



pfSense



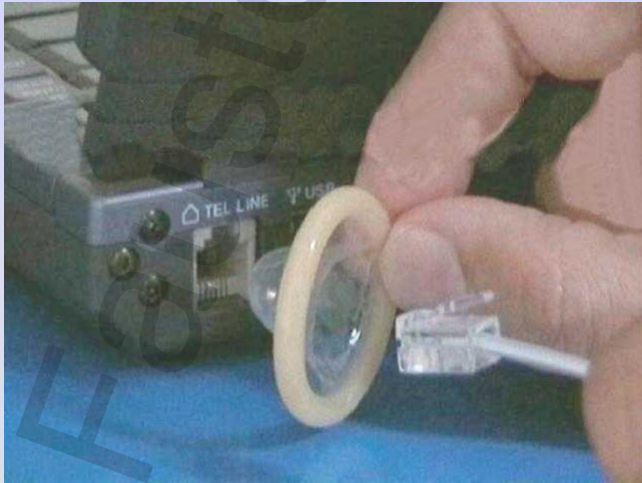
pfSense – Un firewall in 5 minuti
(God help us!)

Fausto Marcantoni
fausto.marcantoni@unicam.it

1



Prevenire è meglio che curare



2

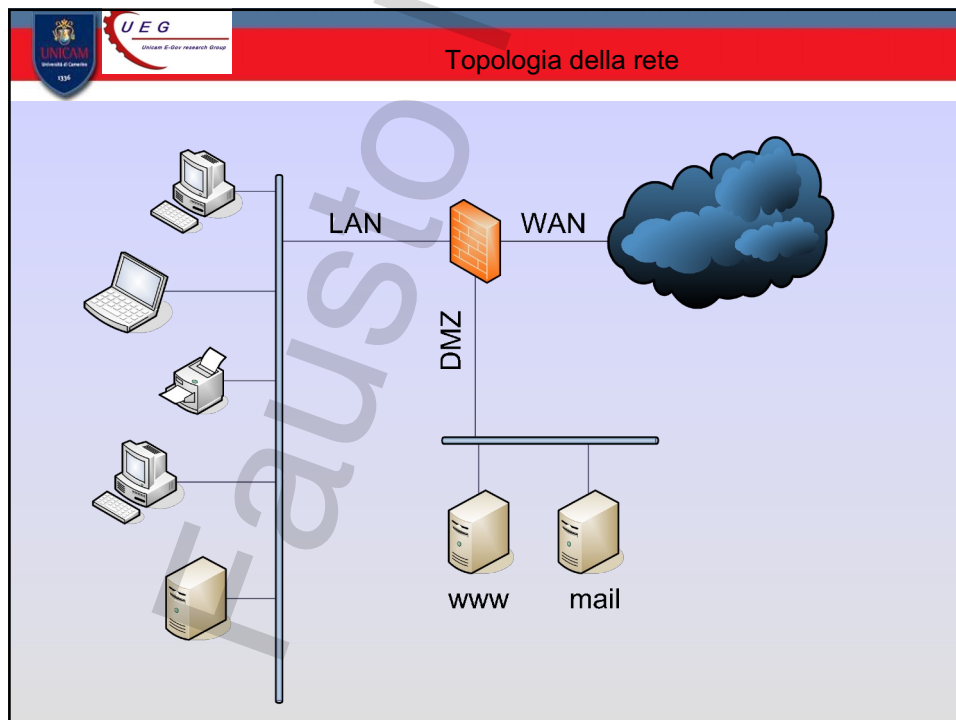


Chi ben comincia ...

- **“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



4



5



6

UNICAM Università di Camerino 1336 UEG Italian E-Dev research Group

pfSense – sito www

<https://pfsense.org/>

pfSense

Get Started Cloud Products Services Support Training Community Download

OPEN SOURCE SECURITY

Secure networks start here.™ With thousands of enterprises using pfSense® software, it is rapidly becoming the world's most trusted open source network security solution.

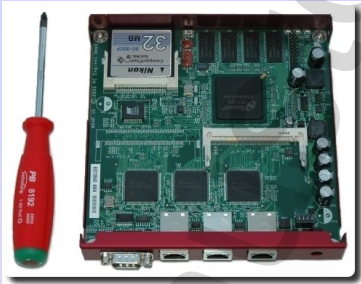
Get Started Now

7

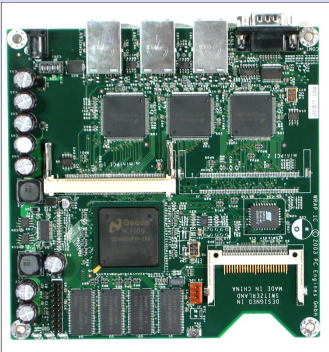
UNICAM Università di Camerino 1336 UEG Italian E-Dev research Group

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

<https://pfsense.org/products/>

Cloud

Netgate 1100

Netgate 2100

Netgate 4200

Netgate 6100

CPU: 8-Core Intel® Xeon® @ 2.0 GHz
RAM: 16 GB DDR4
STORAGE: 512 GB NVMe

1x PCIe 4.0x16 Slot &
1x PCIe 3.0x8 Slot

4x 10 GbE SFP+ Cages
4x 1 GbE SFP Cages
3x 2.5 GbE RJ45 Ports

2x Hot Swappable PSU bays

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

 **FreeBSD®**

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

10




pfSense – 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

UNICAM Università di Camerino 1336 UEG Italian E-Gov research Group

pfSense – software download

Quale file scaricare ???

RELEASE NOTES SOURCE CODE

Version: 2.7.2

Supported by

netgate

DOWNLOAD

13

UNICAM Università di Camerino 1336 UEG Italian E-Gov research Group

pfSense – software download

Quale file scaricare ???

NETGATE INSTALLER

\$0⁰⁰

Shipping calculated at checkout.

Pay in 4 interest-free installments for orders over \$50.00 with shop [Learn more](#)

Customers using Shop Pay Installments might experience a 1-2 day delay in order processing.

Installation Image

SELECT IMAGE TYPE

SELECT IMAGE TYPE

AMD64 Memstick USB (Netgate 1537, 1541, 4100, 4200, 5100, 6100, 7100, 8200, All Other Intel/AMD 64-bit)

AMD64 ISO IPMI/Virtual Machines

AArch64 Memstick ARM (Netgate 1100 and 2100)

Select an Image Type

ADD TO CART FIND A PARTNER

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	23.9	14.0-CURRENT@0c783a37d5d57	RELENG_2
2.7.0	✓	2023-06-29	22.9	14.0-CURRENT@0c59a3b4a5817	RELENG_2

2.6.x

Version	Support	Released	Config Rev	FreeBSD Version	Branch
2.6.0	✗	2022-02-14	22.2	12.3-STABLE@ef1e43d9f2c67	RELENG_2

2.5.x

Version	Support	Released	Config Rev	FreeBSD Version	Branch
2.5.2	✗	2021-07-07	21.7	12.2-STABLE@f440b0cdaa6b7	RELENG_2
2.5.1	✗	2021-04-13	21.5	12.2-STABLE@f440b0cdaa6b7	RELENG_2
2.5.0	✗	2021-02-17	21.4	12.2-STABLE@f440b0cdaa6b7	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@93570467	RELENG_2_4.5
2.4.5	✗	2020-03-26	19.1	11.3-STABLE@93570467	RELENG_2_4.5
2.4.4-p3	✗	2019-09-20	19.1	11.2-RELEASE-p107	RELENG_2_4.4
2.4.4-p2	✗	2019-01-07	18.9	11.2-RELEASE-p47	RELENG_2_4.4
2.4.4-p1	✗	2018-12-03	18.9	11.2-RELEASE-p47	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



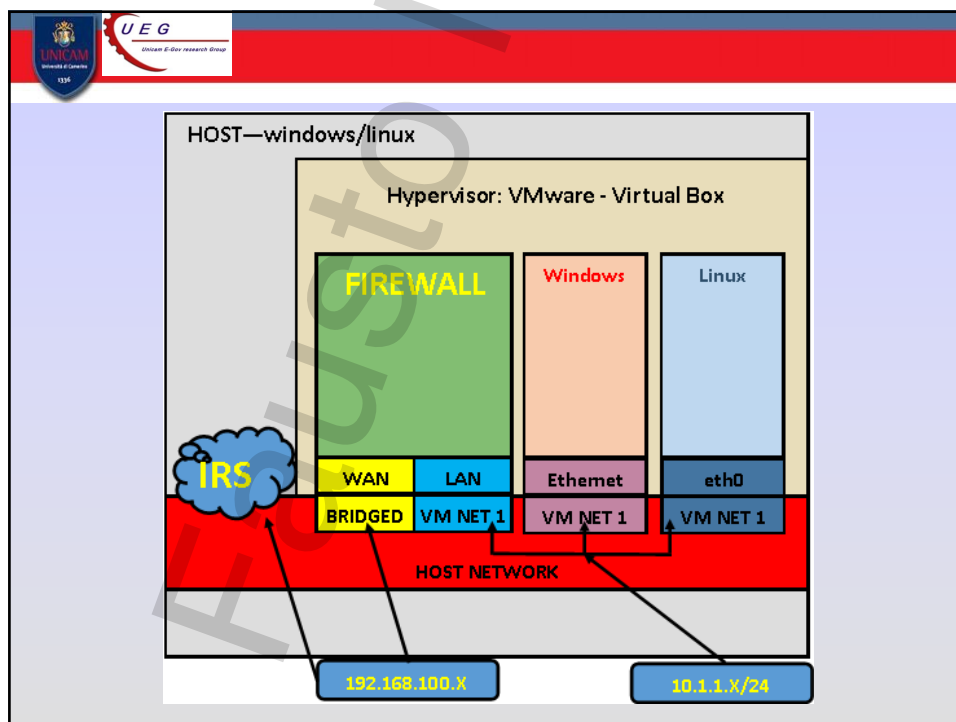

pfSense – installazione

- 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

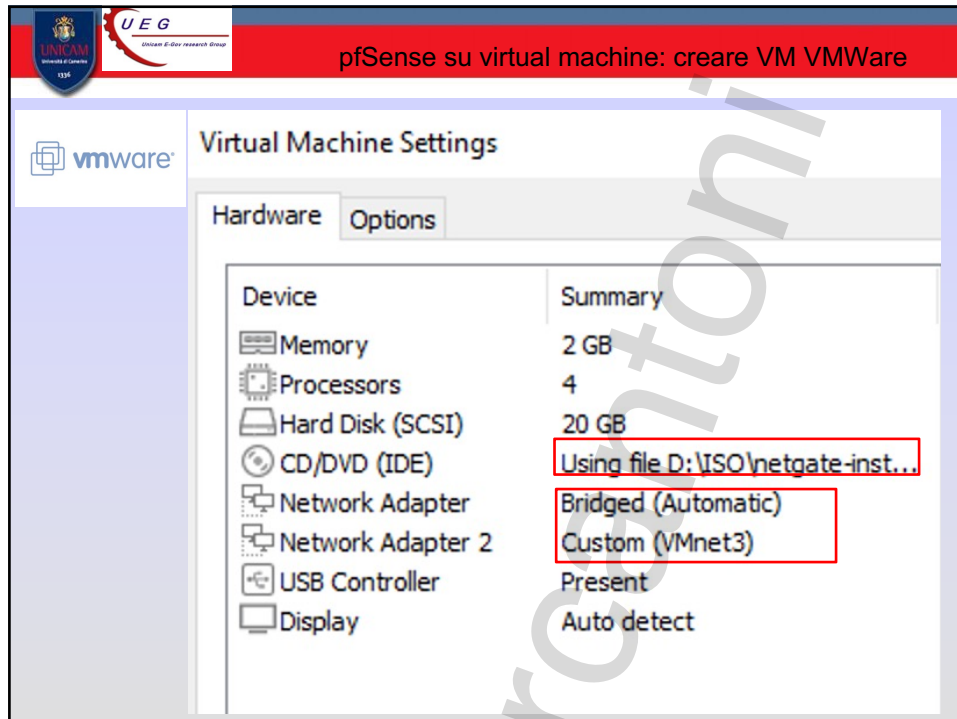
Installation Guides

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

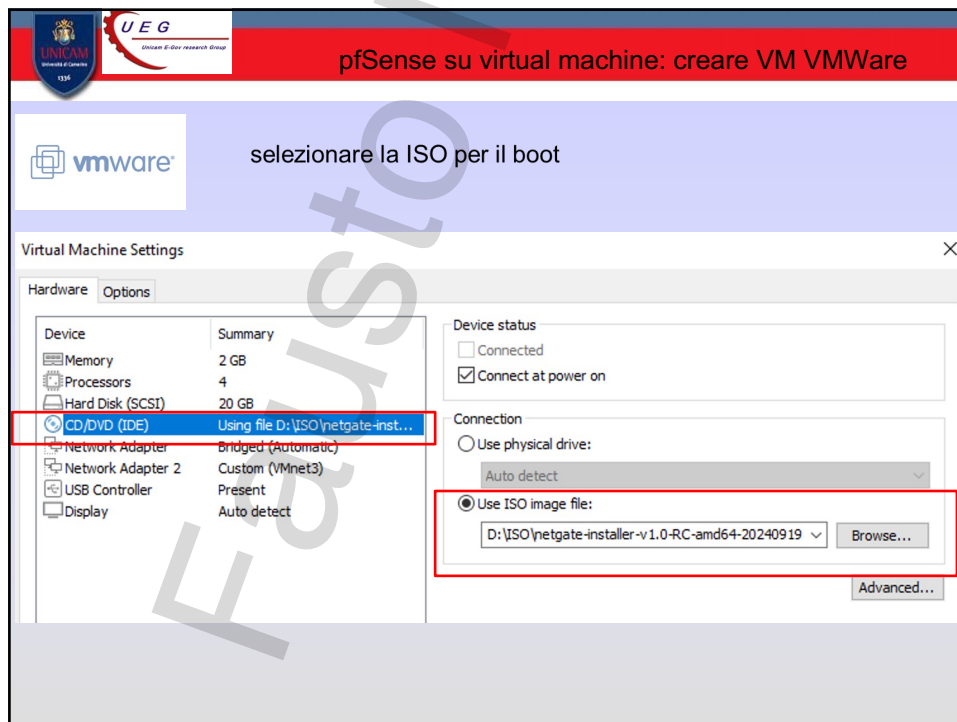
17



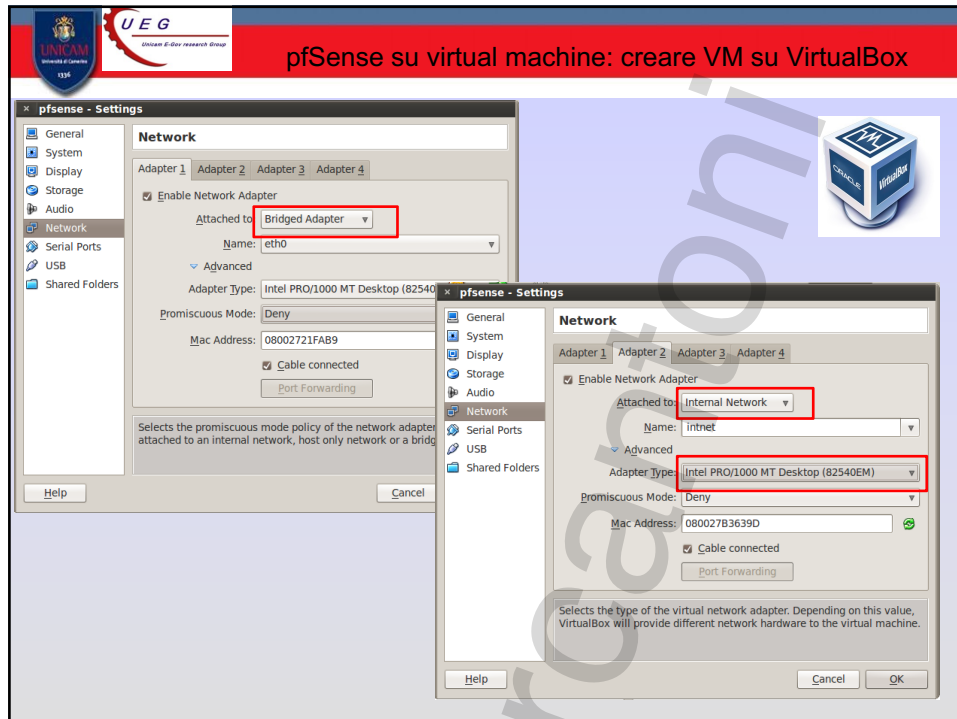
18



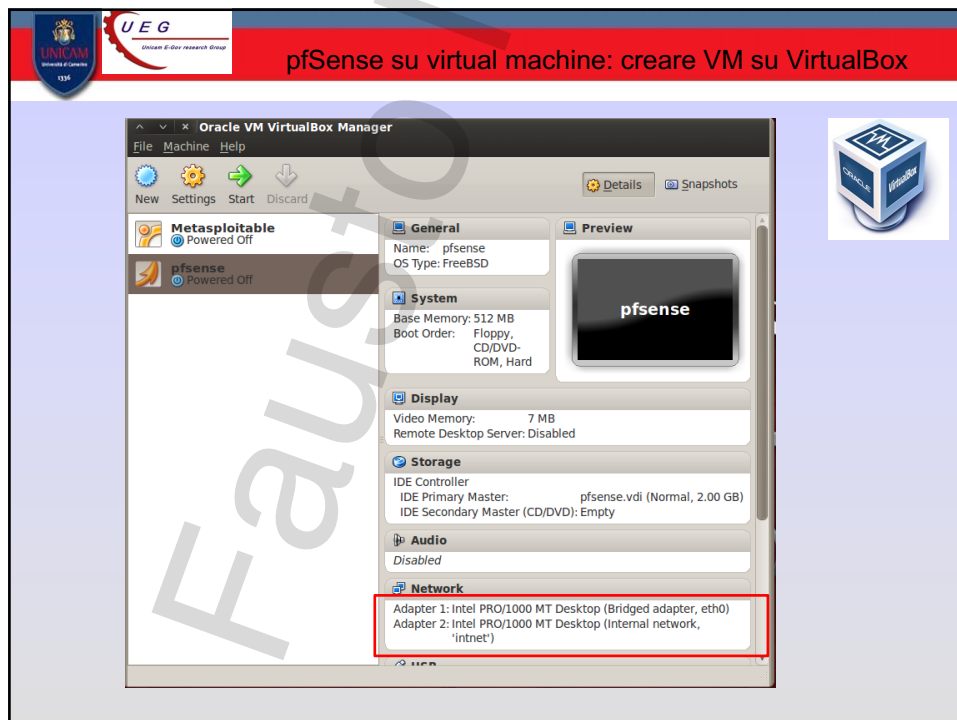
19



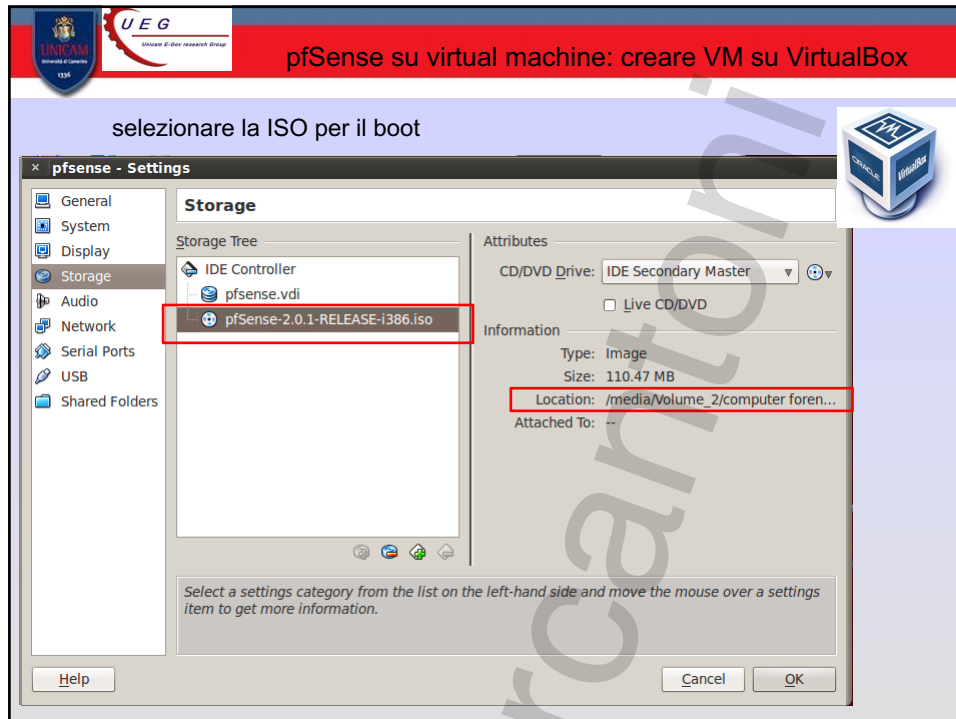
20



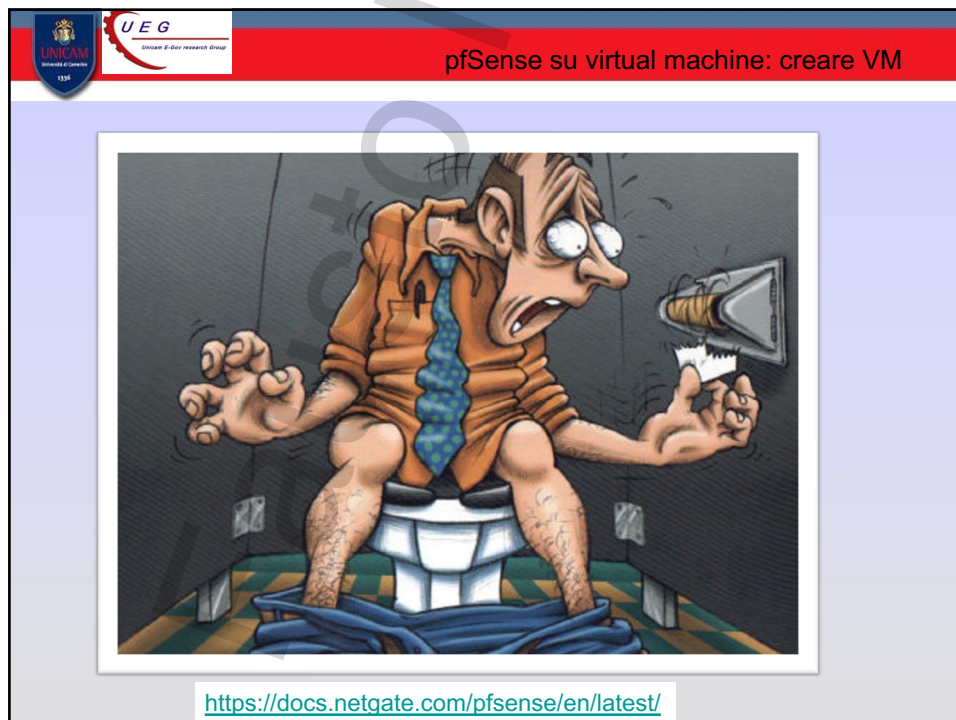
21



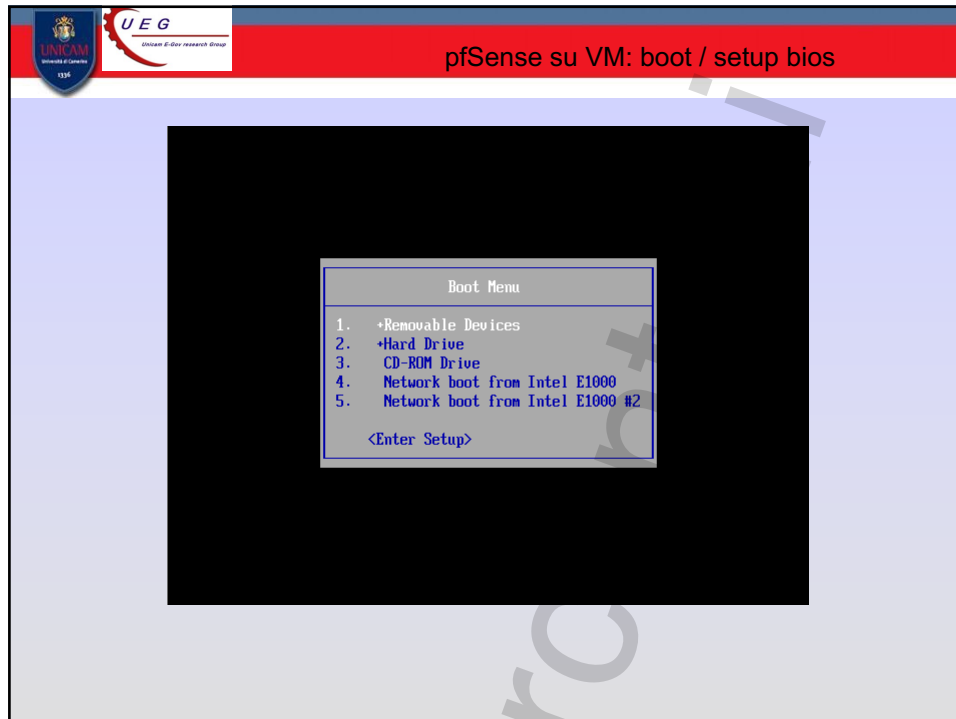
22



23



24



25

The screenshot shows a VM window titled "pfSense su VM: boot". The main text reads: "non riesco ad entrare nel BIOS: è troppo veloce" (I can't enter the BIOS: it's too fast).

Below this, a message box says: "Re: Cannot press ESC to get into BIOS fast enough".

The text continues: "Edit your .vmx file and add the line:"

```

bios.bootDelay = "5000"

```

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

```

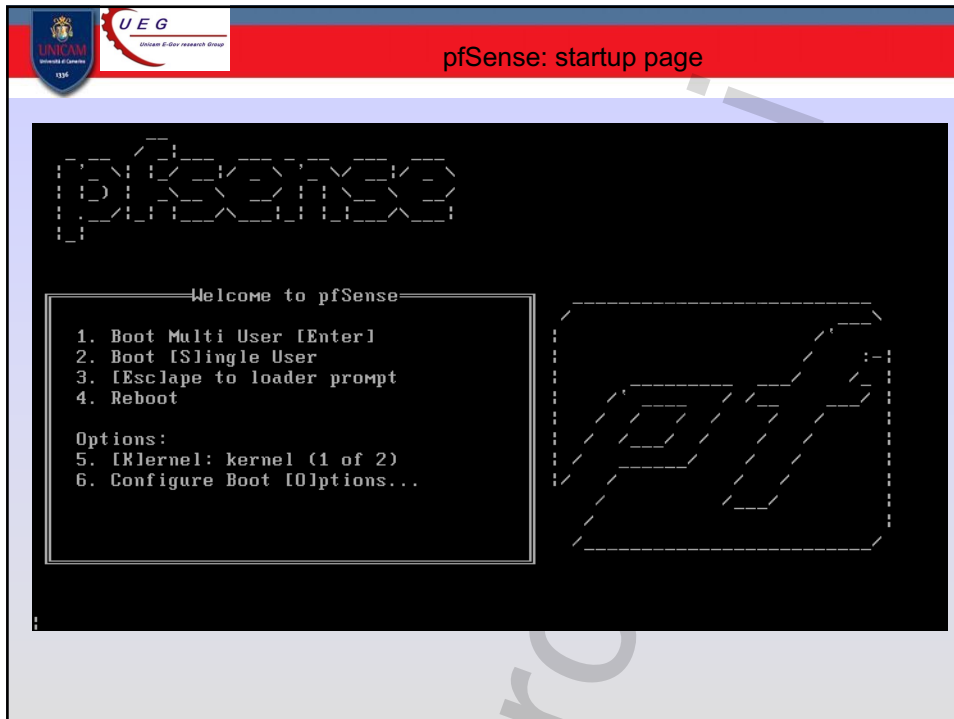
bios.forceSetupOnce = "TRUE"

```

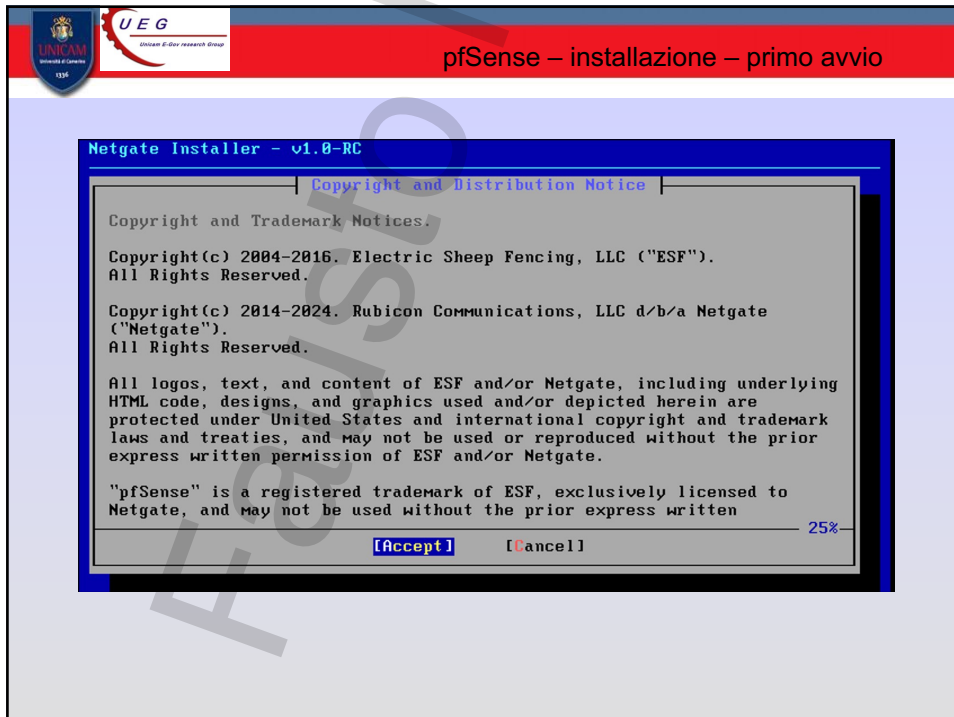
to make the VM enter the BIOS setup at the next boot.

