Technická specifikace

2x Firewall v režimu vysoké dostupnosti pro zabezpečení komunikace LAN-WAN		**Produktové číslo výrobce: FG-200F + FTK-200**
Typ zařízení	Next-Generation Firewall (NGFW) s Unified Threat Management (UTM)	2 x FortiGate 200F, 24x7 Unified Threat Protection 5YR, Next Day Delivery Premium RMA Service FortiClient Security Fabric Agent a FortiToken 200 pro 230 uživatelů + originální transceivery
Formát zařízení	Pro montáž do 19" rozvaděče, výška max 2U	
Napájení	2× redundantní zdroj AC 230 V	
Systémové porty	1× RJ45 sériový konzolový port	
	1× port RJ45 1 Gbps dedikovaný pro správu (Out-of-Band Management)	
	2× port SFP 1 Gbps dedikovaný či konfigurovatelný pro HA komunikaci	
Datové porty	Minimálně 6× port SFP 1 Gbps (nejsou započítány porty pro HA komunikaci)	
	Minimálně 4× port SFP+ 10 Gbps	
Transceivery	8× transceiver SFP 1000Base-SX, MM, 850 nm, Duplex LC	
	4× transceiver SFP+ 10GBase-SR, MM, 850 nm, Duplex LC	
	Jsou vyžadovány originální výrobcem podporované transceivery.	
	Počet transceiverů je uveden na jeden firewall. Od každého dodaného modelu transceiverů musí být na celek dodány 2 transceivery navíc jako rezerva.	
Režim firewallu	Podpora NAT módu (L3)	
Vysoká dostupnost	Podpora HA clusteru v módu Active-Passive (Active-Standby) i Active-Active	
	Podpora heartbeat a synchronizační komunikace přes dvě samostatná rozhraní, případně přes vyhrazené agregační rozhraní složené ze dvou linek.	
	Možnost rozdělení HA clusteru mezi geograficky oddělené lokality (do 100 m)	
Síťové funkce	Podpora virtuálních sítí 802.1q (VLAN)	
	Podpora linkové agregace 802.3ad (LACP)	
	Podpora protokolů IPv4 i IPv6	
	Podpora směrování na základě pravidel (PBR)	
	Podpora dynamického směrovacího protokolu OSPFv2 i OSPFv3	

Technická specifikace

Virtuální privátní sítě	Podpora IPsec tunelů mezi lokalitami (Site-to-Site VPN)	
	Podpora uživatelských IPsec i SSL VPN (Remote Access VPN)	
	Podpora IPsec IKEv1 i IKEv2	
	Podpora uživatelských IPsec i SSL VPN pro minimálně 230 uživatelů	
	Podpora dvoufaktorového ověřování (2FA) pomocí jednorázových kódů pro minimálně 230 uživatelů. Součástí dodávky musí být příslušný počet hardwarových zařízení pro generování těchto kódů.	
	Podpora blokace připojení do VPN pro zařízení s neaktuálním operačním systémem nebo antivirem pro minimálně 230 zařízení	
Ověřování uživatelů	Podpora ověřování uživatelů pomocí protokolů LDAP a RADIUS	
Firewall	Podpora využití uživatelských identit (L8) ve firewallových pravidlech	
Pokročilé funkce	Antivirová kontrola	
	Antispamová kontrola	
	Systém reputace IP adres a ochrany proti botnet sítím	
	Detekce hrozeb pomocí technologie sandbox v cloudu výrobce firewallu	
	Řízení přístupu na web na základě kategorií (URL/Web Filtering)	
	Aplikační kontrola	
	Systém prevence průniků (IPS)	
	SSL inspekce (SSL Decryption)	
	Řízení provozu (Traffic Shaping)	
	SD-WAN	
Propustnost dle výrobce	Firewall	20 Gbps (pro UDP pakety o velikosti 1518 bajtů)
	IPS	3 Gbps
	NGFW	3 Gbps
	Threat Prevention	3 Gbps
	SSL Inspection	3 Gbps
	IPsec VPN	6 Gbps
	SSL VPN	2 Gbps

Technická specifikace

	Je vyžadováno doložení propustností pro uvedené kategorie produktovým listem nebo prohlášením výrobce.
Logování	Logování do centrálního systému pro sběr a analýzu logů, který je součástí předmětu plnění. Systém pro sběr a analýzu logů musí být podporován výrobcem firewallu a musí umožňovat zpětné vyčítání logů firewallem.
	Podpora logování na syslog server
Licence	Jsou požadovány licence pokrývající veškerou výše uvedenou funkcionalitu.
	Licence s časově omezenou platností jsou vyžadovány na dobu 5 let.
Podpora	Je vyžadována podpora 24×7 po dobu 5 let, na hardware i software s dobou odezvy na podnět do 4 hodin.
	V případě nutnosti výměny hardware je vyžadováno doručení nového zařízení nejpozději během dne následujícího po nahlášení závady.

