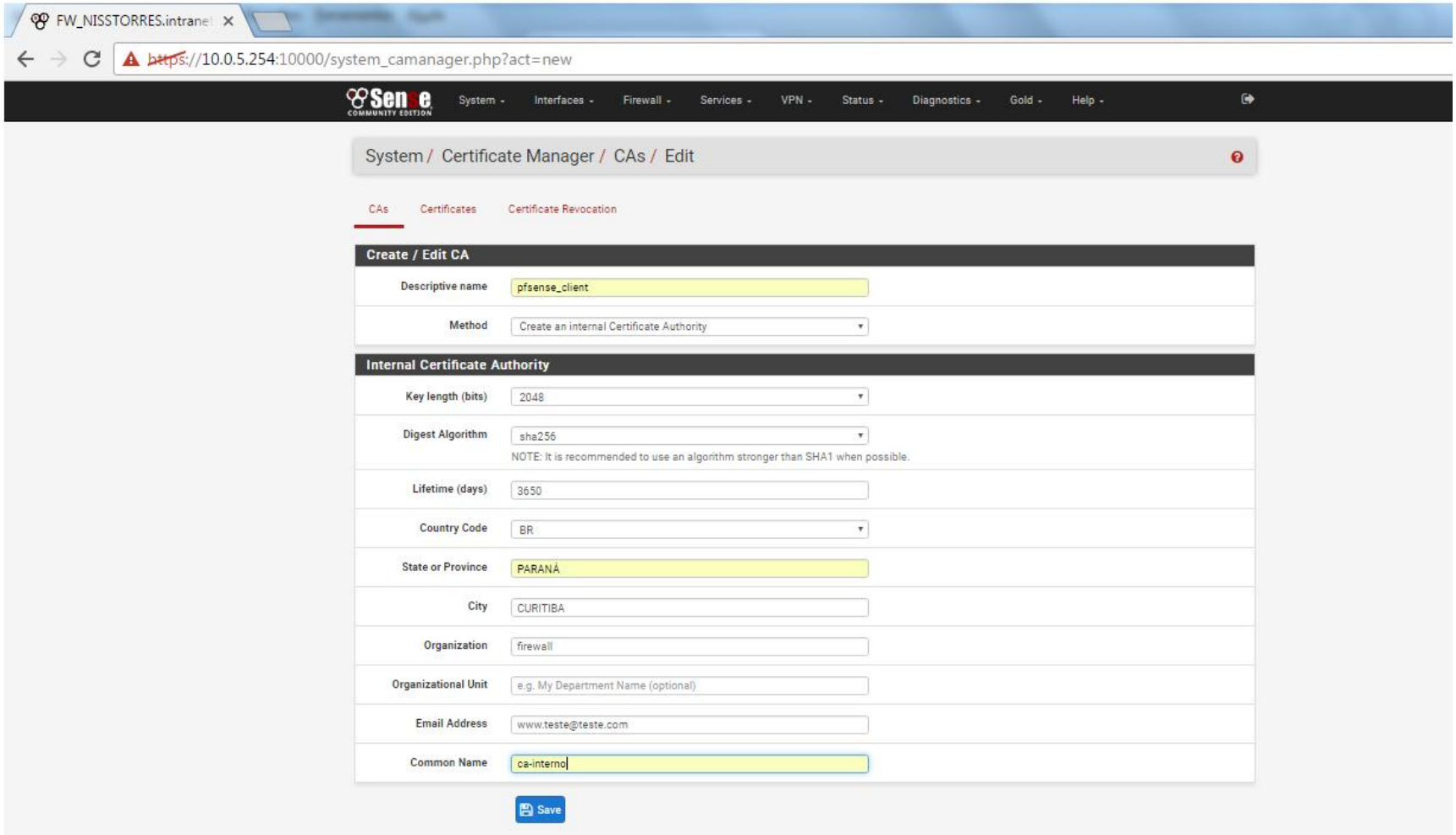
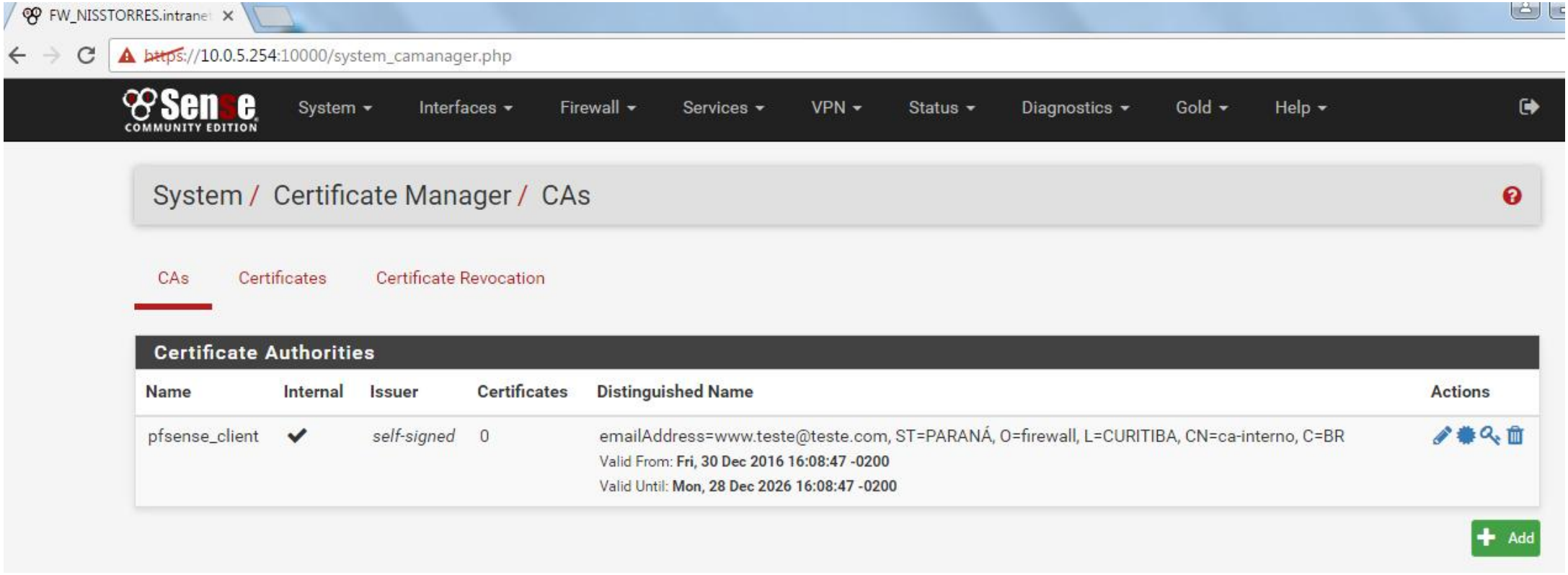
