

Lab 01 – Configuring a VPN with pfSense

Name: Nicholas Leoncito

Course: IS 3423

Date: 9/15/2024

BREAKPOINT 1

ACCESSING THE PFSENSE WEB GUI:

I STARTED BY OPENING THE BROWSER AND NAVIGATING TO THE PFSENSE WEB GUI USING THE IP ADDRESS PROVIDED. AFTER THAT, I LOGGED IN USING THE ADMIN CREDENTIALS.

CONFIGURING THE CERTIFICATE AUTHORITY (CA):

I WENT TO SYSTEM > CERT. MANAGER AND CLICKED ADD TO CREATE A NEW CERTIFICATE AUTHORITY (CA). I FILLED IN THE REQUIRED DETAILS, INCLUDING THE DESCRIPTIVE NAME, KEY LENGTH, AND OTHER BASIC INFORMATION, THEN CLICKED SAVE. I TOOK A SCREEN CAPTURE OF THE UPDATED CERTIFICATE AUTHORITIES TABLE AS REQUIRED.

CREATING THE SERVER CERTIFICATE:

NEXT, I MOVED TO THE CERTIFICATES TAB WITHIN THE CERT. MANAGER. I CLICKED ADD TO CREATE A NEW SERVER CERTIFICATE. I PROVIDED A DESCRIPTIVE NAME, SELECTED THE APPROPRIATE KEY LENGTH, AND ENTERED THE COMMON NAME (IP ADDRESS). AFTER SAVING THE CERTIFICATE, I CAPTURED A SCREENSHOT OF THE UPDATED CERTIFICATES TABLE.

CONFIGURING THE IPSEC VPN:

I WENT TO VPN > IPSEC AND CLICKED ON THE MOBILE CLIENTS TAB. THERE, I ENABLED IPSEC MOBILE CLIENT SUPPORT. I CONFIGURED THE VIRTUAL ADDRESS POOL FOR THE VPN CLIENTS AND ENSURED ALL NECESSARY SETTINGS WERE APPLIED. AFTER SAVING AND APPLYING THE CHANGES, I CAPTURED A SCREENSHOT OF THE UPDATED IPSEC TUNNELS TABLE.

UPDATING IPSEC TUNNELS:

I CREATED THE PHASE 1 AND PHASE 2 DEFINITIONS FOR THE IPSEC TUNNEL. FOR PHASE 1, I SET THE ENCRYPTION ALGORITHMS, IP VERSION, AND AUTHENTICATION METHOD. FOR PHASE 2, I DEFINED THE NETWORK ROUTING AND ENCRYPTION SETTINGS. ONCE I SAVED AND APPLIED THESE CONFIGURATIONS, I TOOK A SCREEN CAPTURE OF THE UPDATED IPSEC TUNNELS TABLE.

ADDING THE PRE-SHARED KEY:

I THEN NAVIGATED TO THE PRE-SHARED KEYS TAB UNDER IPSEC AND CLICKED ADD TO CREATE A NEW PRE-SHARED KEY. I SET THE IDENTIFIER AND KEY (AS PROVIDED IN THE LAB), SAVED THE CHANGES, AND CAPTURED A SCREENSHOT OF THE UPDATED PRE-SHARED KEYS TABLE.

CONFIGURING IPSEC FIREWALL RULES:

FINALLY, I WENT TO FIREWALL > RULES > IPSEC AND ADDED A NEW RULE TO ALLOW VPN TRAFFIC THROUGH THE IPSEC INTERFACE. I SET THE RULE TO ALLOW ANY PROTOCOL AND SAVED THE CONFIGURATION. AFTER APPLYING THE CHANGES, I TOOK A SCREEN CAPTURE OF THE UPDATED IPSEC RULES TABLE.

CERTIFICATE AUTHORITIES TABLE

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
IPsecVPN_yourname	✓	self-signed	0	ST=California, OU=Network Security, O=UTSA, L=Santa Cruz, CN=internal-ca, C=US Valid From: Sun, 15 Sep 2024 20:30:19 +0000 Valid Until: Wed, 13 Sep 2034 20:30:19 +0000		

