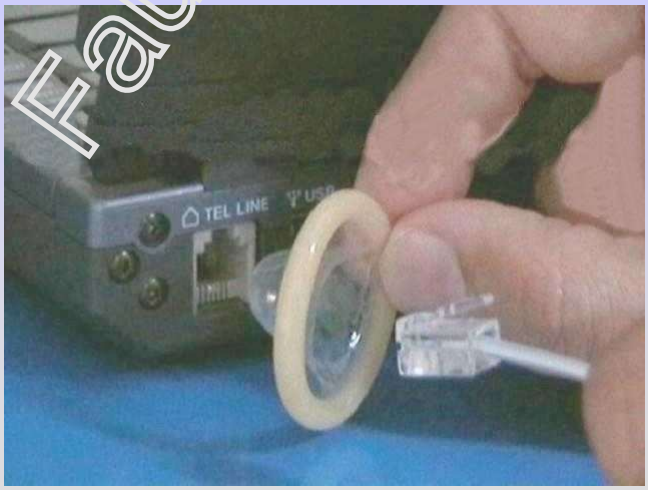
pfSense

pfSense – Un firewall in 5 minuti
(God help us!)

Fausto Marcantoni
fausto.marcantoni@unicam.it

1

Prevenire è meglio che curare



2

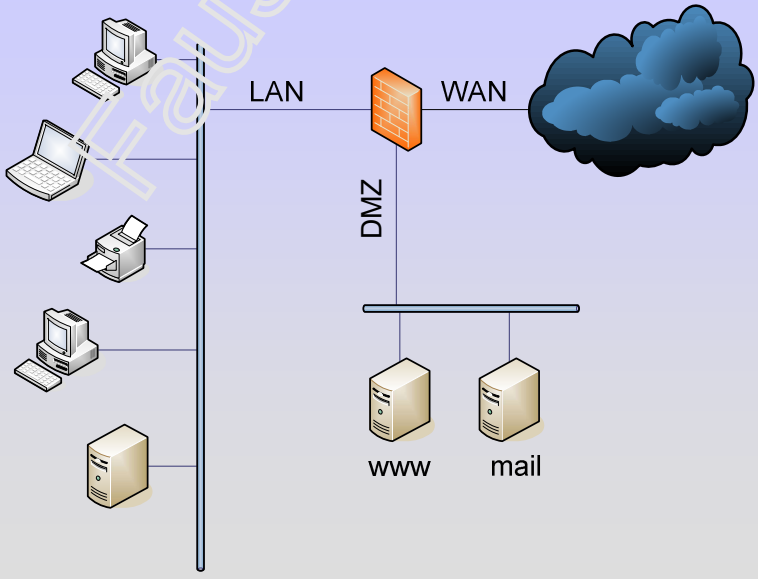
Chi ben comincia …

- **"Tutto ciò che non è espressamente permesso è vietato"**
  - Maggior sicurezza
  - Più difficile da gestire
- **"Tutto ciò che non è espressamente vietato, è permesso"**
  - Minor sicurezza (porte aperte)
  - Più facile da gestire

Un firewall non si compra si progetta

3

Topologia della rete



4

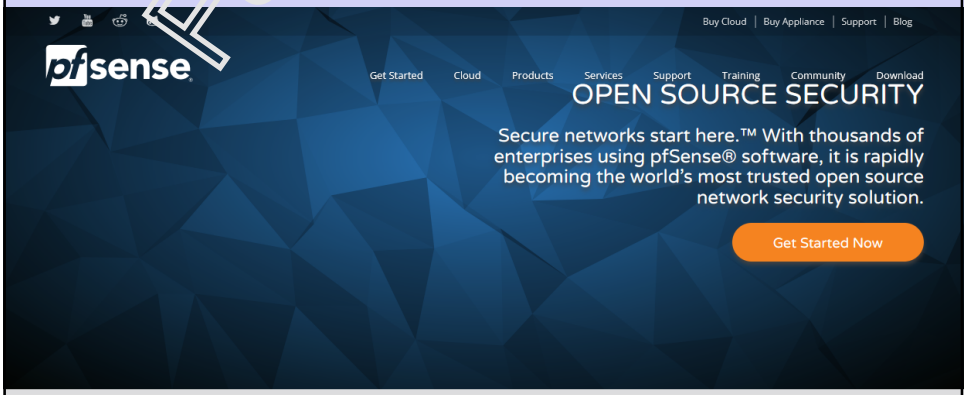
FIREWALL – pfSense

- pfSense in dettaglio
  - Sito wwww
  - Hardware
  - Software
  - Applicazioni embedded
  - Installazione
  - Configurazione
  - Prestazioni (monitoring)

5

pfSensel – sito www

https://pfsense.org/



6

pfSense – hardware

Minimum Hardware Requirements

The minimum hardware requirements for pfSense® software on hardware not sold by Netgate are:

- 64-bit amd64 (x86-64) compatible CPU
- 1GB or more RAM
- 8 GB or larger disk drive (SSD, HDD, etc)
- One or more compatible network interface cards
- Bootable USB drive or high capacity optical drive for initial installation

https://www.freebsd.org/releases/14.0R/

7

pfSensel – functions and features

The main pfSense functions and features are:

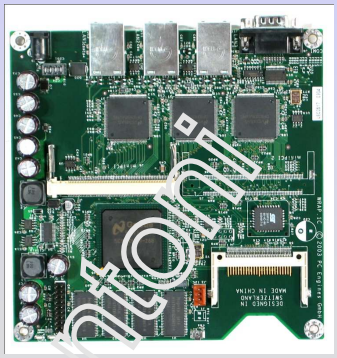
- **Firewall**
- **Stateful**: pfSense is a stateful firewall
- **Network Address Translation (NAT)**
- **Redundancy** allows for hardware failover
- **Load Balancing**
- **VPN**
  - **IPsec**
  - **OpenVPN**
- **Reporting and Monitoring**
  - **RRD Graphs**
  - **Real Time Information**
- **Dynamic DNS**
- **Captive Portal**
- **DHCP Server and Relay**
- **And More...**

8

pfSense – applicazioni embedded

https://www.pfsense.org/hardware/index.html#vendors

http://www.a-enterprise.ch/content/m0n0wall.htm

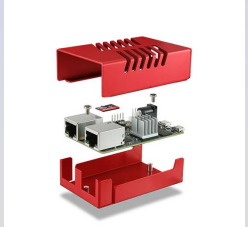


http://www.pcengines.ch/wrap.htm

9

pfSense – applicazioni embedded

https://pfsense.org/products/



10

pfSense – software

FreeBSD
OpenBSD's pf
mini_httpd
PHP configuration subsystem
webGUI

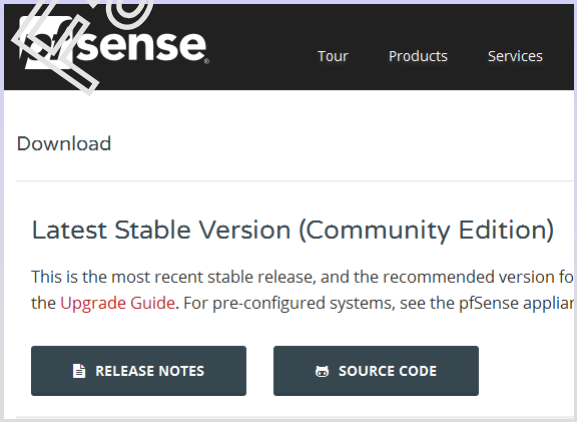
Packages

https://docs.netgate.com/pfsense/en/latest/packages/list.html

11

pfSense – software download

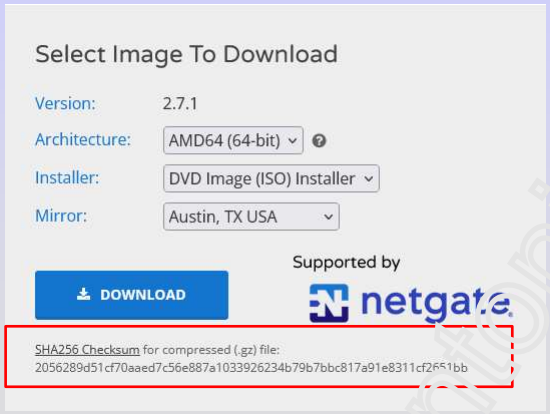
Quale file scaricare ???



12

pfSense – software download

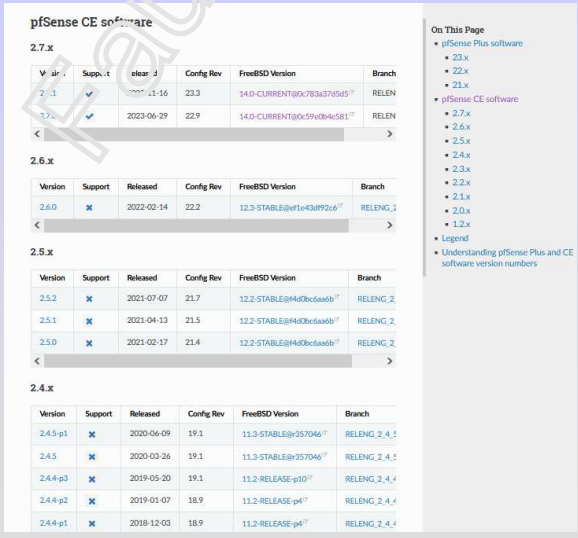
Quale file scaricare ???



13

pfsense download old version

https://docs.netgate.com/pfsense/en/latest/releases/versions.html#pfsense-ce-software



14

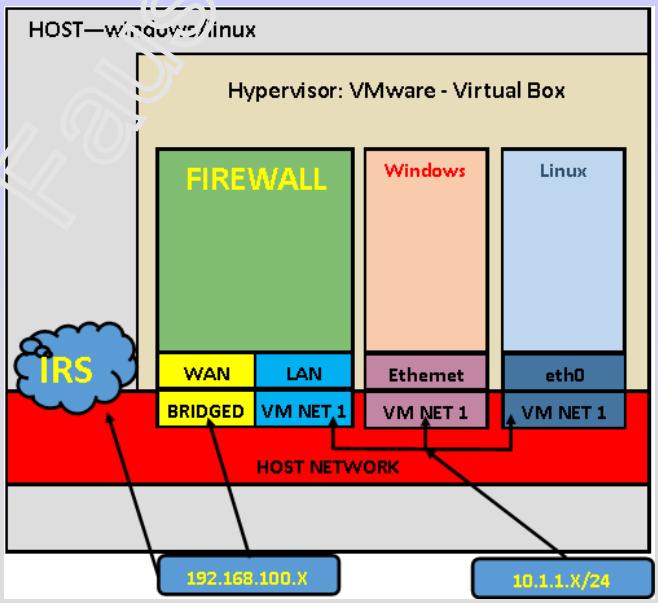
pfSense – installazione

- download the ISO image
- burn the ISO image onto a CD-R (or -RW)
- power up your PC, enter the BIOS and make sure that booting from CD-ROM is **enabled**
- insert CD-ROM
- boot

Installation Guides

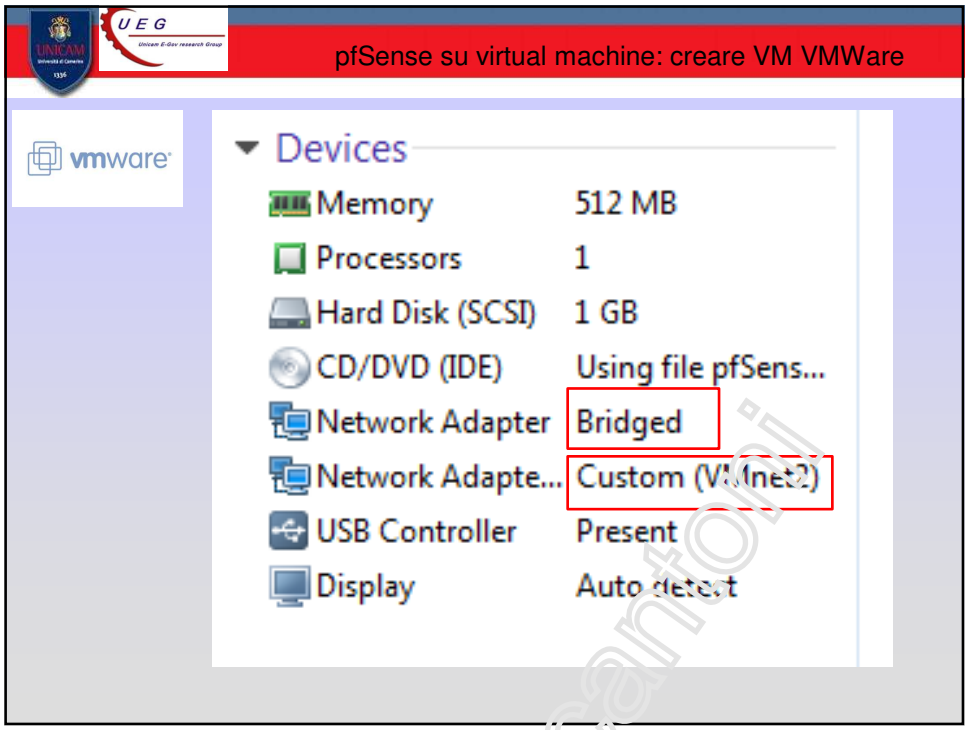
https://docs.netgate.com/pfsense/en/latest/install/download-installer-image.html

15



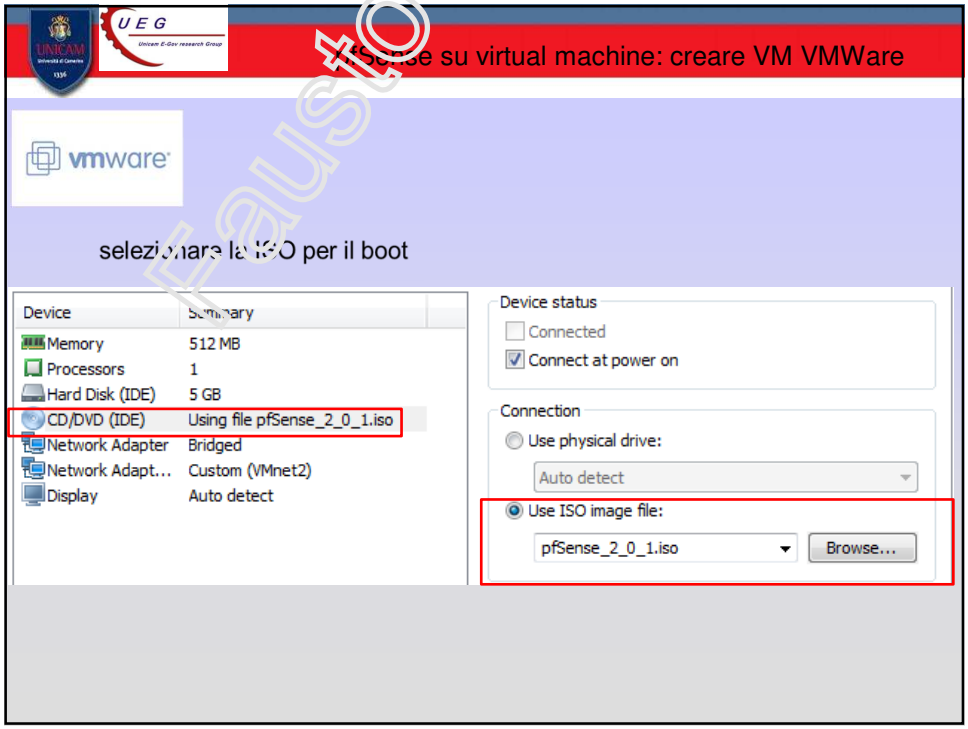
16

pfSense su virtual machine: creare VM VMWare

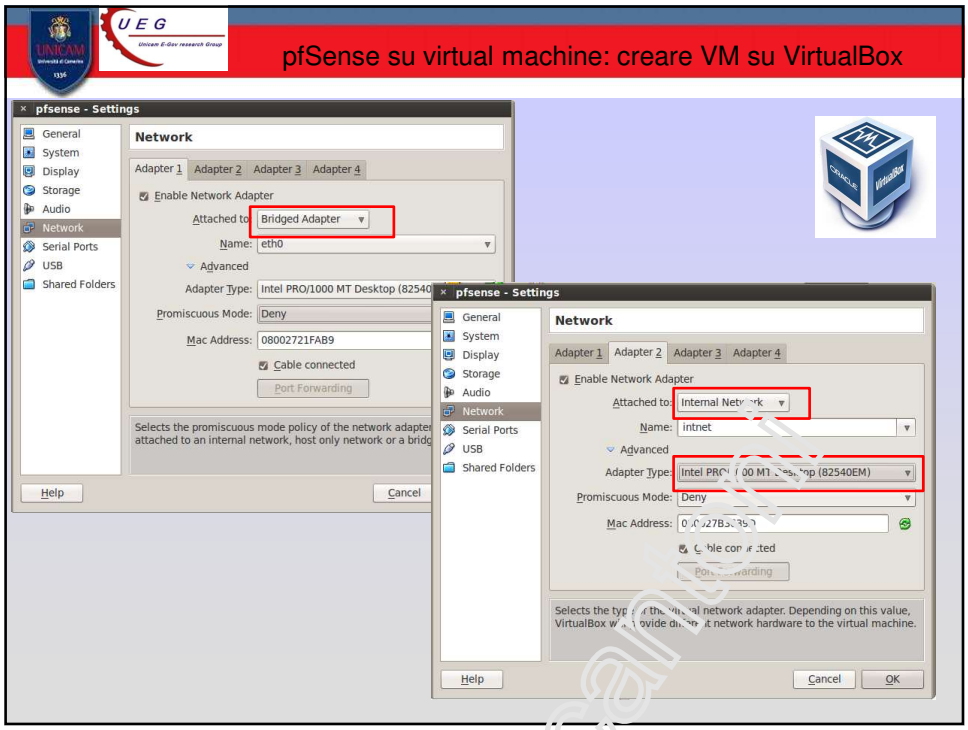


17

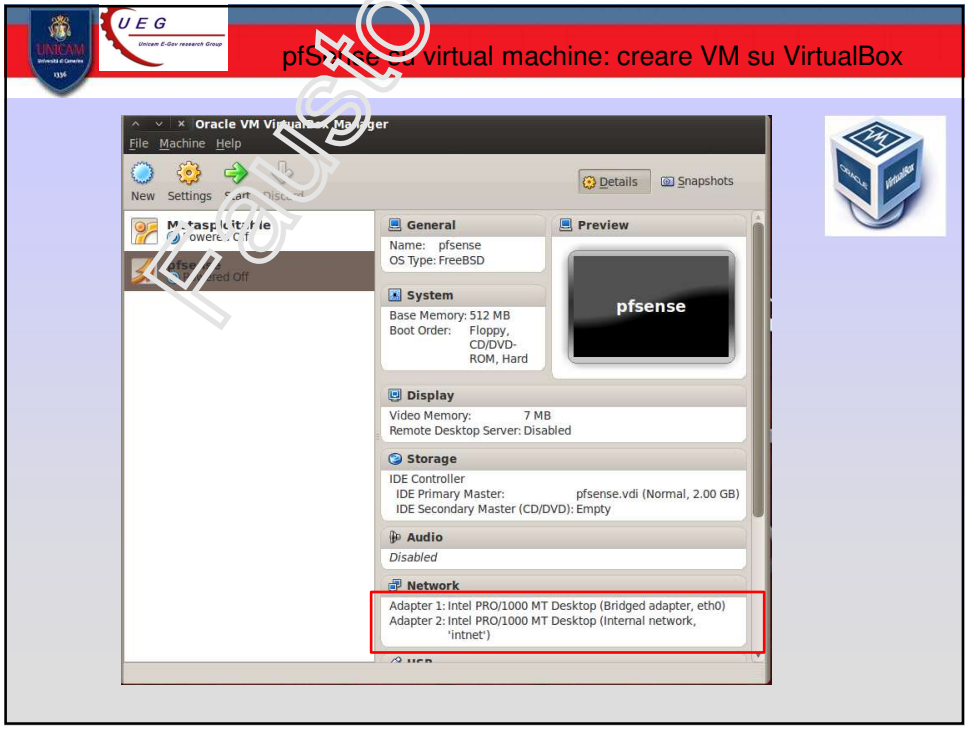
pfSense su virtual machine: creare VM VMWare



18


pfSense su virtual machine: creare VM su VirtualBox
pfsense - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Bridged Adapter
Name: eth0
Advanced
Adapter Type: Intel PRO/1000 MT Desktop (82540
Promiscuous Mode: Deny
Mac Address: 08002721FAB9
Cable connected
Port Forwarding
Selects the promiscuous mode policy of the network adapter attached to an internal network, host only network or a bridg
Help
Cancel
pfsense - Settings
Attached to: Internal Network
Name: intnet
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Deny
Mac Address:
Cable connected
Port Forwarding
Selects the type of the virtual network adapter. Depending on this value, VirtualBox provides different network hardware to the virtual machine.
Help
Cancel
OK

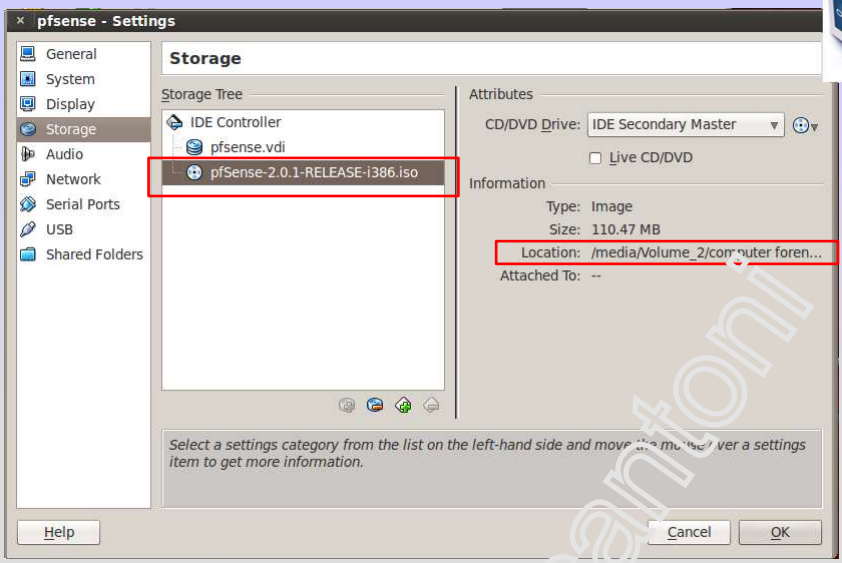
19


pfSense su virtual machine: creare VM su VirtualBox
Oracle VM VirtualBox Manager
File Machine Help
New
Settings
Details
Snapshots
General
Name: pfsense
OS Type: FreeBSD
Preview
pfsense
System
Base Memory: 512 MB
Boot Order: Floppy, CD/DVD-ROM, Hard
Display
Video Memory: 7 MB
Remote Desktop Server: Disabled
Storage
IDE Controller
IDE Primary Master: pfsense.vdi (Normal, 2.00 GB)
IDE Secondary Master (CD/DVD): Empty
Audio
Disabled
Network
Adapter 1: Intel PRO/1000 MT Desktop (Bridged adapter, eth0)
Adapter 2: Intel PRO/1000 MT Desktop (Internal network, 'intnet')

20

pfSense su virtual machine: creare VM su VirtualBox

selezionare la ISO per il boot



21

pfSense su virtual machine: creare VM

https://docs.netgate.com/pfsense/en/latest/

22

pfSense su VM: boot / setup bios

23

pfSense su VM: boot

non riesco ad entrare nel BIOS: è troppo veloce

R... Cannot press ESC to get into BIOS fast enough

Edit your .vmx file and add the line:

```
bios.bootDelay = "5000"
```

which adds a 5000 millisecond (5 second) delay to the boot, or add:

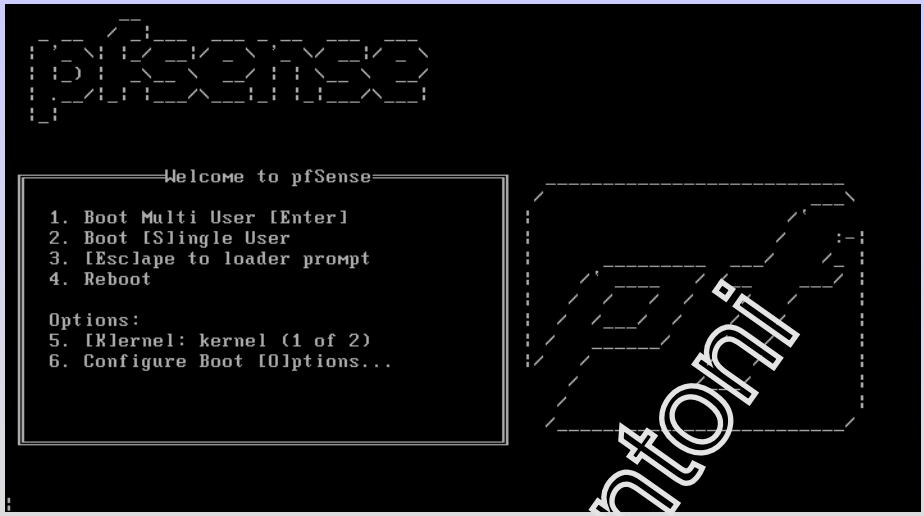
```
bios.forceSetupOnce = "TRUE"
```

to make the VM enter the BIOS setup at the next boot.

Google vmware bios delay

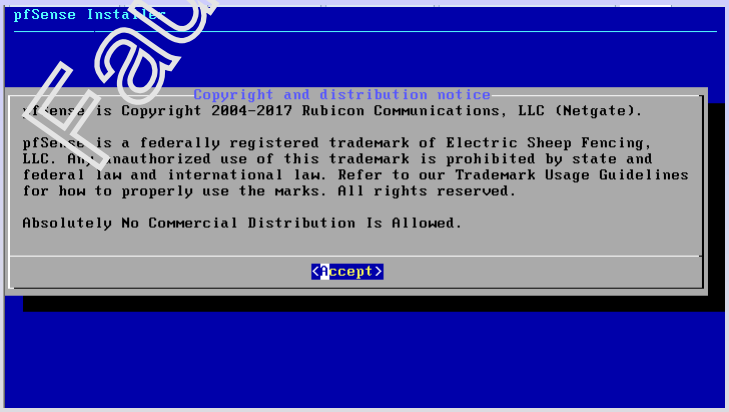
24

pfSense: startup page



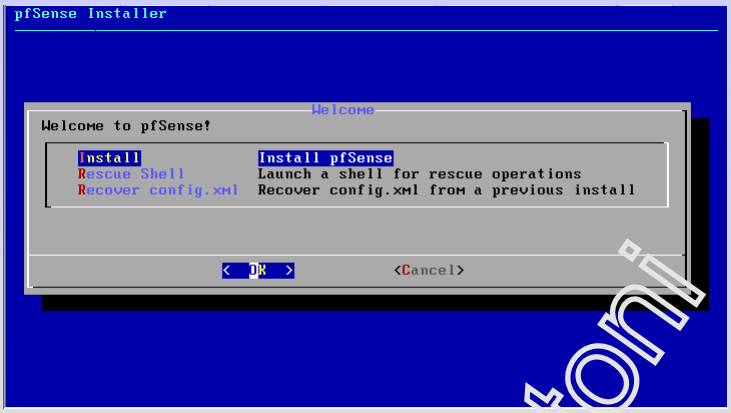
25

pfSense – installazione – primo avvio



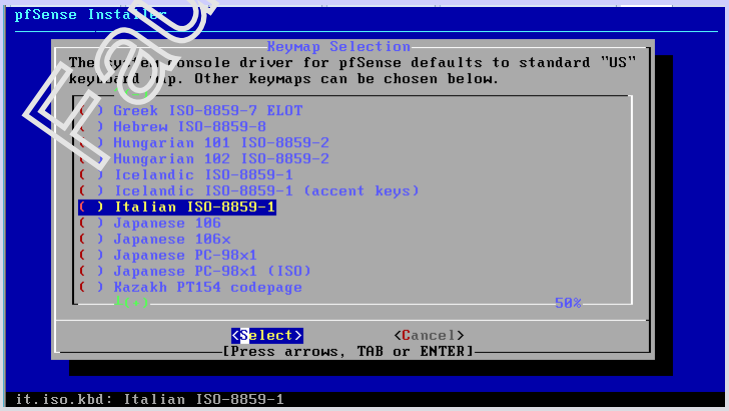
26

pfSense – installazione – primo avvio



27

pfSense – installazione



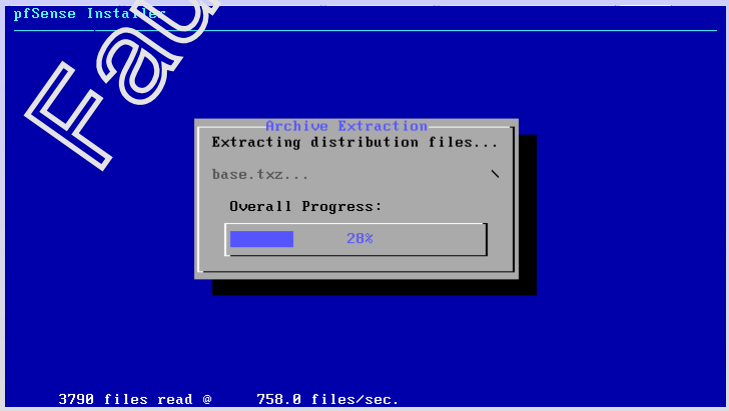
Scegliere il layout della tastiera

28

pfSense – installazione

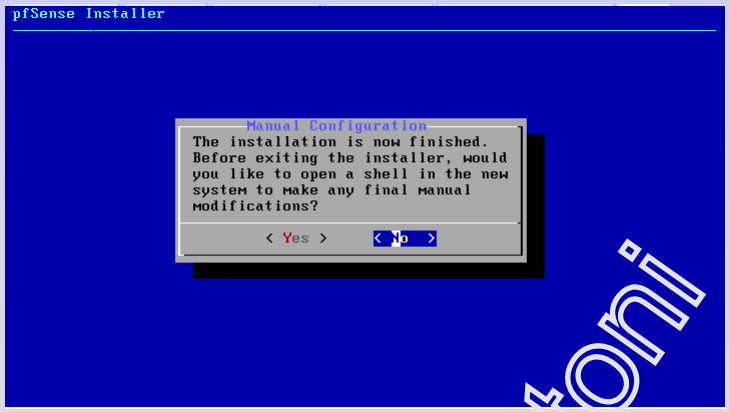
29

pfSense – installazione



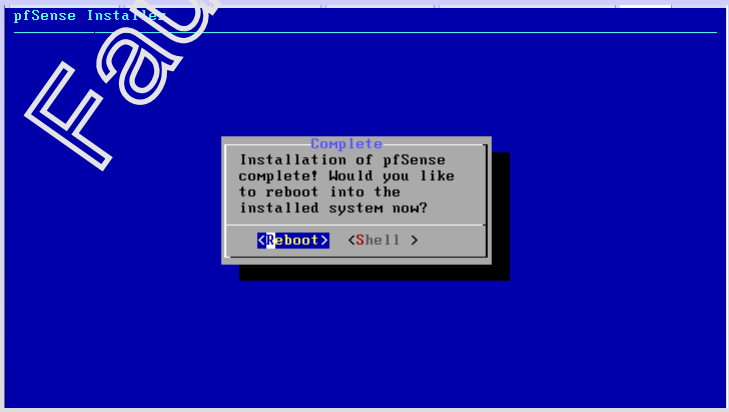
30

pfSense – installazione



31

pfSense – installazione



Fatto …

32

pfSense – installazione

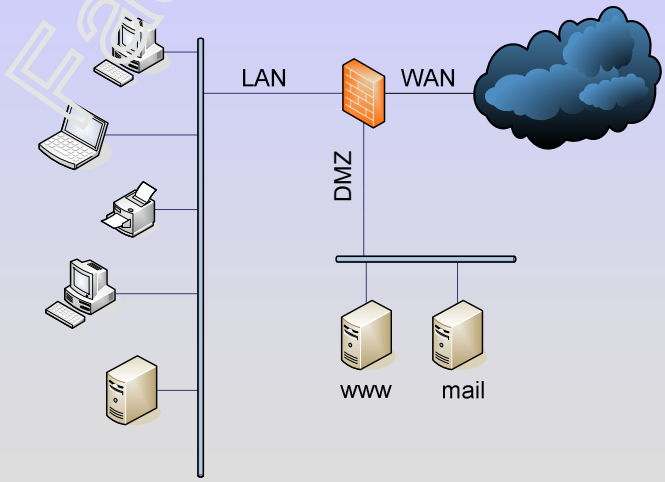
```
The IPv4 LAN address has been set to 10.1.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://10.1.1.1/

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 65fd114079cc108c23c9

*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.100.75/22
 LAN (lan)       -> em1        -> v4: 10.1.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (ssh)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

… Fatto …

33

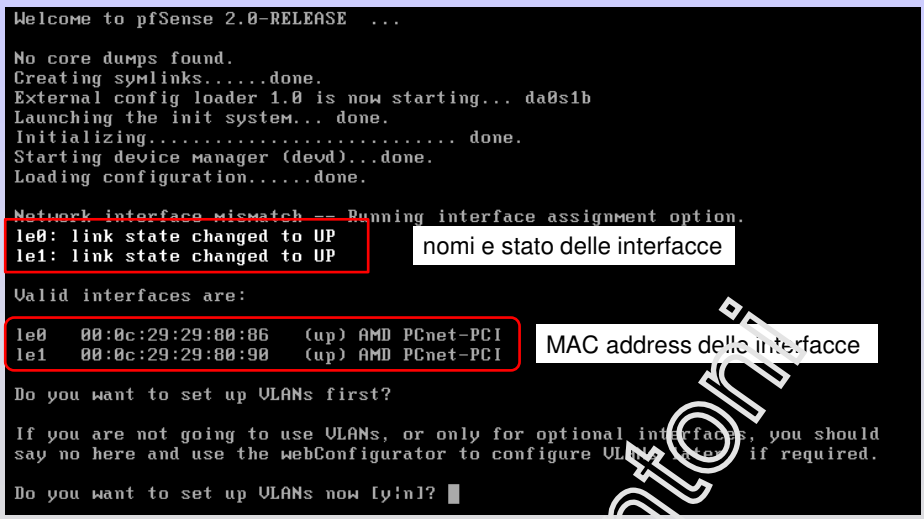
pfSense – configurazione – primo avvio

Assegnazione delle interfacce di rete: LAN – WAN – DMZ



34

pfSense – installazione

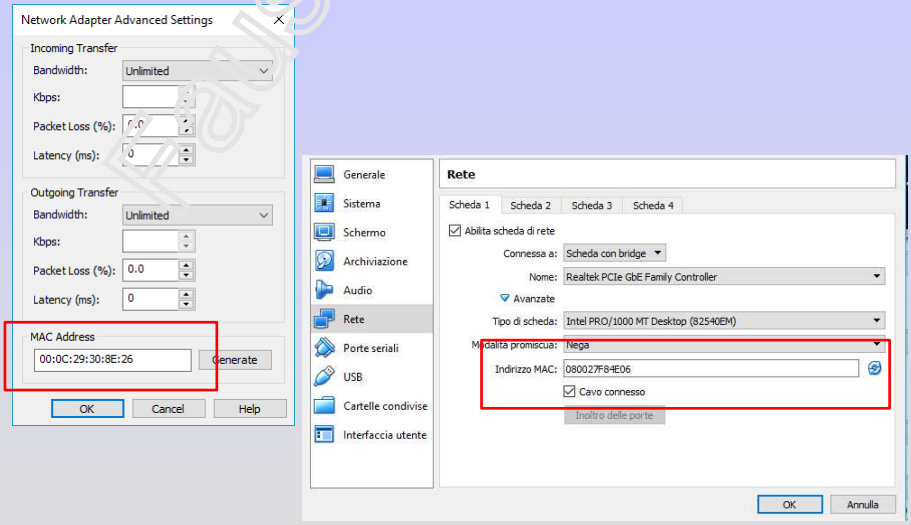


nomi e stato delle interfacce

MAC address delle interfacce

35

pfSense – installazione



36

pfSense su VM: configurazione ethernet

aprire la configurazione della VM con notepad: **pfsense.vmx**

