FortiGate

Zarządzanie siecią na FortiGate i para w klastrze FGCP.

- FortiGate w zarządzaniu siecią: interfejsy, VLAN-y, polityki i NAT
- Para FortiGate w klastrze: FGCP aktywny-pasywny

FortiGate w zarządzaniu siecią: interfejsy, VLAN-y, polityki i NAT

Poziom: średnio

Dotyczy: FortiGate 100F (fw01), FortiOS 7.6 i 8.0, VLAN 10, 20, 30, 40, 98 i 99, CA-Zielona, Graylog

Czas: ~90 min

Zapora FortiGate nie tylko wpuszcza VPN, ale decyduje, kto z kim w sieci Zielonej może rozmawiać, i zapisuje, co się stało. Ta strona pokazuje, jak `fw01` jest podzielony na interfejsy, strefy i polityki, jak działa NAT, kto i skąd może go administrować, jak robimy kopię i aktualizację oraz jak jego logi trafiają do Grayloga. Wracamy tu przed każdą zmianą reguł i przed każdą aktualizacją FortiOS.

ZAŁOŻENIA SCENARIUSZA

zapora to pojedynczy `fw01` z dwoma łączami: światłowodem (`wan1`, 203.0.113.10) i Starlinkiem (`wan2`) z publicznym, ale zmiennym adresem. Magazyn w Swarzędzu jest podłączony do sieci centrali: VLAN 30 kończy się na `fw01` (brama 10.20.30.1), a DHCP dla VLAN 20 i 30 obsługują `dc01` i `dc02` przez przekaźnik na zaporze. Parę FortiGate opisuje Para FortiGate w klastrze: FGCP aktywny-pasywny, a magazyn jako osobną lokalizację z tunelem IPsec site-to-site: Pamiątkowo i Swarzędz między FortiGate a routerem innej firmy.

Skróty użyte na tej stronie (42)

Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie
AD CS	Active Directory Certificate Services: rola Windows Server pełniąca funkcję firmowego urzędu certyfikacji
BMC	Baseboard Management Controller: osobny malutki komputer na płycie serwera, który działa nawet przy wyłączonym serwerze i odczytuje m.in. temperatury czujników
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu

Skrót	Co znaczy
DHCP	Dynamic Host Configuration Protocol: usługa, która sama rozdaje komputerom adresy IP
DMZ	Demilitarized Zone: osobna sieć za zaporą dla usług dostępnych z internetu, odgrodzona od sieci wewnętrznej; w FortiGate 100F tak jest opisany jeden z portów
DNAT	Destination Network Address Translation: podmiana adresu docelowego pakietu, używana do przekierowania ruchu z zewnątrz do serwera wewnątrz sieci
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
EAP-TLS	EAP z TLS: uwierzytelnianie certyfikatem użytkownika albo urządzenia zamiast hasła
FSSO	Fortinet Single Sign-On: mechanizm FortiGate, który podgląda logowania w Active Directory i sam wie, z jakiej grupy korzysta dana osoba, bez proszenia jej o dodatkowe hasło
FTP	File Transfer Protocol: stary protokół przesyłania plików, bez szyfrowania
GB	Gigabyte: miliard bajtów, jednostka pojemności pamięci i plików, tu najczęściej rozmiar modelu albo pamięci karty graficznej
GUI	Graphical User Interface: okienka i myszka zamiast komend
HA	High Availability: wysoka dostępność, czyli działanie mimo awarii jednego elementu
HTTPS	HTTP zabezpieczony szyfrowaniem TLS
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)
IPS	Intrusion Prevention System: moduł zapory, który rozpoznaje w ruchu znane wzorce ataków i może je zablokować, zanim dotrą do serwera
IPsec	Internet Protocol Security: zestaw protokołów szyfrujących i uwierzytelniających ruch sieciowy, na nim stoi tunel VPN typu IKEv2
MGMT	Management: oznaczenie portu zarządzania na urządzeniu; w parze FortiGate to port, przez który wchodzimy na każdą sztukę osobno
NAT	Network Address Translation: podmiana adresów IP na granicy sieci
NPS	Network Policy Server: rola Windows Server obsługująca RADIUS, pośredniczy w sprawdzaniu hasła domenowego przy logowaniu do VPN albo Wi-Fi
RADIUS	Remote Authentication Dial-In User Service: standardowy protokół pytania serwera, czy podane konto i hasło są poprawne
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
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

Skrót	Co znaczy
SFTP	SSH File Transfer Protocol: bezpieczne przesyłanie plików przez SSH
SNAT	Source NAT: podmiana adresu nadawcy w ruchu wychodzącym
SPF	Sender Policy Framework: rekord DNS mówiący, które serwery mogą wysyłać pocztę domeny
SSD	Solid State Drive: dysk półprzewodnikowy
SSH	Secure Shell: szyfrowane zdalne logowanie do serwera
SSL	Secure Sockets Layer: dawna nazwa szyfrowania, dziś formalnie TLS
TCP	Transmission Control Protocol: protokół sieciowy z potwierdzaniem dostarczenia
TFTP	Trivial File Transfer Protocol: bardzo prosty protokół przesyłania plików bez uwierzytelniania, w FortiGate jedna z dróg wysłania kopii konfiguracji
UDP	User Datagram Protocol: szybki protokół sieciowy bez potwierdzeń
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
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
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

Fiszka

Polecenia wykonujemy w CLI FortiOS po zalogowaniu przez SSH na adres `10.20.98.1` z sieci VLAN 98 albo z VPN administratorów, na własnym koncie administratora. Składnię poleceń, których nie oznaczyliśmy źródłem, sprawdzamy w dokumentacji naszej wersji FortiOS przed pierwszym użyciem [1].

□□ TYLKO ODCZYT

Odczyt wersji FortiOS i numeru seryjnego: get system status

```
get system status
```

Pokazuje wersję FortiOS, numer seryjny, nazwę urządzenia, tryb pracy i stan licencji. Pierwsze polecenie przed każdą aktualizacją, przed zgłoszeniem do wsparcia Fortinet i po każdej zmianie wersji [1].

Przykład (poglądowy, układ pól sprawdzamy w naszej wersji):

```
Version: FortiGate-100F v7.6.6,buildNNNN,DATA
Serial-Number: FG100FTK20000000
Hostname: fw01
Operation Mode: NAT
Virtual domain configuration: disable
```

get = FortiOS: polecenia odczytu stanu urządzenia, na przykład get system status pokazuje wersję i numer seryjny

TYLKO ODCZYT

Odczyt konfiguracji jednego interfejsu: show system interface

```
show system interface NazwaInterfejsu
```

Wypisuje tylko ustawienia różniące się od domyślnych, więc krótko pokazuje adres, VLAN, dostęp administracyjny i przekaźnik DHCP wybranego interfejsu.

Przykład (poglądowy, `fw01`):

```
config system interface
    edit "VLAN20_Biuro"
        set vdom "root"
        set ip 10.20.20.1 255.255.255.0
        set allowaccess ping
        set dhcp-relay-service enable
        set dhcp-relay-ip "10.20.10.11" "10.20.10.12"
        set role lan
        set interface "LAG_Rdzen"
        set vlanid 20
    next
end
```

VLAN = Virtual LAN: wydzielona logicznie sieć na tym samym sprzęcie · **DHCP** = Dynamic Host Configuration Protocol: usługa, która sama rozdaje komputerom adresy IP · **show** = FortiOS: wypisuje konfigurację, w podstawowej postaci tylko ustawienia różniące się od domyślnych, a z

wariantem full-configuration także wartości domyślne

TYLKO ODCZYT

Odczyt polityk zapory: show firewall policy

```
show firewall policy NumerPolityki
```

Pokazuje jedną politykę z jej ustawieniami: strefy, adresy, usługi, NAT, profile i logowanie. Bez numeru wypisuje wszystkie polityki w kolejności numerów, która nie musi być kolejnością dopasowania, o czym piszemy niżej.

NAT = Network Address Translation: podmiana adresów IP na granicy sieci · **show** = FortiOS: wypisuje konfigurację, w podstawowej postaci tylko ustawienia różniące się od domyślnych, a z wariantem full-configuration także wartości domyślne

TYLKO ODCZYT

Odczyt tablicy tras: get router info routing-table all

```
get router info routing-table all
```

Pokazuje trasy, którymi `fw01` wysyła pakiety, w tym trasę domyślną przez łącze operatora. Pierwsze polecenie, gdy ktoś mówi, że „nie ma internetu” [2].

get = FortiOS: polecenia odczytu stanu urządzenia, na przykład get system status pokazuje wersję i numer seryjny

TYLKO ODCZYT

Odczyt sesji do jednego serwera: diagnose sys session list

```
diagnose sys session filter dst AdresDocelowy
diagnose sys session list
diagnose sys session filter clear
```

Ustawiamy filtr, wypisujemy sesje przechodzące przez `fw01` i czyścimy filtr, żeby kolejne polecenia nie pokazywały tylko jednego adresu. Wynik zawiera między innymi numer polityki, która przepuściła ruch, i przetłumaczone adresy NAT [2].

NAT = Network Address Translation: podmiana adresów IP na granicy sieci · **diagnose** = FortiOS: polecenia diagnostyczne zapory i zarządzanych przełączników, na przykład diagnose sys sdwan

member pokazuje członków SD-WAN

TYLKO ODCZYT

Podsłuch pakietów na zaporze: diagnose sniffer packet

```
diagnose sniffer packet NazwaInterfejsu 'host AdresSerwera and port NumerPortu' 4 20
```

> (gdzie `NazwaInterfejsu` to nazwa interfejsu albo słowo `any`, a liczby na końcu to poziom szczegółowości i liczba pakietów do pokazania; znaczenie poziomów opisuje dokumentacja naszej wersji [2])

Pozwala sprawdzić, czy pakiet w ogóle doszedł do `fw01` i którędy wyszedł, zanim zaczniemy zmieniać polityki.

diagnose = FortiOS: polecenia diagnostyczne zapory i zarządzanych przełączników, na przykład diagnose sys sdwan member pokazuje członków SD-WAN

TYLKO ODCZYT

Kopia konfiguracji na bkp01: execute backup config sftp

```
execute backup config sftp NazwaPliku.conf bkp01.ad.zielona.example nazwa_usera
HasloUsera HasloSzyfrujace
```

> (gdzie `HasloSzyfrujace` jest opcjonalnym hasłem szyfrującym plik kopii; składnia dla FTP i TFTP różni się w szczegółach [3])

Wysyła pełną konfigurację `fw01` na serwer kopii. Robimy to ręcznie przed każdą zmianą, a automatycznie raz na dobę, jak opisujemy w sekcji o kopii.

FTP = File Transfer Protocol: stary protokół przesyłania plików, bez szyfrowania ·**TFTP** = Trivial File Transfer Protocol: bardzo prosty protokół przesyłania plików bez uwierzytelniania, w FortiGate jedna z dróg wysłania kopii konfiguracji · **execute** = FortiOS: polecenia, które coś wykonują na urządzeniu, na przykład execute backup config wysyła kopię konfiguracji, a execute ha manage otwiera sesję na drugiej zaporze w parze

TYLKO ODCZYT

Odczyt listy rewizji konfiguracji: execute revision list config

```
execute revision list config
```

Wypisuje rewizje konfiguracji zapisane na samym urządzeniu, z numerami potrzebnymi do powrotu [4].

execute = FortiOS: polecenia, które coś wykonują na urządzeniu, na przykład execute backup config wysyła kopię konfiguracji, a execute ha manage otwiera sesję na drugiej zaporze w parze

OSTROŻNIE · NIEODWRACALNE

Powrót do rewizji konfiguracji: execute restore config flash

```
execute restore config flash NumerRewizji
```

Zastępuje bieżącą konfigurację wybraną rewizją i restartuje urządzenie, więc przerywa ruch całej sieci. Sięgamy po to polecenie dopiero wtedy, gdy zmiana zepsuła sieć, a poprawka ręczna jest wolniejsza niż powrót [4].

execute = FortiOS: polecenia, które coś wykonują na urządzeniu, na przykład execute backup config wysyła kopię konfiguracji, a execute ha manage otwiera sesję na drugiej zaporze w parze

Z życia wzięte

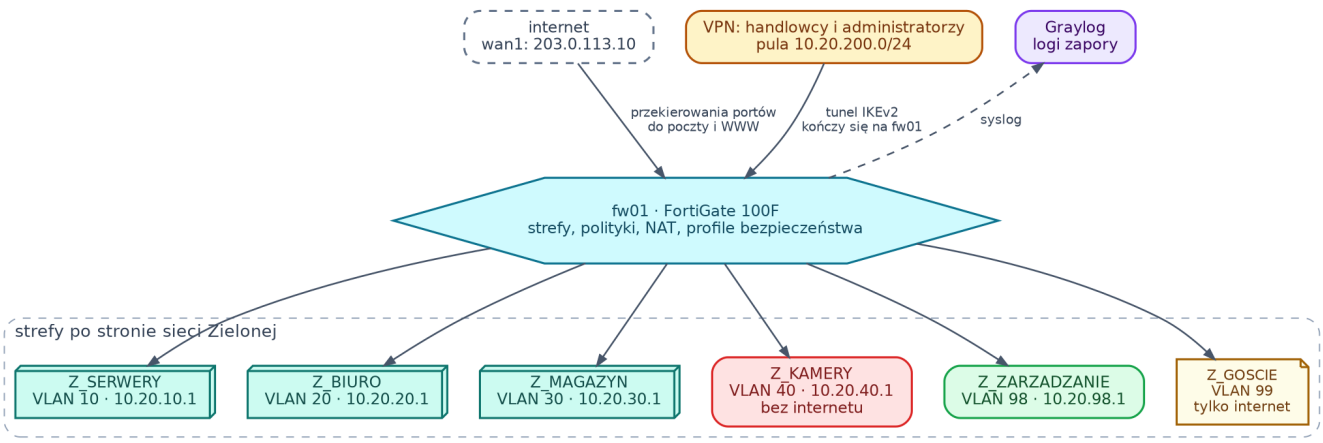
Z ŻYCIA WZIĘTE

Czwartek, 10:30. Marek dzwoni, że skanery w Swarzędzu nie łączą się z WMS po porannej zmianie reguł. Tomek dodał politykę „MAG-do-WMS” na samym końcu listy, a wyżej stoi polityka blokująca cały ruch z magazynu do sieci serwerów. `fw01` dopasowuje ruch od góry do pierwszej pasującej polityki, więc nowa reguła nigdy nie dostaje pakietów. Tomek przeciąga ją nad blokadę, sprawdza `diagnose sys session list` z numerem polityki i zapisuje w komentarzu, po co powstała, bo przed zmianą zrobił kopię, a po niej dopisał ją do wpisu zmiany.

