NETWORK SECURITY

Ch. 9: Intrusion Prevention System

PTIIK
PROGRAM TEKNOLOGI INFORMASI DAN ILMU KOMPUTER

Background

- The explosion of the Internet and e-commerce has caused organizations to become more vulnerable to electronic malice than ever before.
- With the increasing quantity and sophis- tication of attacks on information technology (IT) assets, companies have been suffering from breach of data, loss of customer confidence, and job productivity degradation, all of which eventually lead to the loss of revenue.

Defense - Firewall

- The first step that virtually all organizations connected to the Internet take is to install a firewall
- A firewall acts as a perimeter guard for a network, determining what traffic to allow or deny in and out
- Most firewall allow SMTP, FTP, HTTP, DNS.
  - A policy, “accept” and “deny”, based on various criteria, (such as a source, destination, and protocol in question)

Defense – Firewall (Cont.)

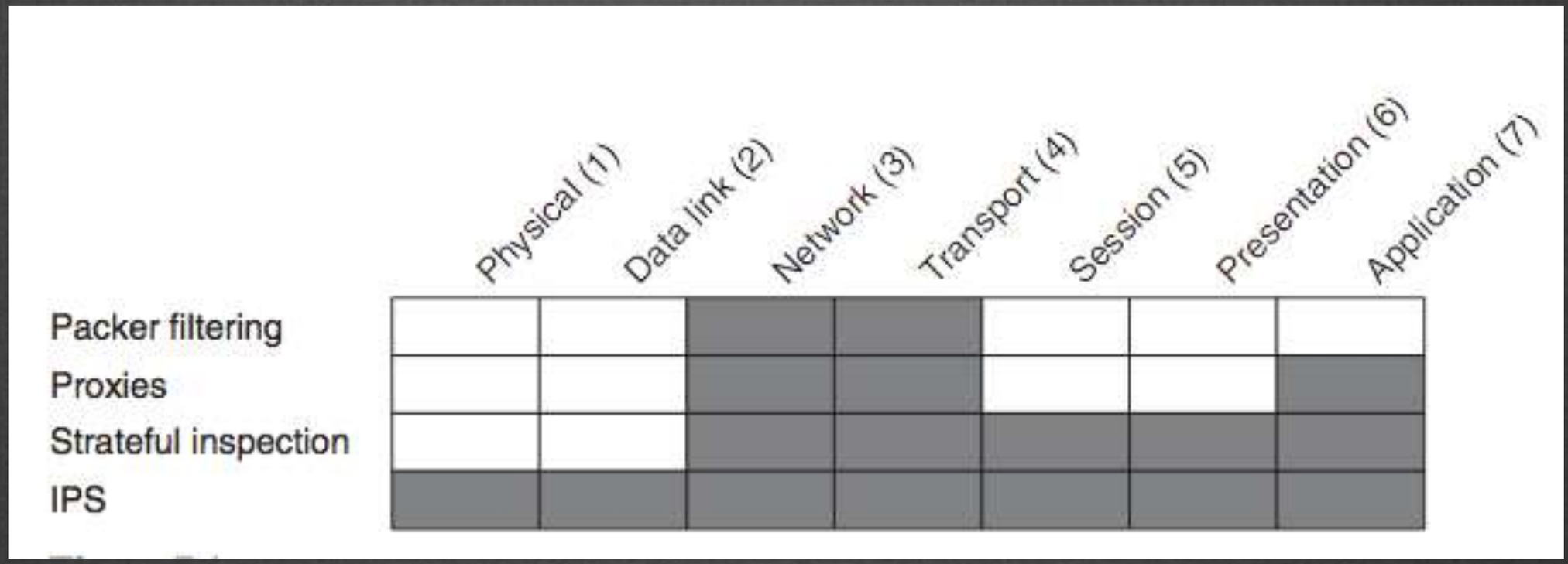
- firewall primary purpose is to protect a private network (usually internal) from a public network (usually the Internet) by checking all data passing between these net- works and preventing unwanted conversations from occurring.

- But is a firewall enough to secure your network?

Defense – Firewall (Cont.)

- Firewalls control what goes in and out of your network, but they cannot look at the content of that traffic.
- As a result, they can do nothing to protect your corporation from attacks contained within the traffic that they allow into your network.

Network Layers and Protection Techniques



- Many enterprises are realizing that people within the corporation often make intrusion attempts

Network Layers and Protection Techniques

- And there are certain situations where, through social engineering or some form of Trojan horse or back door, an attack will actually “show up” as originating from inside the corporate network and spread from within
  - Is a firewall enough to secure your network?” is a resolute “NO”.

