Firewall pfSense
základy administrace

LinuxDays 2017 - Lukáš Malý

O projektu pfSense

- Firewall distribuce – vystavěná na FreeBSD
- Využívá mnoho dalších Open Source projektů
- **pf** (Packet Filter) **Sense** – stavový firewall
- **pf** vyvíjen jako součást OpenBSD
- Předchůdce IPFilter – IPF - IPWF
- Packet Filter poprvé ve FreeBSD 5.3
- **IPFW > IPF > PF**

Historie projektu

- Vznikl v roce **2004** jako fork m0n0wall
- Chris Buechler a Scott Ullrich
- BSD Perimeter LLC
- **2014** pfSense - Electric Sheep Fencing LLC (**ESF**)
- **ESF** Contributor License Agreement
- **2015** Europe OPNsense project
- **2016** Rubicon Communications, LLC

Licence

- BSD licence
- **2014 -** BSD + **ESF** licence
- **2016 -** Apache 2.0 license + **ESF** licence

- **ESF Contributor License Agreement**
- Individual Contributor License Agreement (ICLA)
- Corporate Contributor License Agreement (CCLA)

Firewall pfSense

- Obraz (ISO) s instalátorem
- Memstick obraz s instalátorem – USB Flash
- Embedded (NanoBSD) pro CF – bude ukončena podpora
- amd64, i386
- **pfSense 2.3.4-RELEASE-p1** - FreeBSD 10.3-RELEASE-p19
- ARM ve verzi 2.4.0 – SG-1000 a SG-3100
- Ukončení podpory - i386 a NanoBSD

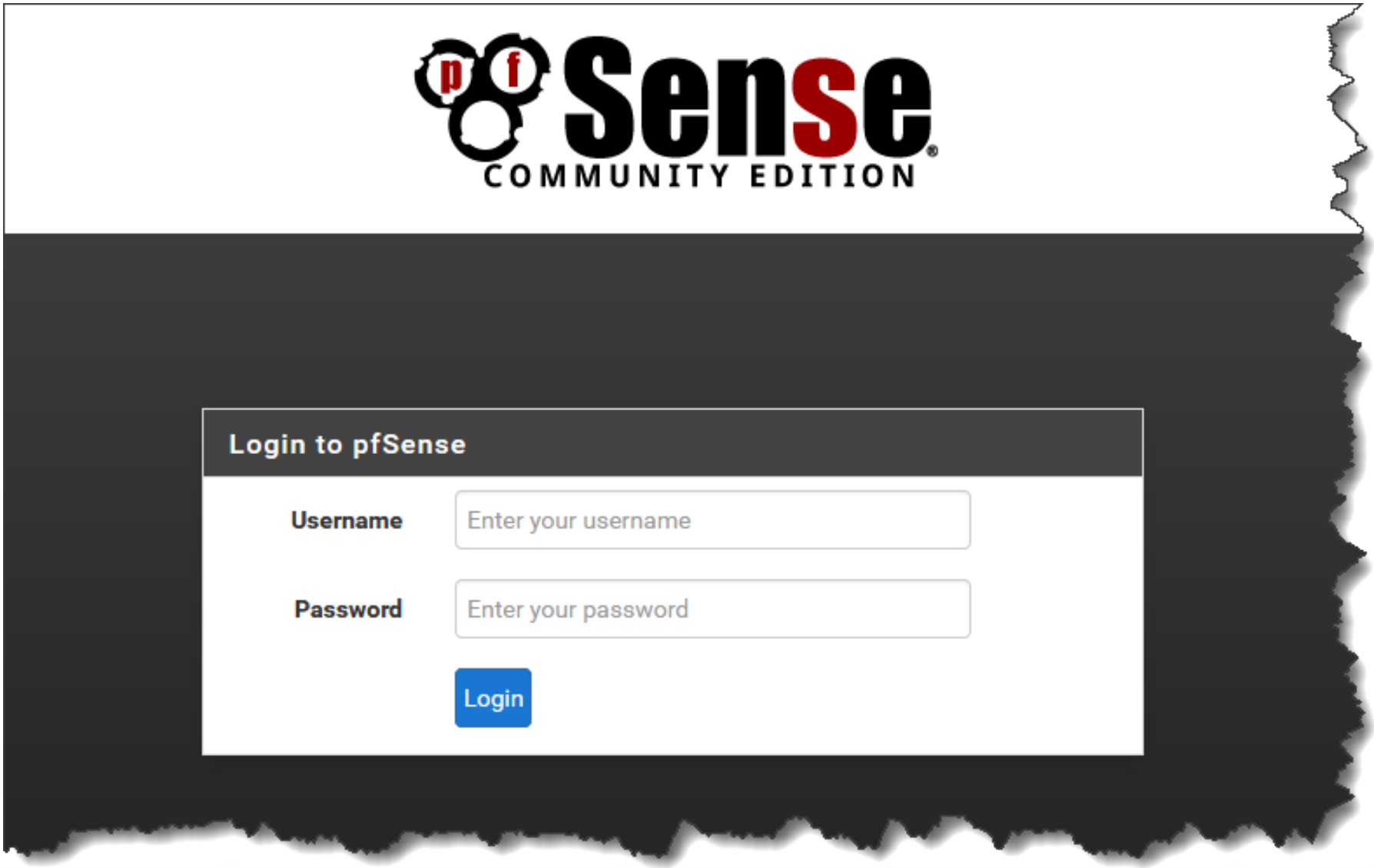
pfSense hardware

- **Běžný dostupný hardware**
- FreeBSD 10.3-RELEASE Hardware Notes
- https://www.freebsd.org/releases/10.3R/hardware.html
- amd64, i386
- PC Engines APU a APU2
- FabiaTech
- Industrial Mini PC Computer

