Agenda

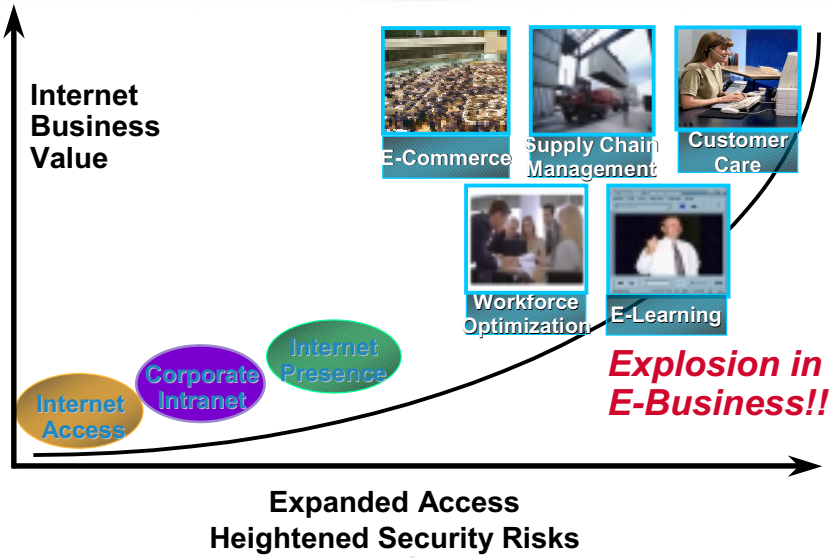
Business drivers

Threats

Migrating to a SAFE infrastructure

Conclusion

The Security Dilemma



Security: Why Should We Care?

- **Computer security is an enabling technology of the Internet**
  - **Privacy, authentication, integrity, fairness**
  - **Security turns the Internet into a serious tool for both business and personal uses**
  - **The limits of security are the limits of the Internet**
- **Attacks raise the cost of doing business**
- **Attacks cause bad publicity**
- **Attacks leave us open to unbounded losses**
- **Attacks INCREASE THE RISK of doing business on the Internet**

The Biggest Risk?

- **The opportunity cost of not participating:**
  - **Competitive advantages**
  - **Revenue and cost improvements**
  - **Expansion of business**
  - **Customer loyalty**
  - **New business models**
- **The benefits of being online more than make up for the risks**

Military vs. Business Security

- **Military security is absolute**
- **Business security is relative**
  - **Risks have to be managed**
  - **Lots of different solutions**
  - **Things fail all the time; smart companies recover and move on**

Agenda

Business drivers

Threats

Migrating to a SAFE infrastructure

Conclusion

Microsoft not alone in suffering security breaches

By Melanie Austria Farmer and Jim Hu
Staff Writers, CNET News.com
October 27, 2000, 10:45 a.m. PT

Microsoft may be one of the biggest names thus far to have its corporate networks hacked, but it's far from alone in having suffered such attacks.

In recent months, America Online and RealNames also have reported incursions on their systems.

Corporations and other entities large and small have often been targets of attacks. Sometimes hackers sneak their way into a company's Web site and deface the site with graffiti or more pointed messages. In September, for instance, a hacker smeared the Web sites of NASA and the Communications Workers of America, among others, with pro-Napster messages.

AOL in June confirmed that hackers had compromised member accounts by means of email attachments sent to AOL employees. At the time of the attack, AOL said it boosted the security of its email systems. An AOL spokesman declined to comment on the measures AOL employs to fight hackers.

Internet keyword service RealNames fell victim to an account hacker in February. The company, which substitutes complicated Web addresses with simple keywords, said the perpetrators may have accessed credit card numbers and passwords.

Microsoft itself has logged other breaches of security. In March and April, test copies of Whistler, a future Microsoft operating system for consumers, were leaked onto the Internet. The company said at the time that it had not yet come to any conclusions about how the internal test builds were being released to the Internet.

Industry experts say that while many companies have been beefing up security measures in an effort to safeguard valuable intellectual property and other data housed in internal systems, they will remain vulnerable to attacks.

Steve England, an intellectual property attorney and partner at Arnold & Porter, said corporate hacking incidents will continue to be a problem and will most likely increase no matter how well-armed companies are against breaches to their data security. Dealing with the aftermath is the real issue, he said.

Get the "Big Picture"
Related News
Message Boards

Quote Snapshot

MSFT 66.81 +2.38
AOL 45.56 +0.63

Real-Time Quotes NEW!

Enter symbol:

Go!

Symbol Lookup

Quotes delayed 20+ minutes

What's your take?

Trusting Employees

Latest Headlines

Enterprise Computing

Communications

Computer Virus Strikes 10 Companies

Updated 1:43 PM ET November 10, 2000

by D. IAN HOPPER, Associated Press Writer

WASHINGTON (AP) - Computers in at least 10 Fortune 500 companies have been infected recently by an annoying but only mildly dangerous Christmas-themed virus that security experts call "Navidad."

The virus, which affects computers using Microsoft's Windows operating system, arrives as a reply when a user sends an e-mail to an infected computer. The attachment, called "NAVIDAD.EXE," is mainly in Spanish, and antivirus experts believe the virus came from South America.

"We've seen at least 100 samples over the last 4 days, including at least 10 Fortune 500 companies," said Vincent Gullotto, top antivirus researcher at security company McAfee.com, adding that many of the virus-ridden e-mails have come from Brazil and Cuba.

When a person opens the Navidad attachment - something security experts always warn against unless the user knows what the attachment is - a message in Spanish reads: "Never press this button." If the button is pressed, a message says: "Feliz Navidad. Unfortunately you have given in to temptation and will lose your computer."

But the computer isn't damaged, which Gullotto says may be because the virus is designed for the Spanish version of Windows. But the virus does place on the computer's desktop an icon that looks like an eye, which stops most programs from being run.

"It's not destructive, but it may cause your Windows system to lock up," Gullotto said. The program can be stopped manually, and several antivirus companies have developed software that both removes and protects against the virus.

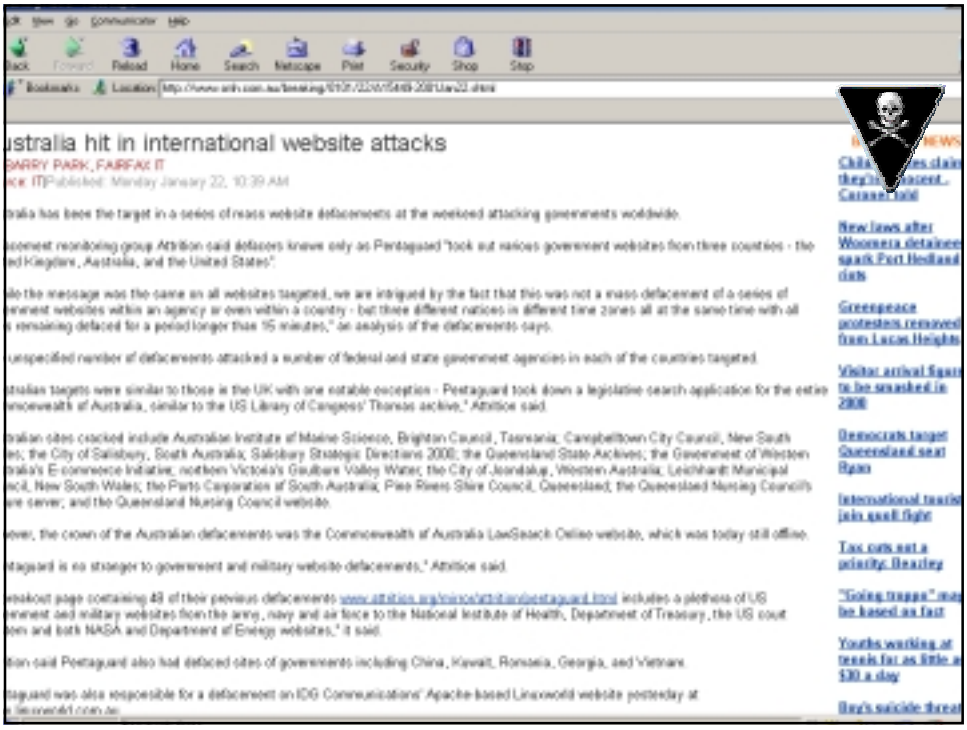
Several viruses in the past have taken holiday themes. One that appeared last year only damaged an infected computer on Christmas Day.

Current quotes (Delayed 20 mins.)
MCAF 7.12 0.00 (0.00%)
MSFT 68.81 2.38 (3.57%)
Quotes

AP Technology News
Amazon.com Launches E-Cards Store
Plans for Playboy.com IPO Scrapped
Boat Pagine Gialle To Buy Start-Up
Non-English Internet Sparks Concern
CMGI To Leave Two Subsidiaries
MarchFirst To Cut 1,000 Jobs
Non-PCs Rule at Trade Show
AP Corrects Gerick Story
Palm, PocketPC Camps Spar in Debate
IBM To Debut Computer Recycling
Meeting on Online Crime Prevention

Business Services
Choose a service
Audio-video store
Go!

