

# NETWORK DEFENSE

## Overview

Network defense refers to the strategies, technologies, and practices used to protect computer networks from unauthorized access, misuse, modification, or destruction. As cyber threats continue to evolve, organizations must implement comprehensive security measures to safeguard their data and systems.

Network defense involves multiple layers of security, including firewalls, intrusion detection and prevention systems, antivirus software, encryption, and secure access controls. This layered approach—often called **Defense-in-Depth**—ensures that if one security measure fails, others are in place to mitigate the threat.

Effective network defense also includes continuous monitoring, regular updates, employee training, and adherence to security policies and regulations. It plays a critical role in maintaining the confidentiality, integrity, and availability of information in both private and public networks.

## Defense-in-Depth

### Assets, Vulnerabilities, Threats

Cybersecurity analysts must prepare for any type of attack. It is their job to secure the assets of the organization's network. To do this, cybersecurity analysts must first identify:

- **Assets** - Anything of value to an organization that must be protected including servers, infrastructure devices, end devices, and the greatest asset, data.
- **Vulnerabilities** - A weakness in a system or its design that could be exploited by a threat actor.
- **Threats** - Any potential danger to an asset.

### Identify Assets

As an organization grows, so do its assets. Consider the number of assets a large organization would have to protect. It may also acquire other assets through mergers with other companies. The result is that many organizations only have a general idea of the assets that need to be protected.

The collection of all the devices and information owned or managed by the organization are assets. The assets constitute the attack surface that threat actors could target. These assets must be inventoried and assessed for the level of protection needed to thwart potential attacks.

Asset management consists of inventorying all assets, and then developing and implementing policies and procedures to protect them. This task can be daunting considering many organizations must protect internal users and resources, mobile workers, and cloud-based and virtual services.

Further, organizations need to identify where critical information assets are stored, and how access is gained to that information. Information assets vary, as do the threats against them. For example, a retail business may store customer credit card information. An engineering firm will store competition-sensitive designs and software. A bank will store customer data, account information, and other sensitive financial information. Each of these assets can attract different threat actors who have different skill levels and motivations.

## **Asset classification**

Asset classification assigns an organization's resources into groups based on common characteristics. The most critical information needs to receive the highest level of protection and may even require special handling.

A labeling system can be used to determine how valuable, how sensitive, and how critical the information is.

Steps for identifying and classifying assets:

- i. **Step 1:** Determine the proper asset identification category:
  - a. Information assets
  - b. Software assets
  - c. Physical assets
  - d. Services
- ii. **Step 2:** Establish asset accountability by identifying the owner of each information asset and each piece of software:
  - a. Identify the owner for all information assets.
  - b. Identify the owner for all application software.
- iii. **Step 3:** Determine the criteria for classification.
  - a. Confidentiality
  - b. Value
  - c. Time
  - d. Access rights
  - e. Destruction
- iv. **Step 4:** Implement a classification schema:
  - a. Adopt a consistent way of identifying information to ensure uniform protection and easier monitoring.

## Asset Standardization

Asset standards identify specific hardware and software products used by an organization.

When a failure occurs, prompt action helps to maintain both access and security. If an organization does not standardize its hardware selection, personnel may need to scramble to find a replacement component. Non-standard environments require more expertise to manage, and they increase the cost of maintenance contracts and inventory.

## Asset Lifecycle Stages

For cybersecurity specialists, part of the job is to manage information assets and related systems throughout that asset's lifecycle.

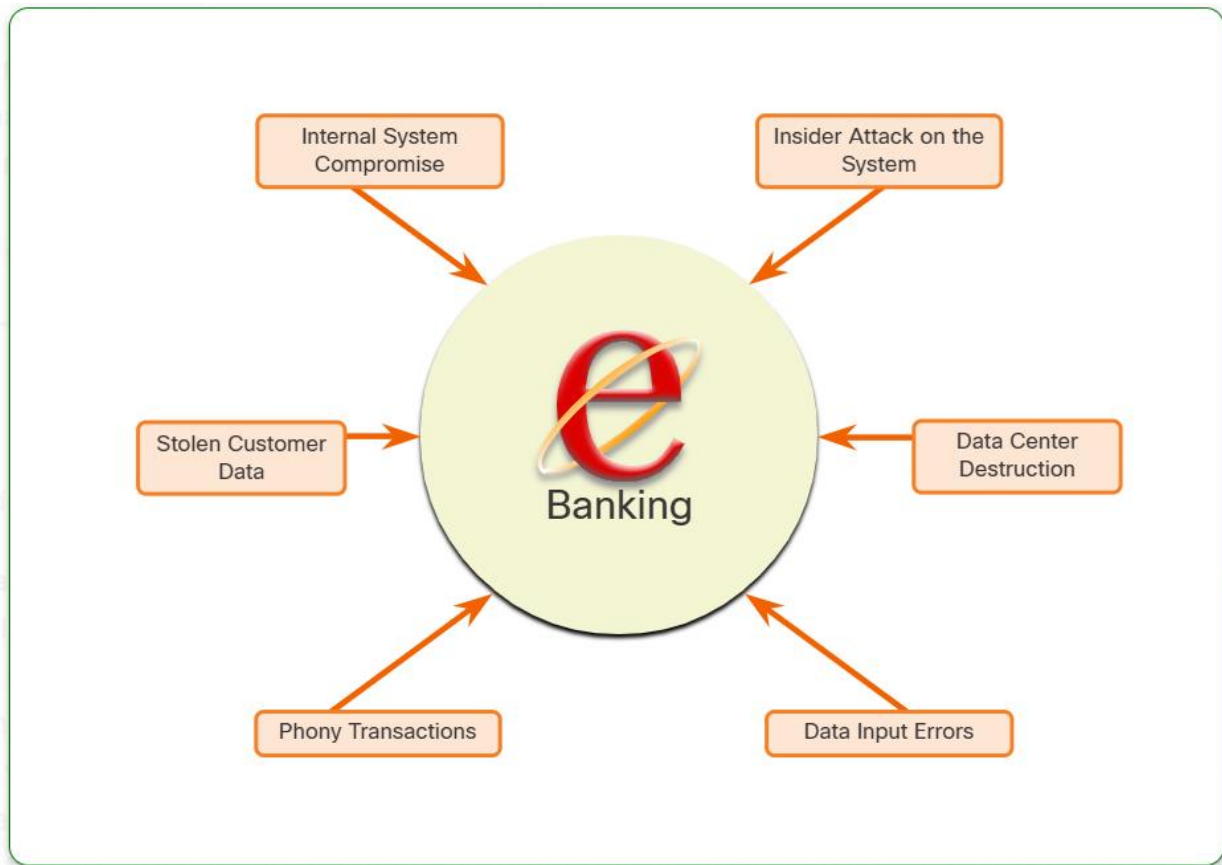
- **Procurement:** The organization purchases the assets based on the needs identified from data gathered to justify the purchase.  
The asset is added to the organization's inventory.
- **Deployment:** The asset is assembled and inspected to check for defects or other problems. Staff performs tests and installs tags or barcodes for tracking purposes.  
The asset moves from inventory to in-use.
- **Utilization:** This is the longest stage of the cycle. The asset's performance is continuously checked. Upgrades, patch fixes, new license purchases, and compliance audits are all part of the utilization stage.
- **Maintenance:** Maintenance helps to extend an asset's productive life. Staff may modify or upgrade the asset.
- **Disposal:** At the end of the asset's productive life, it must be disposed of. All data must be wiped from the asset. Disposal may include dismantling an asset for parts. Any parts that can cause an environmental hazard must be disposed of according to local guidelines.

## Identify Vulnerabilities

Threat identification provides an organization with a list of likely threats for a particular environment. When identifying threats, it is important to ask several questions:

- What are the possible vulnerabilities of a system?
- Who may want to exploit those vulnerabilities to access specific information assets?
- What are the consequences if system vulnerabilities are exploited and assets are lost?

For example, refer to the figure.



The threat identification for an e-banking system would include:

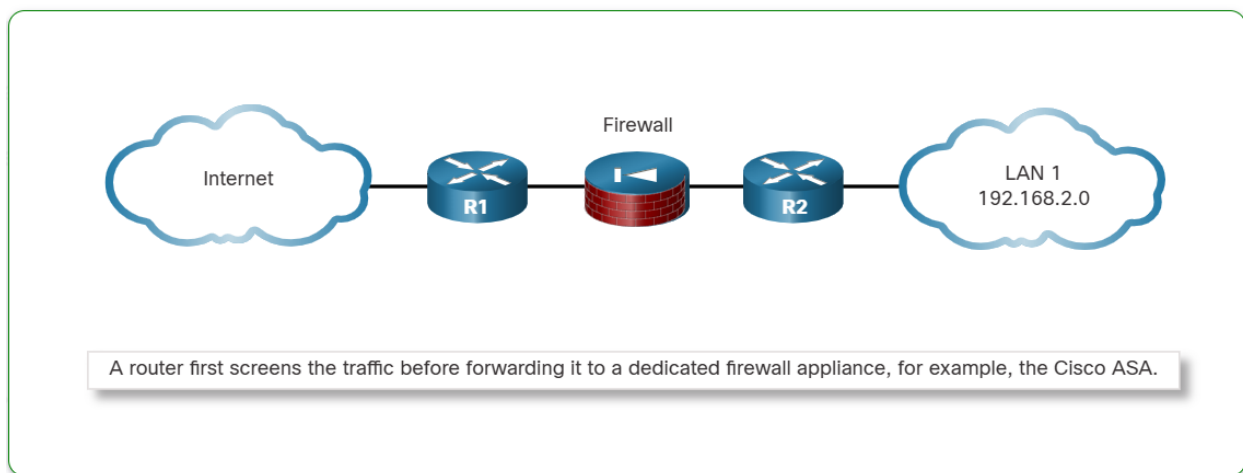
- **Internal system compromise** – The attacker uses the exposed e-banking servers to break into an internal bank system.
- **Stolen customer data** – An attacker steals the personal and financial data of bank customers from the customer database.
- **Phony transactions from an external server** – An attacker alters the code of the e-banking application and makes transactions by impersonating a legitimate user.
- **Phony transactions using a stolen customer PIN or smart card** – An attacker steals the identity of a customer and completes malicious transactions from the compromised account.
- **Insider attack on the system** – A bank employee finds a flaw in the system from which to mount an attack.
- **Data input errors** – A user inputs incorrect data or makes incorrect transaction requests.
- **Data center destruction** – A cataclysmic event severely damages or destroys the data center.

Identifying vulnerabilities on a network requires an understanding of the important applications that are used, as well as the different vulnerabilities of that application and hardware. This can require a significant amount of research on the part of the network administrator.

## Identify Threats

Organizations must use a defense-in-depth approach to identify threats and secure vulnerable assets. This approach uses multiple layers of security at the network edge, within the network, and on network endpoints.

For an example, refer to the figure.



The figure displays a simple topology of a defense-in-depth approach:

- **Edge Router** – The first line of defense is known as an edge router (R1 in the figure). The edge router has a set of rules specifying which traffic it allows or denies. It passes all connections that are intended for the internal LAN to the firewall.
- **Firewall** – The second line of defense is the firewall. The firewall is a checkpoint device that performs additional filtering and tracks the state of the connections. It denies the initiation of connections from the outside (untrusted) networks to the inside (trusted) network while enabling internal users to establish two-way connections to the untrusted networks. It can also perform user authentication (authentication proxy) to grant external remote users access to internal network resources.
- **Internal Router** – Another line of defense is the internal router (R2 in the figure). It can apply final filtering rules on the traffic before it is forwarded to its destination.

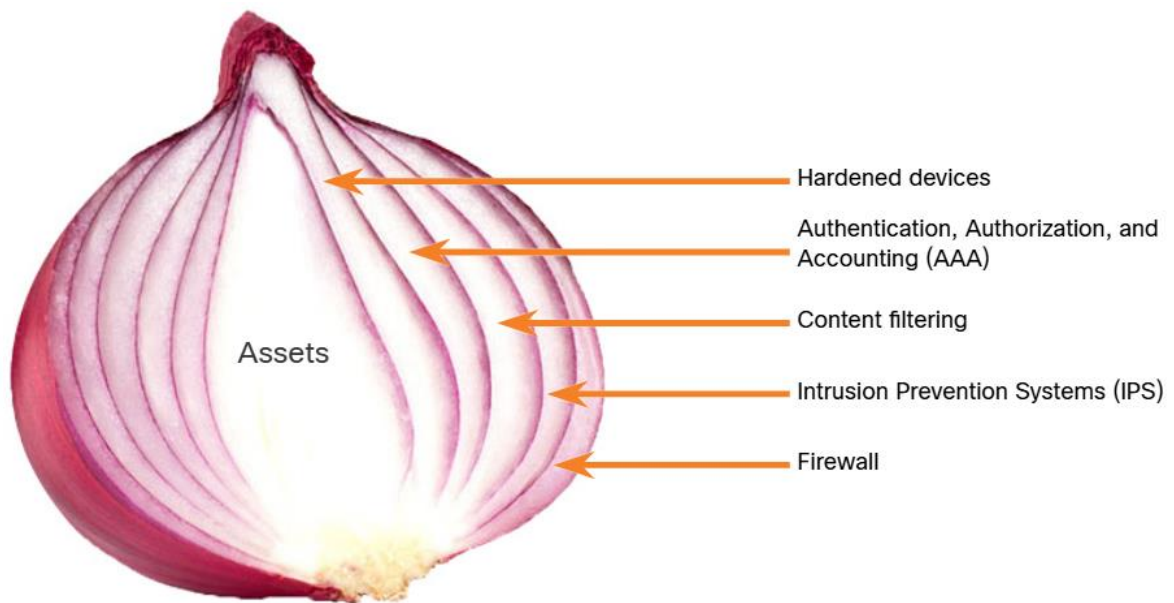
Routers and firewalls are not the only devices that are used in a defense-in-depth approach. Other security devices include Intrusion Prevention Systems (IPS), Advanced Malware Protection (AMP), web and email content security systems, identity services, network access controls, and more.

In the layered defense-in-depth security approach, the different layers work together to create a security architecture in which the failure of one safeguard does not affect the effectiveness of the other safeguards.

## The Security Onion and the Security Artichoke

There are two common analogies that are used to describe a defense-in-depth approach.

- **Security Onion:** A common analogy used to describe a defense-in-depth approach is called “the security onion.” As illustrated in figure, a threat actor would have to peel away at a network’s defenses layer by layer in a manner similar to peeling an onion. Only after penetrating each layer would the threat actor reach the target data or system.  
**Note:** The security onion described on this page is a way of visualizing defense-in-depth. This is not to be confused with the Security Onion suite of network security tools.



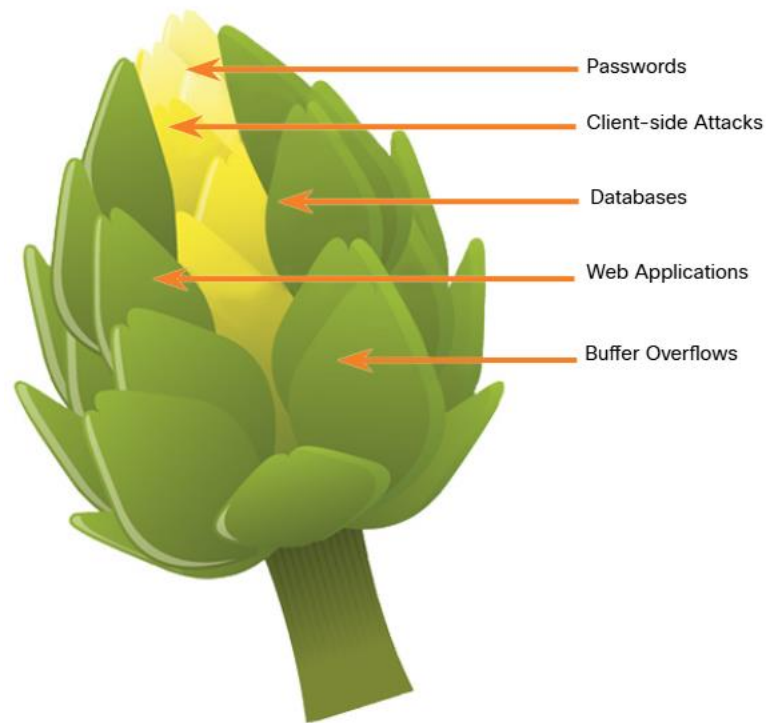
- **Security Artichoke:** The changing landscape of networking, such as the evolution of borderless networks, has changed this analogy to the “security artichoke”, which benefits the threat actor.

As illustrated in the figure, threat actors no longer have to peel away each layer. They only need to remove certain “artichoke leaves.” The bonus is that each “leaf” of the network may reveal sensitive data that is not well secured.

For example, it’s easier for a threat actor to compromise a mobile device than it is to compromise an internal computer or server that is protected by layers of defense. Each mobile device is a leaf. And leaf after leaf, it all leads the hacker to more data. The heart of the artichoke is where the most confidential data is found. Each leaf provides a layer of protection while simultaneously providing a path to attack.

Not every leaf needs to be removed in order to get at the heart of the artichoke. The hacker chips away at the security armor along the perimeter to get to the “heart” of the enterprise.

While internet-facing systems are usually very well protected and boundary protections are typically solid, persistent hackers, aided by a mix of skill and luck, do eventually find a gap in that hard-core exterior through which they can enter and go where they please.



### Defense in Depth Strategies

If an organization only has one security measure in place to protect data and information, then cybercriminals only need to get past that one single defense to steal information or cause other harm. To make sure data and infrastructure remain secure, an organization should create different layers of protection.

- **Layering:** To make sure data and information remains available, an organization must set up different layers of protection, creating a barrier of multiple defenses that work together to prevent attacks. A good example of layering is an organization storing its top-secret documents on a password-protected server in a locked building that is surrounded by an electric fence. A layered approach provides the most comprehensive protection because, even if cybercriminals penetrate one layer, they still must contend with several more defenses. Ideally, each layer should be more complicated to overcome! Defense in depth

does not provide an impenetrable shield, but it will help an organization minimize risk by staying one step ahead of cybercriminals.

- **Limiting:** Limiting access to data and information reduces the possibility of a security threat. An organization should restrict access so that each user only has the level of access required to do their job. An organization should have the right tools and settings, such as file permissions, in place to limit access, as well as the right procedural measures, which define specific steps for doing anything that can affect security. For example, a limiting procedure which requires employees to always consult sensitive documents in a room which has CCTV, ensures that they would never remove such documents from the premises.
- **Diversity:** If all defense layers were the same, it would not be very difficult for cybercriminals to succeed in an attack. The layers must be different so that if one layer is penetrated, the same technique will not work on all the others which would compromise the whole system. Furthermore, an organization will normally use different encryption algorithms and authentication systems to protect data in different states. To accomplish the goal of diversity in defenses, organizations can use security products by different companies as different factors of authentication, such as a swipe card from one company and a fingerprint reader manufactured by a different company — as well as varied security measures, such as time-delay locks on cabinets and supervision by a security staff member upon unlocking it.
- **Obscurity:** Obscuring information can also protect data and information. An organization should not reveal any information that cybercriminals can use to identify which Operating System (OS) a server is running, or the type or make of equipment or software it uses. Error messages or system information should not contain any details that a cybercriminal could use to determine what vulnerabilities are present. Concealing certain types of information makes it more difficult for cybercriminals to attack.
- **Simplicity:** Complexity does not necessarily guarantee security. If an organization implements complex systems that are hard to understand and troubleshoot, this may backfire. If employees do not understand how to configure or manage systems correctly, they may inadvertently introduce vulnerabilities. Simple systems that are easy to understand and maintain are often more secure because they are less prone to misconfiguration and human error. While security needs to be robust, unnecessary complexity can make systems harder to manage and more susceptible to issues.



# **Cybersecurity Operations Management**

## **Configuration Management**

Configuration management refers to identifying, controlling and auditing the implementation and any changes made to a system's established baseline.

The baseline configuration includes all the settings that you configure for a system which provide the foundation for all similar systems — like a template of sorts.

For instance, those responsible for deploying Windows workstations to users must install the required applications and set up the system settings according to a documented configuration. This is the baseline configuration for Windows workstations within this organization.

- Documented configuration resources might include the following:
  - ✓ Network maps, cabling and wiring diagrams, application configuration specifications
  - ✓ Standard naming conventions used for computers
  - ✓ IP schema to track IP addresses
- Hardening the operation systems is an important part of making sure that systems have secure configurations. Configuring log files along with auditing, changing default account names and passwords, and implementing account policies and file-level access control are all used to create a secure OS.

## **Log Files**

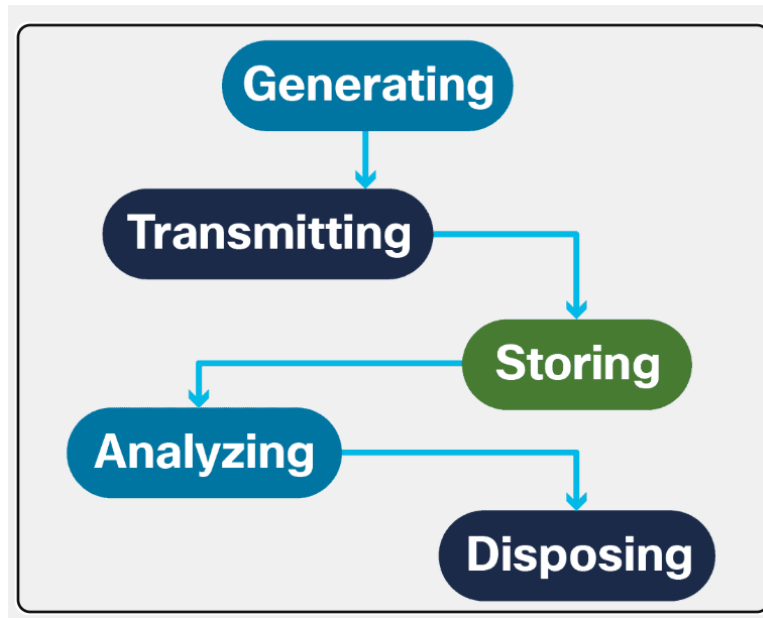
A log records all events as they occur. Log entries make up a log file, with each log entry containing all the information related to a specific event. Accurate and complete logs are very important in cybersecurity.

For example, an audit log tracks user authentication attempts, while an access log records details on requests for specific files on a system. Monitoring system logs will therefore help us determine how an attack occurred and which of the defenses deployed were successful — and which were not.

As an increasing number of log files are generated for computer security purposes, organizations should consider a log management process. Management of computer security log data should determine the procedures for the following:

- Generating log files
- Transmitting log files

- Storing log files
- Analyzing log data
- Disposing of log data



## Operating System Logs and Application Security Logs

### Operating system logs

Operating system logs record events that are linked to actions that have to do with the operating system. System events include the following:

- Client requests and server responses such as successful user authentications
- Usage information that contains the number and size of transactions in a given period of time

### Application security logs

Organizations use network-based and/or system-based security software to detect malicious activity.

This software generates a security log to provide computer security data. These logs are useful for performing auditing analysis and identifying trends and long-term problems. Logs also enable an organization to provide documentation showing that it complies with laws and regulatory requirements.

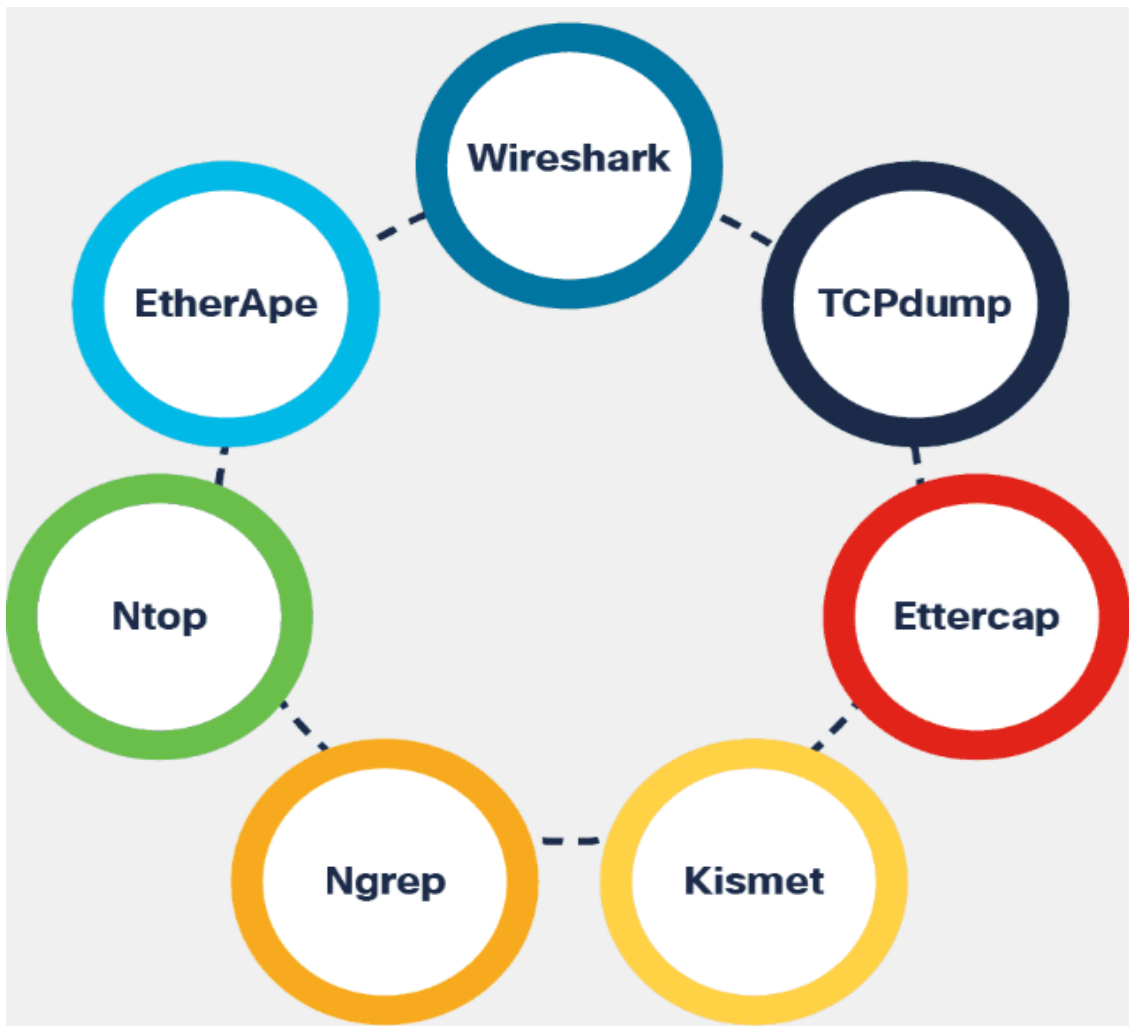
## Protocol Analyzers

Packet analyzers, otherwise known as packet sniffers, intercept and log network traffic.

The packet analyzer captures each packet, looks at the values of various fields in the packet and analyzes its content. It can capture network traffic on both wired and wireless networks.

Packet analyzers perform the following functions:

- Traffic logging
- Network problem analysis
- Detection of network misuse
- Detection of network intrusion attempts
- Isolation of exploited systems



## Physical security

### Fencing and Physical Barriers

Barricades or fencing are often the first things that come to mind when thinking about types of physical security.

In many situations, they are the outermost layer of defense and the most visible. All physical barriers should meet specific design requirements and material specifications.



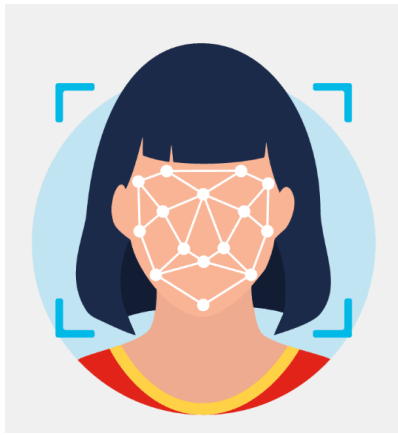
High-security areas often require a ‘top guard’ such as barbed wire or concertina wire. Top guards act as an additional deterrent and can delay the intruder by causing severe injury. However, attackers can still use a blanket or mattress to alleviate this threat.

Local regulations may restrict the type of fencing system an organization can use and it’s important to remember that fences require regular maintenance. Animals may burrow under the fence or the earth may wash out, leaving the fence unstable — this would lead to easy access for an intruder. Fencing systems should be inspected regularly.

Moreover, vehicles should never be parked near a security fence, as this could assist the intruder in climbing over or causing damage to the fence.

### Biometrics

Biometrics are the physiological or behavioral characteristics of an individual, and there are security practices based on identifying and granting access using biometrics.



Biometric authentication systems can include measurements of the face, fingerprint, hand geometry, iris, retina, signature, and voice.

Biometric technologies can be the foundation of highly secure identification and personal verification solutions. The popularity and use of biometric systems have increased because of the rise in security breaches and transaction fraud.

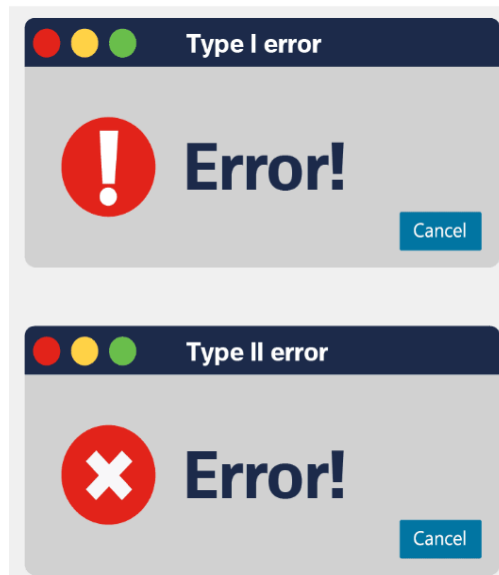
Biometrics can ensure confidential financial transactions and personal data privacy — a well-known example being smartphones, which use fingerprint readers to unlock the device and access apps, including online banking and payment systems.



When selecting biometric systems, there are several important factors to consider, including:

- Accuracy
- Speed or throughput rate
- Acceptability to users
- Uniqueness of the biometric organ and action
- Resistance to counterfeiting
- Reliability
- Data storage requirements
- Enrollment time
- Intrusiveness of the scan

The most important of these factors is accuracy, which is expressed in error types and rates.



The first error rate is Type I errors or false rejections. A Type I error rejects a person who is registered and an authorized user. In access control, where the main objective is to keep cybercriminals away, false rejection is the least important error. It means that someone who should gain access is not granted access.

However, in many biometric applications, particularly retail or banking, false rejections can have a very negative impact on business due to a transaction or sale being lost.

False acceptance is a Type II error. Type II errors allow entry to people who should not have entry, meaning a cybercriminal can potentially gain access. For this reason, Type II errors are normally considered the most important error for a biometric access control system.

The acceptance rate is also an important concept here. Stated as a percentage, it is the rate at which a system accepts unenrolled individuals or imposters as authentic users – so the rate of Type II errors per total instances of granting permission.

## **Surveillance**

Many physical access controls, including deterrent and detection systems, ultimately rely on people to intervene and stop the actual attack or intrusion.

## Application security

### Application Development

- **Developing and testing:** Software is developed and updated in a development environment, where it can be developed, tested and debugged before being deployed. A development environment is less restrictive than the live environment and has a lower security level. Version control software helps track and manage changes to the software code. Developers may also work in a sandbox environment so that code is not overwritten as they develop it. During testing, developers look at how the code interacts with the normal environment. Quality assurance (QA) can find defects in the software. It is much easier to fix any defect found at this phase.
- **Staging and production:** Staging environments should closely match the organization's production environment. By testing in a staging environment, developers can verify that the software runs under the required security settings. After the developer runs and tests security, the program can be deployed to production.
- **Provisioning and deprovisioning:** Provisioning is the creation or updating of software. Deprovisioning is its removal. An organization can use a self-service portal to automate software provisioning and deprovisioning.

### Security Coding Techniques

- **Normalization:** Normalization is used to organize data in a database and help maintain data integrity. Normalization converts an input string to its simplest known form to ensure that all strings have unique binary representations and that any malicious input is identified.
- **Stored Procedure:** A stored procedure is a group of precompiled SQL statements stored in a database that execute a task. If you use a stored procedure to accept input parameters from clients using different input data, you will reduce network traffic and get faster results.
- **Obfuscation and Camouflage:** A developer can use obfuscation and camouflage to prevent software from being reverse-engineered. Obfuscation hides original data with random characters or data. Camouflage replaces sensitive data with realistic fictional data.
- **Code Reuse:** Code reuse means using existing software to build new software, saving time and development costs. Care must be taken, though, to avoid the introduction of vulnerabilities.
- **SDKs:** Third-party libraries and software development kits (SDKs) provide a repository of useful code to make application development faster and cheaper. The downside is that any vulnerability in SDKs or third-party libraries can potentially affect many applications.

## Input Validation



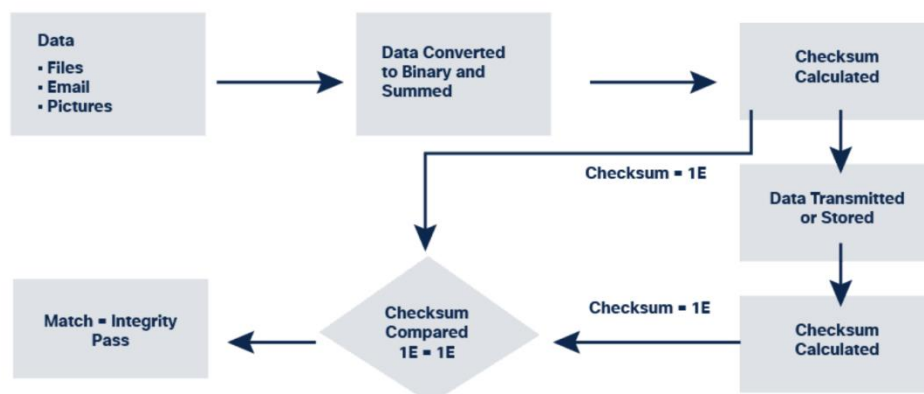
Controlling the data input process is key to maintaining database integrity. Many attacks run against a database and insert malformed data. Such attacks can confuse crash or make the application divulge too much information to the attacker. Scroll down to look at an example — in this case, an automated input attack.

Customers fill out a web application form to subscribe to a newsletter. A database application automatically generates and sends email confirmations back to the customers. When customers receive the email with a URL link to confirm their subscription, attackers have modified the URL link.

These modifications can change the username, email address or subscription status of the customers when they click to confirm their subscription. This way, when the email is returned to the host server, it receives bogus information, which it might not be aware of if it does not check each email address against subscription information.

Hackers can automate this attack to flood the web application with thousands of invalid subscribers to the newsletter database.

## Integrity Checks





Compromised data can threaten the security of your devices and systems. An **integrity check** can measure the consistency of data in a file, picture or record to ensure that it has not been corrupted. The integrity check performs a **hash function** to take a snapshot of data and then uses this snapshot to ensure data has remained unchanged. A **checksum** is an example of a hash function.

- **How a checksum works:** A checksum verifies the integrity of files, or strings of characters, before and after they transfer between devices across a local network or the Internet. Checksums convert each piece of information to a value and sum the total. To test the data integrity, a receiving system repeats the process. If the two sums are equal, the data is valid. If not, a change has occurred somewhere along the line.
- **Hash functions:** Common hash functions include MD5, SHA-1, SHA-256 and SHA-512. These use complex mathematical algorithms to compare data to a hashed value. For example, after downloading a file, the user can verify the integrity of the file by comparing the hash values from the source with the ones generated by any hash calculator.
- **Version control:** Organizations use version control to prevent authorized users from making accidental changes. Version control means that two users cannot update the same object, such as a file, database record or transaction, at the exact same time. For example, the first user to open a document has the permission to change that document; the second person who tries to open it while the first user is still working on it will only be able to access a read-only version.
- **Backups:** Accurate backups help to maintain data integrity if data becomes corrupted. An organization needs to verify its backup process to ensure the integrity of the backup.
- **Authorization:** Authorization determines who access to an organization's resources has based on a need-to-know basis. For example, file permissions and user access controls ensure that only certain users can modify data. An administrator can set permissions for a file to read-only. As a result, a user accessing that file cannot make any changes.