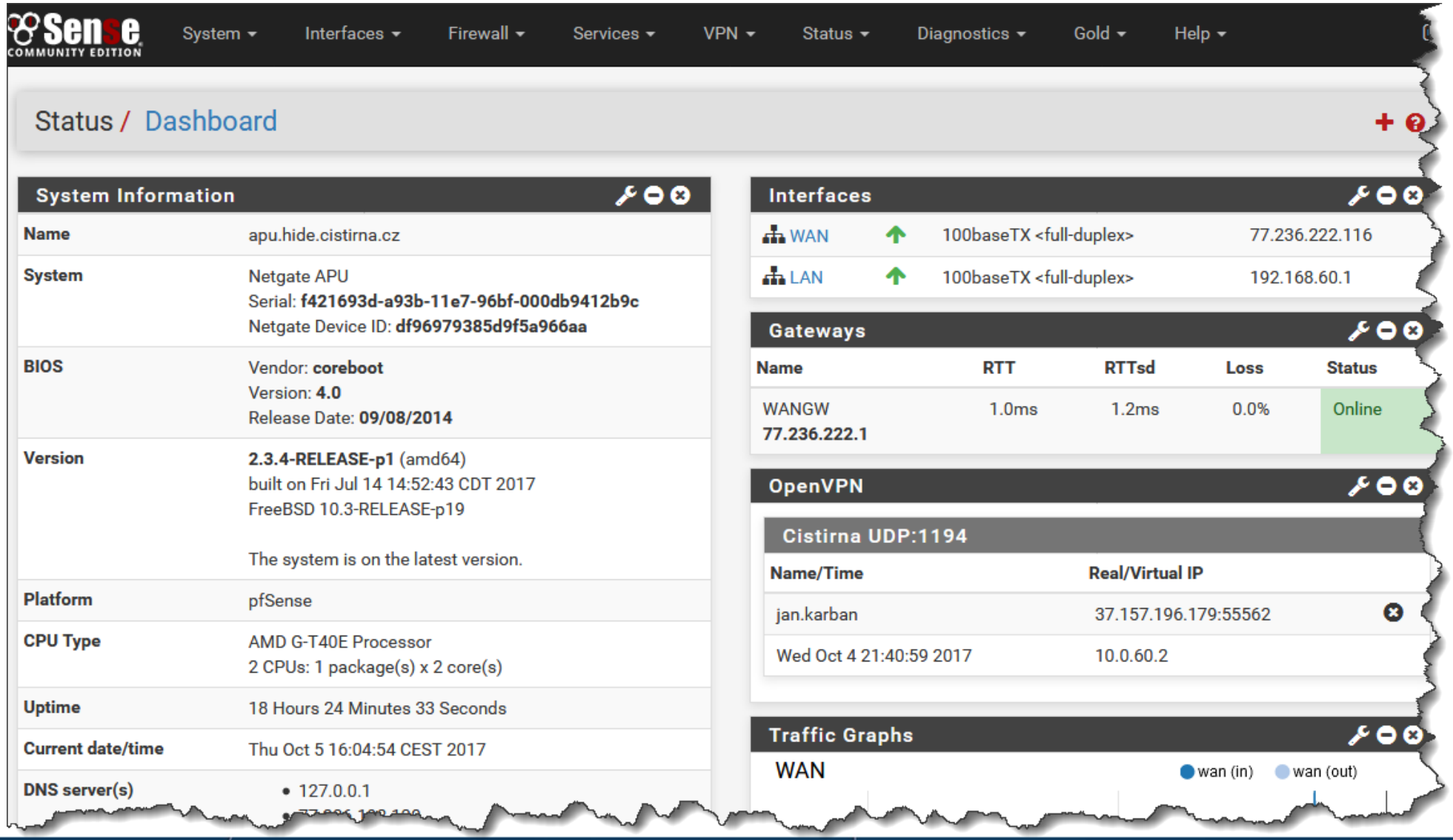
pfSense hardware

- Netgate pfSense Security Gateway Appliances
- **SG-*** SOHO/SMB – Remote Office
- **XG-*** Enterprice – High Availability
- **RCC-*** Netgate HW
- **Cloud**
- pfSense for Amazon AWS
- pfSense for Microsoft Azure
- pfSense for VMware

