Graeme Noble

Follow

37 Followers

About

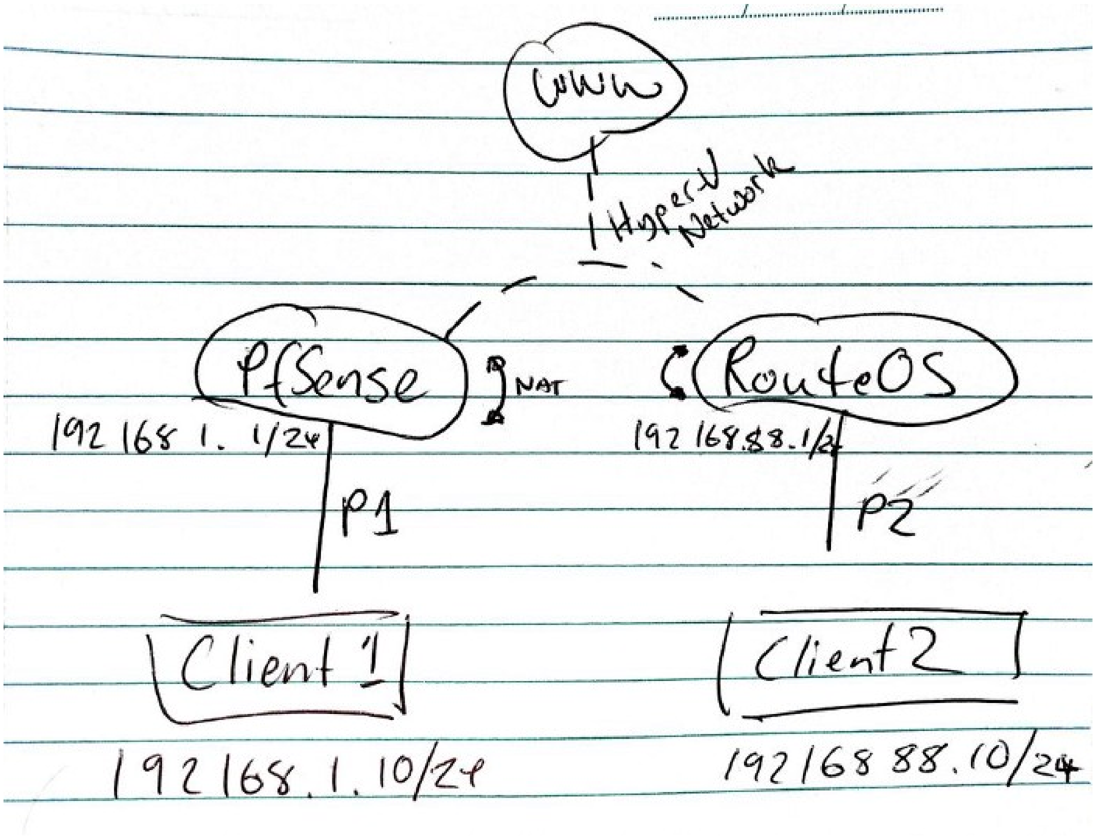
pfSense <-> Mikrotik OpenVPN Site-to-Site

Graeme Noble Sep 13, 2019 · 5 min read

Summary

This guide will provide guidance on setting up a OpenVPN Site-to-Site VPN between a pfSense and Mikrotik devices.

- Hyper-V lab was setup to implement and test the solution.
- IP addressing configuration is intentionally selected as close to vendor defaults.
- Firewall rules are intentionally lax for proof of concept and should be adjusted based on real world implementation.