## Other Application Security Practices

How can you be sure that a piece of software you are installing is authentic or that information is secure when browsing the Internet?

- **Code signing:** code signing helps prove that a piece of software is authentic. Executables designed to install and run on a device are digitally signed to validate the author's identity and provide assurance that the software code has not changed since it was signed.
- **Secure cookies:** Using secure cookies protects information stored in cookies from hackers. When your client systems interacts with a server, the server sends a HTTP response that instructs your browser to create at least one cookie. The cookie then stores data for future requests while you are browsing that website. Web developers should use

cookies with HTTPS, to secure cookies and prevent them from being transmitted over unencrypted HTTP.

## **Managing Threats to Applications**

Organizations can implement various measures to manage threats to the application domain.

- **Unauthorized access to data centers, computer rooms, and wiring closets**
  - ✓ Implement policies, standards, and procedures for staff and visitors to ensure the facilities are secure.
  - ✓ Conduct regular security audits and physical access control checks.
  - ✓ Use biometric access controls and badge entry systems to limit unauthorized access.
- **Server and system downtime**
  - ✓ Develop a business continuity plan for critical applications to maintain availability of operations.
  - ✓ Create detailed recovery procedures and ensure redundancy systems are in place for high availability.
  - ✓ Develop a disaster recovery plan for critical applications and data, outlining recovery time objectives (RTO) and recovery point objectives (RPO).
- **Network operating system software vulnerability**
  - ✓ Develop a policy to address application software and operating system updates.
  - ✓ Establish a routine patch management process to evaluate, test, and apply security patches promptly.
  - ✓ Install patches and updates regularly and monitor systems for signs of vulnerabilities.
- **Unauthorized access to systems**
  - ✓ Use multi-factor authentication (MFA) to strengthen login security.
  - ✓ Monitor log files in real-time for unauthorized access attempts and unusual activities.
  - ✓ Implement role-based access controls (RBAC) to restrict access to sensitive systems based on job requirements.
- **Data loss**
  - ✓ Implement data classification standards to ensure critical data is treated with appropriate levels of security.
  - ✓ Implement backup procedures, including automated backups to secure locations, ensuring data redundancy.
  - ✓ Regularly test backup recovery processes to ensure data can be restored effectively.

- **Software development vulnerabilities**

- ✓ Follow secure coding practices to prevent common vulnerabilities such as SQL injection, cross-site scripting (XSS), and buffer overflows.
- ✓ Conduct code reviews and static analysis to identify potential flaws in the software before deployment.
- ✓ Utilize automated security testing tools during the development lifecycle to identify security risks early.

## **Network Hardening: Services and Protocols**

### **Network and Routing Services**

Cybercriminals use vulnerable network services to attack a device or to use it as part of an attack. To check for insecure network services, use a port scanner to detect open ports on a device. A port scanner sends a message to each port and waits for a response, which indicates how the port is used and whether it is open.

But beware; cybercriminals also use port scanners for this same reason! Securing network services ensures that only necessary ports are exposed and available.

- **DHCP (Dynamic Host Configuration Protocol):** DHCP uses a server to assign an IP address and other configuration information to network devices. In effect, the device gets a permission slip from the DHCP server to use the network. Attackers can target DHCP servers to deny access to devices on the network, but security measures like DHCP snooping prevent rogue DHCP servers from providing IP addresses to clients by validating messages from sources that are not trusted. A security checklist for DHCP:
  - Physically secure the DHCP server.
  - Apply any software patches.
  - Locate the DHCP server behind a firewall.
  - Monitor DHCP activity by reviewing DHCP logs.
  - Maintain a strong antivirus solution.
  - Uninstall any unused services and applications.
  - Close unused ports.
- **DNS (Domain Name System):** DNS translates a URL or website address, such as `www.cisco.com`, into a numerical IP address. When users type a web address into the address bar, the DNS server will recognize the IP address. Attackers can target DNS servers to deny access to network resources or redirect traffic to rogue websites. Use secure service and authentication between DNS servers to protect them from these attacks. DNS Security Extensions (DNSSEC) uses digital signatures to strengthen authentication and protect against threats to the DNS. A security checklist for DNS:
  - Keep DNS software up to date.
  - Prevent version string from revealing information.

- Separate internal and external DNS servers.
  - Restrict allowed transactions by client IP address.
  - Use transaction signatures to authenticate transactions.
  - Disable or restrict zone transfers and dynamic updates as much as possible.
  - Enable logging and analyze logs.
  - Use Domain Name System Security Extensions (DNSSEC).
  - Sign zones.
- **ICMP (Internet Control Message Protocol):** Network devices use ICMP to send error messages, that a requested service is not available or the host could not reach the router, for example. The ping command is a network utility that uses ICMP to test the reachability of a host on a network. Ping sends ICMP messages to the host and waits for a reply. Cybercriminals can alter the use of ICMP to run reconnaissance, denial of service (DoS) and covert channel attacks. Many networks filter ICMP requests to prevent such attacks.
  - **RIP (Routing Information Protocol):** RIP is a routing protocol that limits the number of hops from source to destination that are allowed in a network path. The maximum number of hops allowed for RIP is fifteen. RIP is used to exchange routing information about which networks each router can reach and how far away those networks are. RIP calculates the best route based on hop count, but cybercriminals can also target routers and the RIP protocol. Such attacks on routing services can affect performance and availability, some attacks can even result in traffic redirection. Use secure services with authentication and implement system patching and updates to protect routing services.
  - **NTP (Network Time Protocol):** Having the correct time within networks is important. Correct timestamps accurately track network events such as security violations. Additionally, clock synchronization is critical for the correct interpretation of events within syslog data files as well as for digital certificates. Network Time Protocol (NTP) is a protocol that synchronizes network computer system clocks. NTP allows network devices to synchronize their time settings with an NTP server. Cybercriminals attack timeservers to disrupt secure communication that depends on digital certificates and to hide attack information. Use NTP Authentication to verify that the server is trusted.

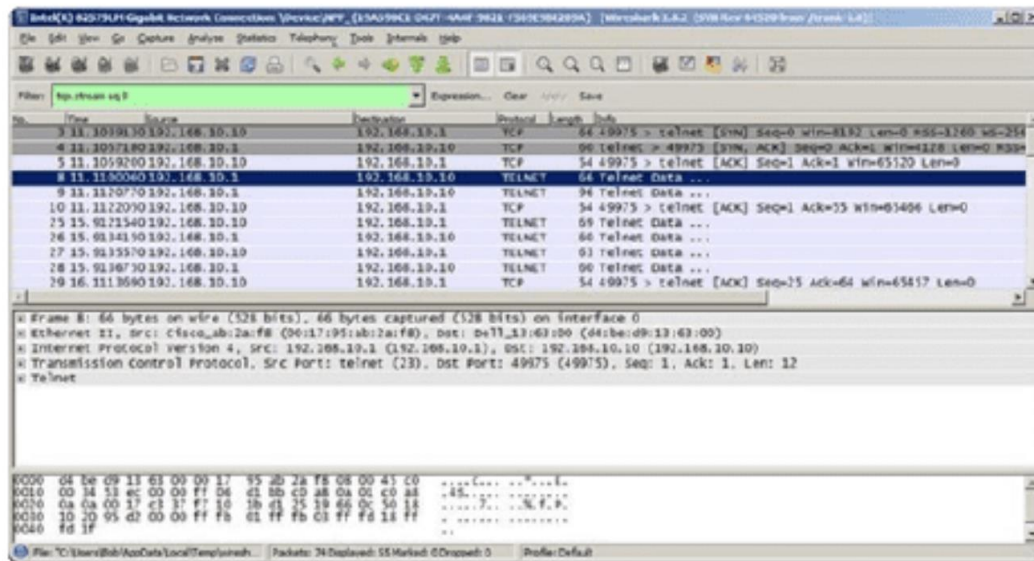
## **Telnet, SSH, and SCP**

**Secure Shell (SSH)** is a protocol that provides a secure (encrypted) remote connection to a device. **Telnet** is an older protocol that uses unsecure plaintext when authenticating a device (username and password) and transmitting data. SSH should be used rather than Telnet to manage connections, as it provides strong encryption. SSH uses TCP port 22, while Telnet uses TCP port 23.

**Secure Copy (SCP)** securely transfers files between two remote systems. SCP uses SSH for data transfer and authentication, ensuring the authenticity and confidentiality of the data in transit.

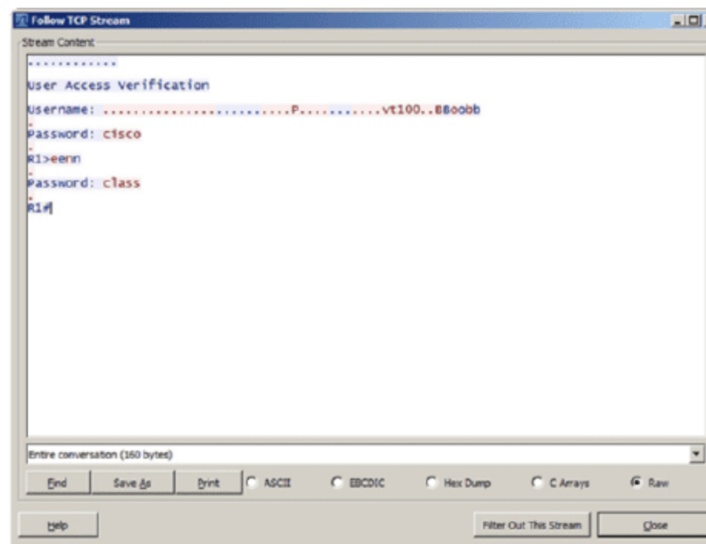
Let's take a closer look

- **Wireshark Telnet Capture:** Wireshark is a powerful network protocol analyzer that cybercriminals can use to monitor network traffic and capture packets. When **Telnet** is used for remote connections, the data, including login credentials, is transmitted in **plaintext**. This means that anyone with access to the network can easily intercept and capture the information.



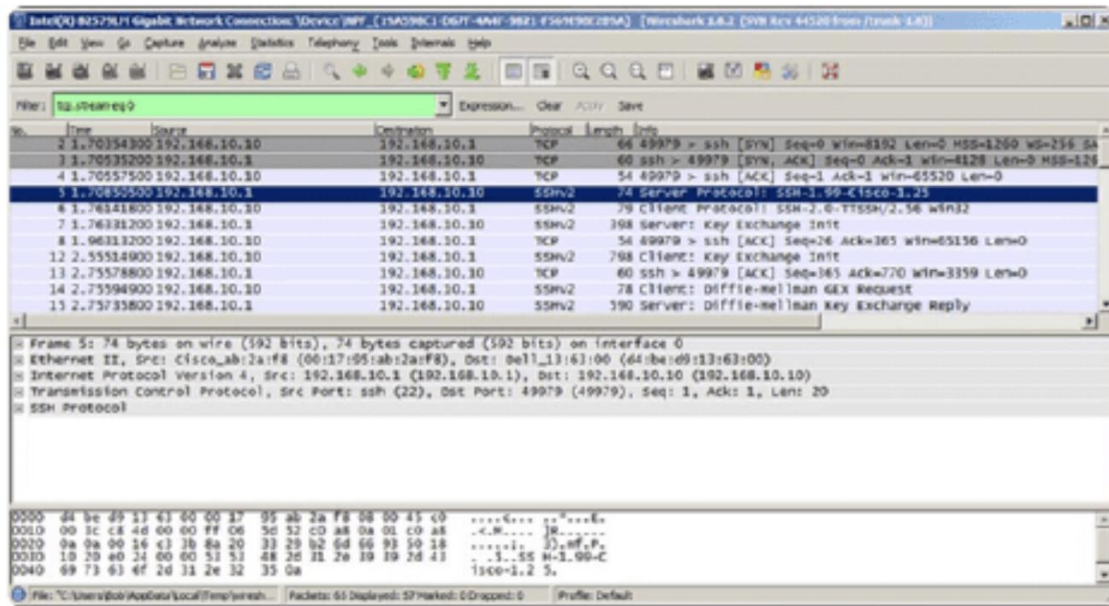
Cybercriminals monitor packets using Wireshark

- **Plaintext Username and Password Capture:** Using Wireshark, cybercriminals can capture the **username** and **password** of the administrator when a Telnet session is initiated. Since Telnet sends data without encryption, the credentials are visible as plaintext, making it easy for attackers to steal login information. This is one of the major security risks of using Telnet, and it's why SSH is highly recommended for secure remote connections.



Cybercriminals capture the username and password of the administrator from the plaintext Telnet session.

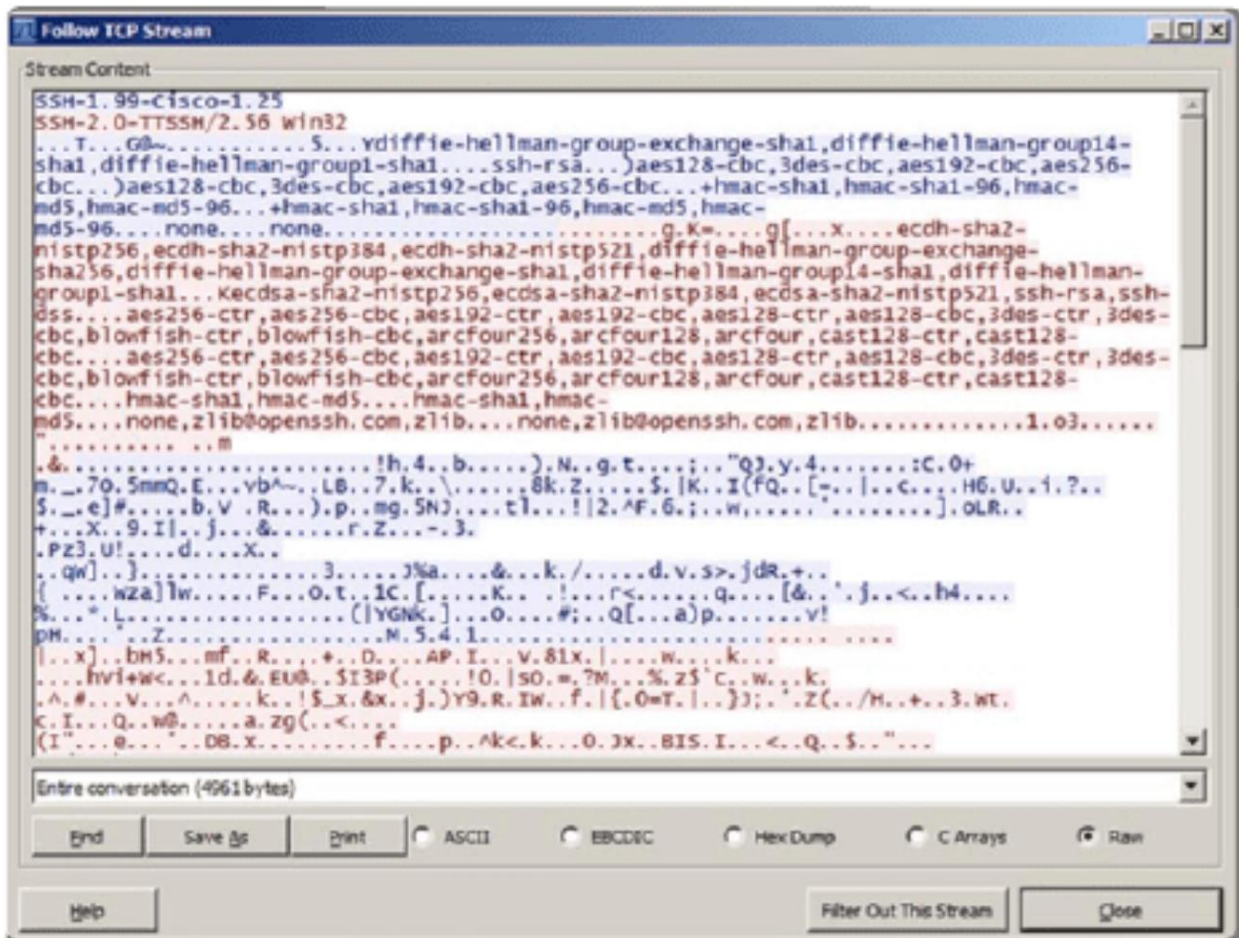
- **Wireshark SSH Capture:** Unlike Telnet, **SSH (Secure Shell)** encrypts the session, preventing unauthorized users from easily capturing sensitive data. However, Wireshark can still be used to track the session by monitoring network traffic. Cybercriminals may use the IP address of the **administrator's device** to identify the ongoing SSH session, but without decryption keys, they won't be able to capture the encrypted username or password. Still, session tracking is a risk, and monitoring tools like Wireshark can be used to identify patterns or suspicious behavior.



The Wireshark view of an SSH session. Cybercriminals track the session using the IP address of the administrator device.

- **Username and Password Encrypted:** With SSH, the **username** and **password** are encrypted, ensuring that even if the packets are captured, the sensitive information remains secure. Unlike **Telnet**, which sends credentials in **plaintext**, SSH uses **strong encryption** algorithms (such as AES, 3DES, or ChaCha20) to scramble the data, making it unreadable to anyone intercepting the communication. This encryption ensures that unauthorized users cannot easily gain access to login details, even if they have access to the network traffic. In the **Wireshark view of an SSH session**, the data appears as **garbled characters** due to the encryption, which adds an extra layer of security. Even if cybercriminals manage to capture the traffic, they would see no useful information—only encrypted, meaningless data. This makes it incredibly difficult to extract usable information from the session, unlike Telnet where everything, including passwords and commands, is transmitted in an easily readable format. Moreover, SSH not only encrypts authentication data but also all the data exchanged between the client and server during the session. This includes the commands you type, the output you receive, and any files that are transferred. As a result, any intercepted traffic cannot be reconstructed into meaningful data without access to the encryption keys, which are never transmitted over the network. This encryption ensures **confidentiality**, **integrity**, and **authentication** of the data. In contrast, **Telnet** leaves the network vulnerable to eavesdropping, man-in-the-middle attacks, and **packet sniffing**.





## Secure Protocols

Attackers can penetrate a network's infrastructure through services, protocols, and open ports. Older protocols leave a network in a vulnerable position, so cybersecurity professionals need to make sure current protocols are being used.

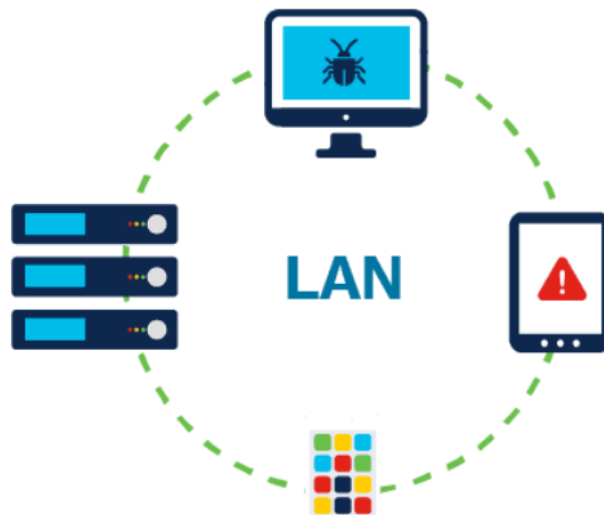
- **SNMP (Simple Network Management Protocol):** SNMP collects statistics from TCP/IP devices to monitor network and computer equipment. SNMPv3 is the current standard — it uses cryptography to prevent eavesdropping and make sure data hasn't been tampered with while in transit.
- **HTTP (Hypertext Transfer Protocol):** (HTTP) provides basic web connectivity and uses port 80. HTTP contains limited built-in security and is open to traffic monitoring when transmitting content, leaving the user's computer open to attack. Let's see how other protocols provide a more secure connection:
  - Secure Sockets Layer (SSL) manages encryption by using an SSL handshake at the beginning of a session to provide confidentiality and prevent eavesdropping and tampering.
  - Transport Layer Security (TLS) is an updated, more secure replacement for SSL.

- SSL/TLS encrypts communication between the client and the server. Where it's used, the user will see HTTPS in the URL field of a browser instead of HTTP.
- **File Transfer Protocol (FTP):** (FTP) transfers computer files between a client and a server. In FTP, the client uses a plaintext username and password to connect. File Transfer Protocol Secure (FTPS) is more secure — it adds support for TLS and SSL to prevent eavesdropping, tampering and forgery on exchanged messages.
- **POP, IMAP and MIME:** Email uses Post Office Protocol (POP), Internet Message Access Protocol (IMAP) and Multipurpose Internet Mail Extensions (MIME) to attach non-text data, such as an image or video, to an email message. To secure POP (port 110) or IMAP (port 143), use SSL/TLS to encrypt mail during transmission. The Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol provides a secure method of transmission. It sends digitally signed and encrypted messages that provide authentication, message integrity and nonrepudiation.

### Network Hardening: Segmentation

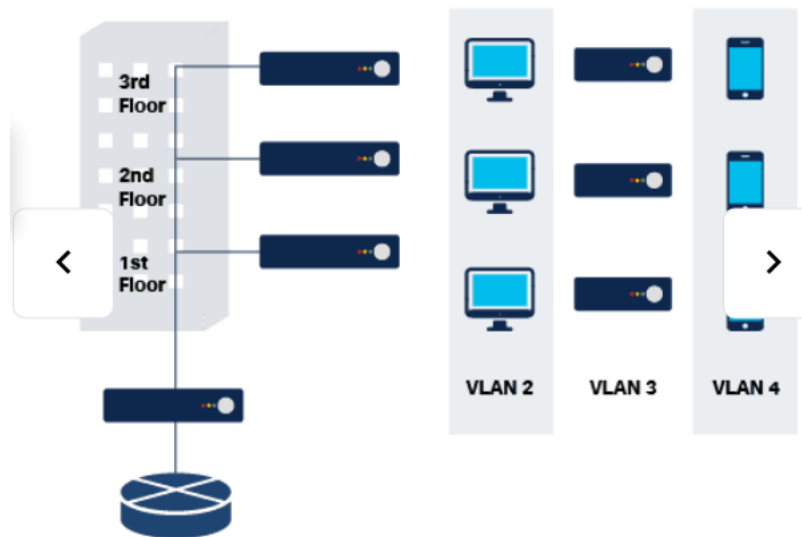
#### Virtual Local Area Networks (VLANs)

The @Company HR Manager is worried about protecting sensitive information about personnel that is stored on the network. Guru suggests using a virtual local area network, a VLAN, to segment the network and create a secure area for the sensitive data.

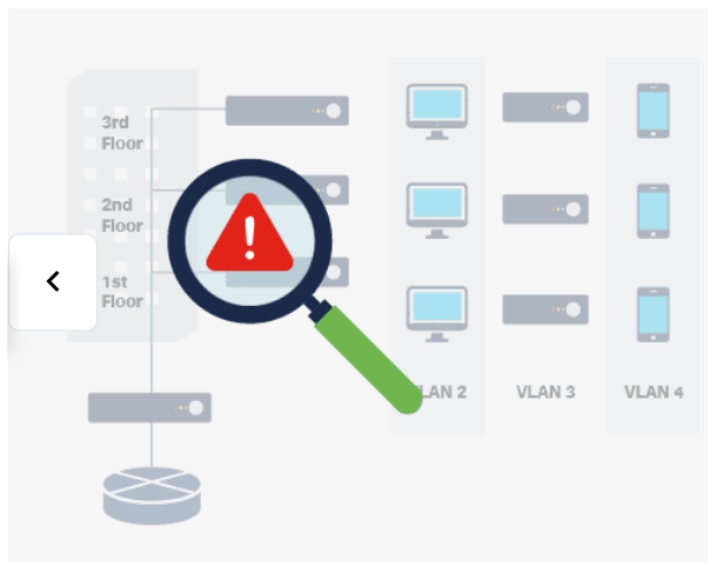


**Devices are grouped:** VLANs provide a way to group devices within a local area network (LAN) and on individual switches. VLANs are not the same as LANs: virtual LANs are based on logical connections, while LANs are based on physical connections. Individual ports on a switch can be assigned to a specific VLAN. Other ports can be used to physically interconnect switches and allow multiple VLAN traffic between switches. These ports are called trunks.





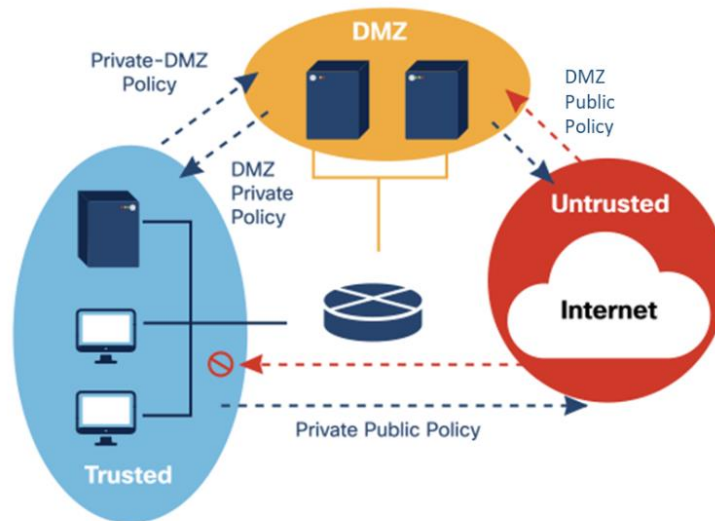
**The network is segmented:** VLANs allow an administrator to segment a network based on factors such as function, project team or application. Devices within a VLAN act as if they are in their own independent network, even though they share a common infrastructure with other VLANs on the same LAN. A VLAN can separate groups of devices that host sensitive data from the rest of the network, decreasing the chances of confidential information breaches — in our example, the HR department looking to protect sensitive data. Trunks allow individuals on the HR VLAN to be physically connected to multiple switches.



**Data is protected:** VLANs provide a way to limit broadcast traffic in a switched network. But beware; cybercriminals can attack VLAN performance and availability. To protect the VLAN, monitor its performance, use advanced configurations and regularly install patches and updates.

## The Demilitarized Zone (DMZ)

A demilitarized zone (DMZ) is a small network between a trusted private network and the Internet.



Let's find out how a DMZ works.

- **Access to Untrusted Networks:** Web servers and mail servers are usually placed within the DMZ to allow users to access an untrusted network, such as the Internet, without compromising the internal network.
- **Zones of Risk:** Most networks have two to four zones of risk: the trusted private LAN, the DMZ, the Internet and an extranet.
  - Within the LAN zone, the risk level is low, and the trust level is high.
  - Within the extranet zone, the risk level is medium-low, and the trust level medium-high.
  - Within the DMZ, the risk level is medium-high, and the trust level is medium-low.
  - Within the Internet zone, the risk level is high, and the trust level is low.
- **Zero Trust Model:** Firewalls manage east-west traffic (traffic that goes between servers within the organization's data center) and north-south traffic (data moving into and out of the organization's network). To protect its network, an organization can implement a **Zero Trust model**. Automatically trusting users and endpoints within the organization can put any network at risk, as trusted users can move throughout the network to access data. Zero Trust networking constantly monitors all users on the network regardless of their status or role

## Hardening Wireless and Mobile Devices

### Wireless Device Security

Wired Equivalent Privacy (WEP) was the first security protocol used for wireless networks. This was replaced by Wi-Fi Protected Access (WPA), which improved the security of wireless connections.

- **WPA configuration:** Wi-Fi Protected Access (WPA) was the computer industry's response to the weaknesses of the WEP standard. WPA-PSK (Pre-Shared Key) is the most common WPA configuration. The keys used by WPA are 256-bit, a significant increase over the 64-bit and 128-bit keys used in the WEP system.
- **WPA features:** The WPA standard provided several security improvements. First, WPA provided message integrity checks (MIC), which could detect if an attacker had captured and altered data passed between the wireless access point and a wireless client. Another key security enhancement was Temporal Key Integrity Protocol (TKIP). The TKIP standard helped to better handle, protect and change encryption keys. Advanced Encryption Standard (AES) superseded TKIP, for even better key management and encryption protection.
- **WPA2 (Wi-Fi Protected Access II):** The Wi-Fi Protected Access II (WPA2) standard was released in 2006. This introduced the mandatory use of AES algorithms and replaced TKIP with the Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP).
- **WPA3 (Wi-Fi Protected Access III):** WPA3 added more features to WPA2 such as maintaining strong cryptographic algorithms and improving key exchange.
- **WPS (Wi-Fi protected Setup):** (WPS) can be used to set up a secure wireless home network. A PIN code is used to connect devices to the wireless network. However, WPS poses major security vulnerability, as the user's PIN can be discovered through brute-force attack. Due to this, WPS should not be used and should be disabled altogether.

### Authentication

Wireless devices have become predominant on most modern networks. They provide mobility and convenience but are vulnerable to a range of cybersecurity issues. They are open to theft, hacking, unauthorized remote access, sniffing, man-in-the-middle attacks, as well as attacks against performance and availability.

The best way to secure a wireless network is to use **authentication** and **encryption**. The original wireless standard, **802.11**, introduced two types of authentication.

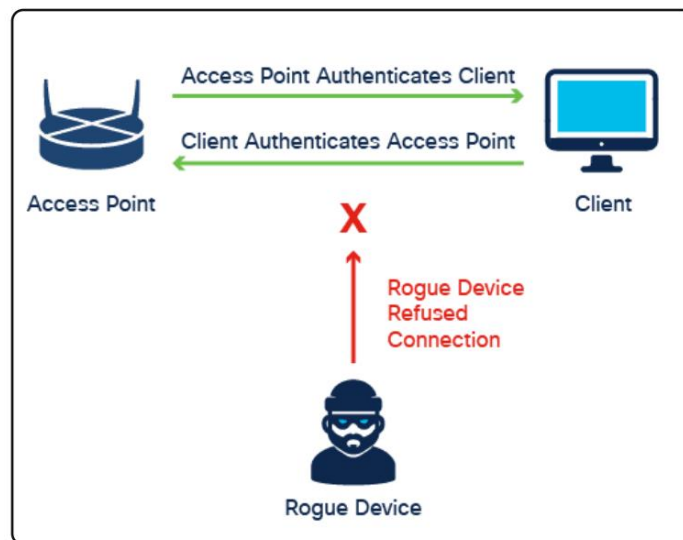
- **Open system authentication:** Any wireless device can connect to the wireless network. Use this method in situations
- **Shared key authentication:** provides mechanisms to authenticate and encrypt data between a wireless client and AP or wireless router

## Authentication Protocols

The Extensible Authentication Protocol (EAP) is an authentication framework used in wireless networks. Let's find out how it works.

1. The user requests to connect to the wireless network through an access point.
2. The access point requests identification data (username) from the user, which is then sent to an authentication server.
3. The authentication server requests proof that the ID is valid.
4. The access point requests proof that the ID is valid from the user, in the form of a password.
5. The user supplies the access point with their password. The access point sends this back to the authentication server.
6. The server confirms the username and password are correct, and passes this information on to the access point and user.
7. The user connects to the wireless network.

## Mutual Authentication



Your wireless network and its sensitive data are susceptible to unauthorized access by hackers using a wireless connection. But what can you do to prevent an attack?

- **Rogue access point:** An access point is any hardware device that enables other wireless devices to connect to a wired network. Any device that has a wireless transmitter and hardwired interface to a network can potentially act as a rogue or unauthorized access point. The rogue access point will often imitate an authorized access point, allowing users to connect to the wireless network but potentially stealing their data or conducting other nefarious activity in the process.

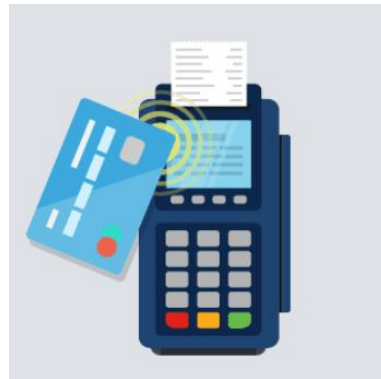
- **Preventing attacks:** When you connect to a rogue access point, the imposter who set it up can request and copy data from your device. This type of man-in-the-middle attack is very difficult to detect and can result in stolen login details and data. Mutual authentication is two-way authentication that can prevent rogue access points. It is a process in which both entities in a communications link authenticate each other before they connect. This enables clients to detect rogue access points and prevent such MitM attacks.

## Communication Methods

Let's take a closer look at how mobile devices connect and communicate.



**Wi-Fi and Bluetooth:** Mobile device can use wireless signals such as Wi-Fi and Bluetooth. You can configure wireless access



**NFC (Near-Field communication):** NFC allows contactless communication between devices. NFC chips uses electromagnetic fields to enable contactless payments, meaning. For instance, that you simply need to hold your device close to a payment terminal to process payment



**IR (Infrared):** infrared provides short-range communication using an IR receiver. For example, IR allows you to control your television through your cell phone.



**USB communication:** The only type of communication on this list that is wired. USB communications allows a mobile device to function as modem or fax. You can connect a mobile device to forensic acquisition devices via USB port if you need to gather information for an investigation

## Mobile Device Management

A mobile device issued by an organization can contain both personal and organizational data — it can be either corporate-owned or corporate-owned personally enabled (COPE).

An organization may also have a bring-your-own-device (BYOD) option. Security and data protection policies need to be applied when there is sensitive corporate information on a user's device.

**Let's look at some of the ways to manage mobile devices.**

- **Storage segmentation and containerization:** Storage segmentation and containerization allow you to separate personal and work content on a device. It provides an authenticated, encrypted area that separates sensitive company information from the user's personal data. Containerization also enables us to:
  - Isolate apps.
  - Control app functions.
  - Delete container information.
  - Remotely wipe the device.
- **Content management:** An organization needs to consider the security risks involved in using applications that share data — for example, Dropbox, Box, Google Drive and iCloud. An identity-management security system can be used to control what data a user can access.
- **Application management:** Whitelisting allows you to **digitally sign** applications so that you can authorize which applications users can install. This helps to ensure that installed applications come from a trusted source. Authentication using strong passwords is a best practice for those applications that require user credentials.

## Mobile Device Protections

Whether a mobile device is owned by the organization or is a personal device used for work, measures need to be put in place to keep it safe from cyber threats.

- **What are the risks?** Threats to mobile devices include:
  - Theft
  - Loss
  - Unauthorized access
  - Operating system risks
  - Application risks
  - Network risks
- **Jailbreaking, rooting and sideloading**
  - Jailbreaking, rooting and sideloading are ways of bypassing a device's limitations to do things that the device is restricted from doing. Users may try

to **jailbreak** (Apple devices) or **root** (Android devices) their device to run an app that is not authorized or available in the store. Jailbreaking removes the restriction that only Apple-authorized apps may run on the device. Rooting bypasses Android's security architecture to allow complete, administrative access to the device. Both pose a risk to the organization. Solutions are available that can detect a jailbroken or rooted device. A device is then marked as noncompliant and removed from the network or denied access to organizational apps.

- Third-party app stores can also pose a risk for organizations because the apps they provide access to have not been evaluated properly. **Sideload**ing occurs when the user goes around the approved app settings to install unapproved apps. This is less invasive than jailbreaking or rooting, but it is still a risk.
- **What are the safeguards?** Safeguards against mobile device threats include the following:
  - **Screen locks** require a password, PIN or pattern to access the device.
  - **Biometric authentication** uses a unique physical characteristic (fingerprint, face, iris or voice).
  - **Context-aware authentication** uses machine learning to determine access based on a user's normal behavior.
  - **Remote wiping** deletes the device's data should the device be stolen or lost.
  - **Full device encryption** can encrypt all data on a mobile device.

## GPS Tracking

Global Positioning System (GPS) uses satellites and computers to determine the location of a device. GPS technology is a standard feature on smartphones and provides real-time position tracking that can typically pinpoint a location to within approximately 5 meters.

Many cell phone apps use GPS tracking to track the phone's location. For example, Facebook allows users to check in to a location, which is then visible to people in their networks. Some apps use geofencing or geolocation, which use radio-frequency identification (RFID) to determine a geographic area instead.

Push notifications sometimes use geolocation and geofencing too. This enables local organizations to 'push' advertising messages based on a user's location settings. Unfortunately, increasingly savvy cyber attackers have started using push notifications to capture data.

