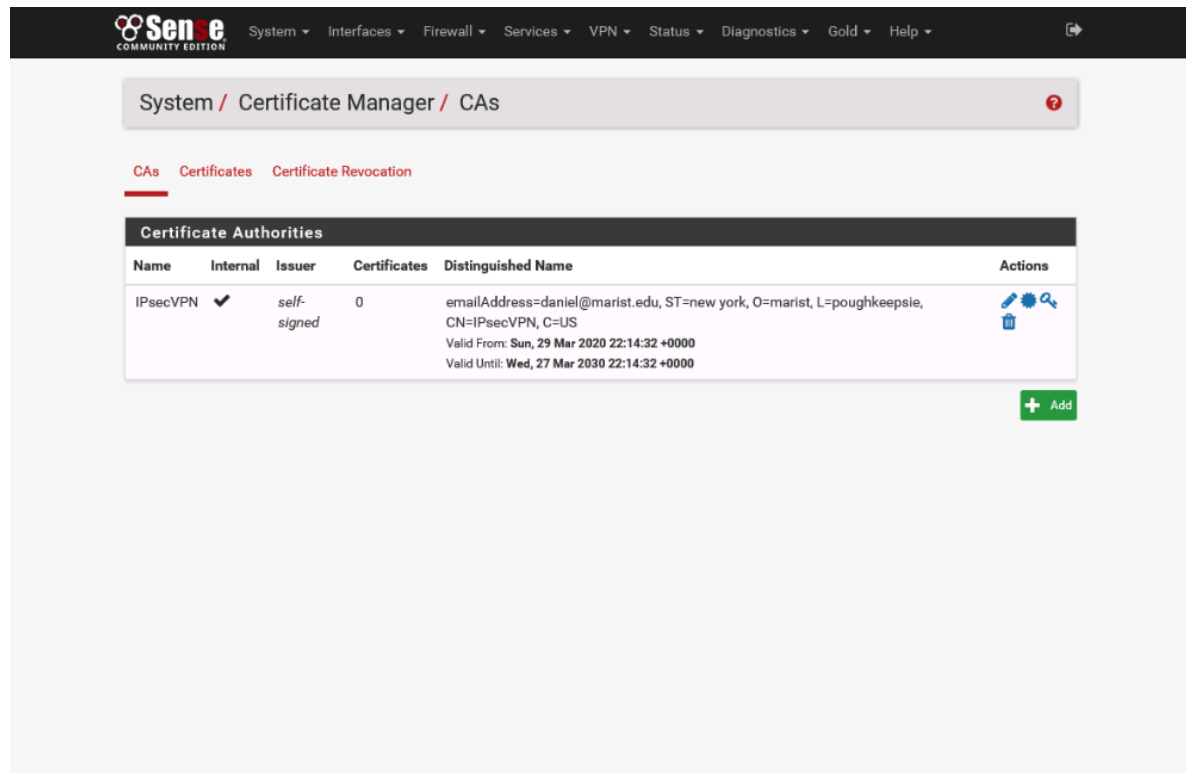


Lab 7




Authors: Daniel Gisolfi, James Ekstract

Section 1

Screen capture showing the resulting Certificate Authorities table

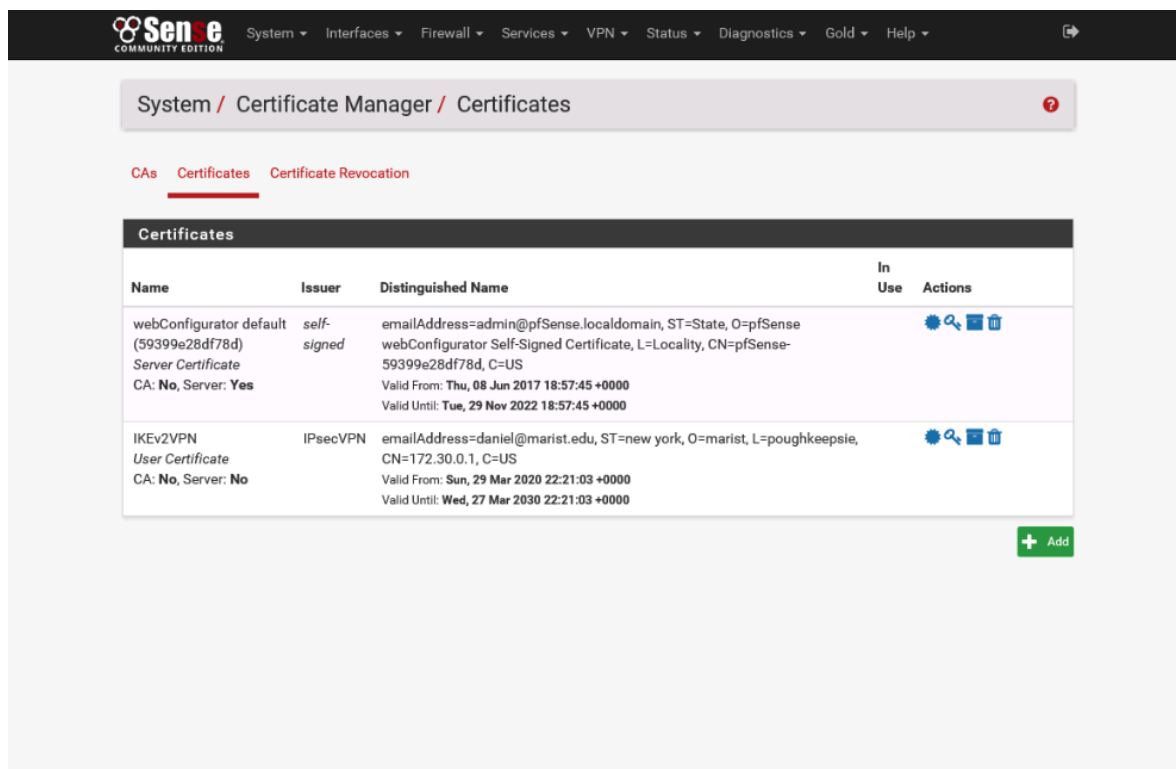


The screenshot shows the Sensei Community Edition web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area displays the 'System / Certificate Manager / CAs' breadcrumb trail. Below this, there are tabs for 'CAs', 'Certificates', and 'Certificate Revocation'. The 'CAs' tab is active, showing a table of Certificate Authorities. The table has columns for Name, Internal, Issuer, Certificates, Distinguished Name, and Actions. One entry is visible: 'IPsecVPN' with a checkmark in