

Załącznik nr 1 do zadania Nr SM/17 pn. „Wydatki inwestycyjne – zakup urządzeń Firewall na potrzeby zabezpieczenia sieci Straży Miejskiej w Opolu”

Software Specifications

Routing Protocols

- IPv4, IPv6, ISO, Connectionless Network Service (CLNS)
- Static routes
- RIP v1/v2
- OSPF/OSPF v3
- BGP with Route Reflector
- IS-IS
- Multicast: Internet Group Management Protocol (IGMP) v1/v2, Protocol Independent Multicast (PIM) sparse mode (SM)/dense mode (DM)/source-specific multicast (SSM), Session Description Protocol (SDP), Distance Vector Multicast Routing Protocol (DVMRP), Multicast Source Discovery Protocol (MSDP), Reverse Path Forwarding (RPF)
- Encapsulation: VLAN, Point-to-Point Protocol (PPP), Frame Relay, High-Level Data Link Control (HDLC), serial, Multilink Point-to-Point Protocol (MLPPP), Multilink Frame Relay (MLFR), and Point-to-Point Protocol over Ethernet (PPPoE)
- Virtual routers
- Policy-based routing, source-based routing
- Equal-cost multipath (ECMP)

QoS Features

- Support for 802.1p, DiffServ code point (DSCP), EXP
- Classification based on VLAN, data-link connection identifier (DLCI), interface, bundles, or multifield filters
- Marking, policing, and shaping
- Classification and scheduling
- Weighted random early detection (WRED)
- Guaranteed and maximum bandwidth
- Ingress traffic policing
- Virtual channels
- Hierarchical shaping and policing

Switching Features

- ASIC-based Layer 2 Forwarding
- MAC address learning
- VLAN addressing and integrated routing and bridging (IRB) support
- Link aggregation and LACP
- LLDP and LLDP-MED
- STP, RSTP, MSTP
- MVRP
- 802.1X authentication

Firewall Services

- Stateful and stateless firewall
- Zone-based firewall
- Screens and distributed denial of service (DDoS) protection
- Protection from protocol and traffic anomaly
- Integration with Pulse Unified Access Control (UAC)
- Integration with Aruba Clear Pass Policy Manager
- User role-based firewall
- SSL Inspection (Forward-proxy)

Network Address Translation (NAT)

- Source NAT with Port Address Translation (PAT)
- Bidirectional 1:1 static NAT
- Destination NAT with PAT
- Persistent NAT
- IPv6 address translation

VPN Features

- Tunnels: Site-to-Site, Hub and Spoke, Dynamic Endpoint, AutoVPN, ADVPN, Group VPN (IPv4/ IPv6/ Dual Stack)
- Secure Connect: Remote access / SSL VPN
- Configuration payload: Yes
- IKE Encryption algorithms: Prime, DES-CBC, 3DES-CBC, AEC-CBC, AES-GCM, SuiteB
- IKE authentication algorithms: MD5, SHA-1, SHA-128, SHA-256, SHA-384
- Authentication: Pre-shared key and public key infrastructure (PKI) (X.509)
- IPsec (Internet Protocol Security): Authentication Header (AH) / Encapsulating Security Payload (ESP) protocol
- IPsec Authentication Algorithms: hmac-md5, hmac-sha-196, hmac-sha-256
- IPsec Encryption Algorithms: Prime, DES-CBC, 3DES-CBC, AEC-CBC, AES-GCM, SuiteB
- Perfect forward secrecy, anti-reply
- Internet Key Exchange: IKEv1, IKEv2
- Monitoring: Standard-based dead peer detection (DPD) support, VPN monitoring
- VPNs GRE, IP-in-IP, and MPLS

Network Services

- Dynamic Host Configuration Protocol (DHCP) client/server/relay
- Domain Name System (DNS) proxy, dynamic DNS (DDNS)
- Real-time performance monitoring (RPM) and IP-monitoring
- Flow monitoring (J-Flow)¹
- Bidirectional Forwarding Detection (BFD)
- Two-Way Active Measurement Protocol (TWAMP)
- IEEE 802.3ah Link Fault Management (LFM)
- IEEE 802.1ag Connectivity Fault Management (CFM)

High Availability Features

- Virtual Router Redundancy Protocol (VRRP)
- Stateful high availability
- Dual box clustering
- Active/passive
- Active/active
- Configuration synchronization

