Tunel do Azure bez VPN Gateway: edge-az01 z strongSwan albo FortiGate-VM fw-az01

Poziom: zaawansowany

Dotyczy: edge-az01 (Rocky Linux 9, strongSwan, nftables), FortiGate-VM w Azure (fw-az01, licencja BYOL albo PAYG), fw01 (FortiGate 100F, FortiOS 7.4/7.6), rtr-mag01 (MikroTik RouterOS 7), Azure VPN Gateway (porównanie), Azure CLI

Czas: ~60 min

Sieć DR w Azure musi być połączona z Pamiątkowem i Swarzędzem tunelem IPsec. Zarządzana brama Azure VPN Gateway robi to wygodnie, ale kosztuje co godzinę i nie przyjmie poczty ani ruchu z internetu, więc Zielona ma dwie tańsze drogi: rozbudowę istniejącego `edge-az01` albo osobną zaporę FortiGate-VM `fw-az01`. Ta strona pokazuje obie, porównuje koszty i odpowiedzialność oraz opisuje tunel ze Swarzędza, który musi działać, gdy `fw01` zniknie razem z serwerownią.

ZAŁOŻENIA SCENARIUSZA

w tym ćwiczeniu `edge-az01` istnieje i działa tak, jak opisuje strona Łącza operatora: światłowód, radiolinia, LTE i 5G oraz przełączanie na FortiGate: sieć `vnet-edge` 10.30.0.0/24, adres 10.30.0.4, publiczny 203.0.113.60, tunele `edge_w1` i `edge_w2` do `fw01` (10.255.60.0/30 i 10.255.60.4/30). `fw-az01` to wariant obok, nie zamiast: podsieci 10.30.0.32/27 i 10.30.0.64/27 w tej samej sieci, interfejsy 10.30.0.36 i 10.30.0.68, publiczny 203.0.113.61, tunele do `fw01` w 10.255.61.0/30 i 10.255.61.4/30 (sprawdziliśmy grep po całej bazie, że te adresy i nazwa `fw-az01` nie występują nigdzie indziej). Swarzędz jest osobną lokalizacją z `rtr-mag01` (203.0.113.40), a sieć DR to 10.31.0.0/16 ze strony Azure jako zapasowa serwerownia Zielonej: architektura, co replikujemy, a co odtwarzamy.

Skróty użyte na tej stronie (25)

Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie
API	Application Programming Interface: sposób, w jaki programy rozmawiają ze sobą
BYOL	Bring Your Own License: przeniesienie własnej licencji na oprogramowanie do chmury zamiast licencji wliczonej w cenę
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
DR	Disaster Recovery: plan przywrócenia działania po poważnej awarii
EPEL	Extra Packages for Enterprise Linux: dodatkowe repozytorium pakietów dla RHEL i klonów
HA	High Availability: wysoka dostępność, czyli działanie mimo awarii jednego elementu
IPsec	Internet Protocol Security: zestaw protokołów szyfrujących i uwierzytelniających ruch sieciowy, na nim stoi tunel VPN typu IKEv2
LDAP	Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA)
MX	Mail Exchanger: rekord DNS wskazujący serwer poczty domeny
NAT	Network Address Translation: podmiana adresów IP na granicy sieci
PAYG	Pay-As-You-Go: płatność za zużycie bez zobowiązań, według cennika; w Azure model zakupu subskrypcji, w Marketplace także licencja wliczona w cenę godziny maszyny
RPC	Remote Procedure Call: sposób, w jaki programy wywołują funkcje na innym komputerze w sieci; kontrolery domeny używają go między innymi do replikacji
RTO	Recovery Time Objective: jak długo wolno nie działać przy awarii
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
SDN	Software-Defined Networking: sieć sterowana programowo przez API; w FortiGate łącznik SDN pozwala zaporze zmieniać adresy i trasy w chmurze, na przykład przy przełączeniu pary w Azure
SKU	Stock Keeping Unit: oznaczenie pozycji handlowej, na przykład konkretnej licencji lub modelu
SMB	Server Message Block: protokół udostępniania plików i drukarek w sieci Windows, na nim stoi zwykły udział sieciowy
SSD	Solid State Drive: dysk półprzewodnikowy
UDR	User-Defined Route: trasa definiowana przez użytkownika w tabeli tras Azure, która zmienia domyślną drogę ruchu z podsieci, na przykład przez zaporę
VDOM	Virtual Domain: domena wirtualna w FortiOS, czyli podział jednej zapory na kilka niezależnych zapór z osobnymi politykami i trasami
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
WMS	Warehouse Management System: system zarządzania magazynem

Skrót	Co znaczy
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

Fiszka

Komendy `az` wykonujemy w Azure CLI w subskrypcji produkcyjnej. Komendy na `edge-az01` wykonujemy w CLI bash jako użytkownik z sudo. Bloki FortiOS wklejamy w CLI `fw-az01` albo `fw01` kontem administratora, a bloki RouterOS w terminalu `rtr-mag01`.

