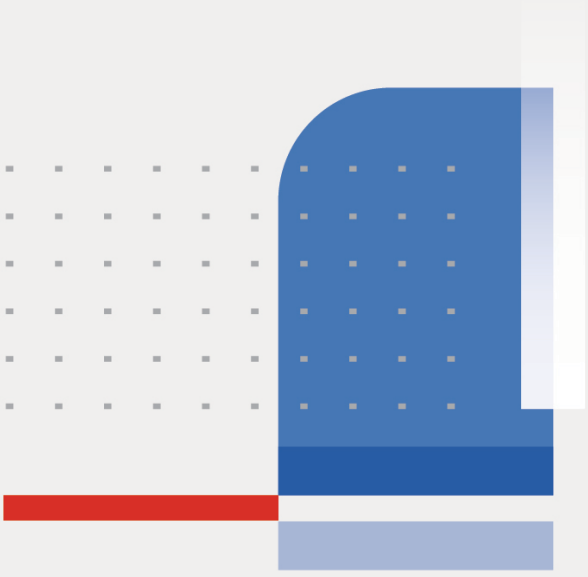

# Getting Started With Cybersecurity

## Lesson Scripts

1.0



FORTINET®
Training Institute

**Fortinet Training Institute - Library**

https://training.fortinet.com

**Fortinet Product Documentation**

https://docs.fortinet.com

**Fortinet Knowledge Base**

https://kb.fortinet.com

**Fortinet Fuse User Community**

https://fusecommunity.fortinet.com/home

**Fortinet Forums**

https://forum.fortinet.com

**Fortinet Product Support**

https://support.fortinet.com

**FortiGuard Labs**

https://www.fortiguard.com

**Fortinet Training Program Information**

https://www.fortinet.com/nse-training

**Fortinet | Pearson VUE**

https://home.pearsonvue.com/fortinet

**Fortinet Training Institute Helpdesk (training questions, comments, feedback)**

https://helpdesk.training.fortinet.com/support/home

# TABLE OF CONTENTS

# Firewall

Welcome to the *Firewall* lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Define firewalls and their evolution.
- Describe how firewalls work.
- Explain the latest firewall status.

As networks began to grow, interconnect with one another, and eventually connect to the internet, it became important to control the flow of network traffic. Firewalls became a means of control that had to evolve and change alongside networks. They are classified into generations defined as first-generation packet filter firewall, also know as stateless firewall, second-generation stateful firewall, third-generation firewall, and next-generation firewall (NGFW).

The first generation of firewall is a packet filter firewall, also known as a stateless firewall. It examines the routing and transport layer protocols information such as source and destination network addresses, protocols, and port numbers. Firewall policies use these attributes to define which packets are allowed through. The rules are ordered in a list and the potential match is performed in order from top to bottom. The last firewall policy can be implicit, denying the packet by default, or explicit, performing the corresponding configured action or either allowing or denying the packet.

A stateless firewall allows a packet to pass if the network addresses, protocol, and port number match those of its firewall policy. If it does not, the packet is either silently dropped or blocked.

Click the buttons for more information.

A drawback of a stateless firewall is that it requires additional configuration to offer a suitable level of protection. For example, it requires an additional firewall policy for return traffic in a session. It also fails to appropriately manage protocols. Stateless firewalls open random ports and use multiple connections, like FTP, with its control and data connections.

Stateless firewalls use a “one-size-fits-all” approach to decide whether to allow traffic to pass. Because of this open approach, bad actors can potentially bypass firewall rules and inject rogue packets through acceptable protocols and ports, or exploit bugs in a computer networking software.

The second generation of firewall, known as a stateful firewall, offsets the limitations of the stateless firewall by developing additional criteria for blocking or allowing traffic.

A stateful firewall is designed to observe the network connections over time by tracking the 5-tuple check and the connection state in its session table. It watches as new network connections are made, and continuously examines the traffic going back and forth between the endpoints. If a connection behaves improperly or if the return traffic does not match the corresponding incoming traffic, the firewall blocks that connection. Any packet that does not belong to a known conversation or does not match an allowed firewall policy is dropped.

Click the button for more information.

While stateful firewalls are an improvement, they still cannot block rogue packets if they are using an acceptable protocol, such as HTTP. The explosion of the World Wide Web promoted HTTP as one of the most frequently used network protocols. The problem is that HTTP is used in many ways, such as in static text content, e- commerce, file hosting, and many other types of web applications. Because they all use the same port number, the firewall is not able to distinguish between them.

Network administrators need to distinguish between approved and malicious applications to determine which ones to pass or block. Firewalls must look deeper into the data payloads to determine how protocols such as HTTP are used.

The third generation of firewall looks deeper into the data payloads. While still stateful, these firewalls understand the application layer protocols and control different uses of the same basic protocol. This is known as application layer filtering. Firewalls that implement application layer filtering can understand protocols such as HTTP, FTP, and DNS.

HTTP can distinguish between browser traffic, a blog, a file sharing site, e-commerce, social media, voice-over-IP and email. UTM firewalls also combine additional protections like antivirus, antispam, an intrusion prevention system (IPS), and a virtual private network (VPN).

Click the underlined terms for more information.

Today, the prevalence of the internet has changed the way of working, playing, entertaining, and doing commerce. Businesses have evolved to take advantage of cheaper, multi-cloud services, and the convenience of mobile and IoT devices has dramatically expanded network edges, thereby increasing the attack surface.

Just as the internet has evolved, so have threat actors. They continue to change in terms of attack methods and level of sophistication. Attacks can now come from trusted users, devices, and applications that spread malware, both unknowingly and with malicious intent.

A firewall must prevent evolving cyberattacks at every edge of the network while delivering security, reliability, and network performance. Next-generation firewalls, like FortiGate, provide these advanced security capabilities.

A next-generation firewall operates like airport security, with both having multiple security checkpoints. Just as a security agent looks at your boarding pass as a first line of defense, a next-generation firewall looks at packets and makes rule-based decisions whether to allow or drop the traffic.

Next, your travel bags are checked by security to see if you are carrying any banned or malicious items. This is similar to the way a next-generation firewall performs deep packet inspection (DPI).

Click the underlined term for more information.

If suspicious items are found in your travel bag, an airport security agent sets the bag aside for enhanced screening. In a similar vein, the next-generation firewall sends malicious content to a sandbox for further analysis.

Click the underlined term for more information.

As networks continue to evolve and introduce new challenges, next-generation firewalls also continue to evolve. For example, next-generation firewalls can control applications, either by classification or by who the user is. Application-level security helps protect web-browsing clients from attacks and threats.

Next-generation firewalls also adopted various segmentation approaches that segregate users, devices, and applications that are aligned to business needs. By segmenting networks rather than using a flat network, the firewall helps eliminate a single point of entry, which used to make it easier for cybercriminals to enter and spread threats across the network. Within these challenges, firewalls are evolving from reactive to proactive devices, using artificial intelligence to enforce security policies.

Next-generation firewalls also deliver high-performance inspection and greater network visibility, with little to no degradation, to support and protect modern, distributed data centers located within a complex and hybrid IT infrastructure. Hybrid data centers offer businesses greater agility, flexibility, and scale on demand, as well as an expanded attack surface that requires an equally evolved security strategy. High-performance inspection includes applications, compute resources, analytics, encrypted data that moves throughout the infrastructure, and data storage across multiple private and public clouds.

You have completed the lesson.

# Network Access Control

Welcome to the *Network Access Control* lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Explain how network access control (NAC) works to protect networks.
- Describe the evolution of NAC, including the introduction of BYOD and IoT devices.
- Identify additional NAC capabilities.
- List the benefits of using NAC.

Network Access Control (NAC) is an appliance or virtual machine that controls access to a network. It has complete visibility into the network profiles and categorizes devices automatically. It evaluates and classifies security-policy compliance by user, device, location, operating system, and other criteria that may detect unusual activity. Many NAC solutions have centralized architecture that improves the control of devices across large and multi-site networks.

NAC began as a network authentication and authorization method for devices joining the network, which follows the IEEE 802.1X standards. The authentication method involved three parties: the client device, the authenticator, and the authentication server. The authenticator could be a network switch or wireless access point that demarks the protected network from the unprotected network. The client provides credentials in the form of a username and password, digital certificate, or some other means, to the authenticator, which forwards these credentials to the server. Depending on the outcome of authentication, the authenticator will either block the device or allow it access to the network.

Another method to control access to a network, especially a publicly available network, is a Captive portal. An example of this is when you connect to a network in a coffee shop. Before gaining access to the network, you may have to interact with a web page that asks you to agree to legal terms before granting access.

As endpoints proliferated across organizations, greater controls were needed. Guest access, Bring Your Own Devices (BYODs) and the Internet of Things (IoTs) have introduced complex problems for network security. The first is that the devices trying to connect to the network are personally owned devices, not assets of an organization. The company's MIS department does not control what runs on these devices, for example, antivirus software or unsafe applications.

