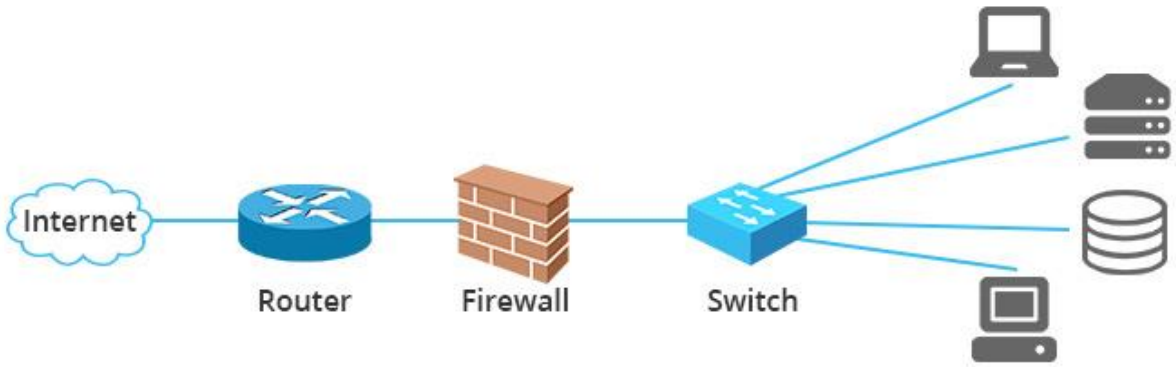
SICUREZZA IN AZIENDA

Router Switch Firewall

La sicurezza in un'azienda è una priorità importante, e l'uso di router, firewall e switch può contribuire in modo significativo a garantire un ambiente di rete sicuro. Questi strumenti sono componenti chiave di una rete aziendale e svolgono funzioni diverse ma complementari per garantire la sicurezza e la connettività affidabile.



ROUTER (INSTRADATORE)

I router possono fornire connettività indipendente da Internet tra edifici di aziende collocati in diverse aree geografiche, o tra le aziende e Internet, o tra le reti dei fornitori di servizi internet.

Un router è un dispositivo di rete utilizzato per instradare il traffico dati tra dispositivi all'interno di una rete locale o tra reti diverse. Svolge funzioni cruciali per il funzionamento delle reti informatiche, locali e in particolare per l'Internet.
In generale i router, in quanto sistemi embedded, hanno il loro sistema operativo e necessitano di essere configurati manualmente da parte dell'amministratore di rete (specifica delle interfacce di rete, abilitazione protocolli e servizi, scheduling del traffico per qualità di servizio) non essendo dispositivi plug and play. A seconda della tipologia del router, per essere configurato esso fornisce un'interfaccia basata su web (accessibile digitando l'indirizzo del gateway nel browser) o attraverso un'apposita console a riga di comando su porta seriale (è il caso ad esempio dei router Cisco Systems, con sistema operativo IOS, e dei router Juniper Networks). Tipicamente questi sistemi sono configurabili da remoto tramite terminale ed inoltre è possibile definire una lista di controllo degli accessi.
I dati trasmessi attraverso una rete, come ad esempio le pagine web o la posta elettronica, viaggiano sotto forma di pacchetti. Il router ha lo scopo di dirigere il traffico di tali pacchetti nel loro tragitto, sia che esso debba attraversare differenti reti locali private, o la rete Internet globale. Un pacchetto viene tipicamente inoltrato da un router a un altro router attraverso le reti che costituiscono un internetwork, come ad esempio Internet, fino a quando non raggiunge il nodo di destinazione.

