InternetWorking Sistemi e Reti

**PROGRAMMA SVOLTO E ATTIVITÀ DI LABORATORIO**

MODULO 1: [**Il livello Trasporto.**](#_Livello_Trasporto)

**Le funzioni del livello Trasporto.** I compiti del livello Trasporto come livello end-to-end. Le porte. I socket e il canale di comunicazione.

**Il protocollo** [**UDP**](#_TCP_e_UDP)**.** Trama e caratteristiche del protocollo UDP come protocollo di tipo connectionless.

**Il protocollo** [**TCP**](#_TCP_e_UDP)**.** Trama e caratteristiche del protocollo TCP come protocollo di tipo connection-oriented. Apertura della connessione TCP tramite il three-way handshake. Disconnessione TCP.

*Attività di laboratorio:* analisi del traffico di rete con Wireshark.

MODULO 2: [**Il livello Applicazione.**](#_IL_livello_applicazione)

Il protocollo [DHCP](#_DHCP): il protocollo DORA. Il protocollo [DNS](#_DNS) e i nomi di dominio. [Reti Microsoft](#_Reti_Microsoft): modello workgroup e a dominio. I protocolli SMB e LDAP; Active Directory e Domain Controller. Il protocollo [HTTP](#_Il_protocollo_http). [NAT](#_NAT): statico, dinamico e PAT.

*Attività di laboratorio:* utilizzo del simulatore Cisco PacketTracer per creare LAN interconnesse e configurare i servizi di rete.

MODULO 3: [**La sicurezza informatica.**](#_La_Sicurezza_Informatica)

[**Le condizioni per avere sicurezza informatica.**](#_Le_condizioni_per)

Il concetto di sicurezza e le condizioni per avere sicurezza informatica: riservatezza, integrità, disponibilità e autenticità. Le minacce per la sicurezza informatica: malware, phishing, spamming, DoS, corruzione accidentale o volontaria di dati e dispositivi, infedeltà dei dipendenti. Le contromisure: antivirus, backup, UPS, norme comportamentali. Business continuity e disaster recovery.

[**La crittografia simmetrica, asimmetrica e ibrida.**](#_La_crittografia_simmetrica,)

La crittografia come strumento per ottenere riservatezza, autenticazione e firma digitale. Algoritmi di crittografia a chiave simmetrica e a chiave asimmetrica: il certificato digitale. La crittografia ibrida. La firma digitale.

*Attività di laboratorio:* utilizzo del software PGP per riservatezza e firma digitale.

MODULO 4: [**Virtualizzazione e cloud computing.**](#_Virtualizzazione_e_cloud)

**Tipologie di virtualizzazione.** La Full Virtualization e la Paravirtualization. Virtualizzazione su Linux con oVirt.

**Cloud computing.** Cloud di tipo SaaS, PaaS e IaaS.

*Attività di laboratorio:* utilizzo del software oVirt per creare e personalizzare VM.

MODULO 5: [**La sicurezza in rete.**](#_La_sicurezza_in)

[Firewall](#_Firewall): stateless, statefull e deep inspection; il Proxy. ACL: standard ed estese. Il protocollo [SSL/TLS](#_SSL/TLS). Il protocollo IPsec. Terminale remoto: protocollo SSH. Il protocollo HTTPS. Le VPN. Reti trust/DMZ. Il cablaggio strutturato ISO/IEC 11801.

*Attività di laboratorio:* utilizzo del simulatore Cisco PacketTracer per implementare funzionalità di Firewall mediante ACL.

# Livello Trasporto

Il livello trasporto è il quarto livello della pila ISO-OSI e il suo compito è di fornire un canale logico di comunicazione end-to-end.

L’accoppiata IP-Porta si definisce Socket ed identifica un processo all’interno di una macchina.

TCP e UDP

Sono i due protocolli che permettono la trasmissione dei dati in rete.

|  |  |
| --- | --- |
| TCP | UDP |
| Transmission Control Protocol è un protocollo affidabile per lo scambio di flussi di byte: utilizza una il sistema a finestra scorrevole il quale permette la ritrasmissione di un segmento in caso di perdita. Il protocollo crea un canale di comunicazione virtuale tra i dispositivi che partecipano alla comunicazione.  Il TCP utilizza il metodo Three-Way Handshake per stabilire una connessione:   1. Il client invia un pacchetto SYN con una richiesta di connessione 2. Il server che ha porte aperte in ascolto riceve la richiesta e invia al richiedente un SYN/ACK 3. Il client per confermare la ricevuta risposta invia un ACK al server come conferma di inizio comunicazione | User Datagram Protocol è un protocollo connectionless non affidabile senza controlli sulla ricezione o sull’ordine di arrivo. È un protocollo nettamente più veloce rispetto al precedente. |

N.B. La dimensione delle PDU è di bite.