2x Firewall v režimu vysoké dostupnosti pro zabezpečení komunikace LAN-LAN		**Produktové číslo výrobce: FG-1100E**
Typ zařízení	Next-Generation Firewall (NGFW) s Unified Threat Management (UTM)	2 x FortiGate 1100E, 24x7 Advanced Threat Protection 5YR, Next Day Delivery Premium RMA Service + originální transceivery
Formát zařízení	Pro montáž do 19" rozvaděče, výška maximálně 3U	
Napájení	2× redundantní za chodu vyměnitelný zdroj AC 230 V	
Systémové porty	1× RJ45 sériový konzolový port	
	1× port RJ45 1 Gbps dedikovaný pro správu (Out-of-Band Management)	
	2× port SFP/SFP+/SFP28/QSFP+ dedikovaný či konfigurovatelný pro HA komunikaci Musí být zvolený port s takovou propustností, aby dle požadavků výrobce firewallu na komunikaci po tomto portu nebyla propustnost zvoleného portu úzkým hrdlem pro výkon firewallu v HA clusteru, a to nejen v módu Active-Passive, ale ani v módu Active-Active.	
Datové porty	Minimálně 8× port SFP+ 10 Gbps (nejsou započítány porty pro HA komunikaci). Je přípustné i použití portů SFP28 osazených SFP+ 10 Gbps transceivery.	
Transceivery	8× transceiver SFP+ 10GBase-SR, MM, 850 nm, Duplex LC	
	2× transceiver podle typu portu použitého pro HA komunikaci pro MMF s dosahem minimálně 100 m po OM3/OM4 s Duplex LC konektorem	
	Jsou vyžadovány originální výrobcem podporované transceivery.	

Technická specifikace

	Počet transceiverů je uveden na jeden firewall. Od každého dodaného modelu transceiverů musí být na celek dodány 2 transceivery navíc jako rezerva.	
Režim firewallu	Podpora NAT módu (L3) i transparentního módu (L2)	
Vysoká dostupnost	Podpora HA clusteru v módu Active-Passive (Active-Standby) i Active-Active	
	Podpora heartbeat a synchronizační komunikace přes dvě samostatná rozhraní, případně přes vyhrazené agregační rozhraní složené ze dvou linek.	
	Možnost rozdělení HA clusteru mezi geograficky oddělené lokality (do 100 m)	
Síťové funkce	Podpora virtuálních sítí 802.1q (VLAN)	
	Podpora linkové agregace 802.3ad (LACP)	
	Podpora protokolů IPv4 i IPv6	
Pokročilé funkce	Antivirová kontrola	
	Aplikační kontrola	
	Systém prevence průniků (IPS)	
	SSL inspekce (SSL Decryption)	
Propustnost dle výrobce	Firewall	75 Gbps (pro UDP pakety o velikosti 1518 bajtů)
	IPS	12 Gbps
	NGFW	8 Gbps
	Threat Prevention	6 Gbps
	SSL Inspection	10 Gbps
	Je vyžadováno doložení propustností pro uvedené kategorie produktovým listem nebo prohlášením výrobce.	
Logování	Logování do centrálního systému pro sběr a analýzu logů, který je součástí předmětu plnění. Systém pro sběr a analýzu logů musí být podporován výrobcem firewallu a musí umožňovat zpětné vyčítání logů firewallem.	
	Podpora logování na syslog server	
Licence	Jsou požadovány licence pokrývající veškerou výše uvedenou funkcionalitu.	
	Licence s časově omezenou platností jsou vyžadovány na dobu 5 let.	
Podpora	Je vyžadována podpora 24×7 po dobu 5 let, na hardware i software s dobou odezvy na podnět do 4 hodin.	
	V případě nutnosti výměny hardware je vyžadováno doručení nového zařízení nejpozději během dne následujícího po nahlášení závady.	

