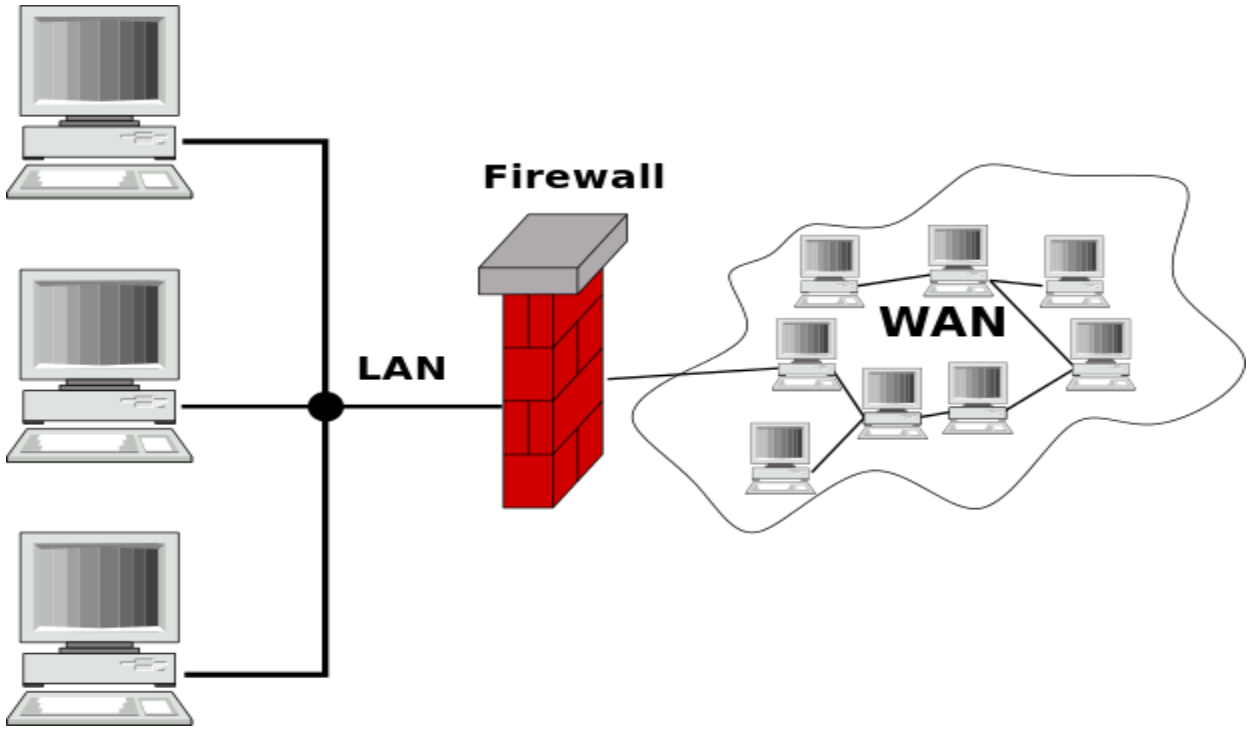
Architetture e strumenti per la sicurezza informatica

Firewall – tipi, architetture, nuove topografie
… e non solo – strategie di inserzione

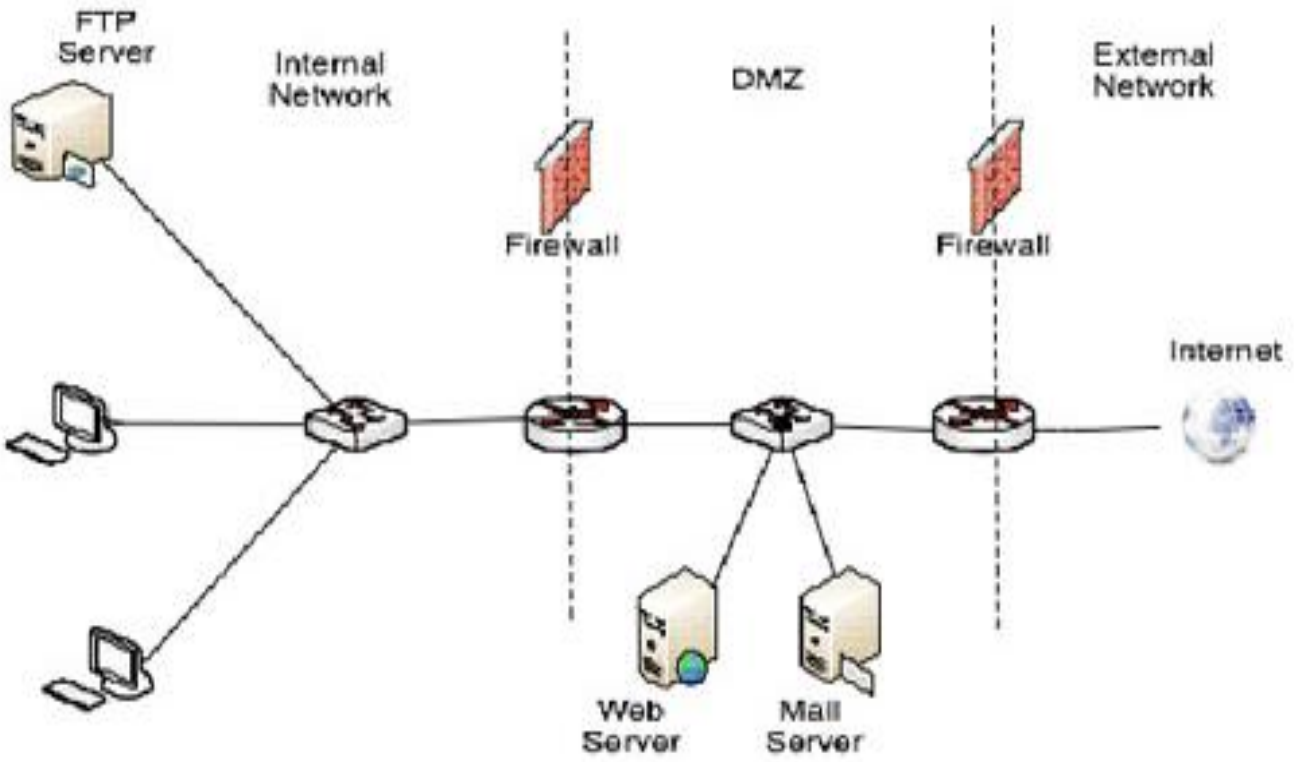
Firewall



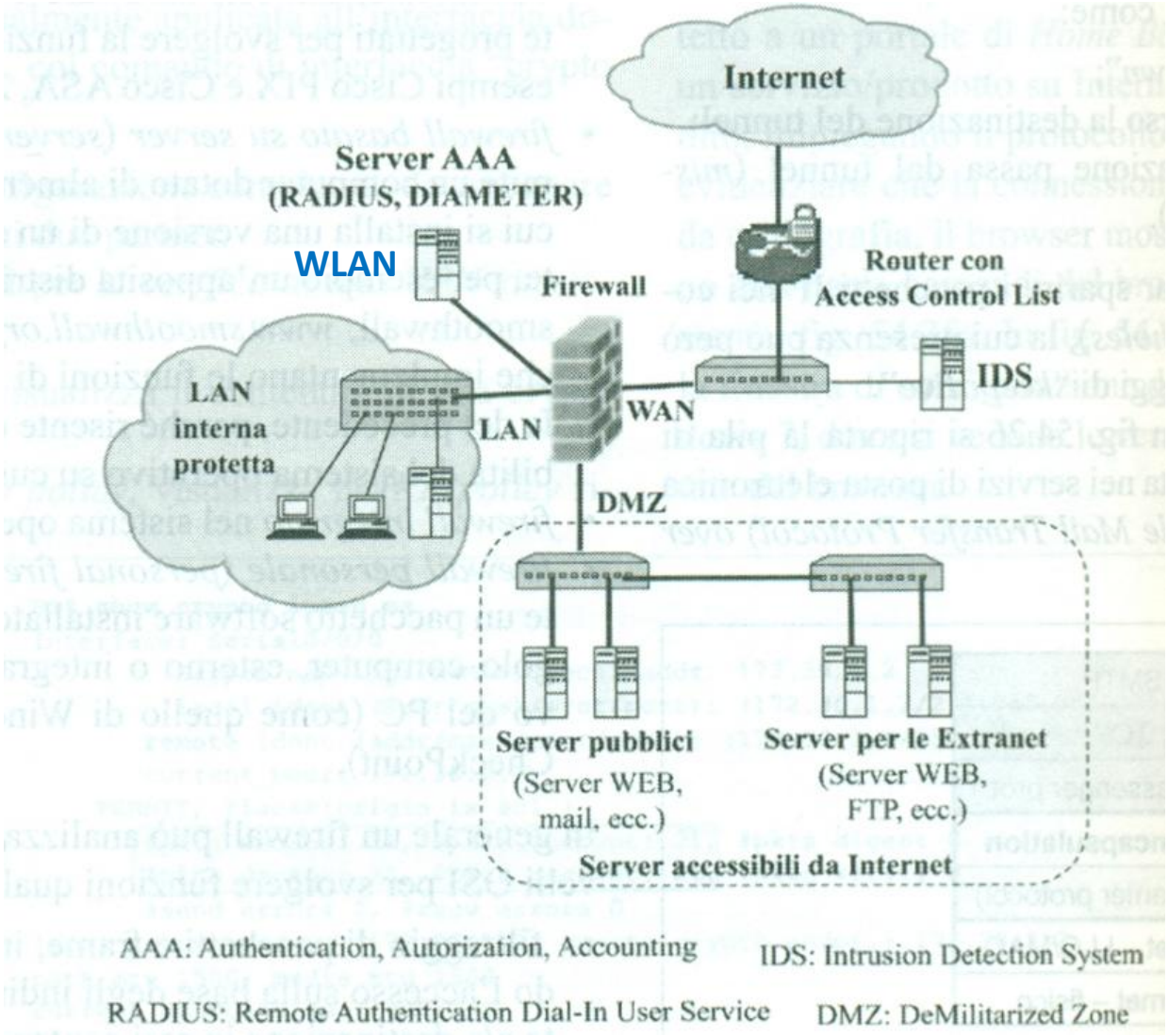
Cos’è il Firewall?

- Dispositivo hardware, software o ibrido
- Canale di controllo e monitoraggio
- Impone restrizioni sui servizi della rete
  - È permesso solo il traffico autorizzato
- Verifica e controlla gli accessi
  - Può implementare allarmi per comportamenti sospetti
- Immune alle penetrazioni
- Fornisce una difesa perimetrale

Firewall: difesa perimetrale



Firewall: fino a 4 tipi di porte

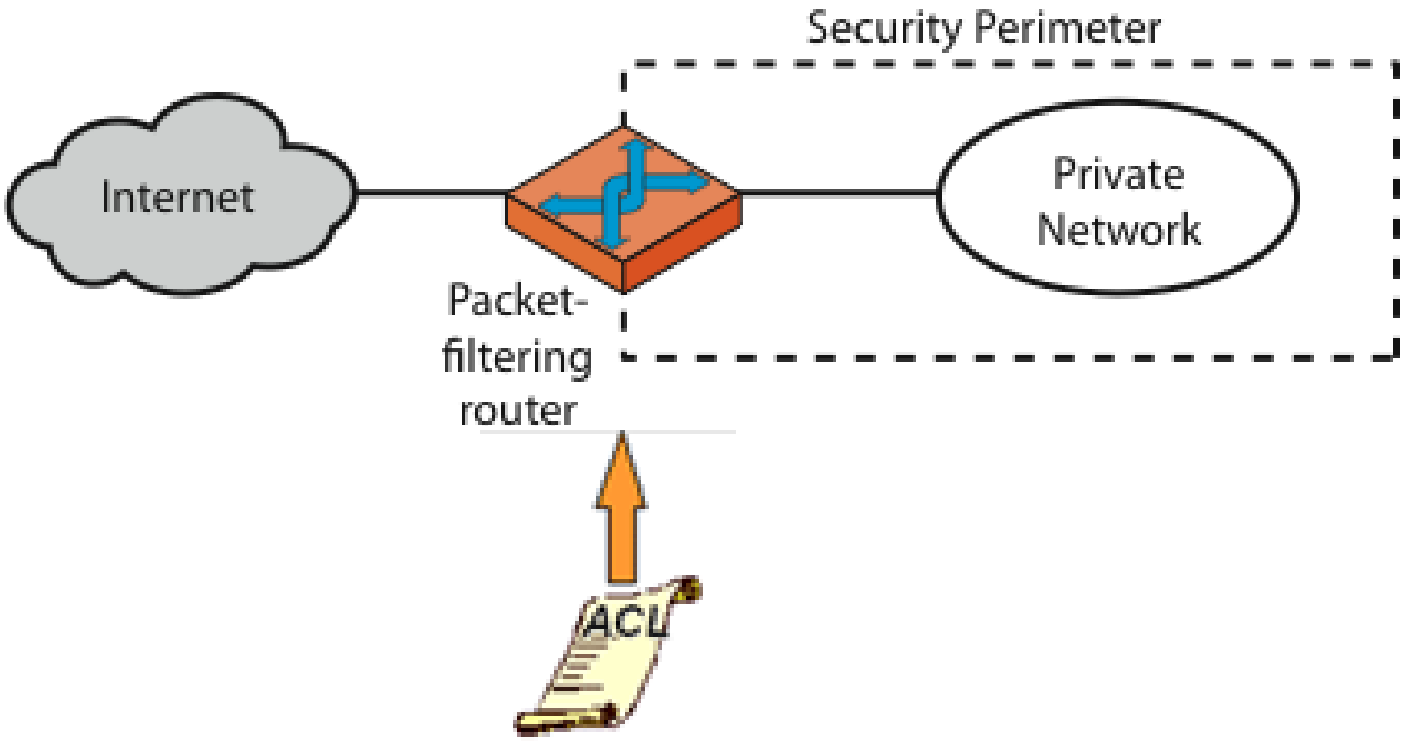


Classificazione dei Firewall

Tipologie:

- Stateless firewall o packet filter firewall
- Stateful firewall o circuit-level gateway
- Application firewall o proxy firewall o application gateway

Firewall – Packet filter



Access Control List: lista ordinata di regole (access control entry) associata alle risorse di un sistema informatico che stabilisce quali utenti o processi possono accedervi e compiere operazioni specificate

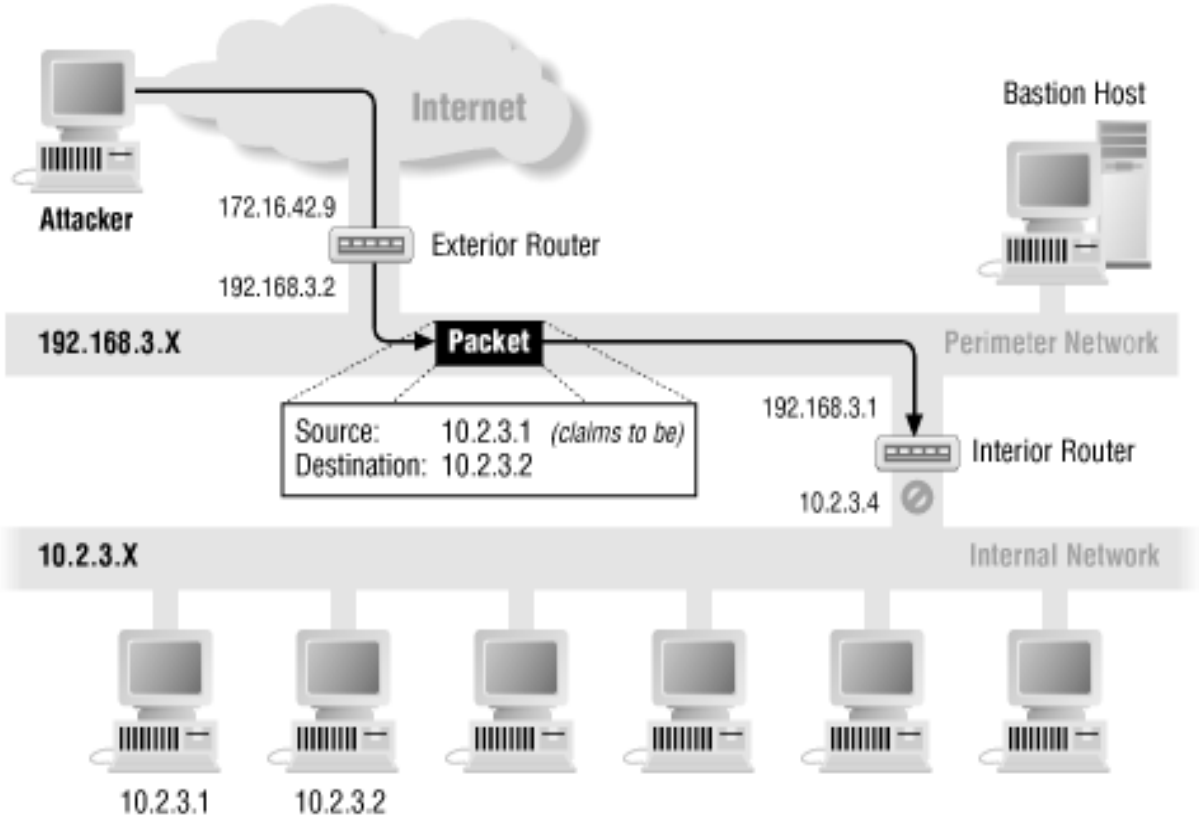
Firewall – Packet filter

- Filtraggio **semplice e leggero**, ma non garantisce un'elevata sicurezza.
- Analizza ogni pacchetto che lo attraversa singolarmente, **senza tenere conto dei pacchetti che lo hanno preceduto.**
- Vengono considerate solo **alcune informazioni** contenute **nell'header del pacchetto**.

Firewall – Packet filter

- Il filtraggio, basato solo sulle informazioni dei primi livelli del modello OSI, non permette al firewall di rilevare gli attacchi su livelli superiori.

- Vulnerabile ad attacchi quali IP spoofing (***Contraffazione dell'indirizzo sorgente)***

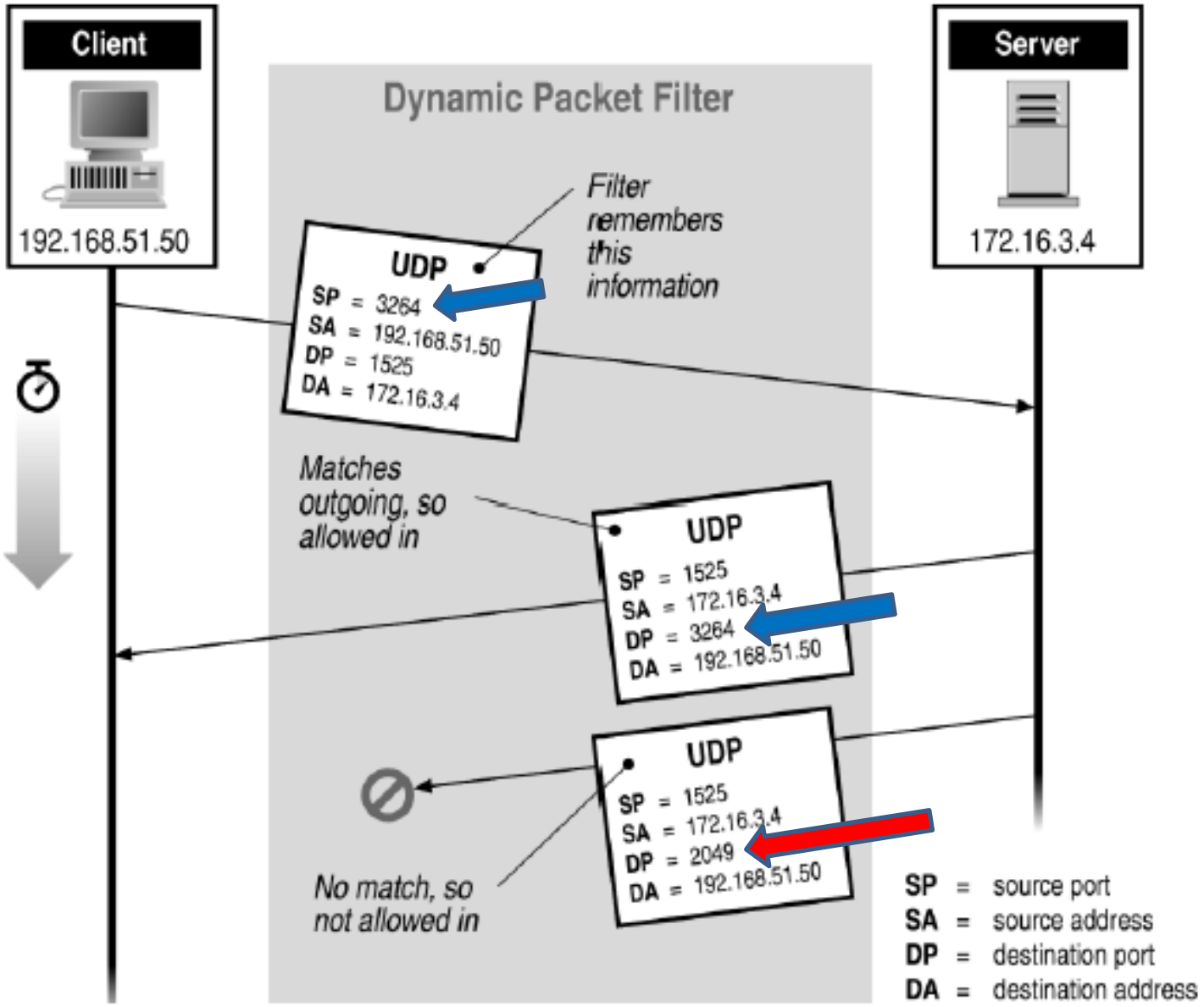


Classificazione dei Firewall

Tipologie:

- Stateless firewall o packet filter firewall
- Stateful firewall o circuit-level gateway
- Application firewall o proxy firewall o application gateway

Stateful Filtering



Firewall – Stateful

- Svolge lo stesso tipo di filtraggio dei packet filter firewall e in più **tiene traccia delle connessioni e del loro stato.**
- Blocca tutti i pacchetti che non appartengono ad una **connessione attiva**, a meno che non ne creino una nuova.
- Previene gli attacchi di tipo ***IP spoofing***, ma comporta una maggiore difficoltà nella formulazione delle regole.

Firewall – Stateful

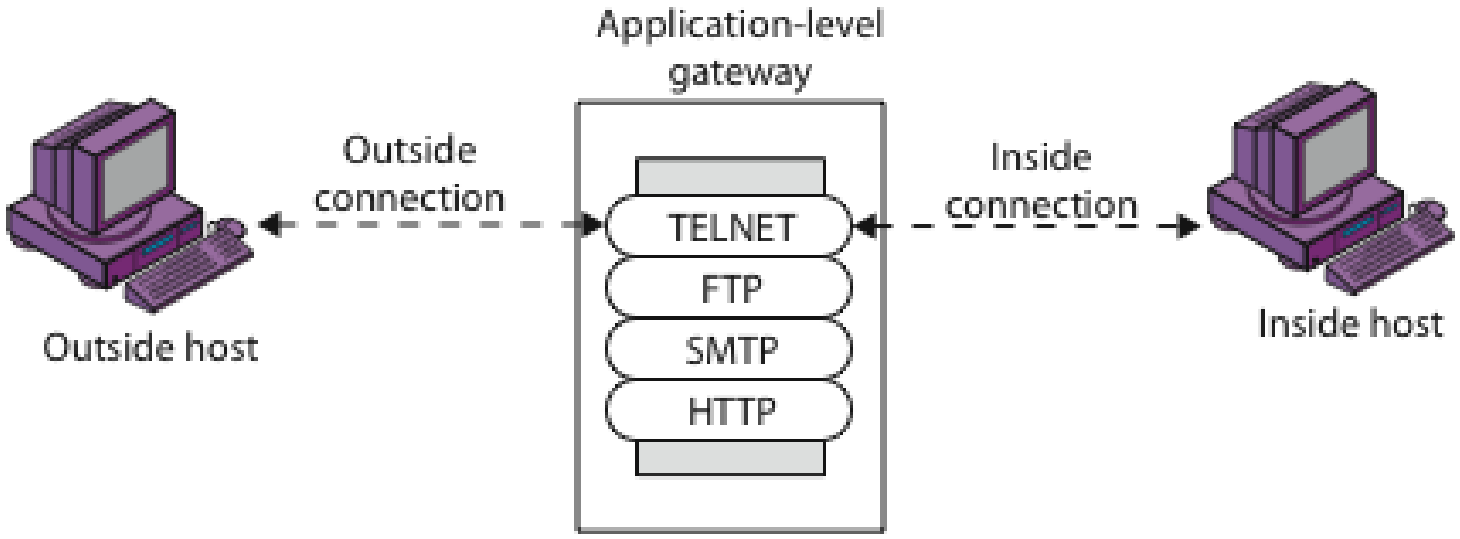
- Non rileva gli attacchi nei livelli OSI superiori al **quarto** ed è sensibile agli attacchi **DoS** che ne saturano la tabella dello stato.
- Rispetto ai packet filter firewall, offre una **maggiore sicurezza** e un controllo migliore sui protocolli applicativi che scelgono casualmente la porta di comunicazione, ma è **più pesante** dal punto di vista delle performance.

