Jak wybrać

# platformę bezpieczeństwa?

FORTINET.

EXCLUSIVE NETWORKS

**Ochrona sieci komputerowych przed współczesnymi zagrożeniami wymaga zastosowania wielu mechanizmów zabezpieczeń z obszarów:**

kontroli dostępu, bezpieczeństwa aplikacji, analizy treści, szyfrowania komunikacji oraz uwierzytelniania i korelacji zdarzeń.

Poszczególne technologie, zaimplementowane w ramach zintegrowanego systemu ochrony NGFW (Next Generation Firewall), zwiększają skuteczność reagowania na zagrożenia.

Czy możliwe jest połączenie funkcji, które zagwarantują najwyższy poziom bezpieczeństwa sieci, treści i ochrony aplikacji, przy jednoczesnym obniżeniu całkowitego kosztu zakupu oraz zapewnieniu elastycznej i skalowalnej możliwości rozwoju? Przedstawiamy zestaw zagadnień, które umożliwią dobór optymalnego rozwiązania.

## Platforma zintegrowana:

### Wirtualizacja w obrębie wszystkich funkcji systemu

Wirtualizacja pozwala budować, w ramach jednej platformy fizycznej lub wirtualnej, wiele niezależnych systemów logicznych. Stosowana jest najczęściej w takich przypadkach jak: zaawansowane konfiguracje z routingiem, konieczność odseparowania stref sieciowych (np. sieci firmowej od infrastruktury OT), zapewnienie indywidualnych mechanizmów ochrony dla niezależnych podmiotów w ramach jednej lokalizacji (business park), obsługa wielu klientów w ramach usług MSSP. Wirtualizacja może dotyczyć wszystkich funkcji bezpieczeństwa oraz sieciowych, realizowanych przez platformę.

### Wszystkie funkcje kompleksowego systemu ochrony można uruchomić w ramach jednej platformy sprzętowej lub wirtualnej

Uruchomienie wszystkich funkcji w ramach jednego urządzenia pozwala obniżyć koszty implementacji kompleksowego systemu ochrony. Wiele platform to z kolei więcej urządzeń, kilka interfejsów oraz bardziej złożona integracja.

### Granularna konfiguracja w zakresie poszczególnych funkcji bezpieczeństwa

Elastyczny system bezpieczeństwa pozwala definiować wiele zbiorów ustawień (profili) w zakresie poszczególnych funkcji, które będą później wykorzystywane w różnych politykach. Funkcje realizowane globalnie w platformie są dużym ograniczeniem.

### Możliwość implementacji w różnych trybach

Możliwość uruchomienia całej platformy lub poszczególnych instancji logicznych systemu w różnych trybach pracy (router z NAT, transparentny, nasłuchu, proxy) ułatwia implementację, a przede wszystkim pozwala dostosować system do różnorodnych warunków pracy sieci.

### Zarządzanie w oparciu o role – RBM

W typowym środowisku teleinformatycznym bardzo często rozdzielone są funkcje administratora sieci oraz oficera bezpieczeństwa. Dlatego tak istotna jest możliwość przypisania poszczególnym administratorom ściśle określonych uprawnień do konkretnych funkcji systemu. Dodatkowym ułatwieniem jest powiązanie tego mechanizmu z zewnętrznymi systemami zarządzania tożsamością. W takiej sytuacji, w wyniku uwierzytelnienia do urządzenia trafia profil dostępowy. W oparciu o niego następnie realizowane są zasady kontroli dostępu do poszczególnych funkcji systemu.

## Firewall:

### Firewall pozwala tworzyć polityki w oparciu o użytkownika domeny

Firewall zapewnia spersonalizowaną politykę bezpieczeństwa. Administrator bazuje na grupach użytkowników, np.: serwis, finanse, administracja. Raporty podają szczegółowe informacje o aktywności użytkowników.

### Parametrami, na podstawie których firewall podejmuje decyzje są: aplikacje, kategorie i adresy URL

Dzięki temu można definiować bardzo uniwersalne polityki, które ułatwiają proces konfiguracji zasad kontroli dostępu. Decyzja (jak analizować komunikację) może być podejmowana niezależnie od adresów IP czy użytkowników, np. na podstawie określonej aplikacji.