Technická specifikace

3x Firewall pro zabezpečení komunikace ve vzdálených lokalitách		**Produktové číslo výrobce: FG-81F**
Typ zařízení	Next-Generation Firewall (NGFW) s Unified Threat Management (UTM)	3 x FortiGate 81F, 24x7 Unified Threat Protection 5YR, Next Day Delivery Premium RMA Service + originální transceivery
Formát zařízení	V provedení pro montáž do 19" rozvaděče nebo v provedení „Desktop“ s příslušenstvím pro uchycení do rozvaděče (rack-mount kit/tray), výška 1U	
Systémové porty	1× RJ45 sériový konzolový port	
Datové porty	Minimálně 2× port SFP 1 Gbps	
	Minimálně 6× port RJ45 1 Gbps	
Transceivery	2× transceiver SFP 1000Base-SX, MM, 850 nm, Duplex LC	
Režim firewallu	Podpora NAT módu (L3)	
Síťové funkce	Podpora virtuálních sítí 802.1q (VLAN)	
	Podpora linkové agregace 802.3ad (LACP)	
	Podpora protokolů IPv4 i IPv6	
Virtuální privátní sítě	Podpora IPsec tunelů mezi lokalitami (Site-to-Site VPN)	
	Podpora uživatelských IPsec i SSL VPN (Remote Access VPN)	
	Podpora IPsec IKEv1 i IKEv2	
Ověřování uživatelů	Podpora ověřování uživatelů pomocí protokolů LDAP a RADIUS	
Firewall	Podpora využití uživatelských identit (L8) ve firewallových pravidlech	
Pokročilé funkce	Antivirová kontrola	
	Antispamová kontrola	
	Systém reputace IP adres a ochrany proti botnet sítím	
	Detekce hrozeb pomocí technologie sandbox v cloudu výrobce firewallu	
	Řízení přístupu na web na základě kategorií (URL/Web Filtering)	
	Aplikační kontrola	
	Systém prevence průniků (IPS)	

Technická specifikace

	SSL inspekce (SSL Decryption)	
	Řízení provozu (Traffic Shaping)	
	SD-WAN	
Propustnost dle výrobce	Firewall	10 Gbps (pro UDP pakety o velikosti 1518 bajtů)
	IPS	1 Gbps
	NGFW	500 Mbps
	Threat Prevention	500 Mbps
	SSL Inspection	500 Mbps
	IPsec VPN	1 Gbps
	SSL VPN	500 Mbps
	Je vyžadováno doložení propustností pro uvedené kategorie produktovým listem nebo prohlášením výrobce.	
Logování	Logování na lokální disk	
	Logování do centrálního systému pro sběr a analýzu logů, který je součástí předmětu plnění. Systém pro sběr a analýzu logů musí být podporován výrobcem firewallu a musí umožňovat zpětné vyčítání logů firewallem.	
	Podpora logování na syslog server	
Licence	Jsou požadovány licence pokrývající veškerou výše uvedenou funkcionalitu.	
	Licence s časově omezenou platností jsou vyžadovány na dobu 5 let.	
Podpora	Je vyžadována podpora 24×7 po dobu 5 let, na hardware i software s dobou odezvy na podnět do 4 hodin.	
	V případě nutnosti výměny hardware je vyžadováno doručení nového zařízení nejpozději během dne následujícího po nahlášení závady.	

2x Kolektor a analyzátor logů v režimu vysoké dostupnosti pro centralizovaný sběr a analýzu logů z firewallů		**Produktové číslo výrobce: FAZ-300F**
	Technické požadavky kupujícího	Typ a podrobný technický popis nabízeného zařízení
Typ zařízení	Systém pro sběr logů z jednotlivých firewallů, jejich centralizované ukládání a analýzu	2 x FortiAnalyzer 300F, 24x7 FortiCare 5YR, Next Day Delivery Premium RMA Service
Formát zařízení	Pro montáž do 19" rozvaděče, výška 1U	

