Cloud, IoT and Enterprise Security

BITS Pilani

Pilani Campus

Nishit Narang
WILPD-CSIS
(nishit.narang@pilani.bits-pilani.ac.in)

innovate achieve lead

BITS Pilani

Pilani Campus

<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 4: Enterprise Security – Securing the Network & Systems

Enterprise = Network + Systems + Data + Humans + …

Source Disclaimer: Content for many of the slides is from the course Textbook(s). Refer Course Handout for list of Textbooks.

Enterprise Security

Securing the Network (Contd.)

IDS/IPS

- Intrusion detection and prevention technology has remained a mainstay at the network perimeter
  - While several firewall technologies are integrating intrusion prevention into their offerings, there has not been a complete shift to this implementation
- Intrusion detection is a method for detecting an attack but taking no action
  - this has been abandoned at the network perimeter when a breach is undesirable
  - it seems to still have a significant implementation in the internal network server segments to passively observe the behaviors of internal network users
  - has all the detection logic of intrusion prevention but without the ability to actively mitigate a threat
- Intrusion prevention is similar to intrusion detection, but has the capability to disrupt and mitigate malicious traffic by blocking and other methods
  - Many IPS devices have purposefully built denial of service mitigation technology
  - can be deployed at the network perimeter
  - should also be considered for implementation in the internal network to protect the most critical assets within the organization
- As the attacks have become advanced, there is debate on the overall advantage of the IDS/IPS
  - However, a defense in-depth strategy is best implemented by including IDS/IPS as an essential network protection mechanism

IDS/IPS: Detection Methods

- IDS/IPS devices use a combination of three methods to detect and mitigate attacks
  - behavior, anomaly, and signature
  - initial IDS/IPS systems were specialized in one method or another
  - Today, it is rare to find a detection method without the others
  - Also because attacks are not always as simple as protocol misuse or a known Trojan signature

IDS/IPS: Behavior Analysis

- Behavioral analysis takes some intelligence from the platform to first gain an understanding of how the network "normally" operates
  - what systems communicate with other systems, how they communicate, and how much
- Any deviation from this baseline becomes an outlier and triggers the IDS/IPS based on this behavioral deviation
  - Example, if a system is compromised, the connection rates exceed what is common for the system
- The primary caveat with this approach is the mistake of baselining malicious traffic within standard network traffic as "normal“
  - This common and almost unavoidable mistake requires the other detection methods to bring real value

IDS/IPS: Anomaly Detection

- Malware writers often attempt to masquerade their application as a legitimate application
  - this method is commonly employed by chat clients, bit torrent, and other P2P applications
  - Such apps are typically not permitted, so developers have written the applications to look harmless
- Anomaly detection at the network perimeter can be extremely effective in analyzing inbound HTTP requests where the protocol is correct, but there has been some manipulation to the packet
- Nonetheless, understanding the RFC specifications for every protocol is a daunting task!!

IDS/IPS: Signature-based Detection

- A consistent method to detect known malicious attacks
- IDS/IPS looks for known patterns in the packets being inspected
- When a signature or pattern match is found, a predetermined action is taken
- Detects the most common, generic attacks
- Ineffective for the more sophisticated attacks
- Another annoyance with this method is the high rate of false positives

With a majority of attacks targeted at the network being Distributed Denial of Service (DDoS) and SQL injection (SQLi), signature-based IPS can be very effective in mitigating these attacks and continue to provide value at the network perimeter

APT Detection and Mitigation

- APT = **Advanced Persistent Threat**
- Are complicated and well disguised malware
  - use complicated zero-day vulnerabilities, multi-encoded malicious payloads, encryption, obfuscation, and clever masquerading techniques
- APT mitigation solutions work by providing a safe environment
  - usually virtualized instances or sandboxes of operating systems are employed, where malicious software can run and infect the operating system
  - The tool then analyzes everything the malicious software did, and decodes the payload to identify the threat and create a "signature" to mitigate further exploitation
  - Technology in this space is new and relatively less known
- Some tools are appliance-based. The decoding and analysis happens on the box. Other vendors provide the service in the cloud

Several manufacturers in the IDS/IPS and NGFW technology areas have made significant progress in providing APT detection and mitigation, both on the box and in the cloud

Securing Network Services (NS)

- Enterprises provide and leverage Internet services such as DNS, e-mail, and file transfer
  - The latest malware threats utilize these common services in order to redirect internal hosts to Internet destinations under the control of the malware writers
  - However, with correctly implemented architecture, this scenario would mostly be a mute point, and with additional security mechanisms, a rare occurrence
- In the next few slides, we will discuss the security implementations for DNS, Email, File Transfers and Websites

