

特集： SSL-VPN に関する 100問 100答

SSL-VPN に関して最もよく聞かれる 100 の質問にシスコの VPN 技術担当およびマーケティング担当者が答えます。
社員によるアクセスや、取引先およびエクストラネットの接続をサポートする
リモート アクセス ソリューションの仕組みを説明します。

CISCO SYSTEMS



THIS IS THE POWER OF THE NETWORK. NOW

100 問 100 答

以下の質疑応答は、2004 年 1 月 15 日に開催された「SSL and IPSec VPNs: Robust Remote Access for Any Environment (SSL および IPSec VPN : あらゆる環境に対応できる安定したリモート アクセス)」と題するシスコシステムズの Web セミナーで実際に行われたものです。このイベントでは、社員のモビリティの必要性、IP Security (IPSec) と Secure Socket Layer (SSL) VPN を配備する時期、そしてこれら 2 つのテクノロジーがもたらす柔軟なリモート アクセス環境というテーマで討議が行われました。

担当者の紹介

Dennis Vogel – SSL-VPN の技術担当者

Dennis Vogel は、Cisco® VPN 3000 コンセントレータ製品のプロダクト マネージャで、IPv6 セキュリティ製品を担当しています。以前はアクセス制御技術の戦略的方向性と Cisco PIX® セキュリティ アプライアンスの製品機能ロードマップの作成を担当していました。1998 年にセキュリティ インターネット サービスユニットの一員として、シスコシステムズに入社しました。

Mark Bornstein – マーケティング担当者

Mark Bornstein は、営業技術およびマーケティングに 15 年以上の経験があります。現在は、シスコのセキュリティ マーケティング チームで、「セキュア コネクティビティ」のプログラム マネージャを務めています。

Pete Davis – 技術担当マネージャ

Pete Davis は、幼い頃からコンピュータとネットワークに携わってきました。15 歳のときには、すでに最年少のネットワーク エンジニアとして、あるインターネット サービス プロバイダーの初期の従業員の一人として働いていました。ニューイングランド州最大の消費者インターネット サービス プロバイダーである Internet Access Company でシステムおよびネットワークの実装と保守を担当していましたが、1998 年以降は、マサチューセッツ州フランクリンの VPN コンセントレータ メーカーである Altiga Networks (2000 年 3 月 29 日にシスコが買収) に勤務しています。プロダクト マネージャとして、VPN 関連の新製品および新機能の開発を担当しています。

シスコの統合化セキュリティ ソリューションは、企業全体のネットワークの保護、ネットワーク可用性の最大化、生産性の向上に役立ちます。

ネットワークをどこにでも安心して拡大できます。

シスコ自己防衛型ネットワークは人的な攻撃やミスからの保護を提供します。
シスコの統合セキュリティ アプローチについての詳細は、以下をご覧ください。
<http://www.cisco.com/jp/powernow/security/>

CISCO SYSTEMS



THIS IS THE POWER OF THE NETWORK. NOW

あらゆる環境に対応できるリモート アクセス :

IPSec と SSL-VPN を使用すれば、すべてのユーザにネットワークを拡大できます。

Q.1

2箇所で2つのコンセントレータを稼働する場合、冗長性を持たせるために最適なプロトコルは何ですか (Virtual Router Redundancy Protocol、負荷分散など) ?

A.1

どちらも1箇所のシステムに耐障害性を持たせるために設計されたプロトコルです。ほとんどのお客様は負荷分散を利用しています。すべての機器をアクティブで接続可能な状態にできるからです。IPSec の場合は、VPN クライアントのバックアップ サーバ機能を複数の場所の冗長構成に使用します。

Q.2

Cisco VPN 3000 コンセントレータ ソフトウェア v4.1 はいつ入手可能になりますか ?

A.2

Cisco VPN 3000 コンセントレータ ソフトウェア v4.1 はすでに入手可能です。

Q.3

使用している Cisco VPN で SSL/IPSec 証明書を認証に使用するにはどうすればよいのですか ?

A.3

IPSec の証明書は、VPN クライアントのネイティブ Certificate Manager または Microsoft Common Application Programming Interface (CAPI) にロードできます (Internet Explorer からアクセスできます)。SSL-VPN の場合は、ご使用の Web ブラウザに証明書がインストールされていれば、利用可能になります。

Q.4

SSL-VPN をサポートするためにコンセントレータのハードウェア要件は変更されましたか ?