## Akceleracja sprzętowa dla firewall, VPN oraz funkcji analizy treści

Akceleracja sprzętowa oznacza, że kontrola pakietów w ramach firewall (szczególnie istotna w przypadku małych pakietów) czy szyfrowanie komunikacji IPSec, realizowane są przez dedykowane układy sprzętowe z bardzo dużą wydajnością oraz z niewielkim wpływem na pracę procesora głównego. W ten sposób całe jego zasoby wykorzystywane są na operacje związane z analizą danych. Większość producentów podaje parametry wydajnościowe dla próbki ruchu w postaci dużych pakietów. Małe pakiety mogą znacząco wpływać na spadek wydajności systemu.

VPN:

## Szyfrowane połączenia IPSec VPN w oparciu o mocne algorytmy kryptograficzne

Nie wszystkie systemy oferują silne algorytmy szyfrowania w ramach platformy podstawowej. W niektórych przypadkach wiąże się to z zakupem dodatkowej licencji. Systemy wyposażone w sprzętową akcelerację pozwalają uzyskać duże przepustowości w zakresie szyfrowanych kanałów. Ważne funkcje w ramach IPSec to: obsługa IKEv2, wsparcie dla NAT Traversal, obsługa Split tunnelingu, dedykowana aplikacja kliencka tego samego producenta, redundancja szyfrowanych połączeń, obsługa różnych topologii, wsparcie dla XVLAN, funkcja dynamicznego zestawiania tuneli, możliwość uruchomienia protokołów dynamicznego routingu w obrębie szyfrowanych tuneli, tunel IPSec jako element mechanizmów SD-WAN.

## Szyfrowane połączenia SSL VPN

Istotnym argumentem jest możliwość weryfikacji poziomu bezpieczeństwa na łączącej się stacji, jak np.: czy aktywne są firewall oraz kontrola antywirusowa, jakie aplikacje uruchomiono (np. wykrycie uruchomionych na zdalnej stacji aplikacji P2P blokuje możliwość zestawienia szyfrowanego połączenia). Kolejnymi ważnymi funkcjami są: obsługa split tunnelingu oraz możliwość przypisania różnych zasad dostępu do zasobów wewnętrznych, dla różnych grup użytkowników w oparciu o tryby pracy: tunel i portalu.

## Kontrola treści ruchu w szyfrowanym tunelu

Realizowane połączenia VPN zapewniają poufność przesyłanych informacji. Stanowią jednak drogę, którą mogą przedostać się do organizacji różne zagrożenia. Nie mając pewności co do stanu bezpieczeństwa zdalnych lokalizacji lub stacji użytkowników mobilnych należy zadbać o kontrolę tych „potencjalnie zaufanych" kanałów komunikacyjnych. Warto zweryfikować czy rozwiązanie umożliwia pełną kontrolę ruchu w terminowanych połączeniach IPSec oraz SSL VPN z wykorzystaniem wszystkich funkcji ochronnych.

## Dedykowany klient IPSec/SSL VPN ze zintegrowanymi funkcjami ochrony

Jeżeli producent rozwiązania nie dostarcza dedykowanego klienta, konieczne jest zastosowanie aplikacji otwartych, które nie posiadają wsparcia, są pozbawione centralnego logowania i zarządzania, bez gwarancji ich stabilności oraz realizowanego poziomu bezpieczeństwa. Dedykowane aplikacje klienckie są na ogół wyposażone w szereg mechanizmów jak: kontrola aplikacji, analiza podatności, ochrona przed malware, współpraca z Sandbox, filtr URL i inne. Te wszystkie funkcje pozwalają rozszerzyć zasady polityki bezpieczeństwa firmy na urządzenia osób pracujących zdalnie.

## Inspekcja komunikacji SSL:

Zdecydowana większość komunikacji WWW realizowana jest obecnie w postaci ruchu szyfrowanego protokołem SSL. HTTPS jest najbardziej popularnym konałem komunikacyjnym, dlatego jego inspekcja jest kluczowa dla zapewnienia bezpieczeństwa.

Wybierając rozwiązanie warto zweryfikować, czy umożliwia ono stosowanie różnych zasad kontroli SSL w poszczególnych politykach firewall oraz czy pozwala definiować wyjątki, dla których szyfrowana komunikacja nie będzie poddawana analizie. Należy również sprawdzić, jaką wydajność oferują poszczególne platformy przy włączonych funkcjach inspekcji SSL oraz modułach ochrony.

