



VPN-1 UTM

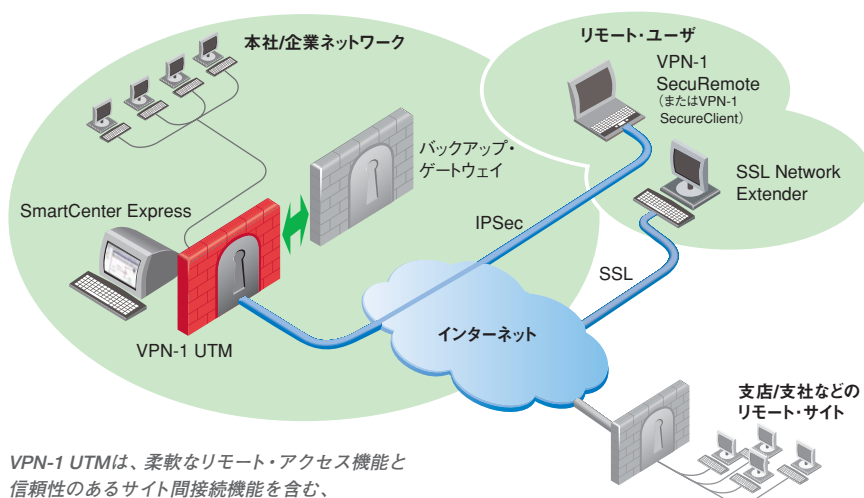
次世代の統合脅威管理ソリューション

課題

常に変化し続ける脅威と、次々に現れる新たなセキュリティ上の課題に直面している今日の多くの企業では、ネットワークを常に安全な状態に維持することのできるソリューションを必要としています。限られた管理リソースや予算で、増え続ける一方のセキュリティ上の脅威に対処するために、最高レベルのセキュリティを提供するシンプルなオールインワン・ソリューションが求められています。

解決策

VPN-1® UTM™は、あらゆる規模の企業に対応するスケーラビリティを備えた統合脅威管理ソリューションです。実績ある各種のセキュリティ機能を1つのソリューションとして提供することにより、セキュリティ環境の簡素化を可能にします。VPN-1 UTMでは、ファイアウォール、侵入防御、アンチウイルス、アンチスパイウェア、Webアプリケーション・ファイアウォール、IPSec VPNおよびSSL VPNの各機能が、容易に管理可能な1つのソリューションに完全に統合されています。Fortune 100企業で採用されているものとまったく同じレベルの、チェック・ポイントの実績あるセキュリティ技術が組み込まれたVPN-1 UTMは、完全に統合されたセキュリティ環境を求める企業に最適なソリューションです。また、チェック・ポイントの統合管理プラットフォームNGXを基盤とするSmartCenter™管理インターフェースにより、管理者はネットワーク上のセキュリティ・コンポーネントをすべて集中制御することが可能になるため、管理業務の煩雑さとそれに伴う負担も軽減されます。



VPN-1 UTMは、柔軟なリモート・アクセス機能と信頼性のあるサイト間接続機能を含む、実績あるUTM (統合脅威管理) 機能を提供します



NGXプラットフォームは、チェック・ポイントの境界、内部、およびWebセキュリティに対する統合されたセキュリティ・アーキテクチャを提供します。

製品の概要

VPN-1 UTMは、あらゆる規模の企業に対応するスケーラビリティを備えた統合脅威管理ソリューションです。実績ある各種のセキュリティ機能を1つのソリューションとして提供することにより、セキュリティ環境の簡素化を可能にします。VPN-1 UTMでは、ファイアウォール、侵入防御、アンチウイルス、アンチスパイウェア、Webアプリケーション・ファイアウォール、IPSec VPNおよびSSL VPNの各機能が、容易に管理可能な1つのソリューションに完全に統合されています。