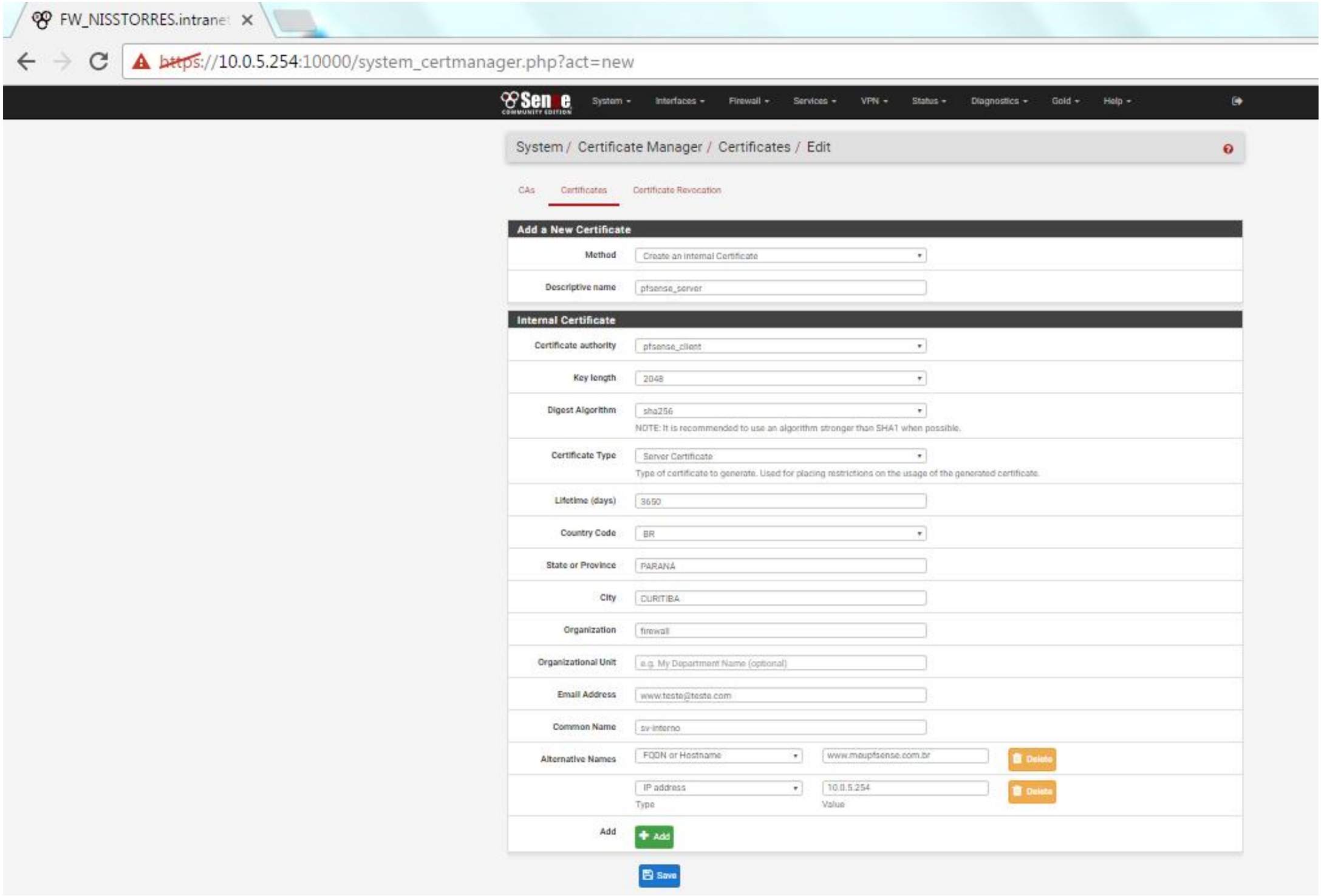
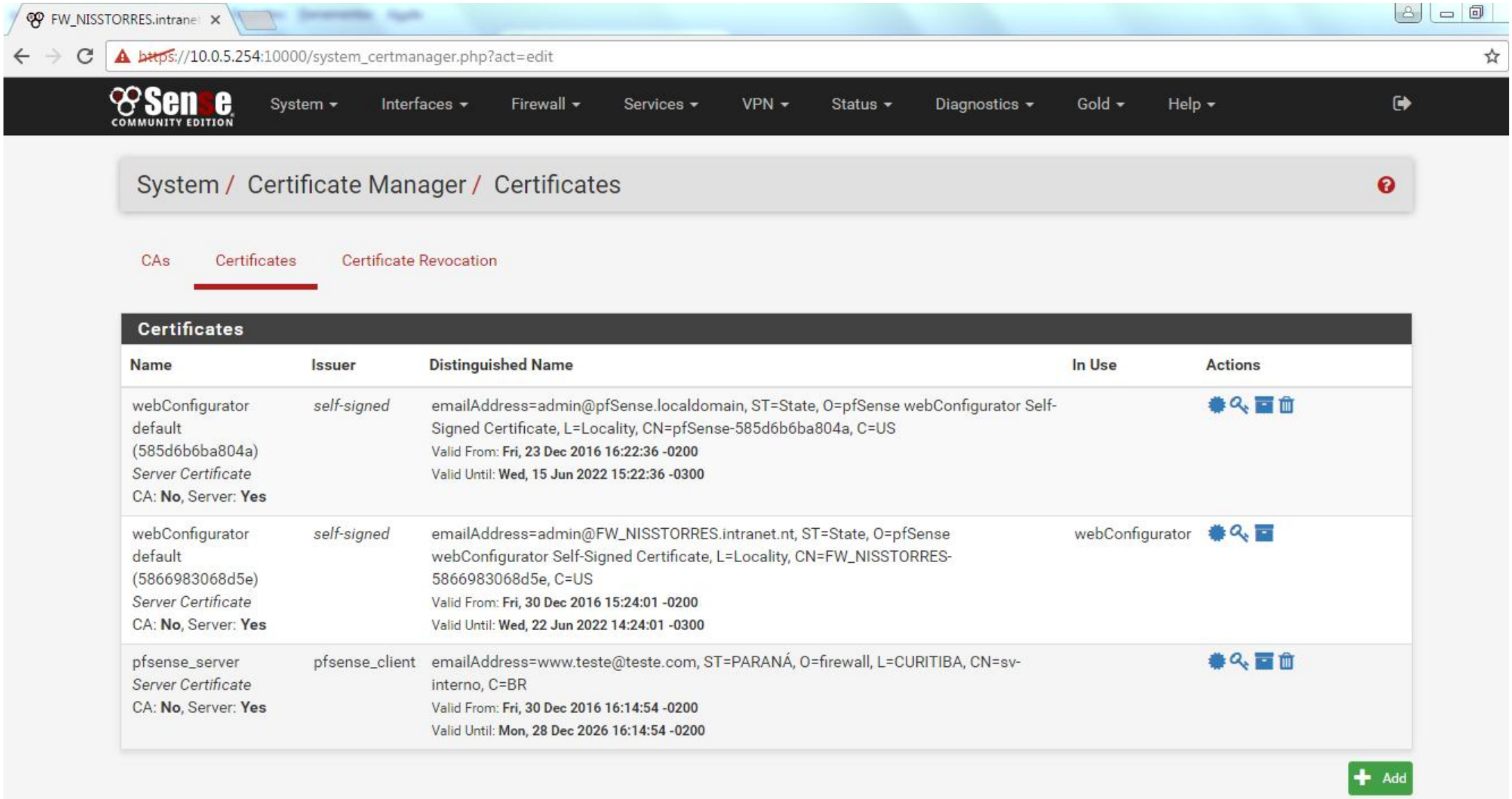
