Rete per la Tetha

Rete per la Tetha

Indice

Introduzione

1.1 Obiettivi del Progetto

L’obiettivo principale di questo progetto è progettare e implementare una rete aziendale che garantisca **sicurezza**, **affidabilità** e **scalabilità** per soddisfare le esigenze operative di un’azienda di produzione di abbigliamento. La rete sarà in grado di supportare gli attuali flussi di lavoro, l'espansione futura e le necessità di protezione dei dati aziendali, con una particolare attenzione alle seguenti aree:

Sicurezza:

- **Segmentazione**: Isolamento delle comunicazioni tra reparti aziendali tramite VLAN.
- **Protezione perimetrale**: Firewall avanzato con IDS/IPS integrati per rilevare e mitigare attacchi.
- **Controllo degli accessi**: Regole ACL granulari per limitare il traffico non autorizzato.

Affidabilità:

- **Ridondanza**: Implementazione di tecnologie come StackWise Virtual, HSRP e firewall in Active/Passive per garantire alta disponibilità.
- **Continuità operativa**: Strumenti di monitoraggio e backup per prevenire interruzioni e garantire il rapido ripristino dei servizi critici.

Scalabilità:

- **Espandibilità della rete**: Progettazione per consentire l'aggiunta di VLAN, dispositivi e sedi aziendali senza dover riprogettare l’architettura.
- **Supporto per l’aumento del traffico**: Utilizzo di tecnologie ad alte prestazioni come fibra multimodale OM4 e uplink 40/100 Gbps.

1.2 Architettura di Rete Proposta

La rete è progettata seguendo un **modello gerarchico a tre livelli**, una best practice consolidata nel networking aziendale per garantire una gestione ottimale del traffico e una chiara separazione funzionale.

Access Layer (Livello di Accesso):

- Connette tutti gli endpoint aziendali, tra cui PC, telefoni VoIP e stampanti.
- Implementa la segmentazione logica tramite VLAN per separare i diversi reparti aziendali.
- Utilizza **switch Cisco Catalyst 9300-48P-A** per supportare dispositivi con PoE+ e garantire uplink ad alta velocità.

Distribution Layer (Livello di Distribuzione):

- Aggrega il traffico proveniente dagli switch di accesso.
- Gestisce il routing inter-VLAN e applica policy di sicurezza avanzate tramite ACL.

- Fornisce ridondanza tramite **StackWise Virtual** e collegamenti in fibra multimodale OM4.
- Utilizza **switch Cisco Catalyst 9500-40X** per il routing Layer 3 e il collegamento con il core layer.

Core/Edge Layer (Livello Core/Edge):

- Offre connettività con la WAN e separa la rete interna dalla DMZ e dalla rete esterna.
- Integra **firewall Palo Alto PA-5220** in configurazione Active/Passive per protezione avanzata.
- Utilizza **router Cisco Catalyst 8500-12X4QC** per connessioni WAN ad alta velocità con HSRP per il failover automatico.

Caratteristiche Distintive

Sicurezza avanzata:

- Firewall con analisi Layer 7.
- IDS/IPS integrati per monitorare il traffico in entrata e uscita.
- Policy ACL configurate per limitare il traffico tra VLAN sensibili.

Ridondanza hardware:

- Configurazioni Active/Passive per firewall e router WAN.
- **StackWise Virtual** per switch di distribuzione.

Gestione centralizzata:

- Monitoraggio continuo tramite **PRTG Network Monitor**.
- Backup automatizzati con **Veeam Backup & Replication**.

---

2. Specifiche della Rete

2.1 Struttura Fisica e Logica

Struttura Fisica

La rete è distribuita in un edificio aziendale a sei piani, con un'infrastruttura centralizzata situata nel data center al piano terra. Gli elementi principali sono:

Access Layer (Livello di Accesso):

- **Switch di accesso dedicati** (1 per piano), configurati per connettere endpoint come PC, telefoni VoIP, stampanti e altri dispositivi.
- Ogni switch di accesso è montato in un rack dedicato, dotato di **patch panel** per terminare i cavi Cat 6A.

Distribution Layer (Livello di Distribuzione):

- Due **switch di distribuzione** situati nel data center, configurati in **StackWise Virtual** per fornire ridondanza e aggregazione del traffico proveniente dagli switch di accesso.

