

# CISCO SYSTEMS



# Sistemi di prevenzione delle intrusioni

*Marco Misitano, CISSP*

*Enterprise Consulting, Security  
misi@cisco.com*

- **Intrusion Detection and the Security Architecture**
- **Deploying Network Sensors**
- **Deploying Host Sensors**
- **Building the Management Infrastructure**

# Intrusion Detection and the Security Architecture

# IDS Components

- **Sensors**

**Specialized software and/or hardware used to collect and analyze network traffic**

**Network IDS: Appliances, modules, embedded**

**Host IDS: Server-Specific Agent**

- **IDS Management**

**Performs configuration and deployment services**

**Alert collection point for monitoring**

**Single device, multi-device**

# IDS Fundamentals: False Positives and False Negatives

- **False Positives:** Benign activity that the system mistakenly reports as malicious
- **False Negatives:** Malicious activity that the system does not detect or report

# IDS Fundamentals: Signatures and Anomalies

- **Signatures** explicitly define what activity should be considered malicious

Simple pattern matching

Stateful pattern matching

Protocol decode-based analysis

Heuristic-based analysis

- **Anomaly** detection involves defining “normal” activity and looking for deviations from this baseline

# Pattern Matching

- **Looking for a fixed sequence of bytes in a single packet. Can be associated with a specific service.**
- **Pros**
  - + simple
  - + direct correlation (highly specific)
  - + reliable alerts (for the specified pattern)
  - + applicable across all protocols
- **Cons**
  - false positive rates (pattern not has unique as assumed)
  - any attack modification lead to false negative
  - does not apply well to stream based traffic (single packet inspection)
  - do not scale can dramatically slow performance (too much to grep and to much to manage!)
  - blind until new pattern is developed
  - evasion is somewhat easy

# Stateful Pattern Matching

- **Matches are made in context within the state of the stream.**
- **Pros**
  - + only lightly more effort than simple pattern matching
  - + direct correlation (highly specific)
  - + reliable alerts (for the specified pattern)
  - + applicable across all protocols
  - + evasion becomes more difficult
- **Cons**
  - false positive rates (pattern not has unique as assumed)
  - any attack modification lead to false negative
  - may require multiple signatures to deal with a single vulnerability
  - blind until new pattern is developed

# Protocol Decode-Based Analysis

- **Decode protocols elements like the client or server in the conversation would do then look for RFC violations (fields content, header and payload size, special characters,...)**
- **Pro**
  - + minimize the chance for false positive (for well defined protocols)
  - + direct correlation (highly specific)
  - + broader method to allow catching variations
  - + reliable alerts (for the specified protocol)
  - + better performance
- **Cons**
  - can lead to high false positive if the RFC is ambiguous (grey area)
  - longer and more complex development time

# Heuristic-Based Analysis

- **Based on algorithmic logic such as statistical evaluations of the type of traffic being presented.**
- **Pros**
  - + some types of suspicious activity cannot be detected through other means
- **Cons**
  - algorithm may require tuning or modification

# Anomaly-Based Analysis

- **Look for traffic that deviates from what is seen “normally”. Issue is to define what “normal” is. If normal is hard-coded then it becomes heuristic-based. Learning what normal is sounds like the panacea but it’s only been limited to academia research so far and with limited success.**
- **Pros**
  - + can detect unknown attack (if implemented properly)
  - + low overhead (no new signature to develop and install)
- **Cons**
  - no intrusion data granularity (no pattern, unknown attacks)
  - highly dependant on what has been learn as normal

# Bottom Line Analysis

- **To do its job right, a good IDS must implement various analysis technology**
- **The number of attacks detected is much more relevant than the number of signature supported or used**
- **IDS challenges are**
  - Minimizing false positive**
  - Minimizing false negative**
  - Keeping up with performance**
  - Handling the large amount of data generated**

