howto, openvpn, pfsense, sitetosite, vpn, apu1c4, pcengines

simple site to site VPN with pfSense and OpenVPN

I just had to set up a simple site to site VPN between a site with a fixed IP (SITE-B) and a site with a dynamic IP (SITE-A). Both routers are running the 'Community Edition' of pfSense and are installed on PC Engines APU.1C4. I have followed the documentation at pfSense.org about how to configure a Site To Site VPN with OpenVPN to get the VPN up and running. Because some things aren't documented there I will put up my own HowTo here. Please do yourself a favour and read the documentation at pfSense.org first because it explains things in more detail than I will do here.



This HowTo will guide you trough the setup of:

- An IPv4 'Site To Site VPN' with OpenVPN on the pfSense platform (2.3.4 at time of writing) as seen in the schema above with the specific settings for the PC Engines APU hardware platform.
- The client will autoconnect to the server and (in the event of disconnection) reconnect automatically.
- The authentication between the client and the server will happen automatically via pre-shared key.

Sources

- pfsense.org OpenVPN Site To Site
- The pfSense Book

Configure the OpenVPN server on SITE-B router

• Navigate to 'VPN - OpenVPN'

COMMUNITY EDITION System	m • Interfaces • Firewall • Servic	es ≠ VPN ≠ Status ≠	Diagnostics + Gold +	- pfsense.site-b.inside - 🕒
VPN / OpenVPN	V / Servers			Lat 🚍 🛛
Servers Clients	Client Specific Overrides Wizards			
OpenVPN Servers Protocol / Port	Tunnel Network	Crypto	Description	Actions
				+ 444
	ofSense is © 2004 - 2017 by Rubicon C	Communications, LLC (Netrate), A	Il Richts Reserved. I view license	n

• On the 'Servers'-Tab click on the '+ Add'-button to add a new server

Servers Clients	Client Specific Overrides Wizards			
Opporal Information				
Disabled	Disable this server			
	Set this option to disable this server without removing it from the list.			
Server mode	Pear to Pear (Shared Key)			
Protocol	UDP *			
Device mode	tus v			
Interface	WAN *			
Local port	1194			
Description	Site_To_She-SITE-A_SITE_8			
	A description may be entered here for administrative reference (not parsed).			
Cryptographic Settin	gs			
Shared key	Automatically generate a shared key			
Encryption Algorithm	AES-256-CBC (256 bit key, 128 bit block)			
Auth digest algorithm	RSA-GHA512 (512-bit) •			
	Leave this set to SHA1 unless all clients are set to match. SHA1 is the default for OpenVPN.			
Hardware Crypto	No Hardware Crypto Acceleration			
Funnel Settings				
IPv4 Tunnel Network	10.4.10.0/30 This is the IPV4 virtual network used for private communications between this server and client hosts expressed using CIDR (e.g. 10.0.8.0/24). The network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting client (see Address Pool).			
IPvő Tunnel Network	This is the IPv6 virtual network used for private communications between this server and client hosts expressed using CIDR (e.g. fe80::/64). The fin network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients (see Address Pool).			
Pv4 Remote network(s)	10.3.2.0/24 IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for no			
Pv6 Remote network(s)	ane to site VPN. These are the IPv6 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the rout tables. Expressed as a comma-separated list of one or more IP/PREFIX. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank: non site-to-site VPN.			
Concurrent connections				
Compression	Specify the maximum number of clients allowed to concurrently connect to this server. Enabled with Adaptive Compression Compress tunnel packets using the LZD algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN			
Tone of Caning	detects that the data in the packets is not being compressed efficiently.			
Duplicate Connection	Allow multiple concurrent connections from cilents using the same Common Name.			
	(This is not generally recommended, but may be needed for some scenarios.)			
Disable IPv6				
Advanced Configurat	ion			
Custom options				
	Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon. EXAMPLE: push 'route 10.0.0.0 255.255.255.0'			
Verbosity level	default			
	None: Only fatal errors Default through 4: Normal usage range 5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets. 6-11: Debug info range			

• In the 'General Information'-section:

- \circ Disable this server: \Box
- Server mode: Peer to Peer (Shared Key)
- Protocol: UDP
- Device Mode: tun
- Interface: set it to whatever external interface you want to have your OpenVPN server listening on. In my case this is 'WAN'.
- Local port: set it to the port you want the local OpenVPN server to listen on. Default is '1194'.
- **Description:** Set an appropriate description e.g. 'Site_To_Site-SITE-A_SITE_B'
- In the 'Cryptographic Settings'-section:
 - $\circ~$ Automatically generate a shared key: $\boxtimes~$
 - Encryption Algorithm: AES-256-CBC (256 bit key, 128 bit block)
 - Auth digest algorithm: RSA-SHA512 (512-bit)
 - Hardware Crypto: No Hardware Crypto Acceleration (this is PC Engines APU specific, if your hardware has crypto support enable it)
- In the 'Tunnel Settings'-Section:
 - IPv4 Tunnel Network: 10.4.10.0/30 (this a very small subnet with 2 useable IP adresses since there is only one server and one client)
 - IPv6 Tunnel Network: leave empty
 - IPv4 Remote network(s): 10.3.2.0/24 (this is a comma separated list for all the networks you want to connect to on the client side (SITE A))
 - IPv6 Remote network(s): leave empty
 - $\circ~$ Concurrent connections: 1
 - $\circ~$ Compression: Enabled with Adaptive Compression
 - Type-of-Service: □ Set the TOS IP header value of tunnel packets to match the encapsulated packet value
 - Duplicate Connection:
 Allow multiple concurrent connections from clients using the same Common Name
 - **Disable IPv6:** ⊠ Don't forward IPv6 traffic
- In the 'Advanced Configuration'-section:
 - Custom options: leave empty
 - Verbosity Level: default
- Click on 'Save'-button

You should now be forwarded to the list with your configured OpenVPN servers under 'VPN - OpenVPN' on the 'Servers'-tab

	Client Specific Override	s Wizards		
OpenVPN Serve	rs			
Protocol / Port	Tunnel Network	Crypto	Description	Actions
UDP / 1194	10.4.10.0/30	Crypto: AES-256-CBC/RSA-SHA512 D-H Params: 0 bits	Site_To_Site-SITE-A_SITE_B (tun)	
				+ Add

• Click on the 'Edit'-button (the pencil) and leave this window open because we will need to copy the 'Shared Key' from this form later.

Configure the OpenVPN client on SITE-A router

• Navigate to 'VPN - OpenVPN'

Syst	tem • Interfaces • Firewall •	Services • VPN •	Status • Diagnostics •	Gold + pfser	ose.site a.inside + 🛛 🕞
VPN / OpenVF	PN / Clients				芝山 🗐 0
Servers Clients	Client Specific Overrides Wize	da			
OpenVPN Clients	Sanuar	Description		Actions	
					+ Add
	p/Sense is © 2004 - 2017 E	V Rubicon Communications, LLC	(Netgate), All Rights Reserved, (view license)	

- Click the 'Clients'-tab
- On the 'Clients'-tab click the '+ Add'-button to add a new OpenVPN client

Last update: 2021/12/09 pages:howtos:pfsense:simple-site-to-site-vpn-with-pfsense-and-openvpn https://wiki.nanoscopic.de/doku.php/pages/howtos/pfsense/simple-site-to-site-vpn-with-pfsense-and-openvpn 23:28

