Załącznik A do SWZ

OPIS PRZEMIOTU ZAMÓWIENIA

1. System bezpieczeństwa typu firewall.

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa oraz musi być zbudowany w sposób redundantny/nadmiarowy, tak aby niedostępność dowolnego elementu systemu nie wpływała na ciągłość świadczenia usługi. W przypadku realizacji wszystkich funkcji przez pojedyncze urządzenie, wymagana minimalna ilość urządzeń to 2. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej wykonawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 9 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy oraz zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 2 portami Gigabit Ethernet RJ-45 do zarządzania.
   - 16 portami GE RJ45
   - 8 gniazdami GE SFP
   - 8 gniazdami 10 GE SFP+

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w redundantne zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 7,7 mln jednoczesnych połączeń oraz 500.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 78 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 70 Gbps dla pakietów 64 B.
4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 28 Gbps.
5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 55 Gbps.
6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 11 Gbps.
7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 10 Gbps.
8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 8 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

Polityki Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    - Translację jeden do jeden oraz jeden do wielu.
    - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu: RIPv2, OSPF, BGP oraz PIM.
2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Kontrola Antywirusowa

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Ochrana przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.

3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie

1. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Ich zakres: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen **na okres 24 miesięcy**.

Gwarancja oraz wsparcie

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta lub jego autoryzowanego przedstawiciela przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu podmiot musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

2. Licencje i wsparcie do istniejącego systemu bezpieczeństwa

Zamawiający oczekuje dostawy wsparcia i dostępu do sygnatur dla urządzeń firmy Fortinet na okres dwóch lat dla następujących produktów:

1. FortiAnalyzer-300F FortiGuard Indicators of Compromise (IOC) Service
2. FortiAnalyzer-300F FortiCare Premium Support
3. FortiGate-200F Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)
4. FortiGate-200F Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)
5. FortiAuthenticator - VM License FortiCare Premium Support (1 - 500 USERS)

3. Oprogramowanie wspomagające system bezpieczeństwa

Kluczowe funkcjonalności:

1. System wspiera bazy danych PostgreSQL oraz MSSQL.
2. System może obsłużyć sieć rozproszoną umożliwiając instalację wieloserwerową na zasadzie serwer centralny i serwery pośredniczące.
3. Podstawowym modułem systemu do monitoringu infrastruktury IT jest moduł do monitorowania i obrazowania stanu urządzeń sieciowych.
4. System musi posiadać odpowiednie licencje do obsługi co najmniej 70 urządzeń.
5. System posiada możliwość rozszerzenie funkcjonalność o dodatkowe moduły:
   a) Moduł analizy wysycenia pasma w technologii NetFlow,
   b) Moduł do zarządzania konfiguracją aktywnych urządzeń sieciowych,
   c) Modułu zarządzania adresacją IP oraz portami przełączników sieciowych,
   d) Moduł analizy logów zapór sieciowych.
6. Wszystkie moduły systemu są dostępne z poziomu jednej i jednolitej konsoli użytkownika bez konieczności przełączania się między odrębnymi systemami i bez konieczności instalacji dodatkowych wtyczek.
7. System pozwala na aktywowanie i dezaktywowanie poszczególnych modułów bez potrzeby ingerencji w pliki systemowe (przy założeniu, że wgrana jest licencja na wykorzystanie tych modułów).
8. Architektura systemu daje możliwość instalacji serwerów dystrybucyjnych w lokalizacjach zdalnych, umożliwiając zarządzanie urządzeniami końcowymi bez konieczności łączenia się z serwerem głównym i nadmiernego obciążania łącza.
9. System umożliwia dywersyfikację uprawnień przynajmniej na dwa poziomy – administrator i użytkownik tylko do odczytu
10. System daje możliwość zawężenia zakresu dostępu do określonych monitorowanych urządzeń, grup, modułów poszczególnemu użytkownikowi.
11. System pozwala każdemu użytkownikami na tworzenie własnych, dedykowanych pulpitów nawigacyjnych.
12. System zawiera osadzony moduł umożliwiający tworzenie zautomatyzowanych, wielopoziomowych procedur IT pozwalających na definiowanie ciągów weryfikacji, działań i reakcji na zdarzenia w sieci bez konieczności tworzenia skryptów i programowania.
13. System pozwala na cykliczne (wg zdefiniowanego w systemie harmonogramu) skanowanie zdefiniowanych segmentów sieci w celu wykrywania nowych urządzeń i automatycznego rozpoznawania i dodawania ich do monitoringu.

