IIS PRIMO LEVI A.S. 2024/25

PROGRAMMA DI SISTEMI E RETI

APPUNTI

Sommario

Sommario

MODULO 1. CRITTOGRAFIA

La crittografia simmetrica

La crittografia simmetrica utilizza una chiave, o un codice segreto, per crittografare e decrittografare i dati. Questa chiave è la stessa sia per l'invio che per la ricezione del messaggio, da cui il termine "simmetrica". Immaginate che la chiave sia come una sorta di serratura: solo chi ha la chiave può aprire il lucchetto e leggere il messaggio.

Ecco come funziona:

1. Crittografia: Il mittente prende il messaggio originale e lo cifra utilizzando una chiave segreta, ottenendo così il testo cifrato. Questo processo rende il messaggio illeggibile a chiunque non abbia la chiave.

2. Trasmissione: Il messaggio cifrato viene inviato attraverso la rete non sicura.

3. Decrittografia: Una volta che il messaggio cifrato arriva al destinatario, questo utilizza la stessa chiave segreta per decodificarlo e leggerlo.

Esempio: Supponiamo di avere un messaggio "CIAO" che vogliamo inviare. Usiamo una chiave "1234" per cifrarlo. Il messaggio cifrato potrebbe apparire come "XKDN" (è solo un esempio casuale). Quando il destinatario riceve "XKDN", utilizza la stessa chiave "1234" per decrittografarlo e ottenere il messaggio originale "CIAO".

Questo approccio è efficace perché solo le persone autorizzate conoscono la chiave necessaria per decifrare i messaggi. Tuttavia, una delle sfide della crittografia simmetrica è la sicurezza della chiave stessa. Se la chiave viene compromessa, i messaggi possono essere letti da terze parti non autorizzate. Questo è il motivo per cui è essenziale gestire le chiavi in modo sicuro e garantire che siano conosciute solo dalle parti autorizzate.

In sintesi, la crittografia simmetrica è uno strumento essenziale per proteggere la privacy e la sicurezza delle comunicazioni online, garantendo che solo mittente e destinatario autorizzati possano accedere al contenuto dei messaggi.

I cifrari DES, 3DES, AES

DES

Il Data Encryption Standard (DES) è un algoritmo di crittografia simmetrica che è stato uno dei più ampiamente utilizzati per molti anni.

Ecco una spiegazione semplificata di come funziona il cifrario DES:

1. Blocco di dati: Il DES opera su blocchi di dati di dimensioni fisse, generalmente 64 bit di lunghezza. Se il messaggio non è una lunghezza multipla di 64 bit, può essere necessario aggiungere del "padding" per raggiungere questa lunghezza.

2. Chiave: Il DES utilizza una chiave di 56 bit per crittografare e decrittografare i dati. Questa chiave viene inserita nell'algoritmo e viene utilizzata per generare una serie di sotto-chiavi che verranno utilizzate durante il processo di cifratura.

3. Sotto-chiavi: Dalla chiave principale di 56 bit, il DES genera 16 sotto-chiavi di 48 bit ciascuna. Queste sotto-chiavi vengono utilizzate durante le varie fasi del processo di crittografia.

4. Fasi di cifratura/decifratura: Il processo di cifratura e decifratura nel DES è composto da 16 fasi. Durante ogni fase, il blocco di dati viene manipolato e combinato con una delle sotto-chiavi generate dalla chiave principale.

5. Operazioni di sostituzione e permutazione: Durante ogni fase, il blocco di dati viene sottoposto a operazioni di sostituzione (S-boxes) e permutazione (P-boxes) che rendono il processo di crittografia non lineare e più sicuro.

6. Iterazione: Il processo di cifratura/decifratura viene iterato 16 volte, ognuna delle quali utilizza una delle sotto-chiavi generate.

7. Output: Alla fine del processo, si ottiene il blocco di dati cifrato o decifrato.

Un aspetto importante del DES è che, poiché utilizza una chiave relativamente corta (56 bit), è diventato vulnerabile agli attacchi brute-force, in cui un attaccante può tentare di decrittografare i dati provando tutte le possibili chiavi fino a trovare quella corretta. Questa è una delle ragioni principali per cui il DES non è più considerato sicuro per le applicazioni moderne.

3DES

Il 3DES, abbreviazione di Triple Data Encryption Standard, è essenzialmente una versione potenziata del Data Encryption Standard (DES) originale. È stato sviluppato come risposta alla scoperta di vulnerabilità nel DES originale, dovute alla lunghezza relativamente breve della chiave di 56 bit.

Ecco una spiegazione semplificata di come funziona il 3DES:

1. Utilizzo di più chiavi: A differenza del DES originale, che utilizza una singola chiave di 56 bit, il 3DES utilizza tre chiavi DES separate, ognuna di 56 bit. Questo porta a una chiave totale di 168 bit.

2. Processo di crittografia: Il processo di crittografia nel 3DES coinvolge tre fasi. Inizialmente, il blocco di dati viene crittografato utilizzando la prima chiave, poi decrittato utilizzando la seconda chiave e infine crittografato nuovamente utilizzando la terza chiave. Questo approccio è noto come "crittografia a triplo passaggio" o "EDE" (Encrypt-Decrypt-Encrypt).

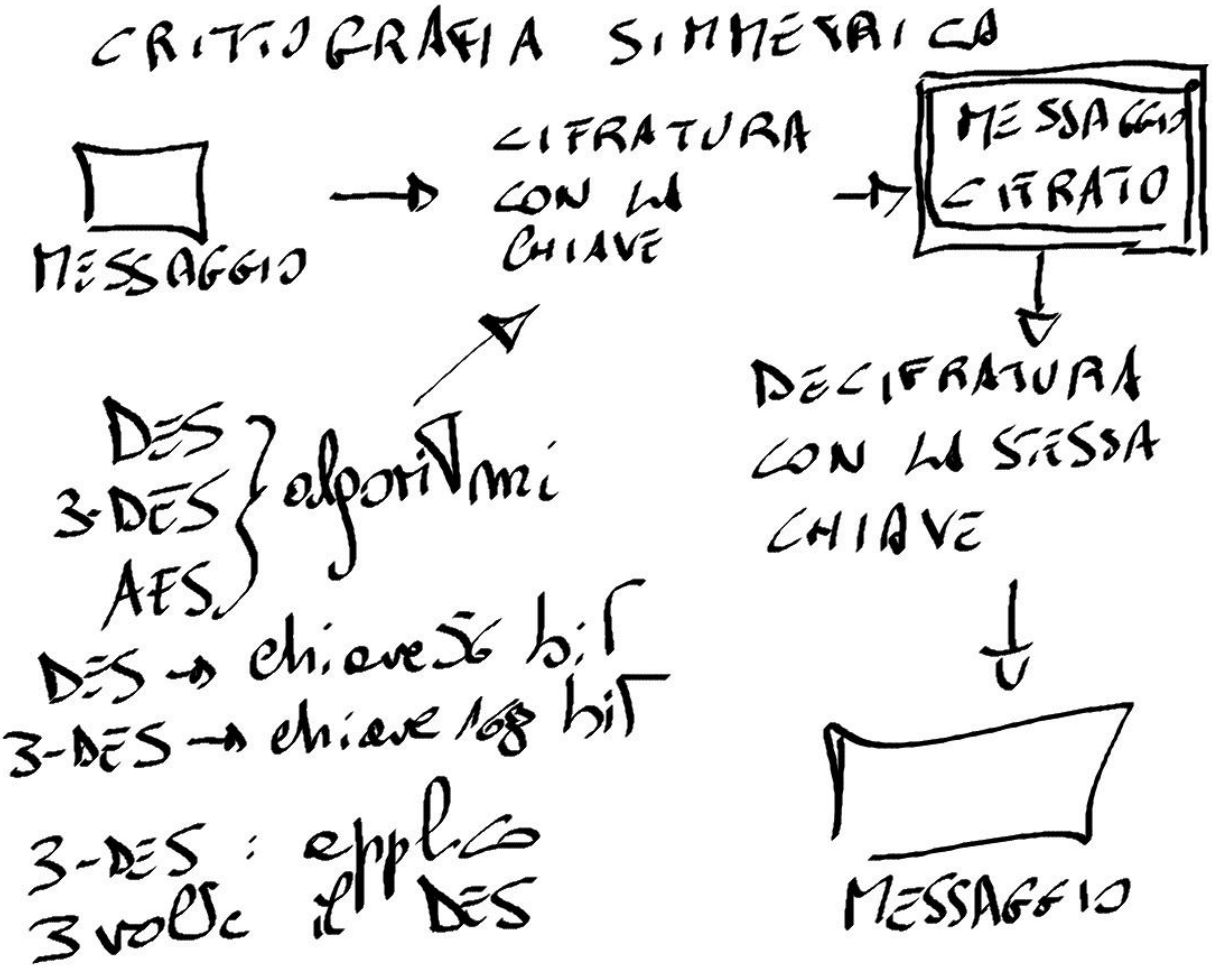
3. Sicurezza potenziata: Grazie all'utilizzo di tre chiavi separate, il 3DES offre una sicurezza molto più elevata rispetto al DES originale. Anche se utilizza l'algoritmo DES, il numero di possibili chiavi diventa significativamente maggiore a causa dell'impiego di tre chiavi separate.

4. Compatibilità: Una delle ragioni principali per l'adozione del 3DES è stata la sua compatibilità con il DES originale. Poiché utilizza lo stesso algoritmo, il 3DES può essere facilmente implementato su infrastrutture esistenti senza la necessità di modifiche sostanziali.

AES (Advanced Encryption Standard)

Il 3 DES offre un livello di sicurezza migliorato rispetto al DES originale, ma nel tempo è stato gradualmente sostituito da algoritmi crittografici ancora più avanzati e sicuri, come il AES (Advanced Encryption Standard). Questo perché, nonostante offra una sicurezza migliore rispetto al DES, il 3DES presenta alcune limitazioni, come la velocità di elaborazione più lenta rispetto agli algoritmi più moderni.

In conclusione, il 3DES è stato un importante passo avanti nella crittografia simmetrica, offrendo una maggiore sicurezza rispetto al DES originale. Tuttavia, a causa dei suoi limiti prestazionali e della disponibilità di alternative più sicure, è stato gradualmente sostituito da algoritmi crittografici più moderni, come AES



La crittografia asimmetrica

La crittografia asimmetrica, nota anche come crittografia a chiave pubblica, è un concetto fondamentale nel campo della sicurezza informatica. A differenza della crittografia simmetrica di cui abbiamo parlato in precedenza, che utilizza una singola chiave per crittografare e decrittografare i dati, la crittografia asimmetrica coinvolge l'uso di due chiavi correlate ma distinte: una chiave pubblica e una chiave privata.

Ecco come funziona la crittografia asimmetrica:

1. Chiavi pubbliche e private: Un ente certificatore preposto genera un paio di chiavi per ogni utente, composte da una chiave pubblica e una chiave privata. La chiave pubblica è disponibile per tutti e viene utilizzata per crittografare i dati, mentre la chiave privata è nota solo al proprietario e viene utilizzata per decrittografare i dati.

2. Crittografia: Se Alice vuole inviare un messaggio a Bob in modo sicuro utilizzando la crittografia asimmetrica, Alice userà la chiave pubblica di Bob per crittografare il messaggio. Anche se tutti possono accedere alla chiave pubblica di Bob, solo Bob può decrittografare il messaggio utilizzando la sua chiave privata.

3. Decrittografia: Una volta che Bob riceve il messaggio cifrato, lo decifra utilizzando la sua chiave privata. Anche se il messaggio è stato crittografato con la sua chiave pubblica (che è disponibile a tutti), solo Bob può decrittografarlo poiché è l'unico ad avere accesso alla sua chiave privata.

4. Firme digitali: Oltre alla crittografia dei dati, la crittografia asimmetrica è utilizzata anche per creare firme digitali. Una firma digitale è un meccanismo che garantisce l'autenticità e l'integrità di un messaggio o di un documento tramite un ente certificatore che garantisce chi è il proprietario della chiave pubblica. Per firmare un documento digitalmente, un utente utilizza la propria chiave privata per crittografare un "hash" del documento. Chiunque abbia accesso alla chiave pubblica dell'utente può verificare la firma decrittografando l'hash e confrontandolo con l'hash del documento originale. Ad esempio il servizio di PEC (posta elettronica certificata) assegna una chiave pubblica e una privata ad un suo cliente e ne garantisce l’identità quando costui firma con la propria chiave privata.

