



CHECK POINT 5800 アプライアンス

中規模環境向けのセキュリティ

CHECK POINT 5800 アプライアンス

中規模環境向けのセキュリティ

メリット

- 先進の脅威対策機能による拡張性に優れたセキュリティ保護
- SSL 暗号化トラフィックの検査時でも妥協のないパフォーマンスを発揮
- 将来を見据えたテクノロジーで今後起こりうるリスクに対応
- 集中管理と LOM による保守性の向上
- 高い性能要件に最適化された「ハイ・パフォーマンス・パッケージ」
- 拡張性に優れたモジュール型のシャーシを採用、柔軟に選択できる I/O オプション

特長

- シンプルな導入と管理
- 「バーチャル・システム」により、1 台のデバイスに複数のセキュリティ・ゲートウェイを統合可能
- ネットワーク拡張スロットを 2 基搭載、Fiber、10 GbE、40 GbE、フェイル・オープン・ポートなど、多彩な I/O カードを装着可能
- 電源、ファンの冗長化、アプライアンス・クラスタリング技術により、単一障害点を排除

概要

Check Point 5800 は、包括的なセキュリティ技術を統合した、中規模環境向けのセキュリティ・アプライアンスです。1U サイズのコンパクトな筐体に、ポートを増強可能な I/O 拡張スロットを 2 基、冗長仕様のファンおよび電源、500GB のハードディスク、または 240GB の SSD、リモート管理を可能にする LOM (Lights-Out-Management) カードを搭載しています。実運用環境で最新の脅威対策を実行できるよう最適化されており、強力なセキュリティで組織の重要な資産や環境を保護することが可能です。

包括的な脅威対策

マルウェアの急増、攻撃者の手口の高度化、新しい未知のゼロデイ脅威の台頭に対処するには、これまでとは異なるアプローチで組織のネットワークやデータを安全に確保することが重要です。チェック・ポイントは、セキュリティ運用の複雑さを削減し、業務効率を向上させながら、勢いを強める新たな脅威へ対抗するために完全に統合された、包括的な脅威対策ソリューションを提供しています。Check Point Threat Prevention ソリューションは、Firewall、VPN (IPSec)、IPS、Application Control、Anti-Bot、Anti-Virus、URL Filtering などの強力なセキュリティ機能に加え、第三者機関によって高く評価された SandBlast™ Threat Emulation および Threat Extraction により、最新の高度な脅威やゼロデイの脆弱性悪用に対する完全な防御機能を提供しています。

実運用環境におけるパフォーマンス ¹	
SecurityPower™ Units (SPU)	1,750 SPU
ファイアウォール・スループット	22 Gbps
IPS スループット	3.05 Gbps
NGFW スループット (Firewall、Application Control、IPS)	2 Gbps
Threat Prevention スループット ²	1 Gbps
理想的なテスト環境におけるパフォーマンス (RFC 3511、2544、2647、1242)	
ファイアウォール・スループット (1518 バイト UDP)	35 Gbps
接続数 / 秒	185,000
同時接続数	320 万 ~ 1,280 万 ³
VPN スループット (AES-128)	10 Gbps
IPS スループット	10 Gbps
NGFW スループット (Firewall、Application Control、IPS)	8.1 Gbps

¹ パフォーマンスの測定は、実運用環境のトラフィック構成、一般的なルールベース、NAT、ログ機能の有効化、最新の推奨シグネチャをオンにし、セキュリティレベルの高い脅威対策機能に基づいて行われています。² Firewall、IPS、Application Control、Antivirus、Anti-Bot、URL Filtering ³ パフォーマンスの測定は、最大メモリに基づいて行われています。

フル装備のセキュリティ・ソリューション

Check Point 5800アプライアンスには、必要な機能を完備した統合型のセキュリティ・ソリューションを次の2種類のフル・パッケージで提供します。

- NGTP : IPS、Application Control、Antivirus、Anti-Bot、URL Filtering、Email Securityの各機能で高度なサイバー脅威を阻止
- NGTX : Threat EmulationとThreat Extractionで構成されるSandBlast Zero-Day ProtectionをNGTPに追加

既知およびゼロデイの脅威を阻止

5800アプライアンスは、Antivirus、Anti-Bot、SandBlast Threat Emulation (サンドボックス)、SandBlast Threat Extractionの各技術によって、既知と未知の両方の脅威から組織を保護します。

