VPN

Una VPN è una rete privata creata all’interno di una rete pubblica.

Esistono due principali tipi di VPN:

-Remote access VPN

-Site to site VPN

Una remote access VPN consente ai singoli utenti di stabilire connessioni sicure con la LAN aziendale remota, in questo modo gli utenti collegati possono accedere alle risorse protette come se fossero interni alla rete. Una remote access VPN è particolarmente adatta per i singoli utenti o per aziende con filiali costituite da piccoli uffici.

Una site to site VPN realizza al meglio il concetto di WAN come insieme di LAN. A sua volta ne esistono due tipi, la intranet-based, che si realizza nel momento in cui diventa necessario collegare in un’unica rete privata tante LAN remote e di conseguenza creare una VPN intranet, e la extranet based, che si realizza quando una società vuole unire sotto la stessa rete un cliente o un fornitore con cui ha uno stretto rapporto, permettendo così la condivisione di risorse.

La loro sicurezza è definita da 3 fattori: autenticazione, tunneling e cifratura.

Si definiscie autenticazione dell’identità il processo attraverso il quale un sistema informatico verifica la corretta identità di un altro sistema informatico. Avviene spesso attraverso una procedura di login, una volta completata la procedura si procederà all’accounting, ovvero al salvataggio di ogni azione svolta dall’utente all’interno della rete.

Il termine tunneling si riferisce a un insieme di tecniche per cui un protocollo viene incapsulato in un altro dello stesso livello, è dunque l’immissione di un pacchetto all’interno di un altro pacchetto prima di essere trasportato su internet

Esistono 3 principali tipi di cifratura, ovvero le Trusted VPN, le Secure VPN e le Hybrid VPN. La prima si affida all’ISP, la seconda ai protocolli di sicurezza mentre la terza a entrambi.

Esistono inoltre molti protocolli per la sicurezza delle VPN, tra i quali IPsec, SSL/TLS, BGP/MPLS.

IPsec è composto da tre diversi protocolli, AH (Authentication header, che garantisce l’autenticazione e l’integrità del messaggio), ESP (Encapsulation Security Payload, fornisce autenticazione, confidenzialità e controllo di integrità del messaggio), IKE (Internet Key Exchange, implementa lo scambio delle chiavi per realizzare il flusso crittografato).

Le differenze tra SSL/TLS sono poche ma sono comunque sufficienti a distinguerli come due diversi protocolli. È un semplice protocollo client-server avente lo scopo di autenticare il server da parte del client e opzionalmente anche viceversa per creare un canale cifrato fra i due. Sta sempre al client iniziare una connessione verso il server per essere autenticato.

Con BGP/MPLS si garantisce la separazione del traffico tra i diversi utilizzatori dei servizi, anche se il traffico utilizza la stessa rete. Gli elementi di una VPN sviluppata in questo modo sono 3: il CE (Customer Edge, è il router del sito aziendale che si connette con l’ISP fornitore del servizio VPN BGP/MPLS), il PE (Provider Edge, è il router di accesso della rete dell’ISP cui sono collegati uno o più CE), il PCR (Provider Core Router, dei Labl Switched Router(LSR) che compongono la dorsale dell’ISP.

Sicurezza:

chiave simmetrica e asimmetrica

La chiave simmetrica è il metodo di crittografare più semplice in quanto utilizza una singola chiave sia in fase di codifica che di decodifica. Presenta però alcuni svantaggi:

-la chiave diventa fissa e quindi facilmente individuabile, a scapito della sicurezza

-la chiave potrebbe cambiare per ogni messaggio ed è quindi necessario trasmettere la chiave nuova attraverso un tunnel sicuro, quando invece si potrebbe inviare direttamente il messaggio

-è necessario un elevato numero di chiavi quando il numero dei possibili trasmettitori aumenta.

La crittografia a chiave asimmetrica permette di comunicare senza dover ricorrere a percorsi segreti per trasmettere le chiavi. In questo tipo di crittografia a ogni utente vengono assegnate due chiavi, una pubblica e una privata ma la chiave privata usata per crittografare il messaggio non può essere usata per decrittografarlo, a questo ci penserà infatti l’altra chiave privata dell’altro utente. In questo modo la chiave pubblica può essere disseminata ovunque mentre la privata dovrà essere conservata da suo proprietario.

