Implementazione di un sistema open source per il Network Access Control

C. Catalano, S. Forestieri, F. Marrone, M. Pericò

Istat

Sommario

1. Scenari
2. Requisiti dell'implementazione
3. La soluzione PacketFence per il NAC
4. Caratteristiche dell'infrastruttura
5. Conclusioni e sviluppi futuri

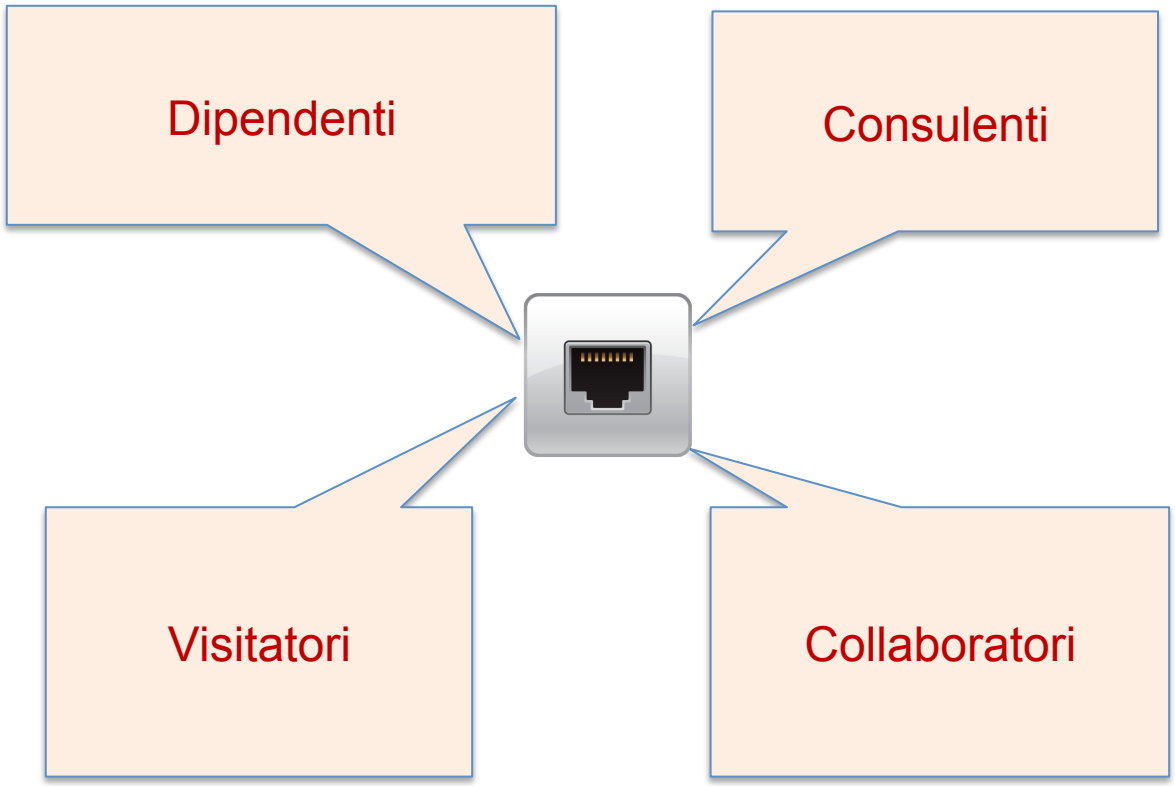
Prima del NAC

- Configurazione manuale delle VLAN
- Difficile gestione della mobilità dell'utente
- Perdita di controllo delle prese utente
- Attestazione di PC esterni nella VLAN interna senza autenticazione
- Nessuna verifica del tipo di dispositivo
- Individuazione dei dispositivi tramite indirizzi IP e MAC-address
- Mancanza di associazione tra utente e dispositivo

