REPORT
INFRASTRUTTURA DI RETE SICURA

Progetto: Architettura di rete aziendale multilivello con DMZ e Firewall Perimetrale.

Obbiettivo: Creare una rete segmentata per 120 host, garantendo sicurezza, scalabilità e servizi automatizzati.

TOPOLOGIA FISICA E SWITCH

Obbiettivo

La connessione è stata suddivisa in 6 piani come richiesto, mantenendo il traffico di ogni livello separato per sicurezza e prestazioni, ma permettendo una gestione centralizzata.

Configurazione Switch e VLAN

Abbiamo utilizzato 6 switch (uno per piano) e implementato le VLAN (Virtual Local Area Network)

1. Creazione VLAN : Abbiamo diviso la rete in 6 sottoreti una per ogni piano dell'edificio.

VLAN 10 = Piano terra
VLAN 20 = Primo piano
VLAN 30 = Secondo piano
VLAN 40 = Terzo piano
VLAN 50 = Quarto piano
VLAN 60 = Quinto piano

Abbiamo usato le VLAN per poter dividere ogni piano e far sì che un problema al piano terra non potesse bloccare altri piani.

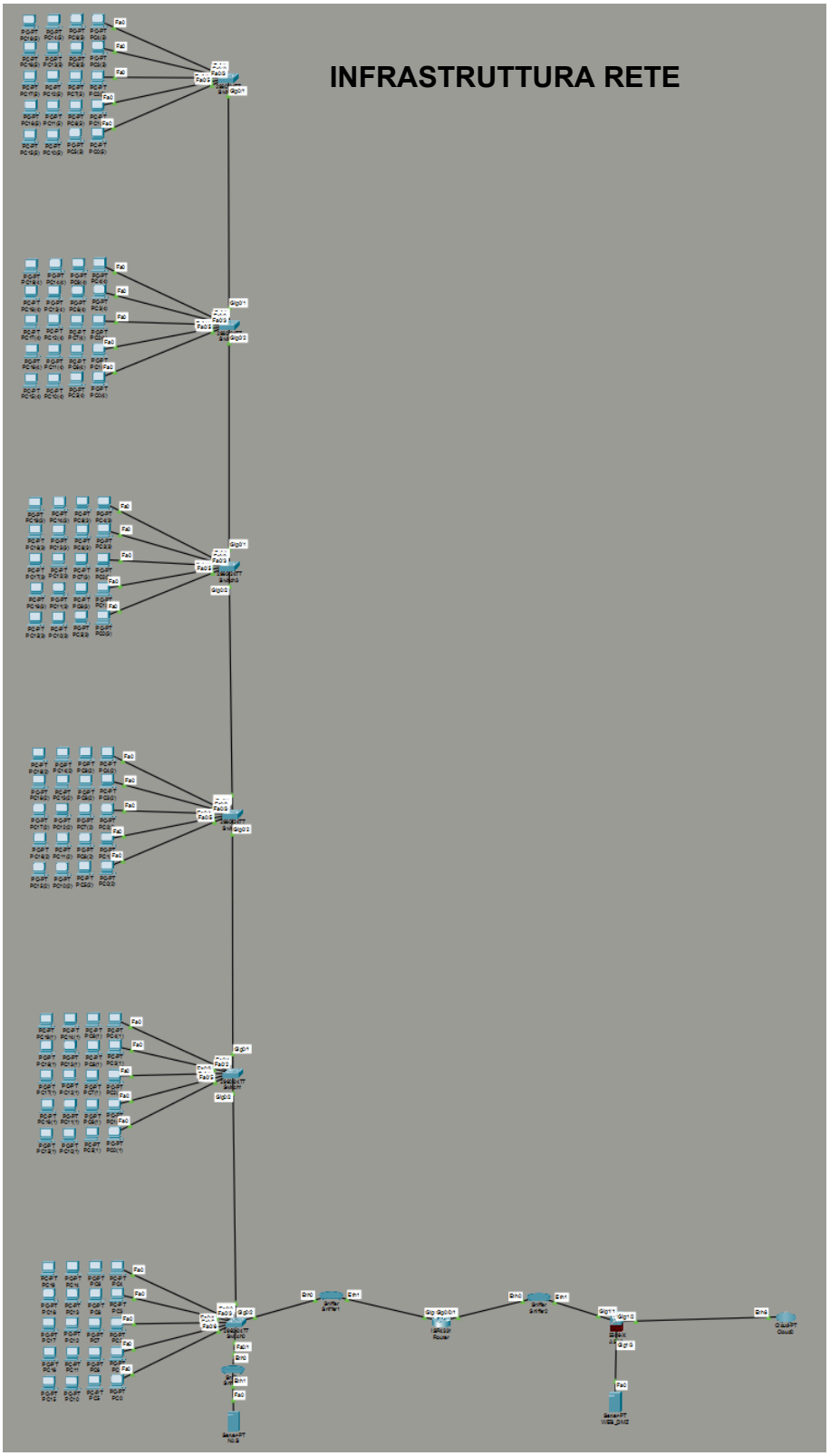
SCREENSHOT VLAN

2. Configurazione TRUNK (Collegamenti tra switch)

Sono state configurate le porte gigabit tra i vari Switch e tra Switch e Router in mod TRUNK
