Sicurezza nei Protocolli TCP/IP

I firewall utilizzano tecniche di **packet filtering** per difendere la propria rete; a tal proposito rivediamo gli strati software che costituiscono l'architettura TCP/IP.

Un **firewall** è un sistema di sicurezza (hardware, software o basato su cloud) che monitora, filtra e controlla il traffico di rete in entrata e in uscita, sulla base di regole predefinite. Lo scopo principale di un firewall è proteggere le reti e i dispositivi da accessi non autorizzati, attacchi informatici e altre minacce.

Il **packet filtering** è una tecnica di controllo del traffico di rete utilizzata dai firewall per analizzare i pacchetti in transito e decidere se consentirli o bloccarli in base a regole definite dall'amministratore. Queste regole vengono applicate a specifici attributi del pacchetto.

Il modello **TCP/IP** (Transmission Control Protocol/Internet Protocol) è un insieme di protocolli utilizzati per connettere dispositivi in rete e permettere loro di comunicare. È la base delle reti moderne, inclusa Internet.

Strati software che costituiscono l'architettura TCP/IP

L'architettura **TCP/IP** è composta da **strati software** che suddividono le responsabilità nella comunicazione di rete. Questi strati lavorano insieme per consentire lo scambio di dati tra dispositivi in rete. Gli **strati software** principali del modello TCP/IP sono:

1. Livello Applicazione

- È il livello più alto e riguarda le **applicazioni utente**.
- Qui si trovano i protocolli che permettono alle applicazioni di scambiare dati in rete.
- **Funzioni principali**:
  - Fornire servizi agli utenti finali.
  - Gestire il formato e la semantica dei dati.
- **Protocolli principali**:
  - **HTTP/HTTPS**: Per la navigazione web.
  - **SMTP**: Per l'invio di email.
  - **FTP**: Per il trasferimento di file.
  - **DNS**: Per la risoluzione di nomi di dominio.
  - **POP3**: Per scaricare email (Outlook, Thunderbird o Apple Mail)

---

2. Livello Trasporto

- Fornisce la **comunicazione end-to-end** tra i dispositivi (garantisce che i dati possano essere inviati da un dispositivo mittente a un dispositivo

destinatario, gestendo tutti gli aspetti della comunicazione lungo il percorso).
    - La **comunicazione end-to-end tra i dispositivi** si riferisce alla capacità di stabilire una connessione **diretta e affidabile** tra due dispositivi, consentendo lo **scambio di dati** dal mittente al destinatario in modo completo e senza interruzioni. Questo concetto è centrale in reti come **Internet** e viene implementato principalmente grazie ai **protocolli di trasporto** come **TCP** (Transmission Control Protocol).
    - "End-to-end" significa che i dati inviati da un dispositivo sorgente raggiungano direttamente il dispositivo destinatario, attraversando la rete (router, switch, server intermedi) ma mantenendo l'integrità e la sequenza dei dati.
      In pratica:
        - **Mittente**: Genera i dati e li invia.
        - **Rete**: Trasporta i dati attraverso più nodi intermedi.
        - **Destinatario**: Riceve i dati nella stessa forma in cui sono stati inviati.
- Si occupa di frammentare e ricomporre i dati, garantendo la consegna.
- **Protocolli principali**:
    - **TCP (Transmission Control Protocol)**:
        - Connessione orientata.
        - Garantisce che i dati arrivino correttamente e nell'ordine giusto.
        - Se un pacchetto si perde, viene ritrasmesso automaticamente.
        - Regola la quantità di dati che il mittente può inviare prima di ricevere una conferma, evitando di sovraccaricare il destinatario.
    - **UDP (User Datagram Protocol)**:
        - Non connessione orientata, quindi più veloce.
        - Utilizzato per applicazioni che non necessitano di affidabilità completa (es. streaming).