# IL livello applicazione

Il livello applicazione rappresenta il settimo livello della pila ISO-OSI e fornisce una serie di protocolli che operano a stretto contatto con le applicazioni.

###### DHCP

Il DHCP (Dynamic Host Configuration Protocol) è un protocollo di livello applicativo per la allocazione automatica degli indirizzi IP tra gli Host. Oltre a quest’ultimo fornisce anche la Subnet mask, il default gateway e il DNS server locale.

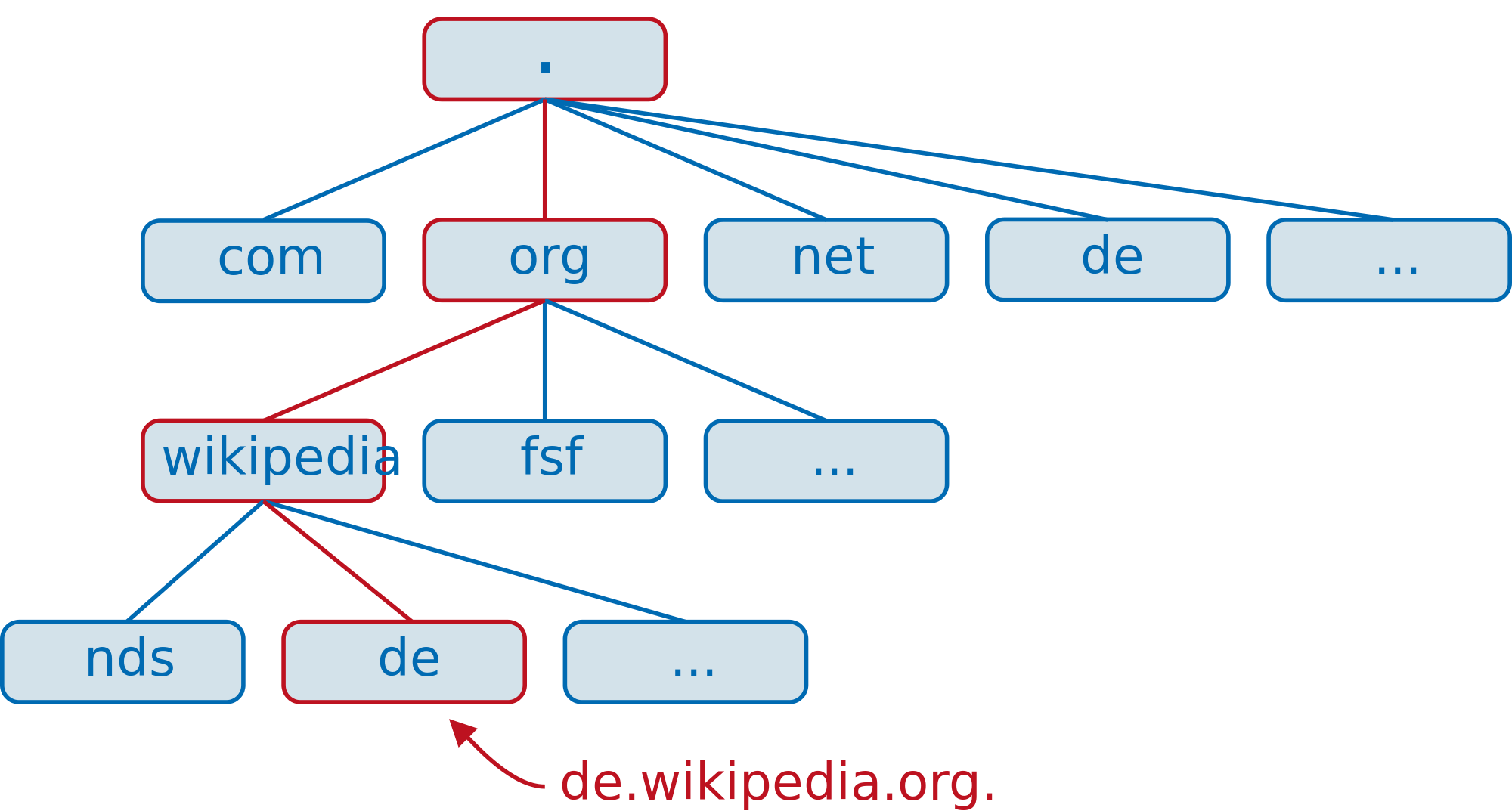
Il protocollo DHCP si basa sul protocollo DORA (Discover Offer Request Ack):

