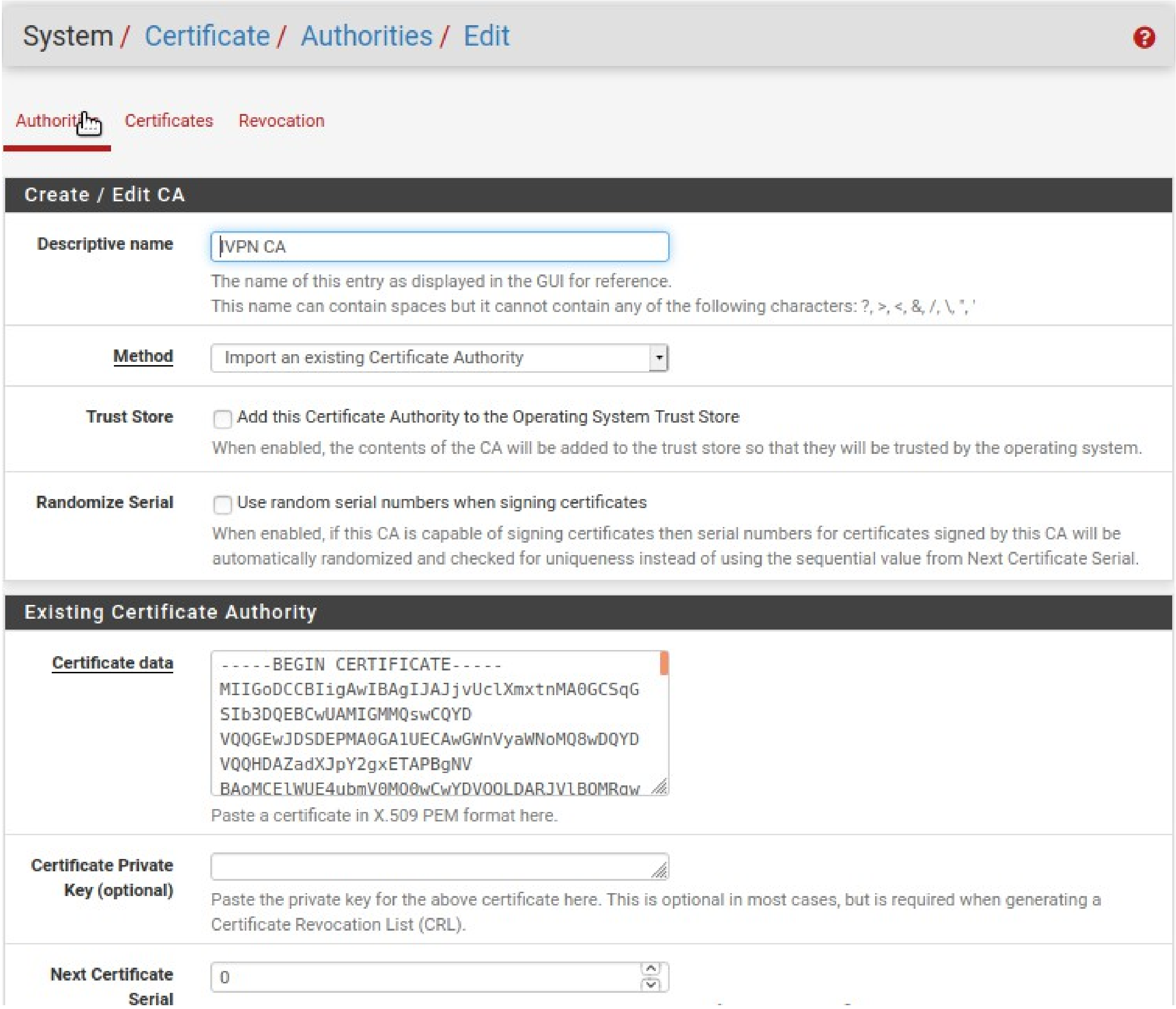
535 pfSense - VPN Configuration

Step 1: Choosing the Right VPN Protocol:

- I commenced the journey of setting up a VPN server by navigating to the VPN section in the pfSense web interface, eager to bolster network security with secure remote access.
- Deliberating between OpenVPN and IPsec, I carefully evaluated the strengths and weaknesses of each protocol, ultimately opting for OpenVPN due to its widespread support and ease of configuration.
- Firm in my decision, I proceeded to configure the server settings, knowing that OpenVPN would serve as the cornerstone of secure remote access for users connecting to the internal network.



