FORCEPOINT
POWERED BY Raytheon

Karta produktu

Protecting the human point.

FORCEPOINT NGFW

Security Management Center (SMC)

SCENTRALIZOWANA ADMINISTRACJA ROZWIĄZANIAMI FORCEPOINT NGFW Z PEŁNĄ, INTERAKTYWNĄ WIDOCZNOŚCIĄ 360° DLA TWOJEJ SIECI

Rozwiązanie NGFW Forcepoint Security Management Center (SMC) to ujednolicone, scentralizowane zarządzanie wszystkimi modelami i wersjami oprogramowania zapór ogniowych nowej generacji Forcepoint (Next Generation Firewalls) - fizycznych, wirtualnych lub w chmurze - w dużych i geograficznie rozproszonych środowiskach korporacyjnych.

Dzięki doskonałej elastyczności, skalowalności i łatwości obsługi SMC sprawia, że zarządzanie dynamicznymi środowiskami zabezpieczeń sieci i wspieranie agresywnych planów rozwoju firmy jest łatwiejsze. Dzięki inteligentnym mechanizmom tego systemu procesy biznesowe prowadzone są w sposób naturalny, a zoptymalizowane funkcje przepływu pracy usprawniają codzienne zadania administracyjne, co zapewnia wysoką wydajność i niski koszt TCO.

SMC zapewnia widoczność 360° w sieciach przedsiębiorstw, zbierając informacje o zdarzeniach związanych z zarządzaniem i monitorowaniem statusu systemów NGFW Forcepoint, punktów końcowych i urządzeń innych producentów w celu przeprowadzenia interaktywnego monitorowania.

Ponadto system SMC może agregować logi NGFW z wielu rozproszonych geograficznie serwerów logów w celu wygenerowania skonsolidowanych raportów, zachowując zgodność danych z przepisami i regulacjami.

Wysoka dostępność

W dzisiejszych czasach firmy nie tolerują żadnych zakłóceń i oczekują nieprzerwanego, całodobowego dostępu do najważniejszych zasobów. Dzięki opcji wysokiej dostępności systemu SMC Forcepoint organizacje mogą zachować stały i nieprzerwany dostęp do logów w celu przeprowadzenia analizy odporności na incydenty i reagowania.

Aplikacja kliencka dla zarządzania bezpieczeństwem

Niezależnie od lokalizacji geograficznej administratorzy mogą bezpiecznie uzyskać dostęp do systemu SMC Forcepoint za pomocą aplikacji klienckiej. Klient taki udostępnia zaawansowany graficzny interfejs użytkownika przeznaczony do konfiguracji, monitorowania, logowania, przeglądania alertów, generowania raportów, aktualizacji i uaktualnień w zaporach ogniowych nowej generacji Forcepoint. Klient SMC Forcepoint dostarcza administratorom całościowego widoku sieci i pozwala na szybki, kontekstowy „drill-down" w celu łatwego i skutecznego zarządzania całym środowiskiem zabezpieczeń.

Główne korzyści

- **Jedno scentralizowane zarządzanie nawet do 2000 NGFW Forcepoint w środowiskach rozproszonych.**
- **Elastyczność i skalowalność dla wdrożeń w dużych rozproszonych środowiskach przedsiębiorstw.**
- **Wysoka dostępność dla sprostania wymaganiom dotyczącym krytycznych usług**
- **Inteligentne polityki i wydajna automatyzacja przepływu pracy w celu szybkiego i precyzyjnego wdrożenia oraz utrzymania NGFW Forcepoint.**
- **Świadomość sytuacyjna i widoczność całej sieci, od centrum danych i obrzeży sieci po oddziały firmy i chmurę.**
- **Opcja wyboru pomiędzy oprogramowaniem a rozwiązaniem typu appliance**