A.4

Cisco VPN 3000 コンセントレータで SSL-VPN をサポートするために必要なのは v4.1 ソフトウェアだけです。ただし、VPN パフォーマンス (サポートできるセッション数) を増強するために、Scalable Encryption Processing-E (SEP-E) カードの使用と、メモリの増設を検討してください (まだ最大メモリを搭載していない場合)。

Q.5

Telnet、TN3270、Windows Terminal Service のような端末サービスへのアクセスに WebVPN を使用できますか ?

A.5

できます。

Q.6

VPN コンセントレータ ソリューションはダウンロード可能な Access Control List (ACL; アクセス制御リスト) をサポートしていますか ?

A.6

サポートしています。Cisco VPN 3000 コンセントレータは RADIUS または Lightweight Directory Access Protocol (LDAP) の認証サーバから ACL をダウンロードできます。

Q.7

VPN コンセントレータは地理的な多様性にどの程度対応できますか ? たとえば、ISP のハイアベイラビリティ データ センターにも対応できますか ?

A.7

Cisco VPN 3000 コンセントレータ ソフトウェアはクラスタ化によって特定の地理的区域内のハイアベイラビリティに対応できます。IPSec クライアントは自動的に複数の地理的領域でのクラスタ化をユーザには透過的に実行します。また、シスコ製ルータは ISP の多様性に対応できるだけの帯域冗長性を備えています。

Q.8

A.4 で言及された SEP-E カードについて詳細を教えてください。

A.8

SEP-E モジュールは、Cisco VPN 3000 コンセントレータ ソフトウェア v4.0 以降、Cisco VPN 3030 以上のコンセントレータに付属しています。

Q.9

IBM Client Access のような端末エミュレーション アプリケーションをこの VPN で使用できますか ?

A.9

TCP ベースであれば使用できます。

Q.10

シスコは無線接続での VPN の設定方法を解説した文書を発表していますか ?

A.10

はい。ワイヤレス セキュリティについての文書や、イーサネット接続とワイヤレス接続での VPN およびモバイル IP の使用方法についての文書を発表しています。ほとんどの資料は、<http://www.cisco.com/jp/powerow/security/> の無線に関するセクションにあります。

Q.11

WebVPN が Citrix をサポートする時期はいつですか ?

A.11

Cisco VPN 3000 は次のリリースで Citrix をサポートします。

Q.12

Cisco SSL-VPN では、Microsoft Windows AD によるユーザ認証は可能ですか ?

A.12

可能です。RADIUS、NT Domain、Active Directory のほか、RSA SecureID のような One-Time Password (OTP)、デジタル証明書やスマートカード証明書を使用して、ユーザを認証できます。

CISCO SYSTEMS



THIS IS THE POWER OF THE NETWORK. NOW

あらゆる環境に対応できるリモート アクセス :

IPSec と SSL-VPN を使用すれば、すべてのユーザにネットワークを拡大できます。

Q.13

Cisco VPN 3000 コンセントレータ ソフトウェア v4.1 には、エクストラネットの機能はありますか？

A.13

あります。パートナーへのエクストラネット接続は、WebVPN の主要なアプリケーションの 1 つです。

Q.14

1 箇所にいる複数のユーザが 1 つの Network Address Translation (NAT; ネットワーク アドレス変換) ネットワークに接続することは可能ですか？

A.14

可能です。単一アドレスではなく、一定のアドレス範囲をサポートするように NAT アドレスを設定できます。

Q.15

Cisco VPN 3060 や Cisco VPN 3080 コンセントレータが同時に処理できる SSL-VPN セッション数はどの程度ですか？

A.15

Cisco VPN 3030 ~ 3080 のコンセントレータに Cisco VPN 3000 コンセントレータ ソフトウェア v4.1 リリースを使用すると、同時に 500 の SSL (WebVPN) ユーザをサポートできます。接続数はクラスタ化によって増やすことが可能です。