The Good News

- There are products available today designed to detect and protect against attacks from traffic in your network, called NIDS
- The bad news is that the perceived value of NIDSs is low because:
  - Overreliance on Firewall.
  - False Alarms.
  - Low Manageability, High Maintenance.
  - Perceived Need to Outsource
  - No Prevention of Attacks

The Good News (Cont.)

- we've ever discussed IDS, so let’s 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 utilize IDS algorithms to monitor and drop or allow traffic based on expert analysis.
- These devices 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,
- This fourth generation is a sign that network security is homogenizing and the IPS of tomorrow will account for multiple dimensions of threat from the convergence of data systems such as virtual private network (VPN) and wireless communication

Detection VS Prevention

- On the surface, IDS and IPS appear competitive.
- They share a long list of similar functions, like packet inspection, stateful analysis, fragment reassembly, Transmission Control Protocol (TCP) segment reassembly, deep- packet inspection, protocol validation, and signature matching
- But these capabilities take a backseat to the starkly different purposes for which they are deployed

Detection VS Prevention (Cont.)

- An IPS operates like a security guard at the gate of a private community, allowing and denying access based on credentials and some predefined rule set, or policy
- An IDS works like a patrol car within the community, monitoring activities and looking for abnormal situations.
  - The purpose of intrusion detection is to provide monitoring, auditing, forensics, and reporting of network activity
  - It operates on the packets that are allowed through an access control device.
  - on the other hand, are loaded with intelligence, using many different techniques to identify potential attacks, intrusions, exploits, and abuses.

Detection VS Prevention (Cont.)

- That positions the IDS well to identify:
  - Known attacks via signatures and rules
  - Variations in traffic volume and direction using complex rules and statistical analysis
  - Communication traffic pattern variations using flow analysis
  - Anomalistic activity detection using baseline deviation analysis
  - Suspicious activity detection using heuristics, flow analysis, statistical techniques, and anomaly detection

Detection VS Prevention (Cont.)

- 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.

New Solution

- Intrusion prevention solutions are intended to provide protection for assets, resources, data, and networks.
- The primary expectation is that they will reduce the threat of attack by eliminating the harmful and/or malicious network traffic while continuing to allow legitimate activity to continue
- 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.

New Solution (Cont.)

- Intrusion prevention solutions are intended to provide protection for assets, resources, data, and networks.
- The primary expectation is that they will reduce the threat of attack by eliminating the harmful and/or malicious network traffic while continuing to allow legitimate activity to continue
- 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.

New Solution (Cont.)

- Intrusion prevention solutions are ideally positioned to deal with:
  - UndesiredapplicationsandactiveTrojanhorseattacksagainstprivatenetworksand applications by using deterministic rules and access control lists
  - Attack packets like those from LAND and WinNuke by using high-speed packet filters
  - Protocol abuse and evasive actions—network protocol manipulations like Fragroute and TCP overlap exploits—by using intelligent reassembly
  - Denial-of-service [DoS, distributed Dos (DDoS)] attacks such as SYN and Internet Control Message Protocol (ICMP) floods by using threshold-based filtering algorithms
  - Application abuse and protocol manipulations—known and unknown attacks against HTTP, FTP, DNS, SMTP, and so on—by using application protocol rules and signatures
  - Application overload or abuse attacks by using threshold-based resource
  - Consumption limits.

The 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.

- So what exactly is an IPS?

