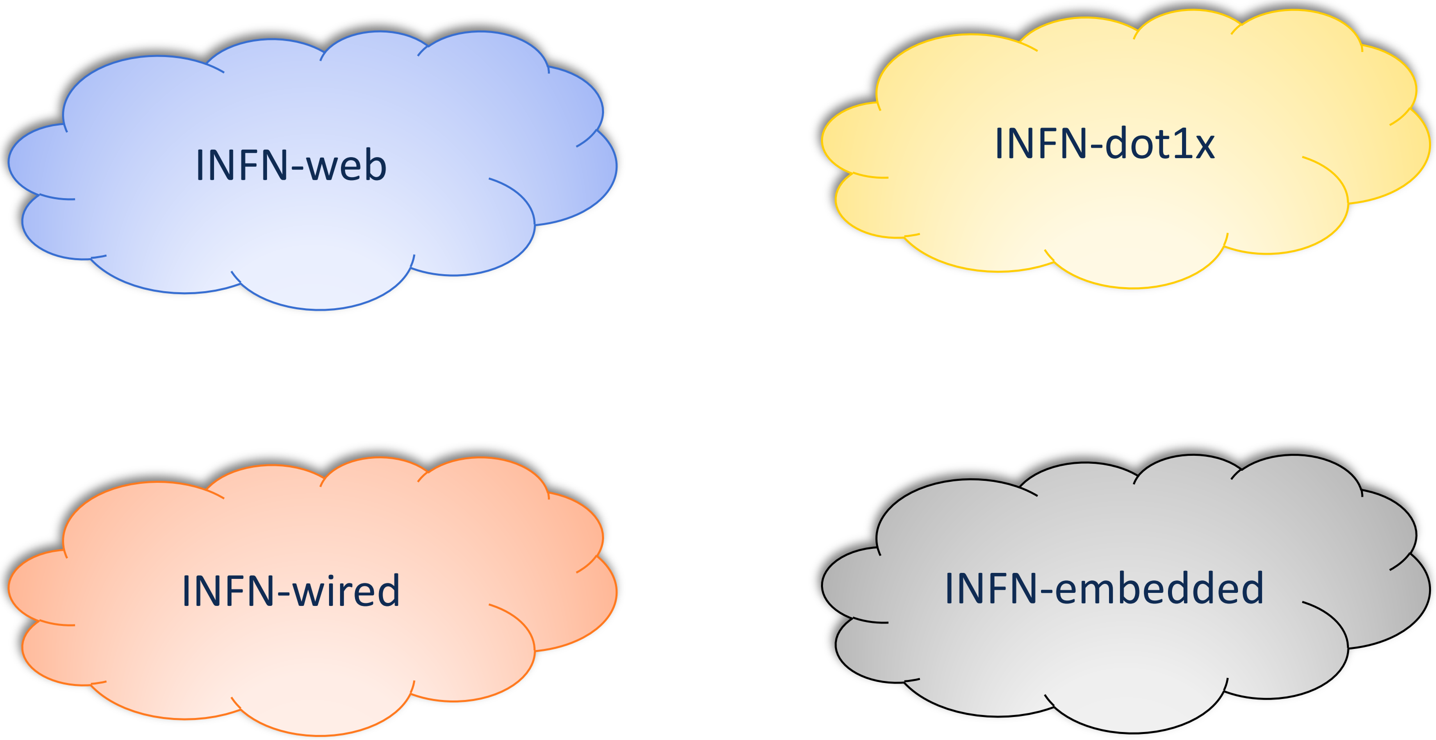
PacketFence

Enrico Becchetti

Obbiettivi

- 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

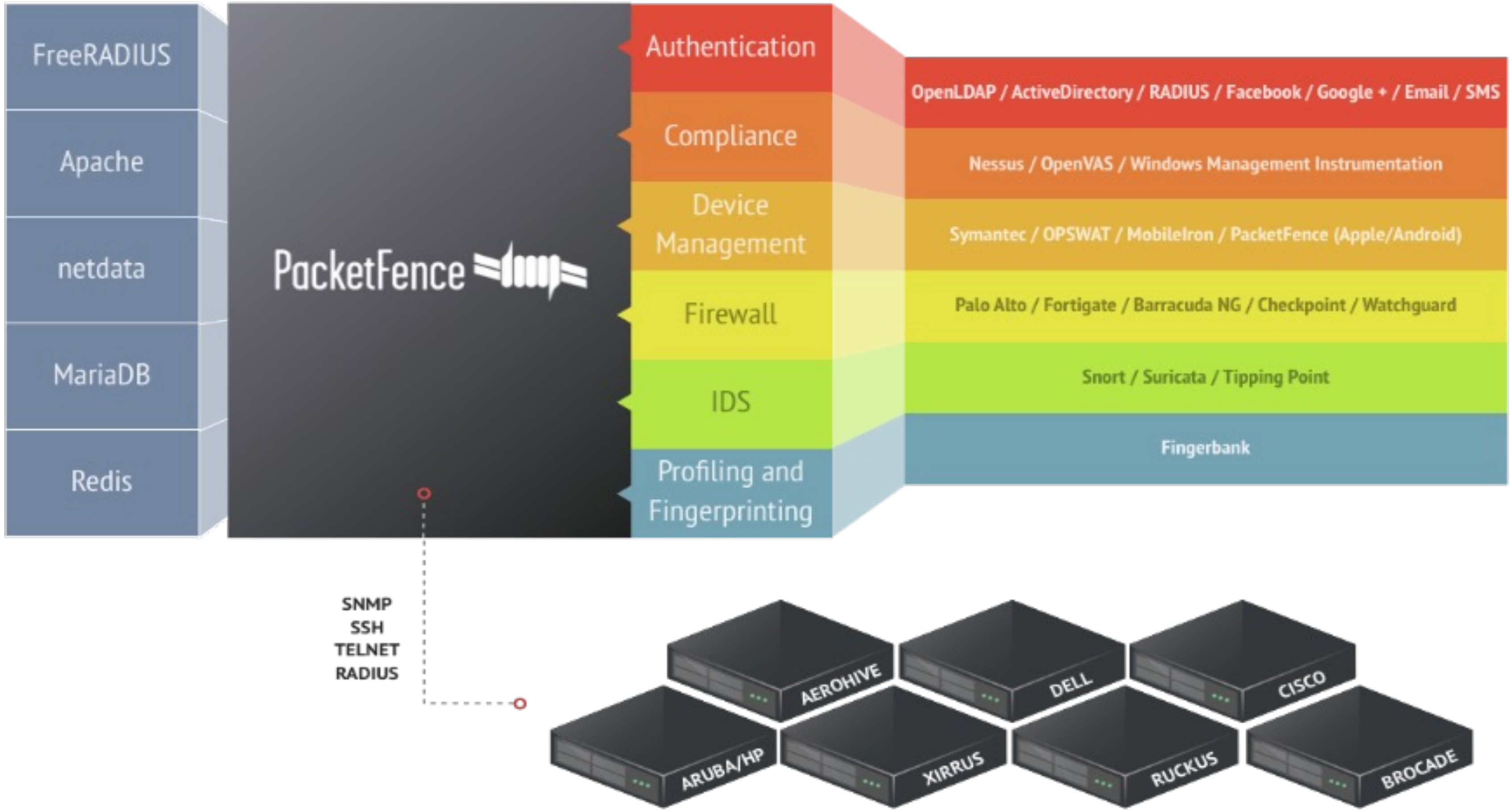
INFN-wired

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)



FreeRADIUS

Apache

netdata

MariaDB

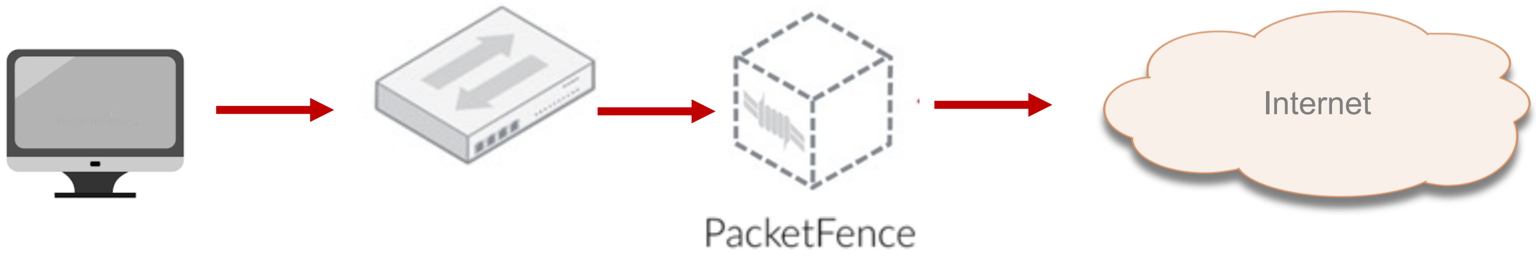
Redis

PacketFence

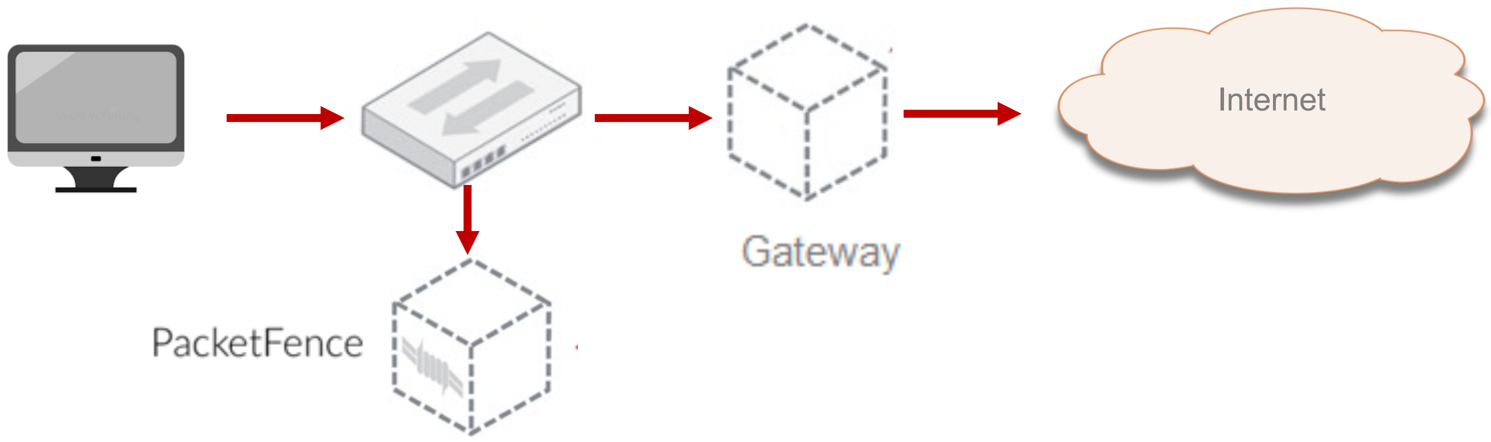
Authentication	OpenLDAP / ActiveDirectory / RADIUS / Facebook / Google + / Email / SMS
Compliance	Nessus / OpenVAS / Windows Management Instrumentation
Device Management	Symantec / OPSWAT / MobileIron / PacketFence (Apple/Android)
Firewall	Palo Alto / Fortigate / Barracuda NG / Checkpoint / Watchguard
IDS	Snort / Suricata / Tipping Point
Profiling and Fingerprinting	Fingerbank

SNMP
SSH
TELNET
RADIUS

- Packetfence modalià inline



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



PacketFence

Installazione e configurazione

Installazione:

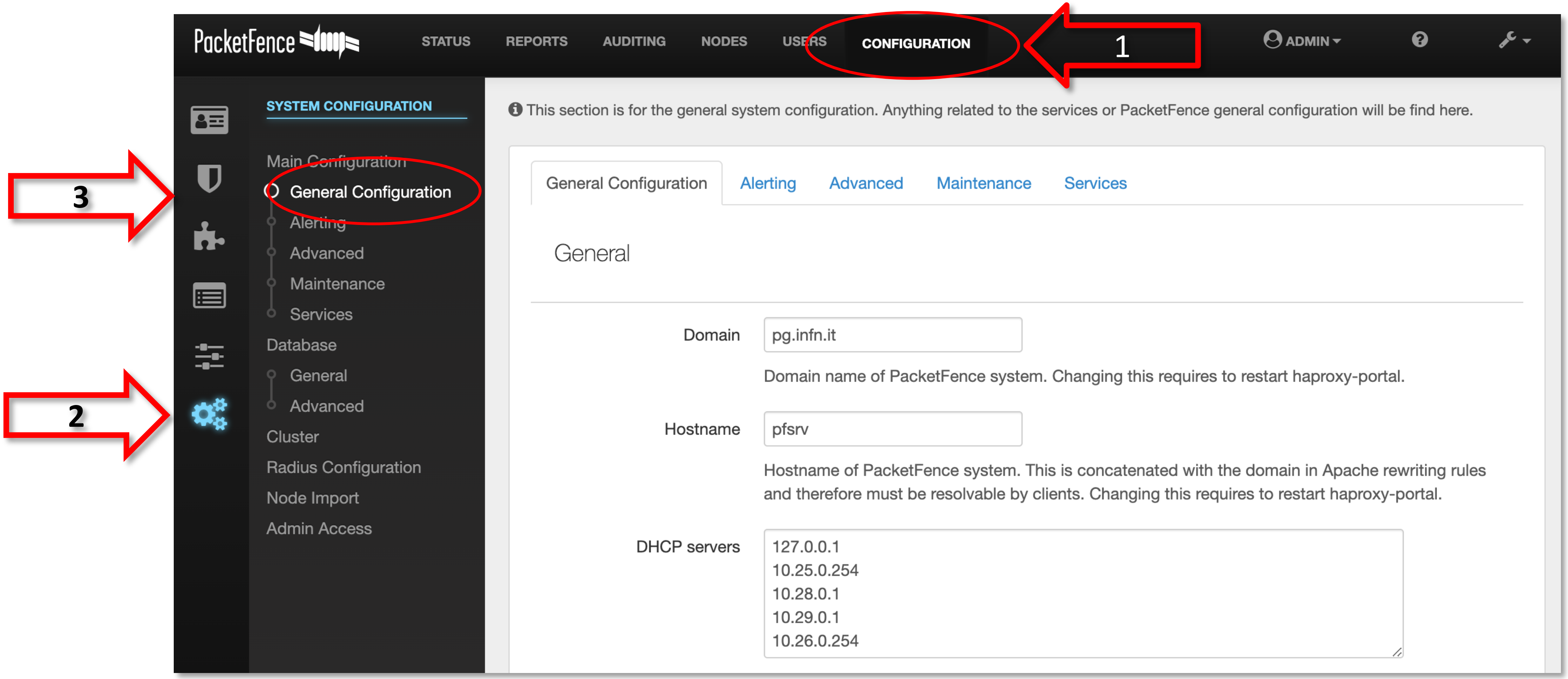
- Appliance preconfigurato https://www.packetfence.org/download.html#/zen
- Immagine ISO Debian 11 con PF12 https://www.packetfence.org/download.html#/releases
- Repository RedHat https://www.packetfence.org/downloads/PacketFence/RHEL8/
- Repository Debian https://www.packetfence.org/downloads/PacketFence/debian/

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/PacketFence_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

CCR Tutorial Days 10-12 ottobre @ LNF



This section is for the general system configuration. Anything related to the services or PacketFence general configuration will be find here.

General

Domain: pg.infn.it

Domain name of PacketFence system. Changing this requires to restart haproxy-portal.

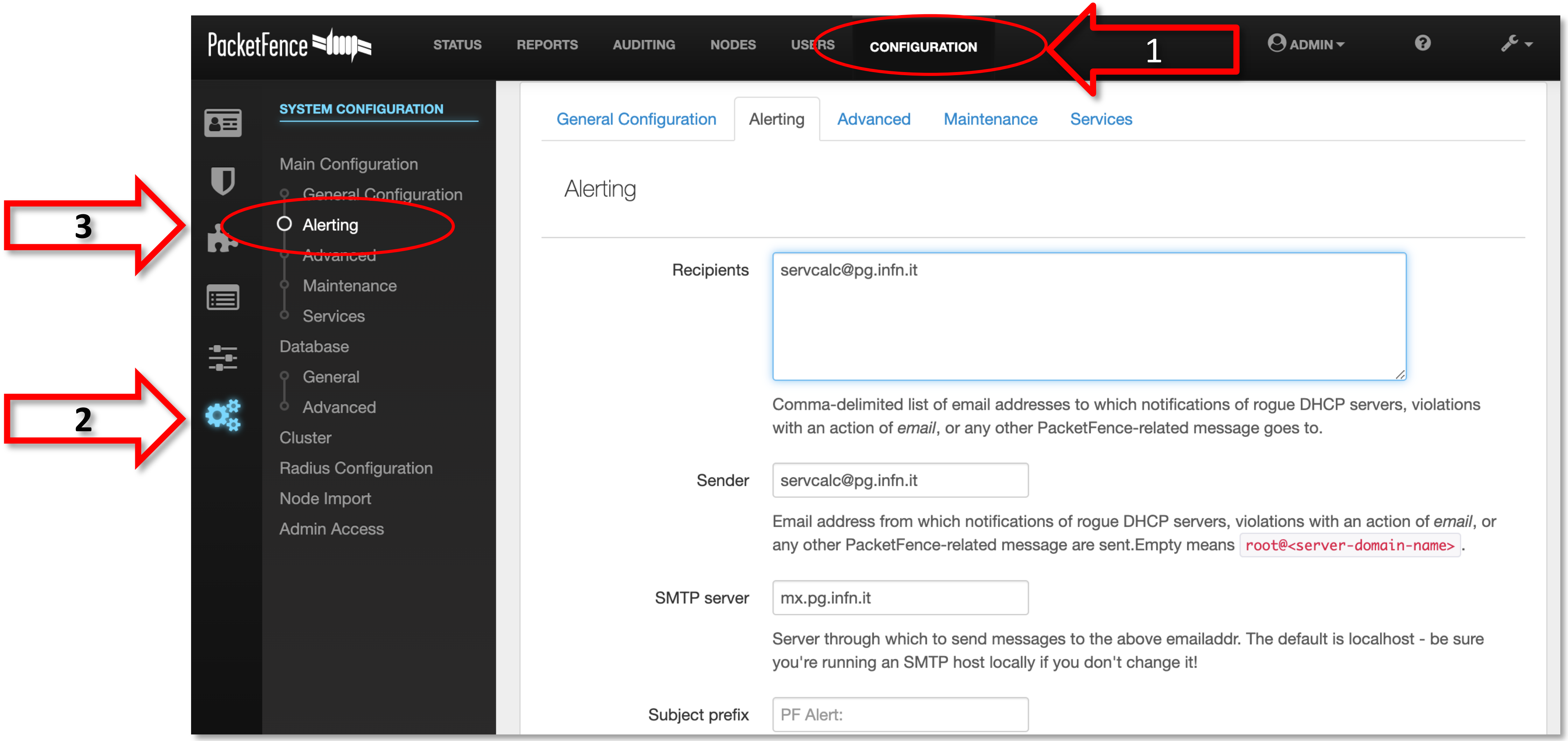
Hostname: pfsrv

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:

```
127.0.0.1
10.25.0.254
10.28.0.1
10.29.0.1
10.26.0.254
```

CCR Tutorial Days 10-12 ottobre @ LNF



Alerting

Recipients: servcalc@pg.infn.it

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.

Sender: servcalc@pg.infn.it

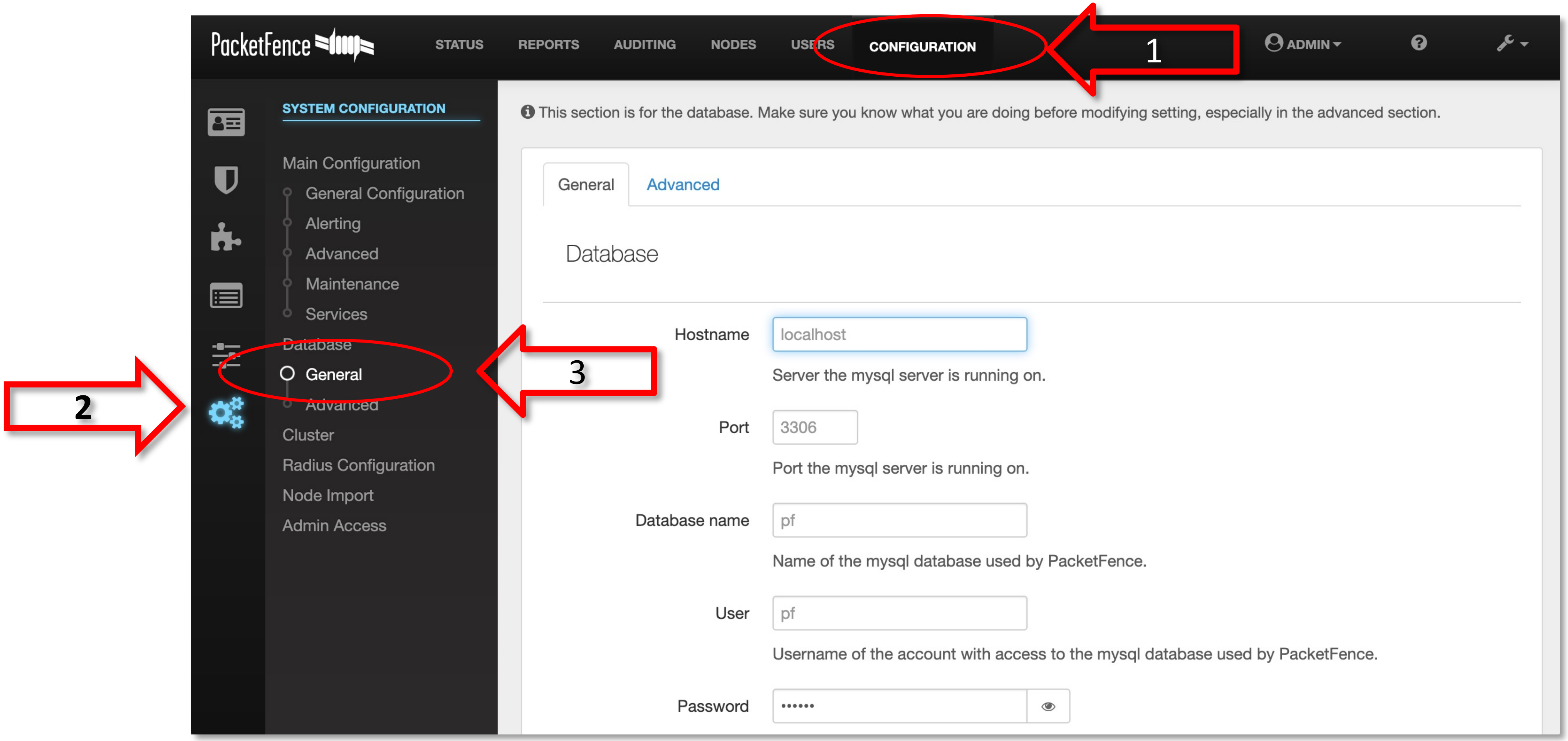
Email address from which notifications of rogue DHCP servers, violations with an action of *email*, or any other PacketFence-related message are sent.Empty means `root@<server-domain-name>`.

SMTP server: mx.pg.infn.it

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!

Subject prefix: PF Alert:

CCR Tutorial Days 10-12 ottobre @ LNF



ℹ This section is for the database. Make sure you know what you are doing before modifying setting, especially in the advanced section.

Database

Hostname: localhost
Server the mysql server is running on.

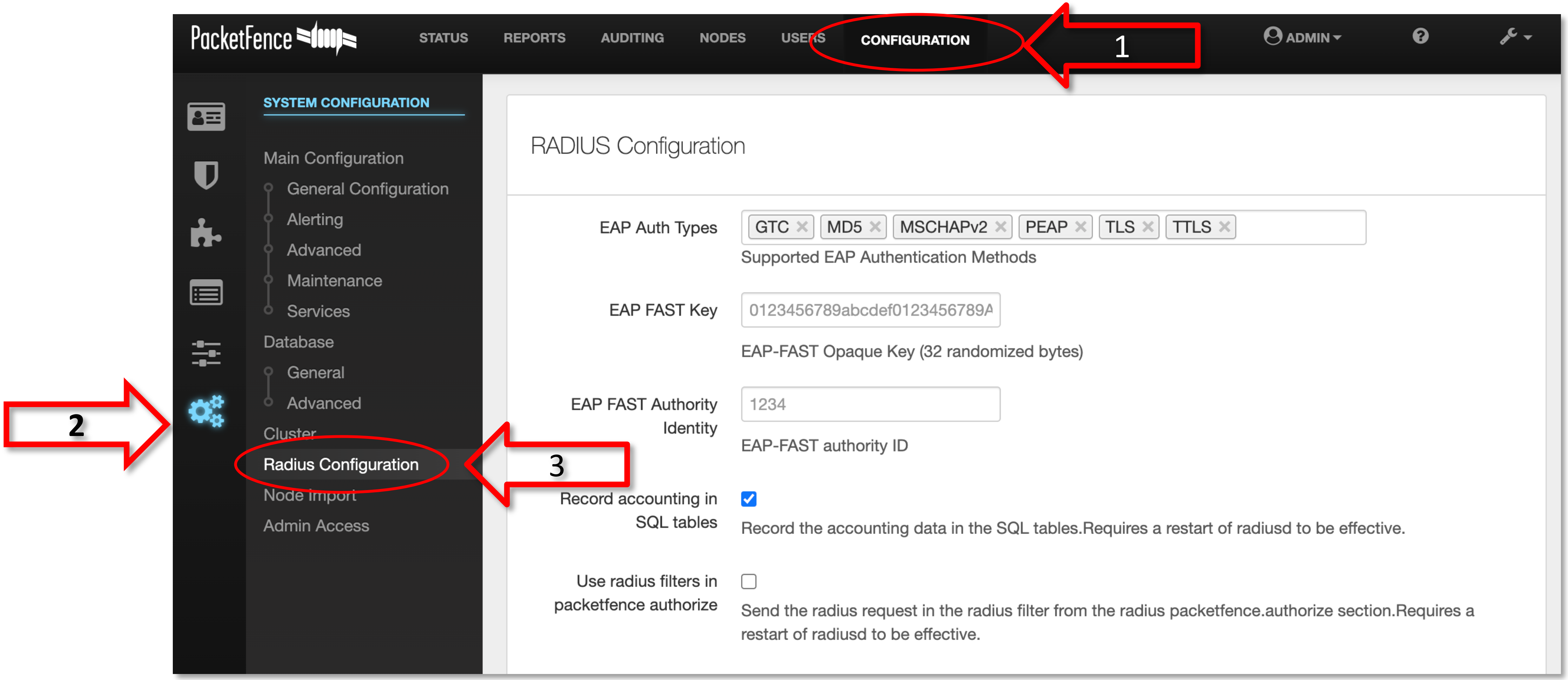
Port: 3306
Port the mysql server is running on.

Database name: pf
Name of the mysql database used by PacketFence.

User: pf
Username of the account with access to the mysql database used by PacketFence.