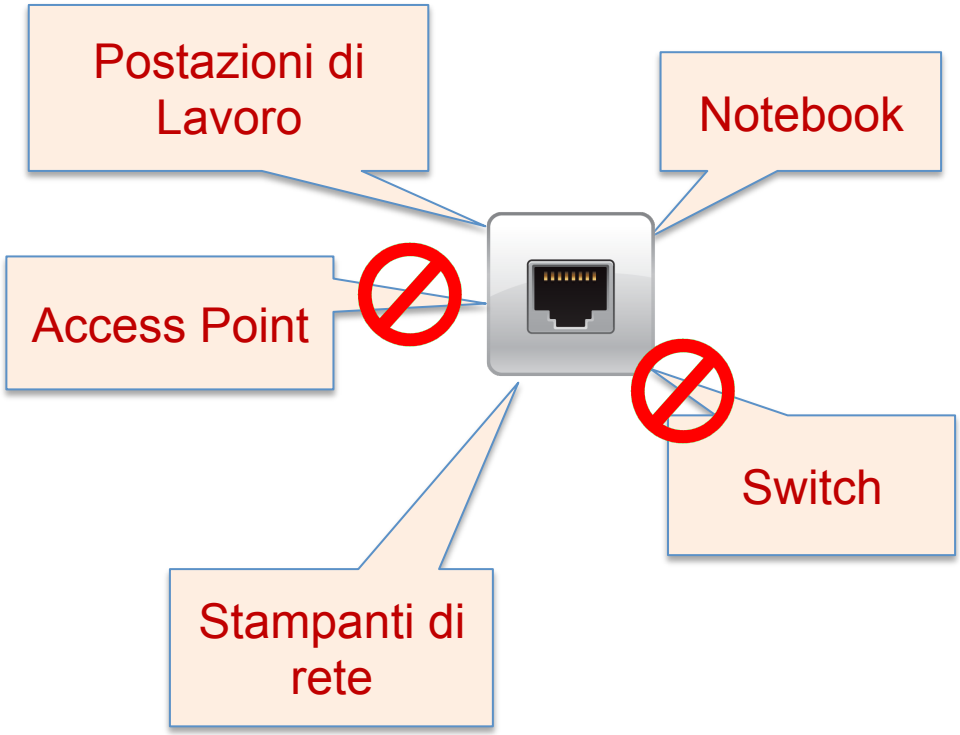
Dopo il NAC

- Configurazione automatica delle porte e delle VLAN
- Verifica dell'identità degli utenti che si collegano in rete
- Monitoraggio continuo dei dispositivi e dell'associazione utente
- Semplice gestione della mobilità degli utenti
- Accesso alle risorse in base all'identità
- Verifica della conformità delle postazioni di lavoro
- Gestione della quarantena dei computer infetti

Gli utenti non sono tutti uguali



I dispositivi non sono tutti uguali



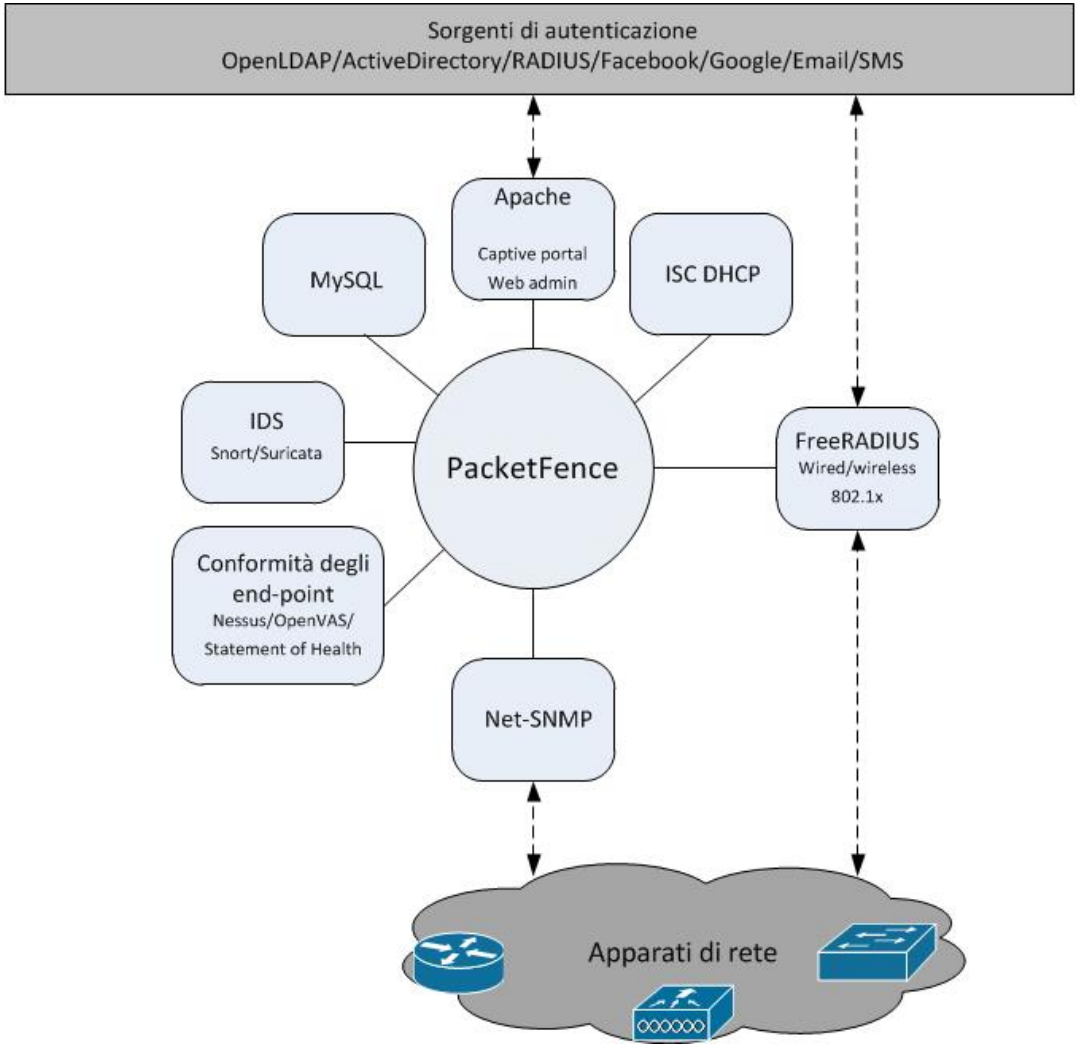
Requisiti dell'implementazione

- Soluzione Agentless
- Compatibilità con i sistemi di autenticazione e autorizzazione presenti in Istituto (AD, ldap, radius)
- Gestione profili utente tramite VLAN
- Compatibilità con gli apparati di accesso alla rete utilizzati in Istituto
- Implementazione di architetture in Alta Affidabilità e Continuità Operativa