Un router degno di questo nome deve essere in grado di gestire almeno 2 linee di dati provenienti da reti IP. Quando un pacchetto dati arriva su una delle linee, il router legge l'Indirizzo IP presente all'interno dell'intestazione del pacchetto per determinare quale sarà la sua destinazione finale. In seguito, confronta

questa informazione con il contenuto della propria tabella di routing e inoltra il pacchetto attraverso la successiva rete, quindi la destinazione.
Un router può essere equipaggiato con vari tipi di connessioni di livello fisico, come ad esempio cavi di rame, fibra ottica, o antenne per la trasmissione radio. Può altresì supportare diversi standard di trasmissione appartenenti al livello di rete. Ciascuna interfaccia di rete viene utilizzata per permettere ai pacchetti di essere instradati da un sistema di trasmissione all'altro. I router possono anche essere utilizzati per connettere due o più sottoreti, gruppi logici di dispositivi di rete ciascuno con un differente prefisso di rete.
Nelle aziende è possibile trovare router di tutte le dimensioni. I router più potenti si trovano solitamente presso le sale macchine degli ISP e negli edifici universitari e della ricerca. Anche le grandi aziende hanno bisogno di router potenti per tenere testa alle richieste sempre più crescenti di traffico intranet.
I router si possono distinguere in base alla rete sulla quale operano. Un router in una Rete Locale (LAN) di una singola organizzazione viene chiamato interior router. Un router che opera su una tratta del provider o su una dorsale di internet viene chiamato exterior router. Quando un router mette in comunicazione una LAN con Internet o con una rete geografica (WAN) viene chiamato border router, o gateway.

Le funzioni principali di un router in dettaglio:

Instradamento dei dati: Un router determina il percorso ottimale per inviare i dati da una sorgente a una destinazione. Questo processo coinvolge l'analisi degli indirizzi IP dei pacchetti di dati e la decisione su quale interfaccia di rete inviarli.
Condivisione della connessione Internet: Spesso, un router è utilizzato per condividere una singola connessione Internet con più dispositivi all'interno di una rete domestica o aziendale.
Utilizzando la tecnologia **(NAT) Network Address Translation**, il router assegna indirizzi IP interni ai dispositivi e gestisce le richieste in uscita e in ingresso per consentire loro di accedere a Internet eseguendo la traduzione degli indirizzi IP privati interni in un unico indirizzo IP pubblico.
NAT (Network Address Translation): I router spesso eseguono la traduzione degli indirizzi IP privati interni in un unico indirizzo IP pubblico, consentendo a più dispositivi interni di condividere una singola connessione Internet.
Sicurezza: I router forniscono una barriera di sicurezza tra una rete locale e Internet. Spesso includono firewall hardware che possono filtrare il traffico indesiderato o pericoloso e proteggere la rete da attacchi esterni.
Gestione del traffico: I router possono essere configurati per prioritizzare o limitare il traffico di rete in base alle esigenze dell'utente. Questo è utile per garantire una distribuzione equa della larghezza di banda o per garantire che determinate applicazioni o dispositivi abbiano priorità nell'utilizzo della connessione.
Connettività wireless: Molti router moderni includono funzionalità di connettività wireless (Wi-Fi), consentendo a dispositivi come computer, smartphone e tablet di connettersi senza fili alla rete.
Creazione di reti locali (LAN): Un router può suddividere una rete in segmenti più piccoli noti come LAN, consentendo la comunicazione tra dispositivi all'interno di ciascun segmento e instradando i dati tra di essi, se necessario.
VPN (Virtual Private Network): Alcuni router supportano la creazione di reti private virtuali per consentire agli utenti di accedere in modo sicuro a risorse di rete da remoto.
In sintesi, un router è un componente fondamentale per la connettività di rete e svolge un ruolo chiave nell'instradamento dei dati, nella condivisione di connessioni Internet, nella sicurezza della rete e in molte altre funzioni relative alla gestione delle comunicazioni tra dispositivi all'interno e all'esterno di una rete.

Firewall: Alcuni router incorporano funzionalità di firewall per filtrare e bloccare il traffico dannoso o non autorizzato tra le reti.

In sintesi, un router è un componente fondamentale per la connettività di rete e svolge un ruolo chiave nell'instradamento dei dati, nella condivisione di connessioni Internet, nella sicurezza della rete e in molte altre funzioni relative alla gestione delle comunicazioni tra dispositivi all'interno e all'esterno di una rete.

