



ネットワーク・セキュリティ

業界をリードするチェック・ポイントのセキュリティ・ソリューションは、ネットワーク環境を常に安全に保ちます。

UTM-1 Total Security

あらゆる脅威に対処するオールインワンUTMアプライアンス

UTM-1™ Total Securityアプライアンスは、ネットワークを保護するために必要なすべての機能とサービスを提供する、短時間で導入可能なオールインワン・セキュリティ・ソリューションです。

主な利点

- 中堅中小規模環境が必要とするセキュリティ対策とパフォーマンスの両立を実現
- 多くの大企業で使用されている実績と信頼性のある技術を採用
- 多種多様なインターネット上の脅威からネットワーク、システム、ユーザを保護
- リモート・アクセスおよびサイト間通信を保護することにより、情報の機密性を維持
- セキュリティの導入および管理を効率化
- SmartDefenseサービスにより、最新の脅威に対応



各アプライアンスには、統合された集中管理環境に加え、包括的なセキュリティ・アップデート・サービス、ハードウェア・サポート、およびカスタマー・サポートが含まれています(セキュリティ・アップデートは、導入時に一括3年分の購入が可能。カスタマー・サポートは特別価格でのご提供)。

NGX™

NGXプラットフォームによりチェック・ポイントの統一されたセキュリティ・アーキテクチャを実現します。

今必要なセキュリティ対策を提供

実績あるアプリケーションの制御と攻撃の防御

UTM-1 Total Securityは、業界最高レベルの実績を誇るファイアウォールを搭載しており、初期設定の状態ですべて種類のアプリケーション、プロトコル、およびサービスを検査することができます。侵入防御技術 (IPS) の SmartDefense™も統合されており、シグネチャとプロトコル・アノマリ (プロトコル異常) に基づいて侵入を検知・防御することで、FTPやHTTP、VoIPなど、ビジネスにとって重要性の高いサービスを既知および未知の攻撃から保護します。また、インスタント・メッセージやP2Pアプリケーションなど、企業では通常必要のないアプリケーションをブロックすることもできます。

ゲートウェイ・アンチウイルス/アンチスパイウェア

ゲートウェイ・アンチウイルス/アンチスパイウェア機能は、エンドポイント・セキュリティを補完する、UTM-1 Total Securityのコア・コンポーネントです。UTM-1 Total Securityは、常時更新されるウイルス/スパイウェア・シグネチャとアノマリ・ベースの検出機能を使用して、ウイルスなどのマルウェアをゲートウェイで遮断します。POP3、SMTP、FTP、およびHTTPの各トラフィックに対しリアルタイムでウイルス・スキャンを実行するため、正規のコンテンツに潜む脅威も検出できます。

アンチスパム機能を備えた包括的なメッセージング・セキュリティ

チェック・ポイントが提供するメッセージング・セキュリティ機能は、組織のメッセージング・インフラストラクチャを包括的に保護します。多次元アプローチの採用により、電子メール・インフラストラクチャの保護と高精度のスパム保護を提供し、電子メールに潜む多様なウイルスおよびマルウェアの脅威から組織を守ります。

| | |
|-------------------------|--|
| IPレピュテーションによるアンチスパム | 悪意ある既知のIPアドレスの動的データベースで送信者のレピュテーションをチェックすることにより、スパムやマルウェアを接続レベルでブロック |
| コンテンツ・ベースのアンチスパム | 画像を利用したスパムや各国語のスパムなど、最新のスパムをパターン・ベースで検出 |
| 拒否/許可リストによるアンチスパム | 拒否リストや許可リストを使用して、明らかなスパム送信者からの電子メールを拒否し、信頼できる送信者からの電子メールを許可 |
| メールのアンチウイルス | メッセージ本文と添付ファイルのスキャンなどにより、多様なウイルスおよびマルウェアをブロック |
| ゼロアワー・アウトブレイク保護機能 | 先進のパターン・マッチング機能と配布分析エンジンにより、新種のスパムおよびマルウェアをブロック |
| SmartDefenseによる電子メールIPS | DoS、バッファ・オーバーフロー攻撃など、メッセージング・インフラストラクチャ自体を狙うさまざまな脅威に対する防御 |