- Collegamenti ridondanti in **fibra multimodale OM4** agli switch di accesso.

Core/Edge Layer (Livello Core/Edge):

- Due **router WAN** configurati con **HSRP** per gestire la connessione alla rete esterna.
- **Firewall Palo Alto PA-5220** in configurazione **Active/Passive** per proteggere il traffico tra WAN, DMZ e LAN interna.

Data Center:

Ospita server e storage critici:

- **Server consolidato** per DHCP, DNS e backup.
- **Server web** per il sito e-commerce, isolato in DMZ.
- **NAS** per l'archiviazione centralizzata.
- Collegamenti in rame Cat 6A e fibra OM4 per alte prestazioni e scalabilità.

Struttura Logica

La rete è segmentata logicamente tramite **VLAN** per isolare i reparti e ottimizzare la gestione del traffico:

VLAN ID	Nome	Funzione
10	Amministrazione	Connessioni del reparto amministrativo.
20	Produzione	Gestisce il traffico della produzione aziendale.
30	Vendite	Connessioni dei dispositivi del reparto commerciale.
40	DMZ	Isolamento del server e-commerce.
50	NAS	VLAN dedicata per archiviazione e backup centralizzati.
70	VoIP	Separazione della telefonia IP.
80	Management	Gestione dei dispositivi di rete (switch, router, firewall).
90	Sistemisti	Accesso riservato agli amministratori di sistema.

2.2 Dispositivi Utilizzati

Dispositivo	Modello	Funzione
Switch di Accesso	Cisco Catalyst 9300-48P-A	Connettere endpoint e gestire VLAN.
Switch di Distribuzione	Cisco Catalyst 9500-40X	Aggregazione del traffico, routing inter-VLAN.
Router WAN	Cisco Catalyst 8500-12X4QC	Connessioni WAN ridondanti con HSRP.

Dispositivo	Modello	Funzione
Firewall	Palo Alto PA-5220	Protezione Layer 7, IDS/IPS integrato.
Server Consolidato	Dell PowerEdge R750	Virtualizzazione, DHCP, DNS e backup.
Server Web	Dell PowerEdge R650	Hosting del sito e-commerce in DMZ.
NAS	Synology RS3621xs+	Archiviazione e condivisione file.

2.3 Protocolli e Tecnologie Implementate

Protocollo/Tecnologia	Funzione
IP (Internet Protocol)	Instradamento e comunicazione tra i dispositivi di rete.
VLAN (802.1Q)	Segmentazione logica della rete per isolare il traffico tra reparti.
STP (Rapid PVST+)	Prevenzione di loop nei collegamenti ridondanti tra switch.
HSRP	Ridondanza per i gateway virtuali delle VLAN.
ACL (Access Control List)	Regole per limitare o consentire traffico specifico tra VLAN e WAN.
SNMP	Monitoraggio dei dispositivi di rete tramite PRTG.
NTP	Sincronizzazione dell’ora tra i dispositivi di rete.
QoS	Prioritizzazione del traffico VoIP e dati critici.
StackWise Virtual	Aggregazione di due switch di distribuzione in un'unica unità logica.

2.4 Software e Licenze

Software/Servizio	Dispositivo Host	Funzione	Licenza
VMware vSphere	Dell PowerEdge R750	Virtualizzazione dei server.	Licenza standard VMware vSphere.
Windows Server 2022	Dell PowerEdge R750 e R650	Servizi DHCP, DNS, Active Directory, server web.	Licenza Windows Server.
PRTG Network Monitor	Dell PowerEdge R250	Monitoraggio centralizzato della rete.	Licenza PRTG 500 sensori.
Veeam Backup & Replication	Dell PowerEdge R750	Backup incrementale e ripristino rapido.	Licenza Veeam Essentials.
PAN-OS	Palo Alto PA-5220	Gestione firewall e IDS/IPS.	Licenza Palo Alto.
Synology DSM	Synology RS3621xs+	Gestione dello storage centralizzato.	Licenza integrata.

3. Configurazioni Tecniche

3.1 VLAN e Segmentazione

Le VLAN sono configurate per segmentare logicamente la rete, isolando i vari reparti aziendali e garantendo sicurezza, performance e una gestione più semplice del traffico.

