



製品の概要

チェック・ポイントの Software Blade アーキテクチャをベースとする Security Gateway Virtual Edition (VE) は、業界最先端のファイアウォールにより、内部と外部双方のセキュリティ脅威から動的な仮想化環境を保護します。

製品の特徴

- 仮想マシン間のトラフィックを検査
- 動的な仮想化環境向けのセキュリティを提供
- 完全に仮想化されたセキュリティ・ゲートウェイ
- 仮想化環境に対応
- プラグ・アンド・プレイで仮想マシン向けのセキュリティを導入
- 物理環境と仮想化環境を統一して管理

主な利点

- Software Blade アーキテクチャにより、物理環境と仮想化環境の両方に包括的なセキュリティを提供
- きめ細やかな設定が可能なファイアウォール・ポリシーと、統合されたクラス最高レベルの侵入防御機能により、仮想マシン間を流れるすべてのトラフィックを検査して仮想マシンを保護
- プラグ・アンド・プレイで導入可能、ネットワーク構成の変更は不要
- 仮想マシンを別のホストに移動するライブ・マイグレーション時や新規仮想マシンの追加時も継続的に保護を提供
- 物理環境と仮想化環境の両方を単一のコンソールから管理できるため、運用管理が容易

Security Gateway Virtual Edition

プライベート/パブリック・クラウド環境に
ワンクリックで仮想化対応セキュリティを導入

課題

サーバ仮想化の急速な普及に伴い、仮想化環境におけるセキュリティ対策の必要性が高まっています。また、外部の脅威という物理環境と同じセキュリティ問題に加えて、仮想化環境固有の問題にも対処する必要があります。例えば、プラットフォーム内の複数の仮想マシン間を流れるトラフィックなど、従来のセキュリティ・ソリューションでは把握できないデータの流れを保護する必要があります。また、インフラストラクチャの拡張やハードウェア障害の際に、仮想マシンを別の物理ホストに移動してオンライン化した場合に、その仮想マシンを自動的に保護するような仕組みも必要となります。

解決策

Software Blade アーキテクチャをベースとする Security Gateway Virtual Edition (VE) は、仮想マシン環境向けの保護機能を 28 万円からという低価格で提供する包括的なセキュリティ・ソリューションです。プラグ・アンド・プレイで容易に導入が可能で、仮想マシンのライブ・マイグレーションを完全にサポートしておりメンテナンスも最少のダウンタイムで行うことができます。また、セキュリティ・ポリシーの自動実施機能を備えているため、新たにオンラインにした仮想マシンも直ちに保護されます。

仮想マシン間のトラフィックを検査

きめ細やかな設定が可能なファイアウォール・ポリシーと、統合されたクラス最高レベルの侵入防御機能により、仮想マシン間を流れるすべてのトラフィックを検査して仮想マシンを保護します。Security Gateway VE は、VMware の VMsafe 技術を活用してハイパーバイザ内でシームレスなセキュリティを実現します。

Security Gateway VE では、外部の脅威から仮想アプリケーションを保護すると共に、各仮想アプリケーションを相互に隔離することもできます。侵入防御技術 (IPS) も統合されており、シグネチャとプロトコル・アノーマリ (プロトコル異常) に基づいて侵入を検知・防御し、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、チェック・ポイントのアップデート・サービスが提供するリアルタイムのアップデートにより、防御機能を常に最新の状態に保つことが可能です。



動的な仮想化環境向けのセキュリティを提供

Security Gateway VEは、仮想マシンを別のホストに移動するライブ・マイグレーションの際も仮想マシンを継続的に保護し、また新たに追加された仮想マシンも自動的に保護します。VMware VMotionとDynamic Resource Scheduler (DRS) を完全にサポートしており、オープン接続を維持しながらセキュリティ・ポリシーを実施することが可能です。メンテナンスや動的なリソース割り当てのために仮想マシンを別のホストに移動する際も、ダウンタイムは発生しません。

また、極めて容易に作成できる仮想マシンは、無秩序に増加しがちですが、Security Gateway VEでは、セキュリティ・ポリシーを自動的に実施して、新たに追加された仮想マシンを既存の仮想マシンから隔離できるため、このような懸念は解消されます。

完全に仮想化されたセキュリティ・ゲートウェイ

Security Gateway VEは、Software Bladeアーキテクチャをベースとする包括的なセキュリティを提供し、仮想マシン間のトラフィックと物理的なネットワークおよびシステムの両方を保護します。ハイパーバイザ・レイヤのシームレスなセキュリティを提供するだけでなく、レイヤ2またはレイヤ3の一般的なゲートウェイとして導入できる柔軟性を備えています。

