REPORT SULLA PROGETTAZIONE DELLA RETE

Report sulla Progettazione della Rete per l'Azienda Theta

1. Introduzione

Questo report forense descrive la progettazione della rete aziendale simulata per l'azienda **Theta**, situata in una sede operativa su sei piani. La rete è stata progettata tenendo conto della sicurezza, dell'efficienza e della gestione del traffico dati in un ambiente aziendale. L'infrastruttura di rete utilizza vari dispositivi di rete, tra cui switch, router, firewall, server, e sistemi di sicurezza per garantire la protezione dei dati aziendali e l'accesso sicuro alle risorse aziendali da parte dei dipendenti e delle risorse esterne. L'architettura implementata è altamente segmentata e configurata per limitare le comunicazioni tra le diverse aree aziendali e per proteggere la rete da attacchi e intrusioni esterne.
La progettazione tiene conto delle specifiche esigenze operative dei vari piani dell'edificio, che sono suddivise nelle seguenti aree funzionali:

- **Piano 1/A**: Front office
- **Piano 1/B**: Server room
- **Piano 2**: Ufficio vendite / Vendite online
- **Piano 3**: Ufficio acquisti / Consegne
- **Piano 4**: Amministrazione
- **Piano 5**: Dirigenza
- **Piano 6**: Reparto IT

2. Topologia di Rete e Dispositivi Utilizzati

La rete aziendale di Theta è stata progettata con una struttura a **6 piani**, con 20 computer per piano. Ogni piano è dotato di uno switch dedicato per connettere i 20 computer presenti. Inoltre è stata configurata una DMZ contenente i server accessibili dall'esterno.
Di seguito sono descritti i dispositivi principali utilizzati nella progettazione:

- **Switch per piano**: Ogni piano è dotato di uno switch per collegare i computer all'interno di ogni VLAN specifica. Ciò permette di isolare il traffico tra i vari piani e di migliorare la gestione delle risorse di rete.
- **Router centrale**: Il router collega tutti gli switch dei vari piani e gestisce il traffico tra le VLAN. È anche responsabile dell'applicazione delle **Access Control Lists (ACL)** per regolare le comunicazioni tra le VLAN.
- **Firewall perimetrale**: Posizionato tra il router interno e la connessione a Internet, il firewall filtra il traffico in entrata e in uscita, applicando regole di sicurezza specifiche.
- **NAS (Network Attached Storage)**: Un dispositivo NAS è stato collegato al router centrale per garantire l'accesso ai dati aziendali da parte di tutti i computer presenti nella rete interna, utilizzato principalmente per i backup dei file.
- **IDS/IPS (Intrusion Detection/Prevention System)**: Sono stati implementati 3 dispositivi IDS/IPS per monitorare il traffico e prevenire le intrusioni nella rete interna.

- **Web Server e Server SMTP nella DMZ**: Un web server e un server SMTP sono stati posizionati nella zona demilitarizzata (DMZ) per garantire un accesso sicuro alle risorse web dall'esterno.

3. Segmentazione della Rete in VLAN

La rete è stata segmentata in **6 sottoreti** distinte, ognuna corrispondente a un piano dell'edificio e associata a una VLAN. Le sottoreti e le rispettive VLAN sono le seguenti:

- **VLAN 10 - Piano 1**: Sottorete 192.168.10.0/24
- **VLAN 20 - Piano 2**: Sottorete 192.168.20.0/24
- **VLAN 30 - Piano 3**: Sottorete 192.168.30.0/24
- **VLAN 40 - Piano 4**: Sottorete 192.168.40.0/24
- **VLAN 50 - Piano 5**: Sottorete 192.168.50.0/24
- **VLAN 60 - Piano 6**: Sottorete 192.168.60.0/24

La segmentazione della rete in VLAN è stata scelta per diverse ragioni:

1. **Sicurezza**: Ogni piano è isolato tramite VLAN, impedendo che il traffico di rete da un piano possa essere facilmente intercettato o compromesso da altri piani. Ciò limita l'esposizione dei dati aziendali e rende più difficile per un attaccante spostarsi lateralmente nella rete.
2. **Efficienza**: La segmentazione in VLAN riduce il dominio di broadcast, migliorando le prestazioni della rete, grazie alla riduzione del traffico di rete non necessario.
3. **Controllo del traffico**: La divisione in VLAN permette, tramite l'implementazione di ACL, di configurare regole di accesso granulari per consentire o negare specifiche comunicazioni tra le sottoreti. Questo garantisce che solo i flussi di traffico autorizzati possano attraversare i confini tra i vari piani.

4. Configurazione del Router e ACL

Il router centrale gioca un ruolo cruciale nella gestione del traffico tra le diverse VLAN. Le ACL sono state configurate per controllare quali VLAN possano comunicare tra loro, permettendo una gestione capillare del traffico di entrata e di uscita.
Questo ci ha permesso di rispettare l'organizzazione gerarchica della società, impedendo ai piani operativi di comunicare direttamente con i piani dirigenziali.
Di seguito vengono elencate le principali configurazioni ACL applicate:

- **VLAN 10**

  - *In entrata*: dalla VLAN 60
  - *In uscita*: verso le VLAN 20,30,40

  Questa configurazione permette al piano 1 front office di ricevere comunicazioni esclusivamente dal piano 6 (reparto IT) e di inviare informazioni ai piani 2 (ufficio vendite), 3 (ufficio acquisti) e 4 (amministrazione).

- **VLAN 20**

  -*In entrata*: dalle VLAN 10, 30, 60
  - *In uscita*: verso la VLAN 10, 30
  Questa configurazione permette al piano 2 (ufficio vendite / vendite online) di ricevere comunicazioni dai piani 1 (front office), 3 (ufficio acquisti), 6 (reparto IT) e di inviare informazioni ai piani 1 e 3.

- **VLAN 30**

  - *In entrata*: da VLAN 10, 20, 40, 60
  - *In uscita*: verso le VLAN 20,40,60
  Questa configurazione permette al piano 3 (ufficio acquisti) di ricevere comunicazioni dai piani 1 (front office), 2 (ufficio vendite), 4 (amministrazione) e 6 (reparto IT) e di inviare informazioni ai piani 2, 4 e 6.

- **VLAN 40**

  - *In entrata*: da VLAN 20, 30, 50, 60
  - *In uscita*: verso le VLAN 30, 50, 60
  Questa configurazione permette al piano 4 (amministrazione) di ricevere comunicazioni dai piani 2 (ufficio vendite), 3 (ufficio acquisti), 5 (dirigenza) e 6 (reparto IT) e di inviare informazioni ai piani 3, 5 e 6.
  Il piano amministrazione svolge quindi la funzione di tramite tra i piani dirigenziali e quelli operativi e viceversa.

- **VLAN 50**

  - *In entrata*: da VLAN 40 e 60
  - *In uscita*: verso la VLAN 40
  Questa configurazione permette al piano 5 (dirigenza) di ricevere comunicazioni dai piani 4 (amministrazione) e 6 (reparto IT) e di inviare informazioni al piano 4.

- **VLAN 60**

  - *In entrata*: dalle VLAN 30, 40
  - *In uscita*: verso tutte le VLAN
  Questa configurazione permette al piano 6 (reparto IT) di ricevere comunicazioni dai piani 3 (ufficio acquisti) e 4 (amministrazione) e di inviare informazioni a tutti i piani. Questo permette al reparto IT di effettuare manutenzione su tutti i dispositivi e di ricevere informazioni dai due snodi principali della rete (piani 3 e 4). Questo perché nel reparto IT troviamo un database aziendale a cui vengono inviate informazioni da archiviare.

