

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: ██████████
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 d50WqXPLYzIo1D5JvIvjuKB0akvVAp69Uckc8H2rDus (RSA)

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


Enter an option: █
```

OPNSense - Captive Portal

Interfaccia WEB

The screenshot displays the OPNSense web interface. On the left is a sidebar menu with the following items: Lobby (selected), Dashboard, License, Password, Logout, Reporting, System, Interfaces, Firewall, VPN, Services, Power, and Help. The main content area is titled "Lobby: Dashboard" and features a "Add widget" button and a "2 columns" dropdown menu. The dashboard contains several widgets:

- Interfaces:** A table showing network interface status. All three interfaces (Guest Net, LAN, WAN) are up and set to "Ethernet autoselect".
- Thermal Sensors:** A widget for monitoring system temperature.
- System Log:** A log entry from 2021-05-20T10:18:01 showing a successful login for user 'root'.
- System Information:** A table providing system details.

System Information	
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

Authenticate using LDAP Visitatori Bologna LoA2 e Disciplinare, Local C

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

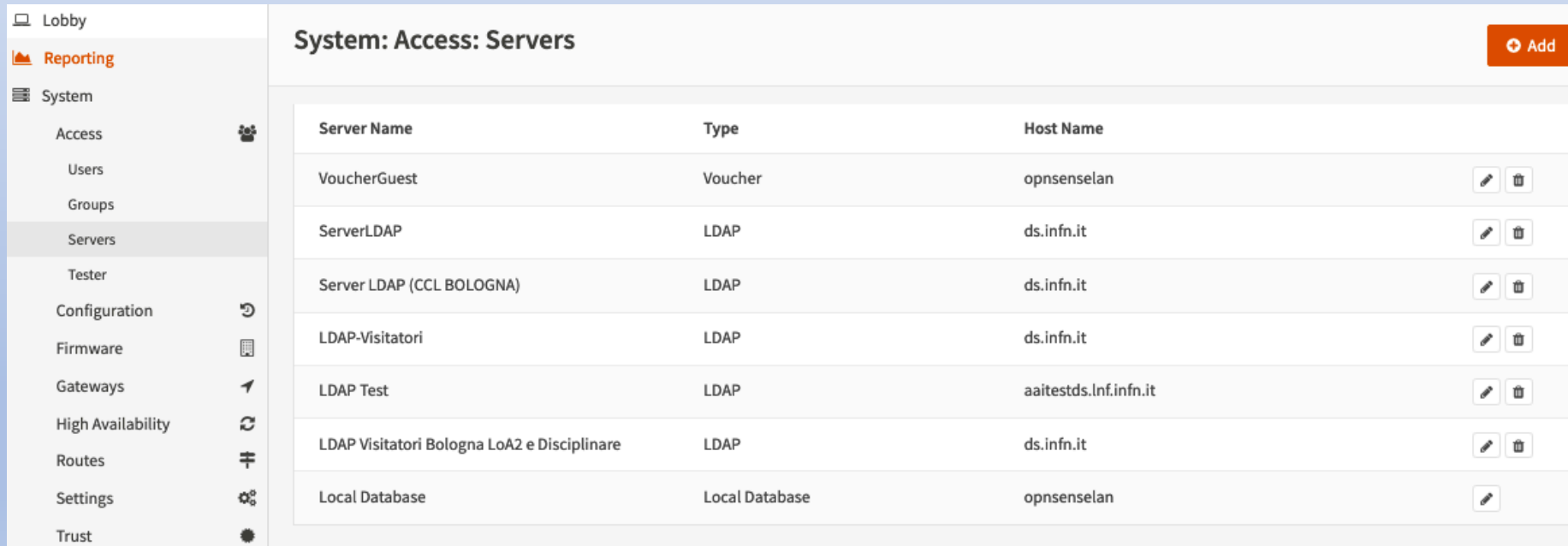
- LDAP-Visitatori
- LDAP Test
- LDAP Visitatori Bologna LoA2 e Disciplinare
- Local Database
- ServerLDAP
- Server LDAP (CCL BOLOGNA)
- VoucherGuest