# Some General Pros and Cons

	Pros	Cons
Host-Based	<ul style="list-style-type: none"><li>• Can verify success or failure of attack</li><li>• Generally not impacted by bandwidth or encryption</li><li>• Understands host context and may be able to stop attack</li></ul>	<ul style="list-style-type: none"><li>• Some impact on host resources</li><li>• Operating system dependent</li><li>• Scalability—Requires one agent per host</li></ul>
Network-Based	<ul style="list-style-type: none"><li>• Protects all hosts on monitored network</li><li>• No host impact</li><li>• Can detect network probes and Denial of Service attacks</li></ul>	<ul style="list-style-type: none"><li>• Switched environments pose challenges</li><li>• Very processor intensive</li><li>• Can't proactively stop some attacks (single packet)</li></ul>

**Should View as Complementary!**

# 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**
- **Remember that Host IDS and Network IDS are complimentary technologies that serve unique functions in the Security Architecture**

# Deploying Network Sensors

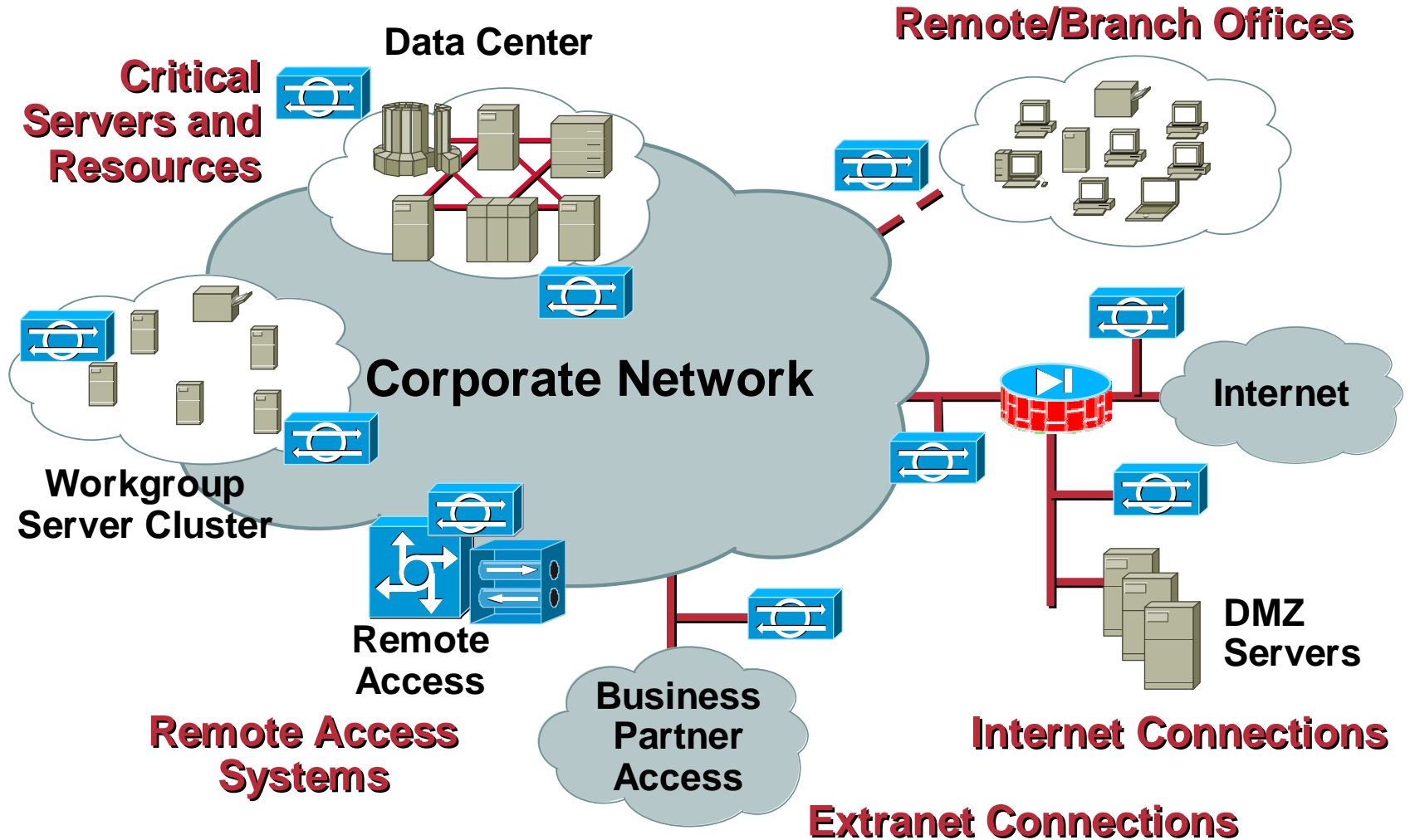
# Network Sensor Deployment Tasks

- 1. Determine what traffic you need to monitor to protect your critical assets**
