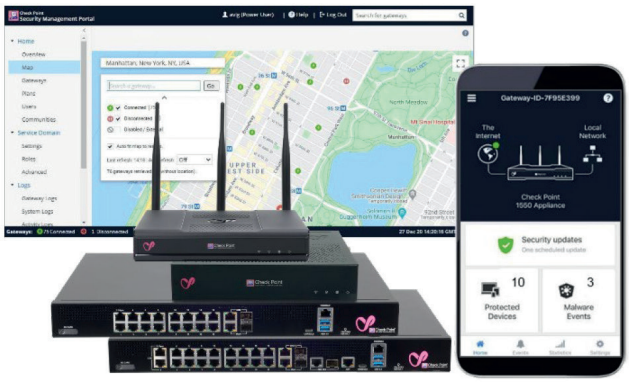
QUANTUM SPARK™ 1600, 1800 BRAMY BEZPIECZEŃSTWA

Proste, bezpieczne, kompleksowe.

Bramy bezpieczeństwa Check Point Quantum Spark to wydajne, zintegrowane urządzenia zapewniające zaporę sieciową, sieć VPN, ochronę antywirusową, widoczność i kontrolę aplikacji, filtrowanie adresów URL, ochronę poczty elektronicznej i funkcję SandBlast Zero-Day Protection. Mają niewielkie rozmiary, a ponadto są proste w konfigurowaniu i zarządzaniu.



QUANTUM SPARK - pełna ochrona dla małych i średnich firm

Ochrona przed każdym zagrożeniem

Łatwość wdrażania i zarządzania

Wielofunkcyjność

NAJWAŻNIEJSZE INFORMACJE

Zaawansowana ochrona, wyjątkowa wydajność

Bramy bezpieczeństwa Check Point Quantum Spark 1600 i 1800 to proste, niedrogie, wielofunkcyjne rozwiązania w obudowie o rozmiarach 1 U, zapewniające bezpieczeństwo klasy korporacyjnej małym i średnim firmom. Chronią one pracowników i sieci przed kradzieżą danych. Duża przepustowość systemu i portów z interfejsami sieciowymi 2,5 i10 GbE w modelu 1800 sprawia, że te zapory nowej generacji nadają się idealnie do sieci w małych firmach i oddziałach dużych przedsiębiorstw.

Kompleksowa ochrona

- Zapora sieciowa nowej generacji
- Sieć VPN między dwoma ośrodkami
- Sieć VPN dla pracowników zdalnych
- Kontrola aplikacji i filtrowanie adresów WWW
- Rozpoznawanie urządzeń Internetu rzeczy
- Zapobieganie włamaniom
- Ochrona antywirusowa
- Ochrona przed botami
- Ochrona przed spamem
- Funkcja SandBlast Threat Emulation (emulacja zagrożeń w środowisku testowym)

Oprogramowanie R80 dla małych i średnich firm

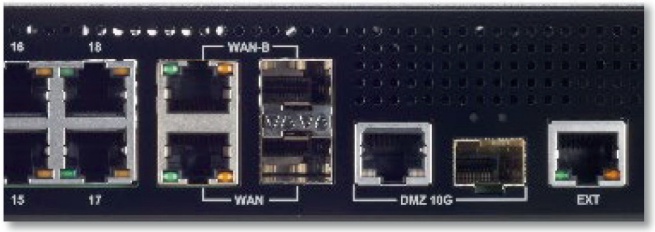
Oprogramowanie R80 zapewnia małym i średnim firmom bezpieczeństwo klasy korporacyjnej, a tym samym zwiększa ich wydajność. Centralnie zarządzane bramy udostępniają użytkownikom następujące funkcje:

- Ujednolicone reguły dostępu: zapora sieciowa, kontrola aplikacji, filtrowanie adresów URL
- Warstwy reguł i reguły szczegółowe
- Akceleracja obiektów domenowych, dynamicznych i czasowych
- Urządzenie VPN z wielordzeniowym procesorem i akceleracja VPN

