



Cisco DTLab 2023/2024

Relazione finale del Project Work

Advanced Network Management System

Gruppo di Lavoro
Simone Rinaldi
Gennaro Bonanno
Francesco Pio Fontana
Valerio Domenico Conte

Indice

Project Abstract	iii
1 Descrizione del problema	1
2 Descrizione delle tecnologie implementate	3
2.1 EPN Manager	3
2.1.1 Caratteristiche	4
2.1.2 Benefici	5
2.1.3 Funzionalità utilizzate	6
2.2 CML & Cisco IOS virtuali	7
2.3 Yersinia	9
3 Descrizione della soluzione	10
3.1 Discovery dei dispositivi	11
3.1.1 Aggiunta manuale	12
3.1.2 Scoperta automatica	13
3.1.3 Bulk Import	14
3.2 Backup delle configurazioni	15
3.3 Misconfiguration detection	19
3.3.1 ACL	19

3.3.2	OSPF	21
3.4	Security	23
3.4.1	CDP Flooding	24
3.4.2	DHCP Starvation	26
3.4.3	HSRP Spoofing	28
4	Conclusioni	30
5	Sviluppi Futuri	32

Project Abstract

Our project work aims to help **Autostrade per l'Italia** enhance its network infrastructure, improving *network availability and security*. We employed **Cisco EPN Manager** to monitor and control network devices, and we simulated a small network topology through **CML** and **virtual Cisco IOS routers** to test our use cases. The final outcome has been the experimentation and learning of the powerful features provided by EPN Manager, understanding also its behavior and feedbacks in case of device configuration errors and cybersecurity attacks.

Capitolo 1

Descrizione del problema

Il nostro Project Work è stato svolto in collaborazione con **Autostrade per l'Italia (ASPI)**. Nel corso del primo incontro con un rappresentante del reparto Network dell'azienda, è stata presentata al nostro gruppo l'infrastruttura alla base della rete di telecomunicazioni ASPI attraverso una panoramica dell'architettura, della rete geografica e delle configurazioni. Le esigenze dell'azienda emerse durante l'incontro sono principalmente due:

1. **disponibilità continua**: è necessario che i diversi apparati di rete siano sempre connessi, attivi e disponibili; di conseguenza, bisogna minimizzare la durata di eventuali *downtime* della rete;
2. **rafforzamento della sicurezza**: ASPI rappresenta un'infrastruttura fondamentale per l'Italia, dunque il servizio offerto deve essere quanto più sicuro possibile, risultando robusto e proattivo.

tivo rispetto a situazioni critiche per la sicurezza come guasti di apparati o attacchi di rete.

Queste esigenze sorgono dall'impiego di nuovi apparati e tecnologie che espongono la rete a potenziali compromissioni; per affrontare questo problema, ASPI sta implementando una forte segmentazione della rete tramite appositi protocolli, isolando i servizi e le stazioni per limitare i danni in caso di attacchi.

Alla luce di quanto detto, il nostro Project Work si pone come obiettivo il miglioramento dei tempi di **riconvergenza** della rete in caso di malfunzionamenti tramite l'utilizzo e l'analisi del comportamento di **EPN Manager**, un sistema di network management avanzato sviluppato da Cisco. A tal fine, simuleremo la porzione di rete che ci è stata presentata (Figura 1.1) attraverso il software **CML**, per poi concentraci sui diversi *use cases* e comprendere le potenzialità del nostro sistema di gestione.

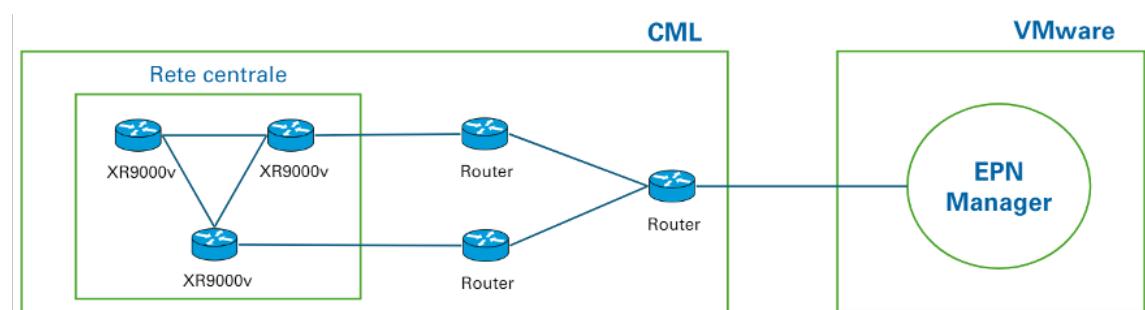


Figura 1.1: Topologia di rete

Capitolo 2

Descrizione delle tecnologie implementate

La principale tecnologia implementata è il software Cisco EPN Manager. Inoltre, per simulare la topologia di rete, abbiamo sfruttato i router virtuali Cisco IOS su CML. Infine, ai fini della sperimentazione di un caso d'uso riguardante la sicurezza della rete rispetto agli attacchi, è stata usata la suite Yersinia.

2.1 EPN Manager

Il software **Cisco Evolved Programmable Network Manager (EPN Manager)** è un potente strumento messo a disposizione degli operatori di rete per agevolarli nella risoluzione di problemi che possono colpire servizi di reti virtuali private. Questo software guida

alla risoluzione dei problemi e all’individuazione della causa principale degli allarmi attivati a partire dalla scoperta dettagliata dei dispositivi, dall’inventario e dalla topologia di rete; facilita ulteriormente il troubleshooting tramite informazioni sullo stato attuale e sugli allarmi sovrapposte alla topologia di rete, cronologia delle modifiche del servizio di rete, funzionalità di test attivi e di raccolta di metriche.

2.1.1 Caratteristiche

EPN Manager rappresenta un sistema di gestione di reti con la peculiarità che è in grado di scoprire la configurazione fisica e logica dei dispositivi gestiti, oltre ai servizi di rete forniti dalla rete stessa, e mantenere una rappresentazione aggiornata dei dispositivi e della topologia di rete. A livello di control plane, il software scopre e conserva le rappresentazioni delle associazioni di "vicinato" in tutta la rete, supportando protocolli differenti tra cui IS-IS, OSPF, BGP e LDP. Le informazioni sui dispositivi di rete vengono organizzate sotto forma di inventario e gli eventi vengono tempestivamente segnalati attraverso alert con diversa priorità. Complessivamente, EPN Manager coadiuva le operazioni di rete nel ridurre:

- i tempi di conoscenza e di azione attraverso capacità di monitoraggio completo;
- il tempo medio di riparazione di guasti attraverso funzionalità di risoluzione problemi che sfruttano informazioni dettagliate

presenti in rete;

- il tempo medio per configurare e migliorare la precisione delle configurazioni di rete attraverso funzionalità di configurazione grafica;
- il tempo dedicato ai task quotidiani di routine attraverso un’interfaccia utente grafica centralizzata per l’amministrazione di rete.

Il ricco set di funzioni di gestione di dispositivi e reti è facilmente accessibile agli operatori tramite una GUI, inclusa una schermata iniziale configurabile che riassume le informazioni principali sullo stato della rete.

2.1.2 Benefici

La scelta di EPN Manager è motivata dal fatto che rappresenta un gestore di elementi e di reti che ci consente di:

- conoscere la nostra rete con maggiore precisione;
- ridurre il tempo di attivazione della capacità di rete;
- ridurre il tempo di conoscenza dello stato della nostra rete;
- ridurre il tempo per ripristinare la capacità di rete.