the Internal column, 'self-signed' as the Issuer, '0' as the number of Certificates, and a Distinguished Name of 'emailAddress=daniel@marist.edu, ST=new york, O=marist, L=poughkeepsie, CN=IPsecVPN, C=US'. The Valid From date is 'Sun, 29 Mar 2020 22:14:32 +0000' and the Valid Until date is 'Wed, 27 Mar 2030 22:14:32 +0000'. An 'Add' button is located at the bottom right of the table.

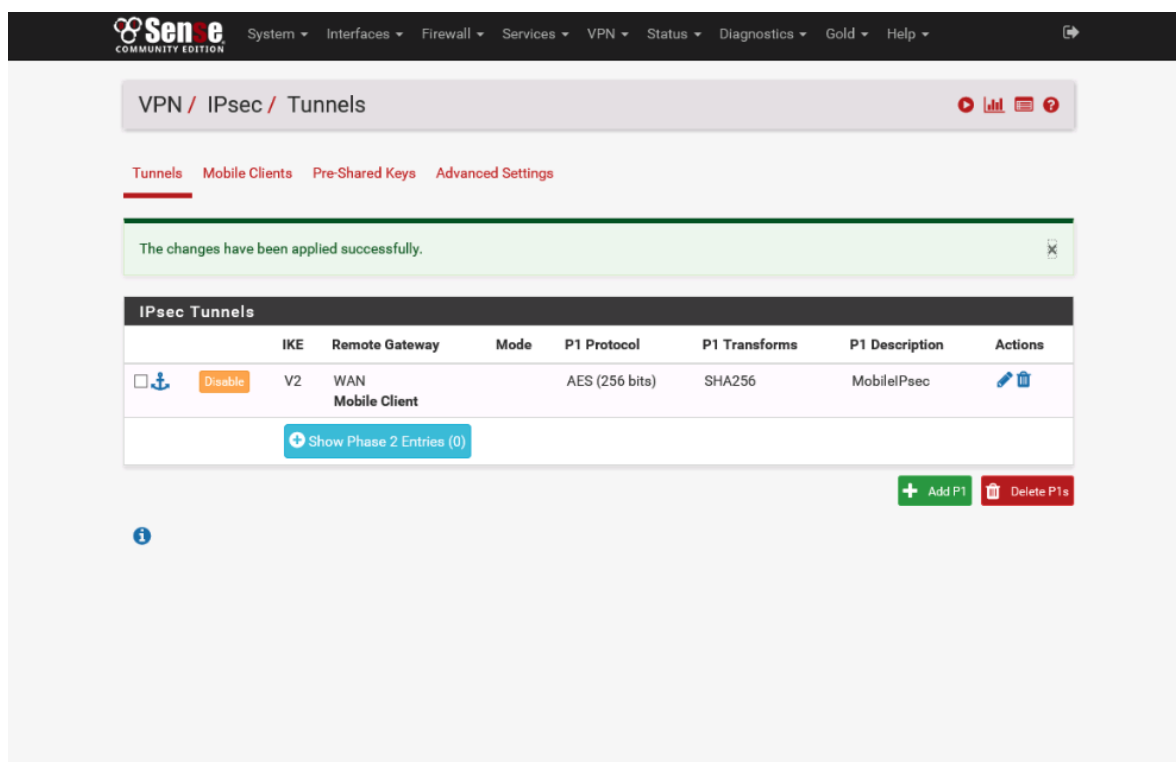
Name	Internal	Issuer	Certificates	Distinguished Name	Actions
IPsecVPN	✓	self-signed	0	emailAddress=daniel@marist.edu, ST=new york, O=marist, L=poughkeepsie, CN=IPsecVPN, C=US Valid From: Sun, 29 Mar 2020 22:14:32 +0000 Valid Until: Wed, 27 Mar 2030 22:14:32 +0000	  