2. Connect sensors to network
3. Apply initial configuration
4. Run for a week or so with initial configuration
5. Analyze the alarms and tune out False Positives
6. Selectively implement response actions
7. Update sensors with new signatures

# Network IDS: Monitoring Traffic

- **Must see **all** of the monitored traffic**
- **Must be able to keep up with monitored traffic**
- **Normally not pass-through devices**
- **Normally limited to monitoring LAN media segments**

# Typical Sensor Placement



# Why at Internet Connections?

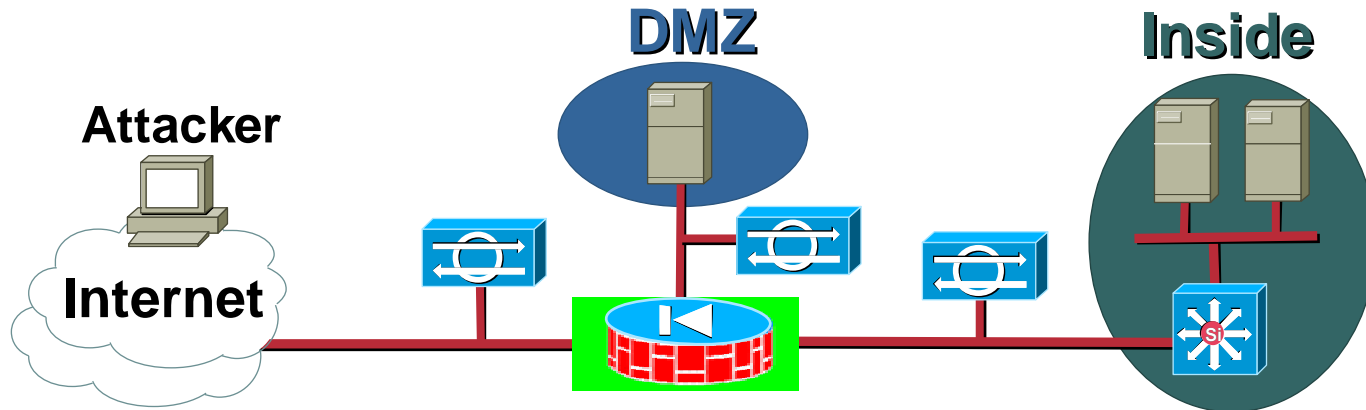
- **Firewalls usually don't protect against data-driven attacks**
- **Consider scenario where you have Web servers on DMZ**

**A number of Web server vulnerabilities discovered during the past year**

**Patches available from vendors, but...**

- **Can be exploited to deny service and/or access the server**

# Sensors on Outside or Inside?



- **Sensor on Outside**

- Sees **everything** including traffic blocked by firewall

- Can't tell what is denied or permitted by firewall

- Tools like Stick and Snot can generate lots of "noise"

