pfSense

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

Fausto Marcantoni
fausto.marcantoni@unicam.it

1

Prevenire è meglio che curare

2

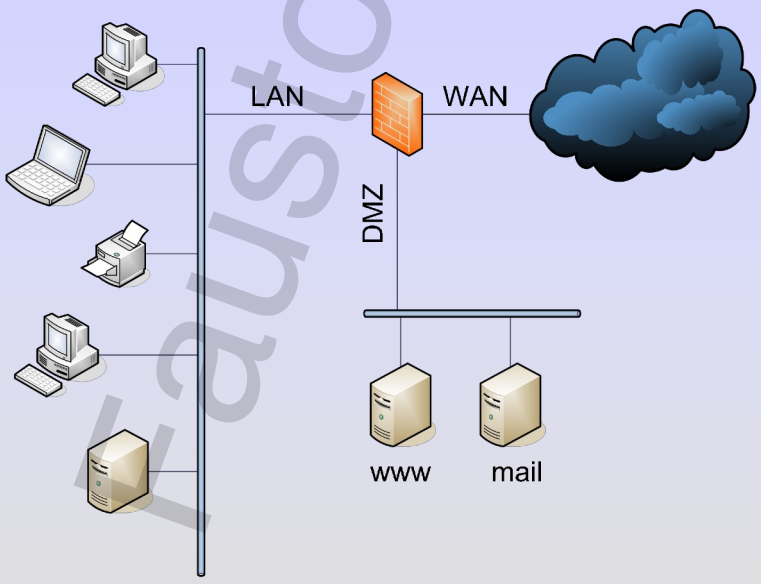
Chi ben comincia …

- **“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

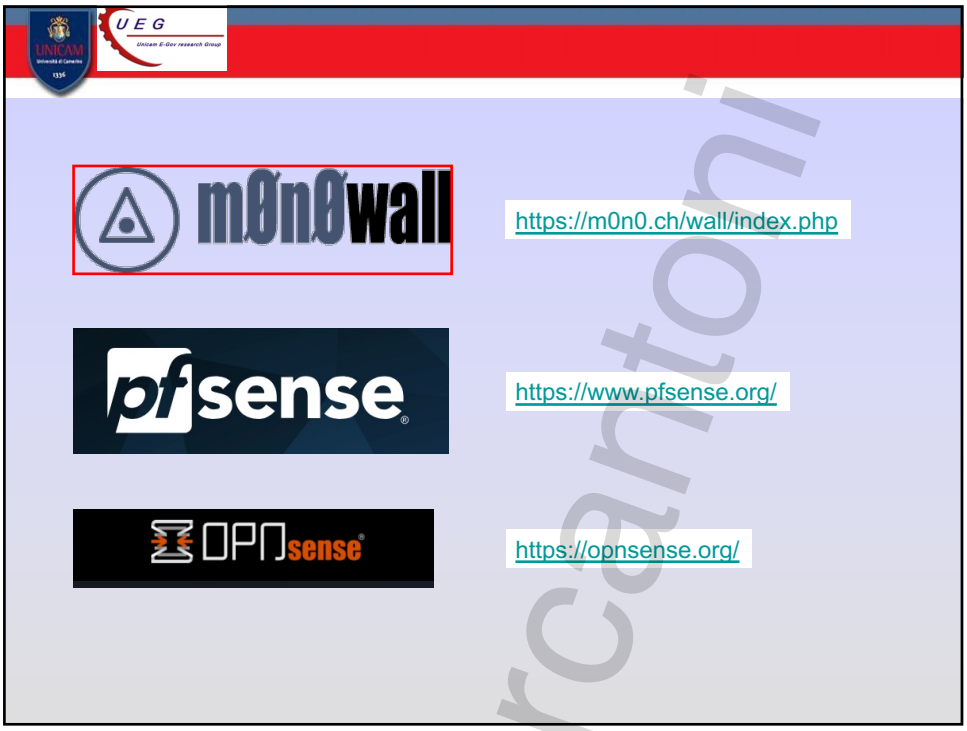
Un firewall non si compra si progetta

3

Topologia della rete



4

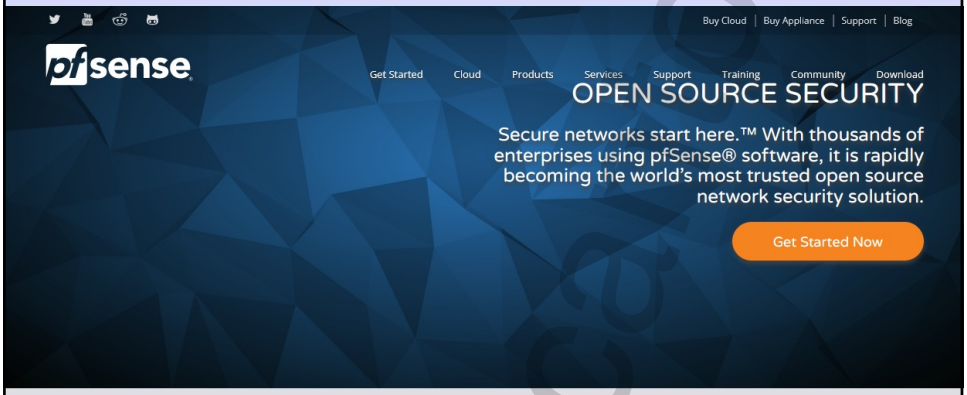


5

6

pfSensel – sito www

https://pfsense.org/

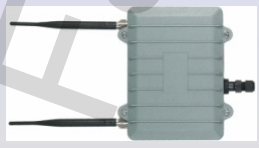


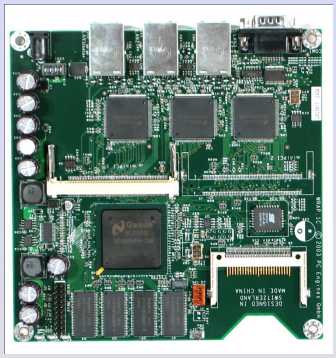
7

pfSense – applicazioni embedded

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

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

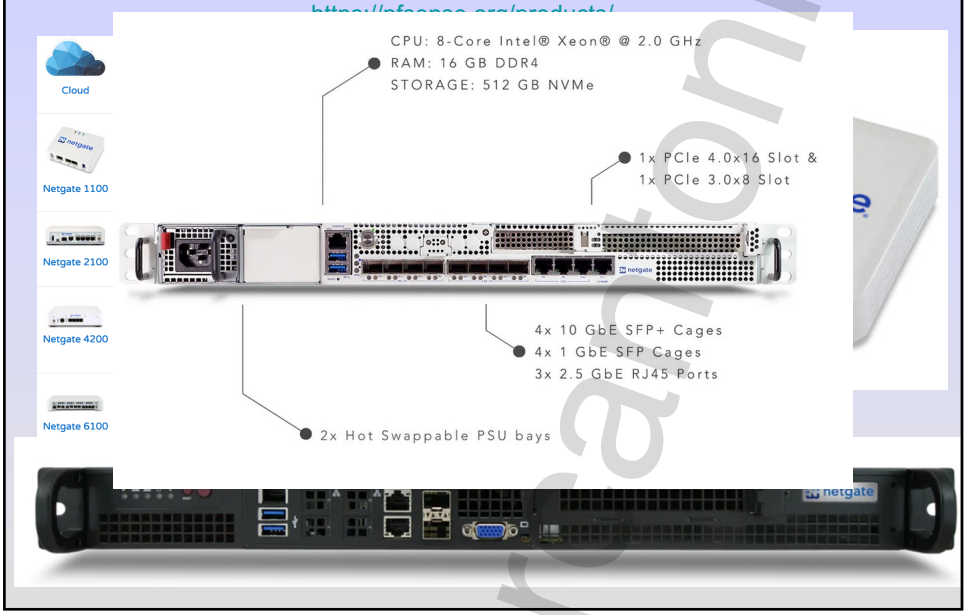




http://www.pcengines.ch/wrap.htm

8

pfSense – applicazioni embedded



9

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/

10

pfSensel – functions and features

The main pfSense functions and features are:

- **Firewall**
- **State Table** 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...**

11

pfSense – software

FreeBSD
OpenBSD's pf
mini_httpd
PHP configuration subsystem
webGUI

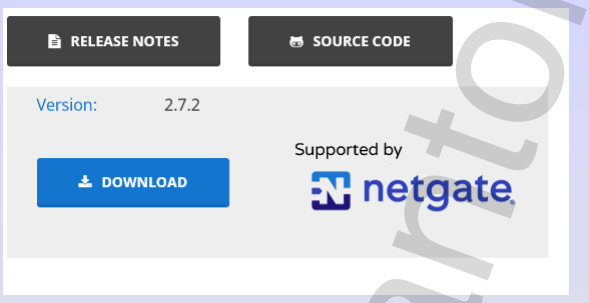
Packages

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

12

pfSense – software download

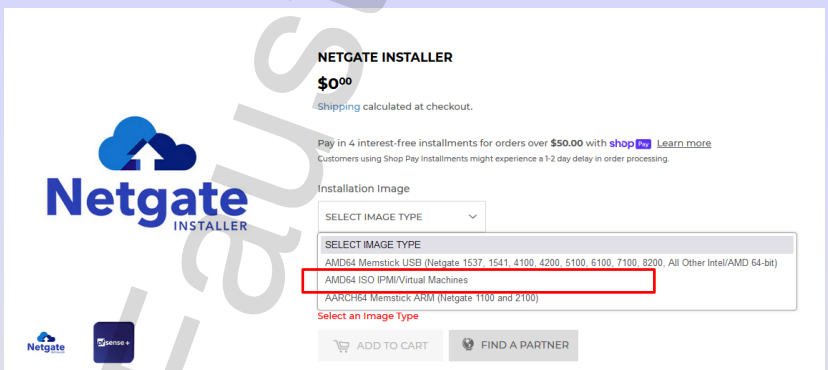
Quale file scaricare ???



13

pfSense – software download

Quale file scaricare ???



14

Repository Mirror

https://atxfiles.netgate.com/mirror/downloads/

https://blog.miniserver.it/pfsense/scarica-pfsense/

15

pfsense download old version

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

pfSense CE software

2.7.x

Version	Support	Released	Config Rev	FreeBSD Version	Branch
2.7.1	✔	2023-11-16	23.3	14.0-CURRENT@0c783a37d5d5	RELEN
2.7.0	✔	2023-06-29	22.9	14.0-CURRENT@0c59e0b4e581	RELEN

2.6.x

Version	Support	Released	Config Rev	FreeBSD Version	Branch
2.6.0	✖	2022-02-14	22.2	12.3-STABLE@ef1e43df92c6	RELENG_2

2.5.x

Version	Support	Released	Config Rev	FreeBSD Version	Branch
2.5.2	✖	2021-07-07	21.7	12.2-STABLE@f4d0bc6aa6b	RELENG_2
2.5.1	✖	2021-04-13	21.5	12.2-STABLE@f4d0bc6aa6b	RELENG_2
2.5.0	✖	2021-02-17	21.4	12.2-STABLE@f4d0bc6aa6b	RELENG_2

2.4.x

Version	Support	Released	Config Rev	FreeBSD Version	Branch
2.4.5-p1	✖	2020-06-09	19.1	11.3-STABLE@r357046	RELENG_2_4_5
2.4.5	✖	2020-03-26	19.1	11.3-STABLE@r357046	RELENG_2_4_5
2.4.4-p3	✖	2019-05-20	19.1	11.2-RELEASE-p10	RELENG_2_4_4
2.4.4-p2	✖	2019-01-07	18.9	11.2-RELEASE-p4	RELENG_2_4_4
2.4.4-p1	✖	2018-12-03	18.9	11.2-RELEASE-p4	RELENG_2_4_4

On This Page
- pfSense Plus software
  - 23.x
  - 22.x
  - 21.x
- pfSense CE software
  - 2.7.x
  - 2.6.x
  - 2.5.x
  - 2.4.x
  - 2.3.x
  - 2.2.x
  - 2.1.x
  - 2.0.x
  - 1.2.x
- Legend
- Understanding pfSense Plus and CE software version numbers

16

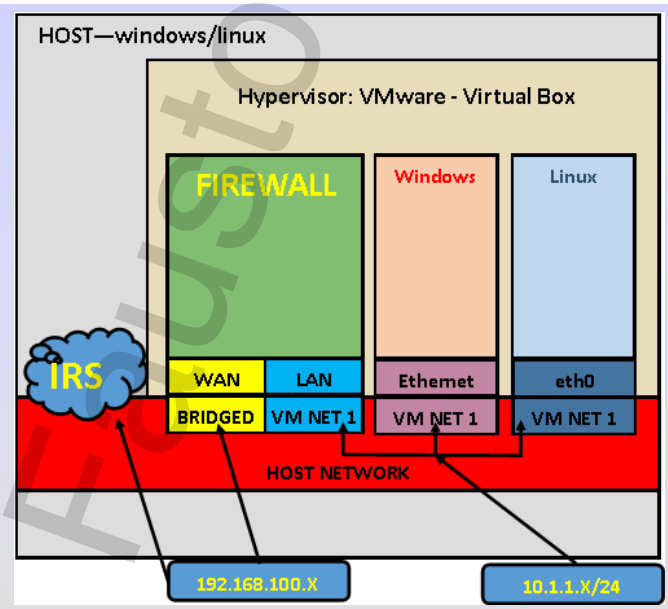
pfSense – installazione

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

Installation Guides

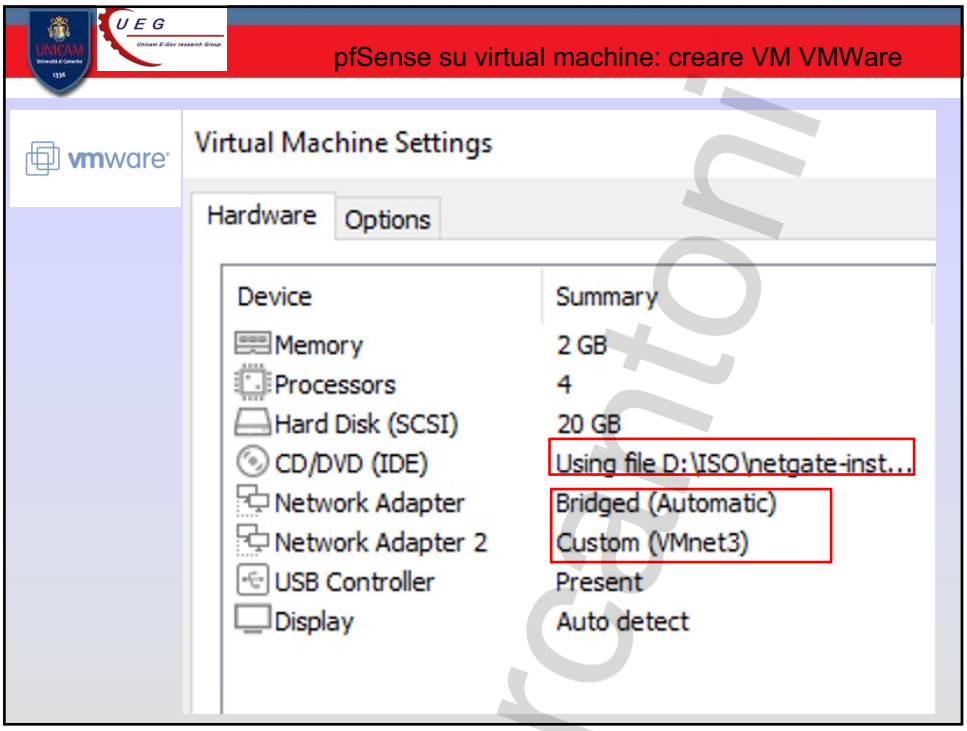
https://docs.netgate.com/pfsense/en/latest/install/download-installer-image.html

17



18

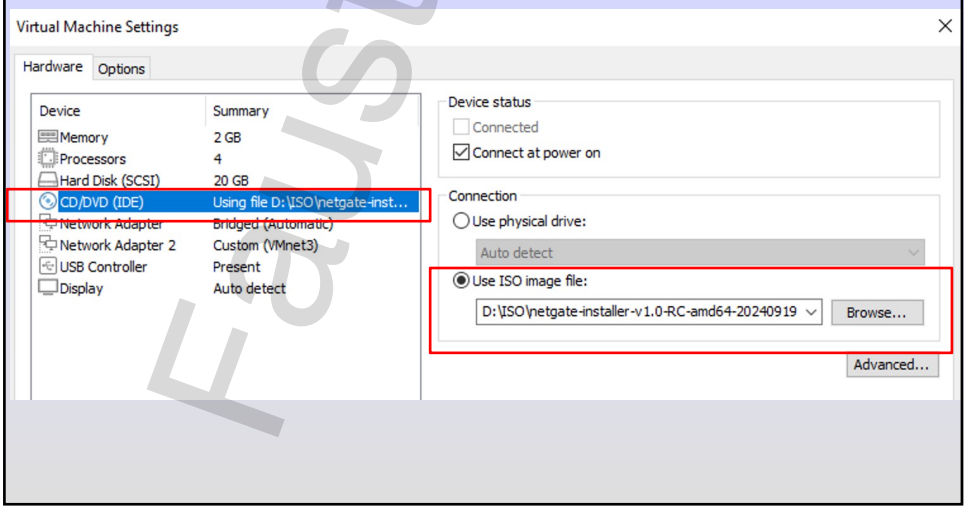
pfSense su virtual machine: creare VM VMWare



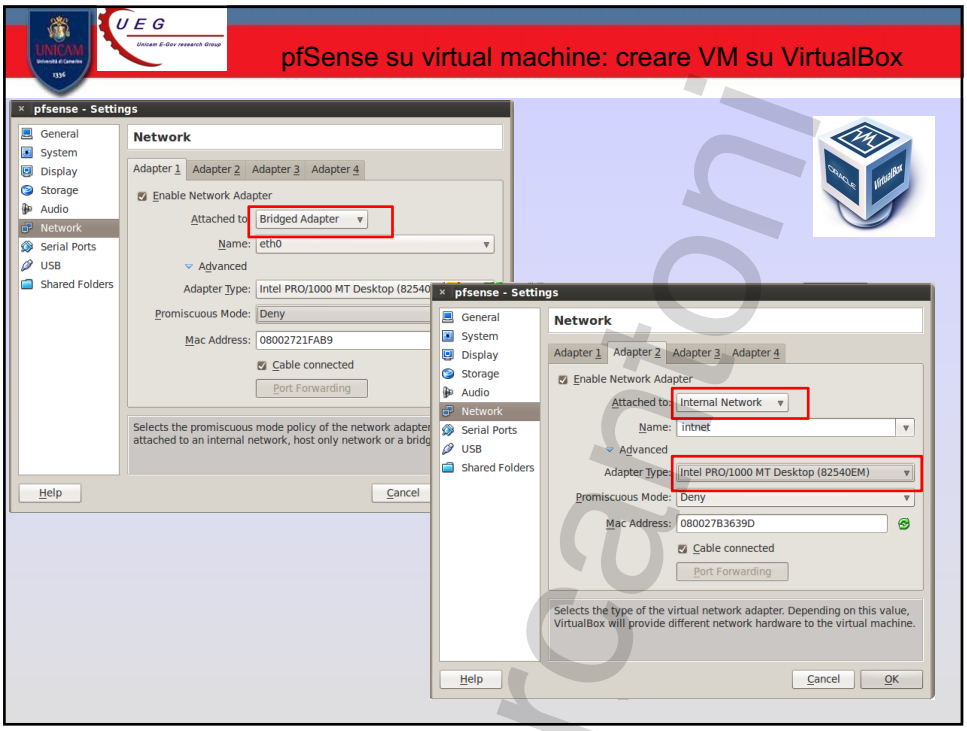
19

pfSense su virtual machine: creare VM VMWare

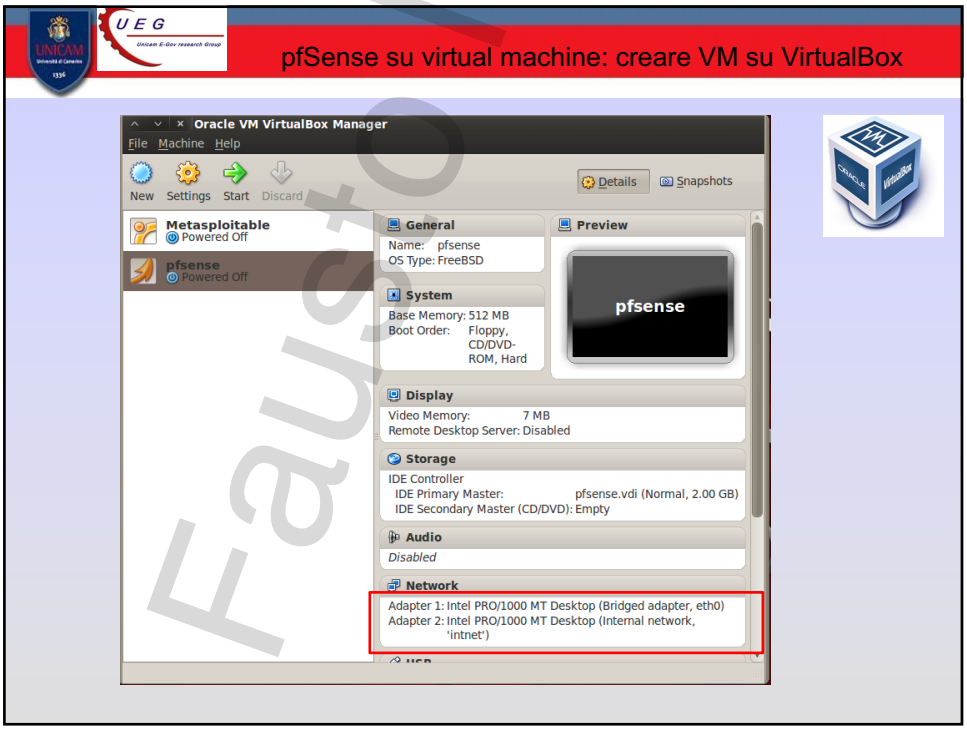
selezionare la ISO per il boot



20



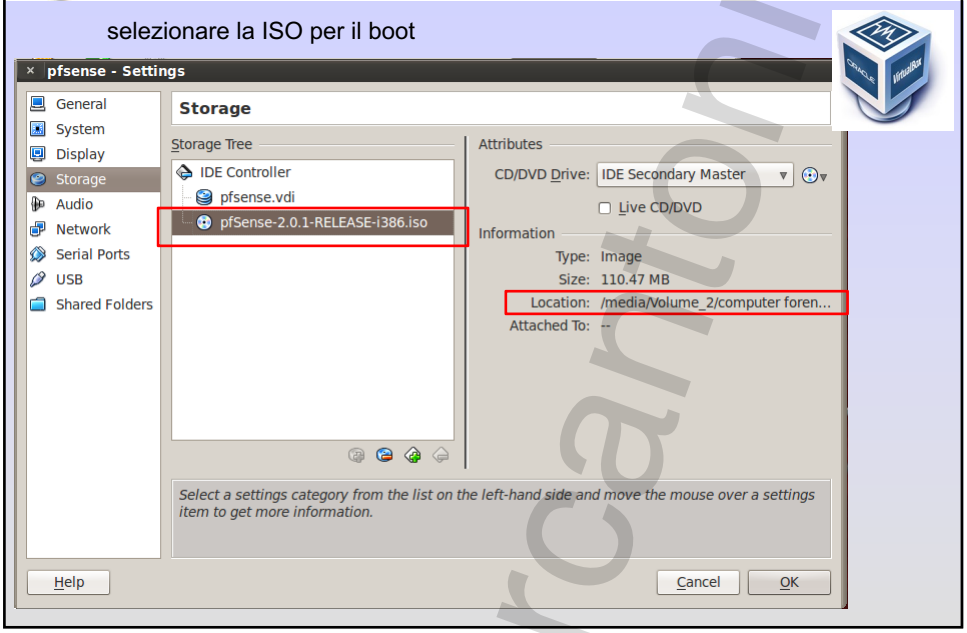
21



22

pfSense su virtual machine: creare VM su VirtualBox

selezionare la ISO per il boot



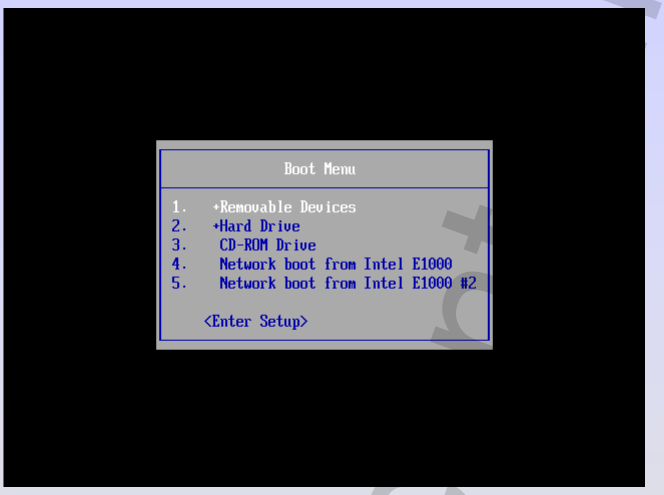
23

pfSense su virtual machine: creare VM

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

24

pfSense su VM: boot / setup bios



25

pfSense su VM: boot

non riesco ad entrare nel BIOS: è troppo veloce

Re: 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.

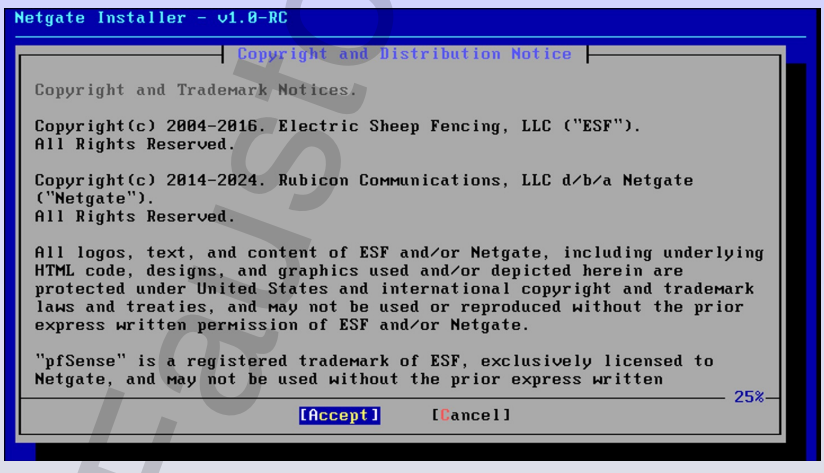
Google vmware bios delay

26

pfSense: startup page

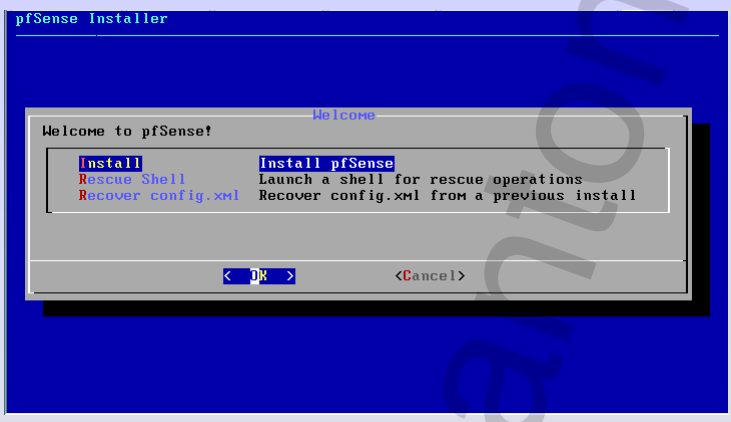
27

pfSense – installazione – primo avvio



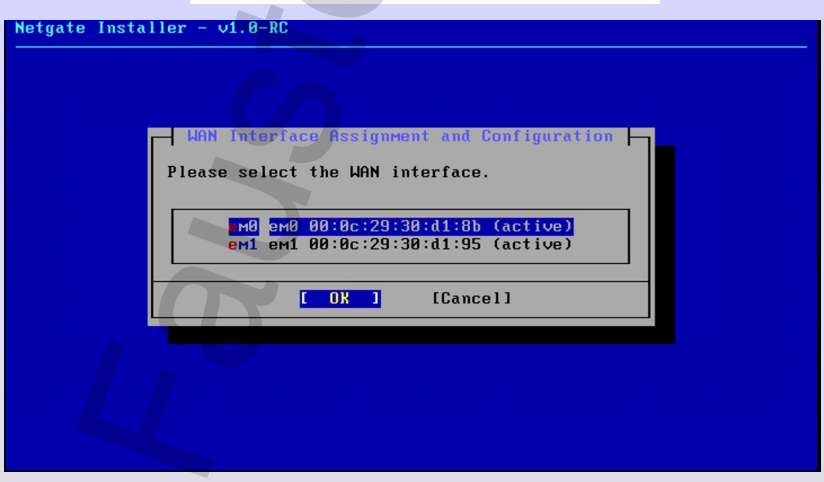
28

pfSense – installazione – primo avvio



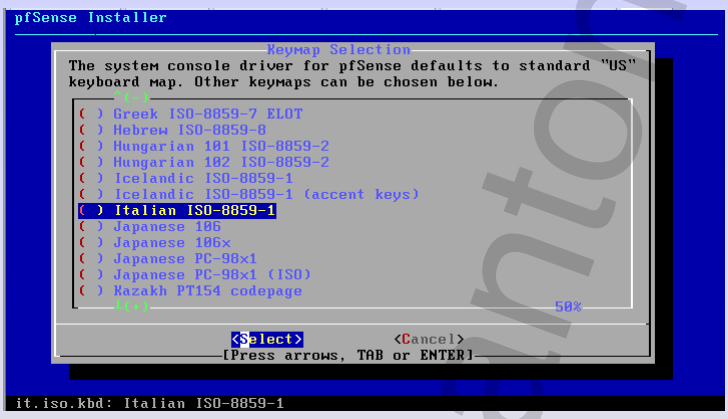
29

Selezionare l'interfaccia di rete della WAN



30

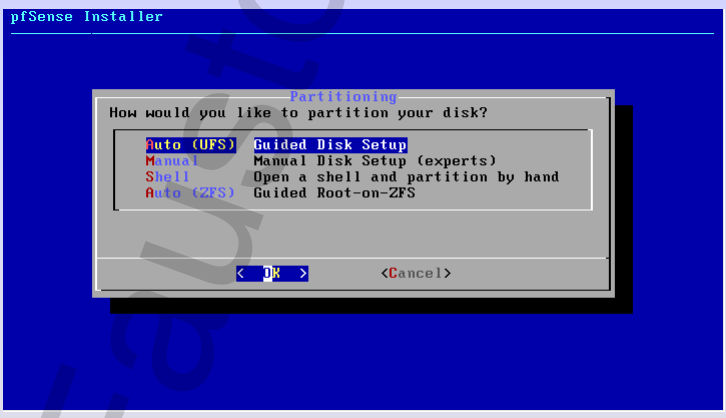
pfSense – installazione



Scegliere il layout della tastiera

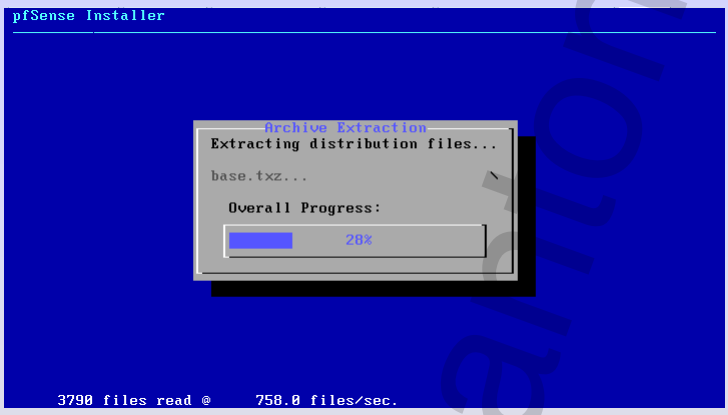
31

pfSense – installazione



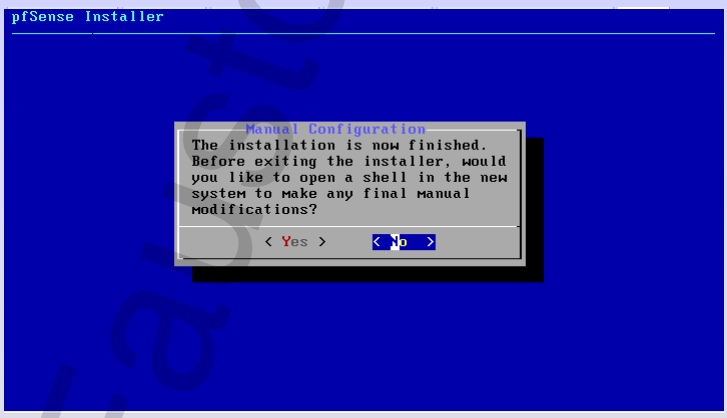
32

pfSense – installazione



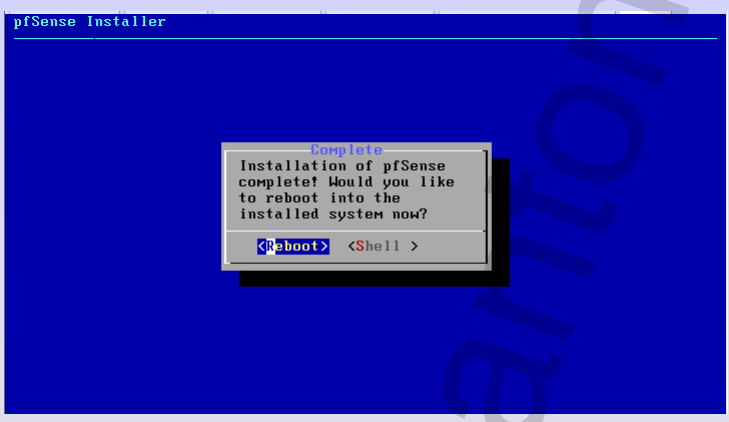
33

pfSense – installazione



34

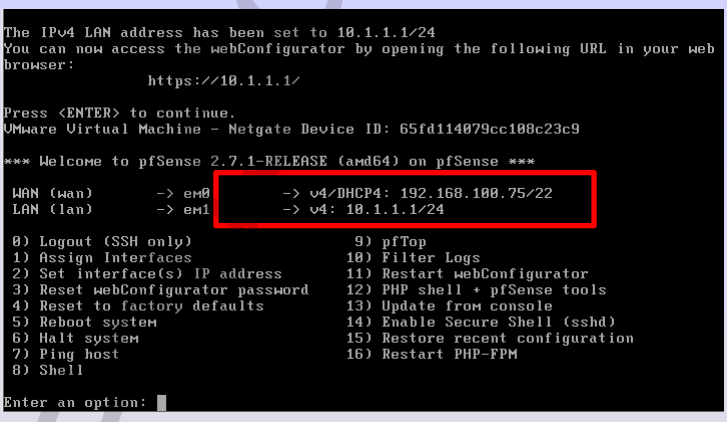
pfSense – installazione



Fatto …

35

pfSense – installazione

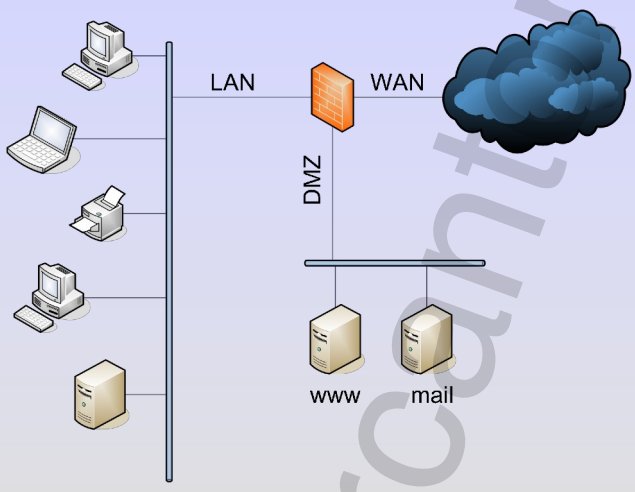


… Fatto …

36

pfSense – configurazione – primo avvio

Assegnazione delle interfacce di rete: LAN – WAN – DMZ



37

pfSense – installazione

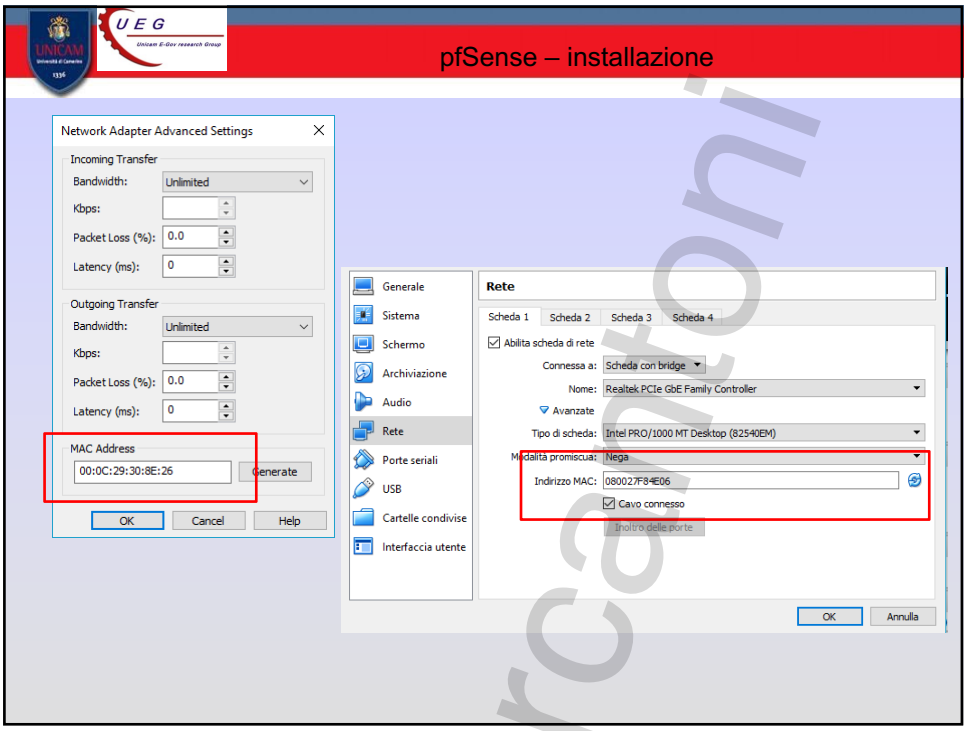
```
Welcome to pfSense 2.0-RELEASE   ...

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]?
```

nomi e stato delle interfacce

MAC address delle interfacce

38

pfSense – installazione



39

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"
```

40

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

41

pfSense – assegnare le interfacce di rete

```
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]? n

*NOTE*  pfSense requires *AT LEAST* 1 assigned interface(s) to function.
        If you do not have *AT LEAST* 1 interfaces you CANNOT continue.