### High Availability

The term ‘high availability’ describes systems designed to avoid downtime as much as possible. The continuous availability of information systems is imperative, not only to organizations but to modern life, as we are all using and relying on computer and information systems more than ever before.

High availability systems typically are based on three design principles.

- **Eliminating Single Points of Failure:** The first principle that defines high availability systems starts with identifying all system devices and components whose failure would result in system-wide failure. Methods to eliminate single points of failure include replacing or removing hot stand-by devices, redundant components and multiple connections or pathways.
- **Providing for Reliable Crossover:** Redundant power supplies, backup power systems and backup communications systems all provide for reliable crossover — the second design principle.
- **Detecting Failures as They Occur:** The third principle is active device and system monitoring to detect many types of events including system and device failures. Monitoring systems may even trigger the backup system in the case of failure.

### System and Data Backups

An organization can lose data if cybercriminals steal it, if equipment fails, or if a disaster or other error occurs, so it’s important to back up data regularly.

A data backup stores a copy of the information from a computer to backup media. When such media is removable, the operator then stores this backup media in a safe place.

Backing up data is one of the most effective ways of protecting against data loss. If the hardware fails, the user can restore the data from the backup once the system is functional again, or even when moving to a new system.

A sound security policy should include regular data backups. Backups are usually stored off-site to protect the data if anything happens to the main facility.

- **Frequency:** Backups can take a long time sometimes, it’s easier to make full backup monthly or weekly and then do frequent partial backup of any data that has changed since the last full backup. However, having many partial backups increases the amount of time needed to restore the data.
- **Storage:** For extra security, transport backups to an approved off-site storage location on daily, weekly or monthly rotations, as required by the security policy.



- **Security:** Protect backups with passwords. The operator will enter the password before restoring the data from the backup media.
- **Validation:** Always validate backups to ensure the integrity of the data.

### Managing Threats to Physical Facilities

Organizations can implement various measures to manage threats to the physical facilities. For example:

- Access Control and Closed-Circuit TV (CCTV - Video Surveillance) coverage at all entrances
- Policies and procedures for guests visiting the facility
- Building security testing, including using both digital and physical means to covertly gain access
- Badge encryption for entry access
- Disaster recovery planning
- Business continuity planning
- Regular security awareness training
- Asset tagging system

## Embedded and Specialized Systems

### Threats to Key Industry Sectors

Over the last decade, cyber attacks like Stuxnet proved that malware attacks could successfully destroy or interrupt critical infrastructures. The Stuxnet worm targeted Supervisory Control And Data Acquisition (SCADA) systems used to control and monitor industrial processes. SCADA and other Industrial Control Systems (ICSs) are used in manufacturing, production, energy and communications systems.

How cyber can attacks like these impact industry sectors and what action can be taken to prevent such attacks from occurring?

## Stuxnet

Stuxnet was a sophisticated computer worm that was discovered in 2010 and is widely considered one of the first cyber weapons to target industrial systems. It was specifically designed to sabotage Iran's nuclear enrichment facilities, particularly the centrifuges at the Natanz facility.

- **Target:** Stuxnet was specifically designed to target Siemens PLCs (programmable logic controllers), which were controlling industrial systems in Iran's nuclear plants, particularly the systems used to control uranium-enriching centrifuges.
- **How It Worked:** The worm was able to infiltrate the target systems by exploiting multiple zero-day vulnerabilities (previously unknown software flaws) in Windows. Once it infected the system, it would manipulate the PLCs to control the speed of the centrifuges, causing them to spin at speeds that would damage them, while simultaneously sending normal operating readings to monitoring systems. This ensured that the attacks remained undetected for a long time.
- **Deployment:** Stuxnet was most likely deployed via a USB drive, which was used to physically transfer the worm to the targeted systems. This was especially notable because it didn't rely on the internet to spread, making it more targeted and difficult to trace initially.
- **Origins and Attribution:** It is widely believed that Stuxnet was a joint operation between the United States and Israel, though neither country has officially confirmed this. The worm was highly sophisticated, indicating state-sponsored involvement with significant resources and expertise.
- **Impact:** Stuxnet caused substantial damage to Iran's nuclear program, damaging around 1,000 centrifuges at the Natanz facility, though the full extent of the damage is hard to quantify. It delayed Iran's nuclear progress by several years. The worm was also a major wake-up call regarding the vulnerability of critical infrastructure to cyber-attacks.
- **Significance:**
  - **Cyber Warfare:** Stuxnet marked the first time a cyber-attack was used for strategic military purposes, targeting physical infrastructure and causing physical damage.
  - **Cybersecurity Awareness:** It demonstrated how vulnerable industrial control systems and critical infrastructure can be to cyber-attacks, leading to significant investments in cybersecurity for such systems.
  - **Cyber-weapon Precedent:** Stuxnet set a dangerous precedent, showing that cyber-attacks could be used as tools of geopolitical conflict, potentially causing both direct and indirect consequences for national security.

- **Legacy:**
  - The Stuxnet attack accelerated the development of cybersecurity protocols for industrial control systems (ICS) and critical infrastructure.
  - It also introduced the concept of "cyber weapons" as part of national defense strategies, and heightened awareness of the potential of state-sponsored cyber-attacks.

## **How to Prevent Stuxnet-Like Attacks?**

To prevent attacks similar to Stuxnet, organizations must implement multi-layered cybersecurity strategies, particularly for critical infrastructure. Here are some key prevention steps:

- **Segment Networks:** Keep industrial control systems (ICS) and other critical infrastructure networks isolated from general IT networks. This "air-gapping" can prevent malware from spreading between systems. Even if one system is compromised, the infection cannot easily reach critical infrastructure.
- **Use Whitelisting:** Implement application whitelisting on all devices, especially those in industrial control systems. This ensures that only authorized software can be executed, blocking any malware or unapproved software, such as Stuxnet.
- **Regular Software and Firmware Updates:** Apply timely patches and updates to all systems, including industrial controllers and operating systems, to close security holes and vulnerabilities. Zero-day exploits like the ones used in Stuxnet can be mitigated by proactively patching known vulnerabilities.
- **USB Device Control:** Since Stuxnet was likely introduced via USB drives, it's essential to limit the use of USBs and other removable media. Employ policies to restrict and monitor their use, and consider using USB endpoint protection solutions that can detect and block malicious files.
- **Network Monitoring and Intrusion Detection Systems:** Set up robust network monitoring and intrusion detection systems (IDS) to spot unusual behavior, such as unexpected communications with external systems or anomalous device behavior. Early detection can help identify threats before they cause harm.
- **Employee Training and Awareness:** Educate employees, especially those working with critical infrastructure, about cybersecurity best practices. This includes awareness of phishing attacks, avoiding the use of unauthorized devices, and following secure protocols for handling sensitive systems.
- **Backup and Recovery Plans:** Ensure that robust backup and disaster recovery protocols are in place. Regular backups of critical data and systems can help recover from a cyber-attack or hardware failure. Data should be stored in multiple locations, including off-site, to safeguard against physical or cyber disasters.

- **Collaboration with Experts:** Work with cybersecurity experts and external auditors who can conduct vulnerability assessments and penetration testing. Regular reviews of your systems will identify weaknesses that could be exploited by attackers.
- **Encryption:** Encrypt sensitive data and communications to protect it from interception or manipulation. Even if attackers manage to access systems, encryption can prevent them from extracting or altering crucial information.

## **The Emergence of the Internet of Things**

The Internet of Things (IoT) is the collection of technologies that enable various devices to connect to the Internet. The technological evolution associated with IoT is changing commercial and consumer environments.

IoT technologies enable people to connect billions of devices, such as cars, industrial machines, robots, appliances, locks, motors, and entertainment devices, to name just a few. This technology affects the amount of data that needs to be protected. As users need to access these devices remotely, they are placed online, which increases the number of potential entry points to that local network in general.

Moreover, with the emergence of IoT, there is much more data to be managed and secured. All these devices, plus the expanded storage capacity and storage services offered through the cloud and virtualization, have led to the exponential growth of data. This data expansion created a new area of interest in technology and business called ‘Big Data.’

IoT devices greatly expand the cyber attack surface. In the IoT, thousands of new devices require access to networks in order to submit data and be managed and operated. Internet-connected smart devices have been infected with malware and used to launch some of the largest DDoS attacks in history. Therefore, IoT device security is extremely important. First, all IoT devices should be evaluated to ensure that they are able to update their firmware with security patches, preferably over wireless networks. In addition, default administrator credentials on these devices should always be changed from the default settings because these settings are publicly known.

## **Special-Purpose Embedded Systems**

Embedded systems work in a variety of industries. You can find special-purpose embedded devices in sectors such as the medical, automotive and aviation sectors.

- **Medical devices:** Devices such as pacemakers, insulin pumps, medical implants and defibrillators are capable of wireless connectivity, remote monitoring and Near-Field Communication (NFC). Vulnerabilities in these medical devices can lead to patient safety issues, medical record leaks or the risk of granting access to the network to cybercriminals, who will move through it in search of a target.

- **Automotive:** In-vehicle systems produce and store the data necessary for the operation of the vehicle along with its maintenance, safety protection and emergency contact transmission. Typically, a wireless interface connects to the Internet and to a diagnostic interface on board. Many vehicles record speed, location and braking maneuvers, and can then send the collected data to the driver's insurance company. Therefore, risks to in-vehicle communications include unauthorized tracking, wireless jamming and spoofing. To secure in-vehicle systems, implement the following countermeasures:
  - Secure system software design practices
  - Basic encryption for all communication between controllers
  - Firewall implementation
- **Aviation:** An aircraft has many embedded control systems such as its flight control system and communication system. Security issues include the use of hard-coded logon credentials, insecure protocols and backdoors. In the same category, Unmanned Aerial Vehicles (UAVs), more commonly called drones, have been used in military, agricultural and cartography applications, among others. Drones are very useful for aerial photography, surveillance and surveying. However, drones are susceptible to hijacking, Wi-Fi attacks, GPS spoofing attacks, jamming and deauthentication attacks, which can allow an attacker to intercept or disable a drone and access its data.

## **Access Control**

### **Physical access controls**

Physical access controls are actual barriers deployed to prevent direct physical contact with systems. The goal is to prevent unauthorized users from gaining physical access to facilities, equipment, and other organizational assets. For example, physical access control determines who can enter (or exit), where they can enter (or exit), and when they can enter (or exit). Here are some examples of physical access controls:

- Guards to monitor the facility
- Fences to protect the perimeter
- Motion detectors to detect moving objects
- Laptop locks to safeguard portable equipment
- Locked doors to prevent unauthorized access
- Swipe cards to allow access to restricted areas
- Guard dogs to protect the facility
- Video cameras to monitor a facility by collecting and recording images
- Mantrap-style entry systems to stagger the flow of people into the secured area and trap any unwanted visitors
- Alarms to detect intrusion

## Logical access controls

Logical access controls are the hardware and software solutions used to manage access to resources and systems. These technology-based solutions include tools and protocols that computer systems use for identification, authentication, authorization and accountability.

Logical access control examples include:

- Encryption is the process of taking plaintext and creating ciphertext.
- Smart cards have an embedded microchip.
- Passwords are protected strings of characters.
- Biometrics are users' physical characteristics.
- Access control lists (ACLs) define the type of traffic allowed on a network.
- Protocols are sets of rules that govern the exchange of data between devices.
- Firewalls prevent unwanted network traffic.
- Routers connect at least two networks.
- Intrusion detection systems monitor a network for suspicious activities.
- Clipping levels are certain allowed thresholds for errors before triggering a red flag.

## Administrative Access Controls

The concept of administrative access controls involves three security services: authentication, authorization and accounting (AAA). These services provide the primary framework to control access, preventing unauthorized access to a computer, network, database or other data resource.

- **Authentication**



Authentication verifies the identity of each user, to prevent unauthorized access. Users prove their identity with a username or ID. In addition, users need to verify their identity by providing one of the following:

- Something they know (such as a password)
- Something they have (such as a token or card)
- Something they are (such as a fingerprint)

In the case of two factor authentication, which is increasingly becoming the norm, the system requires a combination of two of the above rather than just one to verify someone's identity.

- **Authorization**



Authorization services determine which resources users can access, along with the operations that users can perform.

Some systems accomplish this by using an access control list, or an ACL. An ACL determines whether a user has certain access privileges once the user authenticates. Just because you can log onto the corporate network does not mean that you have permission to use the high-speed color printer, for example.

Authorization can also control *when* a user has access to a specific resource. For example, employees may have access to a sales database during work hours, but the system locks them out afterhours.

- **Accounting**



Not related to financial accounting, accounting in AAA keeps track of what users do — including what they access, the amount of time they access resources, and any changes they make.

For example, a bank keeps track of each customer account. An audit of that system can reveal the time and amount of all transactions and the employee or system that executed the transactions. Cybersecurity accounting services work the same way. The system tracks each data transaction and provides auditing results. System administrators can set up computer policies to enable system auditing.

The concept of AAA is like using a credit card. The credit card identifies who can use it, how much that user can spend and accounts for items or services the user purchased.

Cybersecurity accounting tracks and monitors in real time.

### **Federated Identity Management**



Federated identity management refers to multiple enterprises that let their users use the same identification credentials to gain access to the networks of all enterprises in the group.

Unfortunately, this broadens the scope and increases the probability of a cascading effect should an attack occur.

Generally speaking, a federated identity links a subject's electronic identity across separate identity management systems, such as being able to access several websites using the same social login credentials.

The goal of federated identity management is to share identity information automatically across castle boundaries. From the individual user's perspective, this means a single sign-on to the web.

It is imperative that organizations scrutinize the identifying information shared with partners, even within the same corporate group, for example. The sharing of social security numbers, names, and addresses may allow identity thieves the opportunity to steal this information from a partner to perpetrate fraud. The most common way to protect federated identity is to tie login ability to an authorized device.



## Authentication Methods

As we mentioned earlier, users prove their identity with a username or ID. In addition, users need to verify their identity by providing one of the following.

- **What you know**



Passwords, passphrases or PINs are all examples of something that the user *knows*. Passwords are the most popular method used for authentication.

The terms passphrase, passcode, passkey and PIN are all generically referred to as password. A password is a string of characters used to prove a user's identity. If this string of characters relates back to a user (for instance, if it is their name, birthdate or address), it will be easier for cybercriminals to guess this user's password.

Several publications recommend that a password be at least eight characters. Users should not create a password that is so long that it is difficult to memorize, or conversely, so short that it becomes vulnerable to password cracking. Passwords should contain a combination of upper and lowercase letters, numbers, and special characters.

Users need to use different passwords for different systems because if a criminal cracks the user's password once, the criminal will have access to all of the user's accounts. A password manager can help you create and use strong passwords — and means that you do not have to remember each of these passwords, either.

- **What you have**



Smart cards and security key fobs are both examples of something that users have in their possession that can be used for authentication purposes.

A smart card is a small plastic card, about the size of a credit card, with a small chip embedded in it. The chip is an intelligent data carrier, capable of processing, storing and safeguarding data.

Smart cards contain private information, such as bank account numbers, personal identification, medical records and digital signatures, using encryption to keep data safe while providing a means to authenticate.

A security key fob is a device that is small enough to attach to a keyring. In most cases, security key fobs are used for two factor authentication (2FA), which is much more secure than a username and password combination.

For example, let's say you want to access your e-banking, which uses two factor authentication. First, you enter your username (identification). Then, the password, which is your first authentication factor. Then, you need a second one, because it's 2FA. You enter a PIN or card to your security fob, and it displays a number. Proving that you have access to this device, which was issued to you, this number is the second factor, which you then enter to log in to the e-banking account, in this example.

- **Who are you**



Unique physical characteristics, such as a fingerprint, retina or voice, which identify a specific person, are called biometrics. Biometric security compares physical characteristics against stored profiles to authenticate users. In this case, a profile is a data file containing known characteristics of an individual. The system grants the user access if their characteristics match saved settings. A fingerprint reader is a common biometric device.

There are two types of biometric identifiers:

- **Physiological characteristics** — fingerprints, DNA, face, hands, the retina or ear features.
- **Behavioral characteristics** — patterns of behavior such as gestures, voice, gait or typing rhythm.

Biometrics is becoming increasingly popular in public security systems, consumer electronics and point-of-sale applications. Implementing biometrics involves a reader or scanning device, software that converts the scanned information into digital form and a database that has biometric data stored for comparison.

## Multi-Factor Authentication

As we've touched upon earlier, multi-factor authentication uses at least two methods of verification — such as a password and something you have, for example, a security key fob. This can be taken a step further by adding something you are, such as a fingerprint scan.

Multi-factor authentication can reduce the incidence of online identity theft because it means knowing a password will not give cybercriminals access to a user's account.

For example, an online banking website might require a password and a one-off PIN that the user receives on his or her smartphone. In this case, your first factor is your password, and your second factor is the temporary PIN, because it proves you have access to what is registered as your phone.

Withdrawing cash from an ATM is another, simple example of multi-factor authentication, as the user must have the bank card as well as know the PIN before the ATM will dispense cash.

Note that two-factor authentication (2FA) is a method of multi-factor authentication that entails two factors in particular, but the two terms are often used interchangeably.

## Authorization

Authorization controls what a user can and cannot do on the network after successful authentication. After a user proves their identity, the system checks to see what network resources the user can access and what they can do with the resources.

- **When to implement authorization:** Authorization uses a set of attributes that describes the user's access to the network, to answer the question, 'What read, copy, edit, create and delete privileges does this user have?' The system compares these attributes to the information contained within the authentication database, determines a set of restrictions for that user, and delivers it to the local device where the user is connected. Authorization is automatic and does not require users to perform additional steps after authentication. System administrators have set the network up to implement authorization immediately after the user authenticates.
- **Using authorization:** Defining authorization rules is the first step in controlling access. An authorization policy establishes these rules. A group membership policy defines authorization based on users' membership in a specific group. All employees of an organization may have a swipe card, for example, which provides access to the premises, but it might not allow access to a server room. It may be that only senior-level employees and IT team members may access the server room with their swipe cards. An authority-level policy defines access permissions based on an employee's position within the organization.

## **Implementing Accountability**

Accountability traces an action back to a person or process making this change to a system. Accountability then collects this information and reports the usage data. The organization can use this data for such purposes as auditing or billing. The collected data might include the log-in time for a user, whether the user login was a success or failure, or what network resources the user accessed. This allows an organization to trace actions, errors and mistakes during an audit or investigation.

Implementing accountability consists of technologies, policies, procedures and education. Log files provide detailed information based on the parameters chosen. For example, an organization may look at the log for login failures and successes. Login failures can indicate that a criminal tried to hack an account, and login successes tell an organization which users are using what resources and when.

The organization's policies and procedures spell out what actions should be recorded and how the log files are generated, reviewed and stored.

Data retention, media disposal and compliance requirements all provide accountability. Many laws require the implementation of measures to secure different data types. These laws guide an organization on the right way to handle, store and dispose of data. The education and awareness of an organization's policies, procedures and related laws can also contribute to accountability.

## **Access control concepts**

### **Zero Trust Security**

Zero trust is a comprehensive approach to securing all access across networks, applications, and environments. This approach helps secure access from users, end-user devices, APIs, IoT, micro services, containers, and more. It protects an organization's workforce, workloads, and the workplace. The principle of a zero trust approach is, "never trust, always verify." Assume zero trust any time someone or something requests access to assets. A zero trust security framework helps to prevent unauthorized access, contain breaches, and reduce the risk of an attacker's lateral movement through a network.

Traditionally, the network perimeter, or edge, was the boundary between inside and outside, or trusted and untrusted. In a Zero trust approach, any place at which an access control decision is required should be considered a perimeter. This means that although a user or other entity may have successfully passed access control previously, they are not trusted to access another area or resource until they are authenticated. In some cases, users may be required to authenticate multiple times and in different ways, to gain access to different layers of the network.

The three pillars of zero trust are workforce, workloads, and workplace.

- **Zero trust for the workforce:** This pillar consists of people (e.g., employees, contractors, partners, and vendors) who access work applications by using their personal or corporate-managed devices. This pillar ensures only the right users and secure devices can access applications, regardless of location.
- **Zero trust for workloads:** This pillar is concerned with applications that are running in the cloud, in data centers, and other virtualized environments that interact with one another. It focuses on secure access when an API, a microservice, or a container is accessing a database within an application.
- **Zero trust for the workplace:** This pillar focuses on secure access for any and all devices, including on the internet of things (IoT), that connect to enterprise networks, such as user endpoints, physical and virtual servers, printers, cameras, HVAC systems, kiosks, infusion pumps, industrial control systems, and more.

### Network Access Control (NAC) Systems

Network access control (NAC) systems support access management by enforcing organizational policies regarding the people and devices that are attempting to access the network. NAC systems allow cybersecurity professionals to monitor the users and devices that are attached to the network, and manually control access as required.

Network access control systems provide the following capabilities:

- Rapidly enforcing access policies that have been created for different operational conditions.
- Recognizing and profiling connected users and devices to prevent malicious software on non-compliant systems from causing damage.
- Providing secure access to network guests, often through registration portals.
- Evaluating device compliance with security policies by user type, device type, and operating system prior to permitting network access.
- Mitigating security incidents by blocking, isolating, or repairing non-compliant devices.

Because BYOD and IoT networking greatly expand the network attack surface, NAC system automation features make focused control of network access by such devices practical. The NAC system is configured to enforce organizational policies. The relevant policies are enacted to permit or deny network access according to a wide range of factors that the NAC system detects on the devices that are attempting access. Without NAC systems it would be impossible for cybersecurity personnel to evaluate the thousands of devices that could attempt to access the network.

NAC is an important component of a zero-trust security architecture that enforces security policy compliance with all devices and users that attempt to access the network.

## **Account Management**

- **Account Types**

An organization should not share accounts for privileged users, administrators or applications. The administrator account should only be used to administer a system. If a user accesses a malware-infected website or opens a malicious email while using the administrator account, this would put the organization at risk.

Administrators must be aware of the default group and user accounts that might be installed by an operating system. Knowing about these accounts will help an administrator decide which should be permitted and which of these accounts should be disabled.

This is because default accounts such as the guest or administrator account can be a security risk in older systems as attackers are familiar with the default settings used. To improve security, always replace any default accounts and make sure that all account types require a password.

- **Privileged Accounts**

Cybercriminals target privileged accounts. Why? Because these are the most powerful accounts in the organization with elevated, unrestricted access to systems. Administrators use these accounts to deploy and manage operating systems, applications, and network devices.

Organizations should adopt robust practices for securing privileged accounts:

- Identify and reduce the number of privileged accounts.
- Enforce the principle of least privilege. The principle means that users, systems, and processes only have access to resources (networks, systems, and files) that are absolutely necessary to perform their assigned function.
- Revoke access rights when employees leave or change jobs.
- Eliminate shared accounts with passwords that do not expire.
- Secure password storage.
- Eliminate shared credentials for multiple administrators.
- Automatically change privileged account passwords every 30 or 60 days.
- Record privileged sessions.
- Implement a process to change embedded passwords for scripts and service accounts.
- Log all user activity.
- Generate alerts for unusual behavior.
- Disable inactive privileged accounts.
- Use multi-factor authentication for all administrative access.
- Implement a gateway between the end user and sensitive assets to limit network exposure to malware.

Continuously securing and locking down privileged accounts is critical to the security of the organization. Regularly evaluate this process and make adjustments to improve protection.

## **File Access Control**

Let's take a closer look at how **permissions** can help secure data.

Permissions are rules configured to limit folder or file access for an individual or a group. Users should be limited to only the resources they need on a computer system or network. For example, they should not be able to access all files on a server if they only need access to a single folder. It may be easier to provide access to the entire drive, but it is more secure to limit access to only the folder they need. This is the principle of **least privilege** and closely connected to the concept of 'need to know' access. Limiting access to resources also prevents cybercriminals from accessing those resources if the user's computer becomes infected.

- **Full Control:** Users can:
  - See the contents of a file or folder.
  - Change and delete existing files and folders.
  - Create new files and folders.
  - Run programs in a folder.
- **Modify:** Users can:
  - Change and delete existing files and folders.
  - Cannot create new ones.
- **Read and Execute:** Users can:
  - See the contents of existing files and folders.
  - Run programs in a folder.
- **Write:** Users can:
  - Create new files and folders.
  - Make changes to existing files and folders.
- **Read:** Users can:
  - View the contents of files and folders but cannot make any changes.

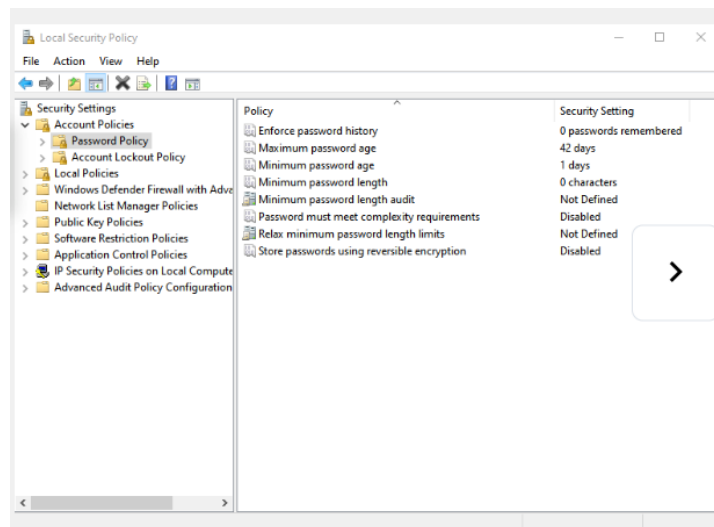
## Account Policies in Windows

In most networks that use Windows computers, an administrator configures **Active Directory** with domains on a Windows server. Windows computers that join the domain become domain members.

The administrator configures a **domain security policy** that applies to all domain members. For example, account policies are automatically set when a user logs in to Windows.

When a computer is not part of an Active Directory domain, the user configures policies through **Windows Local Security Policy**. In all versions of Windows except Home edition, enter 'secpol.msc' at the Run command to open the **Local Security Policy** tool.

- **Password Policy**



An administrator can configure user account policies such as **password policies** and **lockout policies**. In the example shown, users must:

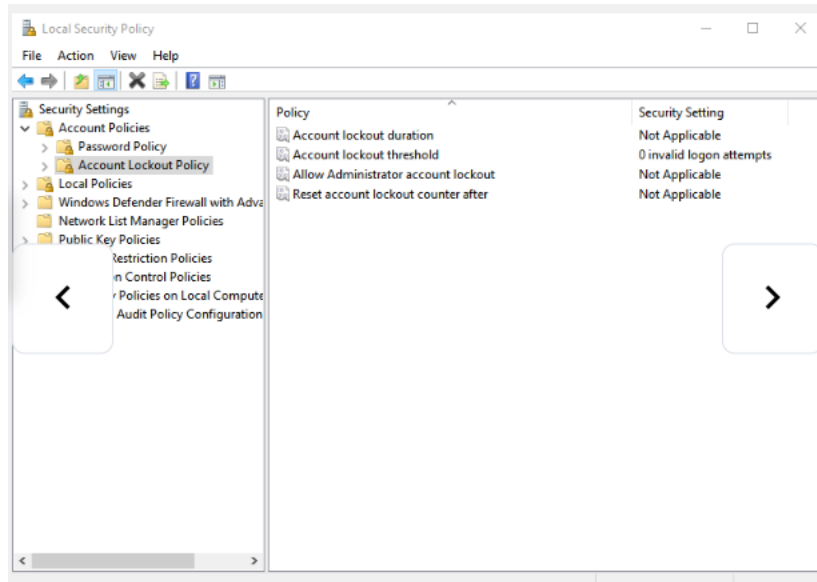
- Change their passwords every **90 days**.
- Use each new password for at least **one day**.
- Passwords must contain at least **eight characters** and meet at least **three of the following four categories**:
  - Uppercase letters
  - Lowercase letters
  - Numbers
  - Symbols

Lastly, the user can **reuse a password** after **24 unique passwords**.

This is just an example; different password policies can be set, depending on organizational requirements and needs.



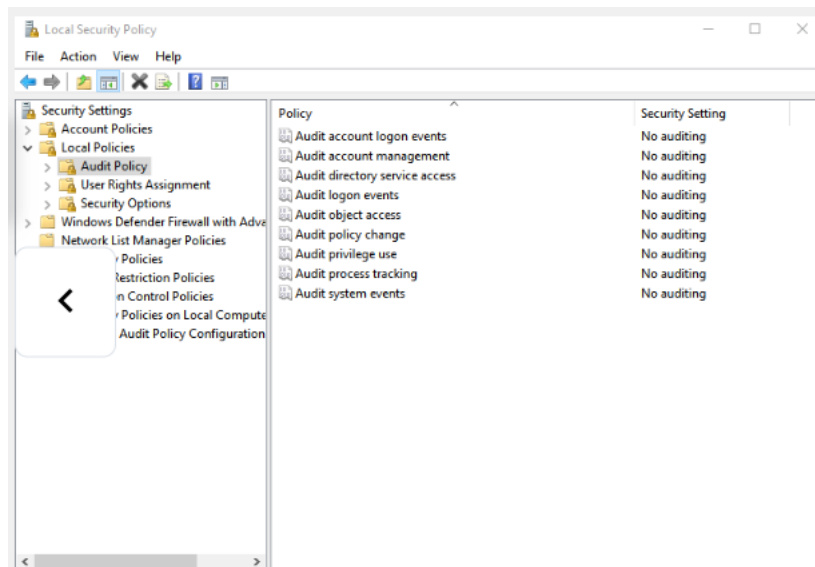
- **Account Lockout Policy**



An **account lockout policy** locks an account for a set duration when too many incorrect login attempts occur.

For example, the policy shown here allows the user to enter the wrong username and/or password **five times**. After five attempts, the account **locks users out for 30 minutes**. After 30 minutes, the number of attempts resets to zero, and the user can attempt to log in again.

- **Audit Policies**



More security settings are available by selecting the '**Local Policies**' folder in Windows. An **audit policy** creates a security log file used to track the following events:

- **Account logon events**
- **Audit account management**
- **Directory service access**
- **Object access**
- **Policy changes**
- **Privilege use**
- **Process tracking**
- **System events**

These logs help monitor and track user activity, system changes, and potential security issues, making them an essential part of system auditing and maintaining security within the network.

## Authentication Management

Authentication and authorization issues include unencrypted credentials, incorrect permissions and access violations. But how do you keep cybercriminals out while still making it easy for authorized users to log in? Authentication management aims to ensure secure sign in while still providing ease of use.

- A **Single Sign On (SSO) solution** allows the user to use one set of login credentials to authenticate across multiple applications. This way, the user only needs to remember one strong password.
- **OAuth** is a standard that enables a user's account information to be used by third-party services such as Facebook or Google.
- A **password vault** can protect and store the user's credentials with a single strong password required to access them.
- Many organizations implement **Knowledge-Based Authentication (KBA)** to provide a password reset should a user forget their password. KBA is based on personal information known by the user or a series of questions.

## Hash-Based Message Authentication Code (HMAC)

**Hash-Based Message Authentication Code (HMAC)** uses an encryption key with a hash function to authenticate a web user. Many web services use basic authentication, which does not encrypt the username and password during transmission. Using HMAC, the user sends a private key identifier and an HMAC. The server looks up the user's private key and creates an HMAC. The user's HMAC must match the one calculated by the server.

VPNs using **IPsec** rely on HMAC functions to authenticate the origin of every packet and provide **data integrity** checking.



## Applications of Cryptographic Hash Functions

As we have seen previously, cryptographic hash functions help us to ensure data integrity and verify authentication. Cryptographic hash functions are used in the following situations:

- To provide proof of authenticity when used with a symmetric secret authentication key such as IP security (IPsec) or routing protocol authentication.
- To provide authentication by generating one-time and one-way responses to challenges in authentication protocols.
- To provide message integrity check proof (such as those used in digitally signed contracts) and Public Key Infrastructure (PKI) certificates (like those accepted when accessing a secure website).

When choosing a hashing algorithm, use SHA-256 or higher, as they are currently the most secure. Avoid SHA-1 and MD5 due to security flaws that have been discovered.

## Access Control Strategies

Access control strategies enable an organization to grant or restrict access to a network device or data.

- **Mandatory Access Control:** Mandatory access control restricts the actions that a user can perform on an object (such as a file, a port, or a device). An authorization rule enforces whether a user can access the object. Organizations use mandatory access control where different levels of security classifications exist. Every object has a label, and every user has a clearance. A mandatory access control system restricts a user based on the security classification of the object and the label attached to the user.
- **Discretionary Access Control:** In systems that employ discretionary access controls, the owner of an object can decide which users can access that object and what specific access they may have. Permissions and access control lists can be used to implement discretionary access control. The owner of a file can specify what permissions (such as read, write, or execute) other users may have. An access control list uses rules to determine what traffic can enter or exit a network.
- **Role-Based Access Control:** Role-based access control depends on the role or job function of the user. Specific rules require permissions to perform certain operations, and users acquire permissions through their role. Role-based access control can work in combination with discretionary access controls or mandatory access controls by enforcing the policies of either one. Role-based access control helps to implement security administration in large organizations with hundreds of users and thousands of possible permissions. Organizations widely accept the use of role-based access control to manage computer permissions within a system, or application, as a best practice.

- **Rule-Based Access Control:** Rule-based access control uses access control lists to help determine whether to grant access. A series of rules is contained in the access control list and the decision to grant access depends on these rules. For example, a rule stating that no employee may have access to the payroll file after hours or on weekends. As with mandatory access control, users cannot change the access rules. Importantly, organizations can combine rule-based access control with other strategies for implementing access restrictions. For example, mandatory access control methods can utilize a rule-based approach for implementation.

## **AAA usage and operation**

### **A. AAA Operation**

A network must be designed to control who is allowed to connect to it and what they are allowed to do when they are connected. These design requirements are identified in the network security policy. The policy specifies how network administrators, corporate users, remote users, business partners, and clients access network resources. The network security policy can also mandate the implementation of an accounting system that tracks who logged in and when and what they did while logged in. Some compliance regulations may specify that access must be logged and the logs retained for a set period of time.

The Authentication, Authorization, and Accounting (AAA) protocol provides the necessary framework to enable scalable access security.

The three independent security functions provided by the AAA architectural framework:

#### **Authentication**

- Users and administrators must prove that they are who they say they are.
- Authentication can be established using username and password combinations, challenge and response questions, token cards, and other methods.
- AAA authentication provides a centralized way to control access to the network.

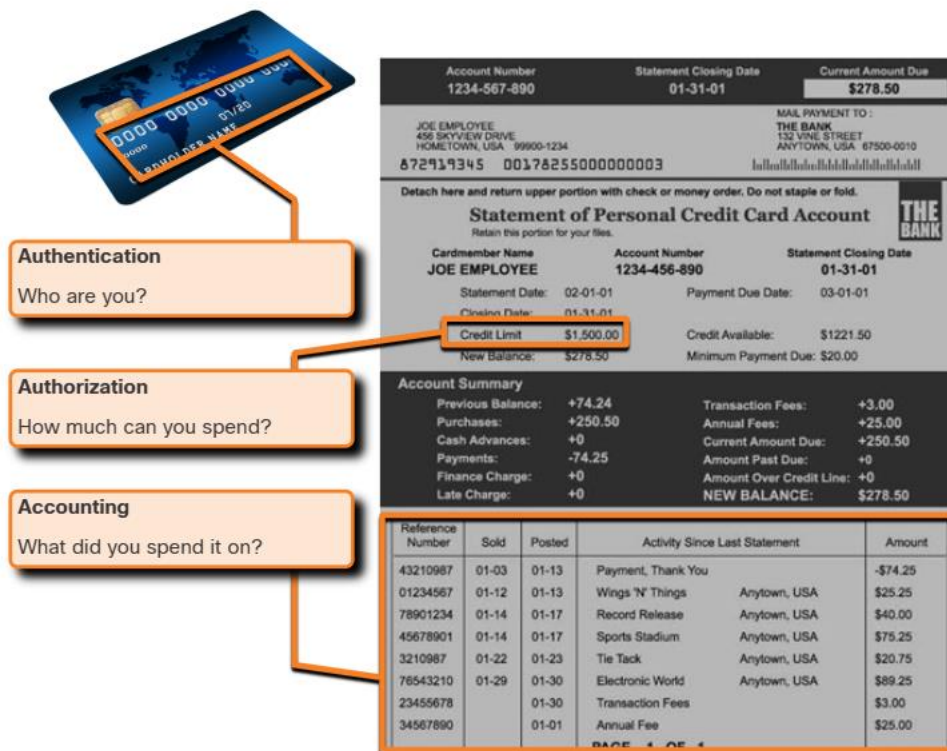
#### **Authorization**

- After the user is authenticated, authorization services determine which resources the user can access and which operations the user is allowed to perform.
- An example is “User ‘student’ can access host server XYZ using SSH only.”