At the bottom right, there is a Google search bar with the text "vmware bios delay" entered.

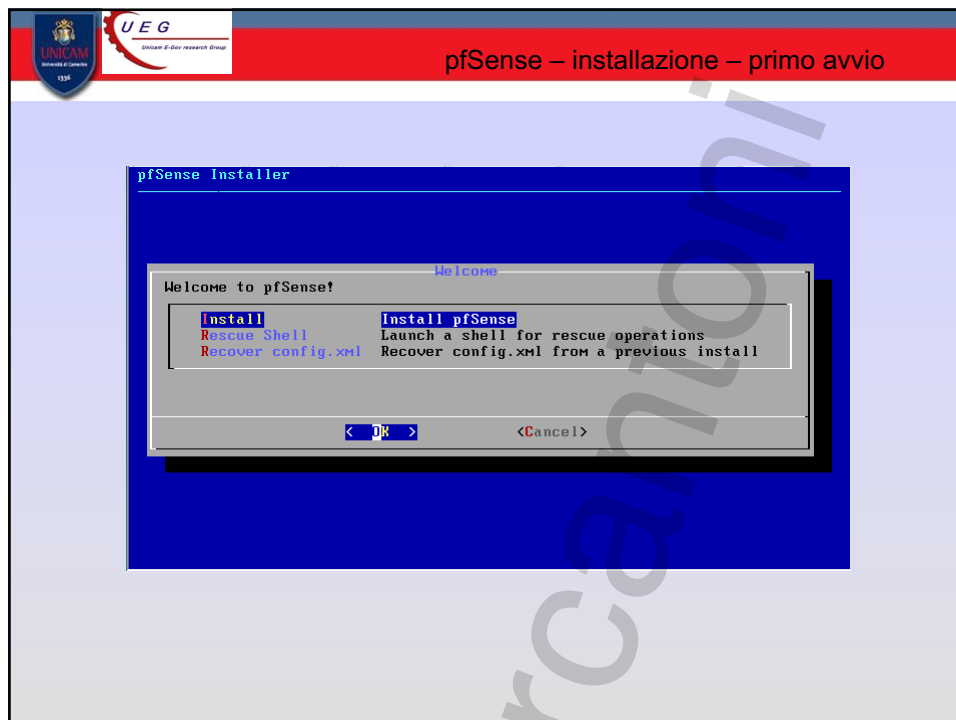
26



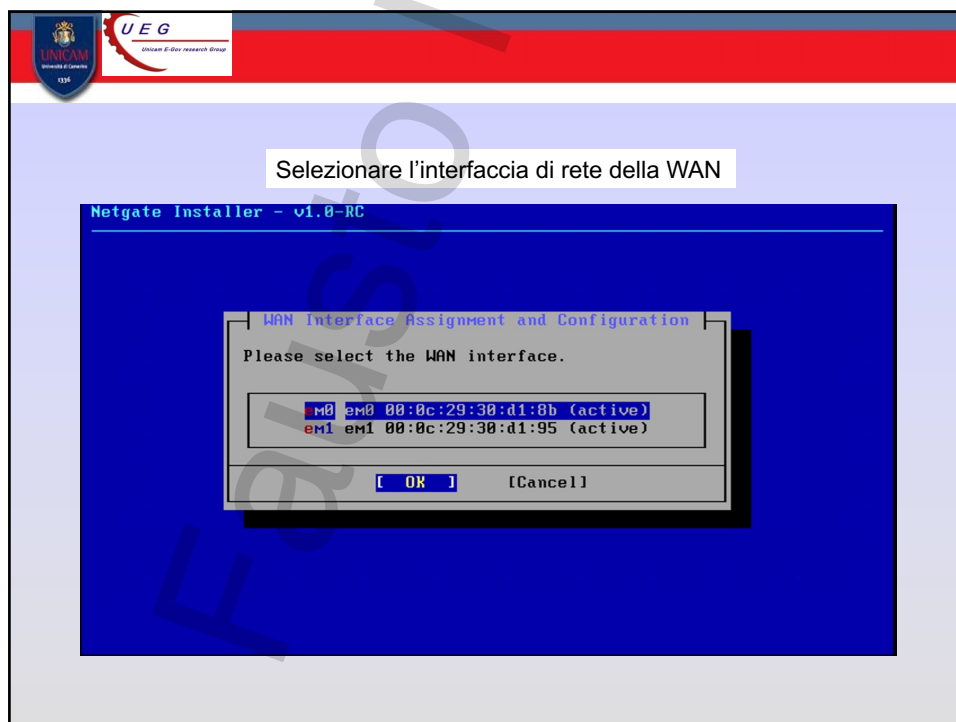
27



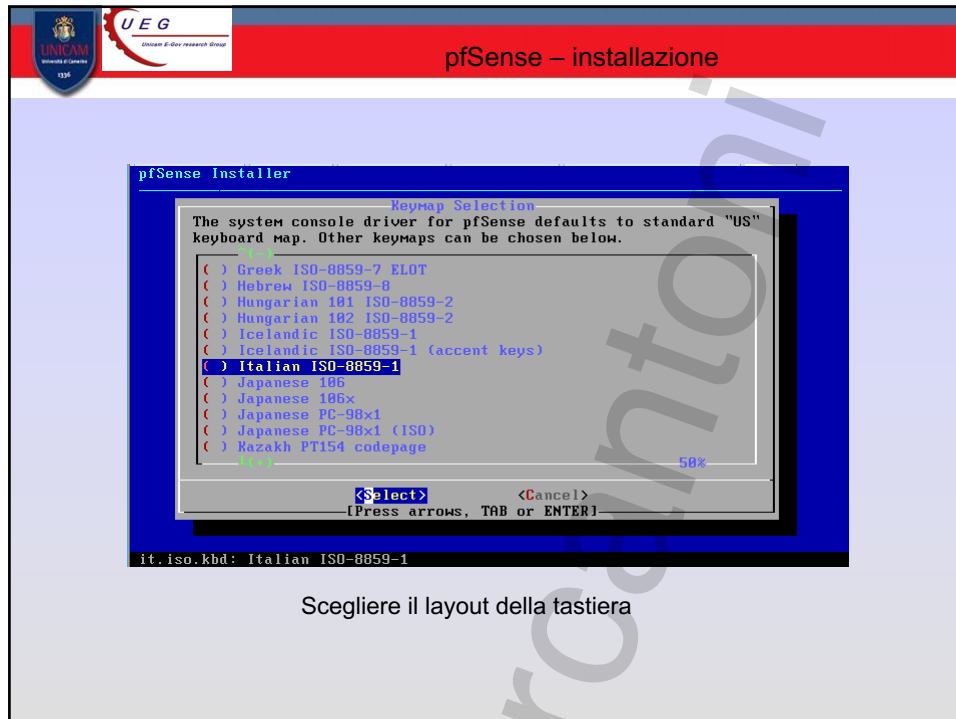
28



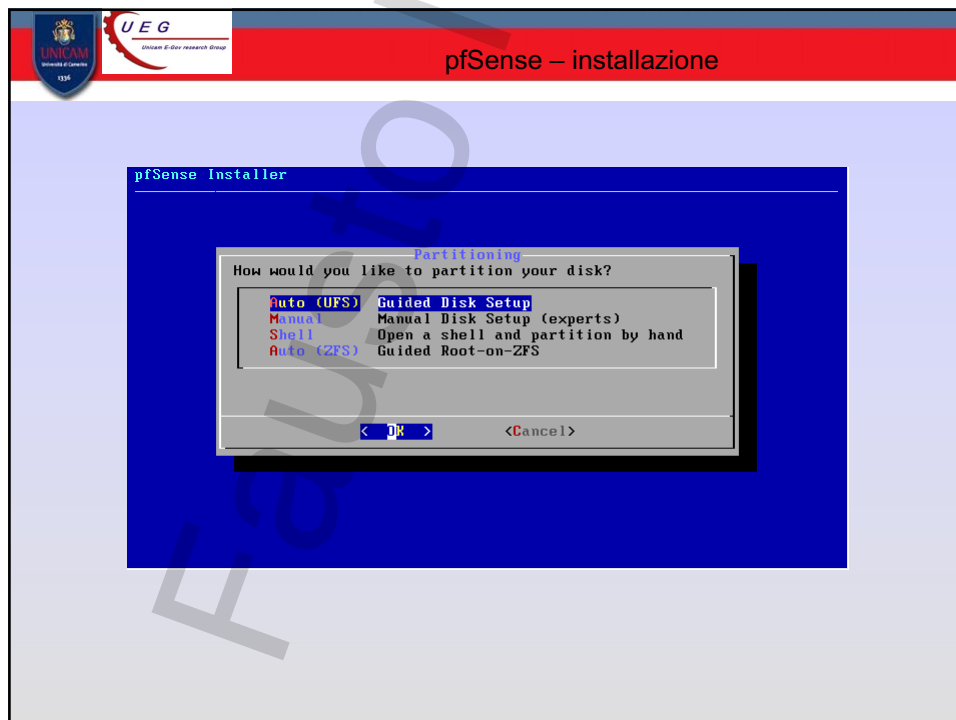
29



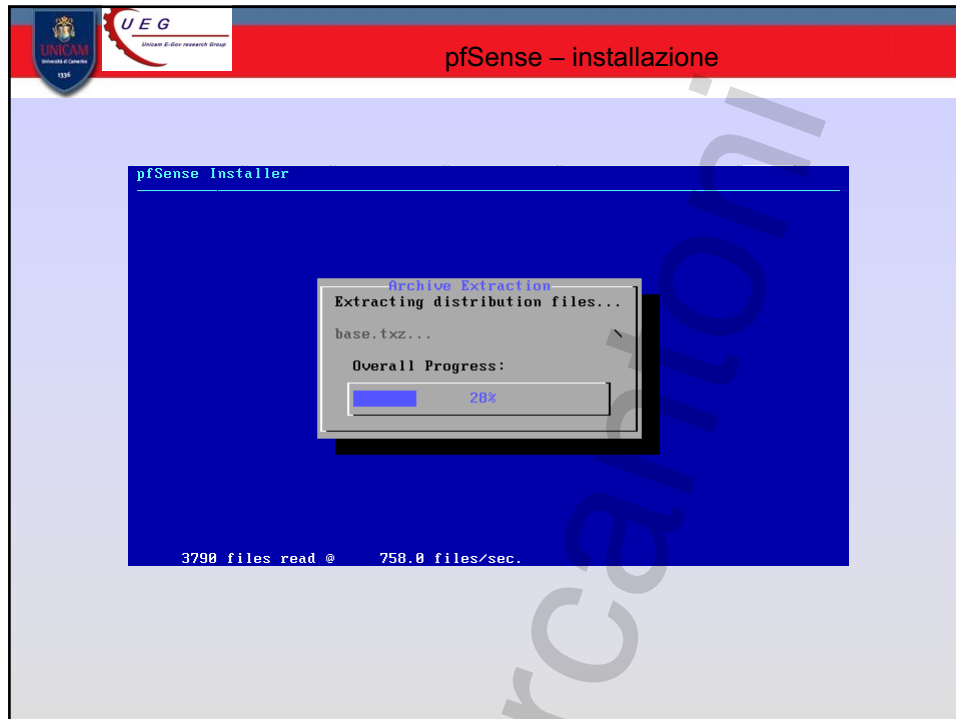
30



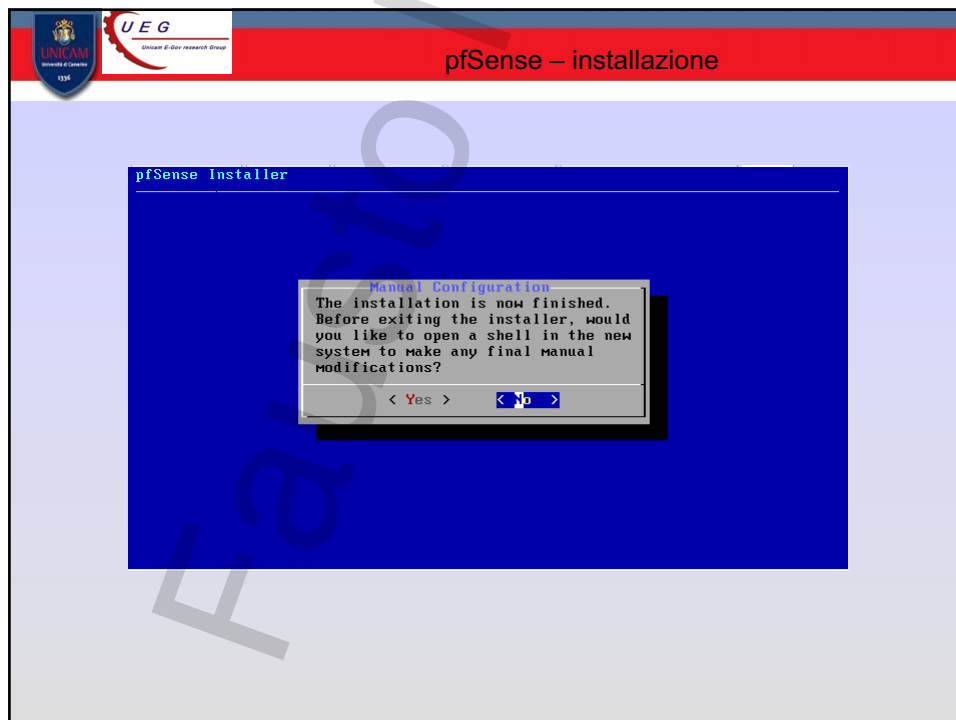
31



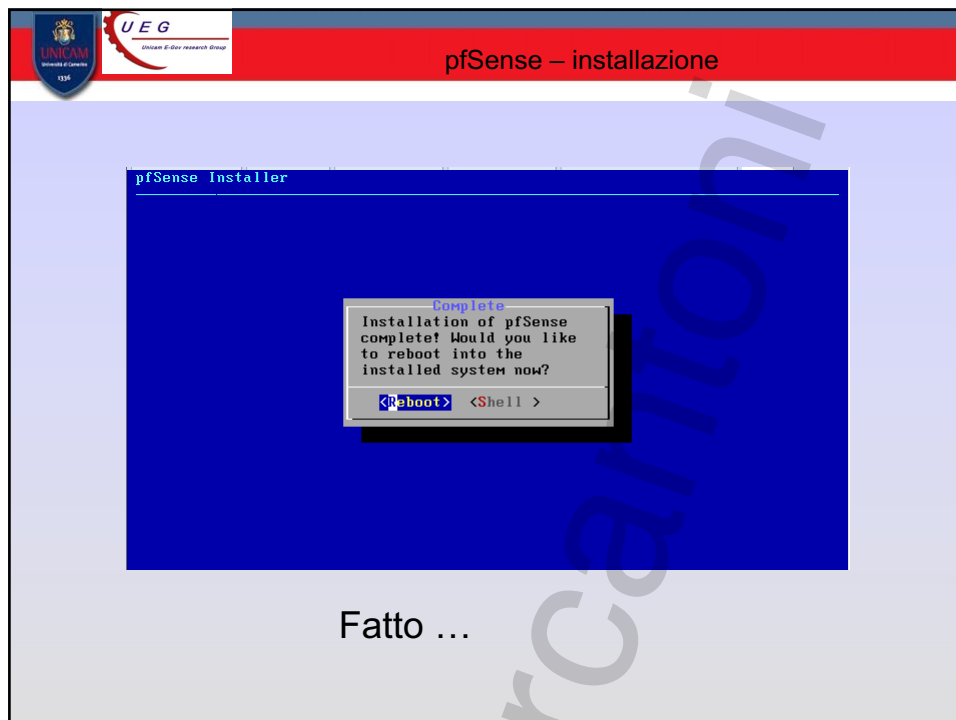
32



33



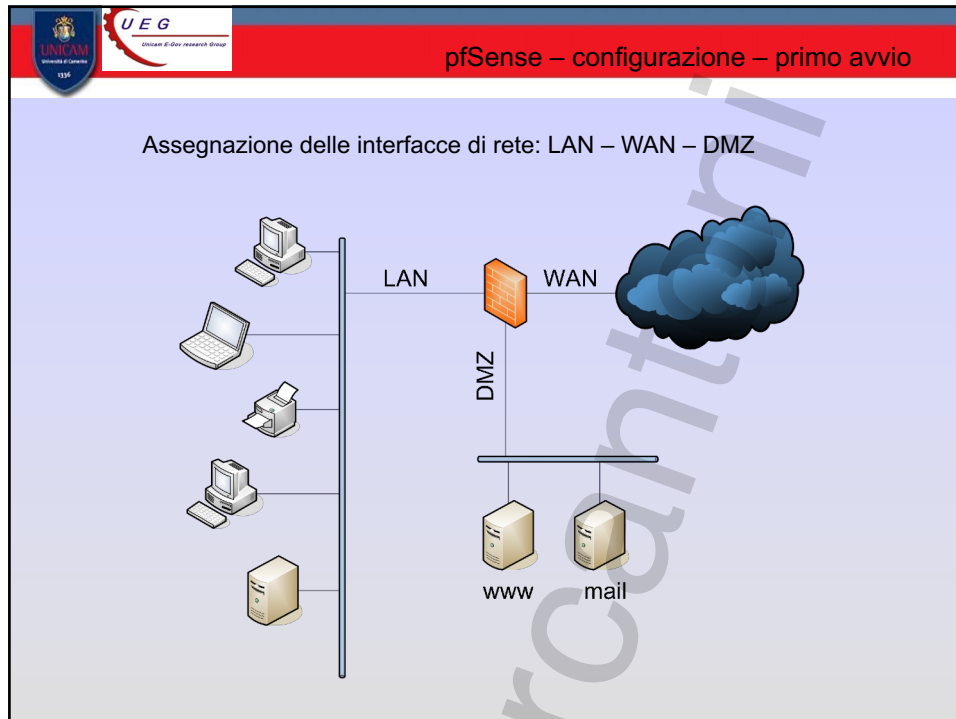
34



35



36



37

UNICAM
Università di Camerino
1336

UEG
University of Engineering and Graphics

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

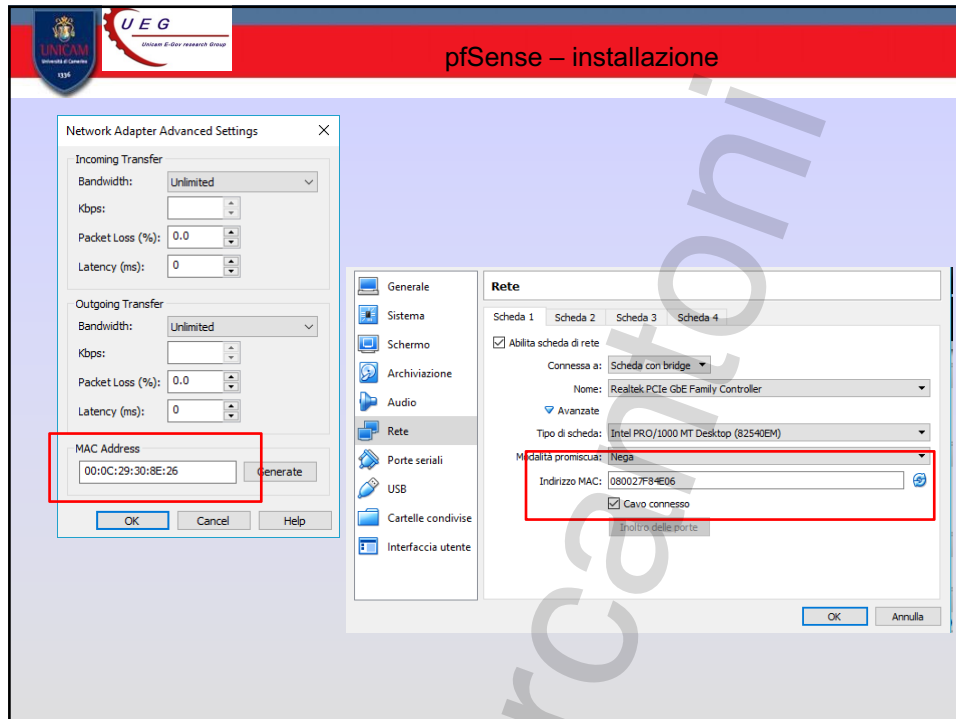
Do you want to set up VLANs first?

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]?
```

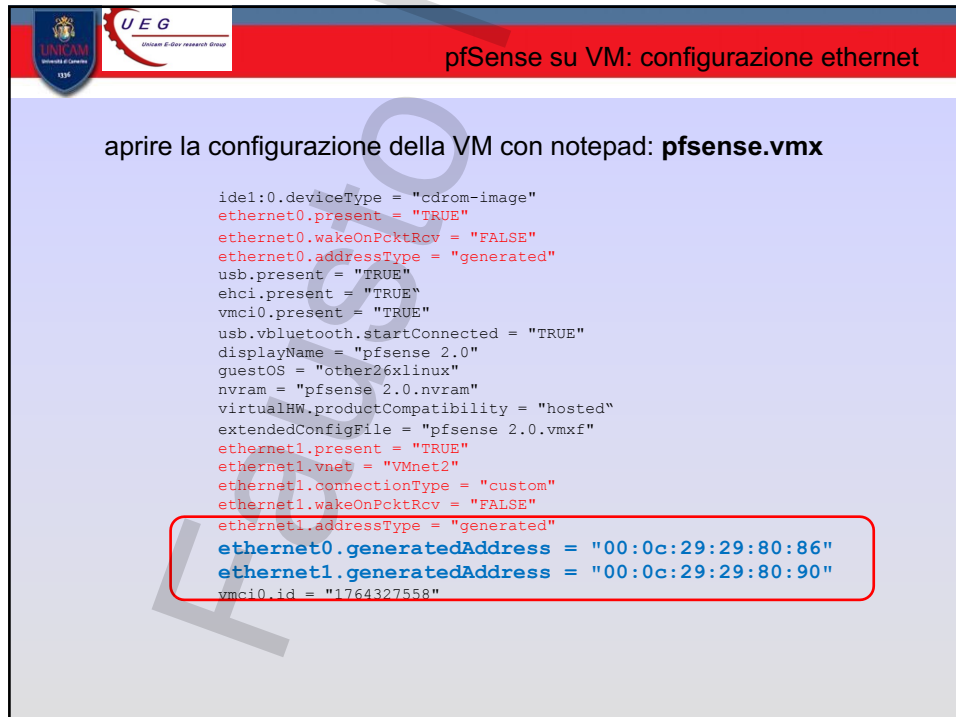
nomi e stato delle interfacce

MAC address delle interfacce

38



39



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.

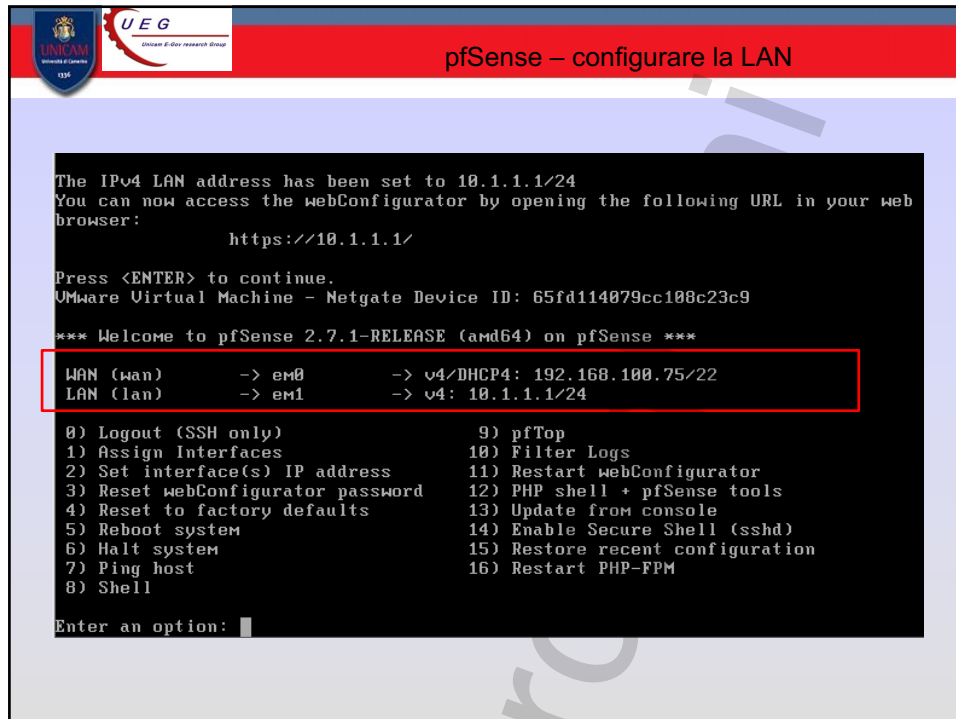
        If you do not have at least 1 *REAL* network interface card(s)
        or one interface with multiple VLANs then pfSense
        *WILL NOT* function correctly.

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.

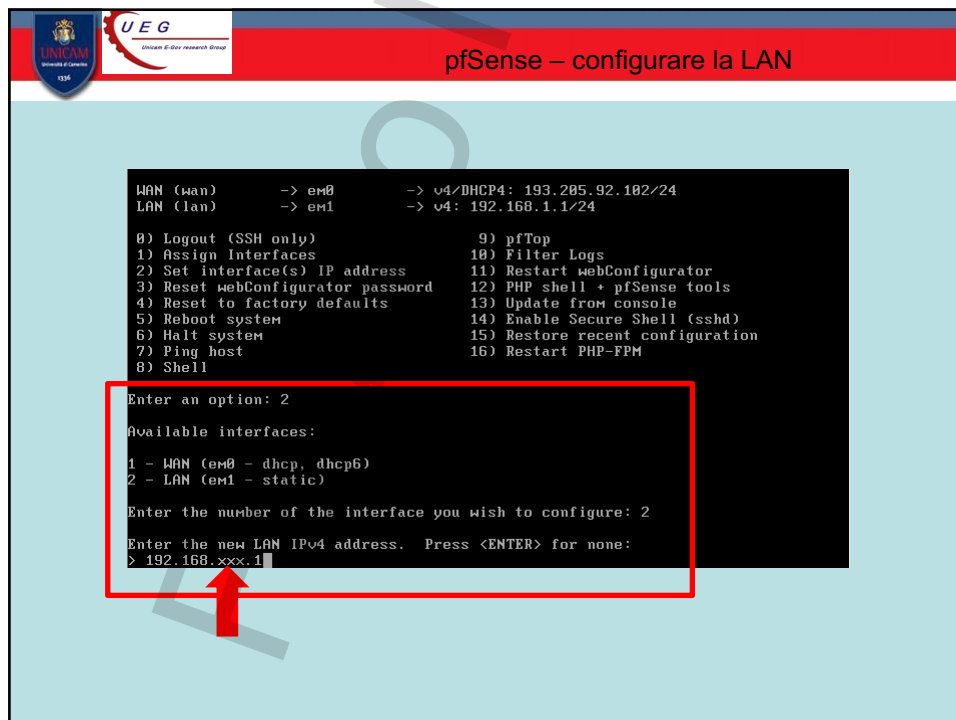
Enter the WAN interface name or 'a' for auto-detection: a
  
