



小規模環境に エンタープライズ・レベルの ネットワーク・セキュリティ

製品の概要

チェック・ポイントのSafe@Office® UTMアプライアンスは、短時間で簡単に導入できるデスクトップ・サイズのアプライアンスです。包括的なエンタープライズ・レベルのセキュリティと企業リソースへの安全なリモート・アクセス機能が必要とする小・中規模の企業に最適です。

Safe@Office UTMアプライアンス

課題

今日、小・中規模の企業が業務を効率化して成長を遂げるためには、社員や外部の関係者が、必要に応じて社内の重要なアプリケーションや情報にアクセスできることが不可欠です。しかしその一方、ほんのわずかな規模でもデータ侵害が発生した場合には、訴訟や罰金・罰則、社会的信用の失墜などの大きなダメージを被るおそれがあります。ハッキング手法やマルウェアもますます高度化しており、データ侵害の発生を防ぐためには、重要データへの厳しいアクセス制限が必須となります。そのため、IT関連の予算や人員が限られている小・中規模の企業では、データ侵害のリスクを最小限に抑えつつ、どこからでも安全に社内の重要なリソースにアクセスできる、低価格で包括的なソリューションが求められています。

解決策

チェック・ポイントのSafe@Office® UTMアプライアンスは、クラス最高レベルの実績を誇るセキュリティとシンプルさを両立させた、低コストのオールインワン・セキュリティ・ソリューションです。簡単な設定だけですぐに運用を開始することができ、SOHOや小規模オフィスなどの組織に適しており、ファイアウォールやIPS、アンチマルウェアなどの包括的な保護機能を低コストで素早く簡単に導入できます。確かな性能、直感的な操作が可能な管理機能、および先進の無線接続機能を備えるこのシンプルなオールインワン・ソリューションは、比類なき効果を発揮します。

セキュリティ

クラス最高レベルのファイアウォールとIPSの統合

Fortune 100 企業でも採用されているチェック・ポイントの技術をベースとする Safe@Office UTM アプライアンスは、業界最高レベルの実績を誇るファイアウォール技術を搭載しています。包括的なネットワーク・アクセス制御 (NAC) ではインスタント・メッセージ (IM) やピアツーピア (P2P) などの好ましくないアプリケーションをブロックでき、先進の侵入防御システム (IPS) ではサービス妨害 (DoS) やポート・スキャン、バッファ・オーバーフローといった既知および未知の脅威から確実に保護できます。

安全なVPN接続

IPSec VPN 接続では、安全なサイト間接続およびリモート・アクセス接続を実現できます。Check Point Endpoint ConnectやSecureClient、SecuRemote、L2TP など複数のVPNクライアントをサポートしているため、さまざまなユーザのニーズへ柔軟に対応できます。

アンチマルウェアとメッセージング・セキュリティ

ゲートウェイに統合されたアンチマルウェア機能は、ワームやウイルスをネットワークの手前でブロックします。また、サイズに制限なく大きな圧縮ファイルでもオンザフライで解凍できるため、徹底的な脅威のスキャンが可能です。チェック・ポイントのメッセージング・セキュリティ機能は、スパムをブロックするだけでなく、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。

製品の特徴

- クラス最高レベルのファイアウォールと侵入防御 (IPS) の統合
- アンチマルウェア、メッセージング・セキュリティ、Webフィルタリング、ネットワーク・アクセス制御 (NAC) を搭載
- ウィザードベースの管理 (セキュリティルールの事前定義、自動アップデート、監視、レポート)
- 802.11n WiFiおよび3Gに対応したシームレスな無線接続
- 幅広いトラフィック管理パラメータによりQoS (サービス品質) を保証

製品の利点

- 小・中規模企業 (SMB) でも、単一アプライアンスで包括的なエンタープライズ・レベルのセキュリティを実現
- 低コストで実現するギガビット・レベルのファイアウォール・パフォーマンス
- ハイ・アベイラビリティ・オプションにより、ビジネス上の重要なアプリケーションを常にセキュリティ機能で保護
- IT 管理者が少ない環境でも迅速かつ容易な導入が可能



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	電子メールの"指紋"情報を既知のスパムのシグネチャが大量に登録された動的なデータベースと照合して、既知のスパムをブロック
拒否/許可リストによるアンチスパム	スパム送信者からの電子メールをブロックし、信頼できる送信者からの電子メールを許可(ドメイン・レベルのブロックや許可も可能)
メールのアンチウイルス	ワームやウイルスをゲートウェイでブロック(POP3、IMAP、SMTPなどの標準的な電子メール・プロトコルとWebベースの電子メールをサポート)
IPSによる電子メール・サーバの保護	サービス妨害(DoS)攻撃のようにメッセージング・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