5. NAS e Accesso ai Dati Aziendali

Un **NAS (Network Attached Storage)** è stato collegato al router centrale della rete interna per fornire un accesso centralizzato ai file aziendali. Il NAS è utilizzato per il backup dei dati e

per la condivisione tra i vari reparti. In questo modo, l'accesso al NAS è consentito solo ai computer appartenenti alla rete interna, affinché i dati siano protetti da accessi non autorizzati.

6. Sicurezza Perimetrale e Gestione del Traffico

Il **firewall perimetrale** è stato configurato per proteggere la rete interna di Theta da minacce esterne.
Si è deciso di disporre il dispositivo tra le tre interfacce principali di nostro interesse:

- **Rete interna**
- **DMZ**
- **Rete esterna (internet)**

Questo ci ha permesso di filtrare il traffico in tutte le direzioni, tramite le seguenti regole:

- **Accesso alla DMZ**: Il firewall consente solo il traffico in ingresso sulle porte 80 (HTTP), 443 (HTTPS) e 25 (SMTP) diretto verso il web server e il server SMTP presenti nella DMZ. Questo permette l'accesso sicuro ai servizi web e di posta elettronica aziendali da parte di utenti esterni.
- **Accesso alla rete interna**: Nessun traffico diretto è consentito dall'esterno alla rete interna. Tuttavia, le risposte a richieste legittime generate dall'interno (ad esempio, quando un computer interno accede a un sito web) sono permesse.
- **Filtraggio da DMZ a rete interna**: Le comunicazioni sulla porta 23 (Telnet) tra la DMZ e la rete interna sono bloccate per evitare potenziali attacchi sfruttando questo protocollo non sicuro.

7. Server nella DMZ

La **zona demilitarizzata (DMZ)** è stata collegata, tramite uno switch, al firewall che permette la connessione a Internet. Al suo interno, sono presenti i servizi pubblici dell'azienda, come il web server e il server SMTP. Questi server sono accessibili dall'esterno per garantire la disponibilità dei servizi aziendali, ma sono protetti dal firewall e configurati in modo da limitare l'accesso alle sole porte necessarie (80, 443, 25).

8. Implementazione dell'IDS/IPS

Informazioni di base dei dispositivi utilizzati:

IDS

Un dispositivo IDS (Intrusion Detection System) è una tecnologia di sicurezza informatica progettata per monitorare e analizzare il traffico di rete o le attività di sistema al fine di rilevare comportamenti sospetti o potenzialmente dannosi. L'IDS può identificare tentativi di intrusione, malware, attacchi informatici o altre violazioni della sicurezza: quando un'eventuale minaccia viene rilevata, l'IDS invia un allarme per avvisare gli amministratori di sistema.