CERTIFICATES TABLE

System / Certificate Manager / Certificates					
CA's Certificates Certificate Revocation					
Search					
Search term <input type="text"/> Both <input type="button" value="Search"/> <input type="button" value="Clear"/>					
Enter a search string or *nix regular expression to search certificate names and distinguished names.					
Certificates	Name	Issuer	Distinguished Name	In Use	Actions
	webConfigurator default (59399e28df78d)	self-signed	emailAddress=admin@pfSense.localdomain, ST=State, O=pfSense webConfigurator Self-Signed Certificate, L=Locality, CN=pfSense-59399e28df78d, C=US		
	Server Certificate CA: No Server: Yes		Valid From: Thu, 08 Jun 2017 18:57:45 +0000 Valid Until: Tue, 29 Nov 2022 18:57:45 +0000		
	IKEv2VPN_pfSense Server Certificate CA: No Server: Yes	IPsecVPN_yourname	ST=California, OU=Network Security, O=UTSA, L=Santa Cruz, CN=202.20.1.1, C=US		
			Valid From: Sun, 15 Sep 2024 20:43:27 +0000 Valid Until: Wed, 13 Sep 2034 20:43:27 +0000		

IPSEC TUNNELS TABLE

UPDATED IPSEC TUNNELS TABLE

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

VPN / IPsec / Tunnels

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

The changes have been applied successfully.

IPsec Tunnels							
IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/>	Disable	V2	WAN Mobile Client	AES (128 bits)	SHA256	14 (2048 bit)	MobileIPsec
Show Phase 2 Entries (0)							

Add P1 Delete P1s

PRE-SHARED KEYS TABLE

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

VPN / IPsec / Pre-Shared Keys

The changes have been applied successfully.

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

Pre-Shared Keys			
Identifier	Type	Pre-Shared Key	Actions
remoteworker01	PSK	password1	

Add

IPSEC RULES TABLE

Firewall / Rules / IPsec

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor](#) the filter reload progress.

Floating WAN LAN DMZ IPsec

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	IPv4 *	*	*	*	*	*	none		IPsec Open	

Add Add Delete Save Separator

BREAKPOINT 2

CONFIGURING THE CERTIFICATE AUTHORITY (CA):

I STARTED BY GOING TO VPN > OPENVPN AND LAUNCHED THE OPENVPN WIZARD. AT THE CERTIFICATE AUTHORITY STEP, I CHOSE TO CREATE A NEW CA. I FILLED IN THE REQUIRED DETAILS, INCLUDING THE DESCRIPTIVE NAME, COUNTRY, STATE, AND ORGANIZATION. AFTER COMPLETING THE FORM, I SAVED THE CONFIGURATION AND CAPTURED A SCREENSHOT OF THE CA CONFIGURATION FORM.

SETTING UP THE CLIENT SETTINGS:

DURING THE OPENVPN WIZARD PROCESS, I PROCEEDED TO THE CLIENT SETTINGS SECTION. I SPECIFIED THE DOMAIN NAME FOR THE CLIENTS AND PROVIDED THE DNS SERVER. ONCE THESE SETTINGS WERE APPLIED, I TOOK A SCREEN CAPTURE OF THE CLIENT SETTINGS SECTION FOR THE LAB REPORT.

CONFIGURING THE TUNNEL SETTINGS:

IN THE TUNNEL SETTINGS SECTION, I DEFINED THE TUNNEL NETWORK, ASSIGNED A LOCAL NETWORK, AND ALLOWED INTER-CLIENT COMMUNICATION. I ALSO SET THE MAXIMUM NUMBER OF CONCURRENT CONNECTIONS AND UNCHECKED THE OPTION FOR REDIRECTING THE GATEWAY. AFTER SAVING THE CONFIGURATION, I CAPTURED A SCREENSHOT OF THE TUNNEL SETTINGS SECTION.

COMPLETING THE OPENVPN CONFIGURATION:

AFTER GOING THROUGH THE WIZARD STEPS, I REVIEWED AND FINALIZED THE OPENVPN SERVER SETUP. I ENSURED THE SETTINGS WERE CORRECT AND COMPLETED THE CONFIGURATION. I TOOK A SCREEN CAPTURE OF THE COMPLETED OPENVPN CONFIGURATION PAGE TO INCLUDE IN THE REPORT.

CONFIGURING THE FIREWALL RULE FOR OPENVPN ON THE WAN INTERFACE:

AFTER SETTING UP OPENVPN, I WENT TO FIREWALL > RULES > WAN TO VERIFY THAT THE APPROPRIATE FIREWALL RULE WAS CREATED. THE RULE ALLOWED OPENVPN TRAFFIC TO PASS THROUGH THE WAN INTERFACE. I TOOK A SCREEN CAPTURE OF THE OPENVPN RULE ON THE WAN RULES TABLE.

