



**Poradnik konfiguracji urządzeń NGFW FortiGate
w zakresie rekomendacji Pełnomocnika Rządu do
Spraw Cyberbezpieczeństwa nr 2026/67a/6
z dnia 21.07.2026**

Praktyczne wdrożenie Rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa nr 2026/67a/6 dotyczące utrzymywania i konfiguracji urządzeń brzegowych, w oparciu o rozwiązanie FortiGate

W dniu 21.07.2026 r. Pełnomocnik Rządu ds. Cyberbezpieczeństwa wydał rekomendację nr 2026/67a/6 dotyczącą utrzymywania i konfiguracji urządzeń brzegowych, której celem jest podniesienie poziomu bezpieczeństwa systemów informacyjnych podmiotów Krajowego Systemu Cyberbezpieczeństwa (KSC). Treść Rekomendacji jest dostępna pod adresem:

<https://www.gov.pl/web/baza-wiedzy/rekomendacja-pelnomocnika-rzadu-do-spraw-cyberbezpieczenstwa-dotyczaca-utrzymywania-i-konfiguracji-urzadzen-na-styku-sieci-i-internetu>

Niniejszy poradnik został opracowany przez inżynierów firmy Fortinet i ma na celu wsparcie administratorów urządzeń FortiGate, często wykorzystywanych na styku sieci, we wdrożeniu zaleceń wymienionych w ww. rekomendacji. Poradnik uzupełniono również o dodatkowe zalecenia i dobre praktyki dotyczące bezpiecznej konfiguracji urządzeń FortiGate, oparte na oficjalnej dokumentacji Fortinet.

Poniższe rekomendacje i odnośniki do dokumentacji odnoszą się do FortiOS w wersji 7.6.7 (gałęzi 7.6). Przed wdrożeniem zaleceń opisanych w niniejszym dokumencie oraz materiałach referencyjnych należy każdorazowo zweryfikować aktualnie zainstalowaną wersję FortiOS na urządzeniu FortiGate i potwierdzić zgodność opisanych zaleceń z daną wersją oprogramowania.

Parametry konfiguracyjne, dostępność poszczególnych funkcji oraz sposób implementacji rekomendowanych ustawień mogą różnić się w zależności od platformy oraz wersji systemu FortiOS. Z tego względu przed wprowadzeniem zmian w środowisku produkcyjnym zaleca się każdorazową weryfikację konfiguracji w oparciu o oficjalną dokumentację Fortinet właściwą dla wykorzystywanej wersji systemu.

**Rekomendacja
nr 2026/67a/6**

**Praktyczne wskazówki do realizacji zaleceń na urządzeniach
brzegowych FortiGate**

1. Zarządzanie urządzeniami

“Utrzymywanie spisu urządzeń brzegowych zawierającego informacje dotyczące rodzajów urządzeń, wykorzystywanych wersji oprogramowania, skonfigurowanych połączeniach wewnętrznych i zewnętrznych między urządzeniami oraz usługach i portach udostępnionych publicznie w sieci internet”

1.1.1. Podstawowe informacje o urządzeniach, takie jak model, numer seryjny, aktywne wsparcie, można sprawdzić m.in.:

- a. Na stronie <https://support.fortinet.com> w zakładce Asset Management → Products → Product List
- b. Bezpośrednio w GUI urządzenia Dashboard → Status
- c. Z poziomu konsoli FortiManager

1.1.2. Wersję oprogramowania można sprawdzić na wiele sposobów, m.in.:

- a. Bezpośrednio w GUI urządzenia Dashboard → Status
- b. Poprzez CLI → polecenie: get system status
- c. Z poziomu konsoli FortiManager
- d. Z poziomu FortiGate Cloud

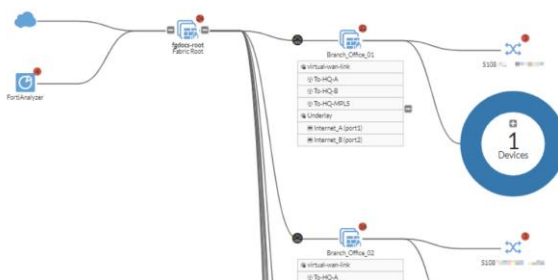
1.1.3. Rekomendowane wersje FortiOS dla poszczególnych urządzeń:

<https://community.fortinet.com/fortigate-3/technical-tip-recommended-release-for-fortios-116639>

1.1.4. Skonfigurowane połączenia wewnętrzne oraz zewnętrzne można zweryfikować w następujący sposób:

- a. Jeżeli podłączone urządzenia wspierają protokół LLDP, to informację o nich można odczytać bezpośrednio na FortiGate <https://community.fortinet.com/fortigate-3/technical-tip-use-lldp-on-fortigate-to-verify-connected-switches-210084>

- b. Topologię połączeń i rozpoznane urządzenia (w tym FortiSwitch oraz FortiAP) można wyświetlić z GUI Security Fabric → Topology



<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/118429/topology>

- c. Dobrą praktyką jest stosowanie spójnego nazewnictwa interfejsów, ich aliasów i ról oraz dodawanie komentarzy bezpośrednio w konfiguracji

<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/154471/interfaces>

- 1.1.5. Skonfigurowane usługi oraz porty dostępne publicznie można zweryfikować w następujący sposób:

- a. Zweryfikować reguły Local-in Policy bezpośrednio w GUI Policy & Objects → Local-in Policy (w przypadku braku zakładki należy ją włączyć w System → Feature Visibility)
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/363127/local-in-policy>
- b. Sprawdzić konfigurację interfejsów i uruchomionych na nich usług administracyjnych bezpośrednio w GUI Network → Interfaces:
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/574723/interface-settings>
- c. Zweryfikować skonfigurowane Virtual IPs bezpośrednio w GUI w zakładce Policy & Objects → Virtual IPs oraz ich wykorzystanie w ramach polityk Firewall:
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/443514/configuring-vips>

*“Cykliczna
aktualizacja
oprogramowania”*

- 1.2.1. Aktualizacja oprogramowania na platformach FortiGate może odbywać się zarówno automatycznie (zalecane dla nienadzorowanych środowisk) jak w sposób w pełni kontrolowany przez administratora.
- 1.2.2. W najnowszych wersjach systemu FortiOS automatyczne aktualizacje są domyślnie włączone dla wszystkich platform. Szczegółowa konfiguracja opisana jest w dokumentacji: <https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/369092/enabling-automatic-firmware-upgrades>
- 1.2.3. W przypadku aktualizacji przeprowadzanej i nadzorowanej przez Administratora urządzenia należy:
 - a. sprawdzić dostępność aktualizacji na oficjalnej stronie dedykowanej danej gałęzi oprogramowania <https://docs.fortinet.com/product/fortigate>
 - b. zweryfikować dokument Release Notes pod kątem znanych błędów, usuniętych podatności oraz ścieżki aktualizacji. Dokument Release Notes dostępny jest na stronie z dokumentacją w ramach konkretnej gałęzi oprogramowania <https://docs.fortinet.com/product/fortigate>
 - c. zweryfikować kompatybilność wersji FortiOS, np. z FortiAP, FortiSwitch, FortiExtender, FortiAnalyzer, FortiManager i innymi systemami bezpośrednio powiązanymi. Aktualizację systemów powiązanych należy wykonać zgodnie z zaleceniami dla danych systemów.
 - d. wykonać aktualizację firmware zgodnie z procedurą <https://community.fortinet.com/fortigate-3/technical-tip-how-to-upgrade-fortigate-firmware-96927>
- 1.2.4. Warto subskrybować kanał RSS z aktualizacjami firmware <https://support.fortinet.com/rss/firmware.xml>

“Wdrożenie procedur wymiany urządzeń, które przestały być rozwijane (End of Life) i dla których zakończyło się wsparcie producenta (End of Service Life)”

