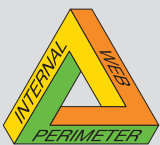


IPSecとSSL VPN導入における考慮事項

本書の内容

- 1 はじめに
- 2 IPSec VPN
- 3 SSL VPN
- 4 IPSec VPNとSSL VPNの比較
- 5 リモート・アクセスのシナリオ



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

はじめに

ここ数年、組織がますます地理的に分散され、モバイル・ワーカーが増えるに従って、リモート・アクセスの接続性を得るためにインターネットや暗号化技術を利用する傾向が飛躍的に高まっています。インターネットを利用したリモート・アクセスには、IPSec VPNとSSL VPNという2つのソリューションが出現しています。そのいずれを選択するかは組織ごとの必要条件によりますが、展開によっては、SSLを使用したネットワーク・レベルのアクセスはIPSecと部分的に重複しているため、多くの場合両方が展開可能です。

本質的に、リモート・アクセスはリモート・エンドポイントからの接続をサポートする必要があります。通常このようなエンドポイントはエンド・ユーザのコンピュータで、ノートPCやデスクトップPCが一般的ですが、個人用携帯型情報端末(PDA)や、キオスクからのちょっとしたアクセス、その他ハードウェア・デバイスの場合などもあります。将来的には、おそらく携帯電話やアプリケーション固有デバイス(レンタカーのチェックインに使用する手持ち式コンピュータなど)といったコンポーネントがリモート・アクセス・クライアントとして使用されることになります。アクセスに使用されるデバイスはますます多様化し、それが新しいリモート・アクセス技術の発達に大きな役割を果たしています。

当然ながら、リモート・アクセス・ユーザのほとんどは、組織のセキュリティ境界の外にあるエンドポイントから、内部のコンピューティング・リソースにアクセスする人です。このようなエンドポイントは、組織に侵入するためのバックドアを求めている攻撃者のターゲットになることがあります(リモート・アクセス・クライアントは組織へのルータとして悪用されかねません)。そのため、リモート・アクセス・エンドポイント自体にセキュリティが導入されています。このようなソリューションには、インストール済みファイアウォールのチェック、アンチウィルス、スパイウェア・チェック、構成のチェックなどがあります。エンドポイント・セキュリティ・チェックを使用すると、エンドポイントの信頼レベルに基づいてアクセスを許可、拒否、制限することができます。

エンドポイント・セキュリティに関連して、VPNゲートウェイにおけるアクセス制御やセキュリティ保護があります。暗号化技術によって堅固なデータ秘匿性とデータ整合性を得ることはできますが、アクセス権を制御することはできません。IPSecでもSSLでも、ユーザがVPNトンネルを確立できるからといって、すべてのリソースにアクセスできてよいとはかぎりません。リモート・アクセス・ソリューションは、必要なリソース以外へのアクセスを管理者が制限可能であることが必要とされます。また、アクセスの起点となるエンドポイントが多様化してきているため、ネットワーク・レベルおよびアプリケーション・レベルの能動的な攻撃防御が実現できれば、安全性の不確かなエンドポイントからの内部サーバに対するセキュリティ・リスクが最小限に抑えられます。

本書では、各組織がそれぞれのニーズに最も適合する技術の選択を支援する背景となる情報、各技術に関連する考慮事項、展開シナリオについて説明します。

技術の基本概要

リモート・アクセスを実現する技術としては、IPSec VPNとSSL VPN(「クライアントレス」VPNとも呼びます)の2つが一般的です。

IPSec VPN

IPSec(IPセキュリティ)VPN展開の典型的な形態は、背後のサーバのVPN終端となる1つ以上のVPNゲートウェイと各リモート・アクセス・ユーザのコンピュータにインストールされるVPNクライアント・ソフトウェアから構成されます。VPNクライアントは、ソリューションによって手動または自動で、どのパケットを暗号化するか、VPNトンネル構築にどのゲートウェイを使用するかを定義します。サイト間VPNでは、ベンダ間の相互運用性が実現されています。IPSecはリモート・アクセスVPNでの使用にも対応していますが、相互運用性についてはサイト間VPNほど優れていません。これは、リモート・アクセスのシナリオへの対応を向上させるため、IPSecには数多くの拡張がなされているからです(NATトラバースなど)。



Intelligent Security



We Secure the Internet.