Specyfikacja Forcepoint NGFW Security Management Center

SERWER ZARZĄDZANIA	
Liczba obsługiwanych urządzeń	Licencja: 2 do 2000 węzłów w ramach jednego serwera zarządzania
Liczba administratorów	Bez ograniczeń
Liczba elementów	Bez ograniczeń
Liczba polityk	Bez ograniczeń
Liczba serwerów logów	Bez ograniczeń
Liczba serwerów Web Portal	Bez ograniczeń
Uwierzytelanianie administratora	Lokalna baza danych, RADIUS, TACACS+
Połączenia z innymi komponentami	Szyfrowane połączenie SSL
SERWER LOGÓW	
Liczba obsługiwanych urządzeń	Bez ograniczeń
Rekordy logów na sekundę	Wydajny system logowania może przetwarzać ponad 500 000 rekordów na sekundę
Połączenia z innymi komponentami	Szyfrowane połączenie SSL, IPv4/IPv6
Wielkość przechowywania logów	Bez ograniczeń
Liczba możliwych przekierowań logów (każdy Log Server)	Bez ograniczeń
WŁAŚCIWOŚCI	
Ogólne	
Klient zarządzania	Typu Java dla Windows i Linux i Java Web Start dla Mac
SMC Application Programming Interface (SMC API)	Udokumentowany interfejs API umożliwiający łatwą integrację produktów i usług firm zewnętrznych, wykorzystuje architekturę REST, w której dane mogą być kodowane jako XML lub JSON
Równocześni administratorzy	Kilku administratorów może wprowadzać zmiany w tym samym czasie. Krytyczne elementy, takie jak polityki, są blokowane do edycji
Dostosowywanie ekranu głównego	Łatwe opcje dostosowywania opcji monitorowania
Wysoka dostępność	Do 4 serwerów typu Standby dla Management Server
Uaktualnienia	Możliwość automatycznego pobierania aktualizacji oprogramowania oraz aktualizacji kontentu
Kopia zapasowa	Zintegrowane narzędzie do tworzenia kopii zapasowych całego systemu, w tym wszystkie konfiguracje zapory ogniowej
Nawigacja	Intuicyjna nawigacja przypominająca przeglądarkę z historią przeglądania i zakładkami
Narzędzia wyszukiwania Spotlight	Wydajne narzędzia wyszukiwania elementów i referencji z szybkimi działaniami kontekstowymi
Szybkie filtrowanie	Wygodne filtrowanie podczas wpisywania w listach elementów, tabelach i komórkach polityk
Obsługa Multi-Selection	Wykonywanie działań i potwierdzeń dokonanych zmian dla setek elementów jednocześnie
Narzędzia systemowe Clean-Up	Umożliwia administratorowi łatwe sprawdzenie nieużywanych elementów i reguł
Administracja	
Eskalacja alertów	Umożliwia administratorowi przekazywanie alertów z systemu za pomocą wiadomości e-mail, SMS, SNMP trap i niestandardowych skryptów
Progi alertów	Defniniowanie progów alertów dla statystyk
Logi audytu	Obszerne informacje audytowe o wszystkich zmianach w systemie
Raporty systemowe	Raporty dotyczące zapasów i audytu na temat działań administratorów
Instalacja Plug-and-Play	Instalacja oparta na chmurze (lub pamięci USB) z opcją „initial policy push”

