Realizzazione di un sistema di Network Access Control (NAC) per la rete ethernet dell’Osservatorio Astronomico di Padova

Amedeo Petrella , Danilo Selvestrel

Premessa

Data la crescente complessità e importanza della rete ethernet dell'Osservatorio Astronomico di Padova, è fondamentale implementare misure di sicurezza robuste ed efficaci. La protezione dei dati personali e scientifici, la salvaguardia delle risorse informatiche e la continuità operativa sono priorità assolute, rendendo cruciale la gestione degli accessi alla rete. Attualmente, l'assenza di un sistema centralizzato di controllo degli accessi espone la rete a potenziali vulnerabilità interne ed esterne.

Un sistema di Network Access Control (NAC) si configura come una soluzione strategica per affrontare queste sfide. Il NAC permette di definire, applicare e monitorare politiche di accesso in base all'identità degli utenti, al tipo di dispositivo utilizzato, alla sua conformità agli standard di sicurezza e alla sua posizione all'interno della rete. Questo approccio proattivo garantisce che solo dispositivi autorizzati e conformi possano connettersi alla rete, riducendo significativamente il rischio di accessi non autorizzati, di diffusione di malware e di interruzioni del servizio.

La realizzazione di un sistema NAC per la rete dell'Osservatorio Astronomico di Padova non è quindi solo un miglioramento tecnico, ma un investimento fondamentale nella sicurezza e nell'affidabilità delle infrastrutture informatiche, essenziale per la tutela dell'integrità delle attività di ricerca e per la protezione del patrimonio scientifico dell'istituzione.

Caratteristiche e limiti di un sistema NAC

L'implementazione di un sistema NAC, pur offrendo notevoli vantaggi in termini di sicurezza, presenta anche alcuni limiti e sfide che devono essere attentamente considerati:

- **Complessità di implementazione e gestione:** Un sistema NAC può essere complesso da progettare, configurare e gestire, specialmente in reti di grandi dimensioni o con un'elevata eterogeneità di dispositivi. Richiede competenze specifiche e un investimento significativo in termini di tempo e risorse.

- **Impatto sulle prestazioni della rete:** L'analisi e l'applicazione delle politiche di accesso possono introdurre una certa latenza o rallentamento, sebbene i sistemi moderni siano progettati per minimizzare tale impatto. È fondamentale una corretta pianificazione e dimensionamento per evitare colli di bottiglia.
- **Falsi positivi e negativi:** La definizione di politiche troppo restrittive può portare a blocchi indesiderati (falsi positivi), mentre politiche troppo permissive possono compromettere la sicurezza (falsi negativi). È necessario un fine tuning continuo per bilanciare sicurezza e usabilità.
- **Compatibilità con dispositivi legacy:** Alcuni dispositivi più datati o non conformi agli standard possono non supportare pienamente le funzionalità richieste da un sistema NAC, rendendo necessaria la previsione di eccezioni o l'aggiornamento dell'hardware.
- **Gestione delle eccezioni:** La necessità di concedere accessi temporanei o speciali a utenti o dispositivi specifici può complicare la gestione delle politiche e richiedere procedure dedicate che potrebbero, se non ben controllate, introdurre delle vulnerabilità.
- **Risorse umane e formazione:** Il personale IT dovrà essere adeguatamente formato per gestire il nuovo sistema, monitorare gli eventi di sicurezza e rispondere prontamente a eventuali incidenti o tentativi di accesso non autorizzato.
- **Costi:** L'acquisizione di software, hardware e la formazione del personale comportano un investimento iniziale che deve essere giustificato dai benefici in termini di sicurezza e resilienza della rete.

Tipologie di implementazione di un sistema NAC

L'implementazione di un sistema NAC può essere realizzata attraverso diverse architetture, ognuna con i propri vantaggi e svantaggi in termini di complessità, costi e flessibilità. Le principali tipologie includono l'implementazione basata su agente, senza agente e ibrida.

Implementazione basata su agente

Questo approccio prevede l'installazione di un software (agente) su ogni dispositivo che si connette alla rete. L'agente raccoglie informazioni sullo stato di sicurezza del dispositivo (ad esempio, aggiornamenti antivirus, patch del sistema operativo) e comunica con il server NAC per l'autenticazione e l'applicazione delle policy.

Pro:

- **Maggiore granularità del controllo:** L'agente può raccogliere informazioni dettagliate sullo stato interno del dispositivo, consentendo un controllo più preciso e basato sulla conformità.
- **Sicurezza continua:** L'agente può monitorare il dispositivo in tempo reale anche dopo che è stato ammesso alla rete, rilevando eventuali cambiamenti nello stato di sicurezza.
- **Applicazione delle policy anche fuori rete:** Alcuni agenti possono applicare le policy anche quando il dispositivo non è connesso alla rete aziendale, utile per il telelavoro.

