Łącza operatora: światłowód, radiolinia, LTE i 5G oraz przełączanie na FortiGate

Poziom: średnio

Dotyczy: łącza światłowodowe GPON i dedykowane, radiolinie, Starlink z publicznym, ale zmiennym adresem IPv4, LTE i 5G, SLA, FortiGate 100F (SD-WAN), adres publiczny 203.0.113.10, przykładowy adres Starlinka 203.0.113.30 i punkt zaczepienia w chmurze 203.0.113.60

Czas: ~140 min

Łącze operatora to droga, którą sieć Zielonej wychodzi do internetu, więc jego awaria zatrzymuje pocztę, VPN i część pracy w magazynie. Opisujemy rodzaje łączy, to, co znaczy SLA, jak połączyć dwa łącza na zaporze FortiGate i jak przyjmować ruch przychodzący, skoro Starlink daje publiczny adres IP, ale zmienny. Porównujemy trzy sposoby na taki adres: dynamiczny DNS, stały punkt wejścia w chmurze i usługi tunelowe, a na końcu stoją listy pytań do operatora i do Starlinka.

ZAŁOŻENIA SCENARIUSZA

w tym ćwiczeniu Starlink w Pamiątkowie ma publiczny, ale zmienny adres IPv4, a 203.0.113.30 to adres przykładowy z puli dokumentacyjnej, który po restarcie zestawu może być inny. Stałe adresy Zielonej to 203.0.113.10 na `wan1` i 203.0.113.60 proponowanej maszyny w chmurze `edge-az01`. Na stronach o tunelach (IPsec site-to-site, IPsec dla pracowników) przyjmujemy to samo, więc tam `fw01` inicjuje tunel ze Starlinka, a druga strona nie zna jego adresu z góry.

Skróty użyte na tej stronie (74)

Skrót	Co znaczy
API	Application Programming Interface: sposób, w jaki programy rozmawiają ze sobą
AWS	Amazon Web Services: chmura Amazonu
CA	Certificate Authority: urząd certyfikacji, który podpisuje certyfikaty

Skrót	Co znaczy
CGNAT	Carrier-Grade NAT: tłumaczenie adresów po stronie operatora, przy którym klient dostaje adres z zakresu 100.64.0.0/10 i nie przyjmie połączeń przychodzących z internetu
CIR	Committed Information Rate: szybkość łącza gwarantowana w umowie, w odróżnieniu od szybkości podanej jako „do”
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
CNAME	Canonical Name: rekord DNS będący aliasem, drugą nazwą wskazującą na już istniejący rekord A
DDNS	Dynamic DNS: usługa, w której zapora sama zgłasza dostawcy DNS nowy adres, gdy się zmieni, więc nazwa nadal wskazuje aktualny adres; używamy jej przy łączu ze zmiennym adresem, na przykład ze Starlinka
DDoS	Distributed Denial of Service: atak z wielu źródeł naraz, który zalewa łącze lub usługę ruchem, aż przestanie odpowiadać zwykłym użytkownikom
DHCP	Dynamic Host Configuration Protocol: usługa, która sama rozdaje komputerom adresy IP
DHCPv6-PD	DHCPv6 Prefix Delegation: mechanizm, w którym operator przydziela klientowi cały prefiks adresów IPv6 (na przykład /56), z którego router rozdaje adresy podsieciom
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
DPD	Dead Peer Detection: okresowe sprawdzanie, czy druga strona tunelu IPsec jeszcze żyje, żeby po awarii łącza tunel nie wyglądał na działający
EC2	Elastic Compute Cloud: usługa AWS wynajmująca gotowe maszyny wirtualne na godziny
EPEL	Extra Packages for Enterprise Linux: dodatkowe repozytorium pakietów dla RHEL i klonów
FQDN	Fully Qualified Domain Name: pełna nazwa hosta razem z domeną, np. docker01.ad.zielona.example
FTTH	Fiber To The Home: światłowód doprowadzony do domu lub budynku abonenta
GPON	Gigabit-capable Passive Optical Network: sieć światłowodowa, w której jedno włókno od operatora dzieli się na wielu abonentów przez pasywne rozgałęźniki; do 2,4 Gb/s w dół i 1,2 Gb/s w górę, wspólnie dla całego drzewa
HTTP	Hypertext Transfer Protocol: protokół stron WWW
HTTPS	HTTP zabezpieczony szyfrowaniem TLS
IETF	Internet Engineering Task Force: organizacja publikująca standardy internetowe jako dokumenty RFC
IKE	Internet Key Exchange: protokół, który przed popłynięciem danych dogaduje między dwiema stronami klucze i reguły szyfrowania tunelu IPsec
IKEv2	Internet Key Exchange w wersji 2: nowsza odmiana IKE, wbudowana w klienta VPN Windows, szybciej wraca do życia po zerwaniu łącza niż starsze protokoły VPN
IP	Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection)

Skrót	Co znaczy
IP56	stopień ochrony obudowy według normy IEC 60529: ochrona przed pyłem i silnym strumieniem wody; według dokumentacji tak oznaczony jest router Starlink Standard, przeznaczony do wnętrz
IP67	stopień ochrony obudowy według normy IEC 60529: szczelna dla pyłu i odporna na zanurzenie; według dokumentacji tak oznaczona jest antena Starlink Standard
IPsec	Internet Protocol Security: zestaw protokołów szyfrujących i uwierzytelniających ruch sieciowy, na nim stoi tunel VPN typu IKEv2
IPv4	Internet Protocol wersja 4: adresy zapisane czterema liczbami z kropkami, na przykład 10.20.10.77
IPv6	Internet Protocol wersja 6: nowszy, dłuższy zapis adresów, w liczbach szesnastkowych oddzielonych dwukropkami
ITU-T	International Telecommunication Union, Telecommunication Standardization Sector: sektor normalizacji Międzynarodowego Związku Telekomunikacyjnego, autor norm X.500 i X.509
LTE	Long Term Evolution: standard komórkowej sieci danych czwartej generacji, którego pierwsze komercyjne sieci ruszyły 14 grudnia 2009 roku
MCA-E	Microsoft Customer Agreement for enterprise: umowa Microsoft dla dużych klientów, w której maszyny w Azure mogą domyślnie wysyłać pocztę na porcie 25
MTA-STS	Mail Transfer Agent Strict Transport Security: zasada opublikowana przez domenę, że poczta do niej ma być wysyłana wyłącznie szyfrowanym połączeniem z serwerem o ustalonej nazwie
MTU	Maximum Transmission Unit: największy pakiet, jaki łącze przepuści bez dzielenia, zwykle 1500 bajtów w Ethernecie, a przy PPPoE 1492
MX	Mail Exchanger: rekord DNS wskazujący serwer poczty domeny
NAT	Network Address Translation: podmiana adresów IP na granicy sieci
NAT-T	NAT Traversal: opakowanie ruchu IPsec w UDP na porcie 4500, żeby przeszedł przez router z NAT, który nie przepuszcza ESP
OLT	Optical Line Terminal: urządzenie operatora w centrali, które obsługuje sieć GPON i rozmawia z urządzeniami u abonentów
ONT	Optical Network Terminal: urządzenie u abonenta, które kończy światłowód GPON i oddaje sygnał jako zwykły Ethernet
ONU	Optical Network Unit: urządzenie sieci optycznej po stronie abonenta, bliskie znaczeniowo ONT
OS2	Optical Single-mode 2: włókno jednomodowe 9/125 µm o małej tłumienności, do łączy między budynkami i na duże odległości, żółta kurtka
PPPoE	Point-to-Point Protocol over Ethernet: sposób logowania do operatora przez Ethernet, w którym łącze wymaga nazwy użytkownika i hasła, a MTU spada zwykle do 1492
PTR	rekord DNS odwrotny: zamienia adres IP na nazwę
RDP	Remote Desktop Protocol: protokół pulpitu zdalnego Windows, uruchamiany poleceniem mstsc
REST	sposób budowania API przez zwykłe żądania HTTP (GET, POST) zamiast osobnego protokołu

Skrót	Co znaczy
RFC	Request for Comments: oficjalny dokument opisujący standard internetowy, na przykład sposób działania danego protokołu; w ITIL także Request for Change, czyli wniosek o zmianę
RJ45	Registered Jack 45: potoczna nazwa ośmiostykowego wtyku i gniazda 8P8C, w którym kończymy kable skrętkowe Ethernetu
SAN	w certyfikatach: Subject Alternative Name, dodatkowe nazwy hosta w certyfikacie; w pamięciach: Storage Area Network, sieć dyskowa
SD-WAN	Software-Defined WAN: funkcja zapory FortiGate, która łączy kilka łączy WAN w jedną strefę, mierzy ich jakość sondą i wybiera łącze według reguł
SFP	Small Form-factor Pluggable: mały wymienny moduł (wkładka), który wsuwamy w gniazdo przełącznika albo karty sieciowej i który zamienia sygnał elektryczny na świetlny
SKU	Stock Keeping Unit: oznaczenie pozycji handlowej, na przykład konkretnej licencji lub modelu
SLA	Service Level Agreement: umowa o poziomie usług, np. 99,9% dostępności
SMB	Server Message Block: protokół udostępniania plików i drukarek w sieci Windows, na nim stoi zwykły udział sieciowy
SMTP	Simple Mail Transfer Protocol: protokół wysyłania poczty
SPF	Sender Policy Framework: rekord DNS mówiący, które serwery mogą wysyłać pocztę domeny
SSH	Secure Shell: szyfrowane zdalne logowanie do serwera
STARTTLS	włączenie szyfrowania w trakcie już nawiązanej, nieszyfrowanej sesji pocztowej
TCP	Transmission Control Protocol: protokół sieciowy z potwierdzaniem dostarczenia
TSIG	Transaction Signature: podpis kluczem wspólnym, którym serwer DNS potwierdza, że aktualizację rekordu wysłał uprawniony klient, na przykład FortiGate w genericDDNS według RFC 2136
TTL	Time To Live: czas życia rekordu lub danych
UDP	User Datagram Protocol: szybki protokół sieciowy bez potwierdzeń
UKE	Urząd Komunikacji Elektronicznej: polski organ nadzorujący rynek łączności i gospodarkę częstotliwościami radiowymi
UPS	Uninterruptible Power Supply: zasilacz awaryjny, podtrzymuje zasilanie urządzeń na czas zaniku napięcia z sieci
VIP	Virtual IP: adres wirtualny, który należy do roli, a nie do jednego serwera, i przechodzi na drugi host, gdy pierwszy przestaje odpowiadać
VLAN	Virtual LAN: wydzielona logicznie sieć na tym samym sprzęcie
VPC	Virtual Private Cloud: prywatna sieć wirtualna klienta w chmurze AWS, w której stawiamy maszyny i zakładamy tablice tras
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
WAN	Wide Area Network: sieć rozległa, czyli strona zapory zwrócona do internetu, na przykład interfejsy wan1 i wan2 zapory fw01

Skrót	Co znaczy
WebSocket	stałe, dwukierunkowe połączenie przeglądarki z serwerem, przez które Home Assistant na żywo odświeża panele; serwer pośredniczący musi przekazywać nagłówki Upgrade i Connection
Wi-Fi	Sieć bezprzewodowa: wygodna w biurze, ale w serwerowni dokłada kolejną możliwą przyczynę awarii
WMS	Warehouse Management System: system zarządzania magazynem
WWW	World Wide Web: strony i aplikacje otwierane w przeglądarce po HTTP albo HTTPS
XFRM	interfejs jądra Linuksa dla tuneli IPsec opartych na trasach: ruch skierowany trasą na taki interfejs jest szyfrowany, a strongSwan wiąże z nim tunel przez identyfikator if_id
ZTNA	Zero Trust Network Access: dostęp do pojedynczych aplikacji po sprawdzeniu użytkownika i stanu jego urządzenia, bez wpuszczania do całej sieci

Fiszka

Komendy FortiOS poniżej dotyczą mechanizmu SD-WAN. W wersji 6.4 i starszych polecenia zaczynają się od `diagnose sys virtual-wan-link`, a od wersji 7.4.4 polecenie `diagnose sys sdwan service` ma osobne warianty `service4` i `service6` [1].

□□ TYLKO ODCZYT

Odczyt członków SD-WAN i wybranego łącza: diagnose sys sdwan member

```
diagnose sys sdwan member
diagnose firewall proute list
```

> „ (pierwsze polecenie wypisuje członków SD-WAN z ich priorytetem i wagą, a drugie pokazuje, który interfejs wybrała reguła jako najlepszy [1])

□□ **SD-WAN** = Software-Defined WAN: funkcja zapory FortiGate, która łączy kilka łączy WAN w jedną strefę, mierzy ich jakość sondą i wybiera łącze według reguł

□□ TYLKO ODCZYT

Odczyt jakości łączy z sondy: diagnose sys sdwan health-check

```
diagnose sys sdwan health-check NazwaSondy
diagnose sys sdwan intf-sla-log NazwaInterfejsu
```

> (gdzie `NazwaSondy` to nazwa health-check, w terminologii FortiOS „Performance SLA”, a `NazwaInterfejsu` to na przykład `wan1`; wynik zawiera opóźnienie, jitter i utratę pakietów [1])

SLA = Service Level Agreement: umowa o poziomie usług, np. 99,9% dostępności

TYLKO ODCZYT

Odczyt reguły wyboru łącza: diagnose sys sdwan service

```
diagnose sys sdwan service4 NumerReguly
```

> (gdzie `NumerReguly` to numer reguły SD-WAN, a w wersjach starszych niż 7.4.4 polecenie ma postać `diagnose sys sdwan service NumerReguly` [1])

SD-WAN = Software-Defined WAN: funkcja zapory FortiGate, która łączy kilka łączy WAN w jedną strefę, mierzy ich jakość sondą i wybiera łącze według reguł

TYLKO ODCZYT

Test trasy z komputera: Test-NetConnection i mtr

```
Test-NetConnection AdresSerweraTestowego -TraceRoute
```

```
mtr -rwc 20 AdresSerweraTestowego
```

> (gdzie `AdresSerweraTestowego` to adres serwera, który odpowiada na ping i leży poza siecią Zielonej; pierwsza komenda działa w Windowsie, druga w Linuksie, jeśli pakiet `mtr` jest zainstalowany)

Przykład (poglądowy, mtr z `mon01` w czasie próby przełączenia):

```
HOST: mon01                  Loss%   Snt   Last   Avg  Best  Wrst
  1.|-- 10.20.10.1            0.0%    20    0.4   0.5   0.3   0.9
  2.|-- AdresBramyOperatora    0.0%    20    2.1   2.4   1.9   4.0
  3.|-- AdresSerweraTestowego 0.0%    20    9.8  10.2   9.5  12.1
```

Po przełączeniu na łącze zapasowe zmienia się drugi przeskok (inna brama operatora) i rośnie opóźnienie, więc porównujemy wynik z zapisem sprzed próby.

