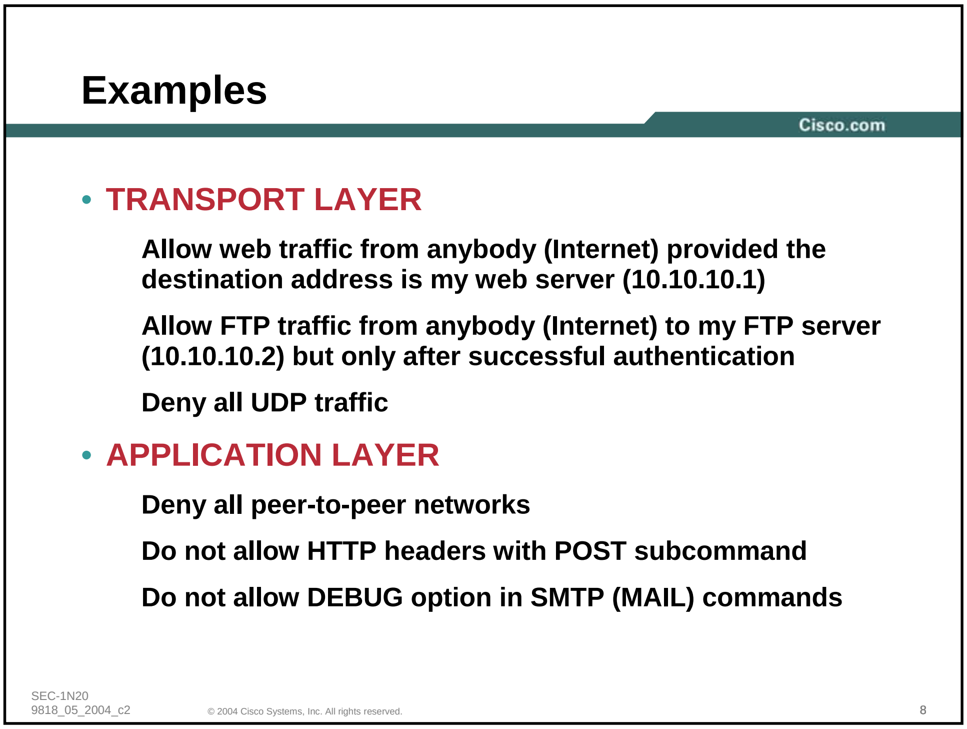
  Do not prompt for authentication if MAC address is 00-1b-15-01-02-03 (IP phone)

- NETWORK LAYER

  Deny everything except outbound packets from 10.10.0.0 255.255.0.0 subnet

  Permit only GRE traffic

  Deny everything except IP traffic from network 192.168.1.0 to network 171.69.231.0



Examples

- TRANSPORT LAYER

  Allow web traffic from anybody (Internet) provided the destination address is my web server (10.10.10.1)

  Allow FTP traffic from anybody (Internet) to my FTP server (10.10.10.2) but only after successful authentication

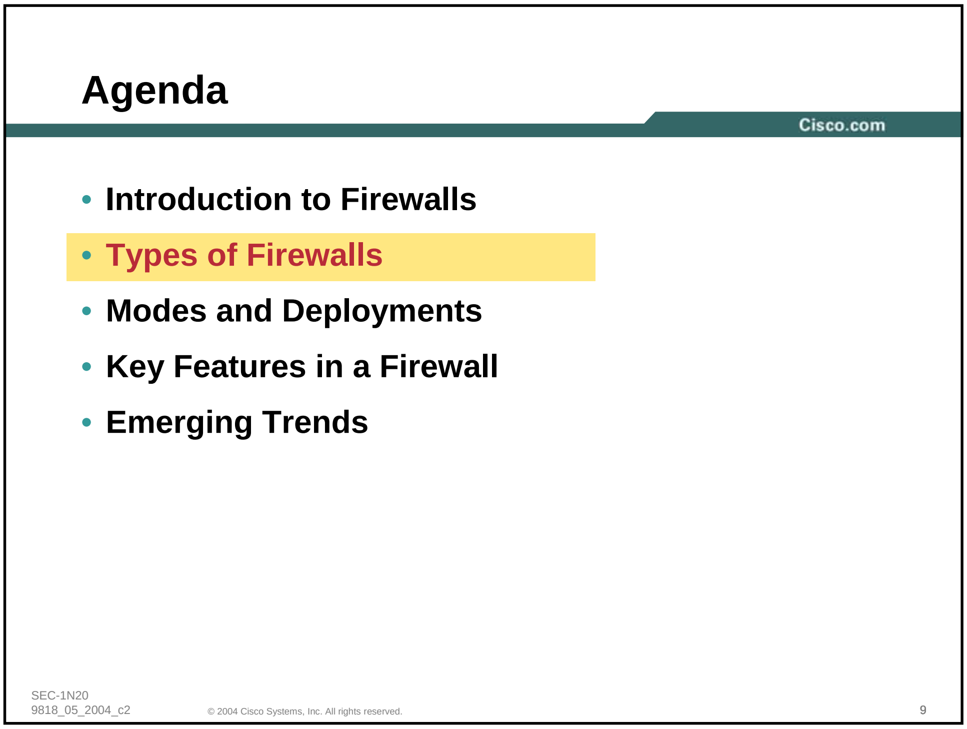
  Deny all UDP traffic

- APPLICATION LAYER

  Deny all peer-to-peer networks

  Do not allow HTTP headers with POST subcommand

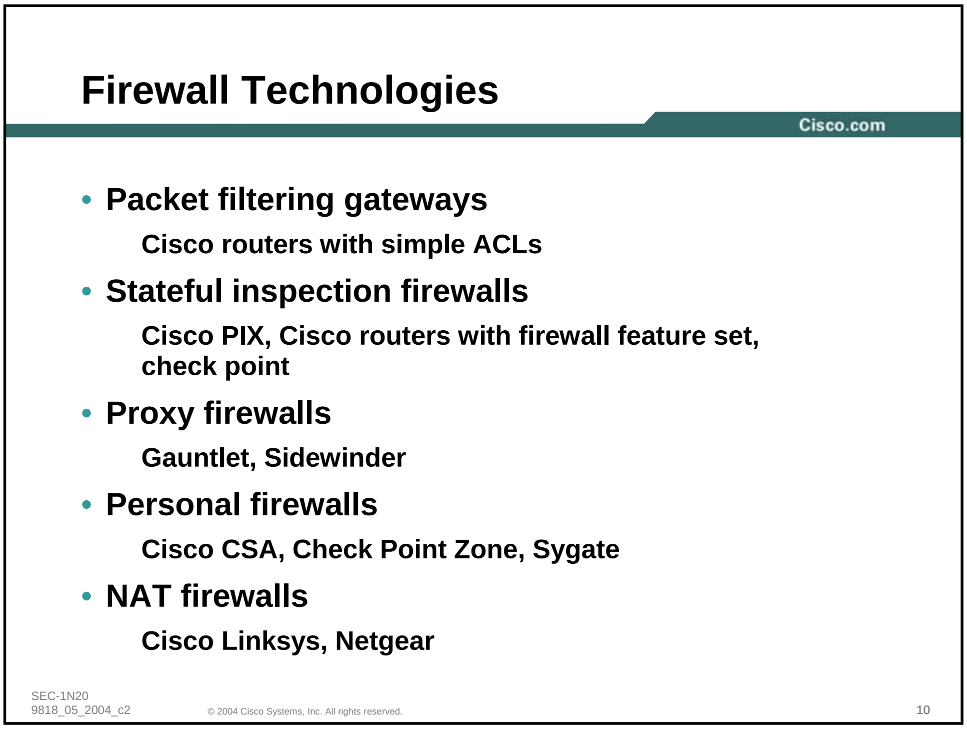
  Do not allow DEBUG option in SMTP (MAIL) commands



Agenda

Cisco.com

- Introduction to Firewalls
- Types of Firewalls
- Modes and Deployments
- Key Features in a Firewall
- Emerging Trends



Firewall Technologies

Cisco.com

- Packet filtering gateways

  Cisco routers with simple ACLs

- Stateful inspection firewalls

  Cisco PIX, Cisco routers with firewall feature set, check point

- Proxy firewalls

  Gauntlet, Sidewinder

- Personal firewalls

  Cisco CSA, Check Point Zone, Sygate

- NAT firewalls

  Cisco Linksys, Netgear

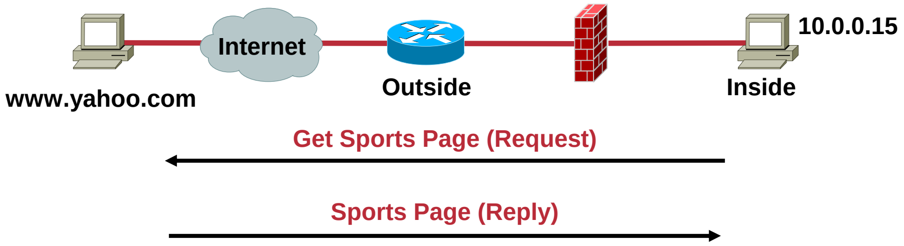
Packet Filtering Gateways

Cisco.com

- Drop/allow packets based on source or destination addresses or ports (some exceptions)
- No state information is maintained; decisions are made only from the content of the current packet
- Integrated feature in routers and switches
- High performance
- Fragmentation may cause a problem

