



Sicurezza architettuale, firewall

05/04/2006

Cos'è un firewall ?



Un firewall è un **sistema di controllo degli accessi** che **verifica tutto il traffico** che transita attraverso di lui

Consente o nega il passaggio del traffico basandosi su una **security policy**

Le sue funzioni:

- Verifica dei pacchetti in transito (IP filtering)

- Mascheramento di indirizzi interni (NAT)

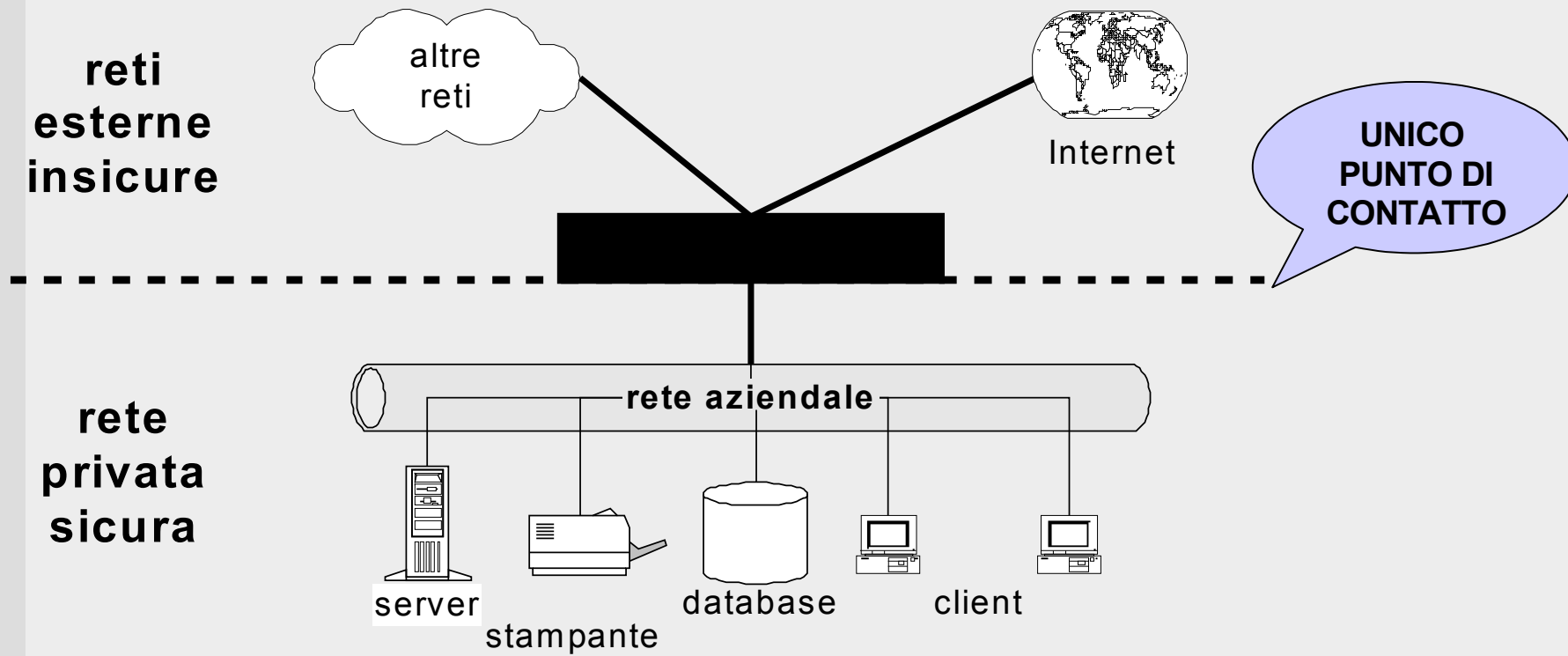
- Blocco dei pacchetti pericolosi e/o non autorizzati

Note da puristi: un firewall, non una firewall e non un "fire wall"

Significa "muro tagliafuoco" in inglese, il "muro di fuoco" è un incantesimo di 4° livello dei maghi...

Firewall: barriera Internet/intranet

Interconnessione **unica** tra **reti esterne** e **rete interna**
(*enforcement point*)



Limiti del firewall



Il firewall controlla **tutto e solo** il traffico che lo attraversa

In caso di *intrusioni dall'interno* il firewall è impotente, in quanto il traffico non lo attraversa

Se il traffico arriva su internet tramite un percorso non controllato non c'è modo per il firewall di controllarlo

Utente connesso via modem e alla LAN

Il firewall è una macchina

Come tale, potrebbe essere violata

Deve essere la macchina meglio protetta e configurata della rete!

Il firewall è un applicatore di regole, ed è **valido solo quanto le regole** che vengono configurate!

Un firewall malconfigurato sarà inefficace o addirittura dannoso

Prima di configurare il firewall, serve una specifica ad alto livello della *policy* (politica) di sicurezza per la Intranet

Policy di “**default deny**”: tutto viene bloccato, tranne ciò che è autorizzato

Nel seguito verranno illustrati alcuni **casi di test** su come configurare i firewall per alcune Intranet aziendali tipiche



Firewall: le tecnologie



Tassonomia dei tipi di firewall

Firewall che operano a network layer

- Packet Filtering

- Stateful Packet Filtering (tra network e transport)

Firewall che operano ad application layer

- Circuit level firewalls (tra transport ed application)

- Application proxy firewalls



Firewall a livello di rete

Packet filter

Stateful firewall

Packet Filter



Filtra i pacchetti soltanto sulla base delle informazioni nell'header

- Indirizzo sorgente, indirizzo destinazione

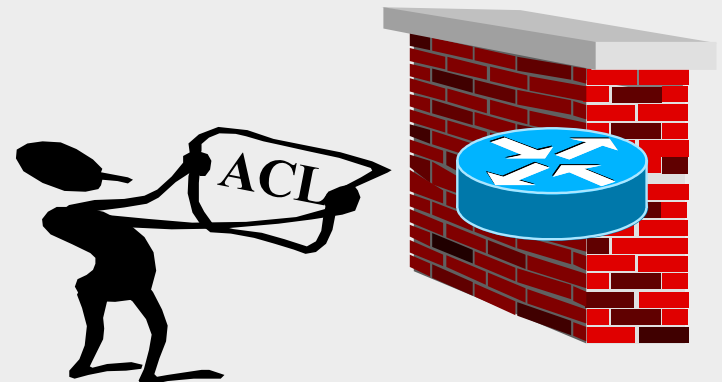
- Porta sorgente, porta destinazione

- Tipo di protocollo

- Opzioni di protocollo

Non si può tracciare la correlazione tra pacchetti in una trasmissione

Non si possono nemmeno esaminare problemi a livello più alto



Cosa possiamo fare con queste regole ?



Basandosi sugli indirizzi, si possono chiudere o aprire il traffico da determinate sorgenti e verso determinate destinazioni

Basandosi sui numeri di porta posso bloccare o permettere servizi noti

Posso bloccare un protocollo

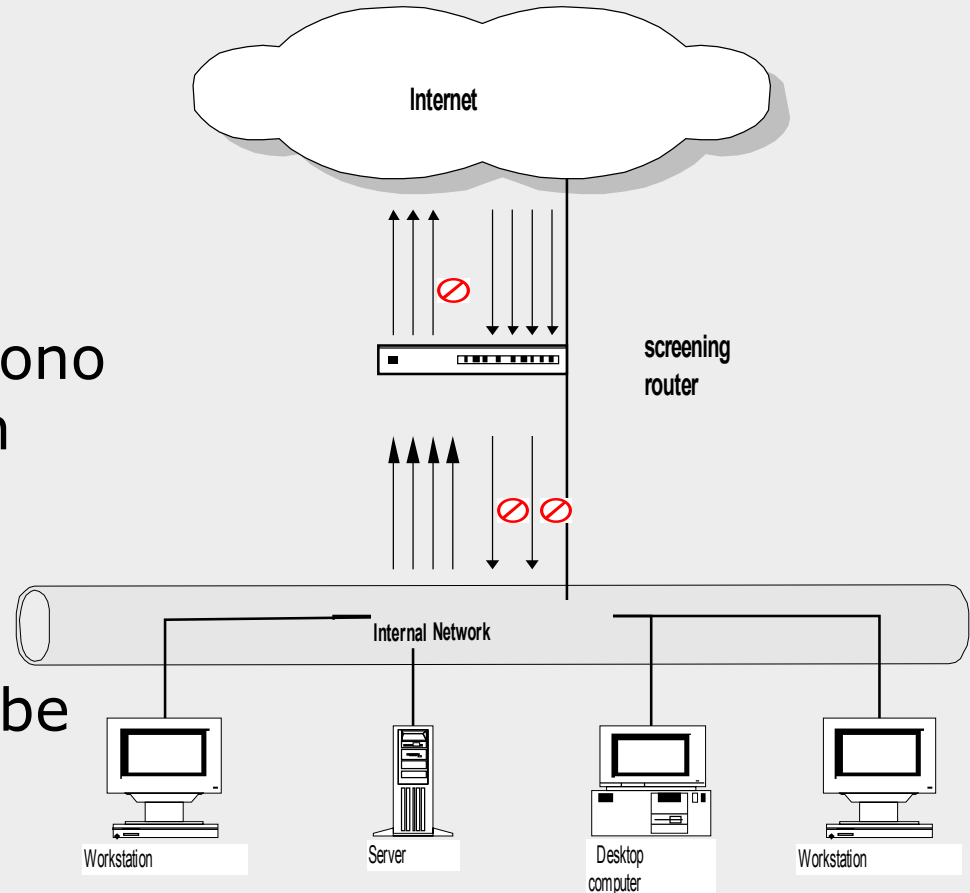
Combinazioni dei precedenti

Es.: se un pacchetto arriva sull'interfaccia *esterna* ed ha un mittente della rete *interna* lo posso bloccare (spoofing)

Es.: se un pacchetto arriva dalla *rete del mio partner* lo lascio accedere: *pericoloso* !

Screening Router

- Un packet filter gestisce solo le informazioni contenute nell'header di network layer
- Le stesse informazioni sono tipicamente gestite da un ROUTER
- Funzione: instradare i pacchetti
- Posso fargli fare entrambe le cose
- Possibile problema di prestazioni





Stateful (Dynamic) Packet Filtering

Il tipo di regole è molto simile al precedente:
sorgente, destinazione, porta, protocollo

Si aggiunge lo stato, riproduzione della macchina a stati del TCP

Es. A un pacchetto SYN deve corrispondere un SYN-ACK con determinati valori, qualsiasi altra risposta va scartata

Se un pacchetto è una risposta legittima a una connessione già autorizzata, può passare

Migliore espressività

Deve tenere traccia delle connessioni:

- Possibili problemi di memoria

- Possibili problemi di performance

Stateful Packet Filtering: altri benefici



Mediante questi algoritmi, i pacchetti di risposta dall'esterno vengono autorizzati solo se inseriti in una comunicazione cominciata dall'interno (default deny su tutto, ottimo !)