IPSecは、世界中で多数のベンダがクライアント、サーバ、ゲートウェイといった複数のモードでソリューションを提供している、成熟した標準技術です。IPSecは強力な暗号化とデータ整合性の仕組みをサポートしています。IPSecはネットワーク層のVPN技術で、それを使用するアプリケーションの種類に関わらず機能します。IPSecでは元のIPデータ・パケットが自身のパケットでカプセル化され、すべてのアプリケーション・プロトコル情報が隠されます。IPSecトンネルのネゴシエーションが完了すると、VPNゲートウェイ背後にある複数の異なったサーバに向けられた複数の接続とアプリケーション・タイプ (Web、電子メール、ファイル転送、VoIP) がトンネルを通じて伝送可能になります。

リモート・アクセスの基本要件

長所

- すべてのIPタイプとサービスに対応 (ICMP、VoIP、SQL*Net、Citrix ICAなど)
- クライアントーサイト、サイト間、クライアント間でも同じ技術ベースが有効
- IPSecクライアントでは他のセキュリティ機能 (パーソナル・ファイアウォール、設定検証など) の組み込みが可能
- VPNゲートウェイは通常ファイアウォール機能と統合され、アクセス制御、コンテンツ検査、攻撃防御、その他のセキュリティ機能が実現

短所

- 通常はクライアント・ソフトウェアのインストールが必要。全てのOSがサポートされているわけではない
- ファイアウォールその他クライアントとゲートウェイの間にあるデバイス (ファイアウォールやNATデバイス) によって接続性が妨げられる場合がある
- ベンダの異なるIPSecクライアントとIPSecサーバ/ゲートウェイの相互運用が通常困難

SSL VPN

SSLは、オンライン・バンキングや電子商取引などのトランザクションの機密性とセキュリティを確保するために今日一般的に使用されている安全な伝送プロトコルです (リンクは<https://www.example.com>などのようにHTTPSで始まります)。ほとんどのWebブラウザがSSLに対応しており、ブラウザがSSL VPNの「クライアント」として使用されるため、「クライアントレス」とも呼ばれています。これは、ベンダのIPSecクライアント機能が各リモート・アクセス・ユーザのコンピュータにインストールされている必要のあるIPSecリモート・アクセスのシナリオと対照的です。SSL VPNとは通常SSL VPNゲートウェイを通じたりリモート・アクセスを指しますが、電子メール・クライアント (例: Microsoft OutlookやEudora) などのSSL対応アプリケーションも含まれます。

SSLはTCPを使用して機能するプロトコルです。IPSecと同様、ネゴシエーションといくつかのパラメータの検証を行う最初の設定フェーズの後に接続が確立できます。

- デジタル証明書を使用し、サーバをクライアントに対して認証する
- 証明書その他の方法で、クライアントをサーバに対して認証する (任意)
- セッション・キーが安全に生成され、これを使用してデータの暗号化と整合性チェックが行われる



Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

SSLでは、さまざまな公開鍵アルゴリズム (RSA、DSAなど)、対称鍵アルゴリズム (DES、3DES、RC4)、データ整合性アルゴリズム (MD5、SHA-1) が使用できます。

SSLリモート・アクセスは2つの方法で展開できます。1つは、SSLソフトウェアを使用して各サーバを個々のリモート・アクセス・ユーザの終端にする方法です。もう1つは、SSL VPNゲートウェイが提供するリモート・ユーザ用SSLインタフェース間で暗号化し、SSL VPNゲートウェイと内部サーバ間では暗号化されていない本来のフォーマットで通信する方法です。

SSL VPNブラウザ・プラグイン

最近では、インストール済みのリモート・アクセス・ソフトウェアでなくブラウザ・プラグインを使用してリモート・エンドポイントからクライアント/サーバ・アプリケーションへのトンネルを構築できるSSL VPNのソリューションが出現してきました。ユーザはWebポータル (通常はSSL VPNゲートウェイ) に対して認証を行い、小さなプラグイン (ActiveXやJavaエージェントなど) をダウンロードします。このようなプラグインはユーザに対して透過的で、SSLを使用してクライアント/サーバ・トラフィックをトンネルします。ただし、これらのプラグインは対応アプリケーションがまちまちです。TCPトラフィックに限定して対応しているものもあり、多くはFTPやVoIPなどの動的アプリケーションに対応していません。

長所

- SSLはInternet Explorer、Netscape Communicator、Mozillaなどすべての主要Webブラウザに標準装備
- メール・クライアント/サーバ (例:OutlookやEudora) などの一般的アプリケーションはSSLに対応
- NAT、プロキシ、ほとんどのファイアウォールに対して透過的に機能 (ほとんどのファイアウォールはSSLトラフィックを許可)
- Webプラグインにより、クライアント/サーバ・アプリケーションについてSSLを使用したネットワーク・レベルの接続性が得られる場合あり

