



SSL VPN が成長するにつれて:

これまで以上に使える SSL VPN

著: リサ・ファイファー (Lisa Phifer) / Core Competence

WatchGuard® Technologies ホワイトペーパー

2009 年 5 月

はじめに

リモートアクセスに比べコストが掛からず、それほど複雑ではない SSL VPN に企業が目を向け始めたのは数年前のことです。初期の SSL VPN はウェブ・ブラウザを使用することにより、普段使用しているビジネス・アプリケーションにリモート・ワーカー達がアクセスしやすくなることを支援し、IPSec VPN クライアントに伴う IT 問題を緩和することに焦点を置いていました。そして、そのバリュー・プロポジションは多くの企業がレガシー VPN について再考し、SSL リモートアクセスの実装を促進させることになったのです。

その後、ビジネス・ニーズは進化し続け、現在の社員達は今までにないほど移動性に増し、幅広いビジネス・アプリケーションやシステムへのアクセス、そして様々なデバイスやロケーションを要求するようになりました。IT 部はより効率的、かつ効果的な方法で常に変化している接続性のニーズに応える方法を必要としています。さらに、業界規制やプライバシー法により強制されているコントロールや可視性を維持しながら、マルウェアや侵害などから企業資産を守らなければなりません。

幸いなことに SSL VPN ゲートウェイも成熟し、最近の製品は過去のアクセス制限を超え IT コントロールも細かになり自動化が増えました。昨今のモビリティ・チャレンジに対応していく上で、企業は SSL VPN にまつわる誤解を解き、SSL VPN をこれまで以上に利用する時期がきています。

誤解 #1: SSL VPN がサポートするのはウェブとブラウザ・インターフェイスのアプリケーションだけである

真実: 最近の SSL VPN ではアクセス方法を選択できるようになっているため、様々な TCP/IP アプリケーション、「クライアントレス」のブラウザ・インターフェイスやシンクライアント SSL トンネリングもサポートできるようになっています。

初期の SSL VPN は HTTP プロキシとしてスタートし、社員が普段使用しているブラウザで VPN ゲートウェイを介しウェブ・アプリケーションにアクセスすることを可能にしました。そして、ウェブベースではないアプリケーションへのアクセスも可能にするため、SSL VPN はブラウザベースの GUI、各ビジネス・プログラムに特有のコンテンツ・トランスレータも実現させました。例えば、ユーザがネイティブ Windows SMB プロトコルに HTTP リクエストを変換させるため、SSL VPN ゲートウェイに依存しネットワーク・ファイルサーバと作用し合う場合、Java フロントエンドを使う場合もあるでしょう。

しかし急速に変化するビジネス・ニーズに遅れず対応していくため、SSL VPN はブラウザ・インターフェイスのアプリケーション以上に拡大しなければなりません。最近では、ブラウザ・ラウンチのシンクライアントを提供し、ウェブベースではないプロトコルを SSL でトンネリングすることで、大抵のアプリケーションをすべてサポートできるようになっています。シンクライアントには特定のポートに送信されたメッセージを阻止するものが多く、VPN ゲートウェイを通じて TCP セッションからプライベート・アプリケーション・サーバに転送します。また、VPN ゲートウェイを介し、全トラフィックをプライベート・ネットワークにルーティングすることで IP パケットを阻止するものの中にはあります。遍在するアクセス・デリバリー・プラットフォームとしてブラウザを利用しながら、SSL VPN シンクライアントでビジネス・アプリケーションのリーチを大きく拡大することが可能になっています。