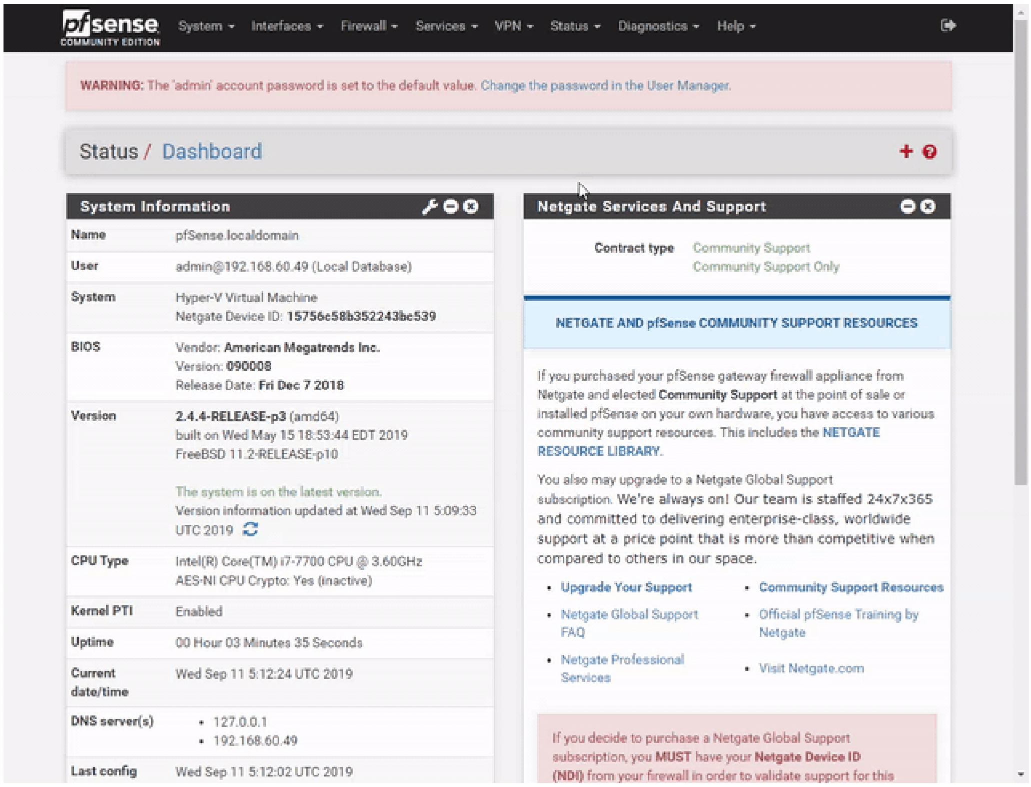


flexible configuration of the two devices, the Mikrotik support for OpenVPN is limited so it is configured as the client device that will dial out.

OpenVPN uses certificate authentication, a CA cert is created on the pfSense machine which will sign two certificates for the configuration, the first a server certificate for pfSense and the second a client cert for the Mikrotik.

1. Create CA cert on pfSense device.
2. Create Server certificate for pfSense OpenVPN server.
3. Create Client certificate for the Mikrotik OpenVPN client.

Additional certificate details are not completed in this documentation, but would be configured based on implementation.



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

Status / Dashboard

System Information

Name	pfSense.localdomain
User	admin@192.168.60.49 (Local Database)
System	Hyper-V Virtual Machine Netgate Device ID: **15756c58b352243bc539**
BIOS	Vendor: **American Megatrends Inc.** Version: **090008** Release Date: **Fri Dec 7 2018**
Version	**2.4.4-RELEASE-p3** (amd64) built on Wed May 15 18:53:44 EDT 2019 FreeBSD 11.2-RELEASE-p10 The system is on the latest version. Version information updated at Wed Sep 11 5:09:33 UTC 2019
CPU Type	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
Uptime	00 Hour 03 Minutes 35 Seconds
Current date/time	Wed Sep 11 5:12:24 UTC 2019
DNS server(s)	• 127.0.0.1 • 192.168.60.49
Last config	Wed Sep 11 5:12:02 UTC 2019

Netgate Services And Support

Contract type Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- **Upgrade Your Support**
- **Community Support Resources**
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

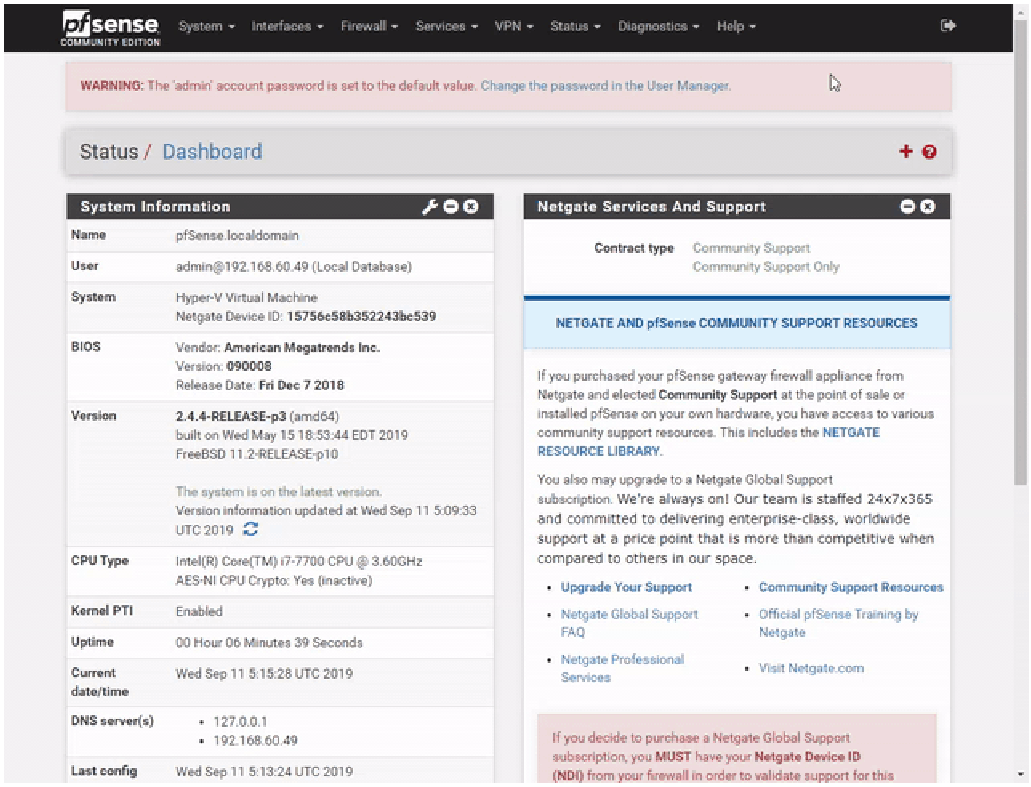
If you decide to purchase a Netgate Global Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this

