Sicurezza dellet reti

La sicurezza delle reti andrebbe introdotta a tutti i livelli dello stack TCP/IP.

Il paradigma di riferimento segue la metodologia defense in depth, in cui vengono applicate le regole di **segmentazione** e **segregazione**

* Segmentazion: partizionare le risorse aziendali
  + Logiche e fisiche
  + Suddividere le reti in sottoreti, evitare share di rete aperti
* Segregazione: applicare controllo degli accessi
  + Definire politiche di accesso cross-segment
  + Applicare le politiche mediante opportune tecnologie

Segmentare e segregare il traffico:

* VLAN
* NAT e PAT
* Firewall
* DMZ

# Virtual Lan (VLAN)

Lan tradizionale

Gli host sono aggregati "fisicamente" mediante dispositivi di rete, quali hub, switch, e router:

* Hub: non differenziano il dominio di collisione né il dominio di broadcast
* Switch: differenziano il dominio di collisione ma non il dominio di broadcast
* Router: differenziano sia il dominio di collisione sia il dominio di broadcast

Problemi delle LAN

Non è detto che host che sono aggregati a livello fisico debbano avere anche la possibilità di condividere le stesse informazioni.

Inoltre, bisogna considerare che un numero cospicuo di dipendenti si sposta ogni anno (di ufficio, di ruolo, ecc).

Ri-cablaggio, ri-indirizzamento, e riconfigurazione sono operazioni molto costose!

VLAN

Mediante VLAN, gli host possono essere raggruppati "logicamente" in base al dipartimento di appartenenza, al tipo di applicazioni, alle funzioni, al livello di riservatezza, ecc.

* Gli host che si trovano all'interno di una VLAN possono comunicare direttamente
* Gli host che si trovano in VLAN differenti possono comunicare mediante l'intermediazione di un dispositivo di rete (router)

Una VLAN segmenta logicamente gli host in sottoreti differenti (domini di broadcast).Ciascuna VLAN è realizzata mediante porte di switching private: i frame di broadcast sono distribuiti solo all'interno della stessa VLAN.

Realizzazione VLAN:

* host possono essere aggregati in VLAN tramite soluzioni software
* è possibile realizzare VLAN mediante configurazione statica o dinamica

Tecniche di realizzazione:

* **Frame filtering**:
  + Il bridge mantiene tabelle di filtering e implementa algoritmi di filtering e di learning esaminando le informazioni di ciascun frame
  + Il router mantiene tabelle di routing e implementa algoritmi di routing
* **Frame tagging**:
  + Si inserisce un identificatore unico nell'header di ogni frame (subito dopo gli indirizzi MAC sorgente e destinazione) quando è inoltrato sulla dorsale della rete

NATting e PATting

Poiché per molte organizzazioni non è necessario che tutti i loro indirizzi siano visibili globalmente. Gli indirizzi **non routable** si possono utilizzare senza chiedere autorizzazione, purché si garantisca che il traffico e gli indirizzi siano limitati alla rete interna.

In questo modo un'organizzazione tipicamente ha la possibilità di progettare una rete che include:

* Host pubblici visibili da internet
* Host privati NON visibili da internet

Gli host privati possono comunicare solo con host privati oppure con host pubblici attraverso:

* Proxy su host pubblici
* NAT

NAT Router

Il **NAT router** (un router con funzionalità di NATting) si interpone tra la rete locale di una organizzazione e Internet:

* Mappa gli indirizzi IP tra due domini
* Garantisce la trasparenza del routing tra gli end system
* Aumenta la sicurezza evitando di rendere visibili all'esterno alcuni computer di una organizzazione

Il **NAT router** svolge due funzioni: NATting e switching.

Port Address Translation

In una versione del NATting è prevista anche la possibilità di "tradurre" non solo l'indirizzo IP sorgente ma anche la porta sorgente (PAT). Molte operazioni di NAT sono in realtà operazioni PAT.

Si gestisce una corrispondenza (binding) tra i due domini tramite una tabella di stato con le corrispondenze tra gli indirizzi e le porte:

* **Binding statico**: la tabella viene configurata manualmente
* **Binding dinamico**: la tabella viene calcolata dinamicamente
  + Cambia nel tempo a seconda del traffico
  + I numeri di porta degli host interni vengono mappati in numeri di porta presi da un pool del PAT router
  + La dimensione del pool determina il numero massimo di connessioni contemporanee a Internet

Firewall

Il **Firewall** è un dispositivo di sicurezza che si interpone tra due reti diverse per controllare e limitare il traffico.

