



# Network Security: Firewall, VPN, IDS/IPS, SIEM

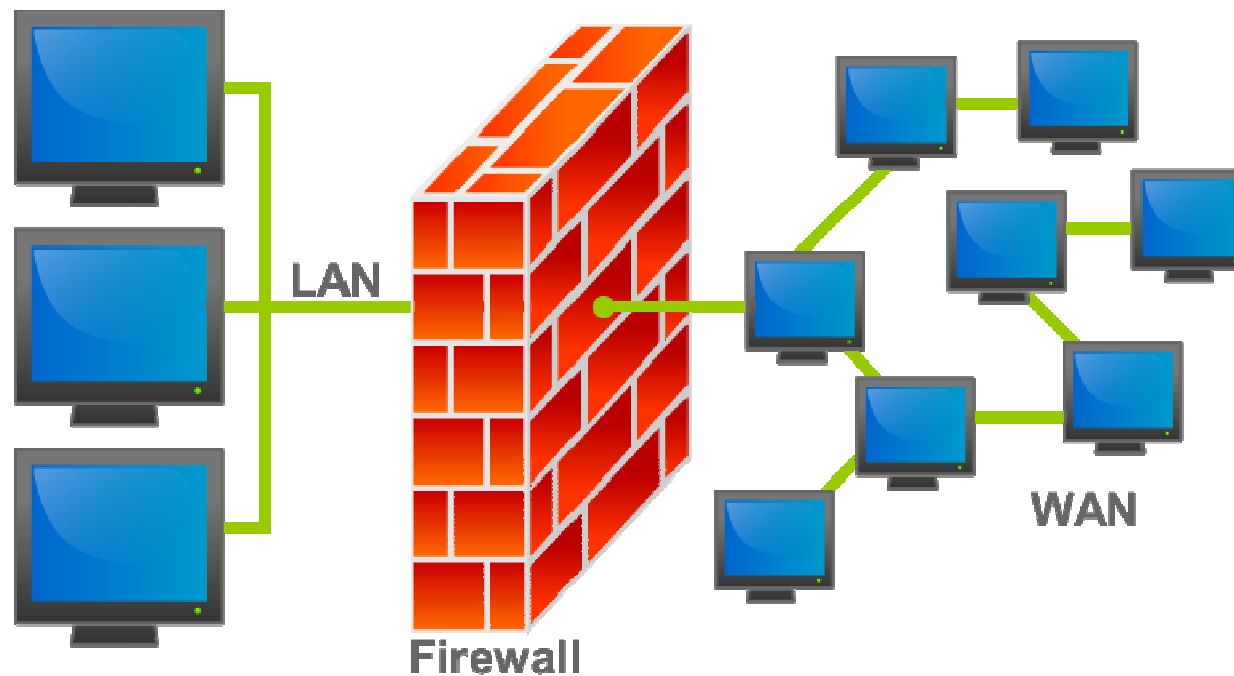
Ahmet Burak Can

Hacettepe University

abc@hacettepe.edu.tr

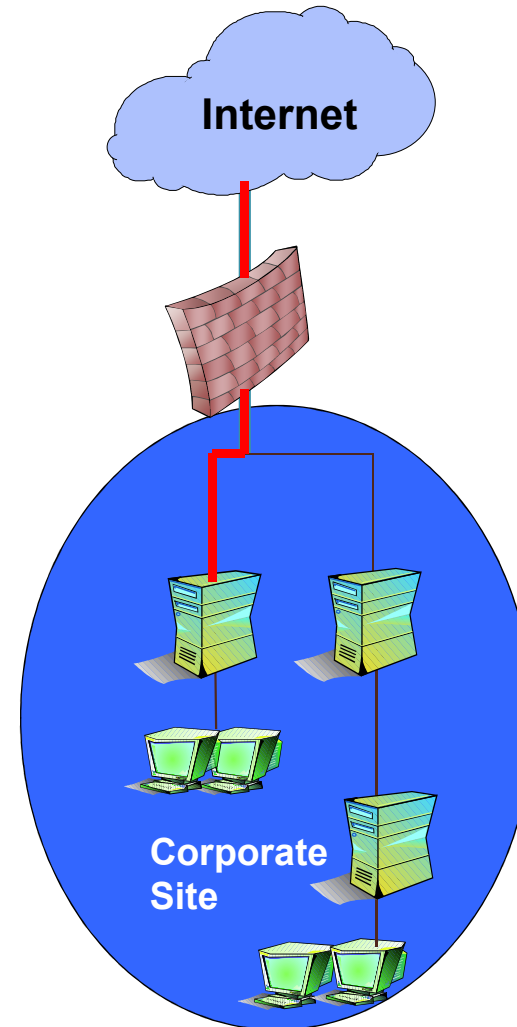
# What is a Firewall?

- A firewall is hardware, software, or a combination of both that is used to prevent unauthorized programs or Internet users from accessing a private network and/or a single computer



# What is a Firewall ?

- A firewall :
  - Acts as a security gateway between two networks
  - Tracks and controls network communications
    - Decides whether to pass, reject, encrypt, or log communications (Access Control)

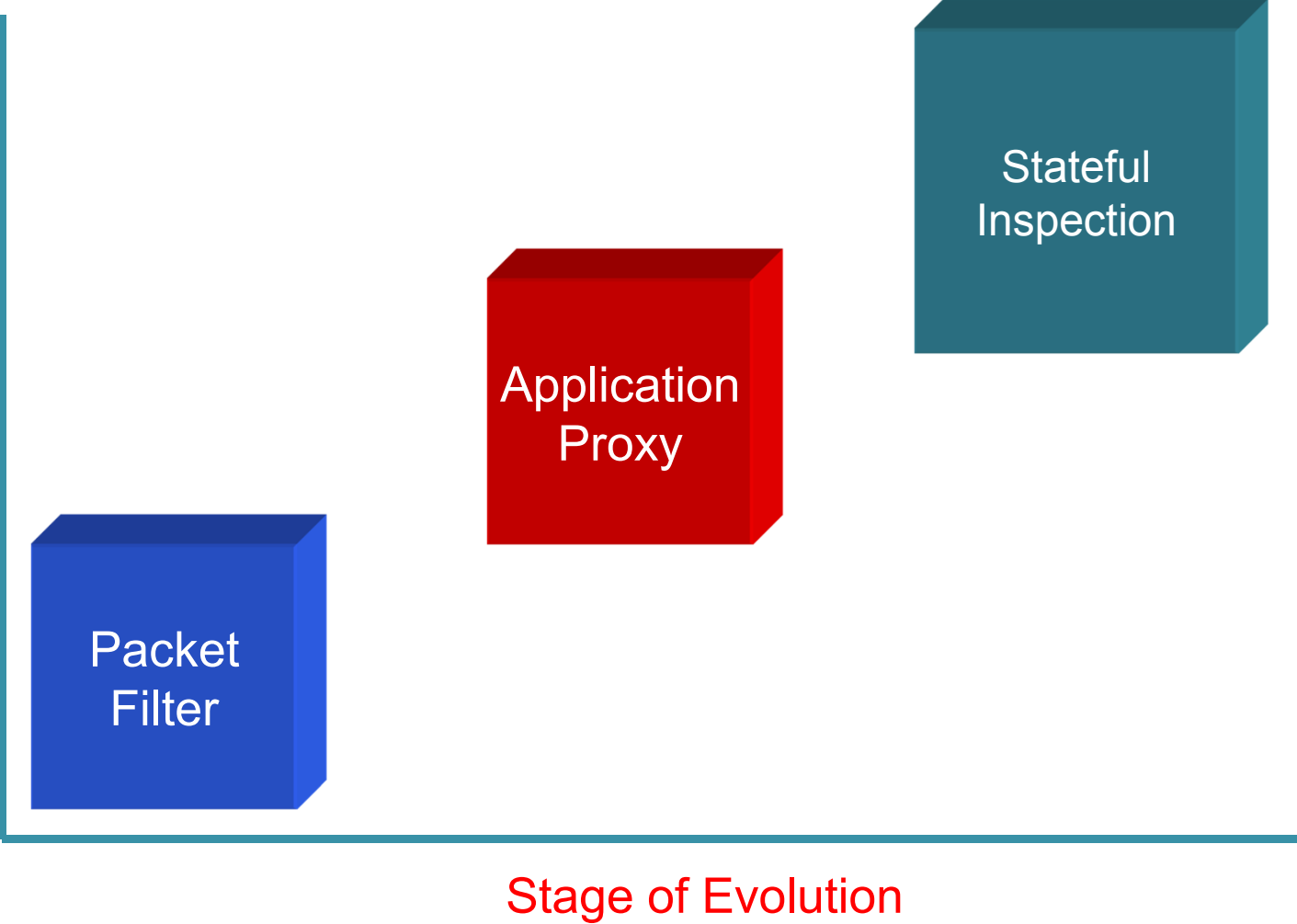




# Hardware vs. Software Firewalls

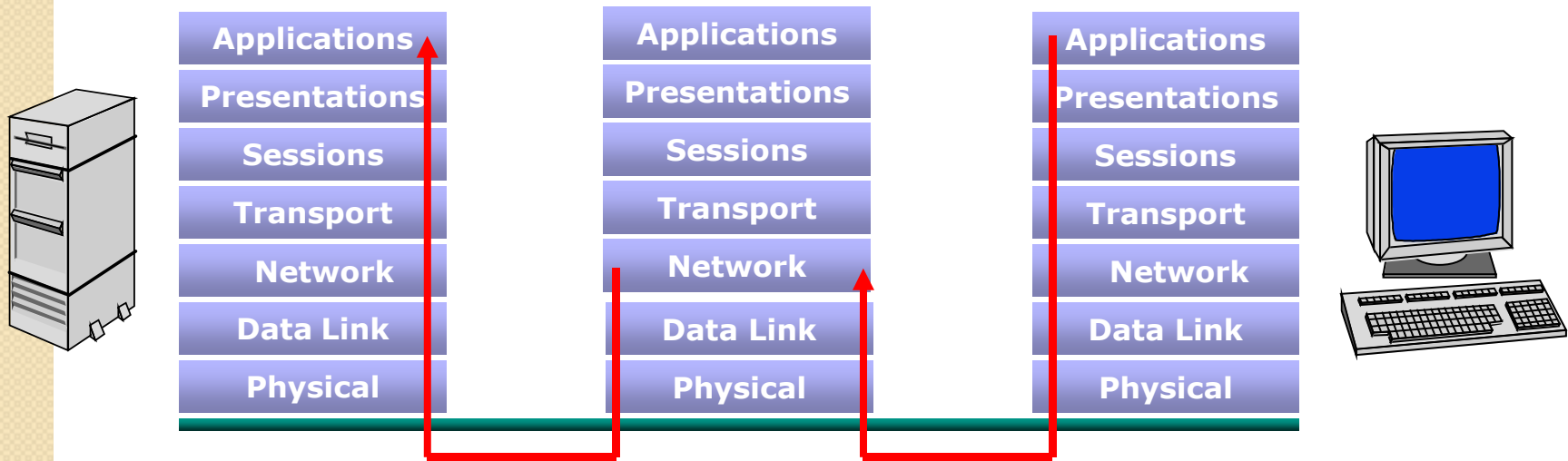
- **Hardware Firewalls**
  - Protect an entire network
  - Implemented on the router level
  - Usually more expensive, harder to configure
- **Software Firewalls**
  - Protect a single computer
  - Usually less expensive, easier to configure

