DOCUMENTAZIONE DESIGN DI RETE

Per il design di rete si è optato per la tecnica della segmentazione che divide una rete locale in parti più piccole allo scopo di migliorarne prestazioni e sicurezza. E' un'operazione che consiste nel delimitare il traffico dati entro specifici segmenti, noti come subnet che agiscono come unità semi-autonome.

La segmentazione di rete rappresenta uno strumento essenziale per la protezione dei network aziendali. Consente, infatti, di rafforzare i controlli di sicurezza concentrandoli sulle singole sottoreti e limitare il **movimento laterale** di eventuali hacker e intrusi.

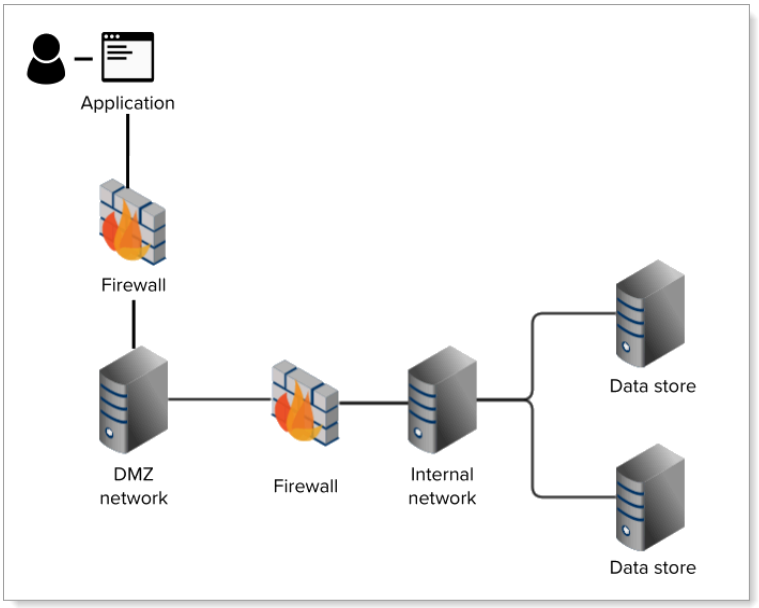
Delimitando i confini di monitoraggio dall'intero network ai singoli segmenti, risulta più semplice analizzare dati ed evidenziare eventuali anomalie, infatti, utilizzando questa tecnica è possibile: **efficientare il monitoraggio - aumentare le prestazioni - localizzare problemi tecnici**.

Oltre all'innegabile innalzamento dei livelli generali di sicurezza, la segmentazione di rete offre diversi altri vantaggi:

- Controllo e limitazione dei danni in caso di incidente dovuto alla minor superficie di attacco su cui un hacker potrebbe agire
- Controllo degli accessi più efficiente e sottoposto a costante monitoraggio
- Miglioramento delle prestazioni con meno congestione sul traffico di rete
- Rafforzamento della protezione di server, risorse e dispositivi endpoint

Per questo si è divisa la rete in:

INTERNET	DMZ	RETE INTERNA



Le minacce Cyber arrivano soprattutto da internet. Motivo per il quale, è necessario che l'azienda adoperi una struttura di rete come quella della multi-tier DMZ, nel quale oltre ad esserci la divisione in zone di rete in base alla criticità degli asset sui segmenti di rete, si aggiungono più livelli di sicurezza (che possono essere firewall, proxy, o altri device e strumenti che offrono servizi di sicurezza).

Detto ciò, si è applicato un ***firewall perimetrale***, utile per definire la sicurezza della rete e per controllare il traffico in entrata e in uscita

Mentre il secondo firewall è stato messo a protezione della rete interna negando ogni accesso.

In questo modo possiamo monitorare le informazioni filtrandole nel caso le ritenga non affidabili e bloccandole se necessario. Tipicamente un firewall definisce ciò che può entrare o uscire dal sistema, utilizzando dei criteri.