Ispezione avanzata, che può ricostruire intere sessioni

HTTP e FTP possono essere ricostruiti

Application content filtering

Posso decidere di bloccare, p.es., tutti i contenuti ActiveX nelle connessioni HTTP

Può fare autenticazione sugli utenti interni (raro)

Può fare accounting sulle connessioni

Network Address Translation (NAT)

Per nascondere gli indirizzi interni



Deframmentazione e options

Pacchetti IP più grandi della MTU vengono frammentati

Gli aggressori spesso usano la frammentazione per nascondere le loro intenzioni o per provocare errori

IP fragment protection

- I pacchetti ICMP vengono deframmentati e analizzati (evita il large ICMP overflow)

- Deframmenta i pacchetti per controllarli

- Può aiutare a migliorare le performance

Pacchetti con IP options devono essere sanitizzati o scartati

- Es. Source routing, ICMP redirection, ecc.

Gestione delle sessioni



Chiamiamo "sessione" una transazione di scambio di dati tra due host su Internet

Abbiamo due protocolli

- TCP (Transmission Control Protocol)

- UDP (User Datagram Protocol)

TCP ha il concetto di "connessione", UDP no, ma entrambi vengono usati per compiere delle sessioni!

TCP, l'abbiamo già visto, è connection-oriented, reliable, robusto

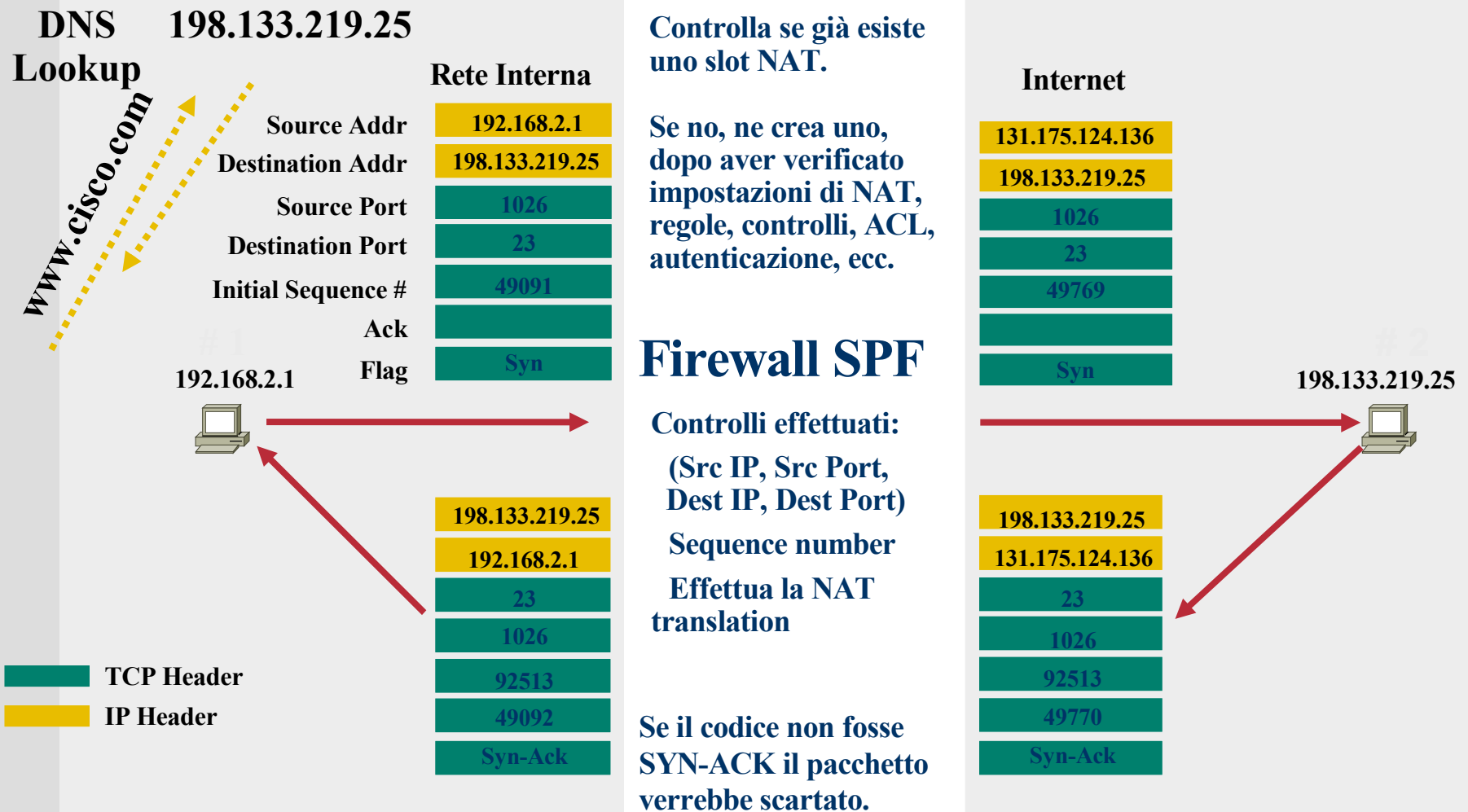
- Numeri di sequenza e di acknowledge

- Macchina a stati ben definita (open connection, data flow, retransmit, close connection)

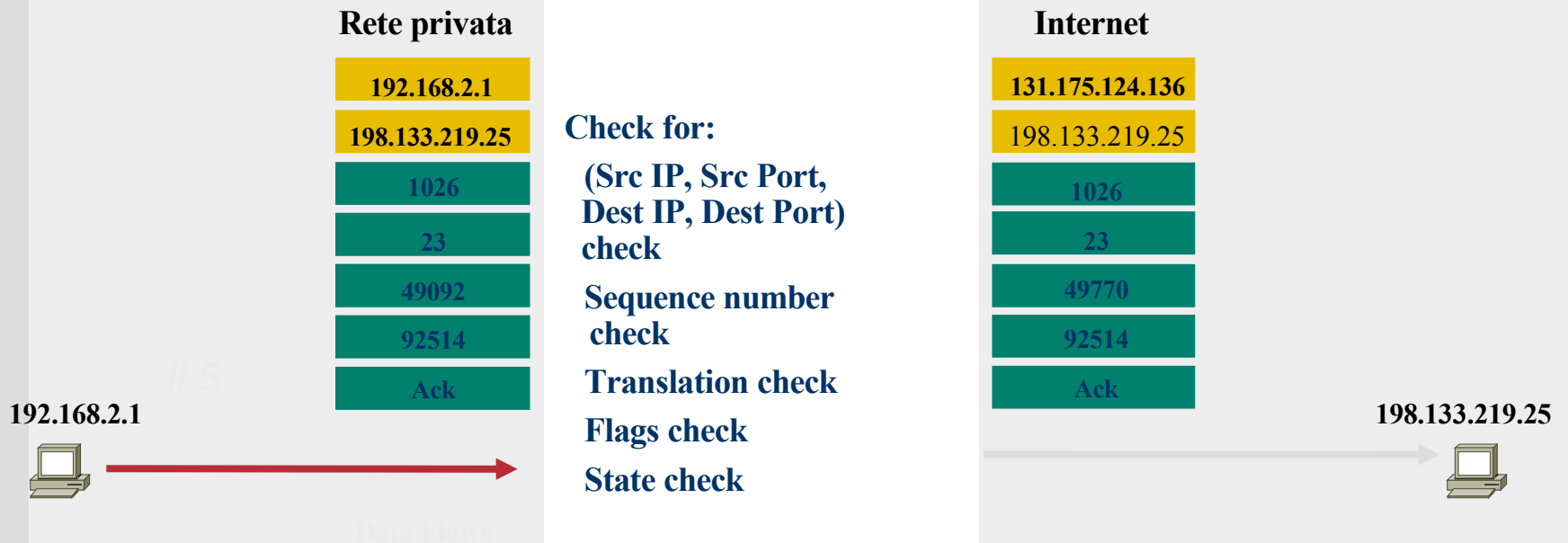
- Meccanismo, implicito o esplicito, per gestire la congestione



Inizializzazione di sessione TCP con NAT



La connessione continua...



TCP Header
IP Header

E nel caso di UDP ?



