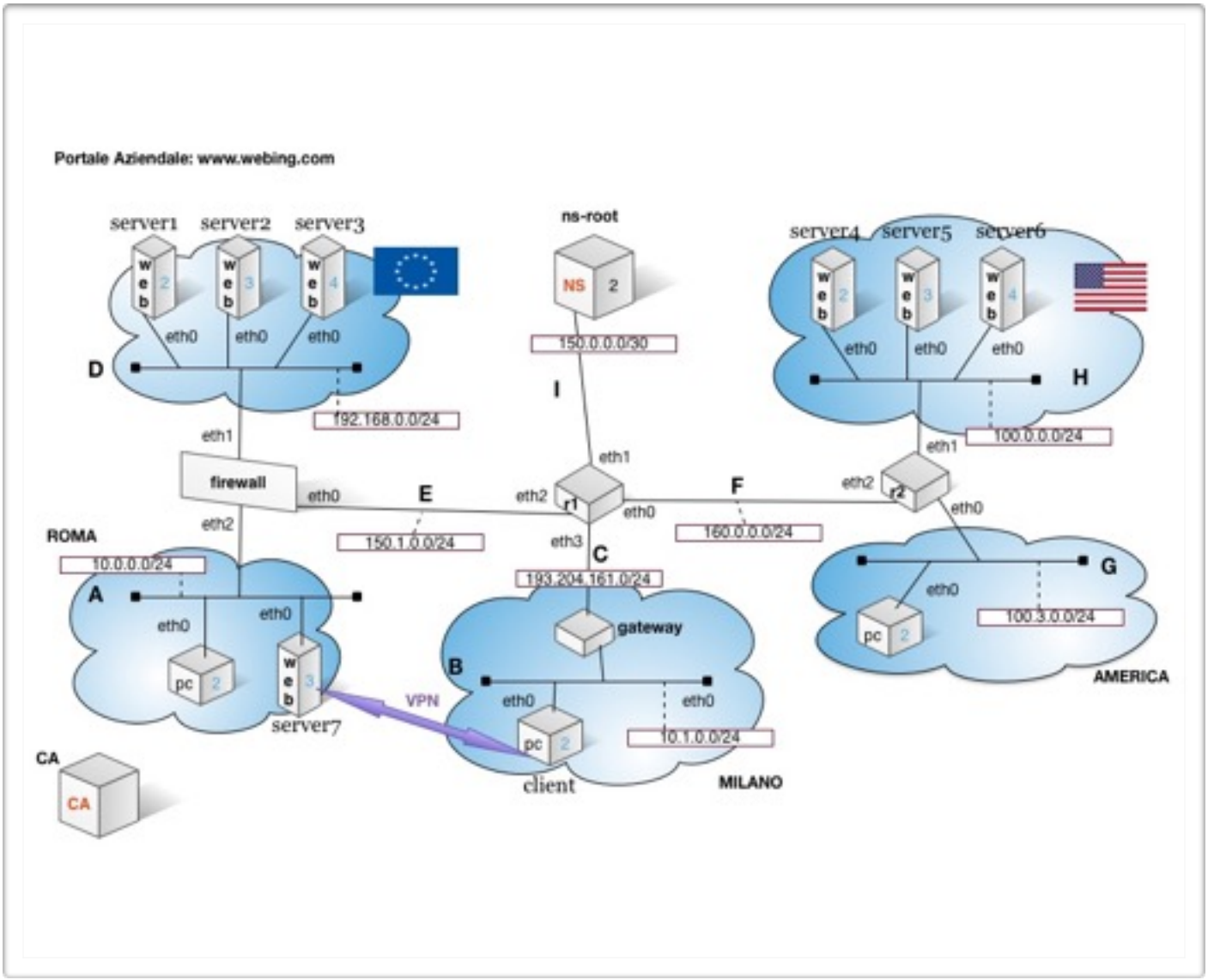
Proposta progetto

Azienda americana di servizi Web



Indirizzamento interno privato

Le filiali di Roma e Milano sono connesse. Come da specifiche, entrambe le reti hanno un indirizzamento interno privato, al fine di estendere il numero di hosts interni qualora fosse necessario.