- Monitors both DMZ and inside traffic

- **Sensors on Inside**

- Sees only traffic **permitted** by the firewall

- You know you need to respond

- Need sensor on each internal leg off firewall

# Network Sensor Deployment Tasks

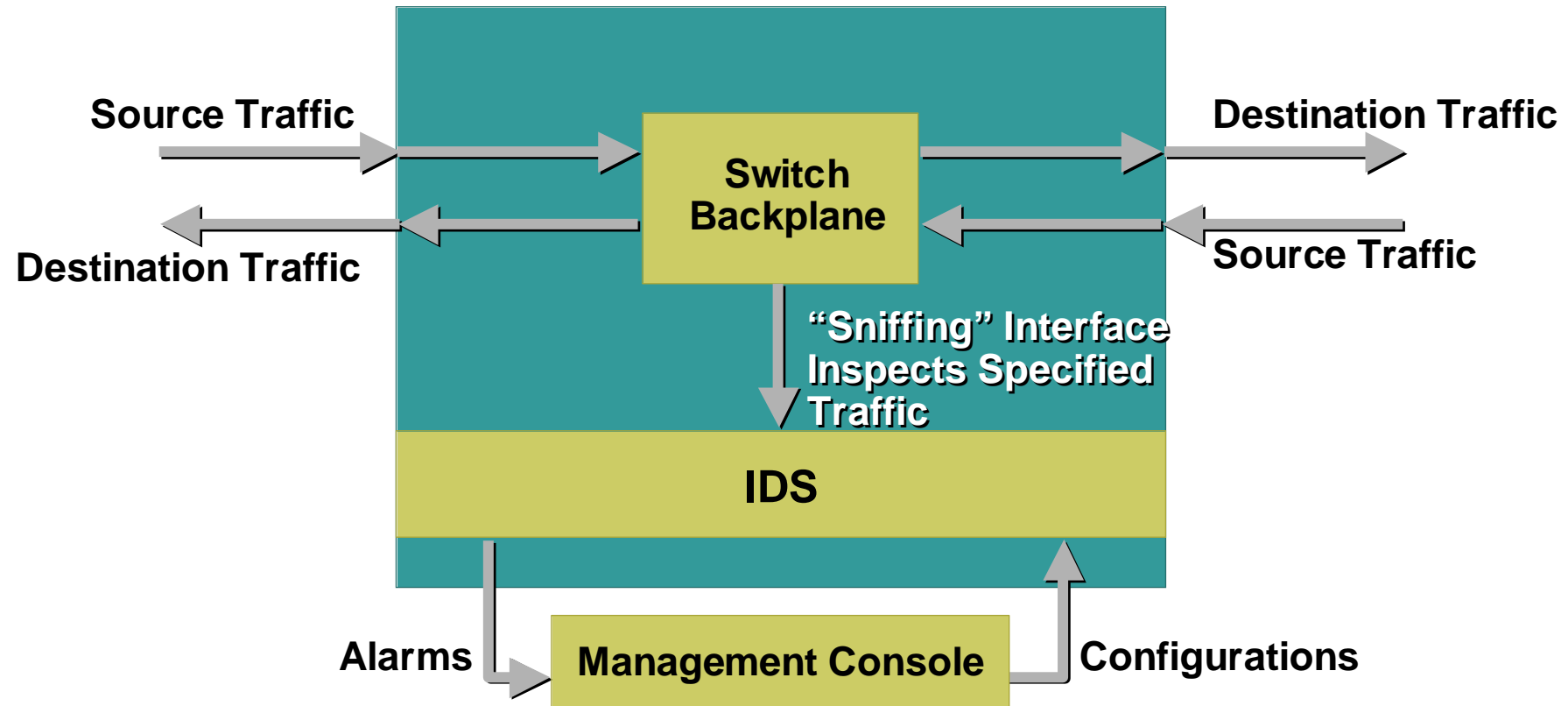
1. Determine what traffic you need to monitor to protect your critical assets
2. **Connect sensors to network**
3. Apply initial configuration
4. Run for a week or so with initial configuration
5. Analyze the alarms and tune out False Positives
6. Selectively implement response actions
7. Update sensors with new signatures

