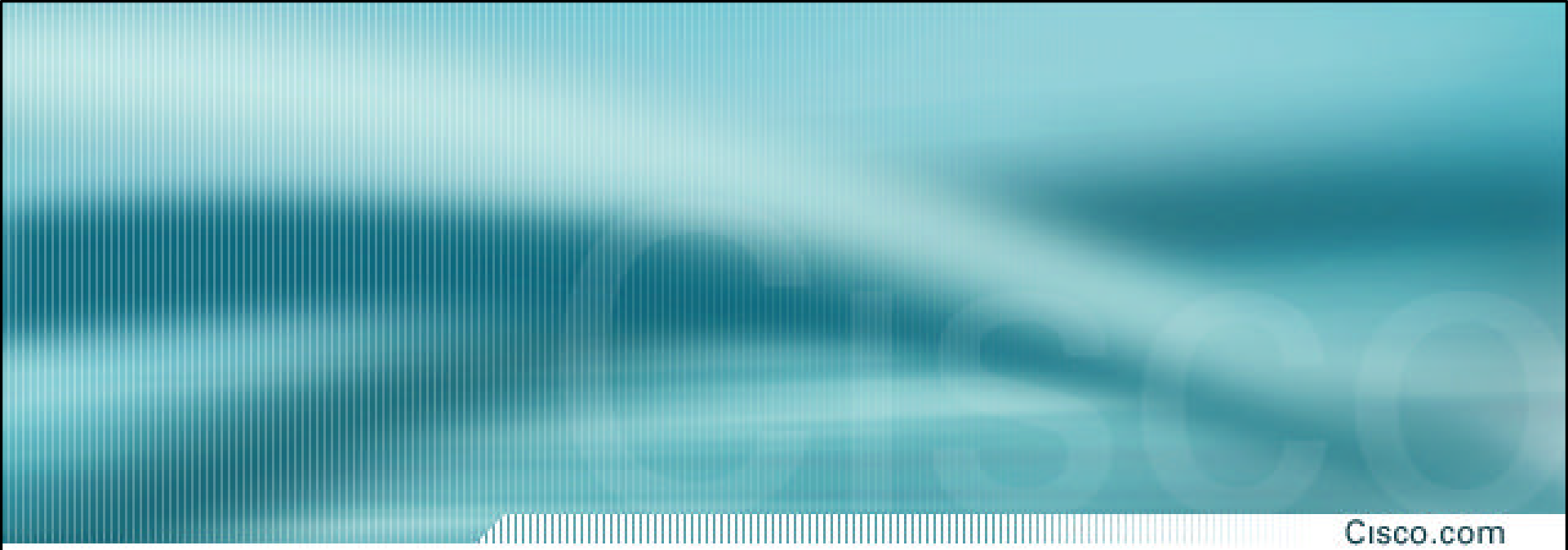


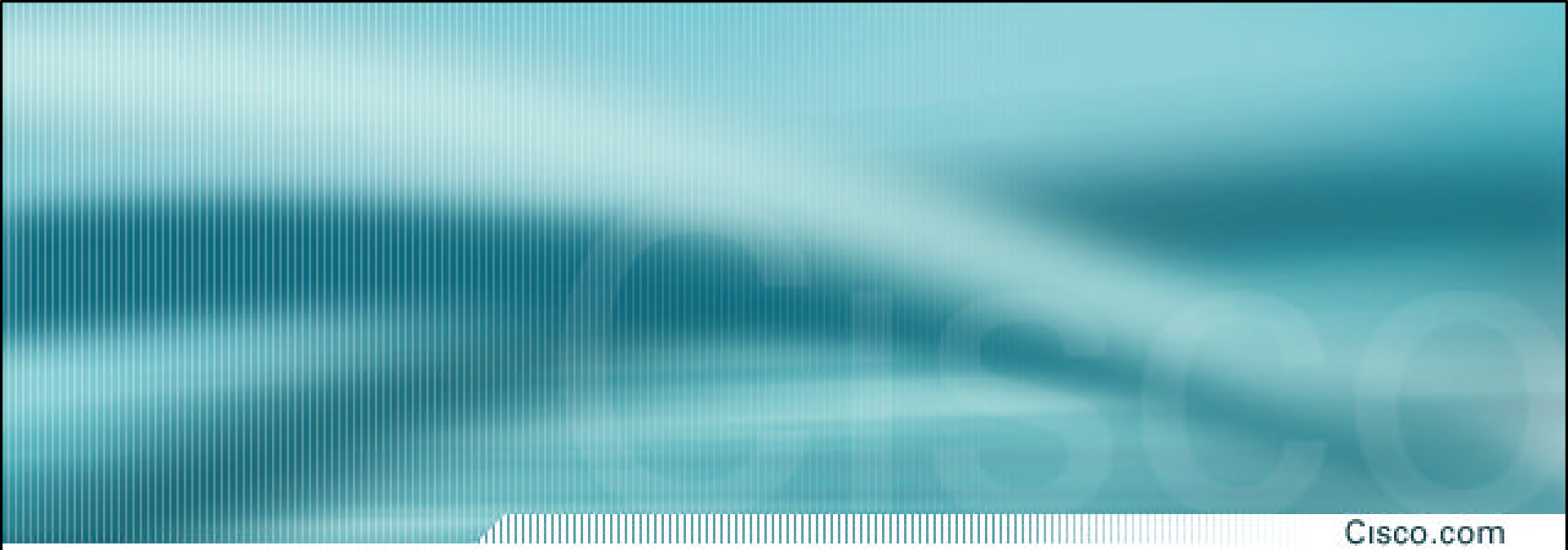
IDS 4.0 Roadshow

Module 1- IDS Technology Overview

Agenda

Cisco.com

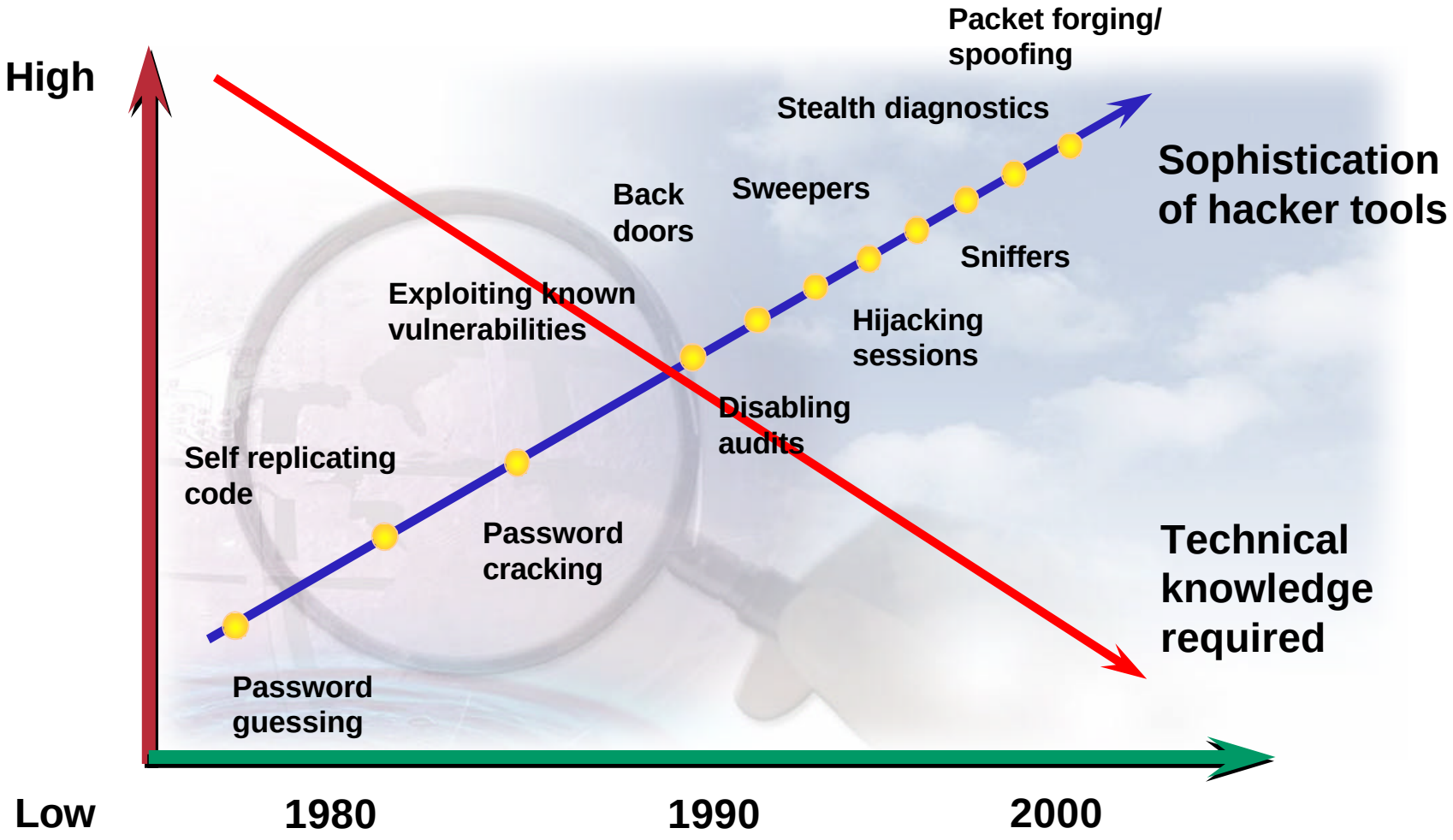
- Network Security
- Network Security Policy
- Management Protocols
- The Security Wheel
- IDS Terminology
- IDS Technology
- HIDS and NIDS
- IDS Communication Overview



Network Security

Threat Capabilities—More Dangerous and Easier to Use

Cisco.com

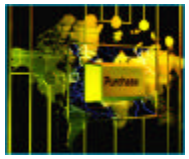


Changing the Role of Security

The need for security is becoming more important because of the following reasons:

- **Required for e-business**
- **Required for communicating and doing business safely in potentially unsafe environments**
- **Networks require development and implementation of a corporate-wide security policy**

