NSE2 Lesson Scripts - Apuntes 1

calculo integral (Instituto Nacional de Educación Media Diversificada Manuel Murillo Toro)

FORTINET NSE Training Institute

NSE 2 Lesson Scripts—English Version

Table of Contents

Lesson 1—Cloud Security

Hello! In this lesson, we explore the mysterious "cloud", what it really is, how it came to be, and some of the security issues that we encounter there.

First, let's de-mystify the cloud. It's amusing that "the cloud" has extremely high public name recognition, but few understand what it really is.

Traditionally, before the cloud, companies and other organizations purchased their own computer systems to run the application software needed to run the business. These computer systems were located in the company's facilities, and managed by teams of employees. While not always the case, often there was more than one computer system (or server) per major application.

This setup was expensive because of the capital cost of the computer hardware and labor cost of the resident experts who kept it all running; but it was worth it. These systems raised overall productivity and helped maintain competitive advantage.

Not long ago, someone noticed that of all their computer systems, only a few were completely busy at any given moment in time. Most were idle, waiting for the next transaction to come in. Bottom line: there were many wasted resources.

So, a new way of using server hardware was developed called virtualization, which actually comes from old technology in mainframe computing that lets a single server run the operating systems and applications from multiple servers simultaneously. The virtualization consolidates workloads onto fewer servers, increasing their utilization, and saves money.

It wasn't long until most datacenters were transformed from rows of computer hardware dedicated to specific applications, into a collection—or pool—of general hardware resources running virtualized applications. It was just the smart thing to do.

Along comes some ingenious entrepreneurs who build enormous datacenters, filled with generalized computer hardware, and offer to rent out portions of this infrastructure so that their customers can run their virtualized applications there, instead of on their own hardware. With that, the cloud is born.

This type of cloud computing is called Infrastructure as a Service or IaaS. There are other types of clouds as well. For example, some cloud providers offer up the infrastructure to run applications with managed services like databases that a customer does not need to patch and maintain, or even complete application environments themselves. This is known as Software as a Service or SaaS. If you've ever used Google mail, or something like it, then you've used SaaS.

In addition, sitting between IaaS and SaaS in terms of functionality and responsibility is the Platform as a Service or PaaS. This includes services where the cloud provider manages much more of the underlying infrastructure, such as OS patching, and abstracts away a lot of the work for users, who in this case acquire a stable environment to run containers. PaaS is becoming increasingly prevalent.

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.

Now let's look at what this means to security.

When applications are hosted in a company's own datacenter, 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. You could say it's a bit cloudy. Bottom line: security is a shared responsibility between the cloud provider and the customer utilizing 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's uptime is the responsibility of the vendor. From a security point of view, the vendor is only responsible 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, the network traffic, and the data applications.

Now, 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 datacenters, 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 "Multi-Cloud" environment, and it comes with a "Multi-Cloud" problem: multiple, independent, uncoordinated security solutions—a problem where complexity can scale geometrically with the number of cloud vendors involved.

Now, highly trained security staff are scarce to start with. Add to that a burden to integrate and operate multiple non-integrated security environments simultaneously … it can be a real problem.

At Fortinet, we have security solutions such as FortiGate, FortiMail, FortiWeb, FortiSandbox, FortiInsight, and others within the Fortinet Security Fabric that are not only at home in a company's data center, providing the same consistent security, they are optimized for all the leading IaaS cloud providers such as Amazon AWS, Microsoft Azure, Google Cloud, VMware, Cisco ACI, Oracle Cloud, and IBM.

To wrap up, we've shown the fundamentals of how "the cloud" came to be, how cloud environments are secured, and described Fortinet's cloud security strategy that scales from simple cloud-only environments to complex multi-cloud environments.

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

Lesson 2—SD-WAN

Hello! In this lesson, we'll explain what SD-WAN is and how it has evolved.

SD-WAN stands for software-defined wide-area network, and it leverages the corporate WAN as well as multi-cloud connectivity to deliver high-speed application performance.

In the past, organizations purchased and operated their own servers to run applications and store critical business data. As a result, they had upfront capital expenses, and they needed to employ a team of highly trained technicians to run these servers. While expensive, the competitive advantage it gave over those who didn't computerize their businesses, made it worthwhile. One early challenge was to make these servers available to various geographically-distributed networks, called local area networks or LANs.

You might recall that a WAN is a computer network that spans a large geographic area and typically consists of two or more LANs. For example, if Acme Corporation spanned multiple cities and continents, each with their own local area network, how would they connect these LANs so that someone in the London office could connect to a database server in Singapore? Traditionally, businesses connected theirs LANs by way of a single, dedicated service provider. Though expensive, they could control and secure this connection while providing access to critical resources. However, this method had limitations. The single point of connectivity was subject to frequent outages, which made it unreliable. In addition, because there was an increasing demand to host business applications in the cloud, known as software as a service (SaaS), higher latency became an issue. SaaS applications, like Salesforce, Dropbox, and Google Apps, and a greater reliance on video and voice conferencing, contributed to the congestion. Businesses began to augment their connectivity by employing multiple providers, or seeking more affordable broadband and other means of internet connectivity. The trend toward increasing hybrid connections, and the growth of cloud applications to support underlying intelligent business decisions, led to the first generation of SD-WAN.

Businesses added multiple dedicated carrier links and load-balancing per application traffic, based on how much bandwidth was available. Although this approach seemed to solve a few bandwidth issues, it added yet another product to solve another network challenge. These point products escalate complexity to the network infrastructure. Why? Because adding multiple products from multiple vendors, each of which have separate management consoles and which often do not fully integrate with other products, becomes a management nightmare for IT security administrators. Still, the first generation of SD-WAN solved a pressing business need: its basic load-balancing techniques allowed the network to make application-intelligent business decisions on hybrid WAN links, including service provider, broadband, and long-term evolution or LTE, which is a standard for wireless broadband communication for mobile devices and data terminals.