Contro:

- **Complessità di deployment:** Richiede l'installazione e la gestione dell'agente su ogni dispositivo, il che può essere oneroso in reti di grandi dimensioni o con un'elevata rotazione di dispositivi.
- **Problemi di compatibilità:** L'agente potrebbe non essere compatibile con tutti i tipi di dispositivi (ad esempio, dispositivi IoT, stampanti di rete) o sistemi operativi specifici.
- **Impatto sulle prestazioni del dispositivo:** L'agente potrebbe consumare risorse del dispositivo, influenzandone le prestazioni.
- **Aggiornamenti e manutenzione:** La gestione degli aggiornamenti e delle patch degli agenti può essere complessa e richiedere risorse significative.

Implementazione senza agente

In questo modello, il sistema NAC non richiede l'installazione di software sui dispositivi. L'autenticazione e la valutazione della conformità avvengono attraverso metodi basati sulla rete, come il monitoraggio del traffico, l'analisi delle impronte digitali dei dispositivi (fingerprinting) o l'utilizzo di protocolli standard (ad esempio, SNMP, WMI) per interrogare i dispositivi.

Pro:

- **Facilità di deployment:** Non richiede l'installazione di software sui dispositivi, semplificando notevolmente il deployment e la gestione.
- **Compatibilità universale:** Può essere applicato a qualsiasi dispositivo connesso alla rete, inclusi quelli che non supportano l'installazione di un agente (stampanti, dispositivi IoT, ecc.).
- **Minore impatto sulle prestazioni del dispositivo:** Non consuma risorse sul dispositivo finale.

Contro:

- **Minore granularità del controllo:** Le informazioni raccolte sullo stato di sicurezza del dispositivo sono meno dettagliate rispetto all'approccio basato su agente.
- **Visibilità limitata post-ammissione:** La capacità di monitorare il dispositivo dopo l'ammissione alla rete è più limitata.
- **Potenziali falsi positivi/negativi:** L'identificazione dei dispositivi e la valutazione della conformità potrebbero essere meno accurate, portando a errori.
- **Dipendenza dalla configurazione di rete:** Richiede una corretta configurazione degli switch, dei router e di altri dispositivi di rete per funzionare efficacemente.

Implementazione ibrida

Questa soluzione combina gli aspetti dell'implementazione basata su agente e senza agente. Alcuni dispositivi critici o gestiti possono avere un agente installato per un controllo

granulare, mentre altri dispositivi non gestiti o non compatibili con l'agente vengono controllati con metodi senza agente.

Pro:

- **Massima flessibilità:** Consente di adattare l'approccio di controllo a seconda del tipo e della criticità del dispositivo.
- **Bilanciamento tra sicurezza e usabilità:** Offre un controllo dettagliato dove è più necessario, mantenendo la semplicità per altri dispositivi.
- **Costo-efficacia:** Permette di ottimizzare gli investimenti, evitando l'installazione di agenti su dispositivi dove non è strettamente necessario.

Contro:

- **Maggiore complessità di progettazione:** Richiede una pianificazione e una configurazione più elaborate per integrare i due approcci.
- **Potenziale eterogeneità degli strumenti:** La gestione di agenti e metodi senza agente potrebbe richiedere strumenti e competenze diverse.
- **Costi potenzialmente più elevati:** Sebbene più flessibile, la combinazione di diverse tecnologie potrebbe comportare costi complessivi maggiori.

La scelta della tipologia di implementazione dipende dalle specifiche esigenze dell'Osservatorio Astronomico di Padova, dalla complessità della rete, dal budget disponibile e dal livello di sicurezza desiderato.

Architettura scelta: Senza Agente (basata su autenticazione MAC Address)

Per l'implementazione del sistema NAC presso l'Osservatorio Astronomico di Padova, è stata selezionata l'architettura **senza agente, basata sull'autenticazione del MAC address**. Questa scelta è stata dettata da una combinazione di fattori, tra cui la facilità di deployment, la compatibilità con l'ampia gamma di dispositivi presenti e la minimizzazione dell'impatto sulle risorse dei dispositivi finali.
L'adozione del protocollo 802.1X avrebbe rappresentato un'alternativa più robusta; tuttavia, la gestione di sistemi legacy o di altri dispositivi come le stampanti sarebbe risultata difficile, se non impossibile.