Check Point SandBlast Zero-Day Protectionソリューションの一つである、クラウドベースのThreat Emulationエンジンは、検出を免れる手法によりハッカーがサンドボックスの回避を試みる手前のエクスプロイト・フェーズで、マルウェアを検出します。ファイルをすばやく隔離し、仮想サンドボックス内で実行して検査することにより、悪意のある挙動をネットワーク侵入前に検出することが可能です。この革新的なソリューションでは、CPUレベルの検査技術とOSレベルのサンドボックス技術を組み合わせることによって、危険性の高い攻撃コードやゼロデイ攻撃、標的型攻撃による感染を高い精度で未然に防ぎます。

さらに、SandBlast Threat Extractionは、攻撃に利用されやすいコンテンツ (アクティブ・コンテンツや組み込みオブジェクトなど) を削除して、潜在的な脅威が排除されたコンテンツのみで再構成し、無害化されたファイルをすみやかにユーザに提供することによって、ビジネス・フローを維持します。

	NGTP	NGTX
	既知の脅威を阻止	既知およびゼロデイの攻撃を阻止
Firewall	✓	✓
VPN (IPSec)	✓	✓
IPS	✓	✓
Application Control	✓	✓
Anti-Bot	✓	✓
Anti-Virus	✓	✓
URL Filtering	✓	✓
SandBlast Threat Emulation	✗	✓
SandBlast Threat Extraction	✗	✓

暗号化トラフィックの検査

インターネットでは、セキュリティ上の理由から、通信をHTTPS、SSL、TLSで暗号化する動きが広がっています。しかし、この暗号化

の方法では、従来型のセキュリティ・ソリューションでは暗号化トラフィックを検査できないため、SSL/TLSが不正なファイルを密かに送信するための攻撃経路として悪用される可能性があります。Check Point Threat Preventionは、暗号化SSL/TLSトンネルの検査に対応しており、暗号化トラフィックに潜むセキュリティ脅威を検出できます。また、暗号化通信で行われる、組織のポリシーに違反するWebサイトの閲覧や業務データのやり取りも確実に発見することが可能です。

包括的なハイ・パフォーマンス・パッケージ

大容量の接続機能を要件とする環境には、事前構成されたハイ・パフォーマンス・パッケージ(HPP)を手頃な価格で導入することができます。このパッケージには、標準のアプライアンス構成に加え、2ポートの10Gb SFP+インタフェース・カード、トランシーバ、大容量の接続性能を可能にする16GBのメモリが含まれています。

	基本	HPP	最大
1 GbEポート (Copper)	10	10	26
1 GbEポート (Fiber)	0	0	8
10 GbEポート (Fiber)	0	2	8
トランシーバ (SR)	0	2	8
40 GbEポート (Fiber)	0	0	4
RAM	8GB	16GB	32GB
電源	1	2	2
LOM	装備	装備	装備

リモート管理および監視

LOM (Lights-Out-Management) カードを使用したアウトオブバンド・リモート管理機能により、アプライアンスの診断、起動、再起動、管理をリモートから実施できます。管理者は、LOM Webインターフェイスを使用して、ISOファイルからOSイメージをリモート・インストールすることもできます。

40 GbE 接続

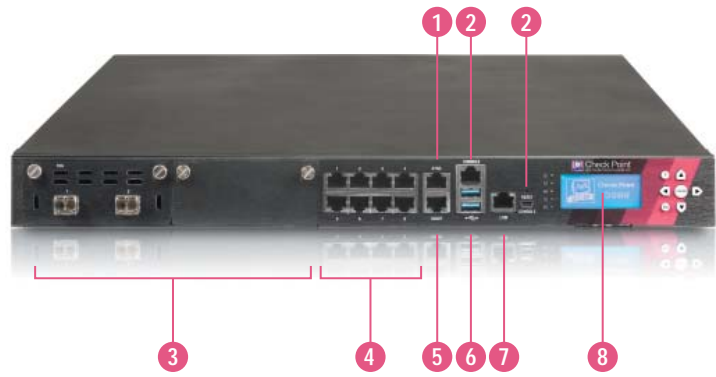
高速なネットワーク接続は、最新の企業ネットワークやデータセンター環境に不可欠です。特に高密度の仮想化サーバを導入しているデータセンターでは重要な要件となります。10 GbEから40 GbEへの移行準備が整っているお客様は、5800アプライアンスによって、40 GbEのセキュリティ環境を迅速に実現できます。Check Point 5800では、最大4個の40 GbEポートを使用して、10 GbEサーバを40 GbEのコア・ネットワークにアップリンク接続できます。