Configurazione delle VLAN sugli Switch di Accesso

Esempio per lo switch di accesso al piano 1:

```
vlan 10
 name Amministrazione
vlan 20
 name Produzione
vlan 30
 name Vendite
vlan 40
 name DMZ
vlan 50
 name NAS
vlan 70
 name VoIP
vlan 80
 name Management
vlan 90
 name Sistemisti
!
interface range fa0/1-12
 description Amministrazione
 switchport mode access
 switchport access vlan 10
!
interface range fa0/13-24
 description Produzione
 switchport mode access
 switchport access vlan 20
```

Configurazione delle Porte Trunk sugli Uplink

Sugli uplink verso gli switch di distribuzione:

```
interface fa0/25
 description To Distribution-Switch-1
```

```
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,70,80,90
 spanning-tree portfast trunk
!
interface fa0/26
 description To Distribution-Switch-2
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,70,80,90
 spanning-tree portfast trunk
```

3.2 Routing inter-VLAN

Il routing tra VLAN è gestito dagli switch di distribuzione Cisco Catalyst 9500 configurati in StackWise Virtual, utilizzando interfacce VLAN con indirizzamenti IP dedicati.

Configurazione degli Switch di Distribuzione:

```
ip routing
!
interface vlan 10
 ip address 192.168.10.1 255.255.255.0
 description Amministrazione
!
interface vlan 20
 ip address 192.168.20.1 255.255.255.0
 description Produzione
!
interface vlan 30
 ip address 192.168.30.1 255.255.255.0
 description Vendite
!
interface vlan 40
 ip address 10.0.40.1 255.255.255.0
 description DMZ
!
interface vlan 50
 ip address 192.168.50.1 255.255.255.0
 description NAS
!
interface vlan 70
 ip address 192.168.70.1 255.255.255.0
 description VoIP
!
interface vlan 80
```

```
 ip address 192.168.80.1 255.255.255.0
 description Management
!
interface vlan 90
 ip address 192.168.90.1 255.255.255.0
 description Sistemisti
```

3.3 Access Control Lists (ACL)

Le ACL vengono utilizzate per controllare il traffico tra VLAN e verso risorse critiche,

Lista delle ACL

1. VLAN 10 (Amministrazione)

Consente l'accesso a risorse critiche come NAS e server di gestione; bloccare l'accesso alla VLAN DMZ e altre VLAN non necessarie.

```
ip access-list extended VLAN_10_ACL
 permit tcp 192.168.10.0 0.0.0.255 192.168.50.0 0.0.0.255 eq 445
 permit tcp 192.168.10.0 0.0.0.255 192.168.80.0 0.0.0.255 eq 22
 deny ip 192.168.10.0 0.0.0.255 10.0.40.0 0.0.0.255
 deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
 permit ip 192.168.10.0 0.0.0.255 any
```

2. VLAN 20 (Produzione)

Limita l'accesso alla VLAN NAS per file sharing; bloccare il traffico verso DMZ e altre VLAN non necessarie.

```
ip access-list extended VLAN_20_ACL
 permit tcp 192.168.20.0 0.0.0.255 192.168.50.0 0.0.0.255 eq 445
 deny ip 192.168.20.0 0.0.0.255 10.0.40.0 0.0.0.255
 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
 permit ip 192.168.20.0 0.0.0.255 any
```

3. VLAN 30 (Vendite)

Limita l'accesso alla VLAN NAS per file sharing e bloccare il traffico verso VLAN sensibili (es. Amministrazione e DMZ).

```

ip access-list extended VLAN_30_ACL
 permit tcp 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255 eq 445
 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
 deny ip 192.168.30.0 0.0.0.255 10.0.40.0 0.0.0.255
 permit ip 192.168.30.0 0.0.0.255 any
```

4. VLAN 40 (DMZ)

Consente solo il traffico necessario verso l'esterno (HTTP, HTTPS); bloccare il traffico verso VLAN interne.

```
ip access-list extended VLAN_40_ACL
 permit tcp 10.0.40.0 0.0.0.255 any eq 80
 permit tcp 10.0.40.0 0.0.0.255 any eq 443
 deny ip 10.0.40.0 0.0.0.255 192.168.0.0 0.0.255.255
 permit ip 10.0.40.0 0.0.0.255 any
```