Accurate application identification, visibility into network performance, and reliable switchover of application traffic between best performing WAN links pivoted SD-WAN as the most sought-after WAN technology across all businesses.

However, security remained a serious consideration for businesses. Even after SD-WAN adoption, businesses kept sending all their sensitive and critical application traffic to data centers for security purposes, or were forced to install a sophisticated firewall solution to inspect their direct internet

access. This added another point product for security, making the network yet more complex, challenging to manage, and delaying cloud adoption.

Businesses needed to address these challenges by integrating security and networking functionalities into a single, secure SD-WAN appliance. This enabled businesses to replace their multiple point products with a powerful, single security appliance, at a reduced cost and ease of management. A strong security posture helped businesses to use cloud applications more affordably, with lower latency, and with a direct internet connection ensuring optimal application performance and best user experience. Continued network performance health checks ensured that the best available WAN link was chosen, based on user-defined application service level agreements. Should a particular link degrade, the SD-WAN device knew to move the connection to the better performing WAN link.

Today, in secure SD-WAN, intuitive business policy workflows make it easy to configure and manage the application needs with the flexibility of prioritizing business-critical applications. 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 helps administrators to quickly redesign policies, based on historical statistics, to improve network and application performance.

Overall, positive outcomes of a secure SD-WAN solution are simplification, consolidation, and cost reduction while providing much needed optimal application performance and best user experience for the enterprise, SaaS, and Unified Communications as a Service (UCaaS) applications. Run-time analytics and telemetry help infrastructure teams coordinate and resolve issues in an accelerated manner, which reduces the number of support tickets and network outages.

Fortinet introduced the term Secure SD-WAN, of which FortiGate® is at the core—the next generation firewall (NGFW) of Fortinet. In addition to the FortiGate® device, the Secure SD-WAN solution includes other advanced networking features.

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

Lesson 3—Endpoint Security

Hello! In this lesson we will learn about endpoint security, what it is and how it has evolved.

Let's define what we mean by an endpoint. In the past, it was defined as any personal device used by an end user, like a desktop computer, laptop, or handheld device. Now, endpoints include the Internet of Things, or IoTs, which encompasses all sorts of gadgets, such as a smart thermostat or fridge in a home.

How have we secured these endpoints and why is endpoint security so important? Endpoints have always been an easy point of entry into a network. Why try to circumvent a firewall when, through social engineering, you can exploit gullible, careless users. As online connections have expanded, the number of attack vectors have multiplied on the endpoints, giving attackers more opportunities to exploit.

Before networks were connected to the internet, bad actors relied on floppy discs to spread malware. An infected disc inserted into a computer would infect that computer. Later, this would include other removable storage devices, such as CDs, DVDs, and USB-connected portable drives. As you can imagine, this attack vector was quite limited in scope. The first endpoint security products were antivirus, or AV, software that would scan devices and your hard drive for malware. They were signature-based, meaning that the antivirus software looked for specific characteristics, fingerprints, or signatures, of the virus. If it found something that had those characteristics, it could quarantine or expunge the program.

All of this changed when home and business networks began to connect to the internet. Many more attack vectors became available to the cybercriminal, such as email phishing, infected websites, bring-your-own-device (BYOD) to work, and social media. These new opportunities proliferated the growth of malware—from tens of thousands per year to hundreds of thousand per day. Also, the bad actors began to exploit security loopholes in operating systems, applications like your web browser, and even relatively inert applications like an MS Word document. Compounding this problem of an expanding attack surface, the very nature of malware changed. Polymorphic malware is designed to change all by itself, mimicking viruses that mutate in the natural world. This meant that signature-based antivirus software was no longer fully effective.

Along came the endpoint protection platform or EPP, which was intended to prevent file-based malware attacks and implement other preventative controls. The method focused on stopping malware before it executed and infected the endpoint. File-based malware is a file downloaded to a device, which when opened, runs malicious code or a script.

EPP provided many prevention-focused services, such as anti-virus, device firewall, web filtering, data protection through encryption, and device control. Device control is a technology that provides built-in security that detects, authorizes, and secures removable storage devices. Web filtering is technology that enables network administrators to control what type of site you are permitted to visit.

However, none of these techniques proved to be the ultimate remedy for endpoint infections. At the time, web filtering was thought to be the solution because it was assumed that web-born malware came only from lewd websites. The possibility remained that malware could pose as an advertisement on a legitimate site.

Given the ever-evolving complexity of attack methods and the expanding attack surface, security professionals came to realize it was impossible to prevent all malware infections. A new strategy was developed to defend the endpoint in parallel to EPP development. That new strategy is called endpoint detection and response, or EDR.

EDR is software used to detect, investigate, and respond to suspicious activities on endpoints. It began as a digital forensics investigation tool, and provided security analysts with the threat intelligence information and tools needed to analyze an attack and to identify the indicators of compromise, or IoC. Analysts were then able to detect malware, some of which dwelled undetected in networks for months or years. Instead of investigating an attack to learn about its anatomy, the tool was also used to detect an ongoing attack in real time. Remediation tools were also added, which enabled analysts to request more information from endpoints, ban processes, isolate endpoints, and block specific IPs. EDR grew into a true detection and response solution, but it was not without problems.

This first-generation EDR mostly used manual methods that were time-consuming and were too slow for fast-moving threats like ransomware. The lack of integration with other security software hindered its ability to respond in an effective and timely manner. Configuring and using EDR demanded high-level expertise, and the analysis of a multitude of alerts, many of which were false positives, was time consuming for the analysts. Vendors partly mitigated these problems by introducing a managed detection and response, or MDR platform, which performed basic alert triage and notified analysts via email. Still, EDR remained too slow and too complicated to become a standard tool in the arsenal of endpoint security software.

