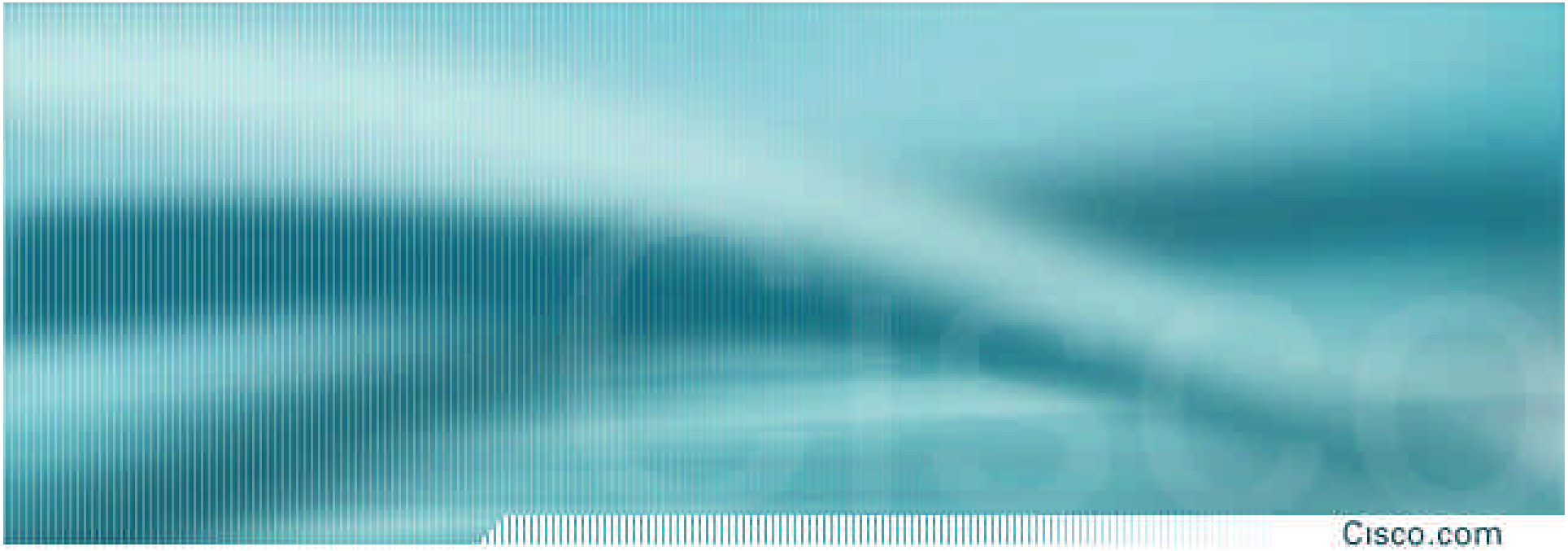


Introduction to Network Security

Agenda

Cisco.com

- **Security Year in Review**
  - Slammer, et. al.
- **Security Policy**
  - Setting a Good Foundation
- **Extended Perimeter Security**
  - Define the Perimeter, Firewalls, ACLs
- **Identity Services**
  - Passwords, Tokens, PKI, Biometrics
- **Secure Connectivity**
  - Work Happens Everywhere, Virtual Private Networks
- **Intrusion Protection**
  - Network, Host
- **Security Management**
  - Wrapping it All Together

Agenda

Cisco.com

- Security Year in Review
  - Slammer, et. al.
- Security Policy
  - Setting a Good Foundation
- Extended Perimeter Security
  - Define the Perimeter, Firewalls, ACLs
- Identity Services
  - Passwords, Tokens, PKI, Biometrics
- Secure Connectivity
  - Work Happens Everywhere, Virtual Private Networks
- Intrusion Protection
  - Network, Host
- Security Management
  - Wrapping it All Together

Security Year in Review

- **Are incidents decreasing?**
- **SQL slammer**
- **Other security headlines**

Are Incidents Decreasing?

Cisco.com

Type of Crime	2001	2002
Theft of Proprietary Information	$151.2	$170.8
Financial Fraud	$92.9	$115.7
Insider Net Abuse	$45.3	$49.9
Sabotage	$5.2	$15.1
Unauthorized Access by Insiders	$6.1	$4.5
Laptop Theft	$8.8	$11.7
Denial of Service	$4.3	$18.4
System Penetration by Outsiders	$19.0	$13.0
Total	**$378M**	**$456M**

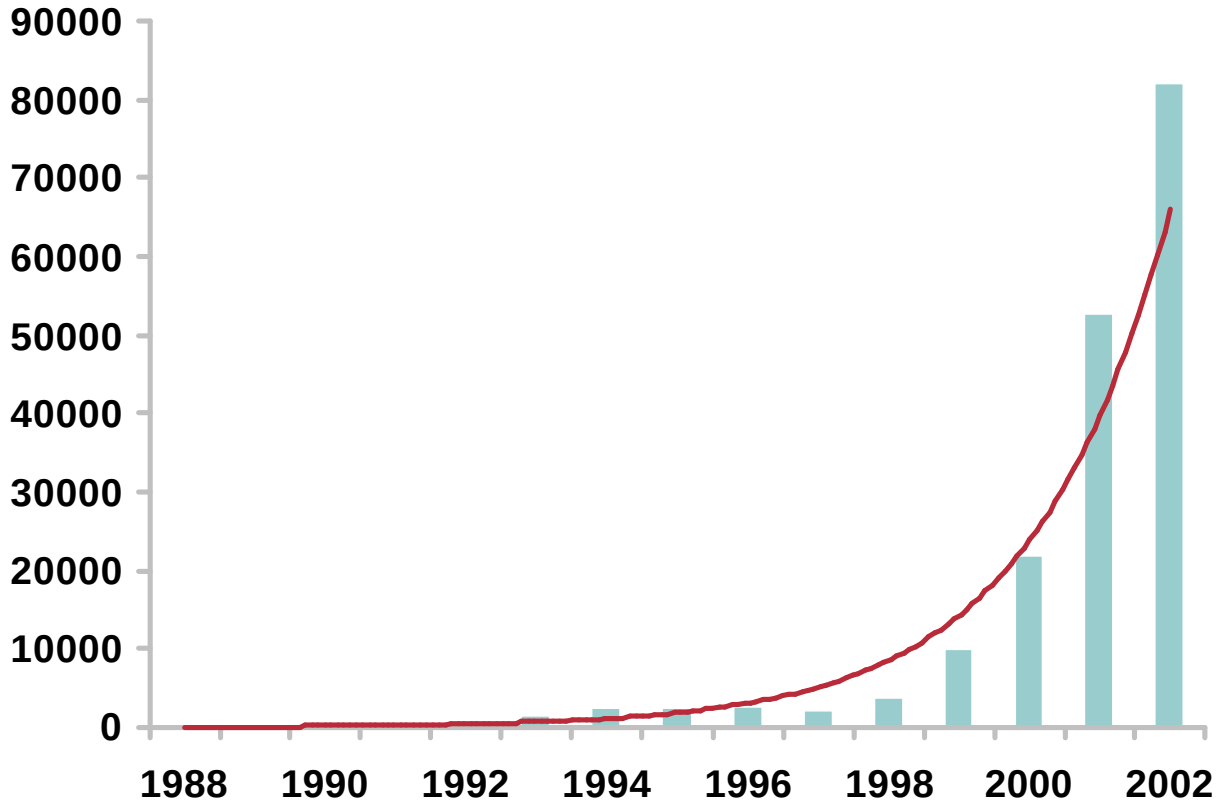
Compare This to the Cost of Implementing a Comprehensive Security Solution!

Source: FBI 2002 Report on Computer Crime

Number of Incidents Always on the Rise

CERT—Number of Incidents Reported (*)

http://www.cert.org/stats/cert_stats.html#incidents



(*) An Incident May Involve One Site or Hundreds (or Even Thousands) of Sites; Also, Some Incidents May Involve Ongoing Activity for Long Periods of Time

Two of the Most Serious Intruder Activities Reported to the CERT/CC in 2002

- **Exploitation of vulnerabilities in Microsoft SQL Server**

  Intruders compromised systems through the automated exploitation of null or weak default SA passwords in Microsoft SQL Server and Microsoft Data Engine; the CERT/CC published advice on protecting systems that run Microsoft SQL Server in CA-2002-04 (February 25, 2002)

  In July 2002, intruders continued to compromise systems and obtain sensitive information by exploiting several serious vulnerabilities in the Microsoft SQL Server; the CERT/CC published additional advice in CA-2002-22 (July 29, 2002)

- **Apache/mod_ssl Worm**

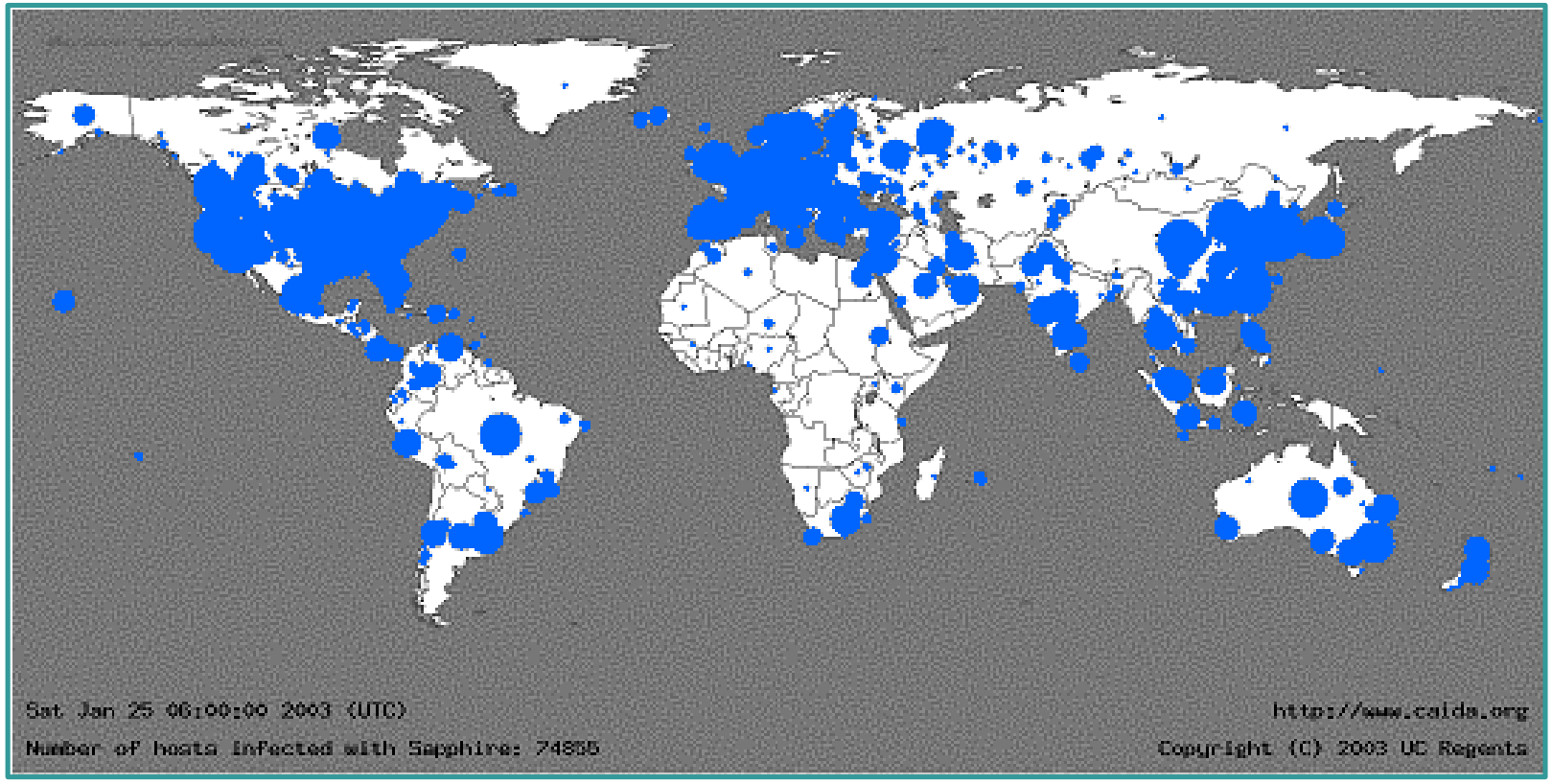
  Intruders used a piece of self-propagating malicious code (referred to here as Apache/mod_ssl) to exploit a vulnerability in OpenSSL, an open-source implementation of the Secure Sockets Layer (SSL) protocol

  The CERT/CC initially published CA-2002-23 (July 30, 2002), describing four vulnerabilities in OpenSSL that could be used to create denial of service; when these and other vulnerabilities finally manifested themselves in the form of the Apache/mod_ssl Worm, the CERT/CC published advice in CA-2002-27 (September 14, 2002)

The SQL Slammer Worm: What Happened?