The E-Business Challenge



E-commerce

Supply chain

Customer care

Workforce optimization

E-learning

Internet business value

Internet access

Corporate intranet

Internet presence

Business security requirements

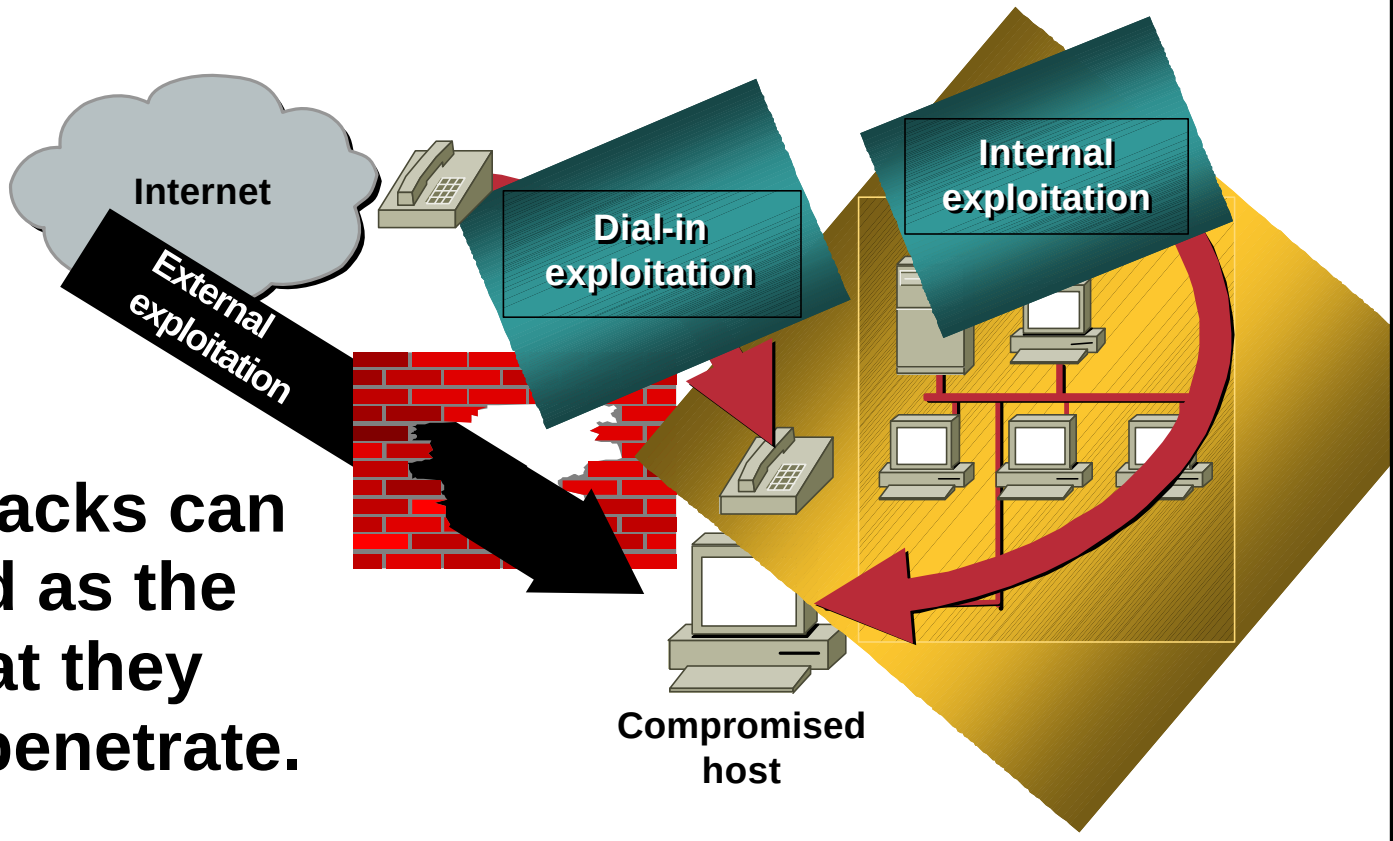
- Defense-in-depth
- Multiple components
- Integration into e-business infrastructure
- Comprehensive blueprint

Expanded access
heightened security risks

Legal and Governmental Policy Issues

- Organizations that operate vulnerable networks will face increasing and substantial liability.
- US Federal legislation mandating security includes the following:
  - GLB financial services legislation
  - Government Information Security Reform Act
  - HIPAA

Variety of Attacks

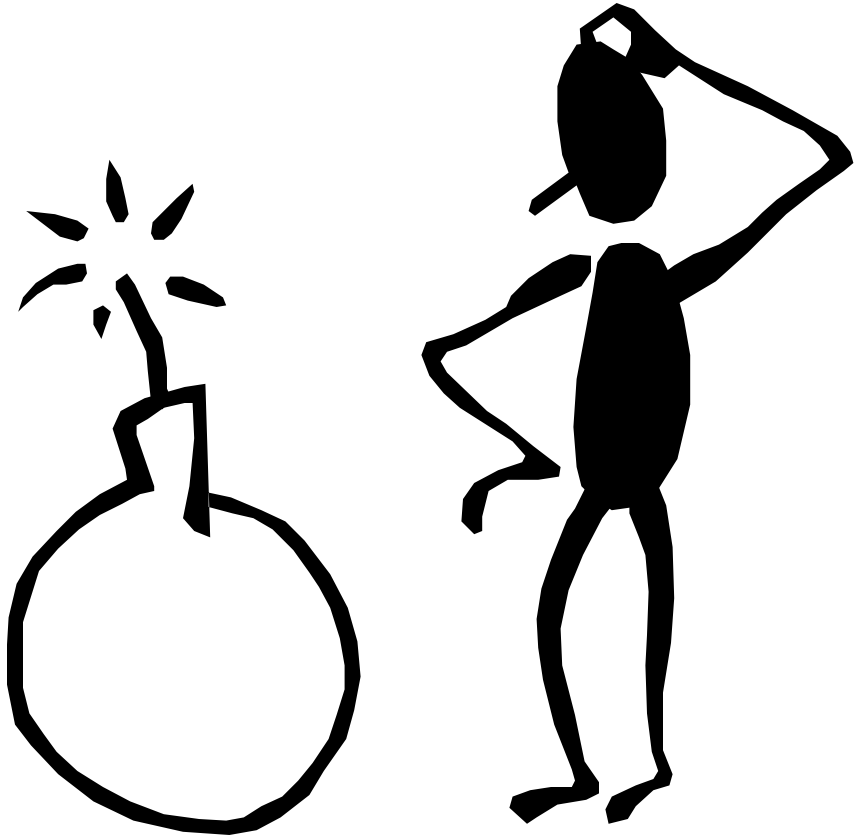


Network attacks can be as varied as the systems that they attempt to penetrate.

Network Security Threats

There are four general categories of security threats to the network :

- **Unstructured threats**
- **Structured threats**
- **External threats**
- **Internal threats**

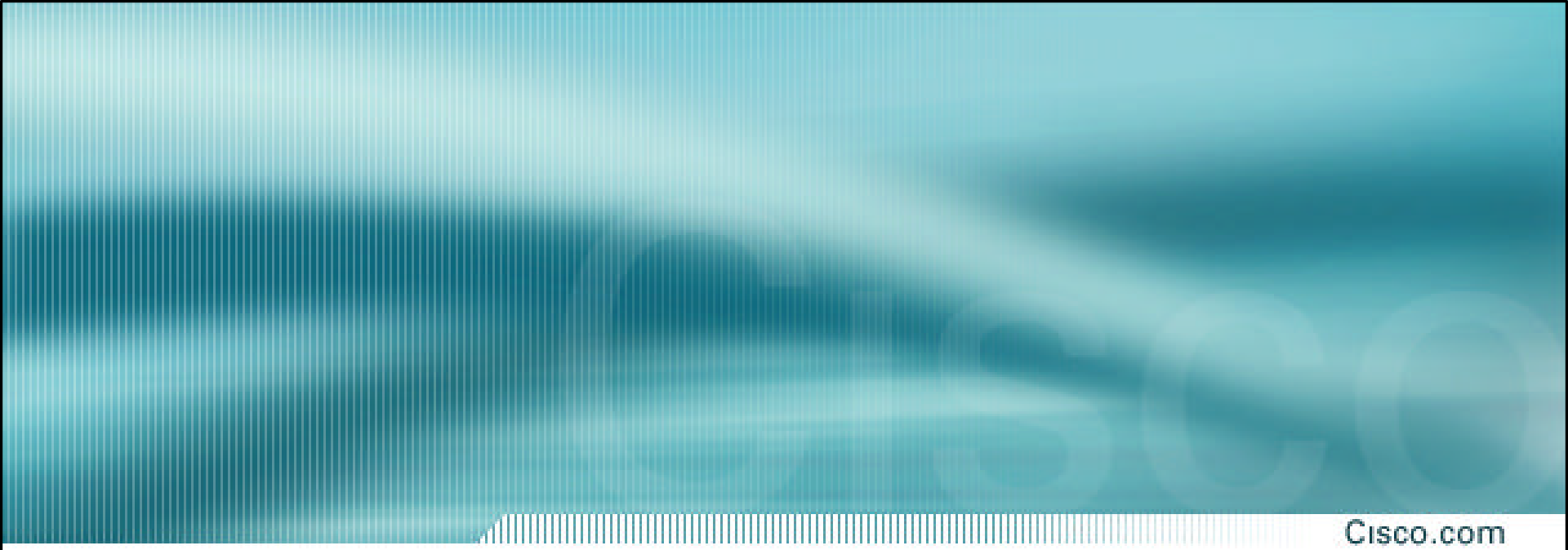


Specific Attack Types

Cisco.com

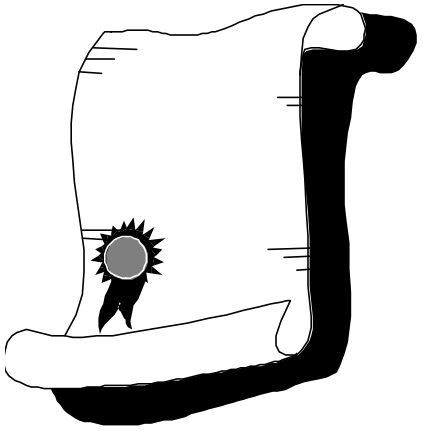
All of the following can be used to compromise your system:

- Packet sniffers
- IP weaknesses
- Password attacks
- DoS or DDoS
- Man-in-the-middle attacks
- Application layer attacks
- Trust exploitation
- Port redirection
- Virus
- Trojan horse
- Operator error



Network 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.”

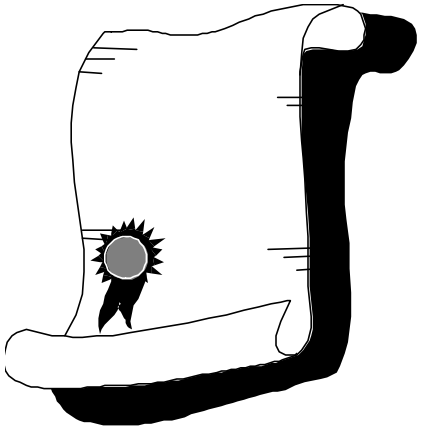
(RFC 2196, Site Security Handbook)

Why Create a Security Policy?

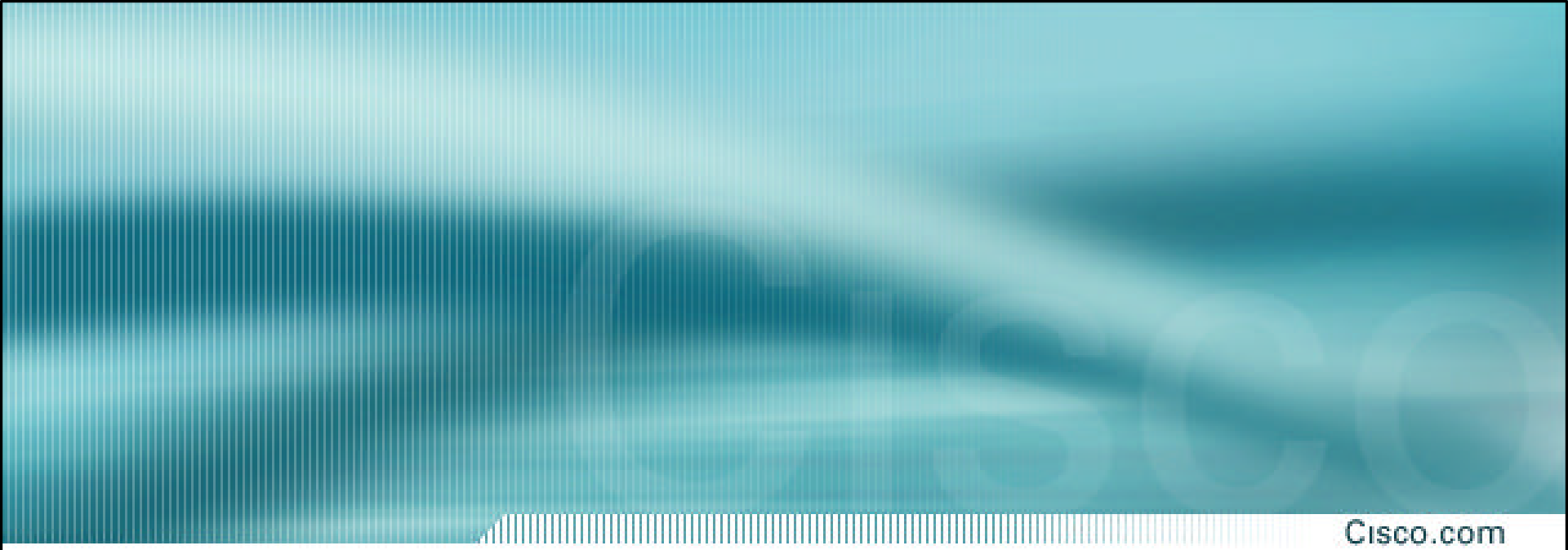
Cisco.com

- 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



Management Protocols and Functions

Configuration Management

- Configuration management protocols include SSH, SSL, and Telnet.
- Telnet issues include the following:
  - The data within a Telnet session is sent as clear text, and may be intercepted by anyone with a packet sniffer located along the data path between the device and the management server.
  - The data may include sensitive information, such as the configuration of the device itself, passwords, and so on.