# Connecting the “Sniffing” Interface

- **Rule-of-Thumb: If you can't see the traffic of interest with a sniffer, then the sensor will not work!**
- **Fairly easy to connect sensor to shared media hub**

**Simply plug sniffing interface into open port on hub**

# Switch-Integrated Sensor



# Network Sensor Deployment Tasks

1. Determine what traffic you need to monitor to protect your critical assets
2. Connect sensors to network
3. **Apply initial configuration**
4. Run for a week or so with initial configuration
5. Analyze the alarms and tune out False Positives
6. Selectively implement response actions
7. Update sensors with new signatures

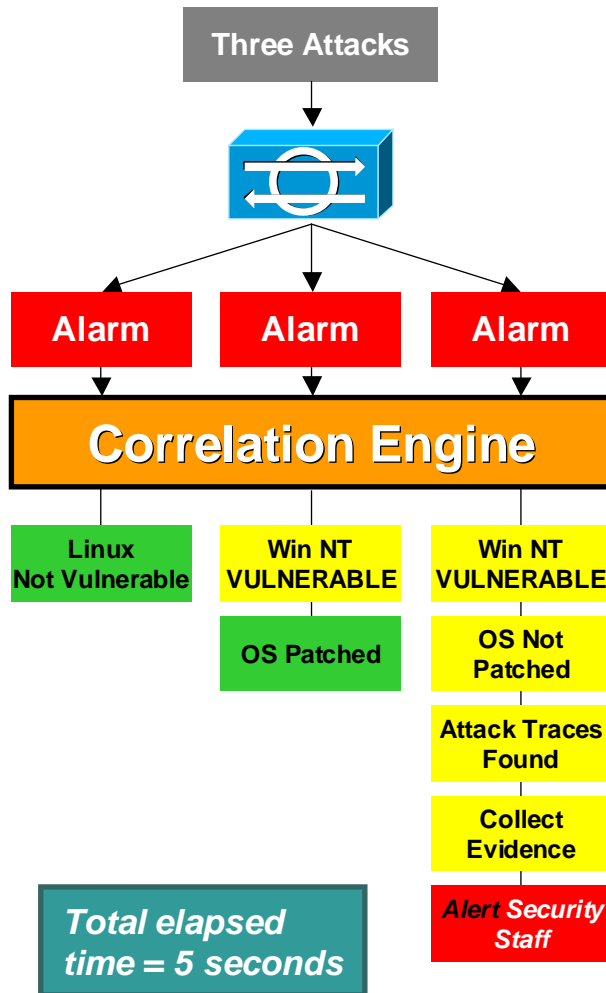
# Network Sensor Deployment Tasks

1. Determine what traffic you need to monitor to protect your critical assets
2. Connect sensors to network
3. Apply initial configuration
4. **Run for a week or so with initial configuration**
5. **Analyze the alarms and tune out False Positives**
6. Selectively implement response actions
7. Update sensors with new signatures

# The False Positive Problem

- **The False Positive problem:**
  - All IDS products are susceptible to False Positives**
  - Too many False Positives turn into white noise, making it harder to notice real attacks**
- **“False Positive” is actually a misnomer**
  - Detected activity is real, but not malicious**
  - e.g., Network Management Station doing node discovery uses ping sweeps**
- **Determining if event is a False Positive can take time**
  - Must understand network environment to determine if event is False Positive or not**

# Correlation



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

# Network Sensor Deployment Tasks

1. Determine what traffic you need to monitor to protect your critical assets
2. Connect sensors to network
3. Apply initial configuration
4. Run for a week or so with initial configuration
5. Analyze the alarms and tune out False Positives
6. **Selectively implement response actions**
7. Update sensors with new signatures

