



Agenda

- **Introduction**

Definition and Deployment

- **Product Updates**

Cisco IOS® Firewall

Cisco PIX™ Firewall

Cisco VPN Client

1303
0955_05F9_c2 © 1999, Cisco Systems, Inc.

www.cisco.com

3



Introduction

1303
0955_05F9_c2 © 1999, Cisco Systems, Inc.

4

What Is a Firewall?



- All traffic from inside to outside and vice-versa must pass through the firewall
- Only authorized traffic, as defined by the local security policy, will be allowed in
- The firewall itself is immune to penetration*

* Bellovin and Cheswick "Firewalls and Internet Security, Repelling the Wily Hacker"

1303
0955_05F9_c2

© 1999, Cisco Systems, Inc.

www.cisco.com

5

Network Security Elements

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

Cisco IOS™



1303
0955_05F9_c2

© 1999, Cisco Systems, Inc.

www.cisco.com

6

Existing Cisco IOS Security Technologies

- **Access control lists**
 - Reflexive access lists
 - Time-based access lists
- **Network Address Translation (NAT)**
- **VPN technologies**
 - IPSec encryption
 - Tunneling (GRE, L2F, L2TP)
- **Policy-based multiinterface support**
- **Event logging**
- **TACACS+/RADIUS authentication**

1303
0955_05F9_c2

© 1999, Cisco Systems, Inc.

www.cisco.com

7

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
- **PIX firewall**

Dedicated firewalling in a high-performance, scalable and fault-tolerant dedicated security appliance, with the most advanced features and application support

Cisco IOS™



1303
0955_05F9_c2

© 1999, Cisco Systems, Inc.

www.cisco.com



8



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 1600, 1700, 2500, 2600, 3600, and 7200 routers
- **Full routing functionality**
- **ICSA certified**

Cisco IOS™



1303
0955_05F9_c2 © 1999, Cisco Systems, Inc. www.cisco.com 10

Cisco IOS Firewall New Features

New Release—12.0(5)T—June 1999

- Per user authentication and authorization (“authentication proxy”)
 - Intrusion detection technology
 - IP fragmentation defense
 - Dynamic per-application port mapping
 - Configurable alerts and audit trail
 - SMTP-specific attack detection
 - New CBAC application support
- MS-Networking, MS Netshow

1303
0955_05F9_c2

© 1999, Cisco Systems, Inc.

www.cisco.com

11

Authentication Proxy

- HTTP-initiated authentication
- Valid for all types of application traffic
- Provides dynamic, per user authentication and authorization via TACACS+ and RADIUS protocols
- Works on any interface type for inbound or outbound traffic

1303
0955_05F9_c2

© 1999, Cisco Systems, Inc.

www.cisco.com

12

Authentication Proxy Highlights

- **Overcomes lock and key limitations**
 - Requires telnet to the router
 - Works with single ACL only
- **No special client required**
- **Supports RADIUS and TACACS+ servers**
 - CiscoSecure
 - Ascend and Livingston RADIUS servers
- **HTTP only, for now**
- **Independent software component**
- **For traffic passing through the router only**

1303
0955_05F9_c2

© 1999, Cisco Systems, Inc.

www.cisco.com

13

Intrusion Detection

- **In-line Intrusion Detection Sensor (51 signatures)**
 - If packets match signature IDS can
 - Send alarm
 - Drop packets
 - Reset the TCP connection
 - Combined with Cisco IOS firewall for Cisco 1720, 2600, 3600 and 7200 router platforms

1303
0955_05F9_c2

© 1999, Cisco Systems, Inc.

www.cisco.com

14

Intrusion Detection

- **Ideal for deployment anywhere you want to create additional visibility into network misuse**
 - Extranet connections**
 - Branch offices**
- **Value-add for current NetRanger™ customers that require additional “lightweight” packet auditing devices on additional connections**

1303
0955_05F9_c2

© 1999, Cisco Systems, Inc.

www.cisco.com

15

Cisco PIX Firewall

- **Dedicated firewall**
 - Integrated hardware/ software appliance**
 - Hardened OS**
- **Strong security**
 - Adaptive Security Algorithm (ASA)**
 - Cut-through proxy**
 - IPSec VPN option (8/99)**
- **Highest performance**
 - Up to more than 256,000 simultaneous sessions**
 - Over 170 Mbps throughput**
 - Over 6,500 connections per second**



1303
0955_05F9_c2

© 1999, Cisco Systems, Inc.

www.cisco.com

16

Cisco PIX Firewall 520

- **Enterprise chassis design**

**Up to 128MB RAM for
over 256,000
simultaneous sessions**

**Most flexible
configuration options**

**Designed for enterprise
environments**



1303
0955_05F9_c2

© 1999, Cisco Systems, Inc.

