WatchGuard

Firebox

XTM eXtensible Threat Management

進化する脅威を
「RED」で迎え撃つ

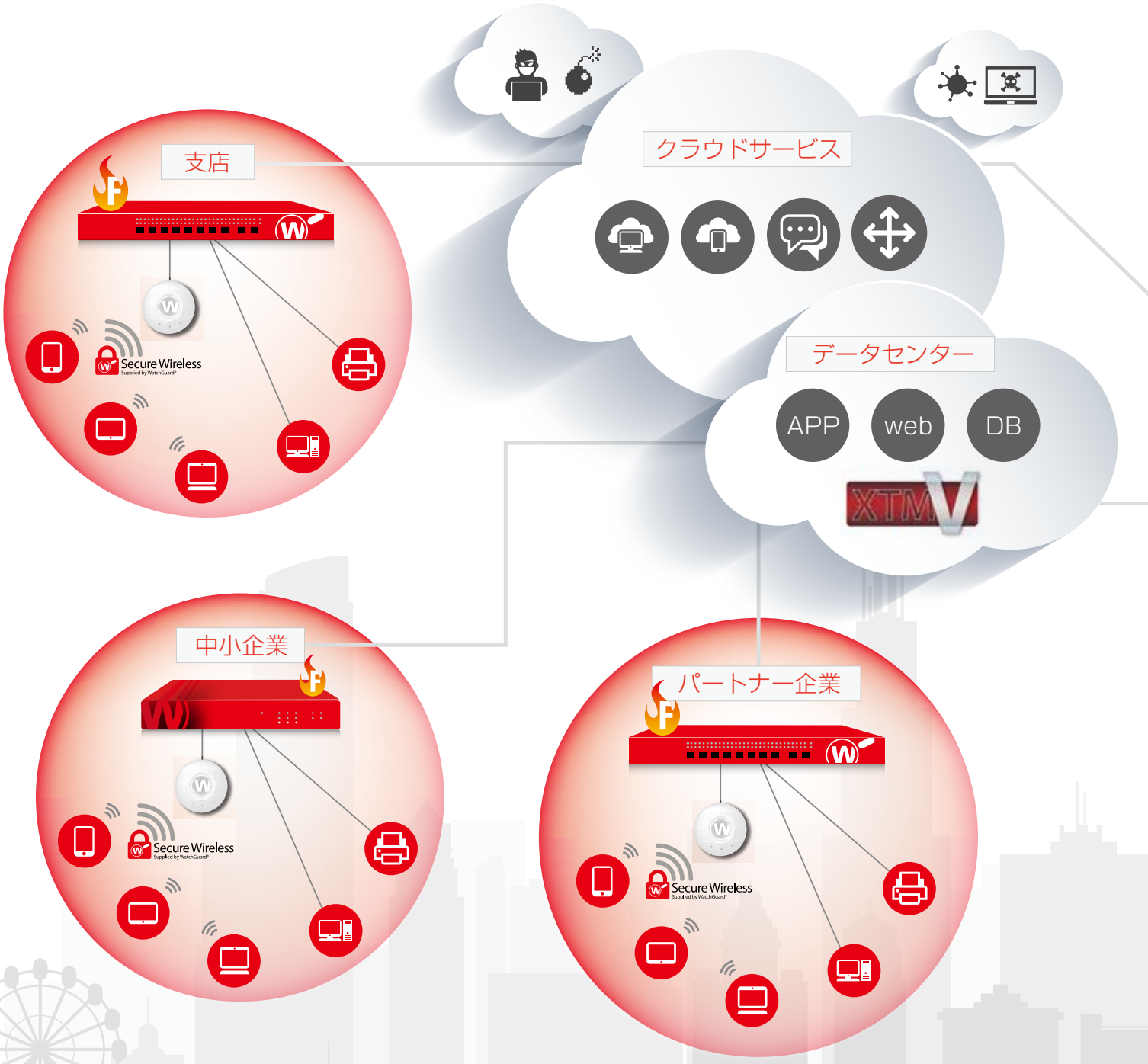
ウォッチガードの使命：

それはサイバー攻撃からビジネスを**「守り抜く」**こと。

現代のビジネスはオンラインのネットワーク抜きでは考えられません。ネットワークはその規模の大小に関係なく、あらゆる場所に張り巡らされています。本社をはじめとして支社／支店、店舗、提携先、データセンター、あるいはノートPCやタブレット、スマートフォンといった個人の無線デバイスなど、あらゆる拠点／機器がつながり、膨大な量の機密情報や個人情報がやり取りされています。

このような環境の中、セキュリティが脆弱な拠点や機器を起点とした標的型のサイバー攻撃が増加の一途を辿っています。今、有線無線を問わず、すべてのゲートウェイとエンドポイントに情報セキュリティ対策が求められています。少しでもほころびがあれば、そこを入口として侵入され、目的先に攻撃が仕掛けられる可能性があります。

ウォッチガードは情報セキュリティのプロフェッショナルとして、こうしたサイバー攻撃による「情報漏えい」や「ビジネスの停止」による被害／損失を防ぐことを使命としています。



