



BUILD WEEK 1

Progetto rete per la compagnia theta

By NexusMind group

C O N T E N T S

1. Linee Generali

2. Preventivo Rete Aziendale

3. Segmentazione delle rete

4. Struttura della rete

5. Presentazione Rete

6. Possibili criticità e consigli

7. Conclusioni e ringraziamenti

1. LINEE GENERALI

L'azienda Theta ci ha richiesto un preventivo per progettare e strutturare la loro rete aziendale. L'azienda si sviluppa su 6 piani, ad ogni piano ci saranno 20 dispositivi. Il budget massimo che l'azienda ha a disposizione è di 280.000 euro, e tale budget verrà utilizzato per l'acquisto dei dispositivi, e per la mano d'opera.

2.1 PREVENTIVO DISPOSITIVI



WORKSTATION HP Z1 G9

Listino: € 761.65

N. pezzi richiesti: 120

Importo complessivo: € 91.398

*** Periferiche input/output
escluse dal valore di 200
euro cad.***



MSI MAG CODEX 6

Listino: € 1.199

N. pezzi richiesti: 120

Importo complessivo: € 143.880



NAS BUFFALO TERASTATION 7120R

Listino: € 7.519

N. pezzi richiesti: 1

Importo complessivo: € 7.519

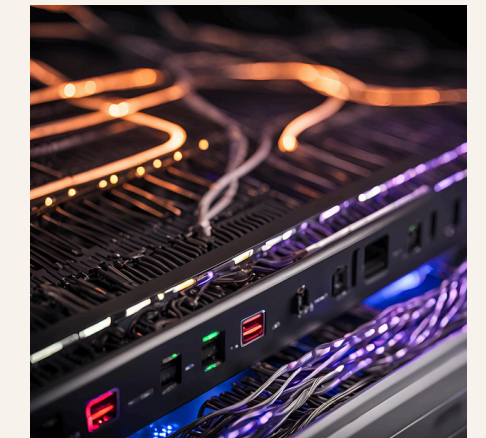


HARDISK SEAGATE IRONWOLF 8TB

Listino: € 198,50

N.pezzi richiesti: 8

Importo complessivo: €1588



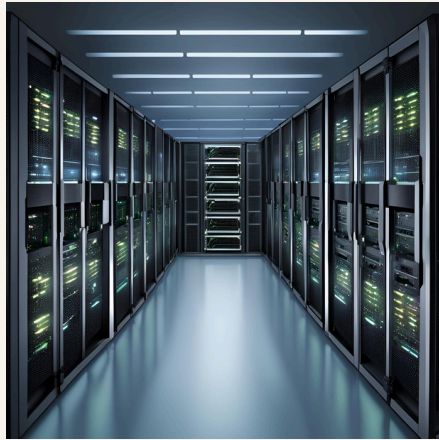
FIREWALL PALO ALTO PA3220

Listino: € 51.680,25

N. pezzi richiesti: 1

Importo complessivo: €
51.680,25

2.2 PREVENTIVO DISPOSITIVI



WEB SERVER DELL POWEREDGE R860

Listino: € 52.500

N. pezzi richiesti: 1

Importo complessivo: € 52.500



SWITCH L3 SWITCH PICOS 1/2.5G

Listino: € 1583,86

N. pezzi richiesti: 2

Importo complessivo: € 3166,52



ROUTER C1117-4P

Listino: € 1063,24

N. pezzi richiesti: 2

Importo complessivo: € 2126,48



IDS/IPS HPE PROLIANT

Listino: € 1.125.78

N. pezzi richiesti: 3

Importo complessivo: € 3377,34



SWITCH L2 S3400-24T4FP (24 PORTE)

Listino: € 535,58

N. pezzi richiesti: 6

Importo complessivo: € 3213,48

2.3 PREVENTIVO DISPOSITIVI

Theta ha bisogno di una serie di dispositivi che possano garantire la connessione verso l'esterno, garantendo anche la sicurezza informatica all'interno dell'azienda.

Ogni singolo dispositivo sarà indispensabile per il buon funzionamento della rete aziendale.

Abbiamo preferito consigliare due scelte diverse per i computer, consigliamo la scelta MSI, in caso l'azienda abbia bisogno di un hardware più prestante dal punto di vista grafico. Tuttavia per ammortizzare il costo complessivo, possiamo certamente optare per un PC HP che soddisfa le necessità dei dipendenti.