La crittografia asimmetrica offre diversi vantaggi rispetto alla crittografia simmetrica. Uno dei principali è che non è necessario condividere la chiave segreta tra mittente e destinatario, rendendo più sicuro lo scambio di dati su una rete non sicura come Internet. Tuttavia, la crittografia asimmetrica è generalmente più lenta e richiede risorse computazionali aggiuntive rispetto alla crittografia simmetrica. Per questo nel caso dei certificati digitali si pre

In sintesi, la crittografia asimmetrica è un importante strumento per garantire la sicurezza delle comunicazioni su Internet, consentendo agli utenti di scambiare informazioni in modo sicuro senza dover condividere segreti crittografici.

RSA

RSA è uno degli algoritmi più noti e utilizzati per la crittografia asimmetrica, che abbiamo appena discusso. È stato sviluppato nel 1977 da Ron Rivest, Adi Shamir e Leonard Adleman, i cui nomi danno origine all'acronimo "RSA". Questo algoritmo è fondamentale per molti protocolli di sicurezza su Internet e viene utilizzato per proteggere la privacy e l'integrità dei dati scambiati online.

Ecco una spiegazione semplificata di come funziona l'algoritmo RSA:

1. Generazione delle chiavi: Il primo passo nel sistema RSA è la generazione di una coppia di chiavi: una chiave pubblica e una chiave privata. Ogni utente che utilizza RSA genera il proprio set di chiavi. La chiave pubblica è destinata alla distribuzione pubblica e può essere conosciuta da chiunque, mentre la chiave privata è mantenuta segreta dall'utente.

2. Crittografia: Per crittografare un messaggio utilizzando RSA, un mittente utilizza la chiave pubblica del destinatario. Il mittente trasforma il messaggio in un numero intero e lo eleva a una potenza modulo un numero, utilizzando la chiave pubblica del destinatario. Questa operazione produce il messaggio crittografato.

3. Decrittografia: Il destinatario riceve il messaggio crittografato e lo decrittografa utilizzando la propria chiave privata. Il destinatario eleva il messaggio crittografato alla potenza della sua chiave privata modulo lo stesso numero utilizzato per la crittografia. Questa operazione riporta il messaggio al suo stato originale.

4. Firme digitali: RSA non è solo utilizzato per la crittografia, ma anche per creare e verificare firme digitali. Per creare una firma digitale, un mittente crittografa un hash del messaggio utilizzando la sua chiave privata. Il destinatario può quindi verificare la firma decrittografando l'hash utilizzando la chiave pubblica del mittente.

5. Sicurezza: La sicurezza di RSA si basa sulla difficoltà di fattorizzare grandi numeri interi in fattori primi. La sicurezza dell'algoritmo dipende dalla lunghezza delle chiavi utilizzate: chiavi più lunghe offrono una maggiore sicurezza, poiché richiedono tempi più lunghi per essere violati tramite attacchi crittografici.

RSA è uno degli algoritmi crittografici più utilizzati in tutto il mondo ed è alla base di molti protocolli di sicurezza su Internet, inclusi HTTPS, SSH e SSL/TLS.

La posta elettronica certificata e le Firme digitali

La posta elettronica certificata (PEC) e le firme digitali sono due strumenti fondamentali per garantire la sicurezza e l'autenticità delle comunicazioni elettroniche. Inoltre, nell'Unione Europea, la posta elettronica certificata è nota come REM.

Posta Elettronica Certificata (PEC)

Posta Elettronica Certificata (PEC) La posta elettronica certificata, o PEC, è un servizio che consente di inviare e ricevere email con valore legale equivalente a una raccomandata con ricevuta di ritorno. Funziona attraverso l'utilizzo di una terza parte affidabile, generalmente un fornitore di servizi di posta elettronica certificata, che garantisce la consegna del messaggio elettronico e ne certifica l'invio e la ricezione.

Dal 2023 la PEC è stata sostituita dalla REM (Registered Electronic Mail). La REM, detta comunemente PEC europea, è lo strumento per l’invio di comunicazioni telematiche che risponde completamente a tutti i requisiti del Regolamento e dello standard ETS richiesti dall’Unione Europea perché la posta elettronica certificata sia valida in tutti gli stati europei.

Il funzionamento della PEC è il seguente:

* Quando invii un'email tramite PEC/REM, la tua email viene criptata e inviata al server del fornitore di servizi PEC/REM. Il server registra l'invio e lo marca con un timestamp, quindi inoltra l'email al destinatario.

* Il destinatario riceve l'email e il server del fornitore di servizi PEC/REM registra anche la ricezione, marchiandola con un timestamp.

* Entrambi l'invio e la ricezione dell'email vengono registrati e certificati, fornendo una prova legale dell'invio e della ricezione dell'email.

Questo rende la PEC/REM uno strumento prezioso per le comunicazioni commerciali, giuridiche e amministrative, poiché fornisce una prova indiscutibile dell'invio e della ricezione di documenti e comunicazioni importanti.

Firme Digitali:

Le firme digitali sono strumenti crittografici utilizzati per garantire l'autenticità e l'integrità di documenti elettronici, messaggi email e transazioni online. Funzionano utilizzando la crittografia asimmetrica: il mittente utilizza la propria chiave privata per firmare digitalmente un documento, e il destinatario può verificare la firma utilizzando la chiave pubblica del mittente.

Il processo di firma digitale di solito coinvolge i seguenti passaggi:

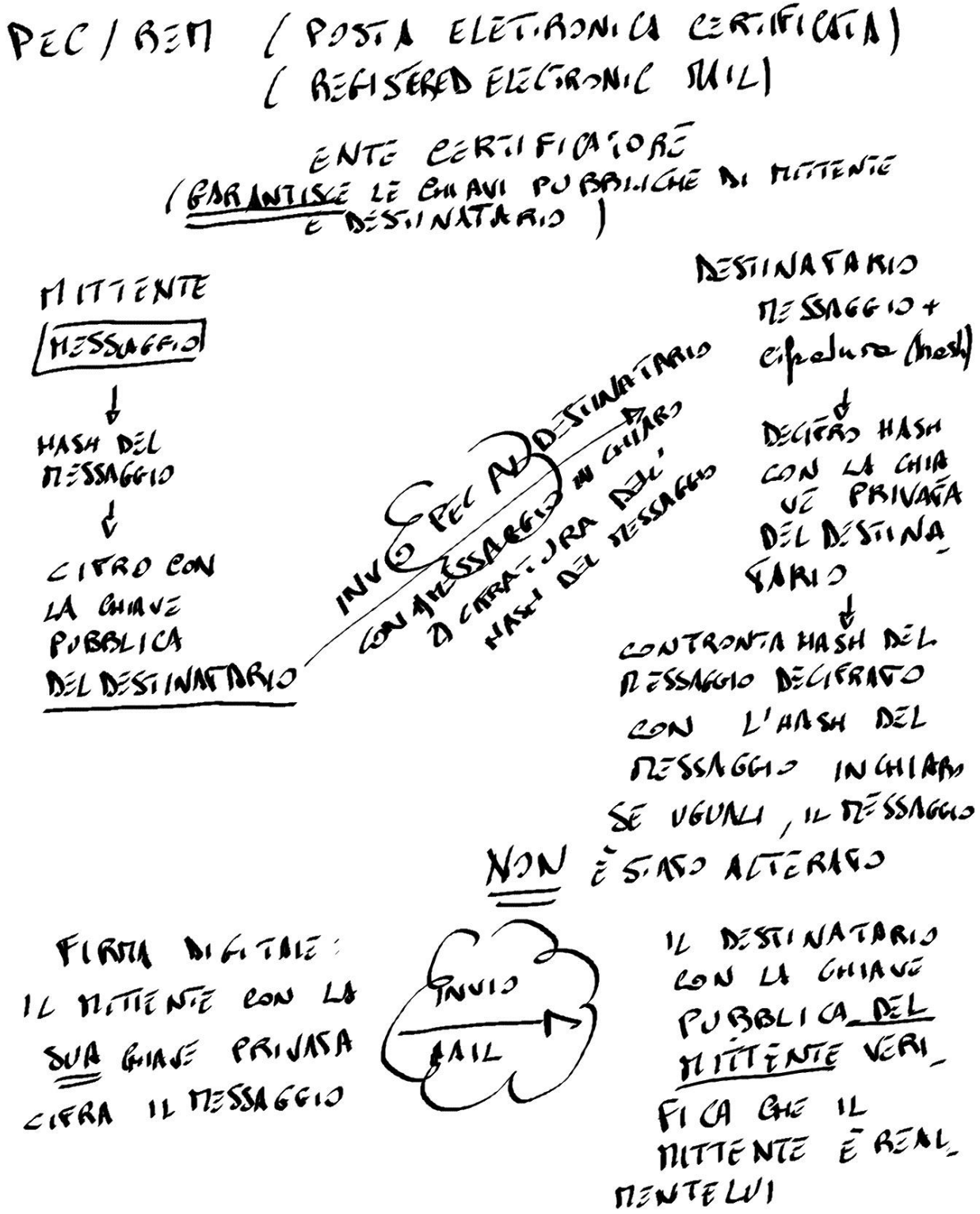
* Il mittente crea una "digest" (un riassunto crittografico) del documento utilizzando un algoritmo di hash crittografico.

* Questo "digest" viene crittografato utilizzando la chiave privata del mittente per creare la firma digitale.

* Il destinatario riceve il documento e la firma digitale e utilizza la chiave pubblica del mittente per decrittografare la firma e ottenere il "digest" originale.

* Il destinatario calcola nuovamente il "digest" del documento ricevuto e lo confronta con il "digest" originale ottenuto dalla firma digitale (AUTENTICITA' DEL MITTENTE). Se i due "digest" corrispondono, la firma è valida e il documento non è stato alterato (INTEGRITA' DEL MESSAGGIO).

Le firme digitali forniscono un alto livello di sicurezza e autenticità alle comunicazioni elettroniche, permettendo di verificare l'identità del mittente e l'integrità dei documenti firmati. Sono ampiamente utilizzate in vari settori, inclusi quello giuridico, finanziario e commerciale, per garantire la validità e la sicurezza delle transazioni e delle comunicazioni online.



I certificati digitali

Come funziona il certificato digitale in pratica

La crittografia asimmetrica viene applicata al certificato digitale rendendolo uno strumento sicuro per scambiare informazioni tra due computer. Tutto il sistema si fonda sull'affidabilità della Certification Authority. E' a questa che ci si rivolge per acquistare un certificato digitale ed anch'essa ha una propria coppia di chiavi.

Quando la Certification Authority ti fornisce i dati del tuo certificato ne cifra le chiavi con la propria chiave privata. Quindi sarà possibile decifrarle con la corrispondente chiave pubblica della Certification Authority.

Questo garantisce che, una volta consegnate al legittimo proprietario, non sarà possibile alterare le chiavi.

In concreto succede questo:

1.Il Client richiede l'apertura di una connessione protetta al Server;

2.Il Server risponde al Client inviandogli:

a.Il proprio ID

b.Il nome della società per la quale è stato emesso il certificato

c.Il proprio common name, che contiene il nome di dominio per il quale il certificato è valido.

d.Il periodo di validità del certificato

e.Il nome della Certification Authority che ha rilasciato il certificato

f.La propria chiave pubblica cifrata con la chiave privata della Certification Authority

3.Il Client verifica la validità dei dati che gli sono stati inviati dal Server e ne decifra la chiave pubblica utilizzando la chiave pubblica della Certification Authority.

4.Il Client usa la chiave pubblica del Server appena ottenuta per cifrare ed inviargli:

a.Il proprio ID

b.Un ID di sessione (che permette al Server di distinguere un Client dagli altri)

5.Le presentazioni tra Client e Server sono finite, ora i due si conoscono e sono in grado di trasmettere e ricevere dati cifrati perchè si sono scambiati prima le chiavi per codificare la comunicazione.

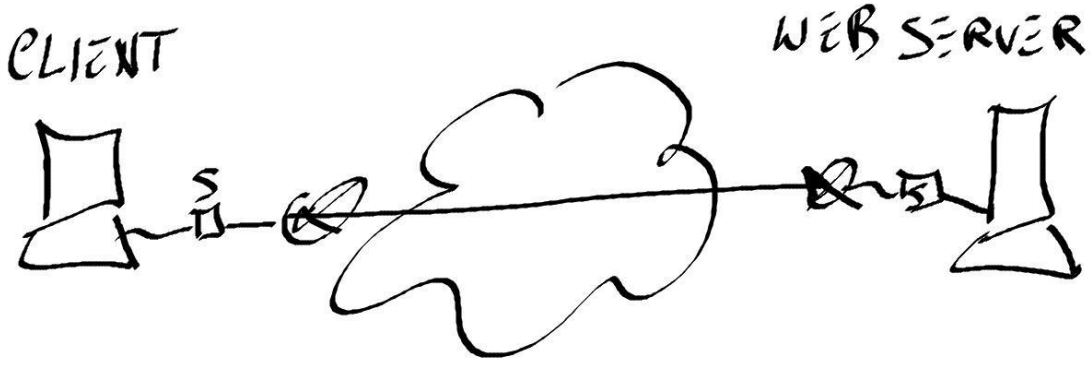
Da questo momento in poi tutti i dati saranno assolutamente protetti.