Second-generation EDR addressed these issues. It was designed to be policy-driven and automated. Through customizable playbooks, analysts can now direct EDR to remediate problems both immediately and automatically. Proactively, analysts can instruct EDR to respond in a specific way should it detect a program or script that behaves suspiciously. Malicious activities trigger automatic blocks to prevent data exfiltration, encryption, and attempts to infiltrate the network. It can stop and roll-back ransomware in real time without necessarily removing the device or disrupting business continuity.

Security professionals quickly realized the advantages of merging EDR and EPP technologies, and most EPP definitions now include both characteristics. A single, integrated agent can prevent the majority of file-based malware at the pre-infection, pre-execution stage, while detecting and responding to malware that evaded prevention at the post-infection stage. A combined EPP and EDR solution also removes integration concerns and simplifies configuration and management for analysts.

EPP and EDR software now includes other preventative controls to improve security hygiene, such as alerting analysts when endpoints don't have the latest security patch or are running unsecure applications. By identifying critical vulnerabilities, security teams can mitigate threats and apply virtual patches or create policies that apply restrictions to endpoints until a software patch is installed. In addition, machine learning (ML) is now included as part of the enhanced AV capabilities, which helps detect malware at the pre-execution stage.

The Fortinet endpoint security products are FortiClient® and FortiEDRTM. The FortiClient® device is fully integrated with other security products that share intelligence data and are managed centrally in what is called the Fortinet Security Fabric.

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

Lesson 4—Firewall

In this lesson, you will learn how firewalls were created to provide rudimentary network security and how they evolved into next generation firewalls to keep up with the ever-changing threat landscape.

As networks began to grow, interconnect, and eventually connect to the internet, it became important to control the flow of network traffic. This control initially took the form of packet filter firewalls that examine the very lowest protocol layers, such as source and destination network addresses, protocols, and port numbers. Firewall rules used these attributes to define which packets were allowed through. If the packet network addresses, protocol, and port number matched those of a packet filtering rule in the firewall, it was allowed to pass through. If it didn't, it was either silently dropped or blocked.

The drawback of packet filter firewalls was that they took a one-size-fits-all approach to decide whether or not to allow traffic to pass, and bad actors could bypass firewall rules. What would stop a bad actor from injecting rogue packets through acceptable protocols and ports, or exploiting a bug in computer networking software? To offset this weakness, additional criteria for blocking or allowing traffic was developed in second generation firewalls.

Second generation firewalls, called stateful firewalls, were designed to observe these network connections over time. They would watch as new network connections were made, and continuously examine the conversation between the endpoints. If a connection behaved improperly, the firewall blocked that connection. Any packets that didn't belong to a known conversation were dropped.

While this was an improvement, second-generation firewalls still couldn't block rogue packets if they were 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 static text content, e-commerce, file hosting, and in many other kinds of web applications. Because they all use the same port number, the firewall is not able to distinguish between them. Network administrators needed to distinguish between these web applications to block the malicious ones and allow the beneficial ones. To determine how protocols such as HTTP are used, the firewall must look deeper into the data payloads.

Third generation firewalls do just that. While still stateful, these firewalls understood the higher-level protocols and the applications inside them, and controlled 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, DNS, and others. In the case of HTTP, it can differentiate between browser traffic to a blog, a file sharing site, e-commerce, social media, voice-over-IP, email, and many more.

Our increasing connections through the internet also precipitated profound changes to the way we work, play, entertain, and do commerce. Businesses evolved to take advantage of cheaper, multi-cloud services, and the convenience of mobile and IoT devices dramatically expanded network edges, thereby increasing the attack surface. Threat actors continue to change in terms of attack methods and sophistication. Attacks now come from trusted users, devices, and applications that spread malware, both unknowingly and with malicious intent.

A firewall must now prevent evolving cyber-attacks at every edge of the network while delivering security, reliability, and network performance. This brings us to the advanced security capabilities that

are found in the next-generation firewall (NGFW). Similar to airport security, a next-generation firewall has 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. Then your travel bags are checked to see if you are carrying any malicious content. This is similar to how a next-generation firewall performs deep packet inspection (IPS). If questionable content is found in your travel bag, enhanced airport screening will set the bag aside to examine further. This is similar to how the next-generation firewall sends malicious content over to a sandbox for further analysis.

As networks continue to evolve and introduce new challenges, next-generation firewalls also evolve. For example, they have the ability to control applications, either by classification or based on 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, which are aligned to business needs. By segmenting networks rather than using a flat network, the firewall helps eliminate a single point of entry, which made it easier for cyber criminals to get inside the network and spread threats across the network.

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 that are 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.

FortiGate® is the next-generation firewall of Fortinet. The FortiGate® device is fully integrated with other security products that share intelligence data and are managed centrally in what is called the Fortinet Security Fabric.

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

Lesson 5—Wi-Fi

Hello! In this lesson, you will learn about Wi-Fi and the security implications of wireless networks.

Wi-Fi is a technology for wireless, local area networking of devices based on the IEEE 802.11 standards. It started small, intended mostly for industrial use, and has grown to be the most common way that all our personal electronic devices connect at home or at the office.

The development of Wi-Fi leveraged many of the same protocols and technology as Ethernet, with one very large difference. All transmissions are happening over the air; meaning that, much like a verbal conversation, anyone listening can hear what is being said.

Originally the authentication and privacy mechanisms for Wi-Fi were very weak . The standard had a simple option to provide encryption called Wired Equivalent Privacy or WEP. WEP used a key to encrypt traffic using the RC4 keystream. However, someone could compromise WEP fairly quickly if they had the right tools and a reasonably powerful machine. The word went out, Wi-Fi was insecure, and the technology, which was just starting to grow, had serious problems.
Stakeholders gathered with IEEE and the Wi-Fi Alliance to produce Wi-Fi Protected Access (WPA). It added extra security features, but retained the RC4 algorithm, which made it easy for users to upgrade their older devices. However, it still didn't solve the fundamental security problem.