Classificazione dei Firewall

Tipologie:

- Stateless firewall o packet filter firewall
- Stateful firewall o circuit-level gateway
- Application firewall o proxy firewall o application gateway

Firewall - Application Level Gateway (o Proxy)



Application-Level Filtering

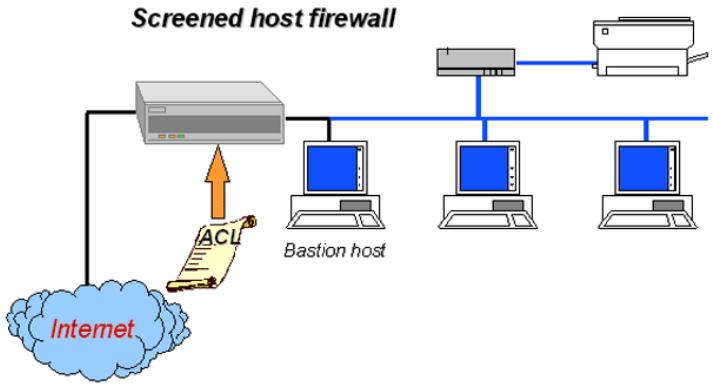
- Opera fino al **livello 7** del modello OSI filtrando tutto il traffico di una singola applicazione sulla base della conoscenza del suo protocollo.
- Analizza i pacchetti nella sua interezza considerando anche il loro contenuto (**payload**) ed è quindi in grado di distinguere il traffico di un'applicazione indipendentemente dalla porta di comunicazione che questa utilizza.

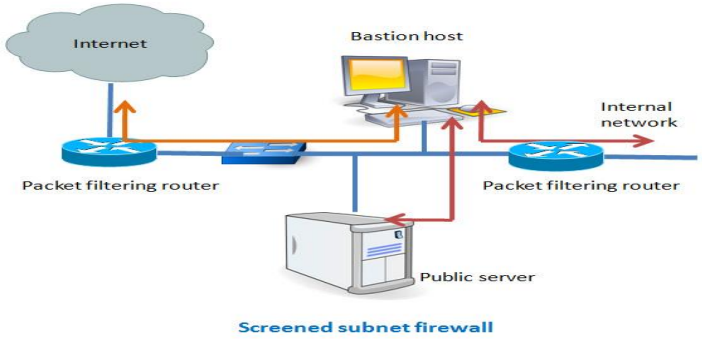
Application-Level Filtering

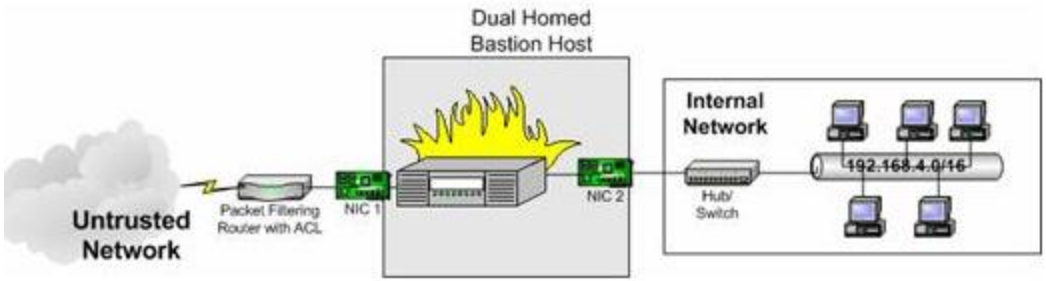
- **Capacità di spezzare la connessione** tra un host della rete che protegge e un host della rete esterna.
- **Intermediario**: è l'unico punto della rete che comunica con l'esterno, nascondendo così gli altri host che vi appartengono.

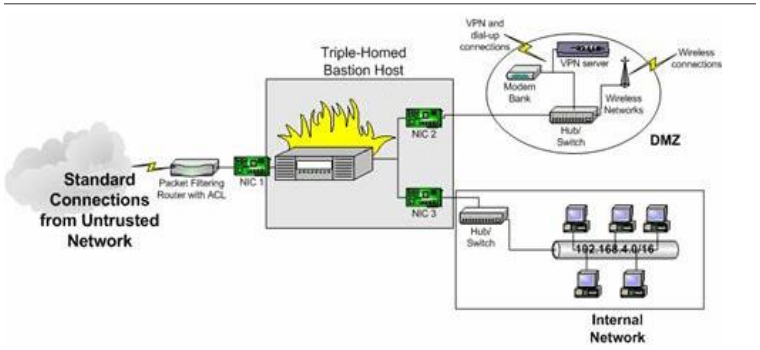
Architetture

- Screened Host (***host di schermatura***)
- Screened Subnet (***subnet di schermatura***)
- Dual Homed Host (*due schede di rete*)
- Multi Homed Host (*più schede di rete*)

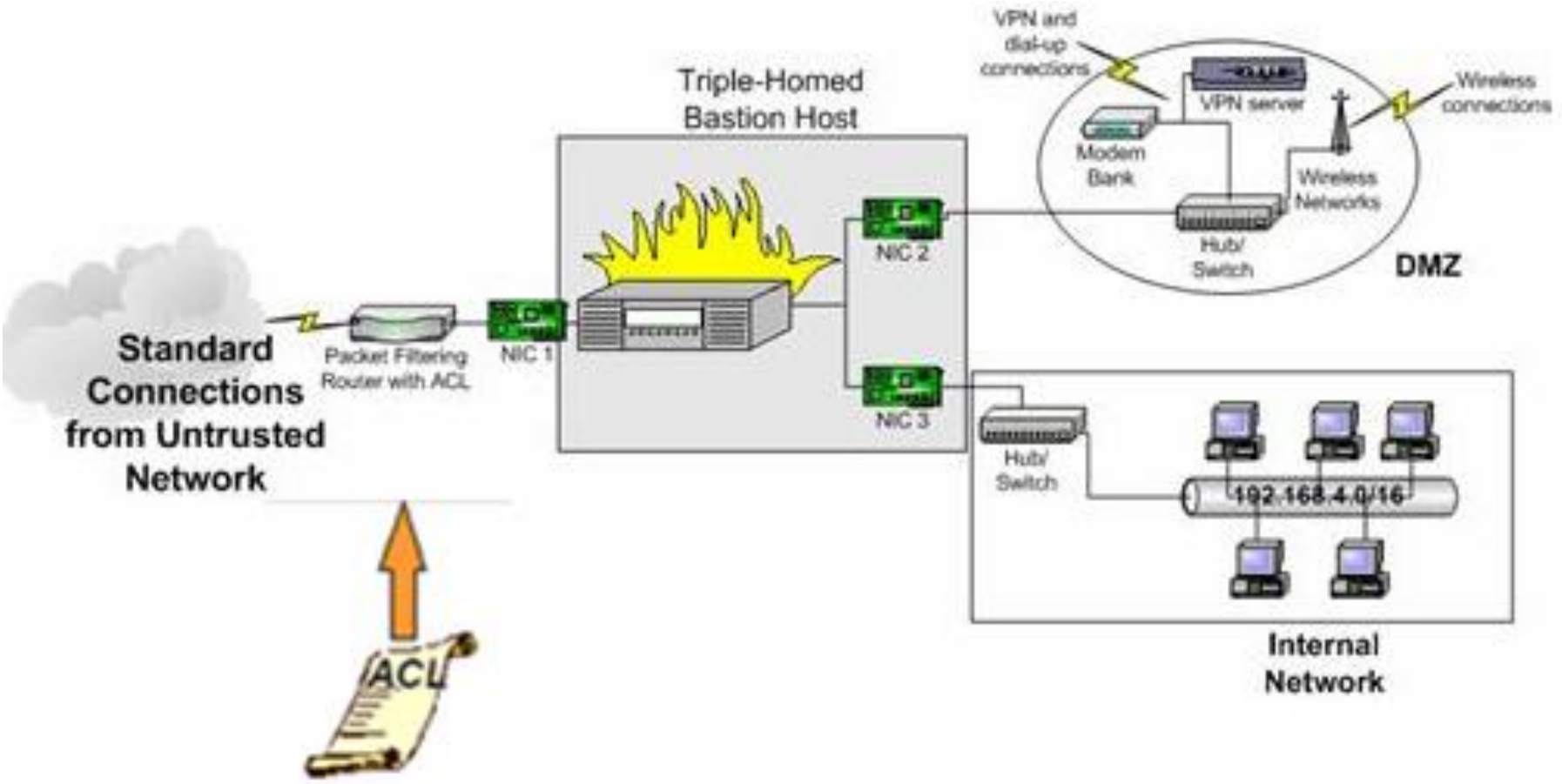




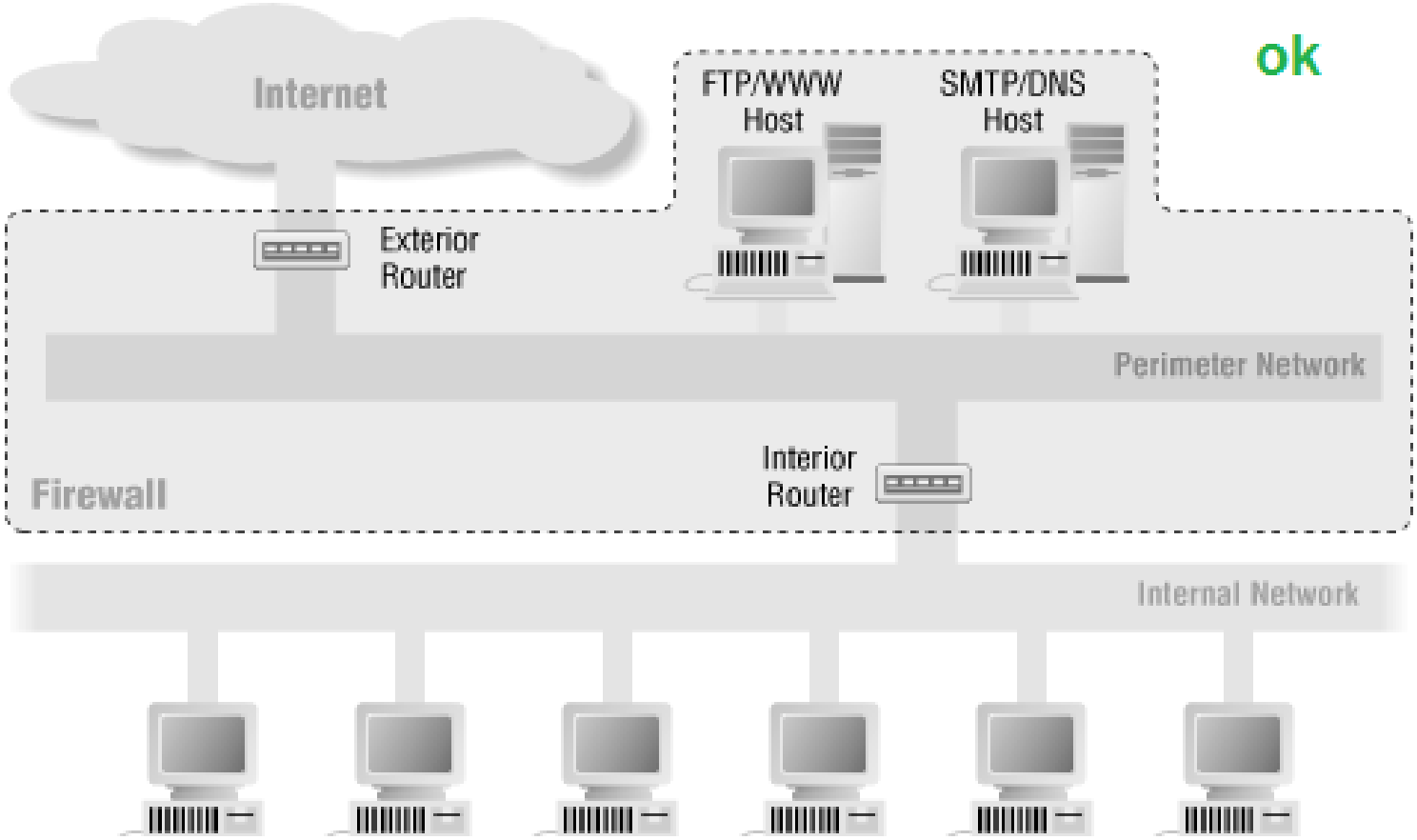




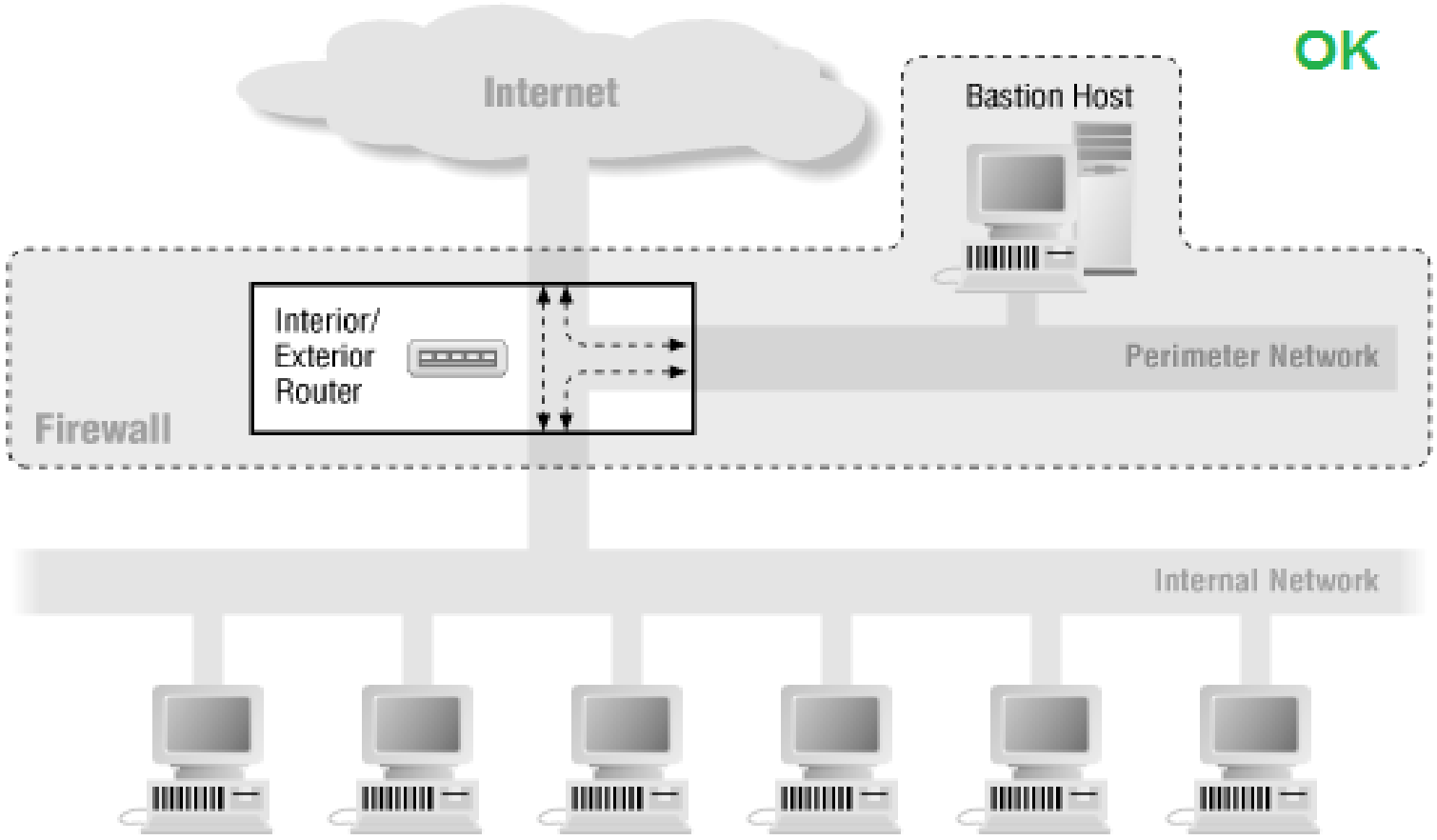
Multi-homed


VPN and dial-up connections
Triple-Homed Bastion Host
VPN server
Wireless connections
Modem Bank
Wireless Networks
Hub/ Switch
DMZ
NIC 2
NIC 1
Standard Connections from Untrusted Network
Packet Filtering Router with ACL
NIC 3
Hub/ Switch
192.168.4.0/16
Internal Network
ACL