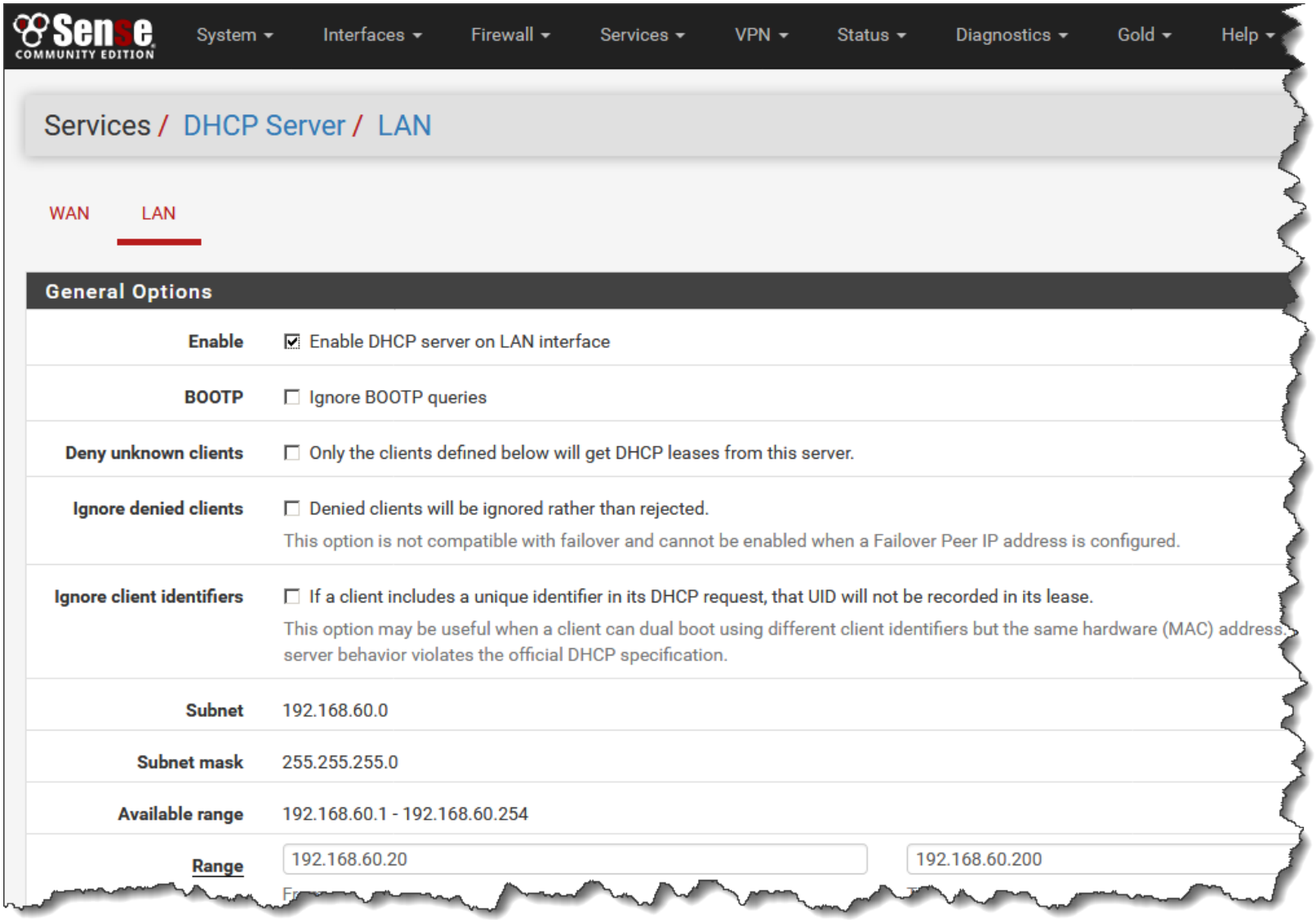
WebGUI - Login



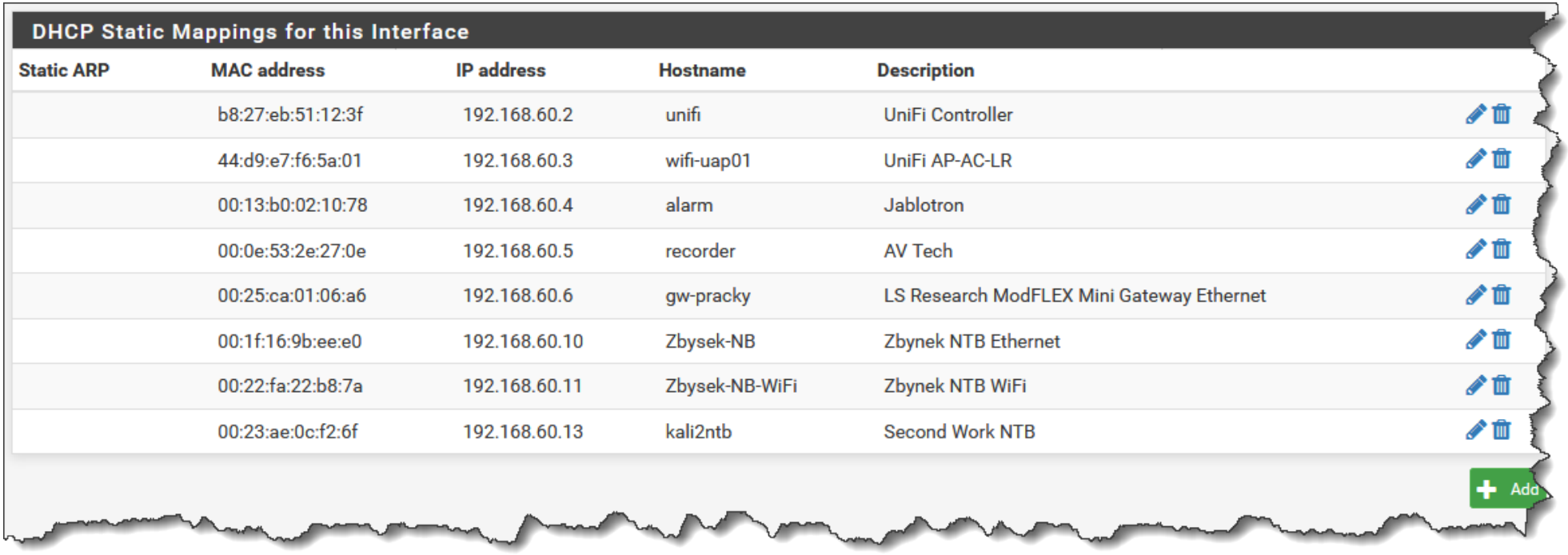
Dashboard


Sense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Status / Dashboard
System Information
Name
apu.hide.cistirna.cz
System
Netgate APU
Serial: f421693d-a93b-11e7-96bf-000db9412b9c
Netgate Device ID: df96979385d9f5a966aa
BIOS
Vendor: coreboot
Version: 4.0
Release Date: 09/08/2014
Version
2.3.4-RELEASE-p1 (amd64)
built on Fri Jul 14 14:52:43 CDT 2017
FreeBSD 10.3-RELEASE-p19
The system is on the latest version.
Platform
pfSense
CPU Type
AMD G-T40E Processor
2 CPUs: 1 package(s) x 2 core(s)
Uptime
18 Hours 24 Minutes 33 Seconds
Current date/time
Thu Oct 5 16:04:54 CEST 2017
DNS server(s)
127.0.0.1
Interfaces
WAN
100baseTX <full-duplex>
77.236.222.116
LAN
100baseTX <full-duplex>
192.168.60.1
Gateways
Name
RTT
RTTsd
Loss
Status
WANGW
77.236.222.1
1.0ms
1.2ms
0.0%
Online
OpenVPN
Cistirna UDP:1194
Name/Time
Real/Virtual IP
jan.karban
37.157.196.179:55562
Wed Oct 4 21:40:59 2017
10.0.60.2
Traffic Graphs
WAN
wan (in)
wan (out)

DHCPv4


Sense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Services / DHCP Server / LAN
WAN
LAN
General Options
Enable
Enable DHCP server on LAN interface
BOOTP
Ignore BOOTP queries
Deny unknown clients
Only the clients defined below will get DHCP leases from this server.
Ignore denied clients
Denied clients will be ignored rather than rejected.
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore client identifiers
If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address.
server behavior violates the official DHCP specification.
Subnet
192.168.60.0
Subnet mask
255.255.255.0
Available range
192.168.60.1 - 192.168.60.254
Range
192.168.60.20
192.168.60.200