Create OpenVPN Server

OpenVPN server is created on the pfSense device, important settings for Mikrotik compatibility:

- Server mode Peer-to-Peer.
- Protocol changed to TCP.
- TLS Key disabled as it's not supported on Mikrotik.

- Encryption Algorithm changed to AES-256-CBC
- AES-256-CBC added to NCP.
- Auth digest algorithm changed to SHA1.
- A IPv4 Tunnel Network is set. (This should be a new unique network, pfSense documentation uses 10.0.8.0/24).
- IPv4 Local networks are set. (The networks on the server side that need to be accessed remotely).
- IPv4 Remote networks are set. (The networks on the client side that need to be accessed remotely).
- Compression is set to Omit Preference.
- Logging level set to 4 for troubleshooting.



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

Status / Dashboard

System Information

Name	pfSense.localdomain
User	admin@192.168.60.49 (Local Database)
System	Hyper-V Virtual Machine Netgate Device ID: **15756c58b352243bc539**
BIOS	Vendor: **American Megatrends Inc.** Version: **090008** Release Date: **Fri Dec 7 2018**
Version	**2.4.4-RELEASE-p3** (amd64) built on Wed May 15 18:53:44 EDT 2019 FreeBSD 11.2-RELEASE-p10 The system is on the latest version. Version information updated at Wed Sep 11 5:09:33 UTC 2019
CPU Type	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
Uptime	00 Hour 06 Minutes 39 Seconds
Current date/time	Wed Sep 11 5:15:28 UTC 2019
DNS server(s)	• 127.0.0.1 • 192.168.60.49
Last config	Wed Sep 11 5:13:24 UTC 2019

Netgate Services And Support

Contract type	Community Support Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.

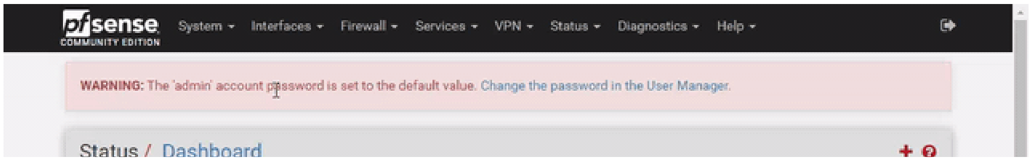
You also may upgrade to a Netgate Global Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

If you decide to purchase a Netgate Global Support subscription, you **MUST** have your **Netgate Device ID** (NDI) from your firewall in order to validate support for this

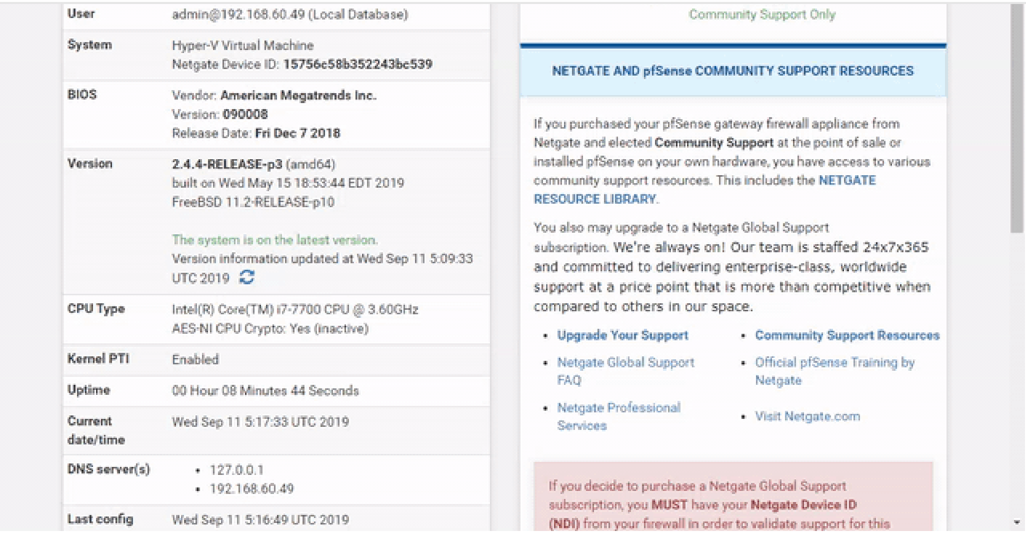
Export client cert for Mikrotik

Export the Mikrotik client cert as a p12 file so it will include the CA cert as a bundle and transfer it to the Mikrotik so the OpenVPN client can be setup.



