

UNICAM
Università di Camerino
1336

UEG
Unicam E-Gov research Group

pfSense



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

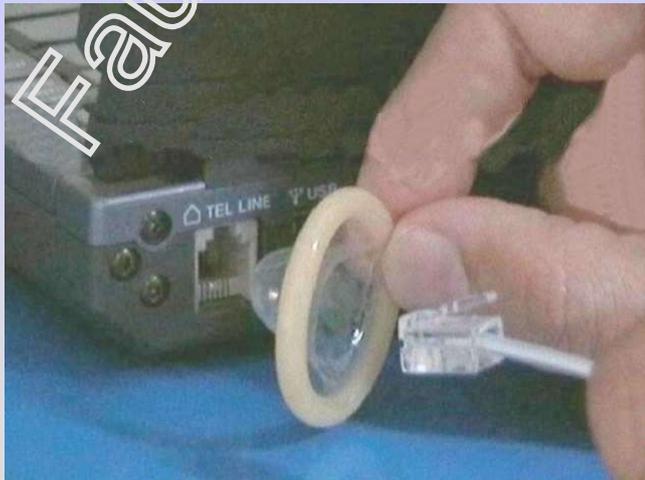
Fausto Marcantoni
fausto.marcantoni@unicam.it

1

UNICAM
Università di Camerino
1336

UEG
Unicam E-Gov research Group

Prevenire è meglio che curare



2

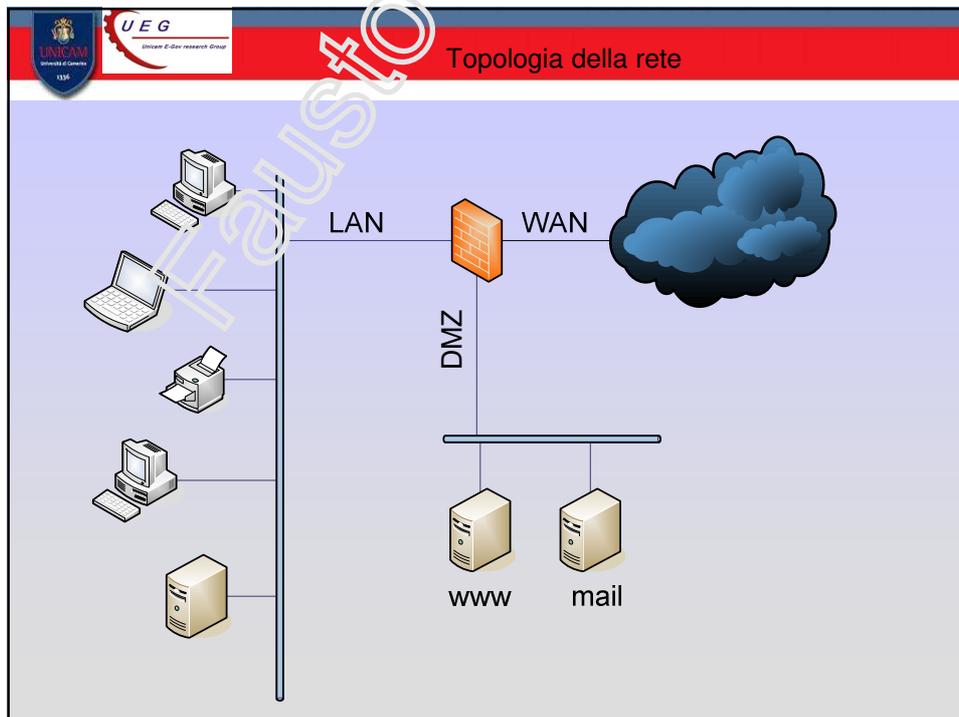



Chi ben comincia ...

- **“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



Slide 5: FIREWALL – pfSense

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

5



Slide 6: pfSense – sito www

<https://pfsense.org/>

Buy Cloud | Buy Appliance | Support | Blog

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

6

UNIVERSITY OF EAST ANGLIA
1316

UEG
University of East Angles research Group

pfSense – hardware

Minimum Hardware Requirements

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

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



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

7

UNIVERSITY OF EAST ANGLIA
1316

UEG
University of East Angles research Group

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...**

8

  pfSense – applicazioni embedded

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



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



<http://www.pceines.ch/wrap.htm>



9

  pfSense – applicazioni embedded

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







10



The screenshot shows the top navigation bar of the pfSense website. On the left, there are logos for UNICAM University of Camerino (founded 1336) and UEG (University of Excellence research Group). The page title is "pfSense – software". The main content area has a light blue background and lists the following components: FreeBSD, OpenBSD's pf, mini_httpd, PHP configuration subsystem, and webGUI. To the right of this list is a small cartoon mascot. Below the list, the word "Packages" is written in bold. At the bottom, a white box contains the URL: <https://docs.netgate.com/pfsense/en/latest/packages/list.html>. A large, faint watermark "Eduardo Marcantoni" is visible across the page.

11



The screenshot shows the "pfSense – software download" page. The navigation bar is identical to the previous slide. The main heading is "Quale file scaricare ???". Below this is a screenshot of the pfSense website's download section. The pfSense logo is at the top left of the screenshot, with "Tour", "Products", and "Services" links to its right. Under the heading "Download", the "Latest Stable Version (Community Edition)" is highlighted. A descriptive paragraph follows: "This is the most recent stable release, and the recommended version for the Upgrade Guide. For pre-configured systems, see the pfSense appliar". At the bottom of the screenshot are two buttons: "RELEASE NOTES" and "SOURCE CODE". A large, faint watermark "Eduardo Marcantoni" is visible across the page.

12

UNICAM University of Camerino 1336 UEG Union E-Gov research Group

pfSense – software download

Quale file scaricare ???

Select Image To Download

Version: 2.7.1

Architecture: AMD64 (64-bit) ?

Installer: DVD Image (ISO) Installer ?

Mirror: Austin, TX USA ?

[Download](#)

Supported by 

SHA256 Checksum for compressed (.gz) file:
2056289d51cf70aaed7c56e887a1033926234b79b7bbc817a91e8311cf2f51bb

13

UNICAM University of Camerino 1336 UEG Union E-Gov research Group

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	✓	2023-06-29	22.9	14.0-CURRENT@0c59e3db4c581	RELENG_2

2.6.x

Version	Support	Released	Config Rev	FreeBSD Version	Branch
2.6.0	✗	2022-02-14	22.2	12.3-STABLE@e1e43d992c6	RELENG_2

2.5.x

Version	Support	Released	Config Rev	FreeBSD Version	Branch
2.5.2	✗	2021-07-07	21.7	12.2-STABLE@f40bcbda6b	RELENG_2
2.5.1	✗	2021-04-13	21.5	12.2-STABLE@f40bcbda6b	RELENG_2
2.5.0	✗	2021-02-17	21.4	12.2-STABLE@f40bcbda6b	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@257046	RELENG_2_4_5
2.4.5	✗	2020-03-26	19.1	11.3-STABLE@257046	RELENG_2_4_5
2.4.4-p3	✗	2019-05-20	19.1	11.2-RELEASE-p10	RELENG_2_4_4
2.4.4-p2	✗	2019-01-07	18.9	11.2-RELEASE-p4	RELENG_2_4_4
2.4.4-p1	✗	2018-12-03	18.9	11.2-RELEASE-p4	RELENG_2_4_4