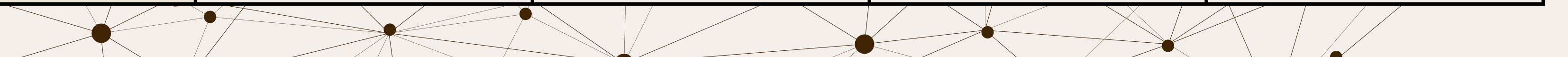
Costo manodopera: € 3100

Costo complessivo con PC HP: € 219.669,07

Costo complessivo con PC MSI: € 272.151,07

3.1 SEGMENTAZIONE DELLA RETE

PIANO E SETTORE	IP NETWORK	IP GATEWAY	IP HOST	IP BROADCAST
0 - Segreteria	192.168.1.0/27	192.168.1.1/27	192.168.1.3/27 192.168.1.30/27	192.168.1.31/27
1 - Marketing	192.168.1.32/27	192.168.1.33/27	192.168.1.34/27 192.168.1.62/27	192.168.1.63/27
2 - Ricerca e Sviluppo	192.168.1.64/27	192.168.1.65/27	192.168.1.66/27 192.168.1.94/27	192.168.1.95/27
3 - Risorse Umane	192.168.1.96/27	192.168.1.97/27	192.168.1.98/27 192.168.1.126/27	192.168.1.127/27
4 - Relazioni Esterne	192.168.1.128/27	192.168.1.129/27	192.168.1.130/27 192.168.1.158/27	192.168.1.159/27
5 - Direzione	192.168.1.160/27	192.168.1.161/27	192.168.1.162/27 192.168.1.190/27	192.168.1.191/27



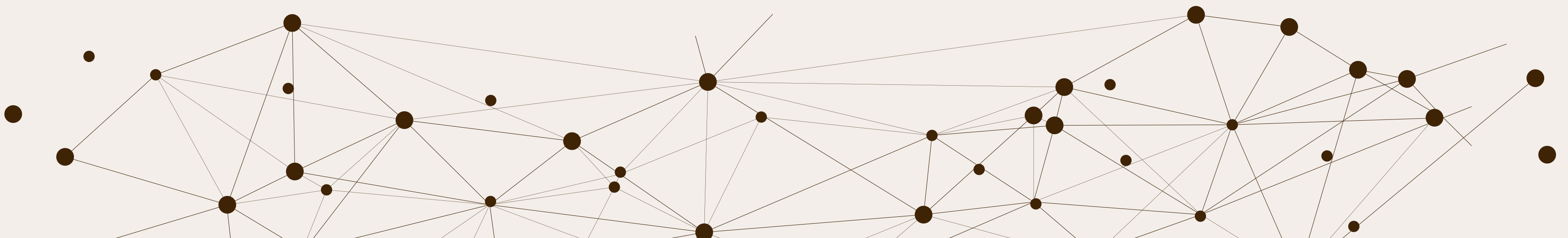
3.2 SEGMENTAZIONE DELLA RETE

L'indirizzo IP privato che abbiamo deciso di utilizzare per l'azienda è di classe C ed è:

192.168.1.0/27. Abbiamo segmentato la rete dividendola in base ai piani che ci sono nel palazzo. A ogni piano della struttura è stato assegnato un settore della azienda e ogni settore grazie al subnetting godrà della propria rete e delle proprie VLAN che andranno a proteggere i computer con dati più sensibili. Nella tabella sotto ci saranno rappresentati gli IP dedicati per la rete di ogni singolo piano.







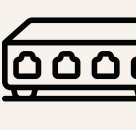


Segmentando la rete con la subnet mask /27 ogni sottorete avrà la possibilità di servire 29 host. Essendo che la richiesta è di 20 host per piano, questa per noi è la soluzione più efficiente. Ogni piano dell'azienda avrà la possibilità di connettere fino a 9 nuovi dispositivi. Se le intenzioni dell'azienda sono quelle di espandersi più velocemente allora il consiglio è di segmentare la rete con una subnet mask /26, in questo modo gli indirizzi IP host di ogni sotto rete salirebbero a 61.

l'IP privato 192.168.1.2/27 è stato riservato al NAS.