Packet Filtering Gateways

Cisco.com



Stateless—Two Separate ACLs Are Required

1. Permit HTTP traffic from 10.0.0.0 to www.yahoo.com
2. Permit HTTP traffic from www.yahoo.com to 10.0.0.0

Stateful Inspection Firewalls

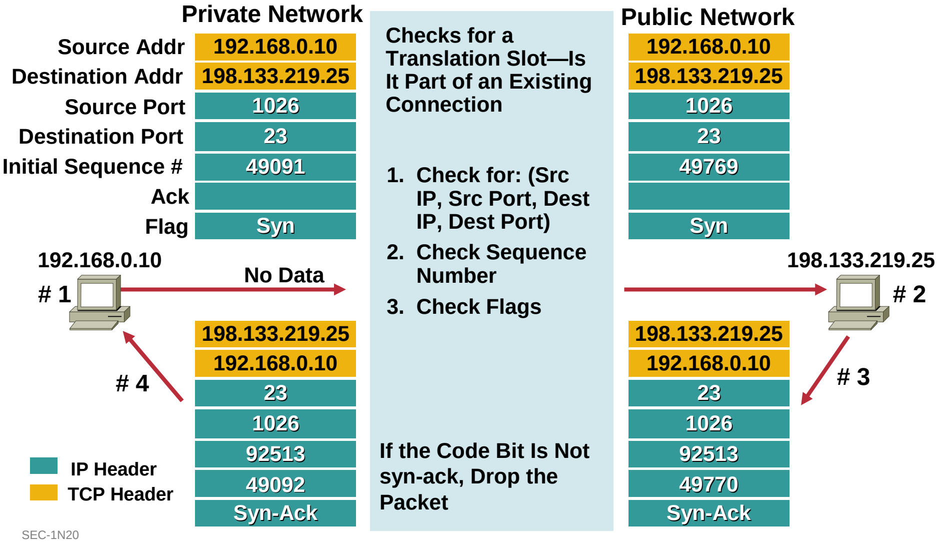
- Packet filtering gateways plus…
- Maintaining state

  Stateful firewalls inspect and maintain a record (a state table) of the state of each connection that passes through the firewall

  - To adequately maintain the state of a connection the firewall needs to inspect every packet
  - But short cuts can be made once a packet is identified as being part of an established connection
  - Different vendors record slightly different information about the state of a connection
- High performance and most popular

Example: Stateful Inspection of a TCP Connection

(A Connection-Oriented Reliable Protocol)



	Private Network	Public Network
Source Addr	192.168.0.10	192.168.0.10
Destination Addr	198.133.219.25	198.133.219.25
Source Port	1026	1026
Destination Port	23	23
Initial Sequence #	49091	49769
Ack		
Flag	Syn	Syn

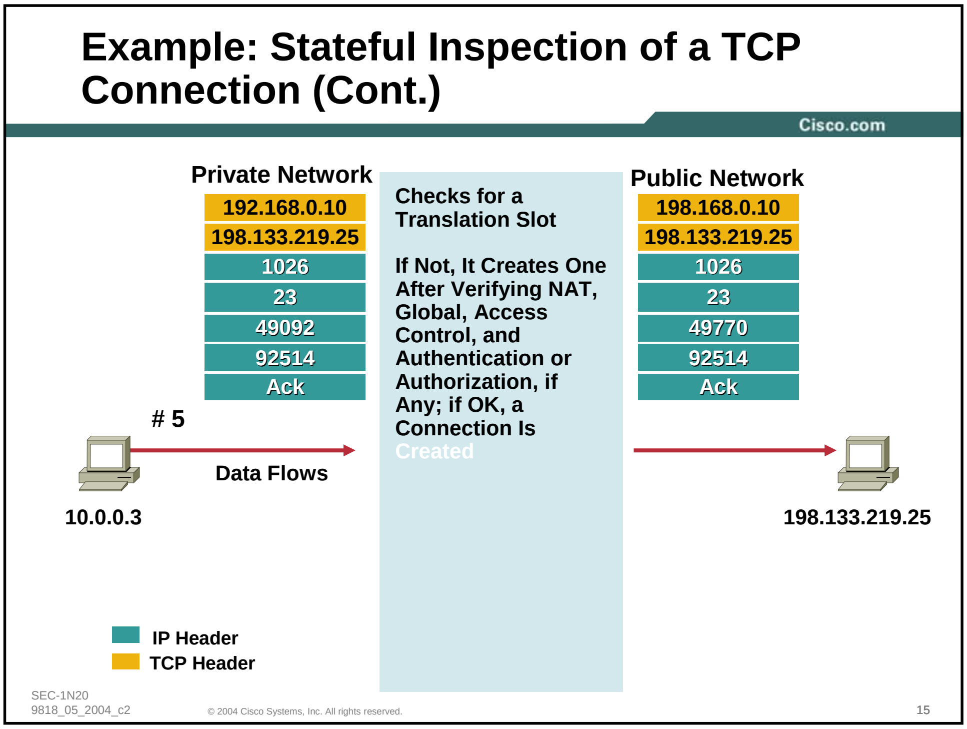
198.133.219.25	198.133.219.25
192.168.0.10	192.168.0.10
23	23
1026	1026
92513	92513
49092	49770
Syn-Ack	Syn-Ack

Checks for a Translation Slot—Is It Part of an Existing Connection

1. Check for: (Src IP, Src Port, Dest IP, Dest Port)
2. Check Sequence Number
3. Check Flags

If the Code Bit Is Not syn-ack, Drop the Packet

🟩 IP Header
🟨 TCP Header



Example: Stateful Inspection of a TCP Connection (Cont.)

Cisco.com

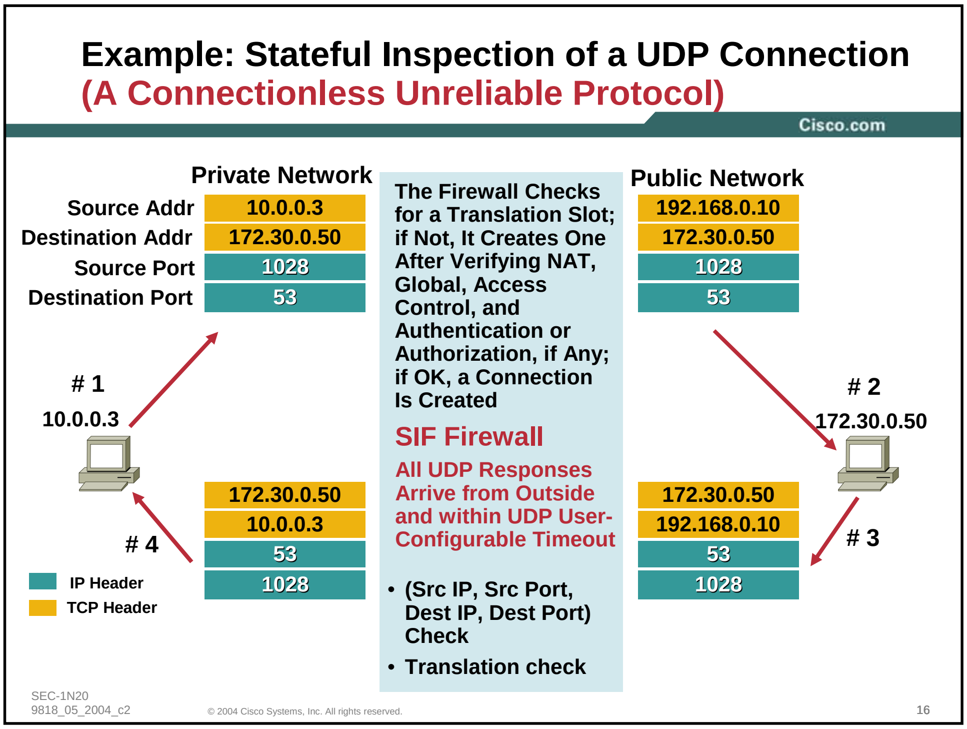
Private Network	Public Network
192.168.0.10	198.168.0.10
198.133.219.25	198.133.219.25
1026	1026
23	23
49092	49770
92514	92514
Ack	Ack

Checks for a Translation Slot

If Not, It Creates One After Verifying NAT, Global, Access Control, and Authentication or Authorization, if Any; if OK, a Connection Is Created

🟩 IP Header
🟨 TCP Header

SEC-1N20
9818_05_2004_c2



Example: Stateful Inspection of a UDP Connection (A Connectionless Unreliable Protocol)

Cisco.com

	Private Network	Public Network
Source Addr	10.0.0.3	192.168.0.10
Destination Addr	172.30.0.50	172.30.0.50
Source Port	1028	1028
Destination Port	53	53

The Firewall Checks for a Translation Slot; if Not, It Creates One After Verifying NAT, Global, Access Control, and Authentication or Authorization, if Any; if OK, a Connection Is Created