Specyfikacja Forcepoint NGFW Security Management Center

Zadania zautomatyzowane	Odświeżanie polityk; archiwizacja, eksport i usuwanie logów; tworzenie kopii zapasowych
Domeny administracyjne	Możliwy podział środowiska na izolowane domeny administracyjne
Import/Export	Eksport i import XML i CSV z opcją rozwiązywania konfliktów pomiędzy instalacjami SMC
Zdalne uaktualnienia	Zdalne, bezpieczne uaktualnienia za pomocą jednego kliknięcia
Kontrola dostępu na podstawie roli administratora	Możliwość definiowania i łączenia ról dostosowywanych, dodatkowo do predefiniowanych ról, jak np. Owner, Viewer, Operator, Editor i Superuser, w celu elastycznej i dokładnej kontroli uprawnień
Zarządzanie licencją	Automatyczne aktualizacje licencji online i raporty o statusie umowy serwisowej
Zarządzanie certyfikatami	Skonsolidowany widok wszystkich certyfikatów i danych uwierzytelniających
Narzędzia Troubleshooting	Rozbudowane zdalne funkcje diagnostyczne: zintegrowane narzędzie do rejestrowania ruchu, diagnostyka, pobieranie konfiguracji (snapshot) z zapory ogniowej nowej generacji i widoki monitorowania sesji
Zarządzanie strategią	
Konteksty wirtualne	Udostępnianie kontekstu typu Master dla różnych domen administracyjnych SMC - do 250 wirtualnych kontekstów a każdy z nich ma własne polityki, tabele routingu itd.
Hierarchiczne zarządzanie strategią	Szablony polityk, sub-polityki, aliasy i sekcje komentarzy reguł sprawiają, że polityki są uporządkowane i czytelne
Identyfikacja aplikacji	Ograniczenie dostępu w oparciu o aplikacje sieciowe i/lub klienckie: • Identyfikacja aplikacji na podstawie zawartości i odpowiednie ograniczanie dostępu • Biała/czarna lista według nazwy, wersji aplikacji, podpisu cyfrowego itp. z wykorzystaniem Forcepoint Endpoint Context Agent
Zarządzanie zmianą	Wdrożenie zmian wymaga przeglądu i zatwierdzenia poprzez drugiego administratora o odpowiednich uprawnieniach
Filtrowanie adresów URL	Ograniczanie dostępu na podstawie kategorii adresów URL
Nazwy domen	Dynamicznie ograniczanie dostępu wg nazw domen
Identyfikacja użytkownika	Tworzenie reguł opartych na użytkownikach z opcją uwierzytelniania lub bez
Strefy	Fizyczne interfejsy mogą być oznaczone strefami i określane w politykach
Geo-ochrona	Ogranicza dostęp wg krajów lub regionów geograficznych
Strategie dot. kontroli	Inspekcja szczegółowa (DPI) i łatwe sposoby na wyłączenie fałszywych alarmów
Polityki Quality of Service (QoS)	Konfiguracja polityk opartych o klasy QoS
Filtrowanie plików na podstawie polityk typu anti-malware	Definiuje, w jaki sposób pliki są sprawdzane przy użyciu reputacji pliku: McAfee Global Threat Intelligence, Anti-Malware Scan lub Sandbox
Network Address Translation (NAT)	• Domyślne reguły NAT • Elementy polityki NAT
Narzędzie walidacji polityk	Pomaga administratorowi znaleźć błędy konfiguracji przed aktywacją polityki
Snapshot polityk	Umożliwia eksplorację i porównanie historii modyfikacji polityk zapory ogniowej
Przywrócenie polityki	Poprzednia wersja polityki może zostać przywrócona i przesłana do zapory ogniowej
Narzędzie Rule Usage Optimization	Umożliwia administratorom sprawdzenie, ile razy każda reguła została dopasowana w danym czasie
Narzędzie wyszukiwania reguł	Zintegrowane narzędzie do wyszukiwania reguł w politykach
Nazwy reguł	Możliwość tworzenia nazw reguł widocznych w logach, statystykach i raportach
Bezpieczne przesyłanie polityk	System automatycznie przywraca poprzednią wersję polityki, jeśli nowa wersja zawiedzie
Konfiguracja	
Trasowanie	Przeciągnij i upuść konfigurację trasowania dla zapór ogniowych i określonych widżetów, aby dodać trasy statyczne i trasy domyślne
Trasowanie dynamiczne	Zaawansowana konfiguracja OSPF i BGP za pomocą intuicyjnego graficznego interfejsu użytkownika
Automatyczny Anti-spoofing	Konfiguracja anti-spoofing jest tworzona automatycznie na podstawie trasowania