14. System umożliwia wykonanie automatycznych działań po wykryciu nowego urządzenia (np. przydzielenie do określonej grupy, dodanie określonych parametrów monitorowania, dodanie określonych profili powiadomień w oparciu o schemat nazwy DNS, adresu IP, kategorię lub typ urządzenia).
15. Konfiguracje urządzeń sieciowych pozyskiwane przez system są przechowywane w bazie danych systemu a nie w formie plików natywnych zarządzanych urządzeń.
16. Przechowywane w bazie danych odczytane konfiguracje są zaszyfrowane.
17. System pozwala na oznaczenie zarchiwizowanych wersji konfiguracji urządzeń jako konfiguracji bazowej, aktualnie funkcjonującej lub roboczej.
18. System pozwala przeglądać dane z czujników sprzętowych związanych z macierzami dyskowymi dla serwerów ze sprzętem HP.
19. System umożliwia wysyłanie przez użytkowników wiadomości do prywatnych kanałów Slack, jeżeli odpowiedni profil użytkownika został zaproszony do kanału.
20. System obsługuje monitorowanie WLC w oparciu o dostawców dla: Aruba, Cisco, Huawei, Autelan, Hongxin i H3C.
21. System obsługuje monitorowanie sprzętu oparte na IPMI dla wybranych dostawców.
22. System pozwala na monitorowanie Meraki REST API.
23. System posiada funkcję „SDN monitoring for Cisco Application Centric Infrastructure (ACI)" pozwalającą monitorować sieć szkieletową, najemców, grupy punktów końcowych oraz ogólną wydajność środowiska Cisco ACI.
24. System pozwala na integrację z ServiceDesk Plus MSP.
25. System pozwala zbiorczo aktualizować protokół monitorowania dostępności (ICMP, TCP, i SNMP) dla urządzeń ze strony Inventory.
26. System umożliwia planowanie i eksportowanie zintegrowanych raportów w formacie pliku XLS.
27. System monitoruje stan dysku, stan portu, stan wentylatora, stan zasilania, stan baterii, wartość czujnika temperatury dla urządzeń NetApp ONTAP (CLUSTER).
28. System monitoruje stan dysku i kondycję dysku modeli urządzeń z serii IBM DS.
29. System pozwala na włączanie / wyłączanie modułów dodatkowych przez użytkownika.
30. System pozwala wybrać użytkownikowi pokazywanie / ukrywanie modułów dodatkowych zgodnych z posiadanymi uprawnieniami.
31. System pozwala w zakresie zarządzania użytkownikiem na tworzenie ról niestandardowych.
32. System pozwala na monitorowanie VPN (Site-to-Site) realizowanych przez co najmniej następujących dostawców: Cisco, Watchguard i Fortinet.
33. System posiada do komunikacji agent – serwer „Push Mode", który powiadomi odpowiednich agentów, aby skontaktowali się z serwerem i zaktualizowali szczegóły monitora. Pozwala to użytkownikom na większe skalowanie poprzez optymalizację częstotliwości komunikacji przez agentów i zmniejszenie zużycia przepustowości.
34. System pozwala na dodawanie przez użytkowników 2-bajtowych znaków w notatkach o alarmach.
35. System umożliwia włączenie uwierzytelniania dwuskładnikowego (TFA).
36. System obsługuje format czasu ISO 8601 (yyyy-MM-ddThh:mm:ss).
37. System obsługuje zmianę znaku produktu, który pojawia się na stopce stron eksportowanych raportów.
38. System pozwala na wyświetlenie strony „Aktywacji licencji" i „Zarządzania licencją" tylko dla użytkowników z dostępem administratora do wszystkich modułów.
39. System wyświetla narzędzie Trace Route jako TraceRoute w zestawie narzędzi.
40. System posiada zmienioną logikę resetowania hasła. Zostało to zaktualizowane w celu zwiększenia bezpieczeństwa.
41. System posiada opcję edycji widżetu na dashboardzie w odpowiedzi interfejsu API.

Wymagania systemowe

1. Wszystkie składniki systemu pochodzą od jednego producenta.
2. System działa zarówno w środowisku Windows Server w wersji co najmniej 2008 (wersje zarówno 32 jaki 64 bit) jak i w 64bit środowisku Linux.
3. Wszystkie elementy systemu mają wsparcie dla środowiska wirtualnego opartego o VMware.
4. Interfejs oprogramowania oraz konfiguracji dostępny jest w całości z poziomu przeglądarki internetowej (Internet Explorer w wersji 10 lub nowszej, Mozilla 44 lub nowszej, Chrome 47 lub nowszej) bez potrzeby instalacji tzw. grubego klienta.