VERIFYING THE OPENVPN RULE IN THE OPENVPN RULES TABLE:

FINALLY, I NAVIGATED TO FIREWALL > RULES > OPENVPN TO ENSURE THE RULE ALLOWING OPENVPN TRAFFIC WAS CORRECTLY APPLIED ON THE OPENVPN INTERFACE. AFTER CONFIRMING THIS, I CAPTURED A SCREENSHOT OF THE OPENVPN RULE ON THE OPENVPN RULES TABLE.

CA CONFIGURATION FORM

Add Certificate Authority

OpenVPN Remote Access Server Setup Wizard

Create a New Certificate Authority (CA) Certificate

Descriptive name	CompanyVPN_CA_Nicholas	A name for administrative reference, to identify this certificate. This is the same as common-name field for other Certificates.
Key length	2048 bit	Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com
Lifetime	3650	Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)
Country Code	US	Two-letter ISO country code (e.g. US, AU, CA)
State or Province	California	Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).
City	Santa Cruz	City or other Locality name (e.g. Louisville, Indianapolis, Toronto).
Organization	UTSA	Organization name, often the Company or Group name.

CLIENT SETTINGS

TUNNEL SETTINGS

The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.

Hardware Crypto

No Hardware Crypto Acceleration

The hardware cryptographic accelerator to use for this VPN connection, if any.

Tunnel Settings

Tunnel Network

172.31.1.0/24

This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.

Redirect Gateway



Force all client generated traffic through the tunnel.

Local Network

172.30.0.0/24

This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

Concurrent Connections

2

Specify the maximum number of clients allowed to concurrently connect to this server.

Compression

Omit Preference (Use OpenVPN Default)

Compress tunnel packets using the LZ0 algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.

Type-of-Service



Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.

Inter-Client Communication



Allow communication between clients connected to this server.

Duplicate Connections



Allow multiple concurrent connections from clients using the same Common Name.

NOTE: This is not generally recommended, but may be needed for some scenarios.

COMPLETED OPENVPN CONFIGURATION

Client Settings

Dynamic IP	<input checked="" type="checkbox"/>	Allow connected clients to retain their connections if their IP address changes.
Topology	Subnet – One IP address per client in a common subnet	
Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".		
DNS Default Domain	securelabsondemand.com	
Provide a default domain name to clients.		
DNS Server 1	172.30.0.1	
DNS server IP to provide to connecting clients.		
DNS Server 2		
DNS server IP to provide to connecting clients.		
DNS Server 3		
DNS server IP to provide to connecting clients.		
DNS Server 4		
DNS server IP to provide to connecting clients.		
NTP Server		
Network Time Protocol server to provide to connecting clients.		
NTP Server 2		
Network Time Protocol server to provide to connecting clients.		
NetBIOS Options	<input type="checkbox"/> Enable NetBIOS over TCP/IP	

OPENVPN RULE ON THE WAN RULES TABLE

Firewall / Rules / OpenVPN

The screenshot shows a table with columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. There is one row selected, showing '0/0 B' in the Protocol column and 'none' in the Queue column. The Actions column contains icons for edit, delete, and save.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4*	*	*	*	*	*	none		OpenVPN OpenVPN Server wizard	

Rules (Drag to Change Order)

Add **Up** **Down** **Delete** **Save** **Separator**

OPENVPN RULE ON THE OPENVPN RULES TABLE

Wizard / OpenVPN Remote Access Server Setup / Finished!

Step 11 of 11

Finished!

OpenVPN Remote Access Server Setup Wizard

Configuration Complete!

The configuration is now complete.

To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Export package.

> Finish

BREAKPOINT 3

ENABLING THE MOBIKE OPTION IN PFSENSE:

I LOGGED INTO THE PFSENSE WEB GUI AND NAVIGATED TO VPN > IPSEC. FROM THERE, I SELECTED THE EXISTING IPSEC TUNNEL AND EDITED THE CONFIGURATION. UNDER THE PHASE 1 SETTINGS, I LOCATED THE MOBIKE (MOBILITY AND MULTIHOMING PROTOCOL) OPTION AND ENABLED IT. AFTER SAVING THE CONFIGURATION AND APPLYING THE CHANGES, I TOOK A SCREEN CAPTURE OF THE ENABLED MOBIKE OPTION IN THE IPSEC TUNNEL SETTINGS.

DISABLING AUTOMATIC IPSEC RULE CREATION:

NEXT, I WENT TO SYSTEM > ADVANCED > FIREWALL & NAT. IN THE IPSEC SECTION, I DISABLED THE OPTION FOR AUTOMATIC IPSEC RULE CREATION. THIS ALLOWED ME TO MANUALLY DEFINE THE NECESSARY FIREWALL RULES FOR IPSEC TRAFFIC. AFTER SAVING THESE CHANGES, I TOOK A SCREEN CAPTURE OF THE DISABLED AUTOMATIC IPSEC RULE CREATION OPTION FOR THE LAB REPORT.

