Progettazione e configurazione di una rete aziendale

Arianna Masciolini, Claudio Pannacci

7 gennaio 2018

Indice

1 Requisiti e soluzioni proposte

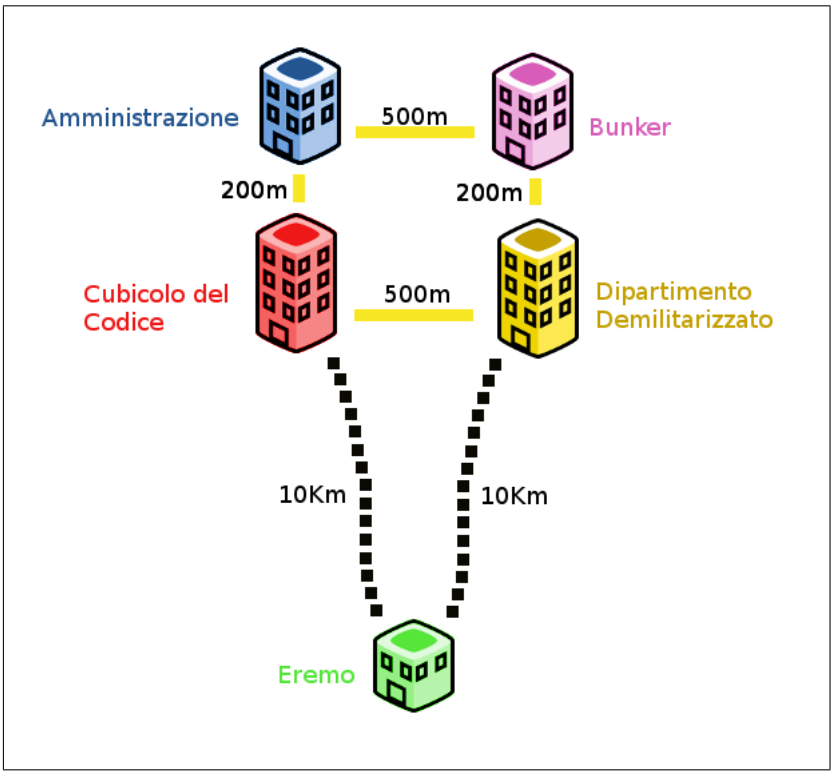

Figura 1: Pianta degli edifici della ditta.

Scopo di questo lavoro sono la progettazione e la configurazione di una rete per conto di una azienda che lavora in ambito informatico. Gli edifici sono dislocati come mostrato in figura e sono richiesti l'accesso protetto ad internet, copertura WiFi nell'edificio D, un server di posta elettronica, un server web, due server DNS, un server proxy, uno di backup ed un server per applicazioni aziendali, da proteggere con particolare attenzione.

Nome edificio	**Numero utenti**	**Server**
Amministazione	100	DNS
Bunker	100	Backup
Cubicoli del Codice	260	Appl. aziendali
Dipartimento Demilitarizzato	240	DHCP, DNS, Web, Mail, Proxy
Eremo	50	-

Tabella 1: Riepilogo.

2 Schema logico della rete

La topologia della rete rispecchia a grandi linee lo schema fisico della stessa. In particolare, a ogni edificio corrisponde un'area del protocollo OSPF, contrassegnata da un colore specifico. Tra queste, l'unica area non corrispondente ad un edificio è, ovviamente, l'area di backbone, che coincide con la sottorete 192.168.0.0/24 e contiene un router per ogni edificio. Il router rappresentato al di fuori dell'area di backbone è un exterior router finalizzato al collegamento con Internet.

