Università di Firenze
Dipartimento di **E**lettronica e **T**elecomunicazioni

Gestione delle Reti di Telecomunicazioni

Virtual Private Networks

Ing. **Tommaso Pecorella**

Ing. **Giada Mennuti**

{pecos,giada}@lenst.det.unifi.it

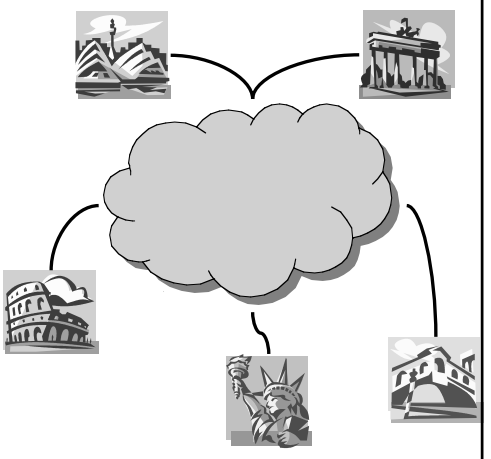
Virtual Private Network (VPN)

Problema:

una multinazionale (o una ditta con più sedi) vuole usare Internet come infrastruttura di rete.

Obiettivo:

offrire un servizio *equivalente* a quello ottenibile tramite l'uso di un'infrastruttura privata.

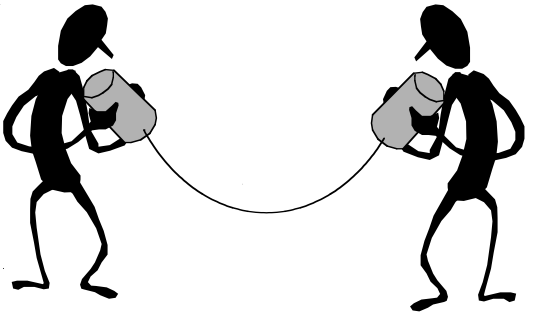


Linea dedicata

Le linee dedicate sono storicamente il primo esempio di Private Network

Vantaggi:
1. realmente dedicate
2. abbastanza sicure
3. QoS prevedibile

Problemi:
1. costo
2. sottoutilizzo
3. difficilmente riconfigurabili

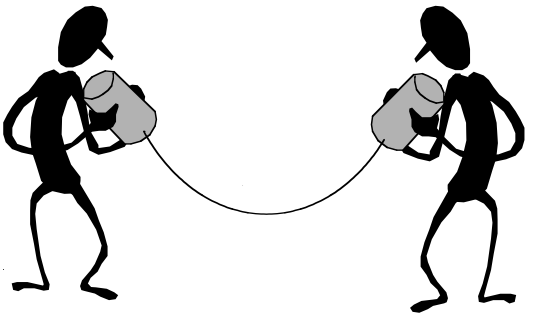


Canali ATM

Un canale ATM è la versione "moderna" di una linea dedicata

Vantaggi:
1. sharing soggetto a SLA
2. abbastanza sicure
3. QoS prevedibile
4. riconfigurabili

Problemi:
1. costo (dip. dallo SLA)
2. cattiva integrazione con IP
3. ATM è morto...

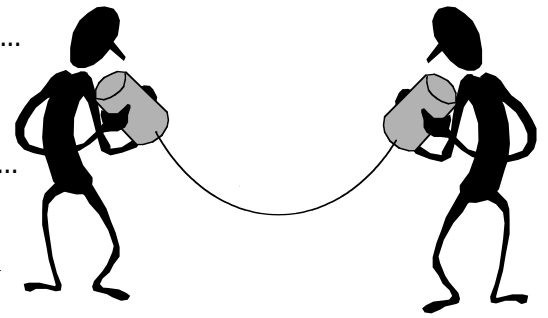


VPN IP-based

Una VPN IP sfrutta Internet

Vantaggi:
1. basissimo costo
2. ottima integrazione con IP, ma...
3. estremamente riconfigurabili

Problemi:
1. QoS imprevedibile a meno che...
2. non sicure, a meno che...
3. difficile configurazione

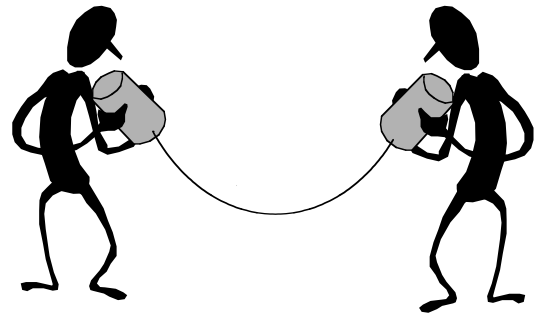


VPN IP-based, how ?