- 1.3.1. Informacje dotyczące cyklu życia produktu są dostępne na oficjalnej stronie Fortinet:
<https://support.fortinet.com/welcome/#/lifecycle>
- 1.3.2. Cykl życia i terminy wsparcia posiadanych urządzeń można sprawdzić bezpośrednio na swoim koncie FortiCloud
<https://docs.fortinet.com/document/forticloud/26.3.0/asset-management/472201>
- 1.3.3. Aby zapewnić nieprzerwane wsparcie techniczne oraz utrzymanie wymaganych standardów bezpieczeństwa, rekomenduje się zaplanowanie wymiany urządzeń z odpowiednim wyprzedzeniem przed terminem End of Support.
- 1.3.4. W przypadku wymiany urządzenia należy zweryfikować rekomendowane rozwiązanie zastępujące obecnie wykorzystywane oraz dopasować je do aktualnych i przyszłych potrzeb organizacji.
- 1.3.5. Warto pamiętać, że do momentu osiągnięcia przez urządzenie statusu End of Support, istnieje możliwość skorzystania z wymiany urządzeń na preferencyjnych warunkach w ramach programu TradeUp.

“Wdrożenie procedur odtworzenia infrastruktury po ataku zmniejszających ryzyko ponownego incydentu, m. in: odtworzenie nowej konfiguracji urządzenia z użyciem zweryfikowanych i niezbędnych elementów konfiguracji, bez bezpośredniego

- 1.4.1. Backup konfiguracji należy wykonywać regularnie oraz każdorazowo po zmianie konfiguracji.
<https://community.fortinet.com/fortimanager-27/technical-tip-how-to-perform-fortigate-config-backup-to-fortimanager-177262>
- 1.4.2. Proces ten może zostać zautomatyzowany za pomocą wbudowanych reguł Security Fabric → Automation
<https://community.fortinet.com/fortigate-3/technical-tip-how-to-send-automated-backups-of-the-configuration-from-a-fortigate-with-an-automation-stitch-using-tftp-ftp-or-sftp-server-and-a-recommendation-for-configuring-a-linux-machine-99783>

*kopiowania całych
bloków.*

*Weryfikacja
obecności
nieautoryzowanych
kont użytkowników.*

*Ponowna instalacja
firmware
udostępnianego
bezpośrednio przez
producenta”*

- 1.4.3. Kopie konfiguracji należy przechowywać w bezpiecznym miejscu, najlepiej w repozytorium z kontrolą dostępu. Jako repozytorium konfiguracji można wykorzystać narzędzie FortiManager.
- 1.4.4. W przypadku konieczności wdrożenia procedur odtworzenia infrastruktury po ataku należy stosować się do oficjalnych zaleceń Fortinet opisanych w poniższym artykule, który uwzględnia zalecenia zawarte w rekomendacji:
<https://community.fortinet.com/fortigate-3/troubleshooting-tip-recommended-steps-to-execute-in-case-of-a-compromised-host-118585>
- 1.4.5. W środowiskach złożonych zaleca się stosowanie systemu centralnego zarządzania FortiManager:
 - a. FortiManager przechowuje kolejne rewizje konfiguracji urządzeń oraz umożliwia ich porównywanie za pomocą funkcji Revision History / Diff, co pozwala zidentyfikować zmiany wprowadzone przed incydem i wybrać wyłącznie zweryfikowane elementy konfiguracji.
 - b. Funkcja Device Database umożliwia przygotowanie nowej konfiguracji urządzenia w centralnej bazie oraz jej kontrolowane wgrywanie na odtworzonym urządzeniu, bez konieczności bezpośredniego przywracania pełnej kopii konfiguracji.
 - c. Funkcja CLI Scripts pozwala wykonać na urządzeniu polecenia sprawdzające konta administratorów, ich uprawnienia i ustawienia dostępu oraz usunąć wykryte nieautoryzowane wpisy.
 - d. Moduł Firmware Management / Firmware Images umożliwia pobranie obrazu FortiOS z FortiGuard lub zaimportowanie zweryfikowanego obrazu producenta, a następnie jego centralną instalację na zarządzanym urządzeniu.