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



The screenshot displays the 'System: Access: Servers' configuration page in OPNSense. The left sidebar shows the navigation menu with 'Servers' selected. The main content area contains a table of servers with the following data:

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:

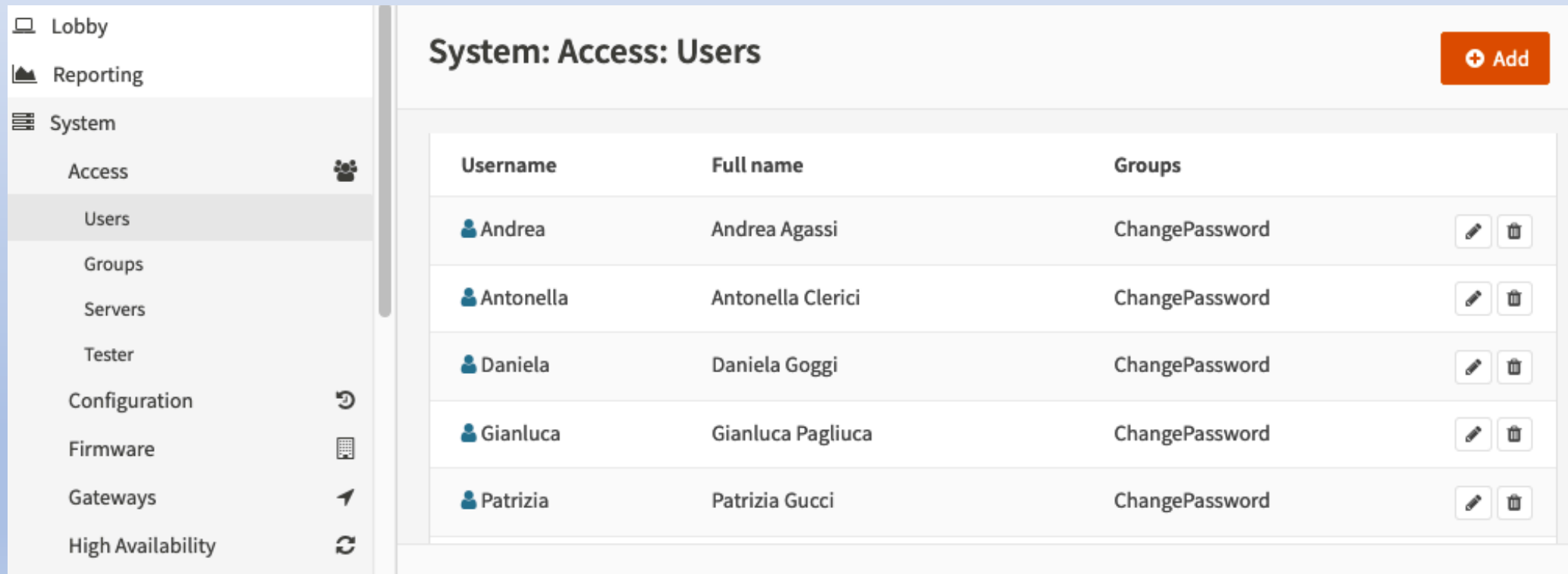
The screenshot shows the OPNSense Captive Portal Voucher generation interface. A modal window titled "Generate vouchers" is open, displaying the following settings:

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











At the bottom of the modal, there are two buttons: "Generate" (orange) and "Close" (white). The background interface shows the "Services" menu with "Captive Portal" selected, and the "Vouchers" sub-menu. The main content area displays "Showing 0 to 0 of 0 entries" and a "Create vouchers" button.

OPNSense - Captive Portal

Local Database:



The screenshot displays the OPNSense web interface. On the left is a navigation sidebar with categories: Lobby, Reporting, System, Access, Users, Groups, Servers, Tester, Configuration, Firmware, Gateways, and High Availability. The 'System' category is expanded, and 'Users' is selected. The main content area is titled 'System: Access: Users' and features an orange 'Add' button. Below the title is a table listing users with columns for Username, Full name, and Groups. Each row includes edit and delete icons.