SIF Firewall

All UDP Responses Arrive from Outside and within UDP User-Configurable Timeout

- (Src IP, Src Port, Dest IP, Dest Port) Check
- Translation check

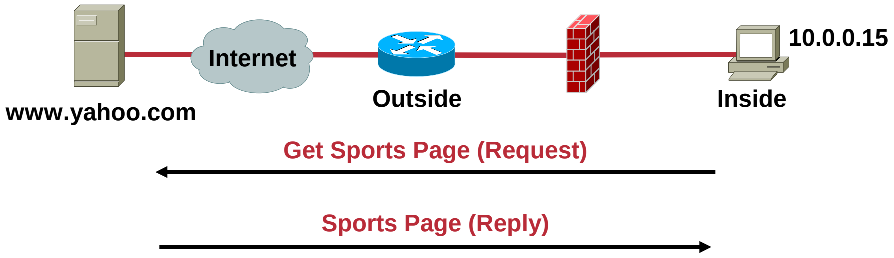
Private Network	Public Network
172.30.0.50	172.30.0.50
10.0.0.3	192.168.0.10
53	53
1028	1028

🟩 IP Header
🟨 TCP Header

SEC-1N20
9818_05_2004_c2

Stateful Inspection Firewalls

Cisco.com

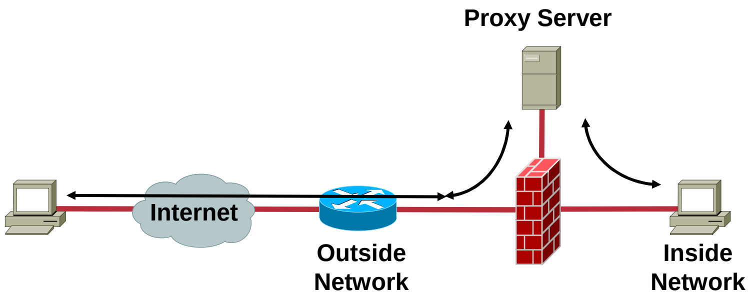


Stateful—Only One ACL Is Required

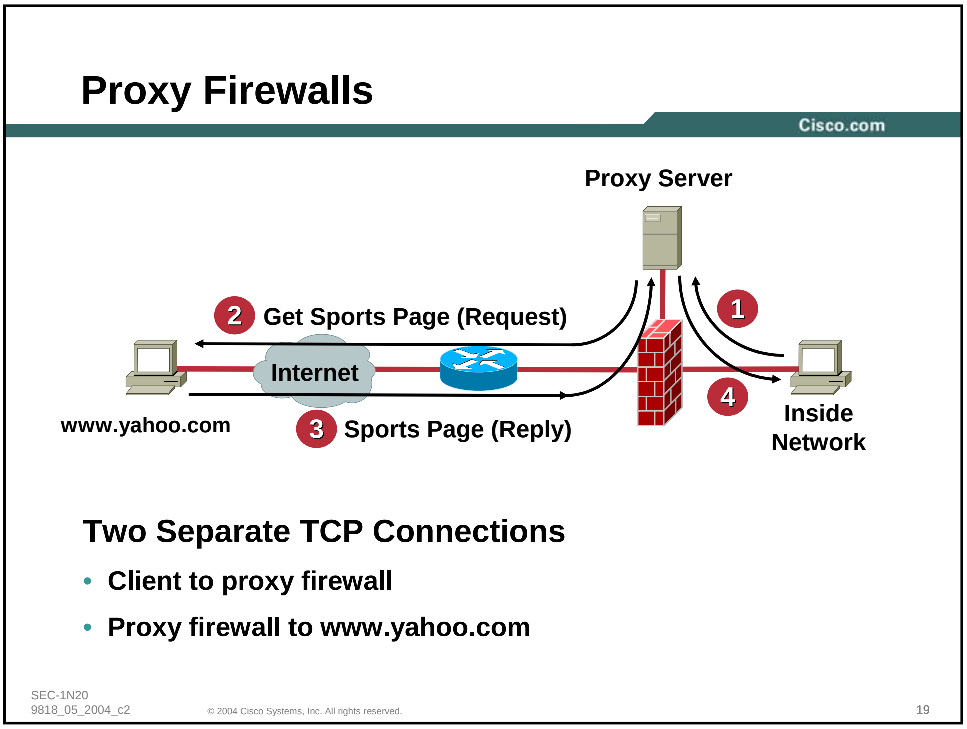
1. Permit HTTP traffic from 10.0.0.0 to www.yahoo.com

Proxy Firewalls

Cisco.com



- All requests and replies pass though a proxy server; no direct connection between a client and the server; everything is proxied—thus the name