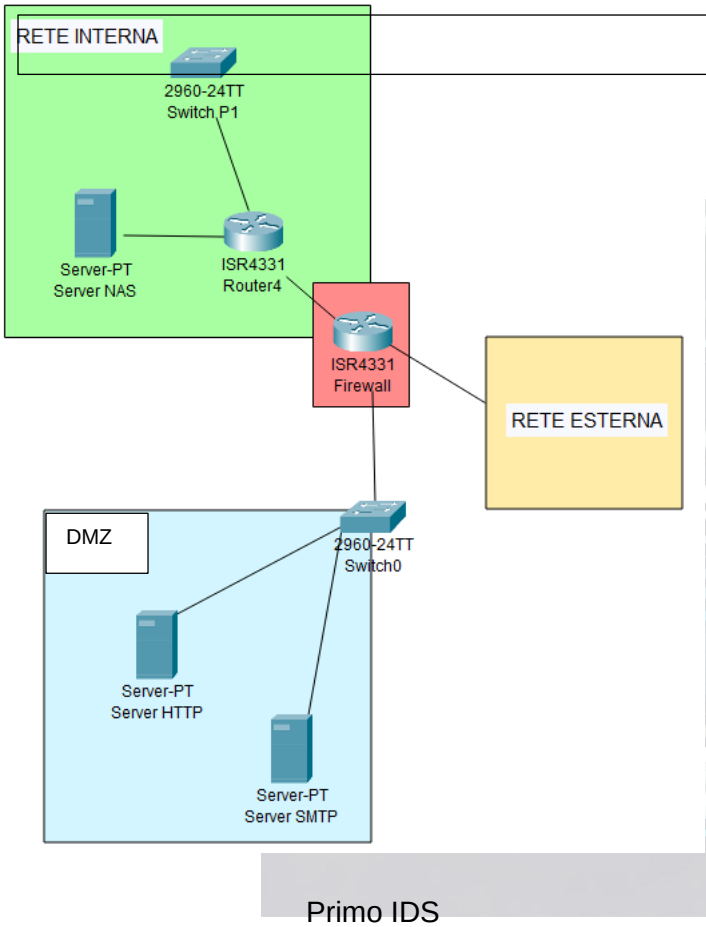
IPS

Un dispositivo IPS (Intrusion Prevention System) è una tecnologia di sicurezza informatica avanzata che non solo rileva le intrusioni o attività sospette, ma è anche in grado di bloccarle

o prevenirle in tempo reale. Gli IPS sono utilizzati per monitorare il traffico di rete e il comportamento dei sistemi, applicando una serie di regole predefinite per identificare modelli di attacco noti, come exploit, malware o scansioni di vulnerabilità. In caso di rilevamento, un IPS può eseguire azioni preventive, come il blocco del traffico sospetto, il filtraggio delle richieste dannose o l'interruzione delle connessioni compromesse.

Posizionamento dei software e dei sensori nella rete Theta

Andremo ora ad analizzare la rete solo nelle sezioni interessate al posizionamento dell'IPS e dei due IDS e i loro sensori.



IPS

multilivello. Questa

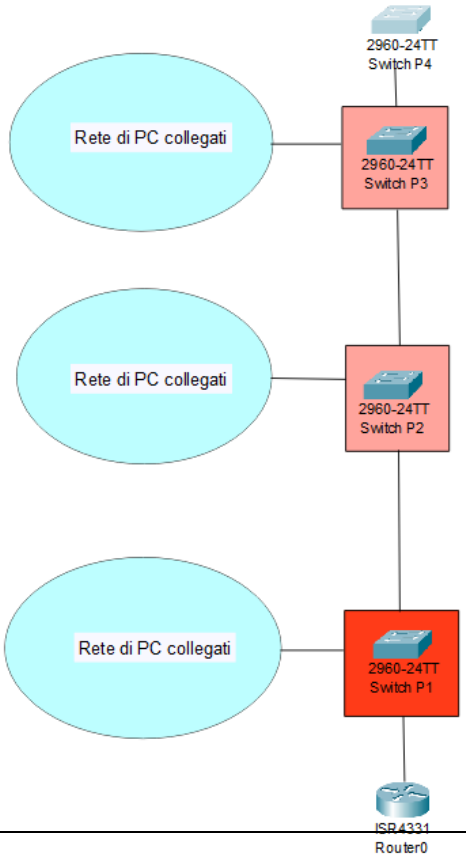
L'IPS è integrato nel firewall CISCO SYSTEMS Cisco ASA 5508-X ed è posizionato strategicamente per gestire il traffico tra la rete interna, la DMZ (Demilitarized Zone) e le reti esterne, garantendo protezione configurazione protegge la rete aziendale dagli attacchi, monitora il traffico tra zone diverse e garantisce che i servizi pubblici nella DMZ non compromettano la rete interna.