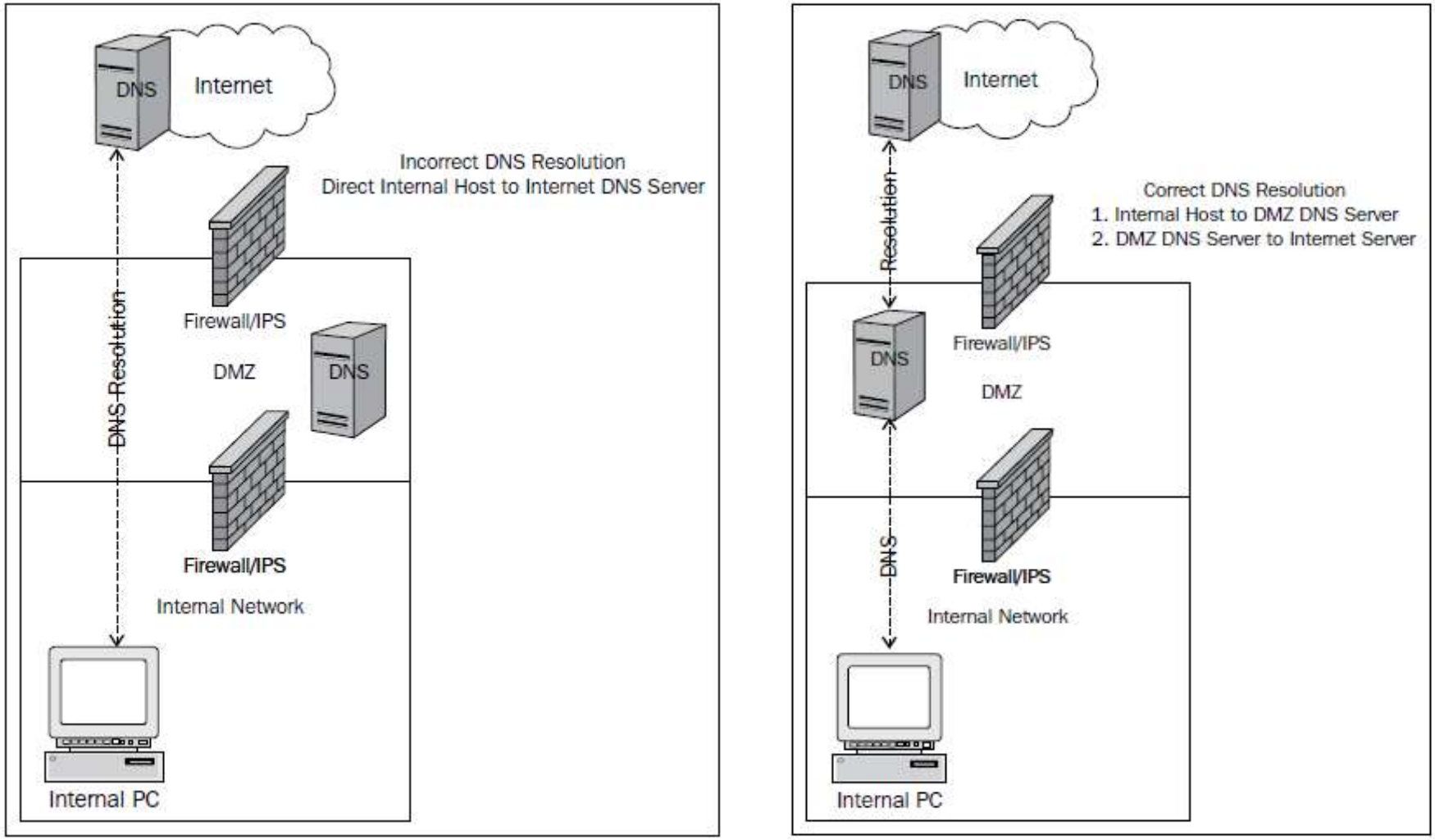
NS: DNS Service Security

- DNS provides a mapping of an IP address to a fully qualified domain name
- A system can be directed anywhere on the Internet with DNS, so the authenticity of the source of this information is critical
- This is where **DNS Security Extensions** (**DNSSEC**) come into play
  - provide authenticity for DNS resolver data
  - DNS data cannot be forged and attacks like DNS poisoning, where erroneous DNS is injected into DNS and propagated, resulting in pointing hosts to the wrong system on the Internet is mitigated. This is a common method used by malware writers and in phishing attacks
- Another area of security in regards to DNS implementation are DNS zone transfers
  - mechanism used in DNS to provide other DNS servers with what domains the DNS server is responsible for and all the details available for each record in the zone

NS: DNS Resolution

- DNS resolution can make for easy exploitation if there is no control on where the mapping information is obtained
  - This has been the main method used by the Zeus botnet
  - Hosts are pointed to maliciously controlled Internet servers by manipulating DNS information
  - The method also relies on compromised or specifically built DNS servers on the Internet, allowing malware writers to make up their own, unique and sometimes inconspicuous domain names

NS: DNS Resolution (2)



Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

NS: DNS Zone Transfer

- A DNS zone transfer should be limited to only trusted partners and limited to only zones that need to be transferred
  - An enterprise may have several domain names for various services they provide to business partners and employees that are not "known" by the general public
    - Example, office-specific records, a VPN URL, SIP address for VoIP, etc
  - While the fact remains that if the service is available on the Internet, it can be found, a simple zone transfer reduces the discovery process significantly
- There may be internal and external DNS implementations with records specific to the network areas they service
  - the internal DNS server may have records for all internal hosts and services, while a DNS server in the DMZ may only have records for DMZ services
  - it is critical to keep the records uncontaminated from other zones
  - Specifically, TXT may give too much information that can be used in a malicious manner against the enterprise

NS: DNSSEC

- Most prevalent DNS attack is **DNS poisoning**, where the DNS information on the Internet is poisoned with false information, allowing attackers to direct clients to whatever IP address they desire
- Security extensions have been added to the DNS protocol by the **Internet Engineering Task Force** (**IETF**) **DNS Security** (**DNSSEC**) specification
  - provides security for specific information components of the DNS protocol in an effort to provide authenticity to the DNS information
- The importance of DNSSEC is that it is intended to give the recipient DNS server confidence in the source of the DNS records or resolver data that it receives