Proxy Firewalls

Proxy Server

2 Get Sports Page (Request)

Internet

1

4

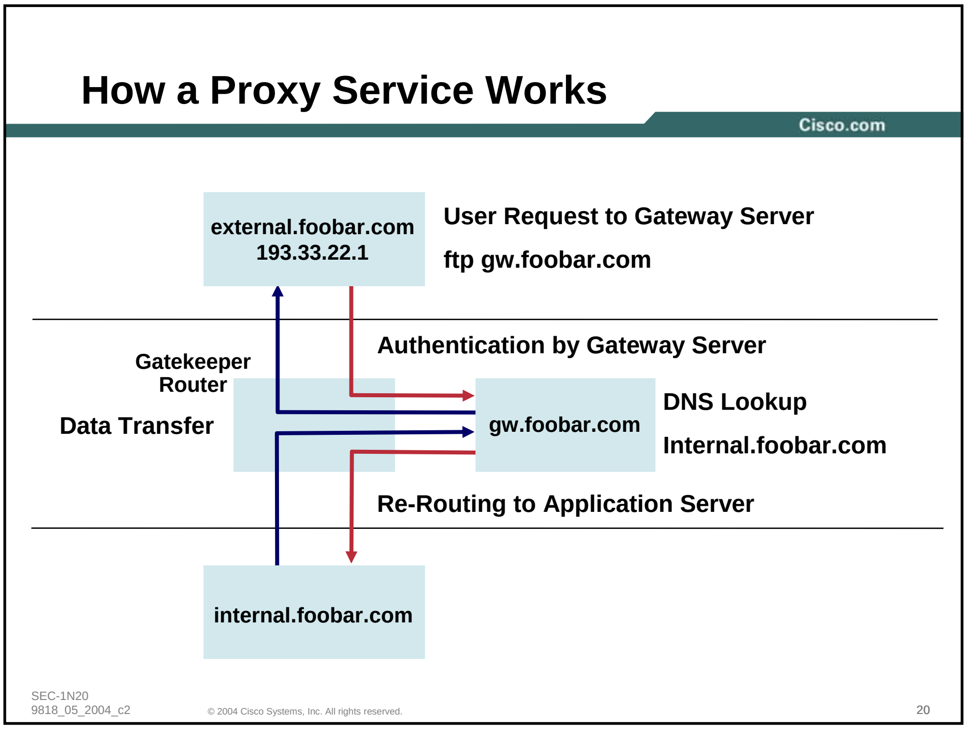
www.yahoo.com

3 Sports Page (Reply)

Inside Network

Two Separate TCP Connections

- Client to proxy firewall
- Proxy firewall to www.yahoo.com



How a Proxy Service Works

external.foobar.com
193.33.22.1

User Request to Gateway Server

ftp gw.foobar.com

Authentication by Gateway Server

Gatekeeper
Router

Data Transfer

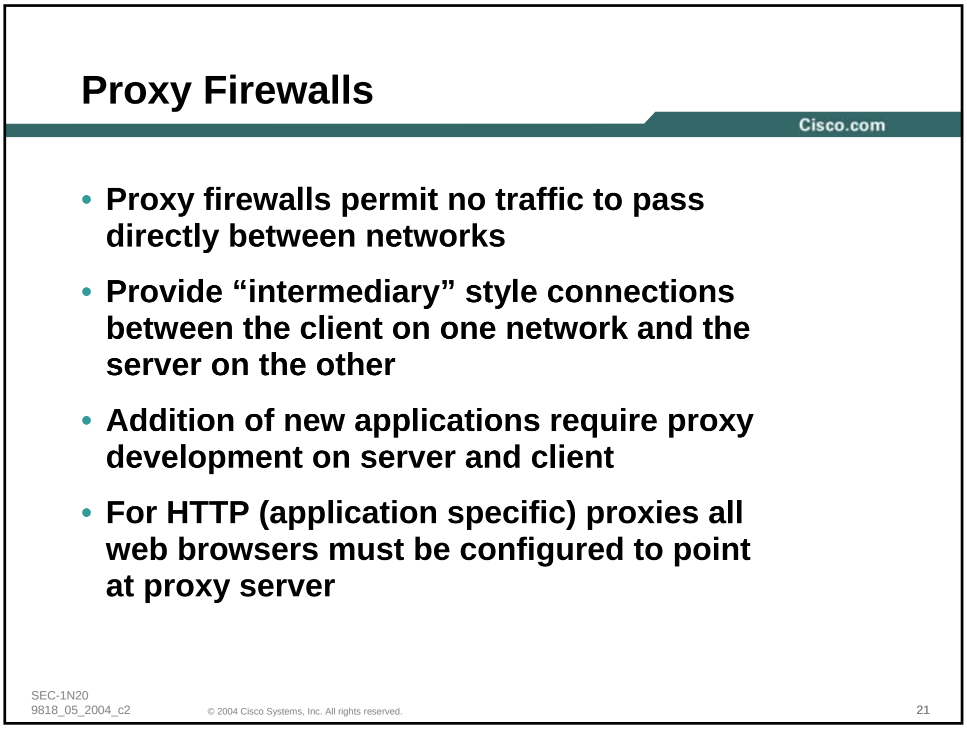
gw.foobar.com

DNS Lookup

Internal.foobar.com

Re-Routing to Application Server

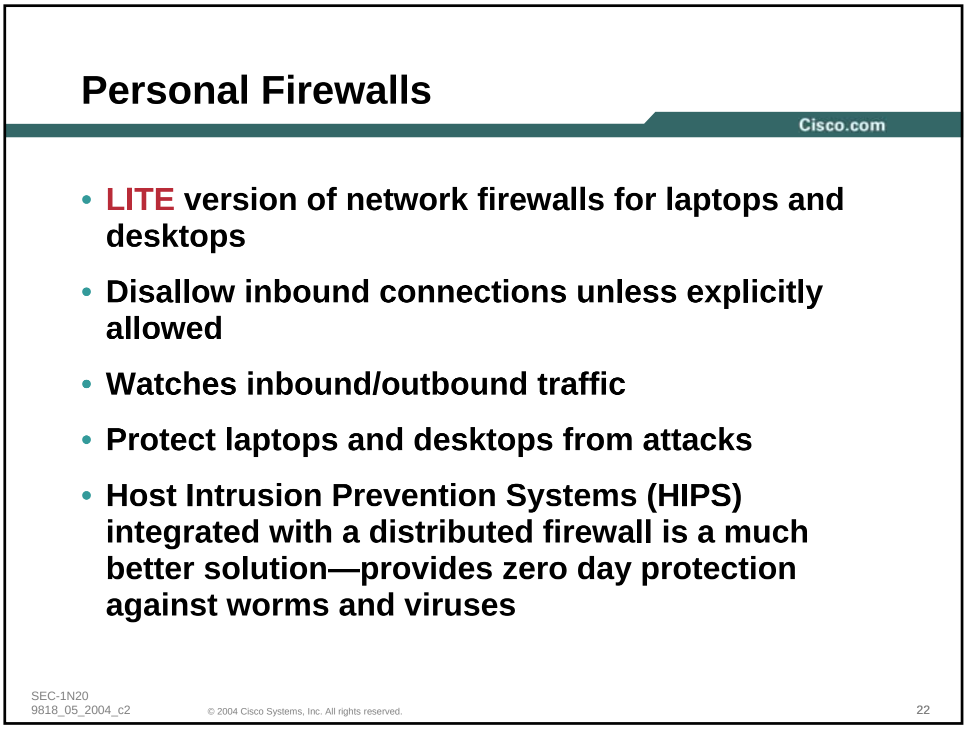
internal.foobar.com



Proxy Firewalls

Cisco.com

- Proxy firewalls permit no traffic to pass directly between networks
- Provide “intermediary” style connections between the client on one network and the server on the other
- Addition of new applications require proxy development on server and client
- For HTTP (application specific) proxies all web browsers must be configured to point at proxy server

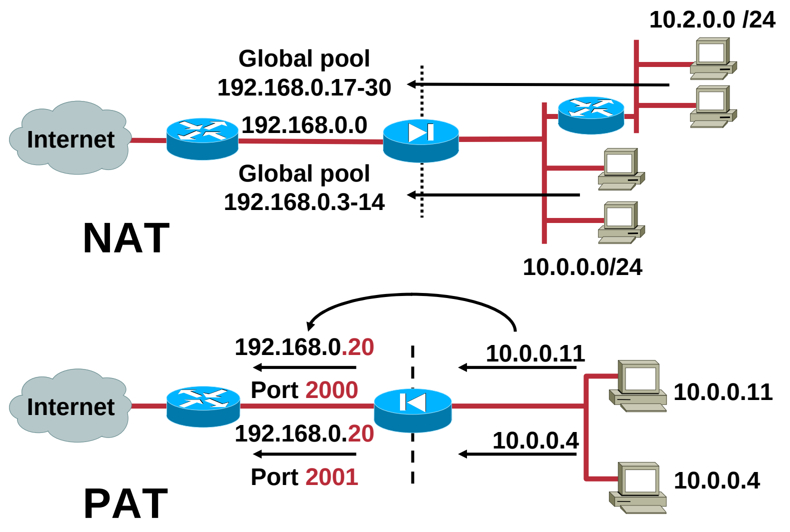


Personal Firewalls

Cisco.com

- LITE version of network firewalls for laptops and desktops
- Disallow inbound connections unless explicitly allowed
- Watches inbound/outbound traffic
- Protect laptops and desktops from attacks
- Host Intrusion Prevention Systems (HIPS) integrated with a distributed firewall is a much better solution—provides zero day protection against worms and viruses

NAT/PAT Firewalls: Concept



10.2.0.0 /24

Global pool
192.168.0.17-30

Internet

192.168.0.0

Global pool
192.168.0.3-14

NAT

10.0.0.0/24

192.168.0.20
Port 2000

10.0.0.11

Internet

10.0.0.11

192.168.0.20
Port 2001

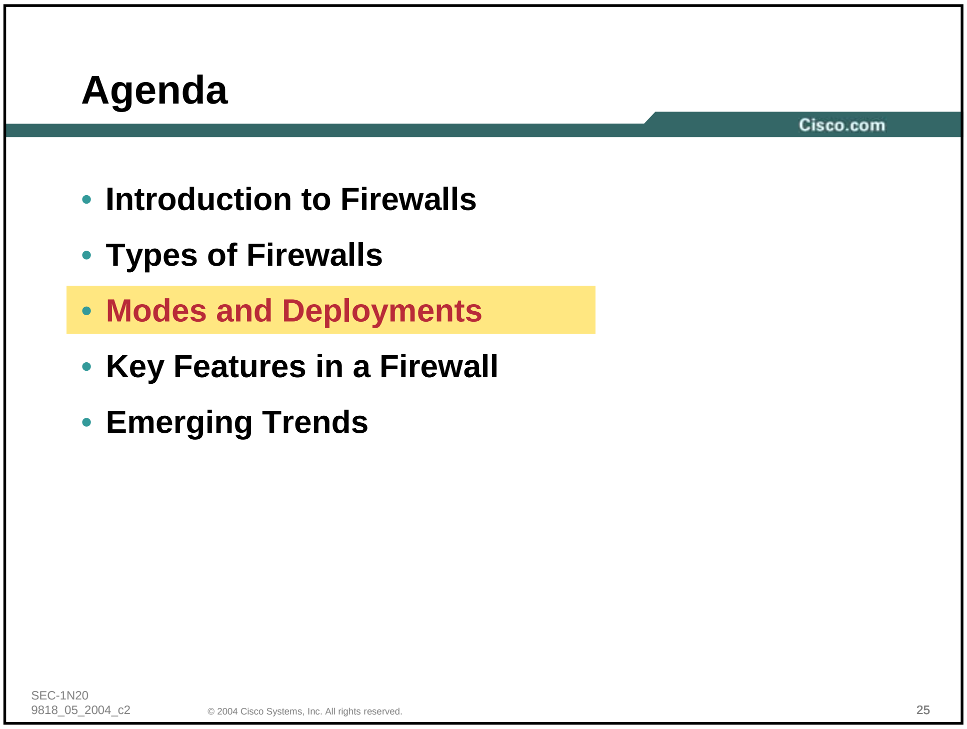
10.0.0.4

10.0.0.4

PAT

NAT Firewalls

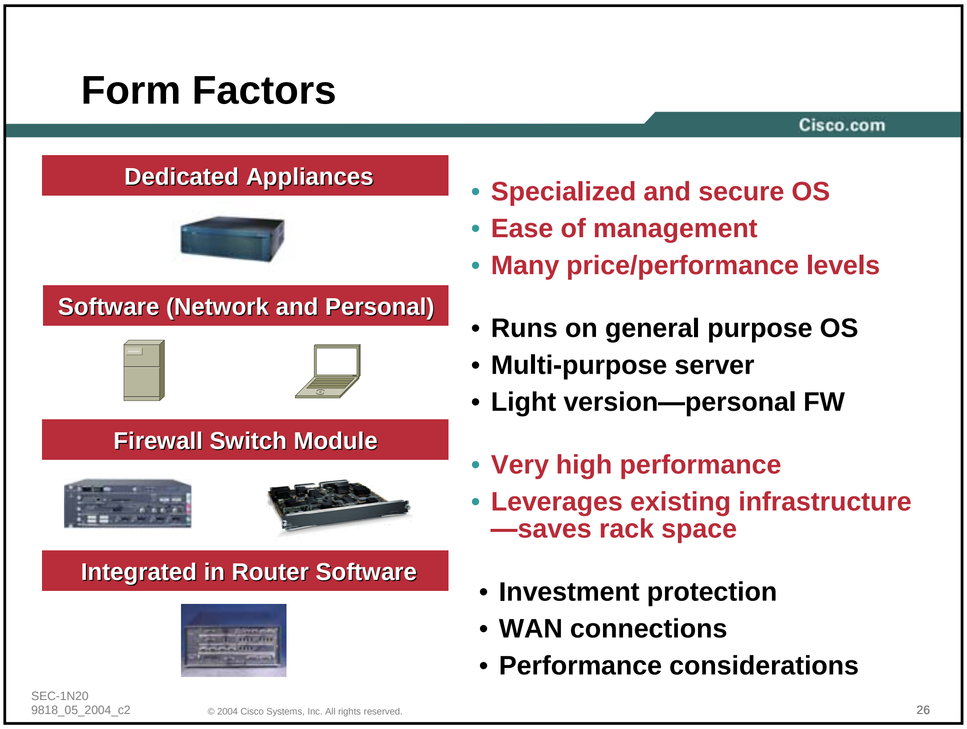
- NAT Firewalls hide all internal addresses—thus protect small networks from external attacks as internal addresses are not exposed
- May offer minimal stateful inspection and basic VPN
- A full fledged stateful firewall is much powerful then basic NAT firewalls