□□ **mtr** = mtr: Linux, łączy ping i traceroute i na bieżąco pokazuje straty i opóźnienia na każdym przeskoku do wskazanego adresu

□□ **TYLKO ODCZYT**

Odczyt adresu publicznego widzianego z internetu: curl

```
curl -s https://AdresUslugiPokazujacejIP
```

> (gdzie `AdresUslugiPokazujacejIP` to adres zewnętrznej usługi, która odpowiada adresem, z którego przyszło zapytanie; uruchamiamy z komputera w sieci Zielonej, więc wynik pokazuje łącze, którym ruch wychodzi w tej chwili)

Przykład (poglądowy, `mon01` przed próbą i po odłączeniu kabla `wan1`):

```
203.0.113.10
203.0.113.30
```

□□ **curl** = client URL: pobieranie i wysyłanie przez HTTP z terminala

□□ **TYLKO ODCZYT**

Odczyt stanu interfejsów zapory: get system interface physical

```
get system interface physical
```

> (polecenie FortiOS wypisuje interfejsy fizyczne z adresem IP, stanem łącza i szybkością portu; dla `wan2` szukamy adresu wydanego przez router

> Starlink w trybie bypass, a układ wyniku sprawdzamy w naszej wersji FortiOS)

IP = Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection)

TYLKO ODCZYT

Odczyt rekordów DNS i ich TTL: dig

```
dig +noall +answer vpn.zielona.example A
dig +noall +answer zielona.example MX
```

> (polecenia pytają o adres nazwy VPN i o rekordy MX domeny; druga kolumna wyniku to TTL w sekundach, czyli czas, przez który inne serwery pamiętają odpowiedź)

Przykład (poglądowy, po obniżeniu TTL przed próbą przełączenia):

```
vpn.zielona.example.    300    IN    A     203.0.113.10
zielona.example.        300    IN    MX    10 poczta.zielona.example.
zielona.example.        300    IN    MX    20 poczta2.zielona.example.
```

W Windowsie ten sam odczyt daje `Resolve-DnsName vpn.zielona.example -Type A` oraz `Resolve-DnsName zielona.example -Type MX`.

DNS = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP · **TTL** = Time To Live: czas życia rekordu lub danych · **VPN** = Virtual Private Network: szyfrowany tunel do sieci firmowej · **MX** = Mail Exchanger: rekord DNS wskazujący serwer poczty domeny · **dig** = domain information groper: odpytywanie DNS

ZMIENIA SYSTEM

Ustawienie drugiego interfejsu jako klienta DHCP: config system interface

```
config system interface
    edit "wan2"
```

```
        set mode dhcp
        set allowaccess ping
    next
end
```

Plik konfiguracyjny: w trybie bypass router Starlink wydaje zaporze adres przez DHCP, więc `wan2` ma tryb `dhcp`. Pozostałe opcje interfejsu i jego dołączenie do strefy SD-WAN sprawdzamy w dokumentacji naszej wersji FortiOS.

DHCP = Dynamic Host Configuration Protocol: usługa, która sama rozdaje komputerom adresy IP · **SD-WAN** = Software-Defined WAN: funkcja zapory FortiGate, która łączy kilka łączy WAN w jedną strefę, mierzy ich jakość sondą i wybiera łącze według reguł

TYLKO ODCZYT

Odczyt tuneli i tras na maszynie w chmurze: swanctl --list-sas

```
sudo swanctl --list-sas
ip route show 10.20.0.0/16
```

> (pierwsza komenda wypisuje ustanowione tunele IKE na `edge-az01` wraz z tożsamością partnera i stanem fazy 2, a druga pokazuje, którym interfejsem XFRM maszyna wysyła ruch do Zielonej; w stanie normalnym widzimy trasę przez `xfrm1`, a po awarii `wan1` przez `xfrm2` [48])

Przykład (poglądowy, `edge-az01` w czasie awarii `wan1`):

```
10.20.0.0/16 dev xfrm2 scope link metric 200
```

IKE = Internet Key Exchange: protokół, który przed popłynięciem danych dogaduje między dwiema stronami klucze i reguły szyfrowania tunelu IPsec · **XFRM** = interfejs jądra Linuksa dla tuneli IPsec opartych na trasach: ruch skierowany trasą na taki interfejs jest szyfrowany, a strongSwan wiąże z nim tunel przez identyfikator if_id · **swanctl** = strongSwan control: polecenie do ładowania konfiguracji i podglądu tuneli IPsec w strongSwan, na przykład swanctl --list-sas pokazuje ustanowione tunele · **ip** = narzędzie do adresów, tras i interfejsów sieciowych

ZMIENIA SYSTEM

Zgłaszanie adresu łącza do dynamicznego DNS: config system ddns

```
config system ddns
    edit 1
        set ddns-server FortiGuardDDNS
        set ddns-domain "NazwaHosta.float-zone.com"
        set use-public-ip enable
        set monitor-interface "wan2"
    next
end
```

Plik konfiguracyjny: wpis DDNS, w którym `fw01` zgłasza aktualny adres `wan2` do FortiGuard DDNS [24]. Po zmianie sprawdzamy, czy nazwa wskazuje adres odczytany poleceniem `get system interface physical`, a pełny opis wariantów jest w sekcji o trzech sposobach na ruch przychodzący.

DNS = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP · **DDNS** = Dynamic DNS: usługa, w której zapora sama zgłasza dostawcy DNS nowy adres, gdy się zmieni, więc nazwa nadal wskazuje aktualny adres; używamy jej przy łączu ze zmiennym adresem, na przykład ze Starlinka

Z życia wzięte

Z ŻYCIA WZIĘTE

Środa, 10:20. Koparka na drodze przy Pamiątkowie przecina kabel światłowodowy operatora, a `fw01` natychmiast traci łącze z internetem. Poczta przestaje wychodzić, pracownicy w domu nie łączą się przez VPN, a w magazynie część usług działa, a część nie i nikt nie wie, którędy idzie łącze do biura. Tomek dzwoni na numer pomocy z umowy: operator potwierdza awarię, ale czas naprawy to „do 24 godzin” i okazuje się, że umowa nie ma gwarantowanego czasu przywrócenia. Po południu Tomek wpina do wolnego portu `fw01` modem LTE, który przeleżał pół roku w szafie, i wychodzące połączenia wracają, ale VPN z domów nadal nie działa, bo adres 203.0.113.10 jest tylko na zepsutym łączu. Do notatki po awarii Tomek zapisuje wniosek: łącze zapasowe ma mieć własny adres publiczny, bo inaczej chroni tylko ruch wychodzący.

Skąd się wzięło

Pierwsze komercyjne sieci LTE ruszyły 14 grudnia 2009 roku w Sztokholmie i Oslo [2]. Standard GPON, czyli sieci światłowodowej, w której jeden światłowód od operatora dzieli się na wielu abonentów, został uchwalony w 2003 roku jako ITU-T G.984 [3]. Z czasem światłowód zaczął

docierać do domów i firm, a LTE i potem 5G dały zapasowy kanał bez kabla.

Internet z satelitów na niskiej orbicie ma krótszą historię. SpaceX wyniosło pierwsze sześćdziesiąt satelitów Starlink 24 maja 2019 roku [13], a 10 lutego 2021 roku w Polsce ruszyła przedsprzedaż zestawów [14]. W czerwcu 2026 roku konstelacja liczyła według Wikipedii około 10,4 tysiąca satelitów [5].

Antena Starlink.

Antena Starlink. Źródło: Wikimedia Commons (autor i wolna licencja podane na stronie pliku).

Moduł FRITZ!SFP GPON.

Moduł FRITZ!SFP GPON. Źródło: Wikimedia Commons (autor i wolna licencja podane na stronie pliku).

Urządzenie ONU w sieci FTTH.

Urządzenie ONU w sieci FTTH. Źródło: Wikimedia Commons (autor i wolna licencja podane na stronie pliku).

Rodzaje i zasada działania

Światłowód GPON

> **Pojęcie: GPON.** Gigabit-capable Passive Optical Network, czyli sieć, w której jeden światłowód od centrali operatora przechodzi przez pasywne rozgałęźniki (splittery) do wielu abonentów. Centrala to OLT, a urządzenie u klienta to ONT albo ONU.

Prędkość GPON w dół wynosi do 2,4 Gb/s, a w górę do 1,2 Gb/s, wspólnie dla wszystkich abonentów jednego drzewa, przy długościach fali 1490 i 1310 nm [3]. Typowy podział to 16 do 64 abonentów na jednym włóknie [3]. Łącze jest tanie, ale niesymetryczne i współdzielone, więc umowa zwykle nie gwarantuje stałej szybkości, a czas naprawy bywa dłuższy niż przy łączu dedykowanym.

Łącze dedykowane

Światłowód dedykowany to osobne włókno albo osobna usługa od budynku do węzła operatora, bez dzielenia z sąsiadami. Daje szybkość symetryczną, często gwarantowaną (CIR), jednoznaczny SLA i krótszy czas naprawy. Kosztuje wielokrotnie więcej niż GPON, więc kupujemy je, gdy awaria jednego dnia kosztuje więcej niż różnica w opłacie.

Radiolinia

Radiolinia łączy dwa punkty falą radiową z antenami kierunkowymi i potrzebuje widoczności między nimi. W pasmach bezlicencyjnych, na przykład 5 GHz, jakość zależy od zakłóceń od innych sieci, a w pasmach licencjonowanych operator ma wyłączność, ale potrzebuje pozwolenia. Radiolinia sprawdza się tam, gdzie kable nie dochodzą, na przykład między budynkami albo jako druga droga o innej trasie niż światłowód. Wymagania UKE co do pozwoleń i mocy sprawdzamy przed zakupem, bo ich dokładnych numerów tu nie podajemy.

Maszt z anteną radiową (Microwave Radio Antenna Tower).

Maszt z anteną radiową (Microwave Radio Antenna Tower). Źródło: Wikimedia Commons (autor i wolna licencja podane na stronie pliku).

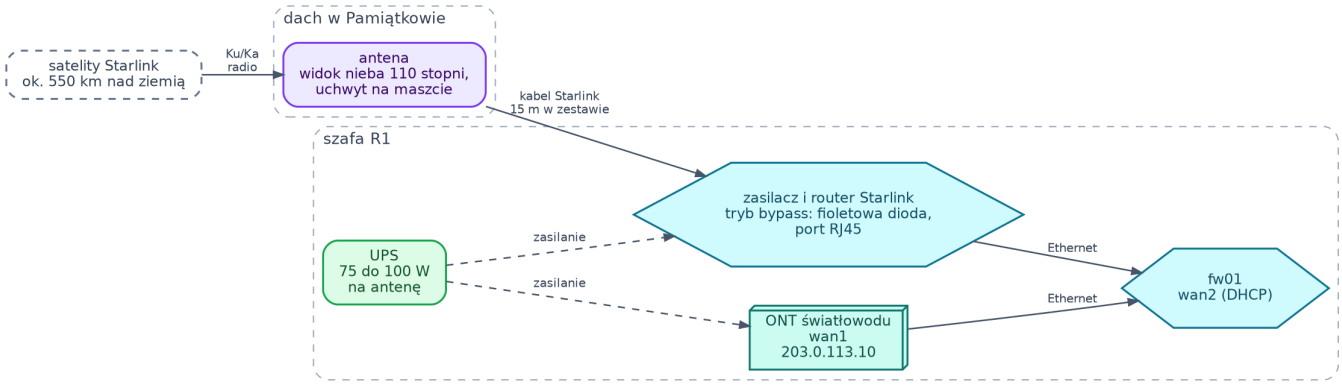
Starlink: internet z satelitów na niskiej orbicie

> **Pojęcie: orbita niska (LEO).** Low Earth Orbit, czyli orbita na wysokości od kilkuset do około dwóch tysięcy kilometrów nad ziemią. Satelity Starlink krążą na wysokości około 550 km, a satelita stacjonarny wisi dużo wyżej, więc sygnał pokonuje krótszą drogę [5].

Zestaw składa się z płaskiej anteny z elektronicznie sterowaną wiązką (phased array), która sama śledzi przelatujące satelity, oraz zasilacza z routerem w środku budynku [5][8]. Satelity szybko przelatują nad głową, więc antena nieustannie przełącza się na kolejny. Opóźnienie wynosi zwykle około 25 do 50 ms, a według opisu planów biznesowych w Polsce szybkość pobierania to 135 do 310 Mb/s, a wysyłania 20 do 44 Mb/s [7][16]. Teoretyczne minimum dla satelity stacjonarnego to 477 ms, więc różnica jest ogromna [5].