NS: Email Service Security

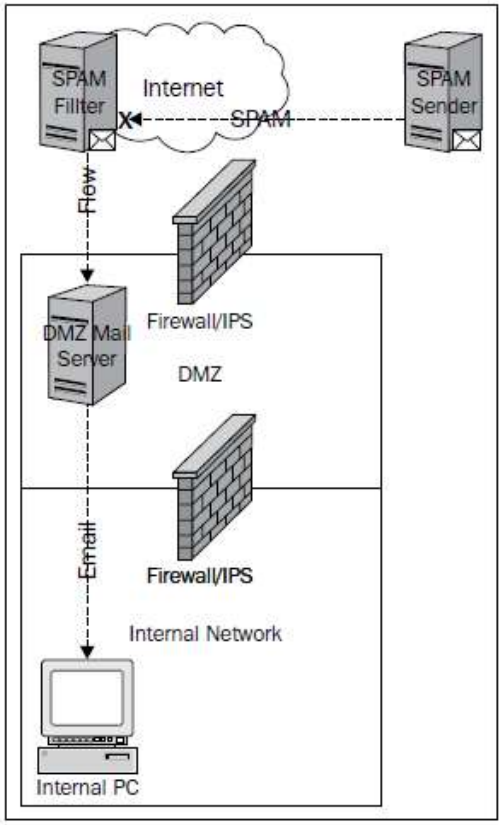
- Email service is a critical business function
- With the increased growth and acceptance of cloud-based services, e-mail is amongst the first to be leveraged
- Some enterprises have already moved their e-mail implementation to the cloud
  - + Enables lower cost and *as-a-service* implementation
  - - enterprises have lower control over email security
- The next few slides will cover common e-mail threats and present methods to secure e-mail services

NS: Spam Filtering

- E-mail is one of the most popular methods to spread malware or lead users to malware hosted on the Internet
  - Most often, this is the single intent of unwanted e-mails in the form of SPAM
  - Receiving SPAM and becoming the source of SPAM while being used as a relay are two sides to the same coin
- Methods to protect the enterprise from SPAM include cloud-based and local SPAM filtering at the network layer and host-based solutions at the client
  - A combination of these methods can prove to be most effective

NS: Spam Filtering @ Cloud

- Works by configuring the DNS **mail record** (**MX**)* to identify the service provider's e-mail servers
  - This configuration forces all e-mails destined to e-mail addresses owned by the enterprise through the SPAM solution filtering systems before forwarding to the final enterprise servers and user mailbox
  - Outbound mail from the enterprise would take the normal path to the destination as configured, to use DNS to find the destination domain email server IP address



Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

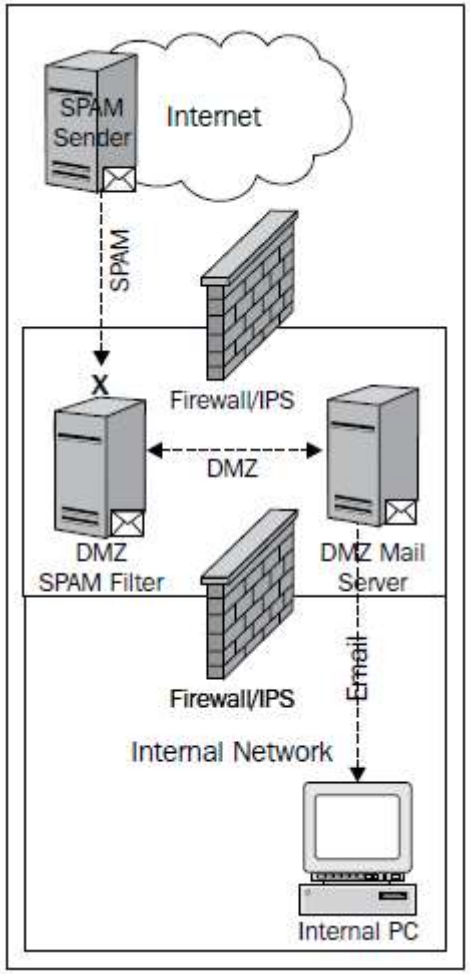
A mail exchanger record (MX record) specifies the mail server responsible for accepting email messages on behalf of a domain name. It is a resource record in the Domain Name System (DNS). It is possible to configure several MX records, typically pointing to an array of mail servers for load balancing and redundancy. Source: Wikipedia

NS: Spam Filtering @ Cloud (2)

- Pros and Cons:
  - + Zero or limited administration of the solution
  - + Reduction in Spam traffic
  - + Reduction in malware and other threats
  - - Significant cost, depending on service fee structure
  - - lack of visibility and control of filters
  - - service failure => no email or unwanted delays
- Enterprise needs to do cost-benefit analysis before taking this option
  - Cost of service
  - Implicit cost (e.g. due to loss of service, or unwanted delays)
  - Benefits (savings due to reduction in spam emails or malware threats)