---

3. Livello Internet

- Si occupa di **instradare i pacchetti** di dati attraverso le reti.
- Gestisce l'indirizzamento dei dispositivi e l’instradamento delle informazioni verso la destinazione corretta, anche su reti differenti.
- **Protocolli principali**:
    - **IP (Internet Protocol)**:
        - Indirizza e trasporta i pacchetti (es. IPv4, IPv6).
    - **ICMP (Internet Control Message Protocol)**:
        - Diagnostica problemi di rete (es. comando "ping" - strumento di rete utilizzato per testare la raggiungibilità di un dispositivo (host) all'interno di una rete IP).

- **ARP (Address Resolution Protocol)**:
  - Traduce gli indirizzi IP in indirizzi MAC (identificatori univoci assegnati a ogni scheda di rete (NIC, Network Interface Card) di un dispositivo dal produttore della scheda di rete).

Funzioni principali del Livello Internet

1. **Instradamento dei pacchetti**:
   Determina il percorso migliore per far viaggiare i pacchetti attraverso una rete interconnessa di router.
2. **Indirizzamento**:
   Utilizza indirizzi IP per identificare univocamente mittenti e destinatari.
3. **Frammentazione e ricomposizione**:
   Divide pacchetti troppo grandi in frammenti, per poi ricostruirli al livello di destinazione.
4. **Consegna "best effort" ()**:
   Non garantisce l'arrivo dei pacchetti o l'ordine corretto. La responsabilità di garantire la connessione affidabile è delegata al livello di Trasporto (es. TCP).

Funzionamento del TCP/IP

- I dati vengono suddivisi in **pacchetti**.
- Ogni pacchetto include informazioni su:
  - Mittente e destinatario (indirizzi IP).
  - Numero di sequenza per ricomporre i dati.
- **TCP** garantisce che i pacchetti arrivino correttamente e nell'ordine giusto.
- **IP** instrada i pacchetti verso la destinazione corretta.

Esempio di comunicazione con TCP/IP

Supponiamo che un utente visiti un sito web:

1. **Applicazione**: Il browser utilizza il protocollo HTTP per richiedere una pagina web.
2. **Trasporto**: TCP divide la richiesta in pacchetti e li numera.
3. **Internet**: IP instrada i pacchetti verso il server del sito web.
4. **Accesso alla Rete**: I pacchetti viaggiano tramite Ethernet o Wi-Fi.

Il processo inverso avviene per ricevere la risposta dal server.

---

4. Livello Accesso alla Rete (o Collegamento Dati)

- È il livello più basso e si occupa della trasmissione dei dati sul mezzo fisico (es. cavi, onde radio).

- Include i protocolli per il funzionamento dei dispositivi hardware, come schede di rete e router.
- **Funzioni principali**:
  - Gestire l'invio e la ricezione di pacchetti sul mezzo fisico.
  - Affrontare errori di trasmissione.
- **Protocolli principali**:
  - **Ethernet**: Per reti cablate.
  - **Wi-Fi**: Per reti wireless.

Confronto con il modello OSI

L'architettura TCP/IP ha **4 livelli**, mentre il modello OSI ne ha **7**. Ogni strato di TCP/IP raggruppa uno o più strati del modello OSI:

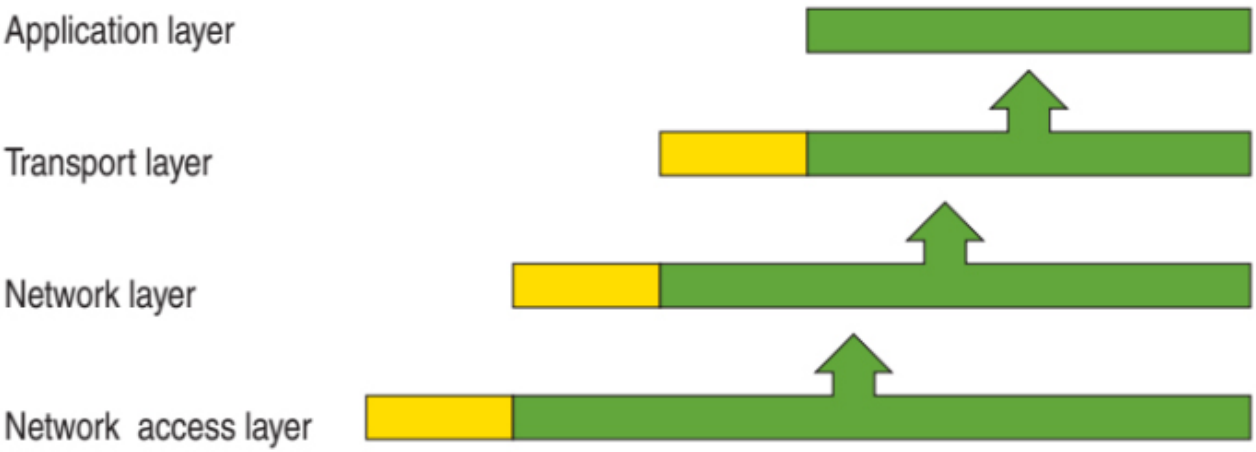
Livello TCP/IP	Strati del modello OSI
Livello Applicazione	Applicazione, Presentazione, Sessione
Livello Trasporto	Trasporto
Livello Internet	Rete
Livello Accesso alla Rete	Collegamento Dati, Fisico