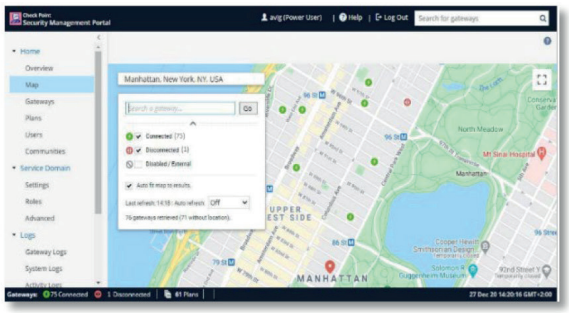
Łączność sieciowa 1/2,5/5/10 GbE

W modelu 1600 dostępne są opcje 1 GbE w technologii miedzi lub światłowodu dla sieci WAN i strefy DMZ. Model 1800 jest wyposażony w port zarządzania 1 GbE, opcję 2,5 GbE dla sieci LAN oraz opcję 10 GbE w technologii miedzi lub światłowodu dla strefy DMZ.

	1600	1800
LAN	16x 1 GbE (miedź)	16x 1 GbE (miedź) plus 2x 2,5 GbE (miedź)
DMZ	1x 1 GbE (miedź/światłowód)	1x 10 GbE (miedź/światłowód)
WAN	1x 1 GbE (miedź/światłowód)	2x 1 GbE (miedź/światłowód)
MGMT		1x 1 GbE (miedź)



Konfiguracja portu 1800



Zarządzanie w chmurze

Intuicyjny webowy interfejs użytkownika umożliwia usługodawcom zapewnienie skutecznej ochrony małym i średnim firmom, a dostępny w chmurze portal zarządzania bezpieczeństwem może zarządzać ponad 10 000 urządzeń Check Point Quantum Spark. Małe i średnie firmy mogą więc bardziej skupić się na swoim rozwoju, ponieważ o ich bezpieczeństwo informatyczne zadba dostawca usług.

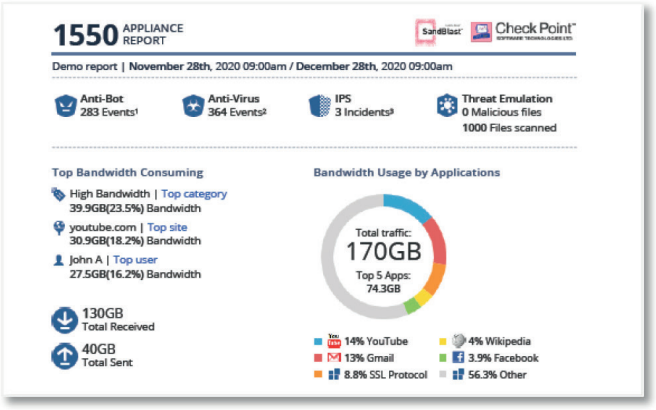
NAJWAŻNIEJSZE INFORMACJE

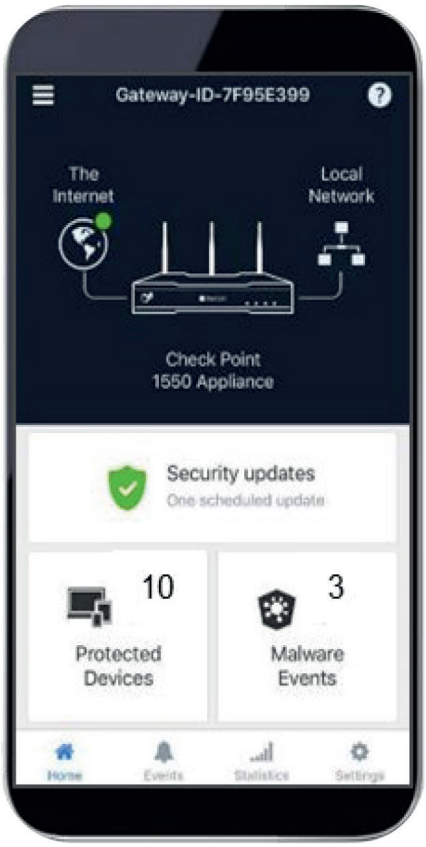
Dużo prostsze zarządzanie bezpieczeństwem

Konfigurację można przeprowadzić w ciągu kilku minut, korzystając ze wstępnie zdefiniowanych reguł bezpieczeństwa oraz konfiguratora „krok po kroku". Bramami bezpieczeństwa Check Point Quantum Spark można wygodnie zarządzać lokalnie za pośrednictwem interfejsu webowego, a centralnie — przy użyciu działającego w chmurze portalu Check Point Security Management Portal (SMP) lub rozwiązania R80 Security Management.