- **Released at 5:30 GMT, January 25, 2003**
- **Saturation point reached within 2 hours of start of infection**
- **250,000–300,000 hosts infected**
- **Internet connectivity affected worldwide**

The SQL Slammer Worm: 30 Minutes after “Release”



- Infections doubled every 8.5 seconds
- Spread 100x faster than Code Red
- At peak, scanned 55 million hosts per second

Network Effects of the SQL Slammer Worm

- Several service providers noted significant bandwidth consumption at peering points
- Average packet loss at the height of infections was 20%
- Country of South Korea lost almost all Internet service for period of time
- Financial ATMs were affected
- SQL Slammer overwhelmed some airline ticketing systems

Agenda

Cisco.com

- Security Year in Review
  - Slammer, et. al.
- Security Policy
  - Setting a Good Foundation
- Extended Perimeter Security
  - Define the Perimeter, Firewalls, ACLs
- Identity Services
  - Passwords, Tokens, PKI, Biometrics
- Secure Connectivity
  - Work Happens Everywhere, Virtual Private Networks
- Intrusion Protection
  - Network, Host
- Security Management
  - Wrapping it All Together

Security Policy

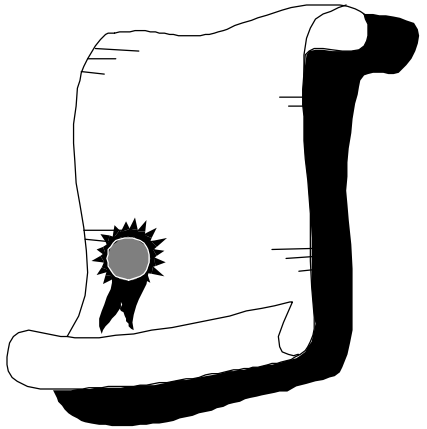
- Setting a good foundation
- What is a security policy
- Why create a security policy
- What should it contain

Start with a Security Policy

- **Security policy defines and sets a good foundation by:**
  - **Definition—Define data and assets to be covered by the security policy**
  - **Identity—How do you identify the hosts and applications affected by this policy?**
  - **Trust—Under what conditions is communication allowed between networked hosts?**
  - **Enforceability—How will the policies implementation be verified?**
  - **Risk Assessment—What is the impact of a policy violation? How are violations detected?**
  - **Incident Response—What actions are required upon a violation of a security policy?**

What Is a Security Policy?

"A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide."



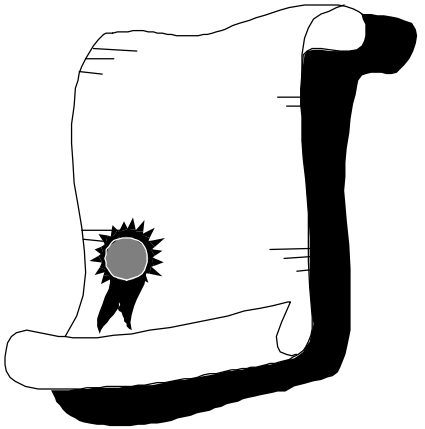
RFC 2196, Site Security Handbook

Why Create a Security Policy?

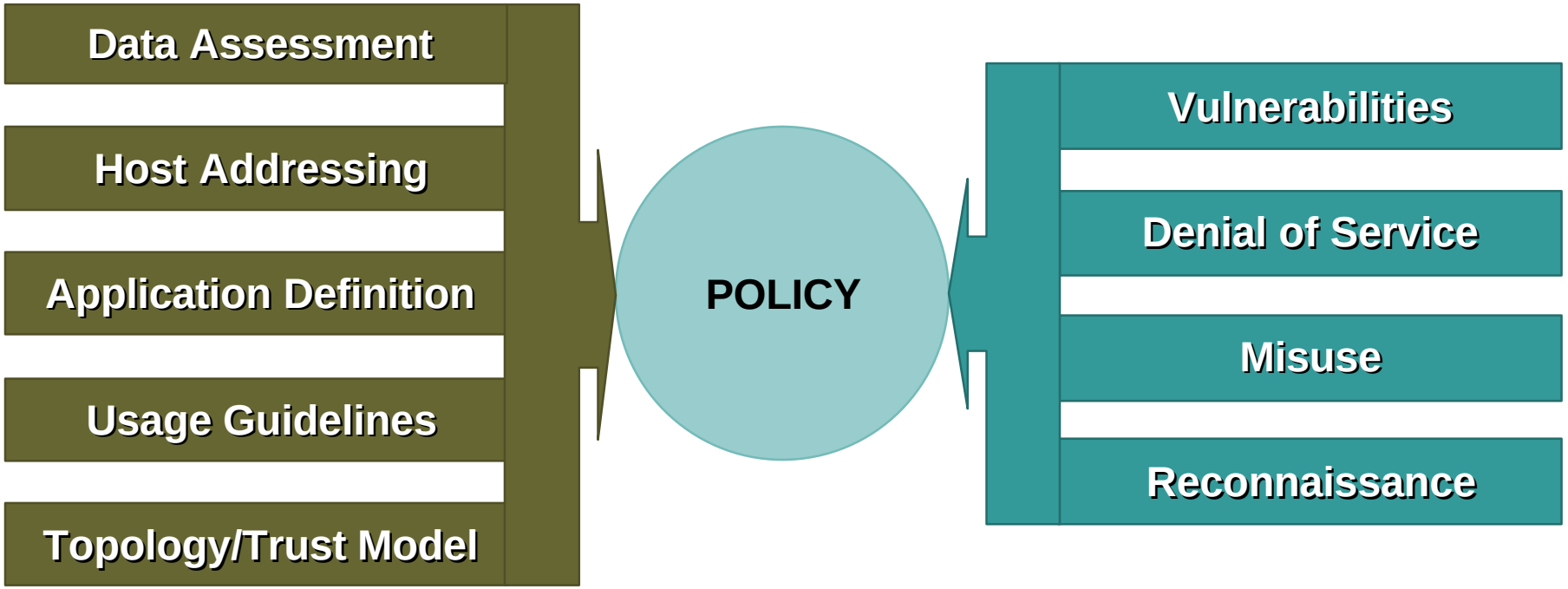
- To create a baseline of your current security posture
- To set the framework for security implementation
- To define allowed and not allowed behaviors
- To help determine necessary tools and procedures
- To communicate consensus and define roles
- To define how to handle security incidents

What Should the Security Policy Contain?

- Statement of authority and scope
- Acceptable use policy
- Identification and authentication policy
- Internet use policy
- Campus access policy
- Remote access policy
- Incident handling procedure



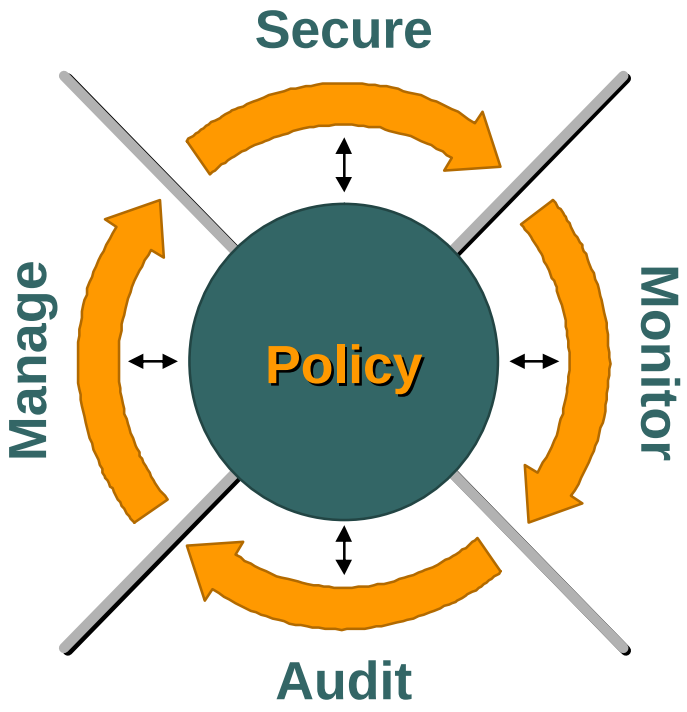
Security Policy Elements



- On the left are the network design factors upon which security policy is based
- On the right are basic Internet threat vectors toward which security policies are written to mitigate

Enforcement

- **Secure**
  - Identity and authentication
  - Filtering and stateful inspection
  - Encryption and VPNs
- **Monitor**
  - Intrusion detection and response
  - Content-based detection and response
  - Employee monitoring
- **Audit**
  - Security posture assessment
  - Vulnerability scanning
  - Patch verification/application auditing
- **Manage**
  - Secure device management
  - Event/data analysis and reporting
  - Network security intelligence



Security Wheel

Risk Assessment

- **Some elements of network security are absolute, others must be weighed relative to the potential risk**
  - **When you connect to the Internet, the Internet connects back to you**
- **Sound operational procedures and management are easier to implement than technical solutions**
  - **You can't secure a bad idea**
- **The cost of secure solutions must be factored into the overall Return on Investment (ROI)**
  - **Security must be included in planning and design**
  - **Effective security requires managerial commitment**

What Is Trust?