On This Page

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

14

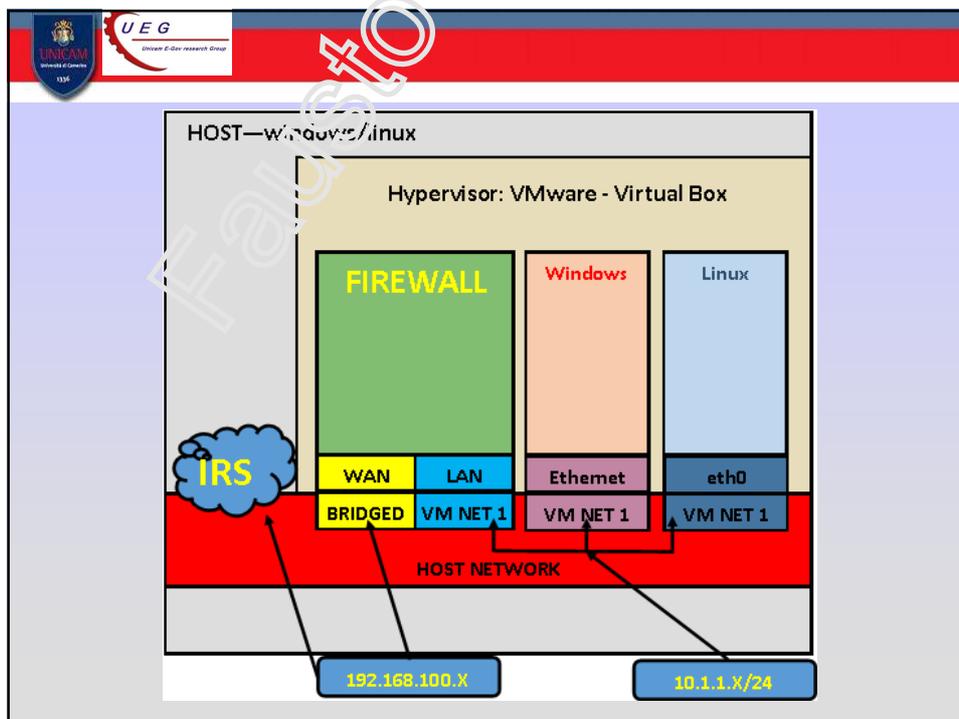
pfSense – installazione

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

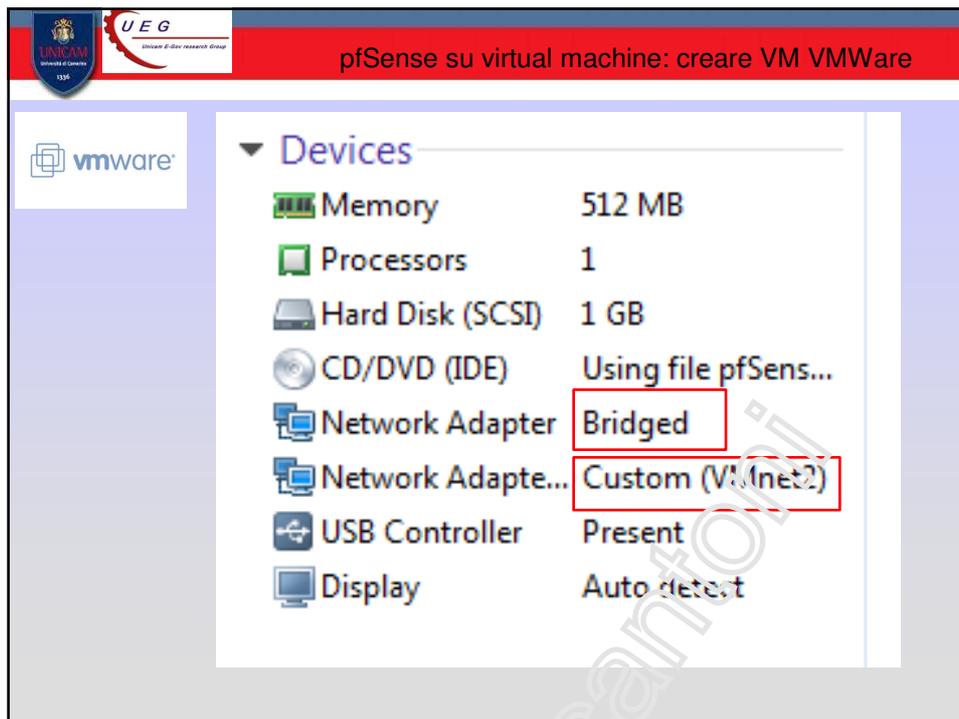
Installation Guides

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

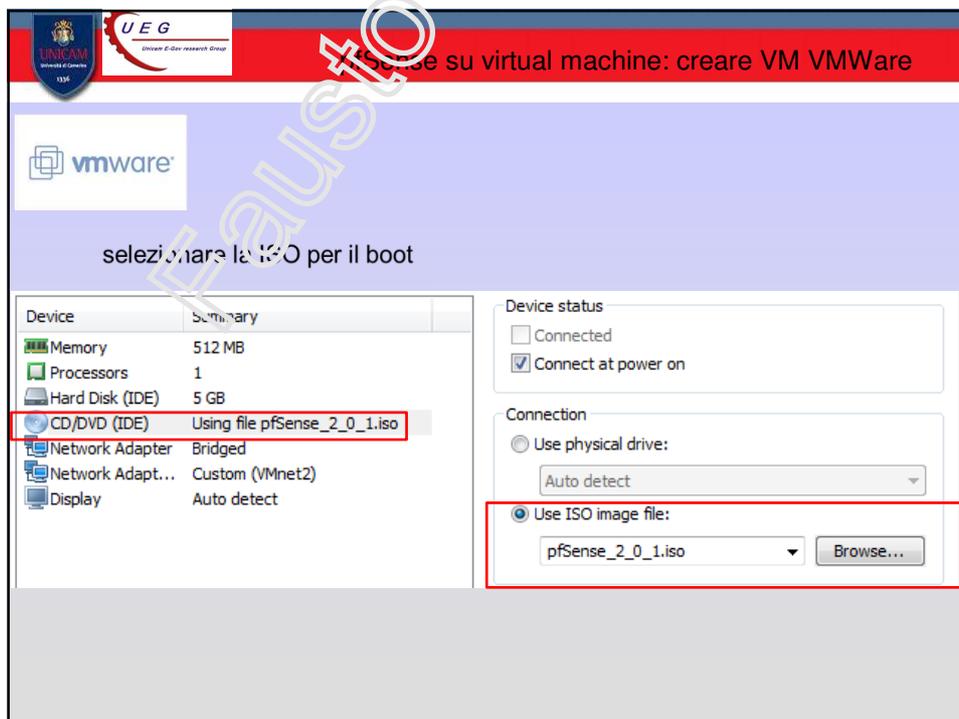
15



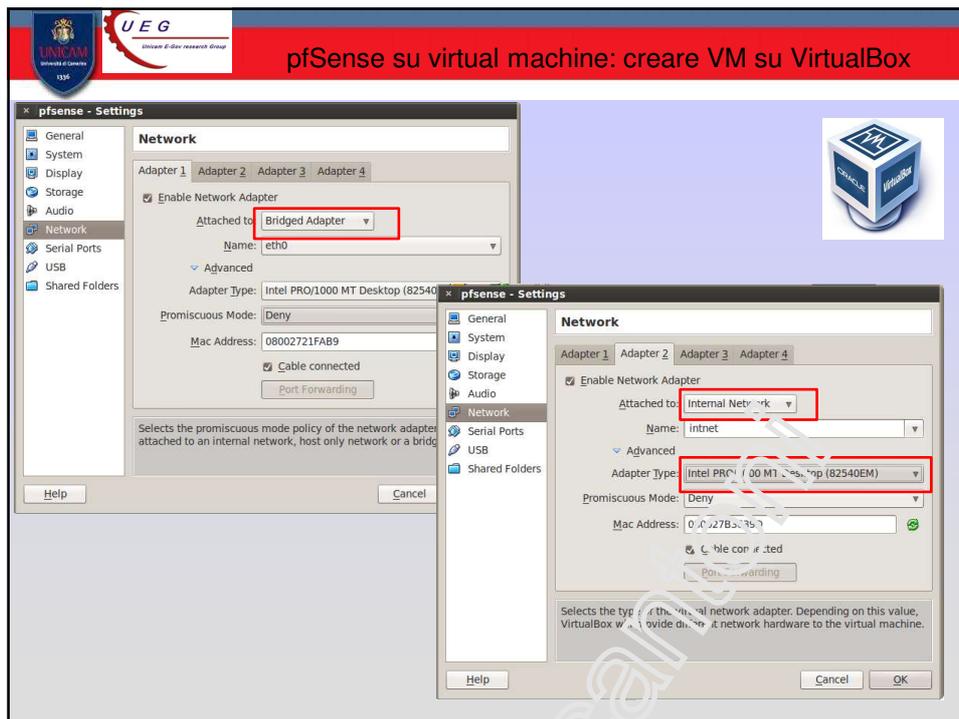
16



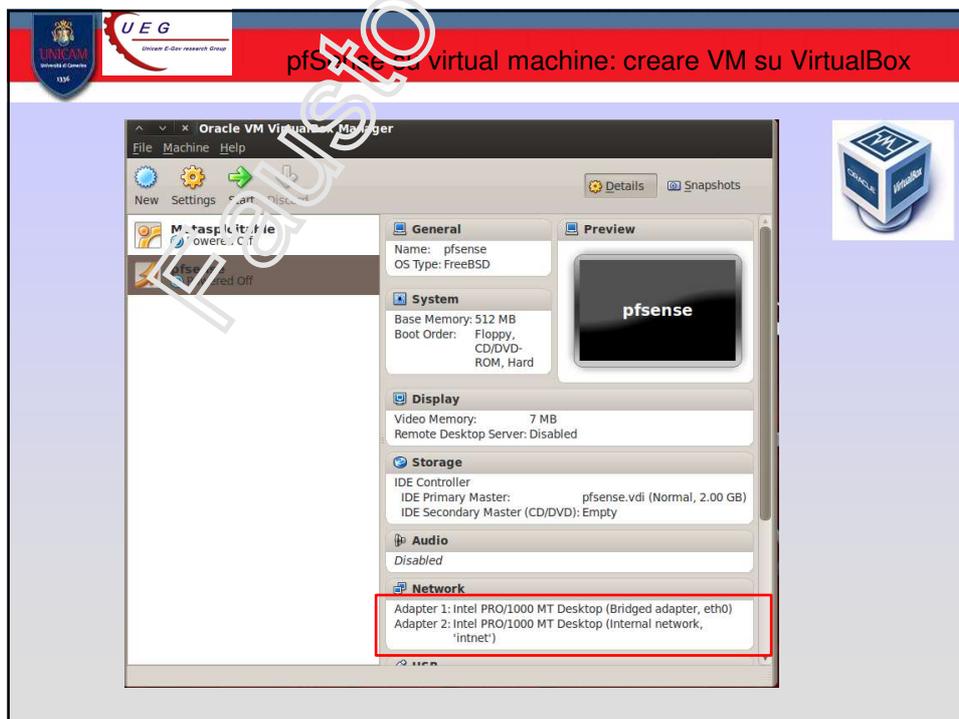
17



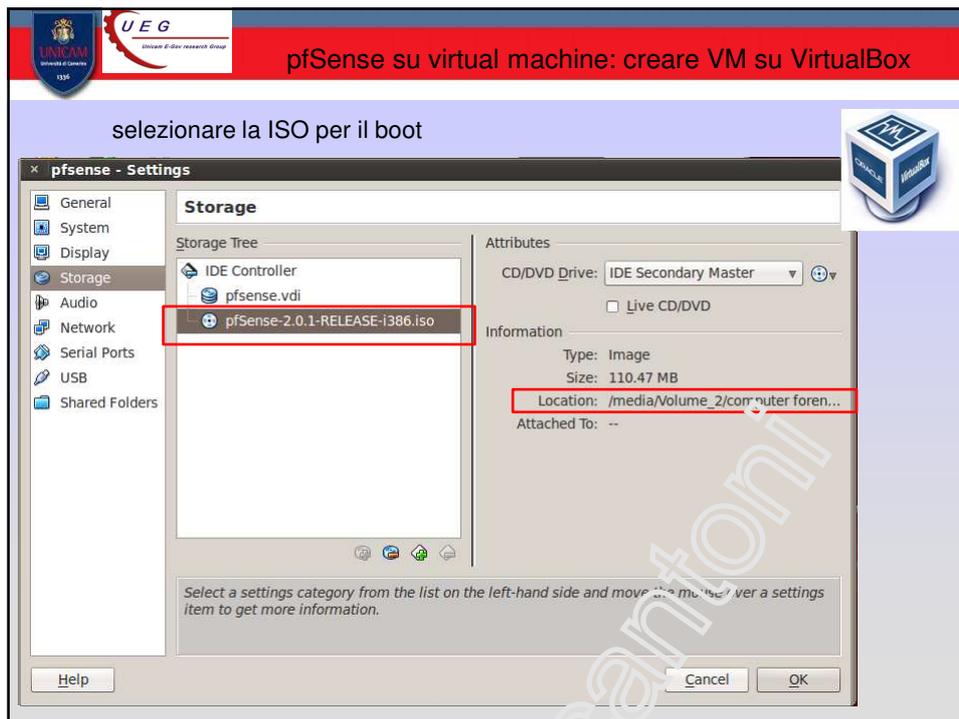
18



19



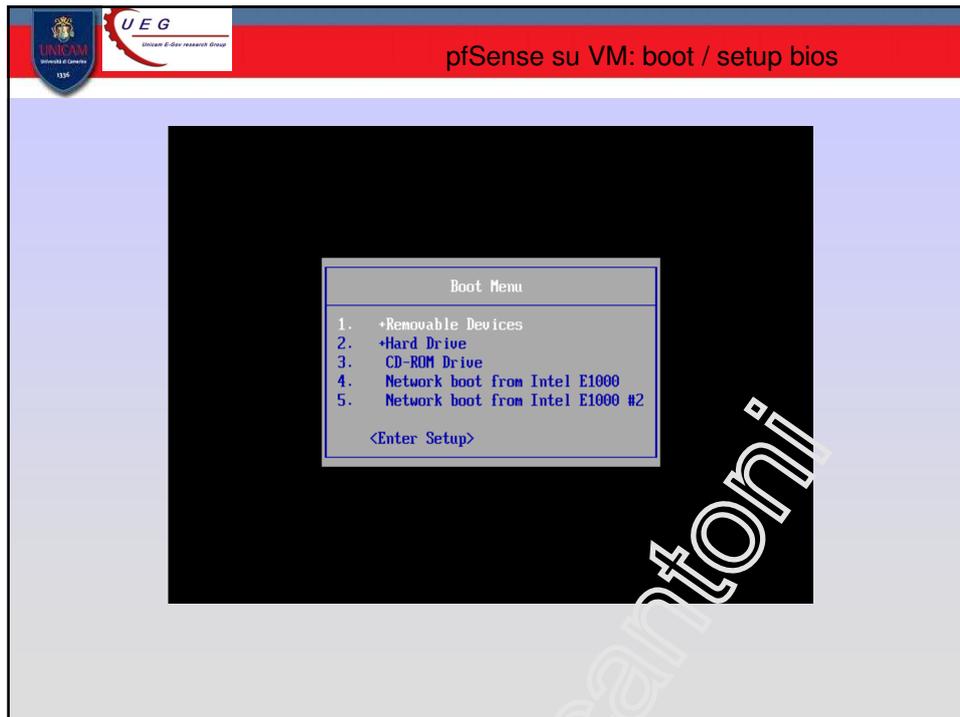
20



21



22



23

The screenshot shows a VM window titled "pfSense su VM: boot". The main text reads: "non riesco ad entrare nel BIOS: è troppo veloce". Below this, a white box contains the following text:

Reason: Cannot press ESC to get into BIOS fast enough

Edit your .vmx file and add the line:

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

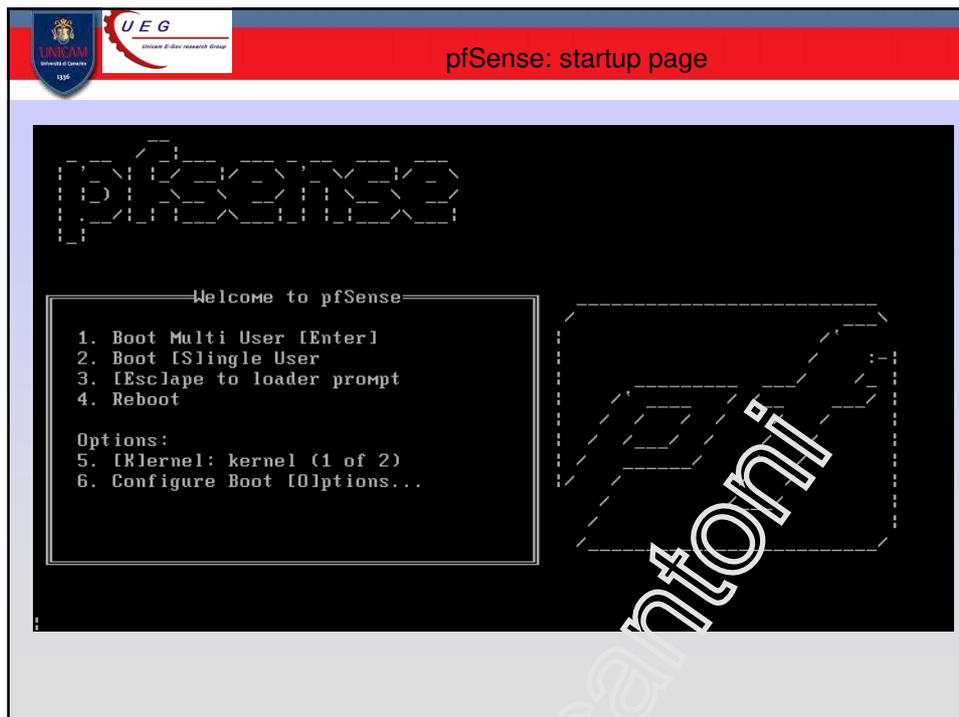
which adds a 5000 millisecond (5 second) delay to the boot, or add:

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

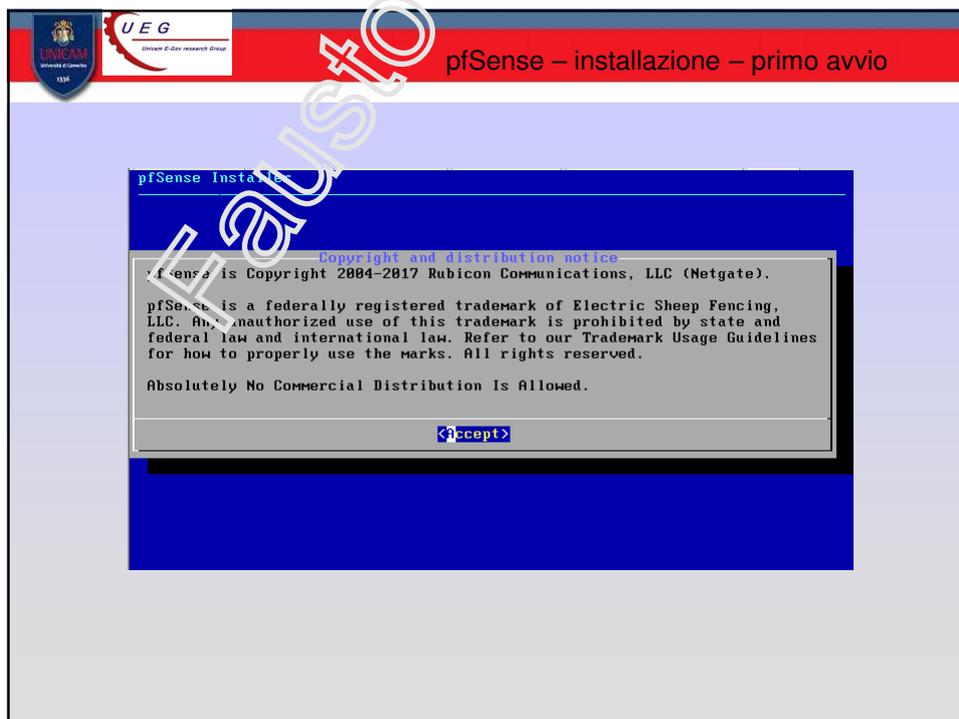
to make the VM enter the BIOS setup at the next boot.