Password: ••••••

CCR Tutorial Days 10-12 ottobre @ LNF



RADIUS Configuration

EAP Auth Types: GTC × MD5 × MSCHAPv2 × PEAP × TLS × TTLS ×

Supported EAP Authentication Methods

EAP FAST Key: 0123456789abcdef0123456789A

EAP-FAST Opaque Key (32 randomized bytes)

EAP FAST Authority Identity: 1234

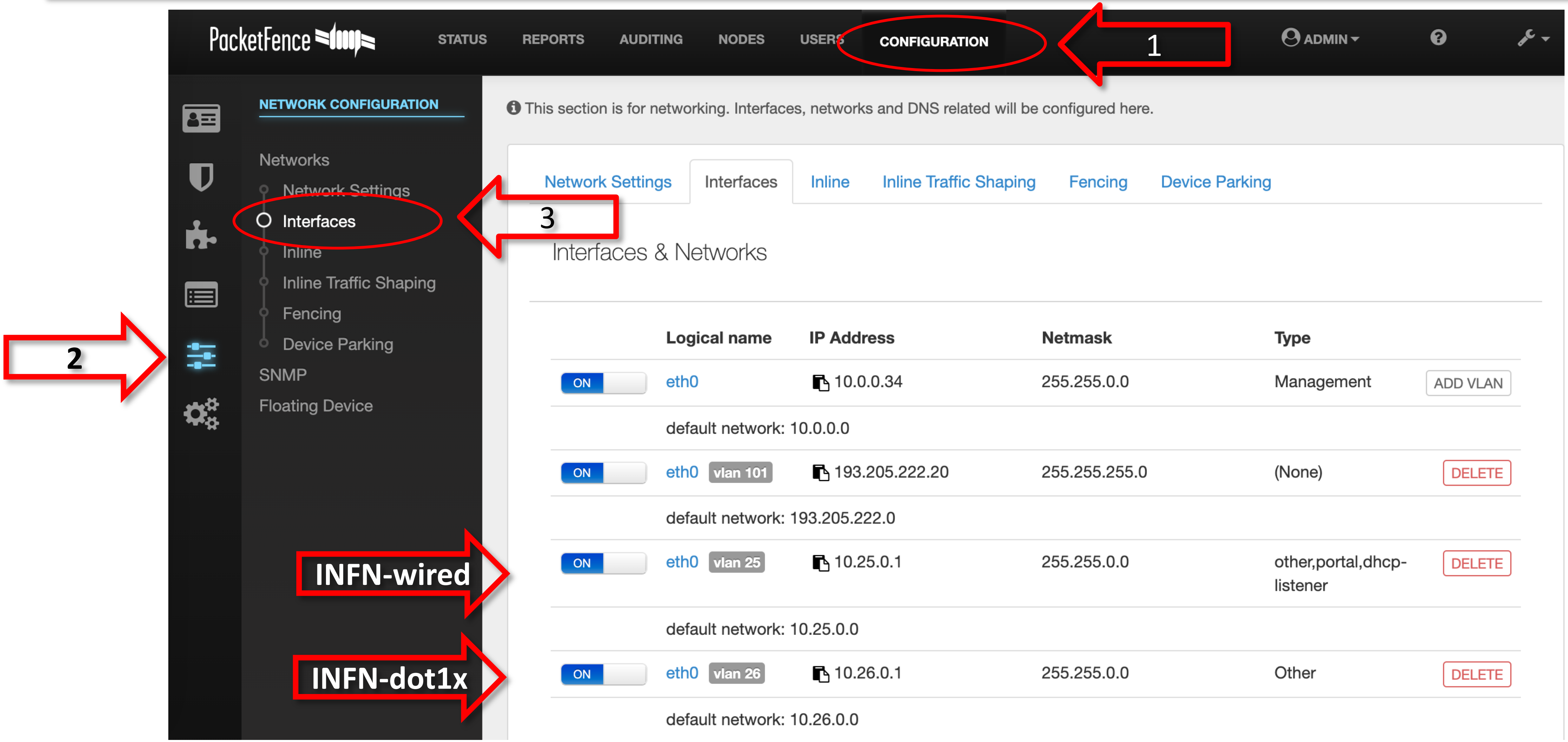
EAP-FAST authority ID

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: □

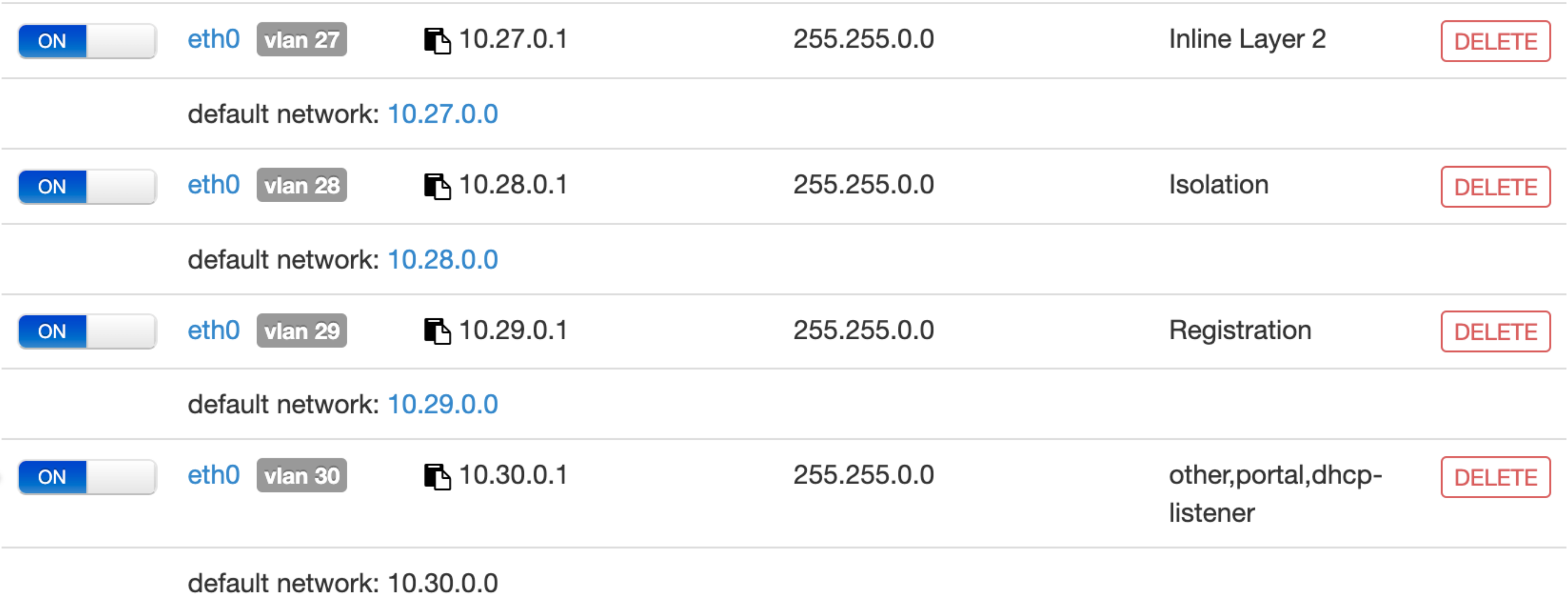
Send the radius request in the radius filter from the radius packetfence.authorize section.Requires a restart of radiusd to be effective.



ℹ This section is for networking. Interfaces, networks and DNS related will be configured here.

Interfaces & Networks

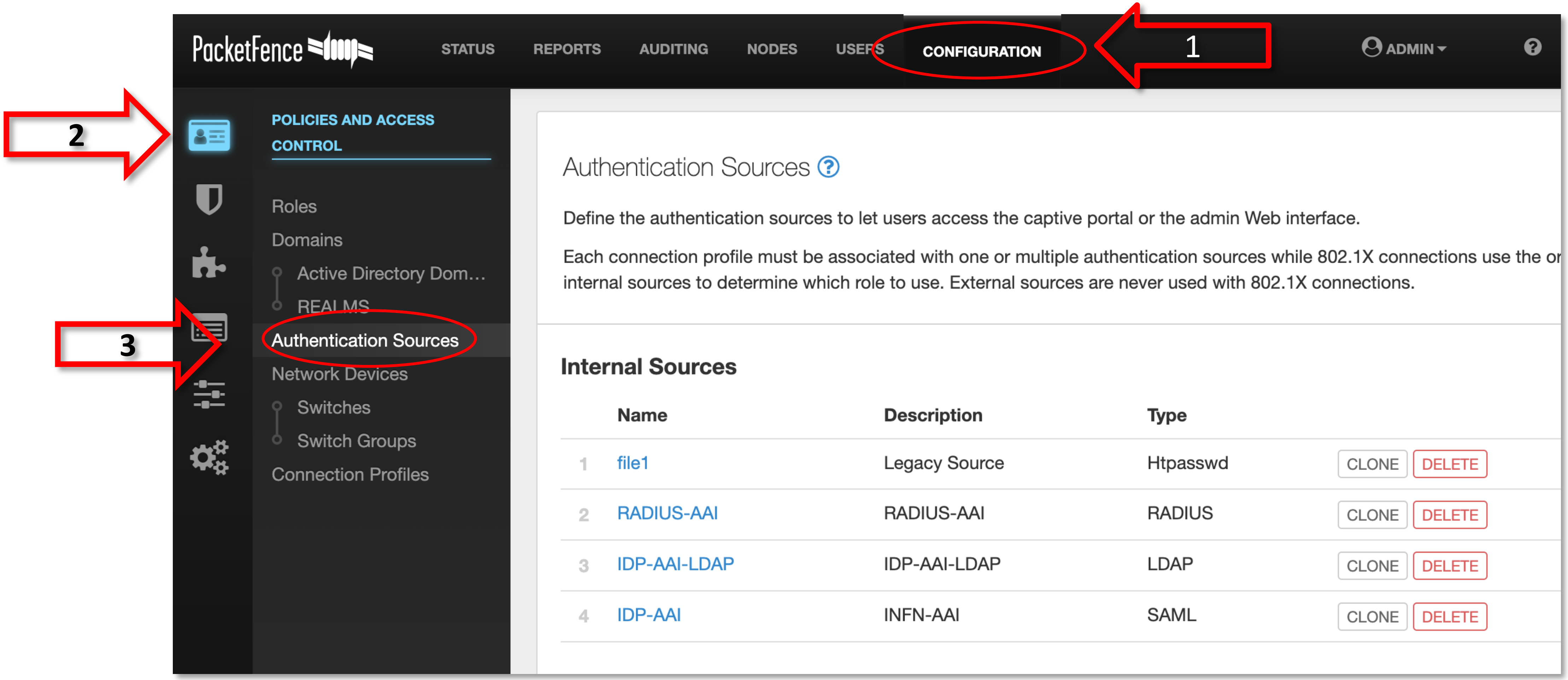
	Logical name	IP Address	Netmask	Type	
ON	eth0	10.0.0.34	255.255.0.0	Management	ADD VLAN
	default network: 10.0.0.0				
ON	eth0 vlan 101	193.205.222.20	255.255.255.0	(None)	DELETE
	default network: 193.205.222.0				
ON	eth0 vlan 25	10.25.0.1	255.255.0.0	other,portal,dhcp-listener	DELETE
	default network: 10.25.0.0				
ON	eth0 vlan 26	10.26.0.1	255.255.0.0	Other	DELETE
	default network: 10.26.0.0				



INFN-web

INFN-embedded

ON	eth0	vlan 27	10.27.0.1	255.255.0.0	Inline Layer 2	DELETE
	default network: 10.27.0.0					
ON	eth0	vlan 28	10.28.0.1	255.255.0.0	Isolation	DELETE
	default network: 10.28.0.0					
ON	eth0	vlan 29	10.29.0.1	255.255.0.0	Registration	DELETE
	default network: 10.29.0.0					
ON	eth0	vlan 30	10.30.0.1	255.255.0.0	other,portal,dhcp-listener	DELETE
	default network: 10.30.0.0					



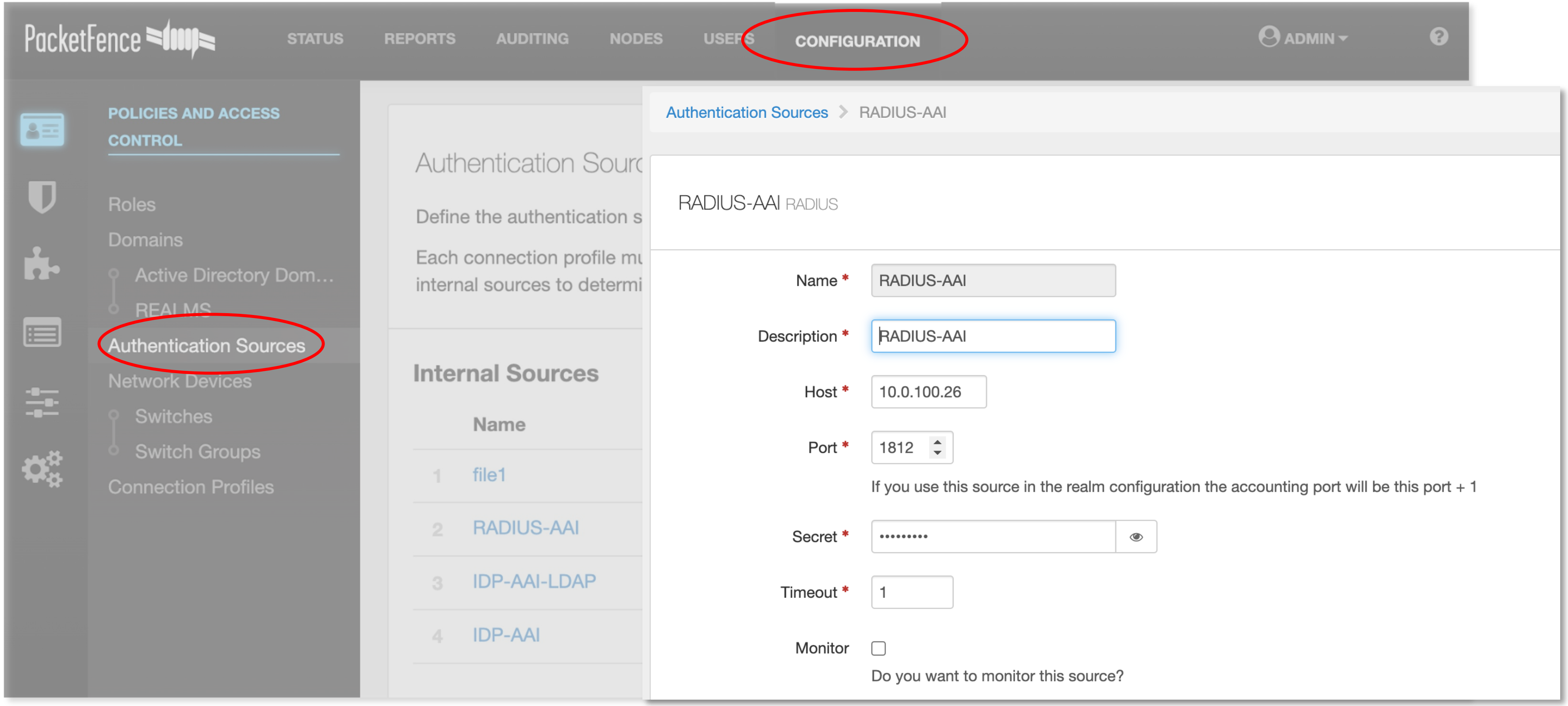
Authentication Sources

Define the authentication sources to let users access the captive portal or the admin Web interface.

Each connection profile must be associated with one or multiple authentication sources while 802.1X connections use the or internal sources to determine which role to use. External sources are never used with 802.1X connections.

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



Authentication Sources > RADIUS-AAI

RADIUS-AAI RADIUS

Name * RADIUS-AAI

Description * RADIUS-AAI

Host * 10.0.100.26

Port * 1812

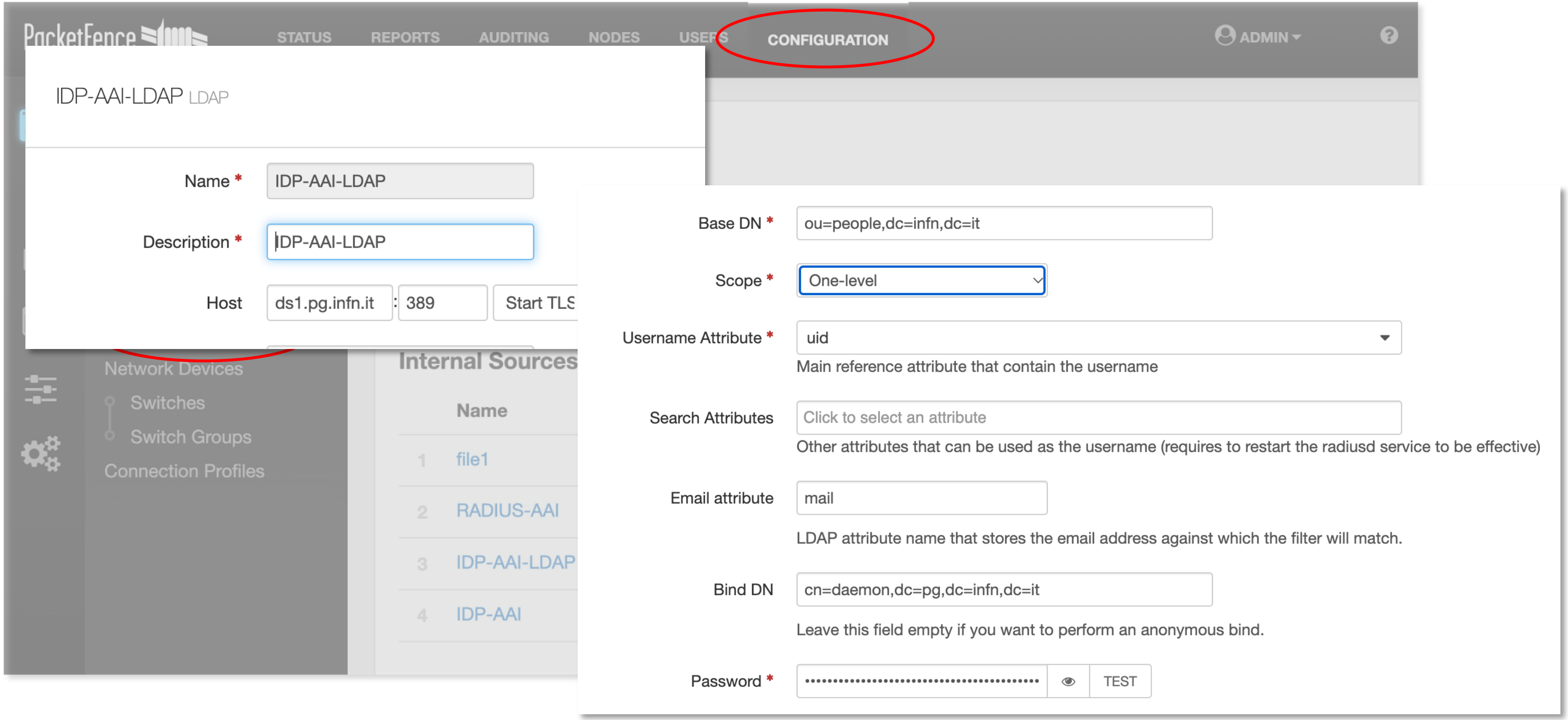
If you use this source in the realm configuration the accounting port will be this port + 1

Secret * •••••••••

Timeout * 1

Monitor □

Do you want to monitor this source?



Internal Sources

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

IDP-AAI-LDAP LDAP

Name * IDP-AAI-LDAP

Description * IDP-AAI-LDAP

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

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

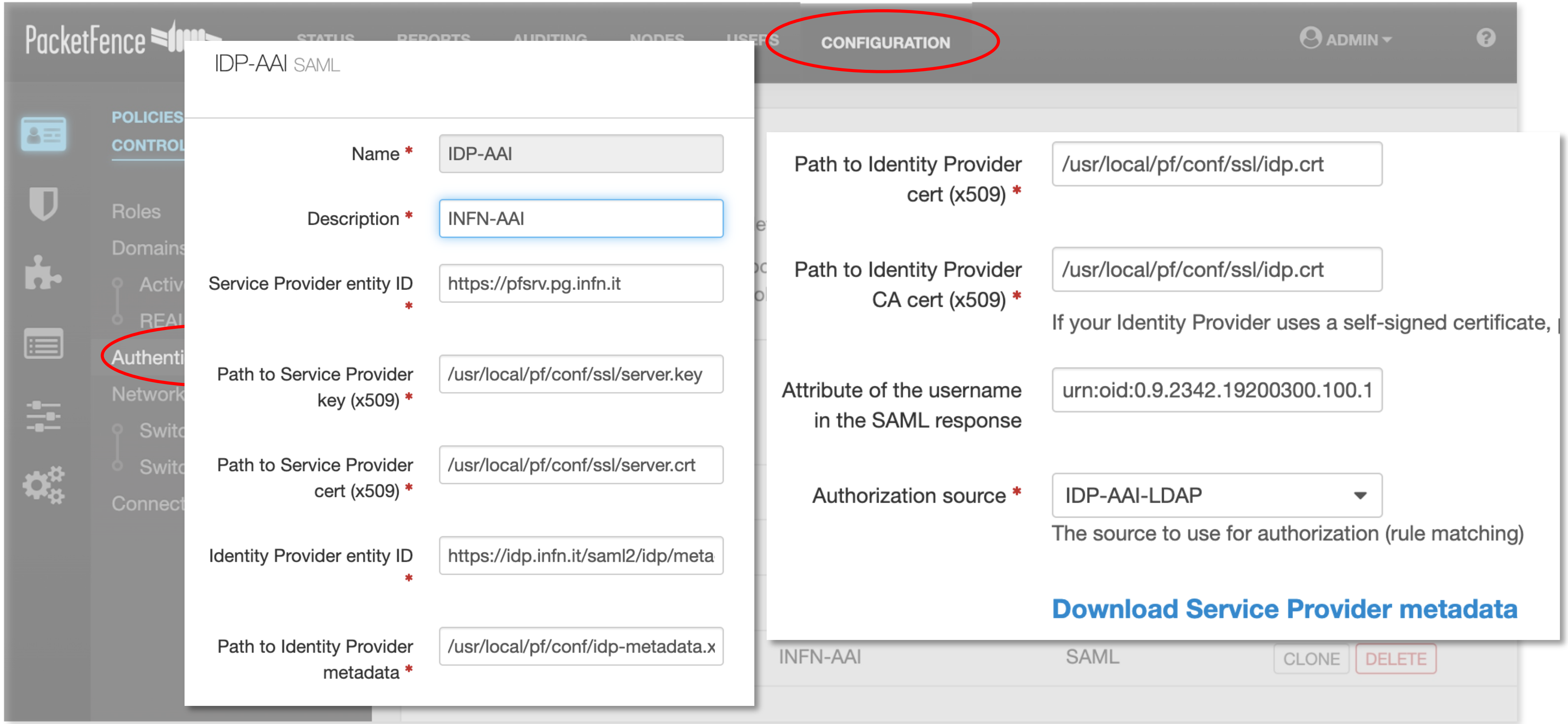
LDAP attribute name that stores the email address against which the filter will match.

Bind DN cn=daemon,dc=pg,dc=infn,dc=it

Leave this field empty if you want to perform an anonymous bind.

Password * •• TEST

CCR Tutorial Days 10-12 ottobre @ LNF



IDP-AAI SAML

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

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

If your Identity Provider uses a self-signed certificate,

Attribute of the username in the SAML response urn:oid:0.9.2342.19200300.100.1

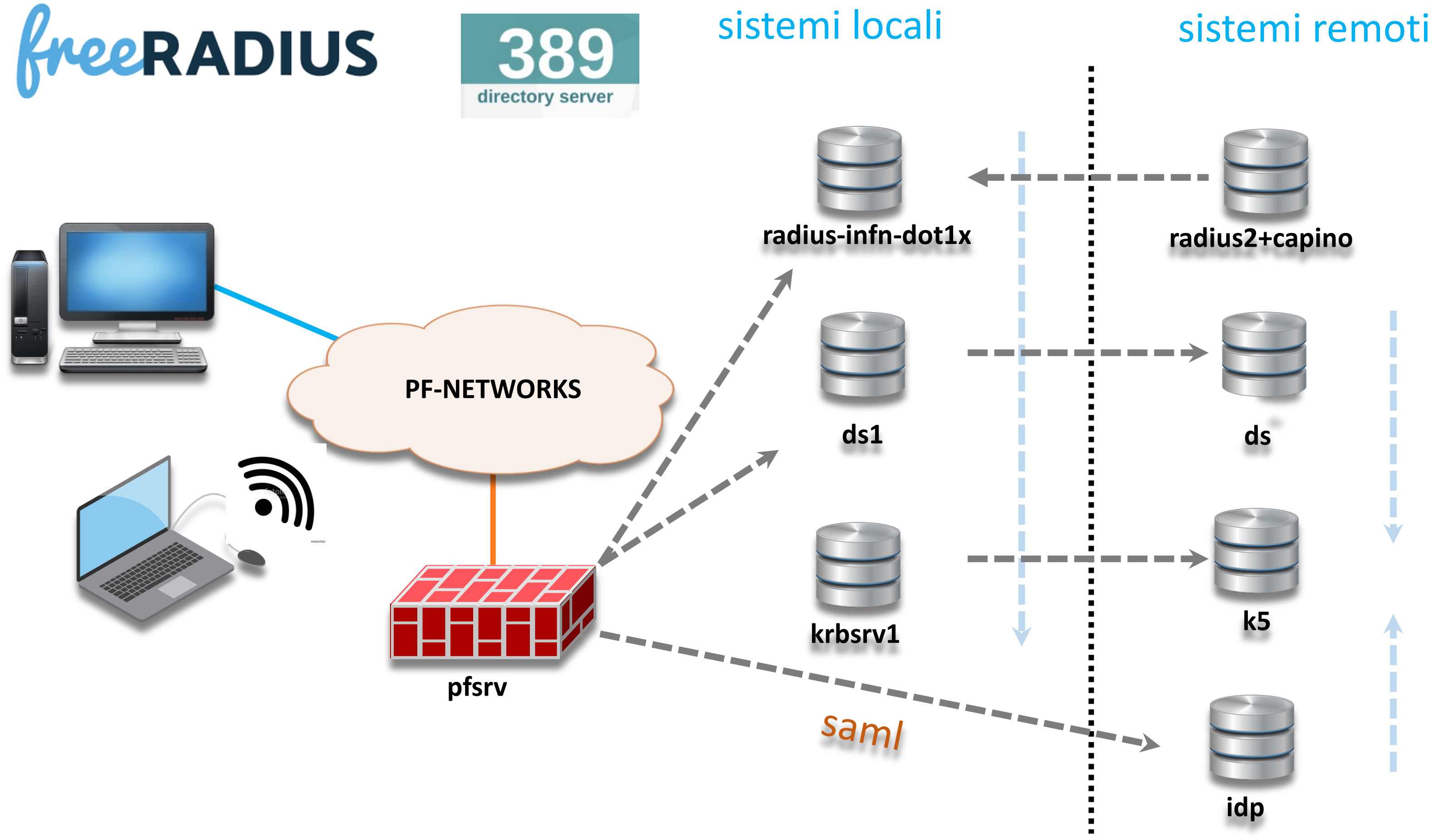
Authorization source * IDP-AAI-LDAP

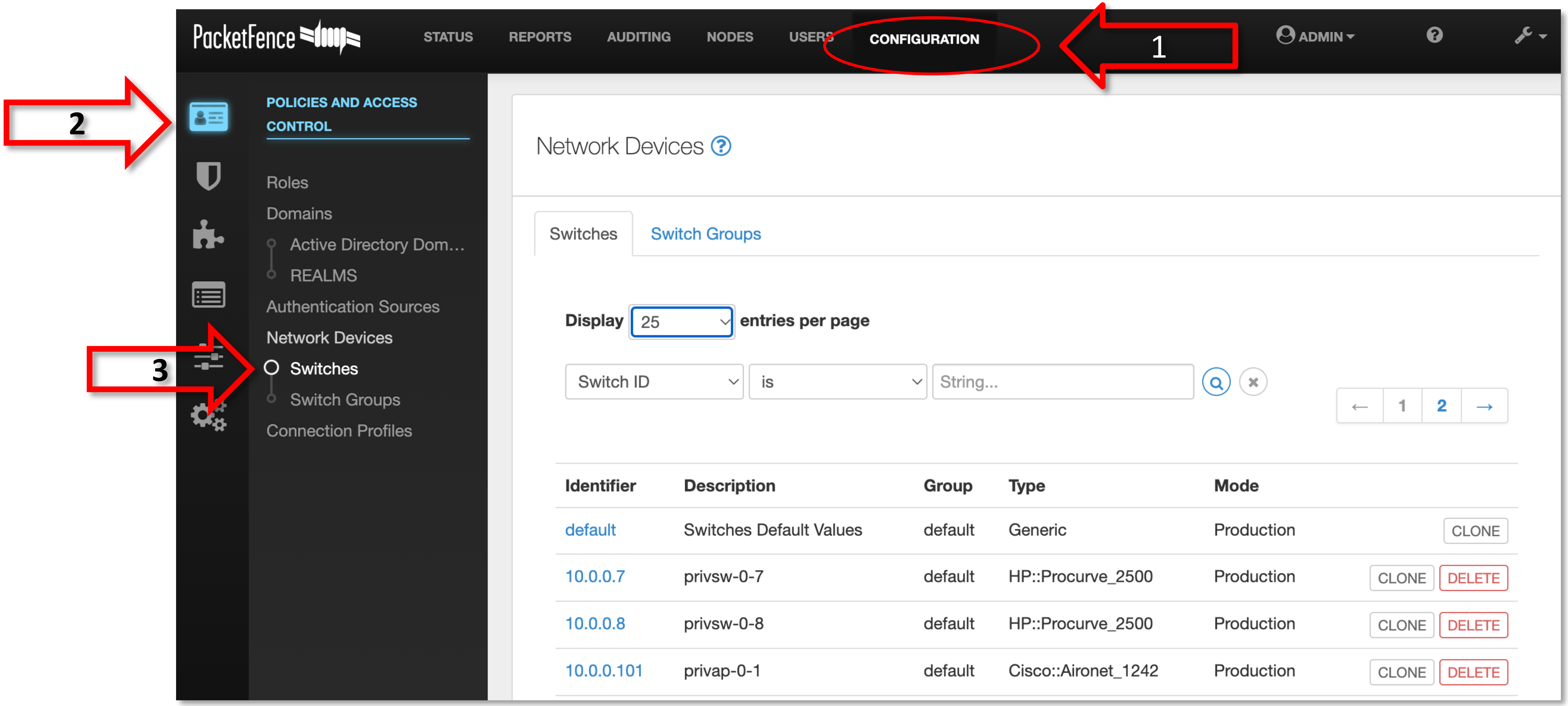
The source to use for authorization (rule matching)