Moduł do monitorowania aktywnych urządzeń sieciowych

1. System umożliwia monitorowanie systemów bez instalacji dodatkowych klientów na serwerach.
2. System posiada funkcjonalność aktywnego monitorowania urządzeń:
   a) Środowisk z systemem operacyjnym Microsoft Windows przez poświadczenia WMI,
   b) Środowisk Linux/Unix przez wykorzystanie poświadczeń CLI (dostęp przez SSH/Telnet),
   c) Pozostałych urządzeń sieciowych obsługujących protokół SNMP v1/2/3.
3. System musi posiadać odpowiednie licencje do obsługi co najmniej 70 urządzeń.
4. System umożliwia logowanie lokalne, z wykorzystaniem poświadczeń domenowych Active Directory lub z wykorzystaniem serwera RADIUS.
5. System umożliwia dywersyfikację uprawnień przynajmniej na dwa poziomy – administrator i użytkownik tylko do odczytu
6. System musi posiadać możliwość uruchomienia co najmniej 5 kont administracyjnych,
7. System daje możliwość zawężenia zakresu dostępu do określonych monitorowanych urządzeń, grup, modułów poszczególnemu użytkownikowi.
8. System pozwala każdemu użytkownikami na tworzenie własnych, dedykowanych pulpitów nawigacyjnych.
9. System posiada funkcjonalność pasywnego monitorowania urządzeń sieciowych przez odbieranie i procesowanie trapów SNMP.
10. Oprogramowanie umożliwia monitoring hostów środowisk wirtualnych VMware i HyperV.
11. System po dodaniu hosta środowiska wirtualnego umożliwia natychmiastowe monitorowanie maszyn wirtualnych znajdujących się na tym hoście,
12. Podczas monitorowania hosta i jego maszyn wirtualnych system pozwala na stworzenie mapy zależności między monitorowanymi środowiskami.
13. W przypadku monitorowania środowisk z systemem Windows, system pozwala dodatkowo na monitorowanie usług, aktywnych procesów Windows oraz eventów w dzienniku zdarzeń Windows.
14. System posiada funkcjonalność automatycznego generowania map sieci na z wykorzystaniem mechanizmów CDP, LLDP, IPROUTE, FDP, ARP.
15. System posiada wbudowany, obszerny zestaw bibliotek MIB.
16. System pozwala na dodawanie i przeglądanie nowych bibliotek MIB,
17. System pozwala na tworzenie własnych monitorów SNMP z wykorzystaniem dodanych bibliotek MIB.
18. System posiada funkcjonalność graficznego prezentowania ważnych wskaźników wydajności i sygnalizacji zagrożeń a uprawnieni użytkownicy powinni mieć możliwość definiowania własnych wskaźników.
19. System umożliwia prezentację grafów ruchu i wydajności interfejsów sieciowych w czasie rzeczywistym.

20. System zawiera zestaw wbudowanych narzędzi administracyjnych takich jak Trace Route, Ping, RDP, Telnet.
21. System umożliwia zdefiniowanie automatycznego śledzenia statusu najważniejszych elementów w monitorowanym środowisku informatycznym i wygenerowanie alertów na podstawie uprzednio zdefiniowanych warunków brzegowych.
22. System pozwala na konfigurację następujących działań w momencie wystąpienia alarmu:
    a) Wysłanie powiadomienia Email,
    b) Wysłanie powiadomienia SMS,
    c) Wysłanie powiadomienia na kanale Slack,
    d) Wykonanie komendy w wierszu poleceń,
    e) Uruchomienie programu/skryptu,
    f) Wysłanie wiadomości SysLog,
    g) Wygenerowanie trapów SNMP,
    h) Zarejestrowanie zgłoszenia,
    i) Rejestrację ticket'u w osobnym systemie wsparcia użytkownika integrującym się z omawianym systemem monitorowania.
23. System pozwala na wgląd w bieżące i historyczne dane o wydajności w formie tabel i wykresów.
24. System umożliwia zdefiniowanie automatycznie generowanych raportów, według ustalonego harmonogramu (np. dziennych, tygodniowych) i przesyłanie ich za pomocą poczty elektronicznej w formacie PDF, XLS.
25. Oprogramowanie umożliwia monitoring błądzenia pakietów w sieci WAN oraz technologii VoIP z wykorzystaniem technologii Cisco IPSLA
26. Oprogramowanie umożliwia monitoring kontrolerów domeny Active Directory, a w szczególności:
    a) Procesów LSASS,
    b) Procesów NTFRS,
    c) Statystyk bazy danych,
    d) Uwierzytelnienia Kerberos na sekundę,
    e) Replikacja usługi Active Directory,
    f) Nowe połączenia LDAP,
    g) NTLM Authentications na sekundę.
27. Statystyki monitorowania Active Directory są dostępne odrębnym widoku zbiorczym.
28. System umożliwia monitoring serwerów MS SQL i Exchange.
29. System umożliwia monitoring komponentów IT z wykorzystaniem własnych skryptów napisanych w Powershell, Linux shell script, VBScript, Perl lub Python oraz pozwala na przypisanie wartości brzegowych oraz profili powiadomień dla wyników tych skryptów.
30. System pozwala na uruchamianie skryptów monitoringu na serwerze centralnym i lokalnie.
31. System umożliwia automatyczne uruchamianie skryptów naprawczych i weryfikacyjnych w sytuacji przekroczenia wartości brzegowych dla zdefiniowanych monitorów.
32. System umożliwia tworzenie zależności między monitorowanymi urządzeniami na zasadzie Parent-Child w celu ograniczenia alarmów z urządzeń niemożliwych do monitorowania ze względna na niedostępności urządzeń sieciowych.
33. System pozwala na definiowanie harmonogramów okien prac konserwacyjnych w celu zmniejszenia ilości powtórzeń alarmów.
34. System posiada wbudowana funkcjonalność monitorowania systemów składowania danych
35. Moduł umożliwia monitorowanie dysków RAID z wykorzystaniem przynajmniej protokołów SNMP/CLI/SMI-S oraz API różnych producentów systemów składowania.
36. Moduł pozwala monitorować i dostarczać informacje w postaci raportów o przynajmniej następujących obszarach RAID:

a) Zasoby fizyczne,
b) Kontrolery,
c) Zasoby logiczne,
d) LUNy,
e) Partycje,
f) Grupy RAID,
g) Grupy dysków wirtualnych,
h) Woluminy,
i) Grupy woluminów,