Printer-friendly format
Send this story to a friend



ustralia hit in international website attacks

ARRY PARK, FAIRFAX IT
ce IT Published: Monday January 22, 10:39 AM

alia has been the target in a series of mass website defacements at the weekend attacking government worldwide.

overnment monitoring group Attrition said defacers knew only as Pentaguard "took out various government websites from three countries - the ted Kingdom, Australia, and the United States".

lso the message was the same on all websites targeted, we are intrigued by the fact that this was not a mass defacement of a series of ernment websites within an agency or even within a country - but three different nations in different time zones all at the same time with all remaining defaced for a period longer than 15 minutes," an analysis of the defacements says.

unspecified number of defacements attacked a number of federal and state government agencies in each of the countries targeted.

tralian targets were similar to those in the UK with one notable exception - Pentaguard took down a legislative search application for the entire mmonwealth of Australia, similar to the US Library of Congress' Thomas archive," Attrition said.

tralian sites cracked include Australian Institute of Marine Science, Brighton Council, Tasmania, Campbelltown City Council, New South es; the City of Salisbury, South Australia; Salisbury Strategic Directions 2000; the Queensland State Archives; the Government of Western tralia's E-commerce Initiative, northern Victoria's Goulburn Valley Water, the City of Joondalup, Western Australia; Leichhardt Municipal ncil, New South Wales; the Ports Corporation of South Australia; Pine Rivers Shire Council, Queensland; the Queensland Nursing Council's ine server; and the Queensland Nursing Council website.

ever, the crown of the Australian defacements was the Commonwealth of Australia LawSearch Online website, which was today still offline.

ntaguard is no stranger to government and military website defacements," Attrition said.

reakout page containing 48 of their previous defacements www.attrition.org/mirror/attrition/pentaguard.html includes a plethora of US ernment and military websites from the army, navy and air force to the National Institute of Health, Department of Treasury, the US court tem and both NASA and Department of Energy websites," it said.

tion said Pentaguard also had defaced sites of governments including China, Kuwait, Romania, Georgia, and Vietnam.

ntaguard was also responsible for a defacement on IDG Communications' Apache-based Linuxworld website yesterday at

NEWS

Chile ... claim they're innocent, Canada told

New laws after Woomera detainee spark Port Hedland riots

Greenpeace protesters removed from Lucas Heights

Visitor arrival figure to be smashed in 2000

Democrats target Queensland seat Ryan

International team to join quoll fight

Tax cuts not a priority: Beazley

"Going troppo" myth be based on fact

Youths working at tennis for as little as $30 a day

Boy's suicide threat

Technology Headlines

Friday March 03 02:00 AM EST

Hacker attack latest in string of online credit card thefts

John Borland, CNET News.com

A hacker attack on a New York e-commerce site is the latest in a string of online break-ins in which credit card numbers were stolen and posted to the Web, sources told CNET News.com today.

Since late January, at least eight small e-commerce sites have been hacked exploiting a known security hole in Microsoft software, according to a security investigator and companies and individuals affected by the attacks. The companies were listed on a taunting Web site posted by a hacker named "Curador" claiming credit for the attacks and listing thousands of stolen credit card numbers, sources said. He claims he seized more than 23,000 credit card numbers.

The incidents come amid heightened concern about Web security after other high-profile attacks. In January, several top-tier sites, including Yahoo and eBay, were shut down after being flooded with requests for information in "denial of service" attacks. No customer or company data were stolen in those attacks.

But close to 350,000 credit card numbers were stolen that same month from music site CD Universe and posted online. A hacker going by the name "Maxus" claimed he had the numbers and tried to extort $100,000 from the Web site. The FBI shut down the site where the credit card numbers had been posted.

Executives at wireless phone site Promobility.net and SalesGate.com confirmed the new attacks, as did the company that provided the Web software for LTA Media and Fedgovtbids.com sites.

A security consultant hired by LTA Media said the first attack targeted a Thai shopping site. Since then, sites in the United States, Canada and the United Kingdom have been hit, said Chris Davis, a Canadian security consultant with Tigor Team who has been retained to investigate the new case.

Law enforcement agencies in several countries are investigating the attack, according to companies who reported the break-ins to Canadian and U.S. officials. Authorities from the U.S. Secret Service, FBI and the Royal Canadian Mounted Police all declined to comment on the case.

The hackers broke in using a security hole in Microsoft's e-commerce Web server software, allowing the download of customer transaction records, several victims said. Curador taunted the victims--and Bill Gates--on his Web site, which was paid for with one of the stolen credit card numbers.

Random Stories from September 2000

- **Hacker compromised NASA's Jet Propulsion Laboratory (JPL) computer system and used it to host illegal activity**
- **Attackers have planted DDoS (distributed denial of service) agents on hundreds of Unix computers**
- **Cracker defaced OPEC's Web site**
- **Hacker was arrested for breaking into a computer at Lawrence Livermore National laboratory**
- **BidBay.com, an online auction site, was the victim of a DoS attack**
- **Crackers broke into Western Union's Web site servers and stole 16,000 customer credit and debit card numbers**
- **IKEA had a security breach that exposed customer information**

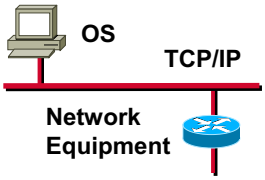
Three Primary Reasons for Security Issues

- Technology weaknesses
- Configuration weaknesses
- Policy weaknesses

And people eager to take advantage of the weaknesses

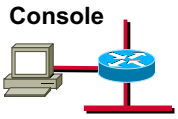
Technology Weaknesses

- TCP/IP protocol weaknesses
  - Sendmail, SNMP, SMTP, DoS (Syn Flood)
- Operating system weaknesses
  - UNIX, Windows NT, Windows 95, OS/2
- Network equipment weaknesses
  - Password protection
  - Lack of authentication
  - Routing protocols
  - Misconfigured firewall holes



Configuration Weaknesses

- Unsecured user accounts
- System accounts with easily guessed passwords
- Misconfigured Internet services
- Unsecured default settings within products
- Misconfigured network equipment



Policy Weaknesses

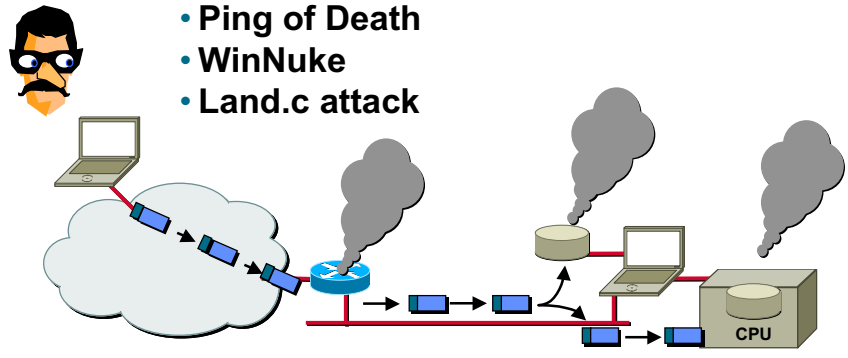
- Lack of written security policy
- Politics
- Business lacks continuity, cannot implement policy evenly
- Logical access controls not applied
- Security administration is lax, including monitoring and auditing
- Software and hardware installation and changes do not follow policy
- Disaster recovery plan is nonexistent

General Threat Types

- Eavesdropping
- Denial of service
- Unauthorized access
- Data manipulation
- Masquerade
- Session Replay
- Session hijacking
- Rerouting
- Repudiation
- Viruses, Trojan Horses, and Worms

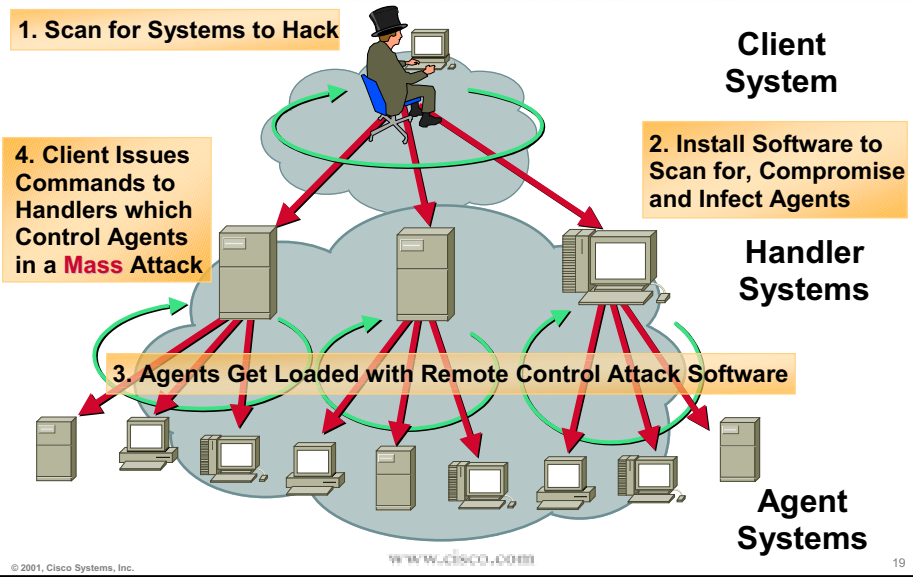
Denial of Service

- TCP SYN attack
- Ping of Death
- WinNuke
- Land.c attack

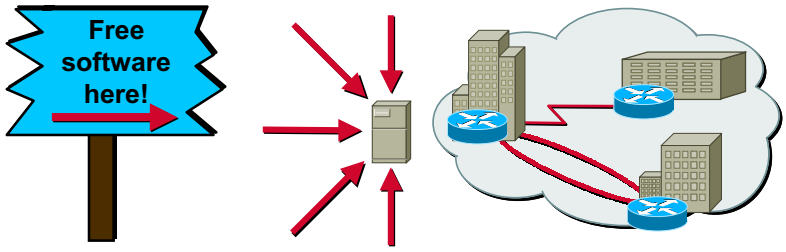


- Prevents authorized people from using a service

DDoS, How Does It Work?