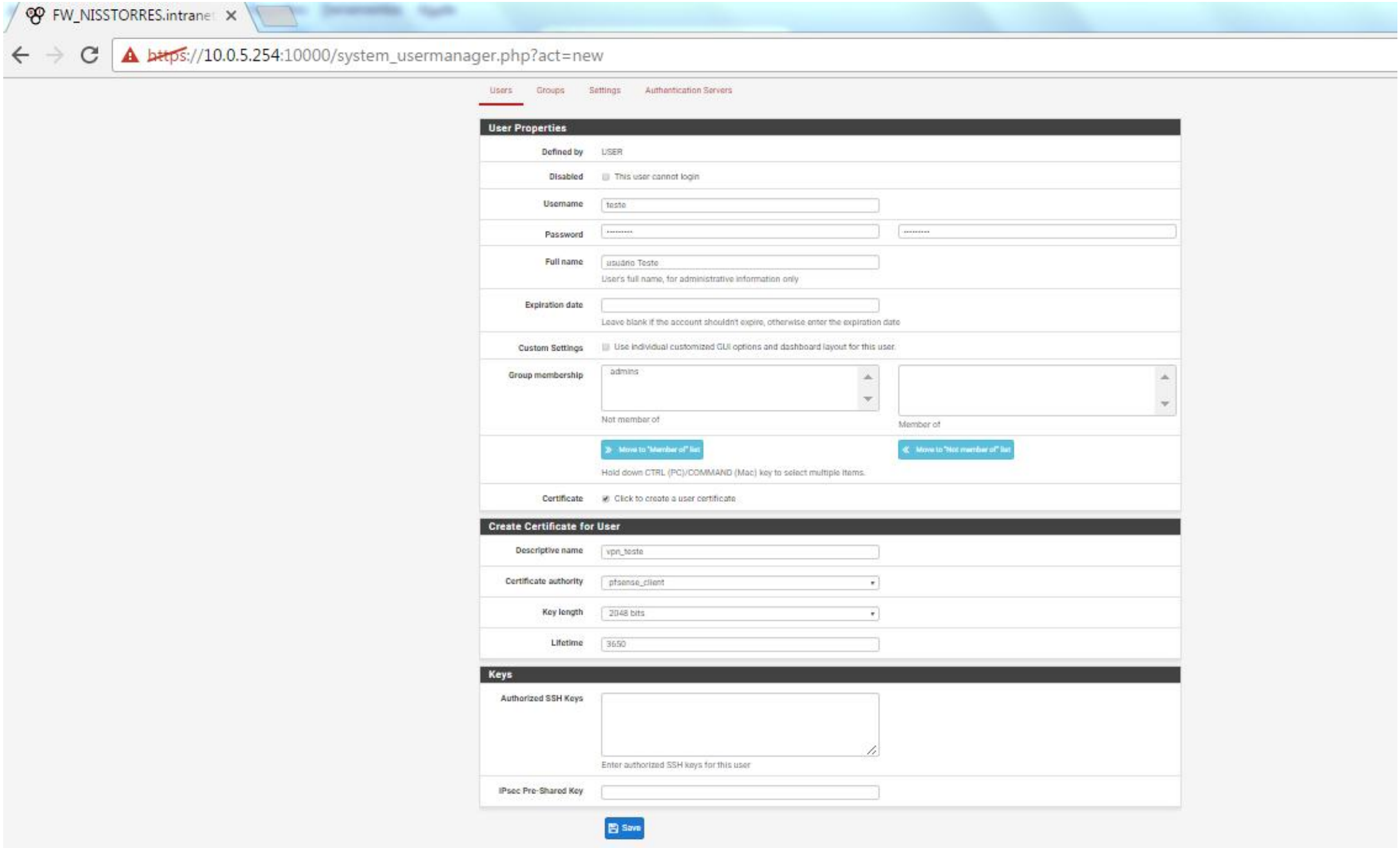
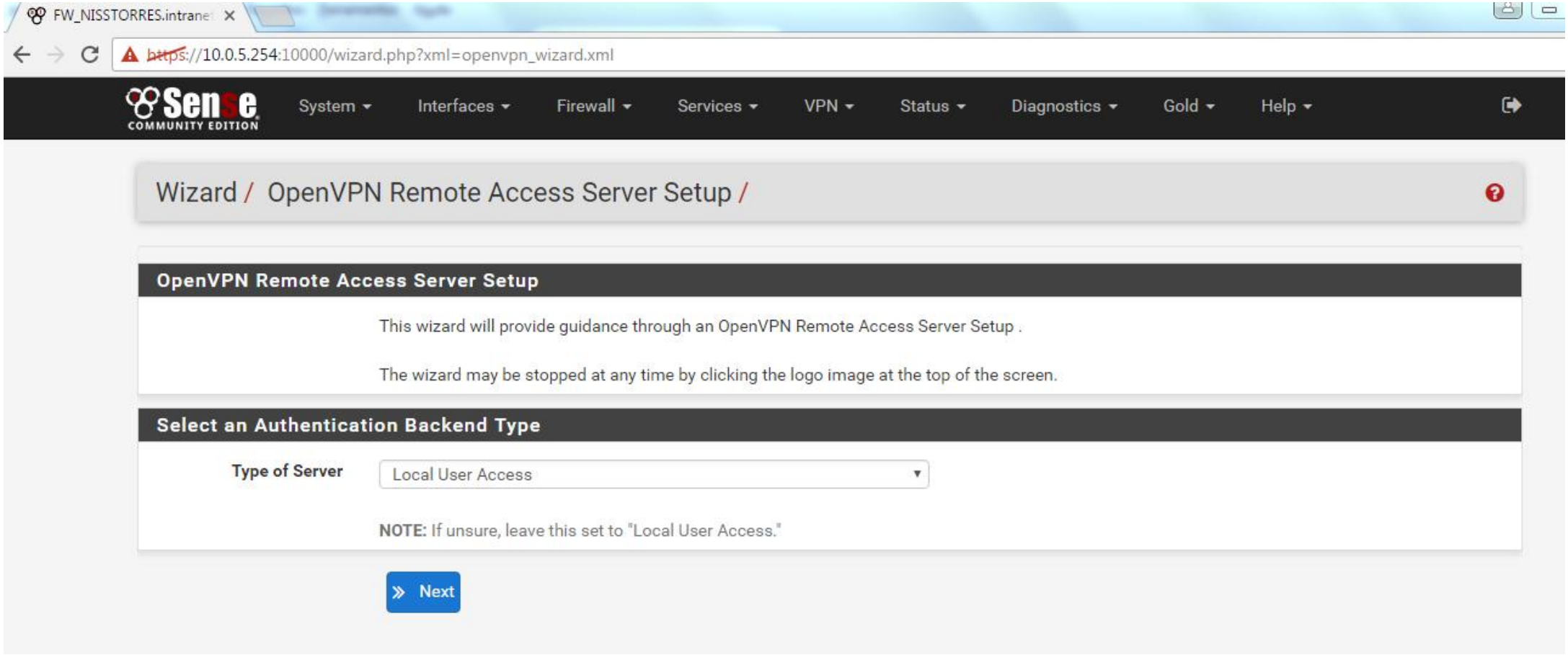