37. Moduł pozwala monitorować i dostarczać informacje w postaci raportów o bibliotekach taśmowych różnych producentów przynajmniej w następujących obszarach:
    a) Zasoby fizyczne
    b) Sterowniki taśm
    c) Porty taśm
    d) Sterowniki dostępu
    e) Porty bibliotek SCSI
    f) Zasoby logiczne
    g) Partycje
    h) Napędy
38. Moduł zapewnia możliwość raportowania prognozującego wysycenie systemów składowania w przyszłości według trendu wzrostu.
39. Moduł opiera się na standardowych bibliotekach MIB opracowanych przez SNIA w obszarze przełączników składowania.
40. Moduł posiada HeatMap'y wizualizujące stan całej sieci w czasie rzeczywistym z jednej strony.
41. System posiada możliwość wirtualizacji dla VMware i Hyper-V, zapewniając wizualną reprezentację relacji między hostami, klastrami i maszynami wirtualnymi.
42. System pozwala na przypisywanie niestandardowych własnych pół do wszystkich urządzeń, w celu uproszczenia zarządzania urządzeniami.
43. System pozwala na importowanie pliku CSV, który będzie nadpisywał wartości pól dodatkowych.
44. System posiada integrację z ServiceNow, pozwalając na:
    a) Rejestrowanie ticketów
    b) CMDB Auto-Sync - umożliwia synchronizację wszystkich zasobów z OPM z ServiceNow
    c) Aktualizacje wszystkich incydentów w ServiceNow w czasie rzeczywistym
    d) Umożliwia agentowi bezpośredni dostęp do migawki urządzenia i migawki alarmu urządzenia zsynchronizowanego z OPM.
45. System posiada możliwość monitorowania EMC Isilon.
46. System umożliwia przypisanie podstawowych monitorów wydajności SNMP podczas wykrywania serwerów, które zostały wykryte bez monitorów domyślnych z wykorzystaniem ważnych poświadczeń SNMP.
47. System umożliwia synchronizację urządzeń, interfejsów i alertów po dodaniu jako dodatek do APM w celu uzyskania lepszej wydajności.
48. System pozwala na użycie opcji kryterium „ifAlias" podczas odkrywania interfejsów sieciowych.
49. System wyświetla podział na strony w opcji „edytuj regułę" dla listy silnika wykrywania reguł, aby wyświetlić wszystkie skonfigurowane kryteria i działania.
50. System posiada optymalizację wydajności dla procesu aktualizacji poświadczeń SNMP v1/v2.
51. System pozwala wyświetlić opcje ustawień raportu w interfejsie użytkownika tylko dla użytkowników z dostępem do zapisu.

52. System wyklucza dostęp do opcji ponownego ładowania w widoku zależności magazynu pamięci na stronie migawki urządzenia dla użytkowników z prawami dostępu „Zapisu Lub Odczytu”.
53. W systemie usunięto ustawienia Trap i opcje Trap Viewer w MSP Central.
54. Dzienniki workflow są tylko wyświetlane z poziomu oprogramowania.
55. System posiada opcję planowania wstrzymania alarmów dla workflow.
56. System pozwala na dostosowanie szablonu HTML dla profili powiadomień e-mail.
57. System posiada raport „wszystkie maszyny wirtualne”, aby wyświetlić dostępne maszyny wirtualne w aplikacji od wielu dostawców wraz z ich stanem zasilania.
58. System obsługuje wiele sond aplikacji dla klientów indywidualnych.
59. System obsługuje znaki dwubajtowe w polu „Wiadomości” podczas akcji generowania alarmu oraz w polach „Temat” i „Wiadomość” podczas wysyłania e-mail.
60. System posiada mechanizm przerwania wykonywania skryptu, jeśli nie została określona pełna ścieżka katalogu wykonania – zapewnia to zwiększenie bezpieczeństwa pracy aplikacji.
61. System pozwala monitorować środowisko Cisco ACI przy użyciu zarządzania IP Out-of-Band dla APIC i Fabrics.
62. System pozwala na monitorowanie adresów URL dla Standard Edition za pośrednictwem add-on.
63. System posiada zabezpieczenie przed atakami typu zipslip podczas przetwarzania zbieranych danych w postaci oczyszczenia ścieżek dla urządzeń monitorujących opartych na agentach.
64. System obsługuje import certyfikatu i przetworzenie go dla hosta Xen podczas nawiązania połączenia z serwerem Xen.
65. System obsługuje dodatek NCM dla wersji aplikacji MSP.
66. System obsługuje monitor dla urządzenia magazynu Dell EMC Powermax.
67. System posiada obsługę interfejsów V3 Admin API.
68. System umożliwia łatwą obsługę pobierania, instalowania oraz konfigurowania wtyczki APM poprzez kliknięcie przycisku w zakładce Application.
69. System posiada biblioteki JavaScript 3D w wersji r137.
70. System w wersji MSP umożliwia zbiorcze zarządzanie urządzeniami i interfejsami na stronie Inventory.
71. System posiada monitor WMware, dzięki któremu można monitorować miejsce na dysku maszyn wirtualnych VMware pod warunkiem instalacji niezbędnych narzędzi na maszynie wirutalnej.
72. System posiada funkcję bezpieczeństwa „File Integrity”, która umożliwia skanowanie w poszukiwaniu wszelkich plików zagrożeń lub zmodyfikowanych plików w katalogu z zainstalowaną aplikacją.
73. System posiada wsparcie dla monitorowania systemów Windows Serwer 2022 oraz Windows 11.