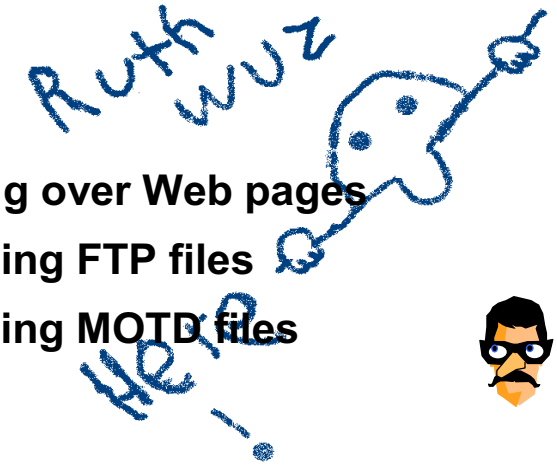


Unauthorized Access: WareZ



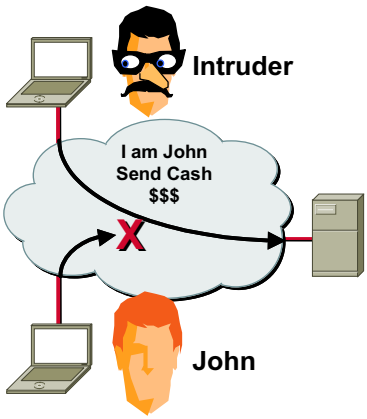
- Accessing and placing unauthorized files or resources on another system
  - GIFs
  - Hacker tools
  - Unlicensed versions of software

Data Manipulation: Graffiti



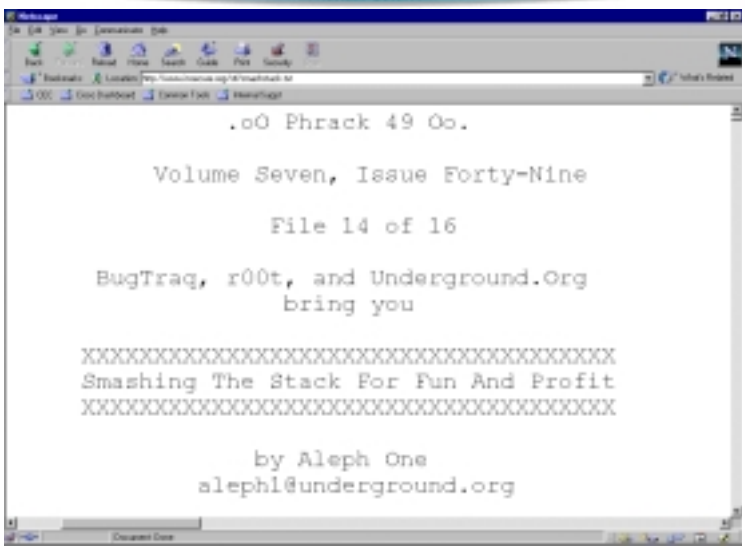
- Painting over Web pages
- Replacing FTP files
- Replacing MOTD files

Session Susceptibilities



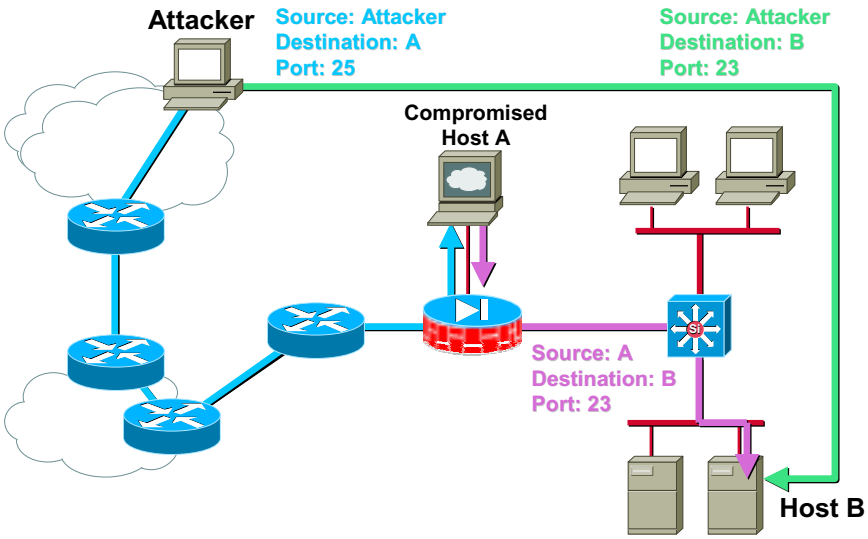
- Session hijacking
- Rerouting
- Repudiation

Application Layer Attacks

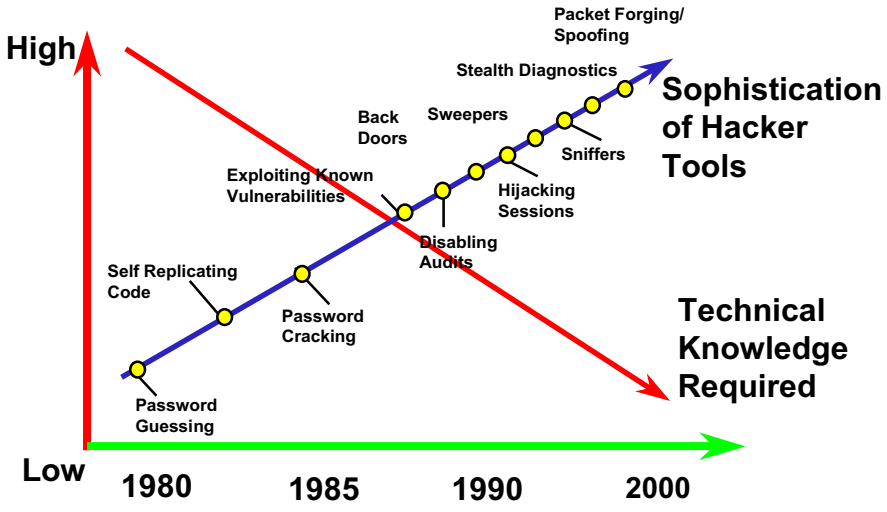


Root Kits

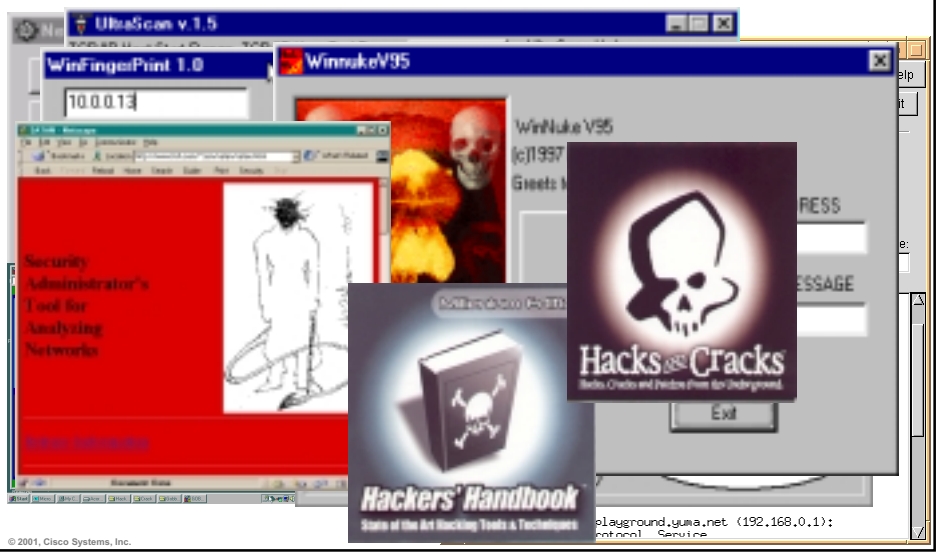
Port Redirection Attack



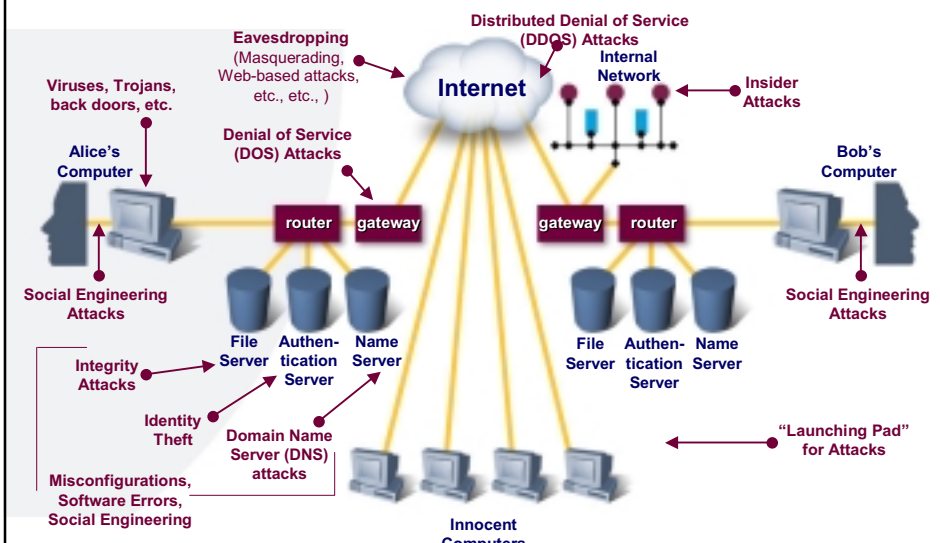
Threat Capabilities



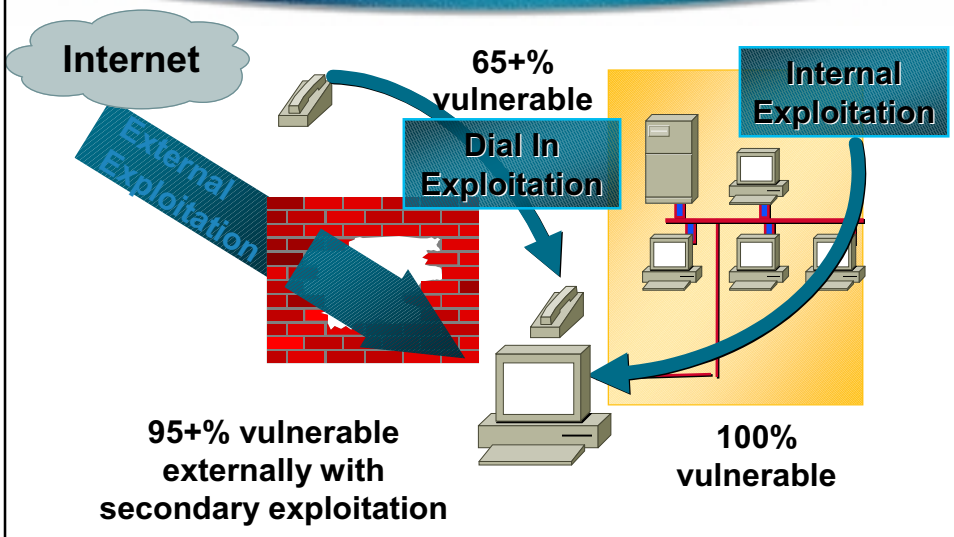
Hundreds of Tools



The big picture



Expected Threats



Source: Cisco Secure Consulting Engagements, 1996-1999

Will We Ever Learn?