Configuration Management Recommendations

When possible, the following practices are advised:

- **Use IPSec, SSH, SSL, or any other encrypted and authenticated transport.**
- **ACLs should be configured to allow only management servers to connect to the device. All attempts from other IP addresses should be denied and logged.**
- **RFC 2827 filtering at the perimeter router should be used to mitigate the chance of an outside attacker spoofing the addresses of the management hosts.**

SNMP

Cisco.com

- SNMP is a network management protocol that can be used to retrieve information from a network device. The TCP and UDP ports SNMP uses are 161 and 162.
- The following are SNMP issues:
  - SNMP uses passwords, called community strings, within each message as a very simple form of security. Most implementations of SNMP on networking devices today send the community string in clear text.
  - SNMP messages may be intercepted by anyone with a packet sniffer located along the data path between the device and the management server, and the community string may be compromised.
  - An attacker could reconfigure the device if read-write access via SNMP is allowed.
- The following are SNMP recommendations:
  - Configure SNMP with only read-only community strings.
  - Set up access control on the device you wish to manage via SNMP to allow only the appropriate management hosts access.

Logging

Logging issues include the following:

- Syslog is sent as clear text between the managed device and the management host on UDP port 514.
- Syslog has no packet-level integrity checking to ensure that the packet contents have not been altered in transit.
- There is a potential for the Syslog data to be falsified by an attacker.
- An attacker can send large amounts of false Syslog data to a management server in order to confuse the network administrator during an attack.

Logging Recommendations

When possible, the following practices are advised:

- **Encrypt Syslog traffic within an IPSec tunnel.**
- **When allowing Syslog access from devices on the outside of a firewall, you should implement RFC 2827 filtering at the perimeter router.**
- **ACLs should also be implemented on the firewall in order to allow Syslog data from only the managed devices themselves to reach the management hosts.**

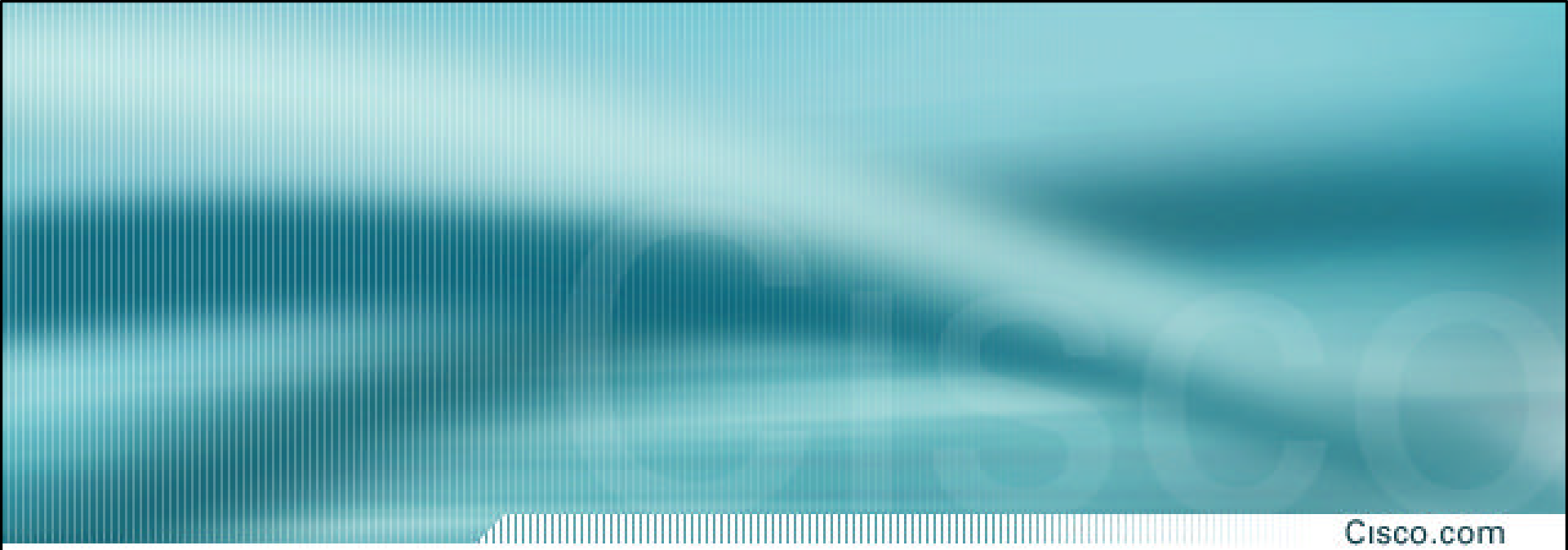
TFTP

- Many network devices use TFTP for transferring configuration or system files across the network. TFTP uses port 69 for both TCP and UDP.
- The following are TFTP issues:
  - TFTP uses UDP for the data stream between the device and the TFTP server.
  - TFTP sends data in clear text. The network administrator should recognize that the data within a TFTP session may be intercepted by anyone with a packet sniffer located along the data path between the requesting host and the TFTP server.
- When possible, TFTP traffic should be encrypted within an IPSec tunnel in order to mitigate the chance of its being intercepted.

NTP

Cisco.com

- NTP is used to synchronize the clocks of various devices across a network. It is critical for digital certificates, and for correct interpretation of events within Syslog data. NTP uses port 123 for both UDP and TCP connections.
- The following are NTP issues:
  - An attacker could attempt a DoS attack on a network by sending bogus NTP data across the Internet in an attempt to change the clocks on network devices in such a manner that digital certificates are considered invalid.
  - An attacker could attempt to confuse a network administrator during an attack by disrupting the clocks on network devices.
  - Many NTP servers on the Internet do not require any authentication of peers.
- The following are NTP recommendations:
  - Implement your own master clock for the private network synchronization.
  - Use NTP Version 3 or above as these versions support a cryptographic authentication mechanism between peers.
  - Use ACLs that specify which network devices are allowed to synchronize with other network devices.

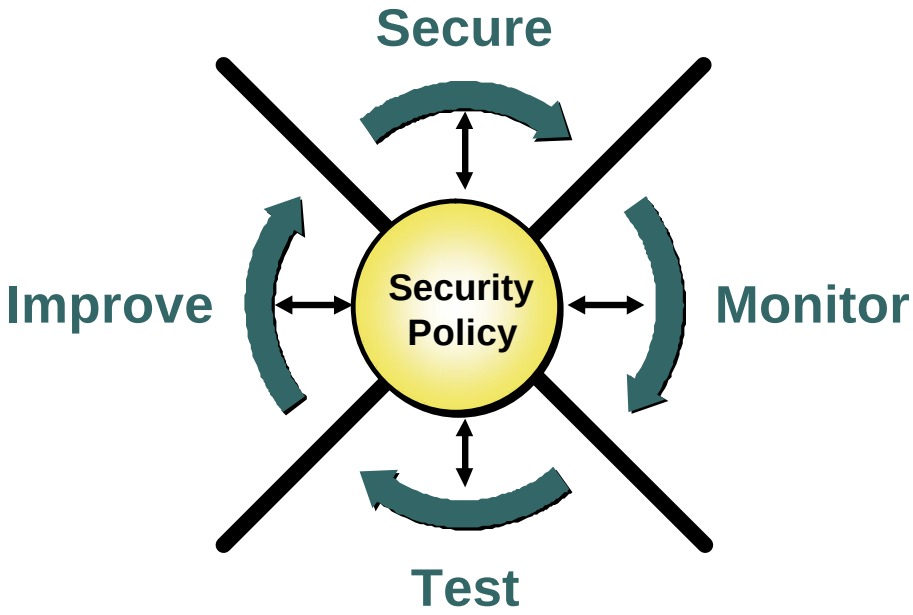


The Cisco Security Wheel

Network Security as a Continuous Process

Network security is a continuous process built around a security policy.

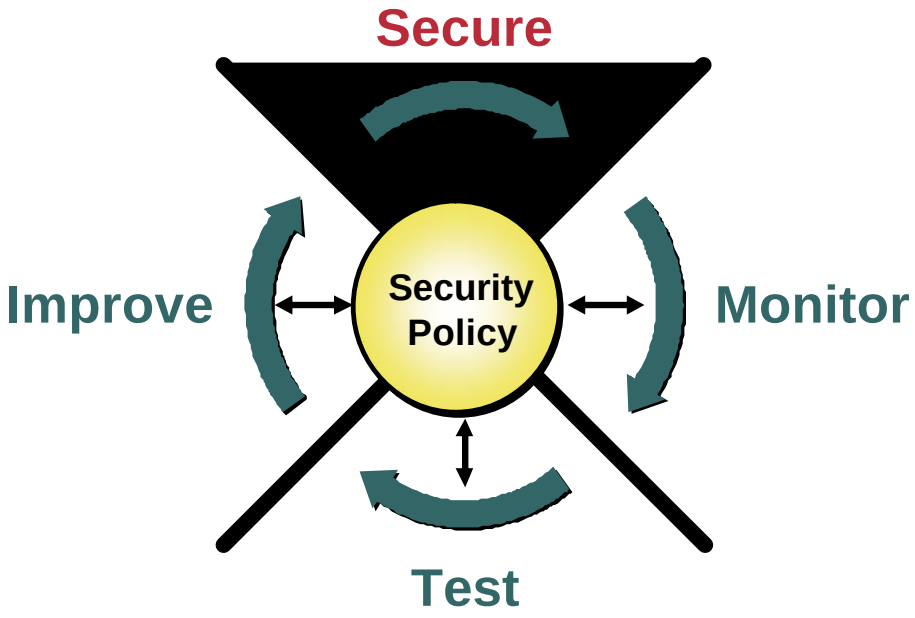
- **Step 1: Secure**
- **Step 2: Monitor**
- **Step 3: Test**
- **Step 4: Improve**



