Chapter 5

5.1.7

You are an IT security administrator for a small corporate network. To increase security for the corporate network, you have installed the pfSense network security appliance in your network. Now you need to configure the device.

In this lab, your task is to configure pfSense as follows:

* Sign in to pfSense using the following case-sensitive information:
  + URL: **198.28.56.18**
  + Username: **admin**
  + Password: **pfsense**
* Configure the DNS servers as follows:
  + Primary DNS server: **163.128.78.93** - Hostname: **DNS1**
  + Secondary DNS server: **163.128.80.93** - Hostname: **DNS2**
* Configure the WAN IPv4 information as follows:
  + Enable the interface.
  + Use a static IPv4 address of **65.86.24.136/8**
  + Add a new gateway using the following information:
    - Type: **Default gateway**
    - Name: **WANGateway**
    - IP address: **65.86.1.1**

KEY:

1. Access the pfSense management console.
   1. From the taskbar, select **Google Chrome**.
   2. Maximize the window for better viewing.
   3. In the address bar, type **198.28.56.18** and then press **Enter**.
   4. Sign in using the following case-sensitive information:
      * Username: **admin**
      * Password: **pfsense**
   5. Select **SIGN IN** or press **Enter**.
2. Configure the DNS Servers.
   1. From the pfSense menu bar, select **System** > **General Setup**.
   2. Under *DNS Server Settings*, configure the primary DNS Server as follows:
      * Address: **163.128.78.93**
      * Hostname: **DNS1**
      * Gateway: **None**
   3. Select **Add DNS Server** to add a secondary DNS Server and then configure it as follows:
      * Address: **163.128.80.93**
      * Hostname: **DNS2**
      * Gateway: **None**
   4. Scroll to the bottom and select **Save**.
3. Configure the WAN settings.
   1. From pfSense menu bar, select **Interfaces** > **WAN**.
   2. Under General Configuration, select **Enable interface**.
   3. Use the *IPv4 Configuration Type* drop-down to select **Static IPv4**.
   4. Under Static IPv4 Configuration, in the IPv4 Address field, enter **65.86.24.136**.
   5. Use the IPv4 Address subnet drop-down to select **8**.
   6. Under Static IPv4 Configuration, select **Add a new gateway**.
   7. Configure the gateway settings as follows:
      * Default: Select **Default gateway**
      * Gateway name: Enter **WANGateway**
      * Gateway IPv4: **65.86.1.1**
   8. Select **Add**.
   9. Scroll to the bottom and select **Save**.
   10. Select **Apply Changes**.

5.1.8

You work as the IT security administrator for a small corporate network. You need to secure access to your pfSense appliance, which is still configured with the default user settings.

In this lab, your task is to:

* Change the password for the default pfSense account from pfsense to **P@ssw0rd (use a zero).**
* Create a new administrative user with the following parameters:
  + Username: **zolsen**
  + Password: **St@yout!**
  + Full Name: **Zoey Olsen**
  + Group Membership: **admins**
* Set a session timeout of **15** minutes for pfSense.
* Disable the webConfigurator anti-lockout rule for HTTP.

KEY:

1. Access the pfSense management console.
   1. From the taskbar, select **Google Chrome**.
   2. Maximize the window for better viewing.
   3. In the Google Chrome address bar, enter **198.28.56.18** and then press **Enter**.
   4. Enter the pfSense sign-in information as follows:
      * Username: **admin**
      * Password: **pfsense**
   5. Select **SIGN IN**.
2. Change the password for the default (admin) account.
   1. From the pfSense menu bar, select **System > User Manager**.
   2. For the admin account, under Actions, select the ***Edit user*** icon (pencil).
   3. For the Password field, change to **P@ssw0rd** (use a zero).
   4. For the Confirm Password field, enter **P@ssw0rd**.
   5. Scroll to the bottom and select **Save**.
3. Create and configure a new pfSense user.
   1. Select **Add**.
   2. For Username, enter **zolsen**.
   3. For the Password field, enter **St@yout!**.
   4. For the Confirm Password field, enter **St@yout!**
   5. For Full Name, enter **Zoey Olsen**.
   6. For Group Membership, select **admins** and then select **Move to Member of list**.
   7. Scroll to the bottom and select **Save**.
4. Set a session timeout for pfSense.
   1. Under the *System* breadcrumb, select **Settings**.
   2. For Session timeout, enter **15**.
   3. Select **Save**.
5. Disable the webConfigurator anti-lockout rule for HTTP.
   1. From the pfSense menu bar, select **System**>**Advanced**.
   2. Under webConfigurator, for Protocol, select **HTTP**.
   3. Select **Anti-lockout**to disable the webConfigurator anti-lockout rule.
   4. Scroll to the bottom and select **Save**.