- Trust is the inherent ability for hosts to communicate within a network design
- Trust and risk are opposites; security is based on enforcing and limiting trust
- Within subnets, trust is based on Layer 2 forwarding mechanisms
- Between subnets, trust is based on Layer 3+ mechanisms

Incident Response

Cisco.com

- **Attacks are intentional, there are no accidental or stray IP packets**
- **Four levels of incident response:**
  - **Network misuse**
  - **Reconnaissance**
  - **Attack**
  - **Compromise**
- **Without incident response plans, only passive defenses have value**

Agenda

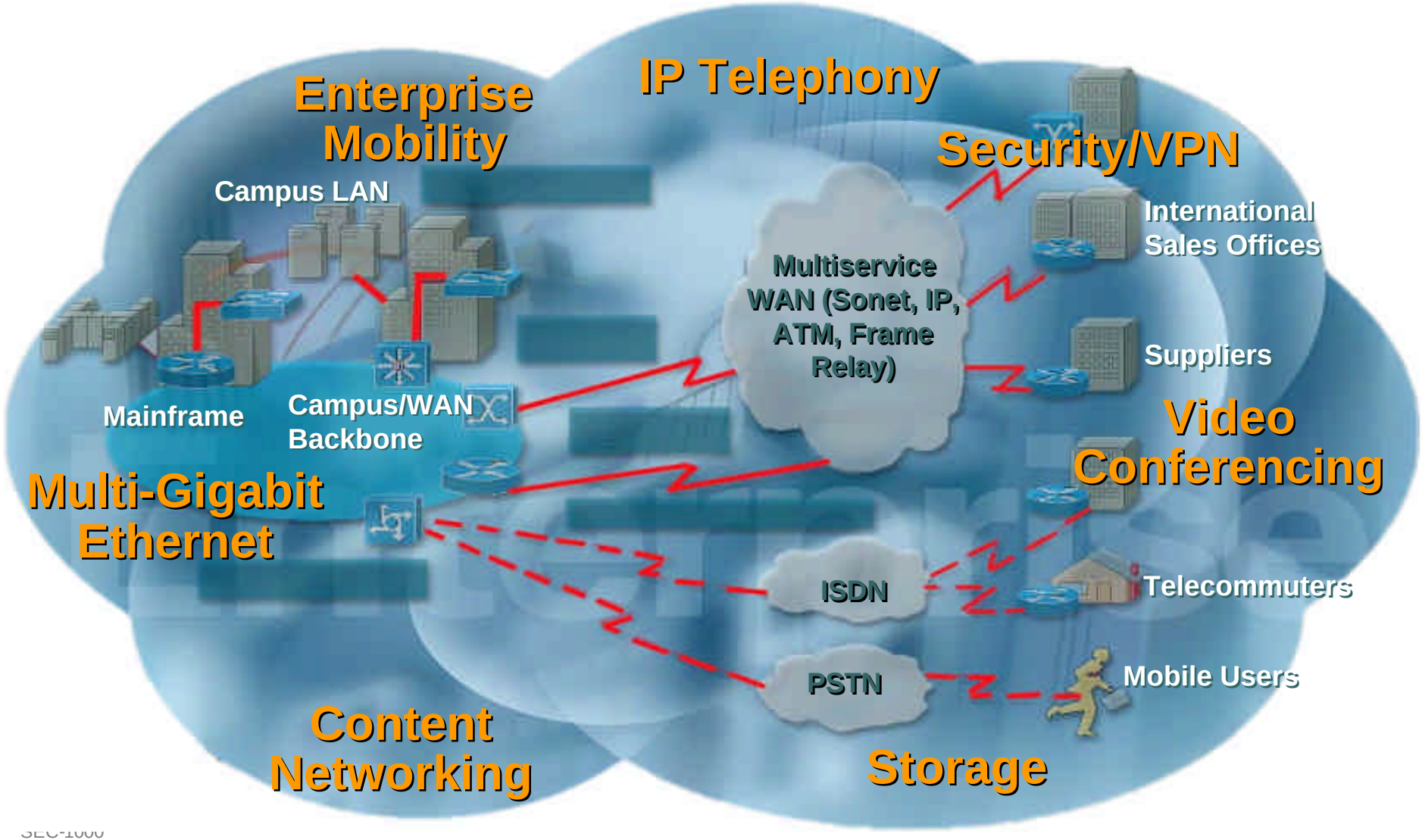
Cisco.com

- **Security Year in Review**
  - Slammer, et. al.
- **Security Policy**
  - Setting a Good Foundation
- **Extended Perimeter Security**
  - Define the Perimeter, Firewalls, ACLs
- **Identity Services**
  - Passwords, Tokens, PKI, Biometrics
- **Secure Connectivity**
  - Work Happens Everywhere, Virtual Private Networks
- **Intrusion Protection**
  - Network, Host
- **Security Management**
  - Wrapping it All Together

Extended Perimeter Security

- **Can you define the perimeter?**
  - **Dissimilar policy boundaries**
- **Access control**
- **Firewalls—first line of defense**

Can You Define the Perimeter?

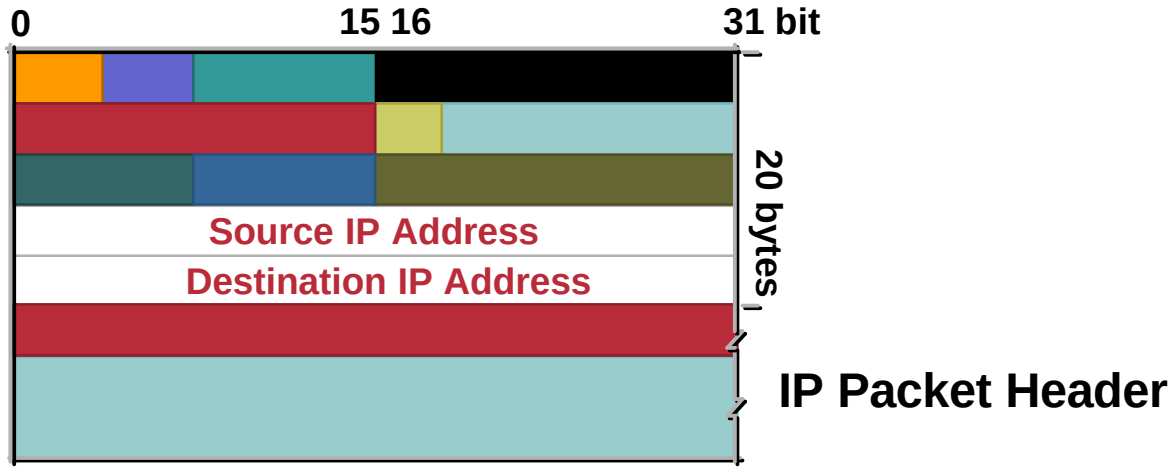


Filtering Network Traffic

- **Examining the flow of data across a network**
- **Types of flows:**
  - **Packets**
  - **Connections**
  - **State**

Access Control Lists (ACLs)

- **Simple ACLs look at information in IP packet headers**



- **Many filters are based on the packets Source and Destination IP address**
- **Extended ACLs look further into the packet or at the TCP or UDP port number in use for the TCP/IP connection between hosts**

The Evolution of ACLs…

- **Dynamic ACLs**

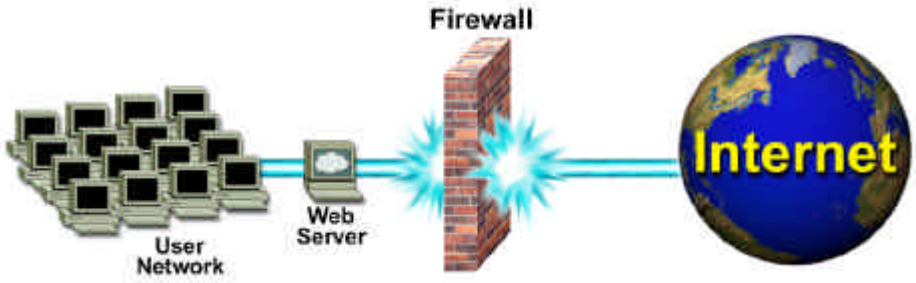
  Lock-and-key filtering (Dynamic ACLs) allows an authenticated user to pass traffic that would normally be blocked at the router

- **Reflexive ACLs**

  Creates a temporary ACL to allows specified IP packets to be filtered based on TCP or UDP session information; the ACL "expires" shortly after the session ends (no sequence #)

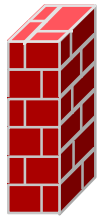
Firewalls

- **Four types of firewalls**
  - **Proxies (application-layer firewalls)**
  - **Stateful**
  - **Hybrid**
  - **Personal**
- **Implementation methods**
  - **Software**
  - **Appliance**



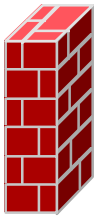
Proxy Firewalls

- 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
- Also provide significant logging and auditing capabilities
- For HTTP (application specific) proxies all web browsers must be configured to point at proxy server
- Example Microsoft ISA Server



Stateful Firewalls

- **Access Control Lists plus…**
- **Maintaining state**



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

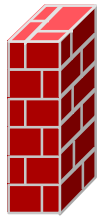
To adequately maintain the state of a connection the firewall needs to inspect every packet

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

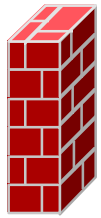
Hybrid Firewalls

- **Hybrid firewalls combine features of other firewall approaches such as…**
  - **Access Control Lists**
  - **Application specific proxies**
  - **State tables**
- **Plus features of other devices…**
  - **Web (HTTP) cache**
  - **Specialized servers SSH, SOCKS, NTP**
  - **May include VPN, IDS**



Personal Firewalls

- **Personal firewalls**
  - **Protecting remote users/home users**
  - **Watching inbound/outbound traffic**
  - **Creating basic rules**



- **Example—ZoneAlarm**

Agenda

Cisco.com

- **Security Year in Review**
  - Slammer, et. al.
- **Security Policy**
  - Setting a Good Foundation
- **Extended Perimeter Security**
  - Define the Perimeter, Firewalls, ACLs
- **Identity Services**
  - Passwords, Tokens, PKI, Biometrics
- **Secure Connectivity**
  - Work Happens Everywhere, Virtual Private Networks
- **Intrusion Protection**
  - Network, Host
- **Security Management**
  - Wrapping it All Together

Identity Services

Cisco.com

- User identity
- Passwords
- Tokens
- PKI
- Biometrics

User Identity

- **Mechanisms for proving who you are**
  - **Both people and devices can be authenticated**
- **Three authentication attributes:**
  - **Something you know**
  - **Something you have**
  - **Something you are**
- **Common approaches to Identity:**
  - **Passwords**
  - **Tokens**
  - **Certificates**

Validating Identity

Cisco.com

- **Identity within the network is based overwhelmingly on IP Layer 3 and 4 information carried within the IP packets themselves**
  - **Application-level user authentication exists, but is most commonly applied on endpoints**
- **Therefore, identity validation is often based on two mechanisms:**
  - **Rule matching**
  - **Matching existing session state**
- **Address and/or session spoofing is a major identity concern**