        If you do not have at least 1 *REAL* network interface card(s)
        or one interface with multiple VLANs then pfSense
        *WILL NOT* function correctly.

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection:
```

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

42

pfSense – configurare la LAN

```
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 (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

43

pfSense – configurare la LAN

```
WAN (wan)       -> em0        -> v4/DHCP4: 193.205.92.102/24
LAN (lan)       -> em1        -> v4: 192.168.1.1/24

 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 (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.xxx.1
```

44

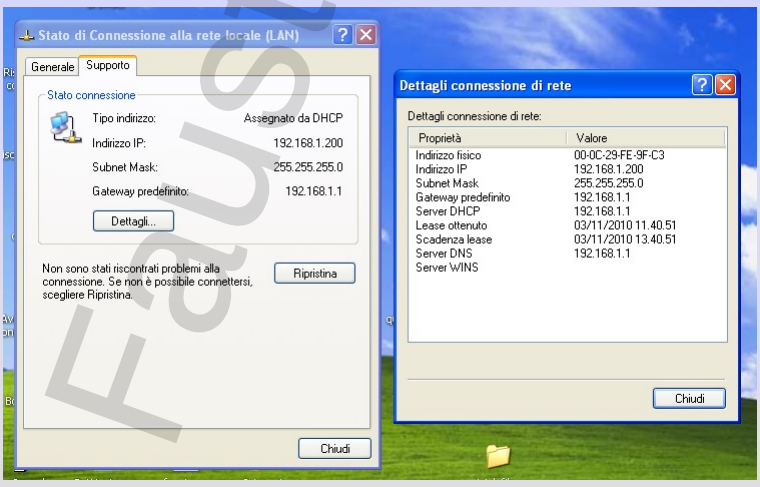
pfSense – configurare la LAN

```
Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.1.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.1.100
Enter the end address of the IPv4 client address range: 192.168.1.200
Disabling IPv6 DHCPD
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

45

Avviare il client

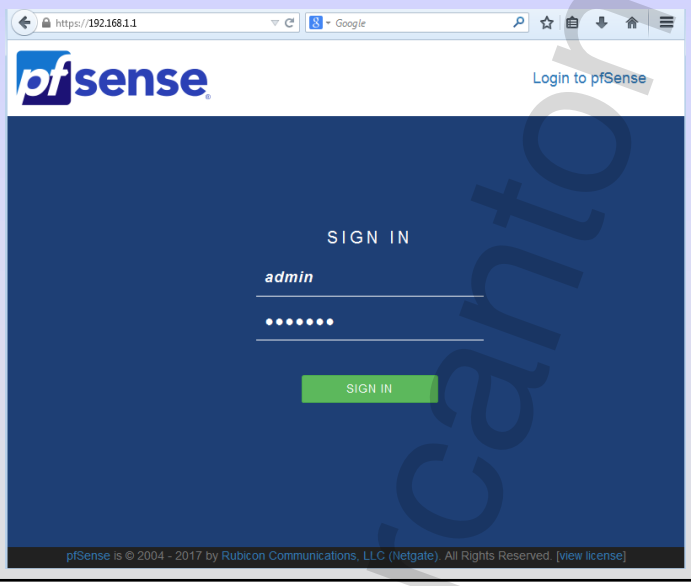
Avviare il sistema sul PC client e controllare gli indirizzi IP



46

pfSense – configurazione - autenticazione

https://192.168.1.1/



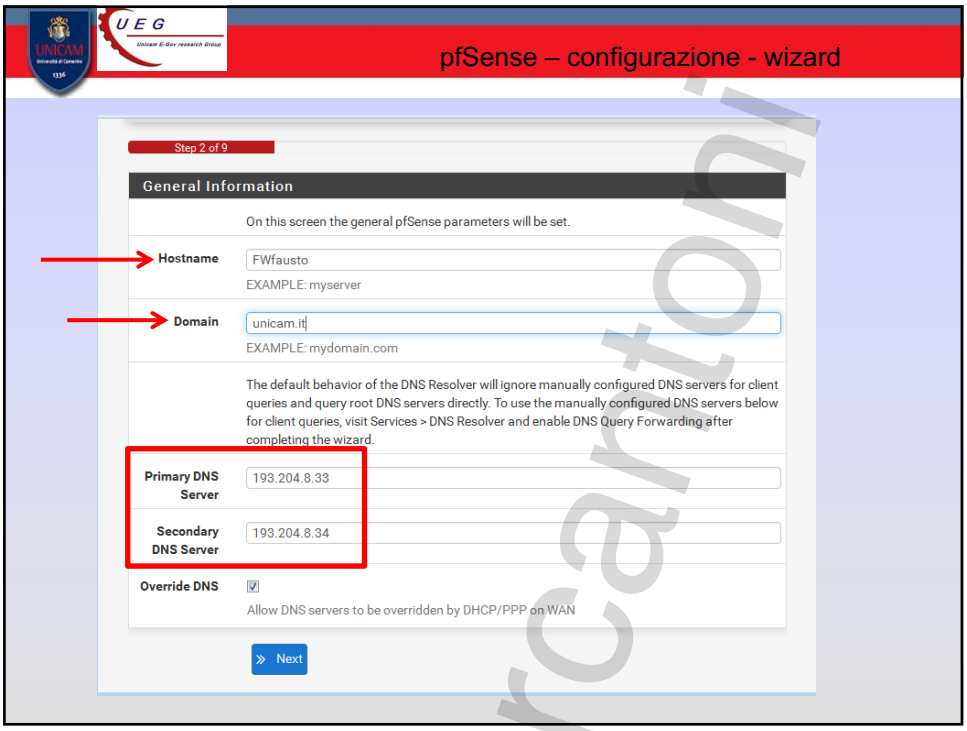
47

pfSense – configurazione – Setup Wizard

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

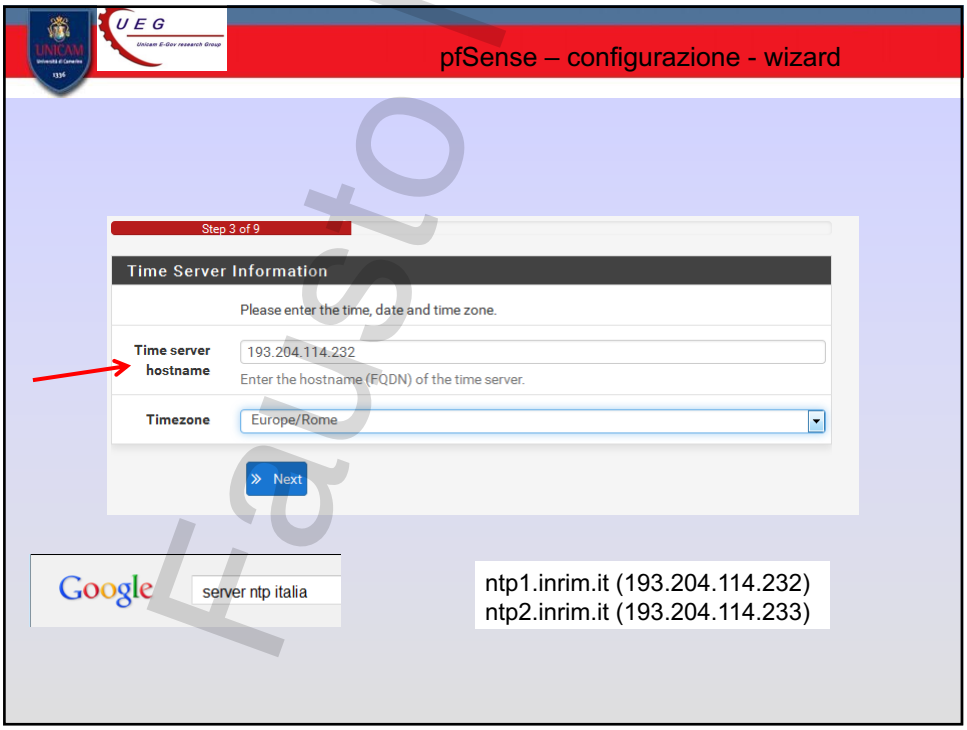
48

pfSense – configurazione - wizard



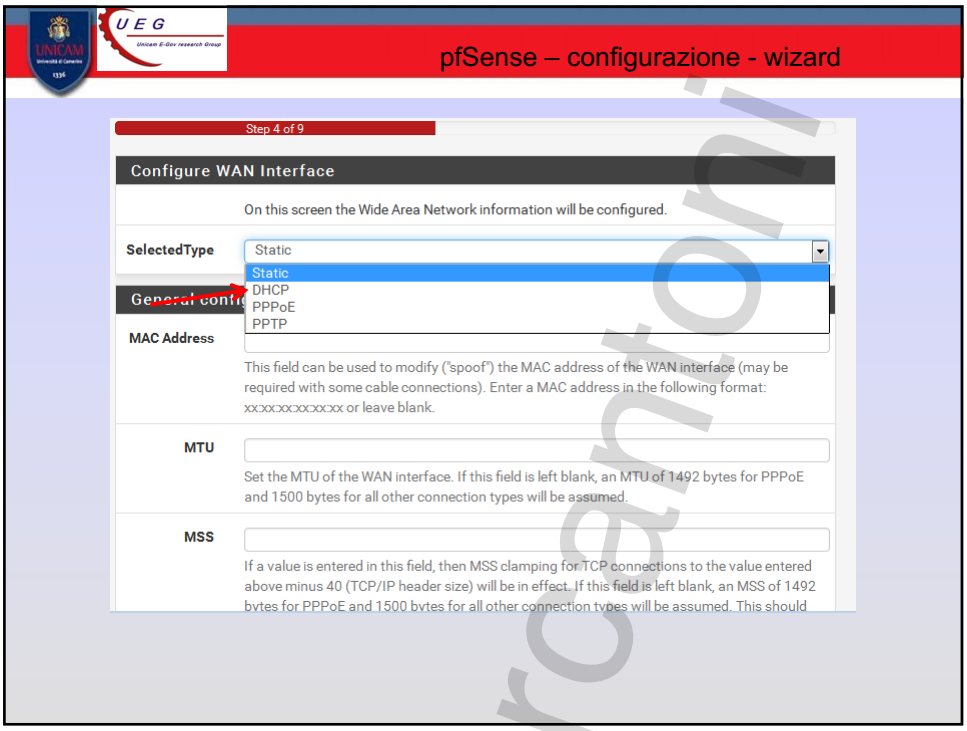
49

pfSense – configurazione - wizard



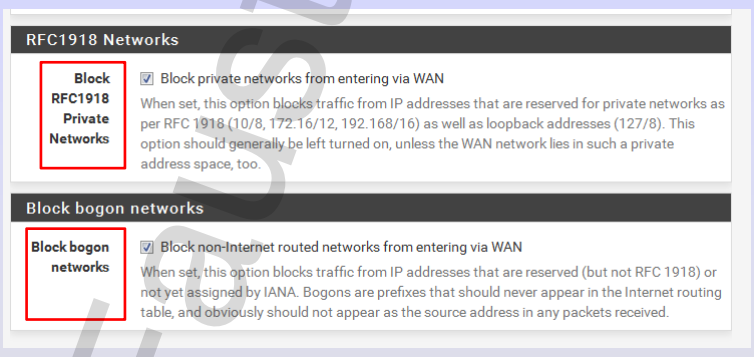
50

pfSense – configurazione - wizard



51

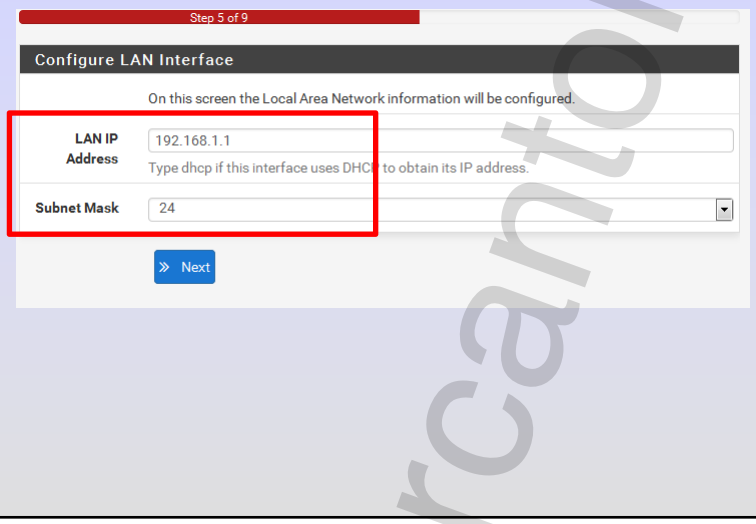
pfSense – configurazione - wizard



https://ipinfo.io/bogon

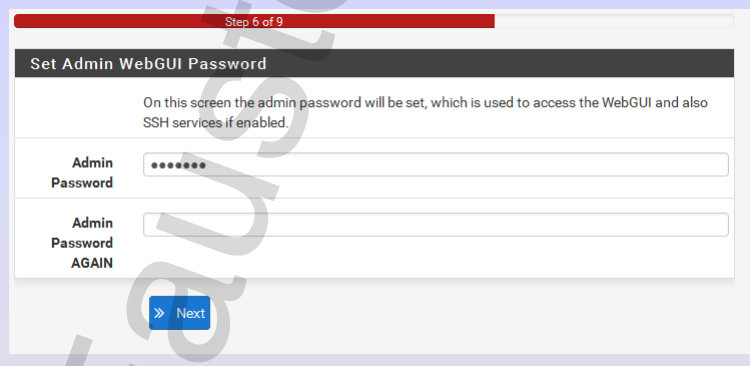
52

pfSense – configurazione - wizard



53

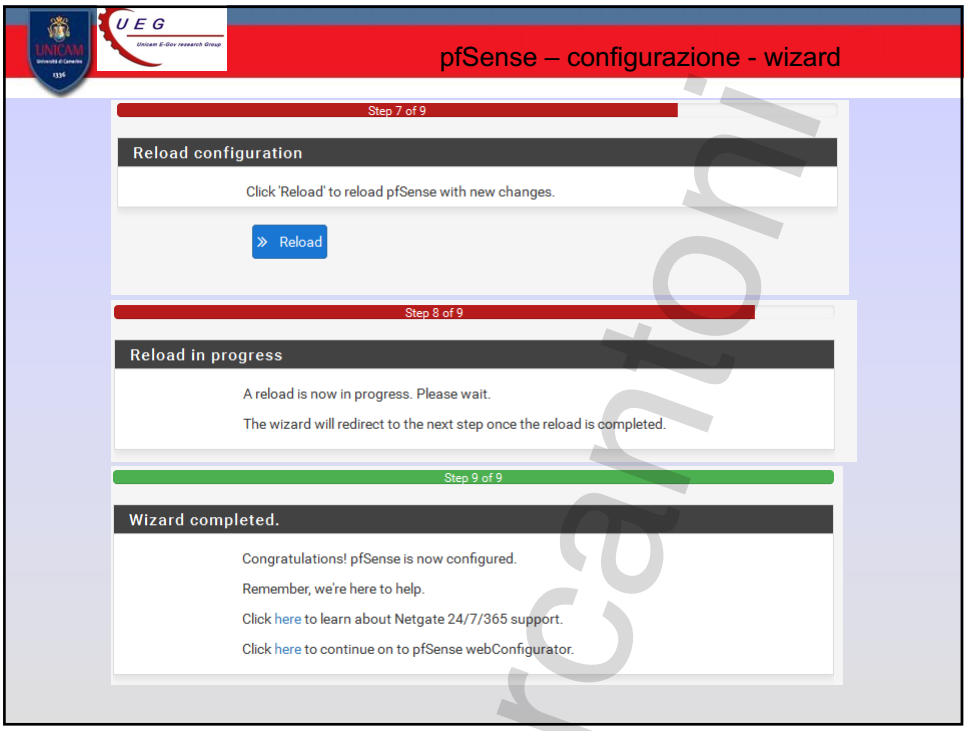
pfSense – configurazione - wizard



default password: pfsense

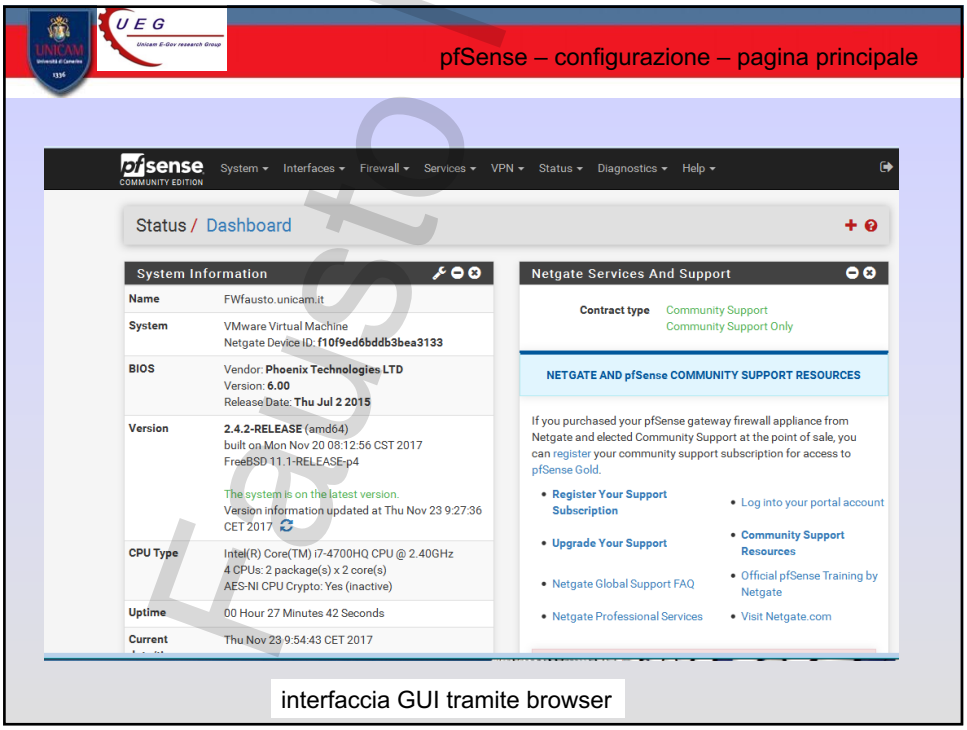
54

pfSense – configurazione - wizard



55

pfSense – configurazione – pagina principale



interfaccia GUI tramite browser

56

pfSense – configurazione - Interfaces

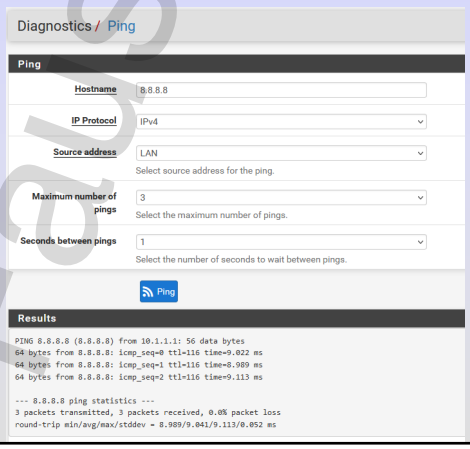
- LAN
  - Configurare l'indirizzo IP del FW e subnet mask
- WAN
  - Tipo di indirizzamento static – dhcp

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

57

Troubleshooting

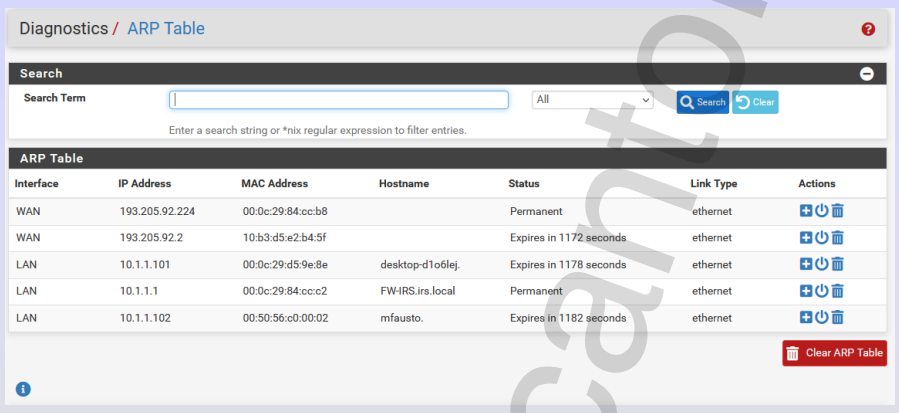
- Localizzazione dei guasti
- Analisi del problema
- Cosa non funzione
- "quello che ***almeno*** funziona"



58

Troubleshooting

Arp table



59

pfSense – configurazione - Services

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.

60

pfSense – configurazione - Services

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.

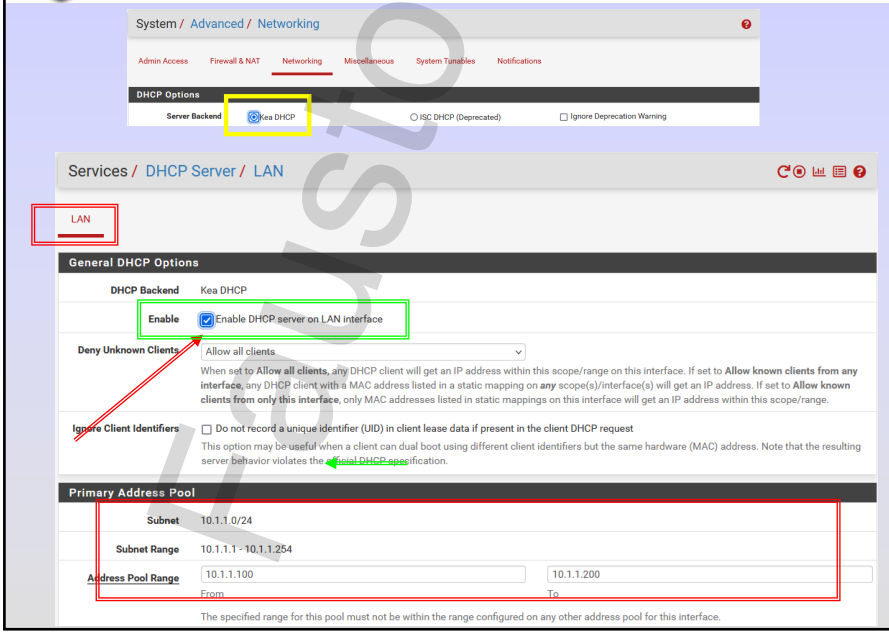
Il Server DHCP è il calcolatore che assegna gli indirizzi IP, e anche il processo che svolge questa funzione. Talvolta questa funzione è incorporata in un router.

Il DHCP relay è 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

61

pfSense – configurazione - DHCP Server



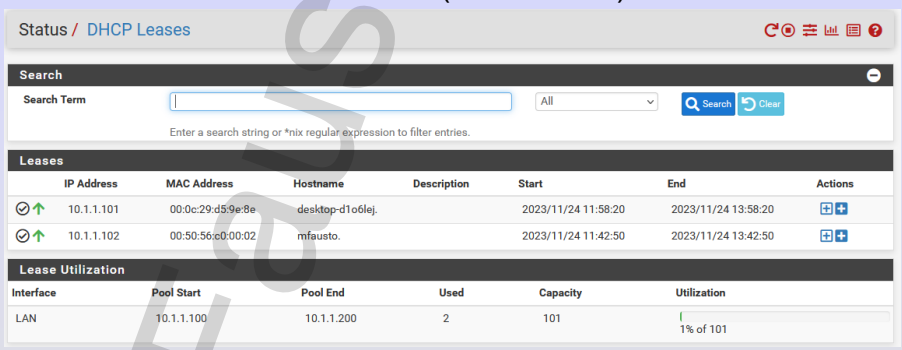
62

pfSense – configurazione - DHCP Server

63

pfSense – diagnostica - DHCP Lease

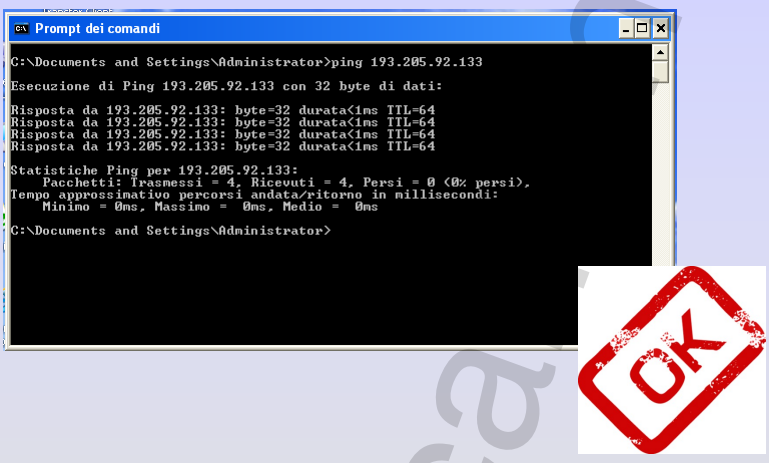
DHCP lease
lease = prendere in affitto
durata di validità (Lease Time)



64

Troubleshooting

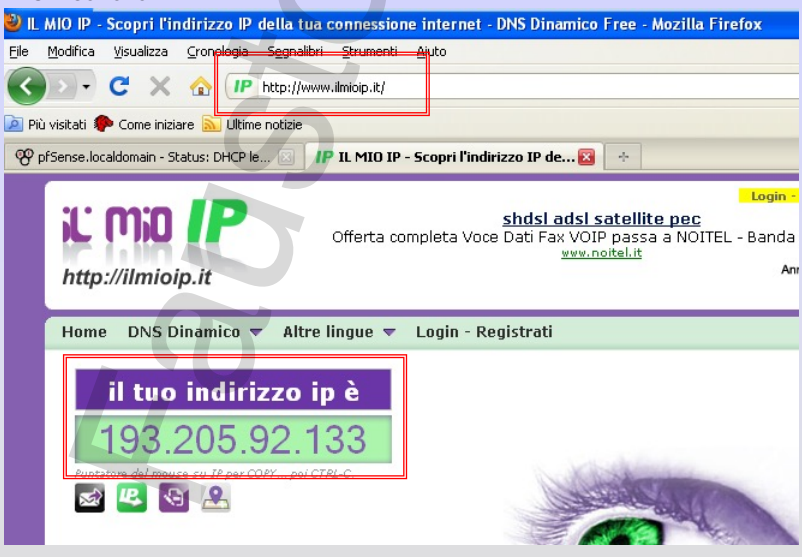
Dalla LAN provare a fare ping sull'indirizzo WAN del firewall



65

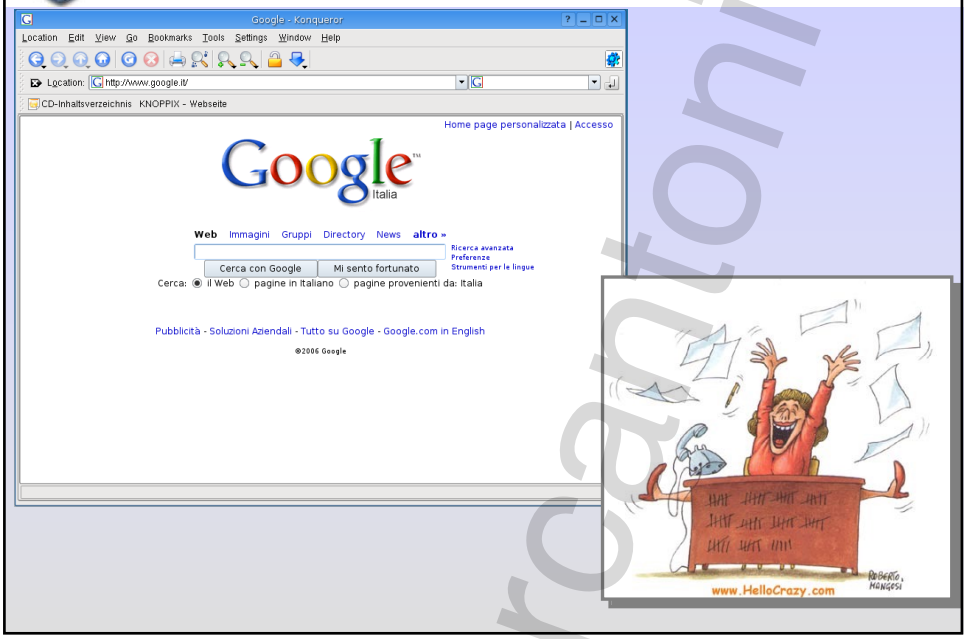
NAT – Network Address Translation

Chi sono io???



66

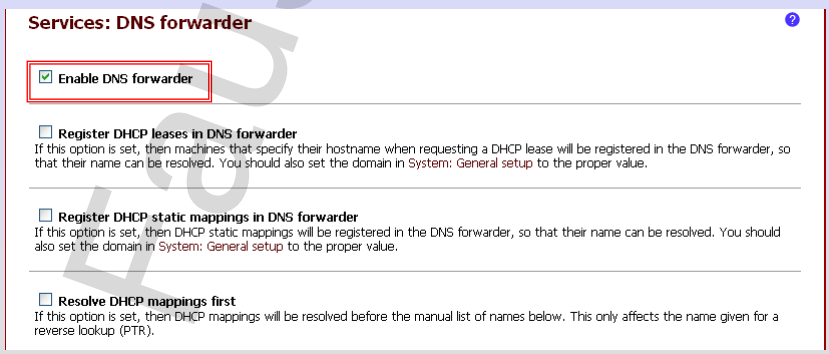
Tutto funziona – wow si naviga



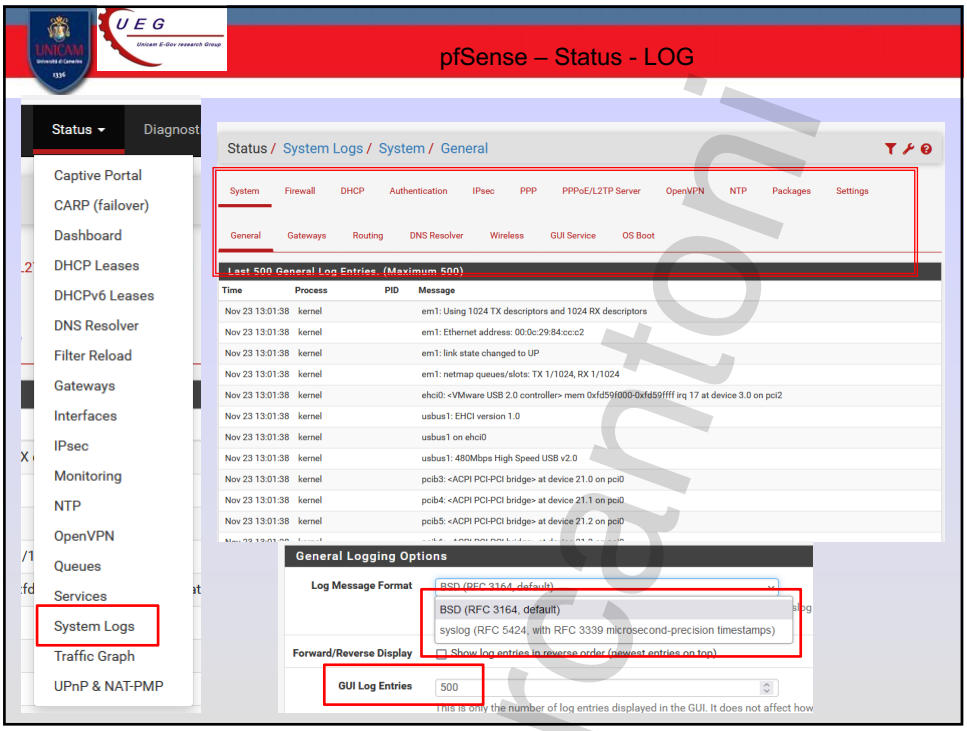
67

pfSense – Servizi - DNS Forwarder

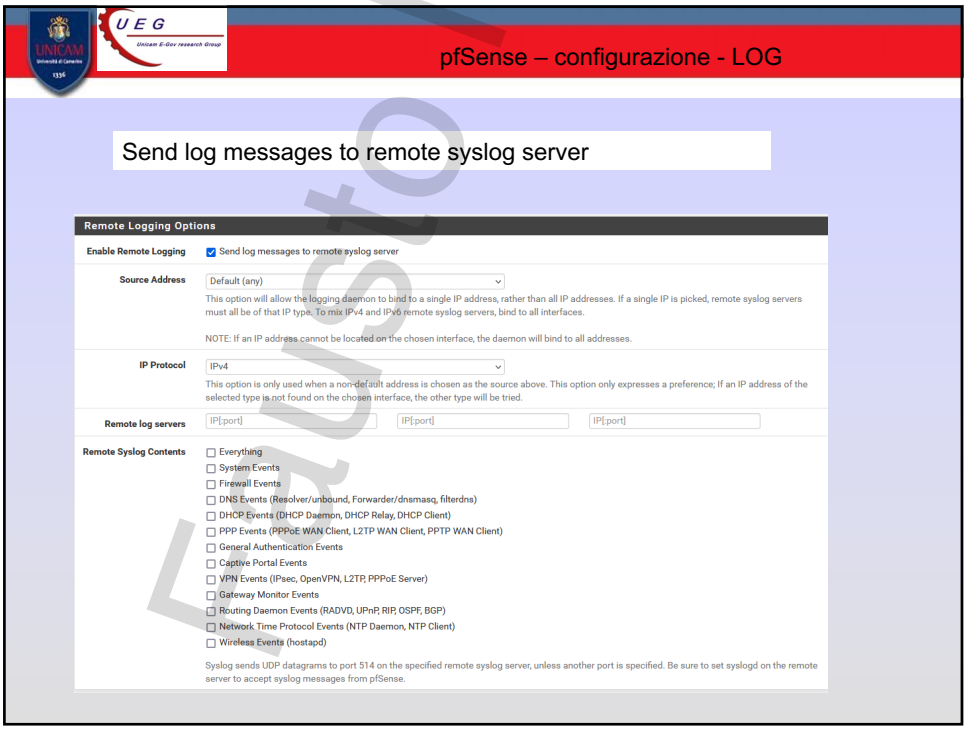
- DNS forwarder
  - Usando il server DNS del vostro provider come "forwarder" farete in modo che le risposte alle vostre richieste siano più veloci e meno pesanti per la vostra rete.
  - Questo si ottiene facendo in modo che il vostro **name server** inoltri le richieste al **name server** del vostro 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.



68



69



70

pfSense – configurazione - Captive portal

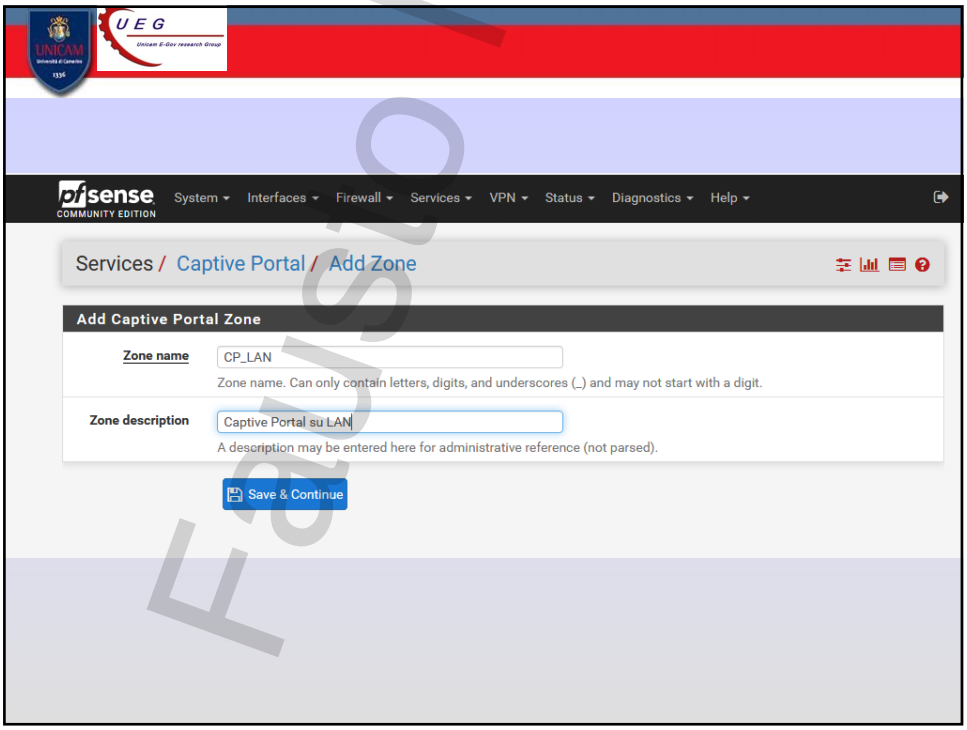
La tecnica del **CAPTIVE PORTAL** forza un client del servizio HTTP su una rete di collegarsi ad una Web page speciale (solitamente per gli scopi di autenticazione) prima di navigare in Internet normalmente.

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

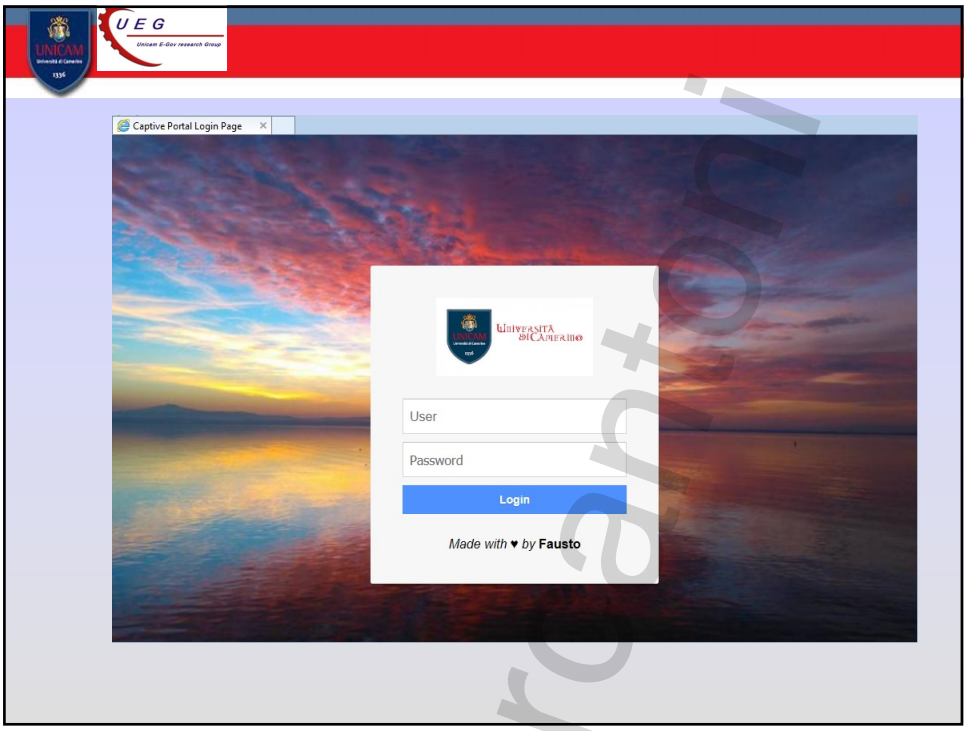
I Captive Portal si usano nella maggior parte dei hotspots Wi-Fi.

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

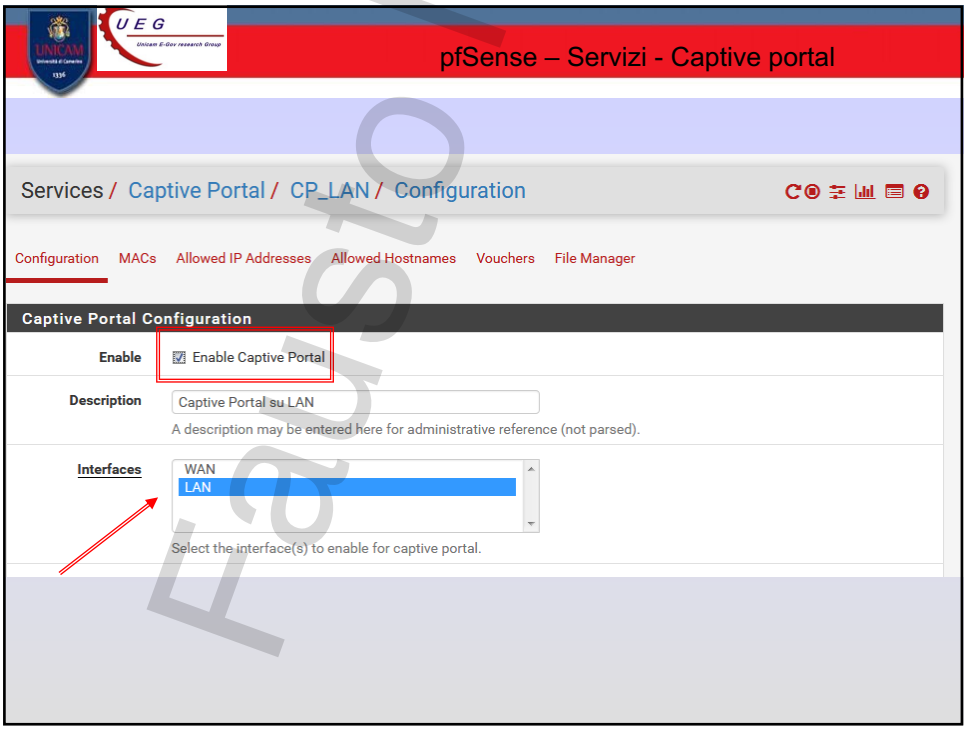
71



72

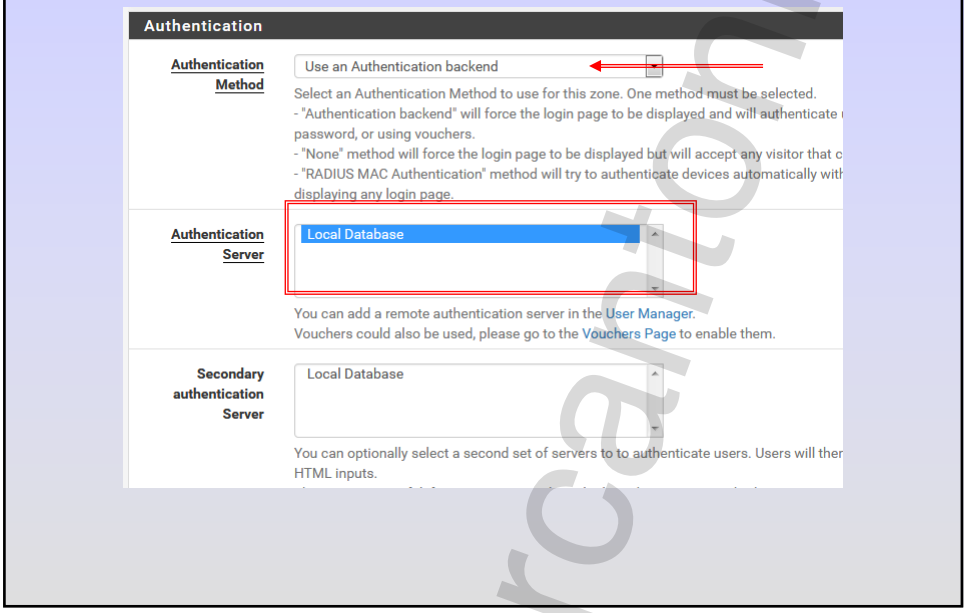


73



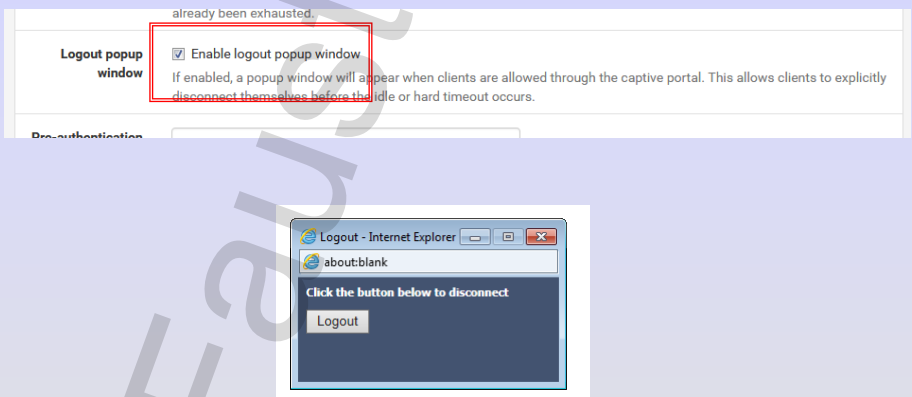
74

pfSense – Servizi - Captive portal



75

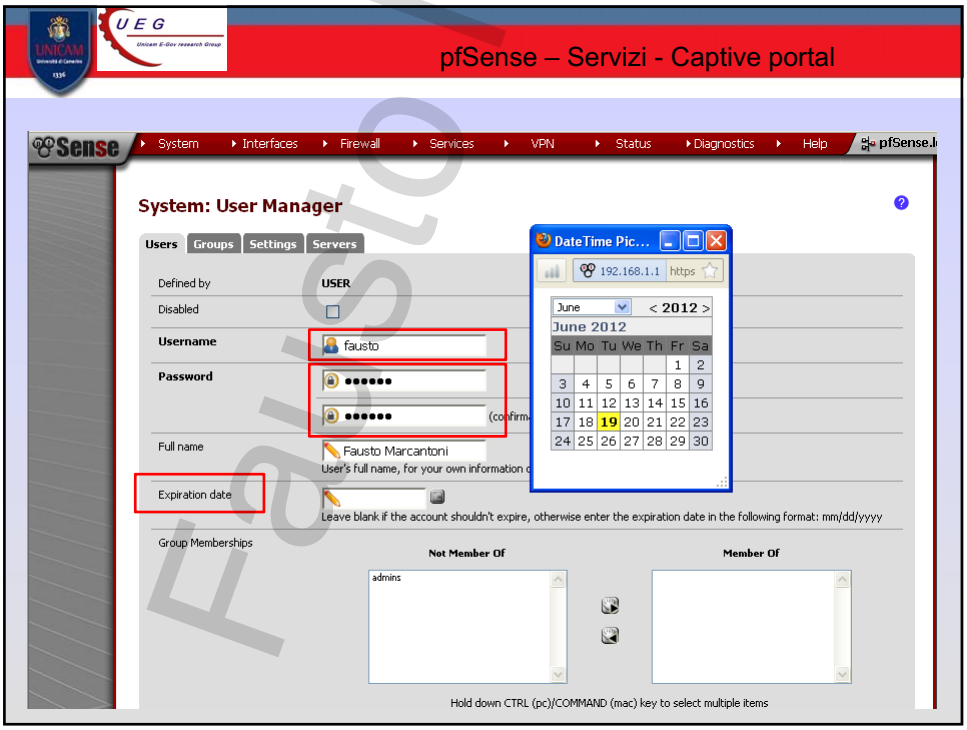
pfSense – Servizi - Captive portal



abilitare i pop-up sul browser

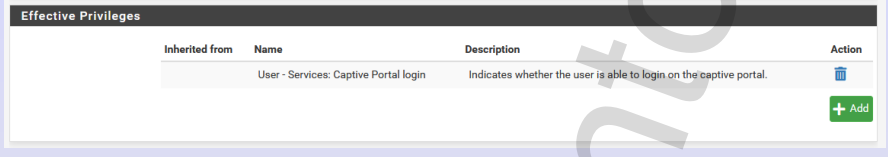
76

77



78

Abilitare l'utente ad utilizzare il Captive Portal

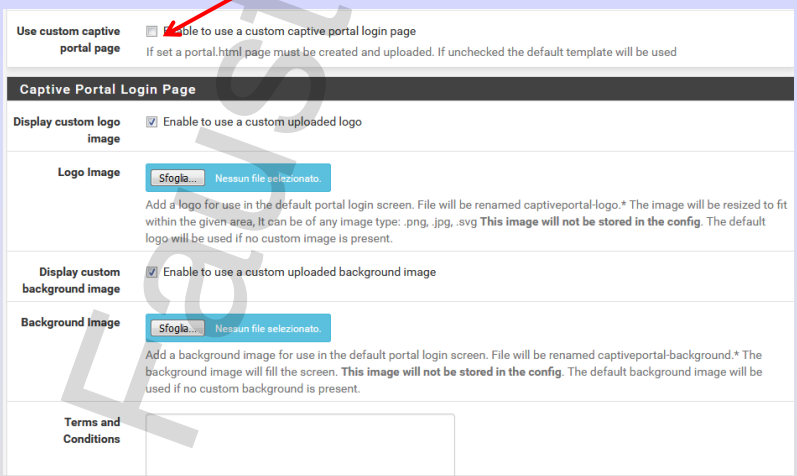


User - Services: Captive Portal login
Indicates whether the user is able to login on the captive portal.

79

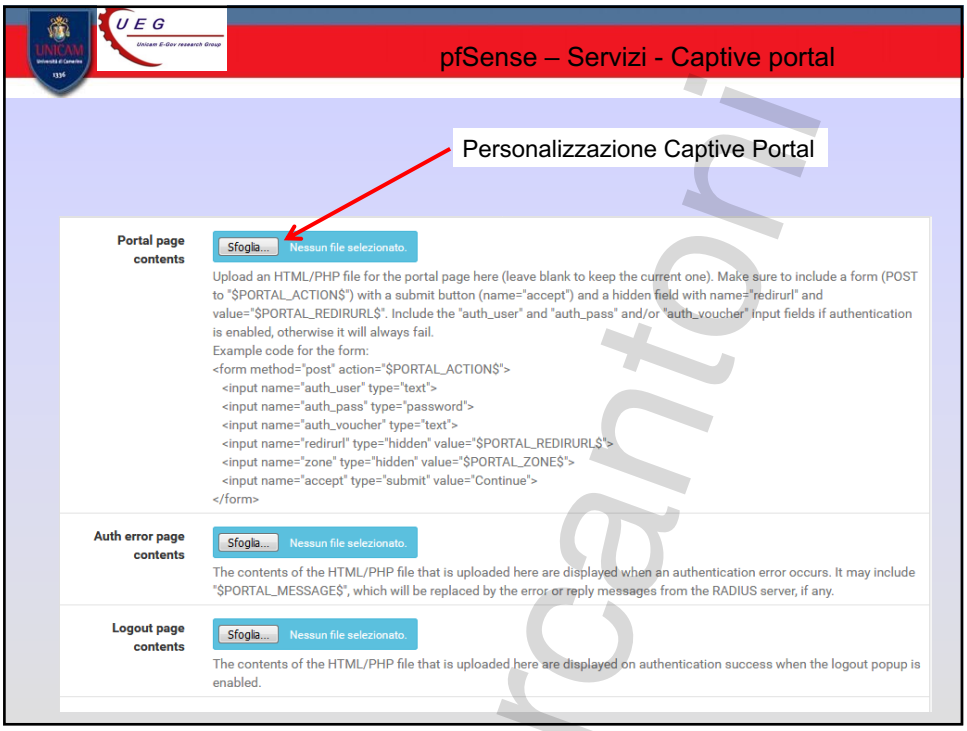
pfSense – Servizi - Captive portal

Personalizzazione Captive Portal



80

pfSense – Servizi - Captive portal



81

pfSense– configurazione - Captive portal

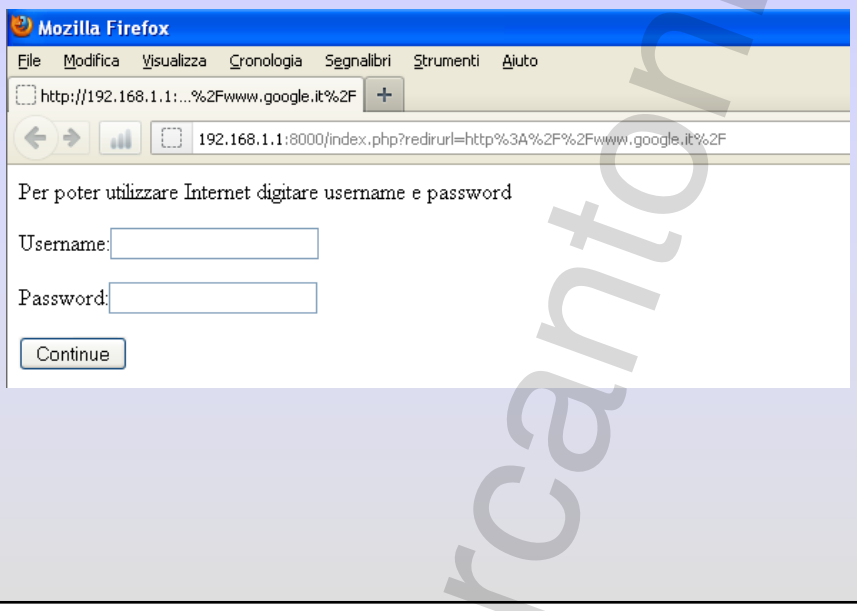
Esempio di pagina " CAPRTIVE PORTAL"