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

Status / Dashboard



User	admin@192.168.60.49 (Local Database)
System	Hyper-V Virtual Machine Netgate Device ID: 15756c58b352243bc539
BIOS	Vendor: American Megatrends Inc. Version: 090008 Release Date: Fri Dec 7 2018
Version	2.4.4-RELEASE-p3 (amd64) built on Wed May 15 18:53:44 EDT 2019 FreeBSD 11.2-RELEASE-p10 The system is on the latest version. Version information updated at Wed Sep 11 5:09:33 UTC 2019
CPU Type	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
Uptime	00 Hour 08 Minutes 44 Seconds
Current date/time	Wed Sep 11 5:17:33 UTC 2019
DNS server(s)	• 127.0.0.1 • 192.168.60.49
Last config	Wed Sep 11 5:16:49 UTC 2019

Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.

You also may upgrade to a Netgate Global Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

If you decide to purchase a Netgate Global Support subscription, you **MUST** have your **Netgate Device ID** (NDI) from your firewall in order to validate support for this

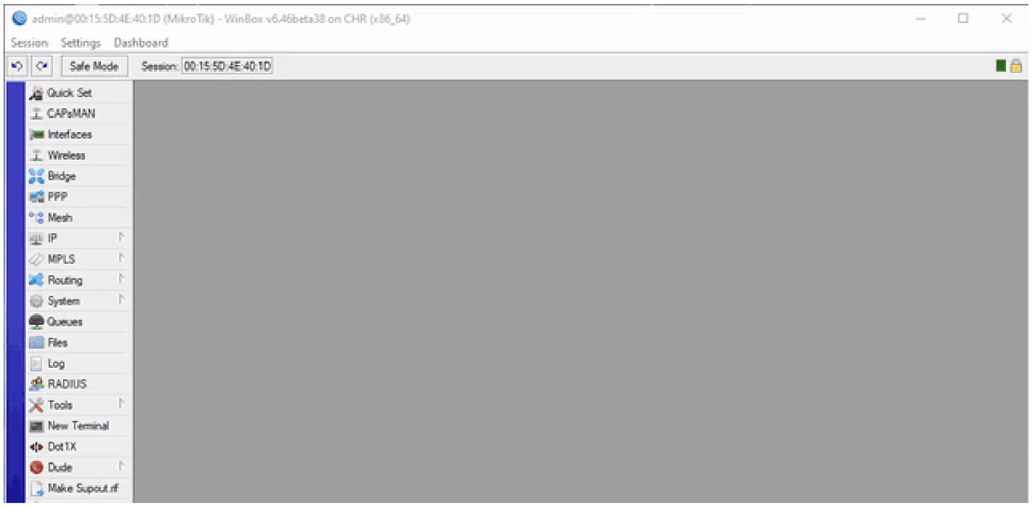
Setup Mikrotik OpenVPN client

Upload the P12 client certificate file to the Mikrotik and import it into System->Certificates, they should be renamed for easier OpenVPN client configuration.

Create a new OpenVPN client interface on the Mikrotik with settings to match OpenVPN server:

- Connect to set to WAN IP of pfSense device.
- A username needs to be set but is not used.
- The correct Mikrotik client certificate selected.
- Auth is set to SHA1.
- Cipher is set AES-256

It will attempt to dial the OpenVPN server, but it will be blocked by pfSense default WAN firewall rules.