Principi del Firewall:

* Il Firewall deve essere l'unico punto di contatto tra la rete esterna e la rete interna
* Solo il traffico autorizzato o non vietato deve riuscire ad attraversare il firewall
* Il firewall deve essere, a sua volta, un sistema sicuro e tenuto sempre sotto controllo

Politiche per la sicurezza della rete

Le politiche si definiscono mediante Accesso Control List (ACL):

* Quali servizi devono essere esplicitamente consentiti o proibiti
* Come devono essere utilizzati
* Eventuali accezioni alle regole

Due regole contrapposte:

* **Negazione implicita**: solo il traffico esplicitamente autorizzato può attraversare il firewall. Tutto il traffico non esplicitamente autorizzato viene bloccato. Favorisce la sicurezza rispetto all'usabilità
* **Accesso implicito**: solo il traffico esplicitamente vietato viene bloccato dal firewall. Tutto il traffico non vietato esplicitamente può attraversare il firewall. Favorisce l'usabilità rispetto alla sicurezza.

Classificazione e fuzionalità dei firewall

* **Livello di esecuzione**:
  + Kernel level: controlli a livello 3 e 4
  + User space level: controlli a livello applicazione
* **Ambito di azione**:
  + Personale
  + Aziendale
* **Realizzazione**:
  + Hardware
  + Software

Si possono identificare due tipologie principali di firewall:

* **Packet Filter**: agisce a livello 3 e a livello 4 dello stack TCP/IP; bloccano o lasciano passare il traffico che attraversa il firewall definendo i protocolli, gli indirizzi IP e le porte che si possono o non possono utilizzare. Spesso viene completato da funzionalità di routing (**router firewall**) per permettere l'instradamento dei pacchetti.
* **Application Gateway** (o **Proxy Firewall**): composto da un insieme di proxy che esaminano il contenuto dei pacchetti a livello applicazione. Un **proxy** è un’applicazione di rete che agisce da intermediario tra client e server.
  + - Modifica una sessione tra due parti (client/server) in due sessioni distinte (client/proxy e proxy/server)
    - È necessario che sia lanciato un processo proxy per ogni applicazione che si vuol far esaminare dal firewall
    - Tutto il traffico della rete deve attraversare il firewall per poter funzionare in ingresso ed in uscita alla rete

Packet filter: tecniche di filtraggio

* **Static packet filtering**: considera i singoli pacchetti come entità individuali, non correlati tra loro.
  + Basso costo computazionale ed economico
  + Non richiede il mantenimento di informazioni di stato
  + Semplice da implementare e gestire
  + Ottima scalabilità
  + Non è in grado di riconoscere pacchetti appartenenti ad una connessione già aperta
  + Non è in grado di riconoscere pacchetti correlati ad una connessione già aperta
  + Vulnerabile a tecniche elementari di firewalking (ottenere informazioni sugli host della rete mediante l'invio di pacchetti ad-hoc)
* **Stateful packet filtering**: Capace di esaminare i gruppi di pacchetti correlati tra loro. Analizza gli header di livello 3 e 4, non analizza header/payload a livello applicazione.
  + Riconosce pacchetti appartenenti ad una connessione già aperta
  + Le risposte provenienti dall'esterno a connessioni legittime vengono autorizzate da regole temporanee
  + Le regole temporanee sono attive solo per il tempo strettamente necessario
  + Più resistente a firewalking
  + Richiede maggiori quantità di memoria per mantenere informazioni relative alle connessioni
  + Richiede maggiore capacità computazionale

Application Gateway: tipologie

* **Proxy Firewall**: I pacchetti devono essere indirizzati espressamente al proxy prima di poter essere inoltrati al destinatario.
  + Consente l'analisi completa del protocollo applicativo, a differenza del firewall packet filtering che permette l'analisi fino al livello 4
  + Meno performante del packet filtering
  + Non consente connessioni dirette verso host esterni
  + I client devono essere appositamente configurati per contattare il proxy firewall
  + Richiede supporto esplicito per tutti i protocolli applicativi
* **Transparent Proxy**:Versione migliorata del Proxy Firewall. In questa implementazione il proxy è "trasparente" ai client, che non richiedono configurazioni particolari. Il traffico viene "automaticamente" dirottato verso il proxy server mediante tecniche di NATting