Questo perché una porta normale (access) può portare una sola VLAN, mentre il TRUNK usa il protocollo 802.1Q per taggare i pacchetti, permettendo a un solo cavo fisico di trasportare il traffico di tutte le VLAN contemporaneamente.

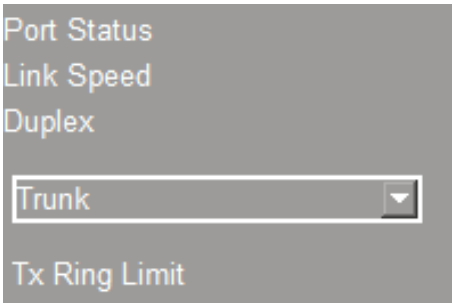
3. Configurazione Access (tra i PC).

Le porte FastEthernet collegate ai PC sono state settate su ACCESS sulla VLAN specifica del proprio piano.

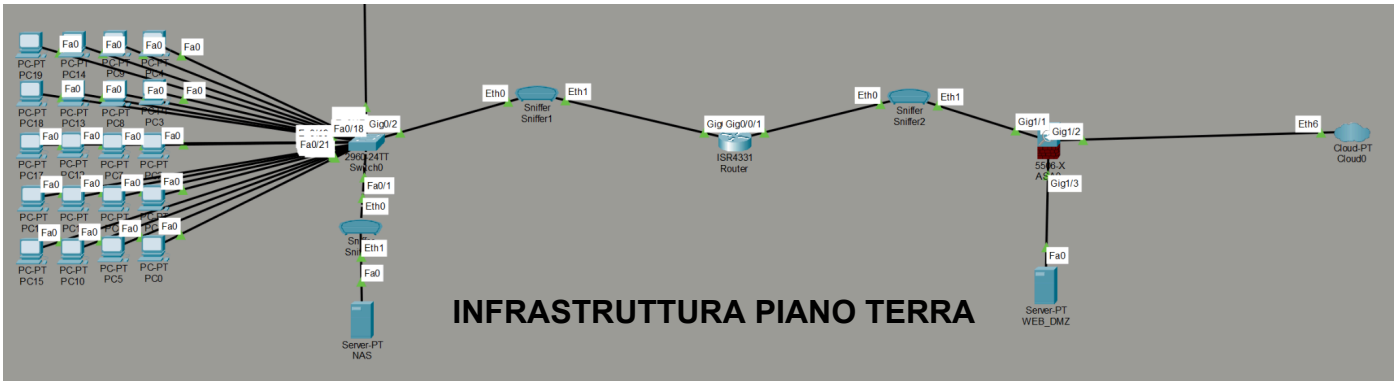


VLAN No	
1	default
10	PIANO_0
20	PIANO_1
30	PIANO_2
40	PIANO_3
50	PIANO_4
60	PIANO_5
1002	fddi-default
1003	token-ring-default
1004	fddinet-default
1005	trnet-default

VLAN DI OGNI PIANO



PORTE TRA SWITCH IN TRUNK



CONFIGURAZIONE ROUTER FIREWALL

È stato usato un Router firewall posizionato al piano terra e collegato allo switch, per far parlare i vari piani con il NAS al piano terra, in questo caso il Router fa da ponte, ed è stato utilizzato anche per assegnare i 120 IP differenti per i vari PC.

Configurazione eseguita: Abbiamo utilizzato un Router @ , configurandolo in modalità "Router-on-a-stick" e come server DHCP.

1. Router-on-a-stick (Sotto interfacce)

Invece di usare 6 cavi fisici per collegare ogni switch al router, abbiamo acceso una singola porta fisica collegando solo lo Switch al piano terra con il Router e creato 6 interfacce virtuali una per ogni VLAN.