DHCPv4 – Statické mapování

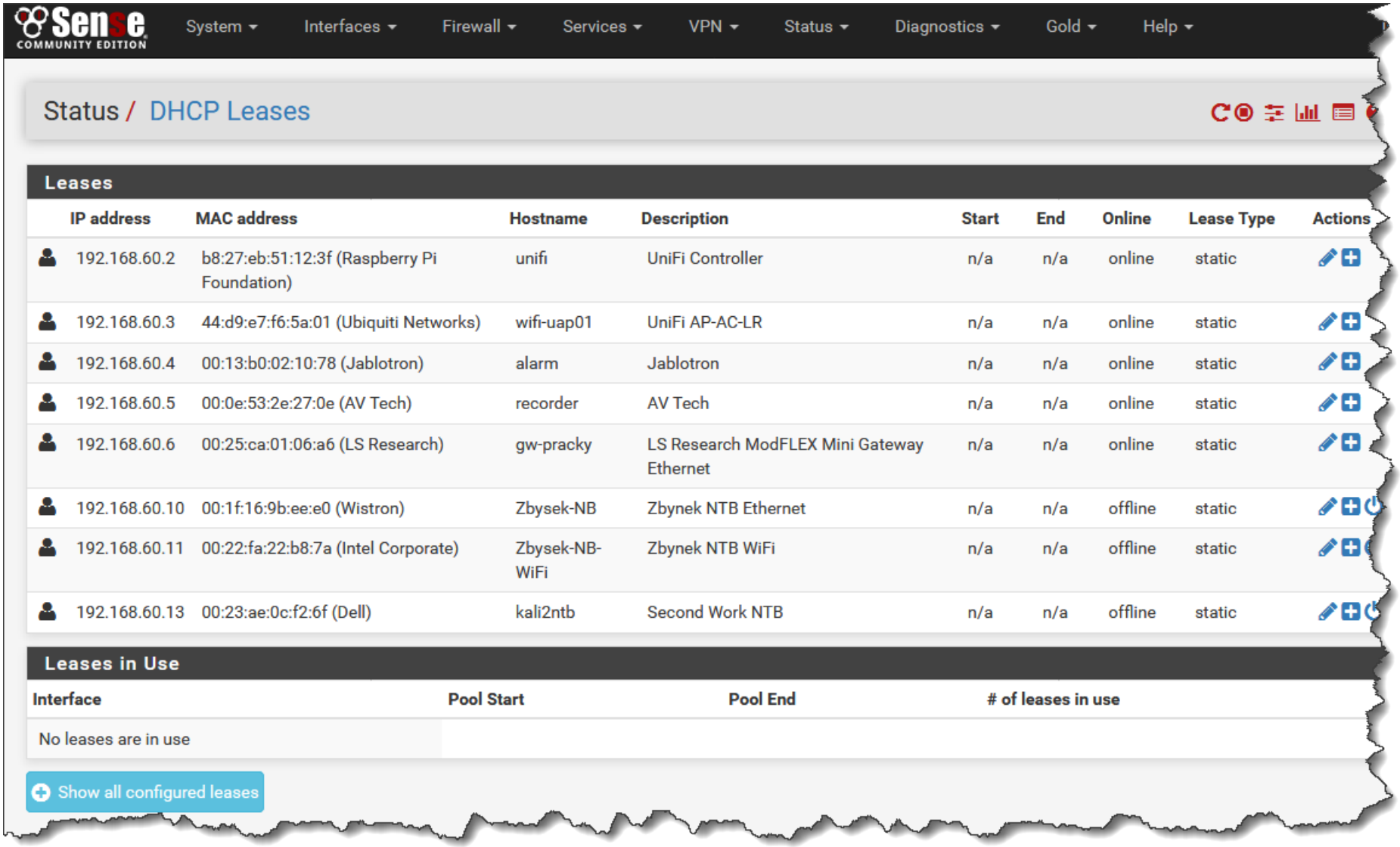


DHCP Static Mappings for this Interface

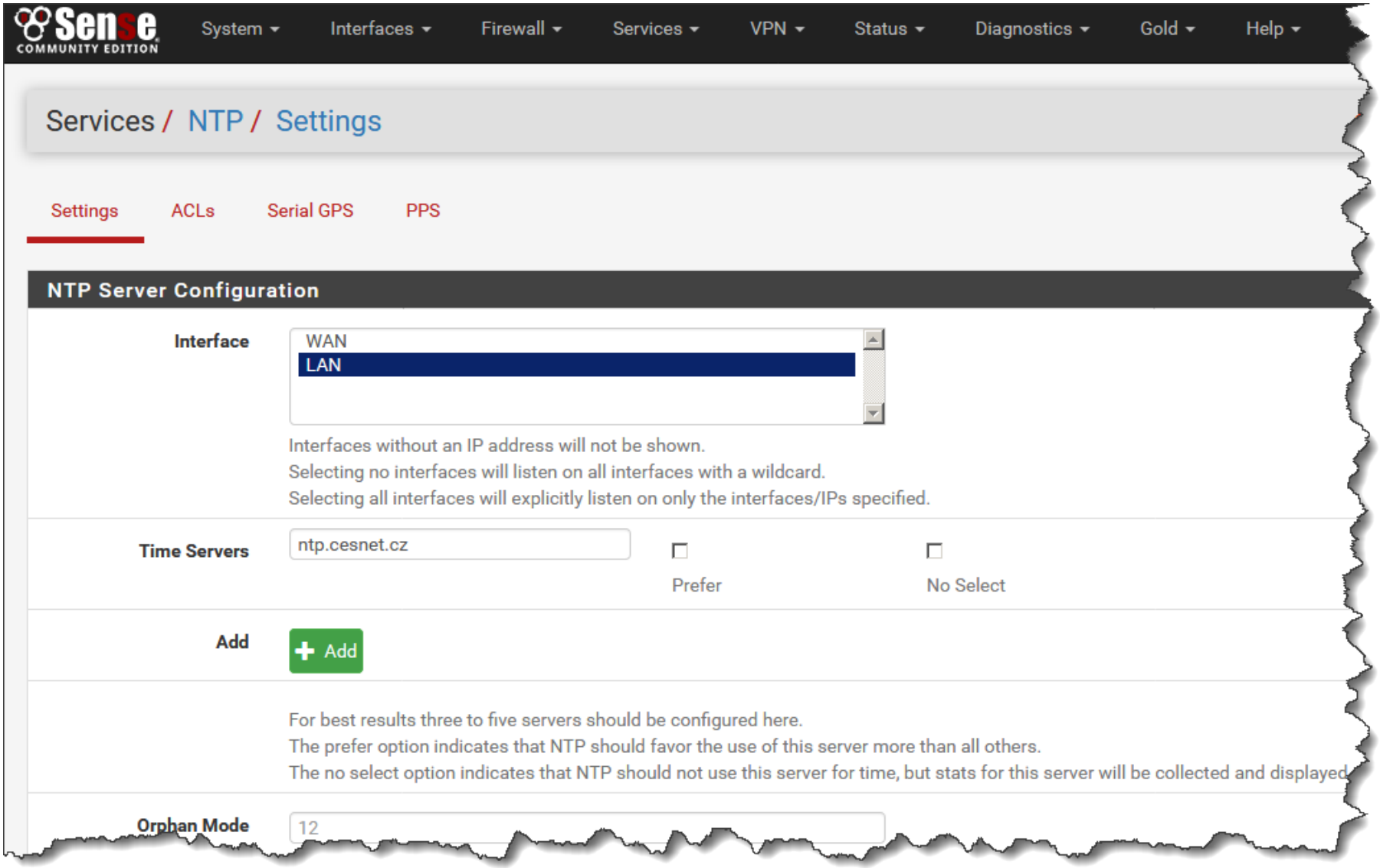
Static ARP	MAC address	IP address	Hostname	Description
	b8:27:eb:51:12:3f	192.168.60.2	unifi	UniFi Controller
	44:d9:e7:f6:5a:01	192.168.60.3	wifi-uap01	UniFi AP-AC-LR
	00:13:b0:02:10:78	192.168.60.4	alarm	Jablotron
	00:0e:53:2e:27:0e	192.168.60.5	recorder	AV Tech
	00:25:ca:01:06:a6	192.168.60.6	gw-pracky	LS Research ModFLEX Mini Gateway Ethernet
	00:1f:16:9b:ee:e0	192.168.60.10	Zbysek-NB	Zbynek NTB Ethernet
	00:22:fa:22:b8:7a	192.168.60.11	Zbysek-NB-WiFi	Zbynek NTB WiFi
	00:23:ae:0c:f2:6f	192.168.60.13	kali2ntb	Second Work NTB

