



SSL Network Extender

Webベースのセキュアなネットワーク・レベルでの接続

課題

多くの企業において、Eメール、ERPソフトウェアをはじめとするネットワーク・アプリケーションが日常的に利用されています。

また、モバイル環境のより一層の普及により、さまざまな場所やネットワーク環境からこれらのアプリケーションにアクセスする必要性が高まっています。今、多くの企業はこれらのアプリケーションやネットワークをあらゆる環境から活用するために、柔軟度の高いリモート・アクセス・アプリケーションを、最低限の労力で導入および運用する方法を模索しています。リモート・アクセスの際に求められる最も重要な点は、あらゆるタイプのアクセスに対応できる堅固なセキュリティ・ソリューションです。

解決策

SSL Network Extender™は、Web環境に対応していないネットワーク・アプリケーションによる接続性をWebベースで可能にする、シンプルな形態のリモート・アクセスを実現します。社員やビジネス・パートナーは、チェック・ポイントのSSL Network ExtenderのWebブラウザのプラグインを利用することで、SSL VPNを用いてコーポレート・ネットワークに容易で安全に接続することを可能にします。SSL Network Extenderは、Check Point VPN-1®のコンポーネントとして統合でき、チェック・ポイント製品のすべてのネットワーク保護機能により、SSL VPN接続のセキュリティを確保します。

SSL VPN 上でのネットワーク・レベルの接続性

SSL Network Extenderは、オンライン・バンキングやe-コマースにおける通信保護に利用されているものと同じSSLプロトコルを使用することで、ネットワーク・レベルの完全な接続を実現します。

リモート・ユーザは、Webブラウザを用いてVPN-1ゲートウェイからプラグインをダウンロードすると、ネットワークにアクセス可能となります。SSL Network Extenderは、Web上でアプリケーション・トラフィックを透過的に通過させ、ユーザがリモート環境から接続先のアプリケーションを実行することを可能にします。

エンドポイント・セキュリティの統合

SSL Network Extenderは、業界で最も高い信頼性を誇るCheck Point Integrity™のクライアント・バージョンと統合することにより、社員、ビジネス・パートナー、顧客、またはその他のネットワークの一時利用者が使用あるいは所有しているリモートPCから安全にネットワーク・リソースを利用できるようになります。SSL Network Extenderは、ネットワークへのSSL VPN接続のセキュリティ・ポリシーを実施し、セッションの機密性を確保するので、組織のセキュリティを維持できます。

リモート接続を行う前にスパイウェアをスキャン

悪意のあるプロセス、キーストローク・ロガー、トロイの木馬がリモート・エンドポイントにインストールされないようにするために、VPN-1は、SSL Network Extenderの接続を許可する前に、これらのプログラムやスパイウェアの有無をスキャンします。VPN-1は、SSL VPNのアクセスを許可する前の段階でスパイウェアを無効にし、あらかじめ管理者が定義したセキュリティ要件を実施することで、IDやパスワードの盗用、データの消失を防止します。



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®対応SSL Network Extender™は、Web経由でのSSL VPNリモート・アクセスを実現し、社員やビジネス・パートナーが容易に企業のリソースにアクセスできるようにします。また、スパイウェアの無効化、セッションの機密性の確保、およびネットワーク・アクセス・ポリシーの実施を行います。

製品の特徴

- SSL VPN上でのネットワーク・レベルの接続
- エンドポイント・セキュリティの統合
- あらゆるIPベースのアプリケーションをサポート
- Check Point VPN-1製品と緊密な統合

製品の利点

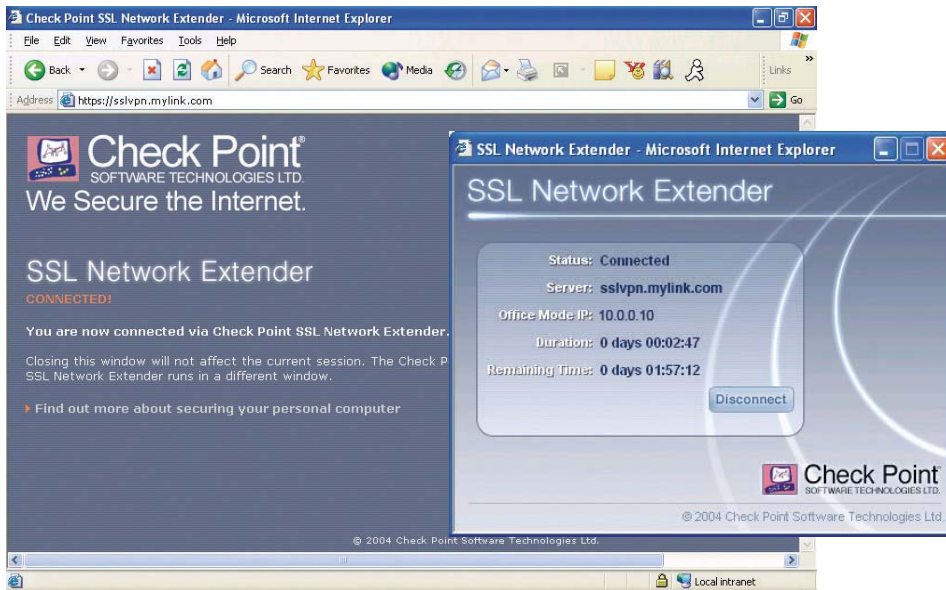
- リモート・アクセスを簡単に導入し、管理コストを削減
- 企業環境で使用されるアプリケーションを幅広くサポート
- 統合されたエンドポイントおよびアプリケーション・セキュリティを兼ね備えたセキュアなリモート・アクセスの実現