A second challenge is that IoT devices are hardware with sensors that transmit data from one place to another over the internet, dramatically expanding the attack surface. Organizations buy IoT-enabled devices from other vendors, and these devices connect back to vendor networks to provide information about product use and maintenance needs.

Organizations tolerate this situation because IoT devices save them time and money. For example, if a printer is low on toner, the vendor could notify the network administrator by email, or even deliver new toner cartridges automatically.

Organizations tolerate using IoT devices because it saves them time and money.

The evident convenience of these devices has made them wildly popular and numerous. However, the variety of devices, the lack of standards, and the inability to secure these devices make them a potential conduit for contagion to enter the network.

Many IoT devices lack the CPU cycles or memory to host authentication and security software. They identify themselves using a shared secret or unique serial number, which is inserted during manufacturing. But this authentication scheme is very limited - should the secret become known, there is likely no way to reset it. Without the ability to install security software, there is little visibility into those devices. Fortunately, NAC evolved to solve these weaknesses.

When MIS introduces NAC into a network, the first thing NAC does is create profiles of all connected devices. NAC then permits access to network resources based on the device profile, which is defined by function. If a device does not have a defined profile or a profile that matches a particular function, they are denied entry. This is like granting individuals access to sensitive information and applications based on their need to know.

For example, NAC can permit an IP camera connection to a network video recorder (NVR) server but would prevent it from connecting to a finance server. Based on its profile, an IP camera has no business communicating with a finance server. NAC will direct the IP camera to its appropriate VLAN and the firewall would do the rest. When access is granted this way, the network becomes segmented by device function. If a device is compromised, malware can infect only those objects that the device is permitted to connect to. So, the compromised IP camera from the earlier example could infect the NVR server, but not the finance server.

This is also applicable for any contractors, partners, and guests who many need to enter an organization’s network. In this case, these users are segmented by profile and can gain secure access to the network while being locked out of restricted areas.

To ensure that the network remains secure, user and device policies are adjusted as people, endpoints, and businesses change.

With the prevalence of Wi-Fi hotspots in public locations and company offices, there is a need for temporary guest access to these networks. NAC enables an organization to manage and authenticate temporary users and devices through a self-service portal. An example temporary guest access is someone accessing a free wi-fi network at an airport.

NAC can be integrated into the security framework, so that when a breach is detected, NAC automatically responds to notify the security operations center (SOC) and coordinates with other security devices to neutralize the threat. It can also generate reports and insights in attempted access across the organization.

NAC integrates with other security point products such as switches and network solutions through the open/RESTful application programming interface (API) or secure shell (SSH).

Network access control is important and helps an organization through the following:

- **Improved Security** - NAC provides oversight of all devices in use across the organization, which means it enhances security while authenticating users and devices the moment they enter the network.

- **Cost Savings** - The automated tracking and protection of devices at scale translates into cost savings for organizations because fewer IT resources are needed.

- **Automation** - As the number and variety of devices organizations use continue to increase, organizations cannot manually verify users and their endpoints' security policies as they attempt to enter the network. The automation features of NAC offer tremendous efficiency to the process of authenticating users and devices and authorizing access.

- **Enhanced IT Experiences** - Seamless access provides a user experience that is frictionless when connecting to the network.

- **Ease of Control** - The visibility features of NAC effectively serve as a 24/7 inventory of all the endpoints authorized by the organization. This is helpful not only when IT needs to determine which endpoints or users have been granted access to the network but also for life-cycle management, when devices must be phased out or replaced.

Click the icons to learn more.

Fortinet offers a network access control solution, named FortiNAC™. It contains all the features identified in this lesson, as well as additional features. FortiNAC easily intigrates with the Fortinet security fabric and can automatically isolate clients if they are not adhering to the set policies.

You have completed the lesson. You are able to:

- Explain how network access control (NAC) works to protect networks.
- Describe the evolution of NAC, including the introduction of BYOD and IoT devices.
- Identify additional NAC capabilities.
- List the benefits NAC has for an organization.

# Sandbox

Welcome to the *Sandbox* lesson. Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Describe a sandbox.
- Understand why sandboxing technology was created.
- Understand how sandboxing technology has evolved.

A sandbox, in the context of computer security, is a system that confines the actions of an application, such as opening a Word document or a browser, within a safe virtual environment. In a sandbox, an application is isolated so that any malicious intent can be uncovered safely, without causing harm to the network. If something unexpected or dangerous happens, it affects only the sandbox, and not the other computers and devices on the network. Sandbox technology is typically managed by an organization's information security team, but is used by network, applications, and desktop operations teams to bolster security in their respective domains.

Threat actors exploit vulnerabilities in legitimate applications in order to compromise a device and from there move through the network to infect other devices. Firewalls and antivirus software can stop known threats, but they are helpless against zero-day attacks. A zero-day attack is when a threat actor exploits an unknown vulnerability. Sandboxing was created as a defense again zero-day attacks.

A sandbox offers an isolated virtual space that mimics computer systems and applications. It allows potential threats to run safely within these virtual systems and analyzes these threats. If a sandbox deems that a file is safe, it does not take any action; but if it detects malicious behavior, it quarantines the file and prevents it from accessing other computers and devices on the network.

The evolution of Sandboxing solutions can be broadly categorized into three generations, starting from their rudimentary beginnings and progressing to advanced and sophisticated solutions available today. **Click on each tile to learn more.**

**First Generation Sandboxing Solutions**

Early sandboxes encountered challenges when trying to share threat intelligence with other security devices due to security architecture dependence on standalone solutions. Standalone solutions could not easily integrate with products from other vendors, forcing the security operations center (SOC) to use a separate management console for each one. Consequently, the process of consolidating and analyzing threat intelligence data was both challenging and time-consuming.

**Second Generation Sandboxing Solutions**

Second-generation sandboxes were better at integrating with other security devices, allowing for improved intelligence sharing. This new approach to network security allowed analysts to correlate threat intelligence centrally and respond to threats from a single pane of glass. Moreover, an integrated network security environment could share information with a threat intelligence service in the cloud, which could then push that intelligence to other networks.

**Third Generation Sandboxing Solutions**

Threat actors are leveraging automation and artificial intelligence (AI) methods to accelerate the development of new security exploits. AI-driven attacks necessitated a third-generation sandbox based on a threat analysis standard.  The third generation of sandbox devices not only help detect breaches in a timely manner they also prevent them from happening. These solutions utilize the universal MITRE ATT&CK security language for categorizing threat models and methodologies.

FortiSandbox™, a Fortinet sandbox product, embodies all the latest features of a sandboxing solution. FortiSandbox is a high-performance security solution that utilizes AI and machine learning (ML) technology to identify and isolate advanced threats in real time. It integrates with other security products in a collective defense called the Fortinet Security Fabric to inspect files, websites, URLs and network traffic for malicious activity, including zero-day threats. It also uses sandboxing technology to analyze suspicious files in a secure virtual environment.

You have completed this lesson. You are now able to:

- Describe a sandbox.
- Understand why sandboxing technology was created.
- Understand how sandboxing technology has evolved.

Thank you for your time, and please remember to take the quiz that follows this lesson.

# Web Application Firewall

Welcome to the Web Application Firewall (WAF) lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Explain how web application firewalls (WAF) are different from traditional edge firewalls.
- Describe the evolution of WAFs and WAF applications.

A web application firewall (WAF) is an appliance or software that monitors HTTP/HTTPS traffic and can block malicious traffic to and from a web application. WAFs target content from specific web applications at the application level, while edge firewalls form secure gateways between the local area network (LAN) and outside servers at the network level. By inspecting HTTP traffic, a WAF can stop attacks that target web application security flaws, such as SQL injection, cross-site scripting (XSS), file inclusion, and security misconfigurations. Because so much time, both at work and at home, is spent interfacing with web applications and web servers, the WAF is a vital component of the arsenal used against bad actors and their malicious online schemes.

The ancestor of the WAF is the application firewall that was developed in the 1990s. Although largely a network-based firewall, it could target some applications or protocols, such as file transfer protocol (FTP) and remote shell (RSH), which is a command line computer program. The debut of the World Wide Web, in 1991, was the “big bang” of the internet universe, which has been expanding at an accelerated pace ever since. The accessibility and openness of the internet permitted anyone to search and explore, but it also permitted bad actors to use it for their own sordid purposes.

As more people and organizations became victims of espionage, theft, and other crimes, developing a defense against HTTP-based cyberattacks became a top priority. Because all web applications used HTTP and either port 80 or port 443, WAF could not rely on traditional edge firewall methods, which based decisions on a blocklist of network addresses and blocked specific protocols and port numbers.

Take a moment to consider this scenario, which provides an example of an attack that uses SQL injection, a common attack method.