Protocollo privo di connessioni

Efficiente, viene usato da vari servizi

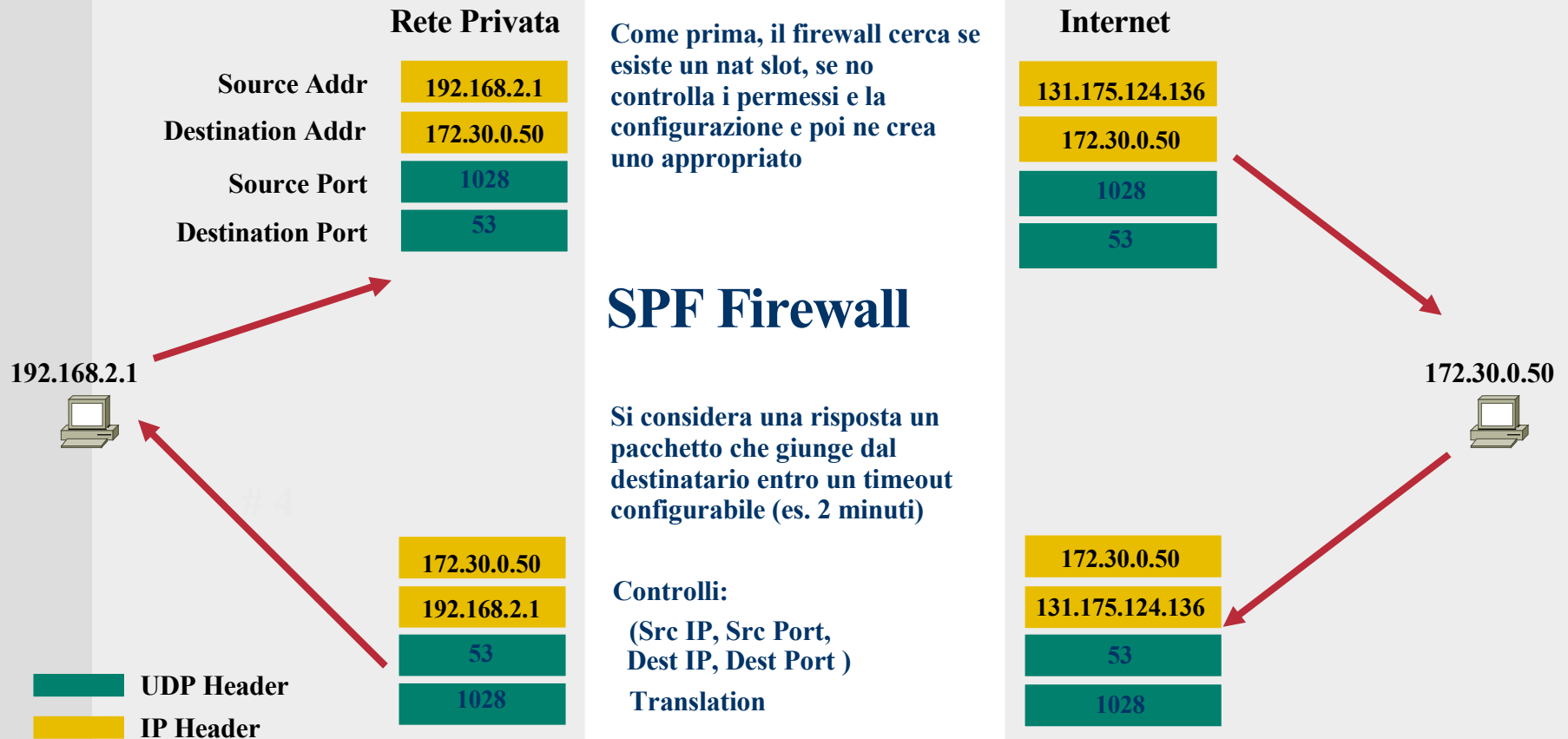
- Servizi di rete: DNS

- Servizi dove le performance servono: VoIP H.323, streaming video

Non si può chiudere a priori, ma difficile da rendere sicuro

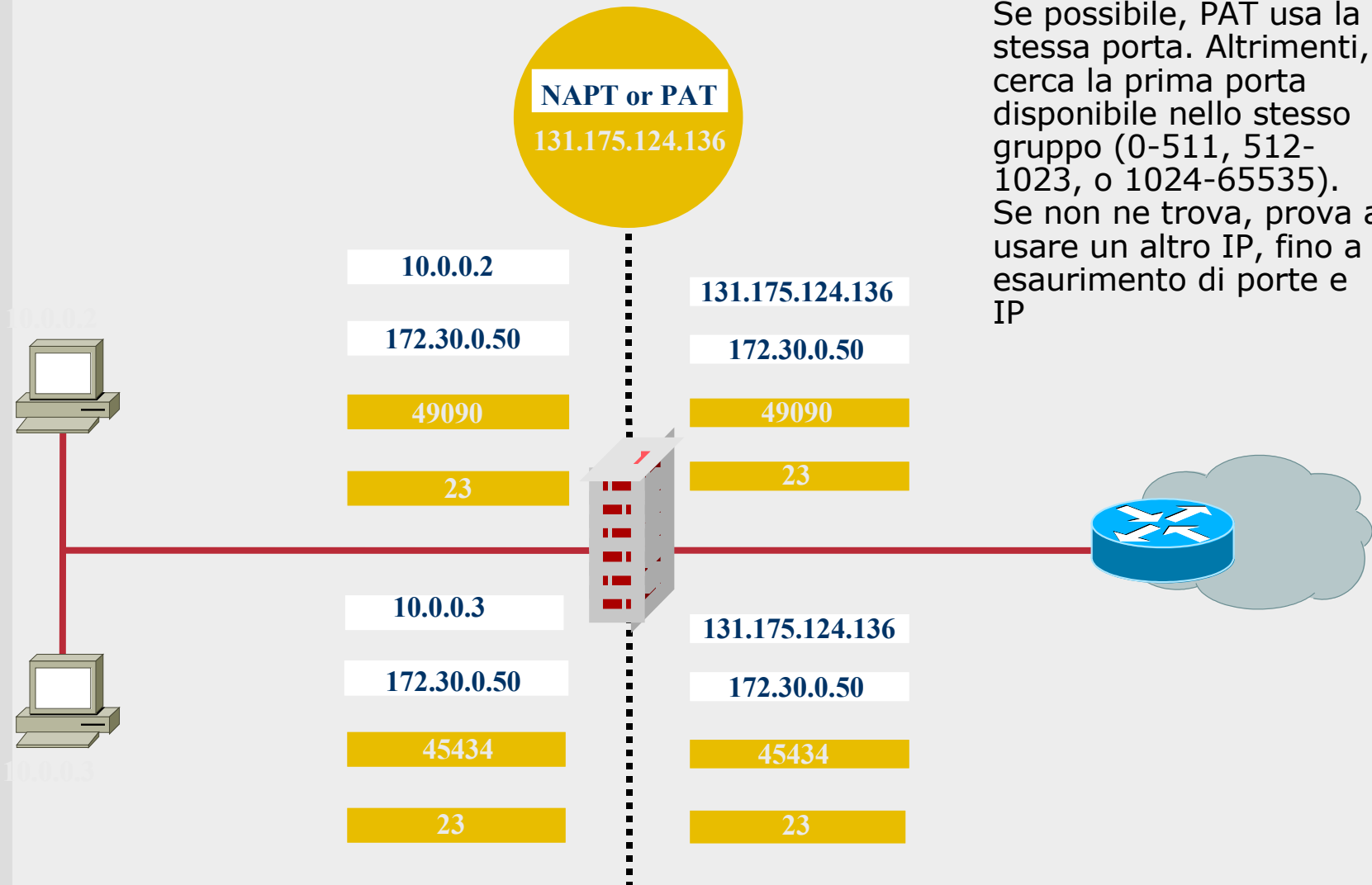
Esiste comunque il concetto di "sessione", e si può usare per NAT e controlli

UDP e NAT intelligente



Port Address Translation—Condivisione di un singolo IP

Se possibile, PAT usa la stessa porta. Altrimenti, cerca la prima porta disponibile nello stesso gruppo (0-511, 512-1023, o 1024-65535). Se non ne trova, prova a usare un altro IP, fino a esaurimento di porte e IP





Ispezione a application layer: FTP

Nel caso di alcuni protocolli è necessaria una ispezione a livello applicativo dei contenuti

Ad esempio, nel caso dell'FTP, è necessaria per

- Preparare le connessioni dinamiche secondarie

- Tracciare le risposte ai comandi FTP

- Generare dati di log

- Effettuare conversioni con il NAT all'interno del protocollo

Preparazione delle connessioni dinamiche

FTP usa canali secondari dinamici per le connessioni

Vengono allocati per:

- Upload di file

- Download di file

- Comandi "DIR", "LS" e simili

FTP in modalità standard

Due canali

Canale comandi inizializzato dal client

Canale dati inizializzato dal server

Connessioni "outbound" (client dietro il firewall)

Devo poter effettuare la connessione outbound verso la porta 21

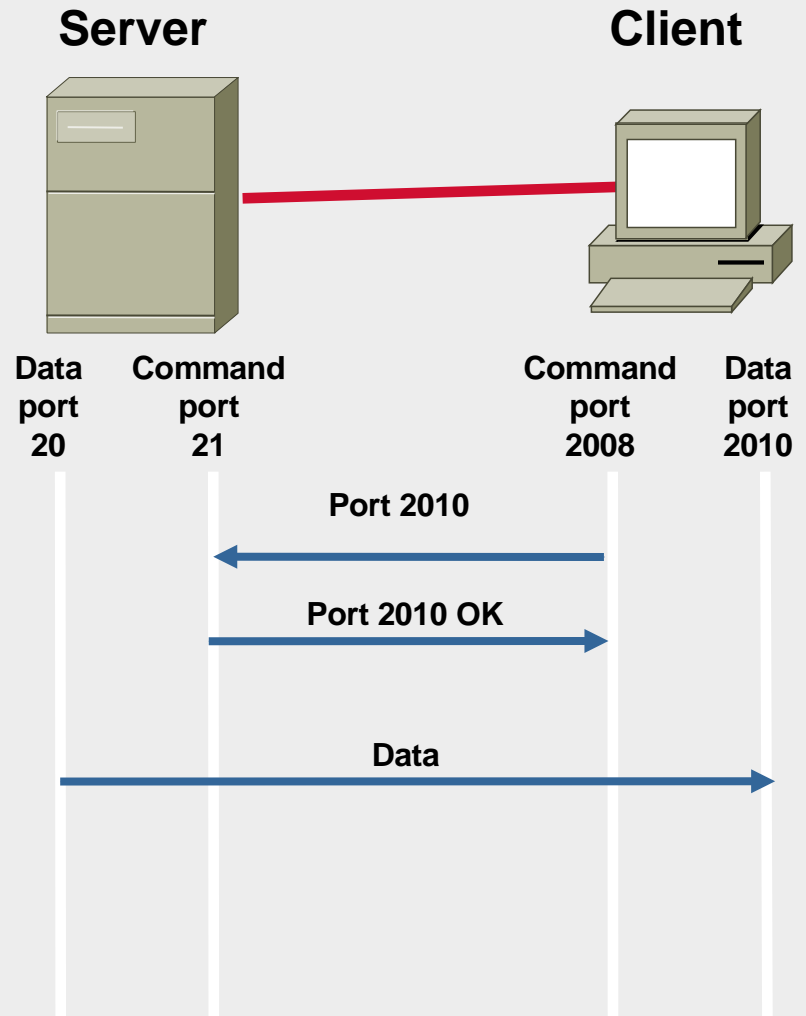
Devo aprire una porta temporanea inbound per la connessione dati

Se uso NAT: il dispositivo NAT deve riconoscere il contenuto della connessione e aprire la porta

Connessioni "inbound" (server dietro al firewall)

Deve essere abilitata la porta 21 sempre

Se al server è consentito iniziare connessioni, nessun'altra regola
Altrimenti, devo aprire una regola temporanea per la connessione outbound