```
<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

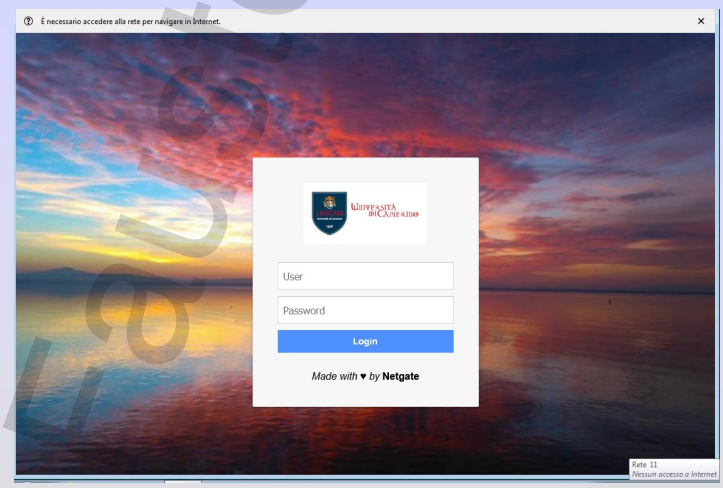
82

pfSense – configurazione - Captive portal

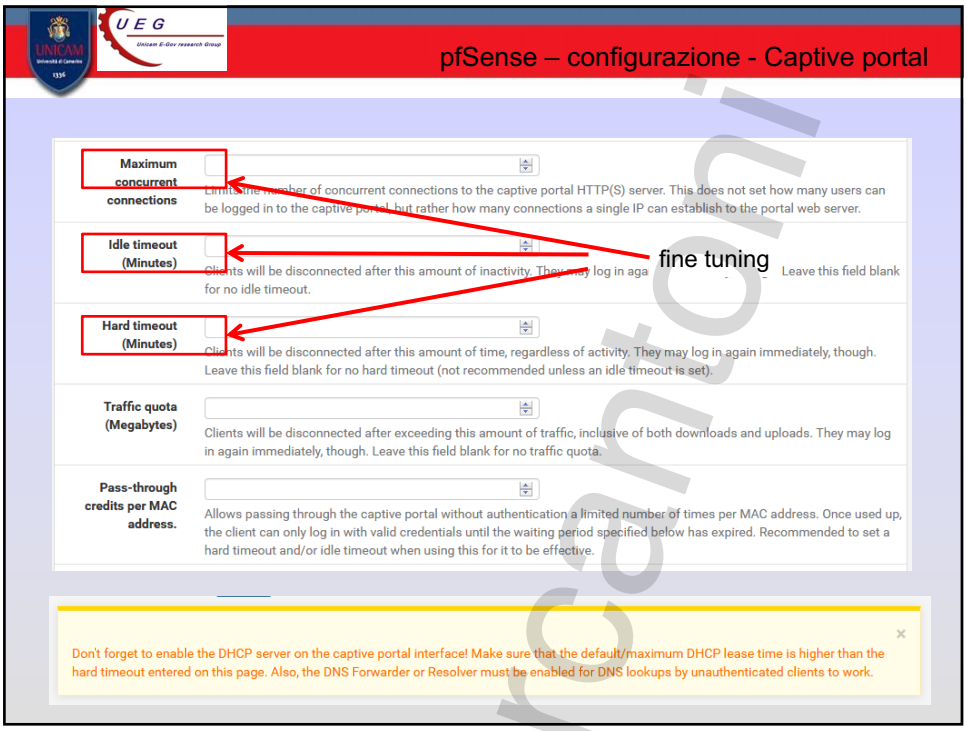


83

pfSense – configurazione - Captive portal



84

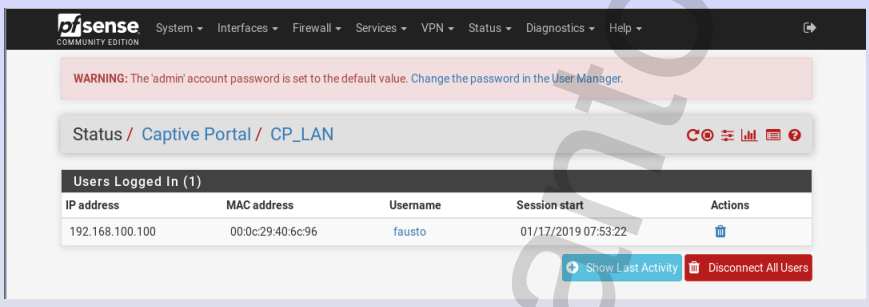


85

86

pfSense – configurazione - Captive portal

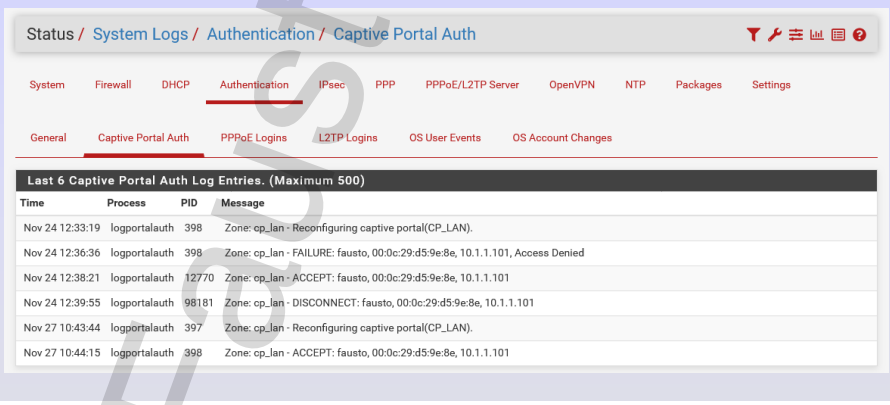
I log di captive portal



87

System LogsAuthenticationCaptive Portal Auth

System Logs →Authentication →Captive Portal Auth

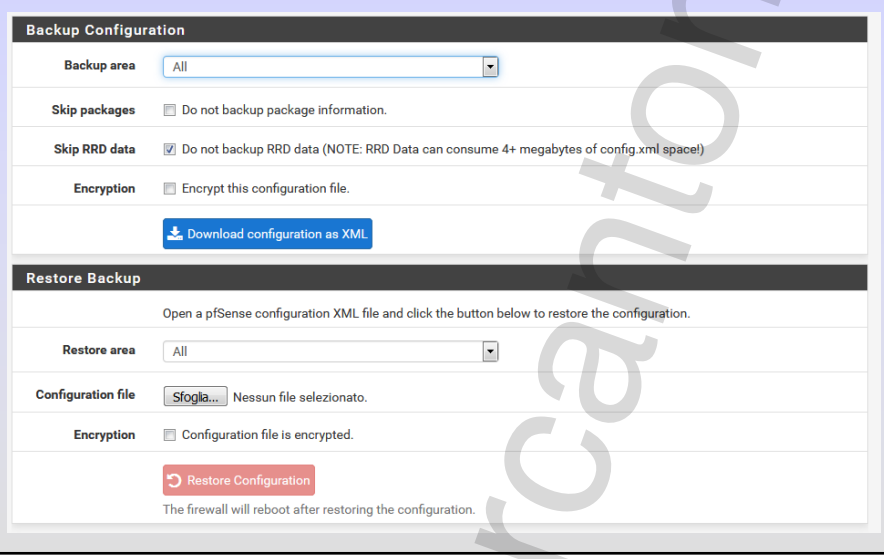


Nov 27 10:44:15 logportalauth 398 Zone: cp_lan - ACCEPT: fausto, 00:0c:29:d5:9e:8e, 10.1.1.101

88

pfSense – backup configurazione -

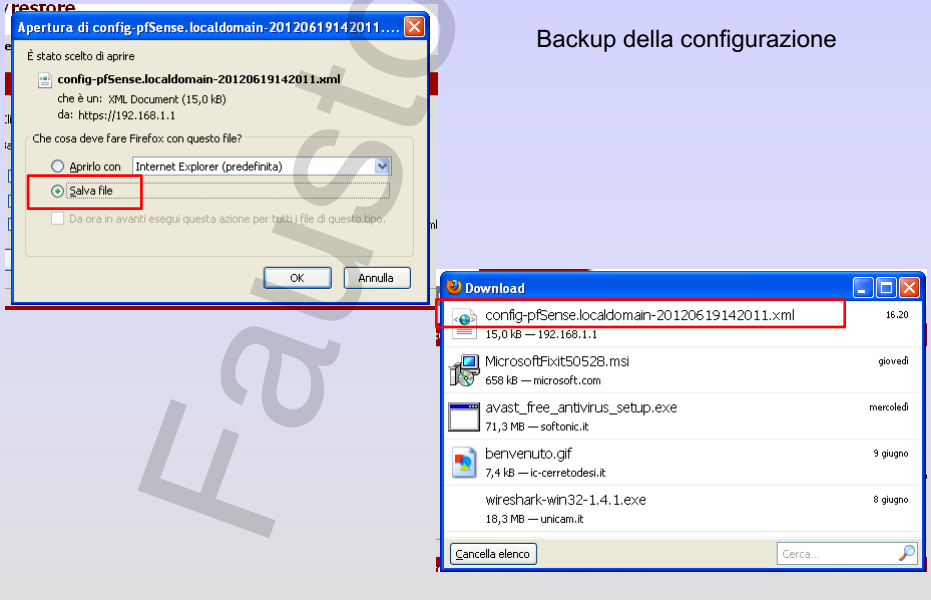
Backup della configurazione



89

pfSense – backup configurazione -

Backup della configurazione



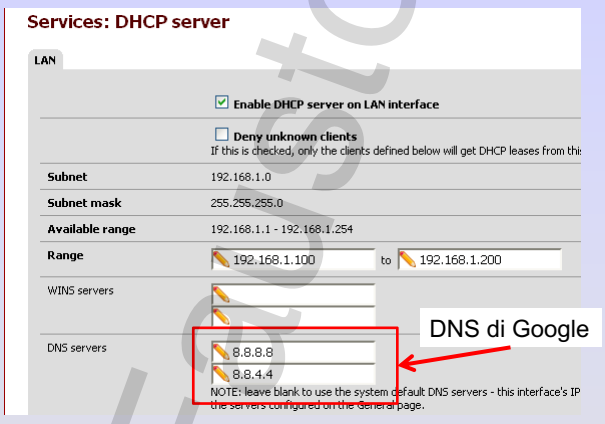
90

pfSense – backup configurazione -

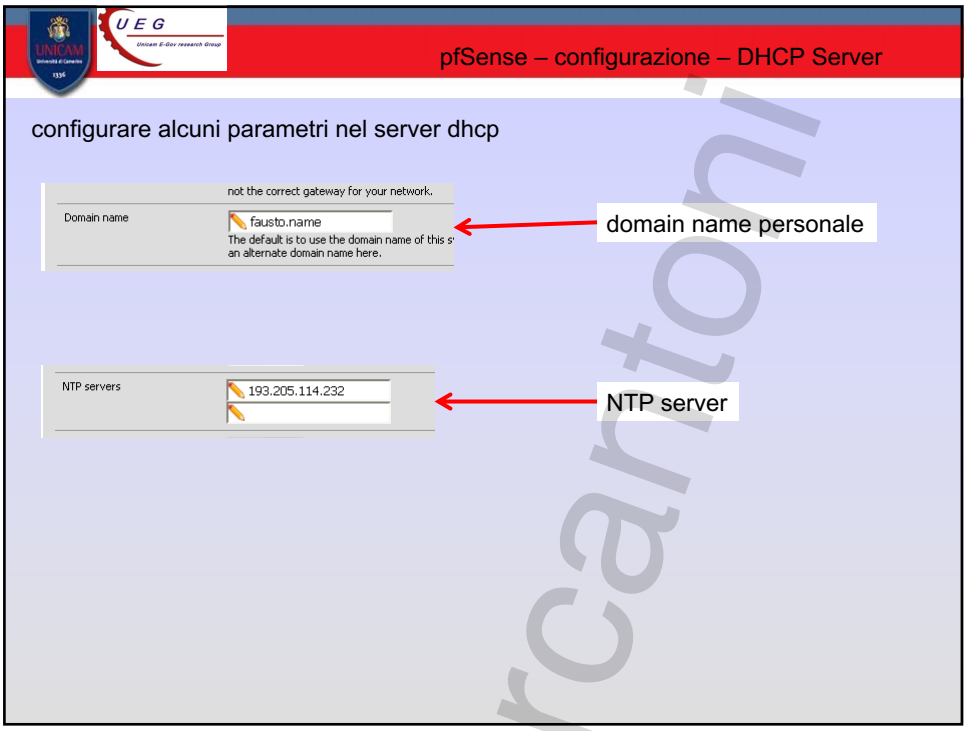
91

pfSense – configurazione – DHCP Server

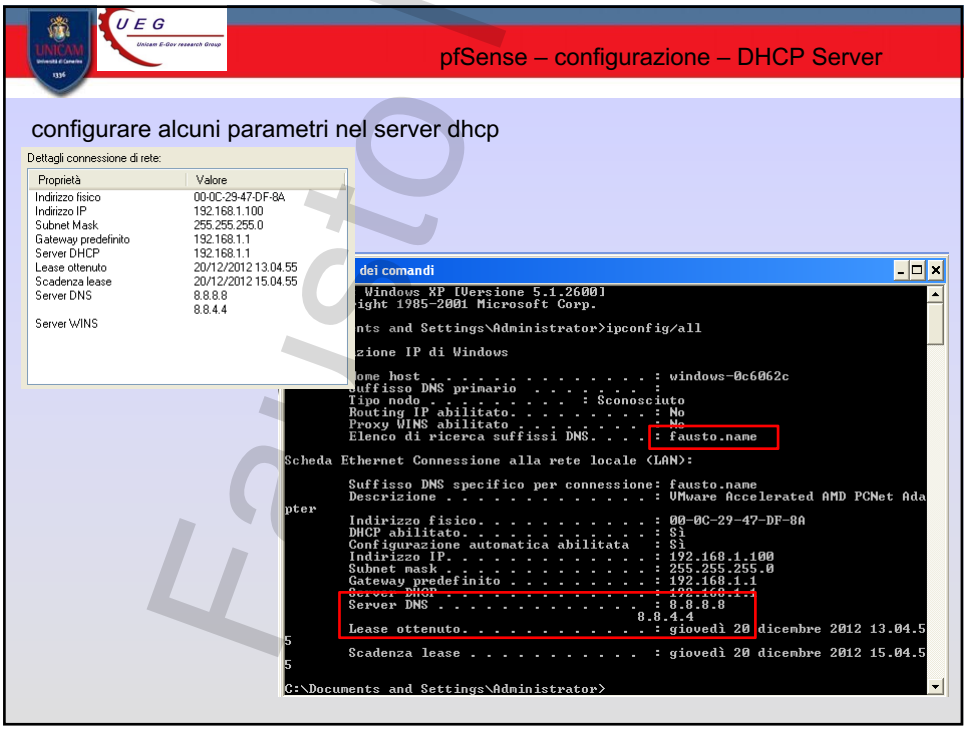
configurare alcuni parametri nel server dhcp