Quella esposta sopra è una generica procedura di comunicazione cifrata.

I dati in concreto scambiati tra Server e Client possono cambiare in relazione al tipo di certificato utilizzato.

Non esiste, infatti, IL certificato digitale.

Piuttosto esistono vari tipi di certificato digitale, ognuno con una propria specifica funzione ed un proprio specifico livello di sicurezza ed una propria specifica destinazione d'uso.



ENTE CERTIFICATORE: GARANTISCE LA CHIAVE PUBBLICA DEL SERVER

CLIENT: RICHIEDE AL SERVER IL CERTIFICATO DIGITALE E LO CONTROLLA USANDO LA CHIAVE PUBBLICA DEL SERVER GARANTITA DALL'ENTE CERTIFICATORE

MODULO 2. LE ARCHITETTURE DI RETE E I PROTOCOLLI esercitazioni in laboratorio con cisco packet tracer

Partizionamento di una rete

A seconda delle esigenze del contesto, potrebbe capitare di dover dividere una rete più grande in sottoreti più piccole. Un esempio è, nel caso di una stanza di un ufficio, la compresenza di più postazioni adibite a scopi differenti, come una di sviluppo e l'altra di management. Come si può riuscire a suddividere questa ipotetica rete?

La risposta risiede nella maschera di sottorete, o subnet mask (SM). La maschera di sottorete è un parametro che indica la dimensione delle sottoreti presenti nell'indirizzo IP. Trattando di indirizzi IP IPv4, la maschera di sottorete sarà composta da 4 byte, cioè 32 bit. Le maschere più utilizzate sono "a multipli di 8", ovvero a seconda della classe dell'indirizzo IP (A, B, C) hanno 8, 16, o 24 "bit a 1". Queste maschere standard permettono di avere all'interno della stessa rete tutti gli host disponibili.

Nel momento in cui si "aggiunge" un numero n di bit a queste maschere standard, si ottengono 2n sottoreti. Questo tipo di partizionamento si ottiene perché, per calcolare indirizzo di rete e di broadcast, si svolgono delle operazioni bit-a-bit tra indirizzo IP e maschera di sottorete, che determinano l'appartenenza alla data sottorete. Per ottenere l'indirizzo di rete conoscendo la maschera di sottorete e l'indirizzo IP si svolge un AND bit-a-bit disponendo prima l'indirizzo IP e poi la SM, mentre per ottenere l'indirizzo di broadcast si svolge l'operazione OR bit-a-bit tra l'IP e il complemento a 1 della SM. Dopo aver trovato i vari indirizzi di rete e di broadcast da adoperare per le varie sottoreti, si può procedere all'assegnazione degli indirizzi IP agli host. Questi indirizzi si possono configurare staticamente, configurando manualmente ogni indirizzo IP sulla scheda di rete del client , oppure si può demandare la configurazione al servizio di DHCP presente sul router.

ESEMPIO

partizionamento in 4 sottoreti Della rete 192.168.1.0/24

Spiegazione

Per partizionare la rete 192.168.1.0/24 in quattro sottoreti, dobbiamo modificare la maschera di sottorete originale (255.255.255.0) per creare quattro sottoreti più piccole. La rete 192.168.1.0/24 ha un totale di 256 indirizzi IP (da 192.168.1.0 a 192.168.1.255).

Ecco i passaggi dettagliati:

1. Determinare il numero di bit da aggiungere alla maschera di sottorete:
    - La maschera originale è /24 (255.255.255.0), che utilizza 24 bit per la parte di rete.
    - Per creare 4 sottoreti, abbiamo bisogno di 2 bit aggiuntivi (poiché 2^2 = 4).
2. Calcolare la nuova maschera di sottorete:

- Aggiungendo 2 bit alla maschera originale /24, otteniamo una nuova maschera di /26.
- La notazione decimale della maschera /26 è 255.255.255.192.

3. Dividere l'intervallo degli indirizzi IP:

- La lunghezza del prefisso /26 implica che ogni sottorete avrà 64 indirizzi (256 indirizzi / 4 sottoreti = 64 indirizzi per sottorete).
- Gli indirizzi di ogni sottorete possono essere determinati incrementando di 64:

4. Elenco delle sottoreti:

- Sottorete 1: PRIMA LAN A DISPOSIZIONE DOPO IL PARTIZIONAMENTO
  - Indirizzo di rete: 192.168.1.0
  - Primo indirizzo utile: 192.168.1.1
  - Ultimo indirizzo utile: 192.168.1.62 (indirizzo di gateway)
  - Indirizzo di broadcast: 192.168.1.63
- Sottorete 2: SECONDA LAN A DISPOSIZIONE DOPO IL PARTIZIONAMENTO
  - Indirizzo di rete: 192.168.1.64
  - Primo indirizzo utile: 192.168.1.65
  - Ultimo indirizzo utile: 192.168.1.126 (indirizzo di gateway)
  - Indirizzo di broadcast: 192.168.1.127
- Sottorete 3: TERZA LAN A DISPOSIZIONE DOPO IL PARTIZIONAMENTO
  - Indirizzo di rete: 192.168.1.128
  - Primo indirizzo utile: 192.168.1.129
  - Ultimo indirizzo utile: 192.168.1.190 (indirizzo di gateway)
  - Indirizzo di broadcast: 192.168.1.191
- Sottorete 4: QUARTA LAN A DISPOSIZIONE DOPO IL PARTIZIONAMENTO
  - Indirizzo di rete: 192.168.1.192
  - Primo indirizzo utile: 192.168.1.193
  - Ultimo indirizzo utile: 192.168.1.254 (indirizzo di gateway)
  - Indirizzo di broadcast: 192.168.1.255

Riepilogo:

- Sottorete 1: 192.168.1.0/26 (192.168.1.0 - 192.168.1.63)
- Sottorete 2: 192.168.1.64/26 (192.168.1.64 - 192.168.1.127)
- Sottorete 3: 192.168.1.128/26 (192.168.1.128 - 192.168.1.191)
- Sottorete 4: 192.168.1.192/26 (192.168.1.192 - 192.168.1.255)

Ogni sottorete ha 62 indirizzi utilizzabili (per host) poiché ogni sottorete perde 2 indirizzi: uno per l'indirizzo di rete e uno per l'indirizzo di broadcast.

DHCP

Il servizio DHCP (Dynamic Host Configuration Protocol) è un protocollo di assegnazione di indirizzi IP alle macchine (computer o dispositivi mobili) in modo totalmente automatico. Questo protocollo viene sempre configurato nel router per ogni rete che andremo utilizzare, per esempio se dovessimo configurare il DHCP per il seguente indirizzo di rete 192.168.2.0 dovremmo eseguire i seguenti passaggi.

COMANDI PER CLI DEL ROUTER CISCO

IP dhcp pool “nome a piacere”; (creazione della famiglia di indirizzi IP)

network 192.168.2.0 255.255.255.0 (indirizzo di rete +maschera di sottorete)

default-router 192.168.2.254 (indirizzo di gateway)

dns-server “indirizzo IP dns” [opzionale]

ip dhcp excluded-address “indirizzo IP di partenza” “indirizzo IP finale” (esclusione di alcuni indirizzi IP con relativo intervallo)

exit (uscita dalla configurazione)

Vantaggi del DHCP:

1. Assegnazione dinamica degli indirizzi IP: Il DHCP consente agli amministratori di rete di assegnare dinamicamente agli host (client) all'interno di una rete indirizzi IP temporanei (noti come lease) anziché indirizzi IP statici. Questo permette di ottimizzare l'utilizzo degli indirizzi IP disponibili nella rete.

2. Allocazione di altri parametri di rete: Oltre agli indirizzi IP, il DHCP può essere utilizzato per assegnare agli host altri parametri di rete essenziali, come il gateway predefinito, i server DNS.

3. Processo di assegnazione: Il processo di assegnazione DHCP coinvolge tre attori principali: il client, il server DHCP e il router o il relay DHCP (se necessario). Il client invia una richiesta DHCP di assegnazione di indirizzo IP alla rete. Questa richiesta viene inoltrata ai server DHCP disponibili tramite un broadcast o unicast. Il server DHCP riceve la richiesta e assegna un indirizzo IP disponibile al client, insieme ad altri parametri di rete. Il client accetta quindi l'assegnazione e inizia a utilizzare l'indirizzo IP e gli altri parametri ricevuti.

4. Lease di indirizzi IP: Gli indirizzi IP assegnati tramite DHCP hanno un tempo di validità limitato, noto come lease time. Questo significa che gli indirizzi IP sono assegnati temporaneamente e devono essere rinnovati periodicamente. Alla scadenza del lease, il client può richiedere un rinnovo dell'assegnazione IP.

5. Scalabilità e centralizzazione: Il DHCP consente di gestire in modo efficiente le configurazioni di rete su una vasta gamma di dispositivi. I server DHCP centralizzati possono essere configurati per gestire le assegnazioni di indirizzi IP per l'intera rete, semplificando la gestione e garantendo una maggiore coerenza nelle configurazioni di rete.

l protocolli DNS, HTTP, FTP

DNS

DNS: Il Domain Name System (DNS) è come una rubrica telefonica per internet. Quando inserisci un nome di dominio come "example.com" nel tuo browser, il DNS traduce quel nome in un indirizzo IP. Questo ti permette di raggiungere il sito che desideri. Il DNS funziona distribuendo le richieste di traduzione dei nomi di dominio a una serie di server specializzati, chiamati server DNS, che collaborano per fornire la risposta giusta al tuo dispositivo. In sostanza, il DNS aiuta a trovare il percorso giusto per raggiungere le risorse su Internet usando nomi di dominio facili da ricordare anziché indirizzi IP complessi.

HTTP

HTTP:Il protocollo HTTP, o Hypertext Transfer Protocol, è come un linguaggio che i browser e i server web usano per comunicare tra loro. Quando digiti un URL come "http://www.example.com" nel tuo browser, stai effettivamente chiedendo al server di example.com di inviarti la pagina web corrispondente. Il protocollo HTTP specifica come questa richiesta e la risposta del server dovrebbero essere strutturate e trasmesse attraverso Internet. In poche parole, HTTP facilita il trasferimento di pagine web e altri contenuti su Internet, consentendo la visualizzazione dei siti web sui tuoi dispositivi.

FTP

FTP (File Transfer Protocol): è un protocollo utilizzato per trasferire file tra computer su una rete TCP/IP (Transmission Control Protocol/Internet Protocol).

FTP è un protocollo client/server, il client richiede i file e il server li fornisce. Per questo al protocollo FTP servono due canali di base per stabilire una connessione:

* Canale di comando: avvia l'istruzione, trasporta le informazioni di base, ad esempio i file a cui accedere

* Canale di dati: trasferisce i dati dei file fra i due dispositivi

Per stabilire una connessione, gli utenti dovranno fornire le credenziali al server FTP, che solitamente usa il numero di porta 21 come modalità di comunicazione predefinita inoltre esistono due diverse modalità di connessione FTP: attiva e passiva.

Nella modalità FTP attiva, il server assume un ruolo attivo approvando una richiesta di dati. Tuttavia, la modalità attiva può incorrere in problemi con i firewall, che bloccano le sessioni non autorizzate da terze parti. Ecco che entra in gioco la modalità passiva. Nella modalità passiva, il server non mantiene attivamente la connessione, quindi sarà l'utente a stabilire sia il canale dati che il canale di comando. Fondamentalmente il server "ascolta", ma non partecipa attivamente, consentendo all'altro dispositivo di gestire la maggior parte del lavoro.

Vantaggi:Con FTP si possono trasferire più file contemporaneamente, riprendere un trasferimento in caso di connessione persa e programmare i trasferimenti.

Svantaggi: Questo protocollo è stato inventato negli anni '70 dello scorso secolo e per questo motivo, non include molte delle misure di sicurezza informatica. I trasferimenti FTP non sono crittografati quindi gli hacker non hanno difficoltà nel leggerli.

Il web server e il server DNS

IL WEB SERVER

Il web server è un software progettato per gestire le richieste dei client su Internet. Il suo compito principale è quello di fornire risorse, come pagine web, immagini, file, etc., ai client che ne fanno richiesta attraverso il protocollo HTTP (Hypertext Transfer Protocol) o HTTPS (HTTP Secure). Ecco alcuni elementi chiave del funzionamento di un web server:

Due esempi dei più noti web server sono: APACHE (open source) e IIS (Internet information service, del mondo Microsoft).

La richiesta di una pagina web ad un web server avviene tramite il protocollo HTTP che lavora a livello applicativo e che comunica con il livello di trasporto (TCP) e successivamente con il livello di rete (IP).