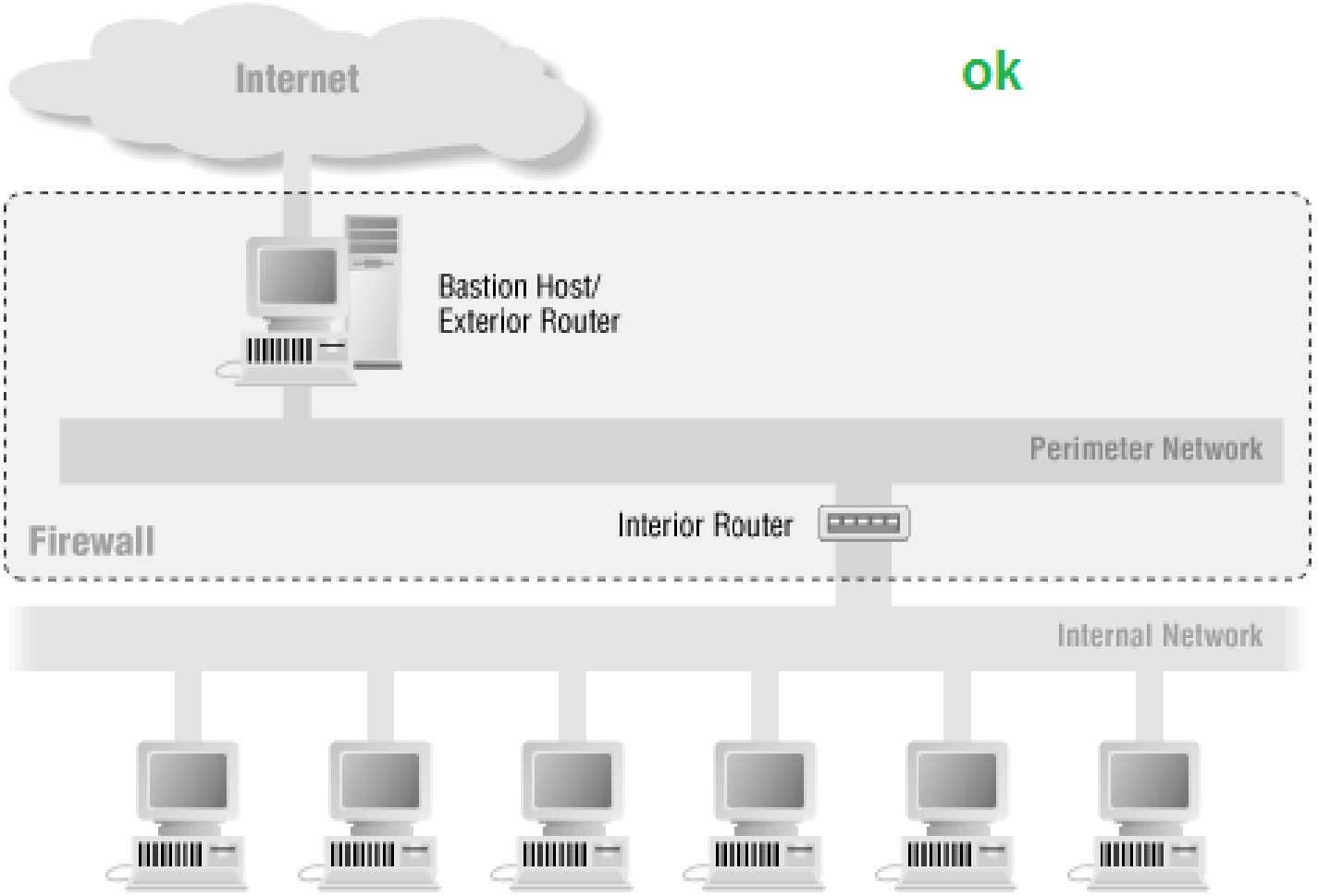
Multi Bastion Host



Merge the Interior Router and the Exterior Router

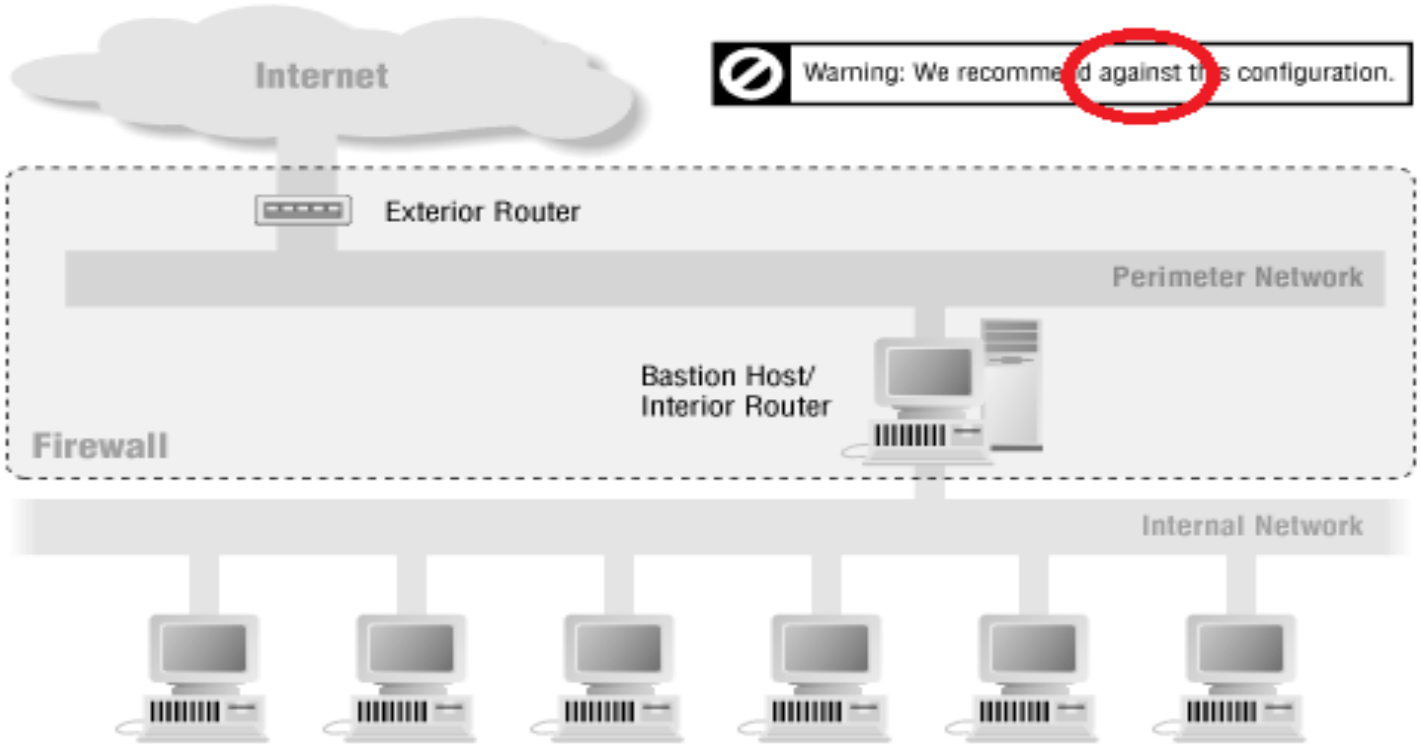


Merge the Bastion Host and the Exterior Router



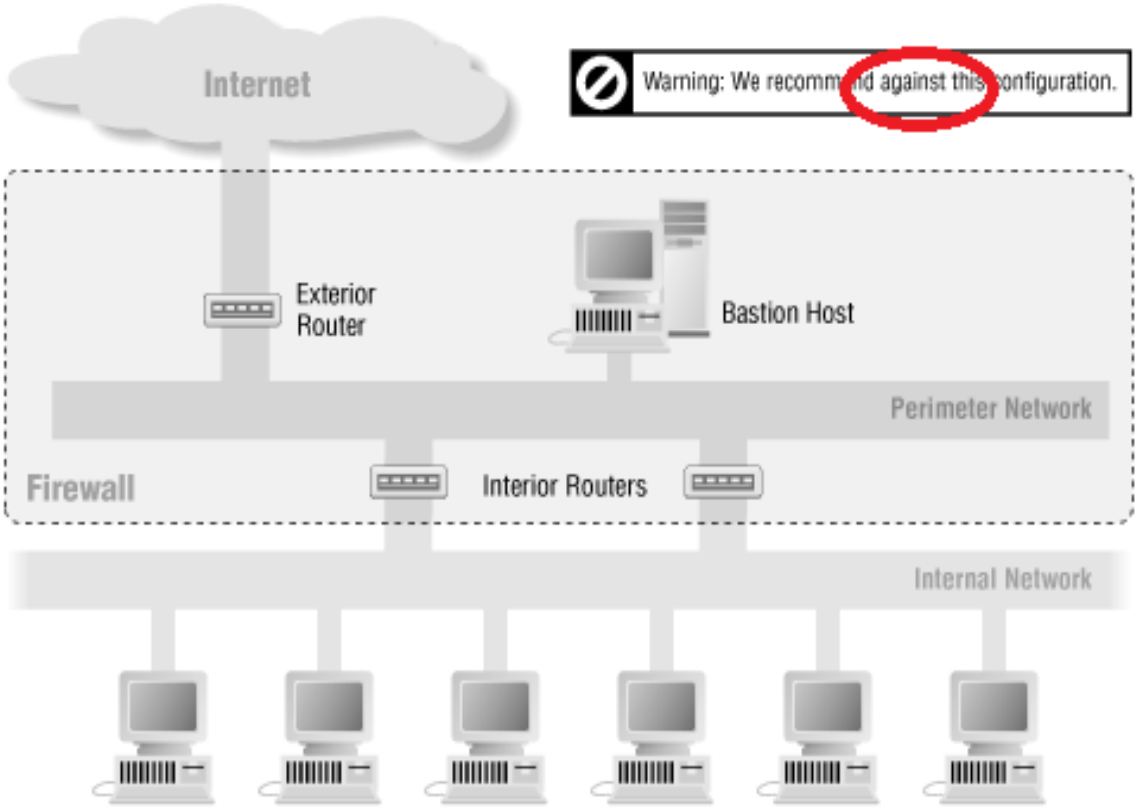
Architetture pericolose

- **Dangerous**
  to Merge the Bastion Host and the Interior Router



Architetture pericolose

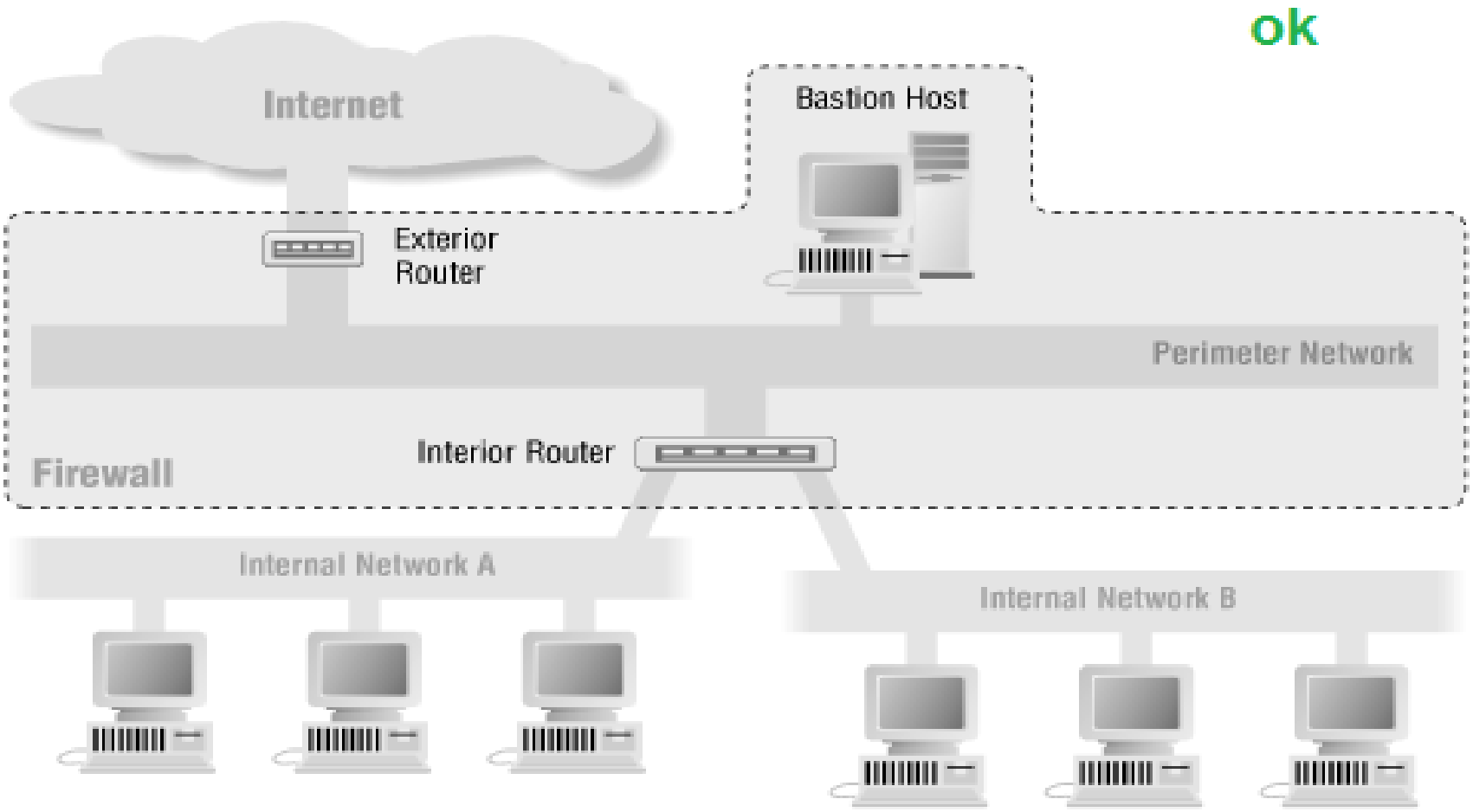
- **Dangerous to Use Multiple Interior Routers**



- **Dangerous**

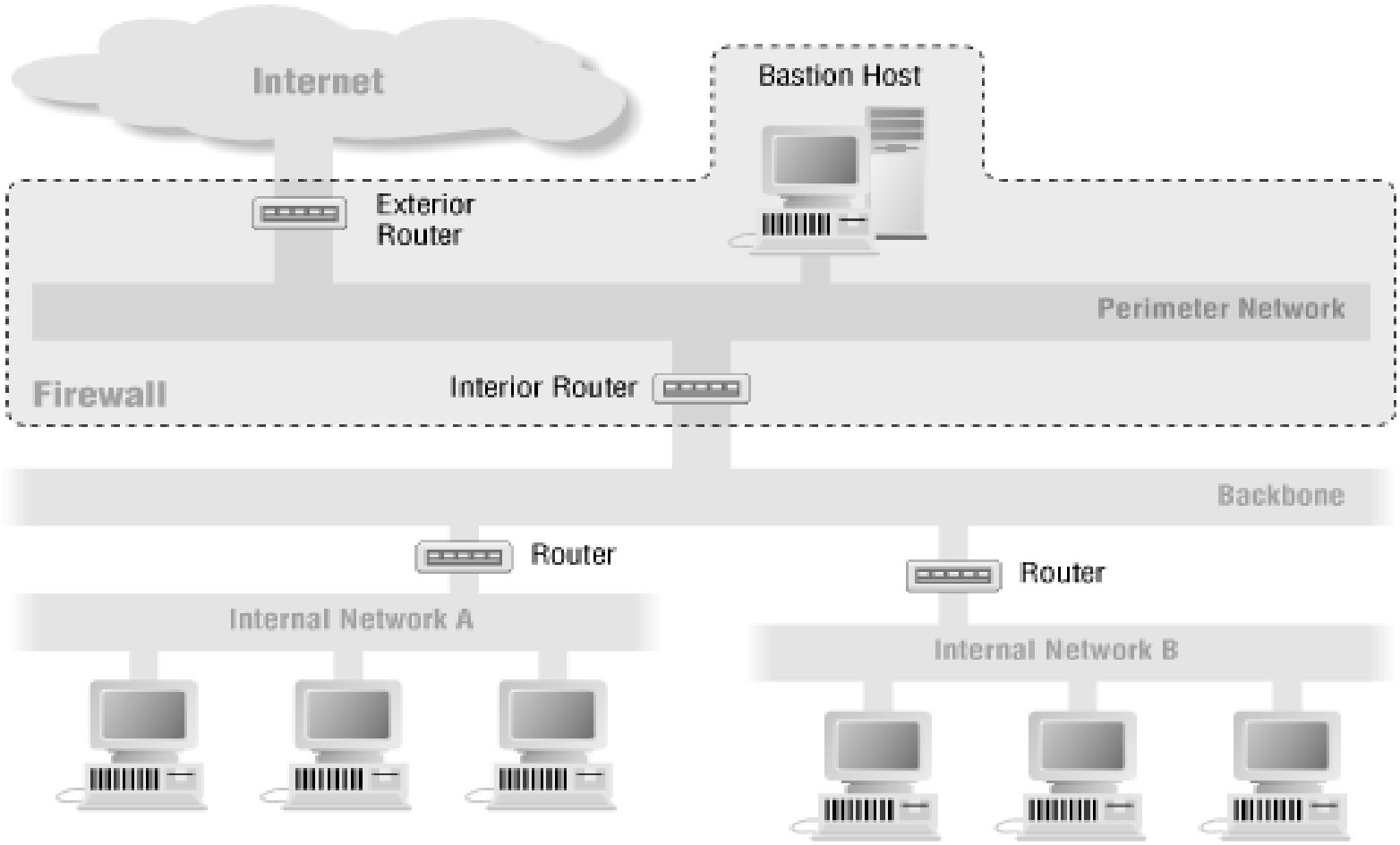
to Use Both Screened Subnets and Screened Hosts

.. se necessario



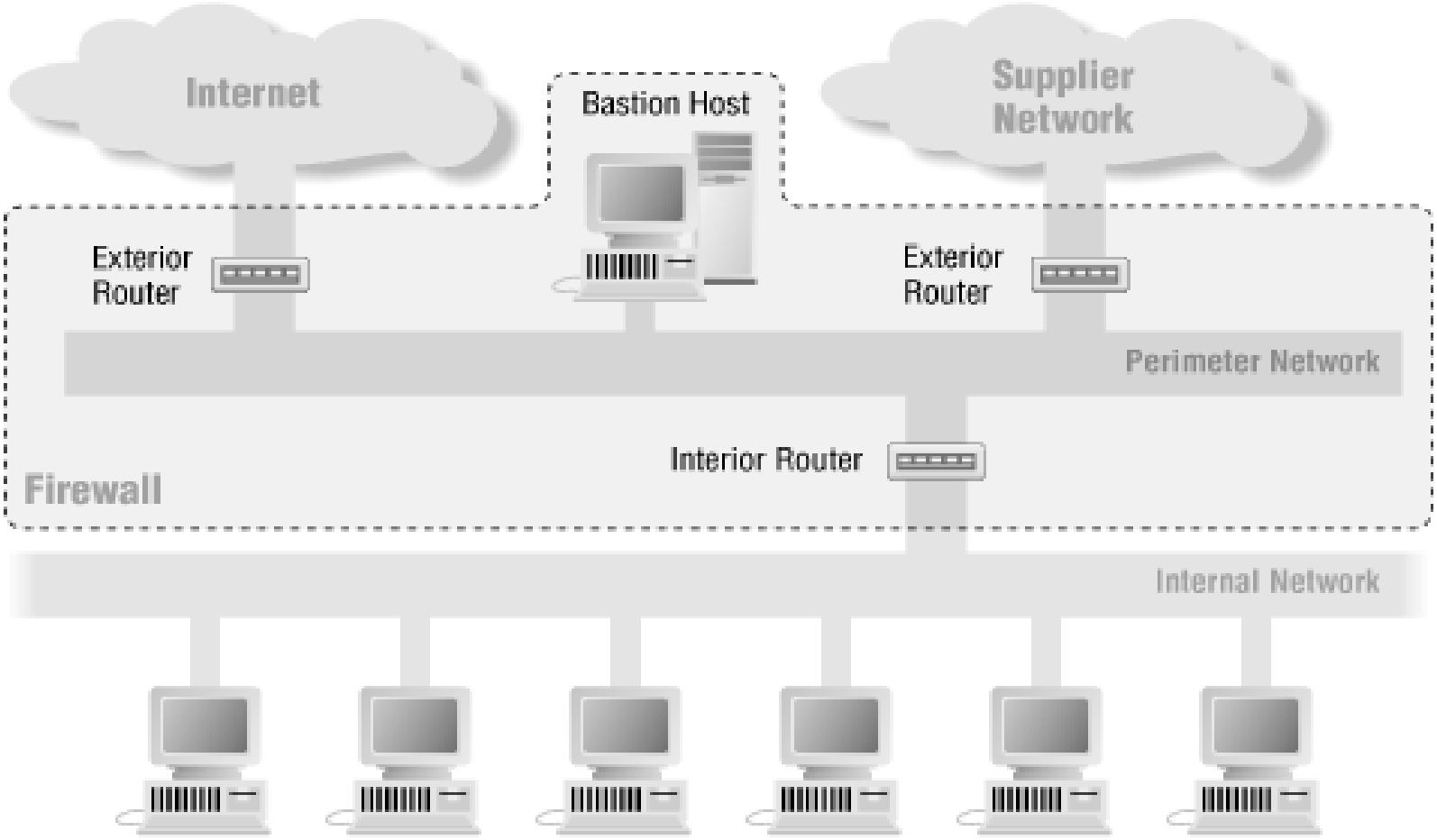
Multiple internal networks (separate interfaces in a single router)

.. se necessario



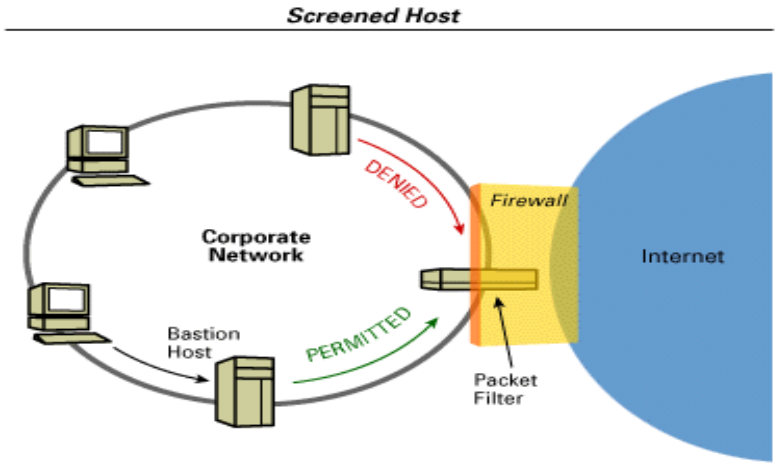
Multiple internal networks (backbone architecture)

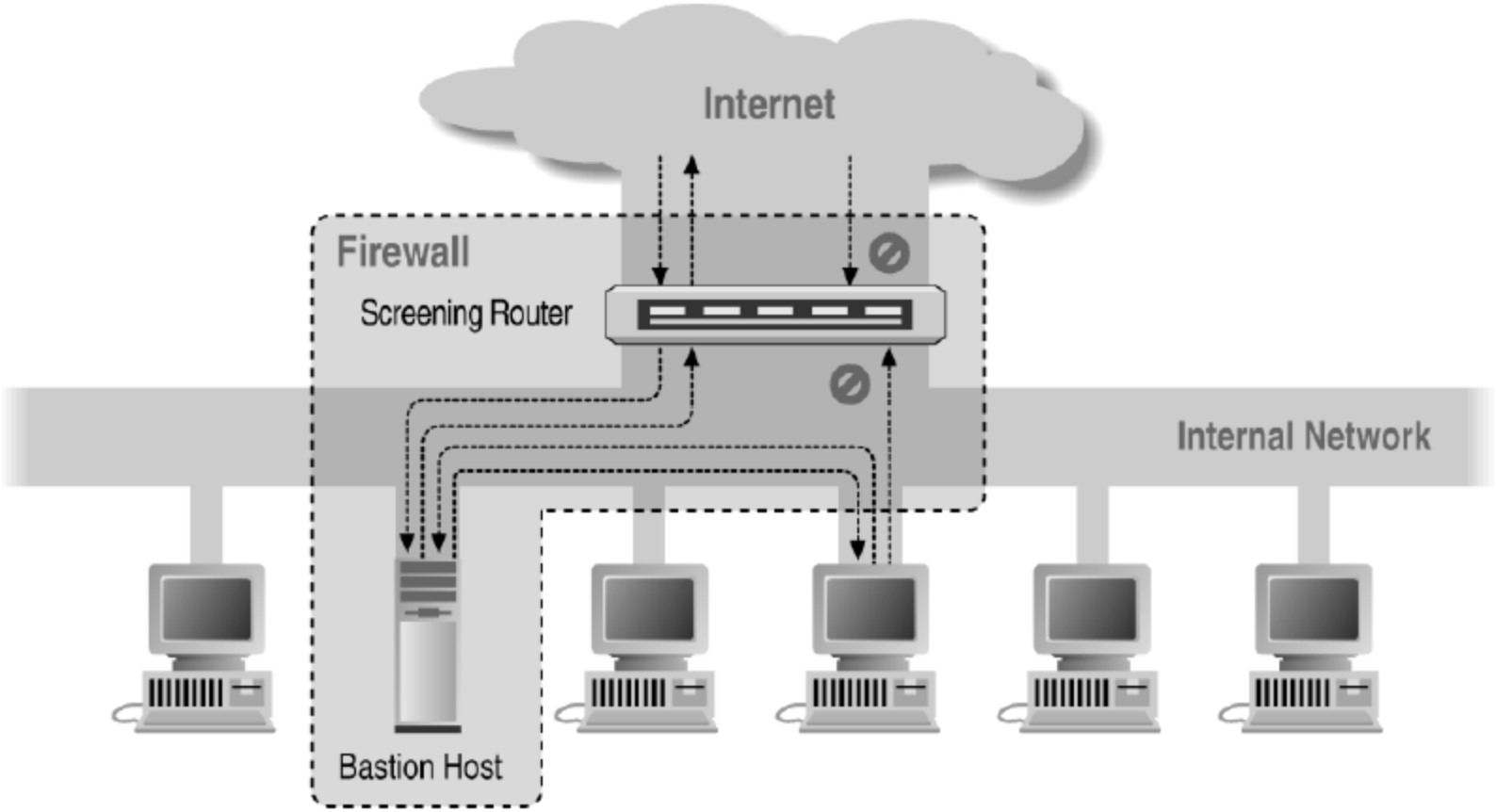
Multiple Exterior Routers



Architettura Screened Host

- Componenti HW (**Router** e **Bastion Host**)
- Servizi forniti da Bastion Host (**Application Gateway**)
- Solo il Bastion Host può aprire connessioni con la rete esterna (tutte le connessioni passano da qui)

