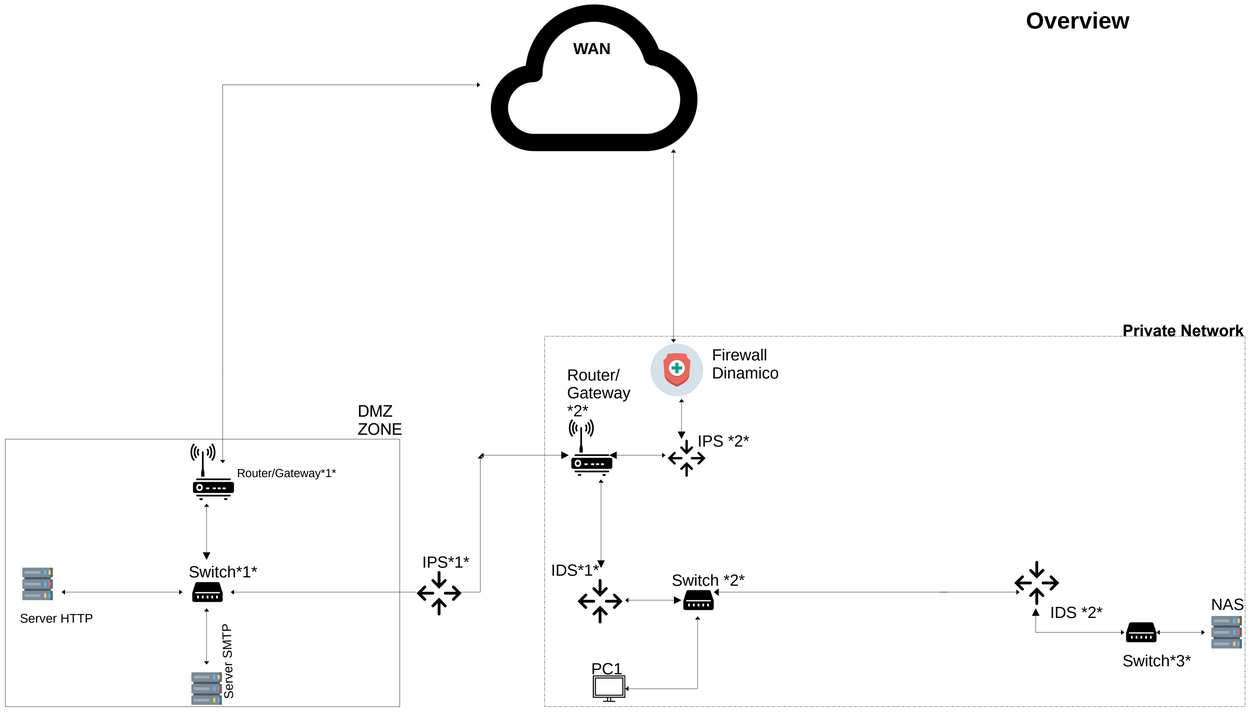
S3L5

Traccia per il progetto: Segmentazione di rete Disegnare una rete con i seguenti componenti:

- Una zona di Internet (rappresentata da un cloud o un simbolo di Internet).
- Una zona DMZ con almeno un server web HTTP e un server di posta elettronica SMTP.
- Una rete interna con almeno un server o nas.
- Un firewall perimetrale posizionato tra le tre zone
- Spiegare le scelte.
- Improving

Overview



WAN (Wide Access Network): Rappresenta la connessione verso la rete esterna.

Firewall Dinamico: Regola il traffico tra la rete esterna (WAN) e quella interna. Permettendo o impedendo (block/reject/pass) l'accesso in base a specifiche regole di sicurezza. Si trova in posizione centrale per garantire la protezione della rete interna.

DMZ: Indica un'area semi-sicura che ospita server esposti al pubblico, come quelli dedicati alla gestione di HTTP e SMTP. È collocata tra la WAN e la rete interna per limitare l'accesso diretto ai server critici.

Router/Gateway DMZ: Collega la rete DMZ alla WAN e indirizza il traffico verso il firewall e la rete interna. Gestisce il traffico in entrata e in uscita dai server esposti.

Server HTTP e Server SMTP: Si tratta di server che offrono servizi pubblici, come la navigazione web (HTTP) e la posta elettronica (SMTP). Sono ubicati nella DMZ per garantire la protezione della rete interna in caso di attacco a questi servizi.

IPS (Sistema di Prevenzione delle Intrusioni): Questo sistema filtra e previene gli attacchi bloccando il traffico dannoso. È posizionato tra la DMZ e la rete interna per difendere dalle minacce esterne.

Router/Gateway Privato: Si occupa dell'instradamento del traffico tra la rete interna e il firewall. Garantisce una comunicazione controllata tra la rete privata e la DMZ/WAN.