Secure the Network

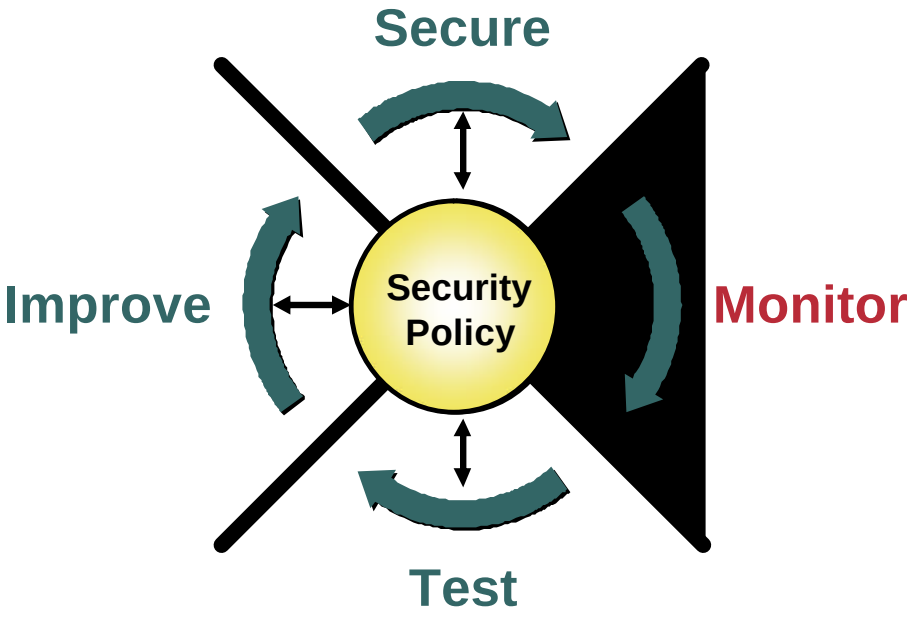
Implement security solutions to stop or prevent unauthorized access or activities, and to protect information:

- **Authentication**
- **Encryption**
- **Firewalls**
- **Vulnerability patching**



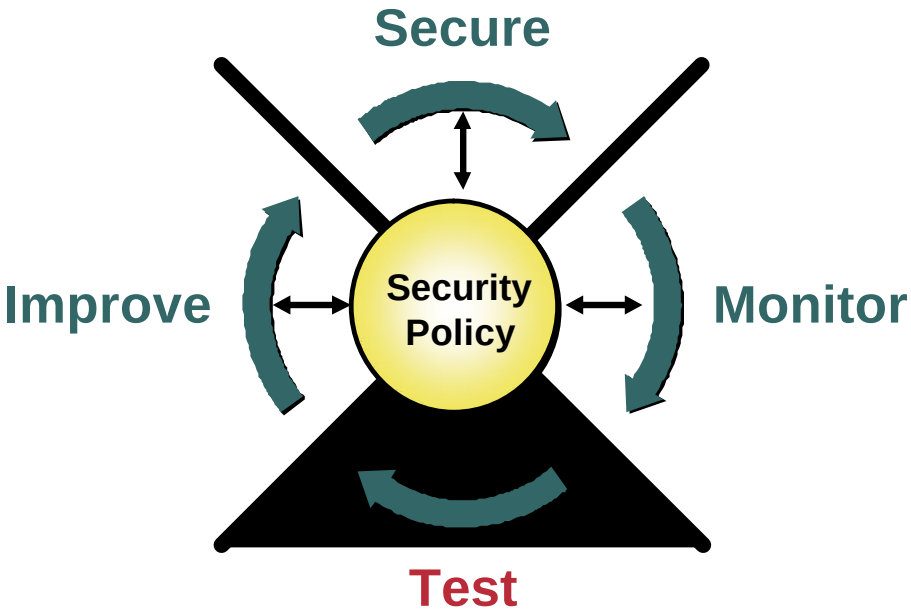
Monitor Security

- Detects violations to the security policy
- Involves system auditing and real-time intrusion detection
- Validates the security implementation in Step 1



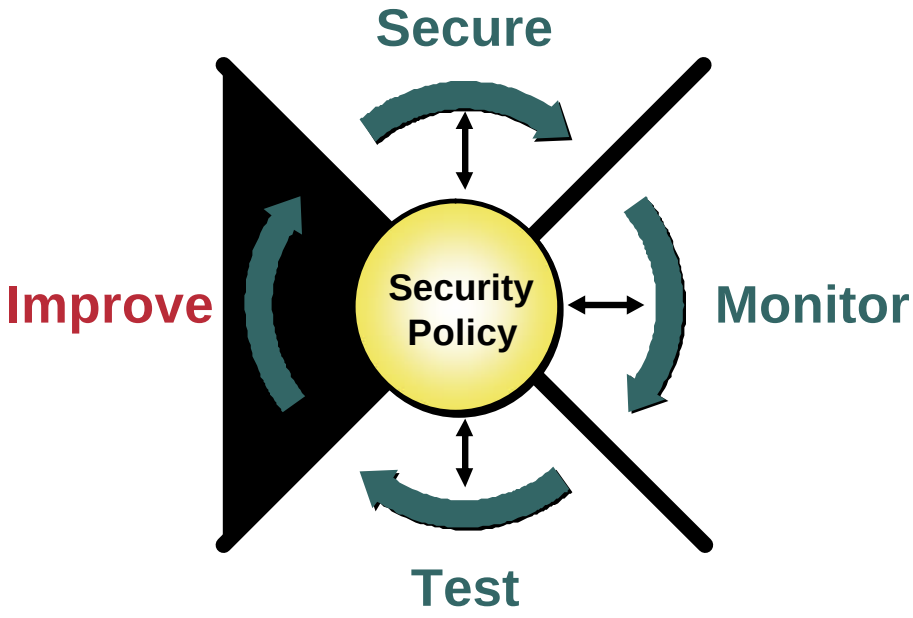
Test Security

Validates effectiveness of the security policy through system auditing and vulnerability scanning



Improve Security

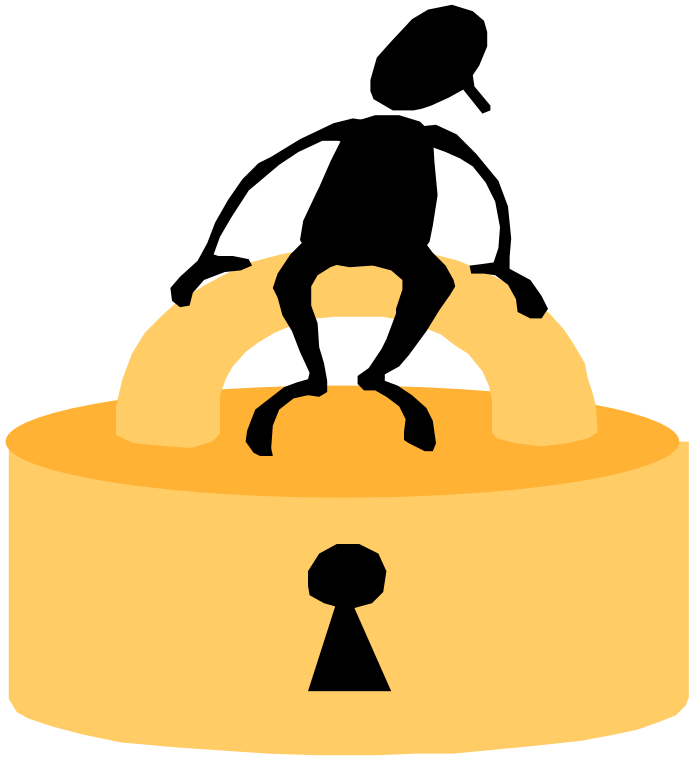
- Use information from the monitor and test phases to make improvements to the security implementation.
- Adjust the security policy as security vulnerabilities and risks are identified.



Intrusion Detection Terminology

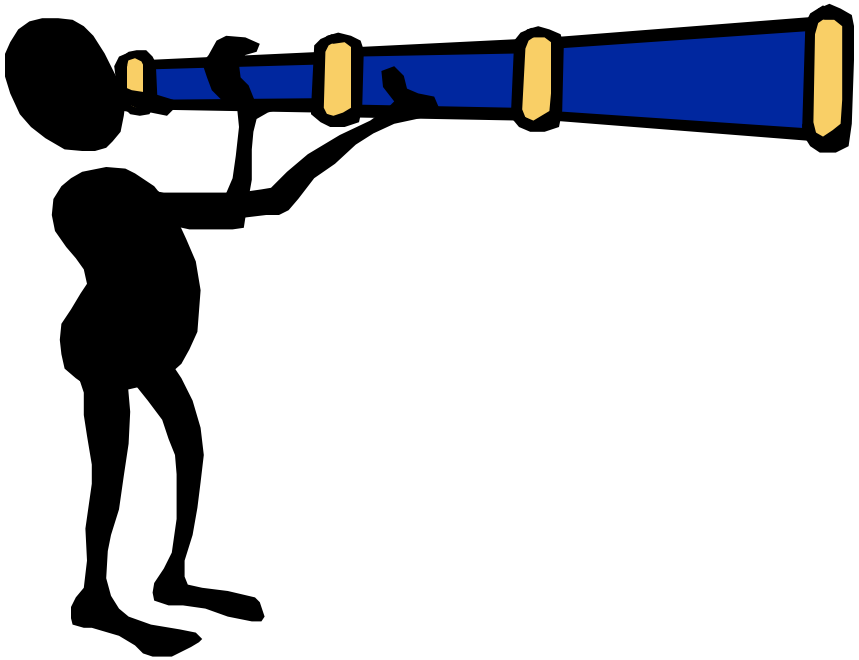
Intrusion Detection

- Ability to detect attacks against networks, including network devices and hosts.
- Types of network attacks are:
  - Reconnaissance
  - Access
  - Denial of service



Reconnaissance

Unauthorized discovery and mapping of systems, services, or vulnerabilities



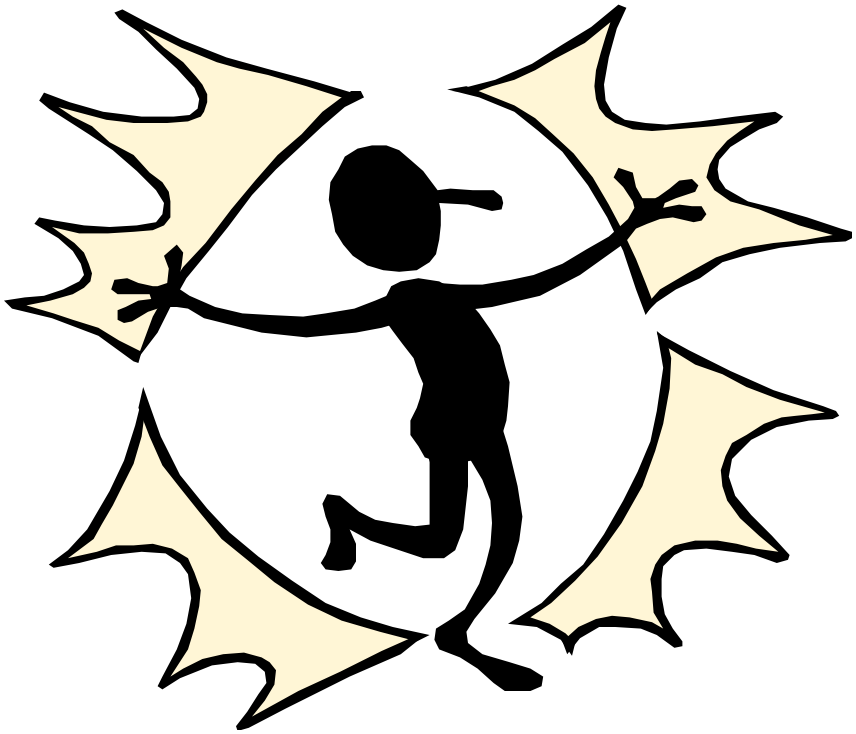
Reconnaissance Methods

- Common commands or administrative utilities—nslookup, ping, netcat, telnet, finger, rpcinfo, File Explorer, srvinfo, DumpSec
- Hacker tools—NMAP, Nessus, custom scripts