#### **Accounting**

- Accounting records what the user does, including what is accessed, the amount of time the resource is accessed, and any changes that were made.
- Accounting keeps track of how network resources are used.
- An example is "User 'student' accessed host server XYZ using SSH for 15 minutes." This concept is similar

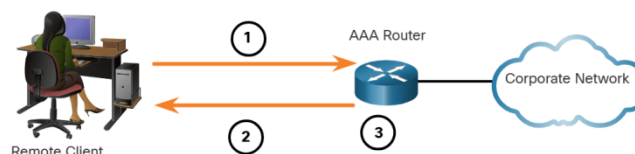
This concept is similar to the use of a credit card, as indicated by the figure. The credit card identifies who can use it, how much that user can spend, and keeps account of what items the user spent money on.



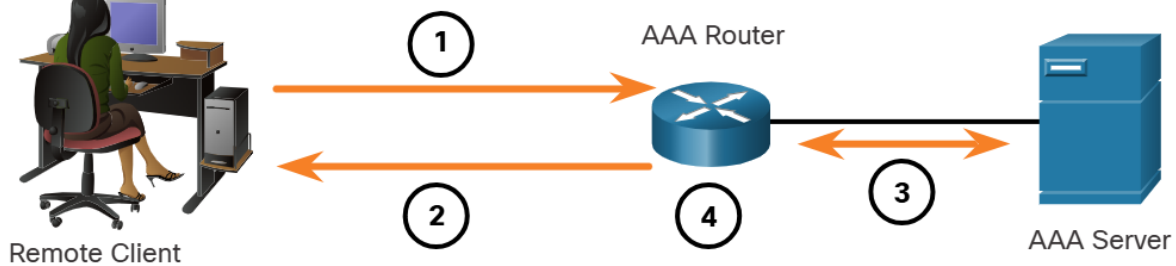
## B. AAA Authentication

AAA Authentication can be used to authenticate users for administrative access or it can be used to authenticate users for remote network access.

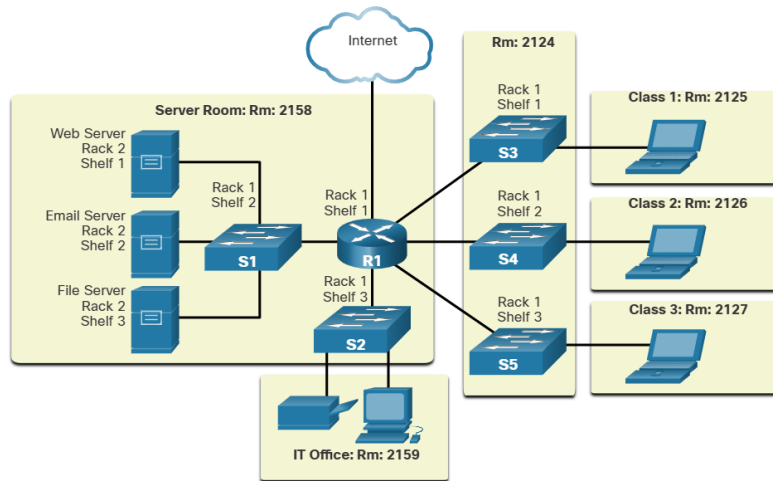
- **Local AAA Authentication:** This method is sometimes known as self-contained authentication because it authenticates users against locally stored usernames and passwords, as shown in the figure. Local AAA is ideal for small networks.



- **Server-based AAA Authentication:** This method authenticates against a central AAA server that contains the usernames and passwords for all users, as shown in the figure. Server-based AAA authentication is appropriate for medium-to-large networks.



### C. AAA Accounting Logs



Centralized AAA also enables the use of the Accounting method. Accounting records from all devices are sent to centralized repositories, which simplifies auditing of user actions.

AAA Accounting collects and reports usage data in AAA logs. These logs are useful for security auditing. The collected data might include the start and stop connection times, executed commands, number of packets, and number of bytes.

One widely deployed use of accounting is to combine it with AAA authentication. This helps with managing access to internetworking devices by network administrative staff. Accounting provides more security than just authentication. The AAA servers keep a detailed log of exactly what the authenticated user does on the device, as shown in the figure. This includes all EXEC and configuration commands issued by the user. The log contains numerous data fields, including the username, the date and time, and the actual command that was entered by the user. This information is useful when troubleshooting devices. It also provides evidence against individuals who perform malicious actions.

1. When a user has been authenticated, the AAA accounting process generates a start message to begin the accounting process.
2. When the user finishes, a stop message is recorded and the accounting process ends.

## **Access Control Lists**

### **What is an ACL?**

Routers make routing decisions based on information in the packet header. Traffic entering a router interface is routed solely based on information within the routing table. The router compares the destination IP address with routes in the routing table to find the best match and then forwards the packet based on the best match route. That same process can be used to filter traffic using an access control list (ACL).

An ACL is a series of IOS commands that are used to filter packets based on information found in the packet header. By default, a router does not have any ACLs configured. However, when an ACL is applied to an interface, the router performs the additional task of evaluating all network packets as they pass through the interface to determine if the packet can be forwarded.

An ACL uses a sequential list of permit or deny statements, known as access control entries (ACEs).

**Note:** ACEs are also commonly called ACL statements.

When network traffic passes through an interface configured with an ACL, the router compares the information within the packet against each ACE, in sequential order, to determine if the packet matches one of the ACEs. This process is called packet filtering.

Several tasks performed by routers require the use of ACLs to identify traffic. The table lists some of these tasks with examples.

- **Limit network traffic to increase network performance**
  - A corporate policy prohibits video traffic on the network to reduce the network load.
  - A policy can be enforced using ACLs to block video traffic.
- **Provide traffic flow control**
  - A corporate policy requires that routing protocol traffic be limited to certain links only.
  - A policy can be implemented using ACLs to restrict the delivery of routing updates to only those that come from a known source.

- **Provide a basic level of security for network access**
  - Corporate policy demands that access to the Human Resources network be restricted to authorized users only.
  - A policy can be enforced using ACLs to limit access to specified networks.
- **Filter traffic based on traffic type**
  - Corporate policy requires that email traffic be permitted into a network, but that Telnet access be denied.
  - A policy can be implemented using ACLs to filter traffic by type.
- **Screen hosts to permit or deny access to network services**
  - Corporate policy requires that access to some file types (e.g., FTP or HTTP) be limited to user groups.
  - A policy can be implemented using ACLs to filter user access to services.
- **Provide priority to certain classes of network traffic**
  - Corporate traffic specifies that voice traffic be forwarded as fast as possible to avoid any interruption.
  - A policy can be implemented using ACLs and QoS services to identify voice traffic and process it immediately.

## Packet filtering

**Packet filtering** controls access to a network by analyzing the incoming and/or outgoing packets and forwarding them or discarding them based on given criteria.

Packet filtering can occur at **Layer 3 (Network layer)** or **Layer 4 (Transport layer)**, as shown in the figure.

- **Layer 3 (Network Layer):** At this layer, packet filtering is based on **IP addresses, subnets, and routing information**. It focuses on the source and destination IP addresses and decides whether to allow or block traffic based on these attributes.
- **Layer 4 (Transport Layer):** At this layer, packet filtering also considers **port numbers** (for protocols like TCP or UDP) in addition to IP addresses. This allows more specific control over traffic based on service types, like allowing HTTP (port 80) while blocking FTP (port 21).

By applying these filters, network security can be enhanced by limiting unwanted traffic and permitting only authorized communications.

## Cisco routers support two types of ACLs:

- **Standard ACLs** - ACLs only filter at Layer 3 using the source IPv4 address only.
- **Extended ACLs** - ACLs filter at Layer 3 using the source and/or destination IPv4 address. They can also filter at Layer 4 using TCP, UDP ports, and optional protocol type information for finer control.



## ACL Operation



ACLs define the set of rules that give added control for packets that enter inbound interfaces, packets that relay through the router, and packets that exit outbound interfaces of the router.

**Note:** ACLs do not act on packets that originate from the router itself.

An inbound ACL filters packets before they are routed to the outbound interface. An inbound ACL is efficient because it saves the overhead of routing lookups if the packet is discarded. If the packet is permitted by the ACL, it is then processed for routing. Inbound ACLs are best used to filter packets when the network attached to an inbound interface is the only source of packets that need to be examined.

An outbound ACL filters packets after being routed, regardless of the inbound interface. Incoming packets are routed to the outbound interface and then they are processed through the outbound ACL. Outbound ACLs are best used when the same filter will be applied to packets coming from multiple inbound interfaces before exiting the same outbound interface.

When an ACL is applied to an interface, it follows a specific operating procedure. For example, here are the operational steps used when traffic has entered a router interface with an inbound standard IPv4 ACL configured:

1. The router extracts the source IPv4 address from the packet header.
2. The router starts at the top of the ACL and compares the source IPv4 address to each ACE in a sequential order.
3. When a match is made, the router carries out the instruction, either permitting or denying the packet, and the remaining ACEs in the ACL, if any, are not analyzed.
4. If the source IPv4 address does not match any ACEs in the ACL, the packet is discarded because there is an implicit deny ACE automatically applied to all ACLs.

The last ACE statement of an ACL is always an implicit deny that blocks all traffic. By default, this statement is automatically implied at the end of an ACL even though it is hidden and not displayed in the configuration.

**Note:** An ACL must have at least one permit statement otherwise all traffic will be denied due to the implicit deny ACE statement.

## Firewall technologies

**Firewall Technologies** are security systems designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. They act as a barrier between trusted internal networks and untrusted external networks, such as the internet, preventing unauthorized access and potential threats. Firewalls can be hardware-based, software-based, or a combination of both.

### Common Firewall Properties

- Firewalls are resistant to network attacks.
- Firewalls are the only transit point between internal corporate networks and external networks because all traffic flows through the firewall.
- Firewalls enforce the access control policy.

### Firewall Benefits

- They prevent the exposure of sensitive hosts, resources, and applications to untrusted users.
- They sanitize protocol flow, which prevents the exploitation of protocol flaws.
- They block malicious data from servers and clients.
- They reduce security management complexity by off-loading most of the network access control to a few firewalls in the network.

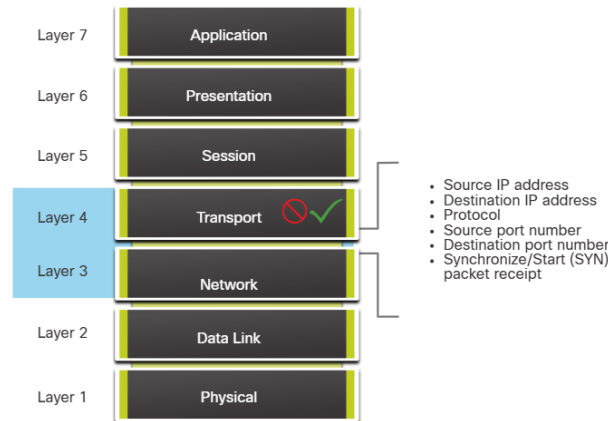
### Firewall Limitations

- A misconfigured firewall can have serious consequences for the network, such as becoming a single point of failure.
- The data: from many applications cannot be passed over firewalls securely.
- Users might proactively search for ways around the firewall to receive blocked material, which exposes the network to potential attack.
- Network performance can slow down.
- Unauthorized traffic can be tunneled or hidden as legitimate traffic through the firewall.

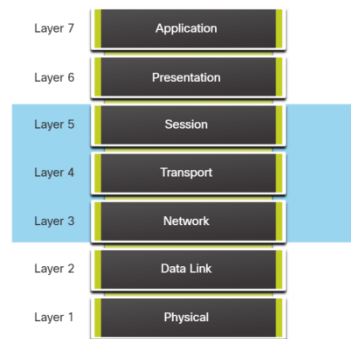
### Types of Firewall

1. **Packet Filtering (Stateless) Firewall:** Packet filtering firewalls are usually part of a router firewall, which permits or denies traffic based on Layer 3 and Layer 4 information. They are stateless firewalls that use a simple policy table look-up that filters traffic based on specific criteria. Packet filtering firewalls are usually part of a router firewall, which permits or denies traffic based on Layer 3 and Layer 4 information. They are stateless firewalls that use a simple policy table look-up that filters traffic based on specific criteria. For example, SMTP servers listen to port 25 by default. An administrator can

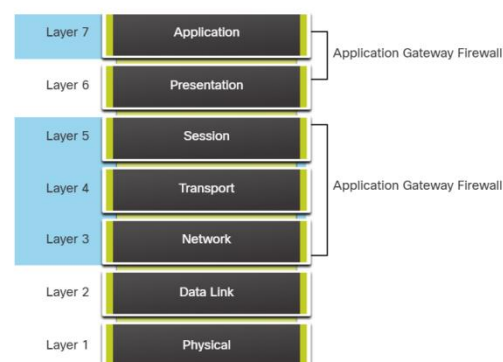
configure the packet filtering firewall to block port 25 from a specific workstation to prevent it from broadcasting an email virus.



2. **Stateful firewall:** Stateful firewalls are the most versatile and the most common firewall technologies in use. Stateful firewalls provide stateful packet filtering by using connection information maintained in a state table. Stateful filtering is a firewall architecture that is classified at the network layer. It also analyzes traffic at OSI Layer 4 and Layer 5.



3. **Application Gateway Firewall:** An application gateway firewall (proxy firewall), as shown in the figure, filters information at Layers 3, 4, 5, and 7 of the OSI reference model. Most of the firewall control and filtering is done in software. When a client needs to access a remote server, it connects to a proxy server. The proxy server connects to the remote server on behalf of the client. Therefore, the server only sees a connection from the proxy server.



4. **Next Generation Firewall:** Next-generation firewalls (NGFW) go beyond stateful firewalls by providing:

- ✓ Integrated intrusion prevention
- ✓ Application awareness and control to see and block risky apps
- ✓ Upgrade paths to include future information feeds
- ✓ Techniques to address evolving security threats

Other methods of implementing firewalls include:

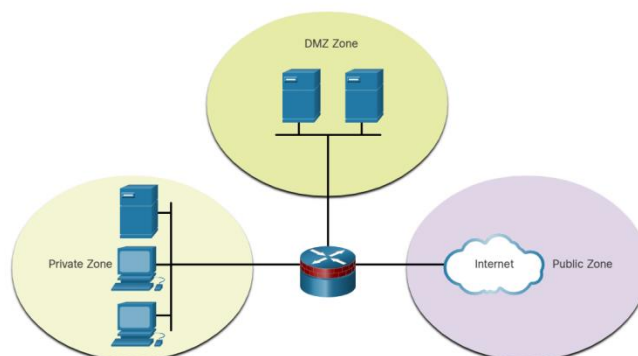
- **Host-based (server and personal) firewall** - A PC or server with firewall software running on it.
- **Transparent firewall** - Filters IP traffic between a pair of bridged interfaces.
- **Hybrid firewall** - A combination of the various firewall types. For example, an application inspection firewall combines a stateful firewall with an application gateway firewall.

### **ZPF (Zero-based Policy Firewall)**

**ZPFs** are an evolutionary step beyond classic firewalls. While classic firewalls based security configuration on router interfaces, a ZPF allows interfaces to be assigned to zones. Security policies are defined based on the zone, and the security relationships between zones. Multiple interfaces can be made members of a zone, and zone policies will be applied to those interfaces. Security requirements can be defined by the nature of the zones, not the IP networks that are communicating through a given interface. There are two configuration models for Cisco IOS Firewall:

- **Classic Firewall** - The traditional configuration model in which firewall policy is applied on interfaces.
- **Zone-based Policy Firewall (ZPF)**- The configuration model in which interfaces are assigned to security zones, and firewall policy is applied to traffic moving between the zones.

If an additional interface is added to the private zone, the hosts connected to the new interface in the private zone can pass traffic to all hosts on the existing interface in the same zone. A simple three-zone network is shown in the figure.



he primary motivations for network security professionals to migrate to the ZPF model are structure and ease of use. The structured approach is useful for documentation and communication. The ease of use makes network security implementations more accessible to a larger community of security professionals.

There are several benefits of a ZPF:

- It is not dependent on ACLs.
- The router security posture is to block unless explicitly allowed.
- Policies are easy to read and troubleshoot with the Cisco Common Classification Policy Language (C3PL). C3PL is a structured method to create traffic policies based on events, conditions, and actions. This provides scalability because one policy affects any given traffic, instead of needing multiple ACLs and inspection actions for different types of traffic.
- Virtual and physical interfaces can be grouped into zones.
- Policies are applied to unidirectional traffic between zones.

When deciding whether to implement IOS Classic Firewall or a ZPF, it is important to note that both configuration models can be enabled concurrently on a router. However, the models cannot be combined on a single interface. For example, an interface cannot be simultaneously configured as a security zone member and for IP inspection.

## **ZPF Actions**

Policies identify actions that the ZPF will perform on network traffic. Three possible actions can be configured to process traffic by protocol, source and destination zones (zone pairs), and other criteria.

- **Inspect** - This performs Cisco IOS stateful packet inspection.
- **Drop** - This is analogous to a **deny** statement in an ACL. A **log** option is available to log the rejected packets.
- **Pass** - This is analogous to a **permit** statement in an ACL. The pass action does not track the state of connections or sessions within the traffic.

## **Rules for Transit Traffic of Zone-Based Policy Firewalls (ZPFs)**

- **If Traffic is Between Zones:** If traffic is traveling between two zones, it will only be allowed if a security policy explicitly allows it. If there is no policy between the zones, traffic will be denied by default.
- **If Policies Are Defined for Traffic:** If a policy is defined for inbound or outbound traffic, then the traffic will be subject to that policy. If no policy is defined, traffic will be denied.

- **If There's Communication between Zones:** If there is a policy permitting communication between two zones (e.g., "Inside" to "DMZ"), traffic will flow according to the policy. If no policy exists, communication will be blocked.
- **If Traffic is Transit Traffic:** If the traffic is passing through the router or firewall (i.e., transit traffic), it must meet the security policies defined for both the **source** and **destination** zones. If the policies don't allow it, the traffic will be dropped.
- **If No Policy Exists Between Zones:** If there is no policy between two zones, the firewall will implicitly deny all traffic between them. If a policy is created later, the firewall will apply that policy.
- **If Traffic is Return Traffic:** If outbound traffic is allowed from a zone, return traffic is automatically allowed based on the established connection. If no outbound traffic has been permitted, return traffic will be denied.
- **If There is a Default Policy for a Zone:** If no specific policy exists for a zone, the default policy for that zone will be applied. If no default policy is set, the traffic will be denied by default.
- **If Traffic is Between Zone Pairs:** If there is a defined security relationship between two zones (e.g., "trusted" and "untrusted"), the traffic will be controlled according to that relationship. If there is no defined relationship, traffic will be denied.

### Traffic to the Self Zone in Zone-Based Policy Firewalls (ZPFs)

Got it! Here's the corrected table with "If Yes, then" and "If No, then" logic for each rule.

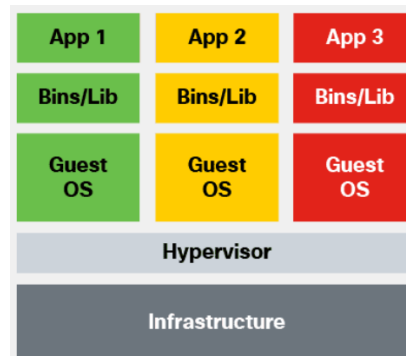
Rule	Traffic Type	Policy Defined (Yes/No)	Action
<b>1. Traffic Destined for the Self Zone (Router/Firewall)</b>	If traffic is directed to the self zone.	<b>If Yes:</b> Pass / Allow traffic	<b>If No:</b> Deny traffic
<b>2. Traffic from Self Zone to Other Zones</b>	If the router/firewall initiates traffic to another zone.	<b>If Yes:</b> Pass / Allow traffic	<b>If No:</b> Deny traffic
<b>3. Traffic for Self Zone Functions (Management/Routing)</b>	If traffic is required for management or routing (SSH, SNMP, OSPF, BGP).	<b>If Yes:</b> Pass / Allow traffic	<b>If No:</b> Deny traffic
<b>4. Traffic to Self Zone for Services (DHCP, DNS, etc.)</b>	If traffic is for services like DHCP, DNS, NTP, etc.	<b>If Yes:</b> Pass / Allow traffic	<b>If No:</b> Deny traffic
<b>5. Traffic from Trusted Zones to Self Zone</b>	If traffic comes from a trusted zone (internal/management).	<b>If Yes:</b> Pass (Default)	<b>If No:</b> Inspect / Deny if restricted
<b>6. Traffic from Untrusted Zones to Self Zone</b>	If traffic comes from untrusted zones (internet/external).	<b>If Yes:</b> Inspect traffic	<b>If No:</b> Deny traffic
<b>7. Dynamic Protocol Traffic (e.g., NAT, VPN)</b>	If traffic is related to NAT or VPN protocols.	<b>If Yes:</b> Pass / Allow traffic	<b>If No:</b> Deny traffic
<b>8. Special Handling (e.g., ICMP for Path MTU Discovery)</b>	If traffic requires special handling (e.g., ICMP).	<b>If Yes:</b> Pass / Allow traffic	<b>If No:</b> Deny traffic

# Cloud security

## Virtualization and Cloud Computing

Virtualization benefits an organization by decreasing the number of physical machines (e.g. servers and workstations) required in the IT environment

### Virtual machines

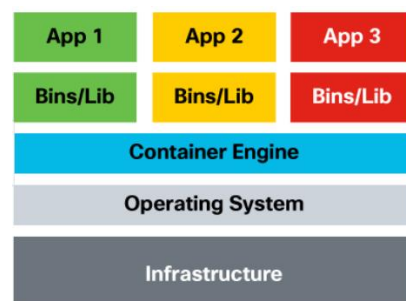


A hypervisor is a software or hardware program that allows you to run multiple independent operating systems on one physical system. It is a key component of virtualization. There are two virtualization methods:

- ✓ Hardware virtualization (type 1 hypervisor) — the guest operating system runs directly on a hardware platform, under the control of the host system.
- ✓ Hosted virtualization (type II hypervisor) — an application running on the host machine is used to create virtual machines that consist entirely of software and contain no hardware components.

Virtual machine environments use an operating system, so they need to be patched. Virtual machines share hardware and run with very high privileges. Be aware that an attacker that compromises a virtual machine may be able to compromise the host machine.

### Containers



Unlike a virtual machine, a container consists of just the application and its dependencies. A container uses an engine for operating system emulation. Docker is an open platform that uses OS-level virtualization to deliver software in packages (containers). You can easily move

containers around and the application will run. Specialized software such as Kubernetes allows you to manage your containers.

If a user or application has elevated privileges within a container, the underlying operating system can be compromised.

### Virtual Desktop Infrastructure (VDI)

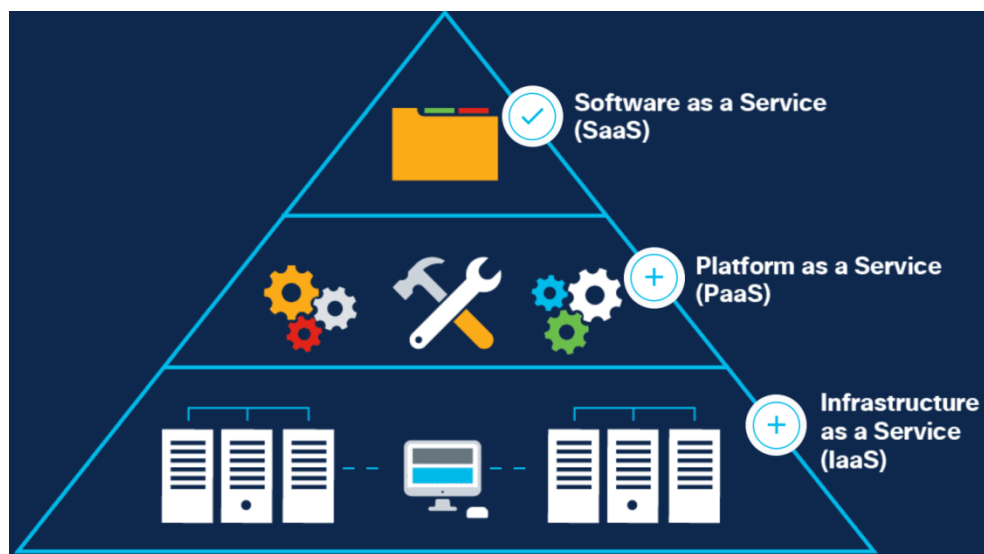


User desktop environments can be stored remotely on a server using thin client or virtual desktops. This makes it very easy to quickly create, delete, copy, archive or download configurations over a network. Desktop virtualization requires high availability and storage capacity.

### Cloud-Based Technology

Cloud-based technologies enable organizations like @Apollo to access computing, storage, software and servers through the Internet. It moves the technology component from the organization to the cloud provider.

Let's recap from Module 1 the three main computing service models, which are collectively known as XaaS ('anything as a service').





- **Software as a Service (SaaS)** allows users to access application software and databases. Cloud providers manage the infrastructure while users store data on the cloud provider's servers.
- **Platform as a Service (PaaS)** lets an organization remotely access the development tools and services used to deliver such applications, on a subscription basis.
- **Infrastructure as a Service (IaaS)** provides virtualized computing resources over the Internet. The provider hosts the hardware, software, servers and storage components, and the user pays for a subscription to these resources.

## Cloud Computing

- **Private Cloud:** A private cloud is a cloud infrastructure used exclusively by one organization. It can be hosted on-site or by a third-party provider, but the resources are not shared with others. This setup provides high security and control, making it ideal for organizations with strict regulatory or data requirements.
  - **Services Offered:** Mainly IaaS and PaaS, and sometimes SaaS.
  - **Examples:** VMware vCloud, OpenStack private cloud, Oracle Private Cloud.
  - **Use Case:** A large financial firm running sensitive workloads internally.
- **Public Cloud:** Public cloud is a cloud environment where resources and services are delivered over the internet and shared among multiple customers. It offers scalability, cost-efficiency, and ease of access.
  - **Services Offered:** IaaS, PaaS, SaaS.
  - **Examples:** Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, Dropbox, Salesforce.
  - **Use Case:** A startup hosting its website and databases on AWS.
- **Hybrid Cloud:** A hybrid cloud combines both private and public clouds, allowing data and applications to move between them. It provides greater flexibility and optimization of existing infrastructure, security, and compliance.
  - **Services Offered:** IaaS, PaaS, SaaS.
  - **Examples:** Azure Arc, AWS Outposts, IBM Hybrid Cloud.
  - **Use Case:** A retail company running customer data analysis in a public cloud while keeping payment data in a private cloud.
- **Community Cloud:** A community cloud is shared by several organizations with similar requirements, such as compliance, security, or mission. It can be managed internally or by a third-party and is used by a specific group of users.

- **Services Offered:** Primarily IaaS and PaaS.
- **Examples:** Government departments sharing infrastructure, CERN's community cloud.
- **Use Case:** A group of healthcare institutions sharing resources to comply with HIPAA regulations.

## Top Threats to Cloud Computing

Cloud computing is susceptible to many of the same threats that affect physical enterprise networks. However, the cloud environment also introduces unique threats.

For instance, if a threat actor successfully compromises a cloud resource, they could do the following:

- Use the cloud computing resources to target other online entities.
- Host malware on respected cloud providers that will appear harmless or even legitimate.
- Abuse the cloud services to launch DDoS attacks, host pirated contents, send email spam, and conduct phishing campaigns.

The following lists some threats associated with cloud computing.

- **Data breaches:** These occur when protected sensitive data is accessed by an unauthorized entity.
- **Cloud misconfiguration:** This occurs when the cloud computing resource is set up incorrectly, making it vulnerable to attacks.
- **Poor cloud security architecture strategy:** Private cloud security is the responsibility of the organization. However, security for public clouds, hybrid clouds, and community clouds becomes a shared responsibility between the organization and the provider. This can introduce vulnerabilities if the cloud security architecture is not fully understood, or is correctly implemented.
- **Compromised account credentials:** This occurs when user accounts or access privileges are not properly secured and are hijacked by threat actors. This can lead to a major security threat if the account has high privileges. For example, in public clouds a service account has the highest privilege for accessing and managing cloud assets. A hijacked service account would enable a threat actor to control all cloud resources.
- **Insider threat:** This occurs when an employee, contractor, or business partner maliciously or unintentionally compromise the cloud service.
- **Insecure software user interface (UI) or application programming interface (API):** Cloud computing uses software UIs and APIs for customers to interact with their cloud services. These interfaces are the most exposed points to the internet and therefore, they are targets for threat actors.

- **Limited cloud usage visibility:** This occurs when the cloud client does not have full visibility into the cloud service, making the identification of safe or malicious files more difficult.

## Domains of Cloud Security

There are many resources available promoting cloud computing security. A widely respected and referenced resource is the Security Guidance for Critical Areas of Focus in Cloud Computing v4 document. Developed by the Cloud Security Alliance (CSA), it promotes best practices to provide security assurance within the cloud computing domains. Specifically, the document covers 14 domains of cloud security.

- **Cloud Computing Concepts and Architectures:** The domain defines cloud computing terminology and details the overall logical and architectural frameworks used in the Security Guidance document.
- **Governance and Enterprise Risk Management:** The domain describes four areas impacted by cloud computing:
  - Governance
  - Enterprise Risk Management
  - Information Risk Management
  - Information Security
- **Legal Issues, Contracts and Electronic Discovery:** The domain describes legal issues associated with cloud computing including the moving of data to the cloud, contracting with cloud service providers, and handling electronic discovery requests in litigation.
- **Compliance and Audit Management:** The domain describes challenges of delivering, measuring, and communicating compliances when organizations migrate from traditional data centers to the cloud.
- **Information Governance:** The domain describes the need to ensure that the use of data and information complies with organizational policies, standards, and strategy including regulatory, contractual, and business objectives.
- **Management Plane and Business Continuity:** The domain describes the need to secure the cloud computing management plane (i.e., the protocols and resources used to manage the cloud). It also describes business continuity and disaster recovery procedures to be used by the cloud provider and the cloud client.
- **Security as a Service:** The domain covers the continually evolving security services delivered from the cloud.
- **Infrastructure Security:** The domain describes cloud-specific aspects of infrastructure security and the foundation for operating securely in the cloud.

- **Virtualization and Containers:** The domain describes the need to secure the virtualization technology and virtual assets which are the foundation for cloud computing.
- **Incident Response:** The domain describes the critical aspects of incident response (IR) including the Incident Response Lifecycle and considerations for responders as they work in a cloud environment.
- **Application Security:** The domain provides guidance on how to securely build and deploy applications in cloud computing environments, specifically for PaaS and IaaS.
- **Data Security and Encryption:** Data Security should be risk-based since it is not appropriate to secure everything equally. The domain describes those controls related to securing the data itself, of which encryption is one of the most important.
- **Identity, Entitlement, and Access Management (IAM):** The domain describes how cloud identity is different than traditional identity management.
- **Related Technologies:** The domain provides background and recommendations for technologies that rely nearly exclusively on cloud computing to operate and for technologies that do not necessarily rely on cloud but are commonly seen in cloud deployments.

## Cloud Infrastructure Security

### Infrastructure Security

The Infrastructure Security domain describes cloud-specific aspects of infrastructure security and the foundation for operating securely in the cloud.

Cloud infrastructure is the foundation on which virtualized cloud resources such as compute, networking, and data storage are built and deployed.

There are two major layers to infrastructure in cloud computing:

- The physical and logical compute (CPU, memory, etc.), networks, and storage are combined to create a cloud.
- The virtual infrastructure managed by a cloud user, that is, the compute, network, and storage assets they access from the resource pools.

Due to the nature of cloud computing, traditional infrastructure security measures based on the control of physical communication paths and insertion of security appliances does not work.

Custom cloud security tools include virtual appliances and software agents that are used to secure virtual environments. However, these tools may introduce bottlenecks when accessing resources, or lead to processor overloading. Therefore, the use of virtual appliances should be carefully evaluated and deployed.

Software-defined networks (SDN) enable new types of security controls and provide an overall gain for network security including:

- Easy network isolation without constraints of physical hardware
- SDN firewalls (security groups in cloud computing) applied to assets based on more flexible criteria than hardware firewalls

### Cloud Security Responsibilities

- **IaaS:** Provider secures infrastructure; customer secures operating systems, applications, and data.
- **PaaS:** Provider secures infrastructure and platform; customer secures applications and data.
- **SaaS:** Provider secures everything; customer manages user access and data.

**Key customer responsibilities include** protecting data, managing identities and access, configuring security settings, monitoring for threats, responding to incidents, and ensuring compliance.

### How to manage these responsibilities:

1. **Protect Data:** Use strong encryption for data at rest and in transit, classify data for proper policies, and regularly back up important data.
2. **Manage Identities and Access (IAM):** Implement multi-factor authentication, apply the principle of least privilege, and regularly review permissions.
3. **Configure Security Settings:** Use cloud security tools (firewalls, security groups), apply secure configurations, and automate policies with scripts or templates.
4. **Monitor and Respond to Incidents:** Enable logging and continuous monitoring, set alerts for suspicious activity, and develop/test cloud-specific incident response plans.
5. **Ensure Compliance:** Understand relevant regulations, use cloud compliance tools, and maintain documentation and audit trails.

*“In summary, cloud providers secure the cloud infrastructure, while customers secure their data, applications, and access within the cloud by following best practices and using available tools to reduce risks”*

### Other Cloud Infrastructure Security Considerations

- **Company Security Policies:** An organization may permit users to download unknown software tools. These un-sanctioned apps may increase employee productivity by permitting them to download and use their favorite software tools. However, unmonitored apps can create security gaps and blind spots. Established, well-defined

company security policies and educating users are effective ways to manage unknown apps.

- **Layered Security:** Cloud resources can be viewed in four layers: hardware, infrastructure, platform, and application layers. Defense-in-depth strategies can be applied to each of these layers. Some layered security options are:
  - Cloud platforms typically have built-in security at the platform level to protect client cloud resources. For example, some CSPs provide built-in DDoS service that clients do not need to configure.
  - A virtual private cloud allocates private subnets that are logically isolated from the internet.
  - While clients will not have access to configure physical firewall devices, CSPs typically provide equivalent firewall functions, or virtual firewalls, such as deny and allow rules and host-level security groups.
  - Flow logs are used to monitor traffic that crosses individual network interfaces.
  - VPNs are used to provide remote user access to the cloud resources, as well as site-to-site connections used in multi-cloud scenarios, or connections between a cloud and on-premises data centers.
  - Identity and access management (IAM) services provide user credential management and user authentication and authorization management. Proper use of IAM is critical to protect cloud resources from being abused.
- **Microsegmentation:** Microsegmentation (also referred to as hypersegregation) leverages virtual network topologies to run multiple, smaller, and more isolated networks without incurring additional hardware costs. Because the networks are entirely defined in software without many of the traditional addressing issues, it is far more feasible to run these multiple, software-defined environments. Microsegmentation techniques allow for more granular control of security for traffic and workflows within the cloud.

## Cloud data Security

### States of Data

The States of Data Domain describes controls related to securing the data itself, of which encryption and hashing are of the most important.

Customer data should be protected in the following three states:

- **Data at rest:** This refers to data that is in storage. Data is in this state when no user or process is accessing, requesting, or amending it. Data at rest can be stored on local devices such as a hard disk in a computer, or a centralized network, such as an organization's server. In cloud computing, data at rest can be stored in a cloud and is

accessible from any computer connected to the internet, usually with subscription. All data that is neither in transit nor in process is considered data at rest.