Jak to działa

Rozwiń: jak to działa pod spodem

`fw01` to FortiGate 100F: urządzenie, które jest jednocześnie routerem między sieciami VLAN, zaporą, bramą VPN i filtrem treści. Wszystko, co kiedykolwiek przechodzi między dwiema sieciami Zielonej albo między Zieloną a internetem, przechodzi przez jego polityki. Przełączniki z Przełączniki: L2 i L3, tablica MAC, VLAN, LACP i STP niczego nie trasują, więc żaden pakiet z VLAN 20 do VLAN 10 nie omija reguł zapory.



Rysunek 1. Strefy fw01: internet i VPN po jednej stronie, sześć stref sieci Zielonej po drugiej, logi płyną do Grayloga. Warto zauważyć, że każda strzałka prowadzi przez fw01, a kamery i goście mają z założenia ograniczone wyjście. (kliknięcie otwiera pełny rozmiar)

Pojęcie: FortiOS. System operacyjny zapór FortiGate. Numer wersji ma postać 7.6.6: pierwsze dwie liczby to gałąź (7.6), trzecia to kolejna poprawka w tej gałęzi.

Pojęcie: strefa. Nazwana grupa interfejsów, do której odwołujemy się w politykach zamiast do pojedynczych interfejsów. Dzięki strefie jedna reguła obejmuje na przykład wszystkie sieci serwerowe, a nowy interfejs dodany do strefy dostaje te same reguły.

Pojęcie: polityka (firewall policy). Jedna reguła zapory: z jakiej strefy, do jakiej, od jakich adresów, do jakich adresów, jakimi usługami, co zrobić (przepuścić albo zablokować) i co przy tym zapisać w logu.

Wersja FortiOS: 7.6 czy 8.0

Na październik 2026 sprawdziliśmy w dokumentacji Fortinet, jakie gałęzie wchodzą w grę dla `fw01`.

Gałąź	Stan w październiku 2026	Uwagi
7.6	dokumentacja pokazuje już wydanie 7.6.7 [5]; na liście zalecanych wydań dla FortiGate 100F (stan z czerwca 2026) stoi 7.6.6, a Fortinet przegląda listę co kwartał [1]	od 7.6.3 tryb tunelowy SSL VPN zastąpiono IPsec [6]; Zielona używa IKEv2, więc nas to nie dotyczy
8.0	8.0.0 z 21 kwietnia 2026, dokumentacja pokazuje już 8.0.1 [7][8]; FortiGate 100F jest na liście obsługiwanych modeli [7]	jest nowa, więc przed wdrożeniem czytamy sekcje „Known issues” i „Upgrade information” w notach wydania

Czy 7.6.x ma już oznaczenie „Mature” (tylko poprawki, bez nowych funkcji), nie potwierdziliśmy: według Fortinet nie da się tego przewidzieć z góry, a status widać w `System > Firmware & Registration` albo w wyniku `get system status` [9]. Daty końca sprzedaży i wsparcia modelu 100F też sprawdzamy w Fortinet Product Life Cycle, bo ich nie potwierdziliśmy.

Proponujemy zostać na gałęzi 7.6 w wydaniu z aktualnej listy zalecanych i wrócić do 8.0 po kilku poprawkach. To decyzja autora bazy. W dyskusji pod listą zalecanych wydań ktoś zgłosił problem z IPsec po 7.6.6 [1], więc przed każdą aktualizacją czytamy w notach wydania sekcję o znanych problemach z IPsec, bo na IPsec stoi VPN Kasi.

Dostęp administracyjny do fw01

Zasada: `fw01` administrujemy tylko z VLAN 98 i z VPN administratorów, zawsze na koncie imiennym, z drugim składnikiem logowania, a konto lokalne zostaje na awarię.

Warstwa	Ustawienie	Po co
Interfejsy	`allowaccess` tylko na interfejsie `VLAN98_Zarzadzanie`: `https`, `ssh`, `ping`; na `wan1`, `wan2` i w VLAN-ach użytkowników pusty [10]	nikt z internetu ani z biura nie widzi panelu
Hosty zaufane	dla każdego administratora `trusthost1` 10.20.98.0/24 i `trusthost2` 10.20.200.0/24 [10]	konto działa tylko z VLAN 98 i z puli VPN
Reguły local-in	polityka `local-in-policy` zawęża dostęp do adresów administratorów i blokuje resztę [11]	druga warstwa niezależna od kont

Warstwa	Ustawienie	Po co
Konta	imienne konta z AD przez RADIUS (NPS na `dc02`), dostęp według grupy `GG_FW_Administratorzy` (propozycja nazwy)	odejście osoby z firmy zamyka dostęp przez AD
Drugi składnik	FortiToken albo MFA po stronie RADIUS, do wyboru przez autora bazy	samo hasło domenowe nie wystarcza
Konto awaryjne	jedno konto lokalne, `admin-restrict-local non-console-only` [12]	wejście, gdy NPS albo AD nie odpowiada
Sesja	`admintimeout` 5 minut, blokada po kilku nieudanych próbach, HTTPS i SSH na własnych portach według uznania [10]	krótsze okno dla przejętej sesji

Trusted hosts i local-in-policy nie łączą się swobodnie: według Fortinet zaufane adresy ustawione na poziomie interfejsu mają pierwszeństwo przed regułami local-in, a przy użyciu local-in zaufane adresy na interfejsie trzeba usunąć [11]. My używamy zaufanych adresów na kontach administratorów, a regułom local-in dokładamy tylko to, czego konta nie obejmują.

Pula 10.20.200.0/24 jest wspólna dla handlowców i administratorów, więc same hosty zaufane nie odróżnią Kasi od Tomka. O tym, kto w ogóle przejdzie uwierzytelnienie, decyduje polityka NPS z członkostwem w grupie `GG_FW_Administratorzy`.

Szkic konta jednej reguły dla wszystkich administratorów z AD (z dokumentacji Fortinet wzięliśmy konto z `wildcard` i `remote-group` [13], a składnię `config user radius` i `config user group` sprawdzamy w dokumentacji naszej wersji):

```
config user radius
    edit "RADIUS_dc02"
        set server "10.20.10.12"
        set secret HasloRadiusa
    next
end
config user group
    edit "GRP_Admini_RADIUS"
        set member "RADIUS_dc02"
    next
end
config system admin
    edit "wildcard_ad"
```

```
        set remote-auth enable
        set accprofile "NazwaProfiluAdministratora"
        set wildcard enable
        set remote-group "GRP_Admini_RADIUS"
        set trusthost1 10.20.98.0 255.255.255.0
        set trusthost2 10.20.200.0 255.255.255.0
        set trusthost3 169.254.0.0 255.255.255.0
    next
end
```

`trusthost3` z zakresem 169.254.0.0/24 dopisujemy wtedy, gdy zapora pracuje w parze: bez niego zdalny administrator z RADIUS nie wejdzie z urządzenia głównego na podrzędne poleceniem `execute ha manage` [14].

Na NPS dodajemy `fw01` jako klienta RADIUS z tym samym sekretem. W parze FortiGate dopisujemy też adres, z którego urządzenie podrzędne wysyła zapytania RADIUS, ale który to adres, sprawdzamy w dokumentacji naszej wersji, bo go nie potwierdziliśmy.

Konto awaryjne ma silne hasło, a to hasło zapisujemy w zalakowanej kopercie w sejfie, nie tylko w Vaultwardenie. Vaultwarden stoi na `docker01`, który działa za `fw01`, więc w dniu awarii zapory hasło z Vaultwardena może być nieosiągalne.

```
config system global
    set admin-restrict-local non-console-only
end
```

Od FortiOS 7.6.0 wartość `non-console-only` blokuje lokalnych administratorów w GUI i CLI, dopóki serwer RADIUS odpowiada, a konsola zostaje otwarta; wartość `all` zablokowałaby także konsolę, więc jej nie ustawiamy [12].

> ⚠ Konsolowe wejście na `fw01` wymaga fizycznego dostępu do szafy R1. Awaryjne konto sprawdzamy w oknie zmian, przez konsolę, zanim będzie potrzebne w nocy.

Interfejsy i VLAN-y Zielonej na FortiGate

FortiGate 100F ma według dokumentacji Fortinet między innymi dwa porty WAN, port MGMT, dwa porty HA, port DMZ, dwanaście portów miedzianych, cztery gniazda SFP i dwa gniazda 10G SFP+ oznaczone X1 i X2 [15]. Dwa porty SFP+ nadają się do łącza z rdzeniem, o czym piszemy

w Para FortiGate w klastrze: FGCP aktywny-pasywny. Przełączniki zostawiamy w roli L2, a każdy VLAN kończy się na `fw01` pod adresem kończącym się na .1.

Interfejs	VLAN	Adres na fw01	Strefa	Uwagi
`wan1`	nie dotyczy	203.0.113.10	strefa SD-WAN	światłowód, VPN i przekierowania portów
`wan2`	nie dotyczy	z DHCP od Starlinka, adres zmienny (w przykładach 203.0.113.30), patrz Łącza operatora	strefa SD-WAN	drugie łącze w trybie bypass, adres publiczny, ale dynamiczny
`LAG_Rdzen`	trunk	bez adresu	bez strefy	agregacja X1 i X2 do `sw01` i `sw02`, niesie VLAN-y poniżej
`VLAN10_Serwery`	10	10.20.10.1/24	`Z_SERWERY`	serwery i maszyny wirtualne
`VLAN20_Biuro`	20	10.20.20.1/24	`Z_BIURO`	przekaźnik DHCP do `dc01` i `dc02`
`VLAN30_Magazyn`	30	10.20.30.1/24	`Z_MAGAZYN`	skanery, przekaźnik DHCP
`VLAN40_Kamery`	40	10.20.40.1/24	`Z_KAMERY`	propozycja z księgi o bezpieczeństwie fizycznym, bez internetu
`VLAN98_Zarzadzanie`	98	10.20.98.1/24	`Z_ZARZADZANIE`	zarządzanie, BMC, przełączniki, `allowaccess` do administracji
`VLAN99_Goscie`	99	10.20.99.1/24	`Z_GOSCIE`	adres .1 według konwencji, do potwierdzenia; DHCP z `fw01`
`vpn_zielona_user`	nie dotyczy	pula 10.20.200.0/24	`Z_VPN`	tunel IKEv2 ze strony EAP-TLS i FSSO

Strona Przełączniki wylicza w trunku VLAN-y 10, 20, 30, 98 i 99. Kamery z VLAN 40 dochodzą z propozycji z księgi o bezpieczeństwie fizycznym, więc trunk i `LAG_Rdzen` musi nieść także VLAN 40, o czym informujemy autora bazy na końcu strony.

Szkic agregacji i jednego VLAN-u, którego składnię sprawdzamy w dokumentacji naszej wersji:

```
config system interface
    edit "LAG_Rdzen"
        set type aggregate
        set member "x1" "x2"
        set lacp-mode active
    next
    edit "VLAN98_Zarzadzanie"
        set vdom "root"
        set type vlan
        set interface "LAG_Rdzen"
        set vlanid 98
        set ip 10.20.98.1 255.255.255.0
        set allowaccess https ssh ping
        set role lan
    next
end
```

Strefy

Strefy grupują interfejsy w sposób, który odpowiada pytaniom o ruch: „biuro do serwerów”, „goście do internetu”. Strona zewnętrzna, czyli `wan1` i `wan2`, tworzy strefę SD-WAN opisaną na stronie o łączach operatora, więc w politykach nazywamy ją `ZONA_WAN` albo nazwą przyjętą w SD-WAN, a nie osobną strefą.