Gateway e servizi integrati:

proxy, firewall, NAT e DM

Spesso i gateway non si limitano a fornire la funzionalità di base a livello di routing ma integrano altri servizi tra i quali il proxy server, il firewall, il NAT (Network Address Translation) e la DMZ (DeMilitarized Zone).

I proxy sono dei programmi che si interpongono tra un client e un server facendo da tramite. Il loro compito è garantire la connettività ai client a loro collegati ai fini di garantire l’efficienza della rete. Vi sono 4 tipi di proxy:

-NOA (Non Anonymous Proxy), che modificano alcuni header e ne aggiungono altri, mostrano l’indirizzo IP del richiedente.

-ANM (Anonymous Proxy Server), che modificano o aggiungono alcuni header ma non mostrano l’IP del richiedente

-HIA (High Anonymous Proxy), che non modificano gli header e non mostrano l’IP del richiedente.

-Proxy Distorcenti, che trasmettono un IP casuale e modificano o aggiungono header.

Il firewall filtra tutti i pacchetti in entrata e in uscita secondo regole prestabilite che contribuiscono alla sicurezza della rete. Un firewall può essere realizzato ad esempio con un computer con almeno due schede di rete, una per l’input e l’altra per l’output, e un software apposito. È possibile gestire il traffico in base agli indirizzi IP di sorgente/destinazione, protocolli, porte, indirizzi MAC ed è anche possibile filtrare URL e parole chiave.

Il NAT serve a traslare un indirizzo IP in un altro. Viene usato per permettere a una rete locale, che usa indirizzi di classe privata, di accedere a Internet usando un solo indirizzo pubblico fornito dall’ISP. Quando un client richiede una pagina web a un server esterno il suo indirizzo e la sua porta vengono traslati e la corrispondenza viene salvata nella tabella. Tutte le comunicazioni non registrate nella tabella vengono eliminate.

La DMZ è una zona in cui sia il traffico WAN che LAN sono fortemente limitati e controllati. Tale zona viene normalmente utilizzata per permettere ai server posizionati sulla DMZ di fornire servizi all’esterno senza compromettere la sicurezza della rete aziendale interna. Può essere realizzata in due modi:

-vicolo cieco, ovvero un segmento della LAN adibito alla DMZ, di solito quello che ospita i server.

-zona cuscinetto, ovvero una zona con due firewall, uno interno e l’altro esterno.

Le soluzioni cloud

Il cloud computing è un insieme di tecnologie informatiche che permettono l’utilizzo di risorse HW e SW, virtualizzate e distribuite secondo un’architettura client/server. È soprattutto la possibilità di distribuire e consumare servizi di information technology attraverso il web. Il grandissimo pregio di questo tipo di tecnologia è che gli utenti finali possono avere accesso a grandi risorse di qualsiasi tipo in maniera del tutto virtuale, abbattendo quindi i costi delle infrastrutture, l’utente, infatti, pagherà l’uso delle risorse solo all’atto del loro effettivo utilizzo. Esistono tre principali tipi di cloud computing:

-private cloud computing, ovvero un ambiente informatico interno all’azienda

-public cloud computing, ovvero una fornitura di servizi esterno all’azienda

-hybrid cloud computing che permette di sfruttare le risorse e i servizi già presenti nell’azienda e di estendere il proprio data center fino al cloud pubblico.

I principali vantaggi sono:

-investimento iniziale contenuto, dato che la modalità d’uso è a servizio, quindi il costo è a consumo o ad abbonamento.

-disponibilità, significa seguire un andamento dell’attività come quello di attivare o disattivare i servizi in funzione delle reali esigenze, si può ad esempio aumentare il numero di utenze in periodo di picco e diminuirle quando il picco è passato, in modo da non pagare servizi quando non sono necessari.

-scalabilità, questo significa abbattere le barriere per l’IT in modo che tutti possano accedere a risorse sofisticate senza costi iniziali e senza requisiti di conoscenza di una struttura Data Center complessa.

-collaborazione, le soluzioni cloud facilitano le aggregazioni di enti pubblici fornendo opportunità di collaborazione senza precedenti.