FTP Server in modalità passiva

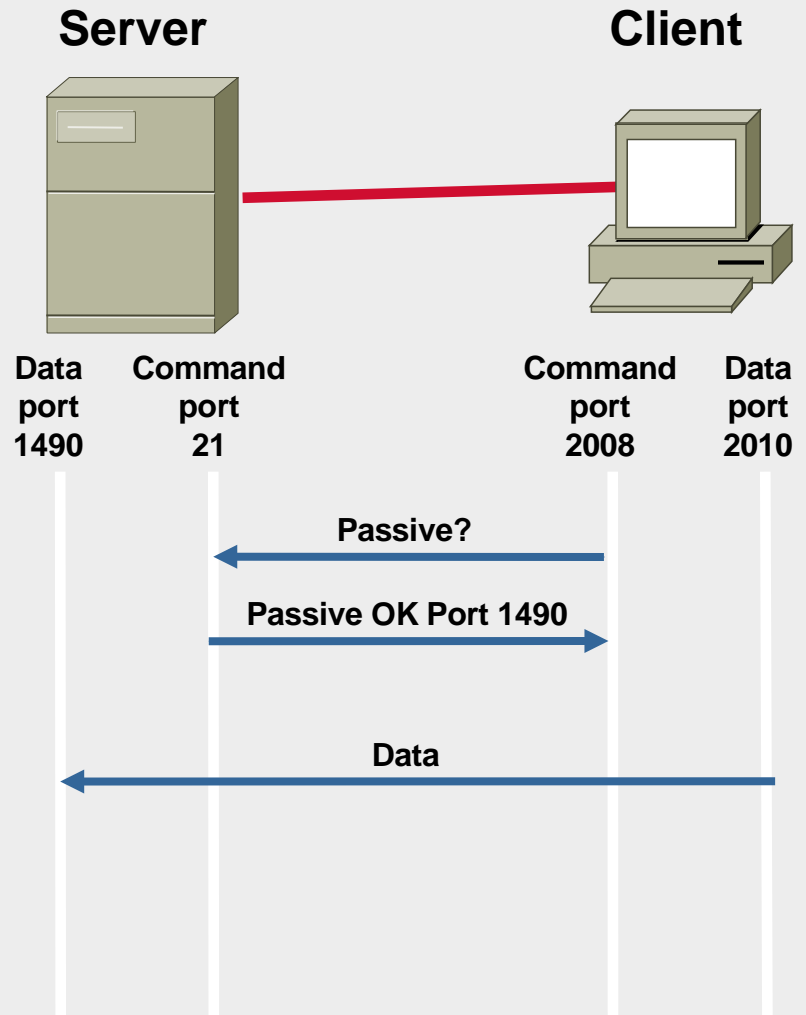
Due canali, sia comandi sia dati,
iniziati ENTRAMBI dal client
Connessione outbound (client
dietro il firewall)

Se le connessioni verso l'esterno
sono consentite, tutto ok

Altrimenti, deve venire aperta
una porta per entrambe le
connessioni verso l'esterno

Connessione inbound (server
dietro il firewall)

Deve venire aperta una porta
temporanea



RealNetworks RDT Mode



Tre canali !

- Control connection (TCP)

- UDP data (UDP)

- UDP resend (UDP)

Connessione outbound (client dietro al firewall)

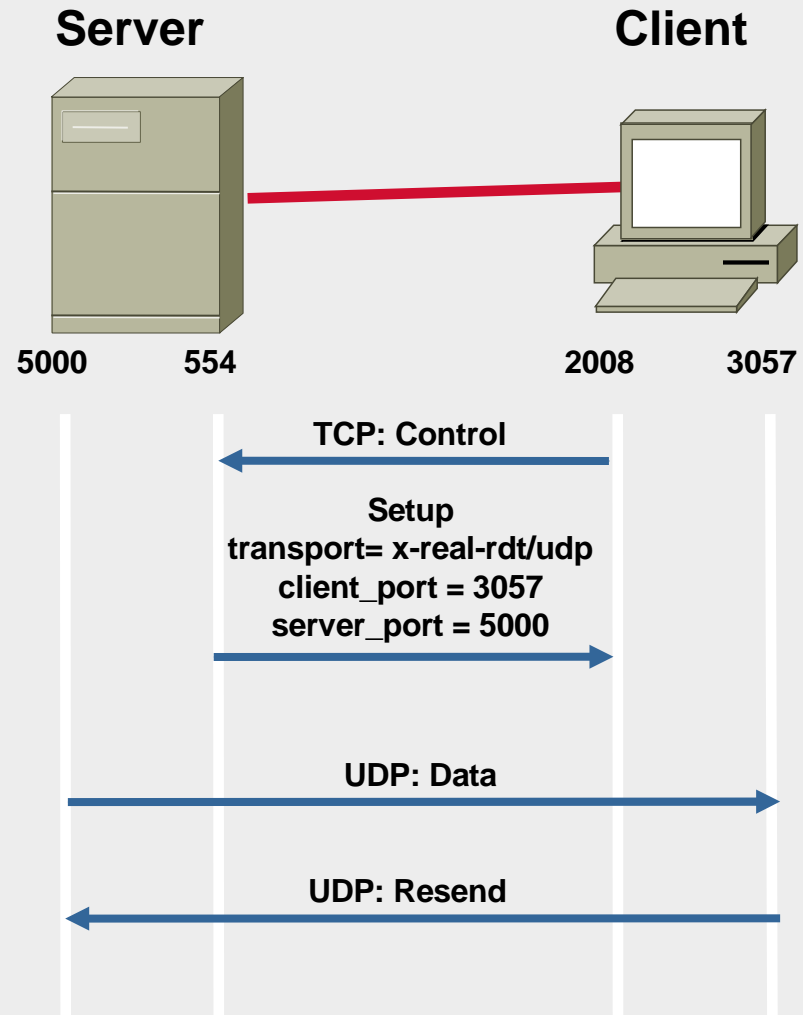
- Se il traffico outbound è consentito, devo solo aprire la porta per UDP data

- Altrimenti devo anche aprire la porta per UDP resend e TCP control temporanee

Connessione inbound (server dietro al firewall)

- Se il traffico outbound è consentito, deve essere aperta la porta per TCP control e una porta temporanea per UDP resend

- Se no, devo aprire anche una porta temporanea per UDP data



Ispezione ad application layer – FTP (2)



Controlla la sequenza di comandi FTP sulla control connection, per evidenziare comportamenti anomali:

- Comandi troncati

- Comandi che terminano inaspettatamente

- Spoofing di risposte/comandi

- Editing del TCP stream

- Scambi di porte non valide

- Uso della pipeline nei comandi

Generazione di log

- Generazione di un record di tutti i file trasferiti

- Registrazione dei motivi per cui l'attivazione del canale secondario è fallita

NAT dell'indirizzo IP contenuto nell'applicazione

- Il comando PORT contiene indirizzi IP che devono essere tradotti

- Application Inspection + NAT abilitano questo

Vantaggi di firewall packet filter

Più veloci ed efficienti delle altre tecnologie

Versatili e adattabili

Possono supportare praticamente qualsiasi protocollo in modo trasparente

Possono consentire l'ispezione ad application layer

Il loro livello di sicurezza, se ben configurati, è perfettamente equivalente a quello di tecnologie ad application layer



Firewall su Application Layer

Circuit Firewall

Application e Proxy Firewall

Circuit Firewall



Fa un relay delle connessioni TCP

Client si connette a una porta TCP del gateway,
che si connette all'indirizzo e alla porta del server

In generale non c'è ispezione del payload del
traffico

Creando per conto del client il circuito virtuale,
controlla la connessione

- Legittimità dell'handshake

- Non forwarda dati fino alla chiusura del 3-way
handshake

Controlla i pacchetti, che possono essere solo:

- Connection request, oppure

- Pacchetti che appartengono a connessione già attiva

Come funziona ?



Il firewall gestisce una tabella di connessioni valide, con:

- L'indirizzo sorgente della connessione

- L'indirizzo destinazione della connessione

- Lo stato della connessione: handshake, established, o closing

- I numeri di sequenza (ACK)

- L'interfaccia fisica da cui i pacchetti entrano

- L'interfaccia fisica da cui i pacchetti escono

I dati vengono fatti passare se combaciano con una delle entry nella virtual circuit table

Quando una connessione termina, viene rimossa la entry

SOCKS: un esempio di Circuit Firewall

Richiede che vengano modificate le applicazioni
(potreste aver visto le impostazioni)

Sostituisce la libreria con delle

chiamate

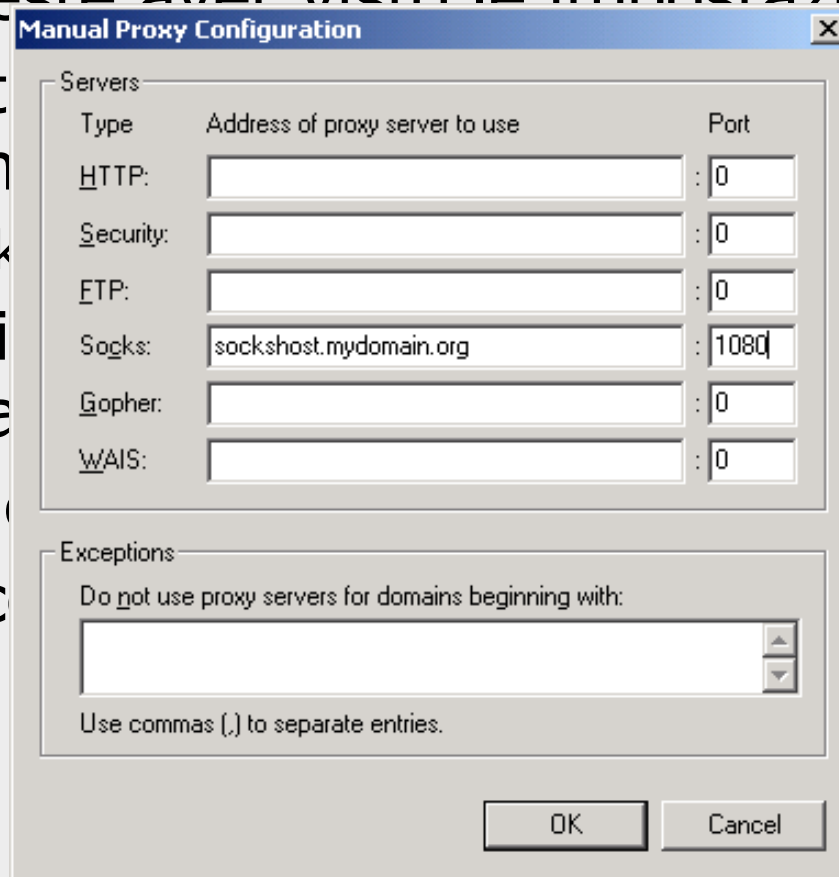
Socks

Le chiavi sono col SOCKS

firewall sessioni virtuali

Può gestire ICMP

Non cambia IP



The image shows a 'Manual Proxy Configuration' dialog box. It has a title bar with a close button. The main area is divided into two sections: 'Servers' and 'Exceptions'. The 'Servers' section contains a table with columns 'Type', 'Address of proxy server to use', and 'Port'. The 'Exceptions' section contains a text box for domains and a note about using commas to separate entries. At the bottom are 'OK' and 'Cancel' buttons.