Agenda

Cisco.com

- Introduction to Firewalls
- Types of Firewalls
- Modes and Deployments
- Key Features in a Firewall
- Emerging Trends



Form Factors

Cisco.com

Dedicated Appliances

- Specialized and secure OS
- Ease of management
- Many price/performance levels

Software (Network and Personal)

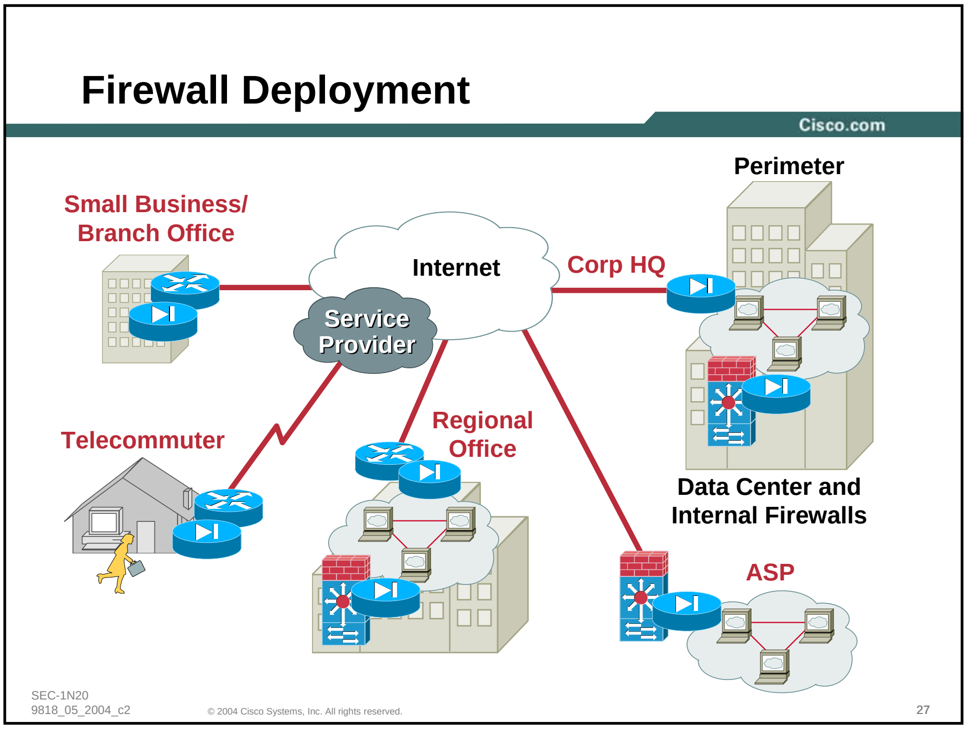
- Runs on general purpose OS
- Multi-purpose server
- Light version—personal FW

