



CCR Tutorial Days 10-12 ottobre @ LNF



PacketFence



Enrico Becchetti


Obiettivi

- Circolare AgID 18/04/2018 n.2/2017
 - consentire l'accesso solo agli aventi diritto (LOA2, disciplinare risorse informatiche, sicurezza informatica, account valido)
 - associazione dispositivo-persona tramite credenziali INFN-AAI
 - «inventario» dispositivi sia quelli attivi sia quelli connessi in precedenza
 - verifica dei computer (S.O. obsoleti, servizi vulnerabili etc.)
- altri...
 - accesso in rete senza alcun software da installare nei computer
 - compatibilità con gli apparati di rete già presenti in Sezione
 - dispositivi «speciali» (stampanti, sistemi presenti nei laboratori, etc)
 - mobilità dei dispositivi all'interno della Sezione/Dipartimento
 - accesso in rete wifi compatibile con TRIP (INFN-dot1x e INFN-web)
 - segnalazione in caso di traffico «anomalo» (p2p e Tor)

Reti



INFN-web



INFN-dot1x



INFN-wired

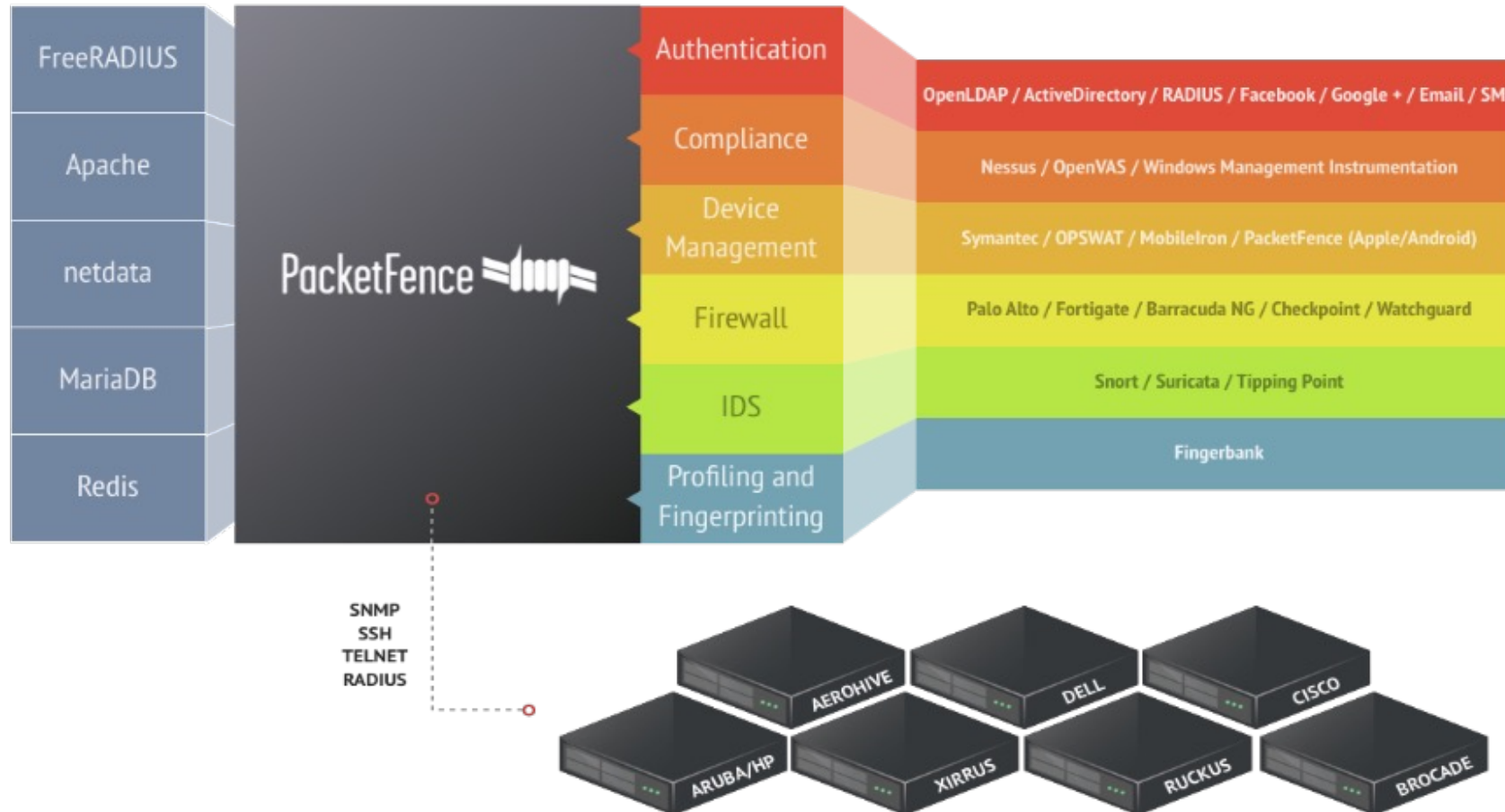


INFN-embedded

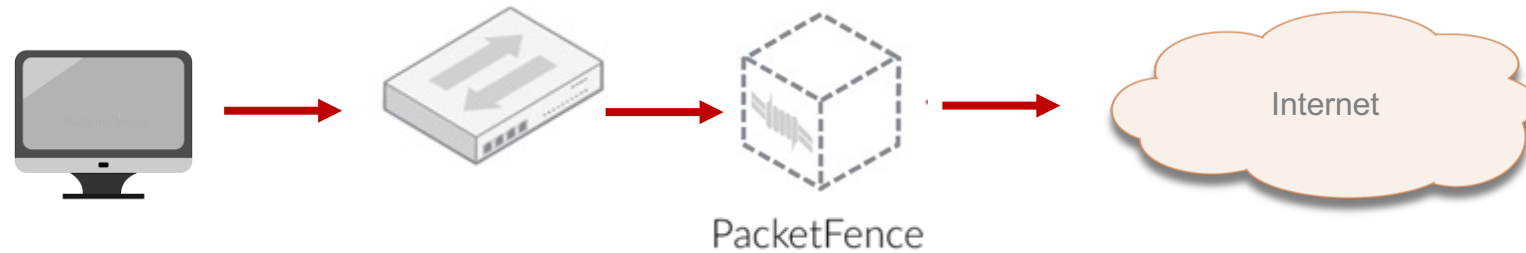
- **PacketFence**

- open source (perl , go e shell script)
- prodotto ben mantenuto (Inverse)
- documentazione
- supporto tramite mailing list
- supporto a pagamento
- HA/scalabile (cluster)
- usa protocolli standard: 802.1x, snmp, etc.

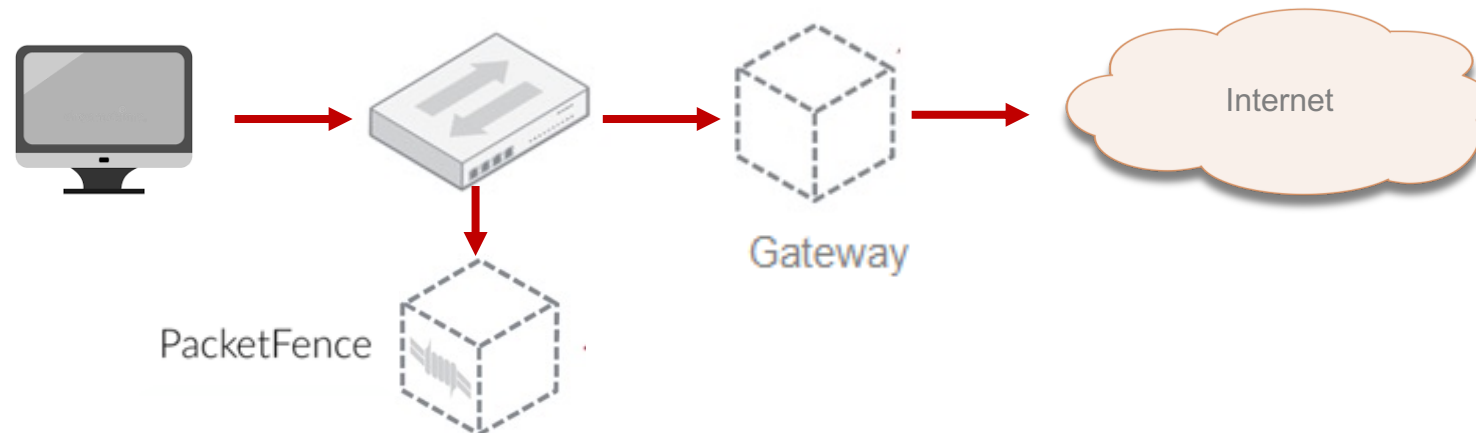
- Repository dedicati (Debian e RedHat Enterprise Linux)
- supporta vari backend di autenticazione: ldap, radius, SAML, ed altri
- integrazione con molti apparati di rete (per esempio Cisco ed HP)
- integrazione con OpenVas (scanner di rete) e Suricata (IDS)
- captive portal
- modalità ibrida sia INLINE che Out-of-band (vlan mode)



- Packetfence modalità inline



- Packetfence modalità out-of-band (vlan mode)



PacketFence 

Installazione e configurazione



CCR Tutorial Days 10-12 ottobre @ LNF



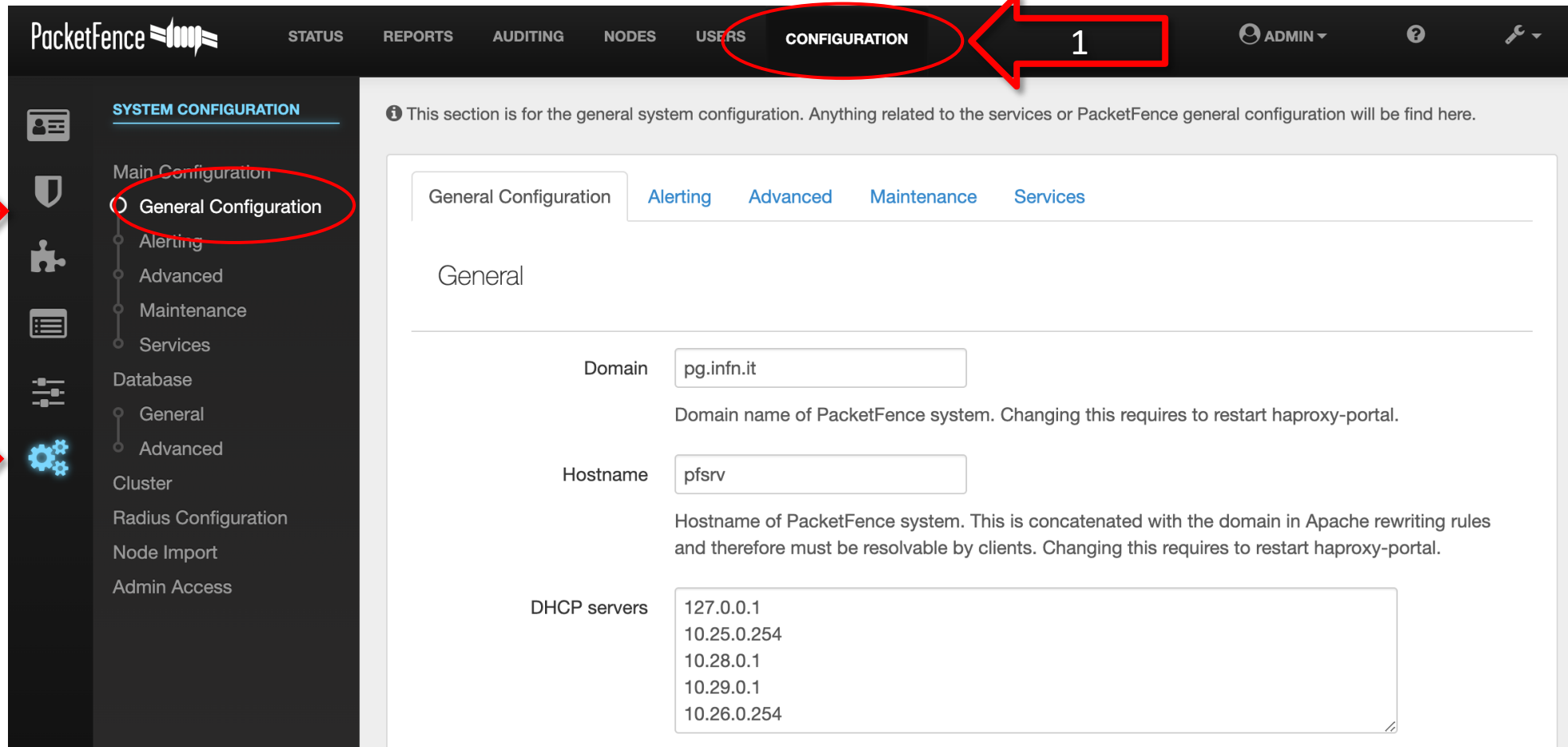
Installazione:

- Appliance preconfigurato <https://www.packetfence.org/download.html#/zen>
- Immagine ISO Debian 11 con PF12 <https://www.packetfence.org/download.html#/releases>
- Repository RedHat <https://www.packetfence.org/downloads/PackageFence/RHEL8/>
- Repository Debian <https://www.packetfence.org/downloads/PackageFence/debian/>

Packetfence@PG versione 8.3:

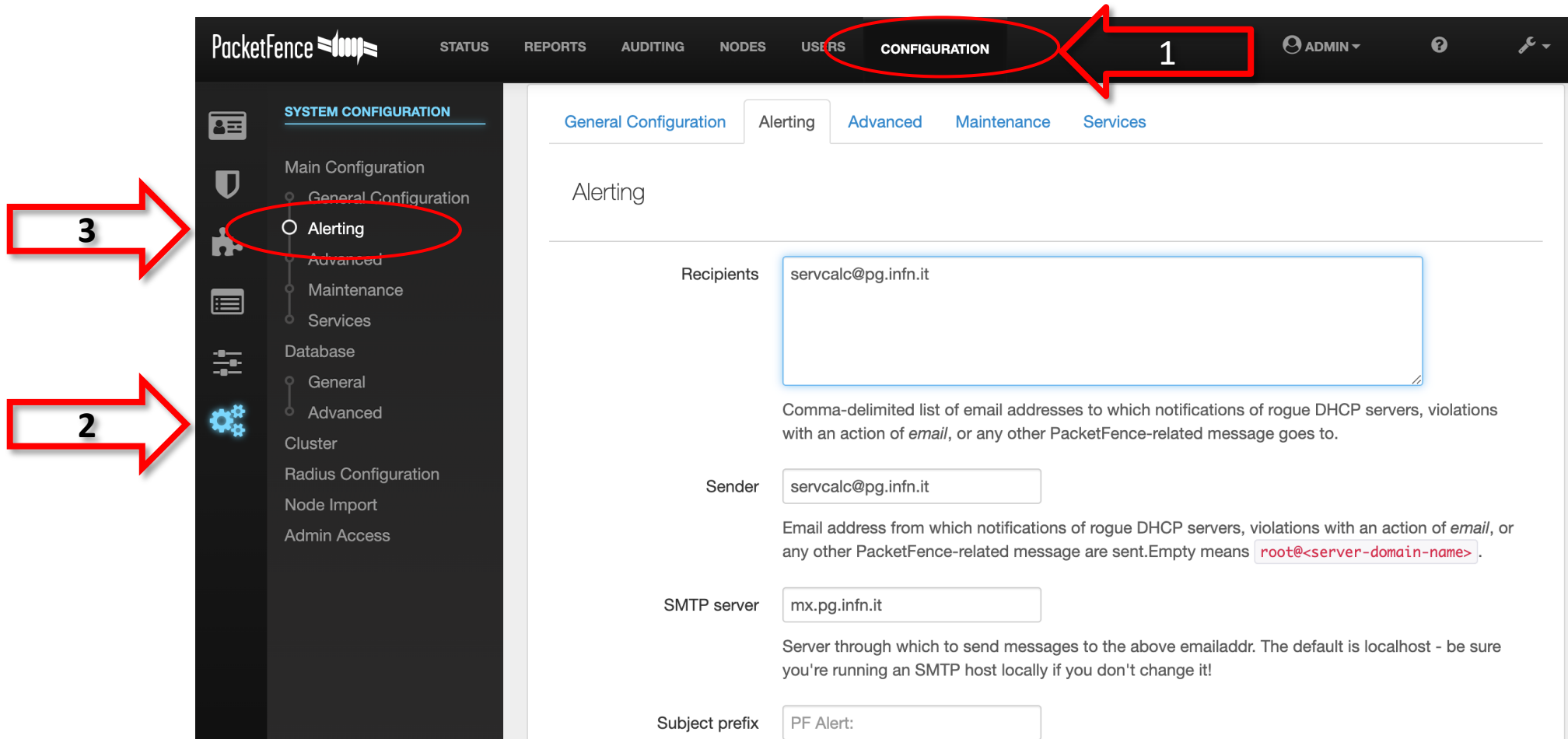
- Macchina virtuale CentOS 7, 4 core , 8GB RAM, 150GB HDD, una scheda di rete
- Guida per l'installazione https://www.packetfence.org/doc/PackageFence_Installation_Guide.html
- Prerequisiti:
 - Disabilitare SELinux, Firewalld eseguire l'update del sistema operativo installare kernel-devel

Al termine dell'installazione, circa 750 pacchetti, si può iniziare la configurazione di Packetfence tramite il link <https://pfsrv.management:1443/configurator>



The screenshot shows the PacketFence web interface. The top navigation bar includes 'STATUS', 'REPORTS', 'AUDITING', 'NODES', 'USERS', and 'CONFIGURATION'. The 'CONFIGURATION' menu item is circled in red and labeled with a red arrow and the number '1'. The left sidebar shows 'SYSTEM CONFIGURATION' with sub-items: 'Main Configuration', 'General Configuration', 'Alerting', 'Advanced', 'Maintenance', 'Services', 'Database', 'General', 'Advanced', 'Cluster', 'Radius Configuration', 'Node Import', and 'Admin Access'. The 'General Configuration' sub-item is circled in red and labeled with a red arrow and the number '3'. The 'General Configuration' sub-item is also circled in red and labeled with a red arrow and the number '2'. The main content area shows the 'General Configuration' page with tabs for 'General Configuration', 'Alerting', 'Advanced', 'Maintenance', and 'Services'. The 'General' tab is selected. The page contains the following configuration fields:

- Domain:** Domain name of PacketFence system. Changing this requires to restart haproxy-portal.
- Hostname:** Hostname of PacketFence system. This is concatenated with the domain in Apache rewriting rules and therefore must be resolvable by clients. Changing this requires to restart haproxy-portal.
- DHCP servers:**



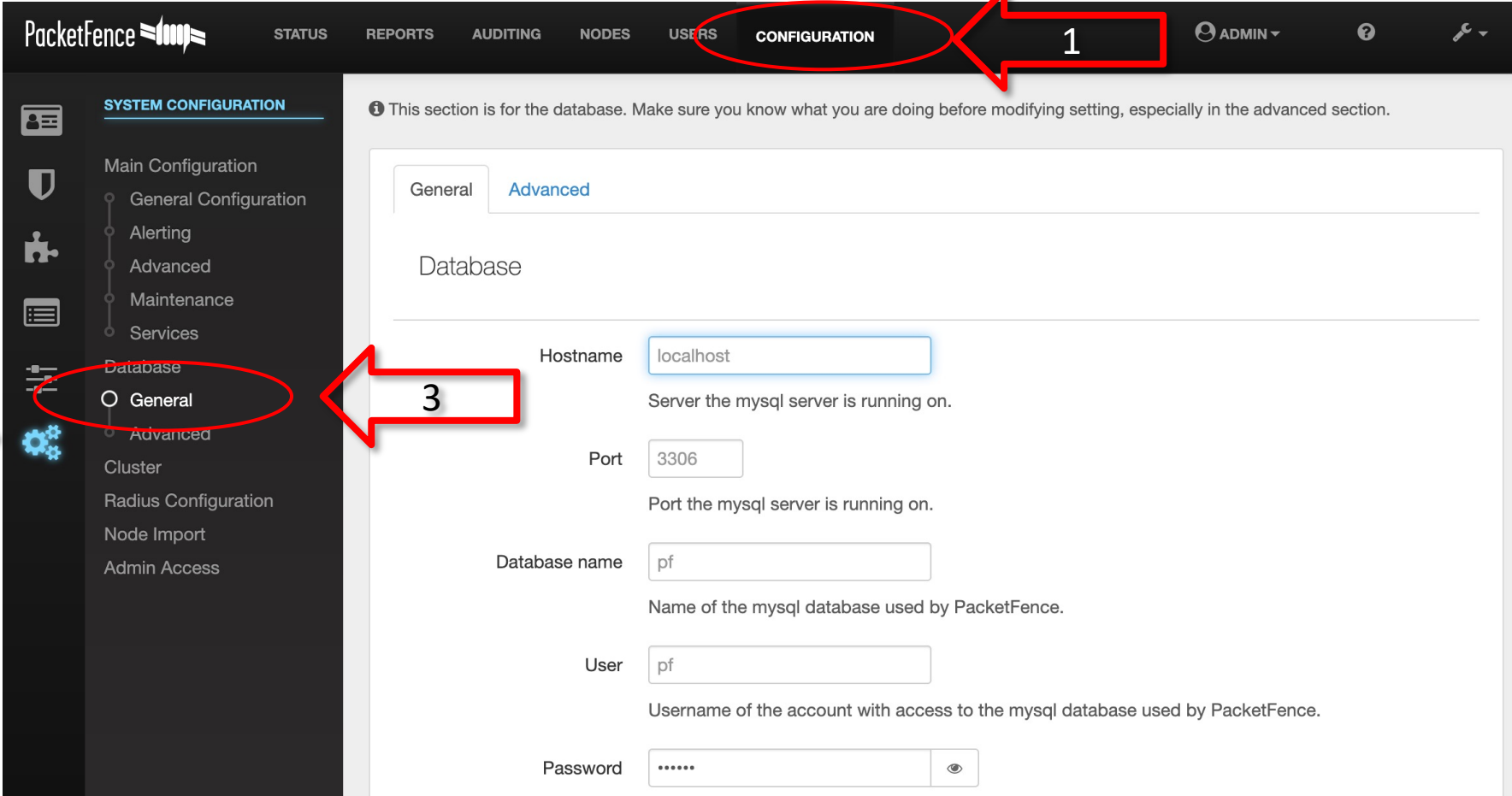
The screenshot shows the PacketFence web interface. The top navigation bar includes STATUS, REPORTS, AUDITING, NODES, USERS, CONFIGURATION (highlighted with a red circle and arrow labeled '1'), ADMIN, and a help icon. The left sidebar shows the SYSTEM CONFIGURATION menu with sub-items: Main Configuration, General Configuration, Alerting (highlighted with a red circle and arrow labeled '3'), Advanced, Maintenance, Services, Database, General, Advanced, Cluster, Radius Configuration, Node Import, and Admin Access. An arrow labeled '2' points to the gear icon in the sidebar. The main content area shows the Alerting configuration page with tabs for General Configuration, Alerting, Advanced, Maintenance, and Services. The Alerting page has the following fields:

- Recipients:
- Sender:
- SMTP server:
- Subject prefix:

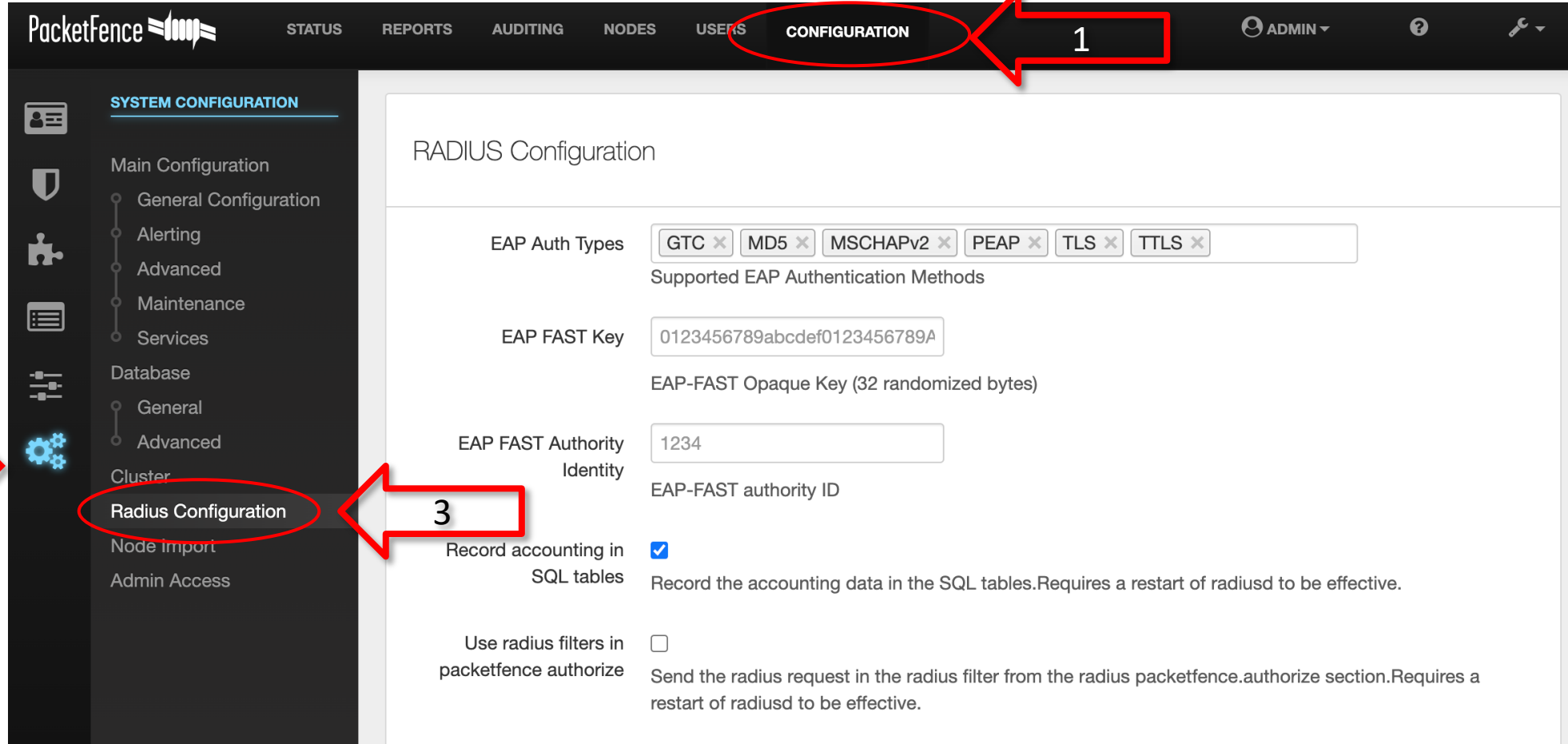
Below the Recipients field, there is a description: "Comma-delimited list of email addresses to which notifications of rogue DHCP servers, violations with an action of *email*, or any other PacketFence-related message goes to."

Below the Sender field, there is a description: "Email address from which notifications of rogue DHCP servers, violations with an action of *email*, or any other PacketFence-related message are sent. Empty means `root@<server-domain-name>`."

Below the SMTP server field, there is a description: "Server through which to send messages to the above emailaddr. The default is localhost - be sure you're running an SMTP host locally if you don't change it!"



The screenshot shows the PacketFence web interface. The top navigation bar includes STATUS, REPORTS, AUDITING, NODES, USERS, and CONFIGURATION. The CONFIGURATION tab is highlighted with a red circle and a red arrow labeled '1'. The left sidebar shows the SYSTEM CONFIGURATION menu with options like Main Configuration, Alerting, Advanced, Maintenance, Services, Database, Cluster, Radius Configuration, Node Import, and Admin Access. The Database section is selected, and the General sub-section is highlighted with a red circle and a red arrow labeled '2'. The main content area shows the Database configuration page with a warning message: "This section is for the database. Make sure you know what you are doing before modifying setting, especially in the advanced section." The configuration fields are: Hostname (localhost), Port (3306), Database name (pf), User (pf), and Password (masked). A red arrow labeled '3' points to the General sub-section in the sidebar.



The screenshot displays the PacketFence web interface. The top navigation bar includes 'STATUS', 'REPORTS', 'AUDITING', 'NODES', 'USERS', and 'CONFIGURATION'. The 'CONFIGURATION' tab is highlighted with a red circle and an arrow labeled '1'. The left sidebar shows 'SYSTEM CONFIGURATION' with sub-items: 'Main Configuration' (General Configuration, Alerting, Advanced, Maintenance, Services), 'Database' (General, Advanced), 'Cluster', 'Radius Configuration', 'Node Import', and 'Admin Access'. 'Radius Configuration' is highlighted with a red circle and an arrow labeled '2'. The main content area is titled 'RADIUS Configuration' and contains the following settings:

- EAP Auth Types:** GTC x MD5 x MSCHAPv2 x PEAP x TLS x TTLS x
- Supported EAP Authentication Methods:** (Label for the above list)
- EAP FAST Key:** 0123456789abcdef0123456789A
- EAP-FAST Opaque Key (32 randomized bytes):** (Label for the above field)
- EAP FAST Authority Identity:** 1234
- EAP-FAST authority ID:** (Label for the above field)
- Record accounting in SQL tables:** Record the accounting data in the SQL tables.Requires a restart of radiusd to be effective.
- Use radius filters in packetfence authorize:** Send the radius request in the radius filter from the radius packetfence.authorize section.Requires a restart of radiusd to be effective.

A red circle and arrow labeled '3' point to the 'Radius Configuration' item in the sidebar.

The screenshot shows the PacketFence web interface. The top navigation bar includes STATUS, REPORTS, AUDITING, NODES, USERS, and CONFIGURATION (highlighted with a red circle and arrow labeled '1'). The left sidebar shows NETWORK CONFIGURATION with sub-items: Networks, Network Settings, Interfaces (highlighted with a red circle and arrow labeled '2'), Inline, Inline Traffic Shaping, Fencing, Device Parking, SNMP, and Floating Device. The main content area is titled 'Interfaces & Networks' and contains a table of interface configurations. The 'Network Settings' tab is selected, and the 'Interfaces' sub-tab is also highlighted with a red circle and arrow labeled '3'. The table lists four interfaces with their logical names, IP addresses, netmasks, and types. Each interface has a toggle switch set to 'ON' and a 'DELETE' button.

Logical name	IP Address	Netmask	Type
<input checked="" type="checkbox"/> eth0	10.0.0.34	255.255.0.0	Management
default network: 10.0.0.0			
<input checked="" type="checkbox"/> eth0 vlan 101	193.205.222.20	255.255.255.0	(None)
default network: 193.205.222.0			
<input checked="" type="checkbox"/> eth0 vlan 25	10.25.0.1	255.255.0.0	other,portal,dhcp-listener
default network: 10.25.0.0			
<input checked="" type="checkbox"/> eth0 vlan 26	10.26.0.1	255.255.0.0	Other
default network: 10.26.0.0			