Add

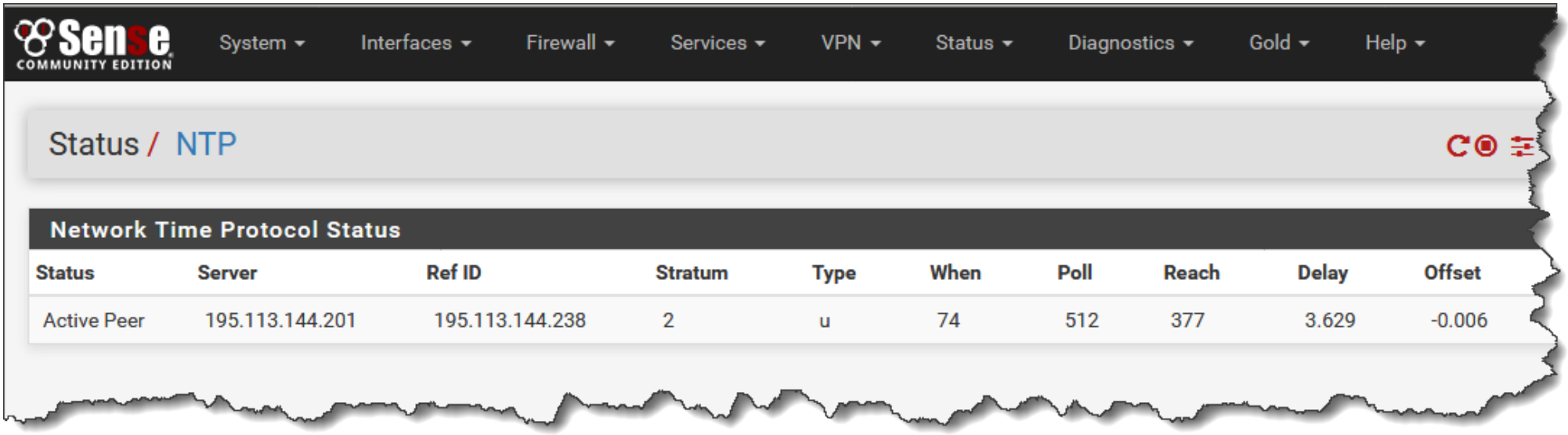
DHCPv4 – Leases



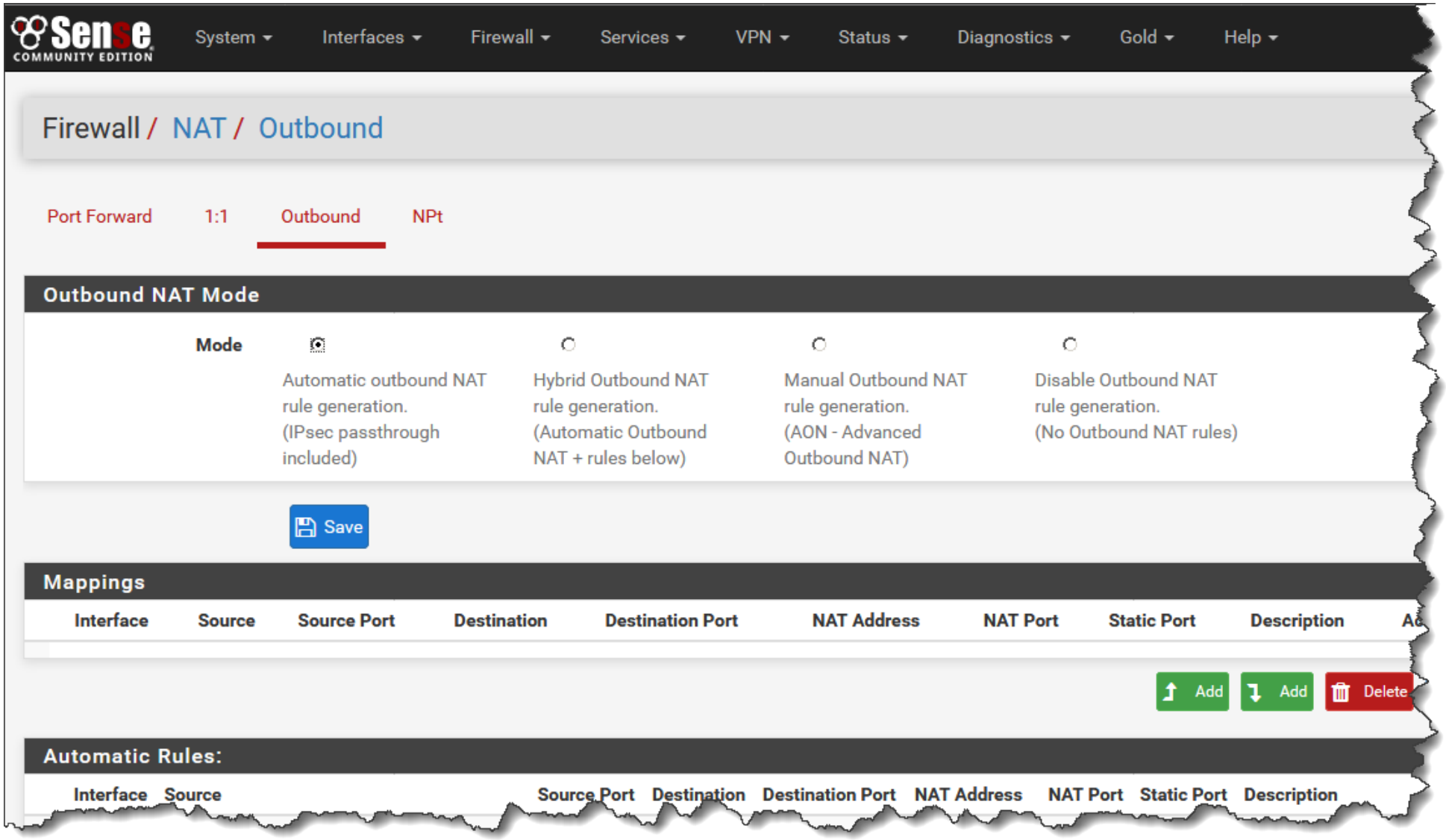
NTP


Sense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Services / NTP / Settings
Settings
ACLs
Serial GPS
PPS
NTP Server Configuration
Interface
WAN
LAN
Interfaces without an IP address will not be shown.
Selecting no interfaces will listen on all interfaces with a wildcard.
Selecting all interfaces will explicitly listen on only the interfaces/IPs specified.
Time Servers
ntp.cesnet.cz
Prefer
No Select
Add
Add
For best results three to five servers should be configured here.