Security Gateway VEは、実績あるセキュリティ機能を単一のソリューションに統合することでセキュリティ環境を簡素化し、導入および管理の効率化を実現します。各仮想マシンは、ファイアウォール、IPS、VPN、アンチウイルス、アンチスパム、URLフィルタリング、Webセキュリティというクラス最高レベルのセキュリティ機能により、外部の脅威から保護され、別の仮想マシンからも隔離されます。またSecurity Gateway VEでは、物理的なセキュリティ・アプライアンスを導入することなく、隔離されたアプリケーションおよび情報を別のアプリケーションから保護できるため、サーバとデータの分離が求められる法令遵守要件にも対応できます。

プラグ・アンド・プレイで仮想マシン向けのセキュリティを導入

仮想マシンやVLAN、仮想スイッチのネットワーク・トポロジ設定を変更することなく、自動的に仮想マシンにセキュリティを適用できるため、管理作業の負担が軽減されます。

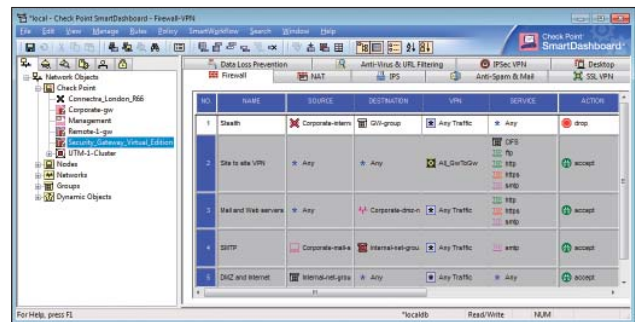
仮想化環境に対応

統合や最適化、投資対効果の向上を目的に、仮想化技術の普及が進んでいますが、従来の物理的なセキュリティ・アプライアンスを使用して仮想マシン間のトラフィックを検査する場合、通常はパフォーマンスの低下やネットワーク・トポロジの複雑化を引き起こします。しかし、Security Gateway VEは仮想システム内で仮想マシンのトラフィックを検査するため、ネットワーク・トポロジに変更を加える必要がなく、パフォーマンスも低下しません。

物理環境と仮想化環境を統一して管理

物理環境と仮想化環境は統一して管理できるため、セキュリティ管理の簡素化が実現されます。また、仮想化環境管理者とセキュリティ管理者の作業は明確に分離することができます。

Security Gateway VEは、チェック・ポイントの他の物理的なセキュリティ・ゲートウェイおよびアプライアンスと同様、Security ManagementまたはMulti-Domain Management (MDM)を使用して管理できます。このため、単一の管理コンソールを使用してすべてのゲートウェイで一貫性のあるセキュリティを提供し、管理コンソールに関するコストも最小限に抑えることができます。



チェック・ポイントのSmartDashboard：物理ゲートウェイと仮想ゲートウェイを統一して管理

仮想インフラストラクチャ向けに最適化されたトラフィックのロギング、レポート、包括的な監査の各機能が用意されているため、効率的に法令遵守を実現することができます。これらの機能では、各種の規制および標準規格 (PCI、SOX、HIPAA、COBIT、ISO 17799) の要件に対応した専用のレポートが提供されます。

Security ManagementとMDMは、仮想マシンに導入することもできます。



仕様

機能	詳細
サポートされるVMwareサーバ	VMware vSphere
サポートされるチェック・ポイントのソリューション	<ul style="list-style-type: none"> ● Security Gateway Software Blade R71+ ● Security Management R71+
仮想アプライアンスの最小要件	<ul style="list-style-type: none"> ● 割り当てメモリ:512MB (2.5GBを推奨) ● ディスク容量:12GB

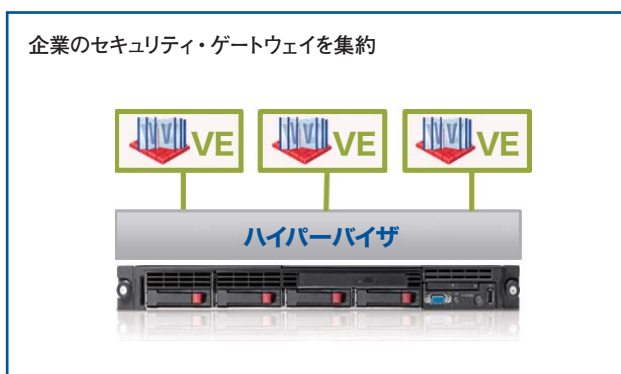
Security Gateway VEの導入シナリオ



きめ細やかなファイアウォールおよびIPSポリシーを
仮想マシン間のトラフィックに適用



ファイアウォールやIPS、VPN、その他のSoftware Bladeを
搭載したSecurity Gateway VEを使用して、
オフィスのコンピュータ/ネットワークおよび資産を保護



セキュリティ・ゲートウェイを仮想化環境に統合



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 800100-J 2010.11 ※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。