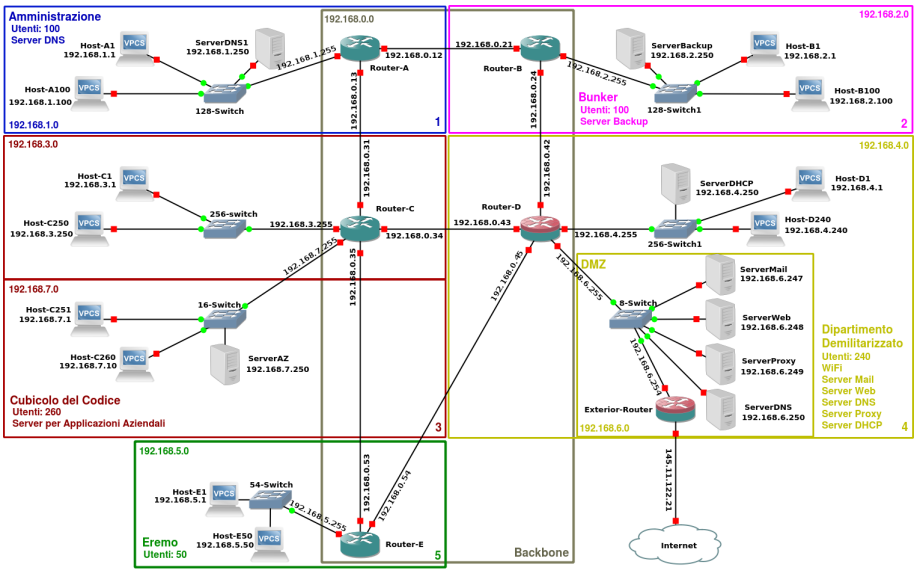

Figura 2: Schema logico.

Collegamenti I quattro edifici più vicini tra loro (A, B, C, D) sono collegati da un anello di fibra ottica, in modo da garantire un servizio veloce ed affidabile. Per motivi economici, non è stato possibile adottare la stessa soluzione per l'edificio E: quest'ultimo è connesso ai restanti tramite VPN (Virtual Private Network), sfruttando le reti pubbliche senza compromettere la sicurezza.

2.1 Edificio A: Amministrazione

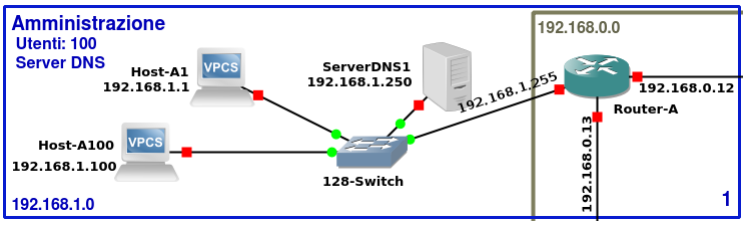

Figura 3: Dettaglio area 1.

L'edificio Amministrazione è il quartier generale dell'azienda, ospita uffici e segreterie. Qui è collocato il server DNS interno, che facilita l'accesso ai dispositivi della rete. Visto il numero non troppo elevato di utenti, a quest'area è assegnata una sola sottorete, la 192.168.1.0/24.

2.2 Edificio B: Bunker

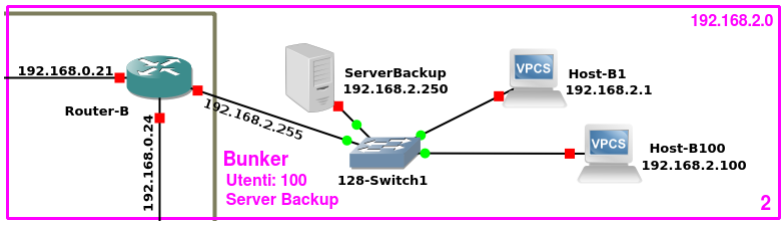

Figura 4: Dettaglio area 2.

L'edificio B, soprannominato Bunker, contiene il server di Backup. La sua sottorete è la 192.168.2.0/24.