```
ide1:0.deviceType = "cdrom-image"
ethernet0.present = "TRUE"
ethernet0.wakeOnPcktRcv = "FALSE"
ethernet0.addressType = "generated"
usb.present = "TRUE"
ehci.present = "TRUE"
vmci0.present = "TRUE"
usb.vbluetooth.startConnected = "TRUE"
displayName = "pfsense 2.0"
guestOS = "other26xlinux"
nvram = "pfsense 2.0.nvram"
virtualHW.productCompatibility = "hosted"
extendedConfigFile = "pfsense 2.0.vmxf"
ethernet1.present = "TRUE"
ethernet1.vnet = "VMnet2"
ethernet1.connectionType = "custom"
ethernet1.wakeOnPcktRcv = "FALSE"
ethernet1.addressType = "generated"
ethernet0.generatedAddress = "00:0c:29:29:80:86"
ethernet1.generatedAddress = "00:0c:29:29:80:90"
vmci0.id = "1764327558"
```


37

pfSense – installazione

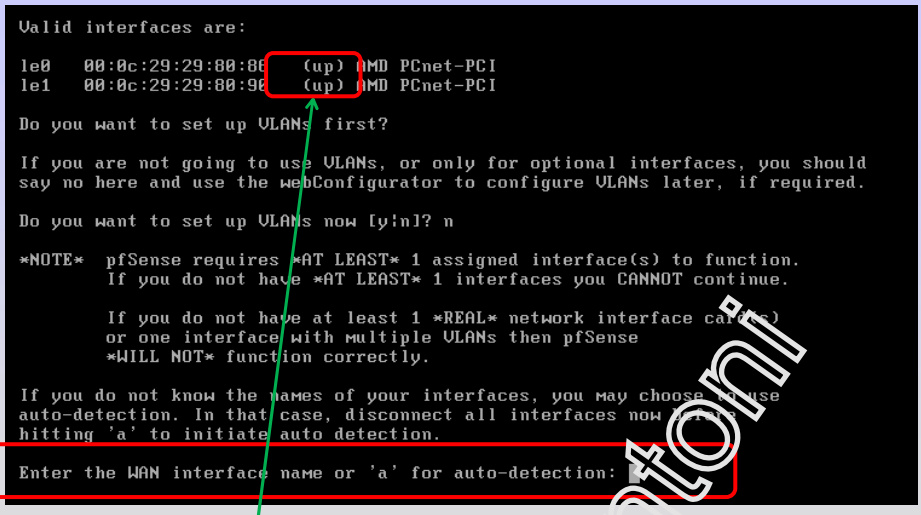
```
Welcome to pfSense 2.0-RELEASE ...

No core dumps found.
Creating symlinks.....done.
External config loader 1.0 is now starting... da0s1b
Launching the init system... done.
Initializing ..... done.
Starting device manager (devd)...done.
Loading configuration......done.

Network interface mismatch -- Running interface assignment option.
le0: link state changed to UP
le1: link state changed to UP

Valid interfaces are:

le0   00:0c:29:29:80:86   (up) AMD PCnet-PCI
le1   00:0c:29:29:80:90   (up) AMD PCnet-PCI