5.1.10

You are the IT administrator for a small corporate network. Several employees have complained of slow internet bandwidth. You have discovered that the user stations on the guest Wi-Fi network are consuming much of your company's bandwidth. You have decided to use pfSense's Traffic Shaper wizard to create the various rules needed to better control the bandwidth usage and to fine-tune the priority for the type of traffic used on your guest Wi-Fi network.

Your network has one LAN and one WAN.

In this lab, your task is to:

* Access the pfSense management console:
  + Username: **admin**
  + Password: **P@ssw0rd** (zero)
* Create a firewall alias using the following specifications:
  + Name: **HighBW**
  + Description: **High bandwidth users**
  + Assign the IP addresses of the high-bandwidth users to the alias:
    - Vera's IP address: **172.14.1.25**
    - Paul's IP address: **172.14.1.100**
* The Shaper must be configured for the GuestWi-Fi interface using:
  + An upload bandwidth of **5** Mbits
  + A download bandwidth of **45** Mbits
* Allow your voice over IP traffic to have priority with:
  + An upload bandwidth of **15** Mbits
  + A download bandwidth of **20** Mbits
* To limit the user stations most likely to hog bandwidth, use the alias created earlier to penalize the offending stations to 2% of the bandwidth.
* Give a higher priority to the following services and protocols:
  + MSRDP
  + VNC
  + PPTP
  + IPSEC
* Change the port number used on the floating rule created for MSRDP as follows:
  + Interface: **GuestWi-Fi**
  + Destination Port Range: **3391**
* Answer the question.

KEY:

1. Sign into the pfSense management console.
   1. In the Username field, enter **admin**.
   2. In the Password field, enter **P@ssw0rd** (zero).
   3. Select **SIGN IN** or press **Enter**.
2. Create a high bandwidth usage alias.
   1. From the pfSense menu bar, select **Firewall** > **Aliases**.
   2. Select **Add**.
   3. Configure the Properties as follows:
      * Name: **HighBW**
      * Description: **High bandwidth users**
      * Type: **Host(s)**
   4. Add the IP addresses of the offending computers to the host(s) configuration:
      * Under Host(s), in the IP or FQDN field, enter **172.14.1.25**
      * Select **Add Host**.
      * In the new IP or FQDN field, enter **172.14.1.100**
   5. Select **Save**.
   6. Select **Apply Changes**.
3. Start the Traffic Shaper wizard for dedicated links.
   1. From the pfSense menu bar, select **Firewall** > **Traffic Shaper**.
   2. Under the Firewall bread crumb, select **Wizards**.
   3. Select **traffic\_shaper\_wizard\_dedicated.xml**.
   4. Under Traffic shaper Wizard, in the *Enter number of WAN type connections* field, enter **1** and then select **Next**.
4. Configure the Traffic Shaper.
   1. Make sure you are on Step 1 of 8.
   2. Using the drop-down menu for the upper Local interface, select **GuestWi-Fi**.
   3. Using the drop-down menu for lower Local interface, make sure **PRIQ** is selected.
   4. For the upper *Upload* field, enter **5**.
   5. Using the drop-down menu for the lower *Upload* field, select **Mbit/s**.
   6. For the top Download field, enter **45**.
   7. Using the drop-down menu for the lower Download field, select **Mbit/s**.
   8. Select **Next**.
5. Prioritize voice over IP traffic.
   1. Make sure you are on Step 2 of 8.
   2. Under Voice over IP, select **Enable** to prioritize the voice over IP traffic.
   3. Under Connection #1 parameters, in the Upload rate field, enter **15**.
   4. Using the drop-down menu for the top Units, select **Mbit/s**.
   5. For the Download rate, enter **20**.
   6. Using the drop-down menu for the bottom Units, select **Mbit/s**.
   7. Select **Next**.
6. Enable and configure a penalty box.
   1. Make sure you are on Step 3 of 8.
   2. Under Penalty Box, select **Enable** to enable the penalize IP or alias option.
   3. In the Address field, enter **HighBW**. This is the alias created earlier.
   4. For Bandwidth, enter **2**.
   5. Select **Next**.
7. Skip steps 4 and 5.
   1. For Step 4 of 8, scroll to the bottom and select **Next**.
   2. For Step 5 of 8, scroll to the bottom and select **Next**.
8. Raise and lower the applicable application's priority.
   1. Make sure you are on Step 6 of 8.
   2. Under *Raise or lower other Applications*, select **Enable** to enable other networking protocols.
   3. Under *Remote Service / Terminal emulation*, use the:
      * MSRDP drop-down menu to select **Higher priority**.
      * VNC drop-down menu to select **Higher priority**.
   4. Under VPN:
      * Use the PPTP drop-down menu to select **Higher priority**
      * Use the IPSEC drop-down menu to select **Higher priority**
   5. Scroll to the bottom and select **Next**.
   6. For step 7 of 8, select **Finish**.  
      Wait for the reload status to indicate that the rules have been created (look for Done).
9. View the floating rules created for the firewall.
   1. Select **Firewall** > **Rules**.
   2. Under the Firewall breadcrumb, select **Floating**.
   3. In the top right, select **Answer Questions**.
   4. Answer the question and then minimize the question dialog.
10. Change the port number used for the MSRDP outbound rule.
    1. For the *m\_Other MSRDP outbound* rule, select the ***edit*** icon (pencil).
    2. Under Edit Firewall Rule, in the *Interface* field, select **GuestWi-Fi**.
    3. Under Destination, use the Destination Port Range drop-down menu to select **Other**.
    4. In both Custom fields, enter **3391**.
    5. Select **Save**.
    6. Select **Apply Changes**.
    7. In the top right, select **Answer Questions**.
    8. Select **Score Lab**.

5.1.13

1. Where should an organization's web server be placed?
   1. DMZ
2. Which of the following is a privately controlled portion of a network that is accessible to some specific external entities?
   1. Extranet
3. You want to create a collection of computers on your network that appear to have valuable data but actually store fake data that could entice a potential intruder. Once the intruder connects, you want to be able to observe and gather information about the attacker's methods. Which feature should you implement?
   1. Honeynet
4. A honeypot is used for which purpose?
   1. To delay intruders in order to gather auditing data
5. Which of the following devices can apply quality of service and traffic-shaping rules based on what created the network traffic?
   1. Application-aware devices
6. You are the office manager of a small financial credit business. Your company handles personal financial information for clients seeking small loans over the internet. You are aware of your obligation to secure clients records, but the budget is an issue for your company.
   1. All-in-one security appliance
7. You are implementing security at a local high school that is concerned with students accessing inappropriate material on the internet from the library's computers. The students use the computers to search the internet for research paper content. The school budget is limited.
   1. Restrict content based on content categories.
8. Which of the following BEST describes a honeyfile?
   1. A single file setup to entice and trap attackers.
9. You are concerned that these computers could pick up viruses that could spread to your private network. You would like to implement a solution that prevents the laptops from connecting to your network unless antivirus software and the latest operating system patches are installed.
   1. NAC
10. A proxy server can be configured to do which of the following?
    1. Restrict users on the inside of a network from getting out to the internet.