INFN-wired

INFN-dot1x



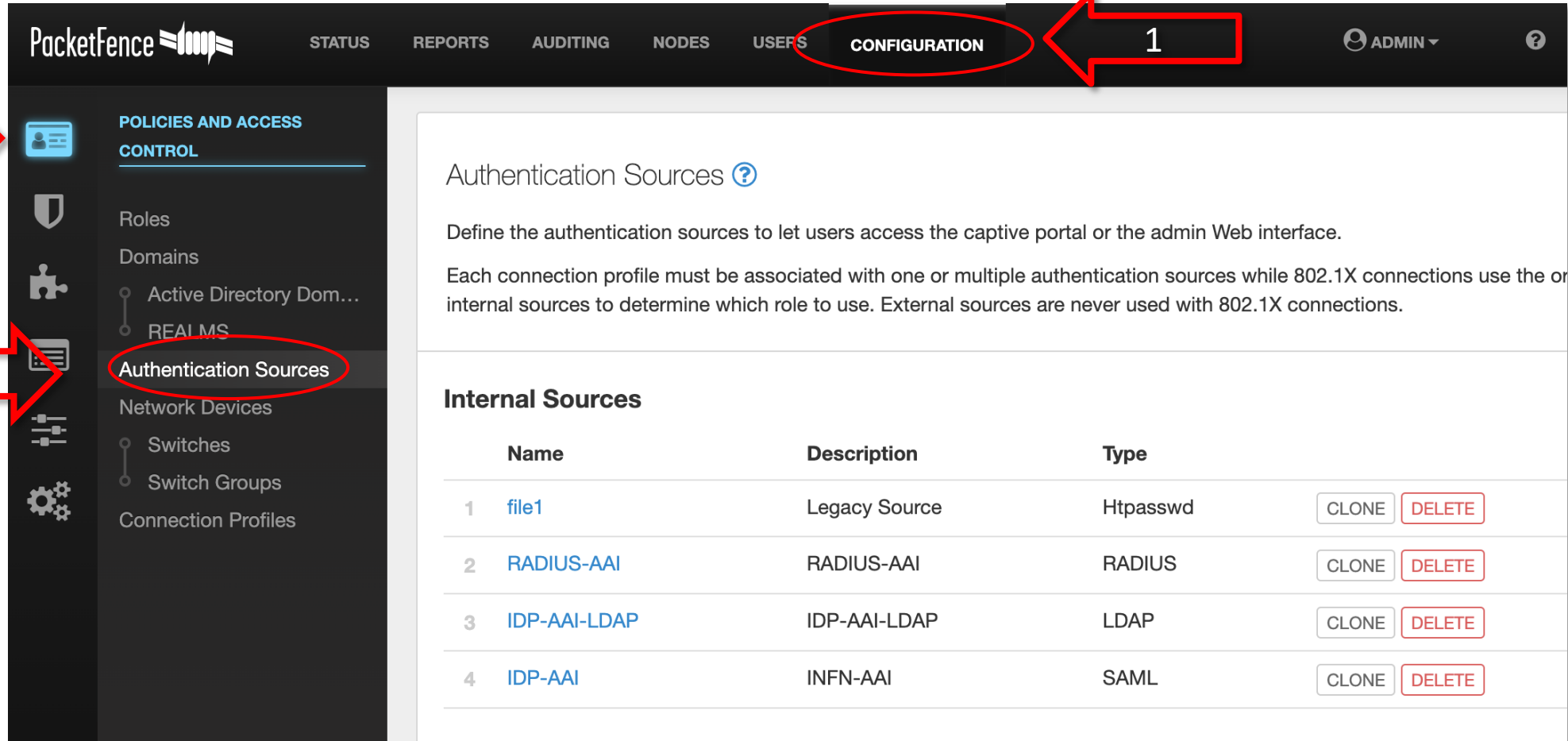
CCR Tutorial Days 10-12 ottobre @ LNF



INFN-web

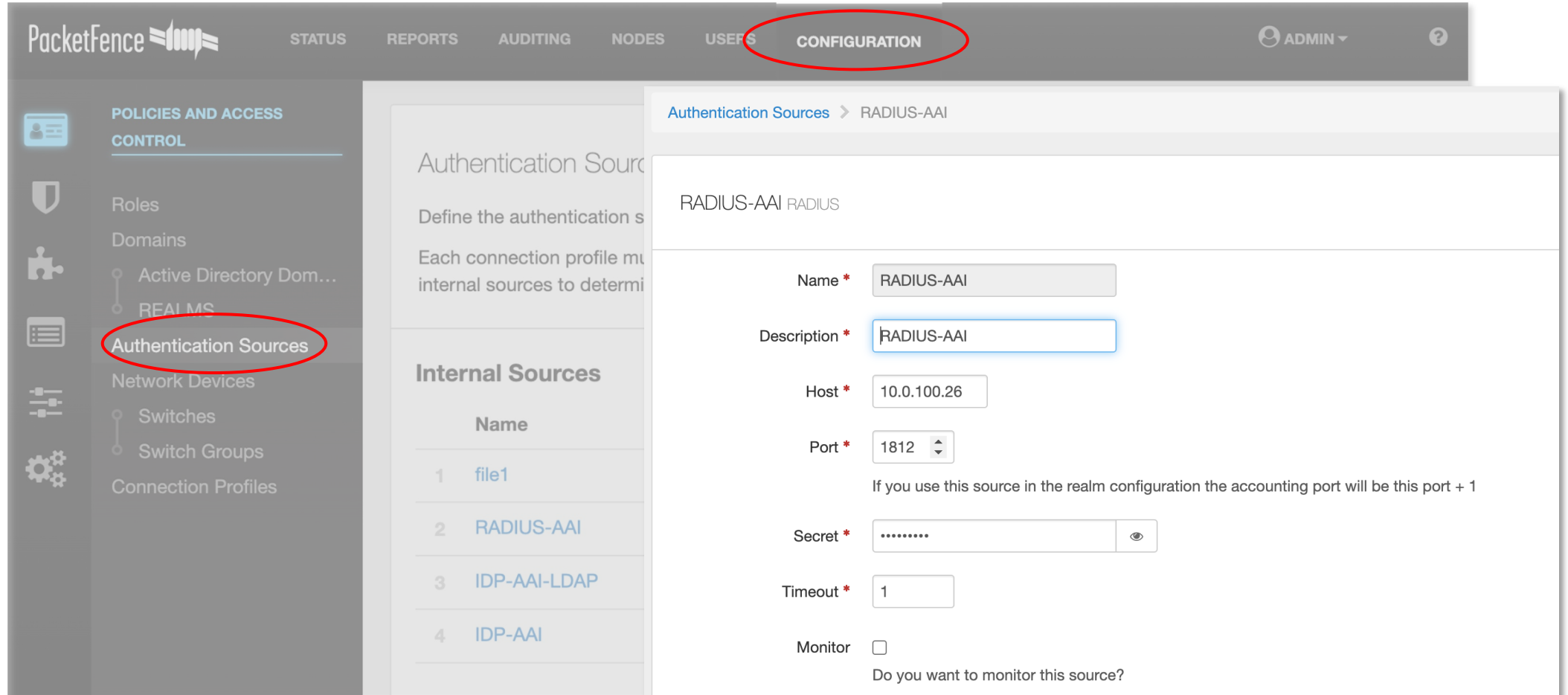
<input checked="" type="checkbox"/>	eth0	vlan 27	10.27.0.1	255.255.0.0	Inline Layer 2	DELETE
default network: 10.27.0.0						
<input checked="" type="checkbox"/>	eth0	vlan 28	10.28.0.1	255.255.0.0	Isolation	DELETE
default network: 10.28.0.0						
<input checked="" type="checkbox"/>	eth0	vlan 29	10.29.0.1	255.255.0.0	Registration	DELETE
default network: 10.29.0.0						
<input checked="" type="checkbox"/>	eth0	vlan 30	10.30.0.1	255.255.0.0	other,portal,dhcp-listener	DELETE
default network: 10.30.0.0						

INFN-embedded



The screenshot shows the PacketFence web interface. The top navigation bar includes STATUS, REPORTS, AUDITING, NODES, USERS, and CONFIGURATION. The CONFIGURATION menu item is circled in red and labeled with a red arrow and the number 1. The left sidebar contains a menu with items like POLICIES AND ACCESS CONTROL, Roles, Domains, REALMS, and Authentication Sources. The Authentication Sources menu item is circled in red and labeled with a red arrow and the number 3. The main content area displays the Authentication Sources configuration page, which includes a table of internal sources.

	Name	Description	Type		
1	file1	Legacy Source	Htpasswd	CLONE	DELETE
2	RADIUS-AAI	RADIUS-AAI	RADIUS	CLONE	DELETE
3	IDP-AAI-LDAP	IDP-AAI-LDAP	LDAP	CLONE	DELETE
4	IDP-AAI	INFN-AAI	SAML	CLONE	DELETE

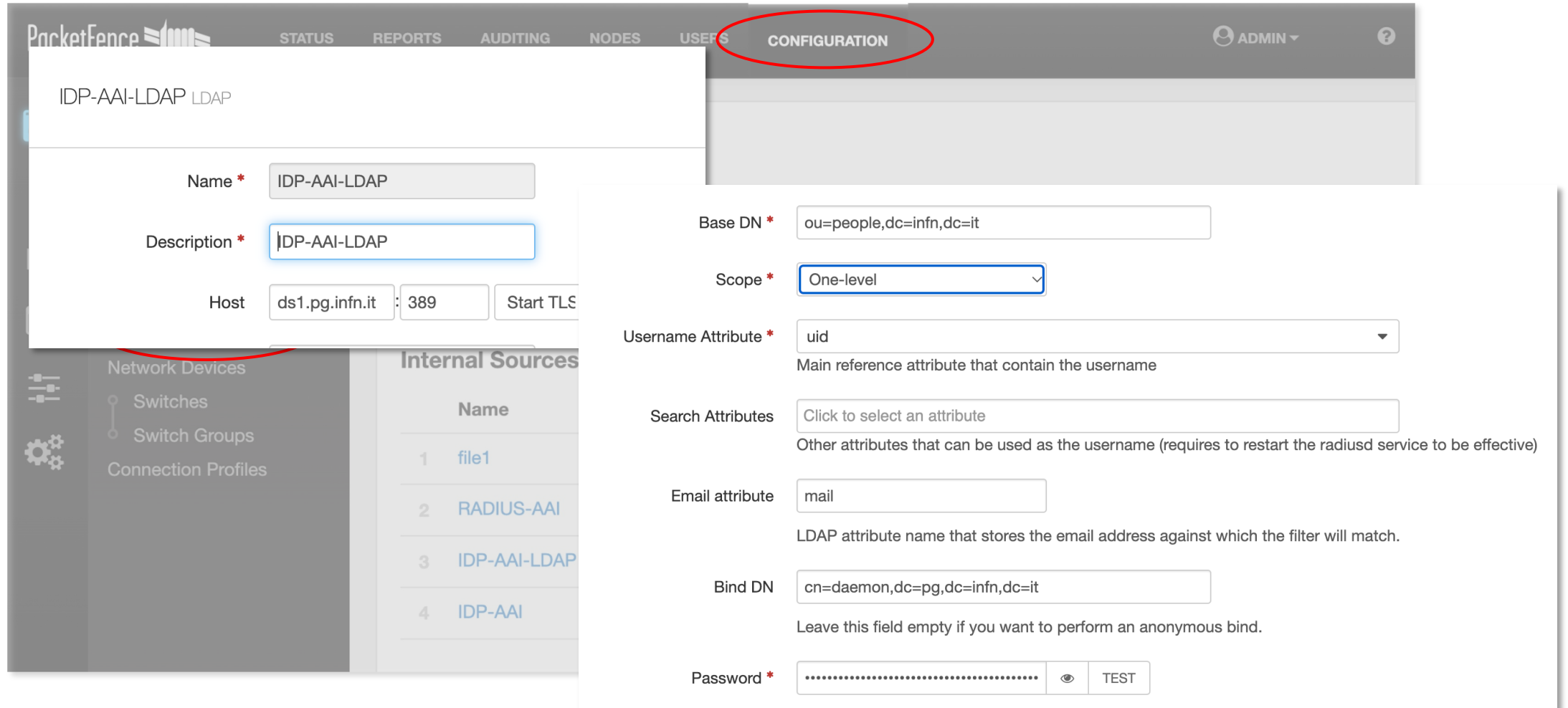


The screenshot displays the PacketFence web interface. The top navigation bar includes links for STATUS, REPORTS, AUDITING, NODES, USERS, and CONFIGURATION (highlighted with a red circle). The left sidebar shows a menu with 'Authentication Sources' highlighted (circled in red). The main content area shows the configuration for a RADIUS-AAI authentication source. The breadcrumb path is 'Authentication Sources > RADIUS-AAI'. The form fields are as follows:

- Name *: RADIUS-AAI
- Description *: RADIUS-AAI
- Host *: 10.0.100.26
- Port *: 1812 (with a note: 'If you use this source in the realm configuration the accounting port will be this port + 1')
- Secret *: [masked]
- Timeout *: 1
- Monitor: Do you want to monitor this source?

Below the form, there is a table of 'Internal Sources':

	Name
1	file1
2	RADIUS-AAI
3	IDP-AAI-LDAP
4	IDP-AAI



The screenshot shows the PacketFence web interface. The top navigation bar includes STATUS, REPORTS, AUDITING, NODES, USERS, and CONFIGURATION (highlighted with a red circle). The user is logged in as ADMIN. The main content area displays the configuration for an LDAP source named "IDP-AAI-LDAP".

IDP-AAI-LDAP LDAP

Name * IDP-AAI-LDAP

Description * IDP-AAI-LDAP

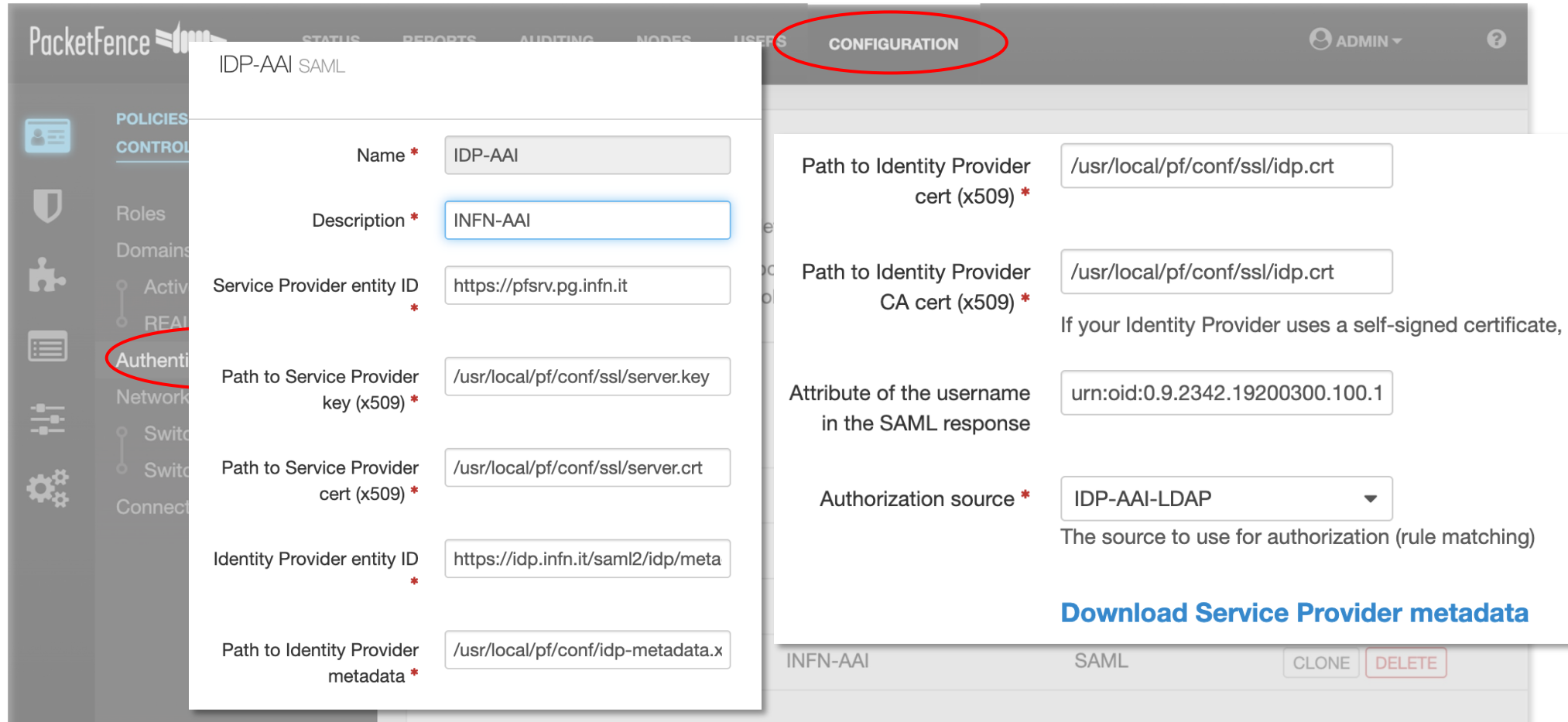
Host ds1.pg.infn.it : 389 Start TLS

Internal Sources

	Name
1	file1
2	RADIUS-AAI
3	IDP-AAI-LDAP
4	IDP-AAI

Configuration Fields:

- Base DN * ou=people,dc=infn,dc=it
- Scope * One-level
- Username Attribute * uid
Main reference attribute that contain the username
- Search Attributes Click to select an attribute
Other attributes that can be used as the username (requires to restart the radiusd service to be effective)
- Email attribute mail
LDAP attribute name that stores the email address against which the filter will match.
- Bind DN cn=daemon,dc=pg,dc=infn,dc=it
Leave this field empty if you want to perform an anonymous bind.
- Password * [masked] TEST



The screenshot displays the PacketFence configuration interface. The 'CONFIGURATION' tab is selected and circled in red. The 'Authentications' menu item in the left sidebar is also circled in red. A modal window titled 'IDP-AAI SAML' is open, showing the following configuration fields:

- Name: IDP-AAI
- Description: INFN-AAI
- Service Provider entity ID: https://pfsrv.pg.infn.it
- Path to Service Provider key (x509): /usr/local/pf/conf/ssl/server.key
- Path to Service Provider cert (x509): /usr/local/pf/conf/ssl/server.crt
- Identity Provider entity ID: https://idp.infn.it/saml2/idp/meta
- Path to Identity Provider metadata: /usr/local/pf/conf/idp-metadata.x

The main configuration page shows the following fields:

- Path to Identity Provider cert (x509): /usr/local/pf/conf/ssl/idp.crt
- Path to Identity Provider CA cert (x509): /usr/local/pf/conf/ssl/idp.crt
- Attribute of the username in the SAML response: urn:oid:0.9.2342.19200300.100.1
- Authorization source: IDP-AAI-LDAP

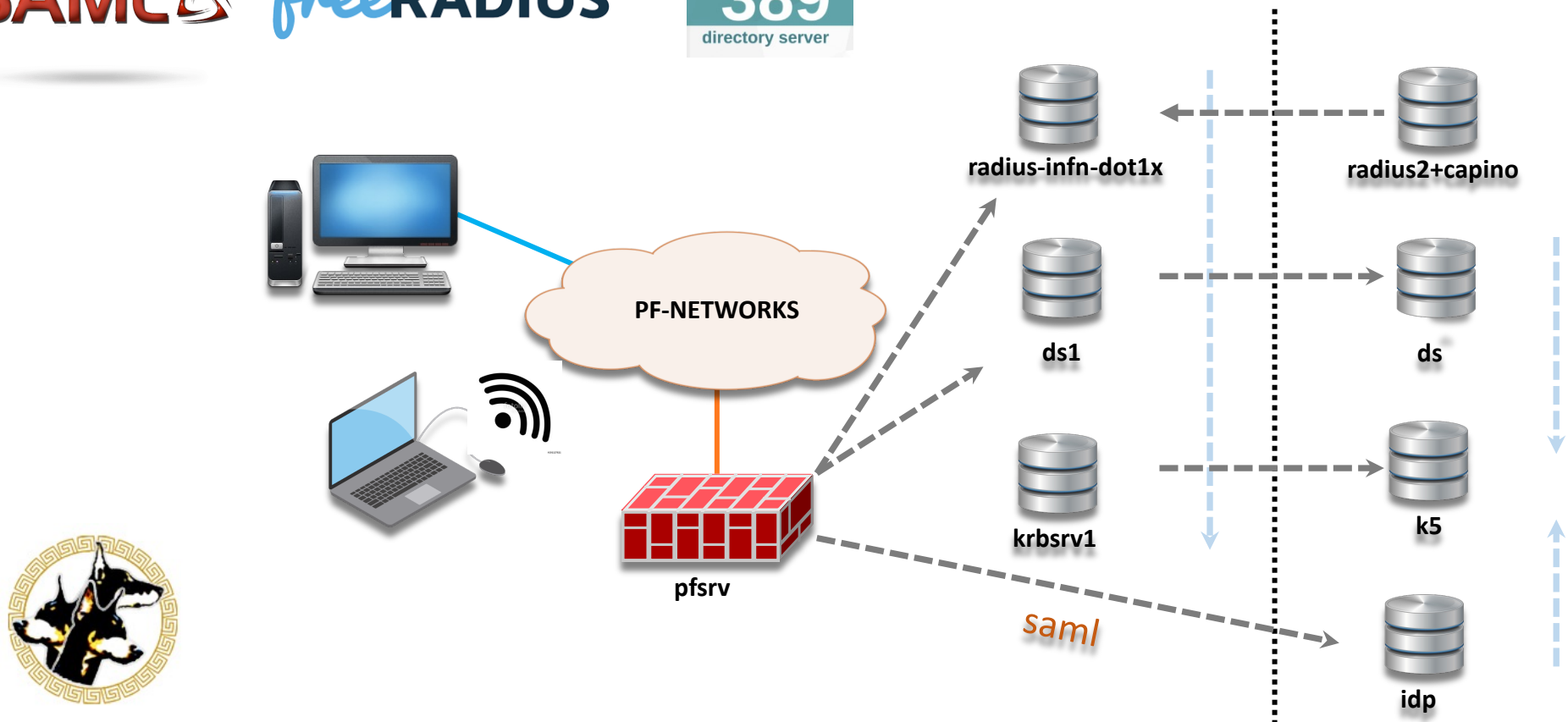
Additional text: 'If your Identity Provider uses a self-signed certificate, ...' and 'The source to use for authorization (rule matching)'. A blue link 'Download Service Provider metadata' is visible. At the bottom, there are buttons for 'CLONE' and 'DELETE'.