```

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

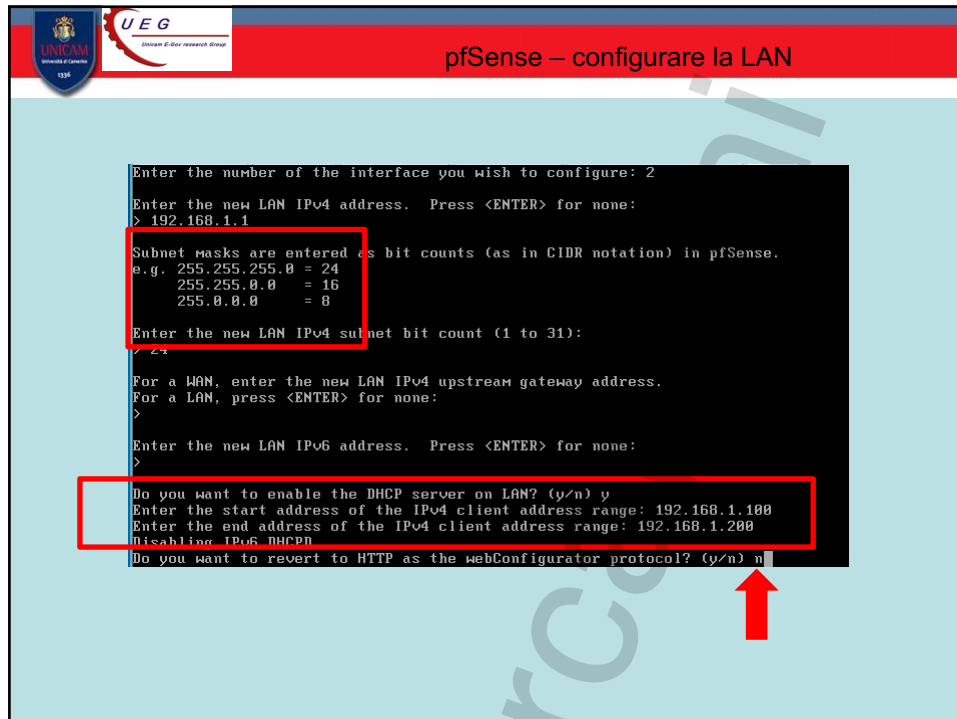
42



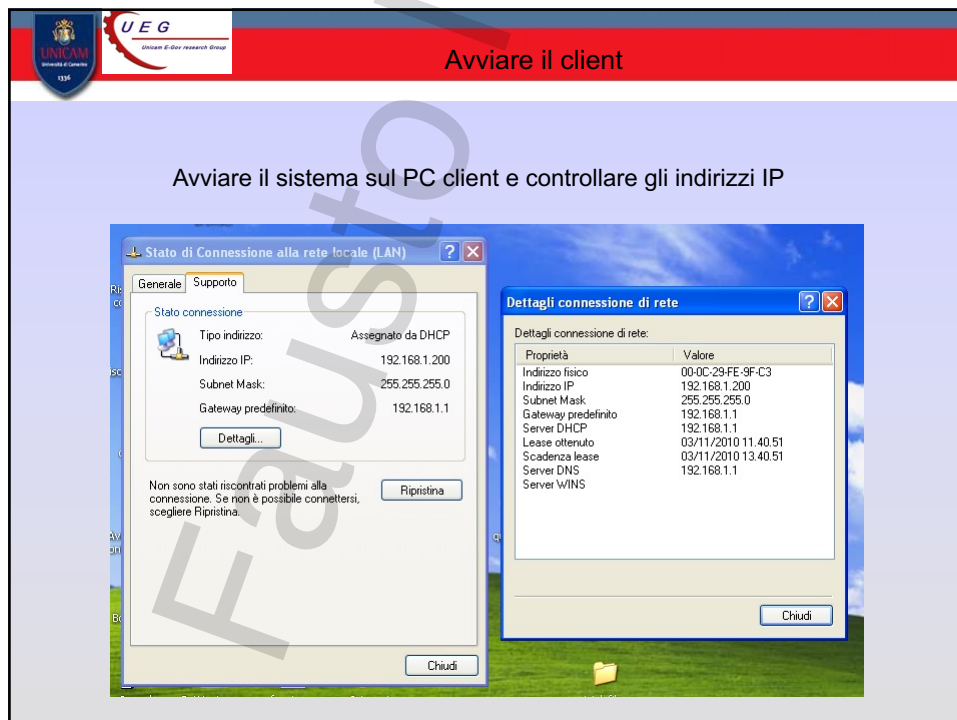
43



44



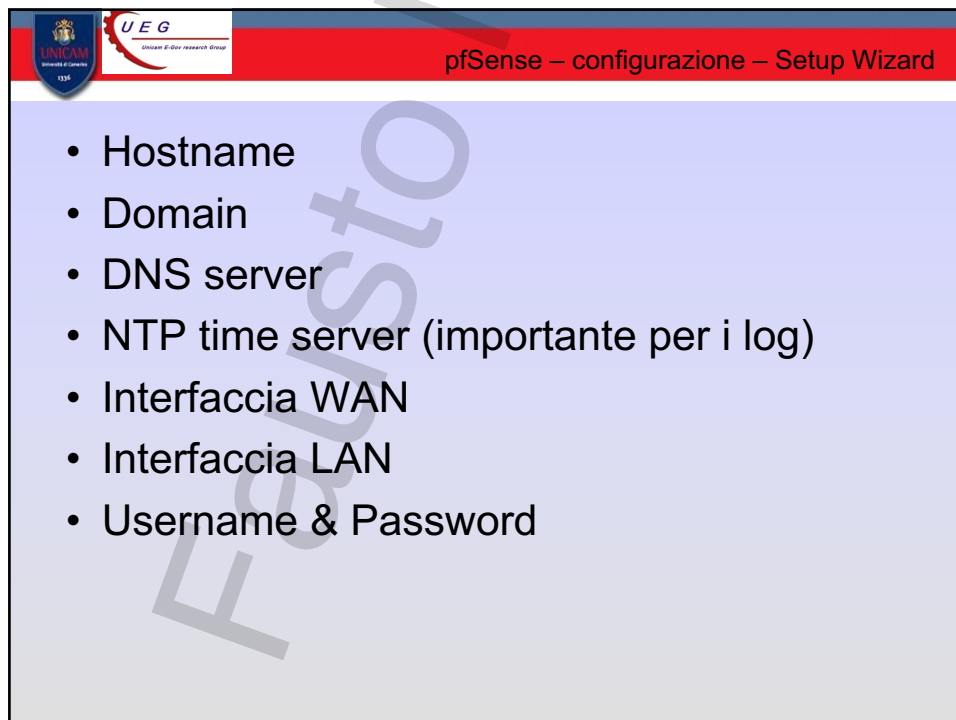
45



46



47



48

UNICAM Università di Camerino 1336 UEG Italian E-Dev research Group

pfSense – configurazione - wizard

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname: FWfausto
EXAMPLE: myserver

Domain: unicom.it
EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server: 193.204.8.33

Secondary DNS Server: 193.204.8.34

Override DNS: ☒
Allow DNS servers to be overridden by DHCP/PPP on WAN

Next

49

UNICAM Università di Camerino 1336 UEG Italian E-Dev research Group

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)

50

UNICAM Università di Camerino 1336 UEG Italian E-Gov research Group

pfSense – configurazione - wizard

Step 4 of 9

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType Static

General configuration

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: xxxxxxxxxxxx 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

51

UNICAM Università di Camerino 1336 UEG Italian E-Gov research Group

pfSense – configurazione - wizard

RFC1918 Networks

Block RFC1918 Private Networks ☒ Block private networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks

Block bogon networks ☒ Block non-Internet routed networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

<https://ipinfo.io/bogon>

52

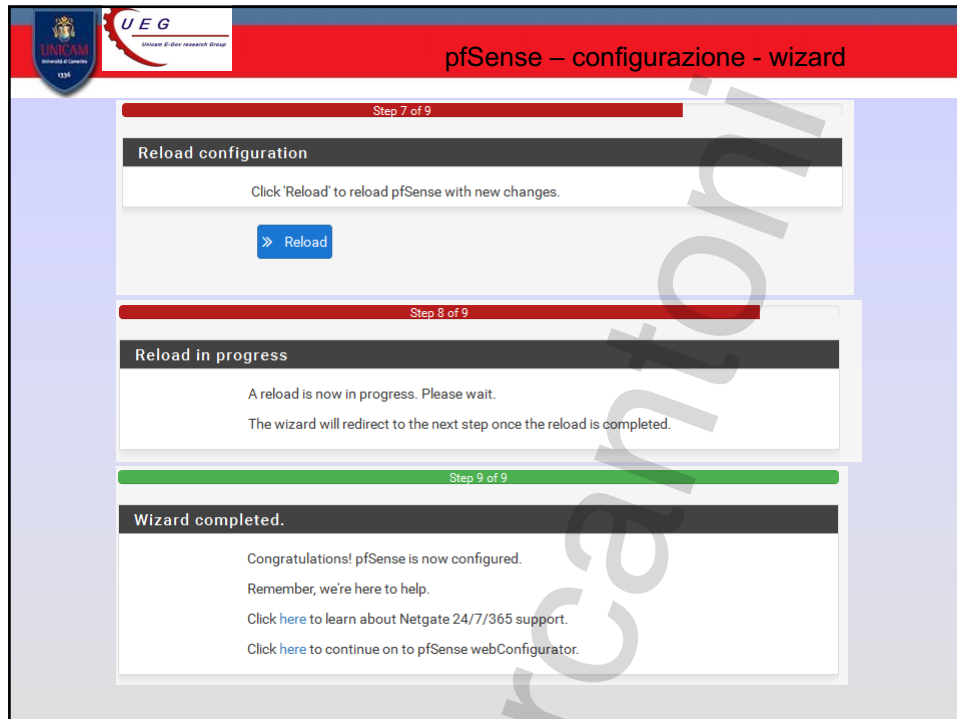
The screenshot shows the 'Configure LAN Interface' step of the pfSense configuration wizard. The interface includes a progress bar at the top indicating 'Step 5 of 9'. Below the title, a message states: 'On this screen the Local Area Network information will be configured.' The form contains two input fields: 'LAN IP Address' with the value '192.168.1.1' and 'Subnet Mask' with the value '24'. A checkbox for 'Type dhcp if this interface uses DHCP to obtain its IP address.' is present but unchecked. A blue 'Next' button is located at the bottom of the form. The background of the wizard is light blue with a large, faint watermark reading 'Marco Antonio'.

53

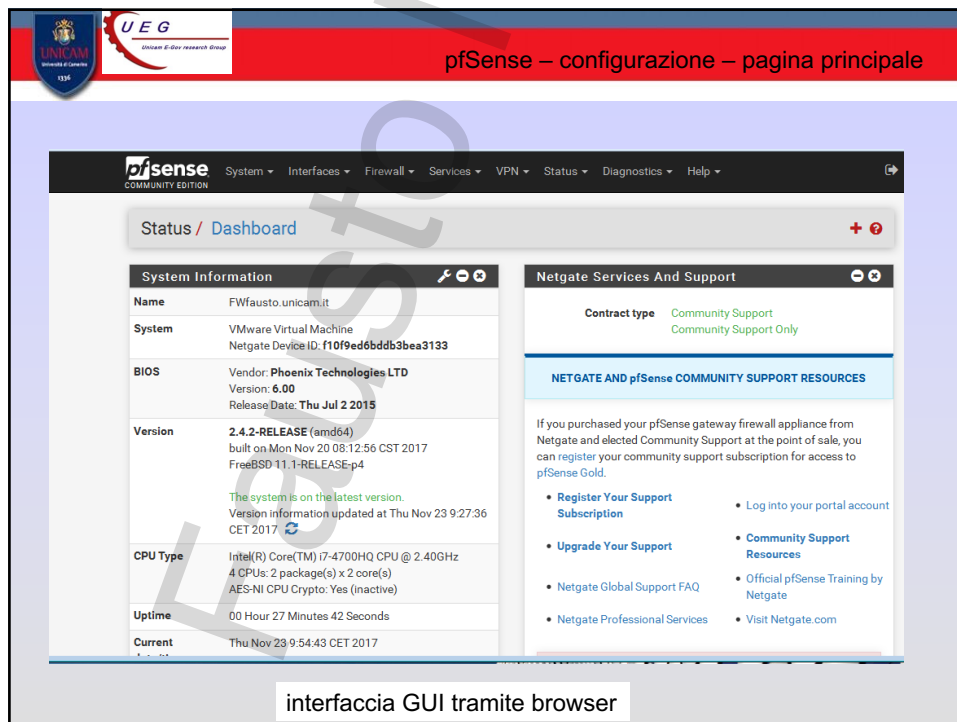
The screenshot shows the 'Set Admin WebGUI Password' step of the pfSense configuration wizard. The interface includes a progress bar at the top indicating 'Step 6 of 9'. Below the title, a message states: 'On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.' The form contains two password input fields: 'Admin Password' and 'Admin Password AGAIN'. The first field shows a masked password of seven dots. A blue 'Next' button is located at the bottom of the form. The background of the wizard is light blue with a large, faint watermark reading 'Marco Antonio'.

default password: pfsense

54



55



interfaccia GUI tramite browser

56




pfSense – configurazione - Interfaces

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

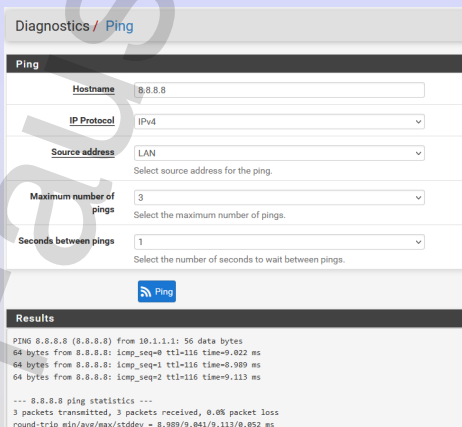
block private network
RFC1918 (10/8, 172.16/12, 192.168/16)

57




Troubleshooting

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



58




Troubleshooting

Arp table

Diagnostics / ARP Table ?

Search

All
Search
Clear

Enter a search string or *nix regular expression to filter entries.

Interface	IP Address	MAC Address	Hostname	Status	Link Type	Actions
WAN	193.205.92.224	00:0c:29:84:cc:b8		Permanent	ethernet	+ ⬇ ⬆
WAN	193.205.92.2	10:b3:d5:e2:b4:5f		Expires in 1172 seconds	ethernet	+ ⬇ ⬆
LAN	10.1.1.101	00:0c:29:d5:9e:8e	desktop-d106lej	Expires in 1178 seconds	ethernet	+ ⬇ ⬆
LAN	10.1.1.1	00:0c:29:84:cc:c2	FW-IRS.irs.local	Permanent	ethernet	+ ⬇ ⬆
LAN	10.1.1.102	00:50:56:c0:00:02	mfausto.	Expires in 1182 seconds	ethernet	+ ⬇ ⬆

Clear 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

System / Advanced / Networking

Admin Access
Firewall & NAT
Networking
Miscellaneous
System Tunables
Notifications

DHCP Options

Server Backend
Kea DHCP
ISC DHCP (Deprecated)
Ignore Deprecation Warning

Services / DHCP Server / LAN

LAN

General DHCP Options

DHCP Backend: Kea DHCP

Enable

Enable DHCP server on LAN interface

Deny Unknown Clients: Allow all clients

Ignore Client Identifiers: ☐ Do not record a unique identifier (UID) in client lease data if present in the client DHCP request

When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.

This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the [RFC 2131](#) specification.

Primary Address Pool

Subnet: 10.1.1.0/24

Subnet Range: 10.1.1.1 - 10.1.1.254

Address Pool Range: From 10.1.1.100

To 10.1.1.200

The specified range for this pool must not be within the range configured on any other address pool for this interface.

62

UNICAM Università di Camerino 1336 UEG Italian E-Dev research Group

pfSense – configurazione - DHCP Server

Servers

WINS servers

WINS Server 1

WINS Server 2

DNS servers

193.204.8.33

193.204.8.34

DNS Server 3

DNS Server 4

Leave blank to use the system default DNS servers: this interfaces IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

63

UNICAM Università di Camerino 1336 UEG Italian E-Dev research Group

pfSense – diagnostica - DHCP Lease

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

Status / DHCP Leases

Search

Search Term All

Enter a search string or *nix regular expression to filter entries.

Leases

IP Address	MAC Address	Hostname	Description	Start	End	Actions
10.1.1.101	00:0c:29:d5:9e:8e	desktop-d1o6lej		2023/11/24 11:58:20	2023/11/24 13:58:20	+ -
10.1.1.102	00:50:56:c0:00:02	mfausto.		2023/11/24 11:42:50	2023/11/24 13:42:50	+ -

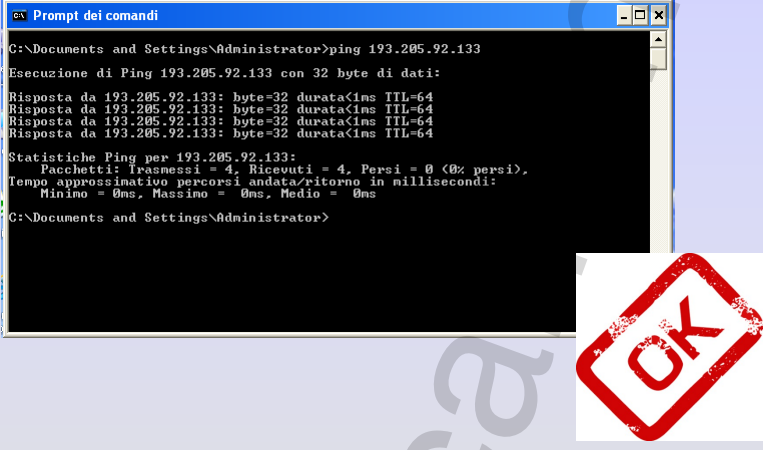
Lease Utilization

Interface	Pool Start	Pool End	Used	Capacity	Utilization
LAN	10.1.1.100	10.1.1.200	2	101	1% of 101

64

Troubleshooting

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



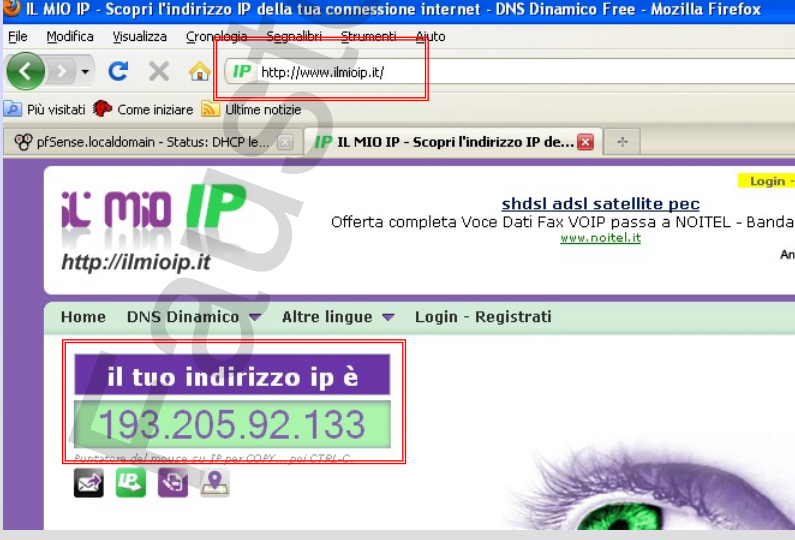
```

C:\Documents and Settings\Administrator>ping 193.205.92.133
Esecuzione di Ping 193.205.92.133 con 32 byte di dati:
Risposta da 193.205.92.133: byte=32 durata<1ms TTL=64
Risposta da 193.205.92.133: byte=32 durata<1ms TTL=64
Risposta da 193.205.92.133: byte=32 durata<1ms TTL=64
Risposta da 193.205.92.133: byte=32 durata<1ms TTL=64
Statistiche Ping per 193.205.92.133:
    Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 0ms, Massimo = 0ms, Medio = 0ms
C:\Documents and Settings\Administrator>
  
```

65

NAT – Network Address Translation

Chi sono io???



IL MIO IP - Scopri l'indirizzo IP della tua connessione internet - DNS Dinamico Free - Mozilla Firefox

File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto

IP http://www.ilmioip.it/

Più visitati Come iniziare Ultime notizie

pfSense.localdomain - Status: DHCP le... IL MIO IP - Scopri l'indirizzo IP de...

Login

il mio IP

shdsl adsl satellite pec

Offerta completa Voce Dati Fax VOIP passa a NOITEL - Banda

www.noitel.it

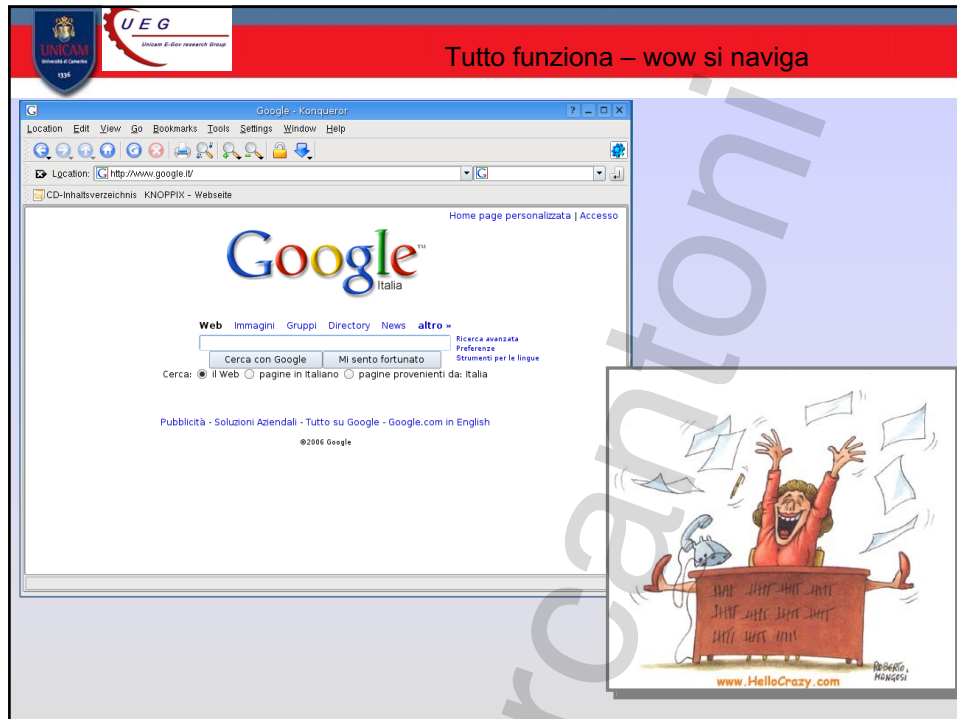
Home DNS Dinamico Altre lingue Login - Registrati

il tuo indirizzo ip è

193.205.92.133

Prendi il tuo IP e CTRL+C

66



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.

Services: DNS forwarder

☒ **Enable DNS forwarder**

☐ **Register DHCP leases in DNS forwarder**
If this option is set, then machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.

☐ **Register DHCP static mappings in DNS forwarder**
If this option is set, then DHCP static mappings will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.

☐ **Resolve DHCP mappings first**
If this option is set, then DHCP mappings will be resolved before the manual list of names below. This only affects the name given for a reverse lookup (PTR).

68

UNICAM Università di Camerino 1356 UEG Italian E-Gov research Group

pfSense – Status - LOG

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

Last 500 General Log Entries. (Maximum 500)

Time	Process	PID	Message
Nov 23 13:01:38	kernel		em1: Using 1024 TX descriptors and 1024 RX descriptors
Nov 23 13:01:38	kernel		em1: Ethernet address: 00:0c:29:84:cc:c2
Nov 23 13:01:38	kernel		em1: link state changed to UP
Nov 23 13:01:38	kernel		em1: netmap queues/slots: TX 1/1024, RX 1/1024
Nov 23 13:01:38	kernel		ehci0: <VMware USB 2.0 controller> mem 0xf59f000-0xf59fff irq 17 at device 3.0 on pci2
Nov 23 13:01:38	kernel		usb1: EHCI version 1.0
Nov 23 13:01:38	kernel		usb1 on ehci0
Nov 23 13:01:38	kernel		usb1: 480Mbps High Speed USB v2.0
Nov 23 13:01:38	kernel		pci3: <ACPI PCI-PCI bridge> at device 21.0 on pci0
Nov 23 13:01:38	kernel		pci4: <ACPI PCI-PCI bridge> at device 21.1 on pci0
Nov 23 13:01:38	kernel		pci5: <ACPI PCI-PCI bridge> at device 21.2 on pci0

General Logging Options

Log Message Format:

Forward/Reverse Display: ☐ Show log entries in reverse order (newest entries on top)

GUI Log Entries:

This is only the number of log entries displayed in the GUI. It does not affect how

69

UNICAM Università di Camerino 1356 UEG Italian E-Gov research Group

pfSense – configurazione - LOG

Send log messages to remote syslog server

Remote Logging Options

Enable Remote Logging ☒ Send log messages to remote syslog server

Source Address:

This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol:

This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; if an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers:

Remote Syslog Contents

☐ Everything

☐ System Events

☐ Firewall Events

☐ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)

☐ DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)

☐ PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)

☐ General Authentication Events

☐ Captive Portal Events

☐ VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)

☐ Gateway Monitor Events

☐ Routing Daemon Events (RADVD, URP, RIP, OSPF, BGP)

☐ Network Time Protocol Events (NTP Daemon, NTP Client)

☐ Wireless Events (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.

