**Załącznik nr 7.3 do SWZ**

**Zakup sprzętu biurowego i komputerowego na potrzeby projektu "Cyberbezpieczna Gmina Pszczółki"**

**Zadanie III – Dostawa i wdrożenie UTM**

## Urządzenie UTM

* System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania.
* Moduł kryptoraficzny zgodny ze standardem FIPS 140-2.
* Rozwiązanie musi wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca)
* Możliwość budowy klastra wysokiej dostępności pracującego trybie Active-Passive lub Active-Active.
* System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej.
* Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy (drugi zasilacz jako wyposażenie opcjonalne).
* Urządzenie w metalowej obudowie o wysokości maksymalnie 1U z możliwością montażu w szafie rack 19" (uchwyty montażowe w komplecie).
* Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB).
* Wbudowany port Ethernet do zarządzania w trybie out-of-band management.
* Wbudowany port USB umożliwiający podłączenie modemów 3G/4G/LTE produkowanych przez firmy trzecie.
* Wbudowany port USB umożliwiający podłączenie pamięci flash i przeprowadzenie konfiguracji w trybie Zero Touch.
* Możliwość rozbudowy o dodatkowe moduły interfejsów sieciowych.

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Pamięć operacyjna RAM (GB): | 8 |
| Przestrzeń do przechowywania logów i raportów (GB) | 120 |
| Liczba fizycznych interfejsów 1000BASE-T | 8 |
| Liczba fizycznych interfejsów 1000BASE-X | 2 |
| Liczba fizycznych interfejsów 10GBASE-X | 2 |
| Liczba wirtualnych interfejsów (VLAN) IEEE 802.1Q | 128 |
| Wydajność Firewall nie mniej niż (Gbps) | 35 |
| Wydajność Firewall IMIX nie mniej niż (Gbps) | 20 |
| Wydajność IPS nie mniej niż (Gbps) | 8 |
| Wydajność FW+IPS+AV nie mniej niż (Gbps) | 2 |
| Wydajność NGFW nie mniej niż (Gbps) | 8 |
| Liczba równoczesnych połączeń | 10 000 000 |
| Liczba nowych połączeń na sekundę | 150 000 |
| Wydajność IPsec VPN (Gbps): | 15 |
| Wydajność dla inspekcji ruchu SSL/TLS (Gbps): | 2 |
| Liczba równoczesnych połączeń SSL/TLS | 55 000 |
| Liczba równoczesnych tuneli SSL VPN | 500 |
| Liczba równoczesnych tuneli IPsec VPN | 2500 |
| Licencja | Minimum 3 lata. |
| Certyfikaty | Urządzenie musi pochodzić z autoryzowanego przez producenta kanału sprzedaży na rynek polski – **załączyć do oferty oświadczenie producenta;**  Serwis musi być świadczony zgodnie z wymaganiami norm ISO 9001 i ISO 27001 dla serwisu rozwiązań informatycznych – **załączyć do oferty certyfikaty dla oferenta.** |

* Zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym.
* Webowy graficzny interfejs administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA).
* Uwierzytelnianianie dwuskładnikowe w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN.
* Wbudowany webowy graficzny interfejs administratora musi oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup;
* Interfejs graficzny administratora musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP.
* Możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
* Automatyczne wylogowanie sesji administratora po zdefiniowanym czasie bezczynności.
* Możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.
* Blokada kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady muszą być swobodnie definiowane przez administratora.
* Mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback).
* Możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa.
* Samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm).
* Śledzenie zmian w konfiguracji (tzw. changelog).
* Elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej.
* Automatyczne powiadamianie za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS).
* Monitorowanie stanu pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i aktualizowane przez producenta.
* Wsparcie dla Netflow v5 (lub jego odpowiednika).
* Monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki muszą być dostępne również dla danych historycznych, z retencją do 12 miesięcy celem śledzenia trendów obciążenia, w ramach webowego interfejsu graficznego urządzenia.
* Możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta urządzenia;
* Wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji.
* Udokumentowane API umożliwiające integrację z systemami firm trzecich.
* Zapora sieciowa musi działać w oparciu o mechanizm Stateful Packet Inspection.
* System powinien umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6.
* Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas.
* Możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej.
* Możliwość definiowania własnych stref zapory sieciowej.
* Blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).
* Filtrowanie widoku stosu reguł na bazie dowolnego ich składnika.
* Routing oparty o polityki SD-WAN wykorzystujące takie kryteria jak: interfejs, sieć, usługa, grupa aplikacji, użytkownik lub grupa użytkowników, brama główna, brama zapasowa czy load-balancing.
* Rozkład ruchu pomiędzy kilkoma interfejsami WAN, z automatyczną diagnostyką łącz oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. Przy podejmowaniu decyzji o przełączeniu ruchu na bramę zapasową poza sondowaniem przy użyciu protokołów ICMP czy TCP brane muszą być pod uwagę również takie kryteria jak jitter, opóźnienie czy utrata pakietów.
* Obsługa routingu statycznego dla ruchu unicast i multicast.
* Obsługa protokołów routingu dynamicznego (RIP, BGP, OSPF).
* Obsługa Protocol Independent Multicast Sparse Mode (PIM-SM).
* Możliwość przekierowania ruchu do nadrzędnych serwerów proxy (upstream/parent proxy) dla IPv4 i IPv6.
* Rozwiązanie powinno pozwolić na definiowanie niezależnych od reguł zapory polis NAT.
* Rozwiązanie powinno pozwalać na tworzenie reguł NAT typu MASQ, SNAT, DNAT
* Możliwość elastycznego kształtowania pasma (Traffic Shaping) dla sieci, użytkowników i aplikacji.
* Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity muszą być przyznawane cykliczne lub niecykliczne.
* Mechanizmy optymalizujące ruch VoIP.
* Podczas klasyfikacji usług rozwiązanie musi uwzględniać wartości Differentiated Services Field Codepoints (DSCP) zawarte w nagłówkach IPv4 jak i IPv6.
* Do kształtowania ruchu wykorzystywane muszą być polisy, którym nadać można odpowiedni priorytet.
* System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection).
* Możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP.
* Możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge).
* Serwer DHCP dla IPv4 oraz IPv6 i DHCP Relay.
* Wsparcie dla IEEE 802.3Q VLAN z możliwością konfiguracji niezależnych puli DHCP.
* Agregowanie linków fizycznych w oparciu o IEEE 802.3ad (LACP).
* Wsparcie dla usług Dynamic DNS takich jak np.. DynDNS, ZoneEdit, EasyDNS, DynAcces itp
* Wsparcie dla IPv6 wraz z tunelowaniem IP 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd).
* Obsługa ramek Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo).
* Tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych.
* Uwierzytelnianie użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta.
* Lokalna baza użytkowników.
* Możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+.
* Uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm).
* Uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO);
* Uwierzytelnianie użytkowników za pośrednictwem agenta
* Captive Portal jako podstawowy mechanizm uwierzytelniania użytkowników w sieci.
* Uwierzytelnieni użytkownicy muszą móc samodzielnie pobrać plik instalacyjny agenta do uwierzytelniania, plik instalacyjny klienta VPN oraz plik z konfiguracją klienta SSL VPN
* Uwierzytelnieni użytkownicy muszą móc samodzielnie wyświetlić statystyki generowanego przez nich ruchu.
* Konfiguracja połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2.
* Połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN
* Mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN
* Mechanizmy IPsec VPN Failover i Failback
* Tworzenie wirtualnych interfejsów tunelowych dla IPsec site-to-site VPN i przesyłanie ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego.
* IPsec NAT Traversal, Dead Peer Detection oraz Xauth.
* Full Tunnel oraz Split Tunnel dla połaczeń IPsec client-to-site VPN jak i SSL client-to-site VPN.
* Bezpłatne oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN.
* połączenia L2TP over IPsec.
* Monitorowanie logów ruchu w czasie rzeczywistym.
* Składowanie oraz archiwizacja logów.
* Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
* Narzędzie do graficznej analizy logów.
* Narzędzie analizy incydentów bezpieczeństwa
* Monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali.
* Przeglądanie logów przy zastosowaniu funkcji filtrujących.
* Wysyłanie raportów via email.
* Eksport raportów do plików PDF, HTML i CSV.
* Możliwość wysyłania logów systemowych do serwerów syslog
* Podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza
* Podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację
* Możliwość zanonimizowania danych w raportach.
* Automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora.
* Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie 5000 sygnatur.
* Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń
* Tworzenie własnych sygnatur IPS
* Selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS.
* Wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet.
* Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP.
* Rozwiązanie powinno wykorzystywać silnik antywirusowy producenta rozwiązania.
* Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.
* System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME.
* Filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek.
* Emulacja skryptów Java.
* Live-lookups t.j. weryfikacja w trybie rzeczywistym bazy zagrożeń producenta
* Ręczna aktualizacja przez pobraną wcześniej bazę sygnatur (Air Gap Pattern Updates)
* Inspekcja ruchu SSL wraz z walidacją certyfikatów.
* Inspekcja ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2.
* Inspekcja ruchu TLS przeprowadzana niezależnie od użytego portu TCP.
* Blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443).
* Tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web.
* Tworzenie globalnych wyjątków inspekcji dla: wyrażeń regularnych, kategorii stron, domen i subdomen.
* Filtrowanie stron web oparte o predefiniowane kategorie z możliwością tworzenia własnych kategorii stron.
* Tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy.
* Polityki filtrujące ruch Web muszą umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól.
* System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web.
* Administrator musi mieć możliwość modyfikowania treści komunikatu w tym dodania logo organizacji.
* Baza danych opisująca co najmniej 3000 aplikacji
* Automatyczna aktualizacja sygnatur aplikacji.
* Wykrywanie i kontrola mikro-aplikacji.
* Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu czy protokołu, na podstawie głębokiej analizy pakietów.
* Blokowanie kategorii aplikacji takich jak np. P2P, Instant Messenger, Proxy and Tunnel, Remote Access, Social Networking, Streaming Media itp.
* Tworzenie własnych grup aplikacji na potrzeby polityk SD-WAN.
* Rozwiązanie klasy Sandbox do ochrony przez zagrożeniami typu Zero-Day.
* Inspekcja i detonacja:
* plików wykonywalnych .exe, .com, .dll
* plików dokumentów.doc, .docx, .docm, .rtf., .pdf.,
* archiwów.zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab.
* Rozwiązanie nie może mieć ograniczeń co do liczby analizowanych plików.
* Analiza behawioralna kodu uruchamianego w środowiskach testowych
* Analiza pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu.
* Ochrona przed exploitami i złośliwym kodem ransomware.

