Captive Portal – OPNSense

Calcolo e Reti Sezione di Bologna

Antonella Monducci

Esigenze - Sostituzione Portale Tino

INFN-Web, autenticazione fornite dal Portale Tino

- Account locali
- Visitatori registrati tramite GOApp
- Tramite script, creazione di un determinato numero di account locali (utili per convegni e conferenze).

OPNSense - Captive Portal

Permette di autenticare

- Account locali <-> Account locali
- Visitatori registrati tramite GOApp <-> Visitatori registrati sull’LDAP nazionale
- Tramite script, creazione di un determinato numero di account locali (utili per convegni e conferenze) <-> Tramite interfaccia web creazione di un determinato numero di voucher

OPNSense - Captive Portal

Hardware:

- 2 vCPU
- 4 GB Ram
- 20 GB Disco
- 3 vEthernet

Software:
is an open source, easy-to-use and easy-to-build HardenedBSD based firewall and routing platform.

https://opnsense.org/about/about-opnsense/

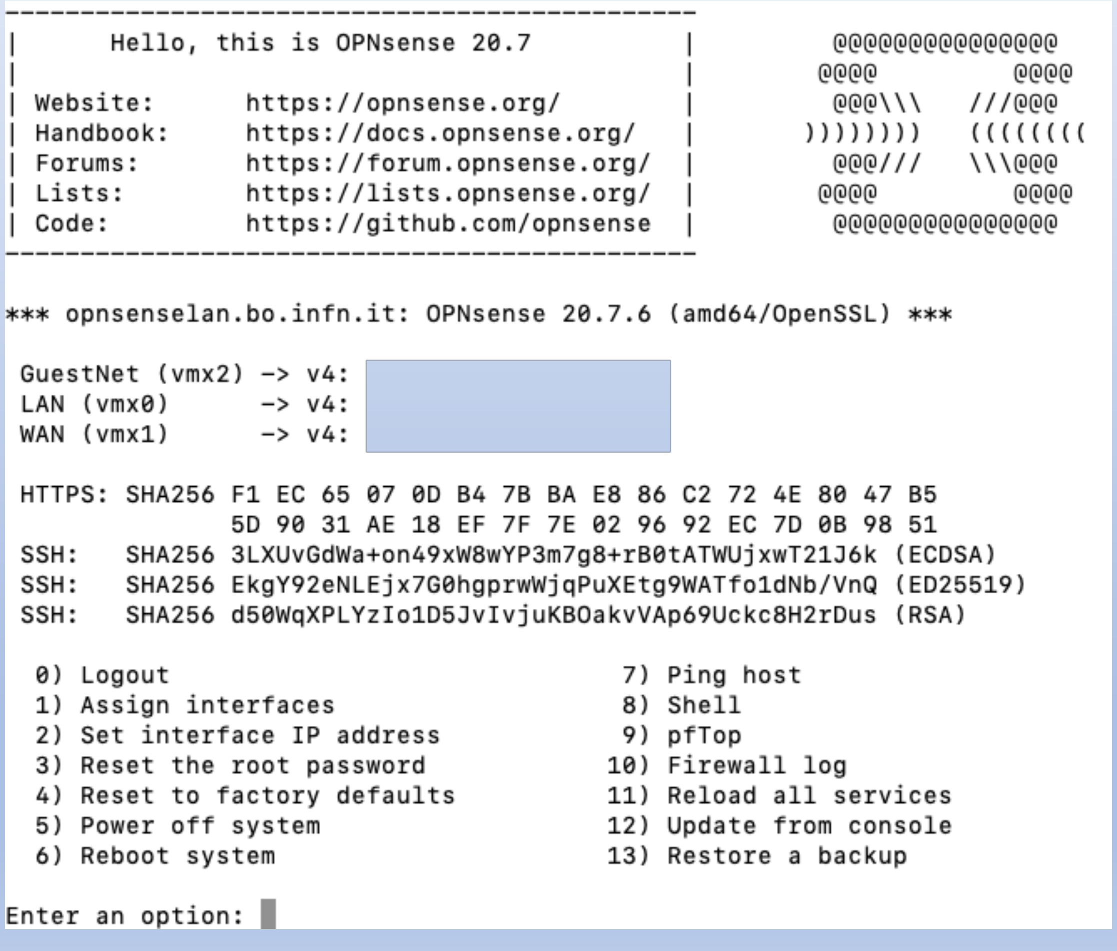
OPNSense - Captive Portal

Le 3 interfacce sono relative a:

- LAN con indirizzo IP privato
  Utilizzata per la gestione della macchina tramite SSH o interfaccia web;
- WAN con indirizzo IP pubblico
  E’ l'interfaccia verso la quale verranno nattate tutte le macchine collegate ed autorizzate alla WiFi INFN-Web;
- GuestNet con indirizzo IP privato su vlan taggata per il dialogo con gli access point.
  L’indirizzo IP assegnato appartiene alla stessa sottorete degli IP che verranno assegnati in DHCP alle macchine collegate ed autorizzate alla WiFi INFN-Web.