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 fatto 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




pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

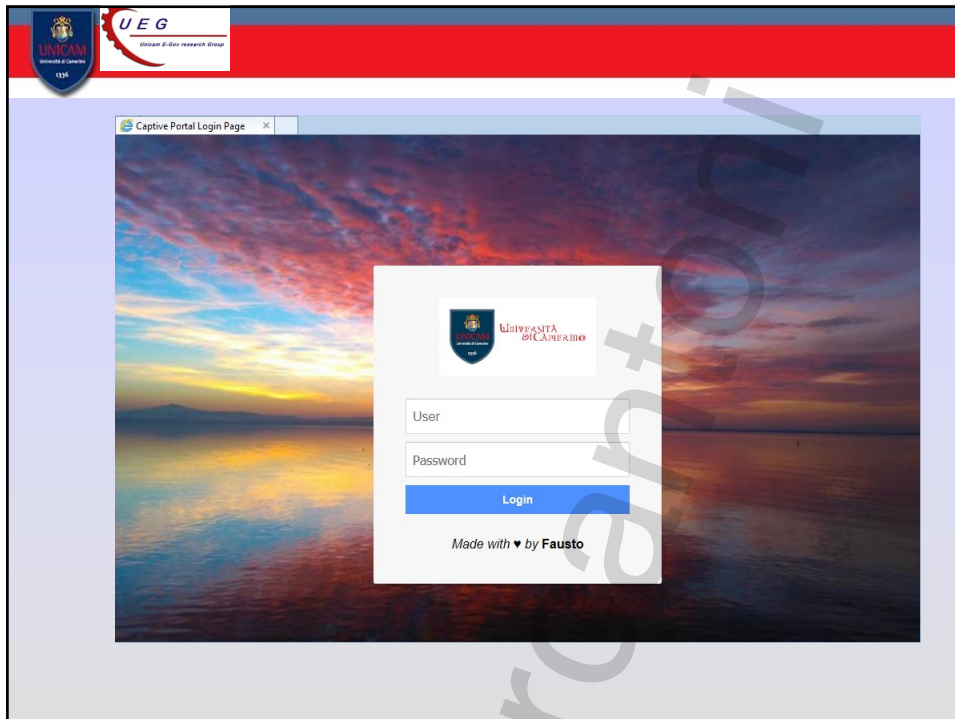
Services / Captive Portal / Add Zone

Add Captive Portal Zone

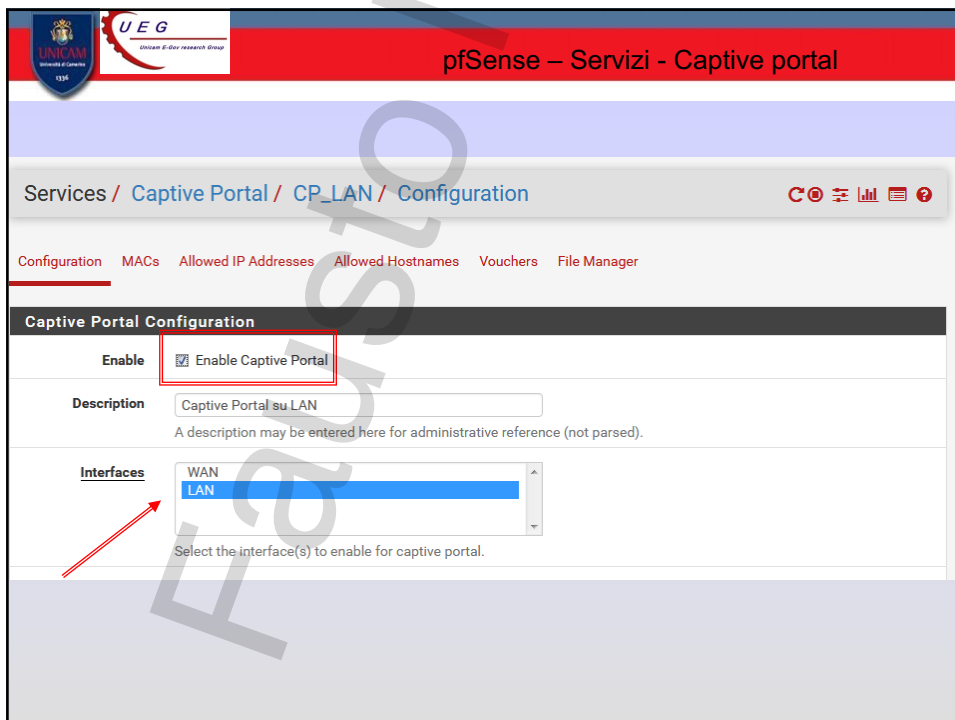
Zone name
Zone name. Can only contain letters, digits, and underscores (_) and may not start with a digit.

Zone description
A description may be entered here for administrative reference (not parsed).

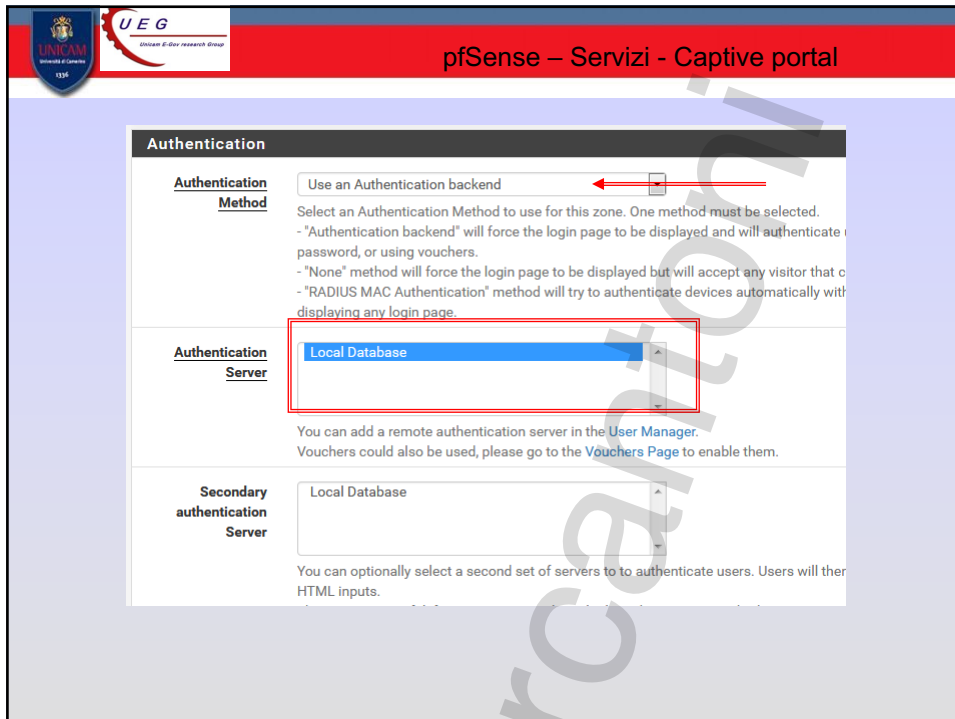
72



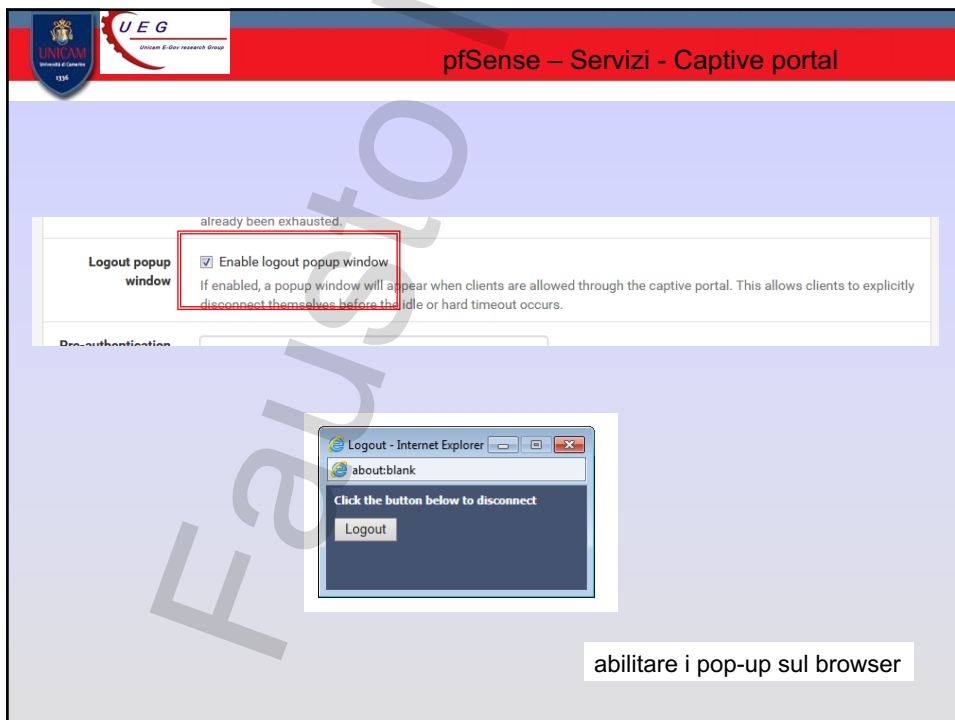
73



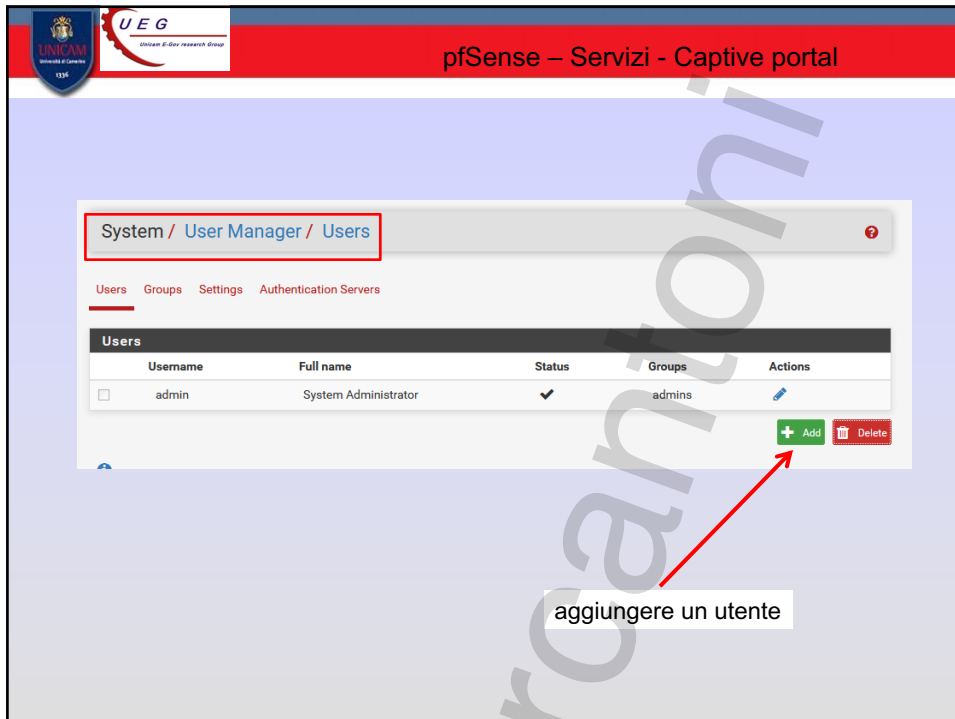
74



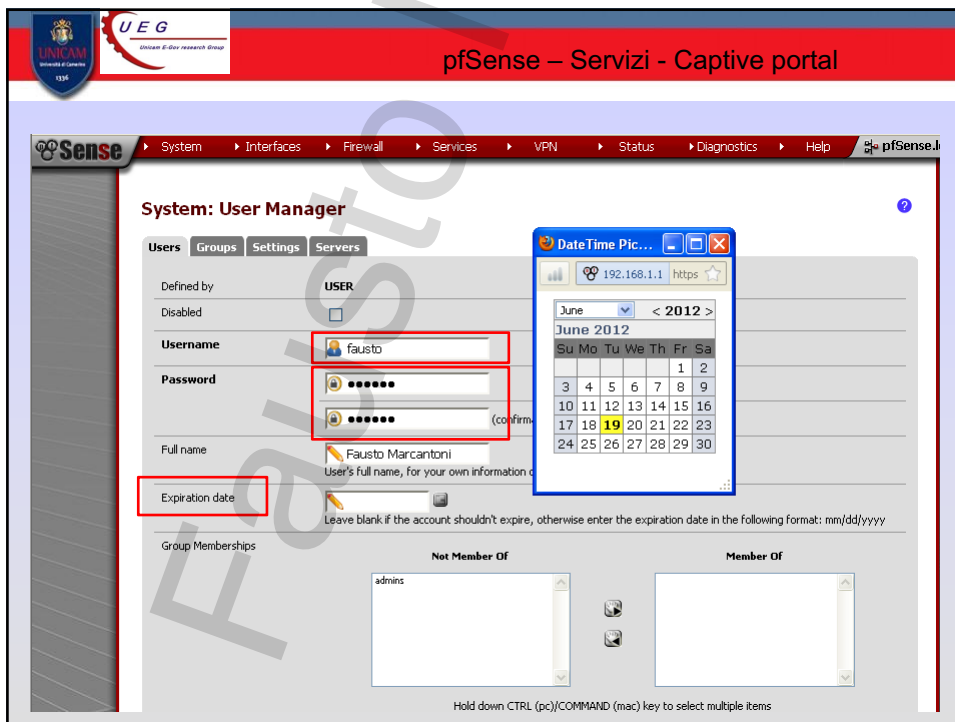
75



76



77



78

Abilitare l'utente ad utilizzare il Captive Portal

Inherited from	Name	Description	Action
	User - Services: Captive Portal login	Indicates whether the user is able to login on the captive portal.	

[+ Add](#)

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

☐ Use custom captive portal page
☒ Enable to use a custom captive portal login page
 If set a portal.html page must be created and uploaded. If unchecked the default template will be used

Captive Portal Login Page

Display custom logo image ☒ Enable to use a custom uploaded logo

Logo Image Nessun file selezionato.
 Add a logo for use in the default portal login screen. File will be renamed captiveportal-logo.* The image will be resized to fit within the given area. It can be of any image type: .png, .jpg, .svg **This image will not be stored in the config.** The default logo will be used if no custom image is present.

Display custom background image ☒ Enable to use a custom uploaded background image

Background image Nessun file selezionato.
 Add a background image for use in the default portal login screen. File will be renamed captiveportal-background.* The background image will fill the screen. **This image will not be stored in the config.** The default background image will be used if no custom background is present.

Terms and Conditions

80

UNICAM
Università di Camerino
1336

UEG
University & Enterprise research Group

pfSense – Servizi - Captive portal

Personalizzazione Captive Portal

Portal page contents Nessun file selezionato.

Upload an HTML/PHP file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST to "\$PORTAL_ACTIONS\$") with a submit button (name="accept") and a hidden field with name="redirecturl" and value="\$PORTAL_REDIRECTURL\$". Include the "auth_user" and "auth_pass" and/or "auth_voucher" input fields if authentication is enabled, otherwise it will always fail.

Example code for the form:

```
<form method="post" action="$PORTAL_ACTIONS$">
  <input name="auth_user" type="text">
  <input name="auth_pass" type="password">
  <input name="auth_voucher" type="text">
  <input name="redirecturl" type="hidden" value="$PORTAL_REDIRECTURL$">
  <input name="zone" type="hidden" value="$PORTAL_ZONE$">
  <input name="accept" type="submit" value="Continue">
</form>
```

Auth error page contents Nessun file selezionato.

The contents of the HTML/PHP file that is uploaded here are displayed when an authentication error occurs. It may include "\$PORTAL_MESSAGES\$", which will be replaced by the error or reply messages from the RADIUS server, if any.

Logout page contents Nessun file selezionato.

The contents of the HTML/PHP file that is uploaded here are displayed on authentication success when the logout popup is enabled.

81

UNICAM
Università di Camerino
1336

UEG
University & Enterprise research Group

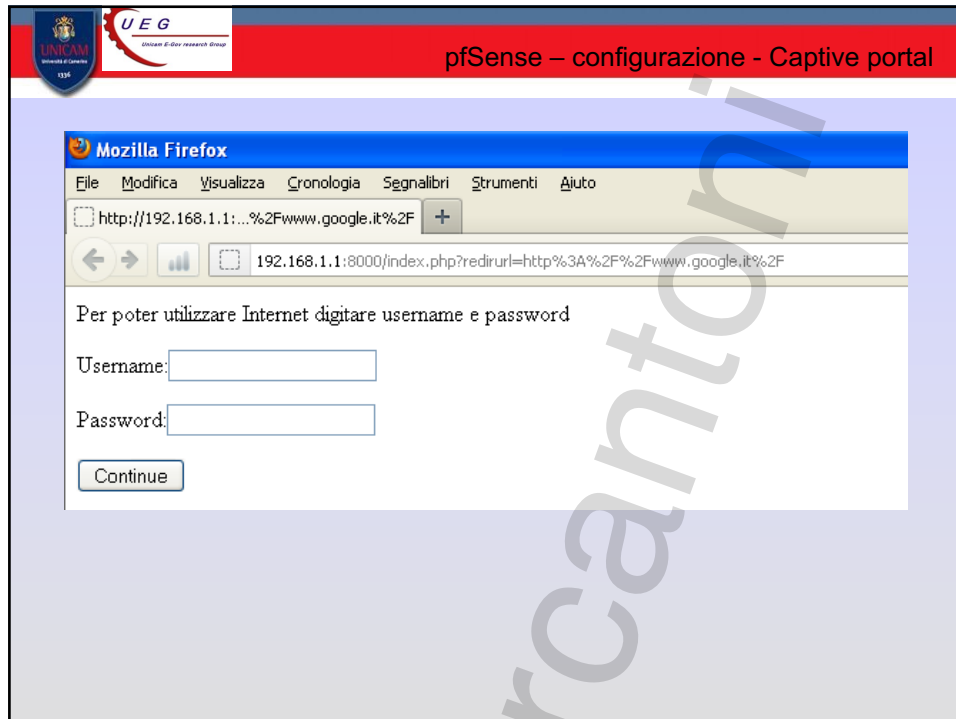
pfSense– configurazione - Captive portal

Esempio di pagina "CAPRTIVE PORTAL"

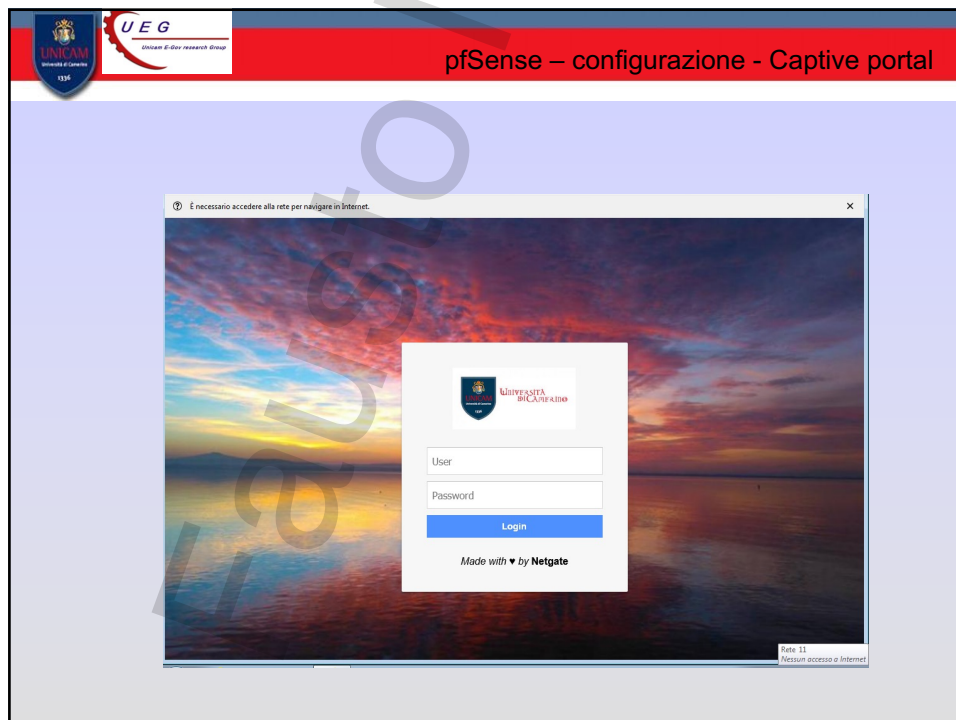
```
<html>
<body>
<form method="post" action="$PORTAL_ACTION$">
  <input name="auth_user" type="text">
  <input name="auth_pass" type="password">
  <input name="auth_voucher" type="text">
  <input name="redirecturl" type="hidden" value="$PORTAL_REDIRECTURL$">
  <input name="zone" type="hidden" value="$PORTAL_ZONE$">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

E' possibile aggiungere anche le immagini

82



83



84

UNICAM Università di Camerino 1336 UEG Italian E-Gov research Group

pfSense – configurazione - Captive portal

Maximum concurrent connections

Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal but rather how many connections a single IP can establish to the portal web server.

Idle timeout (Minutes)

Clients will be disconnected after this amount of inactivity. They may log in again for no idle timeout. Leave this field blank for no idle timeout.

Hard timeout (Minutes)

Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).

Traffic quota (Megabytes)

Clients will be disconnected after exceeding this amount of traffic, inclusive of both downloads and uploads. They may log in again immediately, though. Leave this field blank for no traffic quota.

Pass-through credits per MAC address.

Allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in with valid credentials until the waiting period specified below has expired. Recommended to set a hard timeout and/or idle timeout when using this for it to be effective.

Don't forget to enable the DHCP server on the captive portal interface! Make sure that the default/maximum DHCP lease time is higher than the hard timeout entered on this page. Also, the DNS Forwarder or Resolver must be enabled for DNS lookups by unauthenticated clients to work.

85

UNICAM Università di Camerino 1336 UEG Italian E-Gov research Group

pfSense – configurazione - Captive portal

Services / Captive Portal / CP_LAN / Configuration

Configuration

MACs

Allowed IP Addresses

Allowed Hostnames

Vouchers

File Manager

Adding MAC addresses as pass-through MACs allows them access through the captive portal automatically without being taken to the portal page.

Adding allowed IP addresses will allow IP access to/from these addresses through the captive portal without being taken to the portal page.

Any files that you upload here with the filename prefix of captiveportal- will be made available in the root directory of the captive portal HTTP(S) server. You may reference them directly from your portal page HTML code using relative paths.

86

UNICAM Università di Camerino 1336 UEG Italian E-Dev research Group

pfSense – configurazione - Captive portal

I log di captive portal

The screenshot shows the pfSense web interface for the Captive Portal configuration. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the breadcrumb trail is "Status / Captive Portal / CP_LAN". A table titled "Users Logged In (1)" displays the following data:

IP address	MAC address	Username	Session start	Actions
192.168.100.100	00:0c:29:40:6c:96	fausto	01/17/2019 07:53:22	[Disconnect]

Buttons at the bottom of the table include "Show Last Activity" and "Disconnect All Users".

87

UNICAM Università di Camerino 1336 UEG Italian E-Dev research Group

System LogsAuthenticationCaptive Portal Auth

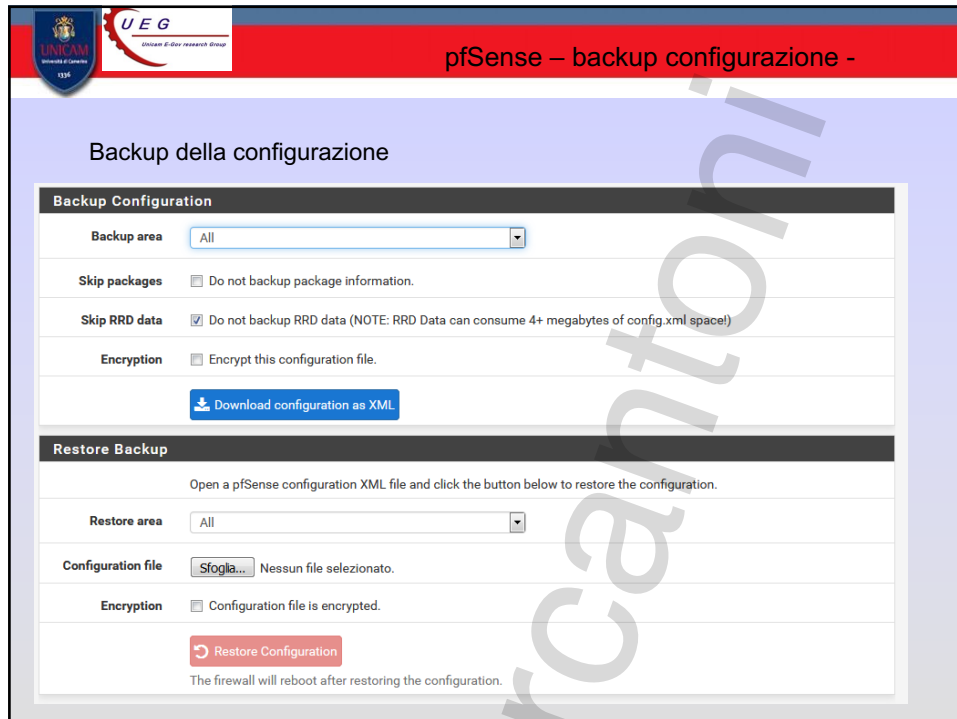
System Logs → Authentication → Captive Portal Auth

The screenshot shows the pfSense System Logs interface, specifically the "Authentication" section and "Captive Portal Auth" sub-section. The breadcrumb trail is "Status / System Logs / Authentication / Captive Portal Auth". Below the navigation tabs, a table titled "Last 6 Captive Portal Auth Log Entries. (Maximum 500)" displays the following data:

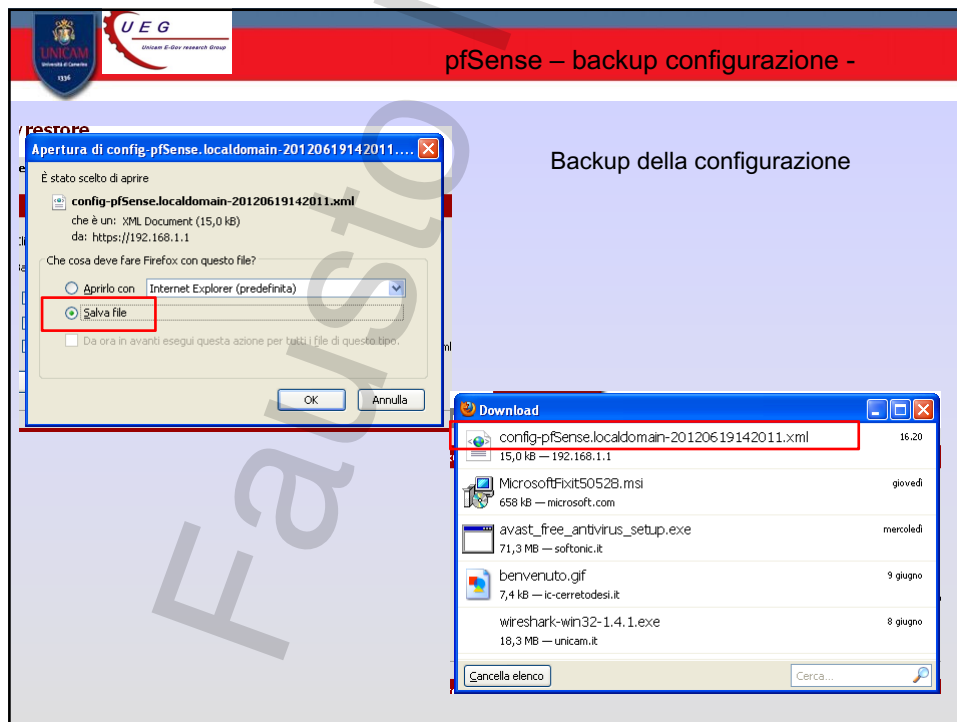
Time	Process	PID	Message
Nov 24 12:33:19	logportalauth	398	Zone: cp_lan - Reconfiguring captive portal(CP_LAN).
Nov 24 12:36:36	logportalauth	398	Zone: cp_lan - FAILURE: fausto, 00:0c:29:d5:9e:8e, 10.1.1.101, Access Denied
Nov 24 12:38:21	logportalauth	12770	Zone: cp_lan - ACCEPT: fausto, 00:0c:29:d5:9e:8e, 10.1.1.101
Nov 24 12:39:55	logportalauth	98181	Zone: cp_lan - DISCONNECT: fausto, 00:0c:29:d5:9e:8e, 10.1.1.101
Nov 27 10:43:44	logportalauth	397	Zone: cp_lan - Reconfiguring captive portal(CP_LAN).
Nov 27 10:44:15	logportalauth	398	Zone: cp_lan - ACCEPT: fausto, 00:0c:29:d5:9e:8e, 10.1.1.101

Below the table, a summary entry is shown: "Nov 27 10:44:15 logportalauth 398 Zone: cp_lan - ACCEPT: fausto, 00:0c:29:d5:9e:8e, 10.1.1.101".

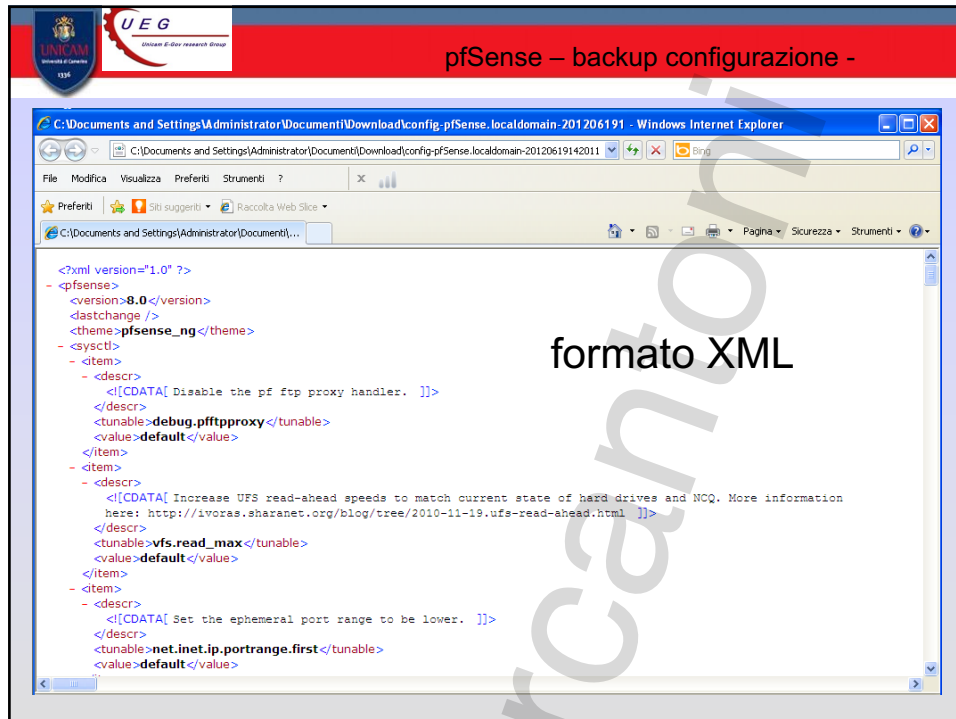
88



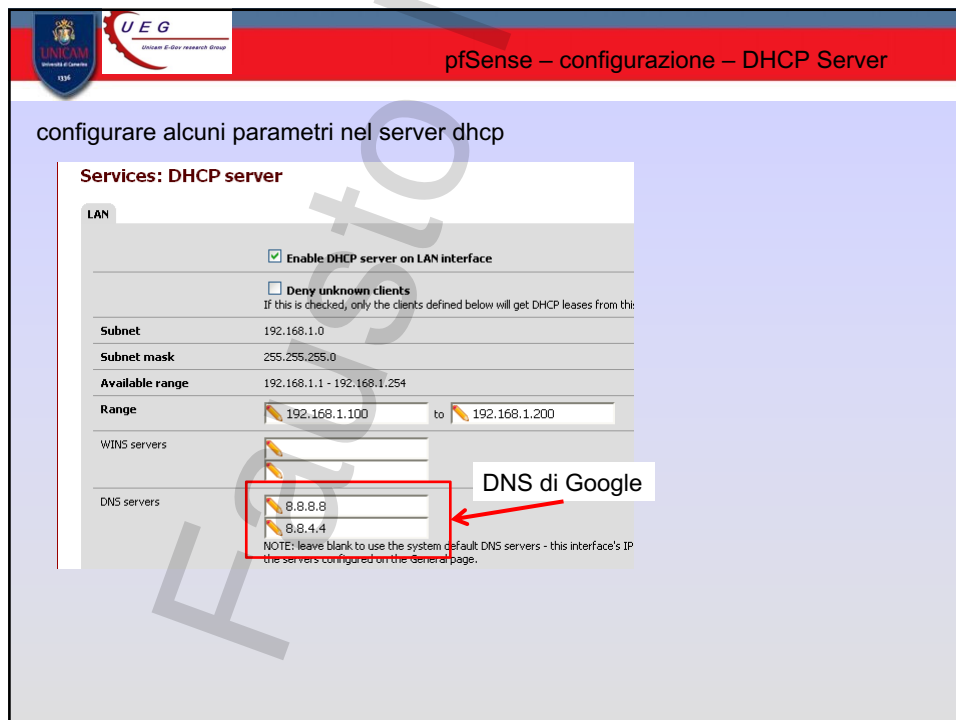
89



90



91



92

UNICAM Università di Camerino UEG Italian E-Dev research Group

pfSense – configurazione – DHCP Server

configurare alcuni parametri nel server dhcp

not the correct gateway for your network.

Domain name domain name personale

The default is to use the domain name of this system. You can enter an alternate domain name here.

NTP servers NTP server

93

UNICAM Università di Camerino UEG Italian E-Dev research Group

pfSense – configurazione – DHCP Server

configurare alcuni parametri nel server dhcp

Dettagli connessione di rete:

Proprietà	Valore
Indirizzo fisico	00-0C-29-47-DF-8A
Indirizzo IP	192.168.1.100
Subnet Mask	255.255.255.0
Gateway predefinito	192.168.1.1
Server DHCP	192.168.1.1
Lease ottenuto	20/12/2012 13.04.55
Scadenza lease	20/12/2012 15.04.55
Server DNS	8.8.8.8
Server WINS	8.8.4.4

dei comandi