Download Service Provider metadata

INFN-AAI SAML

SAML freeRADIUS 389 directory server





Network Devices

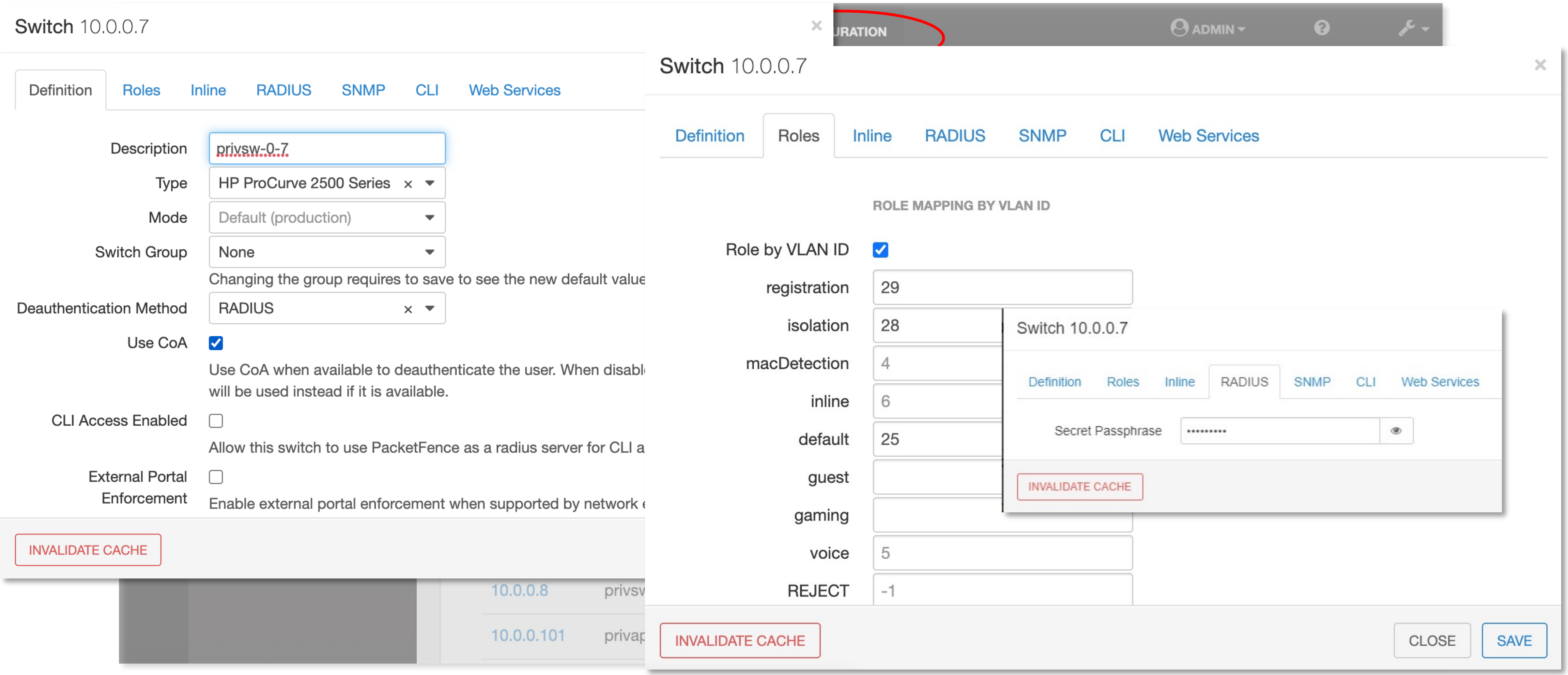
Switches | Switch Groups

Display 25 entries per page

Switch ID | is | String...

← 1 2 →

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



Switch 10.0.0.7

Definition | Roles | Inline | RADIUS | SNMP | CLI | Web Services

Description	privsw-0-7
Type	HP ProCurve 2500 Series
Mode	Default (production)
Switch Group	None
	Changing the group requires to save to see the new default value
Deauthentication Method	RADIUS
Use CoA	☑
	Use CoA when available to deauthenticate the user. When disabl will be used instead if it is available.
CLI Access Enabled	□
	Allow this switch to use PacketFence as a radius server for CLI a
External Portal Enforcement	□
	Enable external portal enforcement when supported by network e

INVALIDATE CACHE

10.0.0.8 privsv

10.0.0.101 privap

Switch 10.0.0.7

Definition | Roles | Inline | RADIUS | SNMP | CLI | Web Services

ROLE MAPPING BY VLAN ID

Role by VLAN ID	☑
registration	29
isolation	28
macDetection	4
inline	6
default	25
guest	
gaming	
voice	5
REJECT	-1

INVALIDATE CACHE

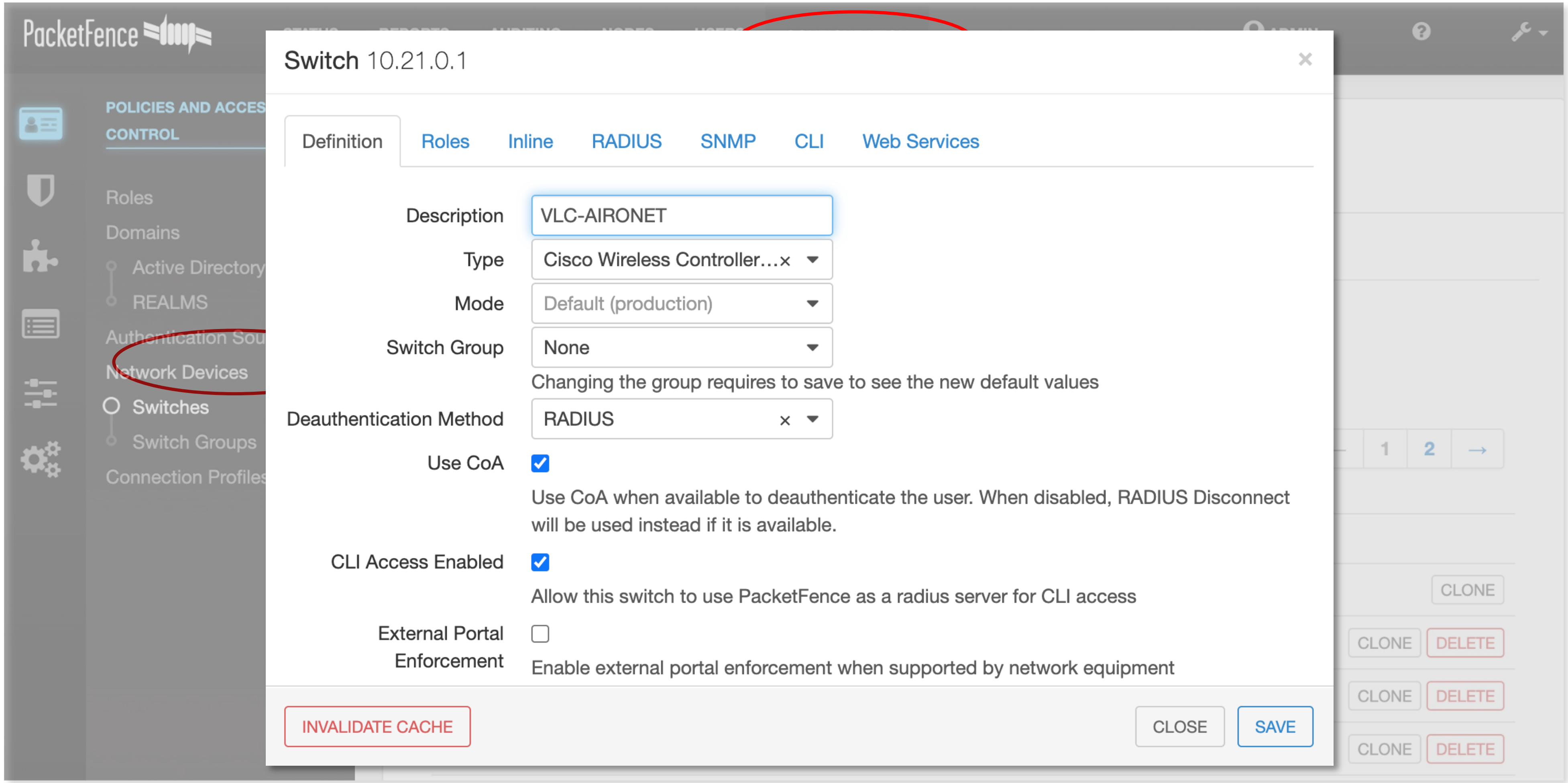
CLOSE SAVE

Switch 10.0.0.7

Definition | Roles | Inline | RADIUS | SNMP | CLI | Web Services

Secret Passphrase: ••••••••••

INVALIDATE CACHE



Switch 10.21.0.1

Definition | Roles | Inline | RADIUS | SNMP | CLI | Web Services

Description: VLC-AIRONET

Type: Cisco Wireless Controller…

Mode: Default (production)

Switch Group: None

Changing the group requires to save to see the new default values

Deauthentication Method: RADIUS

Use CoA: ☑

Use CoA when available to deauthenticate the user. When disabled, RADIUS Disconnect will be used instead if it is available.

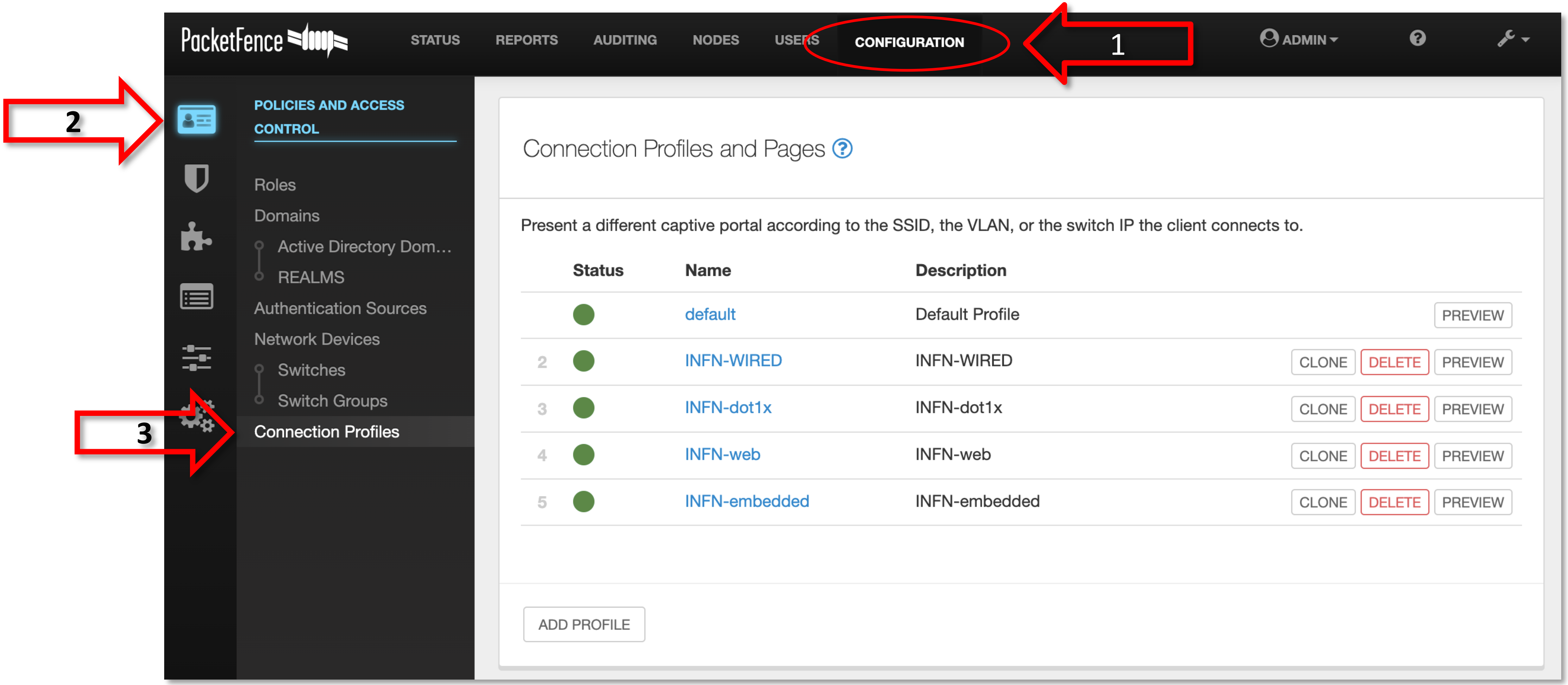
CLI Access Enabled: ☑

Allow this switch to use PacketFence as a radius server for CLI access

External Portal Enforcement: □

Enable external portal enforcement when supported by network equipment

INVALIDATE CACHE | CLOSE | SAVE



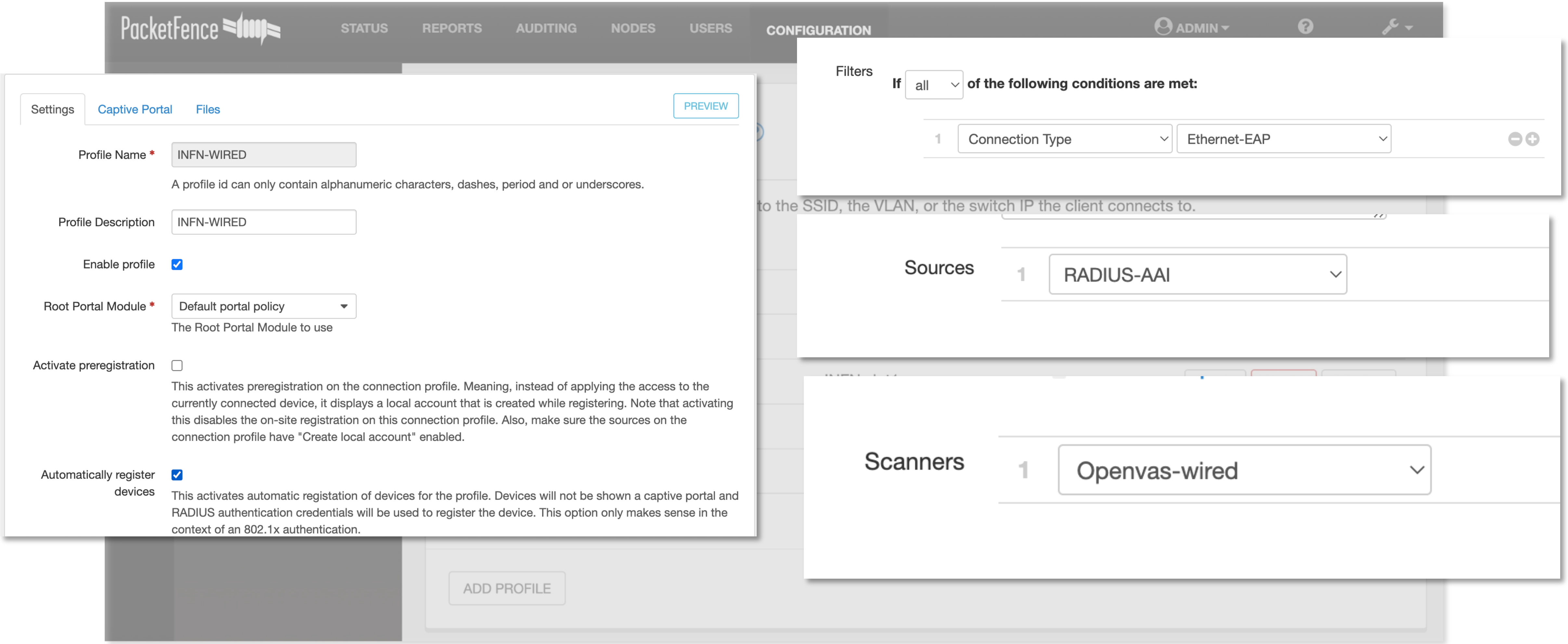
Connection Profiles and Pages ?

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



Profile Name * INFN-WIRED

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

Profile Description INFN-WIRED

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 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 registation 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.

Filters

If all **of the following conditions are met:**

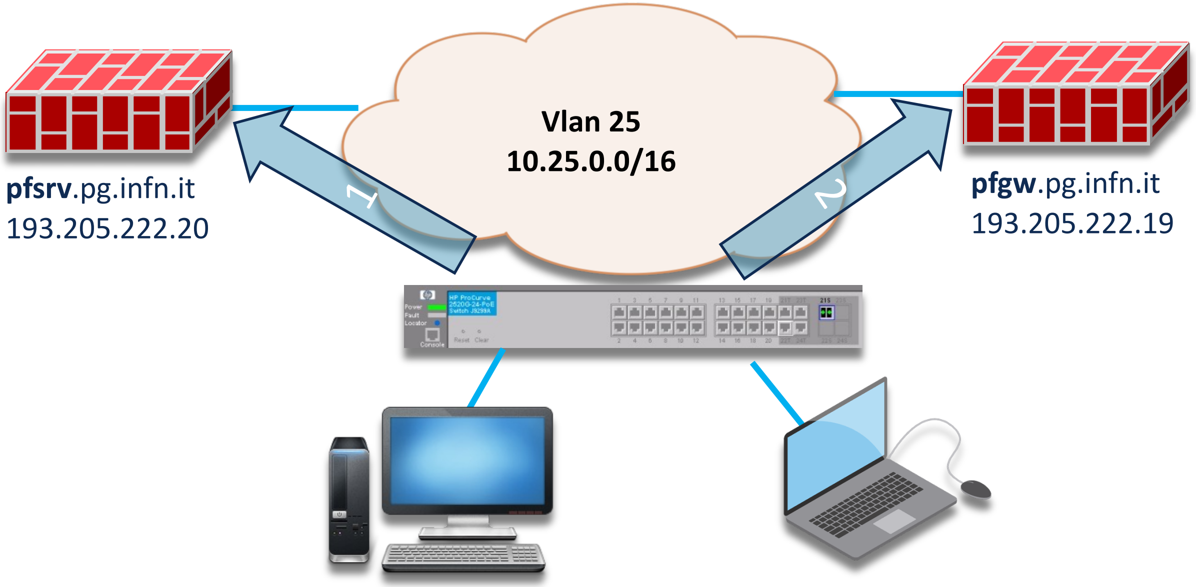
1 Connection Type Ethernet-EAP

to the SSID, the VLAN, or the switch IP the client connects to.

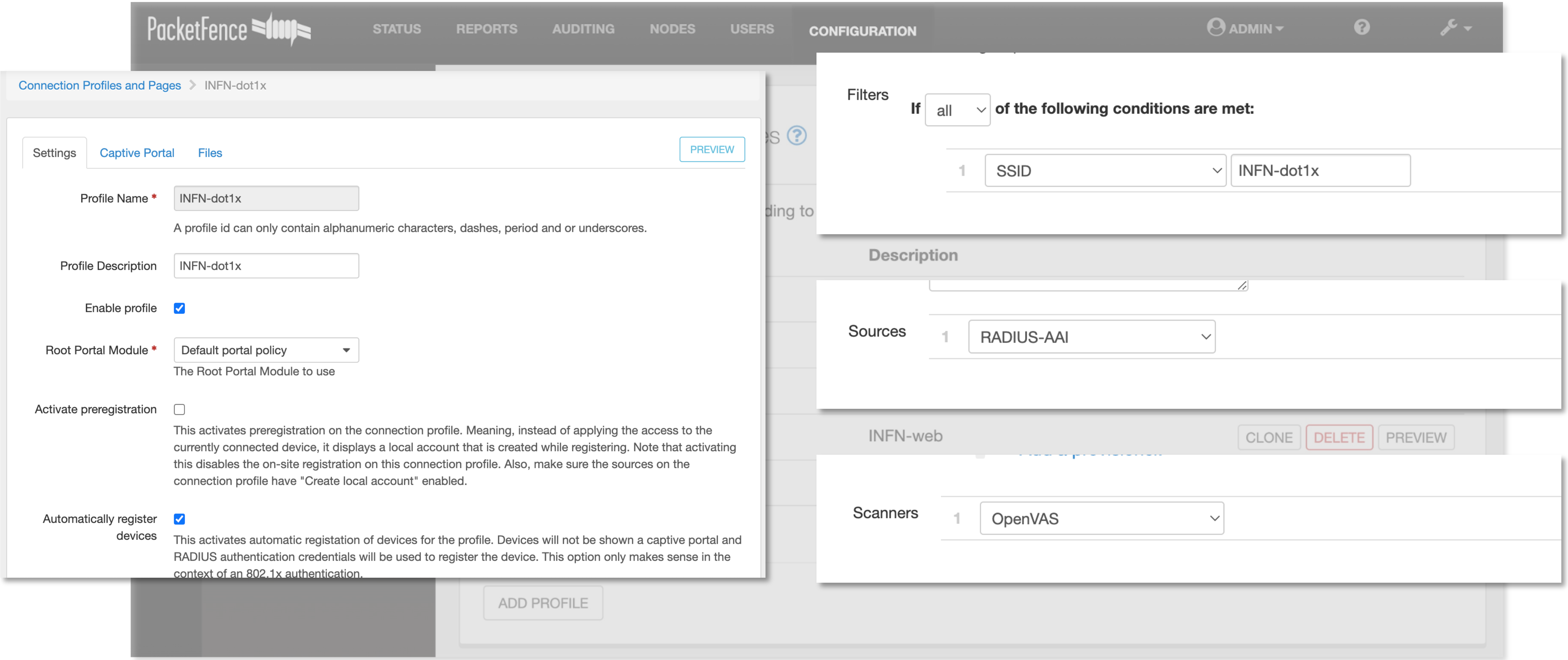
Sources 1 RADIUS-AAI

Scanners 1 Openvas-wired

- INFN-wired (out-of-band)



CCR Tutorial Days 10-12 ottobre @ LNF



Profile Name * INFN-dot1x

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

Profile Description INFN-dot1x

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 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 registation 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.

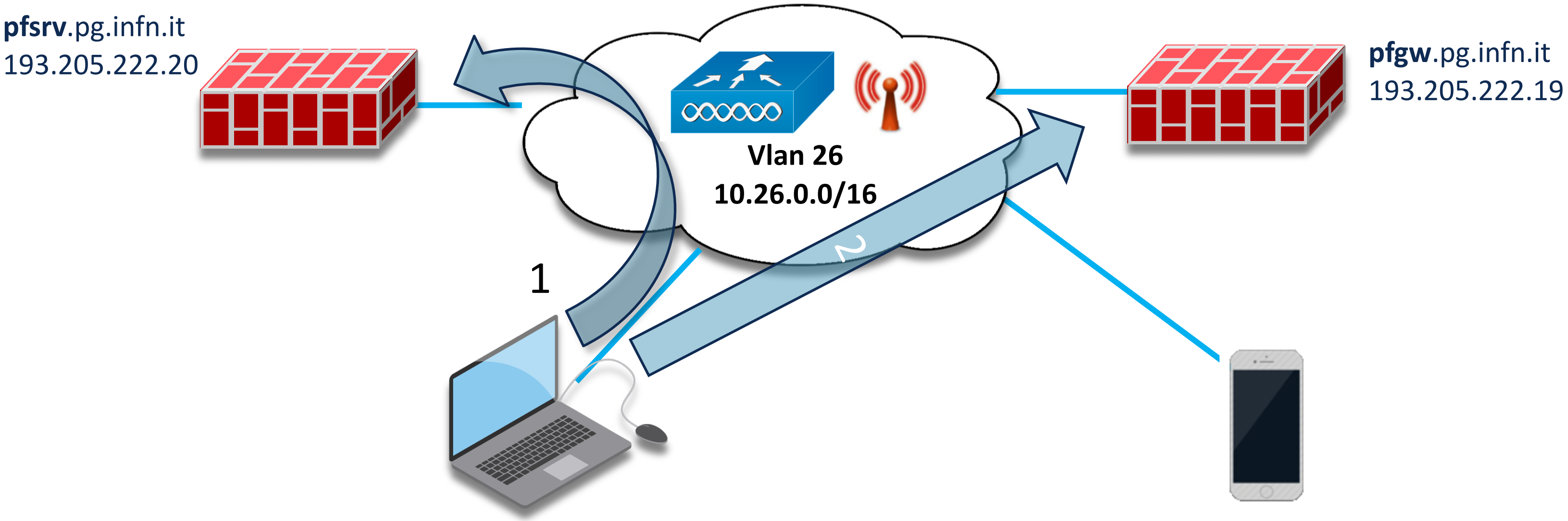
Filters **If** all **of the following conditions are met:**

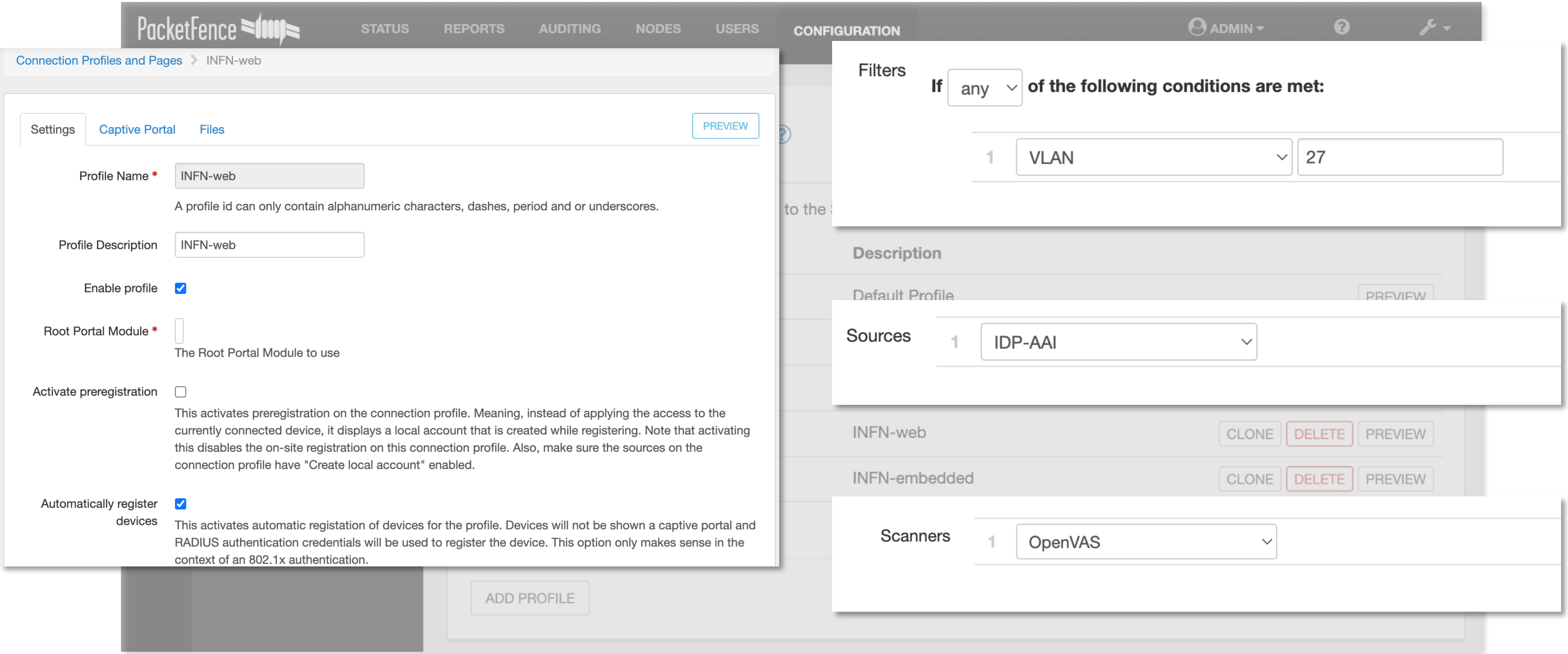
1 SSID INFN-dot1x

Sources 1 RADIUS-AAI

Scanners 1 OpenVAS

- INFN-dot1x (out-of-band)





Connection Profiles and Pages > INFN-web

Settings | Captive Portal | Files

Profile Name * INFN-web

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

Profile Description INFN-web

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 registation 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.