仮想化の利点を活用

Check Point Virtual Systemsにより、組織は仮想化された複数のセキュリティ・ゲートウェイを1台のハードウェア・デバイス上に作成しインフラストラクチャを統合することによって、大幅なコスト削減に加え、セキュリティとインフラストラクチャのシームレスな統合を実現できます。

5800セキュリティ・アプライアンス

- ① 同期ポート(10/100/1000Base-T RJ45)
- ② RJ45/micro USB コンソール・ポート
- ③ ネットワーク・カード拡張スロット (HPP) x 2
- ④ 10/100/1000Base-T RJ45ポート x 8
- ⑤ 管理ポート (10/100/1000Base-T RJ45)
- ⑥ USB 3.0ポート x 2 (ISOインストール用)
- ⑦ LOM (Lights-Out-Management) ポート
- ⑧ グラフィックLCDディスプレイ



オーダー情報

基本構成 ¹	
5800 Next-Gen Threat Prevention、2台までのゲートウェイに対応したローカル管理機能をバンドル	CPAP-SG5800-NGTP
5800 Next-Gen Threat Extraction、2台までのゲートウェイに対応したローカル管理機能をバンドル	CPAP-SG5800-NGTX
ハイ・パフォーマンス・パッケージ ¹	
5800 Next-Gen Threat Preventionハイ・パフォーマンス・パッケージ (10GbE SFP+ポート x 2、SR 10GBトランシーバ x 2、冗長電源、16GBのメモリを装備)	CPAP-SG5800-NGTP-HPP
5800 Next-Gen Threat Extractionハイ・パフォーマンス・パッケージ (10GbE SFP+ポート x 2、SR 10GBトランシーバ x 2、冗長電源、16GBのメモリを装備)	CPAP-SG5800-NGTX-HPP
バーチャル・システム・パッケージ ¹	
5800 NGTPアプライアンス (ハイ・パフォーマンス・パッケージとバーチャル・システム x 10を含む)	CPAP-SG5800-NGTP-HPP-VS10
5800 NGTPアプライアンス2台 (ハイ・パフォーマンス・パッケージとバーチャル・システム x 10を含む)	CPAP-SG5800-NGTP-HPP-VS10-2
5800 NGTXアプライアンス (ハイ・パフォーマンス・パッケージとバーチャル・システム x 10を含む)	CPAP-SG5800-NGTX-HPP-VS10
5800 NGTXアプライアンス2台 (ハイ・パフォーマンス・パッケージとバーチャル・システム x 10を含む)	CPAP-SG5800-NGTX-HPP-VS10-2

¹ SKUは、2年分と3年分用、ハイ・アベイラビリティ (HA) 構成用が用意されています。詳細についてはオンライン製品カタログをご覧ください。

アクセサリ

インタフェース・カード、トランシーバ	
8ポート 10/100/1000Base-T RJ45 インタフェース・カード	CPAC-8-1C-B
4ポート 1000Base-F SFP インタフェース・カード (1000Base SFPトランシーバが別途必要)	CPAC-4-1F-B
1G Fiber ポート用 SFPトランシーバ・モジュール - ロング・レンジ (1000Base-LX)	CPAC-TR-1LX-B
1G Fiber ポート用 SFPトランシーバ・モジュール - ショート・レンジ (1000Base-SX)	CPAC-TR-1SX-B
1000Base-T RJ45用 SFPトランシーバ (Copper)	CPAC-TR-1T-B
4ポート 10GBase-F SFP+ インタフェース・カード	CPAC-4-10F-B
10G Fiber ポート用 SFP+トランシーバ・モジュール - ロング・レンジ (10GBase-LR)	CPAC-TR-10LR-B
10G Fiber ポート用 SFP+トランシーバ・モジュール - ショート・レンジ (10GBase-SR)	CPAC-TR-10SR-B
2ポート 40GBase-F QSFP インタフェース・カード	CPAC-2-40F-B
40G Fiber ポート用 QSFPトランシーバ・モジュール - ショート・レンジ (40GBase-SR)	CPAC-TR-40SR-QSFP-300m
40G Fiber ポート用 QSFPトランシーバ・モジュール - ロング・レンジ (40GBase-LR)	CPAC-TR-40LR-QSFP-10K
4ポート 1GE Copper バイパス (フェイル・オープン) ネットワーク・インタフェース・カード (10/100/1000 Base-T)	CPAC-4-1C-BP-B
2ポート 10GE ショート・レンジ Fiber バイパス (フェイル・オープン) ネットワーク・インタフェース・カード (10GBase-SR)	CPAC-2-10-FSR-B-BP
スベア、その他	
8GB から 16GB へのメモリ・アップグレード・キット (5800 アプライアンス向け)	CPAC-RAM8GB-5000
8GB から 32GB へのメモリ・アップグレード・キット (5800 アプライアンス向け)	CPAC-RAM24GB-5000
16GB から 32GB へのメモリ・アップグレード・キット (5800 アプライアンス向け)	CPAC-RAM16GB-5000
増設 / 交換用 AC 電源 (5600 および 5800 アプライアンス向け)	CPAC-PSU-5600/5800
スライド・レール (5000 アプライアンス向け) (22~32 インチ)	CPAC-RAIL-5000
拡張スライド・レール (5000 アプライアンス向け) (26~36 インチ)	CPAC-RAIL-EXT-5000