SWITCH (COMMUTATORE)

Lo switch di rete, noto semplicemente come "switch," è un dispositivo hardware utilizzato nelle reti informatiche per collegare dispositivi insieme e facilitare la comunicazione tra di essi. La funzione principale è quella di instradare i pacchetti di dati all'interno di una rete locale (Local Area Network, LAN) operando a livello 2 del modello OSI (Data Link Layer) e utilizzando gli indirizzi MAC (Media Access Control) dei dispositivi collegati.
Gli Switch possono essere gestiti con una interfaccia (CLI) riga di comando e accessibile tramite console seriale: telnet o Secure Shell, un agente SNMP (Simple Network Management Protocol) incorporato che consente la gestione da una console remota o una stazione di gestione o un'interfaccia Web per la gestione da un browser web.
Switch non gestiti: non hanno un'interfaccia di configurazione o opzioni. Sono plug and play. Sono in genere gli switch utilizzati in un piccolo ufficio e possono essere montati su desktop o su rack.

Lo switch agisce sull'indirizzamento e sull'instradamento all'interno delle reti LAN mediante indirizzo fisico (MAC), selezionando i frame ricevuti e dirigendoli verso il dispositivo corretto (leggendo il MAC di destinazione). L'instradamento avviene per mezzo di una corrispondenza univoca porta-indirizzo.
Lo switch ha un comportamento analogo a quello del bridge, mentre si differenzia dal router che opera a livello 3 (internetworking), mettendo in comunicazione più reti locali attraverso il protocollo IP, e dall'hub che invece è solamente un ripetitore multiporta di strato fisico ovvero diffusivo senza indirizzamento. L'instradamento attraverso switch è in grado di ridurre il dominio di collisione presente nelle reti locali broadcast in maniera più efficiente ed efficace rispetto al bridge.

Livello 1: Un hub di rete, o un ripetitore, è un semplice dispositivo di rete che non gestisce il traffico che lo attraversa.
Livello 2: Un bridge, che opera a livello di collegamento dati, può interconnettere un piccolo numero di dispositivi in una casa o in ufficio.
Livello 3: uno switch di livello 3 può eseguire alcune o tutte le funzioni normalmente eseguite da un router e può aumentare l'efficienza del traffico.
Livello 4: uno switch di questo livello capacità di traduzione degli indirizzi di rete, ma aggiunge un tipo di distribuzione del carico basato sulle sessioni TCP.[6] Funzioni quali QoS e ACL (quest'ultima disponibile anche per livelli inferiori) permettono ad esempio di dare priorità diverse o bloccare pacchetti con contenuti particolari, specificabili nella programmazione dello switch.
Livello 7: Gli switch di livello 7 possono distribuire il carico in base a localizzatori di risorse uniformi (URL) o utilizzando una tecnica specifica dell'installazione per riconoscere le transazioni a livello di applicazione.

Caratteristiche e funzioni chiave degli switch di rete:

Connessione dei Dispositivi: Gli switch sono utilizzati per connettere dispositivi all'interno di una rete, come computer, stampanti, telefoni VoIP, telecamere di rete e altro. Ogni porta di uno switch può essere utilizzata per collegare un dispositivo.
Instradamento dei Pacchetti: Gli switch determinano a quale dispositivo inviare un pacchetto di dati in base all'indirizzo MAC del dispositivo di destinazione. Ciò consente una comunicazione diretta tra i dispositivi senza generare traffico inutile sulla rete, quindi un instradamento intelligente.

Alta Larghezza di Banda: Gli switch offrono una larghezza di banda elevata all'interno della rete locale. Ciò significa che le comunicazioni tra dispositivi all'interno della LAN possono avvenire a velocità molto elevate ad esempio 10/100/1000 Mbps (Ethernet) o anche 10 Gbps, 40 Gbps e 100 Gbps (Ethernet ad alta velocità).
Segmentazione di Rete: Gli switch consentono la segmentazione della rete in gruppi logici separati, noti come VLAN (Virtual LAN). Questa funzione può migliorare la sicurezza e l'efficienza della rete, consentendo la separazione di diversi reparti o funzioni aziendali.
Gestione del Traffico: Gli switch gestiscono il traffico in modo efficiente, riducendo il numero di collisioni (contrariamente agli hub, che sono dispositivi meno intelligenti). Ciò consente di migliorare le prestazioni della rete.
Ridondanza di Rete: Molti switch supportano funzionalità di ridondanza di rete, come il trunking e l'aggregazione di link, che garantiscono che la rete rimanga operativa anche in caso di guasto di un collegamento.
PoE (Power over Ethernet): Alcuni switch sono in grado di fornire alimentazione elettrica a dispositivi come telefoni IP e telecamere di rete attraverso i cavi Ethernet, semplificando l'installazione e l'alimentazione di dispositivi di rete.
Gestione Remota: Gli switch più avanzati offrono opzioni di gestione remota tramite protocolli come SNMP (Simple Network Management Protocol), consentendo ai professionisti IT di monitorare e configurare lo switch da remoto.
Qualità del servizio (QoS): Gli switch possono supportare il QoS per assegnare priorità al traffico di rete in base alle esigenze, garantendo una migliore gestione della larghezza di banda per applicazioni critiche come videoconferenze o VoIP

