

FORMULARZ OFERTY
Zakup sprzętu sieciowego i akcesoriów komputerowych
na potrzeby Straży Miejskiej w Opolu–
poniżej 130.000 złotych netto

I. NAZWA I ADRES ZAMAWIAJĄCEGO:

Miasto Opole
Straż Miejska w Opolu
ul. Władysława Reymonta 47 B
45-072 Opole

II. OPIS PRZEDMIOTU ZAMÓWIENIA:

Przedmiotem zamówienia jest „Zakup sprzętu sieciowego i akcesoriów komputerowych na potrzeby Straży Miejskiej w Opolu”. Szczegółowy przedmiot zamówienia (minimalne wymagania techniczne) określa załącznik nr 1 do niniejszego formularza.

Osoby uprawnione do porozumienia się z Wykonawcami:

- w zakresie przedmiotu zamówienia: Paweł Chmiel – informatyk tel. 503790095
- w zakresie procedury zakupowej: Marta Grzebińska 691420711 od poniedziałku do piątku w godzinach od 7:00 do godz. 14:00

III. KRYTERIUM WYBORU OFERTY**1. 100 % - cena**

W niniejszym postępowaniu jedynym kryterium oceny ofert jest cena oferty. Oferta z najniższą ceną otrzyma maksymalną liczbę punktów – 100. Pozostałe oferty zostaną przeliczone wg wzoru podanego poniżej. Wynik będzie traktowany jako wartość punktowa oferty w kryterium cena oferty.

$$\text{Cena} = \frac{\text{Cena oferowana minimalna brutto}}{\text{Cena badanej oferty brutto}} \times 100\%$$

Jeżeli wybór oferty najkorzystniejszej będzie niemożliwy z uwagi na fakt, że zostały złożone oferty o takiej samej cenie, Zamawiający wezwie Wykonawców, którzy złożyli te oferty do złożenia ofert dodatkowych.

Zamawiający zastrzega sobie prawo do zamknięcia postępowania bez wybrania jakiegokolwiek ze złożonych ofert, w szczególności w przypadku, gdy najtańsza oferta będzie przekraczała możliwości budżetowe Zamawiającego. Złożone oferty przestaną wiązać, gdy zostanie wybrana inna oferta albo gdy postępowanie zostanie zamknięte bez wybrania którejkolwiek z ofert.

IV. FORMA ZŁOŻENIA OFERTY

Ofertę na Formularzu oferty należy złożyć w terminie **do dnia 25.11.2022r. do godz. 10⁰⁰** w jednej z niżej wymienionych form:

- pisemnej na adres Zamawiającego tj.: ul. Władysława Reymonta 47B, 45-072 Opole
- w wersji elektronicznej na e-mail: marta.grzebinska@strazmiejska.opole.pl

V. Klauzula Informacyjna RODO (dotyczy Wykonawcy będącego osobą fizyczną, w tym prowadzącą działalność gospodarczą podlegającą wpisowi do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, także jako wspólnik spółki cywilnej).

Na podstawie art. 13 ust. 1 i ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE. L. 2016.119.1), zwane dalej RODO, informuję, że:

1. Administratorem Pani/Pana danych osobowych jest Komendant Straży Miejskiej w Opolu ul. Wł. Reymonta 47b, 45-072 Opole.
2. Administrator powołał Inspektora Ochrony Danych nadzorującego prawidłowość przetwarzania danych osobowych, z którym można skontaktować się osobiście w siedzibie administratora lub za pośrednictwem adresu e-mail: iod@strazmiejska.opole.pl.
3. Pani/Pana dane osobowe będą przetwarzane na podstawie Państwa zgody wyrażonej poprzez akt uczestnictwa w tym postępowaniu oraz art. 6 ust. 1 pkt c, f RODO w celu przeprowadzenia postępowania w trybie Zapytania ofertowego i zawarcia umowy.
4. Odbiorcą Pani/Pana danych osobowych mogą zostać uprawnione organy publiczne oraz pozostali uczestnicy biorący udział w postępowaniu w sprawie tego zamówienia. Dane wykonawcy zamówienia mogą zostać umieszczone na stronie Straży Miejskiej w Opolu www.strazmiejska.opole.pl.
5. Pani/Pana dane osobowe będą przechowywane przez okres trwania zamówienia oraz w obowiązkowym okresie przechowywania dokumentacji ustalonym zgodnie z jednolitym rzeczowym wykazem akt obowiązującym w Straży Miejskiej w Opolu.
6. Przysługuje Pani/Panu prawo dostępu do treści swoich danych (art. 15 RODO), prawo ich sprostowania (art. 16 RODO), prawo do usunięcia danych jedynie w przypadkach podanych w art. 17 RODO, prawo do ograniczenia przetwarzania jedynie w przypadkach podanych w art. 18 RODO oraz prawo do cofnięcia zgody wyrażonej poprzez akt uczestnictwa w tym postępowaniu w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
7. Ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, jeśli stwierdzi Pani/Pan, że przetwarzanie danych osobowych dotyczących Pani/Pana narusza przepisy RODO,
8. Podanie przez Panią/Pana danych osobowych jest dobrowolne lecz stanowi warunek konieczny skutecznego złożenia oferty w Zapytaniu ofertowym którego wartość nie przekracza wyrażonej w złotych równowartości kwoty 130.000 netto i zawarcia umowy.

(pkt VI wypełnia oferent)

VI. NAZWA I ADRES WYKONAWCY:

NAZWA.....

ADRES.....

NIP.....

e-mail.....

Osoba upoważniona do kontaktu.....

tel.e-mail.....

Oferuję realizację wymienionego poniżej zamówienia na warunkach opisanych w postępowaniu:

Lp	Nazwa / model	Cena jedn. brutto	ilość	Wartość brutto
1	Firewall Juniper SRX320-SYS-JB		1	
2	Router UTM Juniper SSG 5-SH *		2	
3	Switch Cisco Catalyst C1000-24T-4G-L		2	
4	Switch Cisco CBS110		2	
5	Konwerter światłowodowy gigabit SFP 10/100/1000Base-T Fibrain FMU-APA12G-E		4	
6	Moduł SFP MULTIRATE 155MB~2.67GB, TX:1310NM, SMF, LC DUPLEX, 20KM Fibrain FTS-R27G-S31L-020D		4	
7	Patchcord SC/UPC-LC/UPC, SM, 9/125, duplex, włókno G652D, 2m		4	
8	Patchcord UTP-Kat 6, 2m		10	
9	Patchcord UTP-Kat 6, 3m		10	
10	Patchcord UTP-Kat 6, 5m		10	
11	Patchcord UTP-Kat 6, 10m		10	
12	Mysz optyczna Logitech M90, 1000dpi, USB, przewodowa		5	
13	Mysz optyczna Logitech M190, 1000dpi, USB, bezprzewodowa		1	
14	Klawiatura Logitech K120, membranowa, USB, przewodowa		5	
15	Listwa zasilająca z wyłącznikiem i zabezpieczeniem, 7 gniazd, kabel 1,8m , 19'', 7-8 gniazd		4	
16	Napęd DVD-RW Lite-On eBAU108 Slim USB BOX		1	
17	Śruby M6 mocujące do zamontowania urządzeń w otworach szyn nośnych szafy sieciowej 19''		40	
Suma:				

Podane w zestawieniu nazwy oraz modele urządzeń są związane z koniecznością zachowania pełnej kompatybilności z infrastrukturą oraz systemem użytkowanym przez Zamawiającego.

*W przypadku braku dostępności nowych urządzeń z poz. 2, Zamawiający może dopuścić urządzenia które nie będą fabrycznie nowe.

1. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

** W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie)*

2. Oświadczam, że w przypadku przyznania nam zamówienia, zobowiązujemy się do zawarcia umowy na warunkach określonych w projekcie umowy załączonym do formularza oferty (załącznik nr 2).

3. Oświadczam, że zapoznałem się z opisem przedmiotu zamówienia i nie wnoszę do niego zastrzeżeń, a także zaoferowany sprzęt spełnia wszystkie wymogi (parametry techniczne) szczegółowego opisu przedmiotu zamówienia (załącznik nr 1).

4. Załącznikami do niniejszego formularza oferty stanowiącymi integralną część oferty są to:

- a. Wykaz oferowanego sprzętu wraz z parametrami technicznymi i kwotami brutto.
- b. Pełnomocnictwo (jeżeli jest wymagane).
- c. Aktualny odpis z właściwego rejestru lub centralnej ewidencji i informacji o działalności gospodarczej.
- d. Zaakceptowany (zaparafowany na każdej stronie) wzór umowy.

5. Osobą do kontaktu z Zamawiającym jest

tel.....

6. Termin wykonania zamówienia:

....., dnia.....

.....
podpis osoby uprawnionej

(pieczęć wykonawcy)

Wzór

UMOWA Nr SM

W dniu w Opolu pomiędzy:

Miastem Opole z siedzibą w Opolu, Rynek 1A, 45-015 NIP 7543009977

reprezentowanym przez:

**Krzysztofa Maślaka – Komendanta Straży Miejskiej w Opolu z siedzibą przy
ul. Władysława Reymonta 47 B, 45-072 Opole**

zwanym dalej „Zamawiającym” lub „Kupującym”

a

.....
.....NIP: , KRS: , REGON:

zwanym dalej „Sprzedającym”

reprezentowanym przez:

.....
została zawarta umowa następującej treści:

Umowa jest następstwem dokonanego przez Zamawiającego wyboru oferty w postępowaniu o udzielenie zamówienia publicznego o wartości poniżej kwoty 130.000 złotych netto, na podstawie Zarządzenia Nr SMK.0120.3.2021 Komendanta Straży Miejskiej w Opolu z dnia 26 stycznia 2021r.

§ 1

1. Przedmiotem umowy jest zakup przez Zamawiającego od Sprzedającego sprzętu komputerowego w ramach realizacji zadania pod nazwą „Zakup sprzętu sieciowego i akcesoriów komputerowych na potrzeby Straży Miejskiej w Opolu”, szczegółowo określonego w formularzu ofertowym stanowiącym załącznik nr 1 do złożonej oferty.
2. W ramach realizacji umowy Sprzedający zobowiązany jest dostarczyć przedmiot umowy Zamawiającemu.
3. Strony postanawiają, że odpowiedzialnymi za realizację przedmiotu umowy są:
 - a) w imieniu Zamawiającego: Paweł Chmiel tel. 503 790 095,
 - b) w imieniu Sprzedającego:
4. Sprzedający określi i przekaze Zamawiającemu telefony kontaktowe, numery faksów i adresy poczty elektronicznej oraz dokona innych ustaleń niezbędnych dla sprawnego i terminowego wykonania zobowiązań wynikających z umowy.

§ 2

Termin wykonania zamówienia: od dnia podpisania umowy.

§ 3

Miejsce dostawy: Straż Miejska w Opolu, ul. Władysława Reymonta 47B.

§ 4

1. Sprzedający będzie odpowiedzialny za całokształt, w tym za przebieg oraz terminowe wykonanie zamówienia w okresie umowy.
2. Sprzedający jest odpowiedzialny za jakość, zgodność z warunkami technicznymi i jakościowymi określonymi dla przedmiotu zamówienia