Motivazioni della scelta:

- **Facilità di Deployment:** L'assenza di agenti software da installare su ciascun dispositivo semplifica drasticamente il processo di implementazione. Questo è particolarmente vantaggioso considerando la varietà di hardware e sistemi operativi che sono presenti nella rete dell'Osservatorio, riducendo oneri di gestione e manutenzione iniziali.
- **Compatibilità Universale:** L'autenticazione basata su MAC address consente di controllare l'accesso a qualsiasi dispositivo connesso alla rete, inclusi quelli che non

supporterebbero l'installazione di un agente (come stampanti di rete, sensori, strumentazione scientifica, dispositivi IoT, ecc.). Questa universalità garantisce che tutti i punti di accesso possano essere soggetti alle politiche di sicurezza.
- **Minore Impatto sulle Prestazioni del Dispositivo:** Non essendo richiesto alcun software aggiuntivo sui dispositivi client, non vi è alcun consumo di risorse (CPU, RAM) che potrebbe influire sulle prestazioni degli stessi. Questo è cruciale per dispositivi sensibili o dedicati a compiti specifici che non devono subire rallentamenti.
- **Gestione Centralizzata e Semplificata:** Sebbene la configurazione iniziale della rete e degli switch sia indispensabile, una volta operativo, il sistema consente una gestione centralizzata del controllo accessi tramite indirizzi MAC, garantendo una visione d'insieme chiara e un'applicazione uniforme delle politiche di sicurezza.

Limiti dell'Architettura Scelta:

Nonostante i vantaggi, è fondamentale riconoscere i limiti intrinseci di un'implementazione senza agente basata su MAC address, già richiamati nella sezione "Limiti" generale del documento:

- **Minore Granularità del Controllo:** Le informazioni raccolte sullo stato di sicurezza del dispositivo sono limitate. L'autenticazione si basa principalmente sull'identità del dispositivo (MAC address) e non sul suo stato di conformità interno (es. aggiornamenti antivirus, patch del sistema operativo). Questo significa che un dispositivo autenticato ma compromesso potrebbe comunque accedere alla rete.
- **Visibilità Limitata Post-Ammissione:** Una volta che un dispositivo è ammesso alla rete, la capacità di monitorare continuamente il suo stato di sicurezza o comportamenti anomali è significativamente ridotta rispetto a un sistema basato su agente.
- **Potenziali Falsi Positivi/Negativi e Spoofing del MAC Address:** L'identificazione basata su MAC address può essere soggetta a spoofing, dove un utente malintenzionato potrebbe clonare un MAC address autorizzato per ottenere accesso. È necessario implementare misure aggiuntive (es. port security sugli switch) per mitigare questo rischio. Inoltre, la gestione di cambiamenti di hardware o sostituzioni di dispositivi richiede un aggiornamento manuale delle liste di MAC address autorizzati, potendo generare falsi negativi se non gestito correttamente.
- **Dipendenza dalla Configurazione di Rete:** L'efficacia del sistema dipende fortemente da una corretta e rigorosa configurazione degli switch di rete, che devono supportare anche situazione complesse come switch di ufficio in cascata.
- **Gestione delle Eccezioni:** La necessità di concedere accessi temporanei o speciali a utenti o dispositivi specifici può complicare la gestione delle politiche e richiedere procedure dedicate che potrebbero, se non ben controllate, introdurre delle vulnerabilità.

La consapevolezza di questi limiti è cruciale per la progettazione e l'implementazione di misure di sicurezza complementari, garantendo un approccio olistico alla protezione della rete dell'Osservatorio.

Privacy e Raccolta Dati: MAC Address e Referenti

La raccolta e la gestione degli indirizzi MAC e delle informazioni sui loro proprietari o referenti nell'ambito di un sistema NAC sollevano importanti questioni relative alla privacy e alla protezione dei dati personali. È fondamentale che tali attività siano condotte in piena conformità con le normative vigenti, in particolare il Regolamento Generale sulla Protezione dei Dati (GDPR - Reg. UE 2016/679).

Aspetti Legali e GDPR:

Il MAC address, pur essendo un identificativo hardware, può essere considerato un dato personale quando è associato a un individuo identificabile o a un dispositivo da cui si può risalire a un utente. La sua raccolta, insieme alle informazioni sui referenti (nome, cognome, credenziali OAPd, ecc.), costituisce un trattamento di dati personali soggetto ai principi e agli obblighi del GDPR.

I punti chiave da considerare ai sensi del GDPR sono:

- **Liceità del trattamento:** La raccolta dei MAC address e dei dati dei referenti deve avere una base giuridica legittima. Nel contesto di un sistema NAC per la sicurezza della rete, la base giuridica più appropriata è l'interesse legittimo del titolare del trattamento (l'Osservatorio Astronomico di Padova) a garantire la sicurezza delle proprie reti e dei propri sistemi informatici, ai sensi dell'Art. 6, par. 1, lett. f) del GDPR. È altresì possibile invocare la necessità di adempiere a un obbligo legale o l'esecuzione di un compito di interesse pubblico (Art. 6, par. 1, lett. c) o e)), qualora esistano specifiche normative o disposizioni che impongano o raccomandino tali misure di sicurezza.
- **Minimizzazione dei dati:** Devono essere raccolti solo i dati strettamente necessari per le finalità di sicurezza e controllo accessi. Ciò significa che le informazioni richieste agli utenti per la registrazione (es. nome del dispositivo, referenti) dovrebbero essere limitate a quanto indispensabile per l'identificazione e la gestione degli accessi.
- **Limitazione della finalità:** I dati raccolti devono essere utilizzati esclusivamente per le finalità di sicurezza della rete e di gestione degli accessi, e non per scopi diversi e incompatibili.
- **Trasparenza e informazione:** Gli utenti devono essere chiaramente informati sulle finalità della raccolta dei dati, sulle modalità di trattamento, sulla base giuridica e sui loro diritti (diritto di accesso, rettifica, cancellazione, limitazione, opposizione). Questo dovrebbe essere fatto tramite un'informativa sulla privacy facilmente accessibile.
- **Sicurezza dei dati:** Devono essere implementate misure tecniche e organizzative adeguate per proteggere i dati raccolti da accessi non autorizzati, divulgazione, alterazione o distruzione. Ciò include l'uso di protocolli di comunicazione sicuri (es. HTTPS per il portale di registrazione), l'accesso limitato ai database, la crittografia dei dati sensibili e sistemi di backup.
- **Conservazione dei dati:** I dati devono essere conservati solo per il tempo strettamente necessario al raggiungimento delle finalità per cui sono stati raccolti.

Una politica di conservazione chiara deve definire i periodi di retention per i MAC address e le informazioni associate.

- **Diritti degli interessati:** Agli utenti devono essere garantiti i diritti previsti dal GDPR, inclusi il diritto di accesso ai propri dati, di rettifica, di cancellazione (diritto all'oblio) e di opposizione al trattamento, nei limiti previsti dalla normativa e dalla finalità di sicurezza.

Necessità di Sicurezza e Bilanciamento con la Privacy:

La necessità di sicurezza, come descritto nella premessa, giustifica la raccolta di tali dati. Un sistema NAC basato su MAC address richiede l'associazione di un identificativo hardware a un utente o referente per poter applicare le politiche di accesso. Senza questa associazione, l'efficacia del sistema verrebbe meno, esponendo la rete a rischi significativi.

Il bilanciamento tra la necessità di sicurezza e il rispetto della privacy si ottiene attraverso:

- **Implementazione di misure di sicurezza robuste:** Proteggere i database contenenti i MAC address e le informazioni sui referenti è prioritario per prevenire violazioni dei dati. *Questo obiettivo viene raggiunto tramite l'adozione degli standard di mercato più elevati e l'applicazione delle migliori pratiche per la sicurezza dei sistemi.*
- **Definizione di politiche di accesso chiare:** Specificare chi può accedere ai dati raccolti e per quali scopi. *In effetti l'accesso ai dati è riservato al solo personale del CED e solo per le finalità previste.*
- **Meccanismi di registrazione trasparente:** Il portale di registrazione, pur facilitando la gestione, deve essere accompagnato da un'informativa completa e facilmente comprensibile. *A tale scopo è stato prevista un'apposita pagina di spiegazioni.*
- **Limitazione della visibilità:** la visualizzazione dei dati dei referenti dovrebbe essere limitata solo al personale autorizzato per scopi di gestione e risoluzione problemi. *In effetti solo il personale del CED ha accesso ai dati.*
- **Considerazione per gli ospiti:** La possibilità di registrare dispositivi di ospiti con un referente interno permette di mantenere un controllo sugli accessi temporanei, garantendo comunque una forma di responsabilità e tracciabilità. *Ciò elimina inoltre la necessità di raccogliere i dati degli ospiti, in quanto non essendo personale a contratto, non sono registrati negli archivi dell'OAPd e dell'INAF.*

Il principio della "privacy by design" ha guidato ogni fase della realizzazione del nostro sistema, garantendo che la protezione dei dati fosse intrinseca fin dalla concezione. Questo approccio proattivo ci ha permesso di ridurre al minimo indispensabile la quantità di dati raccolti, evitando così di conservare informazioni superflue. Ogni dato che è stato ritenuto necessario per il funzionamento del sistema è stato poi sottoposto a rigorose misure di protezione, adottando i migliori standard di sicurezza disponibili. Ciò include l'implementazione di protocolli di crittografia avanzati, l'anonimizzazione dei dati ove possibile e l'applicazione di politiche di accesso rigorose per garantire che solo il personale autorizzato possa accedere a informazioni sensibili. In sintesi, la nostra strategia si è concentrata sulla prevenzione e sulla protezione a monte, piuttosto che sulla mera reazione a posteriori, stabilendo un robusto baluardo contro potenziali violazioni della privacy e

garantendo la massima tranquillità agli utenti.

Implementazione

Configurazione

La rete LAN di Padova utilizza switch Extreme Network con firmware EXOS. Questo firmware supporta l'autenticazione tramite indirizzo MAC, sia su un database locale che, tramite RADIUS, su un database remoto. La scelta più razionale è stata l'utilizzo del server RADIUS (NPS) già presente su un nostro Domain Controller Microsoft. Questa soluzione ha permesso di centralizzare il database degli indirizzi MAC e di implementare, tramite script dedicati, un sistema di registrazione autonoma degli indirizzi MAC per gli utenti.