Imagine you run an online business. Customers and partners log in to your site to buy products and services. To access your site, they must use a typical login page that asks them to enter their user ID and password. A user, John Smith, types his user ID-jsmith-and his password into the login page. This information is verified in a back-end database. If the password is true, John Smith is allowed to access your site; but if the password is false, he is not allowed access.

A bad actor, pretending to be John Smith, is attempting to access your site, but he does not know John’s password. The bad actor could try guessing John Smith’s password, but that would be time consuming. Instead, when asked to enter a password, the bad actor types, abc123 or 2+2=4. When these credentials are sent to the database for verification, it is likely that the password abc123 will be identified as false; however, the expression, 2+2=4, which is a valid SQL statement, will be identified as true, and the bad actor will be given access.

By using SQL injection attacks to exploit this flaw, bad actors were able to break in to some sites. To combat this, the first generation of WAFs used blocklists and signature-based HTTP attributes to alert the firewall of an attack, so SQL injection attacks, like the one described in this example, were no longer successful.

The soaring popularity of the internet soon led to an increase in the number and complexity of web applications, which made the signature-based approach to WAFs, obsolete. As well, the number of false positives-alerts of attacks that were, in fact, legitimate connections-grew to proportions that were beyond the capacity of IT security teams. The next generation of WAFs were more intelligent-the firewalls included an element of learning. WAFs would study application behavior and use what they learned to create a baseline. Then, they would use that baseline to evaluate attempts to access applications and determine if those attempts were normal or irregular, and therefore, suspect. The next generation also introduced session monitoring and heuristics, which enabled the firewall to detect variants of known signatures. This was a step forward; however, the IT security teams that were overseeing application learning and defense efforts could not keep up with the rapid mutations of existing methods or increasing number of new exploits. Moreover, there was no defense against zero-day attacks, which exploit an unknown weakness in the code of an application.

The next logical evolution in WAF development was machine learning (ML). Unencumbered by human supervision, behavior analysis could now be done at machine speed and could adapt to the ever-changing attributes of a threat. Other security features that were added to firewalls include the following:

- Distributed denial of service (DDoS) defense
- IP reputation
- Antivirus
- Data loss prevention (DLP)

WAFs could monitor HTTP traffic and stop any action that violated acceptable behavior. They could Identify a user, correlate the user's attempted actions with their permissions, and stop any action that went beyond the scope of their role. WAFs could also share information and collaborate with other security devices in the network, such as other firewalls and sandboxes. This ability allowed WAFs to be part of a collective defense, rather than working independently. Sandboxing capabilities meant that suspicious material could be tested safely, in isolation from the network. Zero-day attacks could be exposed and quarantined in these sandbox environments, and their signatures could be shared with other devices in the network. In addition, any resulting discoveries could be uploaded to a threat intelligence center on the internet, where they could be communicated to other networks.

FortiWeb, Fortinet's version of a WAF, defends both web applications and application programming interfaces (APIs) against all OWASP Top-10 threats, DDOS attacks, bot attacks, and more. FortiWeb uses advanced, ML-powered features to provide real-time protection against known and unknown threats. FortiWeb can integrate with FortiGate and FortiSandbox.

You have completed this lesson. You are now able to:

- Explain how web application firewalls (WAF) are different from traditional edge firewalls.
- Describe the evolution of WAFs and WAF applications.

# Secure Email Gateway

Welcome to the *Secure Email Gateway* lesson.

Click N**ext** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Define a secure email gateway.
- Explain the features of a secure email gateway.
- List the mechanisms that help identify legitimate senders and reduce spoofing.
- Define terms related to a secure email gateway, such as spam and phishing.

Email offers a fast and inexpensive way to communicate. It also affords anonymity. While persons or organizations could broadcast messages or advertising to a vast audience at basically no cost, email also equips bad actors with the means to spread misinformation, promote fraud, steal personal information, and distribute malware. The act of sending unsolicited and irrelevant email to many recipients is called spam. As you have seen, spam that entices recipients to click on a link or download a file is called phishing, so named by America Online in 1996.

The phishing technique relies on human naivety, carelessness, or distraction for it to work. Educating employees or the public about phishing has not ended these attacks. In 2004, 176 phishing attacks were recorded but by 2012 this number had grown to 28,000. And they continue to grow. One source estimated that there were 500 million phishing attacks in 2022. Phishing attacks continue to grow because they are profitable. They remain the leading cause of data breaches, costing as average of $4.35 million per breach.

Secure email gateway (SEG) arose in response to the rising phishing threat and email security in general. SEG is a technology solution designed to protect organizations from email-based threats and ensure the security and privacy of their email communications. It serves as a barrier between an organization's email infrastructure and the external email network, in other words the internet.

The first two features of SEG are content filtering and data loss prevention (DLP). Content filters are used to control and manage the types of content that can be accessed or shared on a network. They are often used in web filtering, email filtering, and data loss prevention (DLP) to enforce content-related policies. DLP strives to prevent the unauthorized or accidental leakage of sensitive and confidential information from an organization. Content filters target a broader range of content, including not only spam but also other types of content such as inappropriate or sensitive data. Technologies used for content filtering can vary widely and may include keyword matching, regular expressions, deep packet inspection, and context-aware analysis.

Like content filters, spam filters aim to manage email and eliminate harmful content, but they serve different purposes and target different types of content. Spam filters aim to reduce the amount of spam that reaches a user’s inbox. They focus on identifying emails based on characteristics commonly associated with spam, such as suspicious sender addresses, excessive use of certain keywords, known spam patterns, and IP addresses with poor reputations. Spam filters are highly automated and use algorithms and heuristics to make decisions about whether an email is spam. They often maintain databases of known spammers and patterns to enhance their accuracy. Common technologies used for spam filtering include Bayesian filters, deny lists, allow lists, and machine learning algorithms.

Click the indicated buttons for more information.

SEG offers authentication and identity verification. It supports various methods to authenticate senders' identities and validate email sources to prevent email spoofing and impersonation. Malware filtering is another feature of SEG. This type of filter scans email attachments and links for malware, preventing potentially harmful content from reaching the recipient's inbox. And SEG can encrypt email to protect the content from unauthorized access during transmission. Some systems can digitally sign emails, which aids in identifying the sender and verifying the integrity of the content.

Click the indicated markers to review the terms and to learn more.

Also working at the level of the receiving email server is the Sender Policy Framework (SPF). When an email is sent, the recipient's email server checks the SPF record of the sender's domain to verify whether the sending server's IP address is authorized to send emails on behalf of that domain. If the sending server's IP address is not listed in the SPF record, the recipient's server may flag the email as suspicious, reject it, or take other actions based on the recipient's email server's configuration. This process helps prevent email spoofing and sender address forgery by verifying the authenticity of the sending server.

SPF works alongside other email authentication technologies like DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting, and Conformance (DMARC) to provide comprehensive email security. While SPF is an effective tool in the fight against email spoofing and fraud, it has limitations, and it should be used in conjunction with other email authentication methods like DKIM and DMARC for a more robust email security strategy.

Click the underlined terms for more information.

You have completed the lesson. You can now achieve these objectives:

- Define a secure email gateway.
- Explain the features of a secure email gateway.
- List the mechanisms that help identify legitimate senders and reduce spoofing.
- Define terms related to a secure email gateway, such as spam and phishing.

# Content Filters

Welcome to the Content Filters lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Define content filtering.
- Describe how content filters work.
- Explain the benefits of content filters.

Content filtering is a process to screen or restrict access to objectionable emails, webpages, executables and other suspicious items. It is a common security measure that is often built into internet firewalls and blocks content that contains harmful, illegal, or inappropriate information. For example, parents often use web filtering to protect their children from improper or graphic material.

Content filters are used in different ways to block access to different types of materials. The common types of content filters include search engine filters, email filters, DNS-base content filters, and web filters. Click the different tabs to learn more about each type.

Search engine filters rate web content according to its text and images. Text and images hold a specific weight, which is measured against a classification set. The weights vary based on whether the classification level is set to off, moderate, or strict. Machine learning helps define the weights to avoid possible false positives. Depending on the resulting value and the size of the document, the content can then be classified as safe, moderate, inappropriate, or rejected from a strict point of view. The search engine result will then display contents if they meet the level of classification set.

Email content filters check the header of incoming mails against real-time blackhole lists. The raw data of the body is scanned for inappropriate content, providing a spam confidence level that is similar to search engine weights. Email content filters also check attachments, identify keywords or potential unauthorized types of files, like executables, and complete the email content filtering. This enables users to block, quarantine, or reject malicious emails, including phishing, while accepting appropriate incoming emails.

Click the icons for more information.

DNS-based content filters check the website during the resolution of the domain through DNS servers using blocklists. If the website is not allowed, the browser is redirected to a replacement message announcing that the page is blocked. Alternatively, a company can define an allowlist, including all company approved websites. DNS-based content filtering would then block all other websites.