Moduł do zarządzania konfiguracją urządzeń sieciowych

1. Moduł zarządzania konfiguracją urządzeń sieciowych jest wbudowanym modułem systemu monitoringu infrastruktury IT na poziomie konsoli systemu.
2. Moduł działa bez konieczności instalacji dodatkowego oprogramowania.
3. Moduł pozwala na zarządzanie konfiguracją urządzeń sieciowych a w szczególności:
   a) Składowanie konfiguracji,
   b) Automatyczne tworzenie kopii zapasowych,
   c) Wersjonowanie kopii zapasowych,
   d) Porównywanie różnych wersji konfiguracji
   e) Tworzenie kopii zapasowych wg harmonogramu,
   f) Dystrybucję konfiguracji i fragmentów konfiguracji na wybranej grupie urządzeń oraz grupowanie ich z odpowiednimi vendorami.
   g) Weryfikację konfiguracji z politykami zgodności

74. Moduł może automatycznie wykrywać zmiany w konfiguracji urządzeń sieciowych,
75. System musi posiadać odpowiednie licencje do obsługi co najmniej 70 urządzeń,
76. Moduł pozwala na weryfikowanie zgodność konfiguracji i zmian w konfiguracji z narzuconymi i zdefiniowanymi standardami i politykami.
77. Konfiguracje urządzeń sieciowych pozyskiwane przez moduł są przechowywane w bazie danych modułu a nie w formie plików natywnych zarządzanych urządzeń.
78. Przechowywane w bazie danych odczytane konfiguracje są zaszyfrowane
79. Moduł pozwala na oznaczenie zarchiwizowanych wersji konfiguracji urządzeń jako konfiguracji bazowej, aktualnie funkcjonującej lub roboczej.
80. Moduł posiada możliwość oceny podatności, w tym posiada widok typu „Grid View".
81. Moduł posiada możliwość zarządzania urządzeniami za pomocą adresu IPv6.
82. Moduł pozwala na aktualizację nazw, interfejsów sieciowych oraz sieci VLAN przy pomocy odpytywania SNMP.
83. Moduł potrafi automatycznie zaktualizować adres IP urządzenia skanowanego, gdy ten się zmieni i wykryje to główny program.
84. Moduł posiada wbudowane API pozwalające na:
    a) Listowanie wszystkich komend,
    b) Eksportowanie konfiguracji urządzeń,
    c) Zatwierdzanie próśb,
    d) Dodawanie urządzeń,
    e) Przypisywanie poświadczeń,
    f) Usuwanie szablonu,
    g) Uruchamianie skanowania sieci
    h) Używania pakietu ICMP w celu testowania dostępności,
    i) Dodawania niestandardowego pola,
    j) Wykonywania kwerendy na własnej bazie danych,
85. Moduł pozwala na eksport podłączonych urządzeń do formatu XLSX.
86. Moduł posiada wbudowane automatyzacje, pozwalające na odblokowanie SNMP na urządzeniach Cisco.
87. Moduł posiada widok CCTV.
88. Moduł posiada możliwość wykonywania akcji typu REST dla urządzeń typu:
    a) Fortigate,
    b) Palo Alto,
89. Moduł pozwala na kopię zapasową out-of-the-box producentów urządzeń:
    a) Alcatel,
    b) AlliedTelesis,
    c) Arbornetworks
    d) Arista,
    e) Avaya,
    f) Belden,
    g) Brocade,
    h) Calix,
    i) Ciena,
    j) CheckPoint,
    k) Cisco,
    l) Dax,
    m) DCNetworks,
    n) Dell,

o) Dlink,
p) Extreme Networks,
q) F5,
r) Fortinet,
s) Fujitsu,
t) H3C,
u) HPE,
v) Huawei,
w) IBM,
x) Junpier,
y) NEC,
z) Nokia,
aa) Nortel,
bb) PaloAlto,
cc) Siemens,
dd) Symatec,

