NAT

NAT (**N**etwork **A**ddress **T**ranslation--> *Traduzione degli indirizzi di rete*) è una tecnica, implementata dal router o dal firewall, che consiste nel modificare gli indirizzi IP dei pacchetti in transito su una rete, generalmente tra una rete privata (come una LAN domestica o aziendale) e Internet. È usato per ridurre il numero di indirizzi IP pubblici necessari e per proteggere i dispositivi interni da accessi esterni diretti.

Il **router** è un dispositivo di rete che instrada i pacchetti di dati tra reti diverse, consentendo la comunicazione tra dispositivi su reti locali e l'accesso a Internet. Funziona leggendo gli indirizzi IP di destinazione nei pacchetti e determinando il percorso migliore per inviarli verso la rete corretta; In pratica serve ad instradare il traffico di una rete verso un'altra rete o verso internet

Il **firewall** non è altro che un software o un dispositivo hardware che analizza il traffico di rete in entrata e in uscita e, in base a regole predefinite, crea una barriera per bloccare virus e minacce esterne.

PERCHE SI HA LA NECESSITA' DELLA NAT?

La necessità del **NAT** (Network Address Translation) nasce principalmente da due esigenze: **risparmiare indirizzi IP pubblici** e **migliorare la sicurezza delle reti private**.

1. Risparmio degli indirizzi IP pubblici

- Gli indirizzi IPv4 disponibili sono limitati, e il NAT permette di utilizzare un solo indirizzo IP pubblico per far comunicare numerosi dispositivi di una rete privata. In questo modo, i dispositivi interni condividono un unico IP pubblico, risolvendo in parte il problema dell'esaurimento degli indirizzi IPv4.

2. Miglioramento della sicurezza

- Il NAT nasconde gli indirizzi IP privati dei dispositivi interni, rendendo la rete meno visibile e meno vulnerabile ad attacchi esterni. Solo l'indirizzo IP pubblico del router è visibile dall'esterno, mentre i dispositivi interni restano protetti dietro il NAT.

3. Gestione semplificata della rete

- Attraverso il NAT, una rete aziendale o domestica può utilizzare una serie di indirizzi IP privati (non visibili dall'esterno) senza richiedere un IP pubblico per ciascun dispositivo. Questo consente una maggiore flessibilità e semplicità nella gestione degli indirizzi IP interni.

In sintesi, il NAT è essenziale per connettere una vasta gamma di dispositivi a Internet in modo efficiente e sicuro, ottimizzando l'uso degli indirizzi IP pubblici e proteggendo le reti private.

Funzioni principali del NAT:

1. **Condivisione dell'indirizzo IP**: Consente a più dispositivi su una rete locale di condividere un singolo indirizzo IP pubblico per comunicare con l'esterno.
2. **Sicurezza**: Nasconde gli indirizzi IP privati interni, riducendo il rischio di accessi non autorizzati dall'esterno.
3. **Traslazione degli indirizzi**: Converte gli indirizzi IP privati in uno o più indirizzi IP pubblici e viceversa.

Tipi di NAT:

- **Static NAT**: Associa ogni indirizzo IP privato a un indirizzo IP pubblico specifico, utilizzato spesso per dispositivi che necessitano di un accesso esterno costante.
- La **Static NAT** (NAT statico) mappa ogni indirizzo IP privato a un indirizzo IP pubblico fisso e specifico, che non cambia mai.
- Quindi, ogni volta che un dispositivo con un certo IP privato si collega all'esterno, utilizza sempre lo stesso indirizzo IP pubblico, rendendo la connessione facilmente identificabile e tracciabile dall'esterno. Questa modalità è utile quando si desidera che determinati dispositivi interni (come server o dispositivi con connessioni costanti) siano accessibili sempre dallo stesso IP pubblico.

Facciamo un esempio semplice per chiarire come funziona la **Static NAT**.

Scenario di esempio con Static NAT

Supponiamo di avere una rete aziendale con un server interno che ha l'indirizzo IP privato **192.168.1.10** e vogliamo che questo server sia sempre raggiungibile dall'esterno con lo stesso IP pubblico.

Impostazioni di Static NAT

1. **IP Privato** del server interno: **192.168.1.10**
2. **IP Pubblico** assegnato staticamente al server: **203.0.113.50**

Funzionamento

- **Configurazione sul router**: Sul router aziendale, configuriamo la Static NAT per associare l'IP pubblico **203.0.113.50** all'IP privato **192.168.1.10**.