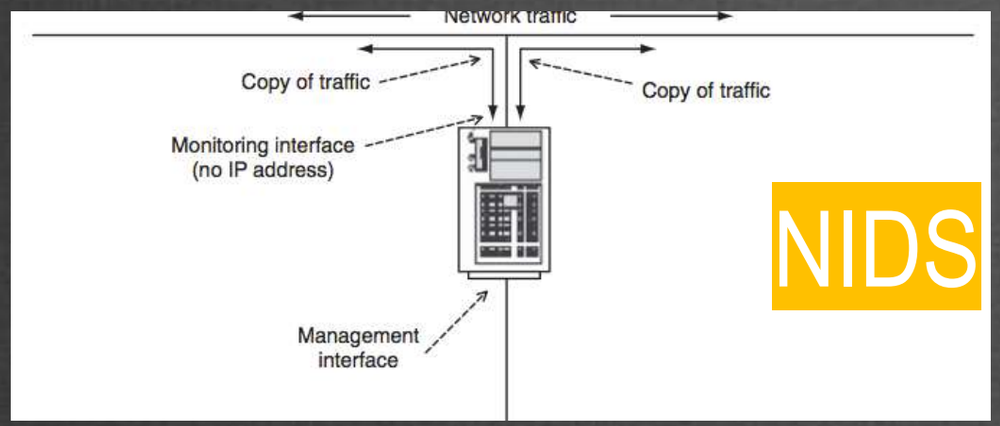
The five types of IPSs

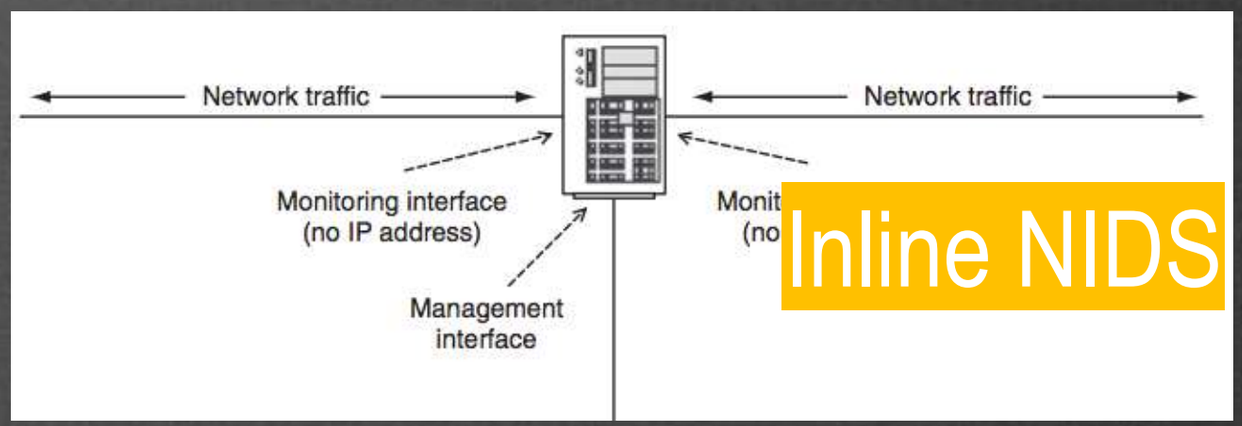
- Inline NIDS,
- Application- based firewalls/IDSs,
- Layer 7 switches,
- Network-based application IDSs, and
- Deceptive applications.

Inline NIDSs

- Most NIDSs would be configured with two network Interface cards (NICs), one for management and one for detection
- The inline NIDS works like a layer 2 bridge, sitting between the systems that need to be protected and the rest of the network