In particolare, i criteri maggiormente utilizzati sono:

Default-deny	**Default-allow**
si definisce a priori una impostazione che diventa predefinita, secondo la quale viene definito a monte tutto quel che può essere autorizzato ad entrare nel sistema. Per conseguenza, tutto ciò che è diverso viene bloccato.	come si può ben immaginare, questo criterio funziona esattamente all'opposto. Si definiscono a priori le limitazioni ovvero tutto quel che non può entrare o uscire dal sistema, mentre di default tutto il resto è legittimato al transito.

Tra i due, il primo criterio è quello più diffuso, in grado di garantire un maggior grado di sicurezza alla struttura informatica.

In primo luogo, uno dei limiti dei firewall sono proprio le loro stesse impostazioni.
Queste tecnologie vengono configurate seguendo determinati parametri e regole che se risultano troppo permissive, possono presentare delle falle ed esporre il sistema informatico al pericolo di essere attaccato.

Di contro l'effettiva usabilità della rete deve essere un compromesso con l'attività di manutenzione e configurazione della stessa.

Nel nostro caso andremo anche a disabilitare tutti i protocolli verso la rete interna lasciando attivi solo http/https verso la rete DMZ. in più verrà creata una black list con all'interno una lista di ip malevoli e richieste Http (con log injection) già conosciute in rete, quest'ultima verrà poi tenuta costantemente aggiornata grazie al monitoring dell'analista aiutato anche dallo strumento SOAR (che spiegheremo in seguito)

Per il design della rete riteniamo quindi utile applicare il firewall FortiGate 100F dell'azienda statunitense Fortinet

Caratteristiche tecniche:

- Identifica migliaia di applicazioni all'interno del traffico di rete grazie ad un'ispezione approfondita e profonda
- Protegge da malware, exploit e siti Web dannosi in traffico crittografato e non crittografato
- Previene e rileva da attacchi noti e sconosciuti
- Traffico crittografato
- Funzionalità di rete avanzate, ad alte prestazioni e capacità VPN IPsec scalabili per consolidare la rete
- Console centralizzata con interfaccia grafica, semplice da utilizzare
- Monitoraggio in tempo reale delle sonde IPS/IDS

In questo modello di firewall è previsto anche il **WAF (web application firewall)** che consente di proteggere le applicazioni Web da attacchi dannosi e traffico Internet indesiderato, inclusi bot, injection e denial of service (DoS) a livello di applicazione.

Inoltre, consigliamo l'attivazione del reverse proxy che è un server che si trova tra i client e un gruppo di server backend, inoltrando le richieste dei client ai server appropriati e rispondendo ai client per conto di quei server. Questo tipo di configurazione offre numerosi vantaggi in termini di sicurezza, prestazioni e gestione del traffico.

Per migliorare ancora di più la vostra sicurezza di rete consigliamo l'implementazione di sistemi di gestione centralizzata e strumenti di monitoraggio, come:

SIEM e **SOAR** e abbiamo optato per un **"Splunk Enterprise"** prodotto da CISCO.

SIEM (Security information and event management) in italiano, gestione delle informazioni e di eventi di sicurezza, è un sistema che permette di archiviare, processare e correlare gli eventi dei Log.

I componenti di un SIEM sono:

- **la raccolta dei dati**: un insieme di dati raccolti da tutti i componenti dell'infrastruttura ovvero, router, server, applicazione, sistemi operativi e firewall.
- **Categorizzazione**: i dati vengono catalogati in un formato comune per facilitare l'analisi.
- **Correlazione**: il sistema analizza i dati per identificare i pattern che potrebbero indicare attività sospette o attacchi.
- **Monitoraggio costante di anomalie**: quando viene rilevata un'anomalia, il SIEM genera un allarme per avvisare il team di sicurezza che, assegnano priorità agli avvisi, identificano le minacce e avviano la risposta o la correzione.
- **Report e Analisi**: il SIEM fornisce un report dettagliato per aiutare a comprendere meglio gli incidenti di sicurezza e migliorare le strategie di difesa.