È chiaro, dunque, che tale network manager ben si presta a supportarci nel nostro lavoro che prevede di migliorare scoperta dei guasti, manutenzione dei dispositivi e riconvergenza della rete.

2.1.3 Funzionalità utilizzate

EPN Manager mette a disposizione moltissime funzionalità, accessibili tramite un'interfaccia grafica intuitiva (Figura 2.1). Le sezioni e le funzionalità per noi di interesse sono state:

- **Inventario**, dove poter aggiunta e scoperta dei dispositivi di rete;
- **Mappa della rete**, dove viene mostrata graficamente la topologia della rete a cui abbiamo connesso il sistema di management, consentendoci di visualizzare i dispositivi e la correttezza dei loro collegamenti;
- **Archivio delle configurazioni**, dove visualizzare i backup delle configurazioni dei network devices ed effettuare operazioni come il rollback o lo scheduling periodico delle archiviazioni;
- **Alarm notifications**, cioè avvisi che tempestivamente ci hanno messo al corrente di cambiamenti nella rete, segnalando dunque eventuali malfunzionamenti dovuti a msiconfiguration di dispositivi o attacchi.

CAPITOLO 2. DESCRIZIONE DELLE TECNOLOGIE IMPLEMENTATE

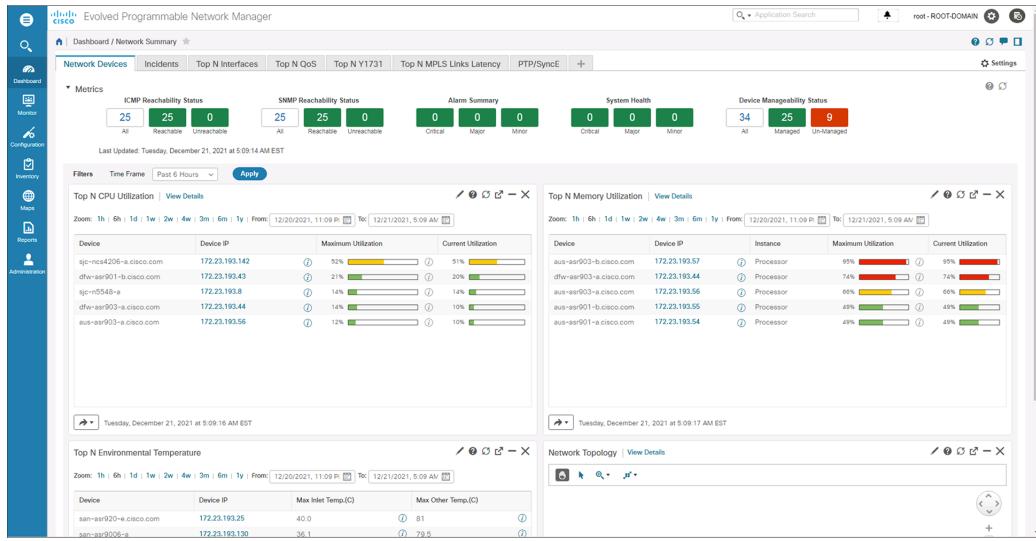


Figura 2.1: Interfaccia grafica EPN Manager

2.2 CML & Cisco IOS virtuali

La piattaforma **Cisco Modeling Labs (CML)** consente di simulare in maniera semplice e veloce una grande varietà di topologie di rete, fornendo dei modelli affidabili per progettare, testare ed effettuare troubleshooting. Il vantaggio, nel nostro caso, è quello di poter testare i casi d'uso in maniera sicura, veloce ed economica dato che utilizzando questa piattaforma ci consente di non dover acquistare fisicamente i dispositivi necessari. CML è dotato di uno store centralizzato dove è possibile ottenere immagini originali dei dispositivi **Cisco IOS (Internetwork Operating System)**. Come anticipato, la nostra topologia è composta da sei router, di cui tre sono core router e tre sono edge router. I router virtuali che abbiamo utilizzato su CML sono differenti a seconda della loro tipologia:

- Core Routers: **Cisco XR9000v**

- Edge Routers: Cisco Catalyst 8000v

Per i core routers abbiamo utilizzato quelli indicati dall’azienda, mentre per gli edge routers abbiamo optato per dei modelli che prevedono un consumo di risorse più basso. I router che eseguono il sistema operativo IOS XR sono dotati di **LPTS (Local Packet Transport Services)**, un sistema di sicurezza e gestione del traffico che serve a proteggere il control plane dei router da attacchi o sovraccarichi. In particolare, questo servizio:

- filtra e gestisce i pacchetti destinati al router IOS XR, per prevenire il sovraccarico del control plane, instabilità o malfunzionamenti;
- limita la velocità dei pacchetti in arrivo, per evitare che il router venga inondato da pacchetti di controllo, proteggendo le risorse come CPU e memoria;
- monitora e controlla il traffico di protocollo (OSPF, BGP...), garantendo che i pacchetti di questi protocolli siano processati correttamente senza creare overload.

Si tratta dunque di router ad alte prestazioni e vengono utilizzati tipicamente in reti di grandi dimensioni, come le reti di backbone. In Figura 2.2 troviamo la nostra porzione di rete simulata su CML.



Figura 2.2: Topologia di rete su CML

2.3 Yersinia

Il tool **Yersinia** è un framework utilizzato in ambito di sicurezza informatica per test di penetrazione sulle reti, in particolare può essere utilizzato per eseguire attacchi di livello 2 del modello OSI (Data Link Layer), sfruttando alcune debolezze in diversi protocolli di rete di questo livello.

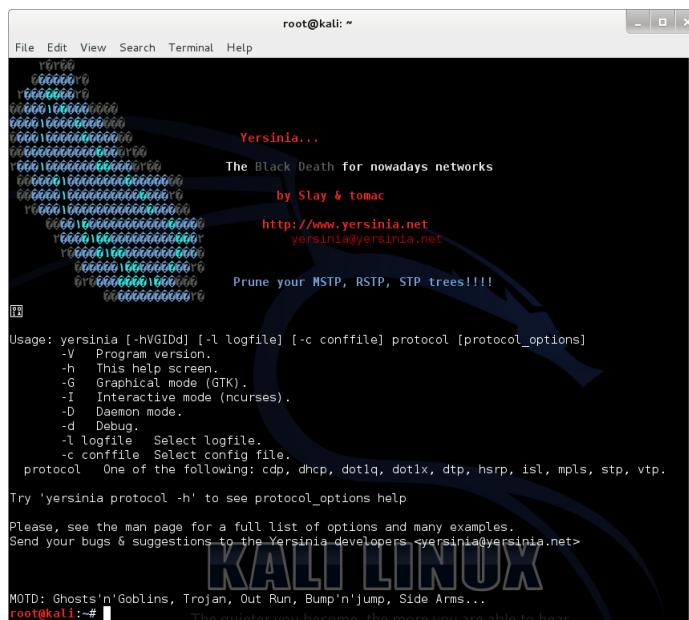


Figura 2.3: Yersinia

Capitolo 3

Descrizione della soluzione

In questa parte del progetto ci siamo occupati di mettere in pratica le conoscenze acquisite su EPN Manager consultando la relativa documentazione [1] con l'obiettivo di testare alcuni scenari di utilizzo. Ci siamo concentrati sui seguenti use cases:

- Discovery dei dispositivi
- Backup delle configurazioni
- Misconfiguration detection
- Security

I primi due casi sono stati proposti dall’azienda mentre gli ultimi due sono stati pensati dal nostro team. Di seguito un’analisi approfondita di ognuno di essi.