- **Accesso dall’esterno**: Ogni volta che qualcuno dall'esterno prova a collegarsi all’indirizzo **203.0.113.50**, il router sa che deve reindirizzare il traffico al server con IP **192.168.1.10**.
- **Connessione dall'interno all'esterno**: Quando il server con IP privato **192.168.1.10** esce su Internet, apparirà sempre come proveniente dall'IP pubblico **203.0.113.50**.

Esempio pratico

1. **Un utente esterno** vuole accedere al sito web ospitato su **203.0.113.50**.
2. La richiesta arriva al router che usa la Static NAT per indirizzare tutto il traffico destinato a **203.0.113.50** verso il server **192.168.1.10**.
3. **Risultato**: L’utente esterno accede al server come se fosse collegato direttamente all’indirizzo pubblico **203.0.113.50**.

Cosa succede se l'IP pubblico 203.0.113.50 non è disponibile?

Se l'indirizzo IP pubblico **203.0.113.50** non è disponibile (per esempio, perché è stato riassegnato o è occupato da un altro dispositivo), ecco cosa può succedere:

1. **Il server diventa irraggiungibile dall'esterno**: Poiché la Static NAT associa in modo fisso **192.168.1.10** a **203.0.113.50**, se questo IP pubblico non è disponibile, chiunque tenti di accedere al server usando **203.0.113.50** non riuscirà a connettersi. La richiesta esterna non verrà indirizzata correttamente verso il server, causando un errore di connessione.
2. **Interruzione del servizio**: Se il server ospita un sito web o un servizio che deve essere accessibile dall'esterno, l'indisponibilità dell’IP pubblico causa un’interruzione del servizio. Gli utenti non potranno accedere alle risorse del server finché l’indirizzo IP pubblico non viene ripristinato o sostituito.
3. **Possibile necessità di riconfigurazione**: Per risolvere il problema, è necessario ottenere un nuovo IP pubblico disponibile (ad esempio **203.0.113.51**) e configurare nuovamente il router per mappare il server **192.168.1.10** al nuovo IP pubblico. Tuttavia, questo implica che tutti coloro che si connettevano all'indirizzo **203.0.113.50** devono ora essere informati del nuovo indirizzo.

Soluzione alternativa: Utilizzo di Dynamic NAT o DNS dinamico

Per evitare l'interruzione del servizio causata da un IP pubblico non disponibile, molte reti usano soluzioni alternative come:

- **Dynamic NAT (DNAT)**: Con DNAT, è possibile assegnare IP pubblici da un pool disponibile, il che rende meno probabile che un singolo indirizzo causi l’interruzione del servizio.

- **DNS dinamico (DDNS)**: Utilizzando un servizio di DNS dinamico, è possibile associare un nome di dominio all'IP pubblico. Così, anche se l'IP cambia, il nome di dominio rimane costante e gli utenti non notano la modifica.

Vantaggio della Static NAT

- Il server è sempre accessibile con lo stesso IP pubblico **203.0.113.50**, che facilita l'accesso esterno e mantiene stabile l'indirizzo pubblico per servizi che richiedono un IP fisso.

- **Dynamic NAT**: Assegna dinamicamente un indirizzo IP pubblico da un pool disponibile ogni volta che un dispositivo interno richiede l'accesso a Internet.
- **PAT (Port Address Translation)** o **NAT Overload**: Permette a molti dispositivi di condividere un solo indirizzo IP pubblico usando numeri di porta per differenziare le connessioni.

Il NAT è essenziale per la gestione efficiente degli indirizzi IP e per migliorare la sicurezza delle reti private.

Ritorniamo allo Scenario di esempio con Static NAT, cioè a quello in cui abbiamo supposto di avere una rete aziendale con un server interno che ha l'indirizzo IP privato 192.168.1.10 e vogliamo che questo server sia sempre raggiungibile dall'esterno con lo stesso IP pubblico e vediamo

LE RAGIONI, PER CUI, QUESTO server DEBBA sempre ESSERE raggiungibile dall'esterno con lo stesso IP pubblico

1. Accesso Affidabile e Costante per gli Utenti Esterni

- Utilizzando un IP pubblico statico, utenti e dispositivi esterni possono raggiungere il server sempre allo stesso indirizzo, senza dover aggiornare le loro configurazioni o URL di collegamento. Questo è essenziale per servizi critici, come server web, server di posta elettronica o server di database, che devono essere accessibili sempre dallo stesso punto di ingresso.

2. Configurazioni DNS Stabili

- Quando un server ha un IP pubblico fisso, il DNS (Domain Name System) può essere configurato per puntare stabilmente al server. Ad esempio, un dominio come www.azienda.com può essere associato sempre allo stesso IP pubblico (203.0.113.50), facilitando l'accesso tramite il nome di dominio. Se l'IP cambiasse, bisognerebbe aggiornare continuamente i record DNS, causando possibili disservizi.

