DESIGNING AND DEPLOYING NETWORK-BASED INTRUSION DETECTION AND PREVENTION SYSTEMS
SESSION SEC-2030

Agenda

• Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
• Network Sensors
• Management Considerations
• Case Study
The Challenge: Security in Modern Networks

The **Number** of Security Incidents Continues to Rise Exponentially

The **Complexity** and **Sophistication** of Attacks and Vulnerabilities Continues to Rise

The Potential **Impact** to the Bottom Line Is Significant

Mitigating the Risk: Defense in Depth

- Comprehensive security policy
- Pervasive security—end to end
- Security in layers
- Multiple technologies working together as opposed to point products
Defense in Depth: The Role of IDS/IPS

- Complementary technology to firewalls
- Been around for more than a decade, started coming into prominence in the late '90s
- Performs deep packet inspection, gaining visibility into detail often missed by firewalls
- Penetration has broadened now that Inline IDS (IPS) has started to gain acceptance

IDS/IPS SYSTEMS
Agenda

- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
  - Terminology and Technologies
  - Complete Architecture
  - Deployment Strategies
  - Organization-Level Concerns
- Network Sensors
- Management Considerations
- Case Study

IDS/IPS Terminology: The Marketing of IDS/IPS

- **IDS** Intrusion Detection System—Traditionally limited to promiscuous sensors
- **IPS** Intrusion Prevention/Protection—The term most commonly applied to an inline IDS sensor, i.e. in the traffic stream
- **IDP** Intrusion Detection and Prevention—Marketing term coined by a vendor for product differentiation
IDS/IPS Terminology:
False Positives Explained

- **False Positive** is the term most likely used to indicate an event that was incorrectly reported; It is typically mistakenly applied to a broad group of possible results
  - **False Positive**: A correctly named false positive is one where the IDS/IPS has triggered an event or alarm based on a flawed algorithm or an analysis error; normally a fairly rare event
  - **Benign Trigger**: The case where a sensor has correctly interpreted network as an attack, but the intentions behind the traffic were not malicious; potentially common
  - **False Alarms (or Noise)**: The case where a sensor has correctly detected than an event has occurred but the event is non-threatening or not applicable to the site being monitored; very likely labeled as a False Positive, very common
- **False Negatives** is the term used to describe when an IDS/IPS misses an attack or event for any reason

IDS/IPS Terminology:
Signatures and Anomalies

- **Signatures** explicitly define what activity should be considered malicious
  - Simple pattern matching
  - Stateful pattern matching
  - Protocol decode-based analysis (including protocol anomalies)
  - Heuristic-based analysis
- **Anomaly** detection involves defining or learning “normal” activity and looking for deviations from this baseline
**IDS/IPS Terminology: Anomalies Defined**

- **Protocol Anomaly**
  Involves looking for deviations from a standard protocol. Useful for identifying deviations from normal behavior. Potentially useful in alerting when something is wrong. Not very useful for helping to decide what is wrong. Usually the alerts are vague, i.e. Protocol Anomaly Detected.

- **Network Anomaly**
  Involves watching or learning the normal traffic levels. If they change, an alarm is generated. False alarm prone but can be combined with other techniques to raise accuracy.

- **Behavioral Anomaly**
  Involves learning normal user behavior. If a change occurs, an alarm is generated. Normally useful only in very tightly controlled environments as behavior changes occur frequently in a network. Frequently successfully used on Host Based IDS/IPS systems.

**IDS/IPS Architecture: Sensors and Management**
IDS/IPS Components

- **Network-Based Sensors**
  Specialized software and/or hardware used to collect and analyze network traffic (either inline or promiscuous)
  Appliances, modules, embedded in network infrastructure (either inline or promiscuous)

- **Security Management and Monitoring**
  Performs configuration and deployment services
  Alert collection and aggregation for monitoring

**Network-Based IDS: The Sensor**

- Network Link to the Management Console
- IP Address
- Passive Interface
- No IP Address
- Monitoring the Network
- Data Capture
- Data Flow
Network-Based IDS: Functions and Capabilities

- Monitors traffic on a given segment promiscuously: SPAN, TAP, VACL capture, etc
- Compare traffic against well known attack patterns (signatures); also look for heuristic attack patterns (i.e. multi-host scans, DoS) and protocol anomalies
- Includes fragmentation and stream reassembly logic for de-obfuscation of attacks
- Primarily an alarming and visibility tool, but also allows active response: TCP reset, blocking, IP session logging