Technická specifikace

Napájení	Interní zdroj AC 230	
Síťová rozhraní	2× RJ45 1 Gbps	
Vysoká dostupnost	Podpora nasazení v režimu HA cluster	
Počet disků	Minimálně 2	2
Disky v RAID skupině	RAID 1 nebo RAID 10	RAID 0/1
Čistá úložná kapacita	Minimálně 4 TB	8TB (2 x 4TB)
Kapacita pro uložení logů	Minimálně 31 dnů při objemu 125 GB logů za den (minimální kapacita při maximální rychlosti sběru logů)	150 GB
Maximální rychlost sběru logů	Minimálně 6000 logů za sekundu	6 750
Maximální rychlost analýzy logů	Minimálně 4000 logů za sekundu	4 500
Funkce	Detailní filtrování logů dle volby uživatele	
	Předdefinované filtry, grafy a reporty	
	Možnost uživatelsky definovatelných reportů	
	Automatizované generování reportů v definovaných časových intervalech	
	Automatizované odesílání vygenerovaných reportů na e-mail	
Kompatibilita	Firewally a systém pro sběr a analýzu logů, kterou jsou předmětem plnění, musí být navzájem kompatibilní a oboustranně podporované výrobcem či výrobci. Kombinace systémů musí umožňovat, aby si firewally mohly ze systému pro ukládání logů zpětně vyčítat požadované historické informace a zobrazovat je přímo v uživatelském rozhraní firewallu.	
Licence	Jsou požadovány licence pokrývající veškerou výše uvedenou funkcionalitu.	
	Licence s časově omezenou platností jsou vyžadovány na dobu 5 let.	
Podpora	Je vyžadována podpora 24×7 po dobu 5 let, na hardware i software s dobou odezvy na podnět do 4 hodin.	
	V případě nutnosti výměny hardware je vyžadováno doručení nového zařízení nejpozději během dne následujícího po nahlášení závady.	

Implementace

Základní informace pro představu o složitosti prostředí:

Technická specifikace

- Hlavní lokalita:
  - Počet datových center: 2 (vzdálenost do 100 m)
  - Počet VLAN v infrastruktuře: do 20
  - Počet firewallových pravidel ve stávajícím řešení (WatchGuard): cca 100
  - Počet IP zařízení v síti: cca 600
  - Počet uživatelů: cca 350
- Vzdálené lokality
  - Počet vzdálených lokalit: 3 (v rámci jednoho města)
  - Počet PC v jednotlivých lokalitách: 5 až 25

Je požadováno:

- Analýza potřeb kupujícího, stávajícího řešení, návrh nového řešení.
- Nasazení systému pro sběr a analýzu logů v hlavní lokalitě
- Náhrada stávajících firewallů na vzdálených lokalitách
- Náhrada stávajícího firewall clusteru na vnějším perimetru v hlavní lokalitě novým LAN-WAN firewall clusterem
- Nasazení nového LAN-LAN firewall clusteru v hlavní lokalitě

Samotné implementační fázi musí předcházet fáze analýzy potřeb kupujícího, stávajícího řešení a návrh nového řešení dle koncepce kupujícího a s ohledem na „best practice“ a doporučení prodávajícího.
Plánování, návrh a nasazování musí probíhat za účasti členů IT oddělení kupujícího.

Po odsouhlasení s kupujícím je možné při implementaci jednotlivé body přizpůsobit.
Body označené jako „Volitelné“ nemusí být kupujícím při implementaci vyžadovány.

Instalační práce:

- Nasazení nového systému pro sběr a analýzu logů
  - Instalace do datového rozvaděče a zapojení
  - Konfigurační fáze
    - Konfigurace sítě
    - Konfigurace HA clusteru

Technická specifikace

        - Konfigurace uživatelských filtrů, pohledů a reportů
    - Nasazení do ostrého provozu
        - Ověření funkčnosti logování
        - Ověření funkčnosti reportů
- Náhrada stávajících firewallů WatchGuard na vzdálených lokalitách (3)
    - Fyzická instalace firewallu v cílových lokalitách
    - Konfigurační fáze (na základě konfigurace stávajícího firewallu a požadavků kupujícího)
        - Konfigurace firewallu do módu NAT/Router
        - Konfigurace požadovaných rozhraní
        - Konfigurace IPsec Site-to-Site VPN mezi vzdálenými lokalitami a hlavní lokalitou
        - Konfigurace zón
        - Konfigurace objektů (adresy, služby apod.)
        - Konfigurace UTM profilů (IPS, aplikační kontrola, antivirová kontrola atd.)
        - Konfigurace firewallových pravidel (přímá konektivita do Internetu + IPsec tunely mezi vzdálenými lokalitami a do hlavní lokalitou)
        - Konfigurace NATování (port forwarding)
        - Volitelně nasazení SSL inspekce
        - Volitelně konfigurace IPsec a SSL Remote Access VPN pro vzdálený přístup uživatelů
        - Konfigurace logování do systému pro sběr analýzu logů
    - Testovací fáze
        - Test firewallových pravidel bez UTM funkcí
        - Test firewallových pravidel se zapnutými UTM funkcemi
    - Nasazení do ostrého provozu
        - Nahrazení stávajícího firewallu novým firewallem
        - Ověření funkčnosti komunikace skrz firewall
        - Dořešení případných problémů
- Náhrada stávajícího firewall clusteru WatchGuard na vnějším perimetru novým LAN-WAN firewall clusterem
    - Instalace jednotlivých firewallů do datových rozvaděčů v oddělených serverovnách a jejich zapojení
    - Konfigurační fáze (na základě konfigurace stávajícího firewallu a požadavků kupujícího)
        - Konfigurace firewallu do módu NAT/Router
        - Konfigurace firewallů do režimu active-passive HA cluster
        - Konfigurace požadovaných rozhraní