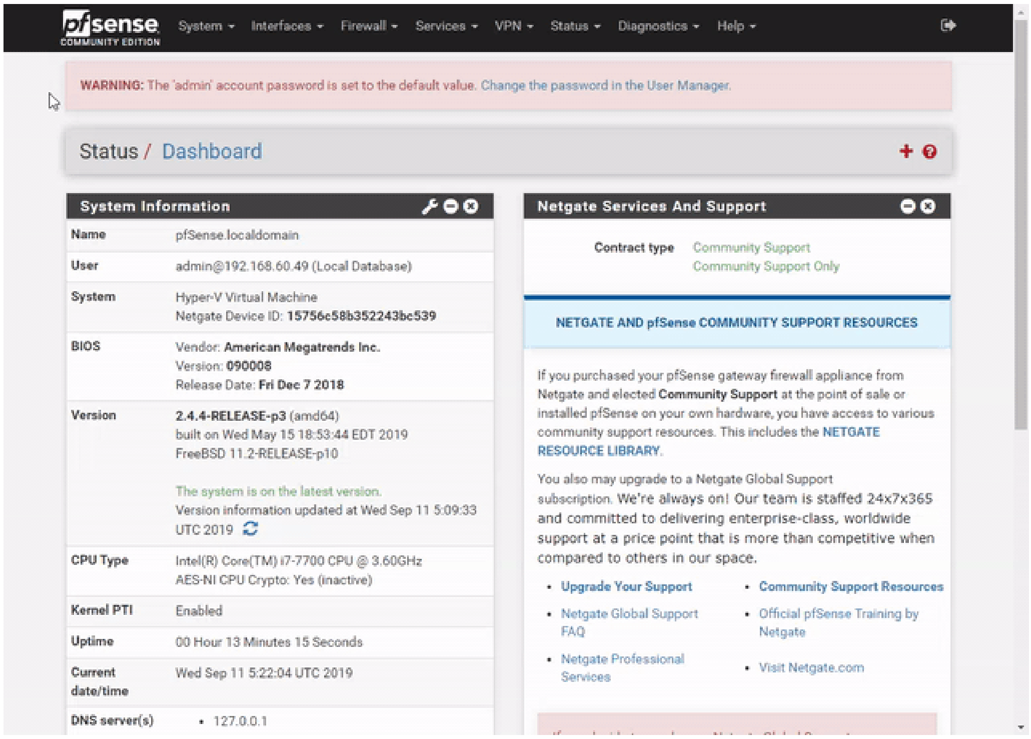


admin@00:15:5D:4E:40:1D (MikroTik) - WinBox v6.46beta38 on CHR (x86_64)

Session: 00:15:5D:4E:40:1D

Update pfSense WAN Firewall Rules

Allow access to the OpenVPN server ports which have been configured on TCP1194, if the WAN address of the Mikrotik is static, configure the rule to this source IP.


pfsense COMMUNITY EDITION
System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

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

Status / Dashboard

System Information

Name	pfSense.localdomain
User	admin@192.168.60.49 (Local Database)
System	Hyper-V Virtual Machine Netgate Device ID: **15756c58b352243bc539**
BIOS	Vendor: **American Megatrends Inc.** Version: **090008** Release Date: **Fri Dec 7 2018**
Version	**2.4.4-RELEASE-p3** (amd64) built on Wed May 15 18:53:44 EDT 2019 FreeBSD 11.2-RELEASE-p10 The system is on the latest version. Version information updated at Wed Sep 11 5:09:33 UTC 2019
CPU Type	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
Uptime	00 Hour 13 Minutes 15 Seconds
Current date/time	Wed Sep 11 5:22:04 UTC 2019
DNS server(s)	• 127.0.0.1

Netgate Services And Support

Contract type Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

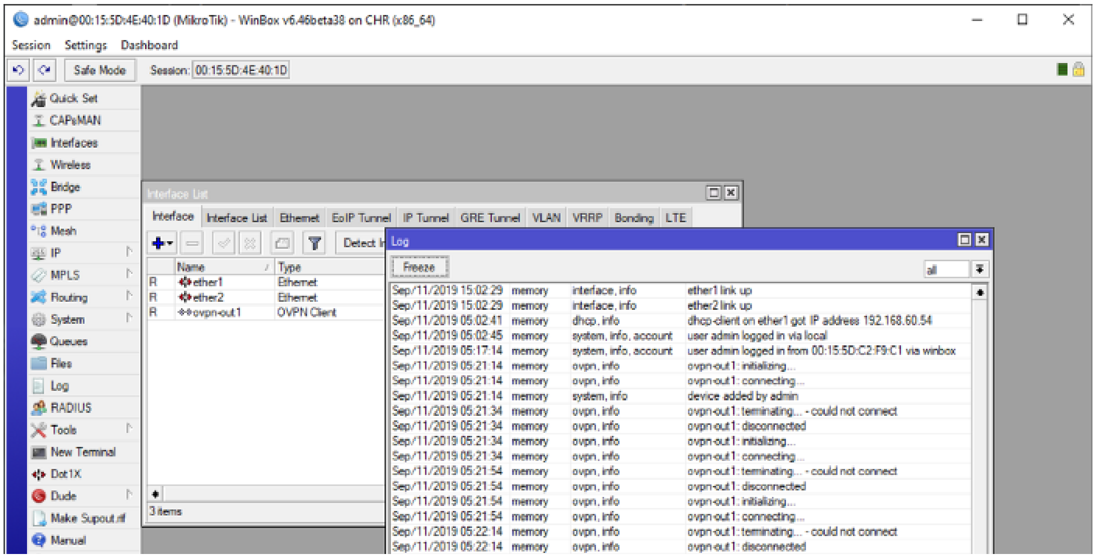
If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- **Upgrade Your Support**
- Netgate Global Support FAQ
- Netgate Professional Services
- **Community Support Resources**
- Official pfSense Training by Netgate
- Visit Netgate.com