- Buffer overflows were first identified in the 1960s
- They were first used to attack networked computers in the 1970s
- The Morris Worm used buffer overflows to attack the Internet in 1989
- Today, buffer overflows are the most common way to attack systems
  - –Two-thirds of all CERT advisories are about buffer overflows

Will We Ever Learn?

- There's a particular bug in Microsoft Internet Information Server
- It was fixed in July 1998
- Another warning was published by Microsoft in July 1999
- In January 2000, the bug was exploited to steal credit card numbers from several Web sites

Good System Administration

"A new study by Cisco Secure Consulting Services offers some insight into where many common vulnerabilities exist in IT network systems. The study, which analyzed 33 midsize and large customer sites over a period of six months, found vulnerabilities in all the customer sites, but almost all the vulnerabilities could be traced to outdated software or lax system administration maintenance, not to inherent flaws in the systems. While the need for careful system administration and continual system security analysis has been well-understood, Cisco's study indicates that most businesses, especially those that are conducting E-commerce activities over the Internet, aren't being careful enough."

Information Week
February 21, 2000,
Issue: 774

Good System Administration

Fundamentals

- Mailing lists
- Patches
- Logging
- Basics
  - Strong or one-time passwords
  - Encryption
  - Switched infrastructure

Tips

- Firewalls or sysadmins?
- After you log it, read or analyze it!

Agenda

Business drivers

Threats

Migrating to a SAFE infrastructure

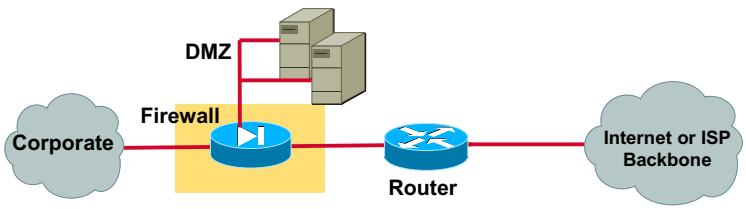
Conclusion

Design Considerations

- Open the corporate network to give users access to resources in the Internet
- Secure the corporate network against attacks from the Internet
- Implement a firewall!

Something to start with: A simple Security design

- Need to connect the trusted network (Corporate LAN) to an untrusted network (Internet)



Firewall only

Which is the right Firewall to choose?

- **Software based Firewall**
- Network hidden to the outside (Proxy)
- All features of underlying OS apply (choice of interfaces, Crypto cards, etc.)
- But:
  1. More security bugs
  2. Difficulty of analysis
  3. Difficulty of testing

- **Appliance**
- Hardened operating system
- Higher performance
- No need for Proxies
- Easy to install
- Easy to maintain
- Lower price point

Firewall criteria

PIX

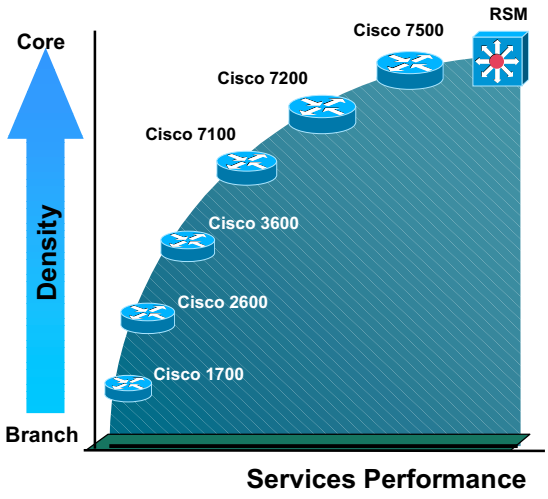
- Optimized appliance
- Stateful failover
- IDS 53 signatures
- URL filtering
- VPN performance
- Aggregated throughput
- LAN interfaces

- **IOS Firewall**
- Router with enhanced functionality
- Stateless failover (HSRP)
- IDS 59 signatures
- SNMPv3
- Enhanced Routing Protocols
- QoS features
- Multicasting support
- WAN interfaces

PIX Firewall Family

IOS Firewall Platforms

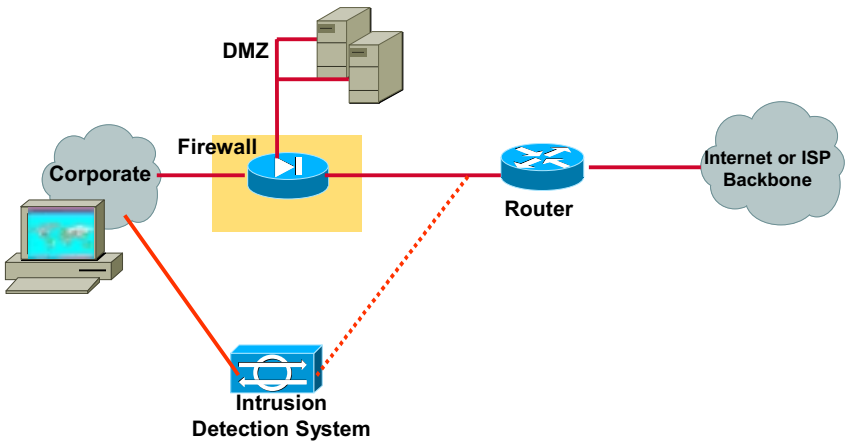
- CBAC
- Java blocking
- DoS detection and prevention
- Real time alerts
- Authentication proxy
- Intrusion detection
- Dynamic port mapping
- Cisco 800, UBR 904, 1600 and 2500 support IOS FW with the exception of IDS and Authentication proxy



Design Considerations

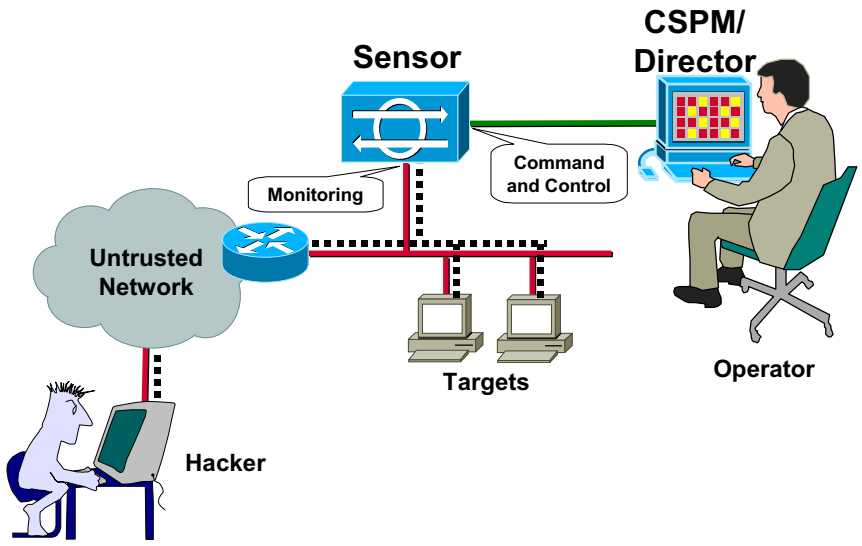
- Want to know about activities as intrusion attempts
- Inspect attacks in data part of packets
- Implement a Real Time Monitoring which tells what is actually going on in the network

Security Design with Real Time Monitoring



Adding Intrusion Detection

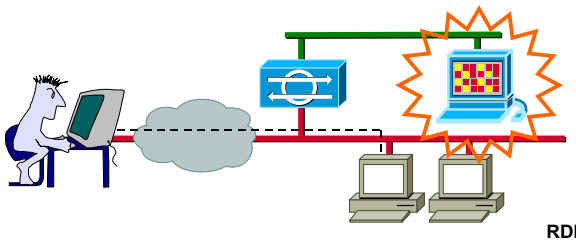
Intrusion Detection



Alarm Display and Logging

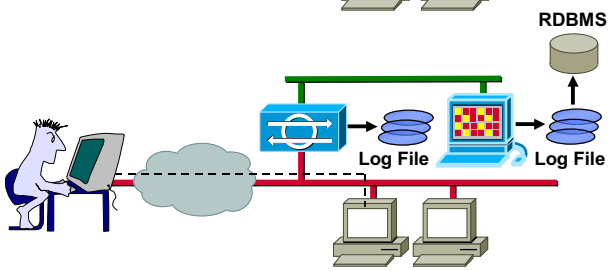
Alarm Display

Alarms are displayed on the CSPM/ Director.



Alarm Logging

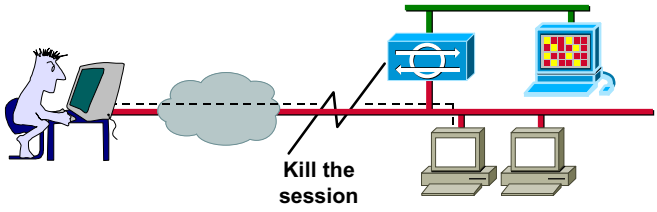
Alarms are logged on the Sensor and CSPM/ Director.