3.1 Discovery dei dispositivi

Il primo step per iniziare a utilizzare EPN Manager con la propria rete è l’aggiunta dei dispositivi di rete che ne fanno parte all’inventario. Le modalità di aggiunta o scoperta di dispositivi supportate sono tre:

1. **Manuale**
2. **Automatica**
3. **Bulk Import**

Queste modalità sono accessibili dalla GUI di EPN Manager andando nella sezione *Inventory > Device Management*. Per quanto riguarda la costruzione esatta della topologia di rete, se sui dispositivi aggiunti è stato abilitato e configurato OSPF, come nel nostro caso, il sistema apprende autonomamente quali sono i link esistenti tra i devices; nella sezione *Maps* possiamo visualizzare graficamente la topologia ricostruita da EPN Manager. Di seguito analizziamo in maniera più dettagliata le modalità di aggiunta e scoperta di network devices.

3.1.1 Aggiunta manuale

La modalità manuale consente di aggiungere un dispositivo alla volta, possiamo usarla per esempio quando vogliamo aggiungere un nuovo tipo di dispositivo. In Figura 3.1 possiamo osservare che bisogna specificare parametri generali come l'indirizzo IP del dispositivo, il ruolo e il gruppo di appartenenza, nonché le sue credenziali SNMP e SSH2. Per velocizzare la compilazione dei parametri necessari all'aggiunta di un dispositivo in futuro è possibile creare dei profili per le credenziali che vorremmo riutilizzare quando necessario.

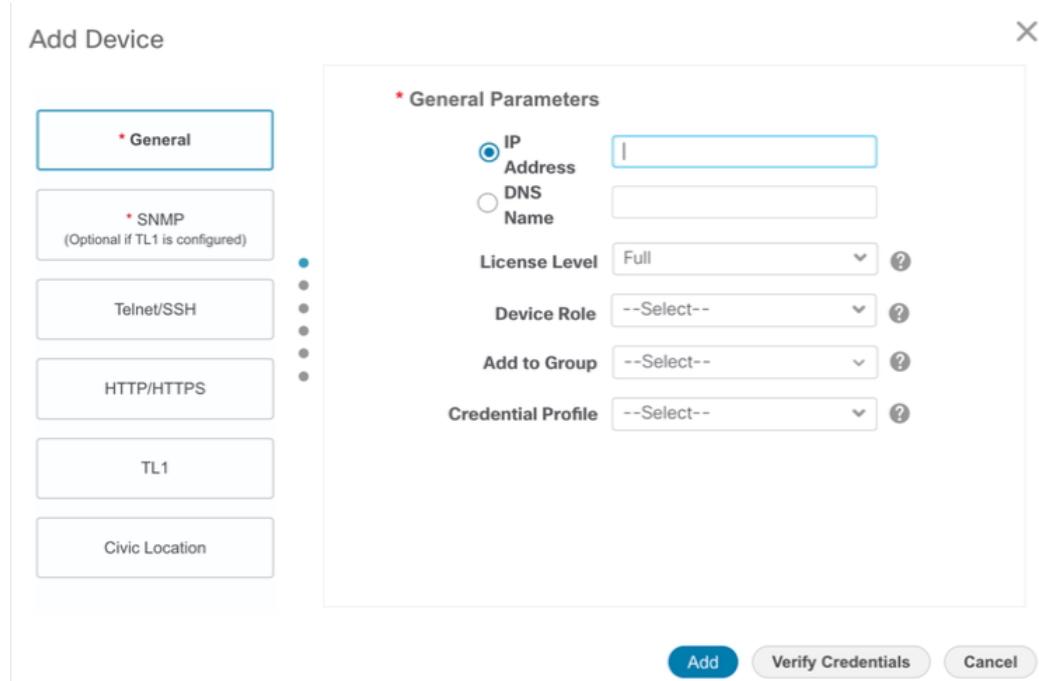


Figura 3.1: Finestra aggiunta manuale

3.1.2 Scoperta automatica

La modalità automatica consente di aggiungere uno o più dispositivi scoprendo i vicini di un dispositivo *seed*. Tale scoperta può avvenire in due modi:

- **Quick Discovery:** vengono effettuate operazioni di ping sweep e polling SNMP dal dispositivo *seed* per determinare la mappa di rete; sono richiesti il nome del dispositivo da trovare, la community SNMP, l'indirizzo IP della rete *seed* e la subnet mask. Questo metodo non è però supportato per la scoperta di dispositivi ottici;

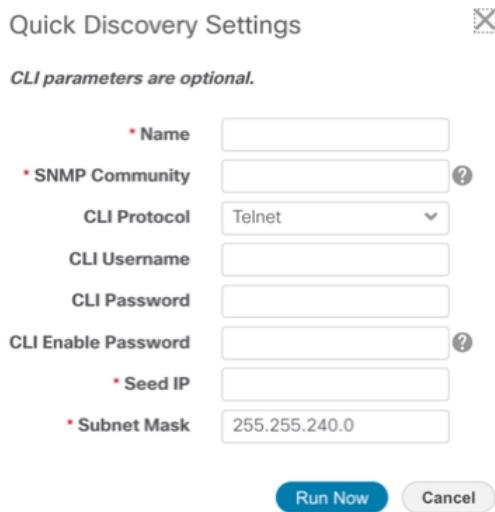


Figura 3.2: Finestra Quick Discovery

- **Discovery with Customized Settings:** possiamo personalizzare impostazioni di protocollo, credenziali e filtro. Questa opzione è utile per specificare impostazioni che vogliamo riutilizzare nel caso in cui dovremo ripetere il processo di scoperta;

inoltre, ci consente di scoprire dispositivi ottici. Questa modalità ci consente di creare, dunque, dei profili personalizzati di scoperta, dandoci la possibilità di scegliere tra molteplici protocolli quello che vogliamo utilizzare per la scoperta, per esempio OSPF, CDP o LLDP.

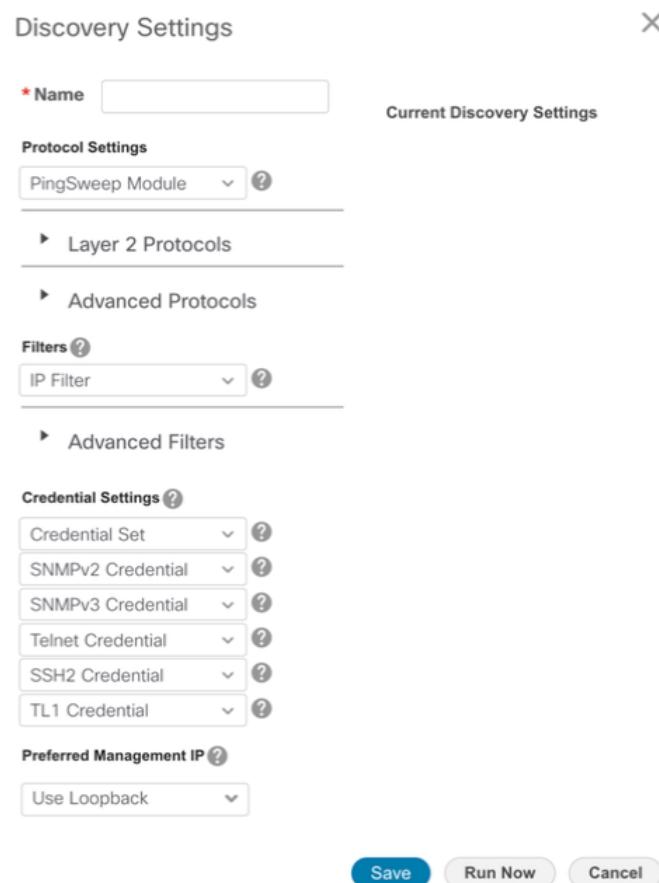


Figura 3.3: Finestra Custom Discovery

3.1.3 Bulk Import

La modalità Bulk Import consente di importare in maniera semplice dispositivi già aggiunti ad altri sistemi di management. Come possia-

mo vedere in Figura 3.4, è sufficiente caricare un file CSV contenente le loro configurazioni e il template CSV è messo a disposizione da EPN Manager stesso.

