Check Point®
SOFTWARE TECHNOLOGIES LTD.

EINEN
SCHRITT
VORAUS

CHECK POINT APPLIANCES

2017

CHECK POINT APPLIANCES

BEDROHUNGSABWEHR DER NÄCHSTEN GENERATION

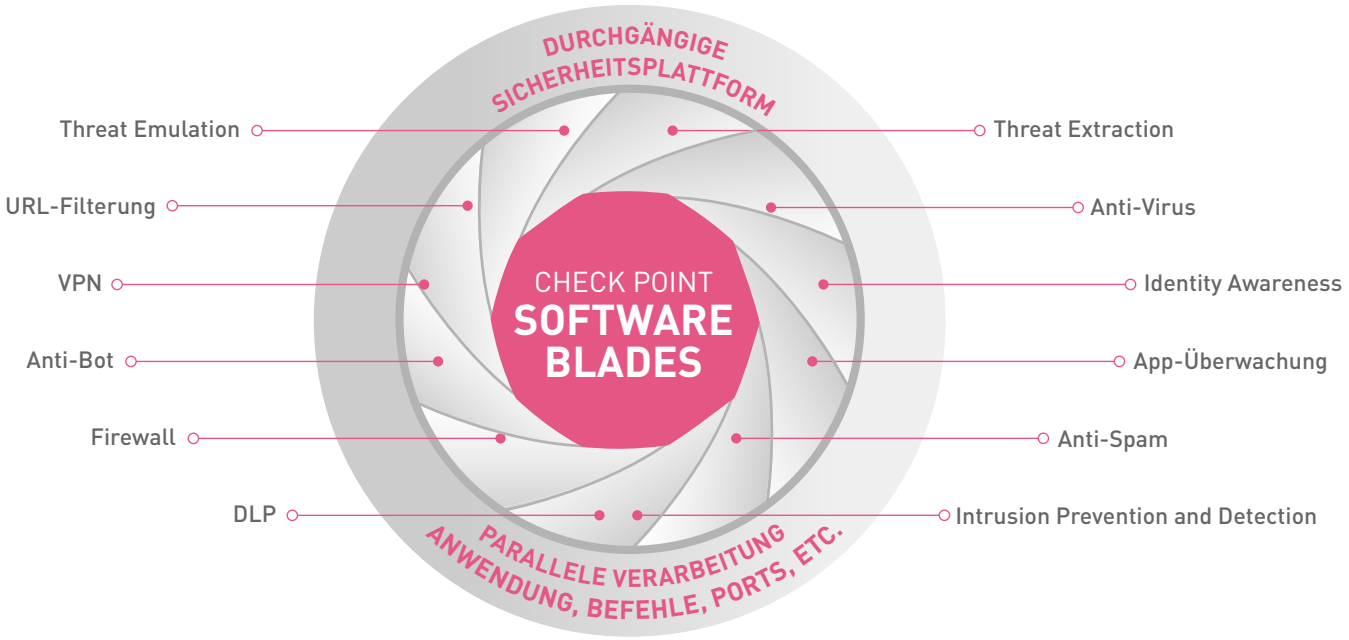
UMFASSENDER SCHUTZ VON GEFAHREN

Der rasante Anstieg an Malware, die immer raffinierteren Methoden der Angreifer und neu entstehende Zero-Day-Bedrohungen erfordern einen neuen Ansatz, um Unternehmensnetzwerke und Daten abzusichern. Check Points Lösung für die Bedrohungsabwehr bietet leistungsstarke Sicherheitsfunktionen wie Firewall, IPS, Anti-Bot, Anti-Virus, Anwendungsüberwachung und URL-Filterung, um bekannte Cyberattacken und Bedrohungen zu bekämpfen. Diese Lösung umfasst jetzt auch die vielfach ausgezeichnete SandBlast™ Threat Emulation und Threat Extraction, die vollständigen Schutz auch vor den komplexesten Bedrohungen und Zero-Day-Schwachstellen leistet.

BEKANNTEN BEDROHUNGEN UND ZERO-DAY-ANGRIFFEN VORBEUGEN

Als Teil der Lösung Check Point SandBlast Zero-Day Protection, erkennt die cloudbasierende Engine für Threat Emulation, Malware bereits während der Exploit-Phase, noch bevor die Hacker Evasion-Techniken für die Verschleierung anwenden und die Sandbox umgehen können. Dateien werden in Quarantäne genommen und in einer virtuellen Sandbox untersucht, um schadhaftes Verhalten erkennen zu können bevor die Malware in Ihr Unternehmensnetzwerk eindringen kann. Die innovative Lösung kombiniert Untersuchungen auf CPU-Ebene und Sandboxing auf Betriebssystem-Ebene, um Infektionen mit den gefährlichsten Exploits, Zero-Day-Angriffen und zielgerichteten Angriffen vorbeugen zu können.

Darüber hinaus entfernt SandBlast Threat Extraction entsprechende Inhalte wie beispielsweise aktive oder eingebettete Inhalte, rekonstruiert Dateien, um mögliche Bedrohungen zu beseitigen, und stellt den Anwendern die bereinigten Inhalte umgehend zur Verfügung, sodass die Geschäftsabläufe nicht beeinträchtigt werden.



IHR SICHERES UND MASSGESCHNEIDERTES BETRIEBSSYSTEM DER NÄCHSTEN GENERATION

GAIA – EIN EINHEITLICHES UND SICHERES BETRIEBSSYSTEM

Check Point GAiA™ ist das sichere Next-Generation-Betriebssystem für alle Check Point Appliances, Open Server und virtualisierten Gateways. Kunden profitieren von diesem hocheffizienten 64-Bit-Betriebssystem, der Vielzahl an Anschlussmöglichkeiten für die Appliances und schlanken betrieblichen Prozessen. GAiA vereinfacht das Management dank der funktionalen Aufgabenverteilung für Nutzer mit verschiedenen Rechten und der rollenbasierenden Administration. Die Möglichkeit, Software-Updates automatisch auszuführen, steigert die operative Effizienz und die funktionsreiche Web-Oberfläche erlaubt es, in Sekundenschnelle bestimmte Befehle oder Attribute zu finden. IPv4- und IPv6-Netzwerke können Acceleration- und Clustering-Technologien sicher nutzen und die aktuellen Unicast- und Multicast-Routing-Protokolle einsetzen.