Proste, intuicyjne raportowanie

W interfejsie webowym widoczne są dzienniki, aktywne komputery oraz raporty godzinowe, dzienne, tygodniowe i miesięczne. Analiza sieci pozwala sprawdzić, które aplikacje i którzy użytkownicy wykorzystują najwięcej przepustowości, natomiast analiza bezpieczeństwa — zobaczyć użytkowników korzystających z ryzykownych serwisów WWW i aplikacji, a także incydenty lub zainfekowane hosty wykryte w okresie raportowania.



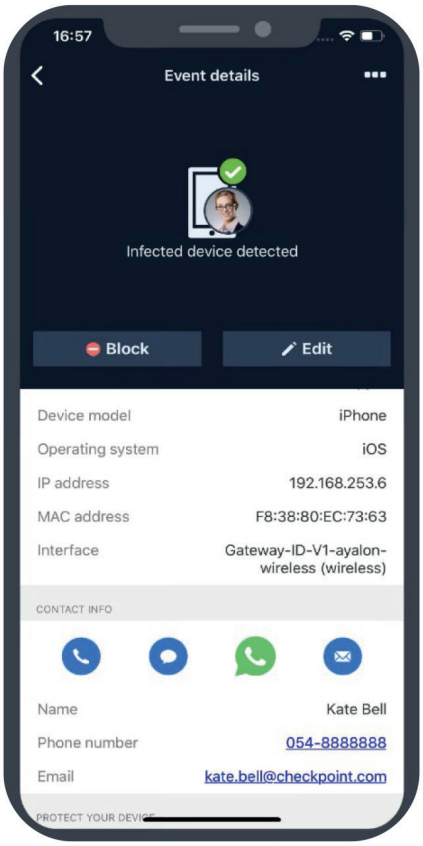


ANDROID APP ON Google play

Aplikacja do zarządzania bezpieczeństwem

Ta intuicyjna aplikacja mobilna monitoruje zdarzenia w sieci w czasie rzeczywistym, ostrzega o zagrożeniach i pozwala je szybko blokować, a ponadto umożliwia konfigurowanie reguł bezpieczeństwa dla wielu bram.

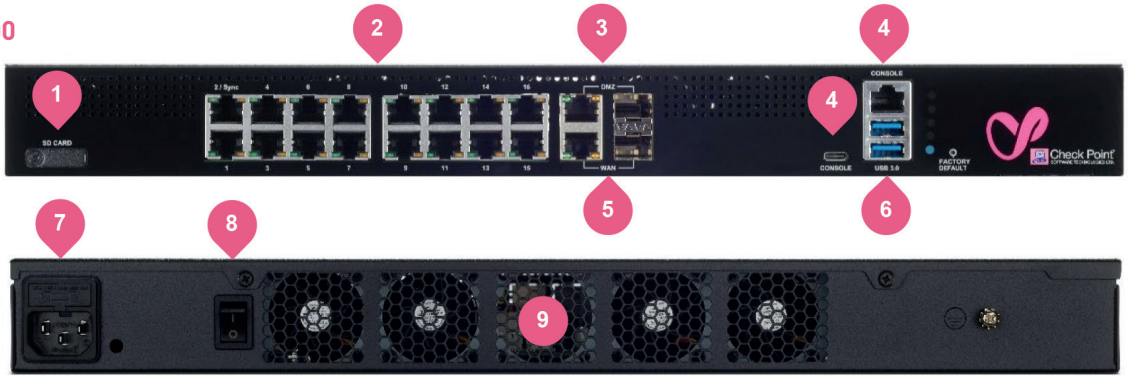
- **Obraz stanu bezpieczeństwa sieci:** widok podłączonych urządzeń i ewentualnych zagrożeń
- **Ostrzeżenia o zagrożeniach w czasie rzeczywistym:** informowanie o atakach i nieautoryzowanych urządzeniach
- **Walka z zagrożeniami na miejscu:** szybkie blokowanie zainfekowanych urządzeń
- **Raporty i wykresy dotyczące statystyk sieci:** wgląd w raporty użycia sieci
- **Zarządzanie wieloma bramami:** zarządzanie bezpieczeństwem za pomocą urządzenia mieszczącego się w dłoni