A ogni livello un pacchetto si compone di due parti chiamate intestazione (**header**) e dati (**payload**).

Questo principio è fondamentale nel funzionamento dei protocolli di rete, in cui ogni livello dell'architettura di rete (ad esempio l'architettura TCP/IP o il modello OSI) gestisce i dati in un formato standard composto da:

1. **Intestazione (Header)**
   L'intestazione è un insieme di informazioni aggiunte al pacchetto dai protocolli del livello corrente. Queste informazioni vengono utilizzate per la gestione e l'elaborazione del pacchetto.
2. **Dati (Payload)**
   Il payload è il contenuto effettivo del pacchetto, ovvero i dati che devono essere trasmessi (ad esempio, una pagina web, un file, o un messaggio). Può anche includere il pacchetto proveniente dal livello superiore.

Quando i dati vengono inviati attraverso i vari livelli, ogni livello aggiunge la propria intestazione al pacchetto. Questo processo è noto come **incapsulamento**.



I **pacchetti IP** possono essere di tipo **unicast**, cioè vengono spediti verso un unico host di destinazione (si intende che un pacchetto o un messaggio inviato attraverso una rete è indirizzato a un **singolo dispositivo specifico** (host), identificato dal suo indirizzo univoco), **multicast**, cioè spediti a un gruppo di host (I dati vengono inviati a un gruppo specifico di dispositivi - ad esempio, streaming live a più utenti) oppure **broadcast**, cioè indirizzati a tutti gli host che possono riceverli nell'ambito della rete logica di appartenenza del mittente (I dati vengono inviati a tutti gli host di una rete locale). Gli indirizzi di multicast e di broadcast sono indirizzi di **destinazione** e non di **origine**, altrimenti potrebbero essere utilizzati da una procedura di attacco che utilizzerebbe una macchina di destinazione per amplificare l'attacco. Un firewall quindi deve rifiutare i pacchetti destinati a un indirizzo di broadcast e i pacchetti il cui indirizzo di origine sia un multicast o un broadcast (Non hanno senso come indirizzi di origine).

l'intestazione del pacchetto IP include effettivamente un campo **Options**. Questo campo è opzionale e serve a fornire funzionalità aggiuntive non coperte dagli altri campi standard dell'intestazione. Tuttavia, è raramente utilizzato nelle reti moderne a causa della complessità che introduce e dell'impatto negativo sulle prestazioni del routing. Lo scopo del source routing è di aggirare i router che possiedono routing table guaste o non corrette. In pratica, il source routing viene comunemente utilizzato solamente dagli attaccanti che tentano di aggirare le misure di sicurezza costringendo i pacchetti a seguire cammini inaspettati. Alcuni sistemi di protezione seguono l'approccio di scartare tutti quei pacchetti che hanno le opzioni IP impostate, senza nemmeno analizzarle. La **tabella di routing** (routing table) è un elemento essenziale di qualsiasi dispositivo di rete abilitato al routing, come router, switch di livello 3 o computer configurato per l'inoltro dei pacchetti. Contiene le informazioni necessarie per determinare il percorso migliore per inviare un pacchetto verso una destinazione specifica.