```

Windows XP (Versione 5.1.2600)
Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig/all

Configurazione IP di Windows

Nome host . . . . . : windows-0c6062c
Suffisso DNS primario . . . . . : 
Tipo nodo . . . . . : Sconosciuto
Routing IP abilitato. . . . . : No
Proxy WINS abilitato. . . . . : No
Elenco di ricerca suffissi DNS. . . . : fausto.name

Scheda Ethernet Connessione alla rete locale (LAN):

Suffisso DNS specifico per connessione: fausto.name
Descrizione . . . . . : VMware Accelerated AMD PCNet Adapter
Indirizzo fisico. . . . . : 00-0C-29-47-DF-8A
DHCP abilitato. . . . . : Si
Configurazione automatica abilitata : Si
Indirizzo IP. . . . . : 192.168.1.100
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.1.1
Server DHCP . . . . . : 192.168.1.1
Server DNS . . . . . : 8.8.8.8
Lease ottenuto. . . . . : giovedì 20 dicembre 2012 13.04.55
Scadenza lease . . . . . : giovedì 20 dicembre 2012 15.04.55

C:\Documents and Settings\Administrator>

```

94

UNICAM
Università di Camerino
1336

UEG
Unicam E-Dev research Group

pfSense – configurazione - Creazione regole

Le "REGOLE"

pfSense
COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Gold FWfausto.unicam.it

Firewall / Rules / LAN

Floating WAN LAN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 6 / 8.69 MiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	⚙️
✓ 1 / 16.28 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	🔗 🛠️ 🗑️

Add Add Delete Save Separator

95

UNICAM
Università di Camerino
1336

UEG
Unicam E-Dev research Group

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
✓ 1 / 1.33 MiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	⚙️
✓ 24 / 207.83 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	🔗 🛠️ 🗑️
✓ 0 / 0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	🔗 🛠️ 🗑️

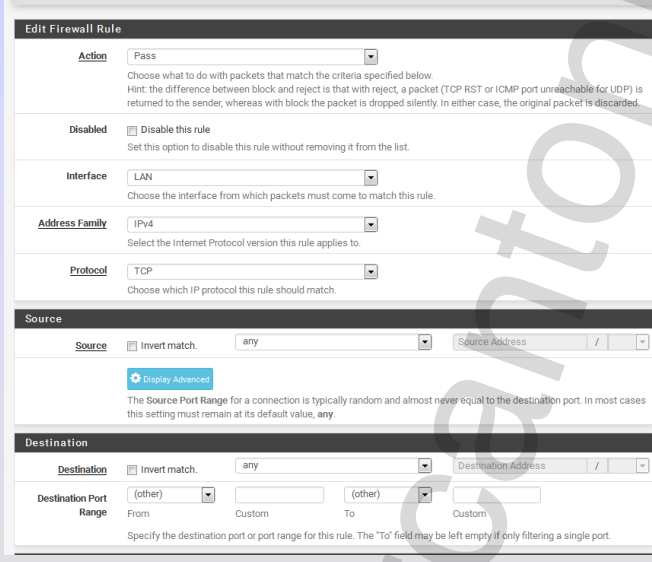
Add Add Delete Toggle Copy Save Separator

TUTTO APERTO

96

UNICAM Università di Camerino 1336 UEG Italian E-Gov research Group

pfSense – configurazione - Creazione regole



Configurare una regola ...

97

UNICAM Università di Camerino 1336 UEG Italian E-Gov research Group

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

UNICAM Università di Camerino 1336 UEG Italian E-Gov research Group

pfSense – configurazione - Creazione regole

Edit Firewall Rule

Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface LAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which IP protocol this rule should match.

Source
Source ☐ Invert match. any Source Address /

Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination
Destination ☐ Invert match. any Destination Address /

Destination Port Range
From (other) Custom To (other) Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Configurare una regola ...

99

UNICAM Università di Camerino 1336 UEG Italian E-Gov research Group

pfSense – configurazione - Creazione regole

... Configurare una regola ...



Attenzione

Ricorda:
Un firewall si progetta

Protocol TCP
TCP
UDP

Source
Source
Type: any
Address: any

Destination
Destination
Type: any
Address: any

Destination port range
from: (other)

100

UNICAM
Università di Camerino
1336

UEG
University of Engineering and Graphics

pfSense – configurazione - Creazione regole

... Configurare una regola ...

Log	☐ Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	 You may enter a description here for your reference.

Mettere descrizioni facili da ricordare e intuitive

101

UNICAM
Università di Camerino
1336

UEG
University of Engineering and Graphics

pfSense – configurazione - Creazione regole

Ricorda:
Un firewall si progetta



CHIUDIAMO TUTTO ...

102

UNICAM  UEG  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	*	*		Anti-Logout 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

103

UNICAM  UEG  pfSense – configurazione - Creazione regole



CHIUDIAMO TUTTO ...
POI APRIAMO QUELLO CHE SERVE

104

UNICAM
Università di Camerino
1336

UEG
University of Engineering and Graphics

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

UNICAM
Università di Camerino
1336

UEG
University of Engineering and Graphics

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

UNICAM Università di Camerino 1336 UEG Italian E-Gov research Group

pfSense – configurazione – Firewall 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_2FIN_WAIT_2	94 / 179	22 KIB / 148 KIB
LAN	tcp	192.168.1.100:49538 -> 192.168.1.1:443	FIN_WAIT_2FIN_WAIT_2	46 / 47	8 KIB / 5 KIB
LAN	tcp	192.168.1.100:49540 -> 192.168.1.1:443	FIN_WAIT_2FIN_WAIT_2	39 / 40	6 KIB / 4 KIB
LAN	udp	192.168.1.101:48421 -> 192.168.1.1:53	SINGLEMULTIPLE	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	MULTIPLEMULTIPLE	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

UNICAM Università di Camerino 1336 UEG Italian E-Gov research Group

pfSense – Status – Traffic Graph

Traffic Graphs

WAN

LAN

Show graphs: WAN, LAN

Refresh Interval: 1

Inverse: On

Unit Size: Bytes

traffico e banda utilizzata

108

UNICAM **UEG** Uniview E-Dev research Group

ARP table

Diagnostics / 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

UNICAM **UEG** Uniview E-Dev research Group

pfSense – Status – Graphs

Status / Traffic Graph

Graph Settings

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

Traffic Graph

LAN

lan (in) lan (out)

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

00:32 00:50 01:40 02:30 02:52

110

UNICAM University of Cambridge 1396 UEG Division E-Dev research Group

pfSense – Package

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term Both

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

Name	Version	Description	
acme	0.1.30	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates.	+ Install
apcupsd	0.3.9_3	"apcupsd" can be used for controlling all APC UPS models. It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN.	+ Install
arping	1.2.2_1	Broadcasts a who-has ARP packet on the network and prints answers.	+ Install
AutoConfigBackup	1.50	Automatically backs up your pfSense configuration. All contents are encrypted before being sent to the server. Requires Gold Subscription from pfSense Portal.	+ Install
Avahi	1.11.2	Avahi is a system which facilitates service discovery on a local network via the	+ Install

111

UNICAM University of Cambridge 1396 UEG Division E-Dev research Group

pfSense – Package - squid proxy

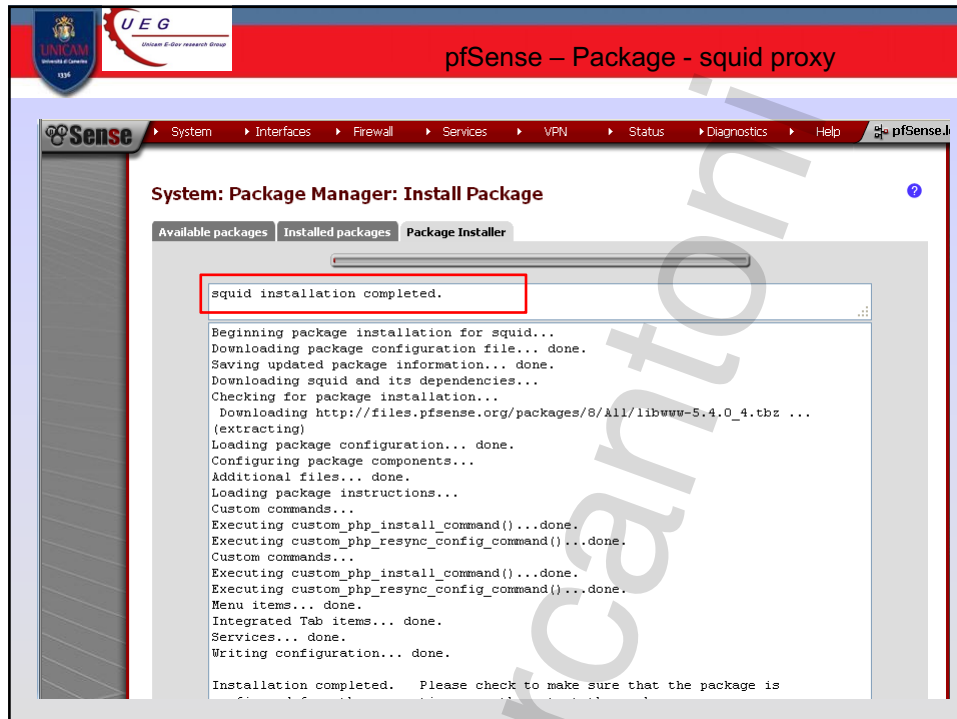



SQUID

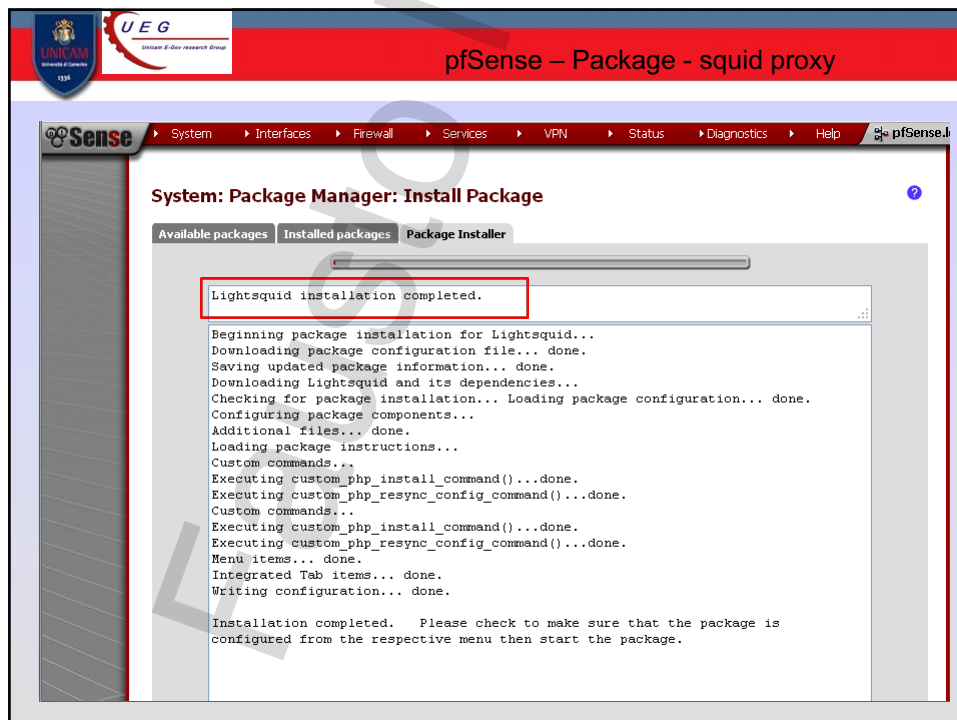
<http://www.squid-cache.org/>

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.	+ 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.	+ Install
squidGuard	1.16.19	High performance web proxy URL filter.	+ Install