製品の特長

- ファイアウォール、侵入防止、アンチウイルス、アンチスパイウェア、Webアプリケーション・ファイアウォール、IPSec VPNおよびSSL VPNの各機能を統合
- Fortune 100企業で採用されているものとまったく同じ、チェック・ポイントの実績ある技術を搭載
- 複数のサイトにまたがるセキュリティ・タスクを集中管理

製品の利点

- 実績あるUTM機能により、強固なセキュリティを実現
- 完全に統合および一元化された管理により、セキュリティ環境をシンプル化
- SmartDefenseサービスにより、防御機能を常に最新の状態に維持

NGXの特長

- インテリジェントなVoIPセキュリティ
- 管理の統一化
- モニタリングの強化



チェック・ポイントは、境界、内部、WEBなど、ネットワークのあらゆる局面に対するセキュリティ・ソリューションを提供します。これにより、企業はネットワークや、ネットワーク・リソース等を安全に保護しながら、高い接続性を実現するリモート・アクセスを提供し、簡単に管理することができます。

実績ある統合脅威管理

VPN-1 UTMは、ネットワーク層およびアプリケーション層に対する既知または未知の攻撃からネットワークを確実に保護します。VPN-1 UTMでは、実績あるファイアウォール機能をはじめ、侵入防御、アンチウイルス、アンチスパイウェア、およびVPNの各機能が1つのソリューションとして提供されるため、単独機能のセキュリティ・ソリューションをいくつも導入せずに済み、セキュリティ環境を簡素化します。チェック・ポイントの他のソリューションと同様に、Webアプリケーション・ファイアウォールやエンドポイント・セキュリティ・モジュールなどの各種追加コンポーネントによって拡張することも可能です。

ビジネスにとって重要性の高いアプリケーションの保護

VPN-1 UTMは、初期設定の状態、事前定義された150以上のアプリケーション、サービス、およびプロトコルを検査します。これにより、企業環境で使用される大半のアプリケーションのトラフィックが、ネットワークに入ってきたときには安全な状態であることが保証されます。保護されるアプリケーションの例を次に示します。

- Voice over IP: 通信コスト削減を図るために、VoIPアプリケーションの採用が多くの企業で急速に進んでいます。VPN-1 UTMは、VoIPプロトコルを包括的にサポートし、ビジネスにとって重要性の高い通信の安全性を確保します。
- インスタント・メッセージングおよびP2Pアプリケーション: これらのアプリケーションは、しばしばワームやウイルス、スパイウェアの攻撃対象となっています。VPN-1 UTMでは、トラフィックの内容を検査するかまたはそのトラフィックが企業ネットワークに入ることを禁止することによって、これらのアプリケーションのセキュリティを確保します。

ゲートウェイでのウイルス、ワーム、およびスパイウェア対策

ワームなどに代表されるマルウェアの多くは、電子メールの添付ファイルやユーザがダウンロードするファイルとしてネットワーク内に侵入し、ユーザがそのファイルを開いた時点で自動的にネットワーク内の全コンピュータへの攻撃を開始します。また現在では、スパイウェアも、ITインフラストラクチャやネットワーク帯域に大きな影響を与える脅威の1つとなっています。そこでVPN-1 UTMでは、ゲートウェイ・アンチウイルスとチェック・ポイントのSmartDefense™技術を組み合わせることにより、ウイルスとスパイウェアをゲートウェイでブロックできるようにしています。VPN-1 UTMのアンチウイルス機能は、電子メール(SMTPおよびPOP3)、Web(HTTP)、およびFTPトラフィックのリアルタイム・スキャンにも対応しているため、正規のコンテンツに含まれる脅威を検出することも可能です。