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

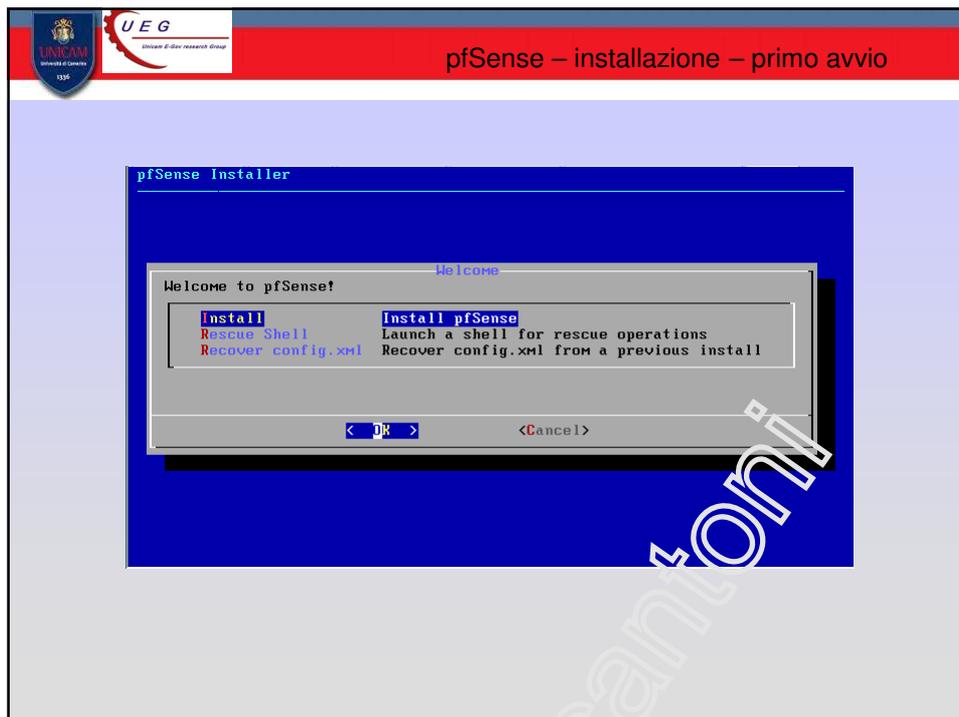
24



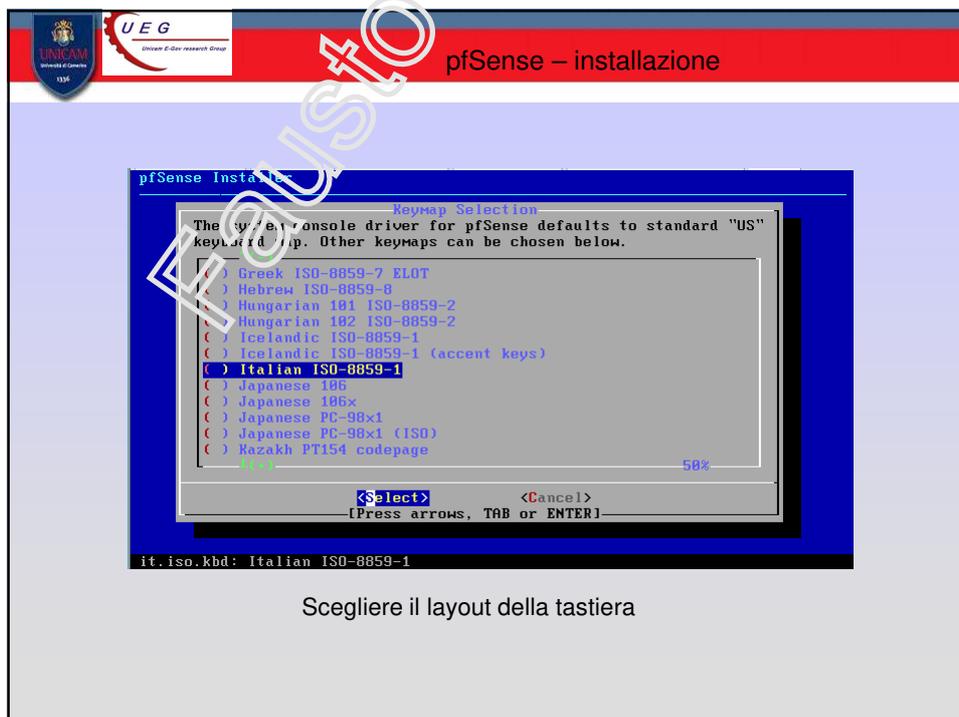
25



26

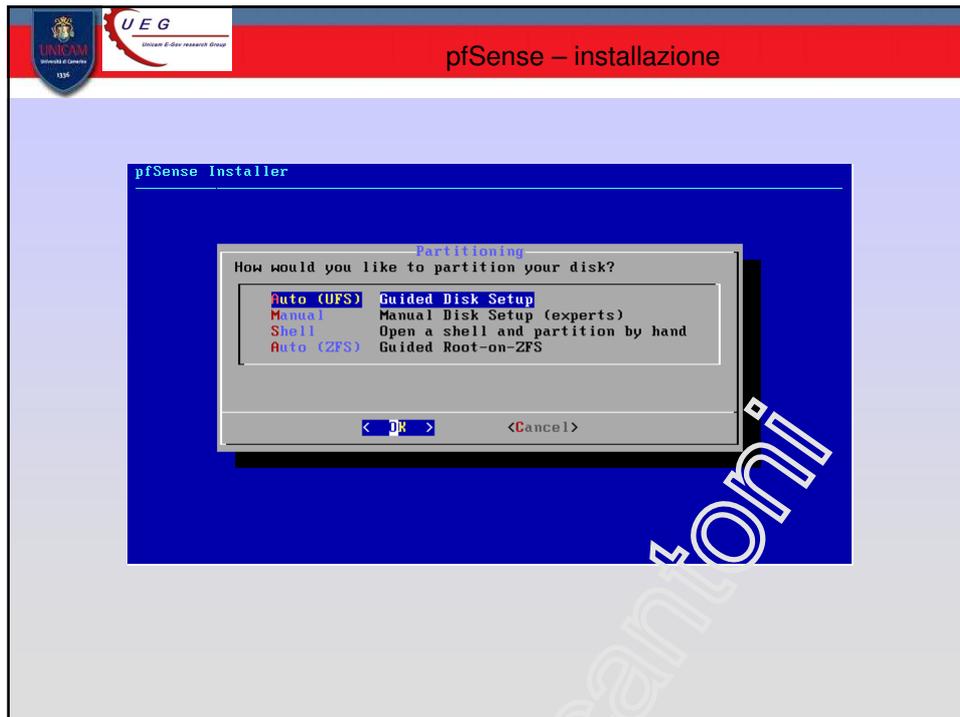


27

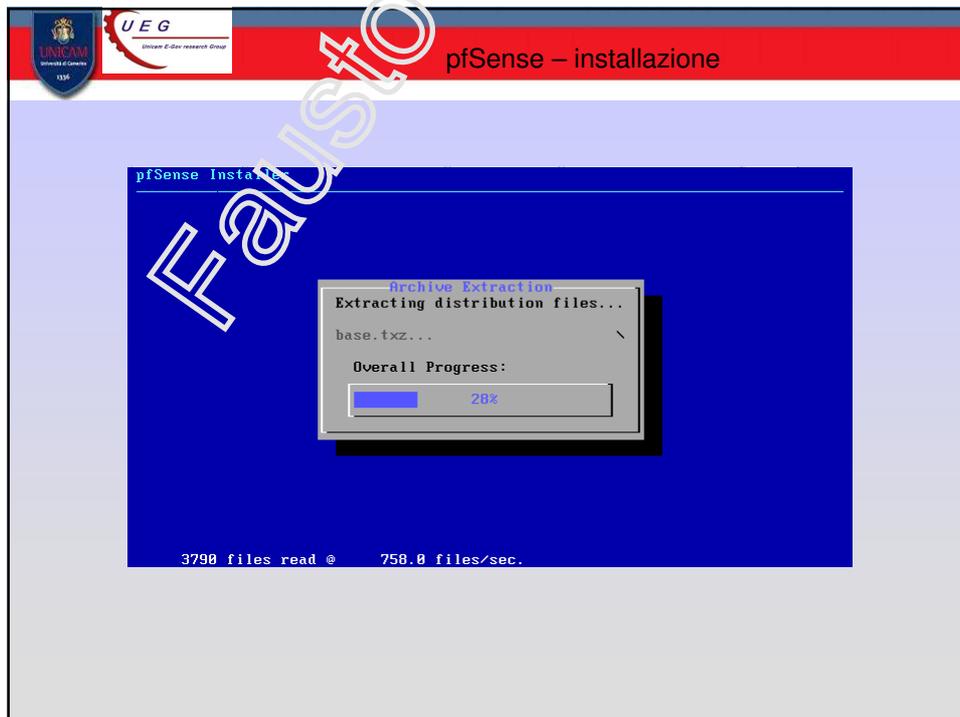


Scegliere il layout della tastiera

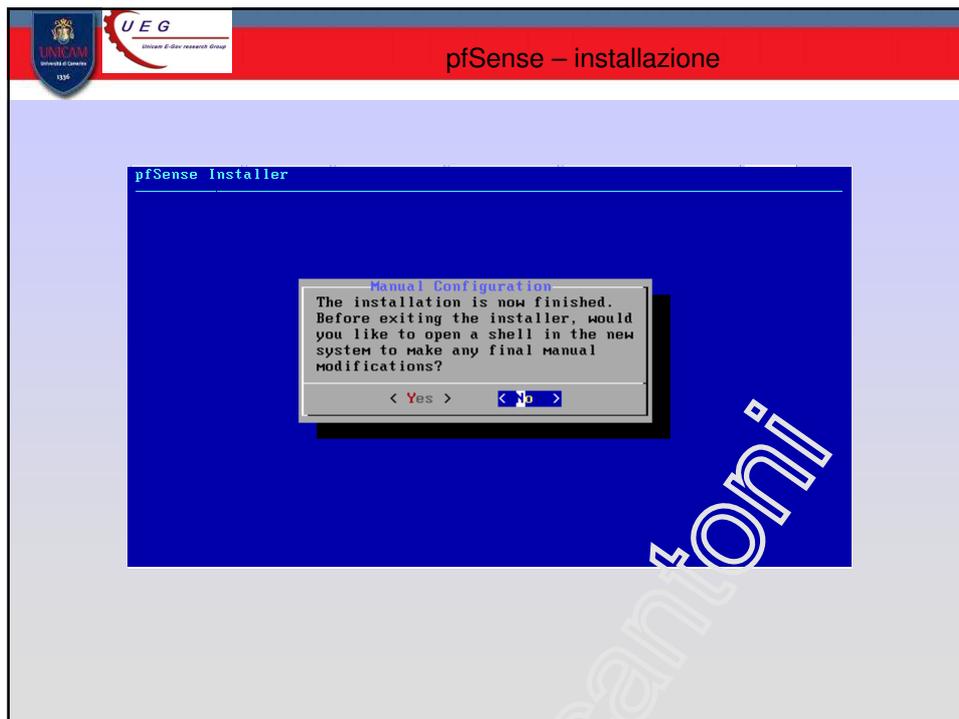
28



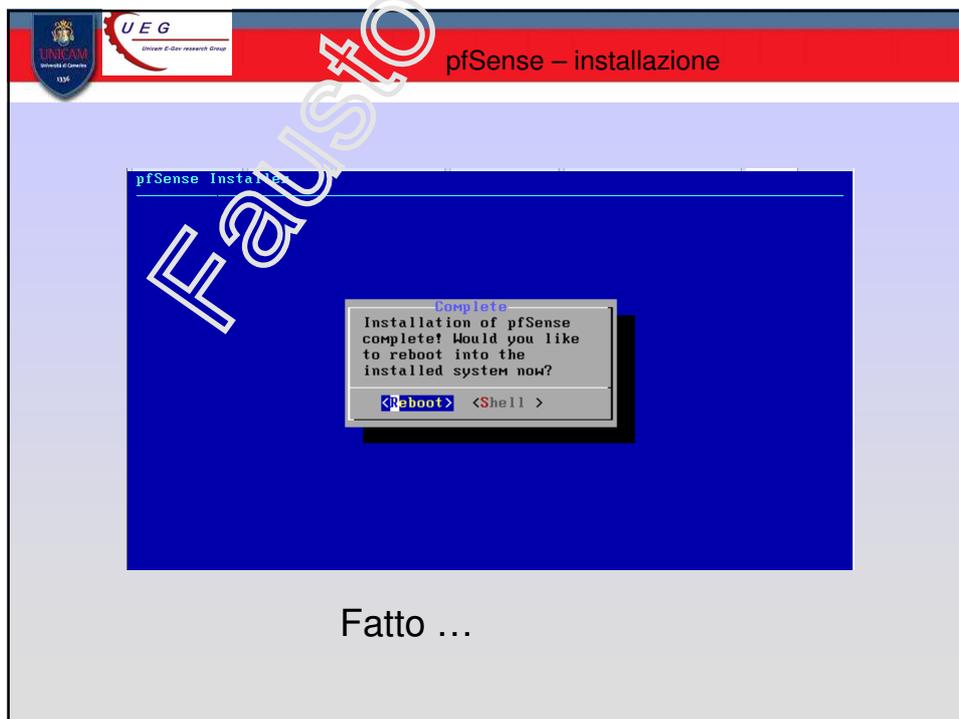
29



30



31



32

UNICAM
Università di Camerino
1336

UEG
Unicon E-Gov research Group

pfSense – installazione

```

The IPv4 LAN address has been set to 10.1.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    https://10.1.1.1/
Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 65fd114079cc108c23c9
*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***
WAN (wan)   -> em0   -> v4/DHCP4: 192.168.100.75/22
LAN (lan)   -> em1   -> v4: 10.1.1.1/24

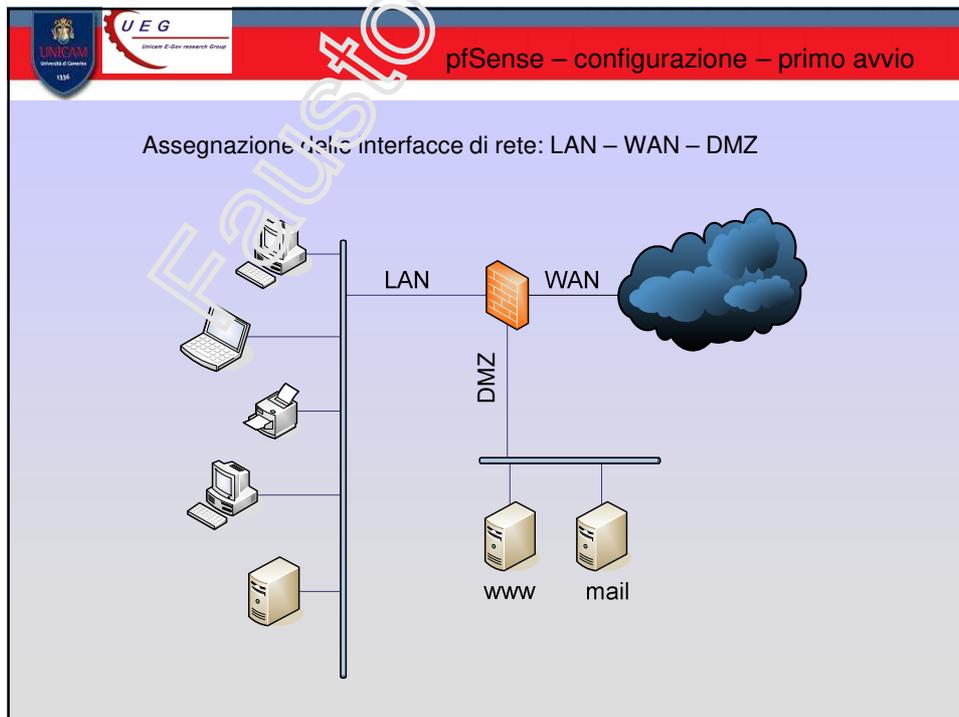
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable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

Enter an option: █

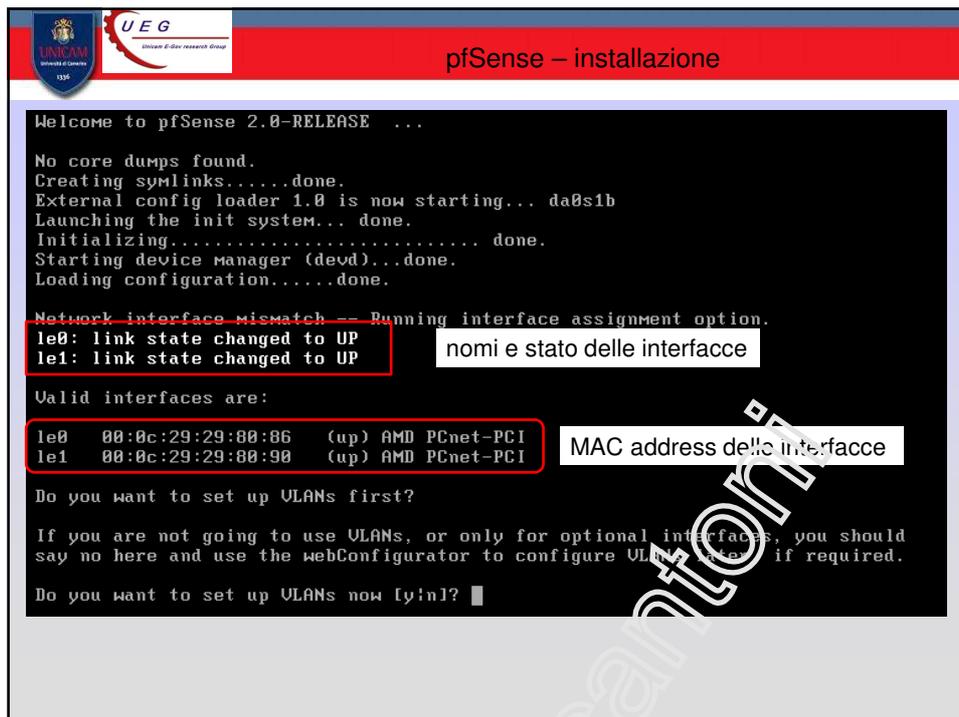
```

... Fatto ...

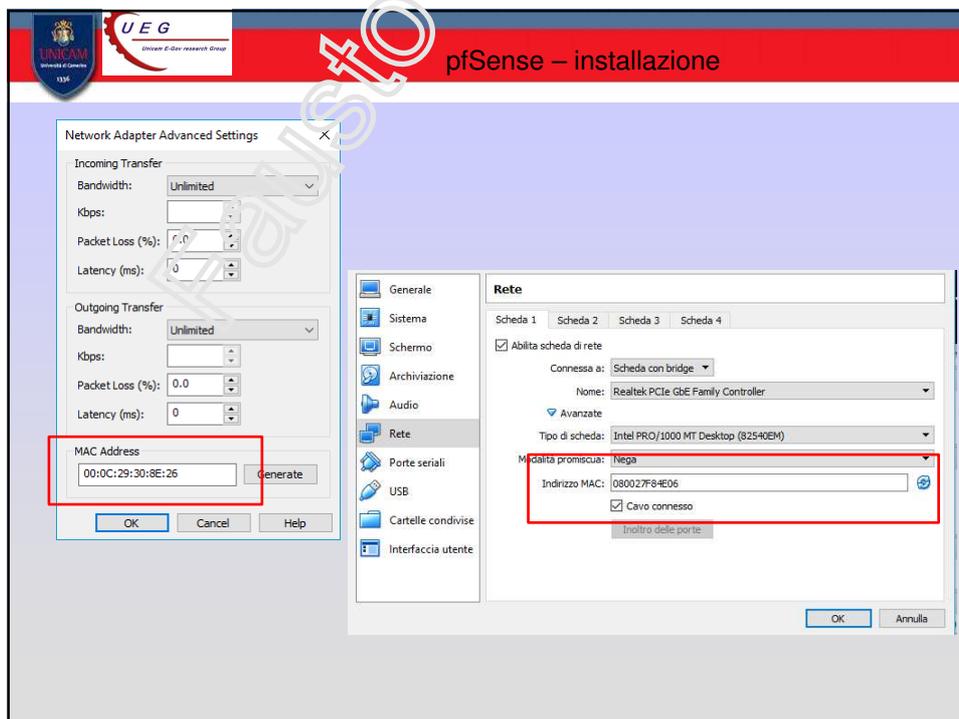
33



34



35



36



pfSense su VM: configurazione ethernet

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

```

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

```

37



pfSense – installazione

```

Welcome to pfSense 2.0.0-RELEASE ...
No core dumps found.
Creating symlinks... done.
External config loader is now starting... da0s1b
Launching the installer... done.
Initializing... done.
Starting device manager (devd)...done.
Loading configuration.....done.

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

Valid interfaces are:

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

Do you want to set up VLANs first?

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

Do you want to set up VLANs now [y;n]?  NO VLANs

```

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

38

UNICAM
Università di Camerino
1336

UEG
Union E-Gov research Group

pfSense – assegnare le interfacce di rete

```

Valid interfaces are:
le0  00:0c:29:29:80:80 (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 and then
hit hitting 'a' to initiate auto detection.

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

```

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

39

UNICAM
Università di Camerino
1336

UEG
Union E-Gov research Group

pfSense – configurare la LAN

```

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

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

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

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

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

Enter an option:

```

40

UNICAM
Università di Camerino
1336

UEG
Unicon-E-Gov research Group

pfSense – configurare la LAN

```

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

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

Enter an option: 2
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.xxx.1

```

41

UNICAM
Università di Camerino
1336

UEG
Unicon-E-Gov research Group

pfSense – configurare la LAN

```

Enter the number of the interface you wish to configure: 2
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.1
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.1.100
Enter the end address of the IPv4 client address range: 192.168.1.200
Disabling IPv6 DHCPD
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

```

42

Avviare il client

Avviare il sistema sul PC client e controllare gli indirizzi IP



The screenshot shows two Windows network configuration windows. The left window, titled 'Stato di Connessione alla rete locale (LAN)', displays the following information:

- Stato connessione: Assegnato da DHCP
- Indirizzo IP: 192.168.1.200
- Subnet Mask: 255.255.255.0
- Gateway predefinito: 192.168.1.1

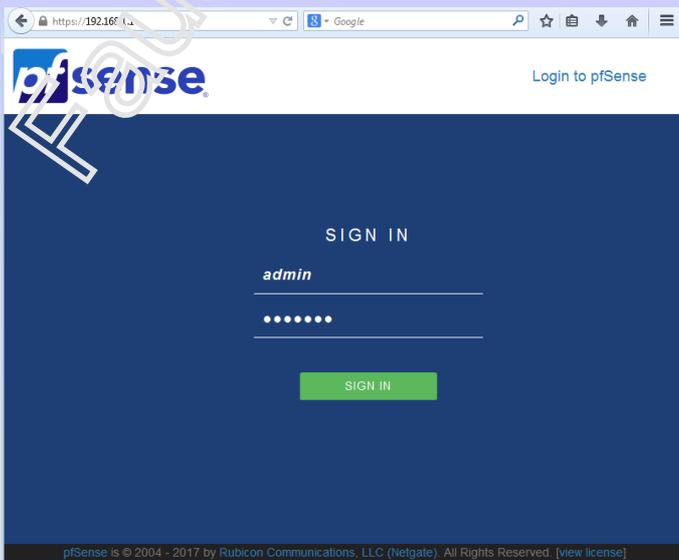
The right window, titled 'Dettagli connessione di rete', displays the following details:

Proprietà	Valore
Indirizzo fisico	00-0C-29-FE-9F-C3
Indirizzo IP	192.168.1.200
Subnet Mask	255.255.255.0
Gateway predefinito	192.168.1.1
Server DHCP	192.168.1.1
Lease ottenuto	03/11/2010 11:40:51
Scadenza lease	03/11/2010 13:40:51
Server DNS	192.168.1.1
Server WINS	

43

pfSense – configurazione - autenticazione

https://192.168.1.1/



The screenshot shows the pfSense login page in a web browser. The browser address bar shows 'https://192.168.1.1/'. The page features the pfSense logo and a 'Login to pfSense' link. Below the logo, there is a 'SIGN IN' section with the following fields:

- Username: *admin*
- Password: A series of six dots representing a masked password.