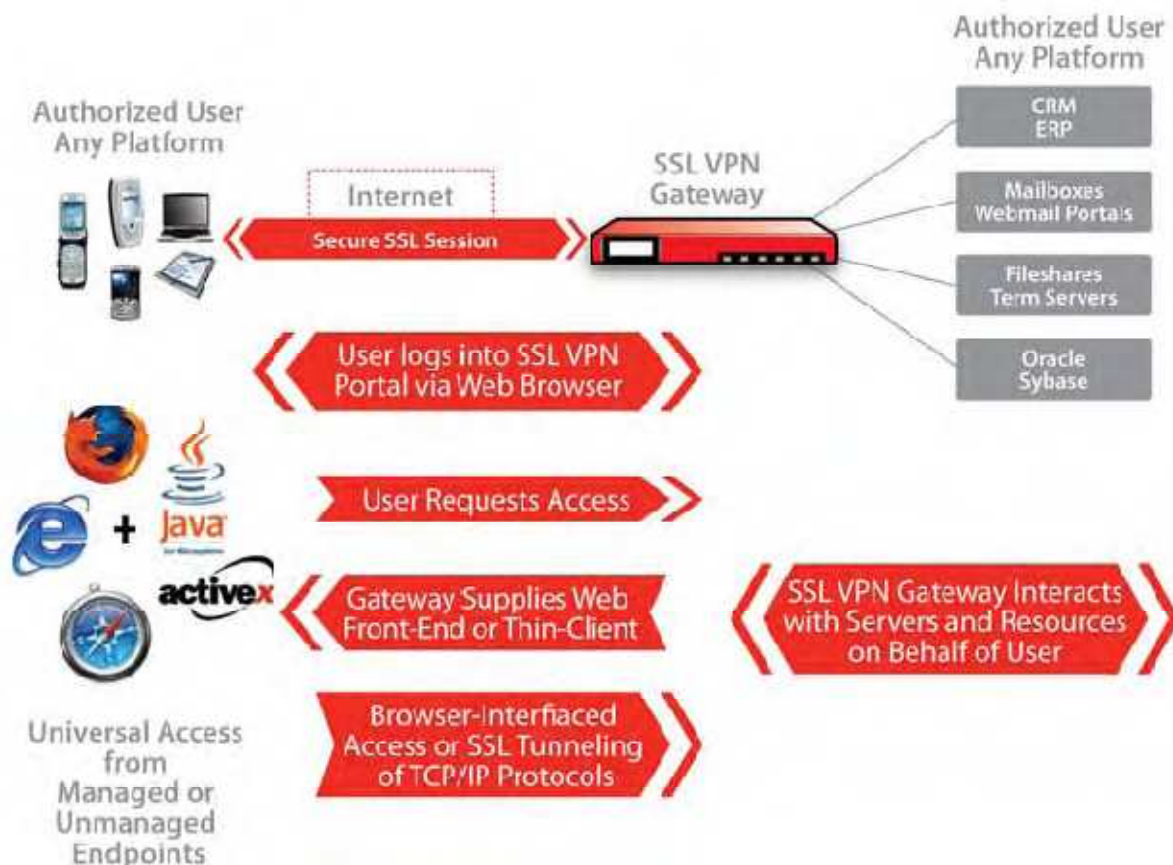


図 1: 柔軟なアクセス方法を提供する SSL VPN

誤解 #2: SSL VPN は普通のウェブ・ポータルと大差ない

真実: SSL VPN は、各ユーザの個人リソースを反映しアプリケーション・アクセス権を強制させる極めてカスタマイズしたポータル・ビューを提供します。

SSL VPN ゲートウェイは、シンプルなウェブアクセス・コンセントレーターとして始まったものかもしれませんが、最近では最新式のダイナミックなアクセス・ポータルを提供するまでになりました。スタティック・ウェブ・ポータルは誰にでも同じシングル・サービスのブラウザベース・ビューを提供するほか、データをコンパートメント化するため、異なるスタティック・ポータルが必要なユーザ・グループのアクセスを各サーバでそれぞれ管理するようになってい

ます。SSL VPN は、認証済みのアプリケーションやリソースにおいて粒度の細かいアクセスを各ユーザに許可したり、カスタマイズ可能なポータルを提供することで、さらに効率的かつ効果的になっています。SSL VPN は認証済みのユーザ情報だけでなく、アクセスを得るために使用されたエンドポイントも考慮する場合があります。アプリケーション・ルールやリソース・ルールは、誰にアクセス権が与えられているのか、そしてどういったアクションを取ることができるのか、リソースの名称、その表示方法といった点を決定するために使われることがあります。組織はそうすることで、シングル・ゲートウェイで全員のアクセスをコントロール、トラックしながら各ユーザや状況に適したポータル・ビューを表示することができます。