System / Certificate / Authorities / Edit

Create / Edit CA

Descriptive name	VPN CA The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '
Method	Import an existing Certificate Authority
Trust Store	□ Add this Certificate Authority to the Operating System Trust Store When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.
Randomize Serial	□ Use random serial numbers when signing certificates When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Existing Certificate Authority

Certificate data

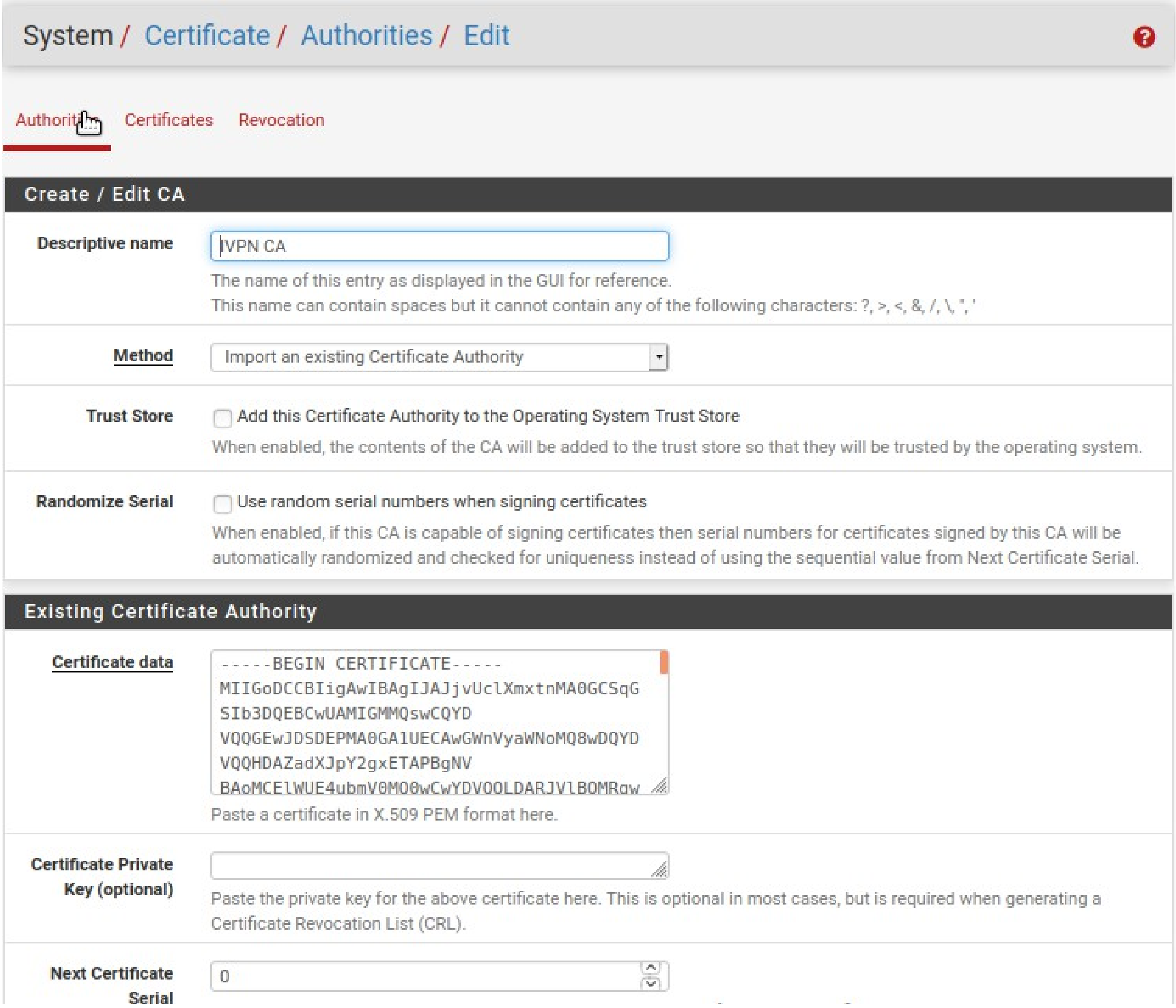
```
-----BEGIN CERTIFICATE-----
MIIGoDCCBIigAwIBAgIJAJjvUclXmxtnMA0GCSqG
SIb3DQEBCwUAMIGMMQswCQYD
VQQGEwJDSDEPMA0GA1UECAwGWnVyaWNoMQ8wDQYD
VQQHDAZadXJpY2gxETAPBgNV
BAoMCElWUE4ubmV0MO0wCwYDVOOLDARJVlBOMRaw
```