NIDS vs Inline NIDS

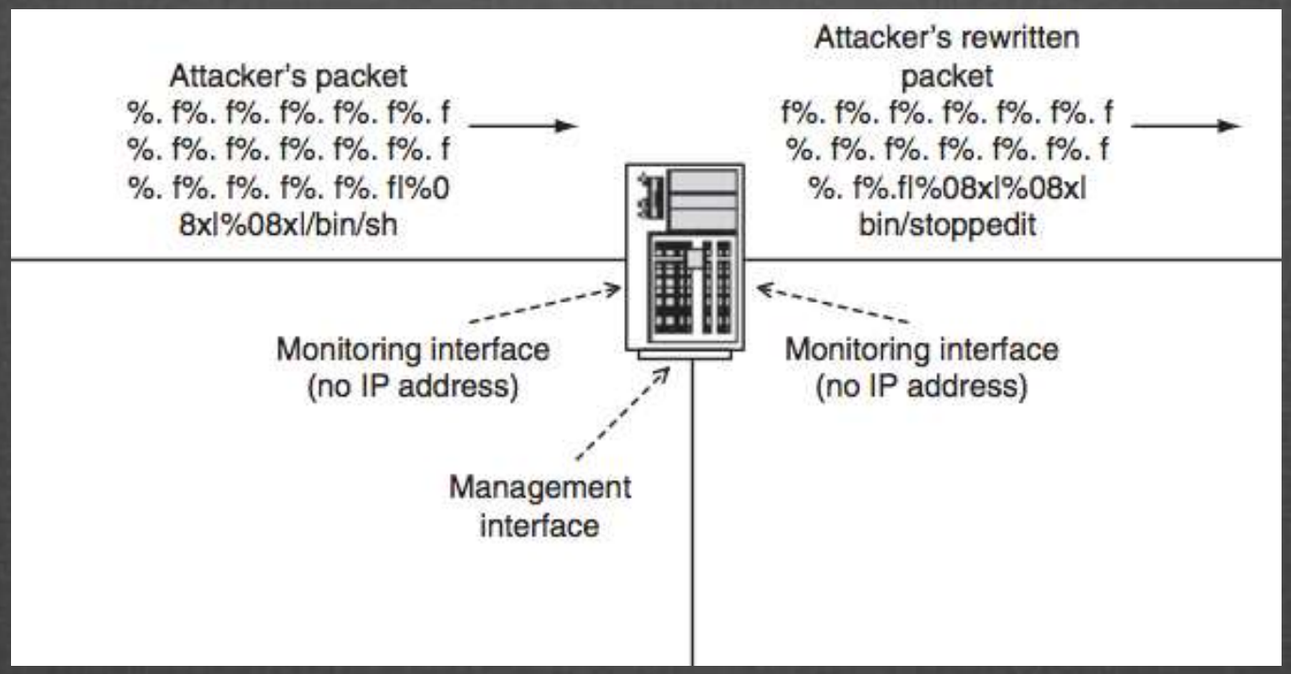




All traffic will pass through the inline NIDS

If a packet contains a piece of information that trips a signature, the packet can be forwarded or dropped and either logged or unlogged