Network-Based IPS: The Sensor

Data Flow

Network Link to the Management Console

Management Interface
IP Address

Transparent Interfaces
No IP Address

© 2004 Cisco Systems, Inc. All rights reserved.
Network IPS: Functions and Capabilities

- Monitors all traffic traversing between two interfaces transparently
- Compare traffic against well known attack patterns (signatures); also look for heuristic attack patterns (i.e. multi-host scans, DoS) and protocol anomalies
- Includes fragmentation and stream reassembly logic for de-obfuscation of attacks as well as TCP/IP packet stream normalization
- Both an alarming and visibility tool as well as a preventive capability through packet filtering; also allows active response: TCP reset, blocking, IP session logging, and packet filtering

Placement Strategies

- Often, IDS/IPS cannot be implemented “everywhere” due to cost restrictions
- Where do you need to detect/stop an intrusion as soon as it occurs?
  - Where an incident would be most expensive (most valuable data)
  - At the entry to a sensitive domain to detect the first successful step of the attacker (most exposed)
  - Between trusted/un-trusted boundaries
- Look at the risks again—make sure you prioritized based on the value of a resource and the exposure involved
IDS or IPS Deployment Considerations

**IDS: Deploy an IDS Sensor in Areas That You Can’t Deploy an Inline Device or Aren’t Allowed to or Don’t Plan to Use Response Actions**

- **Pros:**
  - Deploying the sensor does not have any impact on the network (latency, jitter, etc)
  - Sensor is not inline and therefore a sensor failure can’t impact network functionality
  - Overrunning the sensor with data will not impact network traffic (but it most certainly will impact IDS analysis)

- **Cons:**
  - IDS response actions can not stop the trigger packet and are not guaranteed to stop a connection. IDS response actions are typically better at stopping an attacker more than a specific attack itself.
  - IDS response actions are less helpful in stopping thousands of automated attackers (i.e. Worms) depending on external platform or for email virus’s
  - User deploying IDS response actions must have a well thought out security policy combined with a good operational understanding of their IDS deployments (Correctly tuned sensors are a must)
  - Being out of band, IDS sensors are more vulnerable to network evasion games and must expend significant resources attempting to penetrate

**IPS: Deploy an IPS Sensor into Those Areas Where You Plan to Use and Need Response Actions (Packet Drop)**

- **Pros:**
  - IPS packet drop can stop the trigger packet, packets in a connection or from a source ip address
  - Being inline, the sensor can use stream normalization techniques to reduce or eliminate many of the network evasion capabilities that exist

- **Cons:**
  - Sensor must be inline and therefore sensor errors or failure issues can have an effect on network traffic
  - Overrunning an inline sensor’s capabilities (too much traffic) will impact the network
  - Sensor will have some effect on network timing (latency, jitter, etc). If not understood correctly, this can impact time sensitive applications (VoIP)
  - User deploying IPS response actions must have a well thought out security policy combined with a good operational understanding of their IPS deployments (Correctly tuned sensors are a must)
IDS/IPS Deployment Considerations

General Location Selection Issues

- Purpose of deployment defines location
  - Inside, outside, or DMZ
  - Internal vs. perimeter
  - Response actions vs. passive monitoring
- Trusted vs. non-trusted zones (chokepoints)
- Security operations vs. network operations
IDS/IPS Deployment Considerations

Specific Location Selection Issues

- Location requirements define platform (appliance vs. integrated security module)
- Sensor performance
  - Large network pipes can result in data overflow (IDS) or data disruption (IPS)
  - Proper platform selection is crucial
  - Load balancing issues:
    - Signature (i.e., sweeps and floods) fidelity
    - Data reduction possibilities (IDS): VACL capture
- Highly available or asymmetrically routed networks

IDS/IPS Deployment Considerations

Specific Location Selection Issues

- Encrypted traffic
  - SSL or IPSec
- IDS monitoring sources
  - Network taps
  - SPAN (and RSPAN)
  - VACL capture
  - Aggregation switch
  - In the actual data stream (IPS)
Additional Deployment Considerations: Organizational Issues

- As with all security technologies, it is critical to have a robust security policy
- Intrusion detection technologies cross many different business functions:
  - IT Security—Policy, deployment, monitoring
  - Networking—Traffic direction, active response
  - Server Admins—installation, maintenance
    - Who determines how/where to connect sensors on the network?
    - Switch configuration considerations, tap considerations, management considerations

Incident Response: Policies and Procedures

- Security policy must also address incident response
  - Must be approved by senior management
- Must address containment/recovery procedures
  - Which areas do you respond to first?
  - When do you start severing connections?
  - Under what circumstances do you notify senior management?
  - Under what circumstances do you engage law enforcement (if ever)?
Incident Response: Responding to an Intrusion

