NETWORK

SECURITY

10 Intrusion Prevention System

Contents

- Intrusion Prevention Systems

- Reference:
  - John Wiley & Sons Network Security: Current Status and Future Directions,
    - Chapter 07 : Intrusion Detection vs Intrusion Protection

Background

- Internet and e-commerce boom

  → organizations become more vulnerable to electronic malice

- Increase quantity and sophisticate attacks on IT assets could make companies loss of revenue
  - breach of data
  - loss of customer confidence
  - job productivity degradation

Defense - Firewall

- Firewall acts as a perimeter guard for a network
  - determines which traffic to allow or deny in and out
- Firewall applies policy (accept or deny) by criteria
  - e.g.: allows common services (SMTP, HTTP, FTP, DNS and drops other
  - by criteria (e.g.: source, destination, and port)

Defense – Firewall

- *firewall primary purpose is to protect a private network (usually internal) from a public network (usually the Internet) by checking all data passing between these networks and preventing unwanted conversations from occurring*

Defense – Firewall

- is a firewall enough to secure your network?

Defense – Firewall

- only control what goes in and out
  - cannot look into the content of traffic

- cannot protect attacks contained within the traffic that allowed into the network

Protection Techniques

A view from layered architecture:

LAYER	1	2	3	4	5	6	7
Stateless			O	O			
Proxy			O	O			O
Stateful			O	O	O	O	O
IPS	O	O	O	O	O	O	O

social engineering, Trojan horse or back door may actually "show up" as originating from inside network and spread from within

Is a firewall enough to secure your network?" is a resolute "No."

Good and Bad News

- Good: Many available products to detect and protect
  - NIDS
- Bad: perceived value of NIDSs is low
  - Overreliance on Firewall.
  - False Alarms.
  - Low Manageability, High Maintenance.
  - Perceived Need to Outsource
  - No Prevention of Attacks

IPS

- *we've ever discussed IDS, so skip skip..*

- *The emerging fourth generation of each of these technologies represents a convergence of firewall and IDS and is commonly called intrusion prevention system (IPS)*

IPS

- IPSs use IDS algorithms
  - to monitor and drop or allow traffic based on expert analysis.
- IPSs normally work at different areas in the network and proactively police any suspicious activity that could otherwise bypass the firewall
- IPSs can operate on all layers in the OSI model,

DETECTION VS PREVENTION

- Share similar functions:
  - packet inspection, stateful analysis, fragment reassembly, Transmission Control Protocol (TCP) segment reassembly, deep-packet inspection, protocol validation, and signature matching
- But different purposes of deployment:
  - IDS: provide monitoring, auditing, forensics, and reporting of network activity
  - IPS: protect against false positive attacks

*false positive: event signaling of IDS that produce an alarm when no attack has taken place

- Some attacks are just plain hard to detect with any degree of certainty, and most can only be detected by methods that are nondeterministic in nature

IPS

- intended to provide protection for assets, resources, data, and networks.
- primary expectation is to reduce threat of attacks by eliminating harmful and/or malicious network traffic while continuing to allow legitimate activity
- The goal is a perfect system – no false positives that reduce end-user productivity and no false negatives that create undue risk within the environment.

he difference between IDSs and IPSs

- IDSs can (and should) use nondeterministic methods to divine any sort of threat, or potential threat, from existing and historical traffic.
- IPS must be deterministic—correct—in all of its decisions in order to perform its function of scrubbing traffic.