Il MODELLO ISO/OSI PER TCP/IP ha 4 livelli ognuno con protocolli specifici

LIVELLO APPLICATIVO

PROTOCOLLO HTTP

LIVELLO TRASPORTO

PROTOCOLLO TCP (OPPURE PROTOCOLLO UDP)

LIVELLO RETE

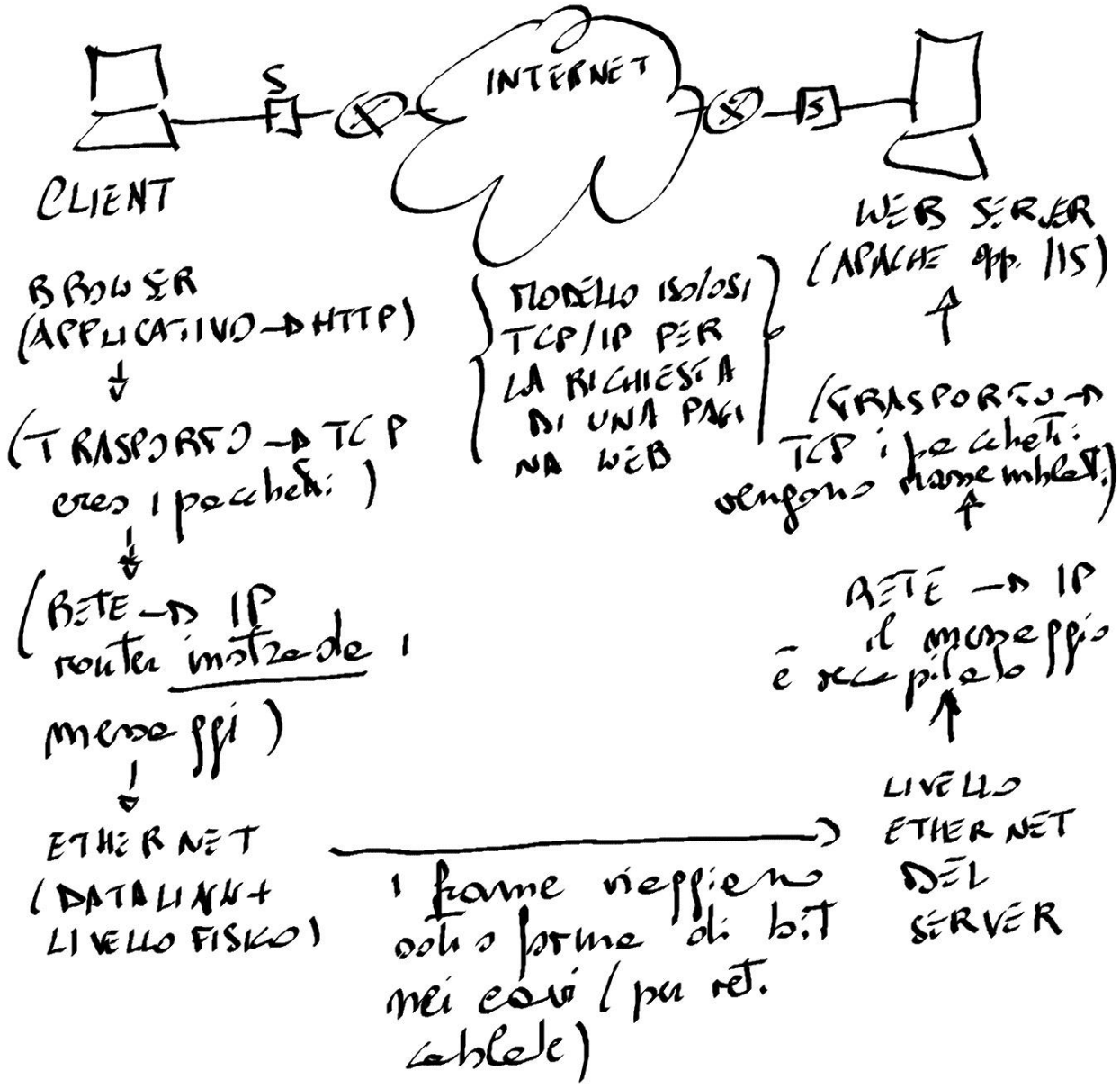
PROTOCOLLO IP

LIVELLO datalink/fisico

ethernet

* Accettazione delle richieste: Il web server riceve richieste dai client tramite HTTP o HTTPS su una determinata porta (generalmente la porta 80 per HTTP e la porta 443 per HTTPS).

SCHEMA DI UNA RICHIESTA (REQUEST) DI UNA PAGINA WEB AD UN WEB SERVER (AD ESEMPIO AMAZON)



* Elaborazione delle richieste: Una volta ricevuta una richiesta, il web server elabora questa richiesta. Questo può includere l'interpretazione dell'URL richiesto, l'accesso ai file o ai dati necessari per soddisfare la richiesta .

* Fornitura delle risorse richieste (il WEB SERVER invia una RESPONSE) : Dopo aver elaborato la richiesta, il web server invia la risorsa richiesta al client che ha fatto la richiesta. Questa risorsa potrebbe essere una pagina web HTML, un'immagine, un file scaricabile, o qualsiasi altra risorsa supportata.

* Gestione delle connessioni: Il web server è in grado di gestire simultaneamente molte connessioni da parte di diversi client. Questo può essere gestito utilizzando thread, processi separati o altri meccanismi di gestione delle connessioni.

* Sicurezza: I web server spesso includono funzionalità di sicurezza per proteggere le risorse ospitate da accessi non autorizzati. Questo può includere autenticazione, autorizzazione, crittografia SSL/TLS e altri meccanismi di sicurezza.

* Configurazione e personalizzazione: I web server sono altamente configurabili e possono essere personalizzati per soddisfare le esigenze specifiche dell'ambiente in cui operano. Gli amministratori di sistema possono configurare regole di routing, gestire la cache, impostare restrizioni di accesso e altro ancora.

* Bilanciamento del carico: Nei casi in cui un singolo server non è in grado di gestire il carico di traffico in arrivo, è possibile utilizzare più istanze di web server e distribuire il traffico tra di loro. Questo viene spesso fatto utilizzando un load balancer, che distribuisce le richieste dei client in modo equo tra i server disponibili, migliorando le prestazioni e la scalabilità del sistema.

* Protezione contro attacchi: I web server sono spesso esposti a varie minacce, come attacchi DDoS (Distributed Denial of Service), tentativi di hacking e vulnerabilità software. Pertanto, includono spesso funzionalità di sicurezza per proteggere contro tali minacce, come la limitazione dei tassi di richiesta, la rilevazione e la prevenzione degli intrusioni (IDS/IPS), la protezione da altri attacchi di applicazioni web, e l'implementazione di regole di firewall.

* Compatibilità con standard e protocolli: I web server devono rispettare standard e protocolli specifici per garantire l'interoperabilità con altri componenti del sistema Internet. Questi includono standard come HTTP, HTTPS, TCP/IP, IPv4 e IPv6, così come protocolli e tecnologie aggiuntive come WebSocket, HTTP/2, SPDY, e altri.

IL SERVER DNS

Il server DNS(Domain Name System) è un servizio che permette di ricavare l'indirizzo IP associato all'URL di un dominio web.

ESEMPIO

Nel server DNS ci sono tabelle con:

INDIRIZZO IP	URL
142.250.190.46	www.google.com
69.63.176.13	www.facebook.com
205.251.242.103	www.amazon.com

Quando viene richiesta una pagina web da un client viene inviata una richiesta (REQUEST) al server DNS,per richiedere l'indirizzo IP associato all'URL.Il server DNS risponde con l'indirizzo IP (RESPONSE).

Configurazione di una rete con servizio DNS in Cisco Packet Tracer:

Creazione della rete LAN: Configura una rete LAN utilizzando Cisco Packet Tracer. Aggiungi i dispositivi necessari come router, switch e computer alla topologia.

Aggiunta e configurazione del server DNS: Seleziona un dispositivo che fungerà da server DNS e configurarne le impostazioni. Puoi utilizzare un computer come server DNS. Assegna un indirizzo IP al server DNS e configura le relative impostazioni.

Configurazione del router: Configurare il router per inoltrare le richieste DNS al server DNS corretto. Utilizza il comando "ip name-server" per specificare l'indirizzo IP del server DNS. Assicurati anche di configurare le impostazioni di routing del router per inoltrare correttamente le richieste DNS alla rete in cui si trova il server DNS.

Configurazione dei dispositivi sulla rete: Configura i dispositivi sulla rete in modo che utilizzino il server DNS corretto. Ad esempio, nelle impostazioni TCP/IP dei computer, specifica l'indirizzo IP del server DNS come server DNS predefinito.

Verifica della connessione: Verifica che la connessione funzioni correttamente utilizzando nomi di dominio anziché indirizzi IP. Prova ad accedere a siti web utilizzando il browser di un PC e verifica che il server DNS risponda correttamente alle richieste di mappatura fra URL e indirizzi IP dei server web.

I messaggi http (request e response) in una PDU

Una PDU (Protocol Data Unit) è semplicemente un termine generico usato per descrivere un blocco di dati che viene trasmesso su una rete. Nei protocolli di comunicazione, come l'HTTP, i dati vengono organizzati in pacchetti o unità di dati, e la PDU rappresenta uno di questi pacchetti.

Ad esempio nel protocollo HTTP, ci sono due tipi principali di messaggi: le richieste (request) inviate dal client al server e le risposte (response) inviate dal server al client. Una PDU nel protocollo HTTP conterrà uno di questi messaggi completi quando viene trasmesso in rete.

Un messaggio HTTP ha una struttura comune, che può essere suddivisa in tre parti principali:

1. Intestazione (Header): Contiene metadati aggiuntivi relativi al messaggio HTTP, come informazioni sul tipo di contenuto, la data e l'ora della richiesta, e così via.

2. Linea di richiesta/risposta: Questa parte varia leggermente a seconda che si tratti di una richiesta inviata dal client o di una risposta inviata dal server. La linea di richiesta indica il metodo HTTP utilizzato (come GET, POST, ecc.), l'URI (Uniform Resource Identifier) richiesto e la versione del protocollo HTTP. La linea di risposta, invece, contiene lo stato della risposta (ad esempio "200 OK" per una risposta di successo), la versione del protocollo HTTP e una breve descrizione dello stato.

3. Corpo del messaggio (Body): Questa parte è opzionale e contiene i dati effettivi trasmessi con il messaggio HTTP. Ad esempio, nel caso di una richiesta POST, il corpo del messaggio conterrà i dati inviati dal client al server, come ad esempio i dati di un modulo web. Nelle risposte, il corpo del messaggio contiene spesso il contenuto richiesto, come una pagina web, un file JSON, o qualsiasi altra informazione specificata nella richiesta.

Quindi, una PDU nei protocolli HTTP conterrà l'intero messaggio HTTP, comprese tutte queste parti: l'intestazione, la linea di richiesta/risposta e, opzionalmente, il corpo del messaggio.

Ruolo delle PDU nei protocolli HTTP

* Le PDU (Protocol Data Units) rappresentano un elemento cruciale nella trasmissione dei dati attraverso le reti informatiche.

* La struttura delle PDU gioca un ruolo fondamentale nell'assicurare l'affidabilità e l'efficienza della comunicazione tra client e server.

Struttura complessa delle PDU

* Le PDU non sono semplici contenitori passivi, ma strutture complesse che includono informazioni di controllo e di gestione.

* Oltre al contenuto effettivo del messaggio HTTP, una PDU conterrà informazioni di intestazione come l'indirizzo del mittente e del destinatario, e numeri di sequenza e di conferma per il controllo degli errori e del flusso.

Frammentazione e ricostruzione delle PDU

* La frammentazione delle PDU in pacchetti più piccoli è un aspetto critico per il trasferimento dei dati attraverso la rete.

* Questo processo permette di adattare la dimensione dei dati alle capacità della rete, riducendo il rischio di perdita di dati o ritardi nella trasmissione.

Elaborazioni delle PDU durante la trasmissione

* Durante il viaggio attraverso la rete, le PDU possono subire elaborazioni aggiuntive, come operazioni di routing e switching.

* Questo può includere l'aggiunta di informazioni di routing supplementari o l'applicazione di politiche di sicurezza per proteggere i dati sensibili.

Ricostruzione delle PDU e interpretazione dei messaggi HTTP

* Quando una PDU raggiunge il suo destinatario finale, è essenziale ricostruirla in un messaggio HTTP completo.

* Questo processo richiede la cooperazione tra il protocollo di comunicazione e l'applicazione che gestisce il messaggio, garantendo l'interpretazione corretta dei dati.