- Following investigation and alarm validation, an appropriate triage solution is put in place
- It is important to understand that this is not the end of the incident life cycle
  - A root cause analysis must be performed
  - A long term fix must be implemented
  - The IDS policy and security policy in general must be updated as appropriate

Planning Ahead: Other Resource Issues

- 24x7x365 monitoring and response capability
  - Cross-functional skill set (networking, security, operating systems, etc.)
  - Staffing and training considerations
  - Escalation paths—constant availability
- Consider outsourced managed security service provider
  - Could employ to augment internal security resources in cooperative fashion
  - Note that service level agreements for outsourced managed IDS/IPS services are difficult to develop
Agenda

• Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
• Network Sensors
  - Sensor Architecture
  - Remote Data Exchange Protocol (RDEP)
  - Sensor App and Micro-Engines
  - Signature Analysis
  - Environment-Based Tuning
  - Active Response
• Management Considerations
• Case Study
First Step: Getting Traffic to Your Network IDS

- Traffic must be mirrored to network sensors (replicated)
- Choices:
  - Shared media—Hubs are not recommended
  - Network taps
  - Switch-based traffic mirroring (SPAN) directly or from aggregation switch
  - Selective mirroring (traffic capture—VACLs)
Using a Network Tap

- Tap splits full duplex link into two streams
- For sensors with only one sniffing interface, need to aggregate traffic to one interface
- Be careful of aggregate bandwidth of two tapped streams

Switch-Based Traffic Capture

- Port Mirroring: SPAN functionality and command syntax varies between product lines and switch vendors
  - Some limit the number of SPAN ports
  - Some allow you to monitor multi-VLAN traffic
    - Note that not all sensor vendors can handle multi-VLAN traffic
- Rule-Based Capture: VLAN ACL Capture/MLS IP IDS
  - Policy Feature Card (PFC) required on Catalyst 6500
  - Allows you to monitor multi-VLAN traffic
  - Use "mls ip ids" when using "router" interfaces or when interface is configured for Cisco IOS FW
    http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/idsm/idsm_2/13074_03.htm
Switch-Based Traffic Capture Example

**Using SPAN (CatOS)**

```markdown
switch>(enable) set span 4/5 6/1 rx create
switch>(enable) set span 401 6/1 rx create
```

- Sets port 5 on module 4 and VLAN 401 to span to the monitoring port on the IDS Module in slot 6

**Using VACL (CatOS)**

```markdown
switch>(enable) set security acl ip WEBONLY permit tcp any any eq 80 capture
switch>(enable) set security acl ip WEBONLY permit tcp any eq 80 any capture
switch>(enable) commit security acl WEBONLY
switch>(enable) set security acl map WEBONLY 401
switch>(enable) set security acl capture-ports 6/1
```

- Captures web traffic on VLAN 401 only, and sends the captured traffic to the monitoring port on the IDS Module in slot 6

IPS Sensor Architecture: The Big Picture

![IPS Sensor Architecture Diagram](image-url)
Sensor Architecture: The Details

- Event Store
- IDAPI (Inter-Process Communication)
- IDS Device Manager
- Transactional Services (RDEP)
- CLI
- NAC
- SensorApp
- MainApp
- Web Server
- SSH/Telnet
- Sensor’s Mgmt Interface and TCP/IP Stack
- Sensing Interfaces

Sensor Architecture: The Components

- **Sensor Interfaces:**
  - Traffic inspection points, TCP Resets, IP Logging
- **SensorApp:**
  - “Sniffing” application
- **MainApp:**
  - Core IDS application
- **Event Store:**
  - Storage for all events (system and alarm)
- **IDAPI:**
  - Communication channel between applications
- **Web Server:**
  - Services all web and SSL requirements, including the IDS Device Manager (the integrated GUI), and transactional services such as remote management and monitoring through RDEP
- **SSH/Telnet:**
  - Services SSH and telnet requirements, for the CLI application
- **Network Access Control:**
  - Application for active response (blocking/shunning)
Event and Alarm Communication: RDEP

- **RDEP**: Remote Data Exchange Protocol
  - XML-based communications protocol between sensors and management apps
  - Encrypted using SSL
  - Event and transaction message entity bodies consist of XML documents
- Used by both IDS Event Viewer (small IDS deployments) and VMS/Security Monitor (large IDS deployments)

RDEP in Action
RDEPv2 or SDEE (Security Device Event Exchange)