# Typical Response Actions

- **IP session logging**
- **TCP resets**
- **Shunning/blocking**

**→ False Positives are very problematic ←**  
**→ Actions configurable per signature ←**

# Network Sensor Deployment Tasks

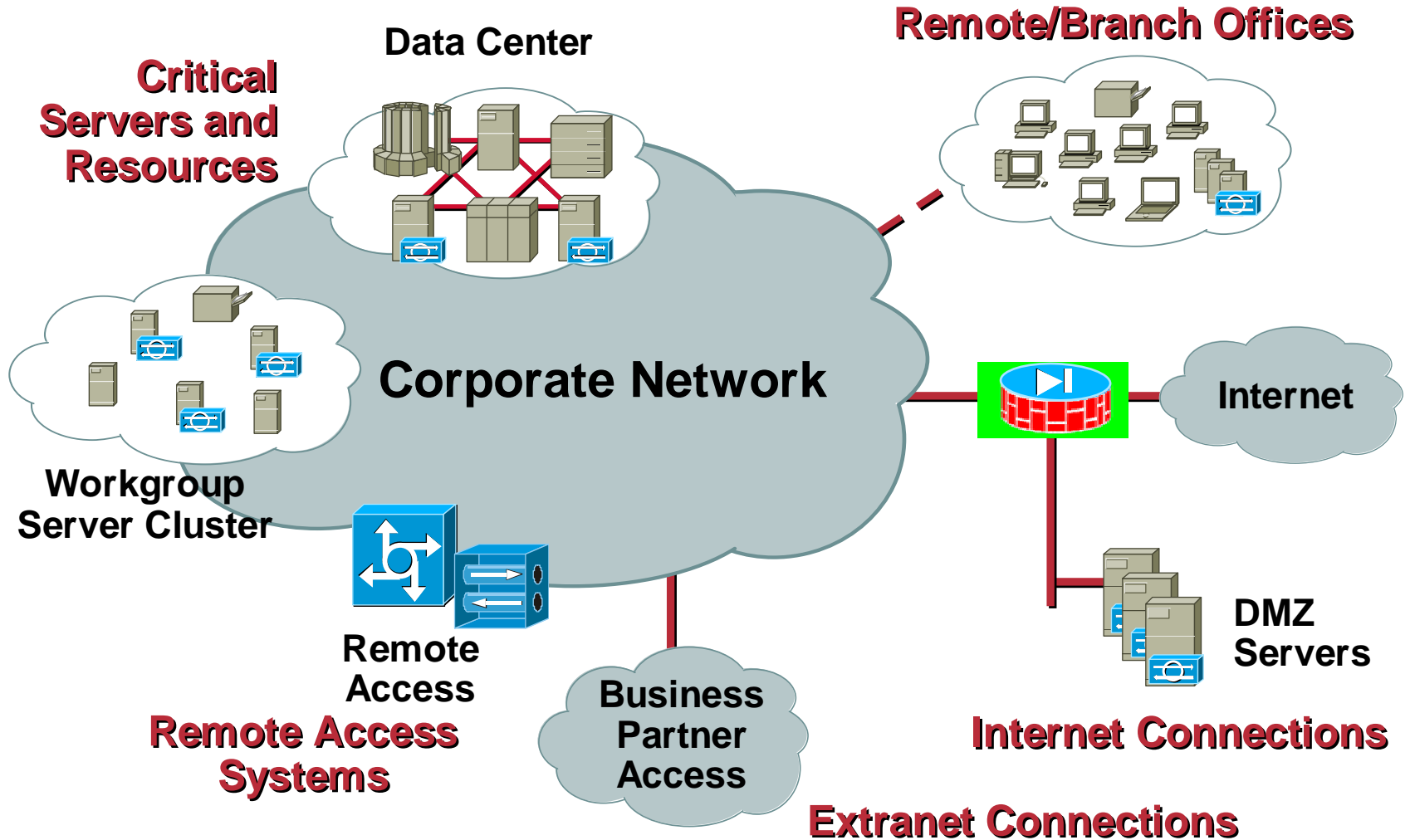
1. Determine what traffic you need to monitor to protect your critical assets
2. Connect sensors to network
3. Apply initial configuration
4. Run for a week or so with initial configuration
5. Analyze the alarms and tune out False Positives
6. Selectively implement response actions
7. **Update sensors with new signatures**

