## LESSON: Virtual Private Networks (VPN)

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

* Checking with the student to see if they have any questions or need further clarification from any subject from the last class “Network Traffic Analysis” 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 regards 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 develop an understanding of virtual private networks (VPNs) and remote access service (RAS). They will explore how VPNs establish secure and encrypted connections over potentially insecure networks, thereby protecting data from unauthorized access. They will also discover real-life applications of VPNs, from travelers securing public Wi-Fi connections to businesses connecting remote offices securely through VPN tunnels. The lesson covers essential VPN features, such as access to restricted content, user privacy, and various VPN protocols, emphasizing their security implications. Additionally, modern VPN deployment options, different modes of VPN use, and critical security considerations are discussed. The lesson also introduces RAS, elucidating its role as a substitute for VPNs on Windows servers, and outlines the steps involved in setting up RAS, from role installation to client configuration and testing, ensuring a comprehensive grasp of VPN and RAS concepts, including potential risks and security measures.

### Objectives

* Define virtual private networks (VPNs).
* Illustrate VPN applications.
* Describe VPN security features.
* Explain how VPNs work.
* Describe the tunneling and split tunneling processes.
* Identify the different types of VPN protocols.
* Explain how to set up and configure a VPN client.
* Identify and analyze the different VPN deployment options available.
* Describe VPN modes of use.
* Explain intranet-based and extranet-based VPN placement options.
* Identify the risks associated with VPNs in business and personal scenarios.
* Explain the security measures that must be considered for securing VPNs.
* Recognize the significance of monitoring and training in improving VPN security and user awareness.
* Define remote access service (RAS).
* Explain how to set up a RAS.