誤解 #3: SSL VPN は PDA や電話からのアクセスをサポートしない

真実: SSL VPN は Windows CE や Symbian、Palm、WAP 電話など、様々なデバイスからでもアクセス可能になりました。

ブラウザベースだけに集中した SSL VPN は、レガシーIPSec VPN クライアントよりも遥かに多くのエンドポイント・デバイスにアクセスできるようにしました。しかし、初期のウェブ・フロントエンドやシンクライアントの中には Win32 PC だけで実行できる ActiveX コントロールや、PDA の小さい画面では使いにくいブラウザ・インターフェイスといった相互作用における新たな懸念も生み出しました。

社員の移動性が上昇するに連れ、ワイヤレス携帯端末からのアクセスを安全にしておくことは企業にとって、もはや賢明なアクションだけではな、くビジネス上必要なことになっています。幸い、SSL VPN も端末プラットフォームのサポートを拡張しているほか、シンクライアントは Linux や Mac OS にもポートされていて、Java のニア・ユニバーサル・リーチにもタップしています。新しいウェブ・フロントエンドは Windows Mobile や Symbian、Palm などのスマートフォンにおいて、自動的にモバイル操作環境に適応するようになってい

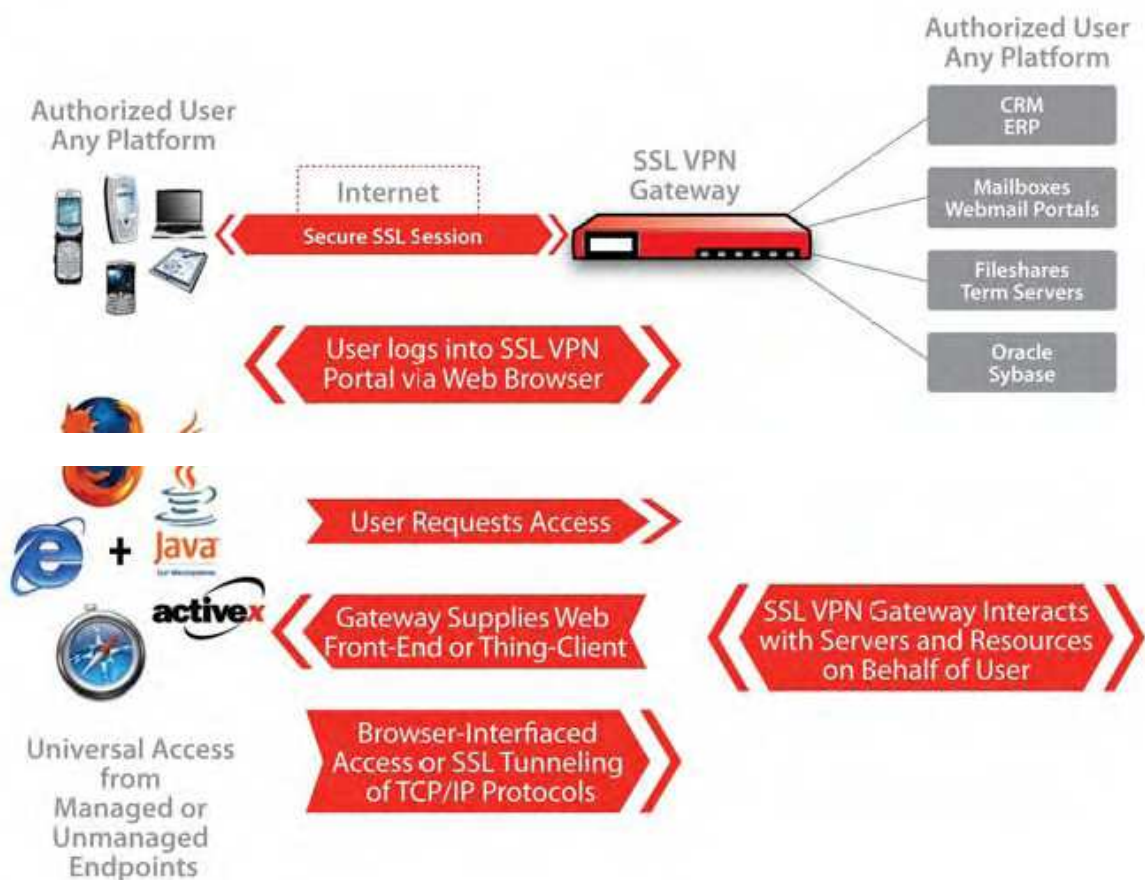


図 2: 様々な端末やアプリケーションをサポートする SSL VPN

誤解 #4: SSL VPN は企業資産をマルウェアや管理していない PC に露呈してしまう

真実: SSL VPN では認証したビジネス・リソースにアクセスを与えるかどうか、そしてその方法などを決定する前に、端末の状態や適合性を評価することができます。

初期の SSL VPN は通常のウェブ・ブラウザを使ってインターネット・カフェやテレワーカーの自宅の PC やビジネス・パートナーなど、管理していない端末からリモートアクセスを作れるようにしました。管理していないシステムは本質的にマルウェアに対し脆弱であり、残念ながら意図していないユーザでさえ機密データを残してしまう傾向が見られます。そのような環境において、認証や暗号化だけのトンネルは充分ではありません。企業のリソースやデータは紛失・盗難・攻撃などから守り隔離しなければなりません。