Web filters are similar to DNS-based content filters with an additional function that categorizes websites. For example, a requirement for schools in the United States is to adhere to the Children’s Internet Protection Act (CIPA), a bill that addresses concerns about children’s access to obscene or harmful content over the internet, such as pornography. Therefore, elementary and high schools use web filters to block material deemed harmful to minors. All websites and their contents are rated through machine learning, so that the access to a specific URL is allowed or blocked according to its category and the user’s profile.

Content filters allow organizations to block access to sites known to carry malware, protecting their data and users from malicious activity.

Content filters also can identify phishing or an exploit kit, blocking the access before it triggers a malicious download. This is important while cyber criminals increasingly develop new, more sophisticated ways to illegally access network and steal data.

Limiting user's access to only specific work-related internet can increase the bandwidth efficiency and enable faster connections for all employees.

Organizations can use web filtering on web sites like social media and online shopping to increase staff productivity.

Click the underlined terms for more information.

You have completed the lesson.

# Secure Wi-Fi

Welcome to the *Secure Wi-Fi lesson*.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

• List common secure wireless protocols and standards.

• Explain the measures you can take to make your wireless network safer.

Wi-Fi, based on the IEEE 802.11 standards, is a wireless technology employed for the local area networking of devices. Its development drew from similar protocols and technology as Ethernet, encompassing IP at the network layer and TCP and UDP at the transport layer. Common technologies include routers, switches, the domain name system (DNS), and, in most cases, wireless networks connect to wired networks. For instance, your home wireless network allows your devices to communicate without physical wired connections, but for external communication beyond your home network, your home router becomes the gateway. This router is physically linked to the wide area network (WAN) through wired connections, such as digital subscriber line (DSL), cable internet, or other technologies.

Click the underlined term for more information.

There is one very large difference between wireless and wired networks, however. Data is not piped through twisted copper wire or fiber optic cable as in most wired networks; rather, data is sent through radio waves or microwaves. This different transmission medium has advantages and disadvantages. The principal advantage of wireless networks is mobility: you can walk around with a device anywhere within Wi-Fi range and not be tethered to a cable. Of course, some mobile devices, such as mobile phones, also use cellular technology, which extends their range. The main *disadvantage* of wireless networks is security. Without following proper security protocols, bad actors can listen in to communication.

Wi-Fi stakeholders introduced an encryption protocol known as wired equivalent privacy (WEP), which was succeeded by Wi-Fi protected access (WPA) versions one and two. WPA2 employs the advanced encryption standard (AES) for encrypting outgoing data, a standard established by the National Institute of Standards and Technology (NIST) in the United States. Furthermore, the technology saw the addition of new, enterprise-grade authentication methods, resulting in two security options for each style. At the home security level, network authentication and key exchange continued to rely on a shared passphrase. On the enterprise security front, the use of 802.1x authentication mechanisms, like those employed in wired networks, was introduced to authenticate users, and establish encryption. Nevertheless, the security of networks, particularly at the home network, remained at risk if poorly chosen or weak passphrases were used.

Released in 2018, Wi-Fi protected access 3 (WPA3) introduced a new, more secure handshake for making connections, an easier method for adding devices to the network, increased key sizes, and other security features. While security technology continued to improve, the bad actors turned their efforts to social engineering techniques. Bad actors exploited human carelessness or naiveté.

Click the indicated icons for more information.

Freely available Wi-Fi in public places comes with risks. Bad actors can set up access points (APs) to act as honeypots in places like coffee shops. The unsuspecting people who connect to these so-called free networks, don’t realize that the hacker has access to everything they are doing online. For example, if you input your account credentials and credit card information, they can get it. Be wary, even if a network name seems legitimate.

In addition, our handheld devices remember networks we've attached to in the past. To help us, they automatically look for the network name or service set identifier (SSID) and connect to that network again when they see it. This means that a hacker can hear your phone looking for the legitimate hotel Wi-Fi you connected to last year, set up a fake AP broadcasting that network name, and trick your device into connecting. These are sometimes referred to as evil twin attacks, which are a type of man-in-the-middle attack used to steal information and infiltrate connecting devices. Unless you notice that your device is now connected to Wi-Fi, you may pass data through the fake AP, again exposing everything you're doing. You should never trust an SSID with open security and use other means to encrypt your communications, such as leveraging the built-in encryption feature on your device or VPN.

When setting up a router/AP, remember to change the SSID name and default passphrase that came with the device. Ensure that you chose a complex passphrase, and that security is enabled on the router so that data is encrypted when sent between devices. Update to the latest firmware, select the latest security protocol, such as WPA3, and use the latest security features. For example, some router/AP software allows you to monitor the devices connected to your network.

Newer APs can perform security inspections of the traffic and can detect and suppress rogue APs. There are legal caveats with AP suppression, which differ between countries and other legal districts. Ensure that you are familiar with the legality of AP suppression before you implement it. Some key features of a secure wireless LAN solution include strong encryption, robust authentication, network and guest network segmentation, access control lists that identify the devices permitted on the network, network monitoring, and much more. And before selecting a secure Wi-Fi protocol, ensure the client software supports it.

Fortinet offers a secure wireless LAN solution, which includes the products FortiAP™, FortiSwitch™, FortiWiFi®, and FortiGate®—a next-generation firewall.

You have completed this lesson. You are now able to:

- List common secure wireless protocols and standards.
- Explain the measures you can take to make your wireless network safer.

# Endpoint Hardening Techniques

Welcome to the *Endpoint Hardening Techniques* lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives.

With the spread of Internet of Things, or IoT, devices, the number of endpoints that need to be secured has increased exponentially. Fortunately, there are many strategies and policies that you use to secure not only traditional client and server endpoints, but the newer network connected devices that have proliferated across all aspects of life. Many of these techniques are geared toward companies and enterprise networks, but you can also use them in your personal and home environments. Remember that one of the greatest threats caused by the spread of endpoints is that of an unsecured device allowing unauthorized access to a network that can be exploited to gather information or compromise other devices.

Hardening endpoints can be broken down into several categories. The first category is using administrative controls to enforce secure passwords and restrict user and network access using the principle of least privilege (PoLP).

The second is hardening the local endpoint protection through a combination of operating system security, boot management, local disk encryption, and data loss prevention (DLP) techniques.

The third is appropriate endpoint maintenance to ensure all devices are patched and updated regularly, have regular policy checkups and have accurate, maintained backups for easy recovery.

The fourth is the monitoring of endpoint devices, which can be done locally through an endpoint protection platform (EPP) client if available, or over the networks the devices are connected to using specialized network intrusion detections systems (IDS). It is also possible to implement endpoint detection and response (EDR) platforms that can preemptively block new, undiscovered attacks and take immediate action against suspicious files and programs.

This lesson covers the first three topics.

The simplest way to harden and protect your endpoints and IoT devices is to ensure that the device has a secure password. This is especially important in household IoT devices, which regularly ship with a default password that the user is not required to change on installation. Tracking down and enforcing secure passwords on all connected devices is a simple first step that can help reduce your overall risk. A common first attack strategy is to scan a network for devices and attempt to log in and gain access to a local device using default passwords.

Another important step in securing endpoints is to ensure that users, especially administrators, have access to only the permissions they need to perform their duties. Many endpoints, even basic IoT devices, grant users the ability to create administrative roles and permissions sets. This allows the creation of authenticated roles that allow users and administrators access to only the features they need on a device. This prevents a weak password or social engineering attack from granting an attacker access to more permissions by accident.

If an attacker gains access to an account with restricted access, it will be much less damaging than if an attacker gains full administrative access because the device is using the default administrative role. The enforcement of permissions based on need is called the principle of least privilege, or PoLP, and is a good rule to follow when defining any security policy, whether for endpoints, authentication, or file access.

For simpler endpoints that can't restrict user or administrative access, consider locking down access with very secure passwords or two-factor authentication, or restricting which IP addresses can access the device using another device, such as a router or firewall.

Thorough defense is very important when hardening endpoints. If there are multiple layers of security, it is more difficult to compromise an endpoint and use it to further attack a network. Remember, a network is only as secure as its most vulnerable endpoint, so having a broader, top-down view when designing and enforcing security can be a great help in determining policies for a network, even if they cannot be applied equally to all devices.

A frequently overlooked area in endpoint security is the hardening of endpoint firmware and boot processes. Most security practices focus on securing devices when they are running and connected to the network. However, threats that attack the firmware and boot processes of endpoint devices have been emerging. Hardening firmware and boot processes is especially important for IoT devices, which lack many of the built-in protections that more traditional desktops, laptops, and servers have integrated over the years to protect against malicious firmware compromise.

Physically securing devices so that attackers do not have physical access is extremely important. It is much easier to compromise a traditional computer system if you have physical access because many devices have an administrator account reset procedure that requires only physical access to the device. Locking down the basic input/output system (BIOS) and other boot-time systems can prevent these types of attacks from being successful.