## Kontrola aplikacji:

### Funkcja wykrywania aplikacji (np. P2, komunikatory, Gmail, itp.) na podstawie głębokiej analizy ruchu oraz ich kontrola

Głęboka analiza ruchu pozwala wykrywać aplikacje niezależnie od wykorzystywanego protokołu czy numeru portu. Administrator ma możliwość zablokowania określonej aplikacji, działającej lokalnie lub w ramach portalu, nie ograniczając jednocześnie dostępu do jego pozostałych elementów.

Warto zweryfikować, jak rozbudowaną bazę sygnatur dostarcza producent oraz czy obejmuje ona zarówno aplikacje sieciowe, jak i cloud. Przydatną funkcją jest możliwość definiowania własnych sygnatur aplikacji - w ten sposób można dostosować działanie mechanizmów ochrony do indywidualnych potrzeb organizacji.

### Zarządzanie pasmem dla aplikacji

Istotną funkcją jest możliwość priorytetyzowania, określenia maksymalnej oraz gwarantowanej wielkości pasma dla aplikacji. W ten sposób można alokować niezbędną ilość zasobów dla usług, które są istotne z punktu widzenia prowadzonej działalności oraz zapobiegać wysycaniu łącza przez mniej ważne serwisy np.: streaming, radio czy serwisy video.

### Polityki bazujące na aplikacjach

Warto zweryfikować, czy system ochrony umożliwia definiowanie polityk, w których parametrem wejściowym (dopasowującym) może być aplikacja lub kategoria aplikacji.

### Rozpoznawanie i kontrola aplikacji SCADA

Kontrola, ochrona i segmentacja ruchu są częstym wymaganiem ze strony firm, w których funkcjonuje infrastruktura przemysłowa. Dla takich aplikacji można dedykować logiczną instancję systemu ochrony, w której będą funkcjonowały mechanizmy zaprojektowane do ochrony urządzeń OT. Warto zweryfikować jak rozbudowanej bazy protokołów SCADA dostarcza producent oraz czy istnieje możliwość definiowania własnych sygnatur. Te są bardzo istotne z punktu widzenia dostosowania systemu ochrony do indywidualnych parametrów sieci przemysłowej.

# Ochrona przed atakami – IPS:

## Szeroka baza sygnatur dostarczana przez producenta sprzętu

Szeroka baza sygnatur z minimalnym współczynnikiem błędnych trafień to duży atut systemu ochrony przed atakami. Określenie przez producenta atrybutów sygnatury (czy chroni klienta/serwer, jakiego OS dotyczy, jaką aplikację zabezpiecza) pozwala w szybki i łatwy sposób definiować zbiory sygnatur, istotnych dla chronionych zasobów. Oszczędzamy w ten sposób zasoby, analizując ruch tylko tymi sygnaturami, które mają sens. Po co stosować na przykład sygnatury chroniące serwer HTTP, skoro takiego serwera nie posiadamy.

## Własne sygnatury IPS

Czasem zdarza się, że aplikacje wewnętrzne działają w oparciu o niestandardową komunikację, która może być blokowana przez predefiniowane sygnatury IPS. W takiej sytuacji niekoniecznie musimy rezygnować z ochrony aplikacji, wyłączając sygnaturę. Zdecydowanie lepszym wyjściem jest opracowanie własnej reguły chroniącej ruch.

## Polityki bazujące na aplikacjach

Warto zweryfikować, czy system ochrony umożliwia definiowanie polityk, w których parametrem wejściowym (dopasowującym) może być aplikacja lub kategoria aplikacji.

## Rozpoznawanie i kontrola aplikacji SCADA

Kontrola, ochrona i segmentacja ruchu są częstym wymaganiem ze strony firm, w których funkcjonuje infrastruktura przemysłowa. Dla takich aplikacji można dedykować logiczną instancję systemu ochrony, w której będą funkcjonowały mechanizmy zaprojektowane do ochrony urządzeń OT.

Warto zweryfikować jak rozbudowanej bazy protokołów SCADA dostarcza producent oraz czy istnieje możliwość definiowania własnych sygnatur. Te są bardzo istotnie z punktu widzenia dostosowania systemu ochrony do indywidualnych parametrów sieci przemysłowej.