TYLKO ODCZYT

Sprawdzenie tuneli i tras na edge-az01: swanctl --list-sas

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

Pierwsze polecenie pokazuje ustanowione tunele z tożsamością partnera, drugie, którym interfejsem XFRM idzie ruch do Zielonej. Po dołożeniu tunelu ze Swarzędza widzimy trzecie połączenie `mag01`.

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

TYLKO ODCZYT

Plik konfiguracyjny: tunel ze Swarzędza na edge-az01 (swanctl.conf)

```
connections {
    mag01 {
        version = 2
        proposals = aes256-sha256-modp2048
        dpd_delay = 10s
        encap = yes
        local_addrs = %any
```

```
        remote_addrs = 203.0.113.40
        local {
            auth = psk
            id = edge-az01.zielona.example
        }
        remote {
            auth = psk
            id = rtr-mag01.zielona.example
        }
        children {
            mag01-dr {
                local_ts = 10.31.0.0/16
                remote_ts = 10.20.30.0/24
                esp_proposals = aes256-sha256-modp2048
                if_id_in = 13
                if_id_out = 13
                start_action = none
            }
        }
    }
}
secrets {
    ike-mag01 {
        id = rtr-mag01.zielona.example
        secret = "HasloPskMag01"
    }
}
```

Fragment dopisujemy do `/etc/strongswan/swanctl/swanctl.conf` obok połączeń `fw01-w1` i `fw01-w2`, tworzymy interfejs `xfrm3` z `if_id 13` i trasę `10.20.30.0/24 dev xfrm3`, potem `sudo swanctl --load-all`. Selektory są tu jawne, bo MikroTik pracuje na politykach i musi dostać lustrzane sieci.

□□ TYLKO ODCZYT

Plik konfiguracyjny: przekazywanie ruchu sieci DR na edge-az01 (edge.nft)

```
table ip edge {
    chain forward {
        type filter hook forward priority filter; policy drop;
        ct state established,related accept
        ct status dnat accept
        ip saddr 10.31.0.0/16 ip daddr 10.20.0.0/16 accept
        ip saddr 10.20.0.0/16 ip daddr 10.31.0.0/16 accept
        ip saddr 10.31.0.0/16 oifname "eth0" accept
    }
    chain postrouting {
        type nat hook postrouting priority srcnat; policy accept;
        ip saddr 10.31.0.0/16 oifname "xfrm*" accept
        oifname "xfrm*" snat to 10.30.0.4
        ip saddr 10.31.0.0/16 ip daddr != 10.0.0.0/8 oifname "eth0" masquerade
    }
}
```

Uzupełnienie pliku `/etc/nftables/edge.nft` ze strony o łączach (łańcuch `prerouting` zostaje bez zmian). Najważniejsza jest linia `accept` przed `snat`: bez niej każdy pakiet z `dc-az01` dochodziłby do kontrolerów w Pamiątkowie z adresem 10.30.0.4, a replikacja AD i Kerberos przez NAT to proszenie się o kłopoty. Ostatnia linia daje maszynom DR wyjście do internetu.

DR = Disaster Recovery: plan przywrócenia działania po poważnej awarii · **AD** = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie · **NAT** = Network Address Translation: podmiana adresów IP na granicy sieci

TYLKO ODCZYT

Wyszukanie obrazu FortiGate-VM w Marketplace: az vm image list --publisher fortinet

```
az vm image list --publisher fortinet --all --output table
```

Wypisuje oferty i plany Fortinet z wersjami. Plan obrazu wyznacza licencję na całe życie maszyny (BYOL albo PAYG), więc wybieramy go świadomie, a nie pierwszy z listy.

BYOL = Bring Your Own License: przeniesienie własnej licencji na oprogramowanie do chmury zamiast licencji wliczonej w cenę · **PAYG** = Pay-As-You-Go: płatność za zużycie bez zobowiązań, według cennika; w Azure model zakupu subskrypcji, w Marketplace także licencja wliczona w cenę godziny maszyny · **az** = Azure CLI: narzędzie chmury Microsoftu

TYLKO ODCZYT

Akceptacja warunków obrazu: az vm image terms accept

```
az vm image terms accept --urn NazwaObrazuUrn
```

Obrazy z Marketplace z planem wymagają jednorazowej akceptacji warunków w subskrypcji, inaczej tworzenie maszyny kończy się błędem.

az = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Utworzenie kart sieciowych zapory z przekazywaniem: az network nic create --ip-forwarding

```
az network nic create --resource-group NazwaGrupyZasobow --name nic-fw-az01-zew --vnet-name vnet-edge --subnet snet-fw-zew --private-ip-address 10.30.0.36 --public-ip-address pip-fw-az01 --network-security-group nsg-fw-zew --ip-forwarding true
az network nic create --resource-group NazwaGrupyZasobow --name nic-fw-az01-wew --vnet-name vnet-edge --subnet snet-fw-wew --private-ip-address 10.30.0.68 --ip-forwarding true
```

