Załącznik nr 8 do SIWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

"Utworzenie systemu e-usług dla Gminy Kondratowice"

Minimalne wymagania sprzętowe:

1. Serwer 1 (32gb) – parametry techniczne:

Seria procesora: Intel Xeon
Taktowanie procesora: 2.1 GHz
Liczba zainstalowanych procesorów: 2 szt.
Maks. obsługiwana liczba procesorów: 2 szt.
Pozostałe informacje o procesorze: Intel Xeon Silver 4110 2.1G, 8C/16T, 9.6GT/s, 11M Cache, Turbo, HT (85W) DDR4-2400
Typ pamięci: DDR4
Rodzaj pamięci: Registered
Zainstalowana pamięć RAM: 32 GB
Maks. wielkość pamięci: 512 GB
Liczba obsadzonych gniazd pamięci: 2
Liczba wszystkich gniazd pamięci: 16
Format szerokości: 3,5'' (LFF)
Obsługa hot-swap dysków: Tak
Liczba zainstalowanych dysków tw.: 4
Maks. liczba dysków w obecnej konfiguracji: 8
Maks. liczba dysków po rozbudowie serwera: 8
Pojemność sumaryczna wszystkich zainstalowanych dysków: 2400 GB
Możliwość instalacji dysków SSD: Tak
Kontroler dysków: Karta
Poziomy RAID: 50 (5+0) , 0 , 6 , 10 (1+0) , 60 (6+0) , 5 , 1
Pamięć kontrolera: 1 GB
Pozostałe informacje o kontrolerze: PERC H730P+ zintegrowany kontroler RAID, 2GB pamięci podręcznej
Grafika: Matrox G200 z 16MB pamięci
Gniazda rozszerzeń: Dwa PCI-Ex16 Gne3 połówkowej wysokości i długości
Interfejs sieciowy: Dwuportowa gigabitowa karta sieciowa
Zarządzanie, monitorowanie, konfiguracja: iDRAC9 Express wraz z dedykowanym portem RJ45
Zewnętrzne porty we-wy: Szeregowy - 1Sieciowy - 2 RJ45iDrac9 - przód 1xusb; tył 1xRJ45 Grafika - 1 tył, USB tył - 2 (2x3.0)USB przód - 1 (1x2.0)USB wew - 1x3.0
Obudowa: Rack 2U
Liczba zamontowanych zasilaczy: 2

Maksymalna liczba zasilaczy: 2
Moc zasilacza: 750 W
Obsługa hot-plug zasilaczy: Tak
Pozostałe informacje: W zestawie szyny do montażu
Gwarancja zewnętrzna 36 miesięcy NBD

2. Serwer 2 (16gb) – parametry techniczne:

Zestaw układów serw.	Intel® C236
Seria procesora serw.	Intel Xeon E3-1200 v6
Taktowanie procesora	3.5
Liczba zainstalowanych procesorów	1 szt.
Maks. obsługiwana liczba procesorów	1 szt.
Pozostałe informacje o procesorze	Intel Xeon E3-1230v6 3.5GHz, 8M cache, 4C/8T, turbo (80W)
Typ pamięci serw.	DDR4
Rodzaj pamięci serw.	Unbuffered
Rodzaj pamięci serw.	ECC
Zainstalowana pamięć RAM	16
Maks. wielkość pamięci	64
Liczba obsadzonych gniazd pamięci	2
Liczba wszystkich gniazd pamięci	4
Interfejs dysku serw.	SATA
Format szerokości dysku	3,5'' (LFF)
Obsługa hot-swap dysków	Tak
Liczba zainstalowanych dysków tw.	2
Maks. liczba dysków w obecnej konfiguracji	4
Pojemność sumaryczna wszystkich zainstalowanych dysków	2 TB
Kontroler dysków	Karta
Kontroler dysków	Hardware
Poziomy RAID	0
Poziomy RAID	1

Poziomy RAID	10 (1+0)
Poziomy RAID	5
Poziomy RAID	50 (5+0)
Podtrzymanie bateryjne	Nie
Pozostałe informacje o kontrolerze	Kontroler SAS/SATA PERC H330 RAID sprzętowy 0,1,10,5,50
Grafika	Matrox G200 z 16 MB pamięci
Napęd optyczny	DVD-RW Dual Layer

Gniazda rozszerzeń serw.