Type	Address of proxy server to use	Port
HTTP:		0
Security:		0
FTP:		0
Socks:	sockshost.mydomain.org	1080
Gopher:		0
WAIS:		0

Exceptions

Do not use proxy servers for domains beginning with:

Use commas (,) to separate entries.

OK Cancel



Pro e contro dei Circuit Firewall

Inizialmente limitati a TCP, possono essere estesi

Spesso richiedono di modificare le applicazioni!

Non validano payload e protocolli applicativi,
possono essere molto veloci e performanti

Tipicamente non fanno content inspection

- Niente URL filtering

- Non gestiscono autenticazione

Application Proxy Firewall

Controlla che i dati siano validi anche a livello del protocollo applicativo

- Valida il protocollo in sé

- Valida oggetti con requisiti di sicurezza all'interno del layer applicativo (per esempio password e richieste di servizi)

Spesso non è del tutto trasparente all'utente e/o alle applicazioni

- Richiede qualche modifica alle applicazioni, a parte eccezioni

- Richiede servizi proxy specifici per ogni protocollo applicativo

Può effettuare autenticazione degli utenti e applicare politiche specifiche

Viene spesso integrato con varie funzioni di filtraggio dei contenuti

I proxy per la sicurezza

I proxy presentano agli utenti un sottoinsieme ridotto e sanitizzato dei servizi offerti dal server

Possono essere usati sia per difendere gli utenti interni che accedono a server esterni, che per difendere i server dall'accesso di utenti esterni ("reverse proxy")

Serve un proxy diverso per ogni protocollo

Solitamente vengono implementati su server che usano sistemi operativi general purpose, non su hw/sw dedicati

Le performance non sono ottimali, il flusso applicativo viene ricostruito due volte

Sono, di per sé, molto sicuri, ma essendo installati su un sistema generico possono essere vulnerabili agli stessi attacchi che affliggono quel sistema operativo

Un esempio di proxy HTTP

www.cisco.com

198.133.219.25

DNS Lookup

Proxy
Client

Application
Protocol
Analysis

Proxy
Server

Public Network

GET /index.html



HTTP: ---- Hypertext Transfer Protocol

HTTP:

HTTP: Line 1: HTTP/1.0 302 Found

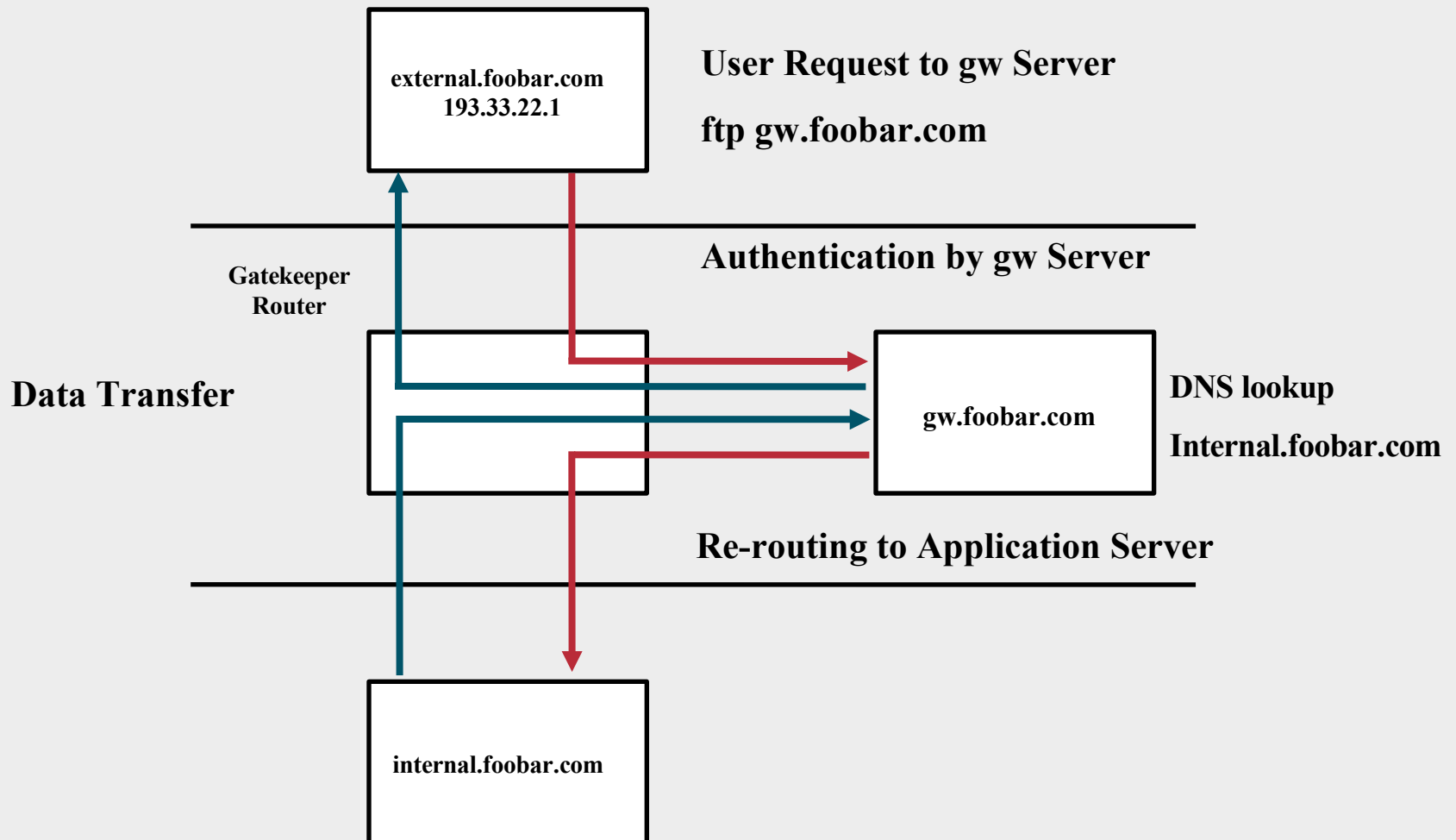
HTTP: Line 2: Server: Netscape-
Enterprise/2.01

HTTP: Line 3: Date: Tue, 08 May 2001
20:52:20 GMT

GET http://www.cisco.com/index.html



Reverse proxy che difende un servizio





FTP attraverso un server proxy

```
<external.user: 63> ftp gw.foobar.com
Connected to gw.foobar.com.
220- gw.foobar.com FTP server ready.
After logging in, use 'site machine' to connect to the desired machine.
220 Time is 1992/07/24 16:48:21 GMT
Name (gw:user): user
331 Password required for user.
Password: password_on_the_gatekeeper_server
230 User user logged in. Please select your host.
Remote system type is UNIX.
ftp> site internal.foobar.com
220 internal FTP server (NCC-1701) ready.
ftp> user user
331 Password required for user.
Password: password_on_internal
230 Welcome on this ftp server : user.
ftp>
```



Telnet attraverso un server proxy

<externalhost.user: 63> telnet gw.foobar.com

Trying...

Connected to gw.foobar.com.

Escape character is '^['.

Gw.foobar.com

login: user

Password: *password_on_the_gatekeeper_server*

Host: internalhost.foobar.com

Access authorized

UNIX(r) System V Release 4.0 (itesec)

login: user

Password: *password_on_the_final_station*

UNIX System V Release 4.0 AT&T NEWS3400

internalhost

Copyright (c) 1984, 1986, 1987, 1988 AT&T

All Rights Reserved

Last login: Mon Jul 13 11:56:28 from someplace.foobar.com

<internalhost.user: 346>



Vulnerabilità dei proxy

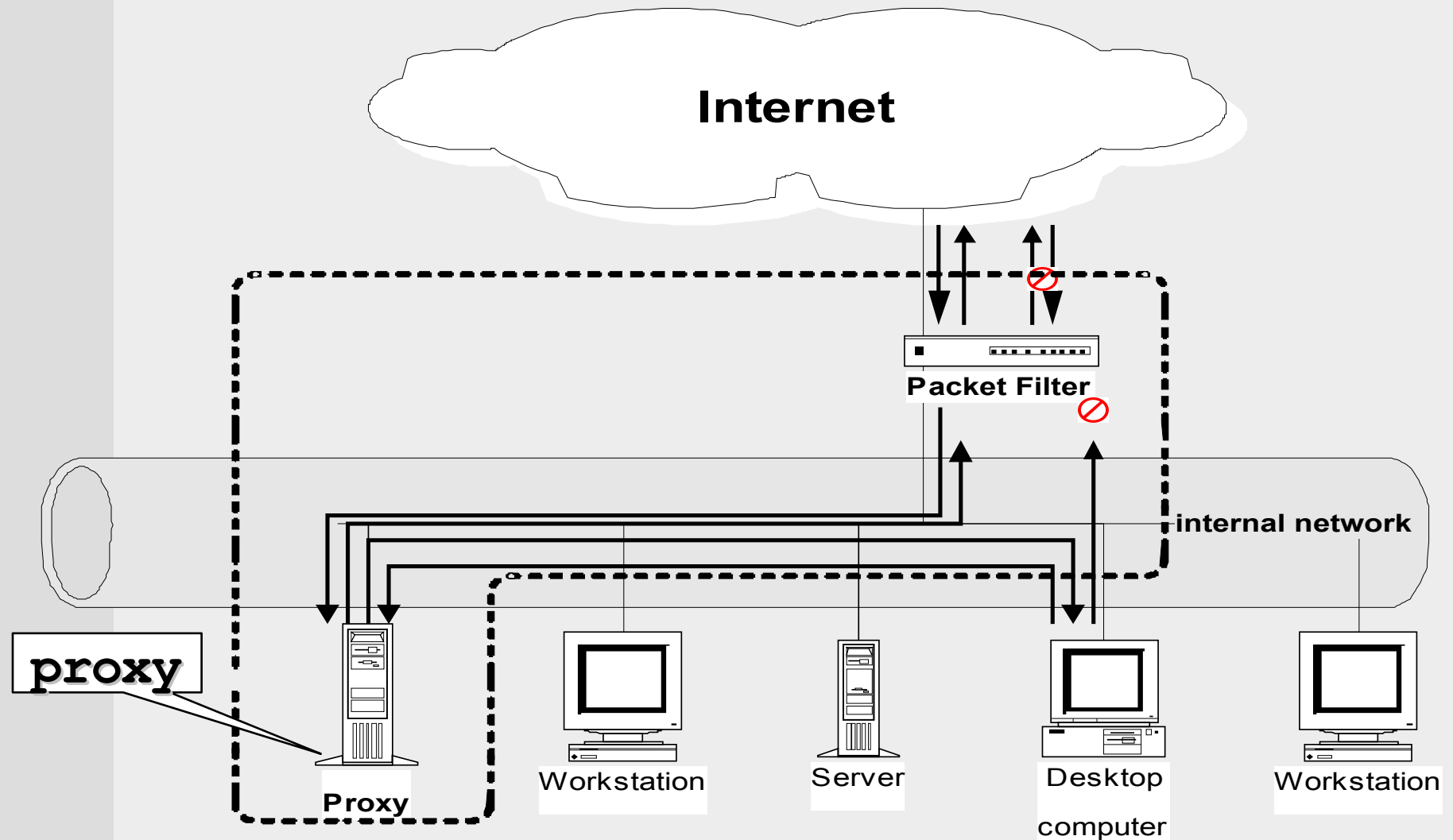
Gran parte dei firewall ad application layer si basano fortemente sul sistema operativo: uso di NDIS, TCP/IP, WinSock, Win32 sotto Windows, uso delle librerie di sistema sotto Linux; uso delle librerie standard C e/o C++ ...