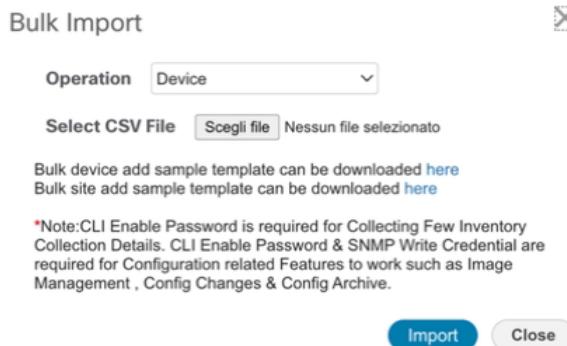


Figura 3.4: Finestra Bulk Import

3.2 Backup delle configurazioni

EPN Manager esegue di default il backup delle configurazioni in due occasioni:

- quando un nuovo dispositivo viene aggiunto all'inventario;
- quando viene ricevuta una notifica una notifica di modifica di un dispositivo.

Nel secondo caso, il sistema attende 10 minuti prima di archiviare la nuova configurazione, in maniera tale da minimizzare il numero di volte che il backup viene effettuato perché in quell'intervallo di tempo potrebbero avvenire ulteriori cambiamenti del dispositivo. Questo tempo di attesa può essere modificato dall'amministratore di rete.

CAPITOLO 3. DESCRIZIONE DELLA SOLUZIONE

Nella sezione **Archives** è possibile consultare la lista dei file di configurazione che sono stati archiviati.

The screenshot shows a table titled 'All Devices' with two tabs: 'Devices' and 'Archives'. The 'Archives' tab is selected. The table has columns for Device Name, IP Address, Date, Created By, Tag, Description, Software Ver..., and Out Of There are 11 entries listed, mostly for CORE-R1, CORE-R2, and CORE-R3 devices, with various creation dates and descriptions like 'root', 'Syslog', and 'Inventory'.

Device Name	IP Address	Date	Created By	Tag	Description	Software Ver...	Out Of ...
CORE-R1.localdomain	10.10.10...	September 09, 2024, 11:24	root		Archived By Job Nar	7.4.1	No
CORE-R1.localdomain	10.10.10...	August 09, 2024, 09:33:12	Syslog		Archived by syslog f	7.4.1	No
CORE-R1.localdomain	10.10.10...	August 11, 2024, 10:01:53	Syslog		Backup has not been	7.4.1	No
CORE-R1.localdomain	10.10.10...	August 09, 2024, 06:05:21	Inventory		Initial version	7.4.1	No
CORE-R2.localdomain	10.10.10...	August 11, 2024, 10:01:17	root		Archived By Job Nar	7.4.1	No
CORE-R2.localdomain	10.10.10...	September 09, 2024, 11:24	root		Archived By Job Nar	7.4.1	No
CORE-R2.localdomain	10.10.10...	August 09, 2024, 12:25:34	Syslog		Archived by syslog f	7.4.1	No
CORE-R3	10.10.10...	August 09, 2024, 04:36:40	Inventory		Archived by inventor	7.4.1	No
CORE-R3	10.10.10...	August 09, 2024, 04:36:01	Inventory		Backup has not been	7.4.1	No
CORE-R3.localdomain	10.10.10...	September 09, 2024, 11:24	root		Archived By Job Nar	7.4.1	No
CORE-R3.localdomain	10.10.10...	August 11, 2024, 10:11:13	Syslog		Backup has not been	7.4.1	No

Figura 3.5: Elenco dei backup effettuati

In questa sezione possiamo visualizzare i dettagli di ogni archivio, come la data di creazione e tutte le configurazioni memorizzate al suo interno. Possiamo filtrare i backup sfruttando data e ora della loro esecuzione.

The screenshot shows a table titled 'Configuration Archive Details' with several tabs at the top: 'Schedule Archive Rollback', 'Schedule Archive Overwrite', 'Edit Tag', 'Schedule Archive Collection', 'Schedule Archive Deploy', 'Show', 'Quick Filter', and a search icon. The table has columns for Latest Config Change, Latest Archive Sync, Software Version, Created By, Tag, Description, and Out of band. One row is selected, showing details for a configuration change on September 09, 2024, at 11:24, with software version 7.4.1 and created by 'root'. It also shows sections for Running Configuration, Startup Configuration, Admin Configuration, and Vlan Configuration, each with their own tabs and comparison options.

Latest Config Change	Latest Archive Sync	Software Version	Created By	Tag	Description	Out of band
September 09, 2024, 11:24...	September 09, 2024, 11:24...	7.4.1	root		Archived By Job Name: J...	Yes
Running Configuration	Startup Configuration	Admin Configuration	Vlan Configuration			
Configurations	There is no Startup configuration available for this Device	Configurations	There is no Vlan configuration available for this Device			
Details		Details				
Compare	Previous Other Version Other Device	Compare	Previous Other Version Other Device			
<input type="radio"/> ► August 11, 2024, 10:01:43 A...	August 11, 2024, 10:01:53 A...	7.4.1	Syslog	Backup has not been perf...	Yes	
<input type="radio"/> ► August 09, 2024, 09:33:12 P...	August 09, 2024, 09:33:12 P...	7.4.1	Syslog	Archived by syslog from 1...	Yes	
<input type="radio"/> ► August 09, 2024, 06:05:21 P...	August 09, 2024, 06:05:21 P...	7.4.1	Inventory	Initial version	No	

Figura 3.6: Dettagli di un archivio

Qui troviamo tre funzionalità interessanti:

- **Schedule Rollback:** questa funzione consente di pianificare il ripristino di una configurazione precedente su uno o più dispositivi. Se si verifica un problema con una configurazione recente, è possibile programmare un rollback alla configurazione precedente che si trova negli archivi, per ripristinare lo stato funzionante del dispositivo;
- **Schedule Collection:** questa opzione permette di pianificare la raccolta delle configurazioni dai dispositivi di rete. Consente di ottenere una copia aggiornata della configurazione attuale di un dispositivo (ad esempio router o switch) e salvarla nell'archivio di Cisco EPN Manager. È utile per monitorare lo stato dei dispositivi e tenere traccia delle modifiche nel tempo;

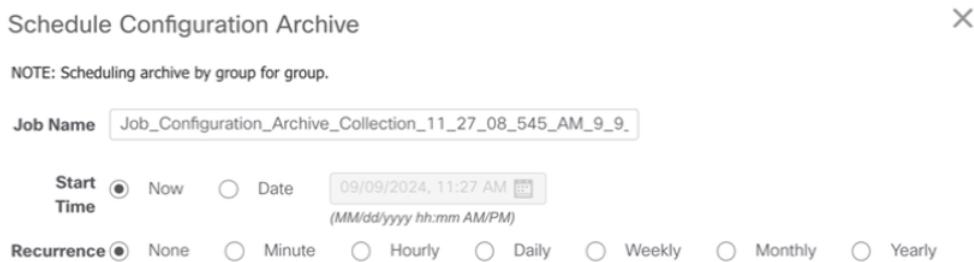


Figura 3.7: Scheduling dei backup delle configurazioni

- **Schedule Deploy:** con questa opzione è possibile pianificare la distribuzione di una configurazione o di aggiornamenti specifici su uno o più dispositivi di rete. Cisco EPN Manager invia la configurazione desiderata ai dispositivi selezionati nell'orario

CAPITOLO 3. DESCRIZIONE DELLA SOLUZIONE

prestabilito, permettendo una gestione automatica e controllata degli aggiornamenti.