Firmware is the software that usually run from a chip on the endpoint. This software is responsible for detecting and reporting hardware connected to the device. After the firmware performs all the hardware checks, it assists in loading the operating system.

Modern computers usually use either the legacy basic input output system (BIOS) or the newer unified extensible firmware interface (UEFI). Both perform similar functions, but UEFI is much newer and usually incorporates a graphical interface and more robust security features.

Understanding how your network endpoints load their operating systems and how to secure any potential compromise is important for preventing firmware malware attacks, where code is inserted into the firmware that can cause endpoints to load malicious software or whole new operating systems that can then be used to compromise other devices. Restricting firmware so that it loads only approved software is one of the most important new features of UEFI over BIOS.

Choosing an OS is not a luxury security administrators usually have, but, if possible, it is always a good idea to select and use an OS that is easy to manage and secure. Many OSs now have built-in security features that make it easier to manage and enforce security policies. In addition, many network security devices can now allow access based on OS type. Having a fixed list of trusted OSs can help you enforce overall network security by allowing only known OS types and versions to access your networks. That way, if a firmware attack compromises a device, which then attempts to connect to the network with an unknown OS, other security devices can deny the access.

While BIOS and UEFI are specific to traditional computers and laptops, most endpoints use some sort of bootloader and firmware to secure and load the OS. Understanding and ensuring these systems are locked down is a fundamental step in endpoint security.

One of the major advantages of using laptops and cell phones for work is that they are portable. One frequent concern about these devices is data security. If a laptop is stolen and the data is not encrypted, it is very easy for the thief to extract useful information. In addition to being harmful to the individual, an unencrypted corporate laptop can contain a wealth of useful information about the corporate security posture. Just viewing browsing history and cached DNS queries on a computer can reveal sensitive network information and security procedures.

Fully securing and encrypting endpoints is a critical aspect of cybersecurity, especially for high-risk devices that may contain a great deal of sensitive information.

The most common way to secure these devices is to use full disk encryption, or FDE. FDE is a software-based solution where the disk is encrypted by the OS. On boot time, the UEFI loads the decrypting information from the OS. The cryptographic keys are usually stored in a trusted platform module (TPM) and protected by a password or other authentication method. After the keys are accessed, the disk can be decrypted, and the OS can be loaded normally. Because the entire disk is encrypted, if it is stolen, no useful information can be retrieved except by attempting to brute force the drive encryption, which is very costly.

Another way to implement full disk encryption is to use a self-encrypting drive, or SED. An SED is a hard drive with a built-in module that automatically handles the encryption and decryption of the contents of the hard drive using instructions from the firmware and OS. Using an SED pushes the cryptographic effort onto the built-in module in the hard drive, rather than the device CPU and software.

A final way to protect data on an endpoint is to use DLP software. This can detect if someone is trying to copy sensitive information from a device or send it over the network. DLP can block or log the transaction for security. Another common use of DLP is to prevent or limit the use of attachable drives, like USB flash drives or external hard drives, to prevent the copying of large amounts of data. DLP can also be network based, where devices inspect network traffic to alert administrators to keywords or other sensitive information being transmitted over networks.

Many modern devices like smartphones automatically use full disk encryption, but on some devices, this may be an option that is disabled by default. Always check if disk encryption and DLP is available on endpoints, especially IoT devices that may not have these features enabled by default.

In any environment, it is extremely important for administrators to be able to update, patch, and back up all connected endpoints. The difficulty of maintaining reliable patching and backup schedules is usually related to the sheer number of different devices and procedures required to perform updates and backups. Having a standardized desktop, laptop, server, and smartphone model and manufacturer for a company can greatly simplify the task of patch and update maintenance. However, this is not always viable because of the need to support critical legacy equipment, and the rise of bring your own device, or BYOD, in work environments.

Keeping patches up-to-date is critical because identifying and closing potential vulnerabilities is a key step in preventing a large-scale cybersecurity attack. Updating OSs, firmware, and vulnerable software programs and applications is a simple and effective way to reduce overall risk. While necessarily effective in preventing zero-day attacks, having a fully patched and updated system can also help slow down and restrict the compromising of systems using common, well-established malware and attack vectors. If your endpoint and network infrastructure is up-to-date and healthy, a new, unknown attack method may be able to compromise a system, but further infiltration may be hindered because no other tools in an attacker’s toolkit will be effective in pivoting to other systems or collecting and exfiltrating data.

In addition to maintaining, patching and updating software, having a comprehensive backup solution for critical endpoints can greatly assist in recovering from cyberattacks or accidents. You should back up critical endpoint devices, like smartphones, laptops, servers, and databases frequently. If a device is compromised, you can then collect forensic information and easily restore the device to the latest “clean” copy, with as little disruption as possible.

Backing up IoT devices, like security cameras or smart locks, depends heavily on the manufacturer, and many such devices do not have backup capability. In this case, having backup equipment that you can configure easily to replace damaged, stolen, or compromised devices should be part of a comprehensive disaster recovery plan. Having a regular backup schedule for all your devices, from computers to cameras, is one of the most effective ways to mitigate a ransomware attack. If you have a current backup of your critical data, it is much easier to restore and recover endpoints affected by ransomware.

You have completed the lesson.

# Endpoint Monitoring

Welcome to the *Endpoint Monitoring* lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives.

The process of hardening endpoints is broken into several categories. This lesson focuses on the fourth category, endpoint monitoring.

This section includes the monitoring of endpoint devices, both locally through an endpoint protection platform (EPP) client if available, or over the networks the devices are connected to using specialized network intrusion detections systems (IDS). It is also possible to implement endpoint detection and response (EDR) platforms that can preemptively block new, undiscovered attacks and take immediate action against suspicious files and programs.

To help in the administration of modern endpoints, many companies have created endpoint solutions to help manage and protect various types of endpoints from cyberthreats. Most endpoint solutions support servers, desktops, laptops, and smartphones, with additional plugins and support for the proliferation of the new, unknown, and IoT devices.

The first endpoint security solution is the endpoint protection platform, or EPP. This developed from the need of administrators to ensure servers and desktops are patched and have the appropriate antivirus software installed. Modern EPP platforms can verify versions of software and firmware, scan the local system for viruses and malware, and enforce data loss prevention and other company-defined security policies. EPP is usually viewed as a defensive measure against malicious attacks, and helps administrators maintain uniform software updates across the enterprise. EPP can also allow basic monitoring and visibility into systems to help administrators identify out-of-date devices, and remotely patch and install software on devices.

Another endpoint solution is endpoint detection and response, or EDR. This is a more proactive security solution that constantly scans a device to detect indicators of compromise, or IOC. If the EDR client detects a suspicious connection, program, or behavior, it can block the action and send an alert. This can help identify and stop threats like ransomware and zero-day attacks that may not have an established signature that would be detected by traditional anti-malware systems.

EDR usually leverages artificial intelligence and large comprehensive databases of known attacks to predict and recognize suspicious files and programs. In addition to detection and immediate response, EDR can trigger alerts to other connected endpoints and allow other endpoints to immediately block the suspicious program or file, even before it can be opened or executed, providing an immediate response against zero-day and other previously unidentified attacks. EDR systems can also have tools to help security investigators gather data on new threats, and quarantine systems that are suspected of compromise.

Both EPP and EDR solutions usually provide monitoring resources to allow security administrators to have top-down visibility on the health of their endpoints, and allow a quick response in case of potential attacks or outages. These are usually a key component in monitoring by a security operations center, or SOC. In addition, many EDR solutions allow an immediate response by automating the process to either lock down devices, or execute operations in response to a threat detected by other parts of the network. For example, a security analyst can publish an updated malware detection rule based on a common vulnerability and exposure (CVE) alert to plug a potential security risk before a patch can be made available by the device manufacturer.

One of the largest challenges in securing new devices is how to connect them to established networks securely. Many companies now allow employees to use BYOD computers and phones (Bring your own device). Because these devices are usually not well-known and not managed by the company, allowing them to connect directly to a corporate network is a large risk.

Having monitoring software and detection in place to identify and isolate unknown devices is a critical step in properly onboarding and securing these devices. If possible, force all new and unknown devices onto an isolated network until they can be secured and registered. You can use a physically separate network, VLAN, or a dedicated Wi-Fi access point to accomplish this. Once a device is registered, usually by hostname, serial number, MAC address, or static IP address, appropriate monitoring software can be installed, and the device moved to a production environment as a known endpoint.

With hard-to-secure devices and unknown endpoints, you should enforce the principle of least privilege. If these devices need access only to a specific internet or internal server, isolate them on a unique network and allow only that specific connection through firewalls and routers. That way, if the device does not meet network compliance because they are not running an appropriate endpoint security solution, it has as limited access to other resources as possible.

Once all known devices are registered, you can configure many network security devices, such as wireless access points, switches, routers, firewalls, and other connectivity points to lock down and not allow unauthorized devices to connect through the network. Disabling devices that are not monitored forces users with unknown devices to register and prevents attackers from attempting to insert their own devices onto the network remotely or by attempting to physically plug in a device locally.