A green 'SIGN IN' button is located below the password field. At the bottom of the page, the copyright notice reads: 'pfSense is © 2004 - 2017 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license]'.

44

UNICAM
Università di Camerino
1336

UEG
Unicam E-Dev research Group

pfSense – configurazione – Setup Wizard

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

45

UNICAM
Università di Camerino
1336

UEG
Unicam E-Dev research Group

pfSense – configurazione - wizard

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname:
EXAMPLE: myserver

Domain:
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:

Secondary DNS Server:

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

46

UNICAM
Università di Camerino
1336

UEG
Unicam E-Gov research Group

pfSense – configurazione - wizard

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname
Enter the hostname (FQDN) of the time server.

Timezone

Google

ntp1.inrim.it (193.204.114.232)
ntp2.inrim.it (193.204.114.233)

47

UNICAM
Università di Camerino
1336

UEG
Unicam 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.

Select a Type
Static
DHCP
PPPoE
PPTP

Generate 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: xxxxxxxxxxxxxx or leave blank.

MTU
Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should

48

The screenshot shows the 'pfSense – configurazione - wizard' interface. At the top left, there are logos for UNICAM and UEG. The main content area is titled 'RFC1918 Networks' and 'Block bogon networks'. Both sections have a checkbox checked, indicating that these networks will be blocked from entering via WAN. A link to 'https://ipinfo.io/bogon' is provided at the bottom.

RFC1918 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 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>

49

The screenshot shows the 'pfSense – configurazione - wizard' interface at 'Step 5 of 9'. The main content area is titled 'Configure LAN Interface'. It contains a form for configuring the LAN interface, with the 'LAN IP Address' and 'Subnet Mask' fields highlighted by a red box. The 'LAN IP Address' is set to '192.168.1.1' and the 'Subnet Mask' is set to '24'. A 'Next' button is visible at the bottom.

Step 5 of 9

Configure LAN Interface

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

LAN IP Address 192.168.1.1
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask 24

Next

50

UNICAM
University of Camerino
1336

UEG
University E-Gov research Group

pfSense – configurazione - wizard

Step 6 of 9

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password

Admin Password AGAIN

» Next

default password: pfsense

51

UNICAM
University of Camerino
1336

UEG
University E-Gov research Group

pfSense – configurazione - wizard

Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

» Reload

Step 8 of 9

Reload in progress

A reload is now in progress. Please wait.
The wizard will redirect to the next step once the reload is completed.

Step 9 of 9

Wizard completed.

Congratulations! pfSense is now configured.
Remember, we're here to help.
Click [here](#) to learn about Netgate 24/7/365 support.
Click [here](#) to continue on to pfSense webConfigurator.

52

The screenshot displays the pfSense configuration interface. At the top, there are logos for UNICAM and UEG, and a red header bar with the text "pfSense – configurazione – pagina principale". Below this, a navigation menu includes "System", "Interfaces", "Firewall", "Services", "VPN", "Status", "Diagnostics", and "Help". The main content area is titled "Status / Dashboard" and is divided into two columns. The left column, "System Information", contains a table with the following data:

Name	FWfausto.unicam.it
System	VMware Virtual Machine Netgate Device ID: f10f9ed6dbd3bea3133
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Jul 2 2015
Version	2.4.2-RELEASE (amd64) built on Mon Nov 20 08:12:56 CST 2017 FreeBSD 11.1-RELEASE-p4 The system is on the latest version. Version information updated at Thu Nov 23 9:27:36 CET 2017
CPU Type	Intel(R) Core(TM) i7-4700HQ CPU @ 2.40GHz 4 CPUs: 2 package(s) x 2 core(s) AES-NI CPU Crypto: Yes (inactive)
Uptime	00 Hour 27 Minutes 42 Seconds
Current	Thu Nov 23 9:54:43 CET 2017

The right column, "Netgate Services And Support", shows the contract type as "Community Support" and "Community Support Only". Below this, there is a section for "NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES" with a text block and several links: "Register Your Support Subscription", "Upgrade Your Support", "Netgate Global Support", "Netgate Professional Services", "Log into your portal account", "Community Support Resources", "Official pfSense Training by Netgate", and "Visit Netgate.com".

interfaccia GUI tramite browser

53

The screenshot displays the pfSense configuration interface for the "Interfaces" section. At the top, there are logos for UNICAM and UEG, and a red header bar with the text "pfSense – configurazione - Interfaces". The main content area is a light blue box containing the following text:

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

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

54

Troubleshooting

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

Diagnostics / Ping

Ping

Hostname: 8.8.8.8

IP Protocol: IPv4

Source address: LAN

Maximum number of pings: 3

Seconds between pings: 1

[Ping](#)

Results

```

PING 8.8.8.8 (8.8.8.8) from 10.1.1.1: 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=116 time=0.822 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=0.909 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=0.113 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 8.309/9.041/9.113/0.052 ms

```

55

Troubleshooting

Arp table

Diagnostics / ARP Table

Search

Search Term: All [Search](#) [Clear](#)

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

ARP Table

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-d1o6lej	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](#)

56




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.

57




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

58

UNICAM
University of Camerino
1336

UEG
University of Engineering Research Group

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

Primary Address Pool

Subnet 10.1.1.0/24

Subnet Range 10.1.1.1 - 10.1.1.254

Address Pool Range 10.1.1.100 From 10.1.1.0 To

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

59

UNICAM
University of Camerino
1336

UEG
University of Engineering 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 interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

60

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.

IP Address	MAC Address	Hostname	Description	Start	End	Actions
10.1.1.101	00:0c:29:d5:9e:8e	desktop-d106lej		2023/11/24 11:58:20	2023/11/24 13:58:20	<input type="button" value="+"/> <input type="button" value="+"/>
10.1.1.102	00:50:56:c0:00:02	mfausto.		2023/11/24 11:42:50	2023/11/24 13:42:50	<input type="button" value="+"/> <input type="button" value="+"/>

Interface	Pool Start	Pool End	Used	Capacity	Utilization
LAN	10.1.1.100	10.1.1.200	2	101	100% / 101

61

Troubleshooting

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

Prompt dei comandi

```
C:\Documents and Settings\Administrator>ping 193.205.92.133
Esecuzione di ping su 193.205.92.133 con 32 byte di dati:
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>
```



62

UEG
University of East Angles research Group

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/

il mio IP
http://ilmioip.it

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

63

UEG
University of East Angles research Group

Tutto funziona – wow si naviga

Google

Location Edit View Go Bookmarks Tools Settings Window Help

Location: http://www.google.it/

CD-Inhaltsverzeichnis KNOPPIX - Webseite

Home page personalizzata | Accesso

Google
Italia

Web Immagini Gruppi Directory News altro

Cerca con Google Mi sento fortunato Ricerca avanzata
Preferenze Strumenti per le lingue

Cerca: il Web pagine in italiano pagine provenienti da: Italia

Pubblicità - Soluzioni Aziendali - Tutto su Google - Google.com in English
©2006 Google

64

UNICAM
Università di Cambrino
1336

UEG
Unicon E-Gov research Group

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).

65

UNICAM
Università di Cambrino
1336

UEG
Unicon E-Gov research Group

pfSense – Status - LOG

Status / System Logs / System / General

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 0xf59f000-0xf59ffff 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

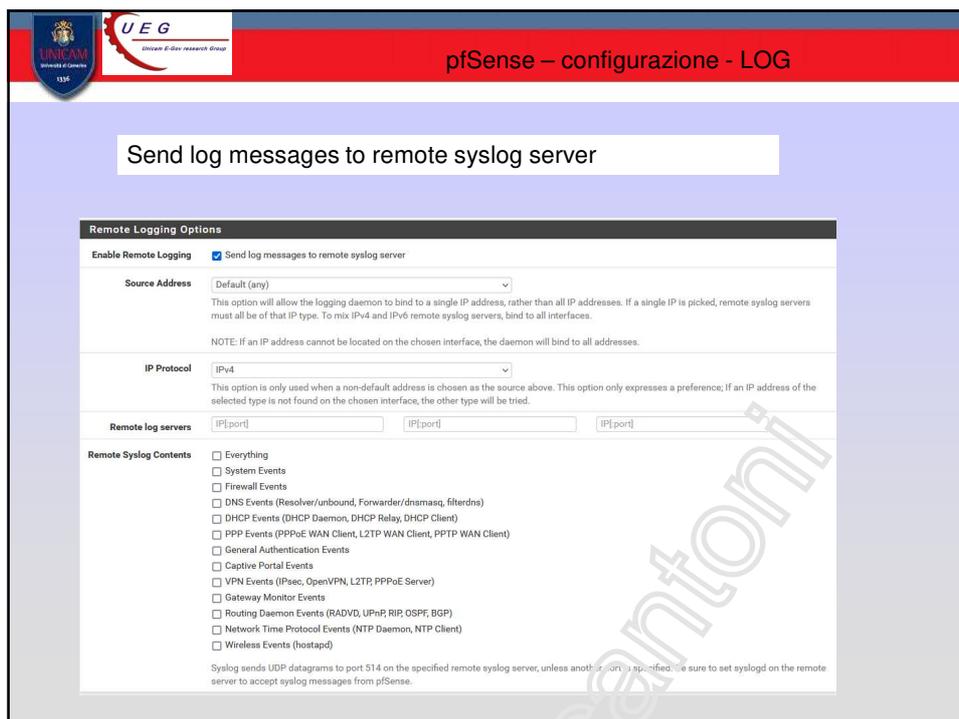
Log Message Format: BSD (RFC 3164, default)

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

GUI Log Entries: 500

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

66



The screenshot shows the 'Remote Logging Options' configuration page in pfSense. The page title is 'Send log messages to remote syslog server'. The 'Enable Remote Logging' section is checked, with the option 'Send log messages to remote syslog server'. The 'Source Address' is set to 'Default (any)'. The 'IP Protocol' is set to 'IPv4'. The 'Remote log servers' field contains three entries, each with a placeholder 'IP[port]'. The 'Remote Syslog Contents' section has several checkboxes, all of which are unchecked. A note at the bottom states: '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.'

67



pfSense – configurazione - Captive portal

La tecnica del **CAPTIVE PORTAL** forza un client del servizio HTTP su una pagina 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 Wired (per esempio gli edifici in condominio, i centri di affari, PMI, P.A.).

68

UNICAM
Università di Camerino
1336

UEG
Unicon E-User research Group

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).

69

Captive Portal Login Page

UNICAM
Università di Camerino
1336

UEG
Unicon E-User research Group

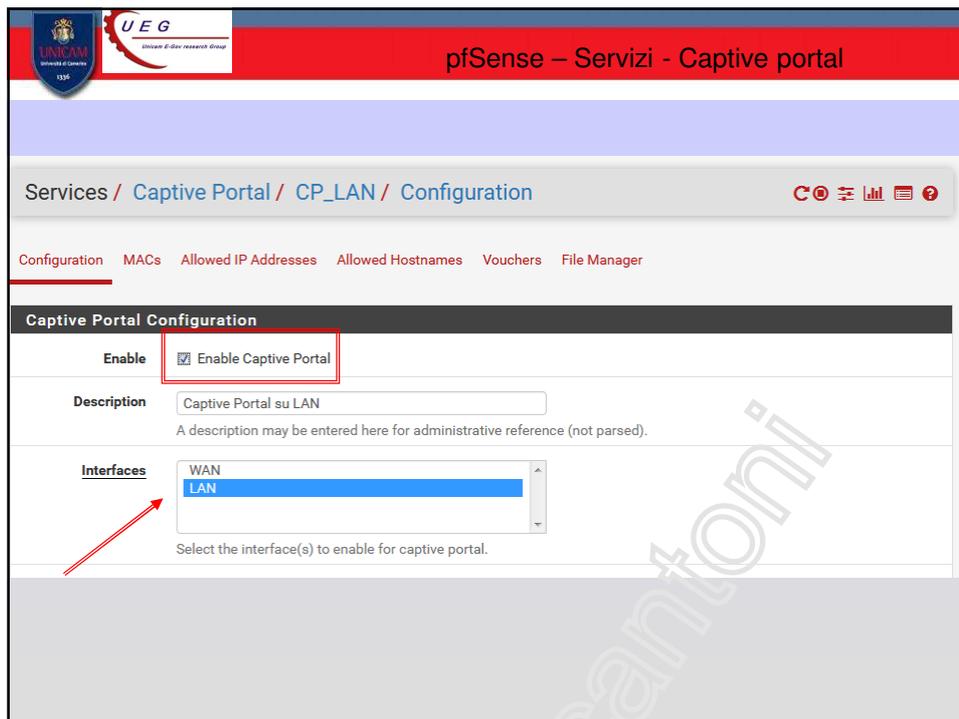
UNICAM
UNIVERSITÀ
di CAMERINO

User

Password

Made with ♥ by Fausto

70



The screenshot shows the pfSense web interface for configuring a Captive Portal. The breadcrumb trail is Services / Captive Portal / CP_LAN / Configuration. The main heading is "Captive Portal Configuration".

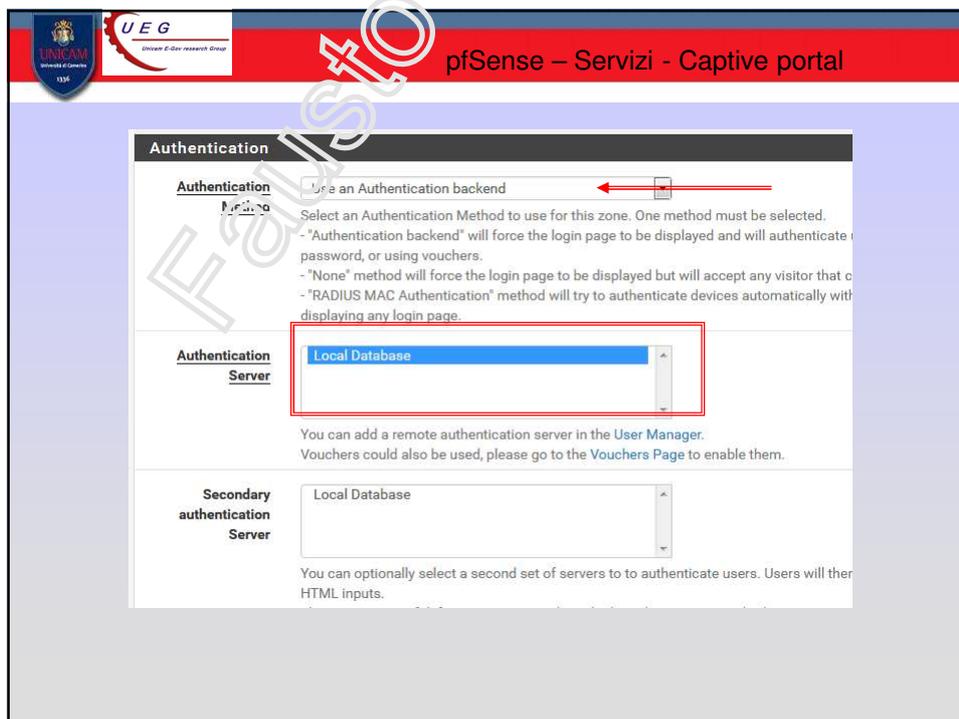
Enable: The checkbox "Enable Captive Portal" is checked and highlighted with a red box.

Description: The text "Captive Portal su LAN" is entered in the description field.

Interfaces: A dropdown menu is open, showing "WAN" and "LAN". The "LAN" option is selected and highlighted in blue. A red arrow points to the "LAN" option. Below the dropdown, it says "Select the interface(s) to enable for captive portal."