La sezione *Compare* fornisce tre possibilità per effettuare un confronto tra la configurazione selezionata per un certo dispositivo con un'altra: possiamo confrontarla con quella immediatamente precedente, con una configurazione ancora più vecchia o con quella di un altro dispositivo. Tale funzionalità è utile, per esempio, per trovare in maniera rapida le differenze tra una running configuration che ha generato un misconfiguration alert ed una "golden configuration", cioè l'ultima configurazione funzionante per quel dispositivo, individuano così gli errori di configurazione che hanno generato quell'alert.

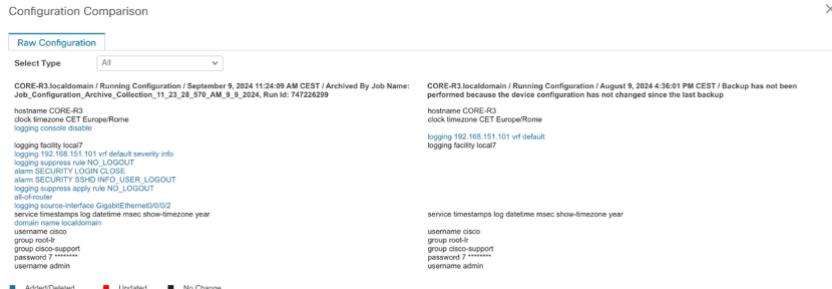


Figura 3.8: Confronto tra configurazioni

Se vogliamo esportare una configurazione archiviata possiamo scegliere due modalità di esportazione:

1. Sanitized: le password presenti vengono mascherate;
2. Unsanitized: le password presenti vengono salvate in chiaro.

Le configurazioni così esportate possono poi essere facilmente deployate sui dispositivi in caso di necessità.

The screenshot shows a window titled "Running Configuration: CORE-R1.locaLdomain". The main area displays the raw configuration in a text editor-like interface. The configuration includes basic system settings like hostname, clock timezone, logging levels, and user authentication. A note at the bottom states: "Configuration Archive Collection Time: September 9, 2024 11:24:09 AM CEST" and "Note: All the sensitive information such as password, SNMP community string will be masked in both Processed Configuration and Raw Configuration. If you want to view sensitive information such as password, SNMP community string, export the configuration using Unsanitized option." Buttons for "Export" and "Close" are visible at the bottom right.

```
!! IOS XR Configuration 7.4.1
!! Last configuration change at Fri Sep 6 17:55:55 2024 by aspi
!
hostname CORE-R1
clock timezone CET Europe/Rome
logging trap informational
logging events level informational
logging console disable
logging facility local7
logging 192.168.151.101 vrf default severity info
service timestamps log datetime msec show-timezone year
logging events link-status software-interfaces
domain name localdomain
username aspi
group root-lr
group cisco-support
secret 10 *****
!
cdp
line console
exec-timeout 0 0
```

Figura 3.9: Finestra esportazione di una configurazione

3.3 Misconfiguration detection

In questo use case ci siamo concentrati sui feedback di EPN Manager in caso di errata configurazione di protocolli, osservando gli alert generati dal sistema. Per testare la misconfiguration detection sono stati introdotti alcuni errori comuni nelle configurazioni dei dispositivi di rete. La prima misconfiguration riguarda ACL (Access Control List) mentre la seconda riguarda OSPF (Open Shortest Path First).

3.3.1 ACL

ACL (Access Control List) è una funzione di sicurezza utilizzata nei router e nei dispositivi di rete per controllare il traffico in entrata e in uscita. Una ACL corrisponde ad una serie di regole che specificano quali pacchetti di dati possono attraversare un'interfaccia di rete in base a criteri predefiniti, come l'indirizzo IP di origine, l'indirizzo IP

di destinazione, il protocollo utilizzato (TCP, UDP, ICMP...), le porte di origine e destinazione, e altro. Per il router CORE-R3 della nostra topologia è stata configurata in maniera errata la ACL in maniera tale da bloccare il traffico in entrata sulla sua interfaccia G0/0, traffico che in realtà dovrebbe essere lasciato entrare perché legittimo.

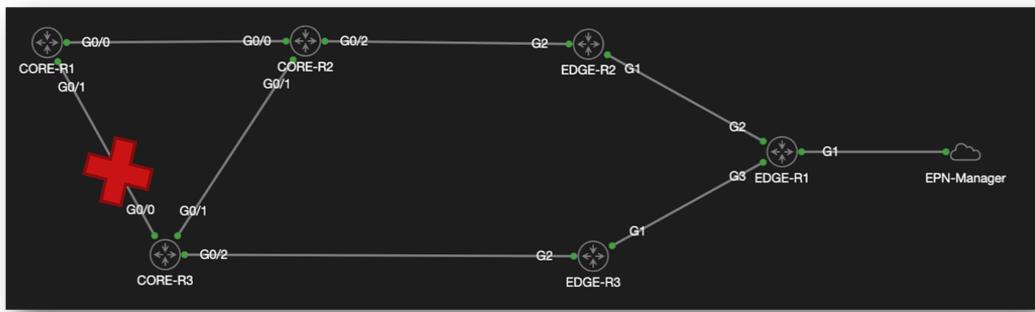


Figura 3.10: ACL Misconfiguration

Quando il router CORE-R1 prova a inviare traffico su quel link, il traffico viene bloccato e viene generato un alert generico di priorità Minor su EPN Manager che segnala l'interruzione della sessione BFD tra i due router (Figura 3.11). Non c'è alcun riferimento specifico ad ACL nell'alert, tuttavia avendo configurato BFD (Bidirectional Forwarding Detection, protocollo di rete utilizzato per rilevare guasti tra due router o switch connessi tramite un link) veniamo comunque avvisati su un problema di comunicazione. Sfruttando la funzionalità *Configuration Comparison* vista prima, abbiamo confrontato la configurazione problematica del router con l'ultima funzionante per individuare il problema (Figura 3.12).