A new standard, based on the Advanced Encryption Standard, or AES, algorithm from the National Institute of Standards and Technology (NIST), was also introduced as Wi-Fi Protected Access 2 (WPA2). This was a lot more secure than WEP. In addition, new enterprise-grade authentication was added to the technology, creating two flavors of each security style. The personal level of security continued to use a shared passphrase for network authentication and key exchange. The enterprise level of security used 802.1x authentication mechanisms, similar to those used on wired networks, to authenticate a user and set up encryption. However, poorly chosen or weak passphrases could still leave networks vulnerable.

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.

It might seem like that's it, wireless is now secure, and there's nothing to worry about. Unfortunately, that is not the case. Hackers have found several ways to exploit human behavior and still get access to the information they want.

Free Wi-Fi Available, is a sign we all look for when in public, yet it comes with risks. Hackers set up access points (APs) to act as honeypots in public areas. 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 legit.

In addition, our handheld devices remember networks we've attached to in the past. In an effort to help us, they automatically look for and attach 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. 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're not just exposed when you're away from home. Many people set up their network at home, but never turn on security. Or if they did, they set it long ago, possibly using WEP or WPA, and never updated to a stronger passphrase. Newer firmware for home wireless routers now offers additional features, such as WPA3 or visibility into the devices on their network. It's a good idea to keep your security up to date, and pick passphrases that are complex and hard to guess. At the very least, change the service set identifier, or SSID, and admin default username and password! Also, keep an eye on your home network and make sure you recognize the devices that are accessing it. If a hacker gets onto the network, they have access to everything on that network. At that point it's no longer a question of reading the wireless traffic you're sending, it's about what devices they can compromise and what data they can get from those devices.

The challenges associated with enterprise class Wi-Fi continue to grow. With IoT, BYOD, and a highly mobile workforce, it's critical to manage access points while also dealing with evolving security threats, be it at the corporate office, remote office, or in your home.

Fortinet offers a wireless product named FortiAP™. It supports the latest Wi-Fi technologies, and integrates with, and is managed by FortiGate®, a next-generation firewall.

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

Lesson 6—Threat Intelligence Services

In this lesson, you will learn how security vendors collect threat information, and provide access to that collected knowledge to detect bad behaviors online.

In the early days of endpoint antivirus products, vendors needed a way to catalog all the known viruses so that their products could confirm whether or not a file contained a virus. Their threat intelligence department did this by taking a sample of each known virus and generating a signature, which represented the contents of the file. In other words, a fingerprint. These virus signature lists were distributed with antivirus software. As time went on and new viruses were detected, each vendor's threat intelligence service distributed updates to their virus signature list. These updates were issued regularly and in a variety of different ways. Updates were released monthly, quarterly, or, in some cases, only once per year.

As the malware developers gained expertise, their malware became more sophisticated and included mechanisms to evade classic signature-based scanning by being able to change their file contents at will. Because the file contents changed, their signatures also changed, allowing malware to sneak by the older antivirus products. This gave rise to a single type of malware becoming an entire malware family of perhaps hundreds of thousands of different files, also known as polymorphic malware, and each performing the same bad behaviors. This problem also happens when do-it-yourself malware kits are placed for sale on the dark web—not to mention the proliferation of malware-as-a-service organizations. Cybercrime has its own business model!

Now we have a new problem: the classic one-to-one signature approach in which each known malware file is represented by one signature in the signature file is obviously not going to scale well, given the potential that the number of new variations of malware will count in the millions or more each day. To handle this new ability for malware to morph into new forms, the vendors' threat intelligence services created ways to detect entire families of malware using only one signature. This is done in a variety of different ways, but they all detect commonalities across the malware family.

Up to now, we've been talking about malware that has been seen and is therefore known to the vendors' threat researchers. What about malware variations that have not yet been seen? Signature-based detection methods will not work. To detect these types of threats, vendors created sandboxing products, which take a suspect file and place it in an environment where its behaviors can be closely analyzed. If the file does something malicious while in the sandbox, it is flagged as malware. This is known as heuristic detection, and it looks for anomaly behavior that is out of the ordinary. In fact, vendors create proprietary heuristic algorithms that can detect never before seen polymorphic samples of malware.

Depending on the particular sandbox product and its configuration, the owner of the sandbox can propagate this new knowledge not only across their own network security environment, but also send the details to the vendor's threat intelligence service so that it can be shared worldwide and protect more people.

Beyond sandboxing, the future of detecting previously unknown malware includes the threat intelligence service's use of artificial intelligence and machine learning to rapidly grade the security threat potential of files as they traverse the network. And it's not just about files. The threat intelligence service catalogs the knowledge about existing or emerging attacks, including the specific mechanisms of the attack, the evidence that the attack has happened—also known as the Indicators of Compromise or IoCs—implications of the attack, attribution of the adversary, and their potential motivations.

As the techniques used by bad actors continue to evolve and become more sophisticated, it's more important than ever to share threat intelligence in real-time, across the entire network security environment. If some security components know about the attack while others wait for periodic signature updates, the attackers may sneak past defenses and cause harm. Security products and threat intelligence services that can act together in real-time stand the best chance of stopping these attacks.

And the sharing of threat intelligence doesn't stop with each vendor's product lineup. Although you would think that after putting in the work required to gather, analyze, and catalog threat information, each vendor would keep that information secret. Almost all vendors share this information with the wider security community. This happens through formal memberships in organizations such as the Cyber Threat Alliance, local, national, and international Computer Emergency Response Teams, or CERTs, as well as numerous private trusted partnerships with other vendors, independent security researchers, and law enforcement. This real-time sharing of threat information allows for a more complete picture of the attack, because no single vendor is going to have all the data, and it isn't the threat intelligence that sets vendors apart, it's what they do with the intelligence with the technology in their products.