Packet Scrubbing

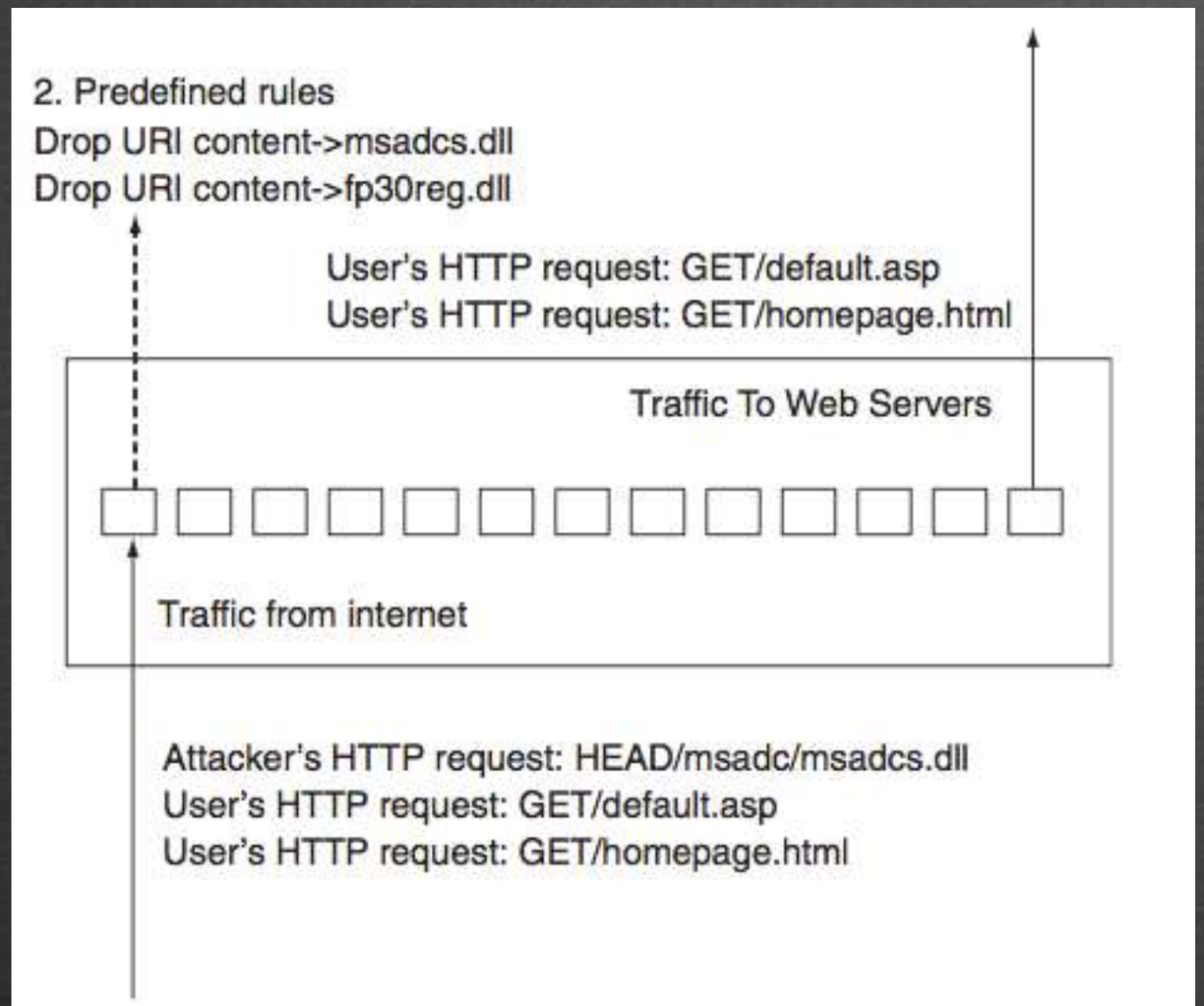


- This type of IPS is useful if you do not want attackers to know that their attacks are unsuccessful or if you want the attacker to continue to attack one of your systems in an attempt to gather more evidence.
- An inline NIDS offers the great capabilities of a regular NIDS with the blocking capabilities of a firewall

Layer 7 Switches

- Traditionally switches were layer 2 devices
- Network engineers mostly use these switches to load balance an application across multiple servers
- with the 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 Capabilities.

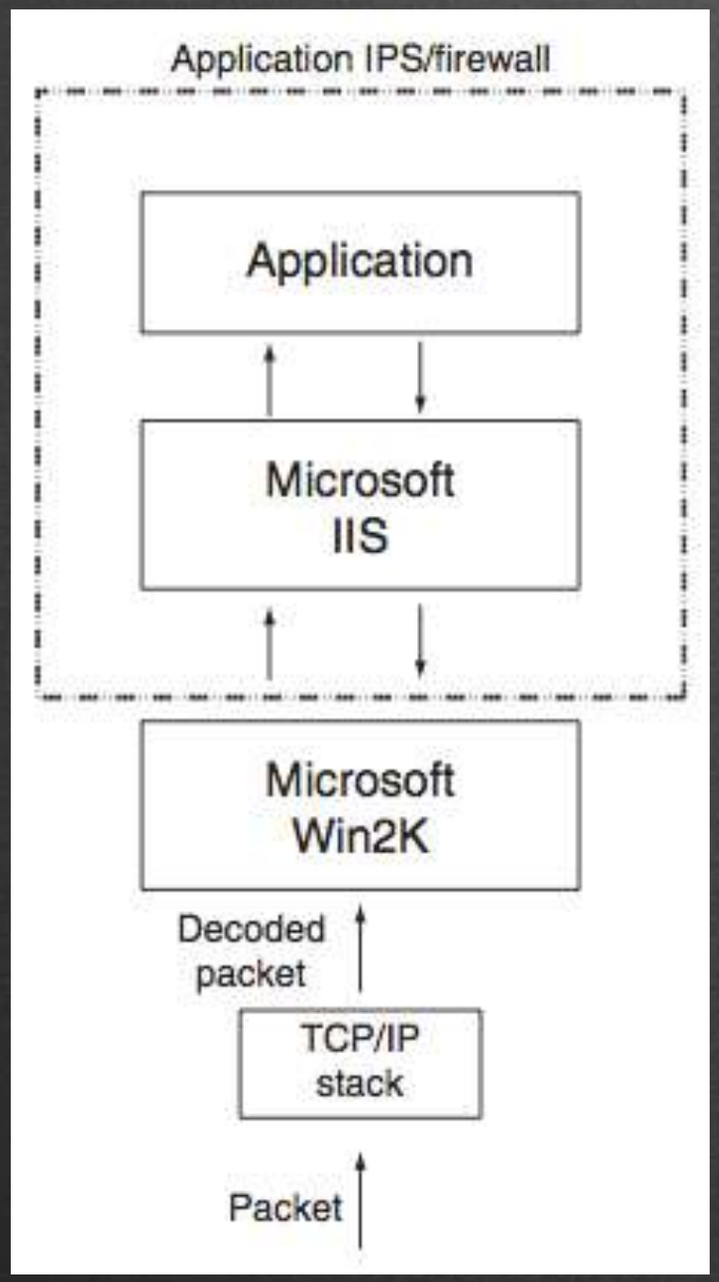


- These devices are built on custom hardware to deliver high performance, even in the most demanding networks
- an easily handle gigabit and multigigabit traffic.
- Placing these devices in front of your firewalls would give protection for the entire network.
- the drawbacks are similar to the inline NIDS

