POLSKO-JAPOŃSKA AKADEMIA TECHNIK KOMPUTEROWYCH

Wydział Informatyki
Specjalizacja: Technologie sieci urządzeń mobilnych oraz chmury obliczeniowej

Szymon Kogut
Numer albumu: 24271

Porównanie modeli scentralizowanych i rozproszonych w wirtualnych sieciach prywatnych

Comparison of centralized and distributed models in virtual private networks

Rodzaj pracy
Magisterska

Imię i nazwisko promotora
dr Tadeusz Puźniakowski

Warszawa 19 stycznia 2026

Streszczenie: Celem pracy jest weryfikacja różnych modeli i protokołów sieci wirtualnych pod kątem stabilności w restrykcyjnym środowisku oraz łatwości utrzymania w projektach o niskim stopniu złożoności infrastrukturalnej.

Porównaniem objęto następujące protokoły: OpenVPN (topologia scentralizowana), Nebula (topologia rozproszona) oraz WireGuard (obie topologie). Przygotowano skrypty automatyzujące proces wdrażania.

W ramach badań przeprowadzono testy wydajnościowe przepustowości, opóźnień i obciążenia zasobów. Zbadano stabilność połączeń w restrykcyjnych warunkach sieciowych oraz łatwość wdrożenia poszczegolnych rozwiązań.

Dodatkowo oceniono skalowalność poszczególnych rozwiązań przy zwiększaniu liczby węzłów.

Słowa kluczowe: vpn, openvpn, nebula, wireguard

Spis treści

Spis rysunków

01. Wstęp

Internet początkowo rozwijał się jako zdecentralizowana sieć tworzona oddolnie przez niezależne podmioty. Z czasem usługi świadczone za jego pośrednictwem zyskały na znaczeniu a wraz z tym uległy monopolizacji przez duże korporacje.

Aspekty takie jak suwerenność danych, ochrona prywatności, ograniczenie kosztów czy potrzeba autonomii to czynniki motywujące użytkowników indywidualnych oraz małe przedsiębiorstwa do zwrócenia się w stronę samodzielnego utrzymywania infrastruktury usług na potrzeby własne.

Niezastąpione przy takim podejściu są sieci wirtualne. Łączą one urządzenia, niezależnie od ich fizycznej lokalizacji. Jest to niezbędne dla zachowania pełni funkcjonalności w porównaniu z komercyjnymi rozwiązaniami.

Niniejsza praca ma na celu przegląd dostępnych rozwiązań z zakresu sieci wirtualnych. Celem jest znalezienie optymalnego rozwiązania dostosowanego do skali projektów o niskim stopniu złożoności infrastrukturalnej.

W związku z powyższym, przy analizie skupiono się nie tylko na pomiarze syntetycznej wydajności poszczególnych rozwiązań, ale również zbadano skalowalność, łatwość wdrożenia oraz stabilność pracy w restrykcyjnych warunkach sieciowych.

02. Słownik pojęć

1. **Lorem** - *Ipsum*

03. Restrykcyjne środowisko sieciowe

Celem pracy jest znalezienie rozwiązania możliwego do wdrożenia w sieciach konsumenckich. Poniższy rozdział definiuje ograniczenia związane z tym środowiskiem.

03.1. Rodzaje NAT

Jest to decydujący czynnik utrudniający nawiązywanie połączeń z urządzeniami spoza sieci lokalnej. W zależności od typu `NAT` za jakimi znajdują się urządzenia, będzie to proces utrudniony bądź w pełni uniemożliwiony.

03.1.1. Static NAT

Przydziela publiczny adres każdemu urządzeniu z puli publicznych adresów. Z tego powodu nie stanowi bariery przy nawiązywaniu bezpośrednich połączeń między urządzeniami. Nie wykorzystywany dla rozwiązań konsumenckich.

03.1.2. Dynamic NAT

Rozwiązanie rzadziej stosowane działające podobne do statycznego. Jedyna różnica jest taka, że adresy przydzielane są w sposób dynamiczny.

