Introduzione al NATTING

I Router CISCO sono in grado di svolgere funzioni proprie di un firewall, in particolare possono effettuare la trasformazione degli indirizzi IP PRIVATI usati dai pc della rete aziendale in indirizzi IP PUBBLICI per poter trasmettere pacchetti in Internet.

Questa operazione si chiama NAT = NETWORK ADDRESS TRANSLATION

Essa consente di utilizzare indirizzi IP PRIVATI nella rete aziendale e di avere un solo indirizzo IP PUBBLICO assegnato all'interfaccia del Router rivolta verso l'esterno; addirittura tale indirizzo IP potrebbe essere assegnato dinamicamente dall' Internet Provider.

In alcuni casi l'azienda potrebbe aver acquistato un piccolo pool di indirizzi IP PUBBLICI, come ad esempio la sottorete 212.1.1.0/29 costituita da 6 indirizzi IP validi.

L'utilizzo di indirizzi IP Privati all'interno dell'azienda non comporta solo un vantaggio economico, peraltro considerevole (si potrebbero risparmiare alcune centinaia di euro al mese) ma agisce in favore della SICUREZZA!

Infatti, i pc con indirizzo IP PRIVATO non sono direttamente accessibili dall'esterno in quanto essi risultano del tutto invisibili in Internet. E' per questo motivo che talvolta l'operazione di NATTING viene anche detta "masquerading", nel senso che essa consente di mascherare gli indirizzi dei pc della rete.

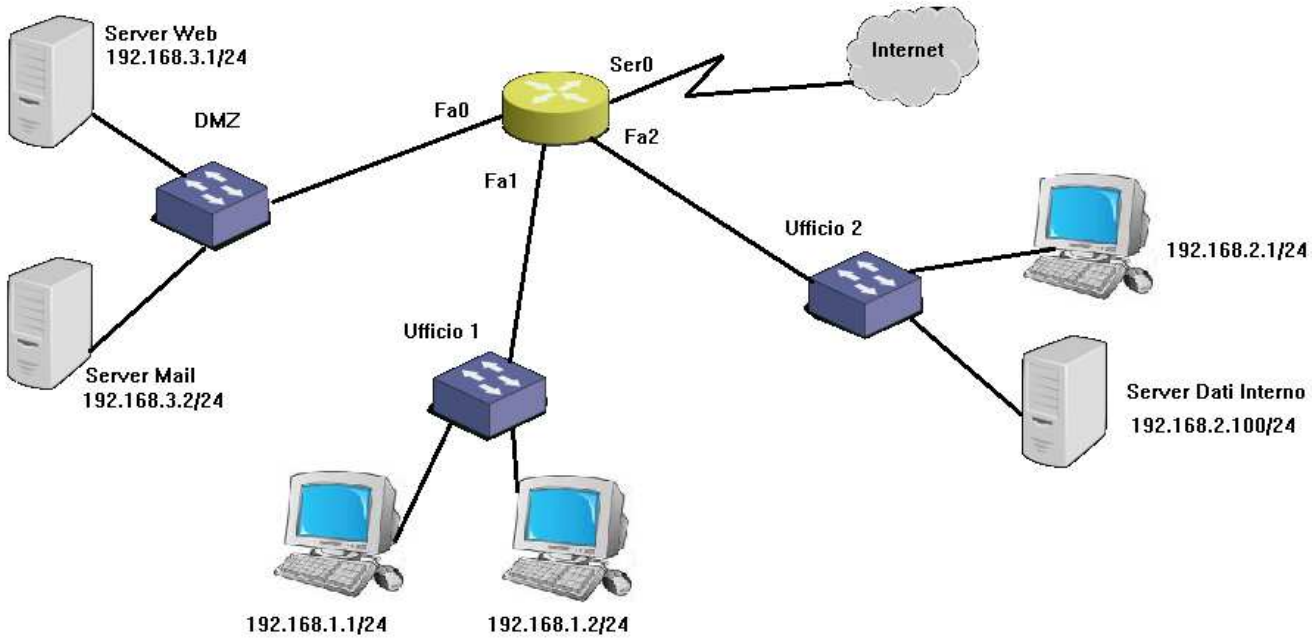
La terminologia CISCO distingue gli indirizzi IP usati nell'operazione di NATTING:

- inside local = indirizzo privato del mittente interno (invisibile in Internet)
- inside global = indirizzo pubblico associato al mittente interno (visibile in Internet)
- outside local/global = indirizzo di destinazione in Internet (pubblico)

