NETWORK SECURITY
INTRUSION DETECTION

Leonardo Querzoni
querzoni@diag.uniroma1.it

SAPIENZA
UNIVERSITÀ DI ROMA

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

INTRODUCTION

- No shielding (firewalls, VPNs, etc.) is 100% intrusion proof!
  - New attack techniques
  - Unexploited “silent” vulnerabilities
  - Misconfigurations
  - Malicious insiders
- Continuously monitor systems and detect attacks

INTRODUCTION

Intrusion detection

> *"the process of **monitoring** the events occurring **in a computer system or network** and analyzing them for signs of intrusions, defined as **attempts to compromise the confidentiality, integrity, availability**, or to bypass the security mechanisms of a computer or network" - NIST*

ATTACKS

Attack: intrusion attempt

- may be blocked by an effective shield

Intrusion: successful attack

An intrusion represents a malicious, externally induced, operational fault.

ATTACKS

Attacks can be classified with respect to:

- Attack type
- Involved network connections
- Source
- Environment
- Automation level

ATTACKS

Attack type: Denial of Service

Goal: shut down a network, computer, or process; or otherwise deny the use of resources or services to authorized users.

Is an attack to availability

ATTACKS

Attack type: Denial of Service

Strategies:

- Consumption of scarce resources
  - Network connectivity
  - Using your own resources against you
  - Bandwidth Consumption
  - Other resources (disk, CPU, etc.)
- Destruction or alteration of configuration information
- Physical destruction or alteration of network components

ATTACKS

Attack type: Probing/Scanning

Goal: identify valid IP addresses in a domain and collect information about them (e.g. what services they offer, operating system used).

This information provides an attacker with the list of potential vulnerabilities that can later be used to perform an attack against selected machines and services.

ATTACKS

Attack type: Probing/Scanning

- Tools: IPsweep, Portsweep, nmap
- Countermeasures are very effective in detecting fast and disperse noisy scan (look for IPs tat make more than N connections in T seconds)
- Stealthy scans are more challenging

ATTACKS

Attack type: Compromises

Goal: breaking into the system and gaining privileged access to hosts

Use known bugs and vulnerabilities

ATTACKS

Attack type: Compromises

R2L - Remote to local attacks

- An attacker who has the ability to send packets to a machine over a network (but does not have an account on that machine), gains access (either as a user or as the root) to the machine
- Usually based on password guessing or known vulnerabilities (e.g buffer overflows in Sendmail).

ATTACKS

Attack type: Compromises

U2R - User to root attack

- An attacker who has an account on a computer system is able to misuse/ elevate her or his privileges by exploiting a vulnerability in computer mechanisms, a bug in the operating system or in a program that is installed on the system
- Example: buffer overflow in Sendmail.

ATTACKS

Attack type: Viruses/Worms/Trojan horses/RootKits

Goal: various + replicate on host machines and propagate through a network

ATTACKS

Attack type: Viruses/Worms/Trojan horses/RootKits

Viruses:

- Programs that persist on compromised devices by attaching them to other programs and infecting them.
- Viruses typically need human interaction for replication and spreading to other computers.

ATTACKS

Attack type: Viruses/Worms/Trojan horses/RootKits

Worms:

- Self-replicating programs that aggressively spread through a network
- Can be categorized depending on the medium used for diffusion: traditional (direct network connection), e-mail (or other client applications), Windows file sharing protocols, hybrid.

ATTACKS

Attack type: Viruses/Worms/Trojan horses/RootKits

Trojan horses:

- Malicious, security-breaking programs that are disguised as something benign.
- Typically the user download and activates the attack on purpose.

ATTACKS

Attack type: Viruses/Worms/Trojan horses/RootKits

Root Kit:

- Piece of software that once installed on a victim's machine takes full control of it by obtaining administration privileges
- Root kits hide their presence on compromised machines by deceiving security systems, thanks to their ability to directly interact at the operating system level.
- They often open up a port to allow a hacker to take full control of the system (RAT o back door).
- Some root kits give a hacker even more control of a machine than a victim may have themselves.

ATTACKS

- Involved network connections:
  - Multiple network connections (e.g. Denial of Service)
  - Single network connection (e.g. Compromises)

ATTACKS

- Source:
    - Single source (e.g. typical port scanning)
    - Multiple sources (e.g. Distributed Denial of Service)

ATTACKS

- Environment: where the attack occurs
  - Intrusion on host machine
  - Network intrusion
  - Intrusion on P2P like environments
  - Intrusion in a wireless network

ATTACKS

Automation level:

- Automated attacks: use automated tools that are capable of probing and scanning a large part of the Internet in a short time period.
- Semi-automated attacks: deploy automated scripts for scanning and compromise of network machines and installation of attack code, and then use the handler (master) machines to specify the attack type and victim's address.

ATTACKS

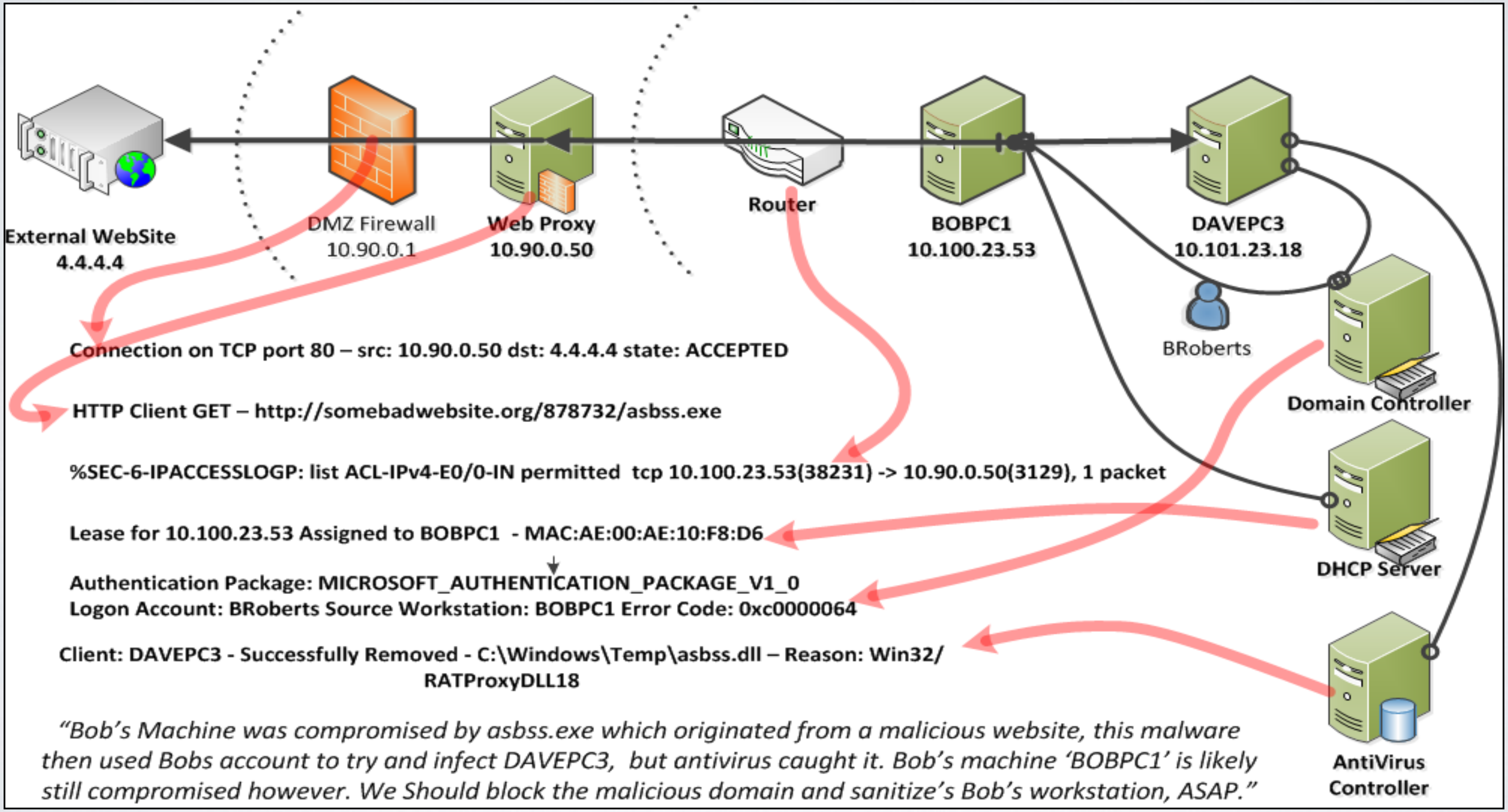
Automation level:

- Manual attacks: involve manual scanning of machines and typically require a lot of knowledge and work.

Manual attacks are not very frequent, but they are usually more dangerous and harder to detect than semi-automated or automated attacks,

MONITORING FOR ATTACKS

A simple attack may impact several subsystems:

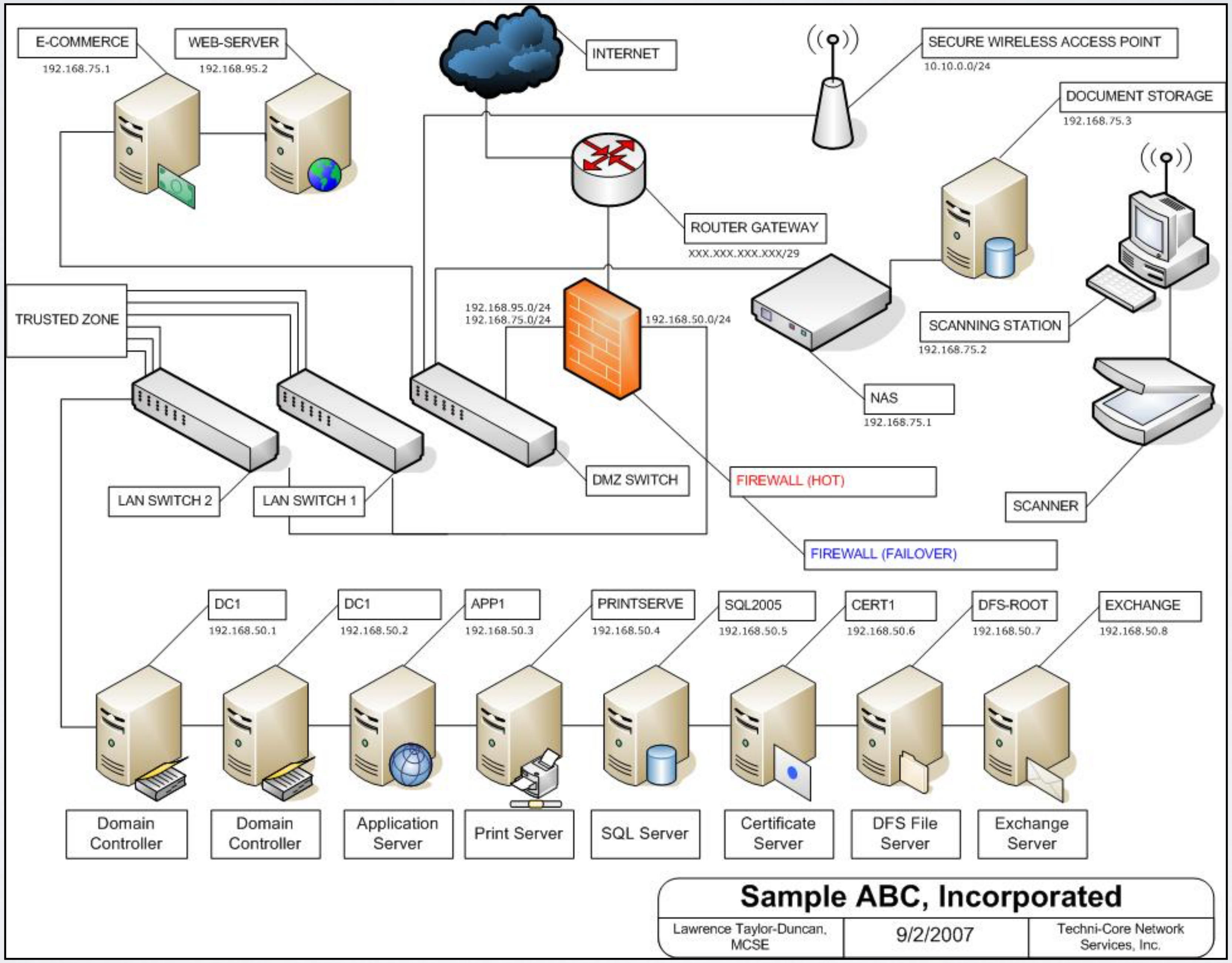


```
Connection on TCP port 80 – src: 10.90.0.50 dst: 4.4.4.4 state: ACCEPTED

HTTP Client GET – http://somebadwebsite.org/878732/asbss.exe

%SEC-6-IPACCESSLOGP: list ACL-IPv4-E0/0-IN permitted  tcp 10.100.23.53(38231) -> 10.90.0.50(3129), 1 packet

Lease for 10.100.23.53 Assigned to BOBPC1  - MAC:AE:00:AE:10:F8:D6

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: BRoberts Source Workstation: BOBPC1 Error Code: 0xc0000064

Client: DAVEPC3 - Successfully Removed - C:\Windows\Temp\asbss.dll – Reason: Win32/
RATProxyDLL18
```

"Bob's Machine was compromised by asbss.exe which originated from a malicious website, this malware then used Bobs account to try and infect DAVEPC3, but antivirus caught it. Bob's machine 'BOBPC1' is likely still compromised however. We Should block the malicious domain and sanitize's Bob's workstation, ASAP."