-sicurezza, i servizi erogati sono conformi alle politiche di privacy e sicurezza della pubblica Amministrazione.

DHCP

Il DHCP è il protocollo per la configurazione degli host utilizzato nelle reti TCP/IP che permette l’assegnazione dinamica di un indirizzo IP, scelto tra quelli disponibili all’interno di un pool di indirizzi definito su un DHCP server, a un client. La configurazione degli host può avvenire in 3 modi:  
-configurazione manuale: è possibile assegnare un indirizzo specifico, caricato manualmente dall’amministratore sul server, a un determinato server

-configurazione automatica: l’amministratore delega al DHCP server il compito di assegnare un IP permanente a ogni macchina che si collega alla rete

-configurazione dinamica: il DHCP server assegna per un tempo predefinito un indirizzo a una macchina, allo scadere del tempo il client può richiedere il rinnovo dell’indirizzo o l’assegnazione di uno nuovo.

Quando un client viene inizializzato entra nella fase detta INITIALIZE, trasmettendo un messaggio DHCPDISCOVER in broadcast e assume quindi lo stato di SELECT. Tutti i server DHCP nella rete locale ricevono il messaggio e quelli programmati a rispondere a quel tipo di messaggio inviano un messaggio DHCPOFFER. Durante lo stato di SELECT il client raccoglie le risposte DHCPOFFER, ne sceglie una e invia al server un messaggio DHCPREQUEST. A questo punto il client passa allo stato di REQUEST. Per confermare la richiesta e attivare il lease dell’indirizzo il server risponde con il messaggio DHCPACK. L’arrivo della conferma di ricezione fa sì che il client passi allo stato di BOUND, ovvero lo stato di normale funzionamento, si memorizzi i parametri che il server gli ha inviato e imposta 2 timer, uno che indica al client quando è il momento di effettuare una richiesta di rinnovo di utilizzo, l’altro indica al client che è scaduto il tempo per rinnovare l’indirizzo. Nel caso in cui il lease venga disdetto dall’host prima del previsto viene inviato un messaggio di DHCPRELEASE, il client torna allora allo stato di INITIALIZE.

Architettura TCP/IP

Il principale protocollo del livello di rete è sicuramente IP, protocollo che si occupa dell’indirizzamento, suddivisione in pacchetti e del trasferimento dei dati. Il protocollo è connectionless, ovvero consente a due host di scambiarsi pacchetto senza stabilire una sessione. Il protocollo IP fornisce l’inidirizzo logico degli host di una rete TCP/IP. A ciascun host viene assegnato un indirizzo IP univoco rispetto alla rete in cui sta lavorando. Quindi il suo indirizzo IP non rappresenta solo l’host ma anche su quale sottorete si trova, consentendo assieme alla subnet mask l’inoltro dei pacchetti da parte dei router solo quando necessario.

Classi

Gli indirizzi IP sono suddivisi per classi

-classe a: adatti a network di grandi dimensioni con un range da 0.0.0.0 a 127.255.255.255

-classe b: adatti a network di medie dimensioni con un range da 128.0.0.0 a 191.255.255.255

-classe c: adatti a network di piccole dimensioni con un range da 192.0.0.0 a 223.255.255.255

-classe d: servono per il multicasting, ovvero per raggruppare servizi di host con un range da 224.0.0.0 239.255.255.255

-classe e: servono per usi futuri con un range da 240.0.0.0 a 255.255.255.254

Vi sono comunque degli indirizzi di default, come quello di rete (0.0.0.0), quello di broadcasst (255.255.255.255) e quello di loopback (127.0.0.1).

ARP

Un’implementazione TCP/IP di norma usa una cache ARP per memorizzare ogni host attraverso la coppia MAC-IP. Quando un host deve inviare dei pacchetti controlla prima se nella sua cache ARP è presente l’indirizzo, altrimenti l’host deve inviare una ARPrequest in cui specifica l’indirizzo del destinatario di cui vuole conoscere il MAC, questo pacchetto viene inviato in broadcast all’indirizzo FF-FF-FF-FF-FF-FF, inoltre il mittente aggiunge il suo indirizzo IP, affinché il destinatario possa aggiungere la coppia di indirizzi alla sua cache ARP. Quando il destinatario riceve la richiesta, dopo aver riconosciuto che l’indirizzo MAC è il suo, allora risponde con un pacchetto ARPreply, aggiungendo l’indirizzo IP corrispondente al suo MAC. Il mittente, ricevuta la risposta, aggiorna la sua cache ARP e inizia la comunicazione.