5. VLAN 50 (NAS)

Limita l'accesso al NAS alle VLAN autorizzate (Amministrazione, Produzione e Vendite); bloccare il traffico non autorizzato.

```
ip access-list extended VLAN_50_ACL
 permit tcp 192.168.10.0 0.0.0.255 192.168.50.0 0.0.0.255 eq 445
 permit tcp 192.168.20.0 0.0.0.255 192.168.50.0 0.0.0.255 eq 445
 permit tcp 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255 eq 445
 deny ip any any
```

6. VLAN 70 (VoIP)

Garantisce la comunicazione tra dispositivi VoIP e server di gestione; bloccare traffico non necessario.

```
ip access-list extended VLAN_70_ACL
 permit udp 192.168.70.0 0.0.0.255 192.168.80.0 0.0.0.255 eq 5060
 permit udp 192.168.70.0 0.0.0.255 192.168.80.0 0.0.0.255 eq 5061
 deny ip 192.168.70.0 0.0.0.255 any
```

7. VLAN 80 (Management)

Consente l'accesso amministrativo a dispositivi di rete e server, bloccare traffico non necessario.

```
ip access-list extended VLAN_80_ACL
 permit tcp 192.168.80.0 0.0.0.255 192.168.10.0 0.0.0.255 eq 22
 permit tcp 192.168.80.0 0.0.0.255 192.168.20.0 0.0.0.255 eq 22
 permit tcp 192.168.80.0 0.0.0.255 192.168.50.0 0.0.0.255 eq 445
 permit ip 192.168.80.0 0.0.0.255 any
```

8. VLAN 90 (Sistemisti)

Consente il traffico necessario per l'accesso amministrativo e per l'autenticazione verso Active Directory.

```
Copia codice
ip access-list extended VLAN_90_ACL
 permit tcp 192.168.90.0 0.0.0.255 192.168.80.0 0.0.0.255 eq 389
```

```
 permit tcp 192.168.90.0 0.0.0.255 192.168.50.0 0.0.0.255 eq 445
 deny ip 192.168.90.0 0.0.0.255 any
```

Implementazione delle ACL

Ogni ACL deve essere applicata all'interfaccia VLAN corrispondente. Ad esempio, per VLAN 10:

```
interface Vlan10
 ip access-group VLAN_10_ACL in
```

3.4 Redundancy (StackWise Virtual, HSRP)

Configurazione di StackWise Virtual sugli Switch di Distribuzione:

switch 1

```
stackwise-virtual

interface TenGigabitEthernet1/0/1
 description StackWise Virtual Link to Switch 2
 no switchport
 stackwise-virtual link 1

interface TenGigabitEthernet1/0/2
 description StackWise Virtual Link to Switch 2
 no switchport
 stackwise-virtual link 1

interface GigabitEthernet0/1
 description Dual-Active Detection Link to Switch 2
 no switchport
 stackwise-virtual dual-active-detection

switch 1 priority 15
```

switch 2

```
stackwise-virtual

interface TenGigabitEthernet1/0/1
 description StackWise Virtual Link to Switch 1
 no switchport
 stackwise-virtual link 1

interface TenGigabitEthernet1/0/2
 description StackWise Virtual Link to Switch 1
 no switchport
```

```
 stackwise-virtual link 1

interface GigabitEthernet0/1
 description Dual-Active Detection Link to Switch 1
 no switchport
 stackwise-virtual dual-active-detection

Standby
switch 2 priority 14
```

Configurazione di HSRP su Router1 (Active):

Per semplicità viene mostrata la configurazione solo per due VLAN, ma i comandi sono uguali per tutte

```
interface GigabitEthernet0/0.10
 description VLAN 10 - Amministrazione
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
 standby 1 ip 192.168.10.254
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string securekey

interface GigabitEthernet0/0.20
 description VLAN 20 - Produzione
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 standby 2 ip 192.168.20.254
 standby 2 priority 110
 standby 2 preempt
 standby 2 authentication md5 key-string securekey
```