In sintesi le PDU nei protocolli HTTP svolgono un ruolo fondamentale nella trasmissione dei dati, garantendo l'efficienza e l'affidabilità della comunicazione tra client e server. La loro struttura complessa e il processo di frammentazione e ricostruzione contribuiscono alla stabilità e alla sicurezza delle comunicazioni su Internet.

Aspetto

Descrizione

Ruolo delle PDU

* Le PDU (Protocol Data Units) sono essenziali per la trasmissione dati.

* Assicurano l'affidabilità e l'efficienza della comunicazione client-server.

Struttura delle PDU

* Oltre al contenuto, includono informazioni di controllo e di gestione.

* Contengono indirizzi mittente/destinatario e dati di controllo.

Frammentazione delle PDU

* Le PDU vengono frammentate per adattarsi alla rete.

* Questo riduce il rischio di perdita di dati o ritardi.

Elaborazioni delle PDU

* Possono subire elaborazioni di routing e switching.

* Aggiunta di informazioni di routing o politiche di sicurezza.

Ricostruzione delle PDU

* Le PDU devono essere ricostruite correttamente.

* Processo necessario per l'interpretazione dei dati.

MODULO 3. LE VLAN

Le VLAN (Virtual Local Area Network) sono un concetto fondamentale nelle reti di comunicazione, utilizzato per segmentare una rete fisica in reti logiche distinte (generalmente un “ufficio” è associato ad una LAN, ad esempio l’ufficio dei programmatori, anche se posso collegare più switch fra di loro ed avere una sola LAN: l’importante è che abbia un solo collegamento, gateway, al router). La VLAN consente di migliorare la gestione, la sicurezza e l'efficienza della rete.

LAN (Local Area Network)

Una LAN è una rete di computer che copre una piccola area geografica, come un ufficio, un edificio o un campus. Le caratteristiche principali di una LAN includono:

* Portata limitata: Copre distanze relativamente brevi, generalmente entro qualche centinaio di metri.

* Velocità elevate: Tipicamente offre velocità di trasmissione elevate (da 100 Mbps a 10 Gbps).

* Proprietà: Di solito, è di proprietà e gestione di un'unica organizzazione.

* Infrastruttura fisica: Include cavi, switch, router e altri dispositivi di rete fisici.

VLAN (Virtual Local Area Network)

Una VLAN, d'altra parte, è una rete logica che permette di raggruppare nodi della rete indipendentemente dalla loro posizione fisica all'interno della LAN fisica. Le VLAN utilizzano lo stesso hardware della LAN, come switch e router, ma suddividono logicamente la rete per fornire vari vantaggi (ad esempio se ho un solo switch collegato al router posso creare due o più VLAN mentre non posso se ho un solo switch avere più di una LAN).

Differenze principali tra LAN e VLAN

1. Segmentazione Logica vs. Fisica:

* LAN: Segmentazione fisica. I dispositivi sono collegati fisicamente tra loro in una rete locale.

* VLAN: Segmentazione logica. I dispositivi possono essere in diverse ubicazioni fisiche ma appartenere alla stessa VLAN.

2. Isolamento del Traffico:

Sia per le LAN che che per le VLAN il traffico rimane isolato al loro interno senza differenze specifiche. Solo in caso di progettazione potrebbe essere utile usare le VLAN perchè una singola postazione di un ufficio potrebbe essere facilmente “spostata”in una LAN virtuale.

LAN: Tutto il traffico è visibile a tutti i dispositivi collegati alla stessa rete fisica.

* VLAN: Il traffico è isolato tra le VLAN, migliorando la sicurezza. Solo i dispositivi all'interno della stessa VLAN possono comunicare direttamente tra loro.

* 3. Gestione e Scalabilità:

* LAN: Meno flessibile in termini di gestione. Aggiungere nuovi dispositivi o segmentare la rete può richiedere cambiamenti fisici nella topologia (ad esempio aggiungere uno switch per creare una nuova rete).

* VLAN: Più flessibile e scalabile. Le modifiche possono essere fatte via software, configurando gli switch per assegnare i dispositivi a VLAN specifiche.

4. Sicurezza:

In ambito di progettazione senza cambiare la struttura fisica per la sicurezza può essere più conveniente usare una VLAN

* LAN: Maggiore rischio di accessi non autorizzati, poiché tutti i dispositivi possono vedere tutto il traffico.

* VLAN: Maggiore sicurezza attraverso l'isolamento del traffico. Si possono creare segmenti di rete isolati per diversi dipartimenti o per separare il traffico pubblico da quello privato.

5. Efficienza del Traffico:

In fase di progettazione senza cambiare la struttura fisica per rendere più efficiente il traffico.

* LAN: Il traffico di broadcast viene inviato a tutti i dispositivi sulla rete.

* VLAN: Il traffico di broadcast è limitato alla VLAN specifica, riducendo la congestione e migliorando le prestazioni.

6. Configurazione:

* LAN: Basata principalmente su connessioni fisiche e configurazioni di rete standard.

* VLAN: Richiede configurazioni sui dispositivi di rete (switch) per definire e gestire le diverse VLAN.

Esempi di Utilizzo delle VLAN

1. Divisione per Dipartimenti: In un'azienda, si possono creare VLAN separate per il dipartimento vendite, marketing, IT, ecc., per garantire che solo i membri del dipartimento possano accedere alle risorse specifiche.

2. Isolamento di Reti Pubbliche e Private: In un ambiente come una scuola o un ufficio con accesso pubblico al Wi-Fi, si può utilizzare una VLAN per isolare il traffico degli studenti o dei visitatori dal traffico amministrativo.

3. Semplificazione della Gestione della Rete: In un campus universitario, si può assegnare una VLAN per ogni edificio o per ogni tipo di utenza (studenti, docenti, personale amministrativo) per semplificare la gestione e la sicurezza della rete.

Le stesse identiche configurazioni possono essere fatte usando solo le LAN ma aggiungendo nuovi switch e cavi per avere più LAN con topologia a stella.

In conclusione, le VLAN rappresentano un potente strumento per migliorare la gestione, la sicurezza e l'efficienza delle reti locali, offrendo una flessibilità che le reti LAN fisiche tradizionali non possono raggiungere senza aggiungere hardware (switch e cavi ethernet).

ESEMPIO: 2 PROGETTI PER LA STESSA AZIENDA, UNO CON LE LAN, UNO CON LE VLAN

Immaginiamo di dover progettare la rete per un’azienda con due LAN distinte: una per i programmatori ed una per i commerciali di una ditta di informatica.

Nel primo caso le due LAN fisiche sono distinte e non condividono switch. Questa è la soluzione più semplice.

PRIMA SOLUZIONE: DUE LAN FISICHE DISTINTE

Collego gli switch della prima LAN programmatori (192.168.1.0/24) tra di loro e poi collego l'ultimo switch al router per il gateway 192.168.1.254. Collego gli switch della seconda LAN commerciali (192.168.2.0/24) tra di loro e poi collego l'ultimo switch al router per il gateway 192.168.2.254. In tutto uso 6 switch, 3 per la prima LAN e 3 per la seconda LAN. Sul router ho due porte fast-ethernet (schede di rete per le LAN interne) su cui configuro il gateway.

PRIMA SOLUZIONE: USO LE VLAN PER CONDIVIDERE LA STESSA RETE FISICA (che usa gli stessi swirìth) PER DUE LAN VIRTUALI DISTINTE

Collego gli switch della prima LAN FISICA tra di loro e poi collego l'ultimo switch al router.

Ho 3 switch solamente ed sul router ho UNA SOLA porta fast-ethernet (scheda di rete per le due VLAN interne) su cui DEVO CONFIGUARE 2 PORTE VIRTUALI (2 schede di rete VIRTUALI SU UNA FISICA per le 2 VLAN interne, su cui configuro i 2 gateway, uno per ogni VLAN)

Prima VLAN, con identificativo 11 creato sugli switch: programmatori (192.168.1.0/24 con gateway 192.168.1.254)

Seconda VLAN con identificativo 22 creato sugli switch: commerciali (192.168.2.0/24 con gateway 192.168.2.254)

Sugli switch devo creare due VLAN e per ogni porta dello switch indicare a che VLAN appartiene:

Prima VLAN, con identificativo 11

Seconda VLAN con identificativo 22

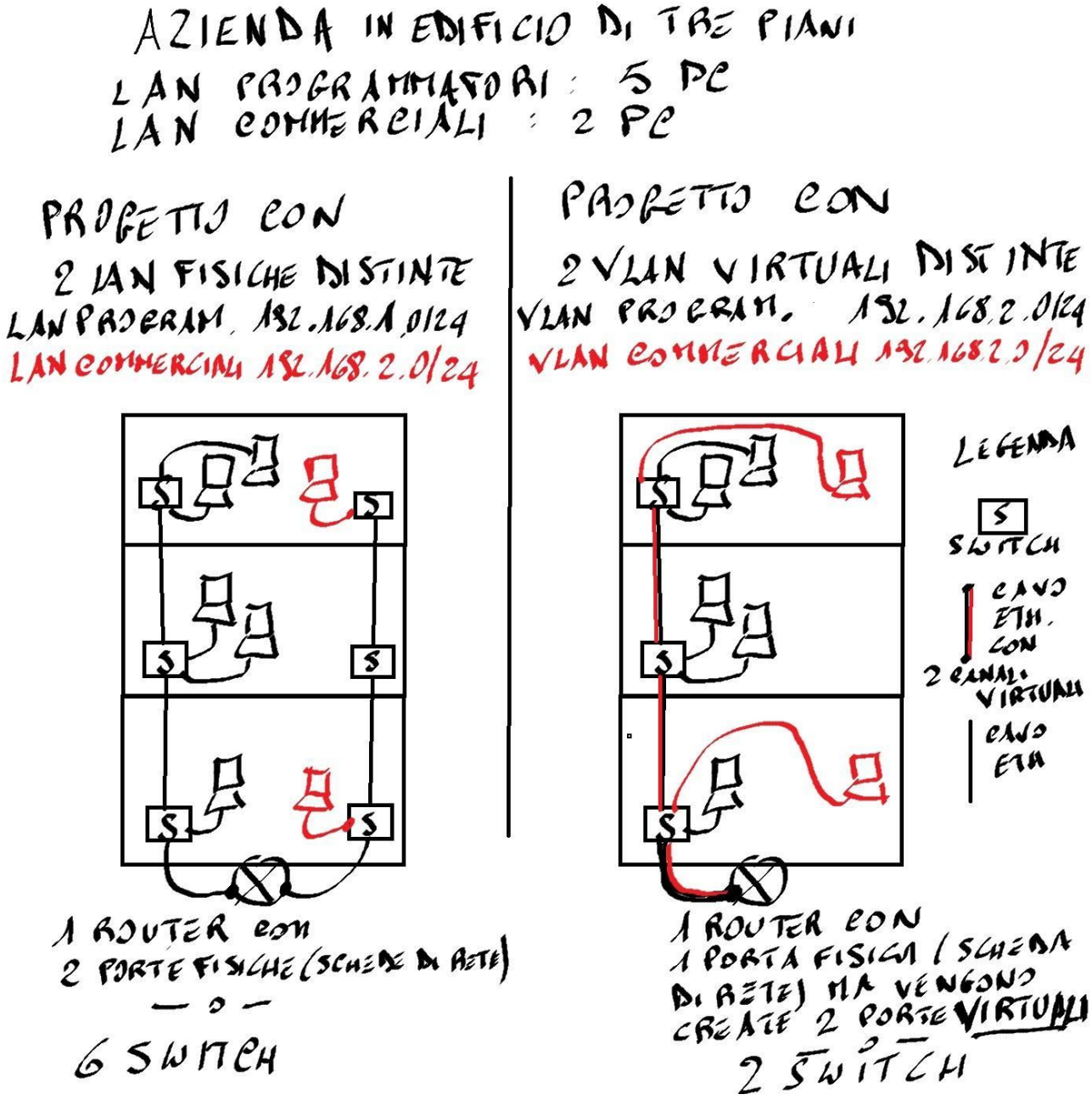
Per le porte dello switch che permettono il collegamento verso il router la modalità della porta deve essere “trunk” (sdoppiata) e devo associare ad essa entrambe le VLAN per permettere a due canali distinti, uno per VLAN di transitare sullo stesso cavo.

Sul router devo configurare due schede di rete virtuale sulla porta fastethernet0/0:

interface “FastEthernet 0/0.10” [Spiegazione: Porta virtuale 0.10 è l'identificativo della scheda di rete virtuale del router]

encapsulation dot1q “numero Vlan” [Spiegazione: indico come “numero Vlan” 11 per indicare la prima VLAN)

ip Address “indirizzo IP del gateway” “maschera di rete” [Spiegazione:indico come “indirizzo IP del gateway” 192.168.1.254 e come “maschera di rete” 255.255.255.0]



Il protocollo VTP e l'inter-VLAN routing (modalità trunk e access)

VTP

Il protocollo VTP, o VLAN Trunking Protocol, è un protocollo utilizzato nei network Ethernet per distribuire automaticamente le informazioni sulle VLAN attraverso una rete troncale. Il principale obiettivo di VTP è semplificare la gestione delle VLAN all'interno di una rete di grandi dimensioni, consentendo agli amministratori di configurare le VLAN su uno switch e far sì che queste informazioni vengano automaticamente propagate a tutti gli altri switch nella rete. 2.