1. Discover 🡪 l’Host invia un pacchetto in broadcast contenente la richiesta di un IP e attende che uno o più DHCP server ricevano il messaggio.
2. Offer 🡪 i DHCP server che hanno ricevuto il messaggio inviano (sempre in broadcast) un pacchetto contenente l’indirizzo IP.
3. Request 🡪 il Client sceglie una delle offerte dei DHCP server e invia un pacchetto con le informazioni del DHCPOFFER; gli altri DHCP server rimettono il loro IP nel pool degli indirizzi disponibili.
4. ACK 🡪 il server risponde con un ACK confermando i parametri della configurazione.

###### DNS

Il DNS (Domain Name System) è una applicazione che consente di utilizzare dei nomi per identificare degli indirizzi IP. Il sistema è basato su un **database distribuito** organizzato gerarchicamente.

Le componenti principali del DNS server sono:

1. Domain Name Space 🡪 specifica la struttura ad albero rovesciato:
   * + 1. Domini radice 🡪 domini di primo livello (Top Level Domain)
       2. Domini intermedi 🡪 domini che hanno dei sottodomini
       3. Domini foglia 🡪 domini che non hanno dei loro sottodomini.
2. Name Server 🡪 è un processo applicativo che contiene informazioni sulle altre zone, inoltre contiene anche i puntatori ad altri Name Server.
3. Resolver 🡪 il resolver è un dispositivo che funge da client che ottiene informazioni dal Name Server.

###### Reti Microsoft

Sono reti le quali hanno il compito di:

* Individuare gli host della rete
* Riconoscere gli host
* Condividere le risorse (periferiche)
* Poter uscire dalla rete locale

Questi servizi sono implementati attraverso protocolli applicativi che operano sulla rete:

* SMB 🡪 Server Message Block, è un protocollo per il riconoscimento e la condivisione delle risorse in una rete tra Host. SAMBA è la sua versione Linux.
* Active Directory Domain Service 🡪 è un raggruppamento logico di utenti e computer gestito in modo centralizzato dal Domain Controller. È un sistema organizzato ad oggetti con un nome che li identifica univocamente e ogni oggetto può contenere degli attributi definiti da uno schema.
* LDAP 🡪 Lightweight Directory Access Protocol è un protocollo per l’interrogazione e la modifica dei servizi di Directory (qualsiasi raggruppamento di informazioni che sia sotto forma di record di dati organizzato in modo gerarchico). Microsoft usa Active Directory che è la medesima cosa: gestisce risorse e identifica utenze.

Esistono due modi per gestire gli utenti in una rete LAN:

* Workgroup 🡪 si utilizza per reti con pochi Host, ogni computer ha un elenco locale degli utenti che possono accederci. Se si vuole aggiungere un utente lo si deve aggiungere in tutti i pc dello stesso workgroup.
* Dominio 🡪 si utilizza con le reti di molti Host, gli utenti sono centralizzati in un server configurato come Domain Controller: l’accesso è autenticato dal server, non dalla macchina locale.

###### Il protocollo http

L’HyperText Transfer Protocol è un protocollo applicativo usato per la comunicazione sul web con una architettura di tipo client-server. Il protocollo si basa sul protocollo di livello trasporto tcp ed è stateless, ovvero non tiene memoria delle sessioni (si utilizzano coockie per ovviare al problema).

Abbiamo diversi metodi per effettuare le richieste http:

* GET (invia una richiesta e passa eventuali parametri tramite URL)
* POST (invia una richiesta e i parametri della richiesta non vengono passati nel URL.);
* HEAD (invia una richiesta http richiedente solo l’intestazione della risorsa, è utilizzato per testare se un determinato server è acceso e funziona ).