Su Router 2 (Standby):

```
interface GigabitEthernet0/0.10
 description VLAN 10 - Amministrazione
 encapsulation dot1Q 10
 ip address 192.168.10.2 255.255.255.0
 standby 1 ip 192.168.10.254
 standby 1 priority 100
 standby 1 preempt
 standby 1 authentication md5 key-string securekey

interface GigabitEthernet0/0.20
```

```
description VLAN 20 - Produzione
encapsulation dot1Q 20
ip address 192.168.20.2 255.255.255.0
standby 2 ip 192.168.20.254
standby 2 priority 100
standby 2 preempt
standby 2 authentication md5 key-string securekey
```

3.5 Firewall e IDS

Il firewall Palo Alto PA-5220 è configurato per gestire le seguenti regole di base:

Regole Firewall:

- **DMZ → WAN**: Consentito solo HTTP/HTTPS per l'e-commerce.
- **LAN → DMZ**: Consentito solo traffico specifico (es. SSH, HTTP).
- **WAN → LAN**: Blocco totale tranne per connessioni VPN autorizzate.

IDS/IPS Palo Alto:

Monitoraggio di:

- Comunicazioni verso indirizzi IP malevoli.
- Traffico anomalo (es. scansioni non autorizzate).
- File sospetti con hash noti.

Regola IDS per IP Malevoli:

```
threat-policy
 category malicious-ip
 action block
```

IOC (Indicator of Compromise)

Gli IOC sono segnali utilizzati per identificare attività malevole sulla rete, come indirizzi IP, domini, hash di file e pattern di traffico anomali. Sono integrati nel firewall **Palo Alto PA-5220** per rafforzare la sicurezza della rete tramite:

Feed Automatizzati

- Aggiornamenti regolari da fonti come **Palo Alto WildFire** e **AlienVault OTX**.
- Blocchi automatici di domini e IP noti per attività malevole.

Regole Personalizzate

- Configurazione manuale per specifici IOC rilevati internamente.

Esempio: Bloccare un dominio sospetto:

```
set security policies from Untrust to Trust action deny destination hacker-domain.com
```

---

4. Monitoraggio e Backup

4.1 Soluzioni Implementate (PRTG, Veeam)

PRTG Network Monitor

PRTG è utilizzato per monitorare in tempo reale lo stato della rete, i dispositivi, e le applicazioni critiche. È stato scelto per la sua capacità di fornire un monitoraggio dettagliato e notifiche proattive su eventuali problemi.

Funzioni principali:

- Monitoraggio di dispositivi e servizi tramite **SNMP**, **NetFlow** e **WMI**.
- Dashboard interattiva per visualizzare lo stato della rete.
- Notifiche personalizzate (via email o SMS) per soglie critiche superate (es. utilizzo CPU > 80%).

Veeam Backup & Replication

Veeam protegge i dati aziendali e i servizi critici attraverso backup incrementali e completi. Supporta il ripristino rapido delle macchine virtuali, delle configurazioni dei dispositivi e dei file aziendali.

Funzioni principali:

- Backup delle virtual machine per servizi **DNS**, **DHCP**, **Active Directory** e **server web in DMZ**.
- Backup incrementali notturni e completi settimanali.
- Backup crittografati salvati su NAS con **RAID 6**.
- Conservazione dei backup per 30 giorni con archiviazione sicura.

4.2 Configurazioni Chiave

PRTG Network Monitor

Dispositivi Monitorati:

Sensore	Dispositivo Monitorato	Protocollo	Funzione
SNMP Traffic Sensor	Switch di accesso e distribuzione	SNMP	Monitoraggio del traffico per interfaccia.
CPU Load Sensor	Server consolidati (R750, R650)	SNMP	Monitoraggio del carico della CPU.
Disk Usage Sensor	NAS (Synology RS3621xs+)	SNMP	Monitoraggio dello spazio disco.

Sensore	Dispositivo Monitorato	Protocollo	Funzione
Uptime Sensor	Firewall (Palo Alto PA-5220)	Ping	Controllo della disponibilità dei firewall.
NetFlow Traffic Sensor	Router WAN	NetFlow	Analisi del traffico di rete.

Configurazioni di Base per SNMP:

Sugli switch di accesso e distribuzione:

```
snmp-server community public RO
snmp-server enable traps
snmp-server location "Data Center"
```

Notifiche configurate per:

- Interruzioni degli uplink.
- Superamento della soglia di utilizzo CPU (>80%).
- Errori di sincronizzazione NTP.