IP ha i seguenti problemi:

1. sicurezza (sniffing, etc.)
2. routing dinamico
3. QoS incerta
4. scarsità di indirizzi

è ugualmente possibile fare una VPN sicura ?



VPN IP-based, how ?

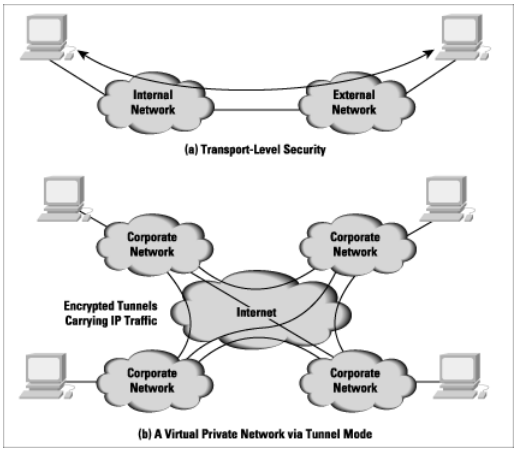
Tecnologie per VPN:

1. sicurezza (sniffing, etc.) ⇨ criptazione (Ipsec, altro)
2. routing dinamico ⇨ VPN layer 2/3
3. QoS incerta ⇨ IntServ/DiffServ o MLPS
4. scarsità di indirizzi ⇨ NAT o IPv6

IPsec (IP secure)

IPsec permette di:

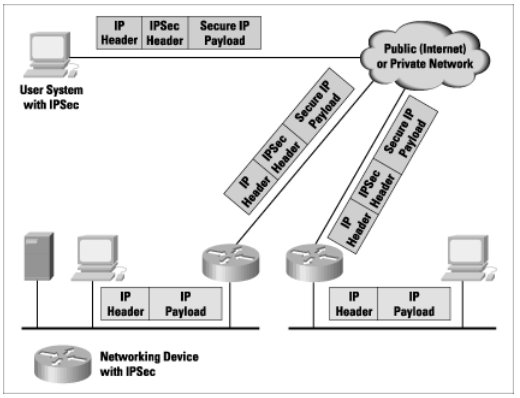
- rendere sicure le comunic. tra diversi uffici di un'org.
- rendere sicuro l'accesso remoto via Internet,
- stabilite connettività intrante/extranet con partner aziendali,
- miglioramenti nella sicurezza del commerci elettronico.



IPsec (IP secure)

scenario IPsec :

- due diverse sedi comunicano tramite un tunnel reso sicuro,
- gli utenti esterni (telelavoro, utenti in viaggio, etc.) accedono alla rete aziendale tramite un canale sicuro,
- attraverso Internet non è possibile "vedere" il contenuto dei pacchetti.



IPsec features

Semplice autenticazione (Authentication Header, AH)

Permette di autenticare il mittente e evitare attacchi "man in the middle". NON cripta il payload.

Autenticazione e criptazione (Encapsulating Security Payload, ESP)

Autenticazione del mittente *e* criptazione del payload. Livello massimo di sicurezza, ma viene "oscurato" il payload IP, quindi crea problemi per il caching, il filtering e la gestione della QoS.

Meccanismi di scambio delle chiavi

IPsec - transport e tunnel

Sia AH che ESP hanno due modalità:

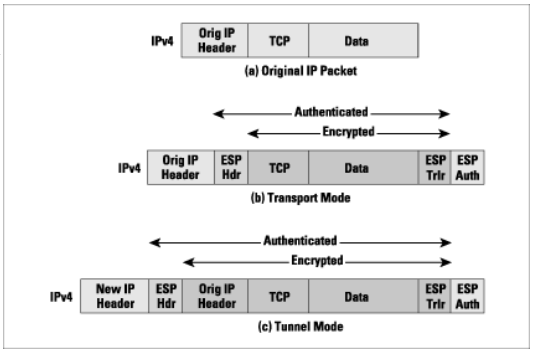
Transport mode

L'header IP originale viene mantenuto

Tunnel mode

L'intero pacchetto IP viene incapsulato in un nuovo pacchetto IPsec.

Nota: nel transport mode si devono ricalcolare i checksum dell'IP e del TCP.



NAT e NAPT

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.