NUTZEN SIE DIE MÖGLICHKEITEN DER VIRTUALISIERUNG

Check Points virtualisierte Systeme ermöglichen es, mehrere virtualisierte Security-Gateways auf einem einzigen Hardware-System zu vereinen. Unternehmen können so durchgängige Sicherheit gewährleisten und dabei ihre Infrastruktur konsolidieren und erhebliche Kosten einsparen. Das schlanke Management dieser virtualisierten Gateways verbessert die betrieblichen Abläufe und die Effizienz und sorgt für die gewünschte Einfachheit – das ist vor allem in IT-Abteilungen mit geringen personellen Ressourcen von Vorteil.

NEUE WEGE, UM DIE LEISTUNGSSTÄRKE VON SECURITY-APPLIANCES ZU MESSEN

Im Gegensatz zu anderen Anbietern, deren Leistungskennzahlen auf optimierten Testkonditionen basieren und deren Policy lediglich eine Regel umfasst („Accept Any"), basiert die Leistungsmessung von Check Points Security-Appliances auf realem Datenverkehr der Kunden, zahlreichen Sicherheitsfunktionen und typischen Sicherheitsrichtlinien. SecurityPower™ bietet eine effektive Metrik für die Wahl der passenden Appliance, die das aktuelle und künftige Verhalten während eines Angriffs und im täglichen Betrieb aufzeigen kann. Kunden können sich somit darauf verlassen, dass sie eine Security-Appliance wählen, die ihren aktuellen Anforderungen entspricht und die Voraussetzungen für künftiges Wachstum geschaffen sind.

SecurityPower

SECURITY-APPLIANCES

Check Point bietet mit der integrierten Next-Generation-Plattform für die Bedrohungsabwehr Kunden jeder Größe den modernsten und aktuellsten Schutz für ihre Daten und Netzwerke und reduziert dabei die Komplexität und die Gesamtkosten. Ganz gleich, ob Sie eine Sicherheitslösung der nächsten Generation für Ihr Data-Center, Ihr kleines, mittelständisches oder großes Unternehmen oder Ihr Home Office suchen, Check Point hat die passende Lösung für Sie.

Niederlassungen	Einsatzbereich	Niederlassungen oder kleine Büros	1100
	Formfaktor	Desktop	1400
	Schnittstellen	1 GbE, 802.11n/ac Wi-FI, 3G/4G	2200
	Firewall-Durchsatz	750 Mbps to 4 Gbps	3100, 3200
	Weitere Funktionen	DSL, Web-Management	
Große Unternehmen	Einsatzbereich	Große Unternehmen	4200, 4400
	Formfaktor	1 HE	4600, 4800
	Schnittstellen	1, 10, 40 GbE	5100, 5200, 5400
	Firewall-Durchsatz	3 bis 35 Gbps	5600, 5800, 5900
	Weitere Funktionen	Flexible I/O-Optionen	12200
Data-Center	Einsatzbereich	Große Unternehmen und Data-Center	12400, 12600
	Formfaktor	2 HE	13500, 13800
	Schnittstellen	1, 10, 40 GbE	15400, 15600
	Firewall-Durchsatz	25 to 128 Gbps	21400, 21700, 21800
	Weitere Funktionen	Geringe Latenz, 40 GbE, Gleichstromversorgung, Lights-Out-Management LOM	23500, 23800
Chassis-Systeme	Einsatzbereich	Data-Center, Telcos, Carrier	41000
	Formfaktor	6 HE bis 15 HE	61000
	Schnittstellen	1, 10, 40 GbE	
	Firewall-Durchsatz	80 bis 400 Gbps	
	Weitere Funktionen	Skalierbare Blade-Plattform, Gleichstromversorgung	
Robuste Systeme	Einsatzbereich	Raue Umgebungsbedingungen	1200R
	Formfaktor	Desktop, DIN-Montage	
	Schnittstellen	1 GbE, 3G/4G-Unterstützung	
	Firewall-Durchsatz	2 Gbps	
	Weitere Funktionen	Gleichstrom- und Wechselstromversorgung	

1400 APPLIANCES

SICHERHEIT FÜR NIEDERLASSUNGEN UND GESCHÄFTSSTELLEN

1430-1450 APPLIANCE
(MIT WIFI-OPTION)

1470-1490 APPLIANCE
(MIT WIFI-OPTION)

ÜBERBLICK

Es ist eine große Herausforderung, die durchgängige, konsistente Netzwerksicherheit im gesamten Unternehmen zu gewährleisten, wenn Niederlassungen, Geschäftsstellen oder Remote-Offices angebunden werden müssen und die Mitarbeiter dort über geringe oder keine IT-Expertise verfügen. Die Büros müssen jedoch über dasselbe Sicherheitsniveau verfügen und vor Cyberbedrohungen und Zero-Day-Attacken geschützt werden, wie der Hauptsitz des Unternehmens. Die Check Point 1400 Appliances sind einfach bereitzustellende und kosteneffiziente Komplettlösungen, die branchenführenden Schutz bieten, um das schwächste Glied im Unternehmensnetzwerk zu schützen – den entfernten Standort.

Mit der vielfach ausgezeichneten Check Point Threat Prevention können Sie Ihr gesamtes Netzwerk vor Cyberbedrohungen schützen – sowohl den Hauptsitz als auch die angebundenen Standorte. Die 1400 Appliances eignen sich optimal für kleine Büros. Für das Management und den Support in kleinen Büroumgebungen steht eine intuitive, webbasierende Management-Schnittstelle zur Verfügung. Unternehmen, die Ihre Sicherheitslösung zentral verwalten möchten, können Check Point Security Management oder Multi-Domain Security Management nutzen, um Hunderte von Geräten an verschiedenen Standorten remote zu verwalten und Sicherheitsrichtlinien konsistent durchzusetzen.