Filters

If any of the following conditions are met:

1 VLAN 27

Description

Default Profile

INFN-web

INFN-embedded

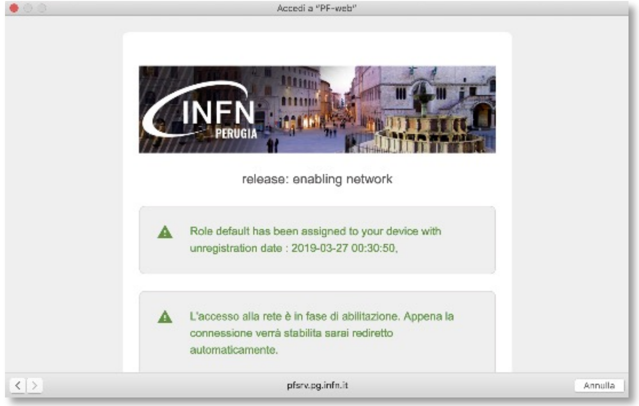
Sources

1 IDP-AAI

Scanners

1 OpenVAS

- INFN-web (inline)



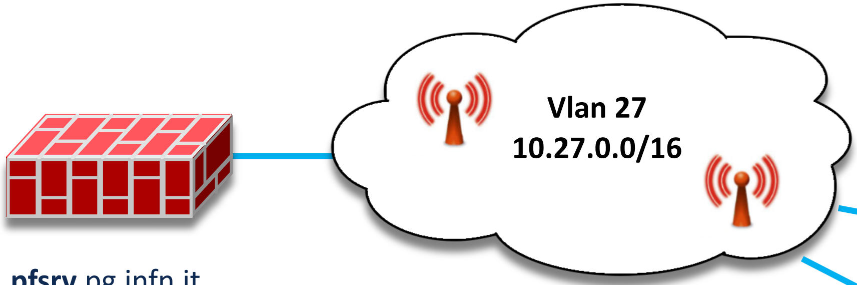
Accedi a "PF-web"

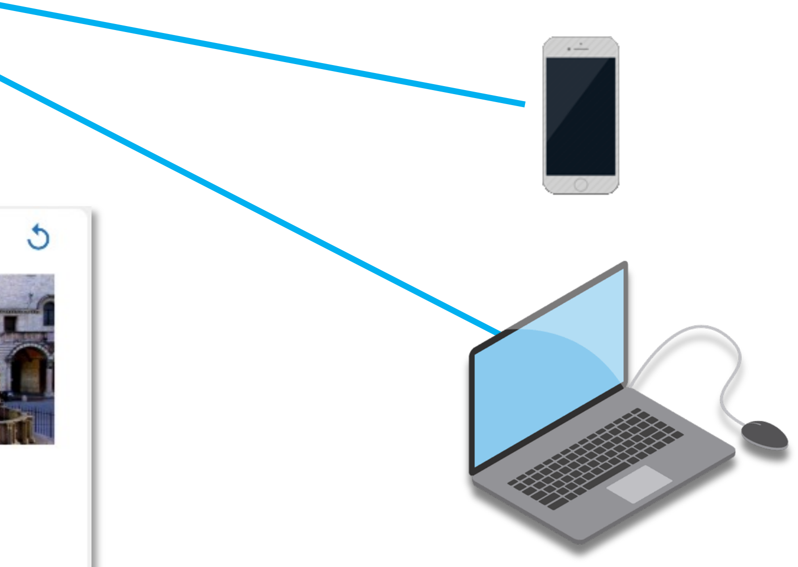
release: enabling network

Role default has been assigned to your device with unregistration date : 2019-03-27 00:30:50.

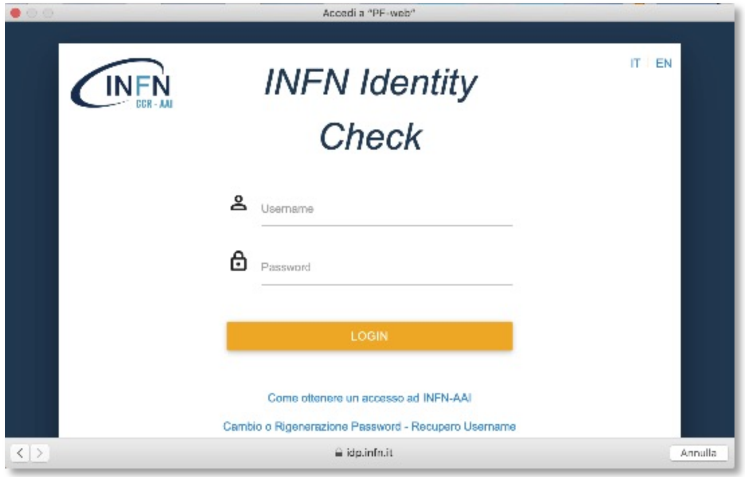
L'accesso alla rete è in fase di abilitazione. Appena la connessione verrà stabilita sarai rediretto automaticamente.

pfsrv.pg.infn.it





pfsrv.pg.infn.it
193.205.222.20



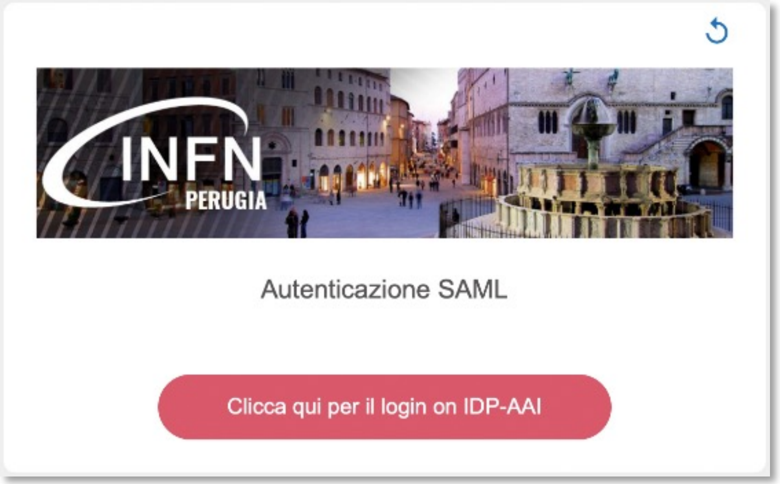
Accedi a "PF-web"

INFN Identity Check

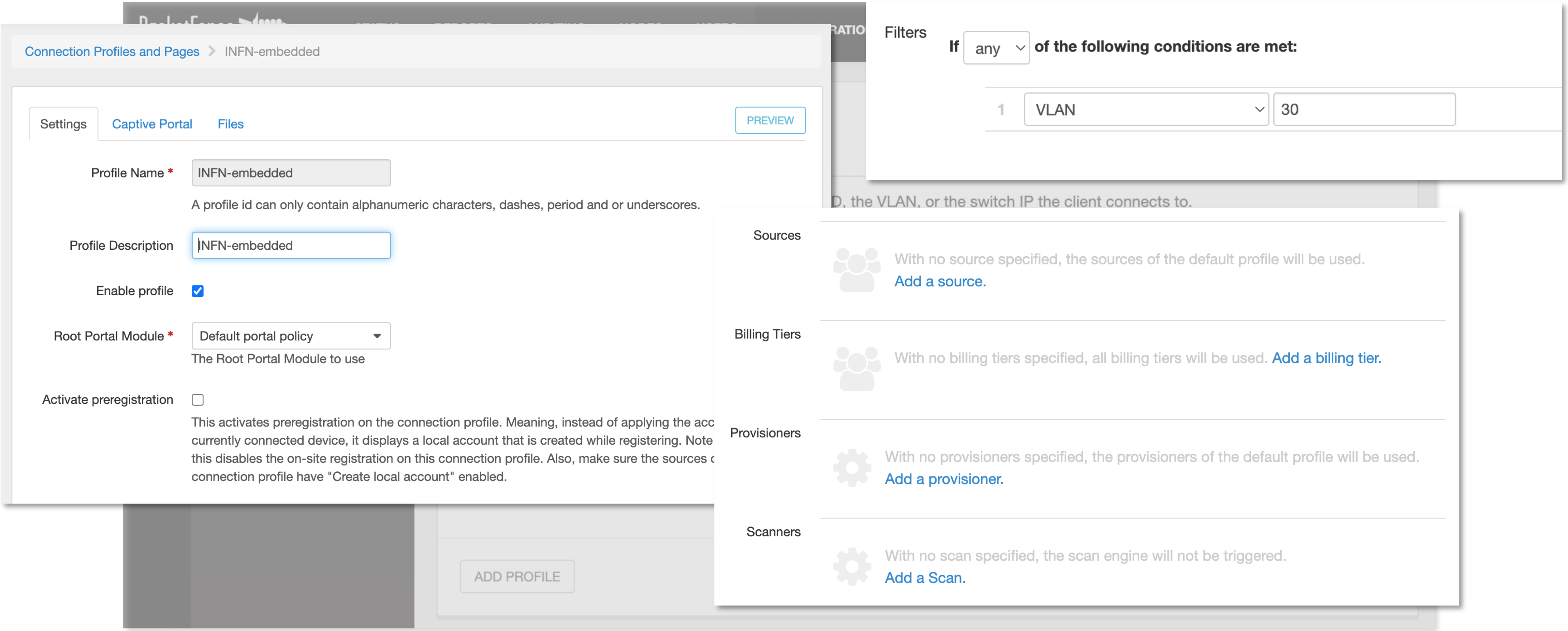
Come ottenere un accesso ad INFN-AAI

Cambio o Rigenerazione Password - Recupero Username

idp.infn.it



Autenticazione SAML



Connection Profiles and Pages > INFN-embedded

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

D, the VLAN, or the switch IP the client connects to.

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.

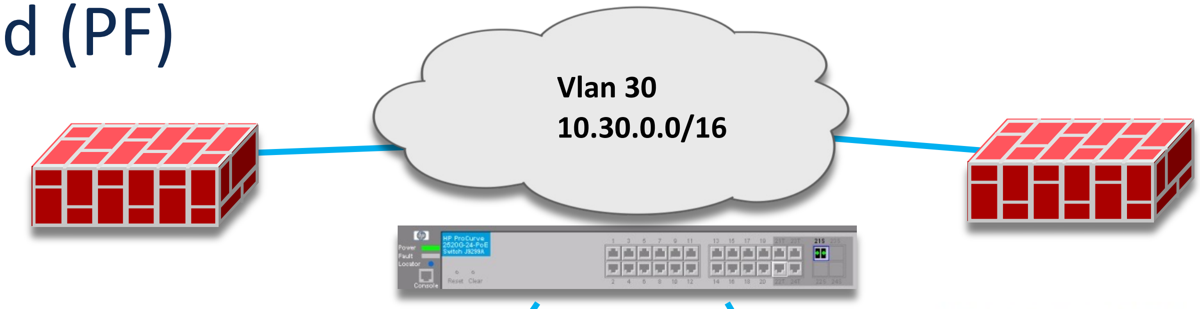
Provisioners

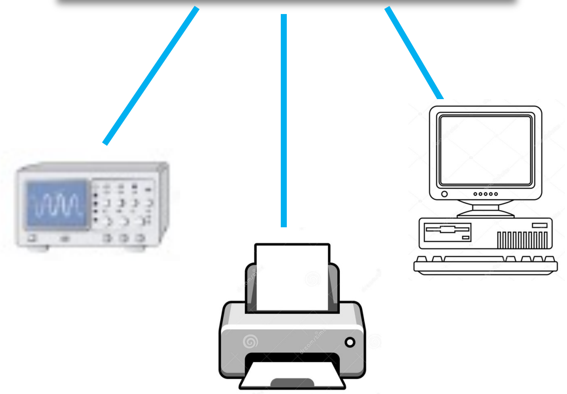
With no provisioners specified, the provisioners of the default profile will be used. Add a provisioner.

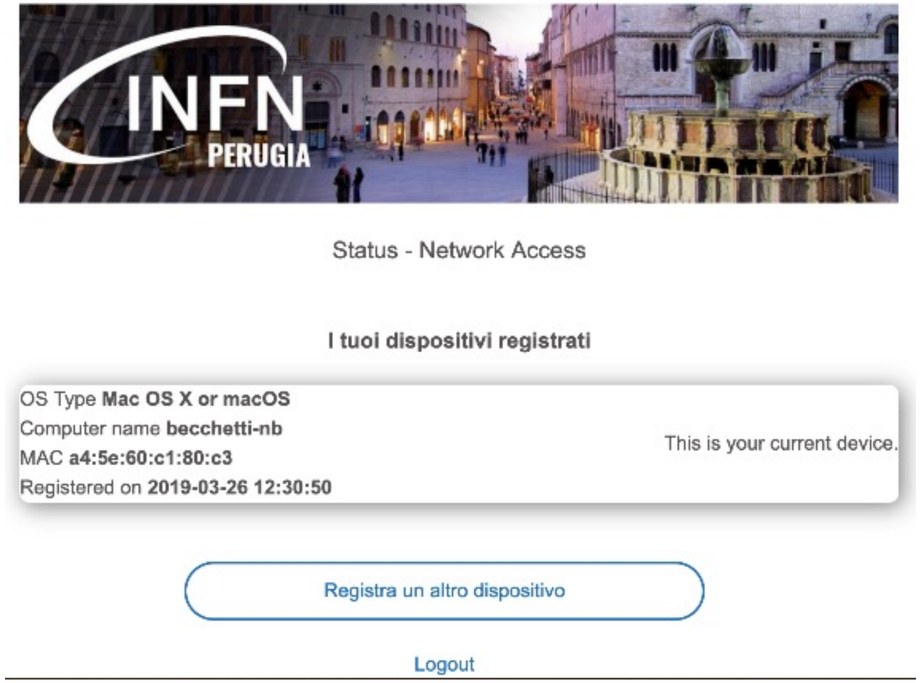
Scanners

With no scan specified, the scan engine will not be triggered. Add a Scan.

- INFN-embedded (PF)





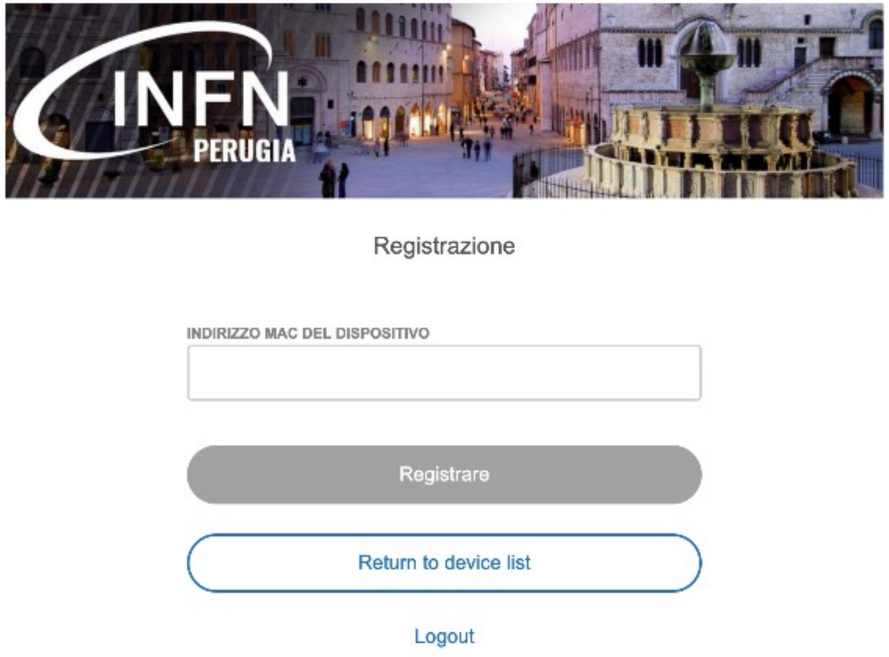


Status - Network Access

I tuoi dispositivi registrati

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

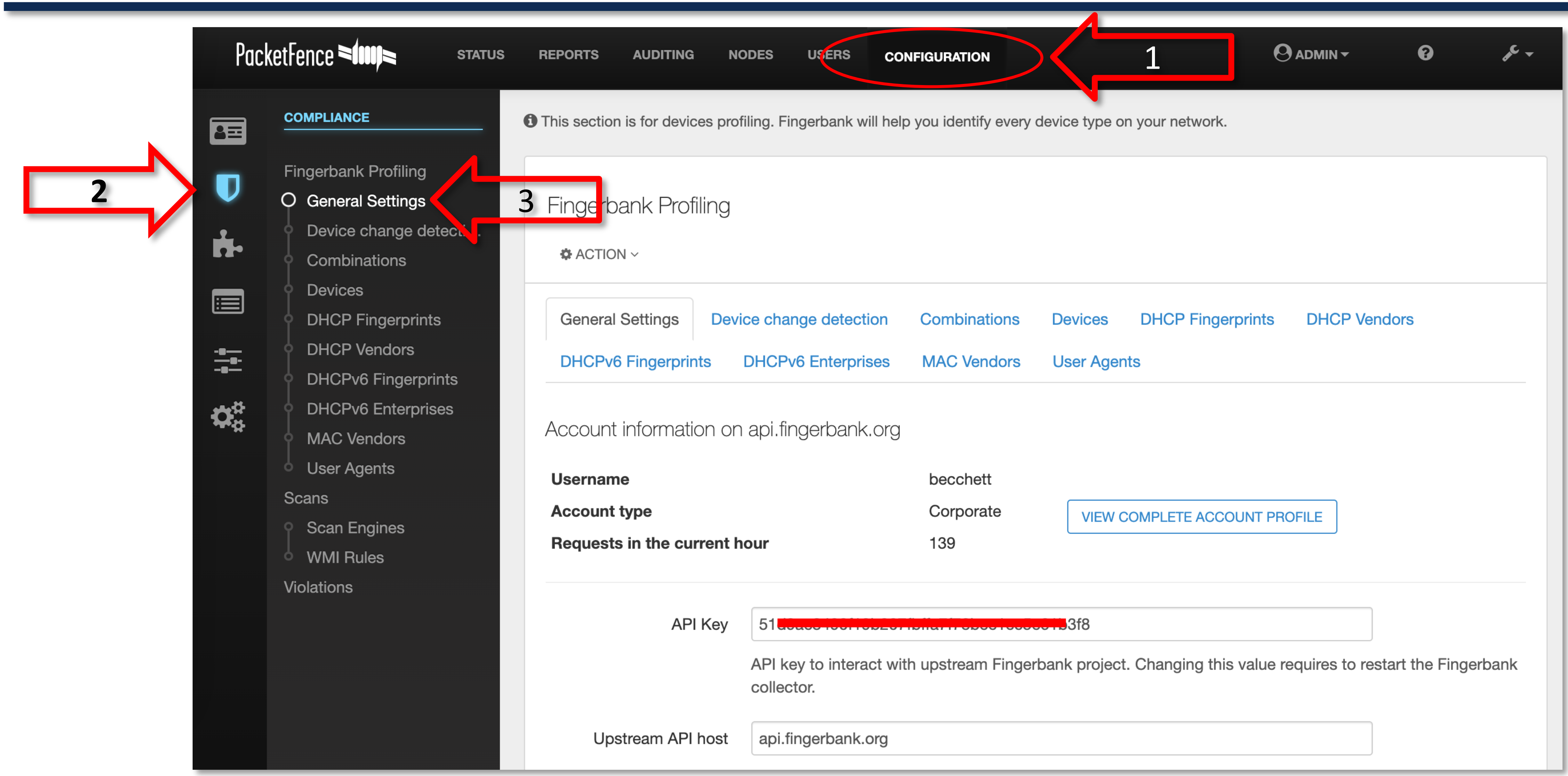
This is your current device.



Registrazione

INDIRIZZO MAC DEL DISPOSITIVO

CCR Tutorial Days 10-12 ottobre @ LNF



This section is for devices profiling. Fingerbank will help you identify every device type on your network.

Fingerbank Profiling

Account information on api.fingerbank.org

Username	becchett
Account type	Corporate
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.

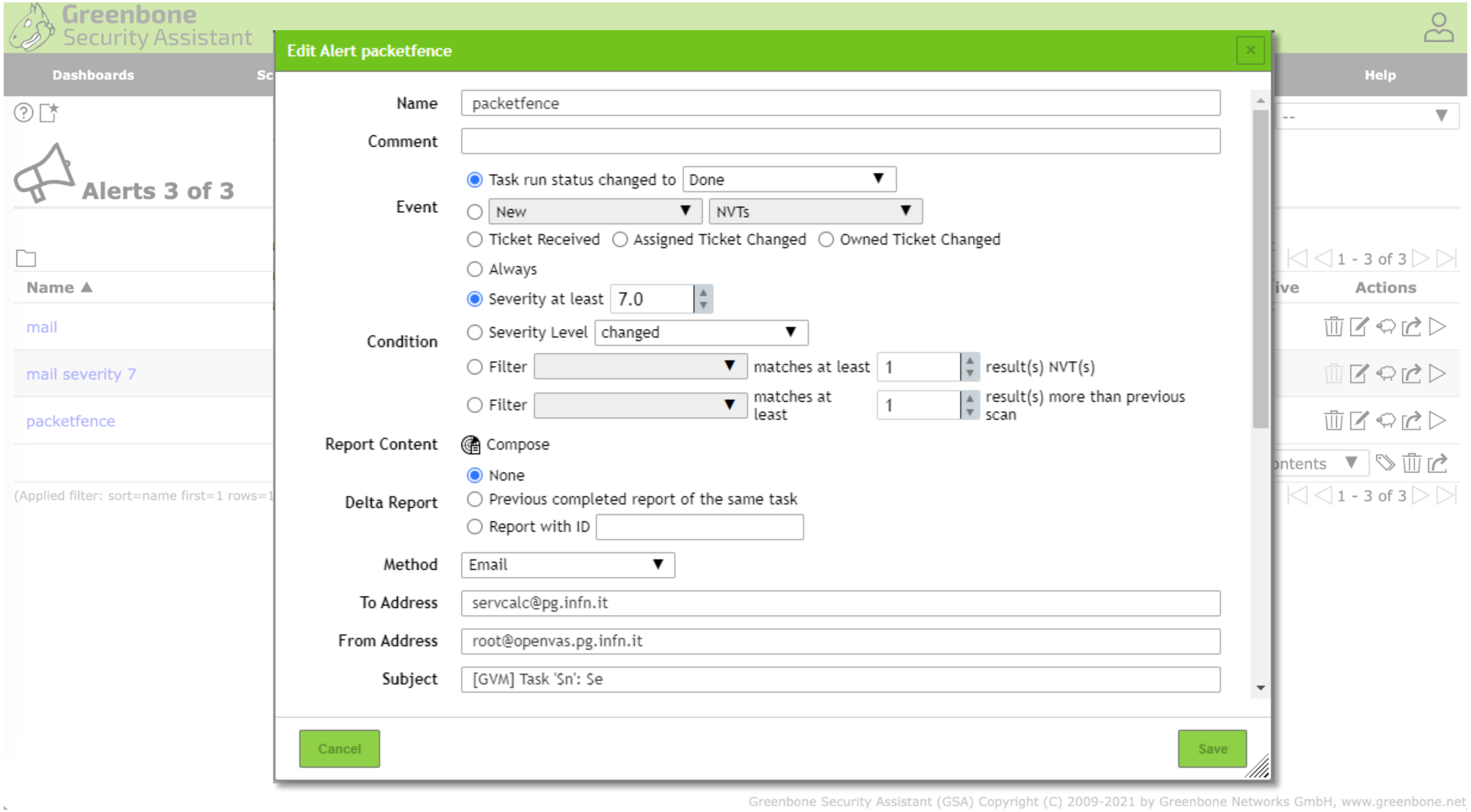
Upstream API host: api.fingerbank.org

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

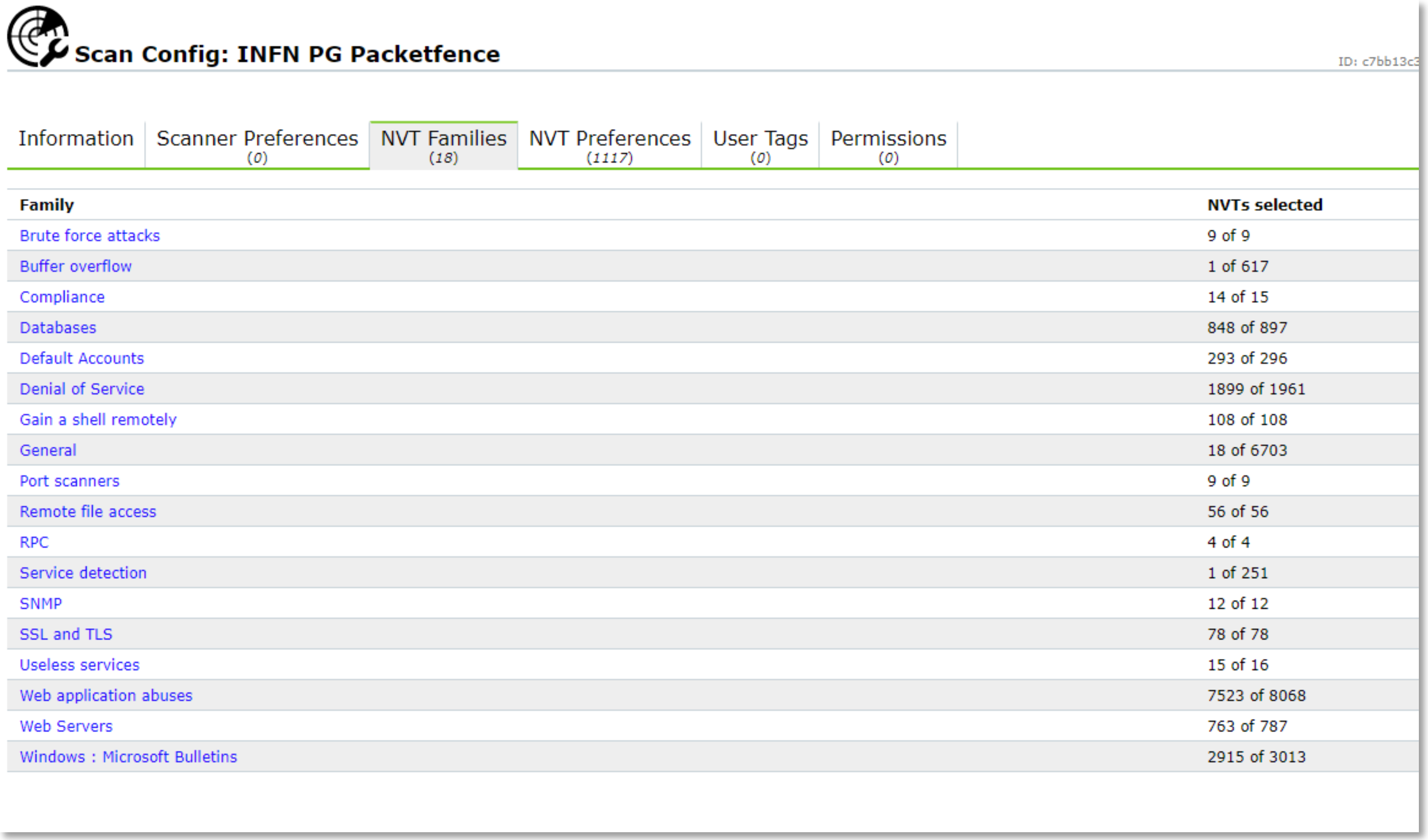
- Rete cablata -> scansioni di tutti i dispositivi
- Rete wifi -> scansione di MacOSX, Windows e Linux
- Report via mail (pdf)
- nessun accesso da remoto (ssh o altro)



Edit Alert packetfence

Name	packetfence
Comment	
Event	● Task run status changed to Done ▼ ○ New ▼ NVTs ▼ ○ Ticket Received ○ Assigned Ticket Changed ○ Owned Ticket Changed
Condition	○ Always ● Severity at least 7.0 ○ Severity Level changed ▼ ○ Filter ▼ matches at least 1 result(s) NVT(s) ○ Filter ▼ matches at least 1 result(s) more than previous scan
Report Content	Compose
Delta Report	● None ○ Previous completed report of the same task ○ Report with ID
Method	Email ▼
To Address	servcalc@pg.infn.it
From Address	root@openvas.pg.infn.it
Subject	[GVM] Task '$n': $e