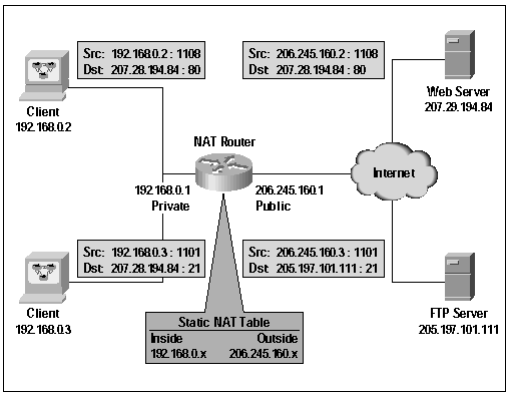
Si usa uno spazio di indirizzi "non routable" (RFC 1918)

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

NAT statico:

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



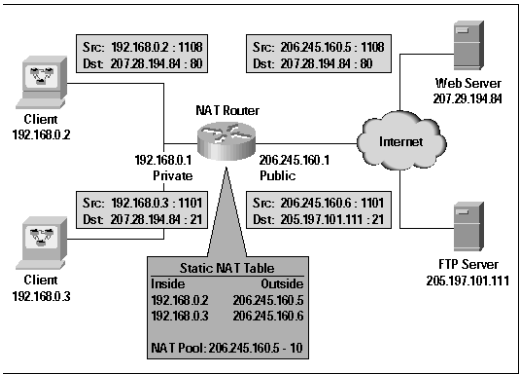
NAT dinamico

NAT statico:

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

Problema:

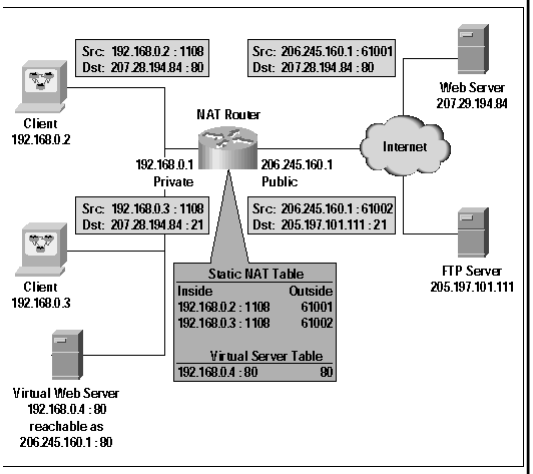
e se due host interni usano la stessa porta ?



NAPT

Network Address and Port Translation

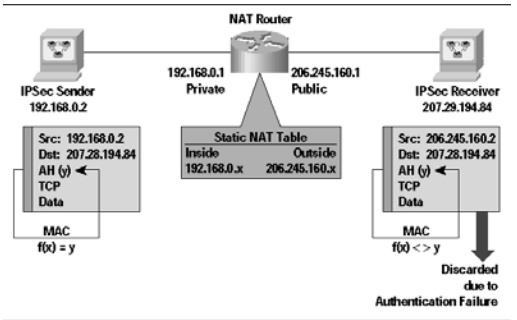
- mapping dinamico tra ind. interni ed esterni, porte dinamiche
- risolve il problema di scarsità degli indirizzi,
- richiede un server stateful più complesso del NAT.



NAPT e IPsec

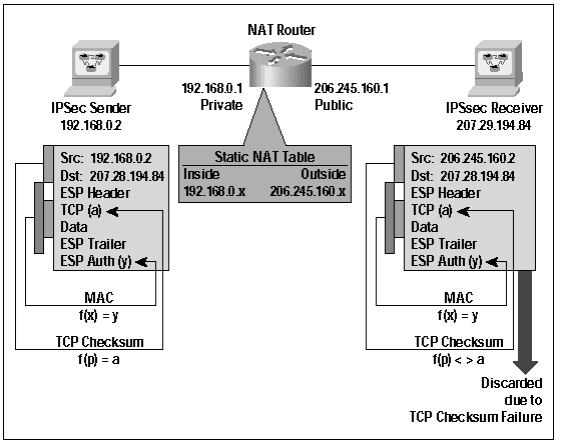
Timete Danaos et dona ferentes

- 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.



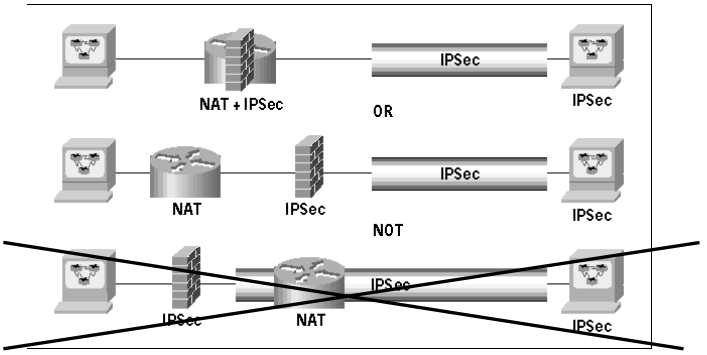
NAPT e IPsec

La modalità ESP ha problemi analoghi alla modalità AH, ma è ancora più intricata la dipendenza dalle cose variate.



NAPT e Ipsec – how to

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



In ogni caso si perde la possibilità di originare comunicazioni IPsec da un host dietro ad un NAT. Inoltre la co-locazione di NAT e IPsec è un potenziale pericolo per la sicurezza.