90. Moduł posiada sekcję audytową pozwalającą na audyt wszystkich historycznych akcji wykonywanych na urządzeniach, wraz z informacją, kiedy i przez kogo.
91. Moduł pozwala tworzyć tagi i używać ich do grupowania użytkowników, urządzeń, grup urządzeń, harmonogramów, konfiguracji, zasad zgodności, profili poświadczeń i powiadomień o zmianach.
92. Moduł pozwala wykluczać blok konfiguracji z uwzględniania podczas identyfikowania zmian między dwiema wersjami konfiguracji.
93. Moduł pozwala na integrację z ServiceNow i synchronizację urządzeń sieciowych z ServiceNow CMDB z NCM Inventory.
94. Moduł pozwala wykrywać urządzenia Palo Alto działające na podatnych wersjach oprogramowania.
95. Moduł pozwala w obszarze zarządzania użytkownikami na tworzenie niestandardowych ról.
96. Moduł pozwala zautomatyzować proces kojarzenia profili poświadczeń z urządzeniami za pomocą reguł poświadczeń.
97. Moduł posiada funkcję reguł poświadczeń.
98. Moduł posiada możliwość edycji nazwy grupy urządzeń.
99. Moduł pozwala na włączanie / wyłączanie modułów dodatkowych przez użytkownika.
100. Moduł pozwala użytkownikom wybrać pokazywanie / ukrywanie modułów dodatkowych, do których mają uprawnienia.
101. Moduł pozwala zautomatyzować proces kojarzenia profili poświadczeń z urządzeniami za pomocą reguł poświadczeń.
102. Moduł pozwala na generowanie raportów audytu bezpieczeństwa dla urządzeń Palo Alto Firewall.
103. Moduł obsługuje uwierzytelnianie klucza publicznego do łączenia się z urządzeniami.
104. Moduł pozwala na integrację z ServiceDesk Plus OnDemand i włączenie tworzenia zgłoszeń dla alertów o błędach tworzenia kopii zapasowych i żądań zatwierdzania konfiguracji.
105. Moduł obsługuje REST API dla urządzeń Arista.
106. Moduł posiada szablon REST dla urządzeń PFSense.
107. Moduł obsługuje poświadczenia REST dla urządzeń PFSense.
108. Moduł otrzymał nowe Configlety REST dla urządzeń PFSense.
109. Moduł otrzymał szczegółowe podsumowanie dla szablonów REST
110. Moduł pozwala sprawdzić listę szablonów urządzeń CLI powiązanych z konkretnym szablonem REST.

111. Moduł posiada zmieniony wygląd okna dialogowego potwierdzenia.
112. Moduł obsługuje konfigurację urządzeń HPE Aruba OS w oparciu o interfejs REST API.

Moduł do zarządzania adresacją IP oraz portami przełączników sieciowych.

1. Moduł zarządzania adresacją IP oraz portami przełączników sieciowych jest wbudowanym modułem systemu monitoringu infrastruktury IT na poziomie konsoli systemu.
2. Moduł działa bez konieczności instalacji dodatkowego oprogramowania.
3. Moduł obsługuje automatyczne wykrywanie segmentów sieci w infrastrukturze IT.
4. Moduł pozwala na skanowanie ręczne lub według zdefiniowanego harmonogramu segmentów sieci w celu identyfikacji wolnych i zajętych adresów IP.
5. System musi posiadać odpowiednie licencje do obsługi co najmniej 2300 adresów IP,
6. Moduł obsługuje adresacje w wersjach IPv4 i IPv6.
7. Moduł pozwala na skanowanie przełączników sieciowych w celu weryfikacji dostępności i zajętości portów oraz wskazania przyłączonych do portów urządzeń.
8. System pozwala na identyfikację nieznanych urządzeń w sieci.
9. Jeśli nieznane urzdzie zostało podłączone fizycznie do portu na monitorowanym przełączniku/routerze system daje możliwość zablokowania tego urządzenia przez administracyjne zablokowanie portu na przełączniku/routerze.
10. Moduł umożliwia integrację z Active Directory w celu przypisania adresowi IP nazwy obiektu w domenie.
11. Moduł pozwala na prezentację podłączonych urządzeń do switcha,
12. Moduł pokazuje przyczynę niepowodzenia skanowania zakresu IP, przy pomocy DHCP.
13. Narzędzie potrafi wybudzać urządzenia sieciowe przy pomocy Wake-On-Lan.
14. Moduł wspiera możliwość skonfigurowania zabezpieczenia typu FailOver, które pozwoli na ciągłą pracę, w przypadku awarii jednego z serwerów.
15. Moduł pozwala na pobranie danych typu ARP z urządzeń Cisco.
16. Moduł posiada zgodność kolumny „Typ karty sieciowej” zgodnie z standardem IEEE OUI.
17. Moduł ma możliwość monitorowania serwera DHCP od Cisco.
18. Moduł ma możliwość monitorowania serwera DHCP od Fortinet.
19. Moduł pozwala identyfikować konflikty IP za pomocą Managera adresów IP.
20. Moduł pozwala oprócz tabel routingu IP i wyszukiwania serwerów DHCP, wykrywać również podsieci z tabel LipRouting, w przypadku urządzeń Cisco.
21. Moduł pozwala w obszarze zarządzania użytkownikami na tworzenie ról niestandardowych.
22. Moduł obsługuje określanie zakresu użytkownika. Można skonfigurować odpowiedni dostęp do grup drzewa Managera adresów IP i mapowania portów przełącznika.
23. Moduł pozwala importować nazwę DNS i stan adresów IP,
24. Moduł obsługuje określanie zakresu użytkowników. Pozwala to skonfigurować system, aby umożliwić użytkownikowi odpowiedni dostęp do grup drzewa Menadżera adresów IP i mapowania portów switchy.
25. Moduł pozwala wyświetlić szczegóły zalogowanego użytkownika dotyczące użytkowników AD logujących się do monitorowanych urządzeń sieciowych
26. Moduł pozwala przechowywać pliki kopii zapasowej menadżera plików konfiguracyjnych w zmienionej lokalizacji.