You have completed this lesson.

# SOAR

Welcome to the *Security Orchestration, Automation, and Response (SOAR) lesson*.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Define Security Orchestration, Automation, and Response (SOAR).
- Describe how SOAR addresses different problems and challenges.
- Explain how SOAR's capabilities can centralize and optimize entire operations.
- Identify different use cases for SOAR.

Security Orchestration, Automation and Response (SOAR) is a hot term in the security industry. SOAR connects tools in your security stack together into defined workflows, which can be run automatically. In other words, SOAR lets you increase your team's efficiency by automating repetitive manual processes.

Automation is very important in today's security world because security teams are overwhelmed. As new tools are developed to address an evolving threat landscape, the analysts using those tools must switch between them to accomplish their day-to-day tasks. One common day-to-day task is responding to alerts. With more security tools comes more alerts, which are addressed in a series of manual processes and context switches-that is switching from one tool to another. More alerts to respond to each day means that you have less time to spend on each alert, which increases the likelihood of mistakes being made. Performance degradation in the face of a flood of alerts is called alert fatigue.

One way to mitigate alert fatigue is simply to hire more analysts. However, there simply aren't enough qualified analysts to hire. If hiring more analysts is not an option, a simple solution to fatigue is SOAR.

SOAR ties together the tools in your security stack. By pulling data in from these sources, SOAR reduces context switching that analysts deal with. Therefore, analysts can perform all their usual investigative processes directly from the source interface.

Further, those processes can be manually or automatically translated into a playbook, which is a flowchart-like set of steps, that can be repeated on demand. By using a playbook, you can ensure that every step in your standard operating procedure is followed. You also have data on exactly what was done, when, and by whom. This capability is called orchestration and automation.

Investigation is another crucial SOAR capability. When a suspicious alert appears, teams can perform their investigative tasks, such as checking threat intelligence sources for a reputation or querying a security information management system (SIM), for related events from within the SOAR platform. The information gleaned from this investigation will determine the required mitigation steps.

Then, because SOAR is a unified workbench of all your security tools, you can take those mitigation steps from within SOAR as well. For example, from within SOAR, you can block traffic from a malicious IP address in your firewall or delete a phishing email from your email server. By building your standard processes into playbooks, you can replace repetitive, time-consuming manual processes with automation at machine speed. Automation frees analysts to devote more time to investigating critical alerts.

Implementing SOAR into your ecosystem does more than just centralize your incident response processes-it optimizes an entire operation. Optimization results in streamlined responses at machine speed, allowing teams to improve collaboration and better manage the never-ending wave of alerts. This is because SOAR allows users to assign alerts to different analysts or teams at different stages of the response process, and for those assigned users to add information to the alert as they work on it, so that others who reference that alert later will have additional context on the investigation.

Teams use playbooks, sometimes called workflows, to respond to alerts or incidents the same way every time. Playbooks work in unison with security teams by taking the steps an analyst would typically implement when responding to an incident.

Playbooks do the repetitive tasks, such as compiling data into a report or sending emails, and can pause when human oversight is needed, such as when implementing a firewall block. Playbooks are the key to the automation capability of SOAR, allowing teams to improve their response speed and consistency, while maintaining human authority over the process. Ultimately, using a playbook can lead to reduced analyst workload and reduced chance of error.

Phishing investigations are one of the most common use cases for SOAR implemented by customers. Without SOAR, an analyst will spend time investigating the sender of a phishing email and key indicators located within the email headers or body. Performing these investigations usually means time spent entering domains and URLs into a threat intelligence platform. If analysts determine that an email is harmful, they will need to spend additional time investigating their email server and their SIM, determining who received the email, determining who clicked on it, deleting it, and so on.

With a phishing investigation playbook, the initial investigation steps are taken automatically, as soon as the phishing email is reported. This way, the analysts will be alerted to only those emails that the playbook determines are suspicious. After the analyst confirms that a reported email warrants further action, the playbook can continue making additional SIM queries, deleting the email from all user inboxes, sending an email to all recipients alerting them of the action taken, and providing helpful tips on what to do if they receive similar phishing messages in the future.

You have completed the lesson. You are able to:

- Define Security Orchestration, Automation, and Response (SOAR).
- Describe how SOAR addresses different problems and challenges.
- Explain how SOAR’s capabilities can centralize and optimize entire operations.
- Identify different use cases for SOAR.

# SIEM

Welcome to the Security Information and Event Management (SIEM) lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Understand what SIEM is.
- Recognize the purpose of SIEM.
- Identify the practical applications of SIEM.

What is a SIEM? Introduced in 2005, SIEM, also known as Security Information and Event Management, analyzes security alerts in real time.

Fundamentally, SIEMs do three things:

One: Collect, normalize, and store events and alerts from the organization's network and security devices, servers, databases, applications, and endpoints in a secure, central location. SIEM collects information from physical devices as well as virtual devices, both on-premises and in the cloud. Investigators had determined that logging in to every system to check for relevant log events was increasingly impossible. Also, if your logs were not secure, you had no guarantee that an attacker hadn't just deleted the entries to hide their activities.

Two: Run advanced analytics on the data, both in real time and across historical data, to identify potential security incidents that should be investigated by a human. The potential incidents are prioritized by risk, severity, and impact. Over time, these security analytics have grown from employing simple cross-correlation rules to monitoring for user-behavioral anomalies, watching for known indicators of compromise (IoC), and applying sophisticated machine learning models.

Three: Prove that all the security controls under the purview of the SIEM are in place and effective. While maintaining security for its own sake should drive security requirements and an appropriate level of investment, the primary driver for purchasing SIEM has been regulatory compliance.

With the rapid advancement of technology in the twenty-first century, there has been a need for numerous new compliance requirements, both legislative and industry sponsored. Some examples are:

- The Payment Card Industry PCI standard
- The Sarbanes-Oxley Act
- The Health Insurance Portability and Accountability Act (HIPAA)
- And the General Data Protection Regulation (GDPR).

Businesses, hospitals, and other organizations who ignore and violate the compliance requirements face punitive fines.

As cyberattacks became stealthier and more sophisticated, demands for information about a cyberattack including its characteristics, purpose, and the extent of network penetration grew more urgent. Here's an alarming fact: Security teams very often did not discover breaches until many months after they had occurred, and then it was more often discovered by a third-party than by their own internal security team.

IT security needed a holistic picture of network activity, and the real-time data collected by SIEM filled this need. SIEM vendors added threat detection capabilities with built-in threat intelligence, historical and real-time analytics, and user and entity behavior analytics (UEBA). And more recently, machine learning has become a

part of the SIEM tool set and is particularly needed when sifting through big data.

Another issue that hindered the greater acceptance of SIEM by organizations was the effort involved to set up, integrate, and use it. The technology was complex and difficult to tune, it was difficult to identify attacks, and it demanded that the user have a high level of skill to know what they were looking for. For all its capabilities, SIEM was not a set-and-forget technology. Two other facts exacerbated the situation. One, IT security suffers from an insufficient number of qualified professionals, and two, the siloed approach used in typical network operations centers (NOCs) and security operations centers (SOCs) increases complexity and causes a lack of network visibility. An environment composed of multivendor, single-point solutions with different operating systems, patch cycles, protocols, and logic, worked counter to interoperability and simplification. The result was greater demand on sparse IT resources, increased chance of human error, and reduced network security visibility.

So while SIEM made great strides moving from an information platform to a threat intelligence center, it remained hamstrung by both external and internal limitations.

The systemic shortage of trained personnel was the impetus for more automation and machine learning in later SIEM devices. Artificial Intelligence more quickly detects trends and patterns in enormous payloads of data than even the cleverest human can. Moreover, time and accuracy are gained by configuring SIEM to automatically respond and remediate.

Recent developments in SIEM have also integrated NOC and SOC, thereby establishing SIEM as the nerve center of all network and security operations. So, from a single pane of glass, IT security gains visibility into the entire network. SIEM simplifies deployment and integration by way of a self-learning, real-time, asset discovery, and device configuration engine. This tool establishes an inventory of network devices, applications, users, and business services. It then builds a topology showing how each object is interconnected, thereby establishing a baseline of normal network behavior. By determining normalcy, and with the aid of machine learning, abnormal behavior can alert analysts of a cyberattack, which can then be stopped before a breach occurs.

SIEM has evolved from an information platform, to a threat intelligence center, to a fully integrated and automated center for security and network operations.

You have completed this lesson. You are now able to:

- Understand what SIEM is.
- Recognize the purpose of SIEM.
- Identify the practical applications of SIEM.