MONITORING FOR ATTACKS

Monitoring data is generated by all IT systems:



MONITORING FOR ATTACKS

Monitoring data is generated by all IT systems:

Network flows

- Traffic flows are metadata records of network communication sessions.
- They capture session details but NOT the actual content (payload).
- The basic identification criteria for any flow record (the "5-Tuple") are:
  - Source IP Address: The originator of the session.
  - Destination IP Address: The recipient of the session.
  - Source Port: The dynamically assigned client port.
  - Destination Port: The service port (e.g., 80 for HTTP, 443 for HTTPS).
  - Protocol: The transport protocol (e.g., TCP, UDP, ICMP).

MONITORING FOR ATTACKS

Monitoring data is generated by all IT systems:

Network flows

- Traffic flows are metadata records of network communication sessions.
- They capture session details but NOT the actual content (payload).
- Flows also contain additional quantitative and state information:
  - Start and End Time: Duration of the conversation.
  - Number of Bytes / Packets: Indicates the volume of data transferred.
  - TCP Flags: Provides session state (e.g., SYN, ACK, FIN, RST).
  - Autonomous System (AS) Number: Useful for tracing external connections to a known network entity.

MONITORING FOR ATTACKS

Monitoring data is generated by all IT systems:

Event/system logs

- IT assets produce log about their activities
- Error logs may include information that is generated in response to a malicious activity (e.g. failed authentication attempts
- Sources:
  - Network appliances
  - Servers
  - Hosts
  - Applications

MONITORING FOR ATTACKS

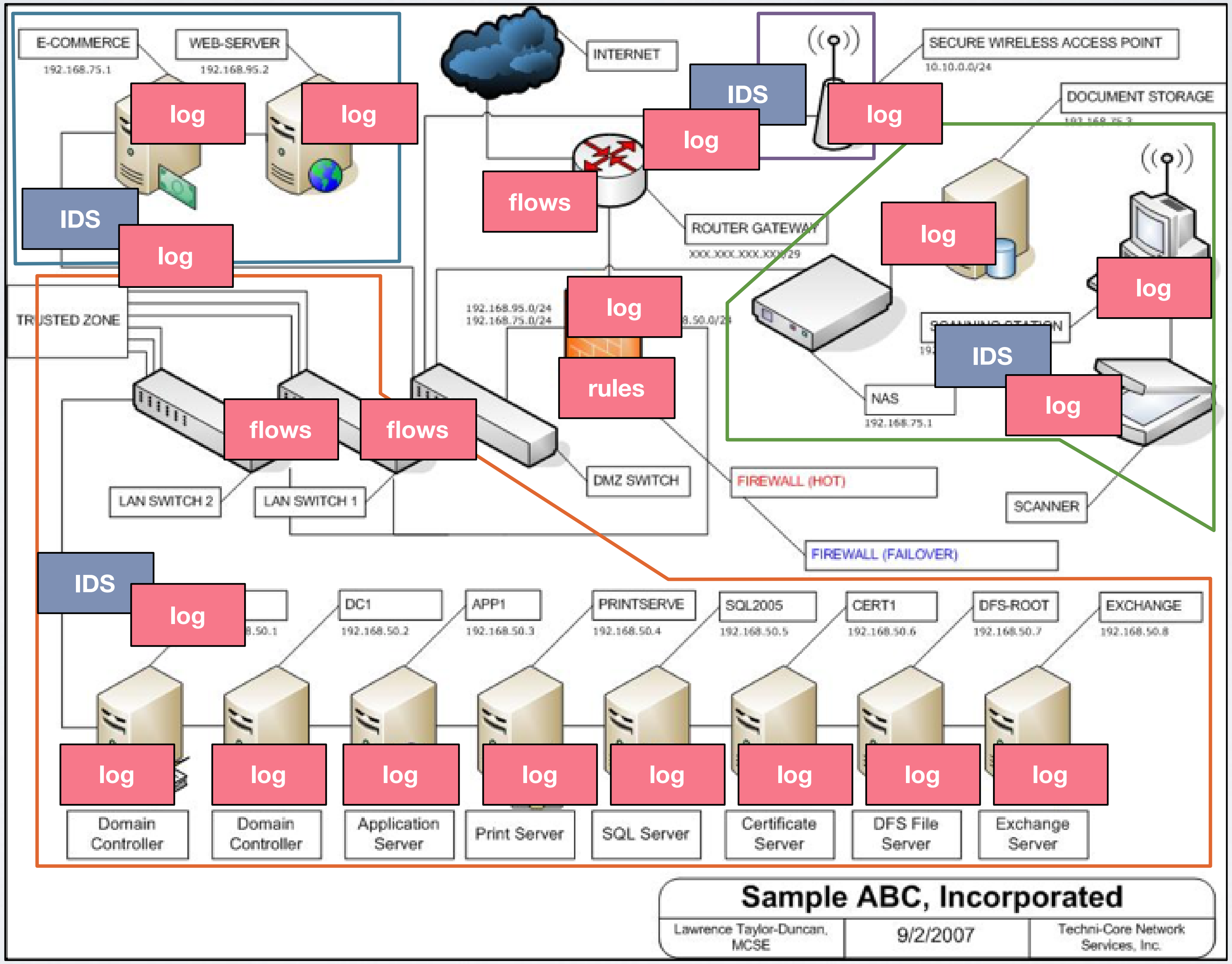
Monitoring data is generated by all IT systems:

Full packet capture

- Includes the payload of network flows.
- When flow records and logs are insufficient, FPC allows security analysts to literally reconstruct the attack and analyze malware payloads or encryption keys. => Useful for digital forensics activities!
- FPC is not typically performed everywhere due to practical limitations:
    - Massive Storage Requirements: Storing all payloads for an enterprise network is impractical and expensive.
    - Performance Overhead: FPC hardware must handle high-speed line rates without dropping packets.
- FPC is often deployed conditionally (only capturing packets that trigger an alert) or on low-volume, high-value network segments.

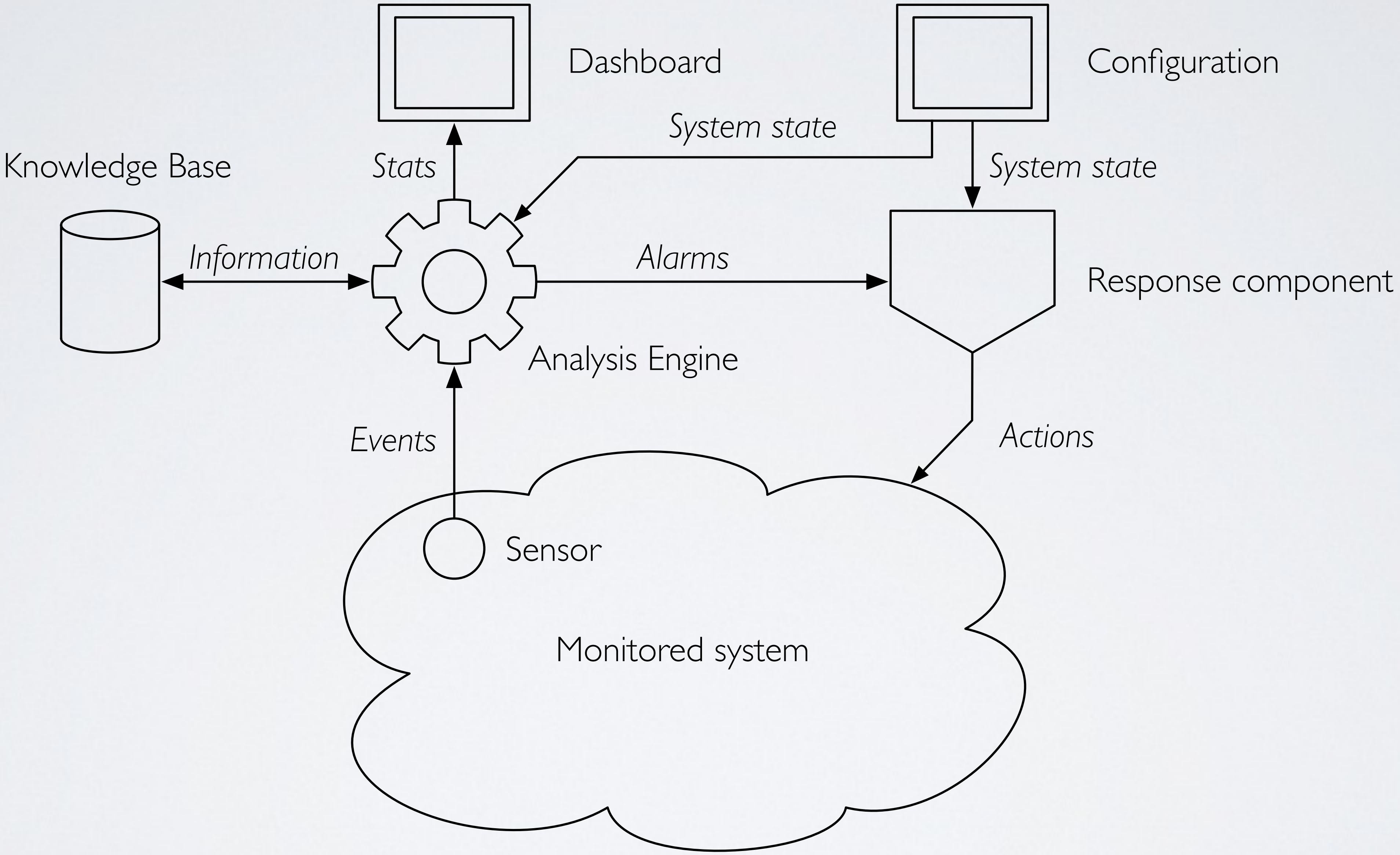
MONITORING FOR ATTACKS

Monitoring data is generated by all IT systems:



INTRUSION DETECTION SYSTEMS

- General framework:



INTRUSION DETECTION SYSTEMS

Desired characteristics for an IDS:

- Detection KPIs
- Timeliness
- Fault tolerance

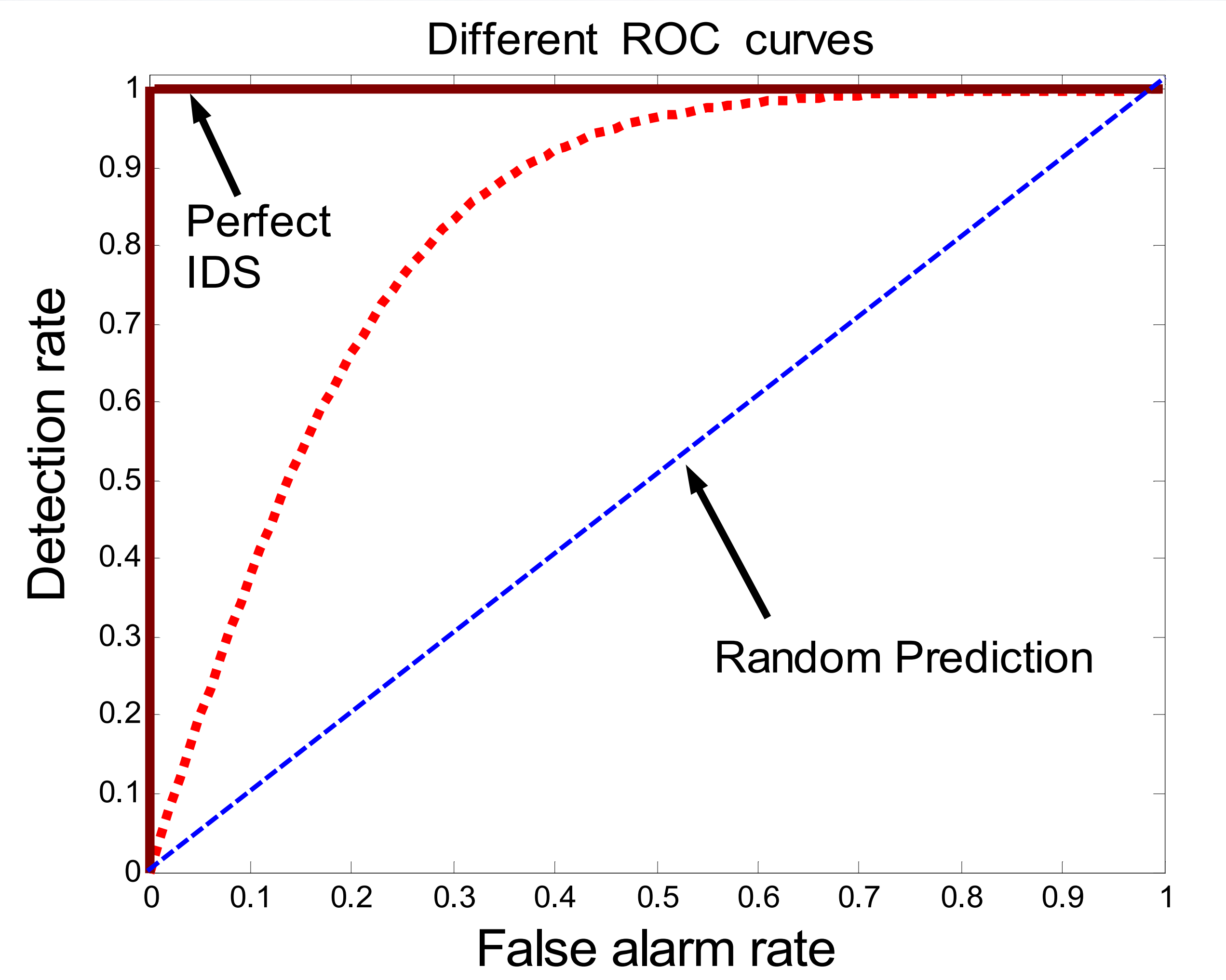
INTRUSION DETECTION SYSTEMS

Detection KPIs

- Detection rate (true positive rate) = identified attacks / total attacks
- False alarms rate (false positive rate) = wrong attack identifications / total normal connections
- Accuracy = (identified attacks + identified normal events) / total events
- Precision = identified attacks / (identified attacks + wrong attack identifications)
- Receiver Operating Characteristics

INTRUSION DETECTION SYSTEMS

The ROC curve represents the trade-off between detection rate and false alarm rate.



INTRUSION DETECTION SYSTEMS

Timeliness

- Includes:
  - Processing time
  - Propagation time
- Response time = Time it takes for the IDS to detect a threat and trigger an alert from the moment the intrusion occurs

INTRUSION DETECTION SYSTEMS

Fault tolerance

- IDSs are vulnerable as well !
- Example: DoS
  - the attacker floods the system with a huge number of obvious false attacks
  - the real attack is obfuscated

INTRUSION DETECTION SYSTEMS

IDSs can be categorized with respect to:

- Monitored system
- Detection methodology
- Time aspects
- Architecture
- Reaction type

INTRUSION DETECTION SYSTEMS

Monitored system: **host based (HIDS)**

- monitor events occurring within a single host
  - network traffic
  - logs
  - running processes
  - file access
  - configuration changes

INTRUSION DETECTION SYSTEMS

Monitored system: **host based (HIDS)**

- monitoring can also be limited to a single specific application
- typical deployment for sensitive hosts (e.g. servers)
- also useful in more complex IDS infrastructures when you want to monitor activity on encrypted channels

INTRUSION DETECTION SYSTEMS

Monitored system: **host based (HIDS)**

- Typical techniques leveraged by host based IDSs:
  - Code analysis
  - Sandbox-based execution
  - Network traffic analysis
  - Filesystem monitoring (integrity checking, attribute checking, access monitor)
  - Log analysis

INTRUSION DETECTION SYSTEMS

Monitored system: **host based (HIDS)**

- The lack of context for detected actions make more difficult to detect attacks.
- Need complex configuration and extensive tuning
- Can have a negative impact on the performance of co-hosted applications

EDR systems are the “active” evolution of HIDS:

- Track all activities within an host (even after a malware already compromised the host)
- Automatically respond by closing processes or isolating the host
- Results are centrally aggregated

INTRUSION DETECTION SYSTEMS

Monitored system: **network based (NIDS)**

- Monitor traffic within specified network segments
- Often deployed at the boundary between separated networks
- Can perform analysis at several layers
  - Application (HTTP, SMTP, POP/IMAP, DNS)
  - Transport/network (IP, TCP, UDP, ICMP)
  - Lower layers (MAC, ARP)

INTRUSION DETECTION SYSTEMS

Monitored system: **network based (NIDS)**

- Deployment type:
  - In line
    - All the traffic it monitor passes through it (gateway/firewall)
    - Can block traffic/attacks > IPS
  - Passive
    - Monitors a copy of the traffic

INTRUSION DETECTION SYSTEMS

Monitored system: **network based (NIDS)**

- Usually works in stealth mode (no IP addresses = higher resistance to attacks)
- High resource usage
- Network-based IDSs can be installed such that they do not have effect on existing computer systems or infrastructures
- Cannot monitor data passing though encrypted channels (SSL, SSH, etc.)
  - But if you set up a TLS proxy…

INTRUSION DETECTION SYSTEMS

Monitored system: **log files (LIDS)**

- Monitor only specific applications such as database management systems, content management systems, accounting systems, etc.
- Has access to types of information that network based or host based IDSs do not have
- Can keep track of session information
- Complex tuning.

INTRUSION DETECTION SYSTEMS

Monitored system: **wireless networks (WIDS)**

- The wireless medium offers new possibilities but also new risks
- Physical layer in wireless networks is essentially a broadcast medium and therefore less secure than wired computer networks.
- There are no specific traffic concentration points (e.g. routers) where packets can be monitored.

Common attacks:

- Rogue access points
- Deauthentication or DoS attacks

INTRUSION DETECTION SYSTEMS

Monitored system: **wireless networks**

- The wireless medium offers new possibilities but also new risks
- Separation between normal and anomalous traffic is often not clear in wireless ad-hoc networks (normal nodes out of sync)
- Directional transmission impedes interception

INTRUSION DETECTION SYSTEMS

Monitored system: **wireless networks**

- Effective deployment is difficult:
  - The network has imprecise boundaries. Where do I need to place sensors ?
  - Attacker location identification is more tricky (triangulation)
  - Continuously scanning multiple networks require expensive hardware (multi-radio support)

INTRUSION DETECTION SYSTEMS

Monitored system: **alerts from IDS (SIEMs ?)**

- Due to the complexity of tasks involved in identifying attacks in a large-scale infrastructure, IDSs can be stacked at different levels with different roles.
- Hierarchical/DAG-based structures
- Simplifies management
- Improves detection rate

INTRUSION DETECTION SYSTEMS

Detection methodology: **misuse detection**

- Strategy based on the knowledge about previously happened attacks.
- Abnormal behaviors are modeled
- Everything that departs from the model is normal behavior
- The system ignores normal behaviors

INTRUSION DETECTION SYSTEMS

Detection methodology: **misuse detection**

- Signature-based IDSs
  - look in a database containing “fingerprints” of known attacks
  - work like AntiVirus software
  - unable to detect new attack types
  - difficult detection of old attack variations
  - signatures DB must be kept up-to-date
  - Example: SNORT or Suricata

INTRUSION DETECTION SYSTEMS

Detection methodology: **misuse detection**

- Rule-based systems
  - Use “if…then” conditions to capture possible attacks
  - Can leverage high-performance rule engines

INTRUSION DETECTION SYSTEMS

Detection methodology: **misuse detection**

- State transition analysis
  - Requires the construction of a finite state machine
    - states correspond to different IDS states
    - transitions characterize certain events that cause IDS states to change
  - IDS states correspond to different states of the network protocol stacks or to the integrity and validity of current running processes, etc.
  - When the automaton reaches a state that is flagged as a security threat, the intrusion is reported as a sign of malicious attacker activity.

INTRUSION DETECTION SYSTEMS

Detection methodology: **misuse detection**

- Machine-learning based techniques
  - Each instance in a data set is labeled as normal or intrusive and a learning algorithm is trained over the labeled data.
  - High degree of accuracy in detecting known attacks and their variations (with respect to signature-based intrusion detection systems).
  - Different classification algorithms: decision trees, modified nearest neighbor algorithms, fuzzy association rules, neural networks, Bayes classifiers, genetic algorithms, genetic programming, support vector machines, adaptive regression splines, etc.

INTRUSION DETECTION SYSTEMS

Detection methodology: **anomaly detection**

- Strategy based on knowledge about the system.
- The normal system behavior is modeled
- Everything that departs from the model is a potential attack

INTRUSION DETECTION SYSTEMS

Detection methodology: **anomaly detection**

- Programmed systems: the system is configured with fixed behavioral models.
  - Default deny: the system expected behavior is accurately modeled. Only modeled states are allowed.
  - Descriptive statistics: the normal behavior of the system is described by a statistical model build on a number of variables
    - Simple statistics, rules, thresholds

INTRUSION DETECTION SYSTEMS

Detection methodology: **anomaly detection**

- Self-learning systems: build automatically a model representing the system normal behavior
  - Non-time series: use stochastic modeling that do not consider time
    - Rule-based modeling
    - Statistical modeling
  - Time series: the model take into account time correlation between events
    - Neural Networks
    - Hidden Markov Models

INTRUSION DETECTION SYSTEMS

Detection methodology: **anomaly detection**

- Rule based methods
  - Characterize normal behavior of users, networks and/or computer systems by a set of rules
  - When rules are broken, an attack is suspected
  - Rules allow a “high-level” description
  - Rules can be derived automatically through “expert systems”

INTRUSION DETECTION SYSTEMS

Detection methodology: **anomaly detection**

- Statistical methods
  - Monitor the user or system behavior by measuring certain variables over time
  - Keep averages of these variables (moving event/time windows) and detect whether thresholds are exceeded based on the standard deviation of the variable
  - More advanced techniques can be used (e.g. probabilistic Bayesian inference)

INTRUSION DETECTION SYSTEMS

Detection methodology: **anomaly detection**

- Statistical methods
  - Outliers detection: data points that are very different from the rest of the data
  - Data points are modeled using a stochastic distribution, and points are determined to be outliers depending on their relationship with this model

INTRUSION DETECTION SYSTEMS

Detection methodology: **anomaly detection**

- Distance based methods
  - Estimating the multidimensional distributions of the data points is difficult and inaccurate
  - Detect outliers by computing distances among points
  - These techniques are based on computing the full dimensional distances of points from one another using all the available features, and on computing the densities of local neighborhoods (clusters)