Strefa	Interfejsy	Ruch wewnątrz strefy
`Z_SERWERY`	`VLAN10_Serwery`	dozwolony, bo to jeden VLAN
`Z_BIURO`	`VLAN20_Biuro`	do ustalenia, domyślnie blokowany
`Z_MAGAZYN`	`VLAN30_Magazyn`	do ustalenia, domyślnie blokowany
`Z_KAMERY`	`VLAN40_Kamery`	blokowany, kamery nie rozmawiają ze sobą
`Z_ZARZADZANIE`	`VLAN98_Zarzadzanie`	dozwolony tylko dla potrzebnych usług
`Z_GOSCIE`	`VLAN99_Goscie`	blokowany, izolacja klientów
`Z_VPN`	`vpn_zielona_user`	blokowany

Interfejs, który jest już użyty w politykach, trasach albo innych obiektach, nie dołączy do strefy ani do strefy SD-WAN, dopóki nie przeniesiemy odwołań na strefę. Dlatego strefy zakładamy

przed polityką, a nie po niej. Parametr `intrazone` strefy i jego wartość domyślną sprawdzamy w dokumentacji naszej wersji.

```
config system zone
    edit "Z_SERWERY"
        set interface "VLAN10_Serwery"
        set intrazone allow
    next
end
```

Obiekty adresów i usług

Każdy adres i usługę w politykach wpisujemy jako nazwany obiekt, a nie jako liczbę wpisaną w regułę. Nazwy układamy według schematu typ, znak podkreślenia, nazwa, żeby lista była czytelna po tygodniu.

Rodzaj	Przykłady nazw w Zielonej
Adres	`ADR_fs01`, `ADR_dc01`, `ADR_sql01`, `ADR_mon01`
Sieć	`ADR_SIEC_Serwery` (10.20.10.0/24), `ADR_SIEC_Zarzadzanie` (10.20.98.0/24), `ADR_SIEC_VPN` (10.20.200.0/24)
Grupa adresów	`GRP_Domena` (`dc01` i `dc02`), `GRP_BMC`
Usługa	`USL_Syslog_Graylog` (UDP 1514), `USL_FSSO_8000` (TCP 8000), `USL_Oracle_1521` (TCP 1521)

```
config firewall address
    edit "ADR_SIEC_Zarzadzanie"
        set subnet 10.20.98.0 255.255.255.0
    next
end
config firewall service custom
    edit "USL_Syslog_Graylog"
        set udp-portrange 1514
    next
end
```

Składnię obiektów sprawdzamy w dokumentacji naszej wersji. Zmiana adresu serwera wymaga wtedy poprawki w jednym obiekcie, a nie w kilkunastu regułach.

Polityki: kolejność, implicit deny i logowanie

`fw01` przegląda polityki od góry do dołu i stosuje pierwszą, która pasuje do pakietu. Jeśli żadna nie pasuje, działa niejawna reguła blokująca (implicit deny), która domyślnie niczego nie zapisuje w logu. Numer polityki jest tylko jej identyfikatorem i nie mówi o kolejności, a kolejność widać w GUI na liście i w wyniku `show firewall policy`.

Dlatego ustawiamy w `config log setting` zapisywanie ruchu zablokowanego przez niejawną regułę [16]:

```
config log setting
    set fwpolicy-implicit-log enable
end
```

Poniższa tabela to propozycja zestawu polityk w kolejności od góry. Wszystkie wiersze są do zatwierdzenia przez autora bazy, a część pochodzi z istniejących stron.

Nazwa	Z	Do	Usługa	Profile i uwagi
`WAN-poczta-do-docker01`	strefa SD-WAN	`Z_SERWERY` (VIP poczty)	porty pocztowe	IPS, bez NAT, log pełny
`WAN-WWW-do-docker01`	strefa SD-WAN	`Z_SERWERY` (VIP WWW)	80, 443	IPS, bez NAT, log pełny
`VPN-adm-do-ZARZ`	`Z_VPN`, grupa administratorów	`Z_ZARZADZANIE`	443 i konsole BMC	wg Zdalne zarządzanie: BMC, IPMI i Redfish w osobnej sieci
`MON-do-ZARZ`	`mon01`	`Z_ZARZADZANIE`	443, UDP 623, UDP 161	z tej samej strony i z Przełączniki
`VPN-do-LAN`	`Z_VPN`, grupy FSSO	`Z_SERWERY`, `Z_BIURO`, `Z_MAGAZYN`	według grup	ze strony EAP-TLS i FSSO
`MAG-do-WMS`	`Z_MAGAZYN`	`ora01`	`USL_Oracle_1521`	log pełny
`KAM-do-mon01`	`Z_KAMERY`	`mon01`, `dc01`	HTTPS, SNMP, NTP	bez internetu, według księgi o monitoringu wizyjnym

Nazwa	Z	Do	Usługa	Profile i uwagi
`BIURO-do-WAN`	`Z_BIURO`	strefa SD-WAN	web	AV, IPS, filtr www, kontrola aplikacji, inspekcja SSL
`SERWERY-do-WAN`	`Z_SERWERY`	strefa SD-WAN	wąska lista	AV, IPS, bez inspekcji SSL
`GOSCIE-do-WAN`	`Z_GOSCIE`	strefa SD-WAN	web	filtr www, adresy prywatne zablokowane
niejawna reguła	wszystko	wszystko	wszystko	blokada, log włączony przez `fwpolicy-implicit-log`

Polityka ze strony o EAP-TLS ma `set nat enable`, czyli serwery widzą klientów VPN pod adresem `fw01`. Reguły z księgi o BMC wskazują pulę 10.20.200.0/24 jako źródło, a taka reguła potrzebuje ruchu bez NAT. Do rozstrzygnięcia przez autora bazy: według nas VPN do sieci wewnętrznej idzie bez NAT, bo bez niego w dziennikach serwerów widać prawdziwy adres z puli i da się go przypisać osobie.

Każdą politykę nazywamy, opisujemy komentarzem (po co powstała i kto o nią prosił) i włączamy logowanie `all` tam, gdzie ruch ma wartość audytową. Polityki „wszystko do wszystkiego na chwilę” nie zakładamy nawet w piątek o 16:00, bo, jak pokazuje strona o Home Assistant, „na chwilę” kończy się widocznym portem w skanie audytora.

NAT: źródłowy i adresy wirtualne

> **Pojęcie: NAT.** Tłumaczenie adresów w pakiecie przechodzącym przez zaporę. Źródłowy (SNAT) podmienia adres nadawcy, żeby odpowiedzi wracały przez zaporę, a docelowy (DNAT) podmienia adres odbiorcy, żeby ruch z internetu trafił do serwera w sieci wewnętrznej.

> **Pojęcie: VIP.** Obiekt FortiGate typu Virtual IP: opisuje zewnętrzny adres i port oraz wewnętrzny adres i port, na które ruch ma zostać przekierowany. Nie mylimy go z adresem wirtualnym keepalived z księgi o wysokiej dostępności.

Ruch wychodzący z sieci wewnętrznych do internetu przechodzi przez politykę z włączonym `nat enable`, więc wychodzi z adresem interfejsu, którym opuszcza `fw01`. Gdy SD-WAN przełączy ruch na `wan2`, adres źródłowy zmieni się na adres drugiego łącza, co zmienia też wynik wszystkich zewnętrznych sprawdzeń „skąd się łączymy”.

Ruch przychodzący z internetu rozpoznajemy po obiekcie VIP użytym jako adres docelowy w polityce. Składnia z dokumentacji Fortinet [17], z adresami Zielonej:

```
config firewall vip
    edit "VIP_poczta_smtp"
        set extip 203.0.113.10
        set extintf "wan1"
        set portforward enable
        set mappedip 10.20.10.42
        set protocol tcp
        set extport 25
        set mappedport 25
    next
end
config firewall policy
    edit 0
        set name "WAN-poczta-do-docker01"
        set srcintf "wan1"
        set dstintf "Z_SERWERY"
        set srcaddr "all"
        set dstaddr "VIP_poczta_smtp"
        set action accept
        set schedule "always"
        set service "SMTP"
        set nat disable
        set logtraffic all
    next
end
```

Przykład w dokumentacji ma `nat enable`, ale my ustawiamy `nat disable`, żeby serwer pocztowy widział adres nadawcy z internetu, a nie adres `fw01`. Poczta potrzebuje prawdziwego adresu nadawcy do oceny SPF i do ochrony przed spamem, jak opisuje strona o MailCow [18]. Nazwę interfejsu docelowego i strefę SD-WAN w polityce sprawdzamy w dokumentacji naszej wersji.

Przekierowania w Zielonej, według istniejących stron:

Port zewnętrzny na 203.0.113.10	Usługa	Cel dziś	Cel po wprowadzeniu równoważenia
25, 465, 587, 143, 993, 110, 995, 4190	poczta MailCow	`docker01`, 10.20.10.42	10.20.10.46 (adres Dockera)

Port zewnętrzny na 203.0.113.10	Usługa	Cel dziś	Cel po wprowadzeniu równoważenia
80, 443	Traefik	`docker01`, 10.20.10.42	10.20.10.66 (HAProxy)
2222	SSH do Gitea, jeśli ma być dostępne z zewnątrz	`docker01`	10.20.10.66

Cele po zmianie opisuje Keepalived i HAProxy. VPN nie potrzebuje obiektu VIP, bo tunel IKEv2 kończy się na samym `fw01`: porty UDP 500 i 4500 na `wan1` obsługuje konfiguracja tunelu, a nie przekierowanie. Od FortiOS 7.6.3 tunel IPsec może używać także TCP 443 [6]. Zielona tego nie włącza, bo port 443 zajmuje przekierowanie WWW do Traefika, więc oba użycia by się wykluczały.

Tabela dotyczy `wan1`, który ma stały adres. Na `wan2` adres jest zmienny, więc obiekt VIP związany z tym interfejsem ma zewnętrzny adres 0.0.0.0, bo przy interfejsie z DHCP Fortinet zaleca właśnie taki zapis [24], a nazwa w DNS musi podążać za adresem, jak opisuje strona Łącza operatora.

Komputery z biura używają wewnętrznych rekordów DNS wskazujących wprost na serwery, więc nie przechodzą przez adres publiczny. Gdyby jednak adres publiczny trzeba było wywołać z wnętrza sieci, `fw01` potrzebowałby przekierowania zwrotnego (hairpin), co opisuje strona o Graylogu.

Profile bezpieczeństwa

Profile bezpieczeństwa to osobne zestawy ustawień dołączane do polityki, a nie osobne reguły. Każdy profil wymaga ważnej licencji FortiGuard na urządzenie, co sprawdzamy w `System > FortiGuard`. Według oferty sprzedawcy 100F ma 1 Gb/s przepustowości przy włączonych profilach zagrożeń i 1 Gb/s przy inspekcji SSL (do potwierdzenia w karcie Fortinet), więc porównujemy te wartości z szybkością łącza operatora [15].

Profil	Co robi	Gdzie włączamy
Antywirus (AV)	skanuje pliki w przechodzącym ruchu pod kątem wirusów	`BIURO-do-WAN`, `SERWERY-do-WAN`
IPS	rozpoznaje w ruchu znane ataki i próby wykorzystania luk	wszędzie, gdzie ruch wchodzi z zewnątrz, i ruch do internetu
Filtr www	blokuje strony według kategorii	`BIURO-do-WAN`, `GOSCIE-do-WAN`
Kontrola aplikacji	rozpoznaje aplikacje niezależnie od portu	`BIURO-do-WAN`
Inspekcja SSL	odszyfrowuje HTTPS na czas kontroli, żeby profile zobaczyły treść	tylko `BIURO-do-WAN`

Tryb inspekcji (flow lub proxy) wybieramy z dokumentacją naszej wersji, zaczynając od flow. Polityki z VIP dla poczty dostają tylko IPS: filtr poczty robi MailCow, a ruch szyfrowany wchodzący do serwera nie jest odszyfrowywany.

> **Pojęcie: inspekcja SSL.** `fw01` pośredniczy w połączeniu HTTPS: z przeglądarką rozmawia certyfikatem podpisanym przez własny urząd, a ze stroną docelową zwykłym szyfrowaniem. Dzięki temu widzi treść i stosuje profile, ale przeglądarka musi ufać urzędowi, którym `fw01` podpisuje certyfikaty.

Dla Zielonej tym urzędem jest CA-Zielona z `dc01`, któremu stacje już ufają przez zasady grupy. Według Fortinet tą drogą idziemy tak: w AD CS publikujemy szablon „Subordinate Certification Authority", składamy wniosek o certyfikat podrzędnego urzędu dla `fw01`, importujemy go w `System > Certificates` i wskazujemy w profilu `ssl-ssh-profile` parametrem `caname` [19]. Szczegóły wniosku, na przykład czy klucz powstaje na `fw01`, czy na Windows, sprawdzamy w dokumentacji naszej wersji. Ten certyfikat jest inny niż certyfikat bramy VPN ze strony Błąd 13801: certyfikat bramy VPN, EKU i SAN. Po przenosinach urzędu na `ca01` urząd inspekcji nie może stać pod `Zielona-CA01`, bo ten ma długość ścieżki 0, więc dostaje certyfikat podrzędny wprost z `Zielona-Root-CA` na ceremonii, jak opisuje strona Projekt PKI Zielonej: dlaczego nie na kontrolerze, hierarchia dwupoziomowa, nazwy, ważność, CRL i AIA (tam też wariant z osobnym urzędem głównym tylko do inspekcji).

```
config firewall ssl-ssh-profile
    edit "SSL_Zielona"
        set caname "NazwaCertyfikatuPodrzednegoCA"
    next
end
```

> ⚠ Podrzędny urząd na `fw01` potrafi wystawić certyfikat dla dowolnej strony, więc kto przejmie `fw01`, przejmie zaufanie stacji. Dlatego dostęp administracyjny z poprzedniej sekcji i kopię konfiguracji (zawiera klucz) traktujemy jak klucz do urzędu certyfikacji.