Intrusion Response

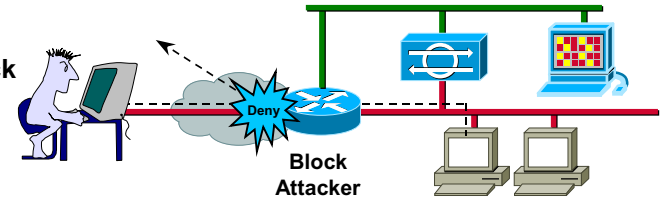
TCP Reset

Automatic kill of offending session.



Shunning

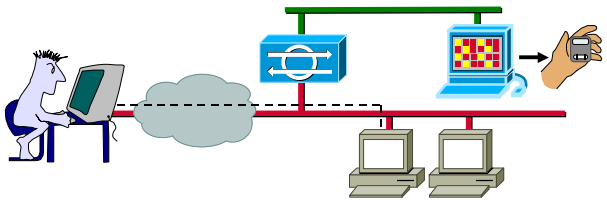
Auto/Manual block of offending IP address.



E-mail and Script Execution

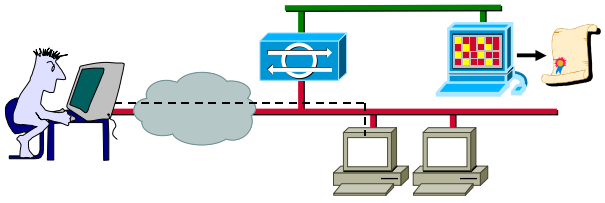
E-mail Notification

Sends notification to e-mail recipient or pager.

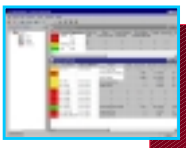


Script Execution

Starts any user-defined script.



Cisco Secure Intrusion Detection



IDS Sensing Portfolio

- Cisco IOS firewall with IDS
- PIX with IDS
- IDS sensor appliances
  - 4210—up to 45Mbps
  - 4230—up to 100 Mbps
- Catalyst 6xxx IDS line card
- IDS director for UNIX
- CSPM for Windows

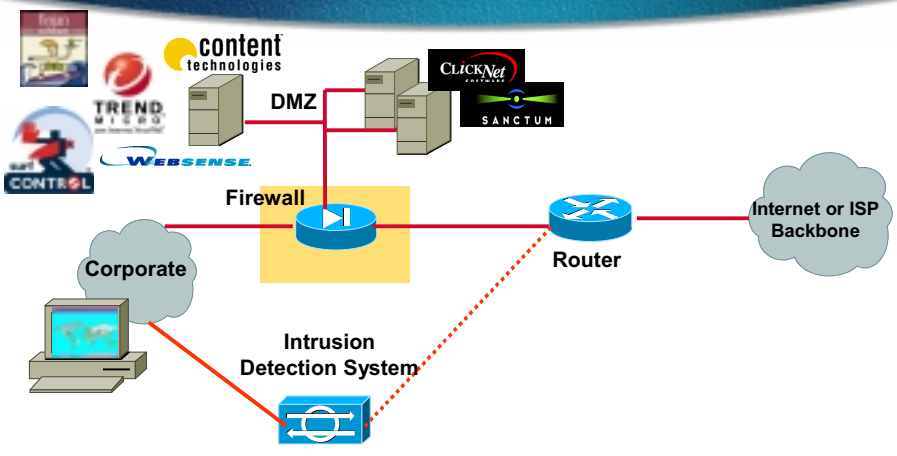
How Cisco IOS Firewall/PIX IDS compares with IDSM/IDS Sensor

Cisco IOS Firewall/PIX with IDS	IDSM/IDS Sensor
• Takes real-time action	•Takes action after detection
• Limited 59/53 signatures	• Full set of signatures
• Has "response=drop" capability (IOS)	• No "response=drop" capability
• No "response=shun" capability	• Has "response=shun" capability (sensor)
•Managed via CLI	• Managed by CSPM or IDS Director (sensor)
• Integrated into network infrastructure with firewall	• Standalone, dedicated processing power

Design Considerations

- Protect yourself against active content in emails
- Protect hosts in the DMZ
- Restrict user access to web pages
- Implement Host based IDS, Email Virus Filtering and URL Blocking

Security Design Advanced

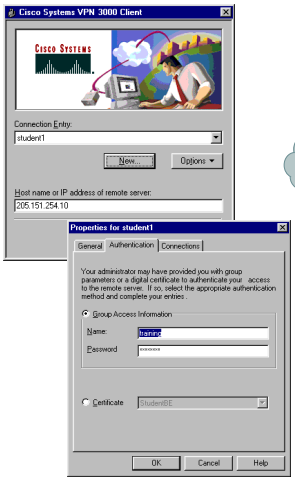


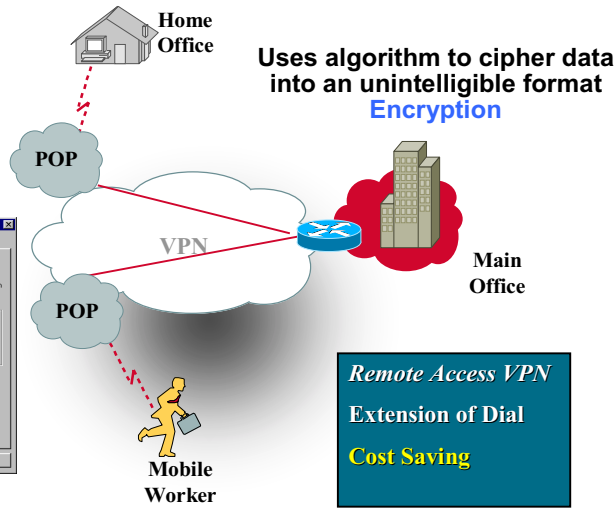
Adding Email Virus Filtering and URL Blocking

Design Considerations

- Give users who are travelling or working from a different location access to the network
- Use an existing transport network to reduce cost of operation
- Connect Remote Access Users securely via the Internet!

Remote Access VPN

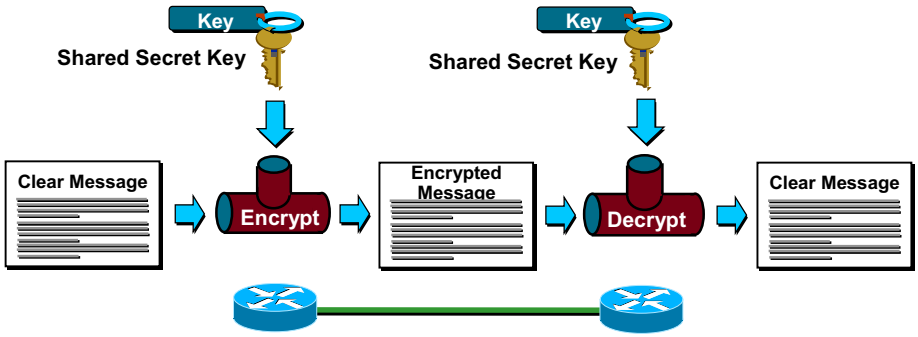




Uses algorithm to cipher data into an unintelligible format
Encryption

Remote Access VPN
Extension of Dial
Cost Saving

DES Encryption

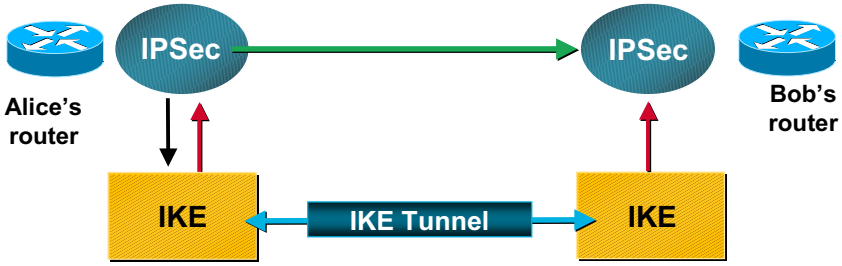


- Encryption turns cleartext into ciphertext
- Decryption restores cleartext from ciphertext
- Keys enable encryption and decryption

How IPSec Uses IKE

1. Outbound packet from Alice to Bob. No IPSec SA

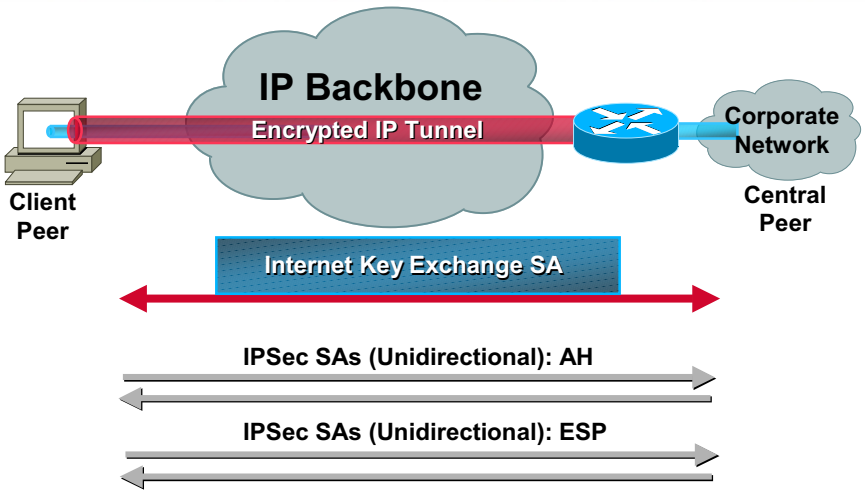
4. Packet is sent from Alice to Bob protected by IPSec SA



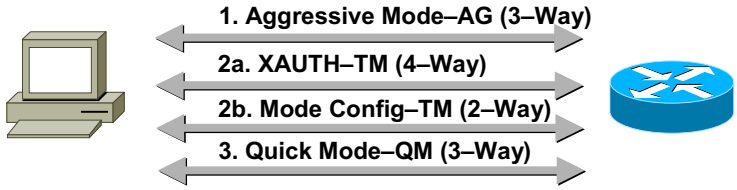
2. Alice's IKE begins negotiation with Bob's