OPNSense - Captive Portal

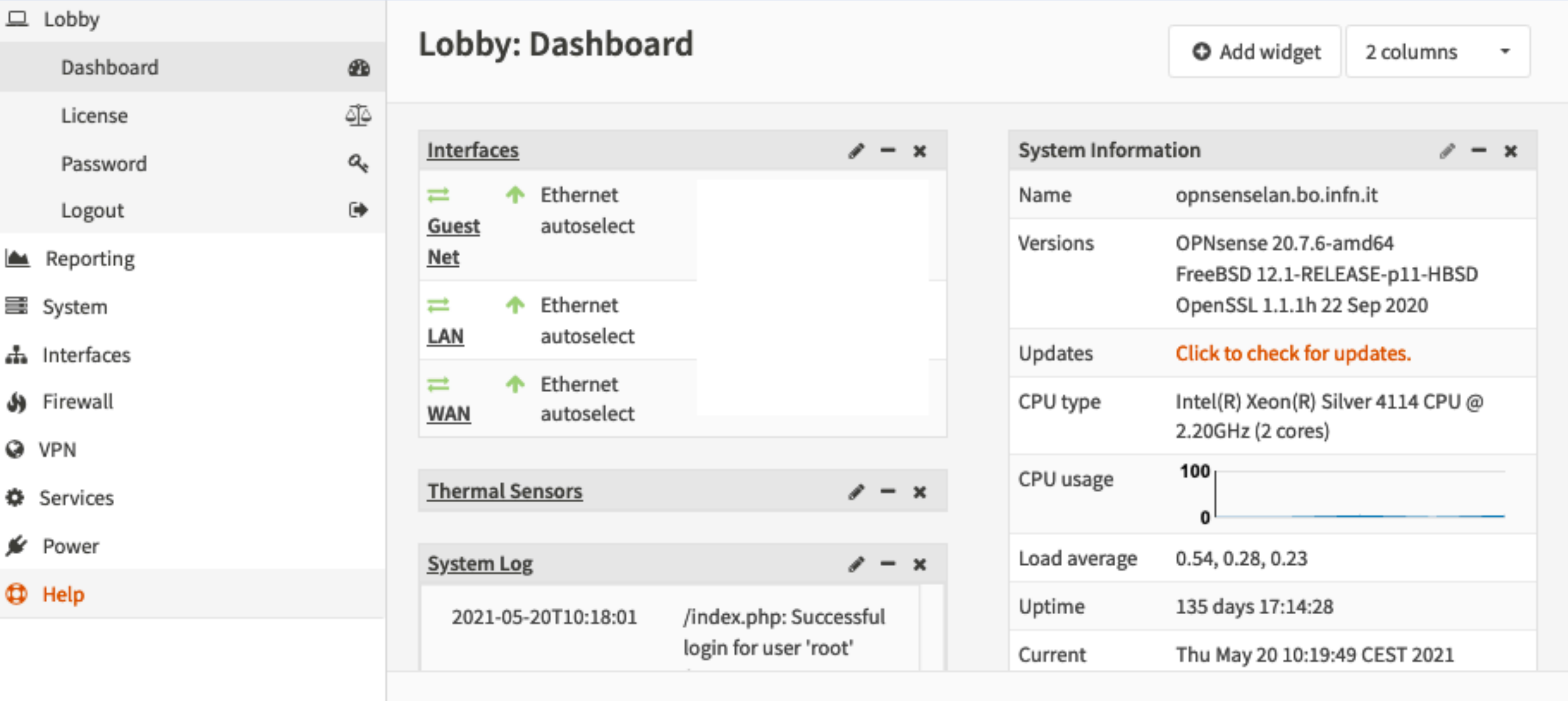
Interfaccia SSH



```
----------------------------------------------
|      Hello, this is OPNsense 20.7          |         @@@@@@@@@@@@@@@
|                                            |        @@@@         @@@@
| Website:      https://opnsense.org/        |         @@@\\\   ///@@@
| Handbook:     https://docs.opnsense.org/   |       ))))))))   ((((((((
| Forums:       https://forum.opnsense.org/  |         @@@///   \\\@@@
| Lists:        https://lists.opnsense.org/  |        @@@@         @@@@
| Code:         https://github.com/opnsense  |         @@@@@@@@@@@@@@@
----------------------------------------------

*** opnsenselan.bo.infn.it: OPNsense 20.7.6 (amd64/OpenSSL) ***

 GuestNet (vmx2) -> v4: [redacted]
 LAN (vmx0)      -> v4:
 WAN (vmx1)      -> v4:

 HTTPS: SHA256 F1 EC 65 07 0D B4 7B BA E8 86 C2 72 4E 80 47 B5
               5D 90 31 AE 18 EF 7F 7E 02 96 92 EC 7D 0B 98 51
 SSH:   SHA256 3LXUvGdWa+on49xW8wYP3m7g8+rB0tATWUjxwT21J6k (ECDSA)
 SSH:   SHA256 EkgY92eNLEjx7G0hgprwWjqPuXEtg9WATfo1dNb/VnQ (ED25519)
 SSH:   SHA256 d50WqXPLYzIo1D5JvIvjuKBOakvVAp69Uckc8H2rDus (RSA)

  0) Logout                              7) Ping host
  1) Assign interfaces                   8) Shell
  2) Set interface IP address            9) pfTop
  3) Reset the root password            10) Firewall log
  4) Reset to factory defaults          11) Reload all services
  5) Power off system                   12) Update from console
  6) Reboot system                      13) Restore a backup

Enter an option: 
```

OPNSense - Captive Portal

Interfaccia WEB



Guest Net	Ethernet autoselect
LAN	Ethernet autoselect
WAN	Ethernet autoselect

```
2021-05-20T10:18:01    /index.php: Successful login for user 'root'
```

Name	opnsenselan.bo.infn.it
Versions	OPNsense 20.7.6-amd64 FreeBSD 12.1-RELEASE-p11-HBSD OpenSSL 1.1.1h 22 Sep 2020
Updates	Click to check for updates.
CPU type	Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz (2 cores)
CPU usage	
Load average	0.54, 0.28, 0.23
Uptime	135 days 17:14:28
Current	Thu May 20 10:19:49 CEST 2021

OPNSense - Captive Portal

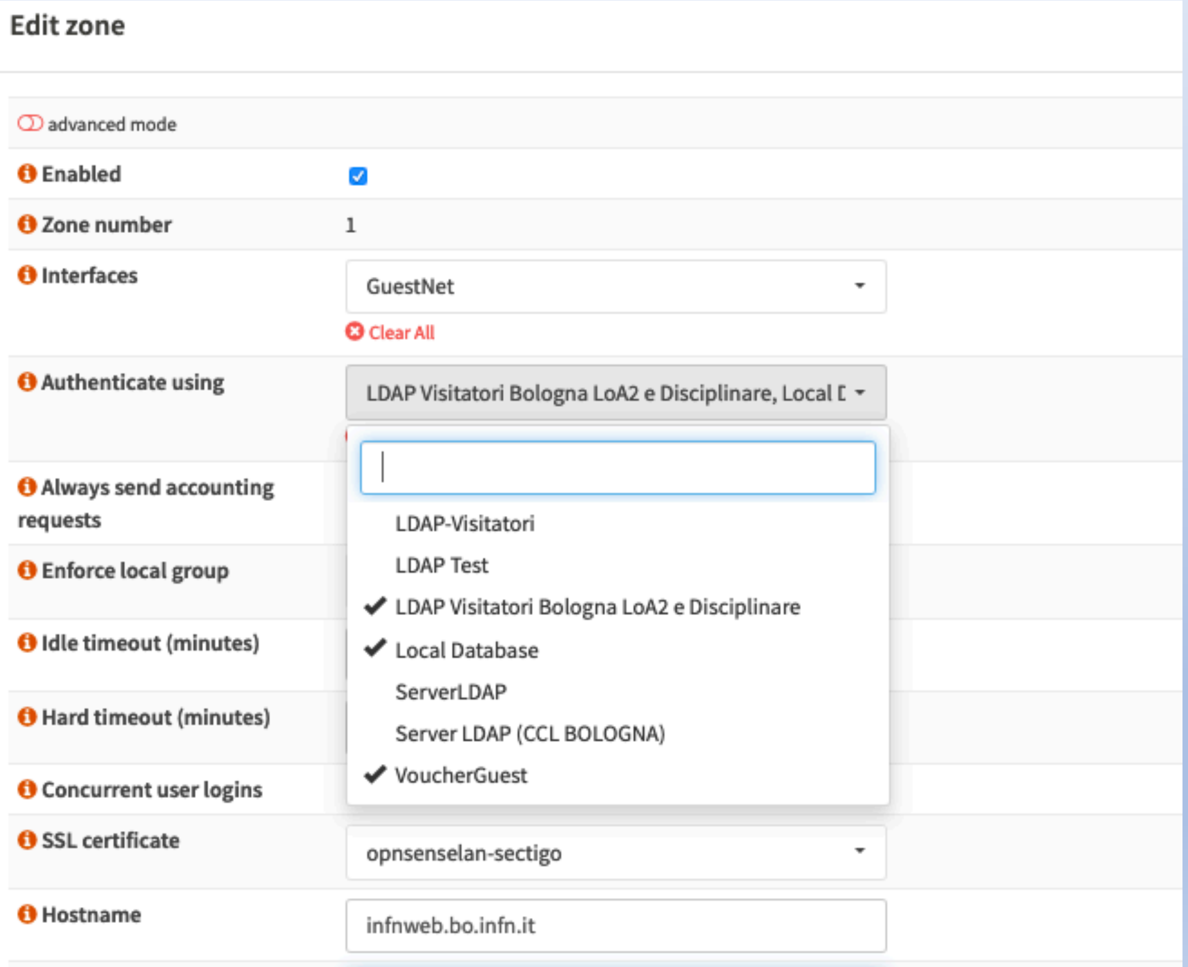
Dopo aver installato OPNSense e opportunamente configurato le interfacce è possibile procedere alla configurazione del captive portal tramite interfaccia web