FW_NISSTORRES.intranet
https://10.0.5.254:10000/system_camanager.php?act=new
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
System / Certificate Manager / CAs / Edit
CAs
Certificates
Certificate Revocation
Create / Edit CA
Descriptive name
pfsense_client
Method
Create an internal Certificate Authority
Internal Certificate Authority
Key length (bits)
2048
Digest Algorithm
sha256
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.
Lifetime (days)
3650
Country Code
BR
State or Province
PARANÁ
City
CURITIBA
Organization
firewall
Organizational Unit
e.g. My Department Name (optional)
Email Address
www.teste@teste.com
Common Name
ca-interno
Save

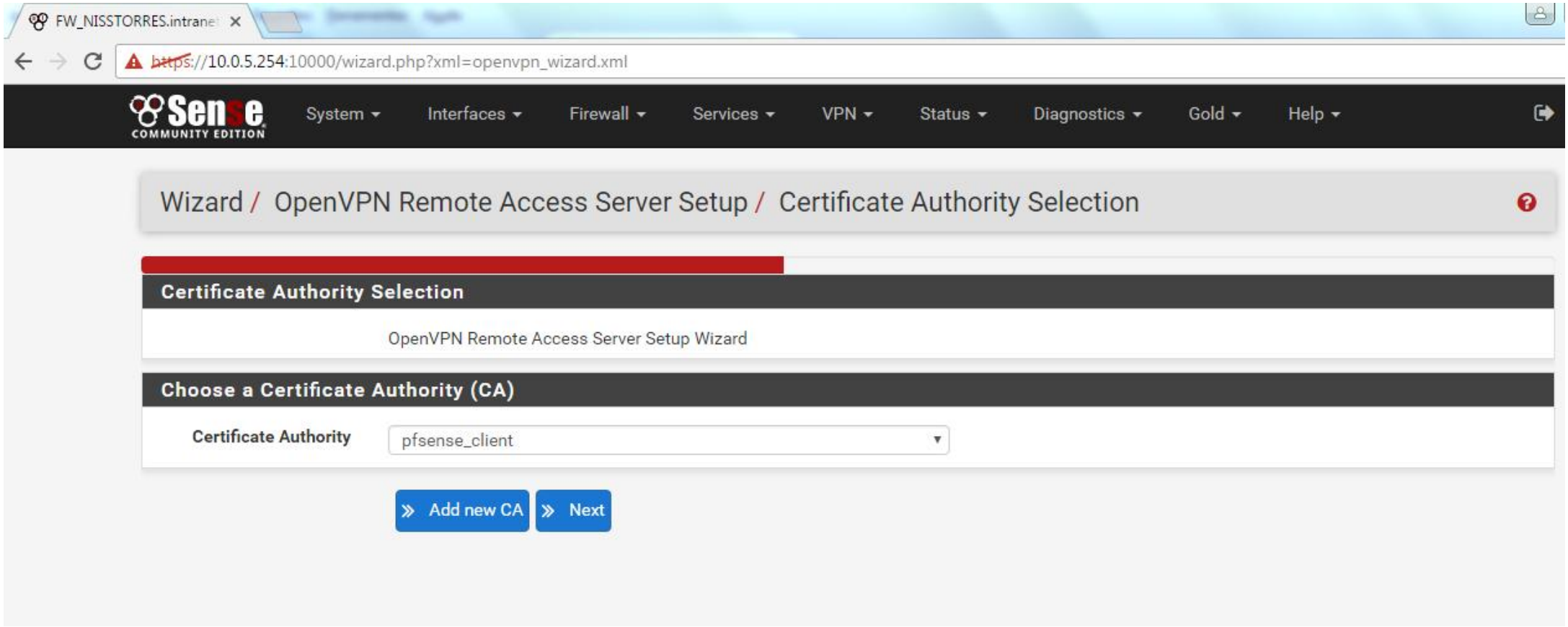

FW_NISSTORRES.intrane
https://10.0.5.254:10000/system_camanager.php
Sense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
System / Certificate Manager / CAs
CAs
Certificates
Certificate Revocation
Certificate Authorities
Name
Internal
Issuer
Certificates
Distinguished Name
Actions
pfsense_client
self-signed
0
emailAddress=www.teste@teste.com, ST=PARANÁ, O=firewall, L=CURITIBA, CN=ca-interno, C=BR
Valid From: Fri, 30 Dec 2016 16:08:47 -0200
Valid Until: Mon, 28 Dec 2026 16:08:47 -0200
Add

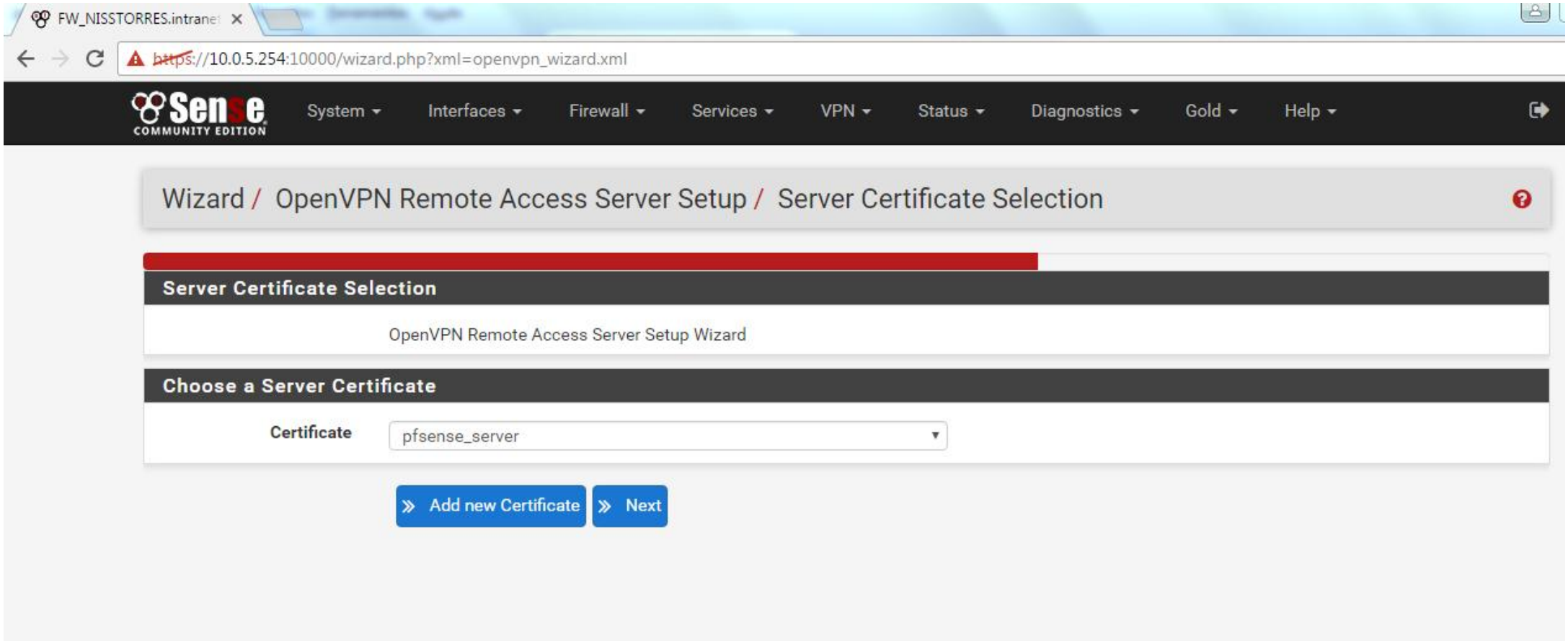

FW_NISSTORRES.intranet
https://10.0.5.254:10000/system_certmanager.php?act=new
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
System / Certificate Manager / Certificates / Edit
CAs
Certificates
Certificate Revocation
Add a New Certificate
Method
Create an internal Certificate
Descriptive name
pfsense_server
Internal Certificate
Certificate authority
pfsense_client
Key length
2048
Digest Algorithm
sha256
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.
Certificate Type
Server Certificate
Type of certificate to generate. Used for placing restrictions on the usage of the generated certificate.
Lifetime (days)
3650
Country Code
BR
State or Province
PARANÁ
City
CURITIBA
Organization
firewall
Organizational Unit
e.g. My Department Name (optional)
Email Address
www.teste@teste.com
Common Name
sv-interno
Alternative Names
FQDN or Hostname
www.maupfsense.com.br
Delete
IP address
10.0.5.254
Type
Value
Delete
Add
Add
Save