La configurazione degli switch si articola in due fasi principali: inizialmente, si abilita l'autenticazione degli indirizzi MAC a livello di switch, indirizzandola a un server RADIUS. Successivamente, si procede alla definizione e configurazione delle porte che saranno soggette a tale autenticazione.

Queste configurazioni per il netlogin (i campi con xxxxxx sono stati mascherati):

Configurazione generale

```
configure radius netlogin primary server xxx.xxx.xxx.xxx 1812 client-ip 192.168.4.225 vr
VR-Default
configure radius netlogin primary shared-secret encrypted "xxxxxxxxxx"
configure netlogin vlan netlogin-vlan
enable radius netlogin
enable netlogin mac
configure netlogin mac authentication database-order radius
```

Configurazione per porta

```
enable netlogin ports 2:6,2:14 mac
configure netlogin ports 2:6 mode mac-based-vlans
configure netlogin ports 2:6 no-restart
configure netlogin ports 2:14 mode mac-based-vlans
configure netlogin ports 2:14 no-restart
enable netlogin authentication failure vlan ports 2:6,2:14
configure netlogin authentication failure vlan guest-vlan ports 2:6,2:14
```

Nella configurazione generale vengono impostati questi valori

- indirizzo del server Radius primario (eventualmente si può aggiungere un server secondario per la ridondanza);
- il secret condiviso dal client (lo switch) e il server Radius;
- la configurazione di una specifica vlan per il netlogin: in realtà questa vlan non viene mai usata perché ha priorità quella passata dal server Radius;
- attivazione del netlogin su Radius;
- attivazione del netlogin basato su indirizzi MAC;
- priorità al database remoto rispetto a quello locale per l’autenticazione MAC.

Nella configurazione per porta (qui si vedono 2 porte configurate allo stesso modo) vengono impostati:

- l'abilitazione del netlogin sulla porta;
- l'attivazione della modalità "mac-based-vlans" che permette allo switch di attribuire, in maniera dinamica, una vlan ad ogni mac address collegato alla porta specificata; la vlan viene fornita dal server Radius. Questa configurazione permette di gestire più mac address su una singola porta: è la situazione che si verifica se, per carenza di disponibilità di porte di rete, in un ufficio è stato installato un ulteriore switch in cascata;
- il parametro "no-restart" che fa sì che la porta non si riavvii ogni volta che viene collegato o scollegato un dispositivo;
- l'abilitazione del fallback nel caso l'autenticazione fallisca sulla porta;
- la definizione della vlan di fallback che viene assegnata alla porta, in caso di autenticazione fallita, e che sostituisce la vlan di default.

Funzionamento

L'implementazione del Network Access Control (NAC) a Padova è avvenuta in due fasi distinte per garantire una transizione fluida e minimizzare l'impatto sugli utenti.

Fase 1: Registrazione dei Dispositivi

Inizialmente, non c'è stato alcun cambiamento per gli utenti. Durante questa fase, tutti gli utenti sono stati invitati a registrare i propri dispositivi tramite un portale dedicato. L'accesso al portale è possibile utilizzando le credenziali OAPd all'indirizzo https://services.oapd.inaf.it/my-devices.php. Questa fase preliminare è cruciale per la raccolta delle informazioni sui dispositivi e la preparazione all'attivazione del sistema. In questo modo l'impatto sugli utenti è sostanzialmente nullo.

Fase 2: Attivazione del NAC

Una volta completata la prima fase di registrazione, si è proceduto con l'attivazione effettiva del NAC, modificando le impostazioni degli switch principali. A seguito di questa attivazione, qualsiasi dispositivo che tenti di connettersi alla rete senza essere riconosciuto viene automaticamente reindirizzato a una speciale rete "Ospiti".

La rete "Ospiti" è configurata come un segmento esterno, fornendo funzionalità limitate. Gli utenti che si collegano a questa rete possono accedere a Internet, ma le interazioni con i dispositivi interni della rete (come server o stampanti) sono consentite solo con le stesse restrizioni applicate a un accesso dall'esterno (ad esempio, dalla propria abitazione).