Le configurazione generali sono ben documentate al seguente link:

https://wiki.opnsense.org/manual/how-tos/guestnet.html

Vediamo nel dettaglio le parti più rilevanti

OPNSense - Captive Portal



Edit zone

advanced mode

Enabled	☑
Zone number	1
Interfaces	GuestNet Clear All
Authenticate using	LDAP Visitatori Bologna LoA2 e Disciplinare, Local D
Always send accounting requests	
Enforce local group	
Idle timeout (minutes)	
Hard timeout (minutes)	
Concurrent user logins	
SSL certificate	opnsenselan-sectigo
Hostname	infnweb.bo.infn.it

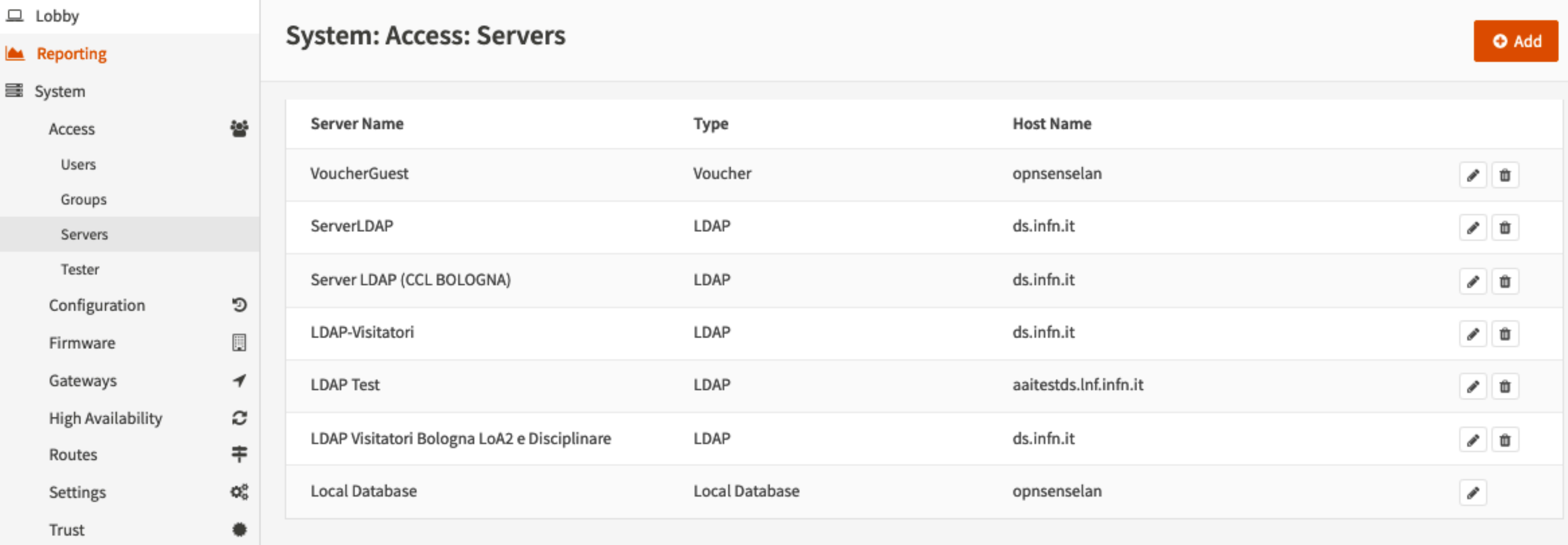
- LDAP-Visitatori
- LDAP Test
- ✓ LDAP Visitatori Bologna LoA2 e Disciplinare
- ✓ Local Database
- ServerLDAP
- Server LDAP (CCL BOLOGNA)
- ✓ VoucherGuest

Definizione degli utenti che potranno collegarsi alla WiFi INFN-Web.

Nella pagina amministrativa del Captive Portal di OPNSense è possibile definire quali gruppi di utenti potranno autenticarsi

OPNSense - Captive Portal

In System -> Access -> Server sono definite le diverse basi dati.
Tra queste potranno essere selezionate quelle da cui prendere gli utenti autorizzati a connettersi alla WiFi INFN-Web

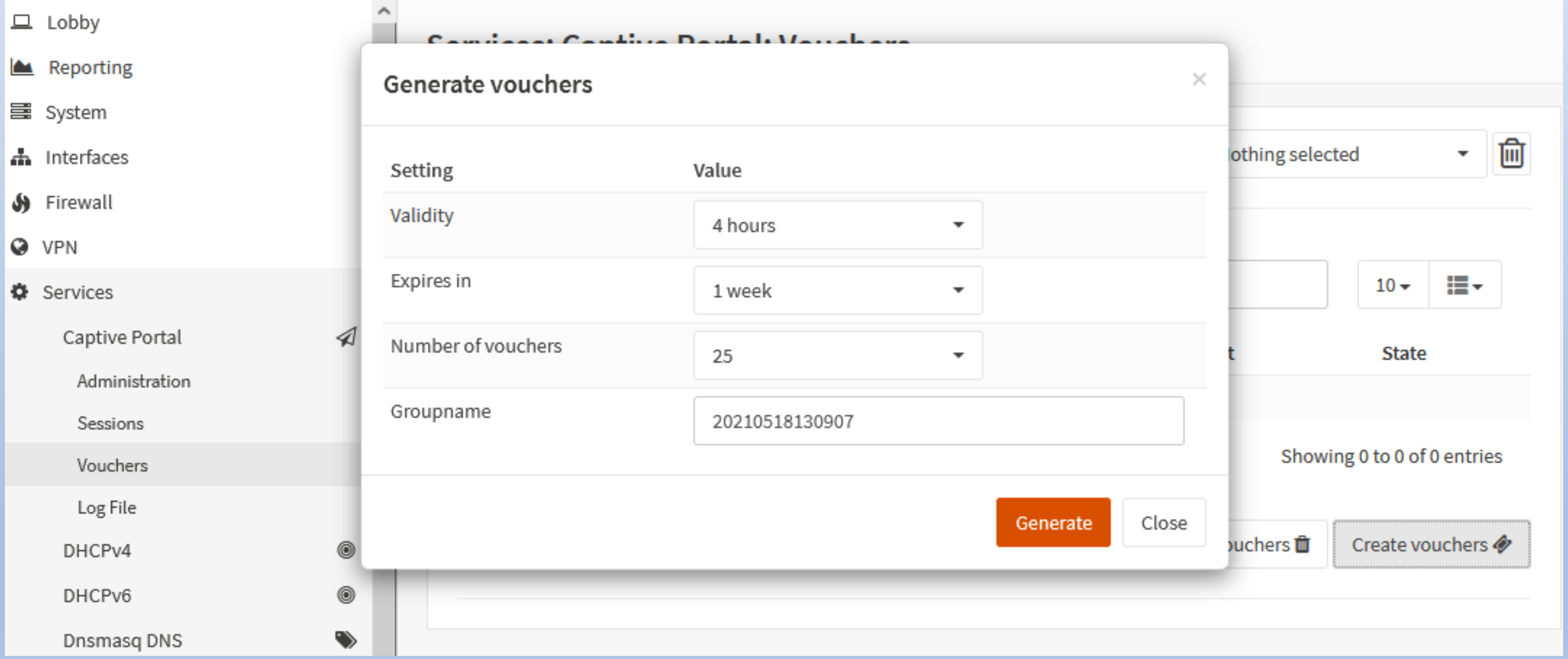


System: Access: Servers

Server Name	Type	Host Name
VoucherGuest	Voucher	opnsenselan
ServerLDAP	LDAP	ds.infn.it
Server LDAP (CCL BOLOGNA)	LDAP	ds.infn.it
LDAP-Visitatori	LDAP	ds.infn.it
LDAP Test	LDAP	aaitestds.lnf.infn.it
LDAP Visitatori Bologna LoA2 e Disciplinare	LDAP	ds.infn.it
Local Database	Local Database	opnsenselan