INTRUSION DETECTION SYSTEMS

Detection methodology: **anomaly detection**

- Profiling methods
  - A profile characterizing the normal execution of protocols and services is generated.
  - Any deviation from the profile is considered as suspicious
  - Immune system inspired approaches
    - Small patterns of system calls happening in legal interactions are collected
    - If an interaction presents a pattern that has not been signaled before an alarm is fired

INTRUSION DETECTION SYSTEMS

Detection methodology: **compound detection**

- Bases its functioning on the maintenance of models for both normal and abnormal behaviors
- Events observed at runtime are compared to the models
- The relative distance of an event from the two models is used to decide if it can be classified as an attack

INTRUSION DETECTION SYSTEMS

Detection methodology: recap

Characteristic	Misuse-Based Detection	Anomaly-Based Detection	Compound-Based Detection
Primary Focus	Known attacks (signatures)	Deviations from normal behavior	Known and unknown attacks (hybrid)
Detection of Zero-Day Attacks	Ineffective	Effective	Effective (due to anomaly component)
False Positive Rate	Low	High	Medium (lower than anomaly-based)
False Negative Rate	High for unknown threats	Low	Low (both known and unknown covered)
Resource Usage	Moderate	High	High (due to dual methods)
Updates Required	Frequent signature updates	Baseline recalibration	Both signature updates and baseline management
Complexity	Low	Moderate to high	High (due to hybrid approach)
Threat Coverage	Limited to known threats	Broad (novel and insider threats)	Comprehensive (combines both)
Best Use Case	Environments with known threats	Dynamic or unpredictable environments	High-security environments requiring broad detection

INTRUSION DETECTION SYSTEMS

Time aspects: on-line tools

- Can check streams of incoming data
- Useful to timely detect attacks and promptly react.
- Require strong processing capabilities
  - Stream processors
  - High-performance rule engines
- Cannot work on events that are produced out of sync (e.g. statistical reports)

INTRUSION DETECTION SYSTEMS

Time aspects: off-line tools

- Post-analysis of audit data
  - Best for reporting or forensics
- Performance is rarely an issue
  - Can perform more complex analysis
- Work on more comprehensive datasets

INTRUSION DETECTION SYSTEMS

Architecture: centralized

- The analysis of the data is performed in a fixed number of locations, independent of how many hosts are being monitored
- We are interested only in the analysis aspects, not on data gathering
- Simplifies configuration and management
- Less fault tolerant and less scalable with respect to load

INTRUSION DETECTION SYSTEMS

Architecture: distributed

- The analysis of the data is performed in a number of locations that is proportional to the number of hosts being monitored
- Complex configuration and management
- Graceful degradation in case of failures
- Easier to customize (single instances can be adapted to ad-hoc duties)
- Distributed agent-based IDSs are an active research area

INTRUSION DETECTION SYSTEMS

Reaction type

- Typically IDSs only report alarms to human administrators
- Non destructive reaction operations can be employed for specific attacks:
  - patching
  - firewall rule injection
- The most common reaction is an increase in the sensitivity of sensors to gather more detailed information.

INTRUSION DETECTION SYSTEMS

Reaction type

Action	Description	Use Case
Dropping Malicious Packets	Blocks specific malicious packets from reaching their destination.	Blocking malicious payloads, e.g., SQL injection, DDoS.
Blocking or Terminating Connections	Terminates suspicious or malicious network connections by sending reset packets.	Stopping brute-force attacks, port scanning, session hijacking.
Blocking IP Addresses (Blacklisting)	Blocks future traffic from specific IP addresses or networks.	Preventing repeated attacks from known malicious IPs, botnets.
Rate Limiting (Throttling)	Limits the rate of certain types of traffic to mitigate flooding or brute-force attacks.	Mitigating DDoS attacks, brute-force login attempts.
Traffic Rerouting (Honeypots)	Redirects malicious traffic to honeypots or controlled environments.	Gathering attack intelligence while protecting critical systems.
Modifying Attack Payloads	Alters or neutralizes parts of malicious payloads before allowing them through.	Preventing buffer overflow attacks or data corruption while allowing legitimate

NETWORK SEGMENTATION

- The typical network design is based on the concept of "internal trust”
  - The world is divided between what is "external" to the network and what is “internal."
  - Everything that is "internal" is considered trustworthy (not a threat).
  - The transfer of data/processes from the "external" to the "internal" is only possible through controlled checkpoints.
- Limitations of the "border defense" approach
  - Protecting the boundary is complex, and mistakes are easy to make.
  - Today's networks have "blurred" boundaries.
  - If an attacker breaches the barrier, nothing can stop them.

ZERO TRUST

- What is Zero Trust?
  - A security model that assumes no user or device should be trusted by default, even if they are "inside" the network perimeter.
  - The approach operates on the principle of “never trust, always verify”.
- Why Zero Trust?
  - Traditional “border defense” security assumes all internal entities are trustworthy, which is inadequate for modern network environments.
  - Designed for today's cloud-centric, hybrid, and remote work models.

ZERO TRUST

Key principles:

- **Verify Explicitly** - Continuously validate access using all available data points (e.g., identity, location, device health).
- **Use Least Privilege Access** - Restrict user permissions to the minimum necessary, reducing potential damage if credentials are compromised.
- **Assume Breach** - Design the network to contain potential breaches and minimize impact.

ZERO TRUST

Key components of a zero trust architecture:

- **Identity and Access Management (IAM)**: Manages user identities and enforces authentication and authorization.
- **Device Security**: Monitors device health and ensures only compliant devices can access resources.
- **Network Segmentation**: Breaks the network into smaller zones, containing breaches and limiting lateral movement.
- **Data Protection**: Secures sensitive data and enforces encryption, ensuring data privacy and compliance.
- **Continuous Monitoring and Analytics**: Tracks user and device behavior for any anomalies.

ZERO TRUST

Benefits:

- **Enhanced Security**: Limits access and minimizes the impact of breaches.
- **Reduced Attack Surface**: No blanket trust within the network.
- **Supports Remote Work and Cloud Services**: Designed for modern, distributed work environments.
- **Compliance and Data Privacy**: Meets regulatory requirements with detailed access controls and monitoring.

NETWORK SEGMENTATION

What is network segmentation?

- A security strategy that divides a network into smaller, isolated protection domains.
- Requires the implementation of controls on the borders that link each pair of network segments.

Advantages

- Hampers the possibility for the attacker to move freely in the network.
- Reduces the attack surface and limits potential damage.
- Allows more granular monitoring and management of traffic.
- Helps meet regulatory requirements by restricting access to sensitive information.

NETWORK SEGMENTATION

Physical segmentation

- Works at the hardware level. Cut the network in physically separated chunks
- Place a firewall between any two network segments that need to transfer data

+ It is as secure as the rules defined on the firewalls

+ Network traffic cannot cross the physical boundaries of the networks (e.g., air-gapped networks and data diodes)

- Many rules to define -> many errors

- Proliferation of network devices

- Inflexible design

NETWORK SEGMENTATION

Logical segmentation

- Works at the software level. Logically cut the network through software defined boundaries
- Place a firewall between any two network segments that need to transfer data

+ As secure as HW segmentation in practice

+ More flexible than physical segmentation

+ Allows for dynamic control

- Still many rules to define, but in a centralised fashion

- Software vulnerabilities may break security guarantees

NETWORK SEGMENTATION

Microsegmentation

- Fine-grained approach, applying segmentation at the application or workload level
- Controls traffic between individual workloads to limit lateral movement

+ Best option for implementing zero-trust architectures

+ Maximum flexibility

+ Support for Hybrid and Cloud Environments

- Complex policy management

- Overhead and scalability

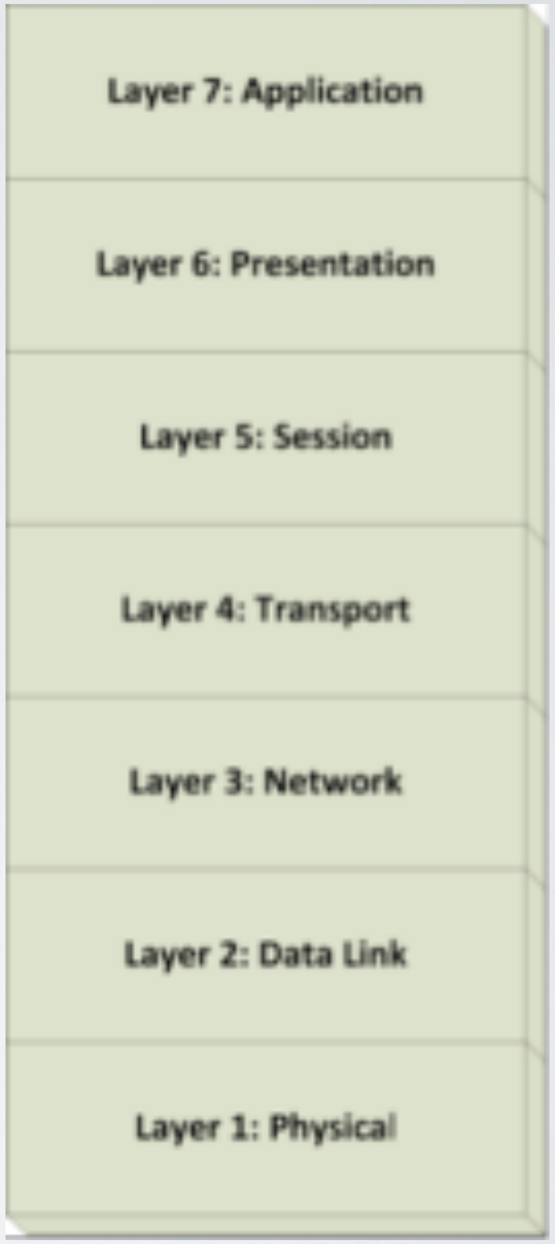
NETWORK SEGMENTATION

Microsegmentation

- Approaches to microsegmentation
  - Network-Based Microsegmentation: Uses IP addresses or subnets to isolate workloads.
  - Application-Based Microsegmentation: Policies are enforced based on application-level identifiers, allowing control and alignment with business logic.
  - User-Based Microsegmentation: Controls access at the user level by assigning access rules based on user identity and role.
  - Process-Based Microsegmentation: Policies are based on specific processes within workloads.

VLAN

- Implements logical segmentation through network devices
  - Works at OSI level 2
  - Implemented by 99.9% of COTS network switches
- Logical multiplexing of several broadcast domains on a single network infrastructure