Richiesta http:

1. <Method> <URL> <schema(versione protocollo http)>
2. <Campo>: <valore>
3. <Campo>: <valore>
4. …
5. Body …

Es:

GET [www.miosito.com](http://www.miosito.com) http/0.9

User-agent: mozzilla;

charset: UTF-8;

risposta http:

1. Version <codice> <descrizione codice di ritorno>
2. <Campo>: <valore>
3. <Campo>: <valore>
4. …
5. Body...

###### NAT

Il Network Address Translation è una tecnica utilizzata dai router che permette di sostituire nell’intestazione di un pacchetto l’IP sorgente o destinazione con un altro indirizzo. Nel caso di una Lan si utilizza un unico punto di accesso ad internet, tutti i pacchetti passano attraverso il ruoter assumendo il suo ip pubblico.

Esistono diversi modi per fare il NAT:

|  |  |  |
| --- | --- | --- |
| NAT Statico | NAT Dinamico | PAT |
| Si usa solitamente per macchine server a cui bisogna garantire sempre lo stesso indirizzo IP. | Ad ogni Host che vuole uscire dalla Lan viene assegnato dal ISP un indirizzo pubblico diverso tra gli indirizzi disponibili nei loro pool. È sconveniente poiché utilizza molti indirizzi pubblici. | Port Address Translation è una tecnica che permette a tutti gli host di una Lan di andare in internet con lo stesso indirizzo pubblico ma con porte diverse. È un sistema efficace ma non performante dal punto di vista della velocità, poiché ogni pacchetto vanno sostituiti sia indirizzo IP che porta. |

# La Sicurezza Informatica

###### Le condizioni per avere sicurezza informatica

La sicurezza informatica è l’insieme delle misure utilizzate per proteggere i dati durante la loro trasmissione sulla rete Internet. Una minaccia è un evento che può causare danni. Ogni minaccia determina un rischio che si calcola con la formula: dove M è il magnitudo, ovvero quanto è grave, e P è la probabilità che accada.

L’Internet Security si deve occupare di garantire:

* Riservatezza 🡪 Solo gli autorizzati possono accedere ai dati
* Autenticità 🡪 I devono non devono essere falsificati
* Integrità 🡪 Il dato non deve essere compromesso
* Disponibilità 🡪 il dato deve essere disponibile

Minacce alla sicurezza:

* Integrità 🡪 Si rompe un hard-disk e avviene perdita dati. Contrastiamo con RAID o Backup.
* Disponibilità 🡪 Salta la corrente e si spegne il pc. Contrasto con UPS
* Integrità 🡪 esistono malware e virus in grado di corrompere i dati. Contrasto con antivirus o buone norme comportamentali.
* Riservatezza 🡪 gli Spyware possono intercettare i tuoi dati. Contrasto con antivirus

Per far fronte a violazioni della sicurezza informatica ci aiutano :

* Disaster Recovery 🡪 insieme delle operazioni atte a ripristinare sistemi, dati, e infrastrutture necessarie all’erogazione di servizi di business per le imprese, a fronte di gravi emergenze che ne intaccano la regolare attività.
* Business Continuity 🡪 capacità di un’organizzazione di continuare ad offrire prodotti o servizi a seguito di un incidente.

###### La crittografia simmetrica, asimmetrica e ibrida

La crittografia è l’insieme di procedure atte a nascondere il significato di un messaggio crittografandolo e renderlo noto solo al destinatario.

Esistono diversi tipi di crittografia, noi ne elenchiamo 3:

* Simmetrica 🡪 si utilizza la stessa chiave sia per cifrare che per decifrare il messaggio. è sottoposto al problema dello scambio delle chiavi. è un algoritmo leggero e quindi performante rispetto agli altri.

Gli algoritmi più famosi per la cifratura simmetrica sono:

* + DES (Data Encryption Stream) ha una chiave di cifratura a 56 bit;
  + 3 DES, chiave di cifratura a 168 bit;
  + IDEA(International Data Encryption Algorithm) chiave a 128 bit;
  + AES (Advanced Encryption Schema) chiave a 128 o 182 o 256 bit.
* Asimmetrica 🡪 si utilizza la chiave pubblica per cifrare il messaggio, e solo chi ha la chiave privata può decifrarlo. La chiave pubblica può essere resa nota a tutti, ma non la privata. L’algoritmo più utilizzato è RSA. Questa cifrature consente inoltre di ottenere autenticazione.
* Ibrida 🡪 si utilizza quando si vuole ottenere sia la riservatezza che la autenticità. Utilizza gli algoritmi simmetrici e asimmetrici.

