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

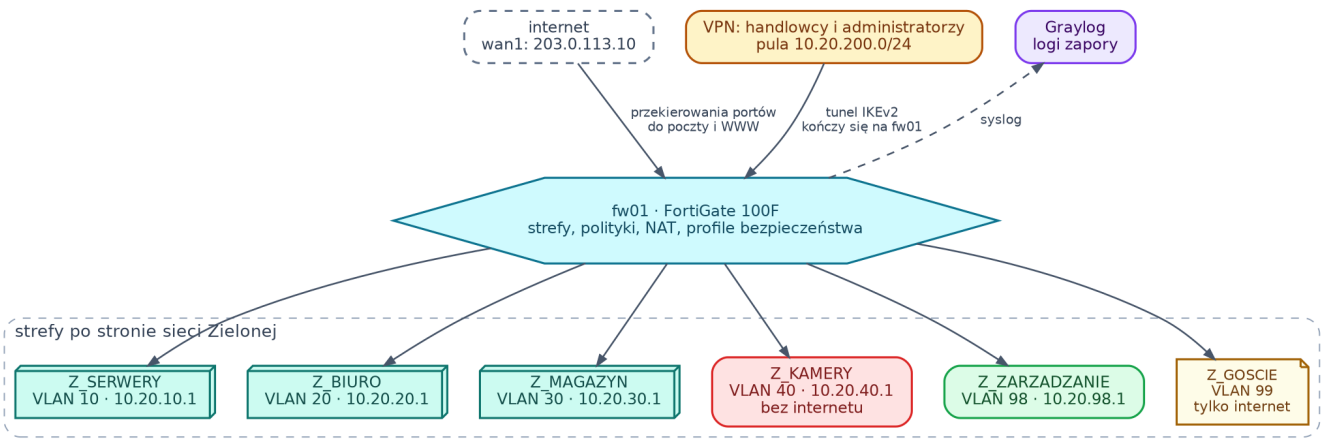
Z ŻYCIA WZIĘTE

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

Revision #12
Created 2026-10-03 19:10:51 UTC by Tomasz Konieczny
Updated 2026-10-26 14:18:15 UTC by Tomasz Konieczny