Specyfikacja Forcepoint NGFW Security Management Center

Site-to-site VPN	– IPsec VPN na podstawie polityk (policy-based) – IPsec VPN na podstawie trasy (route-based) i tunelowanie (GRE, IP-IP)
Mobilny dostęp VPN	– klient IPsec VPN (iOS i Windows) – klient SSL VPN (Android, Mac i Windows) – Clientless SSL VPN Portal
Endpoint Context Agent Management	Rozszerza kontrolę dostępu i widoczność na aplikacje działające na stacjach roboczych
Zarządzanie incydentami	Zintegrowane narzędzia do wspólnego zarządzania incydentami w sieci
Firewall Element Creation Wizard	Tworzy setki elementów zapory ogniowej za pomocą kreatora tworzenia zapory
Uwierzytelnianie użytkownika oparte na przeglądarce	Konfiguruje i dostosowuje łatwą dla użytkowników usługę uwierzytelniania opartą na przeglądarce
Status, statystyki i raportowanie	
Monitorowanie statusu systemu	Informacje o stanie w czasie rzeczywistym dotyczące urządzeń sieciowych i ich połączeń
Monitorowanie statusu urządzenia	Graficzny widok statusu urządzenia
Wykresy dot. sieci	Wizualizacja konfiguracji, topologii i łączności
Monitorowanie sesji	Dedykowane widoki do monitorowania połączeń, VPN security associations (SAs), uwierzytelnionych użytkowników, aktywnych alertów oraz dynamicznych i statycznych tras
Przegląd	Dostosowywanie paneli kontrolnych dotyczących statystyk sieci do monitorowania w czasie rzeczywistym
Geolokalizacja	Pokazuje informacje o kraju dla wszystkich adresów IP za pomocą flag krajów i statystyk geolokalizacji. Pokazuje, skąd pochodzą ataki sieciowe
Raportowanie	Dostosowuje i planuje raporty, które dostarczają szczegółowych informacji o statystykach sieci. Szczegółowe raporty o wykrywaniu złośliwego oprogramowania
Portal webowy	Łatwy dostęp do podglądu polityk, logów i raportów z podziałem na domeny za pomocą przeglądarki
Zarządzanie urządzeniami zewnętrznymi	
Monitorowanie urządzeń zewnętrznych	Umożliwia administratorowi monitorowanie i wyświetlanie zmian statusu dostępności urządzeń zewnętrznych
Log Injestion dla urządzeń zewnętrznych	Odbiór i przetwarzanie logów w formacie syslog z urządzeń zewnętrznych. Bezpośrednia obsługa formatów CEF, LEEF, CLF i WELF
Odbiór NetFlow/IPFIX	Możliwość odbierania i łączenia danych w formatach NetFlow v9 i IPFIX
Statystyki dot. urządzeń zewnętrznych	Graficzne statystyki i raporty tworzone na podstawie logów urządzeń firm trzecich, obsługa simple network management protocol (SNMP)
Liczba obsługiwanych urządzeń zewnętrznych	200 na serwer logów
Licencje	Każde urządzenie zewnętrzne zużywa 0.2 z liczby urządzeń licencjonowanych na serwerze zarządzania
Logi	
Przeglądarka logów	Szczegółowe widoki dla oddzielnych typów logów, np. VPN, filtrowanie plików i endpoint, oprócz wspólnego widoku przeglądania wszystkich logów
Filtrowanie Drag-and-Drop	Interaktywne filtrowanie logów - przeciągnij i upuść dowolną komórkę danych loga w pole typu „query"
Statystyki dot. logów	Tworzy statystyki logów w czasie rzeczywistym i obrazuje trendy
Wizualizacje logów	Znajduje anomalie w zarejestrowanym ruchu w filtrowalnych wizualizacjach logów
Agregacja logów	Agreguje dane po ich przefiltrowaniu i szereguje wg kolumn
Archiwizowanie	Archiwizuje logi w wielu katalogach z użyciem filtrowania
Backup	Zintegrowany mechanizm tworzenia kopii zapasowych dla konfiguracji Log Server'a i danych logów
Eksporty logów	Eksport loga CSV, XML, CEF, LEEF i McAfee Enterprise Security Manager; logi można eksportować do plików PDF i ZIP bezpośrednio z przeglądarki logów
Przekazywanie logów	Przekazywanie logów w czasie rzeczywistym w syslog; format CEF, LEEF, XML, CSV, IPFIX, NetFlow i McAfee Enterprise Security Manager; konfiguracja w zakresie filtrowania, typu danych; i wyboru pola loga
Konteksty przeglądania logów	Skróty do przeglądania różnych typów logów za pomocą dedykowanych zestawów kolumn
Wysoka dostępność	Obsługa konfiguracji HA dla Log Server