The prefer option indicates that NTP should favor the use of this server more than all others.
The no select option indicates that NTP should not use this server for time, but stats for this server will be collected and displayed.
Orphan Mode
12

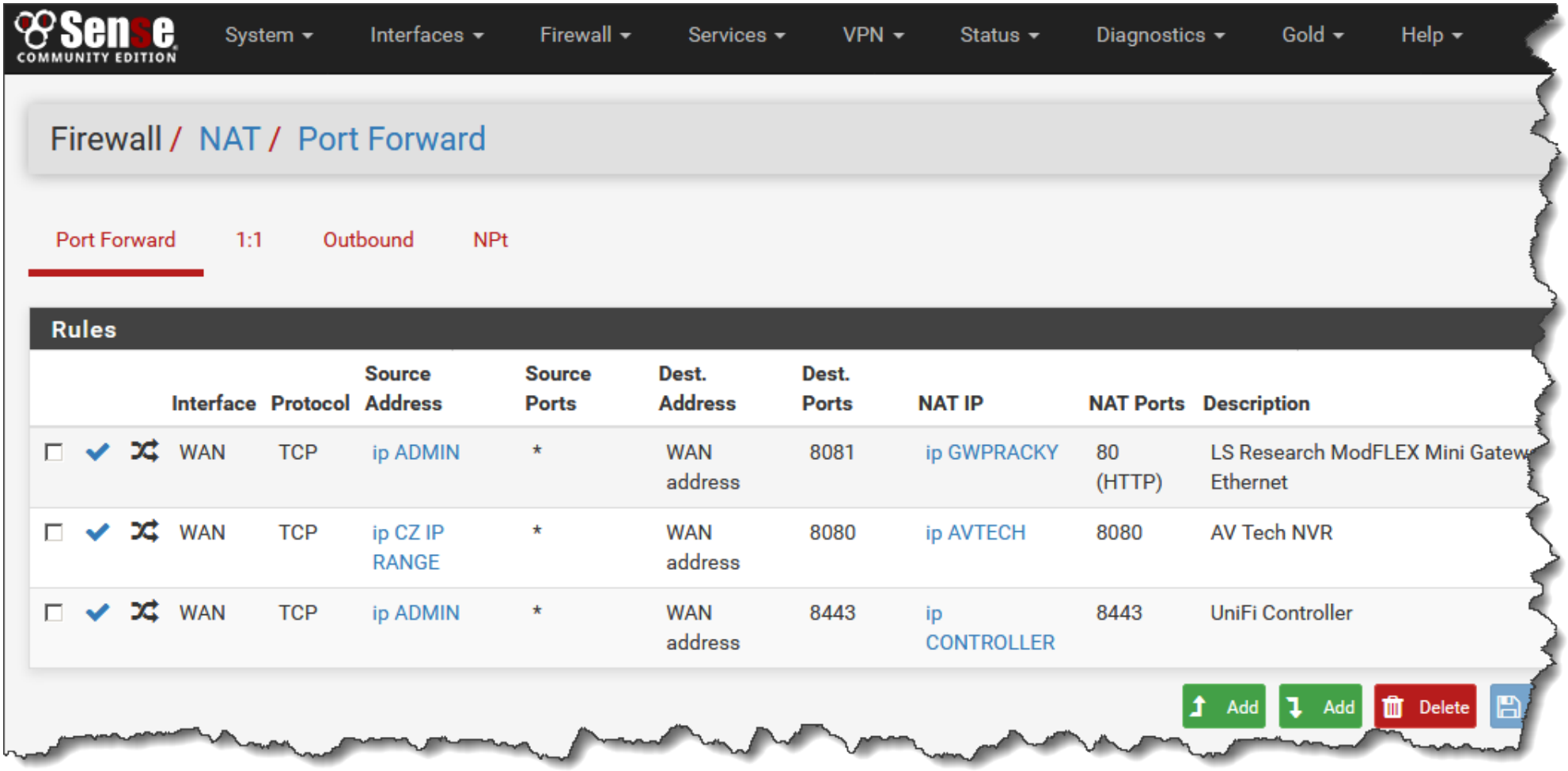
NTP - Status


Sense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Status / NTP
Network Time Protocol Status
Status
Server
Ref ID
Stratum
Type
When
Poll
Reach
Delay
Offset
Active Peer
195.113.144.201
195.113.144.238
2
u
74
512
377
3.629
-0.006