§ 5

1. Sprzedający za wykonanie Przedmiotu Umowy otrzyma wynagrodzenie brutto w wysokości:..... zł brutto (słownie złotych:.....) w tym podatek VAT.
2. Rozliczenie między stronami nastąpi na podstawie faktury, po odbiorze przedmiotu zamówienia. Faktura powinna zawierać następujące dane:
 - a) Nabywca: Miasto Opole, Rynek 1A, 45-015 Opole, NIP 7543009977
 - b) Odbiorca: Straż Miejska w Opolu, ul. Wł. Reymonta 47 B, 45-072 Opole.
3. Zapłata zostanie dokonana na konto Sprzedającego w terminie 21 dni od daty otrzymania faktury.
4. Podstawą do wystawienia faktury jest podpisanie przez Strony umowy protokołu, w którym potwierdzone zostanie prawidłowe wykonanie umowy.
5. Numer rachunku bankowego wskazany w fakturze musi być numerem właściwym do dokonywania rozliczeń na zasadach podzielonej płatności (split payment) i wskazanym w wykazie kont bankowych na tzw. białej liście, zgodnie z zapisami ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług.

§ 6

Strony ustanawiają odpowiedzialność w formie kar umownych z tytułów i w podanych wysokościach:

1. Zamawiający zapłaci Sprzedającemu karę umowną:
 - a) z tytułu odstąpienia od umowy z przyczyn niezależnych od Sprzedającego w wysokości 10% wynagrodzenia umownego.
2. Sprzedający zapłaci Zamawiającemu kary umowne:
 - a) z tytułu odstąpienia od umowy z przyczyn niezależnych od Zamawiającego w wysokości 10% wynagrodzenia umownego
 - b) za zwłokę w wykonaniu przedmiotu umowy w wysokości 0,5% wynagrodzenia umownego za każdy dzień zwłoki.
 - c) za zwłokę w usunięciu wad i usterek w okresie gwarancji w wysokości 0,5% wynagrodzenia umownego za każdy dzień zwłoki licząc od dnia wyznaczonego przez Zamawiającego na usunięcie wady.
2. Strony dopuszczają możliwość dochodzenia odszkodowania w wysokości przekraczającej wysokość zastrzeżonych kar umownych.

§ 7

1. Wykonawca udziela Zamawiającemu gwarancji :
 - a) w zakresie dostarczonych urządzeń na okres 24 miesięcy, nie krótszy jednak niż wynikający z gwarancji udzielanej przez producenta, od daty podpisania protokołu odbioru,
 - b) w pozostałym zakresie Przedmiotu Umowy na okres 36 miesięcy od daty podpisania protokołu odbioru.

2.Okres gwarancji na dostarczone urządzenia liczony jest od daty podpisania protokołu, o którym mowa w § 5 ust. 4 umowy.

3.W okresie gwarancji Sprzedający zobowiązany jest do nieodpłatnego usunięcia usterek/wad w terminie wyznaczonym przez Zamawiającego, który będzie nie dłuższy aniżeli 14 dni.

§ 8

Zmiana treści umowy może nastąpić za zgodą obu stron wyrażoną na piśmie pod rygorem nieważności.

§ 9

W sprawach nieuregulowanych w niniejszej umowie mają zastosowanie przepisy Kodeksu Cywilnego.

§ 10

Niniejsza umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, jeden dla Zamawiającego, jeden dla Sprzedającego.

ZAMAWIAJĄCY/KUPUJĄCY:

SPRZEDAJĄCY:

Załącznik Nr 1 do formularza ofertowego pn. „Zakup sprzętu sieciowego i akcesoriów komputerowych na potrzeby Straży Miejskiej w Opolu ”

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

Wraz z urządzeniem należy dostarczyć:

- akcesoria umożliwiające montaż urządzeń w szafie sieciowej 19”.
- dokumentację techniczną.

Zaofertowany sprzęt musi być fabrycznie nowy, objęty gwarancją producenta (obejmującą naprawę lub wymianę sprzętu w ciągu 72h od momentu zgłoszenia) na okres min. 24 miesięcy z opcją jej przedłużenia.

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

Specification	SRX300	SRX320	SRX340
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
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