Navigation tabs include Configuration, MACs, Allowed IP Addresses, Allowed Hostnames, Vouchers, and File Manager.

71



The screenshot shows the "Authentication" configuration page in pfSense. The breadcrumb trail is Services / Captive Portal / CP_LAN / Configuration / Authentication.

Authentication Method: A dropdown menu is set to "Use an Authentication backend". A red arrow points to this dropdown.

Authentication Server: A dropdown menu is set to "Local Database" and is highlighted with a red box.

Secondary authentication Server: A dropdown menu is also set to "Local Database".

Instructions for the Authentication Method dropdown:

- "Authentication backend" will force the login page to be displayed and will authenticate users using a password, or using vouchers.
- "None" method will force the login page to be displayed but will accept any visitor that can connect.
- "RADIUS MAC Authentication" method will try to authenticate devices automatically without displaying any login page.

Instructions for the Authentication Server dropdown:

You can add a remote authentication server in the User Manager. Vouchers could also be used, please go to the Vouchers Page to enable them.

Instructions for the Secondary authentication Server dropdown:

You can optionally select a second set of servers to to authenticate users. Users will then be able to authenticate using either set of servers.

72

already been exhausted.

Logout popup window Enable logout popup window
If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.

Re-authentication

Logout - Internet Explorer
about:blank
Click the button below to disconnect
Logout

abilitare i pop-up sul browser

73

System / User Manager / Users

Users Groups Settings Authentication Servers

Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	

+ Add Delete

aggiungere un utente

74

The screenshot shows the pfSense User Manager configuration page for a user named 'fausto'. The interface includes a navigation menu at the top with options like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled 'System: User Manager' and has tabs for Users, Groups, Settings, and Servers. The 'Users' tab is active, showing the configuration for the user 'fausto'. The 'Username' field is set to 'fausto', and the 'Password' field is masked with dots. The 'Expiration date' field is empty. A calendar widget is open over the 'Expiration date' field, showing the month of June 2012. The 'Full name' field is set to 'Fausto Marcantoni'. The 'Group Memberships' section shows two empty lists: 'Not Member Of' and 'Member Of'. A watermark 'Fausto Marcantoni' is visible across the page.

75

The screenshot shows the 'Effective Privileges' page for the user 'fausto'. The page title is 'Abilitare l'utente ad utilizzare il Captive Portal'. Below the title is a table with the following data:

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

At the bottom right of the table is a green '+ Add' button. Below the table, there is a text box containing the text: 'User - Services: Captive Portal login. Indicates whether the user is able to login on the captive portal.' A watermark 'Fausto Marcantoni' is visible across the page.

76

UNICAM
Università di Camerino
1336

UEG
Union E-Gov research Group

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

77

UNICAM
Università di Camerino
1336

UEG
Union E-Gov 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="redirect" 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="redirect" type="hidden" value="$PORTAL_REDIRECTURL$">
<input name="zone" type="hidden" value="$PORTAL_ZONES$">
<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.

78




pfSense – configurazione - Captive portal

Esempio di pagina “ CAPRTIVE PORTAL”

```

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

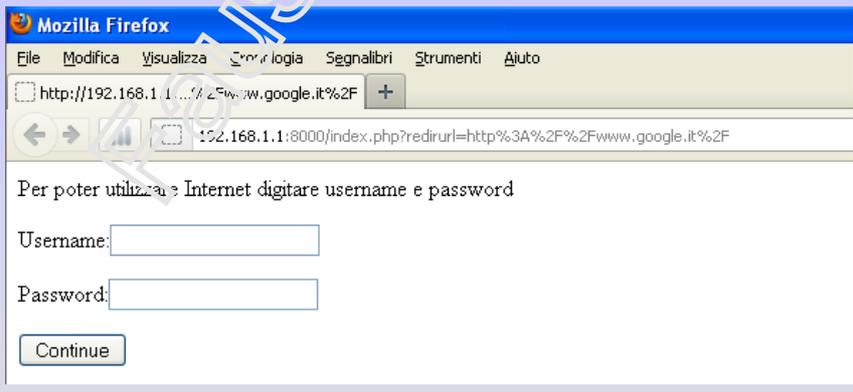
```

E' possibile aggiungere anche le immagini

79




pfSense – configurazione - Captive portal



80

40

UNICAM
Università di Camerino
1336

UEG
Unicon E-Gov research Group

pfSense – configurazione - Captive portal

È necessario accedere alla rete per navigare in Internet.

UNIVERSITÀ DI CAMERINO

User

Password

Login

Made with by Netgate

Nota: 11. Accesso a Internet

81

UNICAM
Università di Camerino
1336

UEG
Unicon 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 timer (Minutes) **fine tuning**
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.

82

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.

83

pfSense – configurazione - Captive portal

I log di captive portal

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / Captive Portal / CP_LAN

Users Logged In (1)

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	

Show Last Activity Disconnect All Users

84

System Logs Authentication Captive Portal Auth

System Logs → Authentication → Captive Portal Auth

Status / System Logs / Authentication / Captive Portal Auth

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

General Captive Portal Auth PPPoE Logins L2TP Logins OS User Events OS Account Changes

Last 6 Captive Portal Auth Log Entries. (Maximum 500)

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

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

85

pfSense – backup configurazione -

Backup della configurazione

Backup Configuration

Backup area: All

Skip package information: Do not backup package information.

Skip RRD data: Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)

Encryption: Encrypt this configuration file.

[Download configuration as XML](#)

Restore Backup

Open a pfSense configuration XML file and click the button below to restore the configuration.

Restore area: All

Configuration file: Nessun file selezionato.

Encryption: Configuration file is encrypted.

[Restore Configuration](#)

The firewall will reboot after restoring the configuration.

86

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

pfSense – backup configurazione -

Backup della configurazione

Apertura di config-pfSense.localdomain-20120619142011....

È stato scelto di aprire

config-pfSense.localdomain-20120619142011.xml
 che è un: XML Document (15,0 kB)
 da: https://192.168.1.1

Che cosa deve fare Firefox con questo file?

Apriilo con Internet Explorer (predefinita)

Salva file

Da ora in avanti esegui questa azione per tutti i file di questo tipo.

OK Annulla

Download

Nome	Dimensione	Data
config-pfSense.localdomain-20120619142011.xml	15,0 kB — 192.168.1.1	16:20
MicrosoftFixit50528.msi	658 kB — microsoft.com	giovedì
avast_free_antivirus_setup.exe	71,3 MB — softonic.it	mercoledì
benvenuto.gif	7,4 kB — ic-cerretodesi.it	9 giugno
wireshark-win32-1.4.1.exe	18,3 MB — unicom.it	8 giugno

Cancella elenco Cerca...

87

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

pfSense – backup configurazione -

formato XML

```
<?xml version="1.0" ?>
<pfsense>
  <version>8.0</version>
  <lastchange />
  <theme>pfsense_ng</theme>
  <sysctl>
    <item>
      <descr>
        <![CDATA[ Disable the pf ftp proxy handler. ]]>
      </descr>
      <tunable>debug.pfftp proxy</tunable>
      <value>default</value>
    </item>
    <item>
      <descr>
        <![CDATA[ Increase UFS read-ahead speeds to match current state of hard drives and NCQ. More information here: http://svoras.sharanet.org/blog/tree/2010-11-19.ufs-read-ahead.html ]]>
      </descr>
      <tunable>vfs.read_max</tunable>
      <value>default</value>
    </item>
    <item>
      <descr>
        <![CDATA[ Set the ephemeral port range to be lower. ]]>
      </descr>
      <tunable>net.inet.ip.portrange.first</tunable>
      <value>default</value>
    </item>
  </sysctl>
</pfsense>
```

88

UNICAM University of Camerino 1336 UEG Union E-Gov research Group

pfSense – configurazione – DHCP Server

configurare alcuni parametri nel server dhcp

Services: DHCP server

LAN

Enable DHCP server on LAN interface

Deny unknown clients
If this is checked, only the clients defined below will get DHCP leases from this interface.

Subnet: 192.168.1.0

Subnet mask: 255.255.255.0

Available range: 192.168.1.1 - 192.168.1.254

Range: 192.168.1.100 to 192.168.1.200

WINS servers:

DNS servers:

8.8.8.8
8.8.4.4

DNS di Google

NOTE: leave blank to use the system default DNS servers - this interface's IP address or the servers configured on the General page.

89

UNICAM University of Camerino 1336 UEG Union E-Gov research Group

pfSense – configurazione – DHCP Server

configurare alcuni parametri nel server dhcp

Domain name: **domain name personale**

NTP servers: **NTP server**

Full DNS lookup away for your network.

Full domain name: If a left field is to use the domain name of this system, an alternate domain name here.

90

UNICAM
Università di Camerino
1336

UEG
Union E-Gov 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 (c) Microsoft Corp. 1985-2001

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 . . . . . : No
Configurazione automatica abilitata . . . . : No
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

```

91

UNICAM
Università di Camerino
1336

UEG
Union E-Gov research Group

pfSense – configurazione - Creazione regole

Le "REGOLE"

pfSense
COMMUNITY EDITION

System ▾ Inet ▾ 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

92

UNICAM
Università di Camerino
1336

UEG
Unicam E-Gov research Group

pfSense – configurazione - Creazione regole

Firewall / Rules / LAN

Floating WAN LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	1/1.33 MiB	*	*	*	LAN Address	443	*	*	*	Anti-Lockout Rule	
<input type="checkbox"/>	24/207.83 MiB	IPv4*	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6*	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

↑ Add ↓ Add Delete Refresh Copy Save + Separator

TUTTO APERTO

93

UNICAM
Università di Camerino
1336

UEG
Unicam 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
Select 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: (other) From Custom To 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 ...

94

UNICAM
Università di Camerino
1336

UEG
Unicon E-Gov research Group

pfSense – configurazione - Creazione regole

... Configurare una regola ...



Attenzione

**Ricorda:
Un firewall si progetta**

Protocol: TCP

Source: TCP/UDP

Source: any

Destination: any

Destination port range: from: other

not
Use this option to invert the selection.

Type: any

Address: any

Single host or alias

Network

PPPoE clients

PPPoE clients

WLAN subnet

WLAN address

LAN subnet

LAN address

97

UNICAM
Università di Camerino
1336

UEG
Unicon E-Gov research Group

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

98

UNICAM
Università di Camerino
1336

UEG
Unicon E-Gov research Group

pfSense – configurazione - Creazione regole

**Ricorda:
Un firewall si progetta**



CHIUDIAMO TUTTO ...

99

UNICAM
Università di Camerino
1336

UEG
Unicon E-Gov research Group

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)

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

100

UNICAM
Università di Camerino
1336

UEG
Unicon E-Gov research Group

pfSense – configurazione - Creazione regole



**CHIUDIAMO TUTTO ...
POI APRIAMO QUELLO CHE SERVE**

101

UNICAM
Università di Camerino
1336

UEG
Unicon E-Gov research Group

pfSense – configurazione - Creazione regole

Quali porte aprire???



**CHIUDIAMO TUTTO ...
POI APRIAMO QUELLO CHE SERVE**

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

102

UNICAM University of Camerino 1336 UEG Union E-Gov 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
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 HTTP	🔗 🗑️
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 ⏩ Delete Save + Separator

103

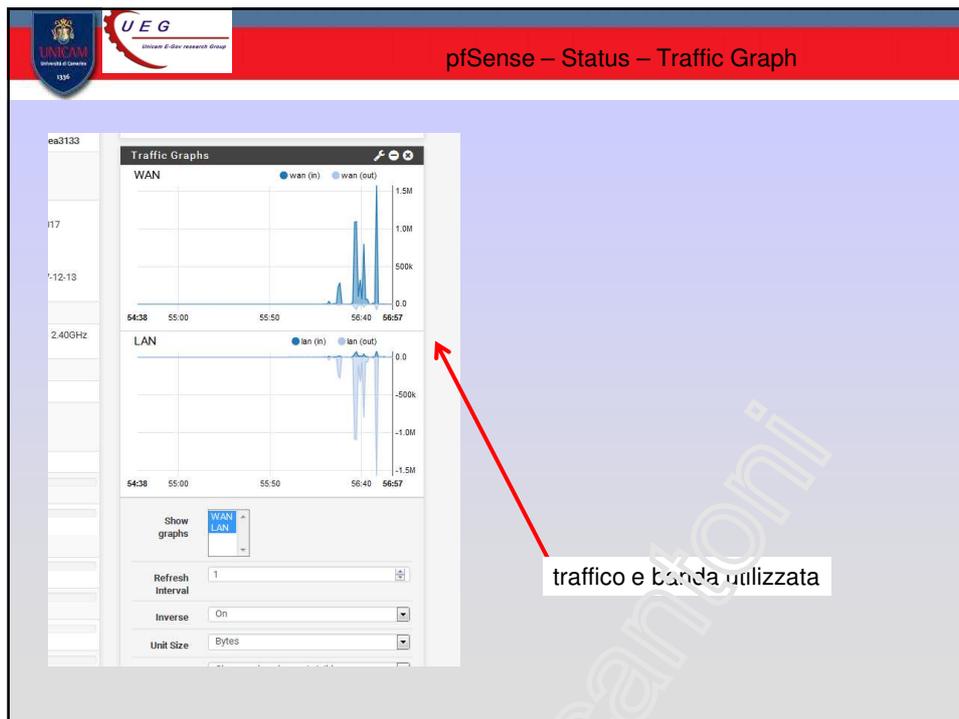
UNICAM University of Camerino 1336 UEG Union E-Gov research Group

pfSense – configurazione – Firewall States

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

Controllare le sessioni e lo stato del firewall

104



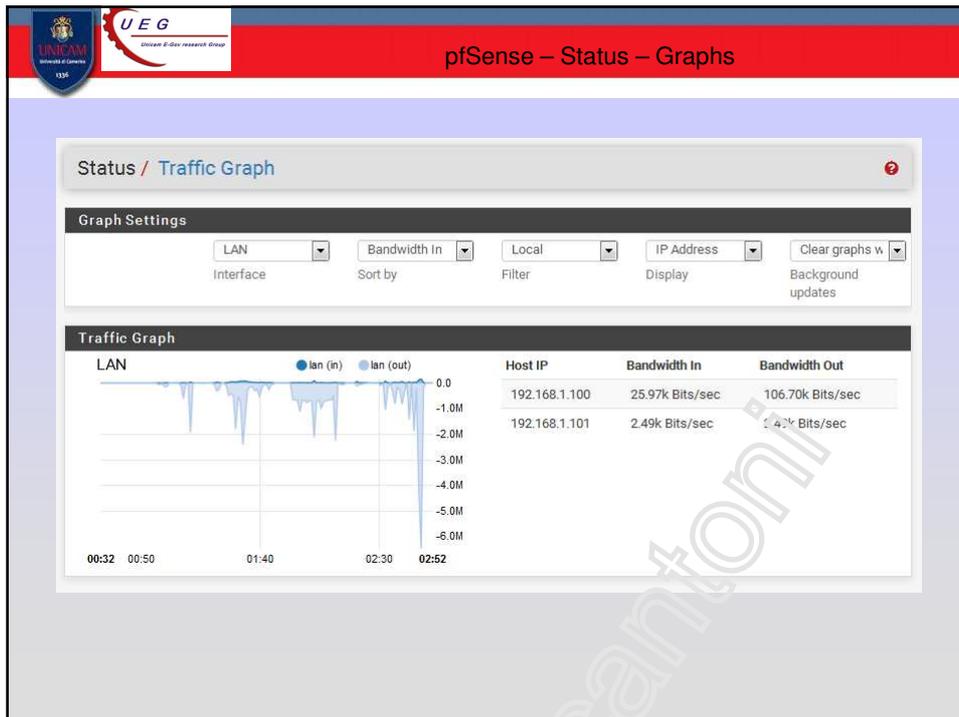
105

ARP table

Diagnostica / ARP Table

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

106



107

System / Package Manager - Available Packages

Installed Packages | Available Packages

Search: Search for: [] Both [v] Search [x] Clear [x]

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

Name	Version	Description	Install
acme	0.1.30	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates.	+ Install
Package Dependencies:		pecl-ssh2-0.0.13 socat-1.7.3.2.2 php56-5.6.31 php56-ftp-5.6.31	
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
Package Dependencies:		apcupsd-3.14.14.2	
arping	1.2.2.1	Broadcasts a who-has ARP packet on the network and prints answers.	+ Install
Package Dependencies:		arping-2.15.1	
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

108

pfSense – Package - squid proxy

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

Name	Version	Description	Install
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

109

System: Package Manager: Install Package

Available packages | Installed packages | **Package Installer**

```

squid installation completed.