NS: Local Spam Filtering

- Only an option when the enterprise is not using a web-hosted/cloud-based email solution
  - With web-based e-mail hosting, the SSL connection exists from the user's browser or e-mail client to the hosted e-mail servers
  - SSL decryption could be possible, but the overhead and privacy implications should be weighed carefully
    - Decrypting SSL by presenting a false certificate in order to snoop breaks SSL theory and is considered a *man-in-the-middle* attack
- Several solutions exist to provide SPAM filtering and e-mail encryption in one appliance
  - may play a role in the enterprise data loss prevention and secure file transfer strategies, providing more than just SPAM filtering



Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

NS: Local Spam Filtering (2)

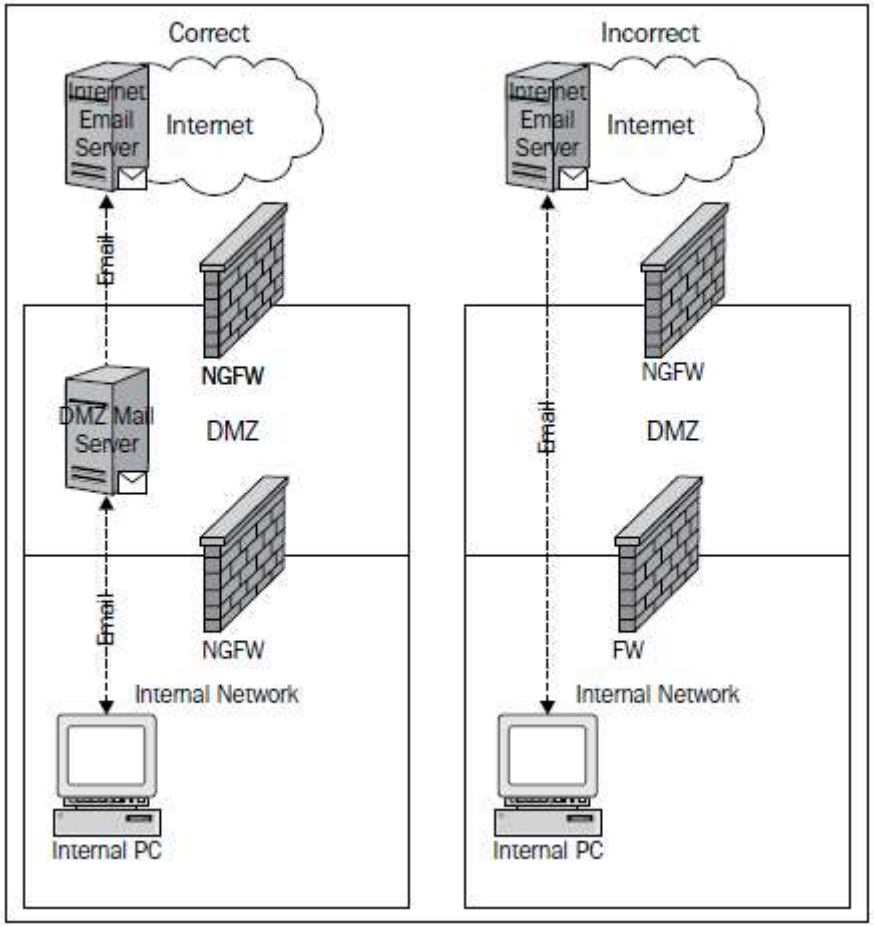
- Pros and Cons:
  - + more control over configuration of filters
  - + vendor continuously updates the appliance to include new block list updates and signatures
  - + ability to also own the DNS infrastructure that tells other e-mail systems where to send e-mail
    - In the event of appliance failure, e-mails can be routed around the failure using DNS to maintain the e-mail service
  - - Technically, a debatable solution if web-based email solution is used
- Again, an enterprise must make an assessment for operational feasibility prior to making the decision to locally detect and mitigate SPAM

NS: Spam Relaying

- Misconfiguration of the enterprise mail servers may lead to exploitation in the form of using the servers as a SPAM relay
  - method uses the server's lack of sender authentication and capability to send e-mails from domains which it does not have authority to send e-mail
- Unfortunately, this misconfiguration is common
  - Internet facing e-mail systems only authenticate for the internal mail relay
  - Internal servers for the requirement of non-human processes to send e-mails, such as the alerting mechanism on a security system
    - The internal server should still have restrictions on sending domains, to avoid the system being misused to send other spoofed e-mails

NS: Spam Relaying (2)

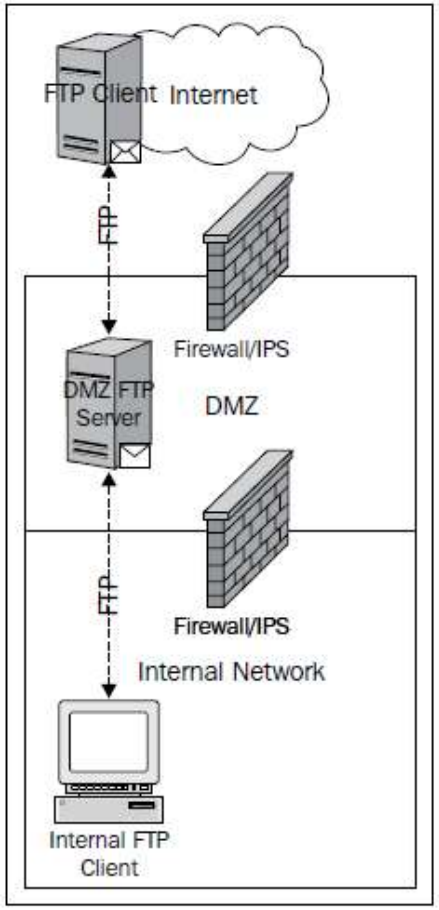
- Prevention:
  - Implement e-mail controls at the firewall to ensure that only the internal mail servers are able to directly send e-mails to the Internet
  - This method reduces the potential impact of end system malware, designed to send SPAM from inside the network
  - Some malware is specifically designed to blast e-mail SPAM from the infected system, thus getting the enterprise blocked by services such as SPAMHAUS



Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

NS: File Transfer Service

- Many times is a necessity to facilitate business operations
  - protocols and methods that are viable options include FTP, SFTP, FTPS, SSH, and SSL; many more proprietary options available too
  - migration to secure protocols has been driven primarily by security standards: PCI DSS, ISO 27001, and NIST
- It is not possible to allow uncontrolled encrypted file transfer from a user's desktop to any Internet destination
  - it would circumvent most network-based security controls
- A method to ensure secure communication and the ability to control what is transferred and to whom is to implement an intermediary transfer host
  - Solution should also require authentication to be used and the user list audited regularly, for both voluntarily and involuntarily terminated employees



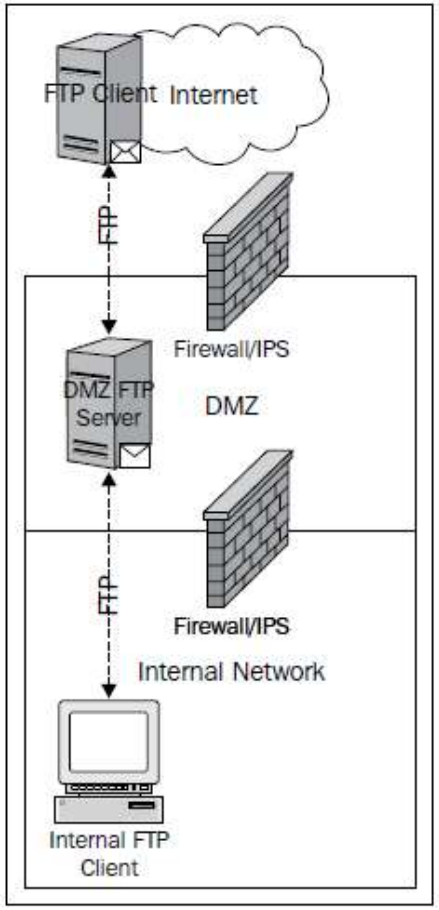
Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

NS: Secure File Transfer

- Not all enterprises that have implemented secure protocols use a secure file transfer
  - Choice by design, such as credit card authorizers, where the risk is accepted due to the overhead and complexity of managing secure communications for a high number of clients
- It can be challenging to implement a secure transfer solution, especially if not using an SSL implementation where encryption can be managed by certificates
  - In instances where SSH or SFTP is used, this can be more complicated to provide authentication and encryption

NS: File Transfer Service

- Many times is a necessity to facilitate business operations
  - protocols and methods that are viable options include FTP, SFTP, FTPS, SSH, and SSL; many more proprietary options available too
  - migration to secure protocols has been driven primarily by security standards: PCI DSS, ISO 27001, and NIST
- It is not possible to allow uncontrolled encrypted file transfer from a user's desktop to any Internet destination
  - it would circumvent most network-based security controls
- A method to ensure secure communication and the ability to control what is transferred and to whom is to implement an intermediary transfer host
  - Solution should also require authentication to be used and the user list audited regularly, for both voluntarily and involuntarily terminated employees



Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

NS: Secure File Transfer

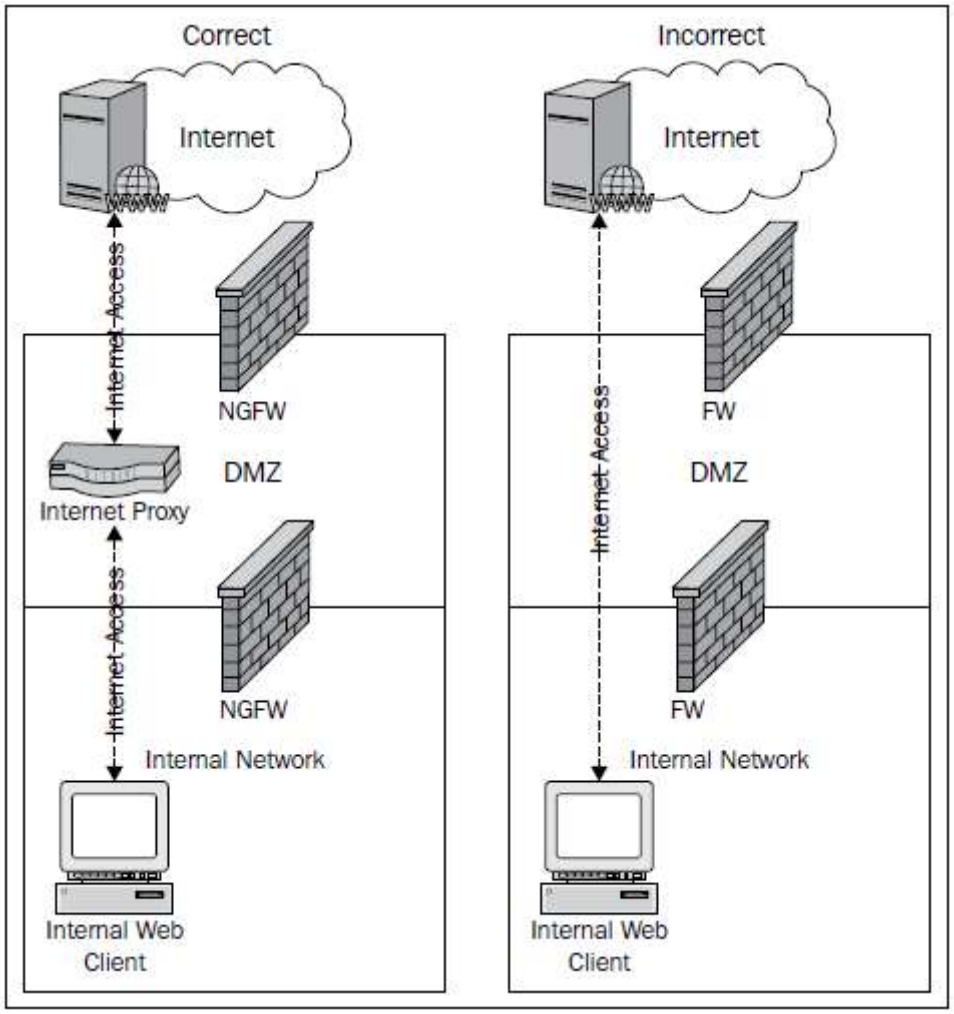
- Not all enterprises that have implemented secure protocols use a secure file transfer
  - Choice by design, such as credit card authorizers, where the risk is accepted due to the overhead and complexity of managing secure communications for a high number of clients
- It can be challenging to implement a secure transfer solution, especially if not using an SSL implementation where encryption can be managed by certificates
  - In instances where SSH or SFTP is used, this can be more complicated to provide authentication and encryption