## Możliwość zapisania pakietu stanowiącego o ataku jako dowód na to, że został on przeprowadzony (Cyber Crime)

Po przeprowadzonym ataku pozostaje ślad w postaci zapisanego pakietu, który następnie można użyć do przeprowadzenia analizy zdarzenia. Niezależnie zapisany materiał może być wykorzystany w procesie dowodowym.

## Sygnatury ochrony dla sieci przemysłowych

W przypadku implementacji w sieciach przemysłowych, istotne będzie jak rozbudowaną bazę sygnatur do ochrony protokołów SCADA dostarcza producent. Sieci przemysłowe charakteryzują się indywidualnymi parametrami, dlatego ważne jest, aby system umożliwiał definiowanie własnych sygnatur, które pozwolą na dostosowanie mechanizmów kontroli do indywidualnych potrzeb.

## Wykrywanie anomalii ruchu i protokołów – ochrona DoS, DDoS (np. 500 sesji TCP od jednego użytkownika, 10 000 sesji do serwera)

DoS oraz DDoS to kłopotliwe formy ataków, przeprowadzane najczęściej z wykorzystaniem sieci Botnet. Do ochrony przed tego typu zagrożeniami stosuje się dedykowane platformy.

## Ochrona przed malware:

### Możliwość analizy dowolnego typu załączników

Nie wszystkie dostępne na rynku, zintegrowane systemy ochrony umożliwiają analizę dowolnego typu plików, które są przesyłane w komunikacji sieciowej. Wynika to głównie z metod skanowania, które wykorzystuje platforma. Wybierając rozwiązanie warto zweryfikować, czy umożliwi ono pełną analizę ruchu oraz z jaką wydajnością może taką analizę realizować. Ważne jest również sprawdzenie czy system analizuje zawartość dla wszystkich najważniejszych protokołów komunikacyjnych: HTTP, FTP, SMTP, POP3, IMAP, MAPI, CIFS, SSH.

### Analiza ruchu dla protokołów działających na niestandardowych portach

Niektóre aplikacje, aby ominąć zabezpieczenia, realizują komunikację z wykorzystaniem niestandardowych portów. Nie wszystkie systemy bezpieczeństwa mogą je jednak rozpoznać i poddać inspekcji przesyłaną zawartość. Warto zweryfikować, czy rozwiązanie analizuję całą komunikację oraz czy wykrywa aplikacje niezależnie od numeru portu.

### Integracja z systemem Sandbox

Analiza załączników w systemach Sandbox jest bardzo istotna w kontekście ochrony przed nowymi zagrożeniami, które nie zostały dotychczas opisane za pomocą sygnatur. Wielu producentów dostarcza dedykowane platformy tego typu, które funkcjonują lokalnie lub w postaci usługi chmurowej. Ważne jest zweryfikowanie, czy rozważany system ochrony ma możliwość współpracy z tego typu mechanizmami oraz jaki jest koszt takiej integracji.

### Ochrona dla urządzeń mobilnych

Urządzenia mobilne stały się efektywnym narzędziem pracy, na którym przechowywane są poufne informacje organizacji. Dlatego warto upewnić się, że zintegrowany system ochrony może chronić przed złośliwym oprogramowaniem atakującym urządzenia mobilne. Warto zweryfikować dla jakich mobilnych systemów operacyjnych taka analiza może być przeprowadzana.

### Content Disarm czyli usuwanie aktywnej treści z dokumentów

Podpięcie do dokumentu aktywnej treści - np. złośliwego makra - jest często stosowaną techniką ataku. Niektóre systemy ochrony umożliwiają usuwanie aktywnego kodu z plików zanim zostaną one dostarczone do użytkownika. Mechanizm taki stosuje się, np. dla dokumentów przesyłanych z zewnątrz do organizacji. Warto zweryfikować czy producent zapewnia mechanizmy, którymi użytkownik będzie mógł odzyskać oryginalny plik po przeprowadzonej analizie w ramach systemu Sandbox.

## Kontrola WWW oraz DNS:

### Filtrowanie ruchu http w oparciu o adresy i kategorie URL

Większość dostępnych na rynku systemów ochrony umożliwia kontrolę ruchu webowego. Taka analiza jest jednym z podstawowych mechanizmów proaktywnej ochrony przed zagrożeniami. Warto zweryfikować, czy producent rozwiązania dostarcza kategorie stron, które są istotne z punktu widzenia bezpieczeństwa: SPAM, phishing, malware, proxy itp. oraz z punktu widzenia produktywności: video, radio, streaming, gry. Istotne jest również, czy kategorie URL zabronione prawem są elementem bazy, w o parciu o którą realizowane jest filtrowanie.