La soluzione PacketFence per il NAC (1/3)

- E’ una soluzione Open Source
- Fa uso dei più comuni standard di rete
- Non richiede l’impiego di dispositivi specifici di alcun vendor
- E’ scritto in codice Perl modificabile
- Ha un Captive Portal facilmente personalizzabile
- Esiste una community OnLine Attiva
- E’ disponibile un supporto commerciale

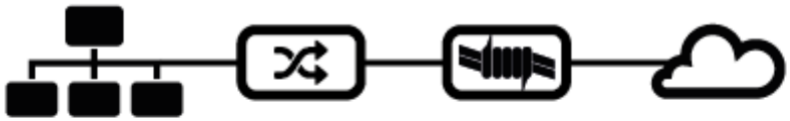
La soluzione PacketFence per il NAC (2/3)



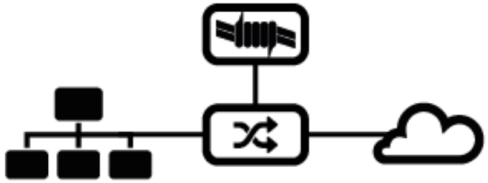
La soluzione PacketFence per il NAC (3/3)

L'applicazione può essere configurata e operare in due modalità:

- IN-LINE Enforcement



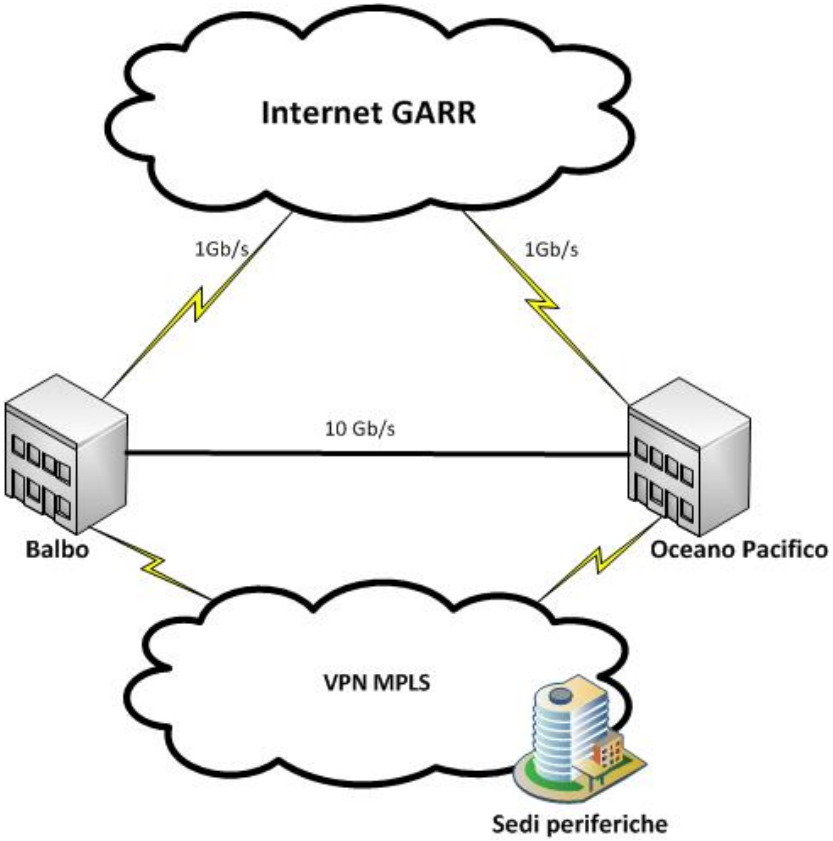
- VLAN Enforcement



L'architettura implementata fa uso esclusivamente della modalità fuori-banda.