Inspekcja SSL zawsze ma wyjątki. Bankowość i serwisy zdrowotne wykluczamy z odszyfrowywania, a aplikacje z przypiętymi certyfikatami (część klientów poczty i narzędzi chmurowych) przestają działać, gdy `fw01` wstawia swój certyfikat. Ustawiamy je w profilu jako wyjątki, a listę wyjątków sprawdzamy w dokumentacji naszej wersji. Zasady informowania pracowników o tym, że ruch HTTPS jest odszyfrowywany, ustala firma, nie administrator.

DHCP i DNS: fw01 czy dc01 i dc02

Domyślnie adresy i nazwy w sieciach domenowych daje Windows, a `fw01` tylko przekazuje zapytania i obsługuje sieć gości.

Sieć	DHCP	Serwery DNS dla klientów	Uwagi
VLAN 10 serwery	adresy stałe albo rezerwacje na `dc01` i `dc02`	`dc01`, `dc02`	ten sam VLAN co kontrolery, przekaźnik niepotrzebny
VLAN 20 biuro	`dc01` i `dc02` przez przekaźnik na `fw01`	`dc01`, `dc02`	według DHCP
VLAN 30 magazyn	`dc01` i `dc02` przez przekaźnik na `fw01`	`dc01`, `dc02`	zakres .100 do .200, 40 skanerów o 6:00
VLAN 98 zarządzanie	adresy stałe	`dc01`, `dc02`	BMC, przełączniki, punkty dostępowe
VLAN 40 kamery	adresy stałe, do ustalenia	brak potrzeby	bez internetu
VLAN 99 goście	serwer DHCP na `fw01`	publiczne serwery DNS, nigdy `dc01`	goście nie mogą widzieć nazw wewnętrznych

Strona o Wi-Fi mówi o DHCP na `fw01` w VLAN 30, a strona o DHCP i strona o macierzy HA o przekaźniku do `dc01` i `dc02`. Przyjmujemy wariant z przekaźnikiem, bo daje przełączanie awaryjne zakresów, i zgłaszamy rozbieżność autorowi bazy.

Serwer DHCP dla gości na `fw01` ma składnię sprawdzoną w dokumentacji Fortinet [20]:

```
config system dhcp server
    edit 1
        set interface "VLAN99_Goscie"
        set default-gateway 10.20.99.1
        set netmask 255.255.255.0
        set dns-server1 1.1.1.1
        set dns-server2 9.9.9.9
        config ip-range
            edit 1
                set start-ip 10.20.99.100
                set end-ip 10.20.99.200
            next
        end
```

```
    next
end
```

Opcja `dns-service default` z przykładu Fortinet użyłaby DNS samego `fw01`, a ten wskazuje `dc01`, więc dla gości ustawiamy serwery DNS wprost. Zakres .100 do .200 i adresy publicznych serwerów DNS są naszą propozycją, nie ustaleniem.

Sam `fw01` też pyta DNS: żeby rozwiązać `dc01.ad.zielona.example` w konfiguracji FSSO albo `bkp01` w kopii, jego systemowy DNS wskazuje `dc01` i `dc02`, a nie serwery FortiGuard. Składnię `config system dns` sprawdzamy w dokumentacji naszej wersji.

Kopia konfiguracji

Kopia konfiguracji `fw01` ma trzy poziomy: automatyczną raz na dobę, ręczną przed każdą zmianą i rewizje zapisywane przez samo urządzenie.

Poziom	Jak	Gdzie leży
Przed każdą zmianą	`execute backup config sftp` z nazwą pliku z datą i numerem zgłoszenia	`bkp01`
Automatyczna, codziennie	automation stitch: wyzwalacz harmonogramowy, akcja `cli-script` z poleceniem kopii [3]	`bkp01`
Rewizje na urządzeniu	`revision-backup-on-logout enable` zapisuje rewizję przy wylogowaniu administratora [4]	pamięć `fw01`

Szkic z dokumentacji Fortinet, z godziną i adresem Zielonej:

```
config system automation-trigger
    edit "kopia_dobowa"
        set trigger-type scheduled
        set trigger-frequency daily
        set trigger-hour 23
        set trigger-minute 58
    next
end
config system automation-action
    edit "kopia_dobowa"
        set action-type cli-script
        set script "execute backup config sftp kopie/fw01.conf bkp01.ad.zielona.example
```

```
nazwa_usera HasloUsera HasloSzyfrujace"
    next
end
```

Sam powiązujący obiekt `automation-stitch` składamy według dokumentacji naszej wersji, bo jego składnia zmienia się między wersjami [3]. Hasło konta kopii zapisane w akcji trafia do pliku kopii otwartym tekstem, więc konto na `bkp01` ma prawo tylko do jednego katalogu i działa wyłącznie z adresu `fw01`. Plik kopii zawiera także klucz podrzędnego urzędu z inspekcji SSL, dlatego szyfrujemy go hasłem i trzymamy w tej samej ochronie co kopie haseł krytycznych.

Kopię sprawdzamy przez odtworzenie. Raz na pół roku, w oknie zmian, ktoś z zespołu czyta zapisany plik i sprawdza, że zawiera politykę `VPN-do-LAN` i obiekty VIP. Nie wiemy dziś, czy kopia istnieje: macierz HA wpisuje „kopia konfiguracji do potwierdzenia”.

Aktualizacje FortiOS

Do aktualizacji dochodzi tak: najpierw sprawdzamy ścieżkę, potem robimy kopię, potem aktualizujemy w oknie, a na końcu potwierdzamy działanie.

1. W narzędziu Upgrade Path Tool wybieramy model 100F, wersję bieżącą i docelową. Narzędzie zwraca najkrótszą przetestowaną ścieżkę z numerami wydań pośrednich [21].
2. W notach wydania każdego kroku czytamy „Upgrade information” i „Known issues”, w tym wpisy o IPsec.
3. Robimy kopię ręczną i sprawdzamy `get system status` oraz licencje FortiGuard.
4. Aktualizujemy w oknie zmian, według poniższej tabeli.
5. Po aktualizacji sprawdzamy `get system status`, tunel IKEv2 z laptopem testowym, połączenie z kolektorem FSSO, przekierowania poczty i napływ logów do Grayloga.

Okno zmian opieramy na kalendarzu Zielonej.

Termin	Czy zmieniamy na fw01
ostatnie trzy dni robocze miesiąca	nie, zamknięcie miesiąca w księgowości
6:00 w Swarzędzu	nie, 40 skanerów loguje się do WMS
piątek po 15:00	nie
15 listopada do 6 stycznia	nie, zakaz zmian w infrastrukturze
wtorek po Patch Tuesday	tylko jeśli okno Windows go nie zajmuje
środa lub czwartek wieczorem, po 19:00	tak, propozycja okna

Wyjątek od zakazu zmian dla krytycznej luki w zaporze zatwierdza pan Zbigniew, to nasza propozycja do decyzji autora bazy. Aktualizacja jednego `fw01` oznacza przerwę w całym ruchu na czas restartu, bez szacunku, którego nie potwierdziliśmy. Dlatego aktualizację bez przerwy w parze opisujemy na stronie Para FortiGate w klastrze: FGCP aktywny-pasywny.

Powrót do poprzedniego obrazu umożliwia druga partycja: `diagnose sys flash list` pokazuje obrazy, a `execute set-next-reboot` wybiera, który wystartuje przy najbliższym restarcie [22].

Logi do Grayloga

100F według oferty sprzedawcy nie ma lokalnego dysku (model 101F ma SSD 480 GB) [15], więc poza krótką pamięcią urządzenia jedyną historią ruchu jest Graylog. Awaria Grayloga oznacza brak dziennika zapory, jak pokazuje scenka „Panel Zapora fw01 pokazuje zero wiadomości” na stronie Graylog: częste problemy.

Konfiguracja wysyłki, z parametrami potwierdzonymi w dokumentacji Fortinet [23], na port wejścia syslog z instalacji Grayloga:

```
config log syslogd setting
    set status enable
    set server "logi.zielona.example"
    set port 1514
    set mode udp
    set source-ip 10.20.10.1
end
```

Tryb `reliable` (TCP, RFC 6587) też istnieje [23], ale czy wejście Syslog TCP w naszym Graylogu rozpoznaje ten sposób ramkowania, sprawdzamy w dokumentacji Grayloga, zanim go włączymy. Format zostawiamy domyślny, bo reguła potoku ze strony Graylog: codzienna praca szuka w wiadomości tekstu `devname=` i rozbija pary klucz i wartość na pola `fg_*`. Adres źródłowy 10.20.10.1 to adres, który strumień `fw-zapora` już zna.

Z `fw01` wysyłamy to, co ma wartość audytową:

- ruch zablokowany, także przez niejawną regułę,
- ruch przechodzący przez przekierowania z internetu,
- zdarzenia administracyjne: logowania do `fw01`, zmiany konfiguracji, nieudane próby,
- zdarzenia VPN: zestawienie i zerwanie tunelu.

Zdarzenia z logowań administratorów dają przydatny alert w Graylogu: logowanie do `fw01` spoza VLAN 98 i puli VPN powinno wywołać wiadomość do zespołu. Panel „Zapora fw01” i strumień `fw-zapora` powstają według strony o codziennej pracy z Graylogiem. Filtr ważności i polecenie generujące wiadomość testową sprawdzamy w dokumentacji naszej wersji.

Zmiana polityki krok po kroku

1. Zapisujemy w zgłoszeniu: kto prosi, po co, na jak długo, kto zatwierdza.
2. Wybieramy okno z tabeli wyżej i robimy kopię ręczną z numerem zgłoszenia w nazwie pliku.
3. Tworzymy obiekty adresów i usług, potem politykę z nazwą i komentarzem, ustawiamy ją w odpowiednim miejscu listy.
4. Sprawdzamy `diagnose sys session list` dla ruchu testowego: numer polityki w sesji ma być naszym.
5. Sprawdzamy w Graylogu, że wiadomość z nową polityką dotarła z polami `fg_policyid` i `fg_action`.
6. Dopisujemy zmianę do dokumentacji w NetBoksie i zamykamy zgłoszenie. Tymczasowe polityki mają harmonogram wygasania, żeby nie zostały po terminie.

Częste błędy

Objaw	Przyczyna	Co robimy
Nowa polityka nic nie przepuszcza	stoi pod szerszą polityką blokującą, bo `fw01` bierze pierwszą pasującą od góry	przenosimy ją nad blokadę i sprawdzamy numer polityki w `diagnose sys session list`
Nie da się dołączyć interfejsu do strefy	interfejs jest użyty w polityce, trasie albo innym obiekcie	przenosimy odwołania na strefę albo usuwamy je, potem dołączamy interfejs
Serwer poczty widzi wszystkich nadawców pod adresem `fw01`	w polityce z VIP włączone `nat enable`	ustawiamy `nat disable` w polityce przekierowania
Wejście na `fw01` z VPN odrzucone, choć z VLAN 98 działa	adres z puli 10.20.200.0/24 poza `trusthost` albo odrzucony przez NPS	sprawdzamy `trusthost`, członkostwo w `GG_FW_Administratorzy` i polityki NPS
Administrator z RADIUS nie wejdzie na urządzenie podrzędne	brak 169.254.0.0/24 wśród `trusthost`	dopisujemy zakres i ponawiamy `execute ha manage`
Konto lokalne nie działa mimo poprawnego hasła	`admin-restrict-local` blokuje je, dopóki NPS odpowiada	wchodzimy przez konsolę albo naprawiamy NPS
Goście widzą nazwy wewnętrzne	serwer DHCP gości wydaje serwery DNS `fw01` wskazujące `dc01`	ustawiamy `dns-server1` i `dns-server2` wprost na publiczne

Objaw	Przyczyna	Co robimy
Po włączeniu inspekcji SSL aplikacja przestaje się łączyć	przypięty certyfikat albo wyjątek bankowości	dodajemy wyjątek w profilu SSL
W Graylogu brak wiadomości z `fw01`	zły adres albo port, regułą nie przechodzi ruch UDP 1514 do `docker01`	sprawdzamy `tcpdump` na hoście Grayloga według strony o częstych problemach
Po aktualizacji VPN nie wstaje	zmiana w IPsec między wydaniami albo niezgodna propozycja	czytamy znane problemy, sprawdzamy `diagnose vpn ike gateway list`, wracamy do poprzedniego obrazu

□□ Ćwiczenia

1. Polityka numer 12 przepuszcza ruch z `Z_MAGAZYN` do `ora01`, a polityka numer 3 blokuje cały ruch z `Z_MAGAZYN` do `Z_SERWERY`. Która działa i dlaczego?

Odpowiedź

Działa ta, która stoi wyżej na liście dopasowania, a numer jest tylko identyfikatorem. Jeśli blokada stoi nad regułą, ruch dopasowuje się do blokady i `fw01` nigdy nie sprawdza polityki numer 12. Przestawiamy dopuszczającą politykę nad blokadę i sprawdzamy numer polityki w sesji.