> (podsieci `snet-fw-zew` 10.30.0.32/27 i `snet-fw-wew` 10.30.0.64/27 oraz adres publiczny Standard `pip-fw-az01` tworzymy wcześniej tak samo jak dla `edge-az01`)

Pierwsza karta to `port1` (zewnętrzny), druga `port2` (wewnętrzny). Bez `--ip-forwarding true` Azure wyrzuca pakiety, których adres docelowy nie jest adresem zapory, czyli cały ruch, który zapora ma przekazywać.

az = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Utworzenie maszyny FortiGate-VM z dwiema kartami: az vm create --nics

```
az vm create --resource-group NazwaGrupyZasobow --name fw-az01 --nics nic-fw-az01-zew nic-fw-az01-wew --image NazwaObrazuUrn --size NazwaRozmiaru --admin-username nazwa_usera
```

```
--admin-password HasloAdministratora
```

> (gdzie `NazwaRozmiaru` to rozmiar obsługujący dwie karty sieciowe, z listy obsługiwanych typów maszyn w dokumentacji Fortinet; gdy CLI zgłosi brak informacji o planie, dopisujemy `--plan-name`, `--plan-product` i `--plan-publisher` z wyniku `az vm image show --urn NazwaObrazuUrn`)

Kolejność kart ma znaczenie: pierwsza na liście staje się `port1`.

CLI = Command Line Interface: praca przez wpisywanie komend w terminalu · **az** = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Plik konfiguracyjny: interfejsy i trasy fw-az01 (FortiOS)

```
config system interface
    edit "port1"
        set mode static
        set ip 10.30.0.36 255.255.255.224
        set allowaccess ping
    next
    edit "port2"
        set mode static
        set ip 10.30.0.68 255.255.255.224
        set allowaccess ping https ssh
    next
end
config router static
    edit 1
        set gateway 10.30.0.33
        set device "port1"
    next
    edit 2
        set dst 10.31.0.0 255.255.0.0
        set gateway 10.30.0.65
        set device "port2"
    next
```

```
    edit 3
        set dst 168.63.129.16 255.255.255.255
        set gateway 10.30.0.33
        set device "port1"
    next
end
```

Bramą w Azure jest zawsze pierwszy adres podsieci (10.30.0.33 dla zewnętrznej, 10.30.0.65 dla wewnętrznej), a adres 168.63.129.16 to usługi platformy Azure, które Fortinet zaleca kierować przez `port1`. Zarządzanie zostawiamy tylko na `port2`, czyli z Zielonej przez tunel.

◫◫ ZMIENIA SYSTEM

Plik konfiguracyjny: tunele z fw01 i rtr-mag01 na fw-az01 (FortiOS)

```
config vpn ipsec phase1-interface
    edit "zielona_w1"
        set interface "port1"
        set ike-version 2
        set peertype any
        set proposal aes256-sha256
        set dhgrp 14
        set remote-gw 203.0.113.10
        set psksecret HasloPskFwAz1
        set dpd on-idle
        set comments "fw01 przez wan1"
    next
    edit "zielona_w2"
        set type dynamic
        set interface "port1"
        set ike-version 2
        set peertype one
        set peerid "fw01-w2.zielona.example"
        set proposal aes256-sha256
        set dhgrp 14
        set psksecret HasloPskFwAz2
        set dpd on-idle
        set comments "fw01 przez wan2 (Starlink, adres zmienny)"
    next
```

```
    edit "mag01"
        set interface "port1"
        set ike-version 2
        set peertype any
        set proposal aes256-sha256
        set dhgrp 14
        set remote-gw 203.0.113.40
        set psksecret HasloPskMagFw
        set dpd on-idle
        set comments "rtr-mag01, tunel awaryjny Swarzedz"
    next
end
```

Tunel przez `wan1` ma po obu stronach stałe adresy, a tunel przez Starlink przyjmujemy jako połączenie przychodzące rozpoznawane po identyfikatorze, bo adres `wan2` się zmienia. Fazy 2, adresy wewnętrzne tuneli (10.255.61.1 i .2, 10.255.61.5 i .6) i polityki piszemy tak samo jak dla `edge_w1` i `edge_w2` na stronie o łączach, a dla `mag01` z selektorami 10.31.0.0/16 i 10.20.30.0/24.

□□ TYLKO ODCZYT

Sprawdzenie tunelu na FortiGate: diagnose vpn tunnel list name

```
diagnose vpn tunnel list name NazwaTunelu
get router info routing-table all
```

Pierwsze polecenie pokazuje stan fazy 1 i 2 oraz liczniki pakietów jednego tunelu, drugie tablicę tras z trasami przez tunele. Wykonujemy na `fw-az01` i na `fw01`.