92

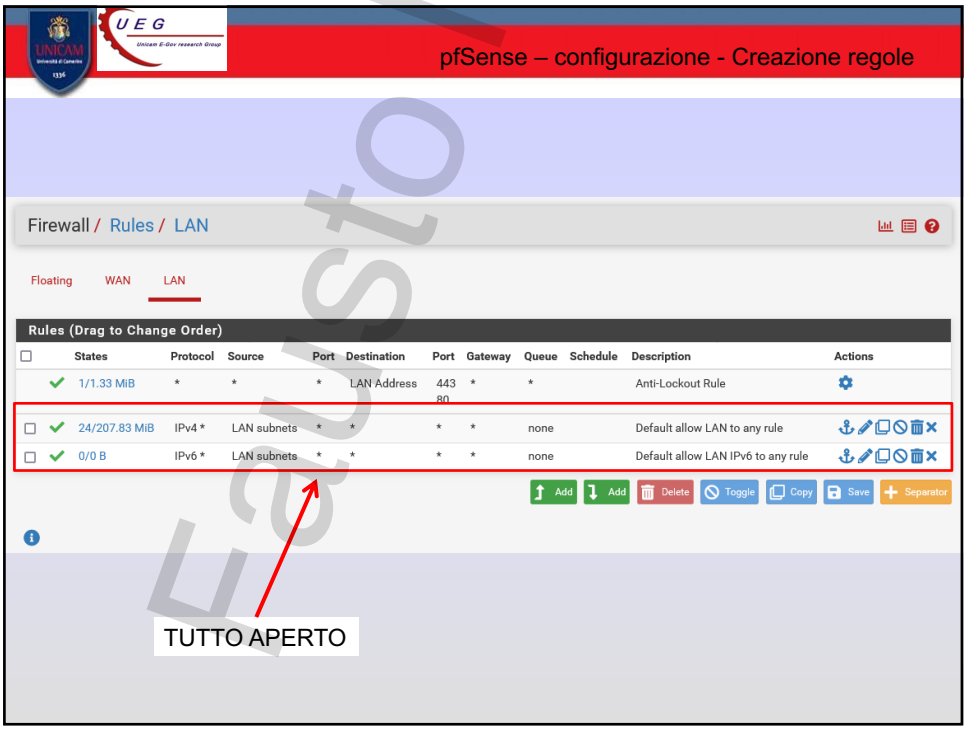


93



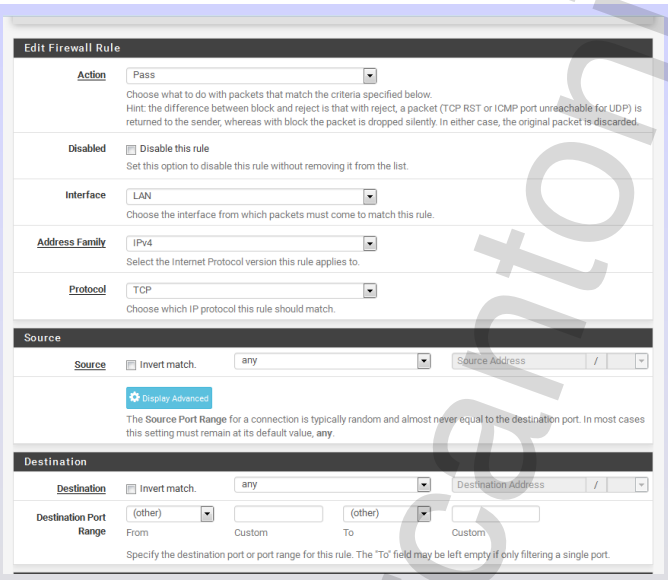
94

95



96

pfSense – configurazione - Creazione regole



Configurare una regola …

97

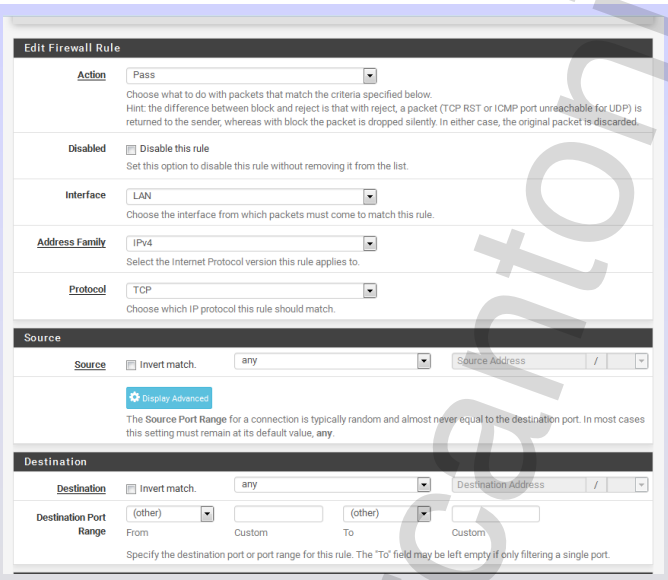
I firewalls mettono a disposizione tre opzioni per il controllo del traffico:

- **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/

98

pfSense – configurazione - Creazione regole

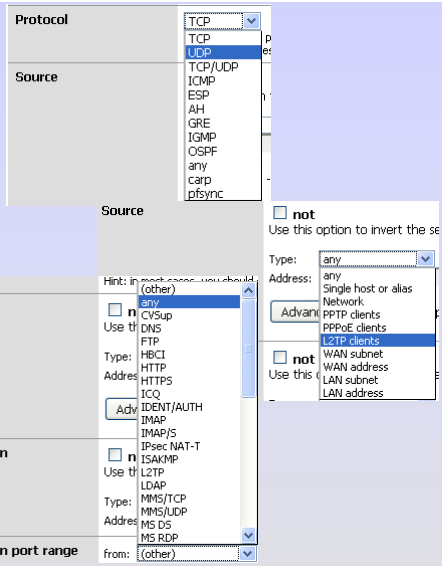


Configurare una regola …

99

pfSense – configurazione - Creazione regole

… Configurare una regola …



Attenzione

Ricorda:
Un firewall si progetta

100

pfSense – configurazione - Creazione regole

… Configurare una regola …

Mettere descrizioni facili da ricordare e intuitive

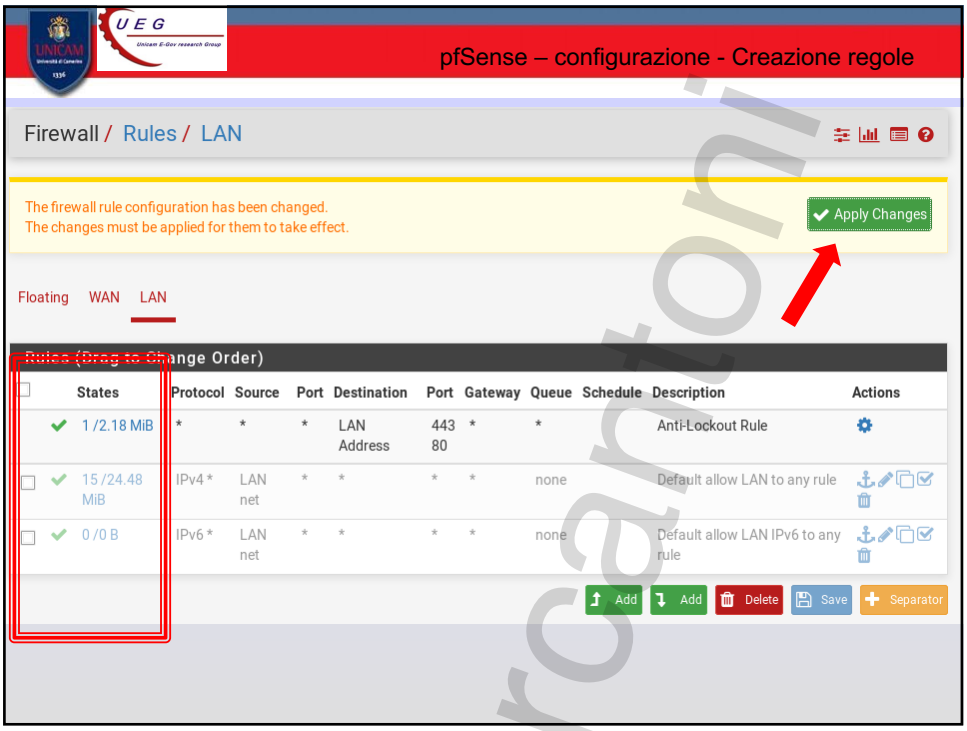
101

pfSense – configurazione - Creazione regole

Ricorda:
Un firewall si progetta

CHIUDIAMO TUTTO …

102



103

104

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
…

105

pfSense – configurazione - Creazione regole

Firewall / Rules / LAN

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0 /11.71 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✓	0 /3 KiB	IPv4 ICMP any	*	*	*	*	*	none		Passa ICMP	
✓	0 /0 B	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		Passa DNS	
✓	0 /0 B	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none		Passa HTTPS	
✓	0 /0 B	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none		Passa HTTP	
✓	0 /0 B	IPv4 TCP	*	*	*	22 (SSH)	*	none		Passa SSH	
✓	0 /0 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	

Add Add Delete Save Separator

106

pfSense– configurazione – Firewall States

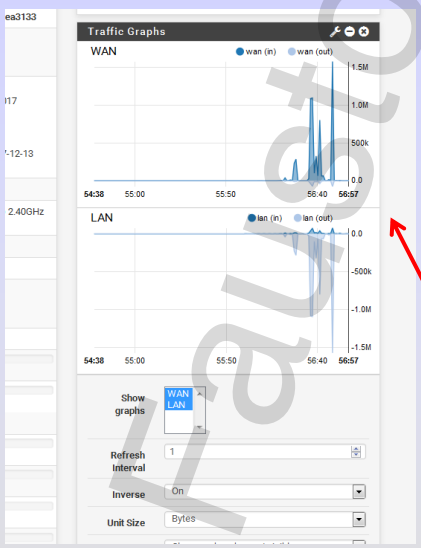
States

Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes
LAN	tcp	192.168.1.100:49537 -> 192.168.1.1:443	FIN_WAIT_2:FIN_WAIT_2	94 / 179	22 KiB / 148 KiB
LAN	tcp	192.168.1.100:49538 -> 192.168.1.1:443	FIN_WAIT_2:FIN_WAIT_2	46 / 47	8 KiB / 5 KiB
LAN	tcp	192.168.1.100:49540 -> 192.168.1.1:443	FIN_WAIT_2:FIN_WAIT_2	39 / 40	6 KiB / 4 KiB
LAN	udp	192.168.1.101:48421 -> 192.168.1.1:53	SINGLE:MULTIPLE	2 / 2	134 B / 182 B
LAN	tcp	192.168.1.100:49541 -> 192.168.1.1:443	ESTABLISHED:ESTABLISHED	5 / 5	945 B / 362 B
WAN	tcp	193.205.92.124:44670 (192.168.1.101:40918) -> 213.254.15.248:80	ESTABLISHED:ESTABLISHED	2 / 3	112 B / 180 B
WAN	icmp	193.205.92.124:26619 -> 193.205.92.2:26619	0:0	5.818 K / 5.818 K	159 KiB / 159 KiB
WAN	udp	193.205.92.124:123 -> 193.204.114.232:123	MULTIPLE:MULTIPLE	2 / 2	152 B / 152 B
WAN	udp	193.205.92.124:51984 -> 193.204.8.33:53	MULTIPLE:SINGLE	1 / 1	67 B / 115 B
WAN	udp	193.205.92.124:51984 -> 193.204.8.34:53	MULTIPLE:SINGLE	1 / 1	67 B / 115 B

Controllare le sessioni e lo stato del firewall

107

pfSense – Status – Traffic Graph



traffico e banda utilizzata

108

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		

109

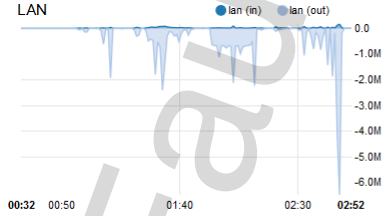
pfSense – Status – Graphs

Status / Traffic Graph

Graph Settings

LAN	Bandwidth In	Local	IP Address	Clear graphs w
Interface	Sort by	Filter	Display	Background updates

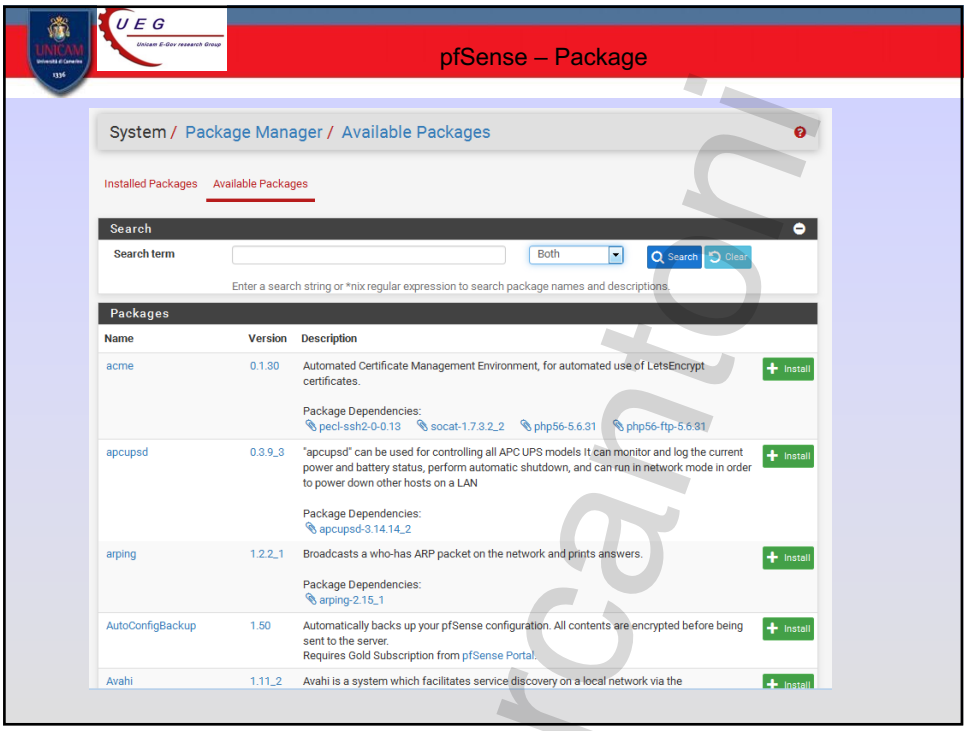
Traffic Graph



Host IP	Bandwidth In	Bandwidth Out
192.168.1.100	25.97k Bits/sec	106.70k Bits/sec
192.168.1.101	2.49k Bits/sec	2.49k Bits/sec

110

pfSense – Package



111

pfSense – Package - squid proxy

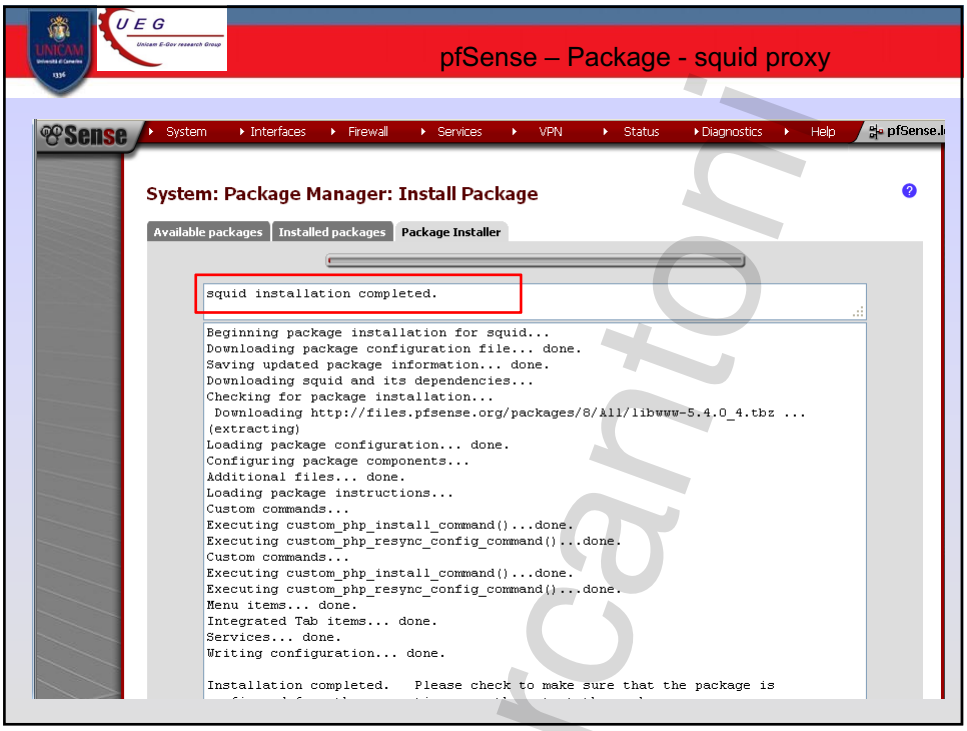
SQUID

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

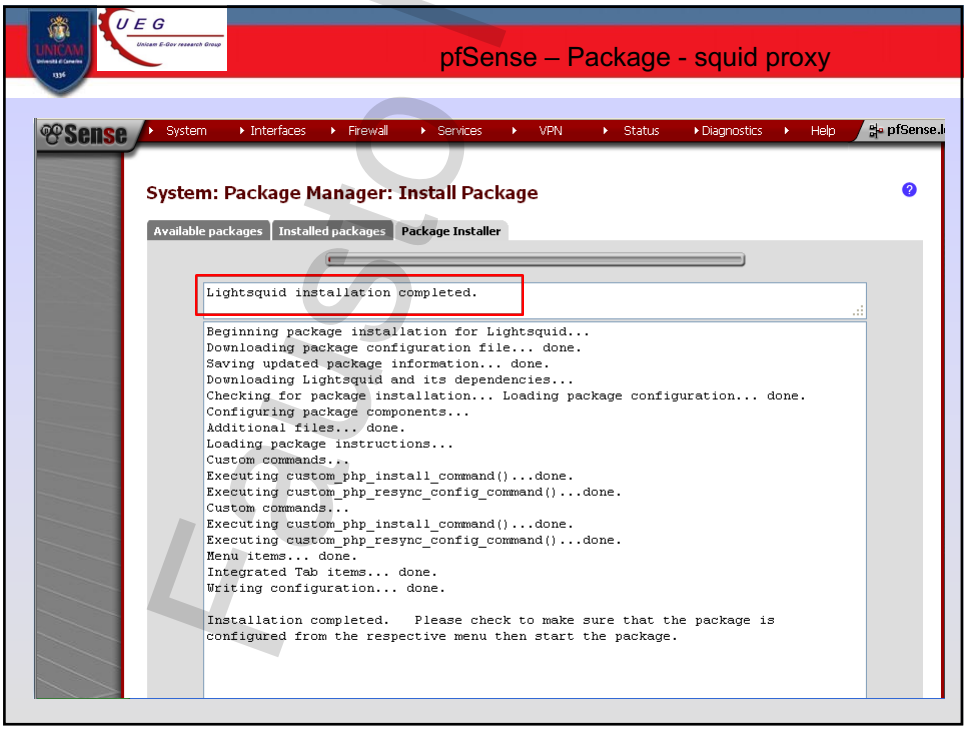
Packages

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	Install
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	Install
squidGuard	1.16.19	High performance web proxy URL filter. Package Dependencies: squidguard-1.4_15 pfSense-pkg-squid-0.4.46	Install

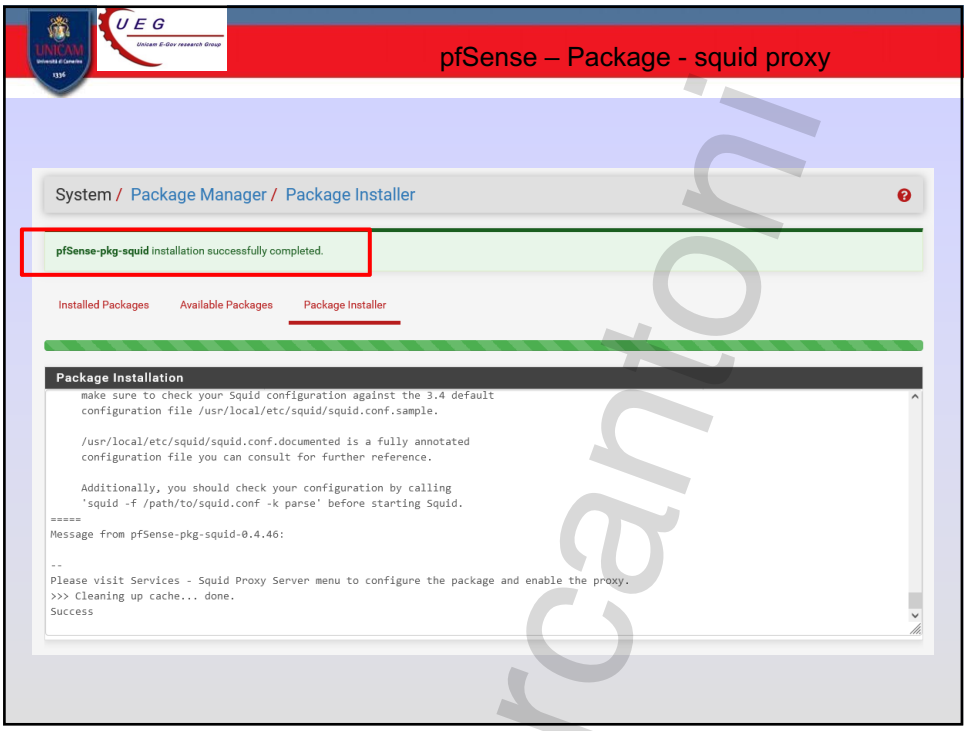
112



113



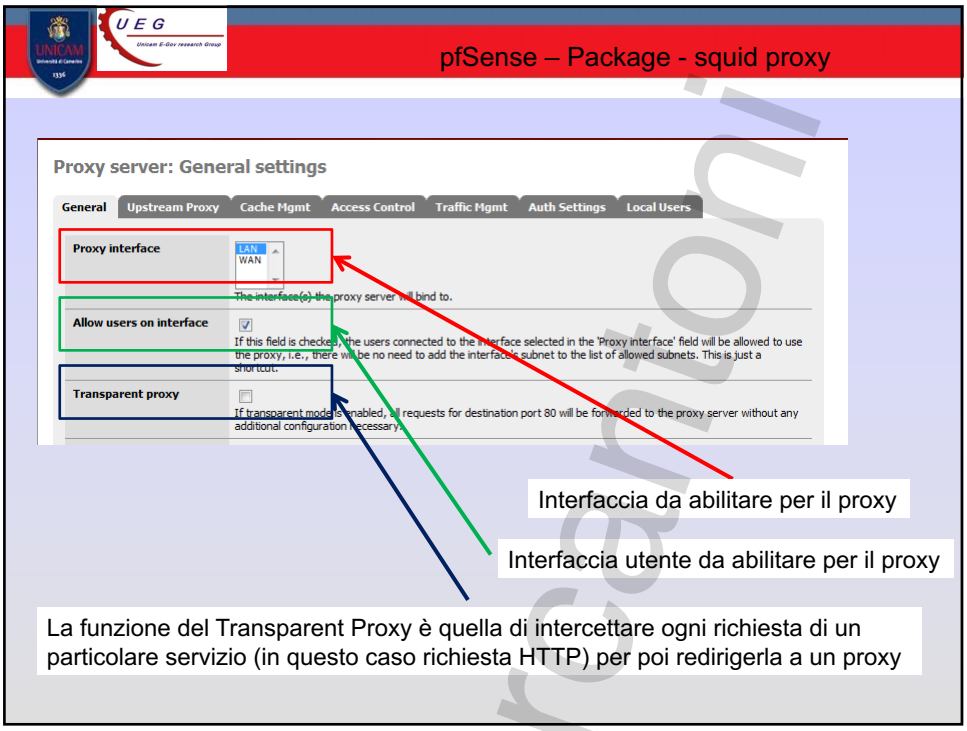
114



115

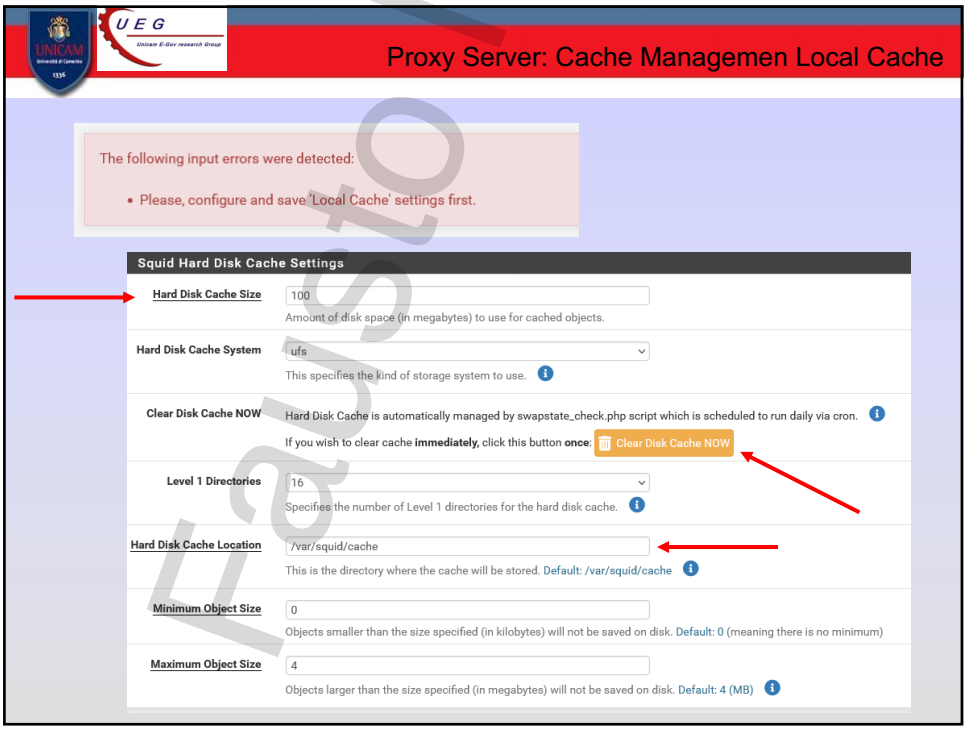
116

pfSense – Package - squid proxy

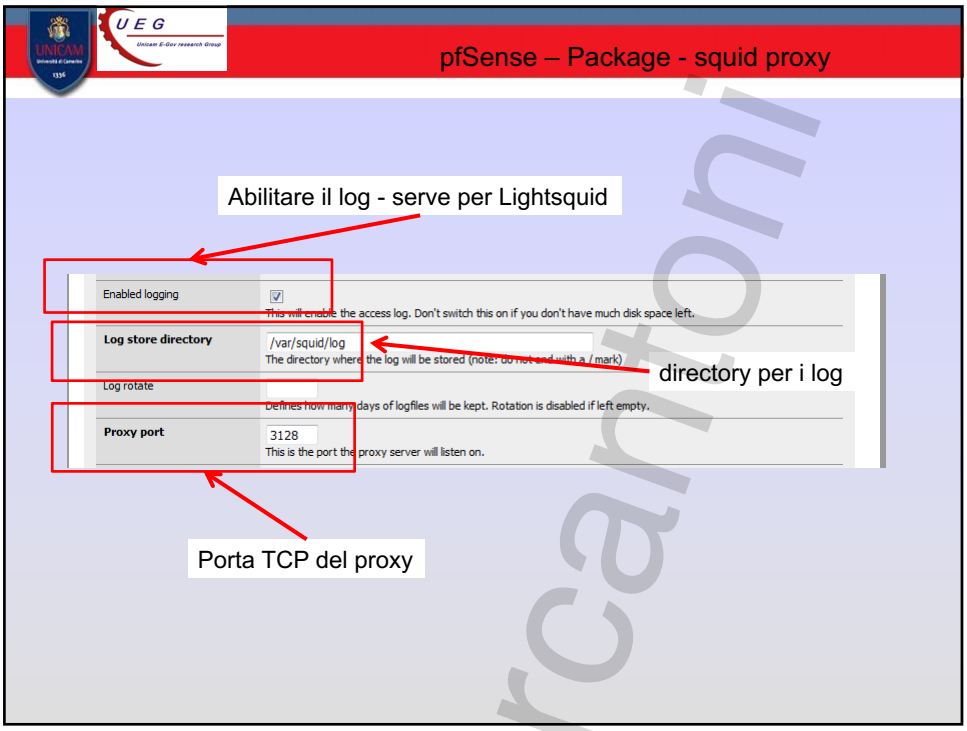


117

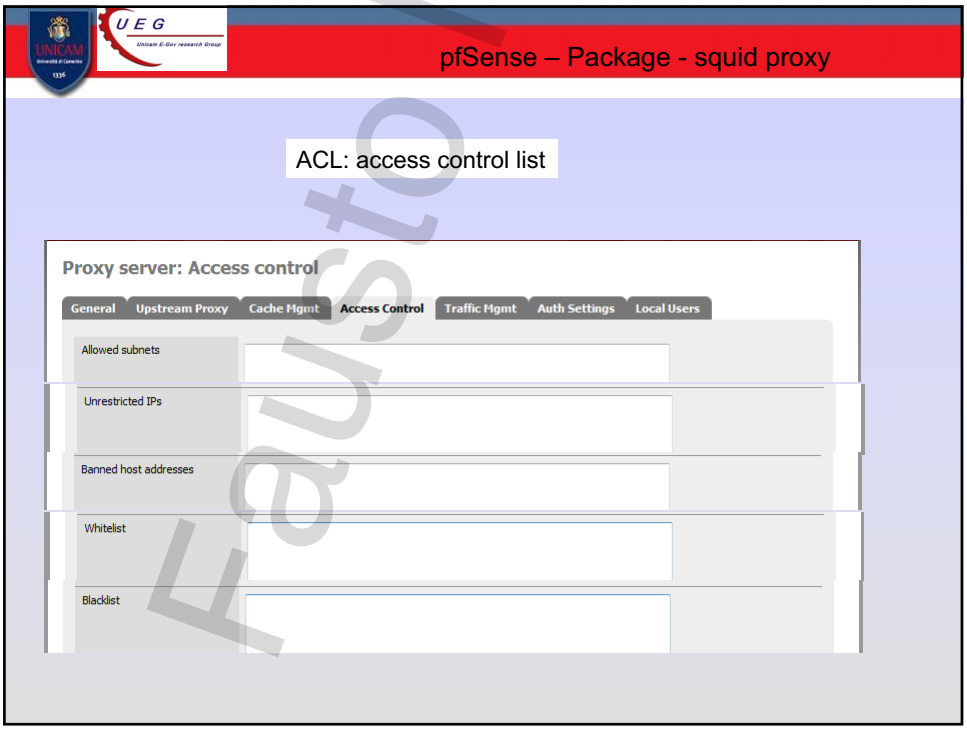
Proxy Server: Cache Managemen Local Cache



118



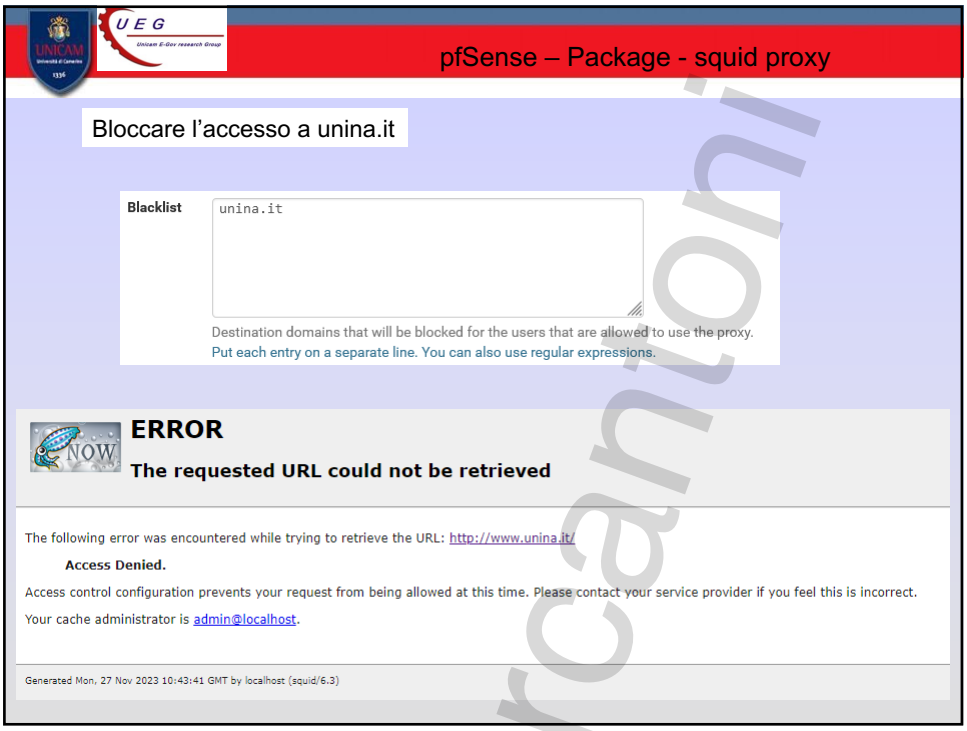
119



120

pfSense – Package - squid proxy

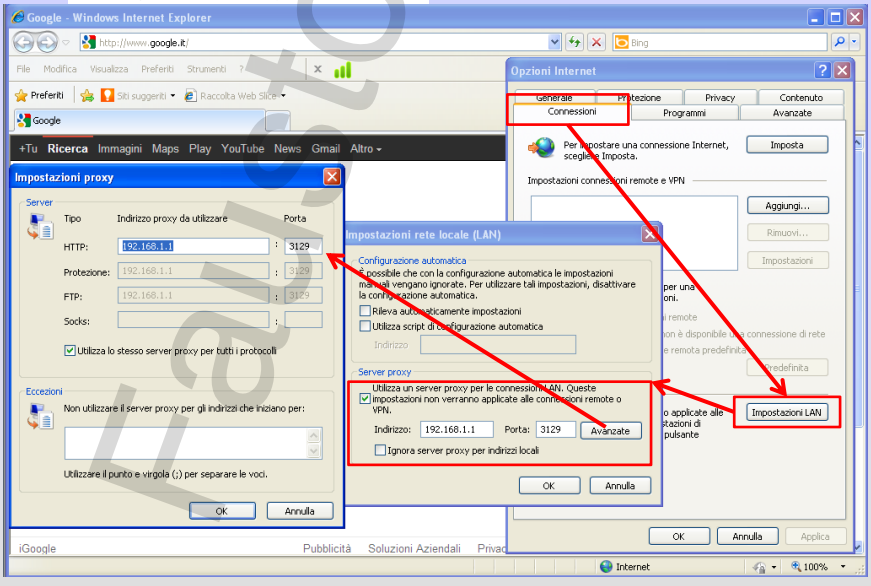
Bloccare l'accesso a unina.it



121

pfSense – Package - squid proxy

Configurare il proxy sul browser



122

pfSense – Package - squid proxy

aggiungere regole sul firewall

Firewall / Rules / LAN

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0 /5.33 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✓	0 /0 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	
✓	8 /1.37 GiB	IPv4 TCP	*	*	*	3128	*	none		per squid	
✓	7 /2.95 MiB	IPv4 TCP	*	*	*	7445	*	none		per squid report	

Add Add Delete Save Separator

123

Lightsquid

System / Package Manager / Package Installer

pfSense-pkg-Lightsquid installation successfully completed.