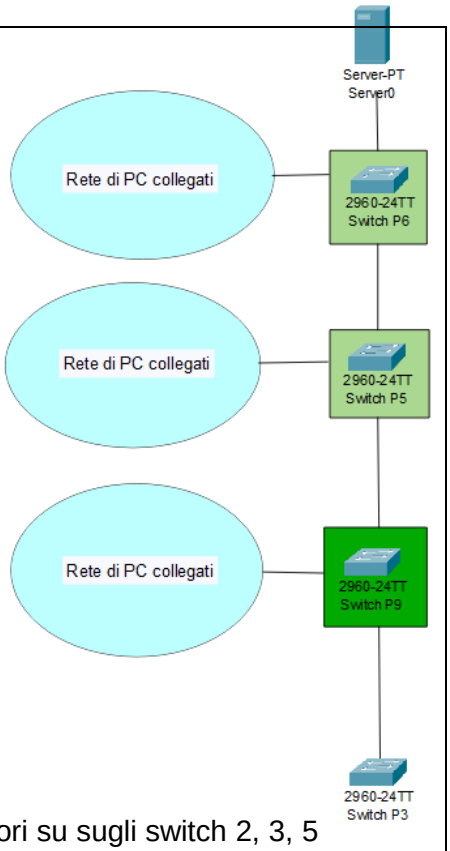
Primo IDS

Lo switch 1 è stato scelto come nodo centrale per l'installazione del software IDS, in quanto funge da punto di accesso primario per il traffico di rete che passa tra i vari switch e dispositivi connessi.

L'IDS su Switch 1 sarà configurato per monitorare l'intero traffico di rete che transita in questa parte della rete, permettendo una visione completa delle comunicazioni. Gli switch 2 e Switch 3 sono stati equipaggiati con sensori IDS che lavorano in sinergia con il software IDS installato su Switch 1.

Questi sensori sono distribuiti nella rete per monitorare i dati a livello di segmento e supportare l'IDS nel rilevamento di attacchi localizzati o nel traffico di rete.





Secondo IDS

Lo Switch 4 è stato scelto, visto il collegamento diretto con lo switch 3, come nuovo nodo per l'installazione di un ulteriore software IDS, in quanto funge da unico punto di accesso per il traffico di rete che deve raggiungere gli switch 5, 6 e il server.
L'IDS su switch 4, come per lo switch 1, sarà configurato per monitorare l'intero traffico di rete che transita nella parte di rete di sua competenza, permettendo una visione completa delle comunicazioni. Gli switch 5 e 6 sono stati equipaggiati con sensori IDS che lavorano in sinergia con il software IDS installato su switch 4. Questi sensori sono distribuiti nella rete per monitorare i dati a livello di segmento e supportare l'IDS nel rilevamento di attacchi localizzati o nel traffico di rete.

Motivazione delle scelte

IDS. L'installazione del software IDS sugli switch 1 e 4 e dei sensori su sugli switch 2, 3, 5 e 6, porterà a una visione integrata e distribuita della rete interna interpiano, aumentando la capacità di rilevamento e risposta agli attacchi.
È stato valutato di optare per software IDS per la rete inter-piano per non rallentare la banda interna. Sistemi attivi come gli IPS potrebbero creare log di falsi positivi eccessivi e le azioni di blocco dei dati potrebbero compromettere la funzionalità della rete interna.

IPS. La presenza di un software di protezione attiva nel nodo di collegamento ad internet servirà fondamentale nel bloccare possibili minacce in entrata e in uscita dalla rete aziendale. L' IPS integrato nel firewall ha il vantaggio di avere un'unica soluzione hardware e ridurre la complessità di gestione.

Hardware utilizzati

CISCO C9200-24P-E. Questo switch ha la funzione port mirroring o SPAN (Switched Port Analyzer), la quale è una funzionalità avanzata degli switch di rete. Consente di duplicare il traffico che transita su una o più porte dello switch verso una porta dedicata per il monitoraggio e l'analisi. Questa tecnica è particolarmente utile per attività di troubleshooting, analisi del traffico, rilevamento delle intrusioni (con strumenti come IDS/IPS), e monitoraggio delle prestazioni della rete. Il traffico copiato può essere analizzato in tempo reale tramite strumenti di sniffing o inviato a dispositivi di sicurezza.
CISCO SYSTEMS Cisco ASA 5508-X. Questo firewall di nuova generazione (NGFW - Next-Generation Firewall) è progettato per offrire sicurezza avanzata alle reti aziendali. Integra funzionalità di firewall tradizionale con strumenti avanzati per la protezione contro minacce informatiche moderne come funzioni IPS.