Una delle caratteristiche del protocollo IP è la sua capacità di dividere un pacchetto di grandi dimensioni, che altrimenti non potrebbe attraversare una

rete, in pacchetti più piccoli chiamati **frammenti**, che possono attraversare la rete per essere **riassemblati** nell'host di destinazione.

Qualunque router può decidere di frammentare un pacchetto, anche se un campo posto nell'intestazione IP può essere utilizzato per evitare che un router frammenti un pacchetto. Tale campo viene utilizzato per conoscere la **MTU** (**Maximun Transmission Unit**) attraverso una tecnica che determina quale sia il pacchetto più grande che possa essere inviato a un host senza subire la frammentazione.

Questa caratteristica del protocollo IP è nota come **frammentazione e riassemblaggio**. È fondamentale per consentire ai pacchetti di grandi dimensioni di attraversare reti con **MTU** (**Maximum Transmission Unit**) più piccole rispetto alla dimensione originale del pacchetto. Vediamo come funziona:

Frammentazione

La frammentazione avviene quando un pacchetto IP supera l'MTU di un segmento di rete lungo il suo percorso. La **MTU** è la dimensione massima di un pacchetto che una rete può trasmettere senza frammentazione. Ad esempio, la MTU standard per Ethernet è 1500 byte.

Processo:

1. **Suddivisione:** Il pacchetto viene suddiviso in frammenti più piccoli, ciascuno con un'intestazione IP completa.
2. **Identificazione:** Ogni frammento conserva lo stesso **identificativo del pacchetto originale** (Identification Field), per consentire la ricostruzione all'arrivo.
3. **Flag e Offset:**
    - **MF (More Fragments):** Indica se ci sono frammenti successivi.
    - **Fragment Offset:** Specifica la posizione del frammento rispetto all'inizio del pacchetto originale.

Riassemblaggio

Il processo di riassemblaggio avviene solo all'**host di destinazione**. I router intermedi non riassemblano i pacchetti frammentati, ma possono ulteriormente frammentarli se necessario.

Dettagli:

- L'host utilizza l'identificativo del pacchetto e il campo Fragment Offset per ricostruire i frammenti nell'ordine corretto.

- Se uno o più frammenti non arrivano, il pacchetto viene considerato perso.

Esempio Pratico

Supponiamo di avere un pacchetto di dimensioni 4000 byte che deve attraversare una rete con un MTU di 1500 byte. L'intestazione IP è di 20 byte.

- **Dimensione utile per i dati (payload):** 1500 - 20 = **1480 byte**.
- **Numero di frammenti:**

$$\text{Numero di frammenti} = \lceil \frac{4000}{1480} \rceil = 3$$

- **Dettagli frammenti:**
  - Primo frammento: 1480 byte (1480 dati + 20 intestazione), Offset = 0.
  - Secondo frammento: 1480 byte (1480 dati + 20 intestazione), Offset = 1480.
  - Terzo frammento: 1040 byte (1040 dati + 20 intestazione), Offset = 2960, **MF = 0** (ultimo frammento).

Campi Coinvolti nell'Intestazione IP

1. **Identification:** Identifica univocamente il pacchetto originale.
2. **Flags:** Include:
   - **DF (Don't Fragment):** Impedisce la frammentazione. Se la frammentazione non è possibile, il pacchetto viene scartato.
   - **MF (More Fragments):** Indica se il frammento è l'ultimo (MF = 0) o ce ne sono altri (MF = 1).
3. **Fragment Offset:** Specifica il punto di inizio del frammento nel pacchetto originale (in unità di 8 byte).

Considerazioni

- **Prestazioni:** La frammentazione introduce overhead (il processo di frammentazione comporta un **costo aggiuntivo** in termini di risorse e prestazioni nella rete: Maggiore utilizzo della larghezza di banda; Aumento della complessità nei router e nei dispositivi di destinazione; Rischio maggiore di perdita di pacchetti; Problemi di compatibilità; Impatto sulle prestazioni) e può ridurre le prestazioni della rete.)
- **Errori:** Se un frammento si perde, l'intero pacchetto è inutilizzabile.