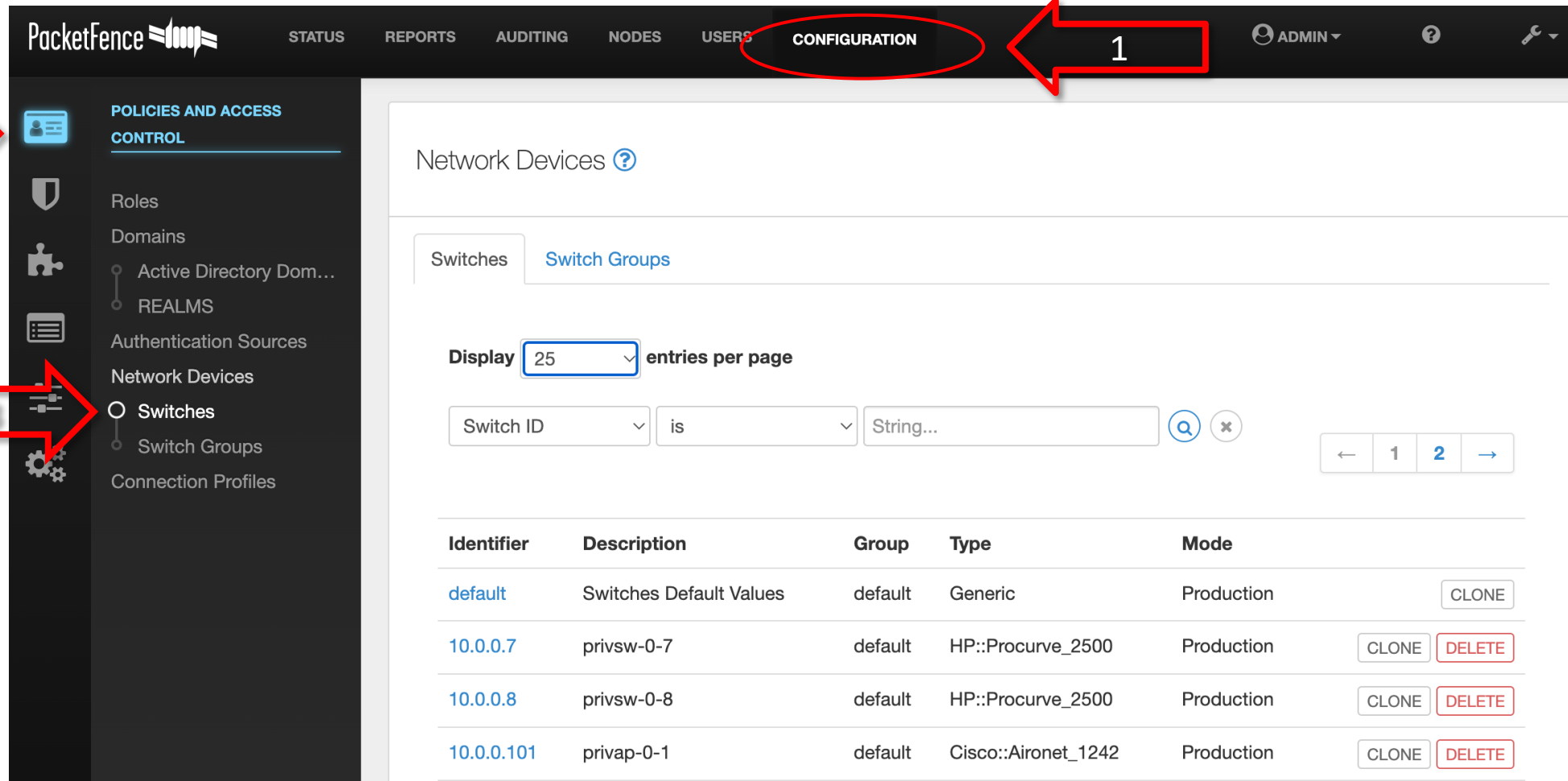
SAML  **freeRADIUS**

389
directory server

sistemi locali

sistemi remoti





The screenshot shows the PacketFence web interface. The top navigation bar includes STATUS, REPORTS, AUDITING, NODES, USERS, and CONFIGURATION (highlighted with a red circle and arrow labeled '1'). The left sidebar contains a menu with 'POLICIES AND ACCESS CONTROL' and 'Network Devices' (highlighted with a red arrow labeled '2'). Under 'Network Devices', 'Switches' is selected (highlighted with a red arrow labeled '3'). The main content area displays 'Network Devices' with tabs for 'Switches' and 'Switch Groups'. It includes a 'Display 25 entries per page' dropdown, a search bar with 'Switch ID is String...', and a table of network devices.

Identifier	Description	Group	Type	Mode
default	Switches Default Values	default	Generic	Production CLONE
10.0.0.7	privsw-0-7	default	HP::Procurve_2500	Production CLONE DELETE
10.0.0.8	privsw-0-8	default	HP::Procurve_2500	Production CLONE DELETE
10.0.0.101	privap-0-1	default	Cisco::Aironet_1242	Production CLONE DELETE



CCR Tutorial Days 10-12 ottobre @ LNF



Switch 10.0.0.7

ADMIN

Switch 10.0.0.7

Definition Roles Inline RADIUS SNMP CLI Web Services

Description

Type HP ProCurve 2500 Series x

Mode Default (production)

Switch Group None

Deauthentication Method RADIUS x

Use CoA

CLI Access Enabled

External Portal Enforcement

ROLE MAPPING BY VLAN ID

Role by VLAN ID

registration	<input type="text" value="29"/>
isolation	<input type="text" value="28"/>
macDetection	<input type="text" value="4"/>
inline	<input type="text" value="6"/>
default	<input type="text" value="25"/>
guest	<input type="text"/>
gaming	<input type="text"/>
voice	<input type="text" value="5"/>
REJECT	<input type="text" value="-1"/>

Switch 10.0.0.7

Definition Roles Inline RADIUS SNMP CLI Web Services

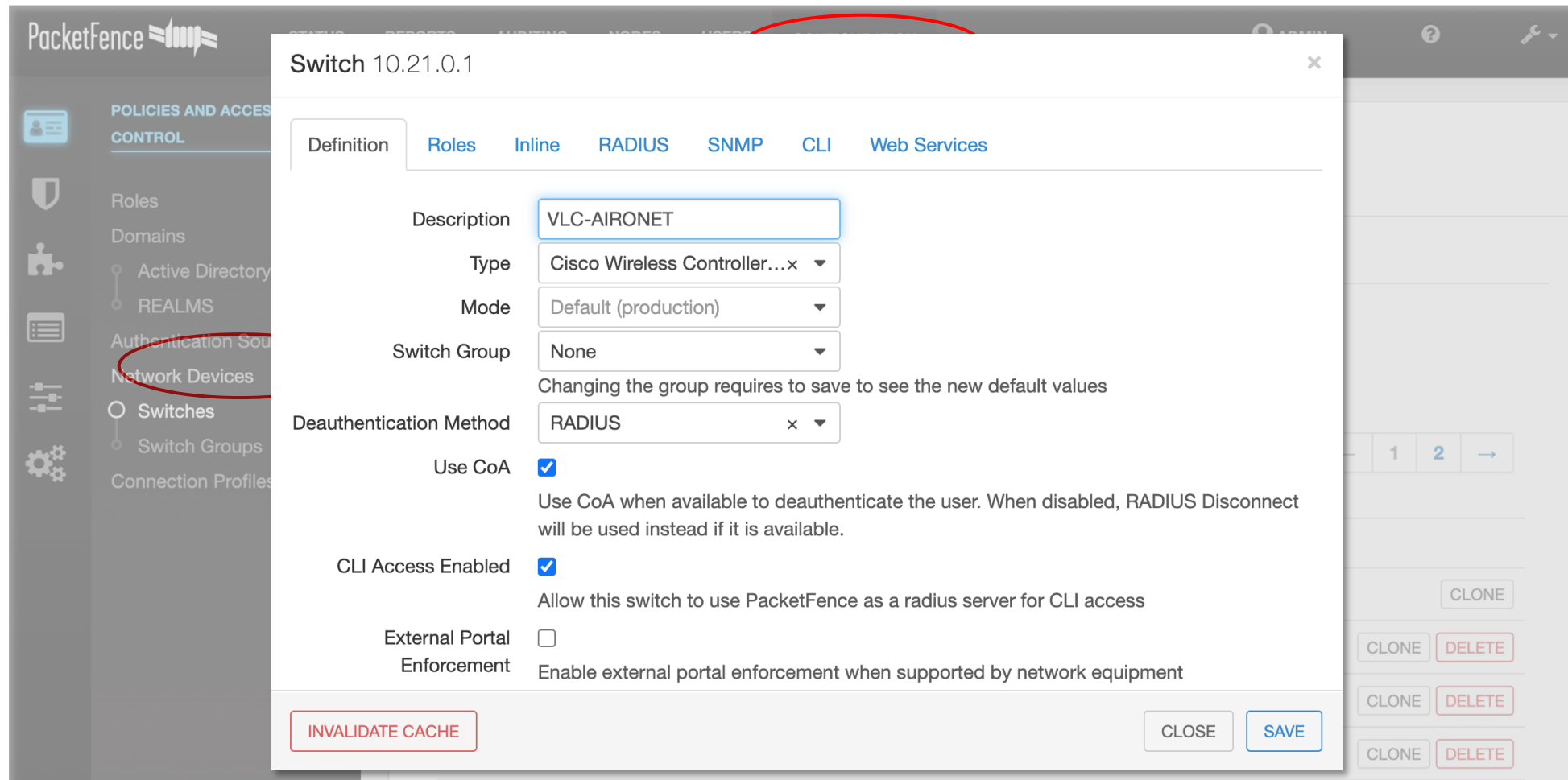
Secret Passphrase

INVALIDATE CACHE

INVALIDATE CACHE

INVALIDATE CACHE

CLOSE SAVE



The screenshot displays the PacketFence web interface. On the left, a sidebar menu shows 'Network Devices' and 'Switches' highlighted. The main content area shows the configuration for a switch named 'Switch 10.21.0.1'. The configuration is organized into tabs: Definition, Roles, Inline, RADIUS, SNMP, CLI, and Web Services. The 'Definition' tab is active, showing the following settings:


- Description: VLC-AIRONET
- Type: Cisco Wireless Controller...x
- Mode: Default (production)
- Switch Group: None
- Deauthentication Method: RADIUS
- Use CoA:
- CLI Access Enabled:
- External Portal Enforcement:

At the bottom of the configuration window, there are buttons for 'INVALIDATE CACHE', 'CLOSE', and 'SAVE'. The background interface shows a list of switches with 'CLONE' and 'DELETE' buttons for each.



CCR Tutorial Days 10-12 ottobre @ LNF



PacketFence  STATUS REPORTS AUDITING NODES USERS **CONFIGURATION** ADMIN ?

2 POLICIES AND ACCESS CONTROL

- Roles
- Domains
 - Active Directory Dom...
 - REALMS
- Authentication Sources
- Network Devices
 - Switches
 - Switch Groups
- 3** Connection Profiles

Connection Profiles and Pages ?

Present a different captive portal according to the SSID, the VLAN, or the switch IP the client connects to.

	Status	Name	Description	
	●	default	Default Profile	PREVIEW
2	●	INFN-WIRED	INFN-WIRED	CLONE DELETE PREVIEW
3	●	INFN-dot1x	INFN-dot1x	CLONE DELETE PREVIEW
4	●	INFN-web	INFN-web	CLONE DELETE PREVIEW
5	●	INFN-embedded	INFN-embedded	CLONE DELETE PREVIEW

ADD PROFILE



CCR Tutorial Days 10-12 ottobre @ LNF



The screenshot displays the PacketFence configuration interface. The top navigation bar includes STATUS, REPORTS, AUDITING, NODES, USERS, and CONFIGURATION. The main content area is divided into several sections:

- Settings:** Includes tabs for Settings, Captive Portal, and Files. A PREVIEW button is visible.
- Profile Name:** Set to INFN-WIRED. A note states: "A profile id can only contain alphanumeric characters, dashes, period and or underscores."
- Profile Description:** Set to INFN-WIRED.
- Enable profile:** Checked.
- Root Portal Module:** Set to Default portal policy. A note states: "The Root Portal Module to use".
- Activate preregistration:** Unchecked. A note states: "This activates preregistration on the connection profile. Meaning, instead of applying the access to the currently connected device, it displays a local account that is created while registering. Note that activating this disables the on-site registration on this connection profile. Also, make sure the sources on the connection profile have 'Create local account' enabled."
- Automatically register devices:** Checked. A note states: "This activates automatic registration of devices for the profile. Devices will not be shown a captive portal and RADIUS authentication credentials will be used to register the device. This option only makes sense in the context of an 802.1x authentication."

Below the settings, there are three configuration sections:

- Filters:** "If all of the following conditions are met:"
 - 1 Connection Type: Ethernet-EAP
- Sources:** 1 RADIUS-AAI
- Scanners:** 1 Openvas-wired

An ADD PROFILE button is located at the bottom of the interface.

- INFN-wired (out-of-band)





CCR Tutorial Days 10-12 ottobre @ LNF



PacketFence STATUS REPORTS AUDITING NODES USERS CONFIGURATION ADMIN

Connection Profiles and Pages > INFN-dot1x

Settings **Captive Portal** Files PREVIEW

Profile Name *
A profile id can only contain alphanumeric characters, dashes, period and or underscores.

Profile Description

Enable profile

Root Portal Module *
The Root Portal Module to use

Activate preregistration
This activates preregistration on the connection profile. Meaning, instead of applying the access to the currently connected device, it displays a local account that is created while registering. Note that activating this disables the on-site registration on this connection profile. Also, make sure the sources on the connection profile have "Create local account" enabled.

Automatically register devices
This activates automatic registration of devices for the profile. Devices will not be shown a captive portal and RADIUS authentication credentials will be used to register the device. This option only makes sense in the context of an 802.1x authentication.

ADD PROFILE

Filters If of the following conditions are met:

1	SSID	<input type="text" value="INFN-dot1x"/>
---	------	---

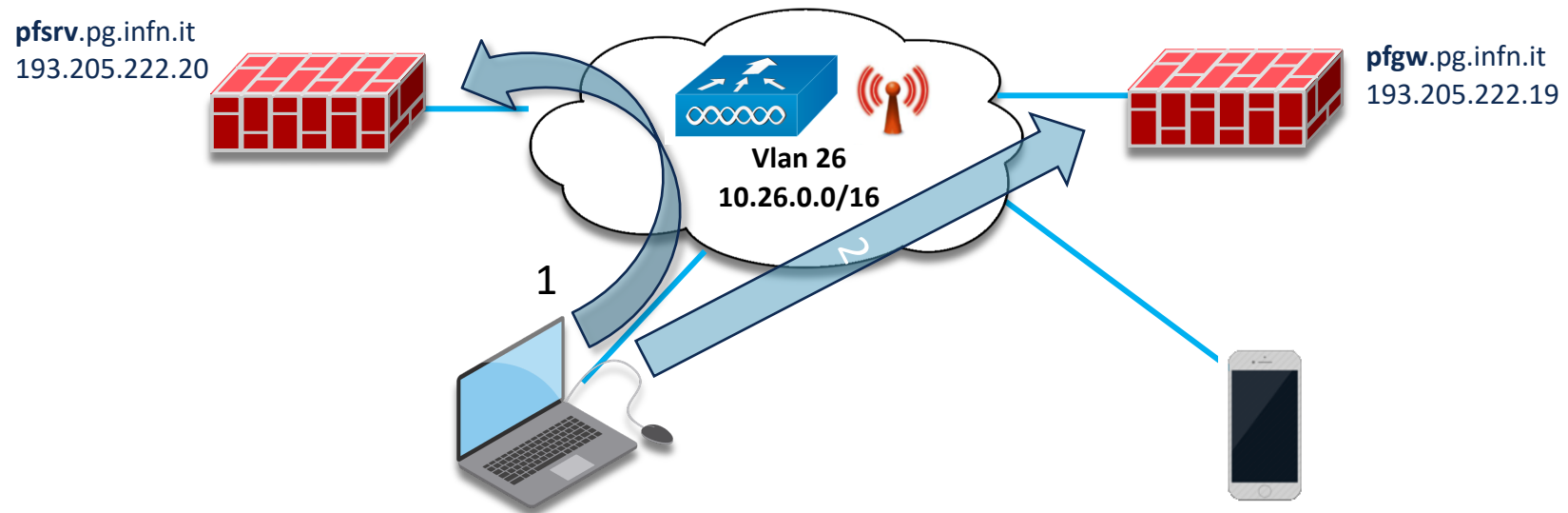
Description

Sources 1

INFN-web CLONE DELETE PREVIEW

Scanners 1

- INFN-dot1x (out-of-band)





CCR Tutorial Days 10-12 ottobre @ LNF



PacketFence STATUS REPORTS AUDITING NODES USERS CONFIGURATION ADMIN

Connection Profiles and Pages > INFN-web

Settings **Captive Portal** Files PREVIEW

Profile Name *
A profile id can only contain alphanumeric characters, dashes, period and or underscores.

Profile Description

Enable profile

Root Portal Module *
The Root Portal Module to use

Activate preregistration
This activates preregistration on the connection profile. Meaning, instead of applying the access to the currently connected device, it displays a local account that is created while registering. Note that activating this disables the on-site registration on this connection profile. Also, make sure the sources on the connection profile have "Create local account" enabled.

Automatically register devices
This activates automatic registration of devices for the profile. Devices will not be shown a captive portal and RADIUS authentication credentials will be used to register the device. This option only makes sense in the context of an 802.1x authentication.