Firewall Switch Module

- Very high performance
- Leverages existing infrastructure —saves rack space

Integrated in Router Software

- Investment protection
- WAN connections
- Performance considerations



Firewall Deployment

Cisco.com

Perimeter

Small Business/
Branch Office

Internet

Service
Provider

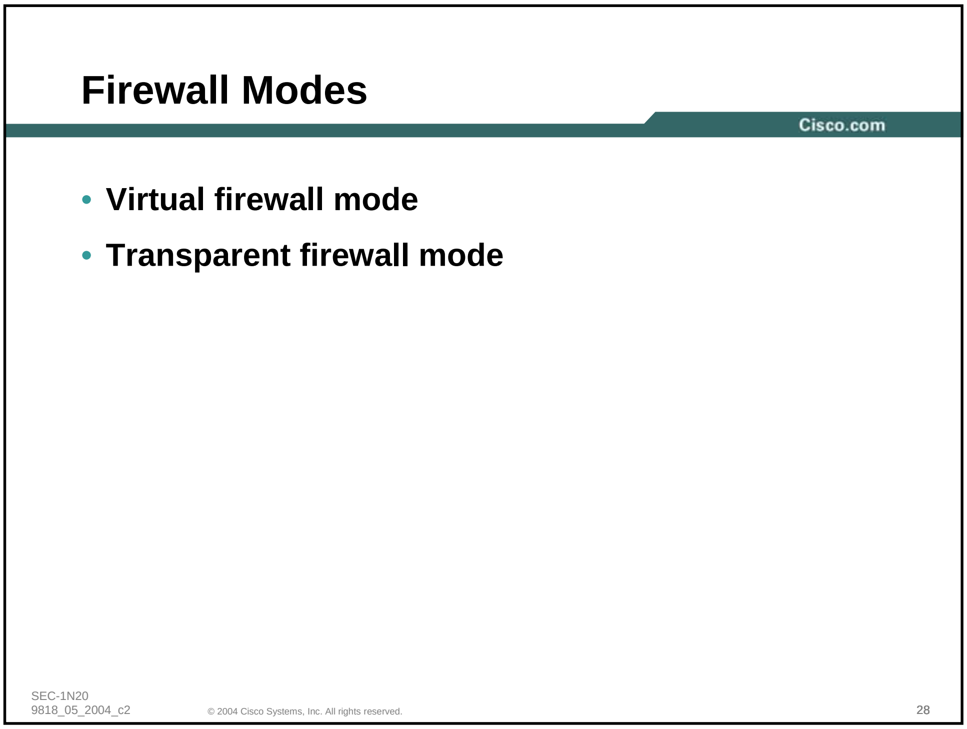
Corp HQ

Telecommuter

Regional
Office

Data Center and
Internal Firewalls

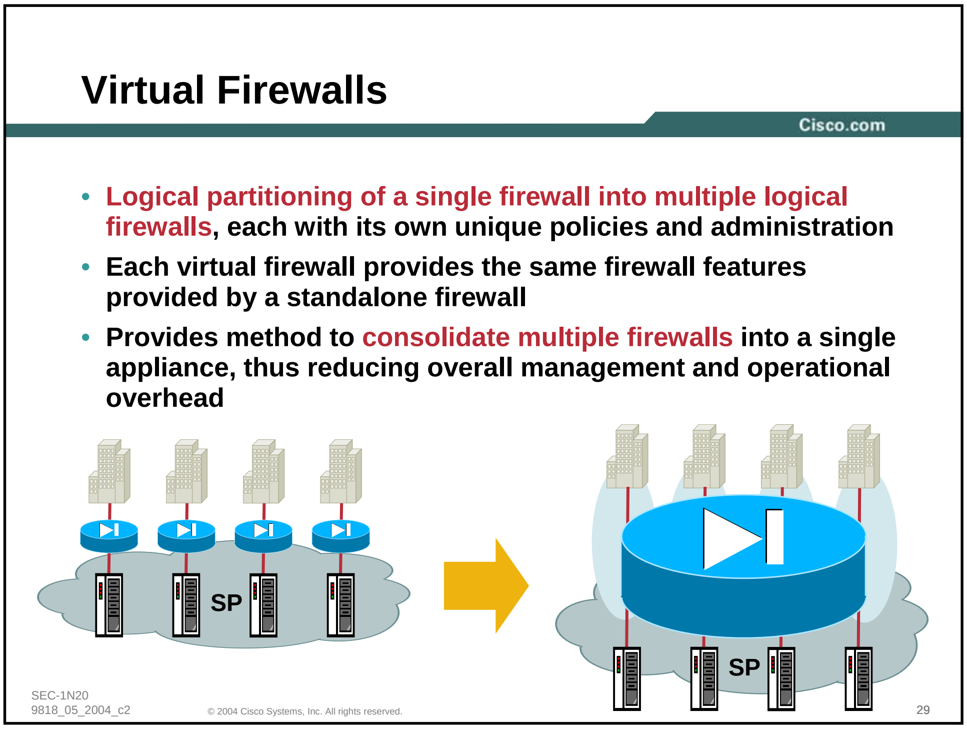
ASP



Firewall Modes

Cisco.com

- Virtual firewall mode
- Transparent firewall mode

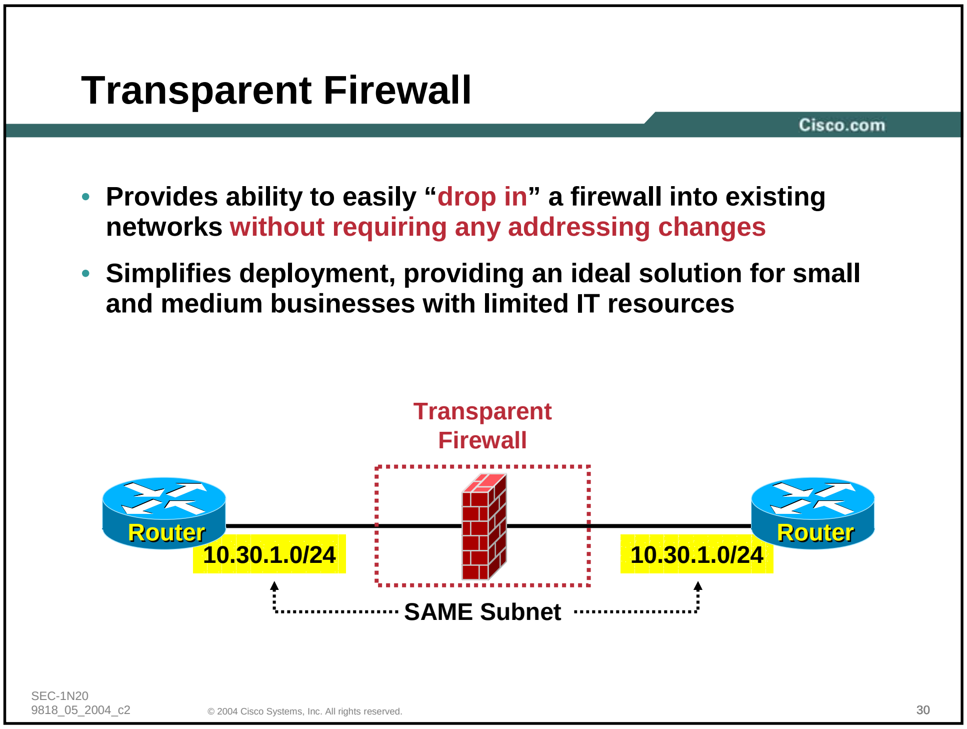


Virtual Firewalls

Cisco.com

- Logical partitioning of a single firewall into multiple logical firewalls, each with its own unique policies and administration
- Each virtual firewall provides the same firewall features provided by a standalone firewall
- Provides method to consolidate multiple firewalls into a single appliance, thus reducing overall management and operational overhead

SEC-1N20
9818_05_2004_c2

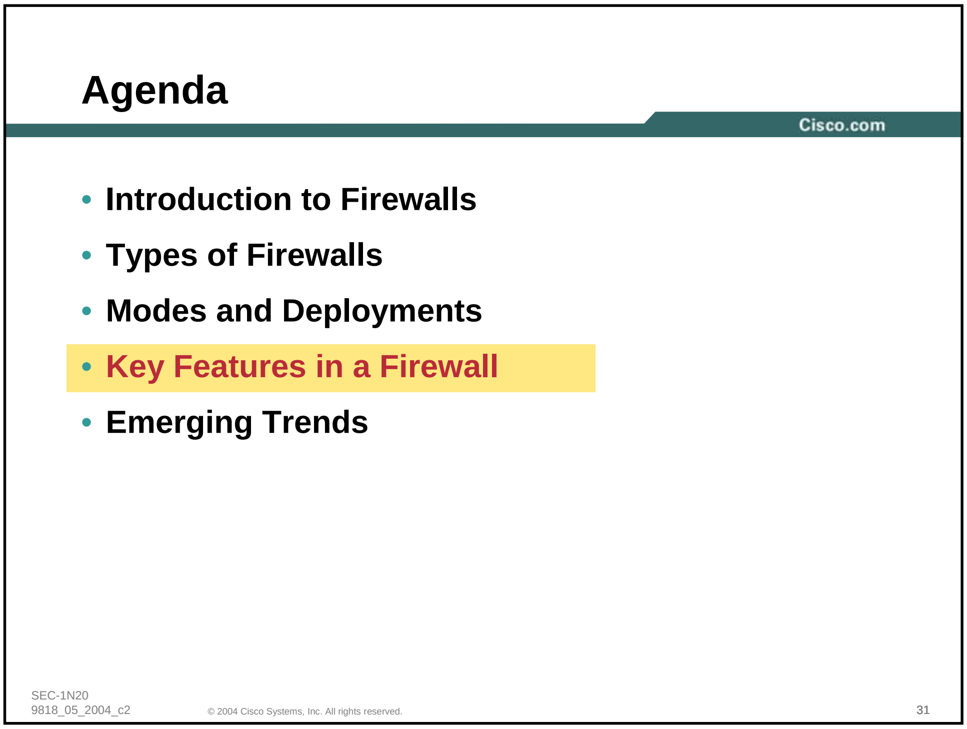


Transparent Firewall

Cisco.com

- Provides ability to easily “drop in” a firewall into existing networks without requiring any addressing changes
- Simplifies deployment, providing an ideal solution for small and medium businesses with limited IT resources

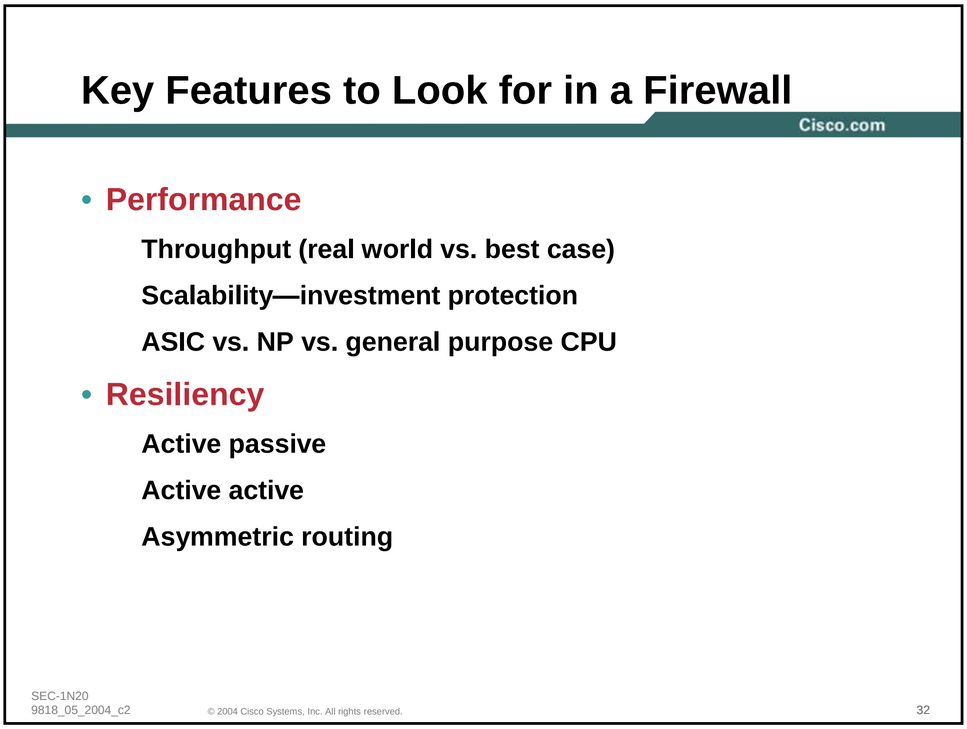
SEC-1N20
9818_05_2004_c2



Agenda

Cisco.com

- Introduction to Firewalls
- Types of Firewalls
- Modes and Deployments
- Key Features in a Firewall
- Emerging Trends



Key Features to Look for in a Firewall

Cisco.com

- Performance

  Throughput (real world vs. best case)