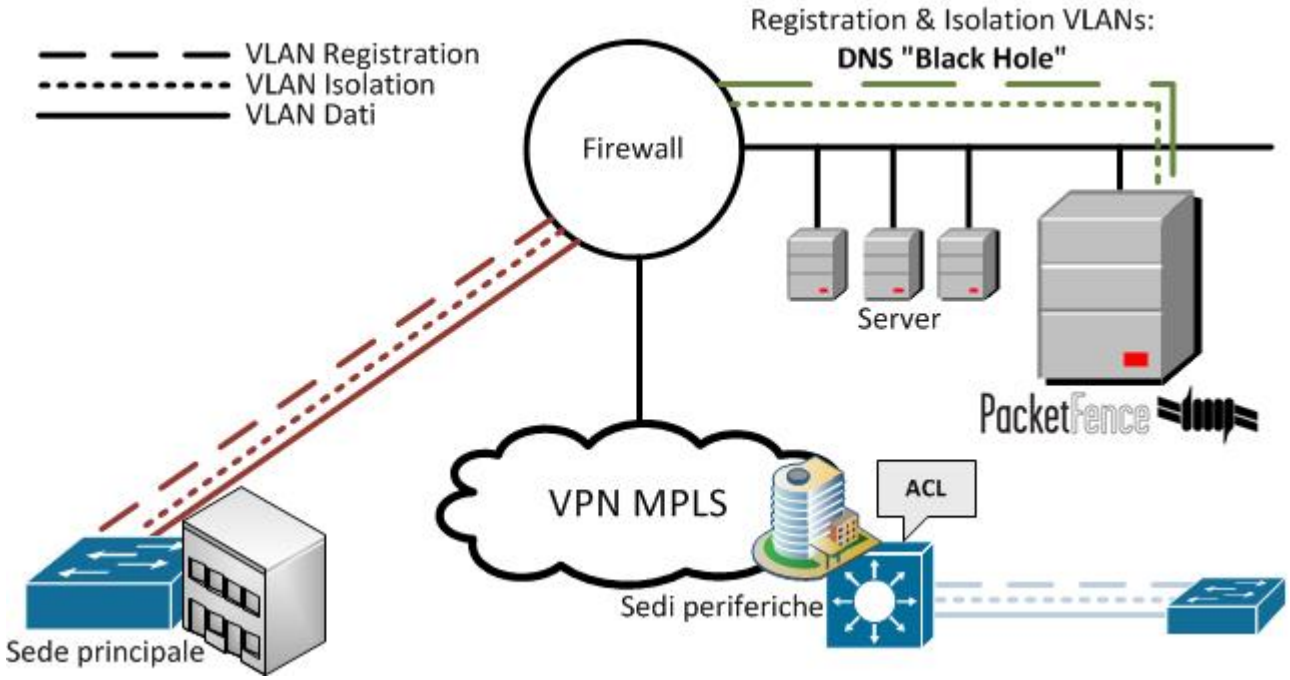
PacketFence interagisce (tramite SNMP e Radius) con gli apparati di accesso per assegnare le VLAN corrispondenti alle policy definite per l'utente.

L’infrastruttura di rete ISTAT



- 2 CED principali con link di accesso verso la rete GARR
- Collegamento end-to-end a 10Gb/s fra le due sedi che ospitano i CED
- Le sedi periferiche sono interconnesse attraverso una VPN MPLS
- Oltre 8000 punti di accesso su tutto il territorio nazionale: prevalentemente PC Windows attestati al dominio, PC Linux o MAC, stampanti di rete, telefoni VoIp e Smartphone.

L’integrazione di PacketFence



Le politiche di sicurezza vengono implementate tramite i dispositivi di rete, gestendone la configurazione delle porte (**VLAN enforcement**) in modo che il client non autenticato (assegnato alla vlan di **registration**) non possa effettivamente fare nulla (attacchi, scansioni di porte, DoS ecc) finché non è stato ammesso in rete.

Utenti di dominio: integrazione con AD

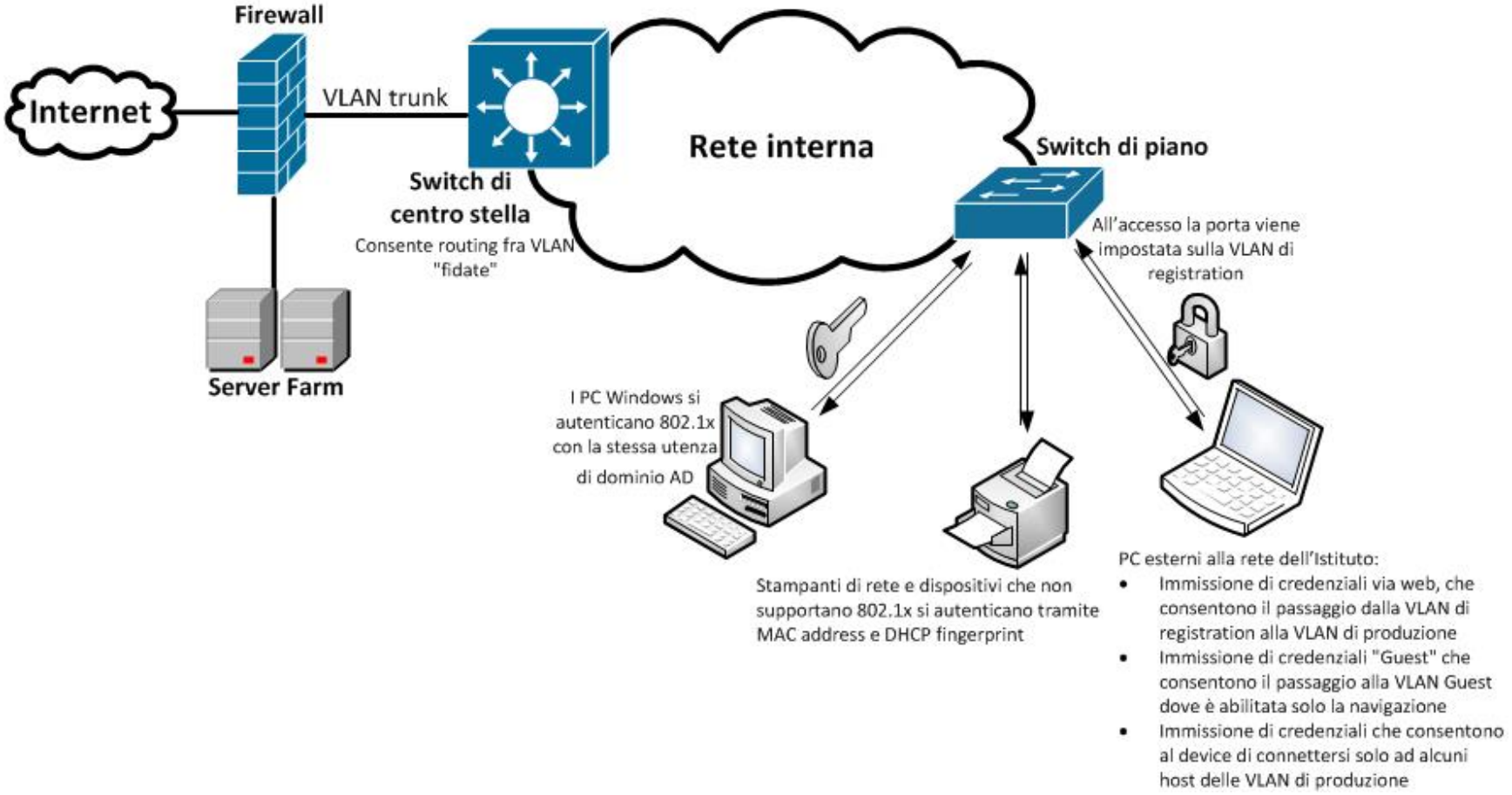
Unica autenticazione alla rete e dominio Microsoft, tramite standard 802.1x:

- Installazione e configurazione Samba, Kerberos, Winbind per il modulo FreeRADIUS
- Creazione su Active Directory di un'utenza di binding e configurazione delle sorgenti di autenticazione in PacketFence
- Configurazione del protocollo PEAP mschap v2 sui client di dominio mediante Policy di Gruppo

Il processo di autenticazione (1/2)

1) Un client sconosciuto viene associato alla VLAN di *registration*, dove il DHCP assegna come DNS l'indirizzo IP del PacketFence.
2) Se il PC è a dominio, si inizia un'autenticazione 802.1x al termine della quale il modulo FreeRADIUS restituisce allo switch la VLAN da assegnare.
3) In assenza di un supplicant 802.1x sul client, lo switch, scaduto un timeout, termina l'invio di pacchetti 802.1x ed effettua un "fallback" all'autenticazione MAC.
4) Stampanti e IP-Phone vengono autenticati utilizzando MAC vendor e il DHCP FingerPrint.
5) Tutti gli altri dispositivi (principalmente PC non a dominio), vengono reindirizzati verso il Captive Portal per l'autenticazione.

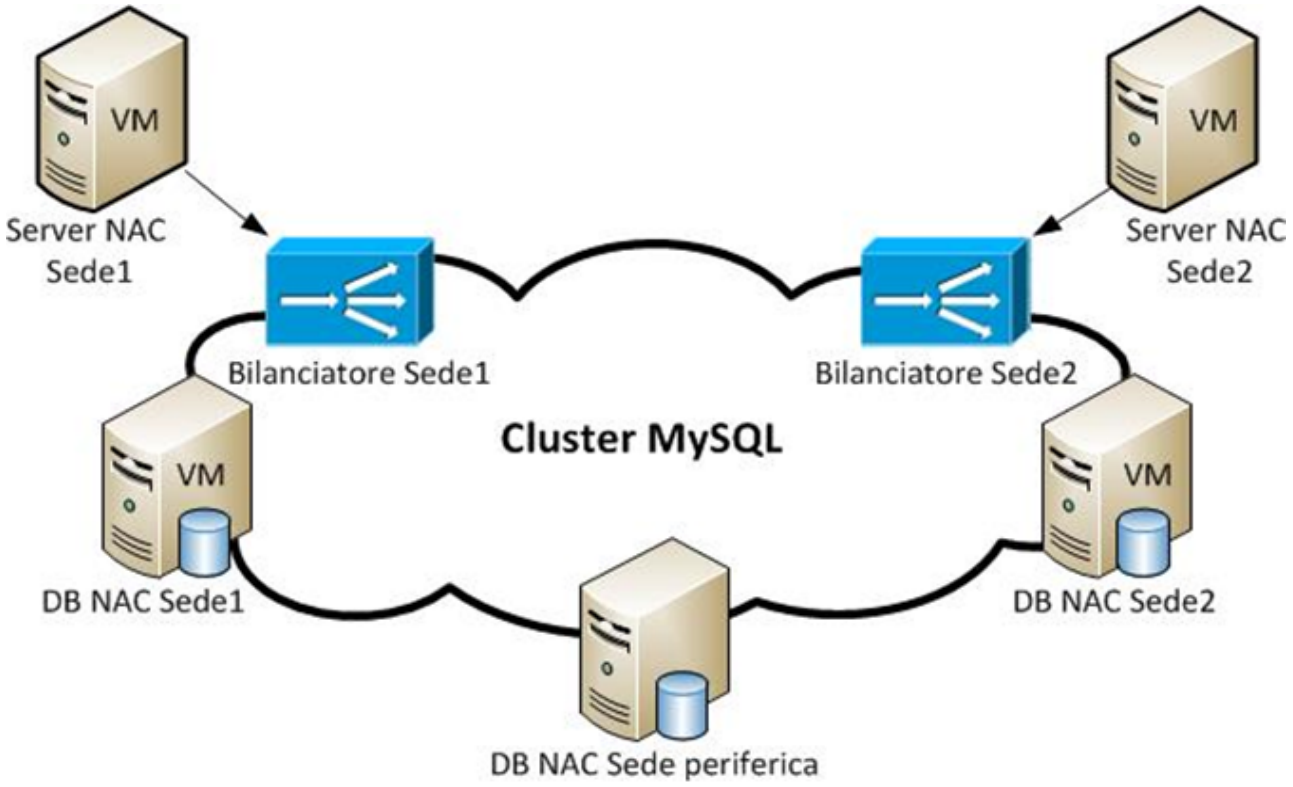
Il processo di autenticazione (2/2)