Beginning package installation for squid...
Downloading package configuration file... done.
Saving updated package information... done.
Downloading squid and its dependencies...
Checking for package installation...
Downloading http://files.pfsense.org/packages/8/A11/libwww-5.4.0_4.tbz ...
(extracting)
Loading package configuration... done.
Configuring package components...
Additional files... done.
Loading package instructions...
Custom commands...
Executing custom_php_install_command()...done.
Executing custom_php_resync_config_command()...done.
Custom commands...
Executing custom_php_install_command()...done.
Executing custom_php_resync_config_command()...done.
Menu items... done.
Integrated Tab items... done.
Services... done.
Writing configuration... done.

Installation completed. Please check to make sure that the package is
  
```

110

The screenshot shows the pfSense web interface. At the top, there are logos for UNICAM and UEG. The main header is "pfSense – Package - squid proxy". The navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The page title is "System: Package Manager: Install Package". Below the title, there are tabs for "Available packages", "Installed packages", and "Package Installer". The "Package Installer" tab is active, displaying a terminal window with the following output:

```
Lightsquid installation completed.

Beginning package installation for Lightsquid...
Downloading package configuration file... done.
Saving updated package information... done.
Downloading Lightsquid and its dependencies...
Checking for package installation... Loading package configuration... done.
Configuring package components...
Additional files... done.
Loading package instructions...
Custom commands...
Executing custom_php_install_command()...done.
Executing custom_php_resync_config_command()...done.
Custom commands...
Executing custom_php_install_command()...done.
Executing custom_php_resync_config_command()...done.
Menu items... done.
Integrated Tab items... done.
Writing configuration... done.

Installation completed. Please check to make sure that the package is
configured from the respective menu then start the package.
```

111

The screenshot shows the pfSense web interface. At the top, there are logos for UNICAM and UEG. The main header is "pfSense – Package - squid proxy". The navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The page title is "System / Package Manager / Package Installer". Below the title, there are tabs for "Installed Packages", "Available Packages", and "Package Installer". The "Package Installer" tab is active, displaying a terminal window with the following output:

```
pfSense-pkg-squid installation successfully completed.

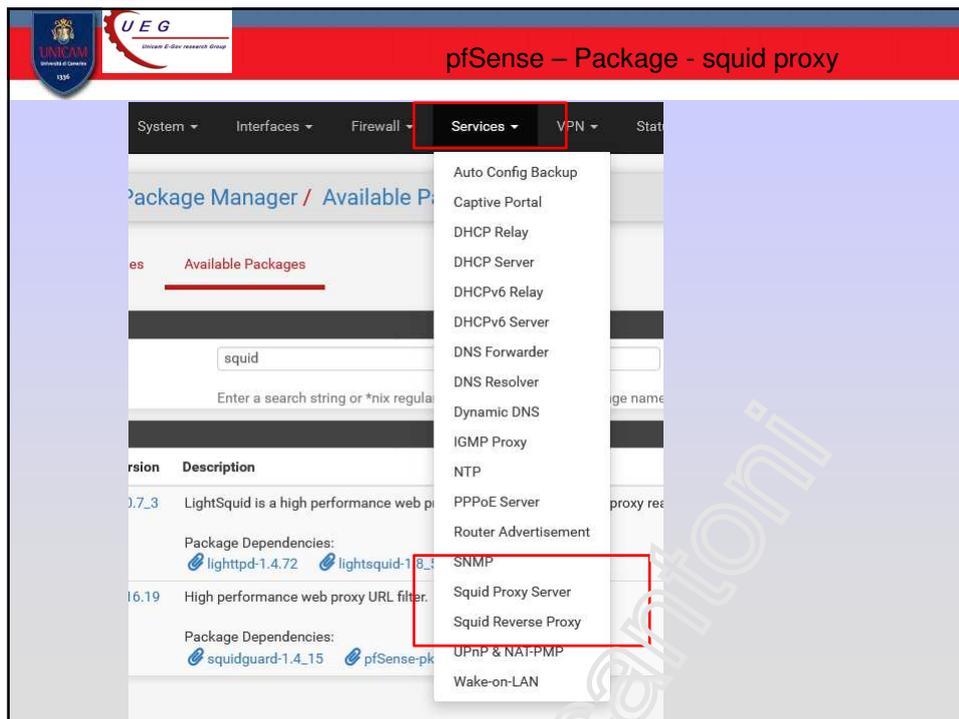
Installed Packages Available Packages Package Installer

Package Installation
make sure to check your Squid configuration against the 3.4 default
configuration file /usr/local/etc/squid/squid.conf.sample.

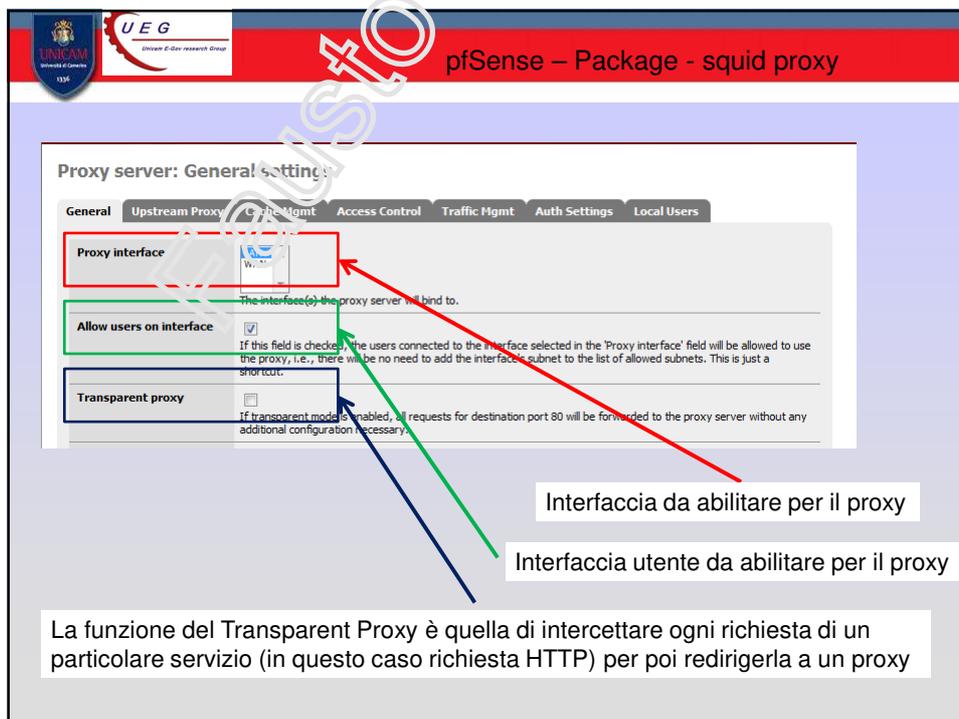
/usr/local/etc/squid/squid.conf.documented is a fully annotated
configuration file you can consult for further reference.

Additionally, you should check your configuration by calling
'squid -f /path/to/squid.conf -k parse' before starting squid.
====
Message from pfSense-pkg-squid-0.4.46:
--
Please visit Services - Squid Proxy Server menu to configure the package and enable the proxy.
>>> Cleaning up cache... done.
Success
```

112



113



114

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)

115

pfSense – Package - squid proxy

Abilitare il log - serve per Lightsquid

Enabled logging
This will enable the access log. Don't switch this on if you don't have much disk space left.

Log store directory /var/squid/log
The directory where the log will be stored (note: do not end with a /mark) **directory per i log**

Log rotate
Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

Proxy port 3128
This is the port the proxy server will listen on. **Porta TCP del proxy**

116

pfSense – Package - squid proxy

ACL: access control list

Proxy server: Access control

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

Allowed subnets

Unrestricted IPs

Banned host addresses

Whitelist

Blacklist

117

pfSense – Package - squid proxy

Bloccare l'accesso a unina.it

Blacklist unina.it

Destination domains that will be blocked for the users that are allowed to use the proxy. Put each entry on a separate line. You can also use regular expressions.

ERROR
The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: <http://www.unina.it/>
Access Denied.
Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.
Your cache administrator is admin@localhost.

Generated Mon, 27 Nov 2023 10:43:41 GMT by localhost (squid/6.3)

118

pfSense – Package - squid proxy

Configurare il proxy sul browser

The screenshot shows the Windows Internet Explorer interface with the 'Internet Options' dialog box open. The 'Connections' tab is selected. The 'Local Area Network (LAN) Settings' dialog box is also open, showing the 'Server proxy' section. The checkbox 'Utilizza un server proxy per le connessioni LAN' is checked, and the proxy address is set to 192.168.1.1 and the port to 3129. A red box highlights the 'Impostazioni LAN' button in the 'Internet Options' dialog.

119

pfSense – Package - squid proxy

aggiungere regole sul firewall

The screenshot shows the pfSense Firewall Rules configuration page. The 'Rules (Drag to Change Order)' table is visible, showing four rules. The rule 'per squid' is highlighted with a red box. The rule details are: States: 8 / 1.37 GiB, Protocol: IPv4 TCP, Source: *, Destination: *, Port: 3128, Gateway: *, Queue: none, Schedule: per squid.

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	

120

The screenshot shows the Lightsquid web interface. At the top, there are logos for UNICAM and UEG. The main header is "Lightsquid". Below the header, there is a navigation menu with "System / Package Manager / Package Installer". A green box highlights the message: "pfSense-pkg-Lightsquid installation successfully completed." Below this, there are tabs for "Installed Packages", "Available Packages", and "Package Installer". A "Package Installation" section contains text about port maintainership and links to FreeBSD bugzilla and documentation. On the right side, there is a sidebar menu with various system tools, and "Squid Proxy Reports" is highlighted with a red box.

121

The screenshot shows the "Squid Proxy Reports: Settings" page. It features a red warning box with the following instructions: "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." Below this, there is an "Instructions" section with a note: "Perform these steps after install IMPORTANT: Click Info and follow the instructions below if this is initial install!". The "Logging Settings" section has a checkbox for "Enable Access Logging" which is checked, with a warning: "Warning: Do NOT enable if available disk space is low." At the bottom, there is a "Proxy Interface(s)" dropdown menu with options: WAN, LAN, and loopback.

122

The screenshot shows the 'Web Service Settings' and 'Report Template Settings' sections of the pfSense configuration interface for the 'squid proxy' package.

Web Service Settings:

- Lightsquid Web Port:** 7445 (Default: 7445)

Report Template Settings:

- Language:** Italian
- Report Template:** Base
- Bar Color:** Red

Refresh Scheduler: 10min (!)

Manual Refresh:

- Refresh:** Will (re)parse today's entries only in Squid's current access.log.
- Refresh Full:** Will (re)parse all entries in all Squid's access logs, including the rotated

A red box highlights the 'Refresh Scheduler' dropdown and the legend below it: 'Select data refresh period. The reporting task will be executed every XX minutes/hours. Legend: (!)(*) Use only with fast hardware (+) Recommended values.'

123

The screenshot shows the 'Lightsquid Web User' configuration page and the 'Rules' section.

Lightsquid Web User:

- Lightsquid Web User:** admin
- Lightsquid Web Password:** [masked]

Links:

- Open Lightsquid
- Open sqstat

Tempo per la connessione esaurito

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

Rules (Drag to Change Order)

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			📌 📄 🗑️

124

UNIVERSITÀ DI CAGLIARI
1336

UEG
Unicon E-Gov research Group

pfSense – Package - squid proxy

ERRORE

LighthSquid 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
\$tplpath	/usr/local/www/lightsquid/tpl
\$templatenam	base
\$langpath	/usr/local/share/lightsquid/lang
\$langname	it
\$reportpath	/var/lightsquid/report
Access to '/var/lightsquid/report' folder	yes
\$graphreport	1

folder content:

no problem!!!

125

UNIVERSITÀ DI CAGLIARI
1336

UEG
Unicon E-Gov research Group

Rapporto accesso sistema Squid

Periodo: Nov 2023

Calendar

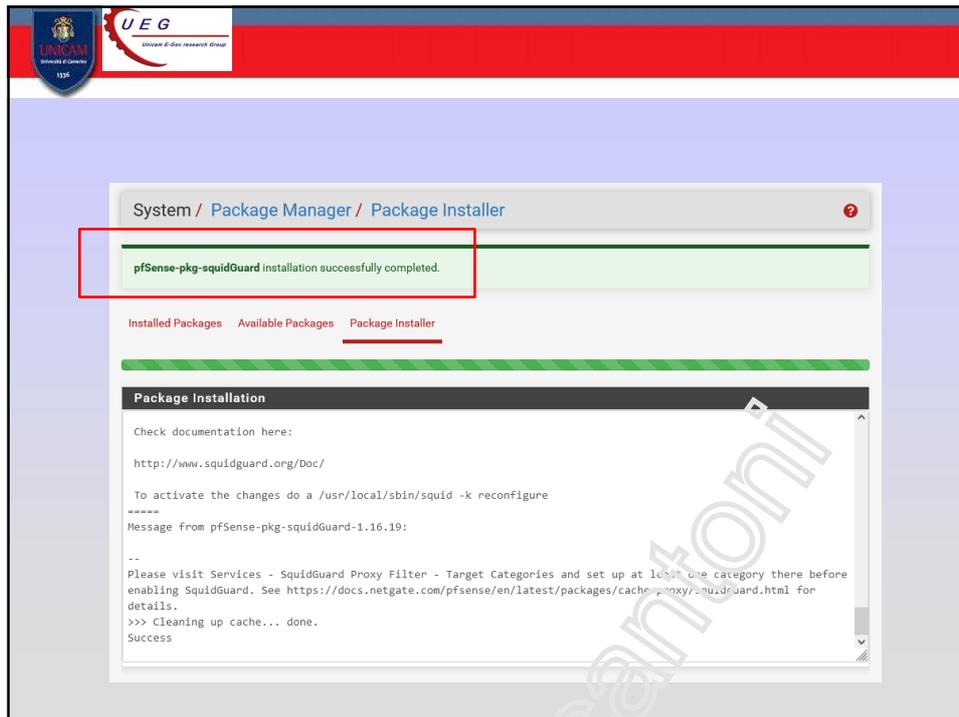
01	02	03	04	05	06	07	08	09	10	11	12
----	----	----	----	----	----	----	----	----	----	----	----

Siti maggiormente visitati	Totale	Gruppo
ANNO	ANNO	ANNO
MESE	MESE	MESE

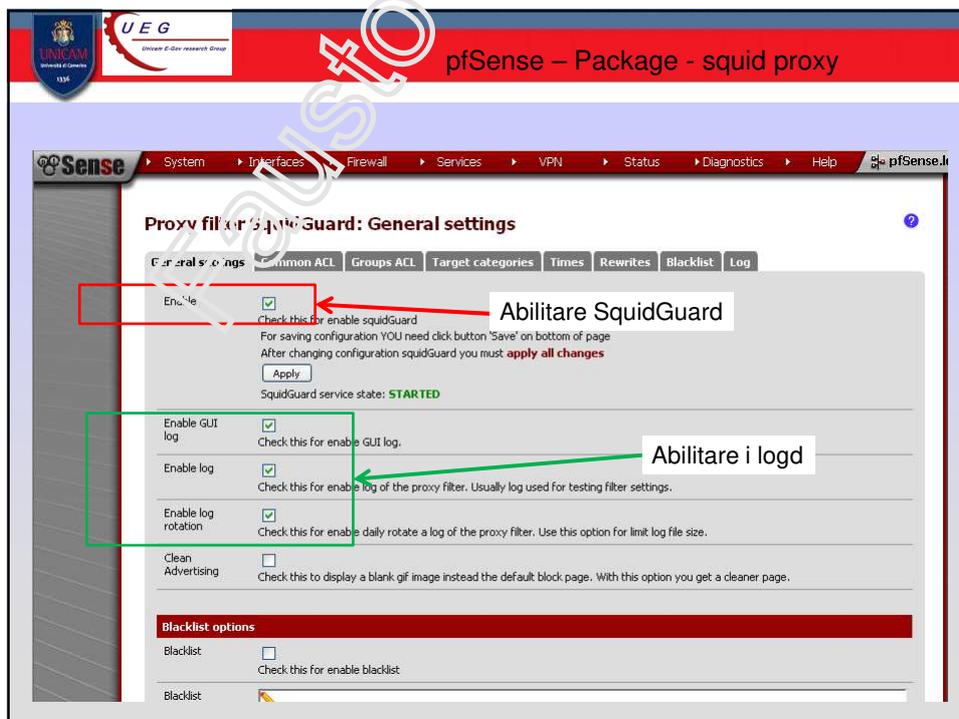
Data	Numero Utenti	Sovradimensionato	Bytes	Media	Click %
27 Nov 2023	gru	1	23.1 M	23.1 M	0.02%
Totale/Media:		1	23.1 M	23.1 M	0.02%

LightSquid v1.8 (c) Sergey Erokhin AKA ESL

126



129



130

pfSense – Package - squid proxy

0%

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/>

133

pfSense – Package - squid proxy

Package / Proxy filter SquidGuard: General settings / General settings

General settings Common ACL Group 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**

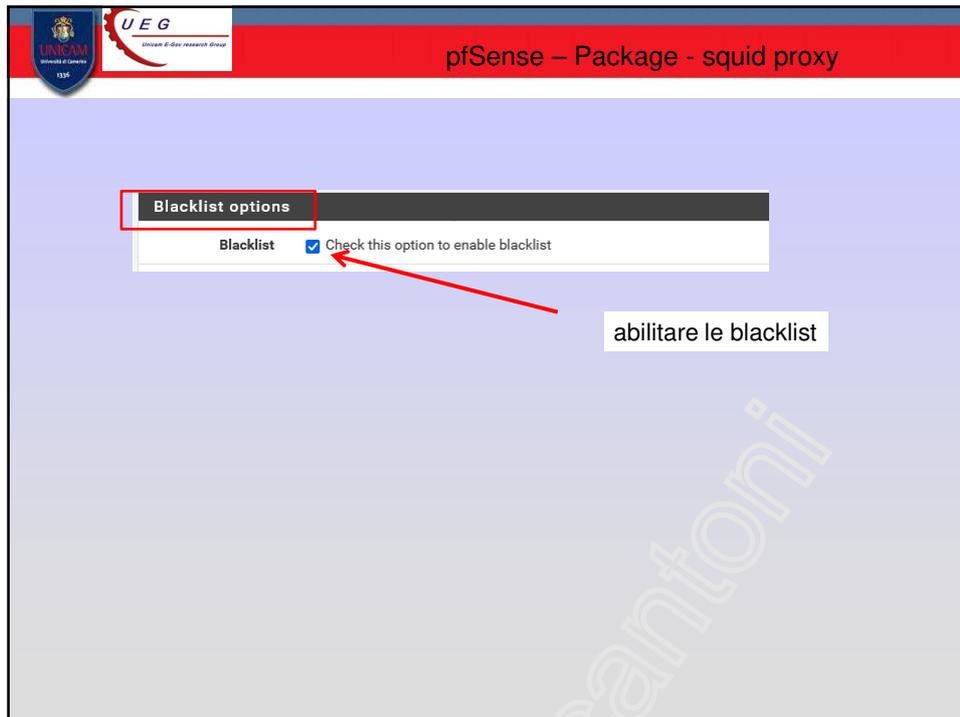
Logging options

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

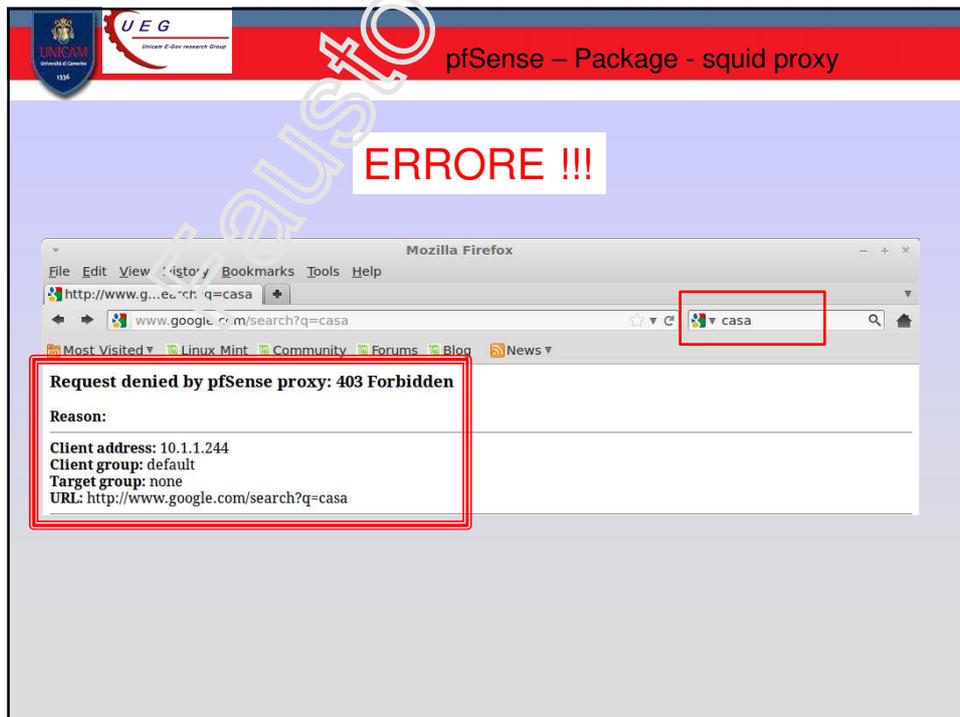
Enable log Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.

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.

134



135



136

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

pfSense – Package - squid proxy

Configurare le regole

Target Rules: all

[rule_browserlists_webfilter]

Default access [all] allow

137

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

pfSense – Package - squid proxy

dominio preso dal gruppo "bank"

ERROR: The requested URL could not be retrieved

ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: <https://192.168.1.1/sgeerror.php?>

Failed to establish a secure connection to [unknown]

The system returned:

[No Error] (TLS code: X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT+broken_cert)

Self-signed SSL Certificate: /O=pfSense GUI default Self-Signed Certificate/CN=pfSense-65688e49997f8

This proxy and the remote host failed to negotiate a mutually acceptable security settings for handling your request. It is possible that the remote host does not support secure connections, or the proxy is not satisfied with the host security credentials.

Your cache administrator is fausto.marcantoni@unicam.it.

Generated Wed, 06 Dec 2023 08:15:21 GMT by FW-IRS (squid/6.3)

138

UNICAM
Università di Camerino
1336

UEG
Unicon E-Gov research Group

pfSense – Package - squid proxy

Use SafeSearch engine

Use SafeSearch engine Enable the protected mode of search engines to limit access to mature content.
At the moment it is supported by Google, Yandex, Yahoo, MSN, Live Search, Bing, DuckDuckGo, OneSearch, Rambler, Ecosia and Qwant. Make sure that the search engines can be accessed. It is recommended to prohibit access to others.
Note: This option overrides 'Rewrite' setting.

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

139

UNICAM
Università di Camerino
1336

UEG
Unicon E-Gov research Group

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 !!!!

140

UNIVERSITÀ DI CAGLIARI UEG Union e-Gov research Group

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.

141

UNIVERSITÀ DI CAGLIARI UEG Union e-Gov research Group

Network Intrusion Detection & Prevention System

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: ids Both Search Clear

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

Packages

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

142

Snort/Suricata

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

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

<https://suricata.io/>




143

pfSense – Package - snort

System / Package Manager / Package Installer

pfSense-pkg-snort installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation

Please note that, by default, snort will truncate packets larger than the default snaplen of 15158 bytes. Additionally, LRO may cause issues with Stream5 target-based reassembly. It is recommended to disable LRO, if your card supports it.

This can be done by appending '-lro' to your ifconfig_ line in rc.conf.
 =====
 Message from pfSense-pkg-snort-4.1.6:
 --
 Please visit Services - Snort - Interfaces tab first to add an interface, then select your desired rules packages at the Services - Snort - Global tab. Afterwards visit the Updates tab to download your configured rulesets.
 >>> Cleaning up cache... done.
 Success

144

pfSense – Package - snort

System / Package Manager / Package Installation

pfSense-pkg-snort installation successfully completed.

Installed Packages Available Packages Package Installation

Package Installation

Please note that, by default, snort will truncate packets larger than the default snaplen of 15158 bytes. Additionally, LRO may cause issues with Stream5 target-based reassembly. It is recommended to disable LRO if your card supports it.

This can be done by appending '-lro' to your ifconfig_line in rc.conf. For example:

```
=====  
Message from pfSense-pkg-snort-4.1.6:  
--  
Please visit Services - Snort - Interfaces tab first to add an interface, then select your desired rules packages at the Services - Snort - Global tab. Afterwards visit the Updates tab to download your configured rulesets.  
>>> Cleaning up cache... done.  
Success
```

Services menu items: Auto Config Backup, Captive Portal, DHCP Relay, DHCP Server, DHCPv6 Relay, DHCPv6 Server & RA, DNS Forwarder, DNS Resolver, Dynamic DNS, IGMP Proxy, NTP, PPPoE Server, **Snort**, UPnP & NAT-PMP, Wake-on-LAN

145

pfSense – Package - snort

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 this 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 topdump 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.

146

The screenshot shows the 'Services / Snort / Updates' page in pfSense. A red box highlights the table of installed rule sets. A red arrow points to the 'Not Enabled' status of the 'Snort GPLv2 Community Rules' package, with the text 'regole installate' next to it. Another red arrow points to the 'Force Update' button, with the text 'aggiornare le regole' next to it.

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: Update Rules

149

The screenshot shows the same pfSense Snort Updates page, but with a 'Rules Update Task' modal dialog box open in the center. The dialog contains the following text: 'Updating rule sets may take a while ... please wait for the process to complete. This dialog will auto-close when the update is finished.' There is a 'Close' button at the bottom right of the dialog. In the bottom right corner of the screenshot, there is a small cartoon image of Charlie Brown and Snoopy sitting on a dock by a lake.

150




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 attraverso una 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.

151




Services / Snort / Updates

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

Install rule MD5 signature

Rule Set Name	MD5 Signature Hash	MD5 Signature Date
Snort Contributor 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	2c26cb4fa3bc03ab9c8e02befcffe1	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

152

Services / Snort / Interfaces

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

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> WAN (em0)	+ ▶	AC-BNFA	DISABLED	WAN	✎ 🗑️

+ Add 🗑️ Delete

Configurare le regole

153

Services / Snort / Interface Settings / WAN - Categories

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

WAN Settings WAN Categories WAN Files 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	Enable	Ruleset: Snort Text Rules	Enable	Ruleset: Snort SO Rules	Enable	Ruleset: Snort OPENAPPID Rules
<input checked="" type="checkbox"/>	Snort GPLv2 Community Rules (Talos certified)	<input type="checkbox"/>	snort_app-detect.rules	<input type="checkbox"/>	snort_browser-chrome.so.rules	<input checked="" type="checkbox"/>	openappid-ads.rules
<input checked="" type="checkbox"/>	Ruleset: FEODO Tracker Botnet C2 IP Rules	<input type="checkbox"/>	snort_attack-responses.rules	<input type="checkbox"/>	snort_browser-ie.so.rules	<input checked="" type="checkbox"/>	openappid-browser_plugin.rules
<input checked="" type="checkbox"/>	Feodo Tracker Botnet C2 IP Rules	<input type="checkbox"/>	snort_backdoor.rules	<input type="checkbox"/>	snort_browser-other.so.rules	<input checked="" type="checkbox"/>	openappid-business_applications.rules
<input checked="" type="checkbox"/>	Ruleset: ET Open Rules	<input type="checkbox"/>	snort_bad-traffic.rules	<input type="checkbox"/>	snort_browser-webkit.so.rules	<input checked="" type="checkbox"/>	openappid-collaboration.rules
<input checked="" type="checkbox"/>	emerging-activex.rules	<input type="checkbox"/>	snort_blacklist.rules	<input type="checkbox"/>	snort_exploit-kit.so.rules	<input checked="" type="checkbox"/>	openappid-database.rules
<input checked="" type="checkbox"/>	emerging-attack_response.rules	<input type="checkbox"/>	snort_botnet-cnc.rules	<input type="checkbox"/>	snort_file-executable.so.rules	<input checked="" type="checkbox"/>	openappid-file_storage.rules
<input checked="" type="checkbox"/>	emerging-botcc.portgrouped.rules	<input type="checkbox"/>	snort_botnet-cnc.rules	<input type="checkbox"/>	snort_file-flash.so.rules	<input checked="" type="checkbox"/>	openappid-file_transfer.rules
<input checked="" type="checkbox"/>	emerging-botcc.rules	<input type="checkbox"/>	snort_browser-chrome.rules	<input type="checkbox"/>	snort_file-flash.so.rules	<input checked="" type="checkbox"/>	openappid-file_transfer.rules
<input checked="" type="checkbox"/>	emerging-chat.rules	<input type="checkbox"/>	snort_browser-firefox.rules	<input type="checkbox"/>	snort_file-image.so.rules	<input checked="" type="checkbox"/>	openappid-games.rules
<input checked="" type="checkbox"/>	emerging-ciarmy.rules						
<input checked="" type="checkbox"/>	emerging-compromised.rules						
<input checked="" type="checkbox"/>	emerging-current_events.rules						

154

The image shows two screenshots from the pfSense web interface. The top screenshot is the 'Alerts' configuration page, showing 'Alert Log View Settings' with 'Interface to Inspect' set to 'WAN (em0)', 'Auto-refresh' checked, and 'Alert lines to display' set to 250. The bottom screenshot is the 'Blocked Hosts' configuration page, showing 'Blocked Hosts and Log View Settings' with 'Refresh and Log View' checked and 'Number of blocked entries to view' set to 500. A watermark 'Eduardo Marcantonio' is visible across the images.

155

The image shows the 'Package - snort' configuration page in pfSense. Under the 'Abilitare' (Enable) section, two checkboxes are checked: 'snort_indicator-scan.rules' and 'snort_scan.rules'. Below this, a terminal command is shown: 'nmap -p 1-65535 -T4 -A -v <IP WAN>'. The bottom part of the screenshot shows the 'Alert Log View Filter' section with '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

156

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 9900-5920 [Classification: Attempted Information Leak] [Priority: 2] (TCP) 193.205.92.225:42308 -> 193.205.92.226:5920
Nov 29 11:47:36	snort	80880	[1:2002910:5] ET SCAN Potential VNC Scan 5800-5920 [Classification: Attempted Information Leak] [Priority: 2] (TCP) 193.205.92.225:42308 -> 193.205.92.226:5920
Nov 29 11:47:37	snort	80880	[1:2010935:3] ET SCAN Suspicious inbound to MySQL port 1433 [Classification: Potentially Bad Traffic] [Priority: 2] (TCP) 193.205.92.225:42310 -> 193.205.92.226:1433
Nov 29 11:47:37	snort	80880	[1:2010935:3] ET SCAN Suspicious inbound to MySQL port 1433 [Classification: Potentially Bad Traffic] [Priority: 2] (TCP) 193.205.92.225:42310 -> 193.205.92.226:1433

157

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

usare i filtri

Advanced Log Filter

Time Process PID Quantity

snort

Apply Filter

Regular expression reference Precede with exclamation (!) to exclude match. Invalid or potentially dangerous patterns will be ignored.

158

pfSense – Package - snort

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

Block offenders
Checking this option will automatically block hosts that generate a Snort alert.

temporizzare il blocco

General Settings

Remove Blocked Hosts Interval: NEVER
 Remove Blocked Hosts After Deinstall: 1 HOUR
 Keep Snort Settings After Deinstall: 12 HOURS
 Startup/Shutdown Logging: 1 DAY

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> WAN (em0)	<input checked="" type="checkbox"/>	AC-BNFA	LEGACY MODE	WAN	

159

pfSense – Package - snort

Services / Snort / Blocked Hosts

Snort 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

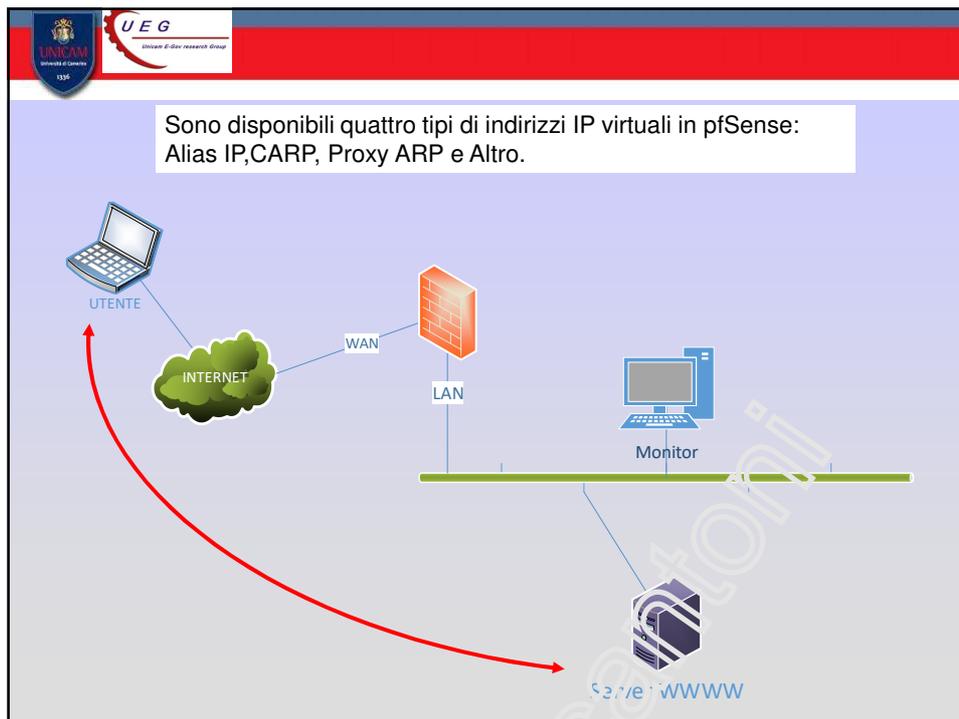
Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)

#	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

160



161

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type: IP Alias CARP Proxy ARP Other

Interface: WAN

Address type: Single address

Address(es): 193.205.92.247 / 32

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password: Virtual IP Password (Enter the VHID group password.) / Virtual IP Password (Confirm)

VHID Group: 1 (Enter the VHID group that the machines will share.)

Advertising frequency: 1 (Base) / 0 (Skew)

The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description: IP Alias per sito web (A description may be entered here for administrative reference (not parsed).)

Save

162

Firewall / Rules / WAN

Floating WAN LAN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/480 B	IPv4 ICMP	*	*	*	*	none			

Aggiungere regola passa ICMP per testare l'IP Alias