Q.16

グループ メンバーシップに基づいて、VPN やダウンロード可能な ACL を適用できますか？

A.16

できます。Cisco VPN 3000 コンセントレータ上で定義されるユーザグループごとにアクセス制御用の ACL を定義できます。実際、シスコではこの方法を推奨しています。

Q.17

SSL-VPN は現在の Cisco VPN 3030 コンセントレータに組み込まれているのですか？それとも異なるデバイスに組み込まれているのですか？

A.17

WebVPN (SSL) / クライアントレス接続は、既存の Cisco VPN 3000 コンセントレータ シリーズのデバイスで Cisco VPN 3000 コンセントレータ ソフトウェア v4.1 を使用することによって可能になります。

Q.18

WebVPN はアプリケーションのパフォーマンスにどのような影響を及ぼしますか？

A.18

SSL-VPN を通じて実行されるアプリケーションへの影響はごくわずかです。コンセントレータに搭載される SEP-E カードによってパフォーマンスを高めることができます。

Q.19

SSL-VPN を使用するために Web ポータルを構築する必要がありますか？

A.19

新たにポータルを追加する必要はありません。Cisco VPN 3000 コンセントレータ ソフトウェアでは、SSL-VPN の設定に IPSec と同じインターフェイスと管理手法を使用します。

Q.20

個々の Cisco VPN 3000 コンセントレータがサポートする SSL-VPN セッション数を教えてください。

A.20

Cisco VPN 3005 コンセントレータは、同時に 50 の WebVPN セッションをサポートします。Cisco VPN 3020 コンセントレータは 200、Cisco VPN 3030 ~ 3080 コンセントレータは 500 のセッションを同時にサポートします。ユニットのクラスタ化によって、サポート能力と耐障害性をさらに強化することも可能です。

Q.21

SSL ソリューションで、ネットワーク内の多様なデバイスに対し、IPSec VPN と同じ運用サポート (サーバ管理やネットワーク サービスなど) とアクセスを提供するにはどうすればよいですか？VPN クライアントのオーバーヘッドは望ましくありませんし、また Citrix は価格が高く、インフラストラクチャに大きな負荷をかけます。

A.21

VPN 3000 を通じて実行される SSL-VPN セッションによってシスコ製ルータへの Tenet セッションをオープンするという方法があります。現在のところ、VPN 3000 以外に SSL-VPN をサポートしているシスコのデバイスはありません。

Q.22

Cisco VPN 3000 コンセントレータ ソフトウェア v4.1 は、Internet Explorer と Mozilla 以外のブラウザを使用しても機能しますか？

A.22

機能します。Cisco VPN 3000 コンセントレータ ソフトウェアには、SSL-VPN に関してブラウザに依存しない手法が採用されているので、Mozilla、Safari、Netscape、Internet Explorer をはじめとして、さまざまなブラウザに対応できます。

Q.23

Cisco VPN 3000 コンセントレータ (中央) と Cisco PIX 501 セキュリティ アプライアンス (リモート) を使用する方法は、望ましい IPSec VPN ソリューションといえますか？

A.23

ヘッドエンドで Cisco VPN 3000 コンセントレータを使用し、ブランチ サイトで Cisco PIX セキュリティ アプライアンスを使用するのは良い方法です。シスコの VPN 製品はすべて互換性があり相互動作が可能です。ヘッドエンドに Cisco VPN コンセントレータを、リモート サイトに Cisco PIX セキュリティ アプライアンスを配置するというソリューションは珍しくありません。

CISCO SYSTEMS



THIS IS THE POWER OF THE NETWORK. NOW

あらゆる環境に対応できるリモート アクセス :