## Montaż i konfiguracja urządzenia

-Wymagany, minimalny zakres prac:

1. Montaż urządzenia w szafie telekomunikacyjnej rack 19”
2. Pierwsze uruchomienie oraz utworzenie tymczasowego hasła administratora
3. Dodanie adresu odbiorcy notyfikacji systemowych i cyklicznie wykonywanych kopii konfiguracji.
4. Aktualizacja oprogramowania systemowego (firmware) do ostatniej publicznie dostępnej wersji
5. Nadanie adresacji interfejsom sieciowym wg, schematu:

|  |  |  |  |
| --- | --- | --- | --- |
| Interfejs | Adres | Strefa | Uwagi |
| Port1 |  | LAN |  |
| Port2 |  | WAN |  |
| Port3 |  | DMZ |  |

1. Konfiguracja adresów serwerów DNS;
2. Konfiguracja właściwej dla miejsca instalacji strefy czasowej oraz adresów serwerów NTP;
3. Konfiguracja statycznych tras routingu

|  |  |  |  |
| --- | --- | --- | --- |
| Sieć | Brama | Interfejs | Dystans administracyjny |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Definicja obiektów sieciowych

|  |  |  |
| --- | --- | --- |
| Nazwa | Adres | Opis |
|  |  |  |
|  |  |  |
|  |  |  |

1. Konfiguracja podstawowych reguł zapory sieciowej (przykład)..
   1. LAN to WAN (General) – komunikacja ze strefy LAN do strefy WAN. Ruch kierowany na bramę (adres IP). Uruchomiona inspekcja ruchu HTTP i FTP, egzekwowanie ogólnych polis IPS, Web, Application Control.
   2. DMZ to WAN (General) - komunikacja ze strefy DMZ do strefy WAN. Ruch kierowany na bramę (adres IP). Uruchomiona inspekcja ruchu HTTP i FTP, egzekwowanie ogólnych polis IPS, Web, Application Control.
   3. LAN to DMZ (General) – komunikacja ze strefy LAN do strefy DMZ
   4. DMZ to LAN (General) – komunikacja ze strefy DMZ do strefy LAN
   5. VPN to WAN (General) - komunikacja ze strefy VPN do strefy WAN. Ruch kierowany na bramę (adres IP). Uruchomiona inspekcja ruchu HTTP i FTP, egzekwowanie ogólnych polis IPS, Web, Application Control.
   6. VPN to LAN (General) – komunikacja ze strefy VPN do strefy LAN
   7. VPN to DMZ (General) – komunikacja ze strefy VPN do strefy DMZ
2. Uruchomienie ochrony Advanced Threat Protection w trybie Log and Drop.
3. Ograniczenie dostępu administracyjnego dla stref innych niż LAN i VPN.
4. Utworzenie wyjątku dla dostępu zdalnego od strony WAN dla wskazanego adresu IP/puli adresów IP;
5. Utworzenie kont użytkowników oraz konfiguracja dostępu zdalnego przez SSL VPN dla

|  |  |  |
| --- | --- | --- |
| Imię | Nazwisko | Firma |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Szkolenie dla 2 administratorów systemów bezpieczeństwa IT – 1 szt.