Antena potrzebuje czystego widoku nieba: dokumentacja zestawu Standard podaje pole widzenia 110 stopni, a każda gałąź, komin czy dach na drodze do satelity przerywa łączność [8]. Pobór mocy zestawu Standard to średnio 75 do 100 W, a zasilacz przyjmuje 100 do 240 V [8]. Antena ma

stopień ochrony IP67, a router tylko IP56, więc router zostaje w budynku [8].



Rysunek 1. Tor sygnału Starlinka w Pamiątkowie: satelity, antena na dachu, kabel do szafy R1, zasilacz z routerem w trybie bypass, zapora fw01 i zasilanie z UPS. Warto zauważyć, że w trybie bypass router tylko przekazuje ruch do portu zapory i nie robi własnego NAT. (kliknięcie otwiera pełny rozmiar)

Plany dzielimy na domowe i biznesowe. W planach domowych Starlink stosuje CGNAT, a w biznesowych planach Priority (nazywanych po polsku „Priorytetowe Lokalne” i „Priorytetowe Globalne”) dane dzielą się na bloki danych priorytetowych, a nowe plany Priority mają według producenta umowną dostępność sieci 99,9 procent (bez zestawu Mini) [6][7].

> **Pojęcie: CGNAT.** Carrier-Grade NAT, czyli tłumaczenie adresów po stronie operatora. Klient dostaje adres z zakresu 100.64.0.0/10, zarezerwowanego do tego celu w RFC 6598, a nie adres publiczny [4].

Przy CGNAT połączenia przychodzące z internetu do firmy nie docierają, więc plan domowy Starlinka nadaje się dla ruchu wychodzącego, ale nie dla VPN ani poczty przychodzącej [10][11]. Plany biznesowe Priority mają opcję publicznego adresu IPv4: według opisu planów w Polsce z września 2026 roku obejmują one publiczny adres IP [7], a według opisów w sieci jest to konfiguracja opcjonalna, którą włączamy w koncie [17][18]. Pomoc Starlink ma artykuł „How do I set my IP address to a public IP?” [15], ale jego treść ładuje się skryptem i nie udało nam się jej odczytać, więc warunków dla Polski (które plany, czy za dopłatą) nie potwierdziliśmy i zostawiamy je jako pytania do Starlinka.

Najważniejsze jest to, czego nie ma: stałego adresu. Zestawiamy, co ustaliliśmy z kilku niezależnych opisów (stan na październik 2026), a gdzie źródła się różnią, piszemy to wprost.

Pytanie	Ustalenie	Źródła
Czy Starlink oferuje stały adres IPv4 w jakimkolwiek planie?	nie, w żadnym planie, także biznesowym	[10][17][18][19]

Pytanie	Ustalenie	Źródła
Czy plan biznesowy daje publiczny adres?	tak, jako opcja planów Priority (także Mobile Priority i Maritime), adres jest routowalny, ale dynamiczny	[17][18]
Co mają plany domowe?	CGNAT z zakresu 100.64.0.0/10, połączenia przychodzące są zablokowane	[4][17][18]
Kiedy adres się zmienia?	po restarcie zestawu, po przeniesieniu zestawu i przy pracach sieci; jeden opis podaje przydział przez DHCP z wiązaniem adresu z urządzeniem na 24 godziny, a sprzedawcy opisują adres „lepki”, który zwykle zostaje, ale bez gwarancji	[18][19][20]
IPv6?	tak, prefiks delegowany przez DHCPv6-PD; większość opisów mówi o /56, wątek użytkowników o /64, więc długość sprawdzamy na naszym zestawie	[17][18][21][22]
Czy źródła się zgadzają?	nie do końca: jeden artykuł prasowy pisze, że nawet klienci biznesowi dostają zwykle CGNAT, co zgadza się z tym, że publiczny adres to opcja do włączenia, a nie ustawienie domyślne	[23]

Wniosek jest prosty: adres na `wan2` będzie publiczny, jeśli włączymy opcję, ale zmieni się przy najbliższym restarcie, więc niczego, co ma przetrwać, nie wiążemy na stałe z jego numerem.

> **Pojęcie: dynamiczny adres publiczny.** Adres routowalny w internecie, który operator przydziela na czas, a nie na stałe. Może się zmienić po restarcie sprzętu albo pracach sieci, więc nazwy DNS, tunele i listy dozwolonych adresów, które opierają się na numerze, przestają działać.

Dla IPv6 opisy podają, że Starlink deleguje klientowi prefiks, a urządzenia za routerem dostają adresy publiczne [18][21]. Domyślna zapora routera Starlink blokuje ruch przychodzący IPv6, a prefiks, choć stabilniejszy, nie jest gwarancją stałego adresu [21][22]. W Zielonej nie planujemy IPv6 wewnątrz sieci, więc VPN i pocztę opieramy na IPv4.

Router Starlink w zwykłym trybie tłumaczy adresy (NAT), więc za nim powstaje drugi NAT i połączenia przychodzące do `fw01` nie dochodzą. Dlatego włączamy tryb bypass: według opisu sprzedawcy w zestawie Standard Gen 3 robimy to w aplikacji Starlink, router przestaje rozgłaszać Wi-Fi, świeci fioletową diodą, a wyjście z trybu wymaga resetu fabrycznego [9]. Zestawy Standard Gen 2 potrzebują przejściówki Ethernet, a zestaw High Performance nie wymaga bypassu [9]. Który wariant mamy w ręku, sprawdzamy w instrukcji kupionego zestawu.

LTE i 5G: trzecia droga

Łącze komórkowe zostaje opcją na trzecią drogę, gdyby padły oba łącza stacjonarne albo antena Starlink przestała widzieć niebo. Operator komórkowy zwykle stosuje CGNAT, więc połączenia przychodzące nie dotrą. Szybkość zmienia się z porą dnia i zasięgiem, a opłata bywa naliczana za wolumen, więc stały adres publiczny za dodatkową opłatą sprawdzamy w ofercie. W Zielonej nie planujemy dziś łącza komórkowego jako członka SD-WAN.

Router 4G LTE.

Router 4G LTE. Źródło: Wikimedia Commons (autor i wolna licencja podane na stronie pliku).

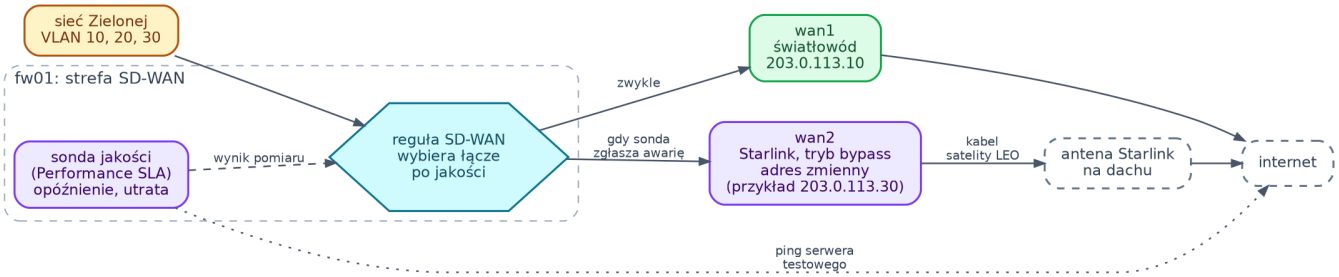
SLA: co operator obiecuje

> **Pojęcie: SLA.** Service Level Agreement, czyli umowa o poziomie usługi. Zawiera dostępność w procentach, czas reakcji i czas naprawy oraz kary za niedotrzymanie.

Dostępność przekładamy na godziny przestoju w roku, mnożąc 8760 godzin przez dopuszczalny ułamek niedostępności: 99 procent oznacza 87,6 godziny, 99,5 procent 43,8 godziny, 99,9 procent 8,76 godziny, a 99,95 procent 4,38 godziny. Sama dostępność nie mówi, jak długo trwa pojedyncza awaria, więc równie ważne są czas reakcji i maksymalny czas naprawy z umowy.

Dwa łącza i SD-WAN na FortiGate

> **Pojęcie: SD-WAN na FortiGate.** Funkcja zapory, która łączy kilka interfejsów WAN w jedną strefę, mierzy jakość każdego łącza sondą i wybiera łącze według reguł. W FortiOS używamy nazw: członkowie (members), strefa (zone), sonda „Performance SLA” (w konfiguracji health-check) i reguły „SD-WAN rules” (w konfiguracji service) [1].



Rysunek 2. Dwa łącza w Zielonej: wan1 światłowodowe z adresem 203.0.113.10, wan2 Starlink w trybie bypass z adresem 203.0.113.30, strefa SD-WAN na fw01 z regułą wyboru łącza i sondą jakości. Warto zauważyć, że sonda mierzy łącze osobnym pakietem do serwera testowego, a nie ruchem użytkowników. (kliknięcie otwiera pełny rozmiar)

Interfejs zostaje członkiem SD-WAN dopiero wtedy, gdy nie jest użyty bezpośrednio w trasach statycznych ani w politykach, więc przy przejściu na SD-WAN przenosimy je do strefy i odwołujemy się do niej [1]. Poniżej szkic konfiguracji, w którym `AdresBramyWan1`, `AdresBramyWan2` i `AdresSerweraTestowego` są do uzupełnienia, a dokładną składnię sekcji `sla` i `service` sprawdzamy w dokumentacji naszej wersji FortiOS:

```
config system sdwan
    set status enable
    config members
        edit 1
            set interface "wan1"
            set gateway AdresBramyWan1
        next
        edit 2
            set interface "wan2"
            set gateway AdresBramyWan2
        next
    end
    config health-check
        edit "SondaOperatora"
            set server "AdresSerweraTestowego"
            set members 1 2
        next
    end
    config service
        edit 1
            set mode priority
            set priority-members 1 2
            set health-check "SondaOperatora"
```

```
        next
    end
end
```

W takiej konfiguracji ruch wychodzi przez członka 1 (`wan1`), a gdy sonda zgłasza awarię, reguła wybiera członka 2 (`wan2`, czyli Starlink). Istniejące sesje przez `wan1` w chwili awarii zrywają się, a nowe idą przez `wan2`. Bramę dla `wan2` wydaje router Starlink przez DHCP, więc sprawdzamy w dokumentacji naszej wersji FortiOS, czy dla interfejsu z DHCP wpis `gateway` jest w ogóle potrzebny.

Wszystkie rodzaje w jednej tabeli

Rodzaj	Szybkość	Gwarancja	Adres publiczny	Typowa rola
GPON (światłowód)	do około 2,4 Gb/s w dół, współdzielone	zwykle brak CIR	stały lub zmienny, zależnie od oferty	podstawowe łącze małej firmy
Łącze dedykowane	symetryczne, z gwarancją	SLA z karami	stały, często blok adresów	podstawowe łącze firmy zależnej od sieci
Radiolinia	zależna od pasma i odległości	zależna od umowy	zależnie od operatora	druga droga albo połączenie między budynkami
Starlink (plan domowy)	zmienna, opóźnienie około 25 do 50 ms	brak	CGNAT	zapas dla ruchu wychodzącego
Starlink (plan biznesowy z publicznym IP)	według opisu 135 do 310 Mb/s w dół i 20 do 44 Mb/s w górę	SLA 99,9 procent według producenta, do potwierdzenia dla Polski	publiczny, dynamiczny (stałego adresu Starlink nie oferuje)	zapasowe łącze Zielonej na `wan2`
LTE i 5G	zmienna	zwykle brak	często CGNAT	opcja na trzecią drogę

W serwerowni

Zielona ma dziś jedno łącze z adresem 203.0.113.10 na interfejsie `wan1` zapory `fw01`. Decyzja autora bazy jest taka, że drugim łączem w Pamiątkowie jest Starlink z publicznym adresem IPv4, wpięty do drugiego portu WAN i połączony z `wan1` w strefie SD-WAN. Według oferty sprzedawcy FortiGate 100F ma dwa porty WAN RJ45, co potwierdzamy w karcie katalogowej. W dokumentacji adres Starlinka to przykładowe 203.0.113.30 (wyszukiwanie po całej bazie potwierdza, że nie jest używany nigdzie indziej), ale prawdziwy adres wyda Starlink, będzie dynamiczny i może się zmienić [17][18].

Zapora jest pojedynczym urządzeniem, więc awaria `fw01` nadal zatrzyma całą sieć, a drugie łącze chroni tylko przed awarią operatora, kabla albo przerwą w dostawie światłowodu. Dzięki własnemu adresowi publicznemu na `wan2` w awarii działa ruch wychodzący, a ruch przychodzący (VPN i poczta) wymaga jednego z trzech sposobów opisanych niżej, bo adres jest zmienny.

Wybór miejsca i montaż anteny

Antena Starlink potrzebuje widoku nieba, a dokumentacja zestawu Standard podaje pole widzenia 110 stopni i zaleca aplikacyjne narzędzie do sprawdzania przeszkód przed montażem [8]. Dlatego miejsce wybieramy w aplikacji, zanim ktokolwiek zrobi otwór w dachu.

