Sicurezza e Gestione delle Reti (di telecomunicazioni)

Tommaso Pecorella
tommaso.pecorella@unifi.it

Corso di Studi in Ingegneria Elettronica e delle Telecomunicazioni
Corso di Studi in Ingegneria Informatica
Facoltà di Ingegneria
Università degli Studi di Firenze

Lezione 07, NAT
aa. 2010/11

Gli elementi del management

Problema

- Gli indirizzi IP sono costosi e pochi
- Non sempre si vuole “far vedere” la struttura interna di una Intranet

NAT e NAPT mascherano un indirizzo tramite un proxy a livello IP.

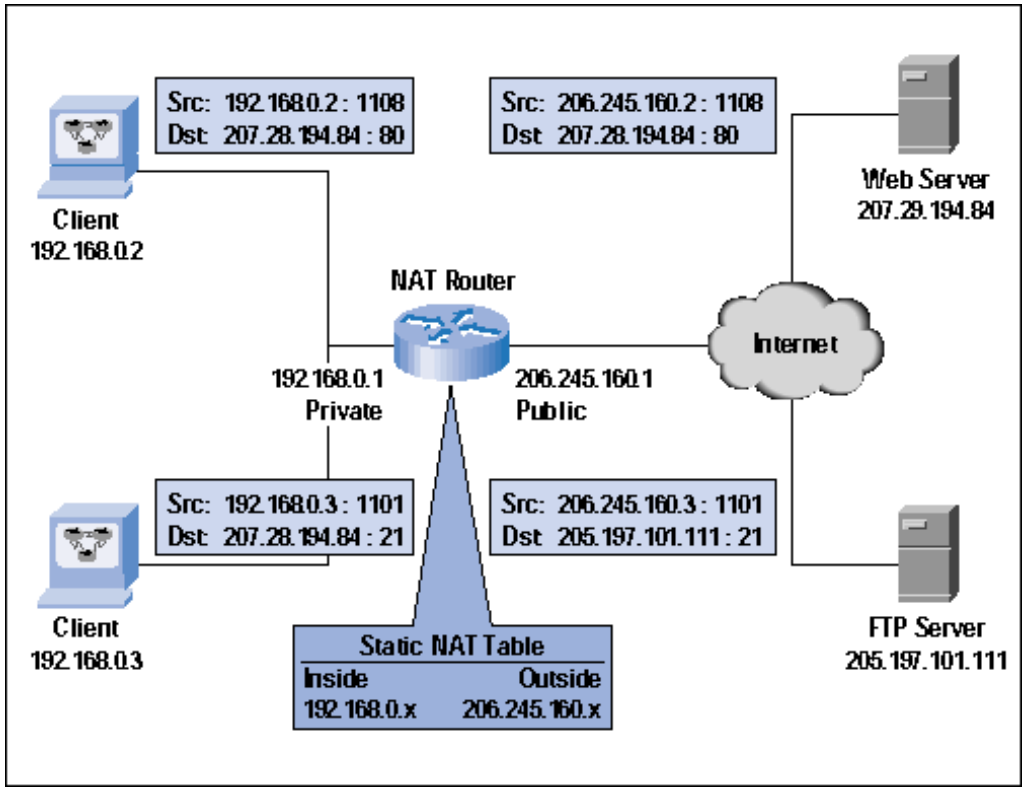
- Si trasforma un indirizzo sorgente (IP number e port) in un altro indirizzo.
- Il server NAT viene visto all’esterno come la sorgente della comunicazione.
- Il NAT è trasparente per l’utente interno.

Si usa uno spazio di indirizzi “non routable” (RFC 1918)

Class	Private Address Range
A	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.255.255
C	192.168.0.0 - 192.168.255.255

NAT Statico

- mapping uno-a-uno tra ind. esterni ed interni,
- uso molto limitato, può servire in congiunzione ad un firewall,
- non risolve il problema di scarsità degli indirizzi,
- molto facile da implementare.

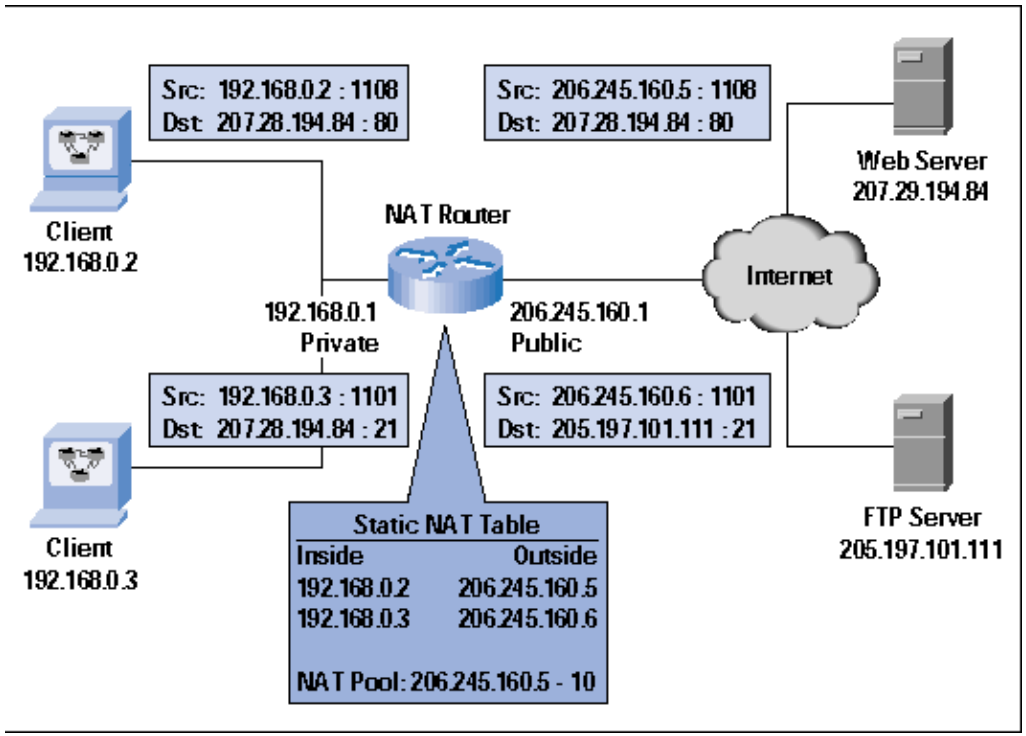


NAT Dinamico

- mapping dinamico tra ind. interni ed esterni,
- risolve il problema di scarsità degli indirizzi,
- richiede un server stateful.

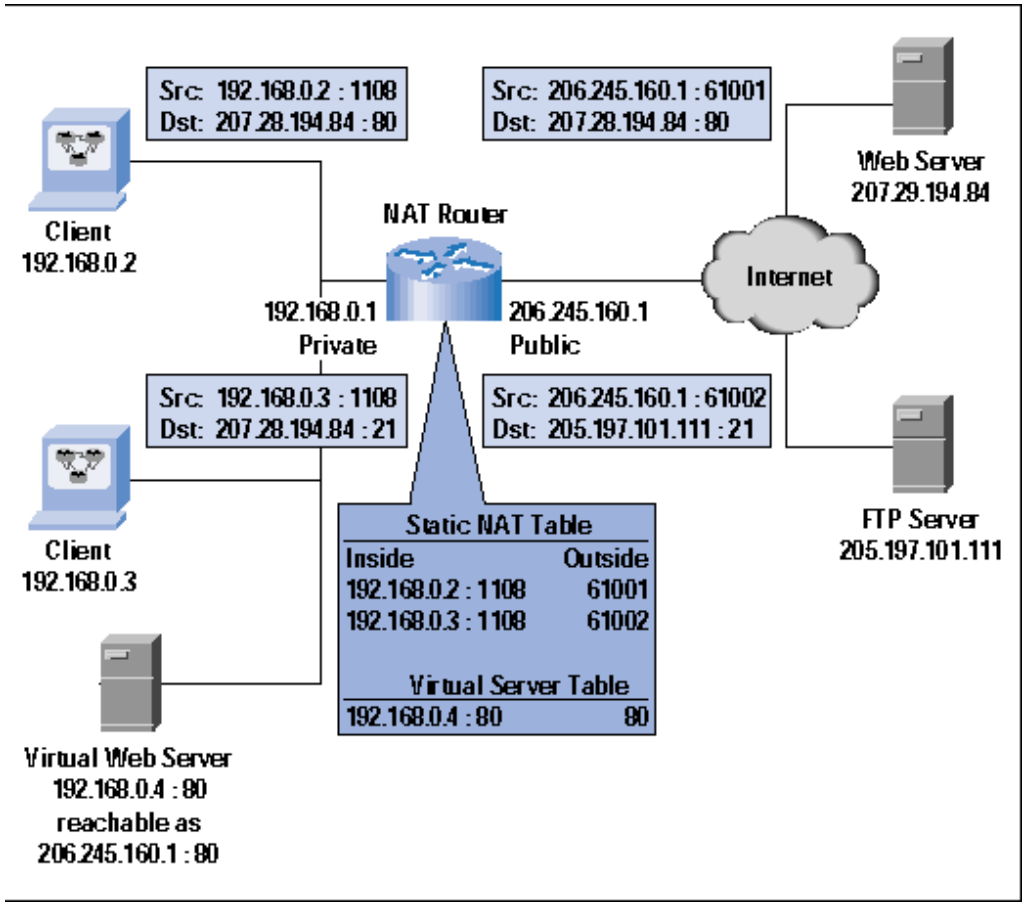
Problema:

- e se due host interni usano la stessa porta ?



NAPT - Network Address and Port Translation

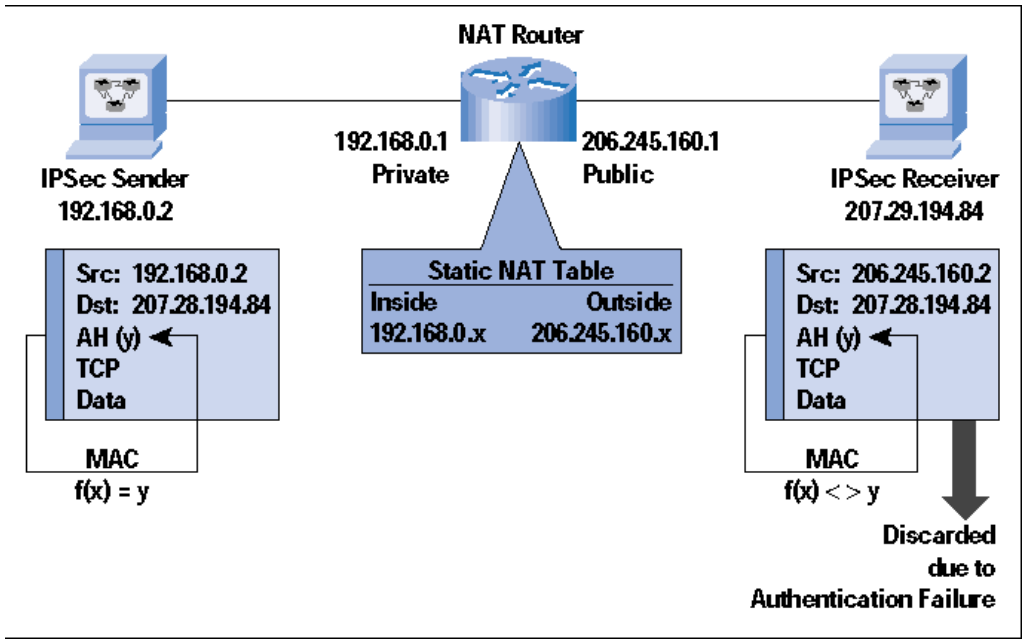
- mapping dinamico tra ind. interni ed esterni, porte dinamiche
- risolve il problema di scarsità degli indirizzi,
- richiede un server stateful più complesso del NAT.



NAPT e IPsec

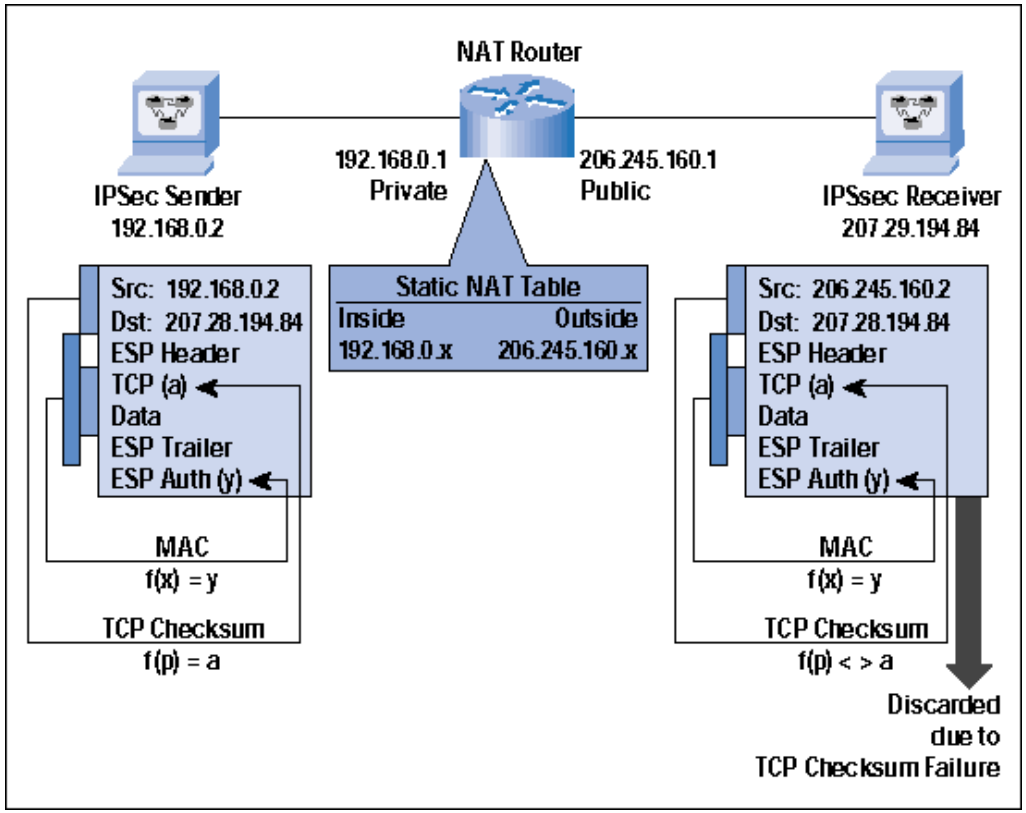
Timete Danaos et dona ferentes

- Il NAT implica un ricalcolo dei checksum IP e TCP… come l'IPsec.
- Le due cose possono interferire *molto* male, portando ad un completo blocco delle comunicazioni.



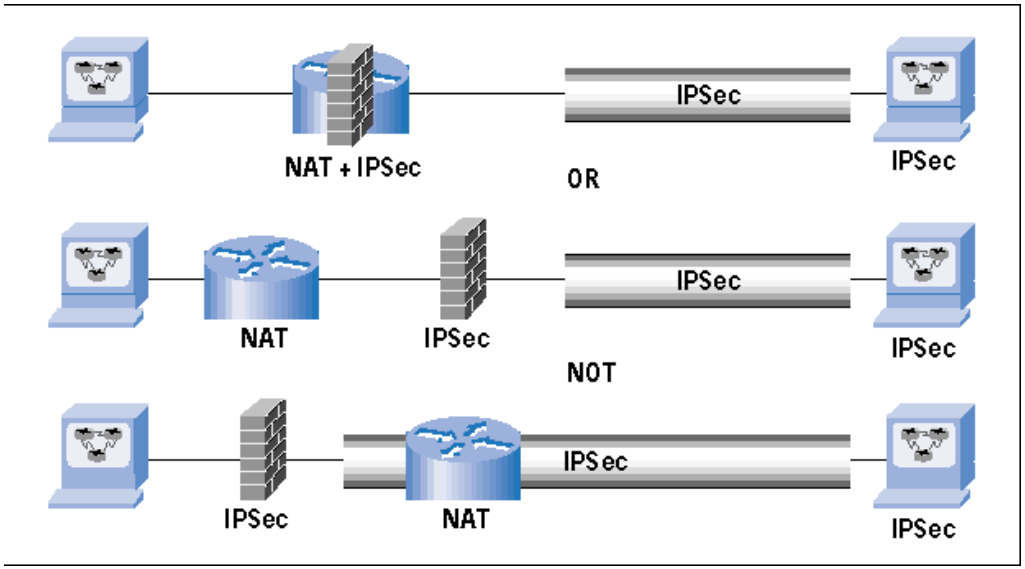
NAPT e IPsec

- La modalità ESP ha problemi analoghi alla modalità AH.