Confirm OpenVPN connectivity

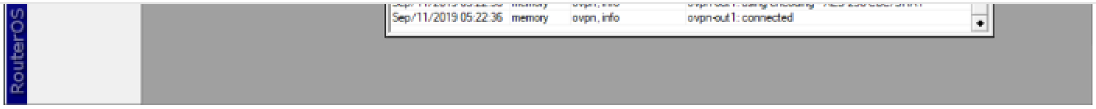
Once firewall rules have been added to allow traffic on the OpenVPN port between the server and client, the Mikrotik should be able to obtain a connection.



	Name	Type
R	ether1	Ethernet
R	ether2	Ethernet
R	ovpn-out1	OVPN Client

3 items

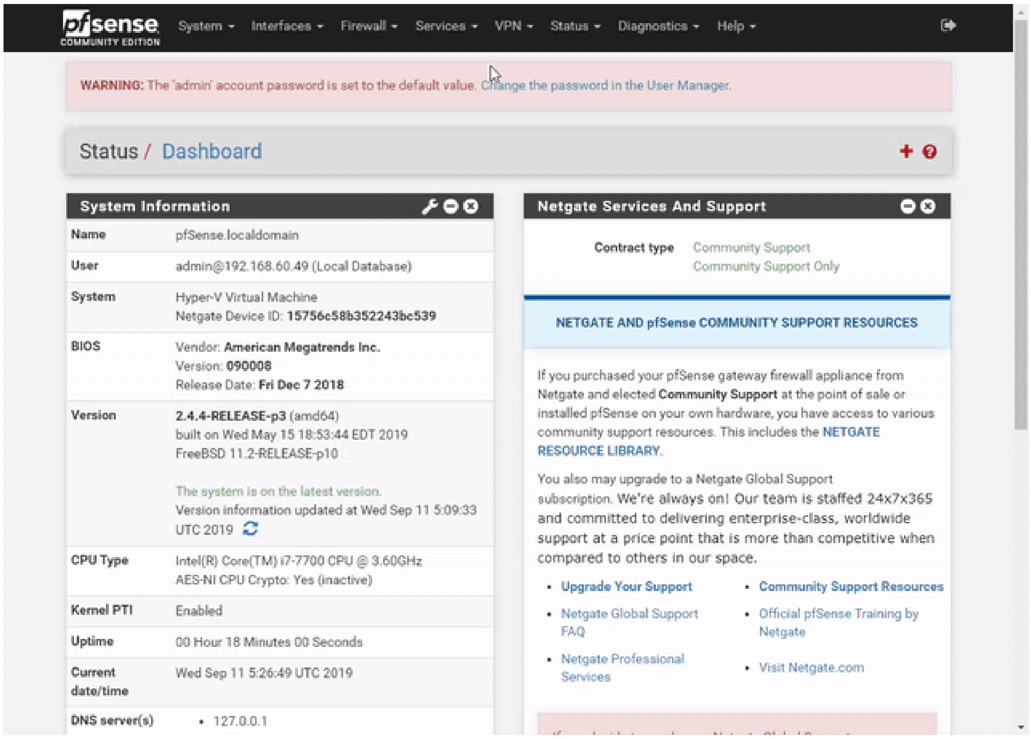
```
Sep/11/2019 15:02:29  memory  interface, info         ether1 link up
Sep/11/2019 15:02:29  memory  interface, info         ether2 link up
Sep/11/2019 05:02:41  memory  dhcp, info              dhcp-client on ether1 got IP address 192.168.60.54
Sep/11/2019 05:02:45  memory  system, info, account   user admin logged in via local
Sep/11/2019 05:17:14  memory  system, info, account   user admin logged in from 00:15:5D:C2:F9:C1 via winbox
Sep/11/2019 05:21:14  memory  ovpn, info              ovpn-out1: initializing...
Sep/11/2019 05:21:14  memory  ovpn, info              ovpn-out1: connecting...
Sep/11/2019 05:21:14  memory  system, info            device added by admin
Sep/11/2019 05:21:34  memory  ovpn, info              ovpn-out1: terminating... - could not connect
Sep/11/2019 05:21:34  memory  ovpn, info              ovpn-out1: disconnected
Sep/11/2019 05:21:34  memory  ovpn, info              ovpn-out1: initializing...
Sep/11/2019 05:21:34  memory  ovpn, info              ovpn-out1: connecting...
Sep/11/2019 05:21:54  memory  ovpn, info              ovpn-out1: terminating... - could not connect
Sep/11/2019 05:21:54  memory  ovpn, info              ovpn-out1: disconnected
Sep/11/2019 05:21:54  memory  ovpn, info              ovpn-out1: initializing...
Sep/11/2019 05:21:54  memory  ovpn, info              ovpn-out1: connecting...
Sep/11/2019 05:22:14  memory  ovpn, info              ovpn-out1: terminating... - could not connect
Sep/11/2019 05:22:14  memory  ovpn, info              ovpn-out1: disconnected
```



```
Sep/11/2019 05:22:36  memory  ovpn, info  ovpn-out1: connected
```