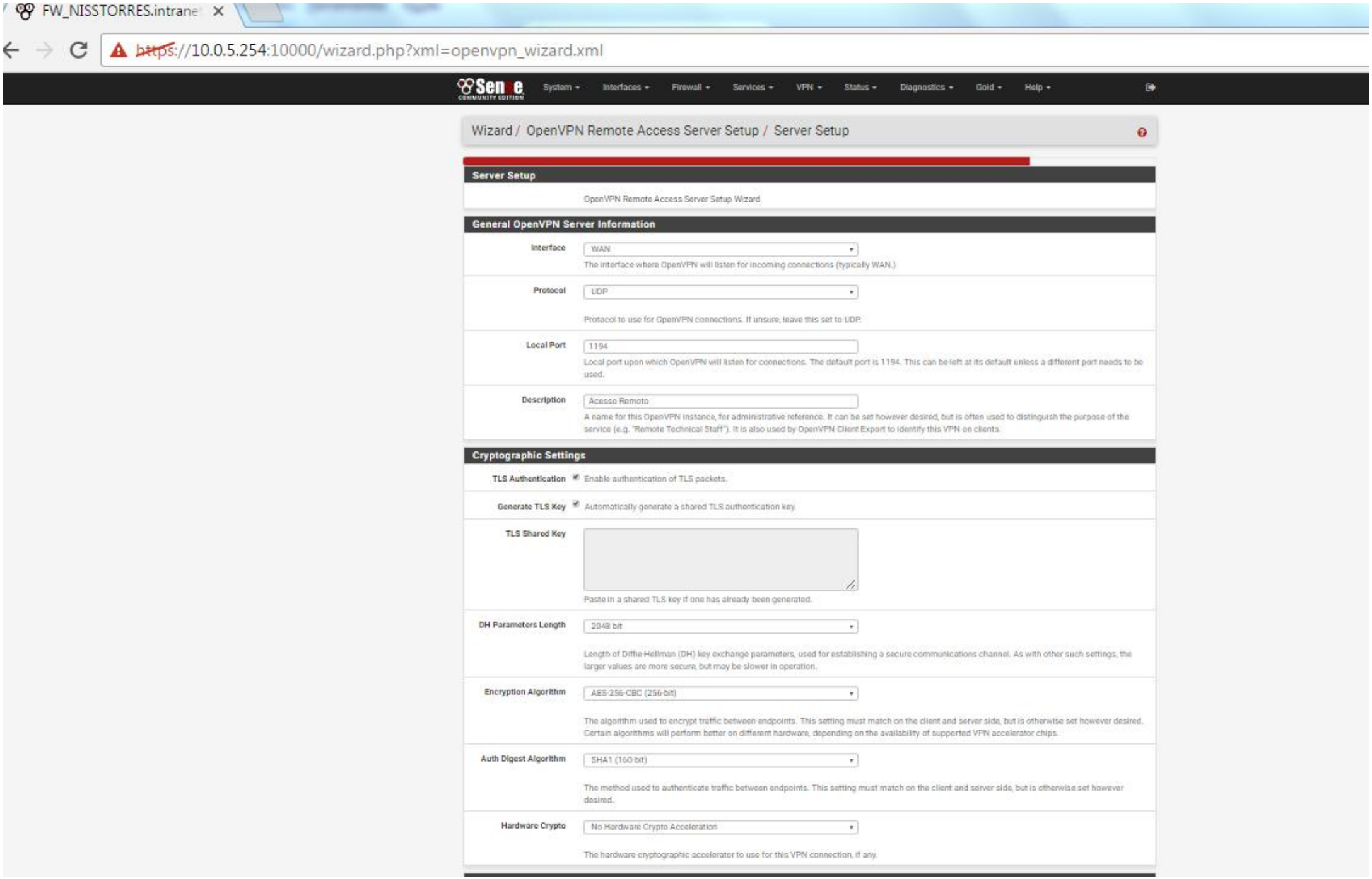

FW_NISSTORRES.intranet
https://10.0.5.254:10000/system_certmanager.php?act=edit
pfSense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
System / Certificate Manager / Certificates
CAs
Certificates
Certificate Revocation
Certificates
Name
Issuer
Distinguished Name
In Use
Actions
webConfigurator default (585d6b6ba804a)
Server Certificate
CA: No, Server: Yes
self-signed
emailAddress=admin@pfSense.localdomain, ST=State, O=pfSense webConfigurator Self-Signed Certificate, L=Locality, CN=pfSense-585d6b6ba804a, C=US
Valid From: Fri, 23 Dec 2016 16:22:36 -0200
Valid Until: Wed, 15 Jun 2022 15:22:36 -0300
webConfigurator default (5866983068d5e)
Server Certificate
CA: No, Server: Yes
self-signed
emailAddress=admin@FW_NISSTORRES.intranet.nt, ST=State, O=pfSense webConfigurator Self-Signed Certificate, L=Locality, CN=FW_NISSTORRES-5866983068d5e, C=US
Valid From: Fri, 30 Dec 2016 15:24:01 -0200
Valid Until: Wed, 22 Jun 2022 14:24:01 -0300
webConfigurator
pfsense_server
Server Certificate
CA: No, Server: Yes
pfsense_client
emailAddress=www.teste@teste.com, ST=PARANÁ, O=firewall, L=CURITIBA, CN=sv-interno, C=BR
Valid From: Fri, 30 Dec 2016 16:14:54 -0200
Valid Until: Mon, 28 Dec 2026 16:14:54 -0200
Add