www.cisco.com

17

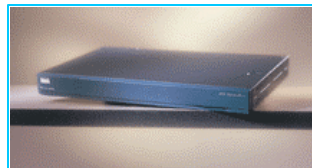
Cisco PIX Firewall 515

- **Low-profile chassis design**

**Up to 64MB RAM for
over 128,000
simultaneous sessions**

**Two configuration
options**

**Designed for a variety
of environments**



1303
0955_05F9_c2

© 1999, Cisco Systems, Inc.

www.cisco.com

18

Cisco PIX Firewall 515

- **Low, fixed cost**
No session-based license
- **Low-profile chassis**
Single rack unit height
Up to six integrated 10/100 Ethernet ports
Designed for small office or simple application environments
- **Network configurable**
No need for floppy drive
- **Software version 4.4**

PIX 515-R

- 32 MB RAM
- No failover
- Two 10/100 ports

PIX 515-UR

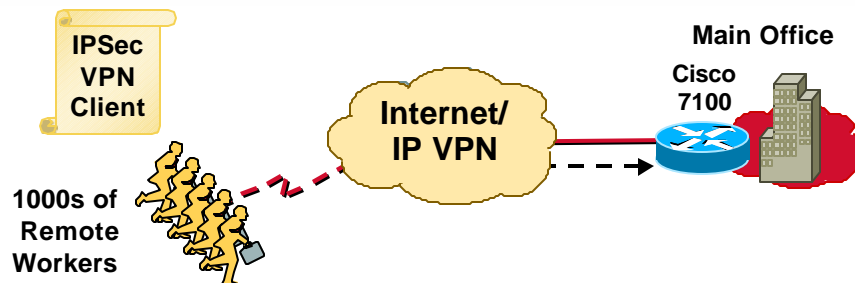
- 64 MB RAM
- Two to six 10/100 ports

1303
0955_05F9_c2 © 1999, Cisco Systems, Inc.

www.cisco.com

19

Remote Access VPN



- **Cost-effectively connect remote workers, customers, and partners**
- **Create a remote access VPN using an IPsec VPN client**
Available soon from Cisco
IPsec in Cisco IOS software fully compatible with Windows 2000 and IPsec built into common versions of UNIX

1303
0955_05F9_c2 © 1999, Cisco Systems, Inc.

www.cisco.com

20

IPSec VPN Client Highlights

Platforms

- Windows 95
- Windows 98
- Windows NT 4.0

Interoperability

- IPSec and IKE with DES and 3DES
- Interoperable with IPSec in Cisco IOS software

Features

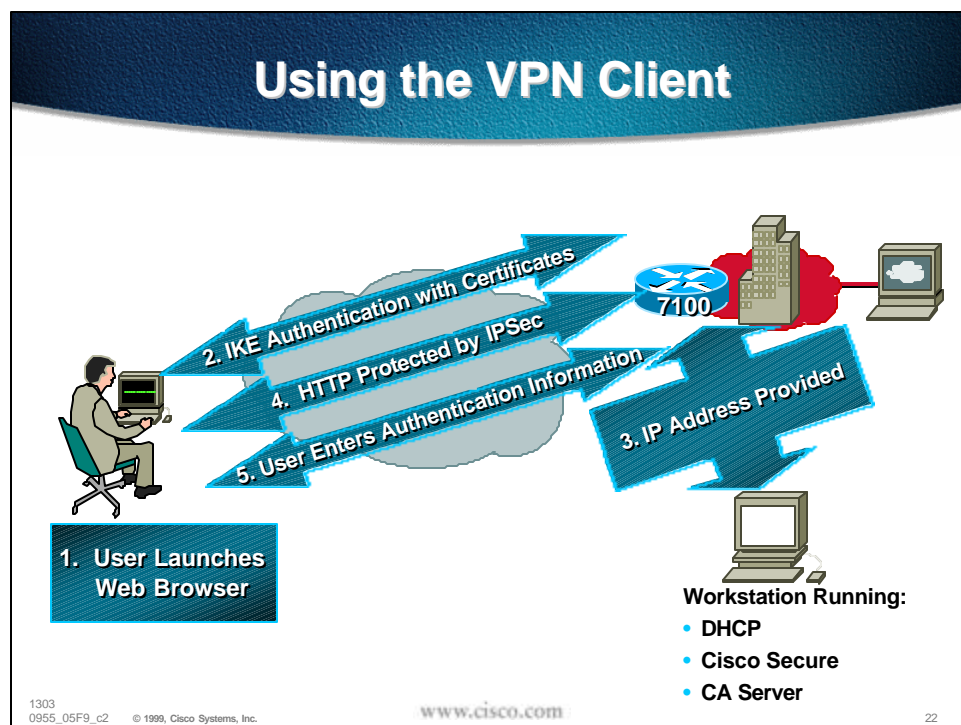
- Simple to use policy editor
- Transparent to end user
- Dynamic addressing
- AAA support through Cisco IOS Firewall feature set authentication proxy
- Digital certificate support from VeriSign, Netscape and Entrust with Certificate Enrollment Protocol (CEP)