###### Firma Digitale

La firma digitale è un certificato, alla pari della firma su carta, che garantisce integrità, autenticità e la non ripudiabilità.

Per poter firmare digitalmente un file necessitiamo di un certificato (che comprende chiave pubblica e privata) firmato da una Certification Authority (CA), il quale lo firma con la sua chiave privata. Poi è necessario firmare con la chiave privata, che è stata fornita il file, che dobbiamo inviare, ma considerato che il file potrebbe essere pesante e ci potrebbe volere tempo per firmarlo, si usa un **algoritmo di Hash** per creare un digest di lunghezza prefissata che identifica il file, e poi lo firmiamo con la nostra chiave privata. Inviamo quindi oltre al file anche il digest contenente la firma digitale.

File

CA

Firma il tuo certificato con la sua chiave privata per validarlo

Creo il digest del file con un algoritmo di Hash

Digest del file

Tua chiave privata

Firmo il file con la mia chiave privata

Digest del file firmato dalla tua chiave privata

Digest firmato

File originale

Firma Digitale

Invio 2 file:

In questo modo chiunque riceverà il mio file potrà grazie alla firma digitale verificare che il pacchetto sia integro e che sia io il mittente. Se invece volessi che il mio pacchetto fosse leggibile solo da una persona in particolare, semplicemente cifro con la chiave pubblica del destinatario in modo che solo e soltanto lui può leggere il contenuto del pacchetto utilizzando la sua chiave privata.

# Virtualizzazione e cloud computing

###### Virtualizzazione

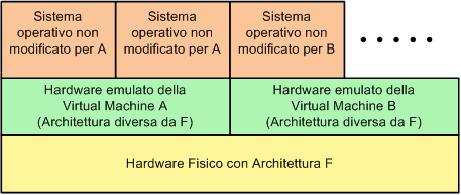
La virtualizzazione è una tecnologia che ti permette di creare delle astrazioni dell’hardware della macchina fisica. Grazie ad un software che si chiama Hypervisor riusciamo a mettere in comunicazione l’hardware fisico con il sistema operativo che risiede nell’hardware virtuale. L’HW può essere installato sopra un altro sistema operativo oppure direttamente nella macchina.

Possiamo riconoscere due tipi di virtualizzazione:

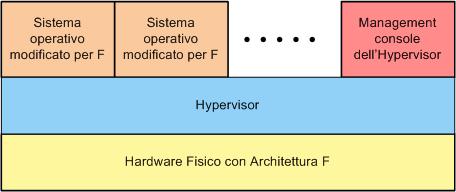
* Full virtualization;
* Paravirtualization.

La Full virtualization 🡪 (il sistema si basa sulla traduzione binaria) l’hypervisor si fa carico di simulare un HW, che può essere diverso da quello fisico, al fine di presentare al O.S. guest un HW a lui noto.

Questo procedimento ha prestazioni limitate poiché il flusso di istruzioni provenienti dal guest deve essere convertito dal HV in un flusso di istruzioni equivalenti compatibili con HW fisico.



Paravirtualization 🡪 sistema nel quale l’HV si occupa solo di tradurre determinate istruzioni del S.O. guest, il quale deve essere modificato in base al HW del host. Questo sistema permette maggiori prestazioni poiché i sistemi guest comunicano direttamente con l’HW fisico. (gli O.S. modificati si precludono di alcune chiamate



###### Cloud Computing

Il cloud computing è un insisme di servizi che vengono resi disponibili attraverso la rete internet.

|  |  |
| --- | --- |
| Vantaggi | Svantaggi |
| * È più economico utilizzare i software nel cloud. * Non si necessita di installare e tenere aggiornati i software. * Non si necessita di hardware. * Nessun costo di manutenzione. * Gestione da remoto. * Permette alle aziende di concentrarsi nel proprio core business. | * Non vi si può accedere in assenza della connessione Internet. |

Esistono diversi tipi di servizi a cui si può accedere tramite la rete internet:

* SaaS 🡪 Software as a Service consiste nell’utilizzo di software resi disponibili online, quindi non installati nella macchina locale.
* PaaS 🡪 Platform as a Service consiste nell’utilizzo di una piattaforma (suite di programmi) online, al posto dei programmi singoli.
* IaaS 🡪 Infrastructure as a Service viene messa a disposizione un hardware in remoto.