Comando Chiave: "encapsulation dot1Q (10,20,30….)"

Questo comando dice al router: "Tutto il traffico taggato con ID (10,20,30…..), deve essere gestito da questa interfaccia virtuale, che ha l'IP 192.168.(10,20,30…).1". Questo funge da Default Gateway per i PC.

2. Server DHCP

Abbiamo configurato 6 Pool DHCP sul Router.

Il DHCP automatizza l'assegnazione degli IP, questo vuol dire che quando un PC si accende, chiede un IP in broadcast, il Router lo intercetta e gli assegna un indirizzo valido per lo specifico piano del PC.

3. Indirizzi Esclusi

Abbiamo escluso i primi 10 indirizzi dal pool (da.1 a .10)

Questo è stato fatto per evitare conflitti IP.
L'indirizzo IP .1 è del router e il .5 è del NAS. Se il DHCP li assegnasse per sbaglio ad un PC la rete crollerebbe (PC conflict).

Configurazione parte firewall

Sono state inserite delle regole per far sì che il Piano 4 (marketing) e il Piano 5 (segreteria) avessero restrizioni nei propri PC.

Piano 4 (marketing) = Alla VLAN di questo piano è stato negato l'accesso al server NAS

Piano 5 (segreteria) = Alla VLAN di questo piano è stato negato l'accesso illimitato ad internet, dando l'opzione di poter visitare solo il sito Dilitrust (sito che verrà utilizzato dalle segreteria)

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# exit
Router(config)#interface GigabitEthernet0/0/0.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
Router(config-subif)# exit
Router(config)#interface GigabitEthernet0/0/0.30
Router(config-subif)# encapsulation dot1Q 30
Router(config-subif)# ip address 192.168.30.1 255.255.255.0
Router(config-subif)# exit
Router(config)#interface GigabitEthernet0/0/0.40
Router(config-subif)# encapsulation dot1Q 40
Router(config-subif)# ip address 192.168.40.1 255.255.255.0
Router(config-subif)# exit
Router(config)#interface GigabitEthernet0/0/0.50
Router(config-subif)# encapsulation dot1Q 50
Router(config-subif)# ip address 192.168.50.1 255.255.255.0
Router(config-subif)# exit
Router(config)#interface GigabitEthernet0/0/0.60
Router(config-subif)# encapsulation dot1Q 60
Router(config-subif)# ip address 192.168.60.1 255.255.255.0
Router(config-subif)# exit
Router(config)#
Router(config)#
Router(config)#ip dhcp pool P0
Router(dhcp-config)# network 192.168.10.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.10.1
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)#ip dhcp pool P1
Router(dhcp-config)# network 192.168.20.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.20.1
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)#ip dhcp pool P2
Router(dhcp-config)# network 192.168.30.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.30.1
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)#ip dhcp pool P3
Router(dhcp-config)# network 192.168.40.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.40.1
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)#ip dhcp pool P4
Router(dhcp-config)# network 192.168.50.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.50.1
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)#ip dhcp pool P5
Router(dhcp-config)# network 192.168.60.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.60.1
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)# ip address 10.0.0.1 255.255.255.252
Router(config-if)# no shutdown

Router(config-if)# exit
%LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to down

Router(config)#
Router(config)#
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down

%LINK-3-UPDOWN: Interface GigabitEthernet0/0/0.10, changed state to down

%LINK-3-UPDOWN: Interface GigabitEthernet0/0/0.20, changed state to down

%LINK-3-UPDOWN: Interface GigabitEthernet0/0/0.30, changed state to down

%LINK-3-UPDOWN: Interface GigabitEthernet0/0/0.40, changed state to down

%LINK-3-UPDOWN: Interface GigabitEthernet0/0/0.50, changed state to down

%LINK-3-UPDOWN: Interface GigabitEthernet0/0/0.60, changed state to down

Router(config-if)#ip route 0.0.0.0 0.0.0.0 10.0.0.2
Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	1/594 KiB	*	*	*	KALI Address	80	*	*		Anti-Lockout Rule	
	0/0 B	IPv4 *	Rete_ Piano_4	*	NAS	*	*	none		Blocco Piano 4 al NAS	
	0/0 B	IPv4 TCP/ UDP	Rete_ Piano_5	*	8.8.8.8	53 (DNS)	*	none		Pass DNS	
	0/0 B	IPv4 TCP	Rete_ Piano_5	*	Siti_Lavoro	443 (HTTPS)	*	none		Pass segretarie Dilitrust	
	0/0 B	IPv4 *	Rete_ Piano_5	*	*	*	*	none		Blocco totale piano 5	
	3/687 KiB	IPv4 *	KALI subnets	*	*	*	*	none		Default allow LAN to any rule	
	0/0 B	IPv6 *	KALI subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