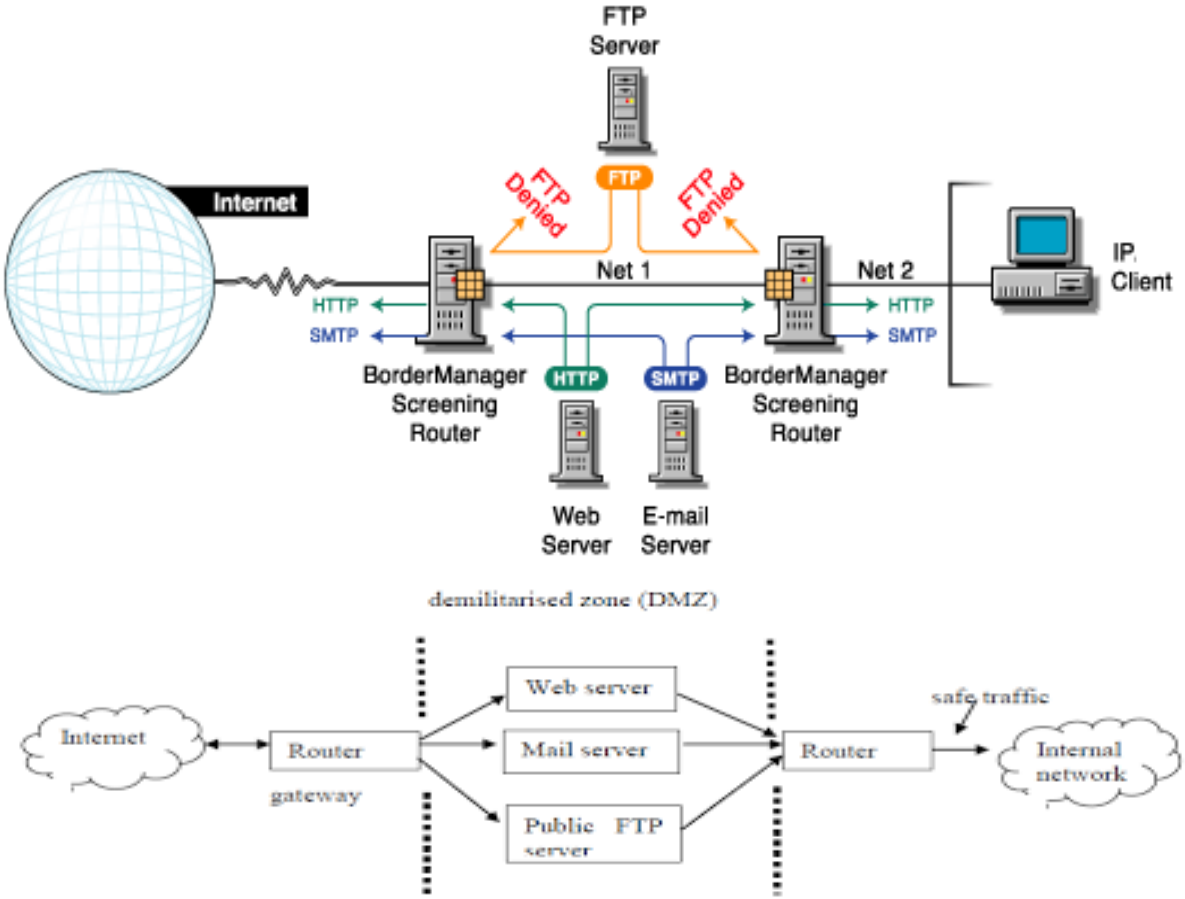


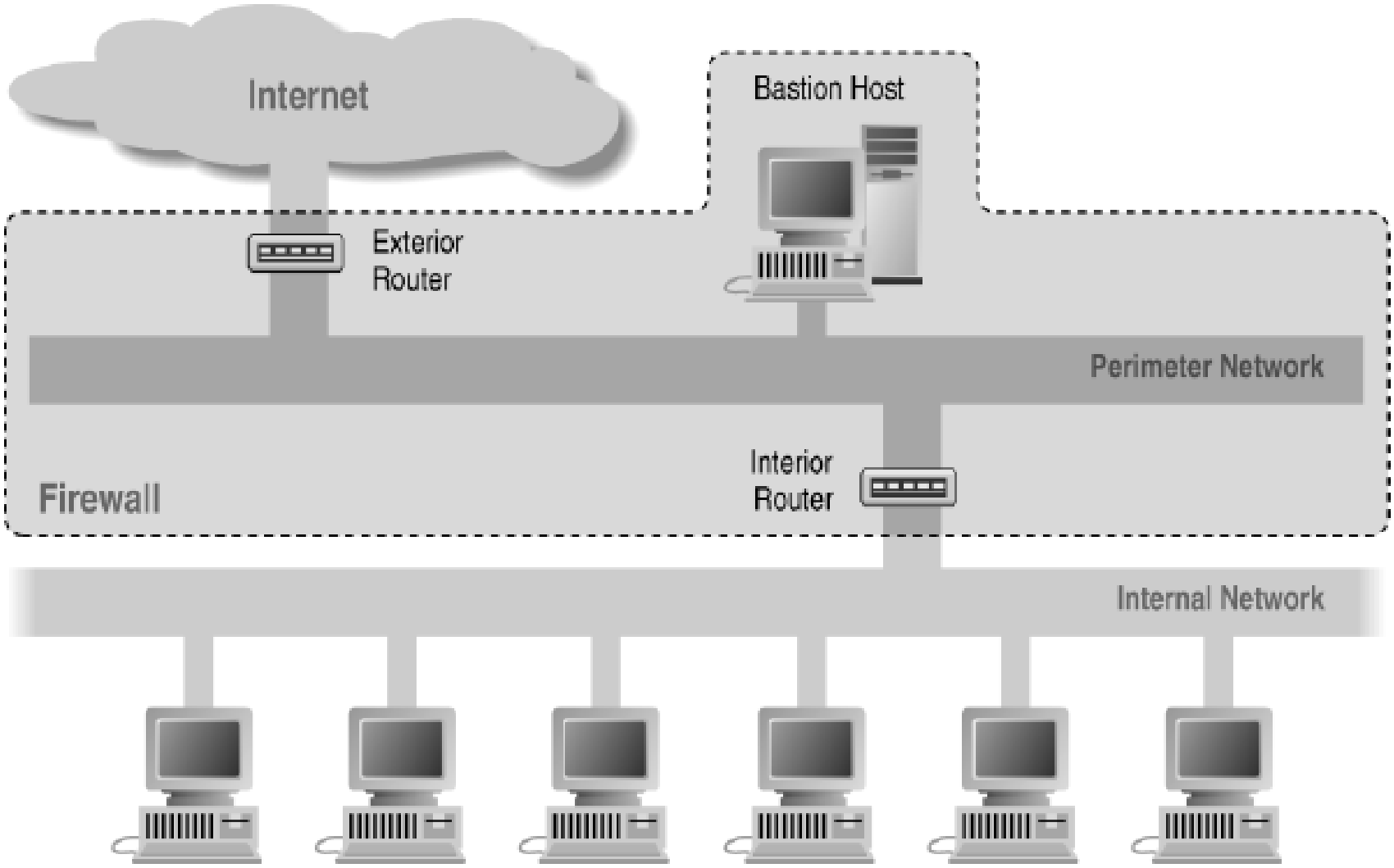


Router di schermatura: indirizza/riceve solo al/dal bastion host

Screened Subnet con due Routers

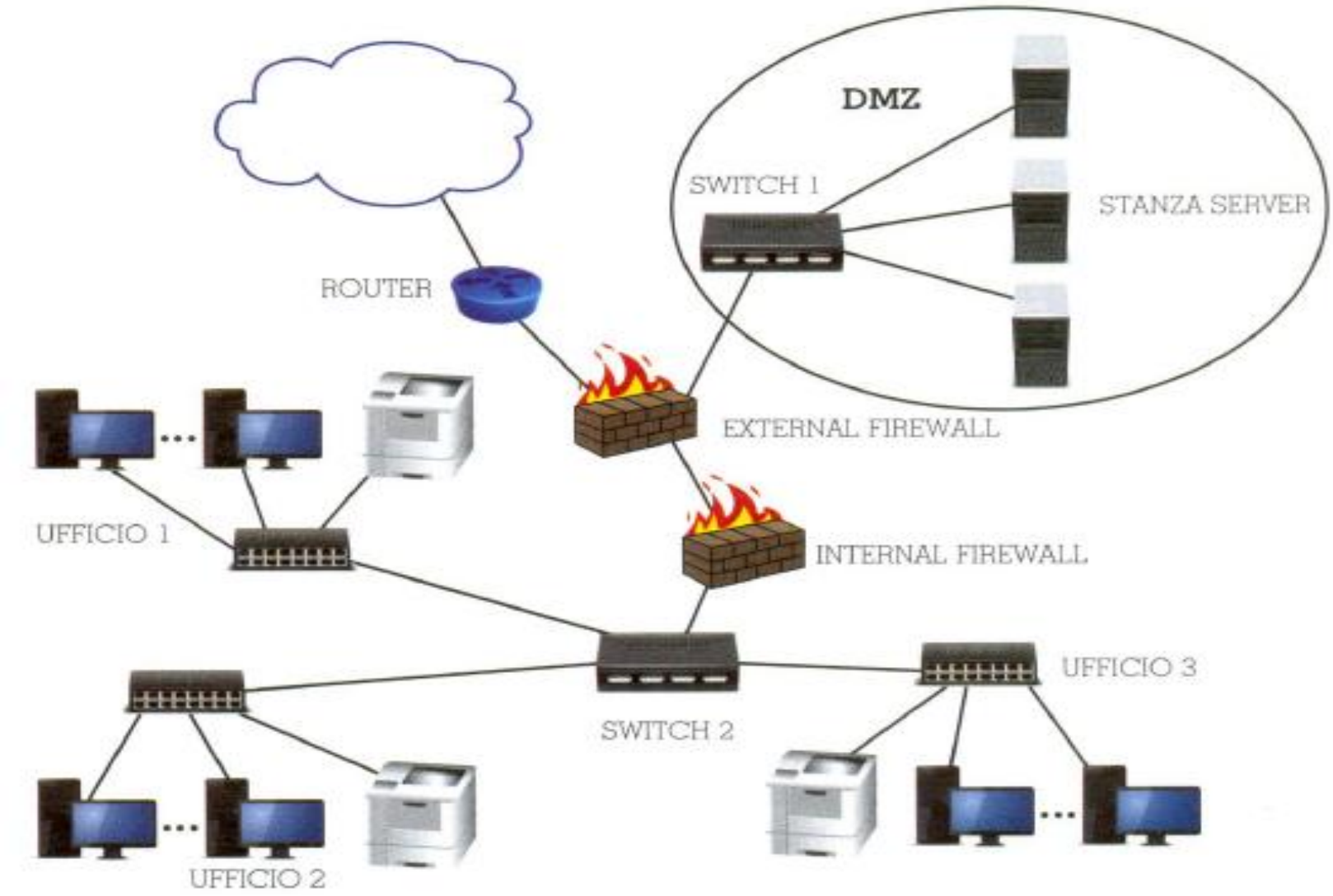
- Componenti HW(**2 Router** e **Bastion Host**)
- Viene isolata una rete tra la rete interna e quella esterna (Screened Subnet)
- Screened Subnet formata da **2 application-level gateway**
- Difficile bypassare, obbligo di riconfigurazione totale della sottorete



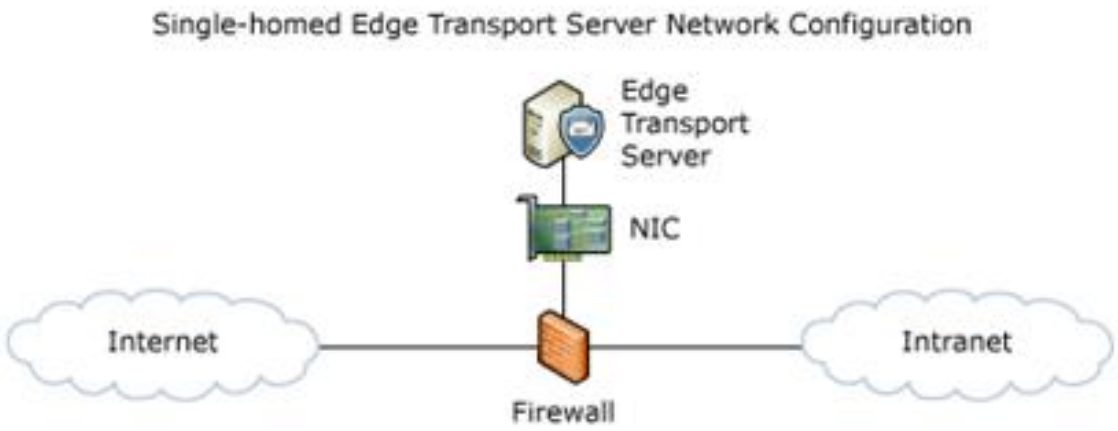


Subnet di schermatura: due router e bastion host in zona DMZ

DMZ in architettura screened subnet



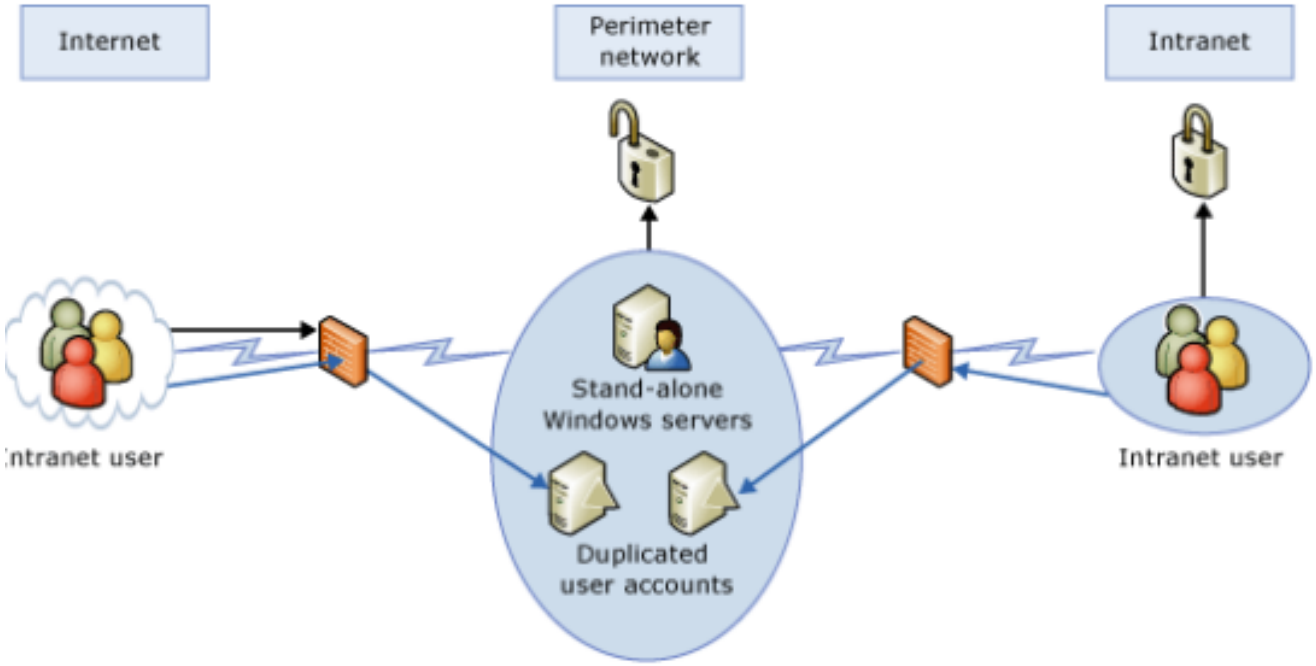
Edge Transport Server in zona perimetrale



Uso di zona perimetrale per gestire la posta elettronica

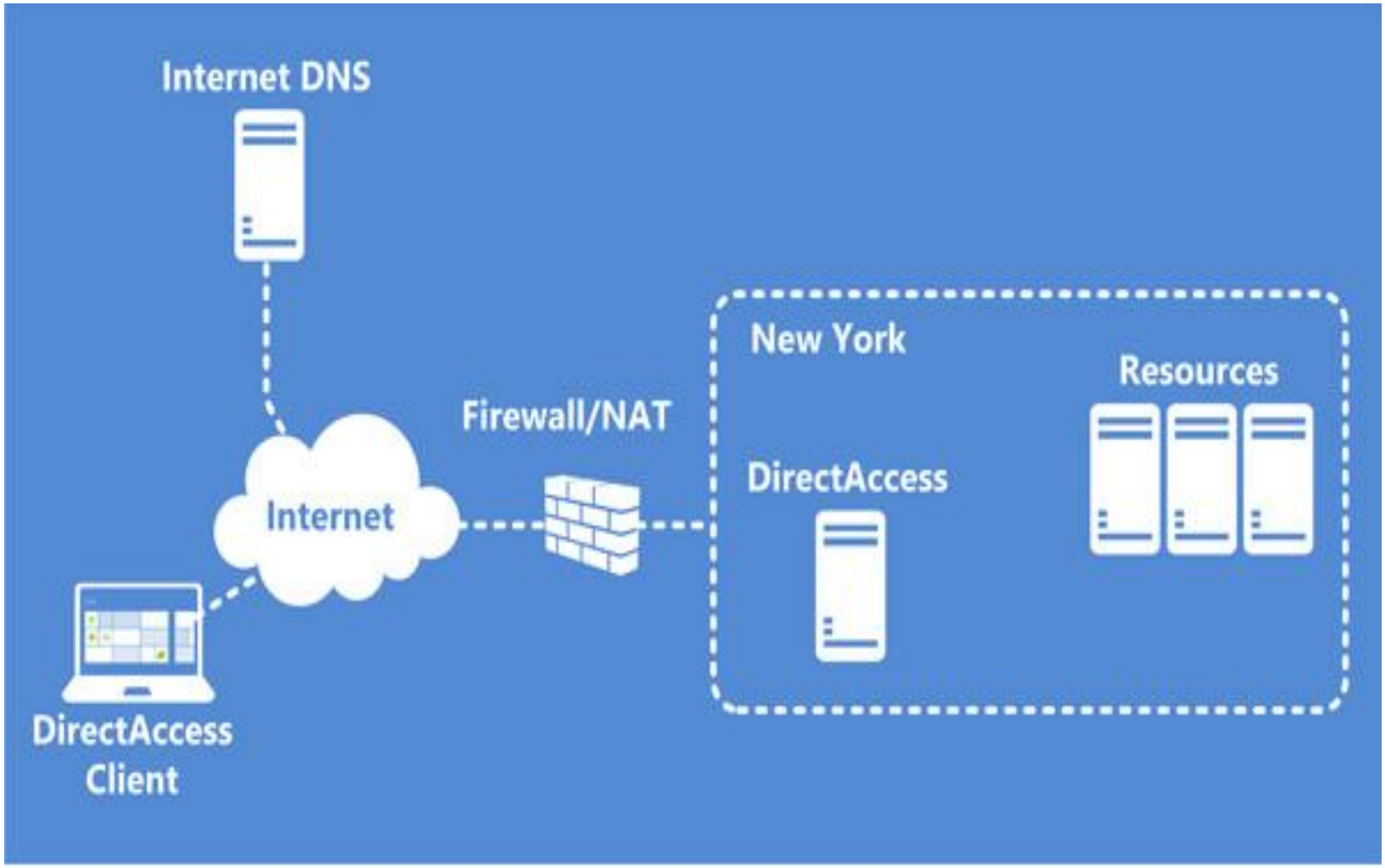
Active Directory Domain Services in zona perimetrale

Uso di zona perimetrale per gestire identità di chi accede alle risorse

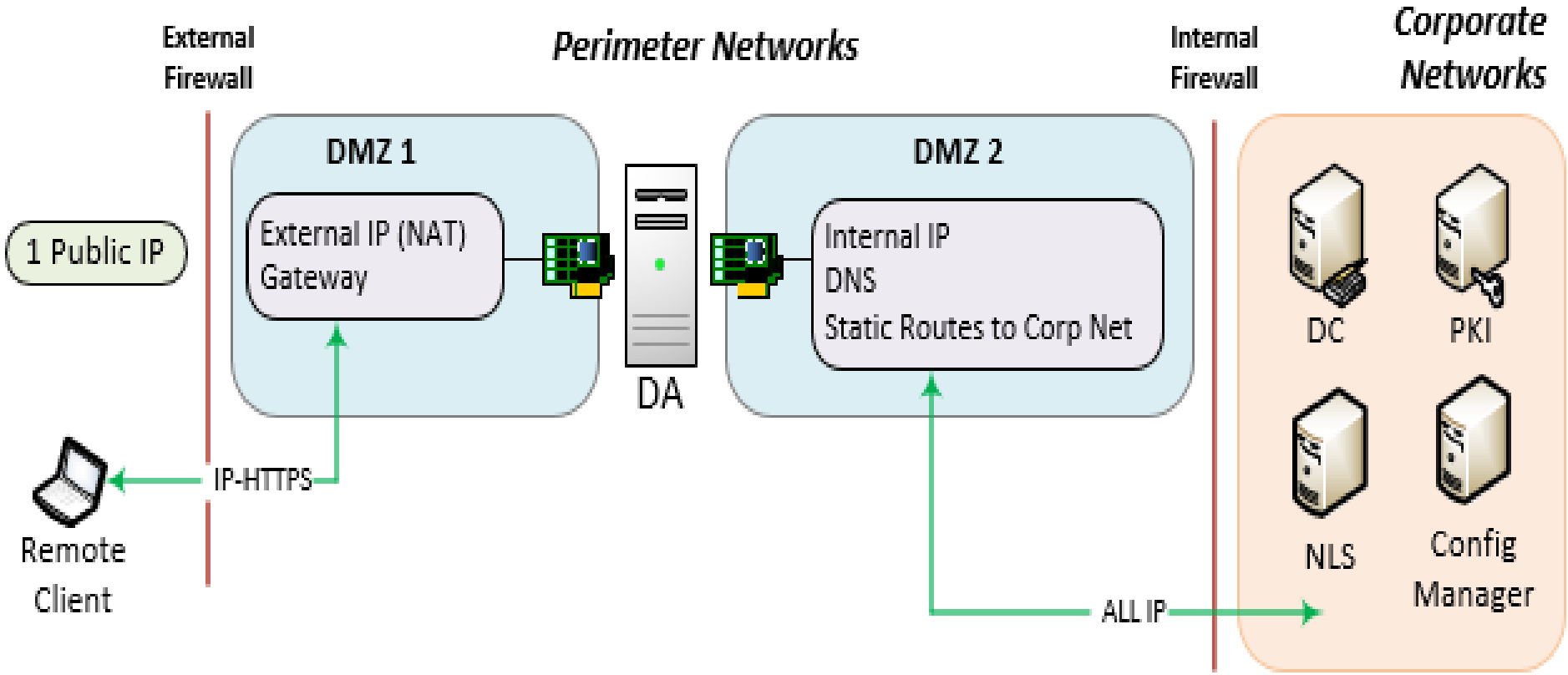


***Active Directory**: un insieme di servizi di rete, meglio noti come directory service, adottati dai sistemi operativi **Microsoft** a partire da Windows 2000 Server e gestiti da un domain controller. Esso si fonda sui concetti di dominio e di directory("elenco telefonico"), ovvero la **modalità con cui vengono assegnate agli utenti tutte le risorse della rete** attraverso i concetti di: account utente, account computer, cartelle condivise ecc... secondo l'assegnazione da parte dell'amministratore di sistema di **Group Policy** ovvero **criteri di gruppo**.*

DirectAccess RemoteDesktopProtocol in zona perimetrale



Esempio: 2 DMZ e server DirectAccess



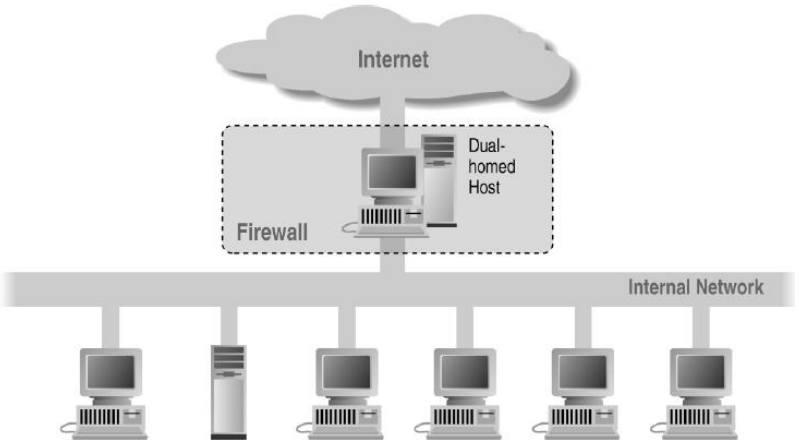
***DirectAcess**: noto anche come Unified Remote Access, è una tecnologia VPN-like che fornisce la connettività intranet ai computer client quando sono collegati a Internet. A differenza di molte connessioni VPN tradizionali, che devono essere iniziate e terminate da un'azione esplicita dell'utente, le connessioni DirectAccess sono progettate per collegare automaticamente non appena il computer si connette a Internet.*

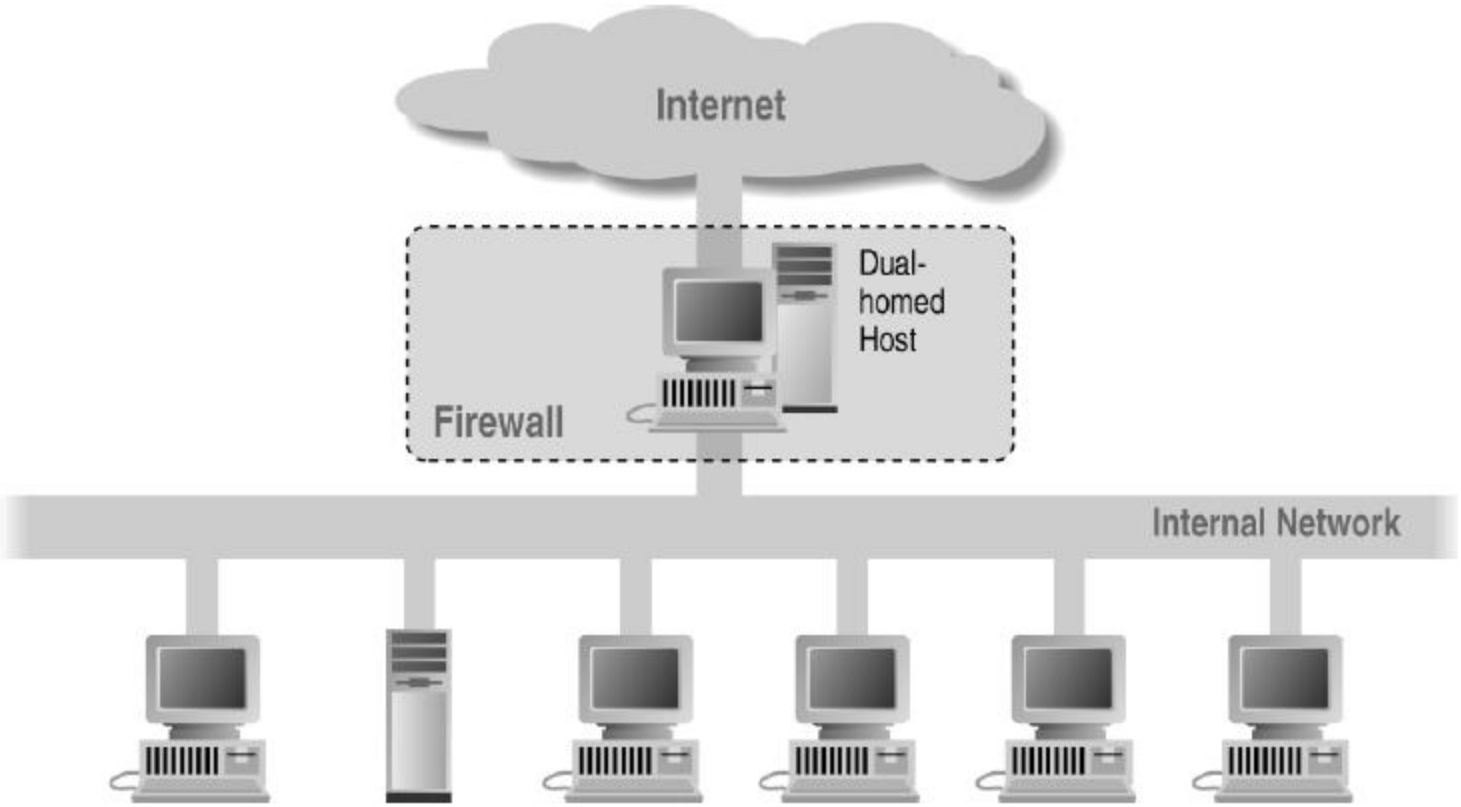
Architettura Dual Homed Host (DHH)

- Dual Homed Host funzione di firewall e di servizi come SMTP e NNTP (Network News Transfer Protocol : applicazione comune *Newsgroup*)
- Host collegato a rete interna ed esterna

  (**2 schede di rete**). Funzione IP-Forwarding
- Importante rimuovere dal DHH utilities e programmi che potrebbero

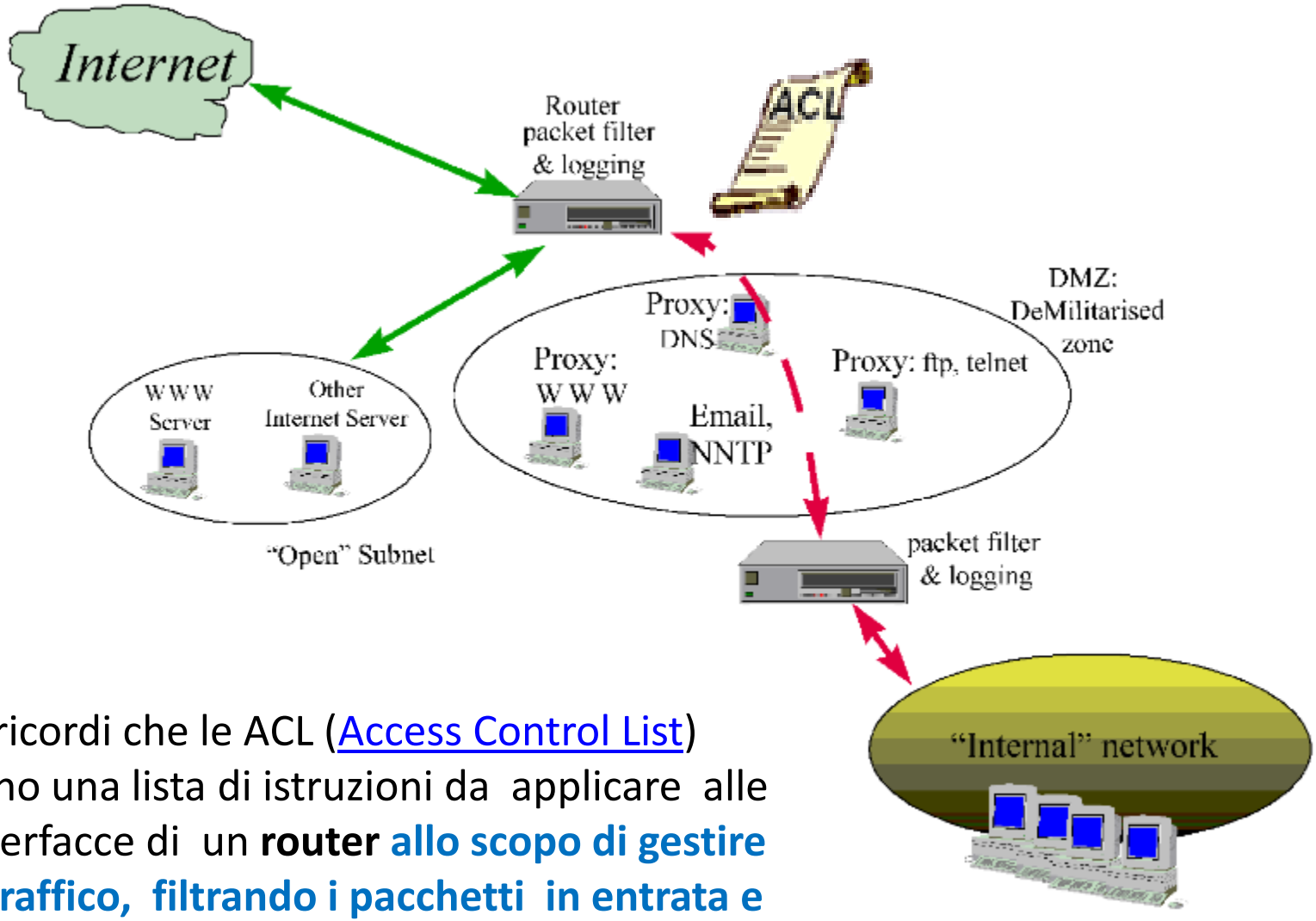
  essere usati per bypass la rete





Funzione di firewall su HOST con 2 schede di rete, solitamente collegato ad un router