- Data in transit: This refers to data which is being transmitted. Therefore, the data is not at rest nor is it being processed. The transmission could be within a single server along its motherboard's bus lines, between devices on a single network, or between networks and possibly across the internet. Using cryptography and hashing to protect data in transit is critical for cloud computing.
- Data in process: This refers to data during initial input, modification, computation, or output. Data is in this state when it is neither in transit nor at rest. Therefore, it is data that is being processed.

## **Cryptography**

Cryptography is the science of making and breaking secret codes.

By storing and transmitting encrypted data, only the intended recipient can read or process it, and only if they have proper knowledge of the secret used in the encryption algorithm.

Encryption is the process of scrambling data so that unauthorized people cannot easily read it.

When enabling encryption, readable data is called plaintext, while the encrypted version is encrypted text or ciphertext. Encryption converts the plaintext readable message to ciphertext, which is the unreadable, disguised message. Decryption reverses the process.

Encryption requires a key, which plays a critical role in encrypting and decrypting a message. The person possessing the key can decrypt the ciphertext to plaintext.

There are two classes of encryption algorithms:

- Symmetric encryption algorithms use the same pre-shared key to encrypt and decrypt data, a method also known as private key encryption. The Advanced Encryption Standard (AES) is a symmetric encryption algorithm that has a fixed block size of 128 bits with a key size of 128, 192, or 256 bits. The U.S. government uses AES to protect classified information.
- Asymmetric encryption algorithms use one key for encryption that is different from the key used for decryption. Asymmetric encryption algorithms include Rivest-Shamir-Adleman (RSA), Diffie-Hellman, ElGamal, and Elliptic curve cryptography (ECC).

## Hashing

**Hashing** is a tool that ensures data integrity by taking binary data (i.e., the message) and producing a fixed-length representation called the **hash value** (i.e., message digest).

Hash functions are **one-way functions** used to verify and ensure data integrity. A hash tool can also verify authentication. It works by using a **cryptographic hashing function** to replace plaintext passwords or encryption keys.

A **cryptographic hash function** has the following properties:

- The input can be any length.
- The output has a fixed length.
- The hash function is one-way and is not reversible.
- Two different input values will almost never result in the same hash.

The U.S. National Institute of Standards and Technology (NIST) developed **SHA**, the algorithm specified in the **Secure Hash Standard (SHS)**. NIST published **SHA-1** in 1994.

**Note:** Message Digest 5 (**MD5**) was another popular hashing algorithm that is no longer considered secure.

**SHA-2** replaced SHA-1 with four additional hash functions to make up the SHA family:

- SHA-224 (224 bit)
- SHA-256 (256 bit)
- SHA-384 (384 bit)
- SHA-512 (512 bit)

SHA-2 is a stronger algorithm, and it is replacing MD5. **SHA-256**, **SHA-384**, and **SHA-512** are the next-generation algorithms.

## Protecting Virtual Machines

Virtual Machines (VMs or VM instances), just like a physical computer, require patches, updates, and antimalware measures to protect them from external threats. The cloud offers additional security options, depending on the specific tools available in a cloud platform, to protect VMs.

- **Plan subnet placement:** Carefully choose the subnet for each instance so that it has only the necessary access to the outside world.
- **Disable unneeded port and services:** Only enable ports and services that are needed to reduce unnecessary exposure to outside.
- **Enforce account management and policies:** The OS in a VM has a default user accounts. Deactivate any default user accounts and create user accounts with best-practice account management policies such as password complexity and least privilege access.



- **Install antivirus/antimalware software and keep it updated:** This can be accomplished through the VM OS, or it might be available as a service from the cloud platform.
- **Install host-based/software firewall and IDP/IPS:** This can be accomplished through the VM OS, or it might be available as a service from the cloud platform.

## Protecting VMs from VM Sprawl Attacks

It is a relatively easy process to create VM instances in a cloud. However, this may lead to a VM Sprawl issue, where an organization has many VM instances that are not properly managed. For example, it is common practice to create multiple VM instances when a project starts just to try different options. Some of these VMs may no longer be used but left running. If these running instances are not monitored and maintained, they eventually become outdated and vulnerable to attacks.

A cloud computing client should implement policies to log and audit cloud resources being used. VM sprawl not only presents potential risks, but it also consumes cloud services unnecessarily, such as VM instances, storage, and unassigned public IP addresses. By logging the use of cloud resources, monitoring the running VMs, and auditing the actual usage, an organization can better manage and protect the VMs they really need.

## Cryptography

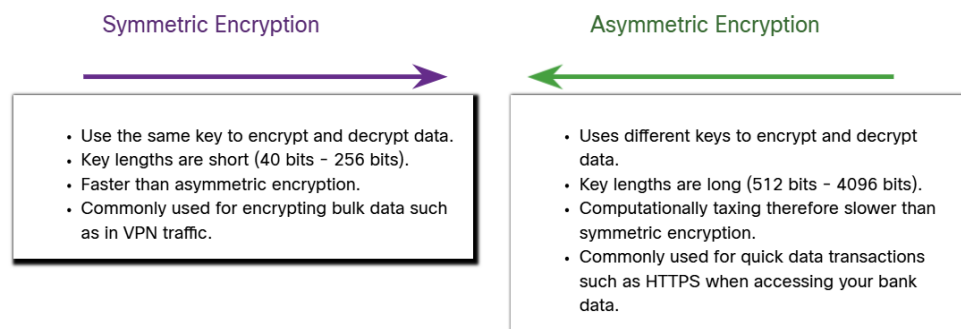
### Data Confidentiality

There are two classes of encryption used to provide data confidentiality; asymmetric and symmetric. These two classes differ in how they use keys.

Symmetric encryption algorithms such as Data Encryption Standard (DES), 3DES, and Advanced Encryption Standard (AES) are based on the premise that each communicating party knows the pre-shared key. Data confidentiality can also be ensured using asymmetric algorithms, including Rivest, Shamir, and Adleman (RSA) and the public key infrastructure (PKI).

**Note:** DES is a legacy algorithm and should not be used. 3DES should be avoided if possible.

The figure highlights some differences between symmetric and asymmetric encryption.

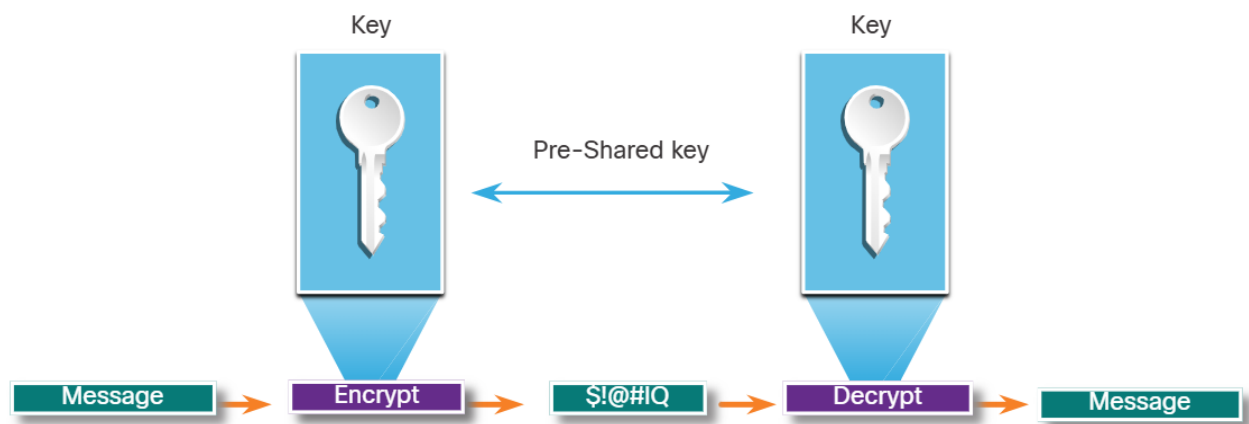


## Symmetric Encryption

Symmetric algorithms use the same pre-shared key to encrypt and decrypt data. A pre-shared key, also called a secret key, is known by the sender and receiver before any encrypted communications can take place.

To help illustrate how symmetric encryption works, consider an example where Alice and Bob live in different locations and want to exchange secret messages with one another through the mail system. In this example, Alice wants to send a secret message to Bob.

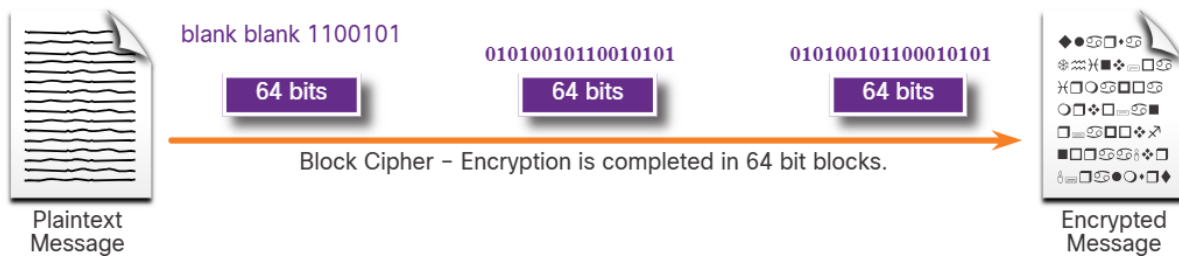
In the figure, Alice and Bob have identical keys to a single padlock. These keys were exchanged prior to sending any secret messages. Alice writes a secret message and puts it in a small box that she locks using the padlock with her key. She mails the box to Bob. The message is safely locked inside the box as the box makes its way through the post office system. When Bob receives the box, he uses his key to unlock the padlock and retrieve the message. Bob can use the same box and padlock to send a secret reply back to Alice.



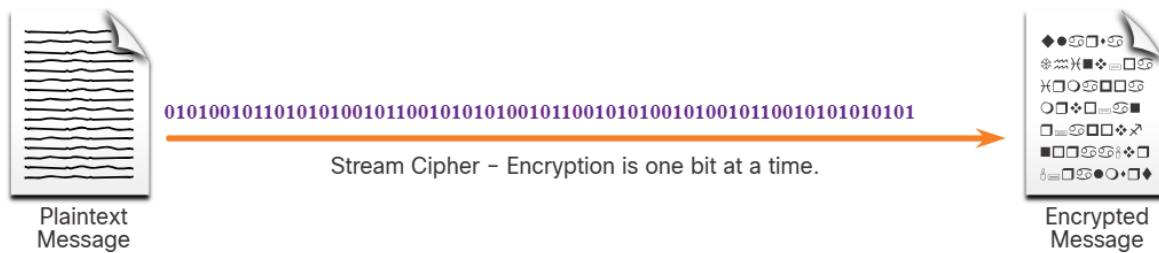
Today, symmetric encryption algorithms are commonly used with VPN traffic. This is because symmetric algorithms use less CPU resources than asymmetric encryption algorithms. This allows the encryption and decryption of data to be fast when using a VPN. When using symmetric encryption algorithms, like any other type of encryption, the longer the key, the longer it will take for someone to discover the key. Most encryption keys are between 112 and 256 bits. To ensure that the encryption is safe, a minimum key length of 128 bits should be used. Use a longer key for more secure communications.

Symmetric encryption algorithms are sometimes classified as either a block cipher or a stream cipher. Click the buttons to learn about these two cipher modes.

- i. **Block ciphers:** **Block ciphers** transform a fixed-length block of plaintext into a common block of ciphertext of 64 or 128 bits. Common block ciphers include DES with a 64-bit block size and AES with a 128-bit block size.



- ii. **Stream ciphers:** Stream ciphers encrypt plaintext one byte or one bit at a time. Stream ciphers are basically a block cipher with a block size of one byte or bit. Stream ciphers are typically faster than block ciphers because data is continuously encrypted. Examples of stream ciphers include RC4 and A5 which is used to encrypt GSM cell phone communications.

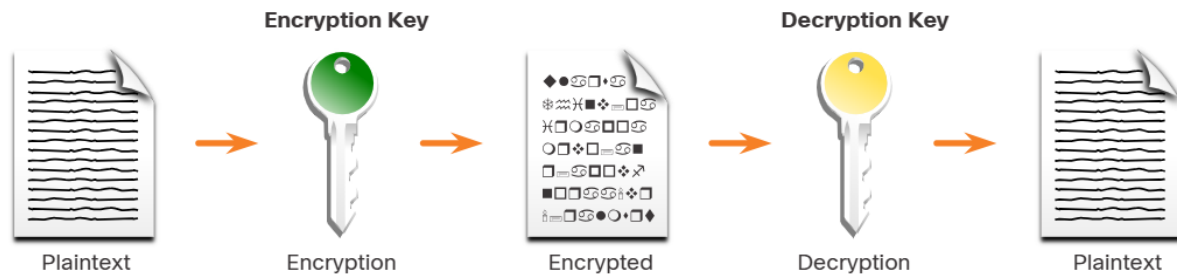


Well-known symmetric encryption algorithms are described in the table.

Symmetric Encryption Algorithms	Description
Data Encryption Standard (DES)	This is a legacy symmetric encryption algorithm. It uses a short key length that makes it insecure for most current uses.
3DES (Triple DES)	The is the replacement for DES and repeats the DES algorithm process three times. It should be avoided if possible as it is scheduled to be retired in 2023. If implemented, use very short key lifetimes.
Advanced Encryption Standard (AES)	AES is a popular and recommended symmetric encryption algorithm. It offers combinations of 128-, 192-, or 256-bit keys to encrypt 128, 192, or 256 bit-long data blocks.
Software-Optimized Encryption Algorithm (SEAL)	SEAL is a faster alternative symmetric encryption algorithm to AES. SEAL is a stream cypher that uses a 160-bit encryption key and has a lower impact on the CPU compared to other software-based algorithms.
Rivest ciphers (RC) series algorithms	This algorithm was developed by Ron Rivest. Several variations have been developed, but RC4 was the most prevalent in use. RC4 is a stream cipher that was used to secure web traffic. It has been found to have multiple vulnerabilities which have made it insecure. RC4 should not be used.

## Asymmetric Encryption

Asymmetric algorithms, also called public-key algorithms, are designed so that the key that is used for encryption is different from the key that is used for decryption, as shown in the figure. The decryption key cannot, in any reasonable amount of time, be calculated from the encryption key and vice versa.



Protocols like **Internet Key Exchange (IKE)**, **SSL/TLS**, **SSH**, and **PGP** use asymmetric encryption to establish secure connections:

- **IKE** is used in VPNs to securely exchange cryptographic keys.
- **SSL/TLS** secures web communication (e.g., HTTPS) by encrypting data between clients and servers.
- **SSH** provides secure remote access and uses key pairs for authentication.
- **PGP** encrypts and signs emails to ensure confidentiality and authenticity.

These technologies rely on asymmetric encryption to protect sensitive information in digital communication.

Asymmetric Encryption Algorithm	Key Length	Description
Diffie-Hellman (DH)	512, 1024, 2048, 3072, 4096	The Diffie-Hellman algorithm allows two parties to agree on a key that they can use to encrypt messages they want to send to each other. The security of this algorithm depends on the assumption that it is easy to raise a number to a certain power, but difficult to compute which power was used given the number and the outcome.
Digital Signature Standard (DSS) and Digital Signature Algorithm (DSA)	512 - 1024	DSS specifies DSA as the algorithm for digital signatures. DSA is a public key algorithm based on the ElGamal signature scheme. Signature creation speed is similar to RSA, but is 10 to 40 times slower for verification.
Rivest, Shamir, and Adleman encryption algorithms (RSA)	512 to 2048	RSA is for public-key cryptography that is based on the current difficulty of factoring very large numbers. It is the first algorithm known to be suitable for signing, as well as encryption. It is widely used in electronic commerce protocols and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.
ElGamal	512 - 1024	An asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key agreement. A disadvantage of the ElGamal system is that the encrypted message becomes very big, about twice the size of the original message and for this reason it is only used for small messages such as secret keys.
Elliptic curve techniques	224 or higher	Elliptic curve cryptography can be used to adapt many cryptographic algorithms, such as Diffie-Hellman or ElGamal. The main advantage of elliptic curve cryptography is that the keys can be much smaller.

## Asymmetric Encryption – Confidentiality

Asymmetric algorithms are used to provide confidentiality without pre-sharing a password. The confidentiality objective of asymmetric algorithms is initiated when the encryption process is started with the public key.

The process can be summarized using the formula:

Public Key (Encrypt) + Private Key (Decrypt) = Confidentiality

When the public key is used to encrypt the data, the private key must be used to decrypt the data. Only one host has the private key; therefore, confidentiality is achieved.

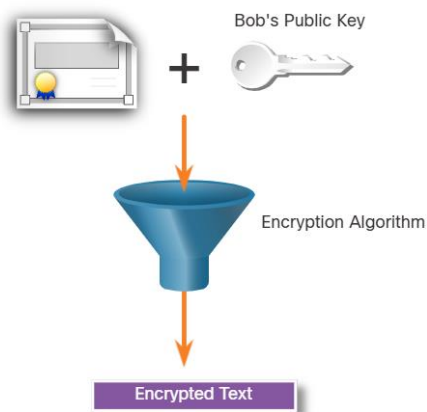
If the private key is compromised, another key pair must be generated to replace the compromised key.

Let's see how the private and public keys can be used to provide confidentiality to the data exchange between Bob and Alice.

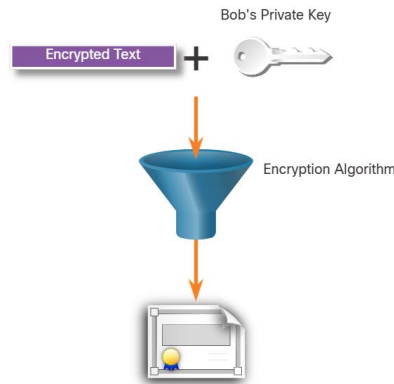
- **Alice Acquires Bob's Public Key:** Alice requests and obtains Bob's public key.



- **Alice Uses the Public Key:** Alice uses Bob's public key to encrypt a message using an agreed-upon algorithm. Alice sends the encrypted message to Bob.



- **Bob Decrypts the Message with His Private Key:** Bob then uses his private key to decrypt the message. Since Bob is the only one with the private key, Alice's message can only be decrypted by Bob and thus confidentiality is achieved.



## Asymmetric Encryption - Authentication

The authentication objective of asymmetric algorithms is initiated when the encryption process is started with the private key.

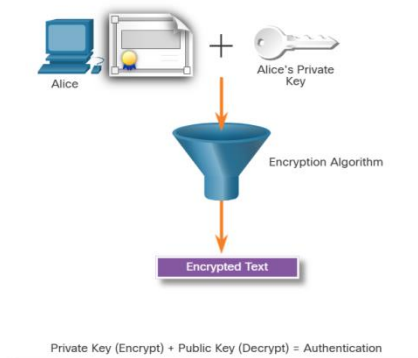
The process can be summarized using the formula:

Private Key (Encrypt) + Public Key (Decrypt) = Authentication

When the private key is used to encrypt the data, the corresponding public key must be used to decrypt the data. Because only one host has the private key, only that host could have encrypted the message, providing authentication of the sender. Typically, no attempt is made to preserve the secrecy of the public key, so any number of hosts can decrypt the message. When a host successfully decrypts a message using a public key, it is trusted that the private key encrypted the message, which verifies who the sender is. This is a form of authentication.

Let's see how the private and public keys can be used to provide authentication to the data exchange between Bob and Alice.

- **Alice Use her private Key:** Alice encrypts a message using her private key. Alice sends the encrypted message to Bob. Bob needs to authenticate that the message did indeed come from Alice.

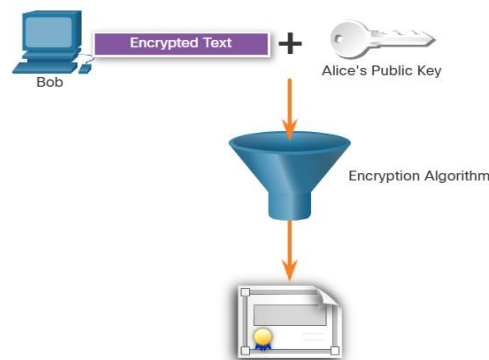


- **Bob requests the public key:** In order to authenticate the message, Bob requests Alice's public key.



Bob needs to verify that the message actually came from Alice. He requests and acquires Alice's public key.

- **Bob decrypts using the public key:** Bob uses Alice's public key to decrypt the message.



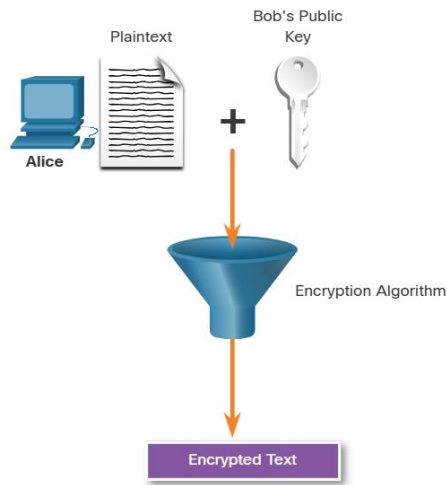
Bob uses the public key to successfully decrypt the message and authenticate that the message did, indeed, come from Alice.

## Asymmetric Encryption - Integrity

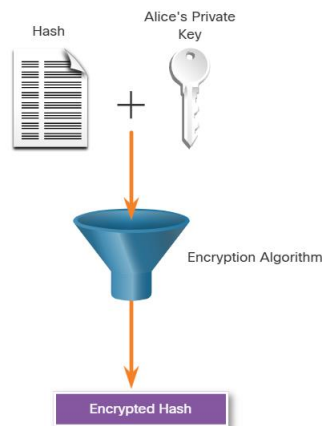
Combining the two asymmetric encryption processes provides message confidentiality, authentication, and integrity.

The following example will be used to illustrate this process. In this example, a message will be ciphered using Bob's public key and a ciphered hash will be encrypted using Alice's private key to provide confidentiality, authenticity, and integrity.

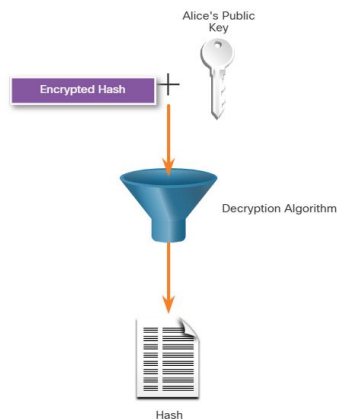
- **Alice uses Bob's public key:** Alice wants to send a message to Bob ensuring that only Bob can read the document. In other words, Alice wants to ensure message confidentiality. Alice uses the public key of Bob to cipher the message. Only Bob will be able to decipher it using his private key.



- Alice encrypts a hash using her private key:** Alice also wants to ensure message authentication and integrity. Authentication ensures Bob that the document was sent by Alice, and integrity ensures that it was not modified. Alice uses her private key to cipher a hash of the message. Alice sends the encrypted message with its encrypted hash to Bob.

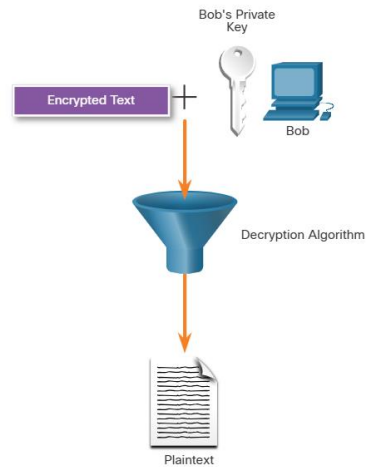


- Bob uses Alice's public key to decrypt the hash:** Bob uses Alice's public key to verify that the message was not modified. The received hash is equal to the locally determined hash based on Alice's public key. Additionally, this verifies that Alice is definitely the sender of the message because nobody else has Alice's private key.





- **Bob uses his private key to decrypt the message:** Bob uses his private key to decipher the message.



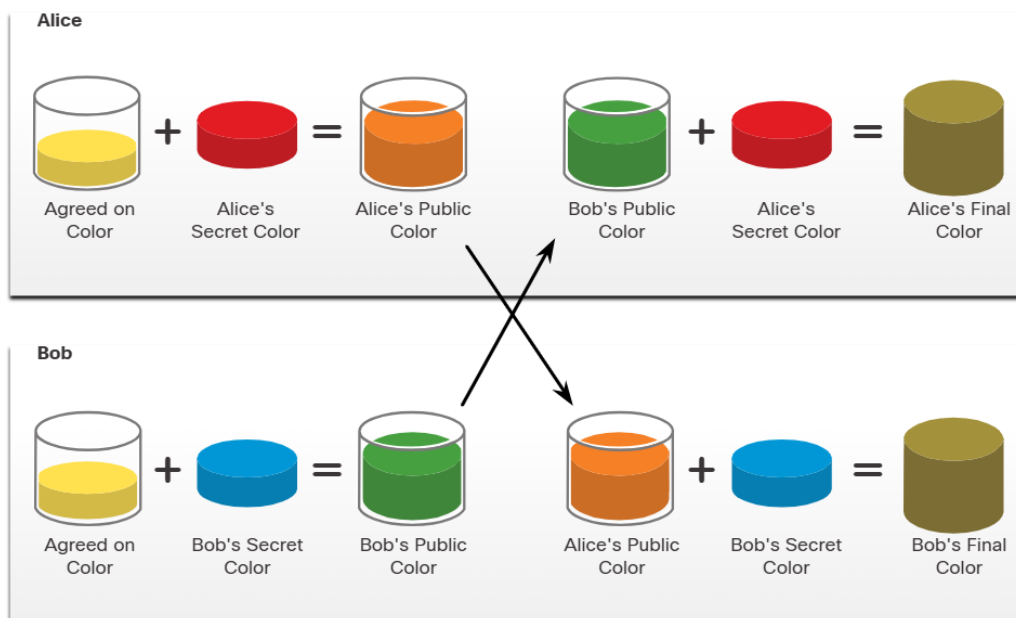
## Diffie-Hellman

Diffie-Hellman (DH) is an asymmetric mathematical algorithm that allows two computers to generate an identical shared secret without having communicated before. The new shared key is never actually exchanged between the sender and receiver. However, because both parties know it, the key can be used by an encryption algorithm to encrypt traffic between the two systems.

Here are two examples of instances when DH is commonly used:

- Data is exchanged using an IPsec VPN
- SSH data is exchanged

To help illustrate how DH operates, refer to the figure.



The colors in the figure will be used instead of complex long numbers to simplify the DH key agreement process. The DH key exchange begins with Alice and Bob agreeing on an arbitrary common color that does not need to be kept secret. The agreed-on color in our example is yellow.

Next, Alice and Bob will each select a secret color. Alice chose red while Bob chose blue. These secret colors will never be shared with anyone. The secret color represents the chosen secret private key of each party.

Alice and Bob now mix the shared common color (yellow) with their respective secret color to produce a public color. Therefore, Alice will mix the yellow with her red color to produce a public color of orange. Bob will mix the yellow and the blue to produce a public color of green.

Alice sends her public color (orange) to Bob and Bob sends his public color (green) to Alice.

Alice and Bob each mix the color they received with their own, original secret color (Red for Alice and blue for Bob.). The result is a final brown color mixture that is identical to the partner's final color mixture. The brown color represents the resulting shared secret key between Bob and Alice.

The security of DH is based on the fact that it uses very large numbers in its calculations. For example, a DH 1024-bit number is roughly equal to a decimal number of 309 digits. Considering that a billion is 10 decimal digits (1,000,000,000), one can easily imagine the complexity of working with not one, but multiple 309-digit decimal numbers.

Diffie-Hellman uses different DH groups to determine the strength of the key that is used in the key agreement process. The higher group numbers are more secure, but require additional time to compute the key. The following identifies the DH groups supported by Cisco IOS Software and their associated prime number value:

- DH Group 1: 768 bits
- DH Group 2: 1024 bits
- DH Group 5: 1536 bits
- DH Group 14: 2048 bits
- DH Group 15: 3072 bits
- DH Group 16: 4096 bits

**Note:** A DH key agreement can also be based on elliptic curve cryptography. DH groups 19, 20, and 24, which are based on elliptic curve cryptography, are also supported by Cisco IOS Software.

Unfortunately, asymmetric key systems are extremely slow for any sort of bulk encryption. This is why it is common to encrypt the bulk of the traffic using a symmetric algorithm, such as 3DES or AES and use the DH algorithm to create keys that will be used by the encryption algorithm.

## Obscuring Data

### Data Masking Techniques

Data masking technology secures data by replacing sensitive information with non-sensitive versions of it. The non-sensitive version looks and acts like the original so that an organizational process can use non-sensitive data with no change needed to the supporting applications or data storage facilities.

Masking most commonly limits the propagation of sensitive data within IT systems by distributing surrogate data sets for testing and analysis. Information can be dynamically masked on the spot if the system or application detects a risky user request for sensitive information.

Data masking can replace sensitive data in non-production environments to protect the underlying information. Several data masking techniques can be used.

All of the below methods ensure that data remains meaningful but changed enough to protect it.

- **Substitution** replaces data with authentic-looking values to apply anonymity to the data records.
- **Shuffling** derives a substitution set from the same column of data that a user wants to mask. This technique works well for financial information in a test database, for example.
- **Nulling out** applies a null value to a particular field, which completely prevents visibility of the data.

### Steganography

Steganography conceals data — e.g. a message — in another file such as a graphic, audio or video file.

The advantage of steganography over cryptography is that the secret message does not attract any special attention. No one would ever know that a picture contained a secret message if they just viewed the file either electronically or in hard copy form.

There are several components involved in hiding data. First, there is the embedded data, which is the secret message. The cover-text (or cover-image or cover-audio) hides the embedded data producing the stego text (or stego image or stego audio). A stego key controls the hiding process.

- **Steganography techniques:** The approach used to embed data in a cover-image is using least significant bits (LSB). This method uses bits of each pixel in the image.
  - A pixel is the basic unit of programmable color in a computer image.

- The specific color of each pixel is a blend of three colors; red, green, and blue (RGB).
- Three bytes of data specify a pixel's color (one byte for each color). Eight bits make up a byte so a 24-bit color system uses all three bytes.
- LSB uses a bit of each of the red, green and blue color components. Each pixel can store three bits

This image shows three pixels of a 24-bit color image. One of the letters in the secret message is the letter T, and inserting the character T changes only two bits of the color. The human eye cannot recognize the changes made to the least significant bits, so the result is a hidden character.

On average, no more than half of the bits in an image will need to change to hide a secret message effectively.

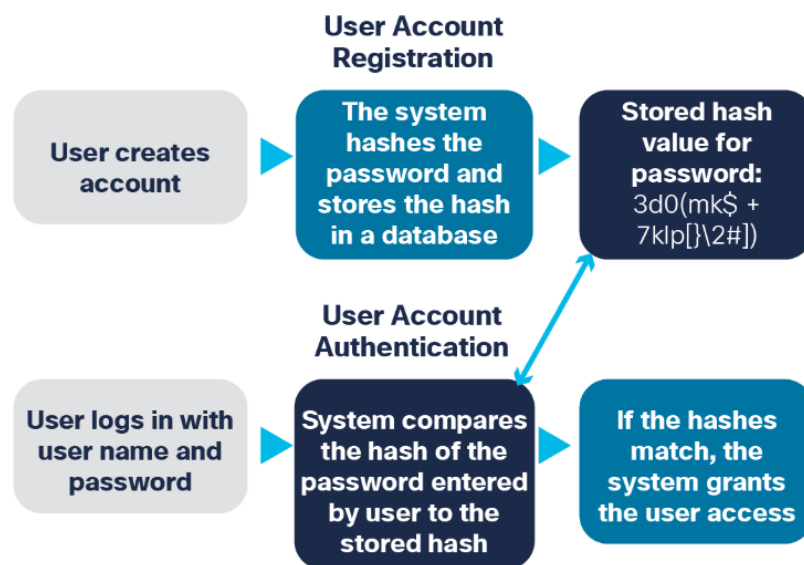
- **Social steganography:** Social steganography hides information in plain sight by creating output that can be read a certain way by some to get the secret message, based on previously set rules and/or definitions. As a result, those who view it in a normal way will not see the message. Teens on social media use this tactic to communicate with their closest friends while keeping others, like their parents, unaware of what the message means. For example, the phrase 'going to the movies' might mean 'going to the beach.' Individuals in countries that censor media also use social steganography to get their messages out by misspelling words on purpose or making obscure references that mean something to those in the know. In effect, they communicate to different audiences simultaneously, sending out two different messages: the apparent message and the secret message.
- **Detection:** Steganalysis follows the discovery that hidden information exists. The goal of steganalysis is to discover this hidden information. Patterns in the stego image create suspicion. For example, a disk may have unused yet reserved areas, which are reserved because they hide information. Disk analysis utilities can report on hidden information in unused clusters of storage devices. Filters can capture data packets that contain hidden information in packet headers. Both of these methods use steganography signatures. By comparing an original image with the stego image, an analyst may pick up repetitive patterns visually.

## Using hashes

Hashing algorithms can turn any amount of data into a fixed-length fingerprint or digital hash. Nobody can reverse a digital hash to discover the original input. If the input changes at all, it results in a different hash.

This works to protect passwords. A system needs to store a password in a form that protects it and keeps it away from prying eyes, while also being able to still verify that a user's password is correct.

This diagram shows the workflow for user account registration and authentication using a hash-based system. You can see that the system never writes the user's password to the hard drive, it only stores the digital hash. This way, the password is truly only known to the user who set it.



## Cracking Hashes

To crack a hash, an attacker must guess the password. The top two attacks used to guess passwords are dictionary and brute-force attacks.

### Brute-force Attack

- **What it is:** This tries every possible combination of characters until the correct password is found.
- **How it works:** The attacker generates hashes of all possible strings, starting from short lengths to longer ones, and compares them to the target hash.
- **Pros:** Guaranteed to find the password if enough time and resources are available.
- **Cons:** Extremely time-consuming and resource-intensive, especially for long or complex passwords.

### Rainbow Tables

- **What it is:** Rainbow tables are precomputed tables of hash values mapped to possible plaintext inputs, designed to speed up cracking.
- **How it works:** Instead of computing hashes on the fly, the attacker looks up the hash in the rainbow table to find the original input.
- **Pros:** Much faster than brute-force or dictionary attacks because of precomputation.

- **Cons:** Large storage requirements; ineffective if passwords are “salted” (random data added before hashing).

## Hybrid Attack

- **What it is:** A combination of dictionary and brute-force attacks.
- **How it works:** Starts with dictionary words but adds variations like numbers, symbols, or capitalization changes (e.g., “password123!”, “P@ssw0rd”).
- **Pros:** More effective than pure dictionary attack because it covers common password modifications.
- **Cons:** Still limited if the password is very complex or unpredictable.

## Salting

Salting makes password hashing more secure.

If two users have the same password, they will also have the same password hashes. A salt, which is a random string of characters, is an additional input added to the password before hashing.

This creates a different hash result even when the two passwords are identical, as shown here. Then, the database stores both the hash and the salt. The same password generates a different hash for different users, because the salt in each instance is different. Meanwhile, the salt does not have to be secret since it is a random number.



## Implementing Salting

A cryptographically secure pseudo-random number generator (CSPRNG) is the best way to generate salt.

CSPRNGs generate a random number that has a high level of randomness and is completely unpredictable, so it is cryptographically secure.

The following recommendations will help ensure successful implementation of salting:

- The salt needs to be unique for every user password.

- Never reuse a salt.
- The length of the salt should match the length of the hash function's output.
- Always hash on the server, in a web application.

Using a technique called **key stretching** will also help to protect against attack. Key stretching makes attempts to figure out passwords work very slowly. This makes high-end attacker hardware that can attempt to crack billions of hashes per second less effective.

### **The steps a database application uses to store and validate a salted password.**

- **To store password:**
  - Use CSPRNG to generate a long, random salt.
  - Add the salt to the beginning of the password.
  - Hash it with SHA-256, a standard cryptographic hash function.
  - Save the salt and the hash in the user's database records.
- **To validate password:**
  - Retrieve a user's salt and hash from the database
  - Add the salt to the password and hash it with the same hash function
  - Compare the hash of the password just submitted by the user trying to log in to the one stored in the database.
  - If the hashes do not match, the password the user has just tried to log in with is incorrect.