SICUREZZA PERIMETRALE (FIREWALL)

Obbiettivo

Proteggere la rete interna da internet ed esporre un Web Server pubblico in una zona isolata,in questo modo se il server viene hackerato, la rete interna resta salva.

Configurazione eseguita

Abbiamo utilizzato un Firewall @

1. Zone e Security Levels

INSIDE (VLAN interna) : Security Level 100 (massima fiducia)

OUTSIDE (Internet): Security Level 0 (Nessuna fiducia)

DMZ (Server Web): Security Level 50 (Fiducia media)

Di default, Questo Firewall permette traffico da livello Alto a Basso (Inside -> Outside), ma blocca tutto da Basso ad Alto. Questo impedisce a Internet di entrare nella rete aziendale.

Routing Statico sul Firewall

Abbiamo aggiunto la rotta: route inside 192.168.0.0 255.255.0.0 10.0.0.1

Il Firewall non conosce la nostra rete interna (VLAN 10-60). Senza questa rotta, quando il Web Server rispondeva a un ping, il Firewall non sapeva dove mandare la risposta e la buttava via. Ora sa che deve passarla al Router (`10.0.0.1`)

Access Control Lists (ACL) e Policy Map

Abbiamo creato una regola (ACL) per permettere il traffico ICMP (Ping) di ritorno.

Anche se il livello di sicurezza lo permette, l'ASA blocca i ping per default perché considera l'ICMP un protocollo "non stateful". Abbiamo dovuto forzare l'ispezione ICMP per permettere la diagnostica.

Regole per rete interna = Il firewall è stato configurato per permettere ai pc di navigare (HTTP/HTTPS), risolvere nomi (DNS) e fare ping. non possono fare altro (es. torrent o connessioni strane verso l'esterno).

regole per la DMZ = il web server deve poter rispondere a internet, ma non deve mai poter iniziare una connessione verso la rete interna. se un hacker prende il server, non può muoversi lateralmente, quindi il firewall è stato settato per fare anche questo.

Regole per l'outside = Il firewall è stato settato anche per far si che da internet nessuno entri tranne chi vuole vedere il sito web.

ASA0

Physical | Config | CLI | Attributes

IOS Command Line Interface

```
Cryptochecksum (unchanged): 381233ad 7be46509 27cb3981 10f61e7a

INFO: Power-On Self-Test in process.
.....................................................................
INFO: Power-On Self-Test complete.

INFO: Starting HW-DRBG health test...
INFO: HW-DRBG health test passed.

INFO: Starting SW-DRBG health test...
INFO: SW-DRBG health test passed.



Type help or '?' for a list of available commands.

ciscoasa>enable
Password:
ciscoasa#conf t
ciscoasa(config)#interface GigabitEthernet1/1
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.0.0.2 255.255.255.252
Waiting for the earlier webvpn instance to terminate...
Previous instance shut down.Starting a new one
ciscoasa(config-if)# no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet1/1, changed state to down
ciscoasa(config-if)# exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#interface GigabitEthernet1/3
ciscoasa(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 172.16.1.1 255.255.255.0
Waiting for the earlier webvpn instance to terminate...
Previous instance shut down.Starting a new one
ciscoasa(config-if)# no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet1/3, changed state to down
ciscoasa(config-if)# exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#route inside 192.168.0.0 255.255.0.0 10.0.0.1
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)#  inspect icmp
ciscoasa(config-pmap-c)#
ciscoasa(config-pmap-c)#exit
ciscoasa(config)#
ciscoasa(config)#exit
ciscoasa#
ciscoasa#
ciscoasa#access-list INSIDE_RULES extended permit tcp 192.168.0.0 255.255.0.0 any eq 80
          ^
% Invalid input detected at '^' marker.

ciscoasa#access-list INSIDE_RULES extended permit tcp 192.168.0.0 255.255.0.0 any eq 443
          ^
% Invalid input detected at '^' marker.

ciscoasa#access-list INSIDE_RULES extended permit udp 192.168.0.0 255.255.0.0 any eq 53
          ^
% Invalid input detected at '^' marker.

ciscoasa#access-list INSIDE_RULES extended permit icmp any any
          ^
% Invalid input detected at '^' marker.

ciscoasa#conf t
ciscoasa(config)#access-list INSIDE_RULES extended permit tcp 192.168.0.0 255.255.0.0 any eq 80
ciscoasa(config)#access-list INSIDE_RULES extended permit tcp 192.168.0.0 255.255.0.0 any eq 443
ciscoasa(config)#access-list INSIDE_RULES extended permit udp 192.168.0.0 255.255.0.0 any eq 53
ciscoasa(config)#access-list INSIDE_RULES extended permit icmp any any
ciscoasa(config)#
ciscoasa(config)#access-group INSIDE_RULES in interface inside
ciscoasa(config)#
ciscoasa(config)#access-list DMZ_RULES extended deny ip 172.16.1.0 255.255.255.0 192.168.0.0 255.255.0.0
ciscoasa(config)#
ciscoasa(config)#access-group DMZ_RULES in interface dmz
ciscoasa(config)#
ciscoasa(config)#access-list OUTSIDE_RULES extended permit tcp any host 172.16.1.10 eq 80
ciscoasa(config)#
ciscoasa(config)#access-group OUTSIDE_RULES in interface outside
```