Paste a certificate in X.509 PEM format here.

Certificate Private Key (optional)	Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).
Next Certificate Serial	0

Step 2: Configuring VPN Server Settings with Precision:

- With determination, I delved into the intricacies of VPN server configuration, navigating through the intuitive interface of pfSense with confidence.
- Guided by the OpenVPN server wizard, I meticulously adjusted the server settings, ensuring seamless compatibility with a diverse range of client devices and network configurations.
- From selecting the appropriate server mode to specifying encryption algorithms, I left no room for error, meticulously tailoring the settings to align with the specific requirements of the network infrastructure.



System / Certificate / Authorities / Edit

Create / Edit CA

Descriptive name: VPN CA

The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '

Method: Import an existing Certificate Authority

Trust Store: □ Add this Certificate Authority to the Operating System Trust Store

When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial: □ Use random serial numbers when signing certificates

When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Existing Certificate Authority

Certificate data:

```
-----BEGIN CERTIFICATE-----
MIIGoDCCBIigAwIBAgIJAJjvUclXmxtnMA0GCSqG
SIb3DQEBCwUAMIGMMQswCQYD
VQQGEwJDSDEPMA0GA1UECAwGWnVyaWNoMQ8wDQYD
VQQHDAZadXJpY2gxETAPBgNV
BAoMCElWUE4ubmV0MO0wCwYDVOOLDARJVlBOMRaw
```

Paste a certificate in X.509 PEM format here.