2.3 Edificio C: Cubicoli del Codice

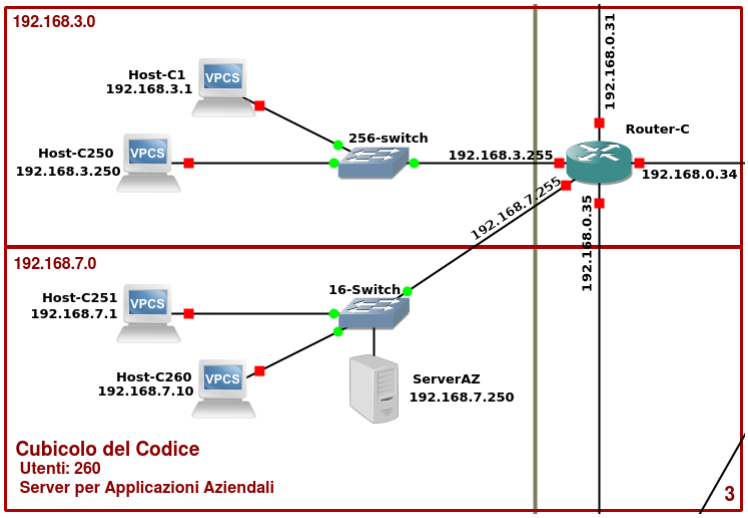

Figura 5: Dettaglio area 3.

Fra gli edifici più articolati il blocco dei Cubicoli del Codice, reparto di sviluppo software. Gli sviluppatori si connettono alla sottorete 192.168.3.0/24 tramite i terminali aziendali. Il server per applicazioni aziendali, gestito solo da pochi sistemisti per ragioni di sicurezza, si trova in una zona separata, corrispondente alla sottorete 192.168.7.0/24.

2.4 Edificio D: Dipartimento Demilitarizzato

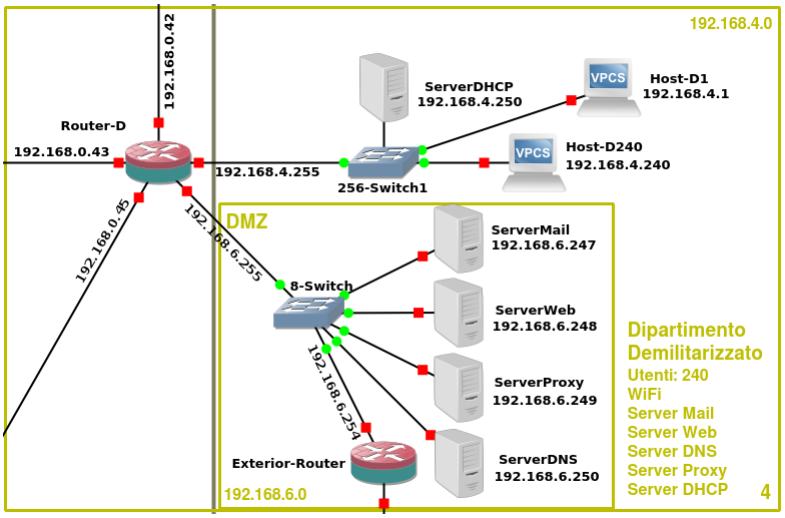

Figura 6: Dettaglio area 4.

Secondo per numero di utenti, il Dipartimento Demilitarizzato è la zona dedicata alle attività promozionali dell'azienda. Fra le principali, il mantenimento del sito web `disditta.it`, hostato dal server web presente nella DMZ. Quest'ultima, corrispondente alla sottorete 192.168.6.0/24 ospita anche numerosi altri server (il server di posta, il server proxy e il server DNS esterno) e l'exterior router: tutto quel che riguarda i servizi Internet offerti e utilizzati dall'azienda.
La sottorete dedicata al personale è invece la 192.168.4.0/24. Poiché per questa zona è stata richiesta la copertura WiFi, gli indirizzi IP vengono assegnati dinamicamente dal server DHCP ivi collocato.