UMFASSENDE SICHERHEIT

Die umfassende Next Generation Threat Prevention (NGTP) nutzt mehrere Sicherheitsebenen, um vor ausgefeilten Cyberbedrohungen zu schützen – mit Anwendungskontrolle, URL-Filterung, Anti-Bot, Anti-Virus und E-Mail-Sicherheit.

ALLGEMEINER ÜBERBLICK

Die Appliance bietet eine Vielzahl an Optionen für Netzwerkschnittstellen wie 1 GbE Ethernet-Ports, 802.11b/g/n/ac WiFi mit Gastzugängen oder drahtlose 3G- und 4G-Verbindungen.

MAXIMALE KAPAZITÄTEN	1430	1450	1470	1490
Firewall-Durchsatz (Mbps) [1]	900	1.100	1.600	1.800
Durchsatz mit Threat Prevention (Mbps) [1]	90	150	175	220
1 GbE-Ports	1x WAN, 1x DMZ, 6x LAN-Switch		1x WAN, 1x DMZ, 16x LAN-Switch	
Wi-Fi-Option	802.11 b/g/n/ac		802.11 b/g/n UND 802.11 n/ac	
Funkbereich	1: 2.4Ghz oder 5Ghz		2 gleichzeitig: 2.4Ghz und 5Ghz	

[1] Die Leistung gemessen bei einem realen, durchschnittlichen Datenverkehr und einem typischen Regelsatz, wobei NAT und Logging aktiviert sind und die höchste Stufe der Bedrohungsabwehr für Sicherheit sorgt.

Weitere Informationen: www.checkpoint.com/products/1400-security-appliances/

1200R RUGGED APPLIANCE

SICHERHEIT FÜR RAUE UMGEBUNGSBEDINGUNGEN

1200R APPLIANCE

ÜBERBLICK

Der Schutz kritischer Infrastrukturen vor Cyberbedrohungen ist mit einzigartigen Herausforderungen verbunden. Es kann sich um schwierige Umgebungsbedingungen handeln und die Systeme nutzen oftmals spezielle Protokolle. Check Points ICS/SCADA-Lösungen für Cybersicherheit ermöglichen umfassenden Schutz vor Bedrohungen und verfügen über ein robustes und widerstandsfähiges Design. Zudem bieten sie eine umfassende Protokoll-Unterstützung, um alle betriebsrelevanten Ressourcen wie Energieversorgungseinrichtungen, Verkehrsleitsysteme, Wasseraufbereitungsanlagen und Produktionsstätten vor Kompromittierungen zu schützen.

Die 1200R Appliance ergänzt Check Points umfassende Familie an Appliances, um verschiedenste Infrastruktur- und Produktionsumgebungen zu schützen und die speziellen Anforderungen dieser erfüllen zu können. So entspricht die 1200R Appliance beispielsweise den Standards IEEE 1613 und IEC 61850-3 für Wärme- und Vibrationsbeständigkeit sowie Störfestigkeit gegen elektromagentische Beeinflussung (EMI). Selbst bei extremen Temperaturen von -40°C bis 75°C sichert diese Appliance Ihre Infrastruktur ab, während andere Appliances hier versagen würden.

UMFASSENDE SICHERHEIT

NEXT GENERATION FIREWALL

NEXT GENERATION THREAT PREVENTION

ALLGEMEINER ÜBERBLICK

1 GbE Ethernet-Ports (Kupfer oder Glasfaser) sind ebenso verfügbar wie die Unterstützung von drahtlosen 3G- und 4G-Verbindungen durch kompatible USB-Modems.

MAXIMALE KAPAZITÄTEN	1200R
Firewall-Durchsatz (Mbps) [1]	700
IPS-Durchsatzt (Mbps) [1]	60
WAN	1x 10/100/1000Base-T RJ45- oder 1x 1000BaseF-Port
DMZ	1x 10/100/1000Base-T RJ45- oder 1x 1000BaseF-Port
LAN	4x 10/100/1000Base-T RJ45-Ports
Montage-Optionen	DIN-Schienenmontage oder Rack-Montage
Industrie-Zertifizierungen	IEEE 1613, IEC 61850-3
Stromversorgung	Wechsel- oder Gleichstrom

[1] Die Leistung gemessen bei einem realen, durchschnittlichen Datenverkehr und einem typischen Regelsatz, wobei NAT und Logging aktiviert sind und die höchste Stufe der Bedrohungsabwehr für Sicherheit sorgt.

Weitere Informationen: www.checkpoint.com/products/industrial-control-systems-appliances/

3000 APPLIANCES

UNTERNEHMENSSICHERHEIT FÜR NIEDERLASSUNGEN

3100 & 3200 APPLIANCE

ÜBERBLICK

Durchgängige Sicherheit erfordert einen konsistenten Schutz über alle Standorte hinweg – nicht nur für das Unternehmensnetzwerk am Hauptsitz. Dasselbe Sicherheitsniveau ist auch für entfernte Standorte und Niederlassungen erforderlich, um einen einheitlichen und umfassenden Schutz vor möglichen Bedrohungen gewährleisten zu können. Die Check Point 3000 Appliances ist die ideale Lösung für kleine Büros, Geschäftsstellen und Niederlassungen.

Die 3000 Appliances bietet Sicherheit auf höchstem Niveau und ohne Kompromisse in einem kompakten Desktop-Design. Die Multi-Core-Technologie, sechs 1-Gigabit-Ethernet-Ports und eine moderne Bedrohungsabwehr ermöglichen es, kleine Büros und entfernte Standorte genauso umfassend zu schützen wie den Hauptstandort. Obgleich des kleinen Formfaktors erzielt die leistungsstarke Appliance bis zu 2,1 Gbps Firewall-Durchsatz und bis zu 140 Mbps Durchsatz bei der Bedrohungsabwehr – und dies unter realen Bedingungen im Unternehmen.