- **IPv6:** IPv6 non supporta la frammentazione dai router. I pacchetti devono essere frammentati alla sorgente.

Il processo di frammentazione comporta un **costo aggiuntivo (**overhead) in termini di risorse e prestazioni nella rete. Questo avviene per diversi motivi:

---

1. Maggiore utilizzo della larghezza di banda

Ogni frammento richiede una propria **intestazione IP**, che occupa spazio nella rete. Questo significa che:

- Più frammenti = più intestazioni.
- Una parte della larghezza di banda viene spesa per trasmettere informazioni di controllo anziché il payload effettivo (i dati utili).

Esempio:
Un pacchetto originale di 4000 byte ha un'unica intestazione IP (20 byte). Se viene frammentato in tre pacchetti, ci saranno tre intestazioni IP (60 byte in totale), aumentando il traffico complessivo.

---

2. Aumento della complessità nei router e nei dispositivi di destinazione

- I router devono frammentare i pacchetti, operazione che richiede calcoli e manipolazione dei dati, rallentando il processo di inoltro.
- L'host di destinazione deve **riassemblare i frammenti**, un'operazione che richiede memoria e tempo per verificare che tutti i frammenti siano arrivati e siano nell'ordine corretto.

---

3. Rischio maggiore di perdita di pacchetti

Quando un pacchetto frammentato attraversa la rete:

- Se anche un solo frammento viene perso, l'intero pacchetto non può essere riassemblato e deve essere ritrasmesso.
- Più frammenti aumentano le probabilità di perdita, soprattutto in reti congestionate.

---

4. Problemi di compatibilità

Alcuni protocolli di rete o applicazioni non gestiscono bene la frammentazione. Ciò può portare a:

- Ritrasmissioni.
- Errori di connessione.
- Maggiore latenza.

---

5. Impatto sulle prestazioni

La frammentazione può rallentare il processo di instradamento e trasmissione, specialmente in reti con molti router o dispositivi con risorse limitate.

Soluzioni per Ridurre l'Overhead

- **PMTUD (Path MTU Discovery):** Scopre la dimensione massima del pacchetto supportata lungo il percorso e la sorgente invia pacchetti adeguati senza frammentazione.
- **IPv6:** In IPv6, la frammentazione è gestita solo dall'host sorgente, riducendo il carico sui router.

Qualunque router può decidere di frammentare un pacchetto, anche se un campo, "**Don't Fragment**" (**DF**), posto nell'intestazione IP può essere utilizzato per evitare che un router frammenti un pacchetto. Tale campo viene utilizzato per conoscere la **MTU** (**Maximun Transmission Unit**) attraverso una tecnica che determina quale sia il pacchetto più grande che possa essere inviato a un host senza subire la frammentazione. Spieghiamo meglio questo concetto:

Frammentazione dei pacchetti IP:

Quando un pacchetto IP supera la dimensione massima di trasmissione (**MTU - Maximum Transmission Unit**) di un segmento della rete, può essere suddiviso in frammenti più piccoli per attraversare quel segmento. Questa operazione è chiamata **frammentazione**. Ogni frammento viene inviato separatamente e riassemblato dal destinatario per ricostruire il pacchetto originale.

Campo "Don't Fragment" (DF):

Nell'intestazione di un pacchetto IP esiste un campo chiamato "Don't Fragment" (DF). Quando questo campo è impostato (1), indica ai router lungo il percorso di **non frammentare** il pacchetto. Se un router riceve un pacchetto con il bit DF impostato e il pacchetto è più grande dell'MTU del prossimo segmento, il router scarterà il pacchetto e invierà un messaggio ICMP "Fragmentation Needed" al mittente.

Scoperta dell'MTU del percorso (Path MTU Discovery):

La tecnica per determinare la dimensione massima del pacchetto che può essere inviato senza frammentazione si chiama **Path MTU Discovery**. Il mittente invia pacchetti con il bit DF impostato; se un pacchetto è troppo grande per un segmento del percorso, viene scartato e il mittente riceve un messaggio ICMP "Fragmentation Needed". Il mittente può quindi ridurre la dimensione del pacchetto e ritentare, iterando questo processo fino a determinare la dimensione massima del pacchetto che può attraversare l'intero percorso senza frammentazione.