Installed Packages Available Packages Package Installer

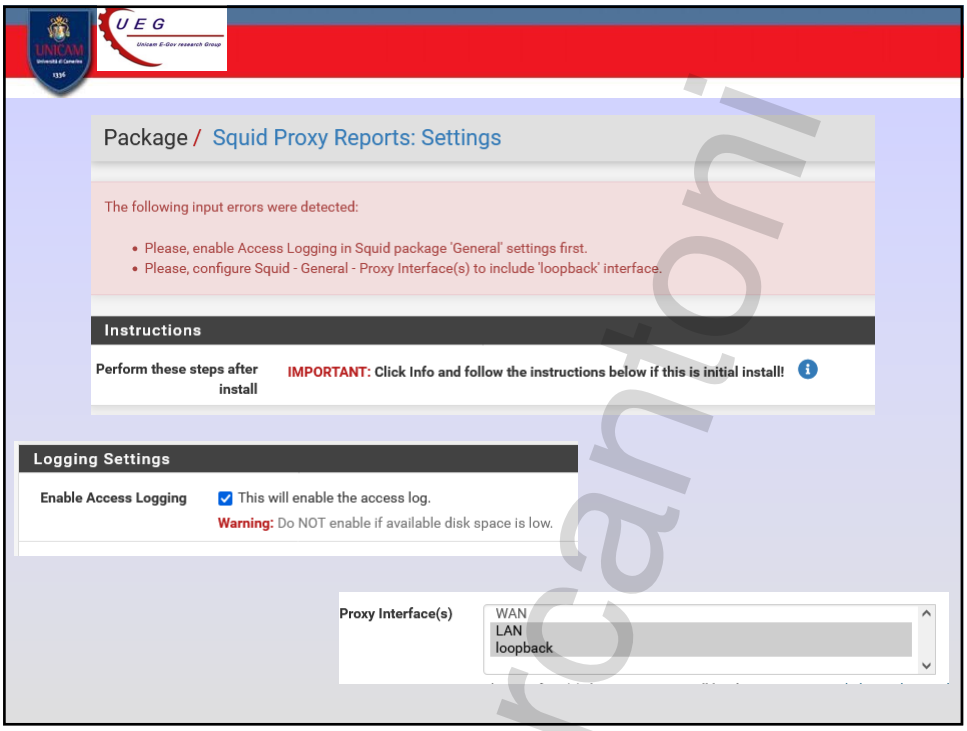
Package Installation

```
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
```

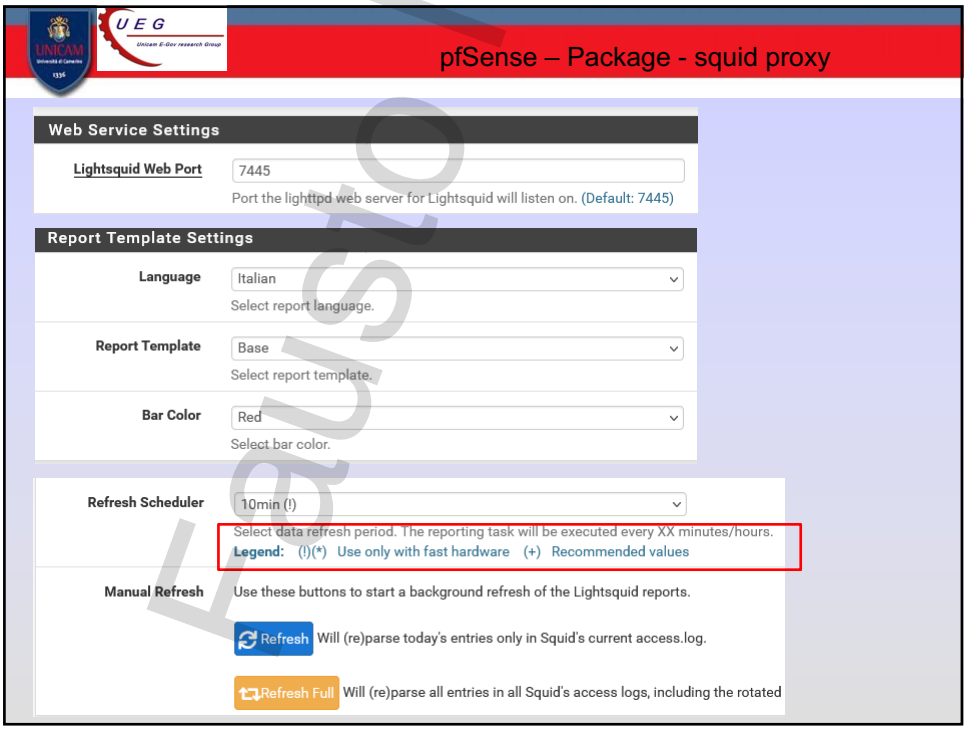
Status ▾ Diagnosti

- Captive Portal
- CARP (failover)
- Dashboard
- DHCP Leases
- DHCPv6 Leases
- DNS Resolver
- Filter Reload
- Gateways
- Interfaces
- IPsec
- Monitoring
- NTP
- OpenVPN
- Queues
- Services
- Squid Proxy Reports
- System Logs
- Traffic Graph
- UPnP & NAT-PMP

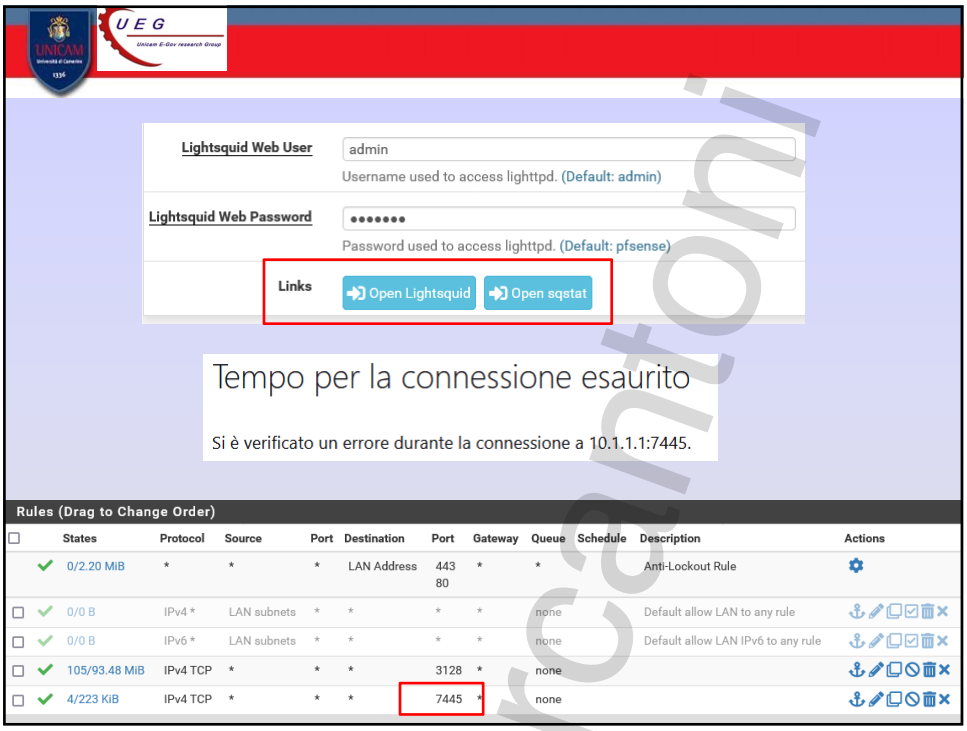
124



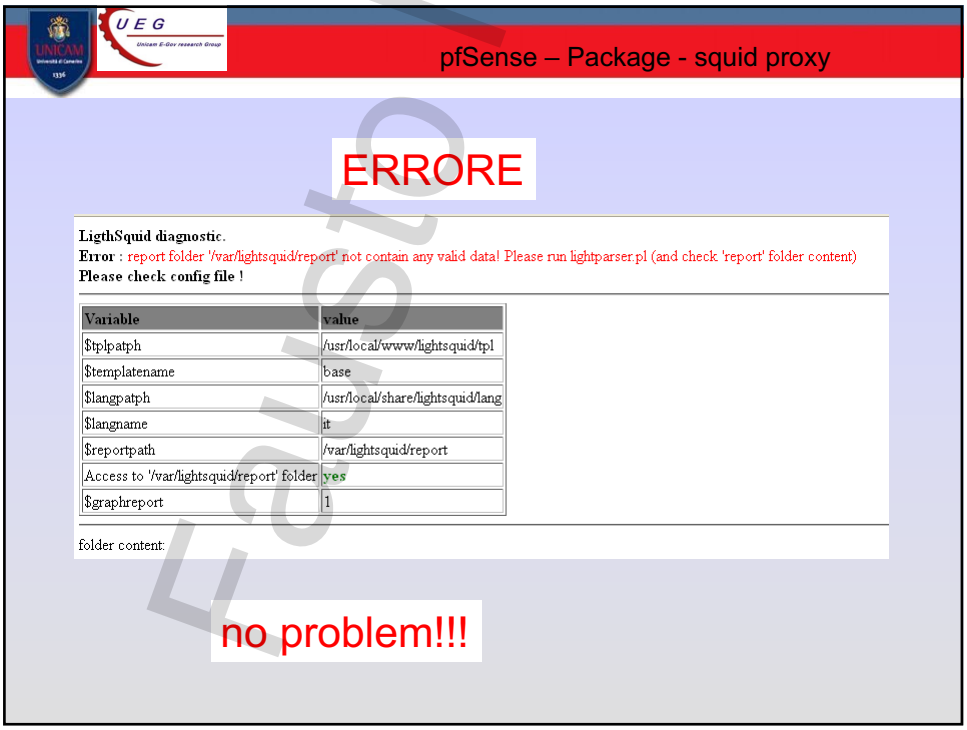
125



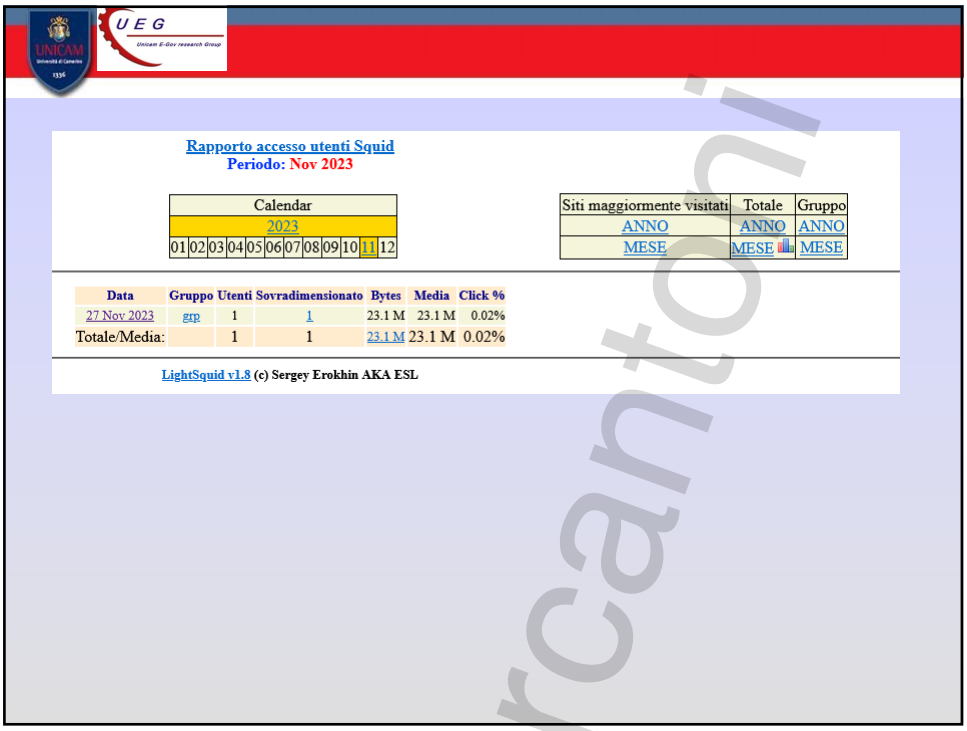
126



127



128



Rapporto accesso utenti Squid
Periodo: Nov 2023

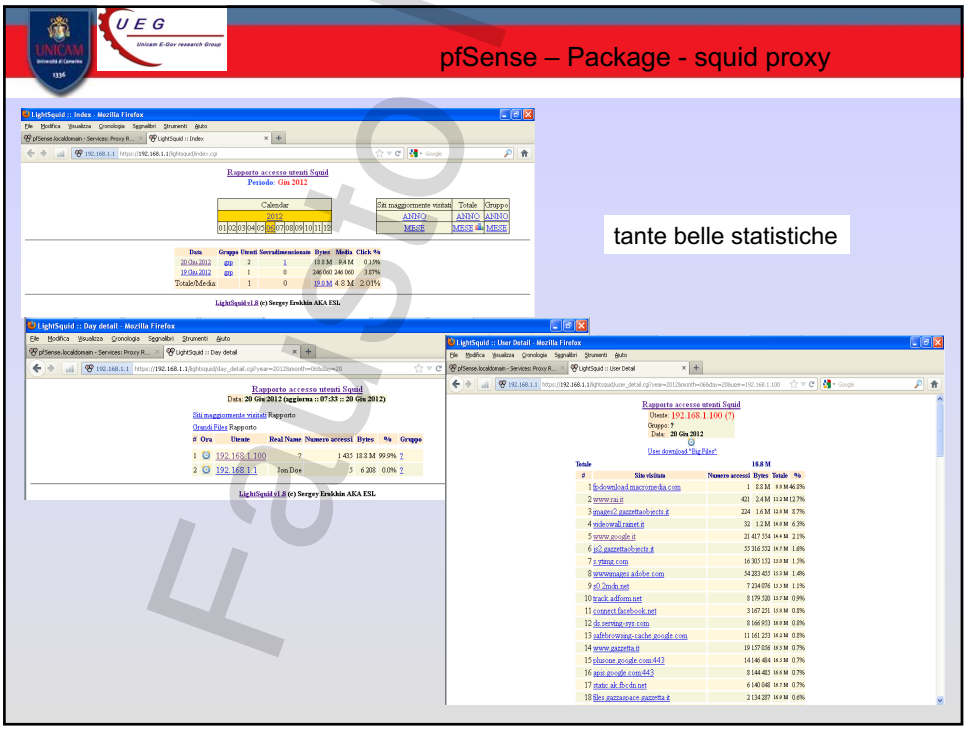
Calendar
2023
01 02 03 04 05 06 07 08 09 10 11 12

Siti maggiormente visitati	Totale	Gruppo
ANNO	ANNO	ANNO
MESE	MESE	MESE

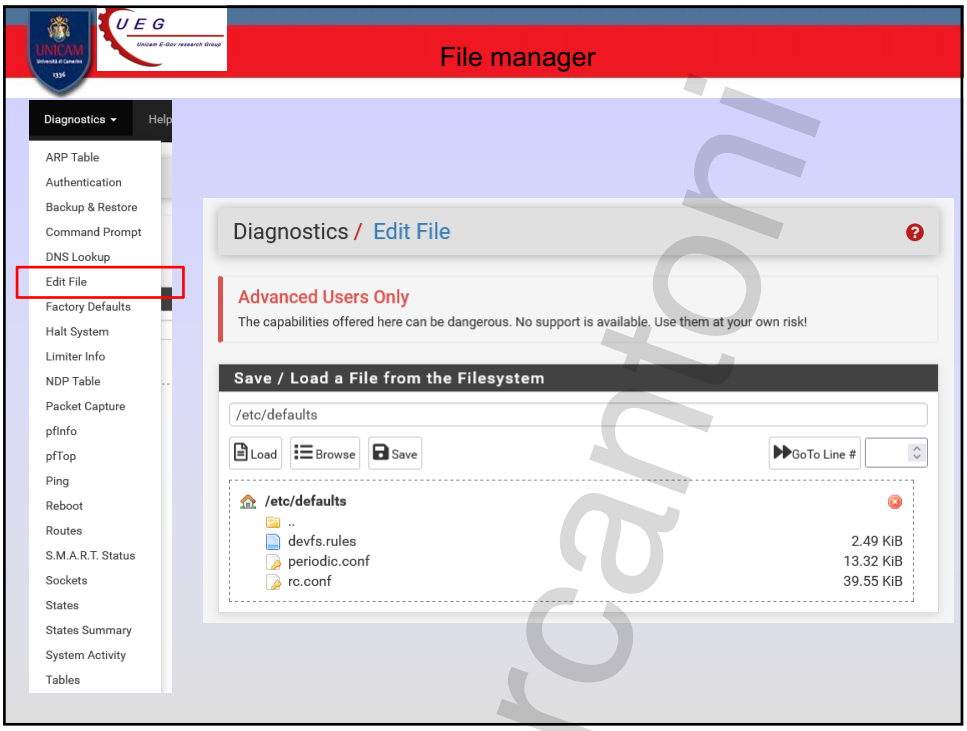
Data	Gruppo	Utenti	Sovradimensionato	Bytes	Media	Click %
27 Nov 2023	grp	1	1	23.1 M	23.1 M	0.02%
Totale/Media:		1	1	23.1 M	23.1 M	0.02%

LightSquid v1.8 (c) Sergey Erokhin AKA ESL

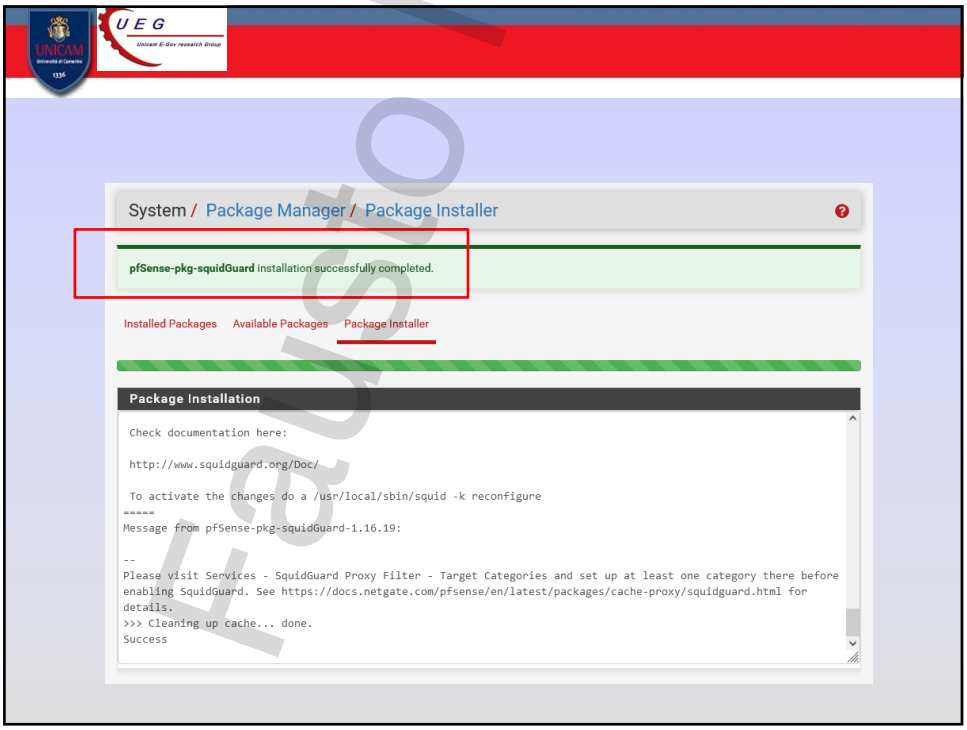
129



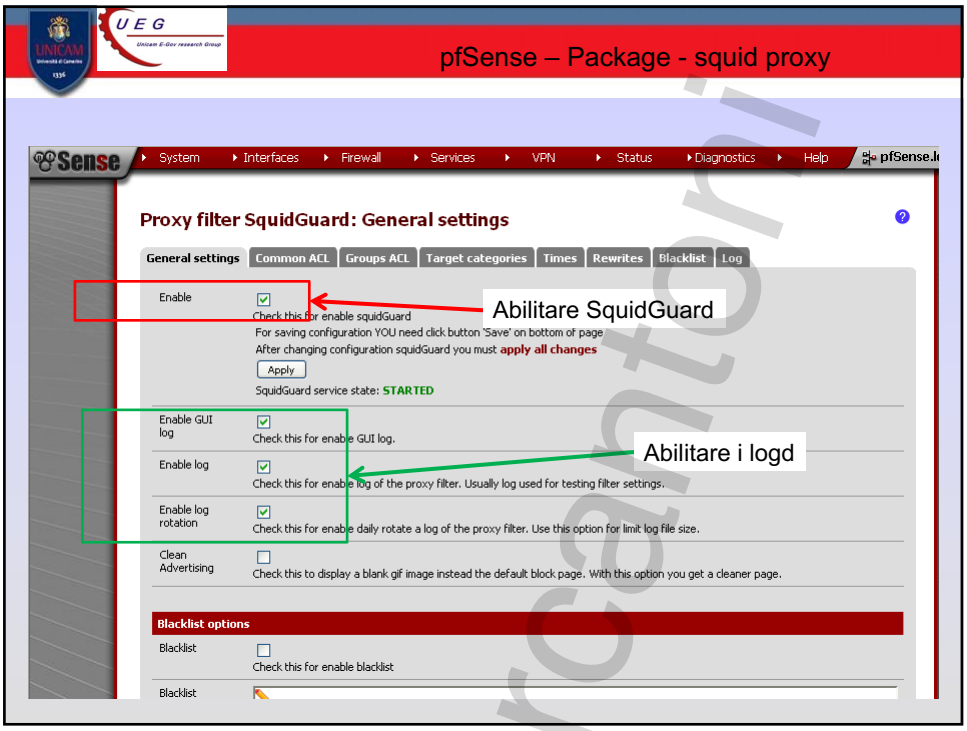
130



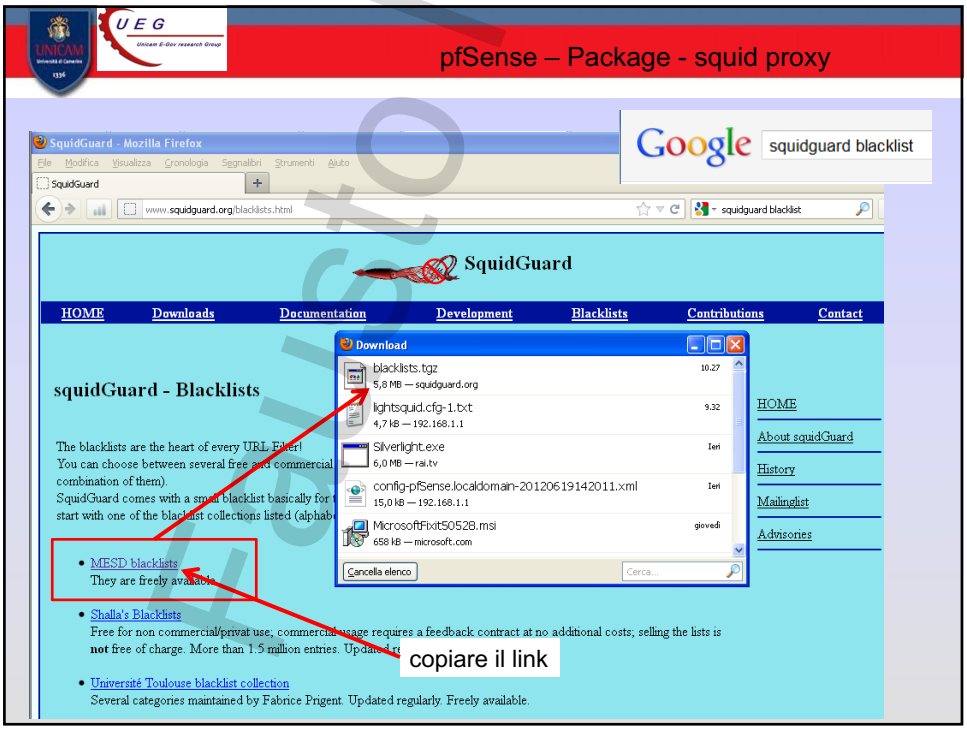
131



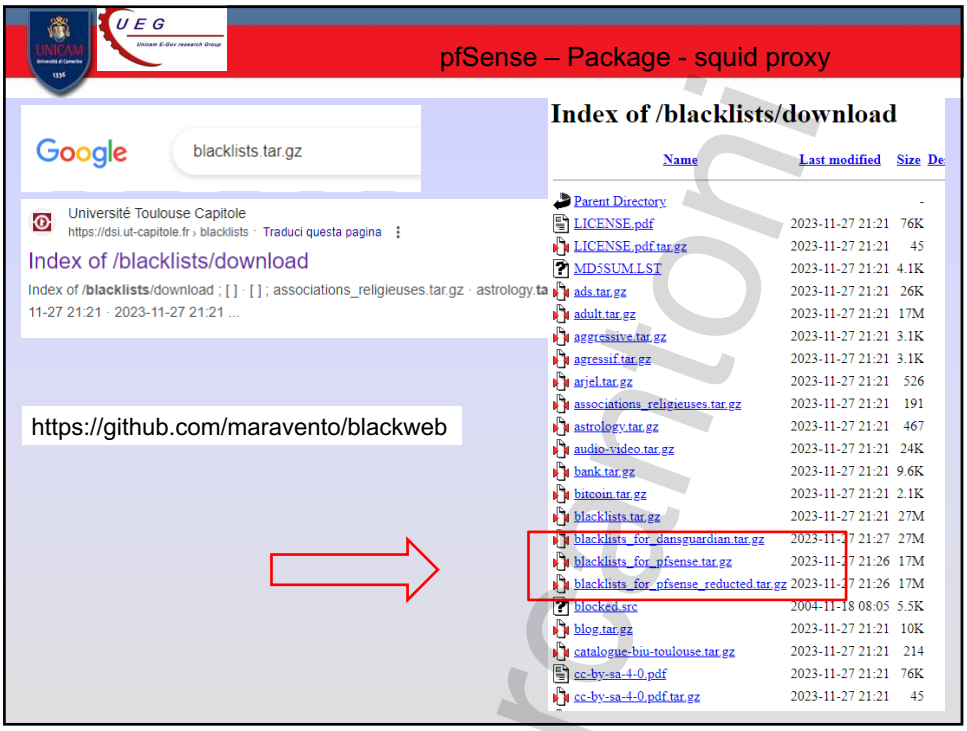
132



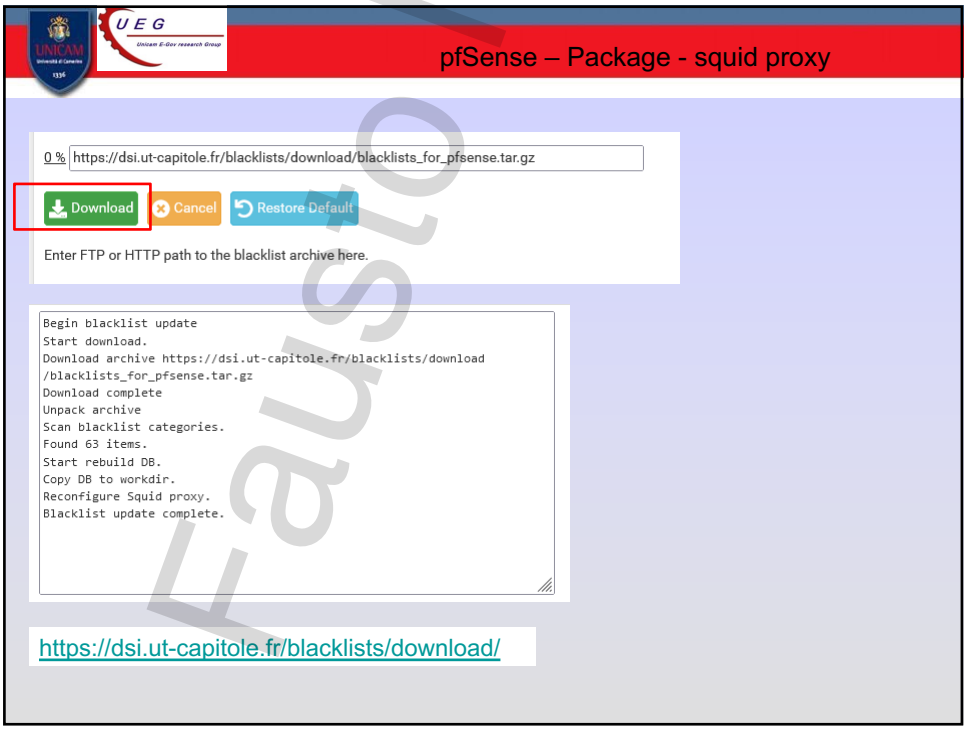
133



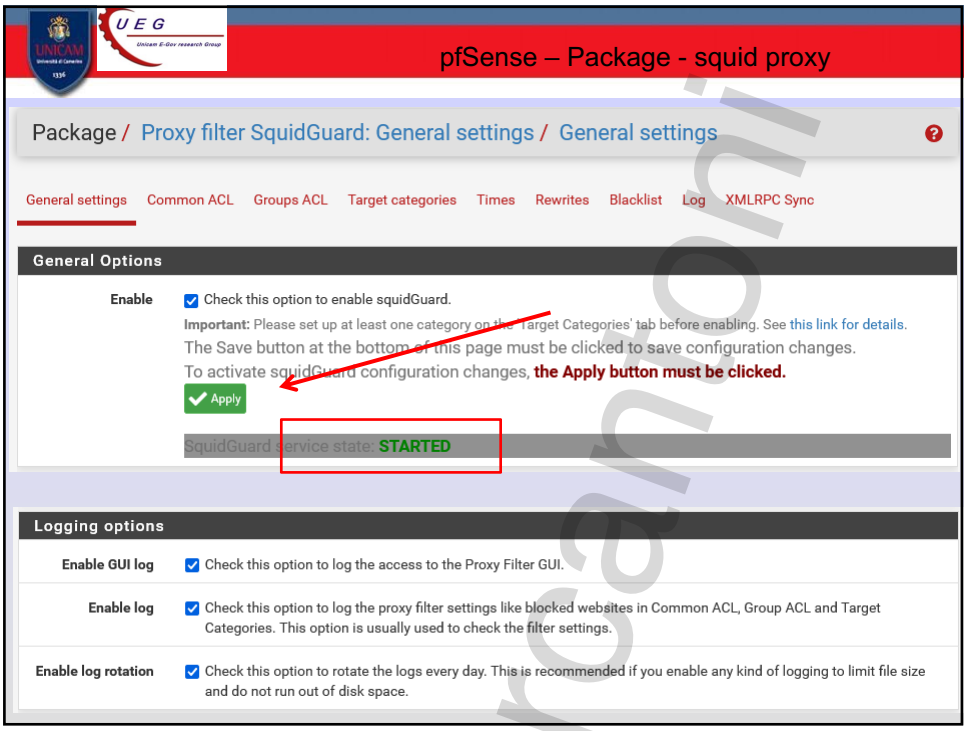
134



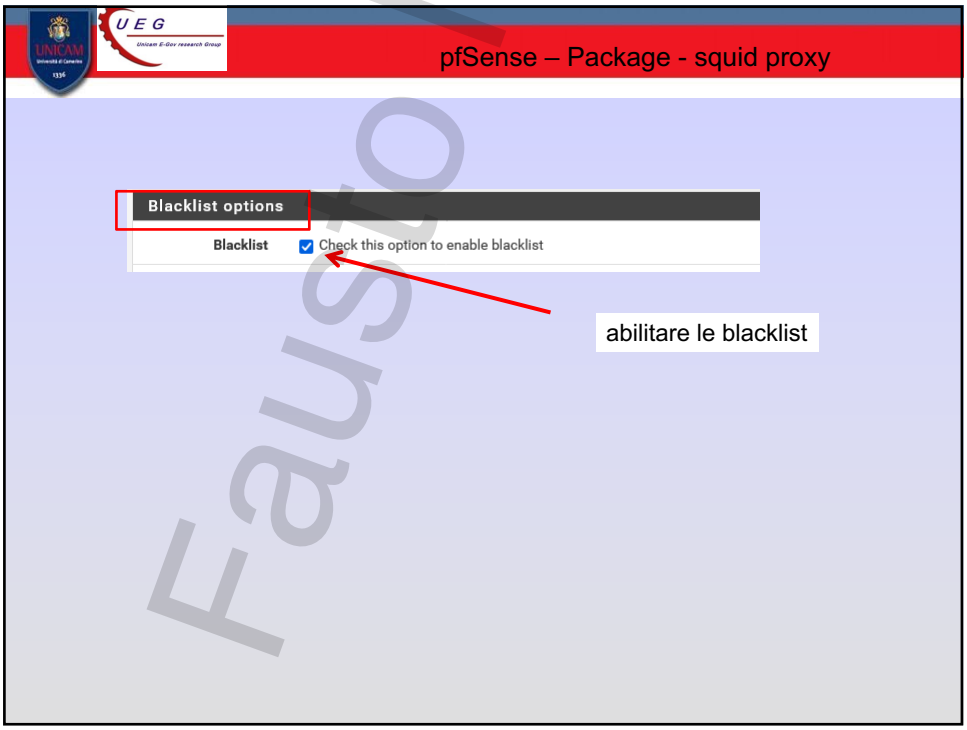
135



136



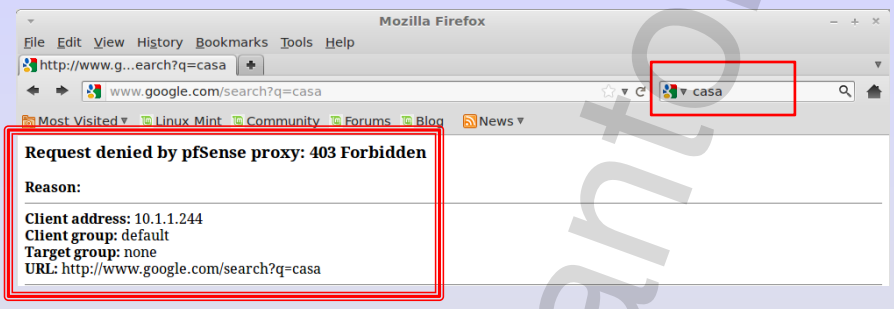
137



138

pfSense – Package - squid proxy

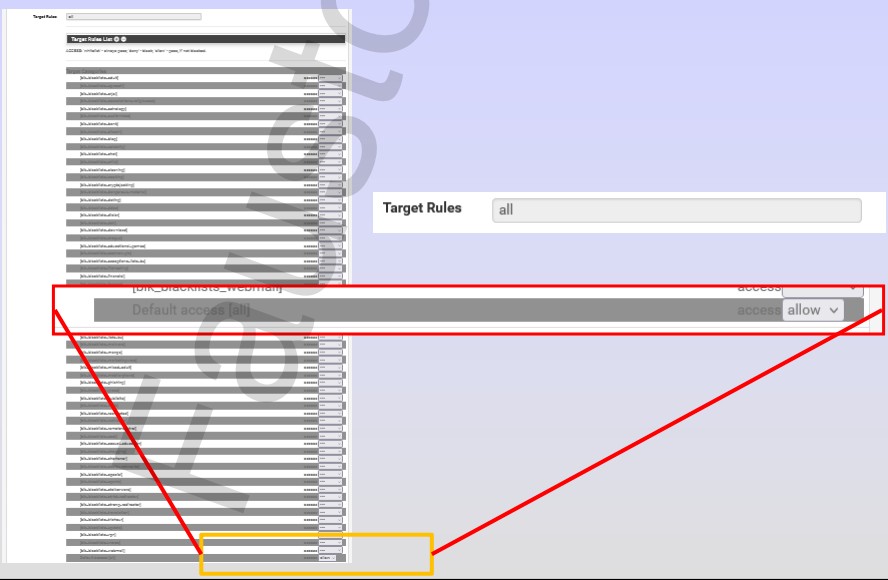
ERRORE !!!