Veeam Backup & Replication

Backup configurati per:

Virtual Machine Critiche:

- **Frequenza:** Incrementale notturno, completo settimanale.
- **Dati protetti:** Active Directory, DHCP, DNS, server web.
- **Tempo di ripristino (RTO):** < 15 minuti per servizi critici.

NAS:

- **Frequenza:** Backup completo dei dati aziendali ogni 24 ore.
- **Conservazione:** Su storage dedicato (RAID 6).
- **Sicurezza:** Crittografia abilitata per dati a riposo e in transito.

Backup Repository Configurato su NAS:

```
RAID 6
Crittografia abilitata
Accesso tramite VLAN dedicata (VLAN 50)
```

Procedure di Ripristino:

Virtual Machine:

- Ripristino su host secondario in caso di guasto hardware.

File Aziendali:

- Ripristino da snapshot del NAS in meno di 30 minuti.

---

5. Disaster Recovery

5.1 Piano di Emergenza

Un piano di disaster recovery efficace è cruciale per garantire la continuità operativa dell'azienda in caso di guasti hardware, attacchi informatici o disastri naturali. Il piano implementato combina ridondanza, backup centralizzato e test regolari.

Componenti Principali

Ridondanza dei Dispositivi:

- **Switch di Distribuzione**: Configurati in **StackWise Virtual** per garantire continuità operativa, eliminando il rischio di singoli punti di guasto.
- **Router WAN**: Configurati con **HSRP** per failover automatico del gateway virtuale.
- **Firewall**: Modalità **Active/Passive**, in cui il firewall secondario subentra automaticamente in caso di guasto del primario.

Backup Incrementali e Completi:

- **Dati e Configurazioni**: Backup incrementali notturni e completi settimanali tramite **Veeam Backup & Replication**.
- **NAS e Virtual Machine**: Copie ridondanti dei dati aziendali e delle VM critiche su storage remoto.

Replica dei Servizi Critici:

- Le **virtual machine (VM)** che ospitano i servizi **DNS**, **DHCP**, **Active Directory** e **server web** sono replicate su un host secondario.

Monitoraggio e Notifiche:

- **PRTG** invia notifiche in caso di problemi di connettività, utilizzo anomalo della CPU o guasti hardware.

Documentazione delle Procedure:

- Ogni fase del ripristino è documentata per garantire che il team IT segua un processo strutturato durante l’emergenza.

Obiettivi di Recovery

- **RTO (Recovery Time Objective)**: Ripristino dei servizi critici in meno di 15 minuti.
- **RPO (Recovery Point Objective)**: Perdita massima di dati accettabile limitata a 24 ore.

5.2 Test di Recovery

Il test regolare delle procedure di disaster recovery assicura che il piano sia efficace e aggiornato.

Procedure di Test

Simulazione di Guasto di un Dispositivo:

- Spegnere uno switch di distribuzione per verificare il failover tramite **StackWise Virtual**.
- Disabilitare uno dei router WAN per testare l'attivazione del gateway **HSRP**.

Recupero Dati:

- Simulare la perdita di una VM (es. **Active Directory**) e verificare il ripristino tramite **Veeam Backup**.
- Effettuare il ripristino di file aziendali critici da snapshot del NAS.

Verifica dei Servizi:

Controllare la piena operatività dei servizi ripristinati, come:

- Autenticazione tramite **Active Directory**.
- Risoluzione **DNS**.
- Accesso al sito web e-commerce ospitato in DMZ.

Sincronizzazione e Integrità:

- Assicurarsi che i dati ripristinati siano sincronizzati con i dispositivi rimanenti.
- Verificare che tutte le policy di accesso e sicurezza siano operative.

Documentazione del Test

Ogni test di recovery è documentato per:

- Identificare eventuali punti deboli nelle procedure.
- Migliorare il piano di disaster recovery.
- Dimostrare la conformità con gli standard aziendali e normativi.

Casi d’Uso e Tempi di Recupero

Scenario	Azione	RTO	RPO
Guasto di uno switch di distribuzione	Failover gestito da StackWise Virtual	0 secondi	Nessuna perdita.
Guasto di un router WAN	HSRP attiva il router secondario	1 secondo	Nessuna perdita.
Perdita di una VM critica	Ripristino tramite Veeam Backup	< 15 minuti	24 ore massimo.
Disastro locale (es. incendio)	Ripristino da storage remoto	< 4 ore	24 ore massimo.