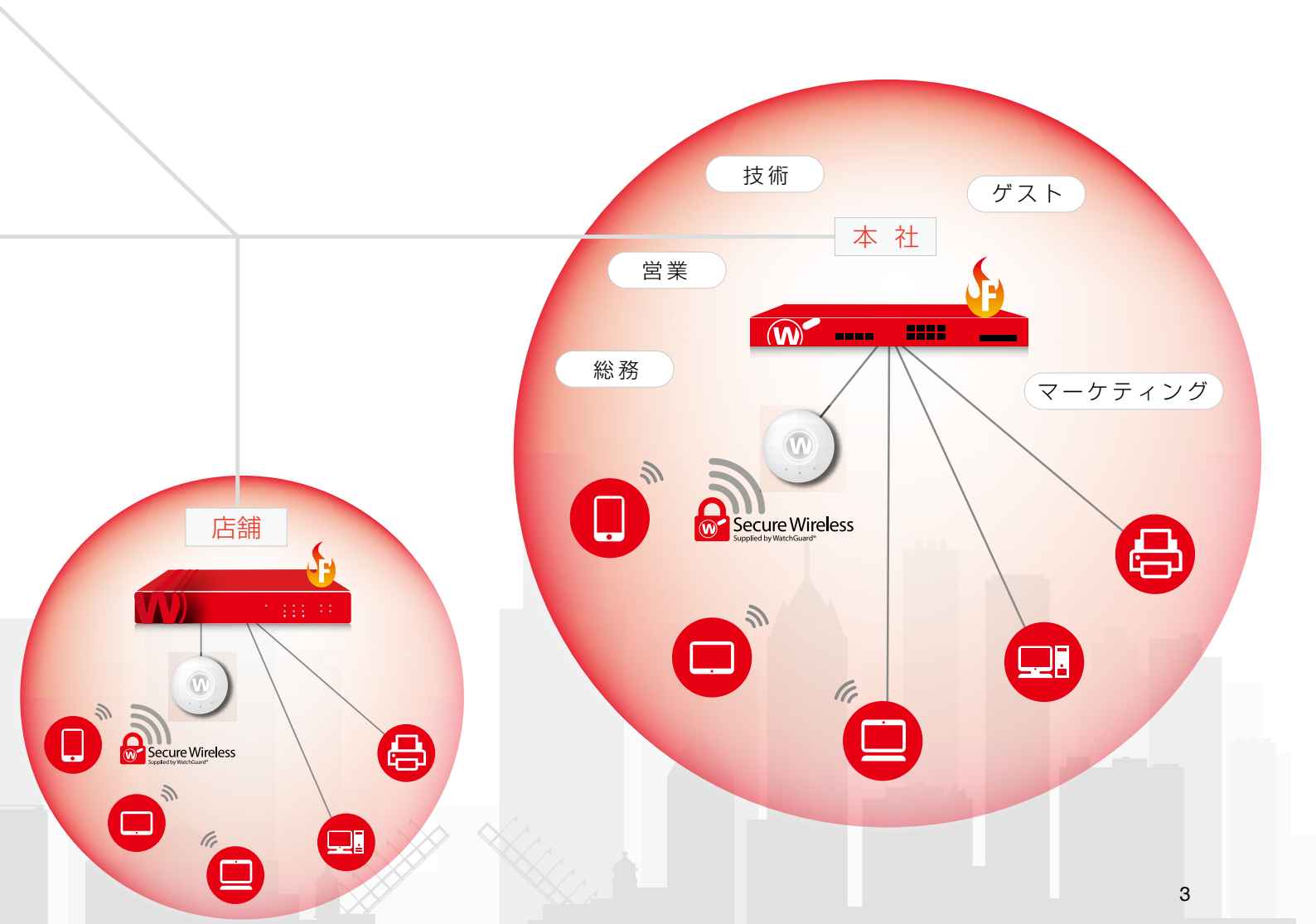
なぜウォッチガードなのか?

求められる「高性能」、「シンプル性」、「低コスト」の三要素を兼ね備えた渾身のセキュリティアプライアンス。

ウォッチガードのUTM(統合脅威管理)／NGFW(次世代ファイアウォール)アプライアンスは、ベストオブブリードの最先端技術が1台のハードウェアに統合されており、SOHO、中小規模、中堅規模、大規模といったあらゆる組織に対して、それぞれ適正なアプライアンスをご用意しています。また、仮想環境や無線LAN環境にも対応しており、包括的かつ柔軟性に富んだ情報セキュリティソリューションの実現を支援しています。

WatchGuard Firebox/XTM はネットワークの全ての脅威に有効なソリューションです。

- 企業のネットワークの保護に必要なすべてのセキュリティ機能を1台に集約
- 各セキュリティ機能を有効にしつつ高いスループットを実現
- ウイルス感染、不正アクセス、迷惑メール、ネットワーク攻撃など、さまざまな脅威をブロック
- Webフィルタリング、アプリケーション制御により、企業の生産性の向上を支援
- 個別のセキュリティ機能を組合せる場合に比べて、優れたROI(費用対効果)を実現
- 導入・運用・管理がシンプルで、手間がかからず専門的な知識も不要
- グラフィカルなレポート機能により、複雑なセキュリティ管理を分かりやすく「見える化」
- 広範かつ強力な防御を可能にするアプリケーションプロキシを採用
- 未知の脅威からネットワークを守る標的型攻撃対策



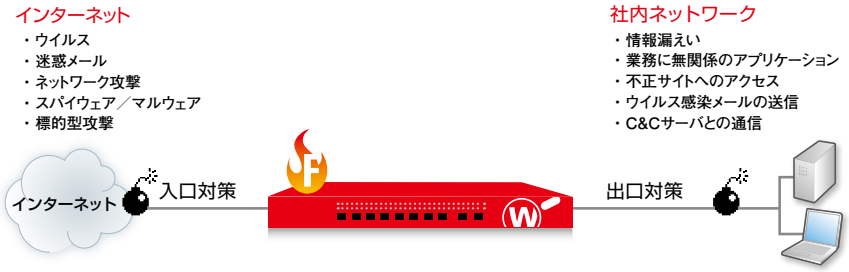
包括的なソリューション
多彩なニーズにお応えする各種先進機能をご用意しています。

Solution1 防御しきれない、巧妙化したマルウェアへの対処と情報漏えい対策

攻撃者は従来の添付ファイルやアプリケーションなどの脆弱性以外にスパム／フィッシングメール、SNSなどのソーシャルメディア、脆弱なWebアプリケーションなど様々な経路と手法を駆使して企業内に侵入し、情報を盗み出そうと考えています。もはや従来のウイルス対策やスパムメール対策などの単体の製品だけで防御することが難しくなっています。