CAPITOLO 3. DESCRIZIONE DELLA SOLUZIONE

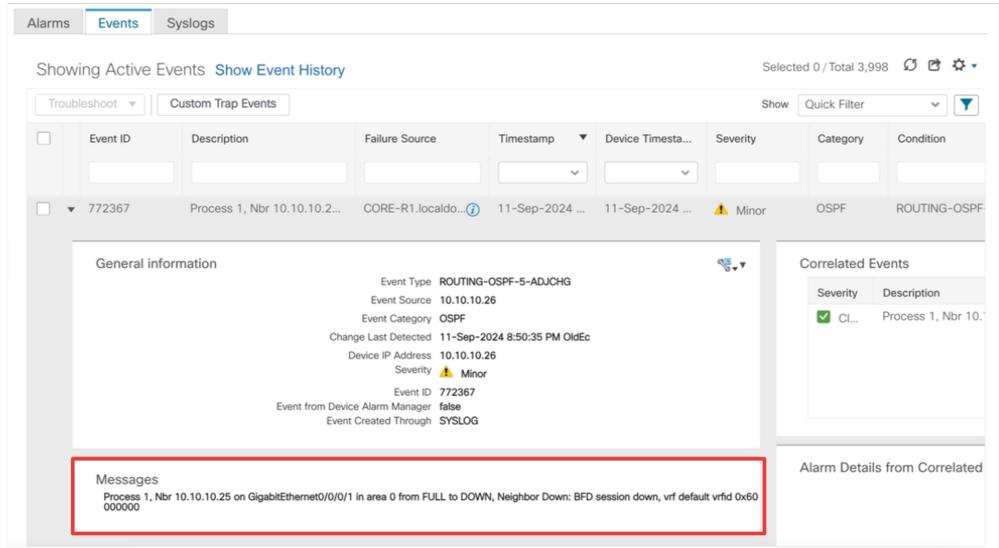


Figura 3.11: ACL Misconfiguration Alert

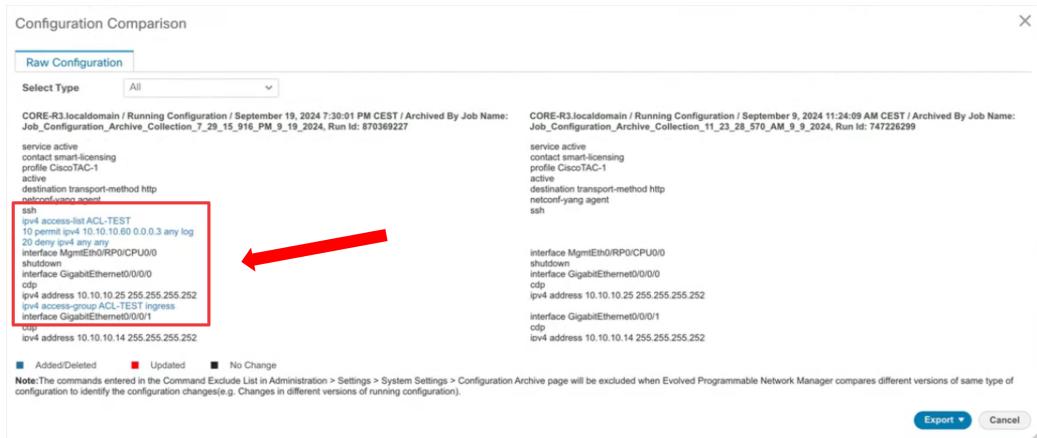


Figura 3.12: Confronto tra configurazioni ACL

3.3.2 OSPF

OSPF (Open Shortest Path First) è un protocollo di routing dinamico, di tipo link-state, utilizzato nelle reti IP per determinare il percorso migliore per il traffico di rete. Sfrutta l'algoritmo di Dijkstra per determinare i percorsi di costo minimo ed è ampiamente impiegato perché è scalabile ed efficiente, supportando reti di diversa dimensione e complessità. In quanto protocollo di routing intra-dominio, lo scambio di

pacchetti sullo stato dei collegamenti (LSP) è limitato ai router che appartengono alla stessa area; un router di confine dell'area si occupa poi di trasmettere una sintesi delle informazioni di routing riguardante le propria area ad un altro router di confine. Abbiamo introdotto la misconfiguration assegnando le interfacce che connettono i router CORE-R1 e CORE-R3 a due aree diverse, quindi, le interfacce G0/1 (CORE-R1) e G0/0 (CORE-R3) avranno Area ID differenti perché la prima appartiene all'area di backbone (Area 0), la seconda all'Area 1.

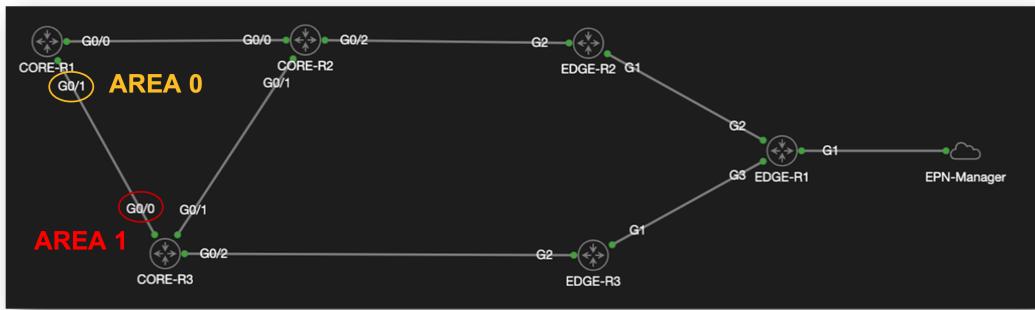


Figura 3.13: OSPF Misconfiguration

Alla ricezione di pacchetti OSPF, viene generato un alert specifico di priorità Major che segnala la ricezione di un pacchetto non valido perché per ricevere dall'area di backbone deve essere stato configurato un collegamento virtuale che però non è stato trovato (Figura 3.14). Anche in questo caso abbiamo messo a confronto la configurazione problematica con l'ultima funzionante (Figura 3.15).

CAPITOLO 3. DESCRIZIONE DELLA SOLUZIONE

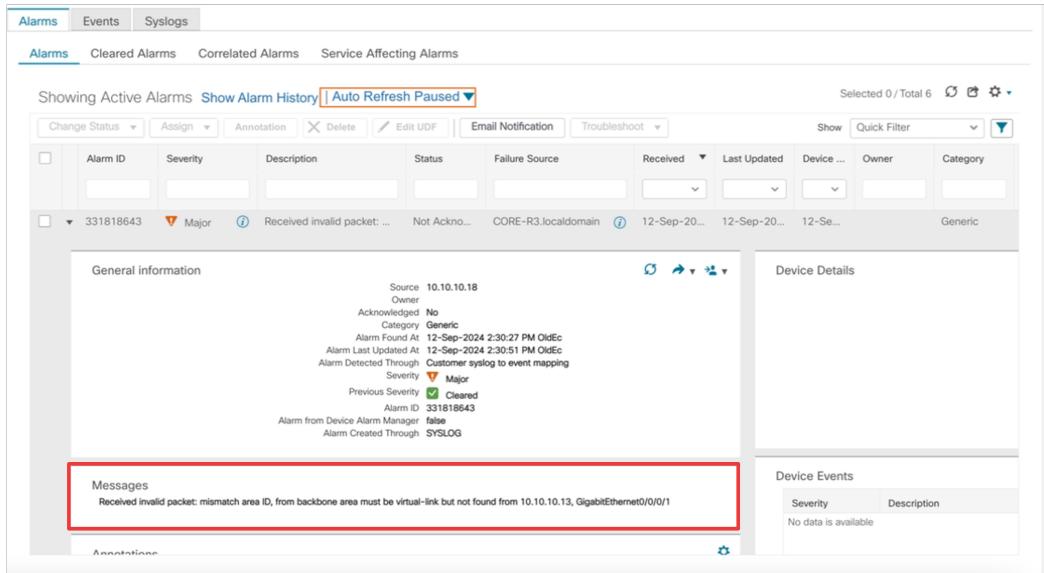


Figura 3.14: OSPF Misconfiguration Alert



Figura 3.15: Confronto tra configurazioni OSPF

3.4 Security

Il framework Yersinia ci ha aiutato nell'effettuare il penetration test della nostra rete per valutare la capacità di EPN Manager di rilevare minacce, osservando i feedback da parte del sistema. Abbiamo simulato tre tipi di attacchi verso dispositivi di rete:

- CDP Flooding

- DHCP Starvation
- HSRP Spoofing

Un rilevamento tempestivo di anomalie permette agli amministratori di rete di agire subito, individuando la precisa problematica in maniera semplice e riducendo il tempo di disservizio della rete che, nel caso di ASPI, può essere particolarmente critico. Di seguito un'analisi più dettagliata dei nostri test e dei conseguenti alert generati da EPN Manager.