SSL VPN は、管理していない PC だけでなくすべての端末において、そうしたチャレンジに対応できるように進化しました。例えば、ユーザを認証したりアクセスを認証する前に、各端末の正当性を評価するルートとして SSL セッションを使うことができます。例えば、SSL VPN の中には端末の OS バージョンやパッチ、ウイルス対策の有無やそのシグネチャーなどについてクエリを出せるものもあります。また、ハードウェア・アドレスやホストの証明書、端末の情報など、その信頼性を探せるものや、管理している端末と企業のセキュリティ・ポリシーとの適合性を確認できる SSL VPN もあります。こうしたインテリジェンスを備えておけば、マルウェアによる脅威を緩和させるためのアクセスを判断することができます。例えば、ポリシーが最低限の安全要求を満たさない端末を拒否したり、準

拠するノートパソコンにトンネルのアクセス権を与えたり、限定した「キオスク・モード」アクセス権を許可したりすることが可能になります。

誤解 #5: SSL VPN 認証はキー・ストローク・ロガーによって危険にさらされることがある

真実: SSL VPN では、強力な認証方法と外部の認証サーバや搭載済みの強力な認証サービスを一緒に使うことで、そういった脅威を阻止できます。

マルウェア自体が進化し、金融利益を得ようとする組織化したサイバー犯罪は個人情報盗むことに集中し、最近ではそうしたケースが増えており、スパイウェアもよく見られるようになりました。特にトロイの木馬では、侵入された端末をリモートから管理できる攻撃用プラットフォームにするケースなどが見られます。キー・ストローク・ロガーを使ったトロイの木馬では、端末のセキュリティ・チェックが完了する前に再利用できるテキスト・パスワードを盗まれてしまう可能性があるため、VPN 管理者が特に懸念する問題です。

最近の SSL VPN はこの脅威に対応しているほか、「仮想キーボード」を表示しテキスト・パスワードを避けるものもあり、二要素認証 (two-factor authentication) を使ったエンタープライズ・サーバと組み合わせることができるものがほとんどです (例: RSA SecurID)。しかし、その強力性、使いやすさ、コストのバランスを取るのにはチャレンジであると言えるでしょう。強力な認証を促進するためにハードウェア・トークンや外部の認証サーバを購入せず、1 回きりのパスワードを生成できる SSL VPN もあります。VPN の強力な認証方法と強力性に欠ける LAN ログインを (例: Active Directory) マップさせ、企業パスワードをキー・ストローク・ロガーにさらすことなくシングル・サインオンを可能にするものもあります。