SDEE—An Industry Standard

- Standardized IDS Communication Protocol adopted by IDSC
- Builds on Cisco RDEP
- XML-based
- Secured using SSL/TLS
- Simplifies management of heterogeneous security deployments and 3rd party integration

ICSA Labs IDS Consortium Announces Network Intrusion Detection System Alert Specification Format


MIDLANDS, UK—February 23, 2004—ICSA Labs, an independent division of Portland-b Corporation, today announced the development of the Security Device Event Exchange (SDEE), an intrusion detection system (IDS) alert format and transport protocol specification. SDEE is an XML-based alert format adopted by the members of the ICSA Labs Intrusion Detection Consortium and created by Cisco Systems and Sourcefire, two leading vendors including Internet Security Systems, Inc. (ISS) and Sourcefire.

IDSC members Jeff Haller and Mike Huil of Cisco Systems, Robert Alkins of ISS, Mimi Kanan of Sourcefire and Marcus Pimental of ThruSpace Corporation contributed the SDEE transport protocol specification format; the team will manage future revisions to the specification.

"Cisco is pleased to have participated in the development of this specification, and help address the industry-wide challenge of normalizing event messages in a common format," said Mike Muhmann, director of engineering at Cisco Systems. "This industry collaboration underscores the advancement of IDS technology adoption today."

Network IDS Sensor Packet Analysis: A Day in the Life of a Packet

Inputs and Outputs:

<table>
<thead>
<tr>
<th>Packets Input</th>
<th>Black Box</th>
<th>Alarms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Actions</td>
<td></td>
<td>Response Actions</td>
</tr>
</tbody>
</table>

© 2004 Cisco Systems, Inc. All rights reserved. Printed in USA.
Network Sensor Packet Analysis:
The Producer

Based on 4.x Sensor Code

Network Sensor Packet Analysis:
Virtual Sensor Processors
Network Sensor Packet Analysis: Virtual Alarm Processors

Signatures Revisited

- Simple pattern matching
  E.g. Look for “root”

- Stateful pattern matching
  E.g. Decode a telnet session to look for “root”

- Protocol Decode and Anomaly detection
  E.g. RPC session decoding and analysis; SNMP protocol anomaly detected from use of Protos Tool

- Heuristics
  E.g. Rate of inbound SYNs—SYN flood?
Signature Output: A Sample Alert

evAlert: eventId=1044479568210931009 severity=informational
originator:
  hostId: sensor
  appName: sensorApp
  appInstanceId: 913
time: 2004/02/05 21:15:39 2004/02/05 21:15:39 UTC
interfaceGroup: 0
vlan: 0
signature: sigId=6255 sigName=SMB Failed SMB Login
subSigId=0 version=S37
participants:
  attack:
    attacker: proxy=false
    addr: locality=OUT 172.16.50.122
    port: 3934
  victim:
    addr: locality=OUT 172.16.50.118
    port: 139

Scaling Analysis: Sensor Micro-Engines

• Traffic analysis is incredibly computationally intensive with large numbers of signatures
• Cisco IDS analysis implemented with a series of micro-engines
• Micro-Engine Types:
  ATOMIC  FLOOD
  OTHER   SERVICE
  STATE.STRING  STRING
  SWEEP  TROJAN
Signature Example: Protection at Layer 2 (Data Link Layer)

- Host Z is a malicious user, attempting to gain access to traffic from Hosts X and Y.
- Host Z sends gratuitous ARP replies, telling all that he is 10.10.10.1 (router), with his MAC address.
- Since ARP replies are broadcast, all hosts on the same L2 subnet see and accept the gratuitous ARP.
- If Host Z is more persistent than the actual router in asserting its identity, Host X and Y will believe that Host Z is the router.
- Host Z has effectively inserted himself in the middle, since Host X and Y will send it their IP traffic.

Signature ID 7105 Detects the above Attack

Alarm Guidance: NSDB

- Most products have an alarm database that provides guidance on alarms.
- Web or text-based DBs can allow addition of custom information or directions for operations staff.
Signature Updates

- Much like anti-virus, network IDS/IPS’s must be kept up to date
- Process must be developed to rapidly update new signatures as released
- Cisco releases regular updates, along with critical updates for major events (e.g. Slammer)
  

Tuning Your Sensors

- Tuning is the most important part of intrusion detection and prevention deployments
  
  The data reduction that results from proper tuning is essential for a fully functional system

- Not every sensor needs to alert on every event
  
  Implementing environment specific configurations increases scalability of the entire system
Tuning: Where to Start