Passwords

- **Correlates an authorized user with network resources**

Passwords

Cisco.com

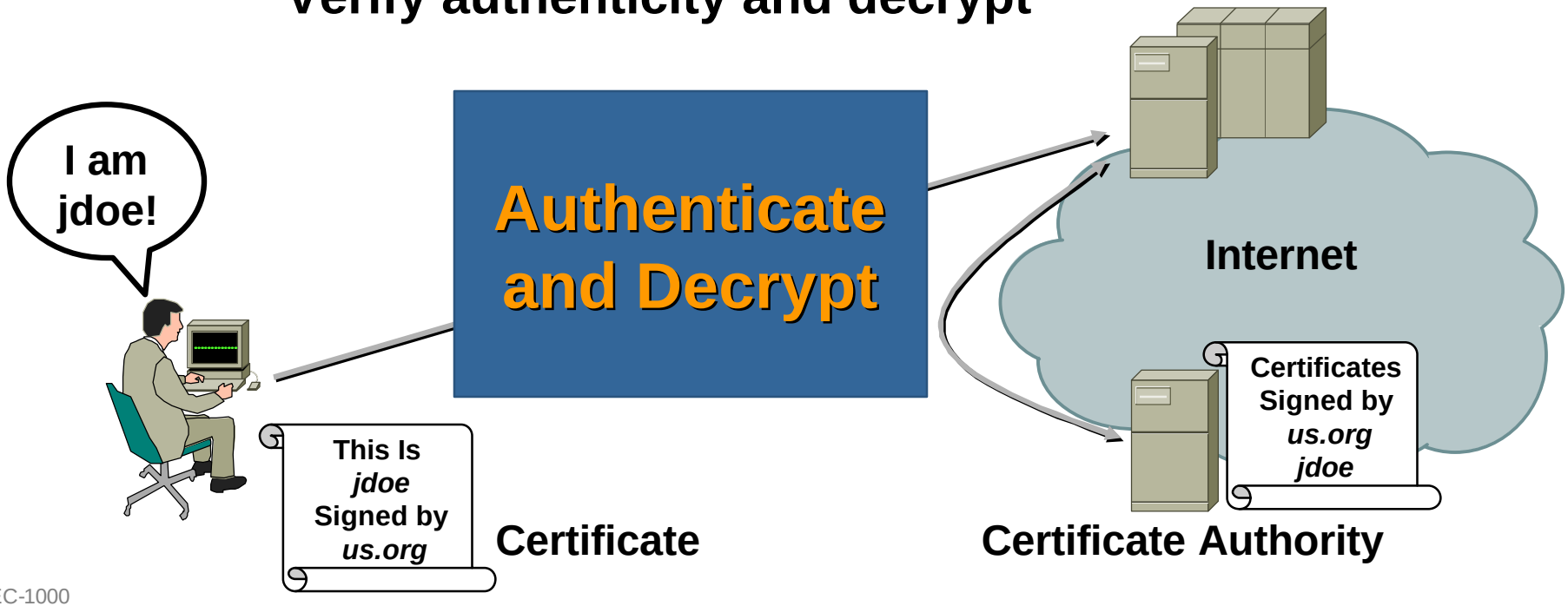
- **Passwords have long been, and will continue to be a problem**
- **People will do what is easiest**
- **Create and enforce good password procedures**
  - **Non-dictionary passwords**
  - **Changed often (90–120 days)**
- **Passwords are like underwear—they should be changed often and neither hung from your monitor or hidden under your keyboard**

Tokens

- **Strong (2-factor) Authentication based on “something you know” and “something you have”**

Public Key Infrastructure (PKI)

- **Relies on a two-key system**
  - **J Doe signs a document with his private key**
  - **Person who receives that document uses JDoe's public key to:**
    - **Verify authenticity and decrypt**



Biometrics

- **Authentication based on physiological or behavioral characteristics**
  - **Features can be based on:**
    - **Face**
    - **Fingerprint**
    - **Eye**
    - **Hand geometry**
    - **Handwriting**
    - **Voice**

- **Becoming more accepted and widely used**
  - **Already used in government, military, retail, law enforcement, health and social services, etc.**

Agenda

- **Security Year in Review**
  - Slammer, et. al.
- **Security Policy**
  - Setting a Good Foundation
- **Extended Perimeter Security**
  - Define the Perimeter, Firewalls, ACLs
- **Identity Services**
  - Passwords, Tokens, PKI, Biometrics
- **Secure Connectivity**
  - Work Happens Everywhere, Virtual Private Networks
- **Intrusion Protection**
  - Network, Host
- **Security Management**
  - Wrapping It All Together

Secure Connectivity

- **Work happens everywhere!**
- **Virtual Private Networks**

Work Happens Everywhere

Increasing Need for Transparent Corporate Connectivity

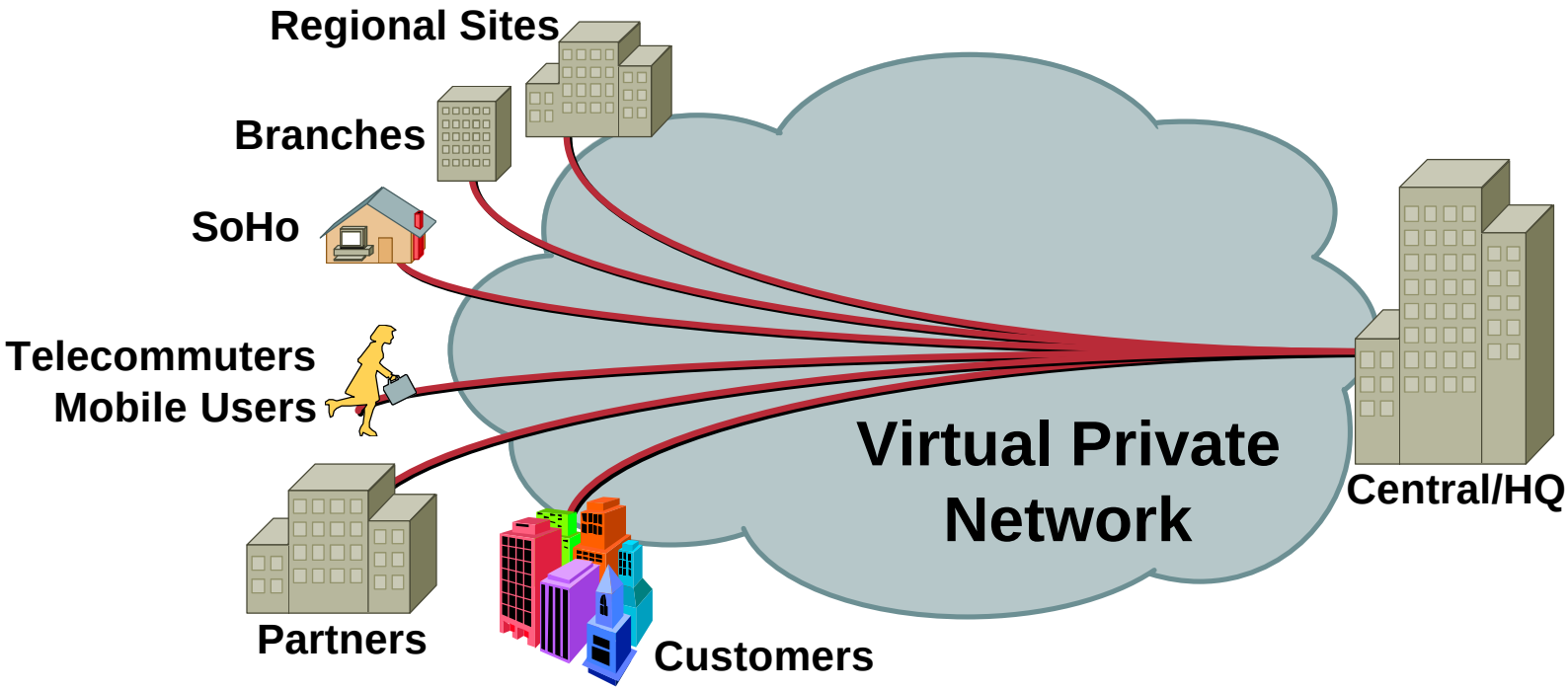
Cisco.com

- **On the road (hotels, airports, convention centers)**
  - **280 million business trips a year**
  - **Productivity decline away from office >60–65%**
- **At home (teleworking)**
  - **137 million telecommuters by 2003**
  - **40% of U.S. telecommuters from large or mid-size firms**
- **At work (branch offices, business partners)**
  - **E-business requires agile networks**
  - **Branch offices should go where the talent is**

Source: On the Road (TIA Travel Poll, 11/99); At Home (Gartner 2001, Cahners Instat 5/01); At Work (Wharton Center for Applied Research)

What Are VPNs?

- **A network built on a less expensive shared infrastructure with the same policies and performance as a private network**



Secure Connectivity

- **Defines “peers”**
  - **Two devices in a network that need to connect**
  - **Tunnel makes peers seem virtually next to each other**
  - **Ignores network complexity in between**
- **Technologies**
  - **PPTP—Point-to-Point Tunneling Protocol**
  - **L2TP—Layer 2 Tunneling Protocol**
  - **IPSec**
  - **Secure shell**
  - **SSL**

