Milani Francesco - 5^AI
21/05/2020

Descrizione e ristrutturazione di una rete telematica

Nell'anno 2019 ho avuto la possibilità di sostenere un mese di stage, previsto scolasticamente. Sono stato assegnato all'azienda DuoLabs di Bassano Del Grappa, dove ho potuto osservare e studiare la rete telematica aziendale.

Descrizione della rete

I dispositivi presenti di rete sono:

- x1 Switch Multilayer Cisco da 32 porte
- x4 Switch ZYXEL AMG-T10B da 8 porte
- x1 Router Cisco RV320
- x1 Server Dati
- x2 Server Web
- x2 Access Point Wi-Fi
- x10 Computer

La struttura gerarchica prevede lo switch multilayer Cisco al centro che ridistribuisce la connessione ai 3 switch e al server dati.
I 3 switch ZYXEL interconnettono i 6 computer, divisi in 3 per switch, più un computer aggiuntivo per il terzo switch.
Lo switch centrale è connesso per l'accesso a internet al router Cisco, connesso a sua volta all'ISP. Inoltre il router stesso sostiene l'interconnessione con il server web e i 2 Access Point per la connessione WiFi.

La rete è stata strutturata anche a livello logico per una miglior suddivisione degli ambiti lavorativi, con la definizione di 4 VLAN.
Le VLAN sono così suddivise:

- VLAN 1 / Laboratorio : SW1 (PC1-PC2)
- VLAN 2 / Programmazione 1 : SW2 (PC3-PC4-PC5)
- VLAN 3 / Programmazione 2 : SW3 (PC6-PC7-PC8)
- VLAN 4 / Segreteria-Presidenza : SW4 (PC9-PC10)

I dispositivi Wi-Fi, ovvero:

- x6 Smartphone
- x5 Tablet
  Sono tutti connessi tramite DHCP senza IP statici, quindi non presentano alcun problema da quel punto di vista.

Problematiche e risoluzioni

La prima problematica emerge al momento di una connessione da parte di dispositivi ospiti, che viene fatto connettere alla rete WiFi aziendale.

Data la mancanza di una rete ospiti predisporrerei l'aggiunta di una VLAN (5), acquistando un ulteriore Access Point, aumentandone quindi il numero a 3.

L'Access Point verrà collegato al Router, ma per ovviare ad altri problemi, come dagli attacchi miranti allo stato della rete provenienti dall'esterno, provvederei a creare una DMZ, così da poter posizionare in quella zona sia l'Access Point per gli ospiti, sia il Server Web.

Risolto il problema della rete ospiti, sarà necessario proteggere la rete anche da attacchi su rete locale.
Per questo il posizionamento di un firewall diventa necessario.

Andrò ad acquistare un'apparecchiatura Cisco Small Business Pro SA 540, che corrisponde alle caratteristiche dell'azienda, essendo progettato per aziende con meno di 100 dipendenti, unendo in un device all-in-one le funzionalità di firewall, VPN e sicurezza per e-mail e WEB.

Il device andrà posizionato dopo il Router, sulla connessione per l'ISP, in modo da poter bloccare la totalità degli attacchi e per poter mantenere sicura la nostra rete.

Andrei inoltre a posizionare un apparecchio minore, come un router Cisco 886, programmandolo in modalità di firewall. Andrebbe posto nella connessione tra DMZ e router principale, così da poter essere un ulteriore schermo tra la zona demilitarizzata e il nostro router principale.

Concludo la mia relazione sottolineando come la rete fosse già solida in precedenza, ma con l'apporto di piccole modifiche è migliorata sotto gli aspetti di sicurezza e stabilità.