Moduł do analizy logów zapór sieciowych

1. Moduł analizy logów zapór sieciowych jest wbudowanym modułem systemu monitoringu infrastruktury IT na poziomie konsoli systemu.
2. Moduł działa bez konieczności instalacji dodatkowego oprogramowania.

3. Moduł umożliwia analizę logów zapór sieciowych od wielu producentów i prezentację analizy ruchu sieciowego przechodzącego przez te zapory sieciowe.
4. System musi posiadać odpowiednie licencje do obsługi co najmniej 2 zapór sieciowych.
5. Moduł umożliwia audyt aktywności użytkowników infrastruktury IT w sieci Internet.
6. Moduł umożliwia analizę polityk i reguł skonfigurowanych na zaporach sieciowych pod kątem ich wykorzystania.
7. Moduł umożliwia analizę tuneli VPN i serwerów proxy w czasie rzeczywistym.
8. Moduł umożliwia przeszukiwanie surowych danych w logach zapór sieciowych.
9. Moduł obsługuje format Juniper SRX, LEEG od Palo Alto oraz logi z pfSense.
10. Moduł pozwala na przeszukiwanie reguł pod kątem odpowiednich adresów IP/obiektów.
11. Moduł pozwala na eksport danych w formatach PDF, CSV oraz XLS.
12. System pozwala na eksport danych w PDF'ie do 50000 wpisów per strona.
13. Moduł posiada raporty typu "drill-down", dzięki którym możemy przechodzić do coraz bardziej szczegółowych elementów.
14. Moduł potrafi pokazywać niewykorzystywane reguły firewall'owe.
15. Moduł wspiera iptables oraz potrafi prezentować reguły oraz raporty zgodności dla niego.
16. Moduł potrafi przeszukiwać wszystkie zapisane dane przy pomocy modułu wyszukiwania po słowach kluczowych.
17. Moduł obsługuje m.in. firewalle producenta:
    a) CheckPoint,
    b) Aventail,
    c) AwStats,
    d) Barracuda,
    e) F5,
    f) Cisco,
    g) Cyberoam,
    h) Fortinet,
    i) PfSense,
    j) PaloAlto,
    k) Juniper,
    l) Huawei,
    m) Securepoint,
    n) SonicWall,
    o) Sophos,
    p) WatchGuard,
    q) WinGate
18. Moduł pozwala na zarządzanie regułami firewalla dla urządzeń:
    a) FortiGate
    b) Sophos XG,
    c) Sophos UTM,
    d) Vyatta
19. Moduł pozwala na zaplanowanie raportów, które będą wysyłane co cykliczny okres, w tym pozwala na dodanie kolumny z ID wpisu, gdy ilość elementów na raporcie będzie większa niż 10.
20. Moduł posiada wbudowaną sekcję raportową dotyczącą wszystkich VPN'ów oraz prezentującą dane zebrane z logów, w tym posiada raport prezentujący dane granularne, takie jak:
    a) Data rozpoczęcia połączenia,
    b) Data zakończenia połączenia,
    c) Czas trwania połączenia,