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]?
```

NO VLANs

http://it.wikipedia.org/wiki/VLAN

38

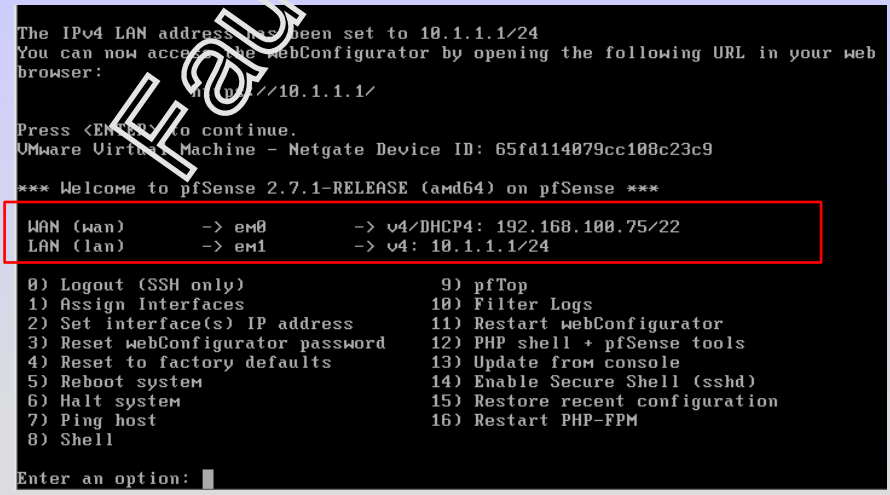
pfSense – assegnare le interfacce di rete



tramite i tools le interfacce possono essere spente/riaccese per meglio individuare quella da utilizzare

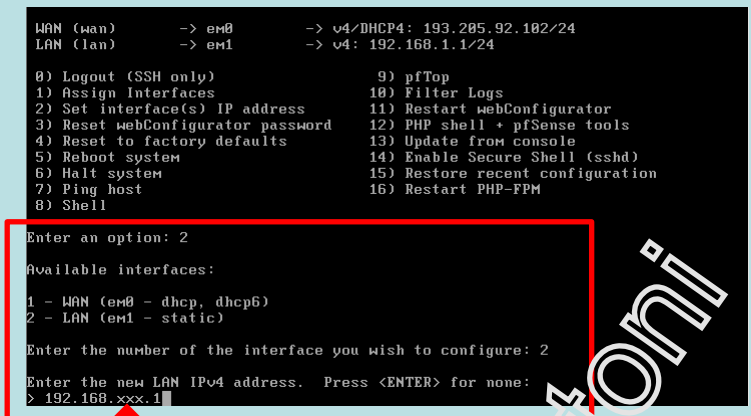
39

pfSense – configurare la LAN



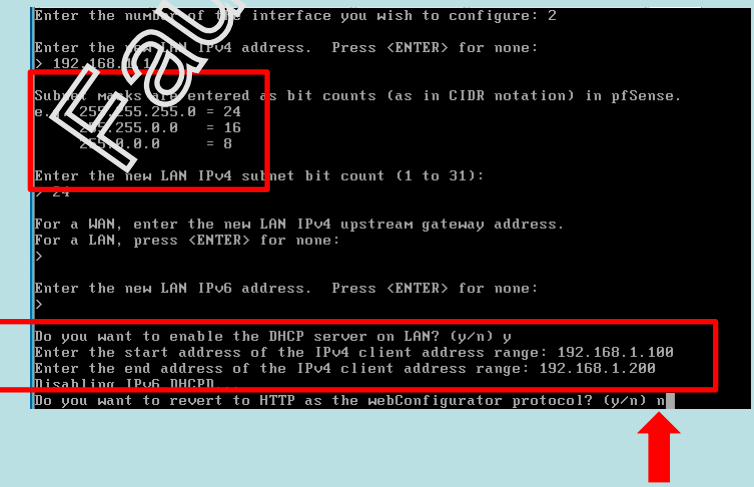
40

pfSense – configurare la LAN



41

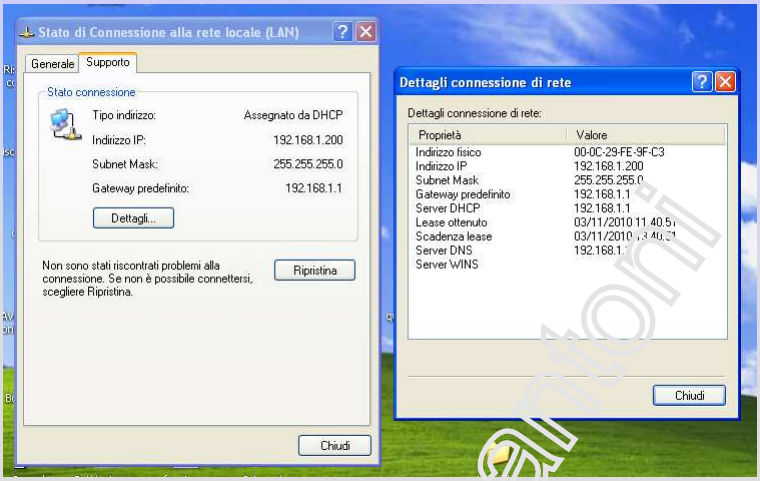
pfSense – configurare la LAN



42

Avviare il client

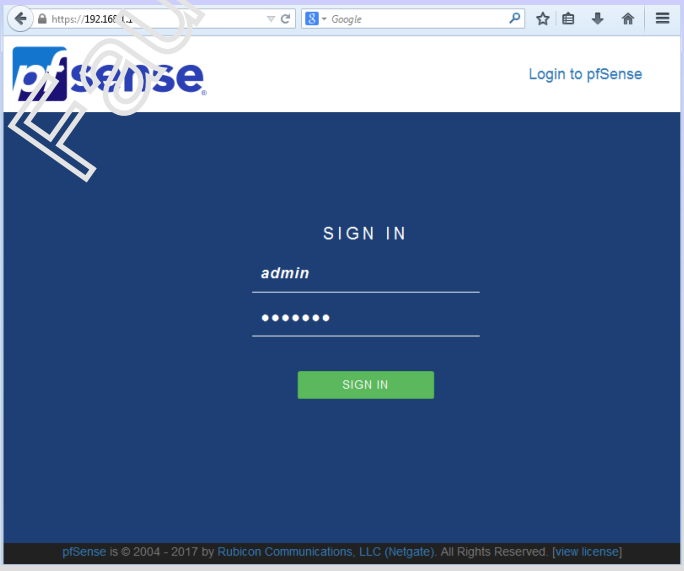
Avviare il sistema sul PC client e controllare gli indirizzi IP



43

pfSense – configurazione - autenticazione

https://192.168.1.1/



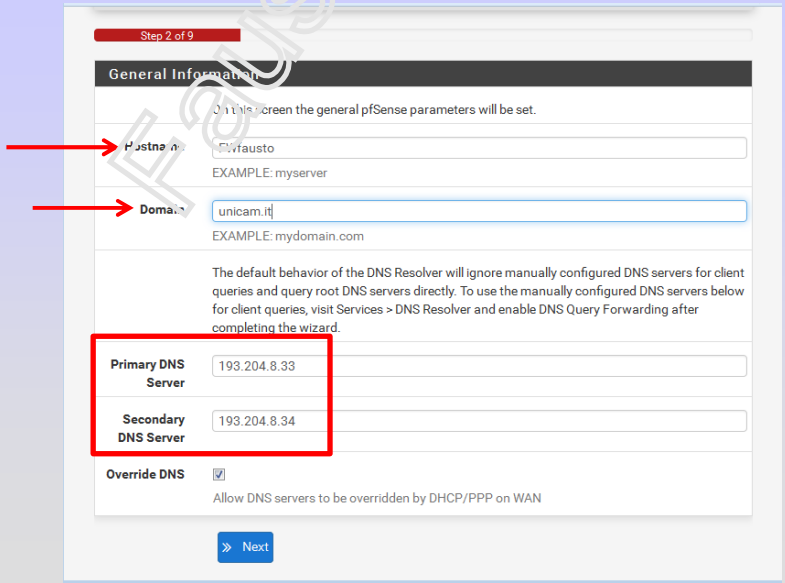
44

pfSense – configurazione – Setup Wizard

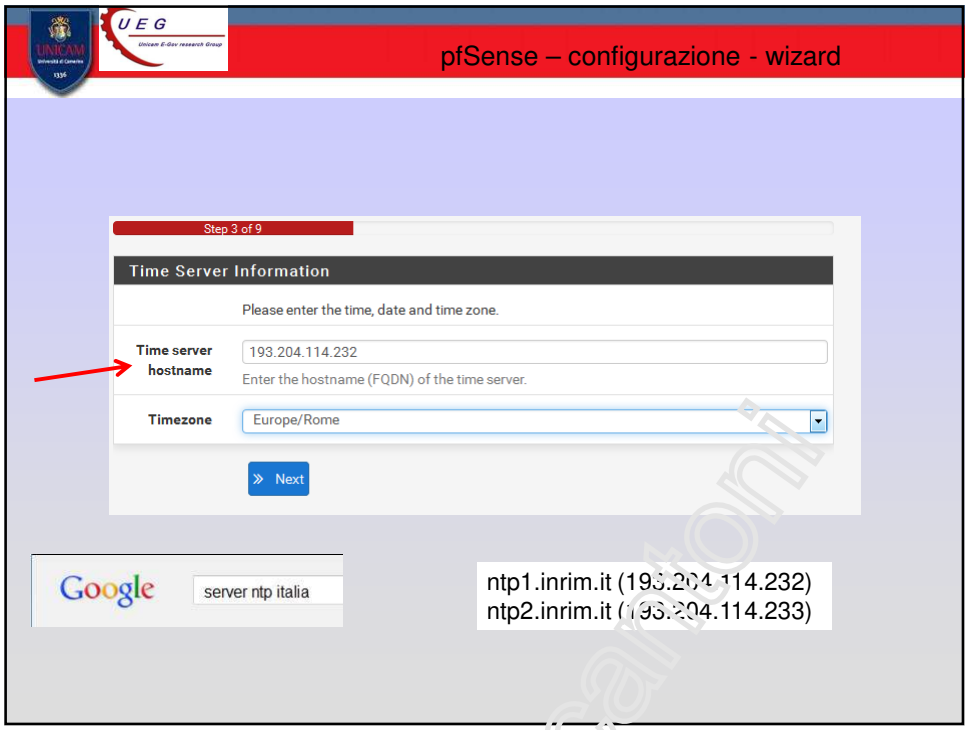
- Hostname
- Domain
- DNS server
- NTP time server (importante per i log)
- Interfaccia WAN
- Interfaccia LAN
- Username & Password

45

pfSense – configurazione - wizard



46

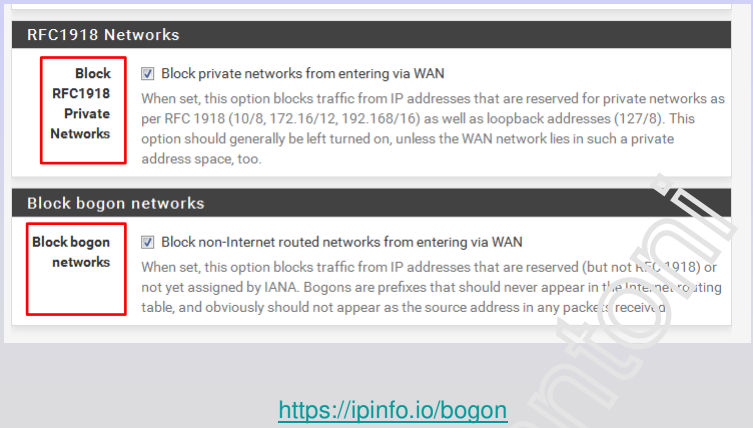

pfSense – configurazione - wizard
Step 3 of 9
Time Server Information
Please enter the time, date and time zone.
Time server hostname
193.204.114.232
Enter the hostname (FQDN) of the time server.
Timezone
Europe/Rome
Next
Google
server ntp italia
ntp1.inrim.it (193.204.114.232)
ntp2.inrim.it (193.204.114.233)

47


pfSense – configurazione - wizard
Configure WAN Interface
On this screen the Wide Area Network information will be configured.
Static
DHCP
PPPoE
PPTP
MAC Address
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU
Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should

48

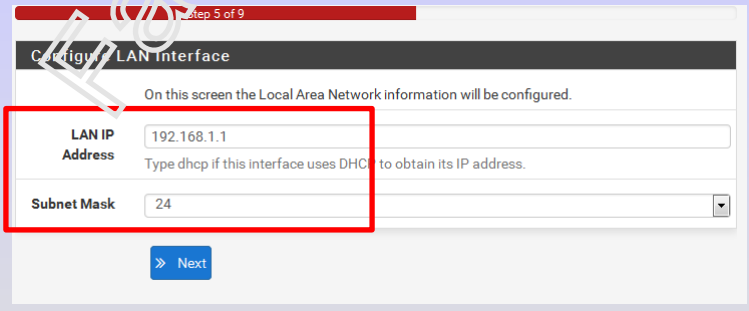
pfSense – configurazione - wizard



https://ipinfo.io/bogon

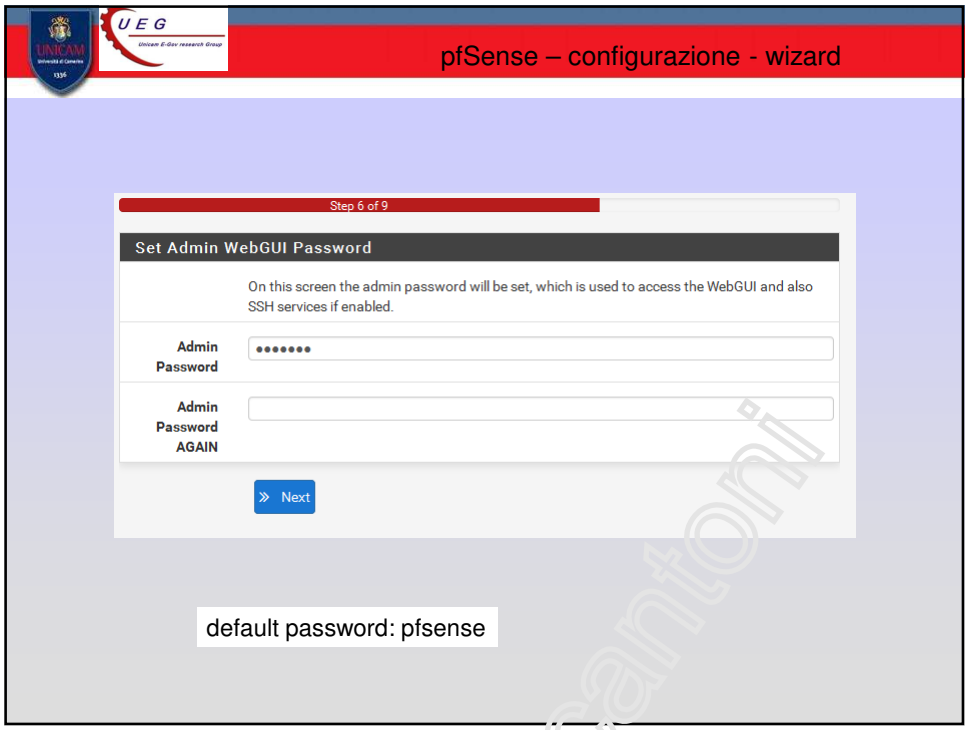
49

pfSense – configurazione - wizard



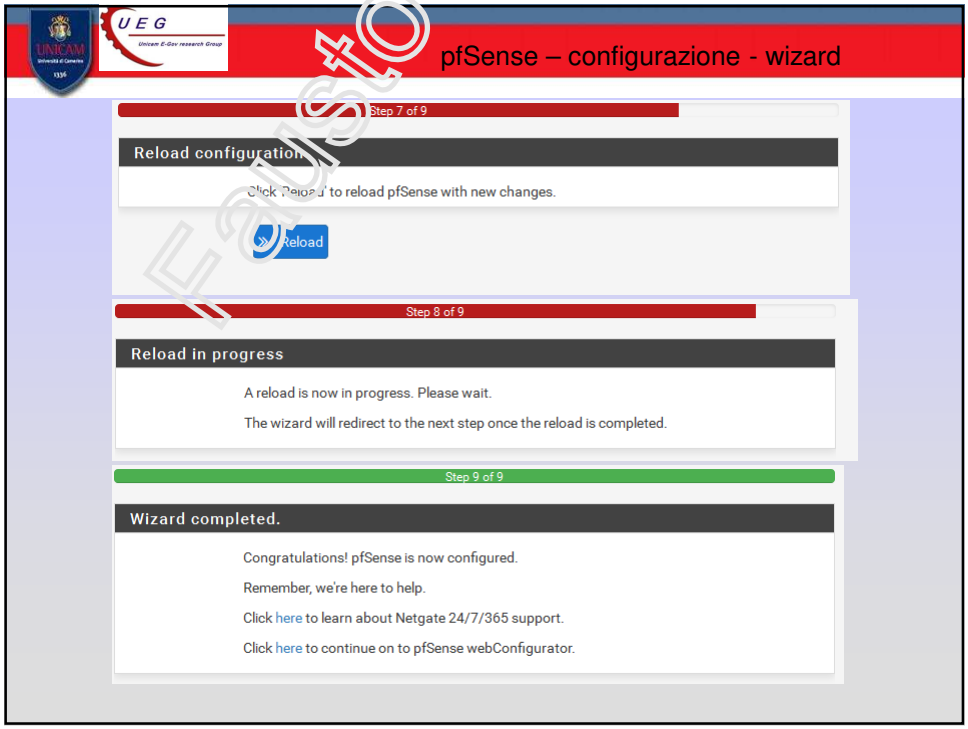
50

pfSense – configurazione - wizard



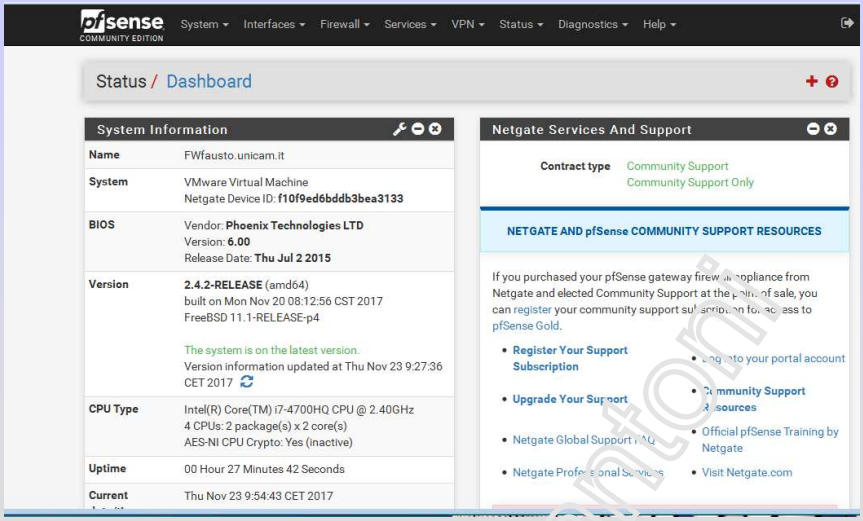
51

pfSense – configurazione - wizard



52

pfSense – configurazione – pagina principale



interfaccia GUI tramite browser

53

pfSense – configurazione - Interfaces

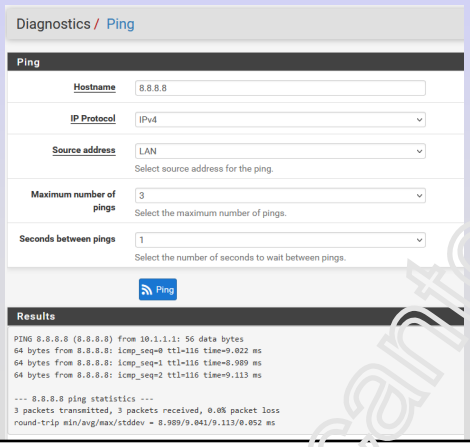
- LAN
  - Configurare l'indirizzo IP del FW e subnet mask
- WAN
  - Tipo di indirizzamento static – dhcp

block private network
RFC1918 (10/8, 172.16/12, 192.168/16)

54

Troubleshooting

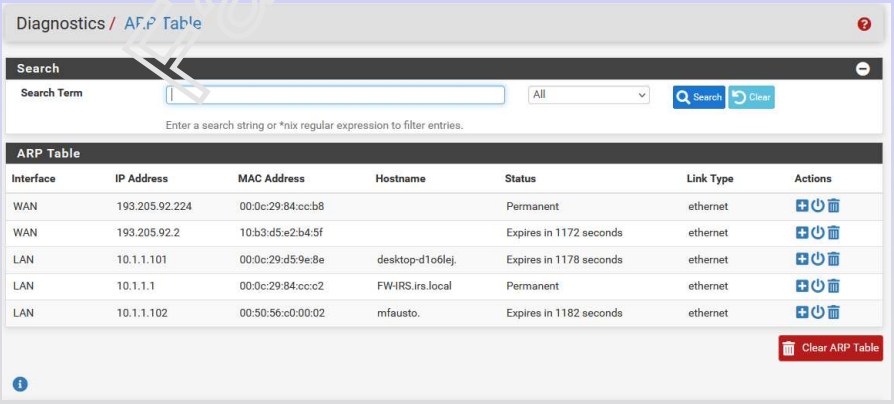
- Localizzazione dei guasti
- Analisi del problema
- Cosa non funzione
- “quello che ***almeno*** funziona”



55

Troubleshooting

Arp table



56

DHCP server

- Il DHCP, acronimo dall'inglese Dynamic Host Configuration Protocol (protocollo di configurazione dinamica degli indirizzi) è il protocollo usato per assegnare gli indirizzi IP ai calcolatori di una rete.
- In una rete basata sul protocollo IP, ogni calcolatore ha bisogno di un indirizzo IP, scelto in modo tale che appartenga alla sottorete a cui è collegato e che sia univoco, ovvero che non ci siano altri calcolatori che stiano già usando quell'indirizzo.
- Il compito di assegnare manualmente gli indirizzi IP ai calcolatori comporta un rilevante onere per gli amministratori di rete, soprattutto in reti di grandi dimensioni o in caso di numerosi computer che si connettono a rotazione solo ad ore o giorni determinati.

57

Il Client DHCP è un calcolatore che ha bisogno di ottenere un indirizzo IP valido per la sottorete a cui è collegato, e anche il programma che si occupa di richiedere l'indirizzo IP e configurarlo.

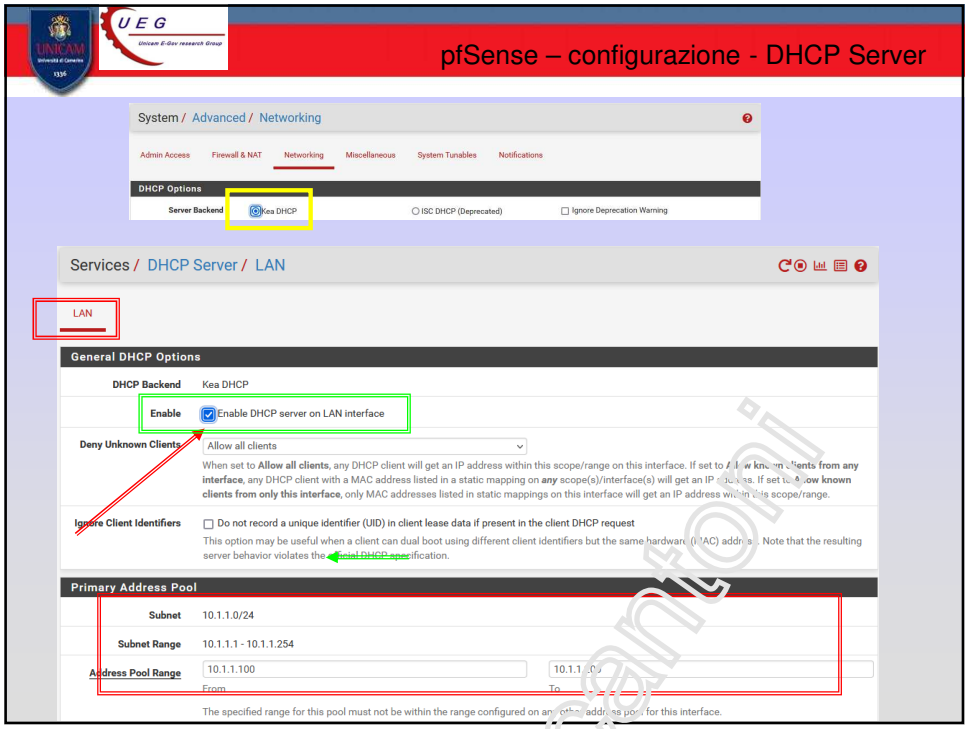
Il Server DHCP è il calcolatore che assegna gli indirizzi IP, e anche il processo che svolge questa funzione. Talvolta questa funzione è incorporata in un router.

Il DHCP relay e il calcolatore (o più spesso una funzione implementata in un router) che si occupa di inoltrare le richieste DHCP ad un server, qualora questo non sia sulla stessa sottorete. Questo componente è necessario solo se un server DHCP deve servire molteplici sottoreti. Deve esistere almeno un DHCP relay per ciascuna sottorete servita. Ogni relay deve essere esplicitamente configurato per inoltrare le richieste a uno o più server.

se nella rete non e' presente un DHCP server, il client (con Sistema Operativo Microsoft) prenderà un indirizzo IP nella classe 169.254.0.0 che è generato automaticamente dal Sistema Operativo e ritenterà la ricerca di un DHCP server nella rete, tutti gli altri Sistemi Operativi non prenderanno nessun indirizzo IP e non tenteranno successive richieste

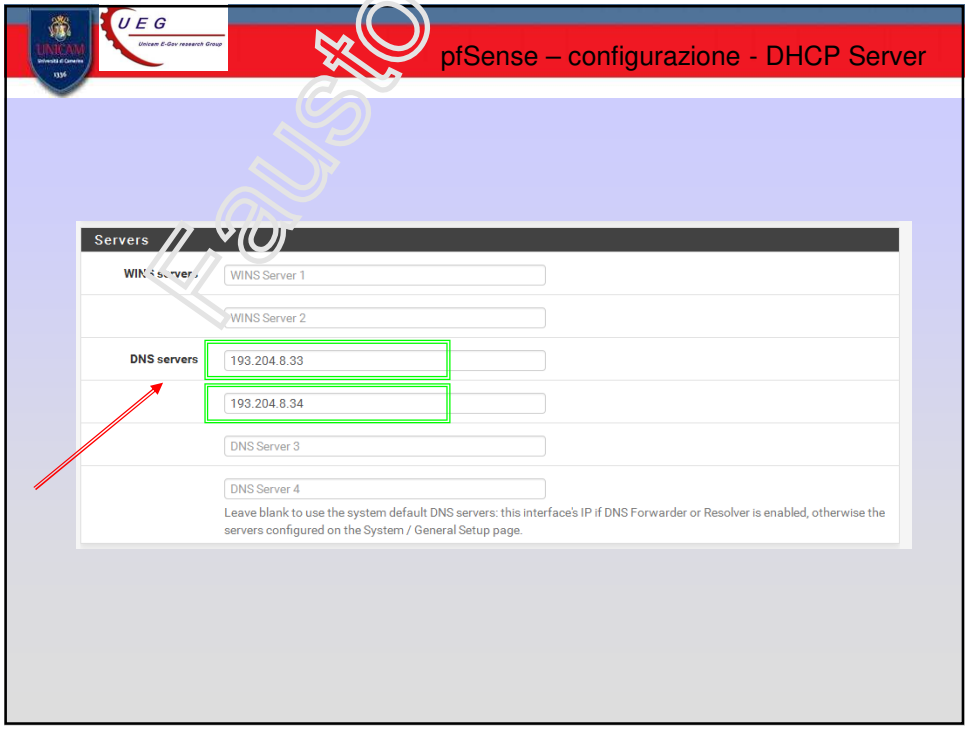
58

pfSense – configurazione - DHCP Server



59

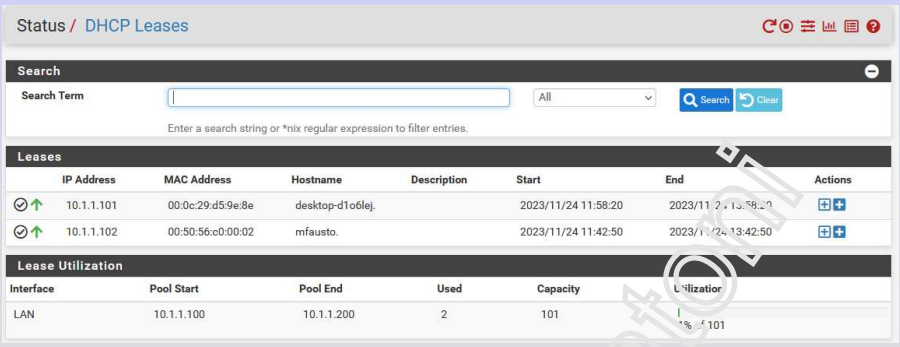
pfSense – configurazione - DHCP Server



60

pfSense – diagnostica - DHCP Lease

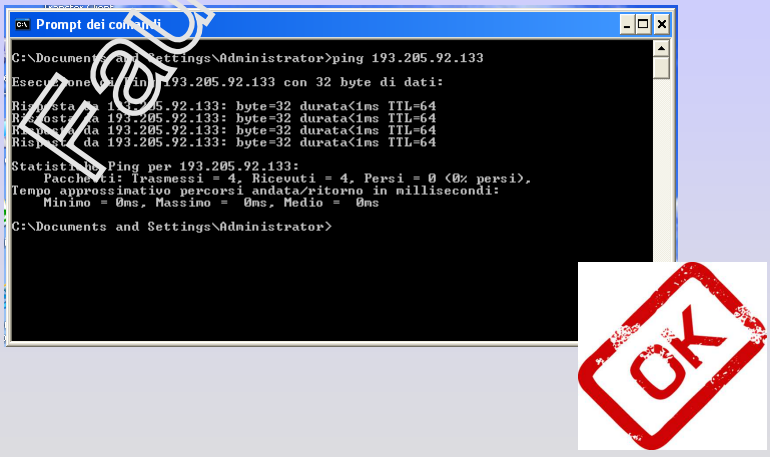
DHCP lease
lease = prendere in affitto
durata di validità (Lease Time)



61

Troubleshooting

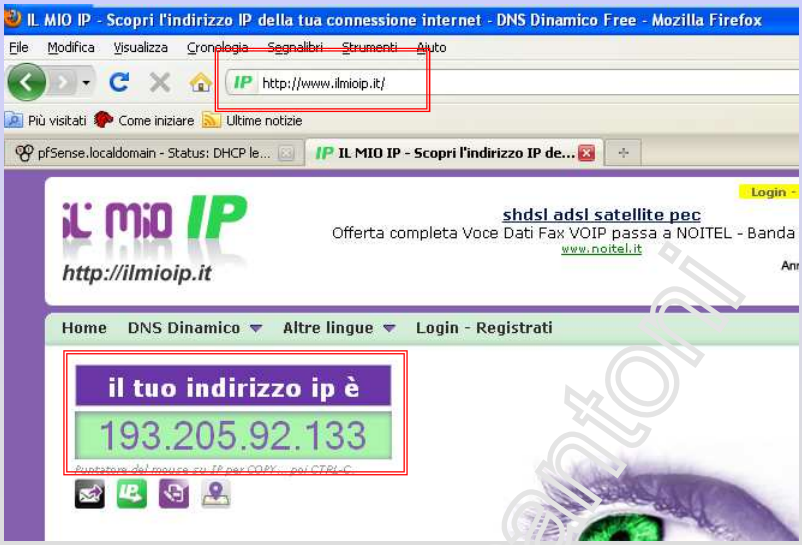
Dalla LAN provare a fare ping sull'indirizzo WAN del firewall



62

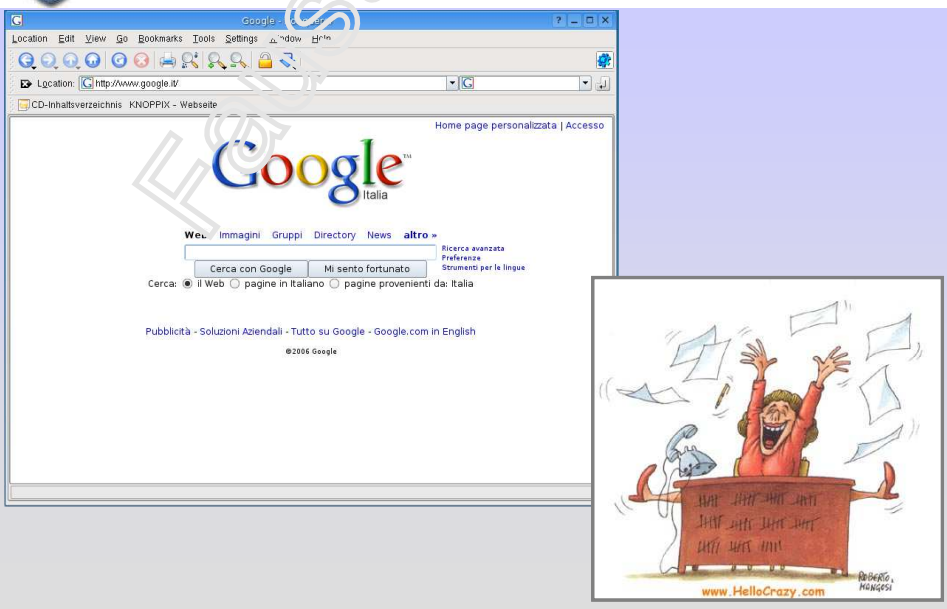
NAT – Network Address Translation

Chi sono io???



63

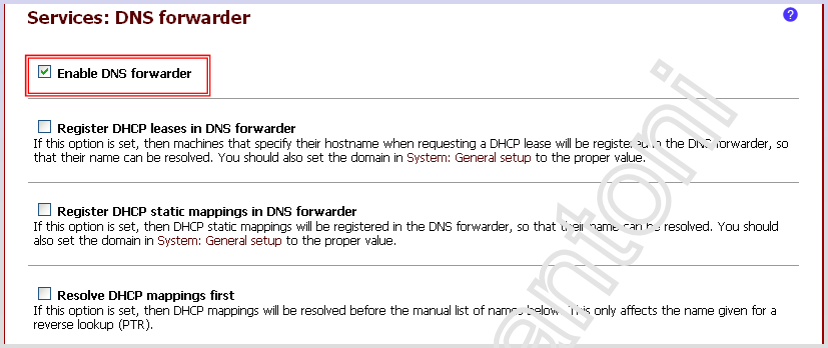
Tutto funziona – wow si naviga



64

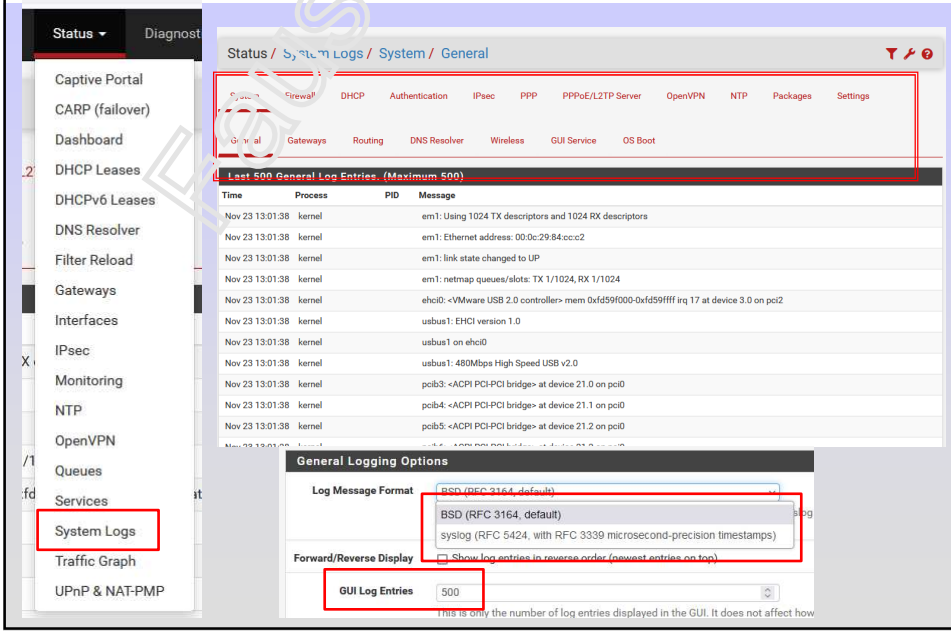
pfSense – Servizi - DNS Forwarder

- DNS forwarder
  - Usando il server DNS del vostro provider come "forwarder" farete in modo che le risposte alle vostre richieste siano più veloci e meno pesanti per la vostra rete.
  - Questo si ottiene facendo in modo che il vostro **name server** inoltri le richieste al **name server** del vostro provider.
  - Ogni volta che ciò accade è come se voi andaste a prelevare direttamente dall'ampia cache del name server del vostro provider, incrementando la velocità delle richieste e alleggerendo il carico sul vostro name server.



65

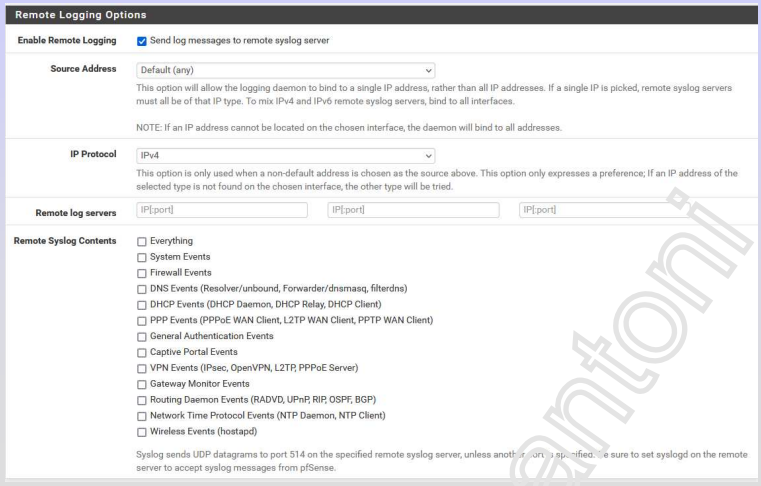
pfSense – Status - LOG



66

pfSense – configurazione - LOG

Send log messages to remote syslog server



67

pfSense – configurazione - Captive portal

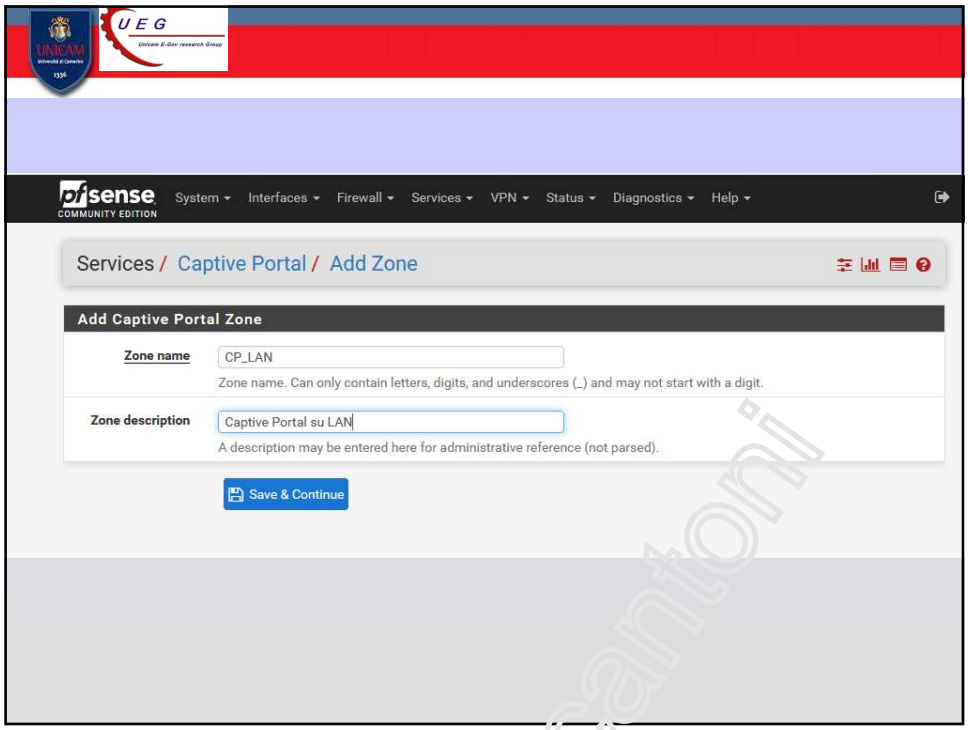
La tecnica del **CAPTIVE PORTAL** forza un client del servizio HTTP su una rete di collegarsi ad una Web page speciale (solitamente per gli scopi di autenticazione) prima di navigare in Internet normalmente.

Ciò è fatta intercettando tutto il traffico HTTP, senza riguardo all'indirizzo, fino a che l'utente non si disconnetta dal CAPTIVE PORTAL.

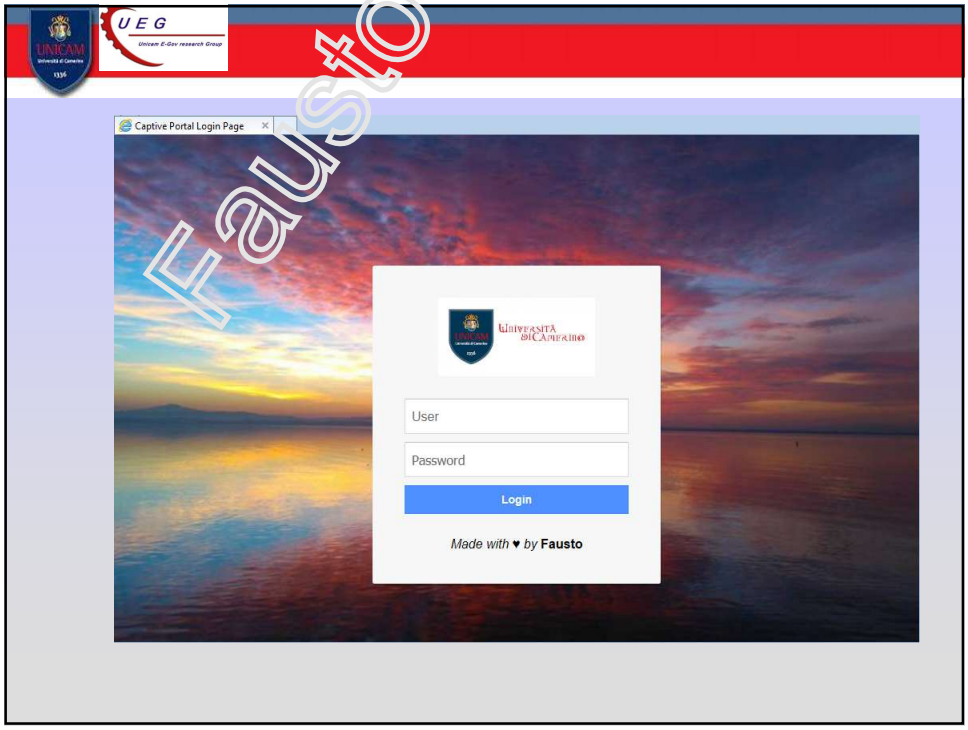
I Captive Portal si usano nella maggior parte dei hotspots Wi-Fi.

Può essere usato per controllare l'accesso a LAN Wiredo (per esempio gli edifici in condominio, i centri di affari, PMI, P.A.).

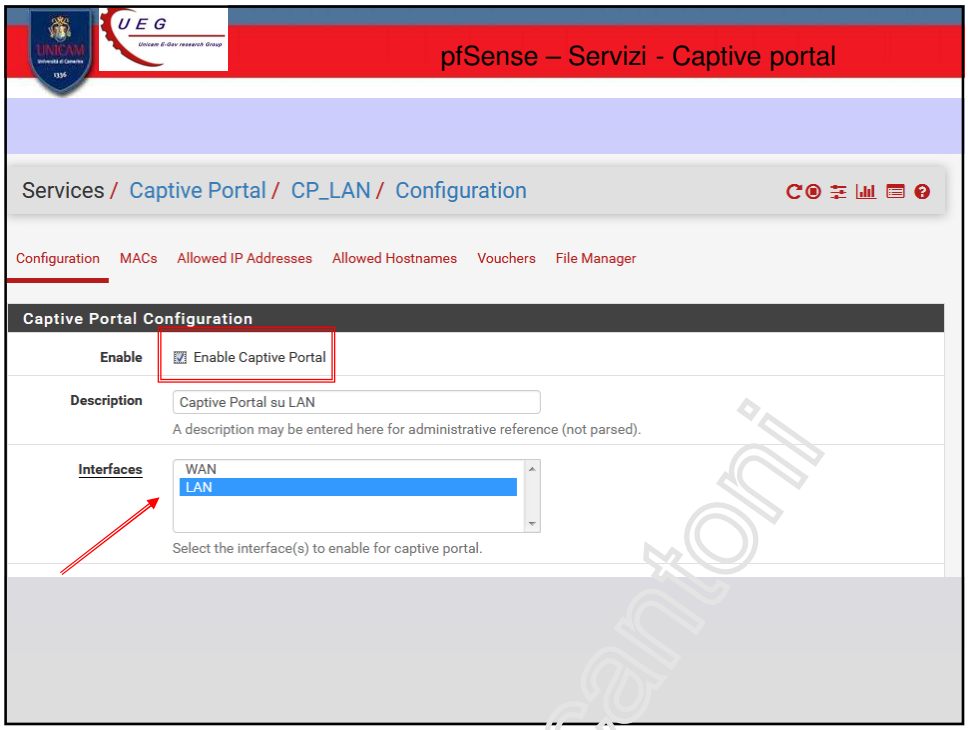
68



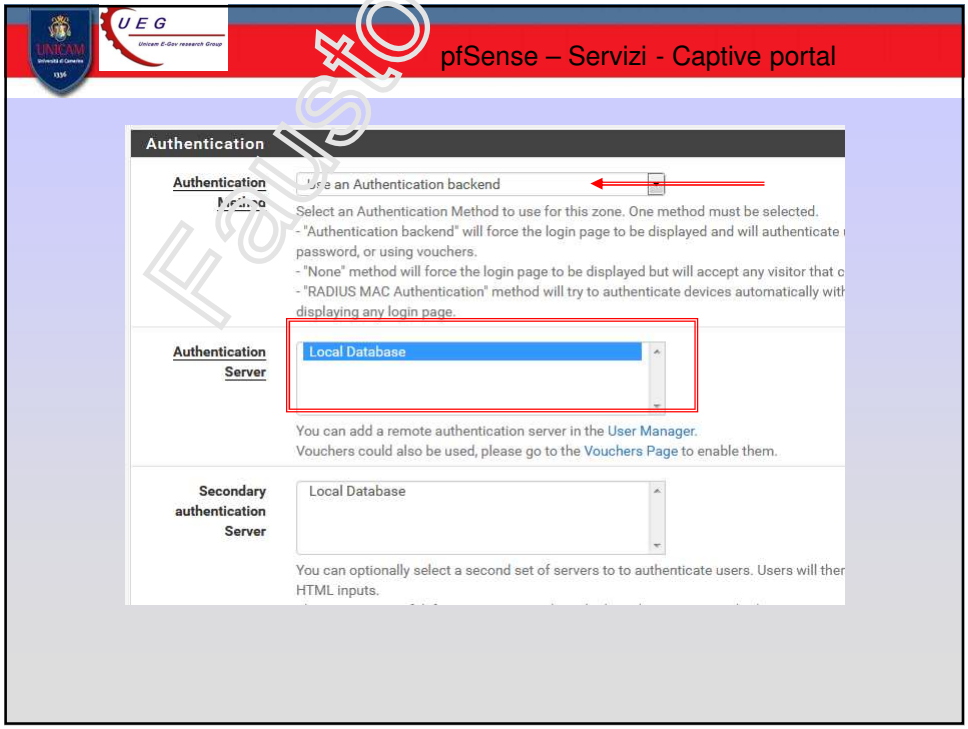
69



70

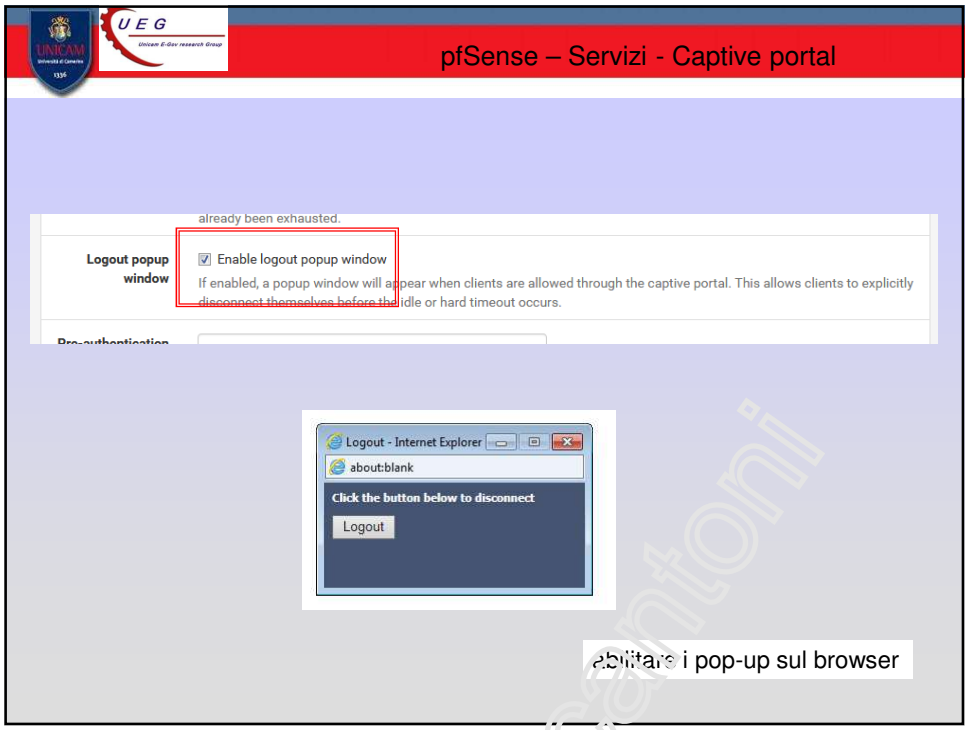


71



72

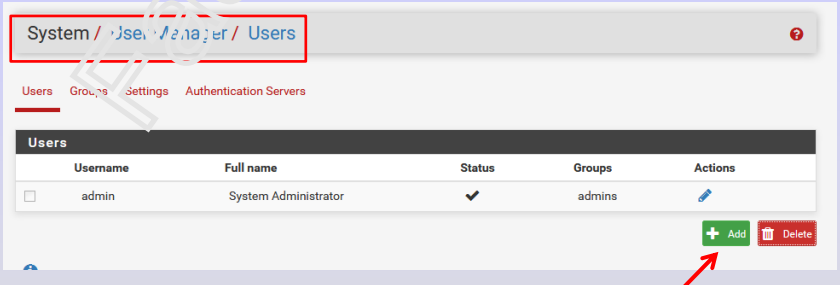
pfSense – Servizi - Captive portal



abilitare i pop-up sul browser

73

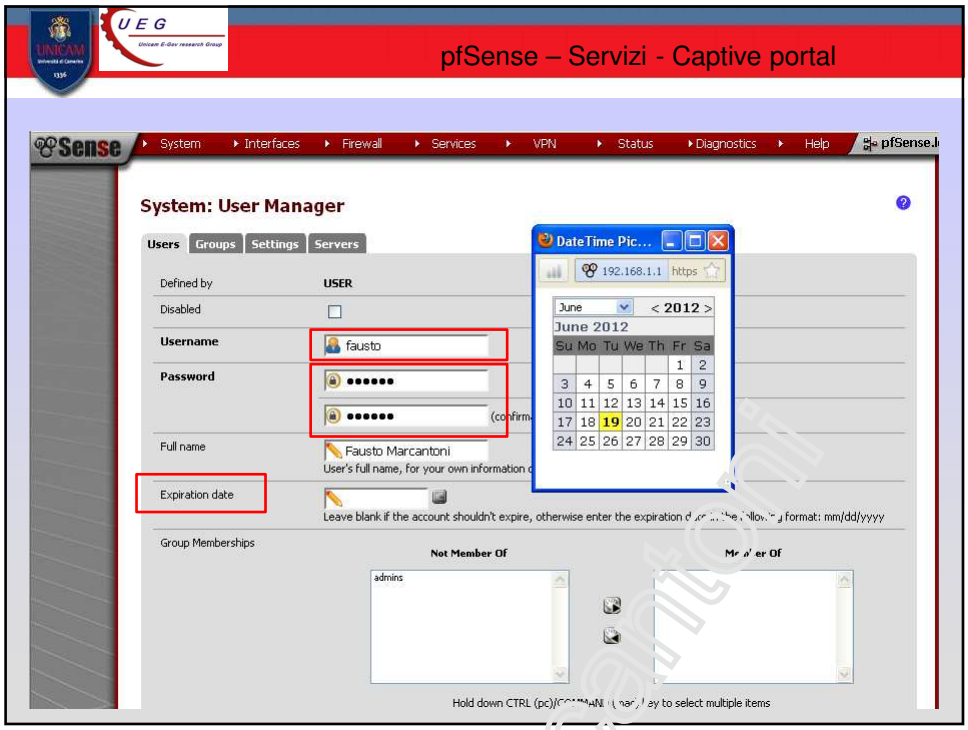
pfSense – Servizi - Captive portal



aggiungere un utente

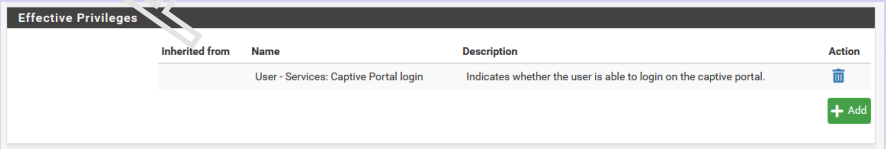
74

pfSense – Servizi - Captive portal



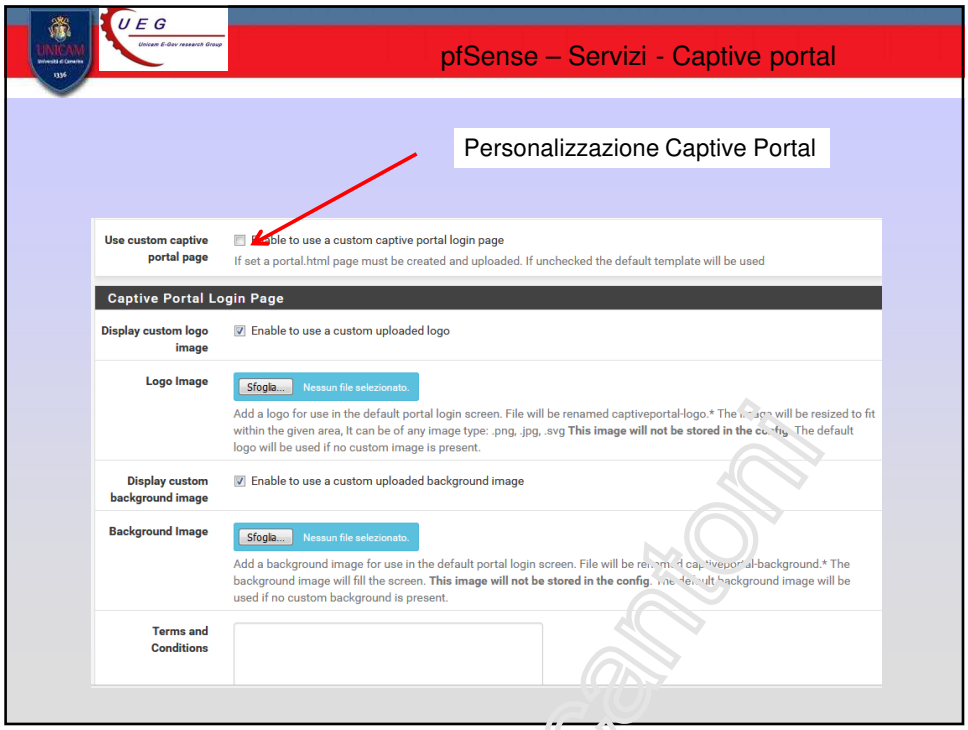
75

Abilitare l'utente ad utilizzare il Captive Portal

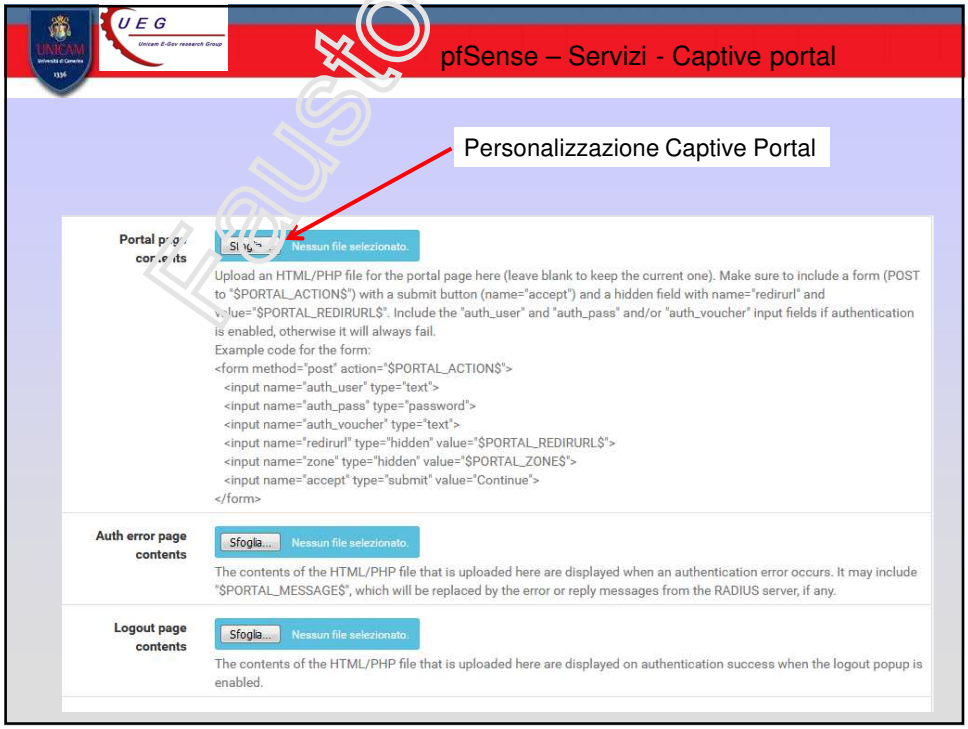


User - Services: Captive Portal login
Indicates whether the user is able to login on the captive portal.

76



77



78

pfSense– configurazione - Captive portal

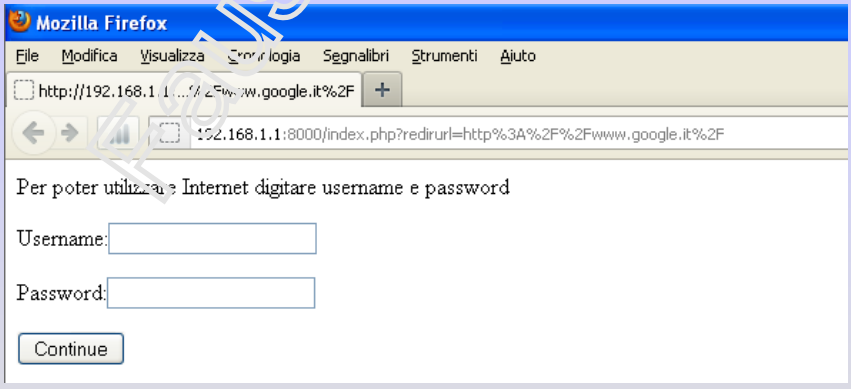
Esempio di pagina " CAPRTIVE PORTAL"