Il portale di registrazione

L'interfaccia del portale è stata concepita per la massima semplicità. Gli utenti devono semplicemente inserire e registrare l'indirizzo MAC del proprio dispositivo. È anche possibile

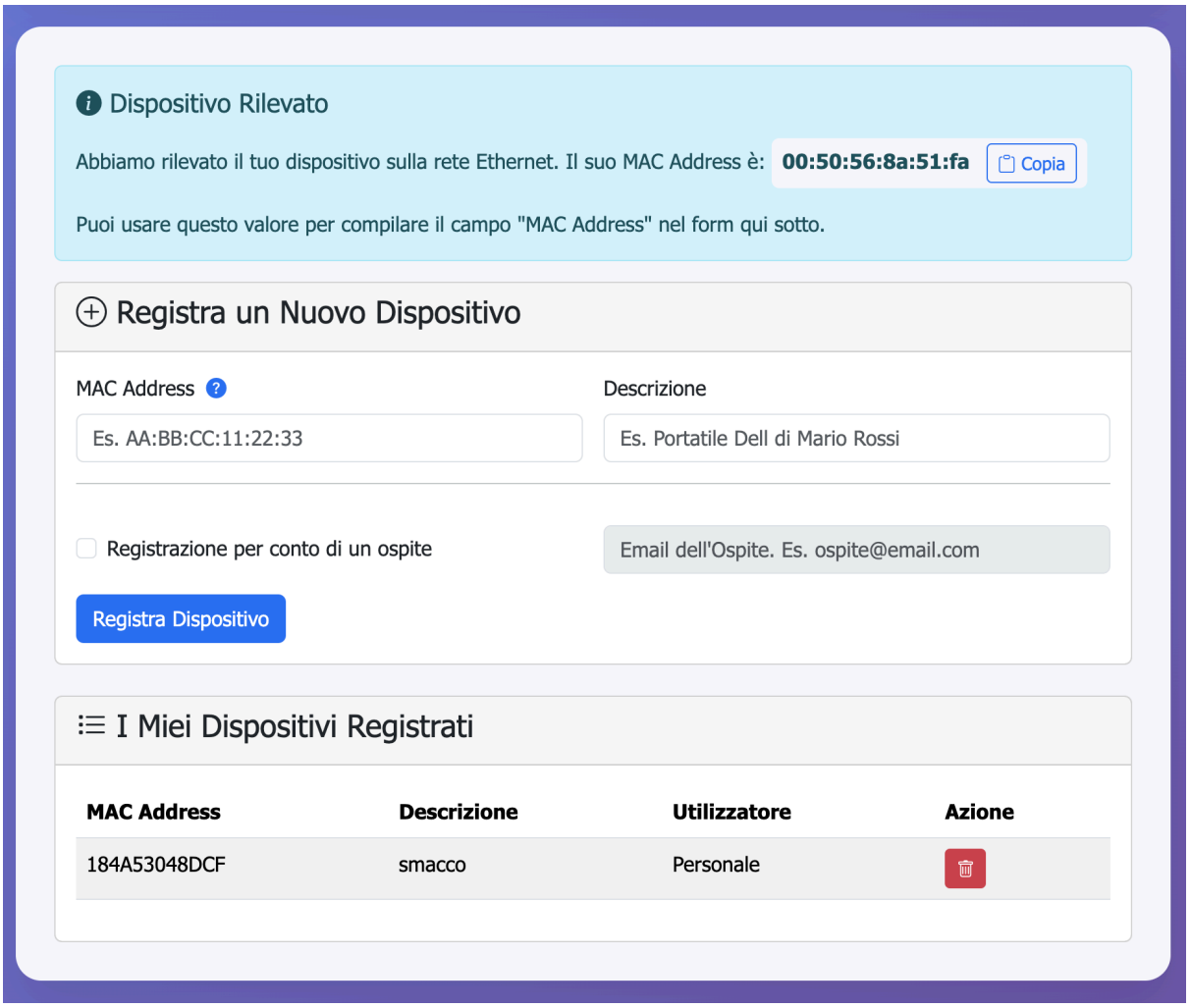
registrare il dispositivo di un ospite che non disponga di un account OAPd, ad esempio per soggiorni molto brevi. Questo permette di risalire al proprietario in caso di problemi.

L'interfaccia si sviluppa su un'unica pagina web, suddivisa in due sezioni: una per l'inserimento dei dati e una per il riepilogo.

Per facilitare l'utilizzo, in particolare per gli utenti stranieri, è stata integrata un'opzione bilingue.

Per assistere gli utenti che potrebbero avere difficoltà a trovare l'indirizzo MAC della propria scheda di rete, oltre a un manuale dettagliato accessibile cliccando sul punto interrogativo accanto all'etichetta "MAC Address" nel campo di inserimento, è stato implementato un sistema di autorilevamento che recupera l'indirizzo MAC e suggerisce all'utente di utilizzarlo per la registrazione. Il sistema di autorilevamento, però, funziona solo se il dispositivo è fisicamente collegato alla rete dell'Osservatorio.

Di seguito è mostrata una schermata di esempio.