□□ ZMIENIA SYSTEM

Dodanie sieci DR do tras i SD-WAN na fw01 (FortiOS)

```
config firewall address
    edit "DR_VNET"
        set subnet 10.31.0.0 255.255.0.0
    next
end
config system sdwan
```

```
    config service
        edit 21
            append dst "DR_VNET"
        next
    end
end
```

Reguła SD-WAN `DoEdge` ze strony o łączach kieruje wtedy do tuneli także ruch do sieci DR. Polityki z `DR_VNET` jako źródłem dopuszczają tylko to, czego potrzebuje kontroler i kopie baz (AD, DNS, Kerberos, LDAP, SMB do `bkp01`), a nie całą sieć serwerów.

DR = Disaster Recovery: plan przywrócenia działania po poważnej awarii · **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 · **AD** = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie · **DNS** = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP · **LDAP** = Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA) · **SMB** = Server Message Block: protokół udostępniania plików i drukarek w sieci Windows, na nim stoi zwykły udział sieciowy

TYLKO ODCZYT

Plik konfiguracyjny: tunel awaryjny rtr-mag01 do Azure (RouterOS)

```
/ip ipsec peer
add name=azure-dr address=203.0.113.60/32 exchange-mode=ike2 profile=zielona-ike2

/ip ipsec identity
add peer=azure-dr auth-method=pre-shared-key secret="HasloPskMag01" \
    my-id=fqdn:rtr-mag01.zielona.example remote-id=fqdn:edge-az01.zielona.example

/ip ipsec policy
add src-address=10.20.30.0/24 dst-address=10.31.0.0/16 tunnel=yes action=encrypt \
    proposal=zielona-esp peer=azure-dr comment="swz do sieci DR"

/ip firewall address-list
add list=pamiatkowo address=10.31.0.0/16
```

Profil `zielona-ike2` i propozycja `zielona-esp` są już na routerze ze strony IPsec site-to-site: Pamiątkowo i Swarzędz między FortiGate a routerem innej firmy. Dopisanie 10.31.0.0/16 do listy `pamiatkowo` wyłącza maskaradę dla ruchu do Azure. W wariancie `fw-az01` adresem

partnera jest 203.0.113.61.

IPsec = Internet Protocol Security: zestaw protokołów szyfrujących i uwierzytelniających ruch sieciowy, na nim stoi tunel VPN typu IKEv2

Z życia wzięte

Z ŻYCIA WZIĘTE

Środa, 9:15. Tomek pokazuje na tablicy, że w scenariuszu „pożar serwerowni” tunel `edge_w1` nie ma się z czym zestawić, bo `fw01` stał w szafie R1. Marek pyta, jak w takim razie skanery dojdą do WMS w Azure. Odpowiedź jest na tej stronie: tunel `mag01` ze Swarzędza do Azure stoi cały czas, nieużywany, i czeka na dzień, w którym `ora-dr01` dostanie adres 10.31.10.32.