NAPT e IPsec – how to

Soluzione: fare PRIMA il NAT e POI applicare IPsec (o farli insieme).



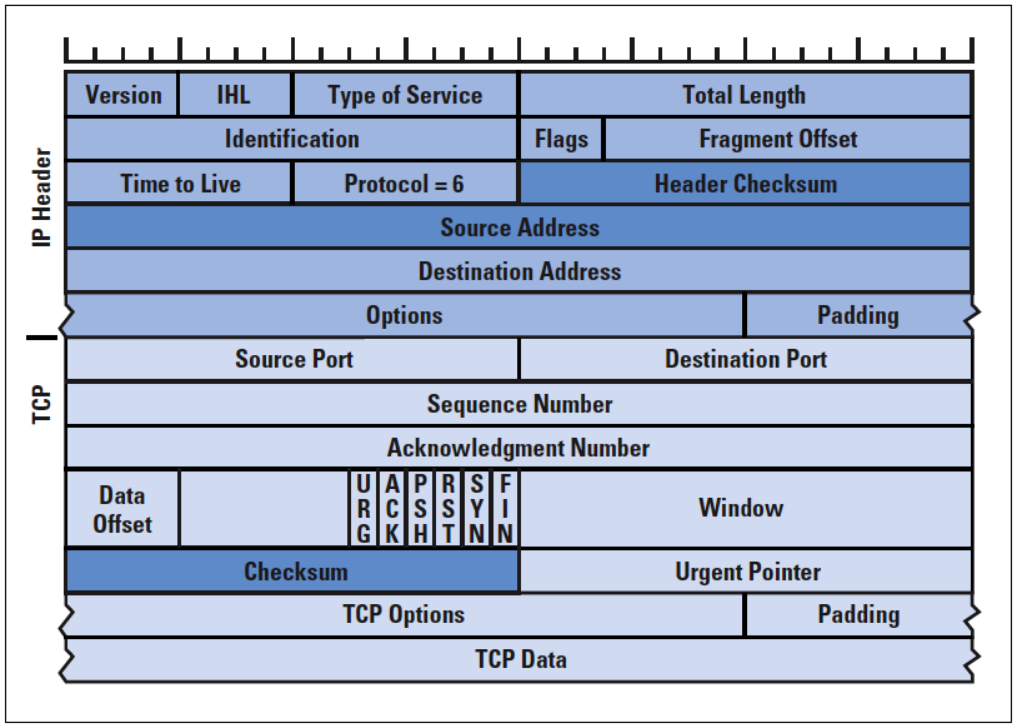
In ogni caso:

- Un host dietro ad un NAT non può cominciare una comunicazione IPsec.
- La co-locazione di NAT e IPsec è un potenziale pericolo per la sicurezza.

Nota: si potrebbe fare un tunnel IP-over-IP... ma fa schifo.

NA[P]T - funzionamento

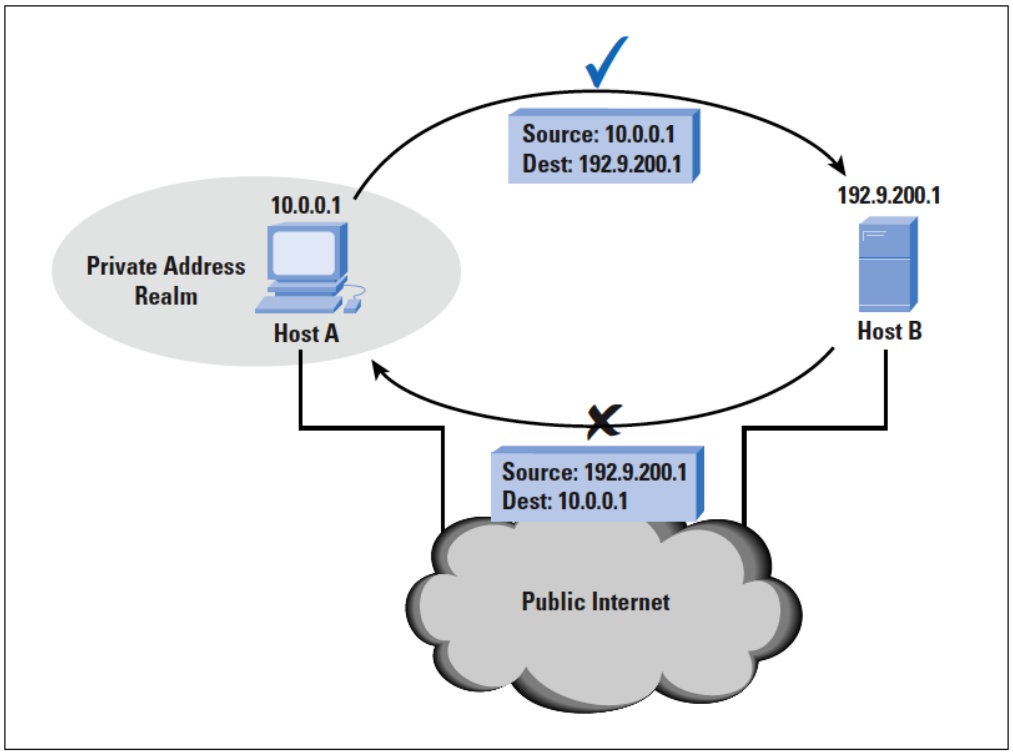
Il NAT nasce nel 1994 (RFC 1631) come un metodo per alleviare il problema della scarsità di indirizzi IPv4



L'RFC 2776 del 2000 definisce il "Network Address Translation— Protocol Translation (NAT-PT)"

NA[P]T - idea di base

In Internet i pacchetti “non routable” non sono trasportati (i router li scartano!) perché l’indirizzo IP NON E’ UNIVOCO !



Quindi serve una traslazione da indirizzo non-routable a un indirizzo routable =¿ NAT !

NA[P]T - operazioni

Operazioni di un NAT:

Arriva un pacchetto sull'interfaccia *interna*

Si cerca un binding, c'è ?

- SI si trasla il pacchetto e si fa il forward
- NO si crea un binding e si fa il forward

Arriva un pacchetto sull'interfaccia *esterna*

Si cerca un binding, c'è ?