# Evolution of Firewalls



# Packet Filter

- Packets examined at the network layer
- Useful “first line” of defense - commonly deployed on routers
- Simple accept or reject decision model
- No awareness of higher protocol layers





# Packet Filter

- Simplest of components
- Uses transport-layer information only
  - IP Source Address, Destination Address
  - Protocol/Next Header (TCP, UDP, ICMP, etc)
  - TCP or UDP source & destination ports
  - TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
  - ICMP message type
- Examples
  - DNS uses port 53
    - No incoming port 53 packets except known trusted servers



# How to Configure a Packet Filter

- Start with a security policy
- Specify allowable packets in terms of logical expressions on packet fields
- Rewrite expressions in syntax supported by your vendor
- General rules - least privilege
  - All that is not expressly permitted is prohibited
  - If you do not need it, eliminate it



# Packet Filter Configuration - I

Every ruleset is followed by an implicit rule reading like this.

action	src	port	dest	port	flags	comment
block	*	*	*	*	*	default

Suppose we want to allow inbound mail (SMTP, port 25) but only to our gateway machine. Also suppose that mail from some particular site SPIGOT is to be blocked.

## Packet Filter Configuration - 2

action	src	port	dest	port	flags	comment
block	SPIGOT	*	*	*	*	We don't trust these site
allow	*	*	OUR-GW	25	*	Connection to our SMTP port

### Example 2:

Now suppose that we want to implement the policy “any inside host can send mail to the outside”.

## Packet Filter Configuration - 3

action	src	port	dest	port	flags	comment
allow	*	*	*	25	*	Connection to outside SMTP port

- This solution allows calls from any port on an inside machine, and will direct them to port 25 on an outside machine.
- So why is it wrong?



## Packet Filter Configuration - 4

- Our defined restriction is based solely on the destination's port number.
- With this rule, an enemy can access any internal machines on port 25 from an outside machine.
- What can be a better solution ?

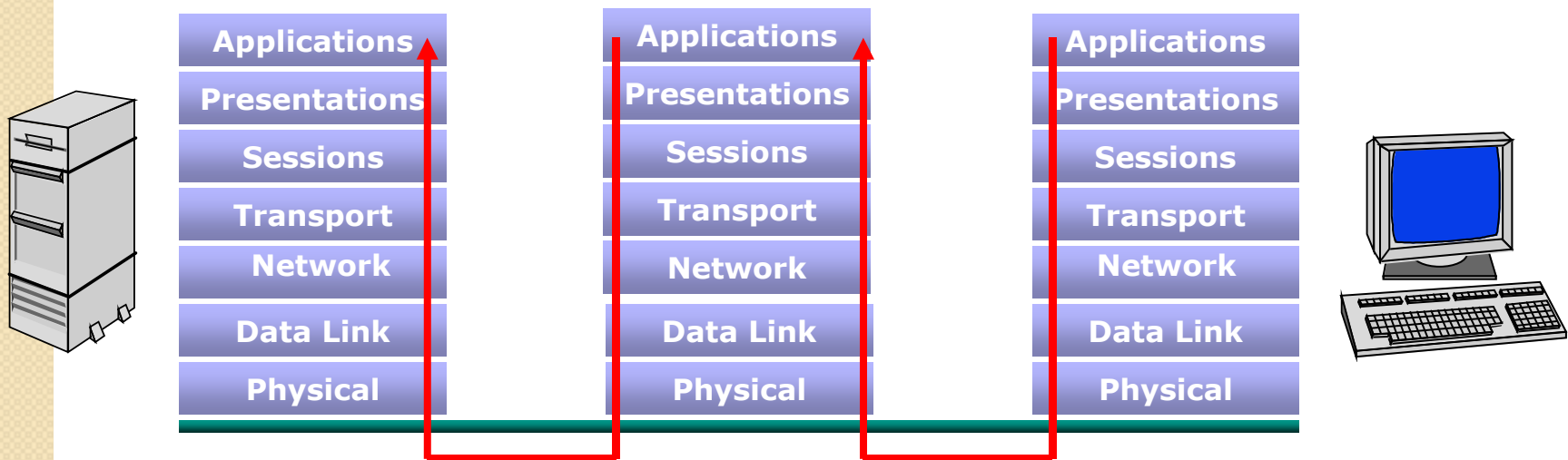
## Packet Filter Configuration - 5

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25	*	Connection to outside SMTP port
allow	*	25	*	*	ACK	SMTP replies

- The first rule restricts that only inside machines can access to outside machines on port 25.
- In second rule, the **ACK** signifies that the packet is part of an ongoing conversation.
  - Packets without **ACK** are connection establishment messages, which are only permitted from internal hosts by the first rule.
  - With the second rule, outside hosts can send back packets to inside hosts on port 25.

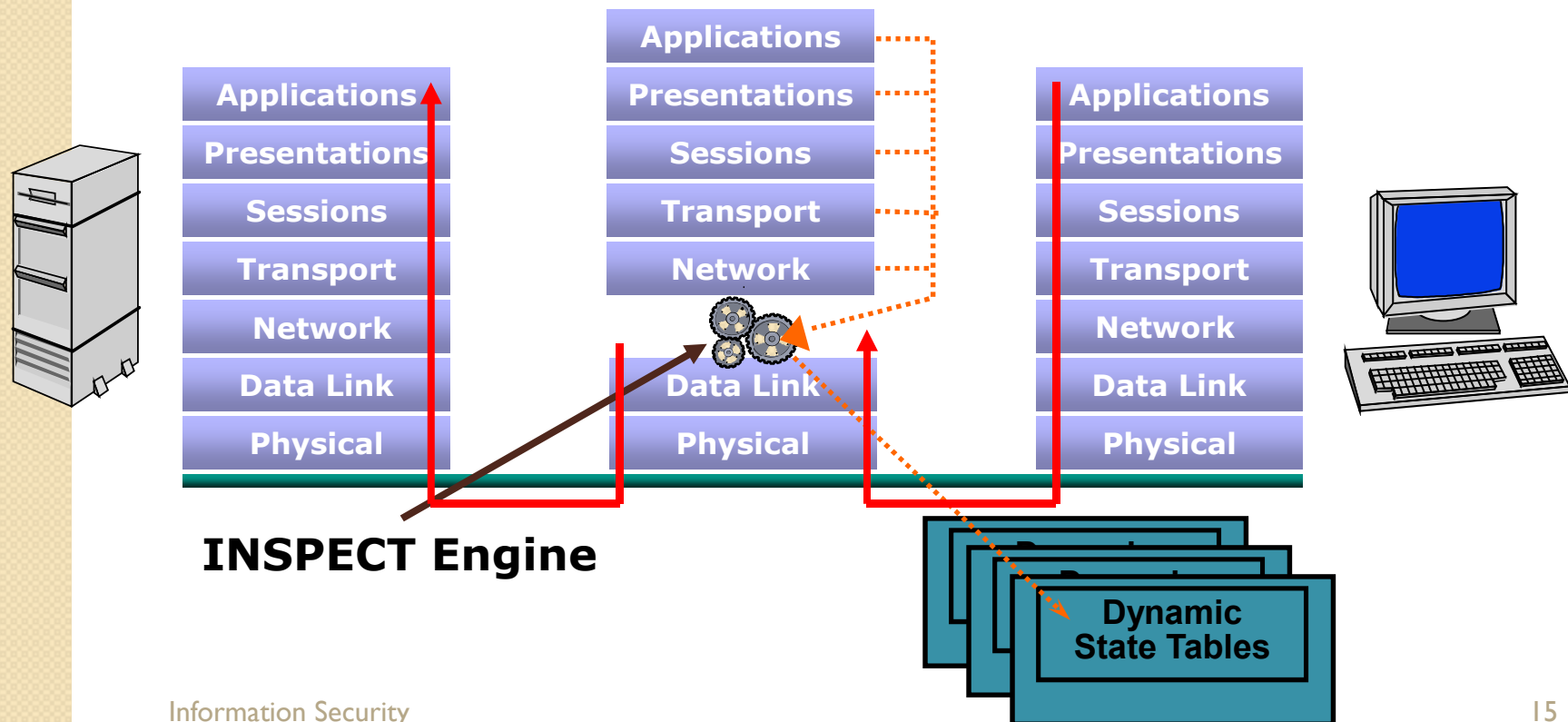
# Application Gateway or Proxy

- Packets examined at the application layer
- Application/Content filtering possible - prevent FTP “put” commands, for example
- Modest performance
- Scalability limited