```
<html>
<body>
<form method="post" action="$PORTAL_ACTION$">
   <input name="auth_user" type="text">
   <input name="auth_pass" type="password">
   <input name="auth_voucher" type="text">
   <input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
   <input name="zone" type="hidden" value="$PORTAL_ZONE$">
   <input name="accept" type="submit" value="Continue">
</form>
</body>
</html>
```

E' possibile aggiungere anche le immagini

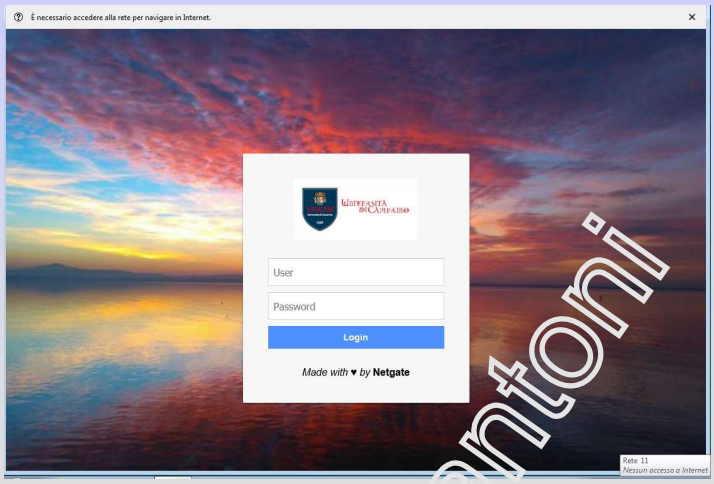
79

pfSense – configurazione - Captive portal



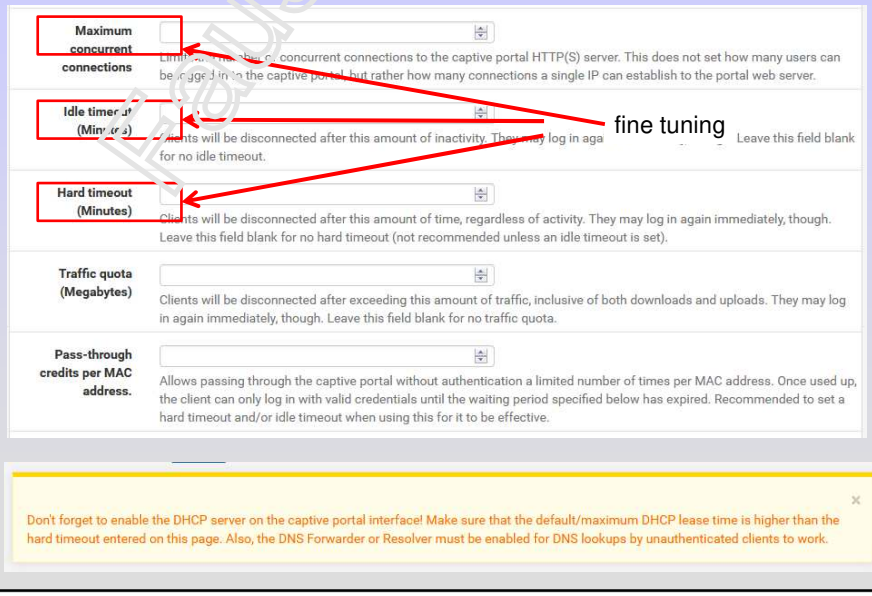
80

pfSense – configurazione - Captive portal



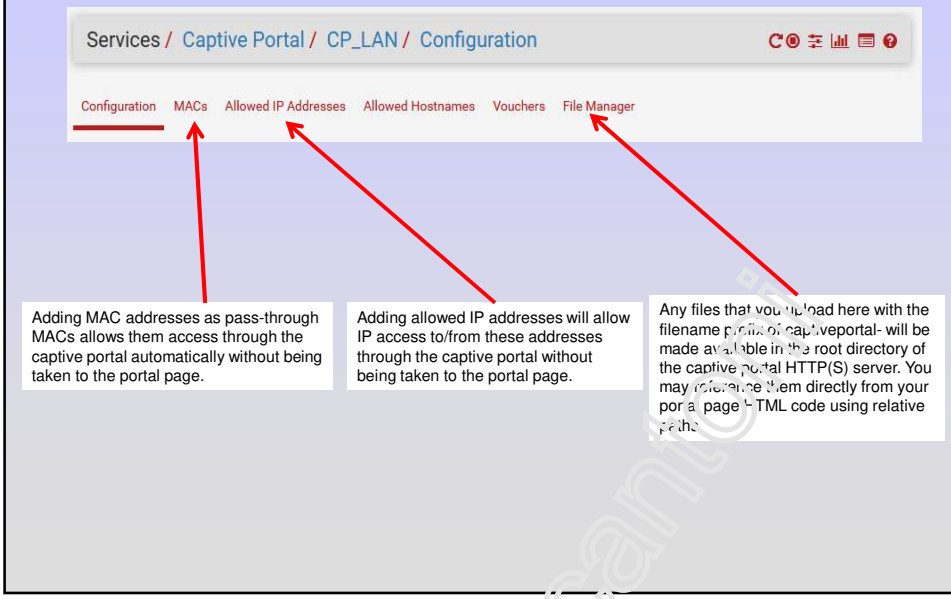
81

pfSense – configurazione - Captive portal



82

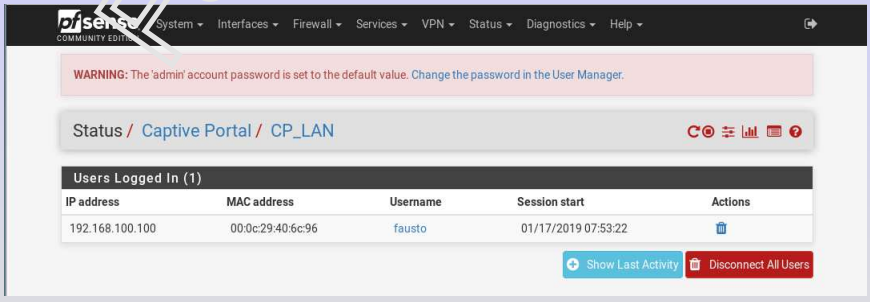
pfSense – configurazione - Captive portal



83

pfSense – configurazione - Captive portal

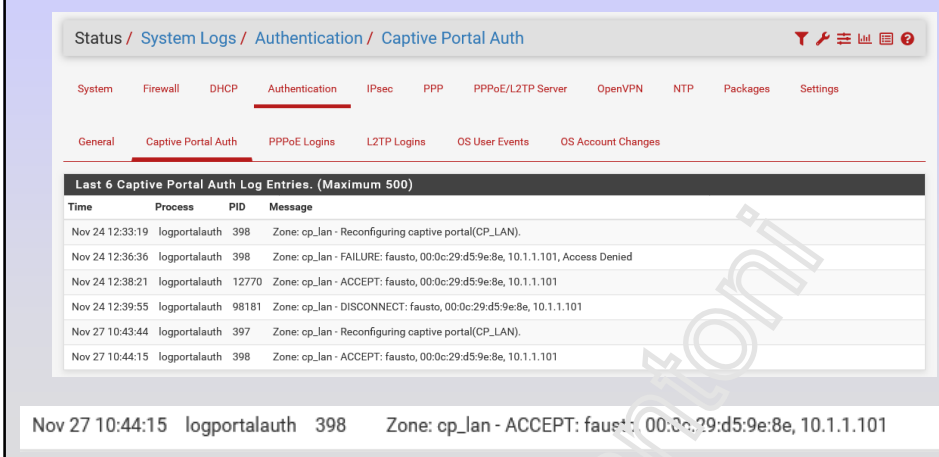
I log di captive portal



84

System LogsAuthenticationCaptive Portal Auth

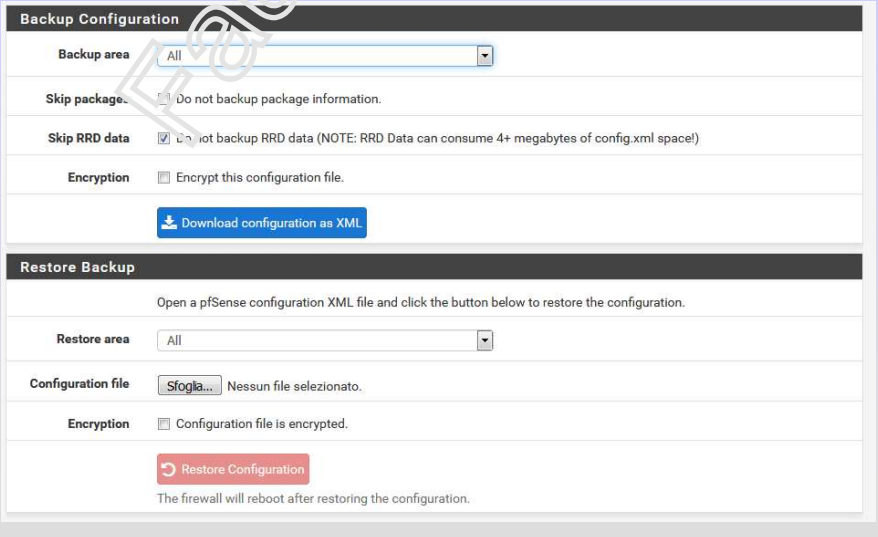
System Logs →Authentication →Captive Portal Auth



85

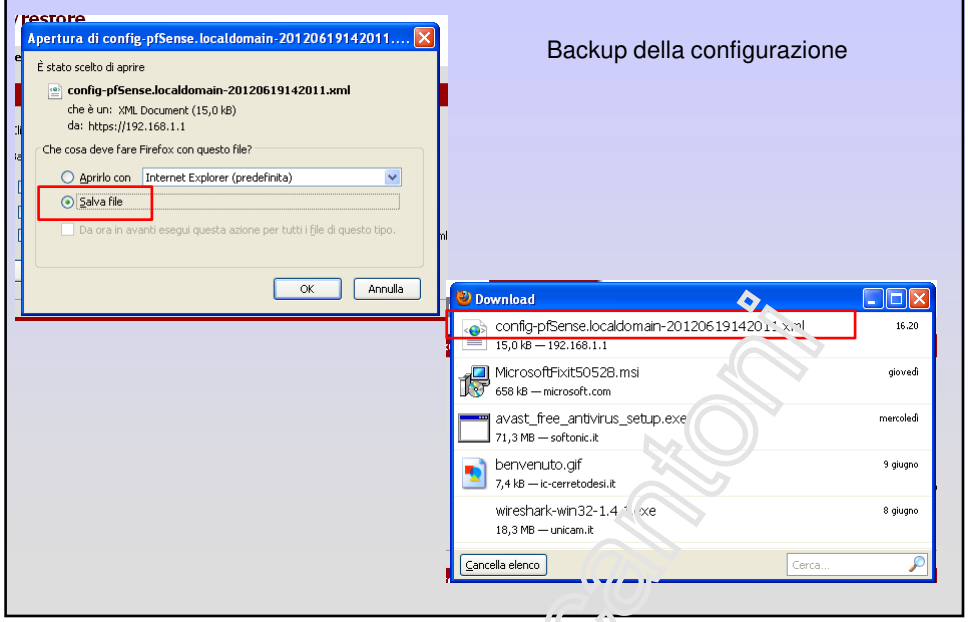
pfSense – backup configurazione -

Backup della configurazione



86

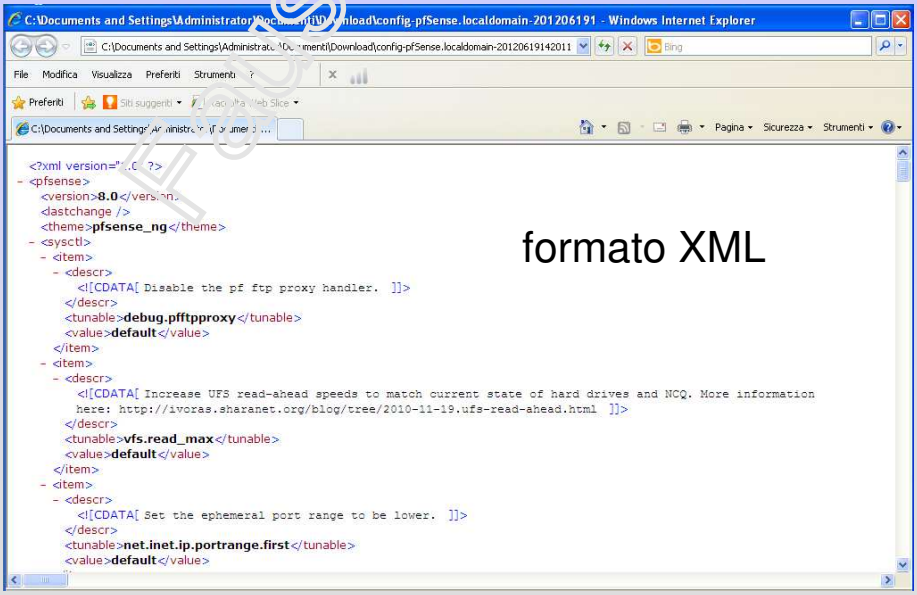
pfSense – backup configurazione -



Backup della configurazione

87

pfSense – backup configurazione -

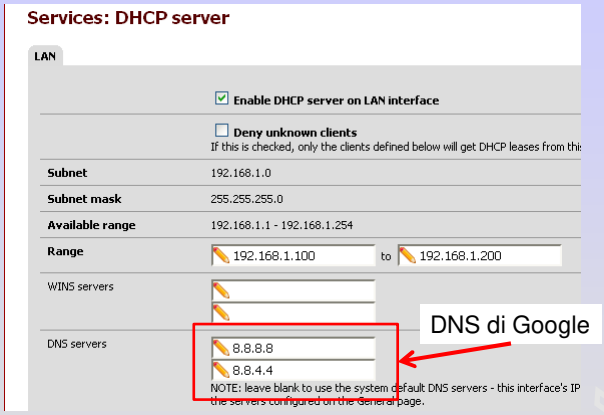


formato XML

88

pfSense – configurazione – DHCP Server

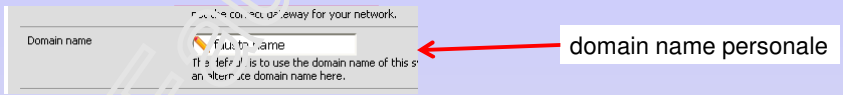
configurare alcuni parametri nel server dhcp

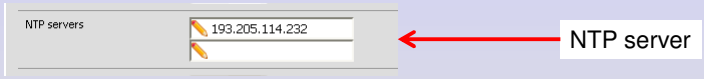


89

pfSense – configurazione – DHCP Server

configurare alcuni parametri nel server dhcp

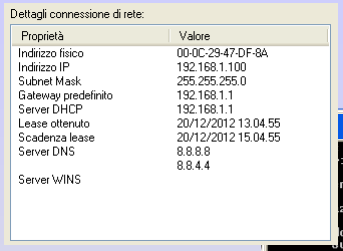


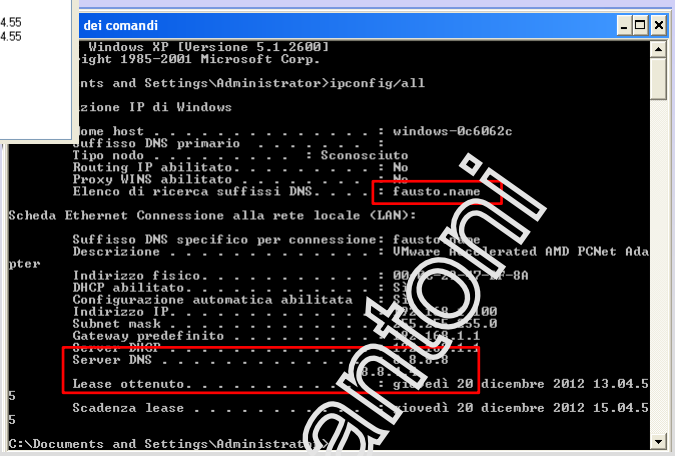


90

pfSense – configurazione – DHCP Server

configurare alcuni parametri nel server dhcp

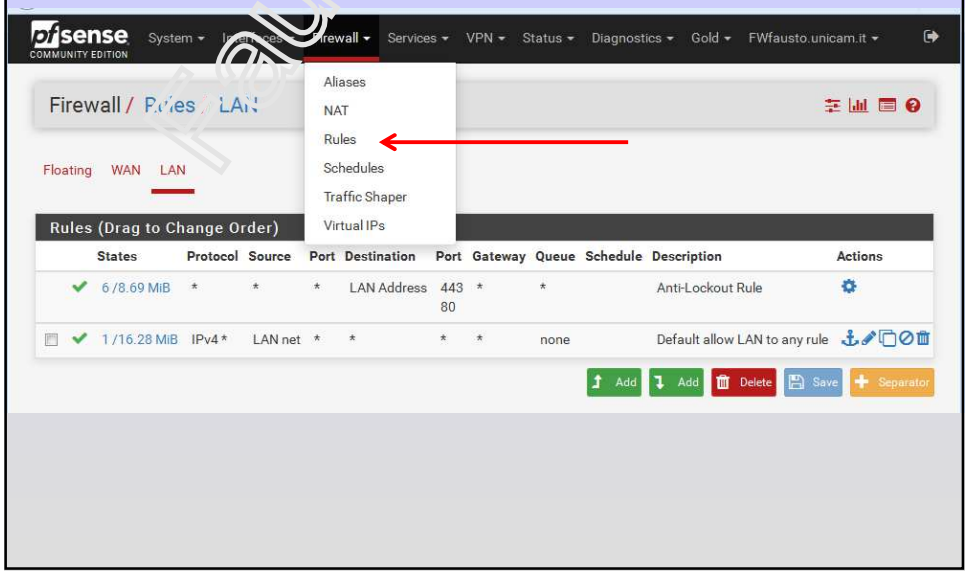




91

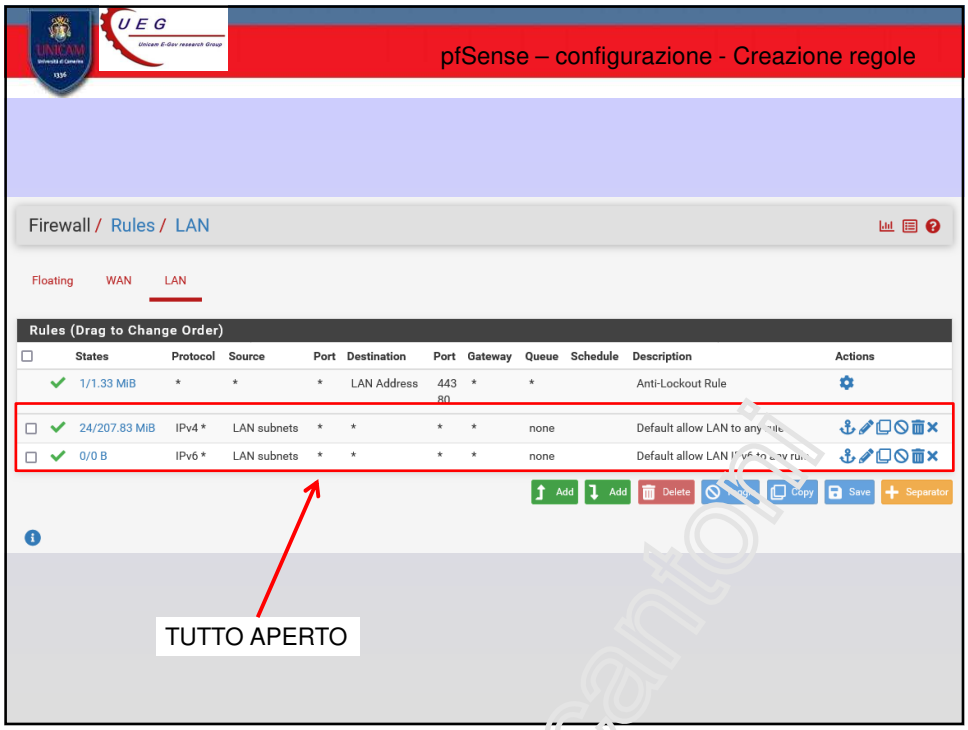
pfSense – configurazione - Creazione regole

Le “REGOLE”



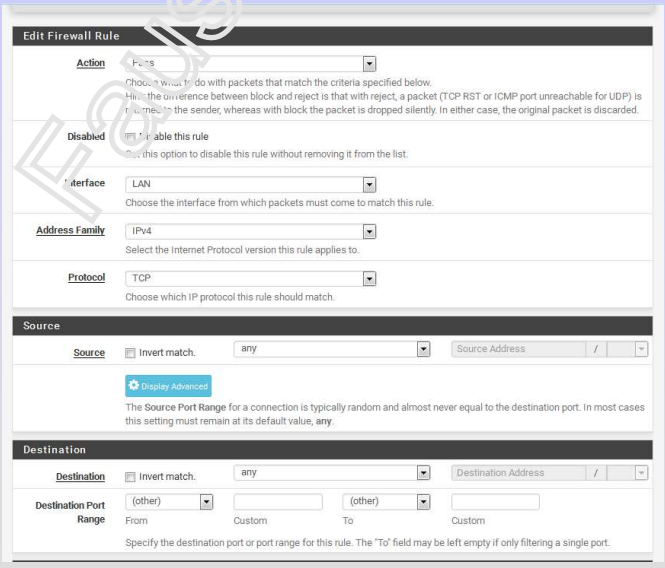
92

pfSense – configurazione - Creazione regole



93

pfSense – configurazione - Creazione regole



Configurare una regola …

94

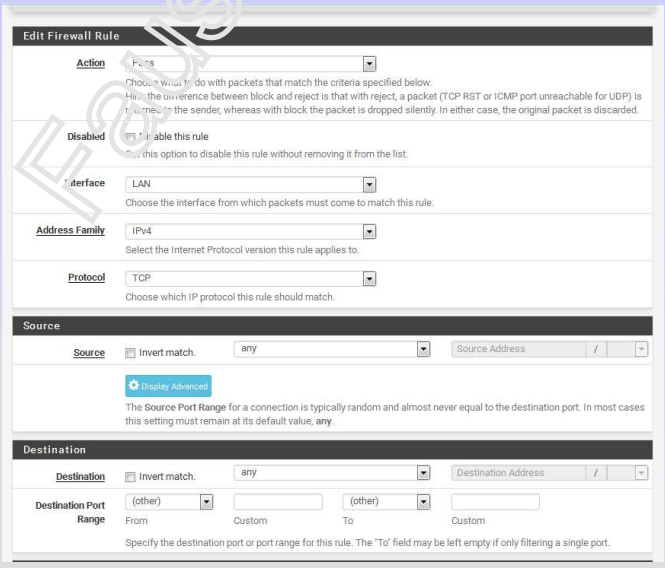
I firewalls mettono a disposizione tre opzioni per il controllo del traffico:

- **Pass o Accept**
  - ✓ Lascia che il traffico passi;
- **Block o Drop**
  - ✓ Scarta il pacchetto in modo silente senza generare messaggi di risposta;
- **Reject**
  - ✓ Rifiuta il pacchetto e risponde con un pacchetto ICMP type3, code 13 (type=Destination Unreachable, Code=Communication administratively prohibited).

https://www.pfsenseitaly.com/

95

pfSense – configurazione - Creazione regole

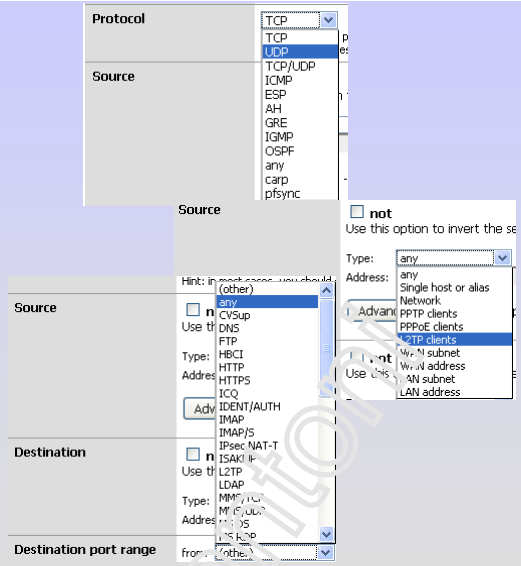


Configurare una regola …

96

pfSense – configurazione - Creazione regole

… Configurare una regola …



Attenzione

Ricorda:
Un firewall si progetta

97

pfSense – configurazione - Creazione regole

… Configurare una regola …

Mettere descrizioni facili da ricordare e intuitive

98

pfSense – configurazione - Creazione regole

Ricorda:
Un firewall si progetta

CHIUDIAMO TUTTO …

99

pfSense – configurazione - Creazione regole

Firewall / Rules / LAN

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	1 /2.18 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✓	15 /24.48 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save Separator

100

pfSense – configurazione - Creazione regole

CHIUDIAMO TUTTO …
POI APRIAMO QUELLO CHE SERVE

101

pfSense – configurazione - Creazione regole

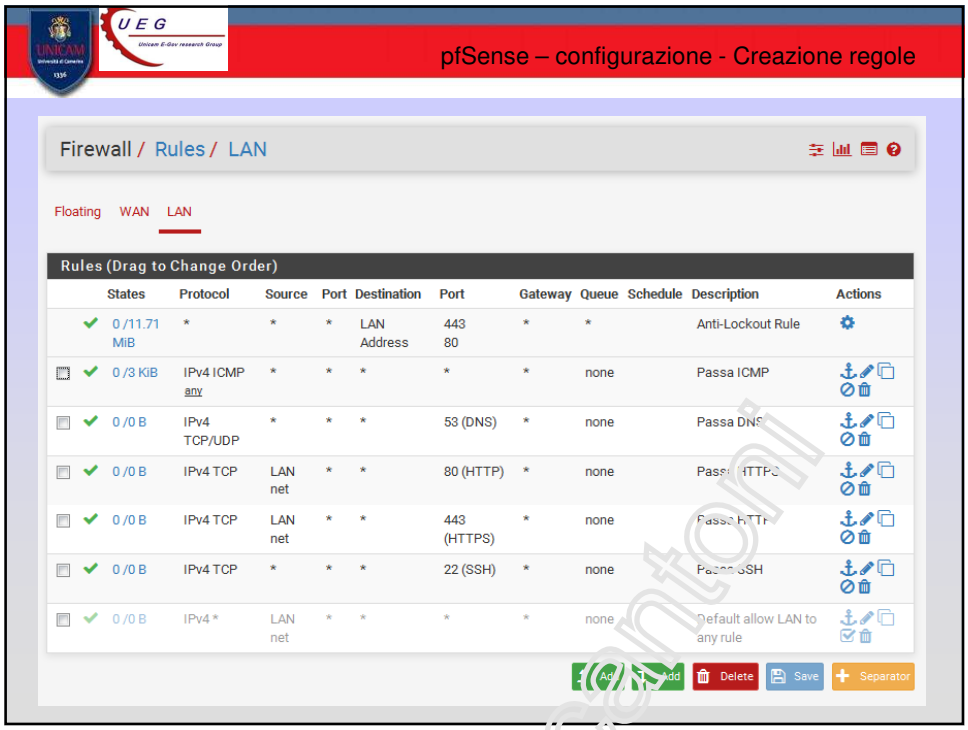
Quali porte aprire???

CHIUDIAMO TUTTO …
POI APRIAMO QUELLO CHE SERVE

Apriamo:
ICMP (ping - traceroute)
HTTP (www)
HTTPS (www sicuro)
SSH (telnet sicuro)
DNS
…

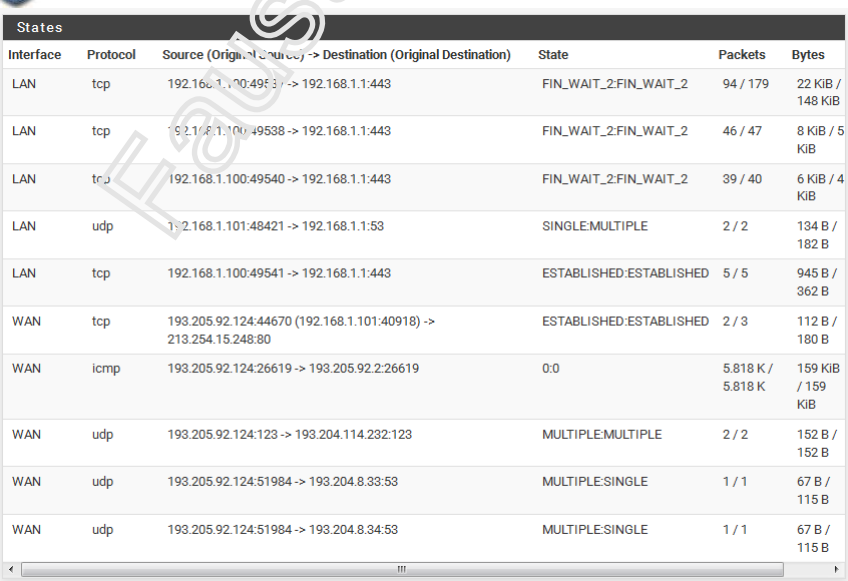
102

pfSense – configurazione - Creazione regole