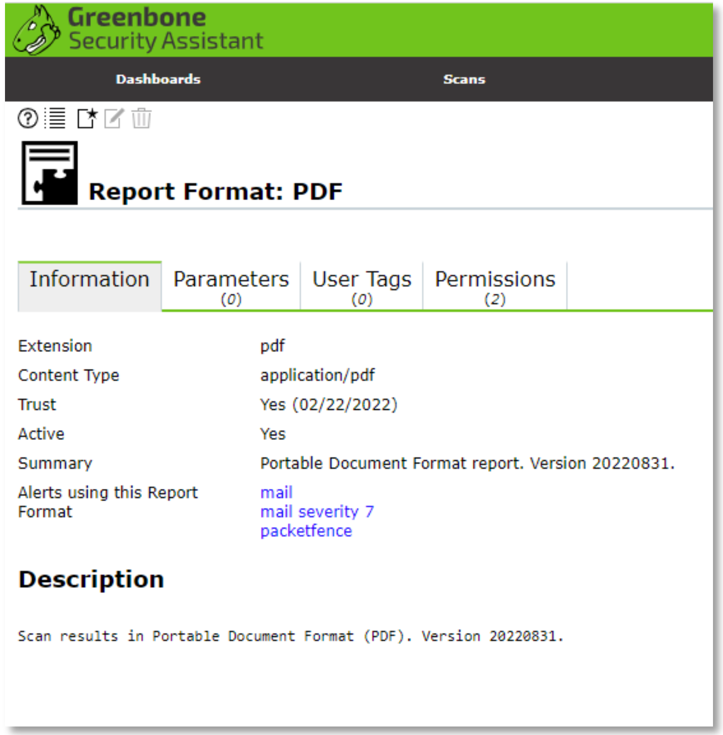
Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net



Scan Config: INFN PG Packetfence

ID: c7bb13c3

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

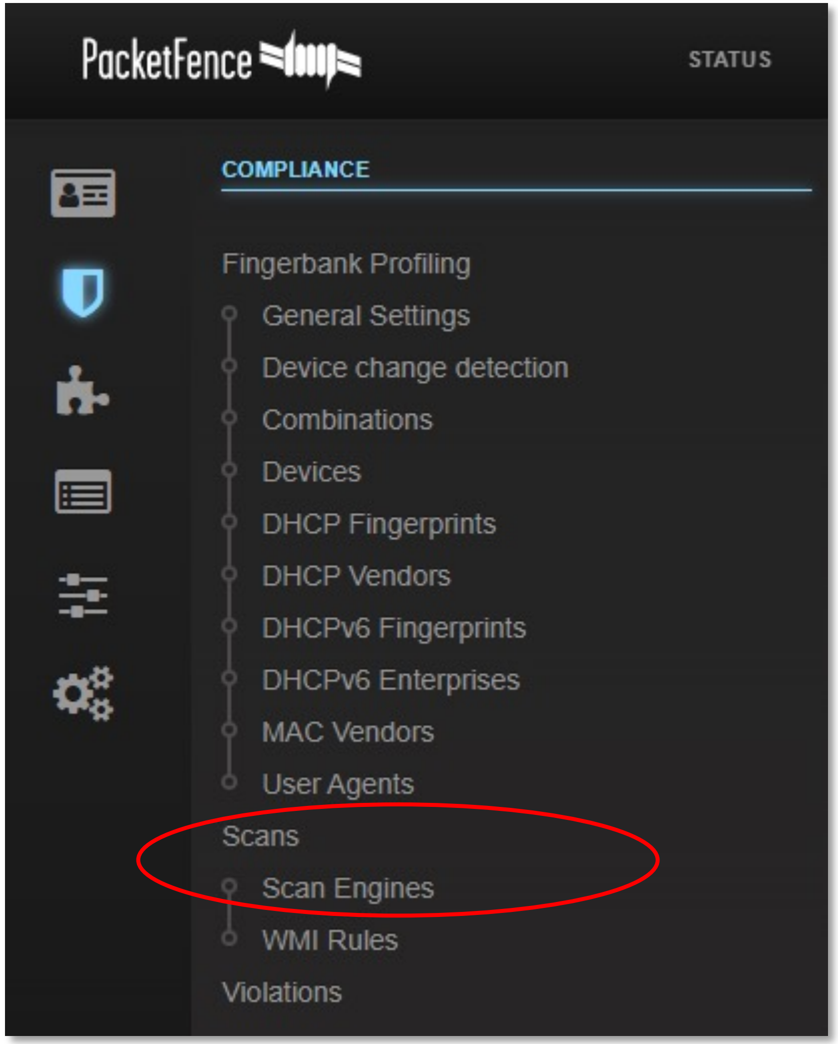


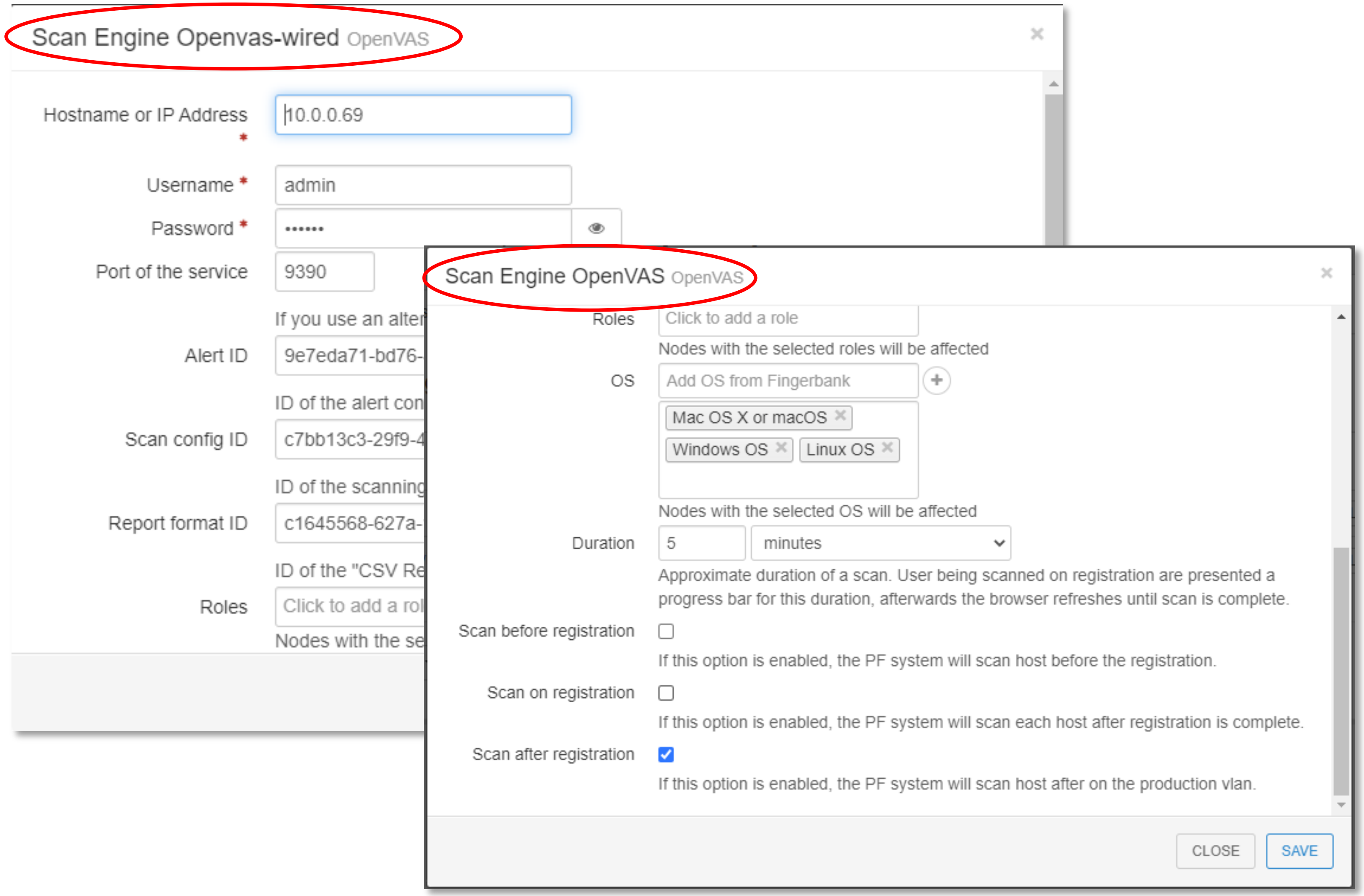
Report Format: PDF

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.





Scan Engine Openvas-wired OpenVAS

Hostname or IP Address *: 10.0.0.69

Username *: admin

Password *: ••••••

Port of the service: 9390

If you use an alter

Alert ID: 9e7eda71-bd76-

ID of the alert con

Scan config ID: c7bb13c3-29f9-4

ID of the scanning

Report format ID: c1645568-627a-

ID of the "CSV Re

Roles: Click to add a rol

Nodes with the se

Scan Engine OpenVAS OpenVAS

Roles: Click to add a role

Nodes with the selected roles will be affected

OS: Add OS from Fingerbank

Mac OS X or macOS × Windows OS × Linux OS ×

Nodes with the selected OS will be affected

Duration: 5 minutes

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 □

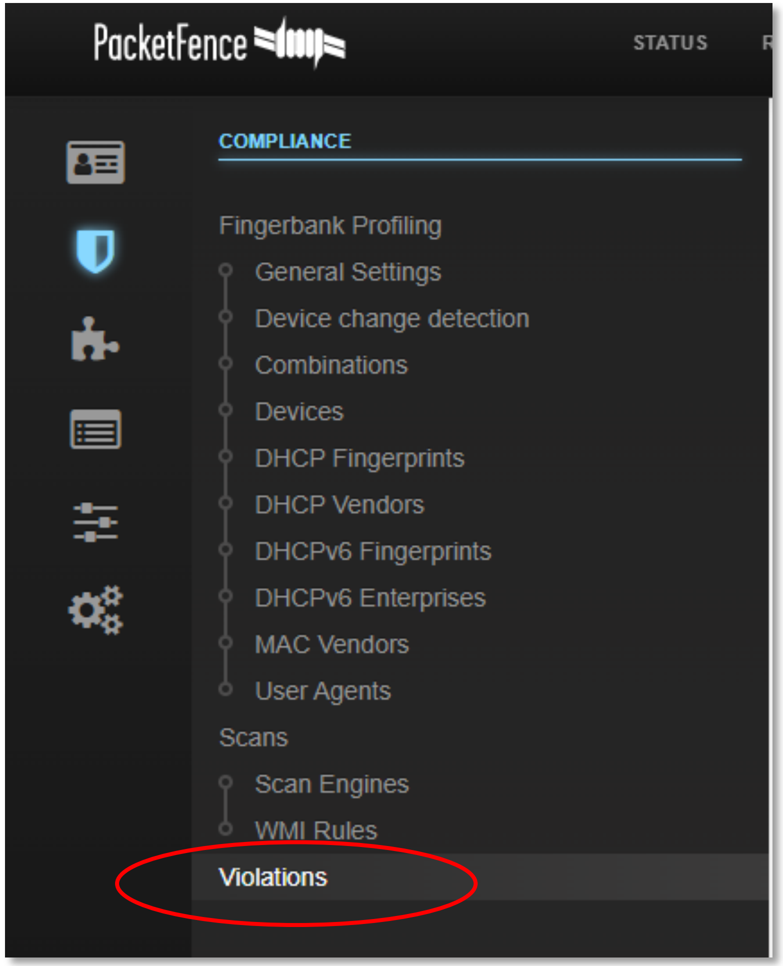
If this option is enabled, the PF system will scan host before the registration.

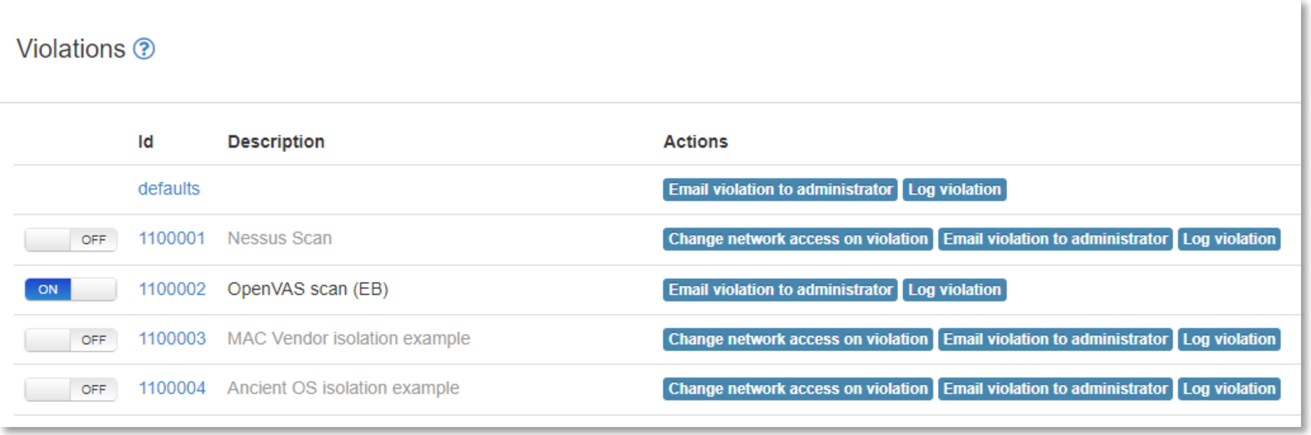
Scan on registration □

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

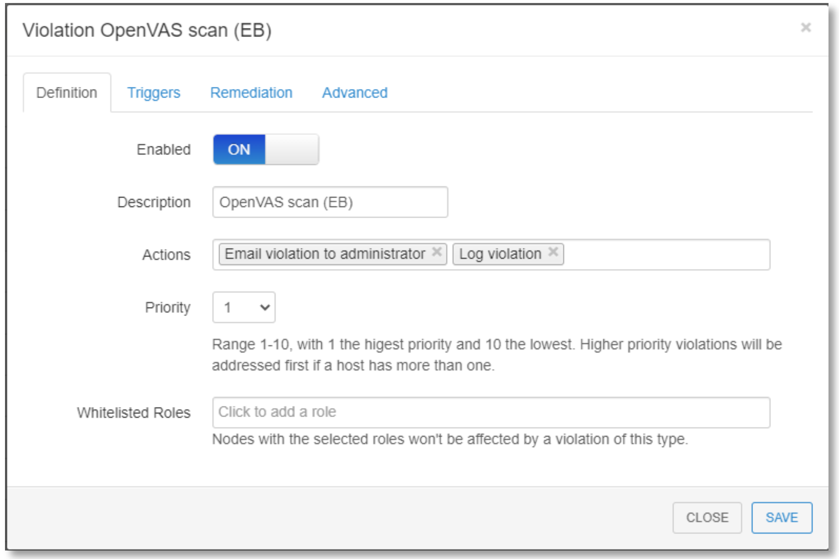
Scan after registration ☑

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




Violations

	Id	Description	Actions
	defaults		Email violation to administrator, Log violation
OFF	1100001	Nessus Scan	Change network access on violation, Email violation to administrator, Log violation
ON	1100002	OpenVAS scan (EB)	Email violation to administrator, Log violation
OFF	1100003	MAC Vendor isolation example	Change network access on violation, Email violation to administrator, Log violation
OFF	1100004	Ancient OS isolation example	Change network access on violation, Email violation to administrator, Log violation


Violation OpenVAS scan (EB)

Enabled: ON

Description: OpenVAS scan (EB)

Actions: Email violation to administrator × Log violation ×

Priority: 1

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

Whitelisted Roles: Click to add a role

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

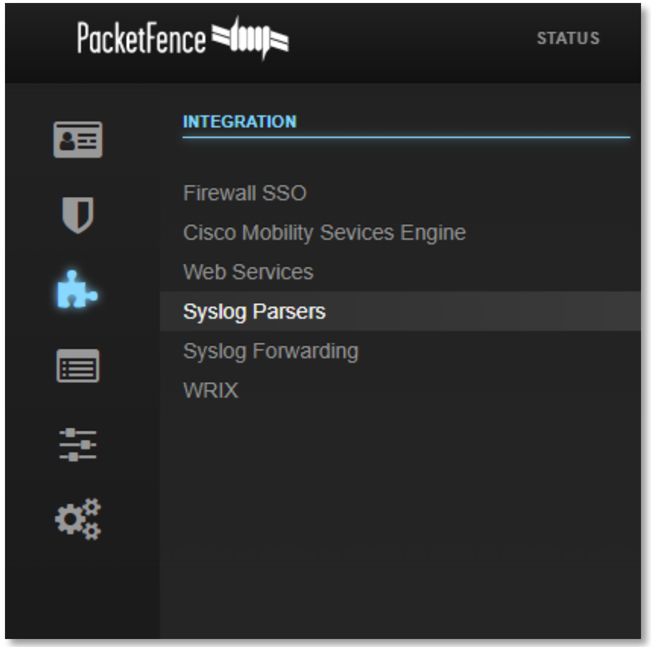
PacketFence

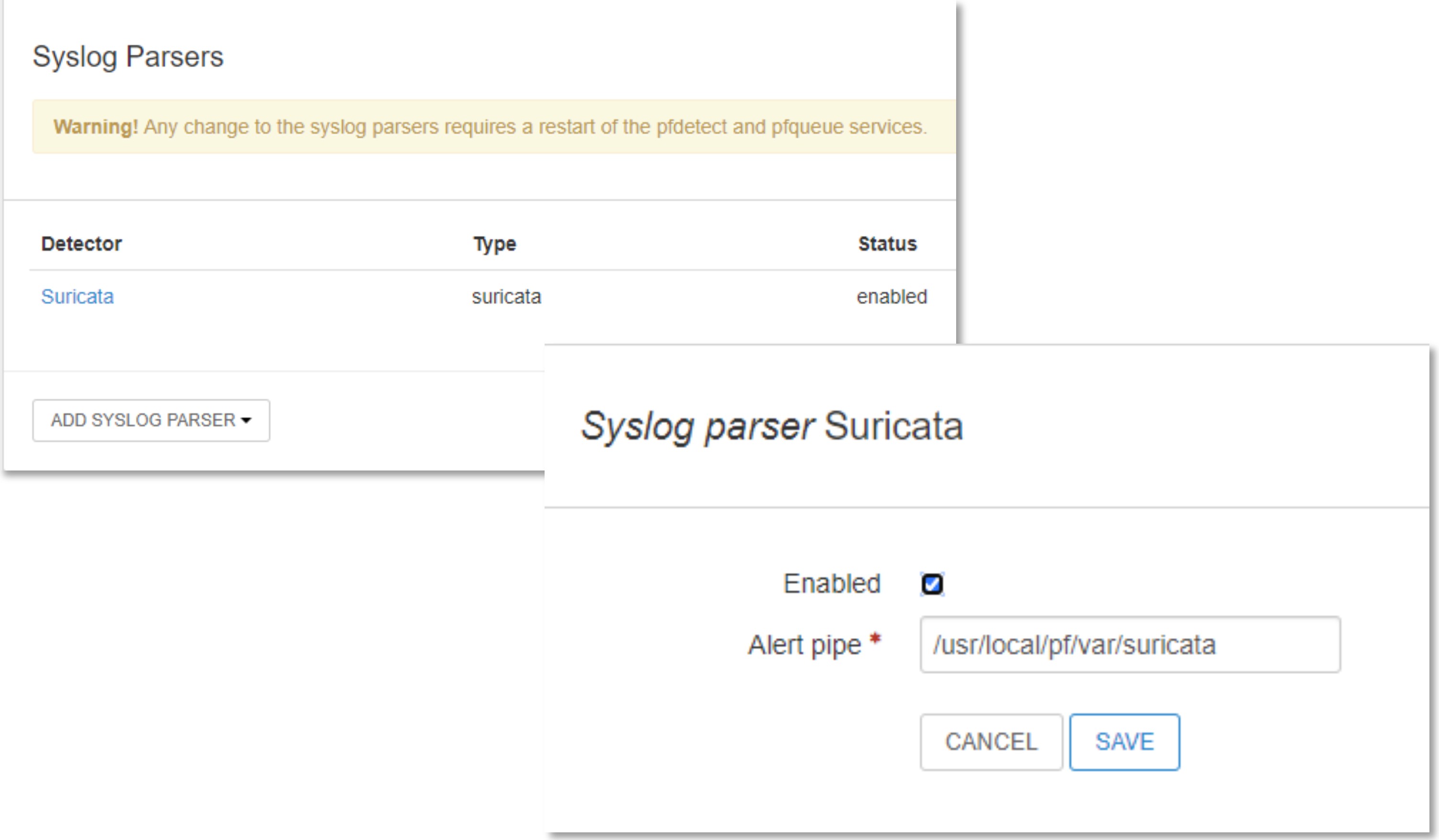
Integrazione IDS Suricata

- 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





Syslog Parsers

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

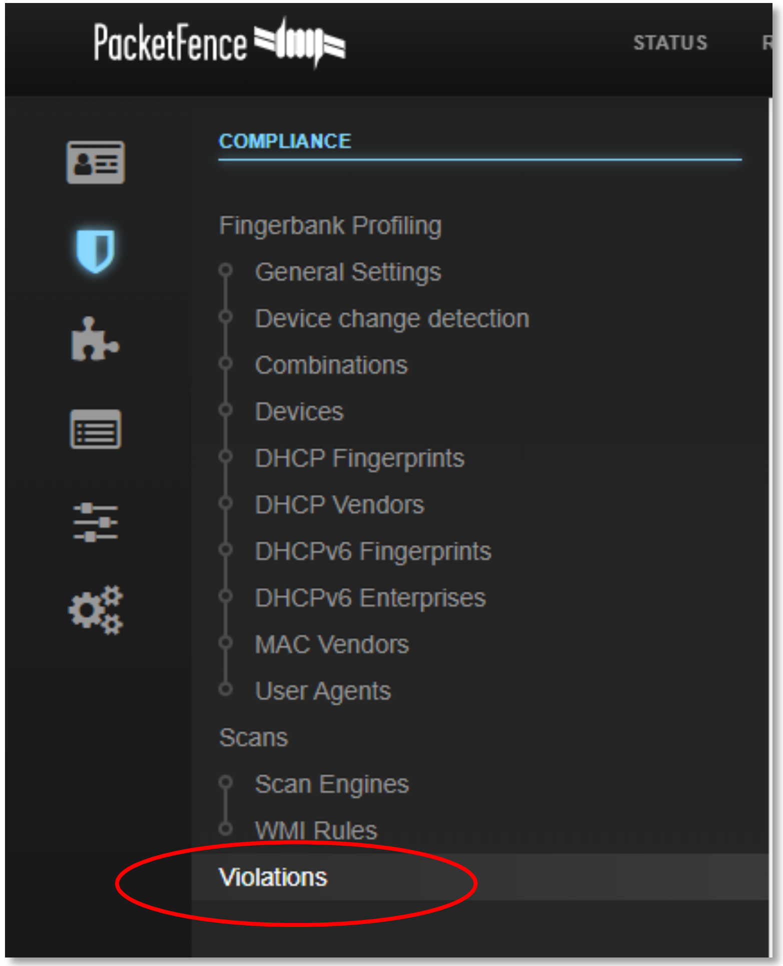
Detector	Type	Status
Suricata	suricata	enabled

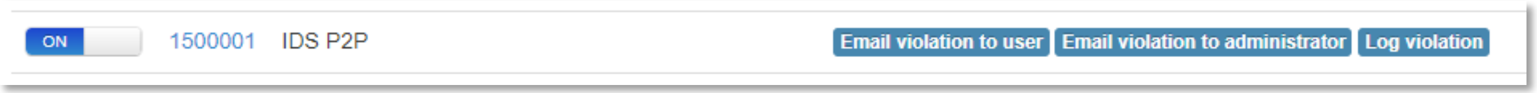
Syslog parser Suricata

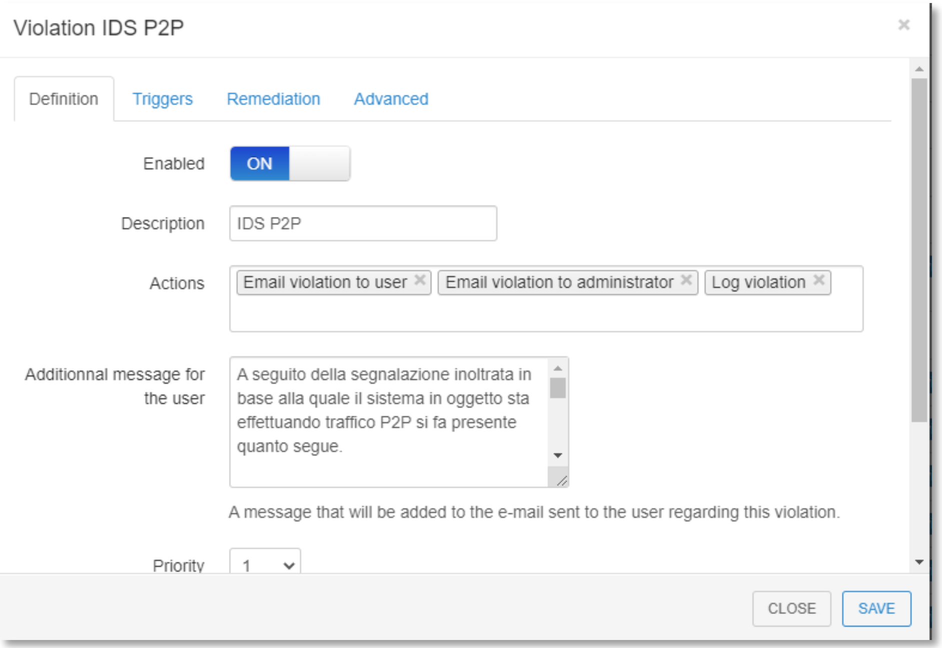
Enabled ☑

Alert pipe * /usr/local/pf/var/suricata

CCR Tutorial Days 10-12 ottobre @ LNF




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


Violation IDS P2P

Enabled: ON

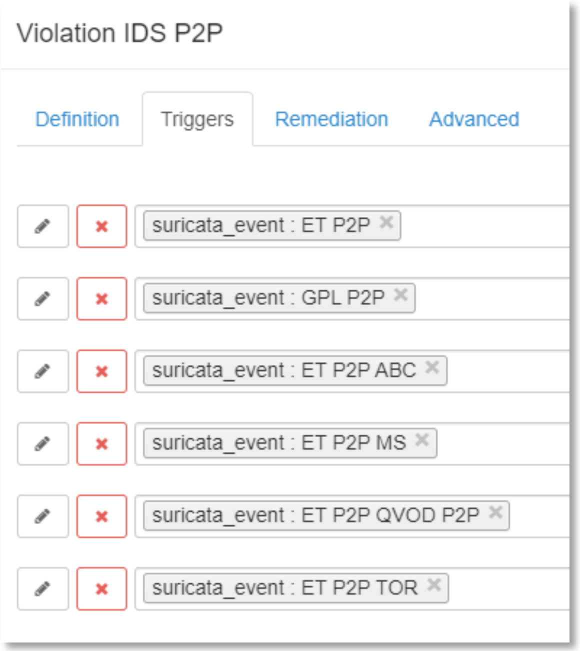
Description: IDS P2P

Actions: Email violation to user × Email violation to administrator × Log violation ×

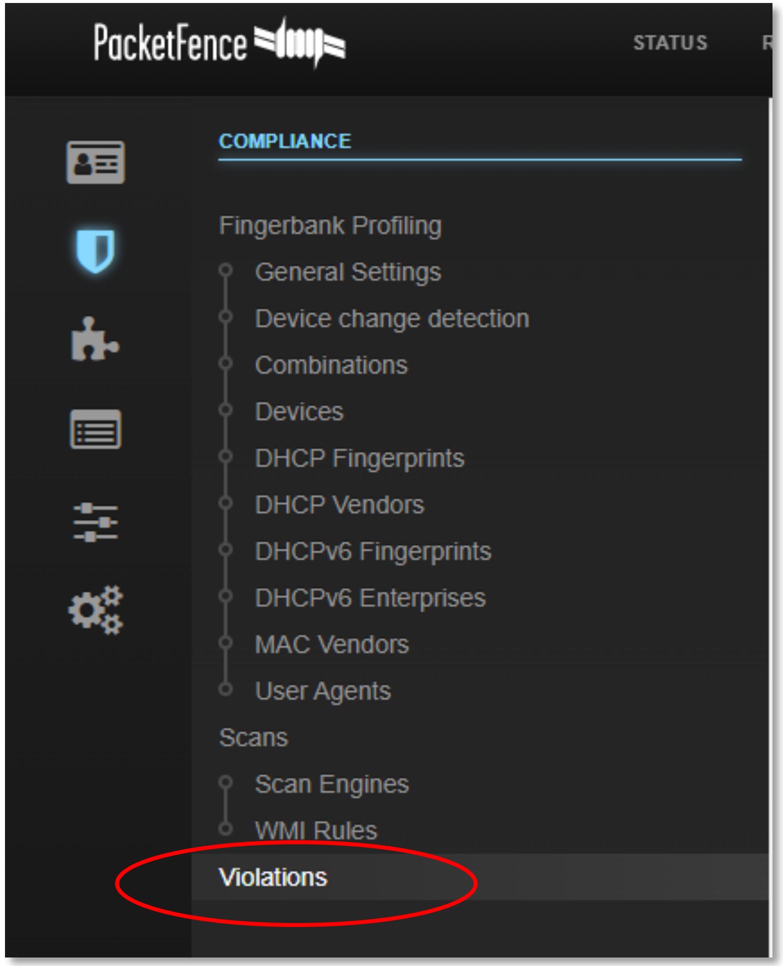
Additionnal message for the user: A seguito della segnalazione inoltrata in base alla quale il sistema in oggetto sta effettuando traffico P2P si fa presente quanto segue.