3.4.1 CDP Flooding

Il **Cisco Discovery Protocol (CDP)** è un protocollo di rete proprietario, sviluppato da Cisco Systems. Viene utilizzato dai dispositivi Cisco per scambiarsi informazioni su una rete locale, facilitando il rilevamento di dispositivi e la gestione della rete. CDP opera a livello 2 del modello OSI e consente a dispositivi come router e switch di scambiarsi dati come versione del sistema operativo, tipo di dispositivo, indirizzi IP, VLAN e molto altro. Un attacco di tipo **CDP Flooding** consiste nel sovraccaricare la rete con un numero eccessivo di pacchetti CDP, disturbando il normale funzionamento della rete. Le conseguenze di un attacco del genere sono:

- saturazione della rete: il traffico malevolo spreca risorse di rete, provocando una diminuzione della capacità disponibile per il

traffico legittimo;

- instabilità dei dispositivi: i devices potrebbero avere difficoltà a gestire questa "inondazione" di pacchetti anomala, potrebbero addirittura andare in crash.

Nel nostro caso, abbiamo inserito su CML un nodo malevolo collegato al ruoter CORE-R2. L'attaccante inonda questo router con un gran numero di pacchetti CDP falsificati.

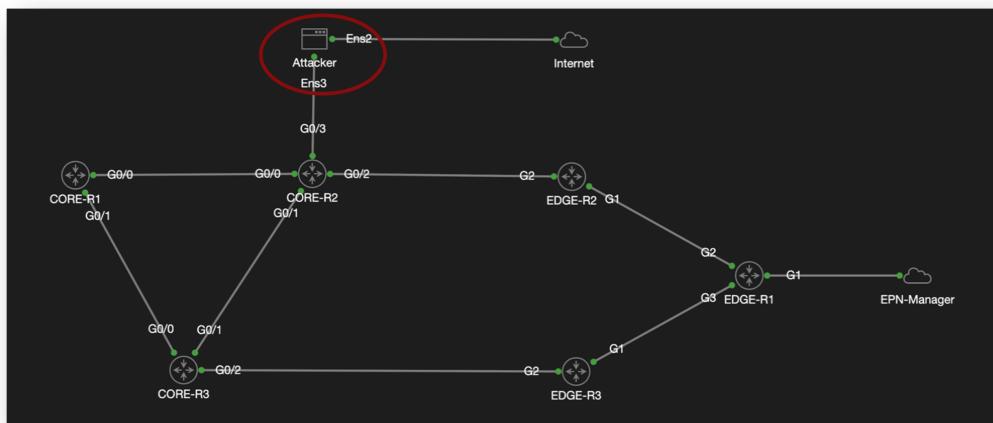


Figura 3.16: Topologia con attaccante CDP

Il feedback da parte di EPN Manager al rilevamento dell'anomalia è un alert di priorità Critical, questo avvisa l'utente che la cache CDP di quel router si è riempita poiché contiene voci riguardanti 1000 nodi vicini. Ovviamente i pacchetti falsificati hanno tutti indirizzi IP sorgente differenti, provocando questa situazione che non rispecchia la realtà.

CAPITOLO 3. DESCRIZIONE DELLA SOLUZIONE

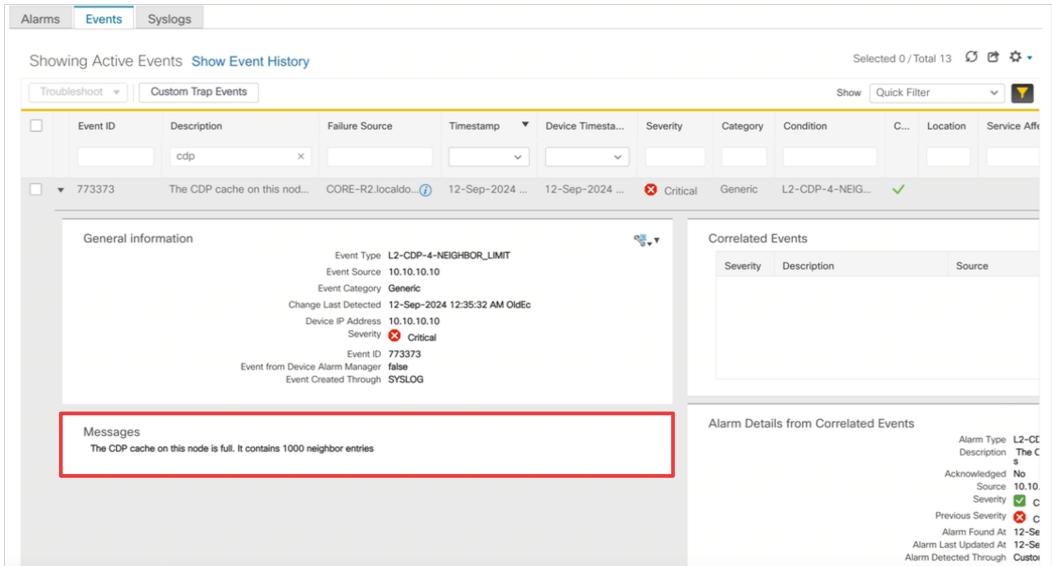


Figura 3.17: CDP Alert

3.4.2 DHCP Starvation

Il **Dynamic Host Configuration Protocol (DHCP)** consente a un server di assegnare automaticamente indirizzi IP e altre configurazioni di rete ai dispositivi client che si connettono a una rete. In questo modo, i dispositivi non devono essere configurati manualmente per accedere alla rete, semplificando la gestione di reti complesse. Una **DHCP Starvation** esaurisce tutti gli indirizzi IP disponibili su un server DHCP, rendendoli non più disponibili per altri dispositivi legittimi. L'obiettivo è dunque impedire a nuovi dispositivi di ottenere un indirizzo IP, bloccando l'accesso alla rete. Per testare questo attacco abbiamo configurato il router CORE-R2 come server DHCP; il nodo attaccante è ancora una volta collegato a questo router.

L'attaccante invia un'enorme quantità di pacchetti DHCP Discovery con indirizzi MAC falsificati per esaurire tutte le assegnazioni di

CAPITOLO 3. DESCRIZIONE DELLA SOLUZIONE

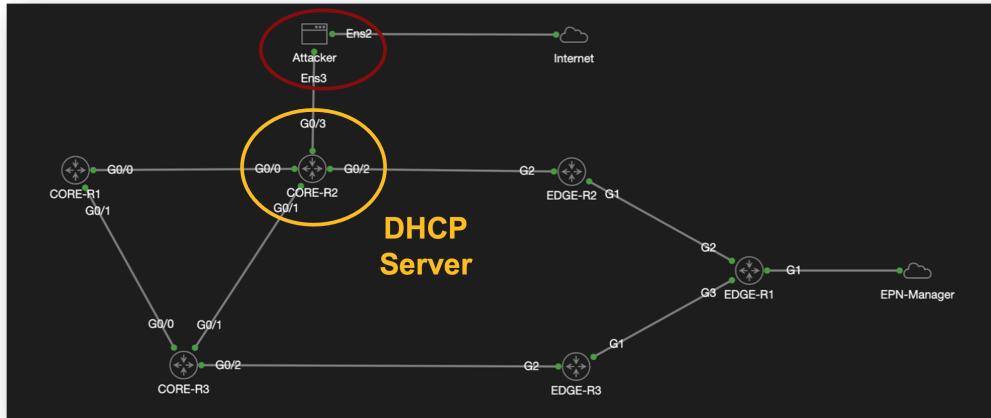


Figura 3.18: Topologia con attaccante DHCP

indirizzi IP. EPN Manager segnala l'anomalia attraverso due alert di diversa priorità, avvisando che il limite sul rate di pacchetti DHCP inviabili è stato superato e che ulteriori pacchetti potrebbero essere persi; questo comportamento è proprio una forma di protezione nei confronti di attacchi del genere.

