CHECK POINT 5400アプライアンス

小規模環境向けのセキュリティ

CHECK POINT 5400 アプライアンス

小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
- 各種デバイスから社内リソースへの安全なリモート・アクセス
- ネットワーク拡張スロットを1基搭載、Fiber、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
- 冗長化とアプライアンス・クラスタリング技術により、単一障害点を排除

概要

Check Point 5400は、包括的なセキュリティ技術を統合した、小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1基、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）	600 SPU
ファイアウォール・スループット	10 Gbps
IPSスループット	1.08 Gbps
NGFWスループット（Firewall、Application Control、IPS）	690 Mbps
Threat Preventionスループット[2]	330 Mbps
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）	22 Gbps
接続数/秒	150,000
同時接続数	320万～1,280万[3]
VPNスループット（AES-128）	2.16 Gbps
IPSスループット	3.9 Gbps
NGFWスループット（Firewall、Application Control、IPS）	3.4 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 5400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

5400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、4ポートの1Gb 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	18
1 GbEポート(Fiber)	0	4	4
トランシーバ（SR）	0	4	4
RAM	8GB	16GB	32GB
電源	1	1	1
LOM	オプション	装備	装備

リモート管理および監視

オプションの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。

安全なリモート・アクセス

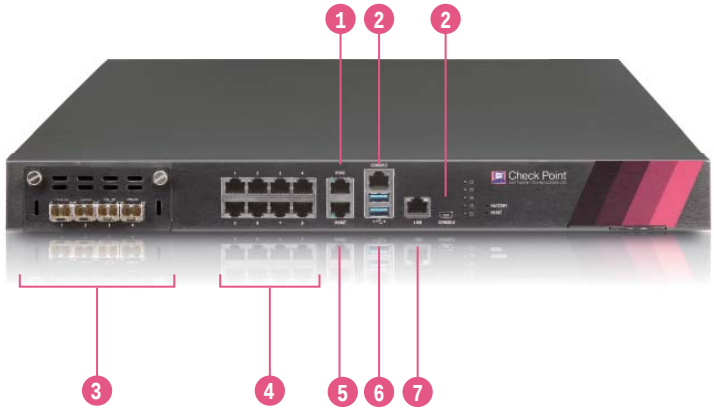
チェック・ポイントの各アプライアンスには、Mobile Access Software Bladeによるモバイル・アクセス接続機能が付属します（5ユーザまで）。スマートフォンやタブレット端末、Windows、Mac、Linuxなど、さまざまデバイスから社内のリソースへ安全にリモート・アクセスできます。

セキュリティ管理の統合

セキュリティ管理機能を内蔵するチェック・ポイントの各アプライアンスは、ローカルでの管理に加えて、統合セキュリティ管理コンソールから集中管理することも可能です。ローカル管理では、そのアプライアンス自体と、隣接するハイ・アベイラビリティ構成のアプライアンス1台を管理できます。

5400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)
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



オーダー情報

基本構成[1]	
5400 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-SG5400-NGTP
5400 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-SG5400-NGTX

ハイ・パフォーマンス・パッケージ[1]	
5400 Next-Gen Threat Preventionハイ・パフォーマンス・パッケージ (1GbE SFP+ポート x 4、SR 1GBトランシーバ x 4、16GBのメモリを装備)	CPAP-SG5400-NGTP-HPP
5400 Next-Gen Threat Extractionハイ・パフォーマンス・パッケージ (1GbE SFP+ポート x 4、SR 1GBトランシーバ x 4、16GBのメモリを装備)	CPAP-SG5400-NGTX-HPP

[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

スペア、その他	
8GBから16GBへのメモリ・アップグレード・キット(5400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(5400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(5400アプライアンス向け)	CPAC-RAM16GB-5000
Lights-Out-Managementモジュール	CPAC-LOM-B
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。

5400セキュリティ・アプライアンス（背面）

1. 電源
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
- 500GB（HDD）x 1、または240GB（SSD）x 1
- 固定レール（スライド・レールはオプション）
- LOM（Lights-Out-Management、オプション）

ネットワーク拡張スロット・オプション（1スロット）

- 8ポート10/100/1000Base-T RJ45カード、最大18ポート
- 4ポート1000Base-F SFP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

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構成でのメモリを使用

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（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

IPv6

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

ルーティング

ユニキャストおよびマルチキャスト・ルーティング（SK98226参照）

- 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）：250W
- 最大消費電力：76.5W
- 最大熱出力：261 BTU/時

寸法

- エンクロージャ：1RU
- インチ法（幅 x 奥行 x 高）17.24 x 16 x 1.73インチ
- メートル法（幅 x 奥行 x 高）438 x 406.5 x 44 mm
- 重量：6.37 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

P/N DS-20161118-5400-2