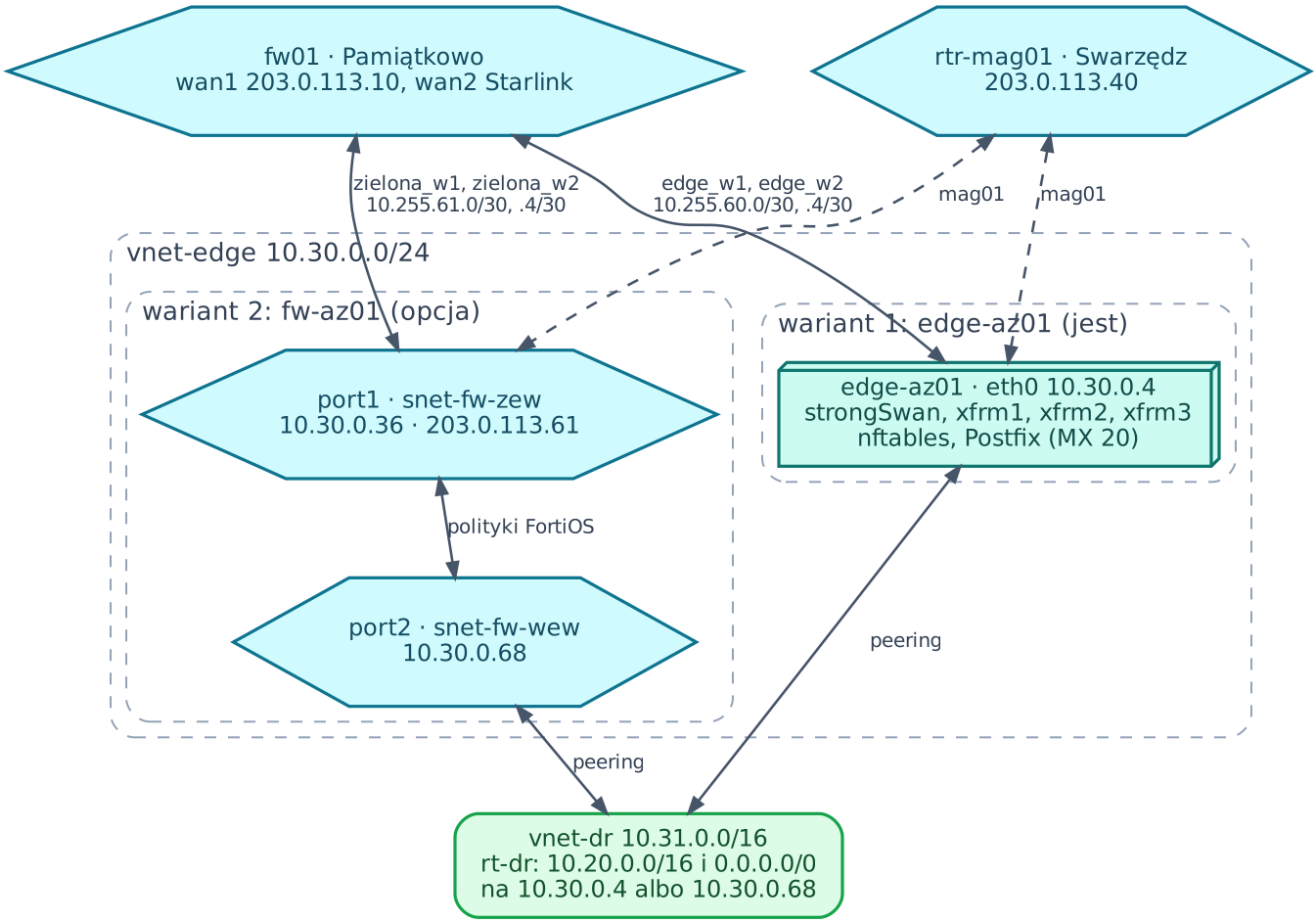
Jak to działa

Rozwiń: jak to działa pod spodem

Dwa warianty obok siebie

> **Pojęcie: maszyna pośrednicząca (NVA).** Maszyna wirtualna w chmurze, która pełni rolę routera albo zapory: przyjmuje ruch innych maszyn i przekazuje go dalej, na przykład do tunelu. Trasy użytkownika w Azure kierują do niej ruch z wybranych podsieci.

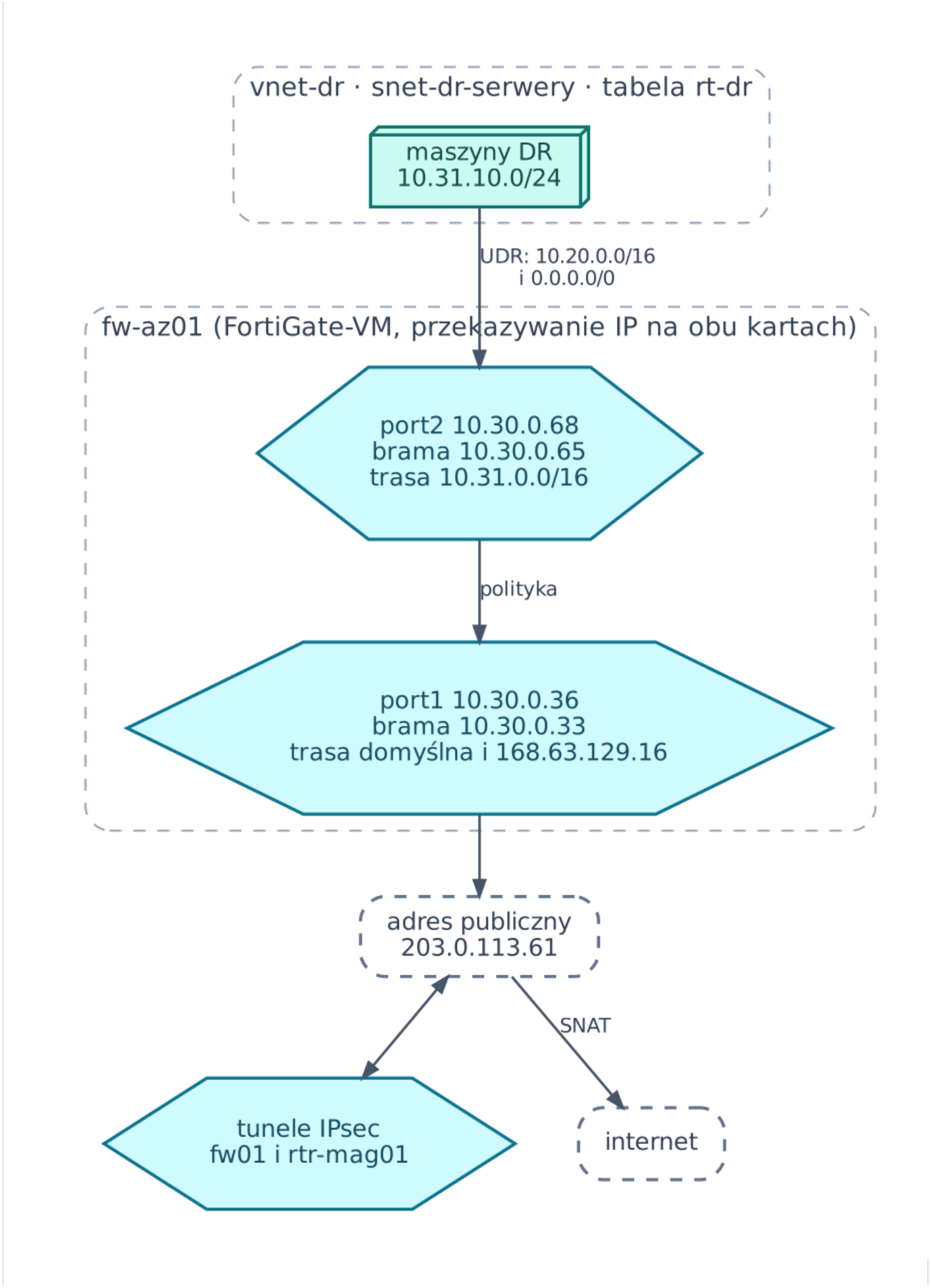
`edge-az01` ma jedną kartę sieciową, tunele strongSwan z interfejsami XFRM i proste reguły nftables. Dołożenie sieci DR to trzy rzeczy: trasa w Azure, wyjątek od podmiany adresu i reguły przekazywania. `fw-az01` to pełna zapora z dwiema kartami, politykami, SD-WAN i VPN dla pracowników w tej samej składni co `fw01`, ale z osobną licencją i większą maszyną.