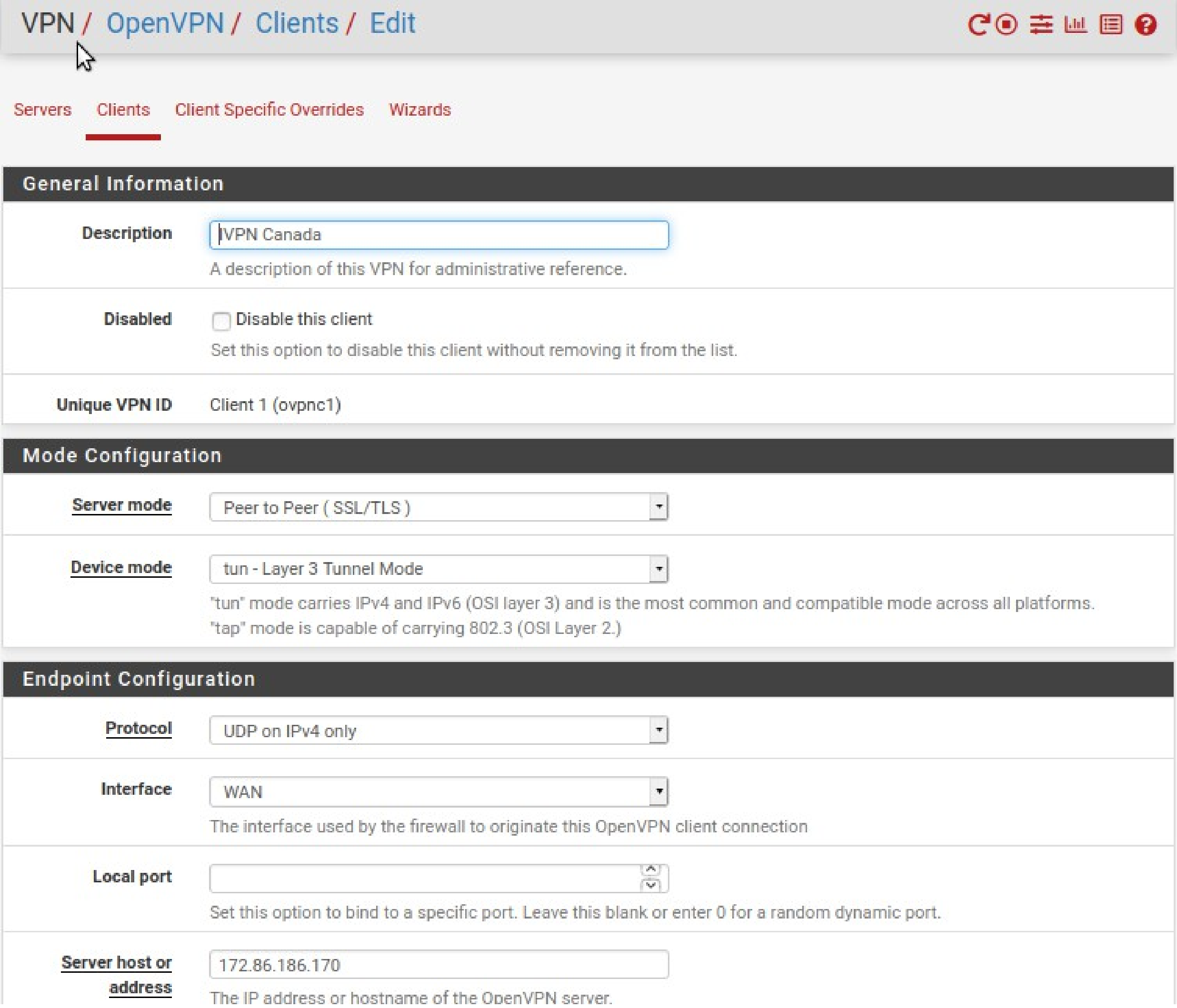
Certificate Private Key (optional):

Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).

Next Certificate Serial: 0

Step 3: Creating User Accounts and Certificates for Seamless Connectivity:

- Transitioning seamlessly to user management, I navigated to the User Manager and Cert Manager sections, ready to create user accounts and certificates crucial for VPN connectivity.
- With a focus on enhancing security and authentication, I diligently added new users and generated certificates signed by the Certificate Authority (CA), laying a solid foundation for secure and encrypted communication.



General Information

Description: IVPN Canada
A description of this VPN for administrative reference.

Disabled: □ Disable this client
Set this option to disable this client without removing it from the list.

Unique VPN ID: Client 1 (ovpnc1)

Mode Configuration

Server mode: Peer to Peer (SSL/TLS)

Device mode: tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Endpoint Configuration