UTM/NGFWによる多層防御

- 複数のセキュリティ機能を1台に統合することで効率的にセキュリティ強度を向上
- 多層防御によりあらゆる攻撃を阻止
- 担当者の管理・保守業務の負荷を軽減



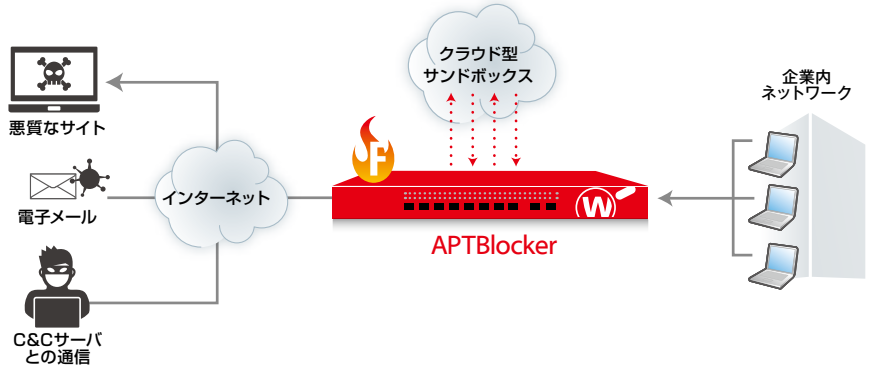
Solution2 変異し続ける悪質マルウェアからの防御

攻撃者はシグネチャベースのセキュリティ対策を容易にすり抜ける変異型やゼロデイ攻撃※を利用したマルウェアを利用し、さまざまな手段で企業情報へのアクセスを試みます。企業のIT環境は、直接の攻撃対象となるリスク以外に、関連企業への踏み台にされ、知らぬ間に加害者になっている可能性もあり、すべての企業に対策が必要となっています。

※ ソフトウェアの修正情報、シグネチャが用意できていない脆弱性への攻撃

WatchGuard APTBlocker による標的型攻撃対策

- APTBlocker:標的型攻撃やゼロデイアタックを検出する業界で最も洗練されたセキュリティプラットフォーム
- シグネチャによる既知のマルウェア検知に加え、ファイル内部に埋め込まれた行動を詳細に分析し、回避行動をとる巧妙なマルウェアも的確に検出
- クラウドベースの次世代型サンドボックスと連携し、ファイルの正確なコード分析により標的型攻撃につながる脅威を検出

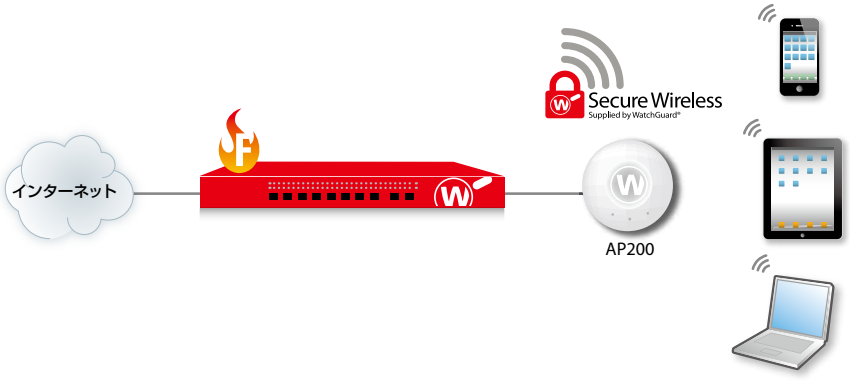


Solution3 無線LANのセキュリティ対策

タブレット、スマートフォンおよびノートPCなどからの無線接続やBYOD（Bring Your Own Device）の普及により、無線LANネットワークに対するセキュリティの課題が増大しています。IT管理者やセキュリティ管理者には企業内の有線と無線LANの両者の安全性を確保することが求められています。

WatchGuard AP200による モバイルセキュリティ

- ウォッチガード製品と連携し、シームレスに無線LANアクセスにもセキュリティを適用
- セキュリティポリシーの順守とデバイスの一元管理により管理負荷を大幅に軽減



Solution4 ネットワークセキュリティの可視化

万が一、セキュリティの事故やマルウェアによる情報漏えいが発見されれば、企業の信頼性や収益にも大きな影響が出ます。セキュリティ管理者は常に企業ネットワーク内を監視し、不正なトラフィックを識別して迅速かつ的確な対処が求められます。

WatchGuard Dimensionによるネットワークセキュリティの監視

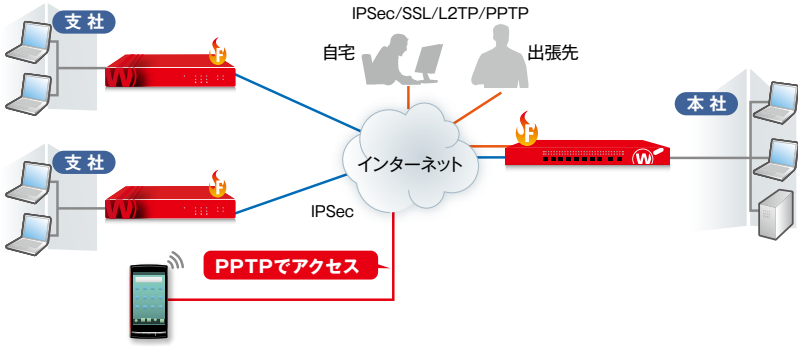
- すべてのトラフィックをリアルタイムで分析し、ネットワークセキュリティの可視化と最適なセキュリティポリシーの策定を支援
- 豊富なレポーティング機能により、役職に応じたサマリおよび詳細レポートを生成
- クライアント端末情報、ユーザやアプリケーションの相関ビュー、ピンポイントのトレンド情報など、ネットワークアクティビティを高次元でビジュアル化
- 必要に応じて個別のログデータまで簡単にドリルダウンして確認

Solution5 拠点間の安全かつ高速な接続

インターネットが必須となるすべてのビジネスにおいて、回線コストの削減とセキュリティ対策の実現は大きな課題となっています。このような課題の解決手段としてインターネットを専用線のように使用することのできるVPN接続は、多くの企業で導入されています。