L'inter-VLAN routing:

L'inter-VLAN routing è un metodo che permette il traffico di rete tra diversi VLAN (Virtual Local Area Network). Questo processo è necessario perché i VLAN segmentano una rete LAN in domini di broadcast

separati, e i dispositivi in VLAN diversi non possono comunicare direttamente senza un dispositivo di routing.

Ci sono due modalità principali per configurare le porte sui switch quando si implementa l'inter-VLAN routing:

1. **Modalità Access**: In questa modalità, una porta dello switch è configurata per appartenere a un solo VLAN. Il traffico che passa attraverso una porta in modalità access ha un'etichetta VLAN specifica e può comunicare solo con dispositivi nello stesso VLAN.

2. **Modalità Trunk**: Una porta in modalità trunk può trasportare traffico per più VLAN. Le porte trunk sono generalmente utilizzate per collegare switch tra loro o per collegare uno switch a un router per l'inter-VLAN routing. Il traffico che passa attraverso una porta trunk include etichette VLAN che identificano a quale VLAN appartiene ogni frame di dati.

Differenze:

* La modalità access è limitata a un solo VLAN per porta, mentre la modalità trunk può gestire più VLAN per porta.

* La modalità access viene utilizzata per connettere dispositivi finali che non hanno bisogno di conoscere informazioni sui VLAN, come computer o stampanti. La modalità trunk è usata per connessioni tra switch o tra switch e router per consentire il routing tra VLAN.

MODULO 4. LA SICUREZZA IN RETE

La DMZ

La DMZ, o Zona Demilitarizzata, è un'area intermedia tra due reti di computer, spesso utilizzata come un punto di transizione tra una rete interna privata e una rete esterna pubblica, come Internet. La sua principale funzione è quella di fornire una sorta di "zona neutra" che protegge la rete interna dai potenziali attacchi provenienti dall'esterno, mentre consente al traffico autorizzato di passare attraverso di essa.

In pratica, la DMZ ospita servizi e risorse che devono essere accessibili dall'esterno, come server web, server di posta elettronica o server DNS. Tuttavia, questi server sono isolati dalla rete interna per ridurre il rischio di compromissione della sicurezza. Ciò viene solitamente fatto attraverso la configurazione di regole firewall che limitano il traffico tra la DMZ e la rete interna, permettendo solo il flusso di dati necessario.

In sintesi, la DMZ è una componente chiave nell'architettura di rete per garantire la sicurezza dei dati e dei servizi esposti su Internet.

STRUTTURA DELLA DMZ

La struttura della DMZ dipende dalle esigenze specifiche dell'organizzazione, ma di solito include diversi elementi:

1. **Server pubblici:** Questi sono server accessibili al pubblico, come server web, server di posta elettronica o server DNS. Sono posizionati nella DMZ per consentire l'accesso dall'esterno.

2. **Firewall:** La DMZ è tipicamente protetta da firewall che controllano il traffico in entrata e in uscita tra la rete interna, la DMZ e Internet. I firewall possono essere configurati per permettere solo determinati tipi di traffico alla DMZ e alla rete interna, fornendo così un controllo granulare sulla sicurezza (configurando correttamente la ACL del firewall sul router).

3. **Reverse Proxy:** In alcuni casi, viene utilizzato un reverse proxy per gestire le richieste provenienti dall'esterno e indirizzarle ai server appropriati nella DMZ. Questo può aumentare la sicurezza e migliorare le prestazioni dei servizi pubblici.

4. **Segmentazione della rete:** La DMZ è spesso implementata come una zona separata nella rete dell'organizzazione, con controlli di accesso rigorosi per limitare la comunicazione tra la DMZ e la rete interna. Questo aiuta a prevenire che eventuali compromissioni nella DMZ si diffondano alla rete interna.

In sintesi, la DMZ è progettata per ospitare servizi accessibili al pubblico in un ambiente controllato e sicuro, separato dalla rete interna dell'organizzazione per proteggere i dati sensibili e i sistemi interni.

HTTPS e Il protocollo SSL/TLS per la crittografia

HTTPS sta per HyperText Transfer Protocol Secure. Alcune cose importanti che includono l'HTTPS sono:

1. Crittografia dei dati: HTTPS utilizza la crittografia SSL/TLS per proteggere i dati scambiati tra il browser e il server web, e rende difficile ai 'utenti esterni' intercettare e manipolare le informazioni trasmesse.

2. Integrità dei dati: HTTPS assicura che i dati trasmessi tra il browser e il server non siano stati alterati durante il trasferimento. Questi viene garantito attraverso l'uso di firme digitali.

3. I motori di ricerca (es.Google) tendono a dare priorità ai siti che utilizzano HTTPS nei risultati di ricerca, perché sono un segno di sicurezza e affidabilità.

Quando si accede ad un sito web tramite HTTPS, la comunicazione tra il tuo browser e il server web è crittografata. I dati trasmessi, quindi, sono codificati in modo che solo il mittente e il destinatario possano leggerli. Per stabilire una connessione HTTPS il server web deve avere un certificato SSL/TLS valido. Questo certificato viene rilasciato da un'autorità di certificazione e contiene informazioni sul server web e una chiave pubblica da utilizzare per crittografare i dati.

* SSL (Secure Sockets Layer) e TLS (Transport Layer Security) sono protocolli di sicurezza utilizzati per stabilire una connessione sicura tra il browser e il server web. SSL è stato il primo protocollo utilizzato da HTTPS, ma poi è stato sostituito da TLS a causa di alcuni problemi.

Quindi, in poche parole, sono dei protocolli crittografici di presentazione usati nel campo dell'informatica che permettono una comunicazione sicura dalla sorgente al destinatario (end-to-end) su reti TCP/IP (Internet) fornendo autenticazione, integrità dei dati e confidenzialità operando al di sopra del livello di trasporto.

* TLS che sta per Transport Layer Security, è un protocollo di sicurezza utilizzato per crittografare il traffico su Internet, garantendo che i dati siano accessibili solo ai legittimi destinatari.

Il suo predecessore era SSL, Secure Sockets Layer, e spesso si fa riferimento a TLS con il doppio nome “SSL/TLS” per la sua maggiore notorietà.

Il funzionamento di TLS si basa sulla crittografia asimmetrica per lo scambio delle chiavi e sulla crittografia simmetrica per la protezione del flusso di dati. Durante una connessione TLS, il server invia al client un certificato per autenticarsi. Dopo la verifica del certificato, il client e il server stabiliscono una chiave di sessione crittografata, che viene utilizzata per proteggere la comunicazione.

TLS è fondamentale per la sicurezza online e viene impiegato in vari servizi come HTTPS, email, messaggistica istantanea e VoIP. È importante per proteggere le informazioni sensibili e garantire che non possano essere intercettate o alterate durante la trasmissione

NAT e PAT

Il NAT, o Network Address Translation, è una tecnica utilizzata nei router per convertire gli indirizzi IP delle reti private in indirizzi IP pubblici e viceversa. Questo permette a più dispositivi all'interno di una rete locale di condividere lo stesso indirizzo IP pubblico per accedere a Internet. In sostanza, agisce come un intermediario tra la rete locale e Internet, mascherando gli indirizzi IP interni per garantire la sicurezza e l'efficienza della comunicazione.

Abbiamo tre tipi di NAT:

Nat statico, con associazione uno a uno tra indirizzo IP interno ed esterno

Nat dinamico, con associazione n a m tra indirizzi IP privati interni ed indirizzi IP pubblici esterni

PAT, un Nat statico, con associazione n a 1 tra indirizzi IP privati interni ed un solo indirizzo IP pubblico esterno

Il PAT, o Port Address Translation, è una variante del NAT che consente di mappare più indirizzi IP privati su un singolo indirizzo IP pubblico utilizzando porte TCP/UDP uniche. In altre parole, mentre il NAT statico mappa un indirizzo IP privato a un indirizzo IP pubblico, il PAT va oltre, mappando più indirizzi IP privati a un unico indirizzo IP pubblico utilizzando le porte per distinguere il traffico. Questo consente a molteplici dispositivi all'interno di una rete privata di condividere la stessa connessione Internet, utilizzando una sola risorsa di indirizzo IP pubblico.

Le reti private virtuali VPN

Le VPN hanno radici che risalgono agli anni '90, quando le aziende iniziarono a esplorare modi per collegare in modo sicuro le loro reti aziendali attraverso internet. Tuttavia, il concetto di una rete privata virtuale moderna è stato sviluppato inizialmente dalla Microsoft.

IL protocollo PPTP (Point-to-Point Tunneling Protocol) serve per creare connessioni sicure tra i dispositivi e i server attraverso internet. Questo protocollo è stato uno dei primi ad essere utilizzati per implementare VPN e rimane ancora ampiamente utilizzato oggi.

Successivamente, altri protocolli come L2TP/IPsec (Layer 2 Tunneling Protocol/Internet Protocol Security) e OpenVPN sono stati sviluppati e adottati per migliorare la sicurezza e le prestazioni delle VPN

Le VPN inizialmente erano principalmente utilizzate dalle aziende per consentire ai dipendenti di accedere in modo sicuro alle risorse aziendali da remoto (ad esempio per lo smart working). Tuttavia, con l'aumento delle preoccupazioni sulla privacy online e la necessità di proteggere le comunicazioni personali, le VPN sono diventate popolari anche tra gli utenti domestici (ad esempio per collegarsi in modo anonimo ad un server situato in un altro paese).

Oggi, ci sono numerose aziende e organizzazioni che forniscono servizi VPN, offrendo una vasta gamma di opzioni in termini di protocolli, server e funzionalità aggiuntive come la protezione da malware e la navigazione anonima. Le VPN sono diventate uno strumento essenziale per coloro che desiderano proteggere la propria privacy online e accedere in modo sicuro ai contenuti Internet da qualsiasi luogo.

Riassumendo possiamo dire che una VPN, o Virtual Private Network, è un servizio che crea una connessione sicura e crittografata su Internet tra il tuo dispositivo e un server remoto gestito dal provider VPN. Questo server può essere situato in qualsiasi parte del mondo.

Questo servizio offre diverse funzionalità, tra cui:

Con cisco packet tracer usiamo come server VPN il router.

Criptazione dei dati: Quando ti connetti a una VPN, il tuo dispositivo stabilisce un collegamento sicuro con il server VPN. Tutti i dati inviati e ricevuti durante questa connessione sono crittografati, il che significa che sono resi illeggibili per qualsiasi persona che cerca di intercettarli.

Esempio: per lo smart working si usa di solito una VPN

Mascheramento dell'indirizzo IP: Quando navighi su Internet tramite una VPN, il tuo vero indirizzo IP viene nascosto e sostituito con quello del server VPN. Questo significa che i siti web e gli altri servizi online vedono l'indirizzo IP del server VPN anziché il tuo.

Esempio: mi collego ad un server VPN in Italia che è collegato ad un server VPN in Australia; posso navigare COME SE fossi in Australia

Sicurezza nelle reti non sicure: Le reti Wi-Fi pubbliche, come quelle nei caffè, negozi o hotel, sono spesso non sicure e vulnerabili agli attacchi informatici. Utilizzando una VPN su una rete pubblica, tutti i dati che invii e ricevi sono crittografati, proteggendoti da potenziali minacce di sicurezza.

Esempio: mi collego al wi-fi di una stazione ferroviaria e navigo in sicurezza

In sostanza, una VPN offre una protezione della privacy e della sicurezza online, consentendoti di navigare in modo sicuro su Internet e accedere a contenuti geograficamente limitati. È importante scegliere un provider VPN affidabile e rispettabile e comprendere le loro politiche di registrazione e privacy prima di utilizzare il servizio.

Un esempio di provider VPN è "NORDVPN", ovvero un servizio a pagamento che offre varie funzionalità di quelle elencate in precedenza.

Intranet, extranet e VPN site to site

INTRANET

Intranet è una rete interna privata usata da un'organizzazione per fornire ai dipendenti accesso esclusivo a strumenti aziendali, documenti e servizi utilizzando tecnologie web comuni.

Serve per facilitare la gestione delle risorse umane, la gestione progetti e le comunicazioni interne. L'accesso è protetto da misure di sicurezza come l'autenticazione con username e password per garantire che solo il personale autorizzato possa accedere.

EXTRANET

Un'extranet è un'estensione dell'intranet aziendale che consente a entità esterne come clienti, fornitori e partner di accedere a progetti condivisi e informazioni riservate in modo sicuro.