3. Negotiation complete. Alice and Bob now have complete set of SAs in place

IPSec Overview



IKE SA in Remote Access VPN



1. Aggressive mode; authenticate, key material, three-way exchange
2a. Extended authentication; username/password
2b. Mode configuration; IP address, DNS, WINS
3. Quick mode; negotiate security parameters and generate keys for IPSec SAs

Establishing the IKE SA

User (Fred) Connects to VPN Concentrator (Wilma) and Initiates ISAKMP Phase 1 Aggressive Mode

Fred Sends SA Proposal Request, DH, ID

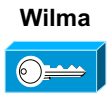
Messages Sent in the Clear

Wilma Sends SA Parameters, DH, ID, Hash

Fred Authenticate D–H Apply Hash

IKE Bi–Directional SA Established

Mode Config and Xauth



Wilma Requests for Username/Password

Wilma Sends ISAKMP_CFG_REQUEST

Fred Replies ISAKMP_CFG_REPLY

Wilma Sends SET (XAUTH=OK)

Fred Replies ACK (XAUTH)

Protected by the IKE SA

Fred Sends a Request for a Number of Attributes; IP Address, DNS, WINS

Fred Sends ISAKMP_CFG_REQUEST

Wilma Replies ISAKMP_CFG_REPLY

Establishing IPSec SAs

Using the Parameters Received Fred Initiates and ISAKMP Phase 2 Oakley Quick Mode

IPSec SA Offer–Transform, Mode, PFS, Authentication, Lifetime →

← Policy Match Accept Offer

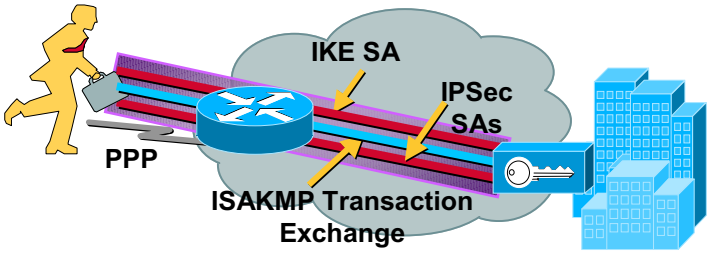
Fred D–H Exchange or Refresh IKE Key →

← Wilma D–H Exchange or Refresh IKE Key

Protected by the IKE SA

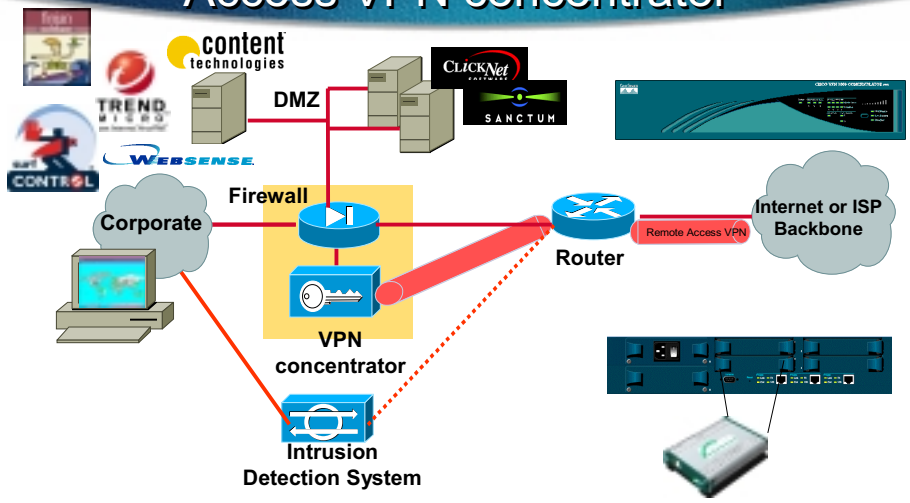
IPSec Outbound SA Established
IPSec Inbound SA Established

Enable Mobile Users with Mode Config IKE Extension



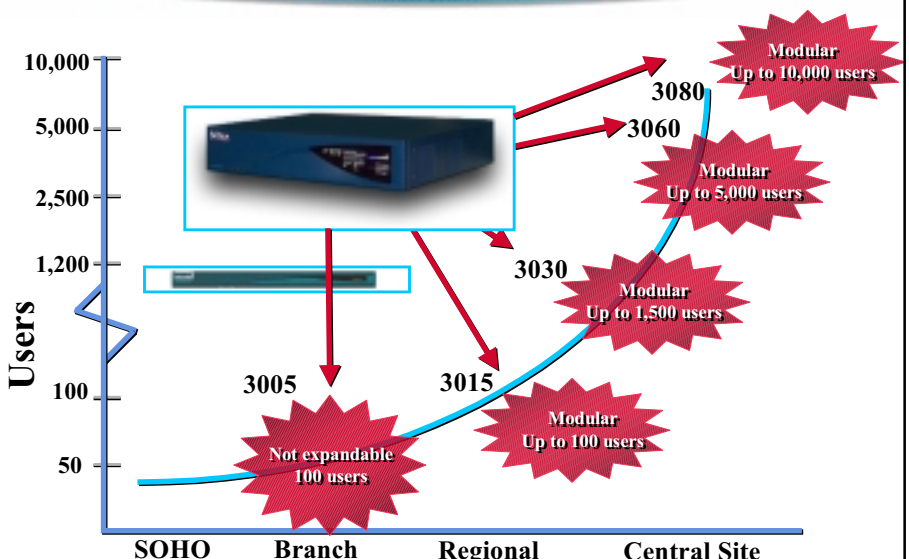
1. Dial ISP using PPP via modem
2. Establish the IKE SA with gateway
3. Send username/password; request security parameters
4. Client has internal attributes, establish IPSec SAs

Security Design with Remote Access VPN concentrator



Adding Remote Access VPN

Cisco VPN 3000 Concentrator Series



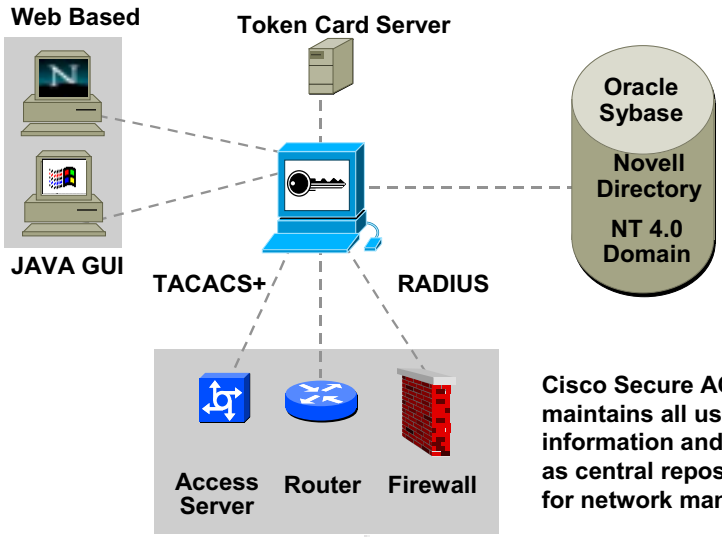
The Internet Challenge

- *How do you know the person at the other end is not a dog?*

Identity Goals

- **Unified user control in the network**
  - **Verify identity with digital mechanisms**
  - **Recognize user, time, and location**
  - **Maintain authorization policy per-user, enterprise-wide**
  - **Keep a record of behavior/actions**

Cisco Secure Access Control Server



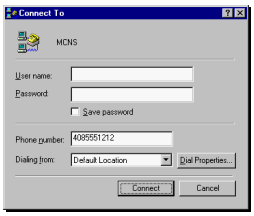
Cisco Secure ACS maintains all user information and acts as central repository for network manager

Authentication—Token Cards and Servers

1.

Uses algorithm based on PIN or time-of-day to generate secure password

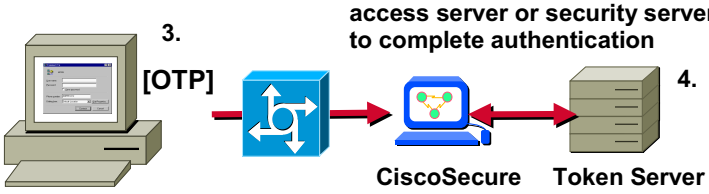
2.



Server uses same algorithm to decrypt password

Sends password to network access server or security server to complete authentication

3. [OTP]



CiscoSecure

4. Token Server

Design Considerations

- Connect branches, business partners and supplier networks to the corporate network
- Use an existing transport network to reduce cost of operation
- Connect Site to Site VPNs securely via the Internet!