Rysunek 1. Dwa warianty tunelu do Azure: edge-az01 z jedną kartą, strongSwan i nftables oraz fw-az01 z port1 w podsieci zewnętrznej i port2 w wewnętrznej; oba trzymają tunele do fw01 przez wan1 i wan2 oraz tunel awaryjny z rtr-mag01, a trasa w sieci DR wskazuje 10.30.0.4 albo 10.30.0.68 (kliknięcie otwiera pełny rozmiar)

Trasy w wariancie z FortiGate-VM

Fortinet opisuje pojedynczą zaporę w Azure jako trzy podsieci: zewnętrzną z publicznym adresem, wewnętrzną (tranzytową) i chronione podsieci z serwerami. Tabela tras przypięta do chronionej podsieci kieruje ruch spoza sieci na wewnętrzny adres zapory, a trasa do własnej podsieci pozwala maszynom w jednej podsieci rozmawiać bez przechodzenia przez zaporę. Prywatne adresy obu interfejsów są przypisane statycznie przy wdrożeniu.


vnet-dr · snet-dr-serwery · tabela rt-dr
maszyny DR
10.31.10.0/24
UDR: 10.20.0.0/16
i 0.0.0.0/0
fw-az01 (FortiGate-VM, przekazywanie IP na obu kartach)
port2 10.30.0.68
brama 10.30.0.65
trasa 10.31.0.0/16
polityka
port1 10.30.0.36
brama 10.30.0.33
trasa domyślna i 168.63.129.16
adres publiczny
203.0.113.61
SNAT
tunele IPsec
fw01 i rtr-mag01
internet

Rysunek 2. Trasy w wariancie fw-az01: maszyny w snet-dr-serwery wysyłają ruch do Zielonej i do internetu przez trasę rt-dr na 10.30.0.68 (port2), zapora wysyła tunele i internet przez port1 z bramą 10.30.0.33 i adresem publicznym 203.0.113.61, a ruch powrotny do 10.31.0.0/16 idzie przez port2 z bramą 10.30.0.65 (kliknięcie otwiera pełny rozmiar)

Licencje FortiGate-VM

Obraz w Marketplace wyznacza licencję na całe życie maszyny: zmiana z BYOL na PAYG albo odwrotnie oznacza nową maszynę i przeniesienie konfiguracji z kopii. Fortinet opisuje to tak: kopia konfiguracji, nowa maszyna z innym planem, odtworzenie konfiguracji przy pierwszym starcie albo później, a dla BYOL zakup licencji u resellera.

Model	Jak płacimy	Co zyskujemy	Na co uważamy
PAYG	godzinowo w rachunku Azure, razem z maszyną	zero rozmów z resellerem, maszynę można wyłączyć	według dokumentacji Fortinet bez domen wirtualnych (VDOM); cena za godzinę z Marketplace, sprawdzamy w kalkulatorze
BYOL	licencja roczna albo wieloletnia od resellera, maszyna osobno w Azure	pełne funkcje zależnie od umowy, wsparcie FortiCare jak dla `fw01`	płacimy za licencję także wtedy, gdy maszyna stoi wyłączona
FortiFlex	punkty zużywane dziennie według konfiguracji, rozliczane z Fortinet	elastyczność przy kilku urządzeniach wirtualnych	tabela punktów w dokumentacji FortiFlex (wydanie 26.3.0), wycena u resellera

Wysoka dostępność zapory w Azure (informacyjnie)

Fortinet opisuje trzy układy pary: aktywny i pasywny z równoważeniem Azure Load Balancer (przełączenie po sondach, według dokumentacji najwyżej około 15 sekund), aktywny i pasywny z łącznikiem SDN (zapora zapasowa przez API Azure przenosi adres publiczny i trasy na siebie) oraz aktywny i aktywny z równoważeniem. Ta sama strona przytacza dostępność według sposobu wdrożenia: strefy dostępności 99,99 procent, zestaw dostępności 99,95 procent, pojedyncza maszyna z dyskiem premium SSD 99,9 procent. Dla zapasowej serwerowni Zielonej para to przesada: jedna zapora, która w razie awarii powstaje z kopii konfiguracji w kilkanaście minut, jest spójna z RTO liczonym w godzinach.

