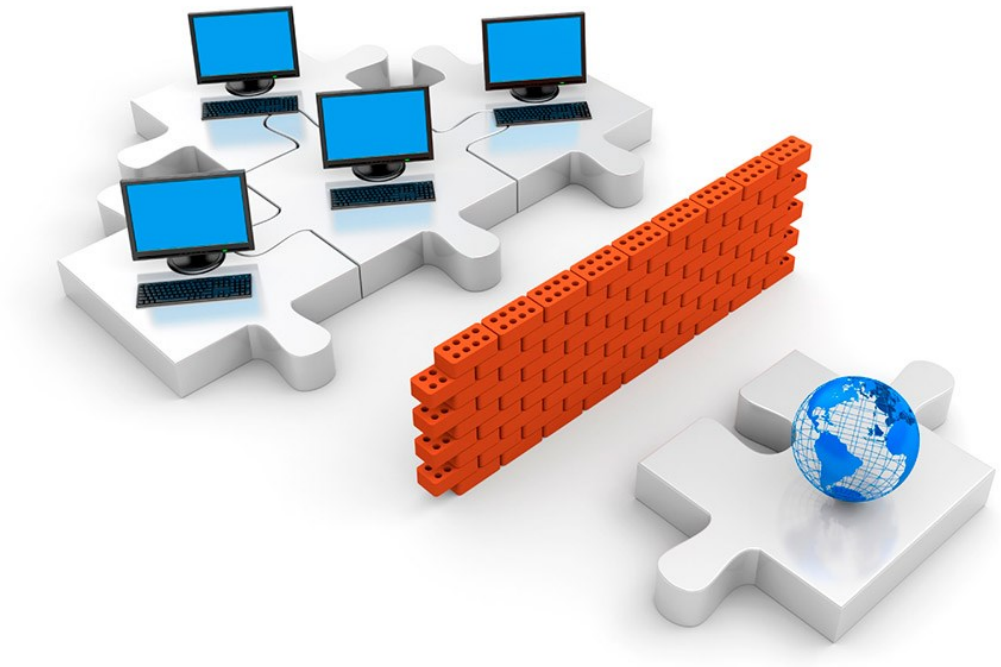
Sicurezza delle reti



Vincenzo Calabrò

IANA

http://www.iana.org/assignments/ipv4-address-space

In tempo recenti, con la diffusione della *best practice* indicata dalla RFC 1918, molte grandi Organizzazioni hanno “restituito” i loro indirizzi IP (specie quelli della classe A) allo IANA.

Lo IANA gestisce anche l’assegnazione di:

- Toplevel Domains
- Private Enterprise SNMP Numbers
- Protocol Numbers
- PPP Numbers
- Multicast Addresses
- MIME Types
- Port Numbers

IP Addressing: CIDR e RFC 1918

Situazione un po' di tempo fa (RFC 1466: guidelines for Management of IP Address Space)

	Total	Allocated	Allocated (%)
Class A	126	49	38%
Class B	16383	7354	45%
Class C	2097151	44014	2%

Table 1: Network Number Statistics (May 1992)

Nel classful addressing la assegnazione degli indirizzi IP era effettuata sulla base della dimensione dell'Organizzazione richiedente:

… meno di 512 indirizzi → due Classi C contigue…

CIDR

I problemi del classful addressing erano sostanzialmente tre:

- *Esaurimento delle reti di classe B*
- *Sovraccarico delle informazioni di routing*
- *Esaurimento dello spazio di indirizzamento*

Il *Classless Inter-Domain Routing viene incontro ai primi due problemi (RFC 1517, RFC 1817)*

CIDR

Il *Classless Inter-Domain Routing* è definito nelle RFC 4623 (*CIDR: the Internet Address Assignment and Aggregation Plan*; ha recentemente superato la RFC 1519 originale)

La "notazione CIDR" è comunque comoda anche a chi non si occupa quotidianamente di routing. Può essere di tipo classico

192.24.8.0/255.255.248.0

oppure compatto

192.24.8.0/21

RFC 1918

E' una *best current practice* di Internet e descrive gli indirizzi IP da usare nelle Organizzazioni private. I sistemi di un'Organizzazione sono classificati in tre classi:

- Quelli che non hanno bisogno di comunicare con l'esterno
- Quelli che accedono a un numero limitato di servizi esterni
- Quelli che richiedono accesso incondizionato all'esterno

Viene incontro al terzo problema (esaurimento dello spazio di indirizzamento)

RFC 1918

Lo IANA ha assegnato a questi usi i seguenti blocchi di indirizzi IP:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

Usando opportunamente questi indirizzi privati all'interno e un certo numero – abbastanza ridotto – di indirizzi pubblici per i sistemi che comunicano all'esterno, si è evitata la saturazione dello spazio di indirizzamento IP su Internet

Bridging, switching e routing

- E’ necessario avere ben presenti i concetti basilari del bridging, dello switching (del livello 2 in generale) e del routing (IP ed eventualmente di altri protocolli ruotabili). Questi concetti sono oggetto di altri corsi ma devono essere stati assimilati bene e devono essere disponibili come strumenti quotidiani di lavoro.
- Diversamente non risulterà chiaro come funziona un qualunque tipo di firewall, un IDS, un backbone, un bilanciatore, un cluster o una infrastruttura virtuale.

NAT, PAT e altri mascheramenti

- Il realistico abbandono di uno spazio di indirizzamento uniforme e l'utilizzo dei range definiti dalla RFC1918 fa sì che si debbano risolvere alcuni problemi di routing per poter collegare alla Internet la rete di un sito: gli indirizzi suddetti infatti sono per policy non ruotabili sulla Internet e qualunque router configurato bene scarterebbe pacchetti che abbiano tali indirizzi come sorgente o destinazione.
- Il Network Address Translation è una tecnica generica per indirizzare il problema: un router di confine o un firewall è opportunamente configurato per cambiare gli indirizzi destinazione e sorgente dei pacchetti da e per la Internet, rispettivamente. Si parla di source-NAT e destination-NAT a seconda di chi inizia il traffico.
- Notare come il problema non si ponga in caso di architettura di firewall di tipo Application Level Gateway, ma solo in caso di Packet Filter
- Al NAT si affianca anche il Port Address Translation per questioni di flessibilità e genericità della configurazione

Dispositivi e altri elementi

Si parlerà continuamente di…

Cablaggio – Thick & thin ethernet, Cat 3-6, coax, twinax, fibre, connettori, permutatori, armadi di derivazione, concentrazione e distribuzione

Tecnologie – Ethernet, Token-Ring, FDDI, ATM, SNA

Hub – managed, unmanaged, multiprotocollo, modulari

Bridge – transparent, SR, SRT, STP

Router – RIP, OSPF, NAT, ARP Proxy; VRRP, HSRP

Switch – layer 2, layer 3, layer 4, layer 7; STP, VLAN, MPLS, VSSP

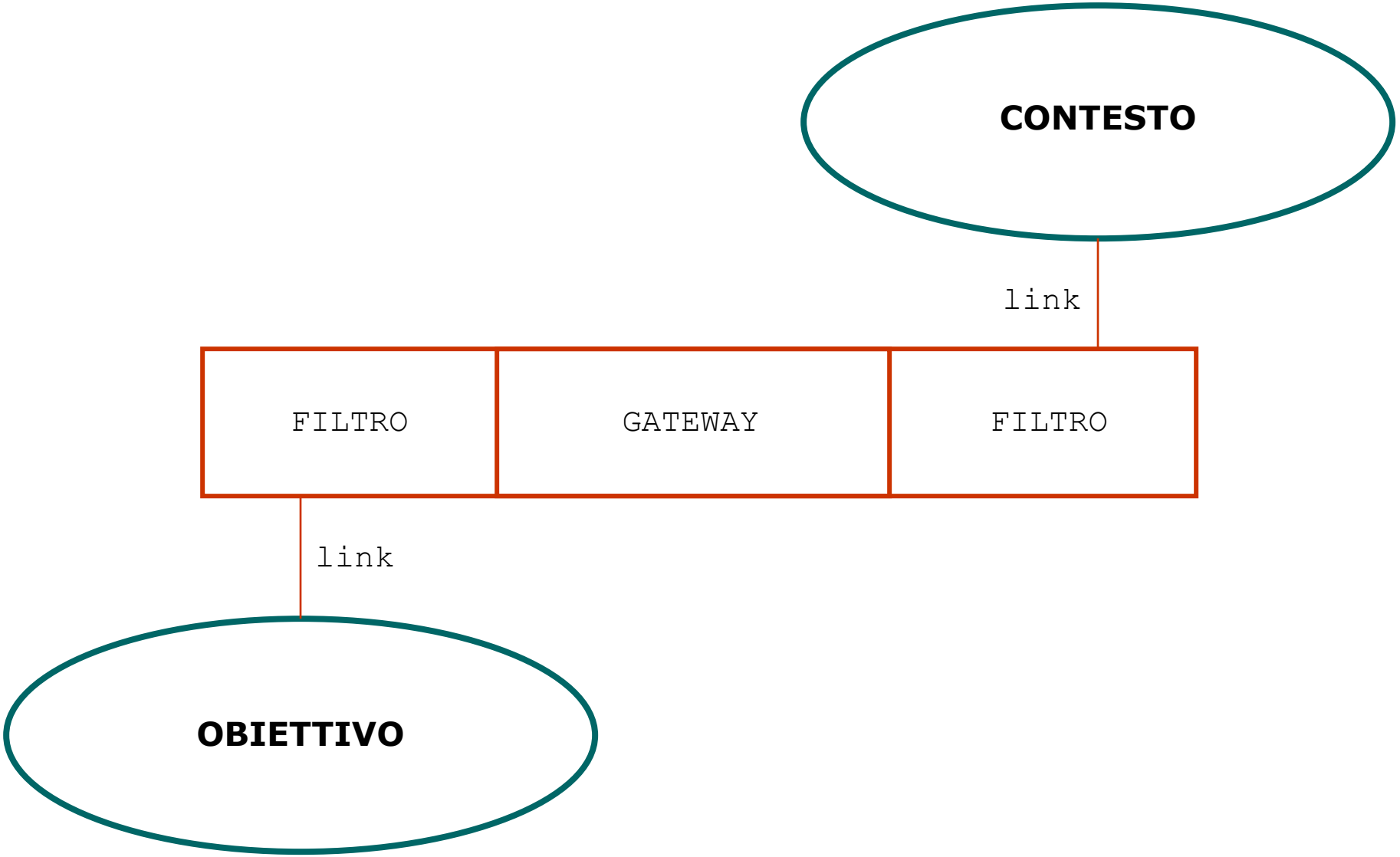
Protocolli – TCP/IP, IPX, NetBIOS, SNA, LLC, ATM, ATM LANE, SNMP

Sistemi Operativi – VMS, MVS, Unix, Ultrix, Windows

Ambienti Operativi – .NET, J2EE

Architetture di firewall

Concetti di base



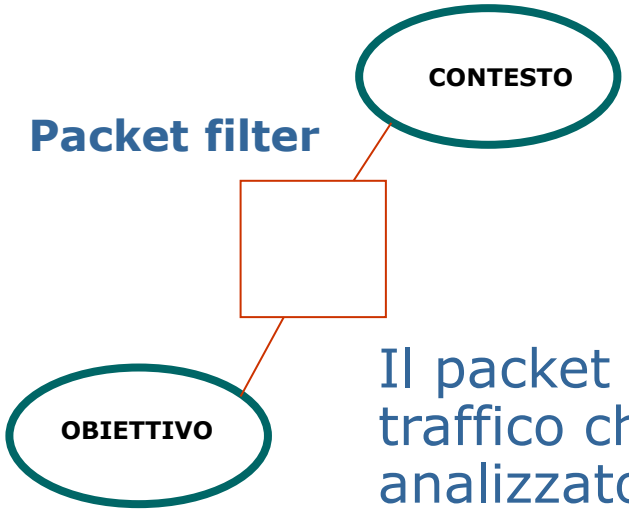
Scelta della policy

Assumendo che tutto il traffico in ingresso e in uscita dalla rete obiettivo passi per il firewall, questo avrà due impostazioni o comportamenti di *default.*

Deny all Tutto è vietato. Permettere il traffico di un certo tipo implica attivare qualcosa di specifico (regola o altro) per quel traffico. Elevata sicurezza.

Allow all Tutto è permesso. Occorre vietare esplicitamente il traffico di un certo tipo attivando qualcosa di specifico (regola o altro) per quel traffico. Semplicità di gestione.

La seconda policy si usa poco in ambiti di sicurezza, tuttavia è molto utilizzata per troubleshooting e traffic shaping.



Packet Filter

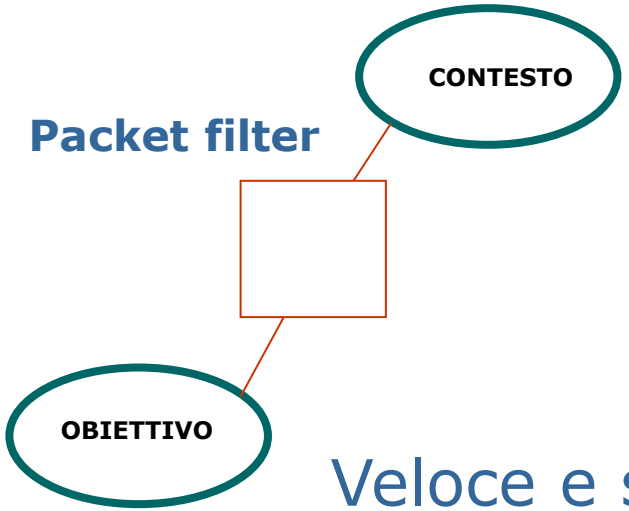
Il packet filter è un *router* con regole per filtrare il traffico che viene processato. Normalmente viene analizzato solamente l'header del pacchetto.

Ruleset: Lista di regole di traffico, che specificano attributi del pacchetto e un'azione.

- Informazioni di Livello 2 o 3: TYPE
- Informazioni di Livello 3 SRCIP, DSTIP
- Informazioni di Livello 4, SRCPORT, DSTPORT
- A volte esiste anche SRCIF
- Una AZIONE

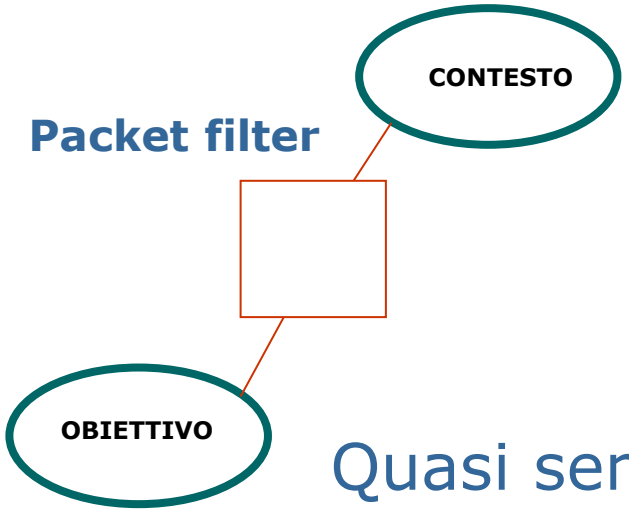
Le regole vengono applicate sequenzialmente.

Policy o regola di *default*: cosa fare del pacchetto se non soddisfa nessuna regola



Packet Filter

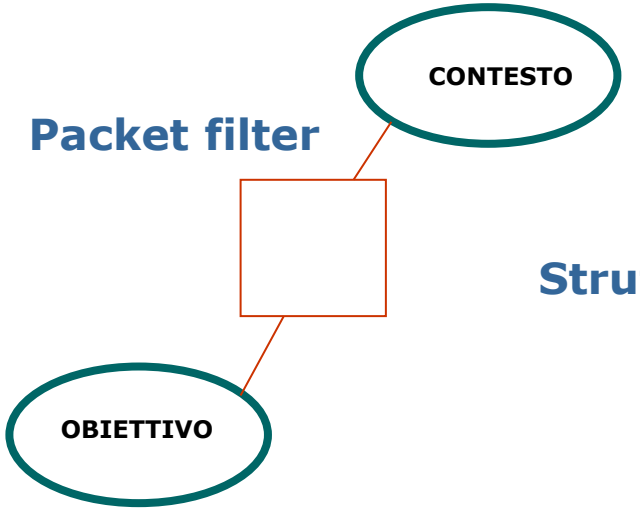
Veloce e semplice: le regole sono applicate su ogni pacchetto senz'alcuna memoria dei pacchetti precedenti (*statelessness*).
Non c'è memoria della provenienza (interfacce) dei pacchetti né connoscenza sulla destinazione.
Mancano meccanismi di autenticazione utente.
Il logging è povero (limitato alle stesse informazioni del ruleset).
Ogni sistema ha la sua sintassi: regole astratte vanno tradotte nel sistema che si usa.



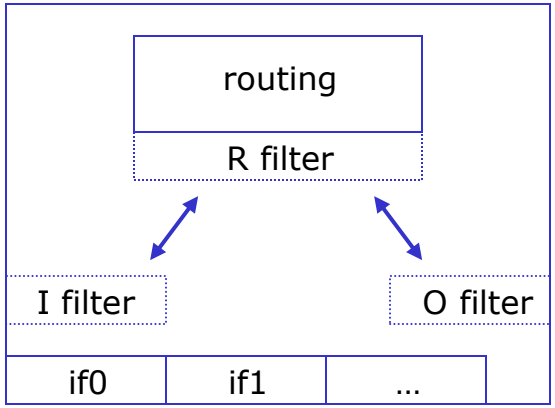
Packet Filter

Quasi sempre il *border router* è dell'ISP e può non essere facilmente controllabile.
Il *ruleset* diventa presto complesso, col rischio di deriva o di non essere più valido a causa di errori di configurazione.
E' opportuno quindi che il *ruleset* sia definito nel modo più semplice possibile e mantenuto tale, ma questo può andare contro le esigenze di utilizzo.
Generalmente soggetti alle debolezze delle specifiche di TCP/IP (es. *spoofing*).

Packet Filter

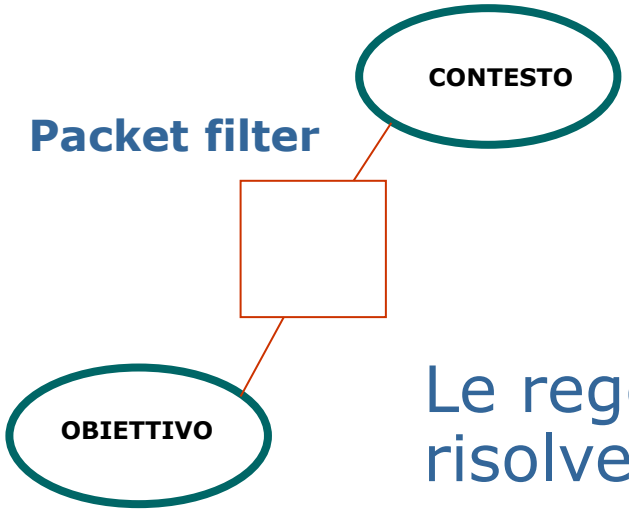


Struttura interna



L'azione di filtraggio dipende da come è fatto il router. Può esistere anche un solo filtro, associato alla logica di routing; un PF più evoluto può avere anche filtri associati alle logiche di *input* o di *output,* nelle varie combinazioni.

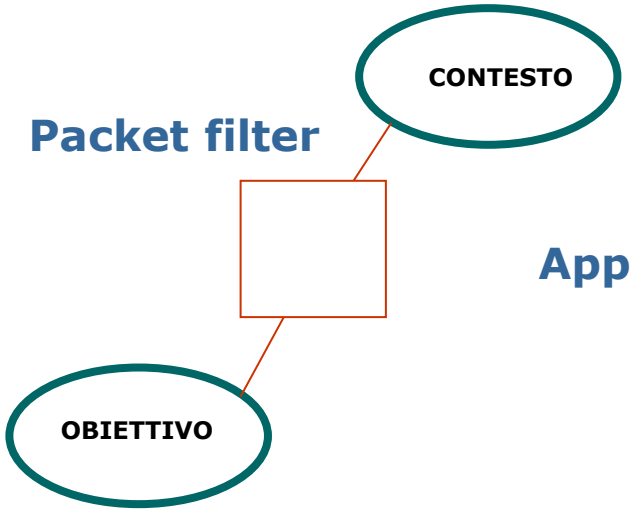
Questo complica, e comunque modifica, il modo di definire le regole, che variano a seconda di marca e modello del router, della topologia dei collegamenti, del numero delle porte e della modalità di impiego.



Packet Filter

Le regole di un packet filter non possono risolvere appropriatamente molti casi.

Non si riesce a discriminare la direzione di un colloquio senza effettuare l'analisi almeno del flag di acknowledge o dell'interfaccia di ingresso (att. allo spoofing).
Vi sono sempre pacchetti senza (inizio) e con (seguito) flag ACK.
Gli IP fragments non contengono i numeri di porta.
Il protocollo FTP dopo la prima connessione negozia una porta per la trasmissione dei dati (anche con PASV).
Altri protocolli "difficili": H323 e T120.
Non tutti sanno bene come funziona X11.
Eccetera …



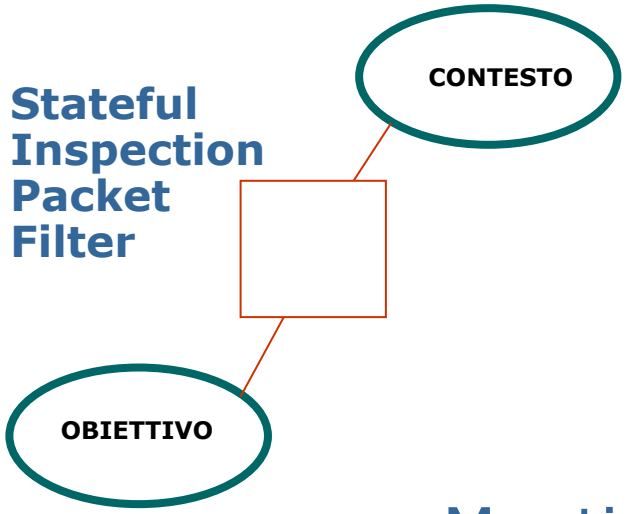
Packet Filter

- Line router (il router con una interfaccia *WAN* per il collegamento al Provider)
- Boundary router (il router più esterno di proprietà)
- Screening router (altri usi di firewalling)
- Router per separare in modo blando diversi domini di sicurezza all'interno di una organizzazione
- Router interni vari
- Applicazioni dove si privilegia la velocità e la priorità del traffico rispetto alla sicurezza

Stateful Packet Filter

Alle funzionalità di filtro già descritte per il semplice Packet Filter, aggiunge la possibilità di analizzare il singolo pacchetto nel contesto della sua comunicazione *(statefulness).*

Introdotto da CheckPoint agli inizi degli anni ’90.



Stateful Packet Filter

Mantiene una tabella delle connessioni.

Analizza e può filtrare il traffico ”in ingresso” non più basandosi sulla porta di destinazione (di solito >1024), ma sulla storia e lo stato di ciascuna connessione. A causa di questo la semantica delle regole del filtro cambia.

Permette una gestione più sicura dei protocolli UDP e ICMP perché si può gestire la “storia” della comunicazione.

Stateful Packet Filter

Nella sua forma basilare, questa tecnologia aggiunge al semplice *filtering* una conoscenza del livello 4 dello stack OSI.

La sua evoluzione permette invece di gestire informazioni anche a Livello 7 (applicazione), per esempio tramite moduli specializzati per determinati protocolli.

Stateful Packet Filter

Esempio di state table

Source addr	Source port	Dest addr	Dest port	Conn. state
192.168.10.4	1030	223.108.16.121	80	Established
181.115.4.1	4761	192.168.10.1	25	Established
192.168.10.19	1211	66.107.147.10	113	Established

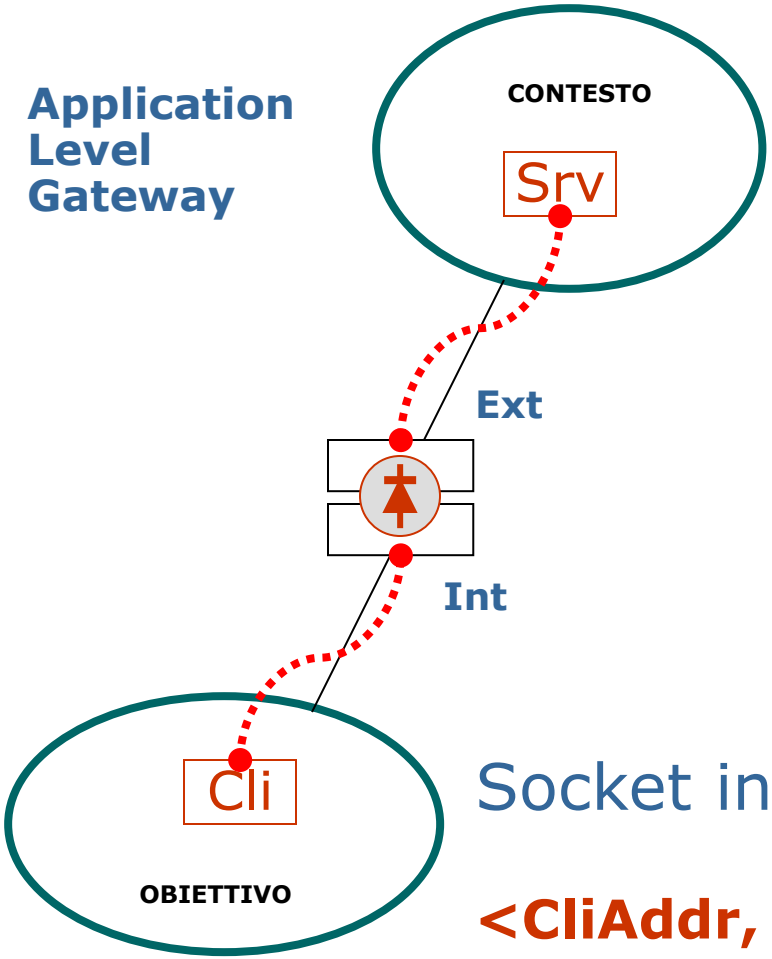
Application Level Gateway

Al contrario dei casi precedenti, un *firewall* di tipo *application level gateway* prevede che non vi sia *routing* tra la rete da proteggere e la rete esterna.

Non è dunque possibile a un sistema situato nella rete interna aprire una comunicazione con un sistema all'esterno, né viceversa.

Il passaggio dell'informazione da una rete all'altra può avvenire, ma solamente per il tramite di un software specializzato: il *proxy* applicativo.

Application Level Gateway



Socket in una comunicazione con PF:

<CliAddr, CliPort, SrvAddr, SrvPort>

Socket in una comunicazione con un ALG:

<CliAddr, CliPort, IntAddr, IntPort>
<ExtAddr, ExtPort, SrvAddr, SrvPort>

Application Level Gateway

La quintessenza del *proxy* è di lavorare a uno specifico livello 7, anche se vi sono proxy molto semplici che ignorano completamente il contenuto applicativo ed intervengono solo per l'apertura e la chiusura delle connessioni (cfr "Circuit Level Gateway").