# Deploying Host Sensors

# Host Sensor Deployment Tasks

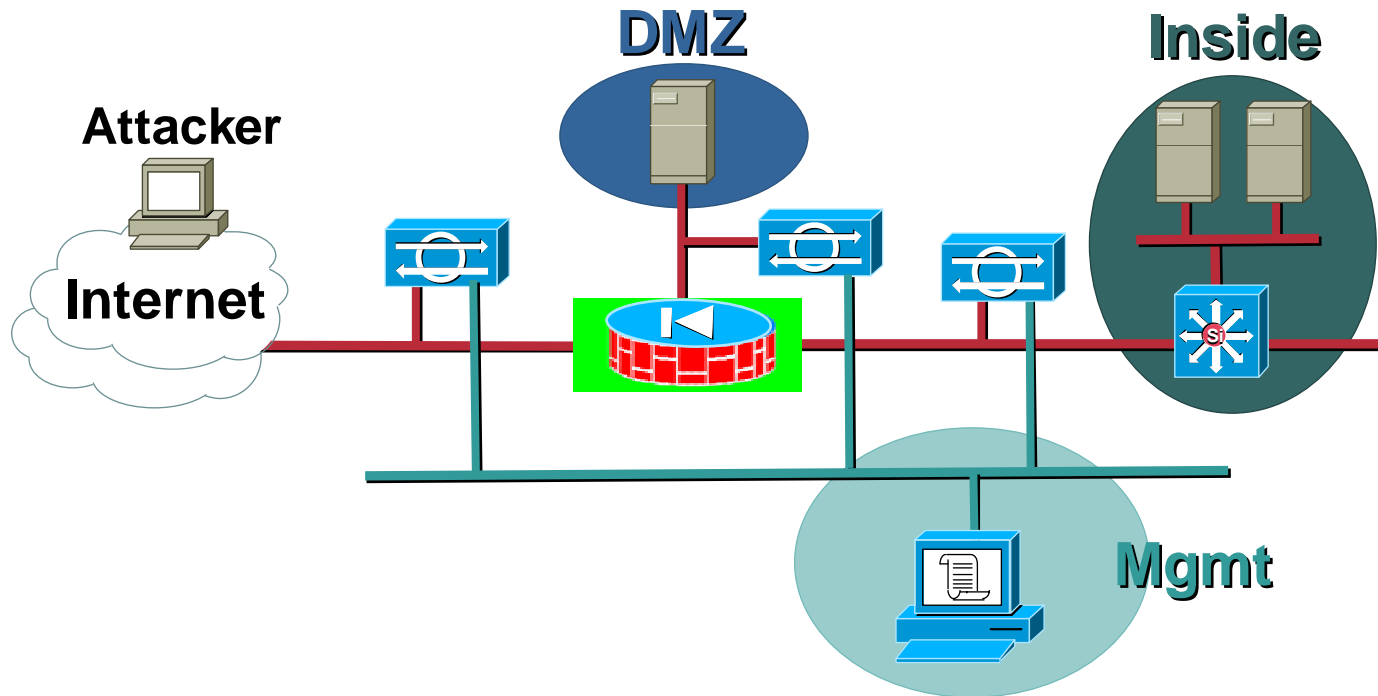
- 1. Determine what hosts you need to monitor to protect your critical assets**
- 2. Install sensor agents on hosts**
- 3. Apply initial configuration**
- 4. Run for a week or so with initial configuration**
- 5. Analyze the alarms and tune out False Positives**
- 6. Selectively implement response actions**
- 7. Update sensors with new signatures**