ACL



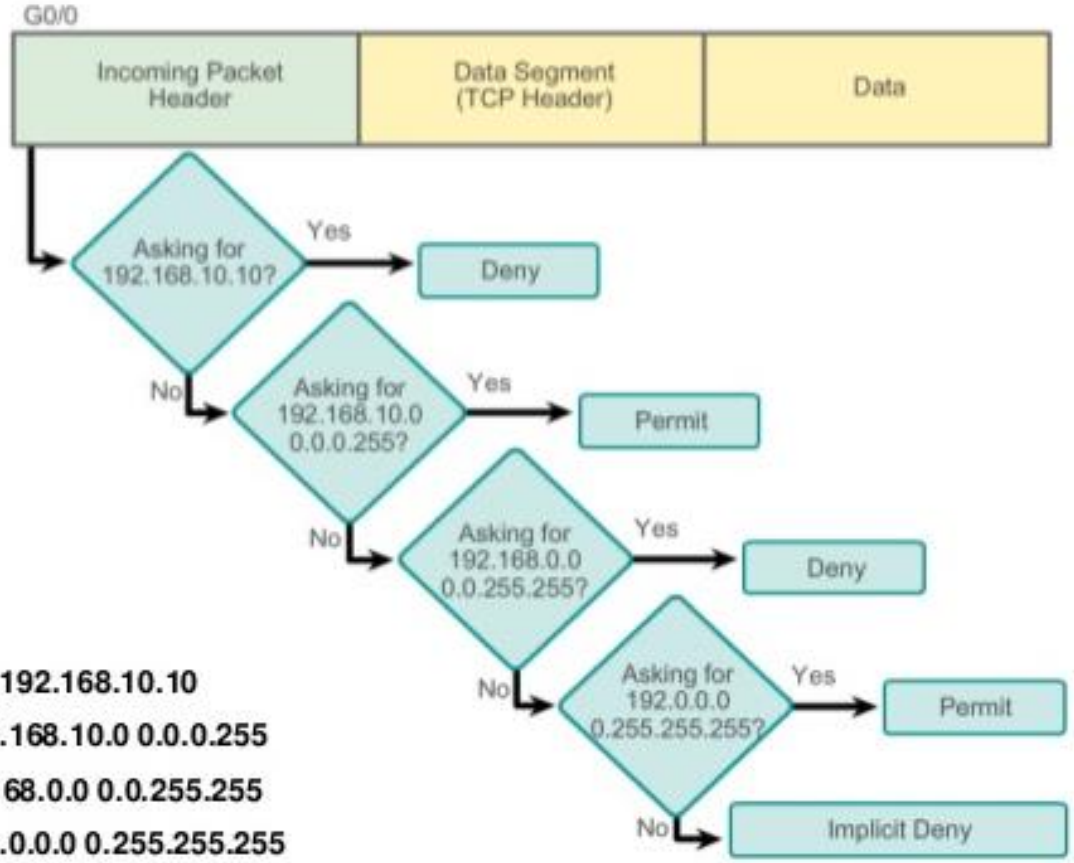
Si ricordi che le ACL (Access Control List) sono una lista di istruzioni da applicare alle interfacce di un **router** **allo scopo di gestire il traffico, filtrando i pacchetti in entrata e in uscita**

ACL standard: controllo sull'indirizzo del mittente

Configuring a Standard ACL

Elaborazione **sequenziale**

inserire regole più restrittive all'inizio



Example ACL

- **access-list 2 deny host 192.168.10.10**
- **access-list 2 permit 192.168.10.0 0.0.0.255**
- **access-list 2 deny 192.168.0.0 0.0.255.255**
- **access-list 2 permit 192.0.0.0 0.255.255.255**

Tipi di ACL per IP (Cisco)

– access list IP standard
– usano solo **indirizzi sorgente** per controllo
– sono identificate con numeri da 1 a 99
– formato: access-list access-list-number {permit|deny} {host|source source-wildcard|any}

– access list IP standard estese
– indirizzi **sia sorgente che destinazione** e, opzionalmente: **protocollo e porta**
– sono identificate con numeri da 100 a 199

ACL estese

Le ACL estese possono effettuare il **controllo** non solo **sull'indirizzo** del **mittente**, ma anche su quello del **destinatario**, su uno specifico **protocollo**, sul **numero di porta** o su altri parametri.

Il controllo effettuato sul protocollo merita una precisazione:

le ACL Standard permettono di negare o no un'intera suite di protocolli (es. IP, …) eseguendo il controllo su un'intera rete e si effettua di conseguenza anche il controllo sul protocollo di comunicazione utilizzato, quindi non permettono di gestirne singolarmente le varie componenti.

Al contrario le ACL estese possono effettuare **controlli sui singoli protocolli** che compongono la suite (es. ICMP, …).

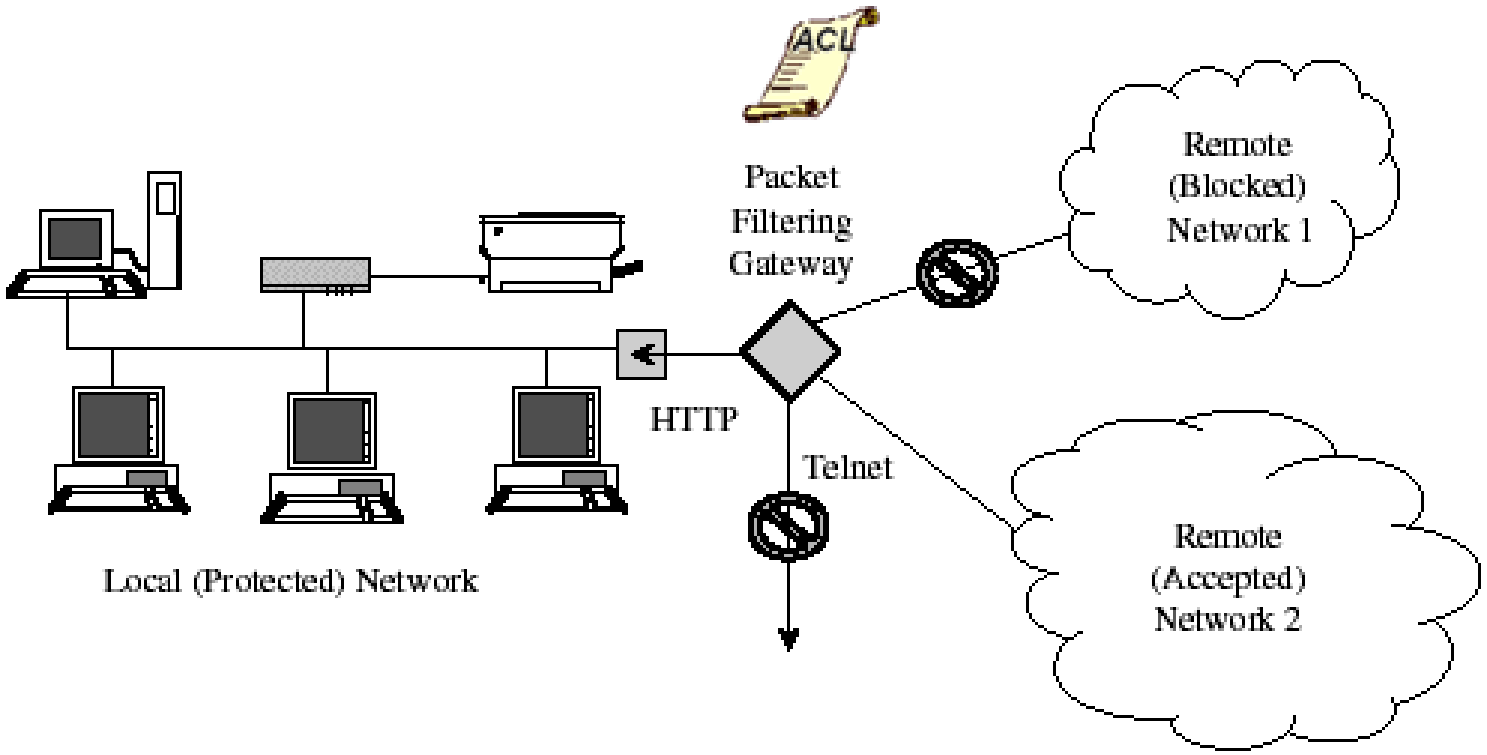
ACL Estese

- Filtrare sulla base di **porte TCP/UDP** per selezionare le applicazioni permesse
- Ci si basa sull'uso delle "***well known ports***"
- utenti sofisticati possono usare ***porte non standard*** per le applicazioni

- Le ACL ***tcp established*** selezionano tutti i pacchetti TCP tranne quelli usati per stabilire la connessione
- Permettere di iniziare connessioni TCP **solo in una direzione**
- **Impedire** che i server interni su TCP siano **visibili** dall'esterno

Esempio di ACL: blocco di indirizzi e protocolli

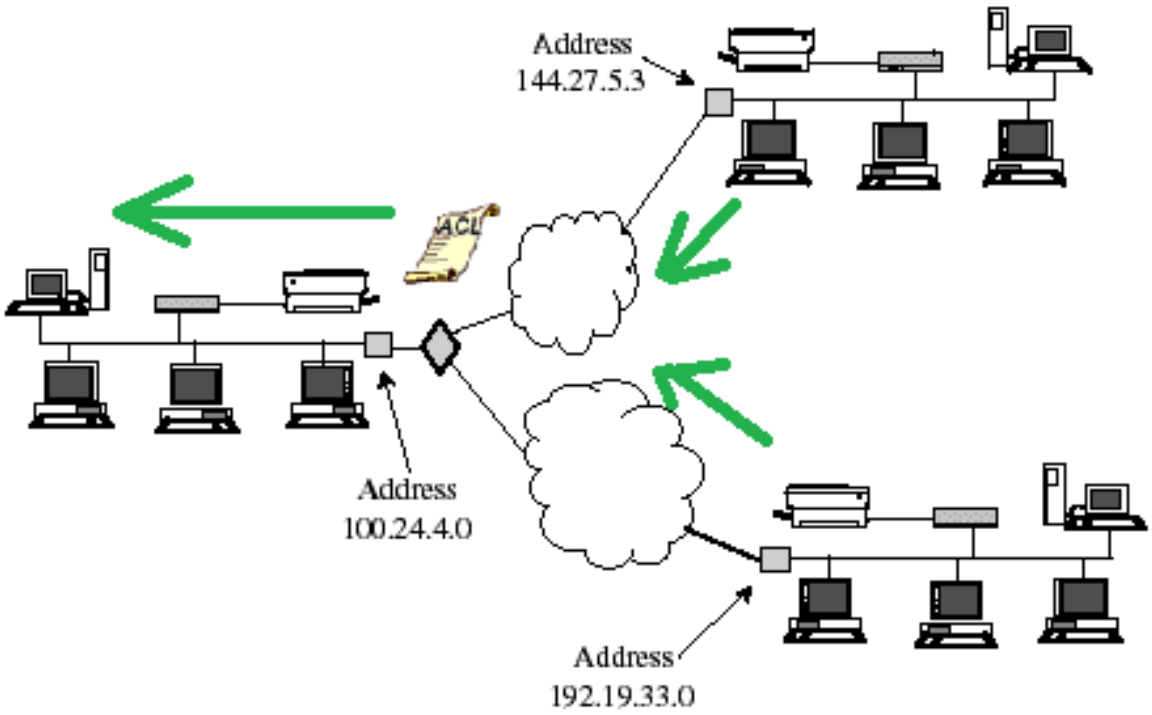
- è **permesso il *traffico* HTTP** solo in connessione con una **particolare rete remota**



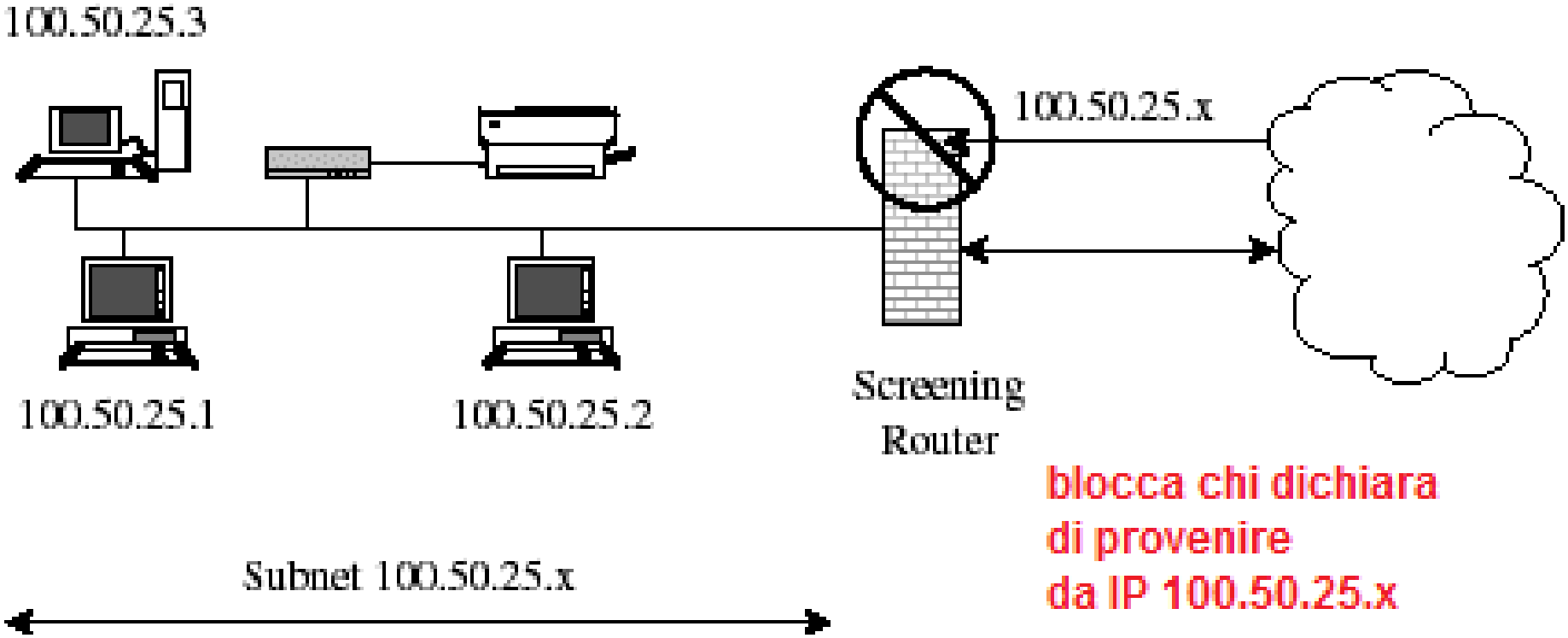
Esempio di ACL

- Una compagnia internazionale potrebbe volere la comunicazione solo tra tre LAN della rete aziendale con particolari **regole** →

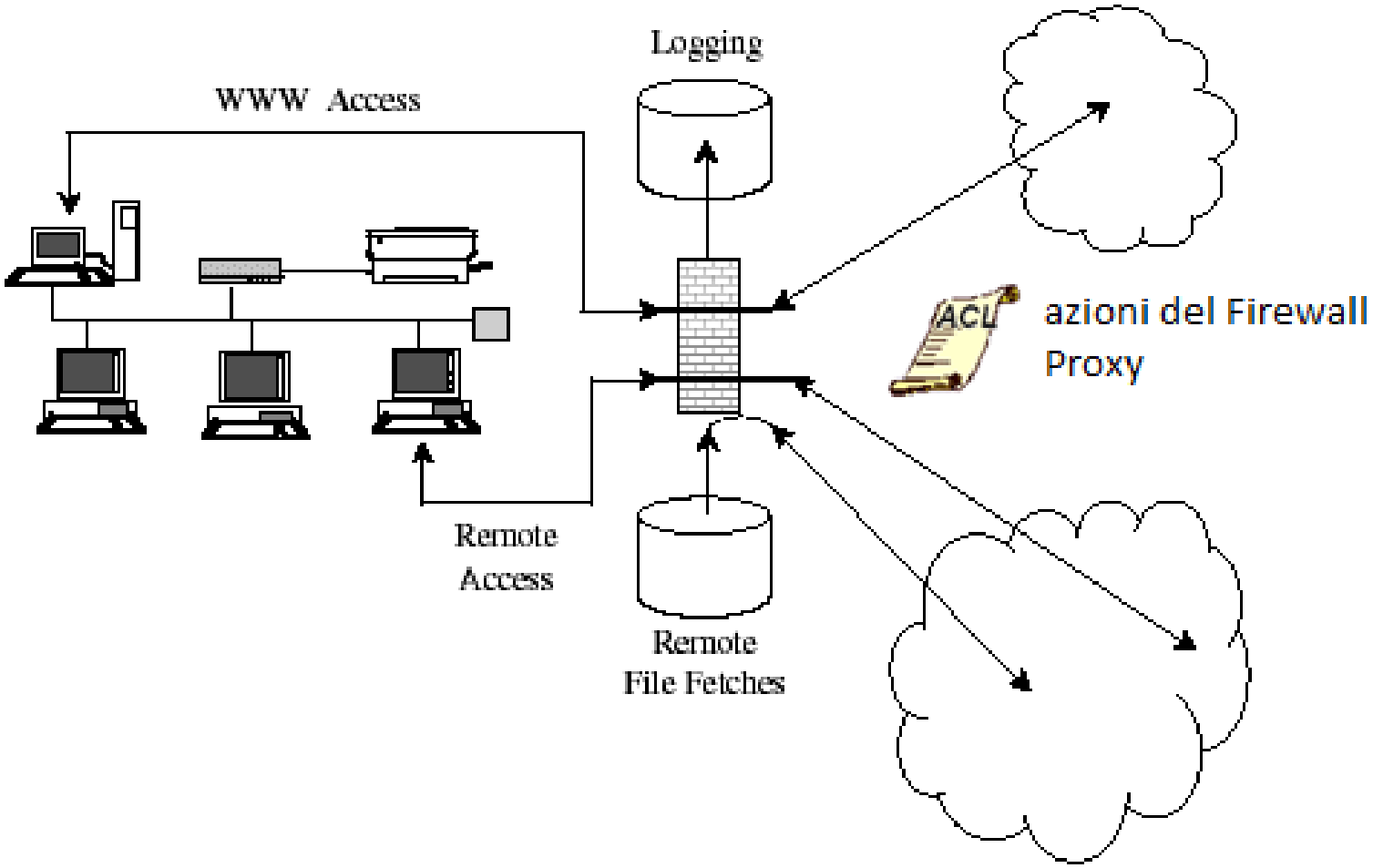
Uso di un **router di schermatura** sulla LAN con IP di rete 100.24.4.0 per permettere *in ingresso* solo le comunicazioni destinate ad host nella rete stessa ed *in uscita* solo le comunicazioni indirizzate ad entrambe le reti 144.27.5.3 e 192.19.33.0



Esempio di ACL: impedire IP Spoofing *semplice*



ACL su Proxy


Logging
WWW Access
ACL
azioni del Firewall
Proxy
Remote
Access
Remote
File Fetches

I firewall sono perfetti?

- A meno che gli attacchi non vengano dall'interno
- In organizzazioni con minacce interne maggiori
  - Banche e strutture militari
- Non proteggono da trasferimenti di file infetti
  - Per la grande quantità di sistemi operativi e file

Internal Segmentation Firewall (*ISFW)*

- Le topografie di rete sono **radicalmente** cambiate dall'introduzione del primo firewall. Il passaggio di un numero sempre maggiore di applicazioni al ***cloud***