Anche altri livelli possono essere analizzati, per esempio per effettuare un'autenticazione basata sull'indirizzo IP. Altri meccanismi sono possibili (userid + password, hw o sw tokens, certificati digitali, ecc).

Application Level Gateway

Un *application level gateway* ha alcuni vantaggi che lo caratterizzano da un *packet filter*.

- Reale separazione delle reti
- Sofisticati meccanismi di autenticazione
- Logging specifico dell'applicazione (comandi)
- *Filtering* dei contenuti
- Controllo e configurazione per utente
- Minore complessità di configurazione

Application Level Gateway

Un *application level gateway* ha ovviamente anche svantaggi, fra cui:

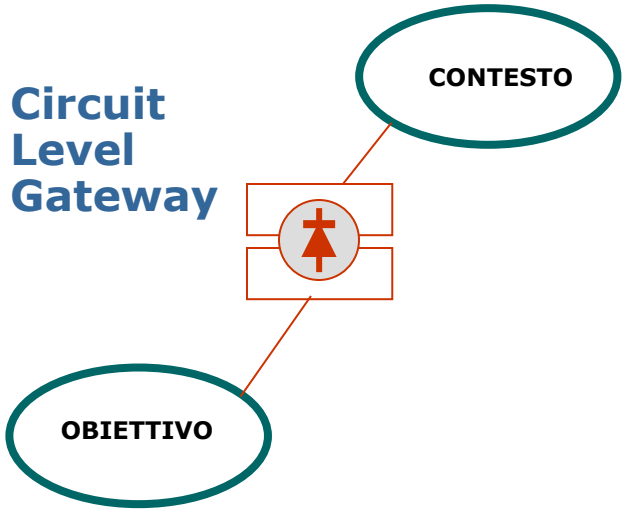
- Necessità di modificare il software
- Necessità di modificare il comportamento
- Prestazioni
- Supporto esteso solo ad alcuni protocolli

Application Level Gateway

Tipiche applicazioni:

- FTP
- Telnet
- HTTP
- SMTP
- NTP

Circuit Level Gateway

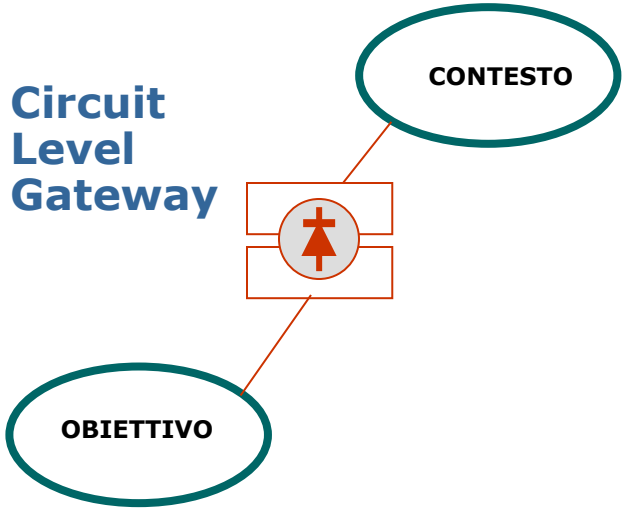


E’ una specie di *application proxy* leggero, che cioè non lavora a livello 7 e trasporta i dati della connessione da dentro a fuori e viceversa.

Può comunque effettuare logging, autenticazione e altre conversioni.

Non essendoci alcun controllo applicativo costituiscono una sorta di *tunnel* attraverso il *firewall* in architettura ALG.

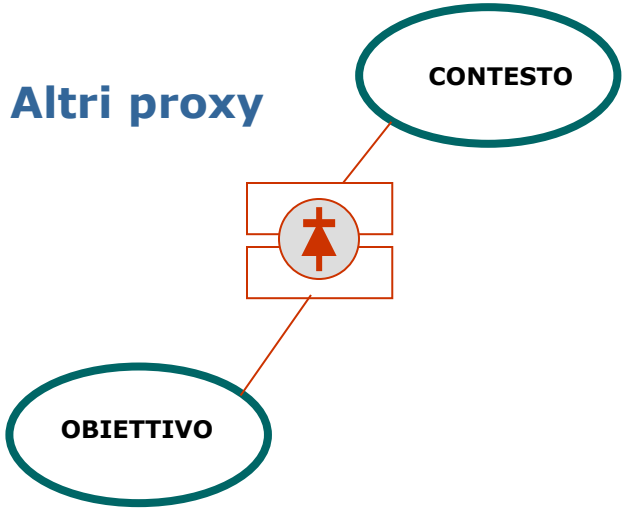
Circuit Level Gateway



Tipiche applicazioni:

- Telnet
- HTTP
- NNTP
- Protocolli proprietari

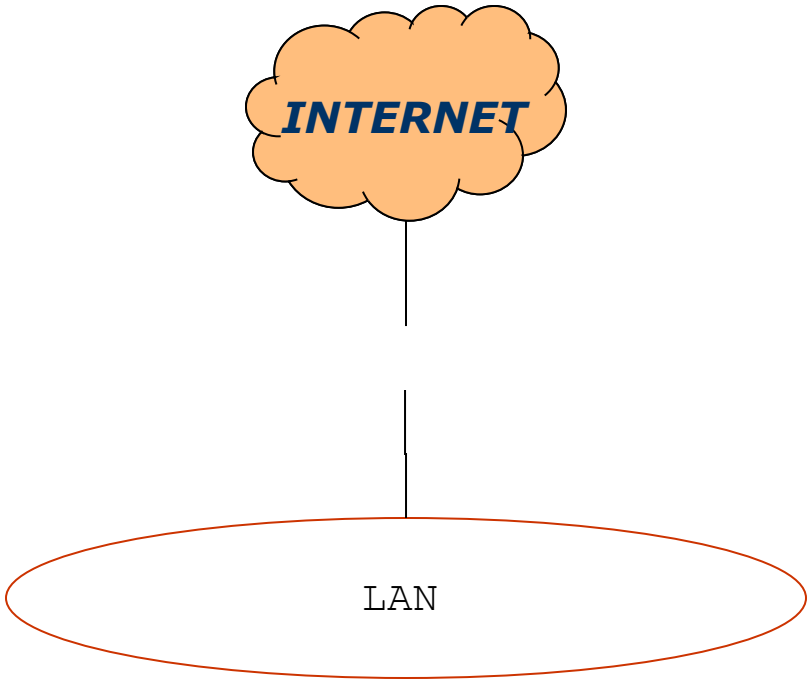
Di solito si può applicare questo tipo di proxy a tutti i casi semplici di applicazioni client-server



Altri proxy

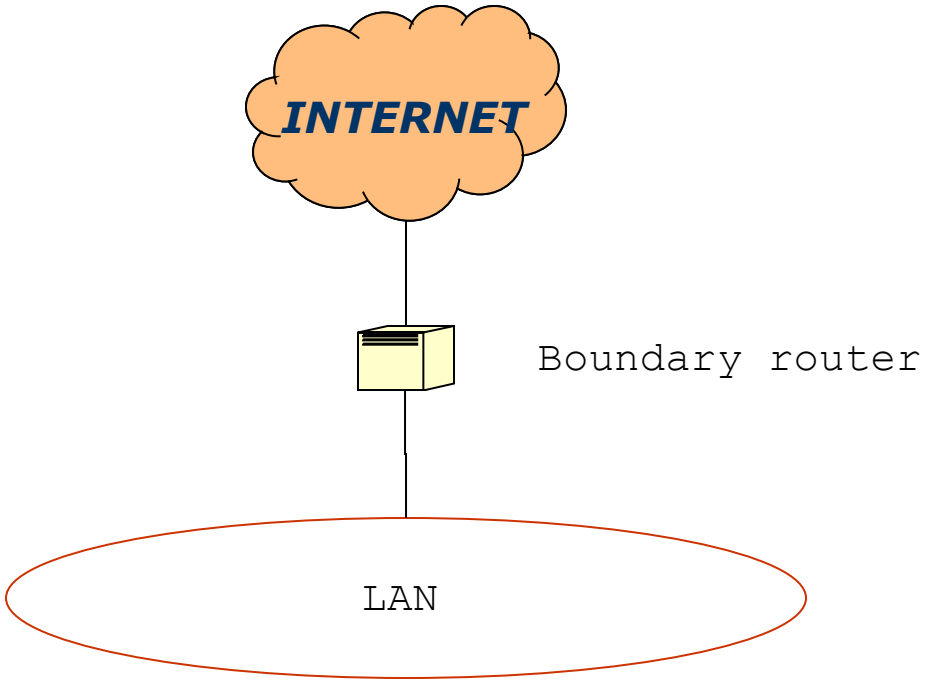
- SSL-izers
- SOCKS proxies

Schemi
Best solution ever?

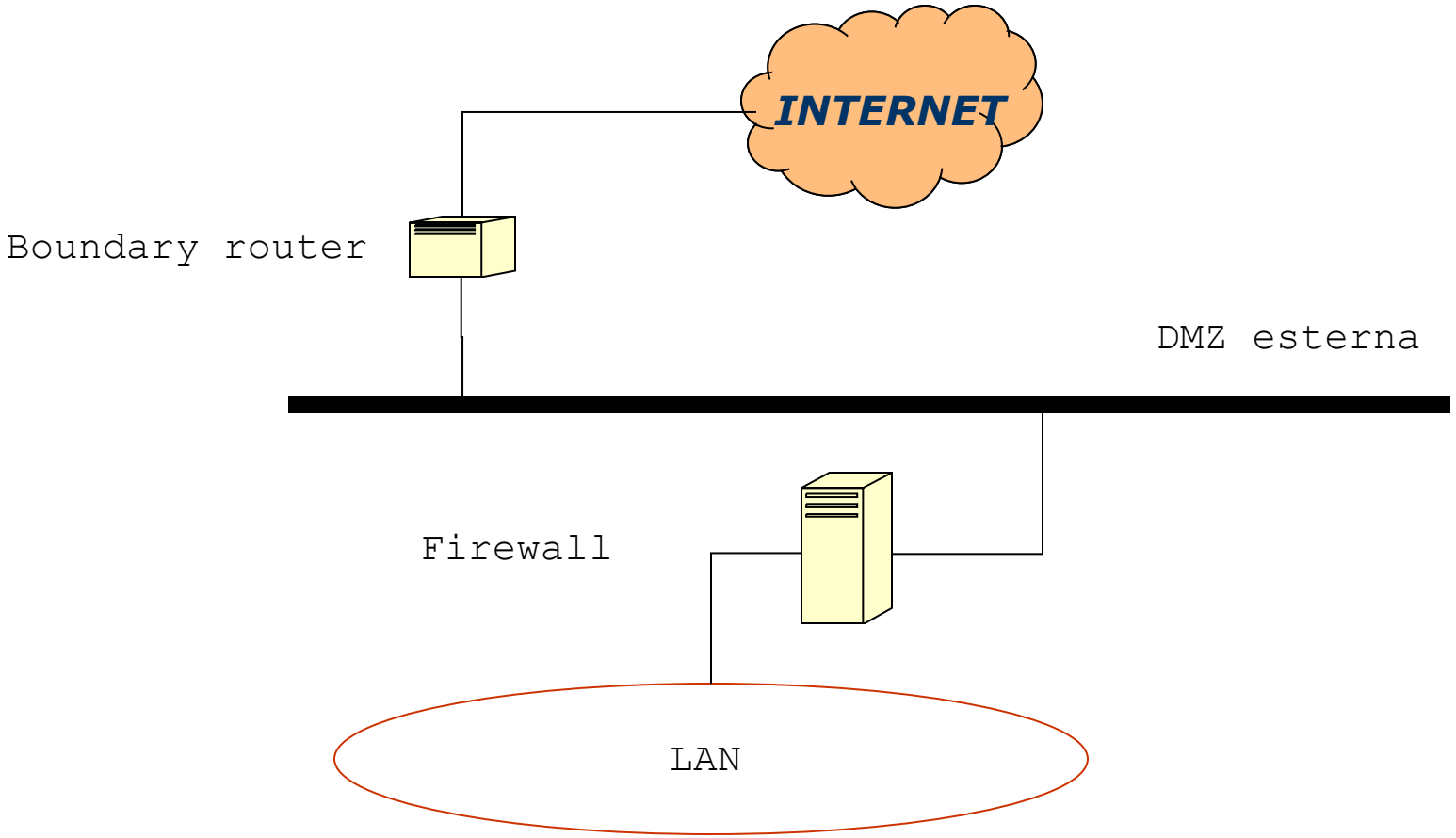


:-)

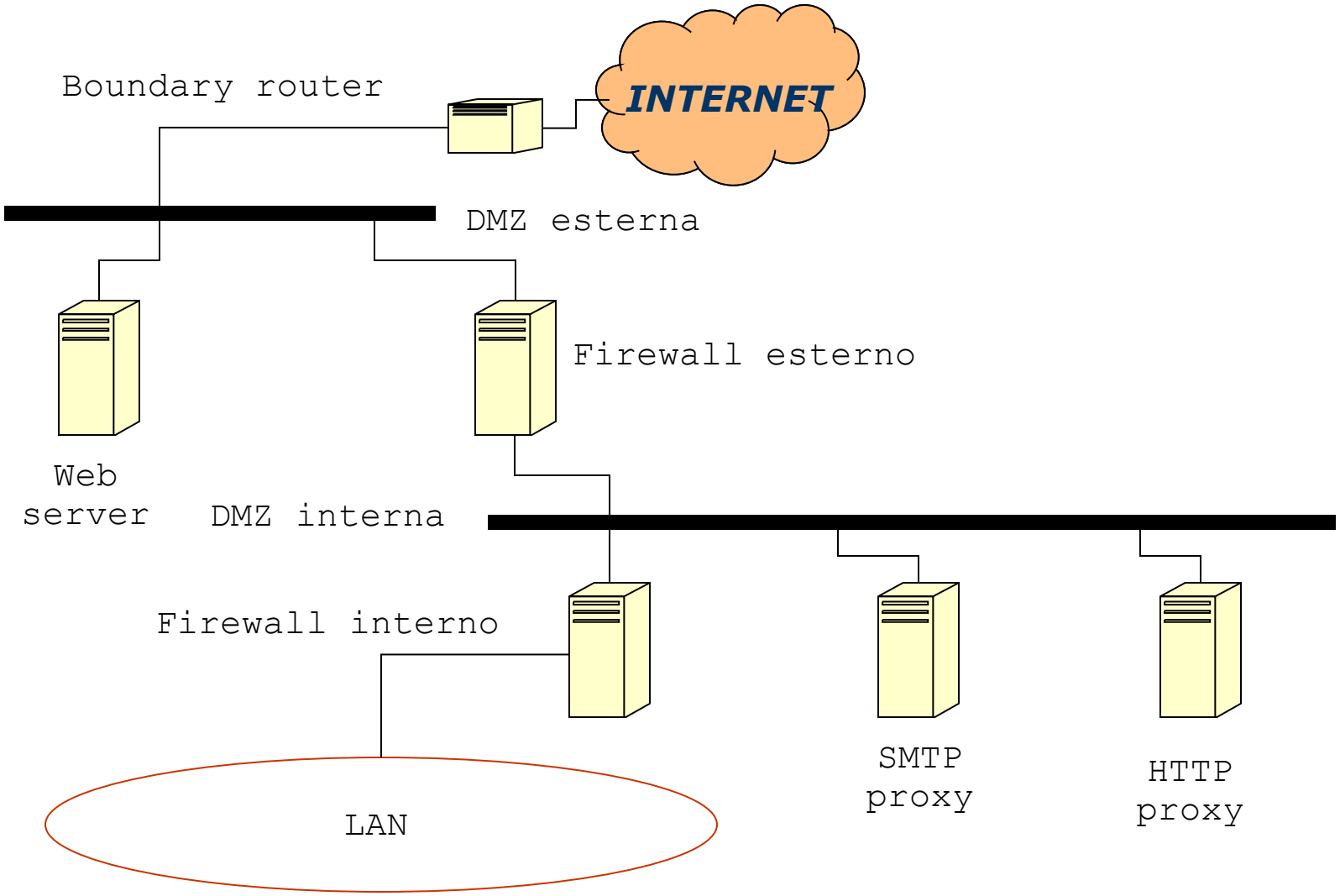
Schemi
Semplice border filter



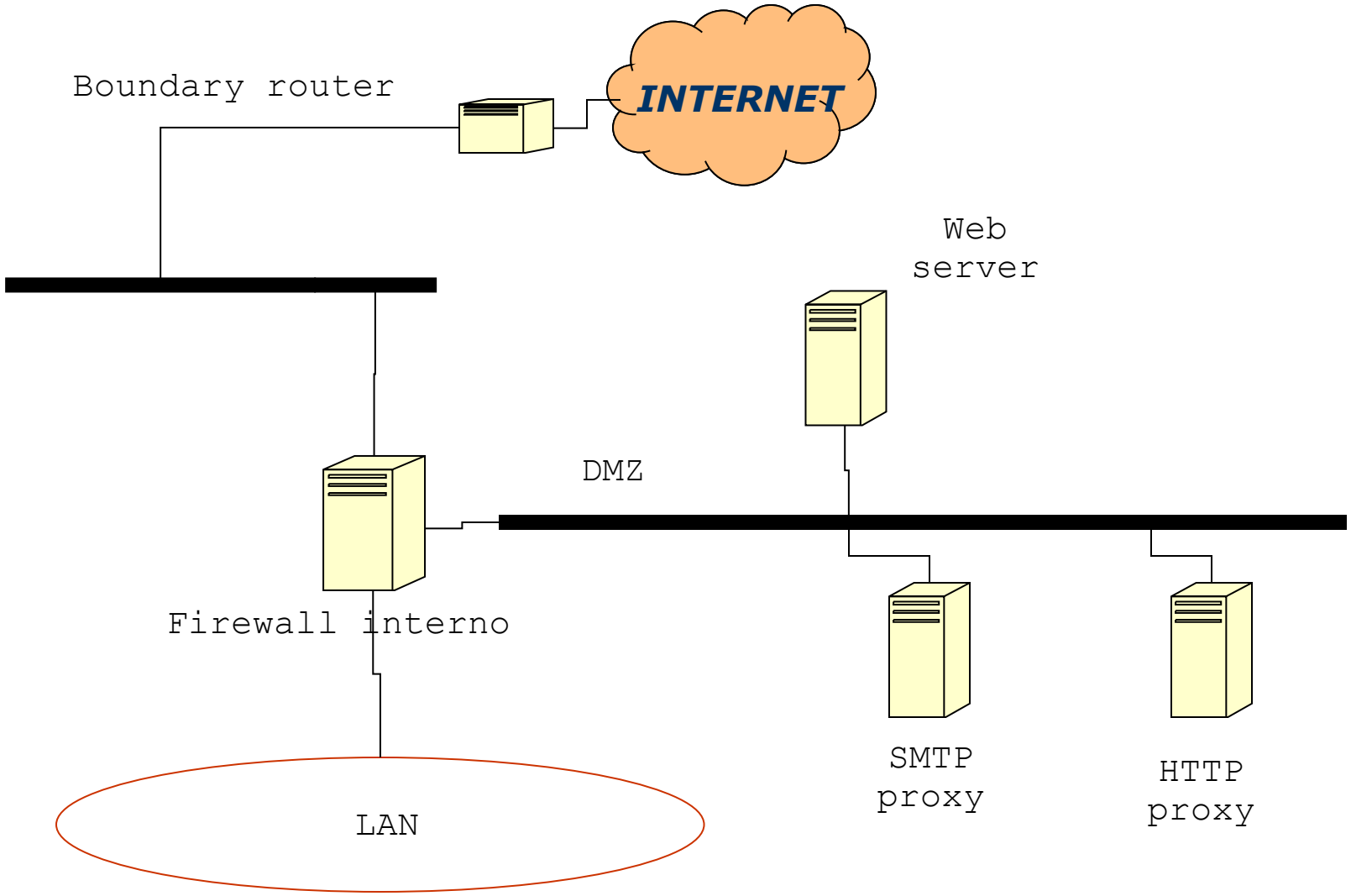
Schemi
Semplice border filter con DMZ e firewall



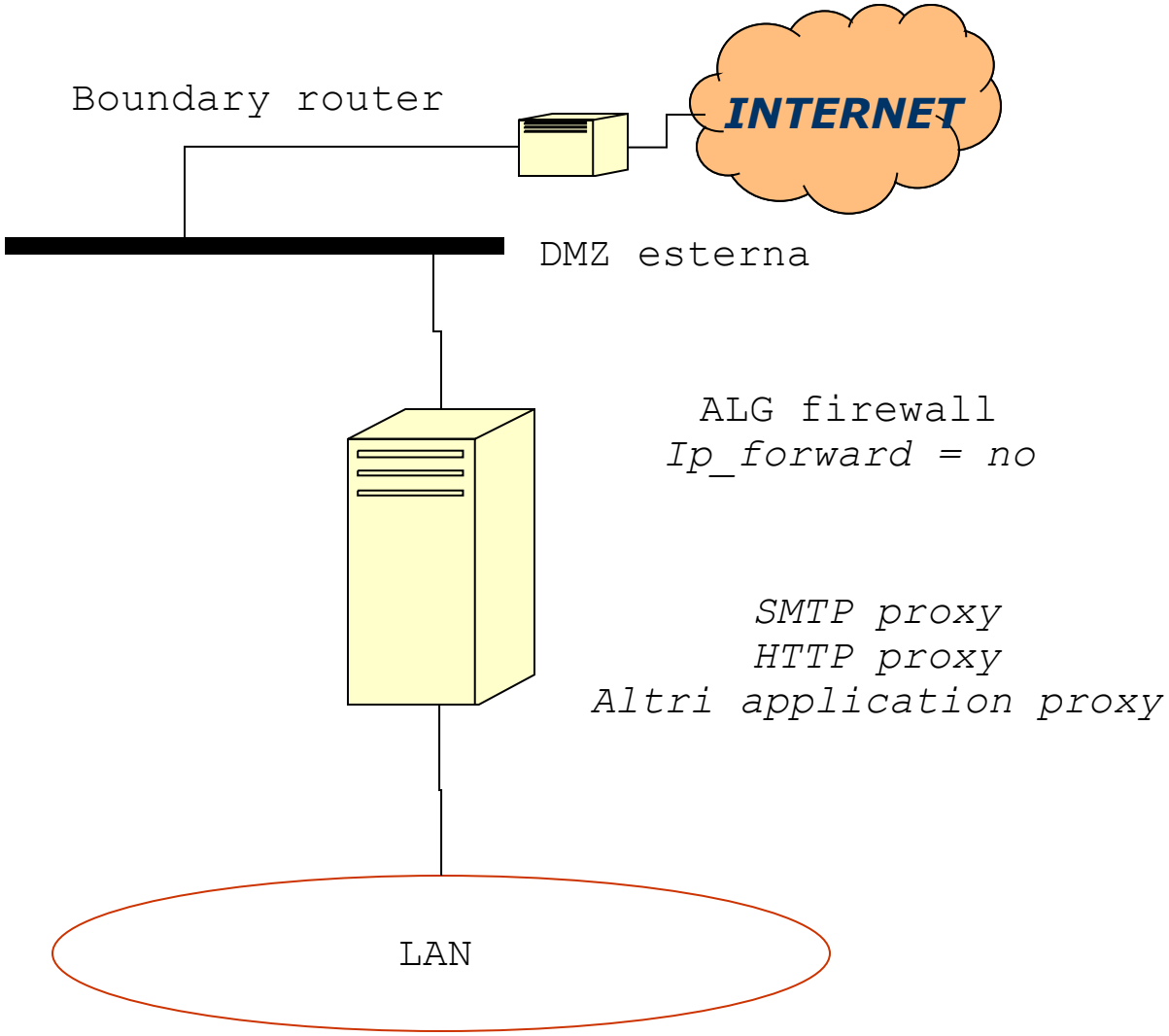
Schemi
Border filter con due DMZ e due fw



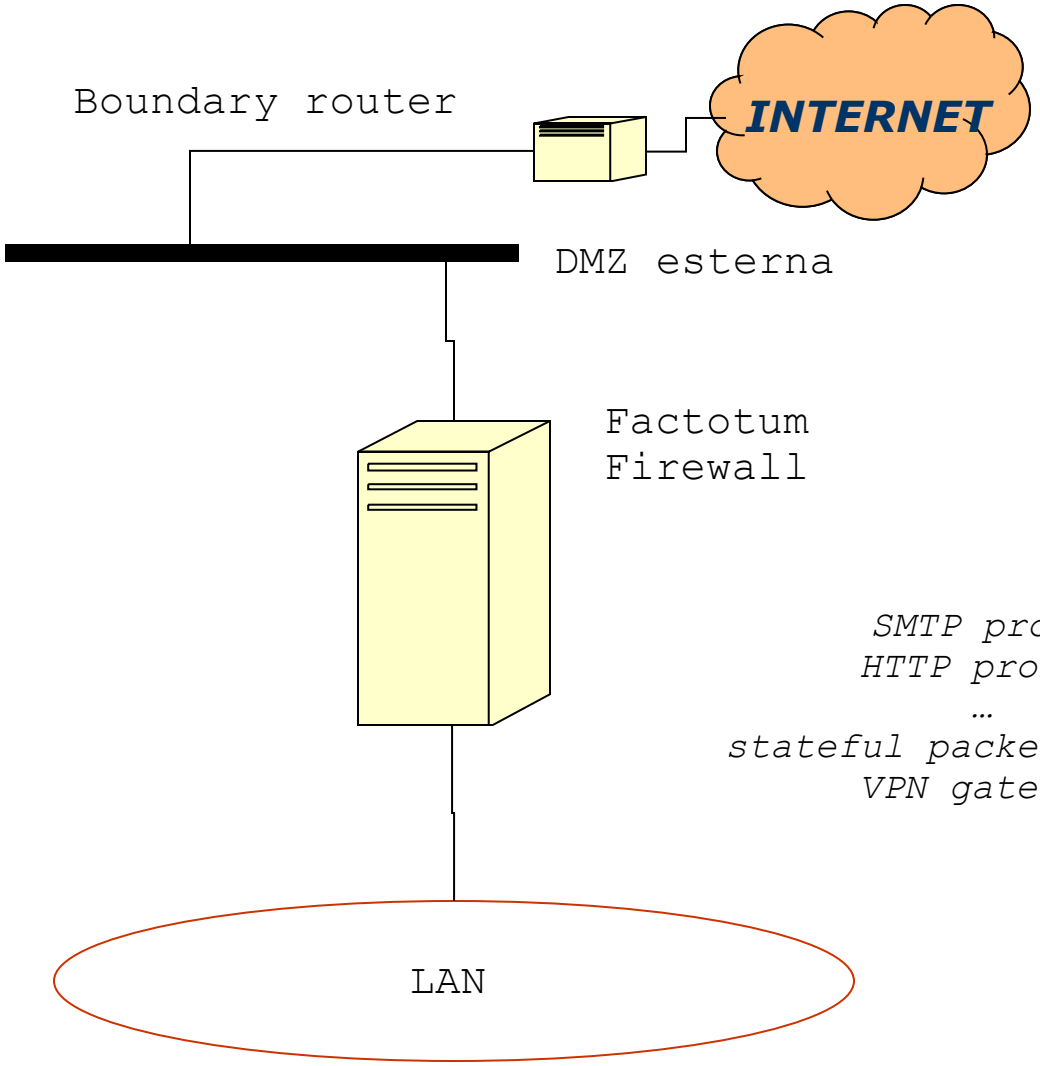
Schemi
Border filter con DMZ e fw multiporta