短所

- TCPサービスのみをサポートし、SSLを介してはHTTPまたはPOP3/IMAP/SMTPしかサポートしないことが多い
- 通常、SSLにはIPSecよりも多くのゲートウェイの処理リソースが必要
- 「クライアントレス」のシナリオでは、標準でインストールされているソフトウェアはない。セキュリティ・ソフトウェアをエンドポイントまで拡張する能力には制限がある (パーソナル・ファイアウォール、整合性チェックなど)
- ファイアウォールでセッションを終端しない場合——組織のファイアウォールに穴をあける必要があるため、ファイアウォールでHTTPS接続内のデータのコンテンツ検査ができない
- Webプラグインは対応アプリケーションが限られているか、実行するためにPCの管理者権限が必要な場合がある
- サイト間VPNには使用されない。通常はIPSecが使用されるため、リモート・アクセスVPNとサイト間VPNには異なる技術を使用する必要がある

IPSEC VPNとSSL VPNの比較

利用する技術の最良の選択は、リモート・アクセス・プロジェクトの必要条件と目的によって異なります。技術が選択された場合、次のステップは、その技術をベースにしたソリューションを提供しているベンダの中でどれが必要条件にもっともよく合致しているかを判断します。性能、管理性、購入/導入コスト、既存インフラストラクチャとの組み合わせやすさ、サポートなどの基準を考慮してベンダを選定します。



Intelligent Security



We Secure the Internet.

	IPSec VPN	SSL VPN
アプリケーション対応	すべてのIPアプリケーション (Webアプリケーション、エンタープライズ、電子メール、VoIP、マルチメディア)	主としてWebアプリケーション
必要なソフトウェア	IPSecクライアント・ソフトウェア	標準Webブラウザ
情報の露出	指定された人/コンピュータのみにアクセスを許可	どこからでもアクセス可能 (インターネット・キオスクなど)。情報は、故意かどうかに関わらず、あとに残される可能性あり
クライアント・セキュリティのレベル	中～高レベル (使用するクライアント・ソフトウェアによる)	低～中レベル (専用ソフトウェアを使用すると中レベルのセキュリティが得られる——ただし、クライアントレスではなくなる)
スケーラビリティ	何万もの導入実績が、高いスケーラビリティを実証	スケーラビリティは高く、導入しやすい
認証方式	複数の認証方式に対応。一部のベンダが組み込みPKIを提供	複数の認証方式に対応。強力な認証を使用するには余分のコストが必要で、アクセス・デバイスが制限される
セキュリティ考察	セキュリティ・インフラストラクチャをリモート・アクセスに拡張。統合セキュリティ (パーソナル・ファイアウォールなど) によりエンドポイント・セキュリティ機能を拡張	情報アクセスとクライアント環境の管理性が制限される。それほど機密性の高くない情報へのアクセスに適する
最適な用途	安全な社員アクセス、サイト間アクセス	外部Web顧客アクセス

上記のIPSecとSSLの長所と短所の考察から、一般的に以下のようなことが言えます。

- プロジェクトの主要条件として以下のいずれかが当てはまる場合は、IPSecが最適なソリューションであることが多いでしょう。
 - 組織が、Webや電子メールのアクセスだけでなく幅広いネットワーク・プロトコルに対応する全般的インフラストラクチャを必要としている場合
 - 組織がリモート・アクセス・ユーザのコンピュータに対して管理権限を持つ場合
 - リモート・アクセス・ユーザのコンピュータに対してセキュリティ制御 (パーソナル・ファイアウォールの必要性など) が必要な場合。たとえば、公共のインターネット・キオスクなどのインターネット・アクセス機器はセキュリティの状態が不明なために、管理者がこのような機器からの機密データへのアクセスを許可したくない場合などが考えられます。



Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

- プロジェクトの主要条件として以下のいずれかが当てはまる場合は、SSLが最適なソリューションであることが多いでしょう。
 - リモート・ユーザがアクセスを必要とするのが、主にWebベースのアプリケーションや電子メールである場合
 - 情報への多様なアクセス（ノートPC、ホームPC、インターネット・キオスクなど任意のインターネット・デバイスからのアクセス）が必要な場合
 - ファイアウォールやISPによりIPSec接続はできない（IPSecのIKEネゴシエーションが許可されない）が、SSLは許可されている場合
 - 組織がリモート・アクセス・ユーザのコンピュータ設定の管理権限を持たない場合
 - リモート・アクセスに必要なソフトウェアをユーザのコンピュータにインストールできない場合