VPN Applications

Site-to-Site Intranet VPN

Extension of Classic WAN

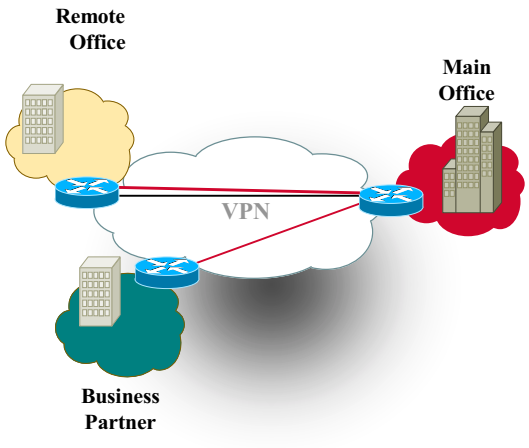
Rich VPN Services

Cost Saving & New Applications

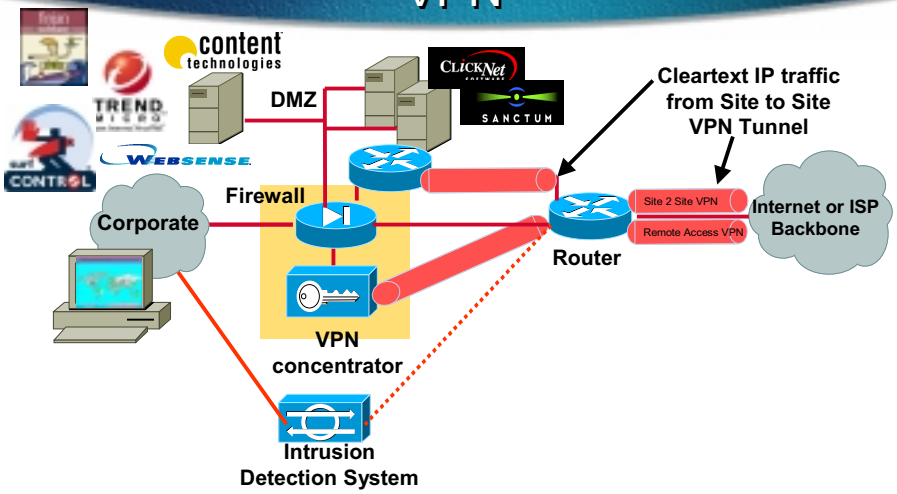
Site-to-Site Extranet VPN

Extends WANs to business partners

New Applications and Business Models



Security Design with Site to Site VPN



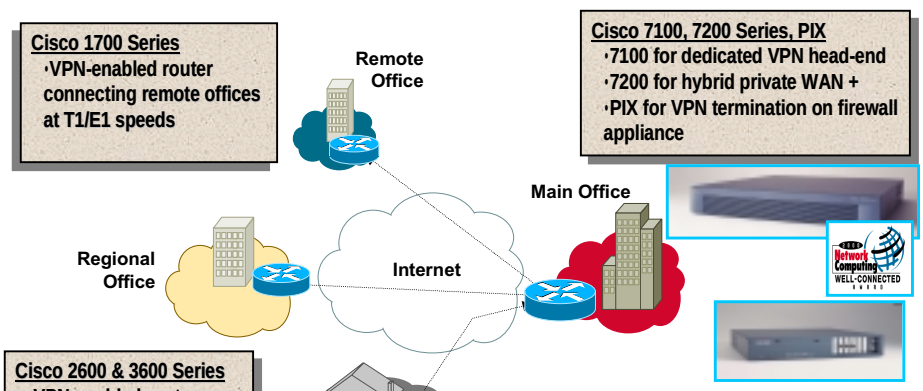
Adding Site to Site VPN

Cisco Site-to-Site VPN Solutions

Scalability for Every Site

Cisco 1700 Series
- VPN-enabled router connecting remote offices at T1/E1 speeds

Cisco 7100, 7200 Series, PIX
- 7100 for dedicated VPN head-end
- 7200 for hybrid private WAN +
- PIX for VPN termination on firewall appliance



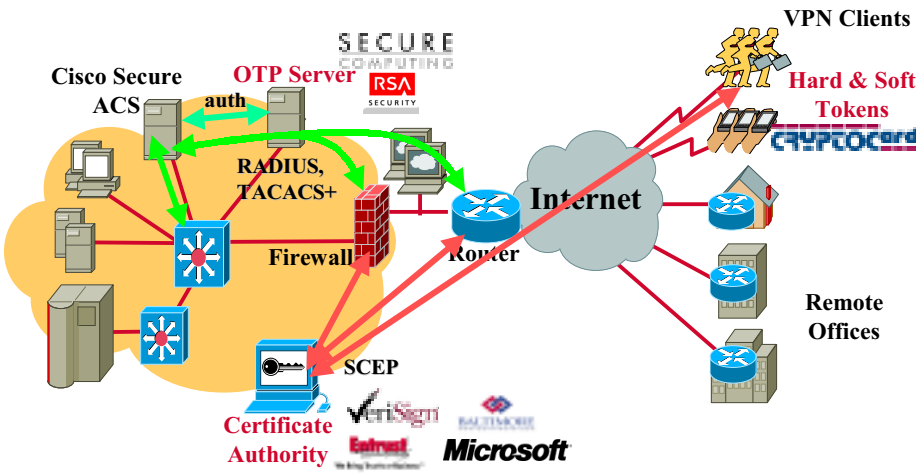
Cisco 2600 & 3600 Series
- VPN-enabled routers connecting branch and regional offices at nxT1/E1 speeds

Cisco 800, UBr900, & 1400 Series
- VPN-enabled routers for ISDN, DSL, and cable connectivity

Public Key Infrastructure

- Certificate Authority (CA) verifies identity and signs digital certificate Certificate equivalent to an ID card
- Enables large-scale IPSec deployment
- Interoperate with: Baltimore, Netscape, Verisign Onsite for IPSec and Entrust VPN Connector

Public Key Infrastructure



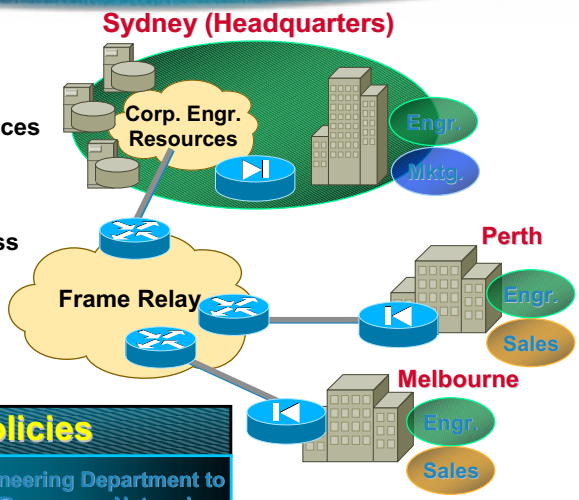
Design Considerations

- **Simplify the management**
- **Multiple Device Management instead of single device management**
- **Implement a Security Policy Management tool!**

Policies in the Network

A set of high-level business directives that control the deployment of network services (e.g. security and QoS)

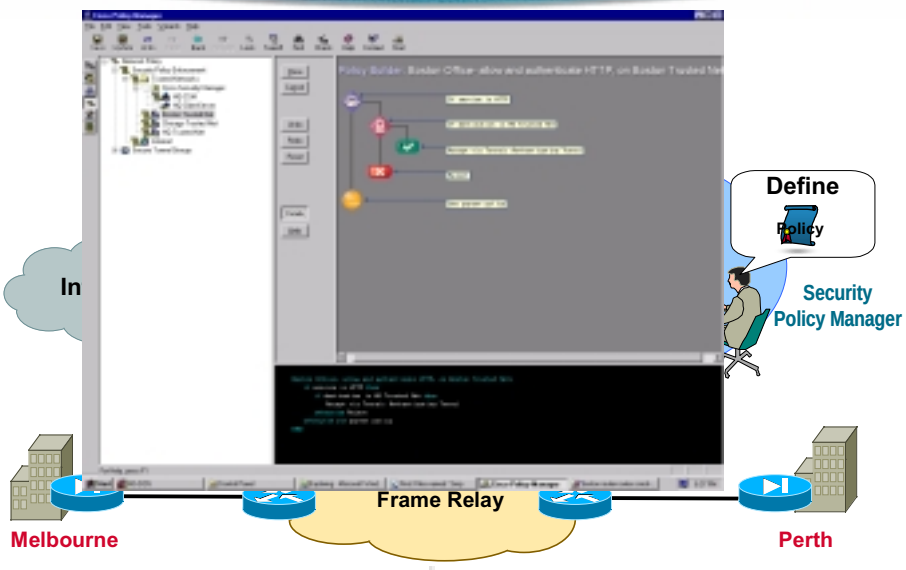
Created on the basis and in terms of established business objectives



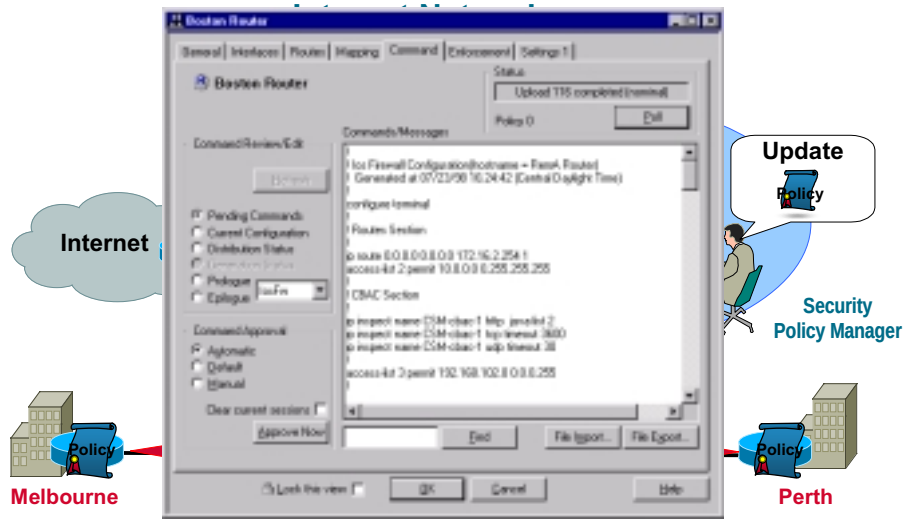
Network Policies

"Allow all Members of the Engineering Department to Access the Corporate Engr. Resources Network Using FTP, Telnet , the Web (HTTP) and DNS."