Schemi
Collapsed ALG

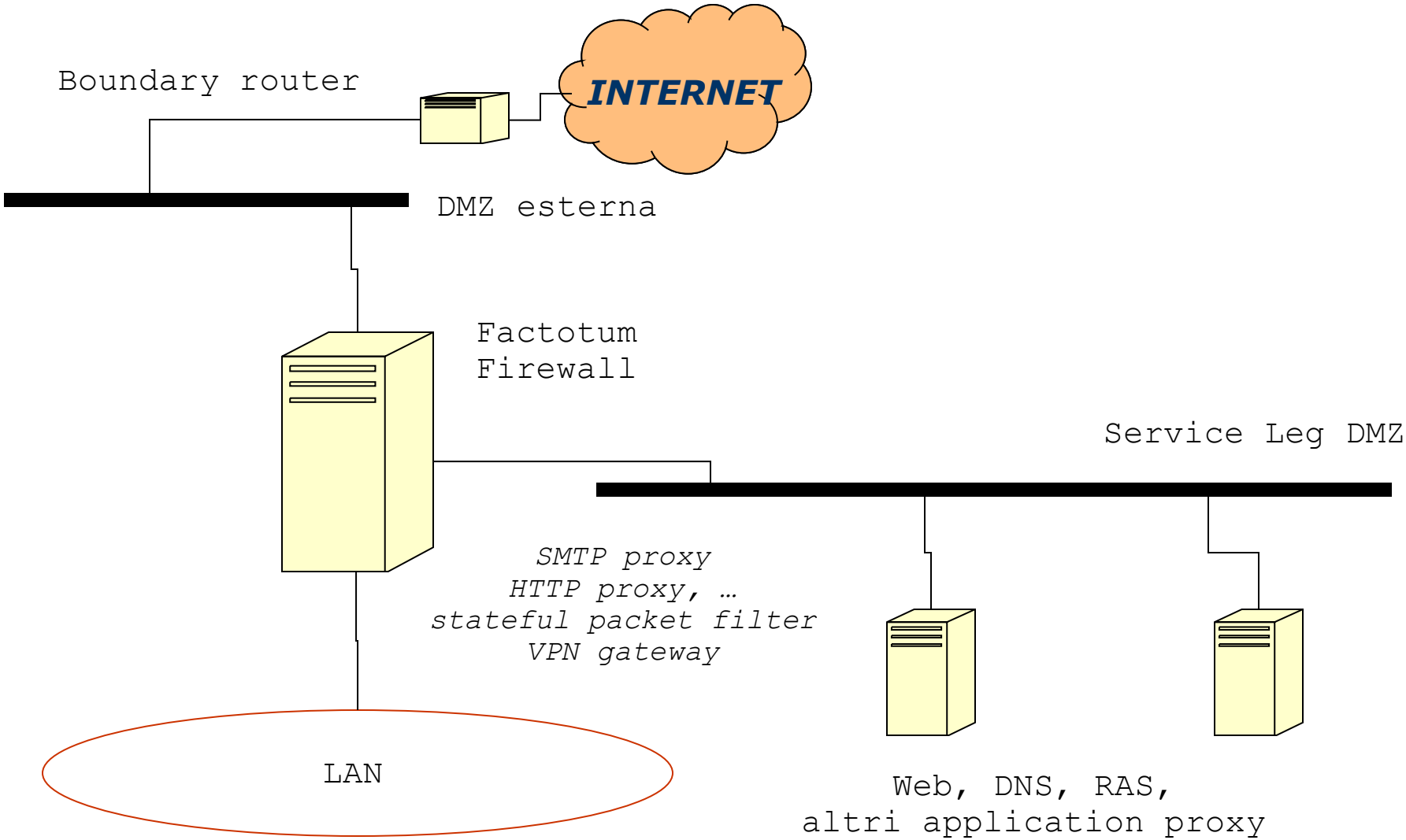


Schemi
Collapsed factotum



SMTP proxy
HTTP proxy.
…
stateful packet filter,
VPN gateway

Schemi
Collapsed factotum con service leg



Current trends

E’ necessario che i firewall si evolvano per essere più proattivi, bloccare i nuovi attacchi e fornire un controllo maggiore.

Le aziende dovrebbero aggiornare i loro firewall e i sistemi di Intrusion Prevention per proteggere il sito e le attività di business, perché gli attacchi divengono sempre più sofisticati.

Come potrebbe essere un **Next-Generation Firewall**?

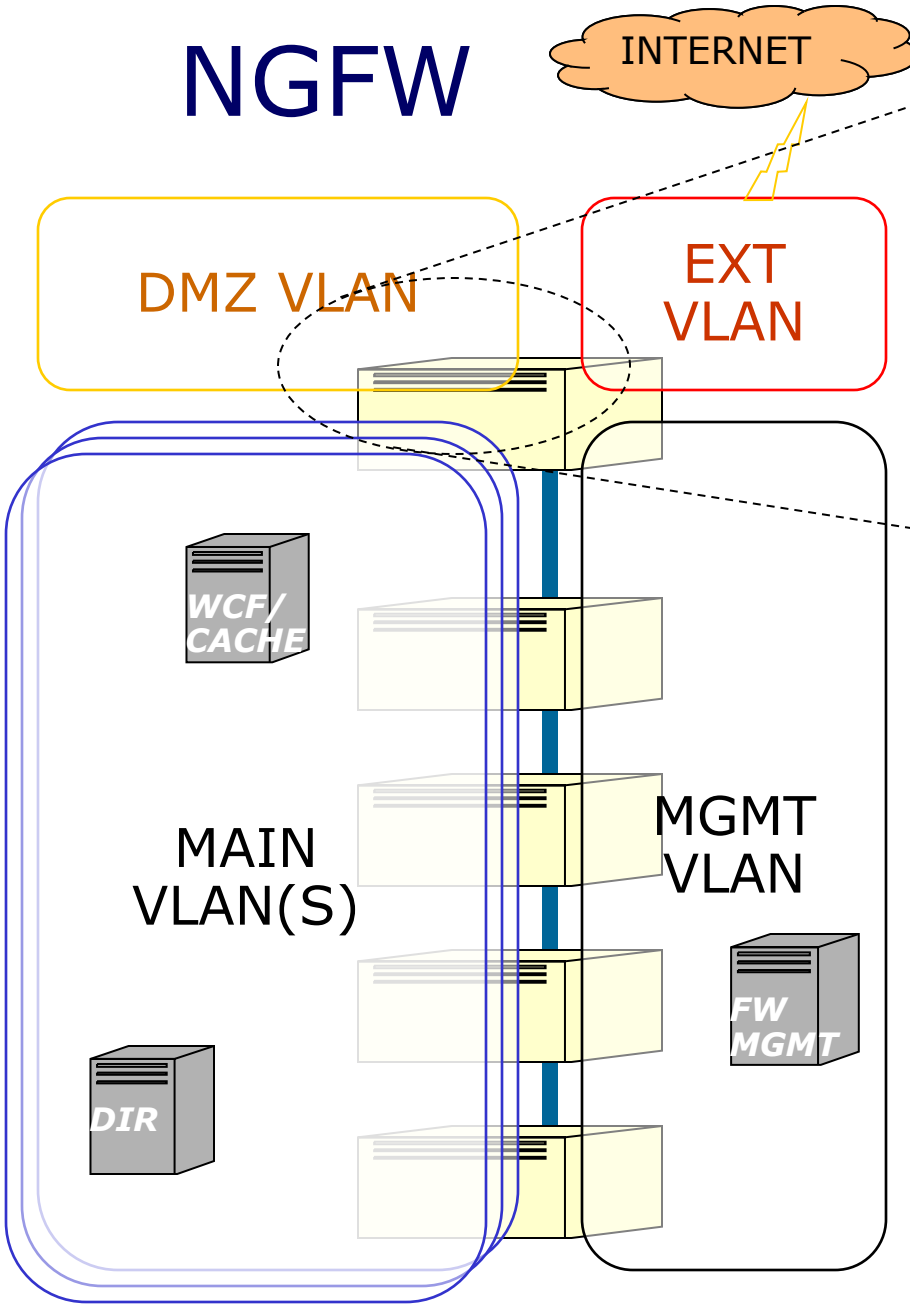
Il primo passo sostanziale è l’integrazione fra le funzionalità di firewall tradizionale (di prima generazione) e quelle di Intrusion Prevention. Inoltre tale sistema dovrà essere in grado di governare l’implementazione e l’applicazione delle policy di sicurezza anche a fronte dei cambiamenti nel modo di lavorare (es web 2.0) e nel modo in cui gli attacchi compromettono i sistemi.

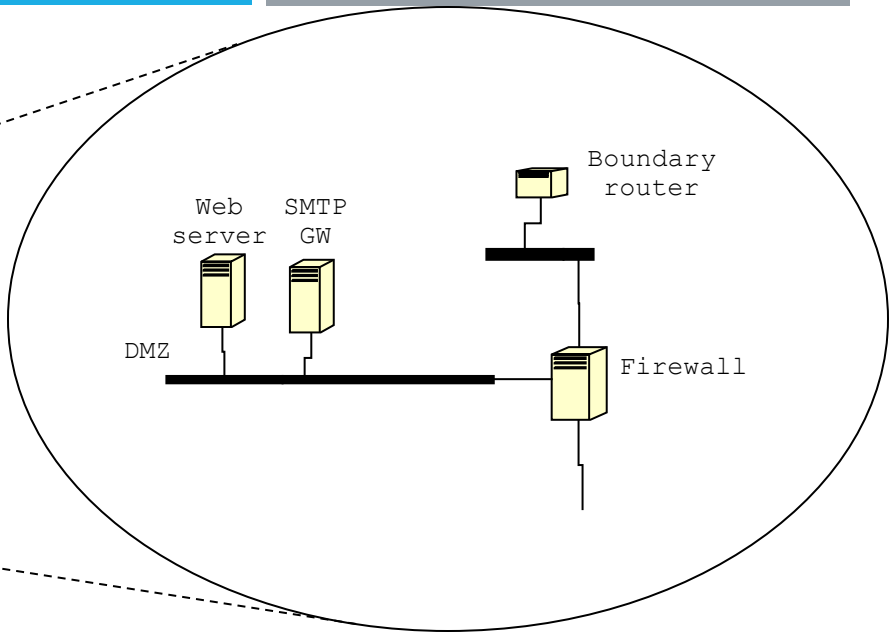
Current trends

In sostanza un NGFW dovrebbe:

- avere le caratteristiche di un firewall di prima generazione
- avere integrate le funzionalità di Intrusion Prevention
- full stack visibility and management
- extrafirewall intelligence
- directory integration
- wire speed

NGFW





In sostanza un NGFW, per avere

- compatibilità con firewall di prima gen.
- funzionalità di Intrusion Prevention
- full stack visibility & management
- extrafirewall intelligence
- directory integration
- wire speed

Dovrebbe essere

integrato nell'infrastruttura!

Firewall management

The fine point

Un configuratore è uno strumento che permette la programmazione del firewall a un livello di astrazione superiore alle regole del motore decisionale e introduce meccanismi di controllo che garantiscono maggiore sicurezza evitando errori di programmazione.

Si riportano brevi esempi di configuratori per Netfilter (Shorewall e FWBuilder) e CISCO ASA (CISCO ASDM e Security Manager).

The fine point

I configuratori sono estremamente utili per effettuare una corretta gestione di singoli dispositivi, soprattutto quando la gestione è affidata a "più mani"

Sono però indispensabili quando occorre gestire una rete complessa di dispositivi. Un configuratore che consente la gestione di una rete di firewall e dell'intera VPN diventa quindi una stazione di configurazione e gestione centralizzata di fondamentale importanza, consentendo a più amministratori di collaborare all'evoluzione della configurazione della rete nel rispetto delle policy di sicurezza definite nell'ambito dell'Organizzazione

Netfilter, ovvero `iptables`

E’ lo *stateful packet filter* del kernel 2.4 e 2.6.

`www.netfilter.org`
sito di riferimento

`iptables-tutorial.frozentux.net`
tutorial

E’ un *framework* integrato nel kernel e capace di caricare plug-in che realizzano specifiche funzionalità di filtering, di tracciatura delle connessioni, statistiche, ecc.

Netfilter, architettura

Chains (liste di regole): sono gli agganci (hooks)

PREROUTING, POSTROUTING,
INPUT, OUTPUT, FORWARD,
user defined

Tables (categorie di liste): funzionalità

mangle, nat, filter

Matches: trigger per le regole

generici, specifici

Targets: azioni da eseguire in caso di match

ACCEPT, DROP, REJECT, QUEUE, RETURN,
DNAT, SNAT, MARK, MASQUERADE,
TOS, TTL, LOG, ULOG

Netfilter configurators

La *command line* di Netfilter è un po' come l'assembler; per motivi pratici (velocità) e di sicurezza (meno errori) conviene usare strumenti di più alto livello. I front-end, basandosi su astrazioni caratteristiche di ciascuno, permettono di esprimere le regole di *netfilter* in modi grafici o testuali; un'azione di *apply* provvederà alla loro compilazione in comandi *iptables* che verranno quindi eseguiti, attivando così le regole.

- **Shorewall**
- **FwBuilder**

Shorewall

Non è un daemon

Astrazione di stateful packet filter con estensioni

Interfacce illimitate

Zone (più if/zona e più zone/if)

Connessioni: tra coppie di zone

Azioni (ACCEPT, DROP, REJECT, …)

Routing, NAT, blacklists

Supporto per VPN

Supporto per TC e accounting

Shorewall

Zone

Shorewall vede la rete in cui opera come un insieme di **zone**.

Vi è sempre un'implicita zona **fw**, che è il firewall stesso.

Le altre zone si dichiarano in `/etc/shorewall/zones`.

Esempio:

```
internal        la rete interna
dmz             la DMZ
external        l'intera Internet
```

Shorewall

Interfacce

Shorewall ha bisogno di sapere a quali interfacce sono connesse le zone.

Le interfacce si dichiarano in `/etc/shorewall/interfaces`.

```
# zona          intf          broadcast     options
internal        eth0          detect
dmz             eth1          detect
external        eth2          detect        norfc1918
```

Shorewall

Policy e rules

Le regole che dichiarano quale traffico permettere o negare sono espresse in termini di zone.

Le regole di default si configurano in `/etc/shorewall/policy`

```
#/etc/shorewall/policy
#SOURCE    DEST        POLICY          LOG LEVEL     LIMIT:BURST
internal   external    ACCEPT
external   ALL         DROP            info
ALL        ALL         DROP
```

Shorewall

Policy e rules

Le eccezioni alle policy sono in `/etc/shorewall/rules`

Per default è ammesso il traffico `fw-fw`

```
#/etc/shorewall/rules
#ACTION         SOURCE          DEST    PROTO  DEST    SOURCE …
#                                                PORT    PORT
ACCEPT          ext             dmz:192.168.1.10 tcp www
ACCEPT          ext:1.4.5.9     dmz:192.168.1.5  tcp 53
ACCEPT          int             dmz:192.168.1.5  udp 53
ACCEPT          fw              ext     all
```

FWBuilder

Interfaccia utente grafica

Policy compiler per vari firewall (iptables, PF, PIX)

Astrazione: oggetti di rete, regole

Manutenzione degli oggetti di rete

Manutenzione delle regole

Associazione regole a oggetti --> compilazione --> deployment

FWBuilder

FWBuilder tree:

Obiects

- Hosts
- Networks
- Addesses
- Address ranges
- Groups
- Firewall itself

FWBuilder

FWBuilder tree:

Firewalls

- Interfaces
- Operating System

FWBuilder

FWBuilder tree:

Services

- IP
- ICMP
- TCP
- UDP
- Custom

FWBuilder

FWBuilder tree:

Policy == Ruleset

Esistono tre ruleset:

- Access policy
- NAT policy
- Routing policy

FWBuilder

FWBuilder tree:

Actions

- ACCEPT
- DENY
- REJECT

FWBuilder

Una regola ha i seguenti campi (con esempi di valori):
Source: Firewall, net-192.168.1.0, …
Destination: Any, Servers on DMZ, …
Service: Any, DNS, HTTP, …
Interface: Outside, all, …
Direction: Incoming, Both, …
Action: Accept, Deny, Reject, …

Vi sono anche campi che consentono di creare relazioni delle regole con l'orario e azioni complesse come marcature di pacchetti o branch ad altro ruleset

CISCO ASDM

PIX e ASA

Il firewall CISCO PIX è stato reingegnerizzato dando vita di recente alla famiglia di prodotti ASA (Adaptive Security Appliance).

Questi dispositivi possono essere controllati e configurati agendo su un'interfaccia locale, l'ASDM (Adaptive Security Device Manager). Fornisce:

- Rapid Configuration (wizards, common policies, sw upgrades, online help)
- Diagnostics (packet tracer, log-policy correlation, packet capture)
- Monitoring (realtime graphics and tabulated security metrics; incident and trend analysis)

CISCO Security Manager

Al contrario dell'ASDM, utile per gestire un singolo dispositivo, CSM consente l'amministrazione centralizzata di una rete di dispositivi, permettendo la definizione e il deployment delle regole da un unico punto e da diversi operatori. Oltre alle funzionalità "ovvie" fornite già dall'ASDM, il CSM offre:

- Standardizzazione: si possono distribuire automaticamente le policy standard ai nuovi firewall
- Scalabilità: si usano gli stessi meccanismi di gestione con pochi dispositivi o con centinaia
- Organizzazione: si possono definire workflow di gestione identificando i ruoli di "operator", "approver", "deployer"
- Auditing: un cruscotto centrale che visualizza lo stato di tutti i firewall gestiti e tutte le operazioni di change effettuate
- VPN: è particolarmente efficace nella configurazione e gestione di una VPN anche complessa (configurazioni site-to-site, full mesh, hub'n'spoke, ecc)

CISCO Security Manager

Esempio di gestione delegata con CSM:

- L'amministratore centrale definisce un'elenco di policy generiche ammesse dappertutto
- Tutti gli amministratori di rete di un'organizzazione possono applicare le policy definite centralmente ai dispositivi di loro competenza
- Localmente gli amministratori possono anche creare nuove policy; un qualunque gruppo di nuove regole specifiche forma una specifica *activity*, soggetta ad approvazione da parte dell'amministratore centrale
- Per le policy generiche pubbliche e, dopo l'approvazione, per le activity create localmente viene creato un *deployment job* la cui esecuzione può essere immediata o schedulata

Virtual Private Networks

Definizione

Una

Virtual Private Network

è una rete di circuiti virtuali opportunamente protetti che trasportano informazioni private.

In questo contesto un circuito virtuale è una connessione, stabilita attraverso una rete di qualunque tipo, tra un sistema mittente e uno destinatario, in questo caso adibita all'incapsulamento del traffico privato tra le due reti a valle dei due sistemi, denominati **gateway**.

Evoluzione delle reti private

Leased lines, analogiche e dedicate (1960→)

X.25, DDS / ISDN, T1 / E1 e loro frazioni (1970→)

Frame relay, ATM (1980→)

Internet VPN (1990→)

IVPN: perché del successo

Costi inferiori alle tradizionali soluzioni

Flessibilità dell'infrastruttura

Scalabilità

Disponibilità

Spontaneo decremento nel tempo del rapporto *costi/benefici*

VPN oursourcing

Vi sono alternative alla costruzione e gestione delle VPN via Internet: acquistarle da qualcuno che poi le gestisce

I provider oggi offrono ancora “reti private” sotto forma di VPN, come servizio che rivendono ai clienti che hanno acquistato la connettività presso di loro

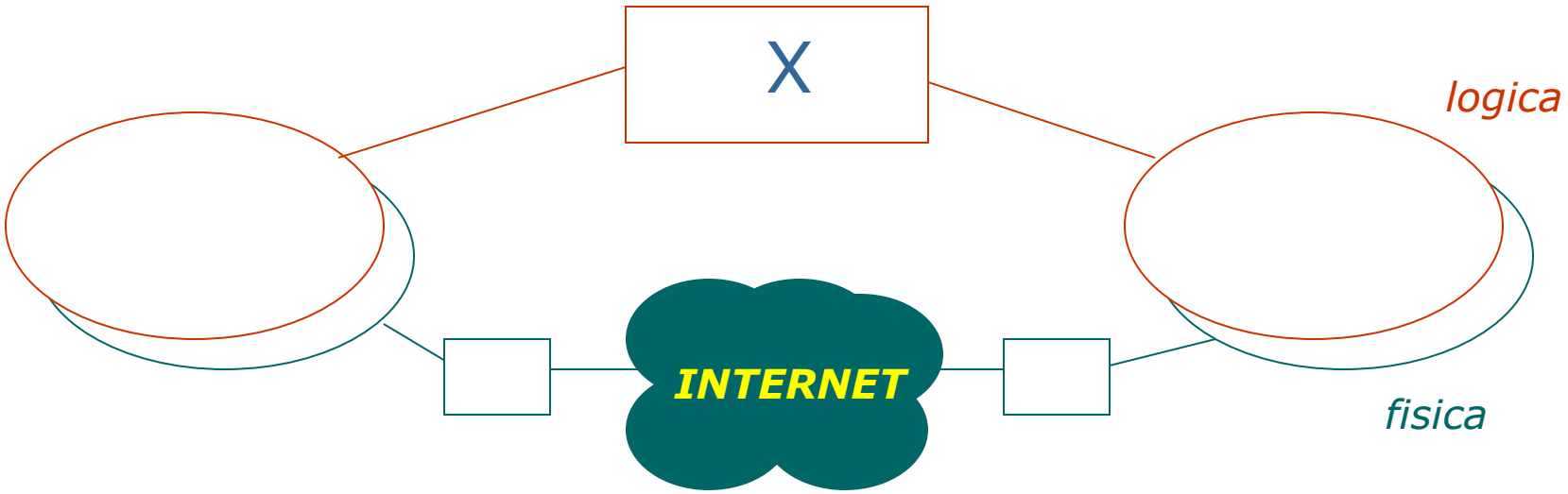
Le tecnologie attuali non sono più *frame relay* e simili ma, per le ormai diffusissime infrastrutture GbE, MPLS

Architetture di VPN

Tunneling → "Virtual"

Connessioni dinamiche

Struttura logica != struttura fisica



Architetture di VPN

Security services → “Private”