### **Preventing Attacks**

Salting prevents an attacker from using a dictionary attack to try to guess passwords. Salting also makes it impossible to use lookup tables and rainbow tables to crack a hash.

- **Lookup tables:** A lookup table stores the pre-computed hashes of passwords in a password dictionary, along with the corresponding password. A lookup table is a data structure that processes hundreds of hash lookups per second.
- **Reverse lookup tables:** This attack allows the cybercriminal to launch a dictionary or brute-force attack on many hashes without the pre-computed lookup table. The cybercriminal creates a lookup table that plots each password hash from the breached account database to a list of users. The cybercriminal hashes each password guess and uses the lookup table to get a list of users whose password matched the cybercriminal's guess. Since many users have the same password, the attack works well.
- **Rainbow tables:** Rainbow tables sacrifice hash-cracking speed to make the lookup tables smaller. A smaller table means that the table can store the solutions to more hashes in the same amount of space.

## Public Key Cryptography

### Using Digital Signatures

Digital signatures are a mathematical technique used to provide authenticity, integrity, and no repudiation. Digital signatures have specific properties that enable entity authentication and data integrity. In addition, digital signatures provide nonrepudiation of the transaction. In other words, the digital signature serves as legal proof that the data exchange did take place. Digital signatures use asymmetric cryptography.

- **Authentic:** The signature cannot be forged and provides proof that the signer, and no one else, signed the document.
- **Unalterable:** After a document is signed, it cannot be altered.
- **Not Reusable:** The document signature cannot be transferred to another document..
- **Non-Repudiated:** The signed document is considered to be the same as a physical document. The signature is proof that the document has been signed by the actual person.

Digital signatures are commonly used in the following two situations:

1. **Code signing** – This is used for data integrity and authentication purposes. Code signing is used to verify the integrity of executable files downloaded from a vendor website. It also uses signed digital certificates to authenticate and verify the identity of the site that is the source of the files.
2. **Digital certificates** – These are similar to a virtual ID card and used to authenticate the identity of system with a vendor website and establish an encrypted connection to exchange confidential data.

There are three Digital Signature Standard (DSS) algorithms that are used for generating and verifying digital signatures:

- **DSA (Digital Signature Algorithm):** DSA is the original standard for generating public and private key pairs, and for generating and verifying digital signatures.
- **RSA (Rivest–Shamir–Adleman):** RSA is an asymmetric algorithm that is commonly used for generating and verifying digital signatures.
- **ECDSA (Elliptic Curve Digital Signature Algorithm):** ECDSA is a newer variant of DSA and provides digital signature authentication and non-repudiation with the added benefits of computational efficiency, small signature sizes, and minimal bandwidth.

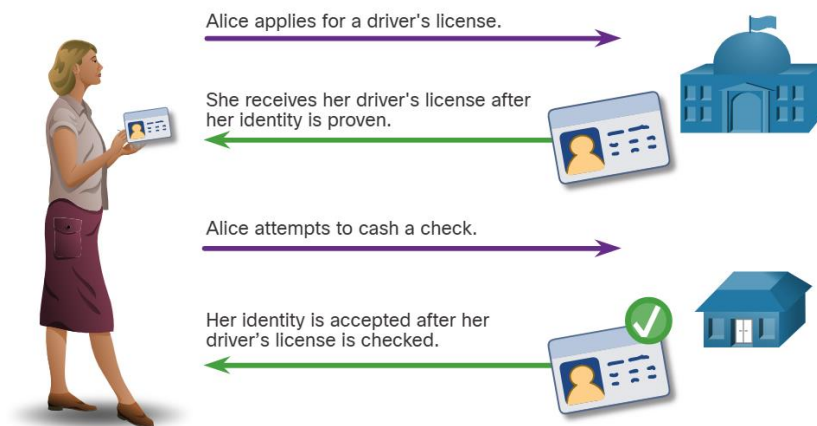


## Public Key Management

Internet traffic consists of traffic between two parties. When establishing an asymmetric connection between two hosts, the hosts will exchange their public key information.

An SSL certificate is a digital certificate that confirms the identity of a website domain. To implement SSL on your website, you purchase an SSL certificate for your domain from an SSL Certificate provider. The trusted third party does an in-depth investigation prior to the issuance of credentials. After this in-depth investigation, the third-party issues credentials (i.e. digital certificate) that are difficult to forge. From that point forward, all individuals who trust the third party simply accept the credentials that the third-party issues. When computers attempt to connect to a web site over HTTPS, the web browser checks the website's security certificate and verifies that it is valid and originated with a reliable CA. This validates that the website identity is true. The certificate is saved locally by the web browser and is then used in subsequent transactions. The website's public key is included in the certificate and is used to verify future communications between the website and the client.

These trusted third parties provide services similar to governmental licensing bureaus. The figure illustrates how a driver's license is analogous to a digital certificate.



The Public Key Infrastructure (PKI) consists of specifications, systems, and tools that are used to create, manage, distribute, use, store, and revoke digital certificates. The certificate authority (CA) is an organization that creates digital certificates by tying a public key to a confirmed identity, such as a website or individual. The PKI is an intricate system that is designed to safeguard digital identities from hacking by even the most sophisticated threat actors or nation states.

Some examples of Certificate Authorities are IdenTrust, DigiCert, Sectigo, GlobalSign, and GoDaddy. These CAs charge for their services. Let's Encrypt is a non-profit CA that offers certificates free of charge.

## The Public Key Infrastructure

PKI is needed to support large-scale distribution and identification of public encryption keys. The PKI framework facilitates a highly scalable trust relationship. It consists of the hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates.

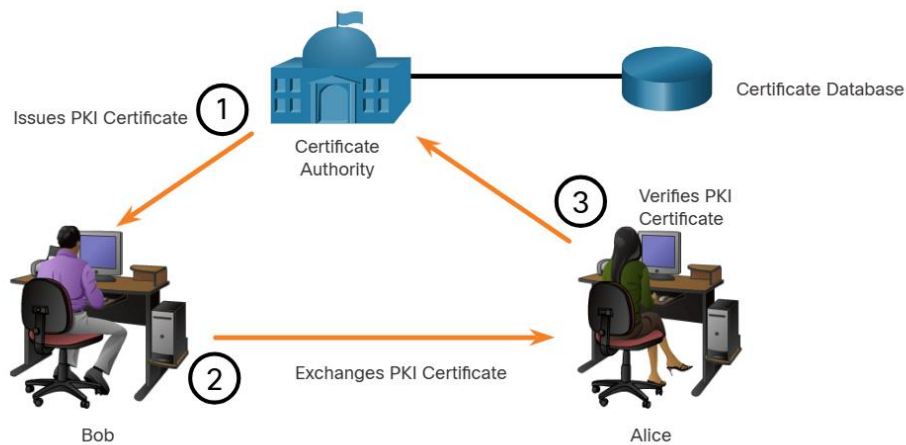
The figure shows the main elements of the PKI.



1. PKI Certificates contain an entity's or individual's public key, its purpose, the certificate authority (CA) that validated and issued the certificate, the date range during which the certificate is valid, and the algorithm used to create the signature.
2. The certificate store resides on a local computer and stores issued certificates and private keys.
3. The PKI Certificate Authority (CA) is a trusted third party that issues PKI certificates to entities and individuals after verifying their identity. It signs these certificates using its private key.
4. The certificate database stores all certificates approved by the CA.

**The next figure shows how the elements of the PKI interoperate:**

- In this example, Bob has received his digital certificate from the CA. This certificate is used whenever Bob communicates with other parties.
- Bob communicates with Alice.
- When Alice receives Bob's digital certificate, she communicates with the trusted CA to validate Bob's identity.



**Note:** Not all PKI certificates are directly received from a CA. A registration authority (RA) is a subordinate CA and is certified by a root CA to issue certificates for specific uses.

## Monitoring common protocol

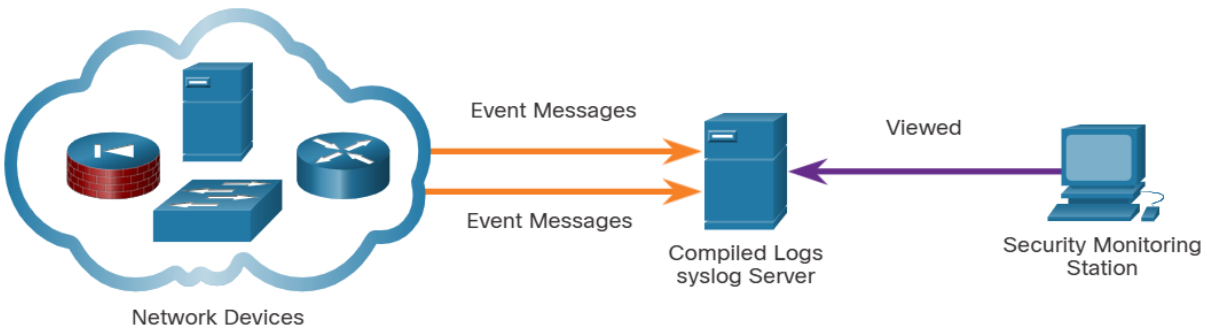
### Syslog and NTP

Various protocols that commonly appear on networks have features that make them of special interest in security monitoring. For example, syslog and Network Time Protocol (NTP) are essential to the work of the cybersecurity analyst.

The syslog standard is used for logging event messages from network devices and endpoints, as shown in the figure. The standard allows for a system-neutral means of transmitting, storing, and analyzing messages. Many types of devices from many different vendors can use syslog to send log entries to central servers that run a syslog daemon. This centralization of log collection helps to make security monitoring practical. Servers that run syslog typically listen on UDP port 514.

Because syslog is so important to security monitoring, syslog servers may be a target for threat actors. Some exploits, such as those involving data exfiltration, can take a long time to complete. This is because the ways in which data is secretly stolen from the network can be very slow. Some attackers may try to hide the fact that exfiltration is occurring. They attack syslog servers that contain the information that could lead to detection of the exploit. Hackers may attempt to block the transfer of data from syslog clients to servers. They may tamper with or destroy log data, or the software that creates and transmits log messages. The next generation (ng) syslog implementation, known as syslog-ng, offers enhancements that can help prevent some of the exploits that target syslog.

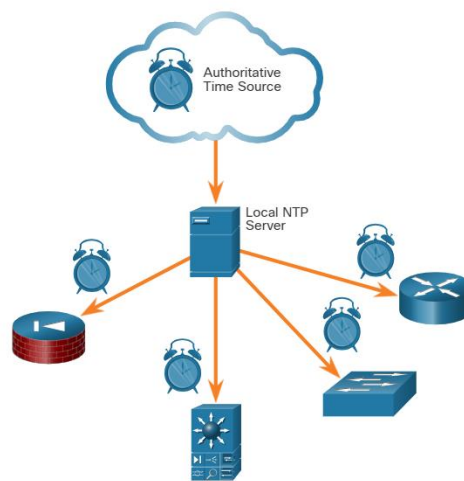
Search the internet for more information about syslog-ng.



## NTP

Syslog messages are usually timestamped. This allows messages from different sources to be organized by time to provide a view of network communication processes. Because the messages can come from many devices, it is important that the devices share a consistent timeclock. One way that this can be achieved is for the devices to use Network Time Protocol (NTP). NTP uses a hierarchy of authoritative time sources to share time information between devices on the network, as shown in the figure. In this way, device messages that share consistent time information can be submitted to the syslog server. NTP operates on UDP port 123.

Because events that are connected to an exploit can leave traces across every network device on their path to the target system, timestamps are essential for detection. Threat actors may attempt to attack the NTP infrastructure in order to corrupt time information used to correlate logged network events. This can serve to obfuscate traces of ongoing exploits. In addition, threat actors have been known to use NTP systems to direct DDoS attacks through vulnerabilities in client or server software. While these attacks do not necessarily result in corrupted security monitoring data, they can disrupt network availability.



## DNS

Domain Name Service (DNS) is used by millions of people daily. Because of this, many organizations have less stringent policies in place to protect against DNS-based threats than they have to protect against other types of exploits. Attackers have recognized this and commonly encapsulate different network protocols within DNS to evade security devices. DNS is now used by many types of malware. Some varieties of malware use DNS to communicate with command-and-control (CnC) servers and to exfiltrate data in traffic disguised as normal DNS queries. Various types of encoding, such as Base64, 8-bit binary, and Hex can be used to camouflage the data and evade basic data loss prevention (DLP) measures.

For example, malware could encode stolen data as the subdomain portion of a DNS lookup for a domain where the nameserver is under control of an attacker. A DNS lookup for 'long-string-of-exfiltrated-data.example.com' would be forwarded to the nameserver of example.com, which would record 'long-string-of-exfiltrated-data' and reply back to the malware with a coded response. This use of the DNS subdomain is shown in the figure. The exfiltrated data is the encoded text shown in the box. The threat actor collects this encoded data, decodes and combines it, and now has access to an entire data file, such as a username/password database.

It is likely that the subdomain part of such requests would be much longer than usual requests. Cyber analysts can use the distribution of the lengths of subdomains within DNS requests to construct a mathematical model that describes normality. They can then use this to compare their observations and identify an abuse of the DNS query process. For example, it would not be normal to see a host on your network sending a query to aW4gcGxhY2UgdG8gcHJvdGVjdC.example.com.

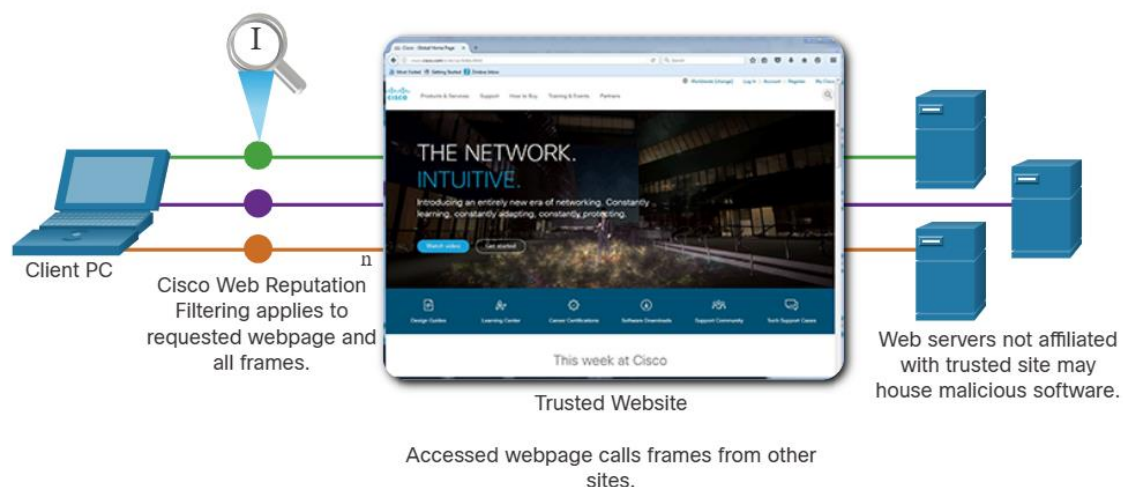
DNS queries for randomly generated domain names, or extremely long random-appearing subdomains, should be considered suspicious, especially if their occurrence spikes dramatically on the network. DNS proxy logs can be analyzed to detect these conditions. Alternatively, services such as the Cisco Umbrella passive DNS service can be used to block requests to suspected CnC and exploit domains.



## HTTP and HTTPS

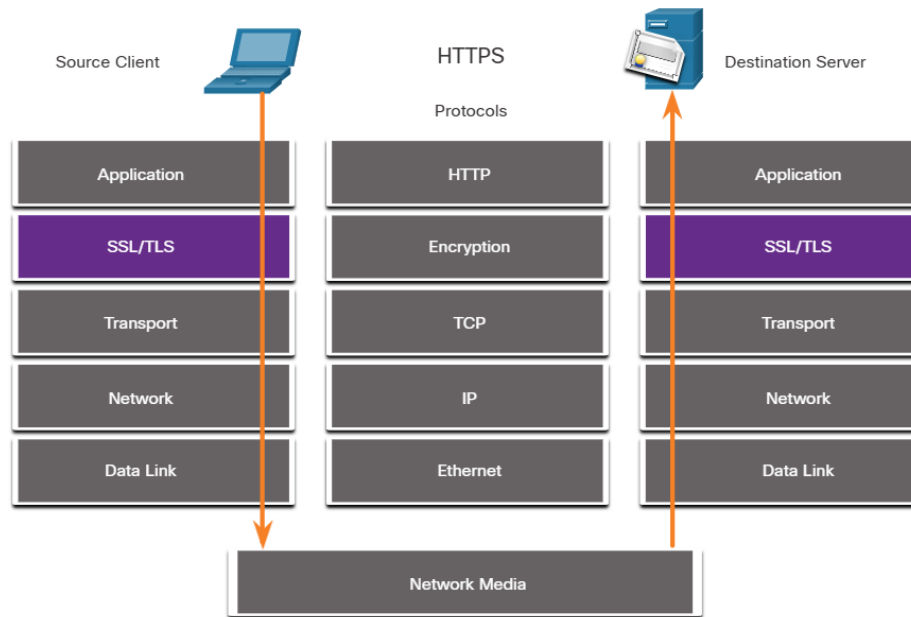
Hypertext Transfer Protocol (HTTP) is the backbone protocol of the World Wide Web. However, all information carried in HTTP is transmitted in plaintext from the source computer to the destination on the internet. HTTP does not protect data from alteration or interception by malicious parties, which is a serious threat to privacy, identity, and information security. All browsing activity should be considered to be at risk.

A common exploit of HTTP is called iFrame (inline frame) injection. Most web-based threats consist of malware scripts that have been planted on web servers. These web servers then direct browsers to infected servers by loading iframes. In iFrame injection, a threat actor compromises a webserver and plants malicious code which creates an invisible iFrame on a commonly visited webpage. When the iFrame loads, malware is downloaded, frequently from a different URL than the webpage that contains the iFrame code. Network security services, such as Cisco Web Reputation filtering, can detect when a website attempts to send content from an untrusted website to the host, even when sent from an iFrame, as shown in the figure.

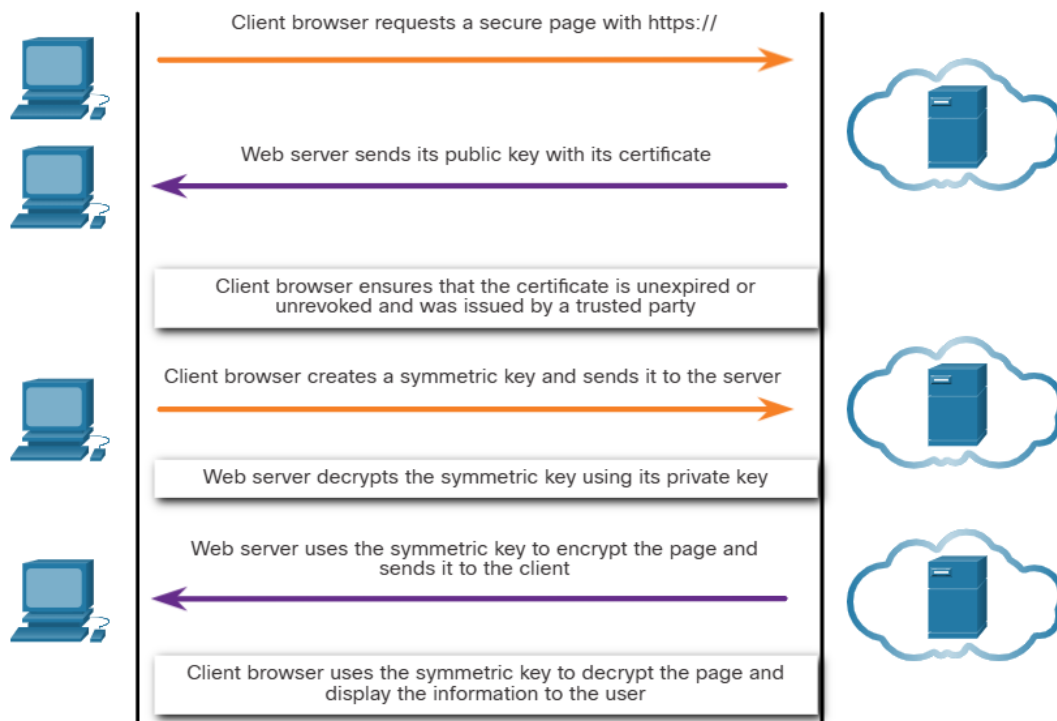


To address the alteration or interception of confidential data, many commercial organizations have adopted HTTPS or implemented HTTPS-only policies to protect visitors to their websites and services.

HTTPS adds a layer of encryption to the HTTP protocol by using secure socket layer (SSL), as shown in the figure. This makes the HTTP data unreadable as it leaves the source computer until it reaches the server. Note that HTTPS is not a mechanism for web server security. It only secures HTTP protocol traffic while it is in transit.



Unfortunately, the encrypted HTTPS traffic complicates network security monitoring. Some security devices include SSL decryption and inspection; however, this can present processing and privacy issues. In addition, HTTPS adds complexity to packet captures due to the additional messaging involved in establishing the encrypted connection. This process is summarized in the figure and represents additional overhead on top of HTTP.

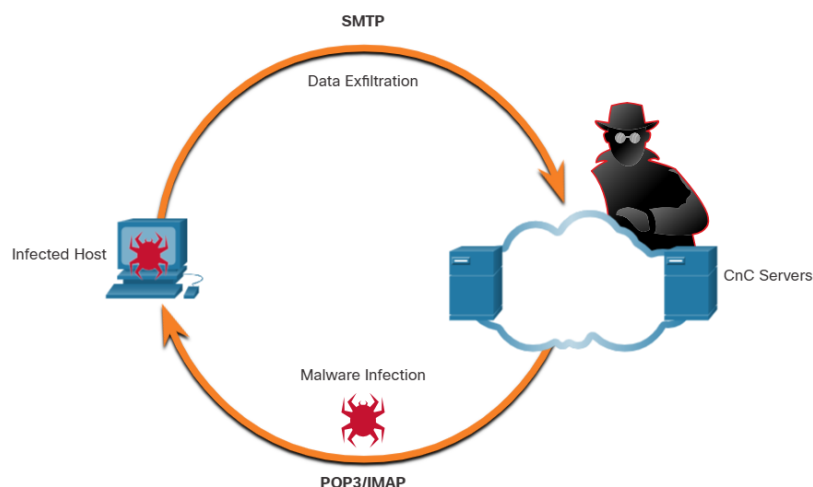


## Email Protocols

Email protocols such as SMTP, POP3, and IMAP can be used by threat actors to spread malware, exfiltrate data, or provide channels to malware CnC servers, as shown in the figure.

SMTP sends data from a host to a mail server and between mail servers. Like DNS and HTTP, it is a common protocol to see leaving the network. Because there is so much SMTP traffic, it is not always monitored. However, SMTP has been used in the past by malware to exfiltrate data from the network. In the 2014 hack of Sony Pictures, one of the exploits used SMTP to exfiltrate user details from compromised hosts to CnC servers. This information may have been used to help develop exploits of secured resources within the Sony Pictures network. Security monitoring could reveal this type of traffic based on features of the email message.

IMAP and POP3 are used to download email messages from a mail server to the host computer. For this reason, they are the application protocols that are responsible for bringing malware to the host. Security monitoring can identify when a malware attachment entered the network and which host it first infected. Retrospective analysis can then track the behavior of the malware from that point forward. In this way, the malware behavior can better be understood and the threat identified. Security monitoring tools may also allow recovery of infected file attachments for submission to malware sandboxes for analysis.



## ICMP

ICMP has many legitimate uses, however ICMP functionality has also been used to craft a number of types of exploits. ICMP can be used to identify hosts on a network, the structure of a network, and determine the operating systems at use on the network. It can also be used as a vehicle for various types of DoS attacks.

ICMP can also be used for data exfiltration. Because of the concern that ICMP can be used to surveil or deny service from outside of the network, ICMP traffic from inside the network is



sometimes overlooked. However, some varieties of malware use crafted ICMP packets to transfer files from infected hosts to threat actors using this method, which is known as ICMP tunneling.

Search the internet for a detailed explanation of the well-known LOKI exploit.

Note: One or all of the available sites in your search might be blocked by your institution's firewall.

A number of tools exist for crafting tunnels. Search the internet for Ping Tunnel to explore one such tool.

## **Security Technologies**

### **ACLs**

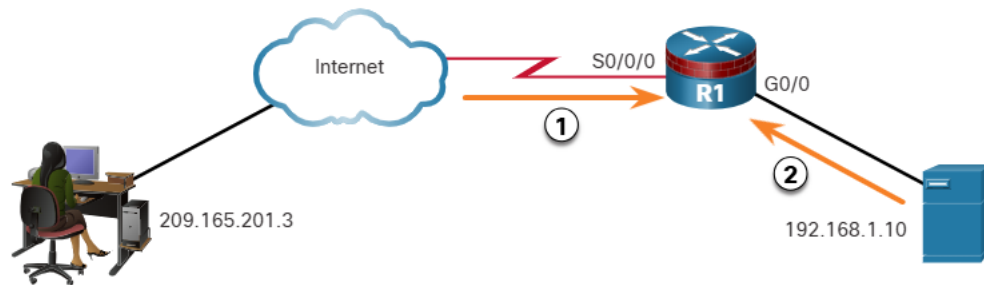
Many technologies and protocols can have impacts on security monitoring. Access Control Lists (ACLs) are among these technologies. ACLs can give a false sense of security if they are overly relied upon. ACLs, and packet filtering in general, are technologies that contribute to an evolving set of network security protections.

The figure illustrates the use of ACLs to permit only specific types of Internet Control Message Protocol (ICMP) traffic. The server at 192.168.1.10 is part of the inside network and is allowed to send ping requests to the outside host at 209.165.201.3. The outside host's return ICMP traffic is allowed if it is an ICMP reply, source quench (tells the source to reduce the pace of traffic), or any ICMP unreachable message. All other ICMP traffic types are denied. For example, the outside host cannot initiate a ping request to the inside host. The outbound ACL is allowing ICMP messages that report various problems. This will allow ICMP tunneling and data exfiltration.

Attackers can determine which IP addresses, protocols, and ports are allowed by ACLs. This can be done either by port scanning, penetration testing, or through other forms of reconnaissance. Attackers can craft packets that use spoofed source IP addresses. Applications can establish connections on arbitrary ports. Other features of protocol traffic can also be manipulated, such as the established flag in TCP segments. Rules cannot be anticipated and configured for all emerging packet manipulation techniques.

In order to detect and react to packet manipulation, more sophisticated behavior and context-based measures need to be taken. Cisco Next Generation firewalls, Advanced Malware Protection (AMP), and email and web content appliances are able to address the shortcomings of rule-based security measures.

### **Mitigating ICMP Abuse**



#### 1. Rules on R1 for ICMP traffic from the Internet

```
access-list 112 permit icmp any any echo-reply
access-list 112 permit icmp any any source-quench
access-list 112 permit icmp any any unreachable
access-list 112 deny icmp any any
access-list 112 permit ip any any
```

#### 2. Rules on R1 for ICMP traffic from inside the network

```
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any echo
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any parameter-problem
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any packet-too-big
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any source-quench
access-list 114 deny icmp any any
access-list 114 permit ip any any
```

## NAT and PAT

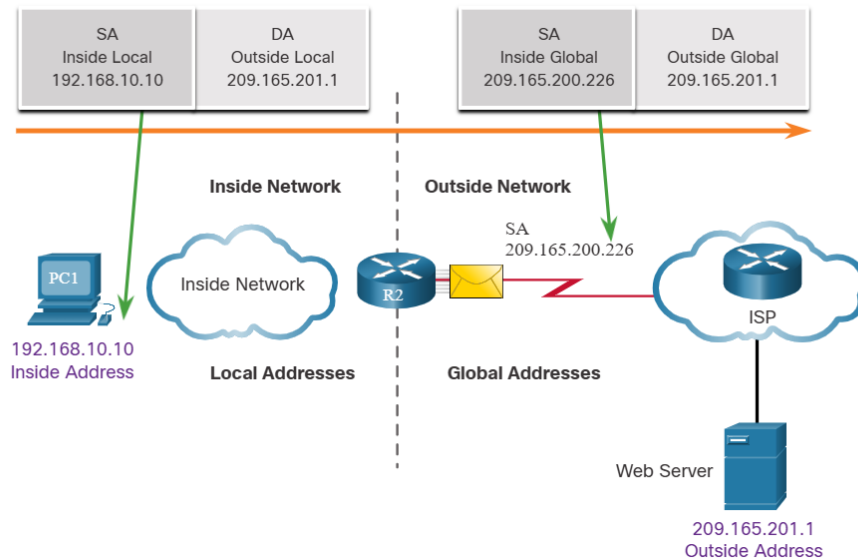
Network Address Translation (NAT) and Port Address Translation (PAT) can complicate security monitoring. Multiple IP addresses are mapped to one or more public addresses that are visible on the internet, hiding the individual IP addresses that are inside the network (inside addresses).

The figure illustrates the relationship between internal and external addresses that are used as source addresses (SA) and destination addresses (DA). These internal and external addresses are in a network that is using NAT to communicate with a destination on the internet. If PAT is in effect, and all IP addresses leaving the network use the 209.165.200.226 inside global address for traffic to the internet, it could be difficult to log the specific inside device that is requesting and receiving the traffic when it enters the network.

This problem can be especially relevant with NetFlow data. NetFlow flows are unidirectional and are defined by the addresses and ports that they share. NAT will essentially break a flow that passes a NAT gateway, making flow information beyond that point unavailable. Cisco offers security products that will “stitch” flows together even if the IP addresses have been replaced by NAT.

NetFlow is discussed in more detail later in the module.

## Network Address Translation



## Encryption, Encapsulation, and Tunneling

As mentioned with HTTPS, encryption can present challenges to security monitoring by making packet details unreadable. Encryption is part of VPN technologies. In VPNs, a commonplace protocol like IP, is used to carry encrypted traffic. The encrypted traffic essentially establishes a virtual point-to-point connection between networks over public facilities. Encryption makes the traffic unreadable to any other devices but the VPN endpoints.

A similar technology can be used to create a virtual point-to-point connection between an internal host and threat actor devices. Malware can establish an encrypted tunnel that rides on a common and trusted protocol, and use it to exfiltrate data from the network. A similar method of data exfiltration was discussed previously for DNS.

## Peer-to-Peer Networking and Tor

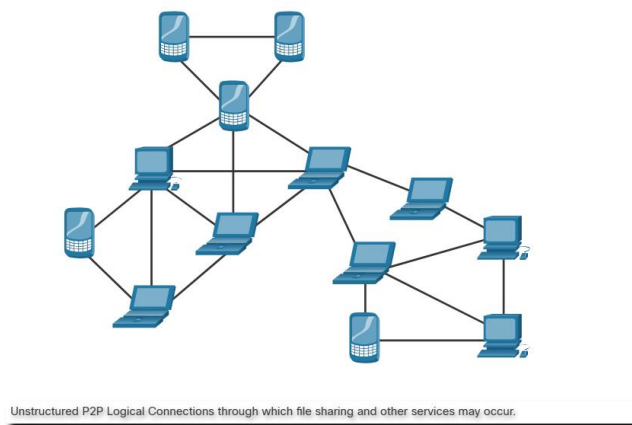
In peer-to-peer (P2P) networking, shown in the figure, hosts can operate in both client and server roles. Three types of P2P applications exist: file sharing, processor sharing, and instant messaging. In file sharing P2P, files on a participating machine are shared with members of the P2P network. Examples of this are the once popular Napster and Gnutella. Bitcoin is a P2P operation that involves the sharing of a distributed database, or ledger, that records Bitcoin balances and transactions. BitTorrent is a P2P file sharing network.

Any time that unknown users are provided access to network resources, security is a concern. File-sharing P2P applications should not be allowed on corporate networks. P2P network activity

can circumvent firewall protections and is a common vector for the spread of malware. P2P is inherently dynamic. It can operate by connecting to numerous destination IP addresses, and it can also use dynamic port numbering. Shared files are often infected with malware, and threat actors can position their malware on P2P clients for distribution to other users.

Processor sharing P2P networks donate processor cycles to distributed computational tasks. Cancer research, searching for extraterrestrials, and scientific research use donated processor cycles to distribute computational tasks.

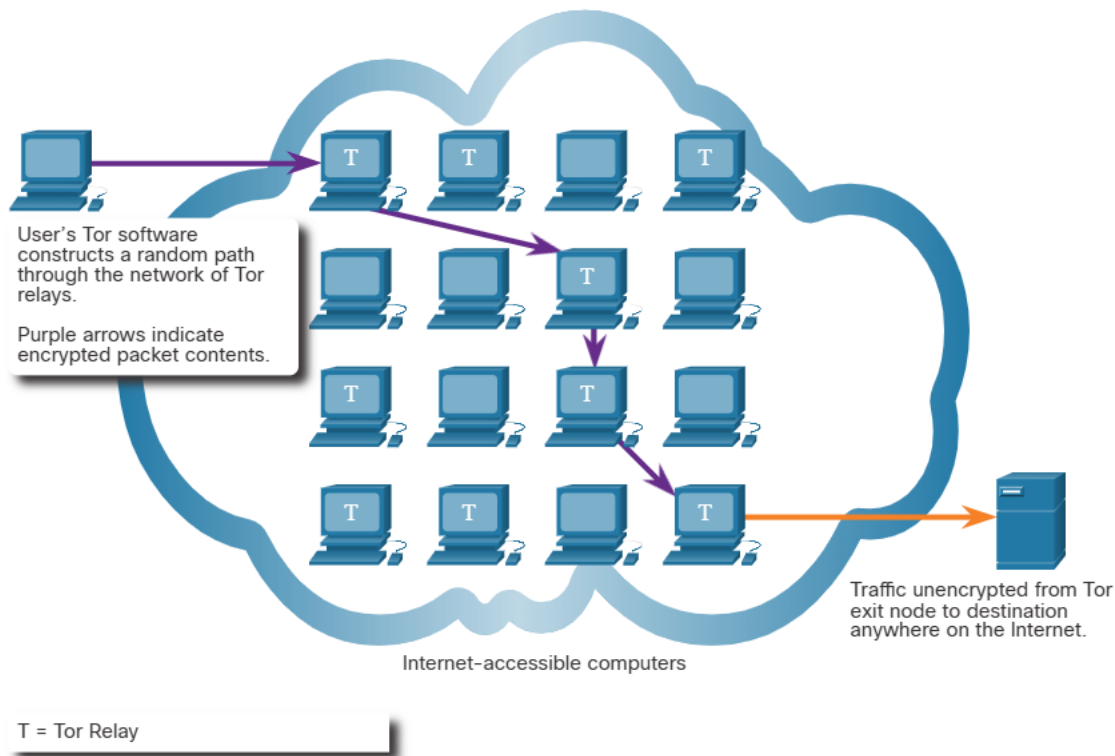
Instant messaging (IM) is also considered to be a P2P application. IM has legitimate value within organizations that have geographically distributed project teams. In this case, specialized IM applications are available, such as the Webex Teams platform, which are more secure than IM that uses public servers.



Tor is a software platform and network of P2P hosts that function as internet routers on the Tor network. The Tor network allows users to browse the internet anonymously. Users access the Tor network by using a special browser. When a browsing session is begun, the browser constructs a layered end-to-end path across the Tor server network that is encrypted, as shown in the figure. Each encrypted layer is “peeled away” like the layers of an onion (hence “onion routing”) as the traffic traverses a Tor relay. The layers contain encrypted next-hop information that can only be read by the router that needs to read the information. In this way, no single device knows the entire path to the destination, and routing information is readable only by the device that requires it. Finally, at the end of the Tor path, the traffic reaches its internet destination. When traffic is returned to the source, an encrypted layered path is again constructed.

Tor presents a number of challenges to cybersecurity analysts. First, Tor is widely used by criminal organizations on the “dark net.” In addition, Tor has been used as a communications channel for malware CnC. Because the destination IP address of Tor traffic is obfuscated by encryption, with only the next-hop Tor node known, Tor traffic avoids block lists that have been configured on security devices.