Webアプリケーション・ファイアウォール

VPN-1 UTMのオプション・コンポーネントであるWeb Intelligence™は、SQLインジェクション、クロス・サイト・スクリプティング、ディレクトリ・トラバースなどの一般的なハッキング技術からWebアプリケーションを包括的に保護します。Web Intelligenceには、Webサーバを標的とするバッファ・オーバーフロー攻撃や悪意のある実行可能コードを検知してブロックする、特許出願中の革新的な技術Malicious Code Protector™が含まれています。Web Intelligenceは、既知と未知の両方の攻撃を防止する、事前対応的な防御機能を提供します。

防御機能を常に最新の状態に維持

事前の対応的な防御を可能にするプロアクティブな防御機能によりセキュリティ・ネットワーク環境を維持し、未知の攻撃から確実にネットワークを保護するために、SmartDefenseというサービスが用意されています。SmartDefenseサービスは、防御機能やポリシーおよびその他のセキュリ

ティ要素に関連する検査情報を常に最新状態にし、継続的に自動更新するためのオプション・サービスです。SmartDefenseサービスで提供されるアップデートは、中央のサーバ管理者が一括ダウンロードして各リモート・サイトに自動配布するか、または、セキュリティ・ポリシーに基づいて個々のVPN-1 UTMゲートウェイに指定の間隔で定期的にチェックさせることができます。

サイト間VPNとリモート・アクセスVPN

VPN-1 UTMには、IPSec VPNとSSL VPNの2つのVPN機能に対応しており、リモート・サイトとリモート・ユーザを容易かつ柔軟に接続することが可能です。VPN-1 UTMの追加オプションであるSSL Network Extender™を使用すると、Webブラウザを介して、WebベースおよびIPベースのネットワーク・アプリケーションから、低コストで効率よくVPNリモート・アクセスを行えるようになります。VPN-1 UTMは、IPSecなどのクライアント・ベースのソリューションを必要とする、次のようなビジネス向けVPNクライアントを幅広くサポートしています。

VPN-1 SecuRemote®: VPN-1 UTMに含まれる製品で、VPN接続を行うクライアントPCにインストールします。データの暗号化と認証を行うことで、リモート・アクセス時における盗聴や改ざんを防止します。

VPN-1 SecureClient™: VPN-1 SecuRemoteが持つクライアント・リモート・アクセスVPN機能に加え、一括集中管理に対応したパーソナル・ファイアウォールと高度な管理機能を提供します。

Microsoft L2TP VPNクライアント: VPN-1 UTMは、Windowsユーザ向けに、Microsoft Windows L2TP VPNクライアントを使用した安全なリモート・アクセスをサポートしています。

すぐに使える強力な認証機能

製品導入と同時に強力な認証を利用する必要がある場合には、チェック・ポイントのワン・クリック証明書を利用できます。VPN-1 UTMには内部認証局が用意されており、VPN-1 UTMゲートウェイおよびリモート・アクセス・ユーザに対してX.509デジタル証明書を発行することが可能です。ワン・クリック証明書により、PKIシステムに手間や費用をかけることなく業界標準の2ファクタ認証を利用できます。