OPNSense - Captive Portal

Generazione di Voucher temporanei:



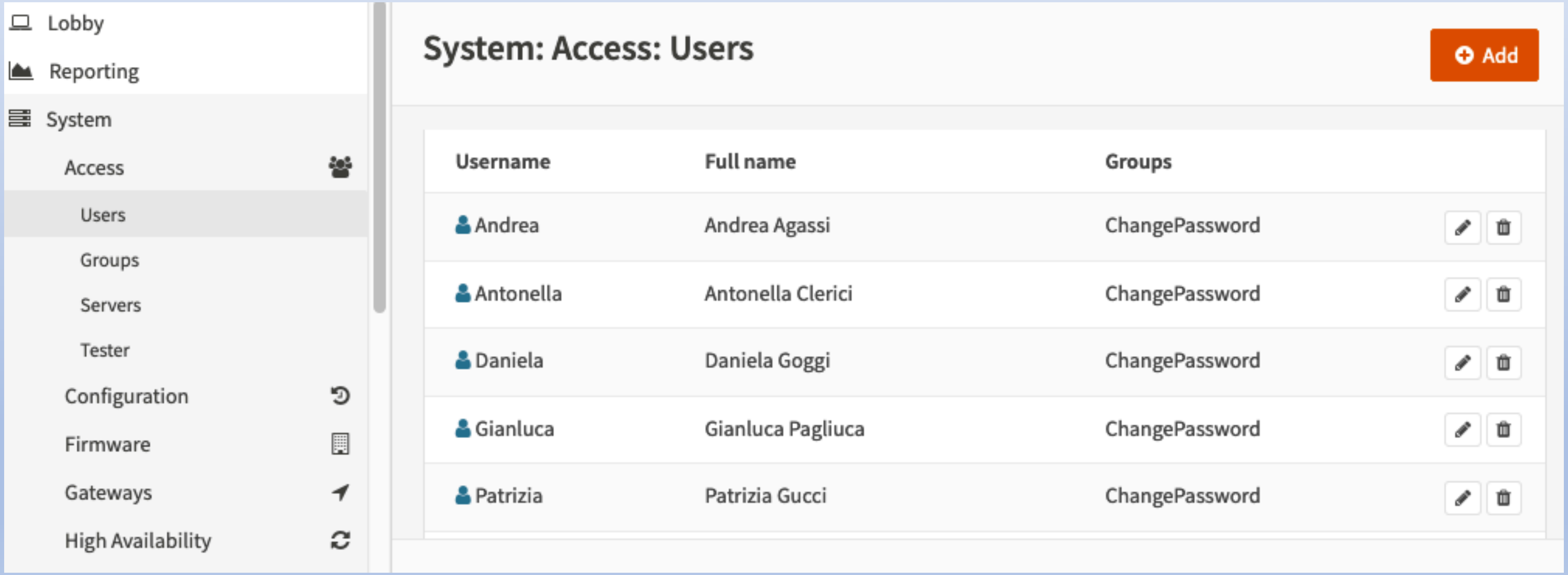
Generate vouchers

Setting	Value
Validity	4 hours
Expires in	1 week
Number of vouchers	25
Groupname	20210518130907

Showing 0 to 0 of 0 entries

OPNSense - Captive Portal

Local Database:



System: Access: Users

Username	Full name	Groups
Andrea	Andrea Agassi	ChangePassword
Antonella	Antonella Clerici	ChangePassword
Daniela	Daniela Goggi	ChangePassword
Gianluca	Gianluca Pagliuca	ChangePassword
Patrizia	Patrizia Gucci	ChangePassword

OPNSense - Captive Portal

Nel nostro caso gli utenti locali fanno parte del gruppo

ChangePassword

è un gruppo creato manualmente al quale è stato dato il privilegio di:

GUI - System: User Password Manager

Una volta collegati alla WiFi INFN-Web possono cambiarsi la password accedendo all’IP dell’interfaccia WAN.

OPNSense - Captive Portal

LDAP Visitatori Bologna LoA2 e Disciplinare

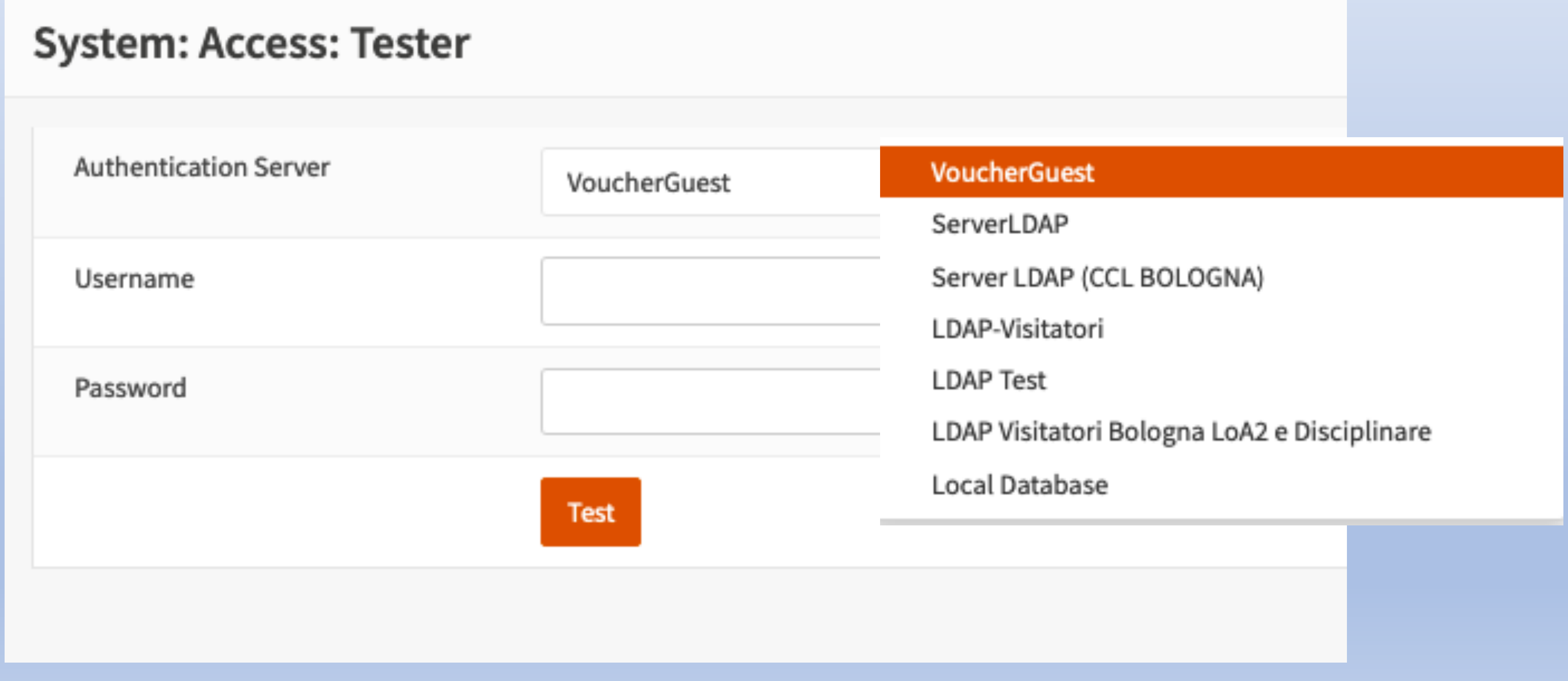
I dati vengono letti collegandosi ad un server LDAP e selezionando gli utenti tramite query.