Technická specifikace

        - Konfigurace linkové agregace k páteřním switchům
        - Konfigurace VLAN
        - Konfigurace IPsec Site-to-Site VPN ke vzdáleným lokalitám
        - Konfigurace zón
        - Konfigurace objektů (adresy, služby apod.)
        - Konfigurace UTM profilů (IPS, aplikační kontrola, antivirová kontrola atd.)
        - Konfigurace komunikace s LDAP anebo RADIUS servery pro ověřování uživatelů
        - Konfigurace firewallových pravidel
        - Konfigurace NATování (port forwarding)
        - Vystavení certifikátu pro SSL inspekci s využitím existující doménové certifikační autority
        - Nasazení certifikační autority, instalace certifikátů do firewallu a do koncových stanic
        - Konfigurace SSL inspekce (včetně výjimek z SSL inspekce)
        - Konfigurace IPsec a SSL Remote Access VPN pro vzdálený přístup uživatelů
        - Ukázková konfigurace alespoň 5 uživatelů a koncových zařízení pro vzdálený přístup (dvoufaktorového ověřování, host-check připojovaného zařízení apod.)
        - Konfigurace logování do systému pro sběr analýzu logů
    - Testovací fáze
        - Test chování firewallu po zapojení mezi testovací síť a ISP
        - Test firewallových pravidel bez UTM funkcí
        - Test firewallových pravidel se zapnutými UTM funkcemi
        - Test SSL inspekce
        - Test vysoké dostupnosti (odpojením jednoho z heartbeat rozhraní, odpojením konektivity, odpojením aktivního nodu firewallu)
    - Nasazení do ostrého provozu
        - Nahrazení stávajícího firewallu novým firewallem LAN-WAN
        - Ověření funkčnosti komunikace skrz firewall
        - Dořešení případných problémů
- Nasazení nového firewall clusteru LAN-LAN
    - Instalace jednotlivých firewallů do datových rozvaděčů v oddělených serverovnách a jejich zapojení
    - Konfigurační fáze (nové nasazení, aktuálně není žádná LAN-LAN firewall nasazen)
        - Konfigurace firewallu do módu pro transparentní kontrolu interního provozu
        - Konfigurace firewallů do režimu active-passive HA cluster

Technická specifikace

        - Konfigurace požadovaných rozhraní
        - Konfigurace linkové agregace k páteřním a distribučním switchům
        - Konfigurace VLAN
        - Konfigurace zón
        - Konfigurace objektů (adresy, služby apod.)
        - Konfigurace UTM profilů (IPS, aplikační kontrola, případně antivirová kontrola)
        - Konfigurace firewallových pravidel
        - Konfigurace NATování (port forwarding)
        - Konfigurace SSL inspekce (včetně výjimek z SSL inspekce)
        - Konfigurace logování do systému pro sběr analýzu logů
    - Testovací fáze
        - Test chování firewallu po zapojení mezi páteřní stoh switchů a distribuční stoh switchů na testovací porty a VLANy
        - Test firewallových pravidel bez UTM funkcí
        - Test firewallových pravidel se zapnutými UTM funkcemi
        - Test SSL inspekce
        - Test vysoké dostupnosti (odpojením jednoho z heartbeat rozhraní, odpojením konektivity, odpojením aktivního nodu firewallu)
    - Nasazení do ostrého provozu
        - Nasazení LAN-LAN firewallu mezi páteřní stoh switchů a distribuční stoh switchů
        - Ověření funkčnosti komunikace skrz firewall
        - Dořešení případných problémů

- Zaškolení
    - Zaškolení obsluhy (5 pracovníků) v rozsahu 5 dnů, po 8 hodinách/1 den na technice kupujícího v prostorách Magistrátu města Havířova

- Předání projektu

- Telefonická podpora
    - Podpora po předání projektu (opravy případných nedostatků, které se před předáním projektu neodhalí) po dobu 2 měsíců v rozsahu 5 člověkodnů (člověkoden - čas odpovídající práci jedné osoby po dobu jednoho pracovního dne)