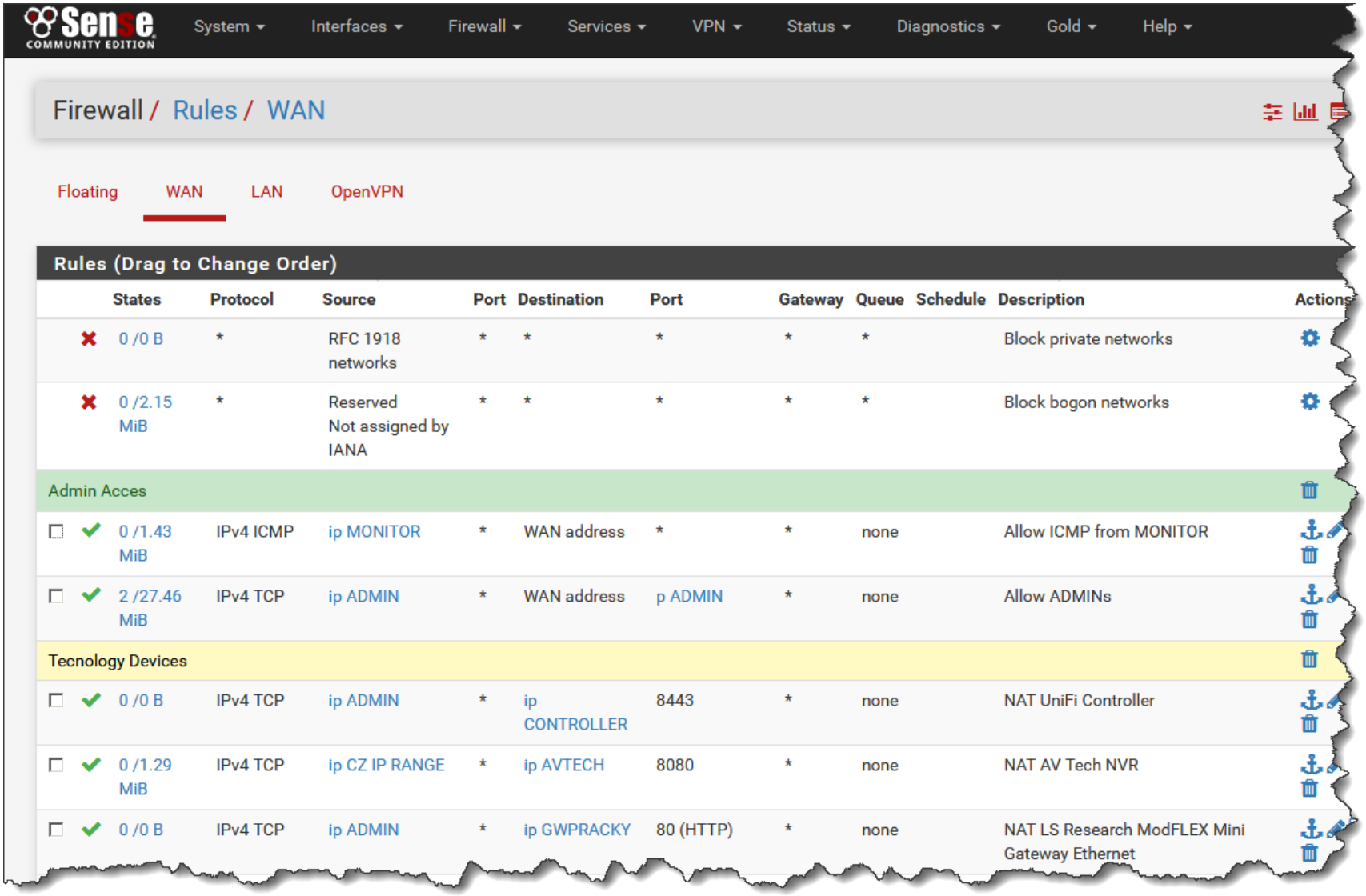
NAT


Sense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
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
Add
Add
Delete
Automatic Rules:
Interface
Source
Source Port
Destination
Destination Port
NAT Address
NAT Port
Static Port
Description

Port Forward



Firewall Rules



Sense COMMUNITY EDITION | System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Gold | Help