UMFASSENDE SICHERHEIT

THREAT PREVENTION

THREAT PREVENTION + SANDBLAST

ALLGEMEINER ÜBERBLICK

Die 3200 Appliance bietet ein kompaktes Design, Multi-Core-Technologie sowie SandBlast Zero-Day Threat Prevention und eignet sich damit optimal als Gateway für kleine Büros, entfernte Standorte und Niederlassungen.

MAXIMALE KAPAZITÄTEN	3100	3200
Firewall-Durchsatz (Gbps) [1]	2,1	2,1
Durchsatz mit Threat Prevention (Mbps) [1]	95	140
1 GbE-Ports (Kupfer) (Base/Max)	6/6	6/6
RAM	8	8
HDD or SSD	1x 320 GB HDD oder 1x 240 GB SSD	1x 320 GB HDD or 1x 240 GB SSD

[1] Die Leistung gemessen bei einem realen, durchschnittlichen Datenverkehr und einem typischen Regelsatz, wobei NAT und Logging aktiviert sind und die höchste Stufe der Bedrohungsabwehr für Sicherheit sorgt.

Weitere Informationen: www.checkpoint.com/products/3200-security-appliances

5000 APPLIANCES

SICHERHEIT DER UNTERNEHMENSKLASSE, FLEXIBLE NETZWERK-OPTIONEN

5100/5200 APPLIANCE

5400 APPLIANCE

5600 APPLIANCE

5800 APPLIANCE

5900 APPLIANCE

ÜBERBLICK

Wenn es um Sicherheit geht, müssen Unternehmen heute nicht mehr die Wahl zwischen Funktionsumfang und Leistung treffen. Die für diesen Zweck bestimmten Check Point 5000 Appliances bieten für kleine und mittelgroße Unternehmensnetzwerke den umfassendsten Schutz vor Bedrohungen und Sicherheit – ohne Kompromisse eingehen zu müssen.

Die Check Point 5000 Appliances vereinen zahlreiche Optionen für Netzwerk-Schnittstellen, Multi-Core-Fähigkeit und höchste Leistung und ermöglichen damit einen herausragenden, mehrstufigen Schutz. Die 5000 Appliances bieten bis zu sechzehn (26) 1-Gigabit-Ethernet-Ports, redundante, im laufenden Betrieb austauschbare Netzteile und ein optionales LOM-Modul (Out-of-Band) in der kompakten Größe von einer Höheneinheit für die Rack-Montage. Sie unterstützen bis zu 22 Gbps Firewall-Durchsatz und bis zu 1 Gbps Durchsatz bei der Bedrohungsabwehr – und dies unter realen Bedingungen im Unternehmen. Damit bieten diese Appliances die höchste Leistung in ihrer Klasse.

UMFASSENDE SICHERHEIT

THREAT PREVENTION

THREAT PREVENTION + SANDBLAST

ALLGEMEINER ÜBERBLICK

Die Serie der 5000 Appliances zeichnet sich durch ein modulares Design und zahlreiche Netzwerk-Optionen aus: Die Gateways bieten nicht nur eine ganze Reihe an Anschlussmöglichkeiten, sondern lassen sich auch sehr flexibel für die Nutzung in jeder Netzwerk-Umgebung anpassen.

MAXIMALE KAPAZITÄTEN	5100	5200	5400	5600	5800	5900
Firewall-Durchsatz (Gbps) [1]	4,2	5,3	10	17,5	22	26
Durchsatz mit Threat Prevention (Gbps) [1]	200 Mbps	250 Mbps	330 Mbps	540 Mbps	1 Gbps	1,4 Gbps
1 GbE-Ports (Kupfer) (Base/Max)	6/14	6/14	10/18	10/18	10/26	10/26
1 GbE-Ports (Glasfaser) (Base/Max)	0/4	0/4	0/4	0/4	0/8	0/8
10 GbE-Ports (Glasfaser) (Base/Max)				0/4	0/8	0/8
40 GbE-Ports QSFP (Base/Max)					0/4	0/4
RAM	8 GB	8, 16 GB	8, 16, 32 GB	8, 16, 32 GB	8, 16, 32 GB	8, 16, 32 GB
HDD oder SSD	1 x 500 GB HDD oder 1 x 240 GB SSD					
Duales, Hot-Swappable Netzteil				optional	optional	optional
Lights-Out-Management (LOM)	optional	optional	optional	optional	inklusive	inklusive
Steckplätze	1	1	1	1	2	2

[1] Die Leistung gemessen bei einem realen, durchschnittlichen Datenverkehr und einem typischen Regelsatz, wobei NAT und Logging aktiviert sind und die höchste Stufe der Bedrohungsabwehr für Sicherheit sorgt.

Weitere Informationen: www.checkpoint.com/products/5000-security-appliances/

15000 APPLIANCES

BEDROHUNGSABWEHR FÜR GROSSE UNTERNEHMEN

15400 APPLIANCE

15600 APPLIANCE

ÜBERBLICK

Große Unternehmen haben die höchsten Anforderungen an die Leistung, die Verfügbarkeit und die Skalierbarkeit. Die 15000 Appliances vereinen umfassenden Schutz mit für diese Zwecke entwickelter Hardware. Diese leistungsstarken Security-Appliances erreichen einen realen Durchsatz bei der Bedrohungsabwehr von 2,5 Gbps, um alle unternehmenskritischen Ressourcen optimal abzusichern.

Die Check Point 15000 Appliances eignen sich hervorragend für große Unternehmensnetzwerke, die eine hohe Leistung und flexible I/O-Optionen erfordern. Falls Sie von 10 auf 40 GbE umsteigen möchten, sind die 15000 Appliances bereit dafür. Die Appliances mit zwei Höheneinheiten bieten drei I/O-Erweiterungssteckplätze für höhere Anschlusskapazitäten, redundante Netzteile (Wechsel- oder Gleichstrom), ein 2x 1 TB RAID1-Disk-Array sowie Lights-Out-Management (LOM) für die Administration remote.