  Scalability—investment protection

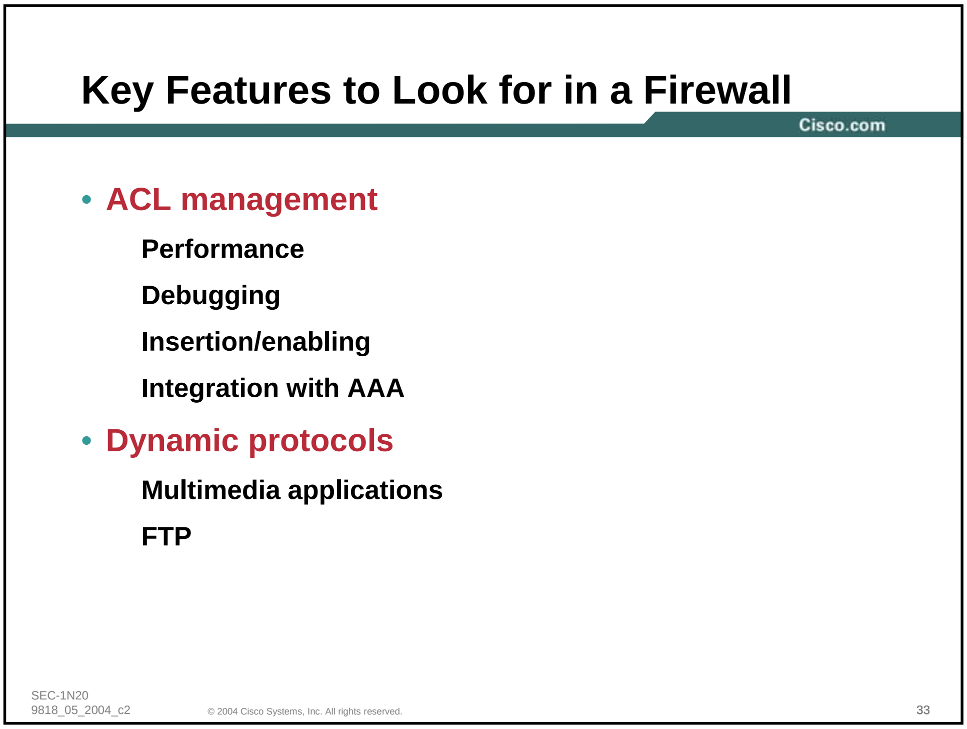
  ASIC vs. NP vs. general purpose CPU

- Resiliency

  Active passive

  Active active

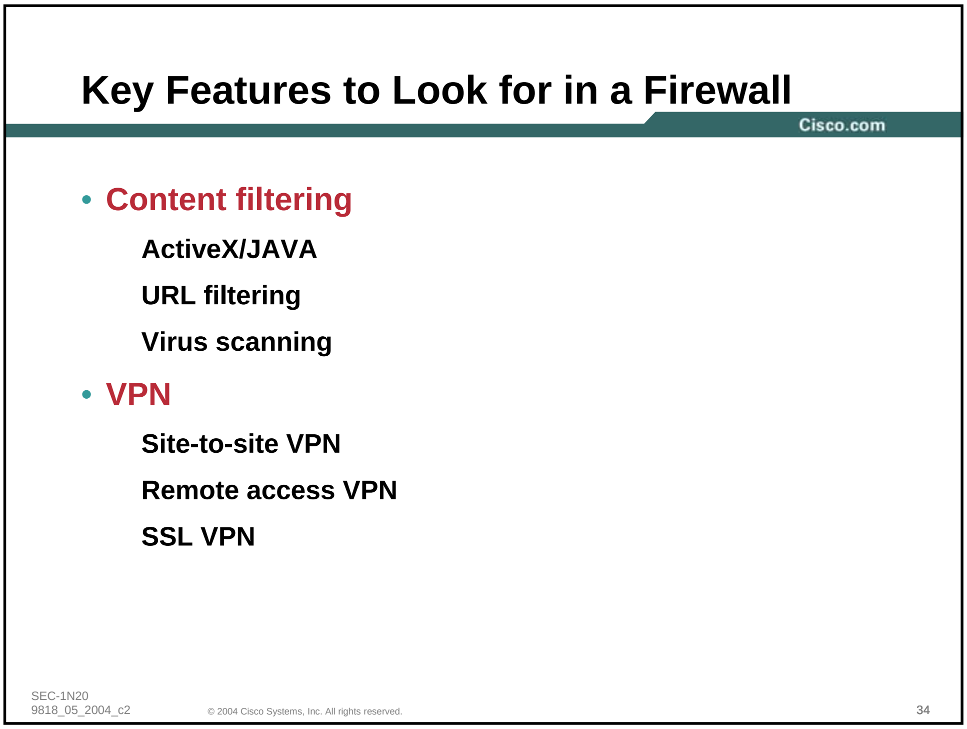
  Asymmetric routing



Key Features to Look for in a Firewall

Cisco.com

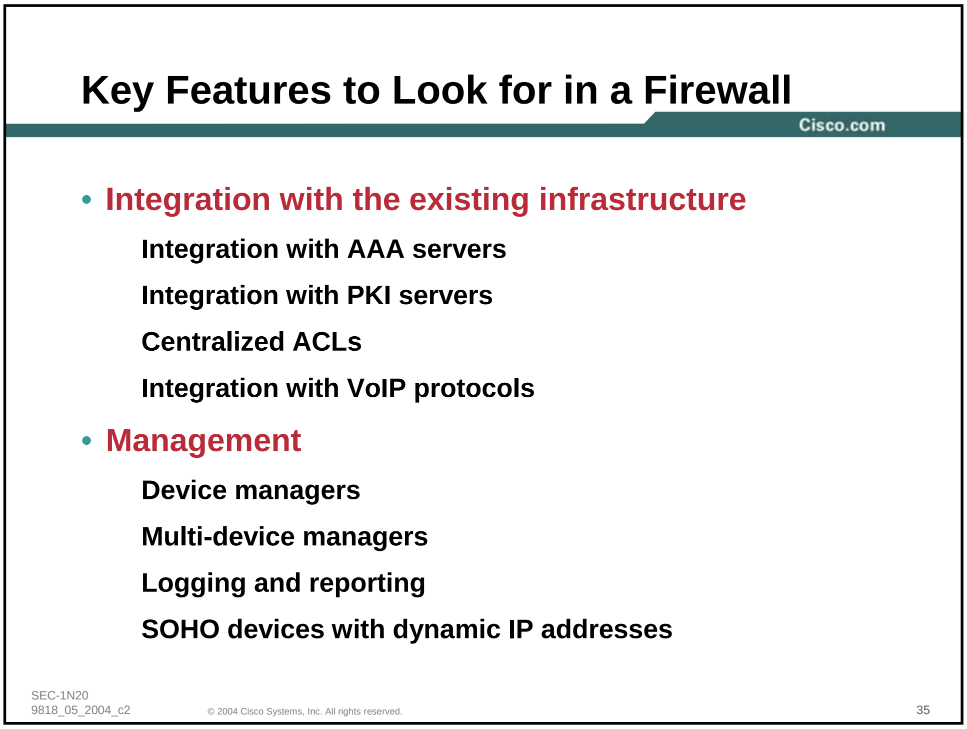
- ACL management
  - Performance
  - Debugging
  - Insertion/enabling
  - Integration with AAA
- Dynamic protocols
  - Multimedia applications
  - FTP



Key Features to Look for in a Firewall

Cisco.com

- Content filtering
  - ActiveX/JAVA
  - URL filtering
  - Virus scanning
- VPN
  - Site-to-site VPN
  - Remote access VPN
  - SSL VPN



Key Features to Look for in a Firewall

Cisco.com

- Integration with the existing infrastructure

  Integration with AAA servers

  Integration with PKI servers

  Centralized ACLs

  Integration with VoIP protocols

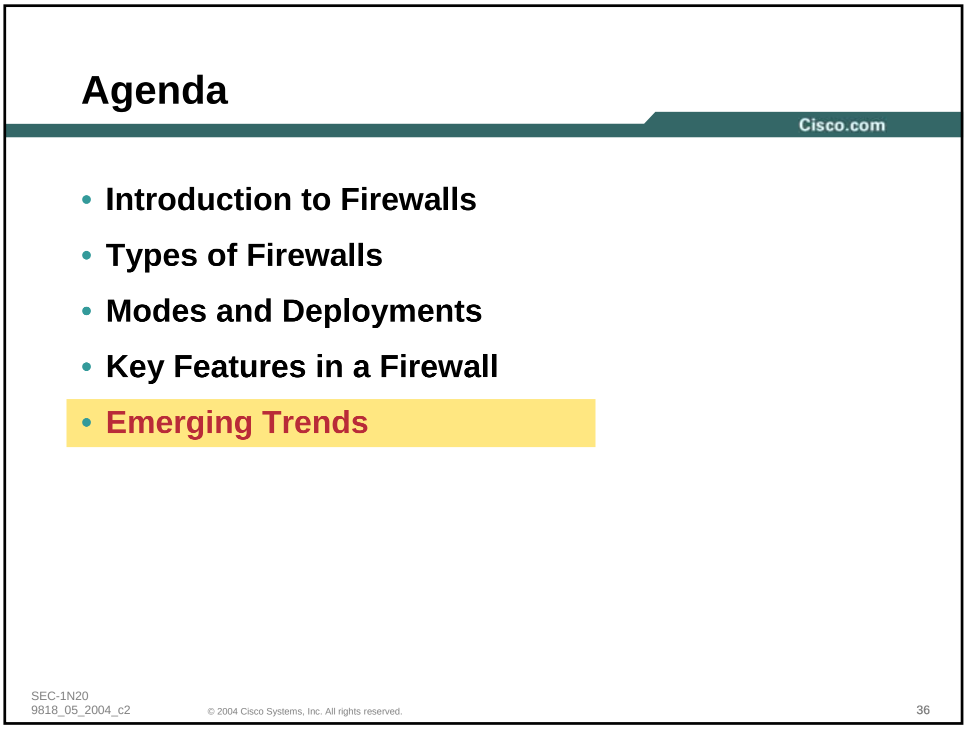
- Management

  Device managers

  Multi-device managers

  Logging and reporting

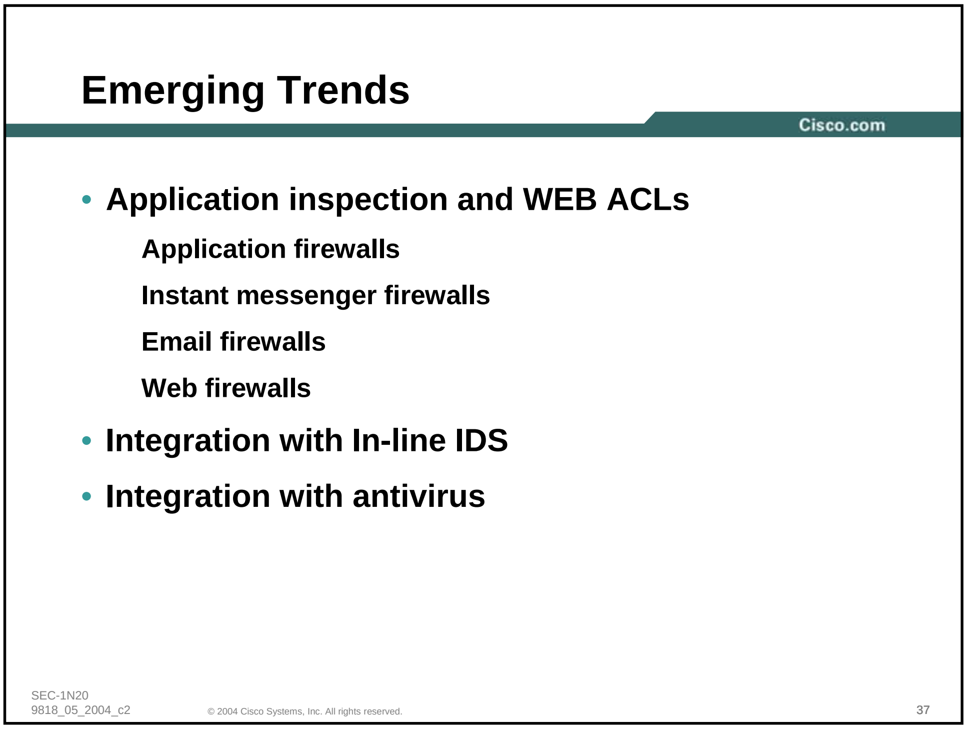
  SOHO devices with dynamic IP addresses