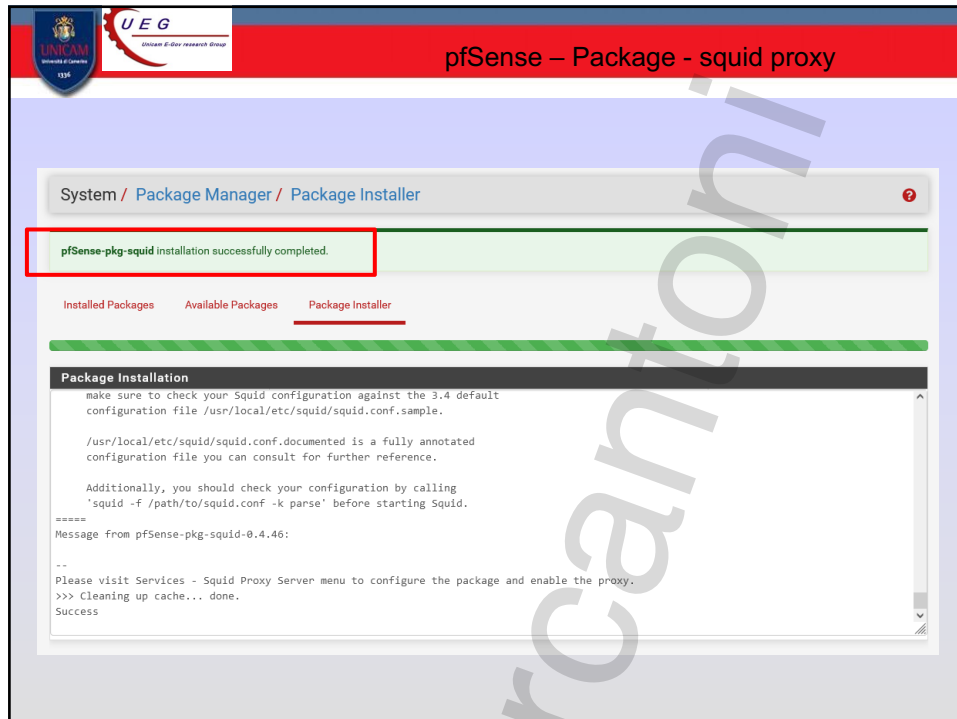
112



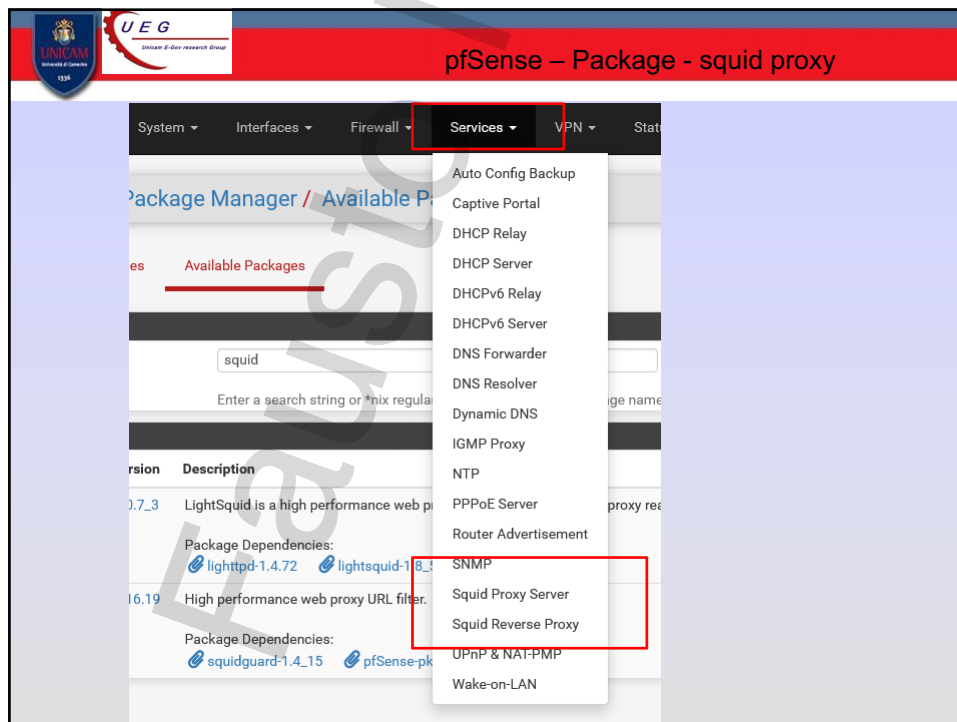
113



114



115



116

UNICAM
Università di Camerino
1336

UEG
University of Engineering and Graphics

pfSense – Package - squid proxy

Proxy server: General settings

General Upstream Proxy Cache Mgmt Access Control Traffic Mgmt Auth Settings Local Users

Proxy interface TAN
WAN

The interface(s) the proxy server will bind to.

Allow users on interface ☒
If this field is checked, the users connected to the interface selected in the 'Proxy interface' field will be allowed to use the proxy, i.e., there will be no need to add the interface's subnet to the list of allowed subnets. This is just a shortcut.

Transparent proxy ☐
If transparent mode is enabled, all requests for destination port 80 will be forwarded to the proxy server without any additional configuration necessary.

Interfaccia da abilitare per il proxy

Interfaccia utente da abilitare per il proxy

La funzione del Transparent Proxy è quella di intercettare ogni richiesta di un particolare servizio (in questo caso richiesta HTTP) per poi redirigerla a un proxy

117

UNICAM
Università di Camerino
1336

UEG
University of Engineering and Graphics

Proxy Server: Cache Management Local Cache

The following input errors were detected:

- Please, configure and save 'Local Cache' settings first.

Squid Hard Disk Cache Settings

Hard Disk Cache Size 100
Amount of disk space (in megabytes) to use for cached objects.

Hard Disk Cache System ufs
This specifies the kind of storage system to use.

Clear Disk Cache NOW Hard Disk Cache is automatically managed by swapstate_check.php script which is scheduled to run daily via cron. If you wish to clear cache immediately, click this button once: **Clear Disk Cache NOW**

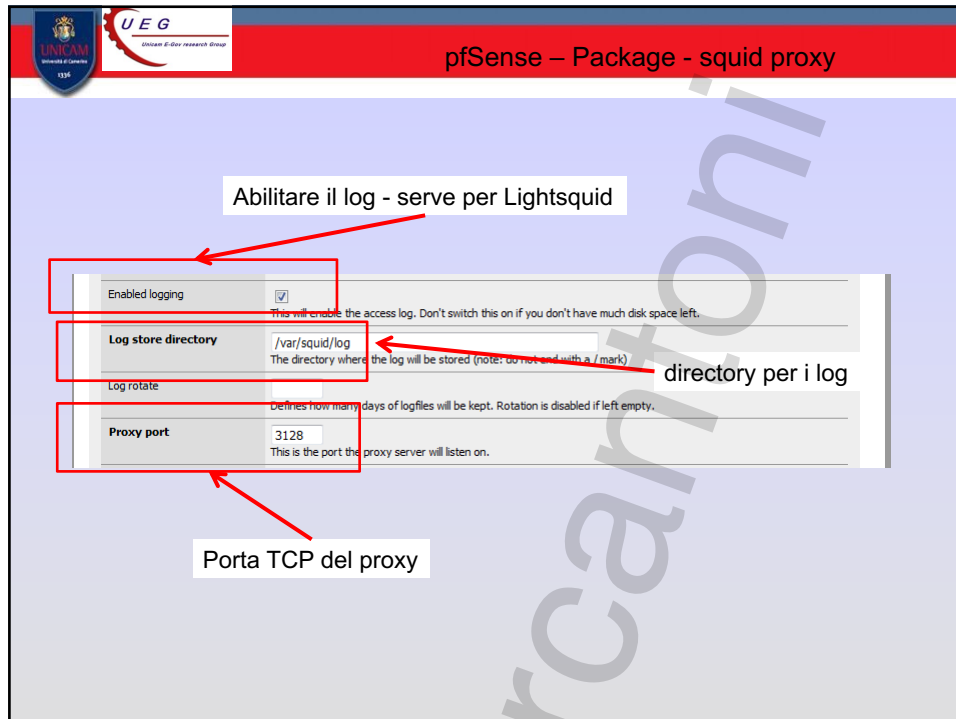
Level 1 Directories 16
Specifies the number of Level 1 directories for the hard disk cache.

Hard Disk Cache Location /var/squid/cache
This is the directory where the cache will be stored. Default: /var/squid/cache

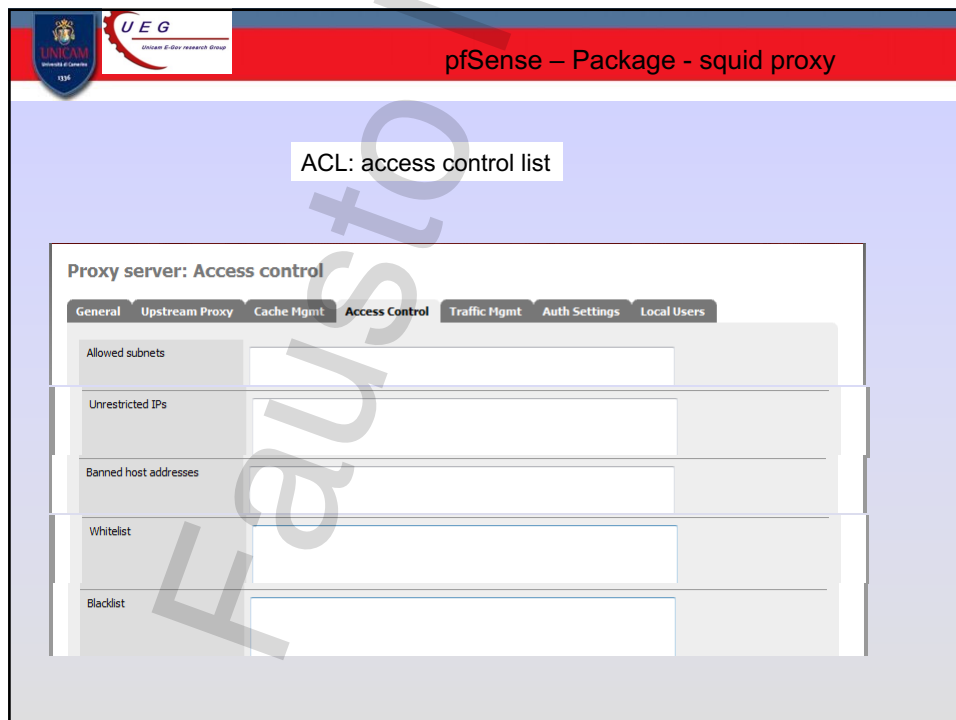
Minimum Object Size 0
Objects smaller than the size specified (in kilobytes) will not be saved on disk. Default: 0 (meaning there is no minimum)

Maximum Object Size 4
Objects larger than the size specified (in megabytes) will not be saved on disk. Default: 4 (MB)

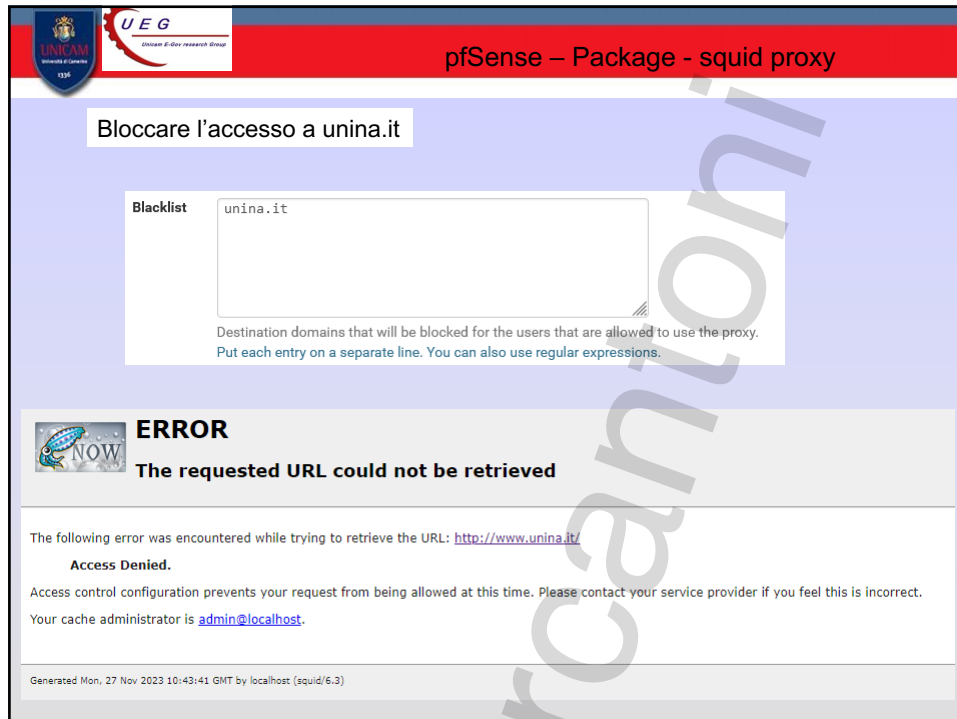
118



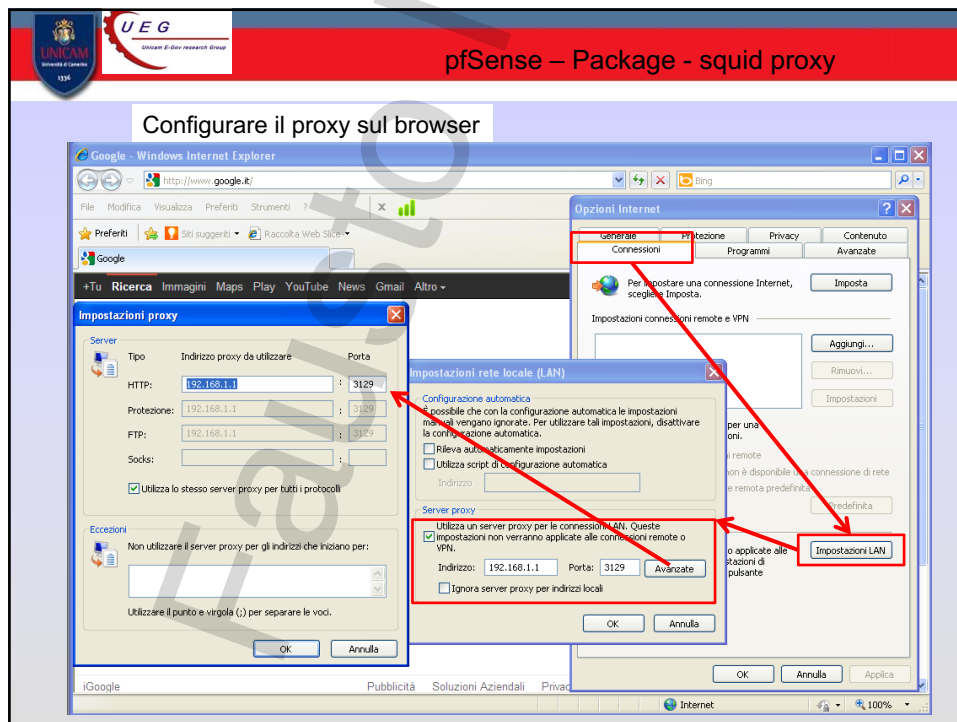
119



120



121



122

UNICAM
Università di Camerino
1336

UEG
Uniview E-Service Group

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	*	*		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

UNICAM
Università di Camerino
1336

UEG
Uniview E-Service Group

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 Diagnostics

- 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

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! [i](#)

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

125

pfSense – Package - squid proxy

Web Service Settings

Lightsquid Web Port
 Port the lighttpd web server for Lightsquid will listen on. (Default: 7445)

Report Template Settings

Language
 Select report language.

Report Template
 Select report template.

Bar Color
 Select bar color.

Refresh Scheduler
 Select data refresh period. The reporting task will be executed every XX minutes/hours.
Legend: (!)(*) Use only with fast hardware (+) Recommended values

Manual Refresh Use these buttons to start a background refresh of the Lightsquid reports.

Will (re)parse today's entries only in Squid's current access.log.

Will (re)parse all entries in all Squid's access logs, including the rotated

126

Lightsquid Web User admin
Username used to access lighttpd. (Default: admin)

Lightsquid Web Password
Password used to access lighttpd. (Default: pfsense)

Links [Open Lightsquid](#) [Open sqstat](#)

Tempo per la connessione esaurito
Si è verificato un errore durante la connessione a 10.1.1.1:7445.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	0/2.20 MIB	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
☐	0/0 B	IPv4 *	LAN subnets	*	*	*	*	none	Default allow LAN to any rule	
☐	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule	
☐	105/93.48 MIB	IPv4 TCP	*	*	3128	*	*	none		
☐	4/223 KiB	IPv4 TCP	*	*	7445	*	*	none		

127

pfSense – Package - squid proxy

ERRORE

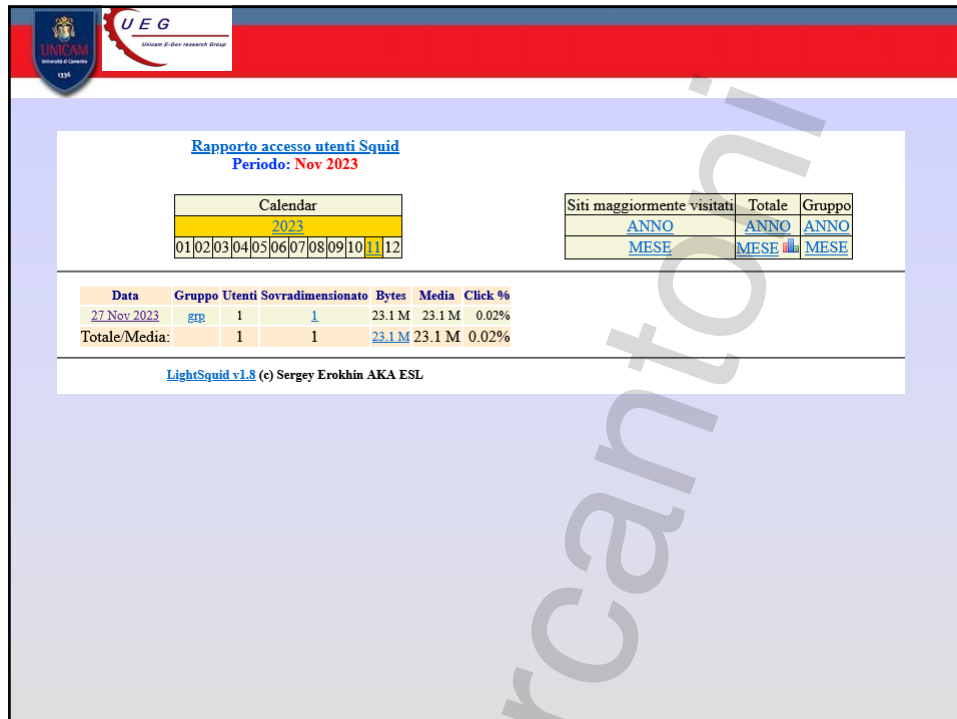
LighSquid diagnostic.
Error : report folder '/var/lightsquid/report' not contain any valid data! Please run lightparser.pl (and check 'report' folder content)
 Please check config file !

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

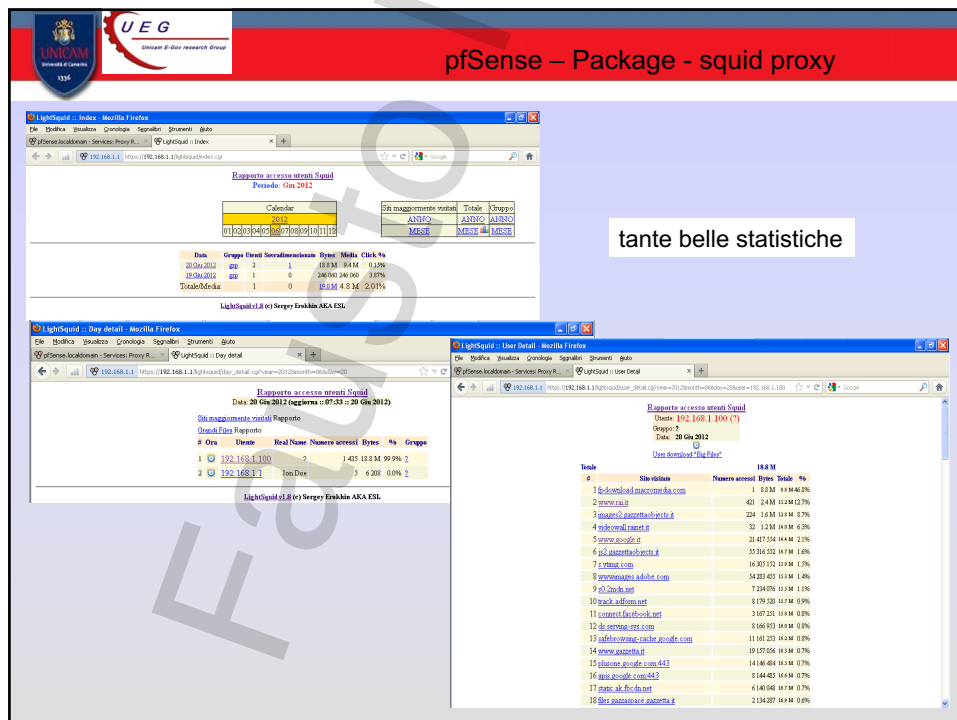
folder content:

no problem!!!

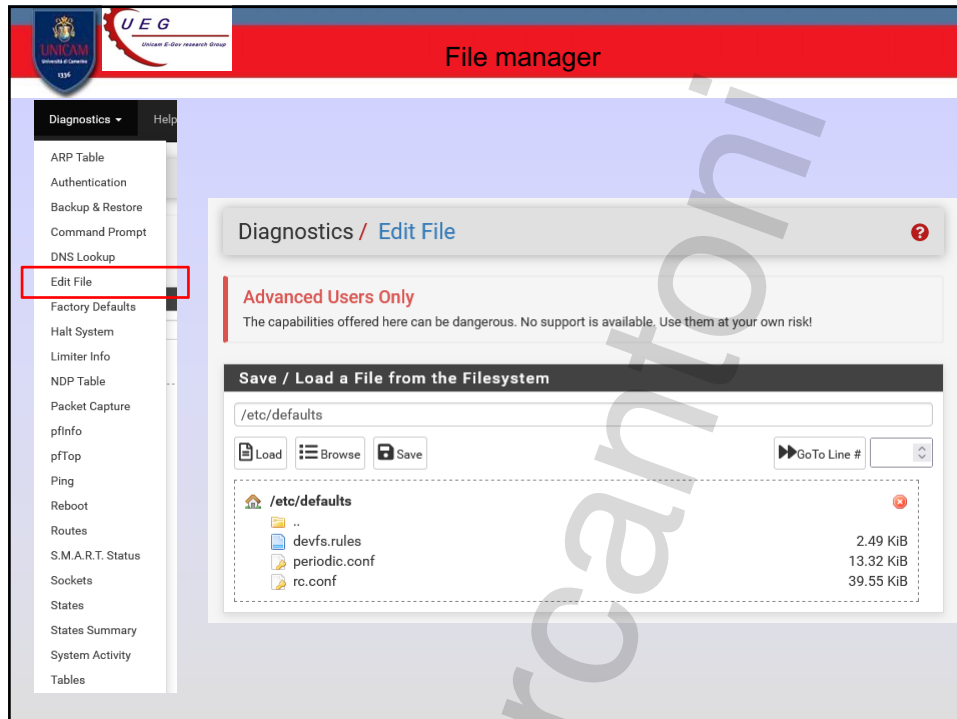
128



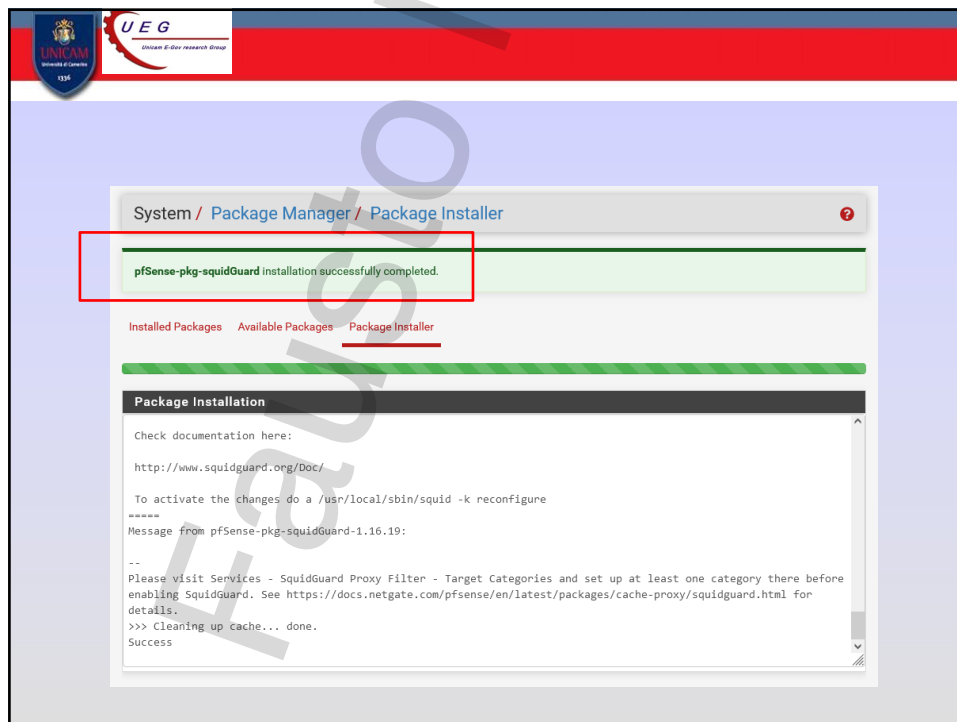
129



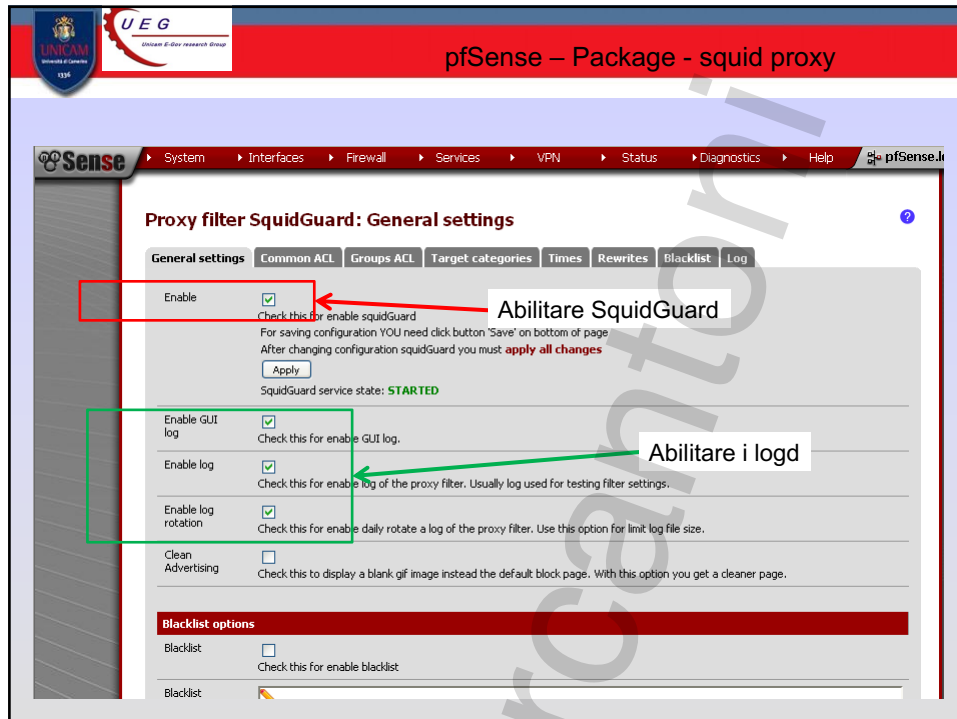
130



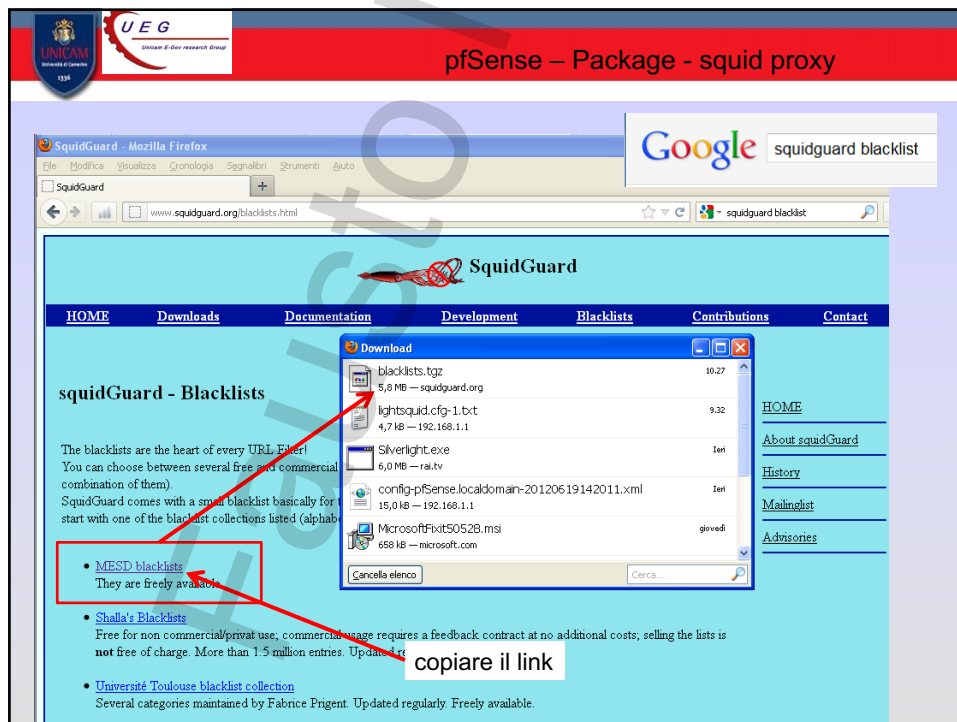
131



132



133



134

UNICAM Université de Caen Normandie 1336 UEG Université E-Ster research Group

pfSense – Package - squid proxy

Google blacklists.tar.gz

Université Toulouse Capitole
https://dsi.ut-capitole.fr/blacklists · Traduci questa pagina

Index of /blacklists/download

Index of /blacklists/download : [] ; associations_religieuses.tar.gz · astrology.ta
11-27 21:21 · 2023-11-27 21:21 ...

<https://github.com/maravento/blackweb>

Index of /blacklists/download

Name	Last modified	Size	De
Parent Directory		-	
LICENSE.pdf	2023-11-27 21:21	76K	
LICENSE.pdf tar.gz	2023-11-27 21:21	45	
MD5SUM.LIST	2023-11-27 21:21	4.1K	
ads.tar.gz	2023-11-27 21:21	26K	
adult.tar.gz	2023-11-27 21:21	17M	
aggressive.tar.gz	2023-11-27 21:21	3.1K	
agressif.tar.gz	2023-11-27 21:21	3.1K	
arjel.tar.gz	2023-11-27 21:21	526	
associations_religieuses.tar.gz	2023-11-27 21:21	191	
astrology.tar.gz	2023-11-27 21:21	467	
audio-video.tar.gz	2023-11-27 21:21	24K	
bank.tar.gz	2023-11-27 21:21	9.6K	
bitcoin.tar.gz	2023-11-27 21:21	2.1K	
blacklists.tar.gz	2023-11-27 21:21	27M	
blacklists_for_dansguardian.tar.gz	2023-11-27 21:27	27M	
blacklists_for_pfsense.tar.gz	2023-11-27 21:26	17M	
blacklists_for_pfsense_reduced.tar.gz	2023-11-27 21:26	17M	
blocked.src	2004-11-18 08:05	5.5K	
blog.tar.gz	2023-11-27 21:21	10K	
catalogue-biu-toulouse.tar.gz	2023-11-27 21:21	214	
cc-by-sa-4.0.pdf	2023-11-27 21:21	76K	
cc-by-sa-4.0.pdf tar.gz	2023-11-27 21:21	45	

135

UNICAM Université de Caen Normandie 1336 UEG Université E-Ster research Group

pfSense – Package - squid proxy

0 % https://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

Download Cancel Restore Default

Enter FTP or HTTP path to the blacklist archive here.

