CHECK POINT
3100 アプライアンス

支社・支店環境や小規模環境向けの次世代セキュリティ・ゲートウェイ

CHECK POINT 3100 アプライアンス

コンパクトな筐体で支社・支店環境や小規模環境向けのセキュリティを実現

メリット

- 先進の脅威対策機能によるセキュリティ保護
- 発生直後の高度なゼロデイ攻撃を防御する独自の技術
- SSL暗号化トラフィックの検査に最適化
- 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
- 統合管理コンソールで管理作業を簡素化

特長

- コンパクトなデスクトップ型の筐体
- シンプルな導入と管理
- サイト間およびクライアント/サイト間VPNにより、支社・支店環境でのセキュアな接続を実現
- 冗長化を実現するクラスタリング技術により、単一障害点を排除

概要

Check Point 3100 アプライアンスは、コンパクトなデスクトップ型の筐体に包括的なセキュリティ技術を統合した、支社・支店環境や小規模環境向けのセキュリティ・ソリューションです。現在および将来のセキュリティ脅威に対応する、高度な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します。

包括的な脅威対策

チェック・ポイントでは、緊密に統合された脅威対策技術と、第三者機関によって高く評価された SandBlast™ Threat Emulation および Threat Extraction の組み合わせにより、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。

従来型のセキュリティ・ソリューションは、検出回避手法を備えるマルウェアに対応できない、許容できないほどの遅延を発生させる、ファイルの検査中に脅威を通過させるなどの問題を抱えています。しかし、Check Point SandBlast なら、多くのマルウェアをネットワークの手前でブロックすることが可能です。このためユーザは、社内外のどこにいても、生産性を犠牲にすることなく、安全に業務を行えます。

主なパフォーマンス

Firewall	IPS	NGFW[1]	Threat Prevention[2]
4 Gbps	1.1 Gbps	850 Mbps	200 Mbps

理想的なテスト環境で測定されたパフォーマンスです。パフォーマンスの詳細については、3 ページをご覧ください。

1. Firewall、Application Control、IPS の各 Software Blade を有効化
2. Firewall、Application Control、URL Filtering、IPS、Antivirus、Anti-Bot、SandBlast Zero-Day Protection の各 Software Blade を有効化

3100 セキュリティ・アプライアンス

1. 管理ポート（10/100/1000Base-T RJ45）
2. 10/100/1000Base-T RJ45 ポート x 5
3. USB ポート x 2（ISO インストール用）
4. RJ45/micro USB コンソール・ポート
5. 電源接続端子

オールインワン・セキュリティ・ソリューション

Check Point 3100 アプライアンスは、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： Application Control、URL Filtering、IPS、Antivirus、Anti-Bot、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

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、従来型のセキュリティ・ソリューションでは、このように暗号化されたトラフィックを検査できません。そのため、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。

クラス最高レベルの管理機能

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、ペアとなるハイ・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。集中管理する場合、管理者は Check Point Security Management サーバを使用することで、内部セキュリティ、メイン・サイト、リモート・サイトを含むネットワーク全体のセキュリティ・ポリシーを一元的に定義できます。

既知およびゼロデイの脅威を阻止

Check Point 3100 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。ファイルを素早く隔離し、仮想サンドボックス内で実行して検査する Threat Emulation エンジンは、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、クラウドでの CPU レベルの検査技術と OS レベルのサンドボックス技術の組み合わせによって、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 (SandBlast)
	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	✓	✓
URL Filtering	✓	✓
Anti-Bot	✓	✓
Anti-Virus	✓	✓
Anti-Spam	✓	✓
SandBlast Threat Emulation	×	✓
SandBlast Threat Extraction	×	✓

パフォーマンス

理想的なテスト環境

- ファイアウォール・スループット (1518バイトのUDPパケット)： 4 Gbps
- IPSスループット： 1.1 Gbps
- NGFWスループット1： 850 Mbps
- Threat Preventionスループット2： 200 Mbps
- VPNスループット（AES-128）： 1.7 Gbps
- 接続数/秒（64バイトのレスポンス）： 4万
- 同時接続数（64バイトのレスポンス）： 320万

実運用環境

- SecurityPower Units： 160
- ファイアウォール・スループット： 2.1 Gbps
- IPSスループット： 350 Mbps
- NGFWスループット[1]： 220 Mbps
- Threat Preventionスループット[2]： 95 Mbps

実際のパフォーマンスは諸条件によって異なります。環境固有の要件に最適なアプライアンスについては、ご相談ください。

1. Firewall、Application Control、IPSの各Software Bladeを有効化。2. Firewall、Application Control、URL Filtering、IPS、Antivirus、Anti-Bot、SandBlast Zero-Day Protectionの各Software Bladeを有効化。

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・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)
- ClusterXLまたはVRRP

ネットワーク（続き）

IPv6

- 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

ハードウェア

基本構成

- オンボード10/100/1000Base-T RJ-45ポート x 6
- CPU x 1、物理コア 4、仮想コア 4 (合計)
- 8 GBメモリ
- 電源 x 1
- 320 GBのHDD x 1、または240 GBのSSD x 1

電力要件

- 電源定格（電源1台）： 40W
- AC入力電圧： 90～264V（47～63Hz）
- 最大消費電力： 29.5W
- 最大熱出力： 100.7 BTU/時

寸法

- エンクロージャ： デスクトップ・サイズ
- サイズ（幅 x 奥行 x 高）： 210 x 210 x 41.9 mm
- 重量： 1.3 kg

環境条件

- 動作時： 温度0～40度（摂氏）、湿度5～95%
- 保管時： 温度-40～70度（摂氏）、湿度5～95%（摂氏60度の場合）

適合規格

- 安全性： UL、CB、CE、TUV GS
- エミッション： FCC、CE、VCCI、RCM/C-Tick
- 環境： RoHS、REACH[1]、ISO14001[1]

[1] 工場認定

オーダー情報

基本構成[1]	
3100 アプライアンス基本構成： 1 GbE Copperポート x 6、8 GB RAM、HDD x 1、AC電源 x 1、Next Generation Threat Prevention（NGTP）セキュリティ・サブスクリプション・パッケージ1年分	CPAP-SG3100-NGTP
3100 SandBlast アプライアンス基本構成： 1 GbE Copperポート x 6、8 GB RAM、HDD x 1、AC電源 x 1、SandBlast（NGTX）セキュリティ・サブスクリプション・パッケージ1年分	CPAP-SG3100-NGTX
スペア、その他	
交換用AC/DC電源（3100アプライアンス向け）	CPAC-PSU-3100
シングル/デュアル・シャーシ・ラック・シェルフ（1400および3100アプライアンス向け）	CPAC-RM-1400/3100

1. SKU は、2 年分と 3 年分用、ハイ・アベイラビリティ構成用、SSD 搭載アプライアンス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。

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 https://www.checkpoint.co.jp

P/N DS-20170330-3100