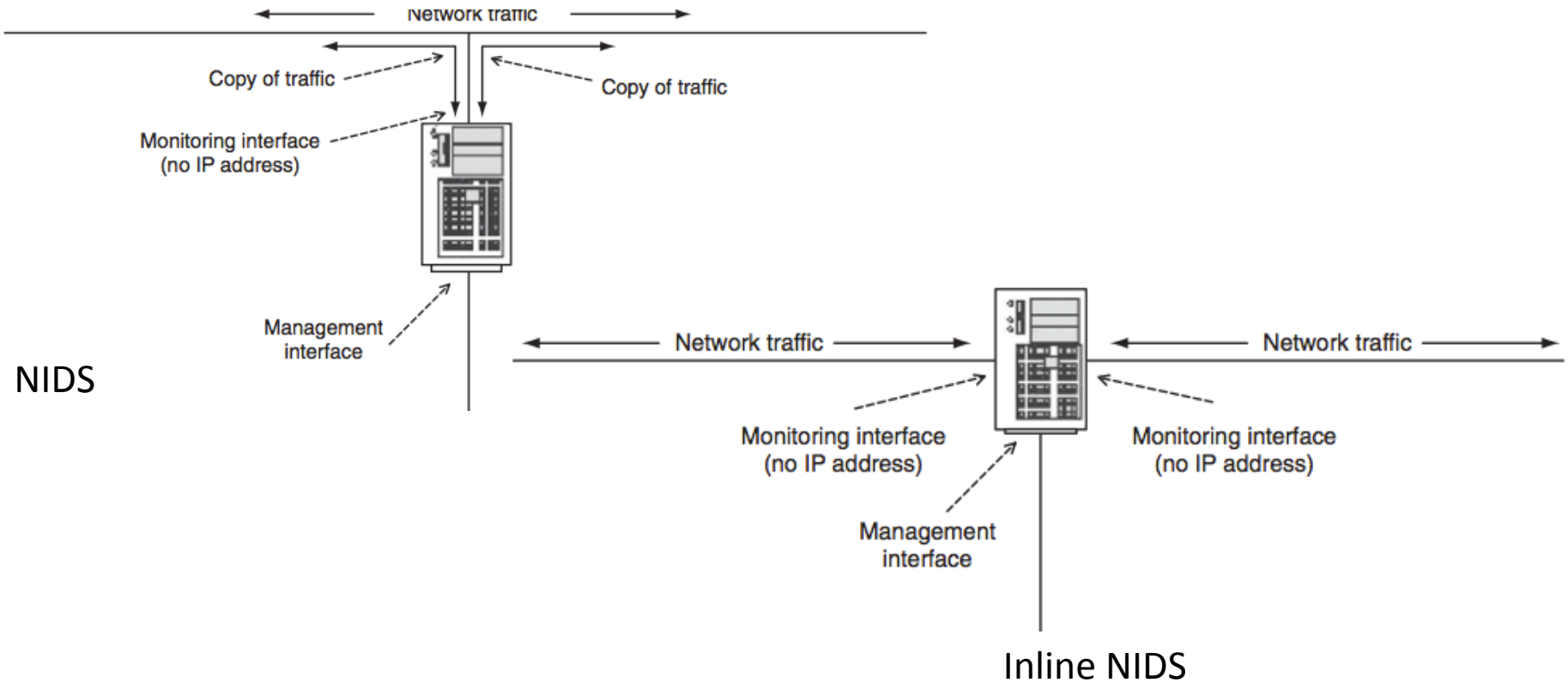
The five types of IPSs

- Inline NIDS,
- Application-based firewalls/IDSs
- Layer 7 switches
- Network-based application IDSs
- Deceptive applications

