## LESSON: Firewalls

## Primer For this lesson and upcoming lessons, instructors are required to ensure the following activities are completed for each lesson

* Checking with the students to see if they have any questions or need further clarification from any subject from the last class “Network Attacks & Mitigations” and self study module.
* Review the “Lesson Opener” and “Real World Scenario” with the learners prior to starting the module.
* Throughout the module, you will find “Consider the Real World Scenario” slides. Review the questions found on these slides, tie the concepts back to the scenario discussed at the start of the lesson as well as content you are presenting, and encourage the learners to share their thoughts.
* For each lesson, you will find a “Pulse Check” slide which is the opportunity for instructors to open a poll to gather feedback from the learners. Leave the poll open for about 1 minute and after you close the poll, share the results with the learners. Encourage the learners to share their thoughts. This information will help the instructors as well as the learners better understand where they are with regard to the lesson.
* Labs are to be demonstrated live for each module. The demonstration of labs is the top priority for the lead instructor. While demonstrating each lab, encourage students to participate and explore.
* At the end of each lesson, it is important to take a few minutes to review the key concepts for the lesson, provide guidance on what the learners can do to prepare for the next lesson, and wrap up with Q&A.
* Instructors should manage breaks based on need, considering both timing and duration. You may take a break if you feel the students need it or if a particularly challenging topic has just been covered.

### Summary

In this lesson, learners will cover fundamental firewall concepts and their vital role in network security. Learners will learn about common misconceptions, core firewall principles, and categories (host-based vs. network-based). They'll explore hardware vs. software firewalls, commercial solutions, and the importance of firewall rules and their order. The lesson delves into AI integration, introduces pfSense, and explains the integration of network services within firewalls. It highlights network address translation (NAT), port forwarding, routing, logging, and monitoring. Purpose-specific firewalls and architectural considerations are discussed. The lesson concludes with next-generation firewalls (NGFWs) and their advanced features.

### Objectives

* Identify the firewall.
* Describe common misconceptions about firewalls.
* Explain the basic working principles of firewalls.
* Explain the different kinds of firewalls.
* List examples of commercial firewalls.
* Explain the concept of firewall rules.
* Explain fail open vs. fail close.
* Describe how AI can be implemented in firewalls.
* Define the pfSense firewall.
* Describe firewall integrated services.
* Explain the features of network management.
* Explain logging and monitoring features.
* List examples of purpose-specific firewalls.
* Describe the concept of architecture considerations.
* Define next-generation firewalls (NGFW).
* Describe deep packet inspection (DPI) technology.
* Explain the functionalities of NGFWs.