```

Begin blacklist update
Start download.
Download archive https://dsi.ut-capitole.fr/blacklists/download
/blacklists_for_pfsense.tar.gz
Download complete
Unpack archive
Scan blacklist categories.
Found 63 items.
Start rebuild DB.
Copy DB to workdir.
Reconfigure Squid proxy.
Blacklist update complete.

```

<https://dsi.ut-capitole.fr/blacklists/download/>

136

pfSense – Package - squid proxy

Package / Proxy filter SquidGuard: General settings / General settings

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync

General Options

Enable ☒ Check this option to enable squidGuard.
Important: Please set up at least one category on the 'Target Categories' tab before enabling. See [this link](#) for details.
 The Save button at the bottom of this page must be clicked to save configuration changes.
 To activate squidGuard configuration changes, **the Apply button must be clicked.**

☒ Apply

SquidGuard service state: **STARTED**

Logging options

Enable GUI log ☒ Check this option to log the access to the Proxy Filter GUI.

Enable log ☒ Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.

Enable log rotation ☒ Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.

137

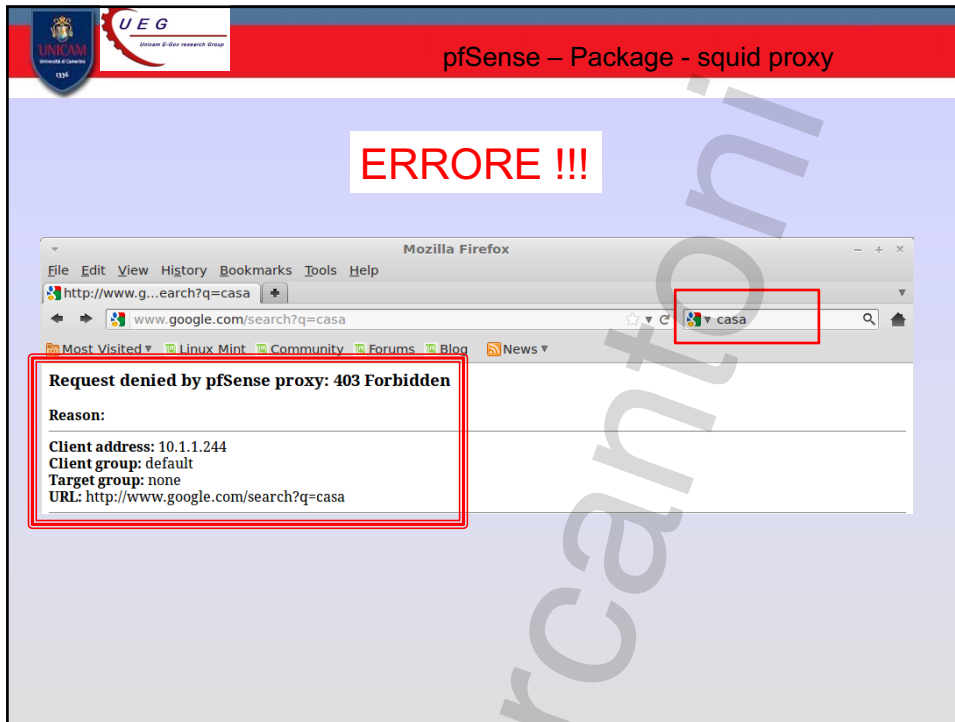
pfSense – Package - squid proxy

Blacklist options

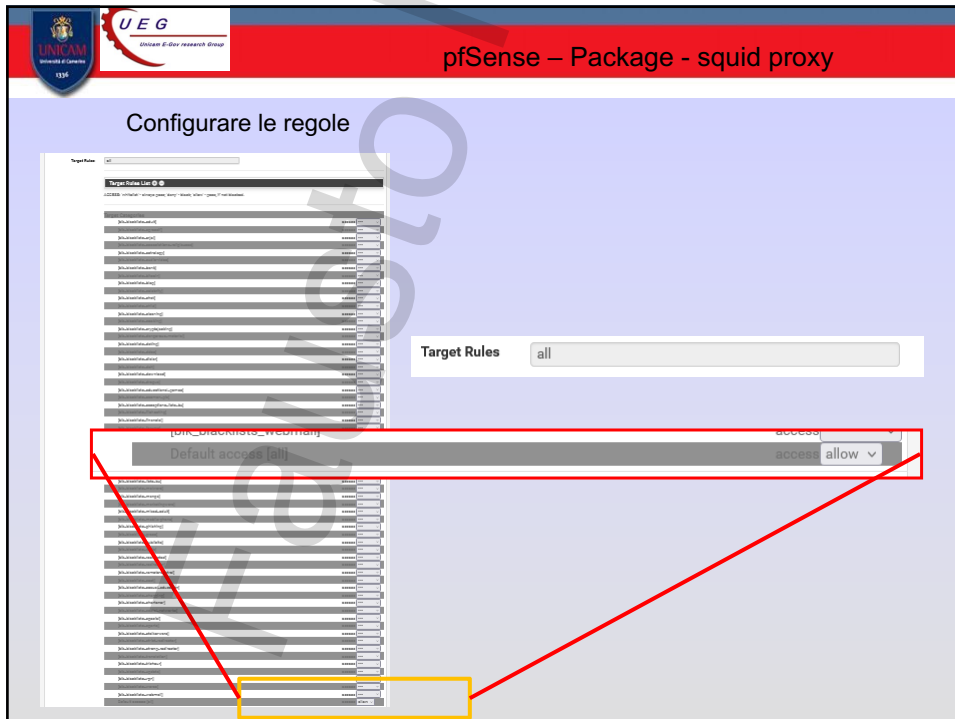
Blacklist ☒ Check this option to enable blacklist

abilitare le blacklist

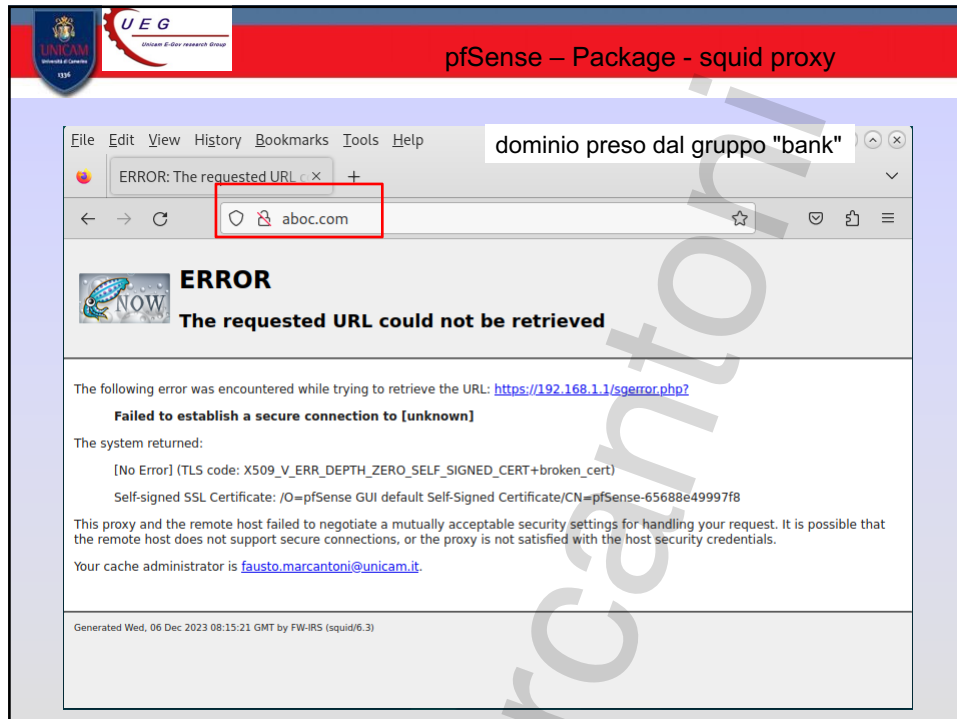
138



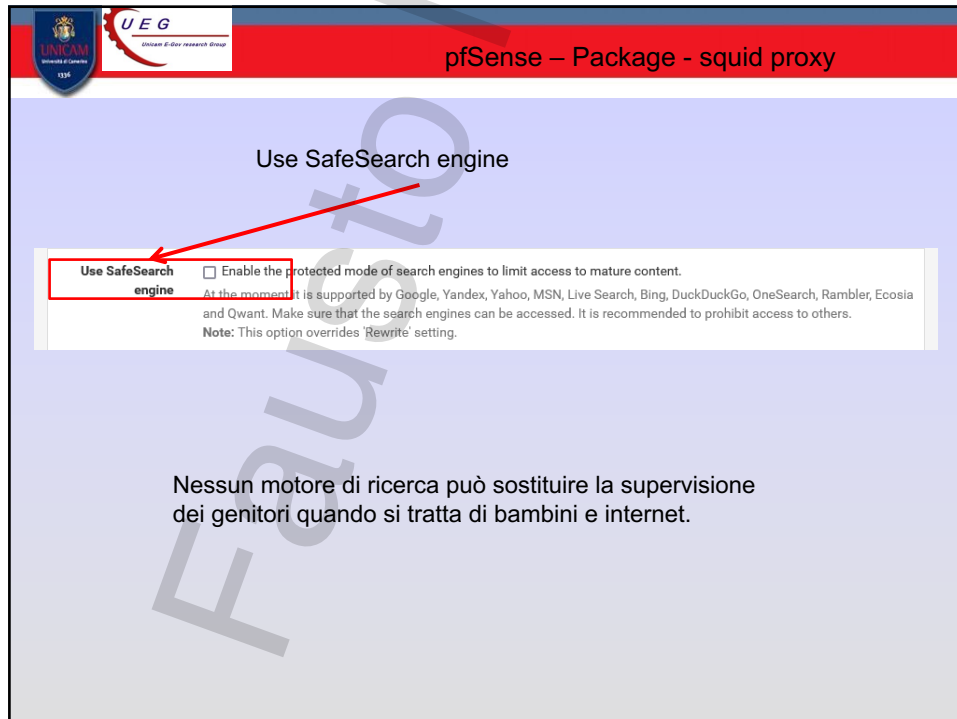
139



140



141



142

pfSense – Package - squid proxy

Package / Proxy filter SquidGuard: General settings / General settings

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync

Le Regole

Le Regole fatte per gruppi di

- Utenti
- Network
- IP address

Temporizzazione delle regole

Debug: LOG !!!!

143

pfSense – Package - squid proxy

Attenzione

Request denied by pfSense proxy: 403 Forbidden

Reason:

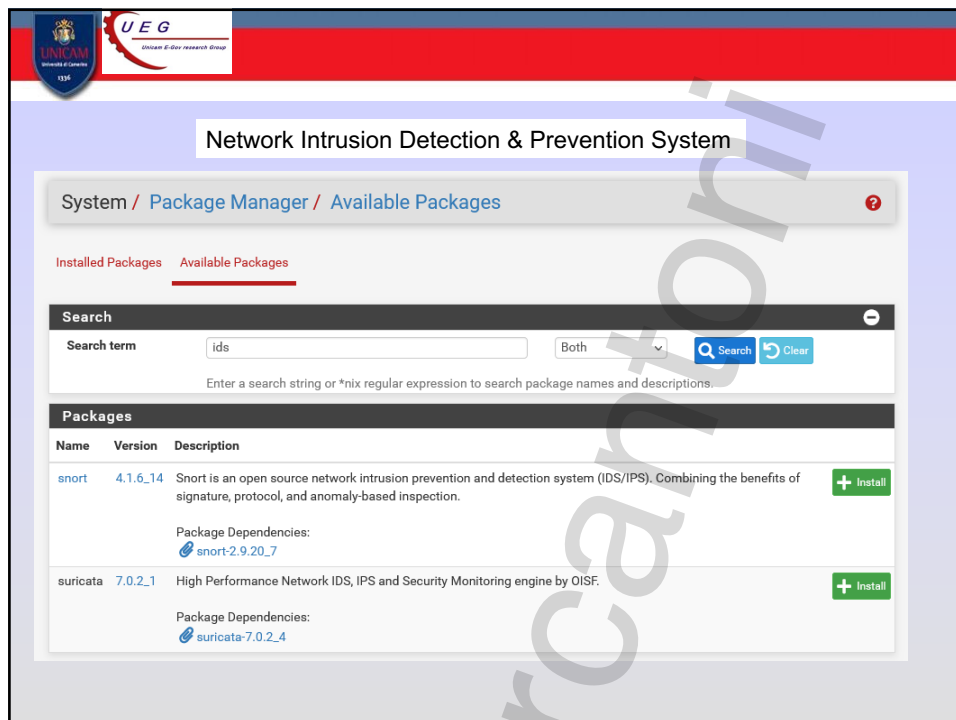
Client address: 10.1.1.244
Client group: default
Target group: in-addr
URL: http://10.1.1.1/

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 the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.

144



145

Snort/Suricata

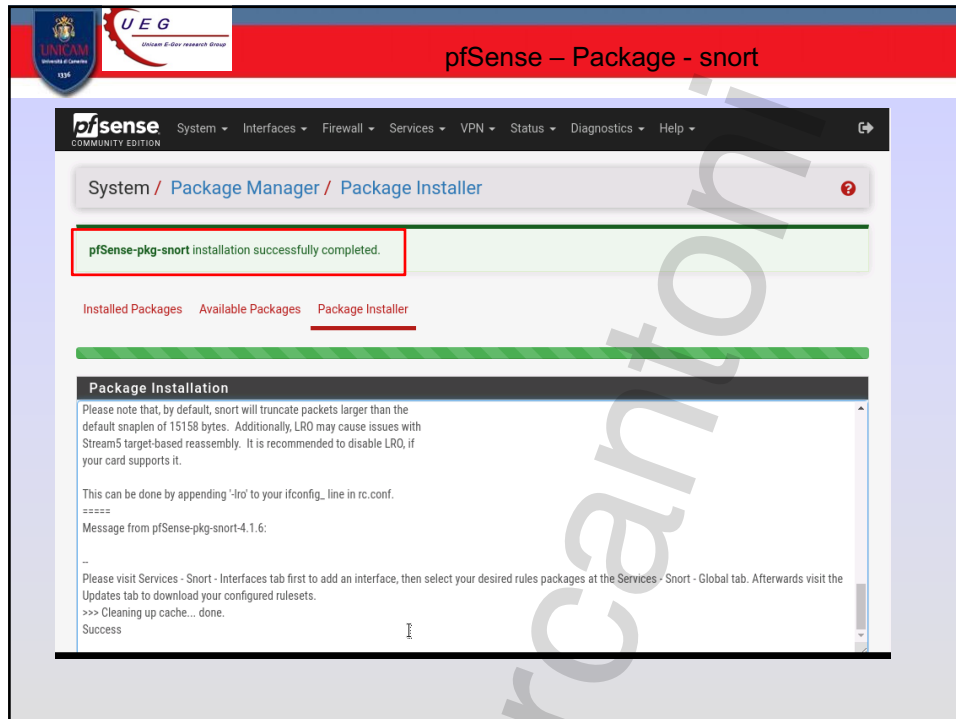
- Snort and Suricata are pfSense software packages for network intrusion detection. Depending on their configuration, they can require a significant amount of RAM. 1 GB should be considered a minimum but some configurations may need 2 GB or more, not counting RAM used by the operating system, firewall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

<https://www.snort.org/>

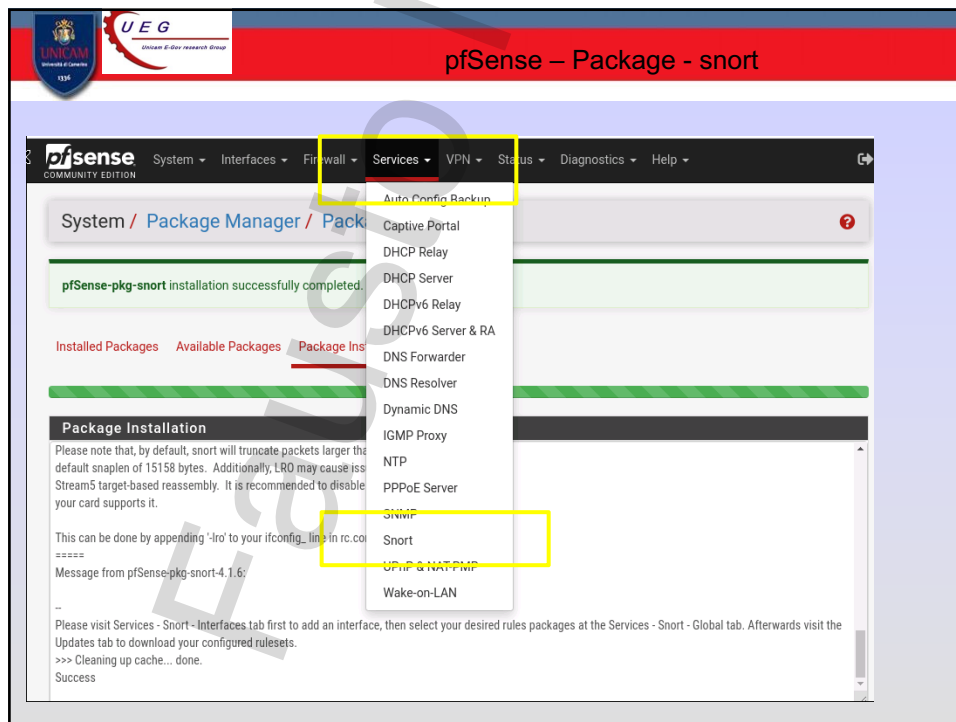
<https://suricata.io/>




146



147



148

Services / Snort / WAN - Interface Settings

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

WAN Settings WAN Categories WAN Rules WAN Variables WAN Preprocs WAN IP Rep WAN Logs

General Settings

Enable ☒ Enable interface **abilitare snort**

Interface WAN (em0)

Choose the interface where this snort instance will inspect traffic.

Description WAN

Enter a meaningful description here for your reference.

Snap Length 1518

Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Alert Settings

Send Alerts to System Log ☐ Snort will send Alerts to the firewall's system log. Default is Not Checked.

Enable Packet Captures ☐ Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

Enable Unified2 Logging ☐ Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.

Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

149

fausto.marcantonio@unicam.it My Account Sign Out

Documents Downloads Products Community Talos Resources Contact

Search Rule Doc Search

Account

Linkcode

Subscription

Receipts

False Positive

Snort License

Resources

Login

Email fausto.marcantonio@unicam.it

Password

Edit

Delete Account

Snort License Agreement

License Terms Accepted YES

Mailing Lists

☐ Snort-users

☐ Snort-sigs

☐ Snort-devel

☐ Snort-openappid

150

UNICAM Università di Camerino 1336 UEG Italian E-Dev research Group

pfSense – Package - snort

prima di tutto ...

per richiedere un oinkcode

Snort Subscriber Rules

Enable Snort VRT ☒ Click to enable download of Snort free Registered User or paid Subscriber rule sets.

[Sign Up for a free Registered User Rules Account](#)

[Sign Up for paid Snort Subscriber Rule Set \(by Talos\)](#)

Snort Oinkmaster Code

Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL)

Snort GPLv2 Community Rules

Enable Snort GPLv2 ☐ Click to enable download of Snort GPLv2 Community rules

The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

Emerging Threats (ET) Rules

Enable ET Open ☐ Click to enable download of Emerging Threats Open rules

ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.

Enable ET Pro ☐ Click to enable download of Emerging Threats Pro rules

151

UNICAM Università di Camerino 1336 UEG Italian E-Dev research Group

pfSense – Package - snort

regole installate

aggiornare le regole

Services / Snort / Updates

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Downloaded	Not Downloaded
Snort GPLv2 Community Rules	Not Enabled	Not Enabled
Emerging Threats Open Rules	Not Enabled	Not Enabled
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort AppID Open Text Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

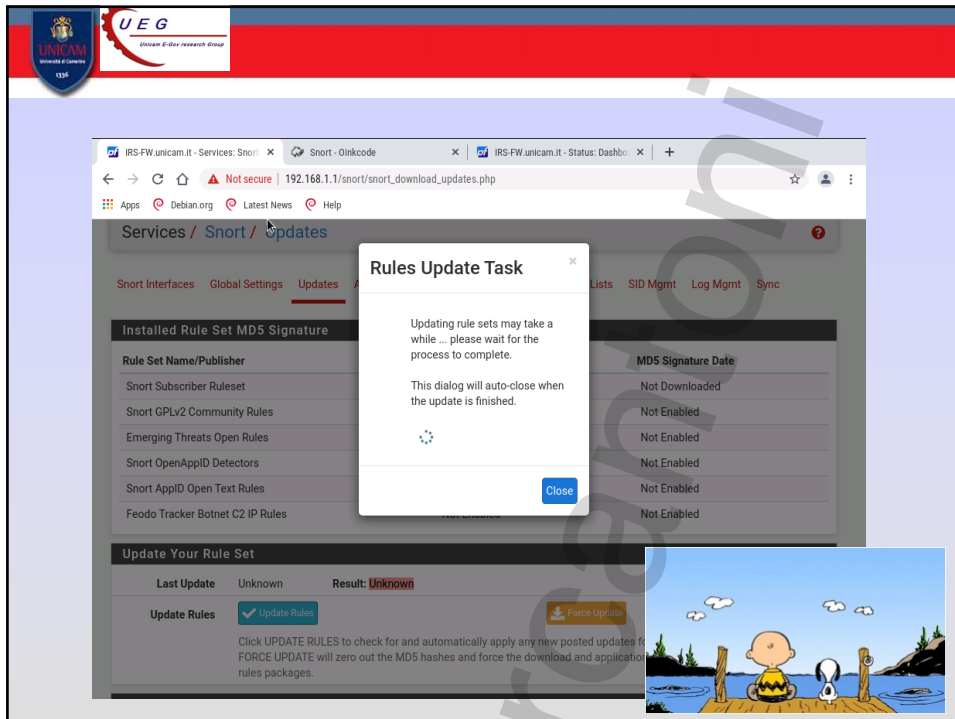
Update Your Rule Set

Last Update: Unknown Result: Unknown

Update Rules

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

152



153

pfSense – Package - snort

Block Settings

Block Offenders ☒ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode Legacy Mode

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. **WARNING:** Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, ems, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Kill States ☒ Checking this option will kill firewall established states for the blocked IP. Default is checked.

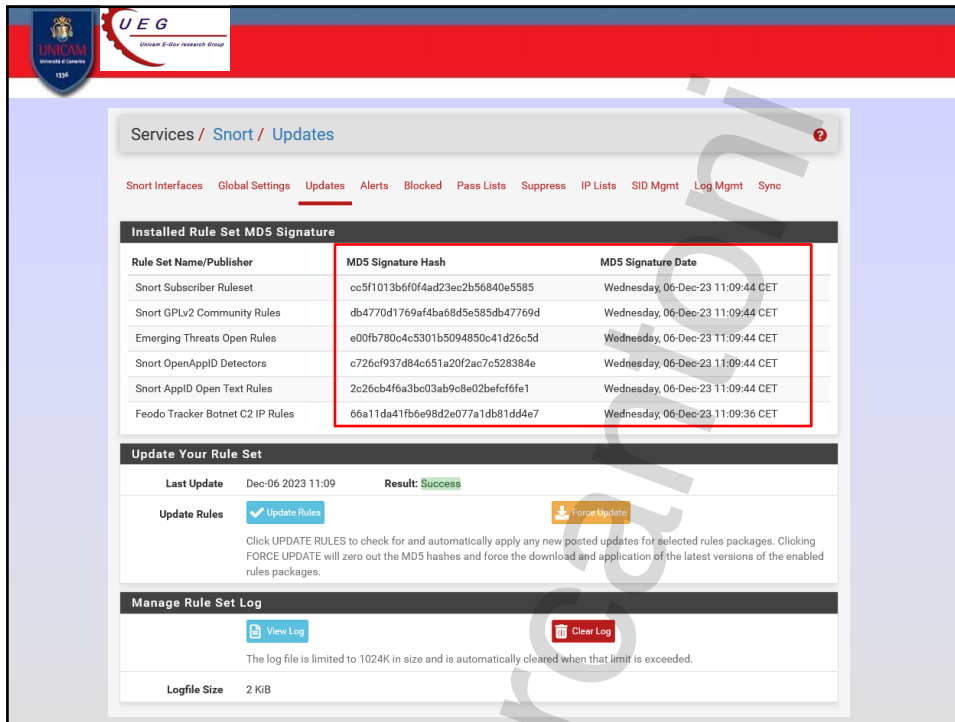
Which IP to Block BOTH

Select which IP extracted from the packet you wish to block. Default is BOTH.

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, ems, 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



Services / Snort / Updates

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	cc5f1013b6f0f4ad23ec2b56840e5585	Wednesday, 06-Dec-23 11:09:44 CET
Snort GPLv2 Community Rules	db4770d1769af4ba68d5e585db47769d	Wednesday, 06-Dec-23 11:09:44 CET
Emerging Threats Open Rules	e00fb780c4c5301b5094850c41d26c5d	Wednesday, 06-Dec-23 11:09:44 CET
Snort OpenAppID Detectors	c726cf937d84c651a20f2ac7c528384e	Wednesday, 06-Dec-23 11:09:44 CET
Snort AppID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Wednesday, 06-Dec-23 11:09:44 CET
Feodo Tracker Botnet C2 IP Rules	66a11da41fb6e98d2e077a1db81dd4e7	Wednesday, 06-Dec-23, 11:09:36 CET

Update Your Rule Set

Last Update: Dec-06 2023 11:09 Result: Success

Update Rules [Update Rules](#) [Force Update](#)

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

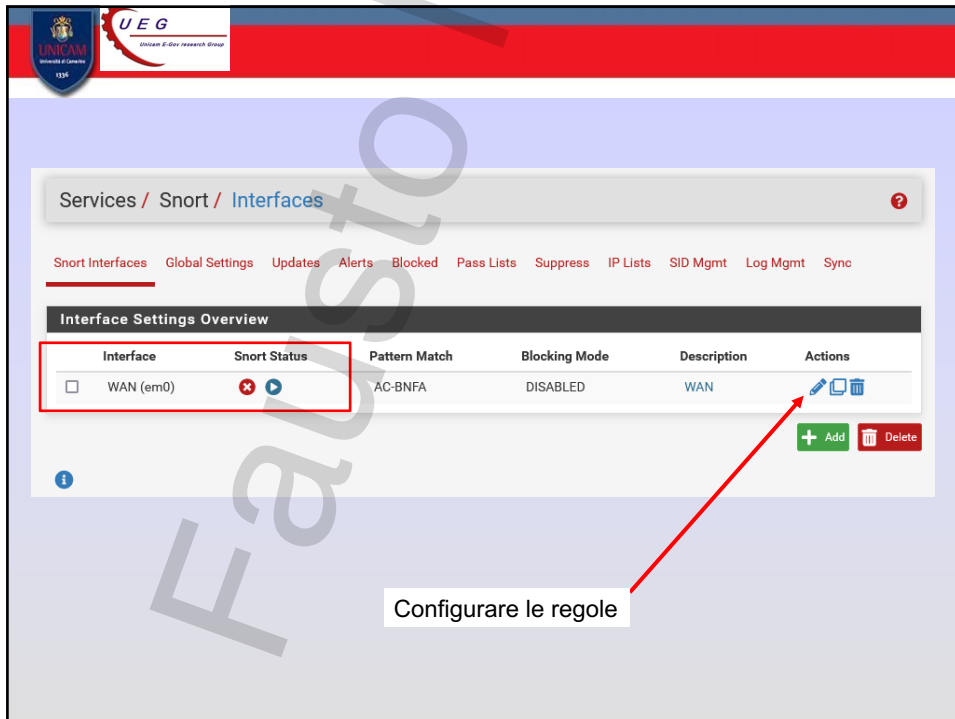
Manage Rule Set Log

[View Log](#) [Clear Log](#)

The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.

Logfile Size 2 KiB

155



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	Configure Copy Delete

[+ Add](#) [Delete](#)

Configurare le regole

156

UNICAM University of Cambridge 1356 UEG Uman E-Ger research Group

pfSense – Package - snort

Services / Short / Interface Settings / WAN - Categories

Short Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

WAN Settings **WAN Categories** WAN Rules WAN Variables WAN Preprocs WAN IP Rep WAN Logs

Select the rulesets (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)

Enable	Ruleset: FEODO Tracker Botnet C2 IP Rules
☒	Feodo Tracker Botnet C2 IP Rules

Enable	Ruleset: ET Open Rules	Enable	Ruleset: Snort Text Rules	Enable	Ruleset: Snort SO Rules	Enable	Ruleset: Snort OPENAPPID Rules
☒	emerging-activex.rules	☐	snort_app-detect.rules	☐	snort_browser-chrome.so.rules	☒	openappid-ads.rules
☒	emerging-attack_response.rules	☐	snort_attack-responses.rules	☐	snort_browser-ie.so.rules	☒	openappid-browser_plugin.rules
☒	emerging-botcc.portgrouped.rules	☐	snort_backdoor.rules	☐	snort_browser-other.so.rules	☒	openappid-bussiness_applications.rules
☒	emerging-botcc.rules	☐	snort_bad-traffic.rules	☐	snort_browser-webkit.so.rules	☒	openappid-collaboration.rules
☒	emerging-chat.rules	☐	snort_blacklist.rules	☐	snort_exploit-kit.so.rules	☒	openappid-database.rules
☒	emerging-ciarmy.rules	☐	snort_botnet-cnc.rules	☐	snort_file-executable.so.rules	☒	openappid-file_storage.rules
☒	emerging-compromised.rules	☐	snort_browser-chrome.rules	☐	snort_file.flash.so.rules	☒	openappid-file_transfer.rules
☒	emerging-current_events.rules	☐	snort_browser-firefox.rules	☐	snort_file-image.so.rules	☒	openappid-games.rules

157

UNICAM University of Cambridge 1356 UEG Uman E-Ger research Group

Services / Snort / Alerts

Short Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Alert Log View Settings

Interface to Inspect: WAN (em0) ☐ Auto-refresh view 250 Alert lines to display. Save

Alert Log Actions Download Clear

Alert Log View Filter

0 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID/SID	Description
------	--------	-----	-------	-------	-----------	-------	----------------	-------	---------	-------------

Services / Snort / Blocked Hosts

Short Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Blocked Hosts and Log View Settings

Blocked Hosts Download Clear

All blocked hosts will be saved All blocked hosts will be removed

Refresh and Log View Save Refresh Default is ON 500 Number of blocked entries to view. Default is 500

Save auto-refresh and view settings

Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)

#	IP	Alert Descriptions and Event Times	Remove
There are currently no hosts being blocked by Snort on Legacy Mode Blocking interfaces.			

Block Settings

Block Offenders ☐ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

Alerts

Blocked

158

UNICAM Università di Camerino 1336 UEG Unican E-Gov research Group

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

UNICAM Università di Camerino 1336 UEG Unican E-Gov research Group

pfSense – Package - snort

Status / System Logs / System / General

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

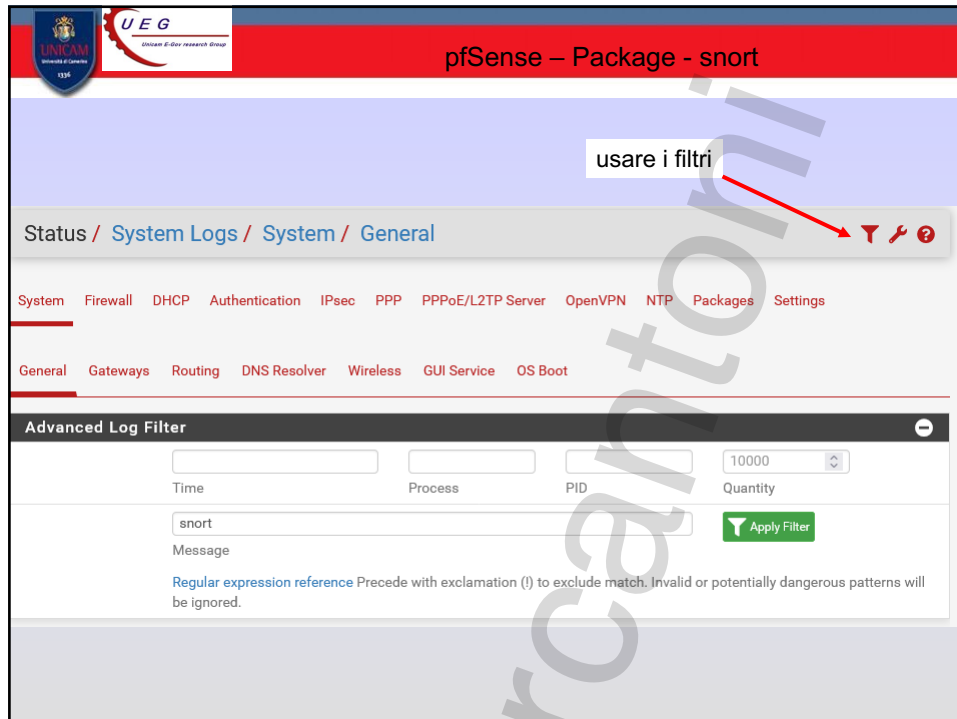
General Gateways Routing DNS Resolver Wireless GUI Service OS Boot

errore: visualizzare il file di log

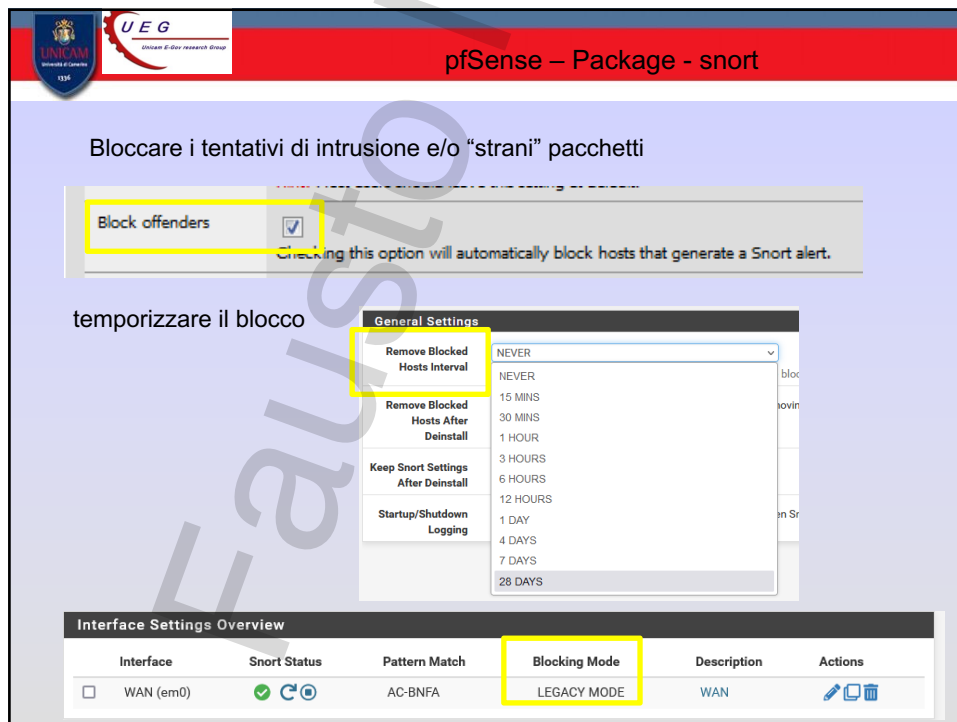
Last 25 General Log Entries. (Maximum 10000)

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

UNICAM Università di Camerino 1336 UEG Italian E-Dev research Group

pfSense – Package - snort

Services / Snort / Blocked Hosts

Short Interfaces Global Settings Updates Alerts **Blocked** Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Blocked Hosts and Log View Settings