Licencja Administrative Domain zapewnia scentralizowane zarządzanie wieloma środowiskami klientów

Dostawcy Managed Security Services (MSSP) potrzebują obniżyć wysokie koszty administracyjne związane z obsługą wielu serwerów zarządzania w wielu domenach. Administrative Domain License umożliwia zarządzanie wieloma środowiskami klientów za pośrednictwem jednego serwera zarządzania. Konfiguracje mogą być ponownie wykorzystywane i współdzielone w wielu domenach w celu szybkiej i skutecznej dystrybucji zmian. Wyjątkowa architektura rozwiązania Administrative Domain upraszcza środowiska biznesowe i MSSP, dzięki czemu są one łatwiejsze i tańsze w utrzymaniu. Kontrola dostępu oparta na rolach (ang. role-based access control, RBAC) zapewnia odpowiednią separację uprawnień administratorów i określa poziom dostępu do domeny. Klienci końcowi korzystający z określonej domeny mogą łatwo uzyskać dostęp do przeglądu raportów, konfiguracji polityk i logów za pośrednictwem bezpiecznego, intuicyjnego portalu internetowego bez konieczności dostępu do serwera zarządzania.

Specyfikacja Forcepoint Administrative Domain License

Domeny	
Maksymalna liczba domen	200
Liczba administratorów	Bez ograniczeń
Liczba zarządzanych urządzeń na domenę	Bez ograniczeń
Liczba elementów na domenę	Bez ograniczeń
Właściwości	
Separacja konfiguracji	Izoluje środowiska klientów w różnych domenach i sprawdza, czy elementy sieciowe klientów są odpowiednio separowane
Podział konfiguracji	Współdzieli elementy, takie jak szablony polityk pomiędzy domenami
Kontrola dostępu	Określa widoczność i definiuje uprawnienia administratorów za pomocą domen
Monitoring	Monitoruje status wszystkich przyznanych domen za pomocą widoku domeny
Dostosowywanie	Możliwość tworzenia własnych szablonów PDF
Narzędzia migracji	Przenosi elementy między domenami za pomocą zintegrowanego narzędzia „move-to”
Import/Export	Import i eksport elementów między różnymi instalacjami SMC i domenami
Konteksty wirtualne	Udostępnia ten sam kontekst typu Master w ramach domen, maksymalnie 250 kontekstów wirtualnych, z których każdy może mieć własne polityki i tabele routingu

Web Portal Server

Forcepoint Web Portal Server udostępnia klientom oraz administratorom portal internetowy do przeglądania logów, raportów, bieżących polityk i historii ich zmian. Administratorzy MSSP mogą konfigurować ilość informacji wyświetlanych w portalu w oparciu o potrzeby klienta.

Web Portal Server Forcepoint obsługuje języki angielski, hiszpański i francuski. Istnieje również opcja dodawania nowych języków.

Główne korzyści

- **Dostęp poprzez przeglądarkę do logów, raportów, polityk i historii ich zmian. Uprawnienia tylko do odczytu.**
- **Dostępny status sieci w czasie rzeczywistym dla zdefiniowanych użytkowników.**
- **Możliwy dostęp poprzez urządzenia mobilne.**

Specyfikacje Forcepoint Web Portal Server

Specyfikacje	
Maksymalna liczba jednoczesnych użytkowników	250 na licencję
Liczba administratorów	Bez ograniczeń
Liczba użytkowników Web Portal	Bez ograniczeń
Uwierzytelnianie użytkownika	Lokalna baza danych Management Server, RADIUS, TACACS+
Połączenia z innymi komponentami	Szyfrowanie SSL
Właściwości	
Polityki bezpieczeństwa	Podgląd najnowszych polityk zapór ogniowych nowej generacji w formacie HTML
Raporty	Podgląd raportów, które mają zostać opublikowane w portalu webowym w formacie HTML
Przeglądanie logów	Przeglądanie i filtrowanie logów w formacie HTML
Szczegółowe informacje dot. logów	Podgląd wizualizacji zdarzeń logów i inne szczegółowe informacje dotyczące logów na oddzielnej stronie HTML
Eksport PDF	Drukowanie raportów i logów w PDF
Komunikaty	Administratorzy mogą określać komunikaty, które będą wyświetlane w portalu webowym
Porównanie polityk	Porównanie różnych wersji polityk zapory ogniowej celem sprawdzenia, czy wdrożono żądanie zmiany
Lokalizacja	Portal webowy obsługuje języki angielski, hiszpański i francuski. Można go łatwo przetłumaczyć, aby obsługiwał inne języki
Dostosowywanie	Dostosowywanie wyglądu portali webowych