Le soluzioni SIEM offrono alle aziende ***numerosi vantaggi*** e rappresentano un componente significativo nella razionalizzazione dei flussi di lavoro relativi alla sicurezza:

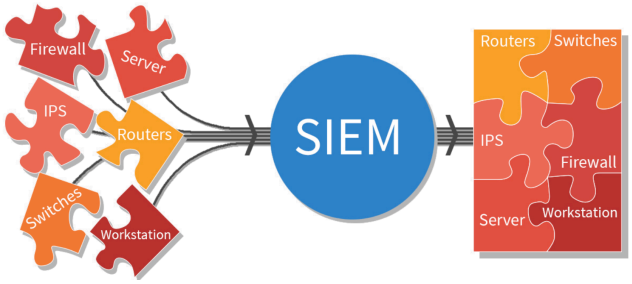
- **Riconoscimento delle minacce in tempo reale** : Verifiche e reporting di conformita centralizzato per l'intera infrastruttura aziendale.

- **Automazione basata sull'AI** : L'automazione avanzata facilita la raccolta e l'analisi dei log di sistema e degli eventi di sicurezza per ridurre l'utilizzo delle risorse interne e, al contempo, soddisfare i rigorosi standard relativi al reporting di conformità.

- **Migliorare efficienza organizzativa** : Una dashboard centrale fornisce una visione unificata dei dati, degli avvisi e delle notifiche di sistema, consentendo ai team di comunicare e collaborare in modo efficiente quando rispondono a minacce e incidenti di sicurezza.

- **Rilevamento di minacce avanzate e sconosciute** : Data la velocità con cui cambia il landscape della cybersecurity, le organizzazioni devono poter contare su soluzioni in grado di rilevare e rispondere sia alle minacce alla sicurezza note che a quelle sconosciute.

Le soluzioni SIEM possono aiutare i team di sicurezza a rispondere in modo più efficace a una vasta gamma di attacchi informatici, tra cui: minacce interne, phishing, ransomware, attacchi DDoS, furto di dati e tracciare le attività di rete di tutti gli utenti, i dispositivi e le applicazioni, migliorando notevolmente la trasparenza dell'intera infrastruttura e rilevando le minacce indipendentemente da dove si accede agli asset e ai servizi digitali.



SOAR (Security Orchestration, Automation and Response), in italiano, l'orchestrazione, l'automazione e la risposta alla sicurezza, è una soluzione software che consente ai team di integrare e coordinare strumenti di sicurezza separati, automatizzare le attività ripetitive e semplificare i workflow di risposta agli incidenti e alle minacce.

Semplificando il triage degli avvisi e assicurando che i diversi strumenti di sicurezza lavorino insieme, le SOAR aiutano i SOC (Security Operations Centers) a ridurre il tempo medio di rilevamento (MTTD) e il tempo medio di risposta (MTTR), migliorando il livello complessivo della sicurezza. Rilevare e rispondere più rapidamente alle minacce per la sicurezza può attenuare l'impatto degli attacchi informatici e far risparmiare alle aziende sui costi.

Per **"Orchestrazione della sicurezza"** si intende il modo in cui le piattaforme SOAR si connettono e coordinano l'hardware e gli strumenti software nel sistema di sicurezza di un'azienda.

Le soluzioni di sicurezza SOAR possono automatizzare le attività ripetitive e di basso livello, come l'apertura e la chiusura dei ticket di assistenza, l'arricchimento di eventi e la priorità degli avvisi. I SOAR possono anche attivare le azioni automatizzate degli strumenti di sicurezza integrati. Ciò significa che gli analisti della sicurezza possono utilizzare i workflow del playbook per concatenare più strumenti ed eseguire l'**automazione delle operazioni** di sicurezza più complesse.