### Możliwość korzystania z zewnętrznych baz IP/ URL dostarczanych przez organizacje typu CERT

W większości krajów funkcjonują ośrodki, które zajmują się cyberbezpieczeństwem, a wynikiem ich analizy są m.in. listy adresów, które są niebezpieczne. Są to na bieżąco aktualizowane listy złośliwych adresów oraz serwisów, które są szczególnie aktywne w danym kraju oraz z których przeprowadzane były ataki w ostatnim czasie. Ważną funkcją systemu ochrony jest możliwość integracji z takimi zewnętrznymi, dynamicznymi bazami, aby informacje w nich zawarte wykorzystywać w ramach codziennej ochrony. Aby podnieść jej skuteczność proces odświeżania informacji z baz powinien odbywać się w sposób automatyczny.

### Zarządzanie pasmem dla kategorii URL

Możliwość priorytetyzowania ruchu oraz zarządzanie pasmem dla poszczególnych stron lub całych kategorii URL jest istotną funkcją, która pozwala oszczędzać zasoby sieciowe dla kluczowych usług, działających w ramach organizacji. Użyteczną funkcją jest również możliwość określenia ilości czasu, z którego użytkownik może korzystać, uzyskując dostęp do określonego typu serwisów.

### Funkcja Safe Search

Wyszukiwanie treści poprzez wyszukiwarki serwisu YouTube jest jedną z metod omijania mechanizmów filtrowania stron. Warto zweryfikować czy system, który odpowiada za kontrolę, umożliwia również inspekcję wyników wyszukiwania w popularnych serwisach.

### Filtrowanie ruchu video w oparciu o kategorie, dostarczane przez producenta

Może to być istotna funkcja w sytuacji, kiedy system wykorzystywany będzie np. do ochrony komunikacji sieciowej w placówce oświatowej.

### Filtrowanie zapytań DNS

Filtrowanie komunikacji DNS w oparciu o adresy URL lub kategorie jest – podobnie jak URL filtering - jednym z podstawowych mechanizmów ochrony proaktywnej. W tym przypadku analizowane są zapytania DNS, które mogą być generowane przez różnorodne aplikacje. Istotną funkcją rozszerzającą możliwości w tym zakresie jest możliwość definiowania wewnętrznej bazy DNS z wyjątkami, własnymi rekordami oraz możliwością modyfikowania odpowiedzi DNS poprzez wskazanie określonych serwisów.

## Ochrona przed wyciekiem danych (mechanizmy DLP)

### Możliwość identyfikacji i zapobiegania wyciekowi danych wrażliwych poza sieć

Systemy analizujące treść i kontrolujące przepływ informacji są zwykle implementowane w postaci dedykowanych rozwiązań – zazwyczaj kosztownych i wymagających dużego nakładu pracy przy wdrożeniu oraz utrzymaniu. Niektóre z oferowanych przez nie funkcji są coraz częściej uruchamiane w ramach zintegrowanych platform bezpieczeństwa. Administrator sieci ma możliwość zapisania sesji określonych użytkowników, może zablokować próbę wysłania informacji, w której znajdują się np.: określone słowa kluczowe, pliki zabezpieczone hasłem itp.

## Uwierzytelnianie:

Mechanizmy uwierzytelniania w zintegrowanych systemach ochrony obejmują szereg aspektów. Począwszy od kwestii dostępu administracyjnego, poprzez uwierzytelnianie w ramach polityk, na zdalnym dostępie VPN kończąc.