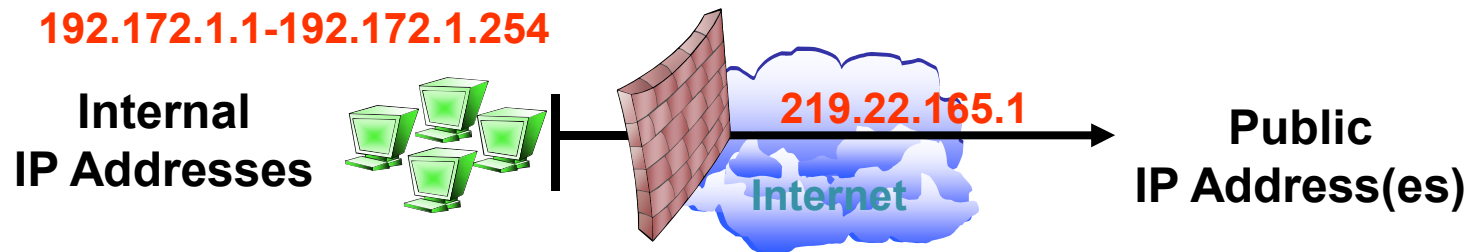


# Stateful Inspection

- Packets Inspected between data link layer and network layer in the OS kernel
- State tables are created to maintain connection context
- Invented by Check Point



# Network Address Translation (NAT)

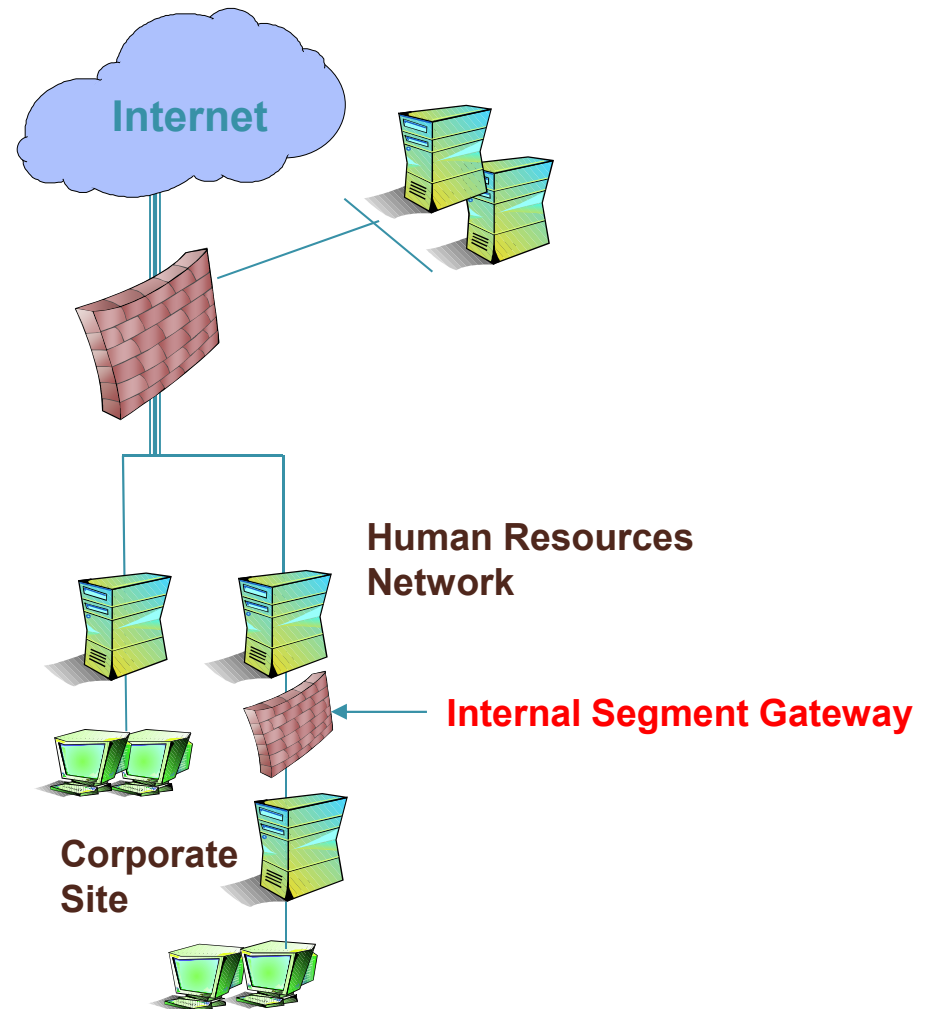


- Converts a network's illegal IP addresses to legal or public IP addresses
  - Hides the true addresses of individual hosts, protecting them from attack
  - Allows more devices to be connected to the network



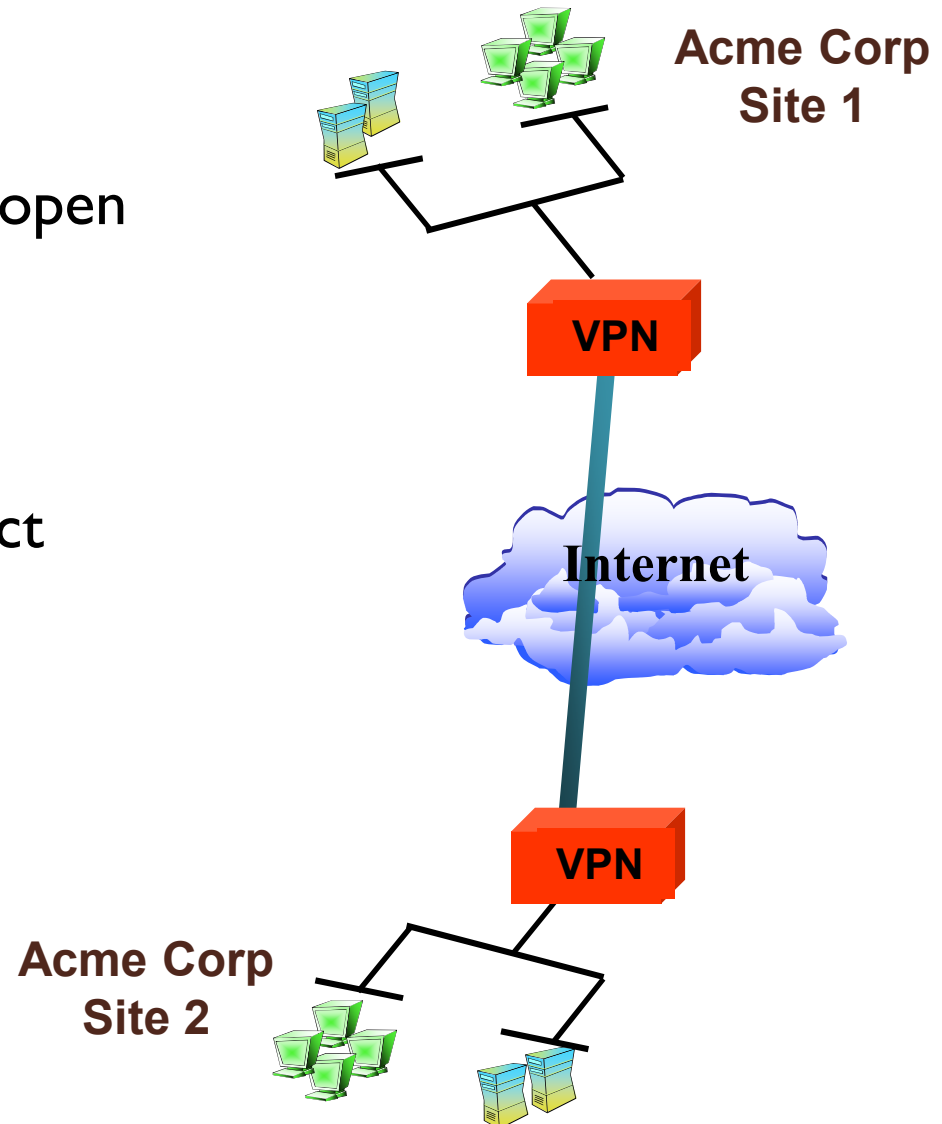
# Firewall Deployment

- Corporate Network Gateway
- Internal Segment Gateway
  - Protect sensitive segments (Finance, HR, Product Development)
  - Provide second layer of defense
  - Ensure protection against internal attacks and misuse



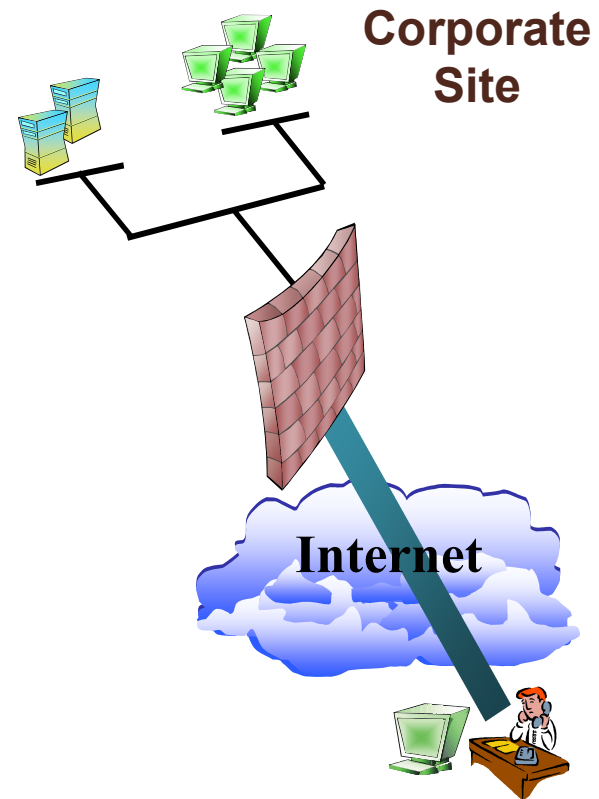
# What is a VPN?