Autenticazione

Controllo accessi

Confidenzialità

Integrità

Architetture di VPN

Remote access o Client To Site

Un utente singolo che si collega a una sede

Site To Site

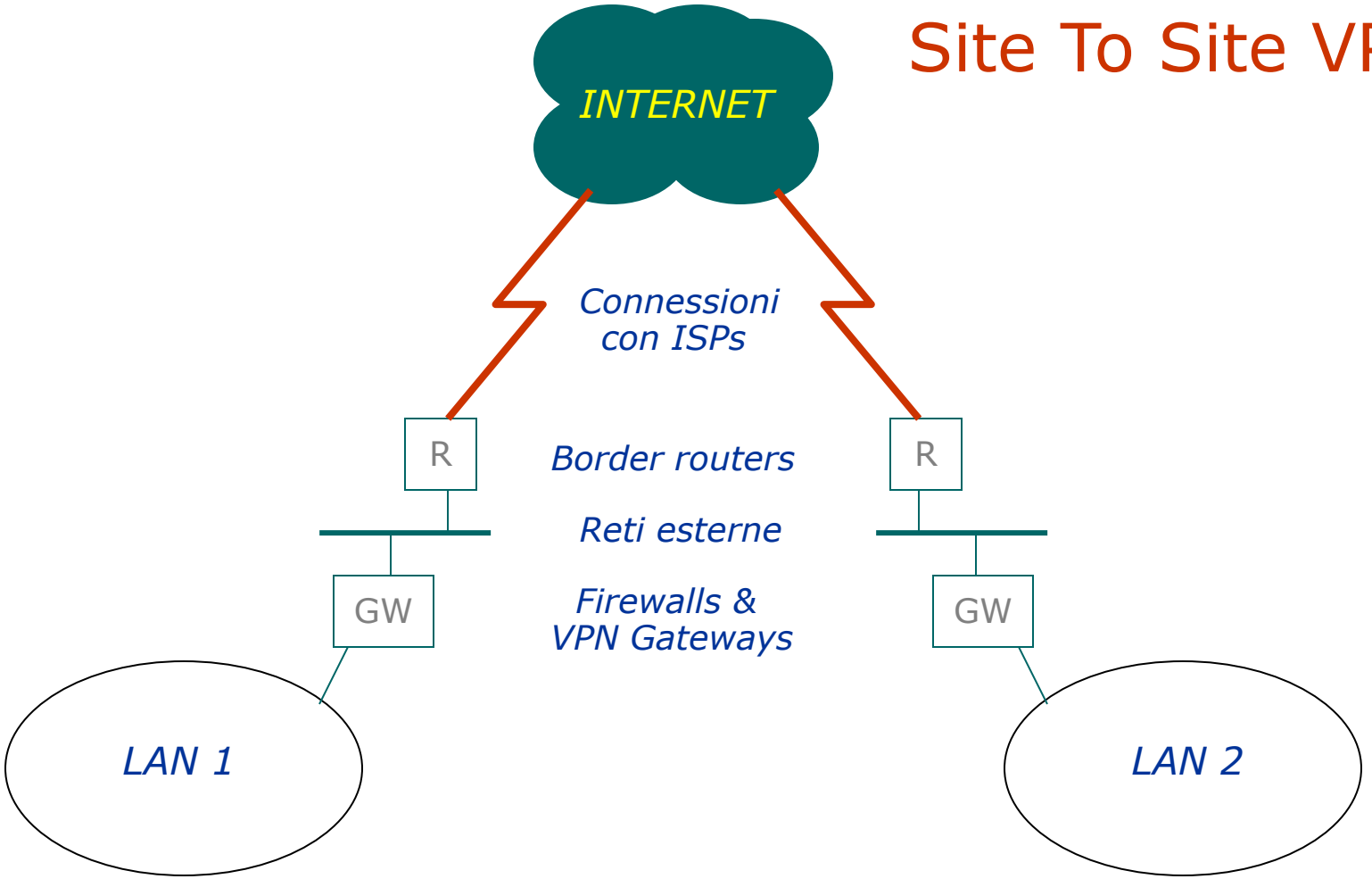
Collega due sedi diverse

Site to Extranet

Collega una sede a una terza parte o *community*

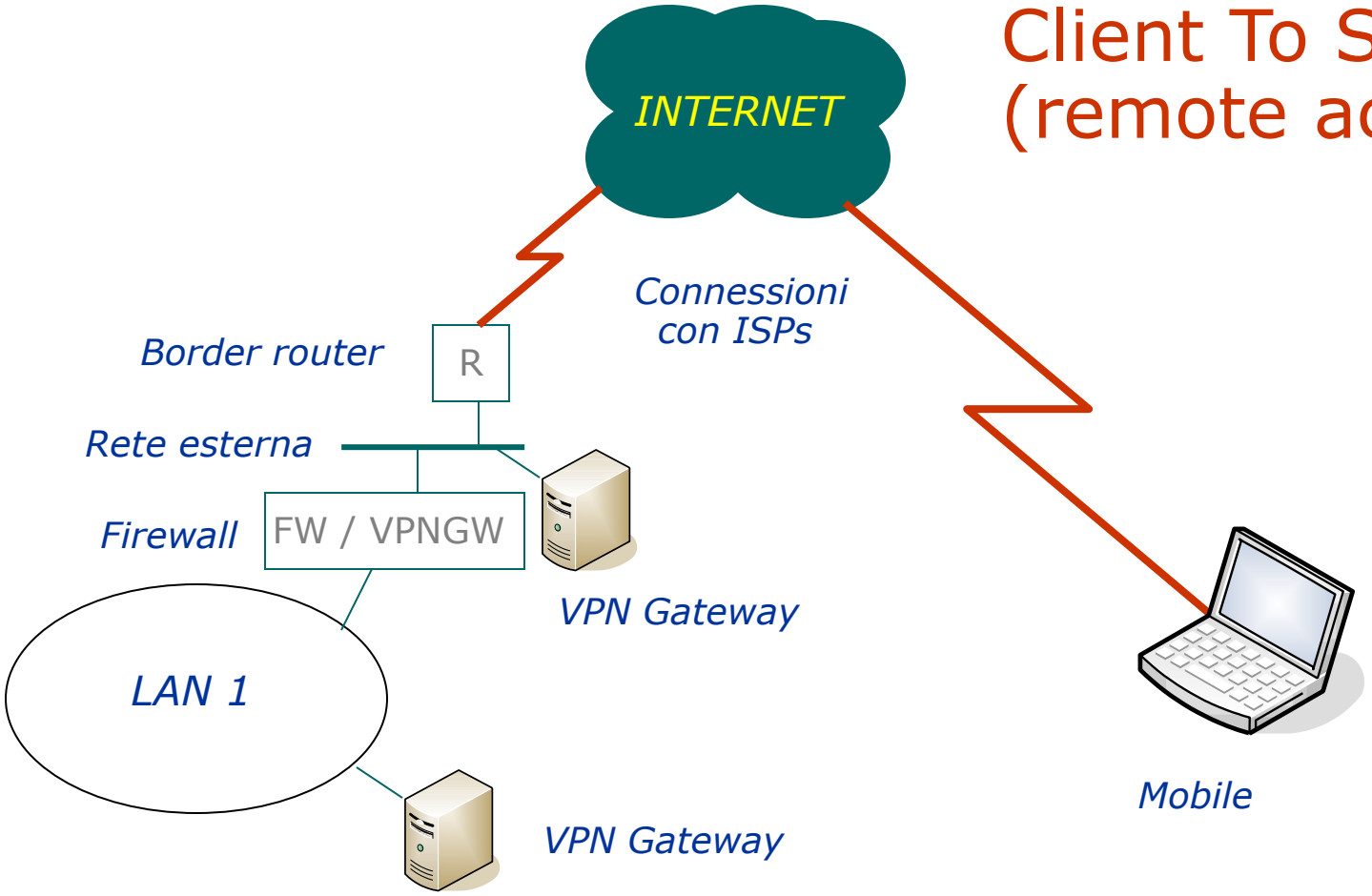
Architetture di VPN

Site To Site VPN



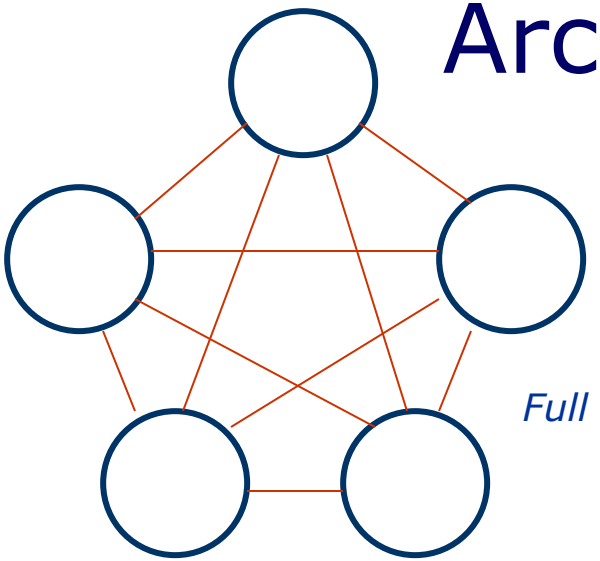
Architetture di VPN

Client To Site VPN (remote access)

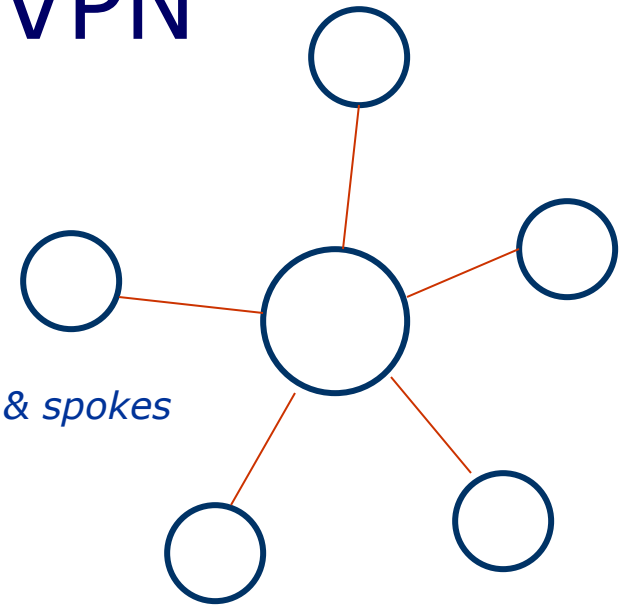


Architetture di VPN

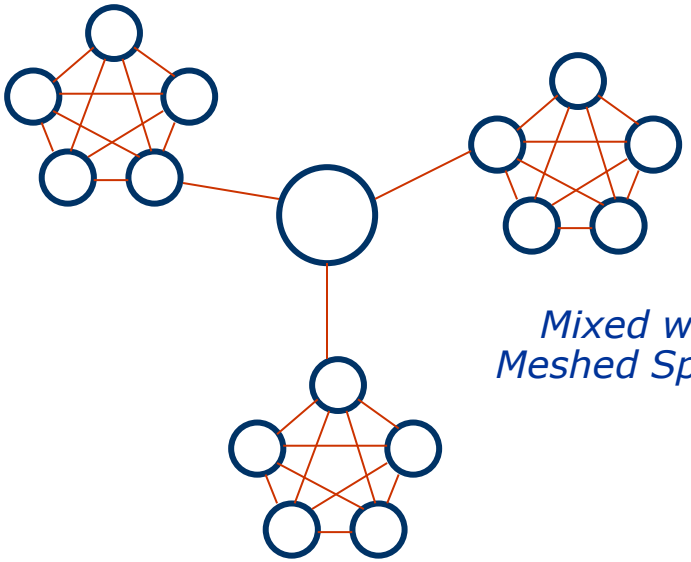
Topologie



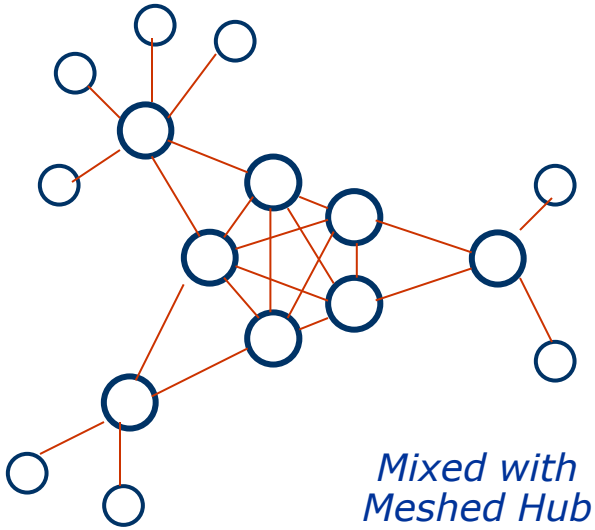
Full mesh



Hub & spokes



Mixed with Meshed Spokes



Mixed with Meshed Hub

Protocolli: PPTP

PPTP – Point-to-Point Tunneling Protocol

Ascend RAS, Windows NT. RFC 2637

Costruito sulla base del PPP, effettua il tunneling a livello 2 (GRE modificato).

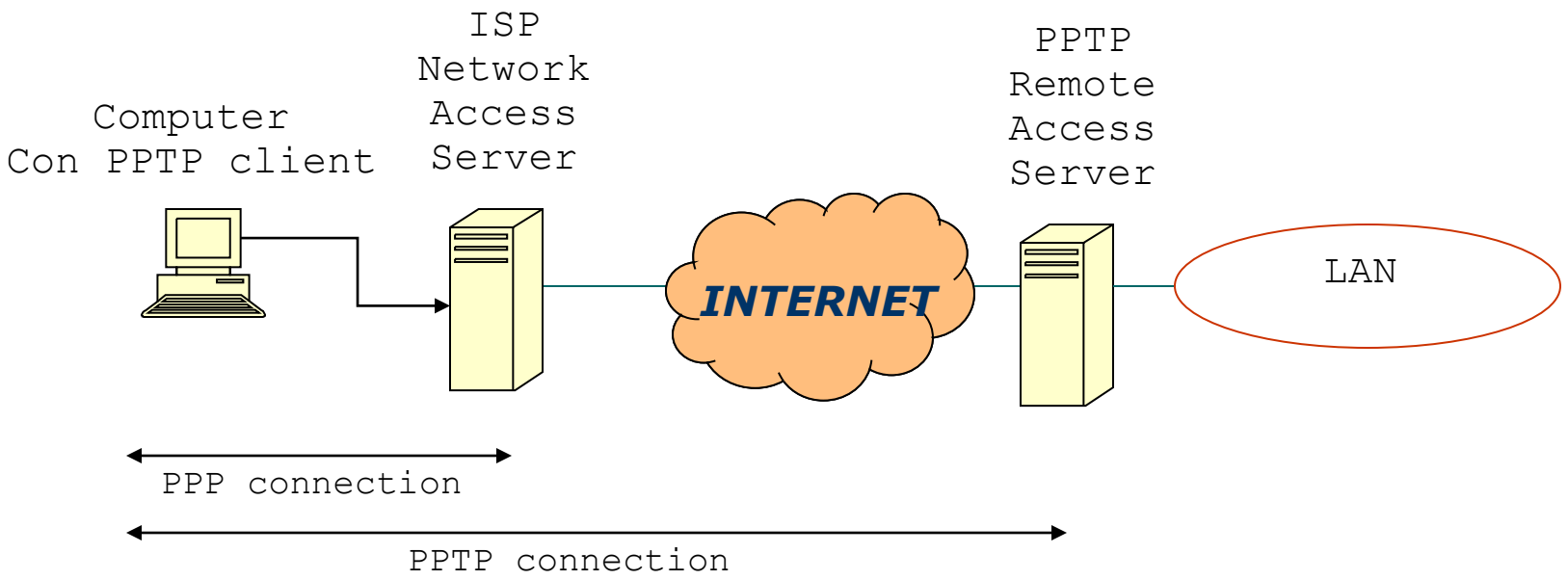
Autenticazione con PAP, CHAP, MS-CHAP

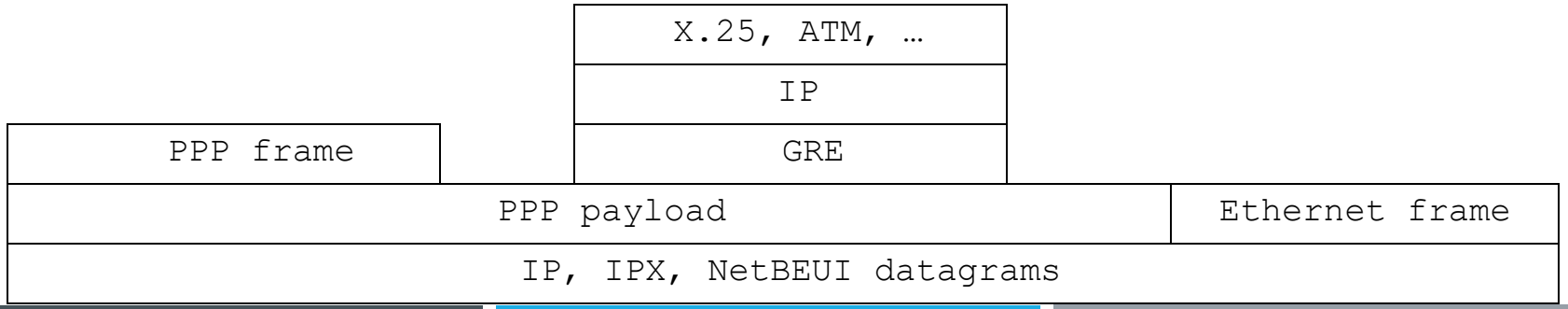
Autenticazione con EAP (RFC 2284)

Encryption con MPPE

Protocolli: PPTP

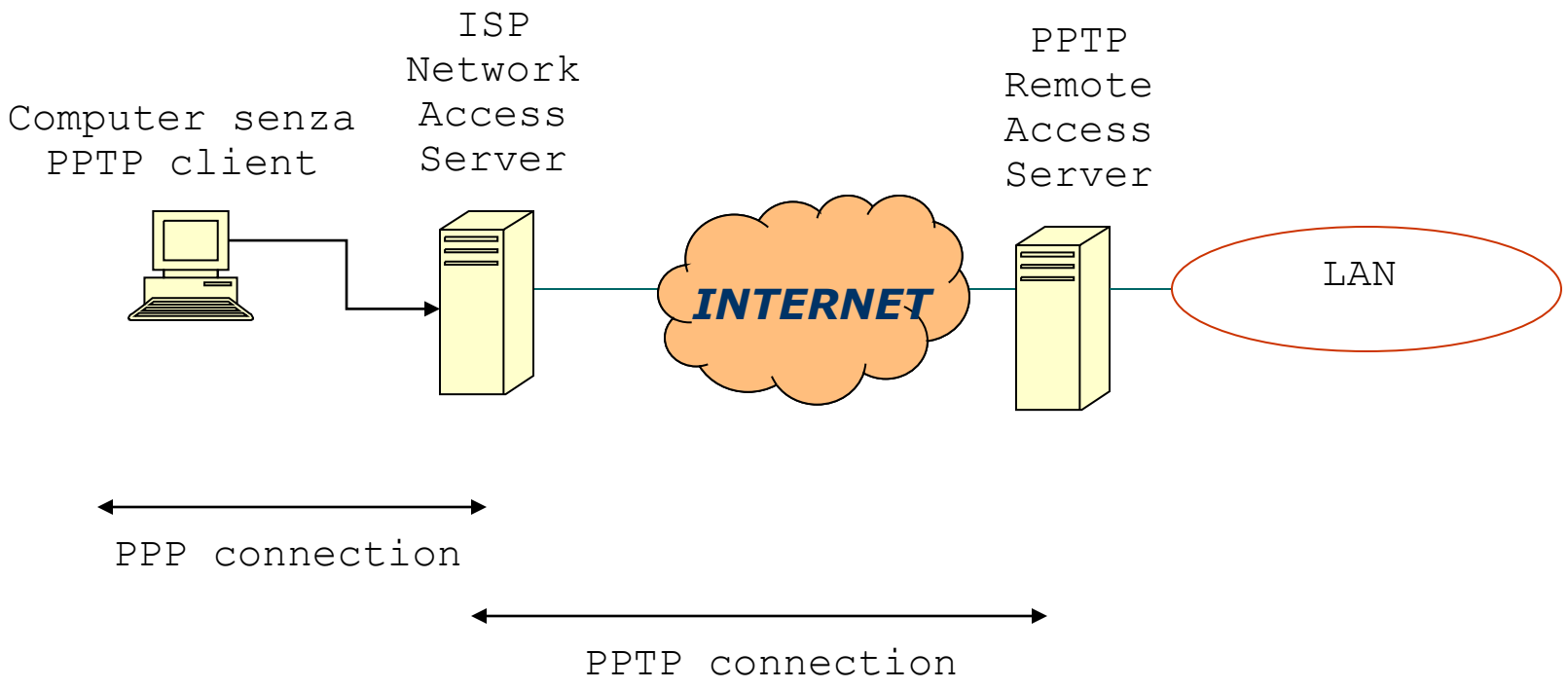
Voluntary tunnel (dinamico)





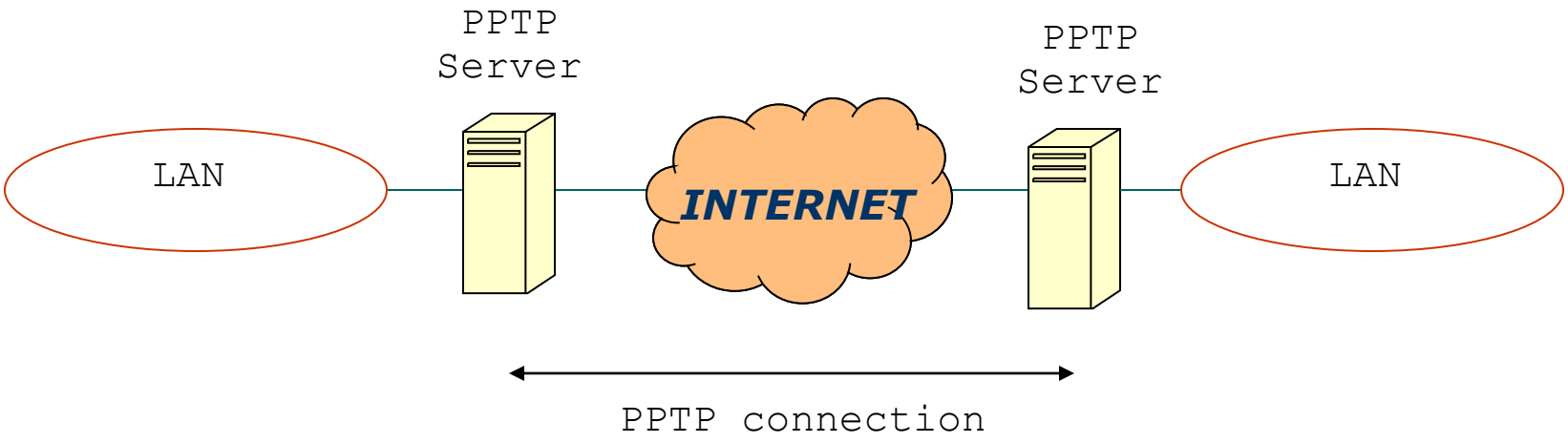
Protocolli: PPTP

Compulsory tunnel (statico)



Protocolli: PPTP

LAN-to-LAN tunnel



Esempio: Microsoft RRAS

Protocolli: L2TP

L2TP – Layer 2 Tunneling Protocol

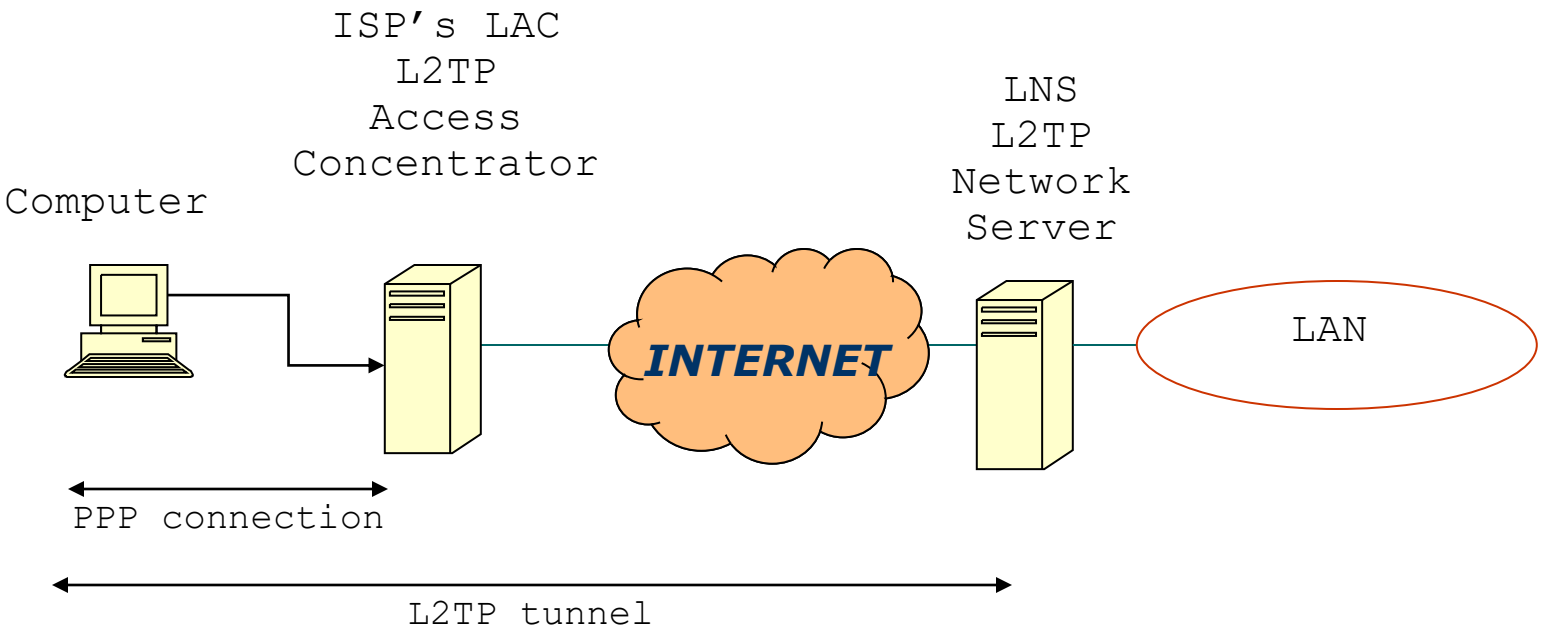
Evoluzione di PPTP e L2F (Cisco), tunneling a livello 2 su UDP, RFC 2661

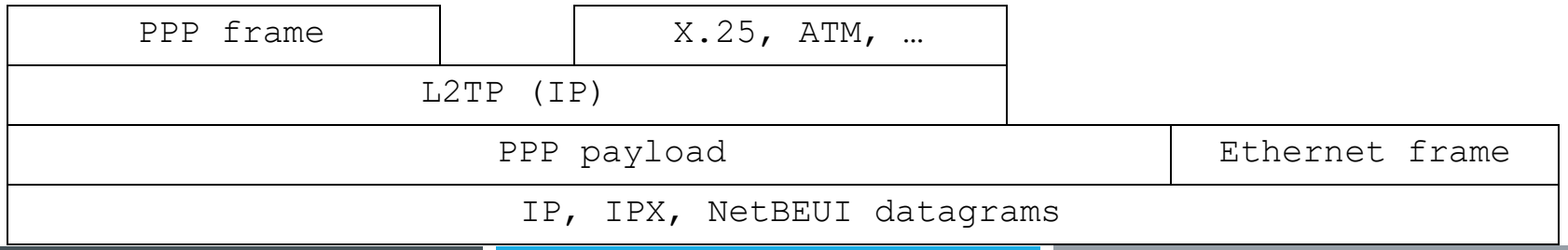
Autenticazione con PAP, CHAP, MS-CHAP, EAP, AH