Layer 7: Application

Layer 6: Presentation

Layer 5: Session

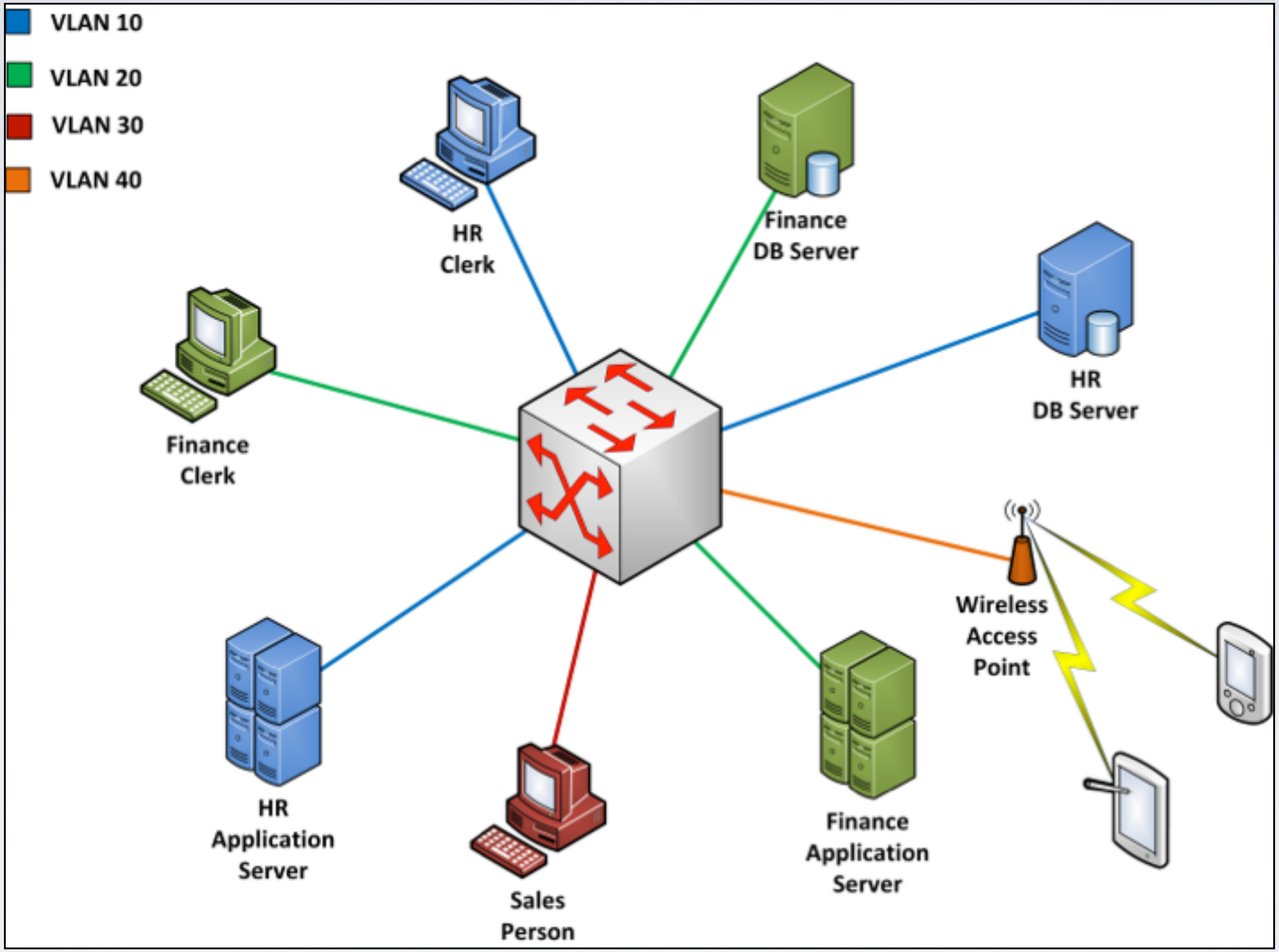
Layer 4: Transport

Layer 3: Network

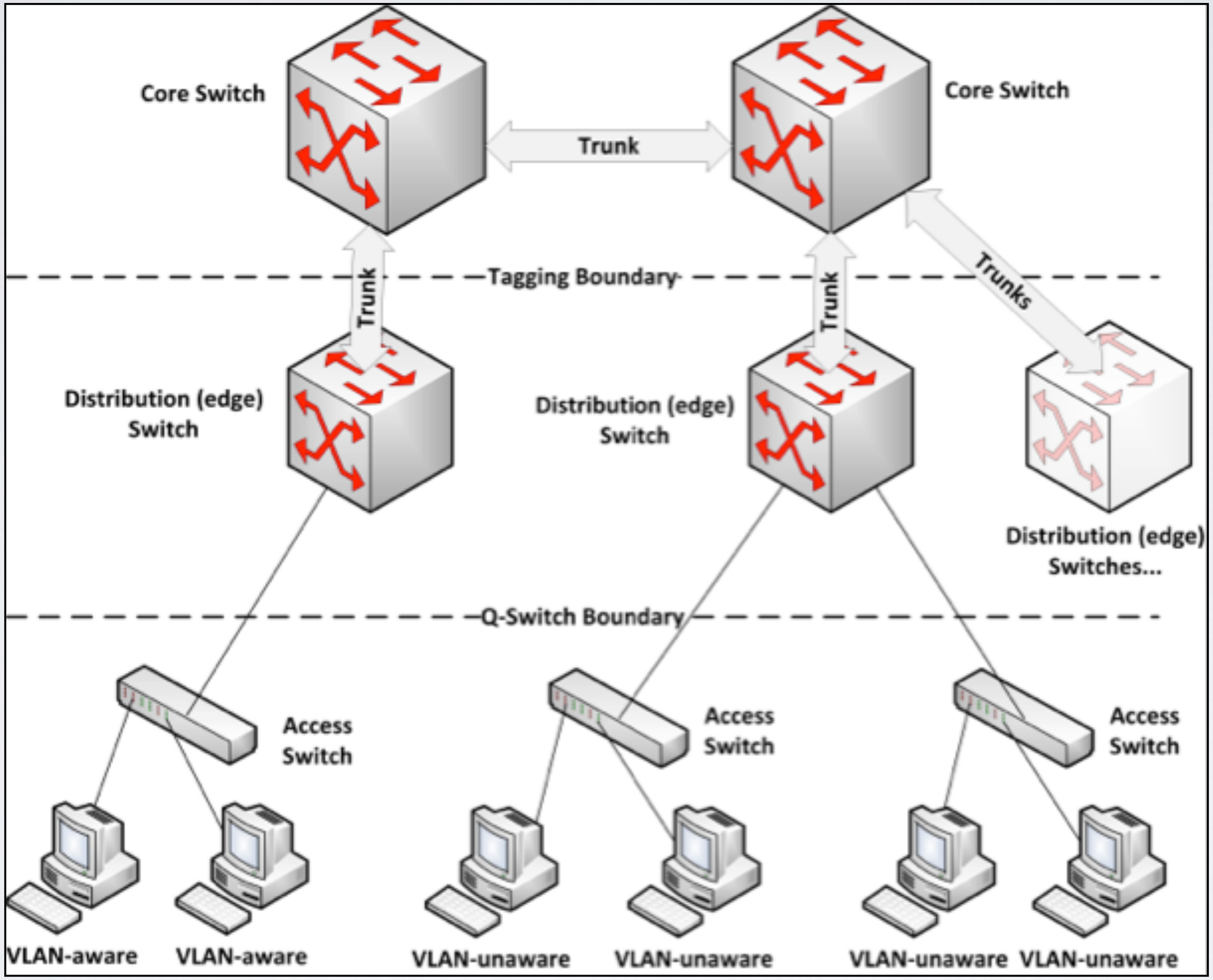
Layer 2: Data Link

Layer 1: Physical

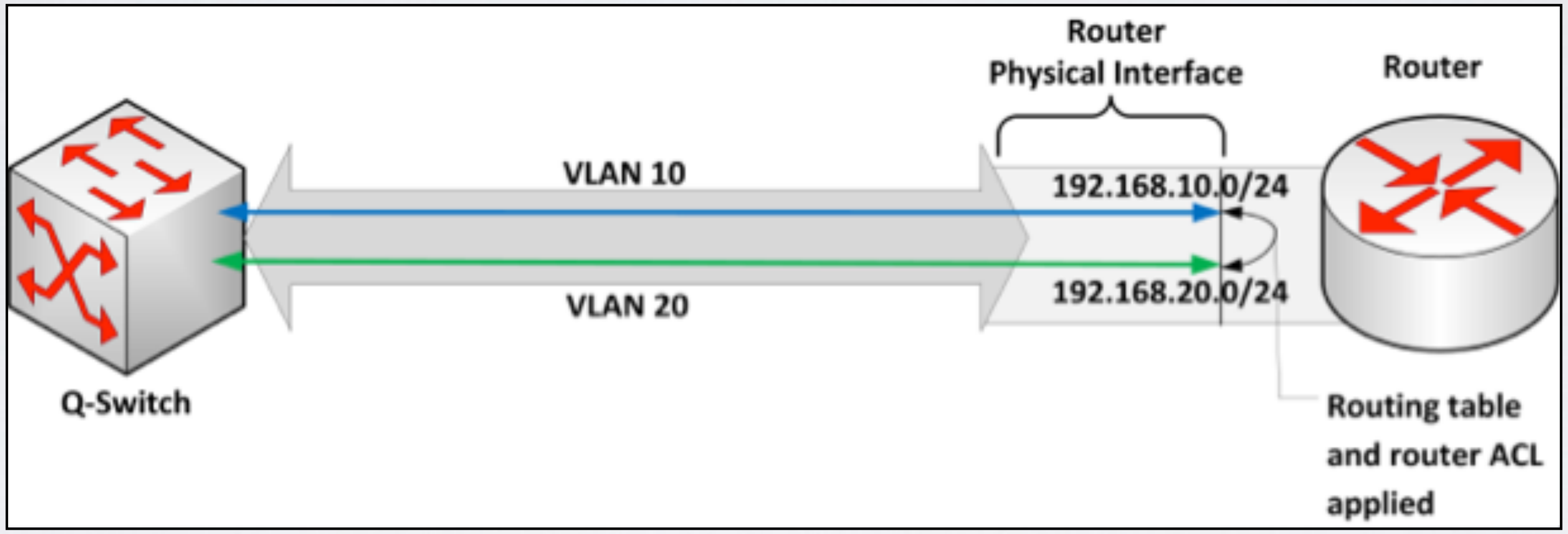
VLAN


🟦 VLAN 10
🟩 VLAN 20
🟥 VLAN 30
🟧 VLAN 40
HR Clerk
Finance DB Server
HR DB Server
Finance Clerk
Wireless Access Point
HR Application Server
Sales Person
Finance Application Server

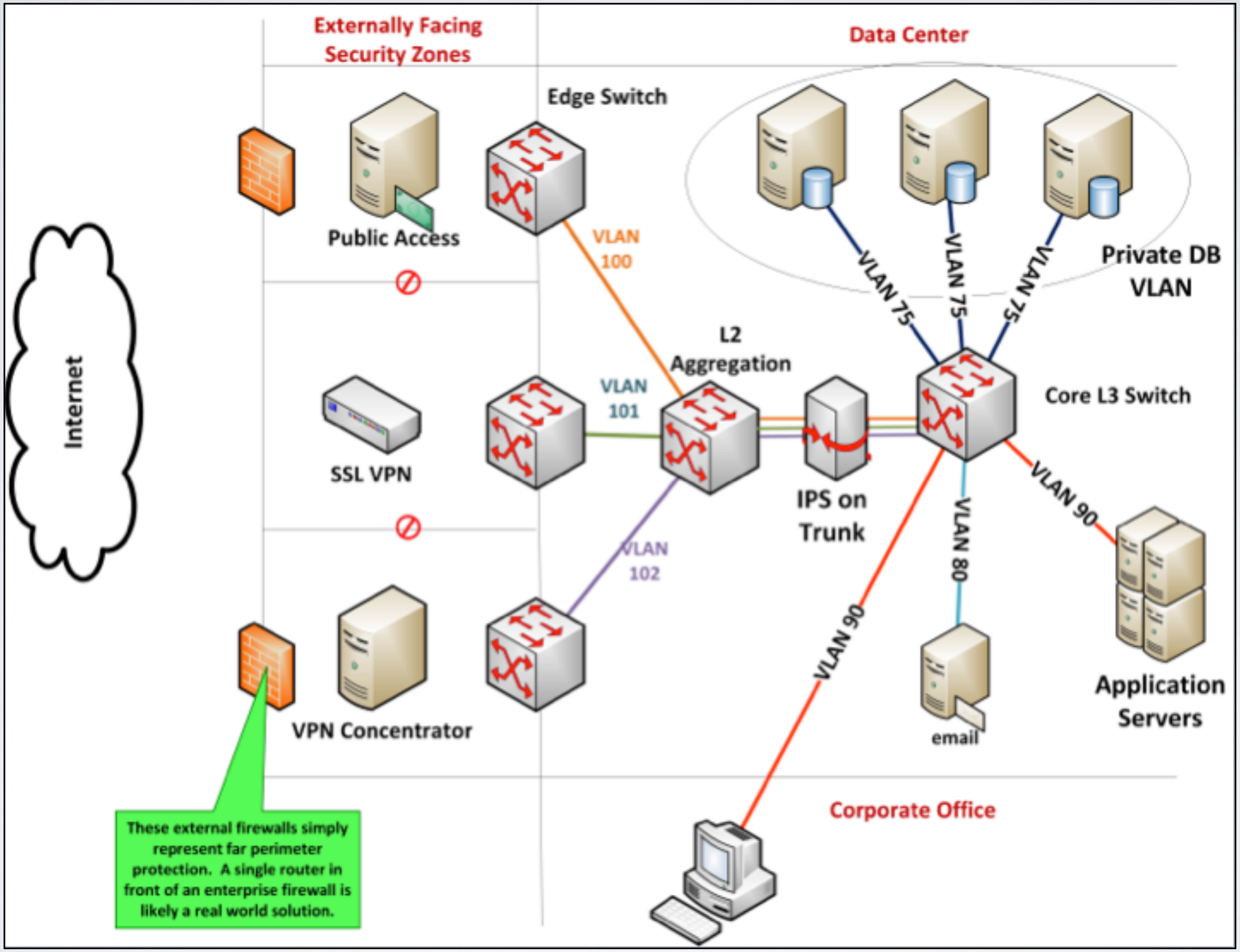
VLAN


Core Switch
Trunk
Core Switch
Tagging Boundary
Trunk
Trunk
Trunks
Distribution (edge) Switch
Distribution (edge) Switch
Distribution (edge) Switches...
Q-Switch Boundary
Access Switch
Access Switch
Access Switch
VLAN-aware
VLAN-aware
VLAN-unaware
VLAN-unaware
VLAN-unaware
VLAN-unaware

