Szczegółowy opis przedmiotu zamówienia do części 1

Niniejszy opis dotyczy zamówienia 2 firewall'i nowej generacji, do pracy w klastrze , w identycznej konfiguracji sprzętowej i funkcjonalnej, z funkcjonalnością IPS (Intrusion Prevention System), kontroli aplikacji AVC/AAC (Aplication Visibility and Control, Application Awareness and Control), URL Filtering, VPN (Virtual Private Network) na potrzeby projektu dofinansowanego w ramach mechanizmu POWER: „Zintegrowany Program Rozwoju Uczelni". W ramach projektu firewall'e mają realizować 3 zadania w ramach sieci Akademii Ignatianum w Krakowie:

a) Umożliwić bezpieczny i efektywny dostęp pracowników do sieci Intranet AIK za pomocą bezpiecznych połączeń VPN,
b) Zabezpieczać dostęp do portali Uczelni (strony WWW etc)
c) Zabezpieczać ruch Internetowy inicjowany z wewnątrz sieci (jak i połączeń VPN).

Poniższa specyfikacja jest wspólna dla obu urządzeń.

Dodatkowo Wykonawca dokona wstępnej konfiguracji i integracji rozwiązania z infrastrukturą Zamawiającego. Na posiadanych przełącznikach Cisco Nexus wymagane będzie: hardening urządzenia oraz konfiguracja m.in. technologii i protokołów w stosunku do zamawianego sprzętu: NTP, SSH, VLAN, TRUNK, LACP, EtherChannel, vPC (Virtual PortChannel), QoS, MTU, IP, Routing, SVI, RSTP/MSTP, STP PortFast, BPDU Filter, BPDU Guard, IGMP Snooping, DHCP Snooping, Dynamic ARP Inspection, Port Security i IP Source Guard.

Wszystkie elementy posiadanych klastrów serwerowych powinny mieć zapewnione wyjście do sieci Internet. W tym celu Wykonawca zobowiązany będzie skonfigurować zamówione firewalle (wg konfiguracji posiadanych firewalli PaloAlto) do:

- podstawową konfigurację usługi resolvera na wszystkich nowych serwerach oraz zmiana konfiguracji obecnych serwerów DNS,
- ustalenie jakie dane mają być logowane w ramach usługi audytowania zdarzeń i dostępów w systemie,
- konfiguracja usługi audytowania zdarzeń zachodzących na nowym systemu według ustalonej polityki,
- konfiguracja rotacji logów,
- hardening usług, w tym konfiguracja Firewall oraz SSH, a także ostrzeżeń zgodnie ze wskazaną polityką,
- konfiguracja serwerów czasu i protokołu NTP,
- konfiguracja i hardening partycji,
- integracja skrzynek pocztowych dla każdej VM z serwerem pocztowym,
- przygotowanie dokumentacji w języku polskim, zawierającej informacje o systemie, jego budowie oraz instrukcje najczęstszych zadań administracyjnych.

Specyfikacja (CPV 32424000-1)

Architektura urządzenia, obudowa, interfejsy

1. Urządzenie będące dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań „serwerowych" bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia
2. Urządzenie pełniące rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall)
3. Urządzenie wyposażone w minimum 4 portów 1 Gigabit Ethernet oraz min 2 porty SFP, w sumie minimum 8 portów dla technologii Ethernet o dostępnej prędkości min. 1Gbit/s
4. Urządzenie obsługuje interfejsy VLAN (802.1Q) na interfejsach fizycznych – minimum 1.000 sieci VLAN
5. Urządzenie wyposażone w dedykowany port konsoli (RS lub USB) oraz dedykowany port Ethernet do zarządzania Out-of-Band
6. Zasilanie umożliwiające zasilanie prądem przemiennym 230V
7. Możliwość montażu w szafie rack 19" (dołączone niezbędne elementy montażowe)

Parametry wydajnościowe

8. Przepustowość teoretyczna urządzenia dla uruchomionych modułów firewall'a oraz kontroli aplikacji na poziomie 2Gb/s, a dla modułów kontroli aplikacji oraz systemu IPS na poziomie 2Gb/s
9. Wydajność dla ruchu rzeczywistego http dla modułów AVC oraz IPS na poziomie 1Gb/s
10. Maksymalna liczba sesji (z kontrolą aplikacji) na poziomie 180 000 z możliwością zestawiania co najmniej 10 000 nowych połączeń na sekundę
11. Wsparcie dla VPN IPSec na poziomie 750 Mb/s.

Funkcjonalność urządzenia

12. Urządzenie nie posiada ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
13. Działanie urządzenia co najmniej w trybie firewall'a L3.
14. Urządzenie obsługuje routing statyczny i dynamiczny (RIP, OSPF, BGP).

15. Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory.
16. Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT)
17. Urządzenie zapewnia mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA), conajmniej active/passive. Synchronizacja konfiguracji może odbywać się poprzez mechanizmy urządzeń bezpośrednio między nimi, bądź za pomocą zewnętrznego systemu zarządzającego, w którym to przypadku system musi być dostarczony wraz ze sprzętem.
18. Urządzenie zapewnia funkcjonalność tzw. Firewall'a Next-Generation w zakresie:
    a. systemu automatycznego wykrywania i klasyfikacji aplikacji (AVC/AAC)
    b. systemu IPS (Intrusion Prevention System)
19. System posiada możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System ma tworzyć kontekst z wykorzystaniem co najmniej poniższych parametrów:
    a. Wiedza o użytkownikach – uwierzytelnienie (poprzez LDAP/AD)
    b. Wiedza o aplikacjach wykorzystywanych po stronie klienta
    c. Wiedza o bieżących zagrożeniach
    d. Baza danych URL
20. Urządzenie umożliwia konfiguracją IPsec IKEv2, w ilości co najmniej 100 tuneli jednokierunkowych.
21. Urządzenie umożliwia konfiguracją SSL VPN Remote Access z możliwością uwierzytelniania w serwerze LDAP/AD. W ramach połączenia VPN system umożliwia stworzenie, kilku różnych grup dostępowych do sieci. System musi posiadać możliwość definiowania powitalnego banneru dla połączenia VPN RA oraz możliwości tunelowania całego ruchu jak i również tzw. „Split tunelingu" (funkcja ta jest konfigurowana per grupa VPN RA). Należy dostarczyć również odpowiednie licencje dla połączeń VPN Remote Access, wymagana jest licencja na 100 jednoczesnych połączeń użytkowników.
22. System wykrywania aplikacji AVC zapewniający:
    a. możliwość klasyfikacji ruchu i wykrywania co najmniej 200 aplikacji
    b. możliwość tworzenie profili użytkowników korzystających ze wskazanych aplikacji
    c. wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji
23. System IPS zapewniający:
    a. możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system)
    b. możliwość pracy w trybie pasywnym (IDS)
    c. możliwość wykrywania i blokowania szerokiej gamy zagrożeń w tym:
        i. złośliwe oprogramowanie
        ii. skanowanie sieci
        iii. ataki na usługę VoIP
        iv. próby przepełnienia bufora
        v. ataki na aplikacje P2P
        vi. zagrożenia dnia zerowego, itp.
    d. możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna)
    e. wiele sposobów wykrywania zagrożeń w tym:
        i. sygnatury ataków opartych na exploitach
        ii. reguły oparte na zagrożeniach
        iii. mechanizm wykrywania anomalii w protokołach
        iv. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego
    f. możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu
    g. wiele możliwości reakcji na zdarzenia w tym takie, jak:
        i. tylko monitorowanie
        ii. blokowanie ruchu zawierającego zagrożenia
        iii. zastąpienie zawartości pakietów
        iv. zapisywanie pakietów
    h. możliwość detekcji ataków i zagrożeń opartych na protokole IPv6
    i. możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności - zbierane są informacje o:
        i. systemach operacyjnych

ii. serwisach
iii. otwartych portach, aplikacjach
iv. zagrożeniach

j. możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych
k. możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.
l. możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji
m. mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne
n. możliwość definiowania wyjątków dla sygnatur z określeniem co najmniej adresów IP źródła lub przeznaczenia
o. możliwość tworzenia reguł do przechwytywania ruchu określonego typu
p. możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS
q. mechanizmy automatyzacji w zakresie wskazania zagrożonych hostów
r. mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa

24. System filtracji URL zapewniający:
a. kategoryzację stron – w co najmniej 40 kategoriach
b. bazę URL o wielkości nie mniejszej niż 100 mln URL

25. Urządzenie zapewnia możliwość wykrywania i śledzenia transferu następujących kategorii plików w ruchu sieciowym:
a. pliki systemowe i wykonywalne
b. pliki graficzne
c. pliki PDF
d. pliki multimedialne
e. pliki pakietu Office
f. pliki skompresowane

26. Urządzenie posiada możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download

27. Wbudowany podsystem wykrywania oprogramowania złośliwego (malware) i jego propagacji w strefie chronionej poprzez
a. sprawdzenie reputacji plików w systemie globalnym
b. sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze)

28. Urządzenie zapewnia możliwość wskazania plików o następujących charakterystykach:
a. pliki wolne od złośliwego kodu
b. pliki zawierające złośliwy kod
c. pliki podejrzane
d. pliki o własnej, zdefiniowanej przez użytkownika kategorii

29. Podsystem wykrywania oprogramowania złośliwego zawiera narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych jako oprogramowanie złośliwe (analiza retrospektywna)