WatchGuard VPN(Virtual Private Network)ソリューション

- 複数のVPN機能を搭載しており、回線コスト削減に大きな効果を発揮し、セキュアで高速VPNネットワークを構築
- 洗練された管理インターフェイスにより、ドラッグ&ドロップで簡単にVPN設定が可能なため、複数の複雑なVPNトンネルの作成も容易で管理者の負荷を軽減
- オフィスとビジネスパートナー間で安全なネットワーク通信を実現し、ウォッチガードのアプライアンスとIPSec対応デバイスの間で暗号化されたトンネルを柔軟に作成

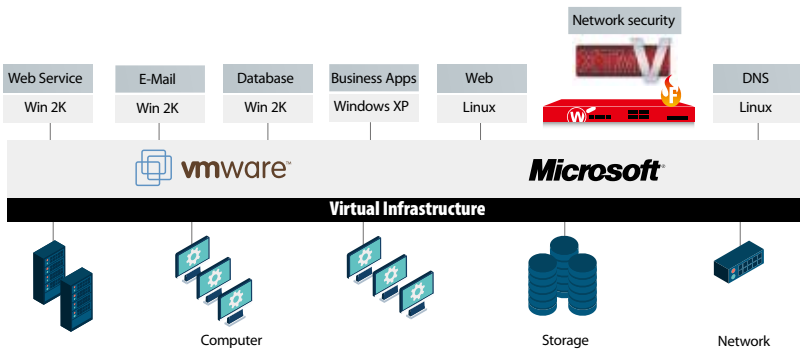


Solution6 仮想環境への導入と効率的な運用

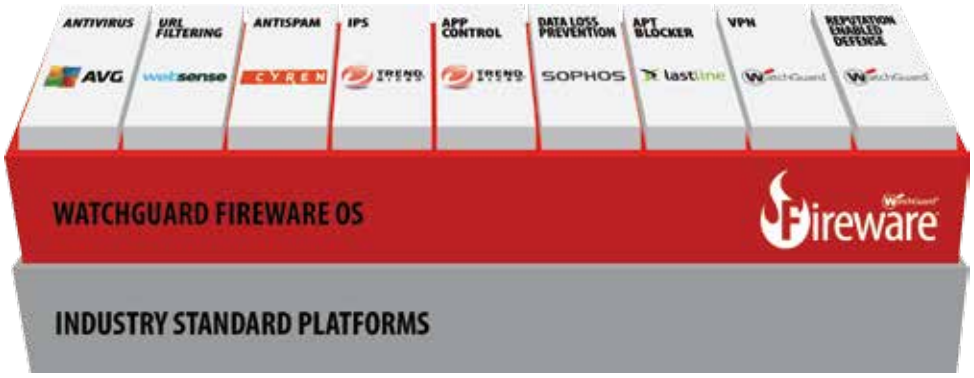
様々な業種・規模の企業が仮想化技術により、ハードウェアや運用コストを削減しています。さらに、物理的な制約、電気容量の削減要求、発熱量の制限などにより、ネットワーク機器やセキュリティアプライアンスにも仮想アプライアンスを利用するケースが増えています。しかし、多くの管理者は運用方法やパフォーマンスの違いを懸念しています。

WatchGuard XTMv(仮想アプライアンス)による仮想環境への対応

- HWアプライアンスと同様に高いセキュリティ機能と共通の管理機能を提供
- 共通のセキュリティ機能や管理機能に加え、柔軟な導入方法により管理者の負荷を軽減
- ホスティング、クラウドなどのサービスプロバイダで、複数のXTMvインスタンスをデータセンターのペリメータで導入



独自 OS に統合されたベストオブブリードのセキュリティ技術



最新の技術を駆使したベストオブブリードのセキュリティ機能群が、ウォッチガードの独自OSであるFirewareで1台のアプライアンスに統合されています。モジュール形式を採用しており、必要に応じて各機能のライセンスを購入することですぐに利用開始できます。

Fireware セキュリティ機能

Gateway AntiVirus
ゲートウェイアンチウイルス

ウイルス、ワーム、トロイの木馬、スパイウェア、アドウェアなどのセキュリティの脅威を最新のシグネチャとヒューリスティックエンジンでブロックします。250万以上の既知のウイルスのほか、シグネチャの自動更新により最新のウイルスにも対応しています。ZIP、RAR、TAR、GZIP、ARC、CABなどの圧縮ファイルのスキャンも実行します。

spamBlocker
迷惑メール対策

有害なスパムメールをリアルタイムでブロックし、ウイルスやマルウェア感染を未然に防ぎます。迷惑メールを一掃することで、日々の業務効率を高め、ネットワークインフラにかかる負荷を軽減します。世界的に広く導入されている検知エンジンを採用し、98%以上の高い検知率で不要メールをブロックすることができます。

WebBlocker
Webフィルタリング

業務に関係のないWebサイトへのアクセスを規制・管理し、生産性を高めるとともに、ウイルス感染や情報漏えいなどを未然に防ぎます。125カテゴリ、5,000万以上のURLに対応しています。ホワイトリスト / ブラックリストでのカスタマイズが可能なほか、ユーザ/グループ/時間などによるポリシー設定も柔軟に行えます。

IPS: Intrusion Prevention Service
不正侵入検知・防御

スパイウェア、SQLインジェクション、クロスサイトスクリプティング、バッファオーバーフローなどのネットワーク攻撃のみならず、15,000以上のシグネチャであらゆる攻撃をブロックします。アップデートを常時行うことで最新の脅威にも対応し、HTTP、HTTPS、FTP、TCP、UDP、DNS、SMTP、POP3など主要プロトコルを全てスキャンします。また、攻撃元として識別されたIPアドレスを自動的にブロックします。