※アプライアンス納入後にアクセサリを追加、交換する場合には、"-INSTALL"を除いたSKUをご指定ください。

5800セキュリティ・アプライアンス(背面)

- ① 冗長電源(HPP オプション)
- ② 冷却ファン



拡張オプション

基本構成

- オンボード10/100/1000Base-T RJ-45ポート x 10
- 8GBメモリ(オプションで16GB/32GB)
- 電源 x 1(オプションで2冗長電源)
- 500GB(HDD) x 1、または240GB(SSD) x 1
- LOM(Lights-Out-Management)
- スライド・レール(22~32インチ)

ネットワーク拡張スロット・オプション(2スロット)

- 8ポート10/100/1000Base-T RJ45カード、最大26ポート
- 4ポート1000Base-F SFPカード、最大8ポート
- 4ポート10GBase-F SFP+カード、最大8ポート
- 2ポート40GBase-F QSFPカード、最大4ポート

フェイル・オープン/バイパス・ネットワーク・オプション

- 4ポート10/100/1000Base-T RJ45カード
- 2ポート10GBase-F SFP+カード

バーチャル・システム¹

- 最大(基本構成/HPP): 10/20

¹ 基本構成、またはHPP構成でのメモリ

ネットワーク

ネットワーク接続

- アプライアンス1台あたりの物理および仮想(VLAN)インタフェース数(合計): 1024/4096(単一のゲートウェイ/バーチャル・システムを使用)
- 802.3adパッシブ/アクティブ・リンク・アグリゲーション
- レイヤ2(透過)およびレイヤ3(ルーティング)モード

ハイ・アベイラビリティ

- アクティブ/アクティブおよびアクティブ/パッシブ-L3モード
- セッション同期(ファイアウォールとVPN)
- セッション・フェイルオーバー(ルーティング変更)
- デバイスおよびリンク障害の検出
- ClusterXLまたはVRRP

ネットワーク(続き)

IPv6

- 機能: Firewall、Identity Awareness、Mobile Access、App Control、URL Filtering、IPS、Anti-Bot、Antivirus
- NAT66、NAT64
- CoreXL、SecureXL、HA with VRRPv3

ユニキャストおよびマルチキャスト・ルーティング(SK98226を参照)

- OSPFv2およびv3、BGP、RIP
- スタティック・ルート、マルチキャスト・ルート
- ポリシー・ベースのルーティング
- PIM-SM、PIM-SSM、PIM-DM、IGMP v2およびv3

物理仕様

電力要件

- AC入力電圧: 90~264V
- 周波数: 47~63Hz
- 電源定格(電源1台): 275W
- 最大消費電力: 110W
- 最大熱出力: 375.3 BTU/時

寸法

- エンクロージャ: 1RU
- インチ法(幅 x 奥行 x 高) 17.4 x 20 x 1.73インチ
- メートル法(幅 x 奥行 x 高) 438 x 508 x 44 mm
- 重量: 8.37 kg

動作環境条件

- 温度: 0~40度(摂氏)
- 湿度: 5~95%(結露なきこと)

保管条件

- 温度: -40~70度(摂氏)
- 湿度: 60度(摂氏)で5~95%(結露なきこと)

適合規格

- 安全性: UL60950-1、CB IEC60950-1、CE LVD EN60950-1、TUV GS
- エミッション: FCC、CE、VCCI、RCM/C-Tick
- 環境: RoHS、REACH、ISO14001

製品に関するお問い合わせ

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

〒160-0022 東京都新宿区新宿 5-5-3 建成新宿ビル6F Tel: 03 (5367) 2500 E-mail: info_jp@checkpoint.com http://www.checkpoint.co.jp