In sintesi:

- **Frammentazione:** Suddivisione di un pacchetto IP in frammenti più piccoli quando supera l'MTU di un segmento della rete.
- **Campo DF:** Indica ai router di non frammentare il pacchetto (0); se il pacchetto è troppo grande e il bit DF è impostato, viene scartato e il mittente viene avvisato.
- **Path MTU Discovery:** Processo per determinare la dimensione massima del pacchetto che può essere inviato senza frammentazione, utilizzando il campo DF e i messaggi ICMP.

Questa gestione è cruciale per ottimizzare l'efficienza della rete e prevenire problemi legati alla frammentazione dei pacchetti.

L'**Internet Control Message Protocol (ICMP)** è un protocollo della suite TCP/IP utilizzato per trasmettere messaggi di controllo e segnalazione di errori nelle reti IP. Opera a livello di rete e consente ai dispositivi, come router e host, di comunicare informazioni riguardanti malfunzionamenti o altre condizioni che influenzano la trasmissione dei pacchetti.

Funzioni principali dei messaggi ICMP:

- **Segnalazione di errori:** Quando un pacchetto IP non può raggiungere la sua destinazione, ICMP invia un messaggio al mittente indicando la natura del problema, come host irraggiungibile o TTL (Time to Live) scaduto.
- **Diagnostica di rete:** Strumenti come ping e traceroute utilizzano messaggi ICMP per verificare la raggiungibilità di un host e tracciare il percorso dei pacchetti attraverso la rete.

Tipi comuni di messaggi ICMP:

- **Echo Request (Tipo 8) ed Echo Reply (Tipo 0):** Utilizzati per verificare la connettività tra dispositivi (ad esempio, tramite il comando ping). Il comando ping è un'utilità di rete utilizzata per verificare la connettività tra il proprio computer e un altro dispositivo su una rete IP. Funziona inviando pacchetti ICMP Echo Request al dispositivo di destinazione e attendendo le risposte ICMP Echo Reply. Questo processo

misura il tempo di andata e ritorno dei pacchetti, fornendo informazioni sulla latenza e sulla raggiungibilità del dispositivo remoto.

- **Destination Unreachable (Tipo 3):** Indica che un pacchetto non può raggiungere la destinazione prevista.
- **Time Exceeded (Tipo 11):** Segnala che il TTL di un pacchetto è scaduto, impedendogli di raggiungere la destinazione.
- **Redirect (Tipo 5):** Informa un host di un percorso alternativo più efficiente per raggiungere una destinazione.

È importante notare che ICMP non è progettato per lo scambio di dati tra applicazioni utente, ma piuttosto per la gestione e il controllo delle operazioni di rete, facilitando la diagnosi e la risoluzione dei problemi di comunicazione.

Ping e **Traceroute** sono strumenti di diagnostica di rete utilizzati per verificare la connettività e analizzare i percorsi dei dati tra un dispositivo sorgente e una destinazione.

Ping:

Il comando `ping` serve a determinare se un dispositivo di rete (come un computer o un server) è raggiungibile e a misurare il tempo impiegato dai pacchetti di dati per viaggiare verso la destinazione e tornare indietro. Funziona inviando una serie di messaggi ICMP Echo Request al dispositivo di destinazione e attendendo le risposte ICMP Echo Reply. I risultati mostrano il tempo di andata e ritorno (round-trip time) dei pacchetti, indicando la latenza della connessione. Inoltre, `ping` può rilevare la perdita di pacchetti, segnalando problemi di rete o di connettività.

Traceroute:

Il comando `traceroute` (o `tracert` su sistemi Windows) traccia il percorso che i pacchetti di dati seguono dalla sorgente alla destinazione, identificando tutti i nodi intermedi (router) attraversati. Utilizza il campo TTL (Time To Live) nell'intestazione dei pacchetti IP, incrementando il valore a ogni tentativo per provocare risposte dai router lungo il percorso. Questo processo consente di mappare il percorso completo e di misurare i tempi di transito tra ciascun nodo, aiutando a individuare eventuali punti di congestione o guasti nella rete.