Application Control
アプリケーション制御

ファイアウォールを通過したアプリケーションを制御します。2,500以上のシグネチャにより1,800以上のアプリケーションに対応し、アプリケーション内の機能を個々に制御することもできます(例:メッセンジャーのチャット機能は「オン」のまま、ファイル転送機能を「オフ」にする)。シグネチャを常時アップデートし、最新のアプリケーションとバージョンアップのみならず、先進的な振る舞い分析により、暗号化されたアプリケーションやセキュリティ対策を回避するアプリケーションにも対応します。

Reputation Enabled Defense
レピュテーションセキュリティ(RED)

クラウドベースのWebレピュテーション(評判照合)サービスとして、アンチウイルスエンジンを含む複数のソースから情報を収集し、サイト毎のレピュテーションポイントにより、Webサイトからのリアルタイム保護を実現します。レピュテーションポイントに応じて、トラフィックをクラウド上でブロックまたはバイパスが可能で、ゲートウェイアプライアンスの負担を軽減し、パフォーマンスを最大50%高めることができます。

DLP: Data Loss Prevention
情報漏えい対策※

企業内ネットワークから外部ネットワークへの個人情報や機密情報の漏えいを防止します。外部に送信されようとしているテキスト本文や添付されたドキュメント内をスキャンし、特定のキーワードを含む情報が外部に送信されないように未然にブロックします。

APTBlocker
標的型攻撃対策※

ウイルス対策や不正侵入検知などシグネチャ型のセキュリティ対策で対応が困難な未知のマルウェアを、クラウド上のサンドボックスと連携することで検知 / ブロックします。先進のフルシステムエミュレーションによるサンドボックス技術を活用した詳細な検知プロセスにより、高度な技術を持つ悪質なマルウェアによる攻撃を阻止します。

※個別オプション: Security Bundleには含まれません。別途オプションライセンスとして購入が必要となります。

円滑なビジネスを推進する各種ネットワーク機能

ウォッチガードでは最先端のセキュリティ機能を提供するだけでなく、ネットワークを快適に利用し、ビジネスの安全性と俊敏性を最大化するための各種ネットワーク機能が用意されています。

ネットワーク機能

トランスペアレントモード

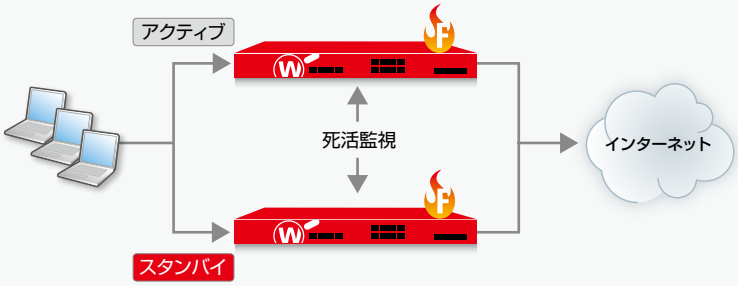
トランスペアレントモードを利用すれば、既存のネットワーク構成に変更を加えることなく、簡単に透過性をもたせることができます。必要な機能だけを容易に適用できるため、新規導入時のセキュリティ構成など、安心してネットワークセキュリティの構築が可能となり、他のネットワークサービスへの影響を考慮した導入プロセス計画を策定することができます。

ロードバランス／トラフィックシェイピング

インターネットの普及に伴い、Webサーバへのアクセス増大と負荷の集中が課題となっています。複数台のサーバで負荷を分散するロードバランス機能により、1台のアプライアンスでルータ機能、ファイアウォール機能、ロードバランス機能が提供できるため、管理面での負荷と導入コストを大幅に軽減することができます。また、優先度の高いトラフィックに対して、ネットワーク帯域を優先的に割り当てるトラフィックシェイピングを適用することにより、さらに詳細なトラフィック管理が可能になります。

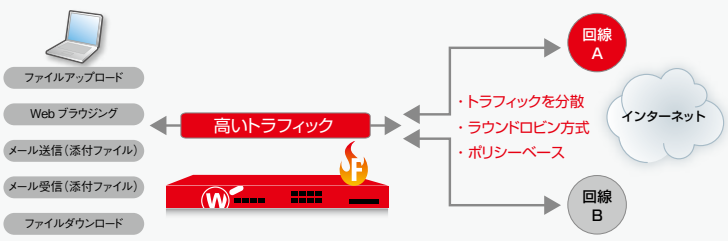
ハイアベイラビリティ（HA構成）

企業の基幹システムやネットワークは24時間365日稼動し続けることが求められています。ウォッチガードのHA構成を導入することで、ダウンタイムを最小化して稼働率を限りなく100%に近づけることができます。万一のハードウェア障害時にもスタンバイ機へ自動的にフェイルオーバすることでダウンタイムを限りなく短くし、業務の継続を維持します。アクティブ／アクティブ構成を採用し、トラフィックの負荷を分散しながら冗長構成による高可用性を提供します。



マルチWAN負荷分散

インターネットの普及によって、業務はよりリアルタイムな活動が求められています。ウォッチガードのマルチWAN負荷分散を導入し、企業のインターネットアクセスを複数の回線に分散することで、より高速で信頼性の高い業務の遂行を実現します。アクセスする回線ごとに重み付けの選択が可能で、高速回線:低速回線=2:1に設定するといったカスタマイズも自由に行えます。また、ポリシーごとに利用回線を振り分けることもできます。



管理ソフトウェア

WatchGuard Dimension™

セキュリティ対策にリアルタイムの可視化ツールで
一歩先のインテリジェンスを実装

役員レベルからネットワーク管理者まで、ビジネスの意思決定にはスピードが要求されます。データを可視化することで、セキュリティ対策への迅速な判断が可能となります。Firebox / XTMに標準で提供されるWatchGuard Dimensionはセキュリティの可視化 / レポートツールを提供し、ネットワークセキュリティの問題の素早い分析と最適なセキュリティポリシーの策定を支援します。

WatchGuard Dimensionによるログ収集とレポート機能

- 複数アプライアンスからのログを集約
- パブリック、プライベートクラウドに対応
- 70種類のレポート形式、エグゼクティブサマリーレポート
- FireWatchおよびThreatMapなどの可視化ツール
- HIPAA、PCIコンプライアンスの特別レポート
- SNMP v2 & v3、Syslog
- 暗号化されたログチャネル
- PDF形式レポートのメール送信

