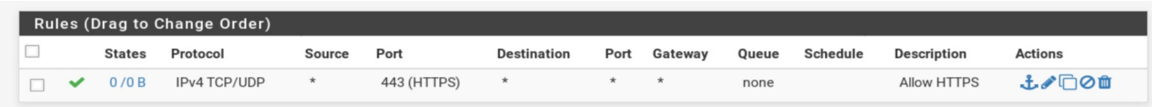
Test Answers - Omer Libich - Project CySA

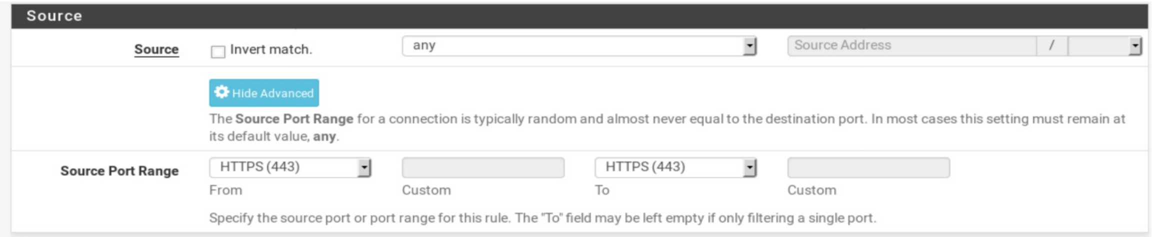
1. What rule should be implemented in order to allow HTTPS traffic?



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	0 /0 B	IPv4 TCP/UDP	*	443 (HTTPS)	*	*	*	none		Allow HTTPS	

In pfSense, to allow HTTPS traffic it is important to open the advanced options under source when creating the rule to be able to specify the source port range:



Source

Source □ Invert match. any Source Address /

Hide Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Source Port Range: From: HTTPS (443) Custom: To: HTTPS (443) Custom:

Specify the source port or port range for this rule. The "To" field may be left empty if only filtering a single port.

By selecting source port range 443 we are allowing HTTPS traffic or HTTP over TLS/SSL.

2. Which Linux OS is PFSense based on?

pfSense is an open source firewall/router computer software distribution based on FreeBSD. It is installed on a physical computer or a virtual machine to make a dedicated firewall/router for a network.

3. Is it important to change the default admin password? What is the default admin password?

Yes! It is extremely important to change the default admin password. Without changing the default admin password anyone with the internal IP address can acces the firewall and change any settings. The default admin password is "pfsense"

4. How do you setup remote connection to the WebGUI and in what situation is this useful?

The remote connection is established by assigning an IP address to the LAN interface of pfSense. Once the IP address is specified, access is permited from an adjacent VM or node (in the same VLAN) to modify settings. This is especially useful for modifying settings in a user-friendly GUI (graphic user interface) and to be able to access settings that are otherwise either inaccessible, or not readily apparent how to access/modify them.

In order to setup remote connection the following steps are required:

-choose option 2 in pfSense "2) Set interface(s) IP address"

-choose the LAN interface (option 2)

-specify IP address (i.e. 192.168.xx.xx)

-enter the new LAN IPv4 subnet bit count ("24" for class 'C' [255.255.255.0])

-enter the new LAN IPv4 upstream gateway address (<ENTER> for none)

-enter the new LAN IPv6 address (<ENTER> for none)

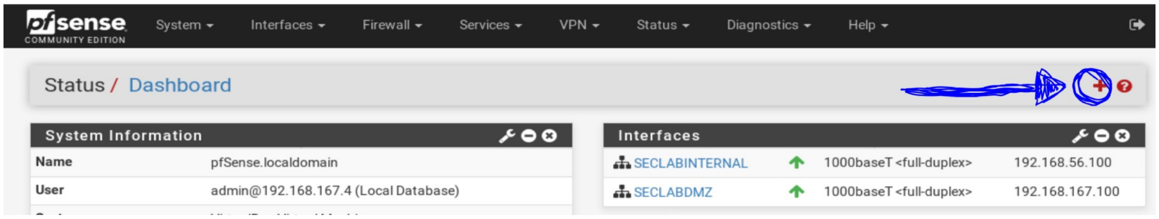
-do you want to enable DHCP server on LAN? (y/n) "n"

-do you want to rever to HTTP as the webconfigurator protocol? (y/n) "n"

You will then receive a message notifying you of the IP address to access the webConfigurator in a web browser window. Press <ENTER> to continue.