- SI si trasla il pacchetto e si fa il forward
- NO si scarta il pacchetto

Allo scadere di un timer

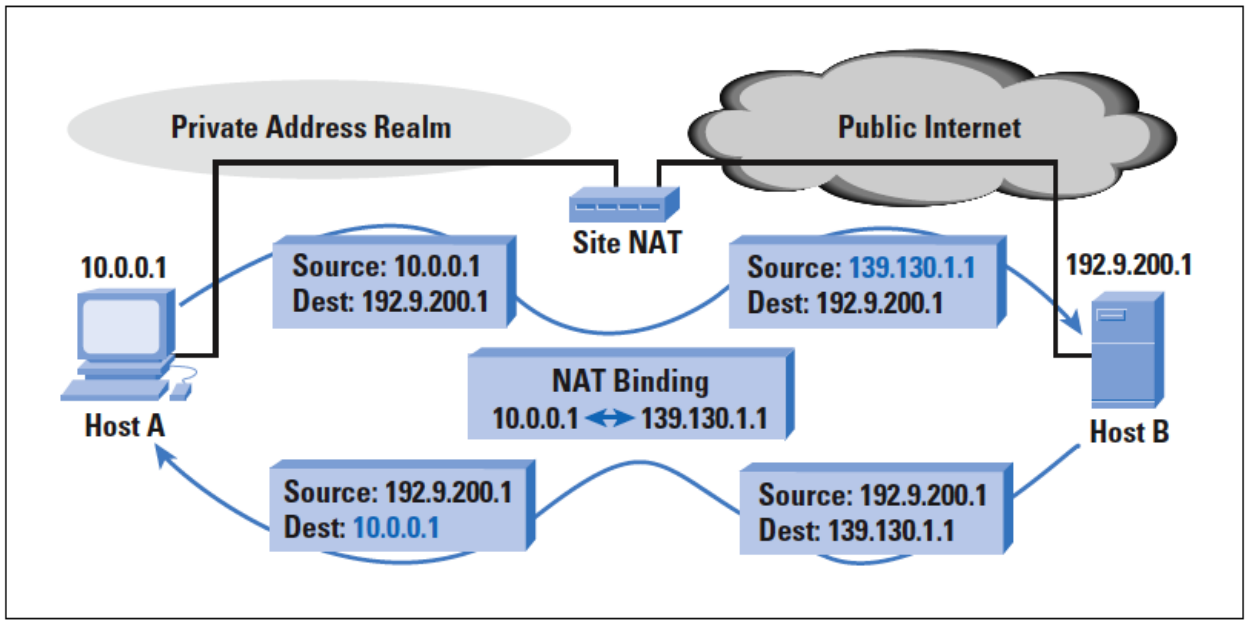
Si cancella il binding

Binding: associazione {IP, Proto, Port}(int) <=> {IP, Proto, Port}(ext)

NAT RFC 1631

Si varia solo l'indirizzo IP. Funziona ma non risolve la scarsità di indirizzi.

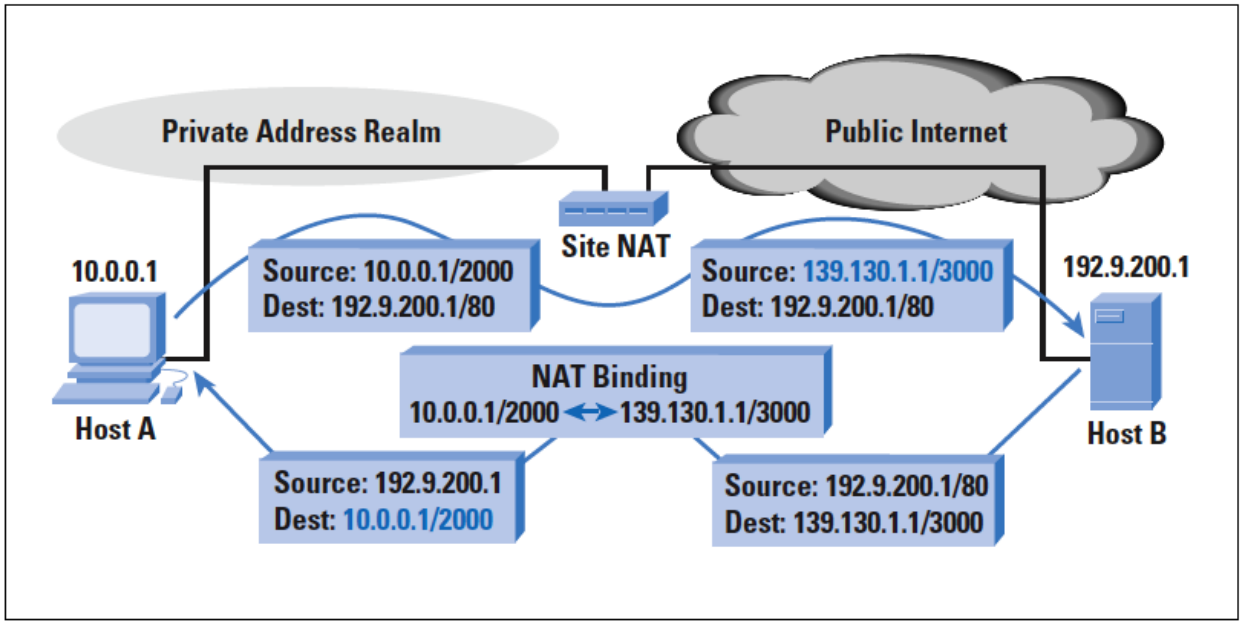
Il numero di indirizzi necessari è pari al numero di PC che vogliono usare *contemporaneamente* lo stesso protocollo.



NAT RFC 2776

Si varia l'indirizzo IP -e- la porta sorgente. Funziona.

Il numero di connessioni contemporanee (bindings) è pari circa a 64000 (well-known ports escluse).



NAT binding

PROBLEMA: cosa è un binding ?

- Binding: associazione {IP, Proto, Port}(int) <=> {IP, Proto, Port}(ext)
- E' in realtà composto da *Binding* e *Filter*

Binding

- Associa indirizzo/porta interna a indirizzo/porta esterna
- Esegue la funzione interno <=> esterno

Filter

- Decide se e quali pacchetti dall'esterno vanno ritradotti

Filter

- Il comportamento del filter genera differenti comportamenti del NAT
- Alcuni sono voluti, altri. . . no

NAT binding

PROBLEMA: cosa è un binding ?

- Binding: associazione {IP, Proto, Port}(int) <=> {IP, Proto, Port}(ext)
- E' in realtà composto da *Binding* e *Filter*

Binding

- Associa indirizzo/porta interna a indirizzo/porta esterna
- Esegue la funzione interno <=> esterno

Filter

- Decide se e quali pacchetti dall'esterno vanno ritradotti

Filter

- Il comportamento del filter genera differenti comportamenti del NAT
- Alcuni sono voluti, altri. . . no

NAT binding

TCP e UDP sono differenti...

TCP, stateful

Il binding è aggiornato in base a un timer che varia a seconda dello stato della connessione e della dimensione della CWIN

UDP, stateless

Il binding è basto solo su un timer e sulla "conoscenza" del comportamento dell'applicazione (i.e., porte utilizzate)

Nel TCP il NAT ha di solito comportamento "symmetric", ossia binding e filter sono basati sulla quintupla {protocollo, IP e porte sorgente-destinazione}. Comportamento logico, ma...

- Le comunicazioni devono partire dall'interno
- Non è possibile fare una "callback", quindi PASSIVE FTP.

NAT binding

Quello che va bene per il TCP non è detto che vada bene per l'UDP !

TCP: uno stream è definito da una quintupla. Il demultiplexing è definito a livello di TCP

UDP: il demultiplexing è fatto a livello *applicativo*.

Una singola applicazione può usare una sola socket in uscita per due stream diversi con destinatari diversi (il TCP non lo permette).