Co	Jak robimy	Skąd wiemy
Miejsce	dach budynku w Pamiątkowie, możliwie blisko szafy R1, z dala od kominów, wentylatorów i drzew	pole widzenia 110 stopni i przerwy od przeszkód [8]
Uchwyt	maszt albo wspornik dopasowany do zestawu, mocowany do konstrukcji dachu przez wykonawcę	instrukcja kupionego zestawu
Przewód	kabel Starlink z zestawu Standard ma 15 m, prowadzimy go bez ostrych zagięć i z uszczelnionym wejściem do budynku	dokumentacja zestawu [8]
Dłuższa trasa	dłuższy kabel kupujemy u producenta, bez własnych przedłużek i złączy	do potwierdzenia w ofercie Starlinka
Zasilanie	zasilacz i router w szafie R1, na wyjściu UPS	pobór średnio 75 do 100 W [8]
Ochrona	pytamy wykonawcę o uziemienie masztu i ochronę przeciwprzepięciową	antena jest najwyższym punktem budynku

Do bilansu UPS dokładamy około 100 W na zestaw Starlink i sprawdzamy czas na baterii według strony UPS: topologie, dobór i baterie. Na UPS stawiamy też urządzenie końcowe światłowodu (ONT), bo przy braku prądu oba łącza muszą żyć tak długo jak zapas energii, a nie tylko jedno.

Podłączenie do fw01: bypass i drugi WAN

Kolejność ma znaczenie, bo adres publiczny trzeba włączyć zanim `wan2` dostanie adres, a bypass zabiera Wi-Fi Starlinka i wymaga resetu, żeby z niego wyjść [9].

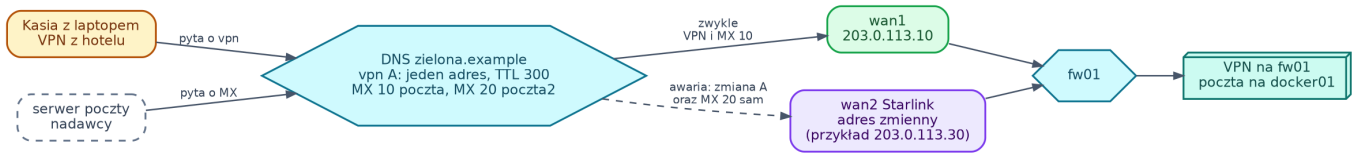
1. Uruchamiamy zestaw w zwykłym trybie, sprawdzamy przeszkody w aplikacji i aktualizujemy oprogramowanie.
2. W koncie Starlink włączamy opcję publicznego adresu IP, o ile plan ją ma (warunki do potwierdzenia, patrz pytania niżej).

3. W aplikacji włączamy tryb bypass, a kabel Ethernet z routera Starlink wpinamy do `wan2` zapory.
4. Ustawiamy `wan2` jako klienta DHCP (fiszka wyżej) i sprawdzamy adres poleceniem `get system interface physical`.
5. Dodajemy `wan2` jako członka 2 strefy SD-WAN według szkicu powyżej i przenosimy do strefy trasy i polityki, które wskazywały `wan1`.
6. Sprawdzamy przełączanie próbą opisaną niżej, zanim uznamy łącze za gotowe.

Oczekujemy, że `wan2` dostanie adres publiczny, w dokumentacji przykładowo 203.0.113.30, a odczytany adres zapisujemy z datą i spodziewamy się, że po restarcie zestawu będzie inny. Jeśli dostanie adres z zakresu 100.64.0.0/10, to nadal jest CGNAT, czyli opcja publicznego adresu nie działa na naszym planie albo w trybie bypass, i wracamy do pytań do Starlinka. Dopóki tego nie sprawdzimy w teście, nie obiecujemy nikomu VPN przez Starlinka.

Adres zmienny i DNS dla VPN i poczty

Sam adres na `wan2` jeszcze niczego nie przełącza: klienci i serwery świata znają nazwy, a nazwy wskazują dziś 203.0.113.10. Przełączanie robimy w DNS strefy `zielona.example`, a czas, przez który inni pamiętają starą odpowiedź, to TTL. Adres `wan2` jest zmienny, więc rekord wpisany ręcznie z adresem Starlinka przestaje być prawdziwy po pierwszym restarcie anteny. Dlatego po tej sekcji opisujemy trzy sposoby, jak ten kłopot obejść.



Rysunek 3. Przełączanie usług w DNS: nazwa VPN wskazuje jeden adres i zmieniamy ją w awarii, a pocztę obsługują dwa rekordy MX o różnych priorytetach, więc nadawca sam próbuje drugi. Warto zauważyć, że oba adresy kończą na tej samej zaporze fw01, a adres wan2 jest zmienny. (kliknięcie otwiera pełny rozmiar)

Usługa	Rekordy DNS	Jak działa przełączenie	Kto je robi
VPN	`vpn.zielona.example` A, TTL 300 s	w awarii zmieniamy adres z 203.0.113.10 na aktualny adres `wan2` (wariant a) albo na stały adres `edge-az01` (wariant b)	my albo skrypt, na początku według alarmu z Zabbixa

Usługa	Rekordy DNS	Jak działa przełączenie	Kto je robi
Poczta przychodząca	`MX 10 poczta.zielona.example` (203.0.113.10) i `MX 20 poczta2.zielona.example` (w wariancie b adres `edge-az01`, w wariancie a nazwa z dynamicznego DNS)	oba rekordy stoją stale, nadawca przy braku odpowiedzi na priorytecie 10 próbuje 20	serwer nadawcy sam
Poczta wychodząca	SPF z adresem 203.0.113.10 i z przekaźnikiem, PTR dla stałego adresu	w awarii wiadomości wychodzą przez przekaźnik, bo adres Starlinka jest zmienny i nie ma PTR	zapora i MailCow, jeśli SPF i przekaźnik są gotowe

Dla VPN nie wystarczy druga nazwa w profilu Windows. Opis konfiguracji VPNv2 mówi, że lista serwerów w profilu to wybór użytkownika, a klient używa tylko wybranego serwera i nie próbuje kolejnych automatycznie [12]. Dwa rekordy A pod jedną nazwą rozdzielałyby użytkowników po połowie, a zachowanie klienta VPN przy dwóch adresach musielibyśmy sprawdzić w teście, więc wybieramy jeden rekord i jego zmianę.

Czas na zmianę skracamy, obniżając TTL do 300 sekund co najmniej dobę przed pierwszą próbą, bo wcześniejsze odpowiedzi wygasają dopiero po starym TTL. Część serwerów DNS nie respektuje krótkich TTL, więc nie obiecujemy zmiany co do sekundy.

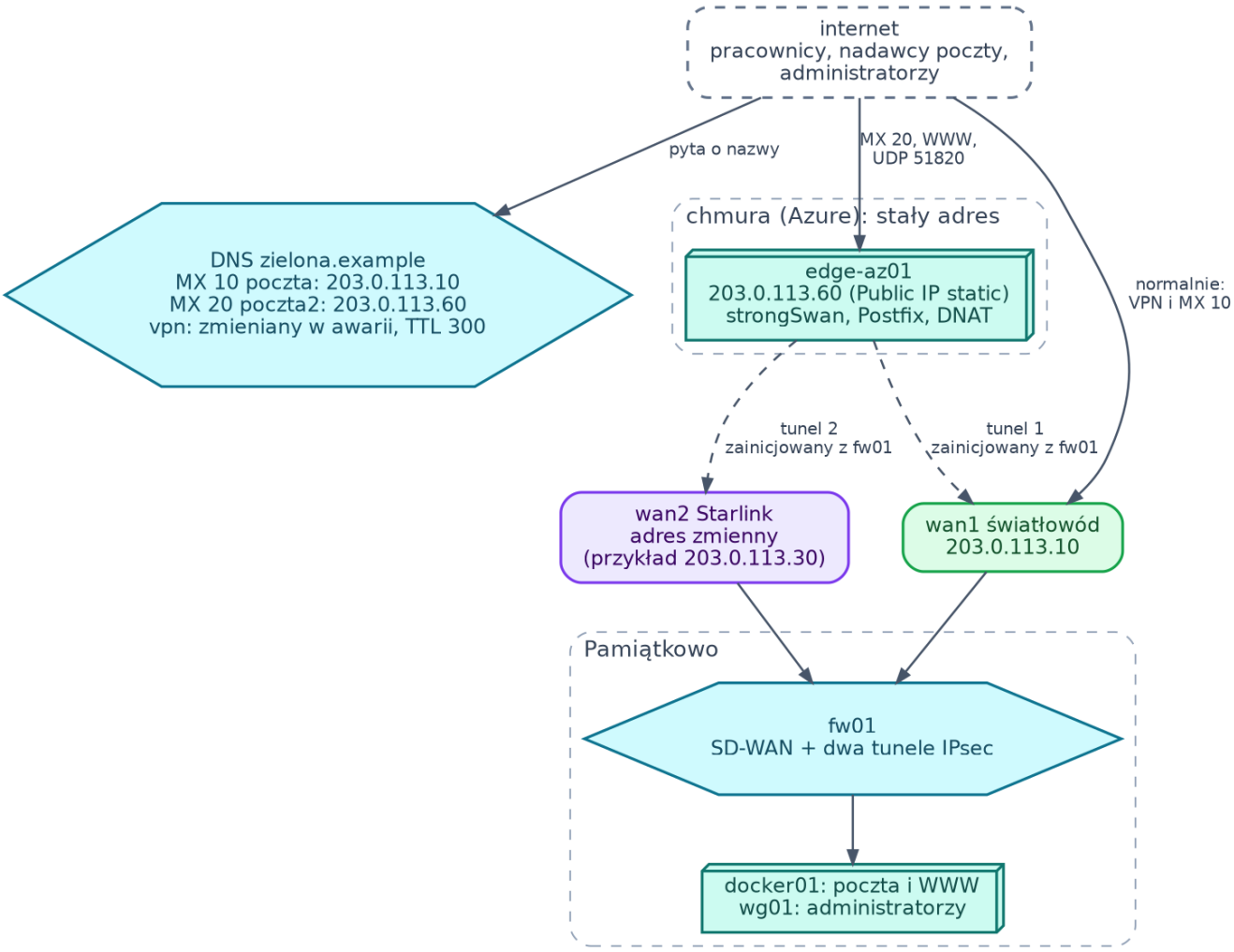
Tunel IKEv2 z EAP-TLS i FSSO: logowanie do VPN certyfikatem użytkownika i grupami z AD ma w przykładzie `set interface "wan1"`, więc słucha tylko na jednym interfejsie. Dla `wan2` potrzebujemy drugiej definicji tunelu albo innego rozwiązania opisanego w dokumentacji naszej wersji FortiOS. Sprawdzamy też, czy odpowiedzi IKE wychodzą tym samym łączem, którym przyszło zapytanie, bo przy złym wyborze trasy tunel nie powstanie. Do zatwierdzenia przez autora zostaje to, kto prowadzi strefę `zielona.example` i czy ma automatyczną zmianę rekordu przez API albo kontrolę stanu.

Dla poczty dokładamy kilka rzeczy do MailCow: instalacja w Dockerze. Przekierowanie portów pocztowych na `docker01` dla `wan2` tworzymy jako obiekt VIP związany z interfejsem `wan2`, bo przekierowanie jest związane z interfejsem. Ponieważ adres `wan2` jest zmienny, w obiekcie VIP dla interfejsu z adresem z DHCP Fortinet zaleca zewnętrzny adres 0.0.0.0, a nie konkretny numer [27]. Nazwę `poczta2.zielona.example` dopisujemy do certyfikatu MailCow, jak opisuje dokumentacja MailCow.

Rekord SPF rozszerzamy tylko o adresy stałe: 203.0.113.10 oraz przekaźnik, przez który wychodzimy w awarii. Adresu zmiennego Starlinka do SPF nie wpisujemy na stałe, bo po zmianie adresu rekord kłamałby, a rekord PTR dla adresu ze Starlinka ustawia właściciel adresu, więc pytamy Starlinka, czy to w ogóle umożliwia. Poczta przychodząca nie ginie przy krótkiej awarii nawet bez MX 20, bo serwery nadawców ponawiają dostarczanie, a drugi rekord skraca opóźnienie.

Trzy sposoby na ruch przychodzący przez zapasowe łącze

Ruch przychodzący (VPN, poczta, strony WWW) potrzebuje adresu, który świat zna z góry, a adres Starlinka tego nie daje. Są trzy drogi: nazwa DNS podążająca za adresem (dynamiczny DNS), stały punkt wejścia w chmurze, do którego `fw01` dzwoni tunelem, oraz usługi, w których to Zielona łączy się na zewnątrz i nie potrzebuje adresu przychodzącego. Rysunek pokazuje wariant b, bo jest najbardziej złożony.



Rysunek 4. Punkt zaczepienia w chmurze: maszyna edge-az01 ze stałym adresem 203.0.113.60 trzyma dwa tunele IPsec do fw01, jeden przez wan1 i jeden przez wan2, a ruch z internetu (MX 20, WWW, WireGuard administratorów) wchodzi na stały adres i idzie tunelem do Zielonej tym łączem, które działa. Warto zauważyć, że tunele inicjuje fw01, więc zmienny adres Starlinka nie ma znaczenia dla ich zestawienia. (kliknięcie otwiera pełny rozmiar)

Pojęcie: DDNS. Dynamic DNS, czyli usługa, w której zapora sama zgłasza dostawcy DNS nowy adres, gdy się zmieni, a nazwa nadal wskazuje aktualny. Rekord ma krótki TTL, więc zmiana adresu jest widoczna po kilku minutach, nie po dobie.

Pojęcie: punkt zaczepienia w chmurze. Mała maszyna wirtualna ze stałym adresem publicznym u dostawcy chmury (Azure albo AWS), z którą `fw01` ma stałe tunele przez oba łącza. Ruch z internetu wchodzi na stały adres maszyny i idzie tunelem do Zielonej tym łączem, które akurat działa. W Zielonej proponujemy maszynę `edge-az01` z adresem 203.0.113.60 (adres przykładowy, bo prawdziwy wyda dostawca).