2. Zarządzanie dostępem

“Wyłączenie dostępu do panelu administracyjnego urządzenia bezpośrednio z sieci Internet”

- 2.1.1. Dostęp do panelu administracyjnego na interfejsach WAN należy wyłączyć w GUI Network → Interfaces
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/574723/interface-settings>
- 2.1.2. Weryfikacja aktualnej konfiguracji dostępu administracyjnego jest możliwa z poziomu widoku Local-in Policy
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/363127/local-in-policy>

„Ograniczenie dostępu zdalnego do usług urządzenia z sieci zewnętrznej do koniecznego minimum. W przypadku potrzeby ich dostępności, zabezpieczenie dostępu poprzez usługę VPN z wdrożonym mechanizmem uwierzytelniania wieloskładnikowego”

- 2.2.1. W przypadku potrzeby zapewnienia dostępu do usług urządzenia z sieci zewnętrznej należy skonfigurować dostęp z wykorzystaniem VPN (IPsec).
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/785501/forticlient-as-dialup-client>
- 2.2.2. Sposób konfiguracji uwierzytelniania wieloskładnikowego opisano w poniższym artykule:
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/419391/applying-multi-factor-authentication>

„Ograniczenie dostępu do panelu zarządzania urządzeniem jedynie z dedykowanych, wewnętrznych adresów IP (whitelisting)”

- 2.3.1. W celu ograniczenia dostępu do panelu zarządzania jedynie z określonych wewnętrznych adresów IP należy skonfigurować Stacje Zaufane (tzw. Trusted Hosts) zgodnie z poniższym artykułem:
<https://community.fortinet.com/fortigate-3/technical-tip-configuring-administrator-access-to-a-fortigate-using-trusted-hosts-93225>

*„Ustawienie
unikalnych,
bezpiecznych haseł
dla każdego
urządzenia”*

- 2.4.1. W celu wymuszenia stosowania unikalnych, bezpiecznych haseł należy skonfigurować i wdrożyć politykę haseł na urządzeniu zgodnie z poniższym artykułem:
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/364729/password-policy>

*„Wdrożenie
wieloskładnikowego
uwierzytelnienia we
wszystkich usługach i
serwisach, w których
jest to możliwe”*

- 2.5.1. FortiGate umożliwia wdrożenie różnych metod uwierzytelniania wieloskładnikowego, m.in. FortiToken, FortiIdentity Cloud, SMS, e-mail, a także rozwiązania oparte na protokołach RADIUS lub SAML.
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/14906/administrator-account-options>
- 2.5.2. FortiGate umożliwia wykorzystanie FortiToken Mobile do realizacji uwierzytelniania wieloskładnikowego. Dla wybranych modeli określona liczba tokenów jest dostępna bez konieczności zakupu dodatkowej licencji.
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/877068/registering-fortitoken-mobile>
- 2.5.3. FortiGate umożliwia wykorzystanie usługi FortiIdentity Cloud do realizacji uwierzytelniania wieloskładnikowego. W zależności od modelu i posiadanego wsparcia określona liczba użytkowników może być dostępna bez konieczności zakupu dodatkowej licencji.
<https://docs.fortinet.com/document/fortigate-cloud/latest/administration-guide/715559/forticloud-subscriptions>
- 2.5.4. Zaleca się wdrożenie centralnego systemu zarządzania tożsamością i dostępem administracyjnym, np. FortiAuthenticator lub innego rozwiązania integrującego się z urządzeniami za pośrednictwem LDAP, RADIUS, TACACS+ lub SAML.
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/14906/administrator-account-options#Using>

3. Konfiguracja

„Zapewnienie segmentacji sieci w oparciu o funkcje biznesowe oraz poziom krytyczności systemów oraz monitorowanie i filtrowanie ruchu sieciowego przekraczającego granicę segmentów”

- 3.1.1. Należy zaplanować podział sieci na segmenty funkcjonalne. W tym celu można wykorzystać np. sieci VLAN.
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/402940/vlan>
- 3.1.2. FortiGate umożliwia definiowanie i konfigurację stref bezpieczeństwa (Zone).
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/116821/zone>
- 3.1.3. Należy określić role interfejsów zgodnie z ich przeznaczeniem.
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/574723>
- 3.1.4. Ruch sieciowy pomiędzy segmentami powinien być kontrolowany i filtrowany za pomocą Firewall Policy, z zastosowaniem odpowiednich profili bezpieczeństwa, m.in. IPS, AV oraz Application Control, z włączoną deszyfracją oraz włączonym logowaniem na polityce (Log Allowed Traffic).
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/656084/firewall-policy>