La configurazione adottata è la seguente:

Hostname or IP address:	ds.infn.it
Port:	389
Base DN:	dc=infn,dc=it
Authetication conteiners:	ou=People,dc=infn,dc=it
Extended Query:	&(schacUserStatus=urn:schac:userStatus:it:infn.it:godiva-role:visitatore:attivo+ttl*)(isMemberOf=i:infn:bo::v:visitatore)(edupersonentitlement=urn:mace:infn.it:disciplinare-it)(eduPersonAssurance=urn:mace:infn.it:loa2)
User naming attribute:	Mail

OPNSense - Captive Portal

Possibilità di testare le credenziali:



System: Access: Tester

Authentication Server: VoucherGuest

Username

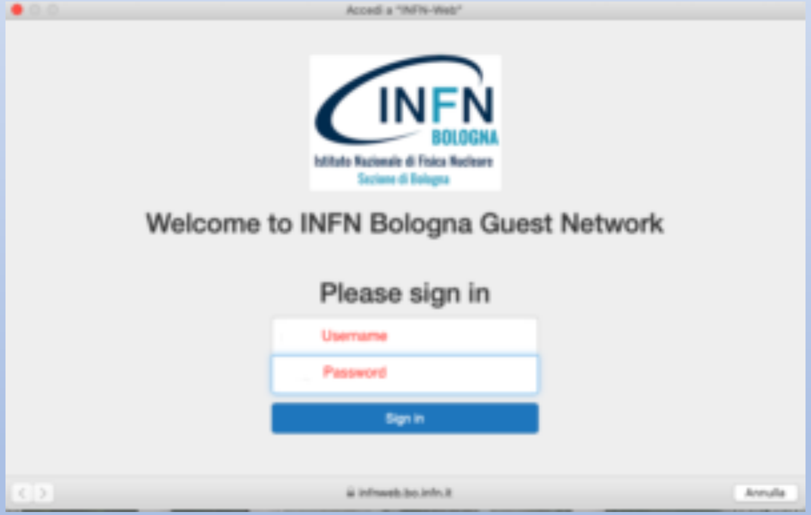
Password

Test
VoucherGuest
ServerLDAP
Server LDAP (CCL BOLOGNA)
LDAP-Visitatori
LDAP Test
LDAP Visitatori Bologna LoA2 e Disciplinare
Local Database

OPNSense - Captive Portal

OPNSense permette di personalizzare la pagina di login dell’utente.

E’ possibile scaricare e modificare il template di default



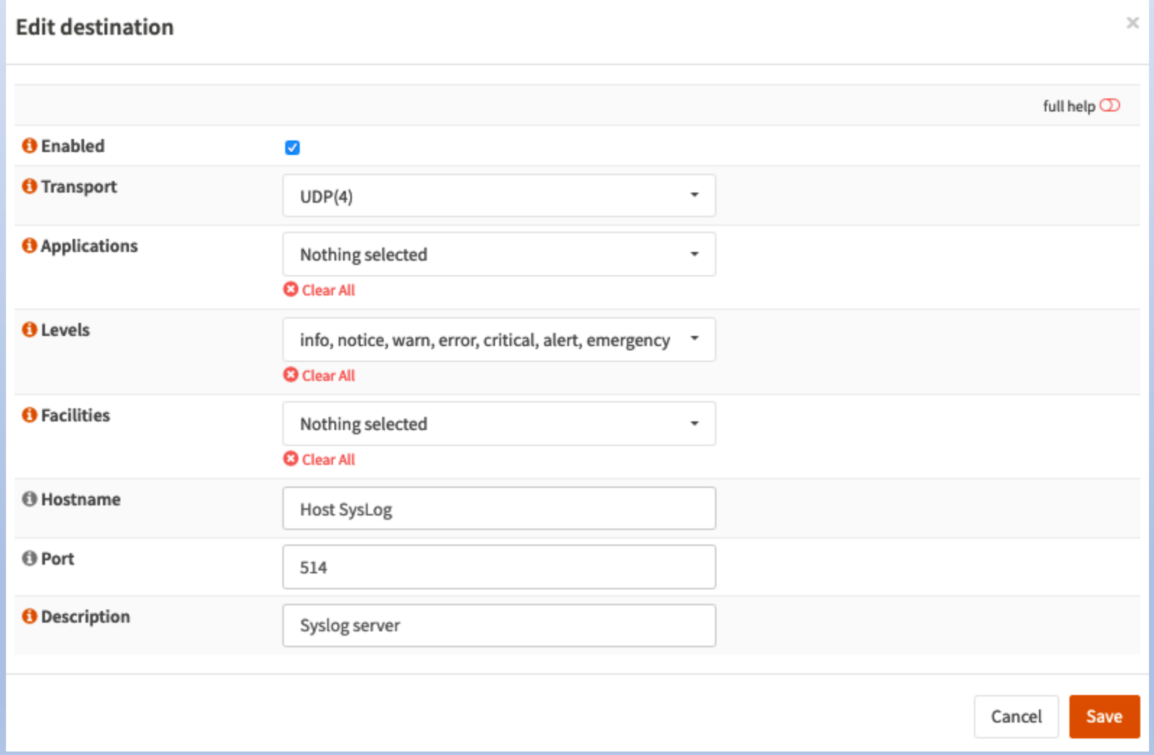
Accedi a "INFN-Web"