PCI Express Generation 3 expansion slots using expansion card riser	Specification
PCIE_G3_X16	(Slot 1) one half-height, half-length x16 link for processor 1
	(Slot 2) one full-height, half-length x16 link for processor 1
PCIE_G3_X8	(Slot 1) one full-height, half-length x4 link for processor 1
	(Slot 2) one half-height, half-length x8 link for processor 1

Interfejs sieciowy	Jedna dwuportowa gigabitowa karta sieciowa Broadcom BCM 5720
Zewnętrzne porty we-wy serw.	Szeregowy -1 Sieciowy - 2 RJ45 Grafika - 2 USB - 5 (2 tył, 2 przód, 1 wew)
Obudowa serw.	Rack 1U
Liczba zamontowanych zasilaczy	1
Maksymalna liczba zasilaczy	1
Moc zasilacza	250
Informacje o gwarancji	3 lata NBD
Informacje dodatkowe	Serwer zawiera szyny w zestawie.

3. Oprogramowanie do serwerów

Windows Server 2012	-	2 sztuki
Win CAL 2016 User PL	-	30 sztuk

4. Szafa teleinformatyczna wraz z osprzętem

a) Szafa teleinformatyczna

Dane techniczne:

Szerokość:	19"
Wysokość:	42U
Szerokość zewnętrzna:	600 mm
Wysokość zewnętrzna:	2050 mm
Głębokość zewnętrzna:	1000 mm
Materiał:	blacha stalowa
Wykończenie powierzchni:	malowanie farbą proszkową
Grubość blachy:	2,0 mm (+/- 0,2 mm)
Grubość profili montażowych:	1,2 mm (+/- 0,2 mm)
Konstrukcja ramy:	skręcana
Nośność szafy:	- kółka do 300 kg - stopki do 1000 kg
Stopień ochrony:	IP 20
Masa:	ok. 106 kg
Kolor:	czarny (RAL9004)
Drzwi przednie:	przeszklone - zamykane na klucz
Drzwi tylne:	stalowe perforowane - zamykane na klucz
Osłony boczne:	stalowe - zamykane na klucz

b) Półka stała 19" 1U głęb. 650mm, czarna, 4 punkty mocowania – 2 sztuki

Wymiary
- Szerokość: 48,26 cm (19")
- Wysokość: 44,45 mm (1U)
- Głębokość: 650 mm

c) Półka stała 19" 1U głęb. 450mm

Wymiary
- Szerokość: 48,26 cm (19")
- Wysokość: 44,45 mm (1U)
- Głębokość: 450 mm

d) Półka wysuwana pod klawiaturę i mysz 1U 19”

e) Listwa zasilająca 19" gniazdo 9 x CEE 7/5 wtyk IEC320 C20

Standard:	1U/19"
Gniazda:	9 x CEE 7/5
Wtyk:	1 x IEC 60320 C20
Obudowa korpusu:	aluminiowa
Materiał gniazd:	samogasnące tworzywo ABS
Prąd znamionowy urządzenia:	16A

Maksymalne obciążenie:	3500W
Długość przewodu zasilającego:	1.8m
Dodatkowe informacje:	dioda sygnalizacyjna LED
Wyposażenie dodatkowe:	zestaw śrub mocujących wraz z koszyczkami i podkładkami

f) Organizator kabli 1U 19" 4 metalowe uchwyty, czarny

g) Patch panel UTP kat.5e 24 porty LSA z półką 1U/19" – 2 sztuki

SPECYFIKACJA

Ogólne	
- szerokość:	19"/483mm
- wysokość:	1U/44mm
- kategoria:	5E
- klasa:	D / 100 MHz / 1 Gb/s
- ilość portów:	24 RJ45 z polami opisowymi
- półka montażowa:	tak
Obudowa	
- materiał obudowy:	blacha stalowa walcowana na zimno
- wykończenie powierzchni:	malowana farbą proszkową
- kolor:	czarny
Gniazdo	
- korpus:	Termoplastyczne tworzywo ABS spełniające wymogi UL 94 V-0
- trwałość:	> 750 cykli
- materiał styków:	fosforobrąz
- powłoka styków:	1,25 µm warstwa złota na 2,5 µm warstwie niklu
- siła docisku styków:	100 g na styk
- siła rozłączania:	50N przez 60s
Złącze szczelinowe	
- sekwencja:	568A/B
- typ złącza:	LSA
- trwałość:	> 200 cykli
- materiał noży:	fosforobrąz
- przyjmuje przewody:	22-26AWG
- korpus:	plastik