- A VPN is a private connection over an open network
- A VPN includes authentication and encryption to protect data integrity and confidentiality



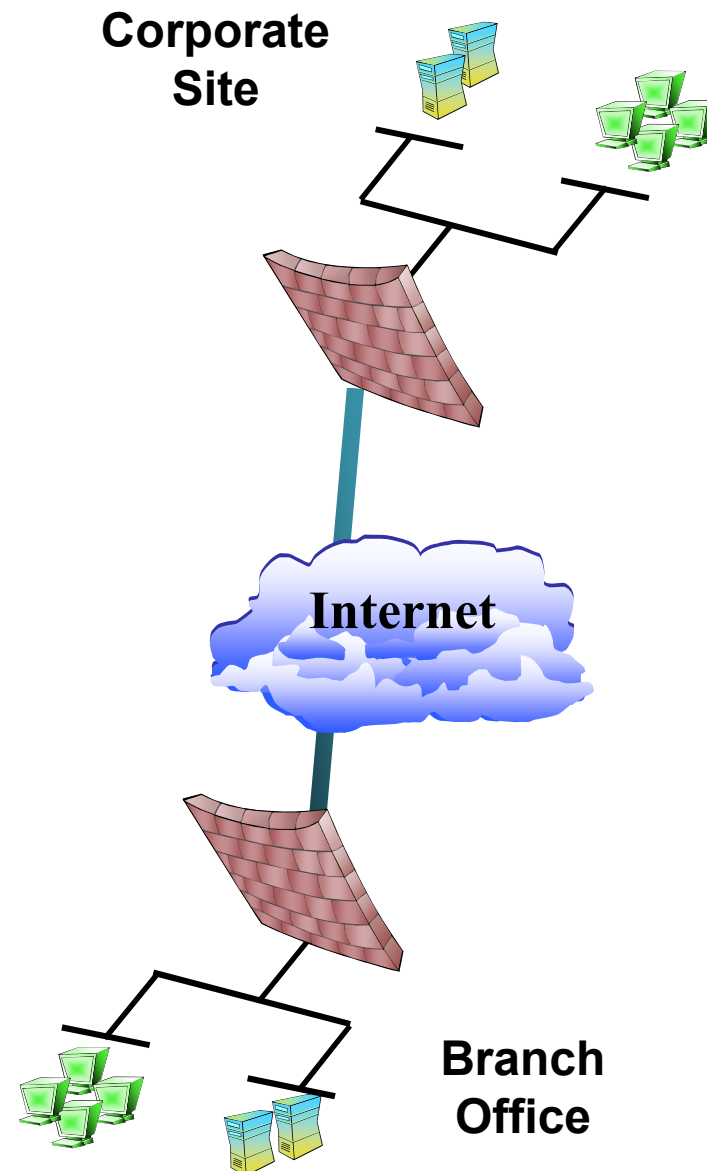
# Types of VPNs

- Remote Access VPN
  - Provides access to internal corporate network over the Internet
  - Reduces long distance, modem bank, and technical support costs
  - PAP,CHAP,RADIUS



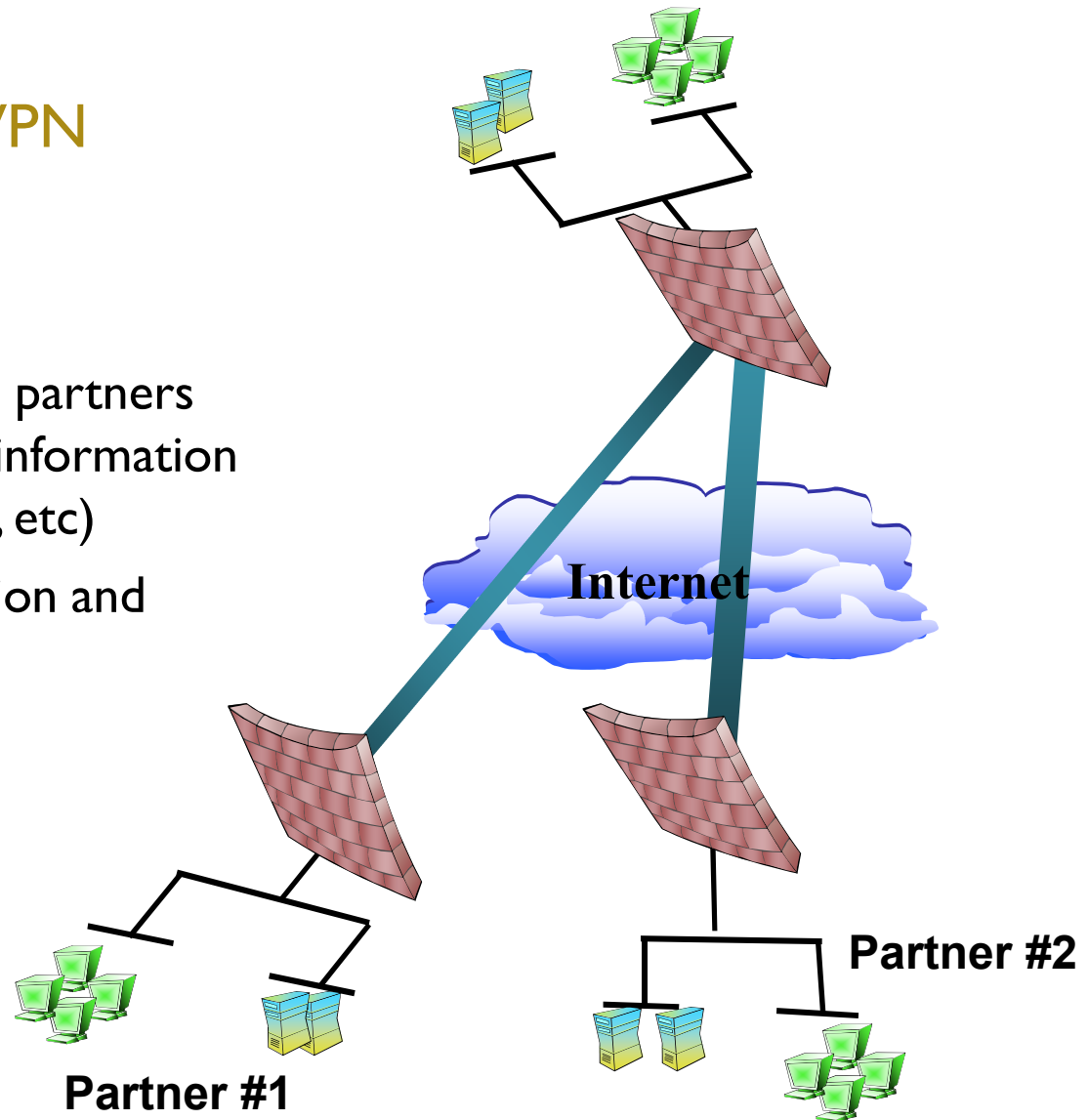
# Types of VPNs

- Remote Access VPN
- Site-to-Site VPN
  - Connects multiple offices over Internet
  - Reduces dependencies on frame relay and leased lines



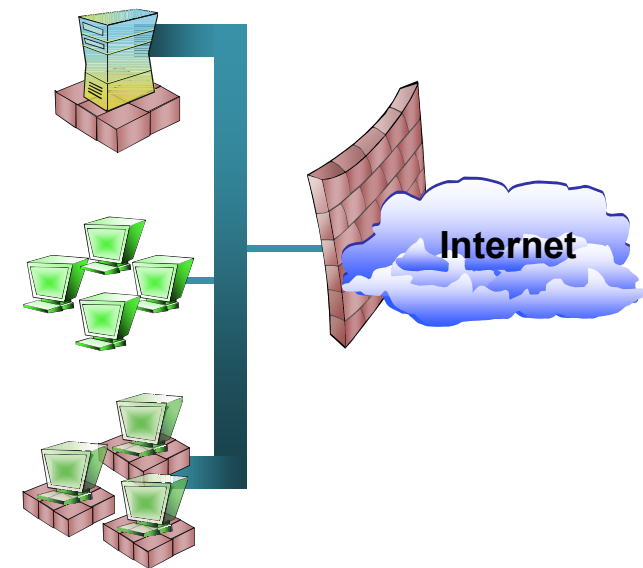
# Types of VPNs

- Remote Access VPN
- Site-to-Site VPN
- Extranet VPN
  - Provides business partners access to critical information (leads, sales tools, etc)
  - Reduces transaction and operational costs



# Types of VPNs

- Remote Access VPN
- Site-to-Site VPN
- Extranet VPN
- Client/Server VPN
  - Protects sensitive internal communications



*LAN clients with sensitive data*



# Overview of IDS/IPS

- **Intrusion**
  - A set of actions aimed at compromising the security goals (confidentiality, integrity, availability of a computing/networking resource)
- **Intrusion detection**
  - The process of identifying and responding to intrusion activities
- **Intrusion prevention**
  - The process of both detecting intrusion activities and managing responsive actions throughout the network.