Policy/Management

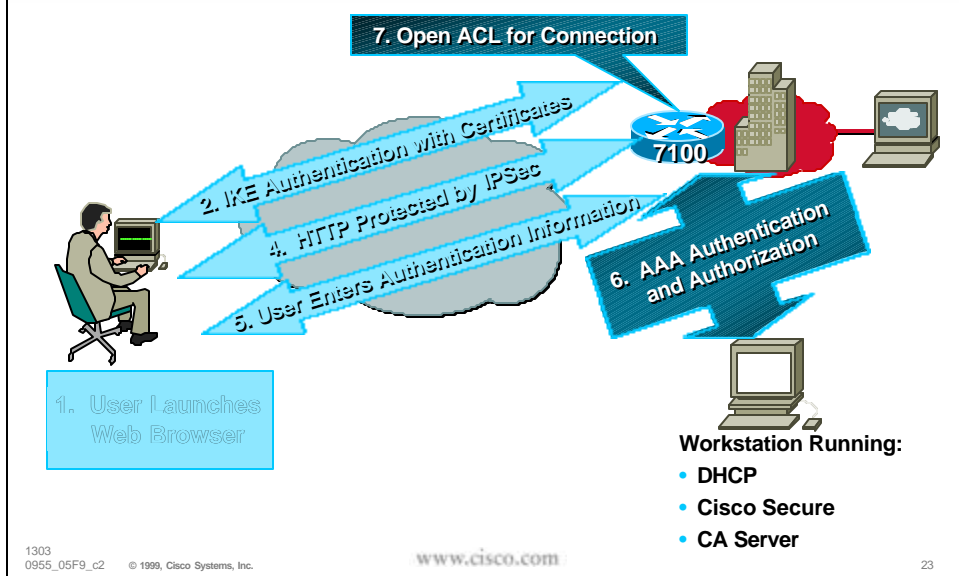
- Centrally configurable policy
- Can prevent end-users from changing policy
- Optionally prevent direct Internet access when IPSec tunnel is active

IPSec VPN Client

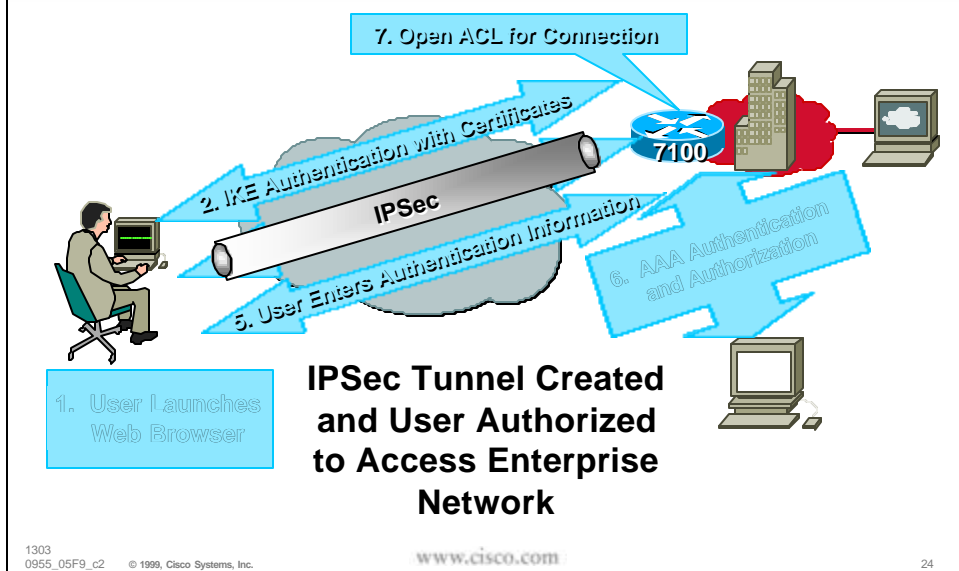
1303
0955_05F9_c2 © 1999, Cisco Systems, Inc. www.cisco.com 21



Using the VPN Client



Using the VPN Client





When to Buy What Firewall?

	
PIX Firewall	Cisco IOS Firewall
<ul style="list-style-type: none">• Dedicated device<ul style="list-style-type: none">Multilevel security policy enforcement• High-volume Internet sites<ul style="list-style-type: none">256K connections• Specific application requirements<ul style="list-style-type: none">URL filteringUnique NAT applications	<ul style="list-style-type: none">• Integrated solution<ul style="list-style-type: none">Cost effective• Highly scalable<ul style="list-style-type: none">Home office to enterprise• Intranet protection• Familiar Cisco IOS configuration

1303
0955_05F9_c2 © 1998, Cisco Systems, Inc. www.cisco.com

26

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



1303
0955_05F9_c2

© 1999, Cisco Systems, Inc.

www.cisco.com

27

Thank You

Kurt Kruger
Security Product Marketing

1303
0955_05F9_c2

© 1999, Cisco Systems, Inc.

28