• Most sensors ship with a default signature configuration
  This is a good starting point for an initial deployment in most cases

• Start by monitoring high/medium severity alarms
  Prioritize the tuning of the high priority alarms, and then move on to the mediums

How to Tune a Sensor: Techniques

• Understand the environment and traffic patterns

• List out potential false positives
  Analyze each alert and classify stimulus and response

• Define policy, and policy exceptions
  i.e. Ping sweeps generate alarms, except when coming from the management network

• Turn down severity of signatures not applicable to that environment

• Iterative process: as traffic patterns change, sensors can require re-tuning
Example Tuning Features

- **Signature Specific:**
  - Ports, Protocols, Services, Analysis Length, etc.
- **Filtering:** what networks to alarm on
- **MinHits:** number of events to see before alarm
- **Severity:** what level of alarm to send
- **Alarm Aggregation:** how many alarms to send
  - Alarm Throttle: Summarization characteristics
  - Alarm Interval: Summarization window
  - Choke Threshold: High water mark to force summary
- **Actions:** what to do following an alarm

Customizing Your Signature Set

- **Customize vendor-provided signatures**
- **New environment specific signatures can be created**
- **Cisco Custom Signature configuration tasks:**
  - Select the signature micro-engine that best meets your requirements
  - Enter values for the signature parameters that are required and meet your requirements
  - Save and apply the custom signature to the sensor
- **Signature customization is not trivial**
  - Writing signatures requires detailed knowledge of the attack.
  - Poorly focused signatures will generate false positives and too narrowly focused or outright mistakes might result in false negatives
  - Test, test and test again before you deploy
**Custom Signatures**

Choose Configuration > Sensing Engine > Signature Configuration > Custom Signatures

![Custom Signatures Diagram](image)

**Example: Port 80 Sweeps**

Choose Configuration > Sensing Engine > Signature Configuration > Custom Signatures

![Port 80 Sweeps Diagram](image)
Port 80 Sweeps (Cont.)

Active Response

• Promiscuous IDS’s allow a number of response actions to be taken when an alert is generated:
  
  TCP resets  
  Blocking using an external device  
  IP session logging

→ False Positives Can Be Problematic ←
→ Actions Configurable per Signature ←
Active Response

- IPS (Inline IDS) operates on the actual network packets instead of copies
  - Deny action to drop trigger packet, TCP connection packets or IP source address
  - TCP/IP Stream Normalization can be enforced on the packets traversing the network to prevent ambiguities or defeat deceptive techniques

→ False Positives Are Still Problematic ←
→ Actions Configurable per Signature ←

Configuring Response Actions

Choose Configuration > Sensing Engine > Signature Configuration > Custom Signatures
Forensics

- Logs traffic associated with a signature trigger (pcap format)
- Generally, only trigger and subsequent packets logged
- Does impact sensor performance
- Usage guidelines:
  - Tuning: Use during sensor tuning for event analysis and subsequent signature tweaking
  - Forensics: Useful to monitor "critical" signatures/resources
  - Handy tip: Use with a custom signature to monitor a specific service/server/user
  - Do not log unless you know what you plan to use the log for

IP Logging: Session Capture

- When signature fires, sensor logs packet data associated with the event: (source ip, connection, or trigger packet)
- Pros:
  - Useful for both troubleshooting of false positives and forensics
  - User must be technically competent to use to full advantage
- Cons:
  - Places a potentially considerable resource burden on the sensor (Imagine logging every packet the sensor gets)
TCP Resets: Session Sniping

- For TCP applications, connection is prematurely terminated by a RST sent from “sniffing” interface
- Must guess correct TCP sequence number and successfully insert RST into session
  - Makes TCP Resets somewhat unreliable especially when source and destination are “close”
- Certain applications will automatically reconnect and resend (e.g., SMTP), making this less effective
- Note that initial trigger packet will make it to its destination, so can’t necessarily stop event
  - Code Red 1 was a single packet attack and couldn’t be reset
- **Conclusion**: TCP Resets are a temporary solution while you readjust your security posture

Gotchas: TCP Resets and SPAN

**If You Use TCP Resets, You Must Enable Input Packets** so Switch Will Accept RST Packets on SPAN Port (Check your switch to determine exact support for IDS Reset packets)

```
set span <src_mod/src_ports...|src_vlans...|sc0> <dest_mod/dest_port> [rx|tx|both]
[inpkts <enable|disable>]
[multicast <enable|disable>]
[filter <vlans...>]
```