IPSec と SSL-VPN を使用すれば、すべてのユーザにネットワークを拡大できます。

- Q.24**
SSL-VPN と IPSec VPN は両立できないのですか？つまり 1 箇所で両方のソリューションを提供することはできますか？
- A.24**
シスコの製品を使用すれば、同じ場所の同じプラットフォームで SSL-VPN と IPSec VPN を同時にサポートできます。
- Q.25**
SSL-VPN の暗号化レベルはどの程度ですか？
- A.25**
標準的な Web ブラウザのほとんどは Triple Data Encryption Standard (3DES)、DES、RC4-128、40 ビット暗号化をサポートしています。シスコは 3DES(168 ビット)暗号化を推奨しています。
- Q.26**
Cisco VPN 3000 コンセントレータ ソフトウェア v4.1 と現在のバージョンの SSL オプションにはどのような相違点がありますか？
- A.26**
v4.1 より前のバージョンの Cisco VPN 3000 コンセントレータ ソフトウェアはクライアントレス VPN をサポートしていません。Cisco VPN 3000 コンセントレータ ソフトウェア v4.1 では、コンセントレータの接続に SSL-VPN を使用できます。
- Q.27**
現在 IPSec TCP 接続のポート 443 を使用していますが、SSL-VPN を使用するには、接続ポートを変更しなければなりませんか？
- A.27**
IPSec/TCP と WebVPN を同じ TCP ポートで同時に実行することはできません。したがって、TCP443 (デフォルトの HTTPS ポート) で WebVPN を使用するためには、IPSec/TCP 接続を別の TCP ポートに移す必要があります。
- Q.28**
同時セッション数が 500 では足りません。同時セッション数を数千規模に増加する計画はありますか？
- A.28**
Cisco VPN 3000 コンセントレータ ソフトウェアでは、複数のデバイスをクラスタ化することによって、サポート可能なセッション数を数千規模に拡大できます。また、このソフトウェアには、複数のコンセントレータ間での動的かつ統合的な負荷分散機能もあります。したがって、利益を損なうことなくインフラストラクチャに投資し、必要に応じて機能を追加していくことができます。たとえば、高価なデバイスを 1 つ購入するのではなく、小規模なデバイスをいくつか購入すれば、必要に応じて拡張することも、冗長構成にすることも可能です。
- Q.29**
同一の Cisco VPN 3000 コンセントレータで IPSec と SSL-VPN を両方使用できますか？
- A.29**
できます。
- Q.30**
Cisco VPN 3005 コンセントレータで SSL-VPN を使用できるようにするには、何が必要ですか？
- A.30**
Cisco VPN 3000 コンセントレータ ソフトウェア v4.1 にアップグレードする必要があります。SmartNET[®] サポート契約を結んでいるお客様は無料で v4.1 にアップグレードできます。
- Q.31**
IPSec と SSL-VPN を両方使用するのは賢明な方法といえますか？
- A.31**
通常、IPSec と SSL-VPN はそれぞれ異なる問題を解決します。このように補完的に機能するため、単一のソリューションであらゆるリモート アクセス ユーザの要求に対応できます。
- Q.32**
発表されている同時セッション数と一致していません (<http://cco-stage.cisco.com/jp/product/hs/security/vpn3000con/comp/>)。明確に説明してください。
- A.32**
このデータシートは現在改訂作業中であり、近々更新されます。
- Q.33**
Cisco SSL-VPN では、Novell NDS によるユーザ認証は可能ですか？
- A.33**
ネイティブにはサポートしていませんが、RADIUS プロキシを通じて認証できます。
- Q.34**
IPSec と SSL-VPN では、ハードウェア要件は異なりますか？
- A.34**
いいえ、シスコのソリューションではハードウェア要件は異なりません。同じハードウェアとソフトウェアを備えた同じプラットフォームで IPSec と SSL-VPN をサポートできます。VPN パフォーマンスを最高レベルにするために、SEP-E アクセラレーションカードの使用を推奨します。
- Q.35**
小規模なハードウェア クライアント (NETGEAR/Linksys など) をシスコのコンセントレータ シリーズと一緒に機能させることはできますか？
- A.35**
できません。Linksys 製品にはハードウェア VPN 機能がないためです。IPSec または SSL-VPN のパススルー モデルであれば一緒に使用できます。



あらゆる環境に対応できるリモート アクセス：

IPSec と SSL-VPN を使用すれば、すべてのユーザにネットワークを拡大できます。

Q.36

現在の企業は SSL-VPN と IPSec を両方必要としていますか？ また、今後ほとんどの企業は複数の場所に両方を展開する必要が生じると考えられますか？

A.36

SSL-VPN 接続と IPSec 接続の同時サポートには多くのお客様が関心を示されています。シスコのソリューションなら、お客様のリモート アクセス ニーズのすべてを単一のプラットフォームでサポートできます。