# La sicurezza in rete

Il cablaggio strutturato ISO/IEC 11801.

*Attività di laboratorio:* utilizzo del simulatore Cisco PacketTracer per implementare funzionalità di Firewall mediante ACL.

###### Firewall

Il firewall è una applicazione che lavora a livello 7 e serve per filtrare il traffico di rete a seconda delle policy di sicurezza che vengono scritte nelle ACL (Access Control List).

Esistono 4 tipi di firewall:

|  |  |  |  |
| --- | --- | --- | --- |
| State less | State Full | Deep Inspection | Proxy |
| Lavora a livello 3 e filtra il traffico o per ip mittente o destinatario | Lavora a livello 4 perché tiene traccia delle connessioni TCP che si creano e filtra i pacchetti sia per ip mittente che destinatario | Lavora a livello 7 e permette di ispezionare filo al dato del pacchetto e riconosce eventuali firme di virus o malware. | È un particolare tipo di firewall che si mette tra il client e il server, uscendo lui dalla rete locale. Inoltre fornisce un sistema di caching, permette di effettuare l’autenticazione e bloccare le connessioni in uscita verso specifici indirizzi. |

Le ACL 🡪 Access Control List sono delle tabelle nelle quali vengono scritte le policy di sicurezza dalla più stringente alla meno stringente.

Esistono 2 tipi di ACL:

|  |  |
| --- | --- |
| Standard | Estese |
| Permettono di filtrare solo a livello 3, quindi si implementano con il firewall stateless.  Le access list riservate per le standard sono dalla 1 alla 99. | Permettono di filtrare il traffico a livello 3 ma anche per l’ip destinatario, oltre al mittente. Permettono inoltre di lavorare a livello 4, implementando un firewall di tipo statefull. Le access list riservate per le standard sono dalla 100 alla 199. |

###### SSL/TLS

È una suite di protocolli che serve per ottenere un canale di comunicazione cifrato. SSL/TLS fa parte della famiglia di Secure VPN. Si usano per fare le VPN Remote Access.

I protocolli principali sono Record e HandShake Protocol

|  |  |
| --- | --- |
| HandShake Protocol | Record |
| È il protocollo che stabilisce la connessione tra client e server scambiando i certificati e decidendo i protocolli di cifratura ed hash.  <client> invia al server una richiesta di connession includendo gli algoritmi di cifratura simmetrici che lui può utilizzare per cifrare la comunicazione.  <server> invia la client il proprio certificato digiale, e invia gli algoritmi di cifratura e di hash scelti tra quelli che gli ha inviato il client.  <client> verifica il certificato del server, e se è chi veramente dice di essere, invia al server il suo certificato digitale.  <server> conferma la ricezione del pacchetto e inizia la comunicazione. | Serve per cifrare simmetricamente la comunicazione. |

###### IPSec

è l’acronimo di IP Securiy ed è una alternativa agli SSL/TLS. Si utilizza per realizzare VPN site to site e remote access. IPSec si basa su 3 protocolli principali:

|  |  |  |
| --- | --- | --- |
| AH | ESP | IKE |
| Authentication Header garantisce l’autenticazione e l’integrità del messaggio, ma non offre confidenzialità. | Encapsulating Security Payload garantisce autenticazione, confidenzialità e integrità del messaggio. | Internet Key Exchange implemente la sambio delle chiavi per il flusso crittografato. |

IpSec può essere utilizzato sia in modalità trasporto che modalità tunneling:

|  |  |
| --- | --- |
| Trasporto | Tunneling |
| La comunicazione avviene tra Host, e si usa per le VPN Remote Access.  Vengono inclusi agli header del pacchetto gli header dei protocolli IPSec utilizzati. | La comunicazione avviene tra gateway, e lo si utilizza per le VPN site to site. I pacchetti vengono incapsulati dentro altri pacchetti sfruttando molta potenza di calcolo. |

Esistono inoltre due tipi di VPN site-to-site che si possono sviluppare con IPSec:

|  |  |
| --- | --- |
| Intranet-based | Extranet-based |
| Si usa quando si vogliono unire delle sedi di una società distaccate. Si usa per unire più reti private in una unica rete all’interno di una WAN | Si usa quando due aziende vogliono collaborare tra loro scambiandosi dati in modo sicuro, collega le die Lan delle aziende ma non garantisce l’accesso alle loro Intranet. |

###### SSH

È l’acronimo di Secure SHell e permette di autenticarsi e connettersi ad Host remoti in un canale cifrato ed interagire a riga di comando. Il suo predecessore è il Telnet.