Le funzionalità di orchestrazione e automazione di SOAR gli consentono di fungere da console centrale per la **risposta agli incidenti di sicurezza** (IR). Il report di Cost of a Data Breach di IBM ha rilevato che le organizzazioni con un team IR e un piano IR testing hanno identificato le violazioni 54 giorni prima rispetto a quelle che non dispongono di nessuno dei due elementi.

La tecnologia SIEM è emersa per la prima volta come strumento di reporting della conformità. I SOC hanno adottato i SIEM quando si sono resi conto che tali dati potevano fornire informazioni cruciali per le operazioni di cybersecurity. Le soluzioni SOAR sono nate per implementare le funzionalità incentrate sulla sicurezza che mancano alla maggior parte dei SIEM standard, come l'orchestrazione, l'automazione e le funzioni della console.

Pertanto l'implementazione di entrambi gli strumenti porterebbe un grande vantaggio all'azienda in termini di sicurezza e risposta agli incidenti in quanto, possono creare una soluzione di sicurezza più completa e reattiva.

SIEM	SOAR
Raccolta, analisi e monitoraggio dei log e degli eventi di sicurezza in tempo reale.	Automazione e orchestrazione delle operazioni di sicurezza, inclusa la gestione degli incidenti e la risposta alle minacce
Correlazione degli eventi, rilevamento delle minacce, gestione degli incidenti e conformità	Automazione delle risposte agli incidenti, orchestrazione tra diversi strumenti di sicurezza, gestione dei casi

SIEM e SOAR, per aiutarti a comprendere l'importanza di rafforzare le SecOps della tua organizzazione. SecOps è una collaborazione tra i team della sicurezza (Sec) e delle operazioni (Ops) di un'organizzazione. L'obiettivo di SecOps è migliorare la resilienza di un'organizzazione contro le minacce informatiche, eliminando i silos e prevenendo e rispondendo in modo più efficiente ai potenziali attacchi.

Oltre all'applicazione di questi strumenti è necessario assicurarsi che i server e tutte le applicazioni siano aggiornati con le ultime patch di sicurezza quindi è altamente consigliato consultare il sito NIST (National Institute of Standards and Technology)

In aggiunta verrà implementato il **POLP**. (Proponiamo il software della STRONG DM)
Il principio del privilegio minimo (POLP) è uno dei principi fondamentali nella protezione degli ambienti IT.

Vantaggi del privilegio minimo

Maggiore sicurezza: Limitare le autorizzazioni di ciascun utente solo a ciò che è strettamente necessario, riduce la superficie di attacco dei sistemi critici. In particolare, POLP riduce il rischio di utilizzo sia involontario che dannoso di dati e applicazioni, indipendentemente dal fatto che tali azioni provengano dagli utenti stessi o da aggressori esterni che ne hanno compromesso le credenziali.

Ad esempio, POLP riduce il rischio di infezione da ransomware, poiché la maggior parte degli account utente non avrà i privilegi amministrativi necessari per installare il malware. E anche se viene eseguito, sarà in grado di crittografare solo i dati a cui ha accesso l'account utente, quindi lo strumento POLP riduce il danno che può essere inflitto.

Ma nei peggiori dei casi vi sono solidi piani di risposta e ripristino agli incidenti.

Ancora, riteniamo necessario prevedere un corso di *formazione del personale non tecnico* per rendere la loro esperienza nella rete più consapevole e sicura.

Iniziando con sondaggi e questionari per capire il livello delle competenze dei dipendenti e fissare dei meeting online o in azienda per introdurre concetti di base sulle minacce comuni (phishing, malware, ransomware) e far capire l'importanza di utilizzare credenziali (password) forti e uniche.
Ma anche incentivare il *personale IT* a ottenere certificazioni riconosciute e fare corsi di aggiornamento per rimanere sempre al passo con le nuove tecnologie e minacce.