Software compatibili

Il progetto prevede l'implementazione di un sistema di sicurezza avanzato basato su software open source per garantire il monitoraggio, la prevenzione, l'analisi e il blocco delle minacce nella rete aziendale. L'infrastruttura si avvale di Suricata come motore di prevenzione delle intrusioni (IPS), Zeek per il rilevamento delle intrusioni (IDS), e un sistema di gestione centralizzato SIEM open source per la correlazione e l'analisi degli eventi di sicurezza.

Andremo a vedere ora cosa sono e il loro funzionamento, su quali dispositivi verranno installati e come saranno gestiti in maniera centralizzata.

Software per l'IPS

SURICATA Suricata è un motore open source avanzato per il rilevamento e la prevenzione delle intrusioni che fornisce una protezione in tempo reale contro minacce e attacchi informatici. Suricata analizza e monitora il traffico di rete, utilizzando regole basate su firme per rilevare attacchi come DDoS, exploit, malware, tentativi di intrusione e altre attività sospette. È in grado di ispezionare diversi protocolli di rete, tra cui HTTP, DNS, FTP, TLS e SMB, garantendo una protezione completa e una visibilità approfondita delle comunicazioni di rete. Grazie al suo supporto per il multi-threading, è in grado di gestire elevati volumi di traffico senza compromettere le prestazioni. Oltre al rilevamento delle intrusioni, genera log dettagliati e report su eventi di sicurezza, con la possibilità di esportare i dati per analisi approfondite o integrazione con sistemi SIEM.

Software per gli IDS

Zeek Zeek è un potente framework open source per il monitoraggio e l'analisi del traffico di rete. A differenza di altri sistemi IDS/IPS, Zeek offre una visibilità dettagliata su tutta la rete, consentendo di rilevare minacce e anomalie non solo tramite il rilevamento di attacchi ma anche monitorando il comportamento generale del traffico. La sua capacità di scripting avanzata consente agli utenti di creare regole personalizzate per identificare comportamenti sospetti e automatizzare risposte. Zeek genera log dettagliati che possono essere utilizzati per analisi forensi, investigazioni e reporting. È frequentemente integrato con altri strumenti di sicurezza come SIEM per migliorare la visibilità e la gestione degli eventi.

Gestione centralizzata

SIEM SIEM (Security Information and Event Management) è una soluzione avanzata per la raccolta, l'aggregazione, l'analisi e la gestione degli eventi di sicurezza. Raccoglie i log provenienti da vari dispositivi di rete, server e applicazioni per monitorare in tempo reale attività sospette e minacce, applicando tecniche di correlazione per identificare attacchi o anomalie. Un SIEM fornisce anche strumenti per l'analisi forense e la reportistica, essenziali per investigazioni e conformità alle normative di sicurezza.