Encryption

- **Symmetric Cryptography**

  Uses a shared secret key to encrypt and decrypt transmitted data

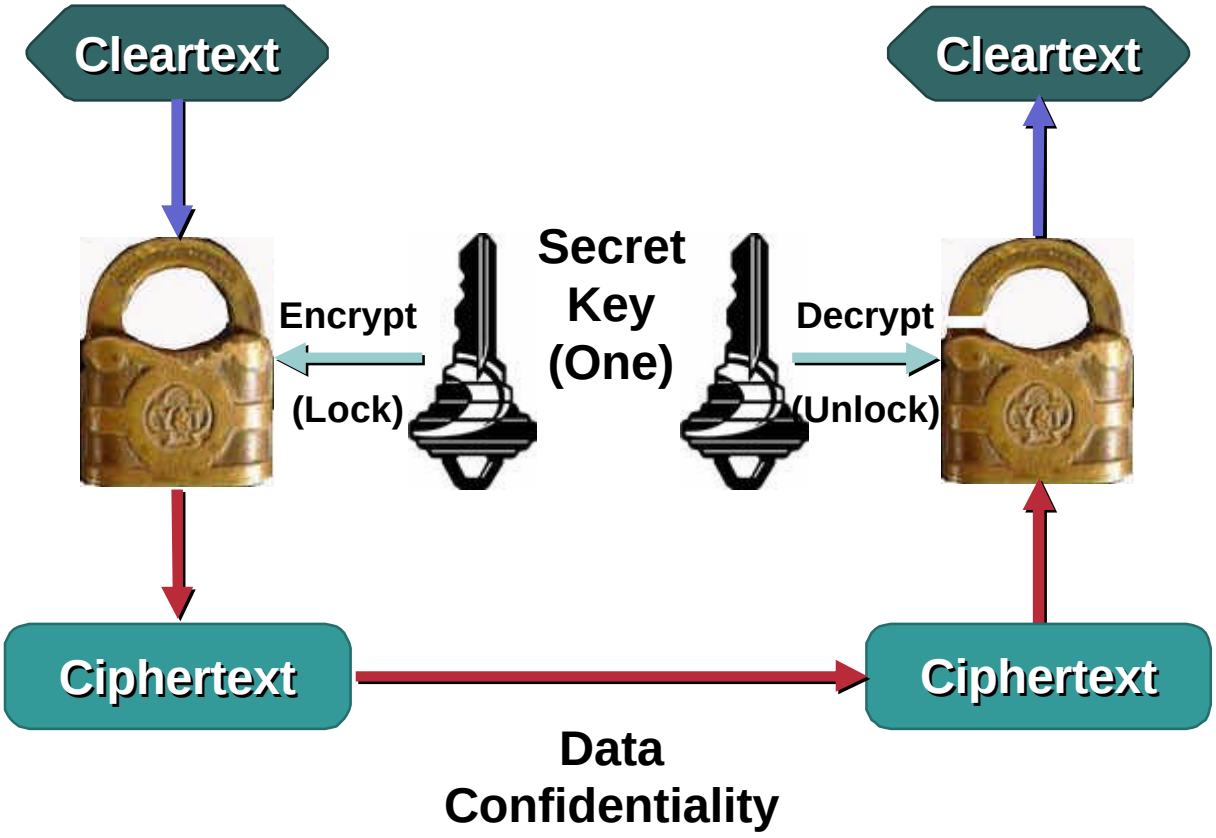
  Data flow is bidirectional

- **Provides data confidentiality only**

  Does not provide data integrity or non-repudiation

- **Examples: DES, 3DES, AES**

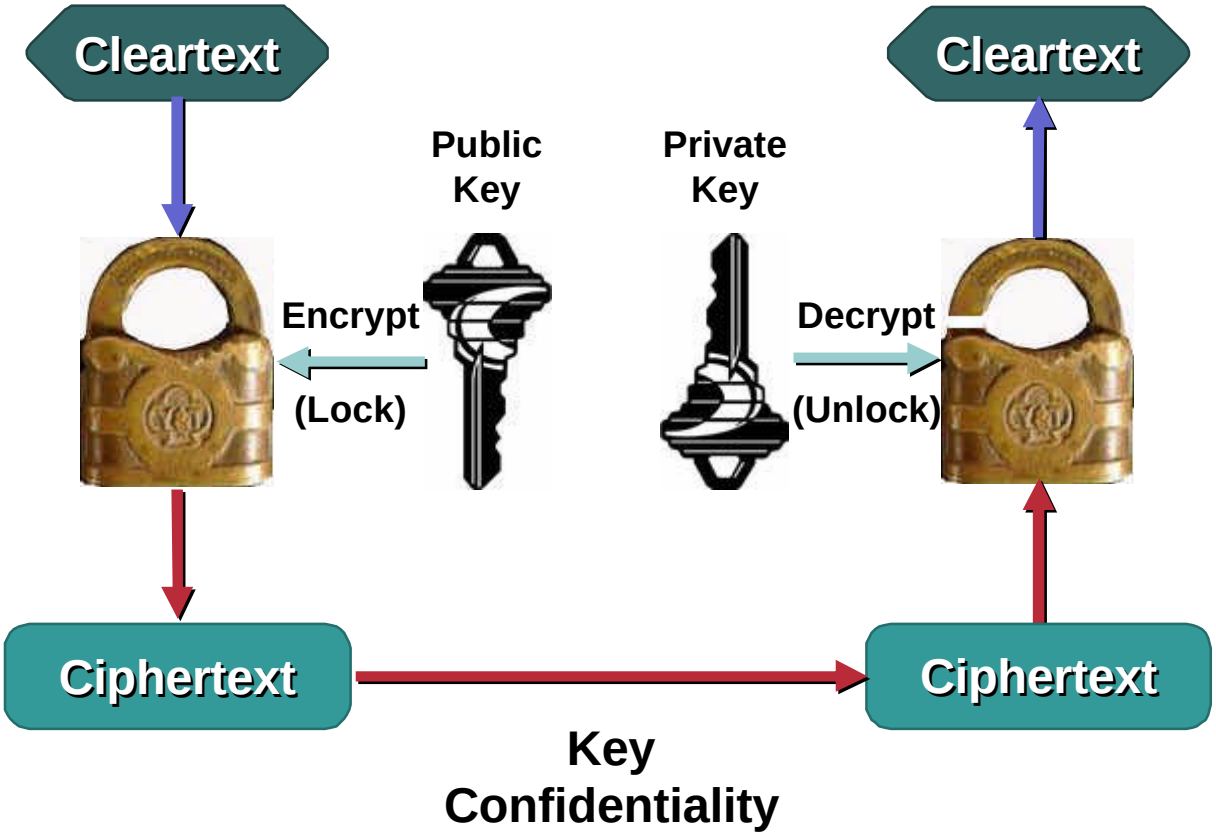
Symmetric Cryptography



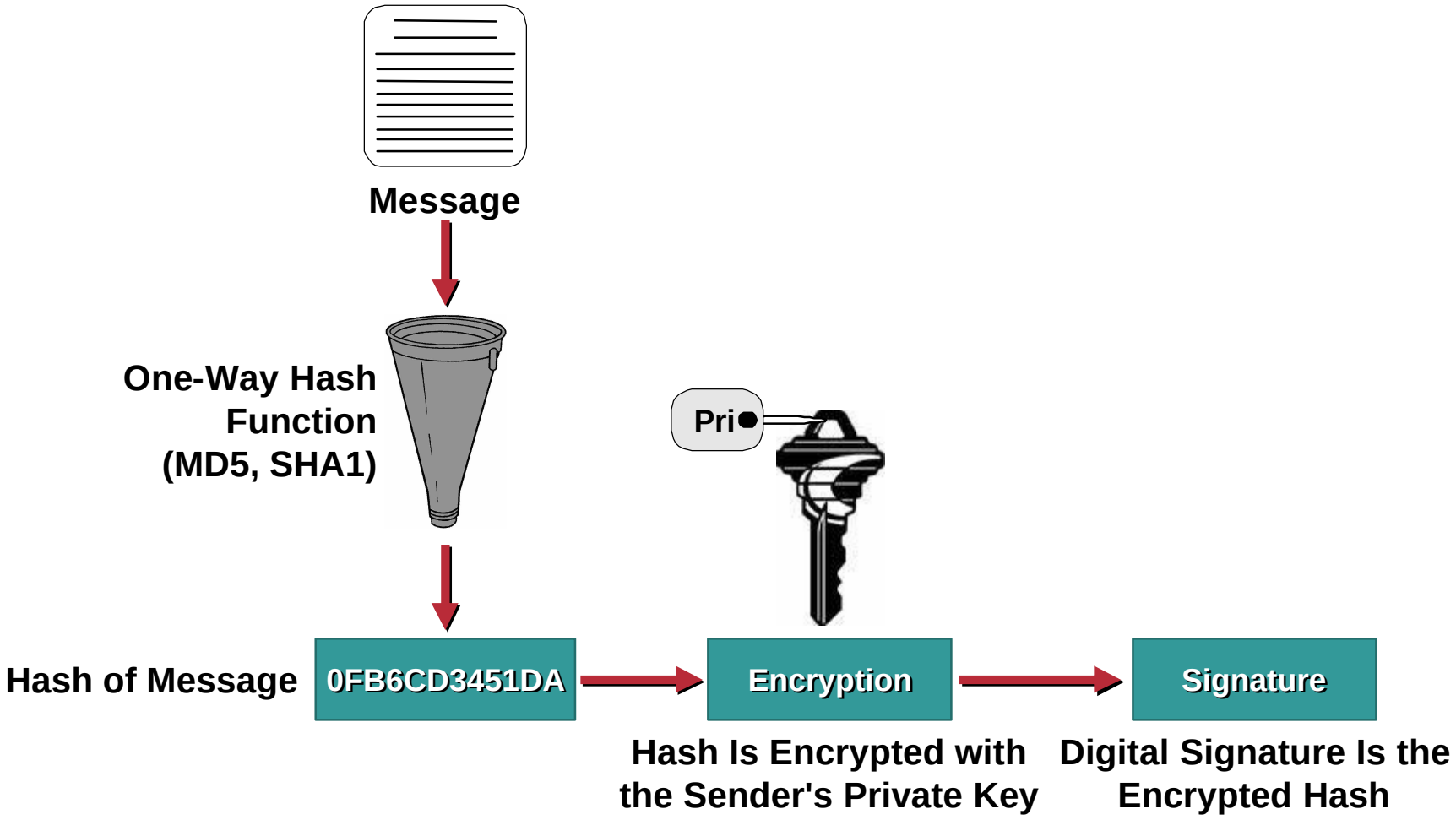
Encryption

- **Asymmetric cryptography**
  - **Also known as Public Key Cryptography**
  - **Utilizes two keys: private and public keys**
  - **Two keys are mathematically related but different values**
- **Computationally intensive**
- **Provides data confidentiality**
  - **Can provide for data integrity as well as non-repudiation**
- **Examples: RSA Signatures**

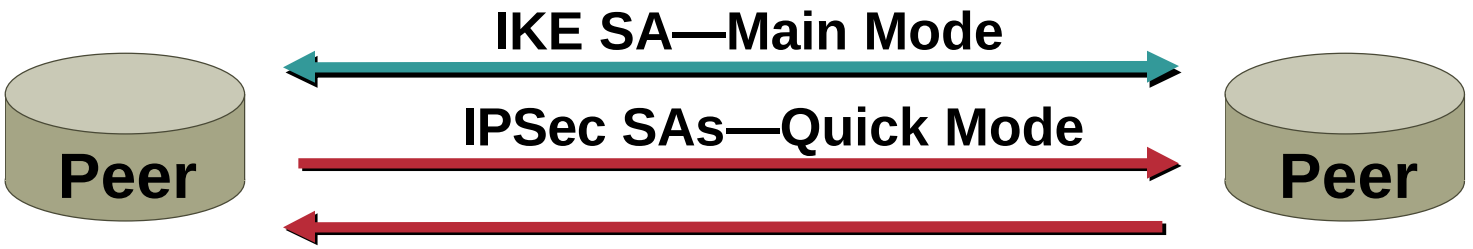
Asymmetric Cryptography



Digital Signatures



Security Association

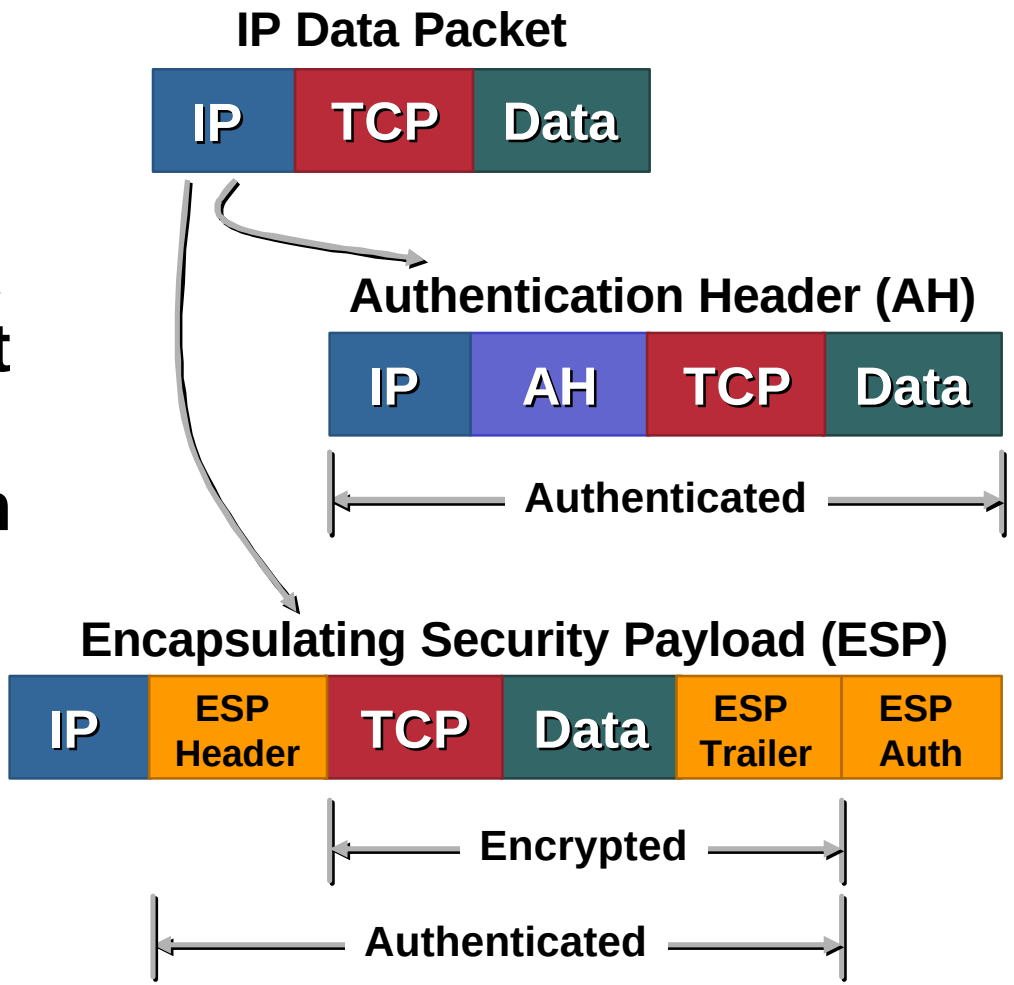


- **A Security Association (SA) is an agreement between two peers on a common security policy, including:**
  - **If and how data will be encrypted**
  - **How entities will authenticate**
  - **Shared session keys**
  - **How long the association will last (lifetime)**
- **Types of security associations**
  - **Uni-directional (IPSec SAS)**
  - **Bi-directional (IKE SAS)**

What Is IPSec?