Architettura del sistema (1/2)

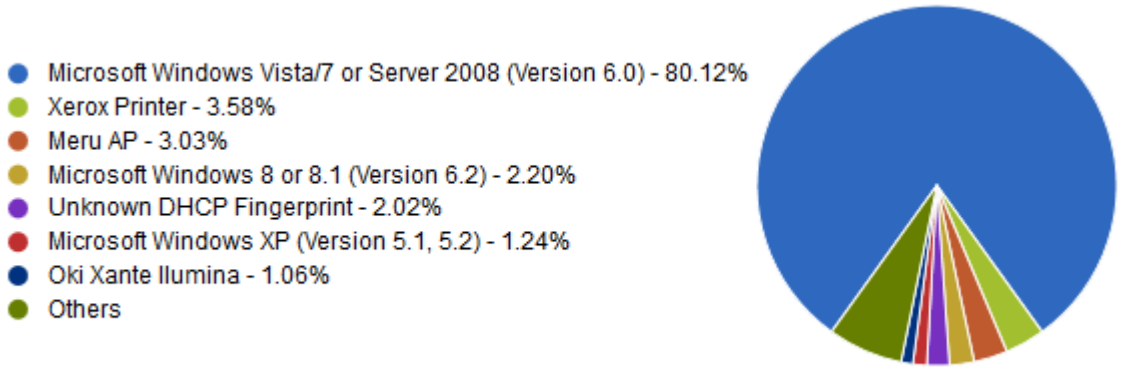
- L'applicativo è stato installato su macchine virtuali Linux Debian
- Due server PacketFence nei CED principali
- Configurazione ad hoc degli switch con entrambi i server RADIUS per autenticazione 802.1x+MAC
- Ridondanza dei DNS per le VLAN di registration e isolation
- DHCP Failover
- MySQL Galera Cluster

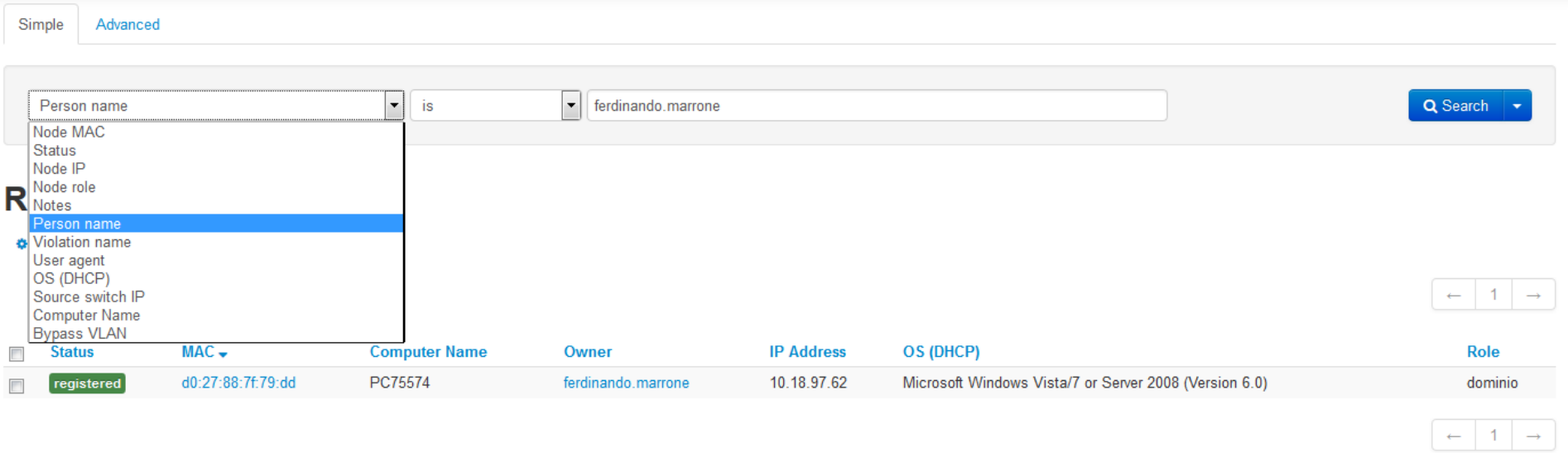
Architettura del sistema (2/2)