Q.37

1 台の Cisco VPN 3030 コンセントレータ上に IPSec と SSL-VPN を混在させることは可能ですか？

A.37

1 台の Cisco VPN 3030 コンセントレータ上に IPSec と SSL-VPN を混在させることは可能です。実際、シスコは、同じプラットフォーム上で両方に対応できるような独自の製品を提供しています。これはお客様の所有コスト軽減に役立ちます。

Q.38

SSL-VPN ソリューションでは、認証手法の一部として Microsoft Active Directory (AD) グループを使用できますか？ それとも Web サーバ上の認証しか使えないのでしょうか？

A.38

Cisco VPN 3000 コンセントレータでは、IPSec と WebVPN のどちらも AD に対する認証が可能です。

Q.39

ハイ アベイラビリティ構成では、ステートフル フェイルオーバーや負荷分散にどのような選択肢がありますか？

A.39

ほとんどのお客様は統合型の負荷分散を利用されています。この方法を使用すると、環境に対する許容度が広がり、耐障害性が強化されます。

Q.40

SSL-VPN を使用するためには、認証設定を変更する必要がありますか？

A.40

変更は必要ありません。シスコは、負荷分散やクラスタ化、ユーザ認証など、Cisco VPN 3000 コンセントレータ上のグローバル コンフィギュレーション パラメータの多くを WebVPN で使用できるように設計しています。これらのパラメータは、設定の複製や変更を行わなくても、IPSec でも SSL-VPN で機能します。

Q.41

SSL-VPN ソリューションでは、証明書のようなものを使用しますか？

A.41

ヘッドエンド デバイスには、他の HTTPS (SSL) Web サーバと同様に、それ自体の証明書があります。クライアントは、クライアント側の証明書、またはユーザ名とパスワード (または OTP) 認証によって識別されます。

Q.42

DMZ (非武装地帯) にある Web サーバへのセキュリティと比較して、SSL-VPN を使用する利点は何ですか？

A.42

単一のサーバではリモート ユーザが要求するすべてのアプリケーションへのアクセスをサポートできるとは限りません。サーバは、必要とされるさまざまな認証方式、フィルタリング、管理制御に対応します。

Q.43

Microsoft VPN クライアントを使用して Cisco VPN 3000 コンセントレータ ソフトウェアにアクセスすることは可能ですか？

A.43

可能です。Cisco VPN 3000 コンセントレータ ソフトウェアは Microsoft Point-to-Point Tunneling Protocol と L2TP/IPSec クライアントをサポートしています。

Q.44

SSL-VPN ソリューションでは、どこにウィルス対策ソフトウェアを配置したらよいですか？

A.44

ウィルス対策ソフトウェアはシスコのすべてのセキュリティ製品と補完的に機能します。SSL-VPN 製品はデバイスの接続に対するセキュリティを提供し、ウィルス対策ソフトウェアはファイルの感染を防止および除去します。補完的な技術を組み合わせることによって、高レベルのデバイス セキュリティが実現します。

Q.45

現在、100 のトンネルに対応可能な Cisco VPN 3005 コンセントレータを使用しています。強化モデルは 200 のトンネルをサポートしていますが、ソフトウェアをアップグレードすれば、200 のトンネルに対応できるのですか？

A.45

できます。これはソフトウェアのアップグレードによって得られる機能なので、既存のハードウェアをそのままご利用いただけます。ただし、200 の IPSec トンネルをサポートするには、64 MB メモリが必要です。