1. Dlaczego do polityki z przekierowaniem poczty ustawiamy `nat disable`, a do polityki „biuro do internetu” `nat enable`?

Odpowiedź

Przy ruchu wychodzącym adresy prywatne biura nie są routowalne w internecie, więc `fw01` podmienia adres nadawcy na własny. Przy ruchu przychodzącym do serwera pocztowego chcemy, żeby serwer widział prawdziwy adres nadawcy z internetu, bo od niego zależy ocena SPF i ochrona przed spamem. Dlatego tu źródła nie podmieniamy.

1. Skąd `fw01` wie, że ma wpuścić Tomka na konto z AD, skoro w konfiguracji jest jedno konto `wildcard_ad`?

Odpowiedź

Konto z `wildcard` i `remote-group` pasuje do każdego użytkownika, którego uwierzytelni serwer RADIUS z grupy. O tym, kto w ogóle przejdzie uwierzytelnienie, decyduje polityka NPS z członkostwem w `GG_FW_Administratorzy`. Zaufane adresy ograniczają, skąd konto może się zalogować.

1. Dlaczego kopii konfiguracji `fw01` nie traktujemy jak zwykłego pliku konfiguracyjnego?

Odpowiedź

Plik zawiera hasła i sekrety, w tym hasło konta kopii z automatu, a po wdrożeniu inspekcji SSL także klucz podrzędnego urzędu certyfikacji. Kto go przejmie, może udawać dowolną stronę HTTPS wobec stacji, które ufają CA-Zielona. Dlatego plik szyfrujemy i trzymamy z ograniczonym dostępem.

Powiązane: VPN: tunel przez cudzy internet · IPsec i IKEv2 po ludzku · EAP-TLS i FSSO · Para FortiGate w klastrze: FGCP aktywny-pasywny · Przełączniki: L2 i L3, tablica MAC, VLAN, LACP i STP · Łącza operatora · DHCP · Graylog: codzienna praca · Macierz wysokiej dostępności usług Zielonej

Źródła:

1. Technical Tip: Recommended release for FortiOS, Fortinet Community: lista zalecanych wydań, dla FortiGate 100F 7.6.6 (stan z czerwca 2026)
2. CLI troubleshooting cheat sheet, Fortinet Document Library: polecenia `get system status`, `get router info routing-table all`, `diagnose sys session`, `diagnose sniffer packet`
3. Technical Tip: How to send automated backups of the configuration with an automation stitch i Encrypted Scheduled Automatic configuration backup: składnia `execute backup config` dla FTP, SFTP i TFTP, ostrzeżenie o haśle w kopii
4. Technical Tip: How to save and restore configuration changes using revisions i Using the revision option to revert to a previous configuration: `execute revision list config`, `execute restore config flash`, `revision-backup-on-logout`
5. FortiGate / FortiOS 7.6, Fortinet Document Library: najnowsza pokazana wersja 7.6.7
6. SSL VPN tunnel mode replaced with IPsec VPN, FortiOS 7.6.4 Release Notes: od 7.6.3 dla wszystkich modeli, IPsec może używać TCP 443
7. FortiOS 8.0.0 Release Notes i Change Log: FG-100F wśród obsługiwanych modeli, wydanie 8.0.0 z 2026-04-21
8. FortiGate / FortiOS 8.0, Fortinet Document Library: najnowsza pokazana wersja 8.0.1
9. Technical Tip: Firmware release for a Mature version, Fortinet Community: znaczenie oznaczeń Feature i Mature

10. Technical Tip: System administrator best practices, Fortinet Community: `trusthost`, `admintimeout`, blokada logowania, `allowaccess`
11. Technical Tip: Limitations of trusted hosts and local-in policies i Configure local-in policy to restrict unauthorized administrative access
12. Technical Tip: Restrict local admin authentication when remote authentication server is running: `admin-restrict-local` od 7.6.0
13. Technical Tip: Overriding FortiGate administrator profiles using RADIUS authentication: konto `wildcard` z `remote-group`
14. Technical Tip: How to allow remote administrators to login to the slave unit: `trusthost` 169.254.0.0/24 i `execute ha manage`
15. FortiGate 100F and 101F fast path architecture, FortiOS 7.2.8 (lista portów) i oferta sprzedawcy datacenter360.ca (przepustowości, brak dysku w 100F), do potwierdzenia w karcie Fortinet
16. Technical Tip: How to configure the logging of Denied Traffic: `fwpolicy-implicit-log`
17. Technical Tip: Virtual IP (VIP) port forwarding configuration
18. Ta baza wiedzy: Instalacja MailCow na docker01 od zera i Keepalived i HAProxy
19. Microsoft CA deep packet inspection, FortiOS Administration Guide i Technical Tip: Issue SSL certificates with Microsoft CA for deep packet inspection: szablon Subordinate Certification Authority, `caname`
20. Technical Tip: How to configure FortiGate as DHCP server
21. Fortinet Upgrade Path Tool
22. Troubleshooting Tip: Fix an HA cluster upgrade: `diagnose sys flash list`, `execute set-next-reboot`
23. Technical Tip: How to configure syslog on FortiGate, log syslogd setting, CLI Reference i Configuring multiple Syslog servers: tryby `udp`, `reliable`, formaty
24. Technical Tip: Configuring the external IP address of a virtual server with DHCP addressing mode: VIP z adresem 0.0.0.0 na interfejsie z DHCP

Para FortiGate w klastrze: FGCP aktywny-pasywny

Poziom: średnio

Dotyczy: dwa FortiGate 100F (fw01-a i fw01-b), FortiOS 7.6 i 8.0, FGCP, rdzeń sw01 i sw02, VLAN 98

Czas: ~80 min

Jedna zapora to dziś pojedynczy punkt awarii całej Zielonej: internet, VPN handlowców, poczta i DHCP dla skanerów w Swarzędzu zależą od jednego pudełka. Ta strona opisuje, jak dwa FortiGate pracują jako jedna zapora w protokole FGCP: kto jest główny, jak urządzenia sprawdzają się nawzajem, co się dzieje z sesjami, jak okablować parę, jak ją zbudować, zaktualizować i przetestować. Wracamy tu przy zakupie drugiej sztuki, przy każdej aktualizacji pary i po każdym przełączeniu.

ZAŁOŻENIA SCENARIUSZA

zapora to para `fw01-a` i `fw01-b` w FGCP aktywny-pasywny, z rdzeniem `sw01` i `sw02` i adresem pary 10.20.98.1 w VLAN 98. Zielona ma dwa łącza: światłowód (`wan1`) i Starlink (`wan2`) z publicznym, ale zmiennym adresem, przy czym `wan2` zostaje poza monitorowaniem pary. Magazyn jest w sieci centrali (VLAN 30 na parze). Pozostałe strony zwykle przyjmują pojedynczy `fw01`: FortiGate w zarządzaniu siecią: interfejsy, VLAN-y, polityki i NAT.

Skróty użyte na tej stronie (27)

Skrót	Co znaczy
BMC	Baseboard Management Controller: osobny malutki komputer na płycie serwera, który działa nawet przy wyłączonym serwerze i odczytuje m.in. temperatury czujników
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
CRC	Cyclic Redundancy Check: suma kontrolna dopisana do odpowiedzi czujnika, dzięki której wykrywamy przekłamany odczyt
DHCP	Dynamic Host Configuration Protocol: usługa, która sama rozdaje komputerom adresy IP
FGCP	FortiGate Clustering Protocol: mechanizm Fortinet, w którym dwie zapory FortiGate działają w parze i druga przejmuje ruch, gdy pierwsza przestaje odpowiadać

Skrót	Co znaczy
FSSO	Fortinet Single Sign-On: mechanizm FortiGate, który podgląda logowania w Active Directory i sam wie, z jakiej grupy korzysta dana osoba, bez proszenia jej o dodatkowe hasło
HA	High Availability: wysoka dostępność, czyli działanie mimo awarii jednego elementu
HTTPS	HTTP zabezpieczony szyfrowaniem TLS
ICMP	Internet Control Message Protocol: protokół diagnostyczny sieci, którym działa między innymi ping
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)
IPsec	Internet Protocol Security: zestaw protokołów szyfrujących i uwierzytelniających ruch sieciowy, na nim stoi tunel VPN typu IKEv2
LACP	Link Aggregation Control Protocol: protokół z normy IEEE 802.1AX, w którym dwa urządzenia uzgadniają łączenie kilku kabli w jedno łącze logiczne; jedna sesja zostaje zawsze na jednym kablu
MAC	Media Access Control: unikalny adres fizyczny karty sieciowej, przypisany fabrycznie
MC-LAG	Multi-Chassis Link Aggregation Group: agregacja łączy do dwóch osobnych przełączników, która działa jak jeden przełącznik dla serwera
RADIUS	Remote Authentication Dial-In User Service: standardowy protokół pytania serwera, czy podane konto i hasło są poprawne
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
SMS	Short Message Service: krótka wiadomość tekstowa na telefon, która dociera także bez internetu
SPOF	Single Point of Failure: element, którego awaria zatrzymuje całą usługę, bo nie ma dla niego zamiennika
SSH	Secure Shell: szyfrowane zdalne logowanie do serwera
SSL	Secure Sockets Layer: dawna nazwa szyfrowania, dziś formalnie TLS
TCP	Transmission Control Protocol: protokół sieciowy z potwierdzaniem dostarczenia
UDP	User Datagram Protocol: szybki protokół sieciowy bez potwierdzeń
VLAN	Virtual LAN: wydzielona logicznie sieć na tym samym sprzęcie
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
WMS	Warehouse Management System: system zarządzania magazynem

Fiszka

Polecenia wykonujemy w CLI FortiOS po zalogowaniu przez SSH na adres zarządzania wybranego urządzenia (10.20.98.30 dla `fw01-a`, 10.20.98.31 dla `fw01-b`) albo na adres pary 10.20.98.1, który odpowiada na urządzeniu głównym. Składnię opatrzoną źródłem sprawdziliśmy w artykułach Fortinet; strony podręcznika `docs.fortinet.com` o konfiguracji klastra otwierały nam się w tym środowisku tylko jako spis treści [11], więc resztę sprawdzamy w dokumentacji naszej wersji FortiOS przed pierwszym użyciem.

TYLKO ODCZYT

Stan klastra: get system ha status

```
get system ha status
```

Pokazuje tryb pracy, listę członków z numerami seryjnymi, który z nich jest główny i czy konfiguracje są zgodne. Pierwsze polecenie po każdym przełączeniu, przed aktualizacją pary i po niej [3].

Przykład (poglądowy, układ pól sprawdzamy w naszej wersji):

```
HA Health Status: OK
Mode: HA A-P
Primary: fw01-a, FG100FTK20000001, HA cluster index = 0
Secondary: fw01-b, FG100FTK20000002, HA cluster index = 1
```

get = FortiOS: polecenia odczytu stanu urządzenia, na przykład get system status pokazuje wersję i numer seryjny

TYLKO ODCZYT

Porównanie konfiguracji obu urządzeń: diagnose sys ha checksum cluster

```
diagnose sys ha checksum cluster
```

Wypisuje sumy kontrolne konfiguracji każdego członka: globalną i dla domeny `root`. Różnica oznacza, że urządzenia nie są zsynchronizowane. Rozbieżną część znajdujemy poleceniem `diagnose sys ha checksum show root NazwaTabeli`, a po naprawie wymuszamy ponowne policzenie przez `diagnose sys ha checksum recalculate` [7].

diagnose = FortiOS: polecenia diagnostyczne zapory i zarządzanych przełączników, na przykład diagnose sys sdwan member pokazuje członków SD-WAN

TYLKO ODCZYT

Pełna konfiguracja HA wraz z wartościami domyślnymi: show full-configuration system ha

```
show full-configuration system ha
```

Pokazuje także ustawienia, których nie zmienialiśmy, na przykład interwał heartbeatu i margines czasu pracy. Sprawdzamy tym polecenie na obu urządzeniach, bo część ustawień HA nie synchronizuje się między nimi [3][5].

HA = High Availability: wysoka dostępność, czyli działanie mimo awarii jednego elementu · **show** = FortiOS: wypisuje konfigurację, w podstawowej postaci tylko ustawienia różniące się od domyślnych, a z wariantem full-configuration także wartości domyślne

TYLKO ODCZYT

Wejście na urządzenie podrzędne: execute ha manage

```
execute ha manage NumerUrzadzenia NazwaAdministratora
```

> (gdzie `NumerUrzadzenia` to numer członka klastra z listy podpowiedzi polecenia, a jego znaczenie sprawdzamy w dokumentacji naszej wersji; konta z RADIUS potrzebują zakresu 169.254.0.0/24 wśród `trusthost`, o czym piszemy w FortiGate w zarządzaniu siecią [12])

Otwiera sesję CLI na drugim urządzeniu z poziomu pierwszego, co przydaje się, gdy adres zarządzania podrzędnego jeszcze nie działa.