In sintesi, uno switch di rete è un componente fondamentale per la creazione di reti locali efficienti, poiché facilita la connettività dei dispositivi e migliora le prestazioni della comunicazione all'interno della rete.

FIREWALL (MURO DI FUOCO)

Un firewall è un dispositivo hardware o software progettato per proteggere una rete informatica o un sistema da minacce esterne, regolando il traffico di rete in base a regole e criteri di sicurezza definiti. Il suo obiettivo principale è quello di prevenire accessi non autorizzati e proteggere la rete da intrusioni, malware e altre minacce alla sicurezza.
I firewall si dividono in host-based e network-based a seconda della natura del sistema che proteggono.
Un host-based firewall (personal firewall o firewall software), è un'applicazione software che controlla il traffico uscente ed entrante di un singolo computer.
Un network-based firewall (network firewall o firewall hardware), è un componente hardware stand-alone che viene posto sul confine di una rete in modo da filtrare tutto il traffico che questa scambia con l'esterno, per questo viene anche detto firewall perimetrale.

Le funzioni di un firewall e le sue principali funzioni

Filtraggio del Traffico: Il firewall analizza il traffico di rete in arrivo e in uscita, determinando se deve essere consentito o bloccato in base a regole predefinite. Ad esempio, il firewall può bloccare il traffico proveniente da indirizzi IP sospetti o da porte non autorizzate.
NAT (Network Address Translation): Molte reti domestiche e aziendali utilizzano il NAT per nascondere gli indirizzi IP interni. Il firewall può eseguire il NAT, traducendo gli indirizzi IP interni in un indirizzo IP pubblico, consentendo a più dispositivi interni di condividere una singola connessione Internet.

Proxy: I firewall proxy agiscono come intermediari tra gli utenti e i server di destinazione. Gli utenti si connettono al firewall e questo si connette al server di destinazione a nome loro, nascondendo gli indirizzi IP degli utenti.
Ispezione dei Pacchetti: Alcuni firewall avanzati eseguono l'ispezione dei pacchetti, analizzando il contenuto dei pacchetti di dati per rilevare malware, intrusioni o attività sospette. Questa tecnica è conosciuta come firewall stateful o next-generation firewall
Regole di Accesso: I firewall sono configurati con regole di accesso che specificano quali tipi di traffico sono consentiti o bloccati. Queste regole possono essere basate su indirizzi IP, porte, protocolli e altro.
VPN (Virtual Private Network): Alcuni firewall supportano la creazione di tunnel VPN sicuri per consentire a dipendenti o utenti remoti di accedere in modo sicuro alle risorse aziendali attraverso Internet.
Rilevamento delle Minacce: I firewall possono essere integrati con sistemi di rilevamento delle minacce (IDS/IPS) per rilevare attività sospette o minacce alla sicurezza e intraprendere azioni appropriate.
Logging e Monitoraggio: I firewall tengono registri di tutte le attività di rete, che possono essere utilizzati per l'analisi dei problemi e l'investigazione di violazioni della sicurezza.

I firewall sono una componente critica nella difesa della sicurezza informatica e vengono utilizzati sia a livello di singoli computer che a livello di reti aziendali per proteggere dati sensibili e risorse da minacce esterne e interne. La configurazione e la manutenzione adeguata dei firewall sono essenziali per garantire la sicurezza della rete.

Giovanni Saponaro