Blocked Hosts [Download](#) [Clear](#)
All blocked hosts will be saved All blocked hosts will be removed

Refresh and Log View [Save](#) ☒ Refresh
Save auto-refresh and view settings Default is ON Number of blocked entries to view. Default is 500

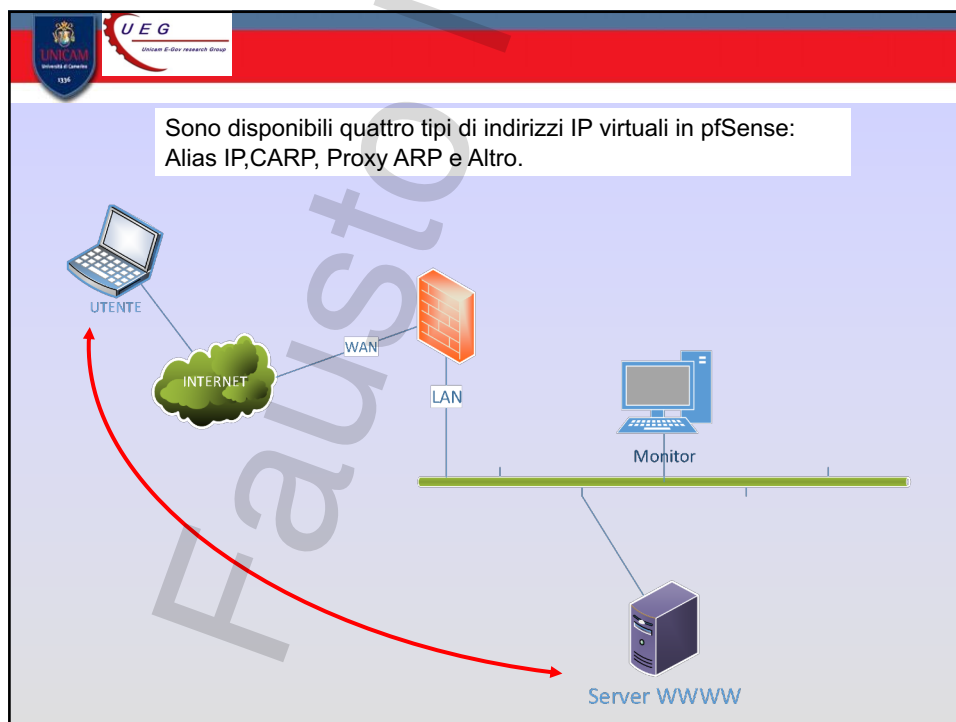
Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)

#	IP	Alert Descriptions and Event Times	Remove
1	193.205.92.219	ET SCAN Suspicious inbound to MySQL port 3306 – 2023-12-06 11:39:33 ET SCAN Potential VNC Scan 5900-5920 – 2023-12-06 11:39:35 ET SCAN Suspicious inbound to Oracle SQL port 1521 – 2023-12-06 11:39:37	×

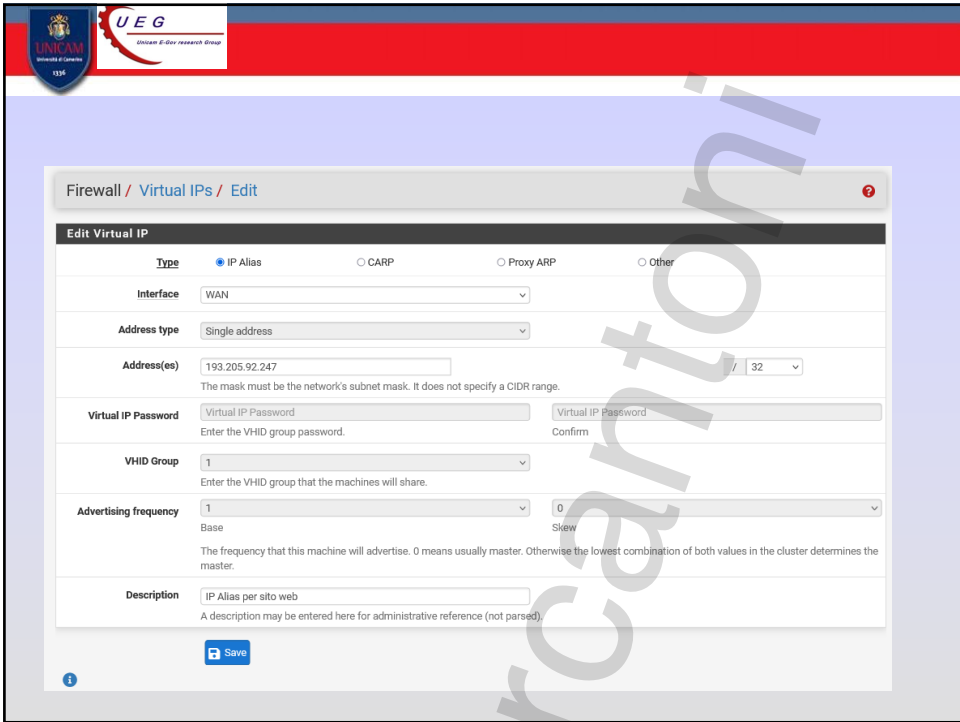
1 host IP address is currently being blocked Snort on Legacy Blocking Mode interfaces.

Sbloccare l'host

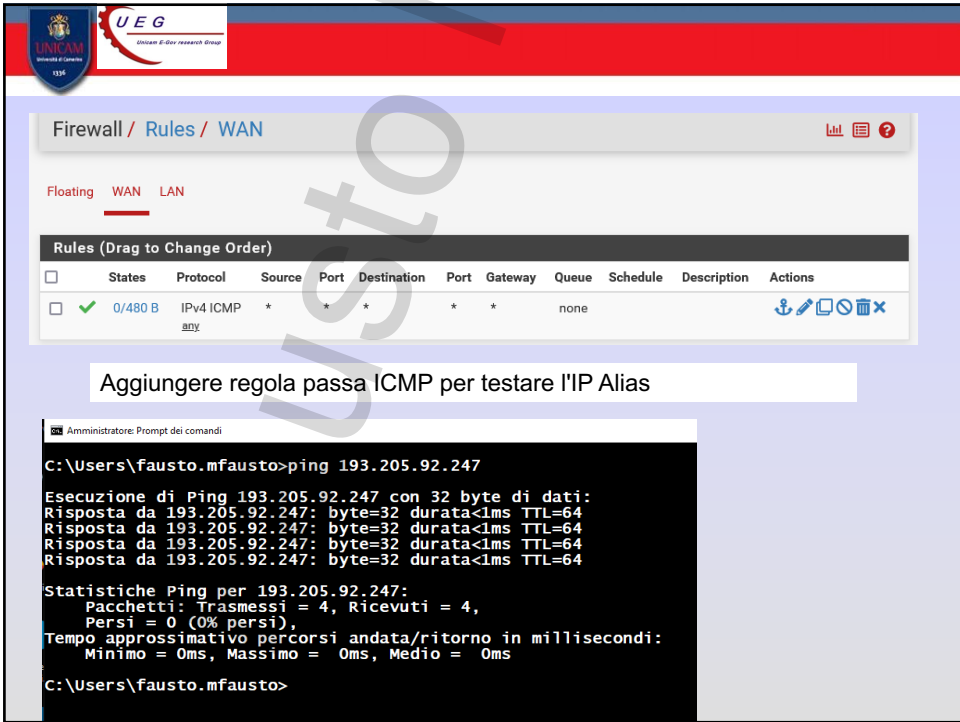
163



164



165



166

Firewall / NAT / 1:1

Port Forward 1:1 Outbound NPT

NAT 1:1 Mappings

☐	Interface	External IP	Internal IP	Destination IP	Description	Actions
☒	WAN	193.205.92.247	192.168.1.11	*		Edit Copy Delete

[Add](#) [Add](#) [Delete](#) [Toggle](#) [Save](#)

Firewall / Rules / WAN

Floating WAN LAN

Rules (Drag to Change Order)

☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	0/0 B	IPv4 ICMP any	*	*	*	*	*	none			Edit Copy Delete
☒	2/63 KiB	IPv4 TCP	*	*	*	80 (HTTP)	*	none			Edit Copy Delete

[Add](#) [Add](#) [Delete](#) [Toggle](#) [Copy](#) [Save](#) [Separator](#)

167

Metasploit2 - Linux

Non sicuro | 193.205.92.247

Importa preferiti Barra dei segnalibri MEGA 1.41% The NeoSmart Files

metasploitable2

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

168



169

Interfaces / Wireless

Interface Assignments Interface Groups **Wireless** VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Interfaces / Wireless / Edit

Wireless Interface Configuration

Parent Interface: run0 (Ralink 11n Adapter, class 6/2, rev 2.00/1.01, addr 2)

Mode: Access Point

Description: AP-IRS
A description may be entered here for administrative reference (not parsed).

Save

Interfaces / Interface Assignments

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Interface	Network port	
WAN	em0 (00:50:56:2b:c7:16)	
LAN	em1 (00:50:56:22:d5:f9)	Delete
WIFI	run0_wlan0 (AP-IRS)	Delete

Save

170

Interfaces / WIFI (run0_wlan0)

General Configuration

Enable ☒ Enable interface

Description WIFI
Enter a description (name) for the interface here.

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

Static IPv4 Configuration

IPv4 Address 192.168.3.1 / 24

IPv4 Upstream gateway None [+ Add a new gateway](#)

Common Wireless Configuration - Settings apply to all wireless networks on run0.

Persist common settings ☐ Preserve common wireless configuration through interface deletions and reassignments.

Standard 802.11ng

802.11g OFDM Protection Mode Off
For IEEE 802.11g, use the specified technique for protecting OFDM frames in a mixed 11b/11g network.

Channel 11b/g/n - 6
Legend: wireless standards - channel # (frequency @ max TX power - TX power allowed in reg. domain)
Not all channels may be supported by some cards. Auto may override the wireless standard selected above.

Channel width Auto
Channel width for 802.11n mode. Not all cards may support channel width changing.

171

Network-Specific Wireless Configuration

Mode Access Point

SSID IRS-WiFi

Minimum wireless standard Any
When operating as an access point, allow only stations capable of the selected wireless standard to associate (stations not capable are not permitted to associate)

Allow intra-BSS communication ☐ Allow packets to pass between wireless clients directly when operating as an access point
Provides extra security by isolating clients so they cannot directly communicate with one another

Enable WME ☒ Force the card to use WME (wireless QoS)

Hide SSID ☐ Disable broadcasting of the SSID for this network (This may cause problems for some clients, and the SSID may still be discovered by other means.)

WPA

Enable ☒ Enable WPA

WPA mode WPA2

WPA Pairwise AES (recommended)

WPA Key Management Mode Pre-Shared Key

WPA Pre-Shared Key unicom2023
WPA Passphrase must be between 8 and 63 characters long

172

Services / DHCP Server / WIFI

LAN **WIFI**

General DHCP Options

DHCP Backend: Kea DHCP

Enable: ☒ Enable DHCP server on WIFI interface

Deny Unknown Clients: ☐ Allow all clients

Ignore Client Identifiers: ☐ Do not record a unique identifier (UID) in client lease data if present in the client DHCP request

Primary Address Pool

Subnet: 192.168.3.0/24

Subnet Range: 192.168.3.1 - 192.168.3.254

Address Pool Range: From 192.168.3.10 To 192.168.3.200

The specified range for this pool must not be within the range configured on any other address pool for this interface.

173

Firewall / Rules / WIFI

Floating WAN LAN **WIFI**

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	✓	18/159 KiB	IPv4 *	WIFI subnets	*	*	*	none		

Status / Wireless

Rescan has been initiated in the background. Refresh this page in 10 seconds to see the results.

Status (WIFI)

Nearby Access Points or Ad-Hoc Peers

SSID	BSSID	CHAN	RATE	RSSI	INT	CAPS
0x00000000	ea:40:66:7d:e6:d1	6	54M	-21:-51	300	EP RSN HTCAP WME
Unicam-Guest	70:db:98:15:c3:d0	6	54M	-29:-57	102	E BSSLOAD HTCAP WME
eduroam	70:db:98:15:c3:d2	6	54M	-34:-67	102	EP BSSLOAD HTCAP RSN WME

Associated or Ad-Hoc Peers

ADDR	AID	CHAN	RATE	RSSI	IDLE	TXSEQ	RXSEQ	CAPS	ERP
5e:3e:11:59:33:3f	1	6	58M	6.5	0	172	13392	EPS	AQEPHTTr

Rescan

174



175



176

UNICAM
Universit  di Camerino
1334

UEG
Univ. E-Gov research Group

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

UNICAM
Universit  di Camerino
1334

UEG
Univ. E-Gov research Group

pfSense – Package - antivirus

pfSense

System | Interfaces | Firewall | **Services**

Status: Dashboard

System Information

Name	pfSense.localdomain
Version	2.0-RELEASE (i386) built on Tue Sep 13 17:00:00
	Unable to check for updates.
Platform	pfSense
CPU Type	Intel(R) Core(TM)2 Duo CPU
Uptime	00:11
Current	Thu Nov 24 9:26:55 UTC 201

- Antivirus
- Captive Portal
- DHCP Relay
- DHCP Server
- DNS Forwarder
- Dynamic DNS
- IGMP proxy
- Load Balancer
- OLSR
- OpenNTPD
- PPPoE Server
- RIP
- SNMP
- UPnP & NAT-PMP
- Wake on LAN

178

UNICAM
University of Coimbra
1396

UEG
Universidade E-Gov research Group

pfSense – Package - antivirus

Antivirus: General page

General page HTTP proxy Settings

Service	Status	Version
HTTP Antivirus Proxy (Stopped)	Stopped	havp-0.91_1 HTTP Antivirus Proxy
Antivirus Server ()	Stopped	ClamAV 0.97.2/13985/Thu Nov 24 03:07:14 2011

Antivirus Update

[Start Update](#)

Update status

2011.11.24 09:24:27 Antivirus update started.
2011.11.24 09:24:27 Antivirus database already is updated.
2011.11.24 09:25:10 Antivirus update end.

Antivirus Base Info

Database	Date	Size	Ver.	Signatures	Builder
main.cvd	2011.10.11	29.33 M	54	1044387	sven
daily.cvd	2011.11.23	0.72 M	13985	31487	guitar
safebrowsing.cvd	2011.11.24	19.40 M	33906	878906	google
bytecode.cvd	2011.11.22	0.05 M	154	38	edwin

File scanner

Path:
Enter file path or catalog for scanning.

☒ Squid cache path (scan you squid cache now).
☒ Common DB path.
☒ Temp path.

Scanner status

Not found.

179

UNICAM
University of Coimbra
1396

UEG
Universidade E-Gov research Group

pfSense – Package - antivirus

Antivirus: HTTP proxy (havp + clamav)

General page HTTP proxy Settings

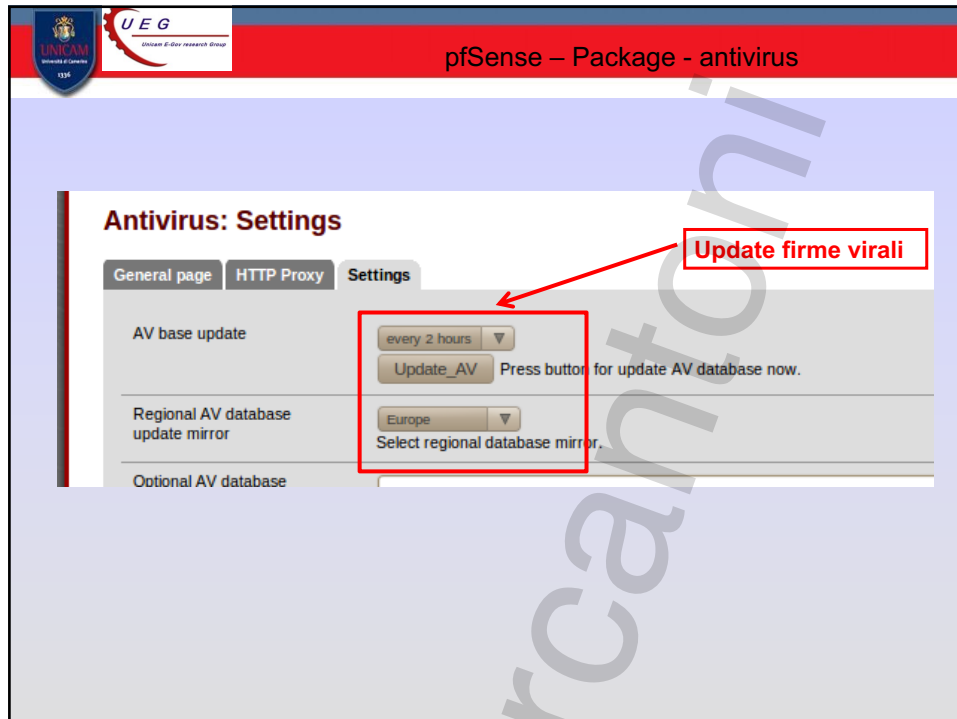
Enable ☒ Check this for enable proxy.

Proxy mode **Parent for Squid**
Select interface mode:
standard - client(s) bind to the 'proxy port' on selected interface(s);
parent for squid - configure HAVP as parent for Squid proxy;
transparent - all http requests on interface(s) will be translated to the HAVP proxy server without any client(s) additional o
parent for squid with 'transparent' Squid proxy);
internal - HAVP listen internal interface (127.0.0.1) on 'proxy port', use you own traffic forwarding rules.

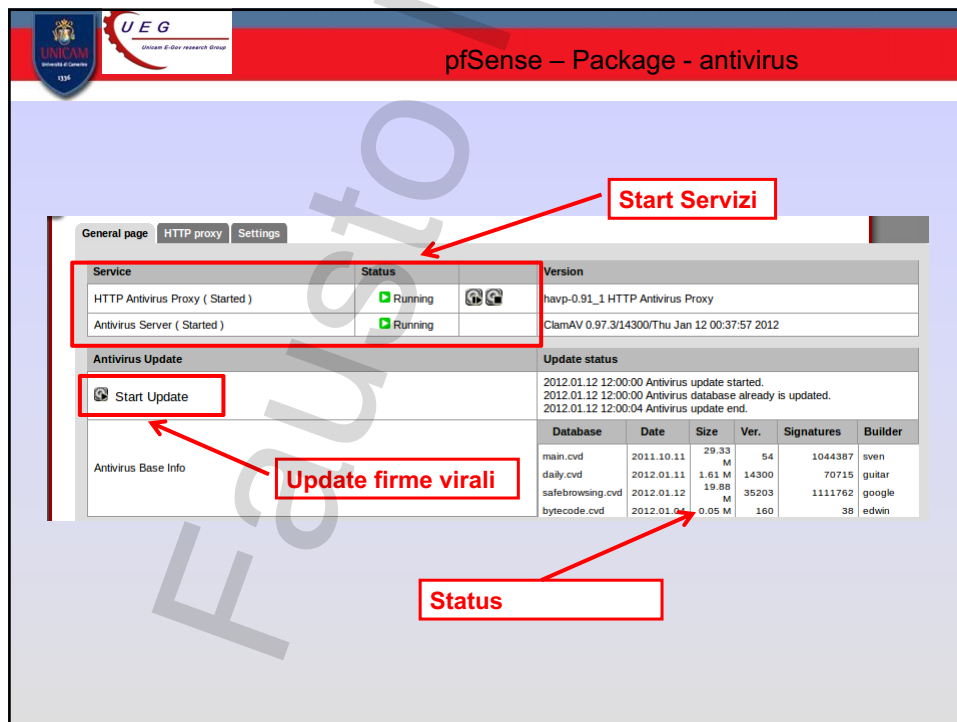
Proxy interface(s) WAN LAN loopback
The interface(s) for client connections to the proxy. Use 'Ctrl' + L.Click for multiple selection.

Proxy port 3125
This is the port the proxy server will listen on (for example: 8080). This port must be different from Squid proxy.

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

UNICAM
Università di Camerino
1336

UEG
University of Engineering and Graphics

pfSense – Captive Portal Https Login

Captive Portal Https Login

System: Certificate Authority Manager

CAs Certificates Certificate Revocation

Name	Internal	Issuer	Certificates	Distinguished Name
CAinformatica	YES	self-signed	1	emailAddress=root@informatica, ST=Macerata, O=informatica, L=Camerino, CN=internal-ca, C=IT
ca intermediate1	YES	external	0	emailAddress=root@informatica, ST=Macerata, O=informatica, L=Camerino, CN=caintermediate1, C=US

Additional trusted Certificate Authorities can be added here

intermediate certificate authority

Internal Certificate Authority

185

UNICAM
Università di Camerino
1336

UEG
University of Engineering and Graphics

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

186

UNICAM Università di Camerino 1336 UEG Italian E-Gov research Group

pfSense – Captive Portal Https Login

Captive Portal Https Login

HTTPS private key

export key

System: Certificate Manager

File Download

Do you want to open or save this file?

Name: CAinternalbase.key
Type: HTML Document, 1.63KB
From: 10.10.10.1

Open Save Cancel

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. [What's the risk?](#)

In Use

Open direttamente
Fare Copia e Incolla del certificato

189

UNICAM Università di Camerino 1336 UEG Italian E-Gov research Group

pfSense – Captive Portal Https Login

Captive Portal Https Login

HTTPS intermediate certificate

export key

System: Certificate Manager

File Download - Security Warning

0% of system_camanager.php from 10.10.10.1 Com...

Do you want to open or save this file?

Name: ca+intermediate1.crt
Type: Security Certificate, 1.54KB
From: 10.10.10.1

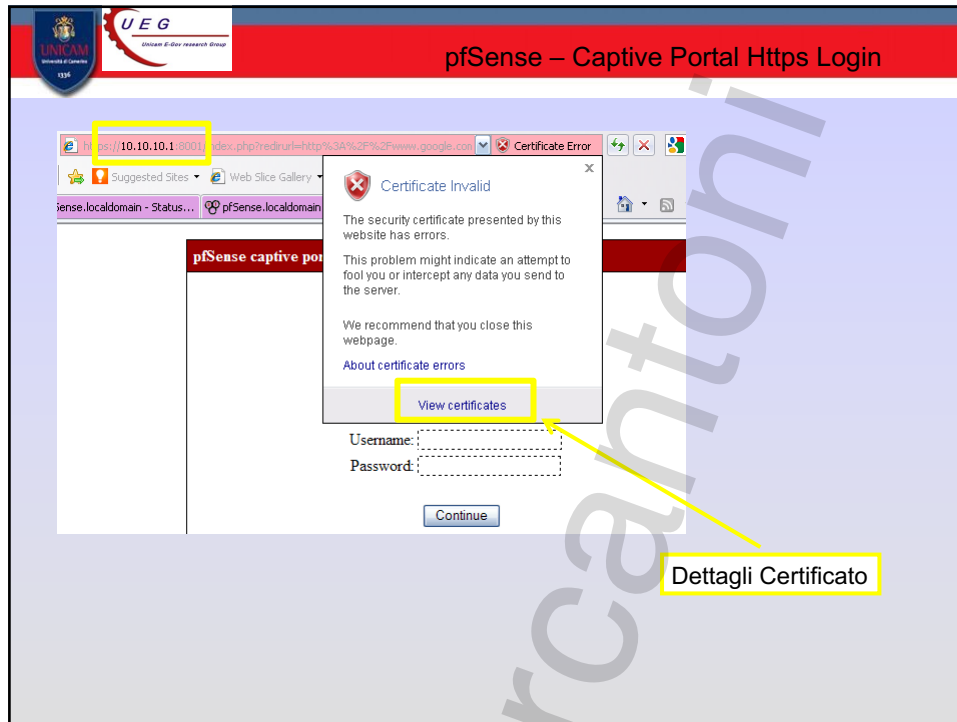
Open Save Cancel

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. [What's the risk?](#)

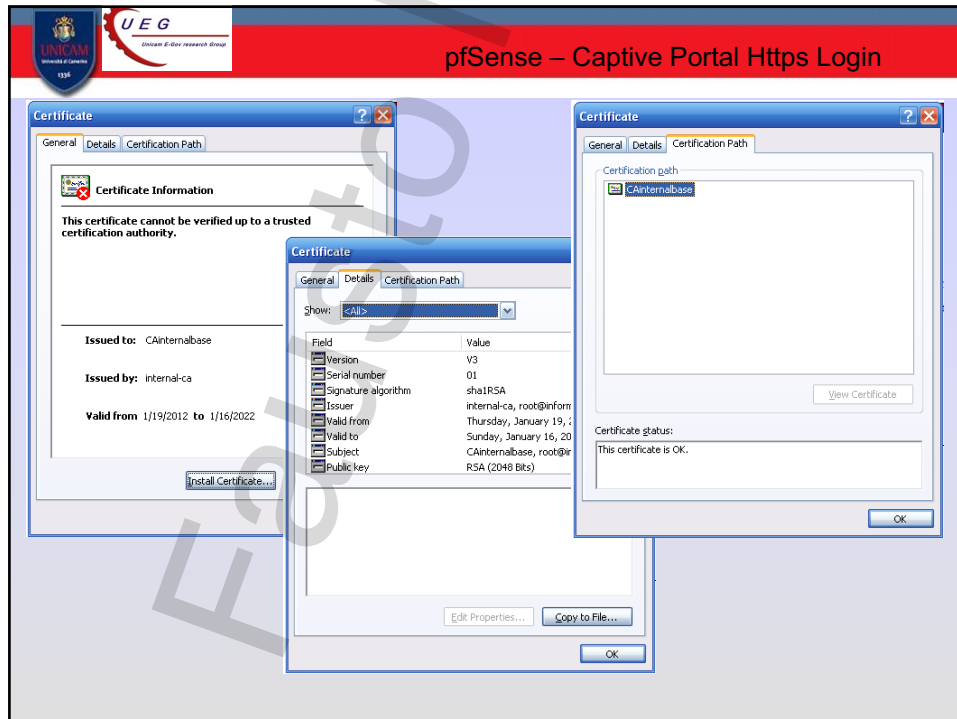
erata,
ca, C=IT
erata,
mediate1, C=US

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

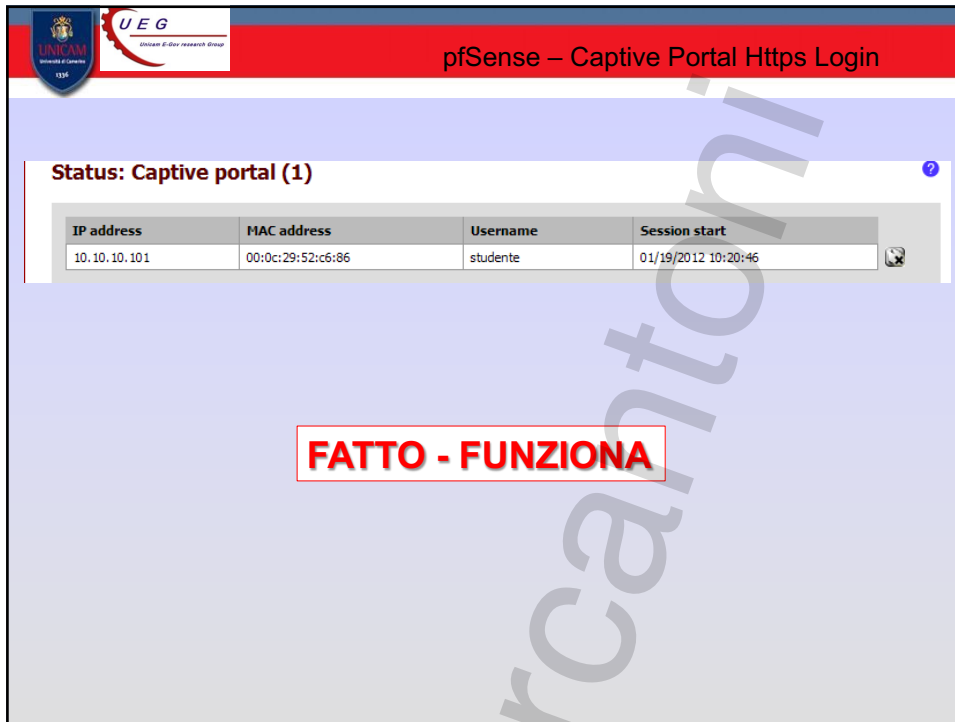
190



191



192



The screenshot shows the pfSense Captive Portal login interface. At the top, there is a header bar with the UNICAM logo on the left and the text "pfSense – Captive Portal Https Login" on the right. Below the header, the status is indicated as "Status: Captive portal (1)". A table displays the session details for the first portal.

IP address	MAC address	Username	Session start
10.10.10.101	00:0c:29:52:c6:86	studente	01/19/2012 10:20:46

Below the table, the text "FATTO - FUNZIONA" is displayed in a red box. A large, diagonal watermark "Fausto Marcantoni" is visible across the entire page.

193