---

6. Scalabilità

6.1 Possibilità di Espansione Futura della Rete

La rete è stata progettata per garantire una facile scalabilità, sia in termini di hardware che di configurazioni logiche. Questo approccio consente all'azienda di espandere la rete in base alle esigenze future senza dover apportare modifiche strutturali significative.

Elementi di Scalabilità

1. **VLAN e Segmentazione**
    - La configurazione attuale supporta fino a **4094 VLAN**, secondo lo standard IEEE 802.1Q.
    - Nuove VLAN possono essere create per:
        - Nuovi reparti o sedi aziendali.
        - Servizi dedicati come **R&D**, gestione eventi o guest Wi-Fi.

Esempio: Creazione di una VLAN per un nuovo reparto:

```
vlan 100
 name Ricerca&Sviluppo
interface vlan 100
 ip address 192.168.100.1 255.255.255.0
```

6. Scalabilità

6.1 Possibilità di Espansione Futura della Rete

La rete è stata progettata per garantire una facile scalabilità, sia in termini di hardware che di configurazioni logiche. Questo approccio consente all'azienda di espandere la rete in base alle esigenze future senza dover apportare modifiche strutturali significative.

Elementi di Scalabilità

1. VLAN e Segmentazione

- La segmentazione logica garantisce che ogni nuovo reparto sia isolato senza impatti sulle VLAN esistenti.

2. Dispositivi di Rete

Switch di Accesso

- Gli switch **Cisco Catalyst 9300-48P-A** supportano fino a 48 porte per endpoint su ogni piano.
- Possono essere impilati con tecnologia **StackWise** per aggiungere ulteriori porte senza modificare le configurazioni esistenti.

Switch di Distribuzione

- Gli switch **Cisco Catalyst 9500-40X** sono predisposti per uplink a **40/100 Gbps**, garantendo capacità sufficiente per supportare nuovi switch di accesso e server.
- Scalabilità lineare grazie alla configurazione in **StackWise Virtual**, che permette di gestire più switch come un'unica unità logica.

Router WAN

- I router **Cisco Catalyst 8500-12X4QC** supportano:
  - Nuove connessioni WAN ad alta velocità.
  - Configurazioni **SD-WAN** per integrazione con cloud o sedi remote.

3. Server e Storage

Server Virtualizzati

- Il server **Dell PowerEdge R750** è configurato con **VMware vSphere**, consentendo la creazione di nuove VM per nuovi servizi aziendali.
- **Espandibilità**:
  - **RAM** fino a 2 TB.
  - **Storage** fino a 32 TB con dischi aggiuntivi.

NAS

- Il **Synology RackStation RS3621xs+** supporta:
  - Espansione dello storage tramite unità aggiuntive.
  - Aggiunta di nuovi volumi per esigenze specifiche di archiviazione.

4. Espansione della WAN

- L’attuale configurazione WAN consente di:
  - Incrementare la larghezza di banda con nuovi moduli di interfaccia ad alta velocità.
  - Aggiungere connessioni secondarie per resilienza o accesso dedicato a cloud.

5. Endpoint e Telefonia VoIP

- La VLAN VoIP (70) è configurata per supportare l’aggiunta di telefoni IP per ogni PC senza necessità di modificare gli switch esistenti.
- Gli switch di accesso forniscono **PoE+**, eliminando la necessità di alimentatori esterni per i dispositivi.

6. Cablaggio e Infrastruttura

- **Uplink in fibra multimodale OM4**:
  - Predisposti per aggiornamenti a velocità di **40/100 Gbps**.
- **Canaline passacavi**:
  - Dimensionate per ospitare un’espansione del 30% rispetto al cablaggio attuale.

- **Rack di rete**:
  - Progettati per ospitare ulteriori apparecchiature senza modifiche strutturali.

Esempi di Espansione

Scenario	Azione Necessaria	Impatto sulla Rete
Nuovo reparto aziendale	Creazione di una nuova VLAN e configurazione IP	Nessun impatto sulle VLAN esistenti.
Incremento degli endpoint	Aggiunta di switch di accesso impilati	Configurazione trasparente tramite StackWise.
Incremento della banda WAN	Aggiunta di interfacce ad alta velocità	Nessun downtime per la rete esistente.
Aumento del numero di server	Nuove VM o espansione hardware server R750	Configurazione lineare senza downtime.

