



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 28 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 poszczególnych rozwiązań.

Dodatkowo oceniono skalowalność poszczególnych rozwiązań przy zwiększaniu liczby węzłów.

Słowa kluczowe: vpn, openvpn, nebula, wireguard

Spis treści

01. Wstęp	1
01.1. Motywacje	1
01.2. Cel	1
01.3. Prace powiązane.....	1
02. Słownik pojęć	2
03. Restrykcyjne środowisko sieciowe.....	3
03.1. Rodzaje NAT	3
03.1.1. Static NAT	3
03.1.2. Dynamic NAT.....	3
03.1.3. Network Address and Port Translation (NAPT)	3
03.1.4. Carrier-grade NAT	4
03.2. Metody obejścia NAT.....	5
03.2.1. UDP Hole Punching	5
03.2.2. STUN (Session Traversal Utilities for NAT)	5
03.2.3. TURN (Traversal Using Relays around NAT)	5
03.3. Wysokie opóźnienia i jitter	6
03.4. Utrata pakietów.....	6
03.5. Blokada protokołu UDP.....	6
04. Badane modele	7
05. Model scentralizowany.....	7
06. Model rozproszony.....	7
07. Badane protokoły	8
07.1. Kryteria doboru.....	8
07.2. OpenVPN	8
07.3. WireGuard	8
07.4. Nebula.....	8
08. Metodyka badań	9
08.1. Narzędzia pomiarowe i metryki	9
08.2. Metodyka oceny złożoności wdrożenia	9
08.3. Scenariusze testowe.....	9
08.3.1. Scenariusz bazowy	9
08.3.2. Scenariusz restrykcyjny	9
08.3.3. Scenariusz skalowalności	9
09. Konfiguracja środowiska	10
09.1. Automatyzacja procesu wdrażania	10
09.2. Konfiguracja OpenVPN	10
09.3. Konfiguracja WireGuard w modelu rozproszonym	10
09.4. Konfiguracja WireGuard w modelu scentralizowanym	10
09.5. Problemy napotkane podczas implementacji	10
10. Analiza wyników.....	11
10.1. Badanie wydajności sieciowej.....	11
10.2. Analiza obciążenia zasobów systemowych	11
10.3. Odporność na trudne warunki sieciowe.....	11
10.4. Analiza skalowalności.....	11
10.5. Ocena złożoności konfiguracji i utrzymania	11

11. Podsumowanie	12
11.1. Synteza wyników.....	12
11.2. Wnioski końcowe.....	12
12. Bibliografia	13
13. Załączniki	14

Spis rysunków

1. Schemat działania mechanizmu NAT/PAT.....	3
--	---

01. Wstęp

01.1. Motywacje

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.

Z uwagi na niską adopcję IPv6 oraz ograniczenia nakładane przez dostawców usług internetowych stawiane dla prosumentów zasobów sieciowych, 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.

01.2. Cel

Sieci nastawione na użytkowników końcowych stanowią wyzwanie dla każdego kto chce zajmować się utrzymaniem usług na własną rękę - brak publicznego adresu IPv4, restrykcyjny wariant NAT-u, brak możliwości administracji routerem brzegowym, niska stabilność łącza.

Praca ma na celu analizę wad i zalet dostępnych rozwiązań w domenie sieci wirtualnych oraz ocenę procesu ich wdrażania.

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

01.3. Prace powiązane

Temat wydajności protokołów sieci VPN jest obiektem wielu prac badawczych. Głównym celem, większości tych prac, jest porównanie syntetycznej wydajności osiąganej przez te protokoły, poprzez pomiary wykonywane w laboratoryjnych warunkach. [4, 1, 2, 3]

Niniejsza praca różni się w tym zakresie od tych dostępnych, ponieważ kładzie nacisk na rozwiązania o niskim progu wejścia, zakładając, że użytkownik końcowy operuje w nietypowym środowisku sieciowym bez dostępu do infrastruktury klasy korporacyjnej czy zaawansowanego wsparcia technicznego.

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. Niewykorzystywany dla rozwiązań konsumenckich.