This is where Fortinet excels. Our threat intelligence service is known as FortiGuard® Labs. Spanning ten distinct security disciplines, hundreds of researchers at FortiGuard® Labs scour the cyberthreat landscape, and proactively seek out new avenues of attack every day to discover (and ideally preempt) emerging threats. The FortiGuard® Labs certified and proven security protection provides comprehensive security services, updates, and protection for the full range of Fortinet Security Fabric solutions.

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

Lesson 7—SOAR

Hello. In this lesson we will take a look at Security Orchestration, Automation and Response (SOAR). SOAR is a hot term in the security industry, so it's important to not only know what it is but to be familiar with the problems and challenges that are addressed by SOAR. But before we get to that, let's first examine the basics.

What is SOAR? SOAR connects all of the other 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 have to switch between them in order 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 obvious way to mitigate alert fatigue is simply to hire more analysts. However, thanks to a cyber-security skills shortage, there simply aren't enough qualified analysts to hire. So if hiring more analysts is not an option, how do we solve alert fatigue? Simple, with SOAR.

As mentioned, SOAR ties together the tools in your security stack. By pulling data in from all of these sources, SOAR reduces context switching that analysts have to deal with. So, analysts can perform all of 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.

Let's explain playbooks in more detail. Teams use playbooks, sometimes called workflows, as a way 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 to implement 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.

So there you have it—a primer on SOAR—what it is, what problems it addresses, and how it helps. The Fortinet SOAR product is named FortiSOAR™ and encompasses all of these features and more.

Thank you for your time. And don't forget to take the quiz!

Lesson 8—Network Access Control

Hello! In this lesson, we will introduce you to Network Access Control (NAC) and explain how it has evolved.

NAC is an appliance or virtual machine that controls device access to the network. It began as a network authentication and authorization method for devices joining the network, which follows the IEEE 802.1X standards. The authentication method involves 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. Pending 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. If you've ever connected to a network in an airport, hotel, or coffee shop, you might remember interacting with a web page that asked you to agree to legal terms before granting access.

Later, NAC evolved to accommodate guest access, Bring Your Own Device (BYOD), and the Internet of Things (IoT). For a couple of reasons, BYOD and IoT devices introduced new security challenges. One, BYODs are personally owned, not assets of an organization. So, MIS does not control what runs on these devices, for example, antivirus software or unsafe applications. Two, IoT devices are hardware with a sensor 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 cartridge automatically. In a smart home, IoT devices regulate heat and humidity, remotely control the locks on doors, monitor what's in the fridge, and even help with your grocery list s.

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, and 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. This is similar to granting individuals access to sensitive information based on their need to know. For example, NAC would 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 NVR has no business communicating with a finance server. 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.

While NAC proved highly effective at managing numerous unprotected devices, it had shortcomings over its evolution. Some NAC solutions were designed to help with BYOD onboarding in wireless networks, but performed badly in the wired portion of the network. Other solutions were developed to work within a single vendor environment, but couldn't automatically profile third-party devices. Some had good visibility into small, simple networks, but didn't scale well into large, distributed networks.

Today, most NAC solutions have redressed these limitations. They have more complete visibility into the network and are better at categorizing devices automatically. They effectively perform in both Ethernet and wireless networks. Many NAC solutions have centralized architecture that improves managing devices across large and multisite networks. Critically, NAC must also be integrated into the security framework, so that when a breach is detected, NAC automatically notifies the security operations center (SOC) and coordinates with other security devices to neutralize the threat.

Fortinet offers a network access control solution, named FortiNAC™. It contains all of the features identified in this lesson.

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

Lesson 9—Sandbox

Hello! In this lesson, we will explain what a sandbox is, why it was invented, and how it has evolved.

A sandbox, within the computer security context, is a system that confines the actions of an application, such as opening a Word document or a browser, to an isolated virtual environment. Within this safe virtual environment, the sandbox studies the various application interactions to uncover any malicious intent. So 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 to compromise the device, and from there move through the network to infect other devices. Exploiting an unknown vulnerability is known as a zero-day attack. Before sandboxing, there was no effective means to stop a zero-day attack. Firewalls and antivirus software could stop known threats, but they were helpless against zero-day attacks.

A sandbox provided an isolated virtual environment that mimicked various computer devices, operating systems, and applications. It allowed potential threats to play out within the safety of these virtual systems. If the sandbox concluded that the suspicious file or activity was benign, no further action was needed. However, if it detected malicious intent, the file could be quarantined or the activity could be stopped on the real device.

Many of the early sandboxes failed to tightly integrate with other security devices within the network. While a sandbox might identify and defeat a zero-day attack, this vital threat intelligence was not always shared with the other network security devices in a timely fashion. However, the failure to communicate and coordinate had less to do with a defect of sandbox technology than a security architecture that was built upon point solutions. Point solutions, which could not be fully integrated into other vendors' products, meant that the security operations center (SOC) required a management console for each product. So, attempts to aggregate threat intelligence data was difficult and time consuming.

The second generation sandbox came about to correct the siloed, piecemeal approach. Sandboxes were equipped with more integration tools or partnered with other product vendors to improve integration. As a result, they could share threat intelligence with other security devices, such as firewalls, email gateways, endpoints, and other sandbox devices more effectively. The 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 to a threat intelligence service in the cloud, which could be pushed to other networks.

Today, threat actors are innovating automation and artificial intelligence (AI) techniques to accelerate the creation of new malware variants and exploits, and to discover security vulnerabilities more quickly,

with the goal of evading and overwhelming current defenses. To keep pace and accelerate detection of these new threats, it is imperative that AI-learning is added to the sandbox threat analysis process.