Welcome to INFN Bologna Guest Network

Please sign in

OPNSense - Captive Portal

Configurazione dei log di Sistema

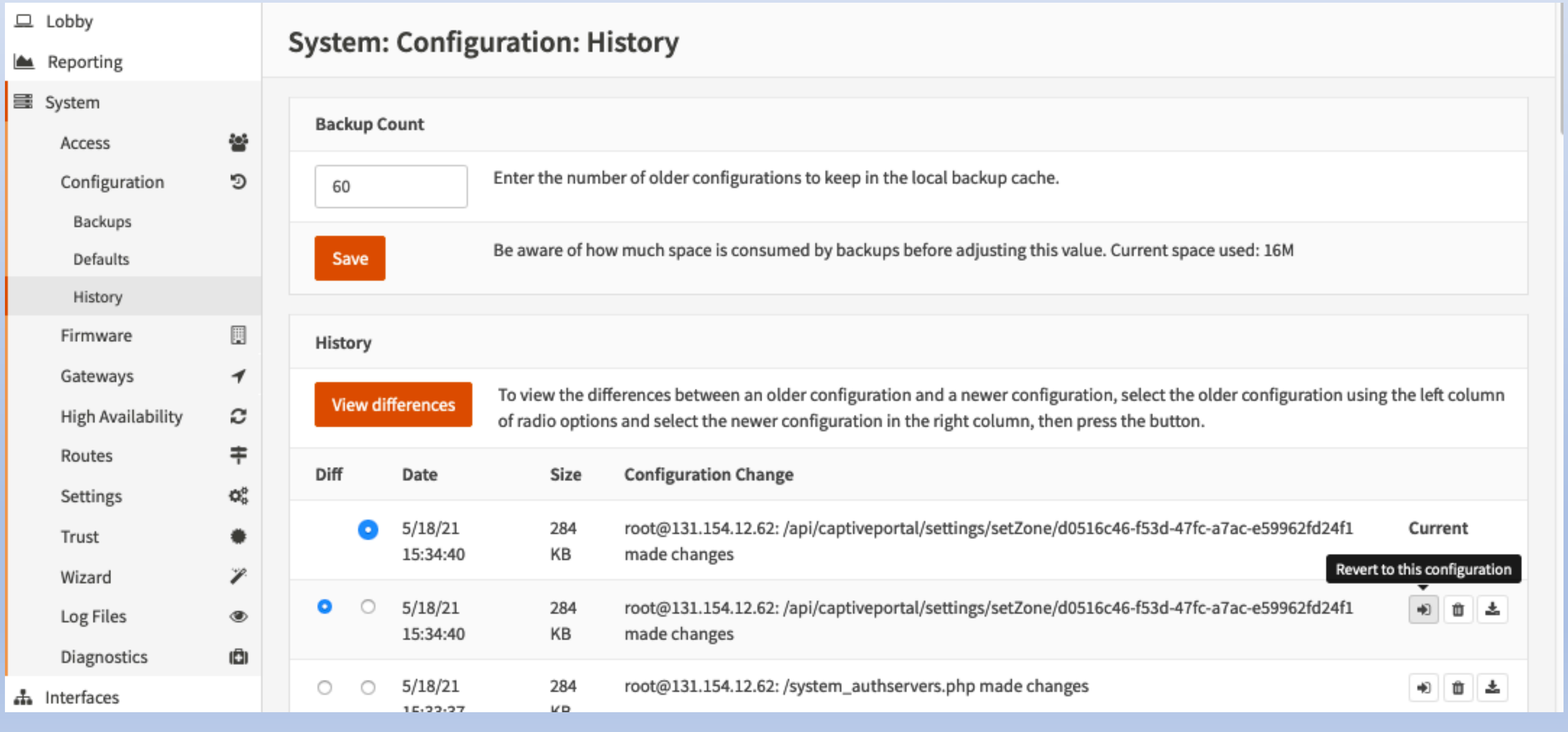


Edit destination

Enabled	☑
Transport	UDP(4)
Applications	Nothing selected Clear All
Levels	info, notice, warn, error, critical, alert, emergency Clear All
Facilities	Nothing selected Clear All
Hostname	Host SysLog
Port	514
Description	Syslog server

OPNSense - Captive Portal

Backup e Restore



System: Configuration: History

Backup Count

60

Enter the number of older configurations to keep in the local backup cache.

Save

Be aware of how much space is consumed by backups before adjusting this value. Current space used: 16M

History

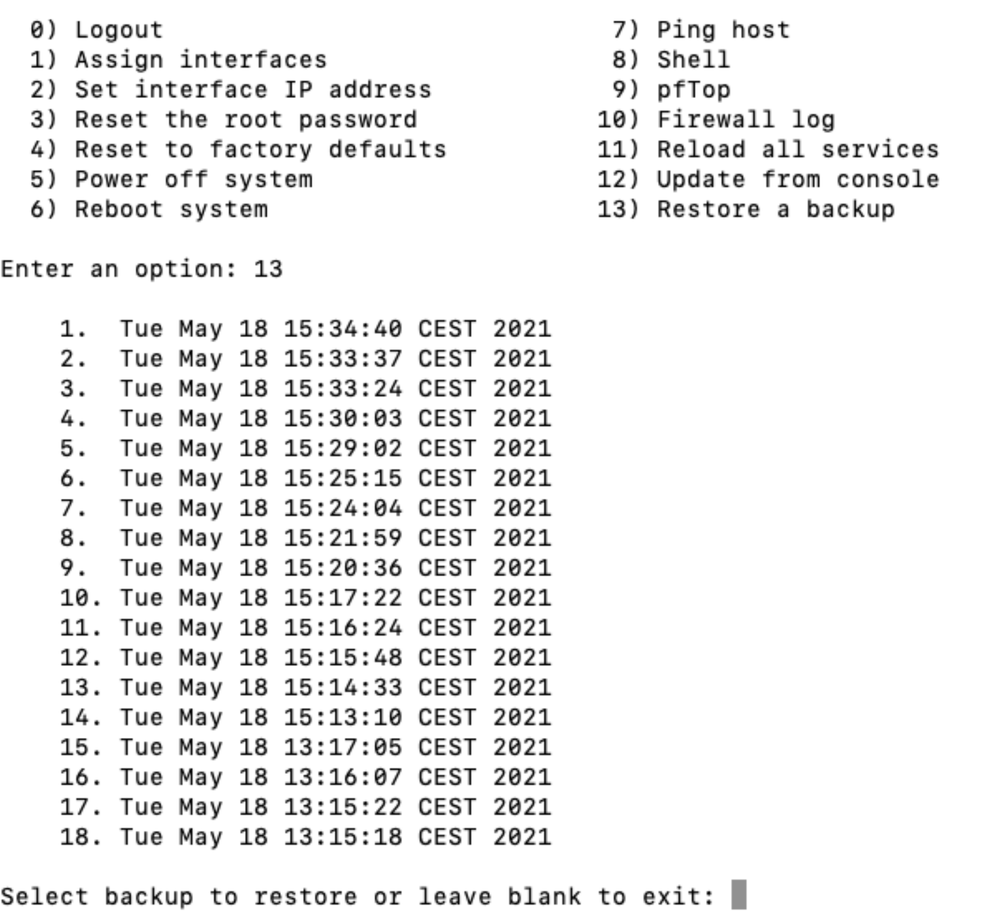
View differences

To view the differences between an older configuration and a newer configuration, select the older configuration using the left column of radio options and select the newer configuration in the right column, then press the button.

Diff		Date	Size	Configuration Change	
	●	5/18/21 15:34:40	284 KB	root@131.154.12.62: /api/captiveportal/settings/setZone/d0516c46-f53d-47fc-a7ac-e59962fd24f1 made changes	Current
●	○	5/18/21 15:34:40	284 KB	root@131.154.12.62: /api/captiveportal/settings/setZone/d0516c46-f53d-47fc-a7ac-e59962fd24f1 made changes	
○	○	5/18/21 15:33:37	284 KB	root@131.154.12.62: /system_authservers.php made changes	