Serve un diverso comportamento del NAT nel caso di UDP

NAT binding

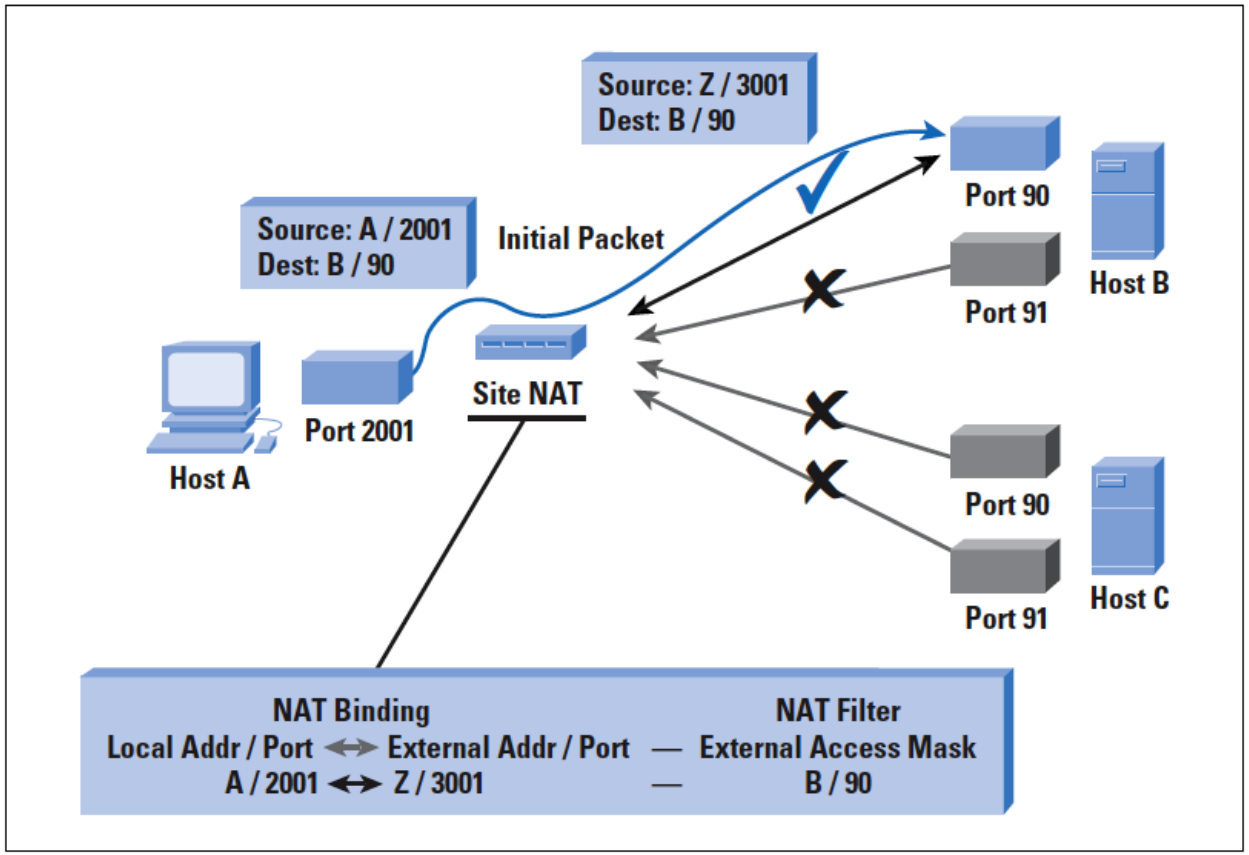
Il comportamento del NAT per l'UDP è gestito da come il Filter viene eseguito nel caso di UDP.

Esistono 4 diversi behaviour:

1. Symmetric NAT
2. Full Cone NAT
3. Restricted Cone NAT
4. Port Restricted Cone NAT

In base a come si comporta il NAT alcuni applicativi possono o meno funzionare, in parte o del tutto.

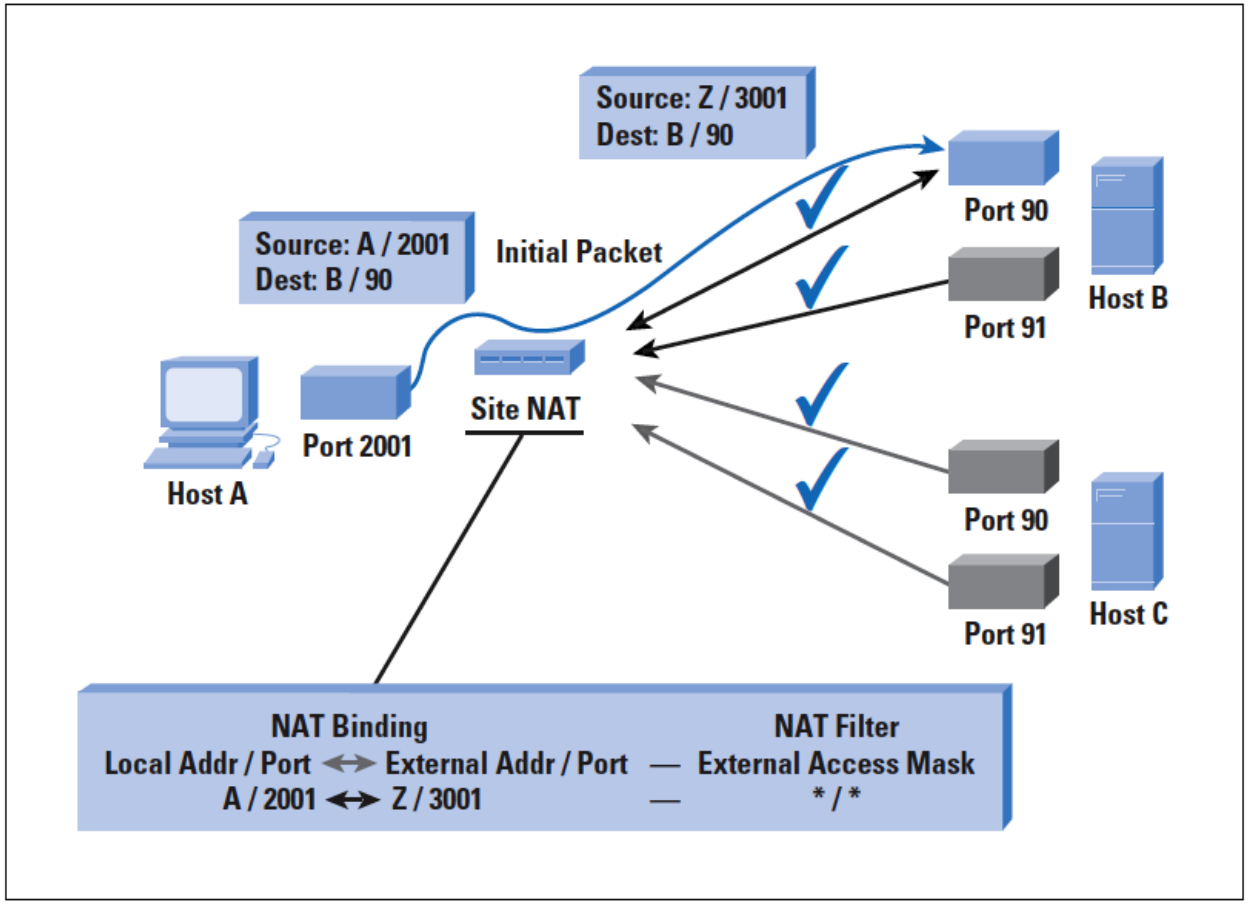
Symmetric NAT (UDP)



Esattamente come il symmetric NAT del TCP

Non funzionano i programmi che hanno bisogno di referral & handover (es. MSN)