NS: User Authentication

- For SSH, SFTP, and other such protocols, there are two methods of authentication, namely user credentials and keys
  - 1) Enterprise configures either locally or using directory services, such as Windows Active Directory for users that can access the service
    - Security implications involved:
      - For local accounts, the fact that they are locally stored on the server may leave them vulnerable to compromise
      - The system administrator will also have to manually manage user credentials on each and every system configured
      - For systems that rely on a central user directory, the implementation must be thought out to ensure that any compromise of the system does not lead to a compromise of the internal user directory
  - 2) Authentication via **Simple Public Key Infrastructure** (**SPKI**)
    - private-public key combination can be used for authenticating systems, applications, and users

NS: Securing Internet Access Service

- Internal user access to the Internet is probably deemed a more critical service than even e-mails
- To provide some level of security and monitoring, the use of Internet proxy technology is required
- There are standalone proxy solutions and the aforementioned NGFWs have this feature, which allows for URL filtering based on category and known malicious destinations



Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

NS: Securing Websites

- Internet accessible websites are the most targeted asset on the Internet due to common web application security issues, such as SQL injection
- There are several approaches to securing websites, but it is truly a layered security approach requiring:
  - Secure Coding
  - Firewalls
  - IPS

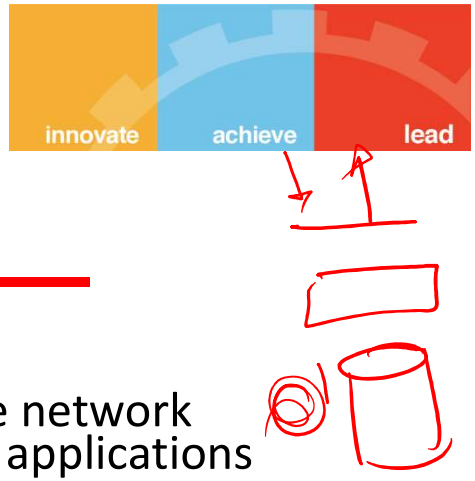
NS: Websites: Secure Coding

- Utilizing a **secure software development lifecycle** (**S-SDLC**) is the best method to ensure that secure coding practices are being followed
  - framework for how the coding process is to be completed with testing and validation of the code
  - process is iterative for each new instance of code or modified portions of code
- Several open source and commercial products available for testing not only via web scanning, but source code analysis as well
- Vulnerabilities identified should be documented and tracked through remediation within a centralized vulnerability or defect management solution
- Secure coding must be the focal point of the security strategy for securing web applications

NS: Websites: NGFW

- NGFW can be leveraged to protect Internet-facing enterprise websites and applications
  - Threats within seemingly benign connection attempts to the web servers can be detected and mitigated with the application aware firewall
  - The benefit of using a next generation firewall is that access can be provisioned by applications, such as web browsing, and is not restricted by TCP port
  - NGFW can also be used for inspecting and mitigating all illegitimate traffic, such as denial of service attacks, before they reach the web servers