103

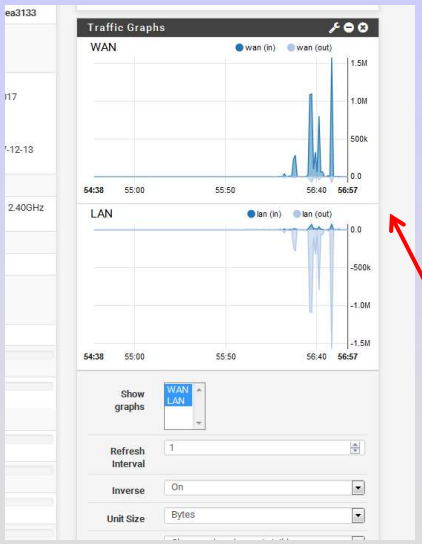
pfSense– configurazione – Firewall States



Controllare le sessioni e lo stato del firewall

104

pfSense – Status – Traffic Graph



traffico e banda utilizzata

105

ARP table

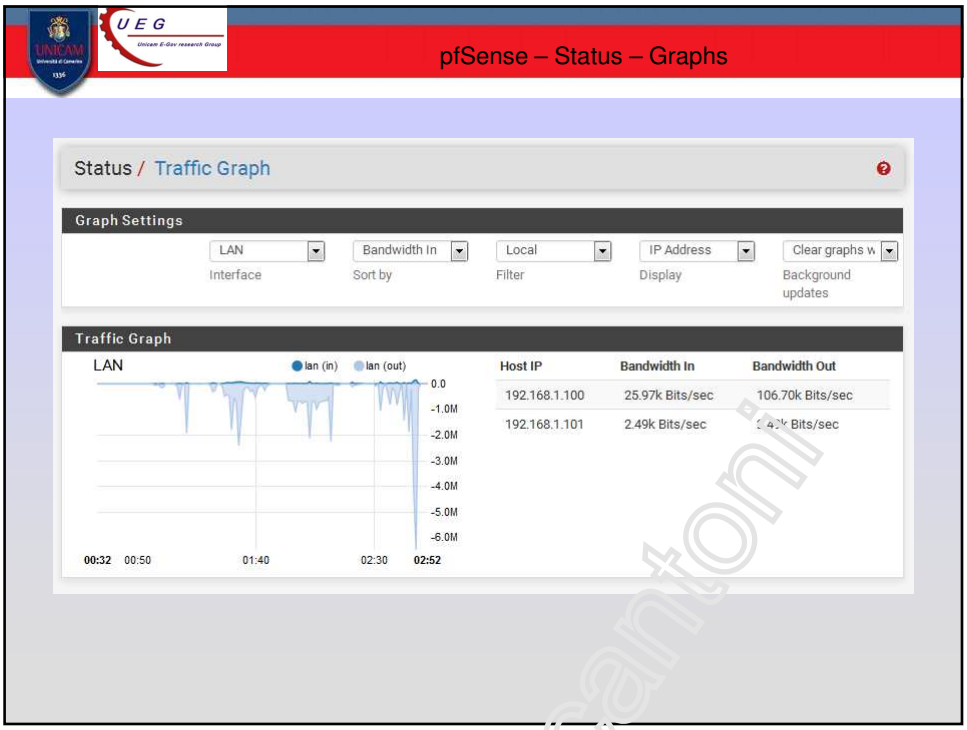
Diagnostics / ARP Table

ARP Table

Interface	IP address	MAC address	Hostname	Actions
LAN	192.168.1.1	00:0c:29:ed:68:f5	fwfausto.unicam.it	
LAN	192.168.1.101	00:0c:29:66:eb:7b	pentest	
WAN	193.205.92.124	00:0c:29:ed:68:eb	pfsense.amministrazione.unicam	
LAN	192.168.1.100	00:0c:29:40:6c:96	studente-PC	
WAN	193.205.92.2	08:96:ad:f6:85:00		

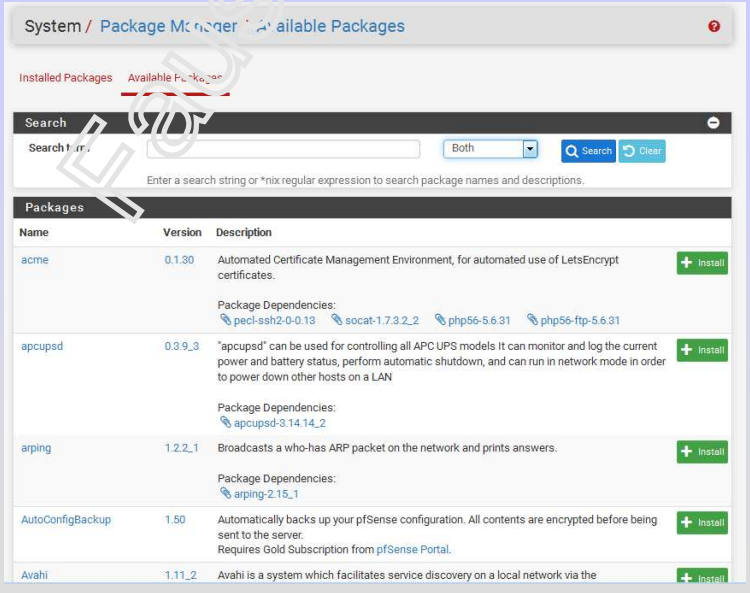
106

pfSense – Status – Graphs



107

pfSense – Package



108

pfSense – Package - squid proxy

SQUID

http://www.squid-cache.org/

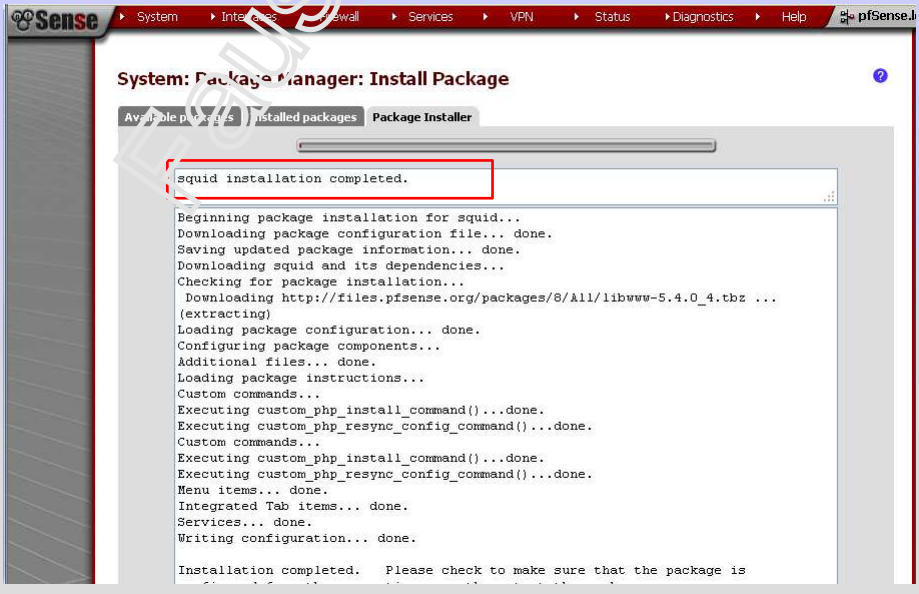
Packages

Name	Version	Description
Lightsquid	3.0.7_3	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package. Package Dependencies: lighttpd-1.4.72 lightsquid-1.8_5
squid	0.4.46	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP/HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP. Package Dependencies: squidclamav-7.2 squid_radius_auth-1.10 squid-6.3 c-icap-modules-0.5.5_1
squidGuard	1.16.19	High performance web proxy URL filter. Package Dependencies: squidguard-1.4_15 pfSense-pkg-squid-0.4.46

Install

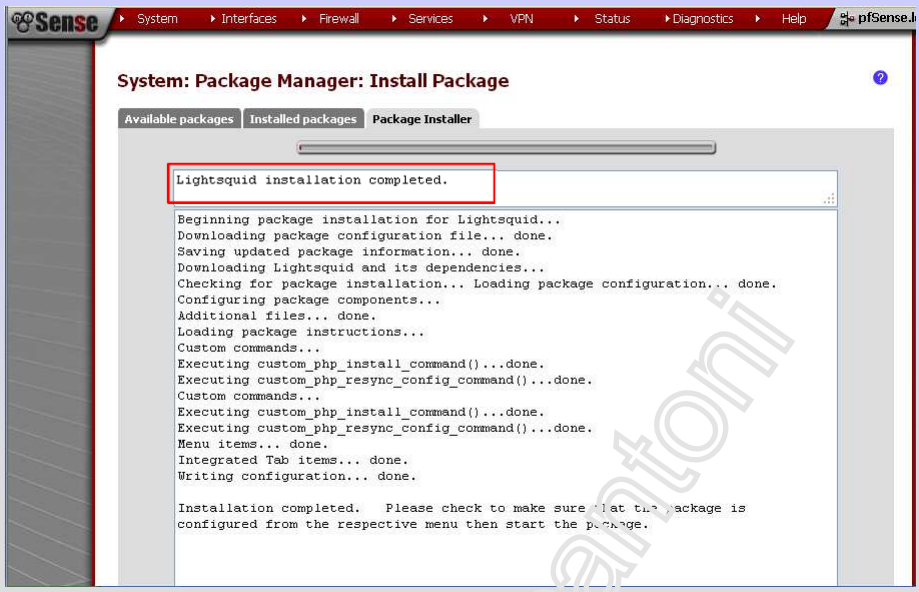
109

pfSense – Package - squid proxy



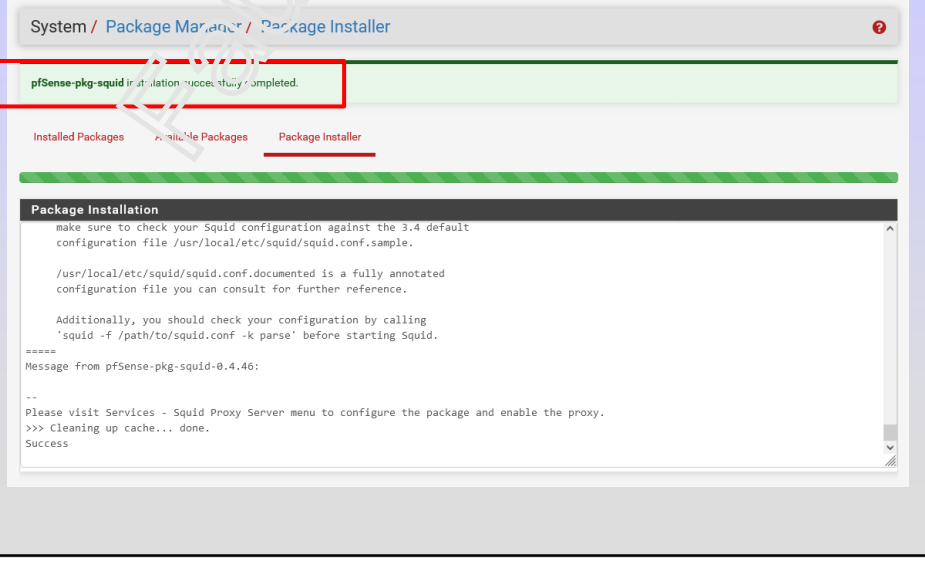
110

pfSense – Package - squid proxy



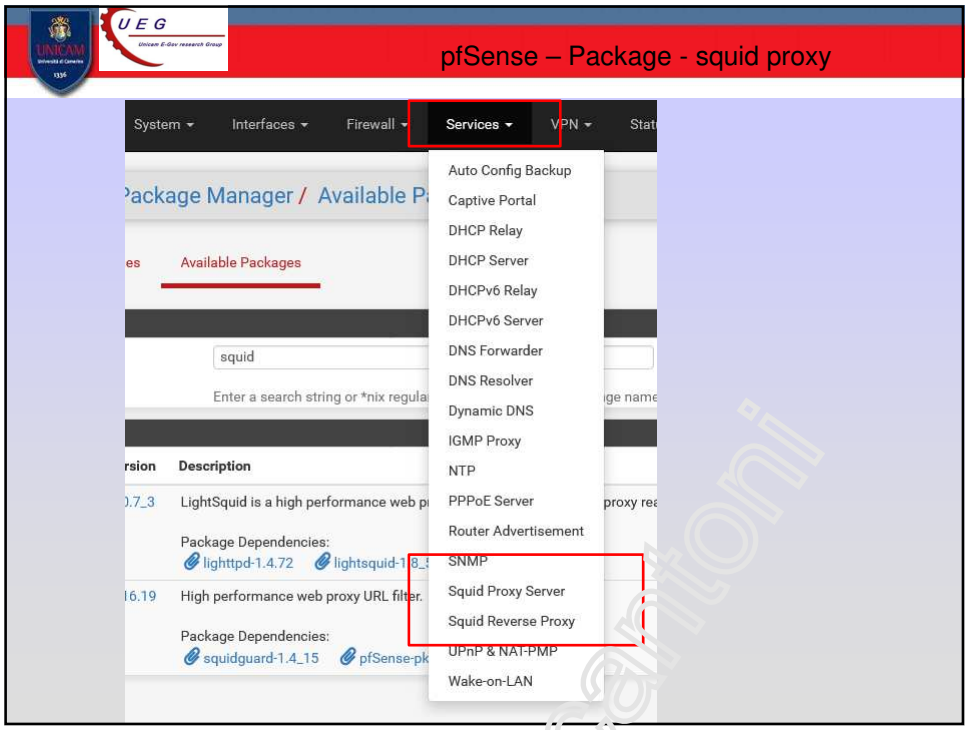
111

pfSense – Package - squid proxy



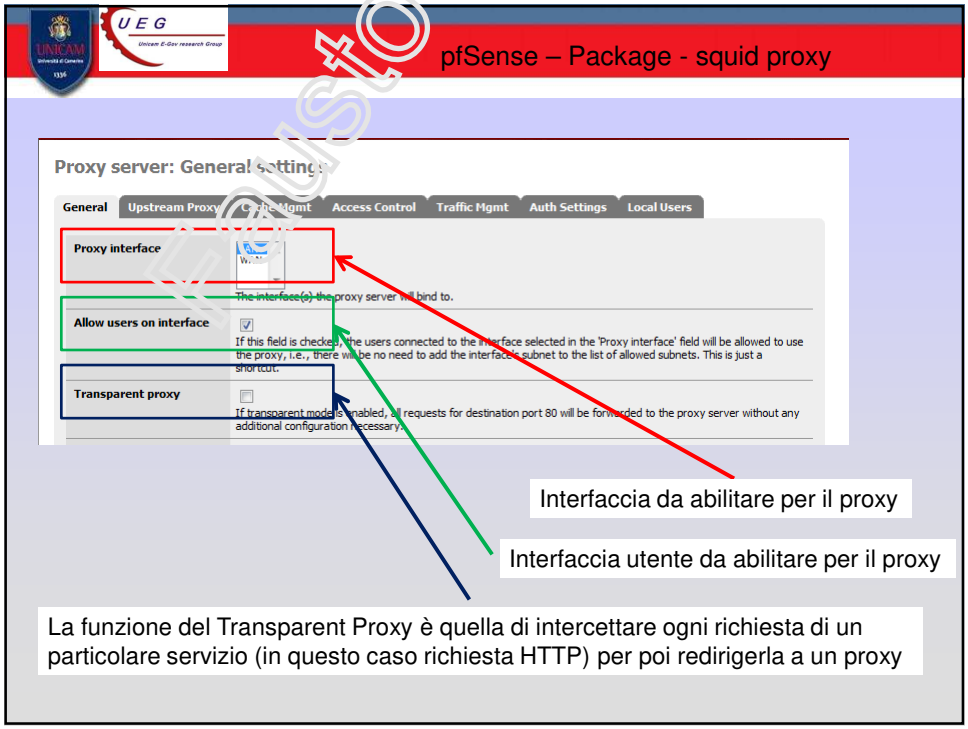
112

pfSense – Package - squid proxy

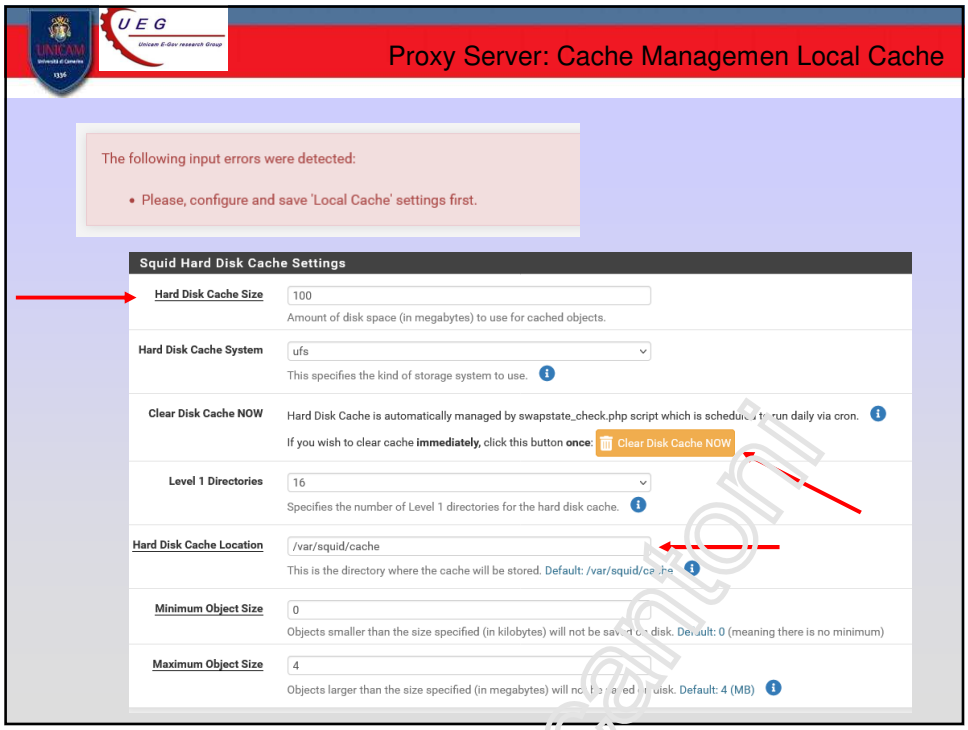


113

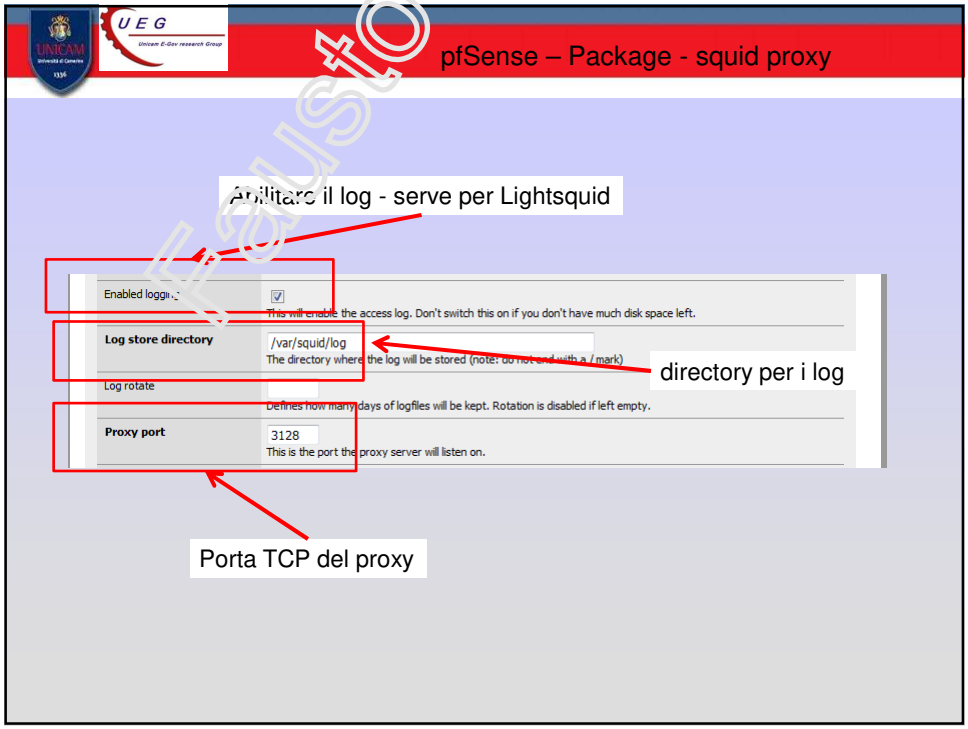
pfSense – Package - squid proxy



114



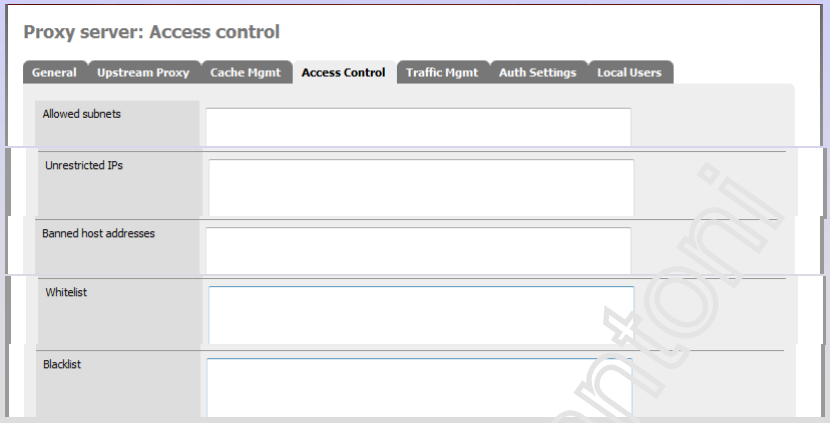
115



116

pfSense – Package - squid proxy

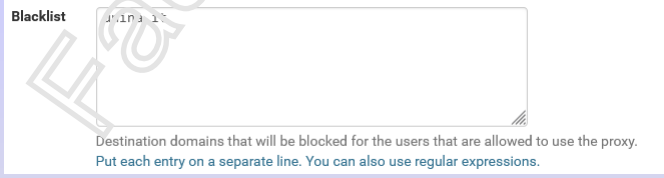
ACL: access control list



117

pfSense – Package - squid proxy

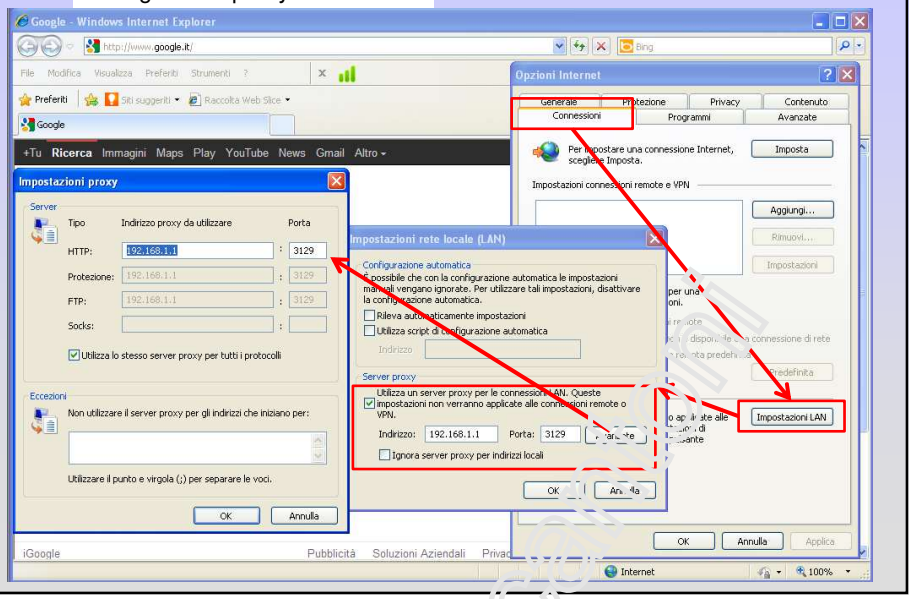
Bloccare l'accesso a unina.it



118

pfSense – Package - squid proxy

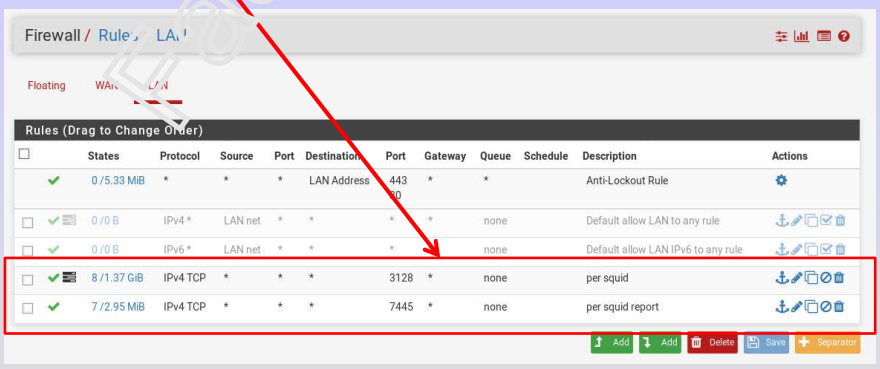
Configurare il proxy sul browser



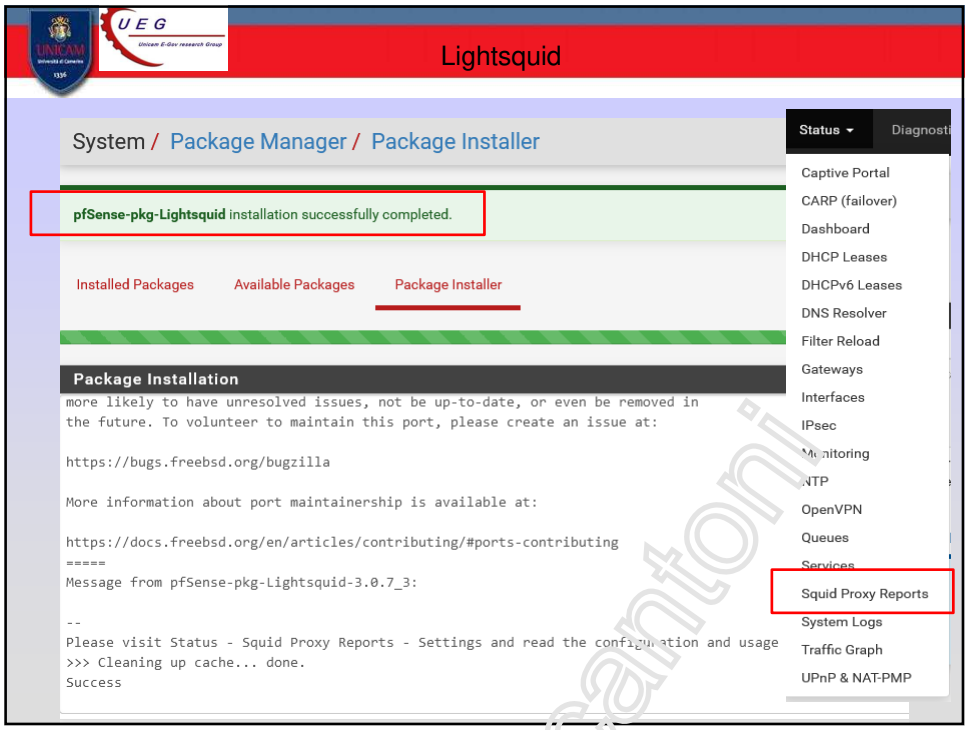
119

pfSense – Package - squid proxy

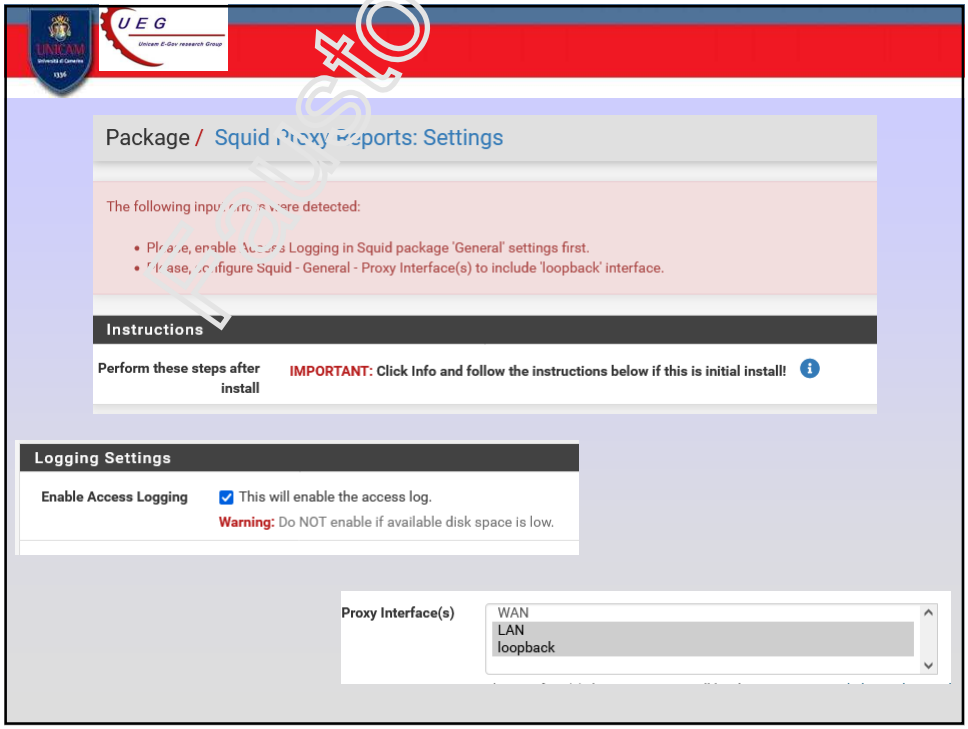
aggiungere regole su firewall



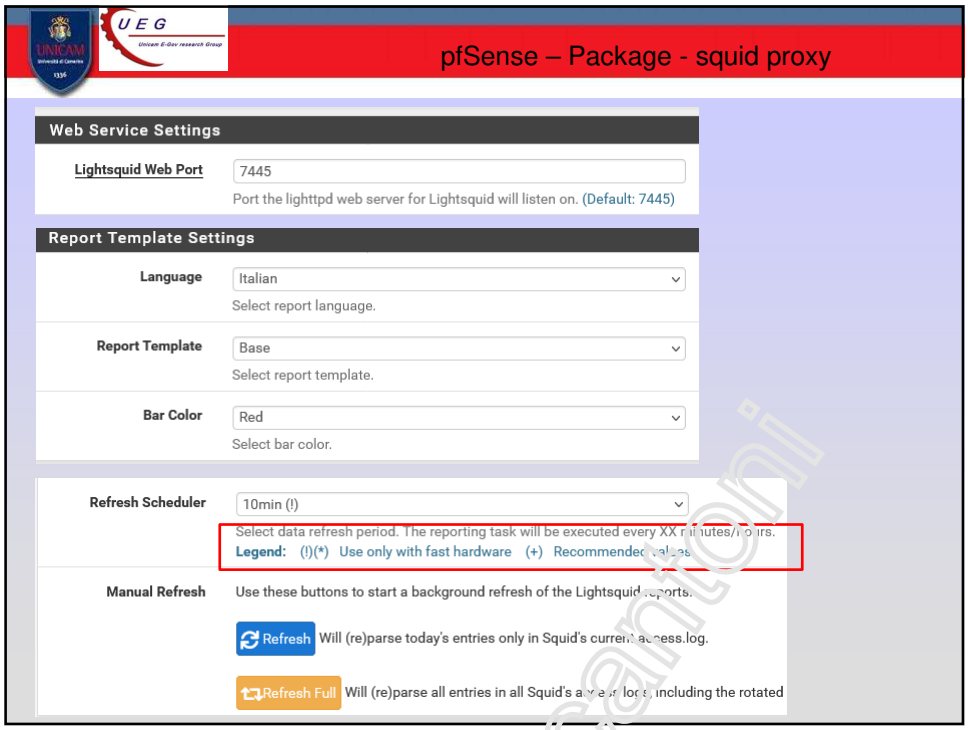
120


Lightsquid
System / Package Manager / Package Installer
Status
Diagnosti
pfSense-pkg-Lightsquid installation successfully completed.
Installed Packages
Available Packages
Package Installer
Package Installation
more likely to have unresolved issues, not be up-to-date, or even be removed in
the future. To volunteer to maintain this port, please create an issue at:
https://bugs.freebsd.org/bugzilla
More information about port maintainership is available at:
https://docs.freebsd.org/en/articles/contributing/#ports-contributing
=====
Message from pfSense-pkg-Lightsquid-3.0.7_3:
--
Please visit Status - Squid Proxy Reports - Settings and read the configuration and usage
>>> Cleaning up cache... done.
Success
Captive Portal
CARP (failover)
Dashboard
DHCP Leases
DHCPv6 Leases
DNS Resolver
Filter Reload
Gateways
Interfaces
IPsec
OpenVPN
Queues
Squid Proxy Reports
System Logs
Traffic Graph
UPnP & NAT-PMP

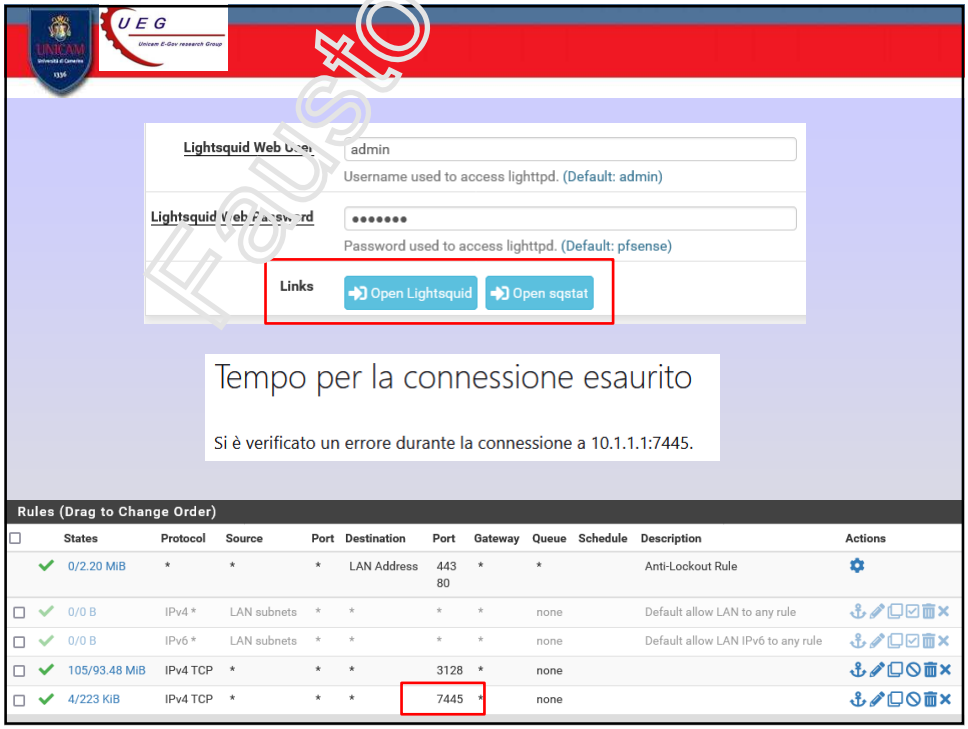
121


Package / Squid Proxy Reports: Settings
The following input errors were detected:
Please enable access Logging in Squid package 'General' settings first.
Please configure Squid - General - Proxy Interface(s) to include 'loopback' interface.
Instructions
Perform these steps after install
IMPORTANT: Click Info and follow the instructions below if this is initial install!
Logging Settings
Enable Access Logging
This will enable the access log.