リモート・アクセスのシナリオ

リモート・アクセスの必要条件は組織によって異なりますが、IPSecとSSLのいずれを導入するかを判断するために役立つ、リモート・アクセス・ユーザのカテゴリがいくつかあります。

以下のシナリオは、組織に適切な技術を選択する際の支援となるものです。大まかな傾向として2つが挙げられます。まず管理下に置かれた社員のPCから公共のインターネット・キオスクなどへとエンドポイントが多様化するに従って、最適シナリオがIPSecからSSLになることが多くなります。2つ目は、シナリオが純粋なクライアント／サーバ・アプリケーションから純粋なWebアプリケーションに向かうに従って、最適シナリオがIPSecからSSLになっていくということです。

また、SSLとIPSecの両方を導入するのが最適であるようなシナリオもあるということも重要な点です。

使用頻度の高いリモート・ユーザ：たとえば、システム・アドミニストレータやシステム・エンジニアなどです。このようなユーザは、通常IPSecユーザです。IPSecが適していることを示す考慮事項として重要なものは2つあります。1つは、ユーザがおそらく仕事の一環として特定の非Webアプリケーションを使用しているという点です。もう1つは、たいいていの場合組織がクライアント環境を所有、管理しているという点です。

使用頻度の低いリモート・ユーザ：ホームPCからネットワークにアクセスしているデイ・エクステンダなどがその例です。このようなユーザにはSSL VPNが適しています。ホームPCは部分的に管理された環境で公共的に誰もが使用できるわけではなく、組織でなく社員が管理しています。リモートPCには、ファイアウォールやアンチウィルスなどのセキュリティ・ソフトウェアがある場合もない場合もあります。組織では、このようなユーザからのアクセスをどの程度許可するかを検討する必要があります。たとえば、パーソナル・ファイアウォールのあるPCからの要求の場合はアクセスを多く許可し、パーソナル・ファイアウォールのないPCからのアクセスは制限する、といったことが考えられます。SSL VPNのベンダはさまざまなセキュリティ手段をSSL VPN製品に使用しているため、この判断においては、特定のSSL VPNソリューションが備えているセキュリティの程度も考慮します。

モバイル社員：たとえば、販売の担当者やマネージャなどです。技術の選択肢としてはIPSecかSSL、またはその両方があります。組織が所有するノートPCを使用しているモバイル・ワーカーの場合は、IPSecが適しています。これは、環境が管理下にあることと、パーソナル・ファイアウォールなどのセキュリティ・ソフトウェアが装備されているIPSecクライアントが多いことによるものです。ただし、SSLを付加的なアクセス技術として考慮に入れても良い場合もあります。たとえば、多くのモバイル社員はホテルのビジネス・センタのPCやインターネット・キオスクなど公共のコンピュータを使用できます。このように管理下でない環境では、SSLが電子メールやイントラネットWebアクセスに適していますが、管理されていないPCにクライアント・ソフトウェアをインストールすることはできないので、クライアント／サーバ・アプリケーションは使用できません。



Intelligent Security

Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

オンサイト・ワーカー: たとえば、コンサルタントや契約業者などのようなユーザです。このような場合、SSL VPNのほうが適していると考えられます。オンサイト・ワーカーは自分のPCを使用して作業することが多いのですが、ネットワークへのアクセスも必要とします。社員のPCにクライアント・ソフトウェアをインストールしなくても安全に情報にアクセスできるようにするには、SSL VPNがよい手段となります。

エクストラネット・パートナー: たとえば、情報の共有のためにWebポータルにアクセスしたり、Webアプリケーションにアクセスしたりするパートナーです。パートナー・エクストラネット・リモート・アクセスには、SSL VPNが適しています。これは、パートナーが組織の管理下でないPCから情報にアクセスするためです。SSL VPN製品により、パートナーの情報を集約するのに便利なユーザWebポータルが実現します。またこのソリューションには、エクストラネット・リソースのために別のエクストラネット・ネットワークを構築する必要がなくなるという付加的メリットもあります。ただし、クライアント/サーバ・アプリケーションへのアクセスが必要な組織では、IPSecのほうがよいソリューションとなるでしょう。これは、エクストラネット環境にはソフトウェアのインストールが必要であり、クライアント・ソフトウェアの

チェック・ポイントのIPSecとSSLのソリューション

IPSec VPN	IPSec VPNとSSL VPN	SSL VPN
VPN-1とSecureRemote またはSecureClient	VPN-1とSSL Network Extender	Connectra Web Security Gateway (SSL Network Extenderを含む)