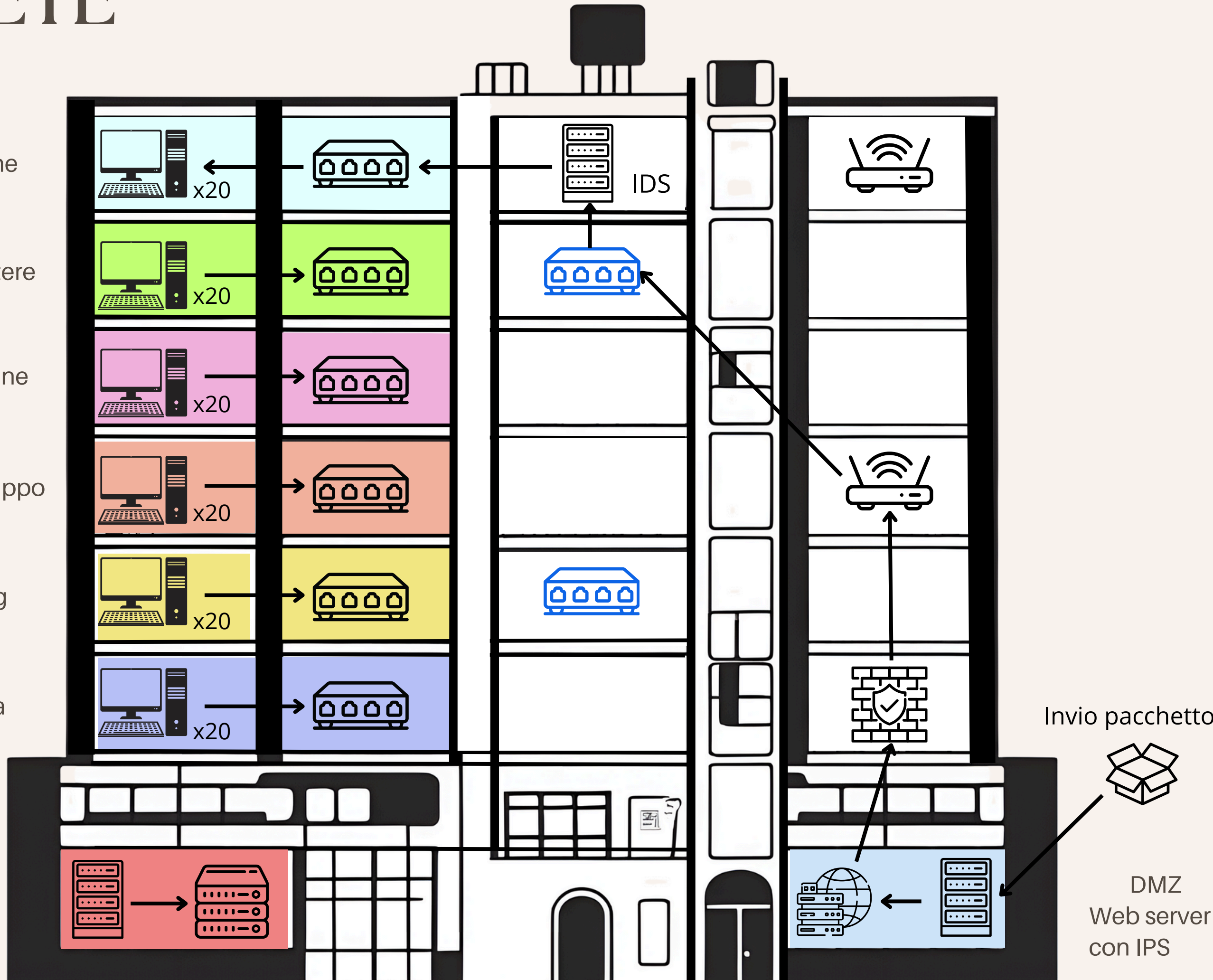
4. STRUTTURA RETE

LEGENDA:

-  • Pacchetto dati
-  • IDS/IPS
-  • Web Server
-  • Firewall
-  • Router gateway
-  • Switch L3
-  • Switch L2
-  • Server NAS
-  • PC

- 6 - Direzione
- 5 - Relazioni estere
- 4 - Risorse Umane
- 3 - Ricerca e Sviluppo
- 2 - Marketing
- 1 - Segreteria

NAS con IDS



5.1 PRESENTAZIONE RETE

Nella pagina precedente vi è una rappresentazione astratta di come la rete verrà strutturata, abbiamo diviso in vari colori ogni sottorete. Anche se in figura viene mostrato un solo PC, importante ricordarsi che in realtà per ogni sottorete ci sono 20 host.

Come si può vedere dalla figura, ogni piano ha uno switch di livello 2 dedicato, a quello switch saranno collegati tutti gli host di quel piano. Ogni piano sarà poi collegato ad uno switch di livello 3 che permetterà la comunicazione tra i vari piani, essendo che i piani sono su reti diverse abbiamo bisogno di uno strumento più intelligente per poterli far comunicare fra loro.

Successivamente ogni switch di livello 3 sarà collegato ad un router gateway che gestirà le connessioni verso l'esterno. Abbiamo scelto l'utilizzo di più dispositivi uguali tra loro per gestire al meglio il carico del lavoro. In modo che ci possano essere un minor numero di guasti o rallentamenti. A Protezione della nostra rete ci sarà un Firewall Perimetrale a filtraggio

dinamico, che non permetterà connessioni dall'esterno a meno che non siano già state avviate prima dall'interno. Ad una porta dedicata del nostro firewall è stata collegata la zona militarizzata.