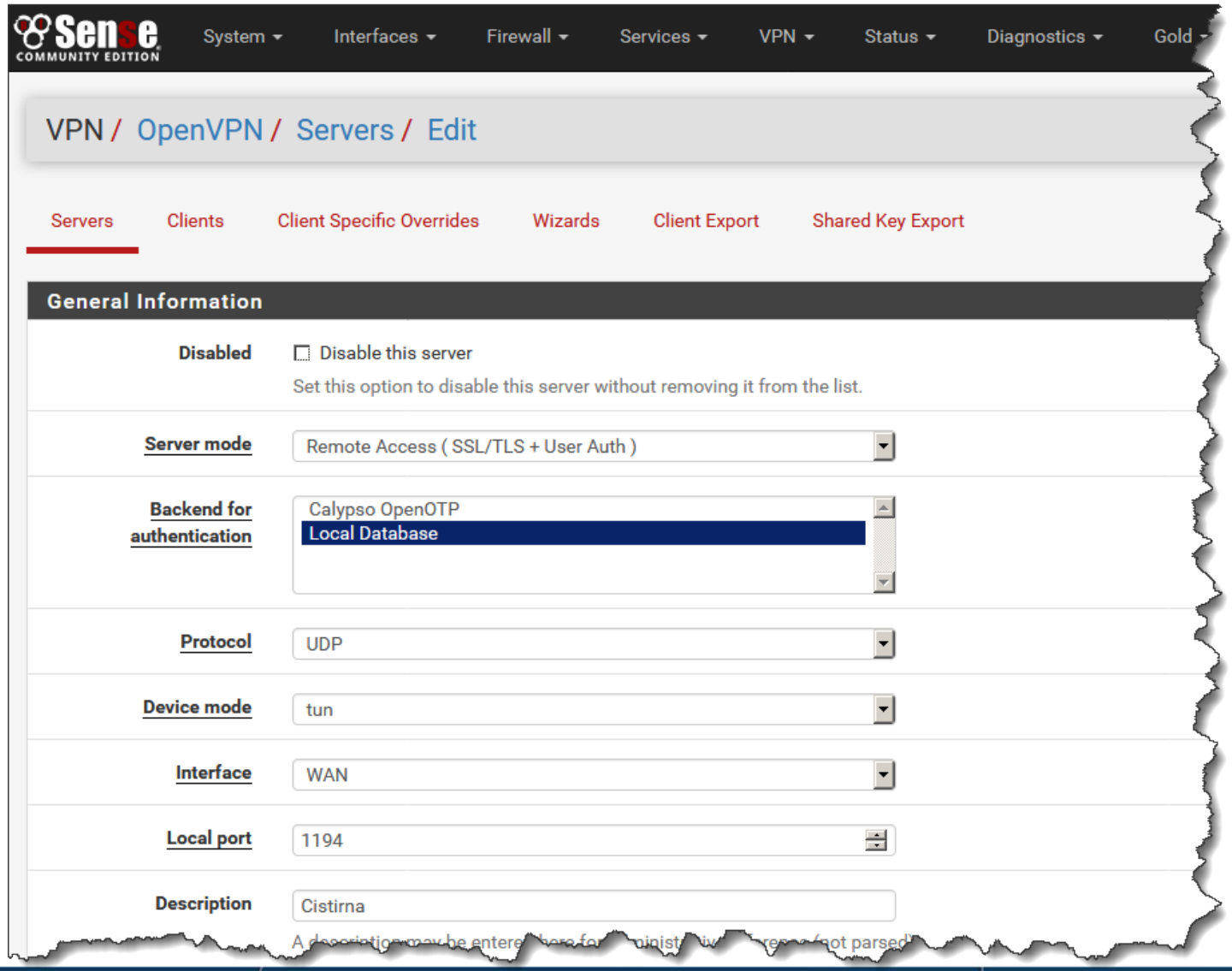
Firewall / Rules / WAN

Floating | WAN | LAN | OpenVPN

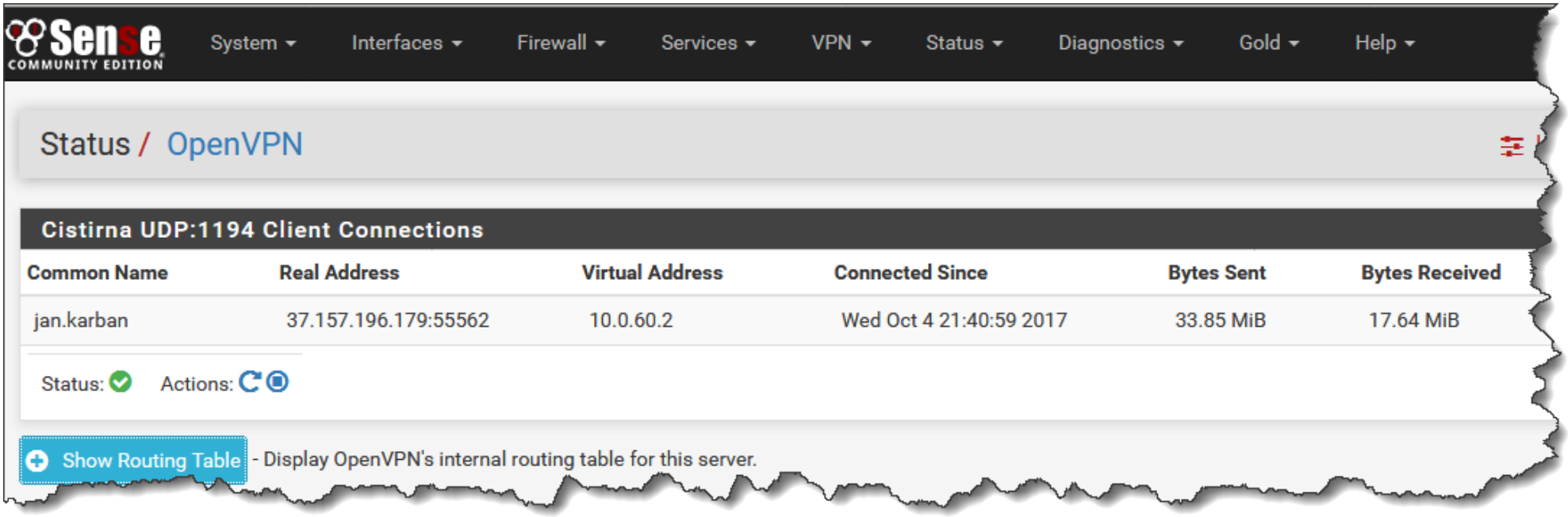
Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✖	0 /0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
✖	0 /2.15 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
Admin Acces											
✔	0 /1.43 MiB	IPv4 ICMP	ip MONITOR	*	WAN address	*	*	none		Allow ICMP from MONITOR	
✔	2 /27.46 MiB	IPv4 TCP	ip ADMIN	*	WAN address	p ADMIN	*	none		Allow ADMINs	
Tecnology Devices											
✔	0 /0 B	IPv4 TCP	ip ADMIN	*	ip CONTROLLER	8443	*	none		NAT UniFi Controller	
✔	0 /1.29 MiB	IPv4 TCP	ip CZ IP RANGE	*	ip AVTECH	8080	*	none		NAT AV Tech NVR	
✔	0 /0 B	IPv4 TCP	ip ADMIN	*	ip GWPRACKY	80 (HTTP)	*	none		NAT LS Research ModFLEX Mini Gateway Ethernet	

OpenVPN


Sense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
VPN / OpenVPN / Servers / Edit
Servers
Clients
Client Specific Overrides
Wizards
Client Export
Shared Key Export
General Information
Disabled
Disable this server
Set this option to disable this server without removing it from the list.
Server mode
Remote Access (SSL/TLS + User Auth)
Backend for authentication
Calypso OpenOTP
Local Database
Protocol
UDP
Device mode
tun
Interface
WAN
Local port
1194
Description
Cistirna

OpenVPN - Status



Dotazy?

Děkuji za pozornost.