Download on the App Store

Brama bezpieczeństwa 1600

1. Gniazdo na kartę SD
2. Przełącznik LAN z 16 portami 1 GbE
3. 1 port DMZ 1 GbE (miedź/światłowód)
4. Port konsoli
5. 1 port WAN 1 GbE (miedź/światłowód)
6. Porty USB
7. 1 zasilacz
8. Włącznik zasilania
9. Wentylatory

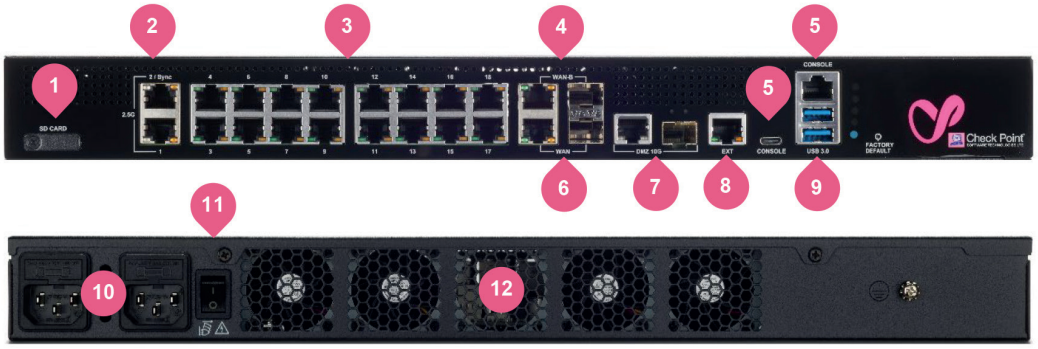


	1600
Warunki testowania produktu w przedsiębiorstwie	
Threat Prevention (Mb/s)1	1500
Next Generation Firewall (Mb/s)2	3200
IPS Throughput (Mb/s)	3500
Firewall Throughput (Mb/s)	4800
Testy wydajności zgodne ze standardem RFC 3511, 2544, 2647, 1242 (LAB)	
Firewall 1518 Byte UDP Packets (Mb/s)	8000
Przepustowość sieci VPN AES-128 (Mb/s)	3200
Liczba połączeń na sekundę	55 000
Concurrent Connections	2 400 000
Oprogramowanie	
Bezpieczeństwo	Zapora sieciowa, VPN, rozpoznawanie użytkownika, QoS, kontrola aplikacji, filtrowanie adresów URL (URLF), system zapobiegania włamaniom (IPS), ochrona przed botami, ochrona przed wirusami, ochrona przed spamem, emulacja zagrożeń w środowisku testowym (sandboxing)
Routing i tworzenie klastrów z transmisją unicast lub multicast	OSPF v2, BGP v4 i 4++, RIP, PIM (SM, DM, SSM), IGMP, ClusterXL High Availability
IPv6	Połączenia w lokalnej sieci i połączenia internetowe, tunelowanie ruchu IPv4 w sieci IPv6 z podwójnym stosem, delegowanie prefiksów
Licencja na dostęp z urządzeń mobilnych (użytkownicy)	500 zdalnych użytkowników klienta SNX lub Mobile VPN
Sprzęt	
Port WAN	1 port RJ-45 10/100/1000 Base-T / 1 port SFP 1000 BaseF (bez transceivera)
Port DMZ	1 port RJ-45 10/100/1000 Base-T / 1 port SFP 1000 BaseF (bez transceivera)
Porty przełącznika LAN	16 portów RJ-45 10/100/1000 Base-T
Port konsoli	1 port USB-C i 1 port RJ-45
Port USB	2 porty USB 3.0
Pamięc masowa	Gniazdo na kartę Micro-SD z opcjami 32 i 64 GB
eMMC	32 GB
Średni czas pracy bez awarii	22,26 lat przy temperaturze 25°C
Wymiary	
Wymiary (szer. x głęb. x wys.)	Obudowa w rozmiarze 1 RU: 430 x 300 x 44,2 mm
Waga	6,17 kg
Środowisko	
Działanie / przechowywanie	0°C ~ 40°C / -45°C ~ 60°C (5~95%, bez kondensacji)
Zasilanie	
Napięcie wejściowe prądu przemiennego	110 – 240 V, 50 – 60 Hz
Zasilacze	Jeden zasilacz 150 W
Zużycie energii (maks.)	71 W
Emisja ciepła	244.31
Certyfikaty	
Bezpieczeństwo	Emisje	Środowisko	UL/c-UL 62368-1 , IEC 62368-1 CB / EMC, EMI EN55024, EN55032 klasa B, VCCI, AS, NZS CISPR 32, IC ICES 03, FCC: część 15 klasaB / RoHS, REACH, WEEE

