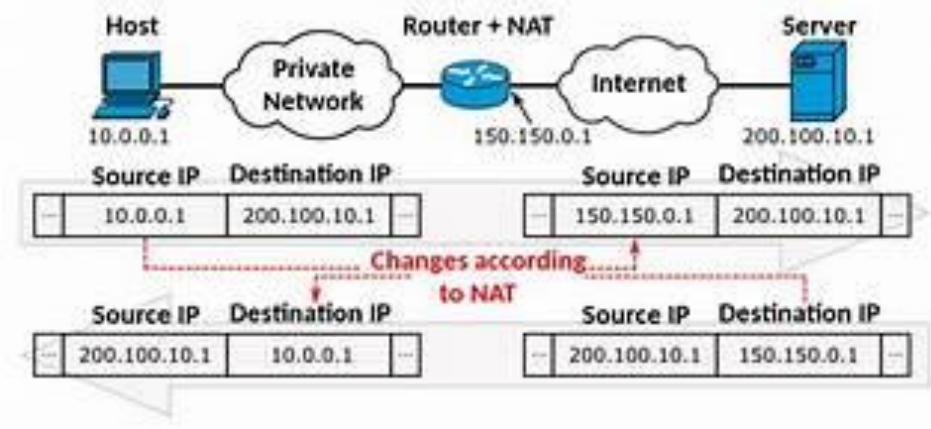
Praktyczna teoria o NAT

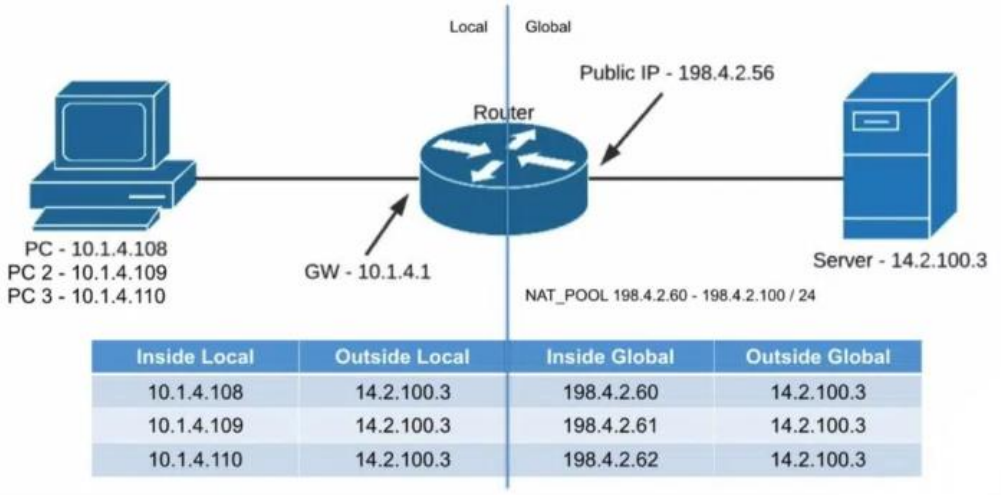


NAT - co to jest i jak działa?

NAT (Network Address Translation) jest kluczowym elementem w sieciach komputerowych, a jej zrozumienie jest istotne w kontekście konfiguracji sieci wirtualnej VPN. Oto kilka praktycznych informacji o NAT:

1. Co to jest NAT:

NAT to technika, która pozwala na mapowanie adresów IP i portów między dwoma różnymi domenami adresowymi. Jest używana, gdy prywatne adresy IP wewnętrznej sieci muszą komunikować się z zewnętrznymi sieciami, takimi jak Internet.



Inside Local	Outside Local	Inside Global	Outside Global
10.1.4.108	14.2.100.3	198.4.2.60	14.2.100.3
10.1.4.109	14.2.100.3	198.4.2.61	14.2.100.3
10.1.4.110	14.2.100.3	198.4.2.62	14.2.100.3

Na powyższym diagramie widać, że urządzenia w sieci prywatnej mają adresy IP z zakresu 10.1.4.0/24, natomiast urządzenia w sieci publicznej mają adresy IP z zakresu 198.4.2.0/24. Aby umożliwić komunikację między tymi sieciami, router NAT mapuje adresy IP i porty źródłowe urządzeń prywatnych na adresy IP i porty docelowe urządzeń publicznych. W ten sposób, urządzenia prywatne mogą nawiązywać połączenia z urządzeniami publicznymi, a urządzenia publiczne mogą odbierać i odpowiadać na te połączenia.