Porównanie wariantów

	`edge-az01` (Rocky Linux 9, strongSwan)	`fw-az01` FortiGate-VM BYOL	`fw-az01` FortiGate-VM PAYG	Azure VPN Gateway
Koszt stały	mała maszyna, dysk, adres publiczny; maszyna już istnieje	maszyna z dwiema kartami, dyski, adres, licencja od resellera	maszyna, dyski, adres, licencja w cenie godziny	opłata godzinowa za SKU bramy i ruch wychodzący; od 30 września 2026 tylko SKU strefowe (AZ), kwoty w kalkulatorze
VPN dla pracowników w awarii	WireGuard dla administratorów (`wg01` przez przekierowanie albo na maszynie), reszta do zaprojektowania	FortiClient tak jak do `fw01`	jak BYOL	Point-to-Site z własnym klientem, osobna konfiguracja
Ruch przychodzący z internetu (poczta, WWW)	tak: Postfix jako MX 20 i przekierowania nftables	tak: VIP i polityki	tak	nie, brama nie przekazuje ruchu z internetu
Łatanie i aktualizacje	my: system, strongSwan, nftables	my: FortiOS, jak na `fw01`	my: FortiOS	Microsoft
Wsparcie producenta	społeczność, dokumentacja strongSwan; obraz Rocky od CIQ z ograniczonym wsparciem Microsoft	FortiCare według licencji	według warunków oferty PAYG	wsparcie Azure
Składnia i wiedza w zespole	Linux, jak reszta serwerów Zielonej	ta sama co `fw01`	ta sama co `fw01`	portal i CLI Azure
Wysoka dostępność	druga maszyna i przełączenie trasy ręcznie albo skryptem	para z Load Balancer albo łącznikiem SDN	jak BYOL	wbudowana w SKU strefowe
Bez Microsoftu	tak, ta sama maszyna stanie w AWS jako EC2	tak, FortiGate-VM jest też w AWS	tak	nie

Cen nie podajemy kwotami, bo zależą od regionu, rozmiaru, umowy i kursu. Do rozmowy z panem Zbigniewem liczymy je w kalkulatorze Azure i w ofercie resellera Fortinet dla naszej konfiguracji, według strony Wymiarowanie i zakup zapasowej serwerowni w Azure: pojemność, koszty i zapytanie do partnera.

> □□ Rocky Linux 9 ma w repozytoriach podstawowych libreswan, a strongSwan pochodzi z EPEL. `edge-az01` używa strongSwan z interfejsami XFRM, więc przy nim zostajemy; libreswan z interfejsami `ipsec-interface` to rozsądna droga dla kogoś, kto nie chce EPEL, ale wtedy przepisujemy konfigurację, a nie tylko składnię.

Rekomendacja dla Zielonej

Na start rozbudowujemy `edge-az01`: maszyna już istnieje, jest opisana i ma tunele przez oba łącza, a koszt sieci DR to kilka reguł. `fw-az01` ma sens wtedy, gdy plan ciągłości wymaga VPN dla wszystkich pracowników prosto do Azure (handlowcy, księgowość z domu) albo gdy audytor oczekuje tej samej kontroli ruchu co na `fw01`. Decyzja należy do autora i pana Zbigniewa, a kryterium jest proste: ile osób ma pracować z odtworzonymi systemami spoza biura i czy rozwiązanie zastępcze dla nich (zdalny pulpit przez bramę, praca z magazynu) wystarczy.

Częste błędy

Objaw	Przyczyna	Co robimy
`dc-az01` widzi kontrolery w Pamiątkowie, ale replikacja zgłasza błędy uwierzytelniania	`edge-az01` podmienia adres na 10.30.0.4	wyjątek `ip saddr 10.31.0.0/16 oifname "xfrm*" accept` przed regułą `snat`
Maszyny DR nie wychodzą do internetu	podsieć prywatna i brak maskarady albo trasy 0.0.0.0/0	trasa domyślna w `rt-dr` na maszynę pośredniczącą i reguła `masquerade` z wyjątkiem 10.0.0.0/8
Zapora `fw-az01` nie przekazuje ruchu między `port2` a tunelem	brak przekazywania IP na karcie w Azure	`az network nic update --ip-forwarding true` dla obu kart
Tunel przez Starlink do `fw-az01` nie wstaje po restarcie zestawu	faza 1 z adresem stałym zamiast połączenia przychodzącego	`set type dynamic`, `peertype one` i `peerid` zgodny z `localid` na `fw01`
Tunel `mag01` stoi, ruch nie płynie	maskarada na MikroTiku albo FastTrack przed regułami IPsec	10.31.0.0/16 na liście `pamiatkowo`, reguły IPsec przed FastTrack, jak w s4-01
Zmiana licencji FortiGate-VM z PAYG na BYOL „nie działa”	licencja jest związana z obrazem maszyny	nowa maszyna z planem BYOL i odtworzenie konfiguracji z kopii