Differenze principali:

- **Ping** verifica la raggiungibilità di un host e misura la latenza complessiva, ma non fornisce informazioni sul percorso seguito dai pacchetti.
- **Traceroute** mostra il percorso completo e i tempi di transito tra i nodi intermedi, ma non si concentra sulla latenza complessiva o sulla perdita di pacchetti.

Entrambi gli strumenti sono essenziali per diagnosticare problemi di rete, identificare colli di bottiglia e comprendere la struttura delle connessioni tra dispositivi su una rete IP.

Il problema è che il firewall verifica solo il primo frammento, perché è in tale frammento che vi sono memorizzate le informazioni testabili. Il primo frammento infatti contiene informazioni relative ai protocolli di alto livello, in base a quel frammento il firewall deciderà se far passare o meno il pacchetto. Una tecnica prevede di consentire il passaggio a tutti i frammenti facendo il controllo solamente sul primo, se il firewall decide di scartarlo, il pacchetto

originale non può essere ricostruito, in quanto il pacchetto parzialmente riassemblato non può essere accettato dall'host.

Consentire il passaggio a tutti i pacchetti eccetto il primo è comunque rischioso in quanto l'host di destinazione manterrebbe i frammenti non scartati in memoria per un certo periodo, in attesa di ricevere il pezzo mancante. Questo esporrebbe il sistema a un rischio terribile: l'attaccante potrebbe usare i pacchetti frammentati rimasti in memoria per sferrare un attacco di tipo **DoS**

Questa è la vulnerabilità legata alla gestione dei pacchetti IP frammentati da parte dei firewall e il rischio di attacchi **DoS** (**Denial of Service**) associati.

Frammentazione dei pacchetti IP:

Quando un pacchetto IP supera la dimensione massima di trasmissione (MTU) di una rete, viene suddiviso in frammenti più piccoli. Il primo frammento contiene l'intestazione IP completa e le informazioni dei protocolli di livello superiore (come TCP o UDP), mentre i frammenti successivi contengono solo parti dei dati originali.

Funzionamento del firewall:

I firewall analizzano i pacchetti in transito per decidere se consentirne o meno il passaggio, basandosi su criteri come indirizzi IP, porte e protocolli. Poiché solo il primo frammento di un pacchetto contiene l'intestazione completa con queste informazioni, il firewall esamina principalmente questo frammento per applicare le sue regole.

Vulnerabilità e rischi:

- **Passaggio dei frammenti successivi:** Se il firewall consente automaticamente il passaggio dei frammenti successivi senza ulteriori controlli, un attaccante potrebbe sfruttare questa caratteristica per inviare dati malevoli nascosti nei frammenti successivi, eludendo le regole del firewall.
- **Scarto del primo frammento:** Se il firewall decide di bloccare il primo frammento, i frammenti successivi, già trasmessi, rimangono in attesa di riassemblaggio nell'host di destinazione. Questi frammenti occupano memoria e risorse di sistema. Un attaccante potrebbe inviare ripetutamente pacchetti frammentati con l'intento di riempire la memoria dell'host, causando un sovraccarico e potenzialmente un'interruzione del servizio, noto come attacco DoS.

Mitigazione dei rischi:

Per proteggersi da tali vulnerabilità, è consigliabile:

- **Configurare il firewall** per analizzare tutti i frammenti dei pacchetti, non solo il primo, al fine di rilevare e bloccare eventuali contenuti malevoli nascosti.
- **Implementare meccanismi di protezione** contro attacchi basati su pacchetti frammentati, come il "Fragmented Packet Protection", che rileva in tempo reale pacchetti IP frammentati sospetti ed esegue operazioni di scarto o limitazione della velocità per proteggere il dispositivo di rete.
- **Monitorare e limitare** il numero di frammenti in attesa di riassemblaggio nell'host di destinazione, per prevenire l'esaurimento delle risorse di sistema.