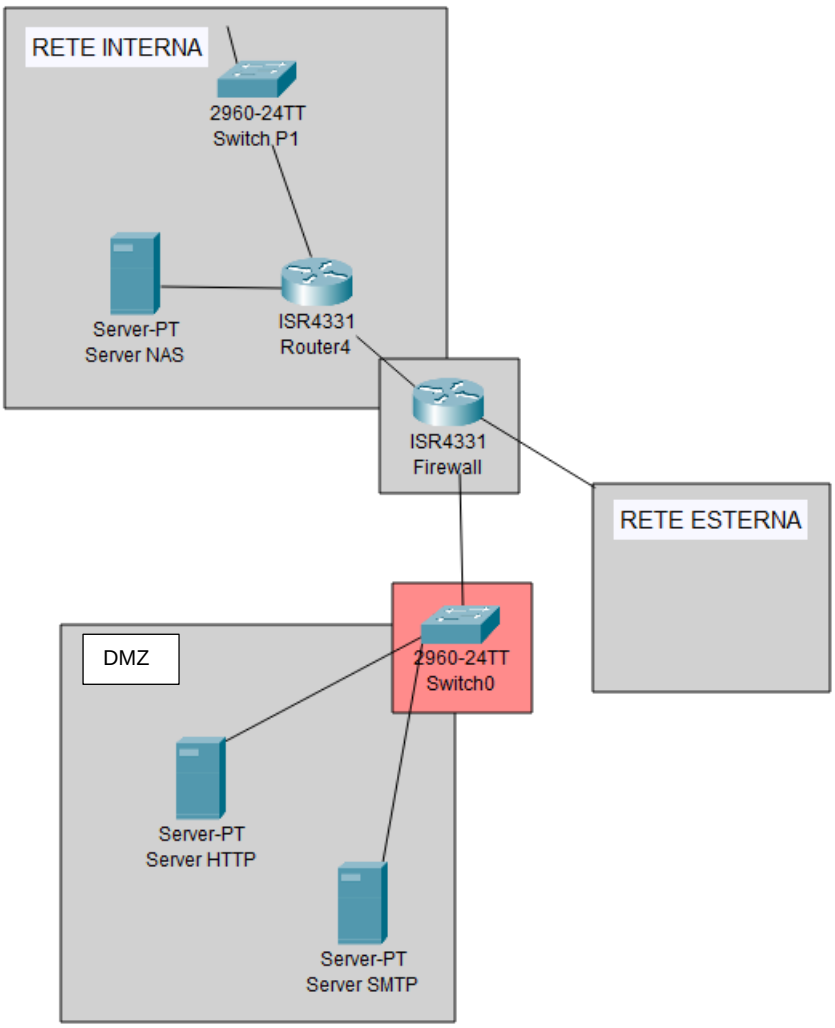
Conclusione e considerazioni sull'interazione dei software *Surricata, Zeek e SIEM*

L'integrazione con strumenti come Zeek e Suricata potenzia ulteriormente la capacità del SIEM di rilevare e rispondere alle minacce. Zeek, con la sua capacità di monitorare e analizzare il traffico di rete in profondità, fornisce al SIEM dettagli sui flussi di rete e sulle anomalie. Suricata, con le sue capacità IPS, invia dati sul traffico di rete sospetto e sugli attacchi prevenuti. Entrambi generano log dettagliati che vengono centralizzati dal SIEM per una visibilità completa e un'efficace gestione delle minacce in tempo reale.

Possibili implementazioni

Reverse Poxy L'installazione di un reverso proxy tra la DMZ e il firewall è una soluzione molto vantaggiosa per migliorare la sicurezza e la gestione del traffico nella rete

aziendale. Un reverse proxy agisce come un intermediario tra i client esterni e i server interni, ricevendo le richieste in ingresso e instradandole verso i server giusti.



Posizionando il reverse proxy nello switch 0 consentirà di proteggere i server interni alla DMZ, riducendo il rischio che attacchi diretti possano compromettere i sistemi aziendali o accedere a dati sensibili dell'azienda stessa.

9. Conclusioni

La progettazione della rete aziendale per l'azienda Theta è stata realizzata tenendo conto dei principi di sicurezza, efficienza e gestione del traffico. La segmentazione della rete in VLAN, insieme alla protezione tramite firewall, IDS/IPS e altre misure di sicurezza, garantisce che la rete aziendale sia robusta e protetta contro minacce interne ed esterne. La configurazione delle ACL e il monitoraggio costante del traffico garantiscono un controllo preciso sulle comunicazioni tra le diverse aree aziendali.