□□ Ćwiczenia

1. Dlaczego tunel ze Swarzędza do Azure stawiamy od razu, a nie w dniu awarii?

Odpowiedź

Bo w dniu awarii `fw01` może nie istnieć, a konfiguracja tunelu po obu stronach, test i poprawki to godziny pracy, których wtedy nie mamy. Tunel zestawiony zawczasu kosztuje prawie nic, a w teście lokalizacji sprawdzamy, że ruch ze Swarzędza dochodzi do sieci DR bez udziału Pamiątkowa.

1. Co dzieje się z ruchem `dc-az01` do `dc01`, jeśli zapomnimy o regule `accept` przed `snat to 10.30.0.4` na `edge-az01`?

Odpowiedź

Pakiety dochodzą do `dc01` z adresem 10.30.0.4 zamiast 10.31.1.11. Kontroler w Pamiątkowie odpowiada na 10.30.0.4, ale lokacja, rejestracja DNS i część protokołów (Kerberos, RPC) oczekują prawdziwego adresu partnera, więc replikacja kończy się błędami albo działa częściowo. Ruch sieci DR przez tunel nie może być podmieniany.

1. Pan Zbigniew pyta, czemu nie kupić po prostu Azure VPN Gateway, skoro to usługa Microsoftu bez łatania. Jakie dwa argumenty podajemy?

Odpowiedź

Po pierwsze brama kosztuje co godzinę przez cały rok, a w zapasowej serwerowni przez większość roku tunel tylko czeka. Po drugie brama nie przyjmuje ruchu z internetu, więc poczta (MX 20) i publikacja usług i tak wymagają maszyny w rodzaju `edge-az01`; mielibyśmy wtedy dwie rzeczy zamiast jednej.

1. Wybraliśmy FortiGate-VM PAYG, a po roku reseller proponuje tańszą licencję BYOL. Jak przechodzimy?

Odpowiedź

Licencja jest związana z obrazem, więc robimy kopię konfiguracji `fw-az01`, wdrażamy nową maszynę z planu BYOL z tymi samymi kartami (albo nowymi z tymi samymi adresami), wgrywamy licencję i konfigurację, sprawdzamy tunele i usuwamy starą maszynę. Przejście planujemy w oknie zmian, poza zakazem od 15 listopada do 6 stycznia.

Powiązane: Łącza operatora: światłowód, radiolinia, LTE i 5G oraz przełączanie na FortiGate · IPsec site-to-site: Pamiątkowo i Swarzędz między FortiGate a routerem innej firmy · Para FortiGate w klastrze: FGCP aktywny-pasywny · Azure jako zapasowa serwerownia Zielonej: architektura, co replikujemy, a co odtwarzamy · WireGuard i OpenVPN: odpowiedniki spoza FortiGate na Linuksie

Źródła (odczyt 1 listopada 2026):

1. docs.fortinet.com, „Single FortiGate-VM deployment” (Azure, FortiOS 8.0: podsieci zewnętrzna, wewnętrzna i chronione, trasy UDR).
2. docs.fortinet.com, „Azure routing and network interfaces” (FortiOS 7.6: `port1` zewnętrzny, `port2` wewnętrzny, statyczne adresy, brama jako pierwszy adres podsieci, 168.63.129.16 przez `port1`, tabela tras z trzema trasami).
3. docs.fortinet.com, „Migrating a FortiGate-VM instance between license types” (licencja zależna od obrazu, PAYG bez VDOM, przeniesienie konfiguracji).
4. docs.fortinet.com, „HA for FortiGate-VM on Azure” (FortiOS 7.2: trzy układy pary, sondy Load Balancer, dostępność 99,99, 99,95 i 99,9 procent).
5. docs.fortinet.com, FortiFlex (Flex-VM), „Points”, wydanie 26.3.0.
6. learn.microsoft.com, „What's new in Azure VPN Gateway” (wycofanie SKU VpnGw1 do 5 bez stref 30 września 2026, nowe ceny SKU strefowych od stycznia 2025), aktualizacja 17 września 2026.
7. Konfiguracja `edge-az01`, `fw01` i `rtr-mag01`: strony Łącza operatora: światłowód, radiolinia, LTE i 5G oraz przełączanie na FortiGate i IPsec site-to-site: Pamiątkowo i Swarzędz między FortiGate a routerem innej firmy.

Revision #2
Created 2026-11-01 18:02:24 UTC by Tomasz Konieczny
Updated 2026-11-01 18:03:48 UTC by Tomasz Konieczny