

Rapporto:

Il progetto è composto da 3 zone diverse: zona interna attendibile per i dipendenti (INSIDE), zona demilitarizzata parzialmente attendibile per utenti interni ed esterni (DMZ) e zona esterna non attendibile per servizi/utenti pubblici (OUTSIDE).

Nella zona interna ci sono 6 piani. Ogni piano rappresenta una subnet e su ogni piano ci sono 20 PC. C'è anche un server NAS situato nella zona interna. A ogni PC viene assegnato un indirizzo IP dinamico tramite server DHCP nella zona demilitarizzata. Il server NAS utilizza un indirizzo IP statico.

Nella zona demilitarizzata ci sono 2 server connessi a uno switch: server WEB e server DHCP. Entrambi hanno un indirizzo IP statico. Il server WEB è responsabile di DVWA, mentre il server DHCP è responsabile dell'assegnazione di indirizzi IP dinamici ai PC nella zona interna.

Nella zona esterna, potrebbero esserci molti utenti, in realtà server. Ma in questo caso l'ho progettata come 2 utenti pubblici (1 PC e 1 laptop) e un server Google.

Tutte queste zone sono collegate tramite un router centrale, un Internet Service Provider e un firewall. Ogni dispositivo ha usi specifici. Il router centrale ha 8 interfacce. Sono collegati 6 switch e 1 server NAS. L'ultima interfaccia è utilizzata per connettersi al firewall.

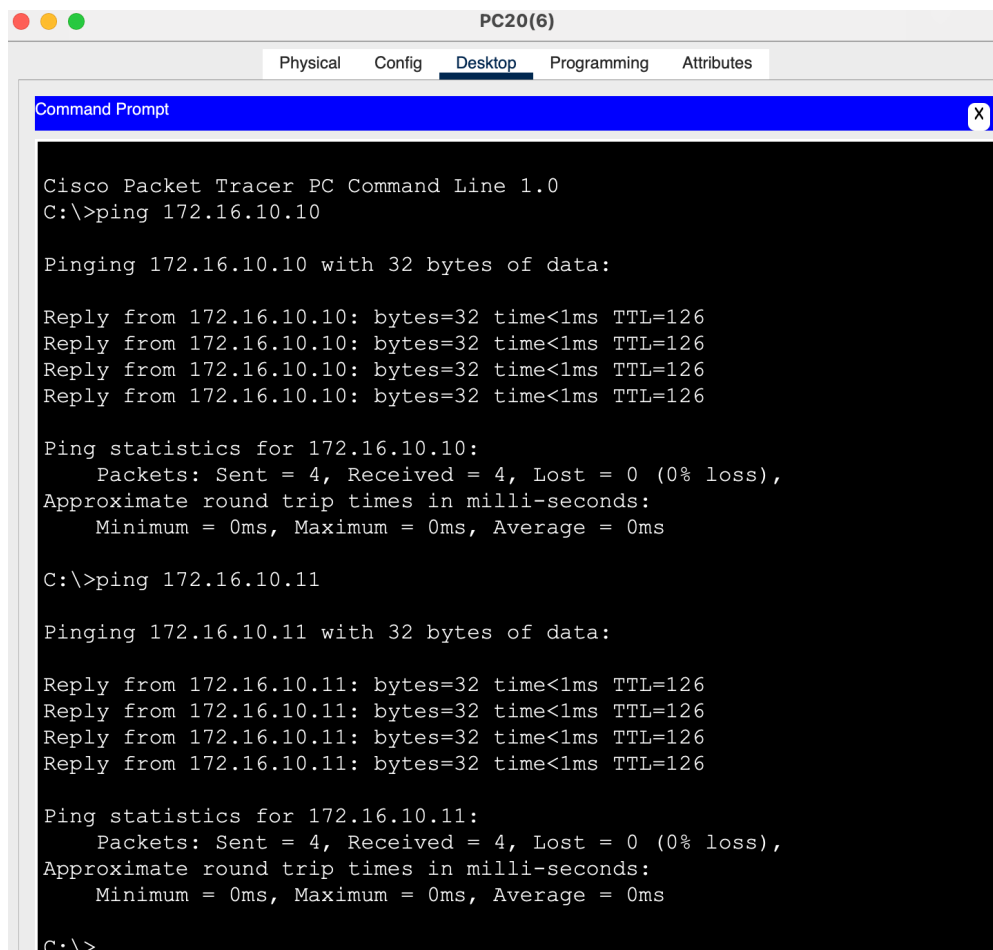
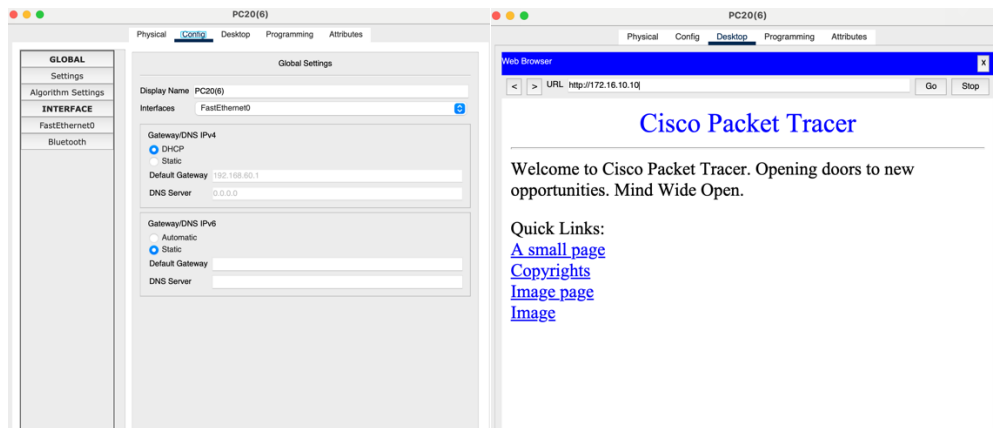
Le interfacce tra il router centrale e il firewall utilizzano l'IP di rete 10.10.10.0/30. Le 3 interfacce del firewall sono in stato attivo. La prima è collegata al router centrale, la seconda all'ISP e l'ultima interfaccia allo switch in DMZ. L'IP di rete tra le interfacce firewall e ISP è 20.20.20.0/30 e l'IP di rete tra le interfacce firewall e DMZ è 172.16.10.0/28. Internet Service Provider (ISP) è descritto come un router, fornisce un accesso tra gli utenti/server nella zona esterna e altre zone. L'IP di rete tra le interfacce dell'ISP e la zona esterna è 8.8.8.0/24.