Conclusione

L'affidabilità e la sicurezza di una rete dipendono da due categorie principali di vulnerabilità: quelle esterne e quelle interne. Le prime sono gestite attraverso un rigoroso controllo dei punti di accesso alla rete interna. Le seconde, invece, richiedono un'attenzione specifica a livello fisico, poiché qualsiasi dispositivo di rete collegato può generare potenziali problemi di sicurezza.
L'implementazione del sistema di Network Access Control (NAC) basato sull'autenticazione MAC address rappresenta un passo significativo verso il rafforzamento della sicurezza della rete ethernet dell'Osservatorio Astronomico di Padova. Nonostante i limiti intrinseci di un'architettura senza agente, la scelta è stata guidata dalla necessità di bilanciare efficacia, facilità di deployment e compatibilità con un'ampia varietà di dispositivi, inclusi quelli legacy e IoT. La gestione attenta degli aspetti legati alla privacy, in conformità con il GDPR, e la definizione di procedure chiare per la registrazione e la gestione degli accessi, garantiranno un ambiente di rete più protetto, resiliente e conforme alle normative, salvaguardando il patrimonio scientifico e la continuità operativa dell'istituzione.

Padova, 11 dicembre 2025

Amedeo Petrella
Danilo Selvestrel

Appendice

How to configure 802.1x based Netlogin with Radius on EXOS (https://extreme-networks.my.site.com/ExtrArticleDetail?an=000081809)

Objective

To configure 802.1x based Netlogin with a Windows Radius server

Environment

- EXOS
- Summit
- BlackDiamond
- Windows Server 2012

Procedure

In this example, users will be authenticated and allowed to talk in the default VLAN. Type the following commands in EXOS with a default configuration that has IP connectivity to the radius server.

- Getting IP connectivity on an EXOS switch

Note: If you plan to use Policy and NAC for 802.1x or MAC authentication use the below article:

- How to configure netlogin dot1x with policy manager in exos

Netlogin Configuration:

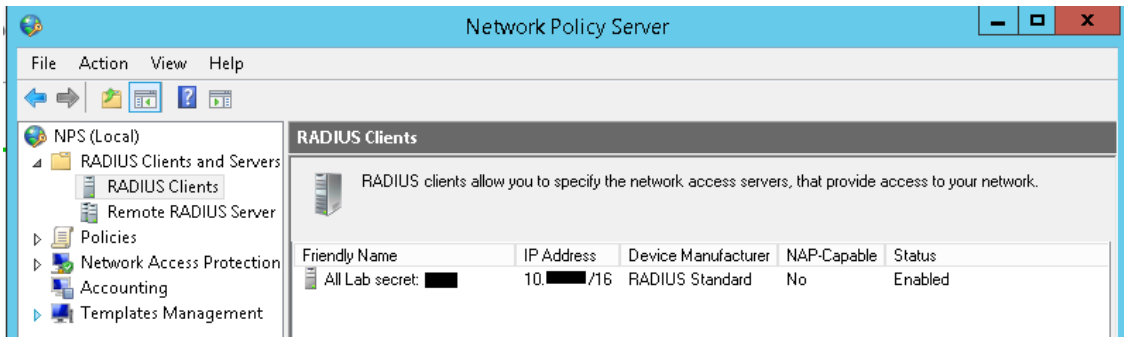
- `create vlan nt_login`
- `configure netlogin vlan nt_login`
- `enable netlogin dot1x`
- `enable netlogin ports <ports> dot1x`

Switch Radius configuration:

- `configure radius netlogin primary server <radius server IP> client-ip <source IP for radius request from switch>`
- `configure radius netlogin primary shared-secret <secret>`
- `enable radius netlogin`

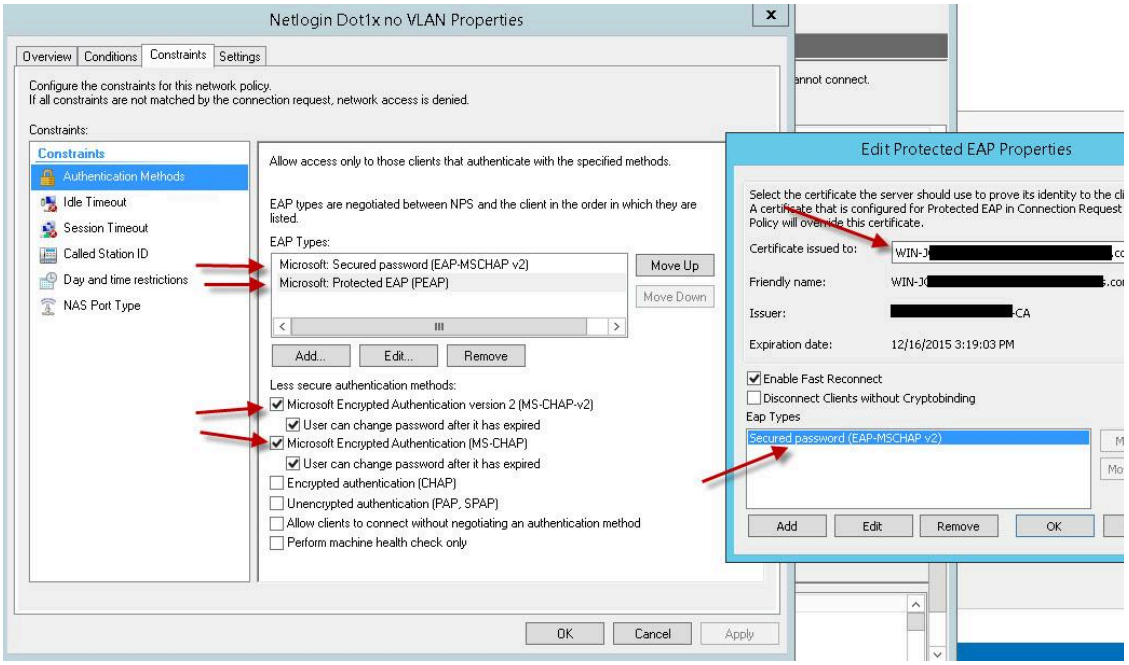
Windows server 2012 NPS configuration:

1. The radius client In the NPS server is used to allow devices to send radius authentication request to the server. Make sure you use the same shared secret configured on the switch. The Radius client IP needs to encompass the switch client IP configured earlier.

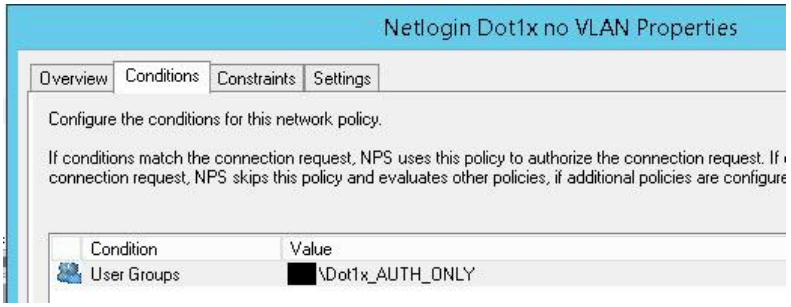


2. In the NPS settings window click on policies. Create a Network policy to allow Dot1x authentication connections that uses MS-CHAP v2 and MS-CHAP, also allow for PEAP, EAP-MSCHAPv2 EAP methods. Make sure to edit your PEAP setting to select the certificate to use.

Note: A Certificate Authority will need to be created to encrypt your logins.



3. Add the group that your Dot1x users are into the NPS policy.



Related Articles:

How to configure Mac-based Netlogin with the local database

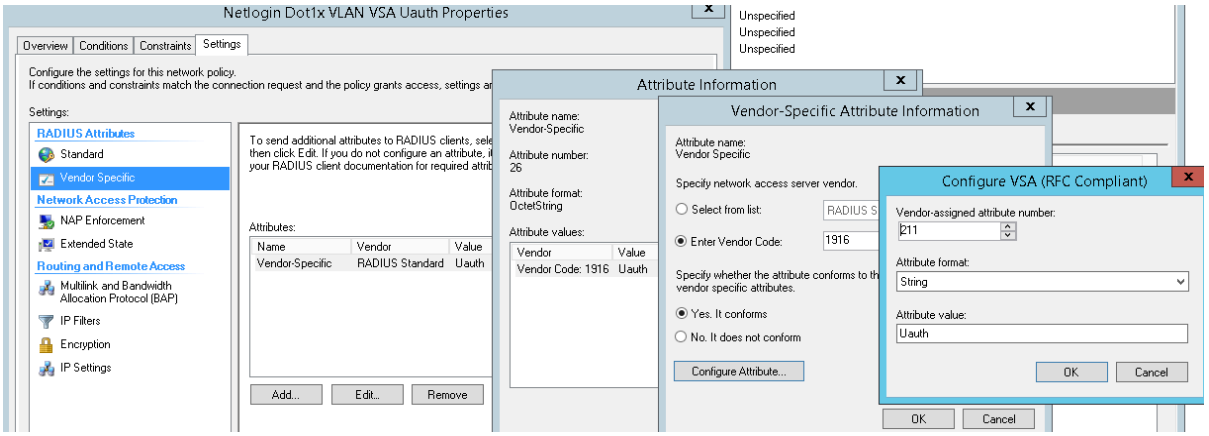
How to configure Mac-based Netlogin with Radius

Additional notes

If you would like to move the authenticated port to another VLAN you will need to send the Extreme VSA to in the RADIUS access accept.

Move port to VLAN "auth" untagged:
This will authenticate a user address through PEAP MSChap V2 and send VSA's to move the user to vlan "auth" as untagged.

Note: the VSA Attribute is Uauth U=untagged auth=vlan.



Note the VSA Attribute is Uauth U=untagged auth=vlan.

Move port to VLAN "auth" tagged:
This will authenticate a user address through PEAP MSChap V2 and send VSA's to move the user to vlan "auth" as tagged.

Note: the VSA Attribute is Tauth T=tagged auth=vlan.