ADD PROFILE

Filters If of the following conditions are met:

1	VLAN	<input type="text" value="27"/>
---	------	---------------------------------

Description

Default Profile PREVIEW

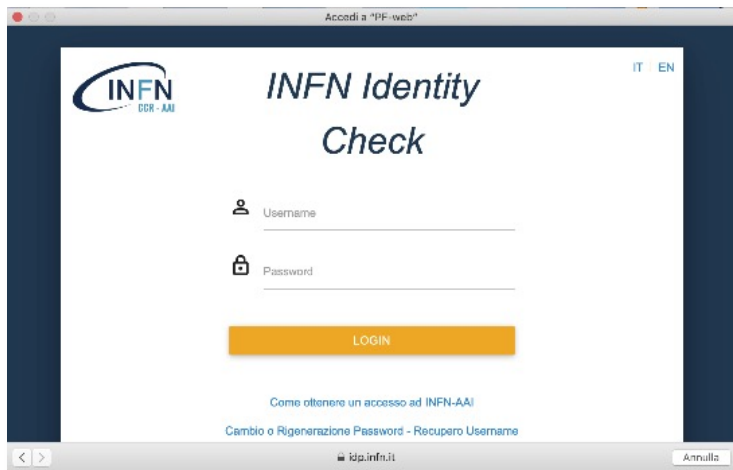
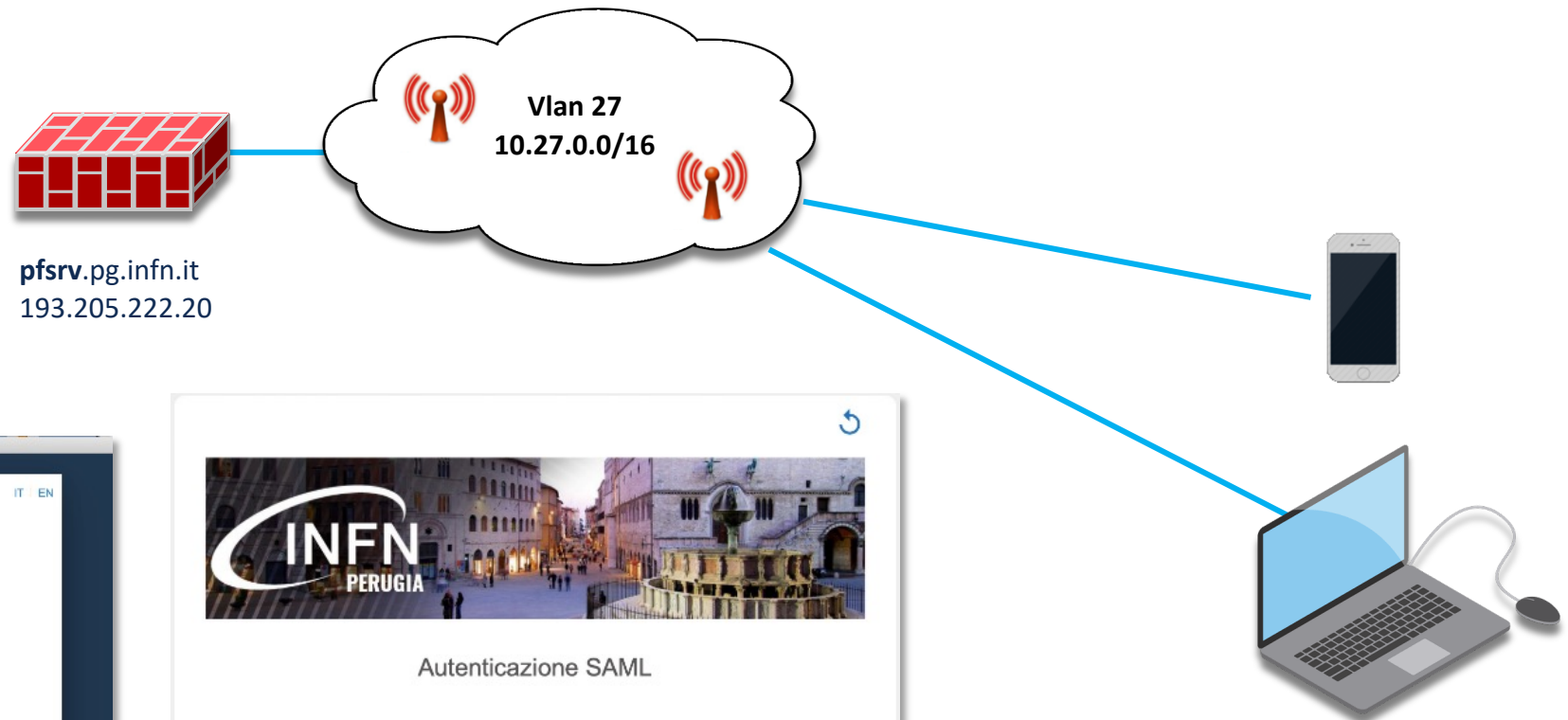
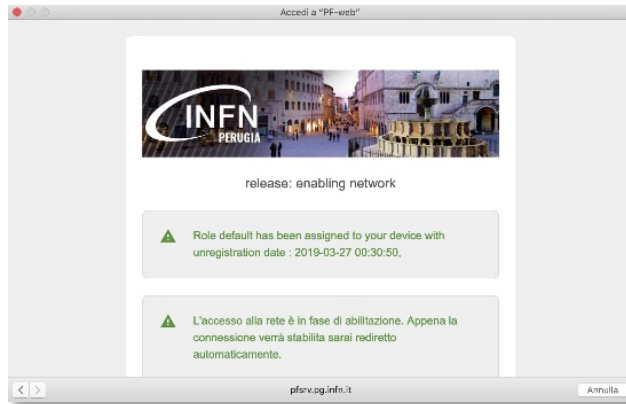
Sources 1

INFN-web CLONE DELETE PREVIEW

INFN-embedded CLONE DELETE PREVIEW

Scanners 1

- INFN-web (inline)





CCR Tutorial Days 10-12 ottobre @ LNF



Connection Profiles and Pages > INFN-embedded

Settings Captive Portal Files PREVIEW

Profile Name * INFN-embedded
A profile id can only contain alphanumeric characters, dashes, period and or underscores.

Profile Description INFN-embedded

Enable profile

Root Portal Module * Default portal policy
The Root Portal Module to use

Activate preregistration
This activates preregistration on the connection profile. Meaning, instead of applying the acc currently connected device, it displays a local account that is created while registering. Note this disables the on-site registration on this connection profile. Also, make sure the sources c connection profile have "Create local account" enabled.

Filters If any of the following conditions are met:
1 VLAN 30

Sources
With no source specified, the sources of the default profile will be used. [Add a source.](#)

Billing Tiers
With no billing tiers specified, all billing tiers will be used. [Add a billing tier.](#)

Provisioners
With no provisioners specified, the provisioners of the default profile will be used. [Add a provisioner.](#)

Scanners
With no scan specified, the scan engine will not be triggered. [Add a Scan.](#)

ADD PROFILE

- INFN-embedded (PF)



Status - Network Access

I tuoi dispositivi registrati

OS Type **Mac OS X or macOS**
 Computer name **becchetti-nb** This is your current device.
 MAC **a4:5e:60:c1:80:c3**
 Registered on **2019-03-26 12:30:50**

[Registra un altro dispositivo](#)

[Logout](#)



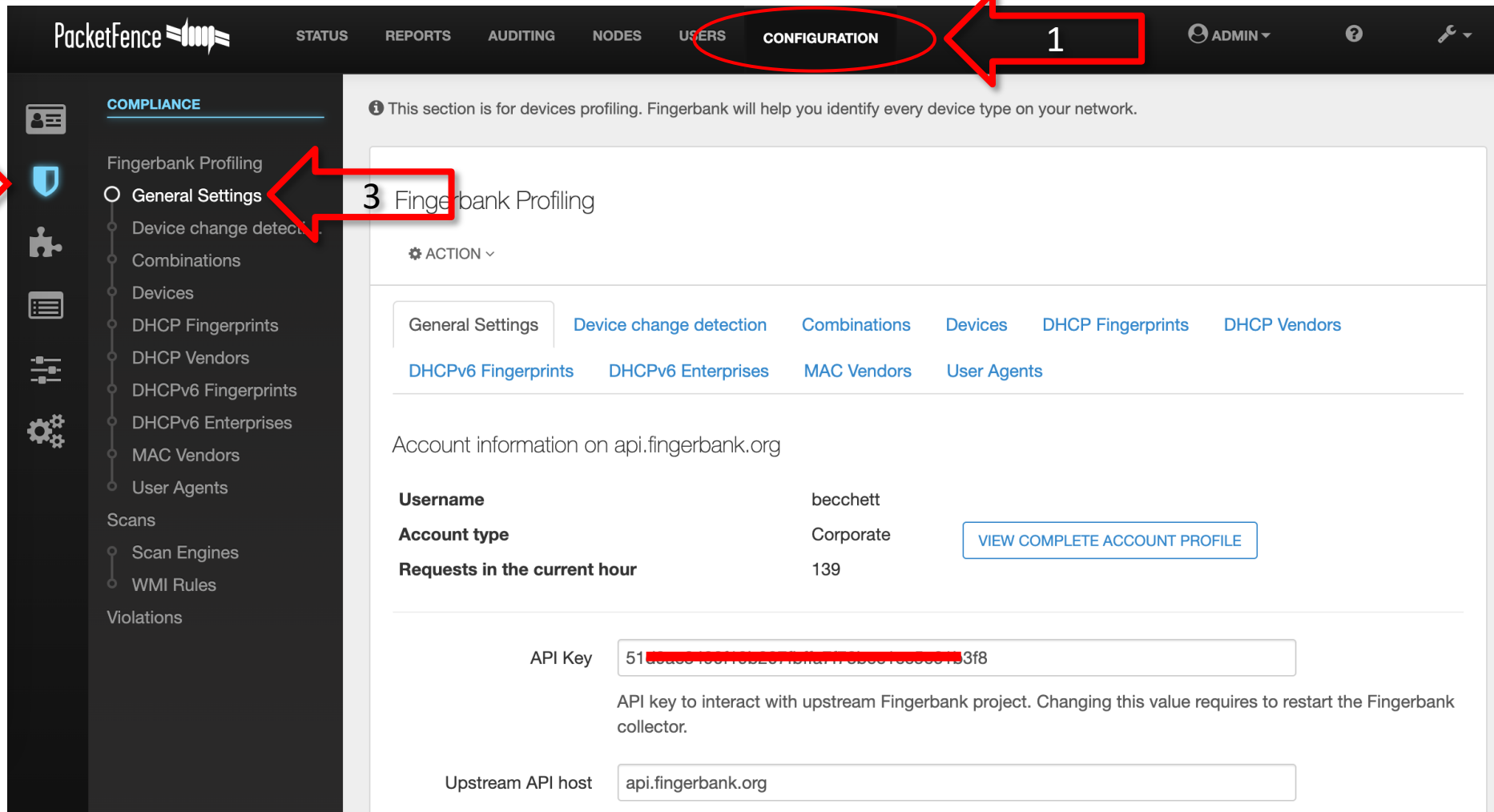
Registrazione

INDIRIZZO MAC DEL DISPOSITIVO

[Registrazione](#)

[Return to device list](#)

[Logout](#)



The screenshot shows the PacketFence web interface. The top navigation bar includes STATUS, REPORTS, AUDITING, NODES, USERS, and CONFIGURATION. The CONFIGURATION menu item is circled in red and labeled with a red arrow and the number '1'. On the left sidebar, the 'COMPLIANCE' section is expanded, and 'Fingerbank Profiling' is selected, indicated by a red arrow and the number '2'. Within the Fingerbank Profiling menu, 'General Settings' is highlighted with a red arrow and the number '3'. The main content area displays the 'Fingerbank Profiling' configuration page. It features a breadcrumb trail: General Settings > Device change detection > Combinations > Devices > DHCP Fingerprints > DHCP Vendors > DHCPv6 Fingerprints > DHCPv6 Enterprises > MAC Vendors > User Agents. The 'General Settings' tab is active. The page contains account information for api.fingerbank.org, including Username (becchett), Account type (Corporate), and Requests in the current hour (139). There is a button labeled 'VIEW COMPLETE ACCOUNT PROFILE'. Below this, there is a field for 'API Key' with a value partially obscured by a red line, and a field for 'Upstream API host' with the value 'api.fingerbank.org'.

PacketFence

STATUS REPORTS AUDITING NODES USERS **CONFIGURATION** ADMIN ?

COMPLIANCE

- Fingerbank Profiling
- General Settings
- Device change detection
- Combinations
- Devices
- DHCP Fingerprints
- DHCP Vendors
- DHCPv6 Fingerprints
- DHCPv6 Enterprises
- MAC Vendors
- User Agents
- Scans
- Scan Engines
- WMI Rules
- Violations

Fingerbank Profiling

ACTION

General Settings Device change detection Combinations Devices DHCP Fingerprints DHCP Vendors

DHCPv6 Fingerprints DHCPv6 Enterprises MAC Vendors User Agents

Account information on api.fingerbank.org

Username	becchett	
Account type	Corporate	VIEW COMPLETE ACCOUNT PROFILE
Requests in the current hour	139	

API Key 51[REDACTED]3f8


API key to interact with upstream Fingerbank project. Changing this value requires to restart the Fingerbank collector.

Upstream API host api.fingerbank.org


PacketFence

Integrazione Openvas/Greenbone

- VM Centos 8, 8GB, 4 core, 30GB HDD, GVM 21.4.3
- Scansione ad ogni accesso in rete
- Profilo «INFN PG Packetfence», categorie con gravi vulnerabilità
- Tempi di scansione -> 4-10 minuti
- Rete cablata -> scansioni di tutti i dispositivi
- Rete wifi -> scansione di MacOSX, Windows e Linux
- Report via mail (pdf)
- nessun accesso da remoto (ssh o altro)



Greenbone
Security Assistant



Dashboards
Help

Alerts 3 of 3

Name ▲

- mail
- mail severity 7
- packetfence

(Applied filter: sort=name first=1 rows=1)

Edit Alert packetfence
✕

Name

Comment

Event Task run status changed to ▼

New ▼ ▼

Ticket Received Assigned Ticket Changed Owned Ticket Changed

Always

Severity at least ▲▼

Condition Severity Level ▼

Filter ▼ matches at least ▲▼ result(s) NVT(s)

Filter ▼ matches at least ▲▼ result(s) more than previous scan

Report Content Compose

None

Previous completed report of the same task

Report with ID

Method ▼

To Address

From Address

Subject

Cancel
Save

1 - 3 of 3

Active	Actions
✖	✎ ⏪ ⏩ ↻
✖	✎ ⏪ ⏩ ↻
✖	✎ ⏪ ⏩ ↻

1 - 3 of 3



CCR Tutorial Days 10-12 ottobre @ LNF



Scan Config: INFN PG Packetfence

ID: c7bb13c3

Information	Scanner Preferences (0)	NVT Families (18)	NVT Preferences (1117)	User Tags (0)	Permissions (0)
-------------	----------------------------	-----------------------------	---------------------------	------------------	--------------------

Family	NVTs selected
Brute force attacks	9 of 9
Buffer overflow	1 of 617
Compliance	14 of 15
Databases	848 of 897
Default Accounts	293 of 296
Denial of Service	1899 of 1961
Gain a shell remotely	108 of 108
General	18 of 6703
Port scanners	9 of 9
Remote file access	56 of 56
RPC	4 of 4
Service detection	1 of 251
SNMP	12 of 12
SSL and TLS	78 of 78
Useless services	15 of 16
Web application abuses	7523 of 8068
Web Servers	763 of 787
Windows : Microsoft Bulletins	2915 of 3013



Greenbone Security Assistant

Dashboards

Scans




Report Format: PDF

Information	Parameters (0)	User Tags (0)	Permissions (2)
-------------	-------------------	------------------	--------------------

Extension	pdf
Content Type	application/pdf
Trust	Yes (02/22/2022)
Active	Yes
Summary	Portable Document Format report. Version 20220831.
Alerts using this Report Format	mail mail severity 7 packetfence

Description

Scan results in Portable Document Format (PDF). Version 20220831.

PacketFence  STATUS

COMPLIANCE

- Fingerbank Profiling
 - General Settings
 - Device change detection
 - Combinations
 - Devices
 - DHCP Fingerprints
 - DHCP Vendors
 - DHCPv6 Fingerprints
 - DHCPv6 Enterprises
 - MAC Vendors
 - User Agents
 - Scans**
 - Scan Engines
 - WMI Rules
 - Violations

Scan Engine Openvas-wired OpenVAS

Hostname or IP Address

Username

Password

Port of the service

If you use an alternative alert ID

Alert ID

ID of the alert configuration

Scan config ID

ID of the scanning engine

Report format ID

ID of the "CSV Report"

Roles

Nodes with the selected roles will be affected

Scan Engine OpenVAS OpenVAS

Roles

Nodes with the selected roles will be affected

OS

Nodes with the selected OS will be affected

Duration

Approximate duration of a scan. User being scanned on registration are presented a progress bar for this duration, afterwards the browser refreshes until scan is complete.

Scan before registration

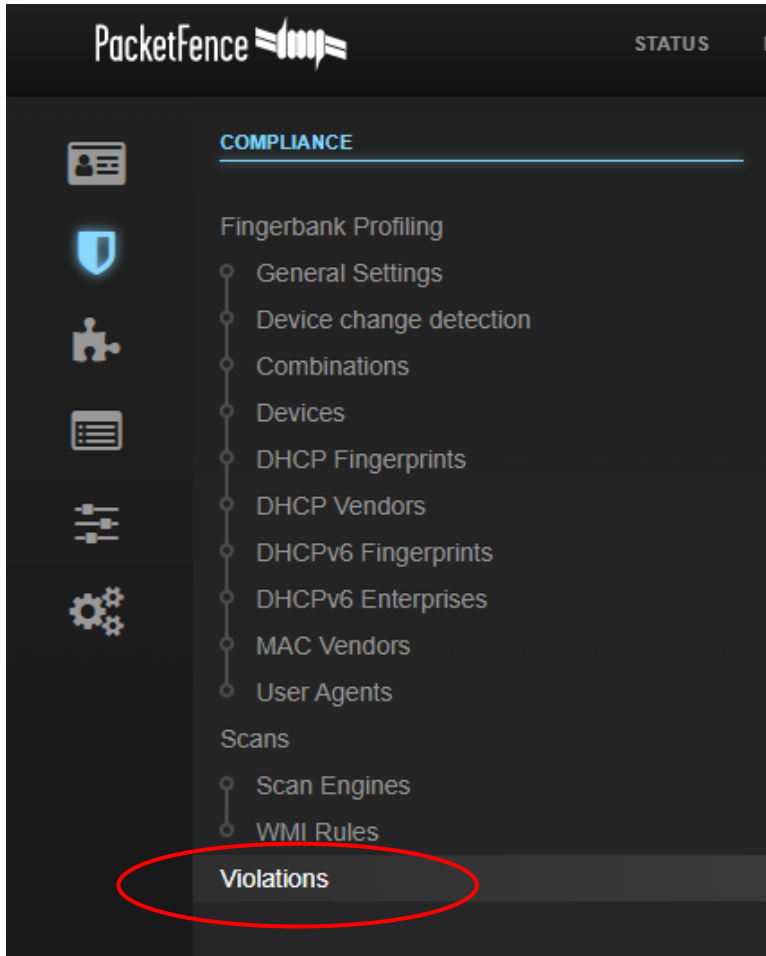
If this option is enabled, the PF system will scan host before the registration.