  e la crescita esplosiva

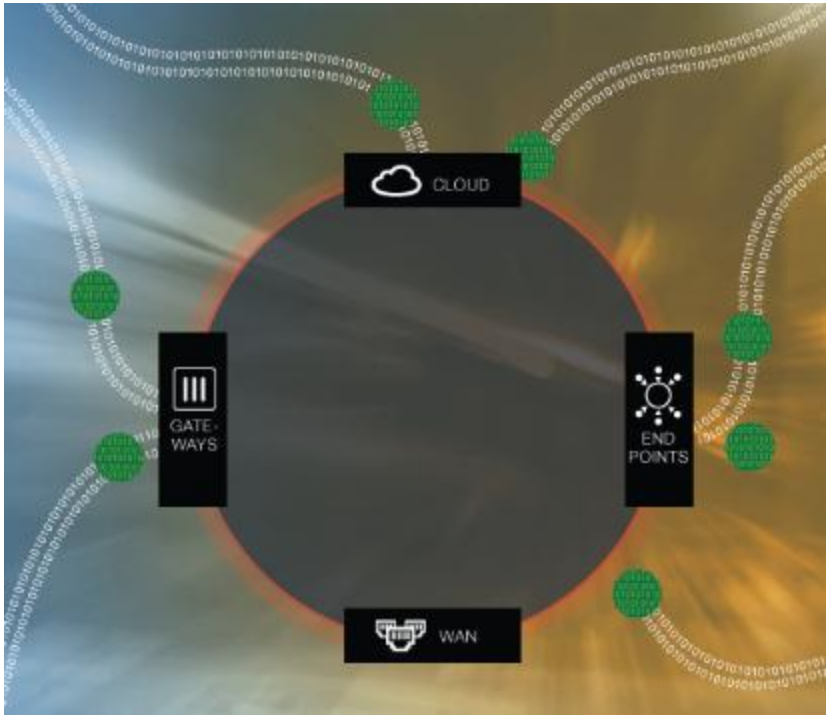
  dei dispositivi che accedono

  alla rete hanno reso il perimetro

  quasi evanescente,

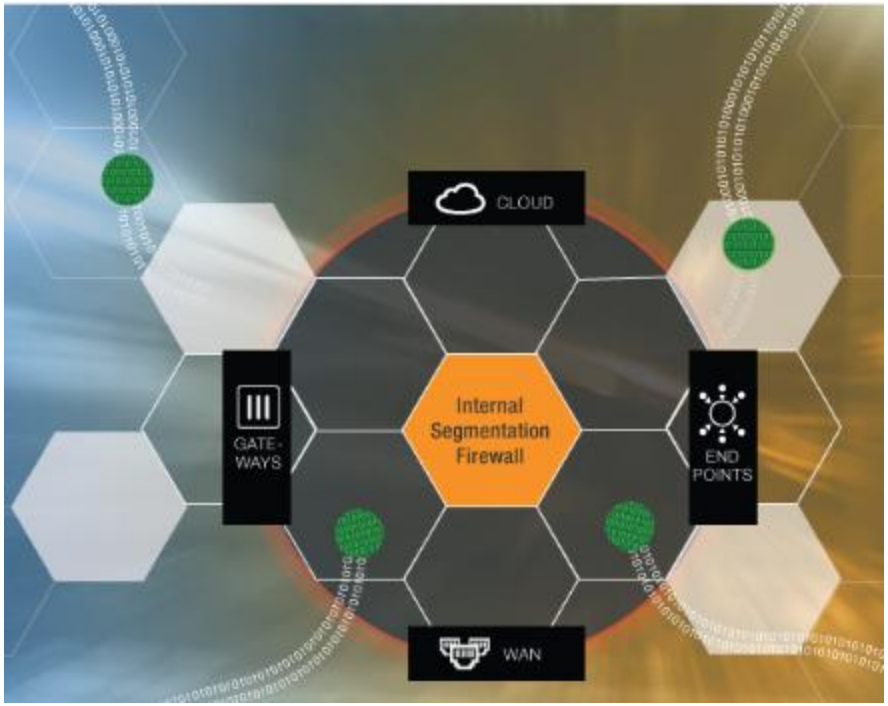
  mentre le minacce

  si sono fatte molto più aggressive

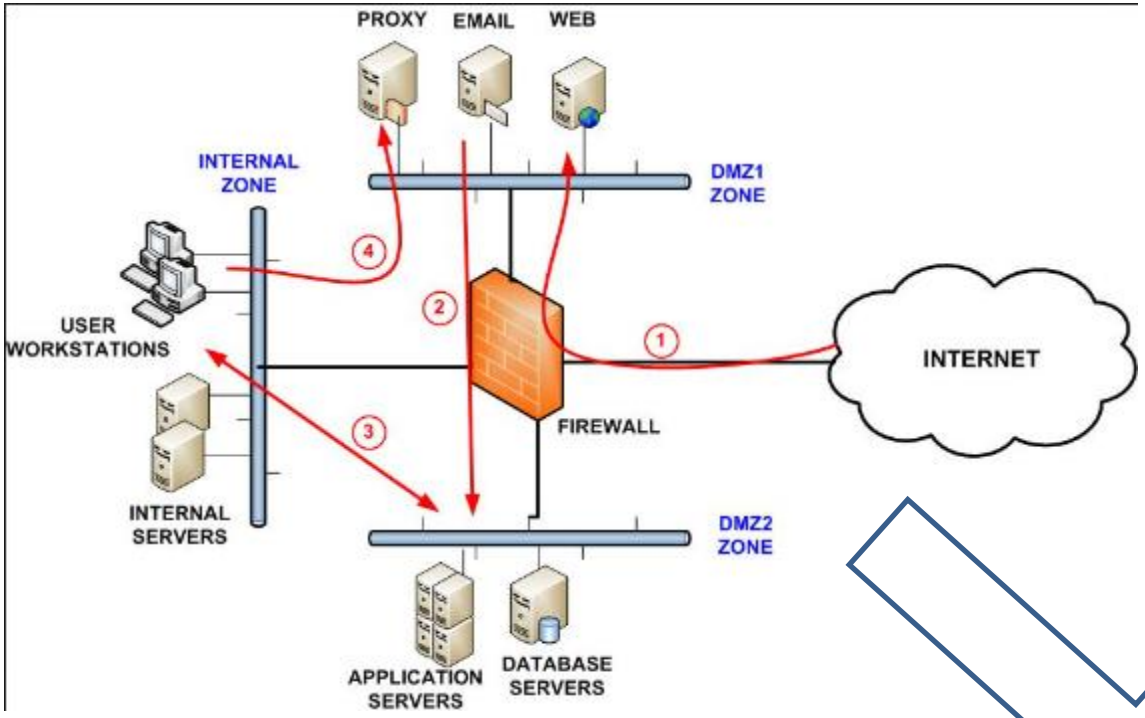


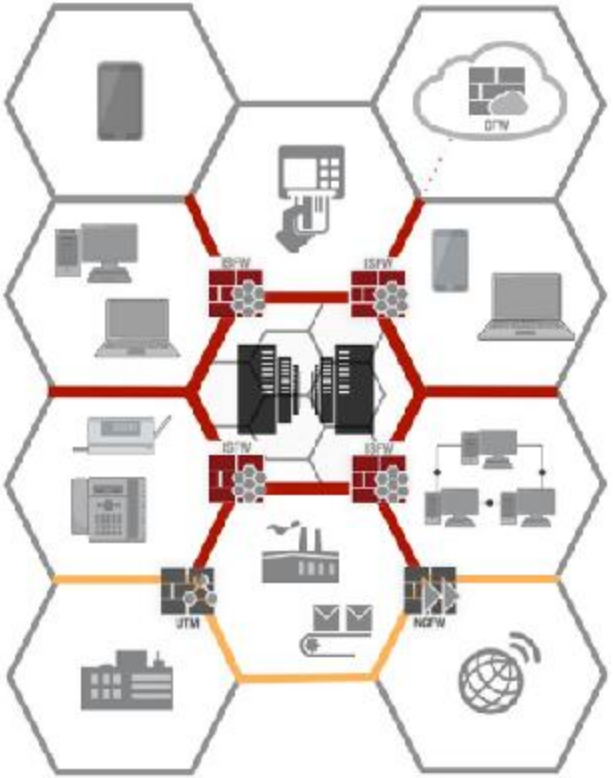
Internal Segmentation Firewall (*ISFW)*

- Per rispondere a questa esigenza è nata una nuova categoria di firewall, **gli Internal Segmentation Firewall (ISFW)**, da collocare in punti strategici della rete interna.
  Questi dispositivi possono
  essere installati davanti
  a specifici server
  o fare da scudo
  contro una serie di dispositivi
  utente o applicazioni web
  eseguite nel ***cloud***.



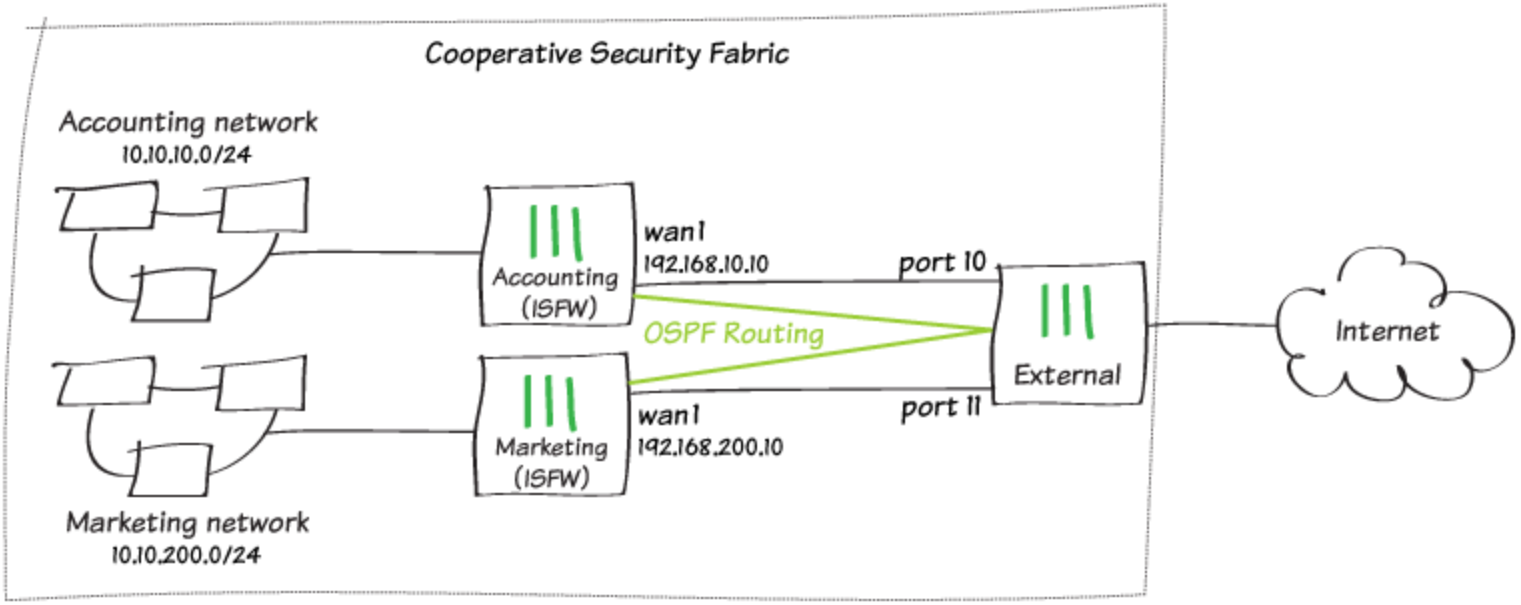
Segmentare:


PROXY
EMAIL
WEB
INTERNAL ZONE
DMZ1 ZONE
USER WORKSTATIONS
INTERNET
FIREWALL
INTERNAL SERVERS
DMZ2 ZONE
APPLICATION SERVERS
DATABASE SERVERS
1
2
3
4

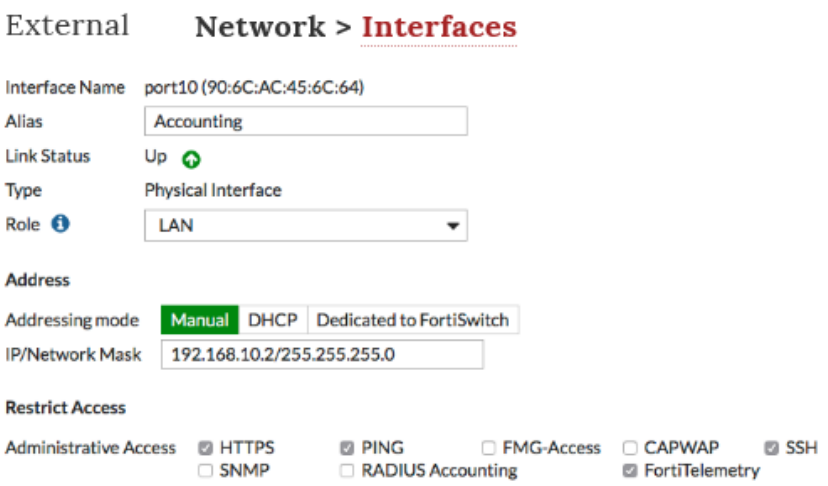


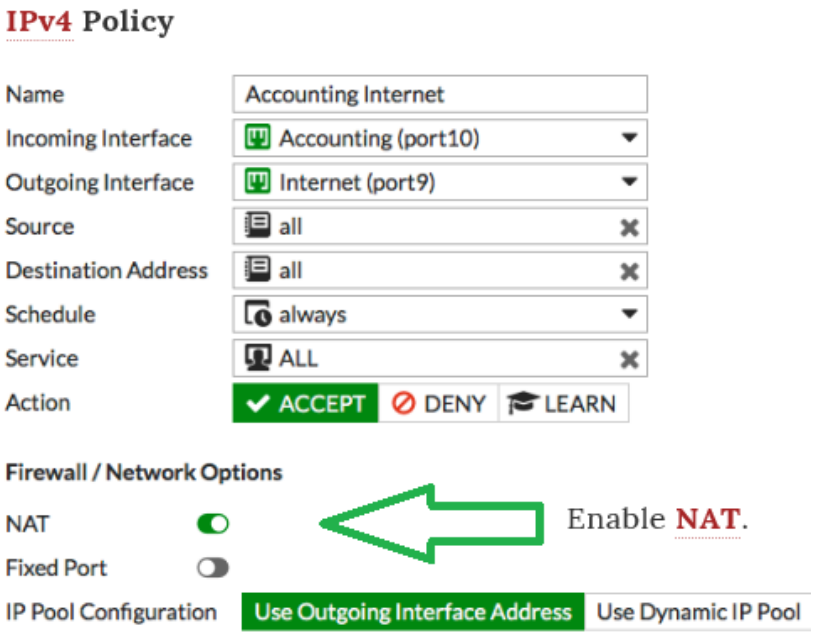
Internal Segmentation Firewall (*ISFW)*

- Indipendentemente da dove vengono collocati, gli **ISFW** assicurano che alle risorse possano accedere solo gli utenti autorizzati, con l'ausilio di un sofisticato meccanismo che collega le **identità degli utenti** a **specifiche policy**.

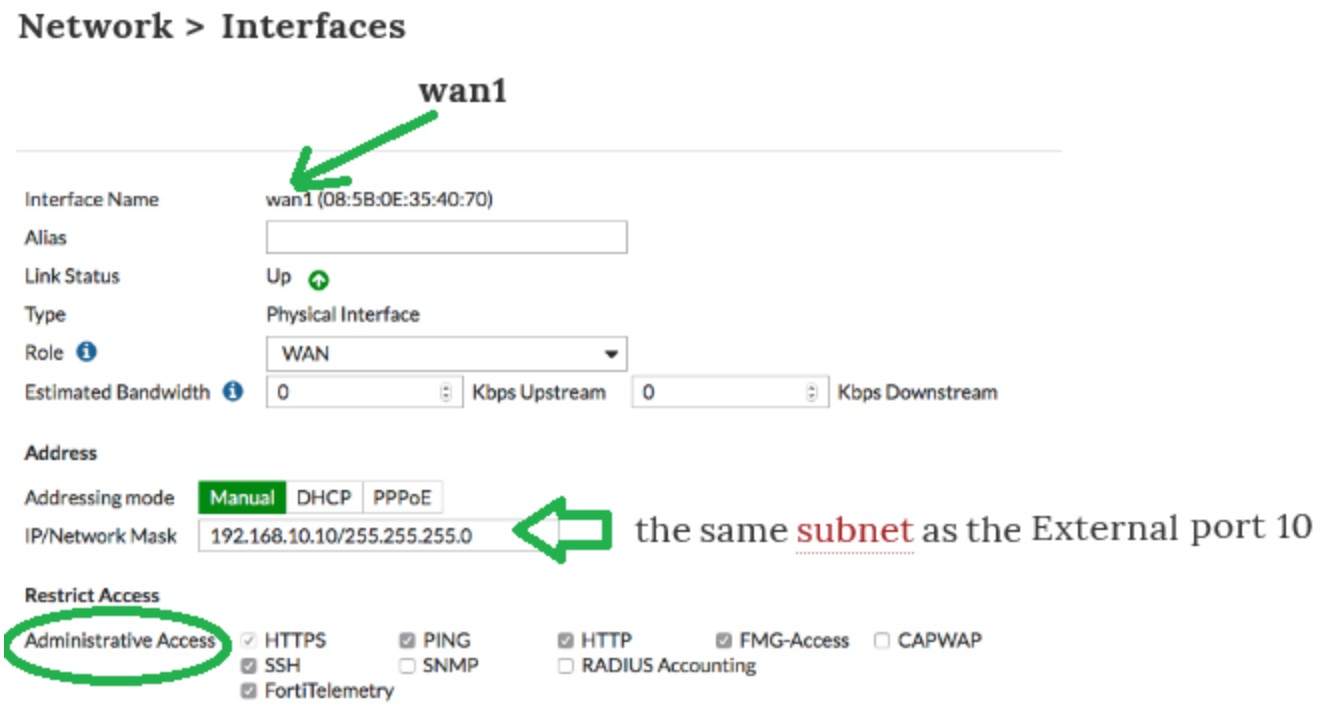


Configurare Gate Esterno: esempio WAN Interna Accounting

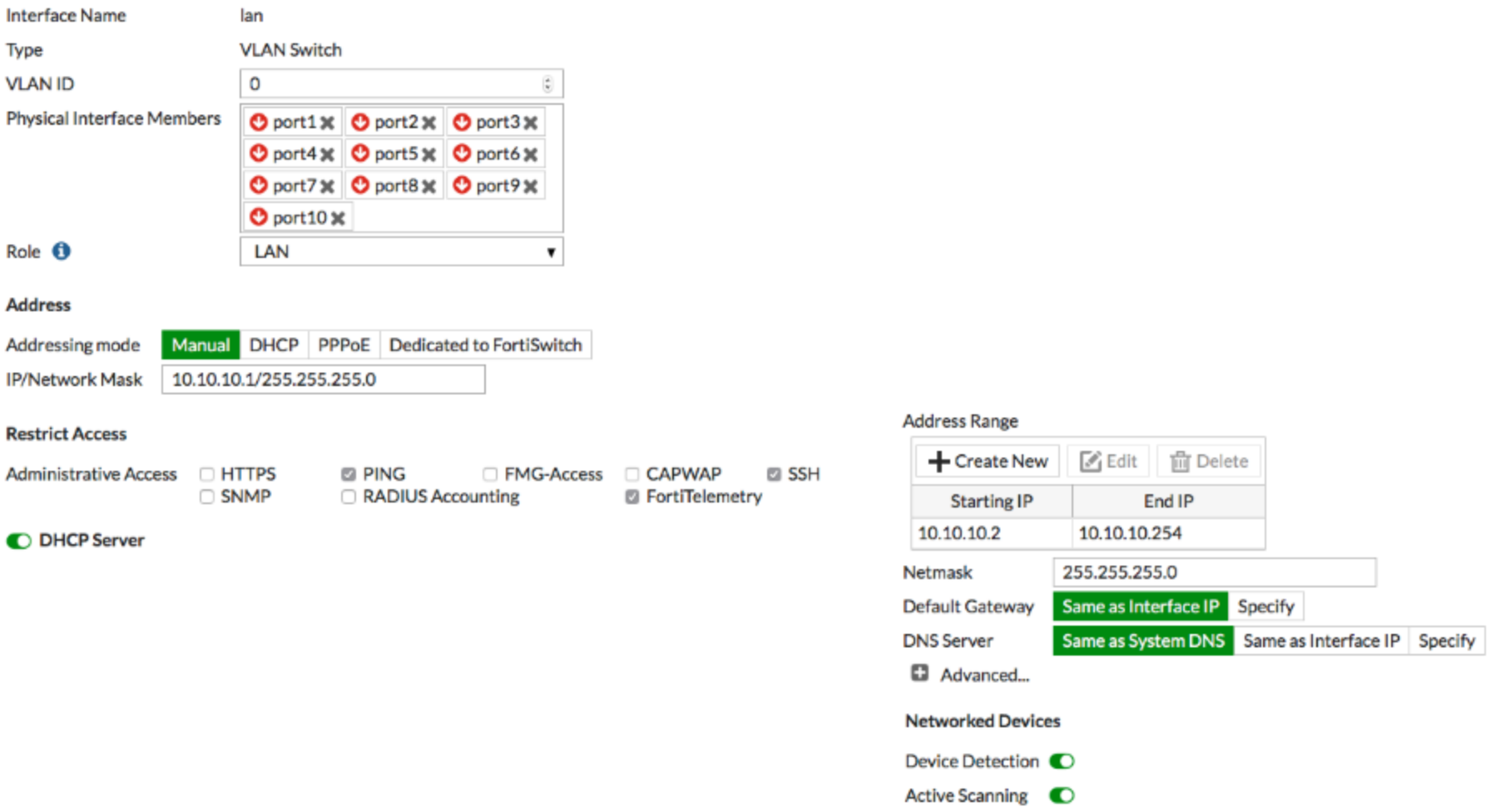




Configurare Gate Esterno: esempio WAN Interna Accounting

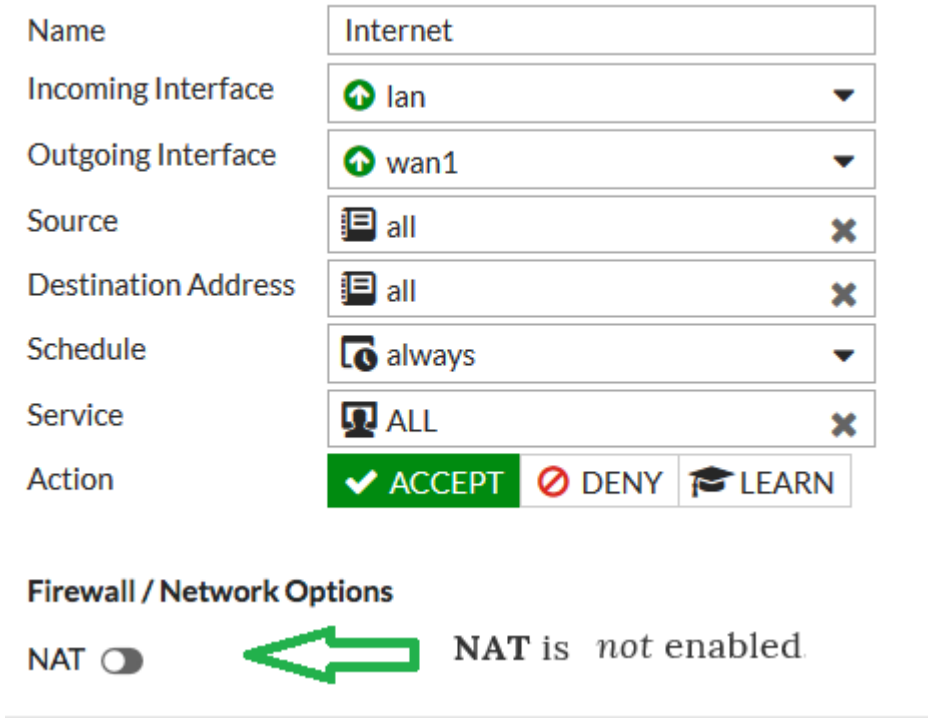


LAN interface



Accesso ad Internet per chi possiede account

IPv4 Policy



Stesso metodo per WAN Marketing

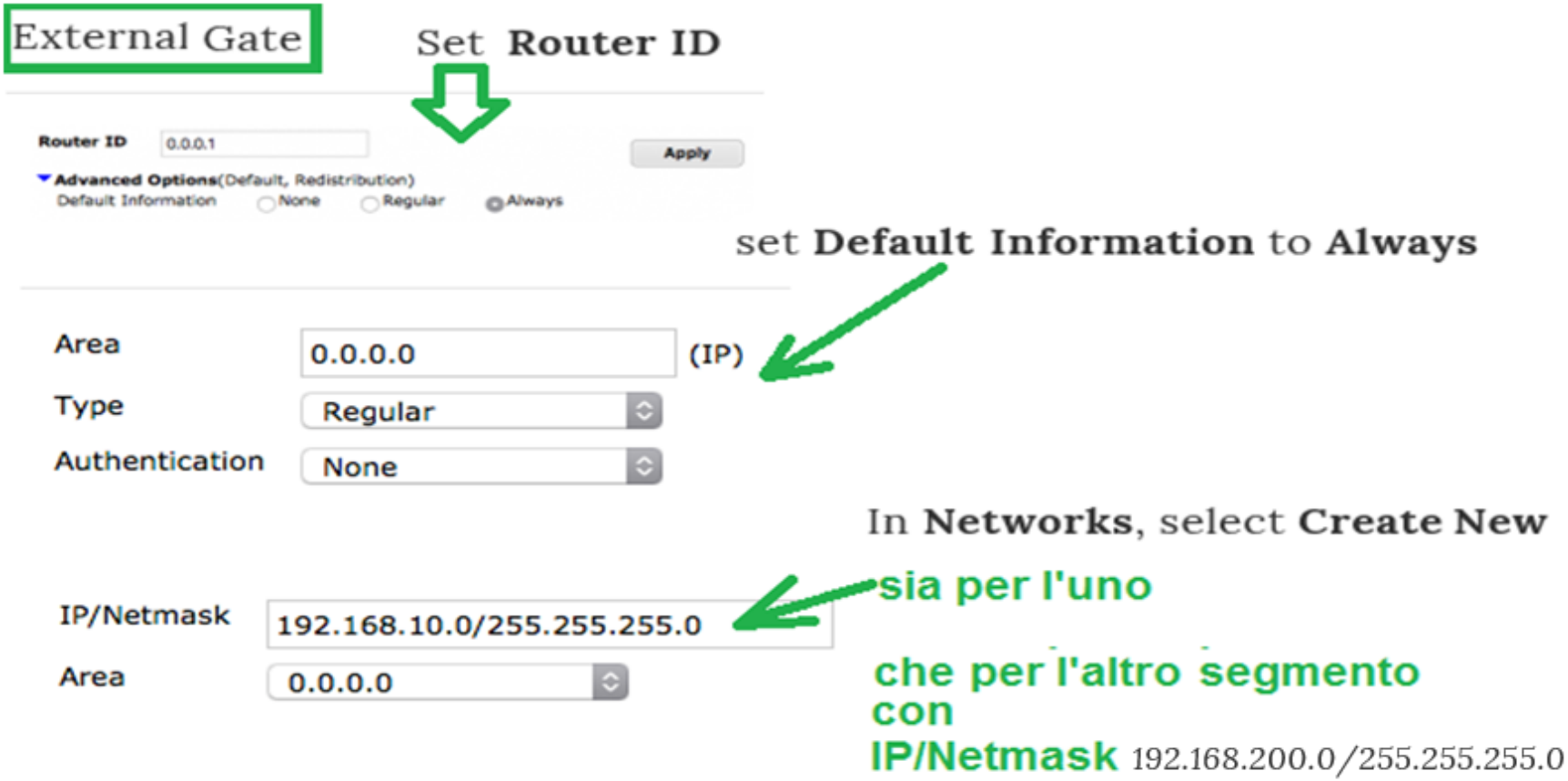
On External

- Configure an interface to connect to the Marketing Gate (this example uses *port 11* with the IP 192.168.200.2)
- Create a policy for traffic from the Marketing Gate to the Internet

On Marketing

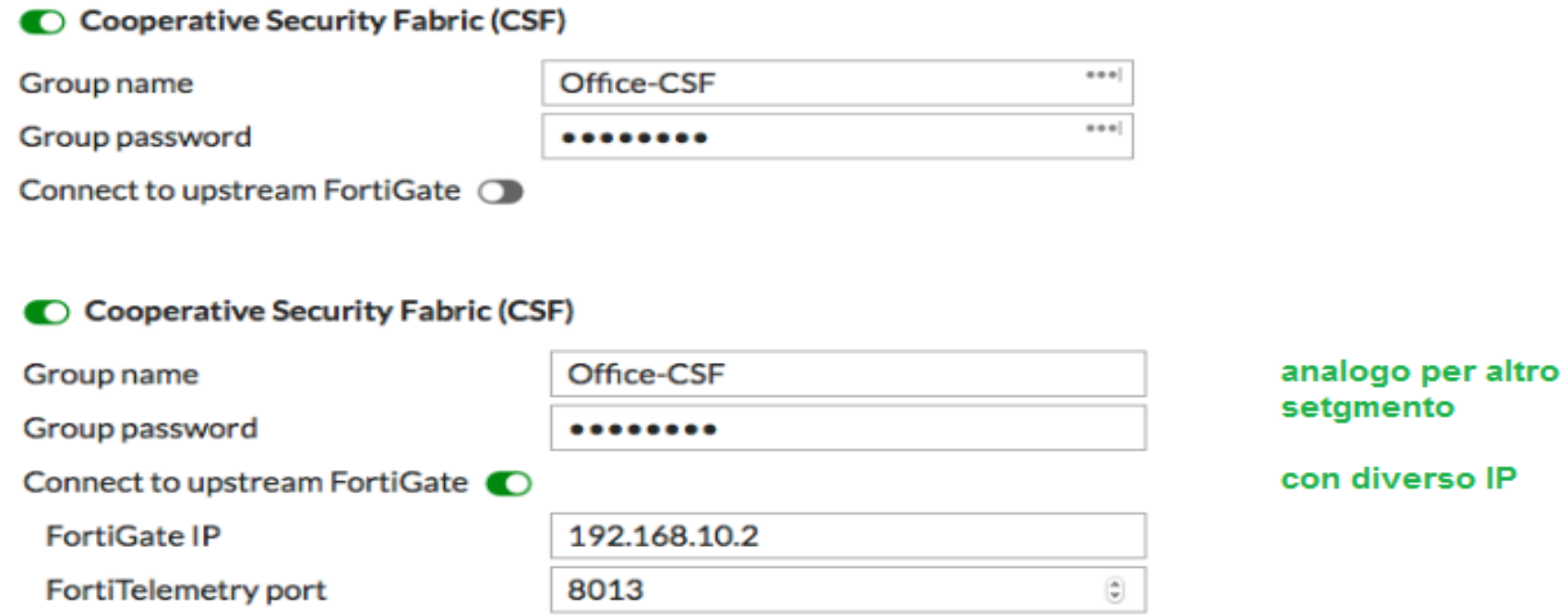
- Configure **wan1** to connect to the External Gate (example IP: 192.168.200.10)
- Configure the **lan** interface for the Marketing Network (example IP: 10.10.200.1)
- Create a policy to allow users on the Marketing network to access the Internet

Open Shortest Path First o *OSPF*

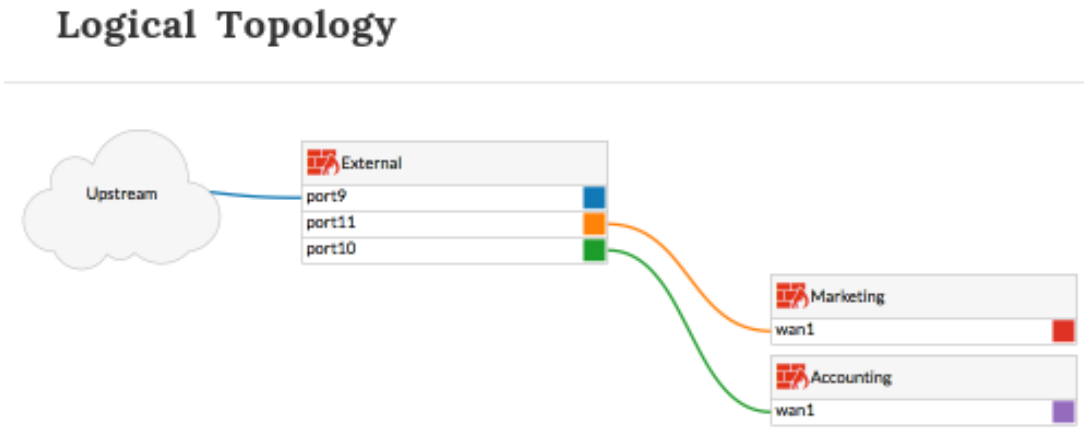


Enable Cooperative Security Fabric

External Gate



Risultato:
topologia fisica e logica



UTM e NGFW: qual è la differenza?