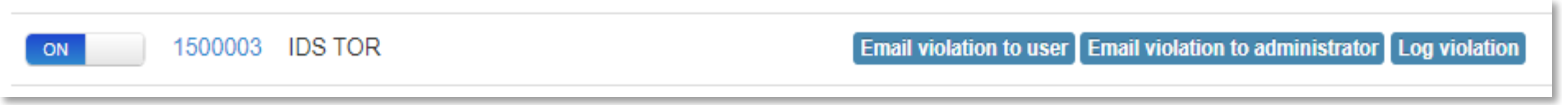
A message that will be added to the e-mail sent to the user regarding this violation.

Priority: 1

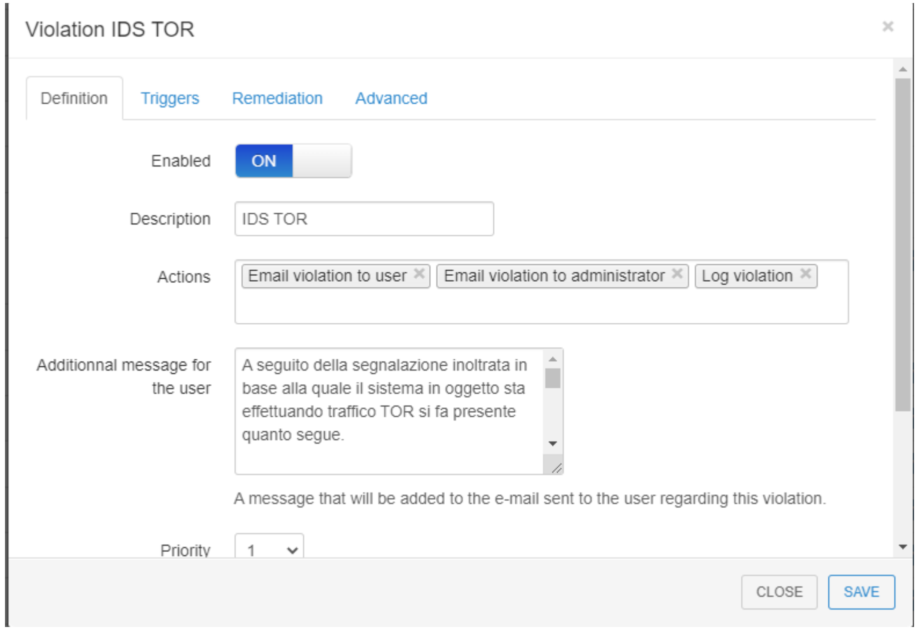

Violation IDS P2P

- suricata_event : ET P2P ×
- suricata_event : GPL P2P ×
- suricata_event : ET P2P ABC ×
- suricata_event : ET P2P MS ×
- suricata_event : ET P2P QVOD P2P ×
- suricata_event : ET P2P TOR ×





1500003 IDS TOR



Violation IDS TOR

Enabled: ON

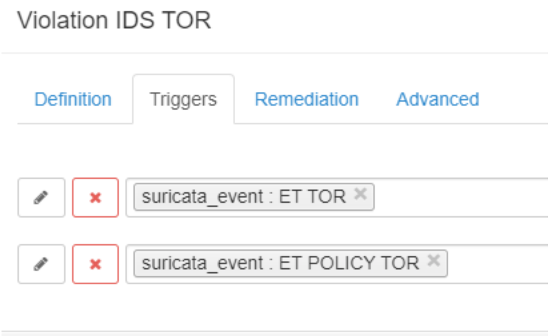
Description: IDS TOR

Actions: Email violation to user × Email violation to administrator × Log violation ×

Additionnal message for the user: A seguito della segnalazione inoltrata in base alla quale il sistema in oggetto sta effettuando traffico TOR si fa presente quanto segue.

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

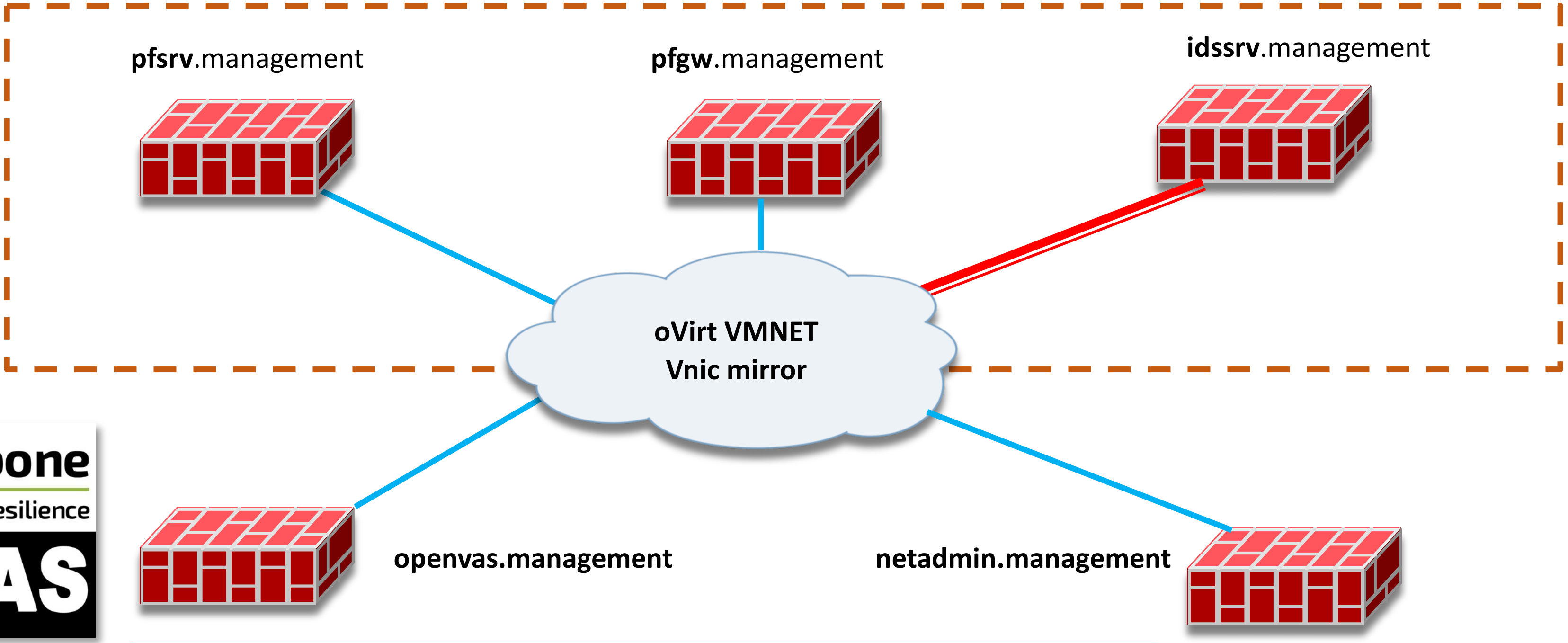
Priority: 1



Violation IDS TOR

suricata_event : ET TOR ×

suricata_event : ET POLICY TOR ×



OPENVAS

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

IDSSRV

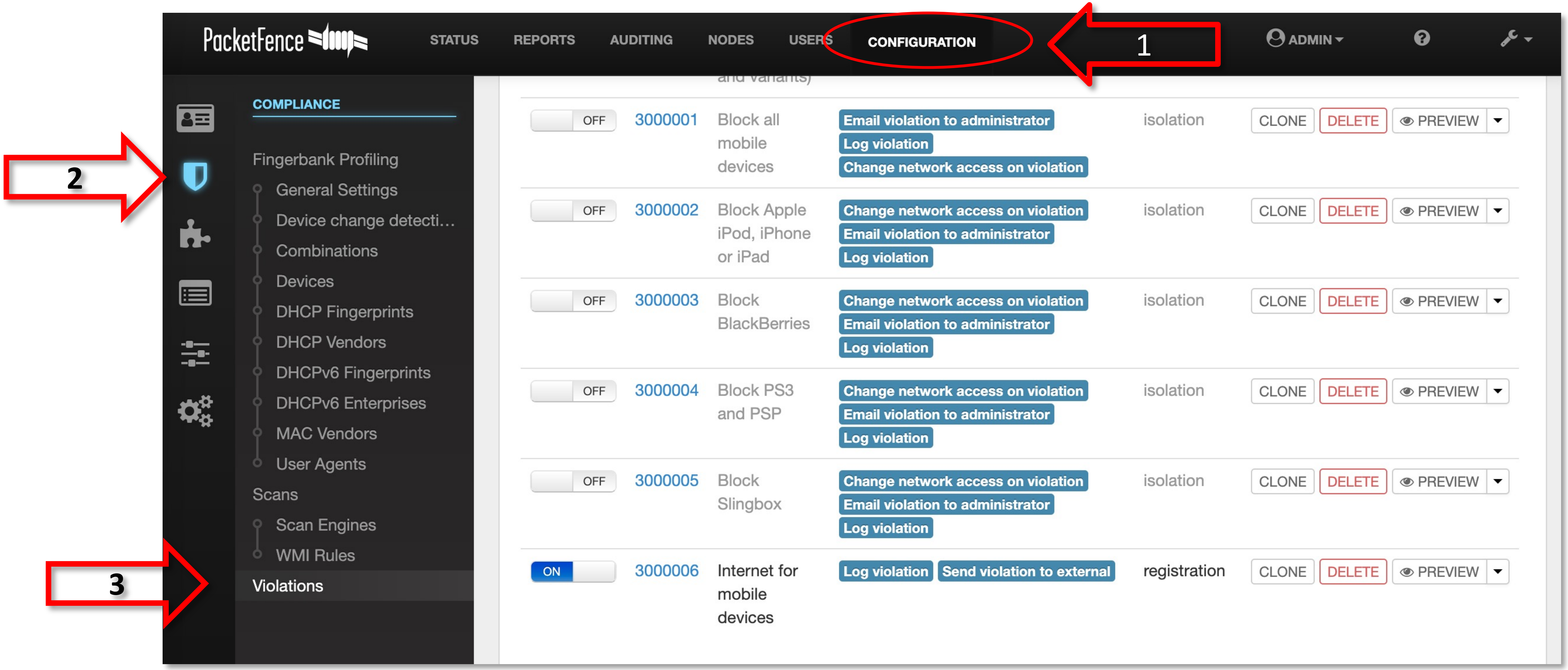
Suricata. Net Flow Analyzer -> PFSRV

PFSRV

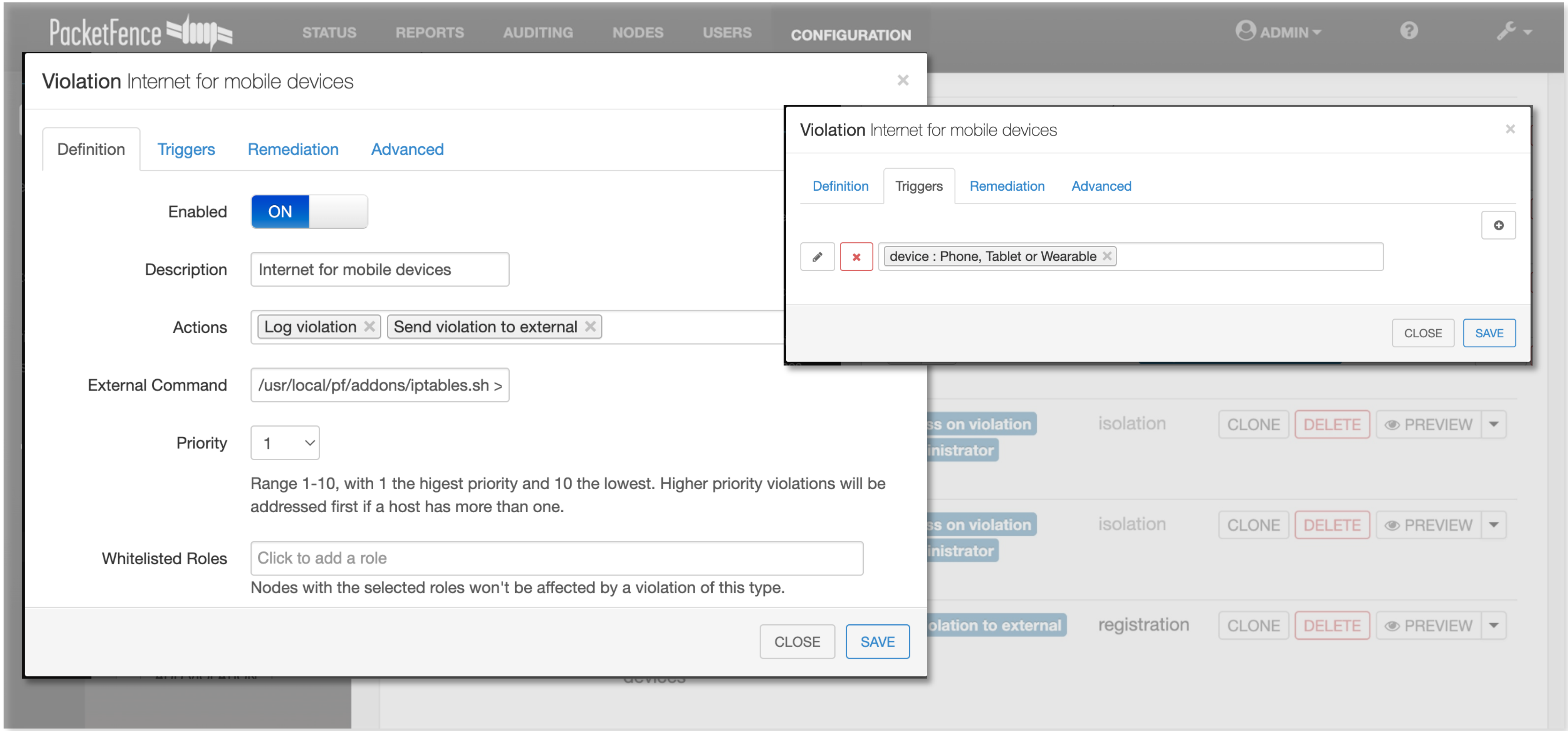
Parsing da IDSSRV -> Violation (P2P/TOR): Email to admin, log violation.

PacketFence

Smartphone/Tablet



		and variants)			
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



Violation Internet for mobile devices

Definition | Triggers | Remediation | Advanced

Enabled: ON

Description: Internet for mobile devices

Actions: Log violation × Send violation to external ×

External Command: /usr/local/pf/addons/iptables.sh >

Priority: 1

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

Whitelisted Roles: Click to add a role

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

CLOSE SAVE

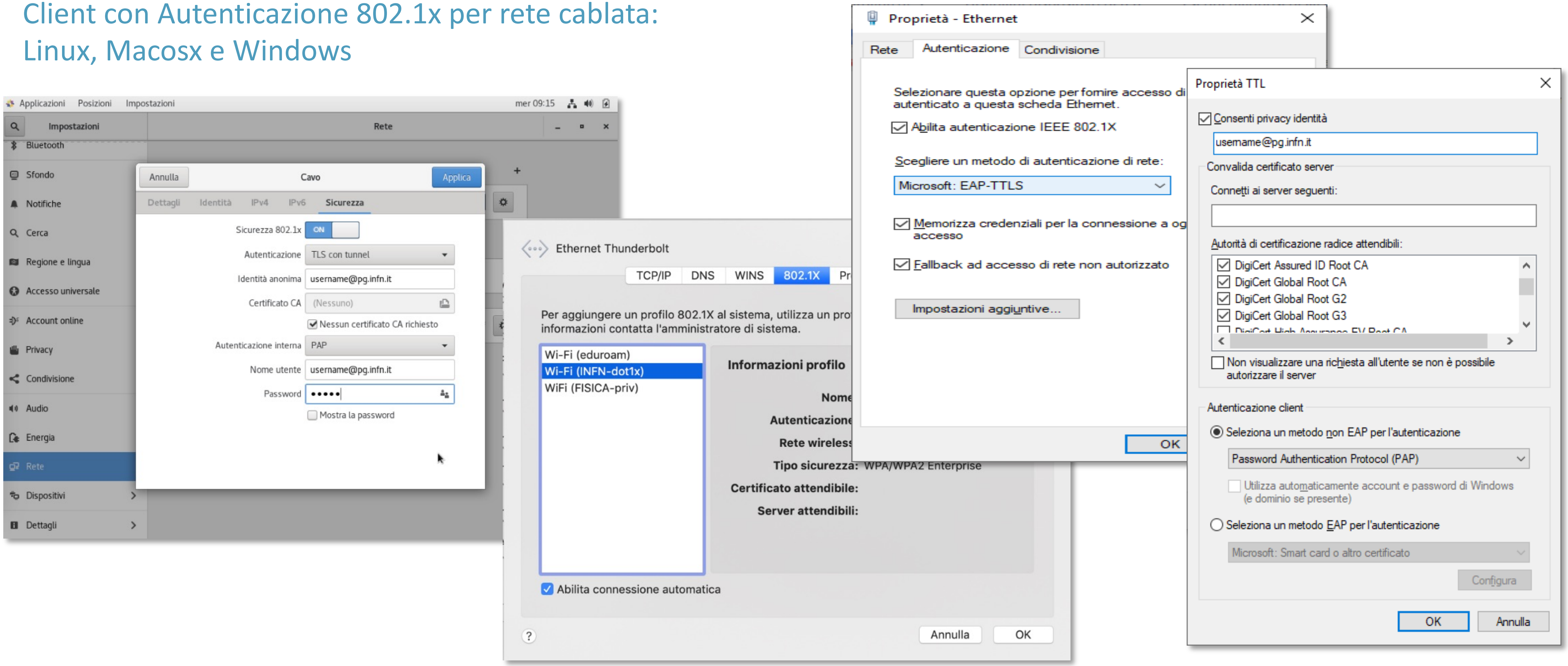
Violation Internet for mobile devices

Definition | Triggers | Remediation | Advanced

device : Phone, Tablet or Wearable ×

CLOSE SAVE

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



Sicurezza 802.1x: ON

Autenticazione: TLS con tunnel

Identità anonima: username@pg.infn.it

Certificato CA: (Nessuno)

☑ Nessun certificato CA richiesto

Autenticazione interna: PAP

Nome utente: username@pg.infn.it

Password: •••••

☐ Mostra la password

Per aggiungere un profilo 802.1X al sistema, utilizza un pro
informazioni contatta l'amministratore di sistema.

Wi-Fi (eduroam)
Wi-Fi (INFN-dot1x)
WiFi (FISICA-priv)

Informazioni profilo

Nome

Autenticazione

Rete wireless

Tipo sicurezza: WPA/WPA2 Enterprise

Certificato attendibile:

Server attendibili:

☑ Abilita connessione automatica

Selezionare questa opzione per fornire accesso di
autenticato a questa scheda Ethernet.

☑ Abilita autenticazione IEEE 802.1X

Scegliere un metodo di autenticazione di rete:

Microsoft: EAP-TTLS

☑ Memorizza credenziali per la connessione a og
accesso

☑ Fallback ad accesso di rete non autorizzato

☑ Consenti privacy identità

username@pg.infn.it

Convalida certificato server

Connetti ai server seguenti:

Autorità di certificazione radice attendibili:

☑ DigiCert Assured ID Root CA
☑ DigiCert Global Root CA
☑ DigiCert Global Root G2
☑ DigiCert Global Root G3
☐ DigiCert High Assurance EV Root CA

☐ Non visualizzare una richiesta all'utente se non è possibile autorizzare il server

Autenticazione client

● Seleziona un metodo non EAP per l'autenticazione

Password Authentication Protocol (PAP)

☐ Utilizza automaticamente account e password di Windows (e dominio se presente)

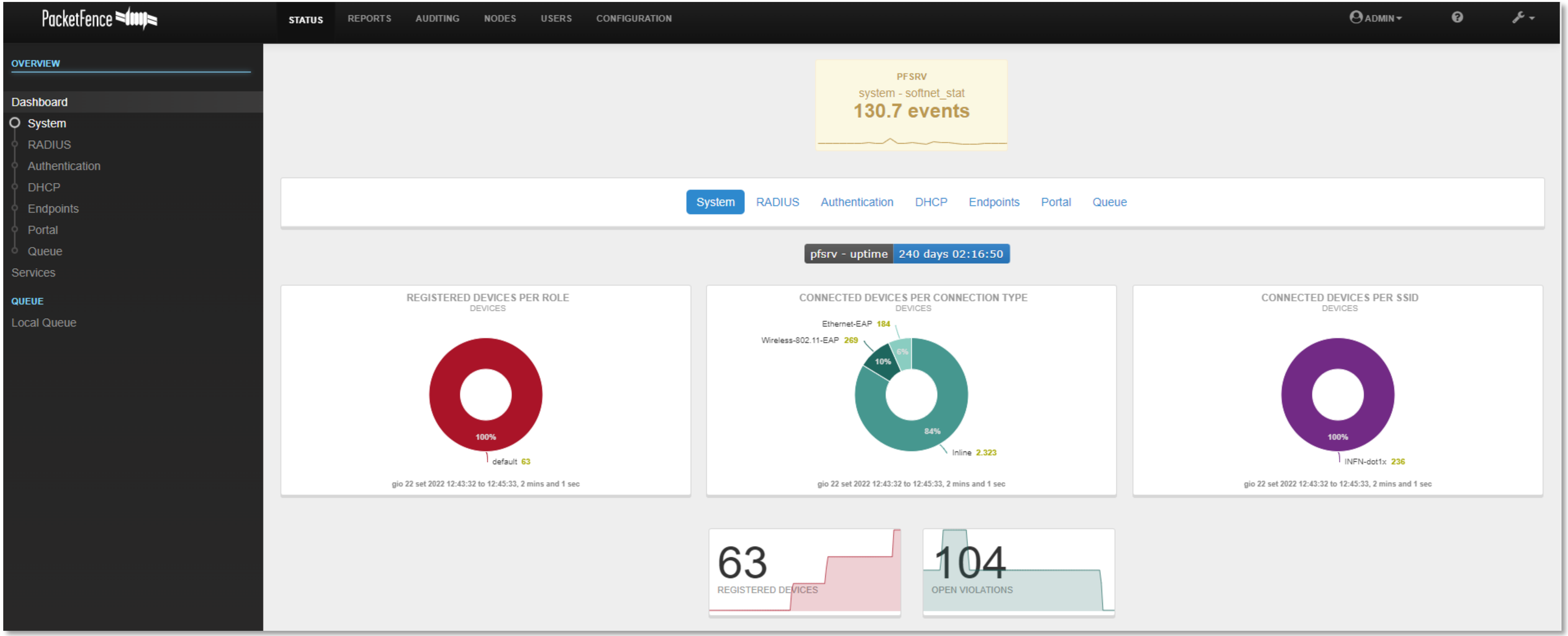
○ Seleziona un metodo EAP per l'autenticazione

Microsoft: Smart card o altro certificato

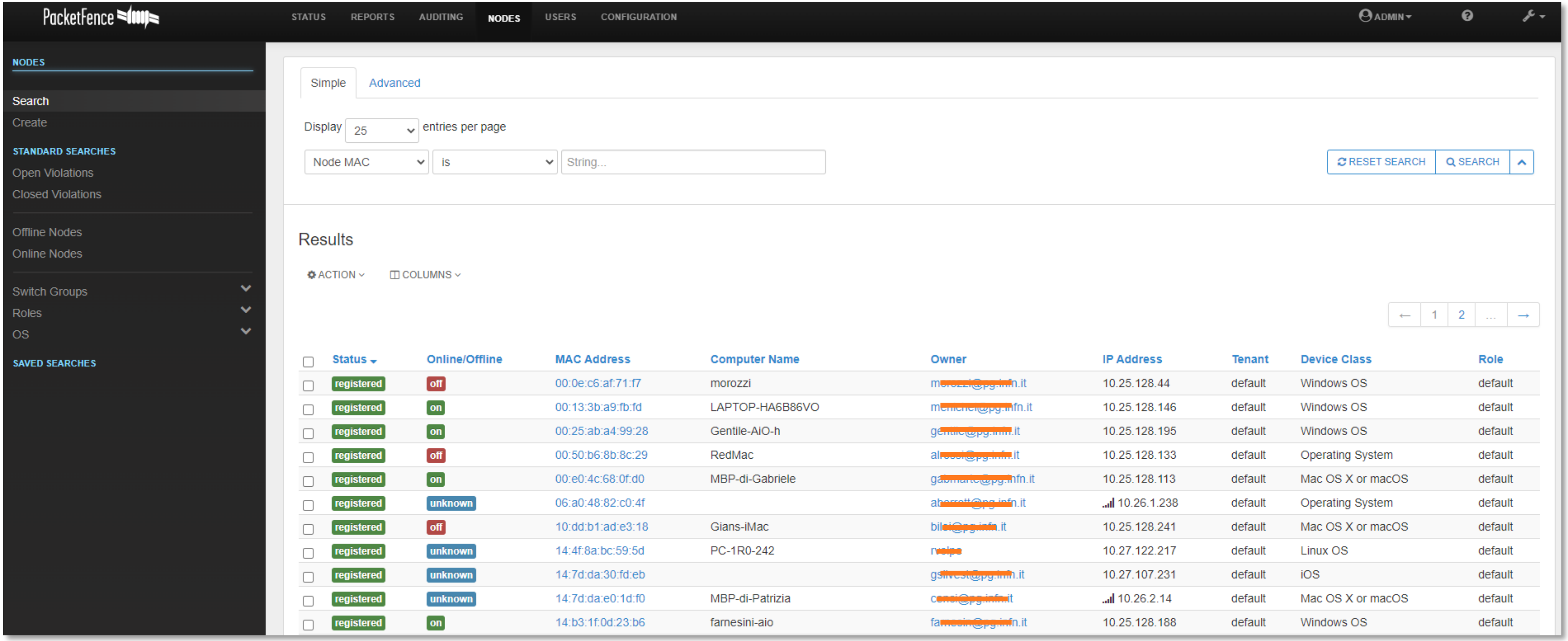
PacketFence

Dashboard

CCR Tutorial Days 10-12 ottobre @ LNF



CCR Tutorial Days 10-12 ottobre @ LNF

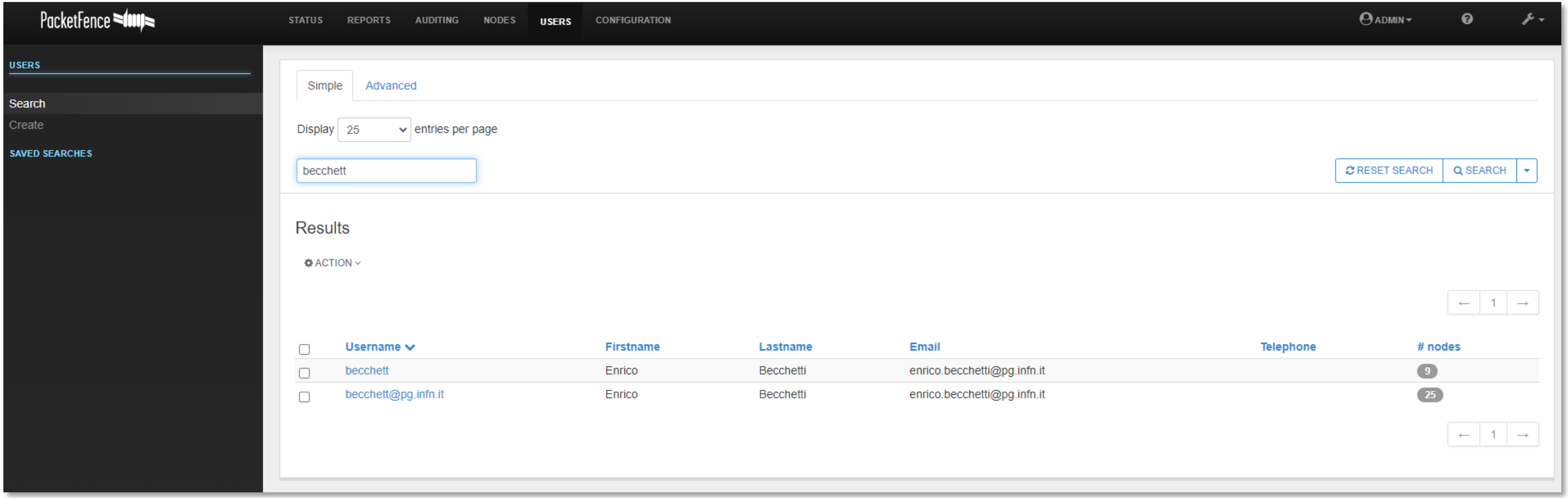


Display 25 entries per page

Node MAC | is | String...