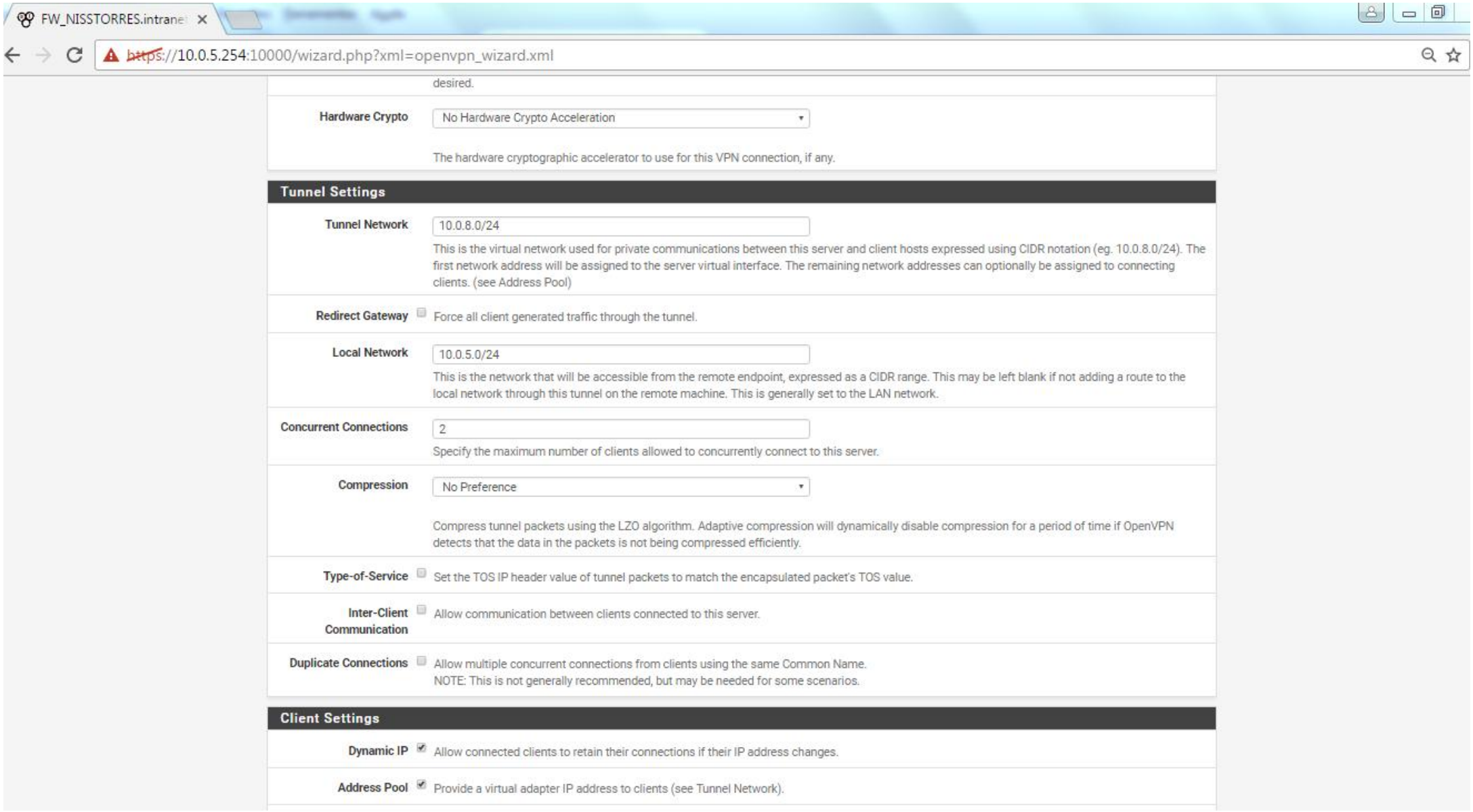

FW_NISSTORRES.intranet
https://10.0.5.254:10000/system_usermanager.php?act=new
Users
Groups
Settings
Authentication Servers
User Properties
Defined by
USER
Disabled
This user cannot login
Username
teste
Password
Full name
usuário Teste
Users full name, for administrative information only
Expiration date
Leave blank if the account shouldn't expire, otherwise enter the expiration date
Custom Settings
Use individual customized GUI options and dashboard layout for this user.
Group membership
admins
Not member of
Member of
Move to "Member of" list
Move to "Not member of" list
Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.
Certificate
Click to create a user certificate
Create Certificate for User
Descriptive name
vpn_teste
Certificate authority
pfsense_client
Key length
2048 bits
Lifetime
3650
Keys
Authorized SSH Keys
Enter authorized SSH keys for this user
IPsec Pre-Shared Key
Save

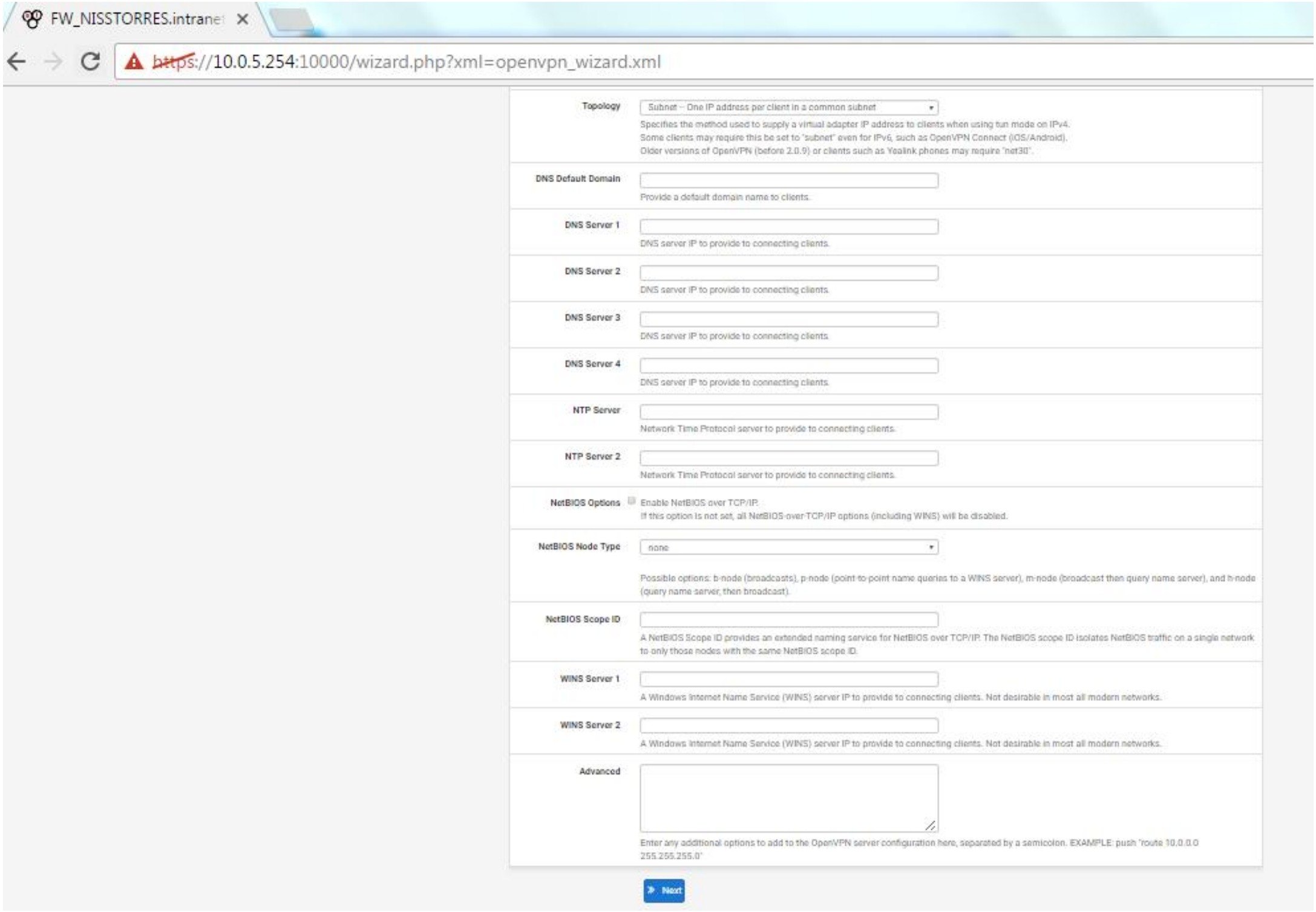

FW_NISSTORRES.intrane
https://10.0.5.254:10000/wizard.php?xml=openvpn_wizard.xml
pfSense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Wizard / OpenVPN Remote Access Server Setup /
OpenVPN Remote Access Server Setup
This wizard will provide guidance through an OpenVPN Remote Access Server Setup .
The wizard may be stopped at any time by clicking the logo image at the top of the screen.
Select an Authentication Backend Type
Type of Server
Local User Access
NOTE: If unsure, leave this set to "Local User Access."
Next