Vulnerabilities and Exploits

- A vulnerability is a weakness that compromises either the security or the functionality of a system.
  - Poor passwords
  - Improper input handling
  - Insecure communication
- An exploit is the mechanism used to leverage a vulnerability.
  - Password guessing tool
  - Shell scripts
  - Executable code

Access



Unauthorized data manipulation, system access, or privilege escalation

Access Methods

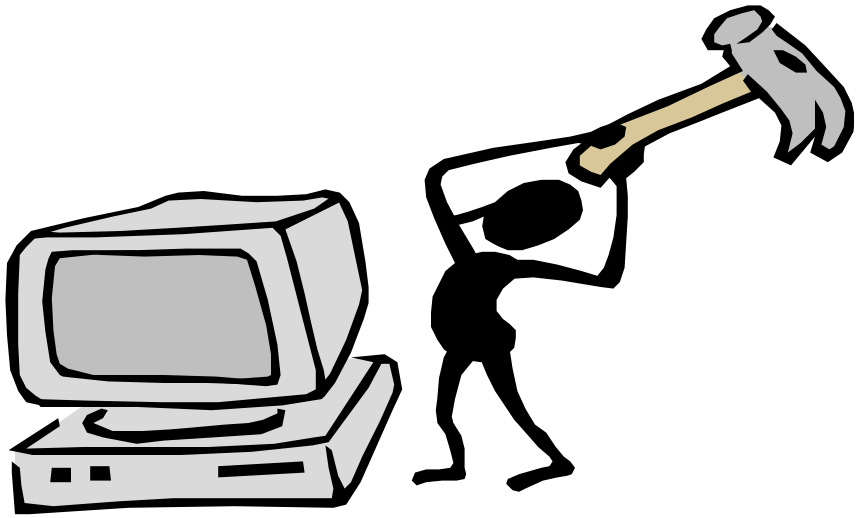
- Exploit easily guessed passwords
  - Default
  - Brute force
- Exploit mis-administered services
  - IP services
  - Trust relationships
  - File sharing

Access Methods (cont.)

- Exploit application holes
  - Mishandled input data—Access outside application domain, buffer overflows, race conditions
  - Protocol weaknesses—Fragmentation, TCP session hijack
- Trojan horses—Programs that introduce an inconspicuous backdoor into a host

Denial of Service

Disable or corrupt networks, systems, or services



Denial of Service Methods

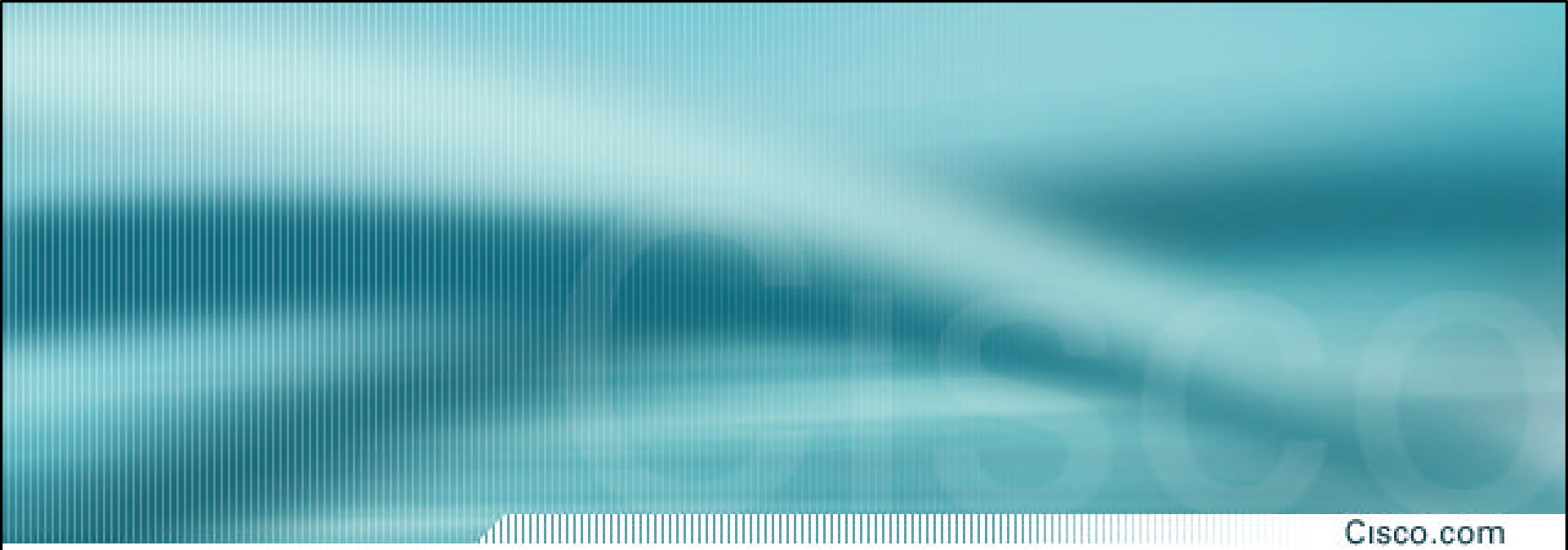
- Resource Overload
  - Disk space, bandwidth, buffers
  - Ping floods, SYN flood, UDP bombs
  - Unsolicited Commercial E-mail (UCE)
- Fragmentation or Impossible Packets
  - Large ICMP packets
  - IP fragment overlay
  - Same Source and Destination IP packet

False Alarms

- **False positive—A situation in which normal traffic or a benign action causes the signature to fire.**
- **False negative—A situation in which a signature is not fired when offending traffic is detected. An actual attack is not detected.**

True Alarms

- **True positive—A situation in which a signature is fired properly when the offending traffic is detected. An attack is detected as expected.**
- **True negative—A situation in which a signature is not fired when non-offending traffic is detected. Normal traffic or a benign action does not cause an alarm.**



Intrusion Detection Technologies

Profile-Based Intrusion Detection

- Also known as Anomaly Detection—Activity deviates from the profile of “normal” activity
- Requires creation of statistical user and network profiles
- Prone to high number of false positives—Difficult to define “normal” activity

Signature-Based Intrusion Detection

- Also known as Misuse Detection or Pattern Matching—Matches pattern of malicious activity
- Requires creation of signatures
- Less prone to false positives—Based on the signature's ability to match malicious activity

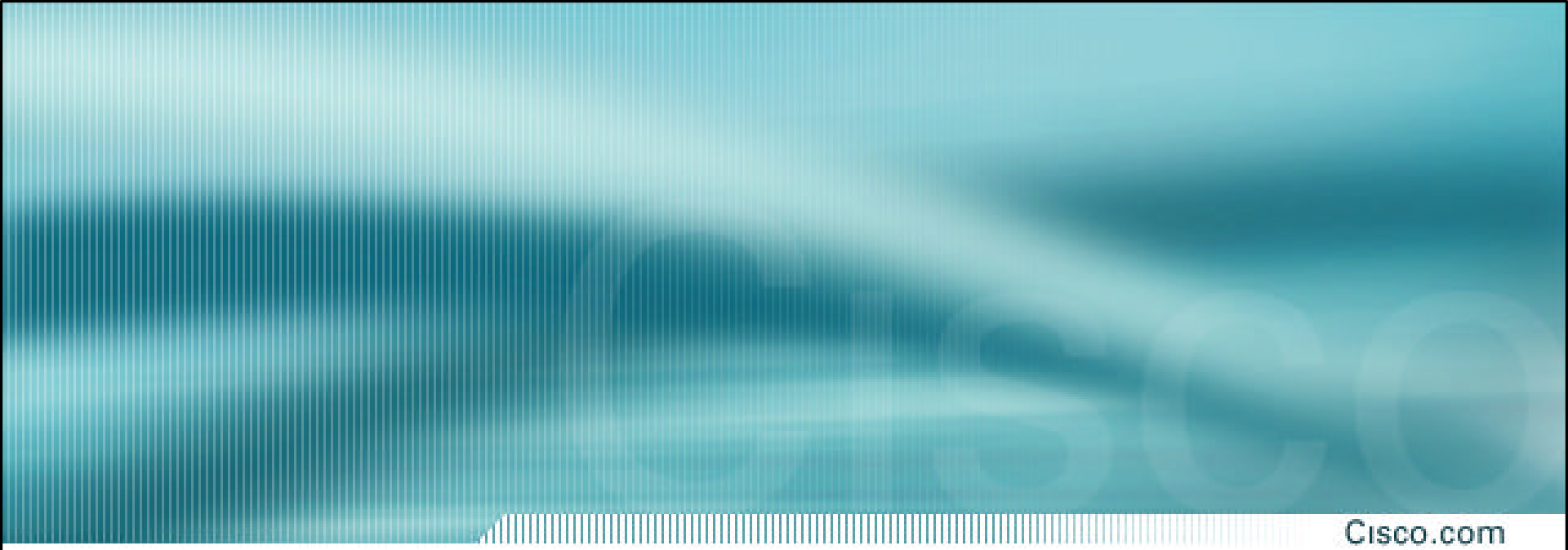
Protocol Analysis

Intrusion detection analysis is performed on the protocol specified in the data stream.

- **Examines the protocol to determine the validity of the packet**
- **Checks the content of the payload (pattern matching)**

Responsive

- Reactive IDSs can respond to an attack.
  - Terminate session (TCP resets)
  - Block offending traffic (ACL)
  - Create session log files (IP logging)
  - Restrict access to protected resources