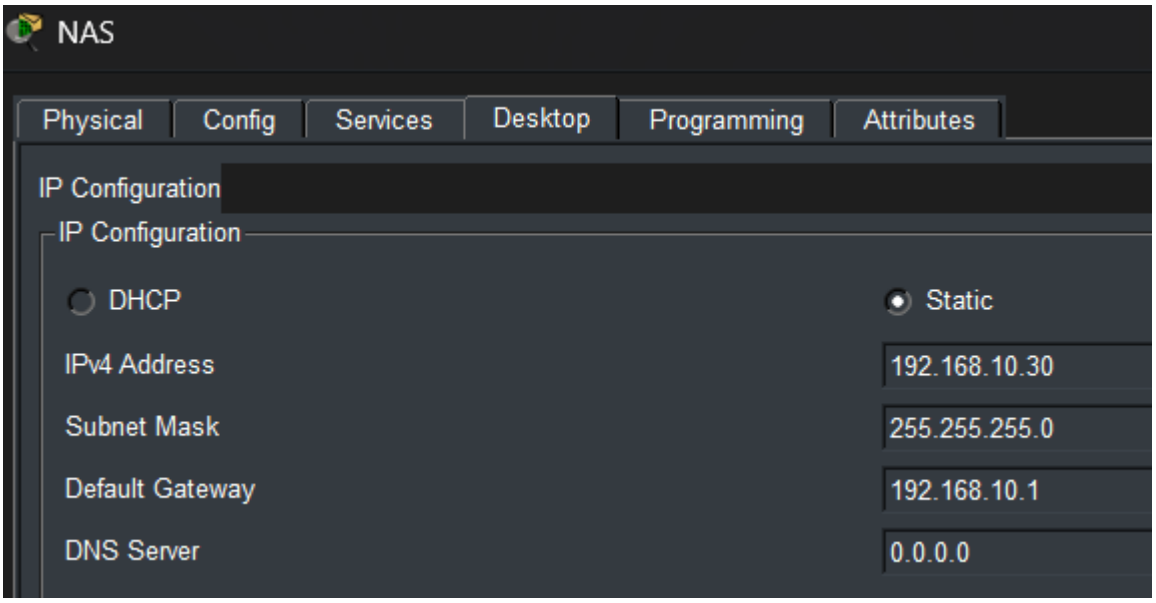
SERVIZI SERVER

NAS (Network Attached Storage)

Posizione : Piano terra (Vlan 10), collegato allo switch Piano_Terra.