NS: Websites: IPS and Web-Application Firewalls



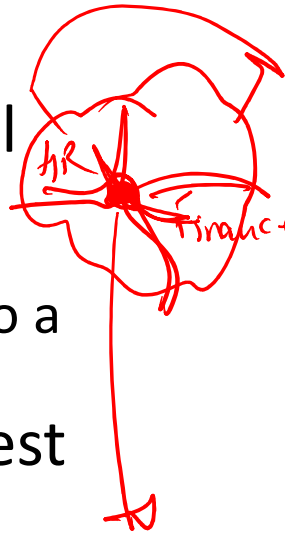
- IPS
  - Intrusion prevention may also be implemented at the network perimeter to mitigate known attack patterns for web applications
  - IPS can provide excellent denial of service protection and block exploit callbacks
- Web-application Firewalls:
  - designed to specifically mitigate attacks against web applications through pattern and behavioral analysis
    - SQL injection, cross-site scripting, command injection, and misconfigurations
  - advanced web application firewalls use another component at the database tier of the web applications. Benefits include:
    - Ability to determine if a detected threat warrants further investigation; i.e. whether the threat was able to interact with the database or not (how safe is the data!!)
    - attacks that do get past the first layer of the web application firewall can be mitigated at the database tier of the network architecture
    - enforce security controls for database access initiated not only by the web application but also by database administrators

A commercial product leader in this space is **Imperva** (http://www.imperva. com). Their solutions provide comprehensive web attack mitigation and database security through database access and activity management capabilities

Network Segmentation

- Even with the most sophisticated security mechanisms, without network segmentation, their value will be greatly undermined
- Internal segmentation is often overlooked, but is extremely important to prevent spread of malware throughout the enterprise
  - advanced threats are introduced through infected consultant systems, unauthorized introduction of personal devices and business-critical applications

Network Segmentation Strategy



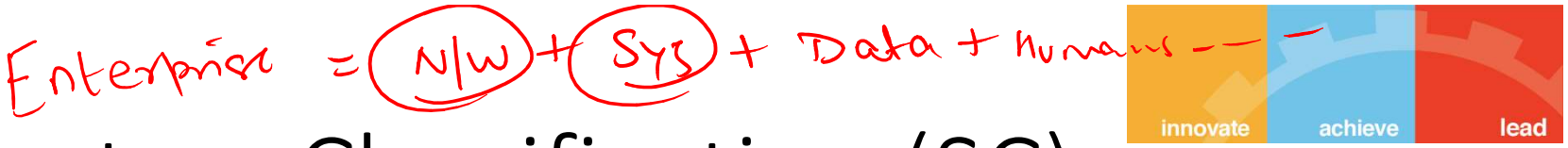
- Before any network segmentation can occur, critical data, processes, applications, and systems must be identified
  - helps determine the complexities of moving the assets to a network segment separated by a firewall
- Network segmentation using a firewall is the simplest network-based security control
- Alongside, highly recommended security monitoring tools, such as **Security Information and Event Management** (**SIEM**) and **File Integrity Monitoring** (**FIM**) should be implemented to ensure that in the event of an attack, there is monitoring for early detection and timely incident response
- In some cases, leveraging data loss prevention tools may be ideal to protect against data leakage

Enterprise Security

Securing the Systems

What we will cover?

- Organization processes and methods to secure enterprise computer systems
  - we will focus on server systems that are used within the enterprise to conduct business functions
- Processes and methods covered:
  - System Classification
  - File integrity monitoring (FIM)
  - Application Whitelisting
  - Host-based intrusion prevention system (HIPS)
  - Host Firewalls
  - System Protection using Anti-virus
  - User account management



System Classification (SC)

- When securing Enterprise Network, Network Segmentation plays a key role:
  - Helps placing systems of high value and criticality in segmented areas of the network
- To identify these systems, it is necessary to understand the important business processes and applications
  - as with any classification model, there should be tiers based on criticality
  - tiers of classification should have a criteria for each level to ensure security and availability requirements are met
  - tier classification may also include service-level agreement information, expected recovery times, and the priority of security incidents involving the systems
- System labels applied will serve as an input to the overall security architecture
  - Labels shall be referenced in other business processes such as change management, user account management, protection tool selection, monitoring, and incident response

Example: System Classification

- A system classification model may look like the following table:

Level	Classification	Process(es)/Function(s)	Requirement
1	Critical	Transaction processing, Deposit functions	Network redundancy, File integrity monitoring, User monitoring, Encryption
2	High	Payroll processing	Network redundancy, User monitoring
3	Medium	Customer e-mail promotion functions	Network redundancy
4	Low	Corporate communication processes	N/A

Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

- Individual systems will not be identified in the table, only processes or functions
- Labeling of the systems should happen in an asset management tool or a **configuration management database** (**CMDB**) if using the ITIL framework

** The enterprise may also decide to create a classification for systems that have regulatory compliance requirements for specific controls to be implemented*

SC: System Management

- An important part of securing systems
  - Includes process of inventory management, system labeling indicating system classification, defining system owners, and required security control mechanisms
  - Plays a significant role in implementing system patching requirements and change management process
- Once systems have been properly classified, asset inventory labels must reflect the classification
  - ensures the correct controls are in place and that policies and standards are enforced

Without asset inventory there is no record of what systems exist, what data is located on the systems, and the risk introduced by the improper securing or loss of the systems!!