- ***Siamo sommersi da acronimi di tutti i tipi, ma non sempre ne conosciamo il reale significato.***
- ***Cos'è la DLP (data loss prevention) e perché ne dovresti aver bisogno? L'IPS (intrusion prevention system) e l'APT (advanced persistent threat) in cosa differiscono e quale dovresti usare?***

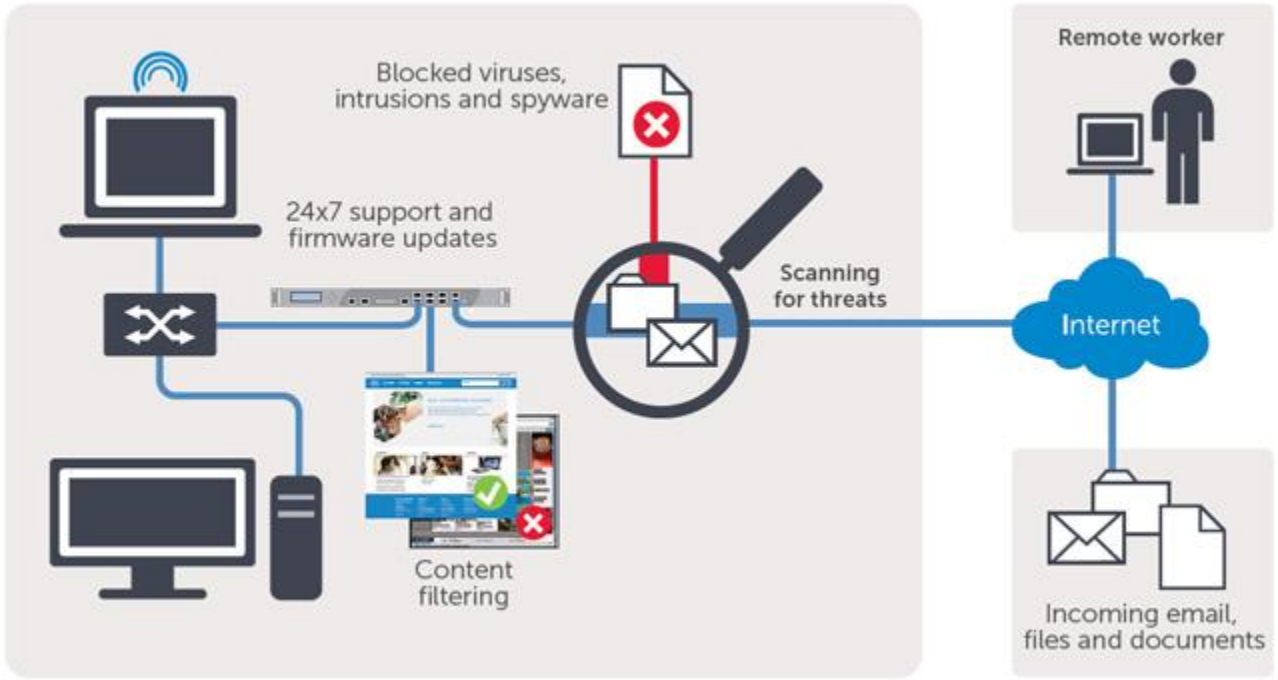
UTM e NGFW

- *Una delle più frequenti domande riguarda il NGFW (next generation firewall): che cos'è e in cosa si differenzia dall'UTM (unified threat management)?*

UTM e NGFW

- *UTM e NGFW non sono poi così differenti come si potrebbe pensare*.
- L'UTM è nato tra le piccole e medie aziende. Solitamente si riferisce a un singolo prodotto con diverse tecnologie di sicurezza integrate (gateway Antivirus, SPAM blocking, URL filtering, Intrusion Prevention, Data Loss Prevention, Reputation Authority, ecc.).
- Le PMI lo amano perché è semplice da implementare e garantisce loro ogni funzionalità di sicurezza di cui hanno bisogno in una sola piattaforma.

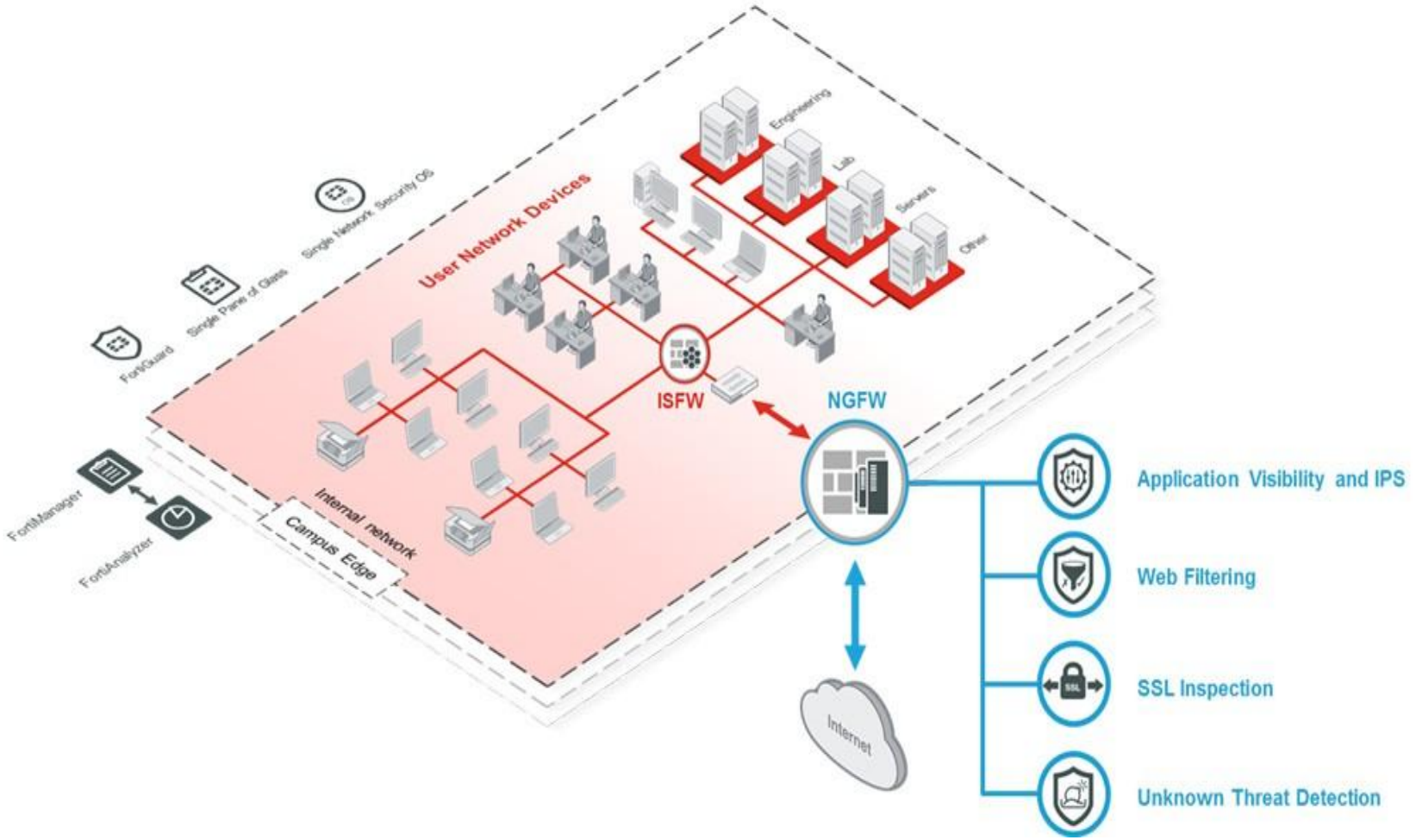
UTM


Blocked viruses,
intrusions and spyware
24x7 support and
firmware updates
Scanning
for threats
Remote worker
Internet
Content
filtering
Incoming email,
files and documents

NGFW

- NGFW è un sottoinsieme di funzionalità, tipicamente presenta solo 2 o 3 moduli che girano su una singola box. Tuttavia, sebbene abbia meno funzionalità, è preferito da molte grandi aziende che tendono a 'dividere' la tecnologia in base a dove debba essere impiegata. Dunque le grandi aziende preferiscono deliberatamente mettere appliance di sicurezza specifiche vicine a ciò che devono proteggere. Per esempio, l'IPS (***intrusion prevention system***) appartiene al perimetro, ma l'AV e il filtraggio SPAM vanno accanto al server di posta elettronica, e così via.

Next generation firewall (NGFW)



UTM e NGFW

- Indipendentemente dalle dimensioni dell'azienda e senza badare a quali soluzioni le persone scelgono, che sia un UTM o un NGFW, può avere senso unificare motori di scansione multipla in una sola box. Non è necessario pagare per hardware aggiuntivo, licenze, contratti di manutenzione ecc.. Inoltre, così facendo si ha migliore possibilità di combattere le minacce multi-vettore di oggi.
- Piuttosto che gestire strumenti di sicurezza separati, con box/console e policy differenti per ciascuna soluzione, unificate la vostra sicurezza.
- Probabilmente la promessa di costi operativi più bassi, unita a livelli di sicurezza maggiori, è ciò che sta guidando la crescita del mercato della sicurezza integrata.

IDS

- Analogia: gli IDS possono essere visti come i sistemi di allarme delle abitazioni
- Lanciano allarmi in caso di attività sospette
- Sono passivi: a differenza dei firewall, hanno il compito di avvisare, non di intervenire

Anomaly detection

- Nella knowledge base mantengono il comportamento “normale”
- Effettuano un’analisi facendo un confronto col comportamento normale
- Tutto ciò che è diverso da questo è un comportamento anomalo

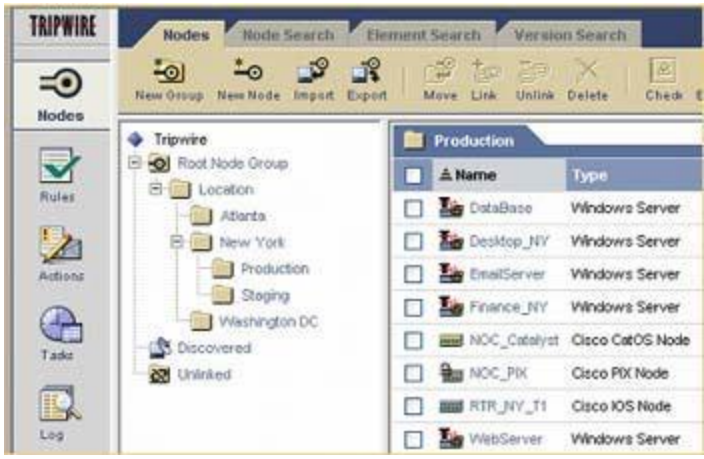
Misuse detection

- Nella KB mantengono il comportamento anomalo
- Effettuano un’analisi cercando i pattern dannosi: hanno un database di firme
- I più usati si basano sul pattern-matching

Anomaly vs Misuse: falsi allarmi

- Falsi negativi: attacchi non rilevati
- Falsi positivi: rilevamento errato
- Gli IDS di tipo *anomaly* producono un maggior numero di falsi positivi e meno falsi negativi
- Gli IDS di tipo *misuse* si comportano in maniera opposta

Host IDS



- Effettuano un'analisi sulla singola macchina host
- Possono essere configurati differentemente da un host all'altro: si guadagna in termini di precisione
- Non hanno una visione generale del comportamento della rete
- I più diffusi si basano sull'analisi del file system, per individuare modifiche non consentite

Limiti

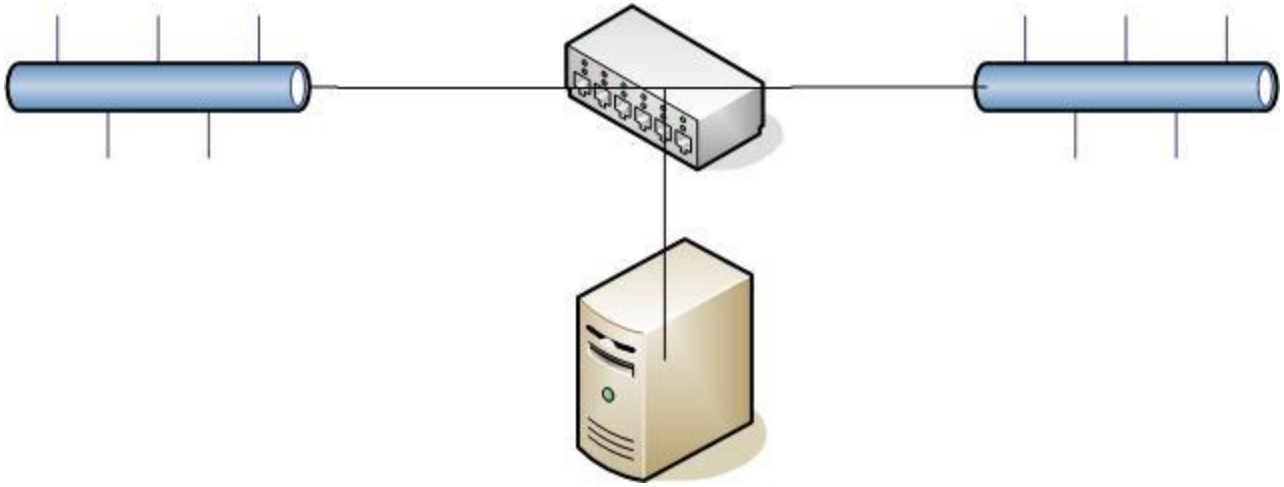
- L'IDS non può essere installato con Firewall perché deve essere "nascosto"
- Sarebbe meglio installare vari sensori IDS in diversi punti della rete per raccogliere un'informazione completa

- *Progettare strategie di inserzione sfruttando pregi di entrambi (IDS e Firewall), segmentare prevedendo autenticazione, unificare motori di scansione multipla in una sola box.*

… altri limiti

- *Il **tempo** tra l'identificazione di un nuovo tipo di attacco e l'aggiornamento del database rappresenta una situazione molto pericolosa. In questo intervallo di tempo l'IDS signature-based non può identificare l'attacco.*
- *I diversi **errori e bug dei software** possono creare pacchetti corrotti e attivare falsi positivi*
- *Errori dovuti a **debolezze nel processo di autenticazione** o debolezze dei **protocolli** usati non vengono considerati anomalie. L'IDS considera il traffico normale se grazie a una debolezza qualsiasi un attaccante riesce ad autenticarsi alla rete con tutti i privilegi a lui assegnati.*
- *Un IDS **non analizza pacchetti criptati**.*
- *Alcuni IDS tengono in considerazione l'indirizzo sorgente del pacchetto nel processo di analisi. Se l'indirizzo nel pacchetto non è quello effettivo del mittente ,vedi IP spoofing,si potrebbero avere dei **falsi negativi** (che **sono situazioni pericolose**)*
- *È molto difficile definire la baseline della rete (cioè la situazione considerata normale) se l'IDS è anomaly-based. questo potrebbe creare tanti falsi positivi (meno pericolo) o falsi negati (situazioni da evitare)*

Network IDS



Effettuano un’analisi sul traffico di rete, alla ricerca di pattern relativi ad azioni dannose

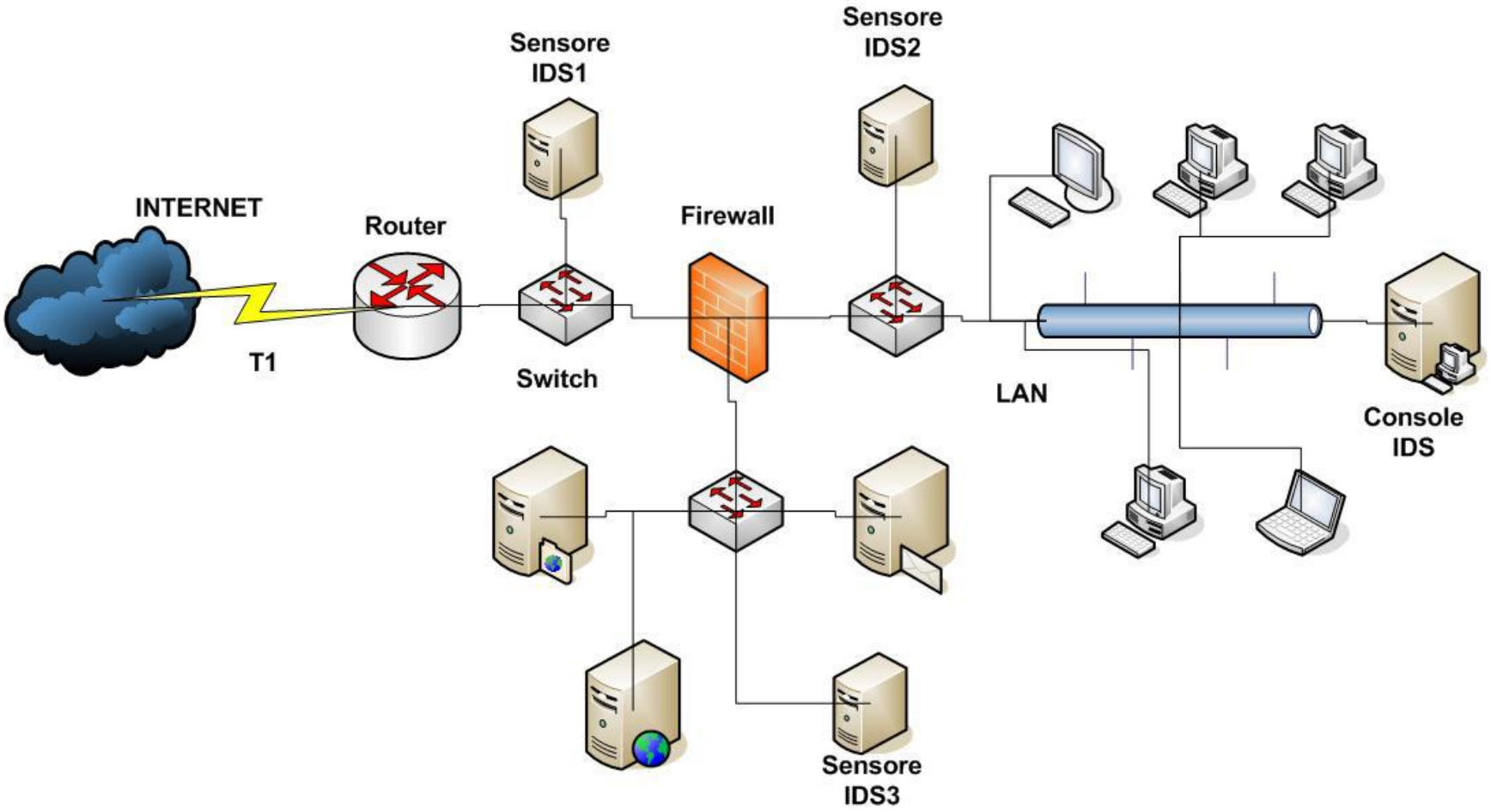
- Si installano sensori:
  - Nascosti
  - In modalità promiscua
  - Con raccolta ed analisi centralizzate

Differenza tra IDS e FIREWALL

- *A differenza del firewall che ,con una Lista di controllo degli accessi, definisce un insieme di regole che i pacchetti devono rispettare per entrare o per uscire dalla rete locale,un IDS controlla lo stato dei pacchetti che girano all'interno della rete locale* ***confrontandolo con situazioni pericolose già successe*** *prima o con* ***situazioni di anomalia definita dall'amministratore di sistema.***
- *Un firewall può bloccare un pacchetto ma un IDS agisce in modo* ***passivo*** *cioè quando rileva la presenza di una anomalia genera un allarme senza però bloccarla.*
- *L'IDS agisce anche al* ***livello del singolo Host*** *facendo 2 snapshots successivi del sistema e confrontandoli per evidenziare situazioni di anomalia (per es aumento di privilegi dei file,un utente semplice diventa amministratore o un file system è stato cambiato)*
- *Se un attacco è stato originato* ***all'interno della rete locale****, LAN, il firewall non può fare niente solo l'IDS può, analizzando la rete,scoprire situazioni di anomalia.*
- *l'IDS (da solo) o il firewall (da solo) non possono garantire la sicurezza del sistema.*

Bisogna combinarli entrambi per poter aumentare il livello di sicurezza in una rete sapendo sempre che la sicurezza non è un prodotto ma un processo in continua miglioramento

Strategie di inserzione



Strategie di inserzione

- A monte del firewall: analizzano tutto il traffico, compresi gli attacchi diretti al firewall
- Nella DMZ: rilevano gli attacchi ai servizi installati
- Nella LAN: analizzano il traffico interno