The systemic shortage of trained personnel was the impetus for more automation and machine learning in later SIEM devices. Artificial Intelligence more quickly detects trends and patterns in enormous payloads of data than even the cleverest human can. Moreover, time and accuracy are gained by configuring SIEM to automatically respond and remediate. Recent developments in SIEM have also integrated NOC and SOC, thereby establishing SIEM as the nerve center of all network and security operations. So, from a single pane of glass, IT security gains visibility into the entire network. SIEM simplifies deployment and integration by way of a self-learning, real-time, asset discovery, and device configuration engine. This tool establishes an inventory of network devices, applications, users, and business services. It then builds a topology showing how each object is interconnected, thereby establishing a baseline of normal network behavior. By determining normalcy, and with the aid of machine learning, abnormal behavior can alert analysts of a cyberattack, which can then be stopped before a breach occurs.

Within a couple of decades, SIEM has evolved from an information platform, to a threat intelligence center, to a fully integrated and automated center for security and network operations.

The Fortinet SIEM product is named FortiSIEM™ and encompasses all of these features, plus others.

Thank you for your time, and please remember to take the quiz that follows this lesson.

# Secure SD-WAN

Welcome to the *SD-WAN* lesson. Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Describe SD-WAN.
- Explain the advantages of using SD-WAN.
- Understand how SD-WAN technology has evolved.

As the use of business-critical, cloud-based applications continues to increase, organizations with a distributed infrastructure of remote offices and an expanding remote workforce need to adapt. In this changing consumer landscape, the most effective solution is to switch from static, performance-inhibited wide-area networks (WANs) to software-defined WAN (SD-WAN) architectures.

SD-WAN (software-defined wide-area network) is a technology that uses software-defined networking (SDN) principles to improve how wide-area networks (WANs) connect across different locations. It helps organizations link users, apps, and data securely, providing better performance and making network management easier through centralized control.

SD-WAN monitors the performance of WAN connections and regulates various types of traffic to ensure consistently high speeds and optimize overall connectivity. It allows application-aware traffic routing and enables fine-tunning such as reserving costly high-speed links for business-critical applications. Unlike the traditional router-centric WAN structure, the SD-WAN model fully supports applications located in on-premises data centers, public or private clouds, and SaaS services like Salesforce, Dropbox, AWS and others.

There are several advantages of using SD-WAN over the traditional WAN solution. Click each tile to learn more.

**Centralized Orchestration**: SD-WAN centrally manages deployments, configurations and operations. This allows network administrators to generate and modify security rules in real time according to the evolving network demands. This feature helps reduce the complexity and resources required by the organization to manage its networks.

**Direct Cloud Access**: SD-WAN eliminates the need for backhauling. It enables direct access to critical cloud services for all users, regardless of their location. So, it eliminate the need to route branch office traffic through the data center regardless of the actual destination.

**Better Application Performance**: SD-WAN can be configured to prioritize business-critical traffic and real-time services like Voice over Internet Protocol (VoIP) and steer it over the most efficient route. Having several options for moving traffic helps reduce packet loss from overloaded circuits and latency due to heavy traffic, improving performance and user experience.

**Increased Business Agility**: With SD-WAN, network planners can deploy updates to all networks simultaneously. This allows the organizations to respond to their changing business needs swiftly and without delay.

**Cost Saving**: SD-WAN allows traffic to be routed efficiently over multiple channels including existing MPLS circuits and the public Internet over LTE and broadband. This reduces the need to increase the bandwidth on costly links, such as MPLS.

**Improved Security**: With the built-in security features, and the ability to restrict access to the network, organizations can protect themselves against internal and external threats more effectively. It is recommended to use SD-WAN solutions that provide a wide range of integrated security features, such as NGFW, IPS, encryption, AV, and sandboxing capabilities that can help prevent data loss, downtime, regulatory violations, and legal liabilities.

SD-WAN technology has undergone three key stages of evolution constantly adapting to the rapidly changing IT landscape. **Click** each tile to learn more.

**Phase 1 - Need for Higher Bandwidth**
SD-WAN was developed as a response to the high cost and limited bandwidth of the traditional WAN. A workaround to these issues was to add multiple dedicated carrier links and load-balancing per application traffic, based on how much bandwidth was available. Adding multiple products from multiple vendors, each with a different management console that do not fully integrate with other products significantly increased complexity of network infrastructure. Still, the first generation of SD-WAN solved a pressing business need: its basic load-balancing techniques allowed the networks to make application-intelligent business decisions on hybrid WAN links, including service provider, broadband, and long-term evolution or LTE.

**Phase 2 - Need for High-Performance**
During this stage, new capabilities such as virtualization failover/failback and application-aware routing were developed. These enhancements were driven by the demand for enhanced performance and agility in WAN operations. This addressed the issue of delays associated with MPLS installation and virtualization enabled network administrators to manage paths from a unified control panel which simplified operational processes.

**Phase 3 - Need for a Unified Security Infrastructure**
**I**n this phase, SD-WAN technology evolved beyond connecting remote branch offices to a unified infrastructure for cloud, mobility and “as-a-service” technologies by integrating security and networking functionalities into a single, secure SD-WAN appliance. This has enabled businesses to replace their multiple-point products with a powerful, single security appliance, at a reduced cost and with increased ease of management.

Secure SD-WAN is the combination of a firewall and SD-WAN functions in one device. This provides increased network security and simplify network administrator task. Fortinet introduced the term Secure SD-WAN.

- Secure SD-WAN makes it easier to manage the application needs and reduce the operational cost of businesses by prioritizing business-critical applications and allocating bandwidth as per its operational requirements.

- A centralized management console provides single, pane-of-glass visibility and telemetry to identify, troubleshoot, and resolve network issues with minimal IT staff.

- Comprehensive analytics on bandwidth utilization, application definition, path selection, and the security threat landscape not only provide visibility into the extended network but help administrators to quickly redesign policies, based on historical statistics, to improve network and application performance.

You have completed this lesson. You are now able to:

- Describe SD-WAN.
- Explain the advantages of using SD-WAN.
- Understand how the SD-WAN technology has evolved.

# ZTNA

Welcome to the *ZTNA* lesson.

Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives.

What is ZTNA?

ZTNA establishes a secure session between an end entity and a network, while ensuring granular control over access to resources and exercising zero trust, regardless of the location of either the end entity or the network.

Part of the zero trust principle is the practice of least privilege access. This means that users are only granted access to the resources necessary to fulfil their job requirements, and no more.

As a network security concept, zero trust operates under the premise that no user or device inside or outside the network should be trusted, unless their identification and security status have been thoroughly checked. Zero trust operates on the assumption that threats, both outside and inside the network, are omnipresent. Zero trust also assumes that every attempt to access a network or an application is a threat.

So, regardless of whether the end entity is remote or on-premises, the connecting computing device automatically establishes an encrypted session with the network. Specifically, this connection takes place between a ZTNA client at the end entity and the ZTNA access proxy, which could be a firewall. The proxy point hides the locations of requested applications from the outside. The proxy directs the client's request to the application, which could be on-site or in the cloud, only if the user meets access requirements.

Other ZTNA components are authentication and security. Because the user is identified through authentication against an on-premises backend server or an Identity-as-a-service (IDaaS), policy can be applied based on the user roles.

Also, the ZTNA policy server enforces policy-to-control access, specifically to applications. For example, access could, in part, be based on geolocation. So, if the remote device is connecting from an unexpected point in the world, access to an application could be denied or privileges reduced.

Likewise, if a device fails a security sanity check, the user could be denied access. Security is composed of firewalls and the ZTNA access proxy, which control access and provide security to application resources.

Unlike IPsec VPN, but similar to SSL VPN, ZTNA is vendor specific. This means that each vendor can implement ZTNA in a way that best suits their specific requirements.

The diagram on this slide is the Fortinet ZTNA solution. The Fortinet ZTNA client is FortiClient.

Also in this diagram, FortiClient Endpoint Management Server (EMS) acts as the ZTNA policy server. When an endpoint device with FortiClient attempts to connect to the network for the first time, it is directed to FortiClient EMS to register. During the registration process, FortiClient provides the server with information about the device, the user, and the security posture of the device. This information is written to tags and shared with the firewall, FortiGate.

Based on the information in the tags, the device can be grouped and certain rules can be applied. The rules act as instructions for FortiGate. FortiGate applies the rules to the device each time it connects to the network. An example of a rule could be that a device with Windows 10 plus antivirus software is allowed access, but a device with Windows 10 and no antivirus software is denied access.

At the end of the registration process, FortiClient EMS generates a digital certificate for the device, and sends the certificate to the device and shares with FortiGate. From this point onward, the device submits the certificate to FortiGate each time it needs to identify itself.

FortiClient is in continuous communication with FortiClient EMS. If the endpoint information changes, the server updates the client tags and resynchronizes with FortiGate.

The ongoing communication between these components is called network telemetry, and it provides agile and dynamic responses to enhance network security.

How does Fortinet ZTNA work?

When the endpoint connects to the ZTNA access proxy, FortiGate challenges the endpoint for device identification.