„Ograniczenie dostępu do paneli administracyjnych i krytycznych systemów z sieci zewnętrznej do koniecznego minimum. W przypadku potrzeby ich dostępności, zabezpieczenie dostępu poprzez usługę VPN z wdrożonym mechanizmem uwierzytelniania wieloskładnikowego”

- 3.2.1. W przypadku potrzeby zapewnienia dostępu do usług urządzenia z sieci zewnętrznej należy skonfigurować dostęp poprzez VPN (IPsec).
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/785501/forticlient-as-dialup-client>
- 3.2.2. Sposób konfiguracji uwierzytelniania wieloskładnikowego opisano w poniższym artykule:
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/419391/applying-multi-factor-authentication>

*„Weryfikacja, czy
hasła w pliku
konfiguracyjnym
urządzenia są
przechowywane w
sposób
uniemożliwiający ich
przejęcie (z
wykorzystaniem
bezpiecznej funkcji
haszującej)”*

3.3.1. FortiGate umożliwia zabezpieczanie haseł zapisanych w pliku konfiguracyjnym z wykorzystaniem mechanizmu PBKDF2. W celu włączenia tej funkcji oraz weryfikacji poprawności konfiguracji należy postępować zgodnie z poniższą instrukcją:
<https://community.fortinet.com/fortigate-3/technical-tip-enforcing-pbkdf2-as-hash-function-for-administrator-accounts-in-fortios-v7-2-11-and-later-220652>

3.3.2. Na urządzeniach z modulem TPM (Trusted Platform Module) można rozważyć włączenie funkcji private-data-encryption:
<https://community.fortinet.com/fortigate-3/technical-tip-how-to-enable-private-data-encryption-feature-on-a-standalone-fortigate-181068>

Przed włączeniem funkcji private-data-encryption należy zapoznać się z wymaganiami i ograniczeniami, szczególnie w zakresie odtwarzania konfiguracji po awarii lub wymianie urządzenia w ramach RMA oraz współpracy z systemem centralnego zarządzania FortiManager, opisanymi w poniższej dokumentacji:

<https://docs.fortinet.com/document/fortigate/7.6.7/fortios-release-notes/335540>

<https://community.fortinet.com/fortigate-3/technical-tip-how-to-restore-a-backup-configuration-file-with-private-data-encryption-enable-97515>

<https://docs.fortinet.com/document/fortigate/7.6.0/best-practices/555436/hardening#:~:text=rma>

<https://docs.fortinet.com/document/fortimanager/7.6.7/administration-guide/30332>