Warning: Do NOT enable if available disk space is low.
Proxy Interface(s)
WAN
LAN
loopback

122



123



124

pfSense – Package - squid proxy

ERRORE

LigthSquid diagnostic.
Error : report folder '/var/lightsquid/report' not contain any valid data! Please run lightparser.pl (and check 'report' folder content)
Please check config file !

Variable	value
$tplpatph	/usr/local/www/lightsquid/tpl
$templatename	base
$langpatph	/usr/local/share/lightsquid/lang
$langname	it
$reportpath	/var/lightsquid/report
Access to '/var/lightsquid/report' folder	yes
$graphreport	1

folder content:

no problem!!!

125

pfSense – Package - squid proxy

Rapporto accesso utenti Squid
Periodo: Nov 2023

Calendar											
Nov											
01	02	03	04	05	06	07	08	09	10	11	12

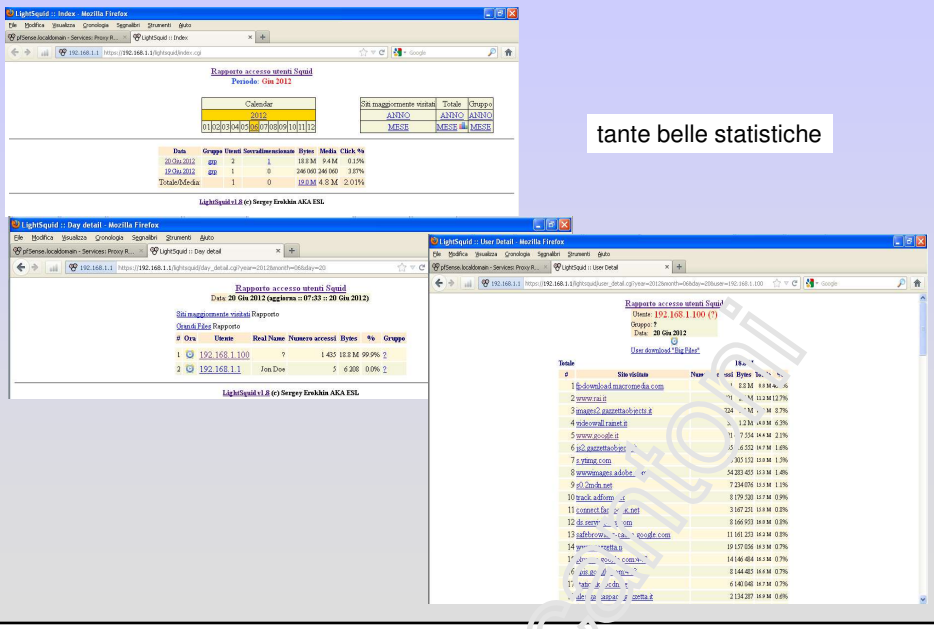
Siti maggiormente visitati	Totale	Gruppo
ANNO	ANNO	ANNO
MESE	MESE	MESE

Data	Gruppo	Utenti	Sovradimensionato	Bytes	Media	Click %
27 Nov 2023	grp	1	1	23.1 M	23.1 M	0.02%
Totale/Media:		1	1	23.1 M	23.1 M	0.02%

LightSquid v1.8 (c) Sergey Erokhin AKA ESL

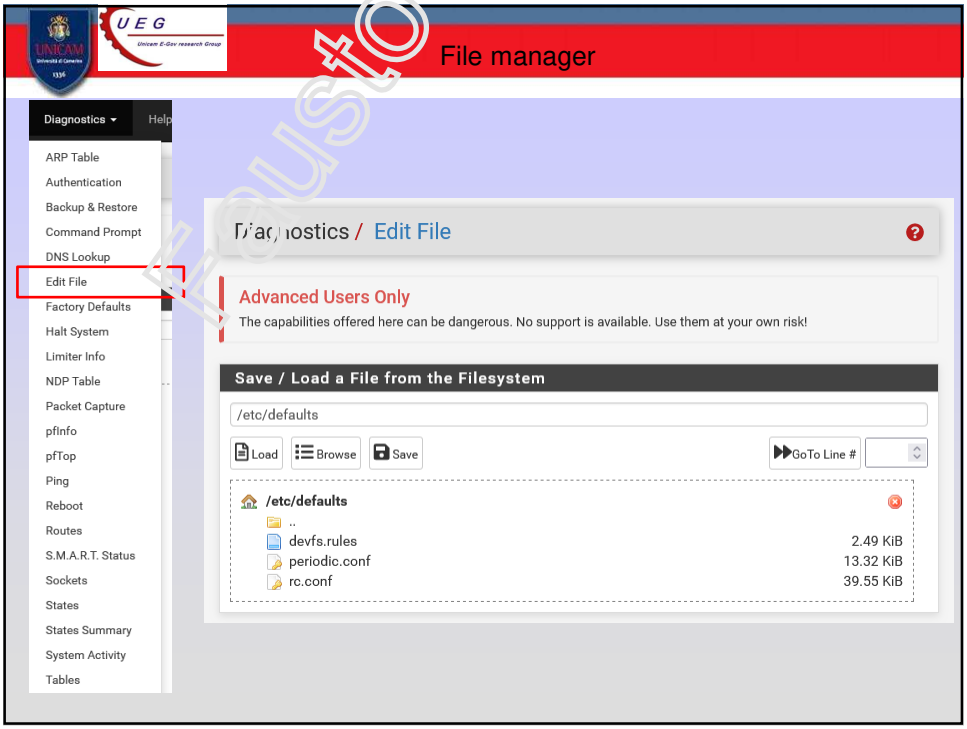
126

pfSense – Package - squid proxy

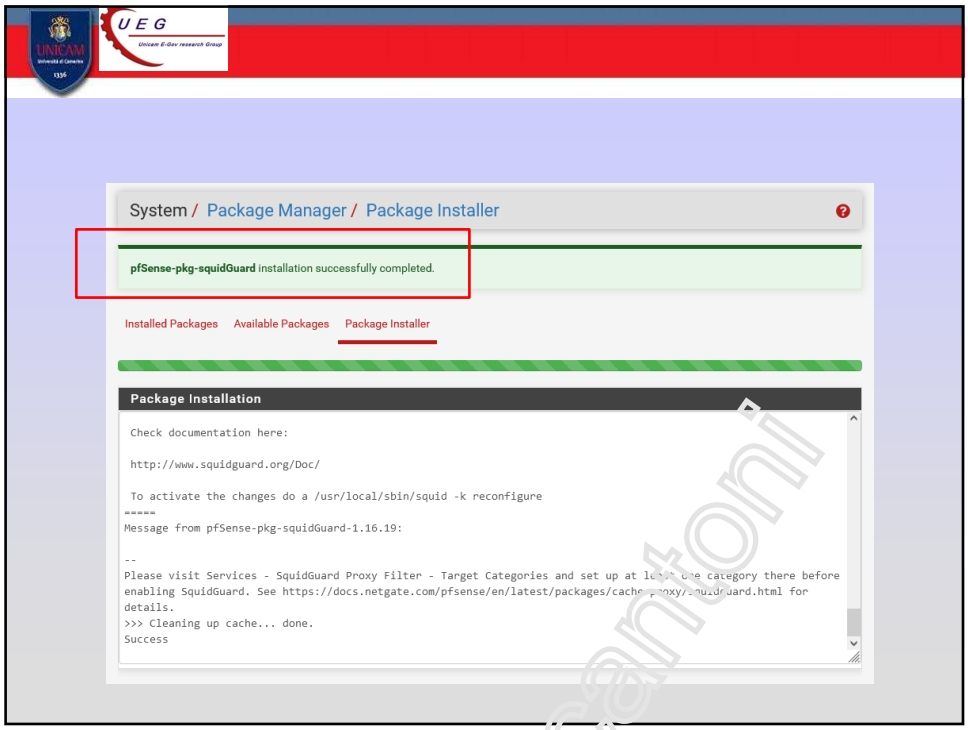


127

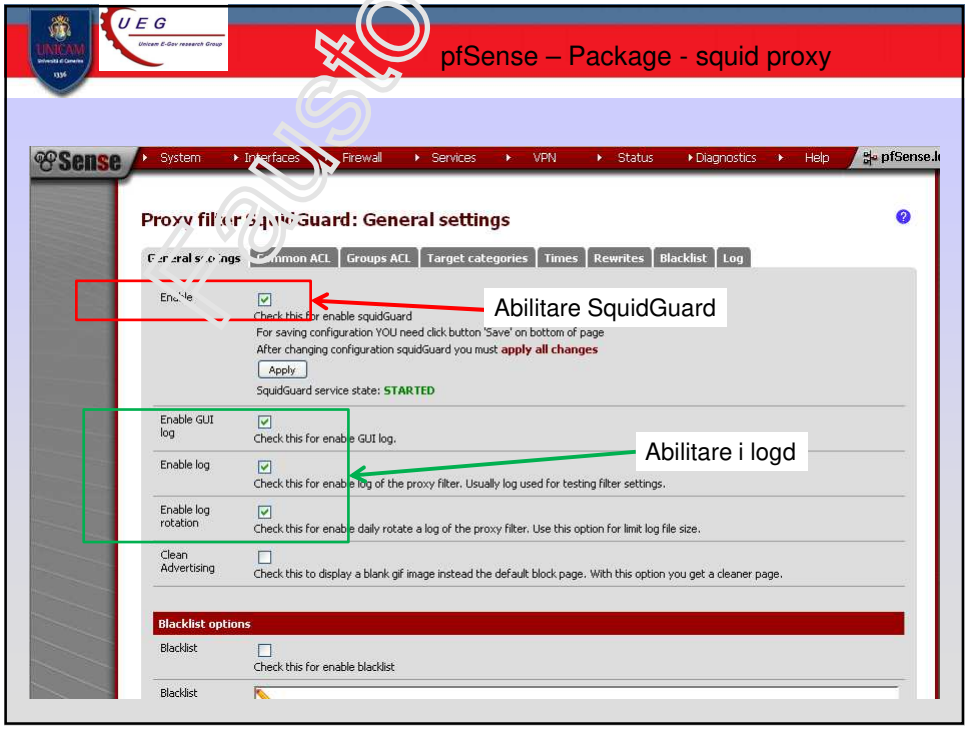
File manager



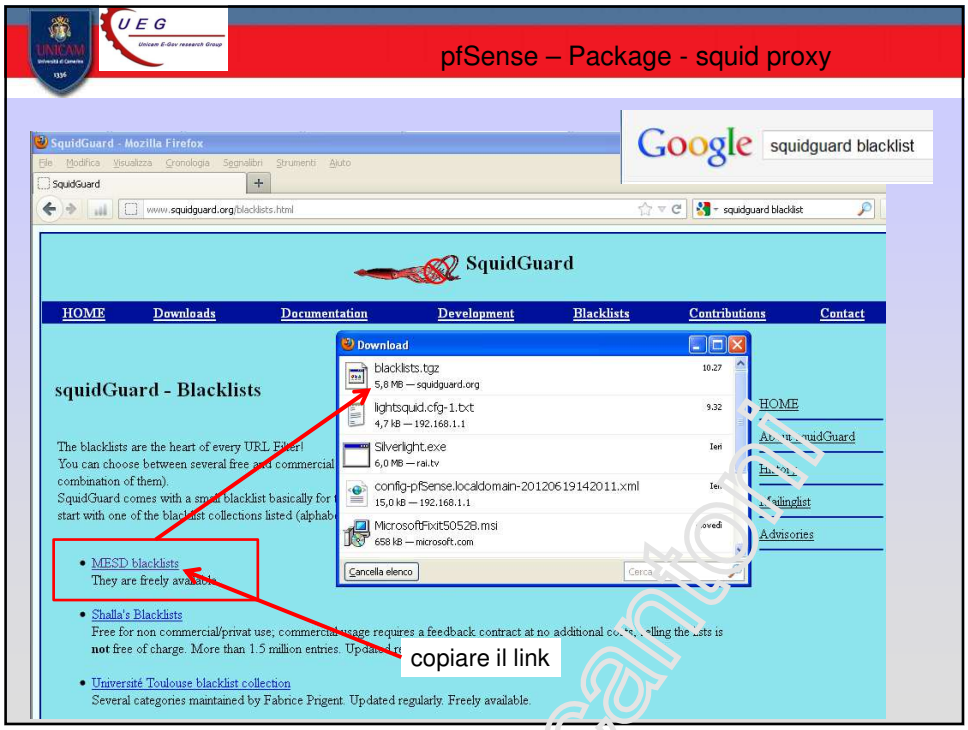
128



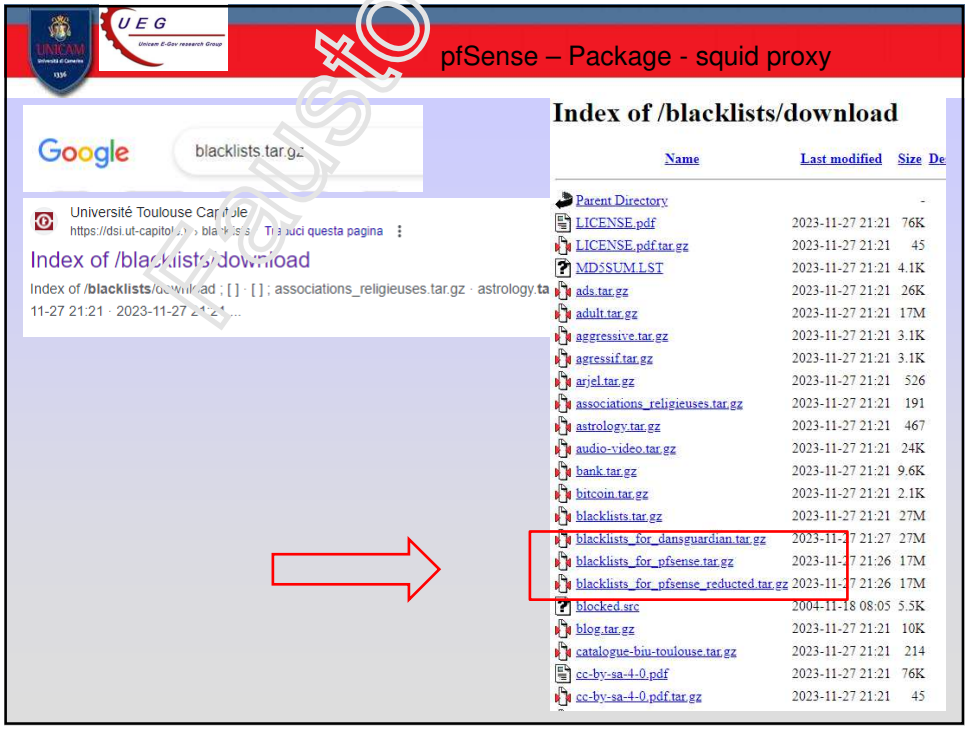
129



130

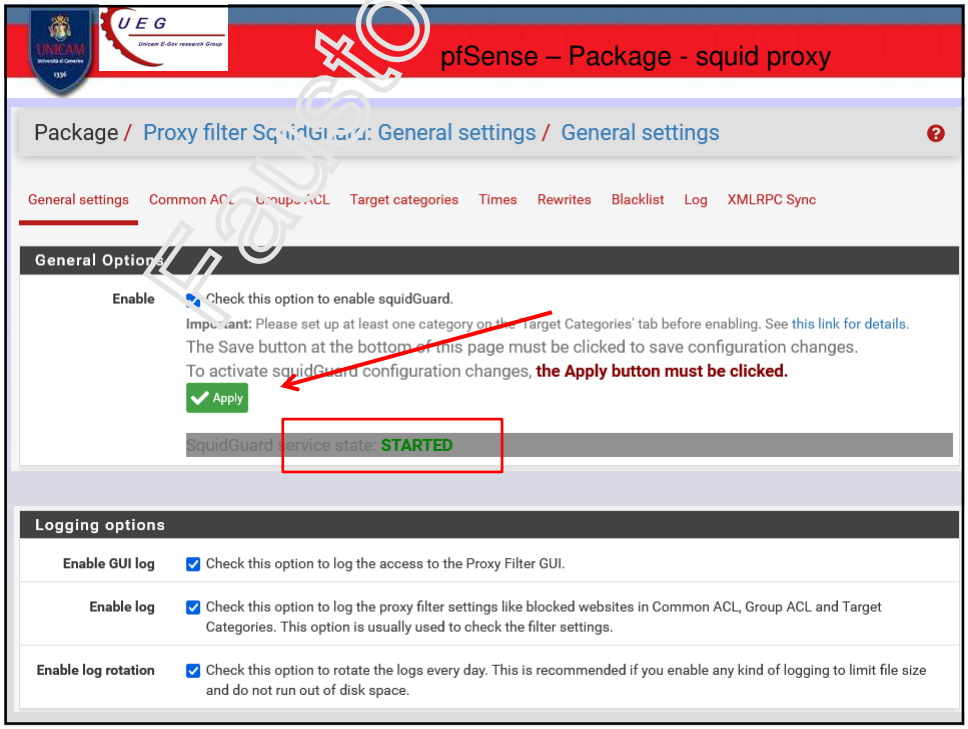


131

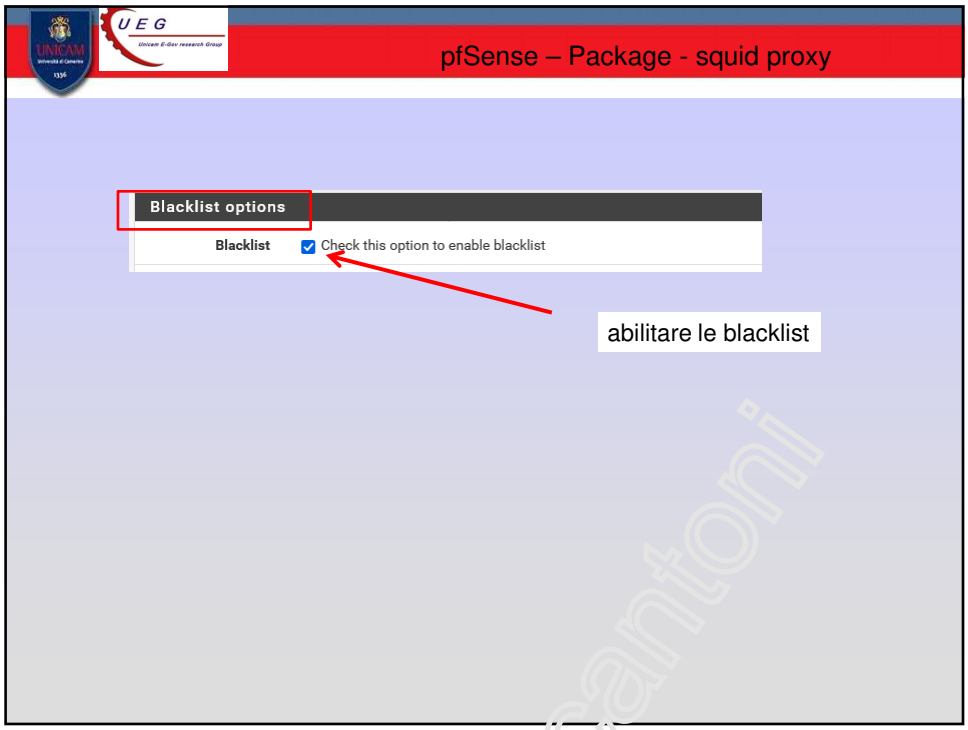


132

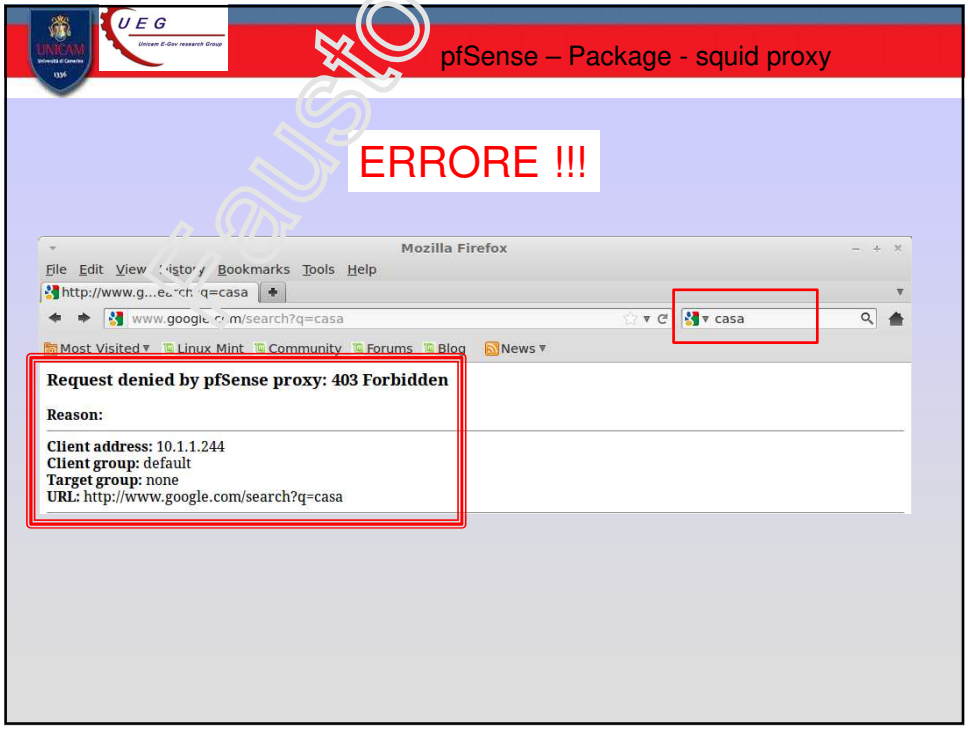
133



134



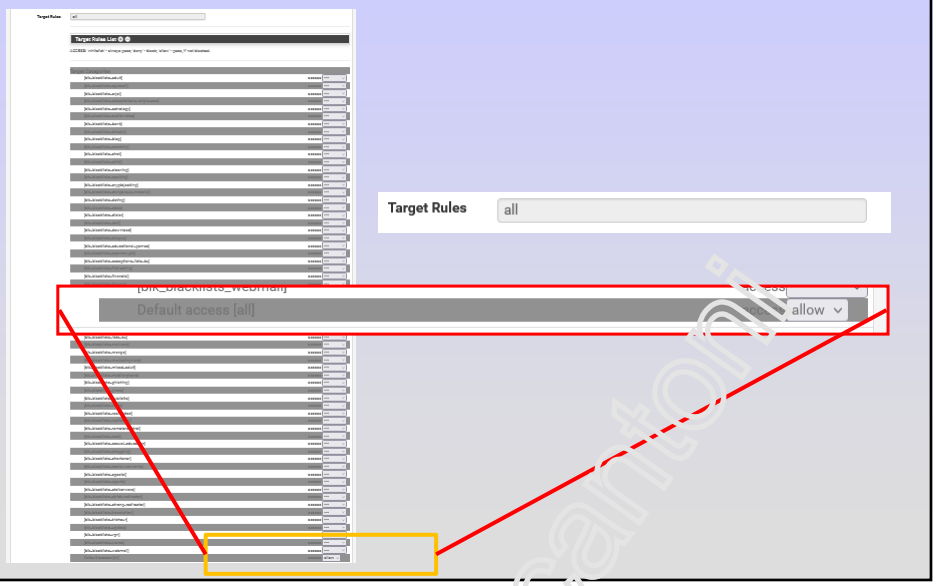
135



136

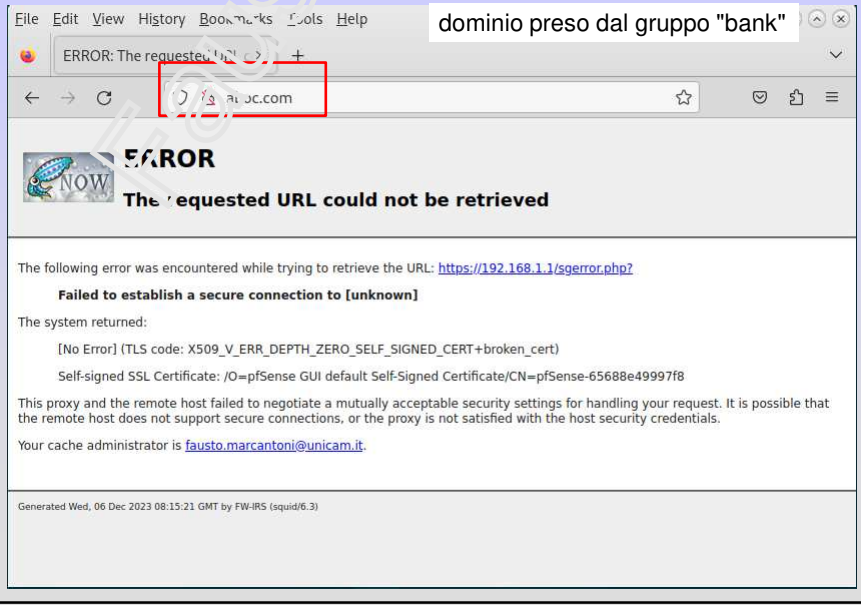
pfSense – Package - squid proxy

Configurare le regole



137

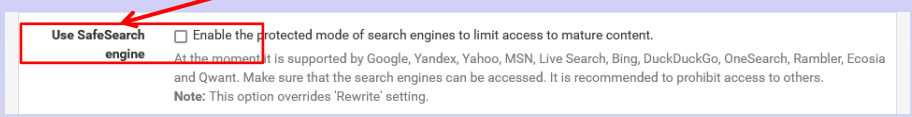
pfSense – Package - squid proxy



138

pfSense – Package - squid proxy

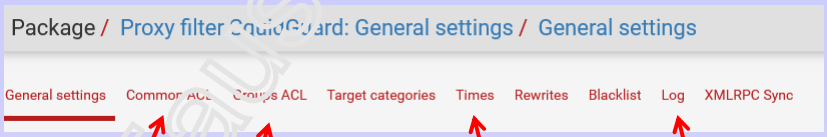
Use SafeSearch engine



Nessun motore di ricerca può sostituire la supervisione dei genitori quando si tratta di bambini e internet.

139

pfSense – Package - squid proxy



Le Regole

Le Regole fatte per gruppi di
•Utenti
•Network
•IP address

Temporizzazione delle regole

Debug: LOG !!!!

140

pfSense – Package - squid proxy

Attenzione

Request denied by pfSense proxy: 403 Forbidden

Reason:

Client address: 10.1.1.244
Client group: default
Target group: in-addr
URL: http://10.1.1.1/

Non posso entrare nella mia rete con indirizzo IP

disable

Do not allow IP-Addresses in URL ☐ To make sure that people do not bypass the URL filter by simply using IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.

141

Network Intrusion Detection & Prevention System

System / Package Manager / Available Packages

Installed Packages | Available Packages

Search

Search term: ids | Both | Search | Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description	
snort	4.1.6_14	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package Dependencies: snort-2.9.20_7	Install
suricata	7.0.2_1	High Performance Network IDS, IPS and Security Monitoring engine by OISF. Package Dependencies: suricata-7.0.2_4	Install

142

Snort/Suricata

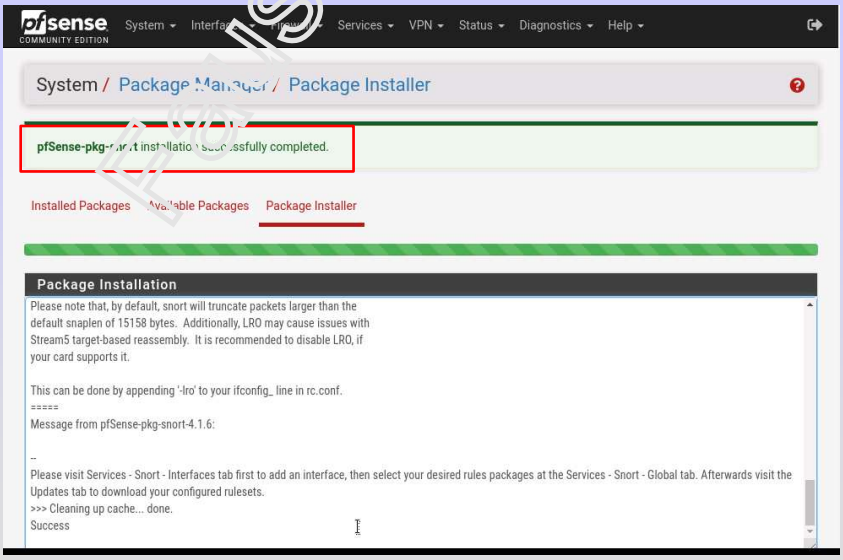
- Snort and Suricata are pfSense software packages for network intrusion detection. Depending on their configuration, they can require a significant amount of RAM. 1 GB should be considered a minimum but some configurations may need 2 GB or more, not counting RAM used by the operating system, firewall states, and other packages.

https://www.snort.org/

https://suricata.io/

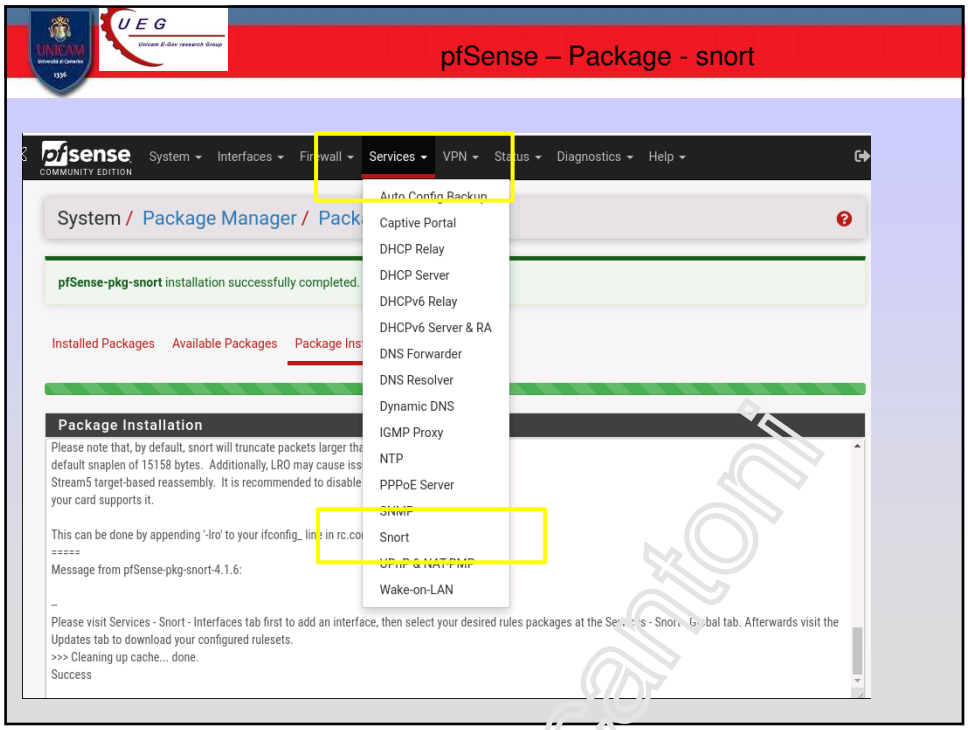
143

pfSense – Package - snort



144

pfSense – Package - snort

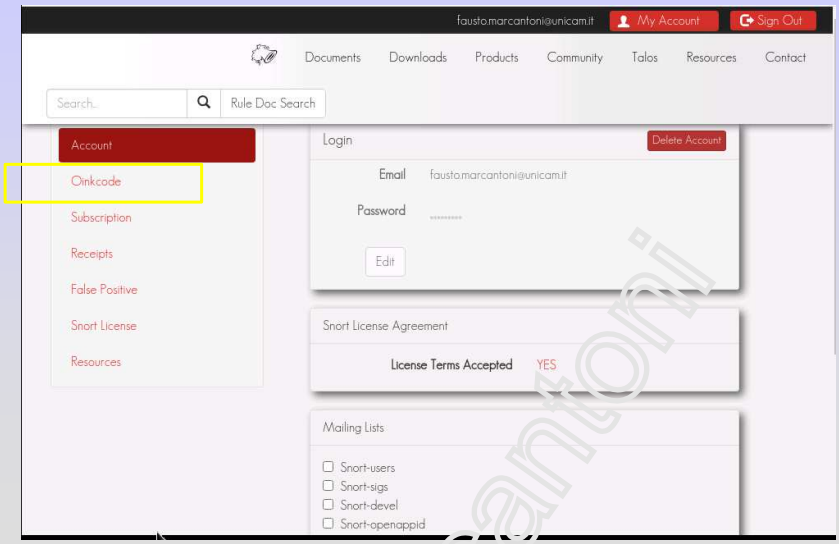


145

pfSense – Package - snort

146

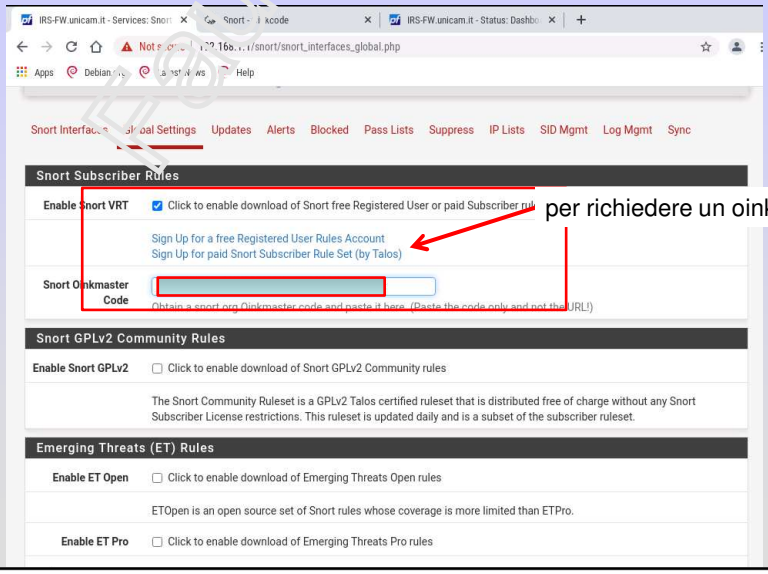
pfSense – Package - snort



147

pfSense – Package - snort

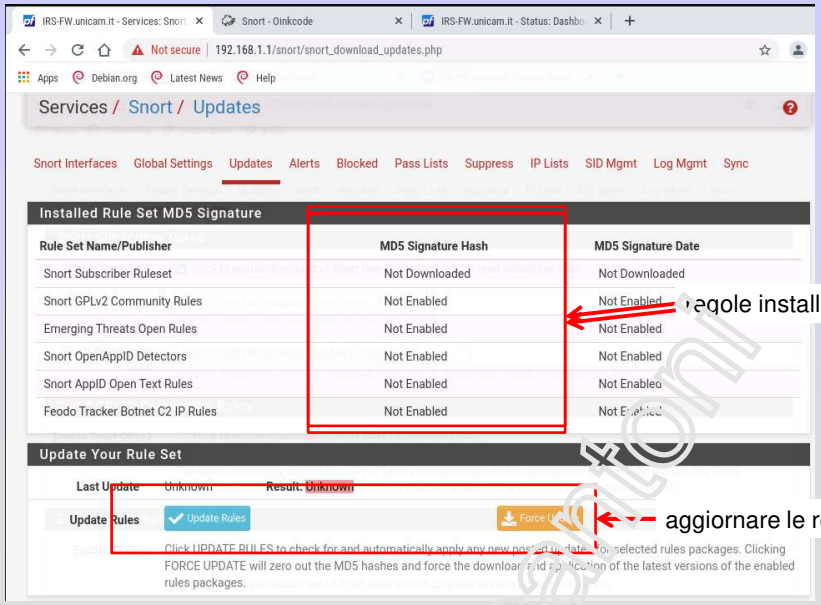