VPN-1

チェック・ポイントは、リモート・アクセス、イントラネット、エクストラネットのVPNに対して最も広範な製品と技術を提供しています。VPN-1®/FireWall-1®セキュリティ・ゲートウェイは、クリティカルなネットワーク・リソースを不正アクセスから保護するとともに、インターネットを利用したビジネス通信の秘匿性を確保します。ネットワークの規模や複雑さを考慮し、最適なゲートウェイ製品をご選択ください。

- VPN-1 Pro™は、大規模で複雑なネットワーク向けの包括的セキュリティ・ソリューションです。
- VPN-1 Expressは、社員数500人程度までの複数サイトのある企業に適した高信頼性セキュリティ製品です。
- VPN-1 Edge™でリモート・サイトや大規模VPN配備のための安全な接続性が得られます。

VPN-1には以下のIPSecとSSLのソリューションが使用できます。

VPN-1 SecuRemote™は、強力で柔軟性のある認証とクライアント側の簡単な設定を含む基本的なIPSec機能を提供します。

VPN-1 SecureClient™はVPN-1 SecuRemoteの強化製品で、集中管理ポリシーによるパーソナル・ファイアウォール、クライアント・セキュリティ保証、IP圧縮、自動インバンド・ソフトウェア・アップデートなど、高度なリモート・アクセス技術を提供します。また仮想アドレスをリモート・アクセス・クライアントに割り当てるOfficeModeも備えており、これで既知のすべてのNAT問題が解消され（この点ではUDPカプセル化も役立ちます）、ユーザが内部LAN上で利用しているように見せることができます。

SSL Network Extender™は、Webを通じた安全なネットワーク・レベルのアクセスを可能にします。リモート・ユーザはWebブラウザを使用してVPN-1にクライアント/サーバ型アプリケーションを接続することができます。



Intelligent Security



We Secure the Internet.

Connectra

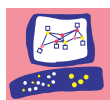
Check Point Connectra™は、統一されたセキュリティ・ソリューションとして、SSL VPNとWebセキュリティが統合された完全なWebセキュリティ・ゲートウェイです。Connectraでは接続性とセキュリティが単一プラットフォームに統合され、業界最高のセキュリティ・ソリューションが提供する安心感とともにSSL VPNを安全に展開することができます。SSL VPNとCheck PointのApplication Intelligence™、Web Intelligence™、Security Management Architecture (SMART) との組み合わせを実現するConnectraは、比類ないセキュリティを備えたWeb接続性を提供します。

SSL Network Extender

Check Point SSL Network Extenderは、ネットワーク・アプリケーションへのリモート・アクセスを必要とするビジネス・パートナーや社員のための、Webを通じた安全なネットワーク・レベルのアクセスを可能にします。SSL Network Extenderは数種のチェック・ポイントのセキュリティ製品に使用でき、リモート・ユーザがインターネットWebブラウザを使用してクライアント/サーバ・アプリケーションに接続可能とします。このWeb使用のネットワーク・レベルの接続性はチェック・ポイント製品への統合コンポーネントとして、単一管理インフラストラクチャに基づいた、業界で最も包括的な機能を備えています。SSL Network ExtenderはConnectraに標準装備されており、VPN-1にはオプションのアドオンとして利用することができます。

チェック・ポイント・ソフトウェア・テクノロジーズについて

チェック・ポイント・ソフトウェア・テクノロジーズは、インターネット・セキュリティ分野において世界をリードする企業で、VPNおよびファイアウォール分野における国際的なマーケット・リーダーとして認められています。当社は、構内、社内、およびWebのセキュリティのためのインテリジェント・セキュリティ・ソリューションを提供します。最高の順応性を持ちインテリジェントな検査テクノロジーであるINSPECT、わずかな総所有コストでセキュリティ・インフラ管理を実現できるSMART Managementを基盤に、チェック・ポイントのソリューションは最高水準の信頼性を誇り、世界中で幅広く導入されています。チェック・ポイントのソリューションは、92カ国で認定された2,300社のパートナーによって販売、統合、保守が行われています。



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@checkpoint.co.jp Tel : 03 (5367) 2500

© 2004 Check Point Software Technologies Ltd.

All rights reserved. Check Point, Application Intelligence, Check Point Express, Check Pointのロゴ, ClusterXL, ConnectControl, Connectra, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FireWall-1 XL, FloodGate-1, INSPECT, INSPECT XL, InterSpect, IQ Engine, Open Security Extension, OPSEC, Provider-1, Safe@Office, SecureKnowledge, SecurePlatform, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SSL Network Extender, 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, およびVPN-1 VSXは、Check Point Software Technologies Ltd.および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および6,496,935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 501337-J 2004.6

IPSec and SSL VPN Deployment Considerations