WatchGuard System Manager

ネットワーク、セキュリティ、アプライアンス全ての設定・運用管理を支援する洗練された統合管理ツール

- アプライアンスに直接接続、スクリプトによるコマンドラインインターフェイス
- Webブラウザによる単一デバイスを管理するためのWeb UI
- 対話型でリアルタイムでのモニタリングとロギングを提供する中央コンソール
- ドラッグ&ドロップVPNの設定、豊富な履歴レポートの提供
- RapidDeployによる容易な設定と導入

無線LANアクセスポイント

AP200

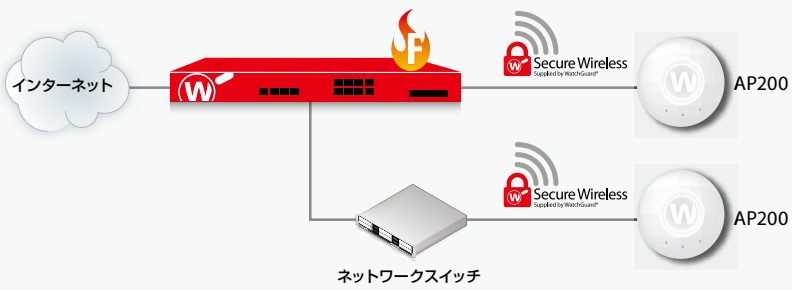
Firebox / XTMと接続し、無線LANアクセスポイントでセキュアな企業内無線環境を構築

Firebox / XTMで提供されるベストオブブリードのセキュリティ機能を無線LANで接続されるデバイスに拡張することで、セキュリティリスクを最小限に抑え、モバイルデバイスによる効率の高いビジネス環境を支援します。有線LAN、無線LANから接続するすべてのユーザに対して一貫したセキュリティポリシーを適用させることが可能となり、すべてのデバイスの設定や監視を1つのコンソールより一元管理する事ができます。

【AP200の主な特長】

- タブレットなどの無線デバイスにも高いセキュリティ機能を提供
- Firebox / XTMのセキュリティ機能を無線トラフィックにも拡張
- Firebox / XTMの管理ツールより一元管理
- 自動的にデバイスを検知し簡単に登録
- シームレスなローミング
- デバイス帯域制御
- 機器ステータス／トラフィック監視
- Radius認証

アプライアンスを
無線LANコントローラとして使用



WatchGuard Network Security Products（小規模オフィス向け）

	Firebox	XTM 2 Series		XTM 3 Series		Firebox M Series
						
モデル	T10/T10-W –	25/25-W XTM 26へ アップグレード可能	26/26-W –	33/33-W –	330 –	M200 –
スループットと接続						
推奨ユーザ数 （プロキシ / FW 利用時）	5 / 10	10 / 20	20 / 30	30 / 40	40 / 75	50 / 75
FW スループット	200 Mbps	240 Mbps	540 Mbps	850 Mbps	1.4 Gbps	3.2 Gbps
VPN スループット	30 Mbps	40 Mbps	60 Mbps	100 Mbps	240 Mbps	1.2 Gbps
AV スループット	70 Mbps	95 Mbps	142 Mbps	175 Mbps	340 Mbps	620 Mbps
IPS スループット	80 Mbps	100 Mbps	226 Mbps	328 Mbps	640 Mbps	1.4 Gbps
UTM スループット	55 Mbps	80 Mbps	108 Mbps	146 Mbps	298 Mbps	515 Mbps
インターフェイス 10/100/1000	3	5	5	5	7	8
I/O インターフェイス	1 Serial / 1 USB	1 Serial / 1 USB	1 Serial / 1 USB	1 Serial / 1 USB	1 Serial / 2 USB	1 Serial / 2 USB
ノード数（LAN IPs）	制限なし	制限なし	制限なし	制限なし	制限なし	制限なし
同時接続（双方向）	7,500	10,000	30,000	40,000	40,000	1,700,000
VLAN サポート	10	50	50	75	75	100
認証ユーザ数	200	500	500	500	500	制限なし
VPNトンネル数						
Branch Office VPN	5	10	40	50	50	50
モバイル VPN IPSec （標準/最大）	5	5/10	5/40	5/55	5/55	75
モバイル VPN SSL / L2TP	5	11	25	55	55	75

すべてのウォッチガードアプライアンスには、以下の機能をご利用いただけます。

（サブスクリプションのライセンス追加により機能が有効になります）

OS機能	
標準	IP address 割り当て：スタティック、DynDNS、PPPoE、DHCP（サーバ、クライアント、リレー） / 独立ポート / VLAN サポート / トランスペアレント/ドロップインモード
拡張ネットワーク [b]	ダイナミックルーティング（BGP、OSPF、RIPv1、2） / ポリシーベースルーティング / ナット：スタティック、ダイナミック、1:1、IPSecトラバーサル、ポリシーベースPAT / トラフィックシェーピング & QoS：8優先キュー、DiffServ、modified strict queuing / バーチャル IP（サーバロードバランス）[a]
可用性 [b]	ハイアベイラビリティ（アクティブ/パッシブ、アクティブ/アクティブクラスタリング）/ VPN フェイルオーバ / マルチWANフェイルオーバ / マルチWANロードバランス / リンクアグリゲーション（802.3ad ダイナミック、スタティック、アクティブ/バックアップ）/ 無線WANフェイルオーバ（ブロードバンド無線ブリッジアクセサリを使用）
無線	
Integrated 無線	Integrated 802.11a/b/g/n、モデル25-W、26-W、33-Wで利用可能
無線アクセスポイント	すべてのモデルがWLANにUTMセキュリティ機能を拡張するためにAP200無線アクセスポイントをサポート / MAC フィルタリングを含む、クライアントレポート、キャプティブポータル技術、802.1X 認証、PCI に準拠したスキャンおよびレポート
無線 WAN	すべてのモデルが携帯接続への無線ブリッジデバイスを拡張するWatchGuard Broadband Extendをサポート / 一部ダイレクトコネクトUSBをサポート
サブスクリプション	
セキュリティサービス	Application Control / Intrusion Prevention Service / WebBlocker / Gateway AntiVirus / APTBlocker / spamBlocker / Reputation Enabled Defense / Data Loss Prevention（ライセンス追加によって機能が有効になります。）
LiveSecurity® サービス	複数年 Multi-year LiveSecurity subscriptions はすべてのモデルで使用可能 / 24/7 support（LiveSecurity Plus）、Gold-level service はXTM330以上のモデルでオプションとして購入可能