prima di tutto …



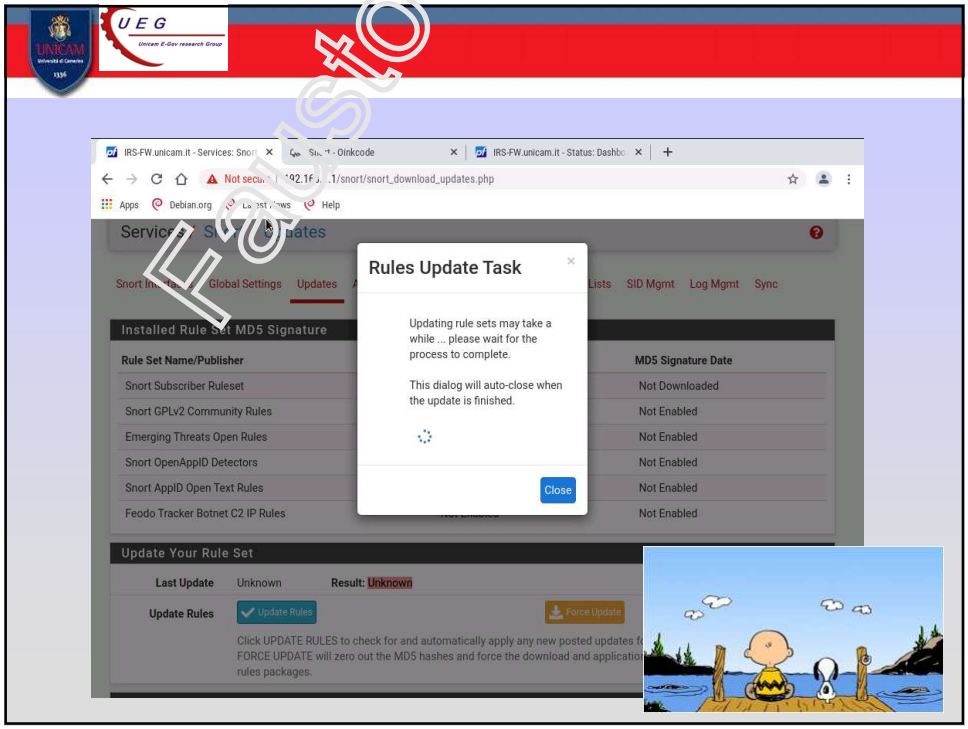
per richiedere un oinkcode

148

pfSense – Package - snort

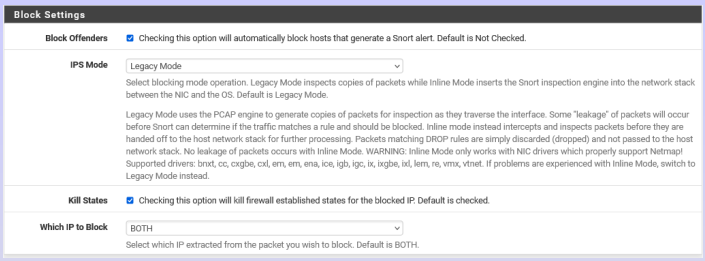


149



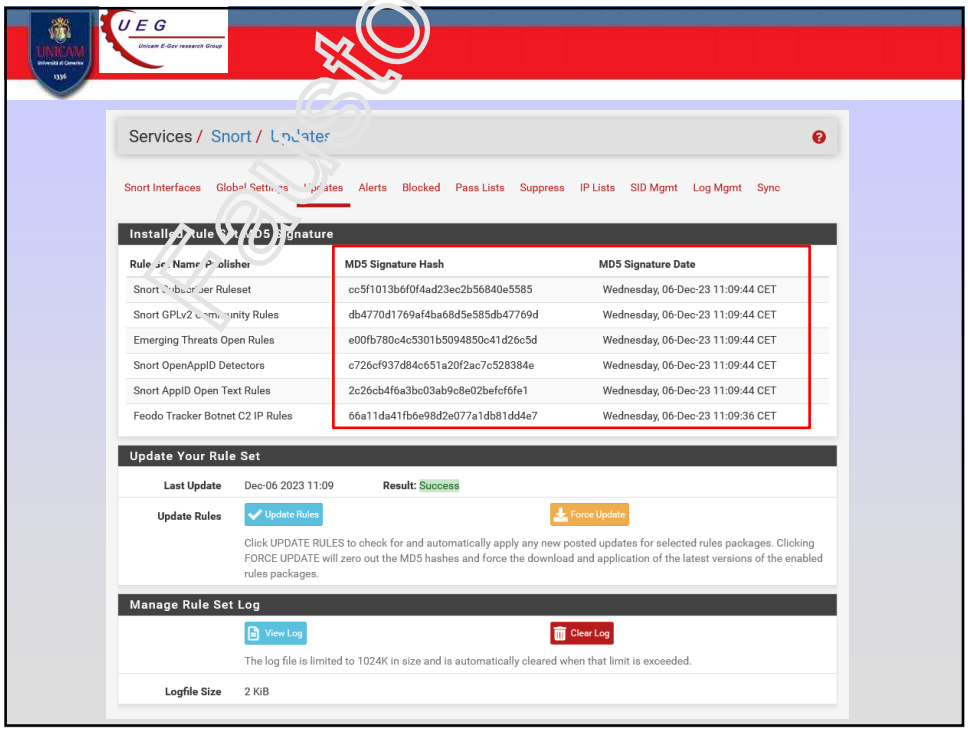
150

pfSense – Package - snort

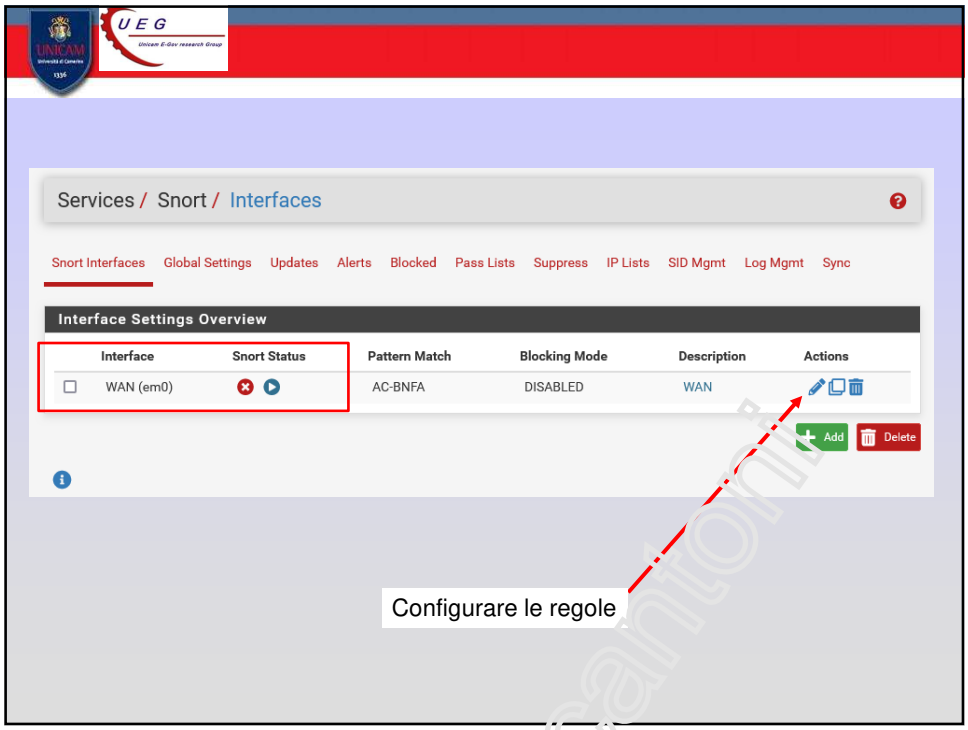


Selezionare il funzionamento in modalità di blocco. La modalità Legacy ispeziona le copie dei pacchetti mentre la modalità Inline inserisce il motore di ispezione Snort nello stack di rete tra la scheda NIC e il sistema operativo. L'impostazione predefinita è la modalità Legacy.
La modalità Legacy utilizza il motore PCAP per generare copie dei pacchetti da ispezionare mentre attraversano l'interfaccia. Si verificherà una certa "perdita" di pacchetti prima che Snort possa determinare se il traffico corrisponde a una regola e deve essere bloccato. La modalità in linea intercetta e ispeziona invece i pacchetti prima che vengano trasferiti allo stack di rete host per un'ulteriore elaborazione. I pacchetti che corrispondono alle regole DROP vengono semplicemente scartati (eliminati) e non passati allo stack di rete host. Con la modalità in linea non si verifica alcuna perdita di pacchetti. ATTENZIONE: la modalità in linea funziona solo con i driver NIC che supportano correttamente Netmap! Driver supportati: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. Se si verificano problemi con la modalità in linea, passa invece alla modalità Legacy.

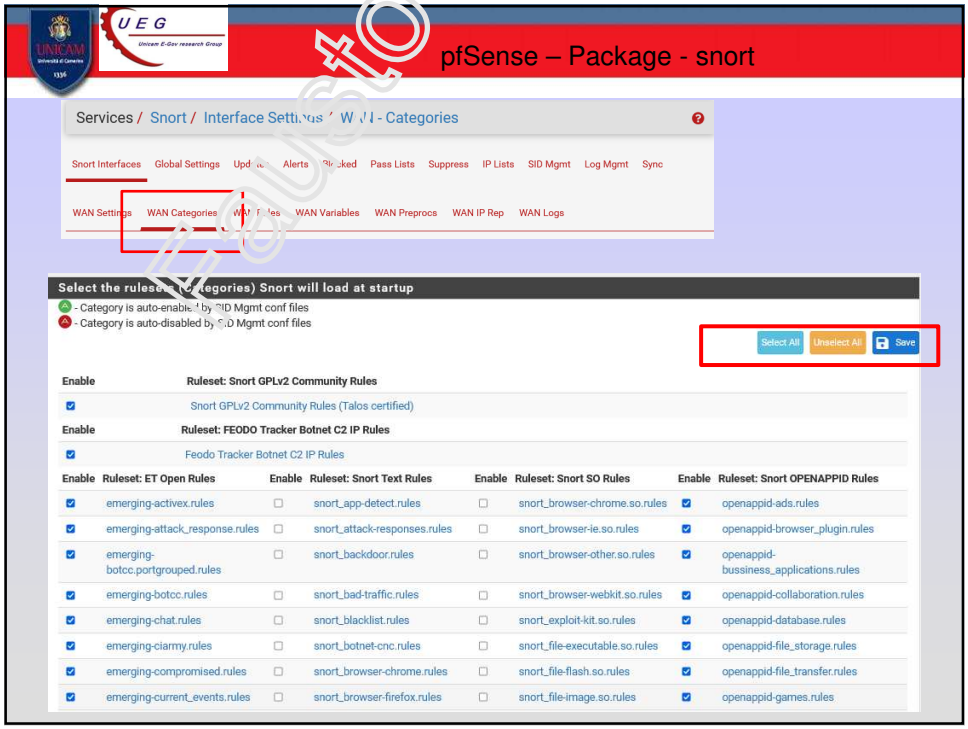
151



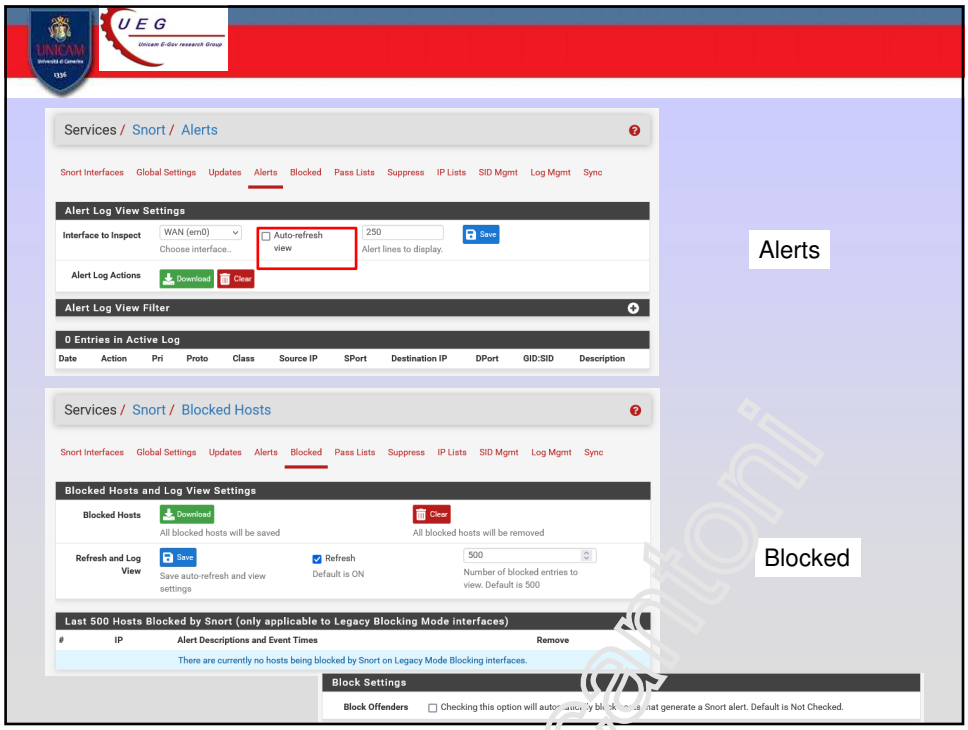
152


Services / Snort / Interfaces
Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
Interface Settings Overview
Interface
Snort Status
Pattern Match
Blocking Mode
Description
Actions
WAN (em0)
AC-BNFA
DISABLED
WAN
Add
Delete
Configurare le regole

153

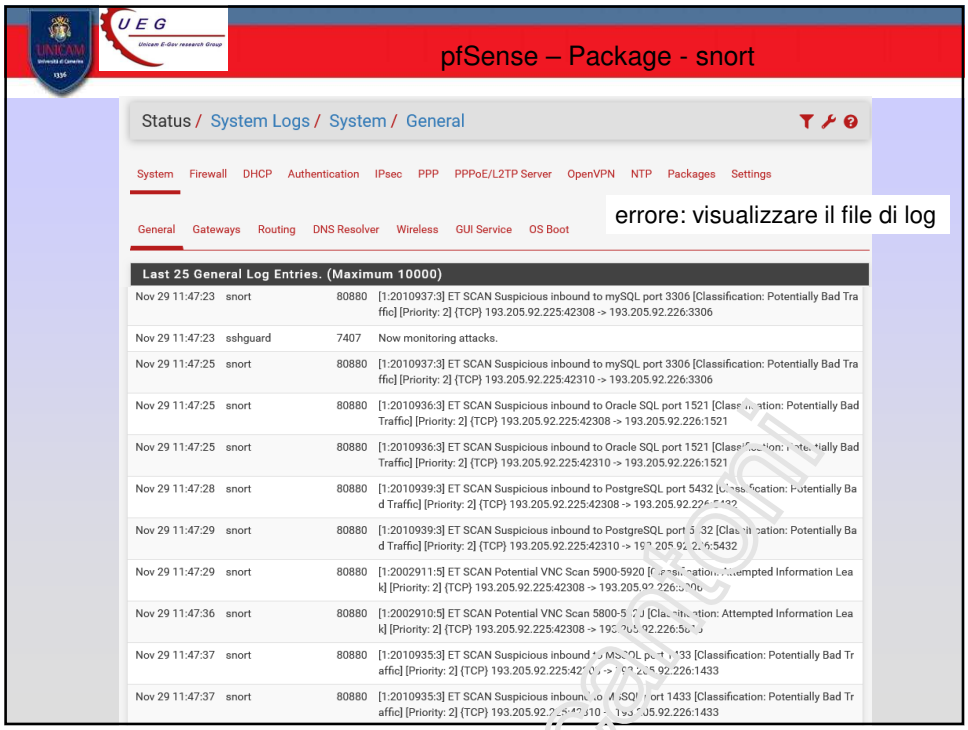

pfSense – Package - snort
Services / Snort / Interface Settings / WAN - Categories
Snort Interfaces
Global Settings
Alerts
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
WAN Settings
WAN Categories
WAN Variables
WAN Preprocs
WAN IP Rep
WAN Logs
Select the ruleset(s) (categories) Snort will load at startup
- Category is auto-enabled by SID Mgmt conf files
- Category is auto-disabled by SID Mgmt conf files
Select All
Unselect All
Save
Enable
Ruleset: Snort GPLv2 Community Rules
Snort GPLv2 Community Rules (Talos certified)
Ruleset: FEODO Tracker Botnet C2 IP Rules
Feodo Tracker Botnet C2 IP Rules
Ruleset: ET Open Rules
Ruleset: Snort Text Rules
Ruleset: Snort SO Rules
Ruleset: Snort OPENAPPID Rules
emerging-activex.rules
emerging-attack_response.rules
emerging-botcc.portgrouped.rules
emerging-botcc.rules
emerging-chat.rules
emerging-ciarmy.rules
emerging-compromised.rules
emerging-current_events.rules
snort_app-detect.rules
snort_attack-responses.rules
snort_backdoor.rules
snort_bad-traffic.rules
snort_blacklist.rules
snort_botnet-cnc.rules
snort_browser-chrome.rules
snort_browser-firefox.rules
snort_browser-chrome.so.rules
snort_browser-ie.so.rules
snort_browser-other.so.rules
snort_browser-webkit.so.rules
snort_exploit-kit.so.rules
snort_file-executable.so.rules
snort_file-flash.so.rules
snort_file-image.so.rules
openappid-ads.rules
openappid-browser_plugin.rules
openappid-bussiness_applications.rules
openappid-collaboration.rules
openappid-database.rules
openappid-file_storage.rules
openappid-file_transfer.rules
openappid-games.rules

154

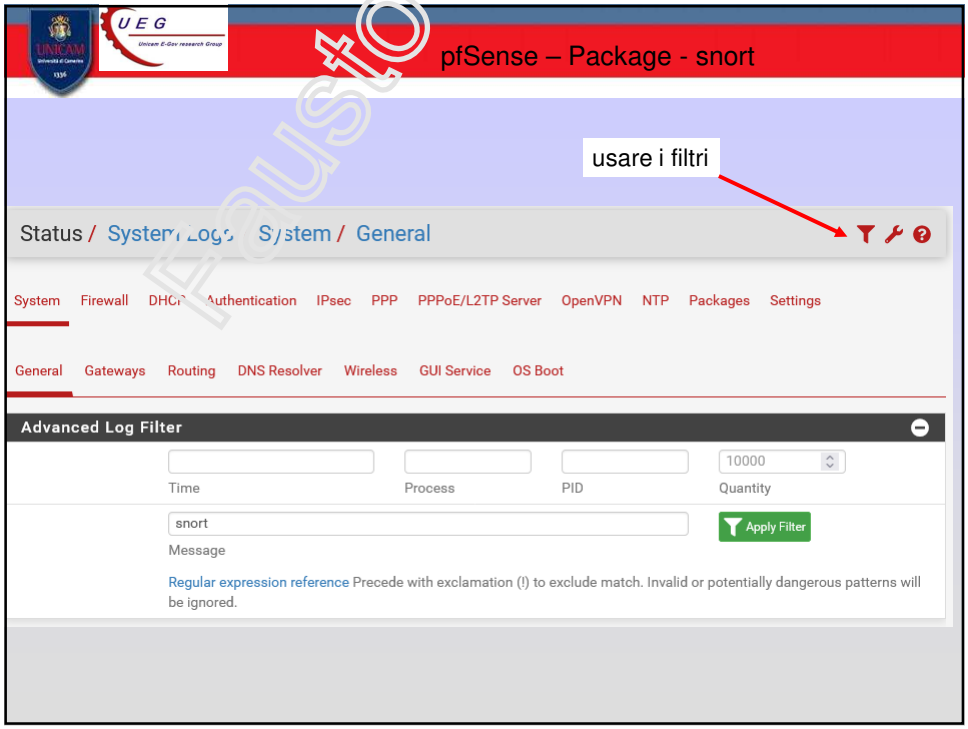


155

156



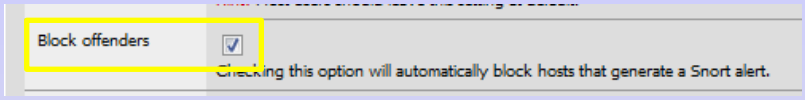
157



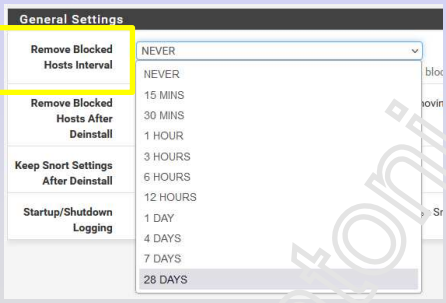
158

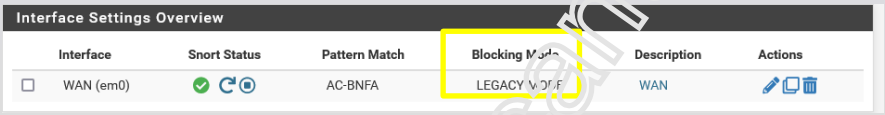
pfSense – Package - snort

Bloccare i tentativi di intrusione e/o “strani” pacchetti



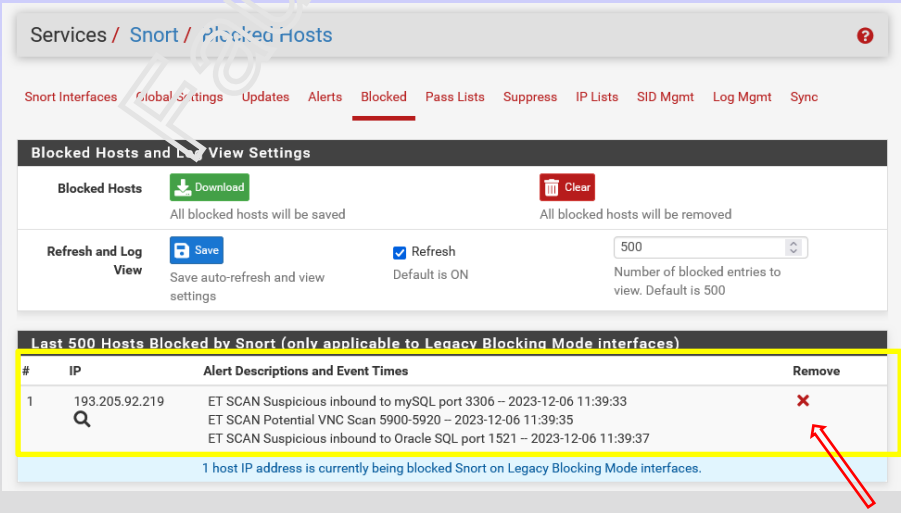
temporizzare il blocco





159