Webフィルタリング

UTM-1 Total Securityアプライアンスは、2,000万以上のURLをカバーする先進のWebフィルタリング機能を備えています。この機能を利用して、自社に合ったWebサイト利用規定を策定することで、社員などによる不適切なWebサイトの閲覧を防止できます。

シンプルな設定によるサイト間VPN接続機能

UTM-1 Total Securityアプライアンスでは、サイト間VPN接続およびリモート・アクセス接続を簡単に設定することができます。従来、他のソリューションでは手動で行われてきたノード間のVPNトンネルおよびVPN全体セキュリティ設定は、1クリックの操作によって新しいサイトやリモート・ユーザの追加が自動的に行われます。

安全で柔軟性に優れたリモート・アクセス

UTM-1 Total Securityアプライアンスは、幅広いVPNエージェントからシームレスに接続できる、IPSecまたはSSLベースの柔軟なリモート・アクセス機能を備えています。これにより、社員やビジネス・パートナーは、リモートから安全に企業ネットワークに接続することができます。

簡単な導入を実現

短時間で導入可能なオールインワン・ソリューション

UTM-1 Total Securityアプライアンスは、最大3年分の一括購入が可能なアップデート・サービスを含む、UTMネットワークのセキュリティに求められるすべての要件が提供されています。(4年目以降のサービスは、追加購入可能)

- セキュリティ機能
- セキュリティ・アップデート
- ハードウェア保証

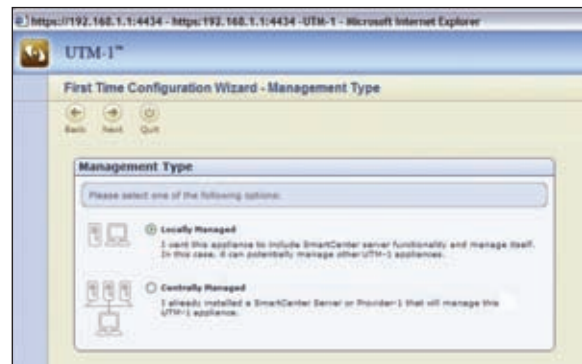
一元的に実行可能な統合管理

UTM-1 Total Securityアプライアンスには、複数のアプライアンスおよび他のチェック・ポイント製品を単一のコンソールから集中管理を行える統合管理環境SmartCenter (スマート・センター) が付属しています。SmartCenterでは、ネットワーク中に複数のゲートウェイが存在する場合でもセキュリティ・ポリシーやゲートウェイの設定などを集中的に一括管理することができ、各サイトやゲートウェイを個別に管理する必要がありません。SmartCenterを利用することで、管理者の負担を軽減し、設定ミスが起きる可能性を低く抑えると同時に、ネットワーク全体にわたって一貫したセキュリティを適用することが可能になります。管理者はSmartCenterに付属する管理GUIであるSmartDashboard (スマート・ダッシュボード) を使用して、セキュリティ・ポリシーの各要素—ファイアウォール・セキュリティ、NAT (ネットワーク・アドレス変換)、QoS (サービス品質)、VPNエージェント・セキュリティ、VPNに関する設定を直感的に定義および管理することが可能です。

短時間でのセットアップ

UTM-1 Total Securityアプライアンスには初期設定ウィザードが付属しており、次の手順で簡単に導入できます。

- ケーブル類を接続し、アプライアンスの電源を入れます。
- 画面に表示されるウィザードに従ってセットアップを行います。
- SmartCenterの管理インタフェースを開きます。