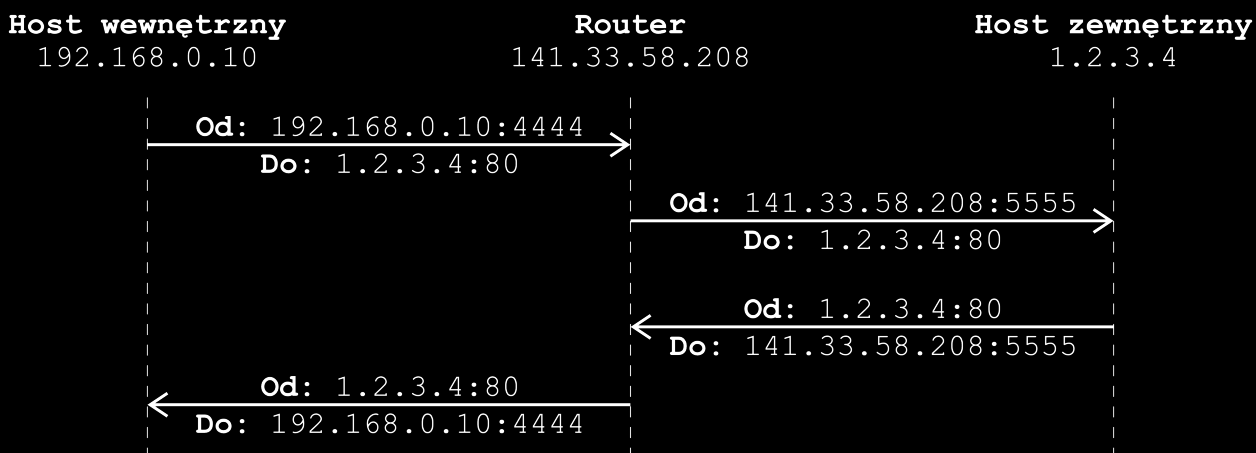
03.1.2. Dynamic NAT

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)

Umożliwia współdzielenie jednego publicznego adresu IP przez wiele urządzeń.

Zasada działania tego mechanizmu opiera się na użyciu portów dla rozróżnienia poszczególnych klientów. Każdy port, każdego urządzenia w sieci wewnętrznej, otrzymuje na żądanie port zewnętrzny routera. NAPT działa jak warstwa translacji. Dla zapytań wychodzących podmienia źródłowy adres IP oraz port na własne. Dla zapytań przychodzących podmienia docelowy adres oraz port na te należące do odbiorcy wewnątrz sieci.



Rys. 1. Schemat działania mechanizmu NAT/PAT

Poszczególne implementacje NATP różnią się poziomem restrykcyjności odnośnie filtrowania przychodzących pakietów.

Full Cone NAT

Najbardziej permissywna 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 współdzieliły wybrany port zewnętrzny pomiędzy adresami docelowymi.

W przypadku gdy oba urządzenia znajdują się za tego typu NAT-em, nie ma możliwości nawiązania bezpośredniego połączenia pomiędzy nimi.

03.1.4. Carrier-grade NAT

Jest to specyficzny przypadek zastosowania NATP. 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 przesyłaniu do routera brzegowego dostawcy.

Warto ponownie odnotować fakt, że jest to specyficzny sposób wykorzystania NATP, aniżeli jego konkretna implementacja. Przykładowo, CGNAT może być w NAT-em symetrycznym, ale równie dobrze może to być Full Cone NAT.

03.2. Metody obejścia NAT

03.2.1. UDP Hole Punching

Ta podstawowa technika polega na wykorzystaniu współdzielonego serwera do wstępnej konfiguracji.

Do tego wymagana jest stałość mapowania zewnętrznych portów przez NAT. Z tego powodu jeżeli obaj klienci znajdują się za symetrycznym NAT-em, nawiązanie połączenia P2P w ten sposób jest niemożliwe.

Diagram

03.2.2. STUN (Session Traversal Utilities for NAT)

03.2.3. TURN (Traversal Using Relays around NAT)

03.3. Wysokie opóźnienia i jitter

VPN z definicji nadaje dodatkowe opóźnienie ponad to bazowe, wynikające z sieci użytkownika. W modelu rozproszonym, opóźnienia są zminimalizowane ponieważ poszczególne urządzenia komunikują się bezpośrednio ze sobą. W modelu scentralizowanym, każdy pakiet musi niejako nadrobić drogę poprzez przejście przez serwer zanim trafi do odbiorcy.