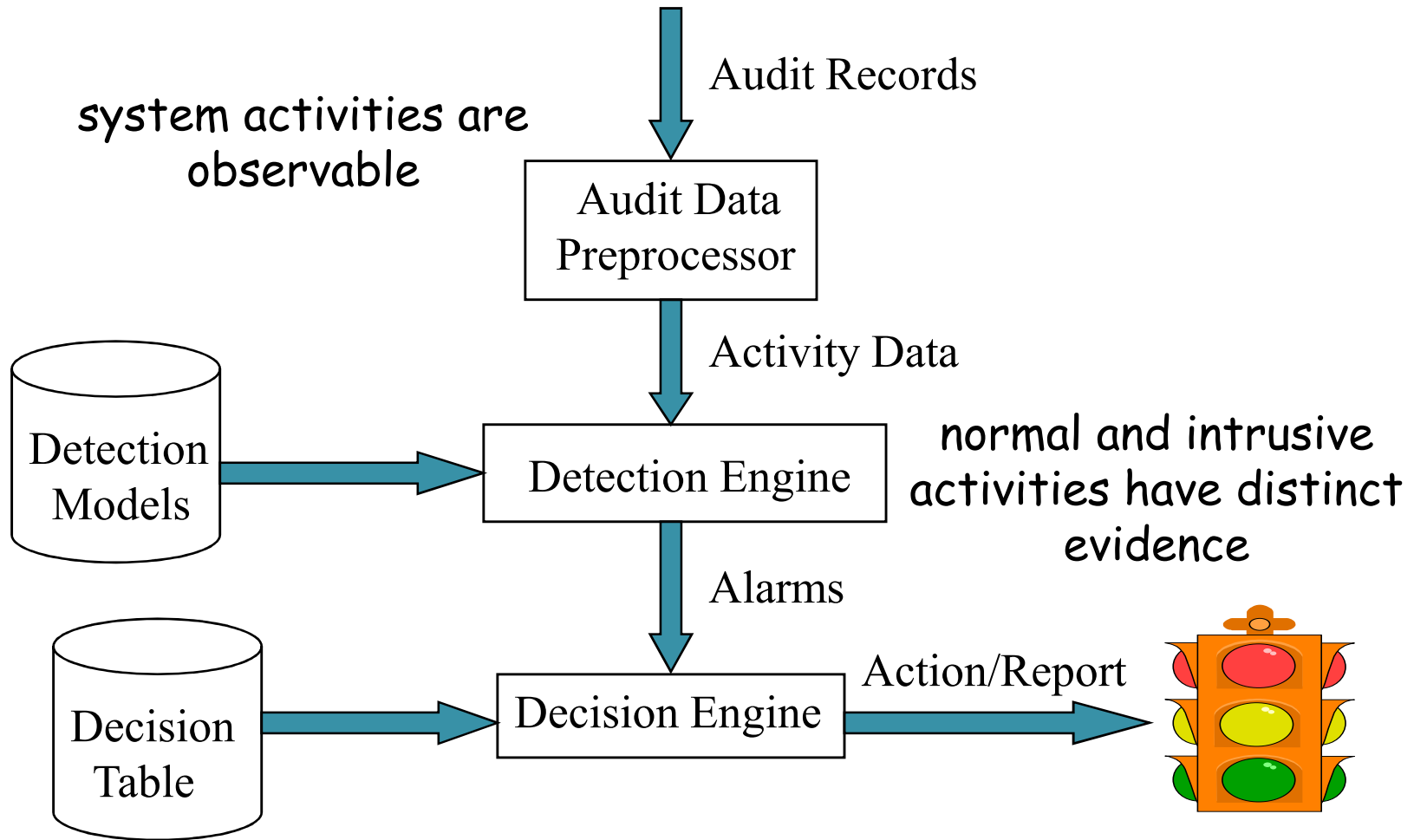


# Overview of IDS/IPS

- **Intrusion detection system (IDS)**
  - A system that performs automatically the process of intrusion detection.
- **Intrusion prevention system (IPS)**
  - A system that has an ambition to both detect intrusions and manage responsive actions.
  - Technically, an IPS contains an IDS and combines it with preventive measures (firewall, antivirus, vulnerability assessment) that are often implemented in hardware.



# Components of Intrusion Detection System





# Intrusion Detection Approaches

- **Modeling**
  - Features: evidences extracted from audit data
  - Analysis approach: piecing the evidences together
    - **Misuse detection** (a.k.a. signature-based)
    - **Anomaly detection** (a.k.a. statistical-based)
- **Deployment: Network-based or Host-based**
  - **Network based**: monitor network traffic
  - **Host based**: monitor computer processes



# Security Information and Event Management (SIEM)

- **LMS** - “**Log Management System**” – a system that collects and store Log Files (from Operating Systems, Applications, etc) from multiple hosts and systems into a single location, allowing centralized access to logs instead of accessing them from each system individually.
- **SLM /SEM**– “**Security Log/Event Management**” – an LMS, but marketed towards security analysts instead of system administrators. SEM is about highlighting log entries as more significant to security than others.
- **SIM** – “**Security Information Management**” - an Asset Management system, but with features to incorporate security information too. Hosts may have vulnerability reports listed in their summaries, Intrusion Detection and AntiVirus alerts may be shown mapped to the systems involved.
- **SEC** - “**Security Event Correlation**” – To a particular piece of software, three failed login attempts to the same user account from three different clients, are just three lines in their logfile. To an analyst, that is a peculiar sequence of events worthy of investigation, and Log Correlation (looking for patterns in log files) is a way to raise alerts when these things happen.
- **SIEM** – “**Security Information and Event Management**” – SIEM is the “All of the Above” option, and as the above technologies become merged into single products, became the generalized term for managing information generated from security controls and infrastructure. We’ll use the term SIEM for the rest of this presentation

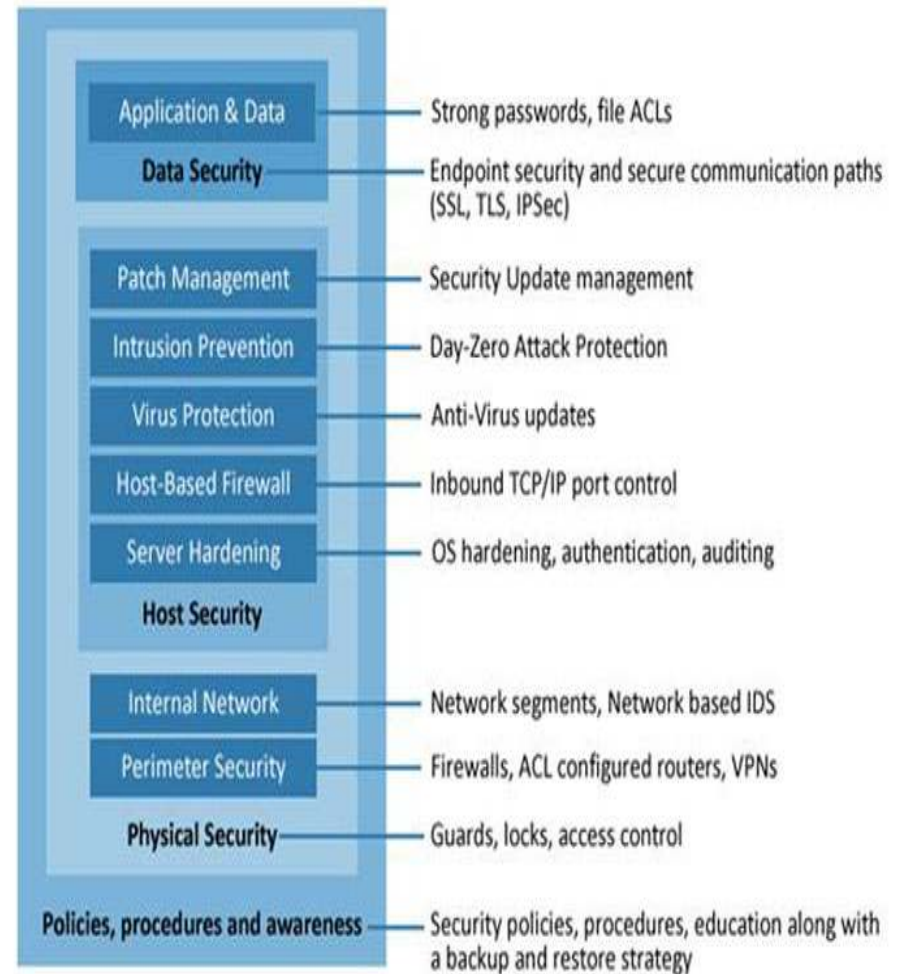
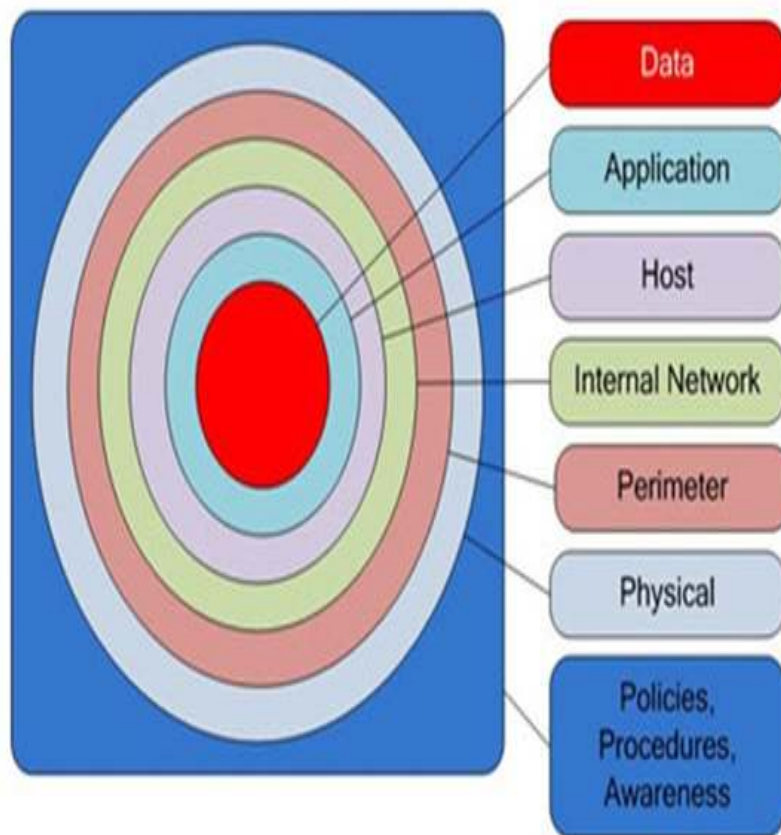