Protocol: UDP on IPv4 only

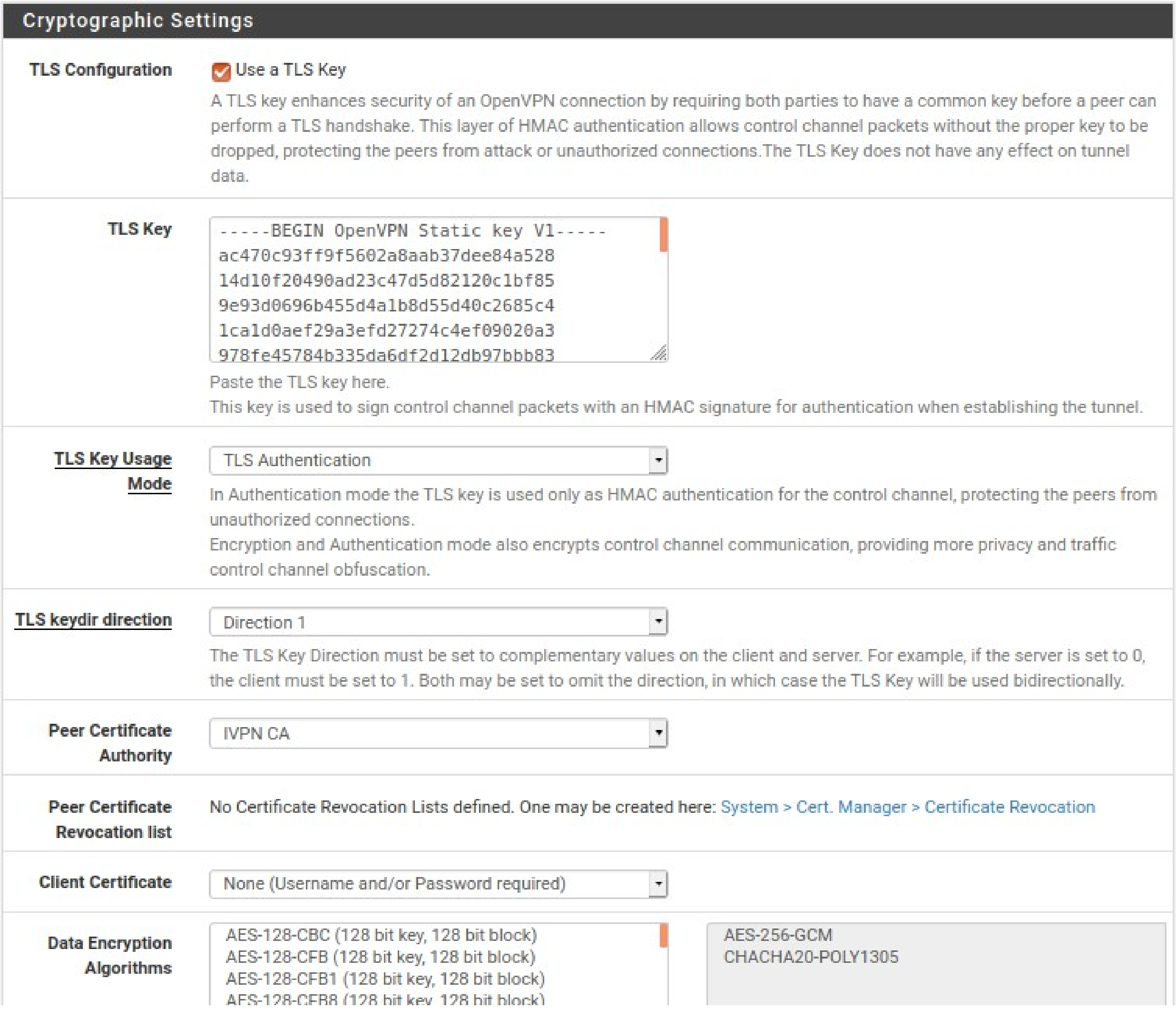
Interface: WAN
The interface used by the firewall to originate this OpenVPN client connection

Local port:
Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.

Server host or address: 172.86.186.170
The IP address or hostname of the OpenVPN server.

Step 4: Exporting and Distributing Client Configuration:

- Equipped with the necessary user credentials and certificates, I proceeded to export client configuration files using the openvpn-client-export package, ensuring a streamlined setup process for remote users.
- With meticulous attention to detail, I meticulously distributed the client configuration files and certificates to each user, emphasizing the importance of secure transmission to safeguard sensitive information.



Cryptographic Settings

TLS Configuration ☑ Use a TLS Key

A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections.The TLS Key does not have any effect on tunnel data.