## Tor Operation

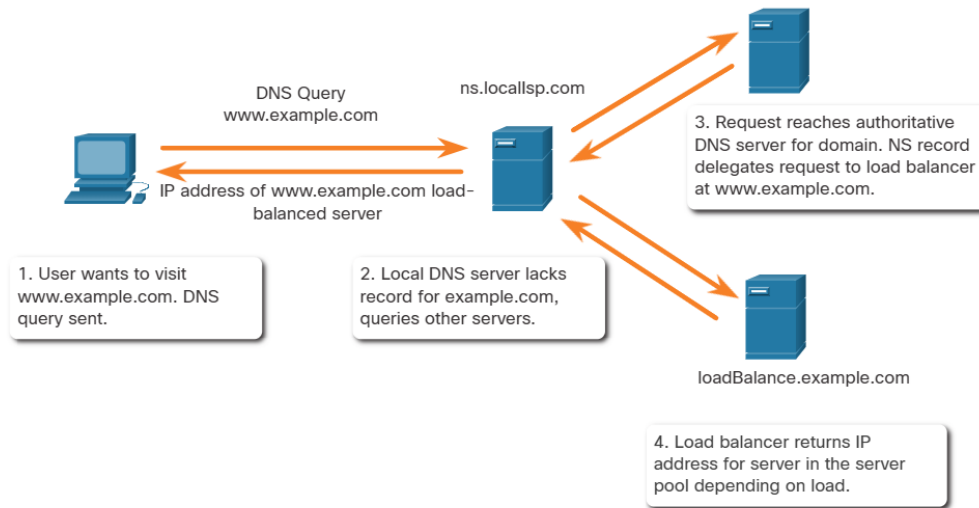


## Load Balancing

Load balancing involves the distribution of traffic between devices or network paths to prevent overwhelming network resources with too much traffic. If redundant resources exist, a load balancing algorithm or device will work to distribute traffic between those resources, as shown in the figure.

One way this is done on the internet is through various techniques that use DNS to send traffic to resources that have the same domain name but multiple IP addresses. In some cases, the distribution may be to servers that are distributed geographically. This can result in a single internet transaction being represented by multiple IP addresses on the incoming packets. This may cause suspicious features to appear in packet captures. In addition, some load balancing manager (LBM) devices use probes to test for the performance of different paths and the health of different devices. For example, an LBM may send probes to the different servers that it is load balancing traffic in order to detect that the servers are operating. This is done to avoid sending traffic to a resource that is not available. These probes can appear to be suspicious traffic if the cybersecurity analyst is not aware that this traffic is part of the operation of the LBM.

## Load Balancing with DNS Delegation



## Network Security Data

### Types of Security Data

#### a. Alert Data

Alert data consists of messages generated by intrusion prevention systems (IPSs) or intrusion detection systems (IDSs) in response to traffic that violates a rule or matches the signature of a known exploit. A network IDS (NIDS), such as Snort, comes configured with rules for known exploits. Alerts are generated by Snort and are made readable and searchable by the Sguil and Squert applications, which are part of the Security Onion suite of NSM tools.

A testing site that is used to determine if Snort is operating is the tesmyids site. Search for it on the internet. It consists of a single webpage that displays only the following text uid=0(root) gid=0(root) groups=0(root). If Snort is operating correctly and a host visits this site, a signature will be matched and an alert will be triggered. This is an easy and harmless way to verify that the NIDS is running.

The Snort rule that is triggered is:

```
alert ip any any -> any any (msg:"GPL ATTACK\_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast\_pattern:only; classtype:bad-unknown; sid:2100498;
rev:8;)
```

This rule generates an alert if any IP address in the network receives data from an external source that contains content with text matching the pattern of uid=0(root). The alert contains the message GPL ATTACK\_RESPONSE id check returned root. The ID of the Snort rule that was triggered is 2100498.

The highlighted line in the figure displays a Sguil alert that was generated by visiting the testmyids website. The Snort rule and the packet data for the content received from the testmyids webpage is displayed in the lower right-hand area of the Sguil interface.

## Sguil Console Showing Test Alert from Snort IDS

The screenshot shows the Sguil-0.9.0 interface. The top bar indicates 'Connected To localhost' and shows the user 'analyst' with ID '2'. The main window is divided into two panes. The left pane displays a table of real-time events, with one row highlighted in yellow. The right pane shows the details of the selected alert, including the Snort rule and the packet data.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion...	5.1482	2020-05-10 21:20:55	209.165.201.17	52332	209.165.200.235	80	6	ET WEB_SPECIFIC_APPS phpSkeSite theme parameter remote file inclusi
RT	1	seconion...	7.1795	2020-05-10 21:20:55	209.165.201.17	52332	209.165.200.235	80	6	ET WEB_SPECIFIC_APPS phpSkeSite theme parameter remote file inclusi
RT	1	seconion...	7.1688	2020-05-10 21:20:52	209.165.201.17	52298	209.165.200.235	80	6	ET WEB_SPECIFIC_APPS phptraverse mp3_id.php GLOBALS Parameter F
RT	1	seconion...	5.1375	2020-05-10 21:20:52	209.165.201.17	52298	209.165.200.235	80	6	ET WEB_SPECIFIC_APPS phptraverse mp3_id.php GLOBALS Parameter F
RT	1	seconion...	5.1580	2020-05-10 21:21:17	209.165.201.17	52414	209.165.200.235	80	6	ET WORM TheMoon.linksys.router 1
RT	1	seconion...	7.1893	2020-05-10 21:21:17	209.165.201.17	52414	209.165.200.235	80	6	ET WORM TheMoon.linksys.router 1
RT	4	seconion...	5.362	2020-05-10 20:58:01	209.165.200.235	6200	209.165.201.17	37071	6	GPL ATTACK_RESPONSE id check returned root
RT	4	seconion...	7.675	2020-05-10 20:58:01	209.165.200.235	6200	209.165.201.17	37071	6	GPL ATTACK_RESPONSE id check returned root
RT	12	seconion...	7.690	2020-05-10 21:20:25	209.165.201.17	52158	209.165.200.235	80	6	GPL EXPLOIT .cnf access
RT	12	seconion...	5.377	2020-05-10 21:20:25	209.165.201.17	52158	209.165.200.235	80	6	GPL EXPLOIT .cnf access
RT	8	seconion...	7.683	2020-05-10 21:20:25	209.165.201.17	52156	209.165.200.235	80	6	GPL EXPLOIT .httr access
RT	8	seconion...	5.370	2020-05-10 21:20:25	209.165.201.17	52156	209.165.200.235	80	6	GPL EXPLOIT .httr access
RT	1	seconion...	5.1055	2020-05-10 21:20:49	209.165.201.17	52238	209.165.200.235	80	6	GPL EXPLOIT /isadmpwd/aexp2.httr access
RT	1	seconion...	7.1368	2020-05-10 21:20:49	209.165.201.17	52238	209.165.200.235	80	6	GPL EXPLOIT /isadmpwd/aexp2.httr access

The detailed view of the selected alert shows the following information:

- Alert Message:** alert ip any any -> any any (msg:"GPL ATTACK\_RESPONSE id check returned root"; content:"uid=0(root)29"; fast\_pattern:only; classtype:bad-unknown; sid:2100498; rev:8; metadata:created\_at 2010\_09\_23, updated\_at 2010\_09\_23; /usr/share/snort/rules/seconion-ens192-1/downloaded.rules: Line 700)
- Packet Data:**

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	209.165.200.235	209.165.201.17	4	5	0	76	13818	2	0	64	53097

TCP	Source Port	Dest Port	R	R	R	C	S	S	S	I	N	Seq #	Ack #	Offset	Res	Window	Urg	ChkSum
	6200	37071	.	.	.	.	.	.	.	.	.	2269574098	3537747796	8	0	181	0	10442

DATA	75 69 64 3D 30 28 72 6F 6F 74 29 20 67 69 64 3D	30 28 72 6F 6F 74 29 6A	uid=0(root) gid=0(root).

### b. Session and Transaction Data

1. **ts:** session start timestamp
2. **uid:** unique session ID
3. **id.orig\_h:** IP address of host that originated the session (source address)
4. **id.orig\_p:** protocol port for the originating host (source port)
5. **id.resp\_h:** IP address of host responding to the originating host (destination address)
6. **id.resp\_p:** protocol of responding host (destination port)
7. **proto:** transport layer protocol for session
8. **service:** application layer protocol
9. **duration:** duration of the session
10. **orig\_bytes:** bytes from originating host



11. **resp\_bytes**: bytes from responding host
12. **orig\_packets**: packets from the originating host
13. **resp\_packets**: packets from responding host

Session data is a record of a conversation between two network endpoints, which are often a client and a server. The server could be inside the enterprise network or at a location accessed over the internet. Session data is data about the session, not the data retrieved and used by the client. Session data will include identifying information such as **the five tuples** of source and destination IP addresses, source and destination port numbers, and the IP code for the protocol in use. Data about the session typically includes a session ID, the amount of data transferred by source and destination, and information related to the duration of the session.

Zeek, formerly Bro, is a network security monitoring tool you will use in labs later in the course. The figure shows a partial output for three HTTP sessions from a Zeek connection log. Explanations of the fields are shown below the figure.

### Zeek Session Data - Partial Contents

1	2	3	4	5	6	7	8	9	10	11	12	13
ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	service	duration	orig_bytes	resp_bytes	orig_pkts	resp_pkts
1320279567	CEv1Z54N5gT3PwJLog	192.168.2.76	52034	174.129.249.33	80	tcp	http	0.082899	389	1495	5	4
1320279567	Ci6Ueb3SkSJHwASNN4	192.168.2.76	52035	184.72.234.3	80	tcp	http	2.56194	905	731	9	8
1320279567	CaTMSv1Sb8HtFunqij	192.168.2.76	52033	184.72.234.3	80	tcp	http	3.345539	1856	1445	15	13

Transaction data consists of the messages that are exchanged during network sessions. These transactions can be viewed in packet capture transcripts. Device logs kept by servers also contain information about the transactions that occur between clients and servers. For example, a session might include the downloading of content from a webserver, as shown in the figure. The transactions that represent the requests and replies would be logged in an access log on the server or by a NIDS like Zeek. The session is all traffic involved in making up the request, the transaction is the request itself.



## Transaction Data

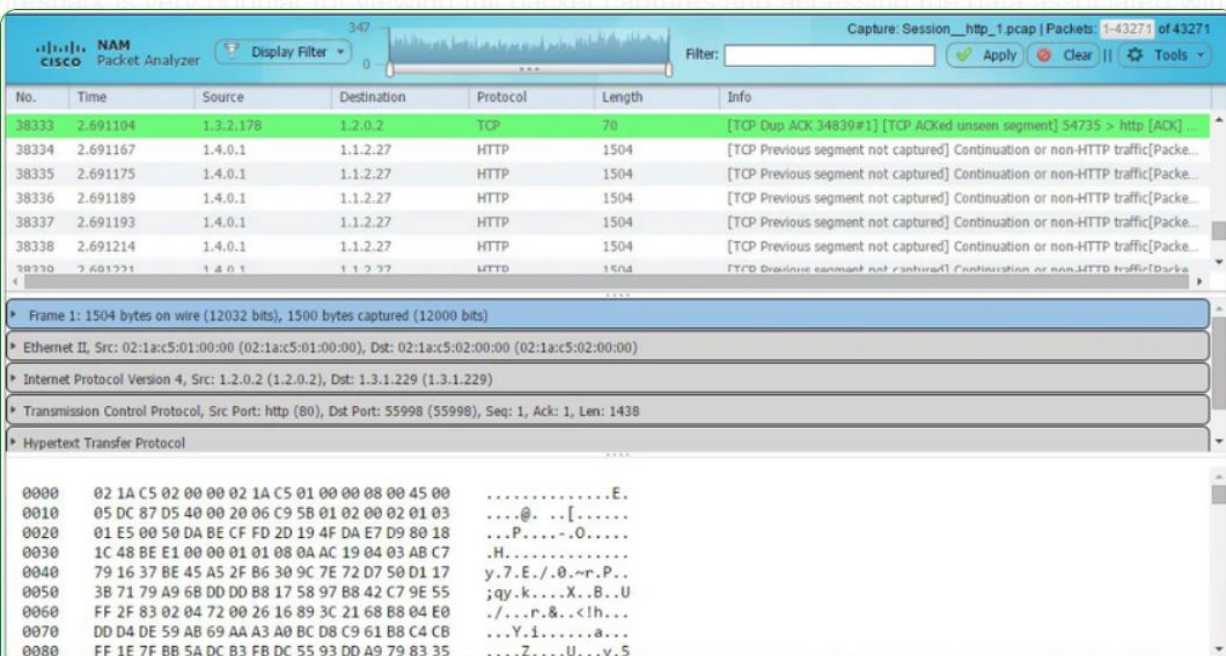


## Full Packet Captures

Full packet captures are the most detailed network data that is generally collected. Because of the amount of detail, they are also the most storage and retrieval intensive types of data used in NSM. Full packet captures contain not only data about network conversations, like session data. Full packet captures also contain the actual contents of the conversations. Full packet captures contain the text of email messages, the HTML in webpages, and the files that enter or leave the network. Extracted content can be recovered from full packet captures and analyzed for malware or user behavior that violates business and security policies. The familiar tool Wireshark is very popular for viewing full packet captures and accessing the data associated with network conversations.

The figure illustrates the interface for the Network Analysis Monitor component of Cisco Prime Infrastructure system, which, like Wireshark, can display full packet captures.

## Cisco Prime Network Analysis Module - Full Packet Capture



No.	Time	Source	Destination	Protocol	Length	Info
38333	2.691104	1.3.2.178	1.2.0.2	TCP	70	[TCP Dup ACK 34839#1] [TCP ACKed unseen segment] 54735 > http [ACK]
38334	2.691167	1.4.0.1	1.1.2.27	HTTP	1504	[TCP Previous segment not captured] Continuation or non-HTTP traffic[Packe...
38335	2.691175	1.4.0.1	1.1.2.27	HTTP	1504	[TCP Previous segment not captured] Continuation or non-HTTP traffic[Packe...
38336	2.691189	1.4.0.1	1.1.2.27	HTTP	1504	[TCP Previous segment not captured] Continuation or non-HTTP traffic[Packe...
38337	2.691193	1.4.0.1	1.1.2.27	HTTP	1504	[TCP Previous segment not captured] Continuation or non-HTTP traffic[Packe...
38338	2.691214	1.4.0.1	1.1.2.27	HTTP	1504	[TCP Previous segment not captured] Continuation or non-HTTP traffic[Packe...
38339	2.691221	1.4.0.1	1.1.2.27	HTTP	1504	[TCP Previous segment not captured] Continuation or non-HTTP traffic[Packe...

Frame 1: 1504 bytes on wire (12032 bits), 1500 bytes captured (12000 bits)		
Ethernet II, Src: 02:1a:c5:01:00:00 (02:1a:c5:01:00:00), Dst: 02:1a:c5:02:00:00 (02:1a:c5:02:00:00)		
Internet Protocol Version 4, Src: 1.2.0.2 (1.2.0.2), Dst: 1.3.1.229 (1.3.1.229)		
Transmission Control Protocol, Src Port: http (80), Dst Port: 55998 (55998), Seq: 1, Ack: 1, Len: 1438		
Hypertext Transfer Protocol		

Hex	ASCII
0000 02 1A C5 02 00 00 02 1A C5 01 00 00 08 00 45 00	.....E.
0010 05 DC 87 D5 40 00 20 06 C9 5B 01 02 00 02 01 03	....@. ..[.....
0020 01 E5 00 50 DA BE CF FD 2D 19 4F DA E7 D9 80 18	...P.....O.....
0030 1C 48 BE E1 00 00 01 01 08 0A AC 19 04 03 AB C7	.H.....
0040 79 16 37 BE 45 A5 2F B6 30 9C 7E 72 D7 50 D1 17	y.7.E./..0..r.P..
0050 3B 71 79 A9 6B DD DD B8 17 58 97 B8 42 C7 9E 55	;qy.k....X..B..U
0060 FF 2F 83 02 04 72 00 26 16 89 3C 21 68 B8 04 E0	./...r.&..< h...
0070 DD D4 DE 59 AB 69 AA A3 A0 BC D8 C9 61 B8 C4 CB	...Y.i.....a...
0080 FF 1E 7F 8B 5A DC B3 FB 0C 55 93 DD A9 79 83 35	...Z....U...y.5

### Statistical Data

Like session data, statistical data is about network traffic. Statistical data is created through the analysis of other forms of network data. Conclusions can be made that describe or predict network behavior from this analysis. Statistical characteristics of normal network behavior can be compared to current network traffic in an effort to detect anomalies. Statistics can be used to characterize normal amounts of variation in network traffic patterns in order to identify network conditions that are significantly outside of those ranges. Statistically significant differences should raise alarms and prompt investigation.

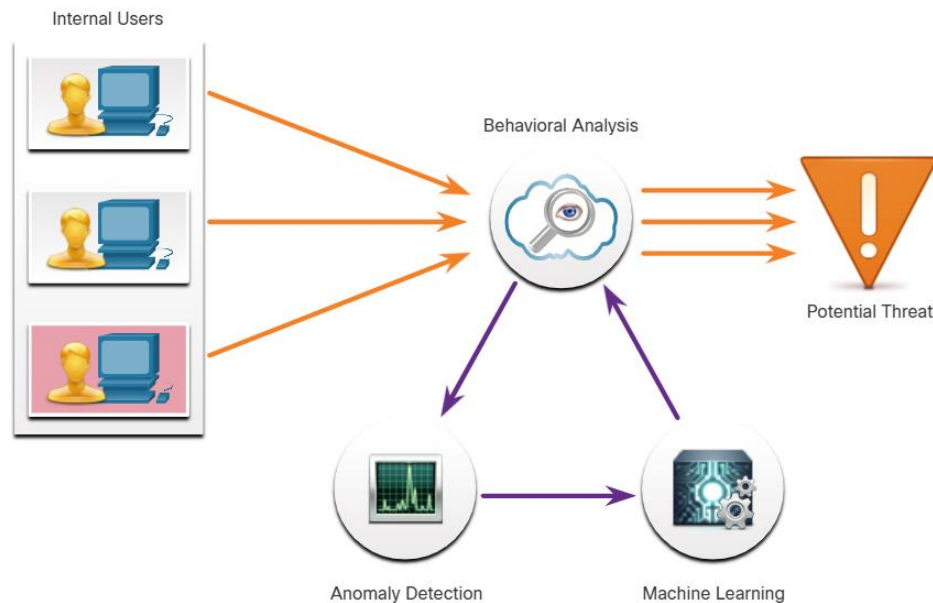
Network Behavior Analysis (NBA) and Network Behavior Anomaly Detection (NBAD) are approaches to network security monitoring that use advanced analytical techniques to analyze NetFlow or Internet Protocol Flow Information Export (IPFIX) network telemetry data. Techniques such as predictive analytics and artificial intelligence perform advanced analyses of detailed session data to detect potential security incidents.

**Note:** IPFIX is the IETF standard version of Cisco NetFlow version 9.

An example of an NSM tool that utilizes statistical analysis is Cisco Cognitive Threat Analytics. It is able to find malicious activity that has bypassed security controls or entered the network through unmonitored channels (including removable media) and is operating inside an organization's environment. Cognitive Threat Analytics is a cloud-based product that uses machine learning and statistical modeling of networks. It creates a baseline of the traffic in a

network and identifies anomalies. It analyzes user and device behavior, and web traffic, to discover command-and-control communications, data exfiltration, and potentially unwanted applications operating in the infrastructure. The figure illustrates an architecture for Cisco Cognitive Threat Analytics.

### Cisco Cognitive Threat Analytics



## End Device Logs

### Host Logs

As previously discussed, host-based intrusion detection systems (HIDS) run on individual hosts. HIDS not only detects intrusions, but in the form of host-based firewalls, can also prevent intrusion. This software creates logs and stores them on the host. This can make it difficult to get a view of what is happening on hosts in the enterprise, so many host-based protections have a way to submit logs to centralized log management servers. In this way, the logs can be searched from a central location using NSM tools.

HIDS systems can use agents to submit logs to management servers. OSSEC, a popular open-source HIDS, includes a robust log collection and analysis functionality. Search OSSEC on the internet to learn more. Microsoft Windows includes several methods for automated host log collection and analysis. Tripwire offers a HIDS for Linux that includes similar functionality. All can scale to larger enterprises.

Microsoft Windows host logs are visible locally through Event Viewer. Event Viewer keeps five types of logs:

- **Application logs** – These contain events logged by various applications.
- **System logs** – These include events regarding the operation of drivers, processes, and hardware.
- **Setup logs** – These record information about the installation of software, including Windows updates.
- **Security logs** – These record events related to security, such as logon attempts and operations related to file or object management and access.
- **Command-line logs** - Attackers who have gained access to a system, and some types of malware, execute commands from the command-line interface (CLI) rather than a GUI. Logging command line execution will provide visibility into this type of incident.

Various logs can have different event types. Security logs consist only of audit success or failure messages. On Windows computers, security logging is carried out by the Local Security Authority Subsystem Service (LSASS), which is also responsible for enforcing security policies on a Windows host. LSASS runs as lsass.exe. It is frequently faked by malware. It should be running from the Windows System32 directory. If a file with this name, or a camouflaged name, such as lsass.exe, is running or running from another directory, it could be malware.

Windows Events are identified by ID numbers and brief descriptions. An encyclopedia of security event IDs, some with additional details, is available from Ultimate Windows Security on the web.

The table explains the meaning of the five Windows host log event types.

Event Type	Description
Error	An error is an event that indicates a significant problem such as loss of data or loss of functionality. For example, if a service fails to load during startup, an error event is logged.
Warning	A Warning is an event that is not necessarily significant but may indicate a possible future problem. For example, when disk space is low, a warning event is logged. If an application can recover from an event without loss of functionality or data, it can generally classify the event as a warning event.
Information	An information event describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, it may be appropriate to log an information event. Note that it is generally inappropriate for a desktop application to log an event each time it starts.
Success Audit	A success audit is an event that records an audited security access attempt that is successful. For example, a user's successful attempt to log on to the system is logged as a success audit event.
Failure Audit	A failure audit is an event that records an audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt is logged as a failure audit event.

## Syslog

Syslog includes specifications for message formats, a client-server application structure, and network protocol. Many different types of network devices can be configured to use the syslog standard to log events to centralized syslog servers.

Syslog is a client/server protocol. Syslog was defined within the Syslog working group of the IETF (RFC 5424) and is supported by a wide variety of devices and receivers across multiple platforms.

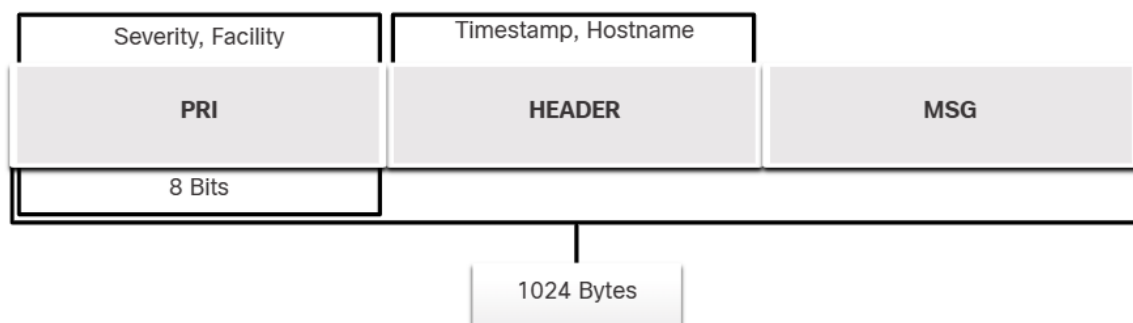
The Syslog sender sends a small (less than 1KB) text message to the Syslog receiver. The Syslog receiver is commonly called "syslogd," "Syslog daemon," or "Syslog server." Syslog messages can be sent via UDP (port 514) and/or TCP (typically, port 5000). While there are some exceptions, such as SSL wrappers, this data is typically sent in plaintext over the network.

The full format of a Syslog message that is seen on the network has three distinct parts, as shown in the figure.

- PRI (priority)
- HEADER
- MSG (message text)

The PRI consists of two elements, the Facility and Severity of the message, which are both integer values. The Facility consists of broad categories of sources that generated the message, such as the system, process, or application. The Facility value can be used by logging servers to direct the message to the appropriate log file. The Severity is a value from 0-7 that defines the severity of the message.

### Syslog Packet Format



The HEADER section of the message contains the timestamp in MMM DD HH:MM:SS format. If the timestamp is preceded by the period (.) or asterisk (\*) symbols, a problem is indicated with NTP. The HEADER section also includes the hostname or IP address of the device that is the source of the message.

The MSG portion contains the meaning of the syslog message. This can vary between device manufacturers and can be customized. Therefore, this portion of the message is the most meaningful and useful to the cybersecurity analyst.

## Server Logs

Server logs are an essential source of data for network security monitoring. Network application servers such as email and web servers keep access and error logs. DNS proxy server logs which document all the DNS queries and responses that occur on the network are especially important. DNS proxy logs are useful for identifying hosts that may have visited dangerous websites and for identifying DNS data exfiltration and connections to malware command-and-control servers. Many UNIX and Linux servers use syslog. Others may use proprietary logging. The contents of log file events depend on the type of server.

Two important log files to be familiar with are the Apache webserver access logs and Microsoft Internet Information Server (IIS) access logs. Examples of each are shown below.

### Apache Access Log

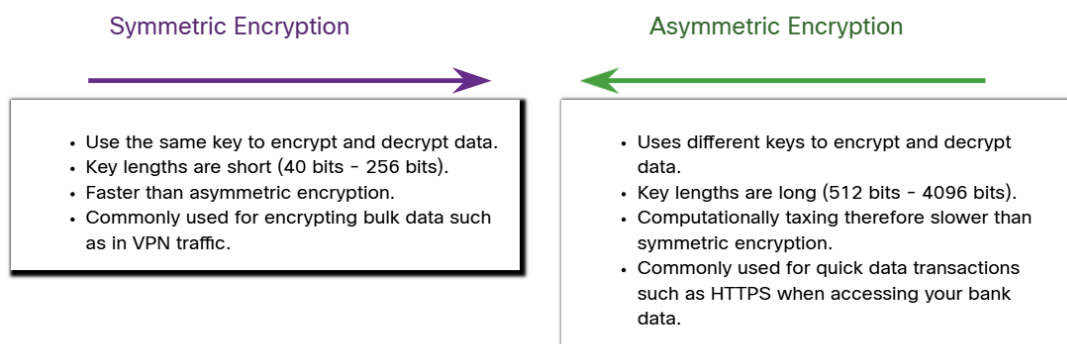
```
203.0.113.127 - dsmith [10/Oct/2016:10:26:57 - 0500] "GET /logo_sm.gif HTTP/1.0" 200 2254
"http://www.example.com/links.html" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101
Firefox/47.0"
```

### IIS Access Log

```
6/14/2016, 16:22:43, 203.0.113.24, -, W3SVC2, WEB3, 198.51.100.10, 80, GET, /home.htm, -, 200, 0, 15321, 159,
15, HTTP/1.1, Mozilla/5.0 (compatible; MSIE 9.0; Windows Phone OS 7.5; Trident/5.0; IEMobile/9.0), -,
http://www.example.com
```

## SIEM and Log Collection

Security Information and Event Management (SIEM) technology is used in many organizations to provide real-time reporting and long-term analysis of security events, as shown in the figure.

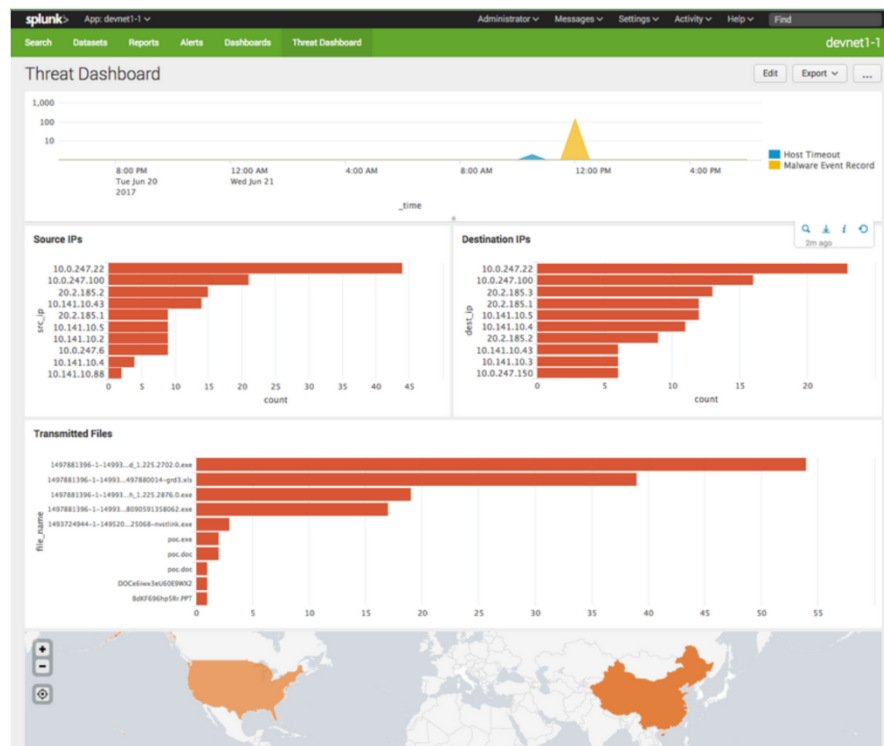


SIEM combines the essential functions of security event management (SEM) and security information management (SIM) tools to provide a comprehensive view of the enterprise network using the following functions:

- **Log collection** – Event records from sources throughout the organization provide important forensic information and help to address compliance reporting requirements.
- **Normalization** – This maps log messages from different systems into a common data model, enabling the organization to connect and analyze related events, even if they are initially logged in different source formats.
- **Correlation** – This links logs and events from disparate systems or applications, speeding detection of and reaction to security threats.
- **Aggregation** – This reduces the volume of event data by consolidating duplicate event records.
- **Reporting** – This presents the correlated, aggregated event data in real-time monitoring and long-term summaries, including graphical interactive dashboards.
- **Compliance** – This is reporting to satisfy the requirements of various compliance regulations.

A popular SIEM is **Splunk**, which is made by a Cisco partner. The figure shows a Splunk Threat Dashboard. Splunk is widely used in SOCs. Another popular SIEM solution is **Security Onion with ELK**, which consists of the integrated **Elasticsearch, Logstash, and Kibana** applications. Security Onion includes other open-source network security monitoring tools.

## Splunk Threat Dashboard





As we know, security orchestration, automation, and response (SOAR) takes SIEM and goes beyond into automating security response workflows and facilitating incidence response. Because of the importance of network security, numerous companies have brought excellent products to the security tools market. However, these tools lack compatibility and require monitoring multiple independent product dashboards in order to process the many alerts that they generate. Because of the lack of cybersecurity professionals to monitor and analyze the large volume of security data, it is important that tools from multiple vendors can be integrated into a single platform. Integrated security platforms go beyond SIEM and SOAR to unify multiple security technologies, processes, and people into a unified team whose components build on rather than impede each other. Security platforms such as Cisco SecureX, Fortinet Security Fabric, and Paloalto Networks Cortex XDR promise to address network security monitoring complexity by integrating multiple functions and data sources into a single platform that will greatly enhance alert accuracy while offering robust defense.

## Network Logs

### Tcpdump

A Large Broadcast Domain



The tcpdump command line tool is a very popular packet analyzer. It can display packet captures in real time or write packet captures to a file. It captures detailed packet protocol and content data. Wireshark is a GUI built on tcpdump functionality. The structure of tcpdump captures varies depending on the protocol captured and the fields requested.

### NetFlow

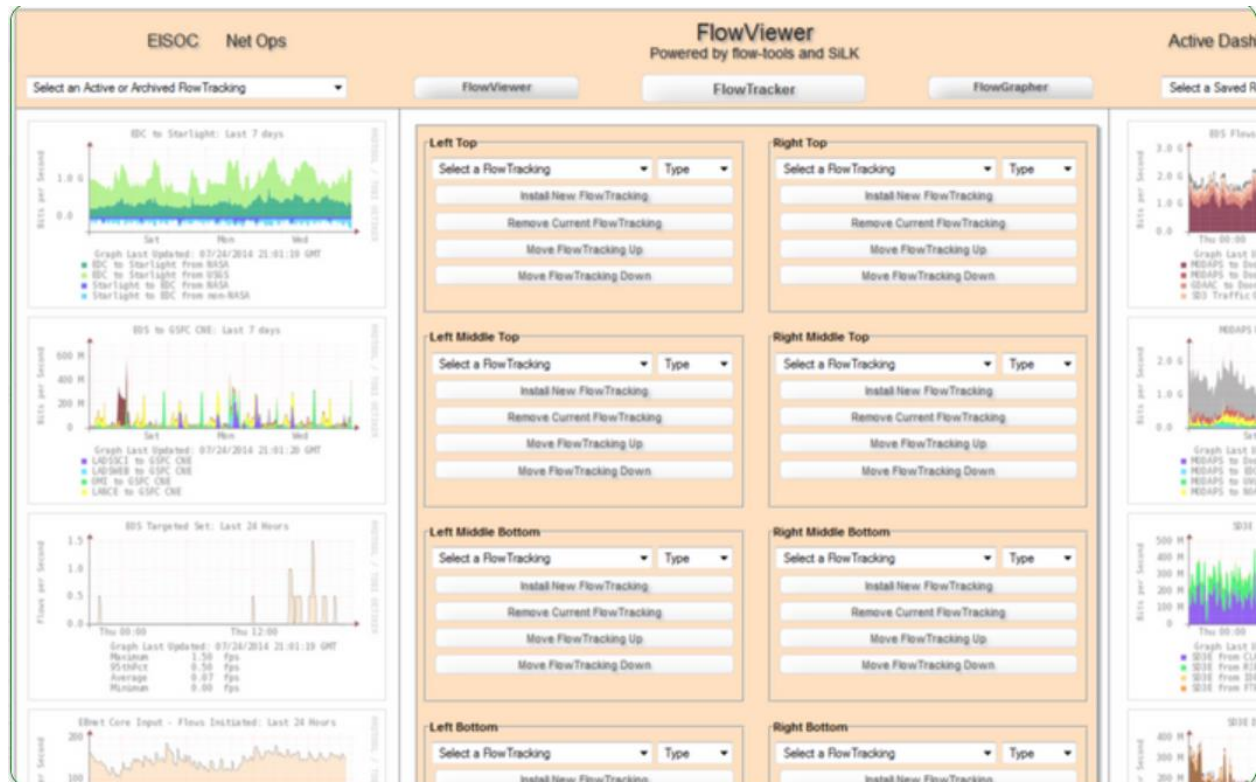
NetFlow is a protocol that was developed by Cisco as a tool for network troubleshooting and session-based accounting. NetFlow efficiently provides an important set of services for IP applications, including network traffic accounting, usage-based network billing, network planning, security, Denial-of-Service monitoring capabilities, and network monitoring. NetFlow provides valuable information about network users and applications, peak usage times, and traffic routing.

NetFlow does not do a full packet capture or capture the actual content in the packet. NetFlow records information about the packet flow including metadata. Cisco developed NetFlow and then allowed it to be used as a basis for an IETF standard called IPFIX. IPFIX is based on Cisco NetFlow Version 9.



NetFlow information can be viewed with tools such as the nfdump. Similar to tcpdump, nfdump provides a command line utility for viewing NetFlow data from the nfcapd capture daemon, or collector. Tools exist that add GUI functionality to viewing flows. The figure shows a screen from the open source FlowViewer tool.

FlowViewer NetFlow Session Data Dashboard



Traditionally, an IP Flow is based on a set of 5 to 7 IP packet attributes flowing in a single direction. A flow consists of all packets transmitted until the TCP conversation terminates. IP Packet attributes used by NetFlow are:

- IP source address
- IP destination address
- Source port
- Destination port
- Layer 3 protocol type
- Class of Service
- Router or switch interface

All packets with the same source/destination IP address, source/destination ports, protocol interface and class of service are grouped into a flow, and then packets and bytes are tallied. This methodology of fingerprinting or determining a flow is scalable because a large amount of

network information is condensed into a database of NetFlow information called the NetFlow cache.