Update pfSense OpenVPN Firewall Rules

A new tab will appear under pfSense firewall rules for the OpenVPN interface, in this example all traffic is allowed, during implementation only traffic required to be allowed over the VPN should be allowed. (Rules added for incoming traffic to pfSense)



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

Status / Dashboard

System Information

Name	pfSense.localdomain
User	admin@192.168.60.49 (Local Database)
System	Hyper-V Virtual Machine Netgate Device ID: **15756c58b352243bc539**
BIOS	Vendor: **American Megatrends Inc.** Version: **090008** Release Date: **Fri Dec 7 2018**
Version	**2.4.4-RELEASE-p3** (amd64) built on Wed May 15 18:53:44 EDT 2019 FreeBSD 11.2-RELEASE-p10 The system is on the latest version. Version information updated at Wed Sep 11 5:09:33 UTC 2019
CPU Type	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
Uptime	00 Hour 18 Minutes 00 Seconds
Current date/time	Wed Sep 11 5:26:49 UTC 2019
DNS server(s)	• 127.0.0.1

Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.

You also may upgrade to a Netgate Global Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Netgate Global Support FAQ
- Netgate Professional Services
- Community Support Resources
- Official pfSense Training by Netgate
- Visit Netgate.com

Add Client Specific Overrides for Mikrotik subnets.

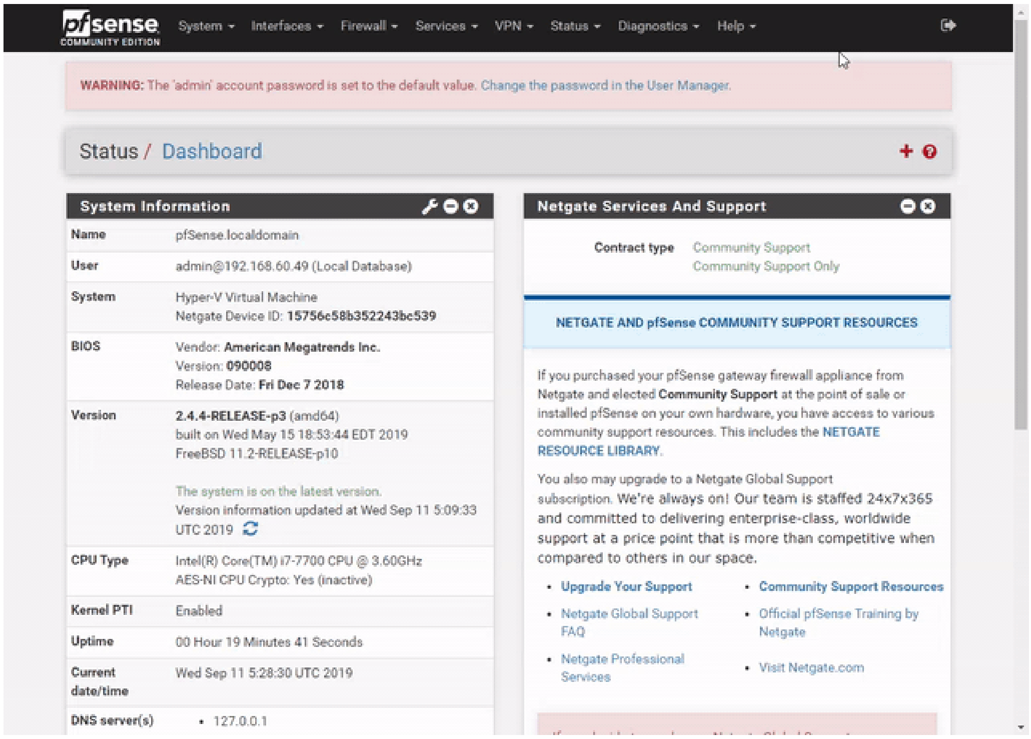
Although all the local/remote subnets have been added to the pfSense OpenVPN server configuration, it doesn't know which clients have which remote subnets and will drop the incoming traffic because it's not in the OpenVPN routing table for that OpenVPN client.

A client specific override is added to the pfSense OpenVPN configuration, this is matched based on the certificate name the client is using, it's best practice to use unique names/certificates for each client during implementation which identify the site/client clearly.

Because the OpenVPN client should be connected you can use the pfSense OpenVPN status page to copy and paste the exact certificate name of the connected OpenVPN client. Important settings are as follows:

- Common Name is set to the client certificate name.