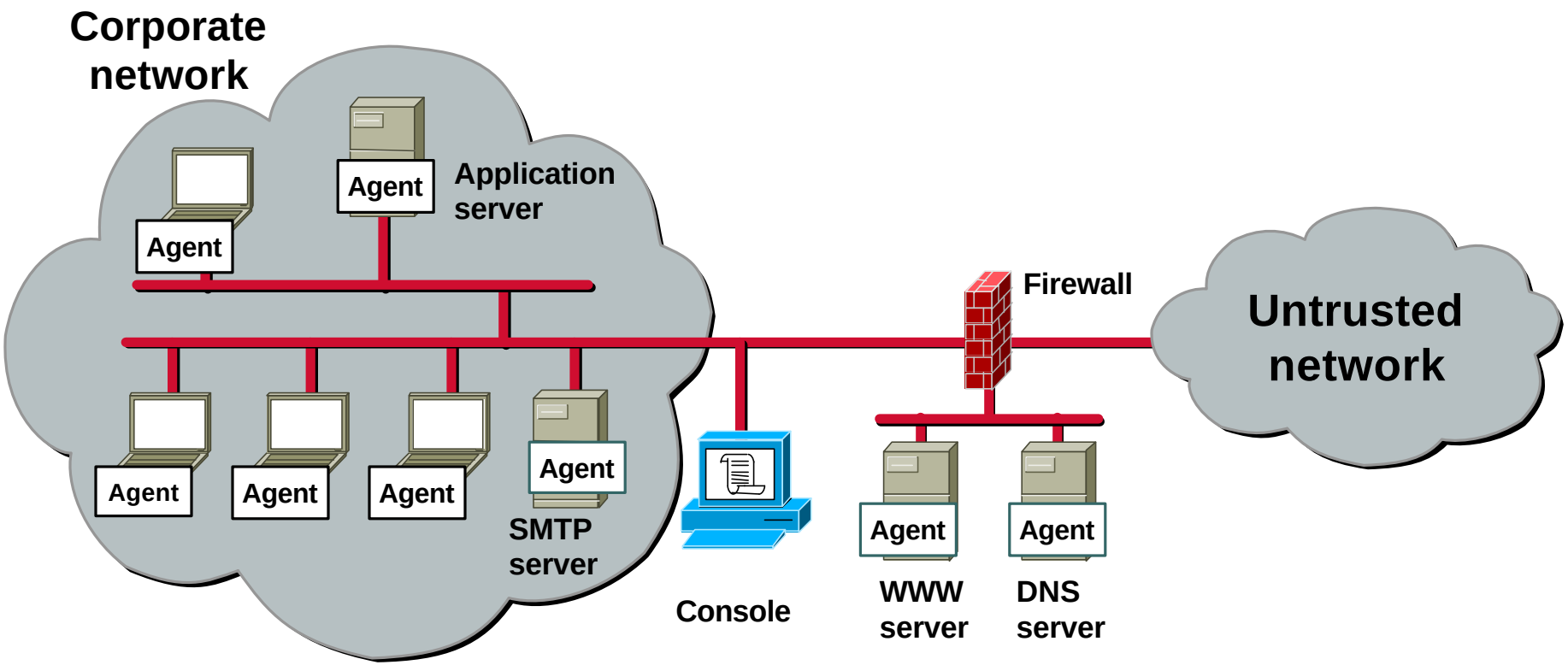


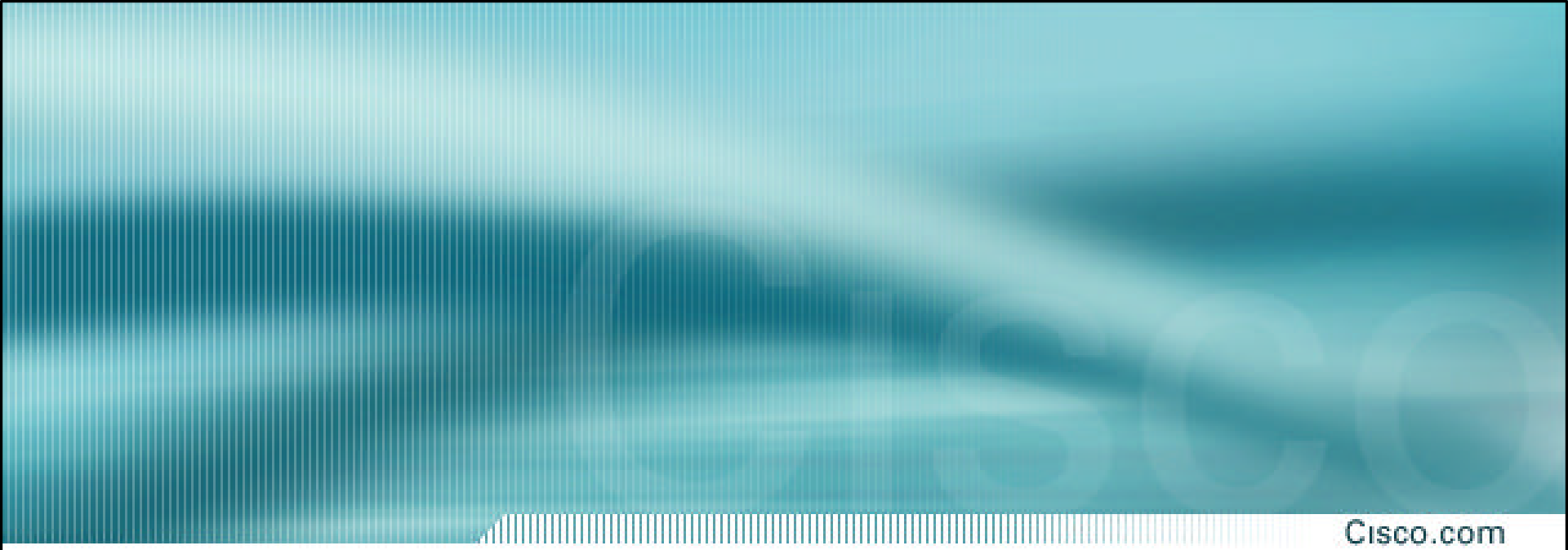
Host-Based Intrusion Protection

HIPS Features

- Agent software is installed on each host.
- Provides individual host detection and protection.
- Detects attacks before encryption and after decryption occurs.
- Does not require special hardware.

Host-Based Intrusion Protection



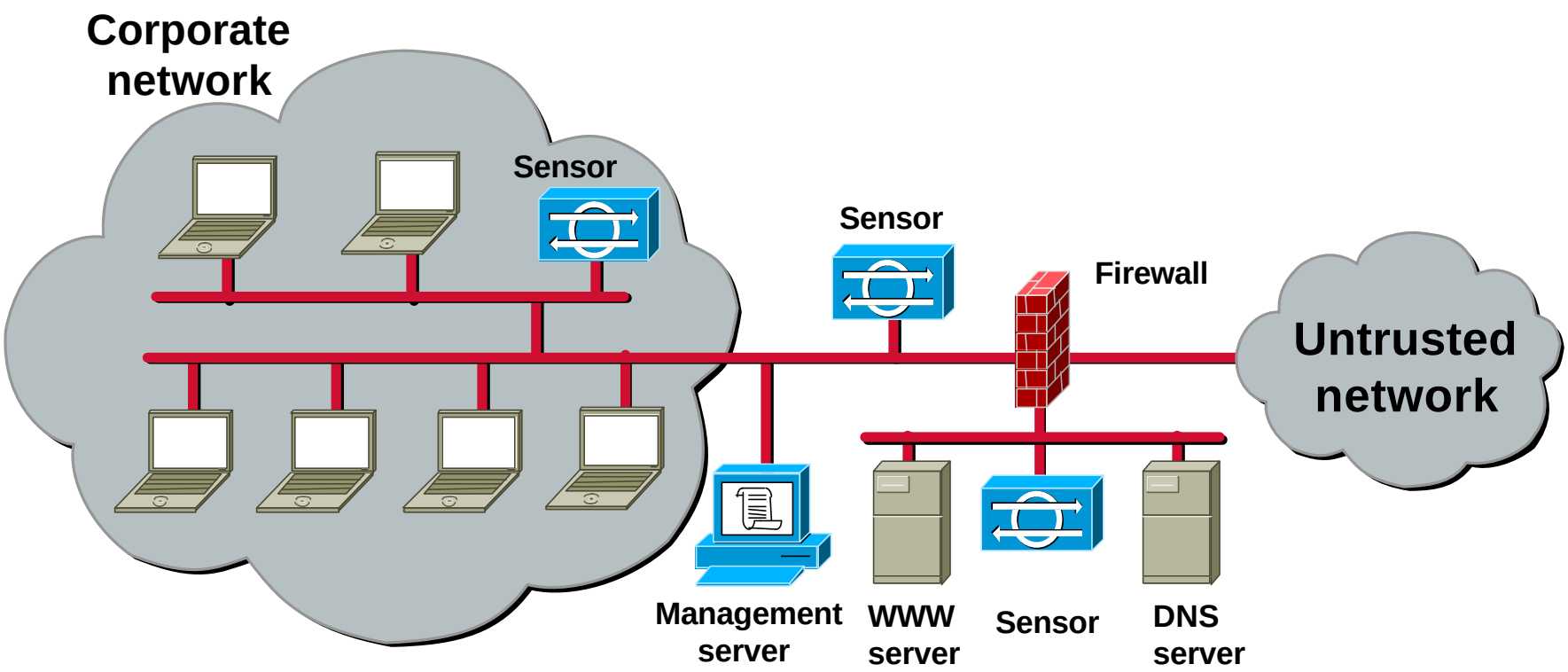


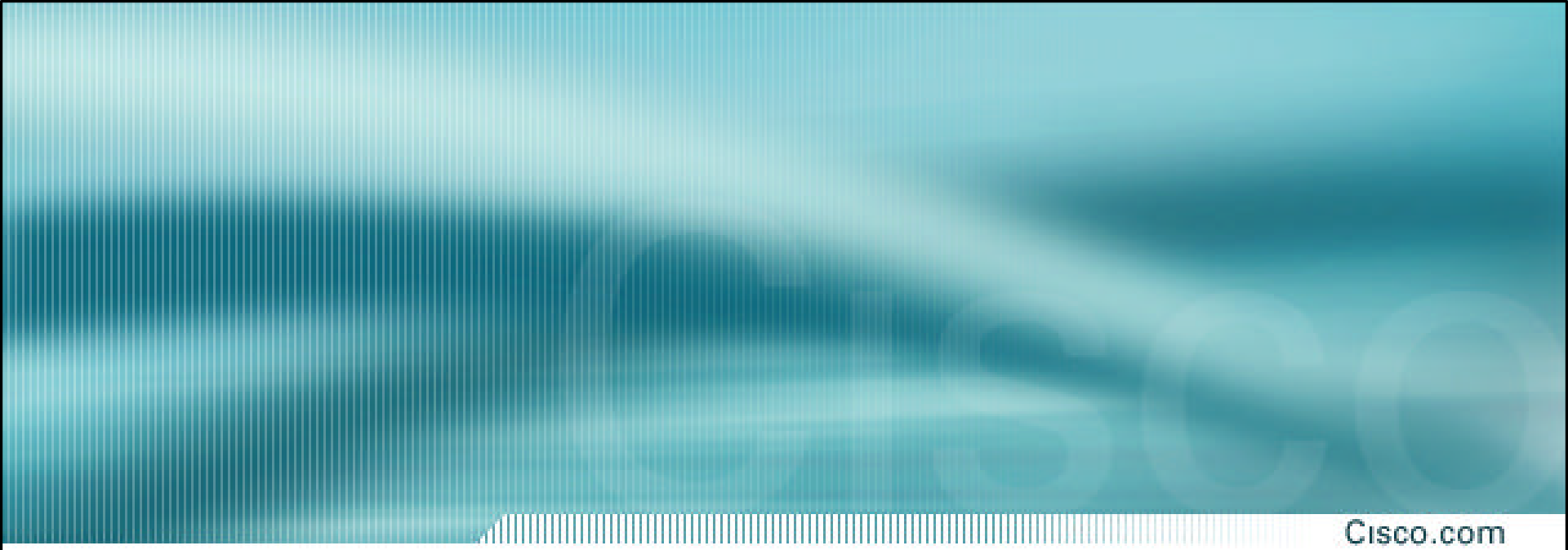
Network-Based Intrusion Detection Systems

NIDS Features

- Sensors are connected to network segments. A single Sensor can monitor many hosts.
- Growth of a network is easily protected. New hosts and devices can be added to the network without additional Sensors.
- The Sensors are network appliances tuned for intrusion detection analysis.
  - The operating system is “hardened.”
  - The hardware is dedicated to intrusion detection analysis.