Jest to zależne od zastosowania, jednak opóźnienie może mieć na tyle duży wpływ by kategorycznie wykluczyć wykorzystanie sieci wirtualnych w pewnych przypadkach.

03.4. Utrata pakietów

W tunelach UDP, utrata pakietów powoduje braki w danych, ale nie zatrzymuje całej transmisji. Natomiast w tunelach TCP może ona spowodować zjawisko TCP Meltdown. Zarówno protokół VPN, jak i aplikacja wewnątrz tunelu próbują jednocześnie retransmitować zgubione pakiety. Skutkuje to lawinowym wzrostem opóźnień, drastycznym spadkiem przepustowości i częstym zrywaniem sesji.

03.5. Blokada protokołu UDP

Blokuje działanie najwydajniejszych protokołów, które domyślnie korzystają z UDP.

04. Badane modele

05. Model scentralizowany

Cały ruch sieciowy jest przekierowywany przez centralny serwer. Nawet gdy oba urządzenia znajdują się blisko siebie, przesył danych dalej odbywa się z wykorzystaniem serwera jako pośrednika.

Konfiguracja i weryfikacja tożsamości użytkowników następuje na serwerze. Umożliwia to zarządzanie całą siecią, bez konieczności ponownego wdrażania poszczególnych klientów.

Sieć w oparciu o publiczny serwer, jako hub dla wszystkich węzłów, usuwa potrzebę nawiązywania bezpośrednich połączeń. Jest to duże uproszczenie w przypadku gdy klient znajduje się za symetrycznym NAT-em.

Centralny węzeł oznacza również pojedynczy punkt awarii oraz wąskie gardło. Przepustowość sieci jest ograniczona wydajnością łącza i procesora serwera centralnego.

06. Model rozproszony

Połączenia nawiązywane są bezpośrednio pomiędzy klientami sieci. Zmniejsza to opóźnienia do minimum. Połączenie może być nawiązane bez użycia dodatkowych serwerów. Opcjonalny serwer służy jedynie do wymiany informacji w procesie inicjalizacji połączenia dla klientów za NAT-em.

Obciążenie rozkłada się na poszczególne węzły, nie ma więc wąskiego gardła. Znika również pojedynczy punkt awarii, zwiększając odporność sieci.

Dla pewnych zastosowań, brak centralizacji staje się minusem. Włączanie nowych klientów do sieci jest utrudnione. Nie ma centralnej kontroli nad działaniem poszczególnych węzłów.

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.

- [1] **Autor:** Joel Anyam i in. **Rok:** 2025 **Tytuł:** Empirical Performance Analysis of WireGuard vs. OpenVPN in Cloud and Virtualised Environments Under Simulated Network Conditions **Link:** <https://www.mdpi.com/2073-431X/14/8/326>
- [2] **Autor:** Erik Dekker, Patrick Spaans **Rok:** 2020 **Tytuł:** Performance comparison of VPN implementations WireGuard, strongSwan, and OpenVPN in a 1 Gbit/s environment **Link:** <https://www.semanticscholar.org/paper/Performance-comparison-of-VPN-implementations-and-a-Dekker-Spaans/974a09aec089fd3d849e0abc11e6b78c5ef97a87>
- [3] **Autor:** Antonio Francesco Gentile i in. **Rok:** 2024 **Tytuł:** Overlay and Virtual Private Networks Security Performances Analysis with Open Source Infrastructure Deployment **Link:** <https://www.mdpi.com/1999-5903/16/8/283>
- [4] **Autor:** Vojdan Kjorveziroski i in. **Rok:** 2023 **Tytuł:** Full-mesh VPN performance evaluation for a secure edge-cloud continuum **Link:** https://www.researchgate.net/publication/382043739_Full-mesh_VPN_performance_evaluation_for_a_secure_edge-cloud_continuum

13. Załączniki

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