Encryption con ESP

Protocolli: L2TP

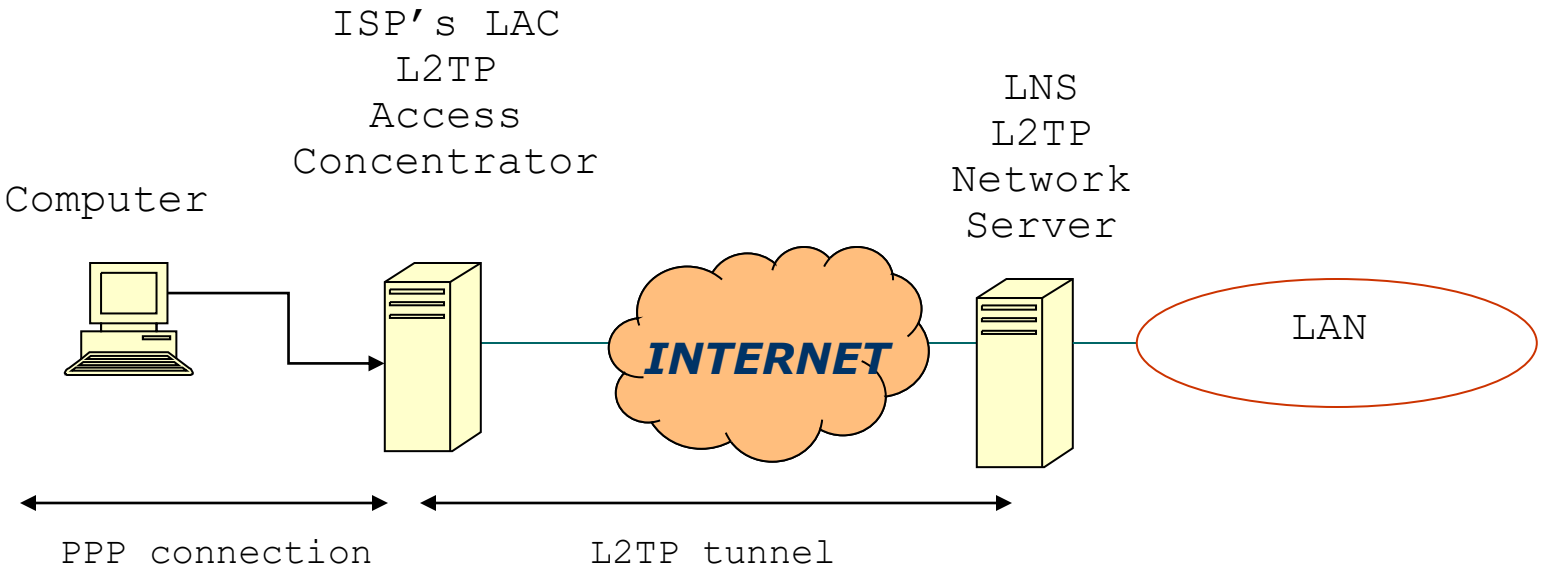
Voluntary tunnel

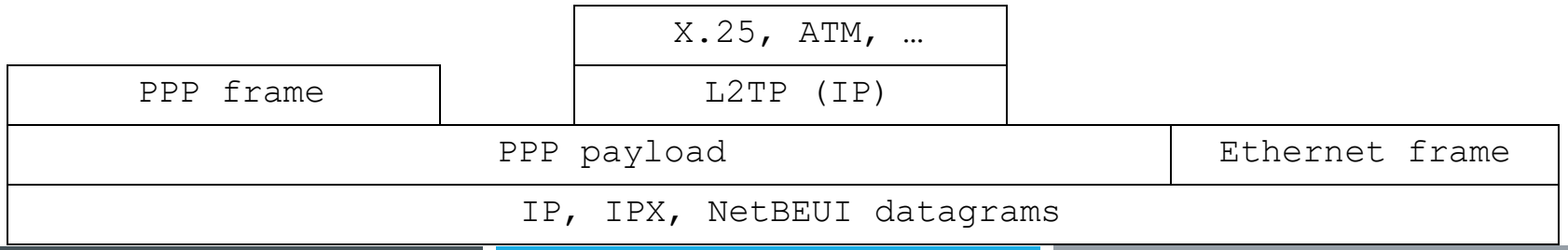




Protocolli: L2TP

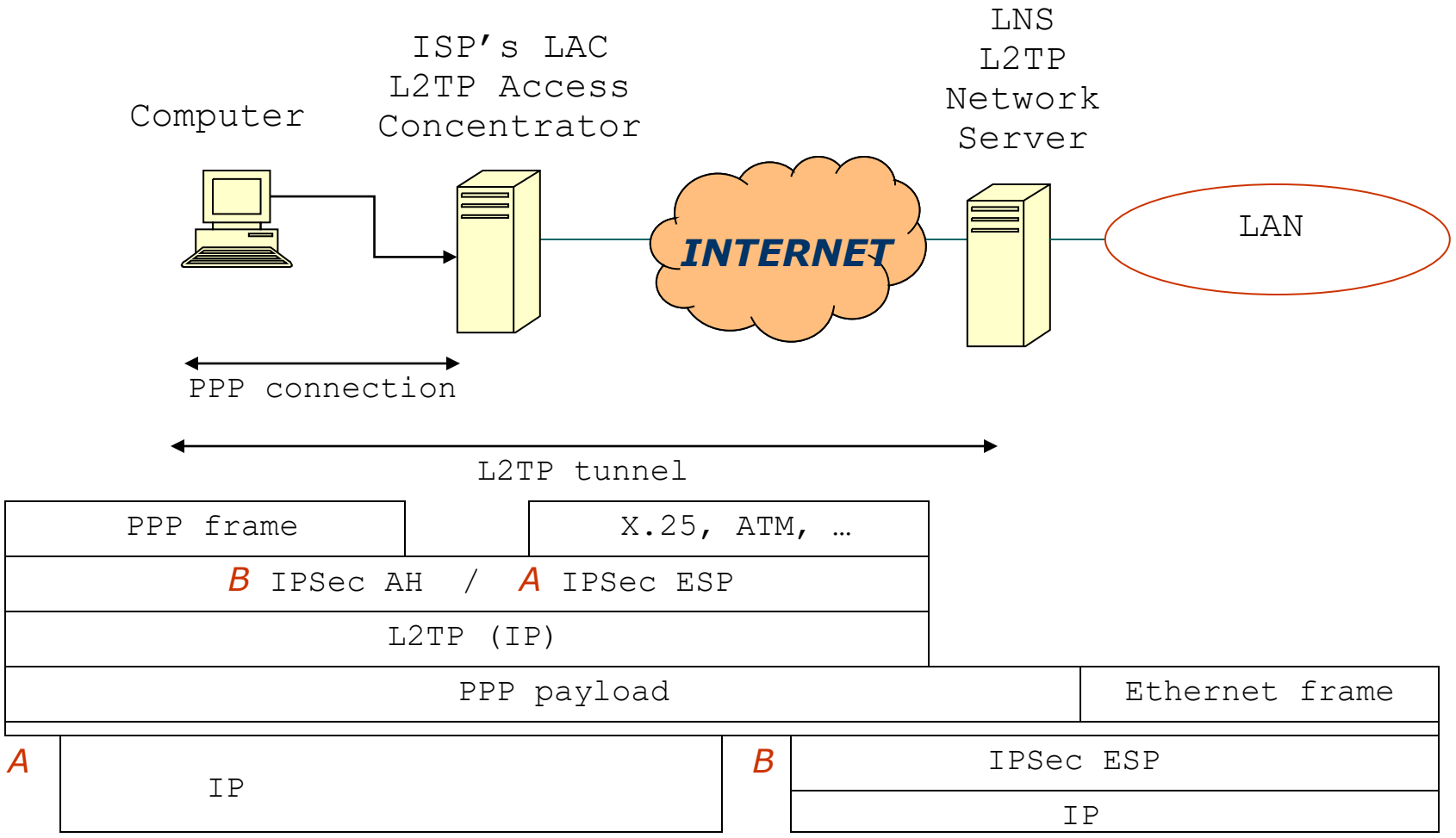
Compulsory tunnel





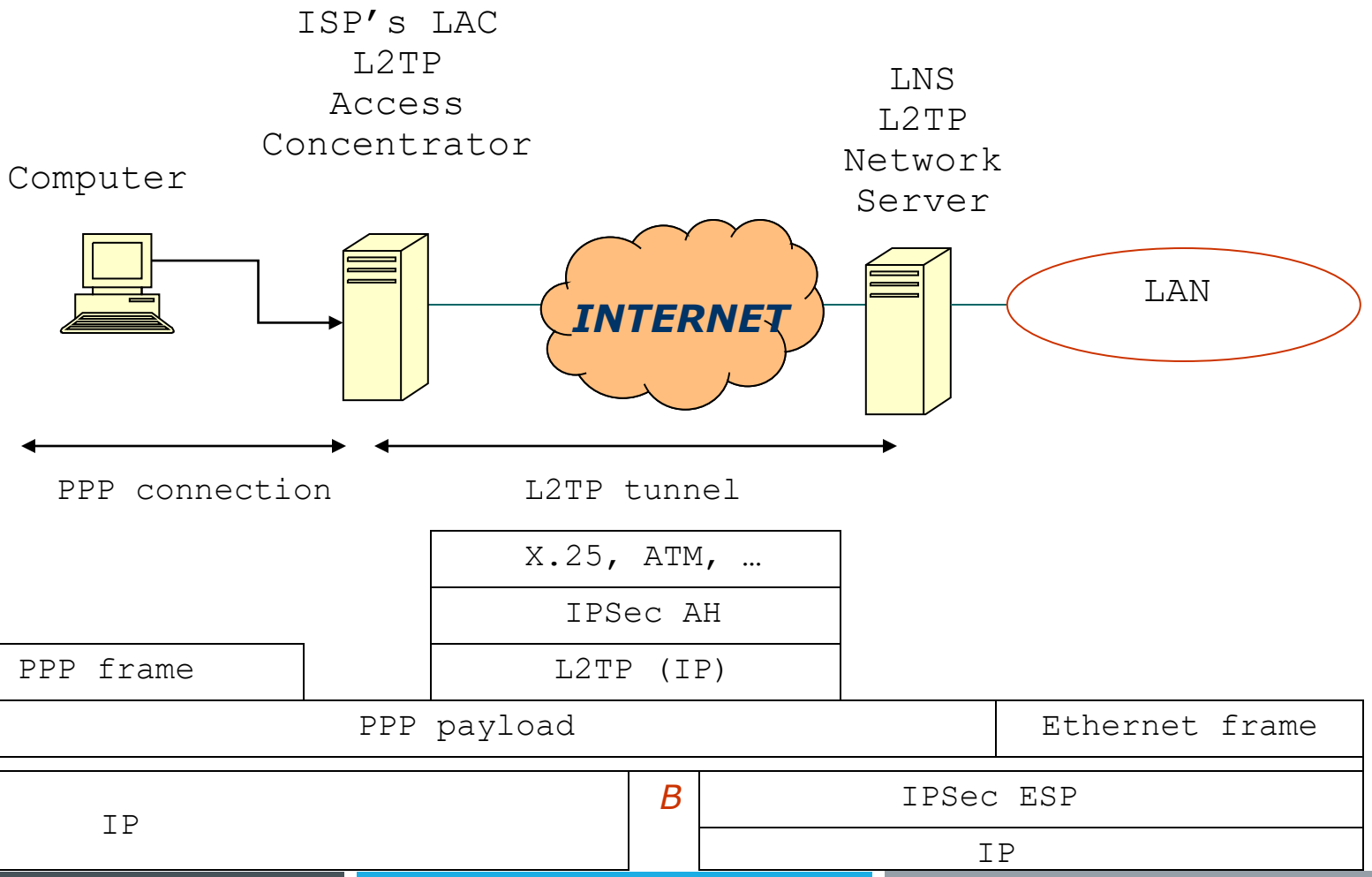
Protocolli: L2TP

Voluntary tunnel con IPSec



Protocolli: L2TP

Compulsory tunnel con IPSec



Protocolli: IPSEC

IPSec – Internet Protocol Security

Livello 3

- ESP, Encapsulating Security Payload
- AH, Authentication Header
- IKE, Internet Key Exchange

Protocolli: IPSEC

IKE: key management

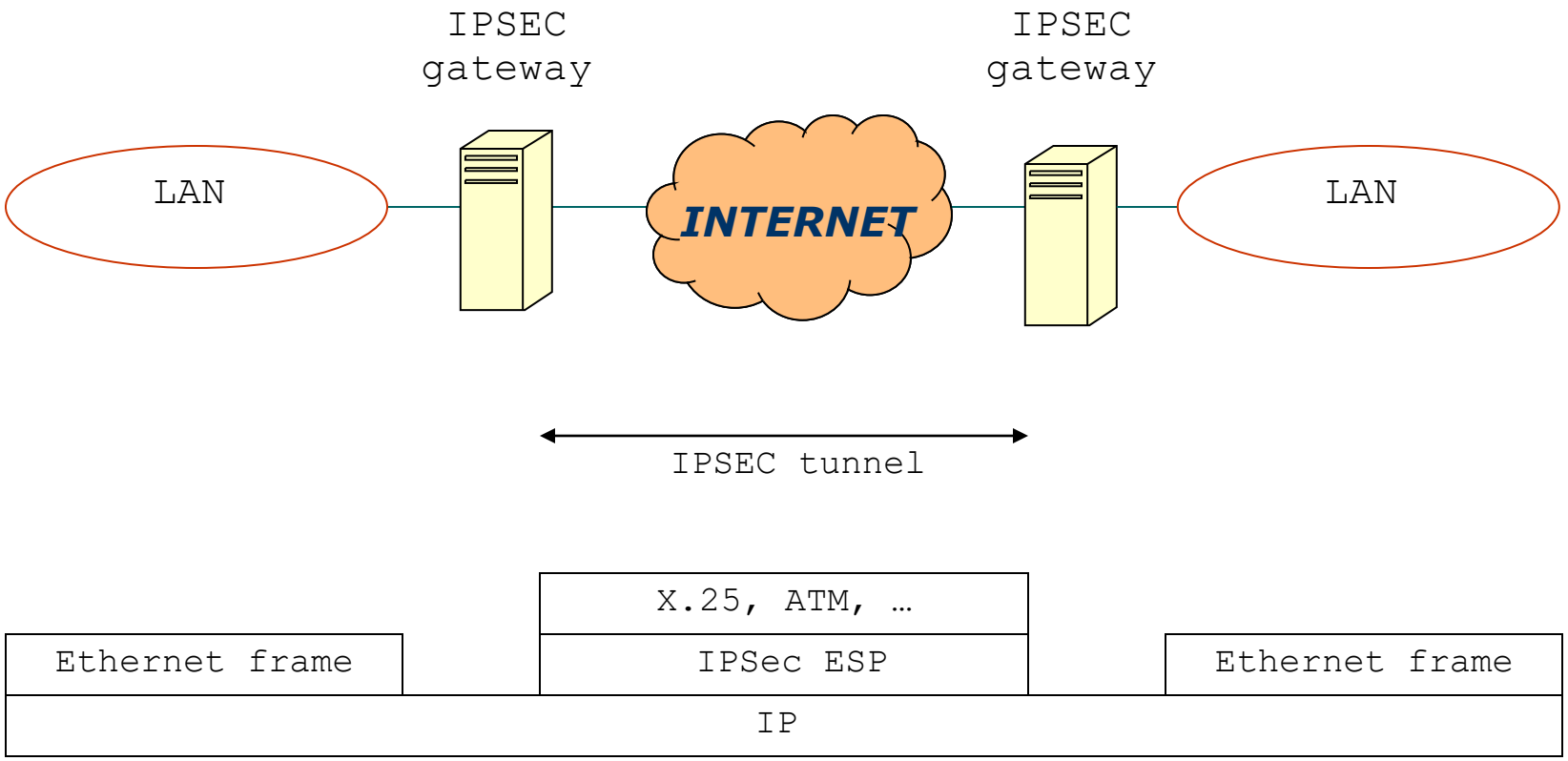
Phase 1 - main mode
stabilisce una coppia di ISAKMP SA, ossia un canale per lo scambio delle chiavi

Phase 2 - quick mode
stabilisce una coppia di IPSec SA, ossia un canale per lo scambio dei dati

Entrambe le fasi sono ripetute periodicamente (prima della scadenza di ciascuna SA) per automatizzare il rinnovo delle chiavi. IKE utilizza UDP porta 500.

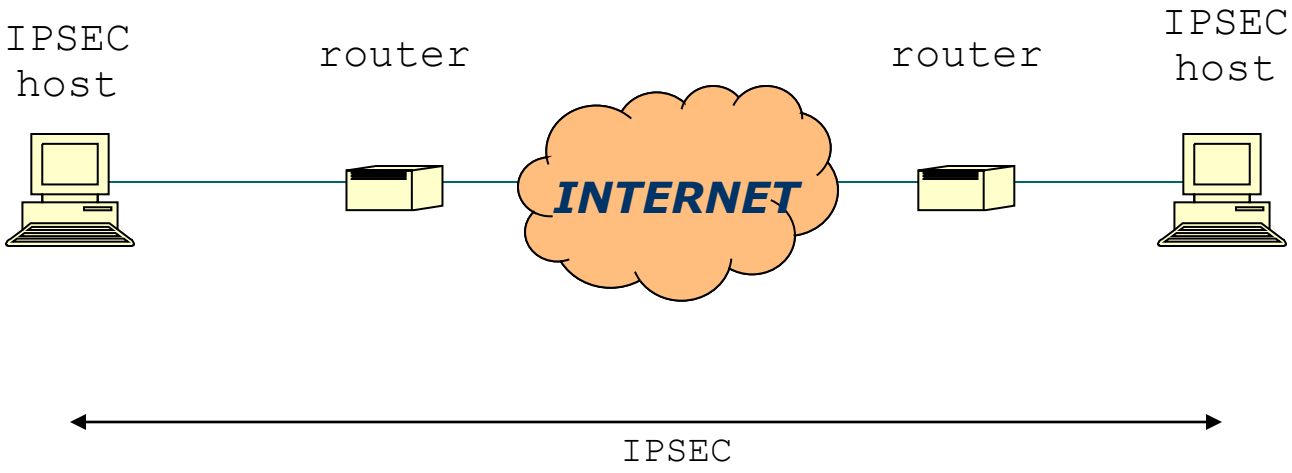
Protocolli: IPSEC

LAN-to-LAN tunnel



Protocolli: IPSEC

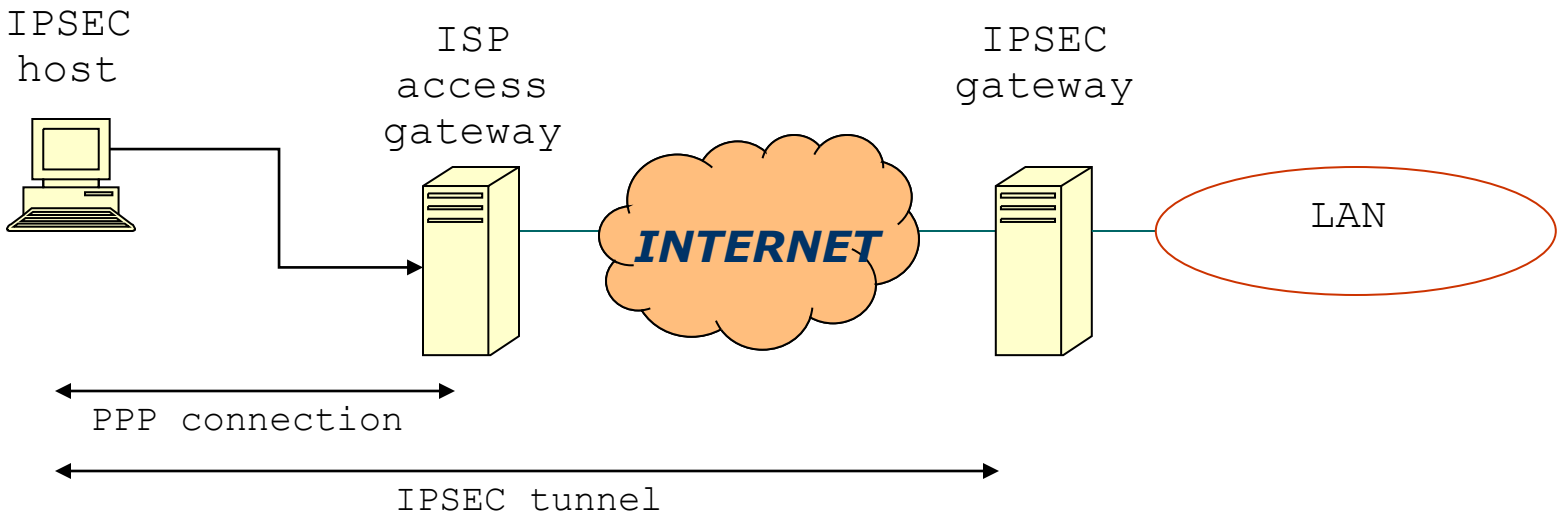
Transport mode

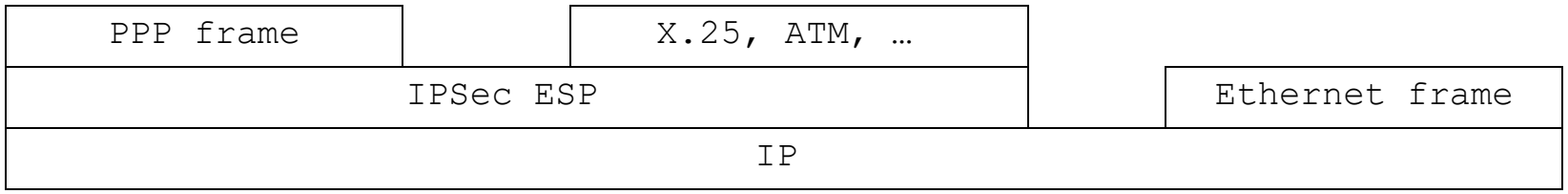


Ethernet frame	X.25, ATM, …	Ethernet frame
IPSec ESP		
IP		

Protocolli: IPSEC

Host-to-LAN tunnel





Protocolli: IPSEC

La diffusione di IPSEC si è scontrata con la diffusione del NAT. IPSEC è infatti incompatibile con il NAT per due motivi

- IKE's payload include l'IP address del computer mittente; dopo il NAT questo viene cambiato invalidando IKE
- AH, e in alcuni casi ESP, elaborano un pacchetto con un header su cui il NAT dovrebbe intervenire

La soluzione è NAT-T (NAT traversal), ossia la capacità di incapsulare in pacchetti UDP l'intero traffico IPSEC

Altre soluzioni

CIPE - Crypto IP Encapsulation

VTUN - Virtual Tunnel

SSL-VPN (commerciali e free)

Ridondanze

HW o appliances: i dispositivi più evoluti hanno la capacità di creare configurazioni Active-Active (anche per load balancing) o Active Passive. Il licensing può variare.

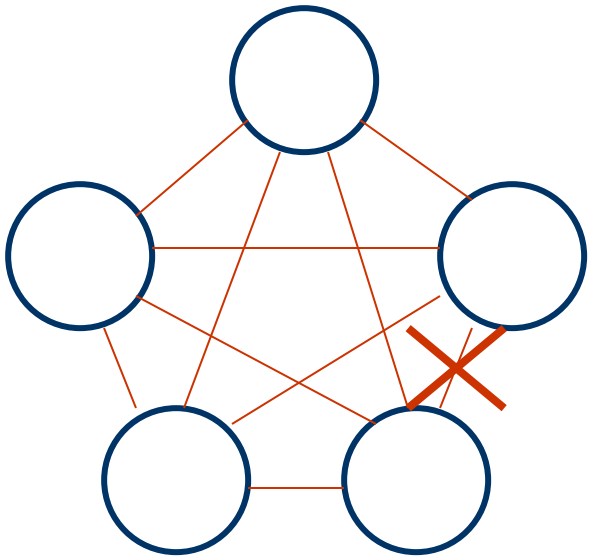
Anche alcuni sw semplici (come OpenVPN) hanno capacità analoghe e consentono di creare VPN GW ridondanti

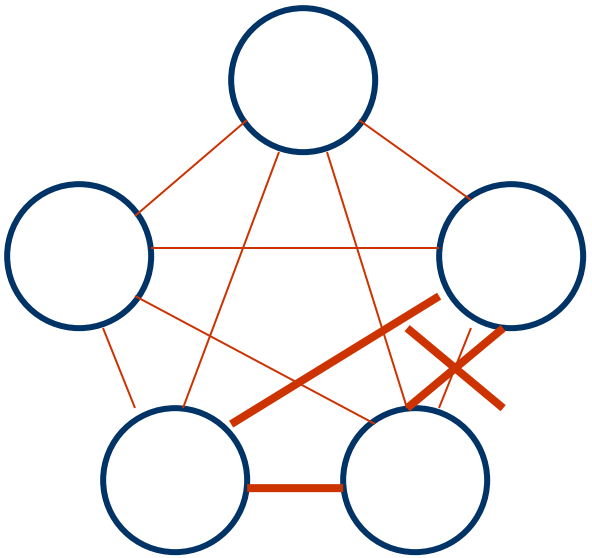
Per i sistemi sw che non hanno capacità di ridondanza intrinseche si può mettere in campo un ambiente di virtualizzazione *(attenzione: in questo modo però si crea un'interdipendenza tra sistemi che probabilmente non è desiderabile)*

Ridondanze

Occorre inoltre osservare che in una topologia full-mesh vi sono delle ridondanze apparenti

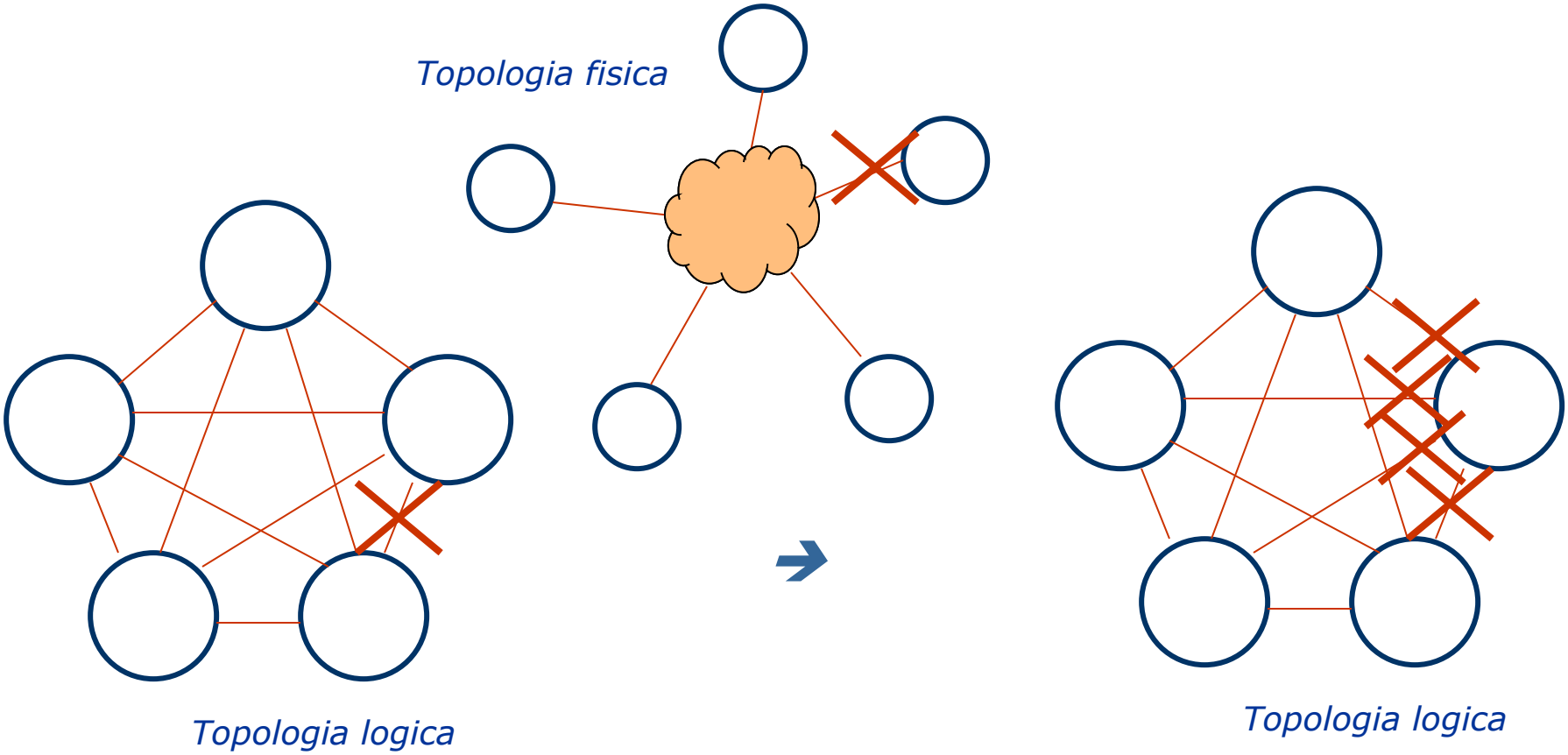
Utilizzando algoritmi di advanced routing come OSPF fra le sedi della full mesh si potrebbe pensare di avere un'interessante ridondanza nelle comunicazioni fra le sedi e le periferie ad esse connesse





Ridondanze

In realtà tutte le topologie fisiche sono hub'n'spokes a meno di non realizzare AS e quindi quella ridondanza in realtà non c'è



Ridondanze

Occorre quindi ridondare il link fisico. Si può fare con più ISP o con uno solo.