Application Firewalls/IDSs

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

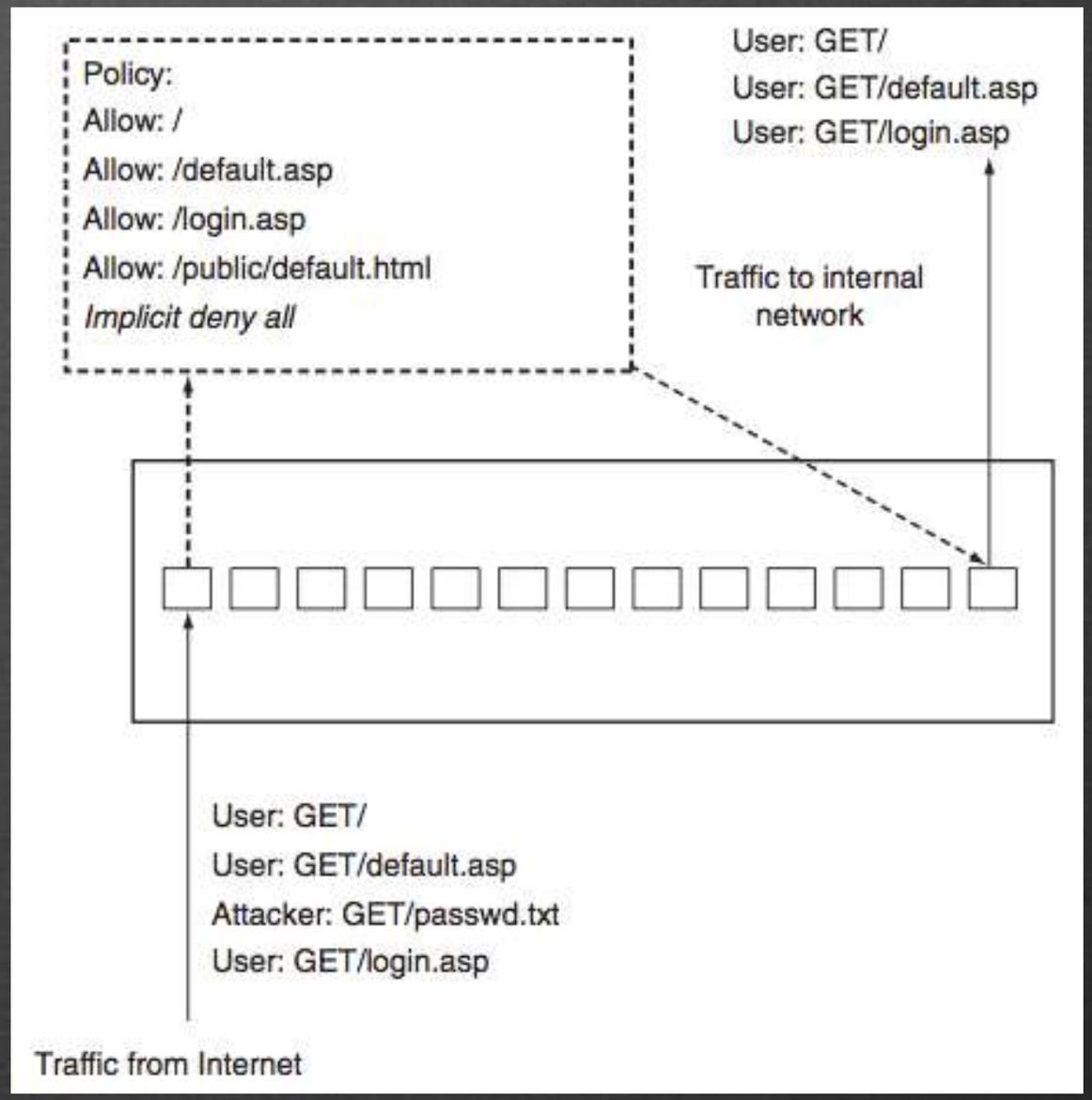
Interaction with the Application



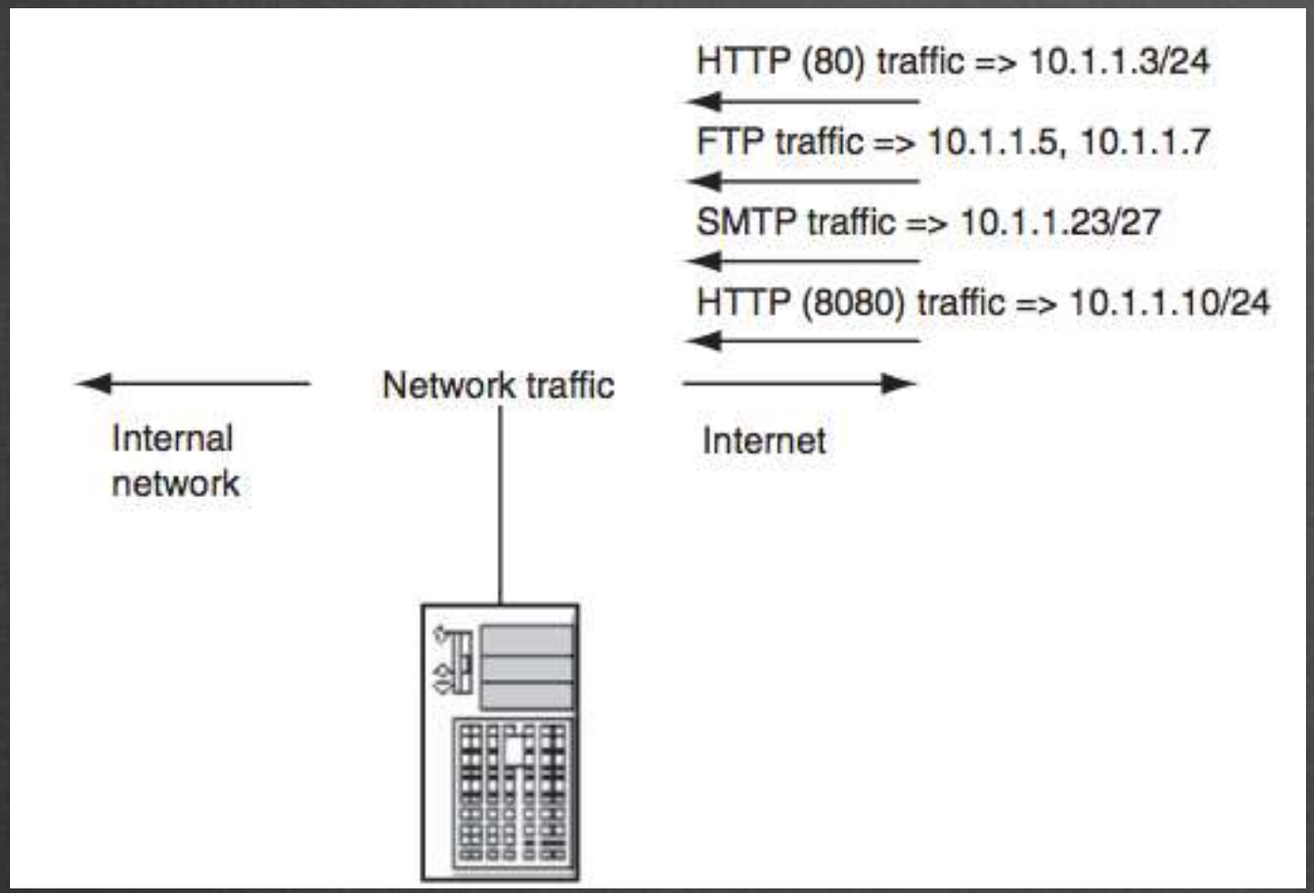
- They do not look at packet-level information; rather, they look at API calls, memory management (i.e., buffer overflow attempts), how the application interacts with the operating system, and how the user is suppose to interact with the application
- This helps protect against poor programming and unknown attacks.
- Application IPSs can profile a system before protecting it

Hybrid Switches

- This type of technology is a cross between the host-based application firewall/IDS and the layer 7 switch
- This type of technology is a cross between the host-based application firewall/IDS and the layer 7 switch
- They inspect specific traffic for malicious content defined by the policy that is configured



Deceptive Applications



This would catch an attacker even if they were to attack a legitimate Web server.

- It watches all your network traffic and figures out what is good traffic, similar to the profiling phase of the application fire- wall/IDS
- Then, 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

Architecture Matters

- There is a more basic difference between IDSs and IPSs architecture.
- the success of the IDS has been possible because it was passive
- any network security device that is going to operate inline must be reliable.
  - Reliability is driven by constant operations and suitability to task
- an IPS solution must consistently block traffic that is malicious or inappropriate while allowing all appropriate traffic to pass by unfettered

Architecture Matters (Cont.)

- IPS solution must have the following qualities:
  - High Availability
  - High Performance
  - Manageability and Scalability.