業界最高レベルのURLフィルタリング・サービスでは、組織独自のWebアクセス規定を策定することが可能です。スパイウェアやウイルス、不適切なWebコンテンツが潜んでいる可能性のある悪意あるWebサイトへのアクセスをブロックできます。

ネットワーク・アクセス制御(NAC)

802.1Xポートベースの認証では、ユーザのアクセス権限や支社・支店環境におけるセキュリティ・ポリシーの遵守状況に基づいてネットワーク・アクセスを制御できます。また、EAP(Extended Authentication Protocol)のサポートにより、RADIUS認証サーバを別途用意することなくWPA Enterpriseおよび802.1Xによるアクセス制御を実施できるため、小規模ネットワークでも簡単にNACを利用できます。

ネットワーク機能

高性能のネットワーク機能

Safe@Officeは、LANスイッチ、DMZポート、WANポート(EthernetまたはADSL)といった本格的なネットワークルータ機能を備えています。また、スタティック・ルーティングおよびダイナミック・ルーティングの機能も備えているため、柔軟な対応が可能です。

Safe@Office 1000N アプライアンスには、最先端のハードウェア・アクセラレーションや6つの1Gbps Ethernetポートなど、優れたネットワーク機能とセキュリティ機能が標準で搭載されています。

安全なホット・スポットのサポート

管理者はWebベースの安全なホット・スポットを作成して、ネットワークへのゲスト・アクセスを容易に許可できます。企業リソースへのアクセスを許可する前に、ユーザ認証や利用規約への同意を求めたりすることも可能です。

高可用性

ビジネス上の重要なアプリケーションをはじめとするさまざまなネットワーク・アクティビティの利用を常に確実とするため、ハイ・アベイラビリティ

ティ・オプションが用意されています。Safe@Office UTM アプライアンスでは、ネットワーク接続とサービスの可用性を常時維持するため、WAN接続の冗長化を行なうWAN Redundancyとロード・バランシング機能がサポートされています。ブロードバンド接続に障害が発生した場合も、バックアップとしてダイヤルアップでのインターネット接続が可能です。(別途外部モデムが必要です)

QoS(サービス品質)

プライオリティによる「優先順位付け」、「帯域保証」、「帯域制限」といった包括的なトラフィック管理機能が用意されており、インターネット接続が1回線だけでも、ビジネス上重要で遅延の許されないトラフィックのQoSを保証できます。無線マルチメディアQoSでは、動画や音声などの各種アプリケーションのトラフィックに優先順位を付けることができます。

無線接続のローミング

Wireless Distribution System(WDS)機能を使用すると、複数のSafe@Office無線アプライアンスを相互接続してネットワークを拡張できます。これにより、ノートPCやPDAなどの無線クライアントは、IPアドレスを変更することなくシームレスに無線ネットワークをローミングできるようにになります。

注：現在日本国内において無線LAN機能は使用できません。お問合せください。

管理機能

短時間での容易なセットアップ

Safe@OfficeにはシンプルなWebベースの管理インターフェースが用意されており、セキュリティ設定はわずか数分で終了します。設定ウィザードを使用して、事前定義されたファイアウォール・ポリシーを選択したり、カスタム・セキュリティ・ポリシーを作成したりできます。セキュリティ・ルールは各種のリモート管理オプションを使用して簡単に変更することが可能です。

ネットワークの監視

Safe@Officeでは、攻撃の試みに関する情報(攻撃元のIPアドレスなどをログに記録し、色分けされたレポートで表示することができます。また、ログに含まれているIPアドレスより管理者を素早く把握するための「WHOIS」ユーティリティは、インターネット上での「ナンバー・ディスプレイ機能」として利用できます。さらにトラフィック監視ツールとパケット・キャプチャ・ツールが用意されており、これらを使用して内向き/外向きのトラフィックを監視および制御することで、帯域を有効に活用することが可能になります。

冗長性のあるインターネット接続

Safe@Office 1000Nと1000NWアプライアンスではPSTNおよびISDNが完全サポートされるほか、各種の3Gセルラー・モデムを利用することも可能です。インターネット接続に障害が発生した場合には、帯域外ダイヤルインを利用してアプライアンスにアクセスできます。

アップデート

オプションとして提供されるサブスクリプション・サービスを利用すると、ソフトウェアやアンチウイルスのアップデート、URLフィルタリング・サービス、定期的なセキュリティ・レポート、アンチスパム、ダイナミックDNSサービスといったサービスを継続的に受けることができます。