## Polityki bazujące na użytkowniku z mechanizmami SSO

Stosowane są różne metody definiowania polityk bezpieczeństwa w ramach firewall. Oprócz standardowych, bazujących na adresach IP często budowane są reguły bezpieczeństwa, w których parametrem wejściowym jest użytkownik lub grupa użytkowników. W takim scenariuszu platforma bezpieczeństwa integruje się z systemem zarządzania tożsamością (np. Active Directory lub Radius), aby czerpać informacje o zdefiniowanych już użytkownikach lub jednostkach organizacyjnych. W momencie, kiedy użytkownik zostaje uwierzytelniony w ramach np. AD, do platformy bezpieczeństwa spływa kontekst użytkownika (informacje: nazwa użytkownika, adres IP, informacja o grupach, do których on należy) i na tej podstawie egzekwowane są odpowiednie polityki, które administrator przewidział dla grupy, do której należy użytkownik. Ważne jest, że logowane informacje są spersonalizowane, a prezentowane dane pokazują aktywność użytkowników niezależnie od systemów, do których są jednocześnie zalogowani.

Stosowane w ten sposób mechanizmy SSO są dużym ułatwieniem dla użytkowników, którzy zostają poproszeni tylko jeden raz poświadczenia dostępu do zasobów organizacji.

## Uwierzytelniania w ramach sesji firewall oraz Captive Portal

Dostęp do strategicznych zasobów organizacji powinien być chroniony w sposób szczególny. Dlatego bardzo często w politykach, które odpowiadają za komunikację z tymi zasobami, wymusza się dodatkowe uwierzytelnienie z wykorzystaniem jednej ze wspieranych metod.

Innym przykładem zastosowania tego mechanizmu jest Captive Portal, przez który świadczony jest dostęp do wybranych fragmentów infrastruktury dla użytkowników gościnnych oraz podwykonawców. Warto zweryfikować, czy rozwiązanie wyposażone jest w funkcje captive portalu oraz czy posiada dodatkowe mechanizmy (np. portal recepcjonistki), które ułatwiają obsługę dostępu gościnnego.

## Wieloskładnikowe metody uwierzytelniania

W przypadku dostępu administracyjnego czy zdalnego poprzez VPN, bardzo często stosowane są dodatkowe - oprócz loginu i hasła - poświadczenia w procesie weryfikacji tożsamości użytkownika. Takie mechanizmy znacząco podnoszą skuteczność ochrony przed nieuprawnionym dostępem. Dodatkowe poświadczenia to najczęściej kody jednorazowe dostarczane mailem, sms'em, tokenem sprzętowym lub programowym, ale coraz częściej do tego celu wykorzystywane są również certyfikaty zlokalizowane na kluczach USB lub metoda PUSH. Informuje ona użytkownika poprzez aplikację mobilną o próbie uzyskania dostępu do zasobów i żąda jej autoryzacji.

Warto zweryfikować, czy rozważany system ochrony wyposażony jest w mechanizmy uwierzytelniania wieloskładnikowego oraz czy można je uruchomić w ramach platformy - eliminując tym samym konieczność zastosowania zewnętrznych systemów.

## Uwierzytelnienie w oparciu o protokół SAML

Protokół SAML stał się powszechnie wykorzystywanym standardem w procesie uwierzytelnienia. Wybierając rozwiązanie warto zweryfikować, czy umożliwia ono zastosowanie tego protokołu, dla jakich scenariuszy uwierzytelnienia oraz czy umożliwia pełnienie funkcji zarówno Identity Provider'a (IdP), jak i Service Provider'a (SP).

## Kontroler sieci bezprzewodowych:

Jednym z podstawowych założeń budowania nowoczesnej infrastruktury sieciowej jest elastyczność w zakresie dostępu do niej poprzez połączenia przewodowe oraz drogą radiową. Aby sprawnie zarządzać elementami infrastruktury powinny one być centralnie zarządzane. W przeszłości do tego celu wykorzystywane były dedykowane platformy centralnego zarządzania punktami dostępowymi AP. Obecnie funkcja kontrolera sieci bezprzewodowych coraz częściej dostępna jest jako element platformy bezpieczeństwa. Takie podejście ma wiele zalet, jak np.: niższe koszty wdrożenia i utrzymania, łatwe zarządzanie (definiowane sieci bezprzewodowe stają się automatycznie elementami, do których przyporządkowywane są polityki ochronne), przeniesienie mechanizmów ochrony na punkt styku z siecią, łatwa implementacja kontroli dostępu do infrastruktury (mechanizmy NAC) i inne.

Wybierając rozwiązanie warto zweryfikować, w jakich trybach mogą być podłączane punkty dostępowe, czy umożliwiają tunelowanie komunikacji wprost do systemu bezpieczeństwa, czy producent dostarcza najnowsze standardy radiowe oraz czy system zapewnia wszystkie istotne dzisiaj mechanizmy jak np.: ochrona przed atakami na sieć bezprzewodową, szybki roaming, możliwość priorytetyzowania ruchu.