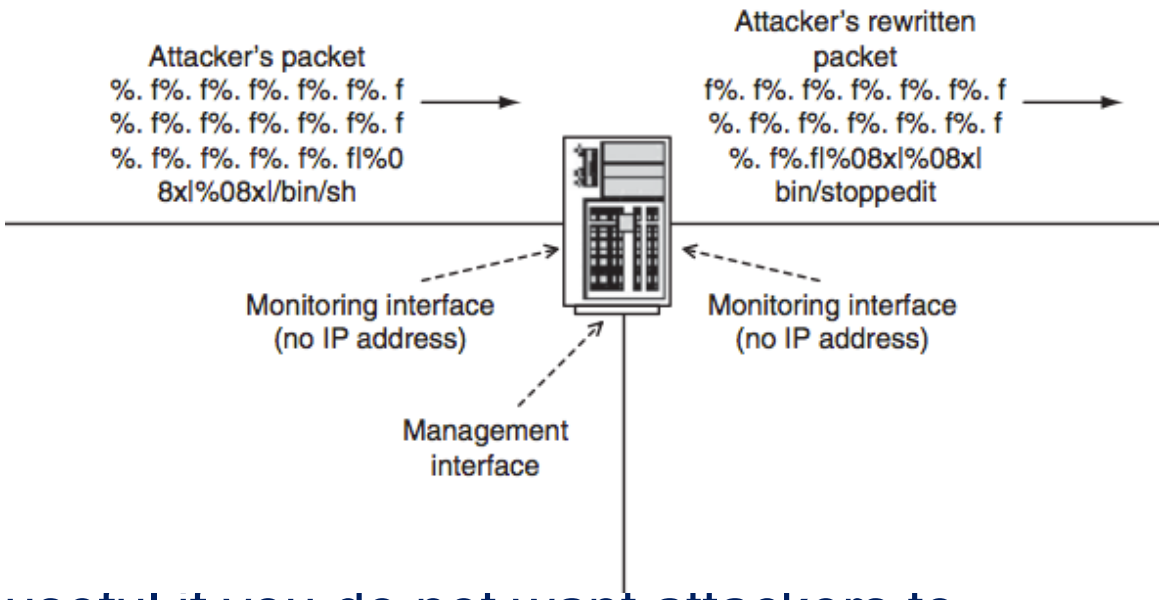
Inline NIDSs

- configured with two network interface cards:
  - management
  - detection
- work as a layer 2 bridge
  - sitting between the systems that need to be protected and the rest of the network

NIDS vs Inline NIDS



NIDS vs Inline NIDS



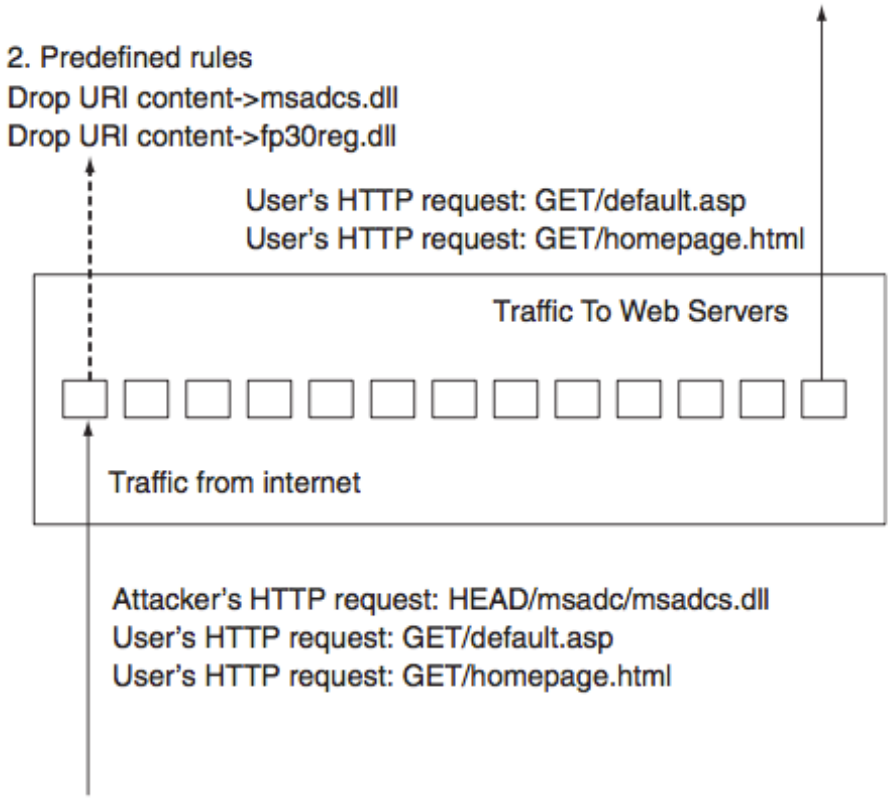
- This type of IPS is useful if you do not want attackers to know that their attacks are unsuccessful or if you want the attacker to continue to attack one of your systems in an attempt to gather more evidence, through *packet scrubbing.*
- Inline NIDS perform capabilities of a regular NIDS with the blocking capabilities of a firewall

Layer 7 Switches

- Traditional switches were layer 2 devices
- Mostly use to load balance an application across multiple servers
- high demands on networks and servers to deliver bandwidth-intensive content, layer 7 switches are on the rise
- In the case of a Web application, they can inspect the URL to direct particular requests to specific servers based on predefined rules