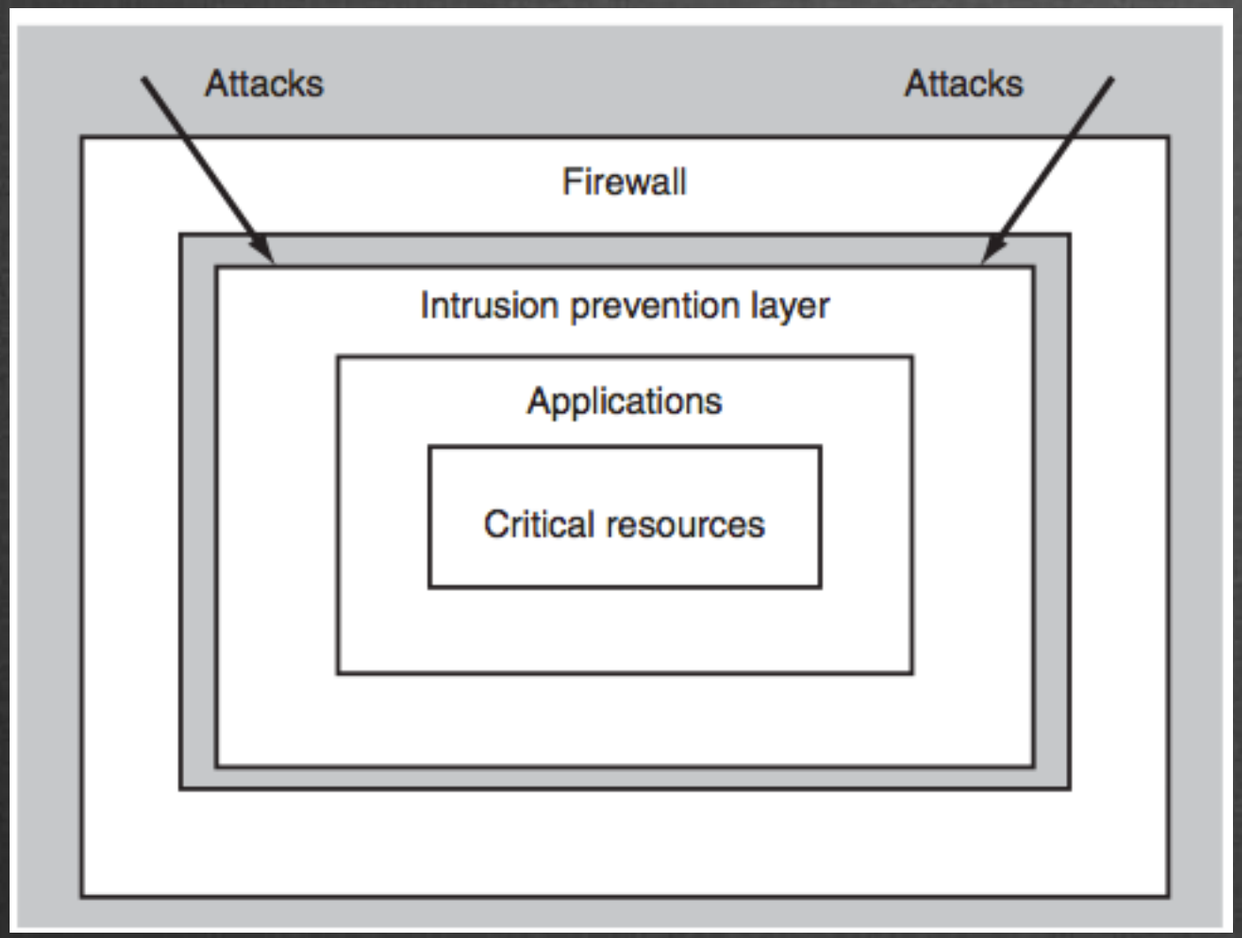
IPS Advantages

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

IPS Requirements: What to Look For

- The term intrusion prevention system is being used indiscriminately to describe a variety of security technologies and solutions
- It is recommended that organizations look for network IPSs that have the following characteristics:
  - An inline device capable of accurately and reliably detecting and precisely blocking attacks accuracy and precision.
  - Operates at line speed with no negative impact to network performance or availability good network citizenship.
  - Integrates effectively into security management environment. Effective security focused management.
  - Needs to easily accommodate prevention for future attacks. Anticipates unknown attacks and easily accepts signatures for newly discovered attacks.

Placement of Intrusion Prevention Layer



- New layer of protection in the network security infrastructure, blocking the attacks and intrusions that pass through the firewall.
  - ✓ Accuracy and precision
  - ✓ Good network citizenship
  - ✓ Effective security-focused management
  - ✓ Anticipates unknown attacks and 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.