UMFASSENDE SICHERHEIT

THREAT PREVENTION

THREAT PREVENTION + SANDBLAST

ALLGEMEINER ÜBERBLICK

Die Serie der 15000 Appliances zeichnet sich durch ein modulares Design und zahlreiche Netzwerk-Optionen aus: Die Gateways bieten nicht nur eine ganze Reihe an Anschlussmöglichkeiten, sondern lassen sich auch sehr flexibel für die Nutzung in jeder Netzwerk-Umgebung anpassen.

MAXIMALE KAPAZITÄTEN	15400	15600
Firewall-Durchsatz (Gbps) [1]	30	30
Durchsatz mit Threat Prevention (Gbps) [1]	1,5	2,5
1 GbE-Ports (Kupfer) (Base/Max)	10/26	10/26
1 GbE-Ports (Glasfaser) (Base/Max)	0/12	0/12
10 GbE-Ports (Glasfaser) (Base/Max)	2/12	2/12
40 GbE-Ports QSFP (Base/Max)	0/4	0/4
RAM	8, 24, 64 GB	8, 24, 64 GB
HDD oder SSD	1 x 1 TB HDD or 1 x 480 GB SSD	2 x 1 TB HDD or 2 x 480 GB SSD RAID1
Hot-Swappbable Netzteil	AC oder DC	AC oder DC
Lights-Out-Management (LOM)	inklusive	inklusive
Steckplätze	3	3

[1] Die Leistung gemessen bei einem realen, durchschnittlichen Datenverkehr und einem typischen Regelsatz, wobei NAT und Logging aktiviert sind und die höchste Stufe der Bedrohungsabwehr für Sicherheit sorgt.

Weitere Informationen: www.checkpoint.com/products/15000-security-appliances/

23000 APPLIANCES

BEDROHUNGSABWEHR IN DATA-CENTERN

23500 APPLIANCE

23800 APPLIANCE

ÜBERBLICK

Data-Center haben die höchsten Anforderungen an die Leistung, die Verfügbarkeit und die Skalierbarkeit. Die 23000 Appliances vereinen umfassenden Schutz mit für diese Zwecke entwickelter Hardware. Diese leistungsstarken Security-Appliances erreichen einen realen Durchsatz bei der Bedrohungsabwehr von 3,6 Gbps, um alle unternehmens-kritischen Ressourcen optimal abzusichern.

Die Check Point 23000 Appliances eignen sich hervorragend für Data-Center-Netzwerke, die eine hohe Leistung und flexible I/O-Optionen erfordern. Falls Sie von 10 auf 40 GbE umsteigen möchten, sind die 23000 Appliances bereit dafür. Die Appliances mit zwei Höheneinheiten bieten fünf I/O-Erweiterungssteckplätze für höhere Anschlusskapazitäten, redundante Netzteile (Wechsel- oder Gleichstrom), ein 2x 1 TB RAID1-Disk-Array sowie Lights-Out-Management (LOM) für die Administration remote.

UMFASSENDE SICHERHEIT

THREAT PREVENTION

THREAT PREVENTION + SANDBLAST

ALLGEMEINER ÜBERBLICK

Die Serie der 23000 Appliances zeichnet sich durch ein modulares Design und zahlreiche Netzwerk-Optionen aus: Die Gateways bieten nicht nur eine ganze Reihe an Anschlussmöglichkeiten, sondern lassen sich auch sehr flexibel für die Nutzung in jeder Netzwerk-Umgebung anpassen.

MAXIMALE KAPAZITÄTEN	23500	23800
Firewall-Durchsatz (Gbps) [1]	34	43
Durchsatz mit Threat Prevention (Gbps) [1]	2,9	3,6
1 GbE-Ports (Kupfer) (Base/Max)	10/42	10/42
1 GbE-Ports (Glasfaser) (Base/Max)	0/20	0/20
10 GbE-Ports (Glasfaser) (Base/Max)	2/20	2/20
40 GbE-Ports QSFP (Base/Max)	0/4	0/4
RAM	16, 64,128 GB	32, 64, 128 GB
HDD oder SSD	2 x 1 TB HDD or 2 x 480 GB SSD RAID1	2 x 1 TB HDD or 2 x 480 GB SSD RAID1
Hot-Swappbable Netzteil	AC oder DC	AC oder DC
Lights Out Management (LOM)	inklusive	inklusive
Steckplätze	5	5

[1] Die Leistung gemessen bei einem realen, durchschnittlichen Datenverkehr und einem typischen Regelsatz, wobei NAT und Logging aktiviert sind und die höchste Stufe der Bedrohungsabwehr für Sicherheit sorgt.

Weitere Informationen: www.checkpoint.com/products/23000-security-appliances/

41000 & 61000 SICHERHEITSSYSTEME

SKALIERBARE MULTI-BLADE-LEISTUNG

41000 UND 61000 SICHERHEITSSYSTEME

ÜBERBLICK

Wenn es um den Schutz von äußerst anspruchsvollen Netzwerk-Umgebungen in Data-Centern, bei Telekommunikationsanbietern und Cloud-Service-Providern geht, sind die Sicherheit und die Leistung zwei äußerst kritische Faktoren, die nicht beeinträchtigt werden dürfen. Die Multi-Blade-Hardware- und -Software-Architektur der 41000 und 61000 Sicherheitssysteme eignet sich optimal für diese Umgebungen. Die Plattform ermöglicht einen realen Firewall-Durchsatz von bis zu 40 Gbps mit der Plattform 41000 und bis zu 120 Gbps mit der Plattform 61000.

UMFASSENDE SICHERHEIT

Die Next Generation Firewall (NGFW) identifiziert und kontrolliert Anwendungen auf Basis eines jeden Users und scant die Inhalte, um Bedrohungen abzuwehren — mit IPS und der Anwendungsüberwachung.