[a]サーバの負荷分散は、XTM2シリーズ、XTM3シリーズ、およびFireboxT10のアプライアンスでは使用できません。 [b]クラスタリングを含む一部の機能は、FireboxT10では使用できません。

WatchGuard Network Security Products（中規模オフィス向け）

	Firebox M Series				XTM 5 Series			
		 Firebox M400/M500  Firebox M440						
モデル	**M300** –	**M400** –	**M440** –	**M500** –	**515** XTM 525へアップグレード可能	**525** –	**535** XTM 545へアップグレード可能	**545** –
スループットと接続								
推奨ユーザ数（プロキシ / FW 利用時）	100 / 150	150 / 300	300 / 500	300 / 500	100 / 150	150 / 350	250 / 500	300 / 750
FW スループット	4 Gbps	8 Gbps	6.7 Gbps	8 Gbps	2 Gbps	2.5 Gbps	3 Gbps	3.5 Gbps
VPN スループット	2 Gbps	4.4 Gbps	3.2 Gbps	5.3 Gbps	250 Mbps	350 Mbps	550 Mbps	750 Mbps
AV スループット	1.2 Mbps	2.5 Gbps	2.2 Gbps	3.2 Gbps	1.5 Gbps	1.7 Gbps	1.8 Gbps	2 Gbps
IPS スループット	2.5 Gbps	4 Gbps	2.2 Gbps	5.5 Gbps	1.6 Gbps	2 Gbps	2.4 Gbps	2.8 Gbps
UTM スループット	800 Mbps	1.4 Gbps	1.6 Gbps	1.7 Gbps	850 Mbps	1 Gbps	1.4 Gbps	1.7 Gbps
インターフェイス 10/100/1000	8	8（2SFP含む）*	25 1G copper [b] 2 10G SFP +	8（2SFP含む）*	6 [a]	6 [a]	6 [a]	6 [a]
I/O インターフェイス	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB
ノード数（LAN IPs）	制限なし	制限なし	制限なし	制限なし	制限なし	制限なし	制限なし	制限なし
同時接続（双方向）	3,300,000	3,800,000	4,000,000	9,200,000	40,000	50,000	100,000	350,000
VLAN サポート	200	300	400	500	100	200	300	400
認証ユーザ数	制限なし	制限なし	制限なし	制限なし	500	500	1,000	2,500
VPNトンネル数								
Branch Office VPN	75	100	300	500	65	75	200	600
モバイル VPN IPSec（標準/最大）	100	150	300	500	75/75	100/100	300/300	1,000/1,000
モバイル VPN SSL / L2TP	100	150	300	500	65	75	300	600

AP200 Specifications

設置環境(屋内 / 屋外)	屋内
ラジオ数	2
アンテナ数	4(内蔵)
サポートする周波数帯 (GHz)	2.400-2.4835 GH z • 2.471-2.497 GH z • 5.150-5.250 GHz
DFS(Dynamix Frequency Selection)	○
周波数帯	5GHz / 2.4GHz
Tx/Rx ストリーム	2x2 MIMO(multiple input multiple output)
最大転送速度	600 Mbps
最大送信出力	17 dBm(10mW/Mhz)
SSID	16(2.4GHz x 8、5GHz x 8)
プレミアム規格エンクロージャ	○
セキュリティ	WPA-PSK、WPA2-PSK、WPA2-PSK Mixed、WPA2-、Enterprise 802.1x、TKIP、AES
イーサネット	1GbE
電源	PoE、A/C アダプタ
MTBF値	約 50万 時間
物理セキュリティ	ケンジントンロック
IEEE準拠規格	802.11a/b/g/n、802.11i、802.1x、802.3af/at、802.1Q

XTMモデルとXTMv Editionでサポート可能なアクセスポイント数

XTMモデル	2 Series*1	3 Series*2	5 Series*2	8 Series	800 Series	XTM1050	1500 Series	XTM 2050	XTM 2520
アクセスポイント数	5台	最大15台	最大35台	70台	100台	100台	100台	100台	100台

XTMv（仮想アプライアンス）	Small Office	Medium Office	Large Office	Datacenter
アクセスポイント数	25台	50台	75台	100台

※アクセスポイント数はライセンスで制限されません。 *1 XTM21, 22, 23 モデルはサポート対象外となっています。 *2 モデルによりサポート台数が異なります。WatchGuard System Manager(WSM)及びFireware XTM OSのバージョン11.8は以降のバージョンをご利用下さい。
[a]XTM5シリーズモデルは1つの10/100インターフェイスを有します。 [b]Firebox M440.25ポートのうち、8ポートをPoEポートとして使用可能。詳細はwww.watchguard.com/T10をご覧ください。