Ping e tracert

Per verificare il corretto funzionamento della rete è possibile utilizzare il comando ping per controllare la raggiungibilità di un qualunque indirizzo IP. È utilizzabile principalmente per 3 scopi:

-verificare se il protocollo TCP/IP è configurato correttamente

-verificare se è in funzione il proprio router/gateway

-verificare se un indirizzo internet è raggiungibile.

Un altro comando utile a verificare il funzionamento della rete è tracert. Il comando, seguito da un indirizoz IP o da un hostname di destinazione, visualizza la serie di router IP utilizzati per il recapito del pacchetto dal proprio computer al destinatario e il tempo impiegato per ogni hop.

RIP

Protocollo molto vecchio, la sua metrica è il numero di hop, la più semplice ma anche la meno efficiente. Nella tabella di routing viene memorizzato solo il percorso più breve e non sono consentiti più di 15 hop, non è di conseguenza applicabile in reti con più di 15 router. Il RIP prevede che le tabelle di routing vengano aggiornate ogni 30 secondi, quindi ogni router menda la propria routing table a tutti i vicini direttamente collegati, generando così una grande quantità di traffico.

OSPF

Il protocollo OSPF si fonda sul concetto di area, un’area è costituita da una o più reti contigue. Con questo tipo di organizzazione si hanno due livelli di routing: routing intra-area, quando la sorgente e la destinazione sono nella stessa area, routing extra-area, quando soregente e destinazione non sono nella stessa area. L’area formata dalle reti che non appartengono a nessuna area più i router di confine di ogni area è detta backbone.

Livello transport architettura TCP/IP

il protocollo TCP/IP per comunicare utilizza le porte di comunicazione, poste dopo l’indirizzo IP, identificate da un numero positivo a 16 bit. I numeri di porte sono assegnati da IANA e suddivisi in 3 gruppi: Well-known ports (0-1023), Registered ports (1024-49151) e Dynamic ports (19152-656535). L’host mittente per inviare un messaggio deve conoscere, oltre all’IP, il numero di porta di destinazione all’interno dell’host remoto. Quindi ogni messaggio deve contenere al suo interno:

-destination port: numero della porta di destinazione presente sull’host ricevente

-source port: numero della porta dell’host mittente nella quale è in attesa il processo che riceve le risposte del destinatario.

TCP

È un protocollo molto diffuso data la sua affidabilità e offre un servizio connection oriented. Una connessione TCP ha le seguenti caratteristiche:

-full dulpex, ovvero la stessa connessione può sia ricevere che trasmettere in contemporanea

-point to point, può avere un solo mittente e un solo destinatario

-necessità l’inizializzazione di variabili di stato da parte del mittente e del ricevente.

Le informazioni di controllo che il processo deve passare al TCP comprendono:  
-source address: indirizzo completo del mittente

-destination address: indirizzo completo del destinatario

-next packet sequence number: il numero di sequenza che TCP deve assegnare al prossimo pacchetto che trasmetterà in quella porta

-current buffer size: dimensione buffer del mittente

-next write position: indirizzo dell’area del buffer in cui il processo pone i nuovi dati da trasmettere

-next read position: indirizzo dell’area del buffer da cui TCP deve leggere i dati per costruire il prossimo segmento da inviare

-timeout: indica il tempo trascorso durante il quale i dati non riconosciuti devono essere ritrasmessi

-flag: è usato per sincronizzare TCP e processo, per segnalazioni di stato, ecc

I campi più importanti del segmento TCP sono:

-source port number: numero di porta sull’host del mittente

-destination port number: numero di porta sull’host del destinatario

-sequence number: numero di sequenza progressivo del primo byte di dati contenuti nel segmento

-header lenght: indica la lunghezza dell’header del segmento TCP

-checksum: è usato per la verifica della validità del segmento.