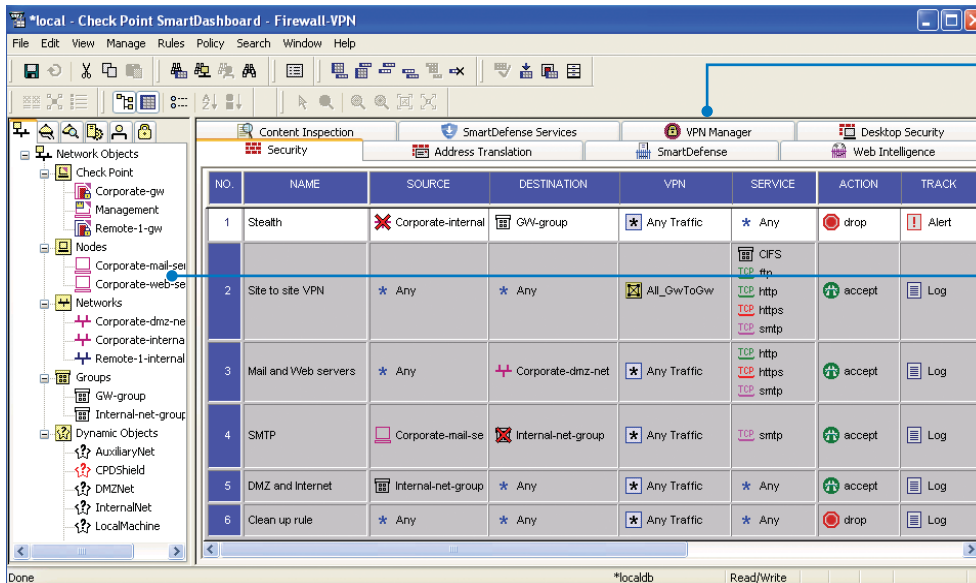
ワン・クリックVPN

ワン・クリックVPNにより、VPN接続に必要なゲートウェイに対する設定を一度の操作で行うことができます。一旦VPNコミュニティを定義すると、イントラネット、エクストラネット、およびリモート・アクセスなどVPN全体のセキュリティ・パラメータを1ステップで設定することができます。VPN接続を行なうVPN-1 UTMゲートウェイをコミュニティ内に定義するだけで、コミュニティに含まれるすべてのゲートウェイ間またはゲートウェイとリモート・ユーザ間で関連付けが行われ、自動的にVPNが有効になります。定義済みのVPNコミュニティに対し新しいサイトが追加された場合、そのサイトは適切なプロパティを自動的に継承し、VPNコミュニティを構成する他のサイトとの間で直ちに安全なIPSecセッションを確立します。

データの機密性

情報データに関するさまざまな法規制が実施されている今日では、データの機密性確保は最重要事項と言えます。VPN-1 UTMは、通信中のデータに対して現時点で最も強力な暗号化アルゴリズムを適用することにより、データの機密性を確実に保護します。VPN-1 UTMでは、次のアルゴリズムがサポートされています。

- 128-256ビットのAES (Advanced Encryption Standard)
- 56-168ビットのTriple DES



セキュリティ・ポリシーおよびアップデートは、すべてのサイトにわたって容易に管理可能

ユーザ、ホスト、ゲートウェイ等を含むすべてのネットワーク・オブジェクトは、SmartDashboardから簡単に定義し、管理可能

SmartDashboard管理インターフェースは、すべてのサイトに対する集中セキュリティ管理環境を提供します。

統合されたエンドポイント・セキュリティ

リモート・ユーザやパートナーは、家庭のPCなどの、安全性が確保されていないデバイス（IT部門の管理下にないデバイス）からネットワークにログインし、電子メールや各種アプリケーションなどの企業リソースにアクセスする場合があります。こうしたリモート・コンピュータがセキュリティ上の脅威となることのないように、VPN-1 UTMでは、ネットワークへのアクセスを許可する前に、ワームやキーロガーなどの悪意あるソフトウェアがリモート・コンピュータにインストールされていないかどうかを調べることができます。また、追加オプションとして利用できるIntegrity™ Clientless Securityにより、リモート・ユーザが各種のセキュリティ・ポリシー（アンチウイルス・ソフトウェアやパーソナル・ファイアウォールが最新であるかどうかなど）を順守しているかどうかをチェックすることも可能になります。

すべてのサイトを集中管理

VPN-1 UTMには、チェック・ポイントのSMART (Security Management Architecture) ソリューション群の一部であるSmartCenterが付属しています。SmartCenterを使用すると、VPN-1 UTMゲートウェイだけでなく、VPN-1 UTM Edge™ アプライアンスなどの他のチェック・ポイント製品も集中管理できます。SmartCenterでは、セキュリティ・ポリシーを集中管理すると共に、これらのポリシーをセキュリティ・インフラストラクチャ全体に配布することができるため、管理者は、各サイトや対応するゲートウェイに対して個別に保守作業を行う必要がなくなります。これにより、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用のシンプルな管理インターフェースであるSmartDashboard™を使用して、ファイアウォール・セキュリティやVPN、NAT（ネットワーク・アドレス変換）、QoS（サービス品質）、VPNクライアント・セキュリティなどのセキュリティ・ポリシーを定義および管理できます。