NIDS





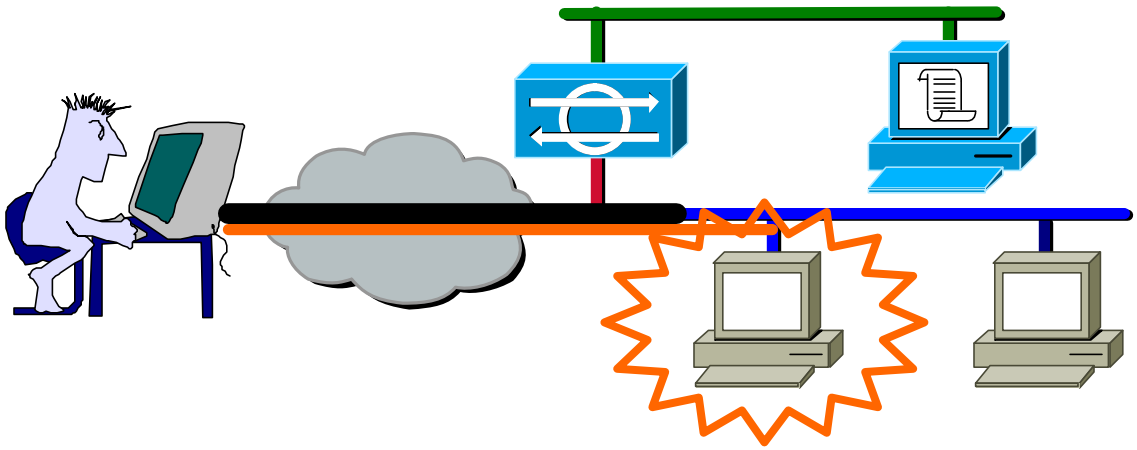
Intrusion Detection Evasive Techniques

Evasive Techniques

- Attempting to elude intrusion detection is accomplished using intrusion detection evasive techniques.
- Common intrusion detection evasive techniques are:
  - Flooding
  - Fragmentation
  - Encryption
  - Obfuscation

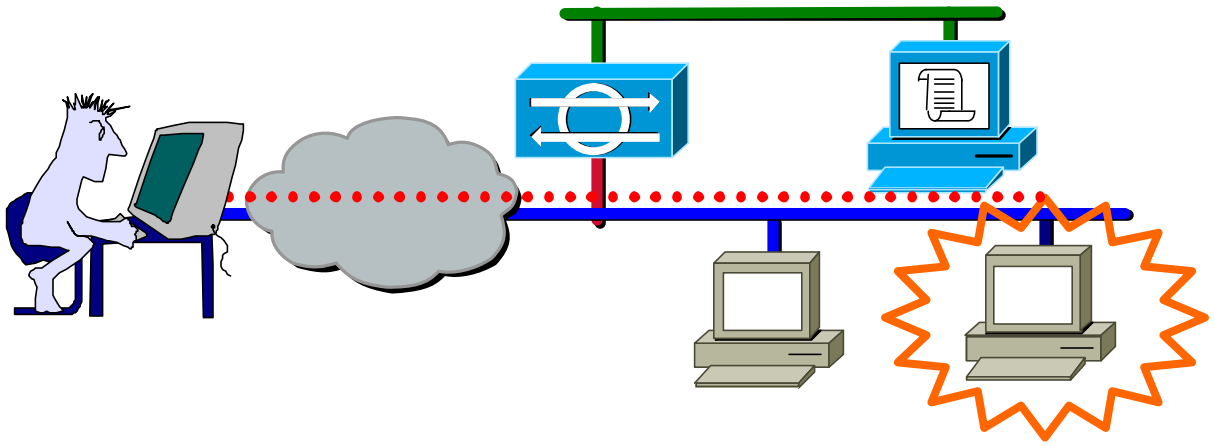
Flooding

Saturating the network with “noise” traffic while also trying to launch an attack against the target is referred to as flooding.



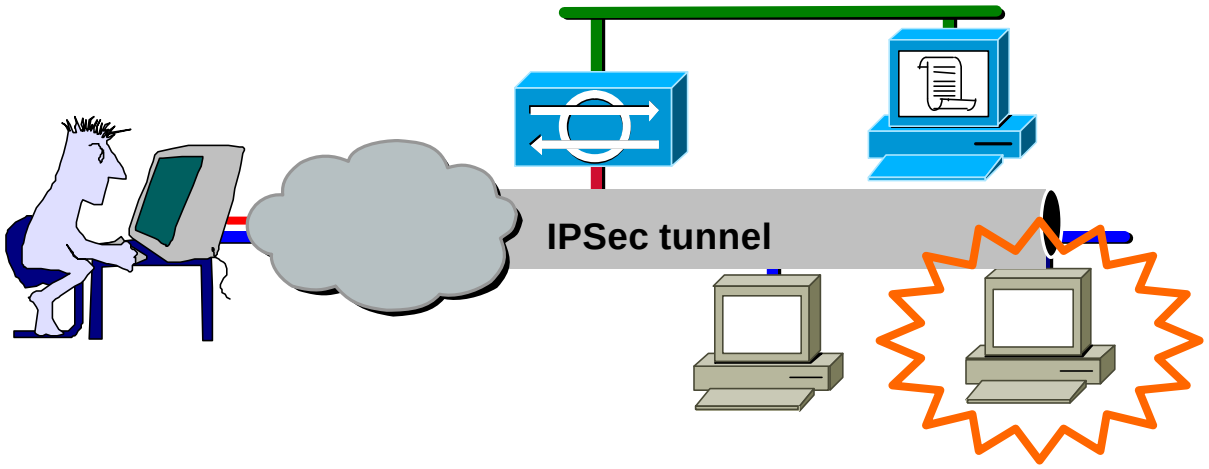
Fragmentation

Splitting malicious packets into smaller packets to avoid detection is known as fragmentation.



Encryption

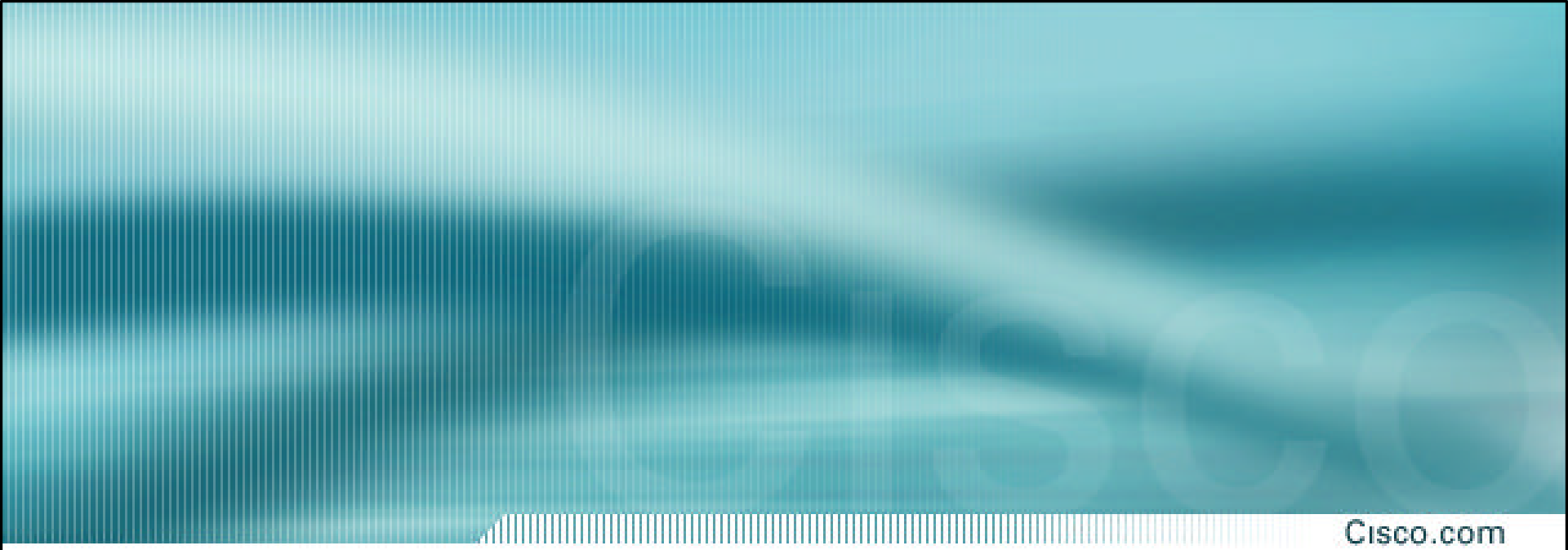
- Launching an attack via an encrypted session can avoid network-based intrusion detection.
- This type of evasive technique assumes the attacker has already established a secure session with the target network or host.



Obfuscation

Disguising an attack using special characters to conceal an attack from an IDS is commonly referred to as obfuscation.

- **Control characters**
- **Hex representation**
- **Unicode representation**



Intrusion Protection

Intrusion Protection Benefits

Cisco.com

Intrusion protection provides:

- Enhanced security over “classic” technologies
- Advanced technology to address the changing threat
- Increased resiliency of e-Business systems and applications
- Effective mitigation of malicious activity and insider threats
- Broad visibility into the corporate datastream
- Greater protection against known and unknown threats

Active Defense System

A complete intrusion protection solution focuses on the following:

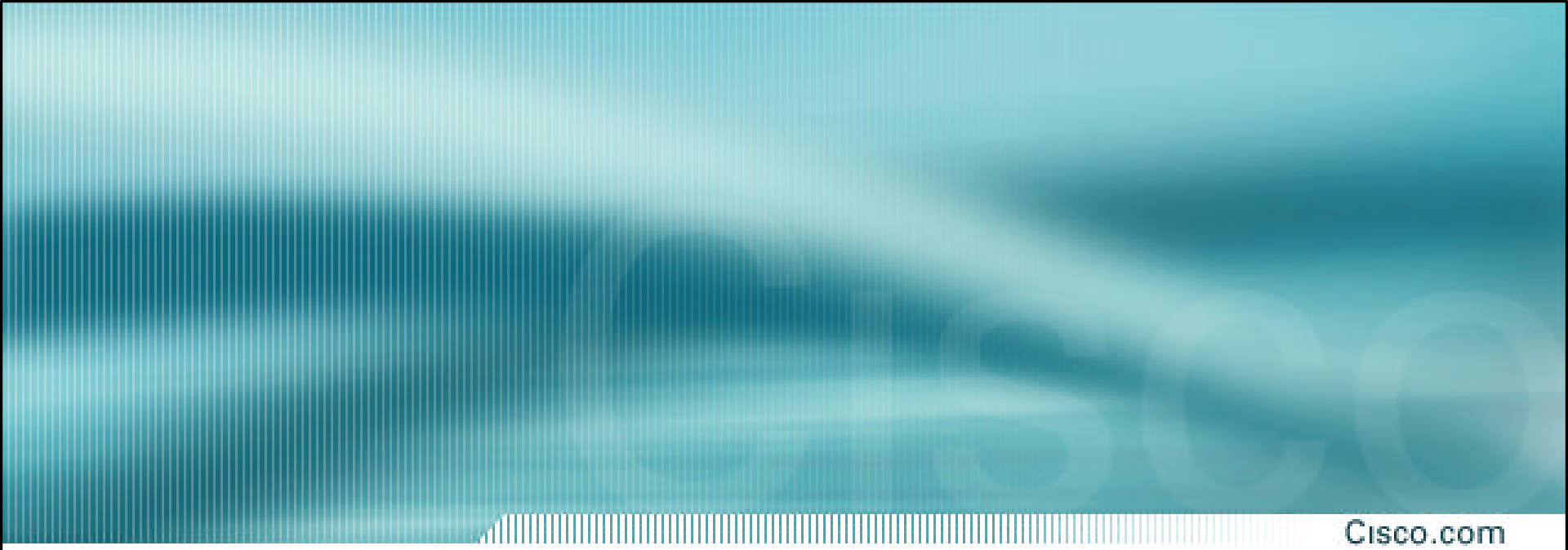
- **Detection—Identify malicious attacks on network and host resources**
- **Prevention—Stop the detected attack from executing**
- **Reaction—Immunize the system from future attacks from a malicious source**