Piano 6, Direzione

Questo è il piano più isolato e delicato dell'azienda. Per questo motivo subito dopo lo Switch di livello 2 abbiamo deciso di posizionare un IDS (Intrusion Detection System), così che ci possa essere un'analisi approfondita dei pacchetti che entrano all'interno della rete e nel caso di pacchetti malevoli si possa decidere di bloccarli. Abbiamo scelto di utilizzare un IDS in modo da evitare che vengano bloccati anche pacchetti legittimi. Questo piano verrà ulteriormente segmentato con delle VLAN dedicate in modo da proteggere ulteriormente i PC più sensibili. Abbiamo successivamente collegato l'IDS ad uno switch di livello 3 per permettere la comunicazione con gli altri piani, essendo di una rete diversa abbiamo bisogno di un dispositivo che permetta la comunicazione tra reti diverse. Da lì poi se un pacchetto è diretto verso la WAN, il pacchetto andrà verso il router gateway, passerà attraverso il firewall e andrà all'esterno.

Dal piano 1 Segreteria al piano 5 Relazioni Esterne

In questi piani tutti gli host verranno collegati prima ai relativi Switch L2, e poi successivamente gli switch di ogni piano verranno collegati agli Switch L3 che gestiranno le comunicazioni tra i piani o eventualmente verso i router gateway. In questi piani non ci saranno controlli di pacchetti, ma ci saranno comunque VLAN a protezione dei PC più sensibili.

5.2 PRESENTAZIONE RETE

NAS

Il NAS Centralizza l'archiviazione dei dati, permettendo a tutti gli host della rete privata di accedere e salvare file in un'unica posizione sicura. Il NAS è connesso a uno switch dedicato per garantire velocità di accesso e sicurezza attraverso un IDS che monitora il traffico diretto verso di esso. Inoltre gli è stata dedicata una VLAN, in modo che se anche l'attaccante entrasse nella sotto rete Segreteria (di cui il NAS fa parte) ci sia meno possibilità di raggiungerlo. All'interno del NAS abbiamo inserito 8 HardDisk da 8TB l'uno. Per l'archiviazione e la gestione dei dati l'azienda avrà a disposizione 64TB.

Zona Demilitarizzata (DMZ)

In questa zona abbiamo posizionato il Web server dell'azienda.

La DMZ è una rete intermedia tra la rete interna e la WAN, progettata per ospitare servizi che devono essere accessibili dall'esterno, come i server http e smtp. A protezione del Web server abbiamo posizionato un IPS (Intrusion Prevention System). L'ips andrà a controllare tutti i pacchetti in entrata, e bloccherà ogni pacchetto che conterrà codice malevolo. In questo caso potrebbero esserci blocchi di pacchetti anche legittimi ma in ogni caso basterà fare di nuovo richiesta dall'utente esterno e la comunicazione avverrà correttamente.

Il Web server sarà colui che offrirà servizi pubblici come il web hosting accessibili dalla rete esterna. Per questo avrà direttamente un IP pubblico.

6. POSSIBILI CRITICITÀ E CONSIGLI

Essendo che secondo il nostro preventivo è possibile strutturare la rete aziendale con un budget massimo di 273.000,00€, il consiglio è di sfruttare il budget rimanente per andare a contrastare una serie di criticità che si potrebbero presentare.

Criticità numero 1, guasto dei dispositivi

Il primo consiglio è magari di aumentare la quantità di acquisto dei dispositivi come Switch L2/L3 e router gateway. Questi dispositivi gestiscono interamente le comunicazioni interne ed esterne dell'azienda, ed è ottimo avere da parte dei dispositivi pronti all'uso in caso di guasto.

Spesa totale: 12.759€

Criticità numero 2, poca sicurezza nella zona demilitarizzata

Il secondo consiglio è magari di aumentare i dispositivi di sicurezza per la DMZ.

Essendo che questa zona è di libero accesso dall'esterno il consiglio è utilizzare un reverse proxy a protezione del web server. Il Proxy andrà a mascherare l'indirizzo IP del server.

Inoltre ci farà da filtro WAF, quindi ogni singolo pacchetto verrà analizzato più volte prima di essere consegnato al web server e farà anche da router gateway per la zona demilitarizzata. Così facendo alleggeriremo il carico di lavoro del Firewall perimetrale che dovrà solo occuparsi di gestire le connessioni in entrata e in uscita dalla LAN.

Spesa totale: 30.000€

Criticità numero 3, Backup in cloud

Il terzo consiglio è di utilizzare una piattaforma per il backup dei dati in cloud, in questo modo periodicamente (una volta al gg) verrà effettuato un salvataggio delle informazioni, che ci potrà tornare utile ai fini di un guasto al server NAS.

Spesa mensile (varia in base al tariffario del cloud)

7. CONCLUSIONI E RINGRAZIAMENTI

Ringraziamo gentilmente l'azienda Theta per averci commissionato questo lavoro, confidiamo in una risposta positiva, per qualsiasi dubbio o chiarimento il Team è a vostra disposizione in qualsiasi momento.

Cordialmente il team:

NexusMind Group