TLS Key

```
-----BEGIN OpenVPN Static key V1-----
ac470c93ff9f5602a8aab37dee84a528
14d10f20490ad23c47d5d82120c1bf85
9e93d0696b455d4a1b8d55d40c2685c4
1ca1d0aef29a3efd27274c4ef09020a3
978fe45784b335da6df2d12db97bbb83
```

Paste the TLS key here.
This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.

TLS Key Usage Mode: TLS Authentication

In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections.
Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.

TLS keydir direction: Direction 1

The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.

Peer Certificate Authority: IVPN CA

Peer Certificate Revocation list: No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager > Certificate Revocation

Client Certificate: None (Username and/or Password required)

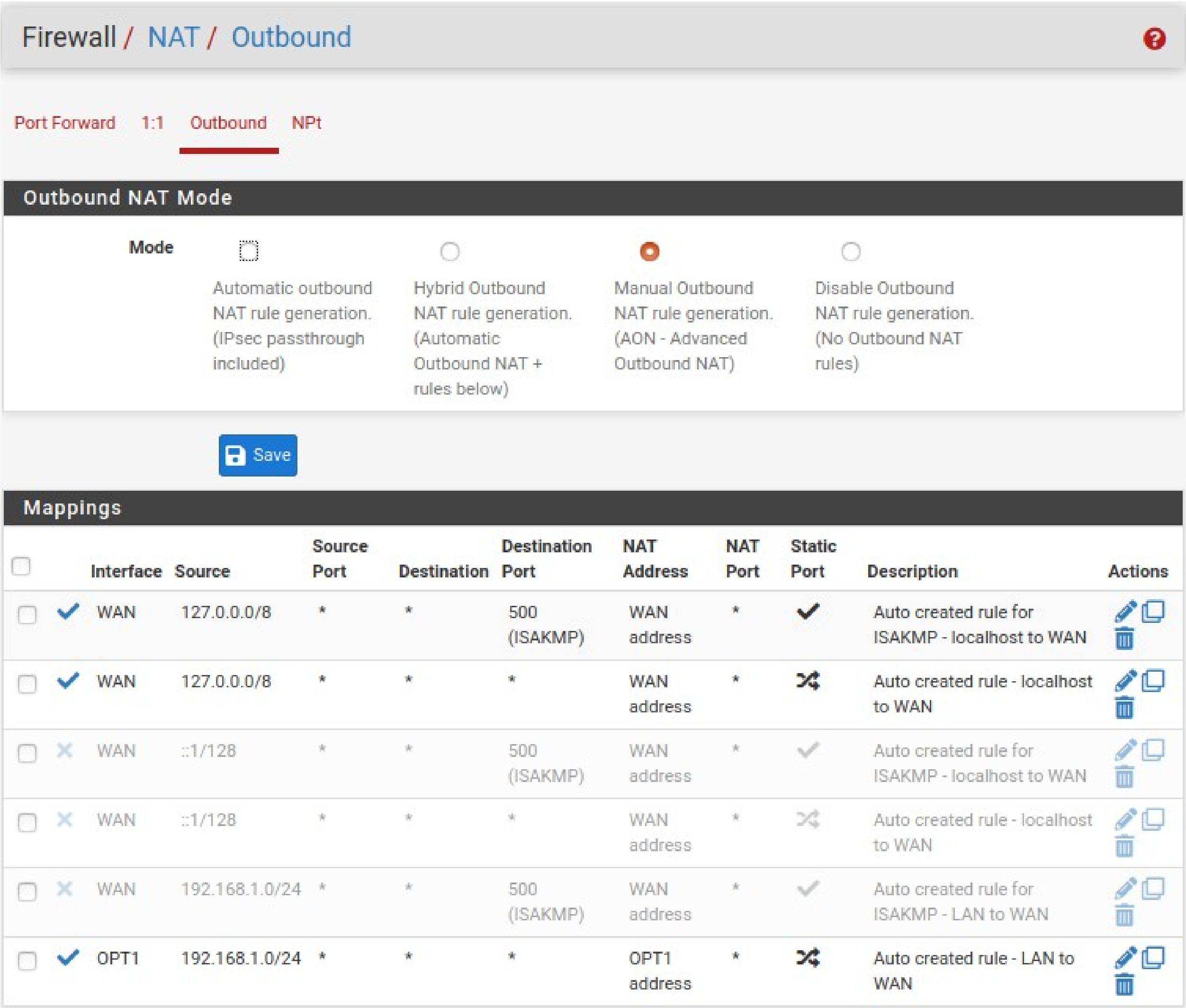
Data Encryption Algorithms

AES-128-CBC (128 bit key, 128 bit block)
AES-128-CFB (128 bit key, 128 bit block)
AES-128-CFB1 (128 bit key, 128 bit block)
AES-128-CFB8 (128 bit key, 128 bit block)

AES-256-GCM
CHACHA20-POLY1305

Step 5: Connecting to the VPN and Testing Connectivity:

- With anticipation mounting, I guided remote users through the process of installing the OpenVPN client application and importing the client configuration file.
- As users connected to the VPN, I closely monitored their experience, ensuring smooth access to internal network resources and verifying proper IP assignment and internet traffic routing.



Firewall / NAT / Outbound

Outbound NAT Mode

Mode

□ Automatic outbound NAT rule generation. (IPsec passthrough included)

○ Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)

● Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)

○ Disable Outbound NAT rule generation. (No Outbound NAT rules)