- Firewall session synchronization
- Device/link detection
- In-Band Cluster Upgrade (ICU)
- Dial on-demand backup interfaces
- IP monitoring with route and interface failover

Management, Automation, Logging, and Reporting

- SSH, Telnet, SNMP
- Smart image download
- CLI and Web UI
- Mist AI
 - Simplified management
 - WAN Assurance
- Junos Space and Security Director
- Python
- Junos OS event, commit, and OP script
- Application and bandwidth usage reporting
- Auto installation
- Debug and troubleshooting tools
- Zero-Touch Provisioning with Contrail Service Orchestration

Advanced Routing Services

- Packet mode
- MPLS (RSVP, LDP)
- Circuit cross-connect (CCC), translational cross-connect (TCC)
- L2/L3 MPLS VPN, pseudowires
- Virtual private LAN service (VPLS), next-generation multicast VPN (NG-MVPN)
- MPLS traffic engineering and MPLS fast reroute

Application Security Services¹

- Application visibility and control
- Application-based firewall
- Application QoS
- Application-based advanced policy-based routing
- Application quality of experience (AppQoE)

Enhanced SD-WAN Services

- Application-based advanced policy-based routing (APBR)
- Application-based link monitoring and switchover with Application quality of experience (AppQoE)

Threat Defense and Intelligence Services¹

- Intrusion prevention
- Antivirus
- Antispam
- Category/reputation-based URL filtering
- Protection from botnets (command and control)
- Adaptive enforcement based on GeolP
- Juniper Advanced Threat Prevention to detect and block zero-day attacks
- Adaptive Threat Profiling

- Encrypted Traffic Insights
- SecIntel to provide threat intelligence

¹Offered as advanced security services subscription licenses.

Hardware Specifications

Specification	SRX300	SRX320	SRX340
Connectivity			
Total onboard ports	8x1GbE	8x1GbE	16x1GbE
Onboard RJ-45 ports	6x1GbE	6x1GbE	8x1GbE
Onboard small form-factor pluggable (SFP) transceiver ports	2x1GbE	2x1GbE	8x1GbE
MACsec-capable ports	2x1GbE	2x1GbE	16x1GbE
Out-of-band (OOB) management ports	0	0	1x1GbE
Mini PIM (WAN) slots	0	2	4
Console (RJ-45 + miniUSB)	1	1	1
USB 3.0 ports (type A)	1	1	1
PoE+ ports	N/A	6 ²	0
Memory and Storage			
System memory (RAM)	4 GB	4 GB	4 GB
Storage	8 GB	8 GB	8 GB
SSD slots	0	0	1
Dimensions and Power			
Form factor	Desktop	Desktop	1 U
Size (WxHxD)	12.63 x 1.37 x 7.52 in. (32.08 x 3.47 x 19.10 cm)	11.81 x 1.73 x 7.52 in. (29.99 x 4.39 x 19.10 cm)	17.36 x 1.72 x 14.57 in. (44.09 x 4.36 x 37.01 cm)
Weight (device and PSU)	4.38 lb (1.98 kg)	3.28 lb (1.51 kg) ⁴ / 3.4 lb (1.55 kg) ⁵	10.80 lb (4.90 kg)
Redundant PSU	No	No	No
Power supply	AC (external)	AC (external)	AC (internal)
DC Input	N/A	N/A	N/A

Specification	SRX300	SRX320	SRX340
Maximum PoE power	N/A	180 W ⁵	N/A
Average power consumption	24.9 W	46 W ⁴ /221 W ⁵	122 W
Average heat dissipation	85 BTU/h	157 BTU/h ⁴ /755 BTU/h ⁵	420 BTU/h
Maximum current consumption	0.346 A	0.634 A ⁴ /2.755 A ⁵	1.496 A
Acoustic noise level	0dB (fanless)	37 dBA ⁴ /40 dBA ⁵	45.5 dBA
Airflow/cooling	Fanless	Front to back	Front to back
Environmental, Compliance, and Safety Certification			
Operational temperature	-4° to 140° F (-20° to 60° C) ⁷	32° to 104° F (0° to 40° C)	32° to 104° F (0° to 40° C)
Nonoperational temperature	-4° to 158° F (-20° to 70° C)	-4° to 158° F (-20° to 70° C)	-4° to 158° F (-20° to 70° C)
Operating humidity	10% to 90% noncondensing	10% to 90% noncondensing	10% to 90% noncondensing
Nonoperating humidity	5% to 95% noncondensing	5% to 95% noncondensing	5% to 95% noncondensing
Meantime between failures (MTBF)	44.5 years	32.5 years ⁴ / 26 years ⁵	27 years
FCC classification	Class A	Class A	Class A
RoHS compliance	RoHS 2	RoHS 2	RoHS 2
FIPS 140-2	Level 2 (Junos 15.1X49-D60)	Level 1 (Junos 15.1X49-D60)	Level 2 (Junos 15.1X49-D60)
Common Criteria certification	NDPP, VPNEP, FWEP, IPSEP (based on Junos 15.1X49-D60)	NDPP, VPNEP, FWEP, IPSEP (based on Junos 15.1X49-D60)	NDPP, VPNEP, FWEP, IPSEP (based on Junos 15.1X49-D60)