Si distinguono le seguenti tipologie di NATTING:

- NAT OVERLOAD (detto anche Port Address Translation) ➔ usato per far uscire in Internet i pc della rete aziendale: tutti i pacchetti escono con mittente l'indirizzo IP Pubblico del Router e un port number identificativo assegnato dal Router stesso
- STATIC NAT ➔ usato per assegnare ai server della DMZ aziendale un indirizzo pubblico con il quale essi sono visti in Internet
- PORT FORWARDING ➔ una variante del NAT Statico che si usa per assegnare ai server della DMZ aziendale l'unico indirizzo IP pubblico del Router. In pratica per Internet è come se fosse il Router la sede dei vari server aziendali.

Per esemplificare la configurazione dei diversi tipi di NAT si considera la seguente tipica rete aziendale:



Tipica rete aziendale con indirizzi IP Privati e con rete DMZ

NAT OVERLOAD

Si vogliono far uscire in Internet tutti i pc della rete aziendale: il Router fungerà come da "prestanome" per i vari pc in quanto tutti i pacchetti inviati in Internet avranno come mittente il Router stesso.

Si supponga che l'interfaccia Ser0 del Router abbia l'indirizzo IP pubblico 212.1.1.1 / 30

Il Router mantiene una tabella dinamica con le corrispondenze tra gli indirizzi IP + porta del pc mittente (inside local) e gli indirizzi IP + porta con cui questi pacchetti usciranno in Internet (inside global).

Se ad esempio il browser del pc 192.168.1.1 manda una richiesta al server web 209.165.201.1 si ha nella suddetta tabella delle traduzioni (nat table):

Inside local	Inside global	Outside
192.168.1.1 : 5008	212.1.1.1 : 5008	209.165.201.1 : 80

Tale tabella può essere visualizzata con il comando:

R# show ip nat translations

Quando arriva un pacchetto da Internet, il Router consulta la suddetta tabella e lo reindirizza di conseguenza al vero destinatario dentro la rete aziendale.

Il Router associa un numero di porta al proprio indirizzo IP pubblico per poter distinguere i diversi traffici di pacchetti in essere: se possibile riprende il numero di porta usato dal mittente, oppure ne mette uno diverso per evitare doppioni e ambiguità.

La seguente tabella mostra come alcuni numeri di porta siano stati opportunamente cambiati:

Inside local	Inside global	Outside local/global
192.168.1.1 : 5008	212.1.1.1 : 5008	209.165.201.1 : 80
192.168.2.2 : 4590	212.1.1.1 : 4590	209.165.201.1 : 80
192.168.2.2 : **5008**	212.1.1.1 : **5009**	209.165.202.129 : 443

I dati di questa tabella sono dinamici: essi rimangono validi solo finché c'è un traffico attivo con un corrispondente in Internet, dopodiché essi vengono rimossi al trascorrere del tempo previsto per il timeout (per default dopo 24 ore).

Il Router ha a disposizione 65535 possibili valori per i numeri di porta (si usano 16 bit), che vengono via via riutilizzati per i diversi traffici di pacchetti.

I comandi di configurazione per il router prevedono innanzitutto che si definiscano le interfacce interne (inside) e quella/e esterne (outside)

```
R(config)# interface Fa0
R(config-if)# ip nat inside
R(config)# interface Fa1
R(config-if)# ip nat inside
R(config)# interface Fa2
R(config-if)# ip nat inside
R(config)# interface Ser0
R(config-if)# ip nat outside
```

Si prosegue con la definizione di una access-list che elenchi gli indirizzi IP dei pc che potranno usufruire del servizio NAT

```
R(config)#  access-list  1 permit  192.168.0.0  0.0.255.255
```

Poi si attiva il servizio di NAT specificando la lista sorgente e l'interfaccia di uscita, di cui si acquisirà l'indirizzo IP

```
R(config)# ip  nat inside  source list 1  interface Ser0  overload
```

STATIC NAT

Per rendere raggiungibili dall'esterno i server della DMZ aziendale, gli si deve associare in modo statico un indirizzo IP pubblico.

Si suppone di avere a disposizione la rete 212.1.1.0 / 29 che consta di 6 indirizzi IP validi, dal 212.1.1.1 al 212.1.1.6.