Layer 7 Switches

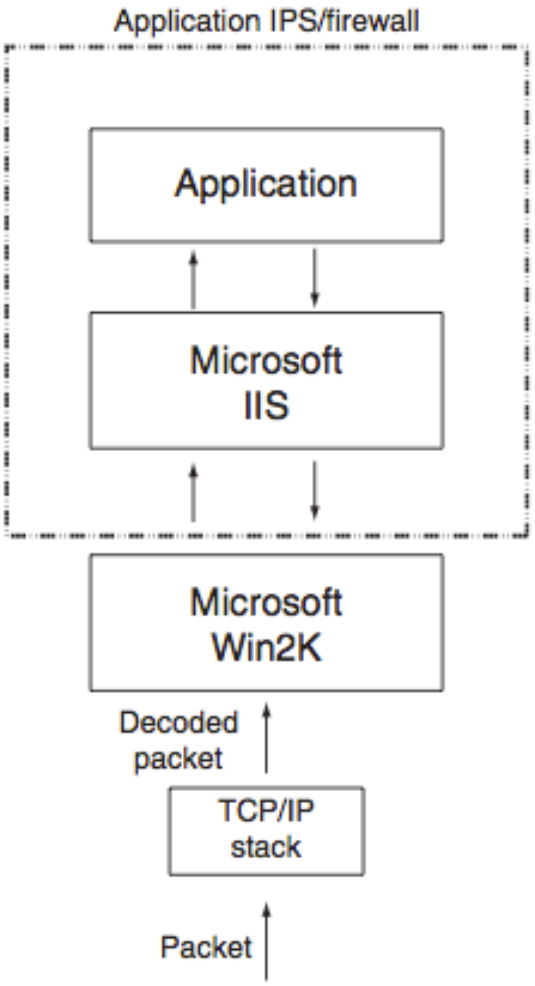
- built on custom hardware with high forwarding performance
  - handle gigabit and multi-gigabit traffic.
- Placing these devices ir front of firewalls
  - give protection for the entire network.
- Effective in stopping DoS type of attacks



Application Firewalls/IDS

- Application firewalls and IDSs are usually marketed as an intrusion prevention solution rather than a traditional IDS solution.
- loaded on each server
- customizable to each application that they protect.