RADIUS = Remote Authentication Dial-In User Service: standardowy protokół pytania serwera, czy podane konto i hasło są poprawne · **CLI** = Command Line Interface: praca przez wpisywanie komend w terminalu · **execute** = FortiOS: polecenia, które coś wykonują na urządzeniu, na przykład execute backup config wysyła kopię konfiguracji, a execute ha manage otwiera sesję na drugiej zaporze w parze

OSTROŻNIE · NIEODWRACALNE

Ustawienie HA na jednym urządzeniu: config system ha

```
config system ha
    set group-id 1
    set group-name "fw01-klaster"
    set mode a-p
    set password HasloKlastra
    set hbdev "ha1" 100 "ha2" 50
    set session-pickup enable
    set override disable
    set priority 200
    set monitor "wan1" "LAG_Rdzen"
end
```

To ustawienia `fw01-a` (priorytet 200). Na `fw01-b` identyczne są `group-id`, `group-name`, `mode`, `password` i `hbdev`, a `priority` wynosi 100. Włączenie HA zmienia adresy MAC interfejsów na wirtualne (sprawdzamy w dokumentacji naszej wersji), więc na chwilę przerywa ruch, a urządzenie o niższej randze dostaje konfigurację od drugiego i traci własną. Dlatego robimy to w oknie zmian i w kolejności z sekcji o budowie pary, nie na działającej zaporze w środku dnia. Składnię `hbdev` z priorytetami i `monitor` potwierdzają artykuły o heartbeatach i wyborze urządzenia głównego [4][5], a nazwę interfejsu `LAG_Rdzen` w `monitor` oraz zachowanie agregacji sprawdzamy w dokumentacji naszej wersji.

HA = High Availability: wysoka dostępność, czyli działanie mimo awarii jednego elementu · **MAC** = Media Access Control: unikalny adres fizyczny karty sieciowej, przypisany fabrycznie

ZMIENIA SYSTEM

Zarezerwowany interfejs zarządzania: ha-mgmt-status

```
config system ha
    set ha-mgmt-status enable
    config ha-mgmt-interface
        edit 1
            set interface "mgmt"
            set gateway 10.20.98.1
        next
    end
end
config system interface
```

```
    edit "mgmt"
        set ip 10.20.98.30 255.255.255.0
    next
end
```

Pierwszy blok jest wspólny dla pary. Drugi, z adresem interfejsu `mgmt`, ustawiamy osobno na każdym urządzeniu: 10.20.98.30 na `fw01-a`, 10.20.98.31 na `fw01-b` [1]. Jak zrobić to tak, żeby synchronizacja nie nadpisała adresu drugiej sztuki, sprawdzamy w dokumentacji naszej wersji. Uwaga na podsieć: Fortinet zaleca dla tego interfejsu podsieć inną niż ta, w której pracuje para [1], a nasze adresy leżą w tej samej podsieci 10.20.98.0/24 co interfejs `VLAN98_Zarzadzanie`. Opisujemy to w sekcji o nazwach i adresach.

□□ ZMIENIA SYSTEM

Kontrolowane przełączenie: diagnose sys ha reset-uptime

```
diagnose sys ha reset-uptime
```

Wykonane na urządzeniu głównym zeruje jego licznik czasu pracy w klastrze, więc przy wyłączonym `override` rolę głównego przejmuje drugie urządzenie [6]. W FortiOS od 7.4.0 jest też wariant `diagnose sys ha reset-uptime-primary-only`, który działa tylko na urządzeniu głównym, więc nie pomylimy sztuk [6]. Sesje bez session pickup zostaną zerwane, więc robimy to w oknie zmian.

□□ **diagnose** = FortiOS: polecenia diagnostyczne zapory i zarządzanych przełączników, na przykład diagnose sys sdwan member pokazuje członków SD-WAN

□□ ZMIENIA SYSTEM

Aktualizacja pary: upgrade-mode

```
config system ha
    set upgrade-mode uninterruptible
end
```

Od FortiOS 7.4.1 tryb aktualizacji pary ustawia `upgrade-mode` z wartościami `simultaneous`, `uninterruptible`, `local-only` i `secondary-only`; wcześniej był parametr `uninterruptible-upgrade` [2]. Wartości domyślnej nie potwierdziliśmy, więc ustawiamy ją jawnie i sprawdzamy `show full-configuration system ha`.

Z życia wzięte

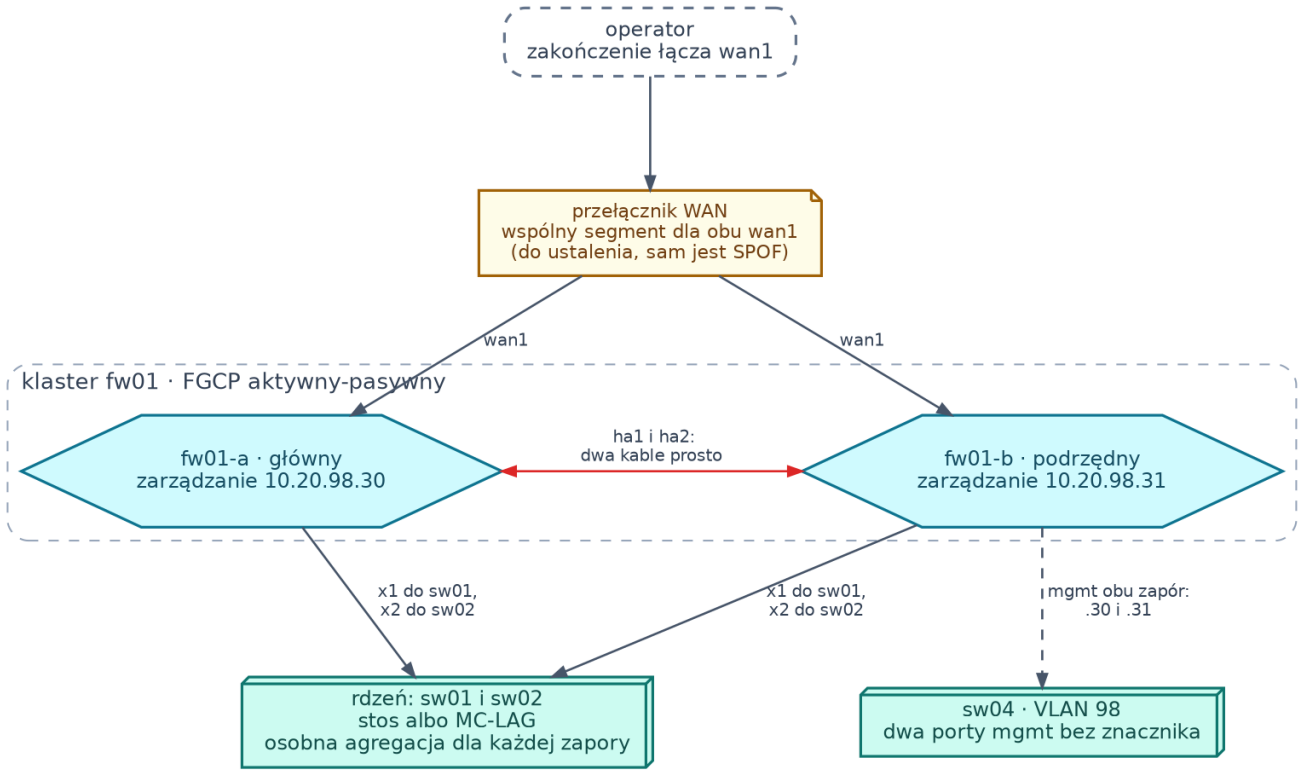
Z ŻYCIA WZIĘTE

Wtorek, 2:40. Zabbix wysyła SMS: `fw01-a` nie odpowiada na ping. Nikt w firmie nie budzi się od tego, bo VPN handlowców i poczta działają dalej: `fw01-b` przejął rolę głównego i odebrał ruch. Rano Tomek wchodzi na adres 10.20.98.1, w `get system ha status` widzi `fw01-b` jako głównego i tylko jednego członka na liście, a po zalogowaniu na konsolę uszkodzonej sztuki znajduje padnięty zasilacz. Zgłasza naprawę, wpisuje wydarzenie do dziennika zmian i nie zmienia ról w ciągu dnia: powrót `fw01-a` na stanowisko głównego zaplanuje na wieczorne okno.

Jak to działa

Rozwiń: jak to działa pod spodem

FGCP (FortiGate Clustering Protocol) to protokół, którym dwa FortiGate rozmawiają ze sobą kablami heartbeat, żeby pracować jak jedno urządzenie: mają wspólne adresy IP i wirtualne adresy MAC na interfejsach, jedno z nich obsługuje ruch, a drugie kopiuje jego konfigurację i czeka. W Zielonej para zastępuje dzisiejsze `fw01`: nazwa `fw01` zostaje nazwą pary, a pojedyncze sztuki nazywamy `fw01-a` i `fw01-b`.



Rysunek 1. Para fw01-a i fw01-b: dwa kable heartbeat prosto między sztukami, osobne łącza X1 i X2 każdej sztuki do sw01 i sw02, porty zarządzania obu sztuk w sw04. Warto zauważyć, że przełącznik WAN po stronie operatora sam jest pojedynczym punktem awarii. (kliknięcie otwiera pełny rozmiar)

Pojęcie: FGCP. Protokół klastrowy FortiGate (FortiGate Clustering Protocol). Dwa urządzenia tego samego modelu z tą samą wersją FortiOS udają jedno, a administrator widzi jedną konfigurację.

Pojęcie: heartbeat. Pakiety, którymi urządzenia klastra co chwilę sprawdzają, czy drugie żyje, i wymieniają stan: dane o konfiguracji, sesjach i interfejsach. Idą osobnymi kablami między dedykowanymi portami HA, nie przez sieć użytkowników.

Pojęcie: urządzenie główne i podrzędne (primary i secondary). Główne obsługuje ruch i jest źródłem konfiguracji. Podrzędne dostaje od niego kopię konfiguracji, a ruch przejmuje, gdy główne zawiedzie. Starsze materiały Fortinet używają słów „master” i „slave”.

Tryb: aktywny-pasywny czy aktywny-aktywny

Cecha	Aktywny-pasywny (a-p)	Aktywny-aktywny (a-a)
Kto obsługuje ruch	tylko główne	oba, ale z zasady rozkładane są tylko sesje wymagające inspekcji treści (UTM) [9]
Co dodatkowo rozkładamy	nic	opcją `load-balance-all` także sesje TCP, opcją `load-balance-udp` także UDP; ICMP, multicast i broadcast nie są rozkładane nigdy [9]
Przepustowość	jak jedna sztuka	zysk tylko tam, gdzie liczy się inspekcja; dla zwykłego TCP i UDP rozkładanie kosztuje narzut [9]
Złożoność	mała	większa: dwa urządzenia naraz przetwarzają ruch, trudniej szukać błędu
Dla Zielonej	proponujemy	nie, dopóki jedna sztuka wystarcza z inspekcją

Zielona ma około 180 osób i jeden operator łącza, więc para ma dać ciągłość, a nie dwukrotną moc. Proponujemy tryb aktywny-pasywny, zgodny z Macierz wysokiej dostępności usług Zielonej. To decyzja autora bazy.

Heartbeat: jak urządzenia sprawdzają się nawzajem

Minimum to jeden interfejs heartbeat, maksimum osiem, a domyślnie większość modeli ma dwa [4]. Interfejs heartbeat nie może być podinterfejsem VLAN, tunelem IPsec, interfejsem redundantnym ani agregacją 802.3ad [4], więc `ha1` i `ha2` w 100F to zwykłe porty fizyczne, a nie część `LAG_Rdzen`. Priorytet każdego heartbeatu (`hbdev`) mieści się w przedziale od 0 do 512, wyższy znaczy preferowany, a domyślnie jest 50 [4]. Domyślnie `hb-interval` wynosi 2 jednostki po 100 ms, a `hb-lost-threshold` 6 pakietów, więc zniknięcie partnera uznajemy po około 1,2 sekundy [4].

Kable heartbeat prowadzimy bezpośrednio między sztukami, bez przełącznika: żaden przełącznik nie psuje wtedy ramek heartbeatu. Fortinet ostrzega, że sprzęt pośredni musi przepuszczać ramki warstwy 2 z typami Ethernetu 0x8890, 0x8891 i 0x8893, a niektóre

przełączniki (jako przykład podano Cisco Nexus) zgłaszają przy nich błędy CRC [4]. Bezpośredni kabel nas z tego zwalnia.

> ⚠ Nie wyjmujemy obu kabli heartbeat naraz w pracującej sieci. Każda sztuka uzna wtedy, że druga zniknęła, i obie spróbują być główne. Taki stan nazywamy podziałem klastra (split brain). Dlatego w teście przełączenia odłączamy tylko jeden kabel.

Które urządzenie jest główne

Wybór zależy od ustawienia `override`. Przy wyłączonym `override` kolejność kryteriów to: liczba działających monitorowanych interfejsów, czas pracy w klastrze, priorytet, numer seryjny. Przy włączonym `override` priorytet wchodzi przed czas pracy: monitorowane interfejsy, priorytet, czas pracy, numer seryjny [5]. Jeśli różnica czasu pracy jest mniejsza niż `ha-uptime-diff-margin` (domyślnie 300 sekund), czas pracy jest pomijany i rozstrzyga priorytet [5].

Każdy restart urządzenia i każda awaria monitorowanego interfejsu zeruje jego „wiek” w klastrze [5], dlatego po restarcie głównego rolę zwykle przejmuje drugie urządzenie i je zostawiamy w tej roli.