**If Monitoring Multiple VLANs, Cisco IDS Sources the Resets into the Correct VLAN**
TCP Resets

• When signature fires, sensor attempts to reset the TCP connection

• Pros:
  Fast enough to break many connections (Code Red 2+, Nimda)
  Lower chance of self-inflicted DoS if False Positive

• Cons:
  TCP Resets are an attempt at ‘Session Hijacking’ and are not always successful
  “Neither snow, nor rain, nor sleet, nor tcp resets …” Mail servers are notorious for always delivering the mail. Less useful to stop a determined attempt, they just keep trying.
  Some switches and taps are not compatible with TCP resets

Blocking (Shunning)

• When signature fires, sensor inserts ACL on router/issues shun command on PIX® Firewall
  Deny subsequent traffic from that source IP address or associated with that specific connection
  Note that initial trigger packets will make it to the destination because of the time required to establish the Block

• Sensor connects to firewall and/or router from management interface
  Need to configure authentication credentials for firewall/router
### Blocking

**Can Be Very Successful in Helping to Implement a Security Policy**

- **Pros:**
  - Best used to thwart an attacker at the first location possible
  - Can be used to block a source address at multiple locations (blocking using more than one router/firewall)
  - Sensor does not have to be inline (can be promiscuous)

- **Cons:**
  - Does not stop the trigger packet or even a connection; used to stop an attacker more than the attack itself
  - Less useful in stopping thousands of automated attackers (i.e. Worms) depending on external platform, or for email viruses
  - User must have a well thought out security policy combined with a good operational understanding of their IDS deployments (correctly tuned sensors are a must)

### Packet Dropping (Inline Only)

**When Signature Fires, Sensor Discards the Packet That Triggered the Alarm**

- **Pros:**
  - Stops the Trigger Packet itself
  - Most useful for events that are triggered frequently (i.e. Worms) because they limit the effect of the event with less impact to other resources (no 2000 line ACL on the border router)
  - Lower chance of self-inflicted DoS if False Positive (unless drop source is used)

- **Cons:**
  - Less useful to stop a determined attacker as he will just move on to other attacks that may not be detected (unless drop source is used)
  - Sensor must be Inline to perform this action

- **Limitation:** Traffic that does not pass through the sensor cannot be scrubbed in this manner
Coordinated Attack Mitigation

When Event Is Triggered, Sensor Reports the Event to a Monitoring Station That Pushes Down Knowledge of the Attack to Multiple Enforcement Endpoints

**Pros:**

- Stops the attack at multiple locations independent of the initial detection
- Most effective response for events that spread rapidly (i.e. Worms) because it distributes the detection/containment knowledge into the network to prevent and contain any spread
- Initial detection sensor can be inline or promiscuous; enforcement points must be inline
- Enforcement points do not have to be full featured IDS/IPS and can therefore be deployed to more locations

**Cons:**

- Requires multiple integrated components to be effective
- This response action, by itself, will not stop the attack; must be combined with an effective first response to be most effective

---

Coordinated Attack Mitigation

**Distributed View through Network Collaboration**

- Dynamic policy enforcement
- Corroboration through shared observations

[Diagram showing network collaboration and security solutions]
DoS/DDoS Attack Mitigation (Riverhead)

MANAGEMENT CONSIDERATIONS
Agenda

- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- Network Sensors
- Management Considerations
  - Management Paradigms
  - Secure Management Guidelines
  - The Intrusion Detection Challenge
  - Scaling IDS Management
- Case Study

Management Paradigms

Device-Level Management

- Small deployments
  - 1–5 sensors
- Low alarm rates

Multi-Device Management

- Medium/large deployments
  - Many sensors
- High alarm rates
Secure Management Guidelines: Out of Band Management

- Monitoring and Management Network Segment
- A conceptual air gap between IDS and Management segment provides the most security

When Out of Band Management Isn’t Possible

- When an “air-gapped” management subnet isn’t possible:
  - Encrypt all in-band communications (SSH, SSL, or IPSec)
  - Firewall all access points to the Management Network
- Use IPSec tunnel between network devices when traversing “un-trusted” networks
  - Aggregate multiple sensors though one tunnel
In-Band Management Through Tunnels

- **Firewall brokers** connection from inside to Management Segment
- **Encrypted tunnels** terminated at firewall or at Management Station

The Intrusion Detection Challenge: Turning Data into Information

The Single Biggest Barrier to Large Scale IDS Deployments Is Dealing with All the Data They Generate

- Intrusion detection systems have a (somewhat well deserved) reputation for being very noisy
- If not solved, this problem will eventually cripple the IDS system
- The challenge is to optimize the entire system to get the most usable information out
The Solution
Alarm Validation: Cisco Threat Response