La sicurezza è fondamentale in un'extranet, quindi l'accesso è regolato tramite VPN o autenticazione forte per assicurare che solo utenti autorizzati possano accedere alle risorse necessarie.

VPN SITE-TO-SITE

Una VPN site-to-site consente di collegare più reti locali (LAN) di diverse sedi, facendole funzionare come un'unica rete.

Questo tipo di VPN è ideale per organizzazioni con molteplici uffici, permettendo la condivisione sicura di risorse tramite un tunnel criptato su Internet, proteggendo i dati da accessi non autorizzati.

In generale, l'intranet migliora l'efficienza interna, l'extranet estende l'efficienza a collaboratori esterni, e le VPN site-to-site uniscono le sedi in una rete sicura, essendo strumenti chiave per una collaborazione efficace e sicura in ambito aziendale.

Intranet, extranet: collegamenti tramite VPN site to site

Per collegare due sedi lontane di una azienda si usa la VPN site to site.

La VPN può essere usata per formare una intranet o una extranet

Una intranet è una rete privata basata su Internet, utilizzata all'interno di un'organizzazione o di un'azienda per facilitare la condivisione di risorse, informazioni e collaborazione tra i dipendenti. È accessibile solo ai membri autorizzati dell'organizzazione e può includere risorse come siti web interni, database, strumenti di comunicazione e altro ancora.

ESEMPIO: l'azienda Barilla è un esempio di intranet. Una intranet può avere varie sedi in città differenti

Una extranet estende il concetto di intranet consentendo l'accesso limitato a determinate parti della rete interna a utenti esterni autorizzati. L'extranet è una porzione dell'intranet che può essere accessibile da utenti esterni attraverso una connessione sicura e controllata.

ESEMPIO: Fiat e Crysler formano una extranet (Due aziende collegate fra di loro in modo sicuro tramite VPN.)

Una VPN site-to-site è una connessione sicura tra due o più reti locali (LAN) attraverso Internet. In pratica, crea un "tunnel" crittografato tra i router o i firewall delle reti coinvolte, offrendo un modo sicuro e affidabile per collegare reti locali distanti attraverso Internet, consentendo alle organizzazioni di comunicare e condividere dati in modo efficiente e sicuro. Una VPN site-to-site permette di collegare in modo sicuro reti locali distanti geograficamente attraverso Internet.

ESEMPIO: sia le intranet che le extranet usano il VPN site to site

I firewall, proxy server e ACL

FIREWALL

1. PRIMA DEFINIZIONE

Un firewall è un dispositivo hardware o un software progettato per monitorare e controllare il traffico di rete, decidendo se permettere o bloccare il passaggio dei dati in base a regole predefinite. Esso funziona a diversi livelli: di rete, strato di trasporto e applicativo. A livello di rete (ACL, access control list), può filtrare il traffico in base agli indirizzi IP sorgente e destinazione. A livello di trasporto, può gestire le connessioni in base ai protocolli come TCP e UDP. A livello applicativo (PROXY SERVER), può controllare il traffico in base alle applicazioni specifiche utilizzate .

SECONDA DEFINIZIONE

Il firewall è un componente di sicurezza informatica che può essere implementato sia a livello hardware che software. Questo sistema è progettato per monitorare e controllare il traffico di rete, decidendo se permettere o bloccare il passaggio dei dati in base a regole predefinite (PERMIT/DENY). Il firewall può

operare a diversi livelli, come il livello di rete, il livello di trasporto e il livello applicativo, e può essere configurato per proteggere una rete o un singolo dispositivo da minacce esterne e interne. Le regole di filtraggio del firewall possono essere personalizzate per soddisfare le esigenze specifiche di sicurezza di un'organizzazione o di un utente.

Il firewall può essere configurato in diversi punti all'interno di un'infrastruttura IT, a seconda delle esigenze specifiche:

1. Dispositivi di rete: Molti router includono funzionalità di firewall che possono essere configurate direttamente tramite l'interfaccia di amministrazione web del dispositivo.

ESEMPIO: ROUTER CISCO CON CISCO PACKET TRACER

2. Server: I sistemi operativi server, come Windows Server e Linux, includono spesso un software firewall integrato che può essere configurato per proteggere il server e le applicazioni in esecuzione su di esso (quando infatti noi disegnamo la rete rappresentiamo il firewall come un server posto subito dopo il router ma poi lo immaginiamo sempre configurato come software sul router)

PERSONAL FIREWALL(DEFENDER per S.O. Windows)

1. Endpoint (singoli pc di una rete): il firewall possono essere implementati sui dispositivi endpoint, come computer desktop, laptop e dispositivi mobili. Questi firewall possono essere configurati tramite il sistema operativo o utilizzando software di terze parti.

FIREWALL NEL CLOUD

2. Cloud: Nei servizi cloud, il firewall può essere configurato per proteggere le risorse ospitate nel cloud, come macchine virtuali, database e servizi web. Le piattaforme cloud come AWS, Azure e Google Cloud offrono strumenti per configurare e gestire i firewall.

PROXY SERVER

Un server proxy è un server che funge da intermediario tra il tuo dispositivo e Internet

Compie 3 funzioni principali :

1. PRIVACY E SICUREZZA

* Nascondere l'indirizzo IP: Il server proxy nasconde il tuo vero indirizzo IP, sostituendolo con il proprio.

* Monitoraggio del traffico: I server proxy possono essere utilizzati per monitorare e registrare il traffico di rete per scopi di sicurezza o di audit.

2. CONTROLLO

* Filtraggio dei contenuti: Può essere configurato per bloccare o filtrare determinati tipi di contenuti o siti web.

* Controllo dell'accesso: Può essere utilizzato per limitare l'accesso a determinati siti web o risorse sulla rete, garantendo la conformità alle politiche aziendali o di rete.

3. CACHE

* Caching: I server proxy possono memorizzare temporaneamente le risorse web richieste dai client, riducendo il carico sui server di origine e migliorando la velocità di risposta complessiva.

* Accelerare l'accesso ai dati: Un server proxy può memorizzare le copie locali dei dati frequentemente richiesti, riducendo così il tempo necessario per accedere a tali dati e migliorando le prestazioni complessive della rete.

LE ACL (ACCESS CONTROL LIST)

ACL, acronimo di Access Control List, è una lista di regole applicata ai dispositivi di rete per controllare il traffico in entrata e in uscita. Le ACL possono essere utilizzate per aumentare la sicurezza della rete, limitando l'accesso a determinate risorse o segmenti di rete.

Esistono due tipi principali di ACL: standard e estese.

ACL Standard: Utilizzano solo l'indirizzo IP di origine per filtrare il traffico. Sono identificate dai numeri da 1 a 99 e 1300 a 1999.

ACL Estese: Possono filtrare il traffico in base a vari criteri, inclusi indirizzi IP di origine e destinazione, protocolli, numeri di porta, ecc. Sono identificate dai numeri da 100 a 199 e 2000 a 2699.

Configurazione di ACL su un Router per una DMZ e una LAN Interna

Scenario:

La LAN interna ha l'intervallo IP 192.168.1.0/24.

La DMZ ha l'intervallo IP 192.200.2.0/24.

L'indirizzo IP pubblico del router è 203.0.113.1.

Il web server è nella DMZ accessibile a tutti

il database è nella LAN interna accessibile solo al web server (che con un servizio di autenticazione con nome utente e password concede gli accessi agli utenti)

Si desidera consentire l'accesso HTTP (porta 80) e HTTPS (porta 443) alla DMZ dal mondo esterno, mentre si blocca qualsiasi altro traffico.

Si desidera consentire tutto il traffico dalla LAN interna verso la DMZ e verso Internet.

Si desidera bloccare il traffico dall'esterno nella LAN

Si desidera consentire al webserver di accedere alla LAN interna dove è posizionato il suo database.

Passaggi per la Configurazione:

Creazione delle ACL :

A) IN ENTRATA VERSO DMZ (Per il traffico in entrata verso il web server 192.200.2.10 nella DMZ:)

access-list 100 permit tcp any host 192.200.2.10 eq 80

access-list 100 permit tcp any host 192.200.2.10 eq 443

access-list 100 deny ip any any

Spiegazione dei Comandi:

access-list 100 permit tcp any host 192.200.2.10 eq 80: Permette il traffico TCP da qualsiasi fonte verso l'indirizzo IP della DMZ (192.200.2.10) sulla porta 80.

access-list 100 permit tcp any host 192.200.2.10 eq 443: Permette il traffico TCP da qualsiasi fonte verso l'indirizzo IP della DMZ (192.200.2.10) sulla porta 443.

access-list 100 deny ip any any: Blocca tutto il traffico rimanente.

B)Per il traffico dalla LAN interna:

B1)IN USCITA VERSO DMZ O INTERNET:

access-list 101 permit ip 192.168.1.0 0.0.0.255 any

Spiegazione dei Comandi:

access-list 101 permit ip 192.168.1.0 0.0.0.255 any: Permette tutto il traffico IP dall'intervallo 192.168.1.0/24 verso qualsiasi destinazione.

B2)IN ENTRATA VERSO LA LAN:

access-list 102 deny ip any 192.168.1.0 0.0.0.255

access-list 103 permit ip host 192.200.2.10 192.168.1.0 0.0.0.255

Spiegazione dei Comandi:

la lista 102 blocca il traffico in ingresso sulla LAN dall'esterno

la lista 103 consente al solo web server di accedere alla LAN interna dove è posizionato il database

Questa configurazione assicura che solo il traffico HTTP e HTTPS può raggiungere la DMZ dall'esterno, mentre tutto il traffico dalla LAN interna è consentito sia verso la DMZ che verso Internet. Protegge inoltre il database e la LAN interna da attacchi hacker.

MODULO 5. LE CONNESSIONI CABLATE E WIRELESS p.120-134 WLAN p.150-168 Le reti mobili

Le WLAN e gli access point (reti wi-fi, IEEE 802.11 e WPA2)

WLAN (Wireless Local Area Network) è un tipo di LAN che permette agli utenti di connettersi a internet ed altre risorse di rete utilizzando la tecnologia wireless ed utilizza lo standard IEEE 802.11 (serie di specifiche che definiscono i protocolli usati in internet, in particolare l' IEEE 802.11 è specifico delle reti wireless)

I dati vengono condivisi tramite degli Access Point AP, dispositivo di rete che funge da 'ponte' tra dispositivi connessi allo stesso. Gli AP ricevono i dati inviati dai dispositivi wireless e li inoltrano sulla rete cablata, permettendo così ai dispositivi wireless di comunicare con altri dispositivi sulla rete o di accedere a risorse Internet.

L'AP è composto da:

* SSID: Service Set Identifier, ovvero il nome della rete wireless; comunica con un Frame (pacchetto di dati a livello datalink) detto beacon

* Password (non obbligatoria): utilizza prevalentemente il protocollo WPA2:

* Wi-Fi Protected Access 2, versione successiva del WPA, assicura una crittografia sicura, usufruendo del protocollo AES (Advanced Encryption Standard) per crittografare i dati e prevenire l'intercettazione da parte di terze parti non autorizzate; senza intaccare le performance, molto più personalizzabile rispetto al predecessore (è in sviluppo la WPA3, 1° edz. 2019)

In breve, le reti WLAN si basano sugli standard IEEE 802.11 e consentono ai dispositivi di comunicare senza fili. Gli access point sono dispositivi che consentono ai dispositivi wireless di connettersi alla rete cablata. E WPA2 è uno standard di sicurezza crittografica utilizzato per proteggere le reti WLAN dagli accessi non autorizzati e per garantire la riservatezza delle comunicazioni wireless.

LE RETI MOBILI

Le reti mobili (1G, 2G, 3G, 4G e 5G)

Le reti mobili sono sistemi di comunicazione wireless che consentono ai dispositivi mobili di connettersi tra loro e accedere ai servizi di comunicazione, dati e internet. Queste reti consentono agli utenti di effettuare chiamate, inviare messaggi, navigare sul web e utilizzare applicazioni su dispositivi come smartphone, tablet e computer portatili.

Le reti mobili funzionano attraverso una serie di torri o antenne che trasmettono segnali radio per coprire un'area geografica.

I dispositivi mobili si connettono a queste torri e trasmettono i loro segnali attraverso onde radio.

Ci sono diversi standard di reti mobili, o "generazioni", che sono evolute nel tempo:

* 1G: La prima generazione, introdotta negli anni ’80, consentiva solo chiamate vocali analogiche.

* 2G: Introdotto alla fine degli anni ’90, consentiva chiamate vocali digitali, messaggistica SMS e MMS e servizi di dati a bassa velocità.

* 3G: Introdotta agli inizi degli anni 2000, offriva una maggiore velocità di trasmissione dati, permettendo l’accesso a internet mobile, videochiamate e servizi avanzati.