Proponujemy `override disable`. Przy włączonym `override` naprawione `fw01-a` wracałoby na głównego samo, w środku dnia, a to drugie przerwanie sesji bez naszej decyzji. Przy wyłączonym wybieramy moment sami poleceniem `diagnose sys ha reset-uptime` [6]. Cena jest taka, że po awarii role zostają odwrócone, aż je zamienimy, co dla sieci nie ma znaczenia, a dla porządku w dokumentacji ma, więc zapisujemy to w dzienniku zmian. Priorytety 200 i 100 zostają jako wskazówka przy remisie i przy równym czasie pracy. `override` i priorytet nie synchronizują się między sztukami, więc ustawiamy je ręcznie na każdej [5].

Monitorowane interfejsy

Interfejs monitorowany to taki, którego zniknięcie zmienia wybór głównego: sztuka z większą liczbą działających monitorowanych interfejsów wygrywa [5]. Dla `fw01` proponujemy monitorować `wan1` i `LAG_Rdzen`. `wan2` zostawiamy poza monitorowaniem, bo drugie łącze obsługuje SD-WAN ze strony Łącza operatora, a utrata łącza zapasowego nie powinna zmieniać roli sztuk.

Monitorowanie pomaga tylko wtedy, gdy awaria jest lokalna: wyrwany kabel, martwy port, awaria przełącznika. Gdy pada łącze u operatora, obie sztuki tracą `wan1` tak samo i przełączenie niczego nie naprawi. Agregacja `LAG_Rdzen` wypada z gry dopiero wtedy, gdy nie

działa żaden jej port (minimalną liczbę łączy sprawdzamy w dokumentacji naszej wersji), więc wyrwanie jednego kabla do rdzenia nie przełącza pary.

Sesje i session pickup

Bez session pickup przełączenie zrywa sesje: użytkownicy przeglądarek odświeżają stronę, ale przesyłanie plików i niektóre protokoły trzeba zacząć od nowa [8]. Z włączonym session pickup urządzenie podrzędne dostaje kopię tablicy sesji, więc część sesji przeżywa przełączenie. Dotyczy to sesji, które nie przechodzą przez inspekcję treści [8]. Sesje UDP i ICMP wymagają osobnej opcji (`session-pickup-connectionless`, składnię sprawdzamy w dokumentacji naszej wersji).

Cena to większy ruch na kablach heartbeat. Fortinet radzi wtedy włączyć `session-pickup-delay`, który ogranicza synchronizację do sesji trwających dłużej niż chwilę, oraz wydzielić interfejs do synchronizacji sesji (`session-sync-dev`) zamiast dzielić go z heartbeatem [8]. W Zielonej w pierwszym kroku zostajemy przy dwóch kablach heartbeat, bo ruch jest umiarkowany, a ewentualne wydzielenie interfejsu planujemy po obserwacji.

Co to znaczy dla Zielonej: sesje skanerów do WMS to zwykły TCP bez inspekcji treści, więc powinny przeżyć przełączenie. Sesje przeglądarek w polityce z inspekcją SSL z FortiGate w zarządzaniu siecią prawdopodobnie nie. Czy tunele IKEv2 handlowców przeżywają przełączenie bez ponownego połączenia, sprawdzamy w teście, a nie zakładamy.

Synchronizacja konfiguracji

Konfigurację zmieniamy tylko na urządzeniu głównym, a pary dbają o resztę. Nie synchronizują się między innymi nazwa urządzenia, priorytet i `override` [5][8], a adres zarezerwowanego interfejsu zarządzania ustawiamy osobno na każdej sztuce [1]. Fortinet zaleca też, żeby sztuki miały różne nazwy hosta przed utworzeniem klastra [8], stąd `fw01-a` i `fw01-b`. Jeśli reguły Grayloga albo Zabbixa szukają `devname=fw01`, poprawiamy je tak, żeby obejmowały obie nazwy.

Zgodność konfiguracji sprawdzamy poleceniem `diagnose sys ha checksum cluster` [7].

> □□ Para nie jest kopią zapasową. Błędna reguła dodana na głównym trafia na podrzędne w tej samej chwili, więc zmiany nadal robimy według procedury z FortiGate w zarządzaniu siecią: kopia pliku przed zmianą, wpis w dzienniku zmian, test po zmianie.

Wymagania i licencje

Obie sztuki muszą być tym samym modelem (100F) i pracować na tej samej wersji i kompilacji FortiOS, a przed dołączeniem drugiej sztuki aktualizujemy ją do wersji pierwszej. Każda sztuka ma własną rejestrację i własne licencje, według Macierz wysokiej dostępności usług Zielonej potrzebne na obie. Tu zapisujemy tylko, że te licencje istnieją i są osobne dla obu urządzeń; warianty i ceny wybiera i płaci pan Zbigniew, a dokładny zakres wymagań sprawdzamy w dokumentacji naszej wersji.

Nazwy i adresy w Zielonej

Element	Wartość	Uwagi
Nazwa pary	`fw01`	tak jak w całej bazie
Urządzenie główne	`fw01-a`, priorytet 200	dzisiejsza zapora produkcyjna
Urządzenie podrzędne	`fw01-b`, priorytet 100	nowa sztuka
`group-name` i `group-id`	`fw01-klaster`, 1	`group-id` zmienia wirtualne adresy MAC, więc dwa klastry w jednym segmencie L2 muszą mieć różne (sprawdzamy w dokumentacji naszej wersji)
Adres pary w VLAN 98	10.20.98.1	odpowiada urządzenie główne
Zarządzanie `fw01-a`	10.20.98.30	port `mgmt` do sw04
Zarządzanie `fw01-b`	10.20.98.31	port `mgmt` do sw04
Adres publiczny	203.0.113.10 na `wan1`	wspólny dla pary, zmienia właściciela przy przełączeniu

Sprawdziliśmy po całej bazie, że adresy 10.20.98.30 i 10.20.98.31 nie występują nigdzie poza tą stroną. Są wolne, ale zwracamy uwagę na regułę z Zdalne zarządzanie serwerem: BMC: karta BMC ma w VLAN 98 ten sam ostatni oktet co serwer w VLAN 10. Serwer `sql01` ma adres 10.20.10.31, ale jest maszyną wirtualną, więc BMC nie ma. Gdyby jednak kiedyś pojawił się fizyczny serwer pod adresem 10.20.10.30 albo 10.20.10.31, jego BMC trafiłoby pod adres zarządzania jednej z zapór. Proponujemy zapisać w NetBoksie oba adresy jako zarezerwowane dla `fw01-a` i `fw01-b`.

> ⚠ **Decyzja do rozstrzygnięcia na początku.** Adresy .30 i .31 leżą w tej samej podsieci 10.20.98.0/24, w której działa interfejs `VLAN98_Zarzadzanie`

> pary (10.20.98.1). Fortinet zaleca dla zarezerwowanego interfejsu zarządzania podsieć inną niż podsieć dostępu do klastra [1]. FortiOS zwykle nie pozwala mieć dwóch interfejsów w tej samej domenie z nakładającymi się podsieciami. Czy zarezerwowany interfejs zarządzania, który pracuje we własnej domenie `vsys_hamgmt`, nakładanie dopuści, sprawdzamy w dokumentacji naszej wersji i w teście na sprzęcie, zanim ułożymy kable. Jeśli nie, mamy dwie drogi: osobna podsieć zarządzania urządzeń (propozycja do decyzji autora bazy, która zmienia adresy .30 i .31) albo rezygnacja z zarezerwowanego interfejsu i wchodzenie na podrzędne poleceniem `execute ha manage`. Pozostaje też ryzyko, że ta sama domena rozgłoszeniowa dochodzi do `fw01` dwiema ścieżkami: przez `LAG_Rdzen` i przez port `mgmt` w sw04.

Na politykę dostępu z VPN administratorów do VLAN 98 (opisaną w Zdalne zarządzanie serwerem: BMC) dopisujemy adresy .30 i .31 jako cel SSH i HTTPS, bo ruch z puli 10.20.200.0/24 do zarządzania urządzeniem podrzędnym przechodzi przez urządzenie główne.

Okablowanie

Skład szafy R1 opisuje Przełączniki: L2 i L3, tablica MAC, VLAN, LACP i STP: `fw01` łączy się z rdzeniem agregacją dwóch łączy 10G, a sw04 zbiera zarządzanie. Przy parze dochodzą kable drugiej sztuki.

Połączenie	Kabel	Uwagi
`fw01-a` `ha1` do `fw01-b` `ha1`	bezpośredni, krótki	pierwszy heartbeat
`fw01-a` `ha2` do `fw01-b` `ha2`	bezpośredni, krótki	drugi heartbeat
`fw01-a` `X1` do sw01, `X2` do sw02	światłowód lub DAC 10G	osobna agregacja LACP tej sztuki
`fw01-b` `X1` do sw01, `X2` do sw02	jak wyżej	druga, niezależna agregacja LACP
`mgmt` obu sztuk do sw04	miedź, port dostępowy VLAN 98 bez znacznika	zarezerwowany interfejs zarządzania
`wan1` obu sztuk	do wspólnego segmentu warstwy 2 z łączem operatora	wymaga małego przełącznika albo konwertera z dwoma portami po stronie zapór
`wan2` obu sztuk	jak wyżej, dla drugiego łącza	według Łącza operatora

Fortinet zaleca, żeby przy agregacji do dwóch przełączników każda sztuka klastra aktywno-pasywnego miała po stronie przełącznika własną grupę LACP [8][10]. Czy dwie osobne grupy

działają przy stosie albo MC-LAG, które wybierzemy w rdzeniu, sprawdzamy w dokumentacji przełączników i w teście, patrząc w tablicę MAC, czy wirtualny adres MAC zapory nie „skacze” między grupami. Dla pary potrzebujemy w rdzeniu czterech portów 10G dla zapór: dwóch w sw01 i dwóch w sw02.

Dwie rzeczy z tabeli są nowe w stosunku do opisu jednej zapory. Po pierwsze, `wan1` obu sztuk musi trafić do tej samej sieci warstwy 2 u operatora, więc potrzebny jest mały przełącznik albo urządzenie z dwoma portami po stronie zapór, a on sam jest nowym pojedynczym punktem awarii. Po drugie, wiele łączy operatorskich wiąże adres MAC urządzenia po stronie klienta, więc przed uruchomieniem pary pytamy operatora, czy wirtualny MAC zapory mu nie przeszkodzi.

Budowa pary krok po kroku

Pierwszy raz robimy to w oknie zmian z kalendarza z FortiGate w zarządzaniu siecią, czyli w środę albo czwartek po 19:00, nie w ostatnich trzech dniach roboczych miesiąca, nie w piątek po 15:00 i nie między 15 listopada a 6 stycznia.

1. Robimy kopię konfiguracji `fw01` ręcznie, na bkp01, i zapisujemy jej nazwę w dzienniku zmian.
2. Wpisujemy w NetBoksie `fw01-a` i `fw01-b`, adresy .30 i .31 i kable z tabeli powyżej.
3. Aktualizujemy `fw01-b` do tej samej wersji i kompilacji co `fw01-a` (`get system status` na obu) i nadajemy mu nazwę `fw01-b`. Nowa sztuka na tym etapie nie ma jeszcze kabli do rdzenia ani do operatora.
4. Na `fw01-b` ustawiamy HA z priorytetem 100, a na `fw01-a` HA z priorytetem 200, według bloku `config system ha` z Fiszki. Hasło klastra zapisujemy w Vaultwardenie i w zalakowanej kopercie obok hasła konta awaryjnego opisanego w FortiGate w zarządzaniu siecią, bo przy awarii `fw01` Vaultwarden bywa nieosiągalny.
5. Łączymy kable `ha1` i `ha2` oraz porty `mgmt`. Sprawdzamy `get system ha status` na obu: `fw01-a` ma być głównym, a `diagnose sys ha checksum cluster` ma pokazywać zgodne sumy.
6. Ustawiamy zarezerwowany interfejs zarządzania i adresy .30 oraz .31 po rozstrzygnięciu kwestii podsieci z sekcji o adresach. Sprawdzamy, że oba adresy odpowiadają z VPN administratorów.
7. Dopiero teraz podłączamy kable `X1`, `X2` i `wan1` drugiej sztuki. Przy rozłączonych portach danych nowa sztuka ma mniej działających monitorowanych interfejsów, więc nie wygra wyboru głównego [5].
8. Wykonujemy test przełączenia z następnej sekcji i dopiero po nim kończymy okno.
9. Aktualizujemy dokumentację: wiersz w macierzy HA, NetBox, reguły Grayloga i Zabbixa dla dwóch nazw.

Kolejność kroków 4 i 7 ma jeden powód. Sztuka, która przegra wybór głównego, dostaje konfigurację od wygranej i własną traci. Gdyby czysta fabrycznie `fw01-b` została głównym, na `fw01-a` zostałaby domyślna konfiguracja zamiast produkcyjnej. Przed krokiem 5 nic nie robimy, dopóki nie mamy świeżej kopii z kroku 1.

Aktualizacja pary bez przerwy

Dla pary ustawiamy `upgrade-mode uninterruptible`, co od FortiOS 7.4.1 zastąpiło parametr `uninterruptible-upgrade` [2]. Przy takim trybie kolejność jest następująca [3]:

1. Wgrywamy obraz FortiOS na urządzenie główne.
2. Główne wypycha obraz na podrzędne.
3. Podrzędne aktualizuje się pierwsze i restartuje, potem wysyła potwierdzenie do głównego.
4. Główne aktualizuje się i restartuje, a w tym czasie podrzędne przejmuje rolę głównego i ruch.
5. Pierwotne główne wraca do klastra już na nowej wersji. Czy znów będzie głównym, zależy między innymi od czasu pracy w klastrze i od `override` [3].