ALLGEMEINER ÜBERBLICK

Das für Carrier geeignete ATCA-Chassis, das von Grund auf dafür entwickelt wurde, die hohen Anforderungen von Data-Centern und Service-Providern an die Verlässlichkeit, die Verfügbarkeit und die Betriebsfähigkeit zu erfüllen, läuft im Hochverfügbarkeits- und Lastverteilungsmodus für die Security-Gateway-Module, die in diesem Chassis untergebracht sind. Falls Unternehmen die Redundanz noch weiter verbessern möchten, können sie ein weiteres Chassis im Hochverfügbarkeitsmodus hinzufügen, sodass alle geschäftskritischen Ressourcen stets verfügbar und optimal geschützt sind.

MAXIMALE KAPAZITÄTEN	41000	61000
Firewall-Durchsatz (Gbps) [1]	bis zu 40	bis zu 120
IPS-Durchsatz (Gbps) [1]	bis zu 25	bis zu 70
10 GbE-Ports (Glasfaser)	bis zu 30	bis zu 60
40 GbE-Ports (Glasfaser)	bis zu 4	bis zu 8
Security-Switch-Module	1 bis 2	2 bis 4
Security-Gateway-Module	1 bis 4	2 bis 12
Netzteile	3 AC oder 2 DC	4 AC oder 2 DC

[1] Die Leistung gemessen bei einem realen, durchschnittlichen Datenverkehr und einem typischen Regelsatz, wobei NAT und Logging aktiviert sind und die höchste Stufe der Bedrohungsabwehr für Sicherheit sorgt.

Weitere Informationen: www.checkpoint.com/products/41000-61000-security-systems/

VIRTUELLE APPLIANCES

SICHERHEIT IN DER PUBLIC UND DER PRIVATE CLOUD

Die breite Akzeptanz und Umsetzung von Cloud-Architekturen – sei es Public, Private oder Hybrid Cloud Computing – wird von dem Wunsch getrieben, den Geschäftsbetrieb effizienter, schneller und flexibler zu gestalten und und die Kosten im Griff zu behalten. Obgleich die Cloud viele Vorteile im Vergleich zu den traditionellen Infrastrukturen bietet, stellt sie Ihr Unternehmen auch vor eine ganze Reihe an Sicherheitsherausforderungen. Check Point bietet ein vollständiges Portfolio für die Sicherheit in der Public und Private Cloud und dehnt damit die klassischen Schutzmaßnahmen auf jede Cloud-Umgebung aus, sodass Sie sich in Ihrer Cloud-Umgebung genauso abgesichert fühlen können wie in Ihrer physischen IT-Umgebung.

DIE SICHERHEITSHERAUSFORDERUNGEN DER PUBLIC CLOUD

Falls Sie Ihre Computing-Ressourcen und Ihre Daten in die Cloud verlagern, können Sie sich die Verantwortlichkeit für die Sicherheit mit Ihrem Cloud Service Provider teilen. Der Kontrollverlust, die Anwendungen und die Daten aus dem Unternehmen zu geben und an einen Cloud Provider – wie Amazon Web Services oder Microsoft Azure – zu übertragen und die daraus resultierenden Herausforderungen, diese Ressourcen zu überwachen und zu steuern, lässt eine Menge Sicherheitsfragen entstehen. Dies gilt vor allem für die anonyme, multi-mandantenfähige Umgebung der Public Cloud.

Viele Unternehmen nutzen hybride Clouds, um die Kontrolle über die Private-Cloud-Infrastruktur zu behalten, die vertraulichen Ressourcen zu schützen und andere wiederum in die Public Cloud auszulagern. Die neue Herausforderung der hybriden Cloud ist es, die Daten, die zwischen dem Unternehmensnetzwerk und der Public Cloud ausgetauscht werden, abzusichern.

Check Point vSEC bietet umfassenden Schutz vor Bedrohungen und eine einzige, zentrale Management-Konsole („Single-Pane-of-Glass"), um den Schutz der Daten und Ressourcen sehr einfach auf Public-Cloud-Umgebungen auszudehnen.

DIE SICHERHEITSHERAUSFORDERUNGEN DER PRIVATE CLOUD

Dass Unternehmen heute vermehrt auf Software-defined-Networking und Private-Cloud-Umgebungen setzen, hat sich als wahrer Segen für die Flexibilität und die Effizienz erwiesen. Gleichzeitig führt dies zu einer dramatischen Zunahme des Datenverkehrs, der im Data-Center in horizontaler Richtung verläuft („Ost-West-Datenverkehr"). Diese Veränderung im Muster des Datenverkehrs führt auch zu neuen Sicherheitsherausforderungen. Mit nur wenigen Maßnahmen für die Absicherungen des horizontalen Datenverkehrs können sich Bedrohungen ungehindert im Data-Center bewegen, wenn sie erst einmal in das Netzwerk eingedrungen sind. Traditionelle Ansätze für die Sicherheit, können mit der Dynamik von virtuellen Umgebungen, in denen flexibel Anwendungen bereitgestellt werden, nicht Schritt halten.

Check Point vSEC bietet durchgängigen und fortschrittlichen Schutz vor Bedrohungen in Private-Cloud-Infrastrukturen, schafft Transparenz und Kontrolle und ermöglicht es, die Sicherheit sowohl physikalischer als auch virtueller Umgebungen zu gewährleisten – und dies mit einer einzigen, einheitlichen Management-Lösung.