Na diagramie są dwie sieci: sieć prywatna i sieć publiczna. Sieć prywatna to sieć wewnętrzna, która używa adresów IP z zakresu 10.1.4.0/24. To znaczy, że każde urządzenie w tej sieci ma adres IP, który zaczyna się od 10.1.4. i kończy się na dowolną liczbę od 0 do 255. Na przykład, komputer A ma adres IP 10.1.4.10, a komputer B ma adres IP 10.1.4.20.

Sieć publiczna to sieć zewnętrzna, która używa adresów IP z zakresu 198.4.2.0/24. To znaczy, że każde urządzenie w tej sieci ma adres IP, który zaczyna się od 198.4.2. i kończy się na dowolną liczbę od 0 do 255. Na przykład, serwer X ma adres IP 198.4.2.100, a serwer Y ma adres IP 198.4.2.5600.

Aby umożliwić komunikację między tymi sieciami, potrzebny jest router NAT. Router NAT to urządzenie, które łączy sieć prywatną i sieć publiczną. Router NAT ma dwa adresy IP: jeden prywatny i jeden publiczny. Na przykład, router NAT ma adres IP 10.1.4.1 w sieci prywatnej i adres IP 198.4.2.1 w sieci publicznej.

Router NAT ma też tabelę, w której zapisuje, jakie adresy IP i porty są mapowane między sieciami. Port to numer, który identyfikuje konkretny typ połączenia. Na przykład, port 80 to port dla protokołu HTTP, który jest używany do przeglądania stron internetowych.

Gdy urządzenie z sieci prywatnej chce nawiązać połączenie z urządzeniem z sieci publicznej, musi wysłać pakiet danych do routera NAT. Pakiet danych to jednostka informacji, która zawiera adres IP i port źródłowy (nadawcy) i adres IP i port docelowy (odbiorcy). Na przykład, jeśli komputer A chce połączyć się z serwerem X, musi wysłać pakiet danych z adresem IP i portem źródłowym 10.1.4.10:1234 i adresem IP i portem docelowym 198.4.2.100:80.

Router NAT odbiera pakiet danych i sprawdza czy ma już wpis w tabeli dla tego połączenia. Jeśli nie ma, to tworzy nowy wpis i mapuje adres IP i port źródłowy na adres IP i port docelowy. Na przykład, router NAT może zmapować adres IP i port źródłowy 10.1.4.10:1234 na adres IP i port docelowy 198.4.2.1:5678. W ten sposób, router NAT zmienia prywatny adres IP i port na publiczny adres IP i port.

Router NAT następnie wysyła pakiet danych do urządzenia z sieci publicznej z zaktualizowanym adresem IP i portem źródłowym. Na przykład, router NAT wysyła pakiet danych z adresem IP i portem źródłowym 198.4.2.1:5678 i adresem IP i portem docelowym 198.4.2.100:80 do serwera X.

Urządzenie z sieci publicznej odbiera pakiet danych i odpowiada na niego, wysyłając pakiet danych z adresem IP i portem źródłowym i adresem IP i portem docelowym zamienionymi miejscami. Na przykład, serwer X wysyła pakiet danych z adresem IP i portem źródłowym 198.4.2.100:80 i adresem IP i portem docelowym 198.4.2.1:5678 do routera NAT.

Router NAT odbiera pakiet danych i sprawdza czy ma wpis w tabeli dla tego połączenia. Jeśli ma, to mapuje adres IP i port docelowy na adres IP i port źródłowy. Na przykład, router NAT może zmapować adres IP i port docelowy 198.4.2.1:5678 na adres IP i port źródłowy 10.1.4.10:1234. W ten sposób, router NAT zmienia publiczny adres IP i port na prywatny adres IP i port.

Router NAT następnie wysyła pakiet danych do urządzenia z sieci prywatnej z zaktualizowanym adresem IP i portem docelowym. Na przykład, router NAT wysyła pakiet danych z adresem IP i portem źródłowym 198.4.2.100:80 i adresem IP i portem docelowym 10.1.4.10:1234 do komputera A.

Urządzenie z sieci prywatnej odbiera pakiet danych i kontynuuje połączenie z urządzeniem z sieci publicznej. W ten sposób, urządzenia prywatne mogą nawiązywać połączenia z urządzeniami publicznymi, a urządzenia publiczne mogą odbierać i odpowiadać na te połączenia.