[+ Add](#)

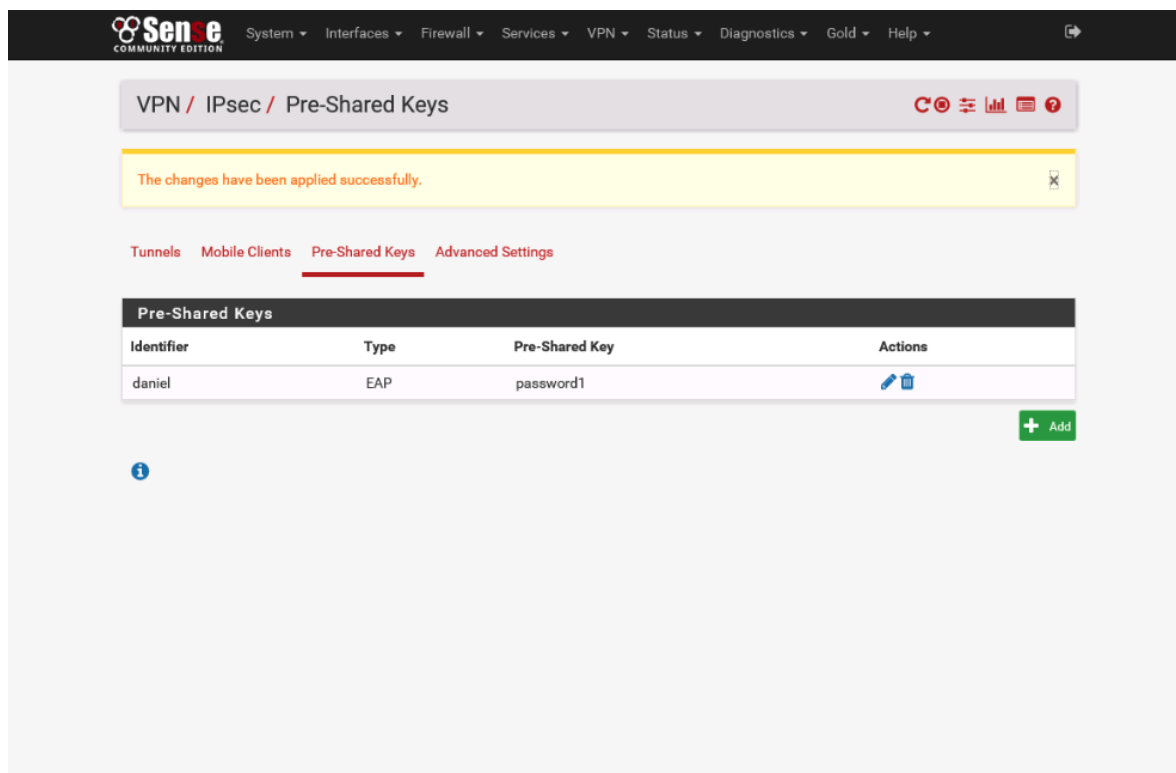
Screen capture showing the Certificates table