AMAZON WEB SERVICES

MICROSOFT AZURE

vSEC FÜR VMWARE NSX

vSEC VIRTUAL EDITION

vSEC OPENSTACK

Weitere Informationen: www.checkpoint.com/products-solutions/private-public-cloud/

SMART-1 APPLIANCES

DAS SICHERHEITSMANAGEMENT IN ZEITEN VON BIG DATA

SMART-1 205, 210, 225, 3050, 3150 APPLIANCES

ÜBERBLICK

Um eine Sicherheitsumgebung sowohl effizient als auch effektiv zu verwalten, benötigen Unternehmen eine Lösung für das Sicherheitsmanagement, die ebenfalls effizient und effektiv ist und heute mehr Daten verarbeiten kann als je zuvor. Check Point Smart-1 Appliances konsolidieren das Sicherheitsmanagement und umfassen das Logging, das Event-Management sowie das Reporting in einer einzigen, für diese Zwecke entwickelten Management-Appliance. Unternehmen können damit ihre Anforderungen an das Daten- und Event-Management in der Big-Data-Ära erfüllen, sich einen transparenten Überblick über Milliarden von Logdaten-Einträgen verschaffen, visuelle Indikatoren, die auf Risiken hindeuten, erhalten, und mögliche Bedrohungen schnell untersuchen.

EINHEITLICHES, INTELLIGENTES SICHERHEITSMANAGEMENT

SINGLE-DOMAIN SICHERHEITS-MANAGEMENT

MULTI-DOMAIN SICHERHEITS-MANAGEMENT

MULTI-DOMAIN LOGDATEN-MANAGEMENT

SMARTEVENT EVENT-MANAGEMENT

ALLGEMEINER ÜBERBLICK

Das für Carrier geeignete ATCA-Chassis, das von Grund auf dafür entwickelt wurde, die hohen Anforderungen von Data-Centern und Service-Providern an die Verlässlichkeit, die Verfügbarkeit und die Betriebsfähigkeit zu erfüllen, läuft im Hochverfügbarkeits- und Lastverteilungsmodus für die Security-Gateway-Module, die in diesem Chassis untergebracht sind. Falls Unternehmen die Redundanz noch weiter verbessern möchten, können sie ein weiteres Chassis im Hochverfügbarkeitsmodus hinzufügen, sodass alle geschäftskritischen Ressourcen stets verfügbar und optimal geschützt sind.

MAXIMALE KAPAZITÄTEN	205	210	225	3050	3150
Managed Gateways	5	10	25	50	150+
Maximale Zahl an Domänen (Multi-Domain-Management)	✗	✗	✗	50	200
Indizierte Logdaten/Sek.	3.000	5.000	11.000	26.000	44.000
SmartEvent Log-File-Größe/Tag (GB)	3,5	6,5	13	40	100
HDD	1x 1 TB	1x 2 TB	2x 2 TB	4x 2 TB	12x 2 TB
RAM	Standard: 4 GB	Standard: 8 GB	bis zu 32 GB Standard: 16 GB	bis zu 256 GB Standard: 32 GB	bis zu 256 GB Standard: 64 GB
SAN-Karte (Glasfaser)	✗	✗	✓	✓	✓

Weitere Informationen: www.checkpoint.com/products/smart-1-appliances/

DDOS PROTECTORS

DENIAL-OF-SERVICE-ANGRIFFE INNERHALB VON SEKUNDEN STOPPEN

10420 / 20420 / 30420 / 40420

4412 / 8412 / 12412

506 / 1006 / 2006

ÜBERBLICK

Die Zahl, die Geschwindigkeit und die Komplexität von Denial-of-Service-Attacken (DoS) und von Distributed-Denial-of-Service-Attacken (DDoS) sind in den vergangenen Jahren unaufhörlich gestiegen. Diese Angriffe sind relativ einfach auszuführen und können einen erheblichen Schaden in Unternehmen, die von der kontinuierlichen Bereitstellung ihrer Online-Dienste abhängig sind, anrichten. Viele Lösungen für den Schutz vor DDoS-Angriffen werden von Internet-Service-Providern bereitgestellt und bieten einen grundlegenden Schutz vor Angriffen auf Netzwerkebene. Doch die heutigen DDoS-Attacken sind vielschichtiger, es kommt häufig zu mehreren Angriffen auf verschiedenen Netzwerk- und Anwendungsebenen. DDoS-Lösungen, die erfolgreich arbeiten, müssen Unternehmen die Möglichkeit bieten, ihre Schutzmaßnahmen an ihre Sicherheitsanforderungen anzupassen, sehr schnell – noch während eines Angriffs – zu reagieren und aus verschiedenen Bereitstellungvarianten zu wählen.

Die DDoS Protector Appliances bieten flexible Bereitstellungsmöglichkeiten, um Unternehmen jeder Größenordnung flexibel und einfach schützen zu können. Darüber hinaus verfügen sie über ein integriertes Sicherheitsmanagement für die Analyse des Datenverkehrs in Echtzeit und eine intelligente Bedrohungsabwehr für den umfassenden Schutz vor DDoS-Attacken. Check Point bietet auch 24/7-Support und Unterstützung, um den zeitnahen Schutz sicherzustellen.

UMFASSENDE SICHERHEIT

ÜBERFLUTUNG DES NETZWERKS UND STARK STEIGENDER DATENVERKEHR

APPLIKATIONSBASIERENDE DOS-/ DDOS-ANGRIFFE

ALLGEMEINER ÜBERBLICK

Die Check Point DDoS Protector™ Appliances blockieren dank des mehrstufigen Schutzes und einer Leistung von bis zu 40 Gbps Denial-of-Service-Attacken innerhalb von Sekunden. Die DDoS Protectors erweitern das Sicherheitsperimeter eines Unternehmens und blockieren zerstörerische DDoS-Attacken bevor diese Schaden anrichten können.

MAXIMALE KAPAZITÄTEN	Enterprise	Data Center	Carrier
Durchsatz (Gbps) [1]	500 Mbps bis 2 Gbps	4 bis 12 Gbps	10 bis 40 Gbps
Maximale Zahl gleichzeitiger Sitzungen	2.000.000	4.000.000	6.000.000
Maximale Rate für die Angriffsvermeidung bei DDoS-Attacken (pps)	1.000.000	10.000.000	25.000.000
Latenz		< 60 Mikrosekunden	
10/100/1000 Ethernet (Kupfer)	4	8	
10 GbE (SFP+)			20
40 GbE QSFP			4
Netzbetrieb		Transparente Weiterleitung (L2)	
Hochverfügbarkeit		Aktiv-Passiv-Cluster	

[1] Die Leistung gemessen bei einem realen, durchschnittlichen Datenverkehr und einem typischen Regelsatz, wobei NAT und Logging aktiviert sind und die höchste Stufe der Bedrohungsabwehr für Sicherheit sorgt.