2. Typy NAT:

W zależności od sposobu mapowania adresów IP i portów, można wyróżnić dwa główne typy NAT:

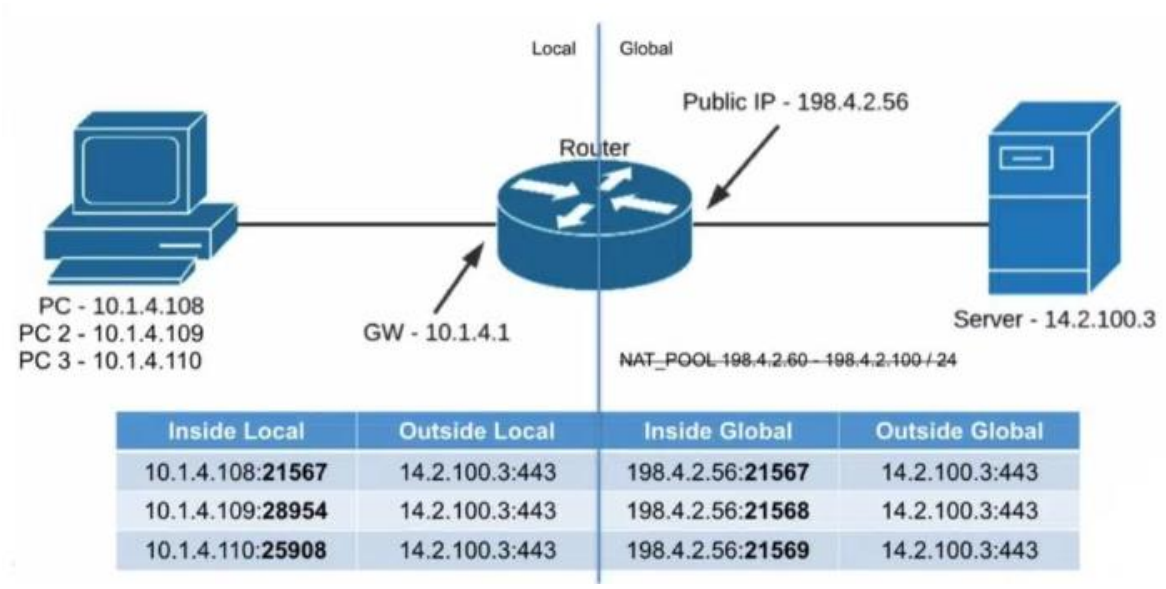
- NAT statyczne: Określone pary adresów IP są ręcznie przypisywane, co oznacza stałe mapowanie między publicznymi a prywatnymi adresami IP. Przykładem może być mapowanie adresu IP 10.1.4.10 na adres IP 198.4.2.10. Taki typ NAT jest prosty w konfiguracji i zapewnia stałą dostępność urządzeń, ale wymaga dużej ilości publicznych adresów IP, co może być kosztowne i nieefektywne.
- NAT dynamiczne: Adresy IP są przydzielane dynamicznie z puli dostępnych publicznych adresów w miarę potrzeb. To bardziej efektywna opcja, ale może prowadzić do problemów, gdy wymagane jest stałe mapowanie. Przykładem może być mapowanie adresu IP 10.1.4.10 na dowolny wolny adres IP z zakresu 198.4.2.0/24. Taki typ NAT oszczędza publiczne adresy IP, ale utrudnia identyfikację i śledzenie urządzeń.

3. Adresy prywatne vs. publiczne:

Adresy IP prywatne (np. 192.168.x.x, 10.x.x.x) są używane wewnątrz sieci lokalnej i nie są routowalne w Internecie. Adresy IP publiczne są przypisane do urządzeń, które są bezpośrednio dostępne z zewnątrz. Aby umożliwić komunikację między sieciami prywatnymi a publicznymi, potrzebny jest NAT.

4. Port Address Translation (PAT):

Jest to rodzaj NAT, który umożliwia wielu urządzeniom w sieci prywatnej udostępnianie jednego publicznego adresu IP. Jest realizowane poprzez mapowanie prywatnych adresów IP wraz z portami na unikalne zestawy portów publicznych. PAT jest często używany w domowych i małych sieciach, aby umożliwić dostęp do Internetu z jednego publicznego adresu IP przydzielonego przez dostawcę usług internetowych.