WatchGuard Network Security Products（大規模オフィス向け）

	XTM 800 Series			XTM 1500 Series		XTM 2520
						
モデル	**850** 860/870へ アップグレード可能	**860** 870へ アップグレード可能	**870** –	**1520-RP** –	**1525-RP** –	**2520** –
スループットと接続						
推奨ユーザ数 （プロキシ / FW 利用時）	1000 / 1500	1150 / 1750	1300 / 2000	2000 / 2500	2000 / 2500	2500 / 5000
FW スループット	8 Gbps	11 Gbps	14 Gbps	14 Gbps	25 Gbps	35 Gbps
VPN スループット	8 Gbps	8 Gbps	10 Gbps	10 Gbps	10 Gbps	10 Gbps
AV スループット	4 Gbps	5.5 Gbps	7 Gbps	8 Gbps	9 Gbps	9.7 Gbps
IPS スループット	5 Gbps	7 Gbps	9 Gbps	11 Gbps	13 Gbps	15 Gbps
UTM スループット	3 Gbps	4 Gbps	5.7 Gbps	6.7 Gbps	6.7 Gbps	up to 10 Gbps
インターフェイス 10/100/1000	14	14	14 [a]	14	6 and four 10G SFP+[b]	12 and four 10G SFP+[b]
I/O インターフェイス	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB
ノード数（LAN IPs）	制限なし	制限なし	制限なし	制限なし	制限なし	制限なし
同時接続（双方向）	5,000,000	7,000,000	9,000,000	10,000,000	15,000,000	15,000,000
VLAN サポート	750	750	1,000	2,000	3,000	4,000
認証ユーザ数	制限なし	制限なし	制限なし	制限なし	制限なし	制限なし
VPNトンネル数						
Branch Office VPN	5,000	6,000	7,000	10,000	10,000	制限なし
モバイル VPN IPSec （標準/最大）	10,000	12,000	14,000	15,000/15,000	20,000/20,000	制限なし
モバイル VPN SSL / L2TP	10,000	12,000	14,000	15,000	20,000	制限なし

XTMv Editions

ライセンス	Small Office	Medium Office	Large Office	Datacenter
スループットと接続				
推奨ユーザ数 （プロキシ / FW 利用時）	30/60	150/350	1000/1500	2500/5000
FW スループット	1 Gbps	2.5 Gbps	5 Gbps	制限なし
UTM スループット	600 Mbps	900 Mbps	1.3 Gbps	
仮想インターフェイス*1	8-10	8-10	8-10	8-10
ノード数（LAN IPs）	制限なし	制限なし	制限なし	制限なし
同時接続（双方向）	30,000	350,000	1,250,000	2,500,000
VLANサポート	50	75	400	4,000
VPNトンネル数				
Branch Office VPN	50	600	6,000	10,000
モバイルVPN IPSec	5	50	800	制限なし
モバイルVPN SSL（標準/最大）	10/50	100/600	6,000/6,000	制限なし
認証ユーザ数	200	2,500	5,000	制限なし

*1 ネットワークインターフェイスの数は仮想環境に依存します。VMware vSphereは10、Microsoft Hyper-Vは8までのアダプタをサポートします。 [a]ファイバポートは10GBase-SR/SWまたは1000BASE-SXとして動作することができます。[b]XTM870アプライアンスは、モデルナンバーWatchGuard XTM870-Fの下で6つのカッパーと8つのファイバー10/100/1000インターフェイスが付属しています。

セキュリティ仕様

セキュリティ

ファイアウォール機能	ステートフルパケットインスペクション、ディープパケットインスペクション、プロキシファイアウォール
アプリケーションプロキシ	HTTP、HTTPS、SMTP、FTP、DNS、TCP、POP3、TFTP
脅威保護	スパイウェア、DoS攻撃、フラグメンテッドパケット、マルフォームパケット、複合型脅威、標的型攻撃
VoIP	H.323. SIP、コールセットアップ、セッションセキュリティ
セキュリティサービス	WebBlocker、spamBlocker、Gateway AntiVirus、Intrusion Prevention Service、Reputation Enabled Defense、Application Control、DLP(Data Leak Prevention)オプション、APTBlockerオプション
ゲートウェイアンチウイルス	250万以上のウイルス定義ファイル
迷惑メール対策	1バイト文字、2バイト文字、画像ベース、ウイルスアウトブレイクなどに対応
Webフィルタリング	125カテゴリ(5,000万以上のURLを登録済み)、HTTP、HTTPSに対応
IPS	15,000以上の攻撃を検知・防御
アプリケーション制御	1,800アプリケーション、2,500シグネチャに対応

VPNおよび認証

暗号化	DES、3DES、AES 128/192/256ビット
IPSec	SHA-1、MD5、IKE pre-shared key、3rd party cert
VPNフェイルオーバ	あり
SSL	シンクライアント、Webエクスチェンジ
PPTP	サーバおよびパススルー
シングルサインオン	トランスペアレントActive Directory認証
XAUTH	Radius、LDAP、Secure LDAP、Windows Active Directory
その他ユーザ認証	VASCO、RSA SecurID、Webベース、ローカル、Microsoft Terminal Service、Citrix XenApp

管理

リアルタイム監視、レポート	WatchGuard Dimension
管理プラットフォーム	WatchGuard System Manager (WSM)
アラームと通知	SNMP v2/v3、メール、管理システムアラート
サーバサポート	ログ、レポート、検疫、WebBlocker、管理
Web UI	Windows、Mac、Linux、Solaris OSをサポート
コマンドラインインターフェイス	ダイレクトコネクト、スクリプト含む

標準ネットワーク

QoS	8 優先キュー、DiffServ、modified strict queuing
IPアドレスアサインメント	静的、DynDNS、PPPoE、DHCP (サーバ、クライアント、リレー)

サポート&メンテナンス

QoS	8 優先キュー、DiffServ、modified strict queuing
LiveSecurity Service	ハードウェア保証、技術サポート(4時間の対応時間)、ソフトウェアアップデート、脅威アラート

認証・基準

QoS	8 優先キュー、DiffServ、modified strict queuing
セキュリティ	ICSA、FIPS 140-2、EAL 4+
安全	NRTL/C、CB
ネットワーク	IPv6 Ready Gold(ルーティング)
特定有害物質指令	WEEE、RoHS、REACH

ウォッチガード・テクノロジー・ジャパン株式会社
〒106-0041 東京都港区麻布台1-11-9 CR神谷町ビル5階　TEL:03-5797-7205　FAX:03-5797-7207
www.watchguard.co.jp

■ お問い合わせ先

PN201507