139

pfSense – Package - squid proxy

Configurare le regole



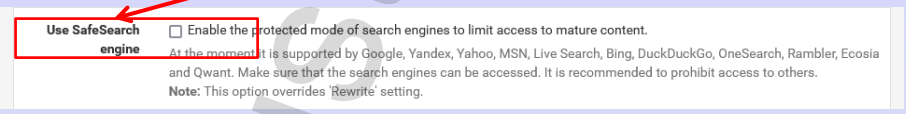
140

pfSense – Package - squid proxy

141

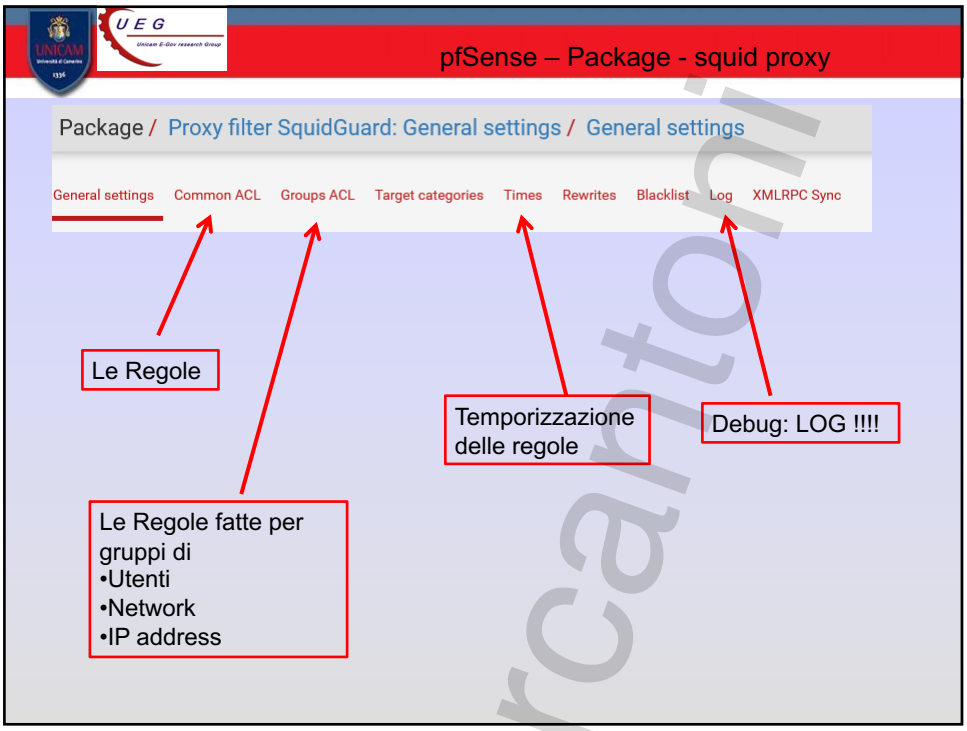
pfSense – Package - squid proxy

Use SafeSearch engine

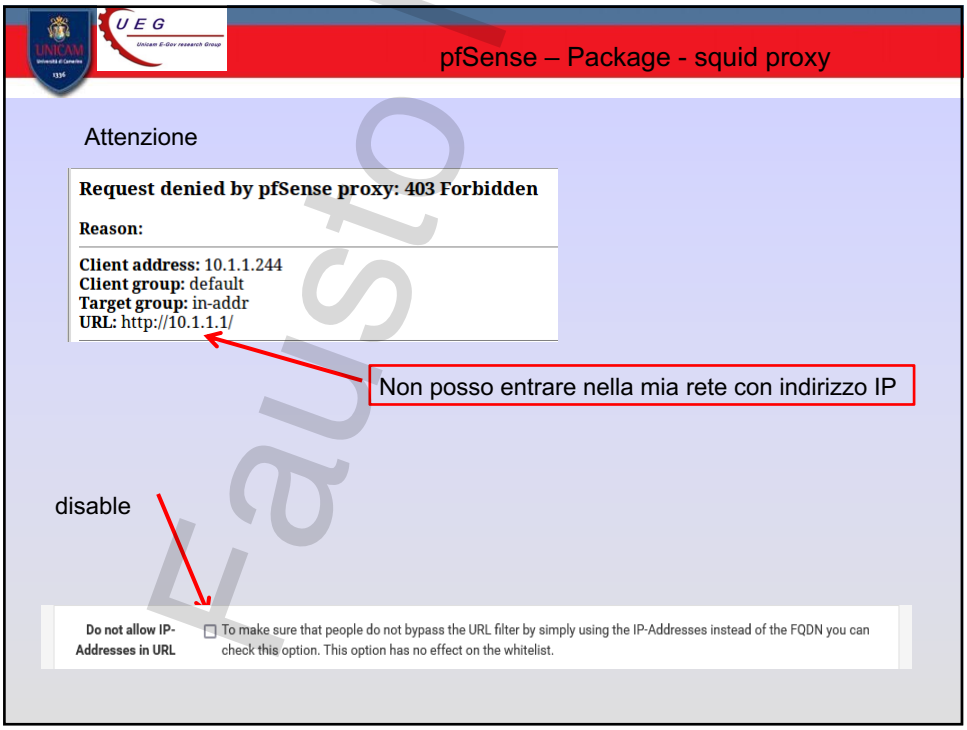


Nessun motore di ricerca può sostituire la supervisione dei genitori quando si tratta di bambini e internet.

142

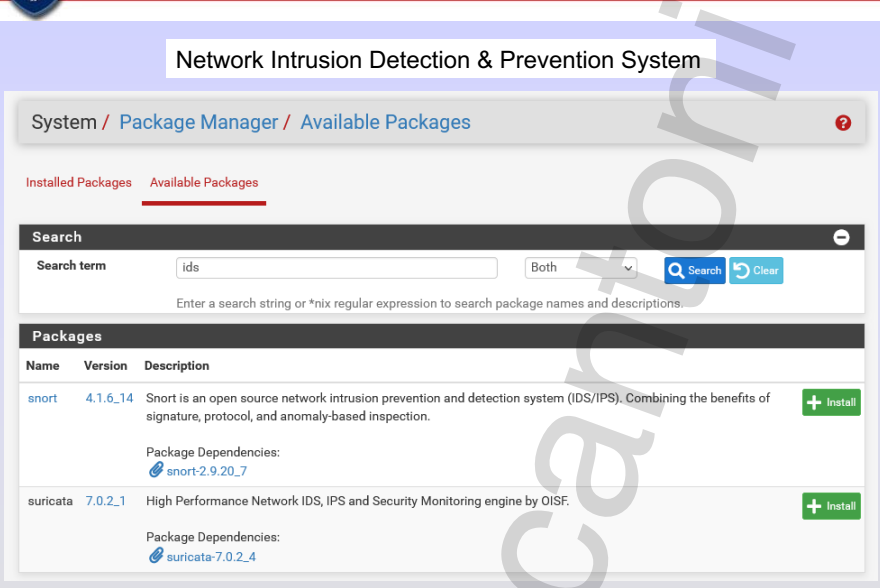


143



144

Network Intrusion Detection & Prevention System



145

Snort/Suricata

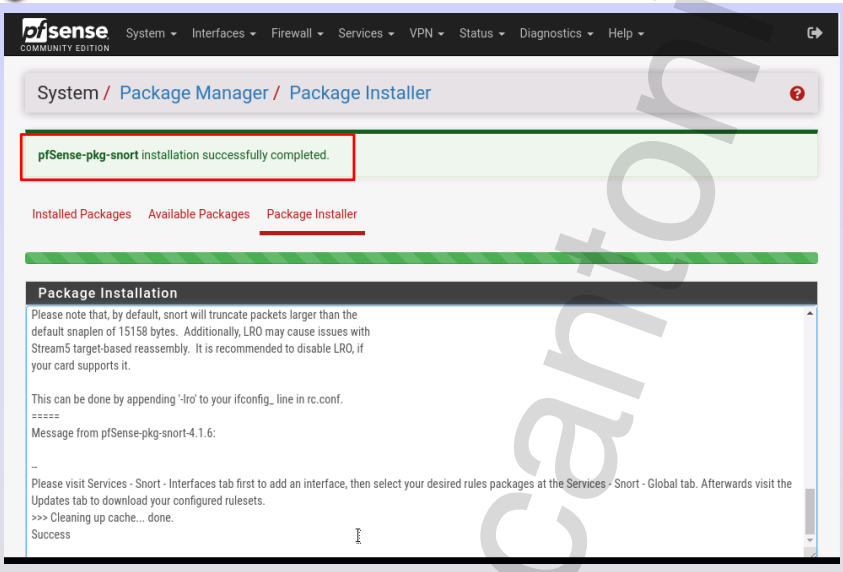
- Snort and Suricata are pfSense software packages for network intrusion detection. Depending on their configuration, they can require a significant amount of RAM. 1 GB should be considered a minimum but some configurations may need 2 GB or more, not counting RAM used by the operating system, firewall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

https://www.snort.org/

https://suricata.io/

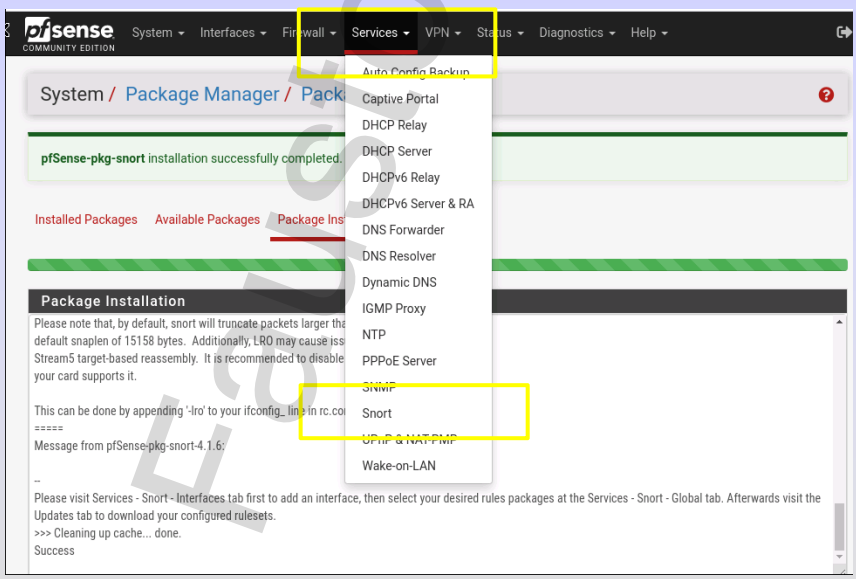
146

pfSense – Package - snort

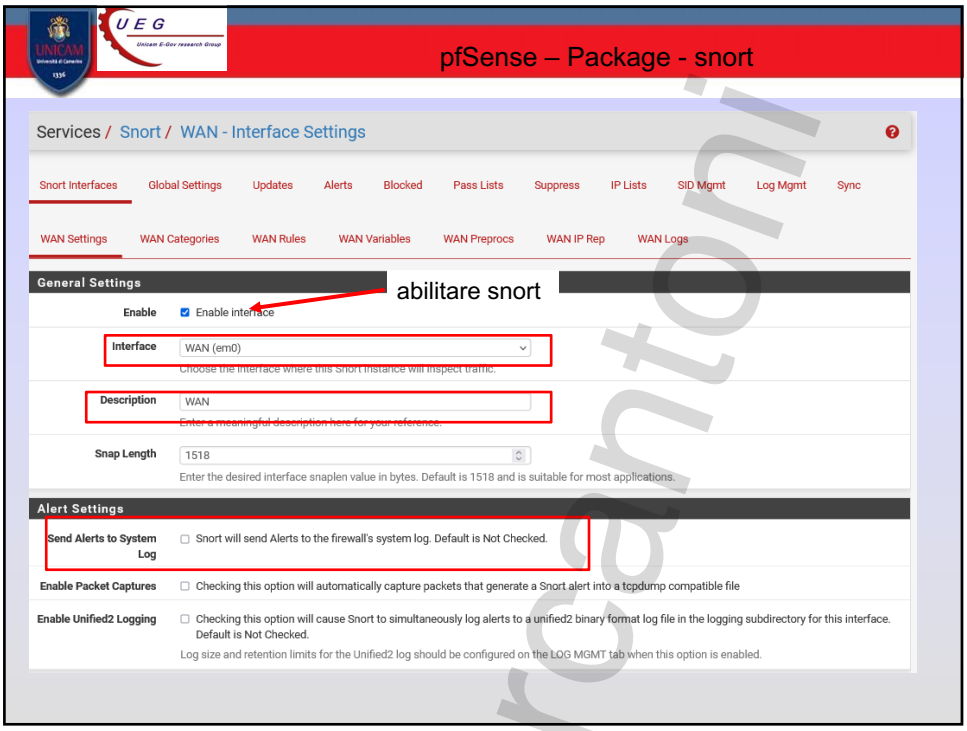


147

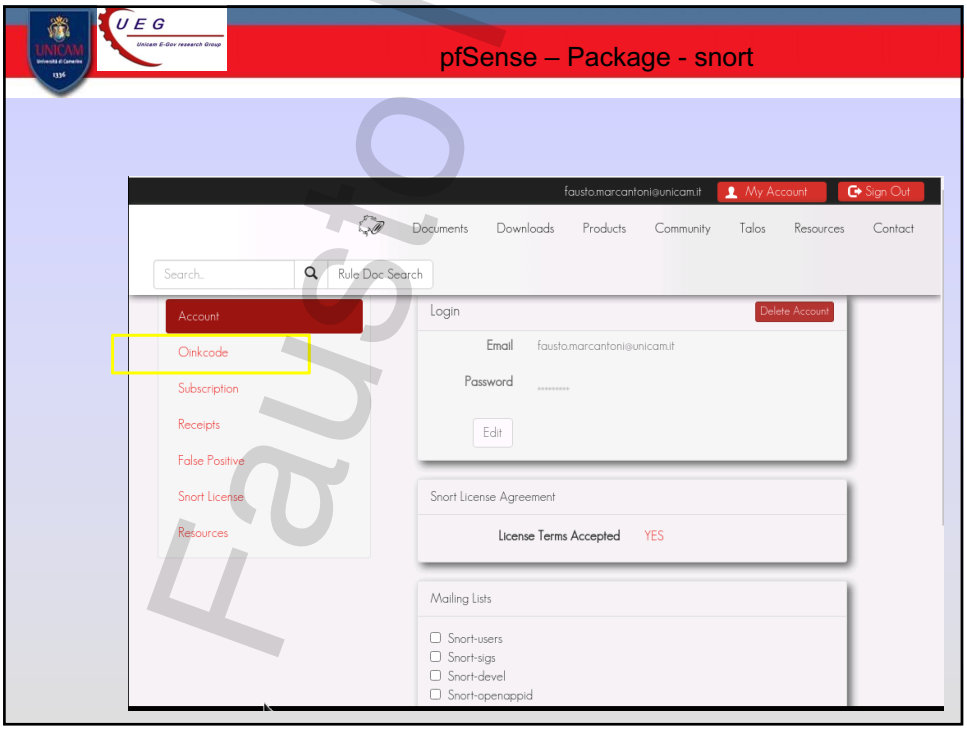
pfSense – Package - snort



148



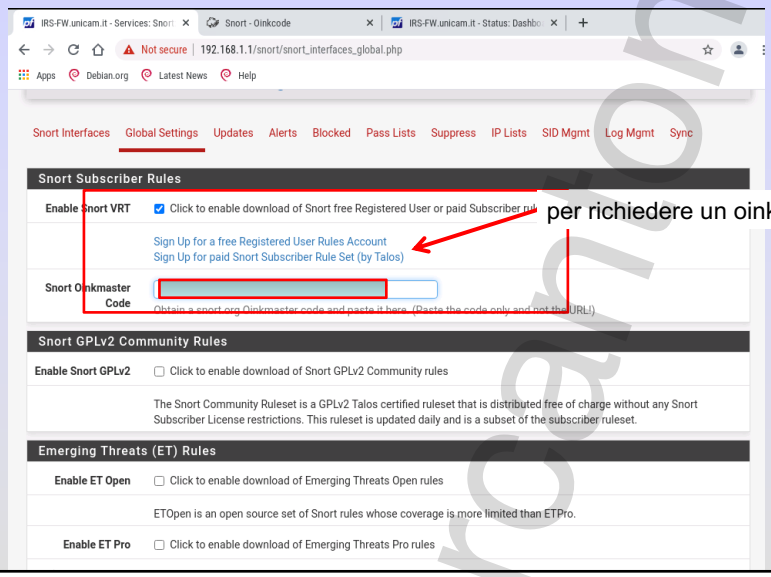
149



150

pfSense – Package - snort

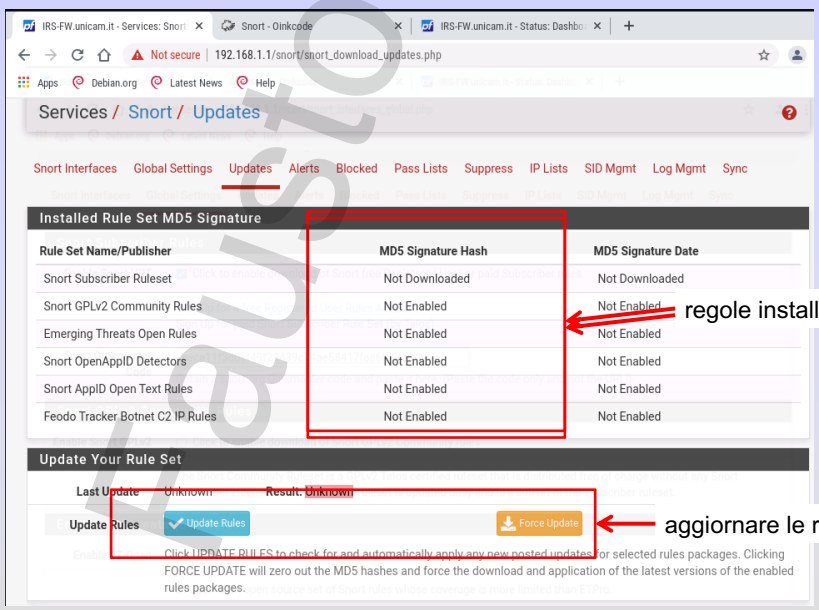
prima di tutto …



per richiedere un oinkcode

151

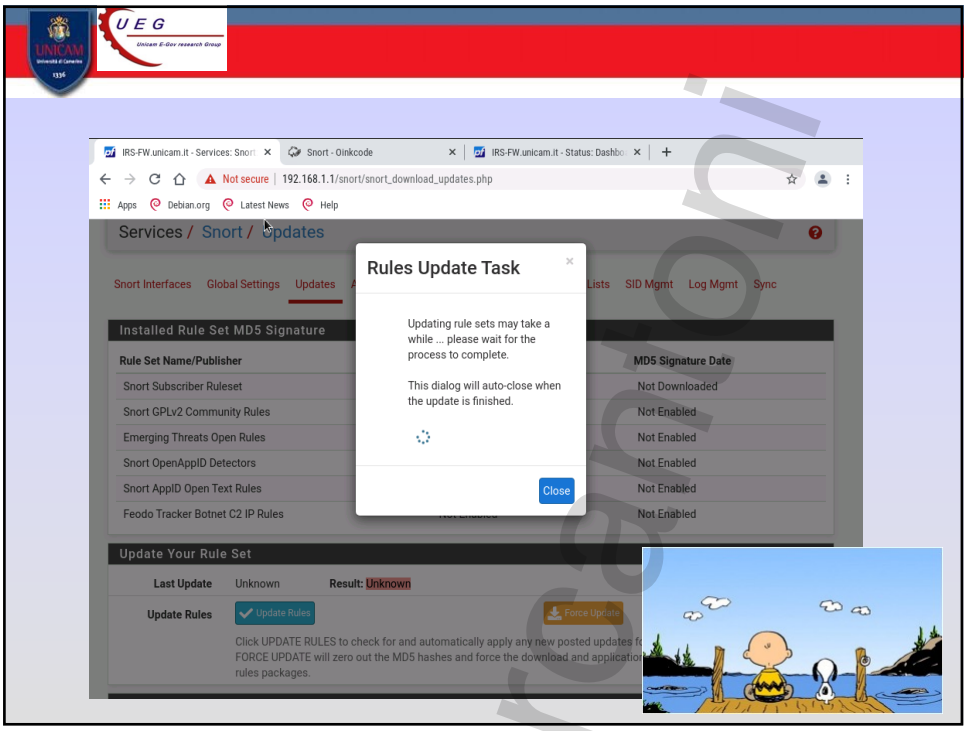
pfSense – Package - snort



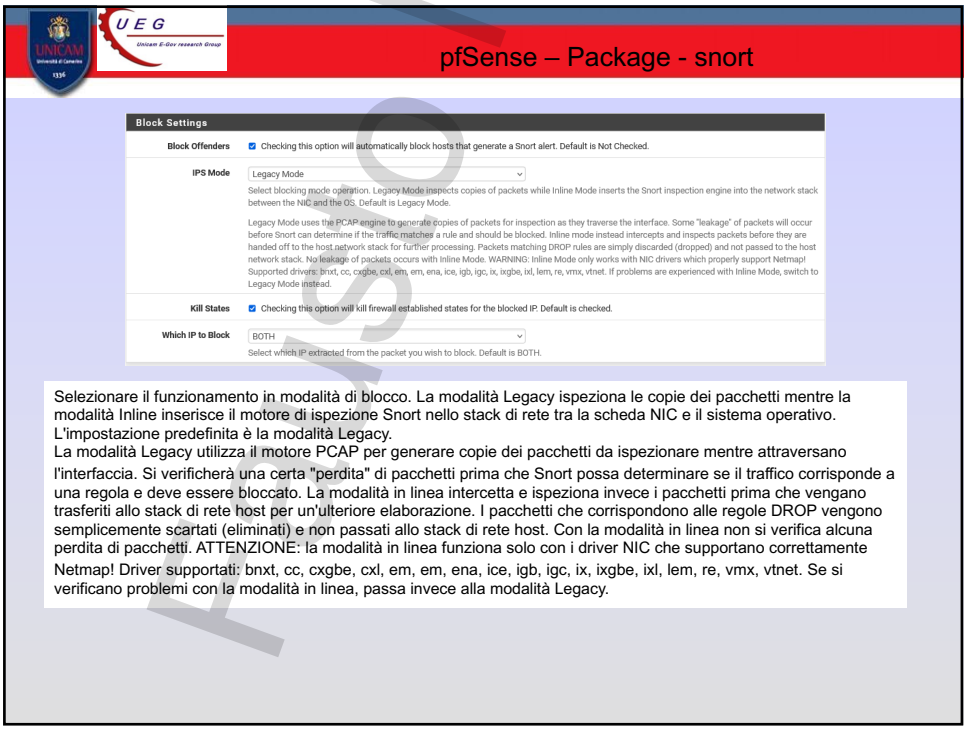
regole installate

aggiornare le regole

152

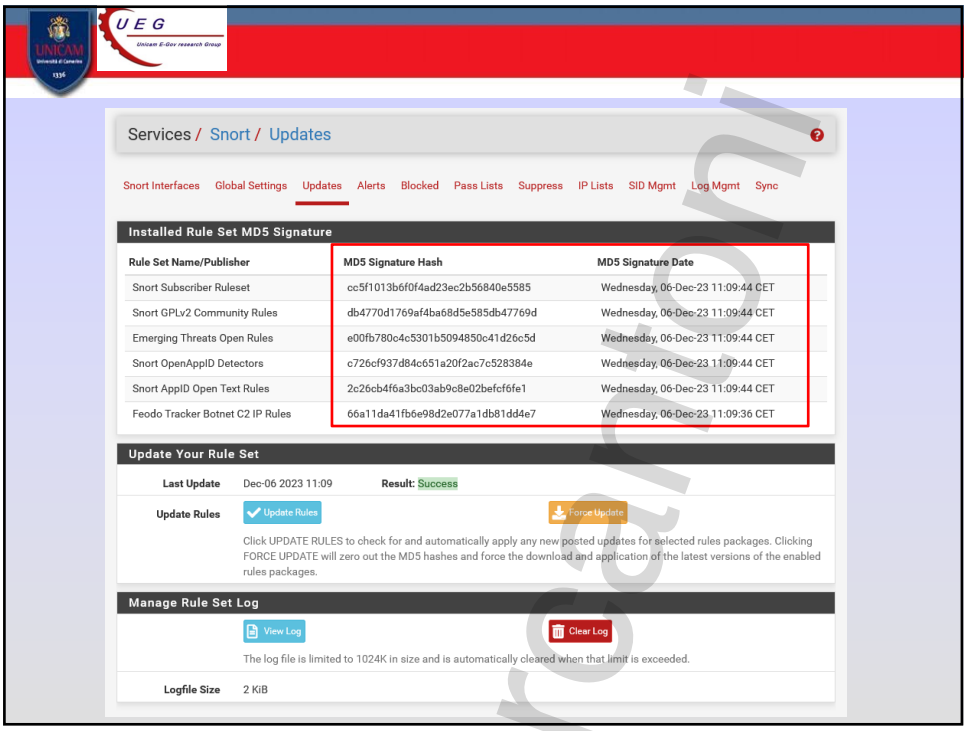


153

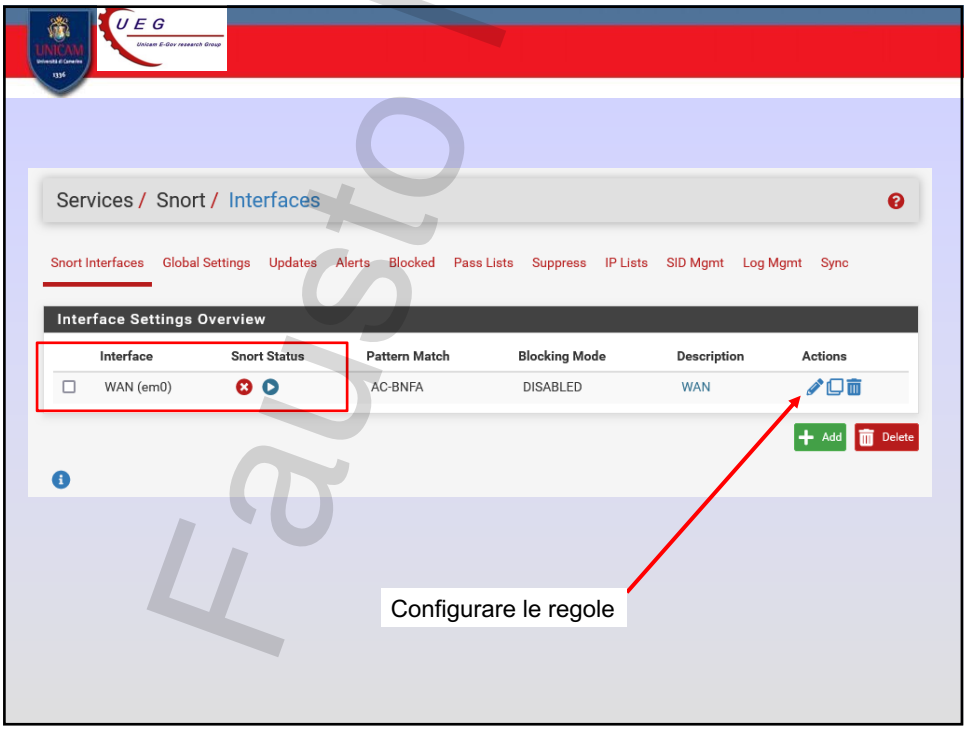


Selezionare il funzionamento in modalità di blocco. La modalità Legacy ispeziona le copie dei pacchetti mentre la modalità Inline inserisce il motore di ispezione Snort nello stack di rete tra la scheda NIC e il sistema operativo. L'impostazione predefinita è la modalità Legacy.
La modalità Legacy utilizza 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.