- **IPSec: An IETF standard* framework for the establishment and management of data privacy between network entities**

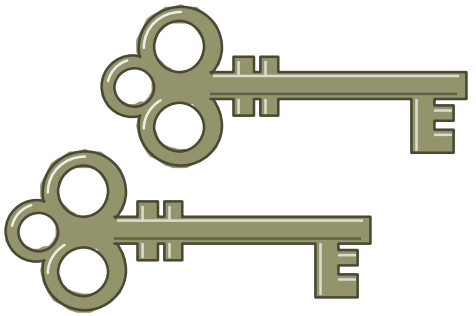
  IPSec is an evolving standard



***RFC 2401–2412**

Key Management

- **IKE = Internet Key Exchange protocols**
- **Public key cryptosystems enable secure exchange of private crypto keys across open networks**
- **Re-keying at appropriate intervals**



An IPSec VPN Is…

- **IPSec provides the framework that lets you negotiate exactly which options to use**
  - **IPSec provides flexibility to address different networking requirements**
- **A VPN which uses IPSec to insure data authenticity and confidentiality**
  - **AH provides authenticity**
  - **ESP provides authenticity and confidentiality**
- **The IPSec framework is open and can accommodate new encryption and authentication techniques**

Agenda

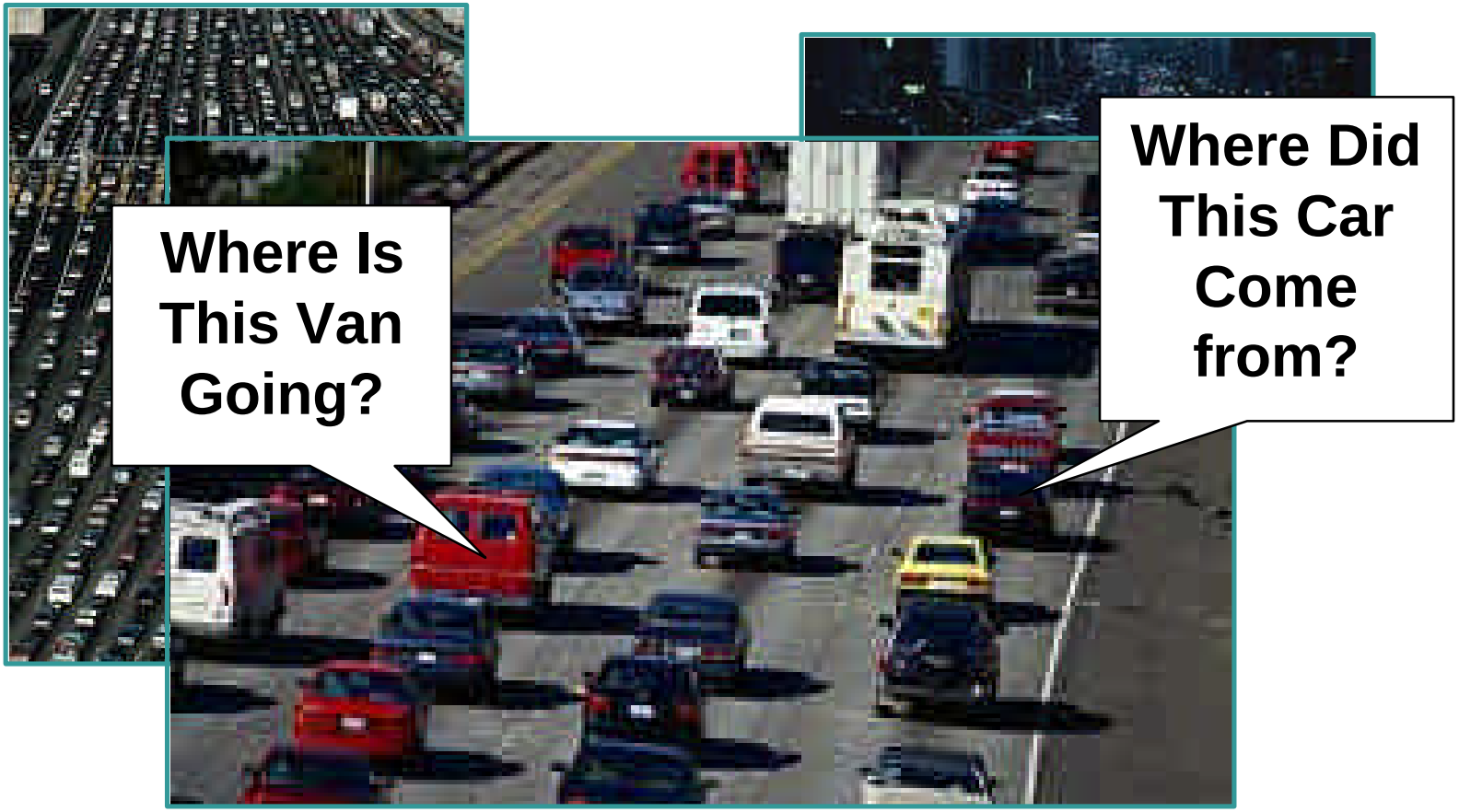
Cisco.com

- **Security Year in Review**
  - Slammer, et. al.
- **Security Policy**
  - Setting a Good Foundation
- **Extended Perimeter Security**
  - Define the Perimeter, Firewalls, ACLs
- **Identity Services**
  - Passwords, Tokens, PKI, Biometrics
- **Secure Connectivity**
  - Work Happens Everywhere, Virtual Private Networks
- **Intrusion Protection**
  - Network, Host
- **Security Management**
  - Wrapping It All Together

Intrusion Protection

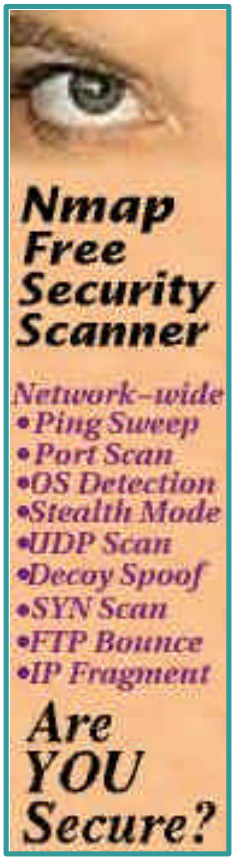
- Monitoring the network and hosts
- Network scanning
- Packet sniffing
- Intrusion detection primer

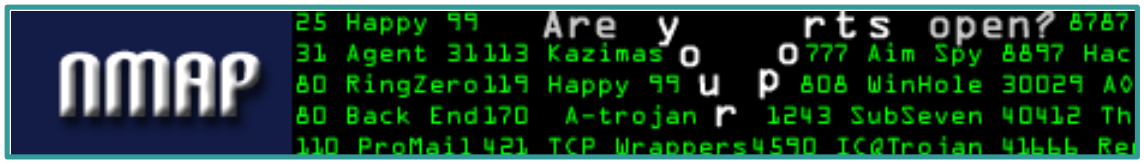
Monitoring



Network Scanning

- **"Active" tool**
  - **Identifies devices on the network**
  - **Useful in network auditing**
- **"Fingerprinting"**
  - **How a scanner figures out what OS and version is installed**
- **Examples: Nmap, Nessus**



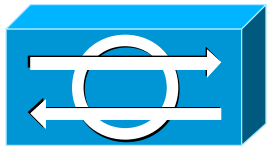


Packet Sniffing

- **Diagnostic tools**
  - **Used capture packets**
  - **Used to examine packet data (filters)**
  - **Can reconstruct sessions and streams**
- **Sniffers can be “promiscuous”**
  - **Passive, listening**
- **Examples: Sniffer, Ethereal**

Intrusion Detection

- **Create a system of distributed "promiscuous" Sniffer-like devices**
  - **Watching activity on a network and specific hosts**
- **Different approaches**
  - **Protocol anomaly/signature detection**
  - **Host-based/network-based**



- **Different IDS technologies can be combined to create a better solution**

Terminology

Cisco.com

- **False positives: System mistakenly reports certain benign activity as malicious**
- **False negatives: System does not detect and report actual malicious activity**

Intrusion Detection Approaches

Cisco.com

Misuse/Signature vs. Anomaly Detection

Network vs. Host-Based

Anomaly vs. Signature Detection

- **Anomaly detection: Define normal, authorized activity, and consider everything else to be potentially malicious**
- **Misuse/signature detection: Explicitly define what activity should be considered malicious**

  Most commercial IDS products are signature-based

Host vs. Network-Based

Cisco.com

- **Host-based "agent" software monitors activity on the computer on which it is installed**
  - **Cisco HIDS (Okena)—System activity**
  - **TripWire—File system activity**
- **Network-based appliance collects and analyzes activity on a connected network**
- **Integrated IDS**
  - **Network-based IDS functionality as deployed in routers, firewalls, and other network devices**