Event ID	Description	Failure Source	Timestamp	Device Timestamp	Severity	Category	Condition	Location	Service Aff
791363	Packet may be Dropped!, R...	CORE-R2.localdom...	13-Sep-2024 ...	13-Sep-2024 ...	Critical	Generic	IP-DHCPD-4-RA...		
790364	Device 'CORE-R2.localdom...	10.10.10.10:CO...	13-Sep-2024 ...	13-Sep-2024 ...	Minor	Generic	GENERIC_EVENT		

Figura 3.19: DHCP Alert

3.4.3 HSRP Spoofing

Hot Standby Router Protocol (HSRP) è un protocollo di routing sviluppato da Cisco che consente a più router di lavorare insieme per garantire la ridondanza e l'alta disponibilità di una rete. Viene utilizzato principalmente per fornire un gateway di default virtuale ai dispositivi in una LAN, in modo che, se il router principale fallisce, un router secondario possa immediatamente prenderne il posto senza interrompere la connettività. Un attacco **HSRP Spoofing** cerca di ingannare questo protocollo affinché il malintenzionato possa prendere il controllo del ruolo di router attivo, con l'obiettivo di intercettare, manipolare o bloccare il traffico di rete. Per questo attacco, oltre ad aggiungere un host attaccante, abbiamo inserito nella rete uno switch collegato all'attaccante e ai due core routers nello stato Active e Standby, rispettivamente CORE-R2 e CORE-R1.

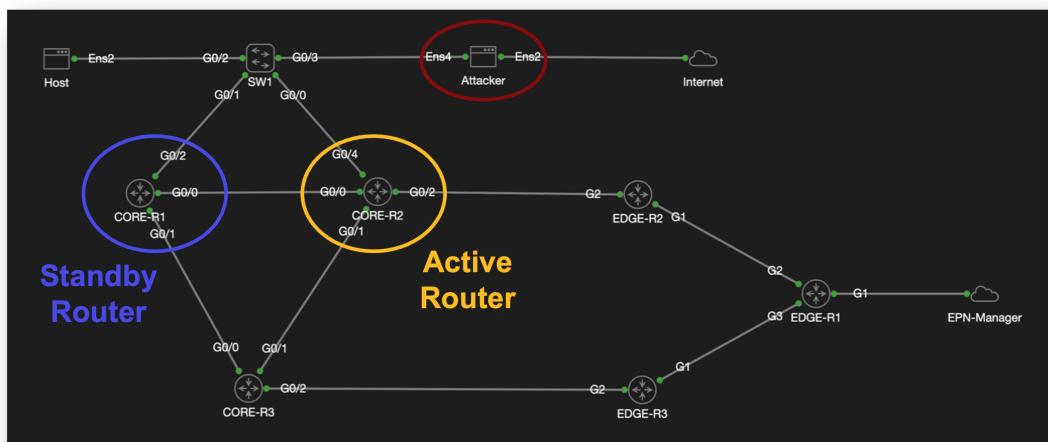


Figura 3.20: Topologia con attaccante HSRP

CAPITOLO 3. DESCRIZIONE DELLA SOLUZIONE

L'attaccante introduce un router falso nella rete, in particolare un dispositivo configurato per partecipare al gruppo HSRP esistente. Questo dispositivo invia pacchetti HSRP con una priorità più alta rispetto ai router legittimi, facendosi eleggere come router attivo. Il risultato è che, in caso di successo, tutti i dispositivi della rete iniziano a instradare il traffico verso il router malevolo, credendo che sia il gateway legittimo. Andando a vedere gli alert generati, di criticità Major, vediamo che i router legittimi passano da stato Active a Init (CORE-R2) e da Standby a Listening (CORE-R1), dunque nessuno dei due è attivo.

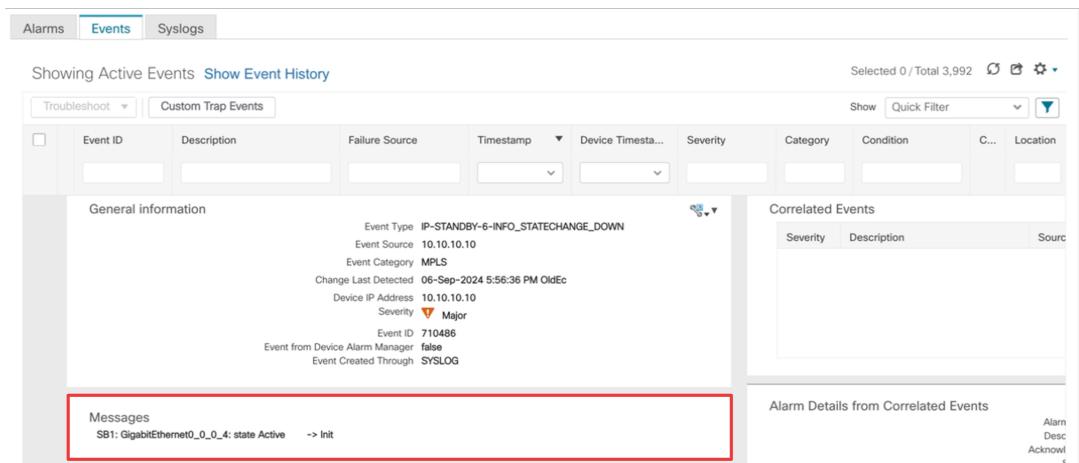


Figura 3.21: HSRP Alert

Capitolo 4

Conclusioni

La soluzione software adottata, cioè EPN Manager, si è rivelata non solo semplice e intuitiva, ma anche molto potente e completa in quanto consente ad un amministratore di rete di poter avere tantissimi aspetti della rete sotto controllo. Suggeriamo dunque fortemente l’adozione di questo tipo di soluzione per la chiarezza della documentazione, la semplicità di utilizzo e la potenza in termini di funzionalità, features che giustificano il costo della licenza del network manager studiato.

Per quanto riguarda gli scenari implementati, i risultati del nostro lavoro sono stati molto interessanti: non solo abbiamo testato alcuni casi d’uso proposti da ASPI, ma ci siamo anche cimentati nella sperimentazione di scenari legati a errori di configurazione, fattori da considerare in quanto ci sono pur sempre degli esseri umani dietro i dispositivi, e attacchi di cybersecurity, eventi di spicco al giorno d’oggi e

soprattutto molto dannoso per infrastrutture grandi e importanti come quella di ASPI. Per quanto riguarda quest'ultimo caso d'uso, è emerso che gli attacchi DoS più semplici sono facili da controllare attraverso le soglie, come i limiti di pacchetti in cache, mentre nel caso di protocolli particolari come HSRP c'è bisogno di prevenire questi eventi in maniera diversa. In conclusione possiamo ritenerci più che soddisfatti nel nostro Project Work.

Capitolo 5

Sviluppi Futuri

Il nostro lavoro è stato realizzato in ambiente simulato; un possibile step futuro può essere dunque il passaggio da uno scenario virtuale ad uno reale, con dispositivi fisici veri e propri all'interno della già esistente infrastruttura di rete. Avendo analizzato le implicazioni di sicurezza in caso di attacchi, preliminarmente si dovrebbe procedere ad implementare un mitigation plan per gli attacchi alla sicurezza, utilizzando per esempio script ad-hoc per determinate tipologie di attacchi che non possono essere controllati tramite soglie e rafforzando l'autenticazione per protocolli come HSRP.

Bibliografia

- [1] Cisco. EPN Manager Documentation. https://www.cisco.com/c/en/us/td/docs/net_mgmt/epn_manager/7_0_0_GA/documentation/overview/bk_cisco_evolved_programmable_network_manager_7_0_documentation_overview.html.