OPNSense - Captive Portal

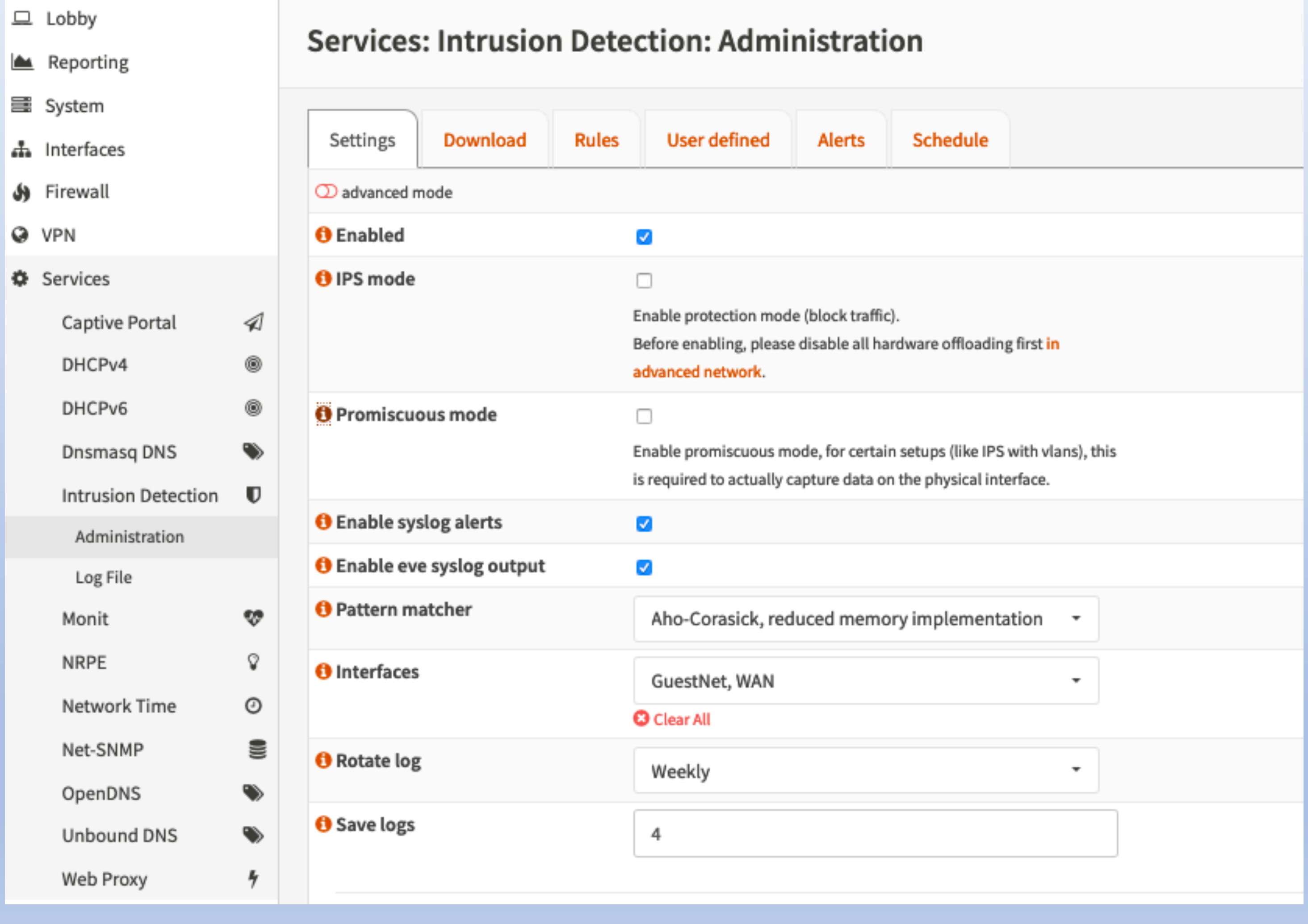
Backup e Restore



```
  0) Logout                              7) Ping host
  1) Assign interfaces                   8) Shell
  2) Set interface IP address            9) pfTop
  3) Reset the root password            10) Firewall log
  4) Reset to factory defaults          11) Reload all services
  5) Power off system                   12) Update from console
  6) Reboot system                      13) Restore a backup

Enter an option: 13

    1.  Tue May 18 15:34:40 CEST 2021
    2.  Tue May 18 15:33:37 CEST 2021
    3.  Tue May 18 15:33:24 CEST 2021
    4.  Tue May 18 15:30:03 CEST 2021
    5.  Tue May 18 15:29:02 CEST 2021
    6.  Tue May 18 15:25:15 CEST 2021
    7.  Tue May 18 15:24:04 CEST 2021
    8.  Tue May 18 15:21:59 CEST 2021
    9.  Tue May 18 15:20:36 CEST 2021
    10. Tue May 18 15:17:22 CEST 2021
    11. Tue May 18 15:16:24 CEST 2021
    12. Tue May 18 15:15:48 CEST 2021
    13. Tue May 18 15:14:33 CEST 2021
    14. Tue May 18 15:13:10 CEST 2021
    15. Tue May 18 13:17:05 CEST 2021
    16. Tue May 18 13:16:07 CEST 2021
    17. Tue May 18 13:15:22 CEST 2021
    18. Tue May 18 13:15:18 CEST 2021

Select backup to restore or leave blank to exit:
```

OPNSense - Captive Portal

Intrusion Detection



Services: Intrusion Detection: Administration

Enabled ☑

IPS mode □
Enable protection mode (block traffic).
Before enabling, please disable all hardware offloading first in advanced network.

Promiscuous mode □
Enable promiscuous mode, for certain setups (like IPS with vlans), this is required to actually capture data on the physical interface.

Enable syslog alerts ☑

Enable eve syslog output ☑

Pattern matcher: Aho-Corasick, reduced memory implementation

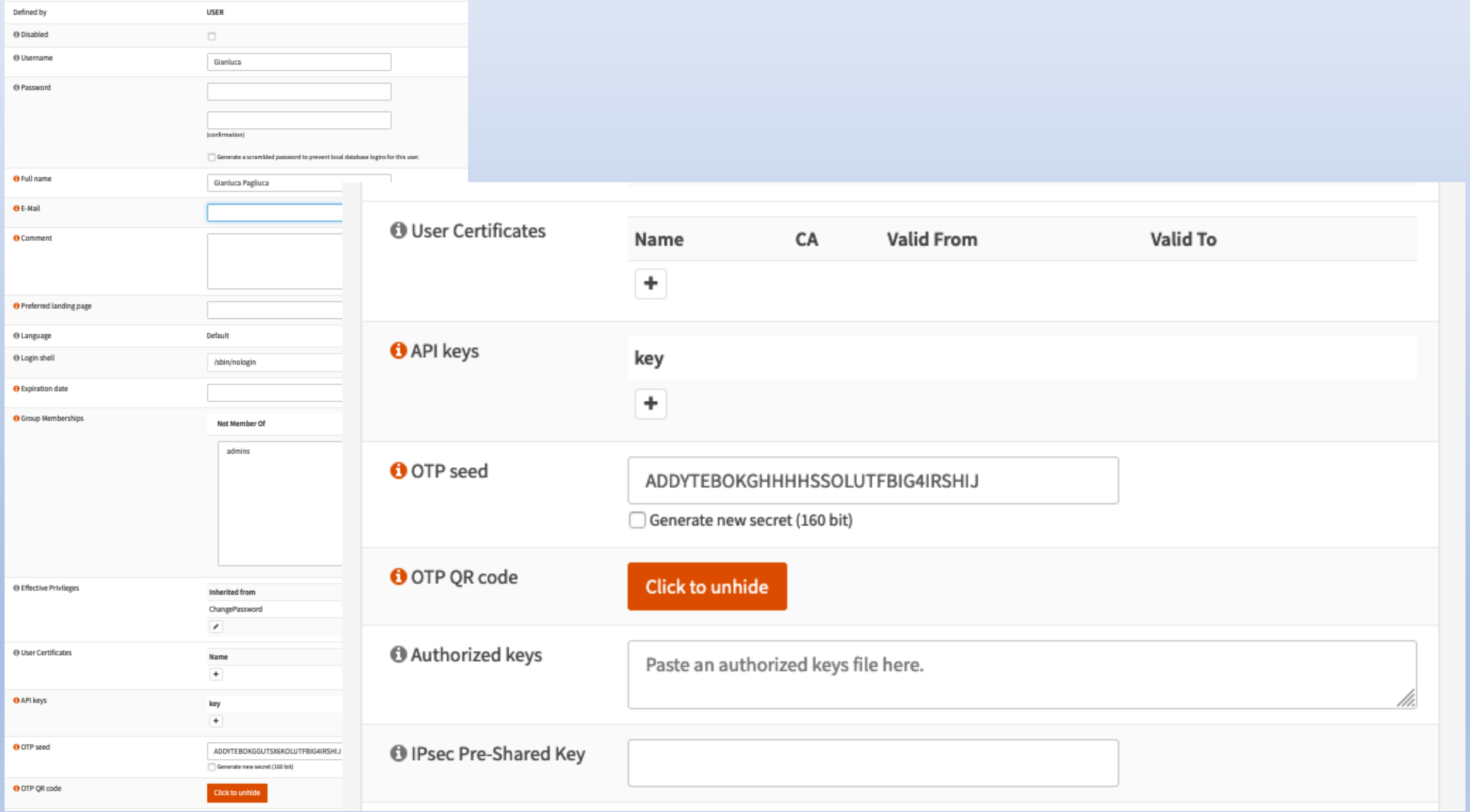
Interfaces: GuestNet, WAN

Rotate log: Weekly

Save logs: 4

OPNSense - Captive Portal

Autenticazione a più fattori



Defined by	USER
Disabled	□
Username	Gianluca
Password	 (confirmation) □ Generate a scrambled password to prevent local database logins for this user.
Full name	Gianluca Pagliuca
E-Mail	
Comment	
Preferred landing page	
Language	Default
Login shell	/sbin/nologin
Expiration date	
Group Memberships	Not Member Of admins
Effective Privileges	Inherited from ChangePassword
User Certificates	Name +
API keys	key +
OTP seed	ADDYTEBOKGGUTSX6KOLUTFBIG4IRSHIJ □ Generate new secret (160 bit)
OTP QR code	Click to unhide