###### HTTPS

È l’acronimo di HyperText Transfer Protocol Over Secure Socket Layer ed è un protocollo per la comunicazione cifrata usato nel web. La porta utilizzata è la 443. Utilizza in’oltre il certificato X.509.

###### X.509

È uno standard di certificati che prevede l’inclusione della chiave pubblica del server (fornite dalle CA al soggetto titolare) al fine di verificarne l’autenticità, l’identità e di creare un canale cifrato per la comunicazione.

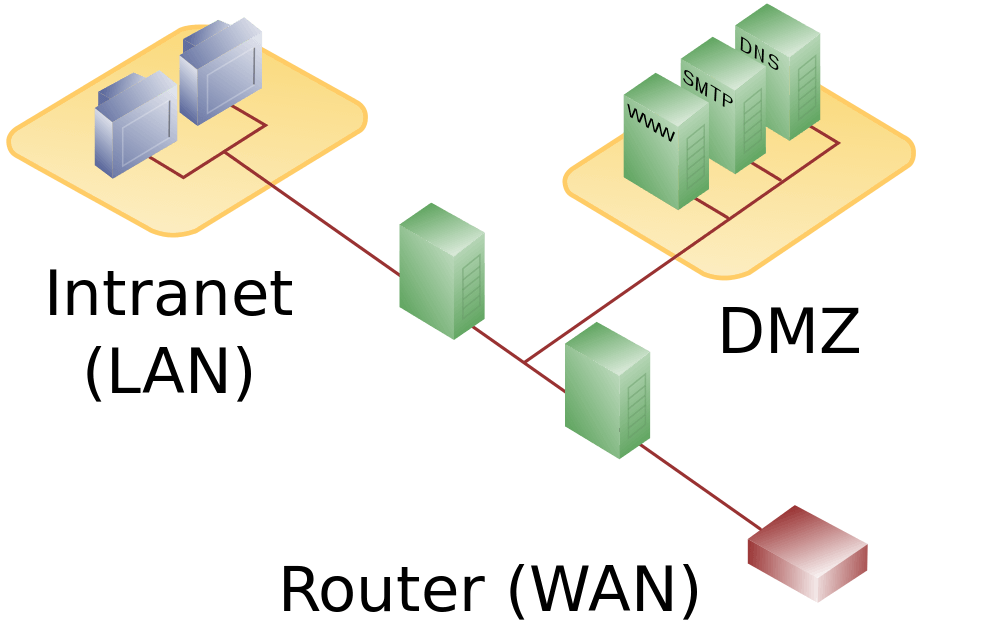
###### Le VPN

La VPN è una tecnica per ottenere una rete privata all’interno di una infrastruttura di rete pubblica.

Le VPN possono essere di due tipi:

|  |  |
| --- | --- |
| Remote Access | Site-to-Site |
| Consentono la connessione cifrata ad una rete Lan ad un singolo Host in qualsiasi parte del mondo si trovi, a patto di avere un collegamento alla rete Internet. | Consentono la connessione remota tra Gateway, collegando due reti private, gli host all’interno delle reti non sanno di comunicare con la sede distaccata passando per una VPN. |

###### Reti Trust/DMZ

Le reti DMZ (DeMilitarized Zone) sono delle reti con Policy di sicurezza meno stringenti rispetto alle reti Trust, dove normalmente vi risiedono i server contenenti servizi pubblici. Le reti Trust invece sono reti con Policy di sicurezza elevate dove vi risiedono computer ad uso locale, per esempio di una azienda.

###### Il cablaggio Strutturato

Il cablaggio strutturato è l’insieme delle norme per garantire semplicità, affidabilità, costi contenuti, flessibilità e rispetto degli standard.

Per il cablaggio strutturato si utilizza una topologia di rete a Stella estesa gerarchica, ovvero che l’intera rete viene divisa in:

* Centro stella di comprensorio 🡪 CD Campus Distributor
* Centro stella di edificio 🡪 BD Building Distributor
* Centro stella di piano 🡪 FD Floor Distributor
* Prese utente 🡪 TO Telecommunication Outlet