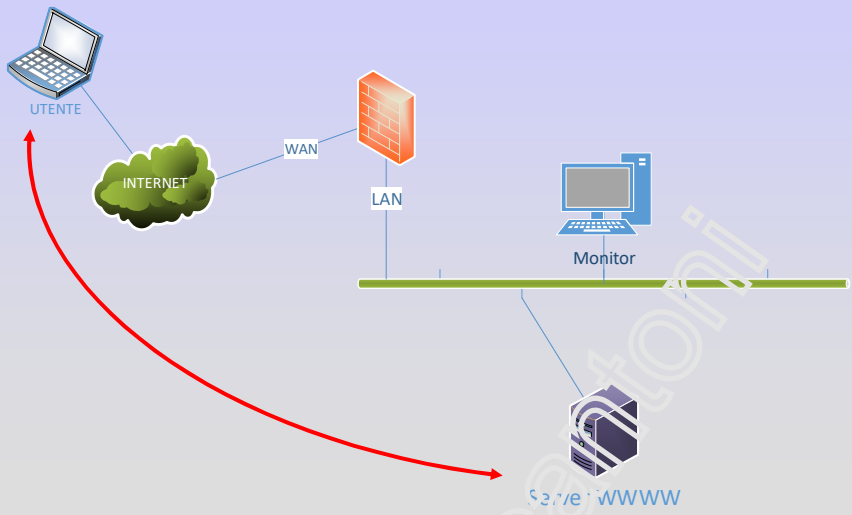
pfSense – Package - snort



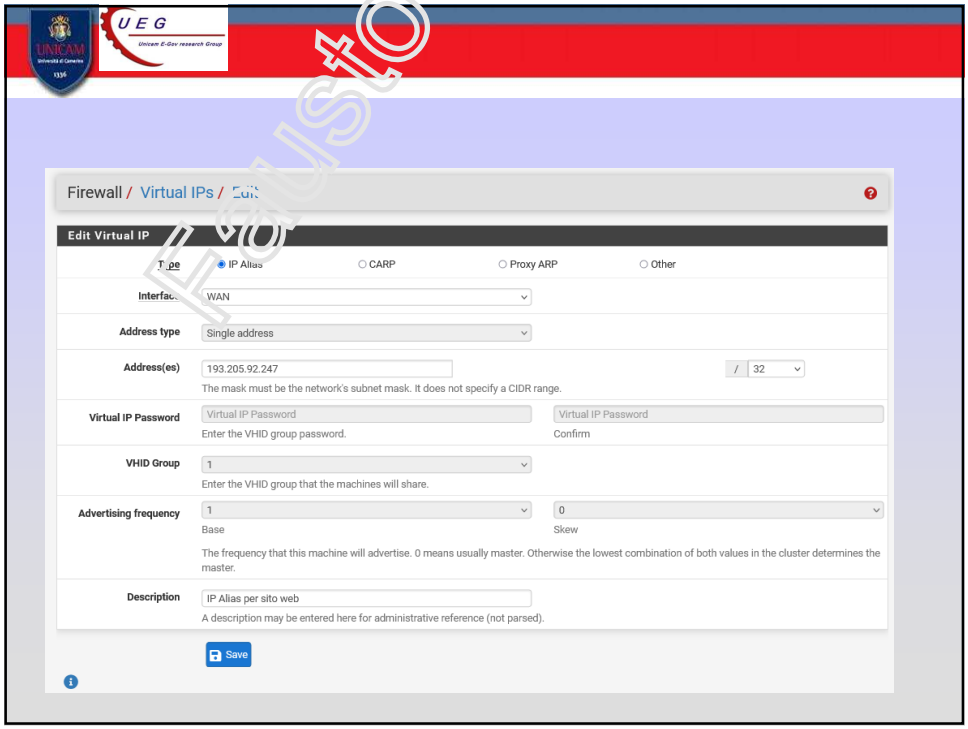
Sbloccare l’host

160

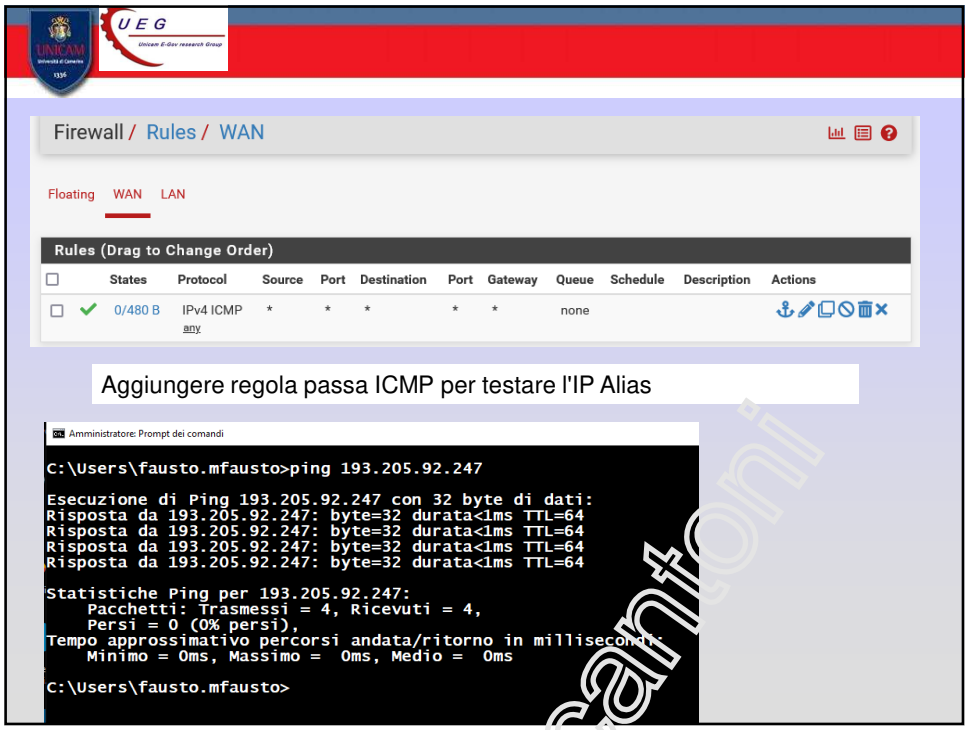
Sono disponibili quattro tipi di indirizzi IP virtuali in pfSense: Alias IP,CARP, Proxy ARP e Altro.



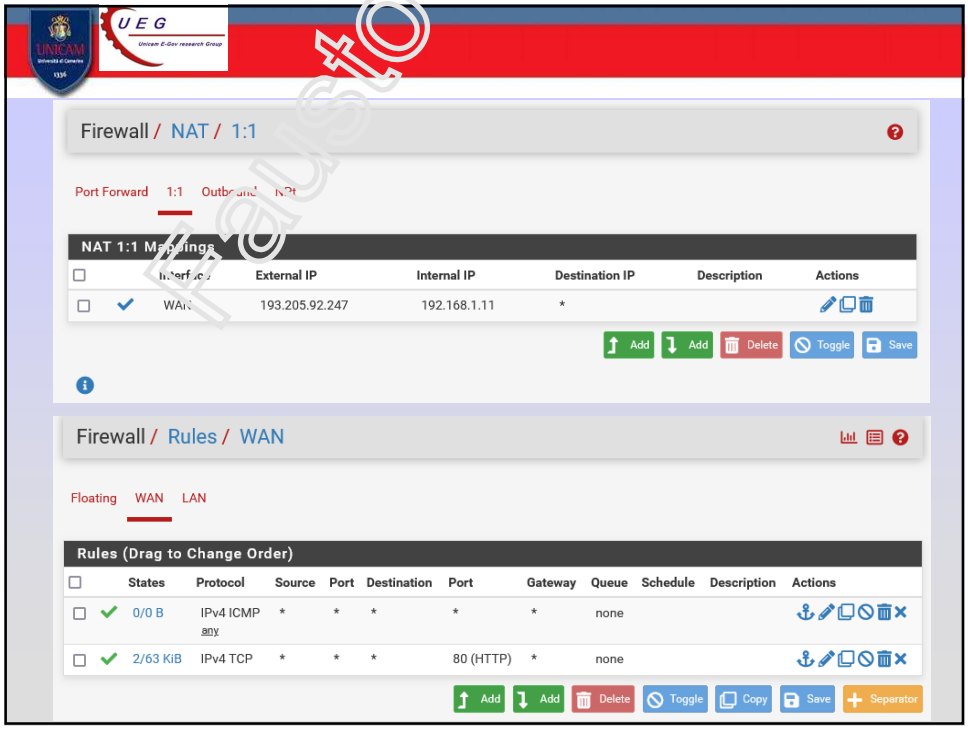
161



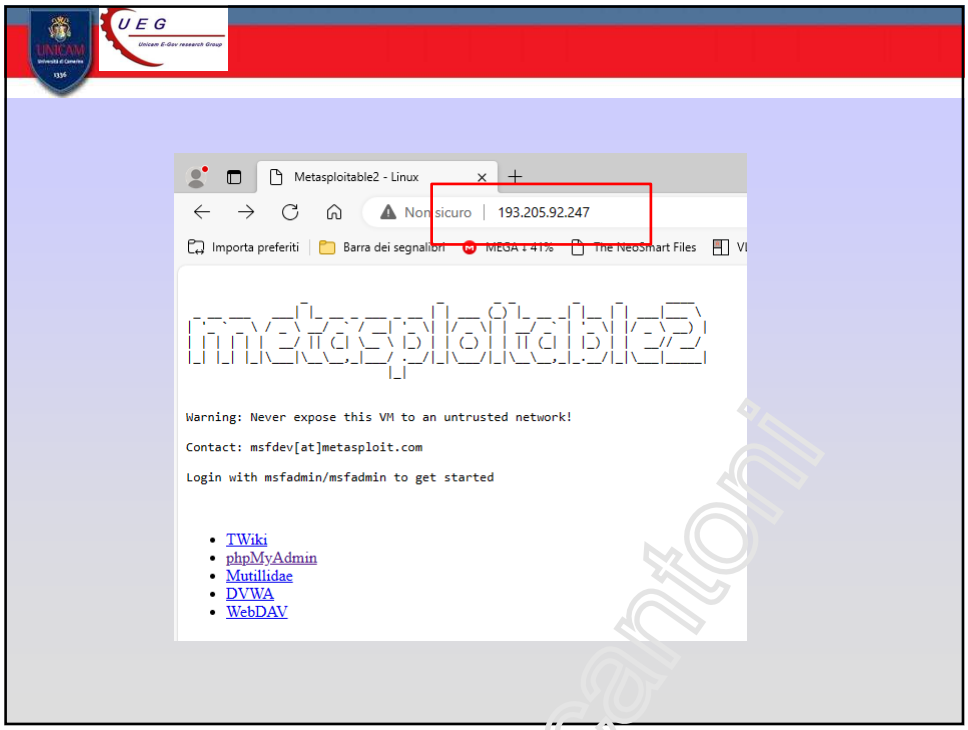
162



163



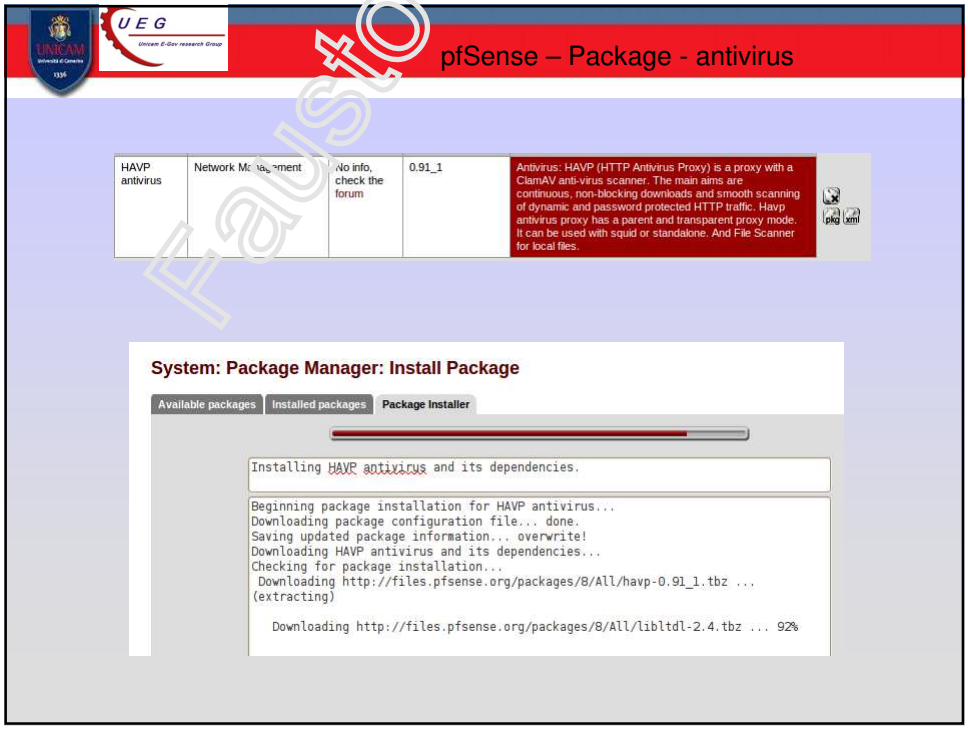
164



165

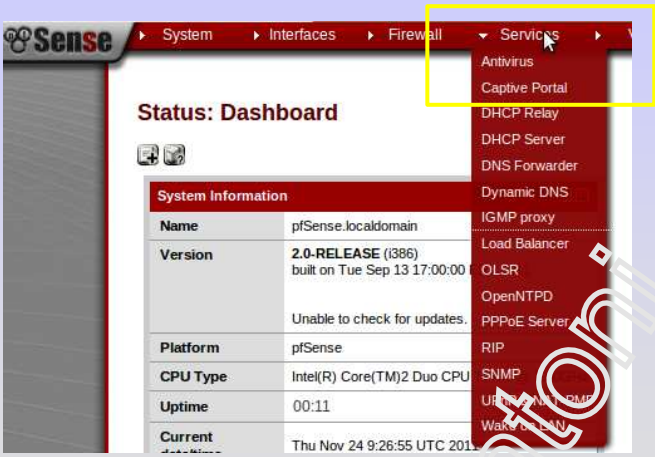
166

167



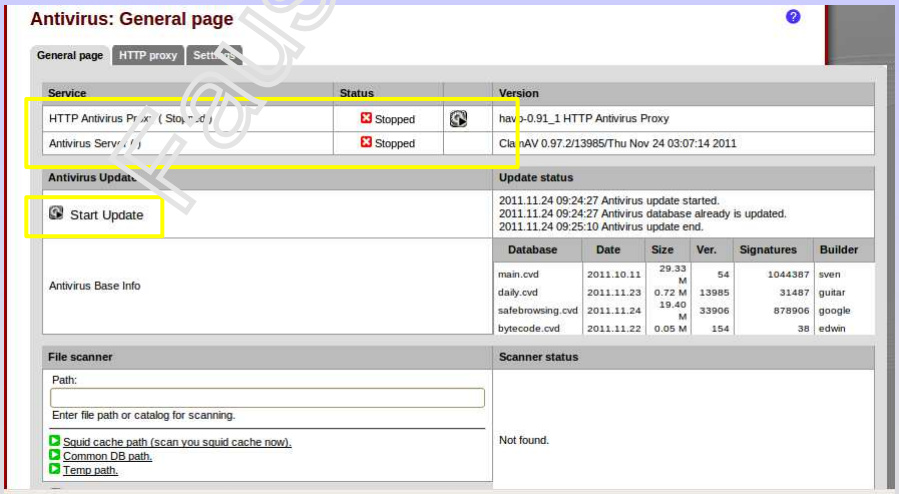
168

pfSense – Package - antivirus



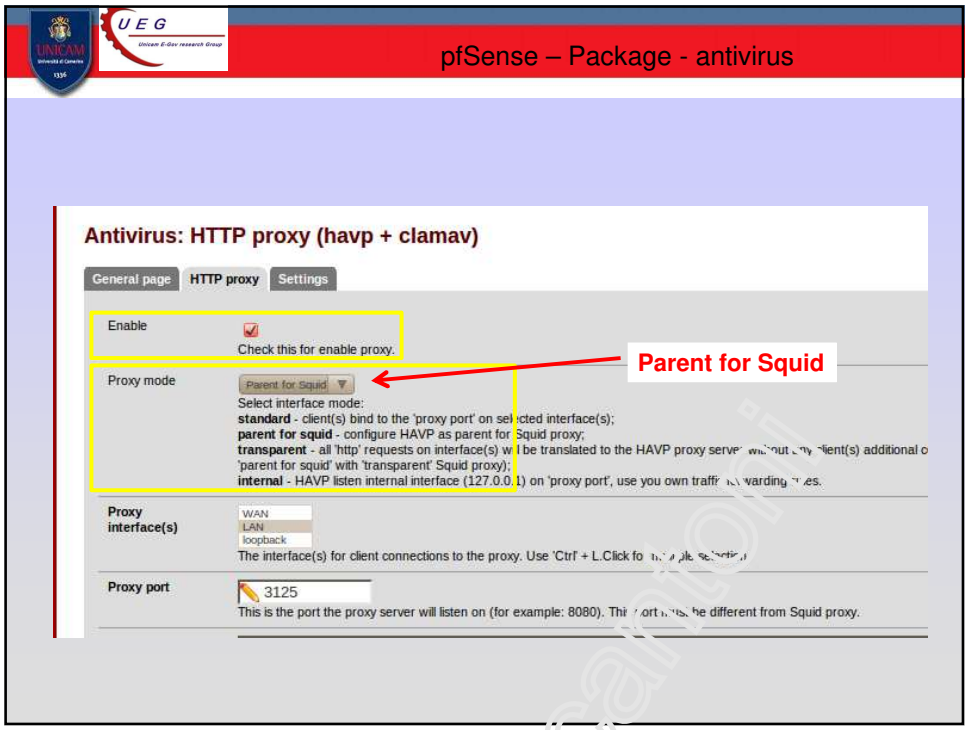
169

pfSense – Package - antivirus



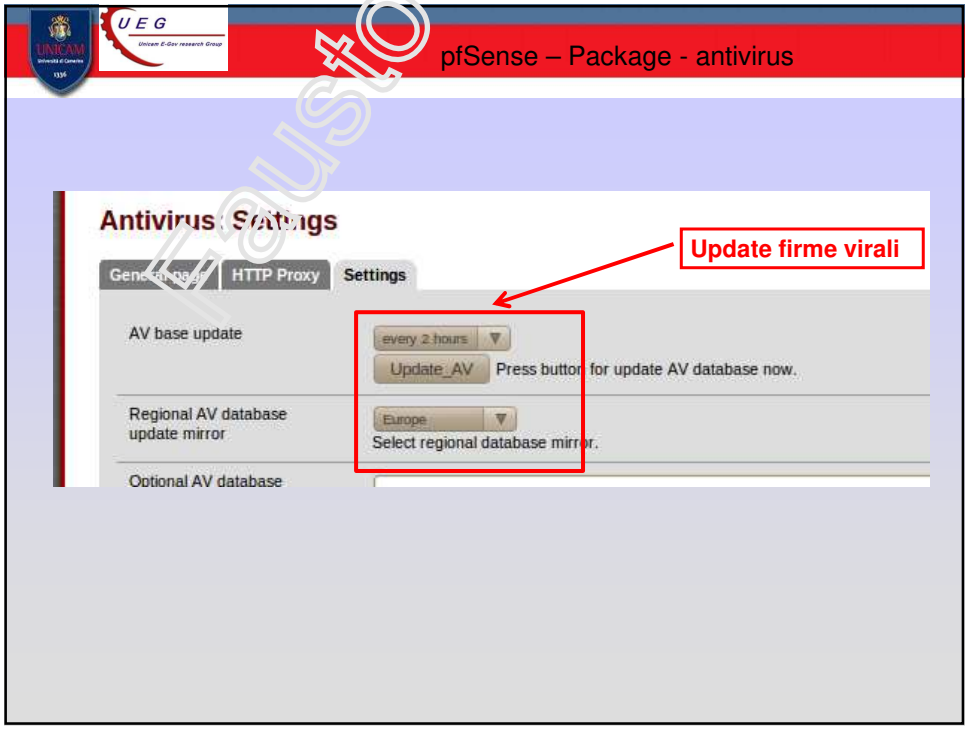
170

pfSense – Package - antivirus



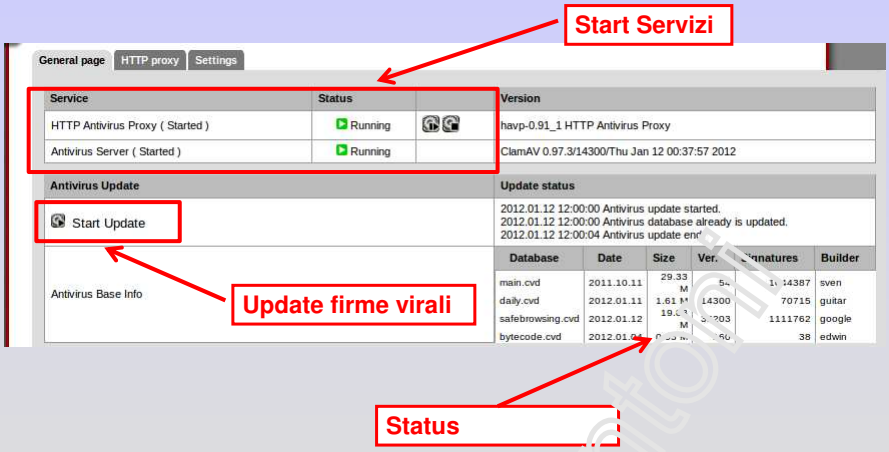
171

pfSense – Package - antivirus



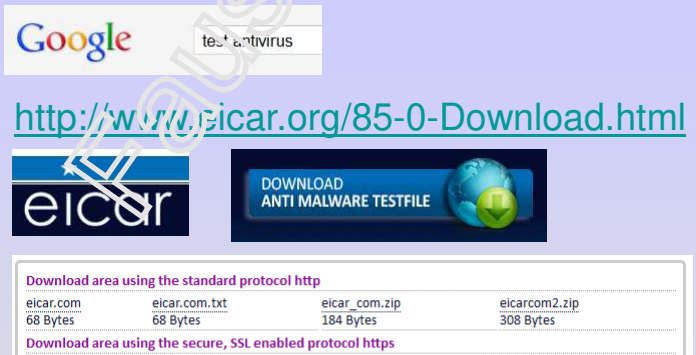
172

pfSense – Package - antivirus



173

pfSense – Package - antivirus



174

pfSense – Captive Portal Https Login

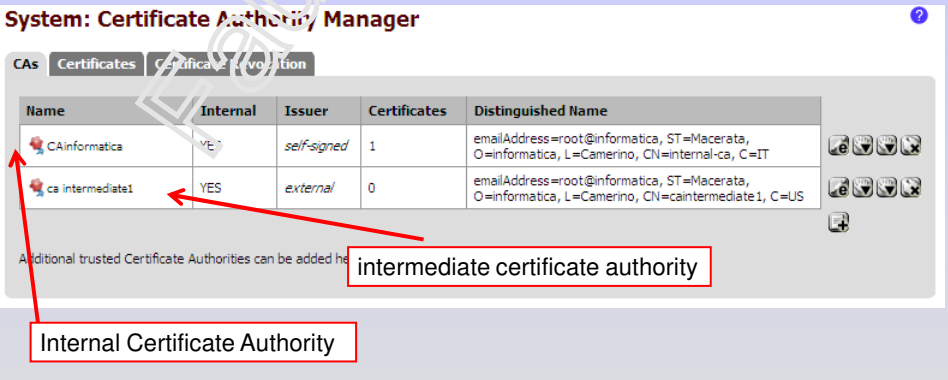
Captive Portal Https Login

I follow the procedure:
System->Cert Manager
then i made the *"Internal Certificate Authority*" in the CAs tab.
Then i made the "*Internal Certificate*" base on the certificate authority.
Later i download the cert and the key and paste on the CP configuration page in the fields *https certificate* and *https private key* respectively.
In the CAs tab i made the *intermediate certificate authority* base on the internal certificate authority.
In every one of them, the common-name is the same, and also in the cp page configuration *https server name*.
i put the ip of my server pfsense in "HTTPS sever name" and works

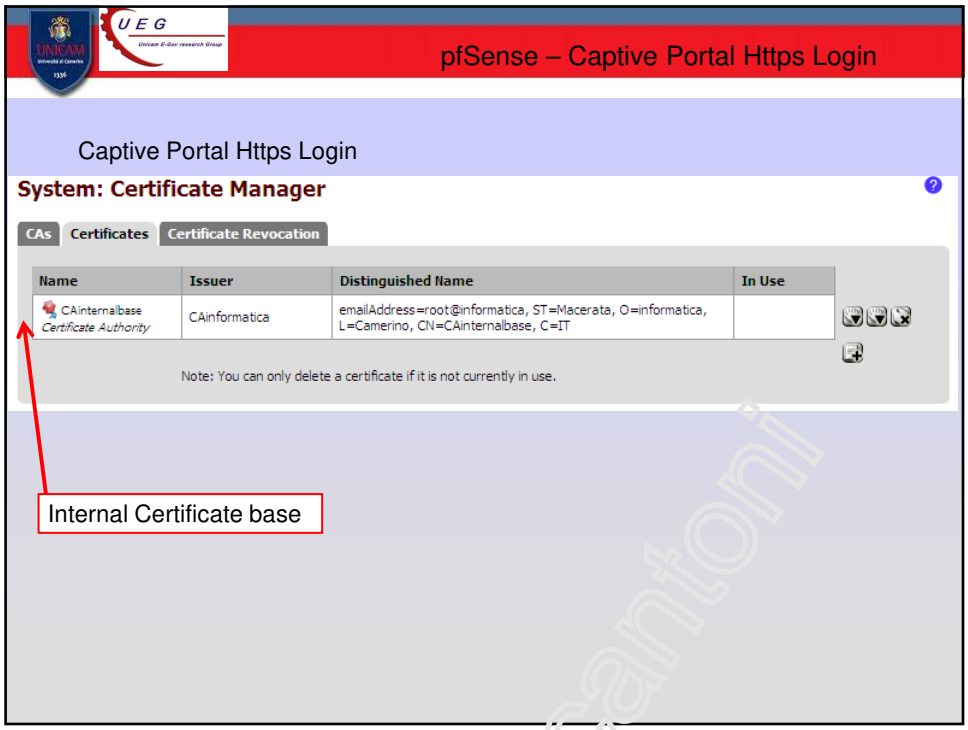
175

pfSense – Captive Portal Https Login

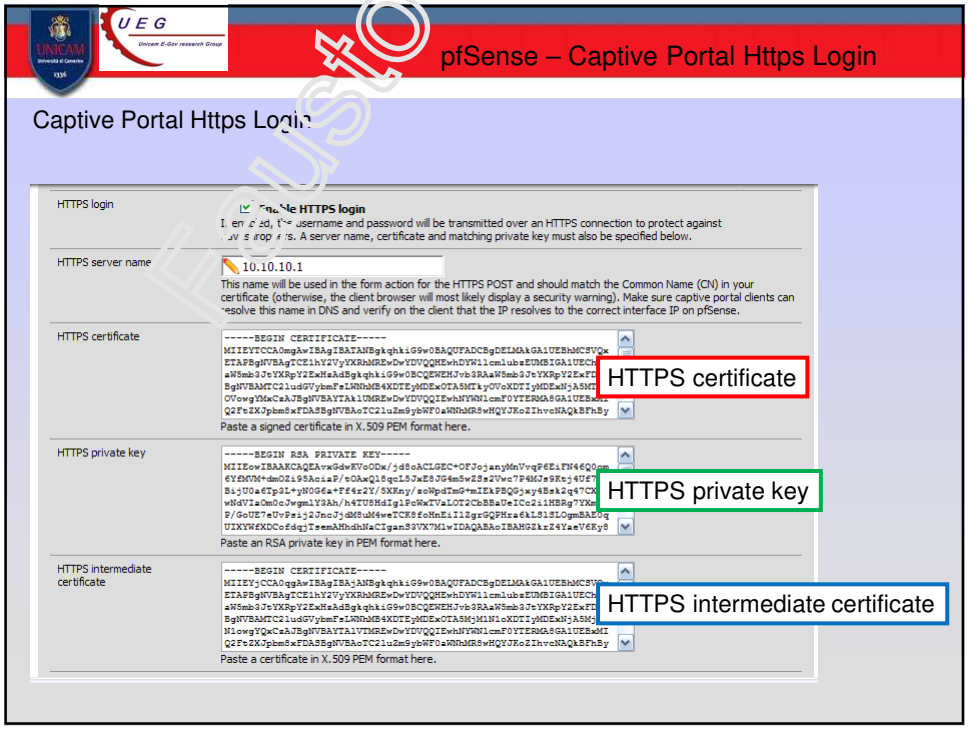
Captive Portal Https Login



176


pfSense – Captive Portal Https Login
Captive Portal Https Login
System: Certificate Manager
CAs
Certificates
Certificate Revocation
Name
Issuer
Distinguished Name
In Use
CAinternalbase
Certificate Authority
CAinformatica
emailAddress=root@informatica, ST=Macerata, O=informatica, L=Camerino, CN=CAinternalbase, C=IT
Note: You can only delete a certificate if it is not currently in use.
Internal Certificate base

177


pfSense – Captive Portal Https Login
Captive Portal Https Login
HTTPS login
HTTPS server name
10.10.10.1
This name will be used in the form action for the HTTPS POST and should match the Common Name (CN) in your certificate (otherwise, the client browser will most likely display a security warning). Make sure captive portal clients can resolve this name in DNS and verify on the client that the IP resolves to the correct interface IP on pfSense.
HTTPS certificate
Paste a signed certificate in X.509 PEM format here.
HTTPS private key
Paste an RSA private key in PEM format here.
HTTPS intermediate certificate
Paste a certificate in X.509 PEM format here.

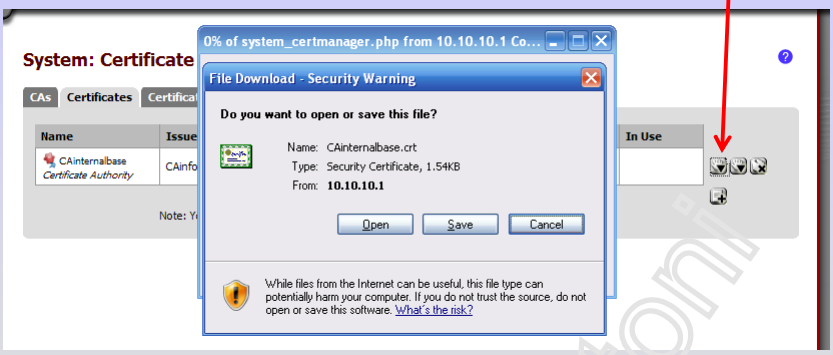
178

pfSense – Captive Portal Https Login

Captive Portal Https Login

HTTPS certificate

export cert



Salvare sul Desktop e aprire con Notepad
Fare Copia e Incolla del certificato

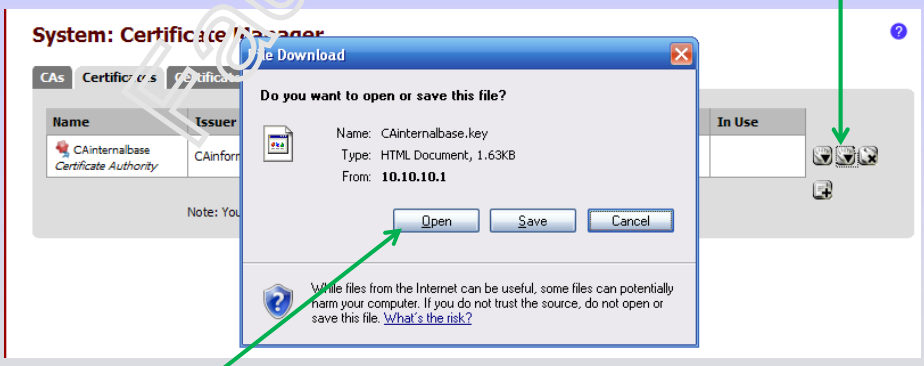
179

pfSense – Captive Portal Https Login

Captive Portal Https Login

HTTPS private key

export key



Open direttamente
Fare Copia e Incolla del certificato

180

pfSense – Captive Portal Https Login

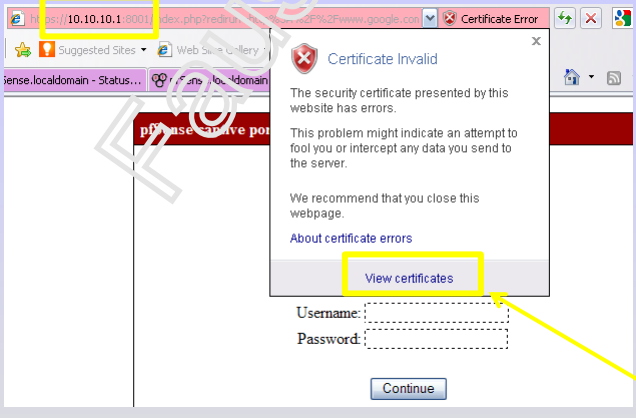
Captive Portal Https Login

HTTPS intermediate certificate

Salvare sul Desktop e aprire con Notepad
Fare Copia e Incolla del certificato

181

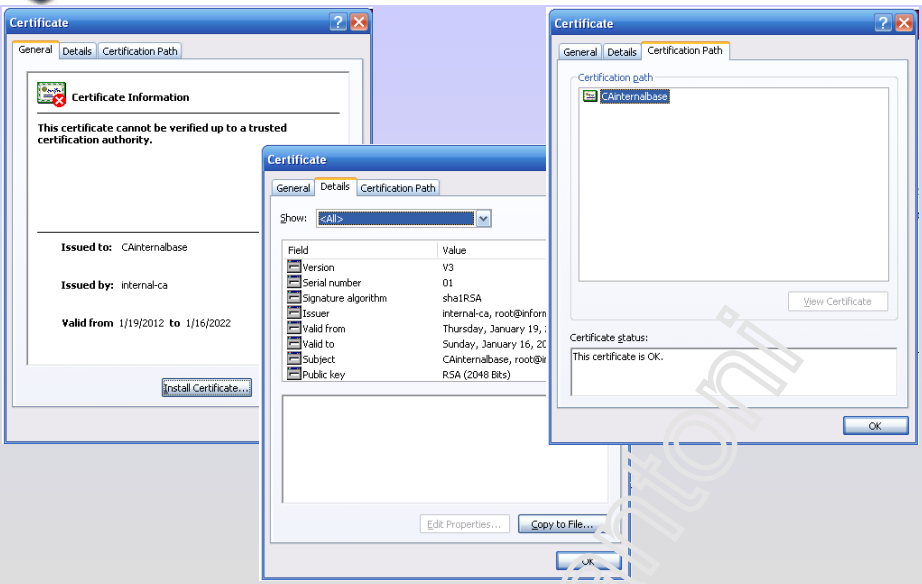
pfSense – Captive Portal Https Login



Dettagli Certificato

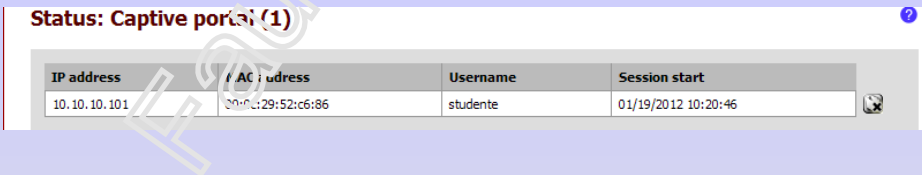
182

pfSense – Captive Portal Https Login



183

pfSense – Captive Portal Https Login



FATTO - FUNZIONA

184