h) Switch 48-port 10/100/1000 Gigabit

Klasa przełącznika	SMART
Zastosowanie	Średnie i duże firmy
Warstwa przełączania	L2
Architektura sieci	GigabitEthernet
Liczba portów 10/100 Mbps	Brak
Liczba portów 10/100/1000 Mbps	44
Liczba portów 10Gb	Brak

Liczba portów PoE (PoE + PoE+)	Brak
Liczba portów PoE+	Brak
Liczba portów COMBO	4
Liczba portów SFP	Brak
Liczba portów SFP+	Brak
Liczba portów QSFP+	Brak
Port konsoli	Nie
Tryb przekazywania	Store-and-forward
Przepustowość	96 Gb/s
Prędkość przekazywania	77.4 Mpps
Bufor pakietów	6 MB
Rozmiar tablicy adresów MAC	16000
Obsługa ramek Jumbo	Tak
Rozmiar ramki Jumbo	12.69 KB
Możliwość łączenia w stos	Nie
Liczba grup VLAN	256
VLAN	- 802.1Q Tagged VLAN - Max. 4094 VIDs - Management VLAN - Asymmetric VLAN - Auto Voice VLAN - Max. 10 user-defined OUI - Max. 8 default OUI - Auto Surveillance VLAN
Obsługiwane protokoły i standardy	- IEEE 802.3 10BASE-T - IEEE 802.3u 100BASE-TX - IEEE 802.3ab 1000BASE-T - IEEE 802.3x Flow Control
QoS	- 802.1p Quality of Service - Kolejkowanie Handling: Strict, Weighted Round Robin (WRR) - 8 kolejek na port - Bandwidth Control : Port-based (Ingress/Egress, min. granularity for 10/100/1000Base-T ports is 15 Kb/s) - 802.1p Priority Queues - DSCP - ToS - TCP/UDP port number - IPv6 traffic class1
Bezpieczeństwo	- Obsługa do 64 adresów MAC na port - Broadcast/Multicast/Unicast Storm Control - Statyczny MAC - D-Link tryb ochronny - DHCP Server Screening - Trusted Host - ARP Spoofing Prevention - Max. 64 wejść - SSL - Obsługa v1/v2/v3 - Obsługa IPv4/IPv6 - Segmentacja (Traffic)

	- Smart Binding1 - Discover connected devices and click to bind - ARP Packet Inspection: 512 entries - IP Packet Inspection: 128 entries - Supports DHCP Snooping
Zarządzanie, monitorowanie, konfiguracja	- Wielojęzyczny interfejs GUI - SmartConsole Utility2 - Simplified CLI - Telnet Server - TFTP Client - IPv6 Neighbor Discovery - Configurable MDI/MDIX - SNMP: obsługa v1, v2, v3 - SNMP Trap - System Log - Max. 500 log entries - BootP/DHCP Client - D-Link Network Assistant support - SNTP - ICMPv6 - IPv4/v6 Dual Stack - DHCP Auto Configuration - RMON v1
Funkcje L2	- IGMP v1/v2 Snooping - IGMP Snooping v3 Awareness - Obsługa 256 IGMP grup - Obsługa do 64 adresów statycznych multicast - IGMP na VLAN - Obsługa IGMP Snooping Querier - Obsługa MLD v1/v2 - Obsługa 256 grup - Fast Leave - 802.1D STP - 802.1w RSTP - 802.3ad Link Aggregation - Port Mirroring: One-to-One, Many-to-One - Obsługa Mirroring for Tx/Rx/Both - Filtrowanie Multicast - LLDP, LLDP-MED
Funkcje L3	
Pozostałe funkcje	- Link Status - Cable Length detection - LED or Port Shutoff - Port Standby mode - System Hibernation mode
Typ obudowy	Rack
Wentylator	Tak
Zasilacz	Wewnętrzny