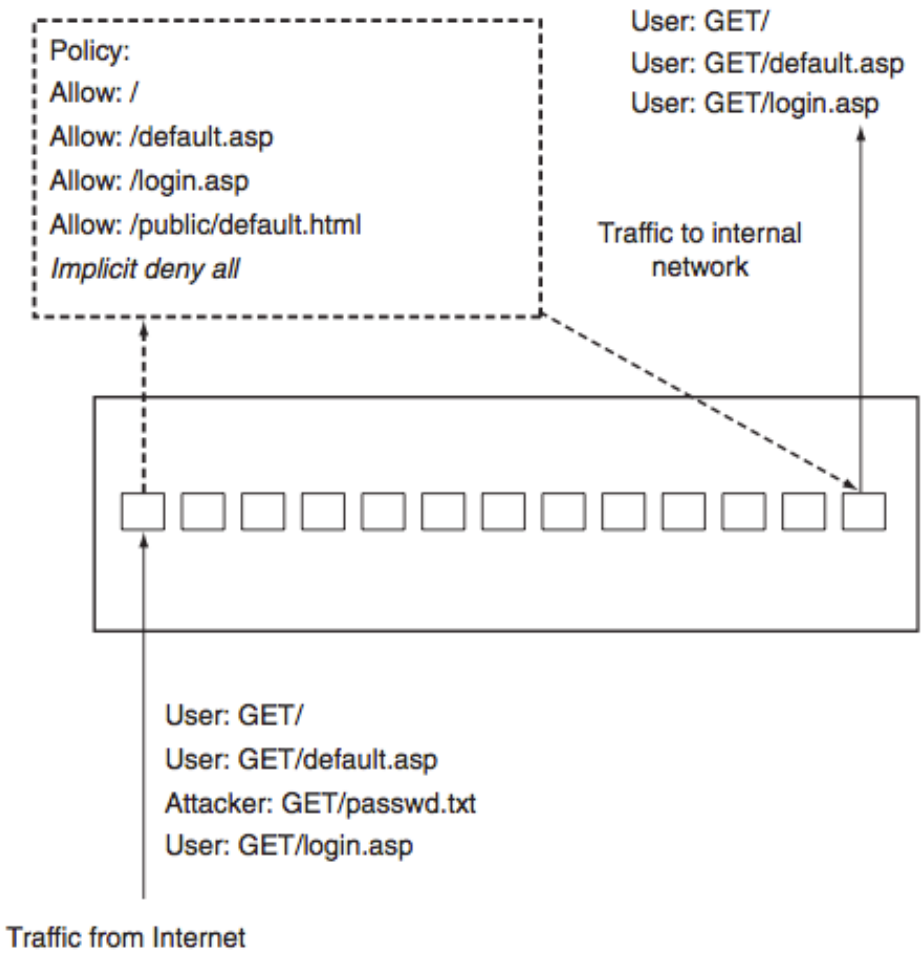
Interaction with the application



- Not look into packet-level information
- Look into API calls, memory management
  - i.e.: buffer overflow attempts
- This helps protect against poor programming and unknown attacks.
- Application IPSs can profile a system before protecting it

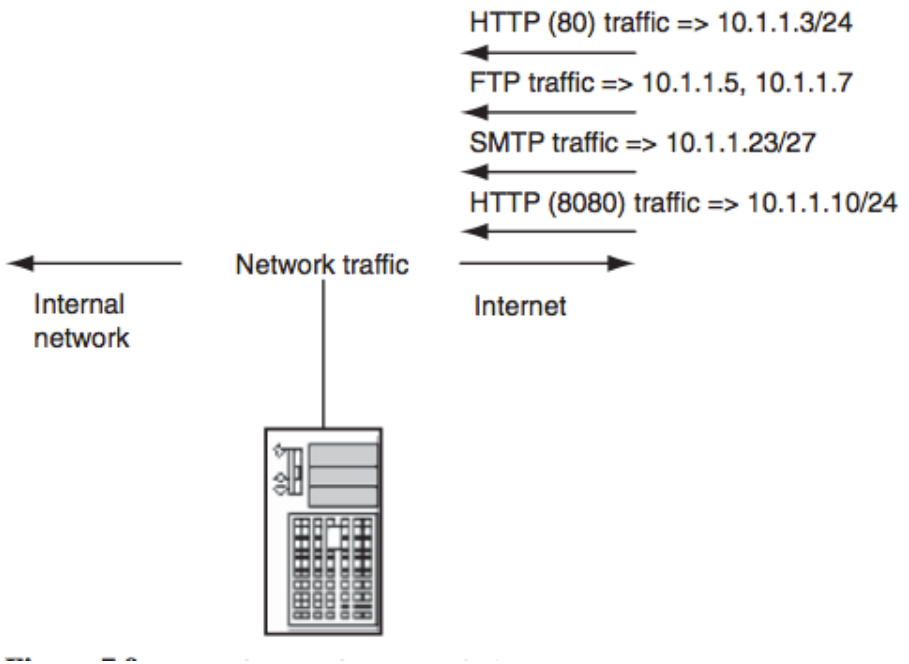
Hybrid Switches

- a cross between the host-based application firewall/ IDS and the layer 7 switch
- inspect specific traffic for malicious content defined by a configured policy



Deceptive Applications

- perform profiling function to decide which traffic is good or bad, similar to profiling phase of application firewall/ IDS
- when it sees attempts to connect to services that do not exist or at least exist on that server
  - it will send back a response to the attacker, and marked
- would catch an attacker even if he or she was to attack a legitimate Web server.



ARCHITECTURE MATTERS

- any network security device must be reliable to operate
  - IDS is passive device, easy to deploy
- High Availability
  - must withstand the toughest network environment
- High Performance
  - able to analyze every packet without any noticeable impact on traffic (high throughput and low latency)
- Manageability and Scalability
  - easy to manage and scalable in deployment

IPS ADVANTAGES

- Speedy End to Intrusions
- Accurate and Reliable Detection
- Active Prevention

What to Look For with IPS

- Accuracy and precision
  - must provide high accuracy and reliability
- Good network citizenship
  - an integral part of network
- Effective security-focused management
  - easy interface, operate as an integral part of security management suite
- Anticipates unknown attacks
  - easily accepts signatures for newly discovered attacks

Conclusion

- The main disadvantage to the IPS is there are few barometers empowering the consumer to know how much software or tools are needed to adequately protect the organization’s systems.