### Lesson Activities and Teaching Strategies

|  |  |  |
| --- | --- | --- |
| Estimated Time | Lesson Portion | Directions |
| 5 min | **Lesson Opener:**  Virtual Private Networks (VPN) | * Introduce learners to the importance of virtual private networks (VPN) in cybersecurity. |
| 5 min | **Real World Scenario:**  Virtual Private Networks (VPN) | * 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:**  Basic VPN Concepts | * Start by introducing the concept of virtual private networks (VPNs). * Explain that they create secure and encrypted connections over potentially insecure networks like the public internet. * Highlight the significance of using VPNs for data protection, shielding it from unauthorized access by hackers, government agencies, or other third parties, even if they can intercept it. * Present statistics from VPN providers to show that billions of users rely on VPNs for internet access, with around 30% using them for personal or business purposes. * Discuss practical examples of VPN use:   + Example A: A traveler needing to secure online banking on public Wi-Fi.   + Example B: A company establishing a secure site-to-site VPN between offices in different locations. * Emphasize how VPNs allow businesses to provide employees with secure access to corporate networks, regardless of their physical location. * Explain the concept of an encrypted tunnel and how it provides access to internal resources. * Describe how VPNs mask users' IP addresses, making their connections appear to originate from different locations and devices. * Explain how VPNs bypass geo-restrictions and enhance online anonymity. * 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:**  VPN Protocols | * Start by explaining the fundamental concept of a VPN, emphasizing its role in creating secure, encrypted connections over less secure networks. * Introduce the concept of "tunneling" in VPNs, drawing parallels between physical tunnels and network tunnels, and explain how tunneling enables data transmission across networks. * Describe the process of tunneling, highlighting its three main steps: Encapsulation, transmission, and decapsulation, and discuss the role of encryption in ensuring security. * Explain the concept of "split tunneling," where users can access multiple networks simultaneously through a VPN, contrasting it with routing all traffic through the VPN. * Introduce various VPN tunneling protocols, focusing on PPTP, L2TP, and IKEv2, and explain their characteristics and typical use cases. * Discuss VPN protocols with integrated security, specifically IPsec and SSTP, and how they enhance privacy and security. * Explore open-source VPN protocols like OpenVPN and WireGuard, emphasizing their community-driven nature and balance between security and performance. * Guide learners through the setup process for OpenVPN, including the installation of a VPN client and configuration using .ovpn files. * Cover the key parameters commonly found in VPN configuration files, such as remote server address, port number, protocol, encryption algorithm, authentication method, and certificate and key files. * 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 | **Cyber Uncovered:**  VPN Deployment Options | * Begin by explaining the diverse deployment methods for VPNs, emphasizing their suitability for different needs and use cases. * Discuss the concept of a hardware VPN, focusing on dedicated devices designed for handling VPN connections, both standalone and integrated into network hardware like routers and firewalls. * Highlight the benefits of hardware VPNs, including robustness, support for multiple simultaneous connections, and enhanced performance and security. * Present the drawbacks of hardware VPNs, including their cost, need for physical installation and maintenance, and lower flexibility compared to software solutions. * Transition to software VPNs, describing how they run on general-purpose operating systems and can be installed on various devices, servers, and routers. * Discuss the advantages of software VPNs, such as flexibility, ease of updating and patching, and the ability to deploy on existing hardware, making them suitable for businesses of all sizes. * Present the drawbacks of software VPNs, including concerns about security compared to dedicated hardware and potential performance impacts from other processes. * Move on to modern deployment options, explaining how new technologies have given rise to mobile VPNs and cloud VPNs to accommodate ever-changing network environments. * Detail mobile VPNs, highlighting their role in maintaining secure connections for mobile devices, both in changing network environments and their user-friendly nature, along with potential limitations in adapting to business needs. * Discuss cloud VPNs, explaining their cloud-based infrastructure, scalability, and the benefits of cloud providers handling maintenance, updates, and security. * Address potential drawbacks related to reliance on cloud providers and data sovereignty concerns. * Conclude by introducing VPN modes of use, distinguishing between remote access VPNs that enable individual users to connect to private networks and site-to-site VPNs, emphasizing their role in connecting geographically separated locations or networks. * Mention the security implications of intranet-based and extranet-based VPNs. * 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. |
| 18-20 min | **Lab:**  L2TP/IPSec 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. |
| 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:**  VPN Security Considerations | * Begin the lesson by introducing the primary focus of VPN risks in business use, highlighting the emphasis on security over privacy. * Explain that this section will address specific risks businesses might face when using VPNs. * Cover the first risk related to protocol vulnerabilities, explaining that even secure protocols like IPsec and OpenVPN have had vulnerabilities in the past and could potentially have more in the future. * Move on to unauthorized access, discussing how weak authentication methods or a culture of credential sharing within an organization can lead to unauthorized users gaining access to the VPN and internal network. * Explain the risk of misconfigured permissions, emphasizing that a VPN must be correctly configured and permissions should be regularly reviewed and updated to prevent unauthorized access to resources. * Discuss the risk of software vulnerabilities, focusing on how VPN client software, when not regularly updated, can have vulnerabilities that attackers might exploit. * Transition to the risks in personal use, pointing out that the main concerns are privacy related. Explain that this section will address risks that individuals might face when using VPNs for personal reasons. * Address the risk of logging and data retention by VPN providers, highlighting how user privacy can be compromised if these logs are accessed by third parties. * Explain the risk of DNS leaks, describing how even if a user's traffic is encrypted through a VPN, their DNS queries might still be sent to their ISP's DNS servers, potentially revealing the websites they visit. * Present the risk of exit node eavesdropping, clarifying that if the VPN server is compromised or set up by a malicious provider, it can eavesdrop on user traffic when decrypting and forwarding it to the final destination. * Move on to the section on security considerations, stressing that while specific risks vary, some security measures are common to most VPN use cases. * Discuss authentication, emphasizing the importance of robust authentication mechanisms, which could include strong password policies, digital certificates with mutual authentication, or multi-factor authentication (MFA) for connections. * Cover protocols, explaining the use of trusted protocols like L2TP combined with IPsec for enhanced security and the avoidance of outdated protocols with known vulnerabilities. * Explain access control measures, encouraging the setting up of access control lists (ACLs) to specify which IP addresses or ranges can access the network and the potential benefits of role-based access control (RBAC). * Discuss additional security measures, focusing on the importance of securing the infrastructure and devices connected to the VPN. * Address network configuration, emphasizing proper routing configurations, network segmentation for restricting access to sensitive areas, and the need for regular review and updating of firewall rules. * Discuss endpoint security, stressing the requirement for anti-malware and patch management solutions to protect against malicious software and ensure software is up-to-date and free from known vulnerabilities. Mention network access control (NAC) solutions for checking device security posture. * Conclude the lesson by discussing monitoring and training, clarifying the importance of accounting for residual risk. * Emphasize the need for logging and monitoring, suggesting the tracking of network activity and the use of intrusion detection systems (IDS) or security information and event management (SIEM) systems for advanced analysis and reporting. * Explain the importance of user training sessions, which should focus on the safe use of VPNs, secure device management, correct connection procedures, and the significance of regular updates and patches. * 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:**  Remote Access Service | * Start the lesson by explaining what remote access service (RAS) is, emphasizing that it's a collection of services and protocols enabling users to remotely access network resources as if they were directly connected to the network. * Introduce the concept that RAS is specifically available on Windows servers and allows administrators to set up a VPN server, manage user authentication, and define network rules. * Move on to the RAS setup flow, clarifying that while the complexity can vary, the general steps are as follows:   + Role Installation: Explain how to add the "Remote Access" role through the Server Manager, highlighting the availability of a setup wizard.   + Service Selection: Describe the need to choose the "Direct Access and VPN (RAS)" service for typical remote access functionality and routing.   + VPN Configuration: Cover the process of defining how the server handles incoming VPN connections, including network topology, interface selection, and authentication methods.   + Address Assignment & Routing Configuration: Explain the options for allocating IP addresses to connected clients, whether through DHCP or a static pool, and the importance of enabling and defining the server's routing capabilities.   + Security Setup: Describe the finalization of encryption, authentication settings, and the implementation of necessary firewall rules to allow VPN traffic, mentioning default traffic blocking.   + Client Configuration: Prepare to guide remote users in setting up their devices to connect to the VPN server.   + Testing: Highlight the significance of verifying the setup's functionality through remote VPN connection testing. * Address role installation in more detail, explaining the use of the "Add Roles and Features Wizard” in the Server Manager on Windows servers. * Mention that the setup wizard will guide users through the configuration options. * Discuss service selection, particularly after installing the "Remote Access" role. Explain that users will be prompted to choose a role service, emphasizing the need to select "DirectAccess and VPN (RAS)" and routing for typical remote access. * Cover VPN configuration, mentioning that Windows will run the "Getting Started Wizard" after installation. * Explain what the wizard covers, including selecting the tunneling protocol, specifying a network interface for incoming connections, and setting up authentication methods. * Address the important steps of address assignment and routing configuration, highlighting the choice between automatic IP address assignment through DHCP or setting up a static address pool for connected clients. * Move on to security setup, clarifying the necessity of choosing encryption methods, configuring user access, and implementing firewall rules to allow VPN traffic. * Conclude the lesson by discussing client configuration, explaining that client devices need to be configured to connect to the VPN. Highlight that Windows provides the ability to enter the server's address and authentication details directly from the system settings under networking. * 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. |
| 20-25 min | **Lab:**  L2TP/IPSec 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. |
| 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 VPN Protocols, VPN Deployment Options, VPN Security Considerations, and Remote Access Service. * 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 |

### 