誤解 #6: SSL VPN は自宅や公共の PC で企業データを流してしまう

真実: SSL VPN は各ユーザの動きを制限することで SSL セッション時のデータを安全に保ち、ログオフの際にデータを削除することで、そのような問題を避けることができます。

細かなアクセス・コントロールを実行することで自宅や公共の PC によるリスクを SSL VPN が減少させるようになったのは最近のことではありません。例えば、ポリシーは完全には信頼していない端末からのシンクライアント SSL や IP トンネルを拒否したり、ファイルの読み取りのみのアクセス権を提供したり、テキスト形式ではなくグラフィック表示にしたりすることができます。さらに大方の SSL VPN では、使用中ではないユーザの接続を終了させ、ユーザのアクティビティ (例: ブラウザ履歴・キャッシュしたオブジェクト、一時ファイル) の形跡を自動的に削除するなど、セッション後のクリーニング・オプションを提供しています。

しかし、SSL VPN がセキュア・リモートアクセスの主要形態になるに連れ、社員も変化しています。SSL VPN ユーザは、管理されていない端末から企業リソースに繰り返し頻繁にアクセスすることが増えており、そうしたユーザにおいては、より幅広いアクセスと幾分のこだわりを許可することで、より生産性を高めることができるでしょう。例えば、安全な仮想デスクトップと SSL VPN を組み合わせることでセッション間も暗号化されている、一貫して安全な実行環境を提供することが可能になります。つまり、管理していない端末すべてが公共の PC ではなく、セキュリティをおろそかにすることなく、ユーザ・エクスペリエンスを改善させることができるようになるのです。

誤解 #7: SSL VPN 接続はよく中断される上に、繰り返しログインする必要がある

真実: VPN はハイ・アベイラビリティとシングル・サインオン技術を使うことでユーザの接続が途切れることなく、仕事に専念することができます。

IPSec VPN ユーザは接続が中断してしまう悩みをご存知でしょう。IP アドレスが変更になるとネットワーク・レイヤー・トンネルを再確立しなければならず、アプリケーション・セッションを中断させたり、何度も VPN または各アプリケーションにログインしなければならない場合があります。IPSec ユーザ、特に移動の多いワイヤレス・ユーザは、そうしたことに苛立ち仕事に専念することができなくなることが少なくありません。

SSL VPN はこうした IPSec の本質的な制限を迂回することができます。接続が途切れた場合でも、素早くそしてユーザの介入なしに、SSL セッションが自動的に維持されます。また、SSL VPN の中には、ネットワーク・ローミングを容易にするものまであります。例えば、一時的に接続が中断した場合、ユーザの認証状態を維持することができたり、シングルサインオンでユーザに気付かれることなく接続を回復させたりすることができます。IP パケットをトンネルする SSL VPN は、ローミング中に変更されることのない仮想アドレスを使うようになっています。ハイ・アベイラビリティ SSL VPN クラスターは、ゲートウェイのメンテナンス時やフェイルした場合でもユーザの接続を維持することができます。

誤解 #8: SSL VPN ポリシーは複雑で管理するのが難しい

真実: SSL VPN は集中ポリシー・マネージャーを使用したり、エンタープライズ認証サーバやディレクトリーと統合させることができるため、管理を簡略させることが可能です。

勿論、SSL VPN ポリシーは手に負えないほど大きくなってしまいう可能性があります。細かなポリシーや複数のアクセス方法、エンドポイント・セキュリティ・チェッカー、カスタマイズできるポータルなどで望んでいる結果を得るためには、VPN 管理者はそのパワーを賢明に、そして巧みに使いこなせなければなりません。