## Kontroler przełączników:

Podobnie jak w przypadku zarządzania siecią bezprzewodową, zintegrowane systemy ochrony coraz częściej wyposażone są w funkcję kontrolera sieci przewodowej. W tej sytuacji z konsoli urządzania można zarządzać przełącznikami szkieletowymi oraz dostępowymi lokalnie oraz w oddziałach firmy. W ten sposób łatwiej zarządzać infrastrukturą, a definiowane fragmenty sieci (VLAN'y) stają się automatycznie parametrami, dla których budowane są polityki bezpieczeństwa oraz definiowane są zasady kontroli dostępu do infrastruktury sieciowej.

## Mechanizmy SD-WAN:

Technologia SD-WAN to zestaw mechanizmów, które usprawniają komunikację w rozproszonej sieci przedsiębiorstwa oraz pozwalają efektywnie wykorzystywać dostępne łącza WAN w celu optymalnego funkcjonowania kluczowych aplikacji. Jej najważniejsze funkcje to: obsługa wielu łączy, redundancja połączeń, podział obciążenia w oparciu o różne kryteria (np.: aplikacje, wielkość ruchu, opóźnienia, straty pakietów), priorytetyzowanie i kolejkowanie ruchu, tworzenie szyfrowanych kanałów komunikacyjnych oraz ich redundancja, kształtowanie komunikacji w oparciu o protokoły dynamicznego routingu w celu zwiększenia niezawodności i zapewnienia spójności infrastruktury, mechanizmy optymalizacji komunikacji i protokołów. Wybierając rozwiązanie warto zwrócić uwagę, czy producent dostarcza centralny system zarządzania mechanizmami SD-WAN oraz narzędzia, które pozwalają monitorować i raportować stan pracy rozproszonej infrastruktury.

## Exclusive Networks

Exclusive Networks jest globalnym liderem dystrybucji z wartością dodaną, obecnym w 150 krajach, dostarczającym zaawansowane technologie cyfrowe w zakresie cyberbezpieczeństwa i cloud. Firma działa w unikatowym modelu „local sale, global scale". Zapewnia on wymianę doświadczeń z ekspertami z całego świata oraz stabilny rozwój w globalnych strukturach, a jednocześnie niezależność, bliskość z partnerami, bezpośrednie wsparcie handlowe i techniczne, świadczone przez osoby, doskonale znające rynek lokalny i posługujące się ich językiem.

Od 2021 roku firma rozszerzyła swój obszar działalności o region CEE, dołączając do swoich struktur Veracomp - największego dystrybutora VAD z ponad 30-letnim doświadczeniem, obecnego w 18 krajach Europy Środkowo-Wschodniej.

Exclusive Networks Poland zapewnia partnerom know-how, zespół 300 ekspertów oraz doskonałą znajomość rynku IT, dbając o długofalowe relacje, oparte na wzajemnym zaufaniu. Ofertę firmy tworzą zaawansowane technologie cyfrowe w zakresie sieci, pamięci masowych i serwerów, cyberbezpieczeństwa, Unified Communications, Cloud i Data Center, rozwiązań przemysłowych i IoT, systemów AV oraz Digital Signage, a także produktów SOHO, grafiki i gamingu.

## Fortinet

Firma Fortinet jest światowym dostawcą rozwiązań cyberbezpieczeństwa, które umożliwiają jej klientom ochronę i kontrolę infrastruktury informatycznej. Jej specjalnie opracowane, zintegrowane technologie wraz z usługami FortiGuard, badającymi zagrożenia, zapewniają klientom niezwykle skuteczną ochronę treści dotrzymującą kroku nieustannie rozwijającym się zagrożeniom.
Z oferty rozwiązań Fortinet korzysta ponad 320 000 klientów na całym świecie, w tym większość przedsiębiorstw z listy Global 1000, usługodawców i instytucji państwowych. Pozwalają im one wzmacniać bezpieczeństwo, upraszczać infrastrukturę sieci i obniżać całkowity koszt posiadania.

**Wiecej na //40.camp.pl**

FORTINET.

EXCLUSIVE NETWORKS