# Background on Network Components

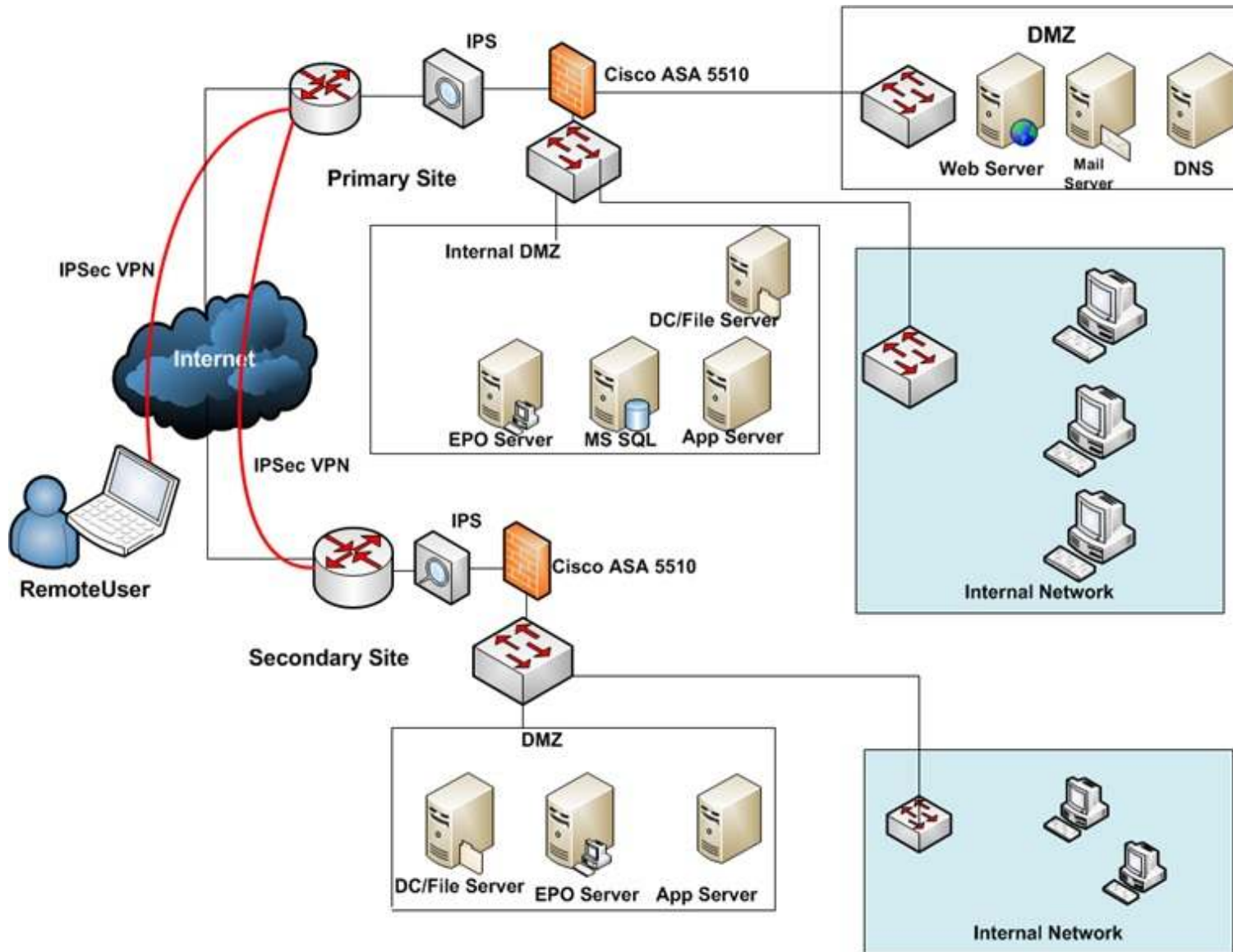
- Router
- Switch (L2 & L3)
- Servers (Application, Database, etc.)
- Firewall
- Demilitarized Zone (DMZ)
- Virtual Private Network
- IPS/IDS

# Defense in Depth

## Defense in Depth Layers



# Typical Corporate Environment

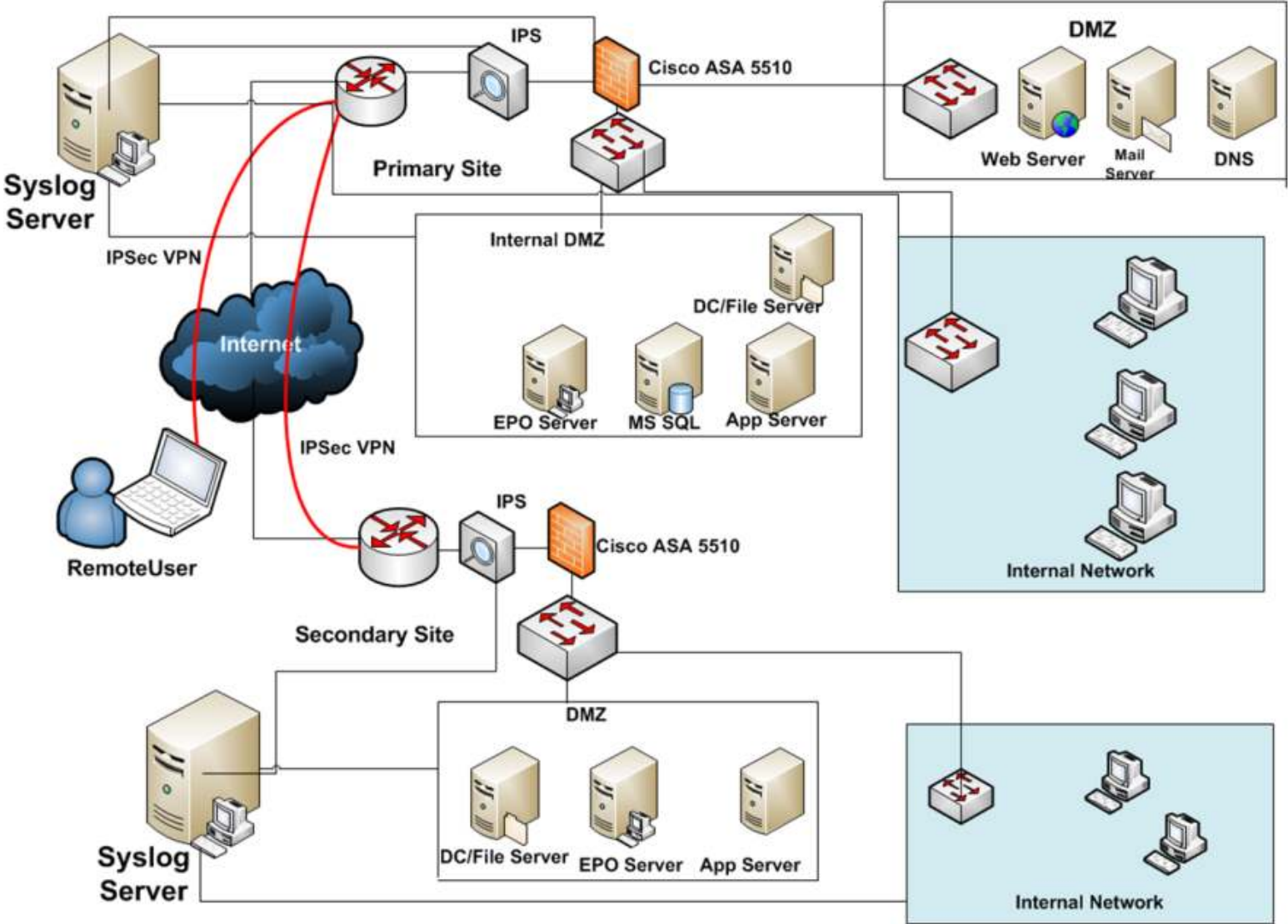




# Log Management

- Log management (LM) comprises an approach to dealing with large volumes of computer-generated log messages (also known as audit records, audit trails, event-logs, etc.).
- LM covers log collection, centralized aggregation, long-term retention, log analysis (in real-time and in bulk after storage) as well as log search and reporting.

# Log Management







# Log Management Challenges

- Analyzing Logs for Relevant Security Intelligence
- Centralizing Log Collection
- Meeting IT Compliance Requirements
- Conducting Effective Root Cause Analysis
- Making Log Data More Meaningful
- Tracking Suspicious User Behavior



## Introduction to SIEM

- The term Security Information Event Management (SIEM), coined by Mark Nicolett and Amrit Williams of Gartner in 2005.
- Describes the product capabilities of gathering, analyzing and presenting information from network and security devices; identity and access management applications; vulnerability management and policy compliance tools; operating system, database and application logs; and external threat data.
- Security Information and Event Management (SIEM) is a term for software and products services combining security information management (SIM) and security event manager (SEM).