NAT

I servizi pubblici offerti dalle due reti sono filtrati dal NAT. Attivando il **full-cone** si ha un'associazione completa e totale tra l'indirizzo interno dell'host e l'indirizzo pubblico, fornito dal dispositivo incaricato di effettuare le operazioni di NAT. In altre parole, la traduzione di indirizzo viene effettuata in modo incondizionato sia verso l'interno che verso l'esterno, consentendo dunque di contattare un host presente nella rete interna a condizione di conoscerne l'indirizzo IP pubblico, determinato e assegnato proprio dalla periferica che esegue il NAT. Tale scelta riduce la necessità di configurazione del dispositivo, a prezzo però di un minore filtraggio nei confronti di pacchetti che giungono dall'esterno.

Routing

Come protocollo routing si è scelto il RIP (*Routing Information Protocol*) di tipo distance vector. La rete ha una natura ibrida ed è composta da uno spazio gestito da routing dinamico e una zona con routing statico. Questa tipologia è stata scelta per rappresentare un rete reale, dove vengono generalmente usati più tipi di routing.

Web

L'azienda offre servizi web all'indirizzo www.webing.com (portale aziendale). Il servizio supporta un *load-balancing* su base geografica, quindi le richieste provenienti dall'America (IP = 100.3.0.0/24) sottostanno a un *redirect* verso la sede americana, mentre le richieste provenienti dall'Europa (IP = 193.204.161.0/24 e IP = 150.1.0.0/24) sono reindirizzate al server europeo.

Per la sede americana è stata implementato un *load-balancing* di tipo **round robin** per i server, al fine di ottimizzare il carico in entrata. Al contrario, per la sede europea, è stato implementato un *load-balancing* di tipo **random**, perché su questa filiale è previsto un carico minore.

Vpn

Sul PC di Milano si può accedere al *server7* presente nella sede di Roma grazie a una VPN configurata *adhoc*. Il software ***openvpn*** è stato installato sul client e sul server con interfacce virtuali rispettivamente: *tuno* ip 10.8.0.1 lato server e *tuno* ip 10.8.0.6 lato client. I certificati del server e del client, presenti nelle rispettive cartelle *server7 :* /etc/openvpn/2.0/keys e pcm/etc/openvpn/2.0/keys, sono stati precedentemente firmati dalla CA (Certification Authority), vista nel progetto come unità indipendente dalla rete.

Firewall

La rete di Roma è protetta da un Firewall, quindi solo alcune connessioni sono permesse. Per consultare le connessioni autorizzate vedere il file **firewall.startup**, nel quale sono specificate le singole regole. Qui di seguito è riportata una tabella riepilogativa:

from host	to host	IP host	autorizzato
PC Roma	server1	192.168.0.2	yes
PC Roma	server4	100.0.0.2	yes
PC Milano	PC Roma	150.1.0.2	yes
PC Milano	server1	150.1.0.12	yes
PC America	PC Roma	150.1.0.2	yes
PC America	server1	150.1.0.12	yes
server1	server4	100.0.0.2	no
server1	PC Roma	10.0.0.2	no

TABELLA DEL NAT

	Private IP	Public IP
server1	192.168.0.2	150.1.0.12
server2	192.168.0.3	150.1.0.13
server3	192.168.0.4	150.1.0.14
server7	10.0.0.3	150.1.0.3
PC roma	10.0.0.2	150.1.0.2
PC milano	10.1.0.2	193.204.161.2

TABELLA TEST

	script
set nat type	./set_nat_type
ping from usa	./ping_roma_milano
ping from roma	./ping_milano_america
ping from milano	./ping_roma_america
test load balancing	./test_load_balancing