Security Management Center Appliance

Forcepoint Security Management Center (SMC) Appliance to kompleksowe urządzenie dedykowane do konfiguracji, zarządzania i monitorowania zapór ogniowych Forcepoint nowej generacji – w formie fizycznej, wirtualnej i w chmurze. Rozwiązanie Forcepoint SMC zapewnia łatwość wdrożenia, co umożliwia szybkie uruchomienie i pracę, łącząc serwer zarządzania NGFW Forcepoint i serwer logów w jeden pakiet plug-and-play działający na zoptymalizowanym serwerze 1U. W miarę wzrostu potrzeb bezpieczeństwa sieci, Forcepoint SMC umożliwia płynne wdrożenie opcji wysokiej dostępności (HA) dla serwera zarządzania.

Opcje wdrożenia SMC

Istnieją trzy sposoby wdrażenia rozwiązania Forcepoint SMC: na systemie operacyjnym klienta, na sprzęcie lub hiperwizorze klienta, bądź jako urządzenie all-in-one w formie SMC appliance.

KOMPONENT	OPCJE WDRAŻANIA FORCEPOINT SMC		URZĄDZENIE
	OPROGRAMOWANIE	ISO IMAGE	
Oprogramowanie SMC	✓	✓	✓
System operacyjny	Dostarczany przez klienta	✓	✓
Sprzęt	Dostarczany przez klienta	Dostarczany przez klienta	✓

Specyfikacja Forcepoint SMC Appliance

WYDAJNOŚĆ	
Obsługiwane zapory	2000
Maks. Ilość domen	200
Indeksowane logów/s	80 000
Zdarzenia dziennie	6 912 000 000
Wielkość loga dziennie (GB)	690
WŁAŚCIWOŚCI FIZYCZNE	
Obudowa	1U
Procesor	2 x Intel Xeon
Pamięć	32 GB
Przechowywanie (HDD)	Pojemność 900 GB (4 X 300 GB, RAID-5), Hot Swappable
Zasilanie	2 x 550W (100V~240V) Hot Swappable
Wymiary	23,9" śr. x 17,09" szer. x 1,68" wys. (60,7 cm śr. x 43,42 cm szer. x 4,28 cm wys.)
Waga	28,26 lbs. (12,82 kg)
Regulacje i zgodność	FCC / ICES / EN55022 / VCCIBSMI / C-Tick / SABS / CCC / MIC Class A i UL60950-1 /Zweryfikowane jako zgodne z Dyrektywą RoHS

Specyfikacja Forcepoint SMC Appliance

NAZWA	KOD PRODUKTU
Forcepoint NGFW Security Management Center Software Subscription	SMC
Forcepoint NGFW Security Management Center 1000 Appliance	SMCAP
Forcepoint SMC High Availability Subscription (dostępna tylko dla oprogramowania i wdrożenia ISO image)	SMCHA
SMC Additional Log Server Subscription	ALS
Optional SMC Domains Feature Subscription (do 200 domen)	ODFSMC
Optional SMC Web Portal Server Subscription	OWPS

KONTAKT
www.forcepoint.com/contact
Biuro Forcepoint Polska
ul. Gintrowskiego 53
02-697 Warszawa
Tel.+48 225 480 100

Anna Zawadzka
Team Leader Territory Manager Poland
anna.zawadzka@forcepoint.com,
tel. 600 301 512

Agnieszka Mucha
Channel Account Manager,
Agnieszka.mucha@forcepoint.com,
tel. 603 990 533

[DATASHEET_FORCEPOINT_NGFW_SECURITY_MANAGEMENT_CENTER_EN] 100030.092917