VLAN

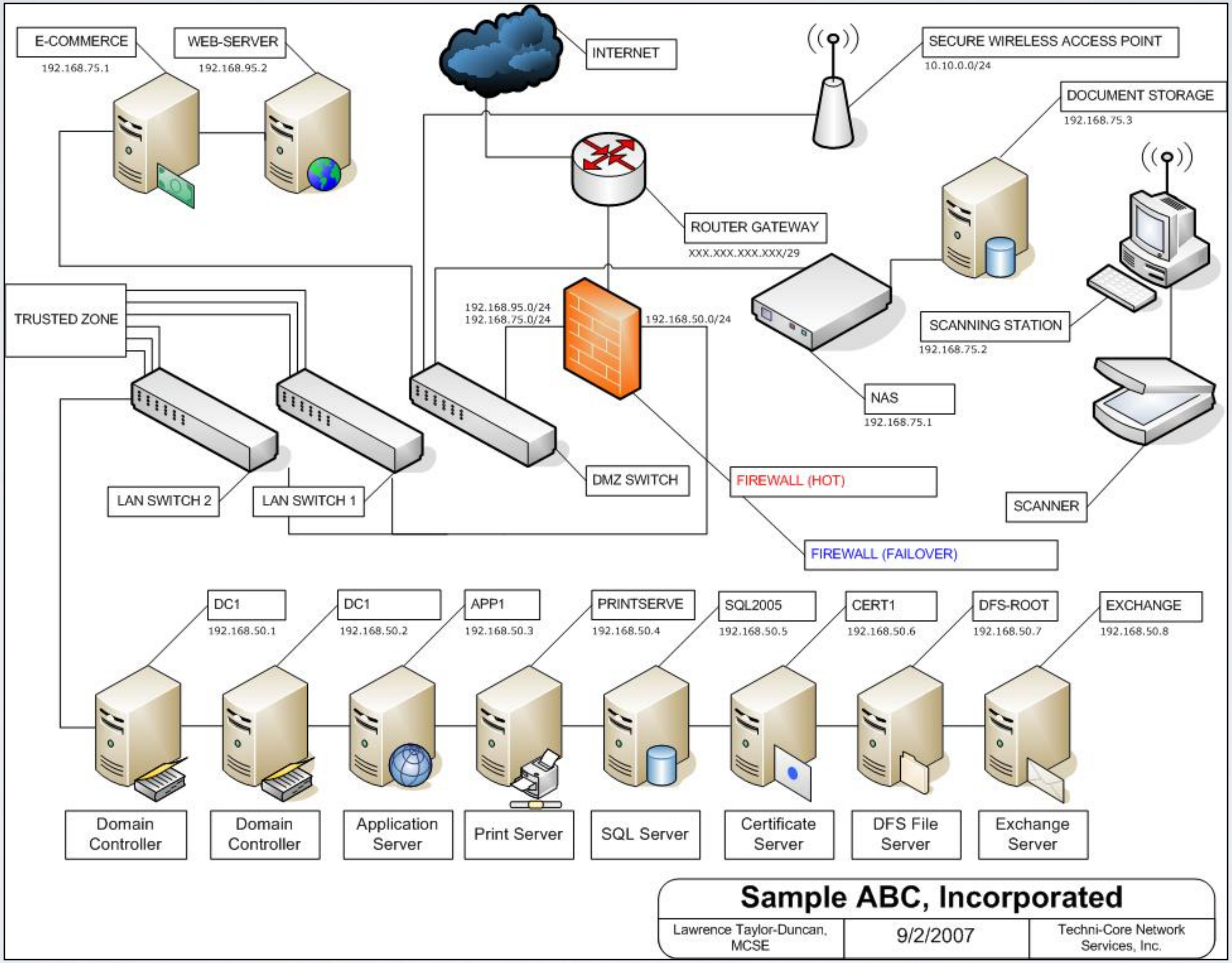

Router
Physical Interface
Router
VLAN 10
192.168.10.0/24
192.168.20.0/24
VLAN 20
Q-Switch
Routing table
and router ACL
applied

NETWORK SEGMENTATION

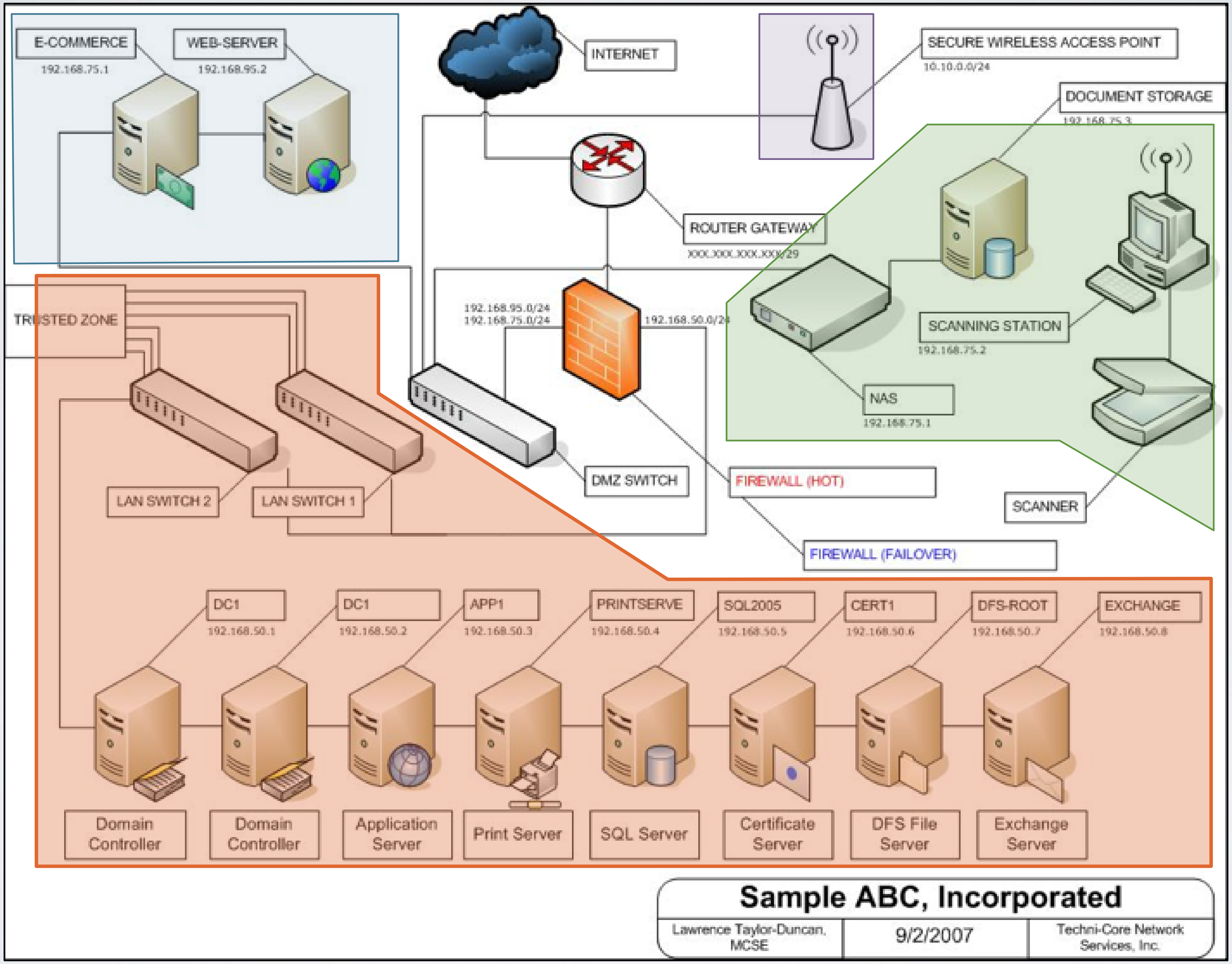


These external firewalls simply represent far perimeter protection. A single router in front of an enterprise firewall is likely a real world solution.