² SRX320 with PoE+ ports available as a separate SKU: SRX320-POE.

³ SRX345 with dual AC PSU model.

⁴ SRX320 non PoE model.

⁵ SRX320-POE with 6 ports PoE+ model.

⁶ SRX345 with DC power supply (operating temperature as per GR-63 Issue 4 2012 test criteria).

⁷ As per GR63 Issue 4 (2012) test criteria.

Performance and Scale

Parameter	SRX300	SRX320	SRX340
Routing with packet mode (64 B packet size) in Kpps ⁸	300	300	550
Routing with packet mode (IMIX packet size) in Mbps ⁸	800	800	1,600
Routing with packet mode (1,518 B packet size) in Mbps ⁸	1,500	1,500	3,000
Stateful firewall (64 B packet size) in Kpps ⁸	200	200	350
Stateful firewall (IMIX packet size) in Mbps ⁸	500	500	1,100
Stateful firewall (1,518 B packet size) in Mbps ⁸	1,000	1,000	3,000
IPsec VPN (IMIX packet size) in Mbps ⁸	100	100	200
IPsec VPN (1,400 B packet size) in Mbps ⁸	300	300	600
Application visibility and control in Mbps ⁹	500	500	1,000
Recommended IPS in Mbps ⁹	200	200	400
Next-generation firewall in Mbps ⁹	100	100	200
Route table size (RIB/FIB) (IPv4 or IPv6)	256,000/256,000	256,000/256,000	1 million/600,000 ¹⁰
Maximum concurrent sessions (IPv4 or IPv6)	64,000	64,000	256,000
Maximum security policies	1,000	1,000	2,000
Connections per second	5,000	5,000	10,000
NAT rules	1,000	1,000	2,000
MAC table size	15,000	15,000	15,000
IPsec VPN tunnels	256	256	1,024
Number of remote access/SSL VPN (concurrent) users	25	50	150
GRE tunnels	256	256	512
Maximum number of security zones	16	16	64
Maximum number of virtual routers	32	32	64
Maximum number of VLANs	1,000	1,000	2,000
AppID sessions	16,000	16,000	64,000
IPS sessions	16,000	16,000	64,000
URLF sessions	16,000	16,000	64,000

⁸ Throughput numbers based on UDP packets and RFC2544 test methodology.

⁹ Throughput numbers based on HTTP traffic with 44 KB transaction size.

¹⁰ Route scaling numbers are with enhanced route-scale features turned on.

WAN and Wi-Fi Interface Support Matrix

WAN and Wi-Fi Interface	SRX300	SRX320	SRX340
1 port T1/E1 MPIM (SRX-MP-1T1E1-R)	No	Yes	Yes
1 port VDSL2 Annex A/M MPIM (SRX-MP-1VDSL2-R)	No	Yes	Yes
4G / LTE MPIM (SRX-MP-LTE-AA and SRX-MP-LTE-AE)	No	Yes	Yes
802.11ac Wave 2 Wi-Fi MPIM	No	Yes	Yes

WAN and Wi-Fi Interface Module Performance Data

Interface Module	Description	Performance
4G/LTE	Dual SIM 4G/LTE-A CAT 6	Up to 300 Mbps download and 50 Mbps upload
Wi-Fi MPIM	Dual band 802.11 a/b/g/n/ac Wave 2 (2x2 MIMO)	Up to 866 Mbps at 5GHz / 300 Mbps at 2.4GHz