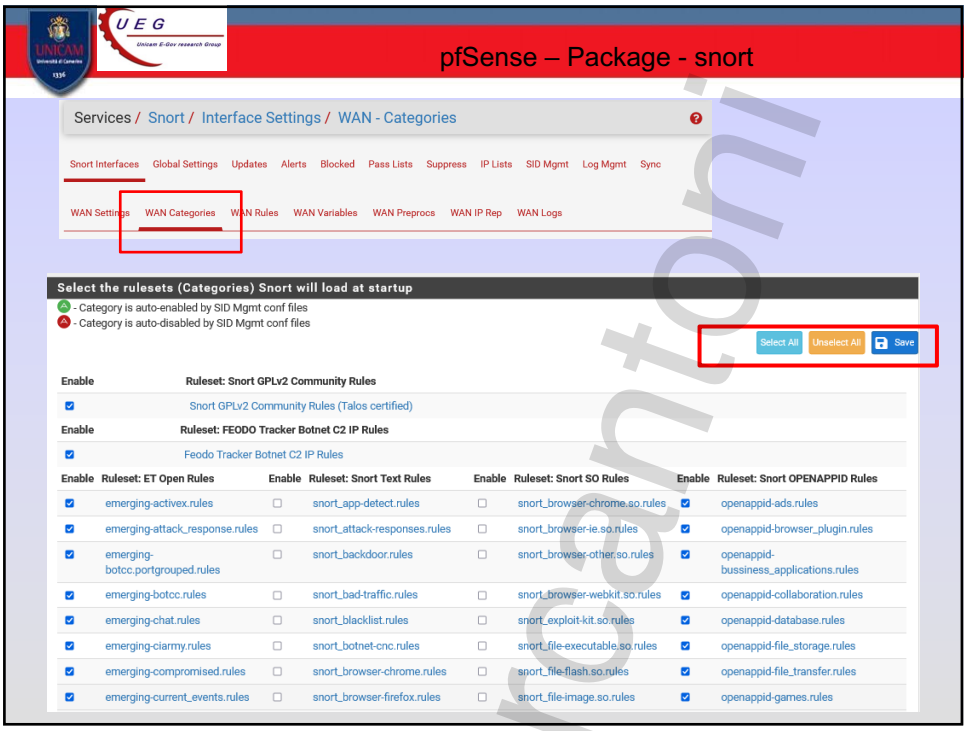
154



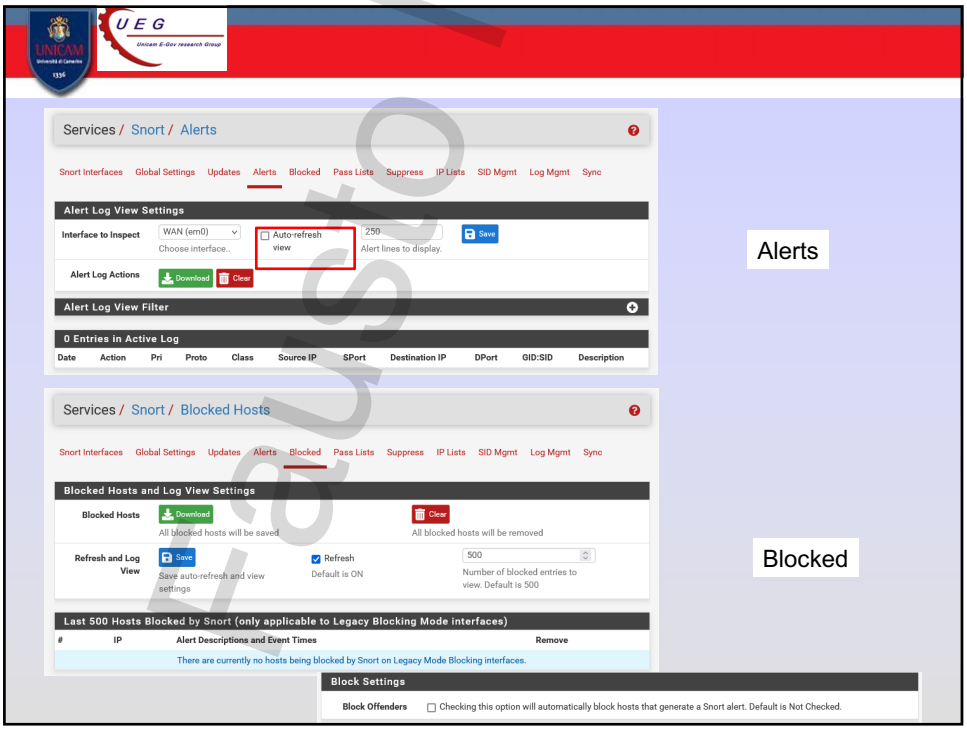
155



156



157



158

pfSense – Package - snort

Abilitare

snort_indicator-scan.rules

snort_scan.rules

nmap -p 1-65535 -T4 -A -v <IP WAN>

Alert Log View Filter

4 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-11-29 11:28:14	⚠	2	TCP	Potentially Bad Traffic	193.205.92.225	59376	193.205.92.226	4333	1:2010938	ET SCAN Suspicious inbound to mSQL port 4333
2023-11-29 11:28:14	⚠	2	TCP	Potentially Bad Traffic	193.205.92.225	59374	193.205.92.226	4333	1:2010938	ET SCAN Suspicious inbound to mSQL port 4333
2023-11-29 11:27:23	⚠	2	TCP	Attempted Information Leak	193.205.92.225	59374	193.205.92.226	5901	1:2002911	ET SCAN Potential VNC Scan 5900-5920
2023-11-29 10:31:27	⚠	3	TCP	Unknown Traffic	142.251.209.19	80	193.205.92.225	36285	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE

159

pfSense – Package - snort

Status / System Logs / System / General

System Firewall DHCP Authentication IPsec PPP PPPoE/L2TP Server OpenVPN NTP Packages Settings

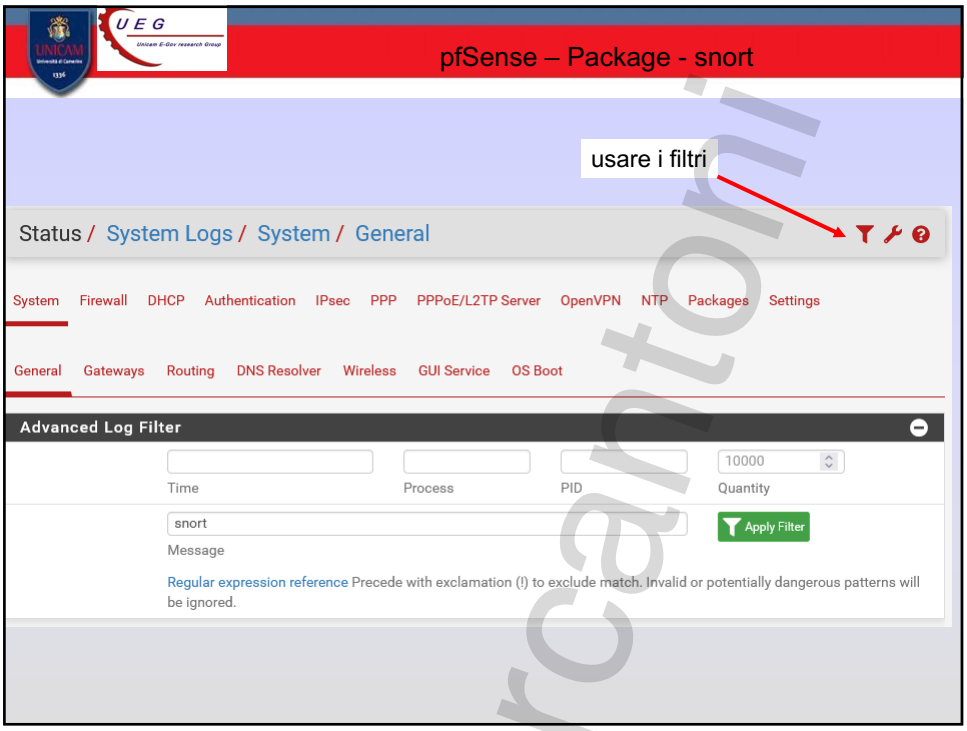
General Gateways Routing DNS Resolver Wireless GUI Service OS Boot

errore: visualizzare il file di log

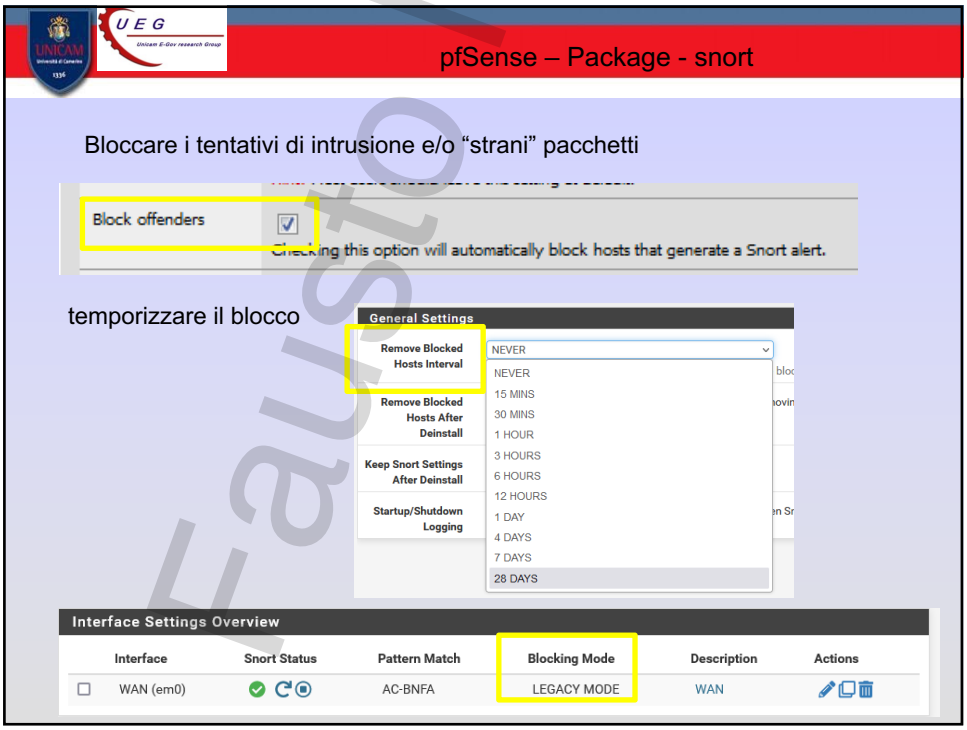
Last 25 General Log Entries. (Maximum 10000)

Nov 29 11:47:23	snort	80880	[1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 193.205.92.225:42308 -> 193.205.92.226:3306
Nov 29 11:47:23	sshguard	7407	Now monitoring attacks.
Nov 29 11:47:25	snort	80880	[1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 193.205.92.225:42310 -> 193.205.92.226:3306
Nov 29 11:47:25	snort	80880	[1:2010936:3] ET SCAN Suspicious inbound to Oracle SQL port 1521 [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 193.205.92.225:42308 -> 193.205.92.226:1521
Nov 29 11:47:25	snort	80880	[1:2010936:3] ET SCAN Suspicious inbound to Oracle SQL port 1521 [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 193.205.92.225:42310 -> 193.205.92.226:1521
Nov 29 11:47:28	snort	80880	[1:2010939:3] ET SCAN Suspicious inbound to PostgreSQL port 5432 [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 193.205.92.225:42308 -> 193.205.92.226:5432
Nov 29 11:47:29	snort	80880	[1:2010939:3] ET SCAN Suspicious inbound to PostgreSQL port 5432 [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 193.205.92.225:42310 -> 193.205.92.226:5432
Nov 29 11:47:29	snort	80880	[1:2002911:5] ET SCAN Potential VNC Scan 5900-5920 [Classification: Attempted Information Leak] [Priority: 2] {TCP} 193.205.92.225:42308 -> 193.205.92.226:5906
Nov 29 11:47:36	snort	80880	[1:2002910:5] ET SCAN Potential VNC Scan 5800-5820 [Classification: Attempted Information Leak] [Priority: 2] {TCP} 193.205.92.225:42308 -> 193.205.92.226:5815
Nov 29 11:47:37	snort	80880	[1:2010935:3] ET SCAN Suspicious inbound to MSSQL port 1433 [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 193.205.92.225:42308 -> 193.205.92.226:1433
Nov 29 11:47:37	snort	80880	[1:2010935:3] ET SCAN Suspicious inbound to MSSQL port 1433 [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 193.205.92.225:42310 -> 193.205.92.226:1433

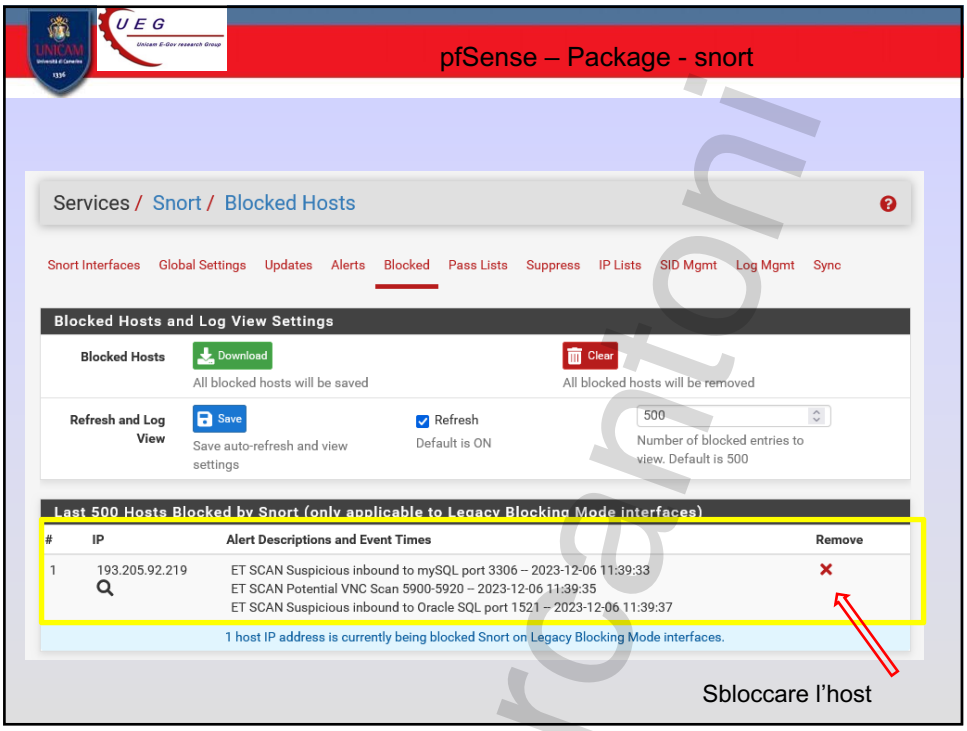
160



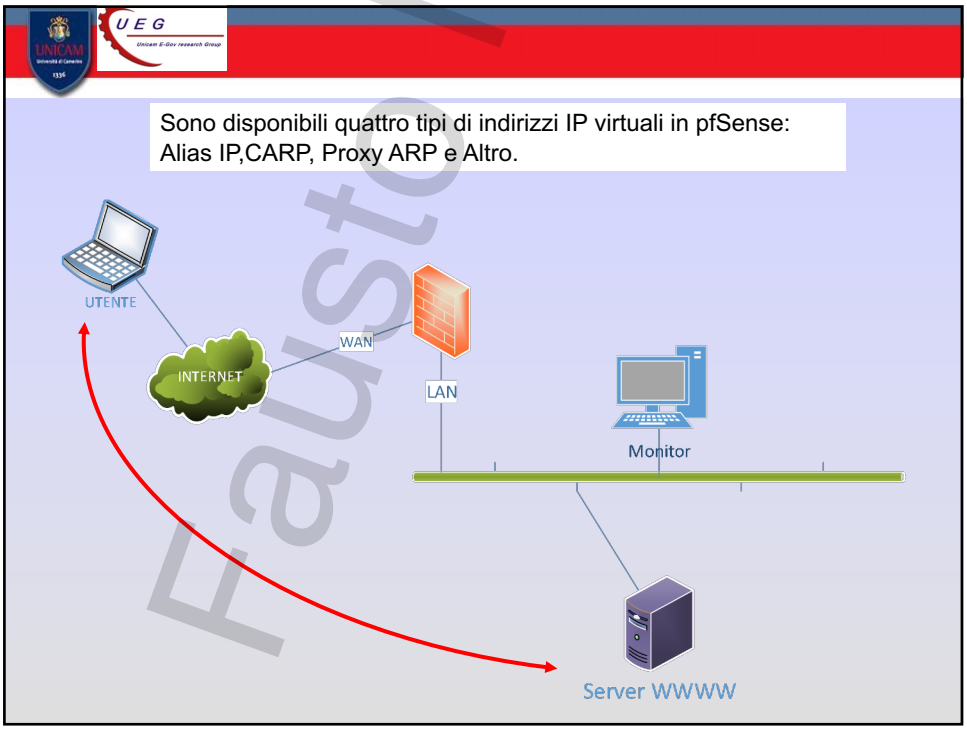
161



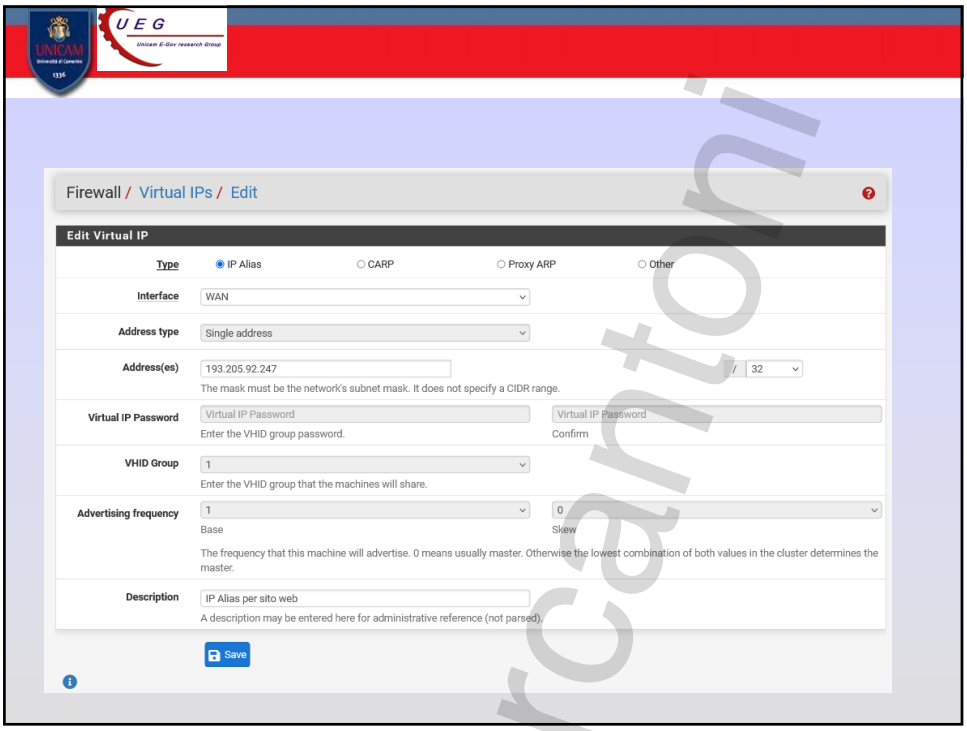
162



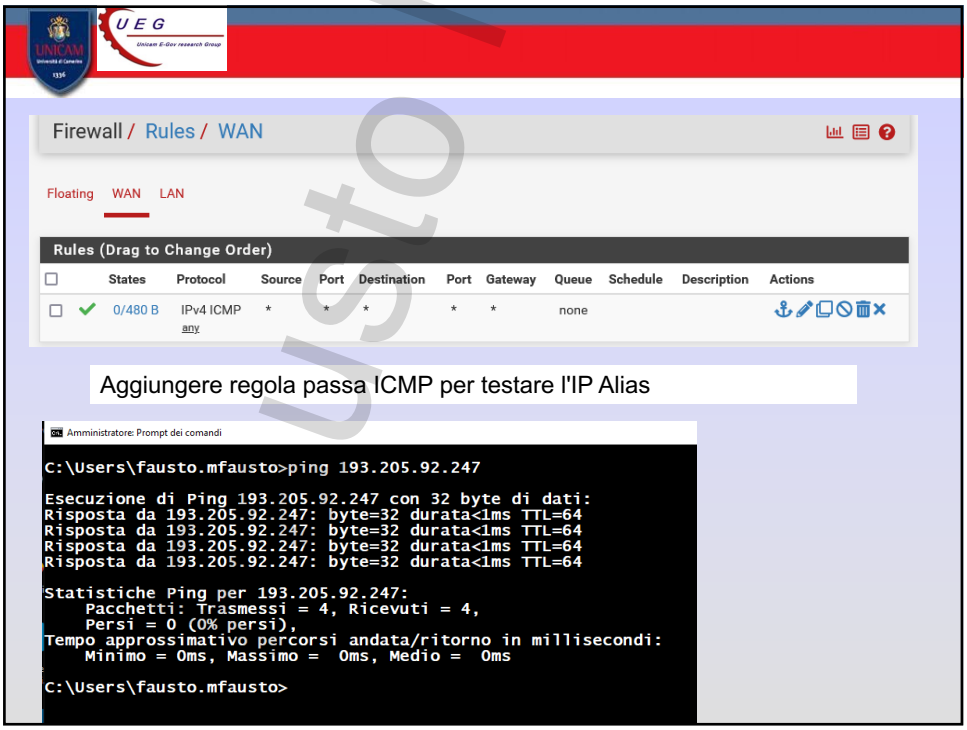
163



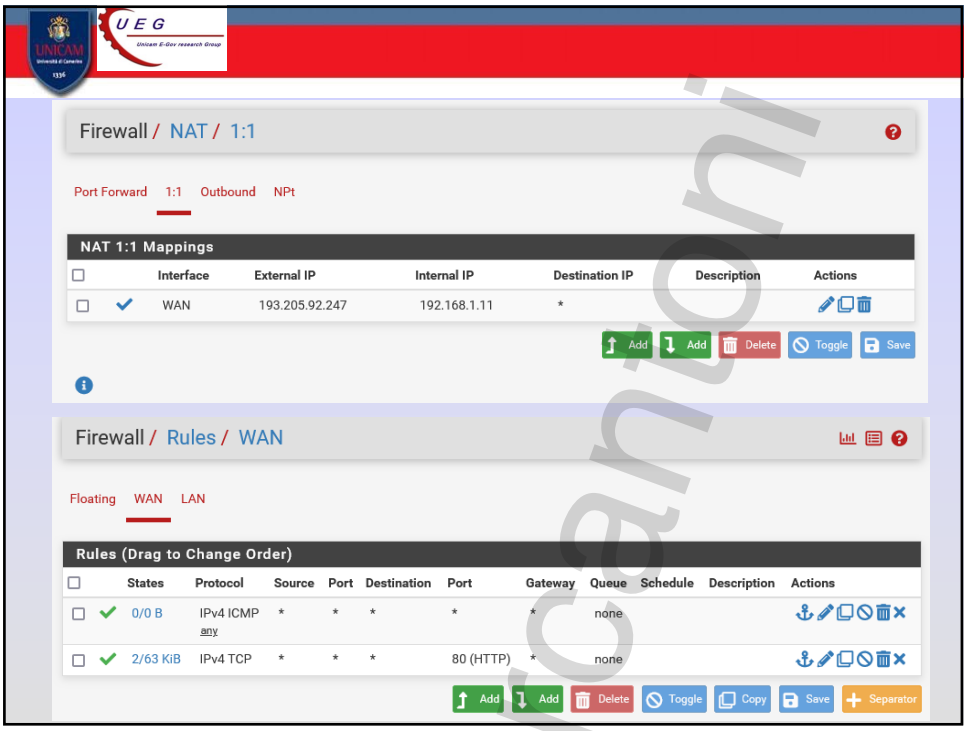
164



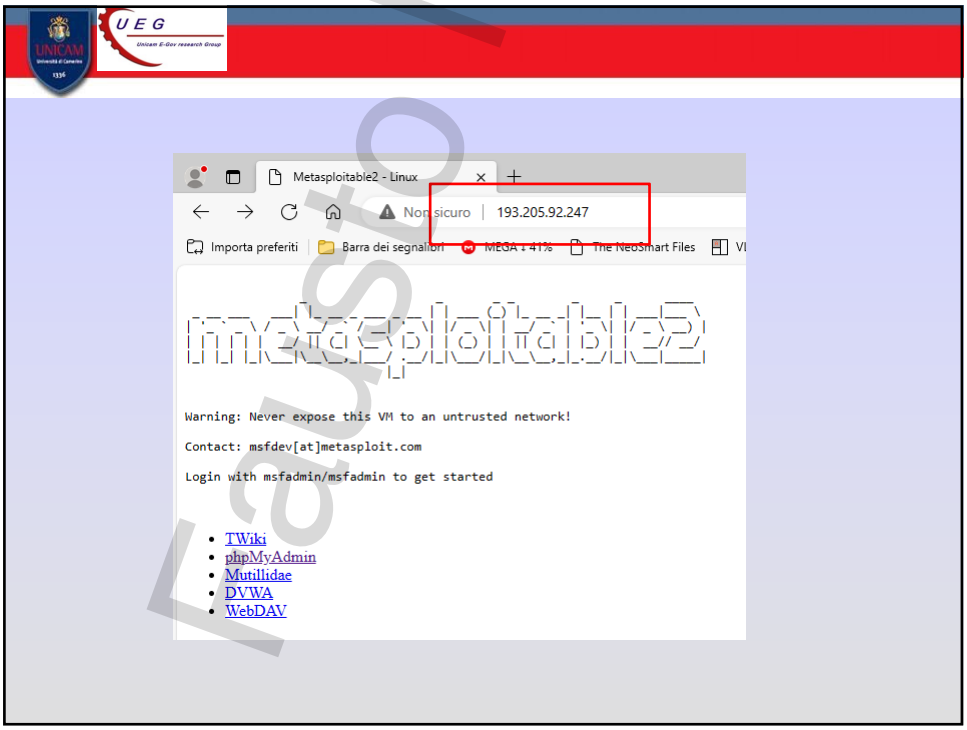
165



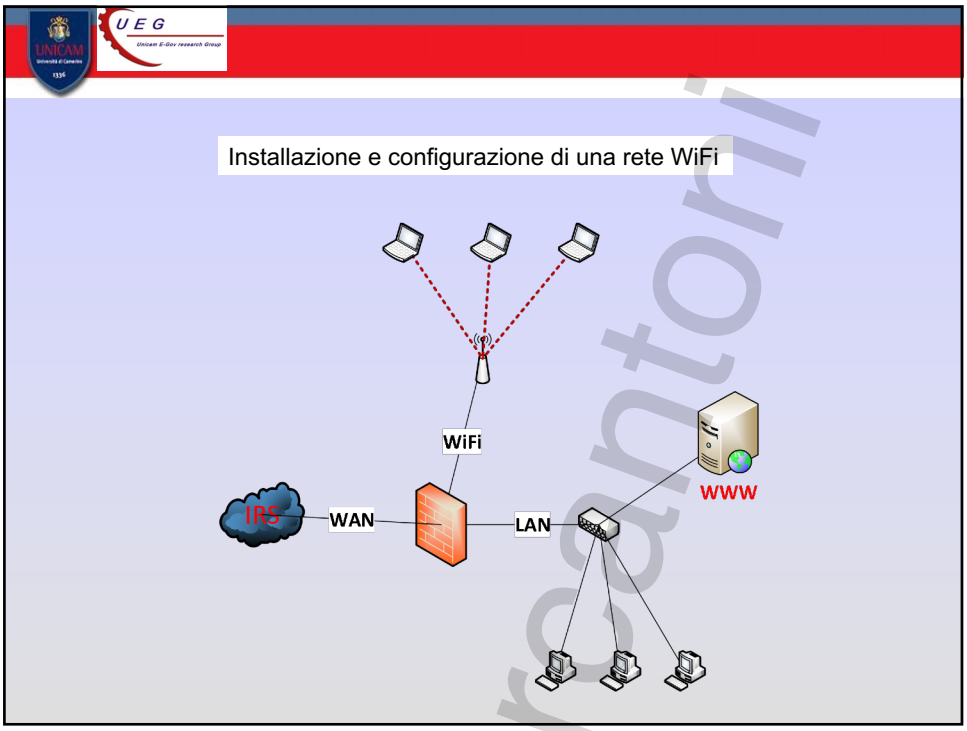
166



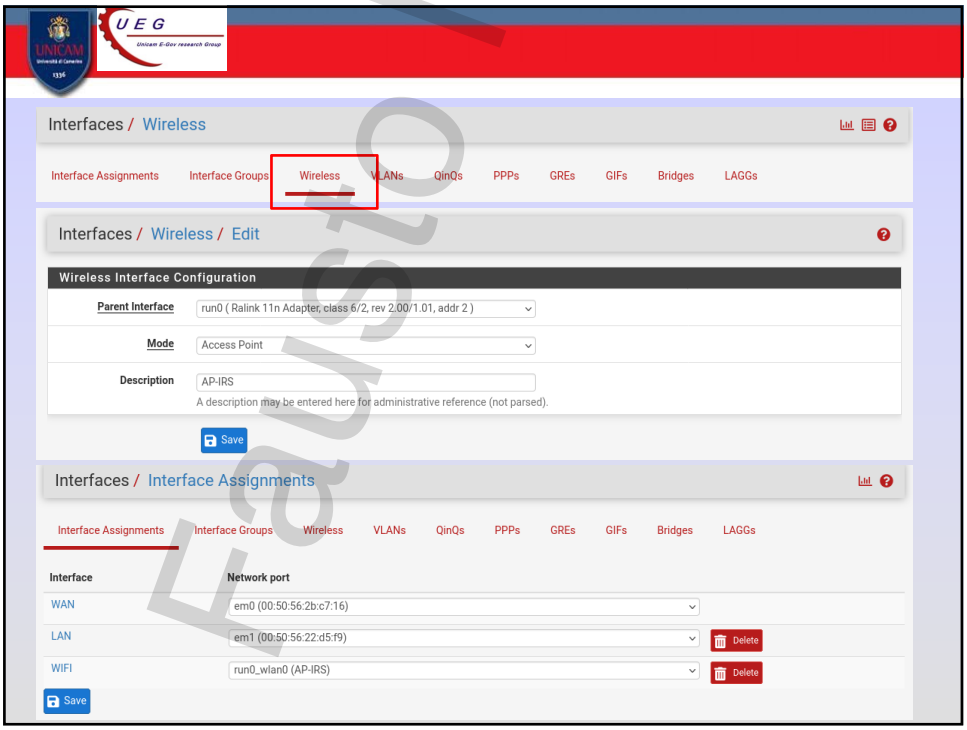
167



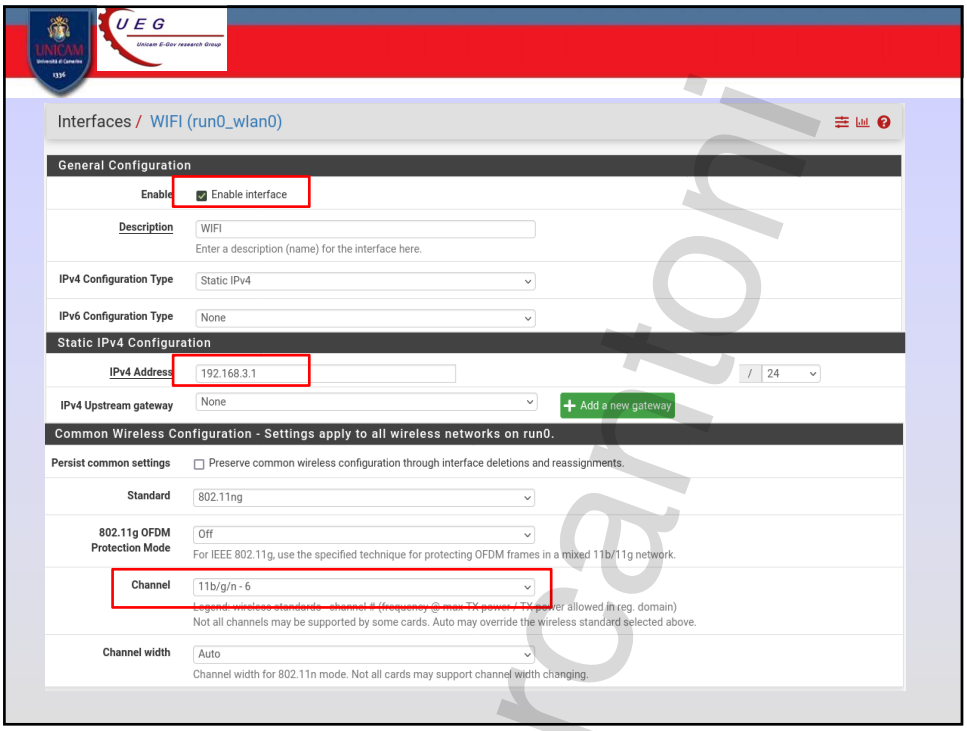
168



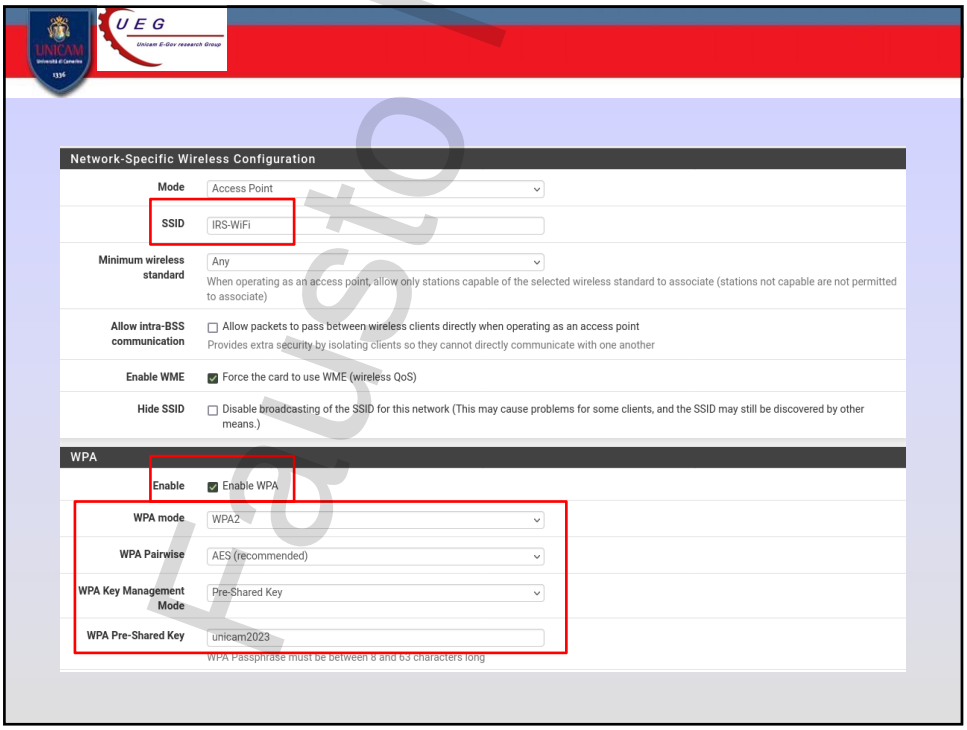
169



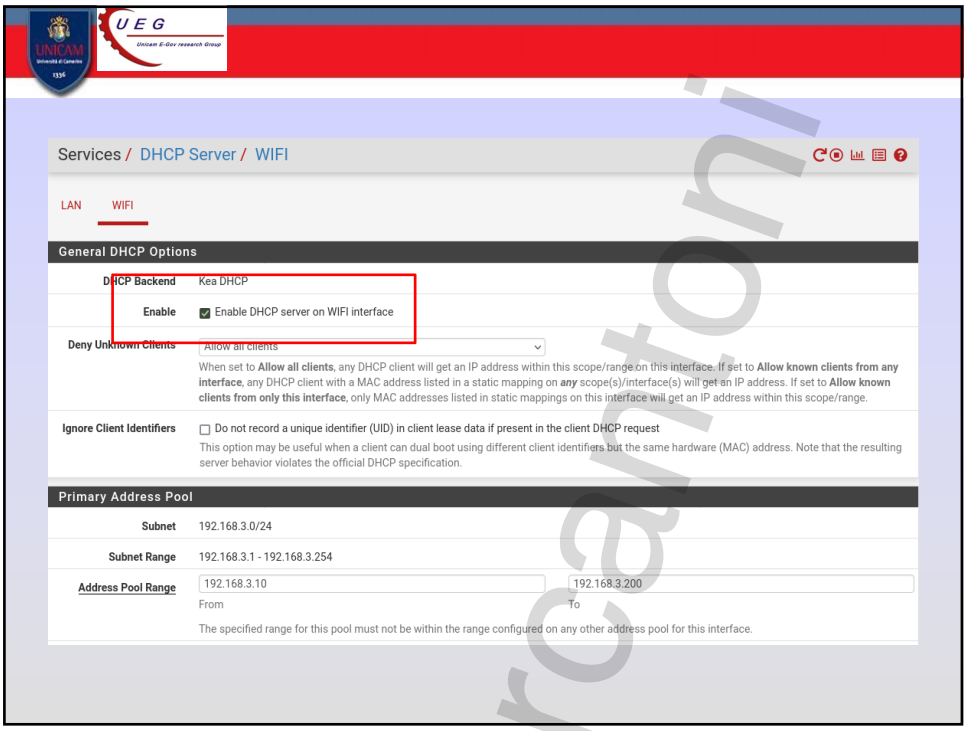
170



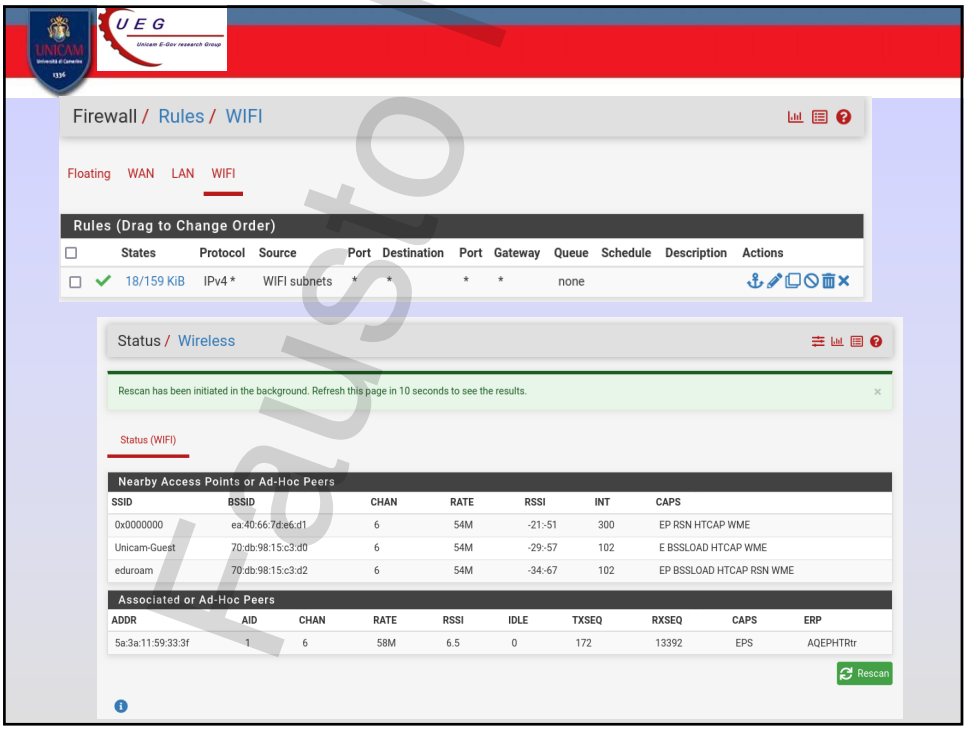
171



172



173

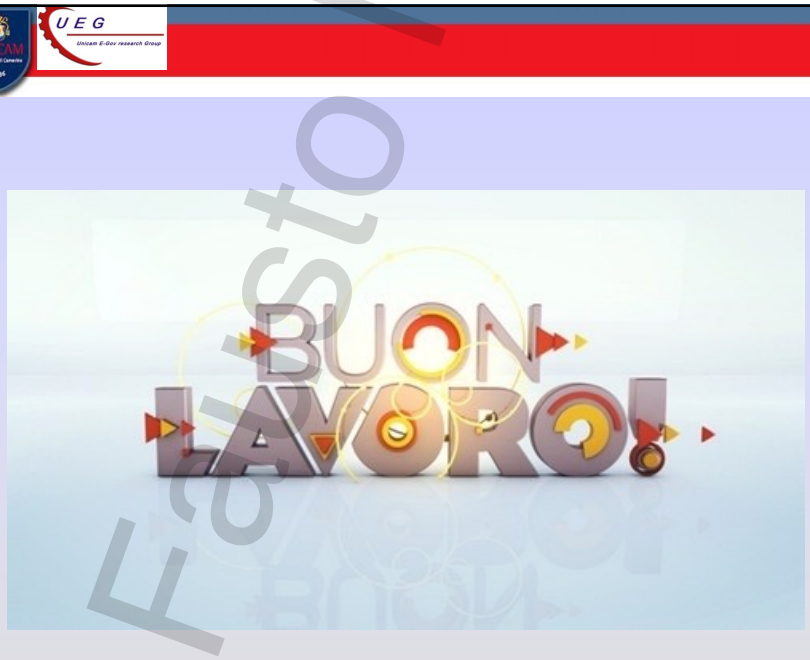


174

How to set up your own OpenVPN server in pfSense

https://www.comparitech.com/blog/vpn-privacy/openvpn-server-pfsense/

175



176

pfSense – Package - antivirus

HAVP antivirus	Network Management	No info, check the forum	0.91_1	Antivirus: HAVP (HTTP Antivirus Proxy) is a proxy with a ClamAV anti-virus scanner. The main aims are continuous, non-blocking downloads and smooth scanning of dynamic and password protected HTTP traffic. Havp antivirus proxy has a parent and transparent proxy mode. It can be used with squid or standalone. And File Scanner for local files.