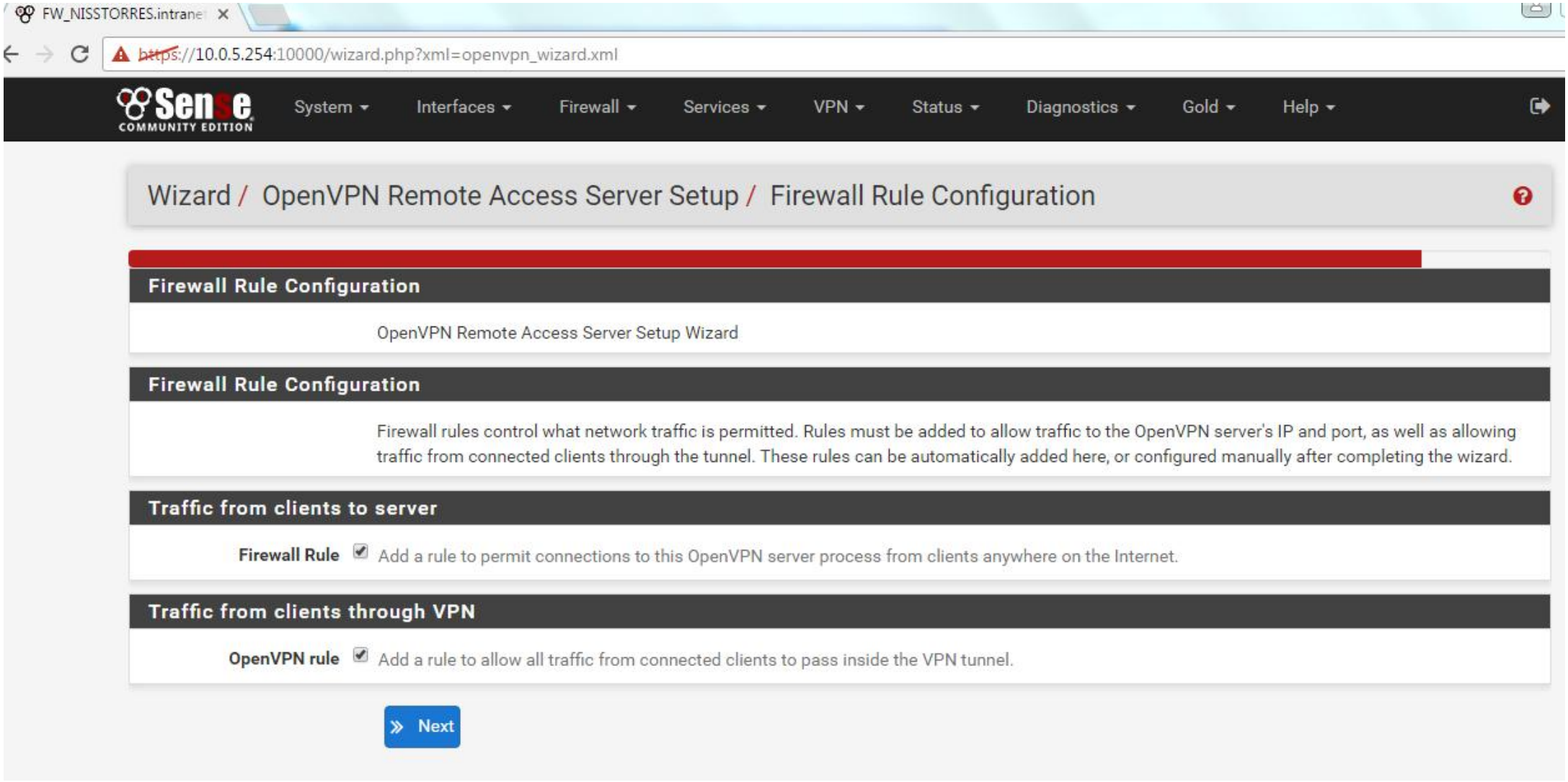

FW_NISSTORRES.intrane
https://10.0.5.254:10000/wizard.php?xml=openvpn_wizard.xml
Sense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Wizard / OpenVPN Remote Access Server Setup / Certificate Authority Selection
Certificate Authority Selection
OpenVPN Remote Access Server Setup Wizard
Choose a Certificate Authority (CA)
Certificate Authority
pfsense_client
Add new CA
Next

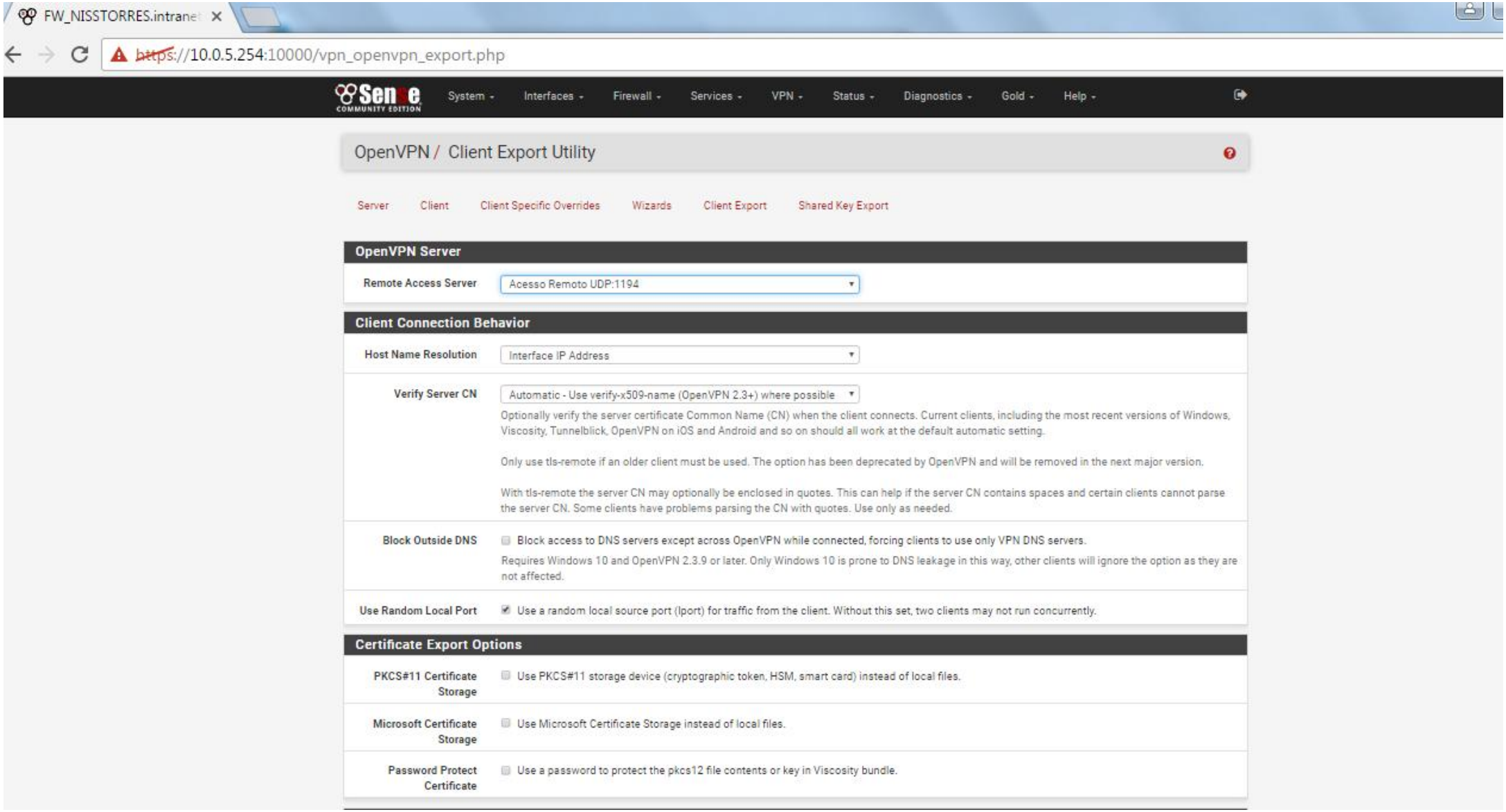

FW_NISSTORRES.intrane
https://10.0.5.254:10000/wizard.php?xml=openvpn_wizard.xml
Sense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Wizard / OpenVPN Remote Access Server Setup / Server Certificate Selection
Server Certificate Selection
OpenVPN Remote Access Server Setup Wizard
Choose a Server Certificate
Certificate
pfsense_server
Add new Certificate
Next