Switch: Collega i vari dispositivi all'interno della rete interna, come PC e NAS.

IDS (Sistema di Rilevamento delle Intrusioni): Questo sistema monitora il traffico della rete privata per identificare eventuali anomalie. È locato nella rete interna e davanti ai dispositivi critici, come PC e NAS, per segnalare possibili intrusioni.

PC1: Rappresenta un dispositivo utente interno collegato alla rete privata. È protetto tramite un IDS e uno switch.

NAS (Archiviazione Collegata alla Rete): È un dispositivo di archiviazione di rete, utilizzato per il backup e la gestione dei dati. Si trova nella rete interna per mantenere i dati protetti e accessibili solamente ai dispositivi autorizzati.

Il firewall dinamico è stato posizionato tra la WAN e la rete interna per filtrare tutto il traffico esterno prima che entri nel sistema. Questo permette di bloccare attacchi o accessi non autorizzati prima che possano raggiungere la DMZ o la rete privata, agendo come prima linea di difesa contro minacce esterne. Tuttavia, il traffico all'interno della DMZ non è bloccato dal firewall, ma viene controllato solo quando tenta di accedere alla rete interna. Nel caso che il server DMZ viene compromesso L'IPS Potrebbe non bastare e un firewall (waf) Può essere una proteziona aggiunta contro le minaccie più soffisticate.

La DMZ (Demilitarized Zone) è una rete intermedia tra la WAN (Internet) e la rete interna, progettata per ospitare server pubblici come web e email. Questi server sono isolati dalla rete interna per limitare i rischi in caso di attacchi. Situata tra la rete esterna e il firewall, la DMZ protegge l'infrastruttura principale, riducendo il rischio di compromissione della rete privata.

In Depth:

Il Router*1* nella DMZ Serve per comunicare con la WAN.

Lo Switch*1* nella DMZ è stato posizionato per collegare i server HTTP e SMTP tra loro, consentendo la comunicazione all'interno della DMZ. Gestisce il traffico locale, assicurando che ogni server riceva il traffico (adeguato).

L'IPS*1* (Intrusion Prevention System) è stato posizionato tra la DMZ e il firewall per monitorare e bloccare attacchi malevoli provenienti dalla WAN verso i server pubblici. Serve a prevenire intrusioni e anomalie nel traffico prima che raggiungano la rete interna. Protegge la DMZ e la rete privata, rafforzando la sicurezza complessiva del sistema.

Il Router/Gateway*2* tra l'IPS e il router principale serve a instradare il traffico filtrato dall'IPS verso la rete interna privata. È locato lì per separare e gestire il traffico autorizzato e sicuro che proviene dalla DMZ e dalla WAN, garantendo che solo il traffico legittimo passi attraverso verso i dispositivi interni.

L'IPS*2* è locato vicino al Router per prevenire intrusioni o attacchi sia nella DMZ (Senso inverso wan-firewall-ips-router-ips-dmz.) che nella rete privata, bloccando gli attacchi in tempo reale prima che possa creare problemi o fare danni brutti.

L'IDS*1* invece è stato posizionato nella rete per rilevare intrusioni sospette e monitorare il traffico, permettendo di identificare potenziali minacce dopo che il traffico è stato filtrato dall'IPS, aggiungendo un ulteriore livello di sicurezza(better be safe than sorry).