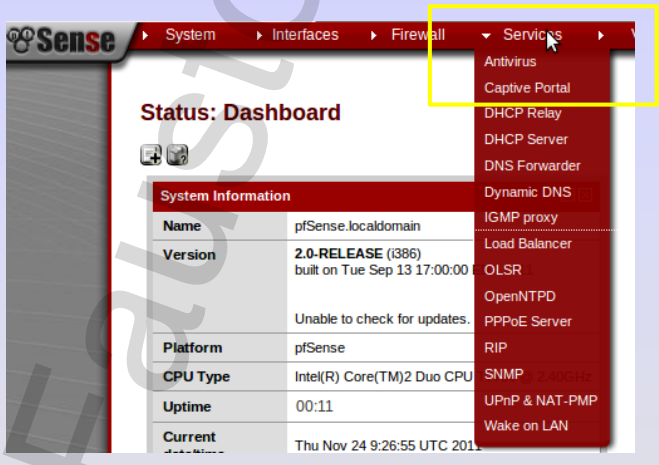
System: Package Manager: Install Package

Available packages | Installed packages | Package Installer

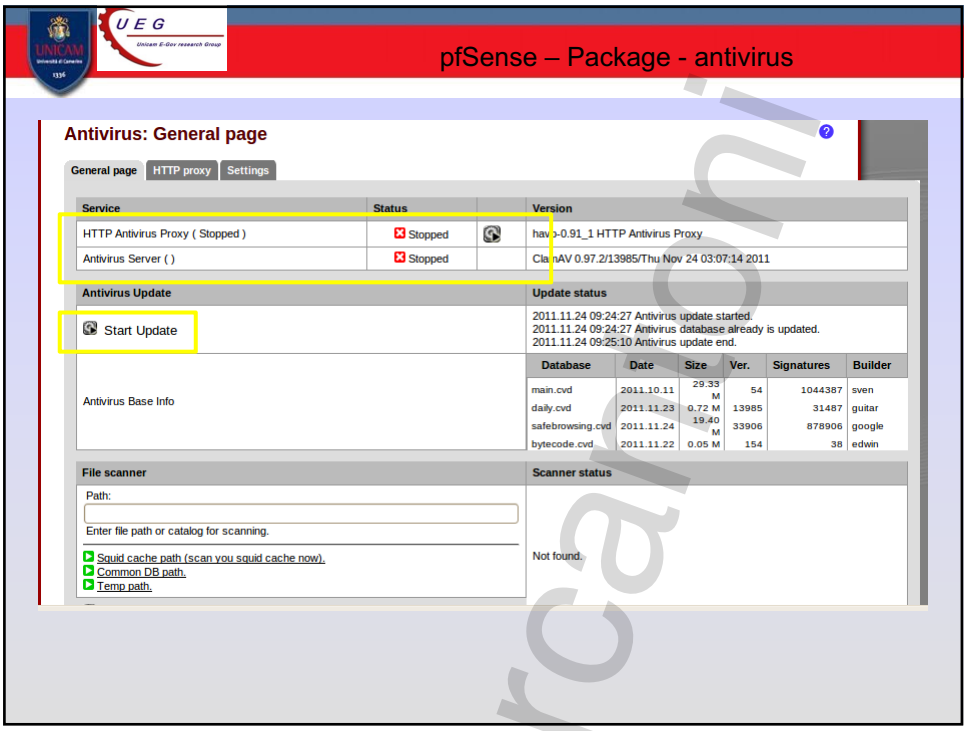
```
Installing HAVP antivirus and its dependencies.

Beginning package installation for HAVP antivirus...
Downloading package configuration file... done.
Saving updated package information... overwrite!
Downloading HAVP antivirus and its dependencies...
Checking for package installation...
 Downloading http://files.pfsense.org/packages/8/All/havp-0.91_1.tbz ...
(extracting)

   Downloading http://files.pfsense.org/packages/8/All/libltdl-2.4.tbz ... 92%
```

177

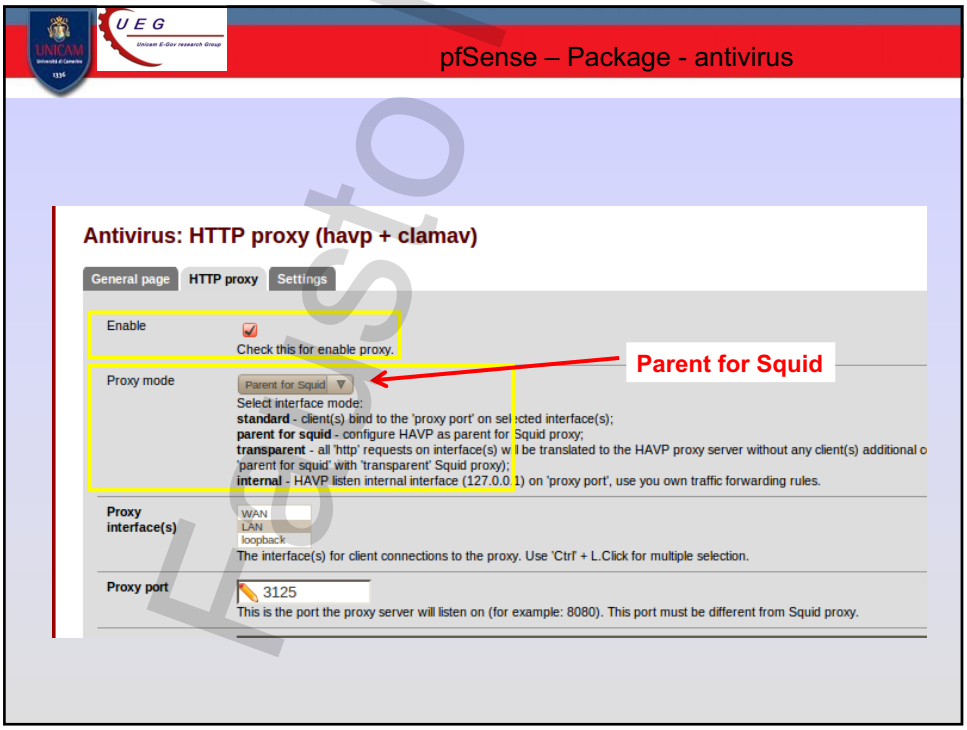
pfSense – Package - antivirus



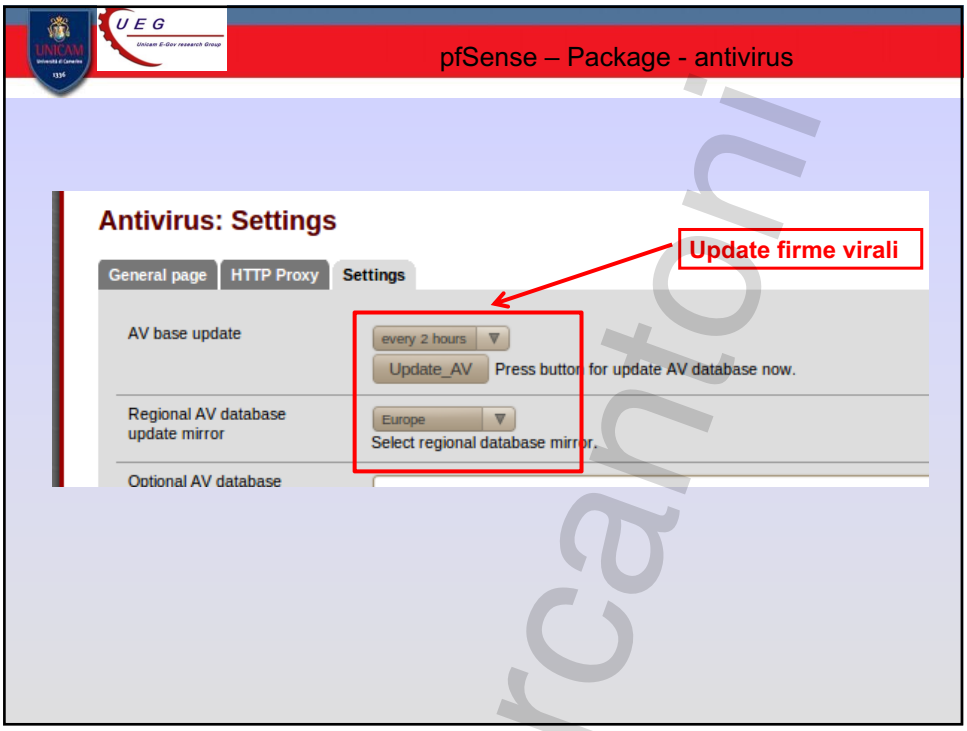
178



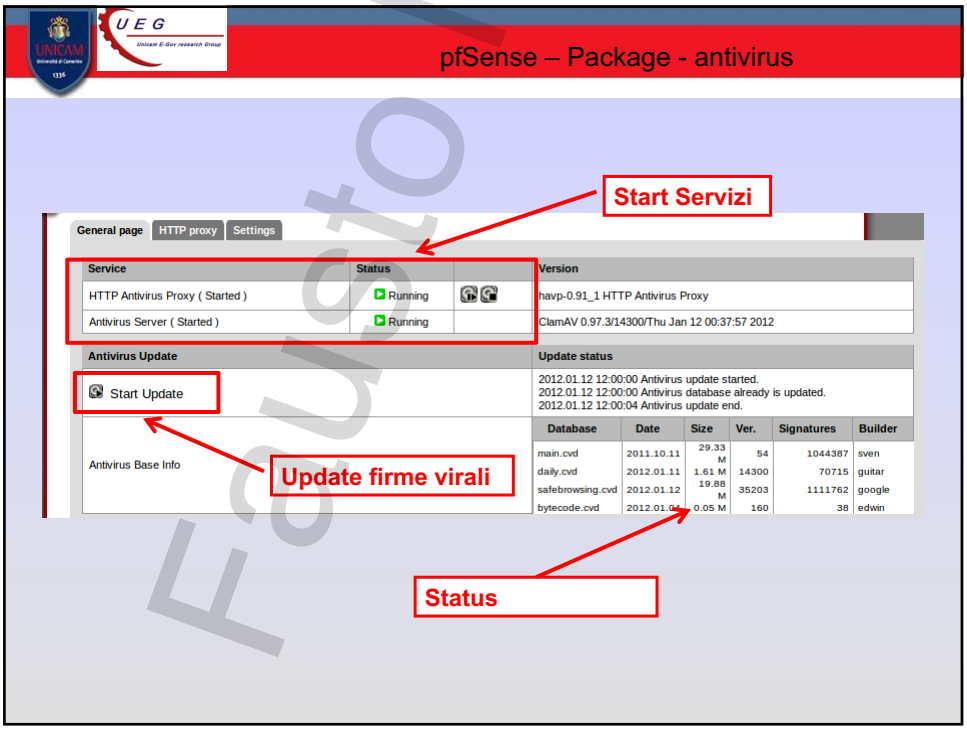
179



180



181



182

pfSense – Package - antivirus

Google test antivirus

http://www.eicar.org/85-0-Download.html

eicar

DOWNLOAD ANTI MALWARE TESTFILE

Download area using the standard protocol http

eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	308 Bytes

Download area using the secure, SSL enabled protocol https

eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	308 Bytes

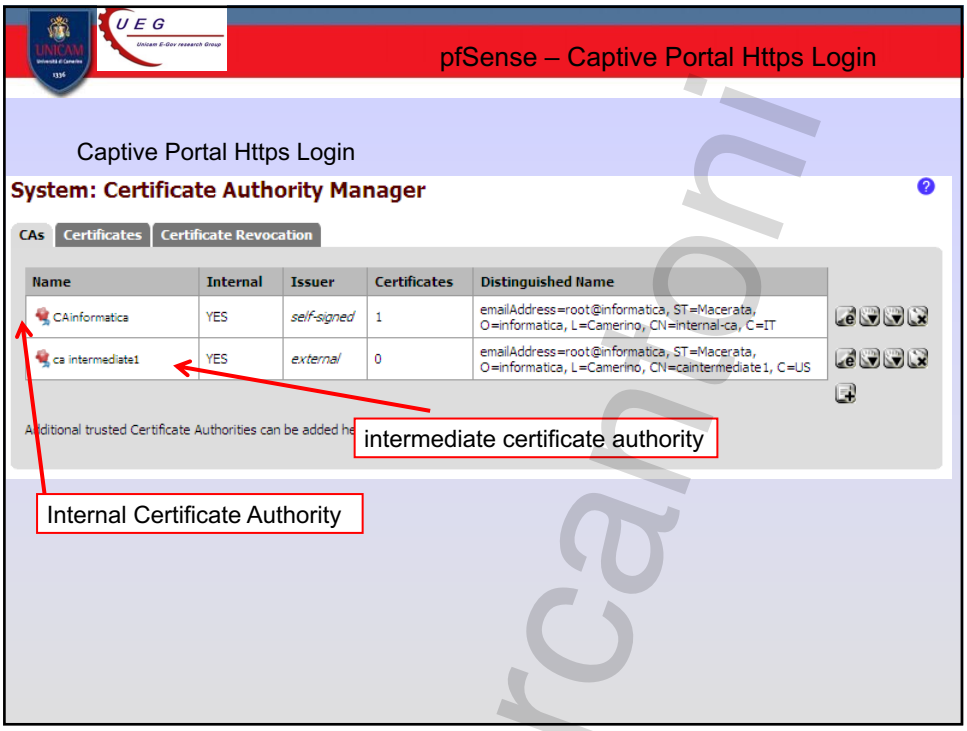
183

pfSense – Captive Portal Https Login

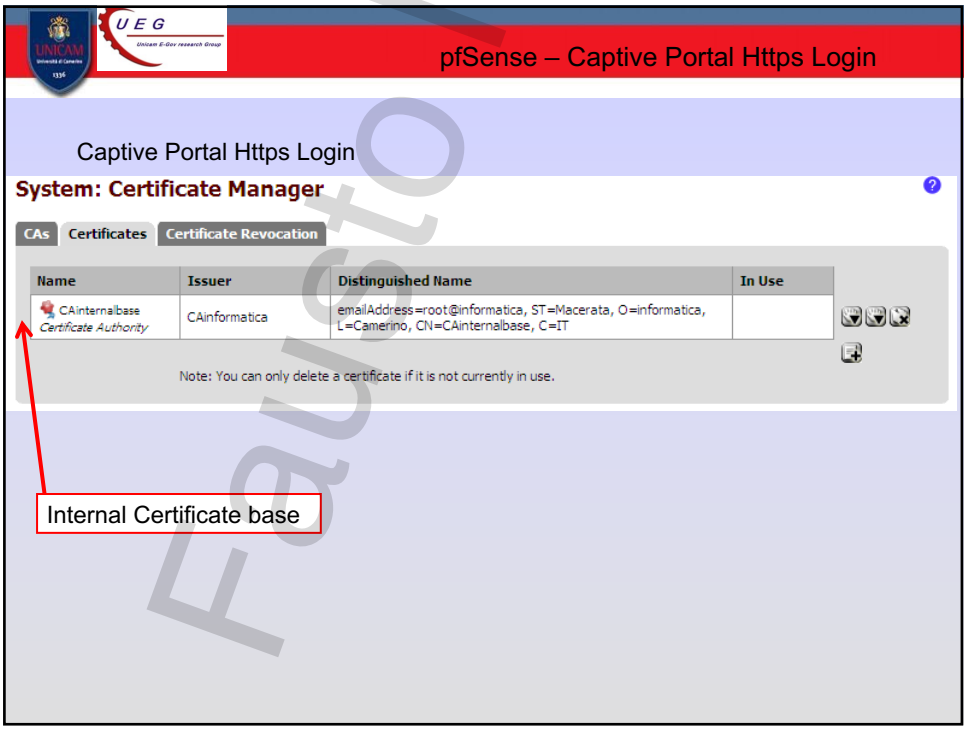
Captive Portal Https Login

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

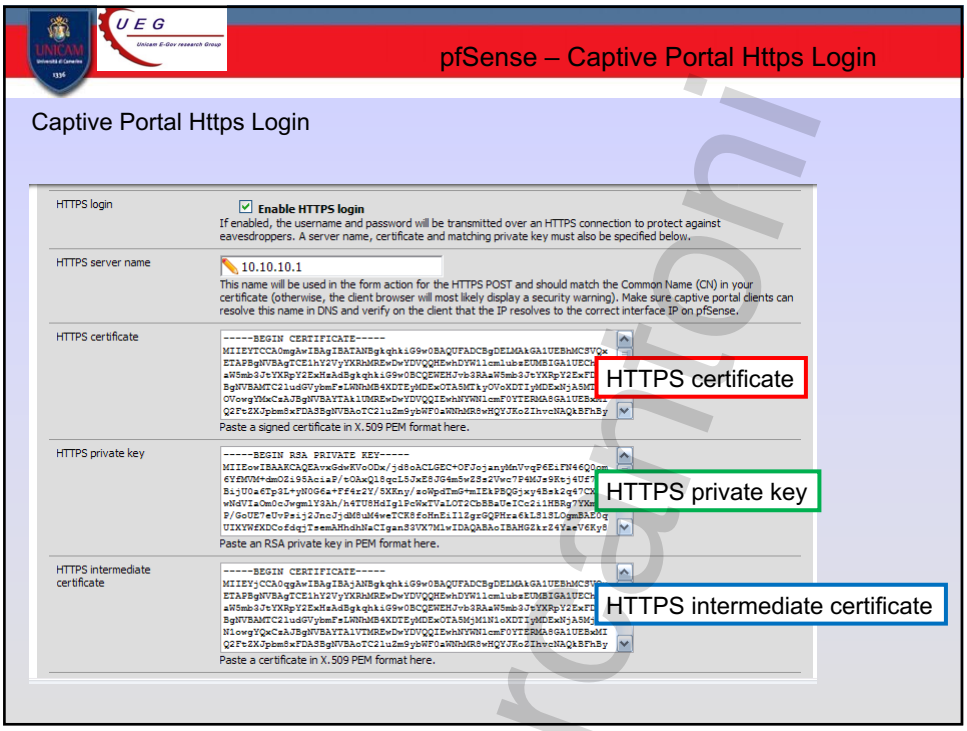
184



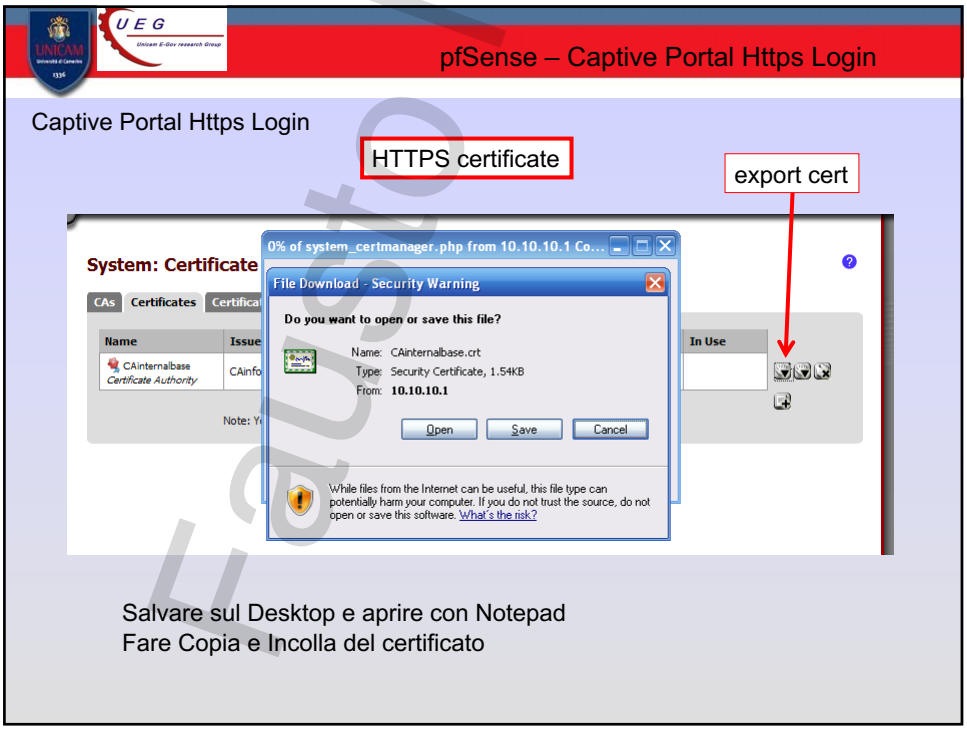
185



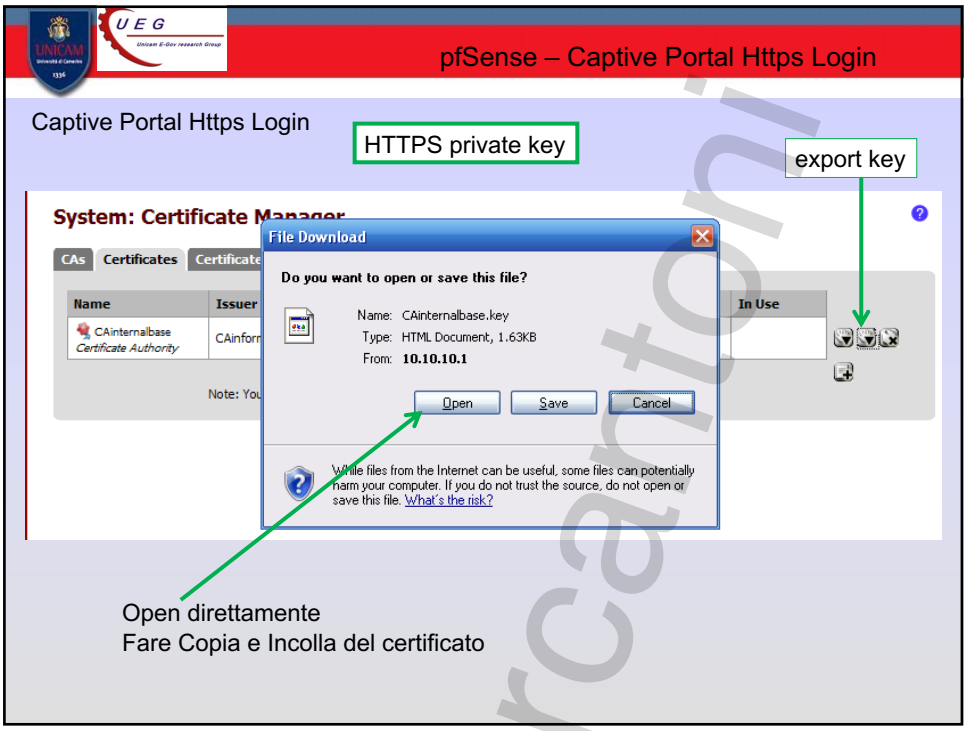
186



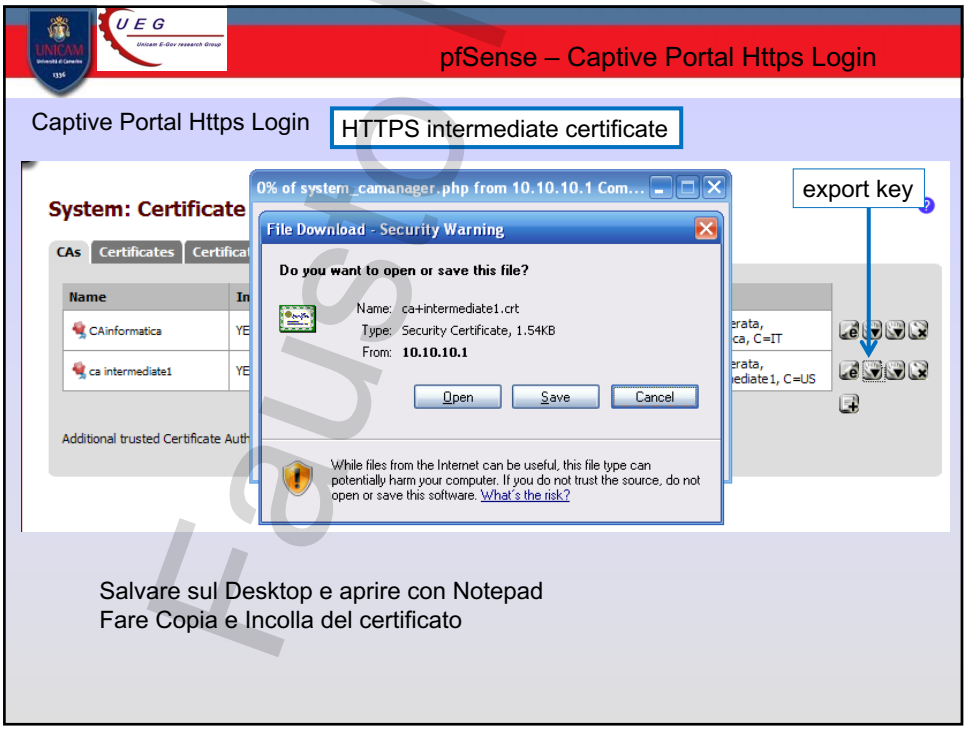
187



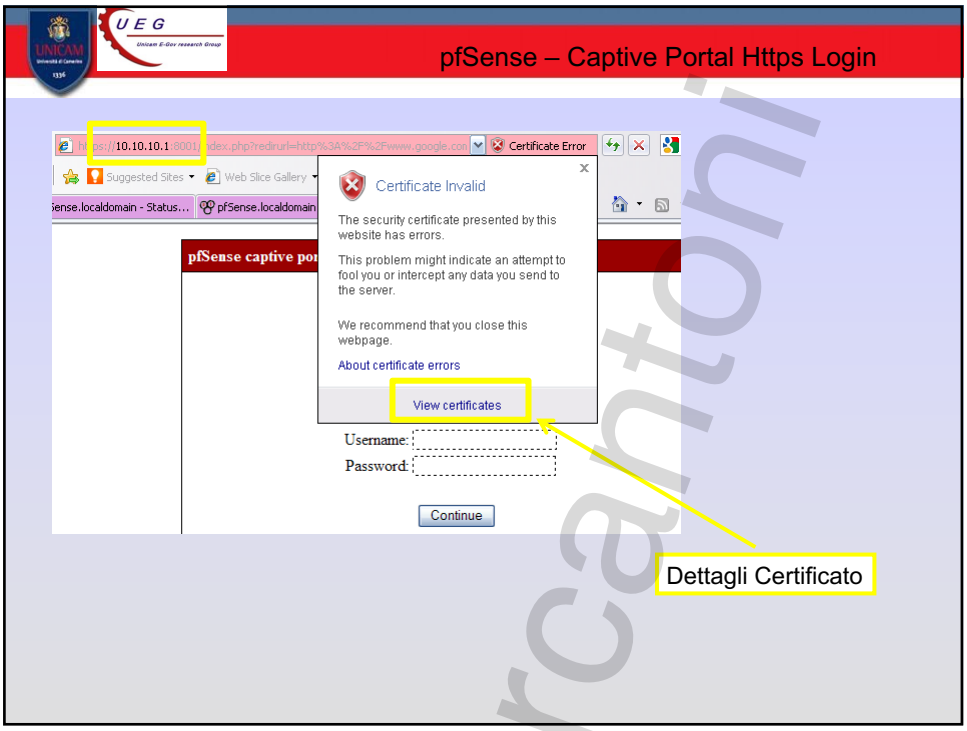
188



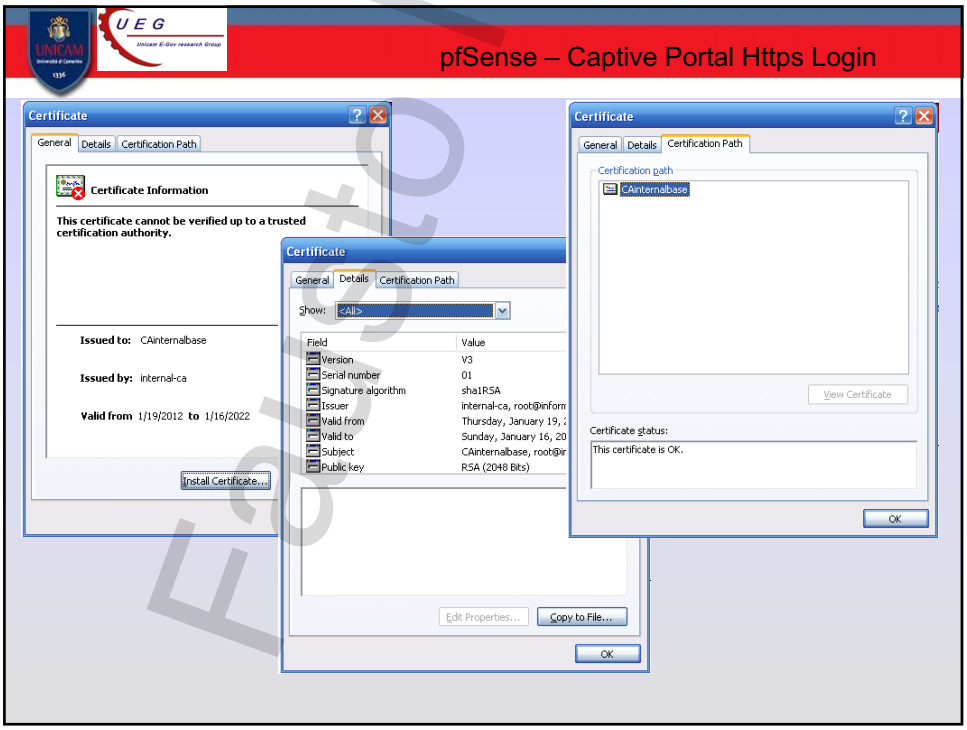
189



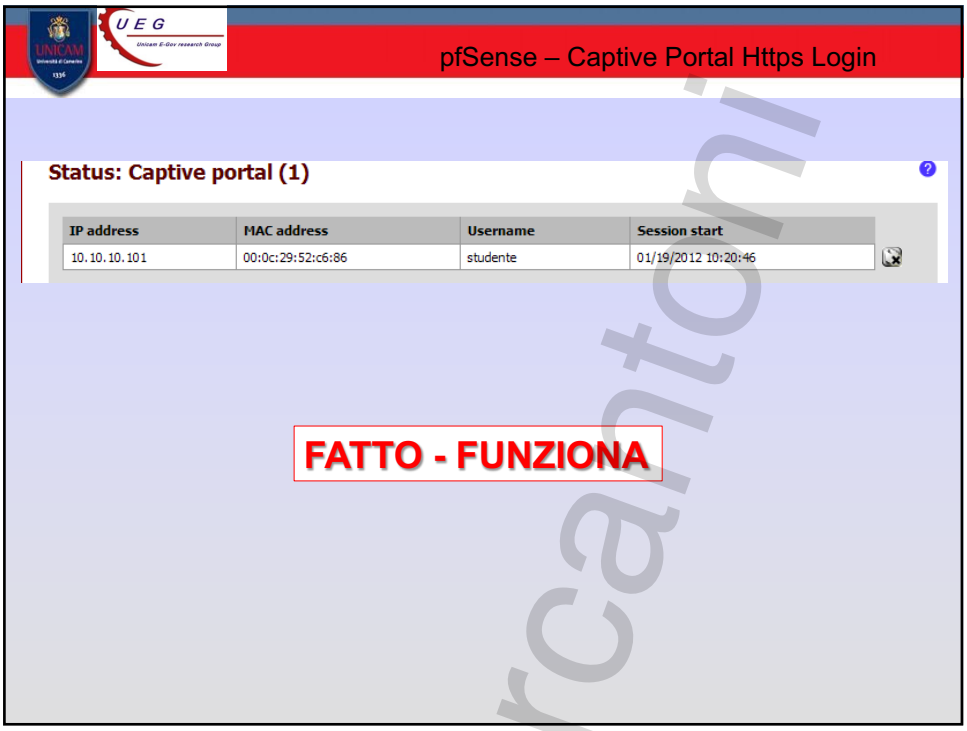
190



191



192



193