- *Con più di un ISP si può diventare Autonomous System, cioè un nodo attivo nella Internet, con responsabilità di sopportare anche traffico altrui. Vi sono anche dispositivi che supportano più connessioni a diversi ISP ma non sono soluzioni generalizzate (es solo email e web)*
- *Con un solo ISP si può invece chiedere un backup per la linea. La soluzione migliore è realizzarlo in tecnologia diversa e che percorra un tragitto fisico diverso da quelli utilizzati dalla linea principale*

OpenVPN

OpenVPN è la più diffusa SSL-VPN opensource

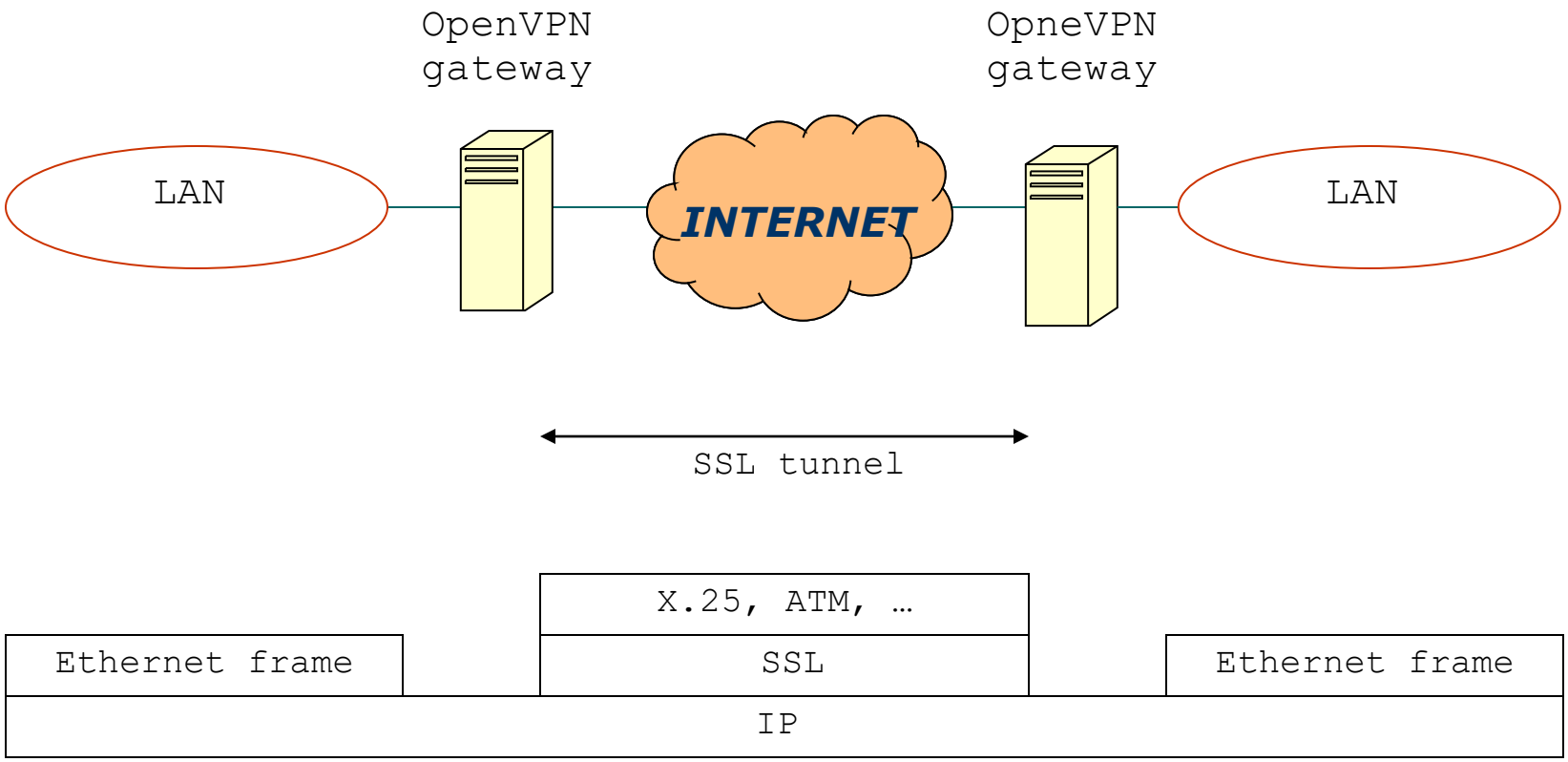
Interamente appoggiata a OpenSSL

Supporta tunneling di entrambi i tipi (L2 e L3), configurazioni site to site e host to site, load balancing/failover gateways, configuration push via internal DHCP

Per Linux, Windows, xBSD, OS X, Solaris

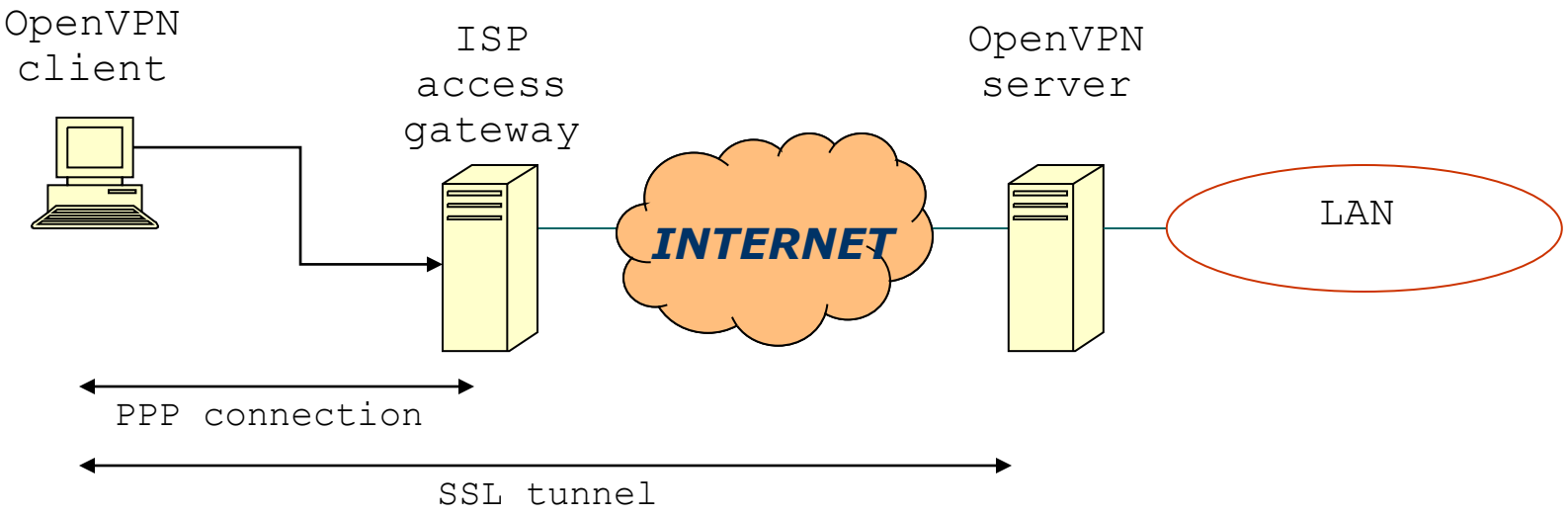
OpenVPN

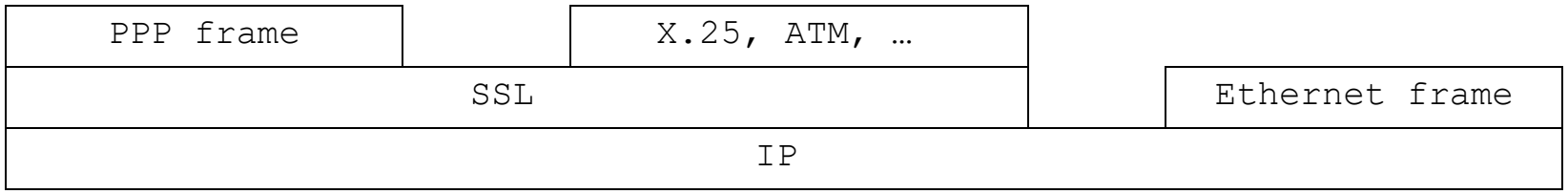
LAN-to-LAN tunnel



OpenVPN

Host-to-LAN tunnel



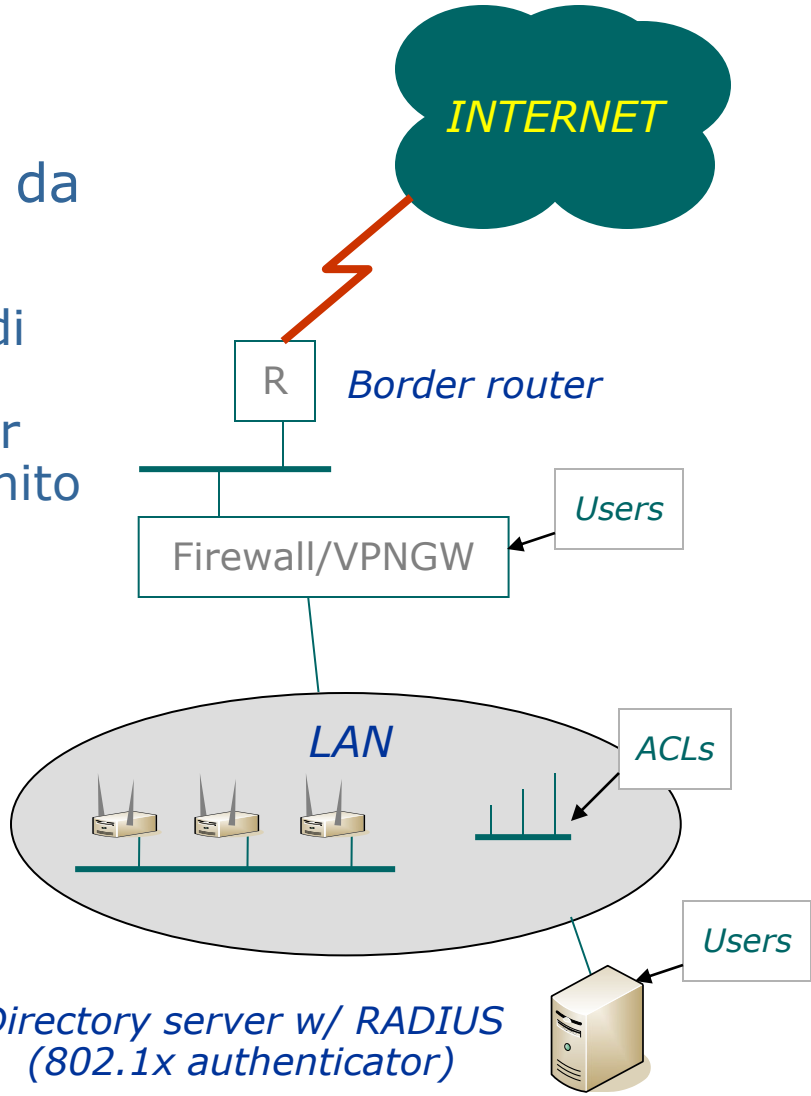


Normalized VPN access

Avere diversi accessi alla rete locale è un'esigenza attuale e diffusa: occorre collegarsi da remoto, dalla sottorete wireless, dalle porte walk-up, oltre che da postazioni fisse.

E' molto comune trovare implementazioni di 802.1x per l'accesso alla rete wireless, di MAC-locking sulle walk-up ports e infine per l'accesso da remoto si usa il Client VPN fornito dal produttore del firewall

In questo modo è difficile avere un controllo generalizzato sui collegamenti alla rete, in quanto i diversi sistemi usano meccanismi di autenticazione incompatibili e/o repository di identità separati. Sarebbe invece auspicabile uniformare il più possibile, soprattutto per quel che riguarda l'autenticazione, i diversi metodi di accesso alla rete

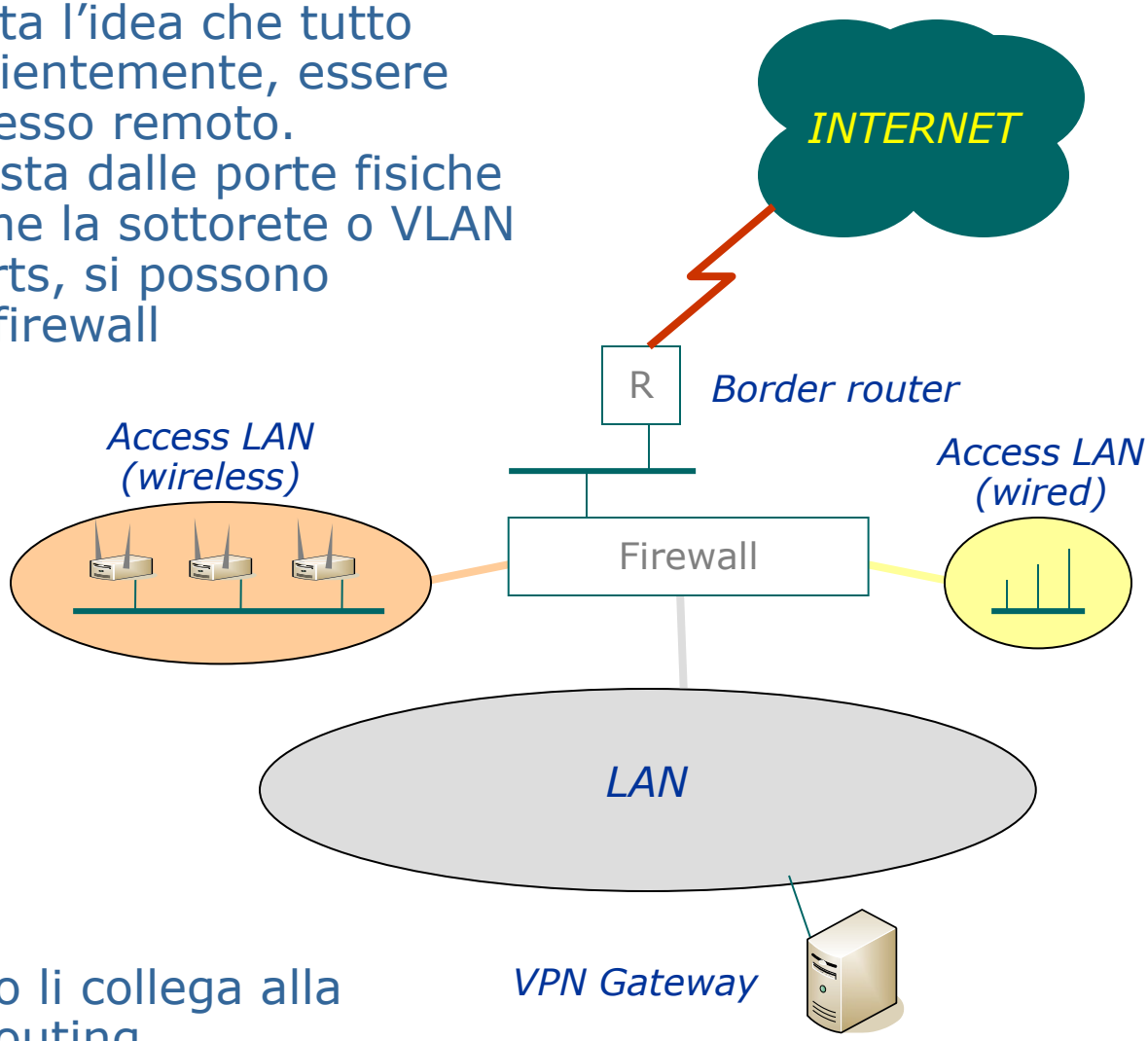


Normalized VPN access

Alla base del ‘normalized’ sta l’idea che tutto possa, facilmente e convenientemente, essere ricondotto a un caso di accesso remoto.
La sottorete o VLAN composta dalle porte fisiche degli Access Point, così come la sottorete o VLAN composta dalle walk-up ports, si possono attestare direttamente sul firewall

Più o meno come fossero DMZ o reti pubbliche, i client vi si connettono senz’alcuna autenticazione particolare, ricevono una configurazione di rete via DHCP e possono comunicare esclusivamente con il gateway VPN

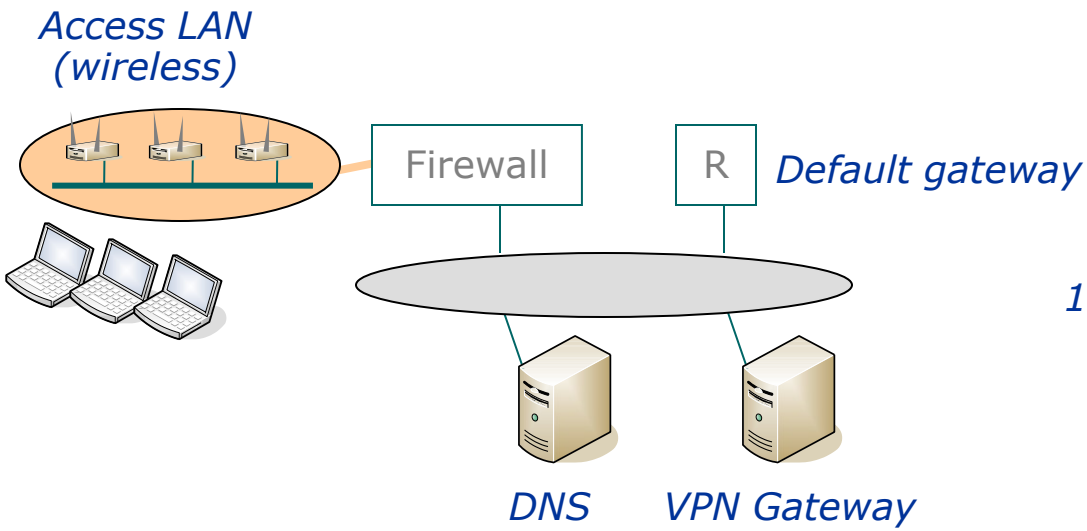
Una volta autenticati questo li collega alla rete locale con bridging o routing



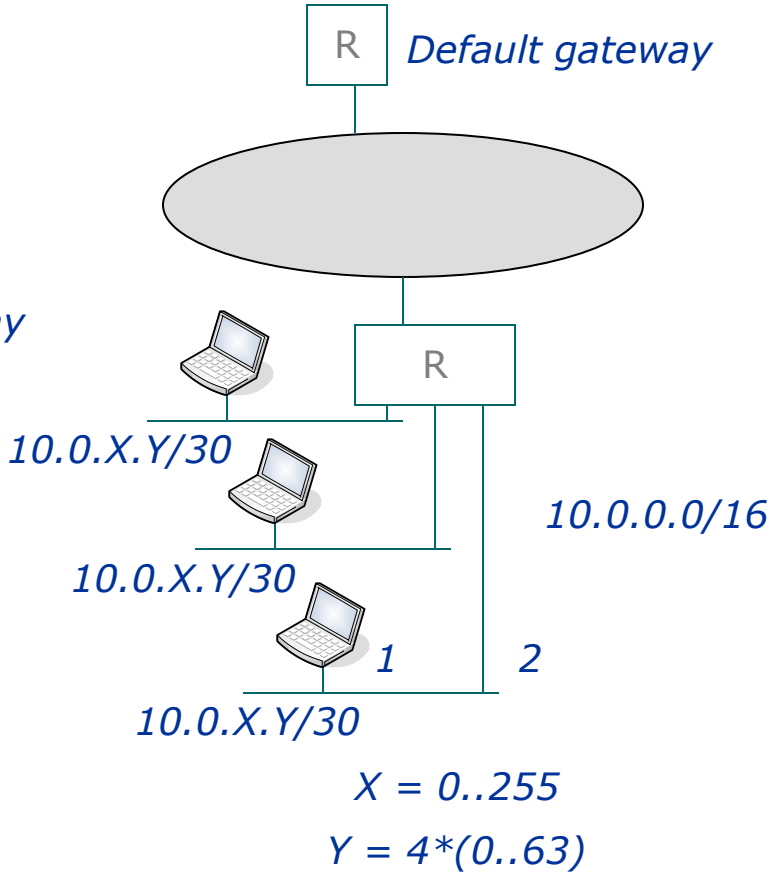
Normalized VPN access

Routing e funzionamento del VPN GW. Ai client mobili si dedica un range di IP address.

VISTA FISICA



VISTA LOGICA



Managing mobility

L’accesso VPN normalizzato è solo il primo passo per l’ottimizzazione degli accessi a una rete o sito singoli. Una rete multisito composita richiede invece ulteriori affinamenti dell’infrastruttura VPN e dei suoi gateway

In particolare occorre indirizzare l’esigenza di mobilità inter-sito, ovvero utenti mobili ma che restano all’interno dell’organizzazione cambiando, anche per brevi periodi, sede.

Sarebbe opportuno quindi che l’accesso normalizzato non fosse limitato alla propria sede, ma a tutte le sedi connesse in VPN

Managing mobility

I problemi tipici della mobilità inter-sito possono sembrare banali, ma lo sono solo apparentemente: il più classico problema è il printing, ma anche la risoluzione dei nomi e l'accesso a Internet

Per esplorare meglio queste problematiche occorre identificare le macro risorse che gli utenti usano ed esplorare quali soluzioni sono disponibili per garantirne l'accesso.

E' possibile adottare due diversi approcci:

- focus on the destination-site
- focus on the home-site

Managing mobility

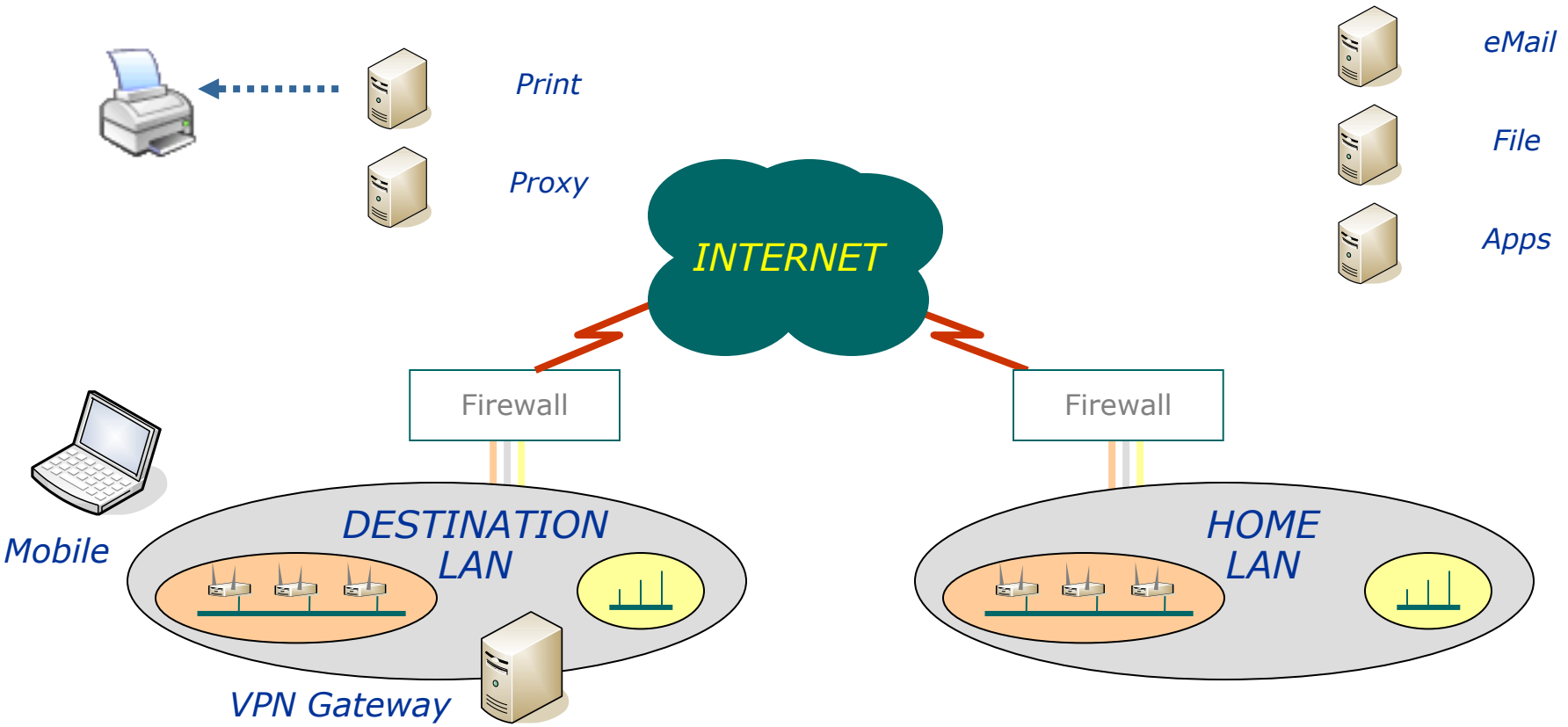
L'utente mobile ha generalmente bisogno di:

- Posta e Calendario — *home*
- Applicazioni aziendali (web, cli-serv, ecc) — *home*
- Informatica personale (Office, ecc)
- Accesso ai file server e documentali — *home*
- Accesso a stampanti — *dest*
- Accesso a Internet — *dest/home*
- Altro (telefonia, applicazioni custom, ecc)

Occorre inoltre disporre di un DNS "enterprise" (cioè valido in tutti i siti dell'azienda)…

Managing mobility

VPN access con focus sul destination site:



Managing mobility

In questa situazione il client si collega e si autentica al VPN gateway della rete di destinzione

- la configurazione di rete per l'autenticazione alle risorse locali (necessaria ad esempio per stampare) è incompatibile con quella della rete di origine
- occorre creare e gestire "profili" di configurazione per i servizi presenti nella HOME LAN (non tutti i software supportano il concetto di "location")
- occorre definire una configurazione del proxy per l'accesso a Internet valida per tutta l'azienda (si può fare con opportune configurazioni automatiche + DNS)
- problema delle stampe, che sono sempre locali
- il routing verso ogni HOME LAN deve funzionare globalmente

Managing mobility

Con il focus sull'home site possiamo spostare la complessità di configurazione dai client all'infrastruttura

L'idea chiave è consentire il routing fra le ACCESS LAN dei vari siti e i VPN GATEWAY di tutti gli altri

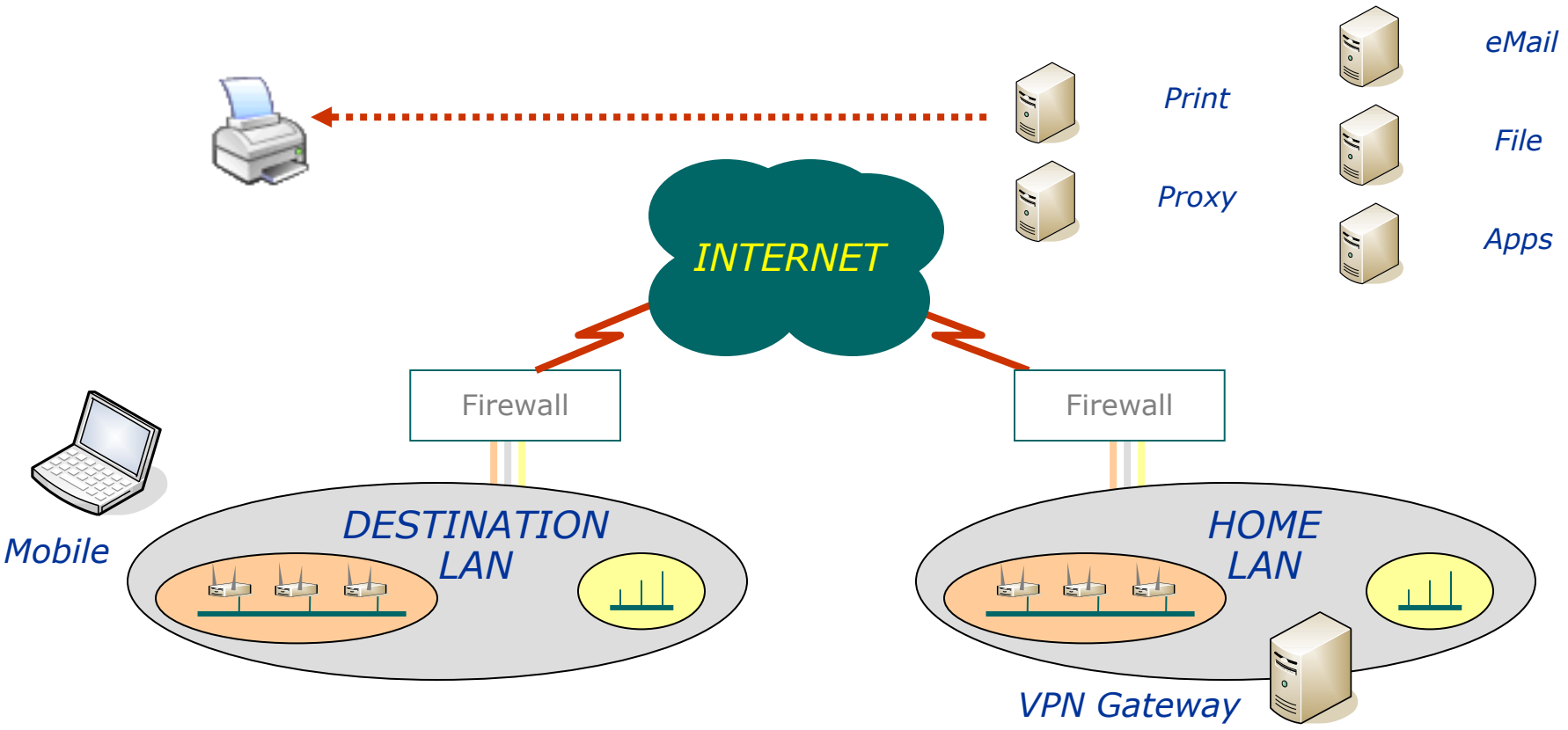
Complesso?!?