1. Obejmuje zaporę sieciową, kontrolę aplikacji, filtrowanie adresów URL, system zapobiegania włamaniom (IPS), ochronę antywirusową, ochronę przed botami, funkcję SandBlast Zero-Day Protection z rejestrowaniem. 2. Includes Firewall, Application Control, I PS with logging.

Brama bezpieczeństwa 1800

1. Gniazdo na kartę SD
2. 2 porty 2,5 GbE
3. Przełącznik LAN z 16 portami 1 GbE
4. 1 port WAN2 1 GbE (miedź/światłowód) (*planowany)
5. Port konsoli
6. 1 port WAN1 1 GbE (miedź/światłowód)
7. 1 port DMZ 10 GbE (miedź/światłowód)
8. 1 port zarządzania 1 GbE (*planowany)
9. 2 porty USB
10. 2 nadmiarowe zasilacze
11. Włącznik zasilania
12. Wentylatory



	1800
Warunki testowania produktu w przedsiębiorstwie	
Threat Prevention (Mb/s)[1]	2000
Next Generation Firewall (Mb/s)[2]	5000
IPS Throughput (Mb/s)	5500
Firewall Throughput (Mb/s)	7500
Testy wydajności zgodne ze standardem RFC 3511, 2544, 2647, 1242 (LAB)	
Firewall 1518 Byte UDP Packets (Mb/s)	17 000
Przepustowość sieci VPN AES-128 (Mb/s)	4000
Liczba połączeń na sekundę	66 000
Concurrent Connections	2 400 000
Oprogramowanie	
Bezpieczeństwo	Zapora sieciowa, VPN, rozpoznawanie użytkownika, QoS, kontrola aplikacji, filtrowanie adresów URL (URLF), system zapobiegania włamaniom (IPS), ochrona przed botami, ochrona przed wirusami, ochrona przed spamem, emulacja zagrożeń w środowisku testowym (sandboxing)
Routing i tworzenie klastrów z transmisją unicast lub multicast	OSPF v2, BGP v4 i 4++, RIP, PIM (SM, DM, SSM), IGMP, ClusterXL High Availability
IPv6	Połączenia w lokalnej sieci i połączenia internetowe, tunelowanie ruchu IPv4 w sieci IPv6 z podwójnym stosem, delegowanie prefiksów
Licencja na dostęp z urządzeń mobilnych (użytkownicy)	500 zdalnych użytkowników klienta SNX lub Mobile VPN
Sprzęt	
Port WAN	2 porty RJ-45 10/100/1000Base-T / SFP 1000BaseF (bez transceivera) *Obsługa WAN2 planowana w nowej wersji oprogramowania
Port DMZ	1 port RJ-45 10 GbE Base-T / port SFP+ 10 GbE (bez transceivera)
Porty przełącznika LAN	2 porty RJ-45 2,5 GbE Base-T plus 16 portów RJ-45 10/100/1000Base-T
Port zarządzania	1 port RJ-45 10/100/1000Base-T *Obsługa portu zarządzania (MGMT) planowana w nowej wersji oprogramowania
Port konsoli	1 port USB-C i 1 port RJ-45
Port USB	2 porty USB 3.0
Pamięc masowa	Gniazdo na dysk SSD 256 GB i kartę Micro-SD z opcjami 32 i 64 GB
eMMC	32 GB
Średni czas pracy bez awarii	15,64 roku przy temperaturze 25°C
Wymiary	
Wymiary (szer. x głęb. x wys.)	Obudowa w rozmiarze 1 RU: 430 x 300 x 44,2 mm
Waga	6,76 kg
Środowisko	
Działanie / przechowywanie	0°C ~ 40°C / -45°C ~ 60°C (5~95%, bez kondensacji)
Zasilanie	
Napięcie wejściowe prądu przemiennego	110 – 240 V, 50 – 60 Hz
Zasilacze	Dwa nadmiarowe zasilacze 150 W
Zużycie energii (maks.)	93,6 W
Emisja ciepła	319,3
Certyfikaty	
Bezpieczeństwo | Emisje | Środowisko	UL/c-UL 62368-1, IEC 62368-1 CB / EMC, EMI EN55024, EN55032 klasa B, VCCI, AS, NZS CISPR 32, IC ICES 03, FCC: część 15 klasa B / RoHS, REACH, WEEE