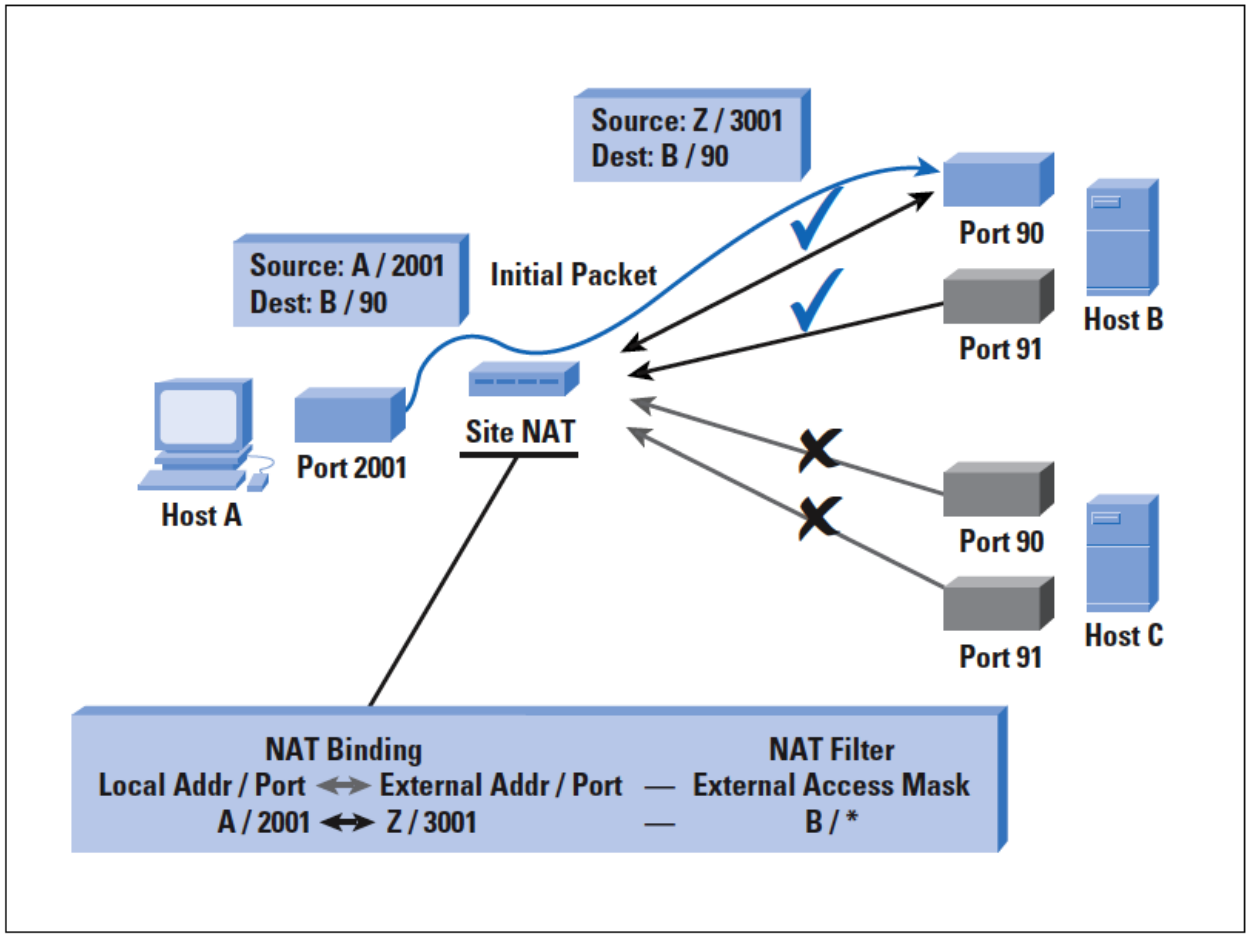
Full Cone NAT



Il Filter non fa nulla. . .

Ottimo, ma TUTTI e TUTTO raggiungeranno il sorgente (anche i malintenzionati, si può fare persino un port scanning).

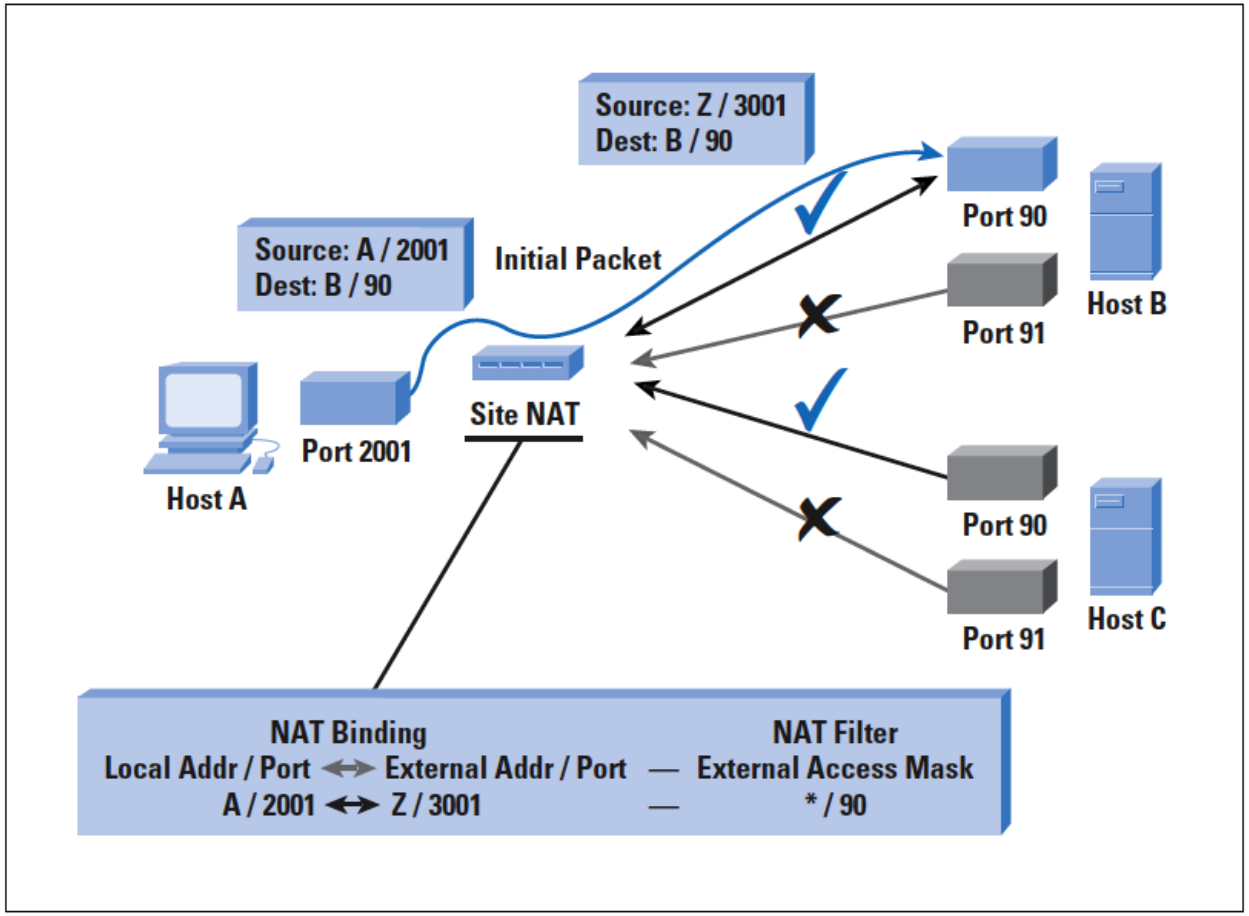
Restricted Cone NAT



Il Filter è basato sull'IP del destinatario.

Limitante, MSN ad esempio non funziona (il mulo neppure).

Port Restricted Cone NAT



Il Filter è basato sulla PORTA del destinatario.

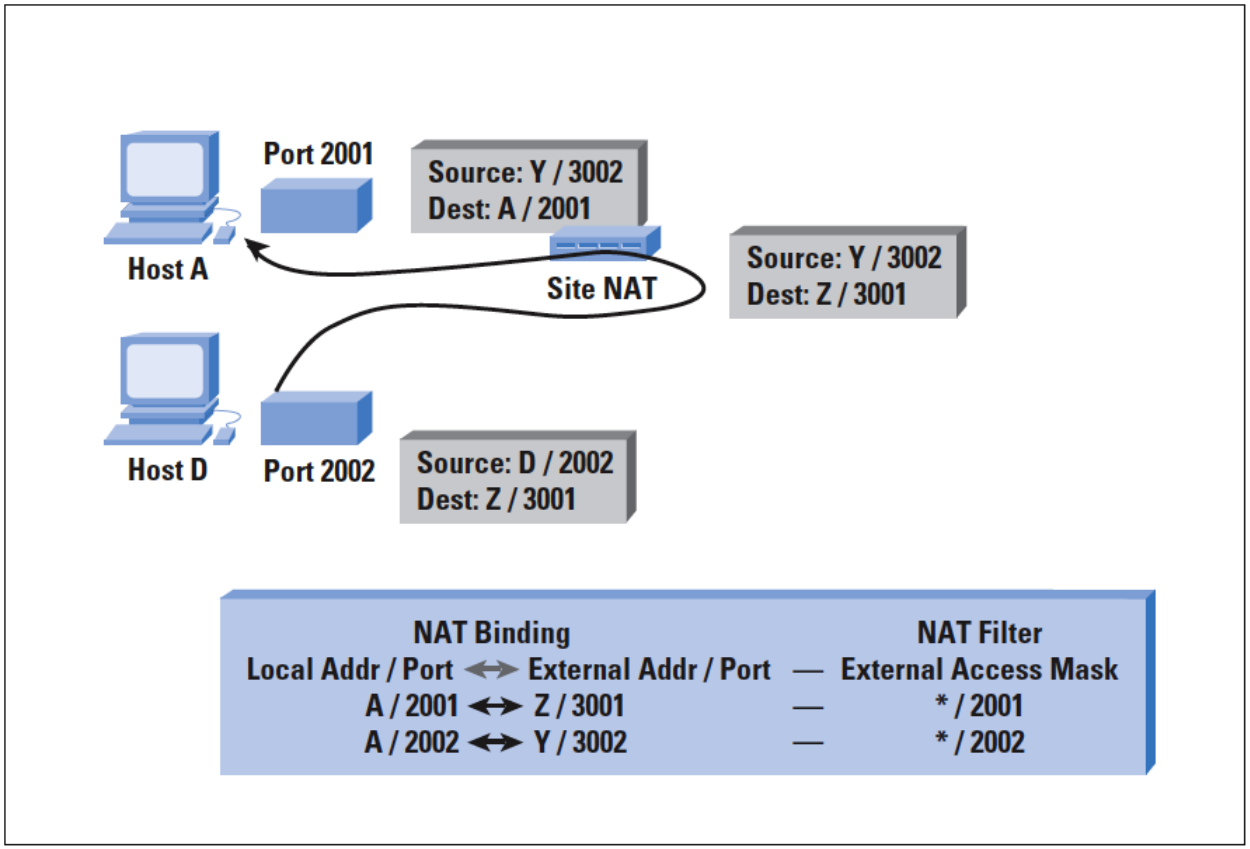
Ora va meglio, funzionano quasi tutti i programmi UDP, anche se con delle limitazioni.