AI-driven attacks necessitated a third-generation sandbox based on a threat analysis standard. Also, it needed to cover the expanding attack surface of businesses due to the digital transformation. The digital transformation refers to the movement of business data, applications, and infrastructure to the cloud.

The challenge of standards-based threat analysis arose due to the struggle to interpret and understand cyber threat methods, which hampered effective responses. MITRE, a non-profit organization, proposed the ATT&CK framework that describes standard malware characteristics categorically. Many organizations embraced MITRE ATT&CK as a standard for threat analysis. So, it became necessary for security products to adopt the MITRE ATT&CK framework. It provided security devices with a common language in which to identify, describe, and categorize threats, which could be shared with and readily understood by other vendor devices.

Lastly, as more businesses adopt digital transformation, there are new organizations or parts of organizations exposed to attacks. One such example is the operational technology (OT) industry, which includes utilities, manufacturing, oil and gas, and many others. Traditionally, OT kept their operational networks internal and separate from their corporate business networks, but increasingly OT networks access corporate and third-party vendor networks. Another example is organizations that offer applications, platforms, and infrastructure as services in the public cloud—AWS and Azure to name a few. They host applications for other businesses, which are accessed through the Internet. These new areas require similar protection against zero-day threats to minimize business disruption and security risks. As a result, sandbox technology evolved to provide wider coverage to these areas and others as they develop.

Fortinet's sandbox product is named FortiSandbox™ and it embodies all of the latest technologies discussed here. It collaborates with other security products to promote a common defense that can be managed from a single pane of glass, which Fortinet calls the Security Fabric. The threat intelligence service provided by Fortinet is named FortiGuard® Labs.

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

Lesson 10—Security Information & Event Management

Hello! In this lesson, we will explain what security information and event management (SIEM) is, and how it has evolved over time.

Introduced in 2005, SIEM analyzes security alerts in real-time. Fundamentally, SIEMs do three things:

One: Collect, normalize, and store log events and alerts from the organization's network and security devices, servers, databases, applications, and endpoints in a secure, central location. SIEM collects information not only from physical devices, but also 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 of 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 appropriate level of investment, in reality, for many organizations, the primary driver for purchasing SIEM has been regulatory compliance.

The first two decades of the twenty-first century has seen a deluge of new compliance requirements, both legislative and industry sponsored. Some examples are the Payment Card Industry (PCI) standard, the Sarbanes-Oxley Act of 2002, the Health Insurance Portability and Accountability Act (HIPAA), and the General Data Protection Regulation (GDPR) in 2018. Businesses, hospitals, and other organizations ignore compliance at their peril, and violators can incur punitive fines.

As cyberattacks became more sophisticated and stealthy, demands for information about a cyberattack—its characteristics, purpose, and the extent of network penetration—grew more urgent. Another alarming fact was that 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 internal security. IT security needed a holistic picture of network activity, and the real-time data collected by SIEM filled this need. In the second stage of development, 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 SIEM's tool set, and is particularly needed when sifting through big data.

Another issue that hindered SIEM's greater acceptance 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 a high-level of skill on the part of the user to know what they were looking for. For all its capabilities, SIEM was not a set it and forget it technology. This situation was exacerbated

by two other facts. 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.

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.

Lesson 11—Web Application Firewall

Hello! In this lesson, we will talk about Web application firewalls (WAFs) and how they have evolved over time. What is a WAF and how does it differ from the traditional edge firewall?

A WAF is an appliance or software that monitors HTTP/HTTPS traffic and can block malicious traffic to and from a web application. It differs from a traditional edge firewall in that it targets the content from specific web applications and at the application level, while edge firewalls fashion secure gateways between the local area network and outside servers at the network level. Specifically, by inspecting HTTP traffic, a WAF can stop attacks originating from web application security flaws, such as SQL injection, cross-site scripting, file inclusion, and security misconfigurations. Given that much of our time, both at work and at home, is spent interfacing with web applications and web servers, the WAF becomes a vital component in our arsenal against bad actors and their malicious online schemes.

The ancestor of the WAF is the application firewall that was first 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 very 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 victim to espionage, theft, and other crimes, developing a defense against HTTP-based cyberattacks became a foremost priority. WAF couldn't rely on traditional edge firewall methods that based decisions on a blocklist of network addresses, and blocked certain protocols and port numbers. As all web applications used HTTP and either port 80 or 443, this approach wasn't very useful.

Let's look at a common attack method called SQL injection. Imagine you run an online business and customers and partners log onto your site to buy products and services. A typical login page asks for a user ID and password. An individual, let's call him John Smith, types his user ID—jsmith—and his password. This information is verified on a backend database. If the password is true, John Smith gets in, but if the password is false, he does not. Now, a bad actor probably doesn't know John's password. He could always guess, but that might take a very long time. Instead, for the password, the bad actor types "abc123 or 2+2=4". When John's credentials are sent back to the database for verification, it is likely that the password "abc123" is false; however, the expression 2+2=4 is true. Due to this flaw, the bad actor was able to break in to some sites. The first generation of WAFs used blocklists and signature-based HTTP attributes to alert the firewall of an attack, so a SQL injection attack, like this, was no longer successful.

With internet popularity soaring, soon the sheer number of web applications and their growing complexity made the signature-based approach obsolete. As well, the number of false positives—alerts of attacks that were in fact legitimate connections—grew to proportions beyond the capacity of IT security teams. In the next generation, WAFs became more intelligent—there was an element of learning by the firewall. The WAF would learn the behavior of the application to create a baseline it could use to evaluate whether attempts to access the applications were normal or irregular, and

therefore suspect. It also introduced session monitoring and heuristics, which permitted the firewall to detect variants of known signatures. This was a step forward, but because application learning was overseen by IT security, defence could not keep up with the ever-expanding number of mutations of existing methods or new exploits. Moreover, there was no defence against zero-day exploits, which exploited an unknown weakness in the code of an application.