Results

□	Status	Online/Offline	MAC Address	Computer Name	Owner	IP Address	Tenant	Device Class	Role
□	registered	off	00:0e:c6:af:71:f7	morozzi	[redacted]	10.25.128.44	default	Windows OS	default
□	registered	on	00:13:3b:a9:fb:fd	LAPTOP-HA6B86VO	[redacted]	10.25.128.146	default	Windows OS	default
□	registered	on	00:25:ab:a4:99:28	Gentile-AiO-h	[redacted]	10.25.128.195	default	Windows OS	default
□	registered	off	00:50:b6:8b:8c:29	RedMac	[redacted]	10.25.128.133	default	Operating System	default
□	registered	on	00:e0:4c:68:0f:d0	MBP-di-Gabriele	[redacted]	10.25.128.113	default	Mac OS X or macOS	default
□	registered	unknown	06:a0:48:82:c0:4f		[redacted]	10.26.1.238	default	Operating System	default
□	registered	off	10:dd:b1:ad:e3:18	Gians-iMac	[redacted]	10.25.128.241	default	Mac OS X or macOS	default
□	registered	unknown	14:4f:8a:bc:59:5d	PC-1R0-242	[redacted]	10.27.122.217	default	Linux OS	default
□	registered	unknown	14:7d:da:30:fd:eb		[redacted]	10.27.107.231	default	iOS	default
□	registered	unknown	14:7d:da:e0:1d:f0	MBP-di-Patrizia	[redacted]	10.26.2.14	default	Mac OS X or macOS	default
□	registered	on	14:b3:1f:0d:23:b6	farnesini-aio	[redacted]	10.25.128.188	default	Windows OS	default

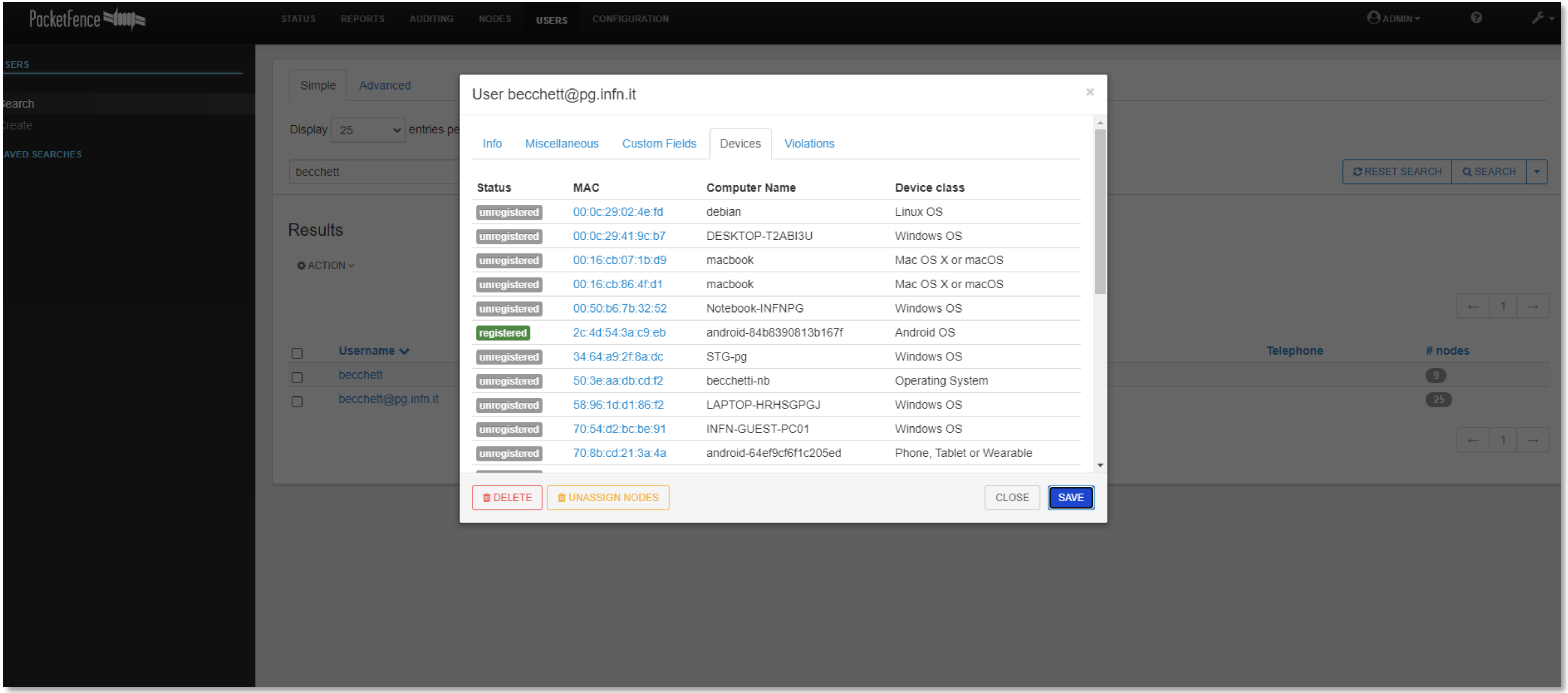


Display 25 entries per page

becchett

Results

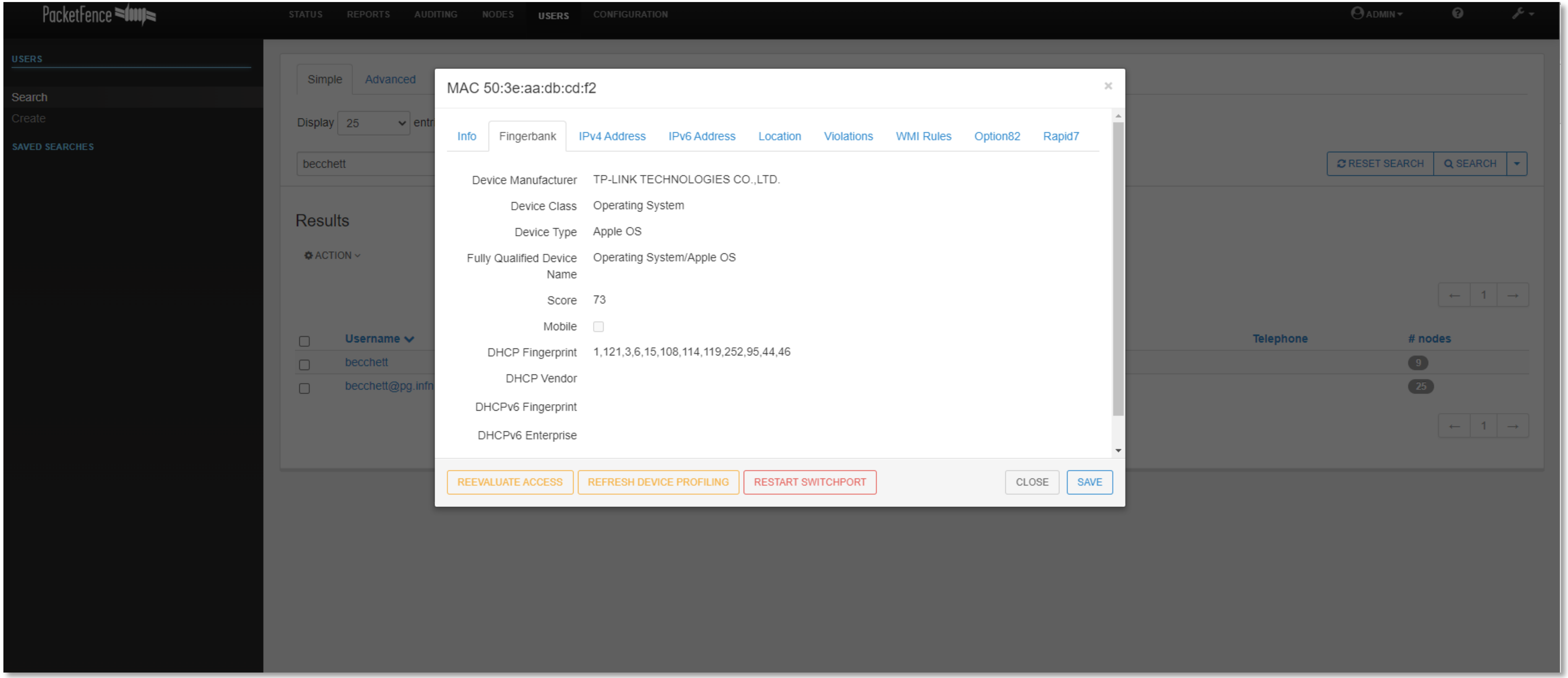
	Username	Firstname	Lastname	Email	Telephone	# nodes
□	becchett	Enrico	Becchetti	enrico.becchetti@pg.infn.it		9
□	becchett@pg.infn.it	Enrico	Becchetti	enrico.becchetti@pg.infn.it		25



User 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

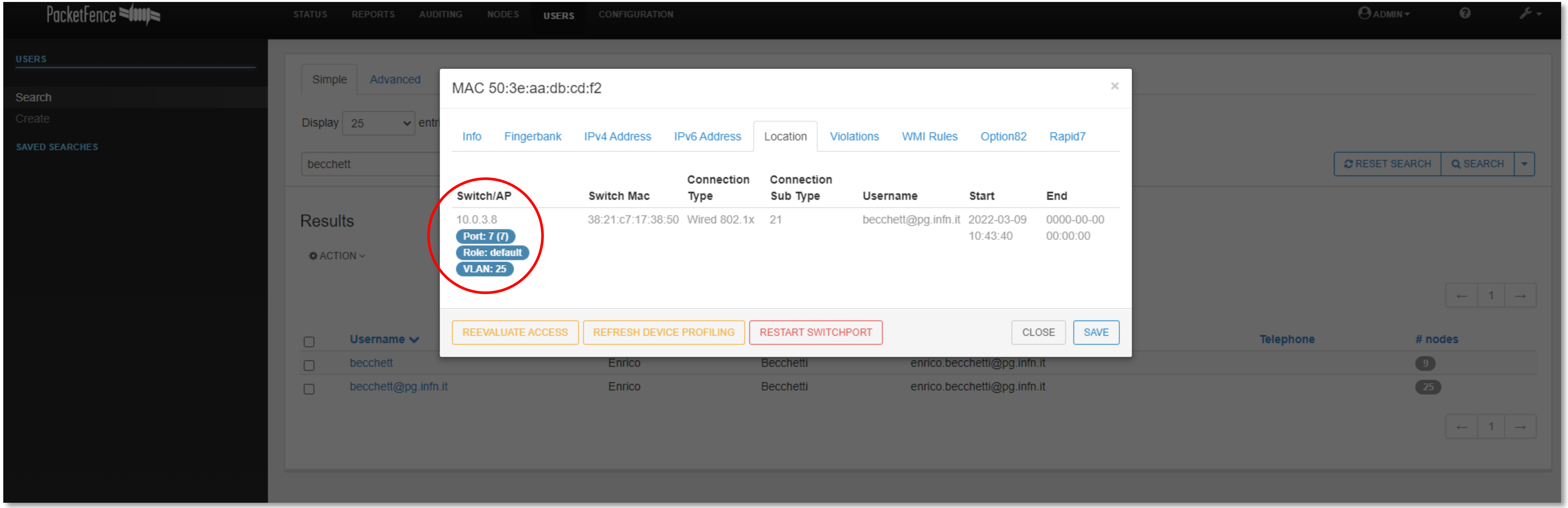
CCR Tutorial Days 10-12 ottobre @ LNF



MAC 50:3e:aa:db:cd:f2

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	

CCR Tutorial Days 10-12 ottobre @ LNF

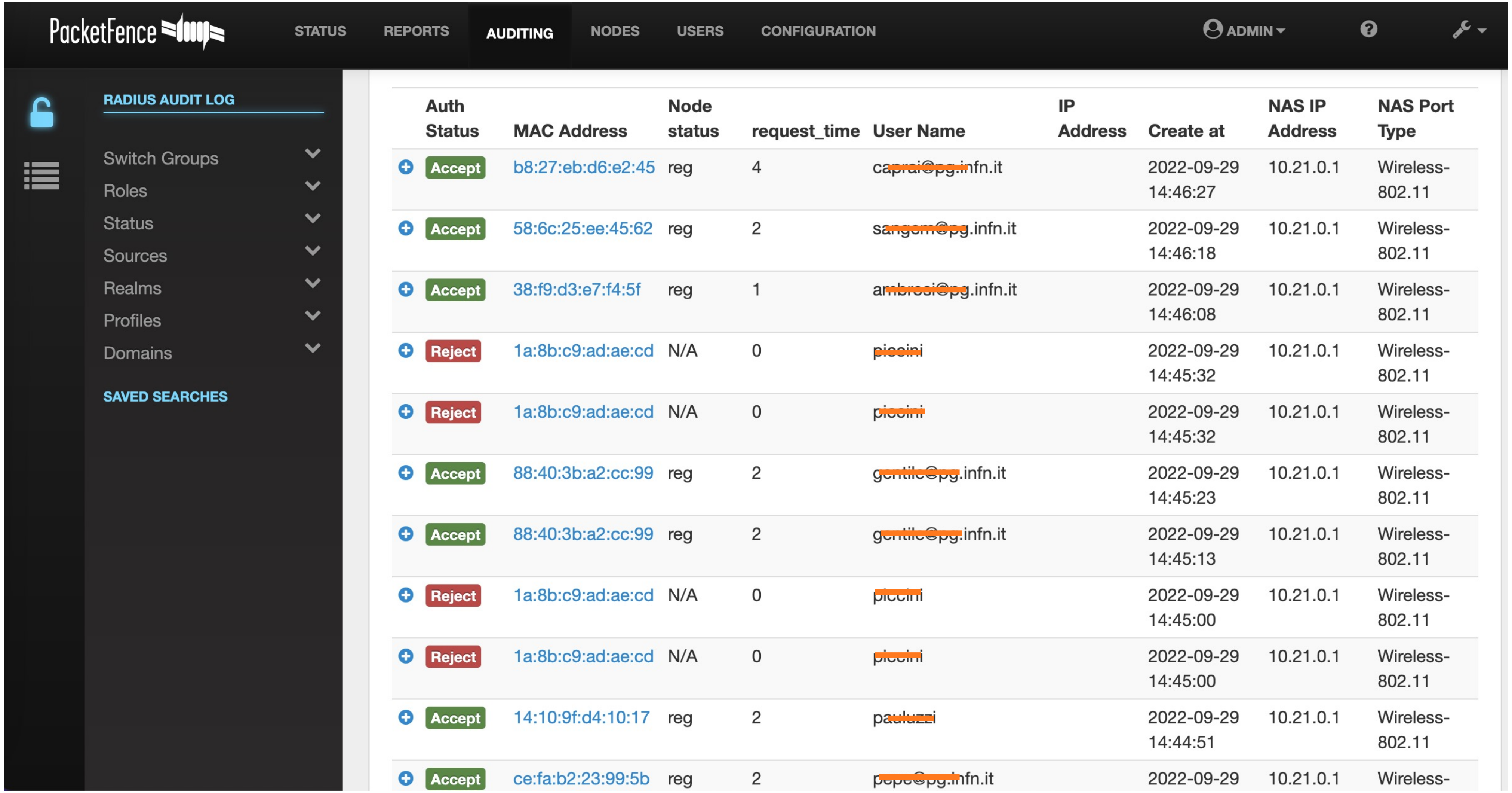


becchett

MAC 50:3e:aa:db:cd:f2

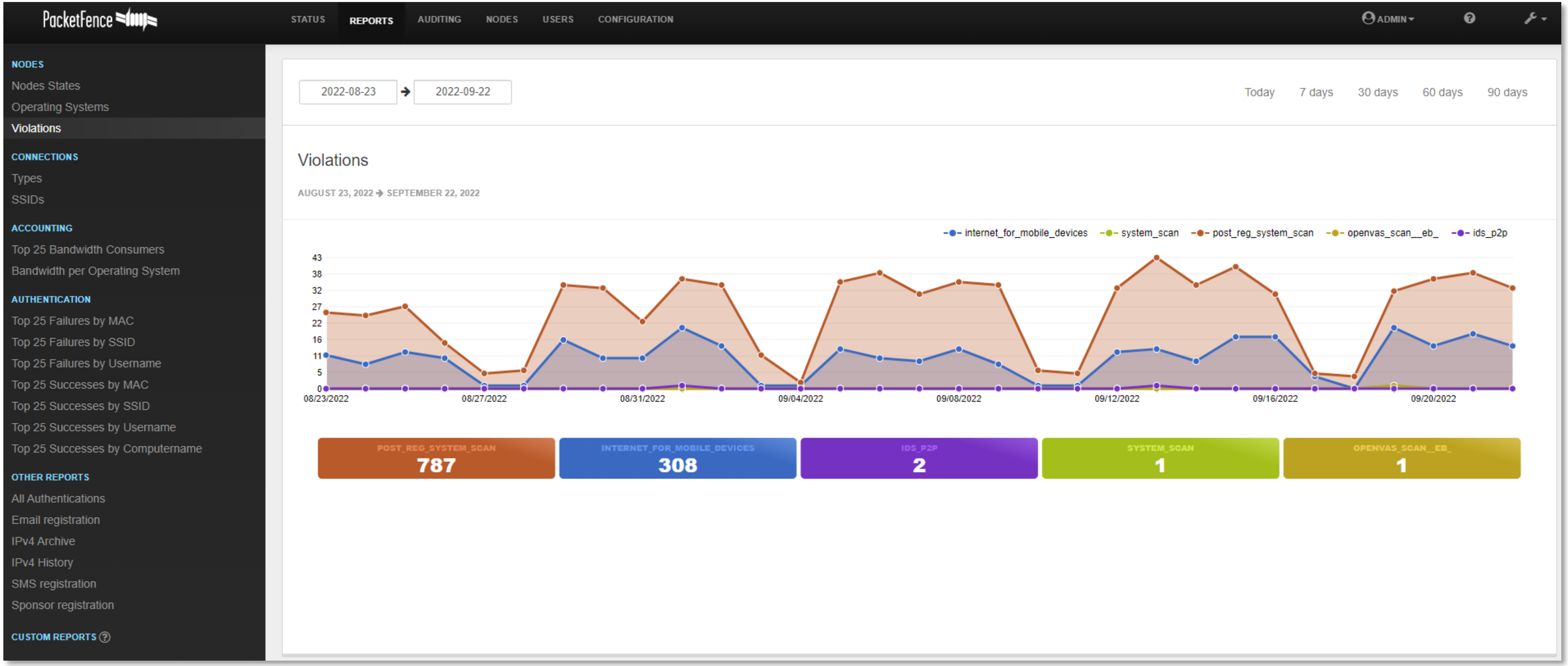
Switch/AP	Switch Mac	Connection Type	Connection Sub Type	Username	Start	End
10.0.3.8 Port: 7 (7) Role: default VLAN: 25	38:21:c7:17:38:50	Wired 802.1x	21	becchett@pg.infn.it	2022-03-09 10:43:40	0000-00-00 00:00:00

Username				Telephone	# nodes
becchett	Enrico	Becchetti	enrico.becchetti@pg.infn.it		9
becchett@pg.infn.it	Enrico	Becchetti	enrico.becchetti@pg.infn.it		25



	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	ca[redacted]nfn.it		2022-09-29 14:46:27	10.21.0.1	Wireless-802.11
+	Accept	58:6c:25:ee:45:62	reg	2	sa[redacted].infn.it		2022-09-29 14:46:18	10.21.0.1	Wireless-802.11
+	Accept	38:f9:d3:e7:f4:5f	reg	1	a[redacted].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	[redacted]		2022-09-29 14:45:32	10.21.0.1	Wireless-802.11
+	Reject	1a:8b:c9:ad:ae:cd	N/A	0	[redacted]		2022-09-29 14:45:32	10.21.0.1	Wireless-802.11
+	Accept	88:40:3b:a2:cc:99	reg	2	g[redacted].infn.it		2022-09-29 14:45:23	10.21.0.1	Wireless-802.11
+	Accept	88:40:3b:a2:cc:99	reg	2	g[redacted].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	[redacted]		2022-09-29 14:45:00	10.21.0.1	Wireless-802.11
+	Reject	1a:8b:c9:ad:ae:cd	N/A	0	[redacted]		2022-09-29 14:45:00	10.21.0.1	Wireless-802.11
+	Accept	14:10:9f:d4:10:17	reg	2	pa[redacted]i		2022-09-29 14:44:51	10.21.0.1	Wireless-802.11
+	Accept	ce:fa:b2:23:99:5b	reg	2	[redacted]nfn.it		2022-09-29	10.21.0.1	Wireless-

CCR Tutorial Days 10-12 ottobre @ LNF



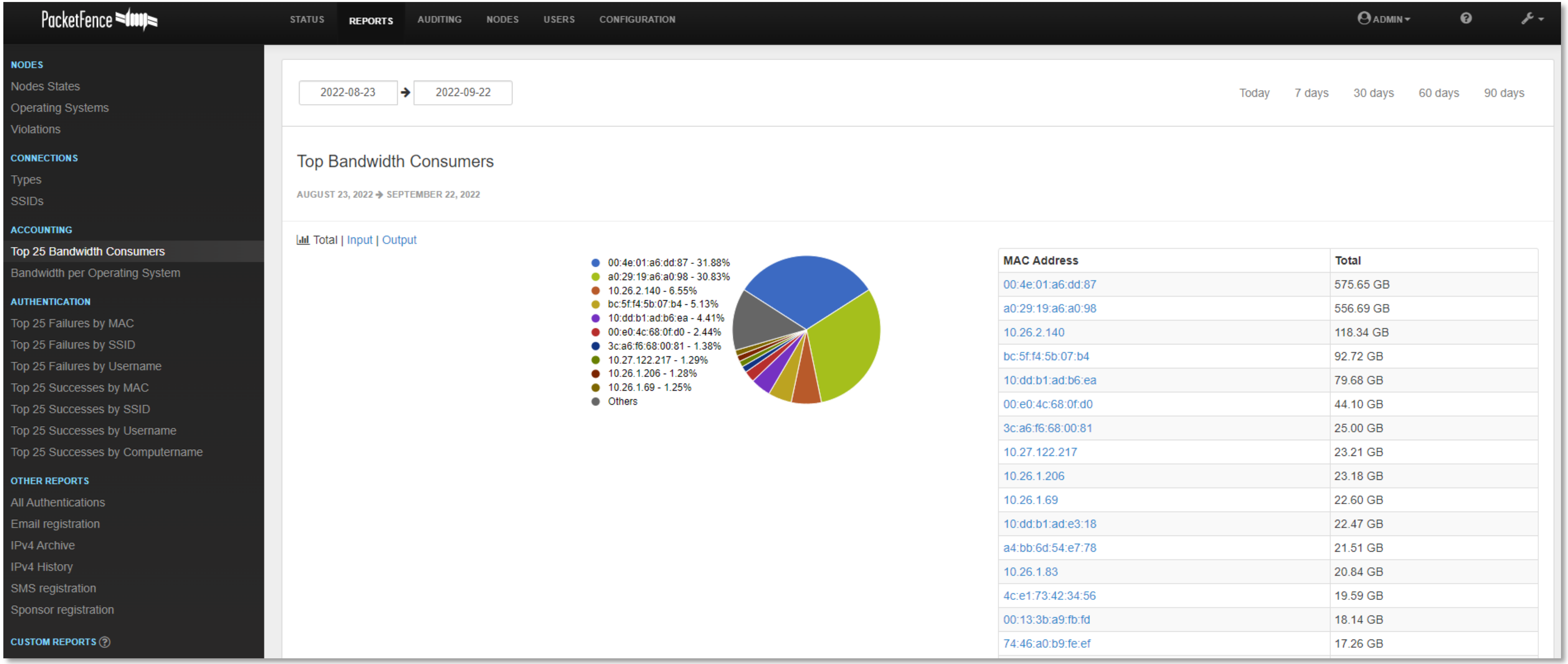
2022-08-23 → 2022-09-22

Violations

AUGUST 23, 2022 → SEPTEMBER 22, 2022

POST_REG_SYSTEM_SCAN	INTERNET_FOR_MOBILE_DEVICES	IDS_P2P	SYSTEM_SCAN	OPENVAS_SCAN__EB_
787	308	2	1	1

CCR Tutorial Days 10-12 ottobre @ LNF



PacketFence

STATUS | REPORTS | AUDITING | NODES | USERS | CONFIGURATION | ADMIN

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 ?

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

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

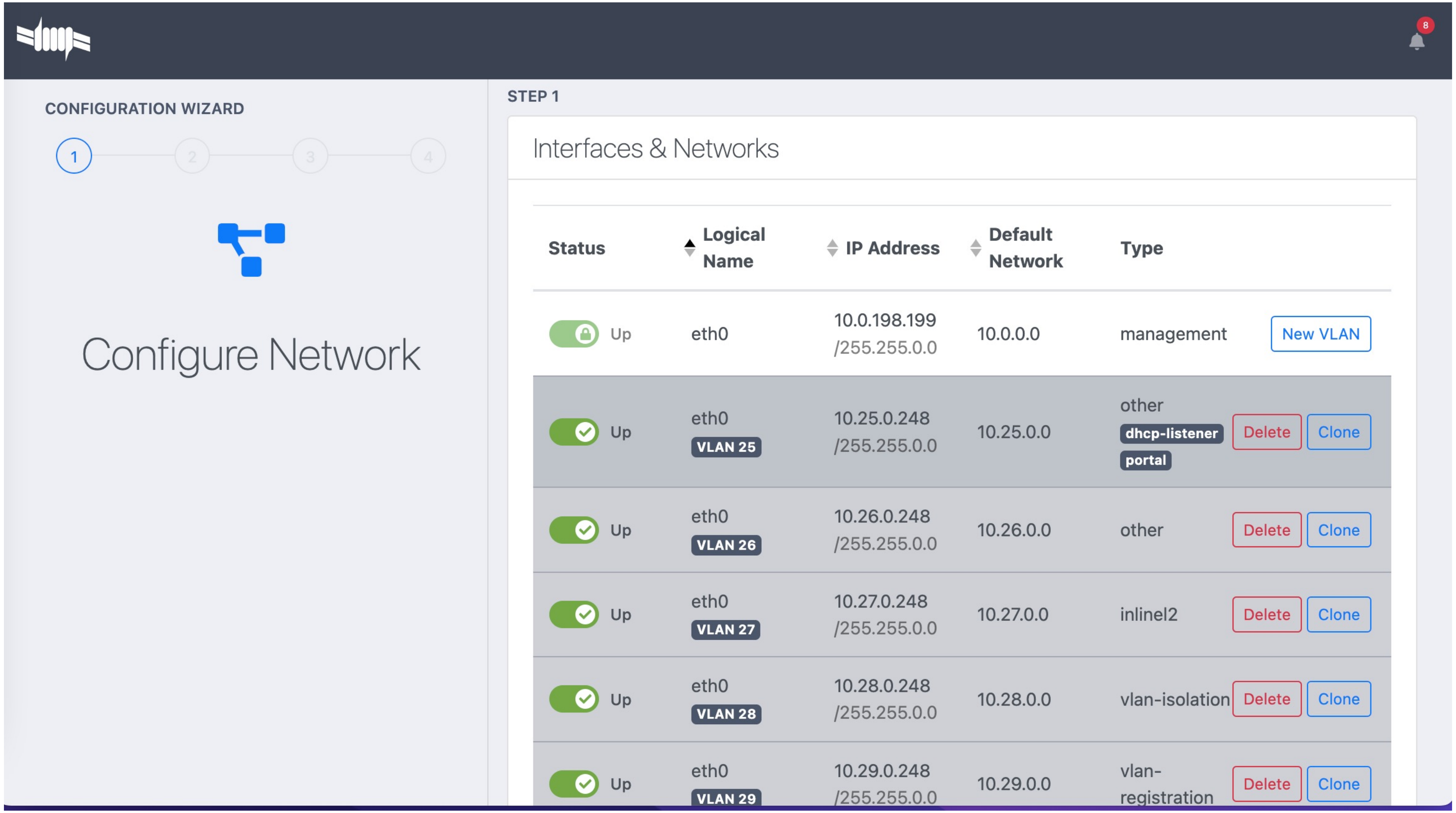
Grazie !