Hairpin ?

E se volessi raggiungere un host nella mia stessa rete ?

L'operazione si chiama *hairpin* e può comportare o meno l'uso di indirizzi esterni

- Potrebbe non essere supportato!



Tipi di NAT - STUN

Come si scopre il tipo di NAT ?

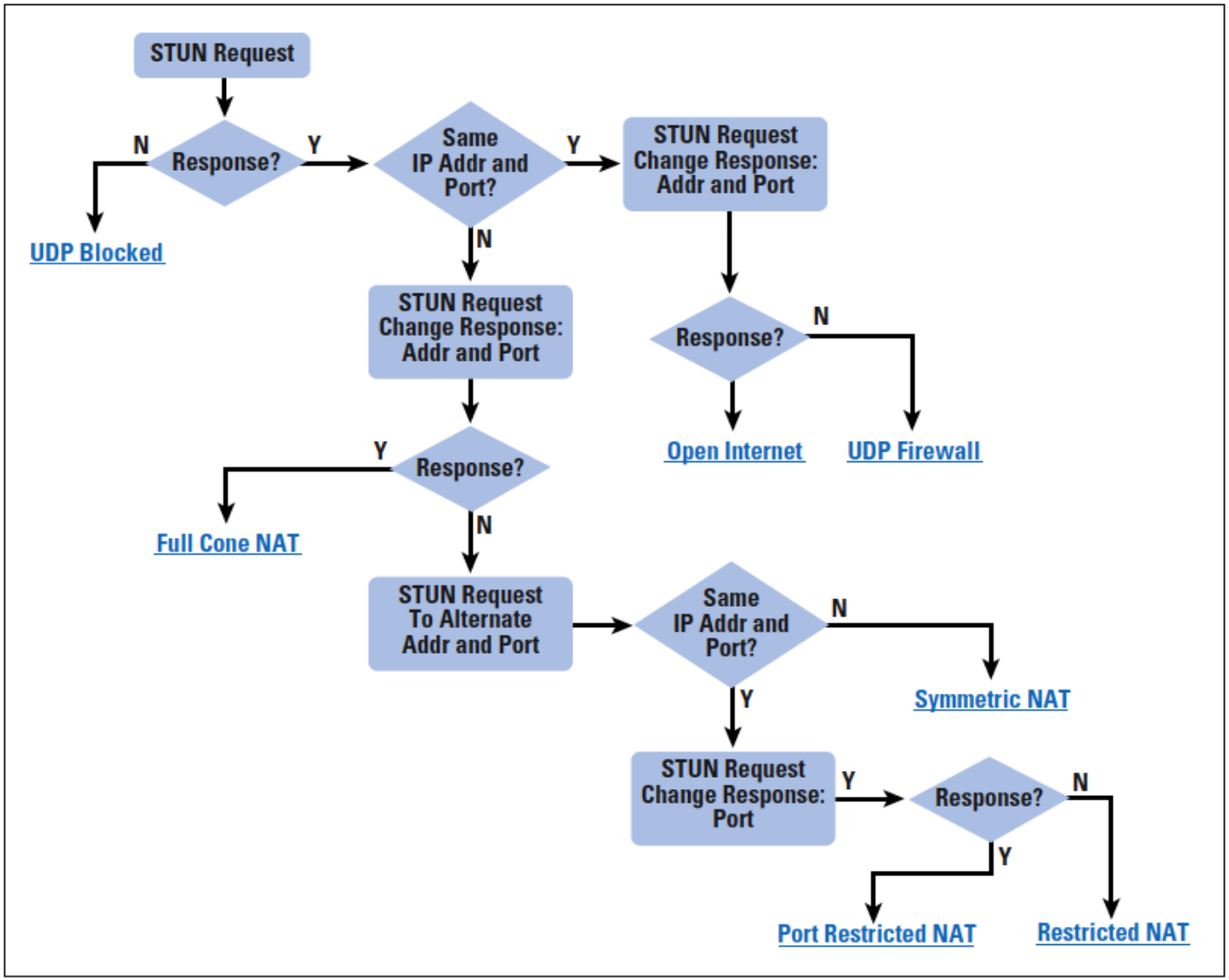
Il NAT tenta di adattarsi all'applicazione, ma le applicazioni tentano di adattarsi al tipo di NAT !

Rosenberg, J., Weinberger, J., Huitema, C., and R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)," RFC 3489, March 2003.

Lo STUN è un protocollo request-reply:

- WTF of address/port this packet came from ? TYVM.
- Due porte sul client, due porte -e- due indirizzi IP sul server.

NAT - STUN


STUN Request
Response?
N
Y
UDP Blocked
Same IP Addr and Port?
Y
N
STUN Request Change Response: Addr and Port
Response?
N
Y
Full Cone NAT
STUN Request Change Response: Addr and Port
Response?
Y
N
Open Internet
UDP Firewall
STUN Request To Alternate Addr and Port
Same IP Addr and Port?
N
Y
Symmetric NAT
STUN Request Change Response: Port
Y
Response?
N
Y
Port Restricted NAT
Restricted NAT

STUN - funzionamento

ATTENZIONE !

Il NAT può essere *non deterministico*, ossia cambiare il suo comportamento a seconda della disponibilità delle risorse

oppure. . .

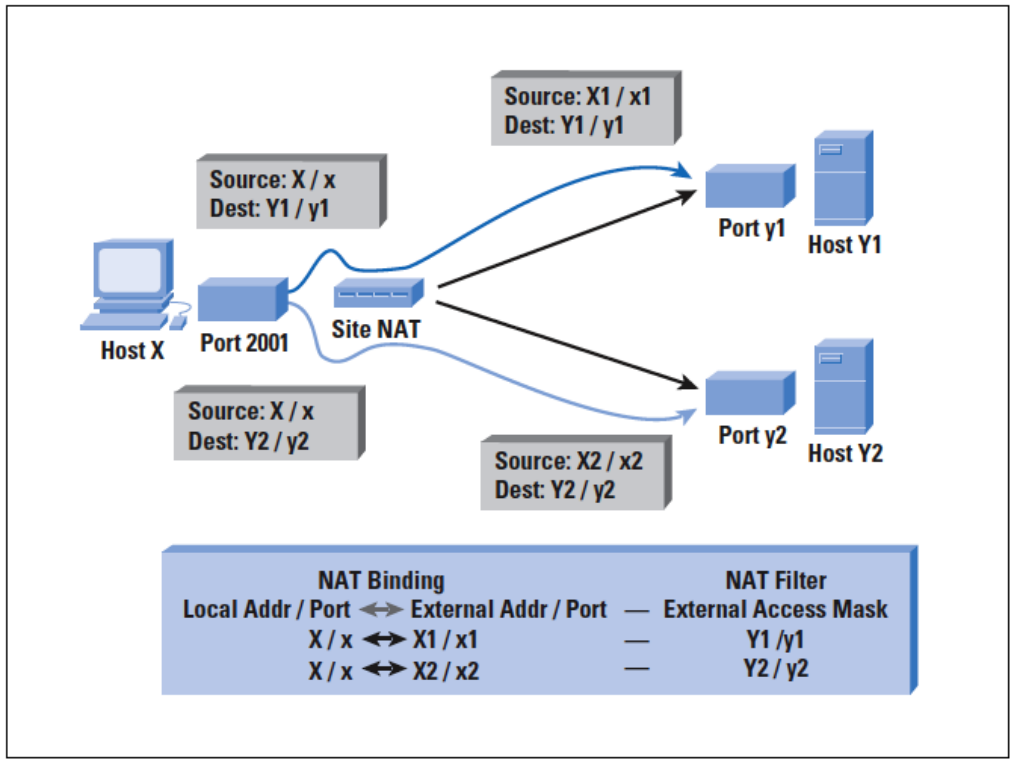
Potrebbero esserci più NAT nel path sorgente / destinazione, nel qual caso la classificazione non è rigorosa e il comportamento non è prevedibile.
Il secondo livello di NAT potrebbe non avere lo stesso comportamento del primo.