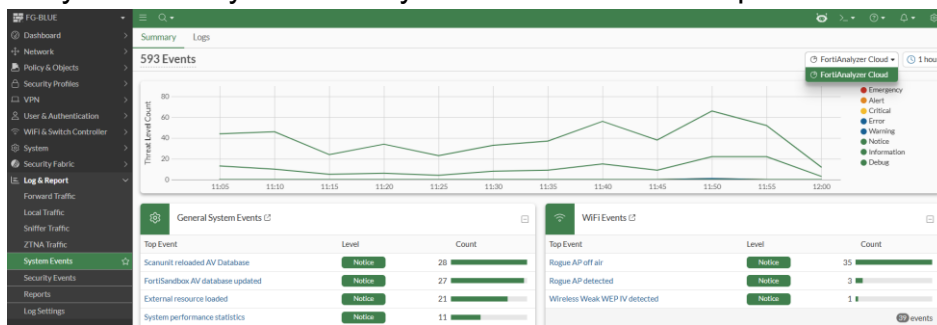
4. Monitoring

*„Cykliczna
weryfikacja kont
użytkowników i ich
uprawnień”*

- 4.1.1. Weryfikacji kont administracyjnych oraz przypisanych profili można dokonać z poziomu interfejsu GUI w zakładce System → Administrators. Konta nieużywane powinny być wyłączane administracyjnie.
- 4.1.2. Weryfikacji lokalnych kont użytkowników korzystających z usług (np. VPN) można dokonać z poziomu interfejsu GUI User & Authentication → User Definition. Konta nieużywane powinny być wyłączane administracyjnie.
- 4.1.3. Dobrą praktyką jest korzystanie z odrębnych kont imiennych dla każdego administratora lub użytkownika, umożliwiających jednoznaczną identyfikację osoby wykonującej poszczególne operacje na urządzeniu.
- 4.1.4. Zaleca się wdrożenie centralnego systemu zarządzania tożsamością i dostępem administracyjnym, np. FortiAuthenticator lub innego rozwiązania integrującego się z urządzeniami za pośrednictwem LDAP, RADIUS, TACACS+ lub SAML.
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/14906/administrator-account-options#Using>
- 4.1.5. W ramach funkcjonalności Automation Stitch należy skonfigurować scenariusz generujący powiadomienie po utworzeniu nowego konta administracyjnego lub zmianie konfiguracji istniejącego konta administratora.
<https://community.fortinet.com/fortigate-3/technical-tip-custom-automation-trigger-for-admin-user-creation-196652>

„Cykliczny monitoring
alarmów
generowanych przez
systemy
bezpieczeństwa
urządzenia”

- 4.2.1. Zdarzenia systemowe można przeglądać bezpośrednio w interfejsie GUI urządzenia FortiGate Log & Report → System Events. Można zastosować filtry i należy zwrócić uwagę na źródło danych: Memory / FortiAnalyzer / FortiGate Cloud itp.



<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/931430/system-events-log-page>

Zdarzenia można również przeglądać centralnie w systemie FortiAnalyzer, który umożliwia ich gromadzenie, filtrowanie i analizę.

- 4.2.2. Na podstawie zarejestrowanych zdarzeń możliwe jest tworzenie i automatyczne generowanie raportów cyklicznych — lokalnie na urządzeniu FortiGate (w zależności od modelu i licencji) lub centralnie w systemie FortiAnalyzer:

- Tworzenie cyklicznych raportów z poziomu FortiGate lub FortiGate Cloud Log & Report → Reports
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/279364/reports-page>
- Zarządzanie raportami w systemie FortiAnalyzer:
<https://docs.fortinet.com/document/fortianalyzer/7.6.7/administration-guide/136416/reports>

<i>„Weryfikacja poziomu logowania i ustawienie logowania dla ważnych zdarzeń m.in. logowania użytkowników, logowania VPN, logowania zmian w konfiguracji”</i>	4.3.1. Poziom logowania oraz ustawienia logowania ważnych zdarzeń na urządzeniach FortiGate można zweryfikować z poziomu GUI Log & Report → Log Settings. Zaleca się ustawienie opcji Event Logging na All. 4.3.2. Należy włączyć rejestrowanie poleceń wykonywanych przez administratorów z poziomu CLI, jak opisano w dokumentacji: https://community.fortinet.com/fortigate-3/technical-tip-enable-audit-log-via-cli-141065
<i>„Zapewnienie przekierowania logów do dedykowanego urządzenia w celu ochrony przed ich utratą”</i>	4.4.1. FortiGate umożliwia przekazywanie logów do zewnętrznych systemów, zarówno poprzez dedykowane integracje, np. z FortiAnalyzeem lub FortiGate Cloud, jak również z wykorzystaniem standardowego protokołu Syslog: a. W celu skonfigurowania przekierowania logów do systemu FortiAnalyzer należy postępować zgodnie z instrukcją w poniższej dokumentacji: https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/712303/configuring-fortianalyzer b. W celu skonfigurowania przekierowania logów do systemu FortiGate Cloud należy postępować zgodnie z instrukcją w poniższej dokumentacji, przy czym należy pamiętać, że w wersji podstawowej (darmowej) logi przechowywane są tylko przez 7 dni. https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/144076/configuring-cloud-logging c. W celu skonfigurowania przekierowania logów do innych zewnętrznych systemów przy użyciu protokołu Syslog należy postępować zgodnie z instrukcją w poniższej dokumentacji: https://community.fortinet.com/fortigate-3/technical-tip-how-to-configure-syslog-on-fortigate-177925