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»

CCR Tutorial Days 10-12 ottobre @ LNF
Packetfence vers. 12.0 – Schede di rete



CONFIGURATION WIZARD

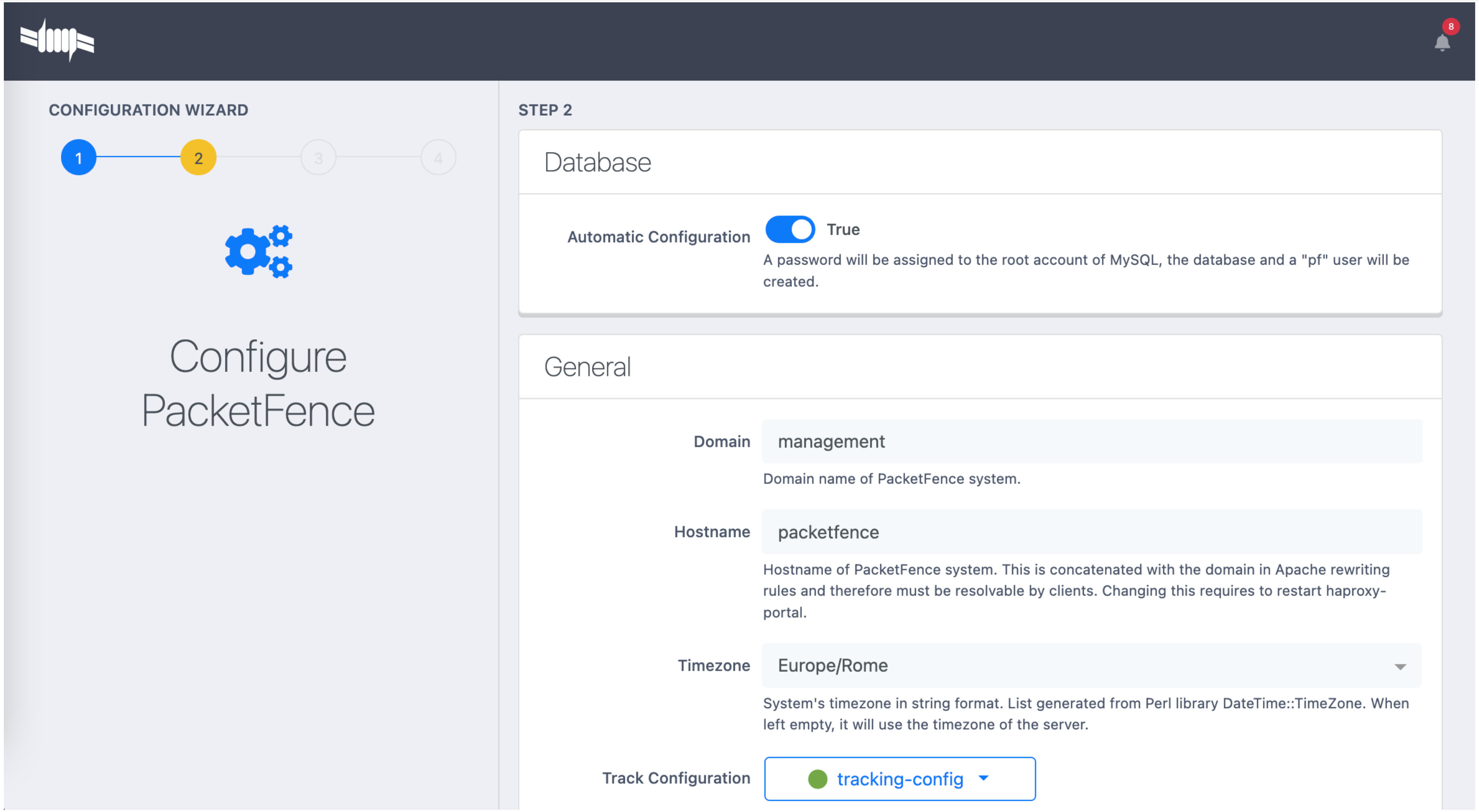
Configure Network

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

CCR Tutorial Days 10-12 ottobre @ LNF
Packetfence vers. 12.0 – Setup di base



STEP 2

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

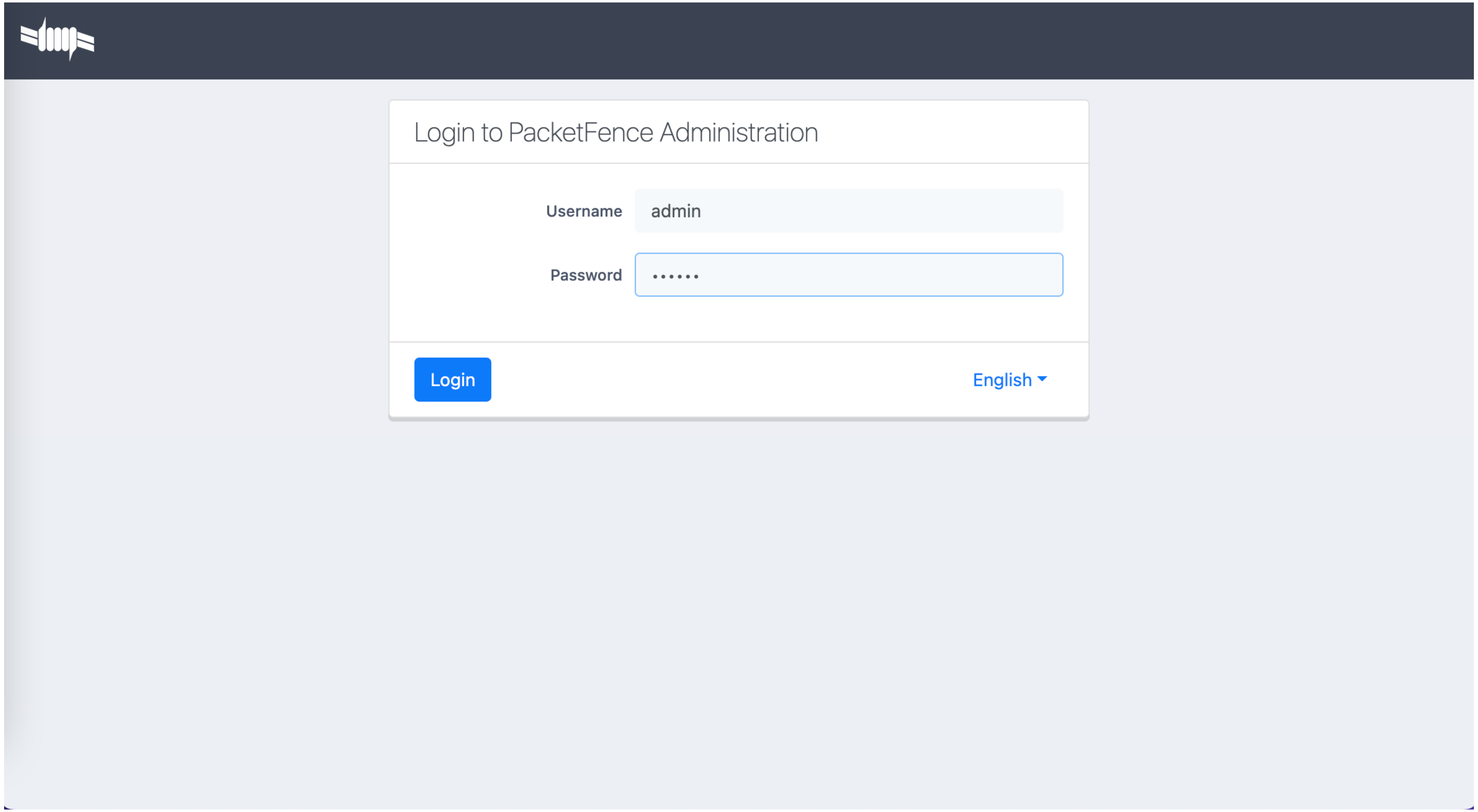
Hostname of PacketFence system. This is concatenated with the domain in Apache rewriting rules and therefore must be resolvable by clients. Changing this requires to restart haproxy-portal.

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

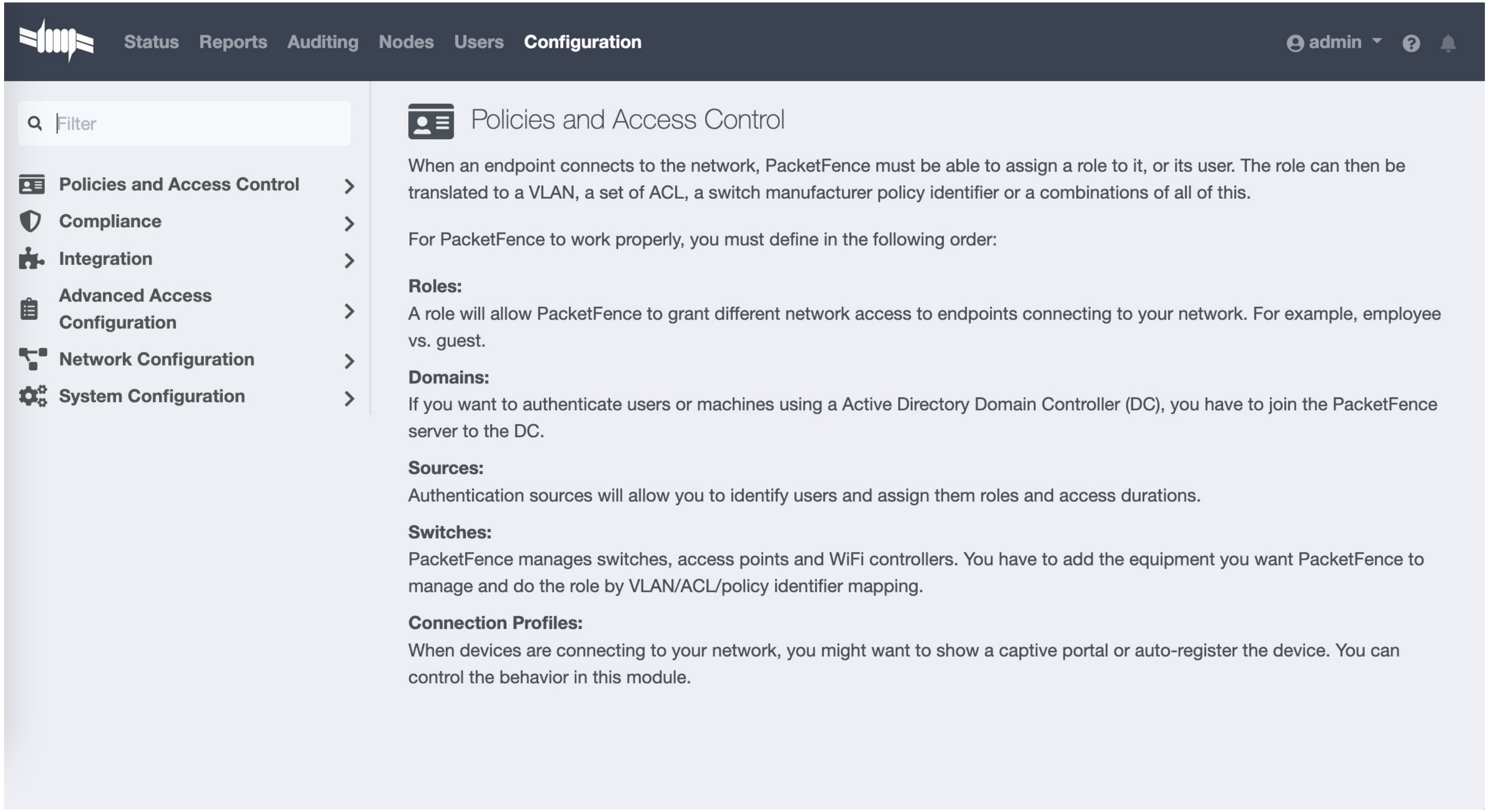


Login to PacketFence Administration

Username: admin

Password: ••••••

CCR Tutorial Days 10-12 ottobre @ LNF
Packetfence vers. 12.0 – Configurazione



Policies and Access Control

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.

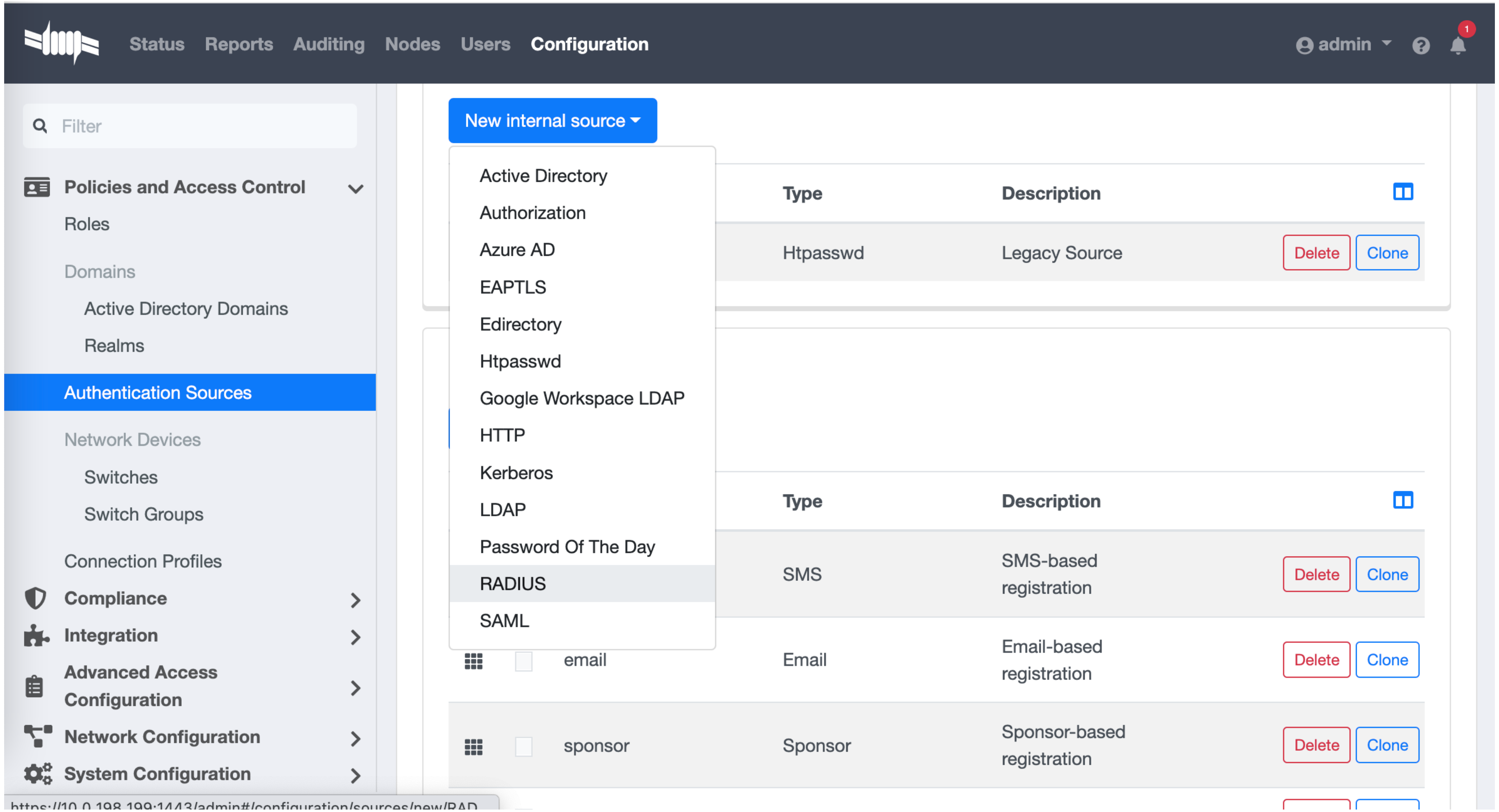
Domains:
If you want to authenticate users or machines using a Active Directory Domain Controller (DC), you have to join the PacketFence server to the DC.

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

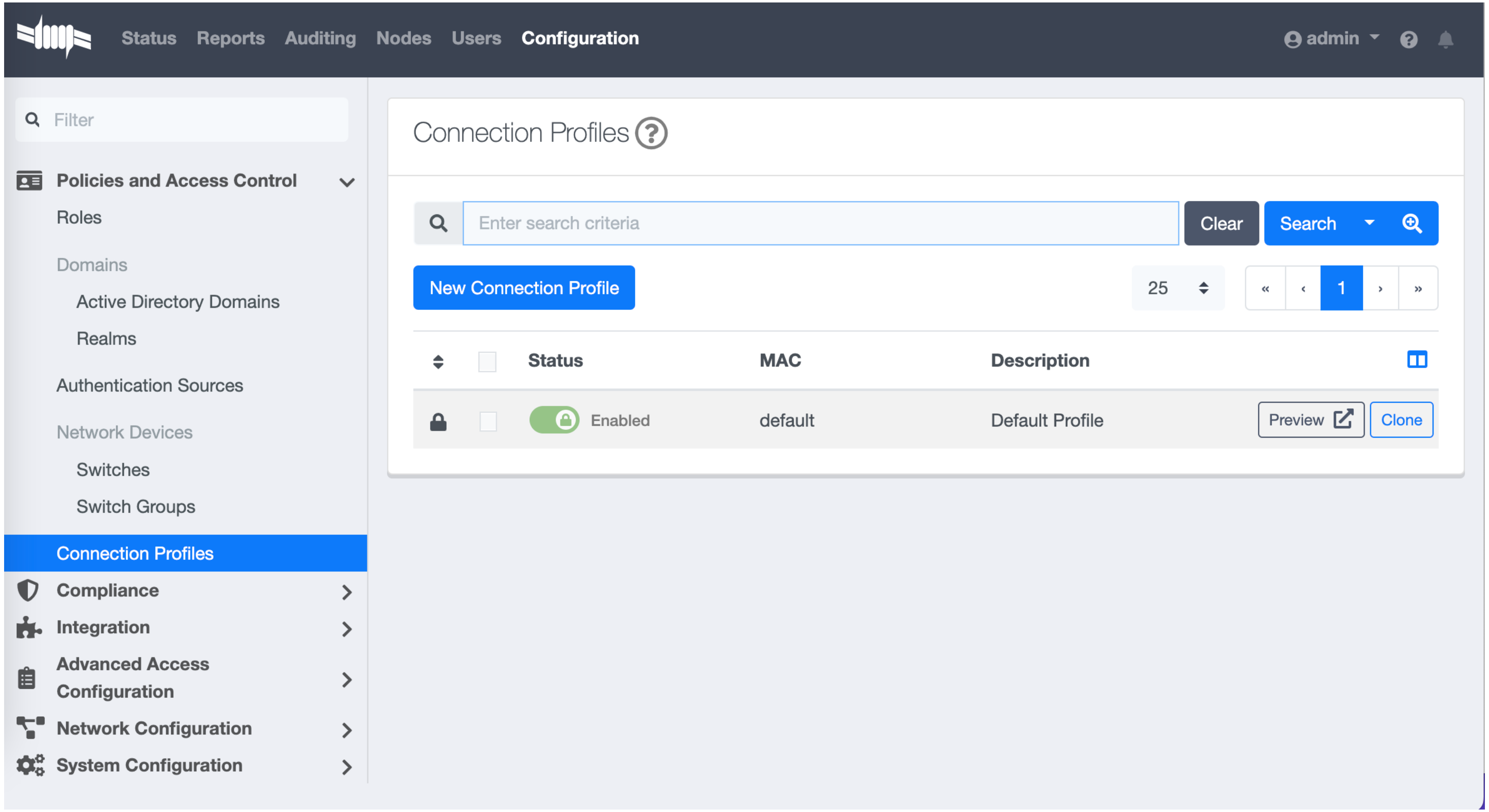


	Type	Description	
	Htpasswd	Legacy Source	Delete Clone

	Type	Description	
	SMS	SMS-based registration	Delete Clone
email	Email	Email-based registration	Delete Clone
sponsor	Sponsor	Sponsor-based registration	Delete Clone

https://10.0.198.199:1443/admin#/configuration/sources/new/RAD

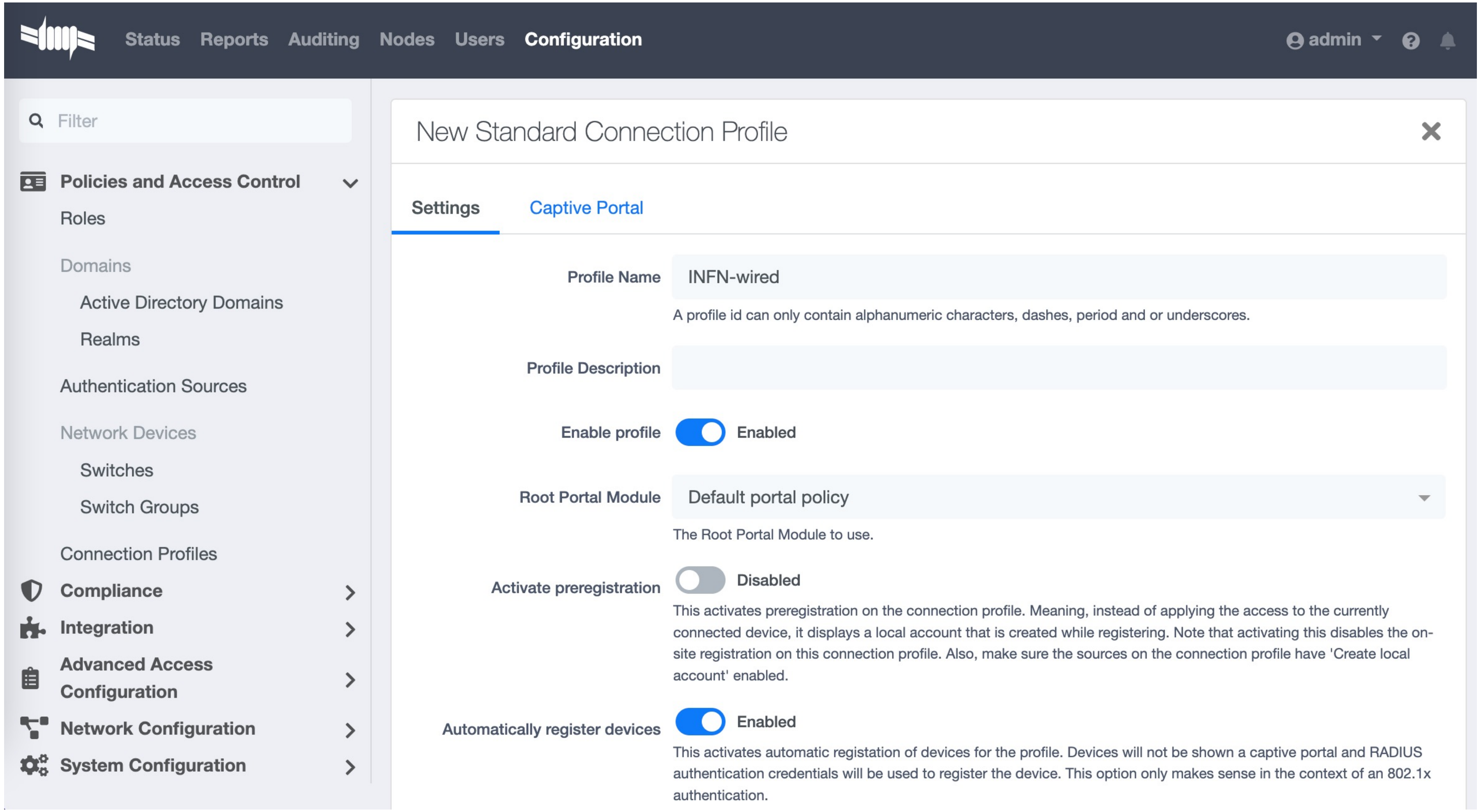
CCR Tutorial Days 10-12 ottobre @ LNF
Packetfence vers. 12.0 – Profili di rete



Connection Profiles

Status	MAC	Description
Enabled	default	Default Profile

CCR Tutorial Days 10-12 ottobre @ LNF
Packetfence vers. 12.0 – Profilo per INFN-wired 1/2



New Standard Connection Profile

Settings | Captive Portal

Profile Name: INFN-wired

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

Profile Description:

Enable profile: Enabled

Root Portal Module: Default portal policy

The Root Portal Module to use.

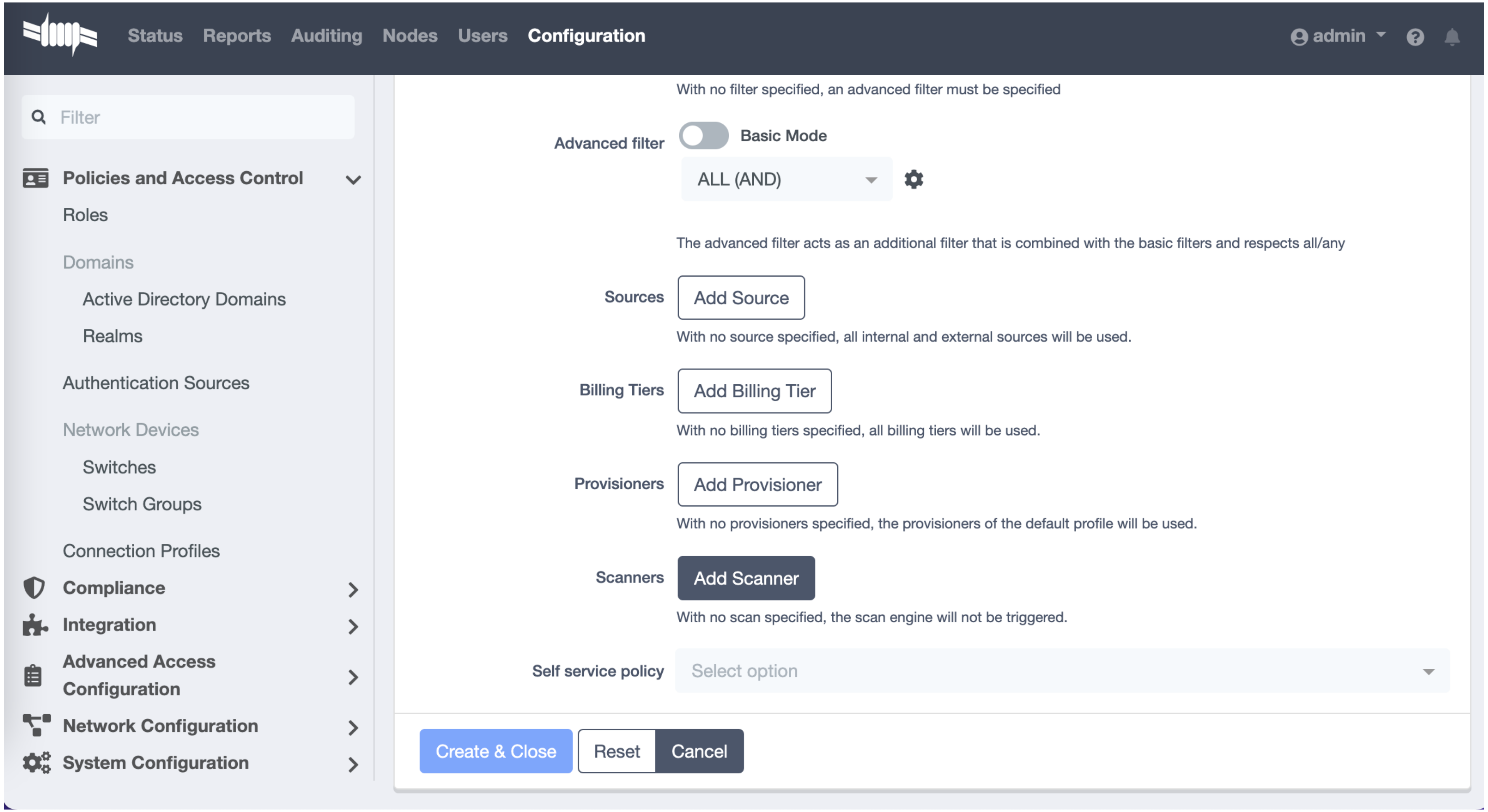
Activate preregistration: Disabled

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

This activates automatic registation 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



With no filter specified, an advanced filter must be specified

Advanced filter: Basic Mode

ALL (AND)

The advanced filter acts as an additional filter that is combined with the basic filters and respects all/any

Sources

With no source specified, all internal and external sources will be used.

Billing Tiers

With no billing tiers specified, all billing tiers will be used.

Provisioners

With no provisioners specified, the provisioners of the default profile will be used.

Scanners

With no scan specified, the scan engine will not be triggered.

Self service policy: Select option