5. Tablet

Liczba rdzeni procesora	4
Częstotliwość	1.3 GHz
Technologia matrycy	IPS
Rozmiar wyświetlacza	10.1 cal
Rozdzielczość	1280 x 800
Pojemność pamięci	2GB
Rozmiar dysku	16 GB
Typ obsługiwanej karty pamięci	microSD 32GB
Rozdzielczość kamery głównej	8 Mpx
Rozdzielczość kamery dodatkowej	0,2 Mpx
System operacyjny	Android
Technologie	Bluetooth GPS
Zawartość opakowania	Ładowarka Tablet Przejściówka Przewód micro USB
Kolor	Czarny
Wi-Fi	802.11 b/g/n
Porty	1 x Jack 3.5 mm 1 x Micro USB
Maksymalna pojemność karty pamięci	32 GB
Wersja Bluetooth	4.0

6. Zestaw komputerowy

Stacja robocza - Parametry techniczne:

Procesor	Intel Celeron G4900 3.1GHz Dual Core 54W CPU
Płyta główna	Chipset B360
Pamięć RAM	4GB (1x4GB) DDR4 2666 DIMM
Dysk twardy 1	256GB M.2 2280 PCIe NVMe Solid State Drive
Dysk twardy 2	1TB 7200RPM SATA-6G 3.5in
Napęd optyczny	Nagrywarka DVD
Karta graficzna	Chipset 630
Karta sieciowa	10/100/1000 Mbps
Liczba portów USB 2.0	x 4
Liczba portów USB 3.1	x 3
Liczba USB na przednim panelu	2 x USB 3.1
Wyjścia/wejścia dźwięku	Line In, Line Out, Słuchawkowe/mikrofonowe (Combo)
Wyjścia/wejścia obrazu	D-Sub / VGA, HDMI

System operacyjny	Windows 10 Pro 64 PL
Akcesoria	Klawiatura, Mysz, Kabel zasilający

Obudowa, płyta główna, klawiatura i mysz powinny posiadać logo tego samego producenta sprzętu.

Monitor - Parametry techniczne:

Przekątna ekranu	19"
Rozdzielczość	1366x768
Typ matrycy	TN
Powłoka matrycy	Matowa
Proporcje ekranu	16:9
Częstotliwość odświeżania	60 Hz
Czas reakcji matrycy	5 ms
Jasność	200
Kontrast	5.x mln :1
Kąt widzenia	65 stopni (pion), 90 stopni (poziom)
Rozmiar plamki w mm	0.2382
Możliwość regulacji	Kąta pochylenia (Tilt)
Możliwość montażu na ścianie	Tak
Standard VESA	100 x 100 mm
Wyjścia/wejścia dźwięku	Słuchawkowe - stereo 3,5 mm
Wyjścia/wejścia obrazu	D-Sub / VGA, HDMI
Wbudowane głośniki	Tak
Liczba głośników	2.0
Moc głośników	2W
Kolor główny	Czarny
Pobór mocy (włączony)	19 W
Napięcie zasilania / zasilacza	230 V
Rodzaj wtyczki sieciowej	Typ E
Zawartość zestawu	Instrukcja obsługi, Kabel audio, Kabel D-Sub, Kabel zasilający

Monitor powinny posiadać logo tego samego producenta sprzętu co stacja robocza.

7. Urządzenie UTM

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. 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 dostawca 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.
Interfejsy, Dysk, Zasilanie:
1. System realizujący funkcję Firewall musi dysponować minimum:

- 7 portami Gigabit Ethernet RJ-45.

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 zasilanie AC.

<u>Parametry wydajnościowe:</u>

1. W zakresie Firewall'a obsługa nie mniej niż 1.8 mln jednoczesnych połączeń oraz 21.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 2.5 Gbps.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 450 Mbps.
4. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 90 Mbps.
5. 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 350 Mbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 160 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 185 Mbps.

<u>Funkcje Systemu Bezpieczeństwa:</u>

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. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.

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 w oparciu o protokoły: 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 dwu-składnikowego.
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 dwu-składnikowego 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.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.
- ICSA lub NSS Labs dla funkcji IPS.
- ICSA dla funkcji IPSec VPN.
- ICSA dla funkcji SSL VPN

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

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 12 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5. Oferent winien przedłożyć dokumenty:
    - Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
    - Certyfikat ISO 9001 podmiotu serwisującego.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.