ノンストップのビジネス環境

VPN-1 UTMは、企業ネットワーク・リソースの可用性を高めるハイ・アベイラビリティ機能をサポートしています。ハイ・アベイラビリティ機能を使用して複数のゲートウェイでクラスタを構成することにより、企業ネットワークの可用性を常に保証できるようになります。万が一プライマリ・

ゲートウェイへのVPN接続に障害が発生した場合は、すべての接続が他のクラスタ・メンバーにシームレスにリダイレクトされます。クラスタにゲートウェイを追加すると、パフォーマンスはほぼニアに向上します。また、ハイ・アベイラビリティを構成するプライマリ・インターフェースに障害が発生した場合、トラフィックはセカンダリ・インターフェースおよびセカンダリ接続として設定したISPに対し経路を変更することが可能で、ハードウェア自体の二重化による冗長性のほか、ISP接続の二重化による回線側の障害にも備えます。障害発生時に確立されていた接続は、フェイルオーバーの際もそのまま維持されます。

VPNに対するQoSのサポート

インターネット・リンクの輻輳や意図しないトラフィックの増加などによりパフォーマンスが低下する可能性のあるVPN環境では、QoSを使用した帯域幅管理によるトラフィック・コントロールが重要になります。VPN-1 UTMの追加オプションであるFloodGate-1®は、ビジネスにとって重要性の高いアプリケーションやユーザに対して優先順位を設定することで、VPNトラフィックを含むネットワーク・トラフィックを最適化します。FloodGate-1を利用することで、ミッション・クリティカルなVPNトラフィックやVoIPなど優先すべきトラフィックは、プライオリティの低いトラフィックより優先されるので、アプリケーションのクオリティを低下させません。

優れたパフォーマンスと導入

VPN-1 UTMは、導入先の規模や必要とするパフォーマンスに応じたさまざまな導入オプションをサポートしており、導入環境や予算に応じて最適なプラットフォームやソリューションを選択できます。

- "Secured by Check Point"ロゴのあるアプライアンスは、VPN-1 UTMソフトウェアがインストール済みです。
- チェック・ポイントのメディア・バックにはSecurePlatform™が含まれます。SecurePlatformはセキュリティを強化したオペレーティング・システムで、チェック・ポイント製品を10分程度でインストールできるセキュリティ・プラットフォームです。

VPN-1製品導入時の推奨プラットフォームの一覧は、以下のサイトをご覧ください。

www.checkpoint.com/products/choice/platforms.html

その他の機能

VPN-1 UTMは、以下のさまざまな実施モジュールおよび管理モジュールをサポートしています。

VPN-1 UTMゲートウェイを追加すると、新たな拠点に対しファイアウォールおよびVPN機能を導入できます。

ハイ・アベイラビリティ対応のVPN-1 UTMゲートウェイを既存のゲートウェイに追加する形で導入すると、ネットワークの可用性と冗長性を高めることができます。

パフォーマンス・アクセラレータ・カード (PCIボード) を追加すると、ハードウェアベースの強力な暗号化処理が可能となり、既存のVPN-1 UTMゲートウェイのパフォーマンスを向上させることができます。

VPN-1 SecureServer™は、個々のアプリケーション・サーバのセキュリティやクライアント/サーバ間の通信を保護するためのVPN/ファイアウォール・アプリケーションです。

ClusterXL®は、ゲートウェイのクラスター間でトラフィックを分散させ、パフォーマンスとスケーラビリティの向上を可能にします。

FloodGate-1は、ポリシーベースのQoS機能を提供し、ビジネスにとって重要性の高いアプリケーションやエンド・ユーザに対して優先順位を設定することで、ネットワークのパフォーマンスを最適化します。