NGXのハイライト

- SSL VPNおよびIPSec VPNの統合
- エンドポイント・セキュリティの統合



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。



SSL Network Extenderは標準的なWebブラウザによりダウンロードし実行されます。

管理対象外の環境におけるセキュアなアクセスの実現

VPN-1は、セキュアWebブラウザを提供することにより、空港内など公共の場所に設置されたインターネット・キオスクのPCなど、ネットワーク管理者による直接的な管理を行えない環境のPC等によるセキュアなアクセスを実現します。ユーザは、SSL Network Extenderで社内ネットワーク環境のWebサイトを安全に閲覧すると同時に、データのセキュリティも確保することができます。セキュアWebブラウザでは、Eメール、添付ファイル、Cookie、パスワードなどのWebセッション・ファイルをリモート・エンドポイントで暗号化することによりデータの安全性を維持します。このため、セッションが終了し、ユーザがPCから離れた後でも、企業の重要な情報の表示や窃取を防止できます。

IPベースのアプリケーションをすべてサポート

SSL Network Extenderを使用することで、IP上で動作するあらゆるアプリケーションを利用することが可能となり、ユーザはあたかもネットワーク内部にいるかのように、任意のIPベースのアプリケーションを利用することができます。SSL Network Extenderは、ICMP、TCP、UDPに加えFTPのような動的なアプリケーションもサポートしています。また、内部IPアドレスを使用するオフィス・モード、スプリット・トンネル、および全トラフィックをトンネルするRoute-All-Trafficモードもサポートしており、さまざまネットワーク環境に柔軟に対応することが可能です。

IPSecおよびSSL VPNソリューションの統合

SSL Network ExtenderはVPN-1と統合されているので、企業は、IPSecおよびSSL VPNリモート・アクセス両方のVPN技術を1つの統合ソリューションとして利用できるようになります。既にVPN-1を利用している環境でSSLを新たに利用開始する場合、あるいは、SSLとIPSecが混在する環境

VPN-1と緊密な統合

SSL Network Extenderを含むすべてのチェック・ポイントが提供するセキュリティ・コンポーネントは、チェック・ポイントが特許を持つステートフル・インスペクション、アプリケーション・インテリジェンスおよびSmartDefense技術により確実に保護されます。SSL Network Extenderは、容易なSSLベースのアクセスと、チェック・ポイント製品が提供するセキュリティ保護機能を統合します。

を新たに構築する場合、いずれの場合でも、これら2種類のソリューションを1つの管理システムから統合管理できるシステムの構築が可能で、リモート・アクセスに関わるコスト削減だけでなく、管理統合による管理コストの削減も実現します。

仕様	
サポートしているアプリケーション	Citrix、FTP、IMAP、POP、rlogin、SMTP、Telnet、TFTP、TN3270、VoIPなど、すべてのIPベースのアプリケーション
認証	LDAP、OPSEC™、RADIUS、SecureID、TACACS、X.509証明書
接続性の機能	オフィス・モード (内部IPアドレスを割り当て) DNS、WINSサーバでの通過
サポートしているWebブラウザの暗号化	3DES、RC4
サポートしているWebブラウザ	Internet Explorer 5.0以降のバージョン (管理者権限が必要)、Integrity Secure Browser
インストール	WebブラウザによりActiveXをダウンロード、Microsoft SMS用MSIパッケージ
サポートしているゲートウェイ	HFA-10以降のバージョンを備えたVPN-1 NGX R60、VPN-1 R55
サポートしているエンドポイント	Windows 2000/XP

その他の製品

SSL Network Extenderは、Check Point Connectra™にも含まれています。

©2005 Check Point Software Technologies Ltd. All rights reserved.
 Check Point, Application Intelligence, Check Point Express, Check Pointのロゴ, 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, NGX, 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 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、サービス・マーク又は登録商標です。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、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 501859-J 2005.10 ※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。