Non quanto sembra, grazie al NAT.

Infatti il routing fra le LAN dei vari siti esiste già e costituisce la VPN complessiva site-to-site. Per far sì che un mobile da una qualunque ACCESS LAN si possa collegare al suo HOME VPN GW basta fare il NAT dell'ACCESS LAN sulla DESTINATION LAN e consegnare al mobile un DNS che funzioni ("enterprise") e che risolva correttamente il nome del GW desiderato

Managing mobility

VPN access con focus sullo home site:



Managing mobility

In questa situazione il client si collega e si autentica al VPN gateway della rete di origine ed è nelle stesse condizioni di quando si collega alla rete di origine da fuori, ossia è realizzato un collegamento VPN normalizzato anche per la mobilità inter-sito

L'unica risorsa locale rimane la stampante, il cui utilizzo implica la definizione di code su stampanti remote sui server della HOME LAN e, sui client, le medesime problematiche del caso precedente, come l'installazione dei giusti driver di stampa

Salvo il caso di un'azienda multisite ristrutturata da poco, in cui queta complessità si può più facilmente indirizzare adottando la medesima infrastruttura di file e print server dappertutto (es. Microsoft AD), occorre pensare a una soluzione di

ENTERPRISE PRINTING

Enterprise Printing

E’ la capacità di un sistema di stampa di essere fruibile anche da utenti mobili all’interno dell’organizzazione; come esempio “non tecnologico” si può pensare alla seguente soluzione

- Si standardizza un certo numero (limitato) di stampanti di rete dotate di capacità di spooling autonomo (es LPD o JD)
- Si adotta una naming convention per le stampanti “enterprise”, che ne identifica facilmente il sito
- Si pubblicano i nomi delle stampanti sull’Enterprise DNS
- Si configurano tutti i PC mobili con lo stesso driver di stampa
- Si istruiscono gli utenti su come “trovare” le stampanti nei siti

Enterprise Printing

Dal primo punto è facile pensare che la soluzione finale debba essere per forza di cose “monovendor”; in tal caso si può optare per la soluzione HP, che si basa sull’Universal Print Driver

- Supporto per un gran numero di modelli di stampanti
- PCL5 e 6, PostScript Level 2 e 3
- Configurazione dinamica dei dispositivi deployabile anche in modo centralizzato
- Managed Print Policies (es uso del colore) per certi dispositivi
- Direct IP printing

Network Devices

Infrastrutture di rete

Come è fatta una rete?

I blocchi principali sono:

- Backbone
  dispositivi di rete che realizzano l'ossatura portante di tutta l'infrastruttura
- Datacenter
  dispositivi di rete adatti al collegamento dei server centrali al backbone
- Distribuzione
  dispositivi periferici e per il collegamento dei client

Dispositivi attivi

Si può definire perimetro di rete l'insieme di quei dispositivi che possono trasmettere informazioni all'esterno del confine logistico del sito in esame (border router, firewalls, access points, ecc.)

- Dispositivi "di perimetro"
- Dispositivi "interni"
- Dispositivi "managed" e "unmanaged"

Dispositivi attivi

Alcune scelte di sicurezza

- warning banners
- accesso sicuro (restrizioni, AAA, SSH, SNMPv3)
- disabilitare servizi non necessari
- routing protocols
- Misure antiattacco (spoof, DOS, frags)
- logging
- blocco delle porte
- upgrades del firmware
- sicurezza fisica

Dispositivi attivi

Warning banners

Non impediscono nulla, ma servono (in molte legislazioni) per dare valore alle eventuali prove da fornire in sedi legali contro un attaccante.

Di solito si dichiara:

- *Utenti autorizzati e uso autorizzato*
- *Logging e monitoring*
- *Attività sospette o illecite avranno conseguenze legali*

Accesso sicuro

Scegliere i metodi di accesso più adatti e disabilitare gli altri

- *Porta seriale (console)*
- *Telnet, SSH*
- *Web (HTTPS)*
- *SNMP*
- *TFTP*

Dispositivi attivi

Attacchi comuni ai dispositivi attivi sono:

- *Spoofing dell'IP addr della stazione di gestione*
- *Attacchi e sniffing di password*
- *TCP session hijacking*
- *Compromissione dell'autentication server*
- *Dial-in*
- *DOS*

Dispositivi attivi

Accesso sicuro

- *Uso di ACL su IP addr*
- *Management VLAN*
- *Accesso con server AAA*
- *Accesso con SSH*
- *Accesso con HTTPS*
- *Attivazione timeout di sessione*

Metodi di autenticazione

- *Username e password*
- *TACACS, TACACS+, RADIUS*
- *Certificati digitali*

Uso delle autorizzazioni

- *Diversi privilegi per diversi utenti (esempio per "read", "port config" e "all config")*

Dispositivi attivi

Gestione delle reti: SNMP

Il Simple Network Management Proocol è disponibile in praticamente tutti i dispositivi di rete maneggiabili, comprese le stampanti, i printer server, i fax server e, spesso in modo nascosto, anche i sistemi operativi.

Semantica del protocollo SNMP: GET, GETNEXT ("WALK"), GETBULK, SET, TRAP

- SNMP Agent
- SNMP Manager

Dispositivi attivi

Sicurezza di SNMP

SNMP è usato diffusamente per monitorare e configurare dispositivi di rete e anche computer o software

- *SNMP version 1, 2c e 3*
- *Uso di ACL*
- *Specificare SNMP per porta*
- *Blocco di SNMP al firewall*

Dispositivi attivi

Dispositivi multilayer

I moderni switch e router sono spesso dotati di funzionalità appartenenti ad altri layer; ad esempio:

- switch dotati di “layer 3 switching”, ovvero una funzionalità di routing semplificata e adatta al routing dei pacchetti fra le VLAN
- router dotati di “layer 2 switching”, ad esempio DLSW, ossia la capacità di effettuare bridging per protocolli non routable (come ad esempio LLC)
- switch dotati di funzionalità “layer 7”, come i bilanciatori di carico applicativo

Dispositivi attivi

Rimozione di funzionalità non necessarie

In ciascun dispositivo vi sono un certo numero di funzioni abilitate per default. Ad esempio:

- *Telnet server*
- *Web mgmt interface*
- *ro SNMP con community "public"*
- *Source Routing*
- *L2 bridging*
- *ICMP*
- *…*

Dispositivi attivi

Esempio: ACL anti-Spoofing

Per un border router (o firewall), si può impostare il blocco dei pacchetti in ingresso con i seguenti Source Ips:

- *127.0.0.0/8 (loopback)*
- *10.0.0.0/16, 172.20.0.0/12, 192.168.0.0/16 (RFC1918)*
- *224.0.0.0/4, 240.0.0.0/5 (multicasts)*
- *255.255.255.255/32 (broadcast)*

Ovviamente occorre bloccare i pacchetti in ingresso con Source Ip uguale a indirizzi della rete interna. E' anche utile filtrare i pacchetti in uscita (*egress filtering*) lasciando passare solo quelli delle network usate e provenienti dai server stabiliti.

Dispositivi attivi

Sincronizzazione del tempo con NTP

Non contribuisce alla protezione da particolari attacchi, ma permette di mantenere informazioni coerenti nei sistemi centralizzati di logging. Utile nel caso di necessità legali.

Port locking

Permette la protezione da allacciamenti indesiderati in rete. MAC locking, 802.1X port authentication

Dispositivi attivi

Sicurezza fisica

I dispositivi infine non devono essere accessibili fisicamente:

- *Armadi e sale chiuse a chiave*
- *Accessibili solo a persone autorizzate*
- *Controllo degli accessi*
- *Backup delle configurazioni*
- *Protezioni contro il fuoco, calore, acqua…*
- *Protezione da alterazioni della corrente elettrica*

Legacy networking

Non esiste solo il TCP/IP!

In giro per le reti si può trovare di tutto! E' necessario conoscere i rudimenti le tecnologie più vecchie per "sapere cosa fare" quando si deve intervenire in ambienti dove queste sono ancora in uso.

Nelle aziende informatizzate da tempo ci può essere ancora IPX, nelle Università DecNet, nelle piccole realtà NetBIOS, dove ci sono gli AS/400 può ancora circolare il DLC, eccetera

Pur se meno di frequente, si possono ancora trovare soluzioni inconsuete nel livello fisico: reti con tecnologie ATM, Token-Ring o FDDI possono essere ancora in giro e vanno riconosciute e gestite.

Legacy systems

SNA

E’ una architettura di rete definita da IBM e ancora molto diffusa soptattutto in ambito bancario e assicurativo, e dove esistono sistemi mainframe.

La gerarchia è fatta tra le PU (physical units) e le LU (logical units), ad esempio i computer e i loro terminali e stampanti

Le reti di mainframe (tipicamente usati da banche e assicurazioni) sono tutte logicamente connesse tramite SNA, all’occorrenza incapsulata in TCP/IP (AnyNet) o mediante altri protocolli di trasporto (es DLSW di CISCO)

All’interno dell’architettura è stata successivamente definita anche l’APPC/APPN, concettualmente simile al networking TCP/IP, ma di livello 2

Protocol Encapsulation

PROTOCOL ENCAPSULATION

Con i protocolli si fa di tutto e nulla vieta di riempire il payload di un pacchetto del protocollo A con segmenti di traffico del protocollo B. Questo consente, a vari livelli dello stack, di trasportare informazioni attraverso reti “aliene”; SNA over TCP/IP, ma anche NBT sono tipici usi attuali dell’encapsulation.

Due mainframe distanti possono essere quindi collegati in APPC fra loro tranquillamente passando attraverso un trasporto TCP/IP che incapsula il protocollo (non routabile) APPC

Non esiste solo il TCP/IP!

Management Station

Network Management Station

E’ un computer dedicato alla configurazione e al monitoraggio di dispositivi di rete; solitamente è anche il manager SNMP e la destinazione delle SNMP traps programmate nei dispositivi.

Network Management Frameworks

Tivoli NetView, HP OpenView. Sono ambienti software dedicati alla realizzazione di sofisticate management stations. Sono dei framework, cioè sono vuoti: forniscono solamente il supporto ai protocolli di base (SNMP), al logging e alla correlazione degli eventi, alla realizzazione di layout grafici della rete e dei sistemi connessi. I Vendor dei dispositivi li arricchiscono con plug-in specifici, che implementano le funzionalità necessarie alla configurazione e alk monitoraggio dei loro dispositivi (di rete e non).

Monitoraggio

Il monitoraggio dei dispositivi di rete permette di misurarne lo "stato di salute".

- *Failures*
- *Prestazioni*
- *Colli di bottiglia*

Sono disponibili alcune tecnologie, tutte basate su un modello *agent* + *manager*

- *SNMP RMON*
- *NetFlow*
- *sFlow*

Monitoraggio

SNMP/RMON-I/RMON-II

Fornisce statistiche basate su una semplice osservazione delle porte (pacchetti e bytes, errori, collisioni): *interface counters.*

Più o meno tutti i dispositivi dotati di un agente SNMP forniscono almeno i contatori di base. I contatori e tutte le altre variabili sono comunque sempre definite nel MIB.

Monitoraggio

NetFlow

Diffusa tecnologia proprietaria CISCO che fornisce informazioni più dettagliate (come statistiche sui protocolli usati).

Non c'è buona standardizzazione essendo una tecnologia proprietaria. L'agente usa inoltre molta CPU, almeno nei dispositivi CISCO.

Monitoraggio

sFlow

RFC 3176, recente. Basata sul campionamento di pacchetti.

Fornisce una quantità di informazioni in più rispetto alle precedenti (L2 to L7, es. headers, 802.1q, userid 802.1x, ecc.).

Se realizzata in HW non impatta le prestazioni dei dispositivi o della rete. Low cost.

Monitoraggio

sFlow

Pur non fornendo informazioni sull'intero traffico ma solamente su un campione dello stesso, può essere sufficientemente efficace per aumentare l'efficienza dei sistemi di monitoraggio, di analisi e di identificazione (p. es. IDS).

Protocolli

802.1q: VLAN

Servono per partizionare la rete in domini separati.

Un gruppo di switch (backbone, datacenter e distribuzione) può condividere un insieme di VLAN in modo che il partizionamento logico della rete sia indipendente dal layout fisico della stessa.

Esistono VLAN per porta (ciascuna porta degli switch appartiene all'una o all'altra VLAN) e VLAN per protocollo; in questo secondo caso è possibile definire diversi layout virtuali della rete, a seconda del protocollo; ad esempio realizzare diversi segmenti per IP (collegati con router) e un'unica rete piatta per LLC e altri protocolli non routable.

802.1q è supportato anche dagli access point, dai router e dai server (es VMWare); questo è necessario per far sì che le porte fisiche consentano diversi collegamenti logici alle VLAN disponibili*

Protocolli

Management VLAN

Un uso basilare delle VLAN nel disegno di una rete di qualunque dimensione (eccetto forse le reti “casalinghe”) consente di definire e realizzare una

rete di gestione dei dispositivi

la cosiddetta “Management VLAN”, dedicata alla gestione dei dispositivi stessi. Su questa rete si affacciano gli IP address di gestione degli switch e dei dispositivi di rete, e la stazione di gestione (SNMP ecc) dell’intera rete.

La “Default VLAN” è particolarmente adatta a questo uso, in quanto ogni porta di uno switch configurato in fabbrica vi appartiene a meno che non venga riconfigurata.

Protocolli

Definizione di VLAN per porta

Ciascuna VLAN è definita da un VLAN-ID (e altre caratteristiche)

Ciascuna porta dello switch collegata a utenze terminali appartiene solitamente a una sola VLAN; il traffico intra-VLAN risolvibile localmente è gestito dallo switch stesso

Nel gergo delle reti i pacchetti appartenenti a una VLAN che devono attraversare i confini di uno switch si dice che vengono "colorati", ossia al pacchetto viene aggiunto un TAG che contiene informazioni sulla VLAN di appartenenza.

Alcune porte dello switch, tipicamente gli uplink ad altri switch o i collegamenti ai server che supportano 802.1q (esempio: nodi dell'infrastruttura virtuale) hanno perciò una diversa configurazione, e sono denominate appunto TAGGED, perché trasportano i pacchetti con TAG da un sistema all'altro.

Protocolli

L3

Gli switch evoluti sono multilayer e consentono di gestire anche il routing. La soluzione è particolarmente efficiente perché di solito il Layer 3 è implementato con la stessa tecnologia dello switching, cioè in HW (ASIC ecc) e quindi molto efficiente.

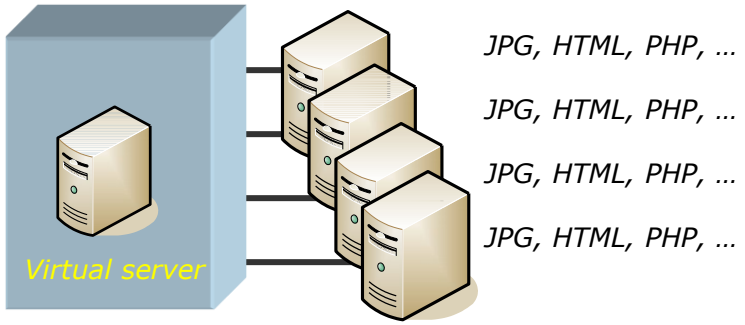
Uno switch L3 consente cioè di definire, in ogni VLAN, una interfaccia di rete virtuale e di assegnarle un indirizzo; questo indirizzo può diventare per esempio il default gateway per quella VLAN (uso più comune).

Le funzionalità di livello 3 vanno abilitate globalmente nello switch, oppure vengono fornite dal Vendor come funzionalità addizionali o installabili

Protocolli

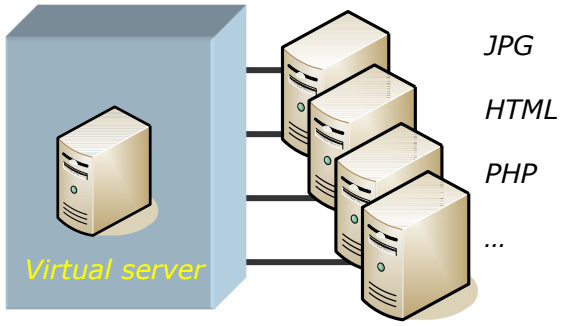
Load balancers

Sono switch dotati di particolari funzionalità a livello applicativo, utili per distribuire il carico su più server identici fra loro (politiche RR o least connection)



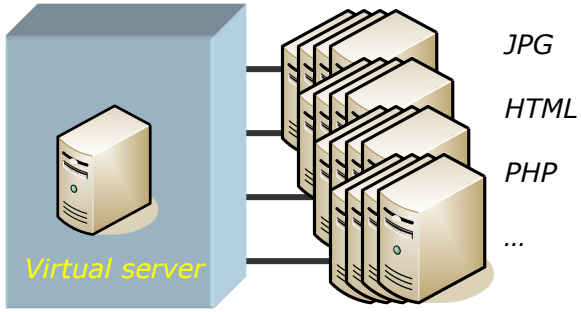
L7 switching

Alcuni switch supportano anche livelli superiori al 3, consentendo di distribuire le richieste ai server in funzione del contenuto indirizzato (politiche URI-based, content based routing)



L7 load balancers

Unendo le due precedenti funzionalità si ottiene una funzionalità dei moderni bilanciatori di traffico (application delivery controllers) come F5 o Foundry Networks



Protocolli

802.3ad: Link Aggregation

E’ un protocollo che permette di associare fra loro più porte dei dispositivi di rete: il traffico di rete viene convogliato su tutte le porte disponibili, realizzando contemporaneamente bilanciamento del carico e ridondanza sul link. Il collegamento tra due switch secondo il protocollo 802.3ad si chiama solitamente “trunk”

Il protocollo 802.3ad si usa anche per collegare in modo ridondante i server agli switch di datacenter, collegamento che in questo caso per il server si chiama “bonding” (o “teaming” o “trunking”). I vantaggi sono gli stessi: ridondanza sul collegamento, bilanciamento del carico e incremento della banda

Protocolli

Link Aggregation bonding policies

Vi sono diverse modalità di funzionamento del bonding:

- round-robin (LB e FT)
- active-backup (FT)
- XOR (LB e FT)
- broadcast (FT)
- 802.3ad (usa il LACP)
- transmit load balancing
- adaptive load balancing

Protocolli

802.1d: Spanning Tree Protocol

I dispositivi layer 2 usano questo protocollo per identificare continuamente la topologia della rete ed evitare che si formino anelli. Bridge e switch usano varie impostazioni (priorità, ecc) per eleggere un “root bridge” e calcolare la propria distanza topologica (in termini di “hop”) da quest’ultimo. L’algoritmo va a convergenza quando i dispositivi riconoscono di non appartenere ad alcun anello; se viene identificato un anello, lo switch topologicamente più “lontano” dal root bridge imposta una porta in BLOCKING

802.1w: Rapid Spanning Tree

Supera alcune limitazioni dello Spanning Tree tradizionale, come il numero massimo di dispositivi in un loop (che non è limitato a 7) e il tempo di convergenza (secondi anziché decine di secondi)

Protocolli

802.1d: PVST

Una importante variante dello Spanning Tree è il Multiple Instance Spanning Tree, o Per VLAN Spanning Tree

I dispositivi fanno cioè girare diverse istanze di STP, una per ogni VLAN. Una sola istanza di STP andrebbe comunque bene se la mappatura delle VLAN coprisse l'intero set di dispositivi; di solito però non è così e gli unici dispositivi che hanno porte in tutte le VLAN sono quelli più centrali

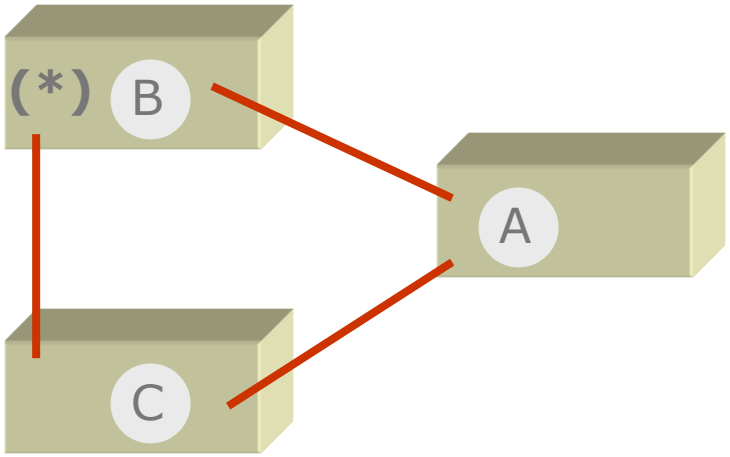
Il PVST fornisce quindi maggior beneficio nei casi di riconfigurazione della rete a seguito di guasti o cambiamenti programmati di configurazione, potendo lavorare non tanto sulla topologia fisica degli switch, ma su quella "logica" costituita dalle VLAN in essi configurate

Protocolli

VRRP

Gli switch dotati di funzionalità di livello 3, così come i router, forniscono un supporto per la ridondanza delle stesse, il VRRP (Virtual Router Redundancy Protocol). E' un protocollo usato da due o più sistemi per mantenere attivo nell'infrastruttura l'indirizzo virtuale usato come router da tutti gli utilizzatori

Consente per esempio di rendere ridondante il default gateway (*) di una rete



I router VRRP si configurano in master (1 solo) e backup (tutti gli altri). Il master può supportare più indirizzi virtuali.

Protocolli

802.1x: Port Authentication

Lo standard 802.1x è stato pensato per consentire il controllo dell'accesso alla rete a livello di porta.

La sicurezza *port-based* prevista da 802.1x permette ai dispositivi di rete di richiedere all'utente un'autenticazione *prima* che questo ottenga accesso alla rete.

Funziona sia con reti *wired* che *wireless*.

Wireless LANs

Dicono che vi siano alcuni vantaggi…:

- Incrementa la mobilità rendendo disponibile la rete dappertutto
- Incrementa la produttività perché le informazioni sono continuamente accessibili
- Elimina le limitazioni e i vincoli imposti dal cablaggio strutturato
- Integra e completa il cablaggio esistente in ambienti "difficili"
- E' di facile e rapida installazione
- Offre supporto a vari OS

Wireless LANs

Ma anche che…:

- Le chiavi WEP a possono essere facilmente compromesse
- L'Initialization Vector è troppo corto e permette il riutilizzo delle chiavi
- Il filtro sui MAC address permette lo spoofing
- Non esiste o è proprietaria la user authentication 802.11x
- Gli Access Point non sono autenticati (rogue APs)
- Alcune caratteristiche di sicurezza sono proprietarie
- Non esiste uno standard per la gestione centralizzata degli AP

Wireless LANs

Gli standard più diffusi sono 802.11a, 802.11b e 802.11g. 802.11n in perenne fase di standardizzazione.

La sicurezza di questi standard consiste nell'autenticazione con MAC address, open (SSID), con uso di un segreto condiviso, o chiavi statiche WEP.

Wireless LANs

Encryption

Wired Equivalent Privacy.

RC4 con chiavi di 40 e 128 bit.

Un Initialization Vector a 24 bit è concatenato alla chiave ad ogni frame ed è trasmesso in chiaro

Wireless LANs

Autenticazione

Open: a ogni stazione che richiede l'autenticazione presentando il corretto SID è consentito l'accesso

Shared-key: l'AP manda al client un challenge che questo deve cifrare con la chiave WEP e restituire all'access point.

Wireless LANs

Rogue Access Points

Sono Access Point fuori controllo e installati in punti della rete cablata accessibili agli utenti.

Prevenzione

- specifica politica di sicurezza
- sicurezza fisica
- infrastruttura wireless supportata
- 802.1X sui dispositivi

Rilevazione

- wireless analyzers/sniffers
- ispezione del traffico sulla rete cablata
- ispezione fisica

Network Access con 802.1x

Tradizionalmente, una rete *wired* consente l'accesso a qualunque dispositivo che possa connettersi al livello fisico, esattamente come avviene in una rete *wireless*.

- Walk-up network ports
- Wireless

Come impedire gli accessi non autorizzati?