- Emerging capability in the market—automated alarm validation
- **Alarm validation:**
  - Make intelligent decisions on the validity of an alarm
  - Increase or decrease the severity of the alarm appropriately

How Threat Response Works

- **Was the attack successful? (eliminate and escalate)**
  - Target vulnerability check (Level 1)
  - OS detection (via NMAP)
  - Detect web servers
  - Detailed system investigation of Windows targets (Level 2)
    - Registry analysis (via Win32 system calls)
      (i.e. service pack check)
    - File system analysis (via SMB) (i.e. capture log files)
    - Level 2 investigation requires login to target box
- **What can be done about it? (remediate)**
  - Forensic evidence retrieval
  - Includes capture of impacted files and logs
**Threat Response Components**

**Server**
- Receives alarms from monitored IDS
- Performs all investigations using agents
- Performs all storage

**Client**
- Browser access to the server for management and monitoring

---

**Agents Defined**

**What is an agent?**
- In Threat Response an agent is a built-in active or passive procedure used to investigate an attack
- Level 0 agents use rule-based analysis (preset upgrade/downgrade)
- Level 1 agents use minimum-impact methods to determine vulnerability and impact
- Level 2 agents connect to the targeted host and look for traces and indicators of a successful attack directly on the affected system

**Why does this matter?**
- Allows deployment with minimum install
- “Just in Time” analysis is always up to date
- Impact of the investigative agents is minimal on end hosts
Intrusion Protection Without Validation

1. An attacker launches auto-scanner script to search for a common Microsoft IIS unicode vulnerability
2. The IDS sensor reports a number of detected attacks against the servers on your network
3. The security administrator sees dozens of real attack events on their IDS and correlation screens; time is wasted investigating each one

<table>
<thead>
<tr>
<th>Three Attacks</th>
<th>Alarm</th>
<th>Alarm</th>
<th>Alarm</th>
</tr>
</thead>
</table>

15 Minutes Manually Investigating Each Alarm
Total Elapsed Time = 45 Minutes

Intrusion Protection with Validation

1. An Attacker Launches Auto-Scanner Script to Search for a Common Microsoft IIS Unicode Vulnerability
2. The IDS Sensor Reports a Number of Detected Attacks against the Servers on Your Network
3. Threat Response Technology Quickly Assesses the Targeted in Real-Time without Prior Network Knowledge or Installed Remote Agent Software

Investigation Steps for Successful IIS Unicode Attack:
1. Does the attack target this OS type? (Level 1)
2. Is the OS vulnerable? (Level 1)
3. Are there traces of a successful attack? (Level 2)
4. Copy and secure forensic evidence (Level 2)
5. Administrator alerted to real and confirmed attack

<table>
<thead>
<tr>
<th>Three Attacks</th>
<th>Linux Not Vulnerable</th>
<th>Win NT VULNERABLE</th>
<th>Win NT VULNERABLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm</td>
<td>OS Patched</td>
<td>OS Not Patched</td>
<td></td>
</tr>
<tr>
<td>Attack Traces Found</td>
<td>Collect Evidence</td>
<td>Alert Security Staff</td>
<td></td>
</tr>
</tbody>
</table>

Total Elapsed Time = 5 Seconds
Scaling Intrusion Detection Management

• Scalability limitations:
  - Sensor-to-console ratio
  - Aggregate event rate

• Solutions:
  - Sensor/Agent Level: Use tuning and alarm validation techniques for data reduction
  - Network Level: Hierarchical deployment
  - Console Level: Event correlation, separate configuration, monitoring, and archive stations
  - User Level: Notification Services

Network Level: Hierarchical Management

Local vs. Global Management Domains

• Local consoles managing local sensors—detailed analysis
• Global consoles managing high level, critical events—event correlation is important here
Console Level: Event Correlation

- Event Correlation: Combining multiple alarms into one meaningful security incident
- Many products trying to solve this problem
- While not completely “solved”, good steps have been made

Console Level: Archival/Trend Reporting Database

- Run on separate platform and database
- Determine how long you want to keep data
  - Regulatory or policy considerations
- Can import alarm data from log files on:
  - Sensors
  - Monitoring consoles
User Level: Scaling Monitoring

- Most products have some sort of notification feature
e.g., E-mail sent when event detected with some event information
- Use notifications to let you know something significant happened
  - Rule of thumb for pager notification: Only page you if it’s something you want to know about at 3am
- Then look at console for details
  - Web-based console functionality (e.g., Security Monitor) make this easier
- Caution: Overuse of notifications can actually lead to a DoS effect on page or mailer systems
Agenda

- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- Network Sensors
- Management Considerations
- Case Study
  Large Bank Example

Example Scenario: Large Bank

- A large bank has implemented a firewall solution according to their policy:
  All communication is denied by default
  Defense-in-depth must be practiced
  All incoming sessions must terminate on an endpoint outside the corporate network
  All incoming malicious content must be removed at the firewall
- Data sensitivity:
  All data of the electronic banking application is very sensitive
  Data in internal Oracle databases is extremely sensitive
  Internal email messages are extremely sensitive
Example Scenario: Large Bank

Enterprise Application Requirements:

- An electronic banking solution is built using HTTPS, CORBA, and MS SQL server (three-tier)
- Hosting of public WWW and DNS servers is needed
- SMTP email is exchanged with the Internet
- Only HTTP is allowed to the Internet, active content must be filtered
- Upper management must read email from the Internet

Example Scenario: Large Bank

- This is the perimeter design chosen to implement the solution:
  
  Integrate NIDS sensors into the system
Example Scenario: Large Bank

IDS Design Requirements:

• First priority is to watch the e-banking application
• Second priority is to watch for other firewall misconfigurations
• Third priority is to watch exposed public servers
• Must monitor outbound traffic (worms, tunnels)
• Provide automatic response, where possible

Watching the E-Banking Application

Three Focused NIDS Systems
Watching for Firewall Misconfiguration

- Two new NIDS sensors (outside, inside):
  - Outside broad, inside policy focused
  - Additional policy configuration on e-banking sensors
  - Optional third sensor in the middle DMZ

Watching the Public Servers

- Two options for NIDS—either focus the outside sensor on public servers, or have dedicated sensors:
  - Additional focusing on “inside” IDS for mail sessions
Watching Outbound Traffic

The “inside” sensor has a broad monitoring policy by default (all default signatures enabled):
Will catch attacks to the outside, used to identify compromised internal hosts (worms, viruses, etc)

IDS Response Actions

DMZ and Inside NIDS talks to nearby PIX’s for blocking:
Only signatures, which are of “true” high severity, and require the establishment of a TCP session, trigger blocking
Outside NIDS performs no blocking as the information it sees is uncontrolled and potentially filled with spoofed data and addresses
IDS Response Actions

• DMZ and Inside NIDS talks to a nearby PIX for blocking:
  DMZ and Internal servers are never blocked with NIDS, can use TCP resets

Example Scenario: Summary

Successful IDS Implementations Depend on Understanding and Following These Guidelines:

• Build a prioritization list on what you need to watch most, based on risks
• Purpose of deployment defines location
• Location requirements define platform
• Carefully design IDS management
Summary

• Intrusion detection/prevention is an exciting, evolving field of technology
• Effective deployment strategies are critical to the successful implementation of the technology
• Intrusion detection/prevention has become a key piece of a defense in depth strategy
While at Networkers…

- SEC-2004: Responding to Security Incidents
- SEC-2006: Managing Security Technologies
- SEC-2031: Understanding and Deploying Host-based Intrusion Protection Technology
- SEC-3030: Troubleshooting Intrusion Detection Systems

Further Reading

- Cisco IDS product documentation
- Cisco IDS Discussion Forum
  http://www.cisco.com/go/netpro
- Proactive Field Notices Tool for signature updates
  http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice
- Document describing SPAN functionality on Cisco switches
- Cisco SAFE Blueprint
  http://www.cisco.com/go/safe
- Cisco Security Advisories (includes a number of security documents)
- Vulnerability information
- Ethereal tool to view IP Session Logs
  http://www.ethereal.com
Recommended Reading

- Cisco Secure Intrusion Detection System
  ISBN: 158705034X
- Managing Cisco Network Security
  ISBN: 1578701031
- Network Security Principles and Practices
  ISBN: 1587050250

AVAILABLE ONSITE AT THE CISCO COMPANY STORE

Recommended Reading

- CCIE Exam Certification Guide: Security
  ISBN: 1587200708
- CCIE Practical Studies: Security
  ISBN: 1587051109

AVAILABLE ONSITE AT THE CISCO COMPANY STORE
Complete Your Online Session Evaluation!

**WHAT:** Complete an online session evaluation and your name will be entered into a daily drawing

**WHY:** Win fabulous prizes! Give us your feedback!

**WHERE:** Go to the Internet stations located throughout the Convention Center

**HOW:** Winners will be posted on the onsite Networkers Website; four winners per day