<i>„Regularne monitorowanie logów pod kątem wystąpienia awarii i anomalii”</i>	4.5.1. Za pomocą wbudowanych reguł Security Fabric → Automation można zautomatyzować proces powiadamiania o awariach i anomaliiach. https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/51460/actions 4.5.2. Zaleca się przekazywanie logów z urządzeń FortiGate do centralnego systemu zarządzania i analizy logów, np. FortiAnalyzer, FortiSIEM lub innego rozwiązania klasy SIEM/Log Management, w celu ich gromadzenia, analizy i korelacji. 4.5.3. Należy skonfigurować automatyczne powiadomienia dotyczące wykrytych awarii, nieprawidłowości i anomalii.
<i>„Cykliczna weryfikacja dostępnych publicznie usług i zasobów pod kątem poprawności reguł dostępowych”</i>	4.6.1. Skonfigurowane usługi oraz porty dostępne publicznie można zweryfikować w następujący sposób: - Zweryfikować reguły Local-in Policy bezpośrednio w GUI Policy & Objects → Local-in Policy (w przypadku braku zakładki należy ją włączyć w System → Feature Visibility) https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/363127/local-in-policy - Zweryfikować skonfigurowane Virtual IPs bezpośrednio w GUI w zakładce Policy & Objects → Virtual IPs oraz ich wykorzystanie w ramach polityk Firewall. https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/443514/configuring-vips 4.6.2. Cykliczną weryfikację dostępu do publicznych usług i zasobów można realizować poprzez analizę użycia polityk bezpieczeństwa. FortiGate umożliwia m.in. sprawdzenie liczby sesji i wolumenu ruchu przechodzącego przez polityki oraz utworzenie spersonalizowanych widoków FortiView dla wybranych usług. https://community.fortinet.com/fortigate-3/technical-tip-how-to-check-the-hit-count-first-hit-last-hit-and-established-session-count-for-single-or-multiple-firewall-policies-through-cli-and-gui-111903

„Regularne tworzenie kopii zapasowych konfiguracji urządzeń brzegowych oraz testowanie procedur odtwarzania po awarii”

4.6.3. Należy cyklicznie generować raporty dotyczące połączeń przychodzących na podstawie logów gromadzonych w zewnętrznym systemie zarządzania logami, np. FortiAnalyzer.

4.6.4. Regularne przeglądy poprawności i spójności polityk bezpieczeństwa można realizować z wykorzystaniem funkcji Policy Consistency Check dostępnej w systemie centralnego zarządzania FortiManager.
<https://docs.fortinet.com/document/fortimanager/7.6.7/administration-guide/233367>

4.7.1. Backup konfiguracji należy wykonywać regularnie oraz każdorazowo po zmianie konfiguracji.

4.7.2. Proces ten może zostać zautomatyzowany za pomocą wbudowanych reguł Security Fabric → Automation.
<https://community.fortinet.com/fortigate-3/technical-tip-how-to-send-automated-backups-of-the-configuration-from-a-fortigate-with-an-automation-stitch-using-tftp-ftp-or-sftp-server-and-a-recommendation-for-configuring-a-linux-machine-99783>

4.7.3. Kopie konfiguracji należy przechowywać w bezpiecznym miejscu, najlepiej w repozytorium z kontrolą dostępu. Jako repozytorium konfiguracji można wykorzystać narzędzie FortiManager.
<https://community.fortinet.com/fortimanager-27/technical-tip-how-to-perform-fortigate-config-backup-to-fortimanager-177262>

4.7.4. W przypadku konieczności wdrożenia procedur odtworzenia infrastruktury po awarii należy stosować się do oficjalnych zaleceń Fortinet opisanych w poniższym artykule:
<https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/702257>

4.7.5. W środowiskach złożonych zaleca się stosowanie systemu centralnego zarządzania FortiManager do automatyzacji wykonywania kopii konfiguracji, przechowywania ich kolejnych wersji oraz wspomagania procesu odtwarzania.