### Lesson Activities and Teaching Strategies

|  |  |  |
| --- | --- | --- |
| Estimated Time | Lesson Portion | Directions |
| 5 min | **Lesson Opener:**  Firewalls | * Introduce learners to the importance of firewalls in cybersecurity. |
| 5 min | **Real World Scenario:**  Firewalls | * Review the real world scenario challenge and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation. |
| 20 min | **Cyber Uncovered:**  Introduction to Firewalls | * Start the lesson with a brief overview of what firewalls are and their importance in network security. * Highlight the analogy between a firewall and a country's border control to enhance understanding. * Explain the core definition of a firewall, which is to filter and control traffic between networks and devices. * Mention the firewall's role in isolating devices, blocking unwanted traffic, and allowing legitimate traffic. * Address the common misconceptions about firewalls, including their confusion with routers, VPN servers, IPS/IDS, and anti-malware solutions. * Clarify the distinctions between these technologies and the specific role of firewalls. * Introduce the fundamental principles behind how firewalls work, including packet filtering, state inspection, and proxying. * Provide examples and explanations for each principle to help learners grasp the concepts. * Explain the key differences between stateful and stateless firewalls. * Illustrate the advantages of stateful firewalls in tracking and analyzing active connections. * Differentiate between host-based and network-based firewalls. * Discuss the use cases and scenarios in which each type is most effective. * Present the pros and cons of hardware and software firewalls. * Help learners understand when each type is most suitable in a network environment. * Introduce learners to common commercial firewall vendors like Check Point, Cisco ASA, Palo Alto, and pfSense. * Highlight the variety of features, services, and support plans offered by these vendors. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 20 min | **Cyber Uncovered:**  Structure and Configuration of Firewall Rules | * Introduce firewall rules and their role in controlling network traffic. * Explain the different actions associated with firewall rules, including Accept/Allow, Reject/Deny, and Drop/Block. * Highlight the importance of rule order and how it affects firewall configurations. * Discuss fail open and fail close settings and when each is appropriate. * Explore the integration of artificial intelligence (AI) in firewall management, covering adaptive threat detection and user behavior analytics. * Provide an introduction to pfSense as an open-source network firewall based on FreeBSD. * Detail the features and benefits of pfSense, such as VPN support, captive portal, and load balancing. * Walk learners through the initial setup of pfSense, configuring interfaces and accessing the WebConfigurator. * Teach learners how to configure firewall rules in pfSense, explaining the components of a rule. * Guide learners on using AI like ChatGPT to suggest firewall rules for specific use cases. * **Give learners a 5 min break** * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 10-15 min | **Break** | * Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break. |
| 20 min | **Lab:**  pfSense Rule Configuration | * Remind learners to use this lab to practice and apply the concepts they have learned throughout the day. * Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance. |
| 20 min | **Cyber Uncovered:**  Firewall Services & Features | * Start by introducing the concept of integrated services in modern firewalls, highlighting the reasons for integrating additional networking services. * Discuss the advantages of integrated services, such as improved security and reduced reliance on multiple vendor solutions. * Explore specific integrated services like DNS, DHCP, and VPN, emphasizing their roles in enhancing network control and security. * Explain the features that firewalls provide for network management, including network address translation (NAT), port forwarding, and routing capabilities. * Delve into network address translation (NAT) and how it conserves public IP addresses while adding a layer of security. * Describe port forwarding as a technique used to direct incoming traffic to specific internal IP addresses and ports, bypassing NAT for certain applications. * Cover routing in firewalls and how it helps determine the paths network packets take, ensuring efficient data flow and security. * Highlight the importance of logging and monitoring in firewalls, showing how these capabilities enhance security controls and provide real-time insights. * Discuss purpose-specific firewalls like proxy firewalls, web application firewalls (WAFs), unidirectional firewalls, and cloud firewalls, explaining their unique roles. * Conclude by addressing architectural considerations, such as determining the number and types of firewalls needed and their placement within the network architecture. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 20 min | **Lab:**  Setting-up Port Forwarding | * Remind learners to use this lab to practice and apply the concepts they have learned throughout the day. * Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance. |
| 5 min | **Pulse Check** | * After the poll is concluded, spend a few minutes asking why students have selected their zones. Encourage them to share with each other. |
| 10-15 min | **Break** | * Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break. |
| 20 min | **Cyber Uncovered:**  NGFW & DPI | * Begin by introducing the concept of next-generation firewalls (NGFWs) as advanced versions of traditional firewalls that integrate modern network traffic filtering functionalities. * Explain the key differences between NGFWs and traditional firewalls, emphasizing enhanced granular control and the ability to identify and block complex threats. * Describe deep packet inspection (DPI) and its role in analyzing data packets to identify, categorize, and manage traffic based on specific data or protocol patterns. * Highlight the distinction between DPI and basic packet filtering, focusing on how DPI examines data payloads for more precise control and threat detection. * Introduce the concept of application awareness and how NGFWs can identify and control traffic based on specific applications, enhancing security policies. * Explore the benefits of integrated security, explaining how NGFWs combine intrusion prevention systems (IPS/IDS) into the firewall to provide advanced threat protection. * Cover the importance of sandboxing in NGFWs and how it isolates and analyzes suspicious code or files in a controlled environment to neutralize potential threats. * Discuss SSL/TLS inspection in NGFWs and its ability to decrypt and inspect encrypted traffic for threats, ensuring security beyond just headers. * Conclude by explaining how NGFWs are equipped for botnet detection, utilizing signature-based analysis, behavioral analytics, and heuristics to identify and mitigate botnet-related traffic. * Summarize the advantages of NGFWs over traditional firewalls, emphasizing their capabilities in deep packet inspection, application awareness, integrated security, sandboxing, SSL/TLS inspection, and botnet detection. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 10-15 min | **Break** | * Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break. |
| 15 min | **Lesson Closure** | * For this first lesson, spend just a few minutes reminding the learners what the key ”take-aways'' were from the lesson and what they should do to prepare for the next module. The take-aways discussion should include key concepts such as Structure and Configuration of Firewall Rules, Firewall Services and Features, and NGFW and DPI * Students should review this information prior to moving to the next module. * Recommend that the students read-ahead and come prepared for the next lesson. * Q&A |

### 