Agenda

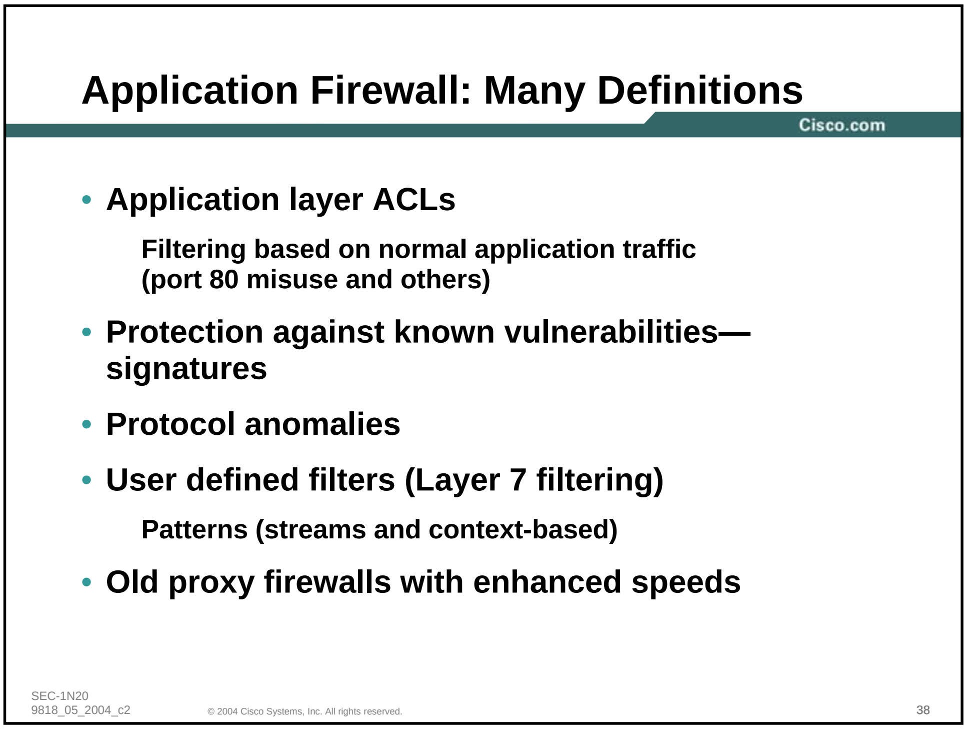
Cisco.com

- Introduction to Firewalls
- Types of Firewalls
- Modes and Deployments
- Key Features in a Firewall
- Emerging Trends



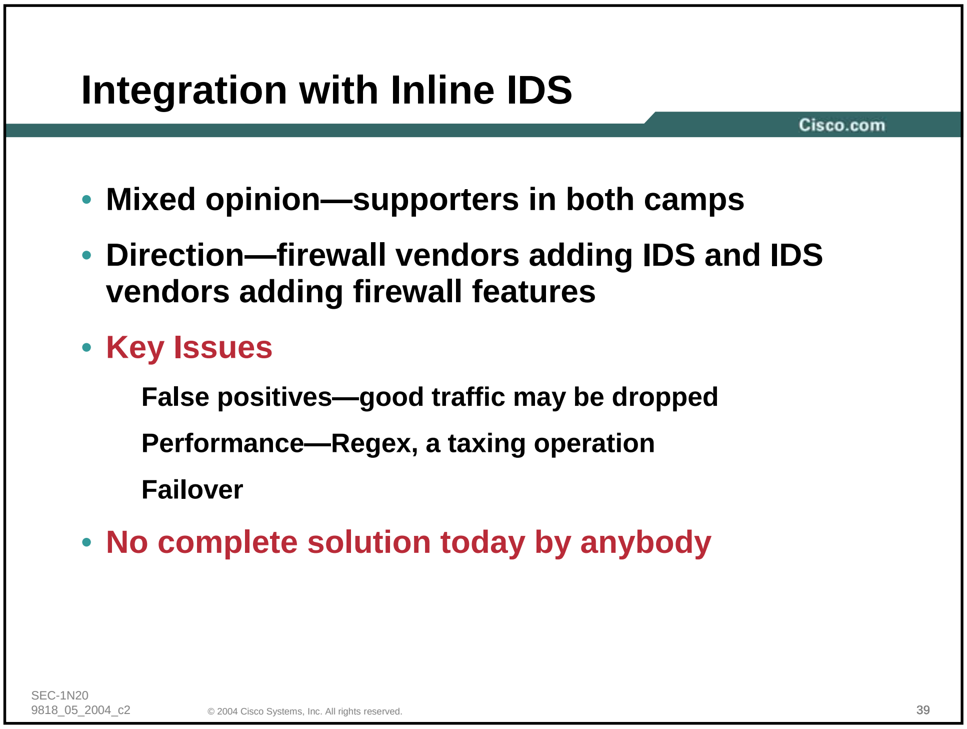
Emerging Trends

- Application inspection and WEB ACLs
  - Application firewalls
  - Instant messenger firewalls
  - Email firewalls
  - Web firewalls
- Integration with In-line IDS
- Integration with antivirus



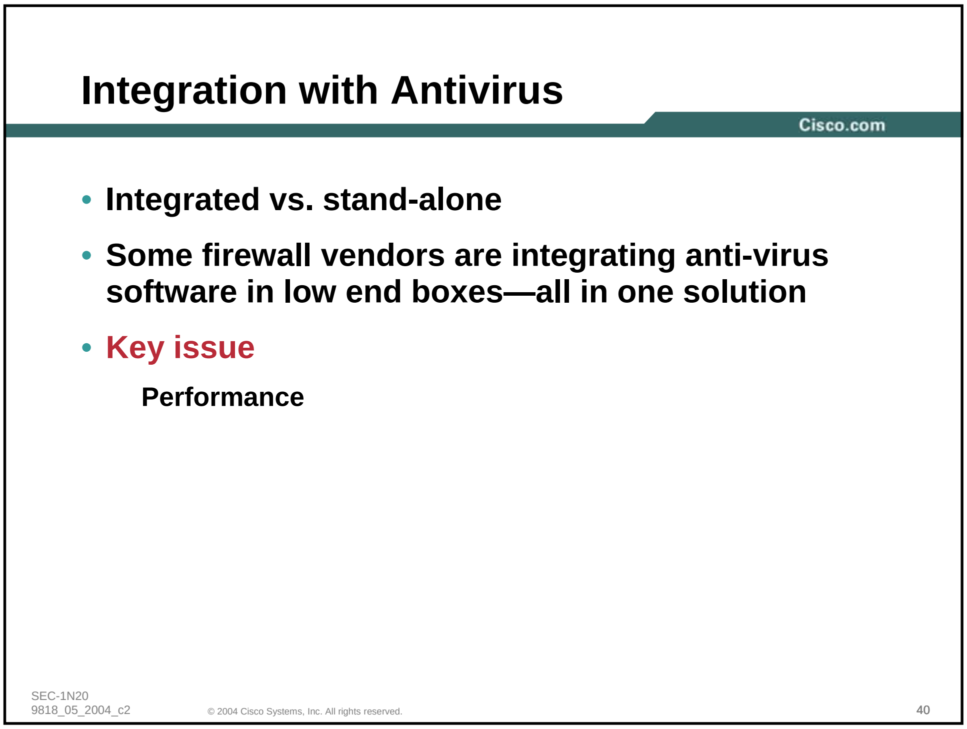
Application Firewall: Many Definitions

- Application layer ACLs
  - Filtering based on normal application traffic (port 80 misuse and others)
- Protection against known vulnerabilities—signatures
- Protocol anomalies
- User defined filters (Layer 7 filtering)
  - Patterns (streams and context-based)
- Old proxy firewalls with enhanced speeds



Integration with Inline IDS

- Mixed opinion—supporters in both camps
- Direction—firewall vendors adding IDS and IDS vendors adding firewall features
- Key Issues
  - False positives—good traffic may be dropped
  - Performance—Regex, a taxing operation
  - Failover
- No complete solution today by anybody



Integration with Antivirus

- Integrated vs. stand-alone
- Some firewall vendors are integrating anti-virus software in low end boxes—all in one solution
- Key issue
  - Performance

THANK YOU

CISCO SYSTEMS ®