Weitere Informationen: www.checkpoint.com/products/ddos-protector/

SANDBLAST APPLIANCES

ABWEHR VON ZERO-DAY-ATTACKEN IN DER PRIVATE CLOUD

TE100X APPLIANCE

TE250X APPLIANCE

TE1000X APPLIANCE

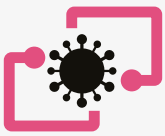
TE2000X APPLIANCE

ÜBERBLICK

Die Zahl an immer raffinierteren Cyberbedrohungen steigt kontinuierlich und viele zielgerichtete Attacken beginnen damit, die Software-Schwachstellen in heruntergeladenen Dateien oder E-Mail-Anhängen auszunutzen. Diese Bedrohungen umfassen neue Exploits oder auch Varianten bekannter Exploits, die nahezu täglich auftreten und für die es noch keine Signaturen gibt. Die Standard-Lösungen können diese Varianten nicht erkennen. Neue und unentdeckte Bedrohungen erfordern auch neue Lösungen, die über die Signaturen für bekannte Bedrohungen hinausgehen.

Check Point SandBlast Zero-Day Protection bietet mit der Malware-Erkennung, die auch Evasion-Techniken aufdeckt, einen umfassenden Schutz vor den gefährlichsten Angriffen und gewährleistet, dass die Mitarbeiter im Unternehmen ausschließlich sichere Inhalte erhalten. Den Kern von Check Points Lösung bilden die beiden einzigartigen Techniken Threat Emulation und Threat Extraction, die die Bedrohungsabwehr auf die nächste Ebene führen.

NEUE UND UNBEKANNTE BEDROHUNGEN ABWEHREN



THREAT PREVENTION

THREAT EXTRACTION

ALLGEMEINER ÜBERBLICK

Check Point bietet eine Reihe von SandBlast Appliances an. Diese eignen sich optimal für Unternehmen, die strengen regulatorischen oder datenschutzrechtlichen Vorgaben unterliegen und die den cloudbasierenden Service SandBlast Threat Emulation nicht nutzen möchten.

MAXIMALE KAPAZITÄTEN	TE100X	TE250X	TE1000X	TE2000X
Empfohlene Zahl an Dateien/Monat	100K	250K	1M	2M
Empfohlene Zahl an Nutzern	bis zu 1.000	bis zu 3.000	bis zu 10.000	bis zu 20.000
Durchsatz	150 Mbps	700 Mbps	2 Gbps	4 Gbps
Zahl der virtuellen Maschinen	4	8	28	56
10/100/1000Base-T RJ45	13	17	14	14
10 GBase-F SFP+	–	–	6	8
Gehäuse	1 HE	1 HE	2 HE	2 HE
HDD	1x 1 TB	1x 1 TB	2x 2 TB RAID1	2x 2 TB RAID1
Netzteile	1	2	2	2

Weitere Informationen: www.checkpoint.com/products-solutions/threat-prevention-appliances-and-software/

BEWÄHRTE SICHERHEIT

ALS FÜHREND ANERKANNT

Ganz gleich, ob Sie eine der aktuellen Appliances oder eine unserer unten stehenden Security-Gateway-Appliances kaufen, Sie können sich sicher sein, dass Sie das Produkt eines führenden Anbieters der Security-Industrie erwerben – ein Produkt, das von den führenden Testlaboren und Analystenhäusern wie Gartner, IDC, NSS Labs und Network World geprüft und anerkannt wurde.

- Check Point ist **SEIT 1997** eines der führenden Unternehmen im Gartner Magic Quadrant für Enterprise Network Firewalls [1]
- Check Point ist **ZUM FÜNFTEN MAL IN FOLGE** eines der führenden Unternehmen im Gartner Magic Quadrant für Unified Threat Management [2]
- Check Point führt den weltweiten Markt für kombinierte Firewall- und UTM-Appliances nach Umsatz an (3. Quartal 2015) [3]
- Die NSS Labs empfehlen Check Point als IPS, als Lösung für die Erkennung von Sicherheitsverletzungen und als NGFW

FÜR DATA-CENTER BIS HIN ZU KLEINEN NIEDERLASSUNGEN

1100 APPLIANCE

2200 APPLIANCE

4200 APPLIANCE

4400 APPLIANCE

4600 APPLIANCE

4800 APPLIANCE

12200 APPLIANCE

12400 APPLIANCE

12600 APPLIANCE

13500 APPLIANCE

13800 APPLIANCE

21400 APPLIANCE

21700 APPLIANCE

21800 APPLIANCE

[1] Gartner, Inc., Magic Quadrant for Enterprise Network Firewalls, Adam Hils, Greg Young, Jeremy D'Hoinne, 22. April 2015

[2] Gartner, Inc., Magic Quadrant for Unified Threat Management, Jeremy D'Hoinne, Adam Hils, Greg Young, Rajpreet Kaur, 27. August 2015

[3] Quelle: IDC Worldwide Quarterly Security Appliance Tracker, 3. Quartal 2015, 14. Dezember 2015

Kontaktieren Sie Check Point

Check Point Software Technologies

Deutschland: Zeppelinstraße 1, 85399 Hallbergmoos
+49-811-998210, E-Mail: contact-germany@checkpoint.com

Österreich: Vienna Twin Tower A1625, Wienerbergstraße 11, 1100 Wien
+43-1-99460-6701, Internet: www.checkpoint.com

Schweiz: Zürcherstrasse 59, 8953 Dietikon
+41-44-316-64-41, Internet: www.checkpoint.com

KONTAKTIEREN SIE CHECK POINT

Weltweiter Hauptsitz
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | E-Mail: info@checkpoint.com
Hauptsitz in den USA
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | Internet: www.checkpoint.com

Januar 2017