1. Szkolenie musi być dedykowane dla 2 administratorów sieci;
2. Szkolenie musi być przeprowadzone przez trenera certyfikowanego przez producenta urządzenia UTM.
3. Zaświadczenie o ukończeniu szkolenia dla uczestników;
4. Po ukończeniu szkolenia, uczestnicy muszą potrafić:
   1. Wyjaśnić, w jaki sposób dostarczony UTM pomaga chronić przed zagrożeniami bezpieczeństwa
   2. Skonfigurować reguły zapory, polityki i uwierzytelnianie użytkowników
   3. Zademonstrować ochronę przed zagrożeniami i powszechnie używane funkcje
   4. Wykonać początkową konfigurację zapory i skonfigurować wymagane ustawienia sieciowe
   5. Wykonać podstawowe zadania związane z rozwiązywaniem problemów, raportowaniem i zarządzaniem
5. Agenda minimalna:

* Czym jest urządzenie UTM;
* Zagadnienia dotyczące wdrażania zapory w typowych scenariuszach
* Wdrażanie zapory przy użyciu kreatora konfiguracji początkowej
* Aktywacja zapory;
* Nawigowanie i zarządzanie zaporą sieciową przy użyciu WebAdmin
* Pierwsze kroki ze strefami i interfejsami w zaporze sieciowej;
* Zaawansowana konfiguracja interfejsu;
* Wprowadzenie do routingu i SD-WAN w zaporze;
* Zaawansowana konfiguracja routingu i SD-WAN w zaporze;
* Rozwiązywanie problemów z routingiem w zaporze;
* Konfigurowanie DNS i DHCP w zaporze;
* Zarządzanie dostępem do urządzeń i certyfikatów;
* Zagadnienia dotyczące konfigurowania dostępu do urządzeń w zaporze;
* Pierwsze kroki z kształtowaniem ruchu w zaporze sieciowej;

Profile SD WAN

1. Tworzenie trasy opartej na zasadach dla scenariusza MPL
2. Konfigurowanie dostępu do urządzenia
3. Interfejsy mostkowe

Pierwsze kroki z regułami zapory i NAT w zaporze;

1. Zaawansowane zarządzanie regułami zapory
2. Rozwiązywanie problemów z regułami zapory
3. Zaawansowana konfiguracja NAT w zaporze
4. Rozwiązywanie problemów z regułami NAT w zaporze
5. Konfigurowanie odszyfrowywania TLS w zaporze
6. Kształtowanie ruchu sieciowego w zaporze

NAT z równoważeniem obciążenia

- Lokalna polityka NAT

Pierwsze kroki z Intrusion Prevention

- Zaawansowana konfiguracja IPS

- Włączanie zaawansowanej ochrony przed zagrożeniami

- Rozwiązywanie problemów z alertami ATP

Połączenia site-to-site;

- Łączenie witryn z zaporą

- Konfigurowanie sieci VPN typu Site-to-Site SSL w zaporze

- Pierwsze kroki z sieciami VPN typu Site-to-Site IPsec w zaporze

- Zaawansowana konfiguracja sieci VPN typu Site-to-Site IPsec w zaporze

- Pierwsze kroki ze zdalnymi urządzeniami Ethernet (RED) w zaporze;

- Tworzenie sieci VPN typu site-to-site IPsec

- Konfiguracja NATing sieci VPN

- Konfiguracja failover VPN

- Konfiguracja VPN opartego na trasach

Autentykacja

- Wprowadzenie do uwierzytelniania w zaporze

- Konfigurowanie serwerów i usług uwierzytelniania w zaporze

- Konfigurowanie SSO w zaporze

- Wprowadzenie do uwierzytelniania w zaporze

- Zaawansowana konfiguracja STAS

- Włączanie uwierzytelniania wieloskładnikowego w zaporze

- Konfiguracja logowania jednokrotnego za pomocą STAS

- Uwierzytelnianie użytkowników za pośrednictwem sieci VPN typu site-to-site

Ochrona sieci;

- Konfigurowanie ochrony sieciowej;

- Limity ochrony sieciowej i kształtowanie ruchu

- Instalacja certyfikatów SSL CA

- Konfiguracja reguły inspekcji TLS

- Konfiguracja niestandardowej polityki internetowej dla użytkowników

Kontrola aplikacji:

- Kształtowanie ruchu aplikacji na zaporze;

Dostęp zdalny:

- Pierwsze kroki z sieciami VPN zdalnego dostępu w zaporze;

- Zaawansowana konfiguracja sieci VPN zdalnego dostępu Sophos w zaporze;

- Konfigurowanie dostępu bez klienta w zaporze;

- Auto provisioning;

Zabezpieczenie sieci wifi:

- Wdrażanie ochrony sieci bezprzewodowej w zaporze;

- Uwierzytelnianie sieci bezprzewodowej

- Tworzenie punktów dostępowych w zaporze;

- Konfigurowanie sieci bezprzewodowych Mesh

Logowanie i raportowanie:

- Uruchamianie i dostosowywanie raportów;

- Zarządzanie logami i powiadomieniami;

Zarządzanie centralne zaporą:

Podsumowanie.