Tecnologia per l’inserzione

TAP

BALANCER

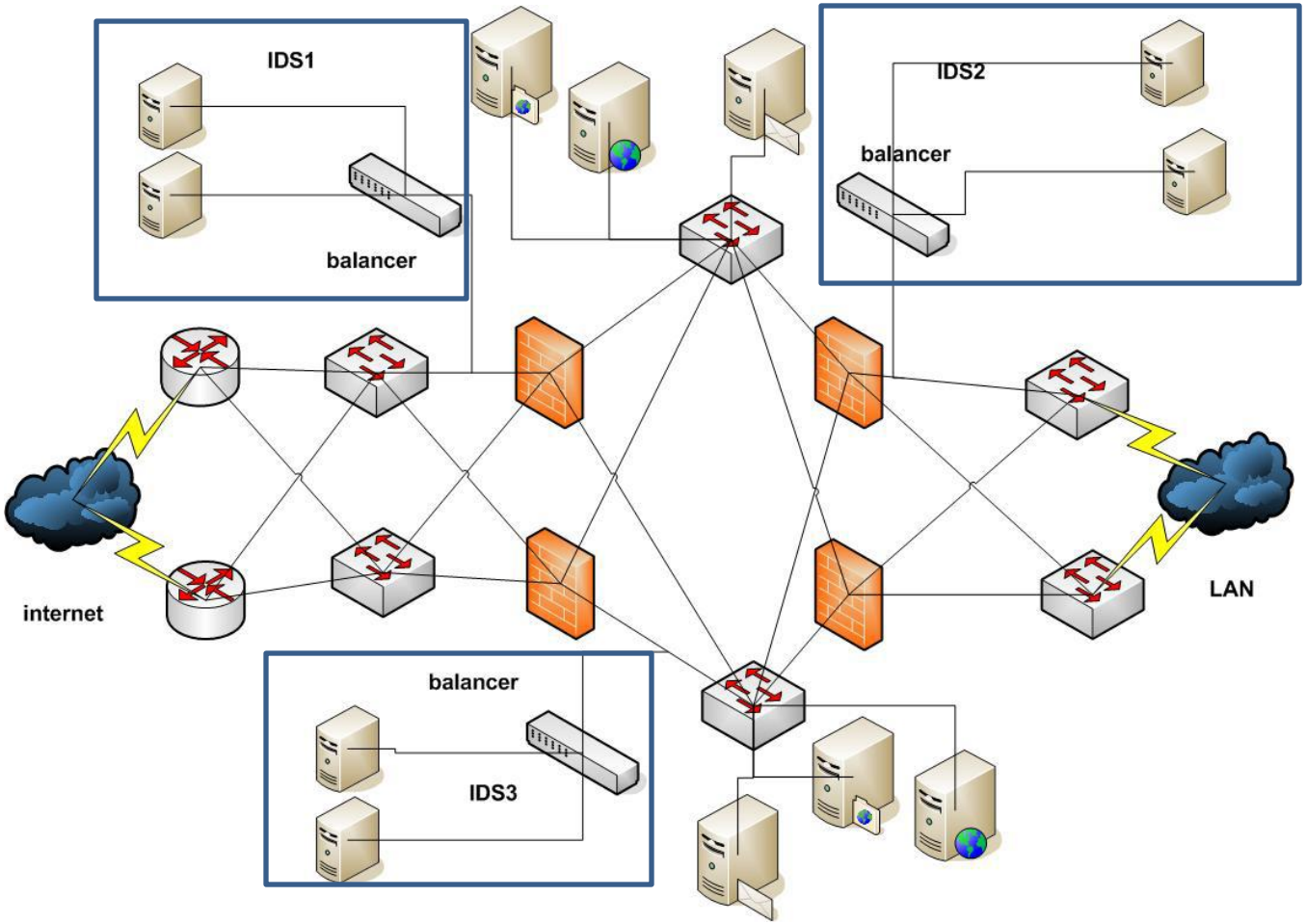
TAP hanno 4 porte:

– Una di input
– La replica dell’input
– Una di output
– La replica dell’output

BALANCER

– Bilanciano il traffico sulle porte
– Si evita che i sensori perdano pacchetti catturati in ingresso

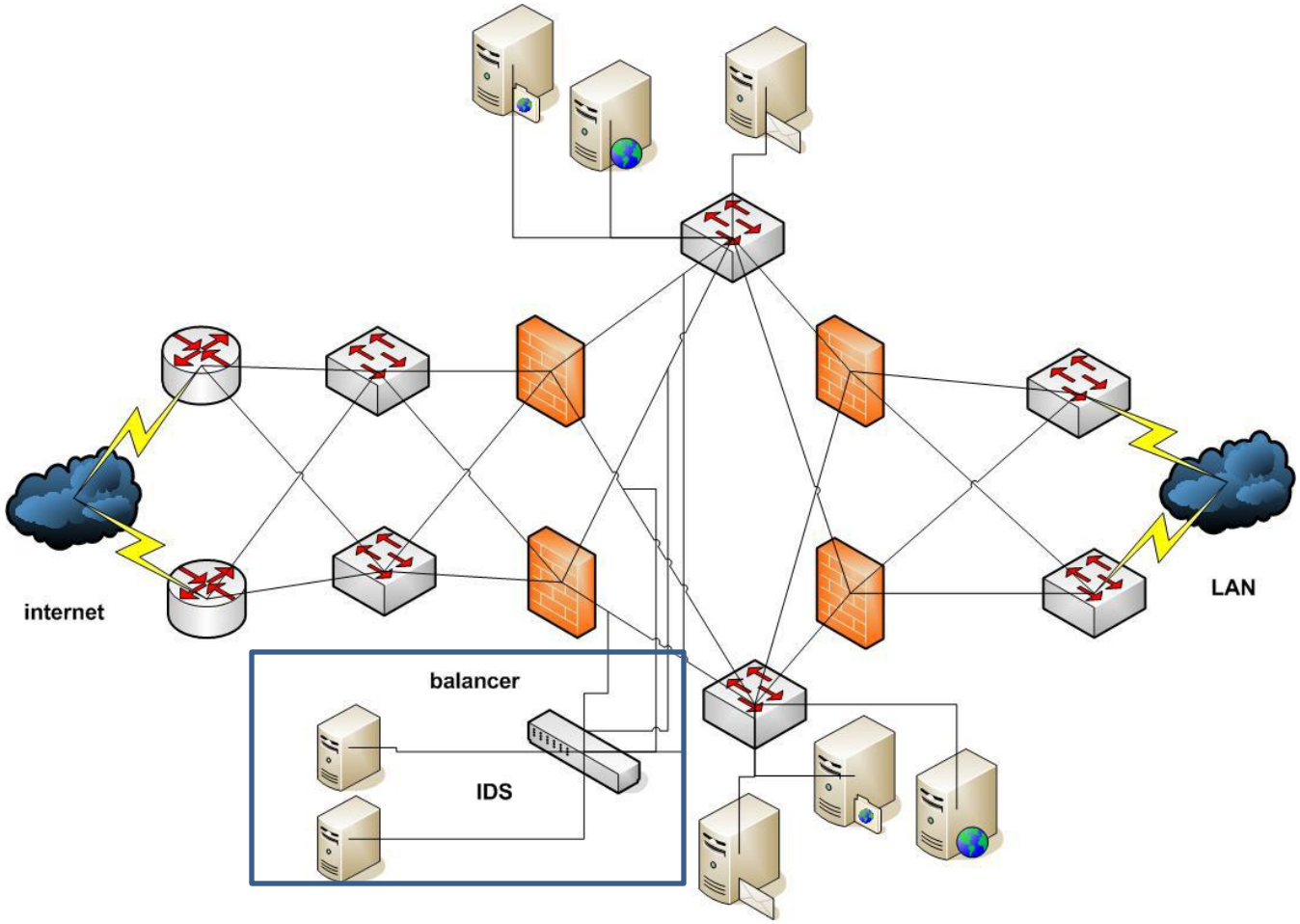
Implementazione di un sistema di rilevamento delle intrusioni per reti



Problema: costi elevati

- Una soluzione di questo tipo comporta costi molto elevati:
  - 3 balancer
  - 6 sensori
  - 12 tap
- Si potrebbe pensare di utilizzare in tutto o in parte prodotti ***open source***

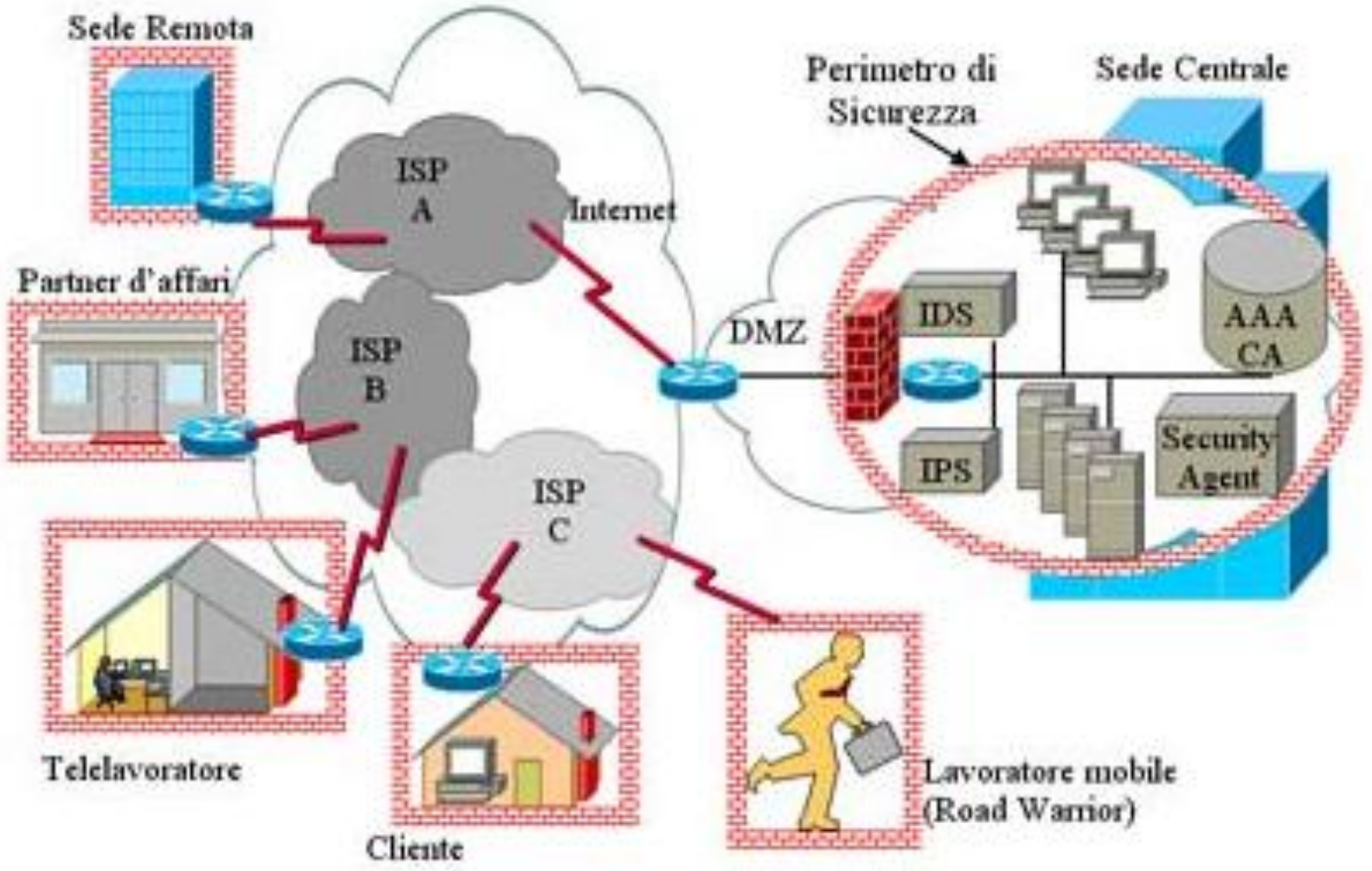
Implementazione di un sistema di rilevamento delle intrusioni per reti: *ridotto*



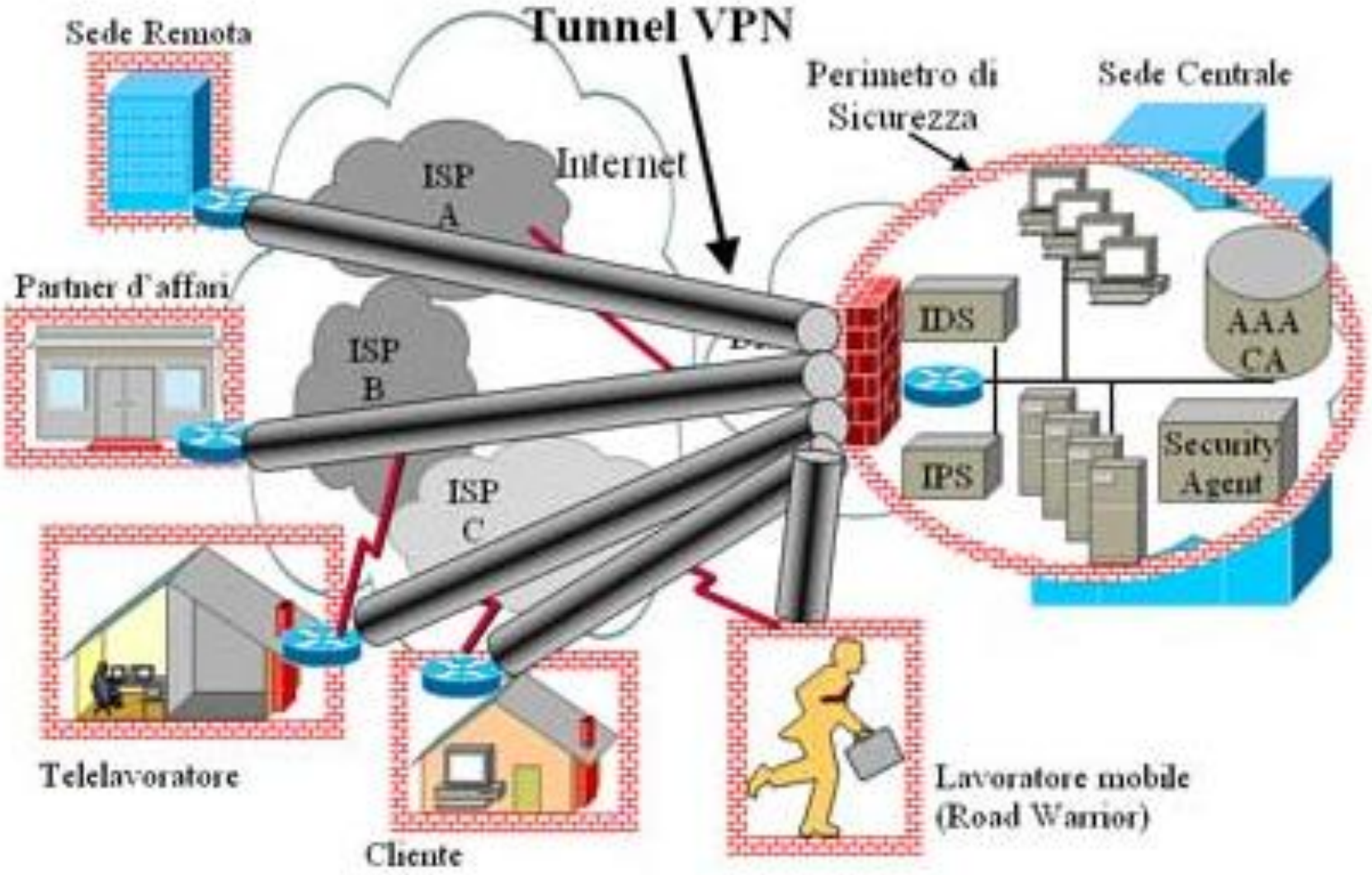
Intrusion Prevention System

- Gli IPS sono sistemi **reattivi** che agiscono nella fase di prevenzione degli attacchi
- Analizzano il traffico, come gli IDS, ma hanno la **possibilità di filtrare pacchetti**, come i firewall
- Problema: DoS indotto da un attaccante mediante *spoofing* di indirizzi consentiti
- Soluzione: blocco dinamico delle connessioni, filtri che agiscono sul singolo pacchetto

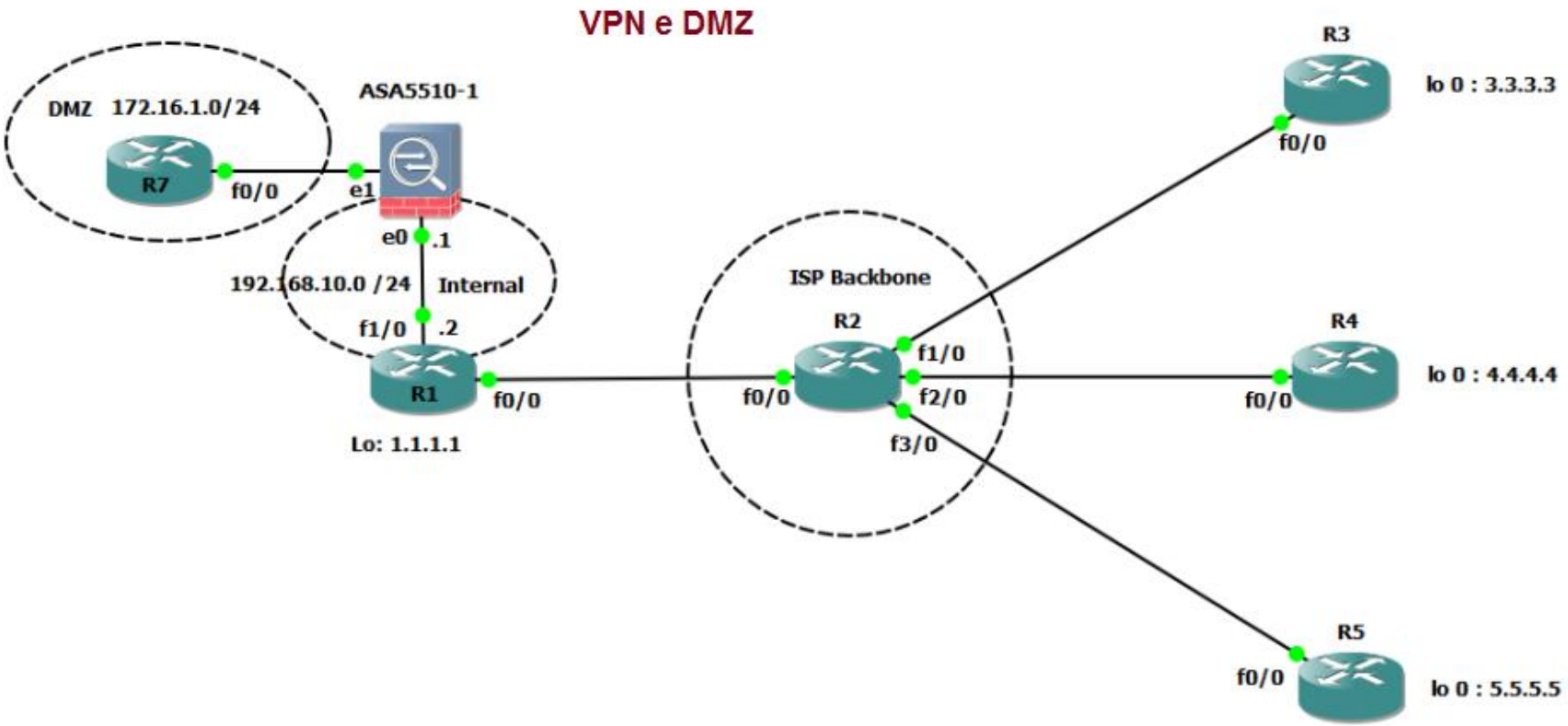
Scenario senza Virtual Private Network



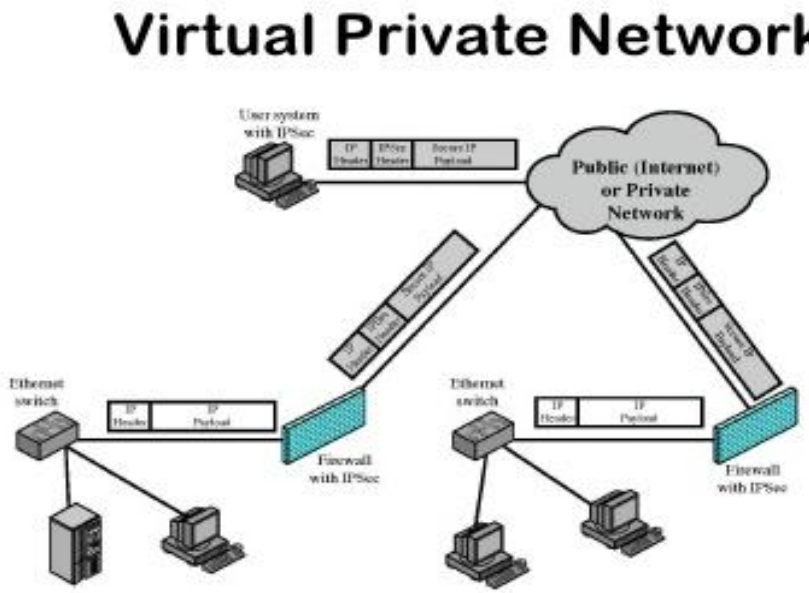
Scenario con VPN

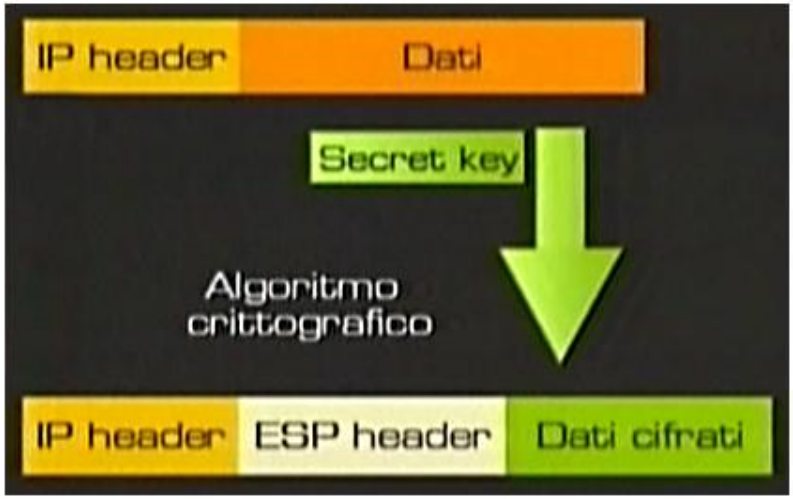


Virtual Private Network



Secure VPN: crittografia e tunneling





Analisi dei messaggi di log

- Quando si hanno diversi sensori, l'analisi dei messaggi di log diventa una procedura dispendiosa
- Si può utilizzare un sistema di raccolta ed analisi centralizzato
- Ad esempio, esistono console che forniscono strumenti per una lettura più agevole

Correlazione degli allarmi

- Altri allarmi e messaggi di log vengono prodotti da:
  - Sistema operativo
  - Altri strumenti di sicurezza
  - Applicativi
- Messaggi di log con livello di dettaglio differente e raccolti in punti differenti della rete
- Si può pensare di correlare i messaggi di log per avere una visione più generale e comunque completa

Correlazione degli allarmi

Ad esempio si possono correlare gli allarmi in base:

- Al ***timestamp***: allarmi relativi ad eventi avvenuti in istanti di tempo vicini
- Agli ***indirizzi IP*** sorgente e/o destinazione: allarmi relativi ad eventi generati dalla stessa sorgente e/o diretti alla stessa destinazione
- Al ***tipo di messaggio***: allarmi relativi ad eventi dello stesso tipo

Backup

Le copie di backup possono essere utilizzate sia per risolvere problemi di sicurezza, sia per risolvere problemi di crash hw

- Servono:
  - Politiche di backup
  - Supporti hw
  - Utility sw

Bisogna stabilire:

– Quali sono i dati sensibili e dove si trovano
– La frequenza con cui si vogliono effettuare i backup
– Quando devono essere effettuati i backup e chi è responsabile di farlo
– Il tipo di backup
– Come vengono gestite le copie

Esempi

Dati sensibili: dati privati di clienti e personale, dati necessari per i vari processi, altri dati utili al sistema informativo

- Si potrebbero effettuare backup in automatico, di notte
- Si potrebbero effettuare backup di sistemi ad intervalli di qualche settimana o un mese e backup incrementali o differenziali ogni settimana o quotidianamente (per i dati molto sensibili)

Supporti hw ed utility sw

- Si possono utilizzare CD o DVD, hard disk o dischi RAID
- Ci sono anche hw dedicati
- Esistono varie utility di supporto che forniscono:
  - Un'interfaccia friendly
  - Strumenti per l'esecuzione automatica
  - La scelta dei vari tipi di backup da effettuare

Consigli

- È utile conservarsi più copie effettuate in date differenti
- Si consiglia di separare il backup dei dati da quelli del sistema per gestirli separatamente
- Effettuare periodicamente copie del sistema su supporti non modificabili
- Fare attenzione alle copie per evitare di smarrirle o danneggiarle

Sistemi di **backup** locale e remoto

Risposta agli incidenti informatici

La risposta agli incidenti è composta da:

- ***Analisi delle informazioni*** che vengono dalla fase di ***rilevamento*** (completate con altre raccolte al momento)
- ***Intervento*** per ***evitare*** o ***ridurre al minimo*** i ***danni***
- ***Configurazione dei sistemi*** per ***eliminare*** le ***vulnerabilità***
- ***Ripristino*** del ***normale funzionamento***

Direzione futura

La tendenza attuale è quella di avere strumenti di analisi anche complessi

- Aiutano ad analizzare grandi moli di dati che riguardano l'attività

"Il peggior nemico della sicurezza è la complessità"

L'evoluzione potrebbe essere un sistema che produce dei piani di soluzione, **dopo** aver riconosciuto il tipo di incidente

- Sistemi di questo tipo potrebbero essere di supporto ai security manager

Fonti

- http://www.di.unisa.it/~ads/corso-security/www/CORSO-0203/Firewall2003/
- http://www.wikipedia.org/wiki/Firewall
- http://www.zerounoweb.it/static/upload/201/0121/2016-ossforti-internal-segmentation-firewall.pdf
- http://www.clubticentro.it/wp-content/uploads/2009/09/CAPUZZI-architetture_e_strumenti_per_la_sicurezza.pdf