The OpenVPN server is restarted to force the OpenVPN client to reconnect and apply the changes, the network routes will now appear in the OpenVPN routing table in the status page.



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

Status / Dashboard

System Information

Name	pfSense.localdomain
User	admin@192.168.60.49 (Local Database)
System	Hyper-V Virtual Machine Netgate Device ID: 15756c58b352243bc539
BIOS	Vendor: American Megatrends Inc. Version: 090008 Release Date: Fri Dec 7 2018
Version	2.4.4-RELEASE-p3 (amd64) built on Wed May 15 18:53:44 EDT 2019 FreeBSD 11.2-RELEASE-p10 The system is on the latest version. Version information updated at Wed Sep 11 5:09:33 UTC 2019
CPU Type	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
Uptime	00 Hour 19 Minutes 41 Seconds
Current date/time	Wed Sep 11 5:28:30 UTC 2019
DNS server(s)	• 127.0.0.1

Netgate Services And Support

Contract type Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

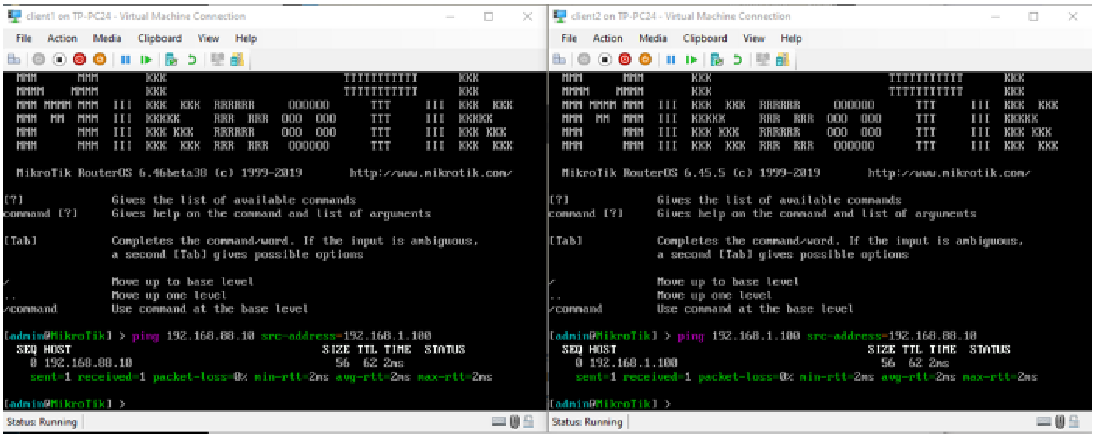
If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.

You also may upgrade to a Netgate Global Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

Network Connectivity Testing

Traffic should now be routing over the OpenVPN connection and not blocked by any firewall rules, perform connectivity testing to ensure the traffic is allowed as expected.


client1 on TP-PC24 - Virtual Machine Connection
File
Action
Media
Clipboard
View
Help
Status: Running
client2 on TP-PC24 - Virtual Machine Connection
File
Action
Media
Clipboard
View
Help
Status: Running

```
  MMM      MMM       KKK                          TTTTTTTTTTT      KKK
  MMMM    MMMM       KKK                          TTTTTTTTTTT      KKK
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
  MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
  MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
  MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK

  MikroTik RouterOS 6.46beta38 (c) 1999-2019       http://www.mikrotik.com/

[?]             Gives the list of available commands
command [?]     Gives help on the command and list of arguments

[Tab]           Completes the command/word. If the input is ambiguous,
                a second [Tab] gives possible options

/               Move up to base level
..              Move up one level
/command        Use command at the base level

[admin@MikroTik] > ping 192.168.88.10 src-address=192.168.1.100
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.88.10                              56  62 2ms
    sent=1 received=1 packet-loss=0% min-rtt=2ms avg-rtt=2ms max-rtt=2ms

[admin@MikroTik] >
```

```
  MMM      MMM       KKK                          TTTTTTTTTTT      KKK
  MMMM    MMMM       KKK                          TTTTTTTTTTT      KKK
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
  MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
  MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
  MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK

  MikroTik RouterOS 6.45.5 (c) 1999-2019       http://www.mikrotik.com/

[?]             Gives the list of available commands
command [?]     Gives help on the command and list of arguments

[Tab]           Completes the command/word. If the input is ambiguous,
                a second [Tab] gives possible options

/               Move up to base level
..              Move up one level
/command        Use command at the base level

[admin@MikroTik] > ping 192.168.1.100 src-address=192.168.88.10
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.1.100                              56  62 2ms
    sent=1 received=1 packet-loss=0% min-rtt=2ms avg-rtt=2ms max-rtt=2ms

[admin@MikroTik] >
```

About Help Legal