Per avviare la comunicazione tra un client e un server sono necessarie tre fasi:

-set-up della sessione TCP: è la fase in cui client e server si scambiano i dati di impostazione utili al trasferimento successivo delle informazioni

-trasferimento dati: è la fase in cui avviene il trasferimento delle informazioni vere e proprie

-release della sessione TCP: fase di disconnessione tra client e server

FTP

È un protocollo per il trasferimento di file tra un client e un server e utilizza due canali per la comunicazione, un canale serve per l’invio di comandi tra client e server, è sempre aperto in direzione client e utilizza la porta 21, l’altro è utilizzato per l’invio dei dati, è sempre aperto in direzione server e utilizza la porta 20. La connessione tra client e server avviene in due modalità:

-FTP Active Mode: il client si collega da una qualsiasi porta N alla porta 21 del server e si mette in ascolto sulla porta N+1, questo però può causare problemi di sicurezza lato client in quanto il firewall potrebbe bloccare le richieste FTP sulla porta in ascolto

-FTP Passive Mode: il client inizia entrambe le connessioni con il server, sia comandi che dati, eliminando così il problema del firewall

HTTP

È il protocollo che regola lo scambio di messaggi tra il web server e il web client. L’acquisizione di una risorsa da parte del client può essere schematizzata in 4 fasi:

-connessione: il client crea una connessione TCP/IP usando il suo nome di domini o indirizzo IP e il suo numero di porta, normalmente la porta 80

-richiesta: il client invia la richiesta di una risorsa mediante una riga di caratteri ASCII

-risposta: la risposta inviata dal server è un messaggio in HTML nel quale è contenuta la risorsa richiesta (o un messaggio d’errore)

-disconnessione: il server subito dopo aver spedito la risorsa si disconnette.

Protocolli per email

SMTP è un protocollo per l’invio della posta elettronica è progettato per occupare il meno possibile il canale. Ed è per questo che utilizza la codifica ASCII a 7 bit per codificare i caratteri del messaggio. Questo protocollo non permette di richiedere i messaggi di posta elettronica a un server, per fare questo è necessario usare i protocolli POP3 o IMAP4.

Il protocollo POP3 gestisce l’autenticazione tramite username e password, non è tuttavia un metodo sicuro in quanto viaggiano in chiaro sulla rete. Con POP3 per leggere i messaggi è prima necessario scaricarli in locale ed eliminare dunque la mail sul server. Non è possibile visualizzare la stessa mail su due client diversi, in quanto, durante la consultazione, il protocollo blocca la casella postale.

Il protocollo IMAP4 i messaggi rimarranno, invece, comunque sul server e sul client ne verrà scaricata soltanto una copia. È quindi possibile accedere alla propria posta elettronica da più client e ritrovarvi tutte le email, purché tutti gli accessi vengano eseguiti in IMAP4 e mai in POP3.

DNS (domain name system)

È un’applicazione che permette di usare dei nomi per identificare una macchina al posto del suo indirizzo IP. Il DNS è formato da tre componenti principali:

-Domain Name Space: specifica la struttura ad albero dei nomi di dominio

-Name Server: è un processo applicativo che contiene informazioni sullo spazio dei nomi

-Resolver: è un programma che ottiene informazioni dal Name Server

Un DNS deve seguire poi le seguenti regole:

-i nomi dei singoli componenti del cammino non devono superare i 63 caratteri

-un cammino completo non deve superare i 255 caratteri

-i nomi non sono case-sensitive

-ogni dominio controlla i suoi sottodomini, quindi se si vuole creare un sottodominio è necessario il permesso del domino padre

UDP

È un tipo di protocollo che non prevede la connessione tra host e mittente, infatti non si ha alcuna garanzia sulla consegna dei dati trasmessi, in quanto i pacchetti possono prendere strade diverse e non arrivare nell’ordine corretto e quelli persi non vengono ritrasmessi. Presenta comunque dei vantaggi, tra i quali:

-nessun ritardo dovuto alla fase di set-up della connessione

-non mantiene lo stato della connessione, un server può tenere molti più client attivi

-il controllo del livello applicativo è più facile, in mancanza di un controllo della connessione, il mittente non viene mai bloccato