5. How do you monitor network traffic?

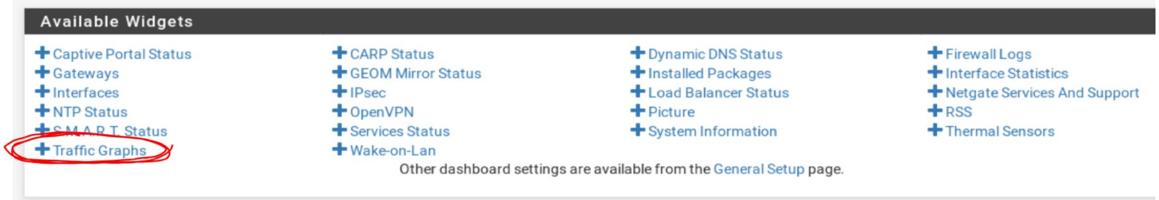
pfSense has a built in widget to monitor network traffic available on the dashboard. To enable it click on the "+" shown in the photo:



Name	pfSense.localdomain
User	admin@192.168.167.4 (Local Database)

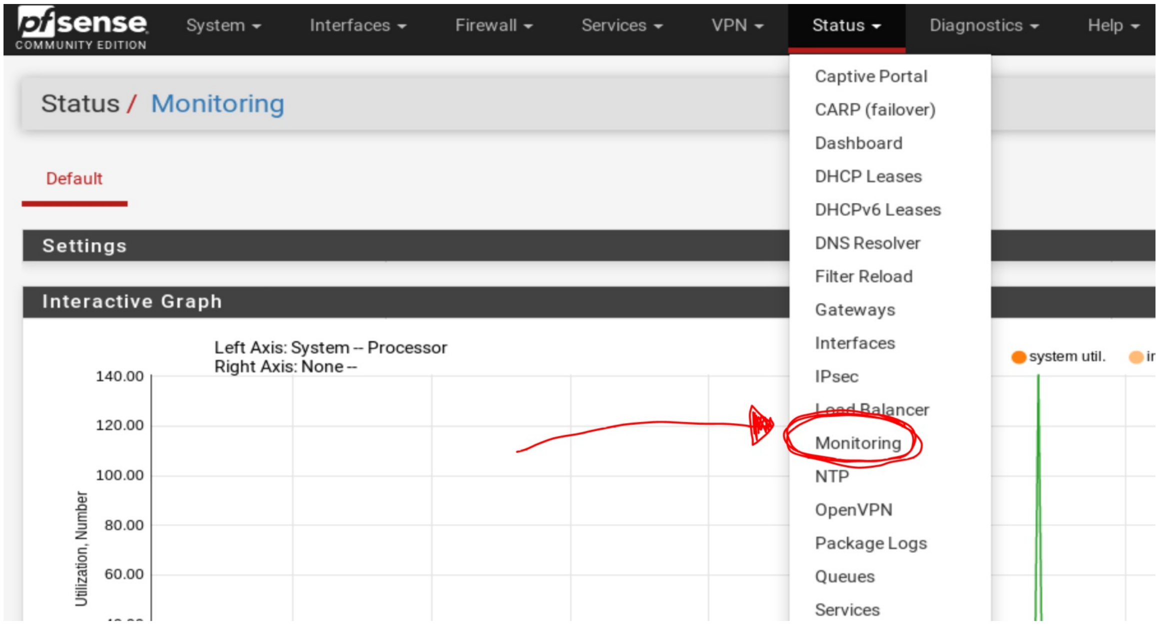
SECLABINTERNAL	↑	1000baseT <full-duplex>	192.168.56.100
SECLABDMZ	↑	1000baseT <full-duplex>	192.168.167.100

Select the "Traffic Graphs" widget to add it to your dashboard:



Other dashboard settings are available from the General Setup page.

Alternatively, one can also access the Monitoring function under the Status menu:



These are two useful ways to monitor network traffic.

6. How do you block inappropriate websites?

A popular tool to filter web content deemed "inappropriate" is to use a package that runs on top of pfSense named "Squid" then a secondary package that is a URL filter named "squidGuard" then add the blacklist from the provided source or choose your own.

I recommend setting a default "deny" setting and then whitelist as necessary.