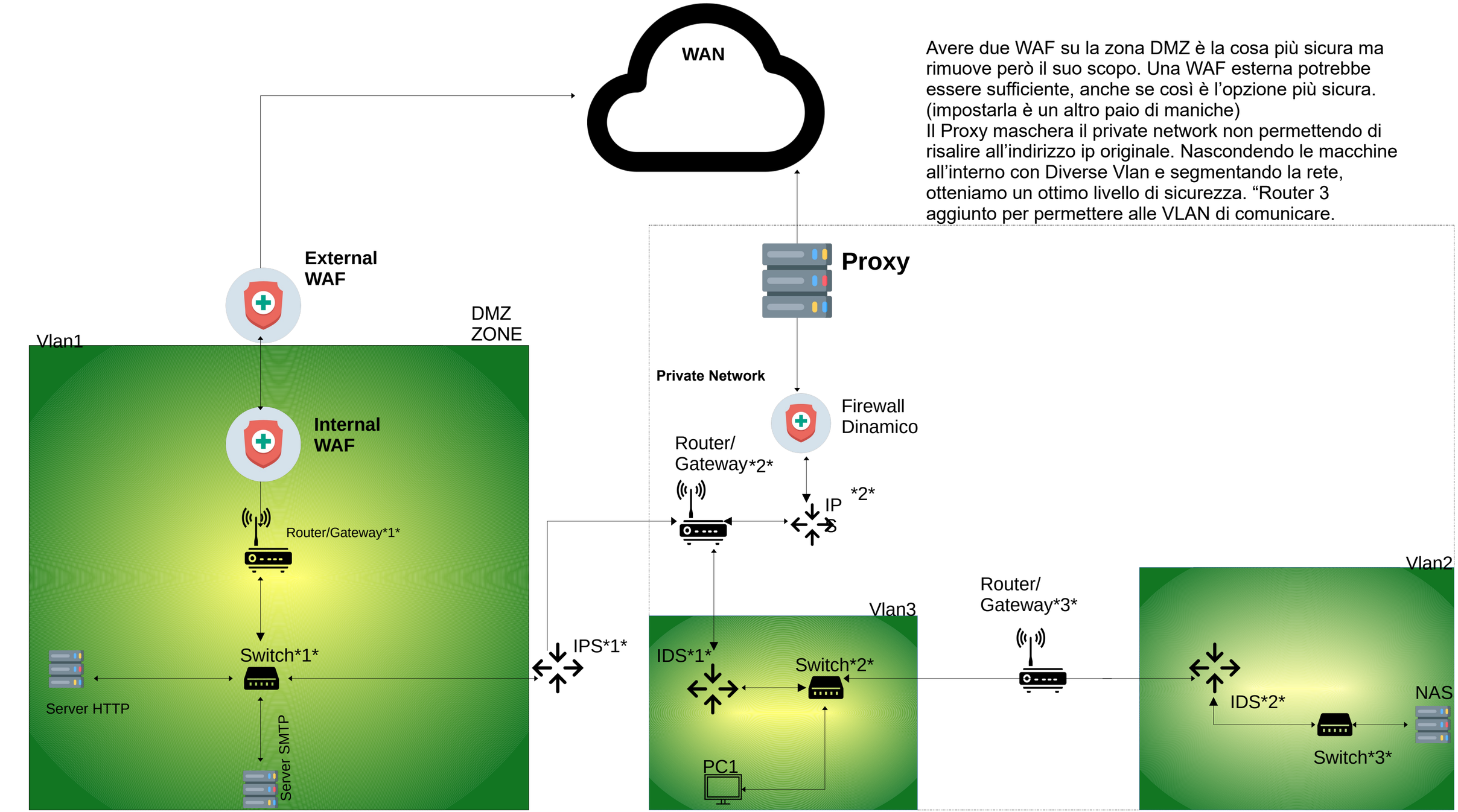
Lo Switch*2* è stato messo per connettere i dispositivi all'interno della rete, permettendo la comunicazione tra server, PC, NAS e altri componenti, permettendo il flusso di dati all'interno della rete privata.

L'IDS*2* aggiuntivo è stato inserito per monitorare specificamente la rete interna e rilevare eventuali attività anomale o intrusioni che potrebbero essere sfuggite ai livelli precedenti di sicurezza, garantendo una sorveglianza costante sul traffico locale (più nascosto possibile e protetto il NAS)

Switch*3* è stato messo per gestire la connessione tra dispositivi specifici come il NAS e altri componenti interni, ottimizzando il traffico locale nella rete privata e separando le comunicazioni in segmenti distinti per migliorare le prestazioni e la sicurezza.

Il NAS (Network Attached Storage) serve per l'archiviazione centralizzata dei dati, permettendo a tutti i dispositivi nella rete privata di accedere, condividere e salvare file in un'unica posizione sicura e facilmente gestibile (Auth permitted)

Considerazioni: Si potrebbe aggiungere 3 vlan per segmentare la rete privata aumentando la sicurezza complessiva, con aggiunta di router gateway ove necessario per lo scabio di dati tra le reti diverse. Aggiunta di un Proxy per il mascheramento dell'indirizzo ip e 2 WAF (su DMZ Waf to Waf aproach) per un complessivo aumento di sicurezza significativo. ex.-


WAN
Avere due WAF su la zona DMZ è la cosa più sicura ma rimuove però il suo scopo. Una WAF esterna potrebbe essere sufficiente, anche se così è l'opzione più sicura. (impostarla è un altro paio di maniche)
Il Proxy maschera il private network non permettendo di risalire all'indirizzo ip originale. Nascondendo le macchine all'interno con Diverse Vlan e segmentando la rete, otteniamo un ottimo livello di sicurezza. "Router 3 aggiunto per permettere alle VLAN di comunicare.
External WAF
Proxy
DMZ ZONE
Vlan1
Private Network
Firewall Dinamico
Router/ Gateway*2*
IP *2*
Internal WAF
Router/Gateway*1*
Switch*1*
IPS*1*
Server HTTP
Server SMTP
Vlan3
IDS*1*
Switch*2*
PC1
Router/ Gateway*3*
Vlan2
IDS*2*
NAS
Switch*3*

Un compromesso accettabile.