SSL Network Extender™は、強化されたSSL VPN機能によりWeb上での完全なネットワーク・レベルのアクセスを提供します。

SmartMap™は、セキュリティ管理ネットワーク中のセキュリティ実施内容に関する詳細情報をグラフィカル・マップで表示し、その整合性を事前に確認できるようにします。

SmartUpdate™は、チェック・ポイント製品のソフトウェアおよびライセンスを集中管理し、企業ネットワーク全体で一貫したセキュリティ・ポリシーの実施を可能にします。

SmartDirectoryは、VPN-1 UTMと1台以上のLDAP対応ディレクトリ・サーバとの統合を可能にします。

SmartView Monitor™は、帯域幅、ラウンド・トリップ時間、パケット・ロスなどのパフォーマンス測定結果をグラフィカルに表示し、ネットワーク・トラフィックに関する状況分析をリアルタイムに行えるようにします。

SmartCenter Plusは、SmartCenterにSmartMap、SmartUpdate、SmartDirectory、SmartView Monitor、およびSmartPortal (Webブラウザを用いてセキュリティ・ポリシーにアクセスするためのWebベースのツール) という各管理モジュールの機能を追加したSmartCenterの拡張版です。

Eventia Reporter™は、チェック・ポイント製品が生成するログ・データを基に、詳細なネットワーク状況およびイベントに関する綿密な情報をグラフ化、リスト化してリアルタイムに表示するレポート・システムです。

UserAuthority®は、e-ビジネス・アプリケーションに対し、統合Webセキュリティ、シングル・サインオン、およびアイデンティティ管理の機能を提供します。

Web Intelligenceは、チェック・ポイント製品にWebアプリケーション・ファイアウォール技術を提供します。

システム要件

VPN-1 UTMゲートウェイとSmartCenter	
プラットフォーム	Check Point SecurePlatform、SecurePlatform Pro
ディスク容量	4GB
メモリ	256MB (512MBを推奨)
SmartConsole	
プラットフォーム	Solaris、Windows 2000/2003/XP/ME/98
ディスク容量	100MB
メモリ	256MB
リモート・アクセス・クライアント*	
プラットフォーム	Windows 2000/XP/2003/Pocket PC 2003 2nd Edition/Handheld PC 2000、Macintosh、Linux
ディスク容量	20MB
メモリ	64MB

*VPN-1 SecuRemote、VPN-1 SecureClient、Integrity SecureClient

サポート・プラットフォームおよびシステム要件に関する詳細は以下のWebサイトをご覧ください。
http://www.checkpoint.com/products/supported_platforms/platforms_appint.html

©2006 Check Point Software Technologies Ltd. All rights reserved.

Check Point, Application Intelligence, Check Point Express, Check Point of the Logo, AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, Eventia, Eventia Analyzer, Eventia Reporter, Firewall-1, Firewall-1 GX, Firewall-1 SecureServer, FloodGate-1, Hacker ID, IMSecure, INSPECT, INSPECT XL, Integrity, InterSpec, IQ Engine, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureXL Turbocard, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 UTM, VPN-1 Power, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, VPN-1 XL, Web Intelligence, ZoneAlarm, ZoneAlarm Pro, Zone Labs, およびZone Labsのロゴは、Check Point Software Technologies Ltd.あるいはその関連会社の商標又は登録商標です。その他の企業、製品名は各企業が所有する商標または登録商標です。本書で記載された製品は米国の特許No. 5,606,668、5,835,726、6,496,935、6,873,988、および6,850,943により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。本書で記載された製品は米国の特許No.5,606,668、5,835,726、6,496,935、および6,850,943により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。

P/N 502123-J 2006.05 ※記載された製品仕様は予告無く変更される場合があります。



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

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