2.5 Edificio E: Eremo

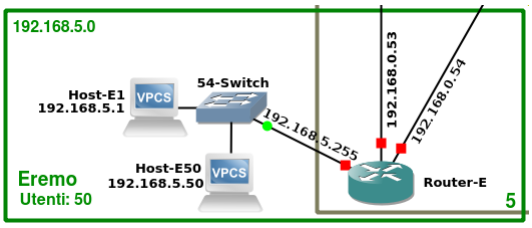

Figura 7: Dettaglio area 5.

La sede legale della ditta, ribattezzata Eremo, conta solo cinquanta utenti e pertanto la sua struttura è particolarmente semplice.

3 Routing

Siccome le sottoreti degli edifici hanno una topologia a stella, per tutti i dispositivi eccetto i router nell'area di backbone, il routing è statico. Sui router interni gira invece il protocollo OSPF, che permette di associare ad ogni edificio un'area, gestibile indipendentemente dalle altre. In prospettiva, ciò potrebbe tornare utile nel momento in cui, a livello di un singolo edificio, si decidesse di adottare una topologia di rete differente dall'attuale.

4 DNS

I due server DNS soddisfano due esigenze differenti.
Il primo, posto nella DMZ, traduce in nomi gli indirizzi dei server cui si accede dall'esterno, ad esempio il server web. Questo è essenziale per la presenza online dell'azienda.
Il secondo permette di accedere più comodamente alle varie macchine in rete e si rifà al precedente per quel che riguarda i server della DMZ.

5 Misure di sicurezza

5.1 Firewall

Per soddisfare gli standard minimi di sicurezza, si è scelto di adoperare due firewall distinti, configurati tramite `iptables`, integrati nei due router del Dipartimento Demilitarizzato. Grazie ad essi, la DMZ risulta protetta sia dagli accessi provenienti dalla rete locale che da quelli esterni. Il firewall collocato tra la rete locale e la DMZ filtra i pacchetti che queste due porzioni di rete si scambiano tramite due catene di regole (`dmzlan` e `landmz`) e funge da NAT. Analogamente, il firewall esterno si serve delle due catene `inetdmz` e `dmzinet` per effettuare il packet filtering tra Internet e la DMZ.

5.2 Hardening: il server per applicazioni aziendali

La sicurezza del server per applicazioni aziendali è stata rafforzata filtrando i pacchetti TCP con un wrapper e facendovi girare il superserver `xinetd`, che a sua volta monitora le richieste ai servizi telnet, SSH e NFS talvolta, come nel caso di telnet, disabilitandoli completamente.

5.3 Monitoraggio della rete

Oltre a raccomandare ai futuri sistemisti di eseguire manualmente i comandi canonici (`ping`, `ifconfig`, `dig`, `netstat`, `tracepath`...), per agevolare il monitoraggio della rete si consiglia di utilizzare il protocollo SNMP.

6 Preventivo di spesa

Assumendo che l'azienda sia già in possesso dei server e di tutti i terminali, il costo delle varie componenti hardware è riportato in tabella.

Componente	**Quantità**	**Prezzo cad.**	**Prezzo tot.**
Router CISCO 4331 ISR	5	1100 $	5500 $
Router CISCO ASR 1001	1	5630 $	5630 $
Modulo fibra	4	40 $	160 $
Switch CISCO SG300-52p	15	775 $	11325 $
Switch CISCO SG300-28p	4	355 $	1420 $
Ubiquiti Networks Unifi WiFi access point	1	130 $	130 $
Fibra ottica	1400 m	6.34 $/m	8876 $
Cavo UTP	3000 m	2.65 $/m	7950 $
VPN		300 $ annui	300 $ annui
		TOTALE:	**41291 $**
		TOTALE (EUR):	**34323 EUR**

Tabella 2: Costo delle componenti hardware

Al costo della componentistica va sommato il costo dell'installazione, pari a 20.000 euro, per un totale complessivo di 54.323 euro.