Cecha	(a) Dynamiczny DNS	(b) Punkt zaczepienia w chmurze	(c) Usługi tunelowe bez publicznego IP
Jak działa	nazwa DNS wskazuje aktualny adres `wan2`, aktualizowany przez `fw01` albo skrypt	stały adres w chmurze, dwa tunele IPsec z `fw01`, ruch wchodzi na chmurę	agent w Zielonej łączy się na zewnątrz z usługą, klienci łączą się z usługą
Co obsługuje	VPN, WWW i poczta z ograniczeniami	przekaźnik poczty, WWW, WireGuard administratorów, VPN pracowników (po teście)	wybrane aplikacje webowe, SSH i RDP administratorów, nie pocztę od obcych serwerów
Adres w profilu VPN	nazwa, bez zmian	nazwa, bez zmian (rekord wskazuje chmurę)	nie dotyczy
Czas przełączenia	czas aktualizacji DDNS plus TTL	tunel jest już gotowy, zmieniamy rekord VPN, a MX 20 działa sam	brak przełączania
Poczta i PTR	brak PTR dla adresu Starlinka, część odbiorców odrzuca taką pocztę	PTR dla stałego adresu w chmurze (Azure: właściwość ReverseFqdn, AWS: formularz)	nie dotyczy
Zależność od	dostawca DNS i jego sposób aktualizacji	dostawca chmury i maszyna do łatania	usługa zewnętrzna, jej plan i limity
Koszt jako struktura	brak nowej maszyny, ewentualna opłata dostawcy DDNS	maszyna, dysk, publiczny adres IPv4, ruch wychodzący z chmury	plan usługi, często zależny od liczby użytkowników
Złożoność	mała	średnia	mała do średniej
Główna wada	chwila bez usługi po zmianie adresu, adres w listach partnerów, brak PTR	dodatkowy host do utrzymania i koszt	nie zastępuje VPN dla całej sieci, poczta nie przechodzi

Wariant a: dynamiczny DNS na fw01

FortiOS ma klienta DDNS w `config system ddns`. Obsługuje FortiGuard DDNS (nazwy w domenach fortiddns.com, fortidyndns.com albo float-zone.com [24]), gotowe serwisy z listy (między innymi dyndns.org i noip.com) oraz genericDDNS zgodny z RFC 2136, czyli aktualizację rekordu własnego serwera DNS [25]. Dostawcę, który ma tylko API HTTP i nie zna RFC 2136, nie wpiszemy w tę sekcję, więc w takim wypadku rekord aktualizuje skrypt na `mon01` uruchamiany z alarmu Zabbixa. Taki skrypt trzeba by zbudować i to jest decyzja autora, a w dokumentacji naszej wersji FortiOS sprawdzamy, czy lista dostawców nie urosła.

```
config system ddns
    edit 1
        set ddns-server FortiGuardDDNS
        set ddns-domain "NazwaHosta.float-zone.com"
        set use-public-ip enable
        set monitor-interface "wan2"
    next
end
```

Plik konfiguracyjny: wpis dla `wan2` w FortiGuard DDNS. Opcja `use-public-ip` jest według Fortinet dostępna tylko dla FortiGuardDDNS i noip.com [25]. Dla `wan1` wpisu nie tworzymy, bo ma stały adres, a gdyby miał być zmienny, dodajemy drugi wpis z własnym `monitor-interface` [51]. Zapora wysyła aktualizację przez łącze, którego dotyczy, więc po zmianie adresu mija chwila, zanim nazwa zacznie wskazywać nowy.

Dla własnej strefy mamy wariant genericDDNS z kluczem TSIG, w którym FortiGate używa algorytmu HMAC-MD5 bez możliwości zmiany [26]:

```
config system ddns
    edit 2
        set ddns-server genericDDNS
        set ddns-server-addr "ddns.zielona.example"
        set ddns-domain "wan2.ddns.zielona.example"
        set ddns-zone "ddns.zielona.example"
        set ddns-auth tsig
        set ddns-keyname "NazwaKlucza"
        set ddns-key "KluczTsig"
        set monitor-interface "wan2"
    next
end
```

Czy DNS publiczny strefy `zielona.example` przyjmie taką aktualizację, zależy od dostawcy strefy, więc wskazujemy osobną poddomenę `ddns.zielona.example`, którą może obsłużyć serwer z obsługą RFC 2136. Kto prowadzi strefę i czy ma API, rozstrzyga strona Domena i strefa publiczna:

rejestrator, dostawca DNS, odnowienia i blokady: strefa jest w Azure DNS, który zmienia rekordy przez portal, Azure CLI i REST API, a aktualizacji według RFC 2136 w jego dokumentacji nie znaleźliśmy. Dla `ddns.zielona.example` zostaje więc delegacja rekordem NS do własnego serwera z RFC 2136 albo skrypt, który zmienia rekord przez API. W profilach VPN zostaje nazwa `vpn.zielona.example`, a w awarii zmieniamy jej rekord na nazwę z DDNS (rekord CNAME wskazujący `wan2.ddns.zielona.example`). Czy klient IKEv2 zaakceptuje certyfikat bramy przy takim łańcuchu nazw, sprawdzamy w teście, bo certyfikat musi mieć w SAN nazwę z profilu.

Wady tego wariantu to propagacja (przez TTL i czas aktualizacji nazwa wskazuje stary adres), adresy wpisane na stałe w listach partnerów i profilach, brak PTR dla poczty oraz zależność od dostawcy DNS. Zaletą jest to, że nie dokładamy żadnej maszyny. Dla samego tunelu `fw01` do `rtr-mag01` DDNS nie jest potrzebny, bo tunel inicjuje `fw01`, jak opisuje strona IPsec site-to-site.

Wariant b: punkt zaczepienia w chmurze

Maszyna `edge-az01` stoi w sieci wirtualnej chmury i ma stały adres publiczny. `fw01` zestawia z nią dwa tunele IPsec IKEv2, jeden przez `wan1` i jeden przez `wan2`, więc przy awarii światłowodu tunel przez Starlink działa dalej. FortiOS nie ma natywnego WireGuard (opisuje to strona WireGuard i OpenVPN), więc tunele robimy w IPsec, a po stronie chmury obsługuje je strongSwan na Rocky Linux 9, jak reszta Zielonej.

Stały adres w chmurze to w Azure publiczny adres IP w wersji Standard, który ma tylko przydział statyczny (wersja Basic została wycofana 30 września 2025), ale konkretnego numeru nie wybieramy, bo przydziela go Azure [28]. W AWS to Elastic IP, czyli statyczny adres IPv4 przypisany do konta, który można szybko przepiąć na inną maszynę [29]. Maszyna przekazuje cudzy ruch, więc w Azure włączamy na karcie sieciowej opcję Enable IP forwarding [30], a w AWS wyłączamy kontrolę źródła i celu (source/destination check) [31].

Warianty zarządzane usuwają potrzebę łatania maszyny, ale mają swoje ograniczenia, które zestawiamy w tabeli.

Wariant zarządzany	Co to jest	Dla Zielonej
Azure VPN Gateway	usługa tuneli IPsec site-to-site, rozliczana godzinowo za bramę (zależnie od SKU) i za ruch wychodzący [32]	adres bramy lokalnej może być nazwą FQDN [33], więc współpracuje z dynamicznym DNS Starlinka, ale to brama tuneli, a nie punkt wejścia: ruchu z internetu na jej adres nie przekazuje do Zielonej, więc potrzebna jest jeszcze maszyna albo inna usługa

Wariant zarządzany	Co to jest	Dla Zielonej
AWS Site-to-Site VPN	dwa tunele na połączenie, z bramą wirtualną albo Transit Gateway, opłata godzinowa za połączenie i za ruch [36]	adres bramy klienta musi być statyczny, wyjątek to uwierzytelnianie certyfikatem z AWS Private CA [34], więc zmienny adres Starlinka wymaga certyfikatu albo stałego adresu urządzenia NAT
FortiGate-VM w chmurze	ten sam system co `fw01`, polityki i SD-WAN w znanej składni, przewodniki Fortinet dla Azure i AWS [35]	jedna składnia i VIP dla ruchu przychodzącego, ale koszt licencji i większej maszyny, modele licencjonowania sprawdzamy w dokumentacji

Koszt opisujemy tylko jako strukturę, bo ceny zmieniają się i zależą od regionu. Sprawdzamy je w kalkulatorach dostawców przed decyzją.

Składnik kosztu	Azure	AWS
Maszyna i dysk	godzinowo według rozmiaru, osobno dysk	EC2 godzinowo według rozmiaru, osobno EBS
Publiczny adres IPv4	opłata nominalna za adres [28]	opłata za każdy adres, także przypisany do działającej maszyny [29]
Ruch wychodzący z chmury	według cennika transferu z Azure	według cennika transferu z EC2 do internetu [36]
Brama zarządzana (wariant)	opłata godzinowa za SKU bramy [32]	opłata godzinowa za połączenie VPN [36]
Licencja FortiGate-VM (wariant)	do sprawdzenia w ofercie Fortinet	do sprawdzenia w ofercie Fortinet

W awarii poczta, WWW i tunele przechodzą przez jedną małą maszynę. Dlatego w normalnej pracy ruch Zielonej nie idzie przez chmurę, a maszyna służy tylko jako stały punkt wejścia i przekaźnik.

Wariant c: usługi tunelowe bez publicznego IP

W tym wariancie nie ma adresu przychodzącego w ogóle: agent w sieci Zielonej sam łączy się na zewnątrz z usługą, a użytkownicy łączą się z usługą. Cloudflare Tunnel daje połączenie zasobów z Cloudflare bez publicznie routowalnego adresu, a demon `cloudflared` otwiera tylko połączenia wychodzące [42]. Aplikacje webowe publikujemy przez nazwę, a protokoły TCP, SSH, RDP i SMB działają przez WebSocket i wymagają `cloudflared` na komputerze użytkownika [43].

Tailscale łączy urządzenia w sieć opartą na WireGuard bez publicznych adresów, a węzeł z rolą subnet router udostępnia całe podsieci Zielonej, jeśli na Linuksie włączymy przekazywanie pakietów [44]. Tailscale nadaje urządzeniom adresy z zakresu 100.64.0.0/10, czyli tego samego,

który Starlink stosuje w CGNAT [45], więc przy adresie z CGNAT na `wan2` sprawdzamy, czy trasy się nie mylą. Headscale to samodzielnie hostowany serwer sterujący zgodny z Tailscale, ale obsługuje jedną sieć i jest przeznaczony dla małych zespołów [46]. ZTNA na FortiGate opisuje strona SSL VPN i ZTNA.

Wariant c nie zastępuje pozostałych: nie obsłuży poczty od obcych serwerów, bo opublikowane usługi to HTTP i HTTPS oraz wymienione protokoły z agentem po stronie klienta [43], i nie zastępuje VPN dla całej sieci. Zostaje dobrym uzupełnieniem dla administratorów i kilku aplikacji webowych, bo działa bez względu na to, którym łączem i z jakim adresem wychodzi `fw01`.

Poczta: drugi MX albo przekaźnik w chmurze

Jest to kłopot niezależny od wariantu, bo poczta wymaga stałego adresu z PTR i SPF. Mamy dwie drogi dla przychodzącej: drugi MX u dostawcy poczty albo przekaźnik Postfix na `edge-az01`. Postfix jako zapasowy MX przyjmuje wiadomości dla domeny na liście `relay_domains`, sprawdza adresy według `relay_recipient_maps` i przesyła je dalej według `transport_maps` [37].

```
relay_domains = zielona.example
relay_recipient_maps = hash:/etc/postfix/relay_recipients
transport_maps = hash:/etc/postfix/transport
smtpd_relay_restrictions = permit_mynetworks reject_unauth_destination
```

Plik konfiguracyjny: fragment `main.cf` na `edge-az01`. Plik `/etc/postfix/transport` ma jedną linię `zielona.example relay:[10.20.10.42]:25`, a plik `relay_recipients` zawiera listę adresów skrzynek Zielonej (bez niej przekaźnik przyjmie wiadomości do nieistniejących adresów i zapcha kolejkę, o czym ostrzega dokumentacja Postfix [37]). Domeny `zielona.example` nie wpisujemy do `mydestination` ani do `virtual_mailbox_domains` [37]. Po stronie MailCow dopisujemy adres `edge-az01` do białej listy postscreen w pliku `data/conf/postfix/custom_postscreen_whitelist.cidr` [38].

Poczta wychodząca w awarii jest trudniejsza, bo adres Starlinka jest zmienny i nie ma PTR. Azure blokuje domyślnie ruch wychodzący na porcie 25 z maszyn wirtualnych poza subskrypcjami Enterprise Agreement i MCA-E i zaleca uwierzytelniony przekaźnik na porcie 587 [39]. AWS też blokuje port 25, a zniesienie wymaga formularza i może obejmować adres Elastic IP z rekordem odwrotnym [40].

Dlatego w awarii wiadomości z `docker01` kierujemy do uwierzytelnionego przekaźnika na porcie 587 (dostawcę wybiera autor), a SPF obejmuje 203.0.113.10 i ten przekaźnik. PTR dla adresu w Azure ustawiamy właściwością `ReverseFqdn` po utworzeniu rekordu A, z poziomu CLI albo PowerShell [41].

Rekomendacja dla Zielonej

Rekomendujemy wariant b jako docelowy, wariant a jako tani etap pierwszy i zapas dla VPN pracowników, a wariant c jako uzupełnienie dla administratorów. Wariant b wygrywa z czterech powodów.