NAT è stato configurato per modificare gli indirizzi IP









Tutti – router centrale, firewall, ISP sono stati configurati per OSPF, in modo che ogni dispositivo abbia familiarità con diverse subnet. Alcune interfacce nel router centrale sono configurate con l'indirizzo IP helper del server DHCP, in modo che i PC interni sappiano dove comunicare per ottenere indirizzi IP dinamici.

Il firewall nega tutte le richieste di default. Quindi ho configurato il firewall per consentire a zone specifiche di comunicare tra loro tramite comandi ACL

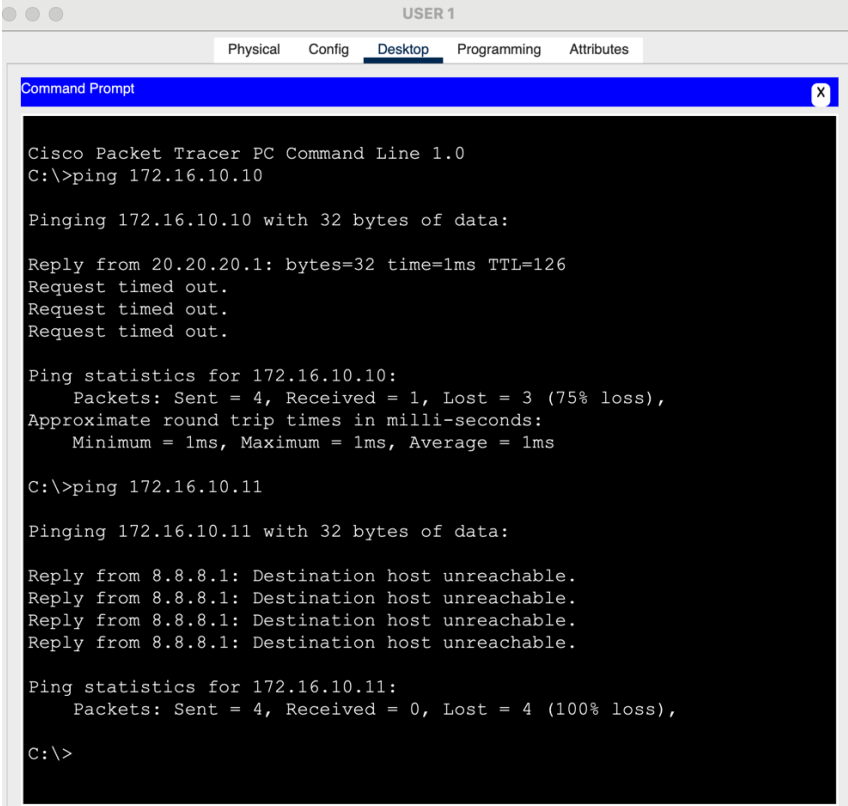
La zona interna può comunicare con DMZ totalmente. In modo che abbia accesso al server web tramite porte 80 e 443 e possa effettuare il ping di entrambi i server. Di seguito alcune figure che mostrano una comunicazione tra un PC interno e una zona DMZ:



Ho configurato il firewall in modo tale che la zona interna possa comunicare solo con il server nella zona esterna. In modo che gli utenti pubblici non abbiano accesso a subnet attendibili:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC20(6)	Google Server	ICMP		0.000	N	0
	Successful	Google...	PC20(6)	ICMP		0.000	N	1
	Failed	PC20(6)	USER 1	ICMP		0.000	N	2
	Failed	USER 2	PC20(6)	ICMP		0.000	N	3

Il firewall è configurato in modo tale che la zona esterna possa comunicare solo con il server WEB. Non ha accesso al server DHCP. Nella figura sottostante possiamo osservare la comunicazione. L'errore Request timed out dovrebbe verificarsi a causa della mancanza di rendering del software Cisco, ma l'errore host unreachable ovviamente ci dice che c'è una restrizione nel firewall:



```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.10.10

Pinging 172.16.10.10 with 32 bytes of data:

Reply from 20.20.20.1: bytes=32 time=1ms TTL=126
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.10.10:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 172.16.10.11

Pinging 172.16.10.11 with 32 bytes of data:

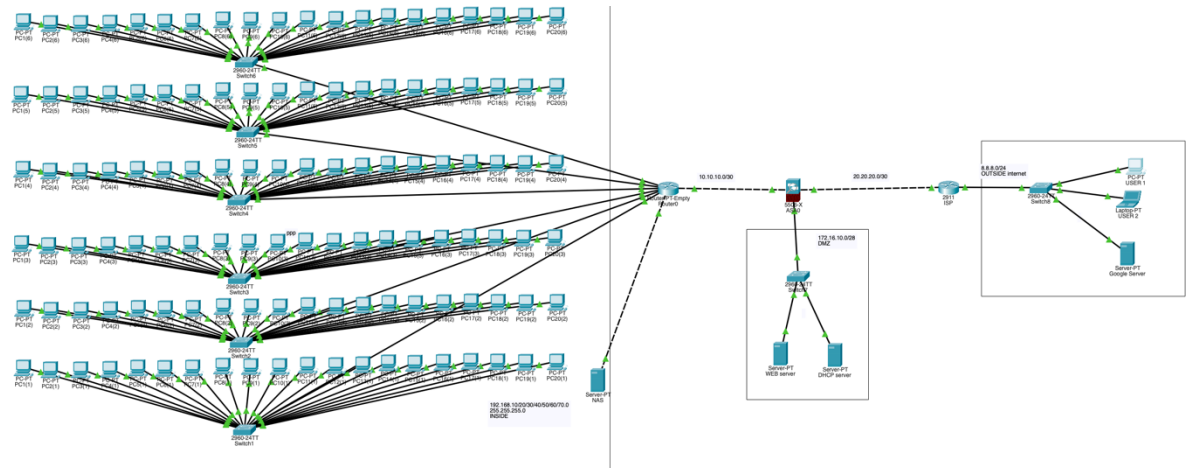
Reply from 8.8.8.1: Destination host unreachable.
Reply from 8.8.8.1: Destination host unreachable.
Reply from 8.8.8.1: Destination host unreachable.
Reply from 8.8.8.1: Destination host unreachable.

Ping statistics for 172.16.10.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>

```

Il progetto Cisco è completo:



Tutte le altre informazioni sono accessibili nel file `progettomain` finale.pkt: come la configurazione OSMF, la configurazione NAT, access-lists, access-groups e così via scrivendo il comando `show start` nella CLI di ciascun dispositivo corrispondente