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 containers:	ou=People,dc=infn,dc=it
Extended Query:	&(schacUserStatus=urn:schac:userStatus:it:infn.it:godiva- role:visitatore:attivo+t*I*)(isMemberOf=i:infn:bo::v:vis itatore)(edupersonentitlement=urn:mace:infn.it:discip linare-it)(eduPersonAssurance=urn:mace:infn.it:loa2)
User naming attribute:	Mail

OPNSense - Captive Portal

Possibilità di testare le credenziali:

System: Access: Tester

Authentication Server	<input type="text" value="VoucherGuest"/>	VoucherGuest
Username	<input type="text"/>	ServerLDAP
Password	<input type="text"/>	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



OPNSense - Captive Portal

Configurazione dei log di Sistema

Edit destination ✕

[full help](#)

Enabled

Transport

Applications
[Clear All](#)

Levels
[Clear All](#)

Facilities
[Clear All](#)

Hostname

Port

Description

OPNSense - Captive Portal

Backup e Restore

System: Configuration: History

Backup Count

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	
<input checked="" type="radio"/>	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 Revert to this configuration
<input type="radio"/>	5/18/21 15:34:40	284 KB	root@131.154.12.62: /api/captiveportal/settings/setZone/d0516c46-f53d-47fc-a7ac-e59962fd24f1 made changes	<input type="radio"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="radio"/>	5/18/21 15:33:37	284 KB	root@131.154.12.62: /system_authservers.php made changes	<input type="radio"/> <input type="checkbox"/> <input type="checkbox"/>

OPNSense - Captive Portal

Backup e Restore

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

The screenshot displays the OPNSense Administration interface for the Intrusion Detection Services. The left sidebar shows the navigation menu with 'Intrusion Detection' selected and 'Administration' highlighted. The main content area is titled 'Services: Intrusion Detection: Administration' and contains several tabs: 'Settings', 'Download', 'Rules', 'User defined', 'Alerts', and 'Schedule'. The 'Settings' tab is active, showing various configuration options:

- advanced mode:** Toggled on (indicated by a red 'x' icon).
- Enabled:** Checked (checkbox).
- IPS mode:** Unchecked (checkbox). Description: Enable protection mode (block traffic). Before enabling, please disable all hardware offloading first in advanced network.
- Promiscuous mode:** Unchecked (checkbox). Description: Enable promiscuous mode, for certain setups (like IPS with vlans), this is required to actually capture data on the physical interface.
- Enable syslog alerts:** Checked (checkbox).
- Enable eve syslog output:** Checked (checkbox).
- Pattern matcher:** Aho-Corasick, reduced memory implementation (dropdown menu).
- Interfaces:** GuestNet, WAN (dropdown menu). Includes a 'Clear All' button.
- Rotate log:** Weekly (dropdown menu).
- Save logs:** 4 (input field).

OPNSense - Captive Portal

Autenticazione
a più fattori

The image shows a user configuration page in OPNSense. On the left is a vertical sidebar with various user attributes, and on the right is a detailed configuration panel for multi-factor authentication.

User Configuration Sidebar:

- Defined by: USER
- Disabled:
- Username: Gianluca
- Password: [input field]
- Confirmation: [input field]
- Generate a scrambled password to prevent local database logins for this user:
- Full name: Gianluca Pagliuca
- E-Mail: [input field]
- Comment: [input field]
- Preferred landing page: [input field]
- Language: Default
- Login shell: /sbin/nologin
- Expiration date: [input field]
- Group Memberships: Not Member Of [input field]
- Effective Privileges: Inherited from ChangePassword
- User Certificates: Name [input field]
- API keys: key
- OTP seed: ADDYTEBOKGLT5XKDLUTFBIG4IRSHIJ
- OTP QR code: Click to unhide

Multi-Factor Authentication Configuration Panel:

Category	Field / Action
User Certificates	Table with columns: Name, CA, Valid From, Valid To. Includes a '+' button.
API keys	key [input field]. Includes a '+' button.
OTP seed	ADDYTEBOKGHHHSSOLUTFBIG4IRSHIJ [input field]. Includes checkbox: Generate new secret (160 bit).
OTP QR code	Click to unhide [button]
Authorized keys	Paste an authorized keys file here. [input field]
IPsec Pre-Shared Key	[input field]

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/ezyjJ	20210520094523	1621842348	28800
kx]RV.lr	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

i Descriptive name	<input type="text"/>
i Type	LDAP ▾
i Hostname or IP address	LDAP
i Port value	LDAP + Timebased One Time Password
i Transport	Local + Timebased One Time Password
	Radius
	Voucher
	TCP - Standard ▾