All NetFlow flow records will contain the first five items in the list above, and flow start and end timestamps. The additional information that may appear is highly variable and can be configured on the NetFlow Exporter device. Exporters are devices that can be configured to create flow records and transmit those flow records for storage on a NetFlow collector device. An example of a basic NetFlow flow record, in two different formats, is shown in the figure.

#### Simple NetFlow v5 Records

```
Date flow start Duration Proto Src IP Addr:Port Dst IP Addr:Port Flags Tos Packets Bytes Flows 2017-08-30
00:09:12.596 00.010 TCP 10.1.1.2:80 -> 13.1.1.2:8974 .AP.SF 0 62 3512 1
```

```
Traffic Contribution: 8% (3/37)Flow information:IPV4 SOURCE ADDRESS:10.1.1.2IPV4 DESTINATION
ADDRESS:13.1.1.2INTERFACE INPUT:Se0/0/1TRNS SOURCE PORT:8974TRNS DESTINATION PORT:80IP TOS:0x00IP PROTOCOL:6FLOW
SAMPLER ID:0FLOW DIRECTION:Inputipv4 source mask:/0ipv4 destination mask:/8counter bytes:205ipv4 next hop
address:13.1.1.2tcp flags:0x1binterface output:Fa0/0counter packets:5timestamp first:00:09:12.596timestamp
last:00:09:12.606ip source as:0ip destination as:0
```

A large number of attributes for a flow are available. The IANA registry of IPFIX entities lists several hundred, with the first 128 being the most common.

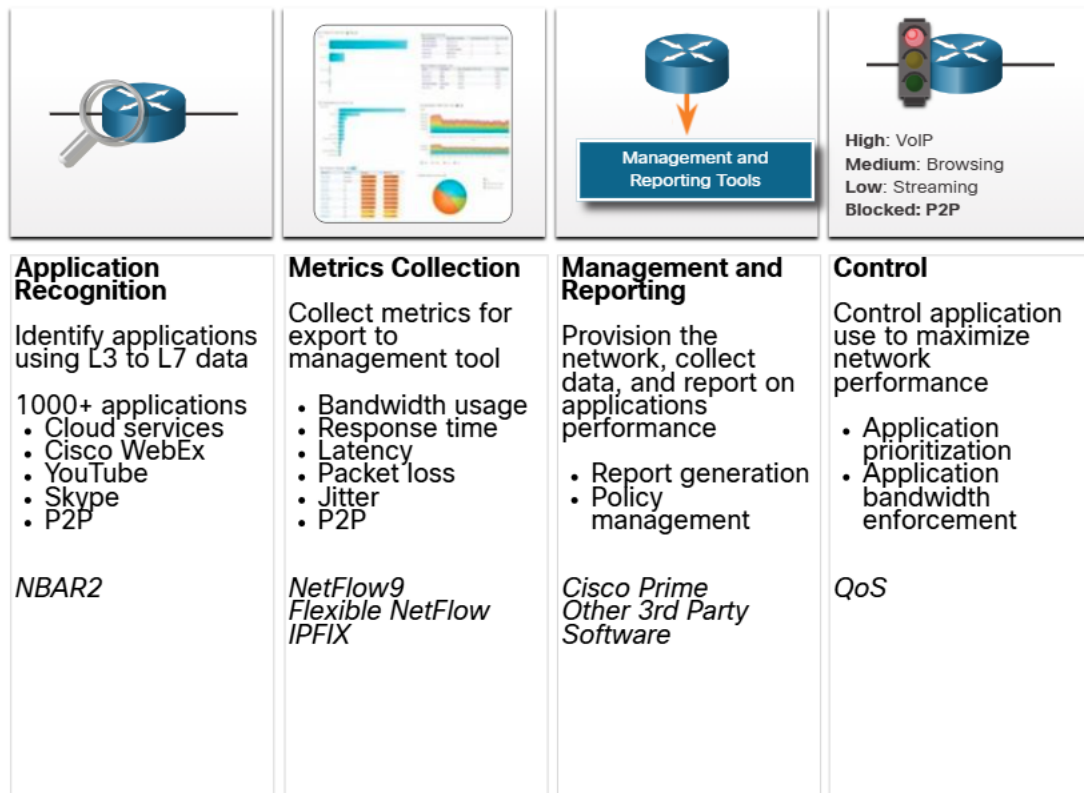
Although NetFlow was not initially conceived as tool for network security monitoring, it is seen as a useful tool in the analysis of network security incidents. It can be used to construct a timeline of compromise, understand individual host behavior, or to track the movement of an attacker or exploit from host to host within a network. The Cisco/Lancope Stealthwatch technology enhances the use of NetFlow data for NSM.

## Application Visibility and Control

The Cisco Application Visibility and Control (AVC) system, which is shown in the figure, combines multiple technologies to recognize, analyze, and control over 1000 applications. These include voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based applications. AVC uses Cisco next-generation network-based application recognition version 2 (NBAR2), also known as Next-Generation NBAR, to discover and classify the applications in use on the network. The NBAR2 application recognition engine supports over 1000 network applications.

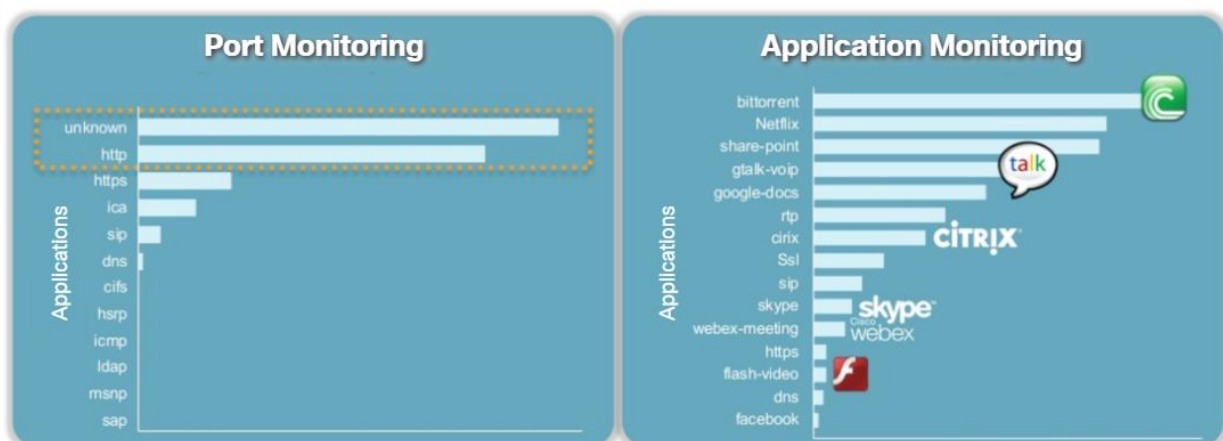
To truly understand the importance of this technology, consider the figure. Identification of network applications by port provides very little granularity and visibility into user behavior. However, application visibility through the identification of application signatures identifies what users are doing, whether it be teleconferencing or downloading movies to their phones.

## Cisco Application Visibility and Control



A management and reporting system, such as Cisco Prime, analyzes and presents the application analysis data into dashboard reports for use by network monitoring personnel. Application usage can also be controlled through quality of service classification and policies based on the AVC information.

## Port Monitoring vs. Application Monitoring



Devices that provide content filtering, such as the Cisco Email Security Appliance (ESA) and the Cisco Web Security Appliance (WSA), provide a wide range of functionalities for security monitoring. Logging is available for many of these functionalities.

WSA devices offer a similar depth of functioning. WSA effectively acts as a web proxy, meaning that it logs all inbound and outbound transaction information for HTTP traffic. These logs can be quite detailed and are customizable. They can be configured in a W3C compatibility format. The WSA can be configured to submit the logs to a server in various ways, including syslog, FTP, and SCP.

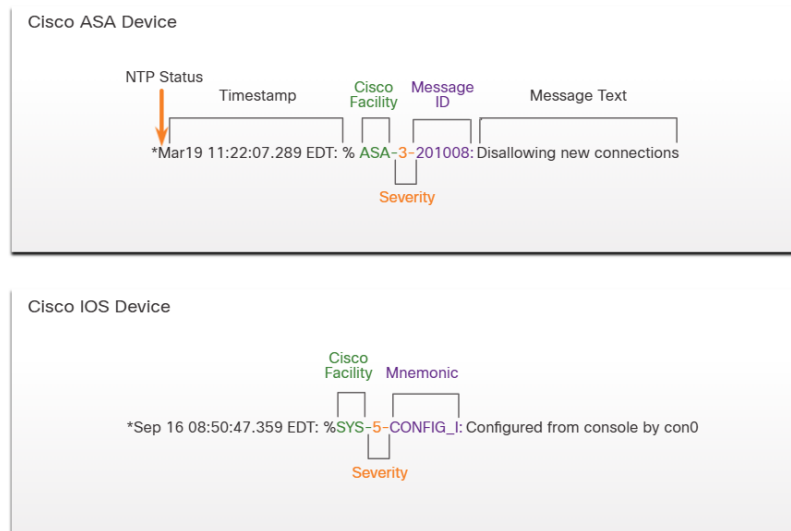
The figure illustrates the “drill-down” dashboards available from Cisco content filtering devices. By clicking components of the Overview reports, more relevant details are displayed. Target searches provide the most focused information.



## Logging from Cisco Devices

Cisco security devices can be configured to submit events and alerts to security management platforms using SNMP or syslog. The figure illustrates a syslog message generated by a Cisco ASA device and a syslog message generated by a Cisco IOS device.

### Cisco Syslog Message Formats



Note that there are two meanings used for the term facility in Cisco syslog messages. The first is the standard set of Facility values that were established by the syslog standards. These values are used in the PRI message part of the syslog packet to calculate the message priority. Cisco uses some of the values between 15 and 23 to identify Cisco log Facilities, depending on the platform. For example, Cisco ASA devices use syslog Facility 20 by default, which corresponds to local4. The other Facility value is assigned by Cisco and occurs in the MSG part of the syslog message.

Cisco devices may use slightly different syslog message formats, and may use mnemonics instead of message IDs, as shown in the figure. A dictionary of Cisco ASA syslog messages is available on the Cisco website.

## Proxy Logs

Proxy servers, such as those used for web and DNS requests, contain valuable logs that are a primary source of data for network security monitoring.

Proxy servers are devices that act as intermediaries for network clients. For example, an enterprise may configure a web proxy to handle web requests on the behalf of clients. Instead of requests for web resources being sent directly to the server from the client, the request is sent to a proxy server first. The proxy server requests the resources and returns them to the client. The

proxy server generates logs of all requests and responses. These logs can then be analyzed to determine which hosts are making the requests, whether the destinations are safe or potentially malicious, and to also gain insights into the kind of resources that have been downloaded.

Web proxies provide data that helps determine whether responses from the web were generated in response to legitimate requests or have been manipulated to appear to be responses but are in fact exploits. It is also possible to use web proxies to inspect outgoing traffic as means of data loss prevention (DLP). DLP involves scanning outgoing traffic to detect whether the data that is leaving the web contains sensitive, confidential, or secret information. Examples of popular web proxies are Squid, CCProxy, Apache Traffic Server, and WinGate.

An example of a Squid web proxy log in the Squid-native form appears below. Explanations of the field values appear in the table below the log entry.

### DNS Proxy Log Example

```
1265939281.764 19478 172.16.167.228 TCP_MISS/200 864
GEThttp://www.example.com//images/home.png - NONE/- image/png
```

Proxy Log Value	Explanation
1265939281.764	<b>Time</b> - in Unix epoch timestamp format with milliseconds
19478	<b>Duration</b> - the elapsed time for the request and response from Squid
172.16.167.228	<b>Client IP address</b>
TCP_MISS/200	<b>Result</b> - Squid result codes and HTTP status code separated by a slash
864	<b>Size</b> - the bytes of data delivered
GET	<b>Request</b> - HTTP request made by the client
http://www.example.com//images/home.png	<b>URI/URL</b> - address of the resource that was requested
-	<b>Client identity</b> - RFC 1413 value for the client that made the request. Not used by default.
NONE/-	<b>Peering code/Peer host</b> - neighbor cache server consulted
image/png	<b>Type</b> - MIME content type from the Content-Type value in the HTTP response header

**Note:** Open web proxies, which are proxies that are available to any internet user, can be used to obfuscate threat actor IP addresses. Open proxy addresses may be used in block list internet traffic.

## Cisco Umbrella

Cisco Umbrella, formerly OpenDNS, offers a hosted DNS service that extends the capability of DNS to include security enhancements. Rather than organizations hosting and maintaining block list, phishing protection, and other DNS-related security, Cisco Umbrella provides these protections in its own DNS service. Cisco Umbrella is able to apply many more resources to managing DNS than most organizations can afford. Cisco Umbrella functions in part as a DNS super proxy in this regard. The Cisco Umbrella suite of security products apply real-time threat intelligence to managing DNS access and the security of DNS records. DNS access logs are available from Cisco Umbrella for the subscribed enterprise. Instead of using local or ISP DNS servers, an organization can choose to subscribe to Cisco Umbrella for DNS and other security services. An example of a DNS proxy log appears below. The table explains the meaning of the fields in the log entry.

### DNS Proxy Log Example

```
"2015-01-16 17:48:41","ActiveDirectoryUserName",  
"ActiveDirectoryUserName,ADSite,Network",  
"10.10.1.100","24.123.132.133","Allowed","1 (A)",  
"10.10.1.100","24.123.132.133","Allowed","1 (A)",  
"Chat,Photo Sharing,Social Networking,Allow List"
```

Field	Example	Explanation
Timestamp	2015-01-16 17:48:41	This is when this request was made in UTC. This is different than the Umbrella dashboard, which converts the time to your specified time zone.
Policy Identity	ActiveDirectoryUserName	The first identity that matched the request.
Identities	ActiveDirectoryUserName,ADSite,Network	All identities associated with this request.
Internal Ip	10.10.1.100	The internal IP address that made the request.
External Ip	24.123.132.133	The external IP address that made the request.
Action	Allowed	Whether the request was allowed or blocked.
QueryType	1 (A)	The type of DNS request that was made.
ResponseCode	NOERROR	The DNS return code for this request.
Domain	domain-visited.com.	This is the domain that was requested.
Categories	Chat,Photo Sharing,Social Networking	The security or content categories that the destination matches.



## Next-Generation Firewalls

Next-Generation or NextGen Firewall devices extend network security beyond IP addresses and Layer 4 port numbers to the application layer and beyond. NexGen Firewalls are advanced devices that provided much more functionality than previous generations of network security devices. One of those functionalities is reporting dashboards with interactive features that allow quick point-and-click reports on very specific information without the need for SIEM or other event correlators.

Cisco's line of NextGen Firewall devices (NGFW) use Firepower Services to consolidate multiple security layers into a single platform. This helps to contain costs and simplify management. Firepower services include application visibility and control, Firepower Next-Generation IPS (NGIPS), reputation and category-based URL filtering, and Advanced Malware Protection (AMP). Firepower devices allow monitoring network security through a web-enabled GUI called Event Viewer.

Common NGFW events include:

- **Connection Event** – Connection logs contain data about sessions that are detected directly by the NGIPS. Connection events include basic connection properties such as timestamps, source and destination IP addresses, and metadata about why the connection was logged, such as which access control rule logged the event.
- **Intrusion Event** – The system examines the packets that traverse the network for malicious activity that could affect the availability, integrity, and confidentiality of a host and its data. When the system identifies a possible intrusion, it generates an intrusion event, which is a record of the date, time, type of exploit, and contextual information about the source of the attack and its target.
- **Host or Endpoint Event** – When a host appears on the network it can be detected by the system and details of the device hardware, IP addressing, and the last known presence on the network can be logged.
- **Network Discovery Event** – Network discovery events represent changes that have been detected in the monitored network. These changes are logged in response to network discovery policies that specify the kinds of data to be collected, the network segments to be monitored, and the hardware interfaces of the device that should be used for event collection.
- **NetFlow Event** – Network discovery can use a number of mechanisms, one of which is to use exported NetFlow flow records to generate new events for hosts and servers.



## Services Provided by NGFW



## Evaluating alerts

### Security Onion

Security Onion is an open-source suite of Network Security Monitoring (NSM) tools that run on an Ubuntu Linux distribution. Security Onion tools provide three core functions for the cybersecurity analyst: full packet capture and data types, network-based and host-based intrusion detection systems, and alert analyst tools. Security Onion can be installed as a standalone installation or as a sensor and server platform. Some components of Security Onion are owned and maintained by corporations, such as Cisco and Riverbend Technologies, but are made available as open source.

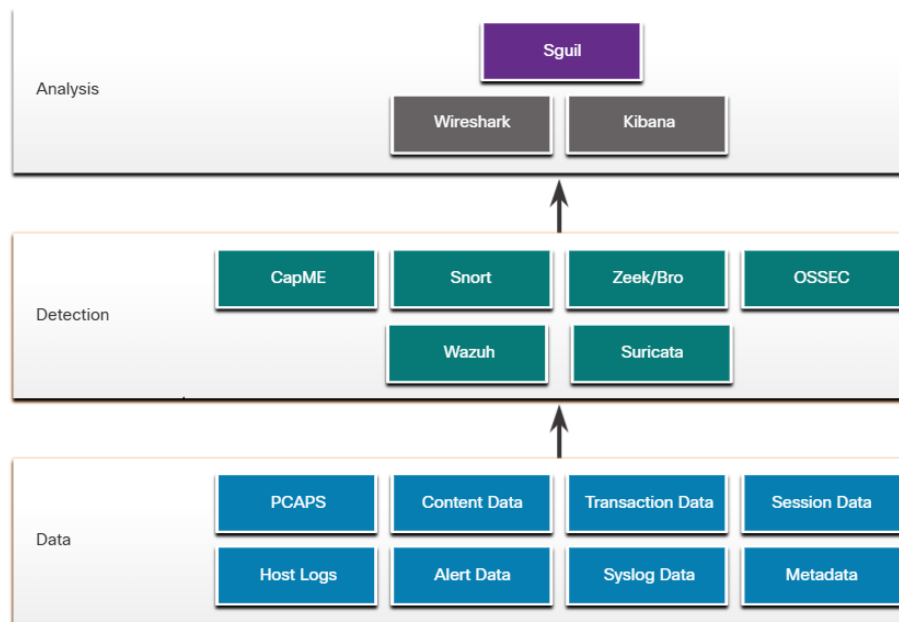
For more information, and to obtain Security Onion, search the internet for the Security Onion website.

**Note:** In some resources, you may see Security Onion abbreviated as SO. In this course, we will use Security Onion.

### Detection Tools for Collecting Alert Data

Security Onion contains many components. It is an integrated environment which is designed to simplify the deployment of a comprehensive NSM solution. The figure illustrates a simplified view of the way in which some of the components of the Security Onion work together.

## A Security Onion Architecture



- **CapME:** This is a web application that allows viewing of pcap transcripts rendered with the tcpflow or Zeek tools. CapME can be accessed from the Enterprise Log Search and Archive (ELSA) tool. CapME provides the cybersecurity analyst with an easy-to-read means of viewing an entire Layer 4 session. CapME acts as a plugin to ELSA and provides access to relevant pcap files that can be opened in Wireshark.
- **Snort:** This is a Network Intrusion Detection System (NIDS). It is an important source of alert data that is indexed in the Sguil analysis tool. Snort uses rules and signatures to generate alerts. Snort can automatically download new rules using the PulledPork component of Security Onion. Snort and PulledPork are open source tools that are sponsored by Cisco.
- **Zeek:** Formerly known as Bro. This is a NIDS that uses more of a behavior-based approach to intrusion detection. Rather than using signatures or rules, Zeek uses policies, in the form of scripts that determine what data to log and when to issue alert notifications. Zeek can also submit file attachments for malware analysis, block access to malicious locations, and shut down a computer that appears to be violating security policies.  
**Note:** Some interfaces within Security Onion have yet to be updated with the Bro to Zeek name change.
- **OSSEC:** This is a host-based intrusion detection system (HIDS) that is integrated into Security Onion. It actively monitors host system operations, including conducting file integrity monitoring, local log monitoring, system process monitoring, and rootkit detection. OSSEC alerts and log data are available to Sguil and Kibana. OSSEC requires an agent to be running on the Windows computers in the enterprise.

- **Wazuh:** Wazuh is a HIDS that will replace OSSEC in Security Onion. It is a full-featured solution that provides a broad spectrum of endpoint protection mechanisms including host logfile analysis, file integrity monitoring, vulnerability detection, configuration assessment, and incident response. Like OSSEC, it requires agents to be running on network hosts.
- **Suricata:** This is a NIDS that uses a signature-based approach. It can also be used for inline intrusion prevention. It is similar to Zeek; however, Suricata uses native multithreading, which allows the distribution of packet stream processing across multiple processor cores. It also includes some additional features such as reputation-based blocking and support for Graphics Processing Unit (GPU) multithreading for performance improvement.

## Analysis Tools

Security Onion integrates these various types of data and Intrusion Detection System (IDS) logs into a single platform through the following tools:

- **Sguil** - This provides a high-level console for investigating security alerts from a wide variety of sources. Sguil serves as a starting point in the investigation of security alerts. A wide variety of data sources are available to the cybersecurity analyst by pivoting directly from Sguil to other tools.
- **Kibana** - Kibana is an interactive dashboard interface to Elasticsearch data. It allows querying of NSM data and provides flexible visualizations of that data. It provides data exploration and machine learning data analysis features. It is possible to pivot from Sguil directly into Kibana to see contextualized displays based on the source and destination IP addresses that are associated with an alert. Search the internet and visit the [elastic.co](http://elastic.co) website to learn more about the many features of Kibana.
- **Wireshark** - This is a packet capture application that is integrated into the Security Onion suite. It can be opened directly from other tools and will display full packet captures relevant to an analysis.
- **Zeek** - This is a network traffic analyzer that serves as a security monitor. Zeek inspects all traffic on a network segment and enables in-depth analysis of that data. Pivoting from Sguil into Zeek provides access to very accurate transaction logs, file content, and customized output.

**Note:** Other Security Onion tools that are not shown in the figure are beyond the scope of this course. A full description of Security Onion and its components can be found at the Security Onion website.

## Alert Generation

Security alerts are notification messages that are generated by NSM tools, systems, and security devices. Alerts can come in many forms depending on the source. For example, syslog provides support for severity ratings which can be used to alert cybersecurity analysts regarding events that require attention.

In Security Onion, Sguil provides a console that integrates alerts from multiple sources into a timestamped queue. A cybersecurity analyst can work through the security queue investigating, classifying, escalating, or retiring alerts. Instead of using a dedicated workflow management system such as Request Tracker for Incident Response (RTIR), a cybersecurity analyst would use the output of an application like Sguil to orchestrate an NSM investigation.

Alerts will generally include five-tuples information when available, as well as timestamps and information identifying which device or system generated the alert. Recall that the five-tuples includes the following information for tracking a conversation between a source and destination application:

- **SrcIP** - the source IP address for the event.
- **SPort** - the source (local) Layer 4 port for the event.
- **DstIP** - the destination IP for the event.
- **DPort** - the destination Layer 4 port for the event.
- **Pr** - the IP protocol number for the event.

Additional information could be whether a permit or deny decision was applied to the traffic, some captured data from the packet payload, or a hash value for a downloaded file, or any of a variety of data.

The figure shows the Sguil application window with the queue of alerts that are waiting to be investigated in the top portion of the interface.

## Sguil Window

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2 2020-07-17 15:55:09 GMT

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion...	7.2088	2020-05-10 23:13:40	209.165.201.17	60572	209.165.200.235	111	6	GPL RPC portmap using TCP 111
RT	3	seconion...	7.2089	2020-05-10 23:16:38	209.165.201.17	60574	209.165.200.235	111	6	GPL RPC portmap NFS request TCP
RT	3	seconion...	7.2090	2020-05-10 23:16:38	209.165.201.17	44811	209.165.200.235	111	17	GPL RPC portmap mountd request UDP
RT	3	seconion...	5.1796	2020-05-10 23:16:38	209.165.201.17	60574	209.165.200.235	111	6	GPL RPC portmap NFS request TCP
RT	3	seconion...	5.1797	2020-05-10 23:16:38	209.165.201.17	44811	209.165.200.235	111	17	GPL RPC portmap mountd request UDP
RT	1	seconion...	5.1814	2020-06-15 18:40:03	209.165.201.17	37517	209.165.200.235	1433	6	ET SCAN Suspicious inbound to MSSQL port 1433
RT	1	seconion...	5.1815	2020-06-15 18:40:03	209.165.201.17	37517	209.165.200.235	5432	6	ET SCAN Suspicious inbound to PostgreSQL port 5432
RT	1	seconion...	5.1816	2020-06-15 18:40:03	209.165.201.17	37517	209.165.200.235	1521	6	ET SCAN Suspicious inbound to Oracle SQL port 1521
RT	1	seconion...	5.1817	2020-06-15 18:40:03	209.165.201.17	37517	209.165.200.235	5810	6	ET SCAN Potential VNC Scan 5800-5820
RT	4	seconion...	3.301	2020-06-15 19:04:14	192.168.0.1		192.168.0.10		1	GPL ICMP_INFO PING *NIX
RT	6	seconion...	7.2138	2020-06-17 15:58:17	209.165.201.17	58016	209.165.200.235	80	6	ET CURRENT_EVENTS QNAP Shellshock CVE-2014-6271
RT	6	seconion...	5.1849	2020-06-17 15:58:17	209.165.201.17	58016	209.165.200.235	80	6	ET CURRENT_EVENTS QNAP Shellshock CVE-2014-6271
RT	1	seconion...	1.2330	2020-06-17 16:42:09	0.0.0.0		0.0.0.0		0	[OSSEC] unix_chkpwd: Password check failed.
RT	1	seconion...	7.4281	2020-06-17 16:45:23	209.165.201.17	58524	209.165.200.235	80	6	ET TROJAN CozyDuke APT HTTP Checkin

IP Resolution Agent Status Snort Statistics System Msgs User Msgs

☐ Reverse DNS ☒ Enable External DNS

Src IP:   
Src Name:   
Dst IP:   
Dst Name:

Whois Query: ☒ None ☐ Src IP ☐ Dst IP

☐ Show Packet Data ☐ Show Rule

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
TCP	Source Port	Dest Port	R	R	U	A	P	R	S	F	
			1	0	G	K	H	T	N	N	
	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum				

DATA

Search Packet Payload ☐ Hex ☒ Text ☐ NoCase

The fields available for the real-time events are as follows:

- **ST** – This is the status of the event. **RT** means real time. The event is color-coded by priority. The priorities are based on the category of the alert. There are four priority levels: very low, low, medium, and high. The colors range from light yellow to red as the priority increases.
- **CNT** – This is the count for the number of times this event has been detected for the same source and destination IP address. The system has determined that this set of events is correlated. Rather than reporting each in a potentially long series of correlated events in this window, the event is listed once with the number of times it has been detected in this column. High numbers here can represent a security problem or the need for tuning of the event signatures to limit the number of potentially spurious events that are being reported.

- **Sensor** – This is the agent reporting the event. The available sensors and their identifying numbers can be found in the Agent Status tab of the pane which appears below the events window on the left. These numbers are also used in the Alert ID column. From the Agent Status pane, we can see that OSSEC, pcap, and Snort sensors are reporting to Sguil. In addition, we can see the default hostnames for these sensors, which includes the monitoring interface. Note that each monitoring interface has both pcap and Snort data associated with it.
- **Alert ID** – This two-part number represents the sensor that has reported the problem and the event number for that sensor. We can see from the figure that the largest number of events that are displayed are from the OSSEC sensor (1). The OSSEC sensor has reported eight sets of correlated events. Of these events, 232 have been reported with event ID 1.24.
- **Date/Time** – This is the timestamp for the event. In the case of correlated events, it is the timestamp for the first event.
- **Event Message** – This is the identifying text for the event. This is configured in the rule that triggered the alert. The associated rule can be viewed in the right-hand pane, just above the packet data. To display the rule, the **Show Rule** checkbox must be selected.

Depending on the security technology, alerts can be generated based on rules, signatures, anomalies, or behaviors. No matter how they are generated, the conditions that trigger an alert must be predefined in some manner.

## Rules and Alerts

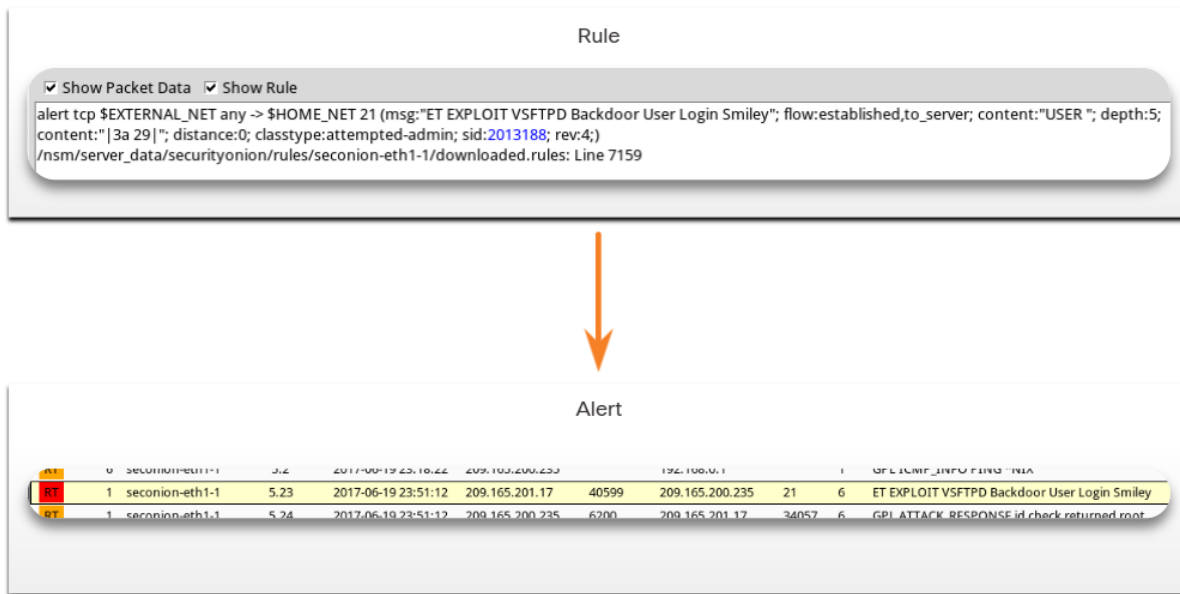
Alerts can come from a number of sources:

- **NIDS** - Snort, Zeek, and Suricata
- **HIDS** - OSSEC, Wazuh
- **Asset management and monitoring** - Passive Asset Detection System (PADS)
- **HTTP, DNS, and TCP transactions** - Recorded by Zeek and pcaps
- **Syslog messages** - Multiple sources

The information found in the alerts that are displayed in Sguil will differ in message format because they come from different sources.

The Sguil alert in the figure was triggered by a rule that was configured in Snort. It is important for the cybersecurity analyst to be able to interpret what triggered the alert so that the alert can be investigated. For this reason, the cybersecurity analyst should understand the components of Snort rules, which are a major source of alerts in Security Onion.

## Sguil Alert and the Associated Rule



## Snort Rule Structure

Snort rules consist of two sections, as shown in the figure: the rule header and the rule options. The rule header contains the action, protocol, source and destination IP addresses and netmasks, and the source and destination port information. The rule options section contains alert messages and information on which parts of the packet should be inspected to determine if the rule action should be taken. Rule Location is sometimes added by Sguil. Rule Location is the path to the file that contains the rule and the line number at which the rule appears so that it can be found and modified, or eliminated, if required.

## Snort Rule Structure and Sguil-supplied Information

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498;
rev:8;)
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692
```

Component	Example (shortened...)	Explanation
rule header	alert ip any any -> any any	Contains the action to be taken, source and destination addresses and port, and the direction of traffic flow
rule options	(msg:"GPL ATTACK_RESPONSE ID CHECK RETURNED ROOT";...)	Includes the message to be displayed, details of packet content, alert type, source ID, and additional details, such as a reference for the rule or vulnerability
rule location	/nsm/server_data/securityonion/rules/...	Added by Sguil to indicate the location of the rule in the Security Onion file structure and in the specified rule file

## The Rule Header

The rule header contains the action, protocol, addressing, and port information, as shown in the figure. In addition, the direction of flow that triggered the alert is indicated. The structure of the header portion is consistent between Snort alert rules.

Snort can be configured to use variables to represent internal and external IP addresses. These variables, \$HOME\_NET and \$EXTERNAL\_NET, appear in the Snort rules. They simplify the creation of rules by eliminating the need to specify specific addresses and masks for every rule. The values for these variables are configured in the snort.conf file. Snort also allows individual IP addresses, blocks of addresses, or lists of either to be specified in rules. Ranges of ports can be specified by separating the upper and lower values of the range with a colon. Other operators are also available.

## Snort Rule Header Structure

```

alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498;
rev:8;)
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692

```

Component	Explanation
alert	the action to be taken is to issue an alert, other actions are log and pass
ip	the protocol
any any	the specified source is any IP address and any Layer 4 port
->	the direction of flow is from the source to the destination
any any	the specified destination is any IP address and any Layer 4 port



## The Rule Options

The structure of the options section of the rule is variable. It is the portion of the rule that is enclosed in parenthesis, as shown in the figure. It contains the text message that identifies the alert. It also contains metadata about the alert, such as a URL that provides reference information for the alert. Other information can be included, such as the type of rule and a unique numeric identifier for the rule and the rule revision. In addition, features of the packet payload may be specified in the options. The Snort users manual, which can be found on the internet, provides details about rules and how to create them.

Snort rule messages may include the source of the rule. Three common sources for Snort rules are:

- **GPL** - Older Snort rules that were created by Sourcefire and distributed under a GPLv2. The GPL ruleset is not Cisco Talos certified. It includes Snort SIDs 3464 and below. The GPL ruleset is can be downloaded from the Snort website, and it is included in Security Onion.
- **ET** - Snort rules from Emerging Threats. Emerging Threats is a collection point for Snort rules from multiple sources. ET rules are open source under a BSD license. The ET ruleset contains rules from multiple categories. A set of ET rules is included with Security Onion. Emerging Threats is a division of Proofpoint, Inc.
- **VRT** - These rules are immediately available to subscribers and are released to registered users 30 days after they were created, with some limitations. They are now created and maintained by Cisco Talos.

Rules can be downloaded automatically from Snort.org using the PulledPork rule management utility that is included with Security Onion.

Alerts that are not generated by Snort rules are identified by the OSSEC or PADS tags, among others. In addition, custom local rules can be created.

## Snort Rules Options Structure

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";  
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498;  
rev:8;)  
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692
```

Component	Explanation
msg:	Text that describes the alert.
content:	Refers to content of the packet. In this case, an alert will be sent if the literal text “uid=0(root)” appears anywhere in the packet data. Values specifying the location of the text in the data payload can be provided.
reference:	This is not shown in the figure. It is often a link to a URL that provides more information on the rule. In this case, the sid is hyperlinked to the source of the rule on the Internet.
classtype:	A category for the attack. Snort includes a set of default categories that have one of four priority values.
sid:	A unique numeric identifier for the rule.
rev:	The revision of the rule that is represented by the sid.

## The Need for Alert Evaluation

The threat landscape is constantly changing as new vulnerabilities are discovered and new threats evolve. As user and organizational needs change, so also does the attack surface. Threat actors have learned how to quickly vary features of their exploits in order to evade detection.

It is impossible to design measures to prevent all exploits. Exploits will inevitably evade protection measures, no matter how sophisticated they may be. Sometimes, the best that can be done is to detect exploits during or after they have occurred. Detection rules should be overly conservative. In other words, it is better to have alerts that are sometimes generated by innocent traffic, than it is to have rules that miss malicious traffic. For this reason, it is necessary to have skilled cybersecurity analysts investigate alerts to determine if an exploit has actually occurred.

Tier 1 cybersecurity analysts will typically work through queues of alerts in a tool like Sguil, pivoting to tools like Zeek, Wireshark, and Kibana to verify that an alert represents an actual exploit.

## Primary Tools for the Tier 1 Cybersecurity Analyst