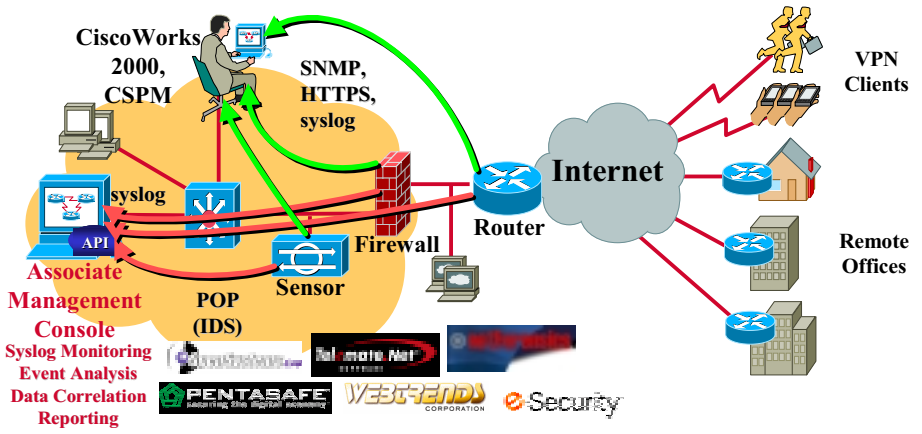
Deploying Security Policies within a Network



Deploying Security Policies within a Network



Security Monitoring Solutions



Cisco SAFE Defined

A comprehensive security framework that enables organizations to safely engage in e-business

Cisco's SAFE….

...is a proven blueprint for designing and implementing secure enterprise networks.

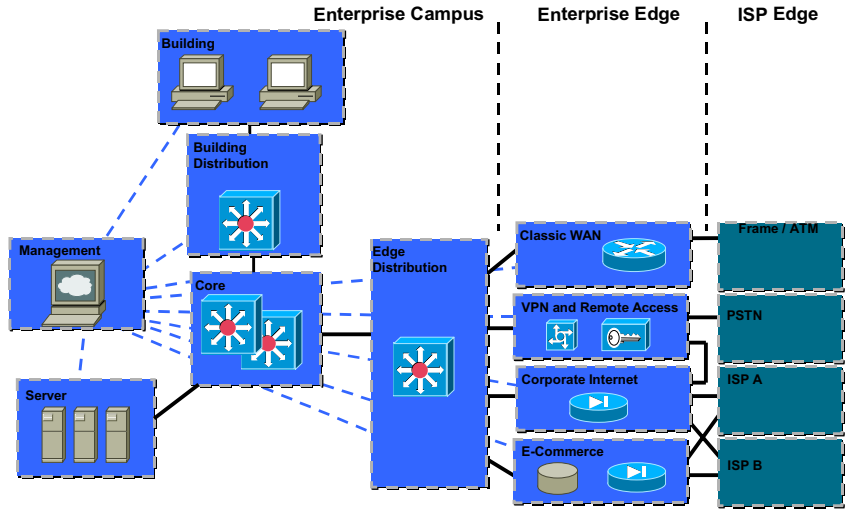
...it provides end users with:

- security best practices
- a modular design details
- attack mitigation details

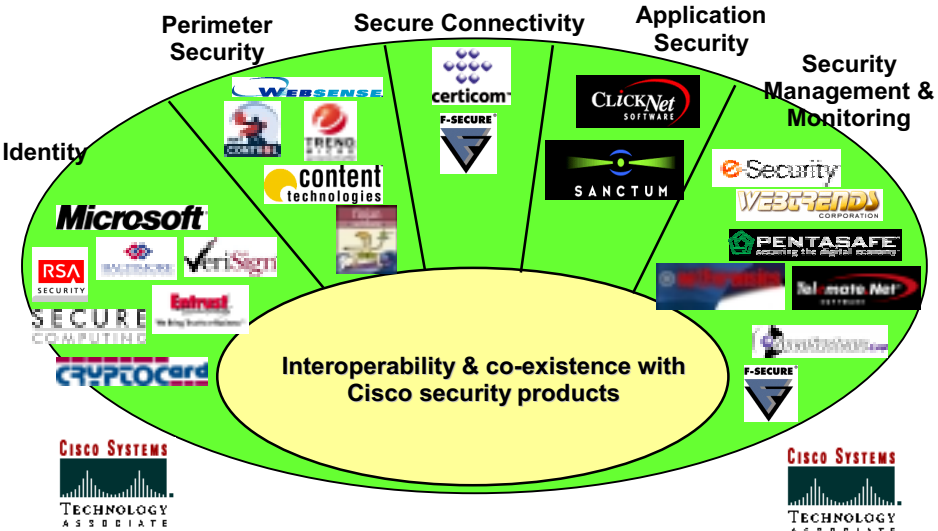
SAFE Caveats

- Assumes a security policy
- Focuses on large businesses
- Network centric
- Baseline blueprint will evolve

Enterprise SAFE Modules



Security and VPN Associate Solutions



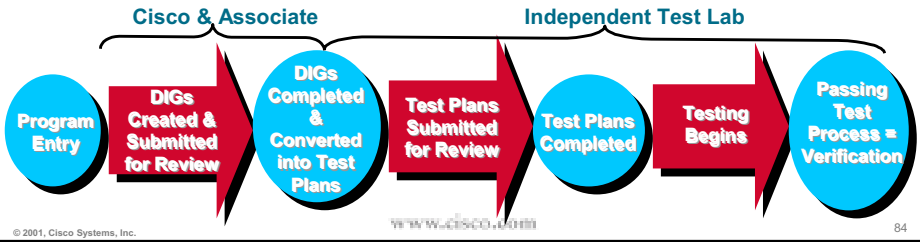
Security and VPN Associate Program Membership Requirements

- Complementary security product/technology
- Endorsement from Cisco employee (e.g. PM, SE, AM)
- Complete a comprehensive web-based application form and legal contract
- Provide at least one customer reference using applicant's product in a Cisco network
- Complete a "Design Guide" document that includes configurations, network diagrams, detailed implementation guidelines
- Successful completion of interoperability testing with independent lab

Cisco Systems Technology Associate

Security and VPN Associate Program Interoperability Testing

- All Associate products must be interoperability tested -- and pass
- Provided by an independent, third-party testing house
  Additional labs under investigation (US, Australia)
- Cisco and Associate will establish DIGs
- Independent lab provides Test Plans for each solution set based on approved DIG
- Ensures high solution interoperability, performance and reliability



Security and VPN Associate Program Web Site

- **Provides up-to-date information on security solutions for Cisco customers, sales teams and channels**
  - **Engagement tool for Cisco sales team**
- **A selection tool for the right Associate or product for a solution**
- **Customer support tool for Cisco TAC**
- **CCO Access:**
  - www.cisco.com/go/securityassociates/
- **Internal Access (VSEC Web site)**
  - wwwin.cisco.com/ent/vsec/sap/index.shtml

Future Partnership Directions

- **Personal Firewalls**
  - **Integrated personal firewall solution in our VPN client is needed**
  - **We're collaborate with leading vendor(s) to fill this gap [e.g. Zone Labs, Network Ice]**
  - **Coexistence initially. Tighter integration will require new interface development and/or new standards support.**
- **VPN & Mobile Clients**
  - **Need to evangelize "intelligent" Cisco VPN solutions through complementary client products**
  - **Results will increase market share and product sales significantly**
  - **Collaborate with leading vendor(s) to fill this gap [e.g. IBM, Apple, HP, Sun] and encourage them to adhere to our Unity client spec**
- **Biometrics**
  - **Smartcard support enhances our authentication solutions tremendously**
  - **Collaborate with leading vendor(s) to fill this gap [e.g. Gemplus, Schlumberger, SecuGen]**
  - **Will require new interface development and/or new standards support**
- **Application Server/Host security**
  - **Complements our perimeter security products and supports SANs efforts**
  - **Collaborate with leading vendor(s) to fill this gap [e.g. Argus Systems, InfraWorks]**

Agenda

Business drivers

Threats

Migrating to a SAFE infrastructure

Conclusion

Implementing SAFE: Where do I start?

- **Develop a security policy based on business requirements and likely threats.**
- **Use modular blueprint for designing and deploying an all-encompassing security solution.**
- **Use Security Associate products to complement Cisco products and features.**
- **Perform a Network Vulnerability Analysis**
- **Maintain security posture through disciplined system/network administration.**

Top 14 Security Vulnerabilities

1. Inadequate router access control: misconfigured router ACLs can allow information leakage through ICMP, IP, NetBIOS, and lead to unauthorized access to services on your DMZ servers.
2. Unsecured and unmonitored remote access points provide one of the easiest means of access to your corporate network
3. Information leakage can provide the attacker with operating system and application versions, user groups, shares, DNS information zone via zone transfers, and running services like SNMP, finger, SMTP telnet, rusers, sunrp, NetBIOS.
4. Hosts running unnecessary services (such as sunpc, FTP, DNS, SMTP) leave ways in.
5. Weak, easily guessed and reused passwords at the workstation level can doom your servers to compromise.
6. User or test accounts with excessive privileges.
7. Misconfigured Internet servers, especially CGI scripts on web servers and anonymous FTP.

Top 14 Security Vulnerabilities (cont.)

8. Misconfigured firewall or router ACL can allow access to internal systems directly or once a DMZ server is compromised.
9. Software that is unpatched, outdated, vulnerable, or left in default configurations.
10. Excessive file and directory access controls (NT/95 shares, UNIX NFS exports).
11. Excessive trust relationships such as NT Domain Trusts and UNIX .rhosts and hosts .equiv files can provide hackers with unauthorized access to sensitive systems.
12. Unauthenticated services like X Windows.
13. Inadequate logging, monitoring, and detection capabilities at the network and host level.
14. Lack of accepted and well promulgated security policies, procedures, guidelines, and minimum baseline standards.

Further Reading

- www.cisco.com/go/safe
- www.cisco.com/go/security www.cisco.com/go/evpn
- www.cisco.com/go/securityassociates
- Networking Professionals Connection (forums.cisco.com)
- Improving Security on Cisco Routers
  http://www.cisco.com/warp/public/707/21.html
- Essential IOS Features Every ISP Should Consider
  http://www.cisco.com/warp/public/707/EssentialIOSfeatures_pdf.zip
- Increasing Security on IP Networks
  http://www.cisco.com/cpress/cc/td/cpress/ccie/ndcs798/nd2016.htm