Ordering Information

	SRXnnn-SYS-JB
Hardware	Included
Management (CLI, JWEB, SNMP, Telnet, SSH)	Included
Ethernet switching (L2 Forwarding, IRB, LACP etc)	Included
L2 Transparent, Secure Wire	Included
Routing (RIP, OSPF, BGP, Virtual router)	Included
Multicast (IGMP, PIM, SSDP, DMVRP)	Included
Packet Mode	Included
Overlay (GRE, IP-IP)	Included
Network Services (J-Flow, DHCP, QOS, BFD)	Included
Stateful Firewall, Screens, ALGs	Included
NAT (static, SNAT, DNAT)	Included
IPSec VPN (Site-to-Site VPN, Auto VPN, Group VPN)	Included
Firewall policy enforcement (UAC, Aruba CPPM)	Included
Remote Access/SSL VPN (concurrent users) ¹¹	Optional
Chassis Cluster, VRRP, ISSU/ICU	Included
Automation (Junos scripting, auto-installation)	Included
MPLS, LDP, RSVP, L3 VPN, pseudo-wires, VPLS	Included

¹¹ Based on concurrent users; two free licenses included

Z racji posiadania w swojej infrastrukturze urządzeń marki Juniper oraz doświadczenia z obsługi urządzeń sieciowych tej marki, Zamawiający preferuje następujący sprzęt:

Modele urządzeń	Prognozowana ilość
Juniper SRX300-SYS-JB lub Juniper SRX320-SYS-JB	3
Juniper SRX340-SYS-JB	1

Urządzenia te będą rozmieszczone w siedzibie głównej (SRX340-SYS-JB) oraz trzech oddziałach zewnętrznych (SRX300-SYS-JB lub SRX320-SYS-JB).

Wraz z dostarczeniem urządzeń należy dostarczyć:

- akcesoria umożliwiające montaż urządzeń w szafie sieciowej 19”.
- dokumentację techniczną.
- certyfikaty / licencje (bezterminowe), pozwalające na jednoczesny zdalny dostęp dla min 20 użytkowników (dotyczy urządzenia w siedzibie głównej).
- oprogramowanie klienckie VPN Client-to-Site w wersji przeznaczonej dla systemu Windows 10.

Zamawiający wymaga, aby w ofercie zostało uwzględnione praktyczne szkolenie techniczne z podstawowej obsługi dostarczonych urządzeń oraz przekazany przewodnik (w języku polskim) przedstawiający proces konfiguracji urządzenia, w tym konfigurację następujących dostępuów zdalnych:

- VPN IPSec (Site-to-Site) umożliwiające połączenie oddziałów zewnętrznych (posiadających dostęp bezpośredni oraz za pośrednictwem zewnętrznych dostawców internetowych). Bezpieczne połączenie powinno umożliwić oddziałom zewnętrznym dostęp do internetu (dotyczy oddziałów podłączonych bezpośrednio) oraz usług Microsoft ActiveDirectory zlokalizowanych w siedzibie głównej.
- VPN (Client-to-Site) dla pracowników, umożliwiających bezpieczną zdalną pracę na komputerze służbowym będącym w sieci lokalnej Zamawiającego w opcji zdalnego pulpitu.

Dodatkowo Zamawiający wymaga dostępności wsparcia technicznego (telefonicznego, e-mail) świadczonego w języku polskim, na etapie wdrażania i podczas konfiguracji urządzeń.

Zamawiający zastrzega sobie prawo rezygnacji ze złożenia zamówienia lub rezygnacji z jego części. W zależności od posiadanych środków, Zamawiający może dokonać zakupu sprzętu w wybranej opcji konfiguracyjnej opisanej w niniejszej specyfikacji.

Zaoferowany sprzęt musi być fabrycznie nowy, objęty gwarancją producenta (obejmującą naprawę lub wymianę sprzętu w ciągu 72h od momentu zgłoszenia) na okres min. 36 miesięcy z opcją jej przedłużenia.

Zamawiający dopuszcza zaoferowanie sprzętu równoważnego do sprzętu przykładowego ujętego w niniejszej specyfikacji. W przypadku zaoferowania urządzeń równoważnych, Wykonawca zobowiązany jest dostarczyć wraz z ofertą, kompletną dokumentację techniczną (w języku polskim) wykazującą równoważność parametrów w zaoferowanym przez siebie sprzęcie w odniesieniu do parametrów wymaganych, opisanych przez Zamawiającego. W przypadku zaoferowania urządzeń równoważnych wymagane będzie dodatkowo przeprowadzenie procesu konfiguracji sprzętu na miejscu w siedzibie Zamawiającego oraz w jego oddziałach, więc należy to uwzględnić w swojej ofercie.