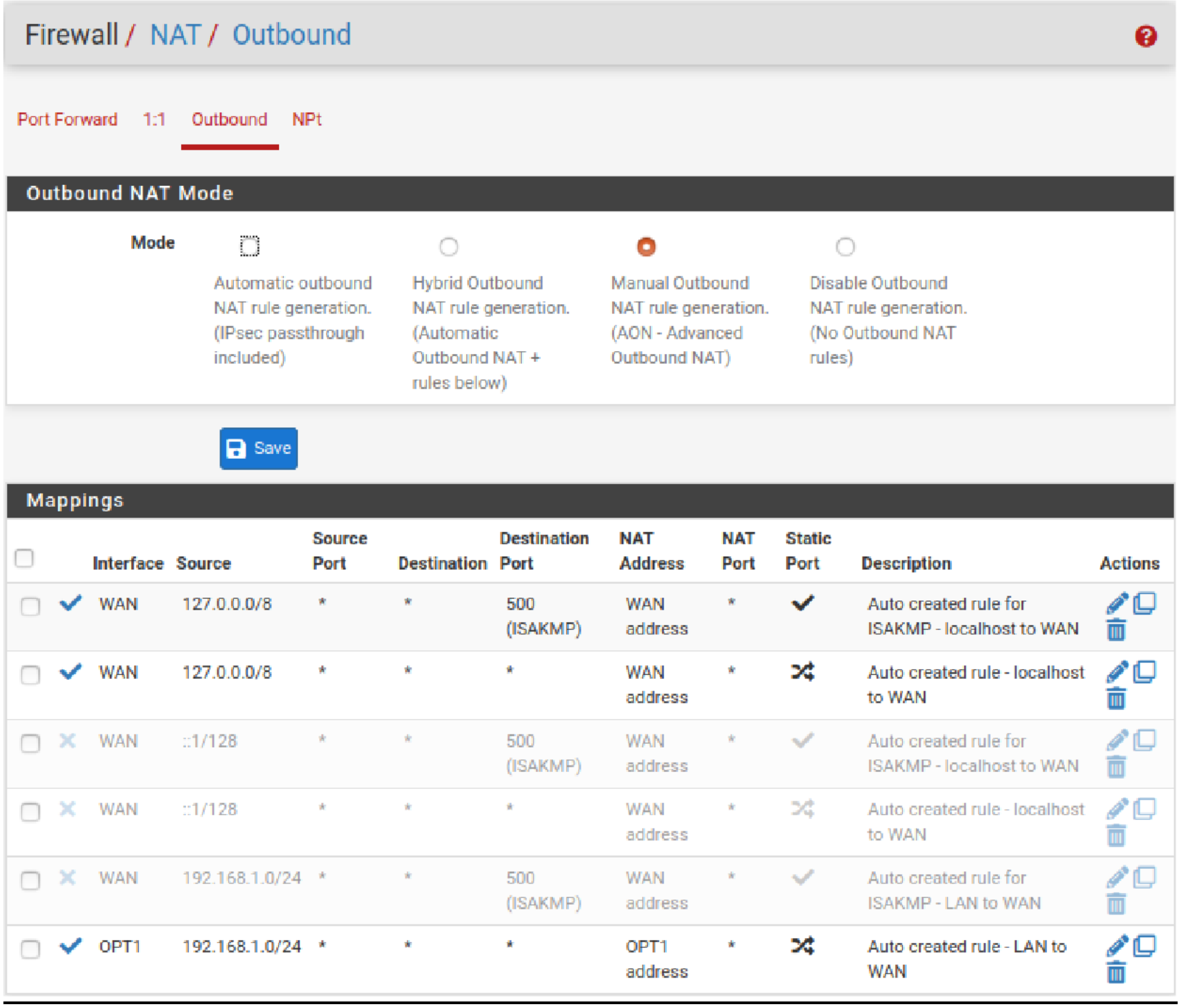
Mappings

□		Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
□	✓	WAN	127.0.0.0/8	*	*	500 (ISAKMP)	WAN address	*	✓	Auto created rule for ISAKMP - localhost to WAN	✎ ⧉ 🗑
□	✓	WAN	127.0.0.0/8	*	*	*	WAN address	*	⤮	Auto created rule - localhost to WAN	✎ ⧉ 🗑
□	✗	WAN	::1/128	*	*	500 (ISAKMP)	WAN address	*	✓	Auto created rule for ISAKMP - localhost to WAN	✎ ⧉ 🗑
□	✗	WAN	::1/128	*	*	*	WAN address	*	⤮	Auto created rule - localhost to WAN	✎ ⧉ 🗑
□	✗	WAN	192.168.1.0/24	*	*	500 (ISAKMP)	WAN address	*	✓	Auto created rule for ISAKMP - LAN to WAN	✎ ⧉ 🗑
□	✓	OPT1	192.168.1.0/24	*	*	*	OPT1 address	*	⤮	Auto created rule - LAN to WAN	✎ ⧉ 🗑

Verification and Troubleshooting:

- In the event of connectivity issues, I conducted a thorough review of VPN server settings and firewall configurations, ensuring that traffic on the OpenVPN port was permitted.

- With a keen eye for detail, I meticulously verified the correctness and validity of user credentials and certificates, consulting OpenVPN logs for insights into any errors or anomalies.



Firewall / NAT / Outbound

Port Forward 1:1 Outbound NPt

Outbound NAT Mode

Mode

○ Automatic outbound NAT rule generation. (IPsec passthrough included)

○ Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)

● Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)

○ Disable Outbound NAT rule generation. (No Outbound NAT rules)

Save

Mappings

□		Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
□	✓	WAN	127.0.0.0/8	*	*	500 (ISAKMP)	WAN address	*	✓	Auto created rule for ISAKMP - localhost to WAN	
□	✓	WAN	127.0.0.0/8	*	*	*	WAN address	*	🔀	Auto created rule - localhost to WAN	
□	✗	WAN	::1/128	*	*	500 (ISAKMP)	WAN address	*	✓	Auto created rule for ISAKMP - localhost to WAN	
□	✗	WAN	::1/128	*	*	*	WAN address	*	🔀	Auto created rule - localhost to WAN	
□	✗	WAN	192.168.1.0/24	*	*	500 (ISAKMP)	WAN address	*	✓	Auto created rule for ISAKMP - LAN to WAN	
□	✓	OPT1	192.168.1.0/24	*	*	*	OPT1 address	*	🔀	Auto created rule - LAN to WAN	