The endpoint sends the device certificate to FortiGate, proving the device identity. Then, FortiGate applies the associated tags and rules and either rejects the request or allows the device to proceed.

FortiGate challenges the endpoint for user authentication.

The endpoint prompts the user for their credentials and delivers the credentials to the access proxy.

In turn, the access proxy sends the user credentials to the backend for authentication.

The authenticating server could be an AD, an LDAP directory, a database, or IDaaS.

The ZTNA access proxy retrieves the user’s identity, along with role information. FortiGate uses the role information to help determine if the user has permission to access the requested network application.

Finally, assuming that the device and user have been identified, and the devices tags and rules plus the user’s roles allow access to the resource, an encrypted session is initiated between the ZTNA client and the ZTNA access proxy, and the user gains access to the application.

You’ve completed the lesson. You can now achieve these objectives.

# Cloud Security

Welcome to the Cloud Security lesson.
Click **Next** to get started.

After completing this lesson, you will be able to achieve these objectives:

- Understand what the cloud is and how it came to be.
- Identify the different types of cloud services.
- Describe how cloud environments are secured.

It wasn't long until most data centers were transformed from rows of computer hardware dedicated to specific applications, into a collection—or pool—of general hardware resources running virtualized applications.

With the help of some ingenious entrepreneurs who built enormous data centers, filled with generalized computer hardware, service providers offered to rent out portions of this infrastructure so that their customers could run their virtualized applications there, instead of on their own hardware. With that, the cloud was born.

This type of cloud computing is called Infrastructure-as-a-Service or IaaS. IaaS provides organizations with networking, storage, physical servers, and virtualization, while users must still provide computers with operating systems, middleware, data, and applications. Middleware is software that acts as a bridge between the OS and applications. An organization uses this type of service when demand for its services or products varies, such as during seasonal holidays when workloads on systems increase. Examples of this type of service provider are Amazon Web Services, Microsoft Azure, and Google Cloud Platform.

There are other types of clouds as well. For example, service providers rent cloud-based platforms for software developers to develop and deliver applications. This service, named Platform-as-a-Service or PaaS, provides the OS and middleware in addition to the elements provided by IaaS. This service makes it easier, more efficient, and cheaper for organizations to build, test, and deploy applications.

A third example is Software-as-a-Service or SaaS. In this cloud service, the software is hosted by a third party. Typically, the end user connects to the application using their browser. Common examples of applications available through SaaS are Google Mail, Salesforce, DocuSign, and Netflix.

Either way, moving the cost of having applications run on expensive, company-owned hardware capital assets to a model where the price is a recurring operating cost is very attractive to most organizations.

When applications are hosted in a company's own data center, the security picture is straightforward: you put the appropriate security technology at the right locations to address the specific security concerns. Providing security for the cloud, however, is not so clear. Security is a shared responsibility between the cloud provider and the customer using the cloud services.

Designed in layers, security includes both the physical components and logical components.

The cloud infrastructure provided by IaaS vendors is protected in various ways. From an availability point of view, the infrastructure is designed by the vendor to be highly available, and it follows that the infrastructure uptime is the responsibility of the vendor. From a security point of view, the vendor is responsible only for securing the infrastructure it provides.

As a customer, when you install one or more virtualized applications in the vendor's cloud infrastructure, you are responsible for securing the access, network traffic, and data applications.

Most vendors supply some form of security tools so that various parts of the customer's cloud application environment can be secured. However, these tools can pose a few problems.
First, these tools tend to provide only a few basic security functions, and they are the same tools the vendors use to secure the underlying infrastructure. If an attacker were to bypass these tools at the infrastructure layer, they would likely be able to bypass them at the customer's application level as well.
Second, and perhaps more important, is the fact that many organizations operate in a hybrid world where some of their applications remain hosted in their own data centers, some in Vendor-A IaaS cloud platform, some in Vendor-B cloud platform, and various others with multiple SaaS vendors. This is what we call a "multicloud" environment, and it comes with a "multicloud" problem: multiple, independent, uncoordinated security solutions--a problem where complexity can scale geometrically with the number of cloud vendors involved.

To make things more difficult, highly trained security staff are scarce. Additionally, it can be a burden to integrate and operate multiple nonintegrated security environments simultaneously. All these factors can be a real problem.

Fortinet has a portfolio of security solutions that are at home in a company's data center, providing the same consistent security, and also optimized for all the leading IaaS cloud providers.

You have completed the lesson. You are able to:

- Understand what the cloud is and how it came to be.
- Identify the different types of cloud services.
- Describe how cloud environments are secured.

# SASE

Welcome to the SASE lesson. Click Next to get started.

After completing this lesson, you will be able to achieve these objectives:

- Describe SASE.
- Understand the core security features of a SASE solution.
- Understand the benefits of using SASE.

As work environments have evolved, so too have user behavior and endpoint protection requirements. Organizations today require that their users have immediate, continuous secure access to network and cloud-based resources and data regardless of location, on any device, and at any time. Organizations must provide this access in a scalable and elastic way that integrates thin edge network sites and remote users into the central infrastructure, and that favors a lean operational, as-a-service model.

SASE technology addresses the needs of this complex network infrastructure by combining Network-as-a-Service with Security-as-a-Service capabilities. SASE is delivered through the cloud as an as-a-service consumption model, to support secure access for today’s distributed and hybrid enterprise networks. This let’s work-from-anywhere and remote workers, take advantage of firewall as a service (FWaaS), secure web gateway (SWG), zero-trust network access (ZTNA), and a medley of threat detection functions. SASE is composed of Security Service Edge (SSE) and SD-WAN.

When properly implemented, a SASE approach allows organizations to apply for secure access no matter where their users, workloads, devices, or applications are located. This becomes a critically important advantage to ensure remote workers' security.  SASE offers flexible and consistent security, reduced IT cost and complexity and fast, seamless user experience.

Fortinet Unified SASE seamlessly integrates essential networking and security technologies delivered through the cloud. Its innovative approach ensures secure access for a hybrid workforce and safeguards applications and data on any cloud. The Fortinet single-vendor SASE solution integrates SD-WAN and a cloud-delivered security service edge (SSE) to deliver networking and security to the network edge and remote workers.

A SASE solution provides integrated networking and security capabilities. These are some of the key features of SASE. **Click** each tile to learn more.

**1- Software-Defined Wide Area Network (SD-WAN)**

SD-WAN employs an overlay structure to streamline operations and enhance user satisfaction by intelligently directing traffic to the most efficient routes for internet, cloud applications, and data centers. Moreover, it facilitates swift deployment of new applications and services while efficiently managing policies across numerous locations.

**2- Secure Web Gateway (SWG)**

SWG provides a secure web experience to protect users, devices and applications from online threats. It filters malware, prevents data loss and enforces internet policy compliance.

**3- Firewall-as-a-Service (FWaaS)**

FWaaS enables the substitution of physical firewall appliances with cloud-based counterparts, offering advanced next-generation firewall (NGFW) security capabilities such as Intrusion Prevention System (IPS), Anti-Malware, SSL Inspection, and Sandbox.

**4- Cloud Access Security Broker (CASB)**

CASB prevents data leaks, malware infection, regulatory noncompliance, and lack of visibility by ensuring safe use of cloud apps and services. It secures cloud applications hosted in public clouds (IaaS), private clouds, or delivered as software-as-a-service (SaaS).

**5- Zero Trust Network Access (ZTNA)**

ZTNA solutions provide secure access to internal applications for remote users. It ensures that no user or device is automatically trusted. Every attempt to access a system, from either inside or outside, is challenged and verified before granting access. It consists of multiple technologies, including multi-factor authentication MFA, secure Network Access Control NAC and access policy enforcement.

**6- Centralized Management**

Centralizing the management of all security features within a single console enables the streamlining of change control, patch management, coordination of outage windows, and policy administration. This approach ensures the delivery of consistent policies across the organization, regardless of where users connect from.

Finally, the multi-edge network environment of today has exposed the limitations of VPN-only solutions, which are unable to support the security, threat detection, and zero-trust network access policy enforcement present at the corporate on premise network. VPN-only solutions cannot scale to support the growing number of users and devices, resulting in inconsistent security across all edges.

The Fortinet secure access service edge (SASE) solution enables secure access to the web, cloud, and applications for a hybrid workforce, while simplifying operations. FortiSASE offers a wide range of security capabilities, including a secure web gateway (SWG); universal zero trust network access (ZTNA); next generation dual mode, cloud access security broker (CASB); and Firewall-as-a-Service (FWaaS).Fortinet is the first vendor to deliver a comprehensive SASE solution. FortiSASE integrates cloud-delivered SD-WAN connectivity with security service edge (SSE), extending the convergence of networking and security from the edge to remote users.

You have completed this lesson. You are now able to:

- Describe SASE.
- Understand the core security features of a SASE solution.
- Understand the benefits of using SASE.