UTM-1 Total Securityアプライアンスは、初期設定ウィザードを使用して簡単に短時間で設定できます。

仕様

| | 保護の詳細 |
|--------------------------|--|
| ファイアウォール | |
| プロトコル/アプリケーション・サポート | 200以上 |
| VoIP保護 | NAT環境を含むSIP、H.323、MGCPおよびSCCP |
| インスタント・メッセージングの制御 | MSN、Yahoo、ICQ、およびSkype |
| ピア・ツー・ピア・ブロック | Kazaa、Gnutella、BitTorrent、Winnyなど |
| ネットワーク・アドレス変換(NAT) | 手動および自動ルールでスタティックNAT/HideNATをサポート |
| IPSec VPN | |
| 暗号化のサポート | AES 128-256ビット、3DES 56-168ビット |
| 認証方法 | パスワード、RADIUS、TACACS、X.509、SecurID |
| 認証局 | 認証局(X.509)を統合 |
| VPNコミュニティ | オブジェクトの作成時にサイト間接続を自動設定 |
| トポロジのサポート | スター型およびメッシュ型 |
| ルート・ベースのVPN | 仮想トンネル・インタフェース、ナンバード/アンナンバード・インタフェースを利用 |
| VPNエージェントのサポート | VPN、デフォルト・ファイアウォールによる包括的なエンドポイント・セキュリティ |
| SSL VPN | |
| SSLベースのリモート・アクセス | 完全に統合されたVPNゲートウェイでSSLベースのオンデマンド・アクセスを提供 |
| SSLベースのエンドポイント・スキャン | ネットワークへの接続を許可する前にエンドポイントをスキャンしてコンプライアンスへの適応状況やマルウェアをチェック |
| 侵入防御 | |
| ネットワーク層での保護 | DoS、ポート・スキャン、IP/ICMP/TCP関連などの攻撃をブロック |
| アプリケーション層での保護 | DNSキャッシュ・ポイズニング、FTPバウンス、不正なコマンドなどの攻撃をブロック |
| 検出方法 | シグネチャ・ベースおよびプロトコル・アノマリ(プロトコル異常) |
| アンチウイルス/アンチスパイウェア | |
| アンチウイルス保護 | HTTP、FTP、POP3、およびSMTPプロトコルを保護 |
| アンチスパイウェア・ブロック | ゲートウェイでのパターン・ベースのスパイウェア・ブロック |
| アップデート | 一元的に実行可能なデیلیー・アップデート |
| Webフィルタリング | |
| URLデータベース | 2,000万以上のURLで30億以上のWebページを網羅 |
| 言語のサポート | 200カ国、70言語以上 |
| アップデート | 一元的に実行可能なデیلیー・アップデート(毎週10万以上の新しいサイトを追加) |
| メッセージング・セキュリティ | |
| 電子メールIPS | SMTP、POP3、およびIMAPプロトコルを悪用する攻撃を防御 |
| パターン・ベースのアンチスパム | シグネチャの動的データベースに基づいてスパムを検出 |
| IPレピュテーション・チェック | 送信者に基づいてスパムおよびマルウェアをブロック |
| シグネチャ・ベースのアンチウイルス | ウイルスおよびマルウェアに対する第一段階の防御 |
| ゼロアワー・アウトブレイク保護機能 | シグネチャ・ベースの保護機能を補完し、シグネチャが存在しない新しい攻撃をブロック |
| 拒否/許可リスト | 特定のドメインおよびユーザをきめ細かく制御 |
| 管理とレポート | |
| 集中管理 | 集中的な管理 |
| モニタリング/ロギング | SmartView Tracker [®] による詳細なモニタリングとロギング |
| レポート | Expressレポート |
| コマンドライン・インタフェース | Telnet、SSH |
| ネットワーク機能 | |
| DHCPのサポート | SecurePlatform [™] DHCPサーバおよびリレー |
| ISPの冗長性 | プロトコル・ベース、送信元/送信先、およびポート経路の決定 |
| ルーティングのサポート | OSPF、BGP、RIP v1/2、マルチキャスト |
| レイヤ2ブリッジのサポート | 既存のネットワークに透過的に統合 |
| パフォーマンスとアベイラビリティ | |
| ハイ・アベイラビリティ | アクティブ/パッシブおよびアクティブ/アクティブ・フェイルオーバー・オプション |
| ロード・バランシング | ClusterXL [®] を使用することでほぼニアな規模拡大が可能 |
| QoS(サービス品質) | Floodgate-1 [®] によるきめ細かいQoS制御 |
| ISPの冗長性 | トラフィックを2番目のインタフェースに自動的に再ルーティング |