An excellent instructional video can be found at this URL: https://www.youtube.com/watch?v=mkXzZDZd5Aw

7. Can you implement an IDS or IPS feature?

pfSense software can act in an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) role with add-on packages like Snort and Suricata. The Snort and Suricata packages share many design similarities, so in most cases the instructions for Snort carry over to Suricata with only minor adjustments.

Source: https://docs.netgate.com/pfsense/en/latest/ids-ips/index.html

8. What are the differences between the different VPN options?

Each VPN solution in pfSense (IPsec and OpenVPN) has pros and cons.

Interoperability

To interoperate with a firewall or router product from another vendor, IPsec is usually the best choice since it is included with nearly every VPN-capable device. It also prevents being locked into any particular firewall or VPN solution. For interoperable site-to-site connectivity, IPsec is usually the only choice. OpenVPN is interoperable with a few other packaged firewall/VPN solutions, but not many. Interoperability in this sense isn't applicable with other VPN types since they are not intended for site-to-site applications.

Authentication considerations

In current versions of pfSense software, all VPN types support user authentication. IPsec and OpenVPN can also work with shared keys or certificates. OpenVPN is a bit more flexible in this regard because it can work with only certificates, only shared keys, only user authentication, or a combination of these. Using OpenVPN with certificates, TLS authentication, and User Authentication is the most secure method. OpenVPN certificates can also be password protected, in which case a compromised certificate alone isn't adequate for connecting to a VPN if it is set to only use certificates. The lack of additional authentication can be a security risk in that a lost, stolen, or compromised system containing a key or certificate means whoever has access to the device can connect to a VPN until that loss is discovered and the certificate revoked.

Ease of configuration

None of the available VPN options are extremely difficult to configure, but there are differences between the options:

IPsec has numerous configuration options and can be difficult for the uninitiated.

OpenVPN requires the use of certificates for remote access in most environments, which comes with its own learning curve and can be a bit arduous to manage. pfSense includes a wizard to handle the most common OpenVPN remote access configurations and the OpenVPN client export packages eases the process of getting the clients up and running.

Client availability

VPN Client software is a program that handles connecting to the VPN and handling any other related tasks like authentication, encrypting, routing, etc. For remote access VPNs, the availability of VPN client software is a primary consideration. All options are cross platform compatible with many different operating systems but some require installing third-party clients. IPsec in EAP-MSCHAPv2 mode, IPsec in EAP-TLS mode, and IPsec in Xauth mode are the only options with client support built into some popular desktop and mobile operating systems. Other operating systems vary and may include more or less IPsec modes or may even include OpenVPN, as is the case with many Linux distributions.

IPsec

IPsec clients are available for Windows, Mac OS X, BSD, Linux, and others. Though the native clients may only support certain specific modes and configurations. General-use IPsec clients are not included in the OS except for some Linux and BSD distributions. A good free option for Windows is the Shrew Soft client. Mac OS X includes both IKEv2 and Cisco (xauth) IPsec support. There are free and commercial options available with a user-friendly GUI.

OSX 10.11, along with Windows 7 and later include support for IPsec in specific modes using IKEv2: EAP-TLS and EAP-MSCHAPv2. Both options are supported by pfSense and are covered in IPsec.

The Cisco-style IPsec client included with OS X and iOS devices is fully compatible with pfSense IPsec using xauth. Configuration for the iOS client is covered in iOS 9 IKEv2 Client Configuration.

Many Android phones also include a compatible IPsec client, which is referenced in Android strongSwan IKEv2 Client Configuration.

OpenVPN

OpenVPN has clients available for Windows, Mac OS X, all the BSDs, Linux, Solaris, and Windows Mobile, but the client does not come pre-installed in any of these operating systems.

Android 4.x and later devices can use a freely available OpenVPN client that works well and doesn't require rooting the device. That client is covered in Android Clients and Installation. Older versions of Android may also be able to use OpenVPN via an alternate client. There are other options available if the device is rooted, but that is beyond the scope of this book.

iOS also has a native OpenVPN client. For more information, see iOS Clients and Installation.

Firewall friendliness

VPN protocols can cause difficulties for many firewalls and NAT devices. This is primarily relevant to remote access connectivity, where users will be behind a myriad of firewalls mostly controlled by third parties with varying configurations and capabilities.