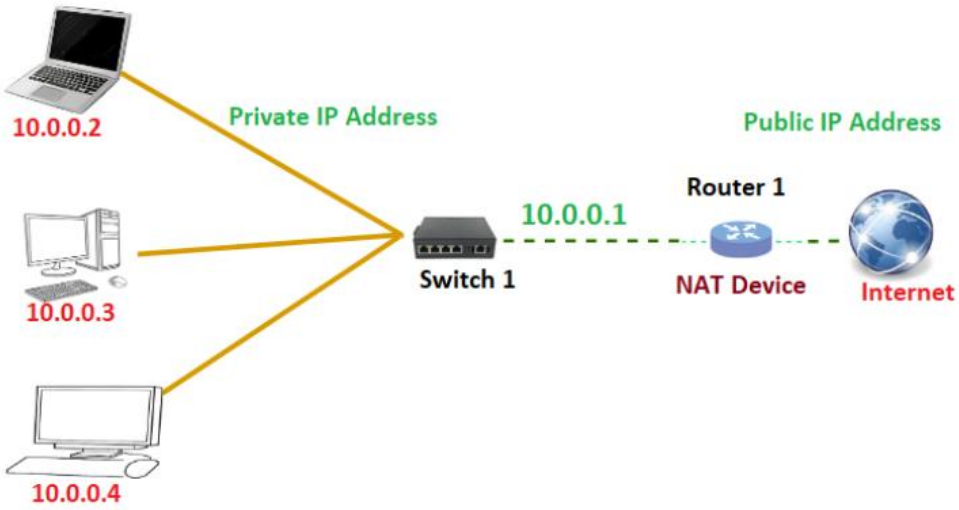


Inside Local	Outside Local	Inside Global	Outside Global
10.1.4.108:**21567**	14.2.100.3:443	198.4.2.56:**21567**	14.2.100.3:443
10.1.4.109:**28954**	14.2.100.3:443	198.4.2.56:**21568**	14.2.100.3:443
10.1.4.110:**25908**	14.2.100.3:443	198.4.2.56:**21569**	14.2.100.3:443

Na powyższym diagramie widać, że urządzenia w sieci prywatnej mają adresy IP z zakresu 10.1.4.0/24, natomiast router NAT ma jeden publiczny adres IP 198.4.2.56. Aby umożliwić komunikację z zewnętrznym serwerem o adresie IP 14.2.100.3, router NAT mapuje adresy IP i porty źródłowe urządzeń prywatnych na porty docelowe publicznego adresu IP. W ten sposób, urządzenia prywatne mogą nawiązywać połączenia z serwerem, a serwer może odbierać i odpowiadać na te połączenia.

5. Rola NAT w VPN:

W kontekście VPN, NAT może być używany do maskowania prywatnych adresów IP klientów, umożliwiając im korzystanie z jednego publicznego adresu IP do komunikacji z zewnętrznym serwerem VPN. VPN (Virtual Private Network) jest technologią, która umożliwia tworzenie bezpiecznych i szyfrowanych połączeń między zdalnymi urządzeniami a siecią prywatną przez Internet.



Na powyższym diagramie widać, że urządzenia w sieci prywatnej mają adresy IP z zakresu 10.0.0.0/24, natomiast serwer VPN ma publiczny adres IP 198.4.2.1. Aby umożliwić komunikację z siecią prywatną, urządzenia muszą nawiązać połączenie VPN z serwerem VPN. Aby to zrobić, muszą użyć NAT, aby zmienić swoje prywatne adresy IP na publiczne adresy IP, które są routowalne w Internecie. Serwer VPN następnie mapuje te publiczne adresy IP na prywatne adresy IP, które są używane w sieci prywatnej. W ten sposób, urządzenia mogą komunikować się z siecią prywatną, jakby były jej częścią.

6. Problemy i wyzwania:

NAT może powodować problemy w przypadku protokołów, które zawierają adresy IP w treści danych, takich jak IPsec. IPsec jest protokołem, który zapewnia bezpieczeństwo i autentyczność danych w sieciach IP. IPsec używa nagłówków i ładunków danych, które zawierają adresy IP źródłowe i docelowe. Jeśli te adresy IP są zmieniane przez NAT, IPsec nie będzie w stanie zweryfikować integralności i tożsamości danych, co spowoduje zerwanie połączenia.

Aby rozwiązać ten problem, można użyć jednej z następujących technologii:

- Traversal Using Relays around NAT (TURN): Jest to protokół, który umożliwia urządzeniom za NAT nawiązywanie połączeń z zewnętrznymi serwerami, które działają jako pośrednicy w przekazywaniu danych. TURN jest często używany w aplikacjach do komunikacji głosowej i wideo przez Internet.
- Session Traversal Utilities for NAT (STUN): Jest to protok