ハードウェア・オプション

安全な無線LAN接続機能

Safe@Office 1000Nアプライアンスは、802.1x、IPSec over WLAN、RADIUS、WEP、WPA、WPA2認証など、複数のセキュリティ・プロトコルをサポートするWiFiアクセス・ポイント機能(802.11b/g/nに対応)を内蔵



しています。また、無線LANセグメント固有のセキュリティ・ルールを設定できる無線LAN専用インターフェースも備えています。この無線インターフェースは、それぞれ固有のセキュリティ・ポリシーと暗号化アルゴリズムを設定した最大4つのバーチャル・アクセス・ポイントに分割することも可能です。

Safe@Office 500W アプライアンスは、無線通信の長距離化と高速化を実現する Super-G および Extended Range(XR) 規格に対応した無線アクセス・ポイント機能を内蔵しています。無線ネットワークは、それぞれ固有のセキュリティ・ポリシーと暗号化方法を設定した複数のバーチャル・アクセス・ポイントに分割することが可能です。リモート・ユーザの認証は、認証規格のWPA2をはじめとするさまざまな方式で行うことができます。

注：現在日本国内において無線LAN機能は使用できません。お問合せください。

内蔵ADSLモデム

Safe@Officeアプライアンスは、オプションで高速ADSLモデムを内蔵することができるため、外部ADSLモデムを導入する必要がなく、ネットワーク環境をシンプルにすることができます。ADSL v2/2+, Annex A, Annex Bなど、最新のADSL規格がサポートされています。

注：現在日本国内においてADSL機能は使用できません。お問合せください。

仕様

Safe@Officeシリーズ	Safe@Office 500 Safe@Office 500W*	Safe@Office 1000N Safe@Office 1000NW*
セキュリティ機能	ファイアウォール、VPN、侵入防御、アンチウイルス、アンチスパム、URLフィルタリング	
オンボード管理	対応	
無線LAN*	802.11 b/g:500W、802.11 b/g/n:1000NW	
3Gモデムのサポート	-	対応
ソフトウェアのバージョン	Embedded NGX 8.1	
Ethernetポート	6ポート (10/100)	6ポート (10/100/1000)
ファイアウォール・スループット	190Mbps	1Gbps
VPNスループット	35Mbps	200Mbps
同時接続数	8,000	60,000
VLAN	32	64
筐体デザイン	デスクトップ・サイズ	
寸法 (W x H x D)	20 x 3.3 x 12.2cm (1000NW : 20 x 3.2 x 13cm)	
動作温度	0°C~40°C	
動作湿度	10%~90% (結露なきこと)	
電源	100~240V、50~60Hz	

* 現在日本国内において無線LAN機能は使用できません。お問合せください。



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

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

© 2003-2010 Check Point Software Technologies Ltd. All rights reserved.

Check Point, Abra, AlertAdvisor, Application Intelligence, Check Point DLP, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Pointのロゴ, Check Point Full Disk Encryption, Check Point Horizon Manager, Check Point Media Encryption, Check Point NAC, Check Point Network Voyager, Check Point OneCheck, Check Point R70, Check Point Security Gateway, Check Point Update Service, Check Point WebCheck, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, DefenseNet, DLP-1, DynamicID, Endpoint Connect VPN Client, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IP Appliances, IPS-1, IPS Software Blade, IPSO, Software Blade, IQ Engine, MailSafe, More, better, Simpler Securityのロゴ, MultiSpect, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, puresecurityのロゴ, Safe@Home, Safe@Office, Secure Virtual Workspace, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, SiteManager-1, Smart-1, SmartCenter, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, SmartEvent, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartProvisioning, SmartReporter, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SmartWorkflow, SMP, SMP On-Demand, SofaWare, Software Blade architecture, softwarebladesのロゴ, SSL Network Extender, Stateful Clustering, Total Security, totalsecurityのロゴ, TrueVector, UserCheck, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Edge, VPN-1 MASS, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VE, VPN-1 VSX, VSX-1, Web Intelligence, ZoneAlarm, ZoneAlarm Antivirus, ZoneAlarm DataLock, ZoneAlarm Extreme Security, ZoneAlarm ForceField, ZoneAlarm Free Firewall, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Security Toolbar, ZoneAlarm Secure Wireless Router, Zone Labs, Zone Labsのロゴは、Check Point Software Technologies Ltd.あるいはその関連会社の商標または登録商標です。ZoneAlarm is a Check Point Software Technologies, Inc. Company.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、5,987,611、6,496,935、6,873,988、6,850,943、7,165,076、7,540,013、および 7,725,737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 500050-J 2010.12 ※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。