UTM-1 Total Securityアプライアンスの仕様

| | UTM-1 130 | UTM-1 270 | UTM-1 570 | UTM-1 1070 | UTM-1 2070 | UTM-1 3070 |
|------------------|---|-----------------------|-----------------------|-----------------------|---------------------|---------------------|
| バージョン | R65、R70 | R65、R70 | R65、R70 | R65、R70 | R65、R70 | R65、R70 |
| 10/100/1000ポート | 4 | 4 | 6 | 6 | 8 | 10 |
| ファイアウォール・スループット | 400 Mbps | 600 Mbps | 1.1 Gbps | 2 Gbps | 3 Gbps | 4.5 Gbps |
| VPNスループット | 100 Mbps | 100 Mbps | 250 Mbps | 250 Mbps | 280 Mbps | 1.1 Gbps |
| 同時接続数 | 30万 | 60万 | 80万 | 110万 | 110万 | 110万 |
| IPSスループット | 300 Mbps ¹ | 380 Mbps ¹ | 700 Mbps ¹ | 900 Mbps ¹ | 1 Gbps ¹ | 4 Gbps ¹ |
| ユーザ数制限 | 無制限 | 無制限 | 無制限 | 無制限 | 無制限 | 無制限 |
| VLAN | 1024 ² | 1024 ² | 1024 ² | 1024 ² | 1024 ² | 1024 ² |
| UTM機能 | Yes | Yes | Yes | Yes | Yes | Yes |
| セキュリティ・アクセラレーション | No | No | No | No | No | Yes |
| 複数サイト管理の統合 | スタンドアロン | Yes | Yes | Yes | Yes | Yes |
| ディスク容量 | 80 GB | 160 GB | 160 GB | 160 GB | 160 GB | 160 GB |
| 筐体デザイン(高さ) | デスクトップ・サイズ | 1U | 1U | 1U | 1U | 1U |
| 外形寸法(mm) | 270 × 145 × 40 | 429 × 255 × 44 | 429 × 255 × 44 | 429 × 255 × 44 | 443 × 381 × 44 | 443 × 381 × 44 |
| 重量 | 1.6 kg (3.52lbs) | 3.7 kg (8.1lbs) | 3.7 kg (8.1lbs) | 3.7 kg (8.1lbs) | 6.5kg (14.3lbs) | 6.5 kg (14.3lbs) |
| 使用環境 | 温度：5℃～40℃、湿度：10%～85% (結露なきこと)、高度：2,500m | | | | | |
| 電源 | 100～240V、50～60Hz | | | | | |
| 電源仕様(最大) | 60W | 65W | 65W | 65W | 250W | 250W |
| 適合規格 | UL 60950; FCC Part 15, Subpart B, Class A; EN 55024; EN 55022; VCCI V-3; AS/NZS 3548:1995; CNS 13438 Class A (検査合格、国家認証申請中); KN22, KN61000-4 Series, TTA; IC-950; ROH | | | | | |

1: デフォルトのプロファイルを使用し、実運用環境のトラフィックでテストを実施

2: 1インタフェースあたりの最大VLANは256

注: すべてのUTM-1モデルには、3年間のハードウェア保証が含まれています。

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

http://www.checkpoint.co.jp/ E-mail: info_jp@checkpoint.com Tel : 03 (5367) 2500