1. Tunele inicjuje `fw01`, więc zmienny adres Starlinka nie ma znaczenia dla ich zestawienia.
2. Poczta dostaje stały adres z PTR i miejsce na SPF, czego Starlink nie da.
3. Przełączenie poczty i tunelu nie czeka na propagację DNS, bo tunel przez `wan2` już stoi, a MX 20 działa sam.
4. Koszt jest mały i przewidywalny: jedna mała maszyna z jednym adresem zamiast stałego adresu, którego Starlink w ogóle nie oferuje.

Ryzyko to dodatkowa maszyna do łatania (włączamy automatyczne aktualizacje i dodajemy ją do Zabbixa) oraz drugi dostawca w naszej awarii. Awaria `edge-az01` nie zatrzymuje normalnej pracy, bo normalnie ruch idzie przez `wan1`. Wybór między Azure a AWS to decyzja autora: proponujemy Azure, bo Zielona i tak planuje konto Microsoft Entra ID w księdze o Intune, a kroki poniżej mają odpowiedniki AWS.

Wariant b krok po kroku

Poniżej Azure z odpowiednikami AWS, a konfigurację FortiGate i strongSwan traktujemy jako szkic do sprawdzenia w laboratorium, tak jak szkice SD-WAN wyżej. Sieć w chmurze to 10.30.0.0/24, maszyna ma prywatny adres 10.30.0.4, a tunele dostają adresy wewnętrzne 10.255.60.0/30 (tunel 1) i 10.255.60.4/30 (tunel 2). Sprawdziliśmy grep po całej bazie, że te zakresy i adres 203.0.113.60 nie występują nigdzie indziej.

Krok 1, zasoby w Azure. Tworzymy grupę zasobów, sieć, publiczny adres Standard, grupę zabezpieczeń z regułami dla IKE, kartę sieciową z przekazywaniem i maszynę z obrazem Rocky Linux 9 z Marketplace. Reguła dla UDP 500 i 4500 przepuszcza ruch z dowolnego adresu, bo adres Starlinka jest zmienny, więc tunel zabezpieczamy długim kluczem albo certyfikatami.

```
az group create --name NazwaGrupyZasobow --location NazwaRegionu
az network vnet create --resource-group NazwaGrupyZasobow --name vnet-edge \
    --address-prefixes 10.30.0.0/24 --subnet-name snet-edge --subnet-prefixes 10.30.0.0/27
az network public-ip create --resource-group NazwaGrupyZasobow --name pip-edge-az01 \
    --sku Standard --allocation-method Static
az network nsg create --resource-group NazwaGrupyZasobow --name nsg-edge
az network nsg rule create --resource-group NazwaGrupyZasobow --nsg-name nsg-edge \
    --name ike --priority 100 --direction Inbound --access Allow --protocol Udp \
    --destination-port-ranges 500 4500 --source-address-prefixes Internet
az network nsg rule create --resource-group NazwaGrupyZasobow --nsg-name nsg-edge \
```

```
    --name uslugi --priority 110 --direction Inbound --access Allow --protocol '*' \
    --destination-port-ranges 25 443 51820 --source-address-prefixes Internet
az network nic create --resource-group NazwaGrupyZasobow --name nic-edge-az01 \
    --vnet-name vnet-edge --subnet snet-edge --public-ip-address pip-edge-az01 \
    --network-security-group nsg-edge --ip-forwarding true
az vm create --resource-group NazwaGrupyZasobow --name edge-az01 \
    --nics nic-edge-az01 --image NazwaObrazuRocky9 --size NazwaRozmiaru \
    --admin-username nazwa_usera --ssh-key-values KluczPublicznySsh
```

Wersje poleceń i nazwę obrazu sprawdzamy w dokumentacji Azure CLI i w Marketplace. W AWS odpowiednikami są instancja EC2 w sieci VPC, Elastic IP, grupa zabezpieczeń z tymi samymi portami i wyłączona kontrola źródła i celu [29][31].

Krok 2, system na maszynie. Włączamy przekazywanie pakietów w systemie (samo ustawienie w Azure nie wystarcza [30]), instalujemy strongSwan, nftables i Postfix i tworzymy dwa interfejsy XFRM, po jednym na tunel. Interfejsy XFRM obsługuje strongSwan od wersji 5.8.0 i jądro Linuksa od 4.19 [47], więc Rocky Linux 9 je ma, a dostępność pakietu strongswan w EPEL sprawdzamy w naszym obrazie.

```
sudo dnf install -y epel-release
sudo dnf install -y strongswan nftables postfix
echo 'net.ipv4.ip_forward = 1' | sudo tee /etc/sysctl.d/90-edge.conf
sudo sysctl --system
sudo ip link add xfrm1 type xfrm dev eth0 if_id 11
sudo ip link add xfrm2 type xfrm dev eth0 if_id 12
sudo ip addr add 10.255.60.2/30 dev xfrm1
sudo ip addr add 10.255.60.6/30 dev xfrm2
sudo ip link set xfrm1 up
sudo ip link set xfrm2 up
```

Nazwę interfejsu `eth0` sprawdzamy poleceniem `ip -br link`, a tworzenie interfejsów XFRM przy starcie systemu dopisujemy do jednostki systemd po pierwszym udanym teście. Dwa interfejsy XFRM to dwa tunele z osobnymi trasami.

Krok 3, strongSwan. Plik `swanctl.conf` opisuje dwa połączenia z osobnymi tożsamościami `fw01-w1` i `fw01-w2` i selektorami 0.0.0.0/0 po obu stronach, bo kierunek ruchu wyznaczają trasy, a nie selektory. W `strongswan.conf` w sekcji `charon` ustawiamy `install_routes = no`, bo własne trasy dodaje skrypt, a nie strongSwan (ustawienie sprawdzamy w dokumentacji strongSwan [47]).

Pokaż pełny przykład (66 linii)

```
connections {
    fw01-w1 {
        version = 2
        proposals = aes256-sha256-modp2048
        dpd_delay = 10s
        encap = yes
        local_addrs = %any
        remote_addrs = %any
        local {
            auth = psk
            id = edge-az01.zielona.example
        }
        remote {
            auth = psk
            id = fw01-w1.zielona.example
        }
        children {
            w1 {
                local_ts = 0.0.0.0/0
                remote_ts = 0.0.0.0/0
                esp_proposals = aes256-sha256-modp2048
                if_id_in = 11
                if_id_out = 11
                updown = /usr/local/sbin/edge-updown.sh
                start_action = none
            }
        }
    }
    fw01-w2 {
        version = 2
        proposals = aes256-sha256-modp2048
        dpd_delay = 10s
        encap = yes
        local_addrs = %any
        remote_addrs = %any
        local {
            auth = psk
            id = edge-az01.zielona.example
        }
```

```
        remote {
            auth = psk
            id = fw01-w2.zielona.example
        }
        children {
            w2 {
                local_ts = 0.0.0.0/0
                remote_ts = 0.0.0.0/0
                esp_proposals = aes256-sha256-modp2048
                if_id_in = 12
                if_id_out = 12
                updown = /usr/local/sbin/edge-updown.sh
                start_action = none
            }
        }
    }
}
secrets {
    ike-w1 {
        id = fw01-w1.zielona.example
        secret = "HasloPskEdge1"
    }
    ike-w2 {
        id = fw01-w2.zielona.example
        secret = "HasloPskEdge2"
    }
}
```

Plik konfiguracyjny: `/etc/strongswan/swanctl/swanctl.conf` (ścieżkę i nazwę usługi sprawdzamy w pakiecie). Opcja `dpd_delay` włącza aktywne sprawdzanie partnera, które bez ustawienia jest wyłączone [48].

Skrypt `updown` dodaje trasę do sieci Zielonej przez ten tunel, który właśnie powstał, i usuwa ją, gdy tunel padnie. Tunel 1 ma niższą metrykę, więc ruch zwykle idzie nim, a gdy tunel 1 padnie, zostaje trasa przez tunel 2.

```
#!/bin/bash
# /usr/local/sbin/edge-updown.sh
case "$PLUTO_CONNECTION" in
    w1) dev=xfrm1; metric=100 ;;
```

```
    w2) dev=xfrm2; metric=200 ;;
    *) exit 0 ;;
esac
case "$PLUTO_VERB" in
    up-client|up-host) ip route replace 10.20.0.0/16 dev "$dev" metric "$metric" ;;
    down-client|down-host) ip route del 10.20.0.0/16 dev "$dev" metric "$metric" ;;
esac
```

Zmienne `PLUTO_CONNECTION` i `PLUTO_VERB` skrypt dostaje od strongSwan [48], a ich zawartość sprawdzamy w logu przy pierwszym teście. Skrypt robimy wykonywalnym (`chmod +x`), a usługę uruchamiamy i ładujemy konfigurację poleceniem `sudo swanctl --load-all`.

Krok 4, przekierowania. Reguły nftables przekierowują wybrane porty z adresu publicznego na serwery Zielonej i podmieniają adres źródłowy na 10.30.0.4, żeby odpowiedzi wróciły do maszyny. Zapora w chmurze, czyli grupa zabezpieczeń, przepuszcza tylko porty z kroku 1, a reguły `forward` z domyślnym `drop` przepuszczają ruch przekierowany i odpowiedzi.

```
table ip edge {
    chain prerouting {
        type nat hook prerouting priority dstnat; policy accept;
        iifname "eth0" tcp dport 443 dnat to 10.20.10.42:443
        iifname "eth0" udp dport 51820 dnat to 10.20.10.95:51820
    }
    chain forward {
        type filter hook forward priority filter; policy drop;
        ct state established,related accept
        ct status dnat accept
    }
    chain postrouting {
        type nat hook postrouting priority srcnat; policy accept;
        oifname "xfrm*" snat to 10.30.0.4
    }
}
```

Plik konfiguracyjny: `/etc/nftables/edge.nft` wczytywany przez usługę `nftables`. Przekierowanie portu 443 na `docker01` ma tę wadę, że w logach serwera widać adres 10.30.0.4 zamiast adresu klienta, więc gdy adres klienta jest potrzebny, zamiast przekierowania stawiamy na maszynie przekaźnik HTTP przekazujący adres w nagłówku. Port 51820 prowadzi do `wg01`, jak na stronie o WireGuard, a pocztę obsługuje Postfix z poprzedniej sekcji, nie przekierowanie.

Krok 5, `fw01`. Dwie fazy 1 z różnymi tożsamościami (`localid`) i interfejsami `wan1` i `wan2`, selektory 0.0.0.0/0, adresy wewnętrzne tunelu, strefa SD-WAN z oboma tunelami, trasa do sieci w chmurze i

polityki dla ruchu z chmury do serwerów. Adres zdalny to `203.0.113.60`, a po zmianie na prawdziwy adres z Azure poprawiamy go w obu tunelach.

Pokaż pełny przykład (64 linii)

```
config vpn ipsec phase1-interface
    edit "edge_w1"
        set interface "wan1"
        set ike-version 2
        set peertype any
        set proposal aes256-sha256
        set dhgrp 14
        set remote-gw 203.0.113.60
        set localid "fw01-w1.zielona.example"
        set psksecret HasloPskEdge1
        set keylife 28800
        set dpd on-idle
        set dpd-retrycount 3
        set dpd-retryinterval 5
        set comments "edge-az01, tunel przez wan1"
    next
    edit "edge_w2"
        set interface "wan2"
        set ike-version 2
        set peertype any
        set proposal aes256-sha256
        set dhgrp 14
        set remote-gw 203.0.113.60
        set localid "fw01-w2.zielona.example"
        set psksecret HasloPskEdge2
        set keylife 28800
        set dpd on-idle
        set dpd-retrycount 3
        set dpd-retryinterval 5
        set comments "edge-az01, tunel przez wan2"
    next
end
config vpn ipsec phase2-interface
    edit "edge_w1_p2"
```

```
        set phase1name "edge_w1"
        set proposal aes256-sha256
        set pfs enable
        set dhgrp 14
        set auto-negotiate enable
        set keylifeseconds 3600
        set src-subnet 0.0.0.0 0.0.0.0
        set dst-subnet 0.0.0.0 0.0.0.0
    next
    edit "edge_w2_p2"
        set phase1name "edge_w2"
        set proposal aes256-sha256
        set pfs enable
        set dhgrp 14
        set auto-negotiate enable
        set keylifeseconds 3600
        set src-subnet 0.0.0.0 0.0.0.0
        set dst-subnet 0.0.0.0 0.0.0.0
    next
end
config system interface
    edit "edge_w1"
        set ip 10.255.60.1 255.255.255.255
        set remote-ip 10.255.60.2 255.255.255.255
    next
    edit "edge_w2"
        set ip 10.255.60.5 255.255.255.255
        set remote-ip 10.255.60.6 255.255.255.255
    next
end
```

Adresy wewnętrzne tuneli są potrzebne, bo bez nich tunel nie działa jako członek SD-WAN z bramą [50]. Teraz SD-WAN: oba tunele jako członkowie jednej strefy, sonda do adresu maszyny w chmurze i reguła, która wybiera tunel przez `wan1`, a przy awarii przez `wan2`. Składnię sekcji `service` i trasy do strefy (w FortiOS 7.x opcja `sdwan-zone`) sprawdzamy w dokumentacji naszej wersji, a przykład z tunelami jako członkami opisuje Fortinet [49].