Per esempio con 802.1x: per collegarsi a una porta dei dispositivi di rete, o per associarsi all’access point wireless, occorre che l’utente esegua un’autenticazione

Extensible Authentication Protocol

EAP (definito nella RFC 3748 → 5247) è un framework che permette di usare diversi metodi di autenticazione

Non definisce però un protocollo vero e proprio, ma solo i messaggi che devono essere scambiati

Per diventare un protocollo di rete c'è bisogno di incapsulare l'EAP in qualche modo

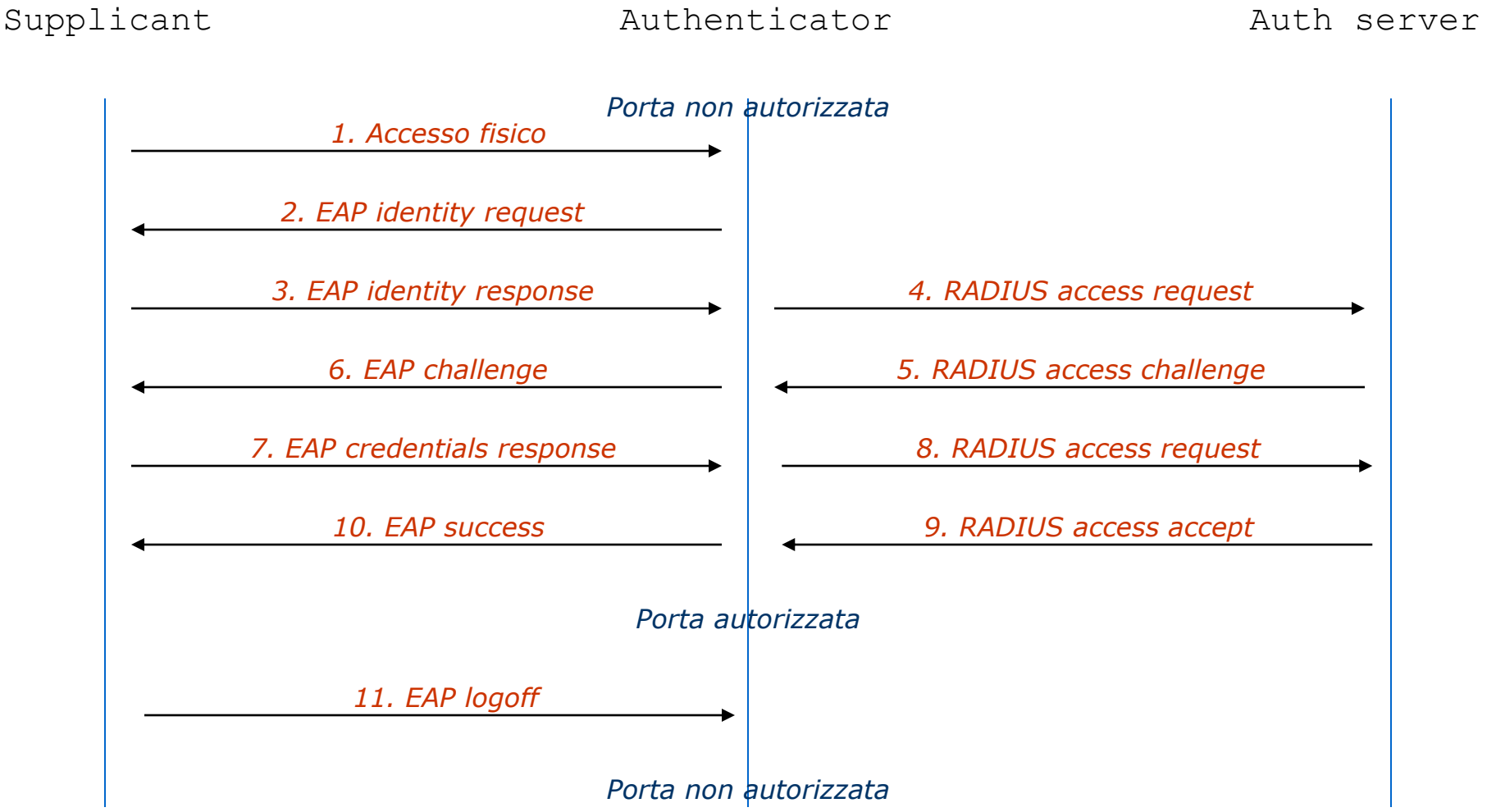
- EAP-MD5
- EAP-TLS
- EAP-TTLS
- EAP-PEAP
- EAP-LEAP
- …

Extensible Authentication Protocol

802.1x utilizza EAP per definire come i vari partecipanti al protocollo devono scambiarsi le informazioni di autenticazione e come questi messaggi devono essere scambiati in rete (EAPoL o EAP Over LAN).

- Clients
- Dispositivi (switches e access points)
- Authentication servers

EAPoL


Supplicant
Authenticator
Auth server
Porta non autorizzata
1. Accesso fisico
2. EAP identity request
3. EAP identity response
4. RADIUS access request
6. EAP challenge
5. RADIUS access challenge
7. EAP credentials response
8. RADIUS access request
10. EAP success
9. RADIUS access accept
Porta autorizzata
11. EAP logoff
Porta non autorizzata

EAP su wireless

- Il Client si associa con l'AP
- L'AP richiede al Client di autenticarsi
- L'utente fornisce le credenziali (user+pass, user+cert, ecc)
- Il Client e l'AuthServer si autenticano reciprocamente
- Viene generata una chiave WEP unica per quel Client (session key)
- Anche l'AP riceve la session key dall'AuthServer
- L'AP manda al Client la sua chiave comune (broadcast key), crittografata con la session key
- Client e AP instaurano la comunicazione usando la session e la broadcast key
- Session e broadcast key sono cambiate di frequente

Authentication Server

L’authentication server può essere un qualunque server RADIUS; questo tipo di server AAA(A) è caratteristico dei Provider e serve per autenticare gli utenti che effettuano un accesso remoto (ad esempio per un collegamento a Internet).

Nelle reti di comune utilizzo applicativo non ci sono server RADIUS, ma si possono realizzare facilmente appoggiando un servizio RADIUS su un ambiente di autenticazione già esistente; in questo modo non si duplica lo spazio degli utenti ma si usano i login di rete già esistenti. Ad esempio, sia Microsoft che Novell forniscono un servizio RADIUS rispettivamente per Active Directory e per NDS

Cosa succede dopo

Dopo l'avvenuta autenticazione la cosa più semplice è abilitare la porta.

In una infrastruttura wireless versatile però è anche possibile associare altre azioni a questa semplice abilitazione. A fronte di un'autenticaizone, gli access point possono associare un TAG al traffico che entra nella rete wired, sia a tutti i pacchetti che selettivamente, a gruppi o anche per ogni utente. Il server RADIUS deve essere opportunamente configurato per mappare utenti e gruppi a specifici attributi definiti in 802.1x

Si possono quindi gestire politiche di QoS specifiche a tutto il traffico wireless fino ad assegnare ciascun utente a specifiche VLAN della rete

Ridondanze

Ridondanze tipiche dei dispositivi di rete

- Alimentazione
- Raffreddamento
- Logica di gestione
- Modularità
- Hot pluggability dei moduli
- Hot upgradeability dei firmware

Ridondanze

Ridondanze nella topologia di rete

Trunk balancing/failover

I collegamenti interswitch possono essere ridondanti e più performanti se realizzati con trunking

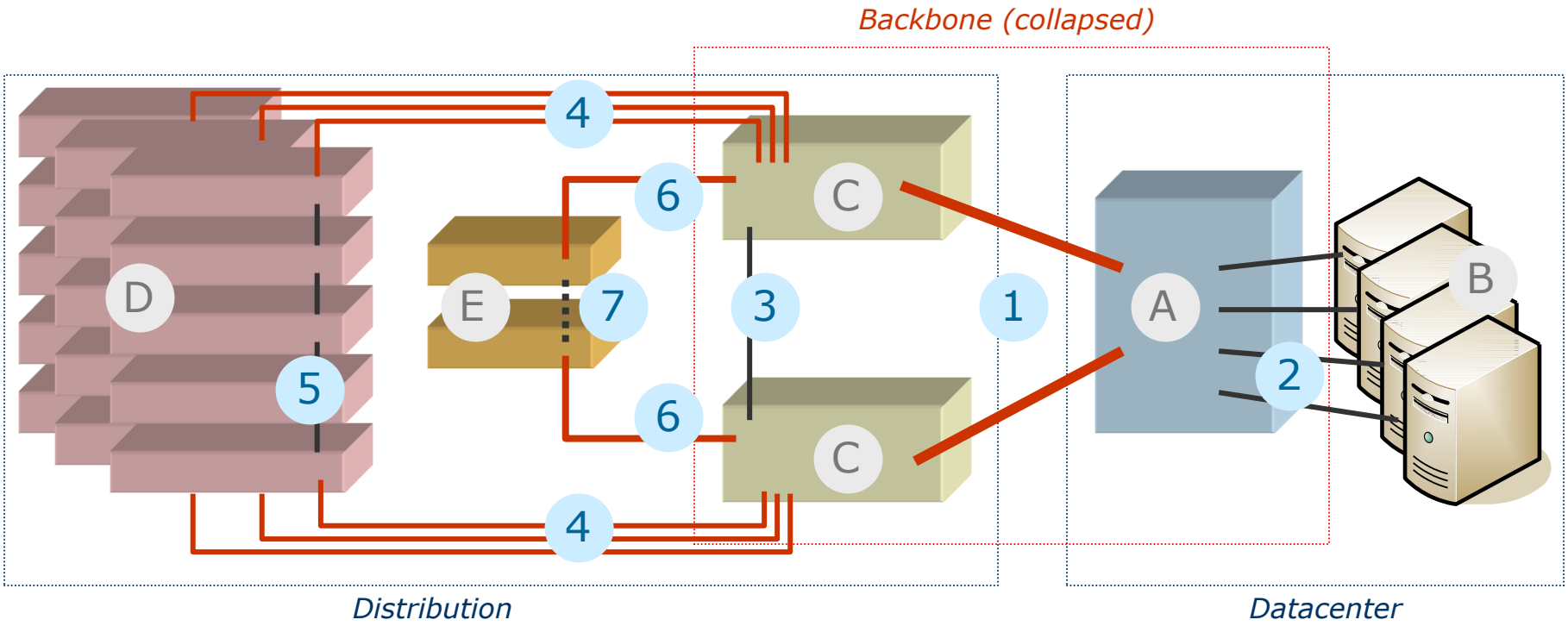
Multiple Distribution-Backbone links (L2)

Per raggiungere la periferia si usano due link che si chiudono ad anello e si lascia che lo Spanning Tree interrompa l'anello al punto periferico più lontano

Multiple Backbone-Datacenter links (L2/L3)

Verso il datacenter può essere adottata la stessa tecnica o più efficacemente si realizzano percorsi multipli e usando il routing

Ridondanze



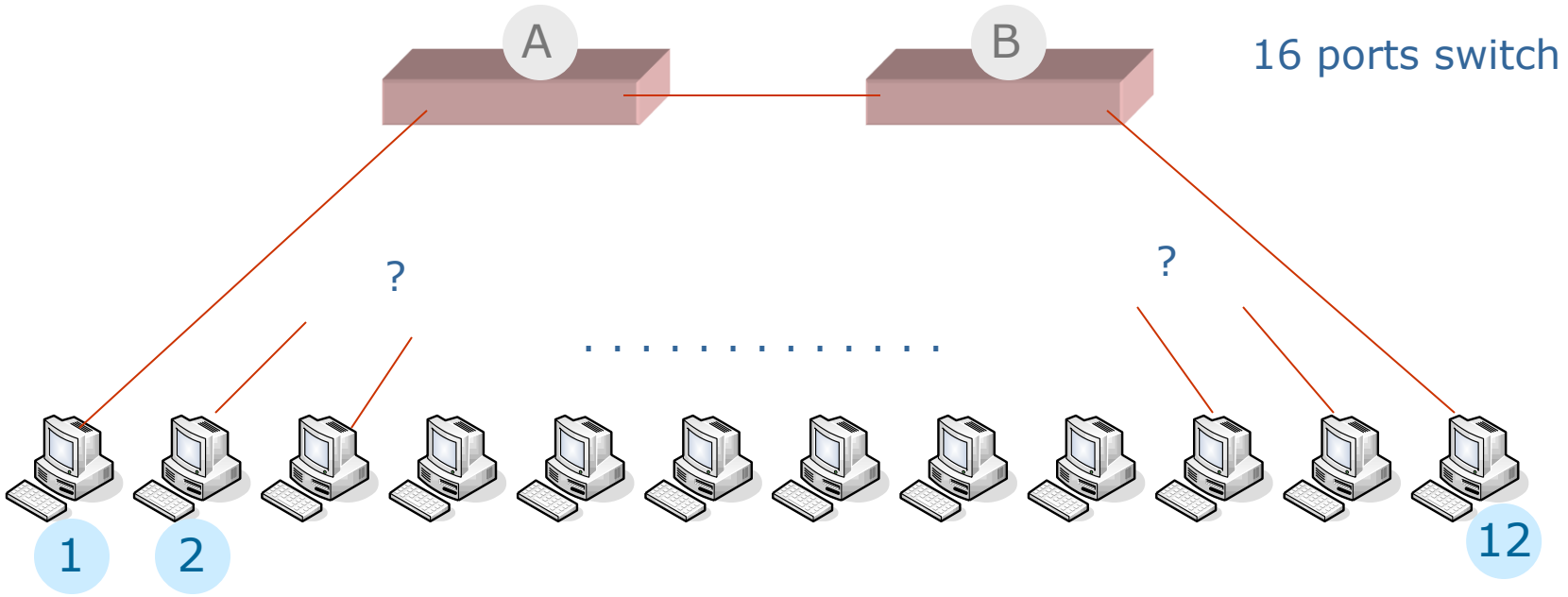
A – Datacenter core switch
B – Server farm
C – Distribution core switch
D – 10/100 distribution stacks
E – GbE distribution stack

1 – 2 x 10GbE trunks (fiber)
2 – 2, 4 GbE bonds (copper)
3 – 2, 4 GbE trunks (copper)
4 – GbE uplinks (fiber)
5 – GbE uplinks (copper)
6 – 2, 4xGbE uplink (fiber)
7 – (opt) 1, 2xGbE uplink (copper)

Ridondanze - esercizio

Problema del supermercato

Come collegare i computer delle casse di un supermercato ai dispositivi attivi in modo "furbo"?



Ridondanze - blade server bonding

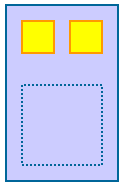
Chassis (fronte)

1	2	3	4
5	6	7	8

(retro)

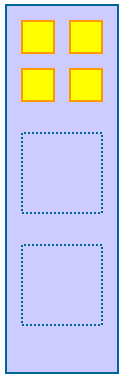
A	1	2	3	4		1	2	3	4	B
	5	6	7	8		5	6	7	8	
C	1	2	3	4		1	2	3	4	D
	5	6	7	8		5	6	7	8	
E	1	2	3	4		1	2	3	4	F
	5	6	7	8		5	6	7	8	

Blade “piccola”



Mezzanine GbE

Blade “grande”

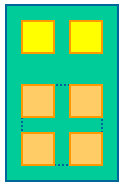


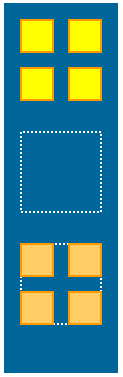
Chassis (fronte)

1	2	3	4
5	6		8

(retro)

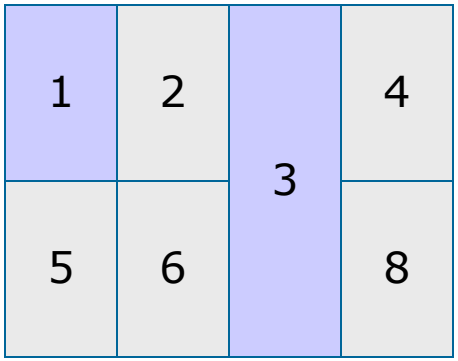
A	1	2	3	4		1	2	3	4	B
	5	6	7	8		5	6	7	8	
C	1	2	3	4		1	2	3	4	D
	5	6	7	8		5	6	7	8	
E	1	2	3	4		1	2	3	4	F
	5	6	7	8		5	6	7	8	



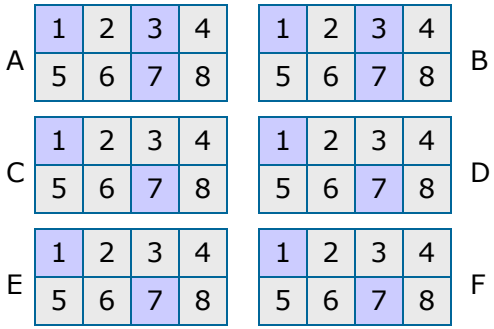


Ridondanze - blade server bonding

Chassis (fronte)



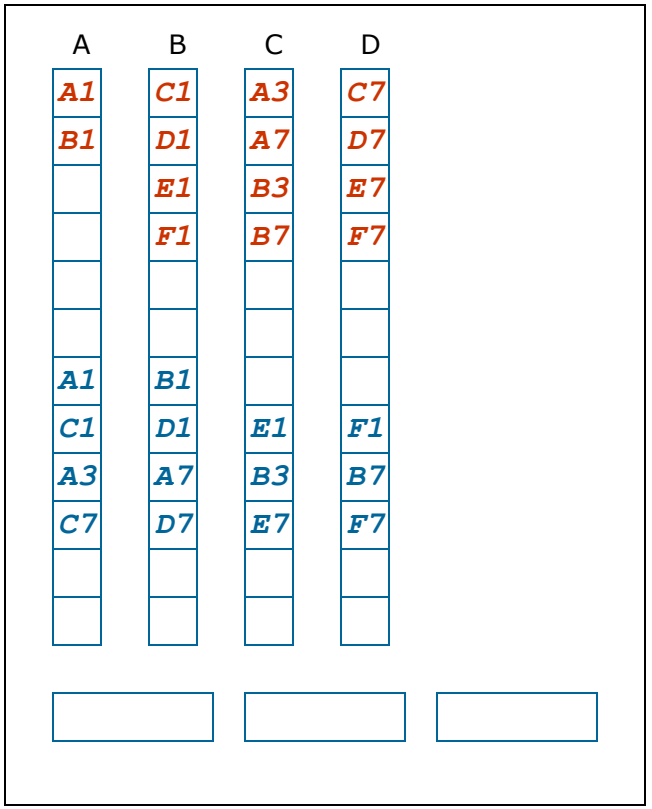
(retro)



NO!

SI'!

Switch modulare



Collegamenti corretti a uno switch modulare

Intrusion Detection & Prevention

Definizione

Con Intrusion Detection si identificano arti e tecniche per scoprire attività anomale, scorrette o non appropriate nei sistemi.

Intrusion Detection Systems

Host-based, Network-based, Stack-based.

Statistical detection, pattern-matching detection.

NIDS

Network-based Intrusion Detection Systems

Catturano il traffico che passa sulla rete.

Filtro di primo livello --> identifica il traffico da analizzare

Secondo livello --> analizzatore di attacchi

Terzo livello --> modulo di intervento

NIDS

Punti di forza:

- Costi modesti
- Analizzatore di pacchetti
- Registrano gli attacchi
- Evidenziano gli attacchi
- Identificazione e risposta real-time
- Usi complementari e verifiche di policy
- Indipendenza da OS

HIDS

Host-based Intrusion Detection Systems

Fanno un auditing sistematico dei log di sistema.

Real-time vs scheduled auditing

Tracciano I/O, Process, Port e Network activity

Modulo di analisi, modulo di intervento

Integrity checkers

Un tipo di host-based IDS è l'*integrity checker*.

tripwire

Falsi positivi

SIDS

Un ibrido dei precedenti due sistemi è costituito dagli

Stack-based Intrusion Detection Systems

Analizzano il traffico di rete pertinente a un singolo sistema

Vi è un solo modulo di filtro+analisi realizzato come estensione dello stack TCP/IP (si aggancia agli *hook* dello stack)

Inbound, outbound & local activity

E' piuttosto leggero, ma occorre una console centralizzata per la gestione di sistemi multipli

{H,S}IDS

Punti di forza:

- Verifica degli attacchi
- Verifica di attività specifiche del sistema
- Reti *switched*
- Crittografia
- Monitoraggio di componenti chiave
- Identificazione e risposta in near real-time o real-time
- Nessun hardware aggiuntivo

Configurazioni miste

Una soluzione particolarmente efficace consiste nell'adottare una miscela delle tipologie di IDS descritte, che consentirebbe di identificare attacchi complessi correlando nel tempo eventi separati. Esempi:

- Telnet (N), su root (H), kill syslog (H)
- Port scan (N), cgi-bin attack (N), HTML defacement (H)
- port scan (N), sendmail attack (N), rootkiit install & exec (H)

Network media

Nelle reti switched occorrono soluzioni per installare i NIDS

Per esempio si può inserire un HUB tra il sistema da analizzare e lo switch. All'hub si collega il NIDS.

Pros:

- Semplice ed economico

Cons:

- Interferisce troppo con il sistema analizzato: il management dell'IDS genera collisioni sull'HUB
- Gli HUB sono a basso costo → failures
- Poco o non applicabile per sistemi multipli, su GbE o dove il traffico complessivo è elevato

Network media

SWITCH: si usa un TAP a cui si collega il NIDS

Pros:

- Fault tolerant
- Nessun impatto sul traffico
- Disaccoppia la rete dal NIDS
- Nessun degrado di prestazioni

Cons:

- Costoso
- Non si può collegare dappertutto e l'applicabilità dipende sostanzialmente dalla topologia dei collegamenti

Network media

SWITCH: si usa la SPAN, una porta a cui viene rediretto il traffico dello switch e a cui si collega il NIDS

Pros:

- Nessuna modifica fisica alla rete

Cons:

- Una sola SPAN per ogni switch, di solito
- Monitorando le (molte) altre porte la SPAN (e il NIDS) si sovraccarica
- Sovraccarico dello switch

Configurazione *stealth* a due porte: il NIDS ha una porta di cattura senza protocolli bound e un'altra di gestione

SNORT

E' un NIDS "leggero" capace di effettuare analisi e logging del traffico IP in tempo reale.

Ha tre modi: sniffer, logger o NIDS.

L'analisi si basa sulla tecnica del *pattern matching*. Quando analizza un pacchetto contenente certi *pattern* specificati nelle sue regole esegue l'azione ad essi associata (logging, alert…).

http://www.snort.org

Intrusion Prevention

Nel tempo gli IDS si sono rivelati poco utilizzabili.

- NIDS sono come guardiani all'ingresso di una Banca, cui è consegnato un pacco di fotografie di delinquenti: quando ne vedono uno suonano l'allarme

- HIDS sono come guardiani all'interno della cassaforte della Banca, che controllano che il contenuto sia ancora lì

Il danno non si può evitare, finché non si dotano i guardiani di armi per impedire l'intrusione.

Intrusion Prevention

Gli IDS sono poco efficaci anche per motivi legati alla complessità dei fenomeni controllati.

- Le regole di *matching* cambiano continuamente
- Per funzionare in modo utile, il riconoscitore ha bisogno di *statefulness*
- Servono tecniche di riconoscimento di anomalie a livello di protocolli continuamente aggiornate
- Servono tecniche di riconoscimento di anomalie su base statistica continuamente aggiornate
- Impegnano il team a essere "pronto all'azione"

Intrusion Prevention

Gli IDS sono nati senza pensare alla prevenzione dell'intrusione, ma solamente all'identificazione, essenzialmente perché limitazioni hw e sw imponevano scelte di compromesso.

- Iniziano gli HIDS
- I NIDS nascono come IDS "estratti" dagli host
- Manca la potenza elaborativa necessaria

La possibilità di prevenzione era negata dalla posizione nella rete.

Intrusion Prevention

La tendenza dei NIPS è stata:

- sfruttare la crescente potenza elaborativa dei processori dedicati e degli ASIC ecc
- mettere la logica di *detection* negli switch di rete
- associare ad essa una (buona) logica di *prevention* (analisi + intervento)

Quando un pacchetto entra nel sistema si prende una decisione "*go/no-go*", nel caso più semplice, oppure si possono realizzare soluzioni più sofisticate implementando servizi di alto livello (content filtering, web o email)

Intrusion Prevention

La tendenza dei HIPS è stata:

- sfruttare la crescente potenza elaborativa dei processori dei computer
- agganciarsi a ogni *hook* che il sistema operativo (kernel, stack, ecc) fornisce
- associare logiche di *prevention* (analisi + intervento) appropriate, modulari, aggiornabili e monitorabili

Per gestire una molteplicità di sistemi con queste caratteristiche occorre un sistema centrale di gestione

Esempi tipici: antivirus e anti-malware in genere

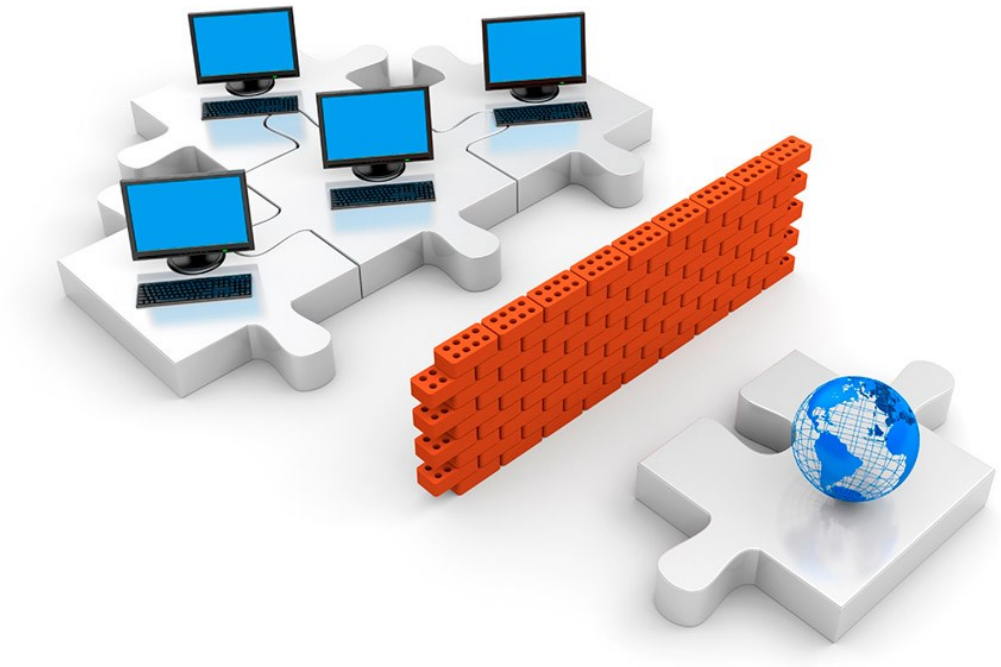
LIDS

E' un HI**P**S per Linux: http://www.lids.org

Oltre alla identificazione delle intrusioni e alla loro notifica, protegge anche il sistema modificando le chiamate del kernel che sovrintendono le operazioni di I/O su directory, files e dispositivi fisici e che controllano i processi e applicandovi politiche di Mandatory Access Control. Include:

- un port scan detector
- protezione dei file
- protezione dei processi
- Access Control Lists

Domande?



Vincenzo Calabrò
info@vincenzocalabro.it