Nazwa „bez przerwy” opisuje zamiar, a nie gwarancję: w chwili przełączenia sesje bez session pickup są zrywane, więc okno zmian zostaje takie jak w tabeli z FortiGate w zarządzaniu siecią, a ścieżkę aktualizacji sprawdzamy w Upgrade Path Tool. Czasu przerwy nie szacujemy, tylko mierzymy w pierwszym oknie (sekcja o teście). Postęp aktualizacji śledzimy poleceniem `get system ha status`, a diagnostykę zaawansowaną opisuje artykuł [3]. Gdy chcemy najpierw przetestować nową wersję na jednej sztuce, tryby `secondary-only` i `local-only` aktualizują tylko wybrane urządzenie, a przełączamy się ręcznie [2].

Po aktualizacji sprawdzamy to samo co przy jednej zaporze: `get system status`, tunel IKEv2 z laptopem testowym, kolektor FSSO, przekierowania poczty i logi w Graylogu.

Test przełączenia

Test robimy po zbudowaniu pary i po każdej większej zmianie, w oknie zmian, z laptopem w VLAN 20 i działającym `ping -t` do adresu 8.8.8.8 i do `ora01`, żeby widzieć, ile odpowiedzi zginęło. Liczby zapisujemy w dzienniku zmian; nie podajemy ich tu z góry, bo zależą od naszego sprzętu.

Test	Jak	Czego oczekujemy	Co zapisujemy
Kontrolowane przełączenie	`diagnose sys ha reset-uptime` na głównym	`fw01-b` zostaje głównym, internet działa	liczba utraconych odpowiedzi ping, czas do powrotu pracy

Test	Jak	Czego oczekujemy	Co zapisujemy
Awaria zasilania głównego	odłączamy zasilanie głównego (po uprzedzeniu Marka)	jak wyżej	jak wyżej; czy VPN laptopu testowego wrócił sam
Wyrwanie kabla `wan1` głównego	odłączamy kabel `wan1`	monitorowany interfejs zmienia wybór głównego	czas do powrotu ruchu
Wyrwanie jednego kabla `X1`	odłączamy jeden kabel do rdzenia	agregacja działa dalej, para się nie przełącza	czy cokolwiek zniknęło z ruchu
Wyrwanie jednego kabla heartbeat	odłączamy `ha1`	klaster zostaje zdrowy dzięki `ha2`	stan w `get system ha status`
Sesje	przed testem otwieramy SSH na `ora01` i transfer pliku, po teście sprawdzamy, czy trwają	SSH i TCP bez inspekcji powinny przeżyć, sesje z inspekcją nie	które sesje przeżyły

Czego nie robimy: nie wyjmujemy naraz obu kabli heartbeat (podział klastra), nie testujemy w piątek po 15:00 ani w zakazie zmian od 15 listopada do 6 stycznia, i nie testujemy o 6:00, kiedy 40 skanerów w Swarzędzu loguje się do WMS.

Inne rozwiązania: FGSP i VRRP

Obok FGCP są dwa rozwiązania, które znamy tylko z opisu i dla Zielonej nie proponujemy ich teraz.

- **FGSP (FortiGate Session Life Support Protocol).** Dwa niezależne FortiGate, z których każdy obsługuje ruch, wymieniają tylko tablicę sesji. Konfiguracji same nie synchronizują, a rozkład ruchu między nimi musi zapewnić coś poza zaporą, na przykład routing. Pasuje do sieci z kilkoma bramami, nie do jednego łącza z jednym adresem publicznym.
- **VRRP.** Protokół, w którym urządzenia dzielą wirtualny adres bramy i jedno z nich go obsługuje. Zakres przełączania obejmuje sam adres, a nie sesje ani konfigurację, więc każdą zmianę musielibyśmy robić na obu sztukach ręcznie. Wygrywa tylko tam, gdzie para ma być zbudowana z różnych urządzeń.

Dla jednej firmy z jednym łączem FGCP daje to samo, a konfigurację prowadzimy raz. Szczegóły obu rozwiązań sprawdzamy w dokumentacji naszej wersji, bo ich tu nie potwierdziliśmy.

Czego para nie chroni

Para usuwa awarię jednej zapory, ale nie usuwa pozostałych punktów z listy w Macierz wysokiej dostępności usług Zielonej.

Dalej pojedyncze	Dlaczego
Szafa R1	obie sztuki stoją w tej samej szafie, więc zasilanie szafy, zalanie czy pożar zabierają obie
UPS	według macierzy HA jest jeden UPS z torami A i B z tego samego urządzenia
Łącze operatora	jedno światłowodowe łącze i jeden adres publiczny; drugie łącze to temat SD-WAN w Łącza operatora
Przełącznik WAN	wspólny segment `wan1` obu sztuk to nowy punkt awarii
Konfiguracja	błąd w regule trafia na obie sztuki naraz, więc kopia konfiguracji jest nadal konieczna
Usługi obok zapory	kolektor FSSO i RADIUS stoją na `dc01` i `dc02`, a nie w parze

Wpis do macierzy HA

Macierz w Macierz wysokiej dostępności usług Zielonej ma dziś wiersz „Zapora, VPN i brama internetowa” z docelowym mechanizmem „druga sztuka w parze HA, tryb aktywny-pasywny (FGCP)”. Wprowadzenia zmian w tej stronie nie robimy; proponujemy autorowi bazy tę treść do wiersza i do SPOF 9.

Pole	Propozycja
Mechanizm docelowy	para `fw01-a` i `fw01-b` w FGCP aktywny-pasywny, `override disable`, session pickup, osobne licencje na obie sztuki (etap 3)
RTO / RPO	RTO 15 min zostaje górną granicą, a wartość rzeczywistą wpisujemy po pierwszym teście przełączenia; RPO 0
Strona	Para FortiGate w klastrze: FGCP aktywny-pasywny
SPOF 9	po parze zostają: jedno łącze, przełącznik WAN, szafa R1 i UPS

Częste błędy

Objaw	Przyczyna	Co robimy
Nowa sztuka przejęła ruch i zniknęła konfiguracja	wygrała wybór głównego, więc podrzędna dostała jej pustą konfigurację	przed łączeniem kabli danych sprawdzamy `get system ha status`, a przywracamy konfigurację z kopii z kroku 1
Klaster się nie tworzy	inna wersja FortiOS, inne `group-name`, `password` albo `group-id`	porównujemy `show full-configuration system ha` i `get system status` na obu sztukach
`diagnose sys ha checksum cluster` pokazuje różnice	zmiana wykonana poza urządzeniem głównym albo przerwana synchronizacja	szukamy tabeli z różnicą według [7], po naprawie wymuszamy `recalculate`
Po restarcie `fw01-a` rolę przejęło `fw01-b`	restart zeruje wiek w klastrze, a `override` jest wyłączone	zostawiamy role, a zamianę robimy poleceniem `diagnose sys ha reset-uptime` w oknie
Po awarii kabla `wan1` nic się nie przełączyło	awaria po stronie operatora, obie sztuki straciły łącze tak samo	to nie jest awaria zapory, sprawdzamy łącze i SD-WAN
Zerwane sesje po przełączeniu	brak session pickup albo sesja z inspekcją treści	sprawdzamy `session-pickup` w `show full-configuration system ha`, a aplikacje z inspekcją testujemy osobno
Przełącznik rdzeniowy widzi „skaczący” adres MAC zapory	jedna agregacja na obie sztuki albo wspólna grupa LACP	każda sztuka ma własną grupę LACP po stronie przełącznika [8][10]
Zalogowany administrator z RADIUS nie wejdzie na podrzędną	brak 169.254.0.0/24 wśród `trusthost`	dopisujemy zakres, jak w FortiGate w zarządzaniu siecią [12]
Adres .30 albo .31 odpowiada, ale nie z VPN	polityka z VPN administratorów do VLAN 98 nie obejmuje nowych adresów	dopisujemy .30 i .31 do obiektu adresowego VLAN 98
Nowa para gubi pakiety do operatora	operator wiąże adres MAC urządzenia po stronie klienta	pytamy operatora o MAC wirtualny pary przed oknem

□□ Ćwiczenia

1. Dlaczego kabli heartbeat nie prowadzimy przez przełącznik rdzeniowy, tylko bezpośrednio między `fw01-a` i `fw01-b`?

Odpowiedź

Heartbeat to ramki warstwy 2 ze specjalnymi typami Ethernetu, które muszą przejść nieruszone. Niektóre przełączniki traktują je jako błędne ramki [4]. Bezpośredni kabel usuwa to ryzyko, a awaria przełącznika nie zabiera nam jednocześnie heartbeatu i ruchu danych.

1. `fw01-a` było głównym, po restarcie jest podrzędnym, a `override` jest wyłączone. Czy to usterka?

Odpowiedź

Nie. Restart zerował wiek urządzenia w klastrze, więc przy wyłączonym `override` czas pracy wyższy ma `fw01-b`, a różnica większa niż 300 sekund rozstrzyga o wyborze [5]. Jeśli chcemy, żeby `fw01-a` wróciło na głównego, robimy to w oknie poleceniem `diagnose sys ha reset-uptime` na `fw01-b` [6].

1. Dlaczego przy dołączaniu nowej sztuki kable `X1`, `X2` i `wan1` podłączamy dopiero po utworzeniu klastra?

Odpowiedź

Przy rozłączonych portach danych nowa sztuka ma mniej działających monitorowanych interfejsów, więc nie wygra wyboru głównego [5]. Gdyby wygrała, jej pusta konfiguracja zastąpiłaby produkcyjną na drugim urządzeniu.

1. Pan Zbigniew pyta, czy dzięki parze FortiGate Zielona przeżyje awarię łącza operatora. Co odpowiadamy?

Odpowiedź

Nie. Obie sztuki dzielą to samo łącze i ten sam adres publiczny, więc awaria po stronie operatora zatrzymuje obie. Para chroni przed awarią zapory, zasilacza, portu albo kabla w rdzeniu. Na awarię łącza potrzebne jest drugie łącze z SD-WAN, o którym piszemy w Łącza operatora.

Powiązane: FortiGate w zarządzaniu siecią: interfejsy, VLAN-y, polityki i NAT · VPN: tunel przez cudzy internet · Przełączniki: L2 i L3, tablica MAC, VLAN, LACP i STP · Łącza operatora · Zdalne zarządzanie serwerem: BMC · Macierz wysokiej dostępności usług Zielonej · Graylog: codzienna praca

Źródła:

1. Technical Tip: HA Reserved Management Interface, Fortinet Community: składnia `ha-mgmt-status` i `ha-mgmt-interface`, osobny adres na każdej sztuce, zalecenie innej podsieci, brak routingu i reguł zapory

2. Technical Tip: New FGCP Cluster Upgrade Mode, Fortinet Community: `upgrade-mode` od FortiOS 7.4.1, cztery wartości
3. Technical Tip: FortiGate HA upgrade procedure and the status during the upgrade, Fortinet Community: kolejność aktualizacji pary, `get system ha status`, `show full system ha`
4. HA heartbeat and communication between cluster units, FortiOS 5.6 Handbook: liczba i rodzaje interfejsów heartbeat, priorytet `hbdev`, typy Ethernetu, `hb-interval` i `hb-lost-threshold` (starsza wersja dokumentacji, wartości domyślne sprawdzamy w naszej wersji)
5. Technical Tip: FortiGate HA primary unit selection process when override is disabled vs enabled, Fortinet Community: kolejność kryteriów, `ha-uptime-diff-margin`, reset wieku, brak synchronizacji `override`
6. Technical Tip: Restoring HA primary role after a failover using diagnose sys ha reset-uptime, Fortinet Community: `diagnose sys ha reset-uptime` i `reset-uptime-primary-only` od 7.4.0
7. Technical Tip: Troubleshooting a checksum mismatch in a FortiGate HA cluster, Fortinet Community: `diagnose sys ha checksum cluster`, `show` i `recalculate`
8. FGCP High Availability Best Practices, FortiOS 6.4 Best Practices: różne nazwy hosta, session pickup, `session-pickup-delay`, `session-sync-dev`, osobne interfejsy przełącznika na każdą sztukę (starsza wersja dokumentacji)
9. Load balancing overview, FortiOS 5.2 Help i Active-passive HA, FortiOS 5.2 Help: co rozkłada tryb aktywny-aktywny, `load-balance-all` i `load-balance-udp` (starsza wersja dokumentacji)
10. FortiGate HA with dual home L3 switches, Fortinet Community: osobna grupa LACP dla każdej sztuki (wątek forum, nie dokumentacja)
11. FortiGate / FortiOS 7.6, Fortinet Document Library i FortiGate / FortiOS 8.0: wersje 7.6.7 i 8.0.1 w dokumentacji; strony o konfiguracji klastra otwierały się tu tylko jako spis treści
12. Technical Tip: How to allow remote administrators to login to the slave unit, Fortinet Community: `trusthost` 169.254.0.0/24 i `execute ha manage`
13. Ta baza wiedzy: Macierz wysokiej dostępności usług Zielonej, Przełączniki: L2 i L3, tablica MAC, VLAN, LACP i STP, Zdalne zarządzanie serwerem: BMC