Scan on registration

If this option is enabled, the PF system will scan each host after registration is complete.

Scan after registration

If this option is enabled, the PF system will scan host after on the production vlan.



PacketFence STATUS

COMPLIANCE

- Fingerbank Profiling
 - General Settings
 - Device change detection
 - Combinations
 - Devices
 - DHCP Fingerprints
 - DHCP Vendors
 - DHCPv6 Fingerprints
 - DHCPv6 Enterprises
 - MAC Vendors
 - User Agents
- Scans
 - Scan Engines
 - WMI Rules
 - Violations**

Violations ?

	Id	Description	Actions
	defaults		Email violation to administrator Log violation
<input type="checkbox"/> OFF	1100001	Nessus Scan	Change network access on violation Email violation to administrator Log violation
<input checked="" type="checkbox"/> ON	1100002	OpenVAS scan (EB)	Email violation to administrator Log violation
<input type="checkbox"/> OFF	1100003	MAC Vendor isolation example	Change network access on violation Email violation to administrator Log violation
<input type="checkbox"/> OFF	1100004	Ancient OS isolation example	Change network access on violation Email violation to administrator Log violation

Violation OpenVAS scan (EB)

Definition **Triggers** Remediation Advanced

Enabled ON

Description

Actions

Priority

Range 1-10, with 1 the highest priority and 10 the lowest. Higher priority violations will be addressed first if a host has more than one.

Whitelisted Roles

Nodes with the selected roles won't be affected by a violation of this type.

PacketFence


Integrazione IDS Suricata

- Virtual machine
- Controllo flussi di traffico
- Identificazione P2P e TOR
- Notifica tramite mail



IDS Server

- Macchina virtuale CentOS 7, 4 core, 8GB Ram, 30GB HDD, 2 schede di rete (management e controllo traffico);
- Suricata 6.0.4 , installato dai sorgenti;
- Regole per P2P e TOR aggiornate tramite cron;
- Log inviati al server Packetfence tramite syslog e memorizzati su file system;
- VM in esecuzione nello stesso hypervisor di Packetfence e Gateway reti nascoste

PacketFence  STATUS

INTEGRATION

- Firewall SSO
- Cisco Mobility Services Engine
- Web Services
- Syslog Parsers**
- Syslog Forwarding
- WRIX

Syslog Parsers

Warning! Any change to the syslog parsers requires a restart of the pfdetect and pfqueue services.

Detector	Type	Status
Suricata	suricata	enabled

ADD SYSLOG PARSER ▾


Syslog parser Suricata

Enabled

Alert pipe *

CANCEL

SAVE

PacketFence  STATUS R

COMPLIANCE

- Fingerbank Profiling
 - General Settings
 - Device change detection
 - Combinations
 - Devices
 - DHCP Fingerprints
 - DHCP Vendors
 - DHCPv6 Fingerprints
 - DHCPv6 Enterprises
 - MAC Vendors
 - User Agents
- Scans
 - Scan Engines
 - WMI Rules
- Violations**

ON 1500001 IDS P2P Email violation to user Email violation to administrator Log violation

Violation IDS P2P

Definition Triggers Remediation Advanced

Enabled ON

Description

Actions

Additional message for the user


A message that will be added to the e-mail sent to the user regarding this violation.

Priority

Violation IDS P2P

Definition Triggers Remediation Advanced

-
-
-
-
-
-

PacketFence  STATUS R

COMPLIANCE

- Fingerbank Profiling
 - General Settings
 - Device change detection
 - Combinations
 - Devices
 - DHCP Fingerprints
 - DHCP Vendors
 - DHCPv6 Fingerprints
 - DHCPv6 Enterprises
 - MAC Vendors
 - User Agents
- Scans
 - Scan Engines
 - WMI Rules
 - Violations**

ON 1500003 IDS TOR

[Email violation to user](#) [Email violation to administrator](#) [Log violation](#)

Violation IDS TOR

Definition **Triggers** Remediation Advanced

Enabled ON

Description

Actions

Additional message for the user

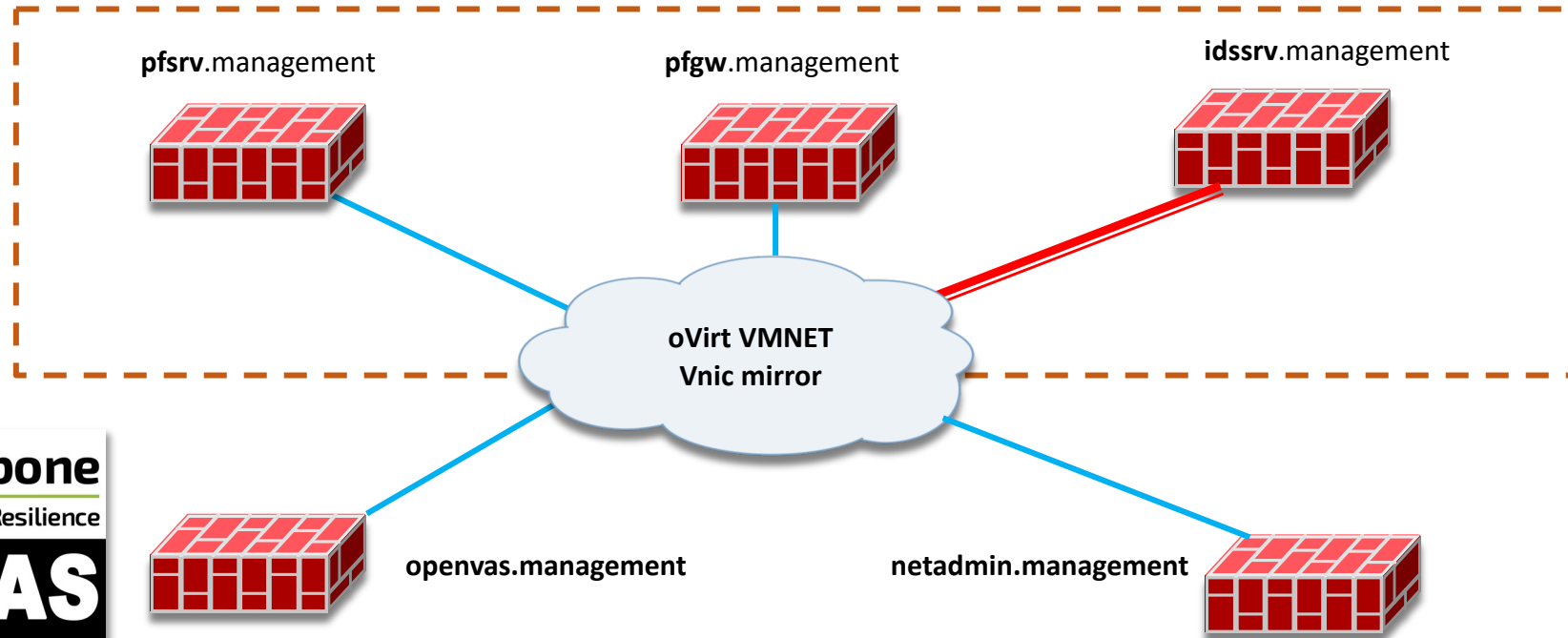
A message that will be added to the e-mail sent to the user regarding this violation.

Priority

Violation IDS TOR

Definition **Triggers** Remediation Advanced

-
-



OPENVAS
Openvas + greenbone -> High Risk: email to admin.

IDSSRV
Suricata. Net Flow Analyzer -> PFSRV

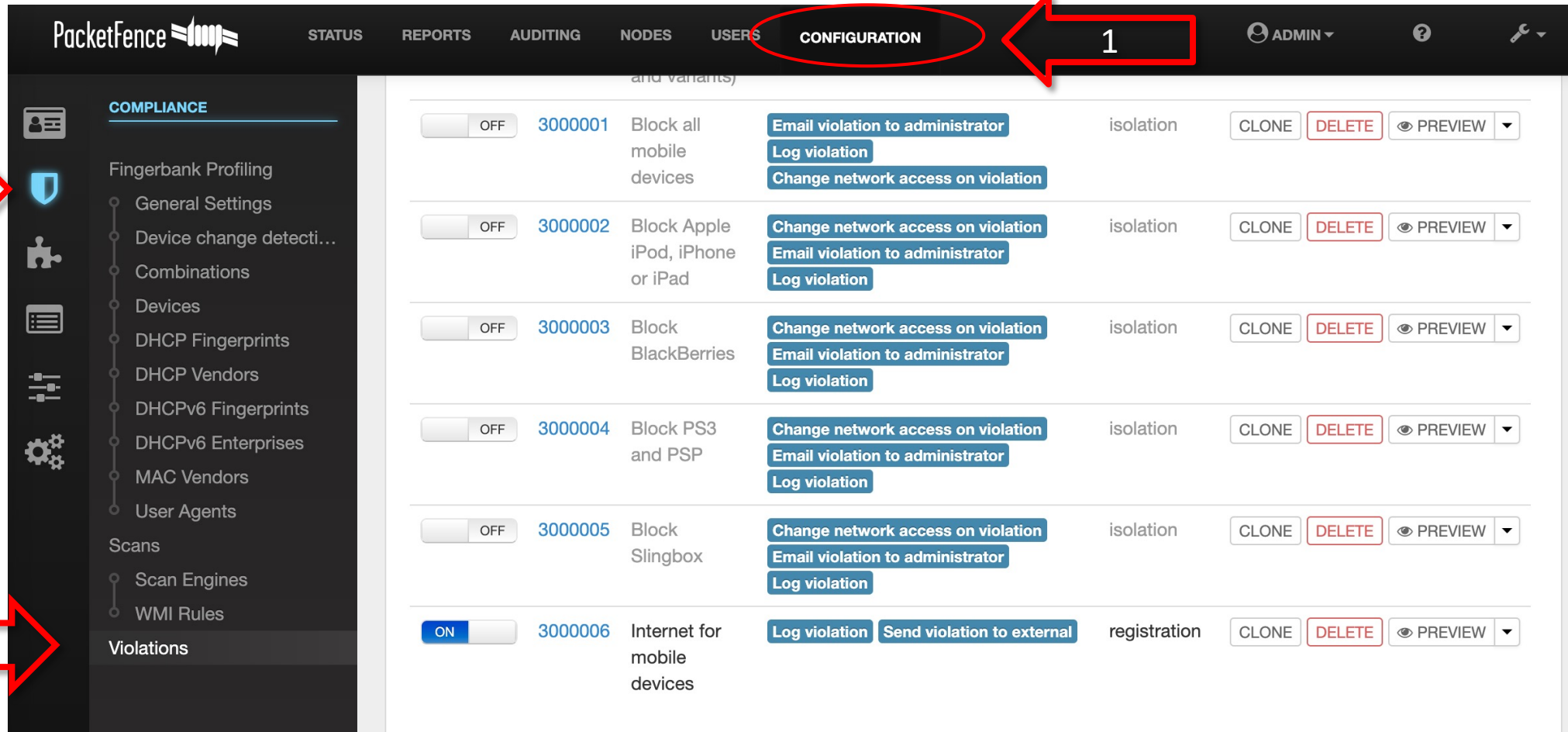
PFSRV
Parsing da IDSSRV -> Violation (P2P/TOR): Email to admin, log violation.



CCR Tutorial Days 10-12 ottobre @ LNF



Smartphone/Tablet



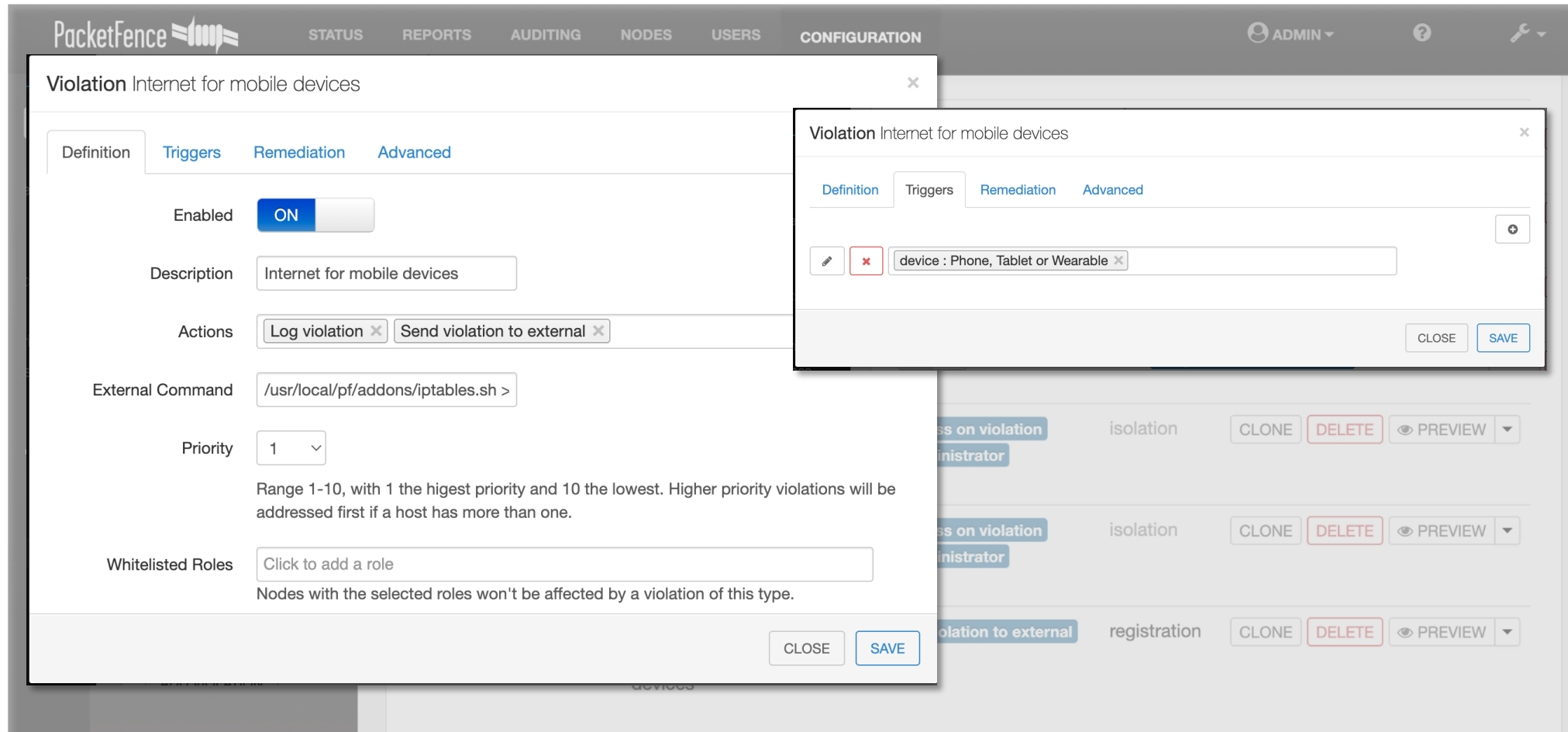
The screenshot shows the PacketFence web interface. The top navigation bar includes STATUS, REPORTS, AUDITING, NODES, USERS, and CONFIGURATION (highlighted with a red circle and arrow labeled '1'). The left sidebar shows the COMPLIANCE section with various sub-items, and 'Violations' is highlighted with a red arrow labeled '3'. The main content area displays a list of configuration rules. Each rule has a status toggle, a rule ID, a description, a list of actions, a status, and control buttons (CLONE, DELETE, PREVIEW).

Status	Rule ID	Description	Actions	Status	Controls
OFF	3000001	Block all mobile devices	Email violation to administrator Log violation Change network access on violation	isolation	CLONE DELETE PREVIEW
OFF	3000002	Block Apple iPod, iPhone or iPad	Change network access on violation Email violation to administrator Log violation	isolation	CLONE DELETE PREVIEW
OFF	3000003	Block BlackBerries	Change network access on violation Email violation to administrator Log violation	isolation	CLONE DELETE PREVIEW
OFF	3000004	Block PS3 and PSP	Change network access on violation Email violation to administrator Log violation	isolation	CLONE DELETE PREVIEW
OFF	3000005	Block Slingbox	Change network access on violation Email violation to administrator Log violation	isolation	CLONE DELETE PREVIEW
ON	3000006	Internet for mobile devices	Log violation Send violation to external	registration	CLONE DELETE PREVIEW

2

1

3



The screenshot displays the PacketFence configuration interface for a violation rule titled "Violation Internet for mobile devices". The interface is divided into several sections:

- Definition:** Includes tabs for "Definition", "Triggers", "Remediation", and "Advanced".
- Enabled:** A toggle switch set to "ON".
- Description:** A text input field containing "Internet for mobile devices".
- Actions:** A list of actions including "Log violation" and "Send violation to external".
- External Command:** A text input field containing "/usr/local/pf/addons/iptables.sh >".
- Priority:** A dropdown menu set to "1". Below it, a note states: "Range 1-10, with 1 the highest priority and 10 the lowest. Higher priority violations will be addressed first if a host has more than one."
- Whitelisted Roles:** A text input field with the placeholder "Click to add a role". Below it, a note states: "Nodes with the selected roles won't be affected by a violation of this type."