Pokaż pełny przykład (39 linii)

```
config firewall address
    edit "EDGE_VNET"
        set subnet 10.30.0.0 255.255.255.0
    next
    edit "EDGE_AZ01"
        set subnet 10.30.0.4 255.255.255.255
    next
end
config system sdwan
    config zone
        edit "EDGE_OVERLAY"
        next
    end
    config members
        edit 21
            set interface "edge_w1"
            set zone "EDGE_OVERLAY"
        next
        edit 22
            set interface "edge_w2"
            set zone "EDGE_OVERLAY"
        next
    end
    config health-check
        edit "SondaEdge"
            set server "10.30.0.4"
            set members 21 22
        next
    end
    config service
        edit 21
            set name "DoEdge"
            set mode priority
            set dst "EDGE_VNET"
            set priority-members 21 22
            set health-check "SondaEdge"
        next
    end
end
```

Polityka dla ruchu z chmury ma jako źródło tylko `EDGE_AZ01` (po przekierowaniu to jest jedyny adres, który widzą serwery) i dopuszcza tylko usługi, które przekierowujemy: SMTP i HTTPS do `docker01` oraz UDP 51820 do `wg01`. Politykę piszemy na wzór polityk ze strony o IPsec site-to-site, z `nat disable` i strefą `EDGE_OVERLAY` jako interfejsem źródłowym. Dokładne obiekty usług i adresów serwerów ustalamy według istniejących obiektów na `fw01`.

Krok 6, DNS i odwrotny rekord. Tworzymy rekord A `poczta2.zielona.example` z TTL 300 na adres z Azure, dopisujemy `MX 20` i dopiero potem ustawiamy `ReverseFqdn`, bo Azure wymaga, żeby rekord A już istniał [41]. Gdy domena ma politykę MTA-STS (MTA-STS i TLS-RPT: szyfrowanie poczty między serwerami, a BIMI informacyjnie), `poczta2` stoi na jej liście MX, więc Postfix na `edge-az01` musi ogłaszać STARTTLS i mieć certyfikat od publicznego urzędu wystawiony na nazwę `poczta2.zielona.example`. Bez tego nadawcy w trybie `enforce` przytrzymają pocztę w kolejkach właśnie w czasie awarii `wan1`.

```
az network public-ip update --resource-group NazwaGrupyZasobow --name pip-edge-az01 \
    --reverse-fqdn poczta2.zielona.example.
```

W awarii `wan1` rekord `vpn.zielona.example` zmieniamy na adres `edge-az01` w wariancie testowym albo na nazwę z DDNS (wariant a). Wariant testowy dla VPN pracowników działa tak: `fw01` słucha IKE na adresie interfejsu typu loopback, a `edge-az01` przekierowuje UDP 500 i 4500 na ten adres przez tunel. Czy FortiOS pozwoli związać tunel dial-up z loopbackiem w naszej wersji, jak zachowa się NAT-T przy przekierowaniu docelowym i którędy wrócą odpowiedzi, sprawdzamy w laboratorium, bo tego nie potwierdziliśmy w dokumentacji. Dopóki test nie przejdzie, dla VPN pracowników w awarii zostaje wariant a.

Krok 7, test przełączenia opisujemy w następnej sekcji i rozszerzamy go o tunele do chmury.

Test przełączenia

Test planujemy poza zamrożeniem zmian od 15 listopada do 6 stycznia, poza zamknięciem miesiąca i nie o 6:00, gdy czterdzieści skanerów loguje się do WMS. Dobę wcześniej obniżamy TTL rekordów `vpn` i MX do 300 sekund, a przed próbą zapisujemy wynik `mtr`, `diagnose sys sdwan member` i `curl`.

1. Odłączamy kabel `wan1` i mierzymy czas, po którym `curl` z komputera pokazuje adres `wan2` (przykładowo 203.0.113.30, w próbie odczytujemy prawdziwy).
2. Sprawdzamy `diagnose sys sdwan member`: `wan1` ma być oznaczony jako niedostępny, a `wan2` jako aktywny.
3. Sprawdzamy tunele do chmury: `diagnose vpn tunnel list name edge_w2` na `fw01` oraz `sudo swanctl --list-sas` i `ip route show 10.20.0.0/16` na `edge-az01`, gdzie trasa ma iść przez `xfrm2`.
4. Zmieniamy rekord `vpn.zielona.example` na adres `wan2` albo nazwę z DDNS (wariant a), a w wariancie testowym na adres `edge-az01`, i mierzymy czas do połączenia VPN z sieci zewnętrznej, na przykład z hotspotu telefonu.

5. Z zewnętrznej skrzynki wysyłamy wiadomość do Zielonej i sprawdzamy, że dociera przez `poczta2`, a w nagłówkach `Received` widzimy `edge-az01`, a nie adres Starlinka.
6. Wysyłamy wiadomość z `docker01` na zewnętrzną skrzynkę przez przekaźnik uwierzytelniony i sprawdzamy w nagłówkach wynik SPF i PTR.
7. Zmieniamy adres `wan2`, restartując zestaw Starlink (po uzgodnieniu okna), i sprawdzamy, że tunel `edge_w2` wraca sam, a nazwa DDNS wskazuje nowy adres.
8. Wpinamy kabel `wan1`, przywracamy rekord `vpn` i sprawdzamy powrót ruchu na `wan1` oraz wpis w dokumentacji.

Co mierzymy	Jak	Wynik
Ruch wychodzący	czas do zmiany adresu w `curl`	do uzupełnienia po próbie
Powrót na `wan1`	czas po wpięciu kabla	do uzupełnienia po próbie
Tunel do chmury po awarii `wan1`	czas do trasy przez `xfrm2`	do uzupełnienia po próbie
VPN	czas od zmiany rekordu do połączenia	do uzupełnienia po próbie
Poczta przychodząca	czas dostarczenia przez MX 20 i `edge-az01`	do uzupełnienia po próbie
Poczta wychodząca	wynik SPF i PTR w nagłówku	do uzupełnienia po próbie
Zmiana adresu `wan2`	czas do odtworzenia tunelu i aktualizacji DDNS	do uzupełnienia po próbie

Parametry sondy (interwał, liczbę nieudanych prób do uznania łącza za martwe i czas powrotu) ustawiamy tak, żeby przełączenie następowało w sekundach, a nie minutach, i sprawdzamy w dokumentacji naszej wersji FortiOS.

Ograniczenia Starlinka w roli łącza zapasowego

- Pogoda i przeszkody: antena traci łączność, gdy coś zasłoni niebo, a opady i śnieg na antenie mogą ją pogorszyć. Zakres temperatur pracy anteny to według dokumentacji od -30 do 50 stopni [8], a wpływ deszczu i śniegu na szybkość sprawdzamy w dokumentacji zestawu.
- Opóźnienie: około 25 do 50 ms zamiast kilku milisekund światłowodu [7][16], co czuć w rozmowach i pracy zdalnej na pulpicie.
- Szybkość wysyłania: według opisu planów 20 do 44 Mb/s [7], więc kopie zapasowe i duże przesyłki w awarii trwają dłużej.
- Limity danych: plany Priority mają bloki danych priorytetowych [6], a co dzieje się po ich wyczerpaniu w Polsce, pytamy Starlinka.
- Adres publiczny: dynamiczny, bo Starlink nie oferuje stałego adresu w żadnym planie [17][18], więc numeru nie wpisujemy na stałe w DNS, profilach VPN ani listach dozwolonych adresów, tylko stosujemy jeden z trzech sposobów z sekcji wyżej.

- Wspólne punkty awarii: pojedyncza zapora `fw01`, wspólne zasilanie budynku i ta sama szafa R1.

Wiemy też o jednej luce: łącze między biurem w Pamiątkowie a magazynem w Swarzędzu nie jest opisane w bazie. Nie wiemy, czy to własny światłowód, VPN między zaporami czy łącze dzierżawione, więc nie rozstrzygamy, czy łącze zapasowe obejmuje także tę drogę.

Co sprawdzamy u operatora

Pytania do operatora łącza naziemnego przed podpisaniem umowy:

- Jaka jest dostępność gwarantowana w procentach w skali roku i jak ją liczymy?
- Jaki jest czas reakcji i maksymalny czas naprawy, w jakich godzinach i czy w święta?
- Jakie kary i rekompensaty przewiduje umowa za niedotrzymanie SLA?
- Czy łącze jest symetryczne, czy szybkość jest gwarantowana (CIR), czy tylko „do”?
- Ile adresów publicznych dostajemy i czy są stałe, czy łącze nie jest za CGNAT?
- Czy dostajemy IPv6 i jaki prefiks?
- Czy operator filtruje ruch (na przykład port 25 poczty) i czy ustawi odwrotny rekord DNS dla naszego adresu?
- Jakie jest zakończenie: rodzaj włókna (OS2), złącze (SC/APC lub LC), szybkość portu i czy urządzenie operatora (ONT) pracuje w trybie mostu (bridge)?
- Czy łącze wymaga znakowania VLAN albo PPPoE, i jaki MTU ustawiamy na `fw01`?
- Którędy biegnie trasa: czy drugie łącze od innego operatora ma całkowicie inną drogę, wejście do budynku i kanał kablowy?
- Jak i z jakim wyprzedzeniem operator zawiadamia o pracach planowych?
- Jaki jest okres umowy, koszt zerwania i możliwość zwiększenia szybkości?
- Czy oferuje ochronę przed atakami DDoS i na jakich warunkach?

Pytania do Starlinka (łącze zapasowe na `wan2`):

- Czy w Polsce plan biznesowy (Priorytetowe Lokalne) ma opcję publicznego adresu IPv4, od którego planu i na jakich warunkach? Nie potwierdziliśmy tego na oficjalnej stronie, bo jej treść ładuje się skryptem.
- Opisy mówią, że adres jest dynamiczny i że stałego adresu nie ma w żadnym planie [17][18]: jak długo trzyma się po restarcie zestawu, kiedy może się zmienić i czy jest płatna usługa stałego adresu albo bloku adresów?
- Gdzie włączamy opcję (konto, aplikacja) i czy działa w trybie bypass na naszym zestawie?
- Czy porty przychodzące (UDP 500 i 4500 dla IKEv2, TCP 25, 443, 587 i 993 dla poczty) są otwarte i czy port 25 wychodzący nie jest blokowany?
- Czy da się ustawić odwrotny rekord DNS (PTR) dla naszego adresu?
- Czy dostajemy IPv6, jaki prefiks i czy działa w trybie bypass?
- Co obejmuje umowna dostępność 99,9 procent, czy dotyczy Polski i naszego zestawu oraz jaki jest czas reakcji wsparcia, czy po polsku?

- Jaki blok danych priorytetowych potrzebujemy na awarię i co dzieje się po jego wyczerpaniu?
- Jaki zestaw (Standard czy High Performance), jaka długość kabla w komplecie, jakie uchwyty i jaka gwarancja?
- Jaki jest okres rozliczenia i czy plan można zmienić bez kary?

Mity i sprostowania

Obiegowa wersja	Jak jest naprawdę
Dwa łącza to dwie niezależne drogi	Dwa łącza w jednym kanale z jednym wejściem do budynku może przeciąć ta sama koparka
99,9 procent dostępności to prawie bez przestojów	To około 8,76 godziny przestoju w roku, w jednej awarii
Starlink zastąpi światłowód także dla VPN	Tylko z publicznym adresem IPv4, a w planach domowych jest CGNAT i połączenia przychodzące nie docierają
Starlink z publicznym adresem ma adres stały	Starlink nie oferuje stałego adresu w żadnym planie, w planie biznesowym adres jest publiczny, ale dynamiczny i może się zmienić [10][17][18]
Satelity oznaczają ogromne opóźnienia	Satelity na niskiej orbicie dają około 25 do 50 ms, a minimum dla satelity stacjonarnego to 477 ms [5][16]
LTE zastąpi światłowód także dla VPN	Przy CGNAT połączenia przychodzące nie docierają
Druga nazwa VPN w profilu Windows zrobi przełączanie	Klient używa tylko wybranego serwera i nie próbuje kolejnych sam [12]
SD-WAN jest tylko dla dużych firm	Dwa łącza i sonda działają w FortiGate także w małej sieci
Szybkość z umowy to szybkość stała	Szybkość „do” nie jest gwarancją

Oś czasu

Data	Wydarzenie
2003	ITU-T G.984: GPON
grudzień 2009	pierwsze komercyjne sieci LTE
24 maja 2019	start pierwszych 60 satelitów Starlink [13]
10 lutego 2021	przedsprzedaż Starlinka w Polsce [14]
czerwiec 2026	około 10,4 tysiąca satelitów Starlink na orbicie [5]

Wątek polski

Dostęp do pasm radiowych i pozwolenia radiowe w Polsce nadzoruje Urząd Komunikacji Elektronicznej, a konkretnych przepisów o radioliniach nie potwierdziliśmy w dostępnych źródłach, więc ich nie cytujemy. Nazwę Starlink podajemy, bo to wybór Zielonej na łącze zapasowe, a operatorów łączy naziemnych nie wymieniamy, bo umowy porównujemy z listą pytań, a nie z marką. Sprzedaż Starlinka w Polsce ruszyła przedsprzedażą 10 lutego 2021 roku [14], a ofertę planów biznesowych opisują dziś polskie serwisy po polsku [7]. Czy publiczny adres IPv4 jest w Polsce dostępny na planie biznesowym, potwierdzamy u Starlinka.