d) Użyty serwer,
e) Adres IP klienta,

21. Moduł wspiera możliwość skonfigurowania zabezpieczenia typu FailOver, które pozwoli na ciągłą pracę, w przypadku awarii jednego z serwerów.
22. Moduł posiada wbudowane raporty zgodności, m.in.: SOX.
23. Moduł pozwala na wykonywanie kopii zapasowych konfiguracji w trybach:
    a) teraz
    b) codziennie,
    c) co tydzień,
    d) co miesiąc.
24. Moduł pozwala na zaplanowanie backupu konfiguracji w okresach: codzienny, tygodniowy (z wybraniem dnia), miesięczny oraz jednorazowy.
25. Moduł pozwala na zarządzanie politykami firewalla przy pomocy API dla firewall'ów FortiGate.
26. Moduł obsługuje integrację ManageEngine ServiceDesk Plus On-Demand w "Notifications Template".
27. Moduł pozwala na raportowanie większości, najmniej i nieużywanych obiektów reguł na podstawie wykorzystania ruchu.
28. Moduł obsługuje raporty audytu bezpieczeństwa dla urządzenia Palo Alto.
29. Moduł pozwala na wysyłanie powiadomień o profilach alarmów do „Jira Service Desk", jako nowe zgłoszenie do pomocy technicznej z opcją „Szablon powiadomienia".
30. Moduł obsługuje raport audytu bezpieczeństwa dla urządzenia Sophos XG.
31. Moduł w obszarze zarządzania użytkownikami obsługuje tworzenie ról niestandardowych.
32. Moduł obsługuje Palo Alto VSYS w raportach ruchu i bezpieczeństwa opartych na danych Syslog.
33. Moduł obsługuje reguły i zgodności dla Palo Alto VSYS z opcjami CLI i API.
34. Moduł obsługuje raporty audytu bezpieczeństwa dla urządzeń Palo Alto VSYS.
35. Moduł obsługuje raporty audytu bezpieczeństwa dla urządzeń Cisco FirePower.
36. Moduł obsługuje zasady serwera Check Point Management dla opcji opartych na „celu instalacji".
37. Moduł umożliwia udostępnienie ustawień Terminala (SSH/TELNET) na stronie konfiguracji użytkownika.
38. Moduł obsługuje raporty dotyczące ruchu i bezpieczeństwa oparte na danych Syslog dla Hillstone Firewall.
39. Moduł posiada raport audytu bezpieczeństwa oparty na analizatorze zapory dla zapory SonicWall.
40. Moduł posiada raport z audytu bezpieczeństwa dla zapory Check Point.
41. Moduł obsługuje raporty audytu bezpieczeństwa dla zapór sieciowych FortiGate.
42. Moduł obsługuje raporty wygaśnięcia reguł dla zapór CheckPoint.
43. Moduł obsługuje reguły i zgodności dla zapór Hillstone z opcjami CLI i importu plików.
44. Moduł obsługuje generowanie raportów z audytu, zapewniając zgodność ze standardami branżowymi GLBA.
45. Moduł obsługuje funkcję wygasania reguł dla zapór Sophos XG.
46. Moduł obsługuje audyt bezpieczeństwa dla
    a) Sophos UTM
    b) WatchGuard M270 (seria M)
47. Moduł posiada raport „VPN Connection status" dla poszczególnych użytkowników VPN.
48. Moduł obsługuje opcję dodawania nazwy zasad firmy Cisco dla funkcji administracji reguł.
49. Moduł obsługuje raporty o ruchu i zabezpieczeniach na podstawie danych Syslog dla Hillstone Firewall
50. Moduł posiada raport audytu bezpieczeństwa dla zapory SonicWall
51. Moduł posiada raport audytu bezpieczeństwa dla zapory Check Point.

52. Moduł umożliwia eksport do plików CSV i XLS tak by były spójne z formatem PDF, aby pokazać pełne szczegóły obiektów w raporcie na stronie przeglądu zasad.
53. Moduł posiada opcję importu dla DHCP w ramach mapowania IP Nazwy użytkownika, aby wypełnić mapowanie nazwy użytkownika i nazwy hosta za pierwszym razem.
54. Moduł posiada sekcje standardów zgodności NERC-CIP w wersji 6
55. Moduł pozwala na przeszukanie danych sesji VPN i najczęstszych użytkowników na urządzaniu w zakładce VPN.
56. Moduł posiada audyt bezpieczeństwa dla zapory Hillstone.
57. Moduł pozwala na administrowanie regułami dla Juniper SRX z CLI.
58. Moduł umożliwia zmianę opcji harmonogramu raportów zarządzania dla codziennych i bieżących zmian dnia (dzisiaj).
59. Moduł posiada opcje konfiguracji usług niestandardowych, takich jak obiekty sieciowe, w funkcji „Analiza wpływu reguł"

Oprogramowanie wspomagające system bezpieczeństwa oraz wszystkie dostarczone moduły należy dostarczyć wraz z 2 letnim wsparciem producenta oprogramowania.

4. Wdrożenie

W ramach postępowania powinna być zapewniona usługa wdrożenia obejmująca:

1. instalacje oraz wstępną konfigurację urządzeń Firewall,
2. zaplanowanie, konsolidacje oraz migracje reguł bezpieczeństwa z obecnych urządzeń Firewall na nowe
3. przełączenie usług na nowe urządzenia w wyznaczonym przez zamawiającego oknie serwisowym
4. instalacja oraz konfiguracja oprogramowania wspierającego system bezpieczeństwa,
5. instalacja i konfiguracja modułów
6. integracja z siecią zamawiającego,
7. szkolenie z obsługi oprogramowania