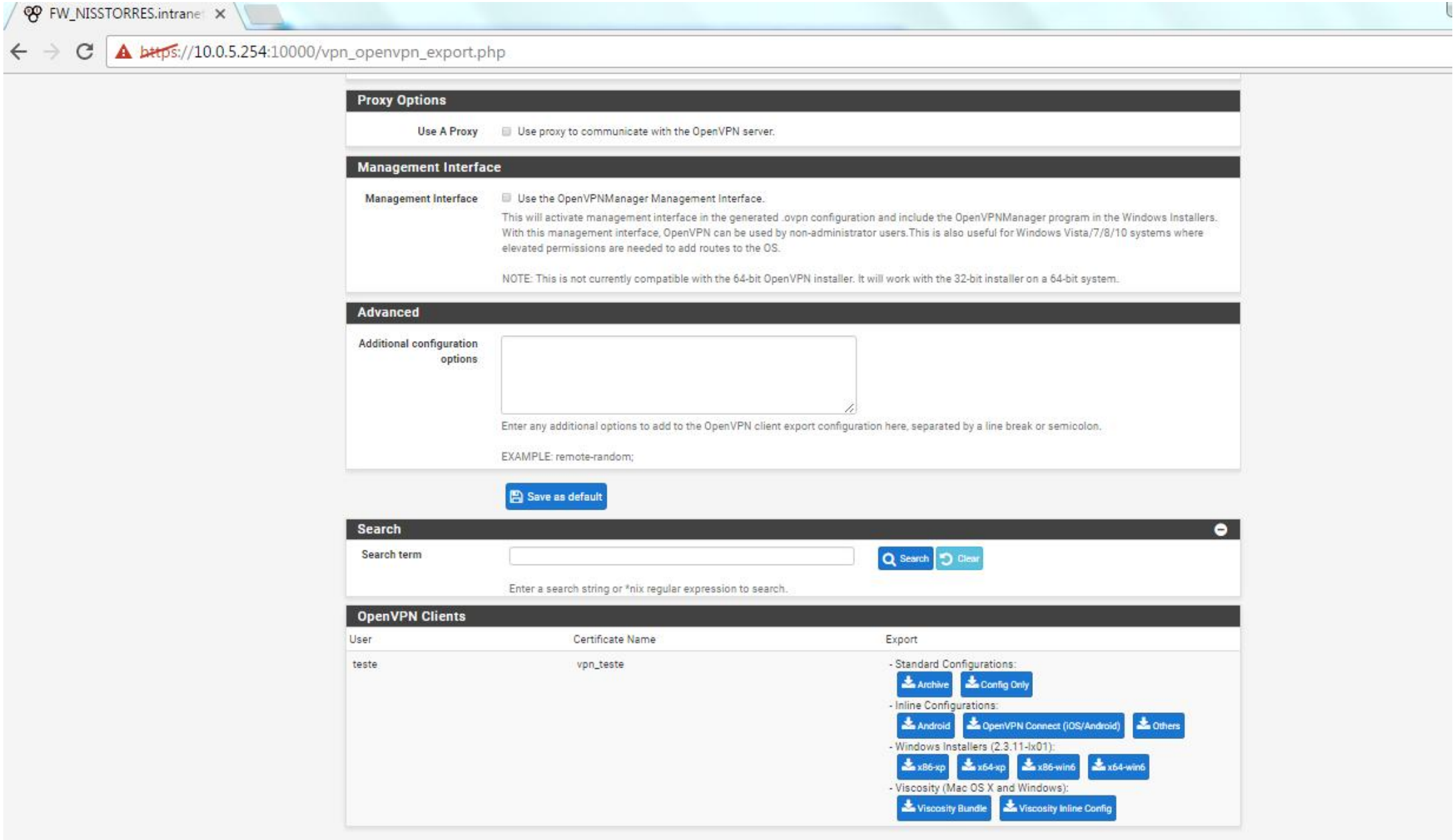

FW_NISSTORRES.intrane
https://10.0.5.254:10000/wizard.php?xml=openvpn_wizard.xml
pfSense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Wizard / OpenVPN Remote Access Server Setup / Server Setup
Server Setup
OpenVPN Remote Access Server Setup Wizard
General OpenVPN Server Information
Interface
WAN
The interface where OpenVPN will listen for incoming connections (typically WAN.)
Protocol
UDP
Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.
Local Port
1194
Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.
Description
Acesso Remoto
A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.
Cryptographic Settings
TLS Authentication
Enable authentication of TLS packets.
Generate TLS Key
Automatically generate a shared TLS authentication key.
TLS Shared Key
Paste in a shared TLS key if one has already been generated.
DH Parameters Length
2048 bit
Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. As with other such settings, the larger values are more secure, but may be slower in operation.
Encryption Algorithm
AES-256-CBC (256-bit)
The algorithm used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.
Auth Digest Algorithm
SHA1 (160-bit)
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.


FW_NISSTORRES.intrane
https://10.0.5.254:10000/wizard.php?xml=openvpn_wizard.xml
desired.
Hardware Crypto
No Hardware Crypto Acceleration
The hardware cryptographic accelerator to use for this VPN connection, if any.
Tunnel Settings
Tunnel Network
10.0.8.0/24
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 can optionally be assigned to connecting clients. (see Address Pool)
Redirect Gateway
Force all client generated traffic through the tunnel.
Local Network
10.0.5.0/24
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
No Preference
Compress tunnel packets using the LZO 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.
Client Settings
Dynamic IP
Allow connected clients to retain their connections if their IP address changes.
Address Pool
Provide a virtual adapter IP address to clients (see Tunnel Network).


FW_NISSTORRES.intranet
https://10.0.5.254:10000/wizard.php?xml=openvpn_wizard.xml
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
Provide a default domain name to clients.
DNS Server 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
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
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
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
A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
WINS Server 2
A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
Advanced
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"
Next


FW_NISSTORRES.intrane
https://10.0.5.254:10000/wizard.php?xml=openvpn_wizard.xml
Sense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration
Firewall Rule Configuration
OpenVPN Remote Access Server Setup Wizard
Firewall Rule Configuration
Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.
Traffic from clients to server
Firewall Rule
Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.
Traffic from clients through VPN
OpenVPN rule
Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.
Next


FW_NISSTORRES.intrane
https://10.0.5.254:10000/vpn_openvpn_export.php
Sense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
OpenVPN / Client Export Utility
Server
Client
Client Specific Overrides
Wizards
Client Export
Shared Key Export
OpenVPN Server
Remote Access Server
Acesso Remoto UDP:1194
Client Connection Behavior
Host Name Resolution
Interface IP Address
Verify Server CN
Automatic - Use verify-x509-name (OpenVPN 2.3+) where possible
Optionally verify the server certificate Common Name (CN) when the client connects. Current clients, including the most recent versions of Windows, Viscosity, Tunnelblick, OpenVPN on iOS and Android and so on should all work at the default automatic setting.
Only use tls-remote if an older client must be used. The option has been deprecated by OpenVPN and will be removed in the next major version.
With tls-remote the server CN may optionally be enclosed in quotes. This can help if the server CN contains spaces and certain clients cannot parse the server CN. Some clients have problems parsing the CN with quotes. Use only as needed.
Block Outside DNS
Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.
Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.
Use Random Local Port
Use a random local source port (lport) for traffic from the client. Without this set, two clients may not run concurrently.
Certificate Export Options
PKCS#11 Certificate Storage
Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.
Microsoft Certificate Storage
Use Microsoft Certificate Storage instead of local files.
Password Protect Certificate
Use a password to protect the pkcs12 file contents or key in Viscosity bundle.


FW_NISSTORRES.intrane
https://10.0.5.254:10000/vpn_openvpn_export.php
Proxy Options
Use A Proxy
Use proxy to communicate with the OpenVPN server.
Management Interface
Management Interface
Use the OpenVPNManager Management Interface.
This will activate management interface in the generated .ovpn configuration and include the OpenVPNManager program in the Windows Installers. With this management interface, OpenVPN can be used by non-administrator users.This is also useful for Windows Vista/7/8/10 systems where elevated permissions are needed to add routes to the OS.
NOTE: This is not currently compatible with the 64-bit OpenVPN installer. It will work with the 32-bit installer on a 64-bit system.
Advanced
Additional configuration options
Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon.
EXAMPLE: remote-random;
Save as default
Search
Search term
Search
Clear
Enter a search string or *nix regular expression to search.
OpenVPN Clients
User
Certificate Name
Export
teste
vpn_teste
- Standard Configurations:
Archive
Config Only
- Inline Configurations:
Android
OpenVPN Connect (iOS/Android)
Others
- Windows Installers (2.3.11-Ix01):
x86-xp
x64-xp
x86-win6
x64-win6
- Viscosity (Mac OS X and Windows):
Viscosity Bundle
Viscosity Inline Config