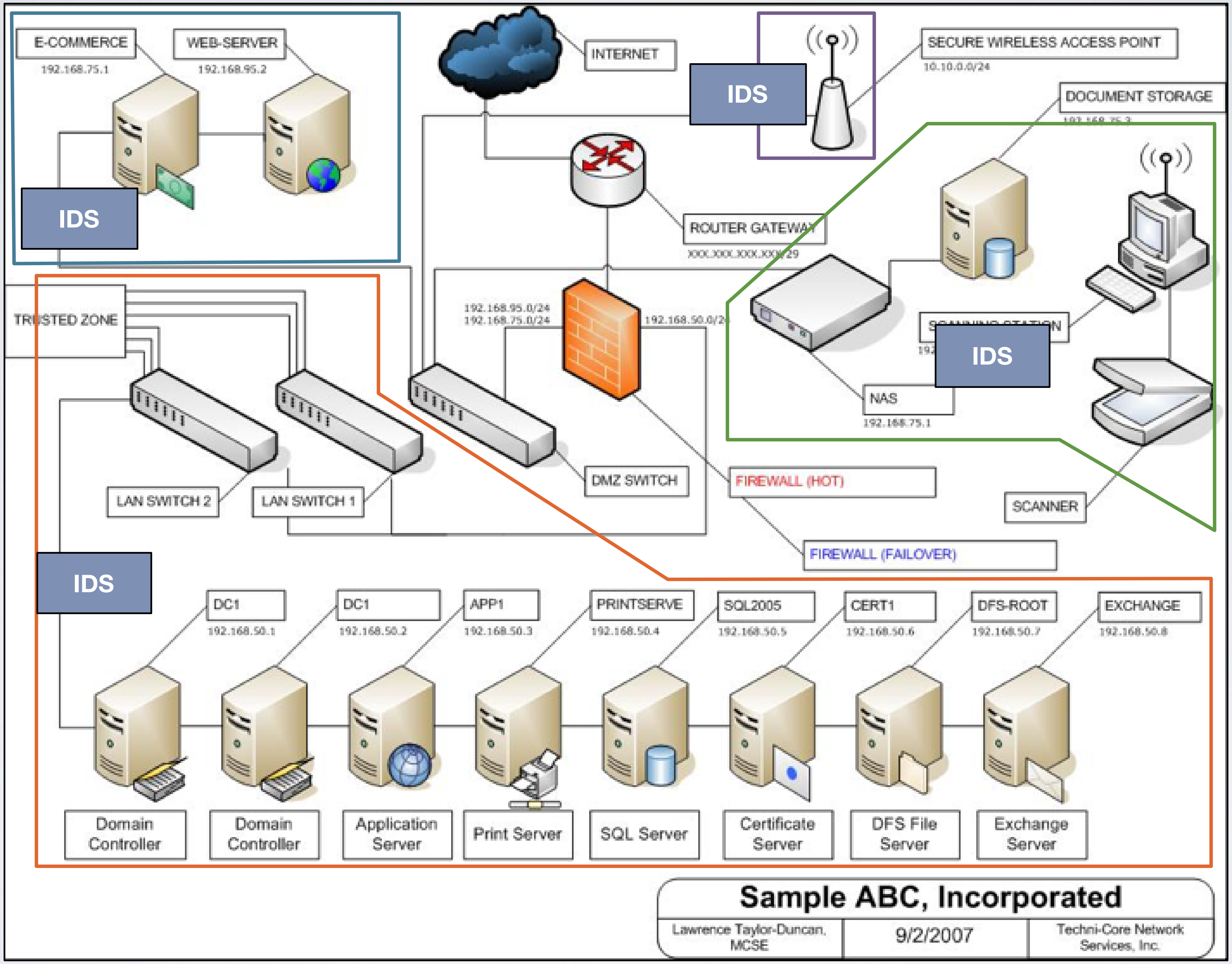
SIEM


E-COMMERCE
192.168.75.1
WEB-SERVER
192.168.95.2
INTERNET
SECURE WIRELESS ACCESS POINT
10.10.0.0/24
DOCUMENT STORAGE
192.168.75.3
ROUTER GATEWAY
XXX.XXX.XXX.XXX/29
TRUSTED ZONE
192.168.95.0/24
192.168.75.0/24
192.168.50.0/24
SCANNING STATION
192.168.75.2
NAS
192.168.75.1
LAN SWITCH 2
LAN SWITCH 1
DMZ SWITCH
FIREWALL (HOT)
FIREWALL (FAILOVER)
SCANNER
DC1
192.168.50.1
DC1
192.168.50.2
APP1
192.168.50.3
PRINTSERVE
192.168.50.4
SQL2005
192.168.50.5
CERT1
192.168.50.6
DFS-ROOT
192.168.50.7
EXCHANGE
192.168.50.8
Domain Controller
Domain Controller
Application Server
Print Server
SQL Server
Certificate Server
DFS File Server
Exchange Server
Sample ABC, Incorporated
Lawrence Taylor-Duncan, MCSE
9/2/2007
Techni-Core Network Services, Inc.

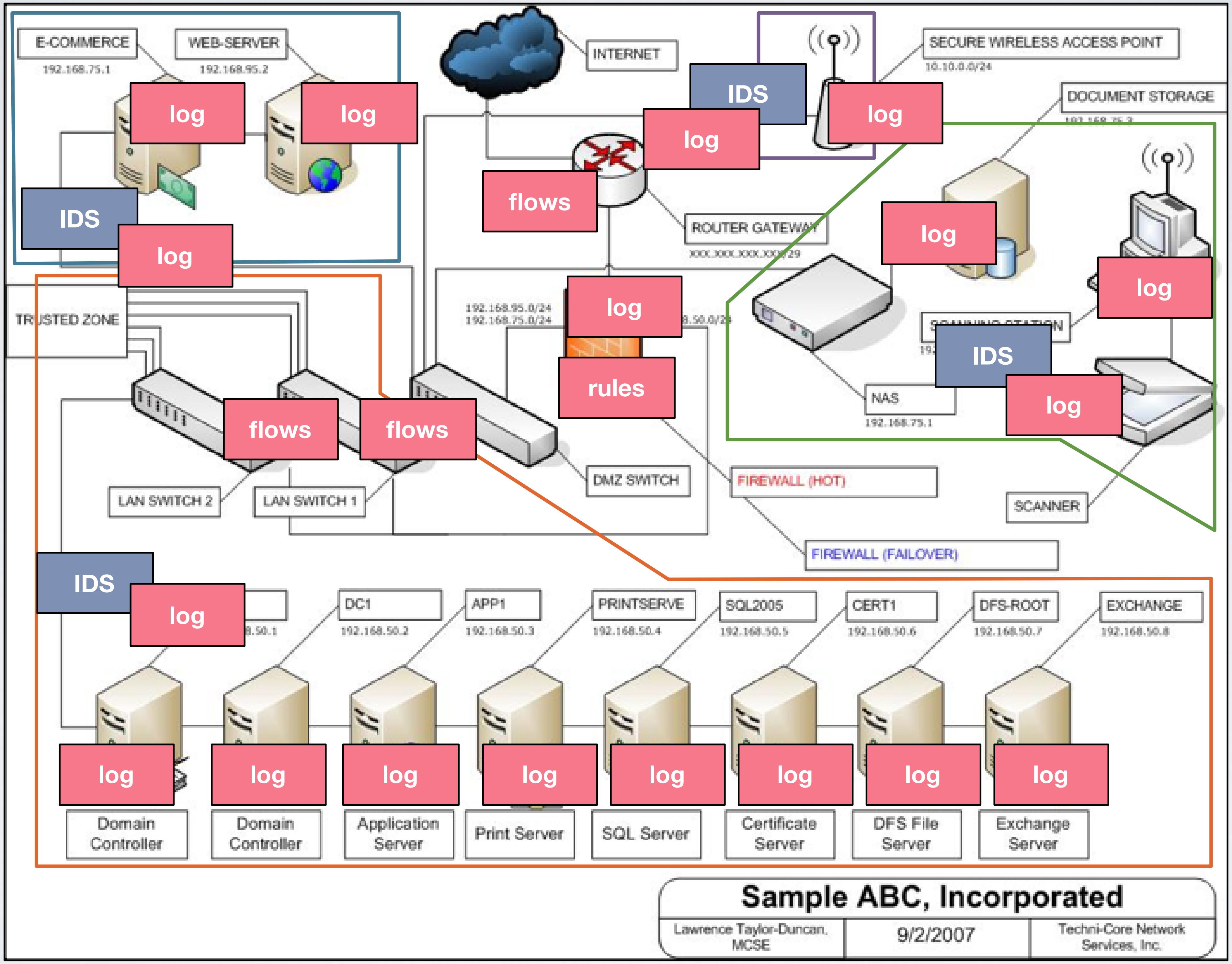
SIEM


E-COMMERCE
192.168.75.1
WEB-SERVER
192.168.95.2
INTERNET
SECURE WIRELESS ACCESS POINT
10.10.0.0/24
DOCUMENT STORAGE
192.168.75.3
ROUTER GATEWAY
XXX.XXX.XXX.XXX/29
TRUSTED ZONE
192.168.95.0/24
192.168.75.0/24
192.168.50.0/24
SCANNING STATION
192.168.75.2
NAS
192.168.75.1
LAN SWITCH 2
LAN SWITCH 1
DMZ SWITCH
FIREWALL (HOT)
SCANNER
FIREWALL (FAILOVER)
DC1
192.168.50.1
DC1
192.168.50.2
APP1
192.168.50.3
PRINTSERVE
192.168.50.4
SQL2005
192.168.50.5
CERT1
192.168.50.6
DFS-ROOT
192.168.50.7
EXCHANGE
192.168.50.8
Domain Controller
Domain Controller
Application Server
Print Server
SQL Server
Certificate Server
DFS File Server
Exchange Server
Sample ABC, Incorporated
Lawrence Taylor-Duncan, MCSE
9/2/2007
Techni-Core Network Services, Inc.

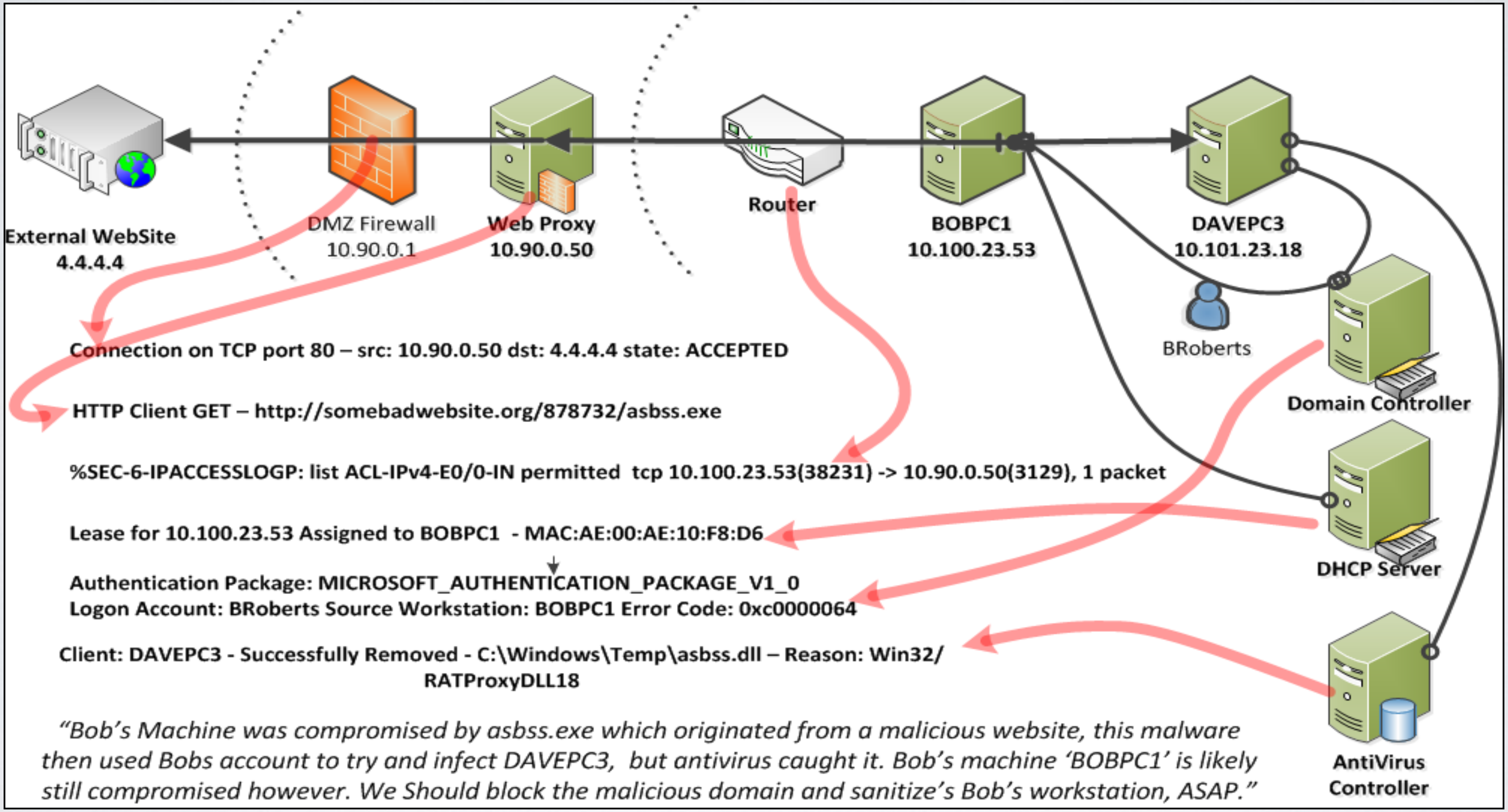
SIEM


E-COMMERCE
192.168.75.1
WEB-SERVER
192.168.95.2
IDS
INTERNET
IDS
SECURE WIRELESS ACCESS POINT
10.10.0.0/24
DOCUMENT STORAGE
192.168.75.3
ROUTER GATEWAY
XXX.XXX.XXX.XXX/29
TRUSTED ZONE
192.168.95.0/24
192.168.75.0/24
192.168.50.0/24
SCANNING STATION
192
IDS
NAS
192.168.75.1
LAN SWITCH 2
LAN SWITCH 1
DMZ SWITCH
FIREWALL (HOT)
SCANNER
FIREWALL (FAILOVER)
IDS
DC1
192.168.50.1
DC1
192.168.50.2
APP1
192.168.50.3
PRINTSERVE
192.168.50.4
SQL2005
192.168.50.5
CERT1
192.168.50.6
DFS-ROOT
192.168.50.7
EXCHANGE
192.168.50.8
Domain Controller
Domain Controller
Application Server
Print Server
SQL Server
Certificate Server
DFS File Server
Exchange Server
Sample ABC, Incorporated
Lawrence Taylor-Duncan, MCSE
9/2/2007
Techni-Core Network Services, Inc.