# Typical Host Sensor Placement



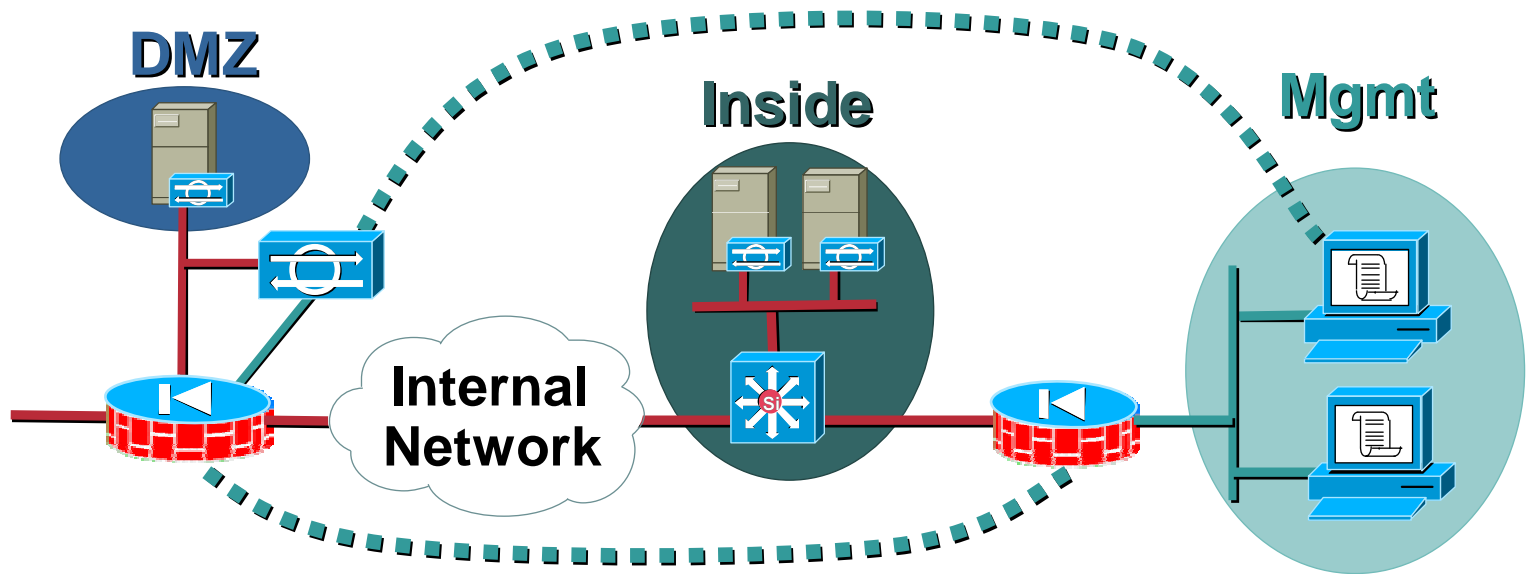
# Building the Management Infrastructure

# Secure Management Out of Band



- Monitoring and Management network segment
- A conceptual **air gap** between IDS and Management segment provides the most security

# Inband Management through Tunnels



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

# Causes for Excessive Event Rates

- **Poorly tuned sensors**
- **Logging every connection on your network**
- **An attacker running IDS DoS tools like Stick/Snot**

**Usually not a problem for sensors inside the firewall**

# So, How Do I Scale?

- **Look at monitoring and configuration separately**

Could be implemented on one platform or could be split up

- **Look at archival/trend reporting subsystems completely separately**

Performance impact of complex queries for reports while inserting events at high rates

- **Scaling configuration management isn't as difficult as monitoring**

Don't make configuration changes often

Not much to configure after initial bootstrap

- **Management Hierarchy**

# Intrusion Detection: Summary

# Summary

- **IDS is a valuable complement to your existing security mechanisms if properly implemented**  
Part of defense-in-depth strategy
- **Network Sensors and Host Sensors are distinct, complimentary technologies**
- **Deploying and managing IDS doesn't have to be difficult**
- **The technical aspects of deploying IDS is just part of the overall task**  
Assemble a cross-functional team
- **Start small, but design/prepare for quick growth**

# CISCO SYSTEMS



EMPOWERING THE  
INTERNET GENERATION