Cisco IDS Solution
Active Defense System

- Network Sensors—Overlaid network protection
- Switch Sensors—Integrated switch protection
- Router Sensors—Integrated router protection
- Firewall Sensors—Integrated firewall protection
- Host Agents—Server and desktop protection
- Comprehensive management—Robust system management and monitoring

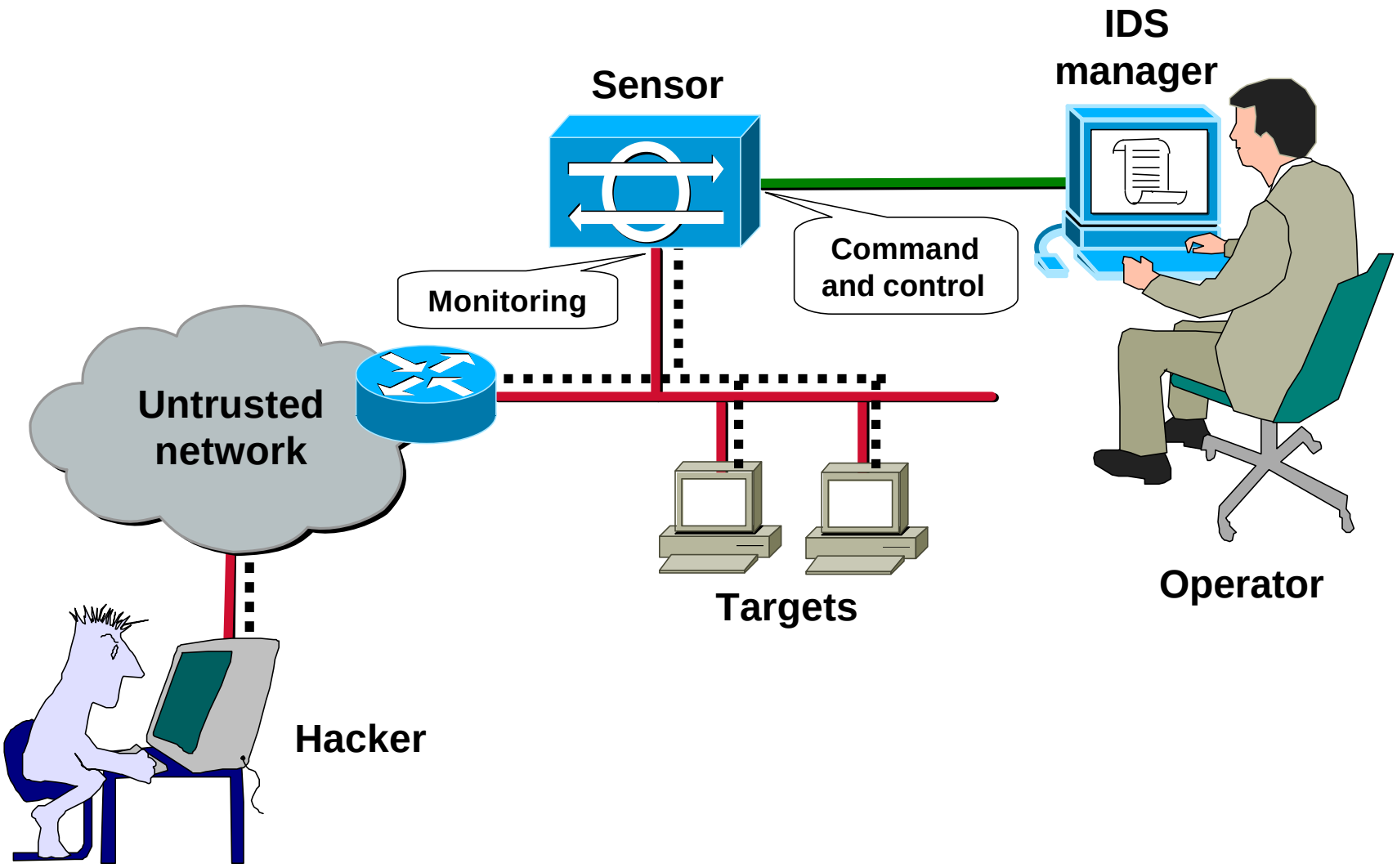
Defense-In-Depth—A Layer Solution

- Application-level encryption protection
- Policy enforcement (resource control)
- Web application protection
- Buffer overflow
- Network attack and reconnaissance detection
- Denial-of-service detection



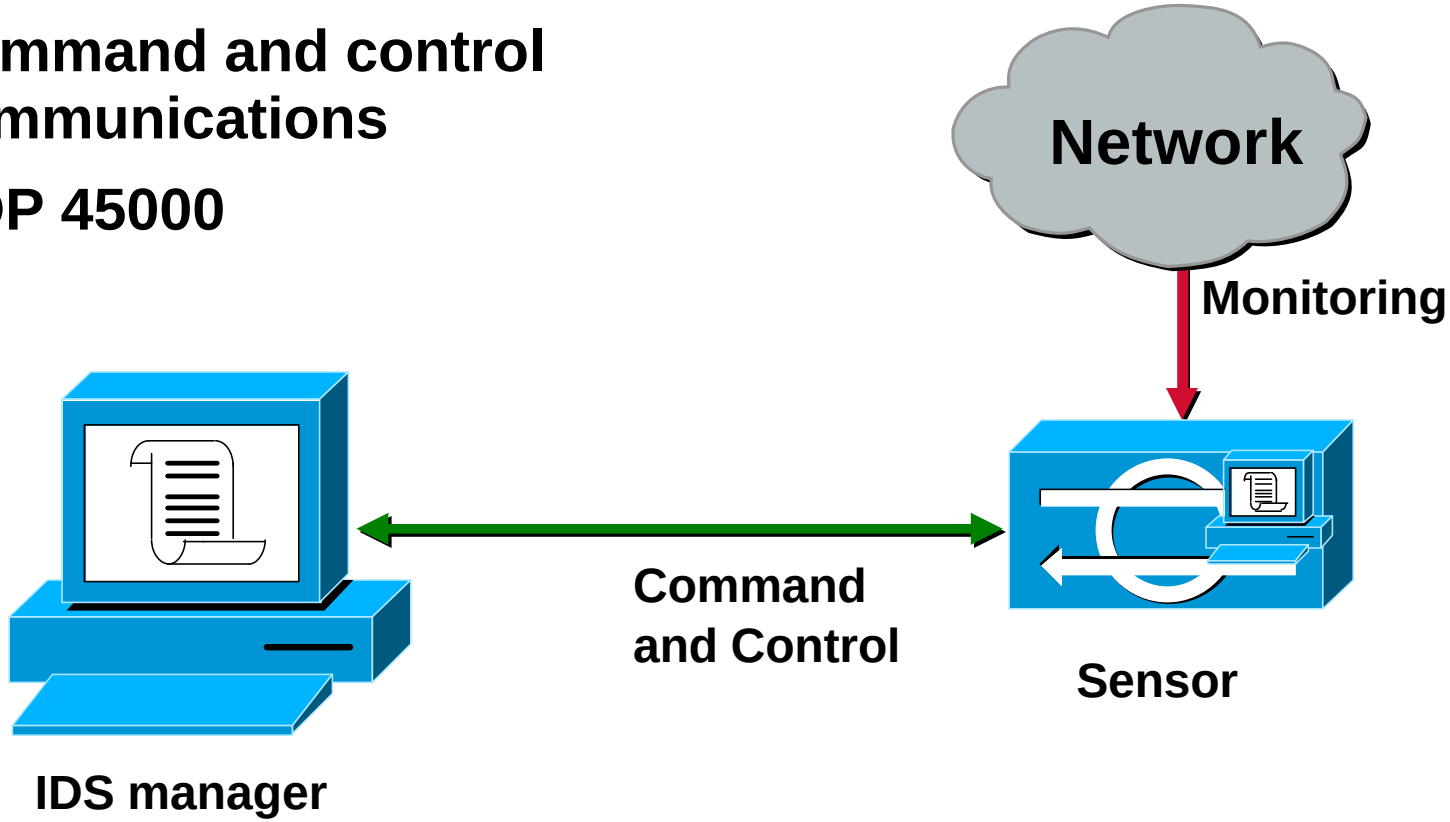
Cisco IDS Communication Overview

Cisco IDS Overview



IDS 3.X Communications—PostOffice Protocol

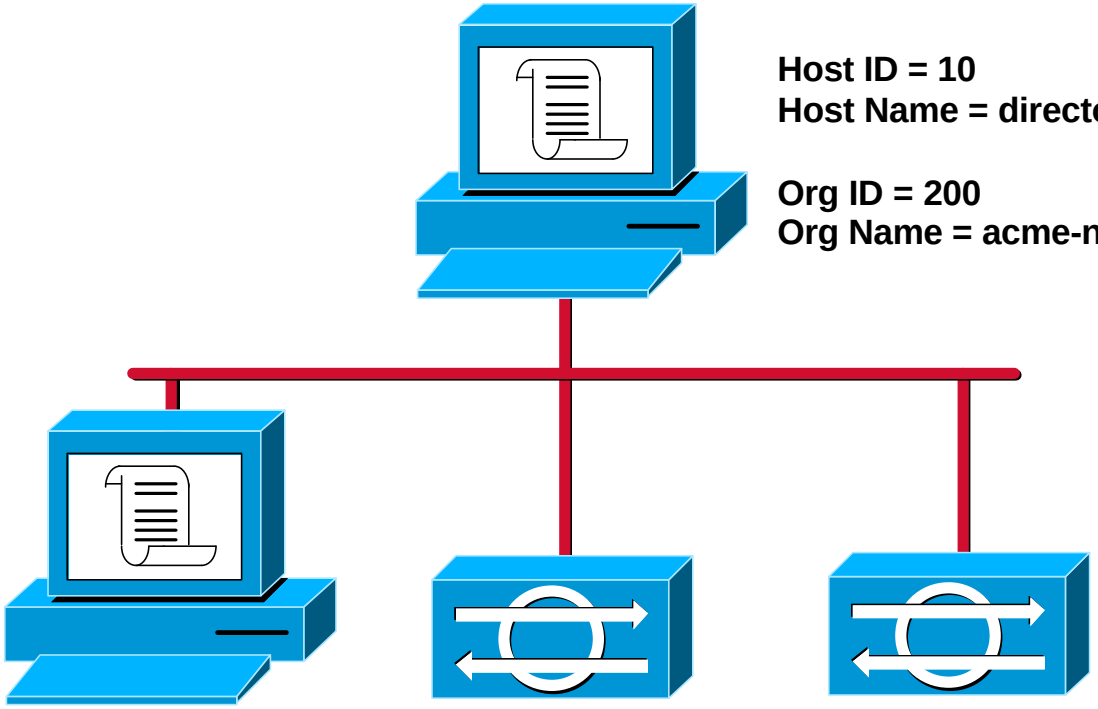
- Command and control communications
- UDP 45000



PostOffice Host Addressing

Cisco.com

- Numeric
  - Host ID
  - Organization ID
- Alpha Numeric
  - Host Name
  - Organization Name
- Combination of host ID and Org ID must be unique
- Host, Organization, and Application ID are used together to route PostOffice traffic



IDS 4.0 Communications—RDEP

Cisco.com

- Replaces PostOffice protocol
- Uses HTTP/HTTPS to communicate XML documents between the Sensor and external systems
- Uses a pull communication model
  - Allows management console to pull alarms at own pace
  - Alarms remain on Sensor until 4-Gb limit is reached and alarms are overwritten