Configurazione : IP statico 192.168.10.5, Gateway 192.168.10.1

Funzionamento : Grazie al settaggio Routing con le VLAN, tutti i PC di qualsiasi piano possono salvare file sul NAS attraverso il Gateway (dispositivo hardware o software che collega due reti diverse, traducendo i protocolli per permettere la comunicazione)



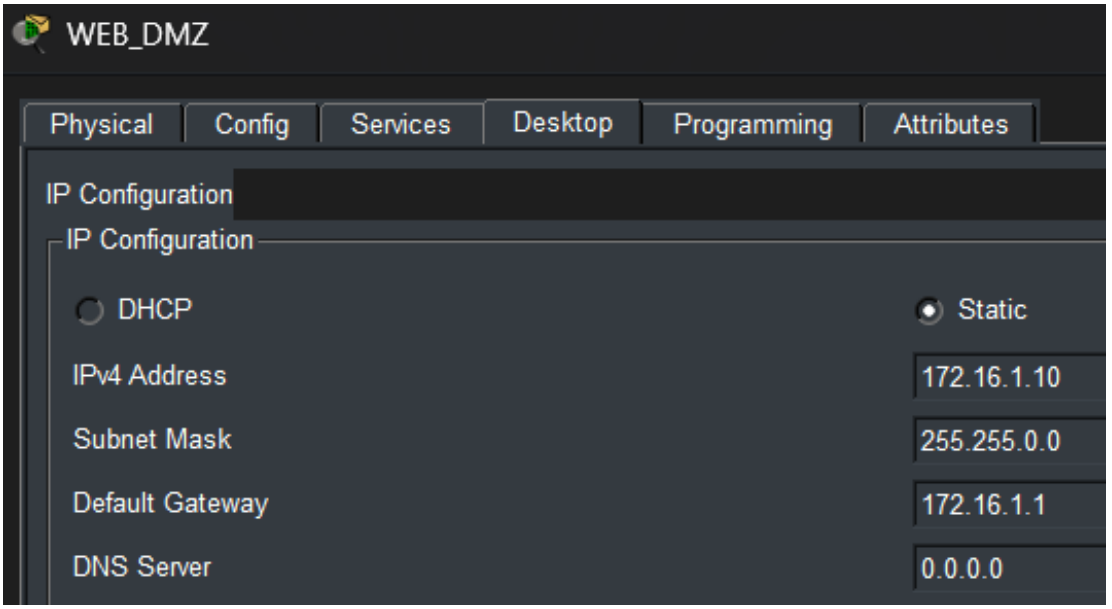
Server Web (DMZ)

Posizione: Zona DMZ (Demilitarized Zone) del Firewall.

Dettagli di Configurazione : Indirizzo IP: Statico 172.16.1.10

Gateway : 172.16.1.1

Funzionalità e Sicurezza : È isolato. Se un hacker compromette questo server, il Firewall (Security Level 50) gli impedisce di saltare nella rete interna (Security Level 100).



SISTEMA DI MONITORAGGIO (IDS/IPS)

Obiettivo : Avere visibilità sul traffico che passa nei punti critici della rete.

Configurazione : Sono stati posizionati 3 Sniffer in punti strategici

1) CORE (analisi traffico interno)

Posizione : sul collegamento Trunk tra Router e Switch Piano_Terra

Utilità e Funzionamento : Questa sonda è fondamentale per rilevare le minacce interne. Se un PC del piano 5, infettato da un malware, cercasse di attaccare un pc su un altro piano, il Firewall perimetrale non se ne accorgerebbe, mentre questa sonda intercetta e segnala questi movimenti anomali all'interno della LAN

2) EDGE (Analisi perimetrale)

Posizione : sul collegamento tra Router e Firewall

Utilità e Funzionamento : Agisce come una seconda linea di difesa dietro al firewall.

Rileva attacchi che sono riusciti a bypassare le regole statiche del firewall.

Rileva tentativi di Command & Control ovvero PC interni che cercano di comunicare con server hacker esterni.

3) ASSET (Protezione dei dati critici - NAS)

Posizione : sul collegamento diretto tra Switch Piano_Terra e Server NAS

Utilità e Funzionamento : Data loss prevention (DLP) e integrità dei file.

Sonda più critica.
Poiché il NAS contiene i dati aziendali sensibili, questa sonda applica filtri molto stringenti.

Analizza specificamente i protocolli di trasferimento file per rivelare:

- Tentativi di accesso non autorizzato
- Esfiltrazione massiva di dati
- Ransomware (malware che limita l'accesso del dispositivo che infetta chiedendo un riscatto) che tenta di cifrare i file condivisi.

Tutte e tre le sonde sono configurate per l'ispezione profonda dei pacchetti (Deep Packet Inspection) sui protocolli ICMP, TCP, UDP e HTTP.
L'architettura a tre livelli garantisce che nessun pacchetto possa raggiungere i dati sensibili senza essere stato scansionato almeno due volte (una volta al perimetro o nel core, e una volta a ridosso del server).