Częste błędy

Objaw	Przyczyna	Co robimy
Po przełączeniu poczta i VPN nie działają	rekord DNS nadal wskazuje 203.0.113.10 albo `wan2` ma adres z CGNAT	zmieniamy rekord `vpn`, sprawdzamy MX 20 i adres `wan2`
`wan2` dostaje adres z 100.64.0.0/10 zamiast publicznego	opcja publicznego adresu wyłączona albo niedostępna na planie	sprawdzamy konto Starlink i pytamy Starlinka
`wan2` nie dostaje adresu	router Starlink nie jest w trybie bypass albo kabel w złym porcie	sprawdzamy fioletową diodę i port, resetujemy ustawienia zestawu
Po włączeniu bypass znika Wi-Fi Starlinka	to skutek trybu bypass [9]	zarządzamy zestawem przez aplikację i `fw01`
Antena często traci łączność	przeszkoda w polu widzenia albo śnieg na antenie	sprawdzamy narzędzie przeszkód w aplikacji i miejsce montażu
Tunel VPN nie wstaje na `wan2`	tunel zdefiniowany tylko na `wan1` albo odpowiedź wychodzi złym łączem	druga definicja tunelu, sprawdzenie tras odpowiedzi
Przełączenie następuje po wielu minutach	sonda ma długie interwały i duży próg niepowodzeń	skracamy interwał i próg, sprawdzamy w dokumentacji
Ruch nie wraca na `wan1` po naprawie	zbyt ostrożny czas powrotu lub reguła z ręcznym wyborem	sprawdzamy czas powrotu i regułę
Brak łączności mimo działającego łącza	interfejs nadal użyty w trasie lub polityce poza SD-WAN	przenosimy trasę i politykę na strefę SD-WAN
Dwa łącza padają razem	wspólna trasa kabla	wybieramy drugie łącze o innej drodze i innym medium
VPN albo poczta przez `wan2` przestały działać po restarcie anteny	adres `wan2` się zmienił, a rekord DNS albo konfiguracja wskazuje stary numer	odczytujemy adres `get system interface physical`, sprawdzamy aktualizację DDNS albo przechodzimy na punkt zaczepienia w chmurze

Objaw	Przyczyna	Co robimy
Tunel do `edge-az01` stoi, ale ruch do Zielonej nie wraca	trasa na `edge-az01` wskazuje tunel, który padł, albo skrypt `updown` nie dodał trasy	sprawdzamy `ip route show 10.20.0.0/16` i log skryptu, dopisujemy trasę ręcznie i poprawiamy zmienne w skrypcie
Poczta z `edge-az01` do `docker01` jest odrzucana przez postscreen	adres maszyny nie jest na białej liście MailCow	dopisujemy adres do `custom_postscreen_whitelist.cidr` [38]
Kolejka na `edge-az01` rośnie od odrzuconych wiadomości	brak listy `relay_recipient_maps`, przekaźnik przyjmuje pocztę do nieistniejących adresów	uzupełniamy listę adresów Zielonej [37]

□□ Ćwiczenia

1. Ile godzin przestoju w roku dopuszcza SLA 99,9 procent?

Odpowiedź

Rok ma 8760 godzin, więc 0,1 procent to 8,76 godziny, czyli około 8 godzin i 46 minut.

1. Dlaczego VPN `vpn.zielona.example` nie działa po przełączeniu na Starlink, mimo że wychodzący ruch idzie?

Odpowiedź

Rekord DNS nadal wskazuje adres 203.0.113.10, który należy do łącza `wan1`. Po awarii zmieniamy rekord na aktualny adres `wan2` (przykładowo 203.0.113.30, bo prawdziwy jest zmienny), a jeśli `wan2` ma adres z CGNAT zamiast publicznego, połączenia przychodzące i tak nie dotrą.

1. Po co przed próbą obniżamy TTL rekordów do 300 sekund i dlaczego poczta nie potrzebuje takiej zmiany?

Odpowiedź

Inne serwery pamiętają starą odpowiedź przez TTL, więc po zmianie rekordu `vpn` użytkownicy trafiliby na stary adres przez cały stary TTL. Poczta ma stale dwa rekordy MX (10 i 20), a nadawca sam próbuje drugi, gdy pierwszy nie odpowiada.

1. Co zmienia się w wyniku `mtr` po przełączeniu na łącze zapasowe?

Odpowiedź

Zmienia się brama operatora na drugim przeskoku i zwykle rośnie opóźnienie. Zapisujemy wynik przed próbą, żeby je porównać.

1. Dlaczego dynamiczny DNS nie rozwiązuje kłopotu z pocztą przychodzącą i wychodzącą przez Starlink?

Odpowiedź

DDNS aktualizuje tylko rekord adresu, więc nazwa wskazuje aktualny adres, ale adres ze Starlinka nie ma rekordu PTR ustawionego przez nas, a część serwerów odrzuca pocztę z adresów bez PTR i dopuszcza w SPF tylko adresy stałe. Stały adres z PTR daje dopiero punkt zaczepienia w chmurze albo przekaźnik u dostawcy.

1. Dlaczego zmiana adresu Starlinka nie zrywa na stałe tuneli do `edge-az01`?

Odpowiedź

Bo tunele inicjuje `fw01`, a `edge-az01` ma stały adres, więc `fw01` zawsze wie, dokąd dzwonić, a strongSwan rozpoznaje `fw01` po identyfikatorze (`localid`), nie po adresie. Po zmianie adresu `wan2` tunel `edge_w2` odtwarza się sam po wykryciu przez DPD, że partner zniknął.

Powiązane: Przełączniki: L2 i L3, tablica MAC, VLAN, LACP i STP, Wkładki SFP i kable DAC: rodziny, zgodność i pomiar mocy optycznej, UPS: topologie, dobór i baterie, MailCow: instalacja w Dockerze, VPN: tunel przez cudzy internet, EAP-TLS i FSSO: logowanie do VPN certyfikatem użytkownika i grupami z AD, Światłowody: rodzaje, złącza, budżet tłumienia i bezpieczeństwo, IPsec site-to-site: Pamiątkowo i Swarzędz między FortiGate a routerem innej firmy, IPsec dla pracowników: FortiClient i dial-up IKEv2 na FortiGate, WireGuard i OpenVPN: odpowiedniki spoza FortiGate na Linuksie, SSL VPN i ZTNA: co z SSL VPN w nowych FortiOS i czym go zastąpić, FortiGate w zarządzaniu siecią: interfejsy, VLAN-y, polityki i NAT

Źródła:

1. Fortinet Community, „Configure and diagnostic commands to check the status of the SD-WAN link”: community.fortinet.com
2. Wikipedia, „LTE (telecommunication)”: en.wikipedia.org/wiki/LTE_(telecommunication))
3. Wikipedia, „Gigabit-capable passive optical network”: en.wikipedia.org/wiki/Gigabit-capable_passive_optical_network

4. IETF, „RFC 6598: IANA-Reserved IPv4 Prefix for Shared Address Space”: rfc-editor.org/rfc/rfc6598
5. Wikipedia, „Starlink”: en.wikipedia.org/wiki/Starlink
6. Starlink, „Priority Plan Transition” (plany Local Priority i Global Priority, umowna dostępność 99,9 procent): starlink.com
7. NANO Komputronik, „Internet Starlink w Polsce: cena, prędkość, rodzaje pakietów i limity danych” (artykuł z 16.09.2026, aktualizacja 30.09.2026): nano.komputronik.pl
8. Starlink, dokumentacja zestawu Standard (pole widzenia, pobór mocy, kabel, stopnie ochrony), w kopii sprzedawcy: obelink.be
9. Satellite Phone Store, „What is bypass mode?” (opis sprzedawcy, nie dokumentacja producenta): support.satellitephonestore.com
10. DishyTech, „Can You Get A Static IP From Starlink?” (opis niezależny, aktualizacja sierpień 2025): dishytech.com
11. TrustMyIP, „Starlink static IP and CGNAT bypass guide” (opis niezależny, grudzień 2025): trustmyip.com
12. Microsoft Learn, „VPNv2 profile XSD” (element Servers): learn.microsoft.com
13. iMagazine, „Pierwsze satelity Starlink już na orbicie”: imagazine.pl
14. Antyweb, „Starlink można już zamawiać na adres w Polsce”: antyweb.pl
15. Starlink Help Center, „How do I set my IP address to a public IP?” (znamy tytuł, treść wymaga JavaScriptu i nie została odczytana): starlink.com
16. Business.org, „Starlink Business Internet Review 2026” (opóźnienie 25 do 50 ms): business.org
17. Starlink Insider, „Starlink Static IP: How To Get It & Viable Alternatives (2026)” (cytuje artykuł Llama Networks „Starlink IP Addressing”, do którego strony nie udało się otworzyć; brak stałych adresów, dynamiczny publiczny adres w planach Business i Maritime, CGNAT w planach domowych, prefiks IPv6 /56): starlinkinsider.com
18. Stallion Information Systems, „Understanding Starlink Public IP Addresses” (opracowanie sprzedawcy z stycznia 2026 według dokumentacji Starlink; opcja dla planów Priority, Mobile Priority i Maritime, adres dynamiczny, wiązanie adresu na 24 godziny, prefiks /56): stallionis.com
19. Metro Wireless, „Starlink persistent IP vs true public static IP” (adres „lepki”, nie stały): metrowireless.com
20. TrustMyIP, „Starlink Public IP Changed? 5 Fixes” (kiedy adres się zmienia, rola DDNS): trustmyip.com
21. CellStream, „Does Starlink Support IPv6?” (prefiks /56 przez DHCPv6-PD, blokada ruchu przychodzącego w routerze Starlink): cellstream.com
22. OpenWrt Forum, „IPv6 Firewall Rule for /64 Assigned Starlink Address” (wątek użytkowników, prefiks /64): forum.openwrt.org
23. Northants Chamber, „Starlink’s IP Limitation and Why it Matters” (artykuł prasowy: klienci biznesowi zwykle też z CGNAT): northants-chamber.co.uk

24. Fortinet Community, „Technical Tip: How to configure Dynamic DNS for FortiGate” (FortiGuard DDNS, domeny fortiddns.com, fortidyndns.com i float-zone.com): community.fortinet.com
25. Fortinet Community, „Technical Tip: How to configure a third party DDNS service” (lista dostawców, genericDDNS według RFC 2136, `use-public-ip` tylko dla FortiGuardDDNS i noip.com): community.fortinet.com
26. DynIP, „FortiGate” (przykład genericDDNS z kluczem TSIG, algorytm HMAC-MD5 stały): dynip.dev
27. Fortinet Community, „Technical Tip: Configuring the external IP address of a virtual server with DHCP addressing mode” (VIP z adresem 0.0.0.0): community.fortinet.com
28. Microsoft Learn, „Public IP addresses” (Standard SKU tylko statyczny, wycofanie Basic 30 września 2025, adresu nie wybieramy): learn.microsoft.com
29. AWS, „Elastic IP addresses” (statyczny adres IPv4, opłata za adresy, przepinanie): docs.aws.amazon.com
30. Microsoft Learn, „Virtual network traffic routing” (typ następnego skoku Virtual appliance, Enable IP forwarding): learn.microsoft.com
31. AWS, „Work with NAT instances” (wyłączenie kontroli źródła i celu): docs.aws.amazon.com
32. Microsoft Learn, „What is Azure VPN Gateway?” (rodzaje połączeń, rozliczenie: godzina bramy i ruch wychodzący, SKU strefowo-nadmiarowe): learn.microsoft.com
33. Microsoft Learn, „About VPN Gateway configuration settings” (brama lokalna z adresem IP albo FQDN, tryby połączenia): learn.microsoft.com
34. AWS, „Customer gateway options for your Site-to-Site VPN connection” (adres statyczny, wyjątek dla certyfikatu z AWS Private CA): docs.aws.amazon.com
35. Fortinet Document Library, „Azure Administration Guide” i „AWS Administration Guide” dla FortiGate public cloud (strony ładują się skryptem, potwierdziliśmy istnienie przewodników i tytuły rozdziałów, a modele licencjonowania zostają do sprawdzenia): docs.fortinet.com, docs.fortinet.com
36. AWS, „What is AWS Site-to-Site VPN?” (dwa tunele, bramy, rozliczenie godzinowe i transfer): docs.aws.amazon.com
37. Postfix, „Postfix Standard Configuration Examples” (zapasowy MX: `relay_domains`, `relay_recipient_maps`, `transport_maps`): postfix.org
38. MailCow, „Whitelist IP in Postscreen”: docs.mailcow.email
39. Microsoft Learn, „Troubleshoot outbound SMTP connectivity issues in Azure” (port 25 blokowany poza Enterprise Agreement i MCA-E, przekaźnik na 587): learn.microsoft.com
40. AWS re:Post, „Remove port 25 restrictions for instances and functions”: repost.aws
41. Microsoft Learn, „Configure reverse DNS for services hosted in Azure” (właściwość ReverseFqdn, wymóg istniejącego rekordu A): learn.microsoft.com
42. Cloudflare, „Cloudflare Tunnel” (połączenia wychodzące z `cloudflared`, bez publicznie routowalnego adresu): developers.cloudflare.com

43. Cloudflare, „Protocols for published applications” (HTTP i HTTPS, TCP, SSH, RDP i SMB z `cloudflared` po stronie klienta): developers.cloudflare.com
44. Tailscale, „Subnet routers”: tailscale.com
45. Tailscale, „What are these 100.x.y.z addresses?”: tailscale.com
46. GitHub, „juanfont/headscale”: github.com
47. strongSwan, „Route-Based VPN” (interfejsy XFRM od wersji 5.8.0, `if_id_in` i `if_id_out`): docs.strongswan.org
48. strongSwan, „swanctl.conf” (opcje `updown`, `dpd_delay`, `start_action`): docs.strongswan.org
49. Fortinet Community, „Technical Tip: Configure FortiGate SD-WAN with an IPsec VPN” (tunele jako członkowie SD-WAN, sondy, reguły): community.fortinet.com
50. Fortinet Community, „Technical Tip: SD-WAN with DDNS type IPsec” (adresy wewnętrzne tunelu potrzebne do pracy jako członek SD-WAN): community.fortinet.com
51. Fortinet Community, „Technical Tip: Creating a second DDNS” (drugi wpis z własnym `monitor-interface`): community.fortinet.com

---

Revision #12
Created 2026-10-03 17:41:18 UTC by Tomasz Konieczny
Updated 2026-10-26 14:23:37 UTC by Tomasz Konieczny