Servers Clients	Client Specific Overrides Witzards
General Information	
Disabled	Disable this client
farmenda.	Set this option to disable this client without removing it from the list.
oerver mode	Peer to Peer (Shared Key) *
Protocol	UDP *
Device mode	tun v
Interface	WAN •
Local port	
Security and the second security of the second seco	Sat this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.
	ane bane boe
Server port	1194
Proxy host or address	
Proxy port	
Proxy Auth Extra options	none *
Server hostname	Infinitely resolve server
resolution	Continuously attempt to resolve the server host name. Useful when communicating with a server that is not permanently connected to the Internet.
Description	Site_To_SiteSITE-A_SITE_B
Cryptographic Settin	025
eer Certificate Authority	No Certificate Authorities defined. One may be created here: System > Cert. Manager
Peer Certificate	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager > Certificate Revocation
Auto generate	Actomatically necessate a charael key
Shared Key	Protochinecking generate a single constant of the second sec
<u>since neg</u>	fd90d0550ffadbeadad76f12ac73013 7caf23dba1ed60fffc75596fe93fbe4e
	END OpenWPM Static key V1
	Paste the shared key here
Encryption Algorithm	AES-286-CBC (256 bit key, 128 bit block)
Auth digest algorithm	RSA-SHA512 (512-6H) *
	Leave this set to SHA1 unless all clients are set to match. SHA1 is the default for OpenVPN.
Hardware Crypto	No Hardware Crypto Acceleration
Tunnel Settings	
IPv4 Tunnel Network	10.4.10.0/30 This is the IPv4 virtual network used for private communications between this client and the server expressed using CIDR (e.g. 10.0.8.0/24). The
	second network address will be assigned to the client virtual interface.
IPv6 Tunnel Network	This is the IPv6 virtual network used for private communications between this client and the server expressed using CIDR (e.g. fe80:/64). The second
	network address will be assigned to the client virtual interface.
IPv4 Remote network(s)	10.4.2.0/24 IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables.
	Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for no site-to-site VPN.
IPv6 Remote network(s)	
	These are the IPv6 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the rout tables. Expressed as a comma-separated list of one or more IP/PREFIX. If this is a site-to-site VPN, enter the remote LAN/a here. May be left blank if
init extension bootstate	non steteto-ste VPN.
mix outgoing bandwidth	perween 100 and 100,000,000 bytes/sec Maximum outgoing bandwidth for this tunnel. Leave empty for no limit. The input value has to be something between 100 bytes/sec and 100
	Mbytes/sec (entered as bytes per second).
Compression	Enabled with Adaptive Compression Compress turnel packets using the L2D 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 value.
Disable IPv6	ig uont torward IPv6 traffic.
pon't pull routes	every one verver from adding toutes to the crient's routing table. This option still allows the server to set the TCP/IP properties of the client's TUN/TAP interface.
Don't add/remove routes	Don't add or remove routes automatically
	Pass routes to -route-upscript using environmental variables.
Advanced Configurat	lon
Custom options	
Custom options	
Custom options	A Enter any additional options to add to the OpenVPN client configuration here, separated by serricolon.
Custom options Verbosity level	Enter any additional options to add to the OpenVPN client configuration here, separated by servicolon.
Custom options Verbosity level	Enter any additional options to add to the OpenVPN client configuration here, separated by servicelon. default • Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.
Custom options Verbosity level	Enter any additional options to add to the OpenVPN client configuration here, separated by serricolon. default • Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being examped by output. None: Only failal errors
Custom options Verbosity level	Enter any additional options to add to the OpenVPN client configuration here, separated by serricolon. default • Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being examped by output. None: Only fistal errors Default Heronic 5 Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TMP/ADP packets and lowercase is use
Custom options Verbosity level	Enter any additional options to add to the OpenVPH client configuration have, separated by semicolon. default • Cach level above all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being examped by output. None: Only finite errors Default Websetters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TCP/UDP packets. 5: Output R and W charatters to the console for each packet read and write. Uppercase is used for TCP/UDP packets. 6:11: Debug info range

• In the 'General Information'-section:

- $\circ~$ Disable this client: $\Box~$
- Server mode: Peer to Peer (Shared Key)
- Protocol: UDP
- Device mode: tun
- Interface: Set to whatever external interface you want your OpenVPN client connect to the OpenVPN server at SITE-B. In my case this is 'WAN'.
- Local port: leave empty
- Server host or address: Set to the FQDN or IP address of the external SITE-B Interface. In this example it is 'site-b.site-b.de'.
- Server port: Set to the same port you have set in the server setup at SITE-B. Default is '1194'.

Proxy host or address: leave empty

```
Proxy port: leave empty
Proxy Auth. - Extra options: none
Infinitely resolve server: ???
Description: Set an appropriate description e.g. 'Site_To_Site-SITE-A_SITE_B'
In the 'Cryptographic Settings'-section:
Peer Certificate Authority: nothing to do here
Peer Certificate Revocation list: nothing to do here
Automatically generate a shared key: □ - This will display a form field in which you can paste the
key from the SITE-B server configuration.
```

Go back to SITE-B router. If you haven't left the window open, navigate to 'VPN – OpenVPN' and select the 'Servers'-tab, click on the 'Edit'button (the pencil) next to the server you have created earlier

~~DISCUSSION~~

From: https://wiki.nanoscopic.de/ - nanoscopic wiki

Permanent link: https://wiki.nanoscopic.de/doku.php/pages/howtos/pfsense/simple-site-to-site-vpn-with-pfsense-and-openvpn

Last update: 2021/12/09 23:28