* 4G: Introdotto nel 2009, offriva velocità di trasmissione dati molto più elevate rispetto alla 3G, consentendo lo streaming video ad alta definizione, i giochi online e una migliore esperienza di navigazione web.

* 5G: La generazione più recente, lanciata negli ultimi anni, offre velocità di trasmissione dati ancora più elevate, riduzione del ritardo di trasmissione (latenza), maggiore capacità della rete e supporto per un numero massivo di dispositivi connessi simultaneamente.

Le reti mobili continuano a evolversi per soddisfare le crescenti esigenze di connettività e supportare nuove tecnologie e applicazioni

routing diretto e indiretto

Il routing diretto e indiretto sono due approcci nella gestione dei pacchetti di dati all'interno di una rete mobile. Nel routing diretto, un pacchetto viene inviato direttamente al suo destinatario utilizzando un percorso predefinito, che può essere determinato tramite algoritmi come il più breve cammino o il percorso migliore. Un esempio è quando invii un messaggio a un amico su una piattaforma di messaggistica istantanea: il messaggio va direttamente al suo dispositivo attraverso un percorso prestabilito su Internet.

D'altra parte, nel routing indiretto, i pacchetti vengono instradati attraverso una serie di nodi intermedi prima di raggiungere la destinazione finale. Questi nodi intermedi sono spesso router che prendono decisioni sul percorso migliore da prendere in base alle informazioni contenute nei pacchetti stessi o nelle tabelle di routing. Un esempio comune di routing indiretto è l'utilizzo di più algoritmi di instradamento dinamico su router differenti su Internet. Quando invii un pacchetto di dati su Internet, questo può passare attraverso diversi router prima di raggiungere la destinazione finale senza che si sappia in anticipo la strada che percorrerà.

La principale differenza tra i due è che nel routing diretto il percorso è già noto e fisso, mentre nel routing indiretto il percorso può variare in base alle condizioni di rete e alle decisioni prese dai router lungo il percorso.

FTTH e ADSL per le reti cablate (cenni)

“FTTH” è l’acronimo di “Fiber to the home”, un tipo di architettura di rete che adopera la fibra ottica dal fornitore all’utente finale. La FTTH fa parte di una più ampia famiglia, denominata “FTTx”. In questa famiglia, i vari tipi di architettura si distinguono in base alla distanza tra il fornitore e l’utente finale. Alcuni tipi di architettura FTTx sono:

* FTTH, “Fiber To The Home”, dove la fibra ottica arriva fino all’appartamento dell’utente;

* FTTB, “Fiber To The Basement”, dove la fibra ottica arriva fino all’edificio dell’utente

* FTTC, “Fiber To The Center”, dove la fibra ottica arriva in una cabina di smistamento entro 300m dall’utente

* FTTN, “Fiber To The Node”, dove la fibra ottica arriva fino a uno snodo distante più di 300m.

Il mezzo trasmissivo adoperato per la trasmissione è la fibra ottica, un materiale, generalmente costituito da filamenti vetrosi, in grado di condurre al suo interno la luce. I cavi in fibra ottica adoperati per la trasmissione di dati sono stati standardizzati per la prima volte nel IEEE 802.3j.

“ADSL”, acronimo di Asymmetric Diagonal Subscriber Line, è una tecnologia che permette, tramite l’attivazione da parte di un ISP e l’installazione di un modem, la connessione ad internet tramite il doppino telefonico (Doppino ritorto). Questa tecnologia è economica rispetto ad altre soluzioni come la FTTH, considerando anche che non necessita dell’installazione di nuovi cavi, ma è soggetta a velocità di trasmissione limitate, in alcuni casi insufficienti (le moderne ADSL arrivano a circa 50 Mb/s in download, valore basso per servizi di streaming ad alta definizione o utilizzi professionali).

MODULO 6. PROGETTAZIONE DI UNA RETE

Rete intranet con router, LAN, DMZ, web server, database server

Una rete intranet con router, DMZ, LAN, web server e database server è un ambiente informatico complesso e strutturato utilizzato all'interno di un'organizzazione per gestire e condividere informazioni in modo sicuro ed efficiente.

Ecco come funzionano i componenti principali:

1. Router: Il router è il dispositivo di rete che gestisce il flusso di dati tra la rete intranet e altre reti, come internet. Regola il traffico di rete e indirizza i pacchetti dati verso le destinazioni appropriate. In una rete intranet, il router è configurato per garantire la sicurezza e il controllo degli accessi.

2. DMZ (Demilitarized Zone): La DMZ è una zona separata dalla rete LAN che fornisce accesso alle richieste esterne, come web server. I server DMZ sono configurati in modo che siano accessibili dall'esterno, ma limitati nell'accesso alla rete interna.

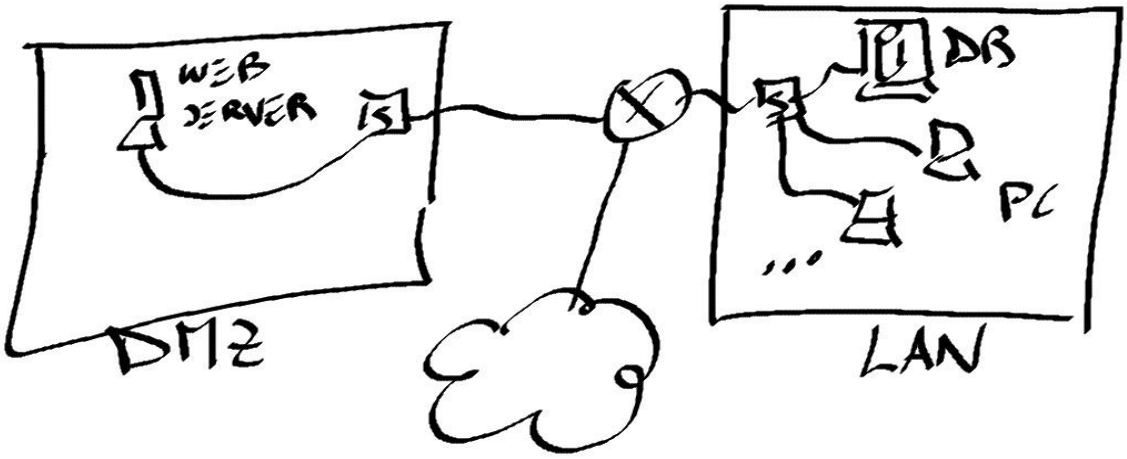
3. LAN (Local Area Network): La LAN è la parte principale della rete intranet, dove sono collegati tutti i dispositivi e le risorse interni dell'organizzazione. Questa include computer, stampanti, dispositivi di archiviazione di rete e altri dispositivi connessi in modo che possano comunicare e condividere dati tra loro.

4. Web Server: Il web server è un server dedicato che ospita siti web, applicazioni web e servizi web all'interno dell'intranet. Fornisce pagine web e risorse online agli utenti all'interno dell'organizzazione. Il web server può essere configurato per accedere ai dati dal database server per fornire informazioni dinamiche ai visitatori del sito web.

5. Database Server: Il database server è un server dedicato che gestisce e archivia i dati utilizzati dalle applicazioni aziendali e dai servizi web. Conserva informazioni come dati dei clienti, dati di inventario, informazioni sui dipendenti e altro ancora. Il database server può essere accessibile solo all'interno della LAN e può essere protetto da misure di sicurezza come autorizzazioni di accesso e crittografia dei dati.

Questi componenti lavorano insieme per creare un ambiente sicuro e funzionale all'interno dell'organizzazione, consentendo ai dipendenti di accedere e condividere informazioni in modo efficiente e protetto.

SCHEMA DELLA SEDE DI UNA AZIENDA (ad esempio la sede di una azienda informatica di Torino)



ACL del FIREWALL su ROUTER

- Tutti possono accedere alla DMZ
- Nessuno (tranne il web server) può accedere alla LAN
- Il web server accede solo al database (DB) posto nella LAN protetta

Reti cablate e reti LAN con access point

Reti Cablate

Le reti cablate si basano sull'utilizzo di cavi fisici per la trasmissione dei dati tra i dispositivi di rete. I dispositivi come computer, switch, router e server sono collegati tra loro attraverso cavi Ethernet o altri tipi di cavi di rete. Le reti cablate offrono solitamente una connettività più stabile e veloce rispetto alle reti wireless, ed è più facile controllare l'ambiente fisico della rete.

Configurazione:

Topologia fisica (per le LAN): Le reti cablate utilizzano cavi fisici per connettere i dispositivi. Le topologie comuni per le reti LAN includono a stella, ad anello e a maglia.

Dispositivi di rete: I dispositivi comuni in una rete cablata includono switch, router, hub e modem. I switch sono spesso utilizzati per creare connessioni point-to-point tra i dispositivi.

Cavi di rete: I cavi Ethernet sono ampiamente utilizzati nelle reti cablate. È importante utilizzare cavi di buona qualità per garantire una connettività affidabile.

Reti LAN con Access Point

Le reti LAN con access point sono reti wireless che utilizzano tecnologie radio per trasmettere dati tra i dispositivi. Gli access point sono dispositivi che fungono da ponte tra i dispositivi wireless e la rete cablata, consentendo ai dispositivi wireless di connettersi alla rete. Le reti con access point offrono maggiore flessibilità e mobilità rispetto alle reti cablate, consentendo ai dispositivi di connettersi senza dover essere fisicamente collegati a un cavo di rete.

Configurazione:

Topologia wireless: Le reti con access point utilizzano tecnologie wireless per connettere i dispositivi. Gli access point agiscono come ponti tra i dispositivi wireless e la rete cablata, consentendo loro di accedere alla rete.

Dispositivi di rete: Oltre agli access point, le reti wireless possono avere anche router, switch e altri dispositivi di rete cablata. È importante configurare correttamente gli access point per garantire una copertura adeguata e una connettività affidabile.

Sicurezza: Le reti wireless richiedono particolare attenzione alla sicurezza, perché i segnali wireless possono essere intercettati da persone non autorizzate. È importante utilizzare crittografia e autenticazione per proteggere la rete e i dati trasmessi.

Inoltre bisogna aggiungere che le due reti(cablate e wireless) vengono integrate per fornire connettività in diverse aree e per diversi tipi di dispositivi.

Le WAN extranet con due o più router e VPN site to site

Una WAN (Wide Area Network) extranet con due o più router e VPN site-to-site è una configurazione comune per connettere reti aziendali geograficamente distanti in modo sicuro e affidabile. In questa configurazione, i router sono collegati attraverso una rete pubblica, come ad esempio Internet, e utilizzano tunnel VPN site-to-site per creare una connessione sicura e crittografata tra le sedi remote.

Ecco come funziona generalmente una connessione WAN extranet con diversi router VPN site to site:

Configurazione dei router

Ogni router viene configurato con le informazioni necessarie per stabilire e gestire la connessione VPN site to site. Queste informazioni includono gli indirizzi IP pubblici dei router, le chiavi di crittografia e altri parametri di configurazione VPN.

Creazione del tunnel VPN

Una volta configurati, i router stabiliscono un tunnel crittografato VPN tra di loro attraverso Internet. Questo tunnel crittografato garantisce la sicurezza e la privacy dei dati trasmessi tra le sedi.

Instradamento del traffico

Dopo aver stabilito il tunnel VPN, i router sono in grado di instradare il traffico tra le reti locali attraverso la connessione VPN. Questo consente alle sedi remote di comunicare tra loro come se fossero sulla stessa rete locale.

Gestione della connessione

I router monitorano costantemente lo stato della connessione VPN e gestiscono eventuali problemi o interruzioni della connessione. Questo assicura che la connessione tra le sedi rimanga attiva e affidabile nel tempo.

Questa configurazione è molto utile per le aziende con sedi distanti che necessitano di condividere risorse e dati in modo sicuro e efficiente. La crittografia VPN garantisce che i dati trasmessi attraverso la connessione siano protetti e siano colpiti da manipolazioni non autorizzate.

Reti mobili a supporto di una rete WAN

Le reti mobili sono sistemi di comunicazione che consentono agli utenti di connettersi ad Internet utilizzando dispositivi mobili come smartphone, tablet o computer portatili. Queste reti si basano su tecnologie wireless e consente agli utenti di accedere ad Internet da ovunque ci sia una copertura di rete mobile.

La WAN (Wide Area Network) è un tipo di rete informatica che copre un' ampia area geografica. Questa rete permette agli utenti di connettersi e comunicare tra loro anche se si trovano in luoghi diversi.

Le reti mobili consentono agli utenti di accedervi da remoto, possono essere inoltre utilizzate come backup di connessione per garantire continuità operativa in caso di interruzioni.

Inoltre le reti mobili possono essere usate per estendere la copertura di rete WAN in aree dove non è disponibile una connessione cablata.