```

Amministratore Prompt dei comandi

C:\Users\fausto.mfausto>ping 193.205.92.247

Esecuzione di Ping 193.205.92.247 con 32 byte di dati:
Risposta da 193.205.92.247: byte=32 durata<1ms TTL=64

Statistiche Ping per 193.205.92.247:
Pacchetti: Trasmessi = 4, Ricevuti = 4,
Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 0ms, Massimo = 0ms, Medio = 0ms

C:\Users\fausto.mfausto>

```

163

Firewall / NAT / 1:1

Port Forward 1:1 Outbound NAT

NAT 1:1 Mappings

Interface	External IP	Internal IP	Destination IP	Description	Actions
<input checked="" type="checkbox"/>	WAN	193.205.92.247	192.168.1.11	*	

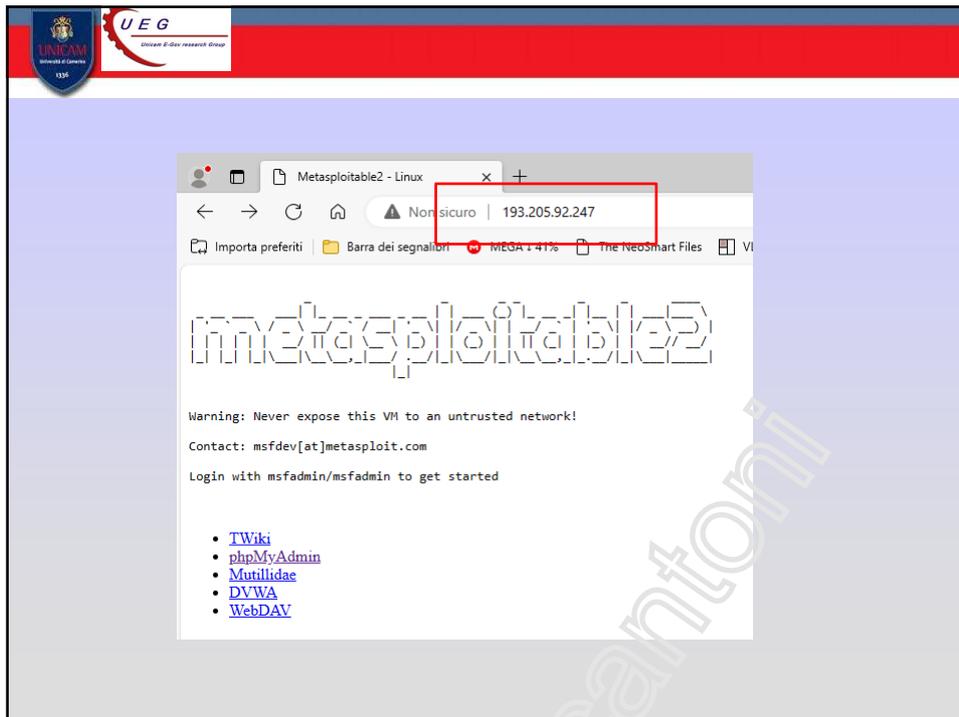
Firewall / Rules / WAN

Floating WAN LAN

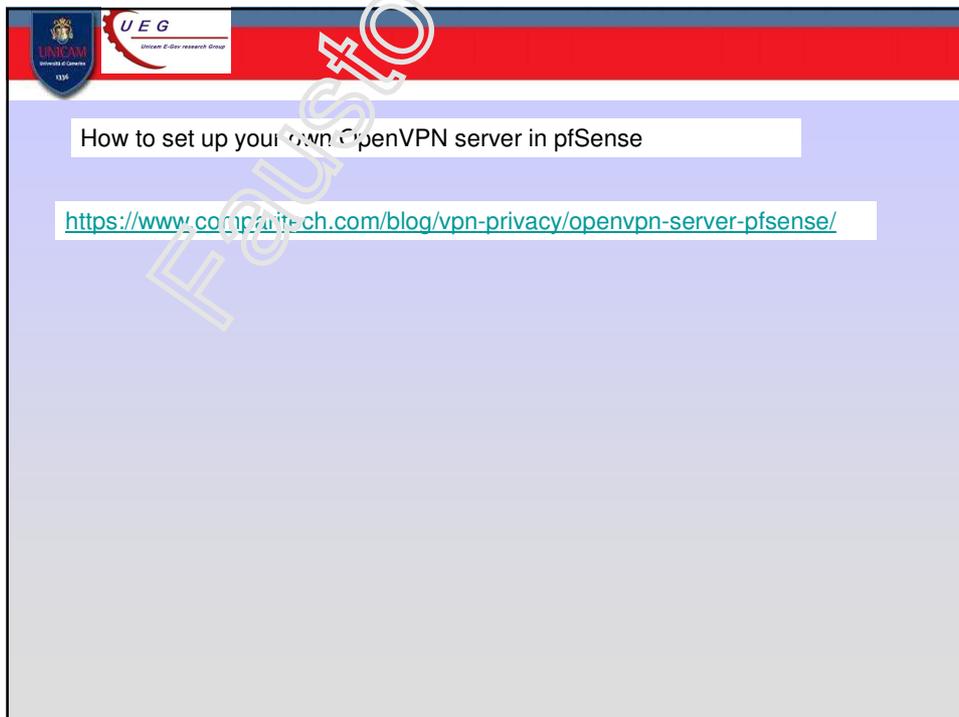
Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 ICMP	*	*	*	*	none			
<input type="checkbox"/>	2/63 KiB	IPv4 TCP	*	*	*	80 (HTTP)	none			

164



165



166



167

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. Havn 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**

```

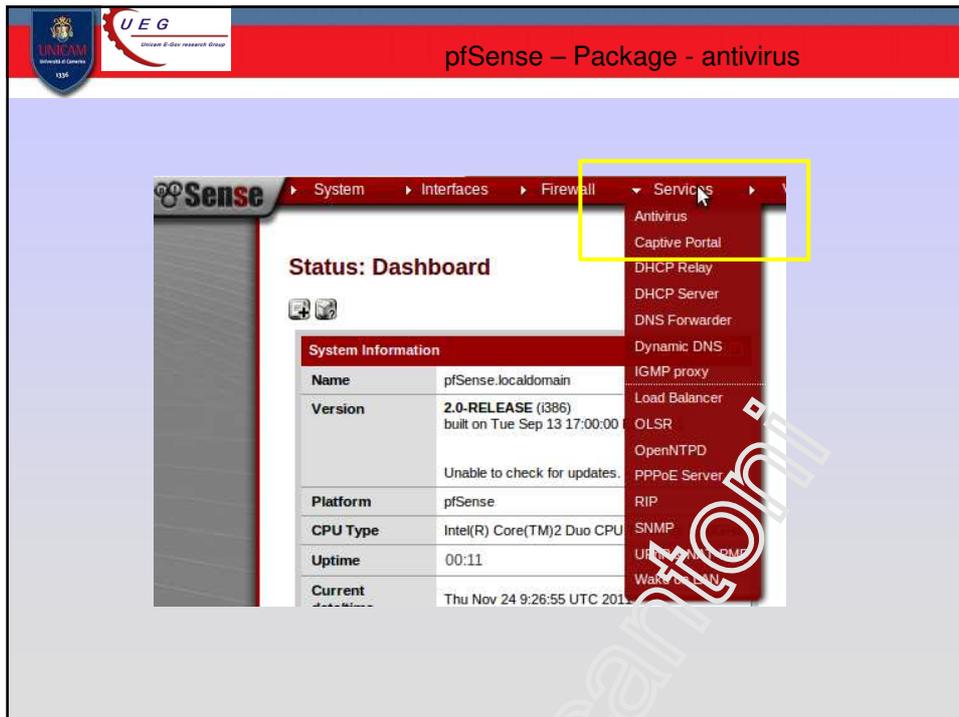
Installing HAVP antivirus and its dependencies.

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)

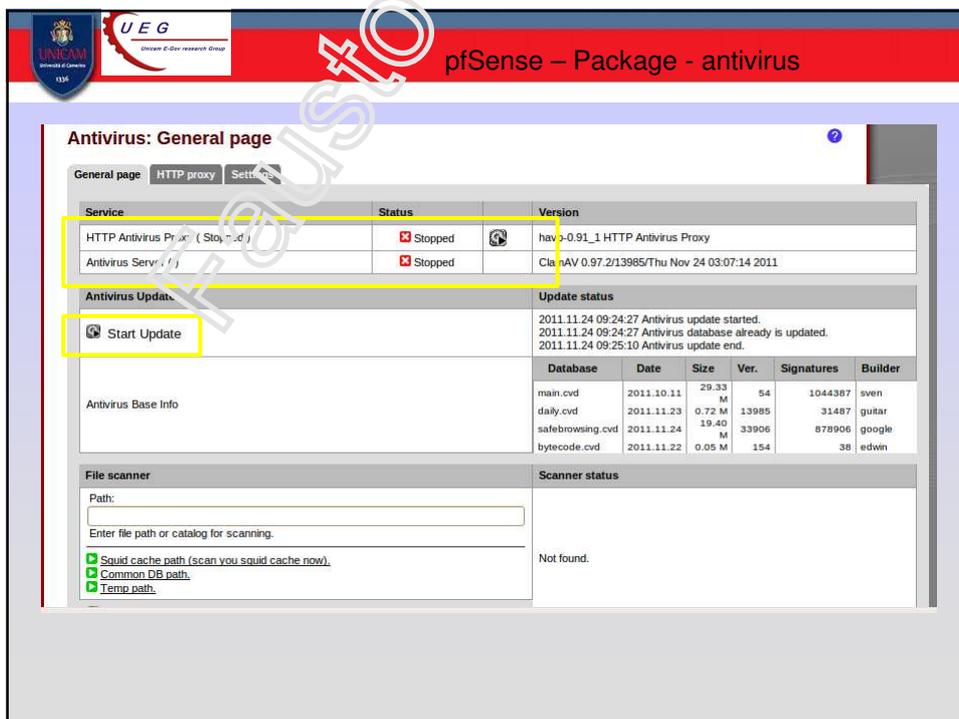
Downloading http://files.pfsense.org/packages/8/All/libltdl-2.4.tbz ... 92%

```

168



169



170

Antivirus: HTTP proxy (havp + clamav)

General page | **HTTP proxy** | Settings

Enable Check this for enable proxy.

Proxy mode Parent for Squid 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 client(s) additional configuration;
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 help.

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

171

Antivirus: Settings

General page | **HTTP Proxy** | Settings

AV base update every 2 hours Update firme virali

Update_AV Press button for update AV database now.

Regional AV database update mirror Europe
Select regional database mirror.

Optional AV database

172

pfSense – Package - antivirus

General page HTTP proxy Settings

Service	Status	Version
HTTP Antivirus Proxy (Started)	Running	havp-0.91_1 HTTP Antivirus Proxy
Antivirus Server (Started)	Running	ClamAV 0.97.3/14300/Thu Jan 12 00:37:57 2012

Antivirus Update

Start Update

Update status

2012.01.12 12:00:00 Antivirus update started.
 2012.01.12 12:00:00 Antivirus database already is updated.
 2012.01.12 12:00:04 Antivirus update end

Database	Date	Size	Ver.	Signatures	Builder
main.cvd	2011.10.11	29.33 M	5-	14387	sven
daily.cvd	2012.01.11	1.61 M	14300	70715	guitar
safebrowsing.cvd	2012.01.12	18.4 M	31703	1111762	google
bytecode.cvd	2012.01.12	0.00 M	60	38	edwin

173

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

174

pfSense – Captive Portal Https Login

Captive Portal Https Login

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

175

pfSense – Captive Portal Https Login

Captive Portal Https Login

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

176

pfSense – Captive Portal Https Login

Captive Portal Https Login

System: Certificate Manager

CA Certificates Certificate Revocation

Name	Issuer	Distinguished Name	In Use
CAinternalbase Certificate Authority	CAinformatica	emailAddress=root@informatica, ST=Macerata, O=informatica, L=Camerino, CN=CAinternalbase, C=IT	

Note: You can only delete a certificate if it is not currently in use.

Internal Certificate base

177

pfSense – Captive Portal Https Login

Captive Portal Https Login

Enable HTTPS login

When enabled, the username and password will be transmitted over an HTTPS connection to protect against MITM attacks. A server name, certificate and matching private key must also be specified below.

HTTPS server name: 10.10.10.1

HTTPS certificate: [Red box: HTTPS certificate]

HTTPS private key: [Green box: HTTPS private key]

HTTPS intermediate certificate: [Blue box: HTTPS intermediate certificate]

178

UNICAM
Università di Camerino
1336

UEG
Unicon E-Gov research Group

pfSense – Captive Portal Https Login

Captive Portal Https Login

HTTPS certificate

export cert

System: Certificate Manager

Name	Issuer
CAinternalbase Certificate Authority	CAinform

Note: You

File Download - Security Warning

Do you want to open or save this file?

Name: CAinternalbase.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?](#)

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

179

UNICAM
Università di Camerino
1336

UEG
Unicon E-Gov research Group

pfSense – Captive Portal Https Login

Captive Portal Https Login

HTTPS private key

export key

System: Certificate Manager

Name	Issuer
CAinternalbase Certificate Authority	CAinform

Note: You

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?](#)

Open direttamente
Fare Copia e Incolla del certificato

180

UNICAM University of Camerino 1336 UEG Union E-Gov research Group

pfSense – Captive Portal Https Login

Captive Portal Https Login **HTTPS intermediate certificate**

System: Certificate

Name	In
CAinformatica	YES
ca Intermediate1	YES

Additional trusted Certificate Authority

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

File Download - Security Warning

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?](#)

export key

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

181

UNICAM University of Camerino 1336 UEG Union E-Gov research Group

pfSense – Captive Portal Https Login

https://10.10.10.1:8001/index.php?redir...&https://www.google.com/ Certificate Error

Certificate Invalid

The security certificate presented by this website has errors.

This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

About certificate errors

View certificates

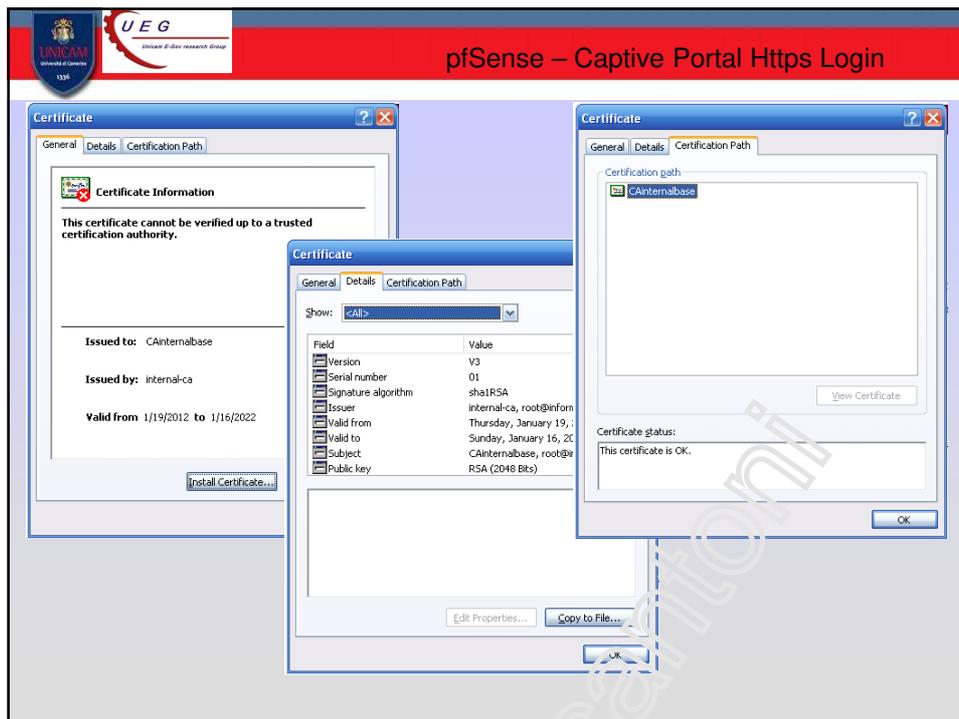
Username:

Password:

Continue

Dettagli Certificato

182



183



184