Adottando queste misure, è possibile ridurre significativamente il rischio di attacchi **DoS** basati sulla frammentazione dei pacchetti IP e migliorare la sicurezza complessiva della rete.

DoS

Un attacco **DoS** (**Denial of Service**) ha lo scopo di ottenere l'esaurimento delle risorse di un sistema che fornisce un servizio, come per esempio un Web server, fino a renderlo non più in grado di erogare il servizio. Gli attacchi vengono abitualmente attuati inviando molti pacchetti di richieste, di solito a un Web server, FTP o di posta elettronica saturandone le risorse e rendendolo instabile. Attualmente gli attacchi DoS sono spesso di tipo criminale, in quanto tentano di impedire agli utenti della rete l'accesso ai siti web vittime dell'attacco. Per rendere più efficace l'attacco in genere vengono utilizzati molti computer inconsapevoli, detti **zombie**, sui quali precedentemente è stato inoculato un programma appositamente creato per attacchi DoS e che si attiva a un comando proveniente dal **cracker** creatore. Quando il programma maligno è diffuso su molti computer, chiamati **botnet**, essi produrranno un flusso incontenibile di dati che travolgeranno come una valanga anche i link più capienti del sito bersaglio.

In questo tipo di attacco l'host di destinazione rinuncia ad assemblare un pacchetto, spedendo un messaggio **ICMP** di tipo **packet reassembly time expired** in risposta al mittente con codice 1, indicante che il tempo per il riassemblaggio dei frammenti è scaduto. Tale messaggio informerà così l'attaccante dell'esistenza dell'host e del motivo per cui il firewall non ha accettato il pacchetto.

Dettagli del processo:

1. **Ricezione dei frammenti:** L'host di destinazione riceve pacchetti IP frammentati che devono essere riassemblati per ricostruire il pacchetto originale.
2. **Timeout di riassemblaggio:** Se l'host non riceve tutti i frammenti necessari entro un intervallo di tempo predefinito, il processo di riassemblaggio fallisce. Questo può accadere, ad esempio, se alcuni frammenti vengono persi durante la trasmissione.

3. **Invio del messaggio ICMP:** Quando il riassemblaggio fallisce a causa del timeout, l'host invia al mittente un messaggio ICMP "Time Exceeded" (Tipo 11, Codice 1) per notificare che il tempo per il riassemblaggio dei frammenti è scaduto.
4. **Informazioni per l'attaccante:** Questo messaggio ICMP può fornire a un potenziale attaccante informazioni sull'esistenza dell'host di destinazione e sul fatto che il pacchetto non è stato accettato a causa del fallimento nel riassemblaggio.

Considerazioni sulla sicurezza:

Gli attaccanti possono sfruttare queste informazioni per dedurre l'esistenza di un host e la sua configurazione di rete. Ad esempio, l'attaccante potrebbe inviare deliberatamente pacchetti frammentati in modo tale da causare un timeout di riassemblaggio, provocando la generazione di messaggi ICMP "Time Exceeded". Analizzando queste risposte, l'attaccante può ottenere dettagli sulla rete di destinazione, utilizzabili per pianificare ulteriori attacchi.

Mitigazione dei rischi:

Per ridurre il rischio associato a questa vulnerabilità, è consigliabile:

- **Configurare il firewall:** Assicurarsi che il firewall gestisca correttamente i pacchetti frammentati, analizzando tutti i frammenti e non solo il primo, per evitare che pacchetti malevoli eludano i controlli di sicurezza.
- **Limitare le risposte ICMP:** Configurare l'host di destinazione per limitare o filtrare l'invio di messaggi ICMP "Time Exceeded" verso fonti non fidate, riducendo le informazioni disponibili per potenziali attaccanti.
- **Monitorare il traffico di rete:** Implementare sistemi di rilevamento delle intrusioni (IDS) per identificare e analizzare attività sospette, come l'invio massiccio di pacchetti frammentati, che potrebbero indicare tentativi di attacco.

Adottando queste misure, è possibile aumentare la sicurezza della rete e ridurre la possibilità che informazioni sensibili vengano rivelate a potenziali attaccanti attraverso messaggi ICMP.