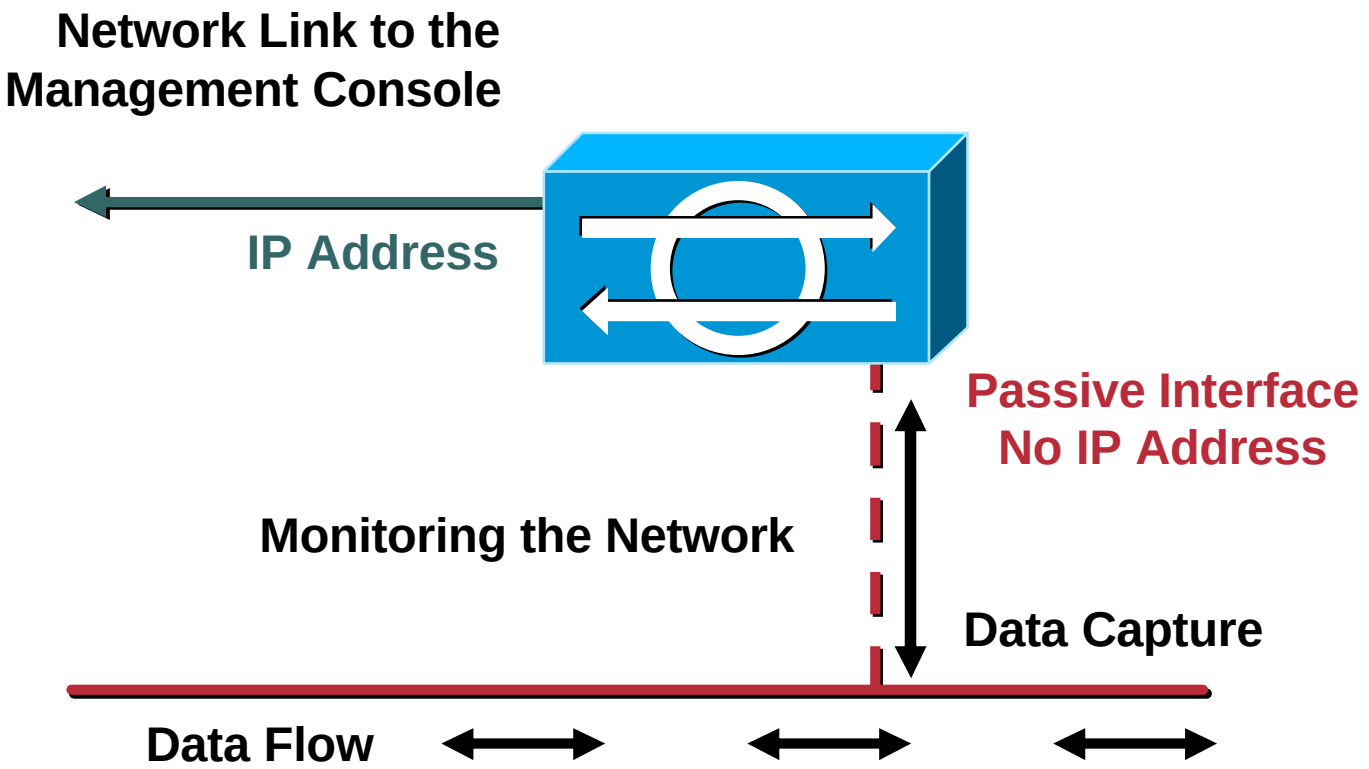
Some General Pros and Cons

Cisco.com

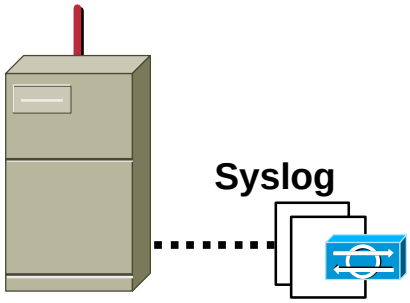
	Pros	Cons
Host-Based	• Can verify success or failure of attack • Generally not impacted by bandwidth or encryption • Understands host context and may be able to stop attack	• Impacts host resources • Operating system dependent • Scalability—requires one agent per host
Network-Based	• Protects all hosts on monitored network • No host impact • Can detect network probes and denial of service attacks	• Switched environments pose challenges • Monitoring multi-gig is currently challenging • Generally can't proactively stop attacks

Should View as Complementary!

Network IDS Sensor



Host IDS Sensor



Passive Agent (OS Sensor)

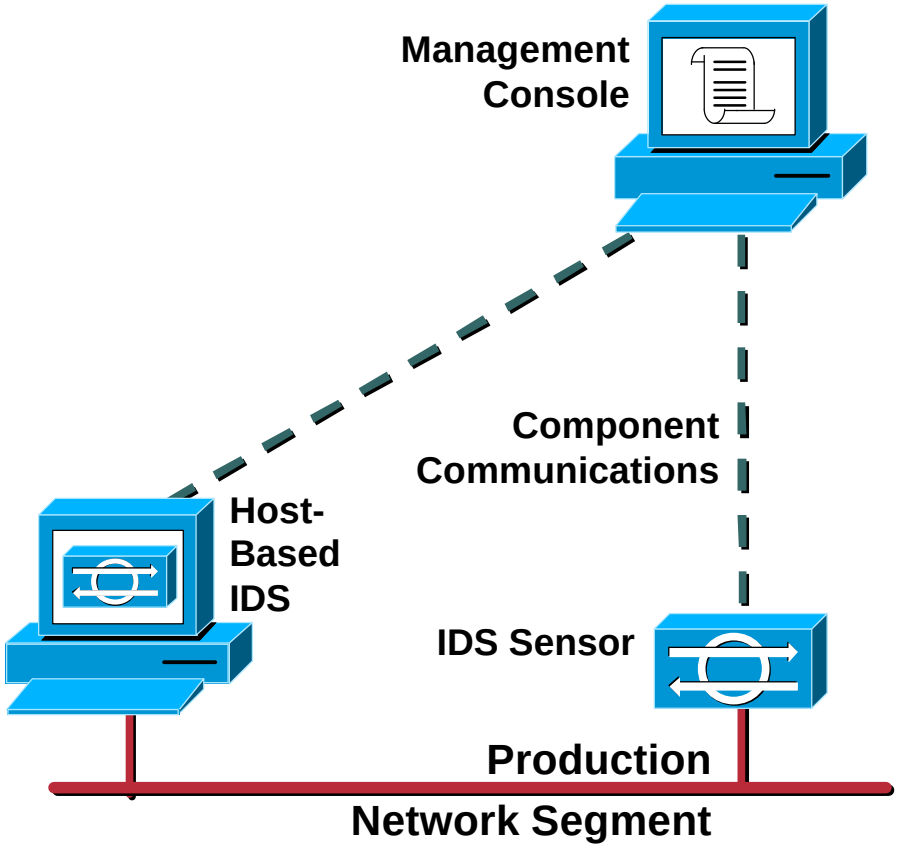
- Syslog monitoring
- Detection
- Wider platform support

Active Agent (Server Sensor)

- Attack interception
- Prevention
- Focused protection

Typical IDS Architecture

- **Management console**
  - Real-time event display
  - Event database
  - Sensor configuration
- **Sensor**
  - Packet signature analysis
  - Generate alarms
  - Response/ countermeasures
- **Host-based**
  - Generate alarms
  - Response/countermeasures



Too Many Choices?

- **Generally, most efficient approach is to implement network-based IDS first**
  - **Easier to scale and provides broad coverage**
  - **Less organizational coordination required**
  - **No host/network impact**
- **May want to start with host-based IDS if you only need to monitor a couple of servers**
- **Vast majority of commercial IDS is signature-based**
- **Keep in mind that IDS is not the "security panacea"**

Agenda

Cisco.com

- **Security Year in Review**
  - Slammer, et. al.
- **Security Policy**
  - Setting a Good Foundation
- **Extended Perimeter Security**
  - Define the Perimeter, Firewalls, ACLs
- **Identity Services**
  - Passwords, Tokens, PKI, Biometrics
- **Secure Connectivity**
  - Work Happens Everywhere, Virtual Private Networks
- **Intrusion Protection**
  - Network, Host
- **Security Management**
  - Wrapping It All Together

Security Management

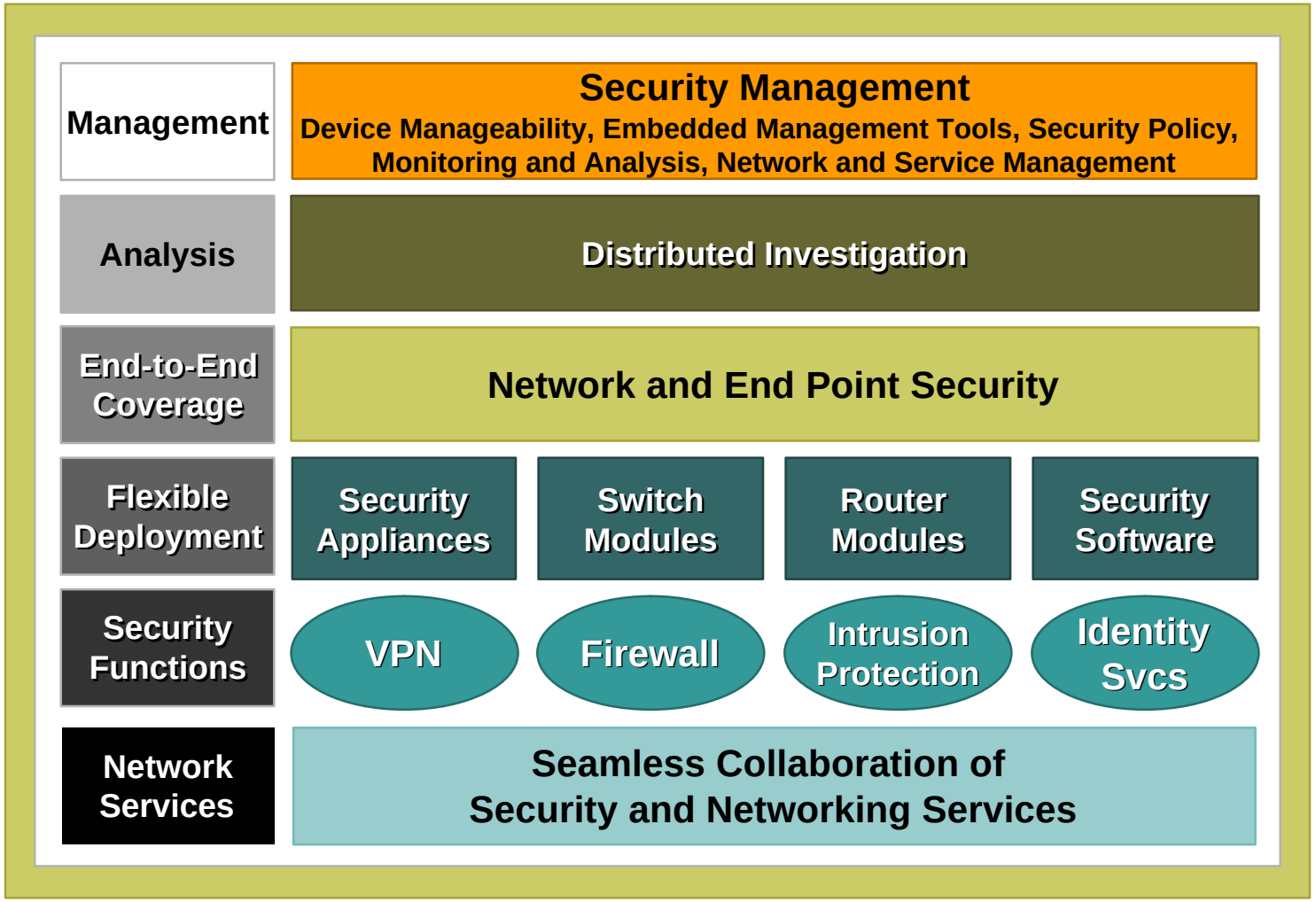
Cisco.com

- **Wrapping it all together**
- **Security management**
  - **Scalable and manageable**
- **Syslog and log analysis**

Wrapping It All Together

- **In the previous sections we discussed:**
  - **Security policy**
  - **Perimeter security and filtering**
  - **Identity services**
  - **Virtual Private Networks**
  - **Intrusion detection and prevention systems**
- **No one system can defend your networks and hosts**
  - **With all this technology, how do we survive?**

Integrated Network Security



Security Management

Cisco.com

- How to manage the network securely
- In-band versus out-of-band management

  In-band management—management information travels the same network path as the data

  Out-of-band management—a second path exists to manage devices; does not necessarily depend on the LAN/WAN
- If you must use in-band, be sure to use

  Encryption

  SSH instead of telnet
- Making sure that policies are in place and that they are working

Syslog

- A protocol that supports the transport of event notification messages
  - Originally developed as part of BSD Unix
- Syslog is supported on most internetworking devices
- BSD Syslog—IETF RFC 3164
  - The RFC documents BSD Syslog observed behavior
- Work continues on reliable and authenticated Syslog
  - http://www.employees.org/~lonvick/index.shtml

Log Analysis

- Log analysis is the process of examining Syslog and other log data
  - Building a baseline of what should be considered normal behavior
  - This is “post event” analysis because it is not happening in real-time
- Log analysis is looking for
  - Signs of trouble
  - Evidence that can be used to prosecute
- If you log it, read and use it!
- Resources
  - http://www.counterpane.com/log-analysis.html

Security = Tools Implementing Policy

Cisco.com

- **Now more than ever**
  - **Identity tools**
  - **Filtering tools**
  - **Connectivity tools**
  - **Monitoring tools**
  - **Management tools**

The Threat Forecast

- **New vulnerabilities and exploits are uncovered everyday**
  - **Subscribe to bugtraq to watch the fun!**
- **Crystal ball**
  - **Attacks will continue**
  - **Greater complexity**
  - **Still see unpatched vulnerabilities taken advantage of**

Conclusions

- Things sound dire!!!
- The sky really is not falling!!!
- Take care of those security issues that you have control over
- Security is a process, not a box!