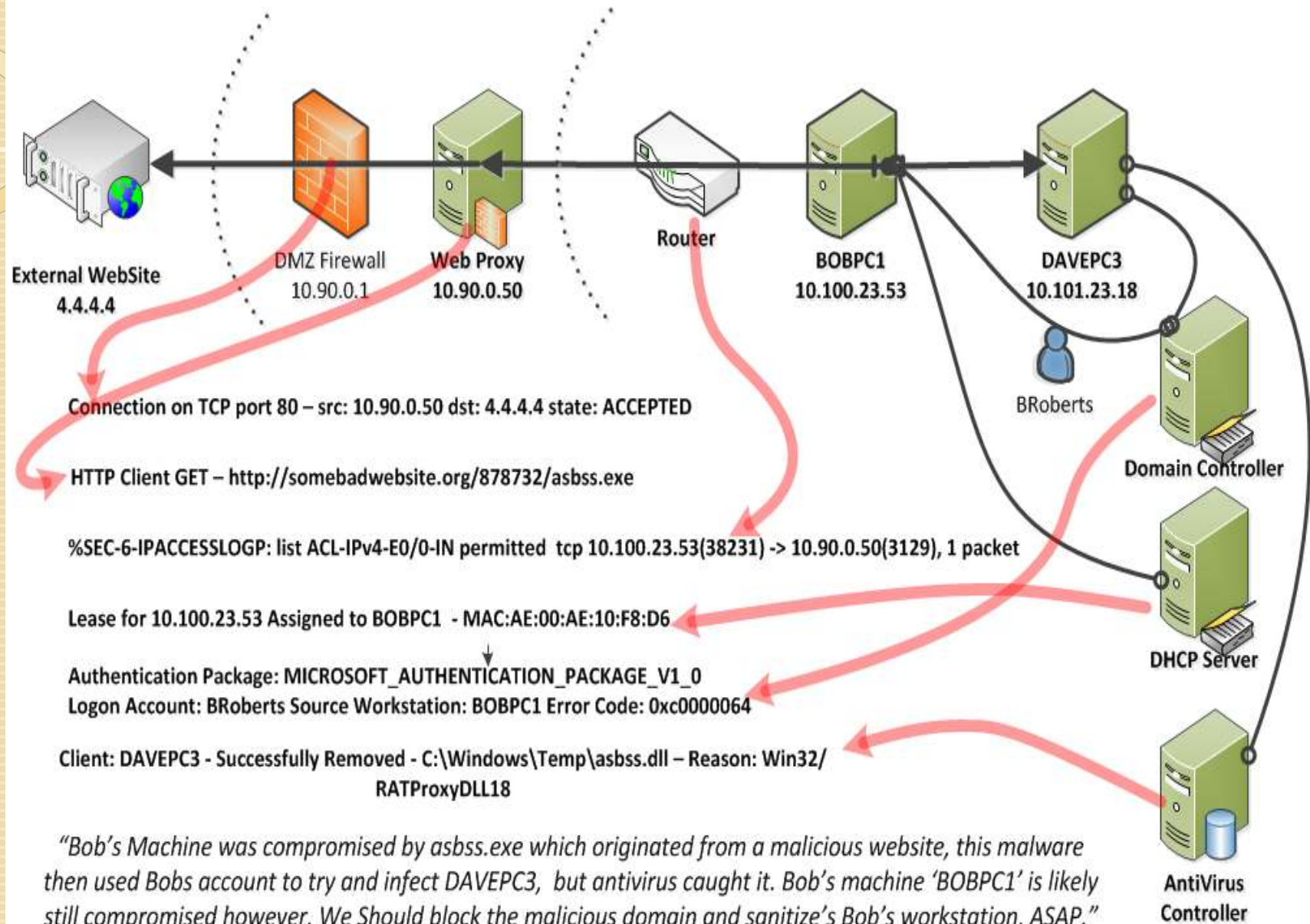
## Key Objectives

- Identify threats and possible breaches
- Collect audit logs for security and compliance
- Conduct investigations and provide evidence

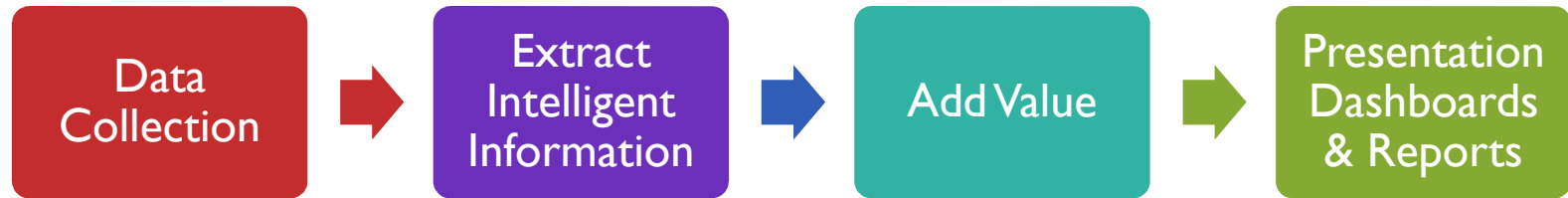
## SIEM vs LM

Functionality	Security Information and Event Management (SIEM)	Log Management (LM)
Log collection	Collect security relevant logs + context data	Collect all logs
Log pre-processing	Parsing, normalization, categorization, enrichment	Indexing, parsing or none
Log retention	Retain parsed and normalized data	Retain raw log data
Reporting	Security focused reporting	Broad use reporting
Analysis	Correlation, threat scoring, event prioritization	Full text analysis, tagging
Alerting and notification	Advanced security focused reporting	Simple alerting on all logs
Other features	Incident management, analyst workflow, context analysis, etc.	High scalability of collection and storage