Un altro strumento che consigliamo di implementare è quello atto al backup e ai piani di ripristino, fondamentali per garantire la continuità operativa e la protezione dei dati aziendali in caso di guasti, attacchi informatici, disastri naturali o altri eventi imprevisti.
Il modello che consigliamo è **Acronis Cyber Backup Advanced for Server.**

Caratteristiche

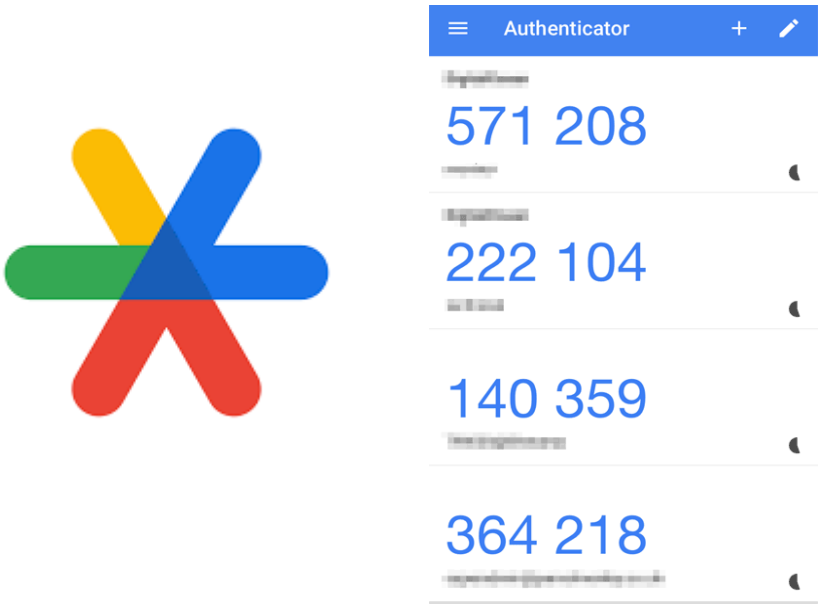
- **Backup Completo:** Protegge server fisici, virtuali, endpoint e dati cloud.
- **Cyber Protection:** Include funzionalità di protezione contro ransomware**.**
- **Ripristino Rapido:** Ripristino rapido dei dati e delle applicazioni critiche.
- **Gestione Centralizzata:** Console di gestione centralizzata per la gestione dei backup.

PRO	CONTRO
Protezione integrata contro ransomware	Prezzi variabili a seconda delle funzionalità richieste
Facilità d'uso e di implementazione	Potrebbe avere funzionalità avanzate limitate rispetto ad altri strumenti
Ottimo supporto per ambienti ibridi	

Molto importante è anche l'*Autenticazione a due fattori (2FA)* che rappresenta un'ulteriore sicurezza per la protezione delle password, è indispensabile prevedere oltre alla password un altro fattore di autenticazione e consigliamo di utilizzare dei soft token che generano un OTP (one time password), codice a 6 cifre, associato ad uno specifico account.
In particolare potrete scegliere di optare per **Google authenticator**, selezionando l'account di interesse permette di creare un codice temporaneo che si potrà utilizzare per l'autenticazione (di solito valido per 30s). Può essere utilizzato anche in modalità offline, configurare più account nell'app, compatibile sia per android che iOS ed è gratuito.

Vantaggi di Google Authenticator

- **Sicurezza Migliorata**: Aggiunge un ulteriore livello di protezione ai tuoi account, riducendo il rischio di accessi non autorizzati.
- **Facilità d'Uso**: L'app è intuitiva e semplice da usare, con un'interfaccia user-friendly.
- **Compatibilità**: Supporta una vasta gamma di servizi online, non solo quelli di Google.



Conclusione

Implementare queste misure di sicurezza aiuterà a proteggere sia il web server esposto pubblicamente che il server applicativo accessibile solo internamente. Questo approccio multilivello garantisce che la sicurezza sia integrata in tutti gli aspetti dell'infrastruttura, riducendo i rischi e migliorando la resilienza contro le minacce.