1. Obejmuje zaporę sieciową, kontrolę aplikacji, filtrowanie adresów URL, system zapobiegania włamaniom (IPS), ochronę antywirusową, ochronę przed botami, funkcję SandBlast Zero-Day Protection z rejestrowaniem. 2. Obejmuje zaporę sieciową, kontrolę aplikacji, system zapobiegania włamaniom (IPS) z rejestrowaniem

ZAMAWIANIE URZĄDZEŃ QUANTUM SPARK 1600, 1800

URZĄDZENIA ZABEZPIECZAJĄCE[1]	
Brama bezpieczeństwa 1600	CPAP-SG1600-SNBT
Brama bezpieczeństwa 1800	CPAP-SG1800-SNBT
AKCESORIA	
Transceiver SFP krótkiego zasięgu (dla portów DMZ/WAN 1000Base-F)	CPAC-TR-1SX
Transceiver SFP dalekiego zasięgu (dla portów DMZ/WAN 1000Base-F)	CPAC-TR-1LX
Transceiver SFP+ krótkiego zasięgu (dla portu DMZ 1800 10 GBase-F)	CPAC-1800-TR-10SR
Transceiver SFP+ dalekiego zasięgu (dla portu DMZ 1800 10 G Base-F)	CPAC-1800-TR-10LR
Karta pamięci SD 32 GB	CPAC-1500-32GB-SD
Karta pamięci SD 64 GB	CPAC-1500-64GB-SD
DODATKOWE MODUŁY SOFTWARE BLADE[2]	
Mobile_Access_Blade_for_50_concurrent_connections	CPSB-MOB-50

1. Należy dodać subskrypcję na NGFW, NGTP lub NGTX. Pakiety promocyjne na 3 i 5 lat obejmują urządzenie zabezpieczające oraz pakiet subskrypcji i wsparcia (zob. niżej). Licencja obejmuje obsługę protokołu SMP.
2. Liczba jednocześnie pracujących zdalnych użytkowników klienta SNX lub Mobile VPN Licencja MOB jest dostępna dodatkowo. Nie wszystkie funkcje portalu WWW Mobile Access są obsługiwane.

Pakiety urządzeń zabezpieczających oraz usług serwisu i wsparcia na 3 i 5 lat

	NGFW	NGTP	SNBT
Brama bezpieczeństwa	✓	✓	✓
Premium Support (odpowiedź w trybie 24x7, aktualizacje oprogramowania i inne usługi)	✓	✓	✓
Opcja PRO Support (proaktywne monitorowanie stanu urządzenia)	✓	✓	✓
Zapora sieciowa	✓	✓	✓
VPN	✓	✓	✓
Połączenia zdalne client-to-site (obejmuje 500 jednocześnie pracujących użytkowników)	✓	✓	✓
Kontrola aplikacji	✓	✓	✓
IPS	✓	✓	✓
Filtrowanie adresów URL		✓	✓
Ochrona antywirusowa i ochrona przed botami		✓	✓
Threat Emulation (emulacja zagrożeń w środowisku testowym)			✓

KONTAKT E-MAIL: INFO@CHECKPOINT.COM STRONA WWW: WWW.CHECKPOINT.COM