03.1.3. Network Address and Port Translation (NAPT)

Zastosowanie `Port Address Translation (PAT)` umożliwia współdzielenie jednego publicznego adresu IP przez wiele urządzeń.

Zasada działania tego mechanizmu opiera się na użyciu portów dla rozróżnienia poszczególnych klientów.

Flow diagram

Poszczególne implementacje `NAPT` różnią się poziomem restrykcyjności odnośnie filtrowania przychodzących pakietów.

Full Cone NAT
Najbardziej permisywna implementacja. Nie wprowadza dodatkowych ograniczeń. Mapowanie portów może być predefiniowane lub definiowane w odpowiedzi na wysyłane zapytania.

Restricted Cone NAT
W tej implementacji host wewnętrzny musi najpierw wysłać zapytanie kierowane na dany adres. Zakres akceptowanych pakietów jest zawężony do pakietów z tym adresem źródłowym.

Port Restricted Cone NAT
W tej implementacji host wewnętrzny musi najpierw wysłać zapytanie kierowane na dany adres oraz port. Zakres akceptowanych pakietów jest zawężony do pakietów z tym adresem źródłowym oraz portem.

Symmetric NAT
Najbardziej restrykcyjna implementacja. Posiada ograniczenia adresu i port z tą różnicą że każda ich kombinacja otrzymuje dedykowany port zewnętrzny. Wcześniejsze implementacje współdzielą wybrany port zewnętrzny pomiędzy adresami docelowymi.

03.1.4. Carrier-grade NAT

Jest to specyficzny przypadek zastosowania `NAPT`. Odnosi się on do jego wykorzystania w sieci wewnętrznej dostawcy internetu. Użytkownik współdzieli jeden adres z innymi klientami dostawcy. Istnieje wiele implementacji `CGNAT`. Natomiast główny podział wynika z wykorzystywanego protokołu.

Popularny mechanizm `DS-Lite` zakłada że klient nie otrzymuje żadnego adresu IPv4 a jedynie IPv6. Pakiety IPv4 są enkapsulowane w pakiety IPv6 przy przesyle do routera brzegowego dostawcy.

Wart ponownego odnotowania jest fakt, że jest to specyficzny sposób wykorzystania `NAPT`, aniżeli jego konkretna implementacja. Przykładowo, CGNAT może być w implementacji `Symmetric`, ale równie dobrze może to być `Full Cone NAT`.

03.2. Wysokie opóźnienia i Jitter

03.3. Utrata pakietów

03.4. Blokada protokołu UDP

07. Badane protokoły

07.1. Kryteria doboru

07.2. OpenVPN

07.3. WireGuard

07.4. Nebula

08. Metodyka badań

08.1. Narzędzia pomiarowe i metryki

08.2. Metodyka oceny złożoności wdrożenia

08.3. Scenariusze testowe

08.3.1. Scenariusz bazowy

08.3.2. Scenariusz restrykcyjny

08.3.3. Scenariusz skalowalności

09. Konfiguracja środowiska

09.1. Automatyzacja procesu wdrażania

09.2. Konfiguracja OpenVPN

09.3. Konfiguracja WireGuard w modelu rozproszonym

09.4. Konfiguracja WireGuard w modelu scentralizowanym

09.5. Problemy napotkane podczas implementacji

10. Analiza wyników

10.1. Badanie wydajności sieciowej

10.2. Analiza obciążenia zasobów systemowych

10.3. Odporność na trudne warunki sieciowe

10.4. Analiza skalowalności

10.5. Ocena złożoności konfiguracji i utrzymania

11. Podsumowanie

11.1. Synteza wyników

11.2. Wnioski końcowe

12. Bibliografia

Podane adresy URL zostały sprawdzone dnia 1 grudnia 2024.

13. Załaczniki

Wszystkie załączniki znajdują się na załączonym do pracy dysku optycznym.

1. Lorem ipsum dolor sit amet
2. Lorem ipsum dolor sit amet
3. Lorem ipsum dolor sit amet