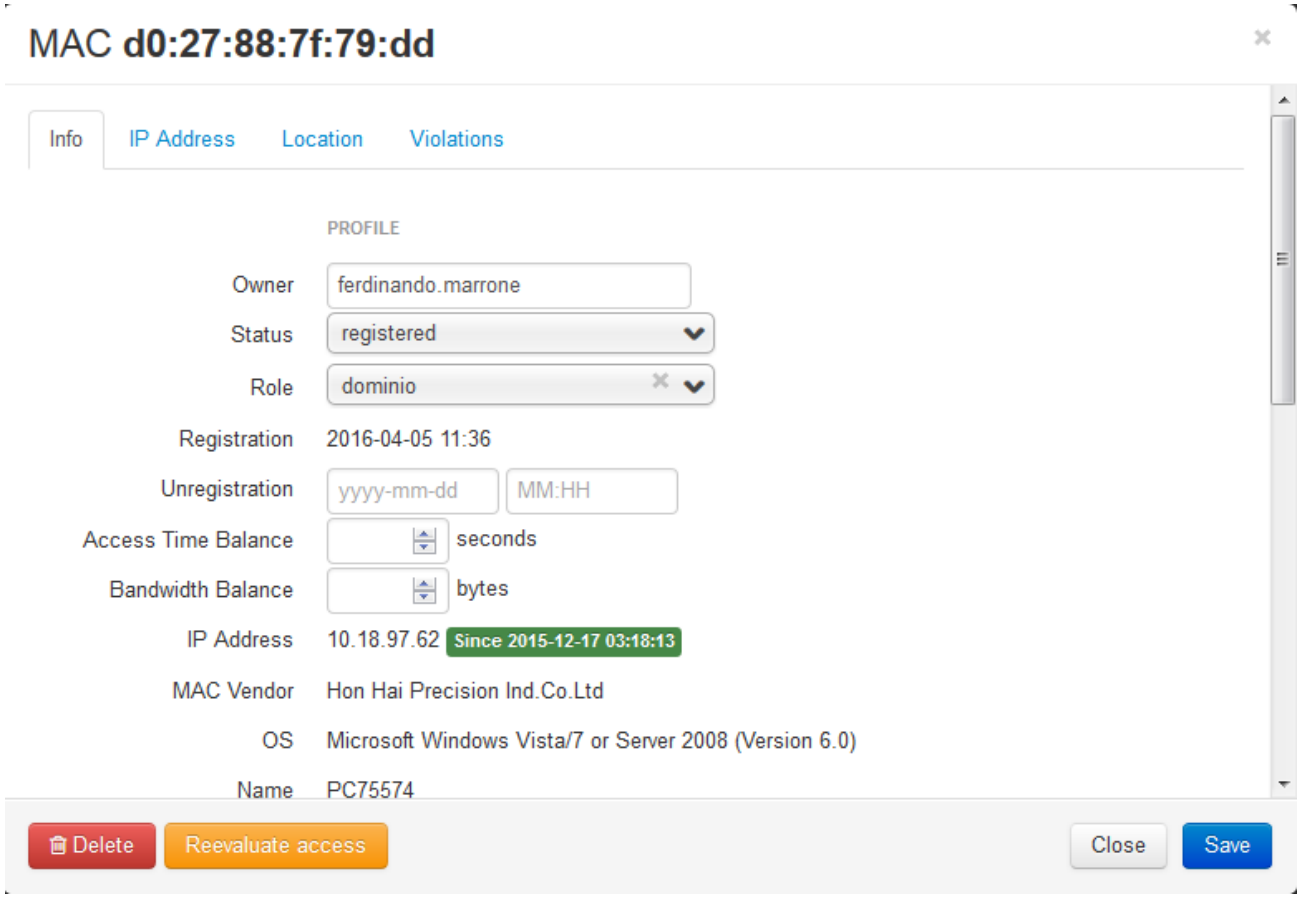


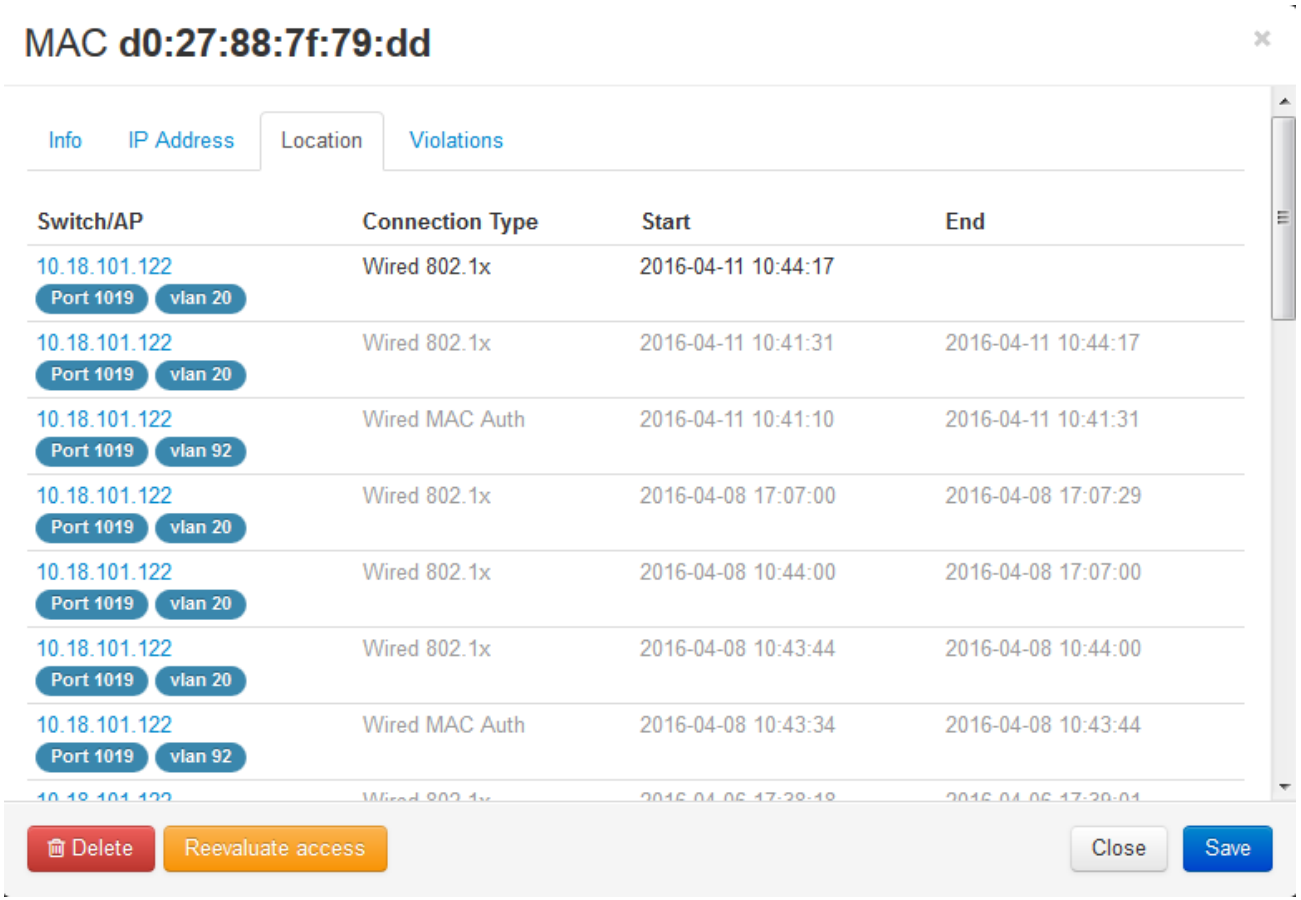
I singoli server PacketFence puntano a DB su indirizzi virtuali gestiti dai bilanciatori

Esempi di report






MAC d0:27:88:7f:79:dd
Info
IP Address
Location
Violations
PROFILE
Owner
ferdinando.marrone
Status
registered
Role
dominio
Registration
2016-04-05 11:36
Unregistration
yyyy-mm-dd
MM:HH
Access Time Balance
seconds
Bandwidth Balance
bytes
IP Address
10.18.97.62
Since 2015-12-17 03:18:13
MAC Vendor
Hon Hai Precision Ind.Co.Ltd
OS
Microsoft Windows Vista/7 or Server 2008 (Version 6.0)
Name
PC75574
Delete
Reevaluate access
Close
Save


MAC d0:27:88:7f:79:dd
Info
IP Address
Location
Violations
Switch/AP
Connection Type
Start
End
10.18.101.122
Port 1019
vlan 20
Wired 802.1x
2016-04-11 10:44:17
10.18.101.122
Port 1019
vlan 20
Wired 802.1x
2016-04-11 10:41:31
2016-04-11 10:44:17
10.18.101.122
Port 1019
vlan 92
Wired MAC Auth
2016-04-11 10:41:10
2016-04-11 10:41:31
10.18.101.122
Port 1019
vlan 20
Wired 802.1x
2016-04-08 17:07:00
2016-04-08 17:07:29
10.18.101.122
Port 1019
vlan 20
Wired 802.1x
2016-04-08 10:44:00
2016-04-08 17:07:00
10.18.101.122
Port 1019
vlan 20
Wired 802.1x
2016-04-08 10:43:44
2016-04-08 10:44:00
10.18.101.122
Port 1019
vlan 92
Wired MAC Auth
2016-04-08 10:43:34
2016-04-08 10:43:44
Delete
Reevaluate access
Close
Save

Conclusioni

Il NAC ha reso possibile:

- rilevare la presenza di Sistemi Operativi non conformi alle politiche d'Istituto (es. Microsoft Windows XP)
- individuare/bloccare gli utenti che utilizzavano il PC con utenza di amministratore locale
- eliminare i dispositivi di rete non autorizzati (es. access-point, switch, hub)
- sanare situazioni di "rogue dhcp" e "loop"

Sviluppi futuri

- Integrazione completa all'infrastruttura wifi
- Autoregistrazione degli utenti ospiti
- Integrazione Vulnerability Assessment tramite script Nessus in sostituzione di Microsoft SoH (Statement of Health)
- Predisposizione di meccanismi di Remediation
- Interfacciamento tramite IDS su firewall proprietario per la messa in quarantena dei client infetti