Two modal windows are overlaid on the main configuration page:

- The top modal window shows the "Triggers" tab, where a trigger is defined as "device : Phone, Tablet or Wearable". It includes "CLOSE" and "SAVE" buttons.
- The bottom modal window shows the "Remediation" tab, which is currently empty. It also includes "CLOSE" and "SAVE" buttons.

In the background, a table lists existing violation rules with columns for name, description, and actions (CLONE, DELETE, PREVIEW).

Client con Autenticazione 802.1x per rete cablata: Linux, MacOSx e Windows

The image displays three overlapping screenshots illustrating network configuration steps:

- Linux (Ubuntu):** Shows the 'Impostazioni' (Settings) application with the 'Rete' (Network) section open. The 'Cavo' (Ethernet) tab is selected, and the 'Sicurezza' (Security) sub-tab is active. The 'Sicurezza 802.1x' toggle is turned ON. The authentication method is set to 'TLS con tunnel'. The identity is 'username@pg.infn.it' and the internal authentication is 'PAP'.
- Windows:** Shows the 'Proprietà - Ethernet' (Ethernet Properties) dialog box. The 'Autenticazione' (Authentication) tab is selected. The 'Abilita autenticazione IEEE 802.1X' checkbox is checked. The authentication method is set to 'Microsoft: EAP-TTLS'. The 'Memorizza credenziali per la connessione a ogni accesso' (Save credentials for connection to every access) checkbox is also checked.
- macOS:** Shows the 'Ethernet Thunderbolt' configuration window. The '802.1X' tab is selected. A list of profiles is shown, with 'Wi-Fi (INFN-dot1x)' selected. The 'Abilita connessione automatica' (Enable automatic connection) checkbox is checked.

Overlaid on the Windows dialog is the 'Proprietà TTL' (TTL Properties) dialog box. It has the 'Consenti privacy identità' (Allow privacy identity) checkbox checked and the identity field set to 'username@pg.infn.it'. Under 'Autorità di certificazione radice attendibili' (Trusted root certification authorities), several DigiCert roots are checked. Under 'Autenticazione client' (Client authentication), the 'Seleziona un metodo non EAP per l'autenticazione' (Select a non-EAP method for authentication) radio button is selected, with 'Password Authentication Protocol (PAP)' chosen in the dropdown menu.



CCR Tutorial Days 10-12 ottobre @ LNF




Dashboard



CCR Tutorial Days 10-12 ottobre @ LNF



PacketFence 

STATUS REPORTS AUDITING NODES USERS CONFIGURATION ADMIN

OVERVIEW

Dashboard

- System
 - RADIUS
 - Authentication
 - DHCP
 - Endpoints
 - Portal
 - Queue
- Services

QUEUE


Local Queue

PFSRV system - softnet_stat **130.7 events**

System RADIUS Authentication DHCP Endpoints Portal Queue

pfsrv - uptime 240 days 02:16:50

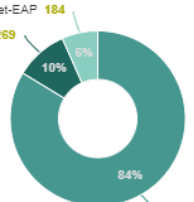
REGISTERED DEVICES PER ROLE DEVICES



100% default 63

gio 22 set 2022 12:43:32 to 12:45:33, 2 mins and 1 sec


CONNECTED DEVICES PER CONNECTION TYPE DEVICES



Ethernet-EAP 184 6%
Wireless-802.11-EAP 269 10%
Inline 2,323 84%

gio 22 set 2022 12:43:32 to 12:45:33, 2 mins and 1 sec

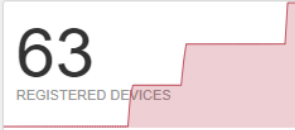
CONNECTED DEVICES PER SSID DEVICES



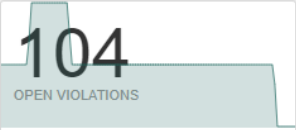
100% INFN-dot1x 236

gio 22 set 2022 12:43:32 to 12:45:33, 2 mins and 1 sec

63 REGISTERED DEVICES




104 OPEN VIOLATIONS





CCR Tutorial Days 10-12 ottobre @ LNF



PacketFence 

STATUS REPORTS AUDITING **NODES** USERS CONFIGURATION ADMIN ?

NODES

Search

Create

STANDARD SEARCHES

Open Violations

Closed Violations

Offline Nodes

Online Nodes

Switch Groups

Roles

OS

SAVED SEARCHES

Simple **Advanced**

Display 25 entries per page

Node MAC is String...

RESET SEARCH SEARCH

Results

ACTION COLUMNS


← 1 2 ... →

<input type="checkbox"/>	Status	Online/Offline	MAC Address	Computer Name	Owner	IP Address	Tenant	Device Class	Role
<input type="checkbox"/>	registered	off	00:0e:c6:af:71:f7	morozzi	morozzi@pg.infn.it	10.25.128.44	default	Windows OS	default
<input type="checkbox"/>	registered	on	00:13:3b:a9:fb:fd	LAPTOP-HA6B86VO	mencheri@pg.infn.it	10.25.128.146	default	Windows OS	default
<input type="checkbox"/>	registered	on	00:25:ab:a4:99:28	Gentile-AIO-h	gentile@pg.infn.it	10.25.128.195	default	Windows OS	default
<input type="checkbox"/>	registered	off	00:50:b6:8b:8c:29	RedMac	alvesi@pg.infn.it	10.25.128.133	default	Operating System	default
<input type="checkbox"/>	registered	on	00:e0:4c:68:0f:d0	MBP-di-Gabriele	gabriele@pg.infn.it	10.25.128.113	default	Mac OS X or macOS	default
<input type="checkbox"/>	registered	unknown	06:a0:48:82:c0:4f		aberratt@pg.infn.it	10.26.1.238	default	Operating System	default
<input type="checkbox"/>	registered	off	10:dd:b1:ad:e3:18	Gians-iMac	bilei@pg.infn.it	10.25.128.241	default	Mac OS X or macOS	default
<input type="checkbox"/>	registered	unknown	14:4f:8a:bc:59:5d	PC-1R0-242	rvoipo	10.27.122.217	default	Linux OS	default
<input type="checkbox"/>	registered	unknown	14:7d:da:30:fd:eb		gsivestri@pg.infn.it	10.27.107.231	default	IOS	default
<input type="checkbox"/>	registered	unknown	14:7d:da:e0:1d:f0	MBP-di-Patrizia	costa@pg.infn.it	10.26.2.14	default	Mac OS X or macOS	default
<input type="checkbox"/>	registered	on	14:b3:1f:0d:23:b6	famesini-aio	famesini@pg.infn.it	10.25.128.188	default	Windows OS	default



CCR Tutorial Days 10-12 ottobre @ LNF



PacketFence 

STATUS REPORTS AUDITING NODES **USERS** CONFIGURATION ADMIN ?

USERS

Search
Create
SAVED SEARCHES

Simple **Advanced**

Display entries per page

[RESET SEARCH](#) [SEARCH](#)

Results

ACTION

<input type="checkbox"/>	Username	Firstname	Lastname	Email	Telephone	# nodes
<input type="checkbox"/>	becchett	Enrico	Becchetti	enrico.becchetti@pg.infn.it		9
<input type="checkbox"/>	becchett@pg.infn.it	Enrico	Becchetti	enrico.becchetti@pg.infn.it		25



CCR Tutorial Days 10-12 ottobre @ LNF



The screenshot shows the PacketFence web interface. A modal window titled "User becchett@pg.infn.it" is open, displaying a table of associated devices. The table has columns for Status, MAC, Computer Name, and Device class. The background interface shows a search for "becchett" with results for "becchett" and "becchett@pg.infn.it".

Status	MAC	Computer Name	Device class
unregistered	00:0c:29:02:4e:fd	debian	Linux OS
unregistered	00:0c:29:41:9c:b7	DESKTOP-T2ABI3U	Windows OS
unregistered	00:16:cb:07:1b:d9	macbook	Mac OS X or macOS
unregistered	00:16:cb:86:4f:d1	macbook	Mac OS X or macOS
unregistered	00:50:b6:7b:32:52	Notebook-INFNPG	Windows OS
registered	2c:4d:54:3a:c9:eb	android-84b8390813b167f	Android OS
unregistered	34:64:a9:2f:8a:dc	STG-pg	Windows OS
unregistered	50:3e:aa:db:cd:f2	becchetti-nb	Operating System
unregistered	58:96:1d:d1:86:f2	LAPTOP-HRHSGPGJ	Windows OS
unregistered	70:54:d2:bc:be:91	INFN-GUEST-PC01	Windows OS
unregistered	70:8b:cd:21:3a:4a	android-64ef9cf6f1c205ed	Phone, Tablet or Wearable



CCR Tutorial Days 10-12 ottobre @ LNF



The screenshot shows the PacketFence web interface. A modal window is open for the MAC address 50:3e:aa:db:cd:f2. The modal displays the following information:

- Device Manufacturer: TP-LINK TECHNOLOGIES CO.,LTD.
- Device Class: Operating System
- Device Type: Apple OS
- Fully Qualified Device Name: Operating System/Apple OS
- Score: 73
- Mobile:
- DHCP Fingerprint: 1,121,3,6,15,108,114,119,252,95,44,46
- DHCP Vendor:
- DHCPv6 Fingerprint:
- DHCPv6 Enterprise:

At the bottom of the modal, there are three buttons: REEVALUATE ACCESS, REFRESH DEVICE PROFILING, and RESTART SWITCHPORT. There are also CLOSE and SAVE buttons.

The background interface shows the 'USERS' section with a search bar containing 'becchett'. The 'Results' section shows a table with columns 'Telephone' and '# nodes'. The table has two rows: one with '9' nodes and another with '25' nodes.



CCR Tutorial Days 10-12 ottobre @ LNF



The screenshot shows the PacketFence web interface. A search for the user 'becchett' is performed, resulting in two entries. A modal window is open for the MAC address 50:3e:aa:db:cd:f2, displaying connection details for the IP address 10.0.3.8. The modal window includes tabs for Info, Fingerbank, IPv4 Address, IPv6 Address, Location, Violations, WMI Rules, Option82, and Rapid7. The 'Info' tab is active, showing a table of connections. The first connection is highlighted with a red circle, and its details are shown below the table. At the bottom of the modal, there are buttons for 'REEVALUATE ACCESS', 'REFRESH DEVICE PROFILING', and 'RESTART SWITCHPORT', along with 'CLOSE' and 'SAVE' buttons.

Switch/AP	Switch Mac	Connection Type	Connection Sub Type	Username	Start	End
10.0.3.8	38:21:c7:17:38:50	Wired 802.1x	21	becchett@pg.infn.it	2022-03-09 10:43:40	0000-00-00 00:00:00


Port: 7 (7)
Role: default
VLAN: 25


REEVALUATE ACCESS REFRESH DEVICE PROFILING RESTART SWITCHPORT CLOSE SAVE



CCR Tutorial Days 10-12 ottobre @ LNF



PacketFence 

STATUS REPORTS **AUDITING** NODES USERS CONFIGURATION ADMIN ? 

RADIUS AUDIT LOG

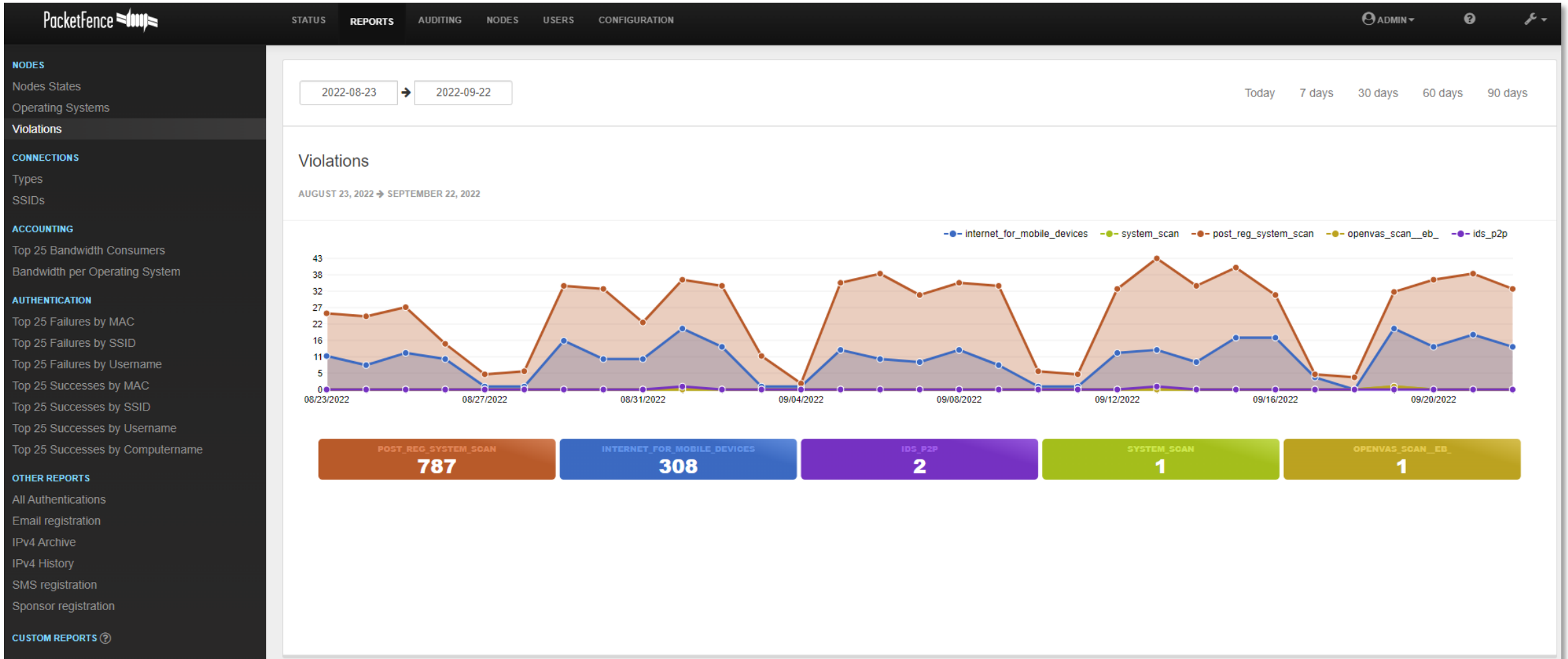
- Switch Groups
- Roles
- Status
- Sources
- Realms
- Profiles
- Domains

SAVED SEARCHES

Auth Status	MAC Address	Node status	request_time	User Name	IP Address	Create at	NAS IP Address	NAS Port Type
+ Accept	b8:27:eb:d6:e2:45	reg	4	caprai@pg.infn.it		2022-09-29 14:46:27	10.21.0.1	Wireless-802.11
+ Accept	58:6c:25:ee:45:62	reg	2	sangoni@pg.infn.it		2022-09-29 14:46:18	10.21.0.1	Wireless-802.11
+ Accept	38:f9:d3:e7:f4:5f	reg	1	ambrosi@pg.infn.it		2022-09-29 14:46:08	10.21.0.1	Wireless-802.11
+ Reject	1a:8b:c9:ad:ae:cd	N/A	0	piccini		2022-09-29 14:45:32	10.21.0.1	Wireless-802.11
+ Reject	1a:8b:c9:ad:ae:cd	N/A	0	piccini		2022-09-29 14:45:32	10.21.0.1	Wireless-802.11
+ Accept	88:40:3b:a2:cc:99	reg	2	gentile@pg.infn.it		2022-09-29 14:45:23	10.21.0.1	Wireless-802.11
+ Accept	88:40:3b:a2:cc:99	reg	2	gentile@pg.infn.it		2022-09-29 14:45:13	10.21.0.1	Wireless-802.11
+ Reject	1a:8b:c9:ad:ae:cd	N/A	0	piccini		2022-09-29 14:45:00	10.21.0.1	Wireless-802.11
+ Reject	1a:8b:c9:ad:ae:cd	N/A	0	piccini		2022-09-29 14:45:00	10.21.0.1	Wireless-802.11
+ Accept	14:10:9f:d4:10:17	reg	2	pauluzzi		2022-09-29 14:44:51	10.21.0.1	Wireless-802.11
+ Accept	ce:fa:b2:23:99:5b	reg	2	pepe@pg.infn.it		2022-09-29	10.21.0.1	Wireless-




CCR Tutorial Days 10-12 ottobre @ LNF





CCR Tutorial Days 10-12 ottobre @ LNF



PacketFence 

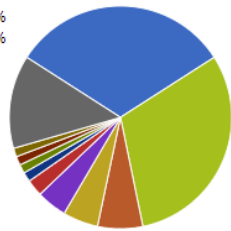
STATUS REPORTS AUDITING NODES USERS CONFIGURATION ADMIN

2022-08-23 → 2022-09-22 Today 7 days 30 days 60 days 90 days

Top Bandwidth Consumers

AUGUST 23, 2022 → SEPTEMBER 22, 2022

[Total](#) | [Input](#) | [Output](#)



- 00:4e:01:a6:dd:87 - 31.88%
- a0:29:19:a6:a0:98 - 30.83%
- 10.26.2.140 - 6.55%
- bc:5f:f4:5b:07:b4 - 5.13%
- 10:dd:b1:ad:b6:ea - 4.41%
- 00:e0:4c:68:0f:d0 - 2.44%
- 3c:a6:f6:68:00:81 - 1.38%
- 10.27.122.217 - 1.29%
- 10.26.1.206 - 1.28%
- 10.26.1.69 - 1.25%
- Others

MAC Address	Total
00:4e:01:a6:dd:87	575.65 GB
a0:29:19:a6:a0:98	556.69 GB
10.26.2.140	118.34 GB
bc:5f:f4:5b:07:b4	92.72 GB
10:dd:b1:ad:b6:ea	79.68 GB
00:e0:4c:68:0f:d0	44.10 GB
3c:a6:f6:68:00:81	25.00 GB
10.27.122.217	23.21 GB
10.26.1.206	23.18 GB
10.26.1.69	22.60 GB
10:dd:b1:ad:e3:18	22.47 GB
a4:bb:6d:54:e7:78	21.51 GB
10.26.1.83	20.84 GB
4c:e1:73:42:34:56	19.59 GB
00:13:3b:a9:fb:fd	18.14 GB
74:46:a0:b9:fe:ef	17.26 GB

NODES
Nodes States
Operating Systems
Violations

CONNECTIONS
Types
SSIDs

ACCOUNTING
Top 25 Bandwidth Consumers
Bandwidth per Operating System

AUTHENTICATION
Top 25 Failures by MAC
Top 25 Failures by SSID
Top 25 Failures by Username
Top 25 Successes by MAC
Top 25 Successes by SSID
Top 25 Successes by Username
Top 25 Successes by Computername

OTHER REPORTS
All Authentications
Email registration
IPv4 Archive
IPv4 History
SMS registration
Sponsor registration

CUSTOM REPORTS



Conclusioni

- Realizzazione delle 4 reti: INFN-web, INFN-dot1x, INFN-wired e INFN-embedded
- Compatibilità con TRIP
- Dispositivi attivi e log degli accessi
- Associazione dispositivo utente tramite username
- Controllo degli accessi con autenticazione 802.1x per la rete cablata
- Controllo con Greenbone
- Controllo con Suricata per la segnalazione nel caso di traffico P2P e TOR



CCR Tutorial Days 10-12 ottobre @ LNF



Grazie !