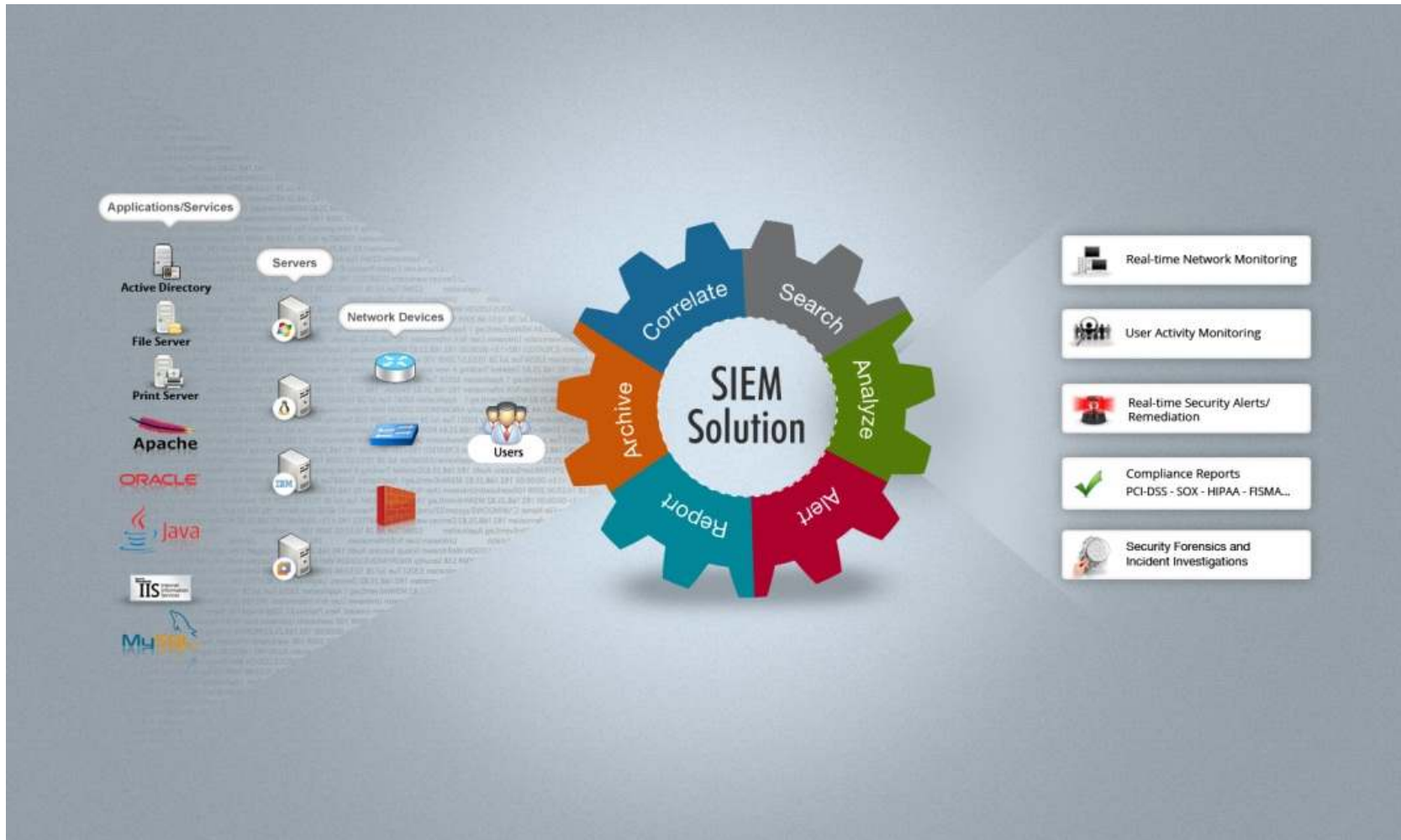
# A SIEM Scenario



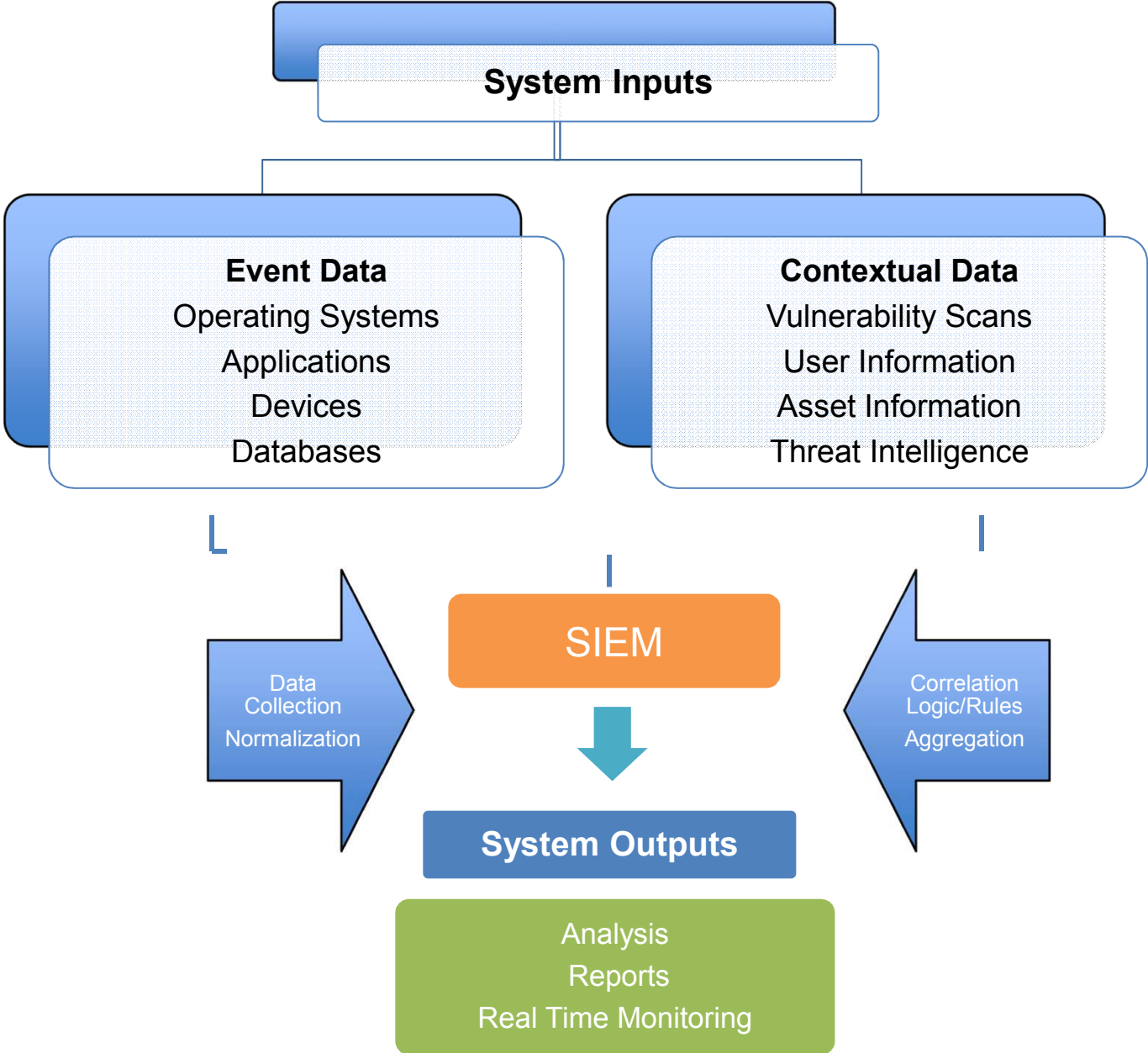
# SIEM Process Flow



# Typical Working of an SIEM Solution



# SIEM Architecture

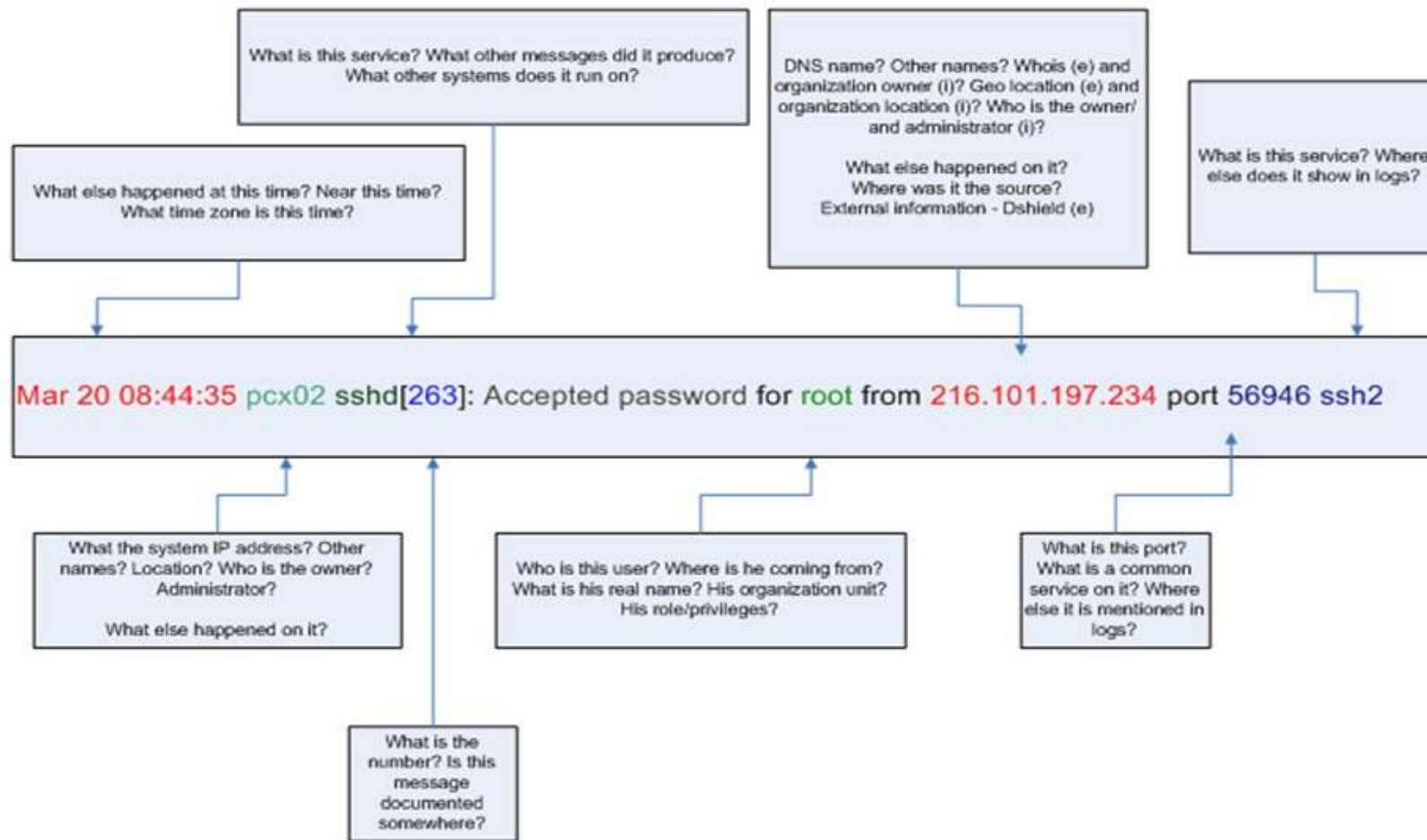




# Typical Features of SIEM



# Context

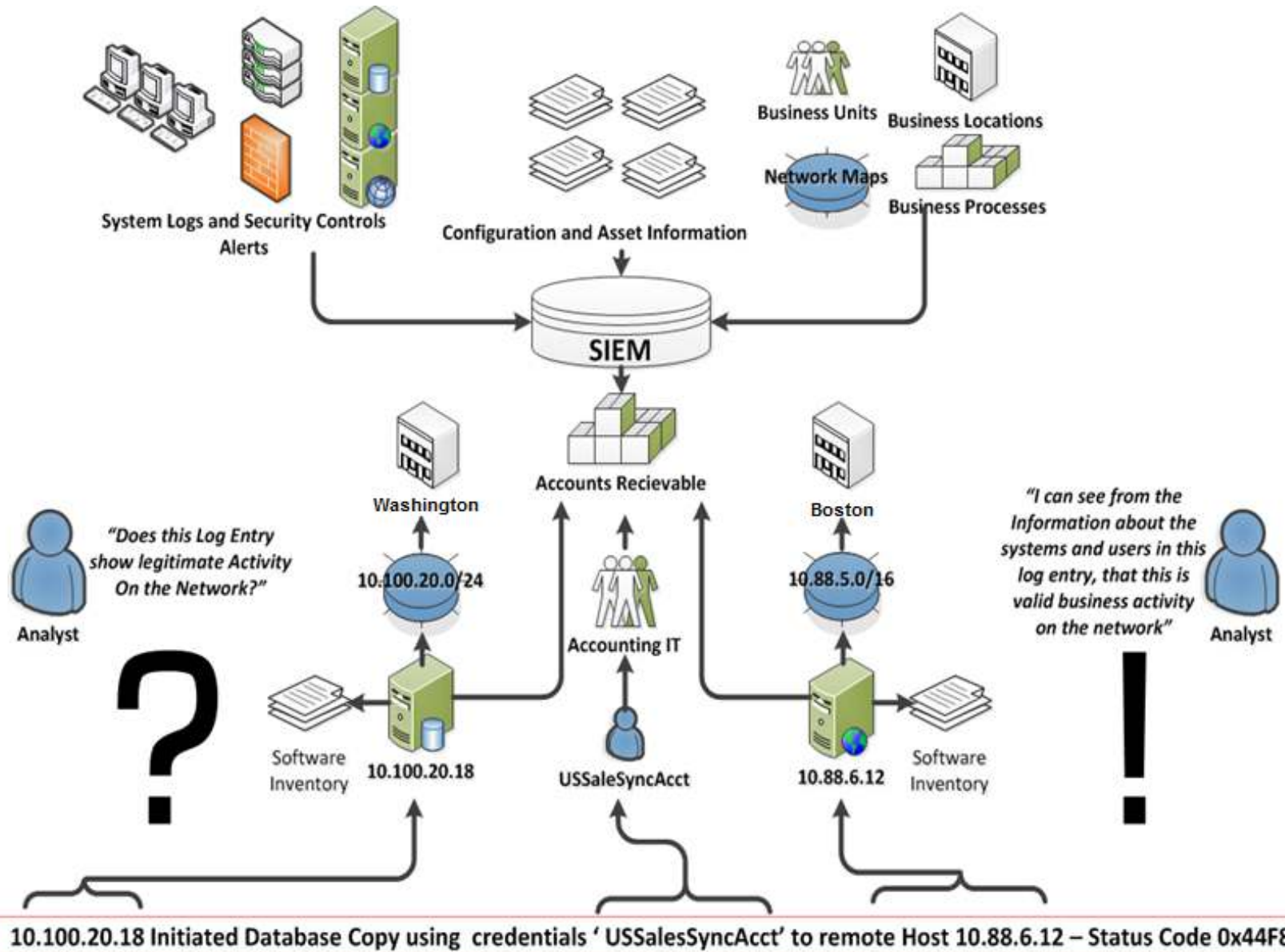




# Adding Context

- **Examples of context**
  - Add geo-location information
  - Get information from DNS servers
  - Get User details (Full Name, Job Title & Description)
- **Add context aids in identifying**
  - Access from foreign locations
  - Suspect data transfer

# How a Log File is Generated in your Network





# The Beauty of Log Correlation

- Log Correlation is the difference between:

```
"14:10 7/4/20110 User BRoberts Successful Auth to  
10.100.52.105 from 10.10.8.22"
```

and...

```
"An Account belonging to Marketing connected to an  
Engineering System from an office desktop, on a day  
when nobody should be in the office"
```



## Why is SIEM Necessary?

- Rise in data breaches due to internal and external threats
- Attackers are smart and traditional security tools just don't suffice
- Mitigate sophisticated cyber-attacks
- Manage increasing volumes of logs from multiple sources
- Meet stringent compliance requirements