3. Supporto a Servizi che Richiedono IP Fissi

- Alcuni servizi o protocolli, come quelli di autenticazione e firewall, richiedono che il server abbia un IP fisso per applicare regole di sicurezza o autorizzazioni. Per esempio, un firewall di un'altra rete può autorizzare accesso solo da IP conosciuti e fissi; con un IP dinamico o variabile, queste autorizzazioni diventerebbero inaffidabili.

4. Stabilità per l'Accesso Remoto e VPN

- In molte aziende, il server interno può essere usato per accesso remoto tramite VPN o per il controllo remoto dei dati aziendali. Avere un IP pubblico stabile garantisce che i dipendenti possano collegarsi al server da remoto senza interruzioni, poiché sanno esattamente quale IP utilizzare per la connessione.

5. Configurazioni Statiche nei Sistemi Esterni

- Se il server deve comunicare con altri sistemi esterni (ad esempio, con server di clienti o partner) che richiedono la whitelist di indirizzi IP specifici, un IP fisso semplifica la configurazione. I sistemi esterni possono includere l'IP pubblico del server nella loro whitelist senza preoccuparsi di futuri cambiamenti di indirizzo.

In sintesi, l'uso di un IP pubblico fisso tramite Static NAT permette una **mappatura stabile** e **affidabile** del server, garantendo accessibilità costante, stabilità del DNS, supporto ai servizi che richiedono IP statici e facilità nelle configurazioni di accesso da remoto.

ATTIVITA' DI LABORATORIO

Configurare la **Static NAT** sul router aziendale per associare un indirizzo IP pubblico a un IP privato

Passaggi per Configurare la Static NAT

Supponiamo di voler associare:

- **IP Privato** del server: **192.168.1.10**
- **IP Pubblico** assegnato al server: **203.0.113.50**

1. Accedere al Router

- Collegatevi al router tramite l'interfaccia di gestione web, SSH, o un'altra modalità disponibile, e accedete con le credenziali di amministratore.

2. Individuare la Sezione di Configurazione NAT

- Nel menu del router, cercate la sezione dedicata al **NAT** o alla **Port Forwarding**. A seconda del modello e del software del router, questa sezione potrebbe avere nomi leggermente diversi come "NAT Settings," "Address Translation," o simili.

3. Creare una Regola di Static NAT

- Nella sezione NAT, selezionate l'opzione per **creare una nuova regola di Static NAT**. La terminologia può variare, ma cercate un'opzione come "Static NAT" o "1:1 NAT".

4. Inserire gli Indirizzi IP

- **IP Privato di Destinazione**: Inserite l'indirizzo IP privato del server interno, in questo caso **192.168.1.10**.
- **IP Pubblico Assegnato**: Inserite l'indirizzo IP pubblico che verrà mappato su questo server, cioè **203.0.113.50**.

5. Configurare il Port Mapping (opzionale)

- Alcuni router permettono di specificare le **porte** che devono essere tradotte. Se volete esporre solo specifiche porte (come 80 per HTTP o 443 per HTTPS), configuratele in questa sezione.
- Se non c'è bisogno di specificare porte particolari, configurate l'opzione per mappare tutte le porte, permettendo così accesso completo all'IP pubblico.

6. Salvare e Applicare le Modifiche

- Salvate la regola di NAT e applicate le modifiche. Il router potrebbe richiedere un riavvio per completare la configurazione.

Come Funziona Dopo la Configurazione

- Ogni volta che un dispositivo esterno invia una richiesta all'indirizzo IP pubblico **203.0.113.50**, il router riconosce la regola di Static NAT e reindirizza automaticamente il traffico verso l'indirizzo IP privato **192.168.1.10**.
- Da questo punto in poi, tutti i pacchetti in arrivo all'IP pubblico vengono reindirizzati al server interno, come se il server fosse direttamente esposto su Internet.

Vantaggi della Configurazione

- **Accesso diretto**: Chiunque conosca l'IP pubblico **203.0.113.50** può accedere al server interno senza dover conoscere il suo IP privato.
- **Sicurezza**: Anche se il server è accessibile dall'esterno, il router mantiene un certo controllo sul traffico, consentendo di applicare altre regole di sicurezza, come firewall e filtraggio IP.

Configurare la Static NAT in questo modo permette al server interno di avere un punto d'accesso stabile e fisso per gli utenti esterni.