ここでは経験がものを言います。十分に成長した SSL VPN 製品は、何年もかけて改良されてきました。グループ・ポリシーやその役割を基本にしたポリシー、再利用できるポリシー・オブジェクトやテンプレートなどのテクニックは、SSL VPN 管理を合理化させました。SMB はウィザードや搭載されているインテグリティ・チェッカー、認証サービスなどからそれ以上の利益を受けることができます。それより規模の大きい企業は、エンタープライズ認証サーバや、複数のゲートウェイ用のシングルポイント・ポリシー管理、適合性の監査やレポートのログを統合することができます。

誤解 #9: SSL VPN は IPSec VPN を実行するほど難しい

真実: SSL VPN は、ユーザの自動エンロールメントや、セルフサービス管理を伴うクライアントレスやシンククライアントなどを提供することで、クライアント・インストールやプロビジョニングを回避することができます。

SSL VPN は、IPSec VPN のクライアント・ソフトウェア・インストール、コンフィギュレーション、アップデートなどに関わるコストに対応できるように作成されました。現在、クライアントレス SSL VPN アクセスは様々なユーザのニーズに応えることができ、ソフトウェア管理を回避することができます。しかしながら SSL VPN シンククライアントは、それとは別のソフトウェア管理が必要なだけなのでは、と懸念する声もあります。

製品によってはそうかもしれませんが、SSL VPN 全製品がそうではありません。シンククライアントやウェブ・フロントエンドは、プラットフォームの依存性を減少させるべく進化しています。インストール可能なクライアントを提供している SSL VPN は、それらを提供するためにポータル・ページ・リンクを使っています。大方、ポータルは自動的にもっとも優れたシンククライアントをスタートさせるようになっているため、ユーザが関与したり推測したりする必要がありません。シンククライアントやウェブ・フロントエンドを必要に応じてダウンロードするということは、使用しているバージョンは常に最新のものであるということです。ポリシーは各セッションごとにゲートウェイで適用されているので、クライアント・コンフィギュレーション・アップデートもありません。SSL VPN はパスワードの更新やポータル・ショートカットのカスタマイズなど、ユーザによる変更を行うためのセルフサービス・ウェブ・インターフェイスも

提供しています。つまり、SSL VPN はインストール・クライアントに掛かるコストを回避するだけでなく、ブラウザ・パラダイムは全体的な管理費用を削減させることもできるのです。

結論

これで SSL VPN が過去数年で明らかに大きく成長したことがお分かりになったことだろうと思います。新しい SSL VPN ゲートウェイは、過去のものよりも大幅に改善され、全体の所有コストも低下しています。しかし、製品機能は様々であるため、ご自分のビジネス・ニーズに見合ったソリューションを注意して選ぶ必要があります。WatchGuard® SSL 100 の詳細については、ウェブサイト www.watchguard.com またはご利用のリセラーまでお問合せください。

WatchGuard® SSL 100 について

使いやすいセキュア・リモートアクセスをお求め安い価格でお探しの場合は、WatchGuard® SSL 100 アプライアンスが中小企業のネットワーク・ソリューションに最適です。ビジネスのニーズにより、SSL の実装をシンプルにしたリ、高度な方法で使うこともできるなど、このアプライアンスの長所はその柔軟性にあります。

- ・ 極めて簡単に使用できるアプライアンスをお探しの小規模ビジネスは、実質的に管理諸経費なしでリモートからスタンダード・ネットワークのリソースにアクセスすることができます。
- ・ より複雑なニーズを持つビジネスは、トンネルとポータル・ベースのリソースを組み合わせ、リモートのデスクトップに対しテクニカル・サポートを行ったり、ユーザやデバイスの細かな基準をベースにしたコントロール・アクセスを行うことが可能になります。

WatchGuard® SSL 100 その他の機能:

- ・ プラグアンドプレイ、オールインワンのアプライアンスでは、ソフトウェア・コンポーネントを追加購入する必要がありません。
- ・ Vista 32 ビットと 64 ビット・サポートを含むクライアントおよびクライアントレス・アクセス
- ・ メールやウェブ会議など必然とされる企業リソースに簡単にアクセスすることができます。オプションの SSH や RDP などノン・ネイティブ・アプリケーションを伴ったウェブ有効デバイスから CRM にアクセスでき、その生産性は極めて高いものとなります。
- ・ ウィルス対策やスパイウェア対策、ファイアウォール・ソフトウェアやその他様々な属性デバイスを含むエンドポイント・コンプライアンスを企業が設定し強制することを許可することにより、総合的なエンドポイント・インテグリティ・チェックでネットワークを確実に保護することができます。
- ・ セッション・クリーンアップは、ファイル削除やキャッシュクリーニングを含む端末からのアクセス形跡をすべて除去するため、他のユーザがネットワーク・リソースに密かに再度アクセスすることで行われるデータ漏れを防ぐことができます。
- ・ 強力な認証などローカルおよび第三者による認証サポートは、認証されているユーザのみがネットワークにアクセスできるようにし侵入者がネットワークに入れないようにします。
- ・ 統合監査はアクセスに関する情報を全て収集し、その源の確認、システム・イベントなどにおいてユ

ーザとシステムベースのアクティビティを集中管理先で素早くチェックします。

- ・ IT 管理者達は、マイクロソフトの Active Directory など第三者による既存の認証ソリューションと統合することができます。また、ローカル認証設定では LDAP サーバに依存したり、SMS ベースのトークンや身元確認のウェブ・キーパッドなど搭載されている二要素認証を使うこともできます。

WatchGuard SSL 100 はビジネスニーズに最適なりモートアクセスをお求め安い価格で提供しています。
WatchGuard® SSL 100 アプライアンスの詳細については www.watchguard.com/ssl を参照なさってください。

著者について

リサ・ファイファー(Lisa Phifer)は、ネットワークとセキュリティ・テクノロジーのビジネス利用に焦点を置くコンサルティング会社、Core Competence Inc. (www.corecom.com)の社長を務めています。Core Competence ではネットワーク構築やその実装、テストなどにおける 27 年の経験を活かし、大規模および小規模企業のリスク管理やビジネス・ニーズに対応するネットワーク・セキュリティ、最適な使用方法についてアドバイスしています。また、リサはワイヤレス、モバイル・セキュリティから仮想プライベート・ネットワーク、ネットワーク・アクセス・コントロールまで、テクノロジー分野の広範囲に渡り教え記事を書いています。

住所: 505 Fifth Avenue South Suite 500 Seattle, WA 98104 U.S.

WEB: www.watchguard.com

営業: 1.800.734.9905

インターナショナル・セールス: +1.206.613.0895

WatchGuard について:

1996 年より、WatchGuard は受賞歴を持つネットワークやビジネスを保護するためのファイアウォールや VPN、セキュリティ・サービスなどを組み合わせた統合脅威管理(UTM)ネットワーク・セキュリティ・ソリューションを構築しています。最近では次世代製品をリリースしたほか、拡張可能な脅威管理(XTM)ソリューションは信頼できるオールインワンのセキュリティ機能も提供し、あらゆるエンタープライズのセキュリティ・ニーズに対応できるスケールと価格を提供しています。ウォッチガード製品は 120 カ国に渡り、1 万 5 千社から成る WatchGuard の代理店パートナーに支持されています。赤い色が特徴の WatchGuard セキュリティ・アプライアンスは、世界中の小売店から教育機関、ヘルスケア機関を含む分野において、50 万台以上が使用されています。WatchGuard 本社は米国ワシントン州シアトルに所在し、北米、ヨーロッパ、アジアパシフィック、南米にオフィスを構えています。同資料における表現に保証はありません。全仕様書は変更される可能性があり、今後の製品や機能などの利用状況については弊社の意向に基づき提供します。©2009 WatchGuard Technologies, Inc.無断複写・転載を禁じます。WatchGuard および WatchGuard のロゴは WatchGuard Technologies, Inc.の米国およびそのほかの国における登録商標あるいは商標です。そのほかすべての登録商標および商標は、各所有者に権利があります。

Part No.WGCE66583_070109