The logical turn in WAF development was machine-learning unencumbered by human supervision. Now behaviour analysis could be done at machine speed and could adapt to the ever changing attributes of the threat. Other security features were augmented to the firewall. Among these assets were distributed denial of service (DDoS) defense, IP reputation, antivirus, and data loss prevention (DLP). The firewall could stop any action that violated acceptable HTTP behavior. It could identify the user and correlate the action they were attempting to do with their permissions, and stop any action that went beyond the scope of their role. The WAF was also designed to share information and collaborate with other security devices in the network, such as other firewalls and sandboxes. This served to integrate the firewall into an interlocking collective defence as opposed to working independently. And sandboxing allowed suspicious material to 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, these new discoveries could be uploaded to a threat intelligence center on the internet, where they could be communicated to other networks.

Fortinet has a WAF named FortiWeb™. FortiWeb™ can be integrated with FortiGate® and FortiSandbox™. FortiGuard® Labs is Fortinet's threat intelligence center, which can provide vital updates to FortiWeb™ and to other Fortinet Security Fabric products.

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

Lesson 12—Secure Email Gateway

Hello! In this lesson, we will explain what secure email gateway is and how it has evolved.

Email was one of the first activities people did when the world went online in the 1990s. It took very little bandwidth because technology allowed for very little. It was also easy, fast, and didn't even cost a postage stamp! It was so easy and inexpensive that it became a means to get a message to many people at little or no cost.

Some of those mass mailings came from legitimate businesses and were equivalent to advertising flyers sent by post, but other mass mailings were sent by more nefarious characters. This was the beginning of spam—the act of sending irrelevant and unsolicited messages on the internet to a large number of recipients.

Individuals could send and receive messages with little verification or accountability. Therefore, they offered anonymity. Initially, people viewed spam more as a nuisance than a threat. But in 1996, America Online (AOL) coined the term phishing to describe the fraudulent practice of sending emails purporting to be from a reputable source, in order to induce individuals to reveal personal information.

For example, some of you may have met Prince Solomon of Abadodo, or another wily character, who wanted to share their wealth with you. Other bad actors registered domain names that were strikingly close to the names of legitimate businesses or organizations and masqueraded as that business in an email, coaxing you to click a link or an attachment that contained malware.

The phishing technique relied on human naivety, carelessness, or distraction for it to work. One of the first responses from businesses was to educate employees about phishing tactics. However, while education may have reduced phishing exploits, it did not eliminate the threat. Something had to be done at the mail server and Internet Service Provider (ISP) levels. In response, businesses installed spam filters on mail servers to stop spam and phishing emails.

Spam filters rely on identifying specific words or patterns in the headers or bodies of messages. To use a simple example, the word cash is common to email spam. If an IT professional added the word cash to the spam filter on their company mail server, the filter would eliminate any email that contained that word.

ISPs also deployed spam filters. In addition to filtering, ISPs turned to strengthening authentication methods. By the end of the first decade of the twenty-first century, ISPs began to implement Sender Policy Framework (SPF), which slowly took shape during that decade but wasn't proposed as a standard until 2014.

SPF is an email authentication method that detects bogus sender addresses and emails.

However, for every defensive measure implemented by legitimate businesses, organizations, and ISPs, the bad actors introduced a countermeasure that circumvented the latest defense.

To return to our simple example, spammers could easily bypass our filtered word, cash, by rendering it as c@sh or some other variant. And while filters became more sophisticated in detecting spam patterns, they were too static and easy to outsmart.

Spamming and phishing are just too lucrative for the bad actors to easily give up. In fact, the number of phishing attacks has grown enormously since the turn of the century. In 2004, 176 unique phishing attacks were recorded. By 2012, this number grew to 28,000. And no wonder; phishing was lucrative. Between lost money and damages, the attacks caused a $500 million loss to businesses and individuals. More recently, during the first quarter of 2020, the Anti-Phishing Working Group (APWG) recorded 165,772 detected phishing sites.

Better defense was needed. Secure email gateways (SEG s) arose to provide more rigorous defense. In addition to the spam filter, SEGs added antivirus scanners, threat emulation, and sandboxing to detect malicious attachments and links in real time. Even if employee education and the spam filter failed, one of these other tools could detect and neutralize the threat. However, the number of false positives, and the sheer volume of attacks, overwhelmed the security teams, who became bogged down in manual remediation.

SEGs continue to evolve as threats evolve.

Today, greater automation and machine learning is built in to SEGs, which alleviates the demands placed on security operations centers (SOCs). Data loss prevention (DLP) is also available to detect and stop the egress of sensitive data.

In some cases, a SEG is integrated with other network security devices, such as edge and segmentation firewalls. These devices collectively form an integrated fabric of security that security professionals can centrally manage from a single pane of glass, and continually update using threat intelligence, as new methods and contagions become known.

Fortinet has a SEG, called FortiMail®. FortiMail® includes all of the features discussed here, plus it integrates with firewalls and sandboxing solutions. You can centrally manage all of these devices using FortiManager®, and update their threat intelligence using FortiGuard® Labs, which is the global threat intelligence and research center at Fortinet.

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

Lesson 13—Web Filter

Hello! In this lesson, we will look at web filtering and the development of this technology.

During the early days of the Internet there were little to no restrictions on what websites you could visit. Unfortunately, some of those sites had malware that could infect the browsing computer. Or, sometimes a website contained content that others objected to. What constitutes objectionable content can be controversial, but these two reasons—security and objectionable content—formed the impetus for the development of web filtering technology.