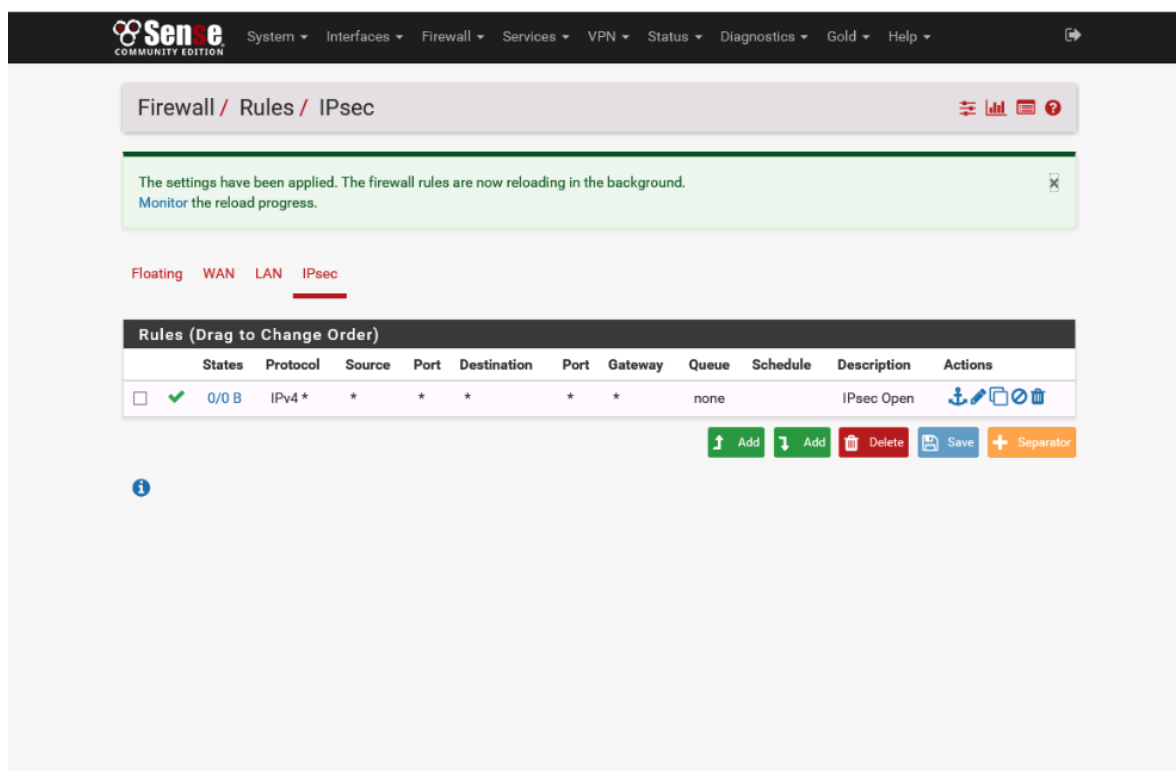
Screen capture showing the IPsec Tunnels table



Screen capture showing the Pre-Shared Keys table



screen capture showing the IPsec Rules table



Section 2

Part 1

The CA configuration form displayed in pfSense

Create a New Certificate Authority (CA) Certificate	
Descriptive name	<input type="text" value="EkstractGisolfi_CA"/> A name for administrative reference, to identify this certificate. This is the same as common-name field for other Certificates.
Key length	<input type="text" value="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	<input type="text" value="3650"/> Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)
Country Code	<input type="text" value="US"/> Two-letter ISO country code (e.g. US, AU, CA)
State or Province	<input type="text" value="New York"/> Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).
City	<input type="text" value="Poughkeepsie"/> City or other Locality name (e.g. Louisville, Indianapolis, Toronto).
Organization	<input type="text" value="Marist College"/> Organization name, often the Company or Group name.
E-mail	<input type="text" value="james.eksract1@marist.edu"/> E-mail address for the Certificate contact. Often the e-mail of the person generating the certificate.

The client settings section of the pfSense OpenVPN wizard

30.0.1/wizard.php?xml=openvpn

DNS Server 3	<input type="text"/> DNS server IP to provide to connecting clients.
DNS Server 4	<input type="text"/> DNS server IP to provide to connecting clients.
NTP Server	<input type="text"/> Network Time Protocol server to provide to connecting clients.
NTP Server 2	<input type="text"/> Network Time Protocol server to provide to connecting clients.
NetBIOS Options	<input type="checkbox"/> Enable NetBIOS over TCP/IP. If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
NetBIOS Node Type	<input type="text" value="none"/> Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).
NetBIOS Scope ID	<input type="text"/> A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID.
WINS Server 1	<input type="text"/> A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
WINS Server 2	<input type="text"/> A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
Advanced	<input type="text" value='push "route 172.30.0.0 255.255.255.0";mute 10;comp-lzo;'/> Enter any additional options to add to the OpenVPN server configuration here, separated by a semicolon. EXAMPLE: push "route 10.0.0.0 255.255.255.0"

Part 2

The completed OpenVPN configuration

Wizard / OpenVPN Remote Access Server Setup / Finished!

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

The OpenVPN rule on the WAN rules table

Firewall / Rules / WAN

Floating **WAN** LAN OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✗	0/0 B	*		RFC 1918 networks	*	*	*	*	Block private networks	
<input checked="" type="checkbox"/>	✗	0/0 B	*		Reserved Not assigned by IANA	*	*	*	*	Block bogon networks	
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	*		WAN address	1194 (OpenVPN)	*	none	OpenVPN VPN Server wizard	

Add Add Delete Save Separator

The OpenVPN rule on the OpenVPN rules table

Firewall / Rules / OpenVPN

Floating WAN LAN **OpenVPN**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 *	*	*	*	*	*	none	OpenVPN VPN Server wizard	

Add Add Delete Save Separator