Se si decide di dividere in due tale rete, si ottengono le sottoreti 212.1.1.0 / 30 e 212.1.1.4 / 30.

La prima può essere usata per assegnare i due indirizzi IP validi al link con il provider (l'interfaccia Ser0 del proprio router e la corrispondente interfaccia seriale del router dell'Internet Provider) e la seconda per la DMZ, dove però un indirizzo IP viene assegnato all'interfaccia Fa0 del router e **rimane un solo indirizzo IP per un unico server**!

In alternativa, la tecnica del natting consente di **sfruttare appieno i 6 indirizzi IP pubblici a disposizione**: 2 vanno al link con il provider e gli altri 4 ad altrettanti server della DMZ.

Si parla di NAT STATICO in quanto vengono fissate delle corrispondenze biunivoche tra indirizzi privati assegnati ai server e indirizzi pubblici con cui essi verranno resi accessibili dall'esterno.

Il NAT STATICO ha anche il vantaggio di lasciare ampia flessibilità di collocazione dei server nelle diverse LAN dell'azienda ferma restando l'assegnazione agli stessi degli indirizzi ip pubblici.

I comandi di configurazione per il server web e il server mail sono rispettivamente:

R(config)# ip nat inside source static 192.168.3.1 212.1.1.3
R(config)# ip nat inside source static 192.168.3.2 212.1.1.4

Avendo assegnato all'interfaccia Ser0 l'indirizzo IP 212.1.1.1 e all'interfaccia del router del provider 212.1.1.2.

Anche per il nat statico si devono specificare le interfacce coinvolte del router se sono inside oppure outside:

R(config)# int Fa0
R(config)# ip nat inside

R(config)# int Ser0
R(config)# ip nat outside

La tabella delle corrispondenze di indirizzi conterrà le seguenti informazioni fisse:

Inside local	Inside global	Outside local/global
192.168.3.1	212.1.1.3	---
192.168.3.2	212.1.1.4	---

PORT FORWARDING

Si tratta di un'altra forma di NAT STATICO che si avvale di un unico indirizzo IP, quello assegnato al router, per poter accedere dall'esterno ai diversi server della DMZ.

Questa tecnica prevede di identificare ciascun server mediante un apposito numero di porta, fisso!

Qualora l'indirizzo IP della interfaccia Ser0 del router fosse 212.1.1.1, si assocerebbero al server web gli indirizzi 212.1.1.1 : 80 e 212.1.1.1 : 443 e al server mail gli indirizzi 212.1.1.1 : 25 e 212.1.1.1 : 110.

I comandi da dare sono:

```
R(config)# ip nat inside source static tcp 192.168.3.1:80  212.1.1.1:80
R(config)# ip nat inside source static tcp 192.168.3.1:443  212.1.1.1:443

R(config)# ip nat inside source static tcp 192.168.3.2:25  212.1.1.1:25
R(config)# ip nat inside source static tcp 192.168.3.2:110  212.1.1.1:110
```

Si noti la specificazione del protocollo tcp oppure udp utilizzato dalla porta in questione.

Come per i casi precedenti, si deve indicare se le interfacce coinvolte del router sono inside oppure outside:

```
R(config)# int Fa0
R(config)# ip nat inside

R(config)# int Ser0
R(config)# ip nat outside
```

La tabella delle corrispondenze di indirizzi conterrà le seguenti informazioni fisse:

Inside local	Inside global	Outside local/global
192.168.3.1 : 80	212.1.1.1 : 80	---
192.168.3.1 : 443	212.1.1.1 : 443	---
192.168.3.2 : 25	212.1.1.1 : 25	---
192.168.3.2 : 110	212.1.1.1 : 110	---

ACL , Routing e Natting: ordine delle operazioni

Il traffico in uscita viene prima filtrato con le ACL, poi sottoposto al routing e poi al natting:

pertanto per uscire in Internet, prima si superano gli sbarramenti delle eventuali access-list , poi si cerca nella tabella di routing l'interfaccia di uscita ed infine si applica la trasformazione dell'indirizzo IP del mittente.

Il traffico in ingresso viene prima filtrato con le ACL, poi sottoposto al natting e poi al routing:

pertanto, per poter entrare, un pacchetto prima deve superare gli sbarramenti delle eventuali access-list, poi viene trasformato cambiando il suo indirizzo di destinazione da pubblico a privato ed infine si vede nella tabella di routing come farlo arrivare a destinazione.