oppure. . .

NAT - classificazione

Back to basis: binding, filtering e timers

- Come viene fatto il binding ?
- Come vengono aggiornati i filters ?
- Quando vengono riavviati timers ?



Questo qui come si classifica ?!?!?!

NAT - Binding

Endpoint independent

Il NAT riusa il binding per tutte le sessioni provenienti dalla stesso IP/porta, l'IP/porta esterno non è valutato.

- E' come un *Full Cone NAT*.

Endpoint address dependent

Il NAT riusa il binding per tutte le sessioni provenienti dalla stesso IP/porta verso lo stesso IP esterno (la porta non si considera).

- E' come un *Restricted Cone NAT*.

Endpoint address and port dependent

Si usa la quintupla IP/porta sorgente/destinazione (e il protocollo).

- E' come un *Symmetric NAT*.

NAT - Port Binding

Port preservation

Il NAT può tentare di mantenere a porta di origine. Se due host interni usano la stessa porta di origine, uno avrà la porta cambiata, uno no.

Port overloading

Il NAT fa port preservation in maniera aggressiva, un secondo tentativo di binding fa scadere il binding esistente.

Port multiplexing

Il NAT si occupa di fare il demultiplexing. All'esterno i pacchetti appaiono come se provenissero dallo stesso IP/porta, il NAT farà il demultiplexing corretto.
MA se due host interni volessero mandare due stream allo stesso host/porta esterno non sarebbe possibile il demultiplexing. In questo caso uno dei due stream avrebbe assegnata una porta diversa. E' un comportamento non deterministico.

NAT - Timer Refresh

Bidirectional

Il timer è rinfrescato dai pacchetti in entrambi i sensi.

Outbound

Solo i pacchetti dall'interno verso l'esterno rinfrescano il timer. E' necessario usare un keep-alive. Inoltre il timer potrebbe essere per-session o per-binding (nel caso di riuso del binding per più sessioni).

Inbound

Solo i pacchetti dall'esterno verso l'interno rinfrescano il timer. Anche in questo caso è necessario un keep-alive.

Transport Protocol state

Come nel TCP, ma si potrebbero usare altre informazioni.
Nota: il Transport Protocol State dà la possibilità di fare attacchi DOS

NAT - External Filtering

Endpoint independent

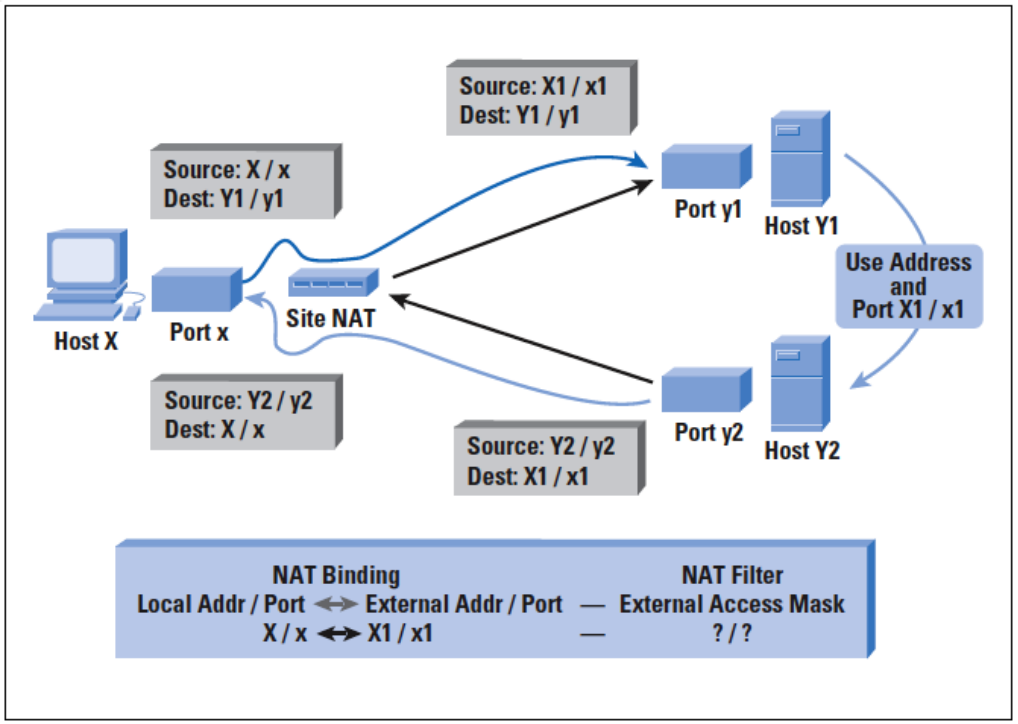
Non filtra o scarta pacchetti.
Full Cone NAT.

Endpoint address dependent

Filtra i pacchetti che non provengono dall'IP originario del binding. *Restricted Cone NAT*.

Endpoint address and port dependent

Filtra i pacchetti che non provengono dall'IP/porta originario del binding. *Port Restricted Cone NAT* o *Symmetric NAT*.



Il Filter può avere un timer separato simile a quello del Binding !

NAT - considerazioni

Applicazioni P2P

Tentano di aggirare i NAT, ma così facendo si creano spesso problemi di sicurezza.
“Bucare” può significare aprire un numero di porte arbitrario.

ICMP

Rischia di fallire miseramente, perché nel payload sono spesso contenute informazioni relative all’IP/porta originante. Stessi problemi che con l’IPsec.

IP fragmentation

Vanno ricostruiti i pacchetti (o mantenute informazioni dal primo frammento) perché nei frammenti successivi manca l’header TCP/UDP. . . ma potrebbe essere un attacco a frammentazione !
E se poi il primo frammento arriva fuori sequenza ?

Altri protocolli possono avere gli stessi problemi.
Il NAT può tentare di modificare il contenuto stesso del payload.

NAT e UPnP - IGD

"Timeo Danaos et dona ferentes". Virgilio, Eneide (II, 49)

Universal Plug and Play (UPnP)

Set di protocolli e procedure per la definizione e l'annuncio di device e servizi.
"A UPnP compatible device from any vendor can dynamically join a network, obtain an IP address, announce its name, convey its capabilities upon request, and learn about the presence and capabilities of other devices."
[Wikipedia]

Internet Gateway Device (IGD) Standardized Device Control Protocol

Permette ad un device UPnP di scoprire l'indirizzo esterno di un NAT e di creare binding/filters per i suoi servizi in maniera automatica. E' implementato in Windows...

Pros: funziona tutto magicamente...TROPPO
Cons: le porte del NAT sono aperte in maniera incontrollata e potrebbero sovrascrivere binding esistenti... come per la porta 80 !!

Copyrights

Le immagini sono tratte da articoli apparsi su:

- The Internet Protocol Journal - ISSN 1944-1134
  `http://www.cisco.com/web/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html`