Un bug in una delle librerie condivise può influire sul comportamento del proxy!

Inoltre, i proxy tipicamente non si occupano dei contenuti degli header a livello più basso, i.e. di fronte a un proxy probabilmente è meglio disporre un packet filter

Si può impostare il packet filter in modo da accettare le connessioni solo se originate dal proxy

Proxy e packet filter in cascata





Proxy Firewall: vantaggi e svantaggi

Vantaggi

- Logging

- Caching

- Autenticazione e autorizzazione

- Politiche basate su utenti/gruppi di utenti

- Mascheramento della struttura della rete (come NAT)

- Filtraggio su contenuti, su URL, ecc.

- Protezione per applicativi "deboli"

Svantaggi

- Scalabilità problematica

- Servizi nuovi richiedono proxy nuovi

- Servizi custom richiedono proxy custom

- Modifiche sul client per il supporto



Architettura a due zone

Accesso alla LAN da Internet



Nella maggioranza dei casi, le intranet aziendali presuppongono che la maggior parte degli utenti sia collocata all'interno del firewall aziendale, e che quasi nessuna connessione giunga dall'esterno

Due problemi violano questo principio

- Utenti remoti che vogliono accedere a servizi pubblici dell'azienda (web, FTP, invio di posta...)

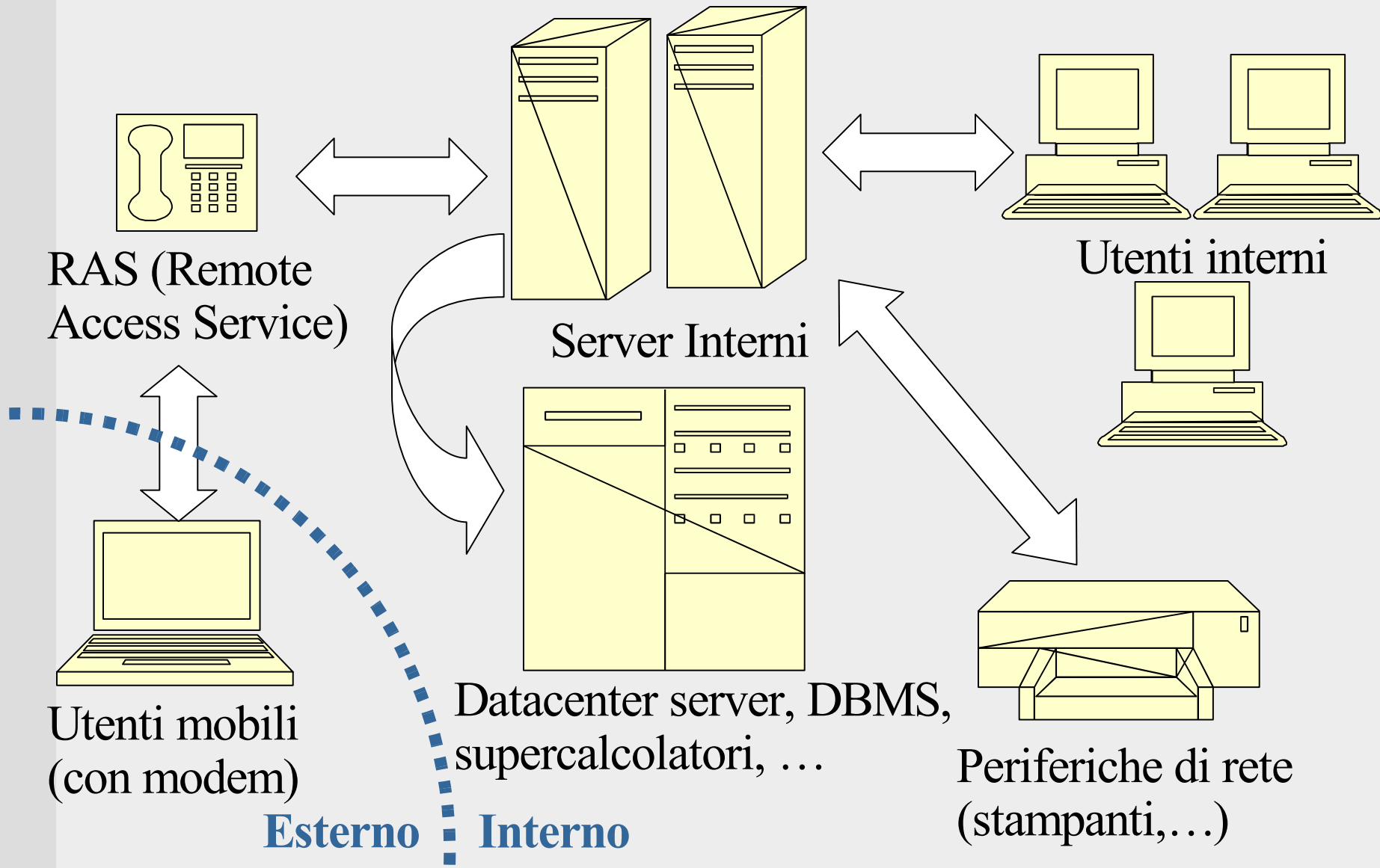
- utenti remoti vogliono accedere alla rete aziendale attraverso Internet o una rete non sicura

Esistono delle soluzioni per ciascuno dei problemi

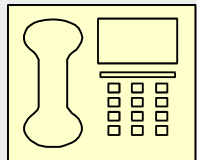
- Architettura a due livelli della rete

- Reti private virtuali (VPN)

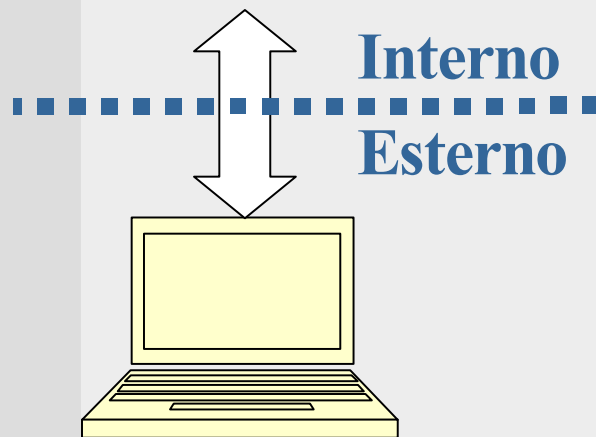
Struttura di una rete aziendale pre-Internet



Sicurezza “prima di Internet”



RAS (Remote Access Service)



Utenti mobili
(con modem)

- Schema di sicurezza di una vecchia rete:
 - Ciò che è “interno” è fidato
 - Ciò che è “esterno” va autenticato
- Autenticazione sui servizi RAS (Accesso Remoto), inizialmente con una semplice coppia login/password
- A volte a questo impianto basilare vengono aggiunti dei “privilegi” d’accesso alle risorse, anche per gli utenti interni (già sui primi sistemi multiutente 20 – 30 anni fa)

Nello scenario di rete che abbiamo presentato:

- I demoni offrono i loro servizi solo all'interno, quindi solo ad utenti già autenticati

- A controllare l'accesso dall'esterno è un RAS, molto semplice e quindi difficile da imbrogliare

- I server di rete sono pochi e ben controllati

- Gli utenti sono "ben addestrati" all'utilizzo del sistema UNIX

Paradossalmente, le vecchie reti aziendali erano meno a rischio di quelle moderne !

Bastava essere sicuri che nessuno potesse entrare via RAS con qualche password troppo banale...

Vi ricordate "War Games" (film) ? Questi erano quei tempi eroici !

Con internet i problemi si complicano...



Al traffico precedente:

- “interno per l'interno”

- “dall'esterno verso l'interno” (che viaggia ora attraverso Internet, non direttamente a un RAS)

Si aggiungono:

- traffico “dall'interno verso l'esterno” (es. navigazione, mail degli utenti in lan)

- Traffico generato dai server societari:

 - dall'esterno verso i server (richiesta pagine web, mail in ingresso)

 - Tra i server di front end e i server di back end (per es. ricerca dati sul DBMS)

 - Il server web potrebbe avere zone riservate ai dipendenti (la intranet aziendale) e zone ad accesso libero...

Per il traffico “interno” e i demoni sui server “interni” valgono le osservazioni fatte in precedenza !

Attenzione però ! L'introduzione di piattaforme Windows e DOS nel lavoro di ufficio diminuisce la capacità tecnica degli utenti !

Per il resto del traffico quelle quelle osservazioni non valgono:

I demoni per definizione eseguono richieste di utenti non autenticati (pensate al demone del servizio web!)