IPsec

IPsec uses both UDP port 500 and the ESP protocol to function. Some firewalls don't handle ESP traffic well where NAT is involved, because the protocol does not have port numbers like TCP and UDP that make it easily trackable by NAT devices. IPsec clients behind NAT may require NAT Traversal to function, which encapsulates the ESP traffic over UDP port 4500.

OpenVPN

OpenVPN is the most firewall-friendly of the VPN options. Since it uses TCP or UDP and is not affected by any common NAT functions such as rewriting of source ports, it is rare to find a firewall which will not work with OpenVPN. The only possible difficulty is if the protocol and port in use is blocked. Some administrators use a common port like UDP 53 (usually DNS), or TCP 80 (usually HTTP) or TCP 443 (usually HTTPS) or to evade most egress filtering.

Cryptographically secure

One of the critical functions of a VPN is to ensure the confidentiality of the data transmitted.

IPsec using pre-shared keys can be broken if a weak key is used. Use a strong key, at least 10 characters in length containing a mix of upper and lowercase letters, numbers and symbols. Use of certificates is preferred, though somewhat more complicated to implement.

OpenVPN encryption is compromised if the PKI or shared keys are disclosed, though the use of multiple factors such as TLS authentication on top of PKI can mitigate some of the danger.

9. Does rule placement order matter and why?

Firewall Rule Processing Order

Rules in pfSense software are processed in a specific order. Understanding this order is especially important when crafting more complicated sets of rules and when troubleshooting. It can be much more complicated, especially when floating rules are involved and out direction rules are used.

Short Version

Rules are always processed from the top of a list down, first match wins. The only exception to that is floating rules without quick set.

Rules defined on the floating tab are processed first

Rules defined on interface group tabs (Including IPsec and OpenVPN) are processed

Rules defined on interface tabs (WAN, LAN, OPTx, etc) are processed last

Longer Version

More accurately, the following order is found in the ruleset:

Outbound NAT rules

Inbound NAT rules such as Port Forwards (including rdr pass and UPnP)

NAT rules for the Load Balancing daemon (relayd)

Rules dynamically received from RADIUS for IPsec and OpenVPN clients

Internal automatic rules (pass and block for various items like lockout, snort, DHCP, etc.)

User-defined rules:

Rules defined on the floating tab

Rules defined on interface group tabs (Including IPsec and OpenVPN)

Rules defined on interface tabs (WAN, LAN, OPTx, etc)

Automatic VPN rules

Floating Rules notes

Floating rules without quick set process as “last match wins” instead of “first match wins”. Therefore, if a floating rule is set without quick and a packet matches that rule, then it also matches a later rule, the later rule will be used. This is the opposite of the other tab rules (groups, interfaces) and rules with quick set which stop processing as soon as a match is made.

10. Which logs would be useful in monitoring traffic on the firewall and why?

Firewall Logs

The Firewall logs are located through the pfSense webGUI at Status > System Logs on the Firewall tab. The logs show all events logged by the firewall. By default, this includes connections blocked by the default deny rule.

How to Read the Logs

Each entry is displayed with the action (triangle or "X", reject is only logged as block), time, interface, source, destination, and protocol.

The action icon depicts the action taken on the connection. "X" indicates a block action, (▶)indicates a pass action. Hover over the link for a text description if the meaning of the icon is not clear. Clicking on the action icon will produce a box that shows which rule caused the action. Using the Settings tab, these rule descriptions may also be shown in a separate column of the rules, or on a second line.

The info icon next to the source and destination addresses will attempt to reverse resolve the IP address into a hostname via DNS.

The minus-square icon next to the source address will add a full block for traffic coming from that IP address via Easy Rule. The plus-square icon next to the destination address also invokes Easy Rule, and will add a pass rule for traffic of this protocol, going from the source IP address to the destination IP address on the destination port.

If the logged entry is from a TCP connection, the TCP flags may also be displayed. For more information, see List of Routing Table Flags.

Firewall Log Dynamic View

The dynamic firewall log view works like the normal Firewall Logs view except it is updated every few seconds using AJAX.

Firewall Log Summary View

The firewall log summary view produces pie charts which summarize the log data. Each item is listed with a chart and a table containing the top five entries in the chart, and “other”.

Summarized data includes actions, interfaces, protocols, source IPs, destination IPs, source ports, and destination ports.

The full content of the log is used to summarize the data, not just the part displayed in the Firewall Logs view.