So, what is a web filter? It's an application that examines incoming webpages to determine if some or all of the content should be blocked. The web filter makes these decisions based on rules set in place by the organization, or individual, who installed the application. There is a corresponding interface that allows you to configure the rules, and determine what gets blocked and what gets through. A web filter can also establish different rules for different types of users. For example, at home a parent may want to enforce stricter rules for children, than for adolescents and adults.

In the United States, libraries were the first to install web filters on their publicly accessible computers in response to community pressure. The federal government passed the Children's Internet Protection Act (CIPA) in 2004 requiring all computers in a public library to have web filters, if that library accepted federal funds for computers that access the Internet. These measures were met with a mixed reception. As web filtering spread from libraries to schools, some argued that censoring information, no matter how offensive, countered the mission of libraries and education. What's more, sometimes the filters were not sophisticated enough to distinguish between art and a lewd photograph, or the filters blocked literature because of an expletive. These legitimate complaints about the limitations of the technology prompted the developers of these applications to design more sophisticated filtering techniques, and to make filter configuration more granular.

While the initial motivation was to protect children, after the technology was developed, its utility for other purposes became apparent. Information could be censored for religious, political, or ideological purposes. In addition, previous misdeeds of a government could be erased from the digital record. Still, on the other side of the ledger, browsing was made safer by developing filters that could block adware, spam, viruses, and spyware. Today, web filtering forms the first line of defense against web-based attacks. In addition to client workstations, web servers, and ISPs, web filters were added to other network devices, such as firewalls, proxy servers, sandbox technology, and wireless access points.

How does a web filter work? A web filter can consult a URL database that lists websites and domains that are known to host malware, phishing, and other harmful tools. With over a billion active websites on the Internet, this can be an onerous task. The URLs found on this naughty list are also known as a deny list. There can also be a allow list, which is a sanctioned list of URLs. Another method that can be used is a filter that looks for a keyword or predefined content. As noted earlier, the problem with this method is the number of false positives; that is, it can inadvertently block legitimate content, such as art. Machine learning may, in time, overcome this deficiency. Other types of web filters, such as the Google search engine, use machine learning to help you find what you are looking for. Like other network security devices, machine learning is the next step in building more effective web filters.

Fortinet has integrated web filters into a number of its products: for example, FortiClient®, FortiGate®, and for wireless access points, FortiAP™.

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

Lesson 14—SASE

Hello! In this lesson, we will introduce you to Secure Access Service Edge SASE, and explain how it has evolved.

SASE is a technology that combines 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.

Network security is a top priority for most organizations, however new challenges have emerged. Rapid and disruptive digital innovation has brought on:

- an Expanding thin edge defined by small branch locations that are attached to the core network
- a Growing amount of off-network users accessing the central data center
- a Challenging user experience for off-network users
- an Expanding attack surface
- Multi-level compliance requirements, and
- Increasingly sophisticated cyber threats

As work environments have evolved, so too have user behavior and endpoint protection requirements. Users no longer access information from a dedicated station within a pre-defined network perimeter confined to a corporate office. Instead, users access information from a variety of locations, such as in the home, in the air, and from hotels. They also access that information from different devices, such as desktop workstations, laptops, tablets, and mobile devices. Adding to this network complexity is the rise of Bring-Your-Own-Device, where users access enterprise systems through personal devices that are not part of the enterprise infrastructure.

Organizations today require that their users have immediate, continuous secure access to network and cloud-based resources and data, including business-critical applications, 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.

Finding solutions that meet these requirements is challenging,

The reasons for this are clear.

While networks have evolved to support the workflows for remote endpoints and users, many outdated network security solutions remain inflexible and do not extend beyond the data center to cover the ever-expanding network perimeter and, therefore, the attack surface. With the advent of new thin edge networks, this challenge is exacerbated.

Secondly, these solutions to converged networking and security oversight require that all traffic, whether coming from thin edge locations or off-network users, runs through the core data center for inspection. This results in:

- High cost

- Complexity
- Elevated risk exposure
- Latency and a poor user experience when accessing multi-cloud-based applications and data

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.

A new scalable, elastic, and converged solution is required to achieve secure, reliable network access for users and endpoints. One which addresses the security of many hybrid organizations, defined by systems and users spread across the corporate, and remote network. That solution is SASE.

A SASE solution provides integrated networking and security capabilities, including:

- Peering, which allows network connection and traffic exchange directly across the internet without having to pay a third party.
- A Next-Generation Firewall NGFW or cloud-based Firewall-as-a-Service FWaaS , with security capabilities including Intrusion Prevention System IPS, Anti-Malware, SSL Inspection, and Sandbox,.
- A Secure Web Gateway to protect users and devices from online security threats by filtering malware and enforcing internet security and compliance policies.
- Zero Trust Network Access ZTNA, which 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.
- Data Loss Prevention DLP prevents end-users from moving key information outside the network. These systems inform content inspection of messaging and email applications operating over the network.
- Domain Name System DNS, which serves as the phone book of the internet and provides SASE with threat detection capabilities to analyze and assess risky domains.

These services deliver:

- Optimized paths for all users to all clouds to improve performance and agility
- Enterprise-grade certified security for mobile workforces,
- Consistent security for all edges, and
- Consolidated management of security and network operations

Although classified as cloud-based, there are common SASE use cases, which may require a combination of physical and cloud-based solutions. For SASE to be effectively deployed in this scenario, secure connectivity with network access controls must be extended from the physical WAN infrastructure to the cloud edge. For example, to roll out access to SASE at branch offices, you may see SASE reliant on physical networking appliances, such as wireless (LTE and 5G), and wired (Ethernet) extenders or Wi-Fi access points.

The goal of SASE is to support the dynamic, secure access needs of today's organizations. Proper SASE service allows organizations to extend enterprise-grade security and networking to the:

- Cloud edge, where remote, off-network users are accessing the network, and
- the Thin edge, such as small branch offices

Fortinet's cloud-based SASE solution is called FortiSASE™.

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