5. Fizyczne i logiczne bezpieczeństwo

„Urządzenia brzegowe powinny znajdować się w zamkniętych, monitorowanych szafach rack w pomieszczeniach z ograniczonym dostępem”

- 5.1.1. Należy ograniczyć fizyczny dostęp do urządzeń FortiGate.
- 5.1.2. Należy wyłączyć automatyczną instalację firmware FortiOS oraz automatyczne przywracanie konfiguracji z USB.
- 5.1.3. Na portach dostępowych należy stosować mechanizmy kontroli dostępu, np. 802.1X, ograniczające możliwość podłączenia nieautoryzowanych urządzeń.
<https://docs.fortinet.com/document/fortigate/7.6.0/best-practices/555436#PhysicalSec>
- 5.1.4. Należy utrzymywać poziom zabezpieczeń BIOS w trybie High (Signed Firmware), który blokuje instalację obrazów FortiOS bez prawidłowego podpisu cyfrowego Fortinet. W wybranych modelach serii G ustawienie to jest realizowane za pomocą fizycznego przełącznika na obudowie urządzenia.
<https://community.fortinet.com/fortigate-3/technical-tip-change-security-level-on-fortigate-g-series-models-202169>

„Zastosowanie redundantnych zasilaczy oraz systemów UPS”

- 5.2.1. Urządzenia wyposażone w dwa zasilacze należy zasilać z dwóch niezależnych obwodów, z czego co najmniej jeden powinien być objęty zasilaniem gwarantowanym, np. z systemu UPS.
- 5.2.2. Utrata zasilania na dowolnym obwodzie zasilającym powinna być automatycznie wykrywana i sygnalizowana z wykorzystaniem mechanizmu Automation Stitch, protokołu SNMP lub innego skonfigurowanego systemu powiadamiania.

Dobre praktyki dla FortiGate

1. Konfigurację urządzenia należy wykonywać zgodnie z zaleceniami producenta opisanymi w Hardening Guide: <https://docs.fortinet.com/document/fortigate/7.6.0/best-practices/555436/hardening>
2. Niezbędny dostęp zdalny należy ograniczyć do zaufanych adresów IP, wykorzystując funkcję Trusted Host dla dostępu administracyjnego <https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/14906/administrator-account-options>
3. W przypadku dostępu zdalnego należy skonfigurować dostęp poprzez VPN, np. IPsec z uwierzytelnianiem MFA <https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/785501/forticlient-as-dialup-client>
4. Dostęp do GUI ograniczyć regułami Local-In Policy lub poprzez dedykowany management VDOM. Policy & Objects → Local-in Policy <https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/363127/local-in-policy>
5. Ustawić limit czasu bezczynności dla administratorów na niską wartość <https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/215451/setting-the-idle-timeout-time>
6. Używać niestandardowych portów HTTPS i SSH dostępu administracyjnego System → Settings → Access <https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/616955/configuring-ports>
7. Wyłączyć obsługę słabych protokołów i algorytmów kryptograficznych. <https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/45329/tls-configuration>
8. Dla administracyjnego dostępu HTTPS należy skonfigurować zaufany certyfikat, którego nazwa FQDN lub adres IP odpowiada adresowi wykorzystywanemu do zarządzania urządzeniem. <https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/499047/using-the-default-certificate-for-https-administrative-access>
9. Wyłączyć użycie protokołów, takich jak HTTP i Telnet <https://docs.fortinet.com/document/fortigate/7.6.0/best-practices/103945/administrative-settings>
10. Zaleca się uzupełnienie mechanizmów ochrony o dane pochodzące z zewnętrznych źródeł informacji o zagrożeniach, np. listy złośliwych domen udostępniane przez CERT Polska. <https://docs.fortinet.com/document/fortigate/7.6.7/administration-guide/9463>
11. W celu szerszej analizy stanu infrastruktury zaleca się korelację logów FortiGate z logami i zdarzeniami pochodzącymi z pozostałych elementów infrastruktury IT, np. za pomocą systemu FortiSIEM.
12. Należy systematycznie aktualizować wiedzę, korzystając z oficjalnej dokumentacji <https://docs.fortinet.com/product/fortigate> oraz z dostępnych materiałów szkoleniowych <https://training.fortinet.com/>