---

7. Cablaggio

7.1 Dettagli sui Cavi Utilizzati (Fibra, Rame)

Il cablaggio è stato progettato per garantire prestazioni elevate, affidabilità e scalabilità futura, utilizzando una combinazione di fibra ottica multimodale OM4 e cavi in rame Cat 6A.

Fibra Ottica

- **Tipo:** Multimodale OM4.
- **Utilizzo:**
  - Uplink tra switch di accesso e distribuzione: Ogni switch di accesso è collegato in fibra agli switch di distribuzione.
  - Collegamenti tra switch di distribuzione e router WAN: Per garantire connettività ad alta velocità.
  - StackWise Virtual sugli switch di distribuzione: Fibra dedicata per il collegamento SVL (StackWise Virtual Link).
- **Vantaggi:**
  - Supporto per velocità fino a 40/100 Gbps su distanze fino a 150 m.
  - Riduzione delle interferenze elettromagnetiche.

Cavi Ethernet

- **Tipo:** Cat 6A.
- **Utilizzo:**
  - Connessioni endpoint: Collegano PC, telefoni VoIP e stampanti agli switch di accesso.
  - Connessioni server e NAS: Cablaggio dedicato verso gli switch di distribuzione.

- **Vantaggi:**
  - Supporto per velocità fino a 10 Gbps su distanze fino a 100 m.
  - Compatibile con **PoE+** per alimentare dispositivi VoIP e access point.

Quantità Stimata di Cablaggio

Elemento	Quantità Stimata	Utilizzo
Fibra Multimodale OM4	300 m	Uplink tra switch e per StackWise Virtual.
Cat 6A Ethernet	600 m	Connessioni endpoint e server.
Patch Panel	6	Terminazione delle connessioni Cat 6A nei rack.
Prese RJ45	300	Per ogni dispositivo endpoint (PC e telefoni VoIP).
Canaline Passacavi	150 m	Distribuite nei piani e nel data center.

7.2 Moduli SFP e Infrastruttura Fisica

Moduli SFP (Small Form-Factor Pluggable)

I moduli SFP sono stati selezionati per garantire compatibilità con la fibra OM4 e supportare le esigenze di velocità e affidabilità.

- **Switch di Distribuzione:**
  - Moduli SFP+ 10 Gbps per uplink tra switch di accesso e distribuzione.
- **Router WAN:**
  - Moduli SFP per interfacce WAN ad alta velocità.
- **Compatibilità:**
  - Tutti i moduli sono compatibili con la fibra ottica multimodale OM4.

Infrastruttura Fisica

La rete è stata progettata con un'infrastruttura fisica ben organizzata per semplificare la manutenzione e supportare eventuali espansioni future.

Rack di Rete:

- **Access Layer:**
  - Ogni piano dispone di un rack dedicato che ospita:
    - Switch di accesso.
    - Patch panel per la terminazione dei cavi Ethernet.

        - Canaline per la gestione dei cavi Cat 6A collegati agli switch.
- **Data Center:**
    - Il data center include due rack ridondanti per ospitare:
        - Switch di distribuzione in StackWise Virtual.
        - Router WAN configurati in HSRP.
        - Firewall Palo Alto PA-5220 in Active/Passive.
        - Server consolidato, server web e NAS.

Canaline Passacavi:

- Installate in ogni piano per contenere i cavi Ethernet e in fibra ottica, mantenendo ordine e riducendo i rischi di danneggiamento.

Prese RJ45:

- Collocate sotto le scrivanie o in prossimità degli endpoint per garantire un accesso comodo e ordinato.

Struttura del Cablaggio

Componente	Caratteristiche	Utilizzo
Fibra Multimodale OM4	Supporto fino a 40/100 Gbps, bassa perdita	Uplink e collegamenti SVL.
Cat 6A Ethernet	Velocità fino a 10 Gbps	Endpoint, server e connessioni PoE+.
Patch Panel	Terminazione ordinata dei cavi Ethernet	Gestione semplificata dei cablaggi.
Rack	Doppio rack ridondante nel data center	Distribuzione, core, server e firewall.