CONFIGURING FIREWALL RULES TO PERMIT IPSEC TRAFFIC:

WITH AUTOMATIC RULE CREATION DISABLED, I NEEDED TO MANUALLY ADD THE APPROPRIATE FIREWALL RULES. I WENT TO FIREWALL > RULES > IPSEC AND CREATED THE FOLLOWING RULES:

ONE RULE FOR ESP PROTOCOL (ALLOWING TRAFFIC FOR IPSEC ENCAPSULATION).

ONE RULE FOR UDP PORT 500 (FOR IKE TRAFFIC).

ANOTHER RULE FOR UDP PORT 4500 (FOR IPSEC NAT-T).

AFTER ADDING THESE RULES AND APPLYING THE CHANGES, I TOOK A SCREEN CAPTURE OF THE FIREWALL RULES THAT PERMIT IPSEC TRAFFIC.

BY COMPLETING THESE STEPS, I ENSURED THAT THE IPSEC CONFIGURATION WAS PROPERLY SECURED AND ALL REQUIRED SCREENSHOTS WERE CAPTURED FOR THE LAB REPORT

ENABLE MOBIKE OPTION IN PFSENSE

Advanced Options	
Disable rekey	<input type="checkbox"/> Disables renegotiation when a connection is about to expire.
Margintime (Seconds)	<input type="text"/>
How long before connection expiry or keying-channel expiry should attempt to negotiate a replacement begin.	
Disable Reauth	<input type="checkbox"/> Whether rekeying of an IKE_SA should also reauthenticate the peer. In IKEv1, reauthentication is always done.
Responder Only	<input type="checkbox"/> Enable this option to never initiate this connection from this side, only respond to incoming requests.
Child SA Close Action	<input type="button" value="Default"/>
Set this option to control the behavior when the remote peer unexpectedly closes a child SA (P2)	
NAT Traversal	<input type="button" value="Auto"/>
Set this option to enable the use of NATT (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.	
MOBIKE	<input checked="" type="checkbox"/> Enable
Set this option to control the use of MOBIKE	
Split connections	<input type="checkbox"/> Enable this to split connection entries with multiple phase 2 configurations. Required for remote endpoints that support only a single traffic selector per child SA.
Dead Peer Detection	<input checked="" type="checkbox"/> Enable DPD
Delay	<input type="text" value="10"/>
Delay between requesting peer acknowledgement.	
Max failures	<input type="text" value="5"/>

DISABLES AUTOMATIC IPSEC RULE CREATION OPTION

Disable Auto-added VPN rules	<input checked="" type="checkbox"/> Disable all auto-added VPN rules. Note: This disables automatically added rules for IPsec.
Disable reply-to	<input type="checkbox"/> Disable reply-to on WAN rules With Multi-WAN it is generally desired to ensure traffic leaves the same interface it arrives on, hence reply-to is added automatically by default. When using bridging, this behavior must be disabled if the WAN gateway IP is different from the gateway IP of the hosts behind the bridged interface.
Disable Negate rules	<input type="checkbox"/> Disable Negate rule on policy routing rules With Multi-WAN it is generally desired to ensure traffic reaches directly connected networks and VPN networks when using policy routing. This can be disabled for special purposes but it requires manually creating rules for these networks.
Allow APIPA	<input type="checkbox"/> Allow APIPA traffic Normally this traffic is dropped by the firewall, as APIPA traffic cannot be routed, but some providers may utilize APIPA space for interconnect interfaces.
Aliases Hostnames Resolve Interval	<input type="text" value="300"/> Interval, in seconds, that will be used to resolve hostnames configured on aliases. Note: Leave this blank for the default (300s).
Check certificate of aliases URLs	<input type="checkbox"/> Verify HTTPS certificates when downloading alias URLs Make sure the certificate is valid for all HTTPS addresses on aliases. If it's not valid or is revoked, do not download it.
Bogon Networks	
Update Frequency	<input type="button" value="Monthly"/>
The frequency of updating the lists of IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA.	
Network Address Translation	

Conclusion

In conclusion, this lab provided a hands-on experience with setting up and configuring a VPN server using pfSense, allowing me to understand the process from creating certificates to configuring IPsec and OpenVPN tunnels. By enabling advanced features like MOBIKE and manually adjusting firewall rules, I gained valuable insight into securing VPN connections and ensuring remote access to network resources. Overall, the lab was a great opportunity to practice VPN configurations and further develop my network security skills.

References

Collaboration