SIEM


E-COMMERCE
192.168.75.1
WEB-SERVER
192.168.95.2
log
log
IDS
log
INTERNET
IDS
log
log
flows
SECURE WIRELESS ACCESS POINT
10.10.0.0/24
DOCUMENT STORAGE
ROUTER GATEWAY
XXX.XXX.XXX.XXX/29
log
log
TRUSTED ZONE
192.168.95.0/24
192.168.75.0/24
log
8.50.0/24
rules
SCANNING STATION
IDS
NAS
192.168.75.1
log
flows
flows
LAN SWITCH 2
LAN SWITCH 1
DMZ SWITCH
FIREWALL (HOT)
SCANNER
FIREWALL (FAILOVER)
IDS
log
8.50.1
DC1
192.168.50.2
APP1
192.168.50.3
PRINTSERVE
192.168.50.4
SQL2005
192.168.50.5
CERT1
192.168.50.6
DFS-ROOT
192.168.50.7
EXCHANGE
192.168.50.8
log
log
log
log
log
log
log
log
Domain Controller
Domain Controller
Application Server
Print Server
SQL Server
Certificate Server
DFS File Server
Exchange Server
Sample ABC, Incorporated
Lawrence Taylor-Duncan, MCSE
9/2/2007
Techni-Core Network Services, Inc.

SIEM



```
Connection on TCP port 80 – src: 10.90.0.50 dst: 4.4.4.4 state: ACCEPTED

HTTP Client GET – http://somebadwebsite.org/878732/asbss.exe

%SEC-6-IPACCESSLOGP: list ACL-IPv4-E0/0-IN permitted  tcp 10.100.23.53(38231) -> 10.90.0.50(3129), 1 packet

Lease for 10.100.23.53 Assigned to BOBPC1  - MAC:AE:00:AE:10:F8:D6

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: BRoberts Source Workstation: BOBPC1 Error Code: 0xc0000064

Client: DAVEPC3 - Successfully Removed - C:\Windows\Temp\asbss.dll – Reason: Win32/
                                  RATProxyDLL18
```

"Bob's Machine was compromised by asbss.exe which originated from a malicious website, this malware then used Bobs account to try and infect DAVEPC3, but antivirus caught it. Bob's machine 'BOBPC1' is likely still compromised however. We Should block the malicious domain and sanitize's Bob's workstation, ASAP."

Source: AlienVault

SIEM

A Security Information and Event Management (SIEM) system aims to provide system administrators with a unified, comprehensive, and consistent view of the security of all IT systems:

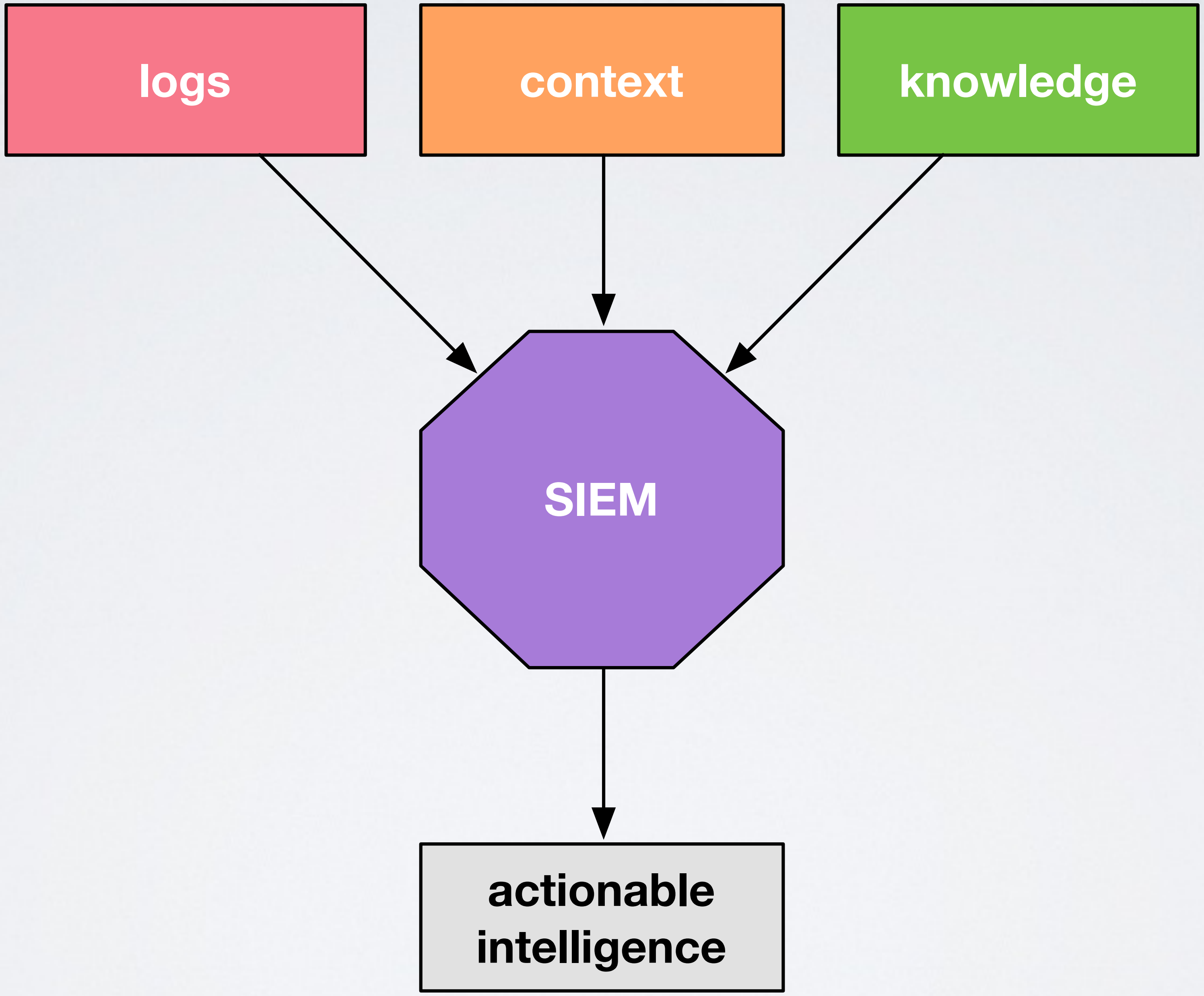
- it is a layer of management and analysis positioned above existing security systems and controls.
- It connects and unifies information contained in pre-existing systems, allowing it to be analyzed and correlated from a single management interface.
- The ultimate goal of a SIEM is to "distill" low-level information into more abstract events, interpret them, and present them in a prioritized and simplified manner to those responsible for managing system security, enabling them to act consistently.

SIEM

Goals:

- Unified Security Visibility - SIEM collects and aggregates logs and events from multiple sources, providing a comprehensive view of security across the organization.
- Incident Detection and Response - Helps detect, prioritize, and respond to security threats in real time.
- Compliance and Reporting - Assists with regulatory requirements by providing logs and reports.

SIEM



logs

context

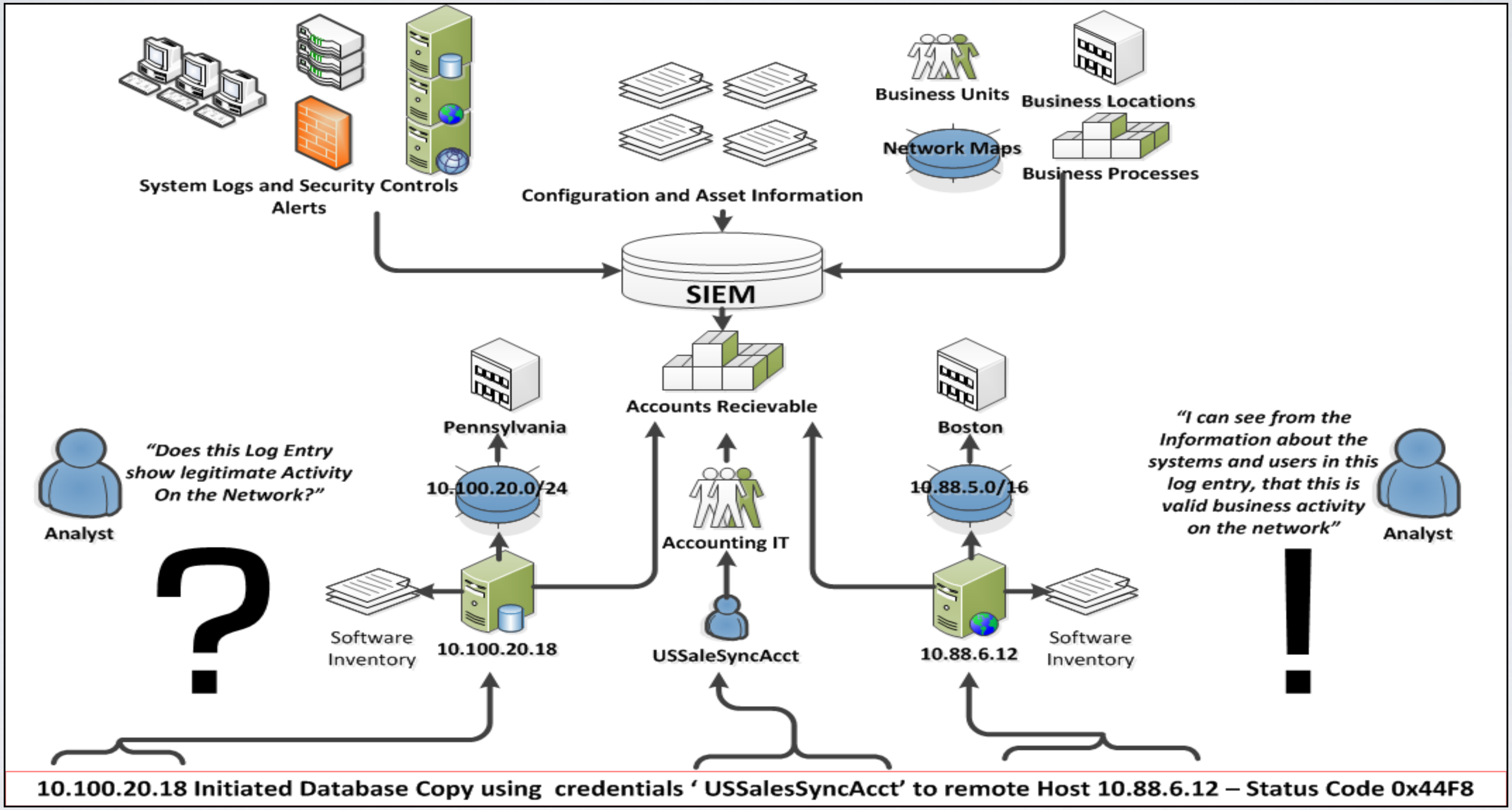
knowledge

SIEM

actionable intelligence

SIEM

- Example



System Logs and Security Controls Alerts
Configuration and Asset Information
Business Units
Business Locations
Network Maps
Business Processes
SIEM
Accounts Recievable
Pennsylvania
Boston
"Does this Log Entry show legitimate Activity On the Network?"
Analyst
10.100.20.0/24
Accounting IT
10.88.5.0/16
"I can see from the Information about the systems and users in this log entry, that this is valid business activity on the network"
Analyst
?
Software Inventory
10.100.20.18
USSaleSyncAcct
10.88.6.12
Software Inventory
!
10.100.20.18 Initiated Database Copy using credentials ' USSalesSyncAcct' to remote Host 10.88.6.12 – Status Code 0x44F8

Source: AlienVault

BIBLIOGRAPHY

- NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS), 2007
- A. Lazarevic, V. Kumar and J. Srivastava, Intrusion Detection: a Survey. In V. Kumar et al. "Managing Cyber Threats: Issues, Approaches and Challenges", Springer, 2005.
- D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford and N. Weaver, The Spread of the Sapphire/Slammer Worm, http://www.cs.berkeley.edu/~nweaver/sapphire/, 2003.
- D. Powell and R. Stroud, Conceptual Model and Architecture, Deliverable D2, Project MAFTIA IST-1999-11583, IBM Zurich Research Laboratory Research Report RZ 3377, Nov. 2001.