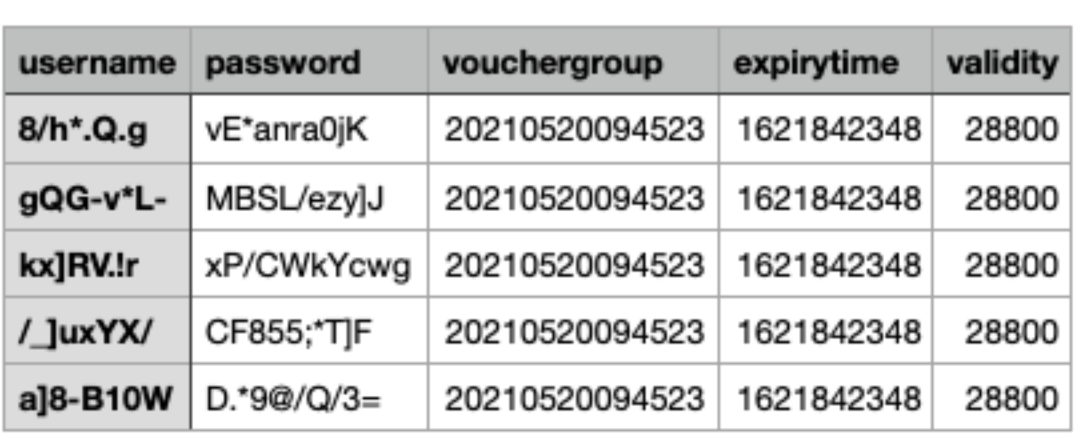
User Certificates	Name CA Valid From Valid To +
API keys	key +
OTP seed	ADDYTEBOKGHHHHSSOLUTFBIG4IRSHIJ □ Generate new secret (160 bit)
OTP QR code	Click to unhide
Authorized keys	Paste an authorized keys file here.
IPsec Pre-Shared Key	

OPNSense - Captive Portal

Domande?

OPNSense - Captive Portal

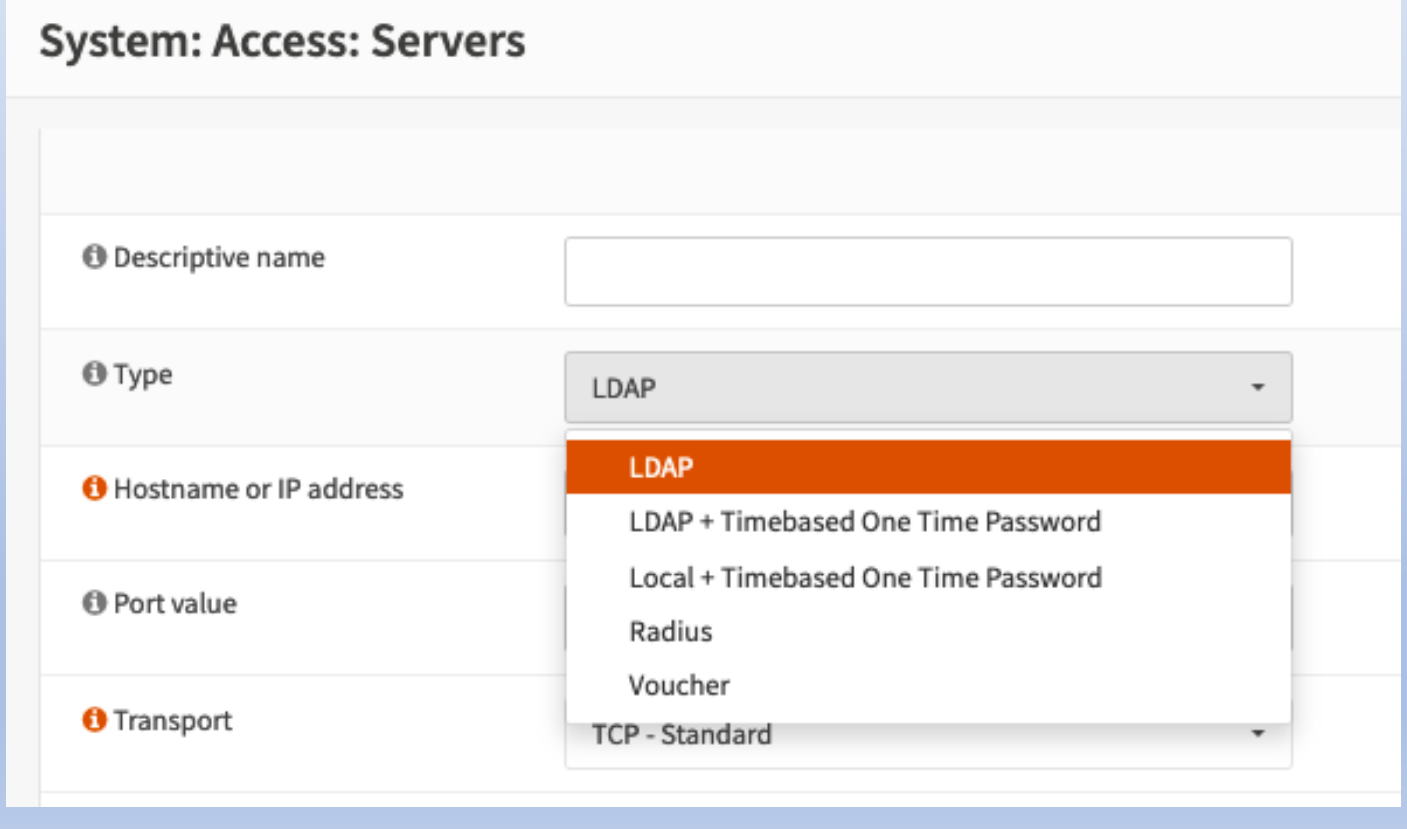
Esempio file voucher:



username	password	vouchergroup	expirytime	validity
8/h*.Q.g	vE*anra0jK	20210520094523	1621842348	28800
gQG-v*L-	MBSL/ezy]J	20210520094523	1621842348	28800
kx]RV.!r	xP/CWkYcwg	20210520094523	1621842348	28800
/_]uxYX/	CF855;*T]F	20210520094523	1621842348	28800
a]8-B10W	D.*9@/Q/3=	20210520094523	1621842348	28800

OPNSense - Captive Portal

Tipologia di base dati:



System: Access: Servers

Descriptive name

Type: LDAP

Hostname or IP address

Port value

Transport: TCP - Standard

LDAP
LDAP + Timebased One Time Password
Local + Timebased One Time Password
Radius
Voucher