Gli accessi sono tanti e in continua crescita, sia per numero che per complessità

L'esigenza dell'efficienza e dei tempi di servizio (time to serve / time to market) si fa sentire più che in una rete “interna”



Architettura di intranet a due zone

Creazione di una rete semipubblica tra intranet e Internet (Zona Demilitarizzata, DMZ)

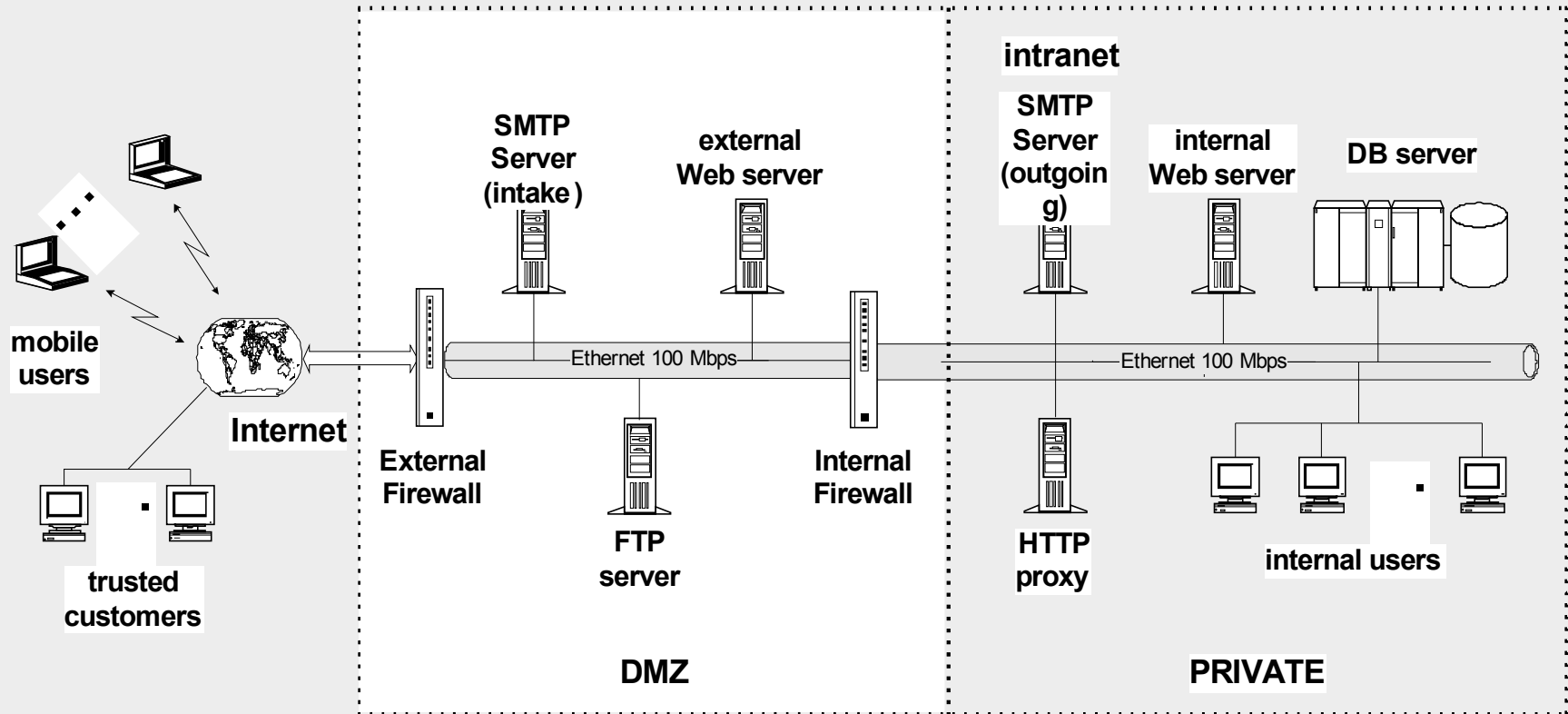
Idea di base: gli utenti esterni possono accedere alla DMZ (limitatamente ai servizi disponibili). Le risorse interne restano nella zona privata e non sono accessibili.

Nella DMZ si ospitano i server pubblici (sito Web, server FTP, DNS, mailserver in ingresso...) che non erogano applicazioni critiche per l'azienda

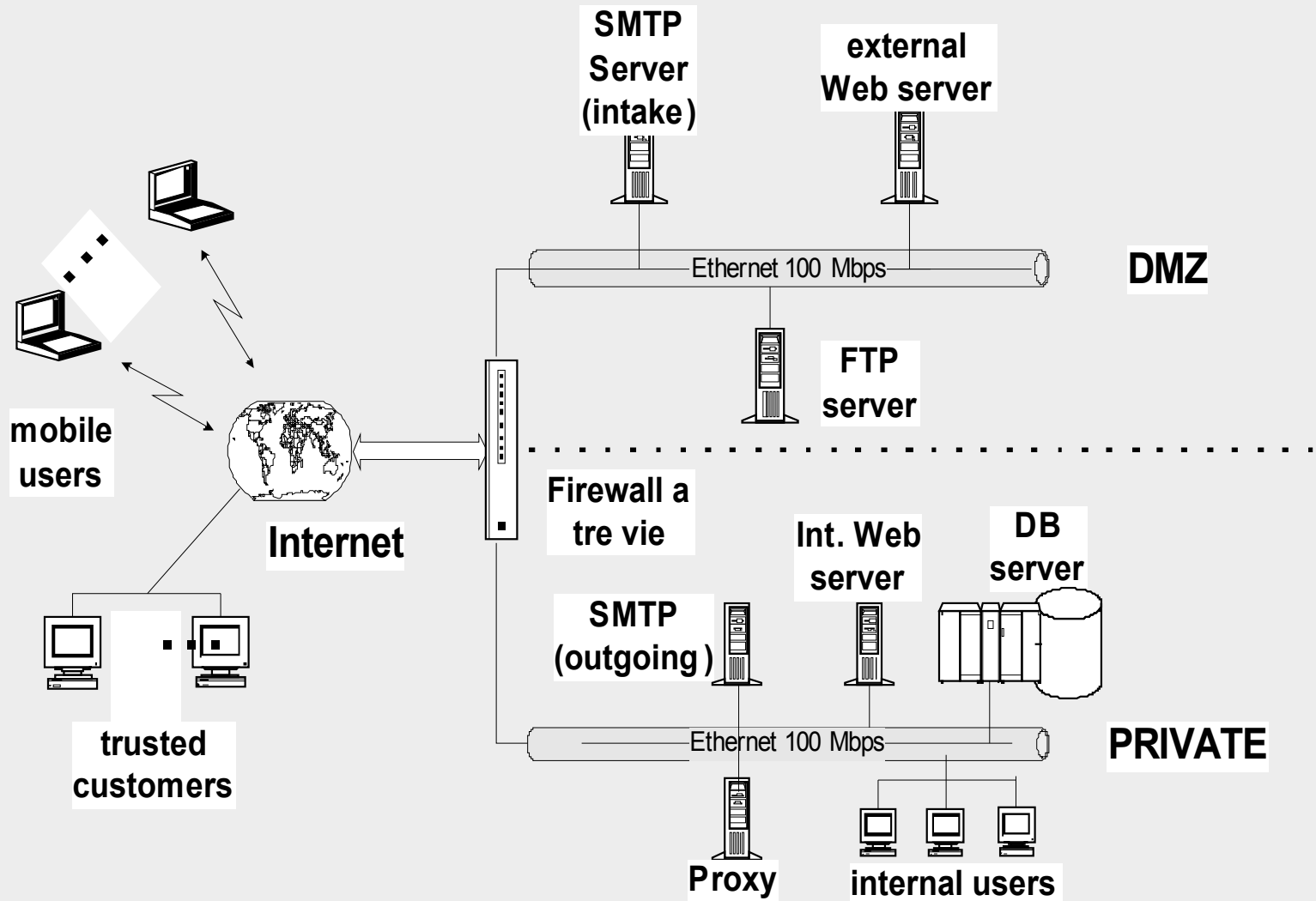
Si usano due firewall dual-homed (o due router) per dividere le zone. In alternativa, un singolo firewall a "tre vie" (o più)

La zona "demilitarizzata" è una zona ad altissimo rischio. Le comunicazioni in arrivo dalla DMZ vanno considerate inaffidabili quanto quelle esterne.

Architettura a due zone



Architettura a due zone (con firewall a tre vie)





Accesso sicuro alle reti remote: VPN

Cos'è una VPN



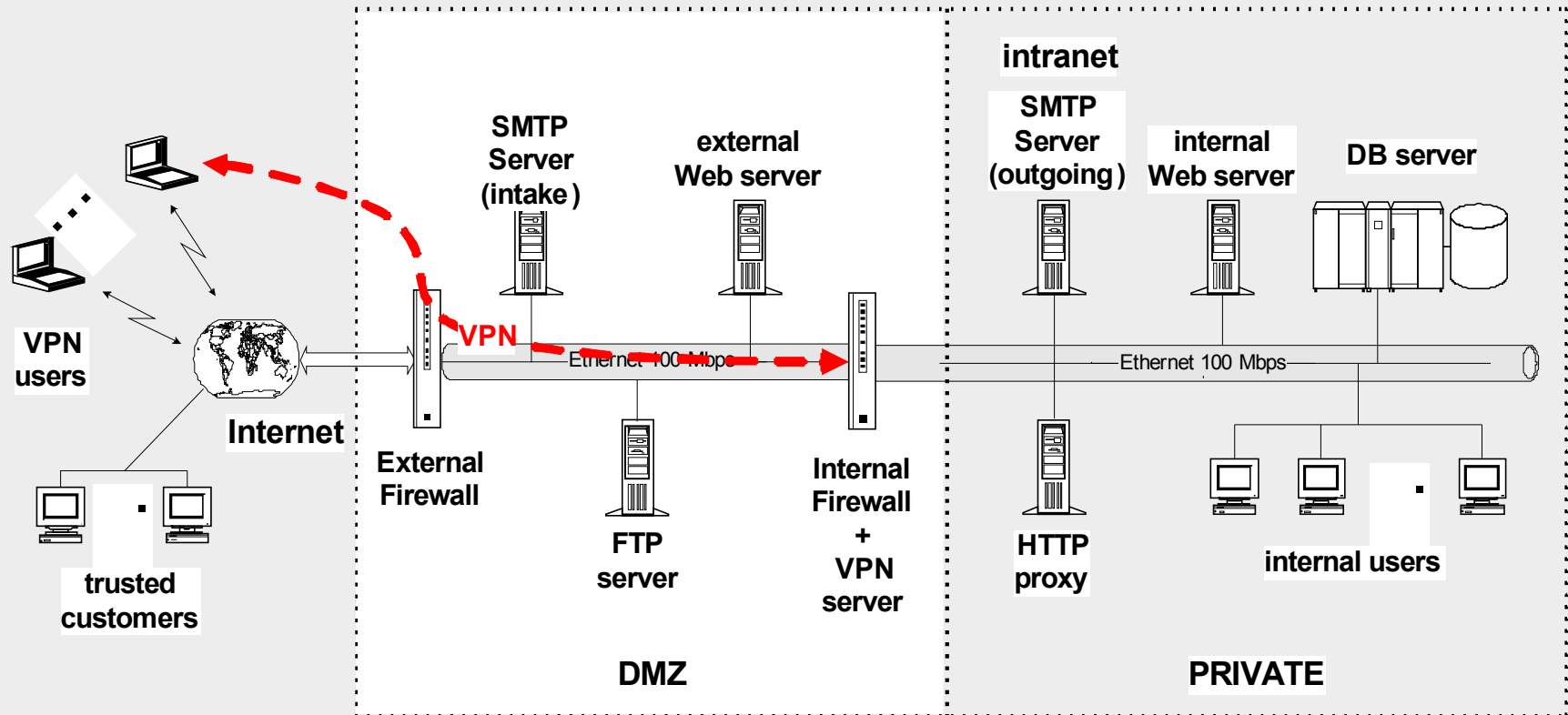
Esigenze:

1. Comunicare da remoto con la rete aziendale, accedere a risorse interne, come se si fosse in ufficio
2. Collegare tra loro sedi periferiche senza spendere capitali in costose linee dedicate
3. Garantire confidenzialità ed integrità ai dati trasmessi su rete pubblica non sicura

VPN, Virtual Private Network: ponte dati crittografato su rete pubblica

Molteplici tecnologie realizzative, ma il concetto di base è sempre lo stesso

Architettura a due zone (con VPN)



Due politiche possibili per la VPN

“tutto il traffico va nel tunnel”

Moltiplicazione del traffico: una richiesta internet dal client entra nel tunnel, attraversa il firewall, passa per il NAT ed esce di nuovo verso internet

Impatto su CPU del firewall/VPN server

Singolo punto di controllo, applicazione di tutte le security policy corporate

“split tunnelling”

Traffico per la rete aziendale entra in VPN, traffico Internet direttamente verso l'ISP

Più efficiente, ma meno controlli

Attaccando il computer tramite la connessione ad Internet si può compromettere la VPN

PPTP

Point-to-point tunnelling protocol, un protocollo proprietario di Microsoft

IPSEC

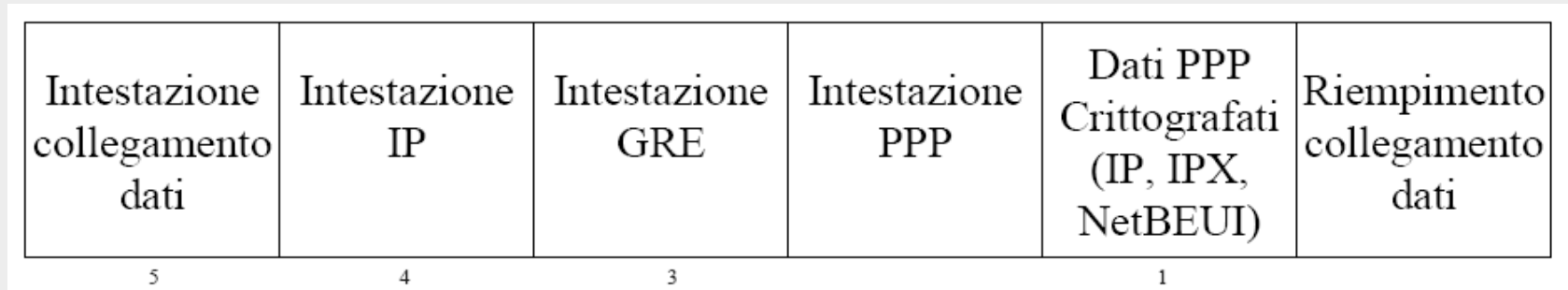
Estensioni di sicurezza del protocollo IPv6, esistono anche per IPv4

Autenticazione e crittografia a livello IP

VPN su SSL / Tunnel SSH

Approfondiremo il protocollo quando parleremo di SSL
Ci limitiamo a vederne l'utilizzo

Struttura pacchetto:



Quando i pacchetti raggiungono la destinazione:
le intestazioni vengono rimosse una alla volta in ordine inverso.
i dati PPP vengono decrittografati

- 1) Creazione struttura PPP, incapsulando i dati PPP crittografati con un header PPP
- 2) Incapsulamento struttura PPP con header GRE (Generic Routing Encapsulation)
- 3) Incapsulamento del pacchetto risultante con header IP
- 4) Incapsulamento del datagramma IP risultante con header e trailer del data link layer in uso (es. Ethernet)

IPSec: componenti fondamentali



AH (Authentication Header)

autenticazione e integrità

ESP (Encapsulating Security Payload)

Autenticazione, integrità e riservatezza

IKE (Internet KeyExchange)

definizione dei parametri di sicurezza,
generazione, rinnovo e scambio delle chiavi
utilizzate

ISAKMP (Internet Security Association and Key Management Protocol)

definizione dei parametri di sicurezza,
generazione, rinnovo e scambio delle chiavi
utilizzate



Security Associations

Le Security Association (SA) contengono le informazioni necessarie per l'esecuzione dei servizi IPSec

Una SA è una connessione unidirezionale che definisce i servizi di Ipsec usati dal traffico che viaggia attraverso di essa.

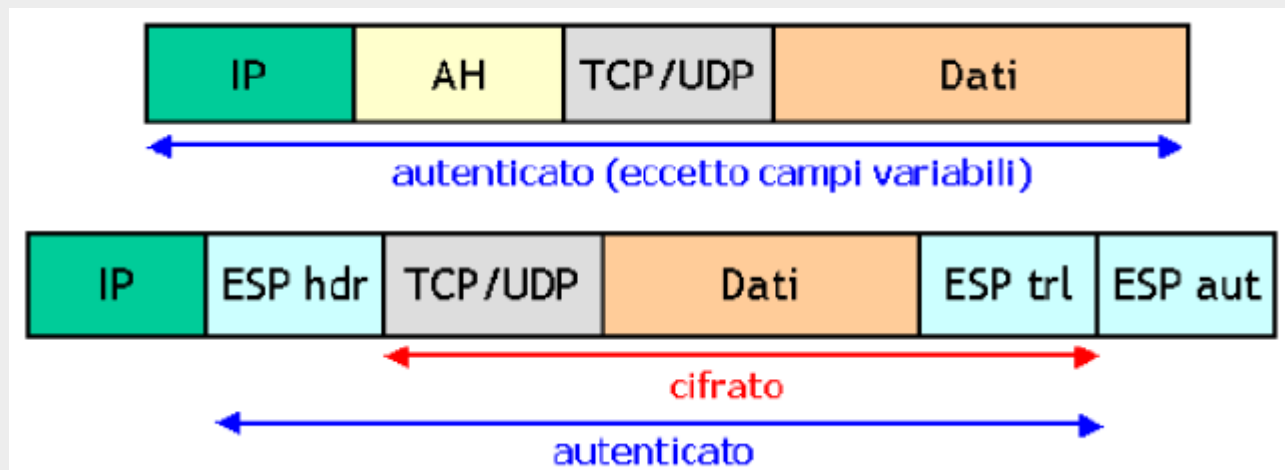
Si può specificare l'uso del protocollo AH o ESP, ma non di entrambi, e l'eventuale tunnelling

Per rendere sicura una comunicazione bidirezionale tra due host o tra due gateway sono necessarie due SA, una in ciascuna direzione.

IPSec: modalità di trasporto

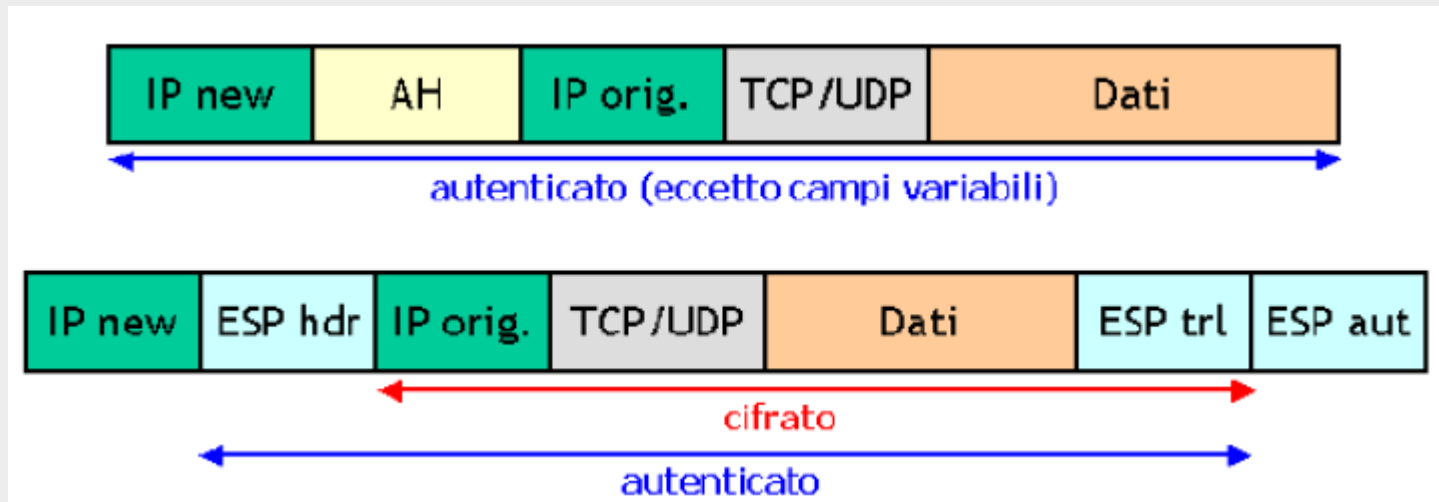
SA possibile solo tra due host e non tra due "security gateway"

gli header AH e/o ESP vengono inseriti tra l'header IP e l'header di trasporto



IPSec: modalità tunnel

Possibile solo tra security gateway
l'intero pacchetto IP originale viene incapsulato in
un nuovo pacchetto



IPSec : Funzionamento



I Fase:

scelta possibili protocolli crittografici e di sicurezza (AH / ESP) da utilizzare nelle comunicazioni

scambio chiave Master, da cui verranno derivate le chiavi da utilizzare per la cifratura e il calcolo dei MAC
verifica identità delle due parti

II Fase (gestione comunicazione):

scelta protocollo comune

scelta chiavi