30. Wraz z urządzeniem zostanie dostarczona dedykowana platforma zarządzająca. Platforma zarządzająca może mieć formę maszyny wirtualnej i spełnia następujące wymagania:
a. umożliwia agregację wszystkich zdarzeń IDS/IPS oraz centralne monitorowanie i analizę działającą w czasie rzeczywistym
b. jest dostępna przez interfejs WEB, bez potrzeby instalacji dodatkowego oprogramowania klienckiego
c. zapewnia interfejs, który może zostać dostosowany do wymagań użytkownika, w szczególności admnistrator posiada możliwość definiowania widoków (dashboard), które spełniają jego indywidualne kryteria
d. ma możliwość konfigurowania limitu powtórzeń danego zdarzenia w określonym czasie zanim zostanie wygenerowany alarm
e. ma możliwość automatycznej konfiguracji pobierania zestawów sygnatur na najnowsze zagrożenia i podatności. Ma możliwość informowania o zmianach w pakietach z nowymi sygnaturami/regułami
f. zapewnia zarządzanie oparte o role, gdzie każdy z użytkowników systemu może mieć różne widoki interfejsu oraz różne możliwości konfiguracyjne w zależności od roli, do której został przypisany
g. zapewnia funkcjonalność typu harmonogram zadań umożliwiającą automatyczne uruchamianie rutynowych czynności administracyjnych takich jak kopie zapasowe, uaktualnienia, tworzenie raportów, stosowanie polityk bezpieczeństwa
h. zapewnia grupowanie urządzeń i polityk w celu ułatwienia zarządzania konfiguracją
i. ma możliwość przechowywania atrybutów hostów definiowanych przez użytkownika takich jak jego krytyczność tak, aby ułatwić czynności monitorowania sieci

j. zapewnia możliwość automatycznego uaktualniania reguł publikowanych przez producenta, automatyczną dystrybucję i stosowanie reguł na urządzeniach IPS
k. ma możliwość wykonywania i odtwarzania kopi zapasowych zarówno urządzeń bezpieczeństwa, jak i platformy zarządzającej
l. zapewnia możliwość wglądu w reguły, które wygenerowały dany incydent oraz powiązanego z nim pakietu
m. zapewnia możliwość synchronizowania czasu pomiędzy wszystkimi komponentami przez protokół NTP
n. zapewnia możliwość logowania wszystkich czynności wykonywanych przez administratora zarówno lokalnie jak i na zdalnym serwerze
o. zapewnia szerokie możliwości generowania raportów włączając w to raporty predefiniowane oraz możliwość kompletnego dostosowania raportów do wymagań użytkownika
p. zapewnia informowanie o zagrożeniach poprzez
    i. wysłanie e-maila,
    ii. wysłanie trap SNMP,
    iii. przesłanie informacji do serwera Syslog,
    iv. uruchomienie skryptu użytkownika
q. posiada zaawansowany system przeszukiwania logów pozwalający na przeprowadzanie analizy
    i. aktualnego stanu danego urządzenia,
    ii. podglądu historii dostępnych zasobów,
    iii. możliwość eliminacji powtarzających się alarmów (tzw. Black Listing)
r. ma możliwość ustanawiania i wymuszania polityki zgodności jak i alarmowania w przypadku jej naruszeń w czasie rzeczywistym
s. ma możliwość przypisywania następujących parametrów w polityce kontroli dostępu dla danych interfejsów, podsieci, vlanów i użytkowników:
    i. dozwolone porty i protokoły
    ii. dozwolone aplikacje według różnych kategorii
    iii. dozwolone kategorie stron internetowych (URL filtering)
    iv. dedykowaną politykę wykrywania zagrożeń IPS dla każdej z reguł zapory ogniowej
    v. sposób traktowania wyspecyfikowanego ruchu w danej regule: przepuszczanie bez analizy, analiza, blokowanie ciche, blokowanie z resetowaniem sesji, blokowanie interaktywne
    v. w ramach funkcji kategoryzacji zapytań HTTP (URL filtering) rozwiązanie ma możliwość interaktywnego blokowania z resetowaniem zapytań. W ramach tej funkcji jest zapewniona możliwość zdefiniowania własnej strony internetowej ostrzegającej o naruszeniu polityki kontroli dostępu i zrzuceniu zablokowanej próby połączenia

31. Urządzenie powinno być objęte 3-letnim serwisem świadczonym bezpośrednio przez producenta, uprawniającym do:
a. wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia,
b. udostępnienia urządzenia zastępczego jeśli usuwanie awarii miałoby trwać dłużej niż 15 dni
c. wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia.
Serwis obejmuje też dostęp do aktualizacji sygnatur IPS, mechanizmów filtrowania webowego i aktualizacji filtrów antymalware'owych przez okres 3 lat.
32. Dostawa powinna obejmować uruchomienie podstawowej konfiguracji firewalli oraz instruktaż wprowadzający, oba zadania dla i przy obecności administratorów do obsługi urządzenia, o czasie min 2 dni roboczych.