CCR Tutorial Days 10-12 ottobre @ LNF




Backup slide




Personalizzazioni & Addon

- Modificato sorgente perl *util.pm* per problema scheda di rete eth0+vlan
- Modificato sorgente perl *openvas.pm* per problema con ultima release di greenbone
- Script PHP per importare dati da INFN AAI (Nome, Cognome, Mail, Sede)
- Script Bash per limitare l'accesso alla rete locale dai dispositivi «smart»


8

CONFIGURATION WIZARD

1 — 2 — 3 — 4

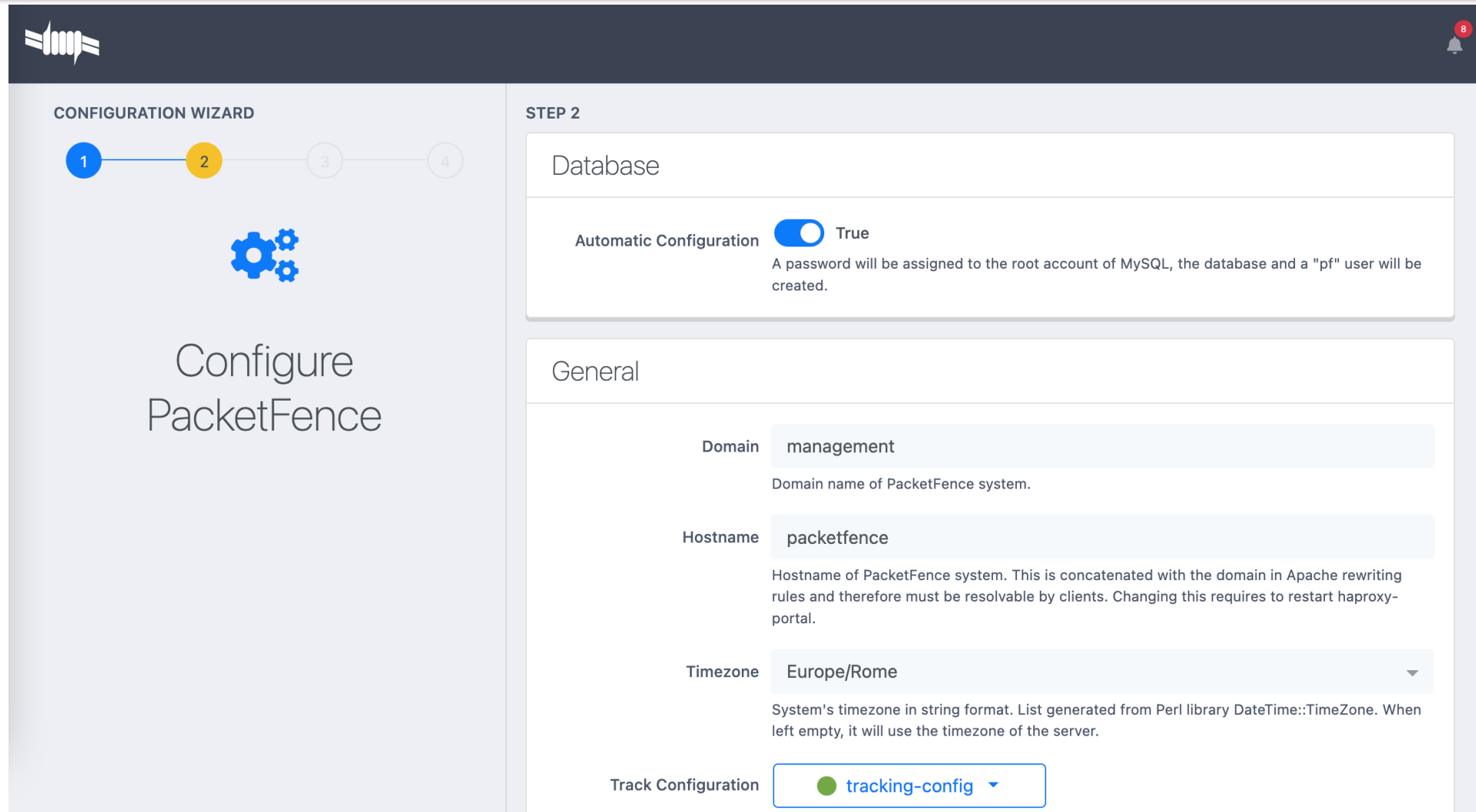


Configure Network

STEP 1

Interfaces & Networks

Status	Logical Name	IP Address	Default Network	Type	
🔒 Up	eth0	10.0.198.199 /255.255.0.0	10.0.0.0	management	New VLAN
✅ Up	eth0 VLAN 25	10.25.0.248 /255.255.0.0	10.25.0.0	other dhcp-listener portal	Delete Clone
✅ Up	eth0 VLAN 26	10.26.0.248 /255.255.0.0	10.26.0.0	other	Delete Clone
✅ Up	eth0 VLAN 27	10.27.0.248 /255.255.0.0	10.27.0.0	inlinel2	Delete Clone
✅ Up	eth0 VLAN 28	10.28.0.248 /255.255.0.0	10.28.0.0	vlan-isolation	Delete Clone
✅ Up	eth0 VLAN 29	10.29.0.248 /255.255.0.0	10.29.0.0	vlan- registration	Delete Clone



The screenshot shows the PacketFence configuration wizard interface. On the left, a sidebar titled "CONFIGURATION WIZARD" features a progress indicator with four steps: 1 (blue), 2 (yellow), 3 (grey), and 4 (grey). Below the progress indicator is a gear icon and the text "Configure PacketFence". The main content area is titled "STEP 2" and is divided into two sections: "Database" and "General".

Database

Automatic Configuration True
A password will be assigned to the root account of MySQL, the database and a "pf" user will be created.

General

Domain: management
Domain name of PacketFence system.

Hostname: packetfence
Hostname of PacketFence system. This is concatenated with the domain in Apache rewriting rules and therefore must be resolvable by clients. Changing this requires to restart haproxy-portal.

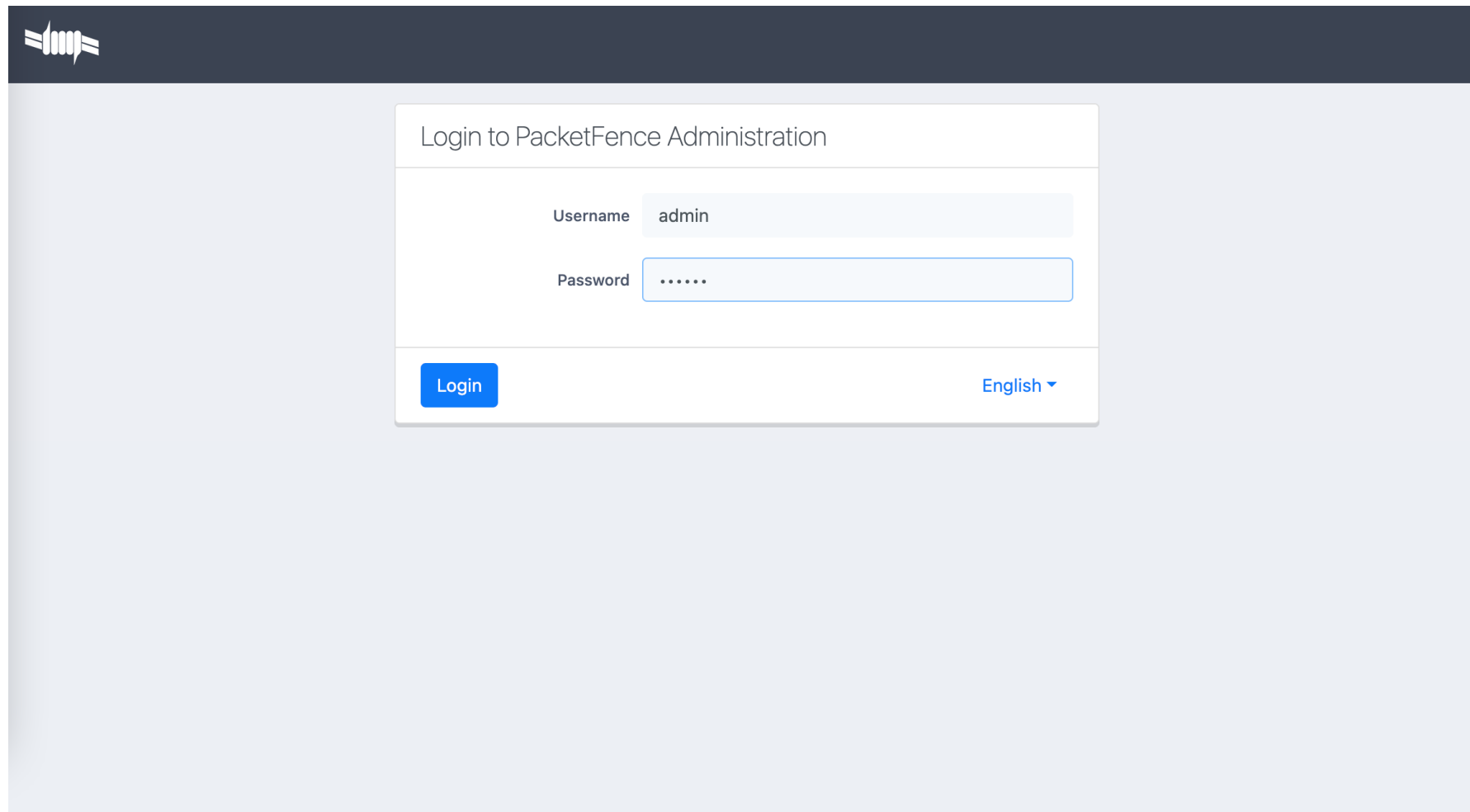
Timezone: Europe/Rome
System's timezone in string format. List generated from Perl library DateTime::TimeZone. When left empty, it will use the timezone of the server.

Track Configuration: tracking-config



CCR Tutorial Days 10-12 ottobre @ LNF

Packetfence vers. 12.0 – Accesso web



The screenshot shows the PacketFence Administration login interface. At the top left, there is a dark blue header with a white icon of a server rack. Below the header, the main content area is light gray. In the center, there is a white login form with a title "Login to PacketFence Administration". The form contains two input fields: "Username" with the value "admin" and "Password" with masked characters ".....". Below the password field is a blue "Login" button. To the right of the button is a language selection dropdown menu showing "English" with a downward arrow.



CCR Tutorial Days 10-12 ottobre @ LNF

Packetfence vers. 12.0 – Configurazione



The screenshot shows the PacketFence web interface. The top navigation bar includes 'Status', 'Reports', 'Auditing', 'Nodes', 'Users', and 'Configuration'. The user is logged in as 'admin'. The left sidebar contains a search filter and a list of configuration categories: Policies and Access Control, Compliance, Integration, Advanced Access Configuration, Network Configuration, and System Configuration. The main content area is titled 'Policies and Access Control' and contains the following text:

When an endpoint connects to the network, PacketFence must be able to assign a role to it, or its user. The role can then be translated to a VLAN, a set of ACL, a switch manufacturer policy identifier or a combinations of all of this.

For PacketFence to work properly, you must define in the following order:

- Roles:** A role will allow PacketFence to grant different network access to endpoints connecting to your network. For example, employee vs. guest.
- Domains:** If you want to authenticate users or machines using a Active Directory Domain Controller (DC), you have to join the PacketFence server to the DC.
- Sources:** Authentication sources will allow you to identify users and assign them roles and access durations.
- Switches:** PacketFence manages switches, access points and WiFi controllers. You have to add the equipment you want PacketFence to manage and do the role by VLAN/ACL/policy identifier mapping.
- Connection Profiles:** When devices are connecting to your network, you might want to show a captive portal or auto-register the device. You can control the behavior in this module.



CCR Tutorial Days 10-12 ottobre @ LNF

Packetfence vers. 12.0 – Server di autenticazione



The screenshot shows the Packetfence Configuration interface. The top navigation bar includes Status, Reports, Auditing, Nodes, Users, and Configuration. The user is logged in as 'admin'. The left sidebar shows the 'Authentication Sources' menu item selected. A dropdown menu for 'New internal source' is open, listing various authentication methods, with 'RADIUS' highlighted. The main content area displays a table of existing authentication sources.

Type	Description	
Htpasswd	Legacy Source	Delete Clone
SMS	SMS-based registration	Delete Clone
Email	Email-based registration	Delete Clone
Sponsor	Sponsor-based registration	Delete Clone



CCR Tutorial Days 10-12 ottobre @ LNF

Packetfence vers. 12.0 – Profili di rete



The screenshot displays the Packetfence web interface. The top navigation bar includes 'Status', 'Reports', 'Auditing', 'Nodes', 'Users', and 'Configuration'. The user is logged in as 'admin'. The left sidebar shows a menu with 'Policies and Access Control' expanded, listing 'Roles', 'Domains', 'Realms', 'Authentication Sources', 'Network Devices', and 'Switch Groups'. The 'Connection Profiles' section is highlighted in blue. The main content area shows 'Connection Profiles' with a search bar, a 'New Connection Profile' button, and a table of profiles. The table has columns for 'Status', 'MAC', and 'Description'. A single profile is listed with 'Status' set to 'Enabled' and 'Description' as 'Default Profile'. There are 'Preview' and 'Clone' buttons for this profile.

Status	MAC	Description
Enabled	default	Default Profile



CCR Tutorial Days 10-12 ottobre @ LNF

Packetfence vers. 12.0 – Profilo per INFN-wired 1/2



The screenshot shows the PacketFence configuration interface. The top navigation bar includes 'Status', 'Reports', 'Auditing', 'Nodes', 'Users', and 'Configuration'. The user is logged in as 'admin'. The left sidebar shows a navigation menu with categories like 'Policies and Access Control', 'Compliance', 'Integration', 'Advanced Access Configuration', 'Network Configuration', and 'System Configuration'. The main content area is titled 'New Standard Connection Profile' and has a search filter. The 'Captive Portal' tab is selected, showing the following settings:

- Profile Name:** INFN-wired. A note below states: 'A profile id can only contain alphanumeric characters, dashes, period and or underscores.'
- Profile Description:** (Empty text field)
- Enable profile:** Enabled
- Root Portal Module:** Default portal policy. A note below states: 'The Root Portal Module to use.'
- Activate preregistration:** Disabled. A note below states: 'This activates preregistration on the connection profile. Meaning, instead of applying the access to the currently connected device, it displays a local account that is created while registering. Note that activating this disables the on-site registration on this connection profile. Also, make sure the sources on the connection profile have 'Create local account' enabled.'
- Automatically register devices:** Enabled. A note below states: 'This activates automatic registration of devices for the profile. Devices will not be shown a captive portal and RADIUS authentication credentials will be used to register the device. This option only makes sense in the context of an 802.1x authentication.'



CCR Tutorial Days 10-12 ottobre @ LNF

Packetfence vers. 12.0 – Profilo per INFN-wired 2/2



The screenshot shows the Packetfence configuration interface for the INFN-wired profile. The top navigation bar includes Status, Reports, Auditing, Nodes, Users, and Configuration. The user is logged in as 'admin'. The left sidebar shows the 'Policies and Access Control' menu with sub-items: Roles, Domains (Active Directory Domains, Realms), Authentication Sources, Network Devices (Switches, Switch Groups), Connection Profiles, Compliance, Integration, Advanced Access Configuration, Network Configuration, and System Configuration.

The main configuration area is titled 'Configuration' and contains the following settings:

- Advanced filter:** A toggle switch is turned off, and 'Basic Mode' is selected. A dropdown menu shows 'ALL (AND)' and a gear icon for settings. A note states: 'With no filter specified, an advanced filter must be specified'.
- Sources:** An 'Add Source' button is present. A note states: 'The advanced filter acts as an additional filter that is combined with the basic filters and respects all/any'.
- Billing Tiers:** An 'Add Billing Tier' button is present. A note states: 'With no source specified, all internal and external sources will be used.'
- Provisioners:** An 'Add Provisioner' button is present. A note states: 'With no billing tiers specified, all billing tiers will be used.'
- Scanners:** An 'Add Scanner' button is present. A note states: 'With no provisioners specified, the provisioners of the default profile will be used.'
- Self service policy:** A dropdown menu with 'Select option' is present. A note states: 'With no scan specified, the scan engine will not be triggered.'

At the bottom of the configuration area, there are three buttons: 'Create & Close' (blue), 'Reset' (white), and 'Cancel' (dark grey).