Security Resources at Cisco

Cisco.com

- **Cisco Connection Online—**

  http://www.cisco.com/go/security

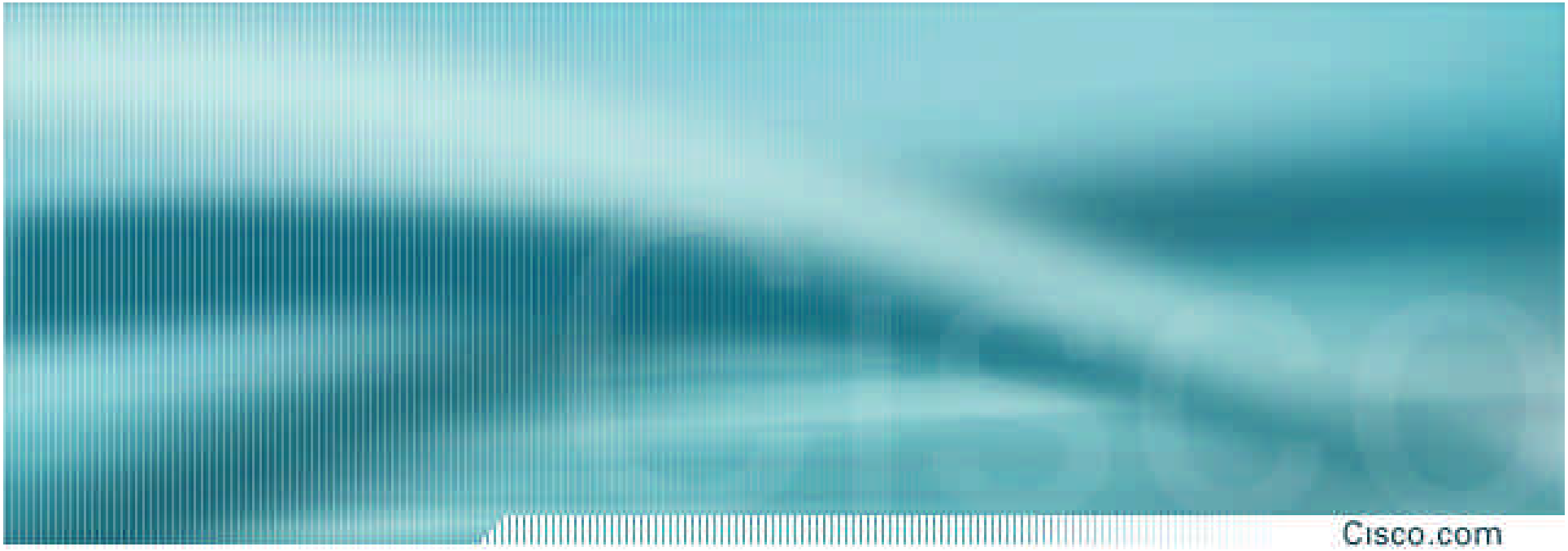
- **Cisco Product Specific Incident Response Team (PSIRT)—**

  http://www.cisco.com/go/psirt

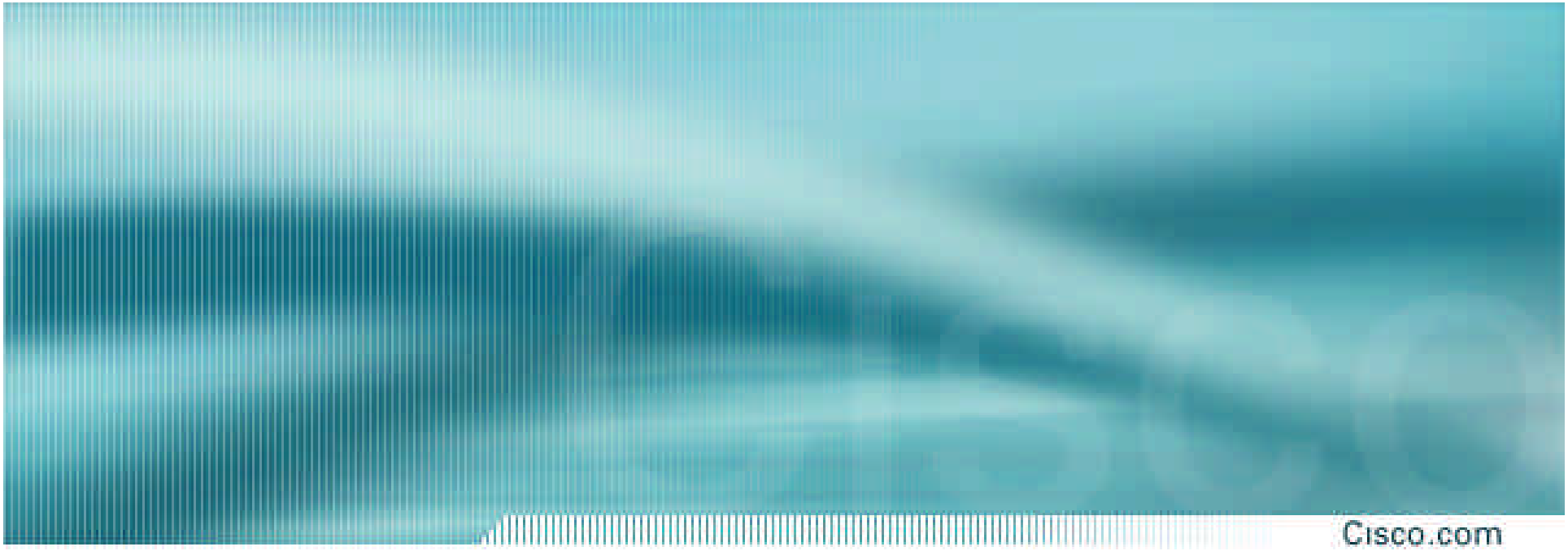
Security Resources on the Internet

Cisco.com

- Cisco Connection Online—http://www.cisco.com
- SecurityFocus.com—http://www.securityfocus.com
- SANS—http://www.sans.org
- CERT—http://www.cert.org
- CIAC—http://www.ciac.org/ciac
- CVE—http://cve.mitre.org
- Computer Security Institute—http://www.gocsi.com
- Center for Internet Security—http://www.cisecurity.org



Thank You



Questions

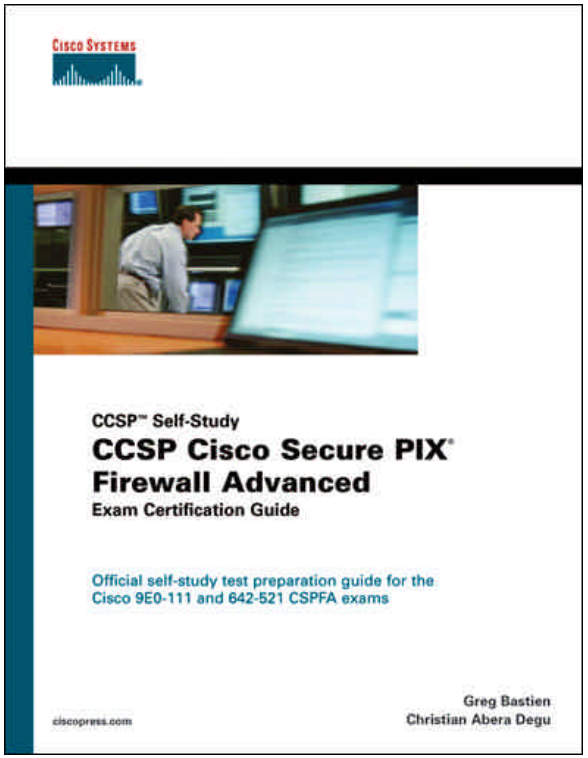
Recommended Reading

Cisco.com

Designing Network Security, Second Ed.
ISBN: 1587051176
Available in Oct 2003

Designing Network Security
ISBN: 1578700434

Managing Cisco Network Security
ISBN: 1578701031



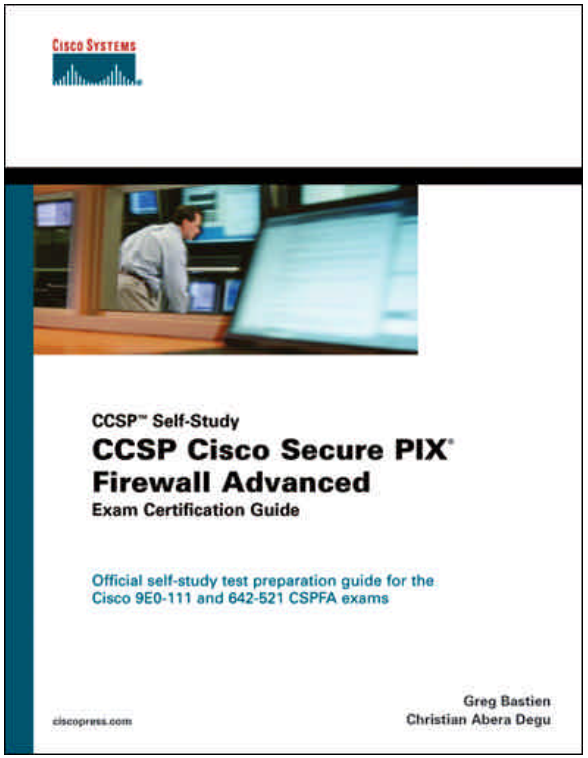
Recommended Reading

Cisco.com

Network Security Principles and Practices
ISBN: 1587050250

Cisco Secure Internet Security Solutions
ISBN: 1587050161

Cisco Secure Intrusion Detection System
ISBN: 158705034X



Recommended Reading

Cisco.com

CCSP Cisco Secure PIX Firewall Advanced Exam Certification Guide
ISBN: 1587200678

CCSP Cisco Secure VPN Exam Certification Guide
ISBN: 1587200708