SC: System Management (2)

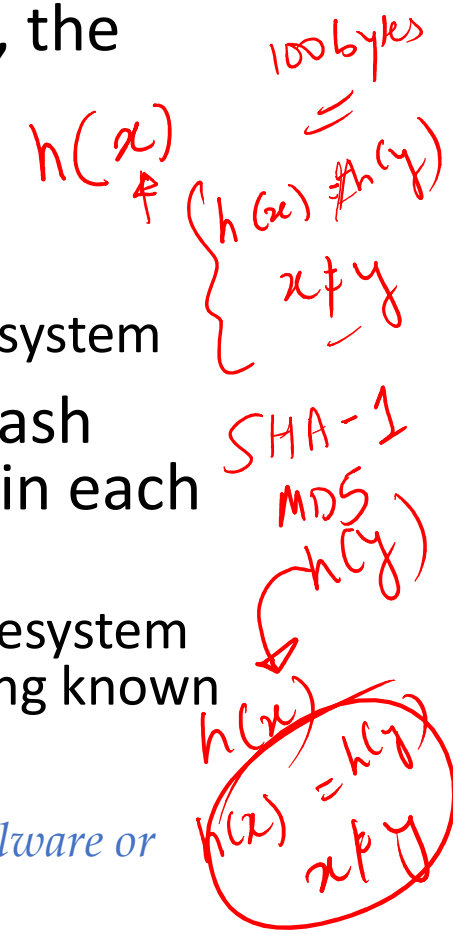
- System patching may be based on
  - A) criticality of the system,
  - B) the severity of the vulnerability, or
  - C) impact of an unpatched software package
- System classification plays a significant role in the patching cycle of systems and must be integrated in the patch and vulnerability management processes
  - When systems remain unpatched and vulnerabilities continue to exist, the window is also extended for malicious actors to exploit

With other weaknesses in the network such as lack of segmentation, systems may be at greater risk when a strict patching cycle is not implemented!!

File Integrity Monitoring (FIM)

- One of the methods used to detect changes to a known filesystem's files, and in the case of Windows, the registry
- when a system has malicious activity, either:
  - changes are made to existing files or
  - harmful files are placed in critical areas of the filesystem
- To detect these changes, FIM tools create a hash database of the known good versions of files in each filesystem location
  - tool can then periodically or real-time scan the filesystem looking for any changes to the installation including known files and directories

A caveat to using this type of tool is the accidental addition of malware or unapproved configuration added to the system ***baseline hash***



FIM Operation Modes

- **Real-time FIM:**
  - all add, delete, and modification actions are detected in real time allowing for almost immediate ability to review and remediate
  - but the constant running of the tool may be taxing to a system that is loaded with several agents for various purposes
- **Manual mode FIM:**
  - least taxing on the system because the scans only run when the console initiates the scan either adhoc or on a schedule
  - IT knows when the system may have higher memory and processor utilization and it ideally will not affect business operations
  - A caveat to this solution is that changes can go undetected for longer periods of time depending on how often scans are run on schedule

Application Whitelisting

- A method to control what applications have permission to run on a system
  - if malicious software is installed on the system, it will not be able to execute
- This model is closer to the trust model discussed in *Lecture 2, Security Architectures*
  - Only trusted applications are allowed to execute
- Tool can also prevent unapproved application install
  - If the application is not preapproved, the installation can be blocked
  - If the installation is successful, the tool can block the application from running

This tool could possibly replace an anti-virus solution and complement other advanced tools in the network such as advanced persistent threat tools and NGFW to provide a layered mitigation implementation!!

HIPS

- **Host-based intrusion prevention system** (**HIPS**) is very similar in concept to network intrusion prevention (discussed earlier)
  - Network-based IPS is a bigger challenge since it is implemented on the network wire, where the applications across various systems can be huge or unknown
  - HIPS leverages being installed on the system it is protecting => it has additional awareness of running applications and services
- Host-based intrusion detection uses the same types of detection methods as the network-based counterpart
  - primary method is signature-based detection as this is the easiest method to implement on a host without taxing the operating system with true behavioral analysis
  - However, it should be noted that a combination of methods should be employed for comprehensive protection

Host Firewall

- Host firewall can be a great method to filter traffic to and from the system
- Firewall should be considered as another layer of defense from intrusion attempts against applications, services, and the host itself
  - solution is similar to application whitelisting in regards to the requirement of knowing what applications are running and how they must communicate
  - Some applications open random ports or have extremely large ranges of ports. Some host firewalls are able to allow dynamic port use, thus alleviating the need to go through the exercise of analyzing the application

Anti-virus

- Anti-virus is considered as a necessary security mechanism for the low-hanging fruit -- **predictable malware**
  - most of it is old, easy to detect, and still dangerous
- Anti-virus primarily use two methods to detect malware:
  - **Signature**: This method looks for known patterns of malware
  - **Heuristics**: In this method the behavior of potential malware is analyzed for malicious actions
- Typically, anti-virus solutions will install an agent on the endpoint, run scans continuously, and any new file introduced is scanned immediately
  - this method of protecting a system can be taxing

Anti-virus are reactive → can only work after the virus is discovered and understood!!

User Account Management (UAM)

- Accounts on a system are some level of access that may be the door in for malicious activity
  - it is easier to use a known account to access a system versus finding another method to exploit the system
  - review of system accounts should be in accordance to the system classification and other security policies
- User Roles and Permissions
  - Need for properly defining system users and roles to perform required tasks
  - Both for server systems and end-user systems (e.g. elevated privileges to install software applications on desktop/laptop)

UAM (2)

- User Account Auditing
  - To detect rogue accounts on systems, the enterprise should perform user account auditing across all systems on a regular basis
  - Accounts should be disabled or deleted at the time of termination as part of a formal process
- Policy Enforcement
  - how the enterprise expects employees to use assets and consequences to actions contrary to policy statements
  - Enforcement may come in the form of an implemented tool, but it may also come from the monitoring of user activity on systems