Q.46

各アプリケーションが 1 つずつトンネルを使用するのですか？

A.46

SSL-VPN (WebVPN) では、アプリケーションの数がトンネル数になるわけではありません。トンネル数は、一意に認証されたユーザの数となります。



あらゆる環境に対応できるリモート アクセス：

IPSec と SSL-VPN を使用すれば、すべてのユーザにネットワークを拡大できます。

Q.47

SSL-VPN は、Macintosh プラットフォーム上の Web ブラウザをサポートしていますか？

A.47

サポートしています。Mac OS X の Safari ブラウザを推奨しています。

Q.48

SSL-VPN はそれだけで十分なセキュリティを備えていますか？それともトークン サーバを併用した方がよいですか？

A.48

あらゆる VPN ソリューションの個人認証にワンタイム認証を追加できます。セキュアなソリューションの構築に必須というわけではありませんが、強く推奨します。

Q.49

WebVPN 4.1 にはクライアントも含まれていますか？

A.49

WebVPN の利点は、標準の Web ブラウザ SSL だけで機能する点です。

Q.50

DMZ にある Web サーバへのセキュリティと比較して、SSL-VPN を使用するセキュリティ上の利点は何ですか？

A.50

SSL-VPN では、Web サーバよりも詳細なユーザ認証を利用できます。また、非 Web アプリケーションへのアクセスも可能です。

Q.51

SSL-VPN は、RSA SecureID ネイティブ認証と Active Directory ネイティブ認証をサポートしていますか？

A.51

はい、両方ともサポートしています。さらに、RADIUS、NT Domain、その他の OTP、デジタル証明書もサポートしています。

Q.52

IPSec を実働用、SSL-VPN をテスト用に稼働させることはできますか？別々のデバイスを用意する必要がありますか？

A.52

両方を同時にサポートできます。ただし、テストのために実働装置を使用することは望ましくありません。新しい機能のテストによってお客様の実働環境に影響が生じる可能性があります。一部のユーザグループでソリューションをテストしながら、異なる実働デバイスで主要な IPSec の機能を稼働させる方法を推奨します。

Q.53

2 台以上の Cisco VPN 3005 コンセントレータを使用すると、1 台の Cisco VPN 3020 コンセントレータを使用すると、どちらがよいでしょうか？

A.53

Cisco VPN 3020 コンセントレータは 1 台で Cisco VPN 3005 コンセントレータの数倍のキャパシティを備えています。一方、複数の Cisco VPN 3005 コンセントレータをクラスタ化すれば、キャパシティと冗長性を増強できます。どちらがよいかは個人や会社の方針によって決まります。製品に障害が発生しても完全なキャパシティが必要であるのか、問題が修正されるまではキャパシティが減少してもかまわないのかによって選択は異なります。

Q.54

企業のファイアウォールとの関係から、Cisco VPN 3000 はネットワークのどこで使用するのが適切でしょうか？

A.54

ほとんどのお客様はファイアウォール上の DMZ インターフェイスの後ろに Cisco VPN 3000 コンセントレータを配備しています。ただし、コンセントレータは、設計やセキュリティのニーズに応じて、ファイアウォールの後ろに配備することも、ファイアウォールと並列に配備することも可能です。

Q.55

WebVPN を使用すると、どのようなことが可能になりますか？

A.55

WebVPN は、Cisco VPN 3000 コンセントレータと、現在 IPSec に対応しているデバイスに、リモート アクセス SSL-VPN のサポートを追加します。SSL-VPN のサポート には追加料金は必要ありません。

Q.56

8 時間ずっと働く社員は SSL-VPN と IPSec のどちらを利用すべきでしょうか？

A.56

一日中接続されているデスクトップを使用する社員には、IPSec の方が適しています。

Q.57

VPN IPSec では Cisco VPN クライアントを使用していますが、同じクライアントを SSL-VPN にも使用するのはですか？

A.57

SSL-VPN では、Web ブラウザの SSL-VPN 機能を使用するので、IPSec VPN クライアントを使用する必要はありません。

Q.58

Cisco VPN 3030 と 3005 のコンセントレータは LAN 間のトンネルをいくつサポートしていますか？

A.58

Cisco VPN 3005 コンセントレータは 100 の LAN 間 IPSec トンネル、Cisco VPN 3030 コンセントレータは 500 の LAN 間トンネルをサポートしています。また、Cisco VPN 3005 コンセントレータは 200 の IPSec リモート アクセス VPN トンネル、Cisco VPN 3030 コンセントレータは 1500 のリモート アクセス トンネルをサポートしています。

CISCO SYSTEMS



THIS IS THE POWER OF THE NETWORK. NOW

あらゆる環境に対応できるリモート アクセス :

IPSec と SSL-VPN を使用すれば、すべてのユーザにネットワークを拡大できます。

Q.59

Cisco VPN 3030 コンセントレータと同等またはそれ以上の機能が得られるような Cisco VPN 3015 コンセントレータ用 SEP-E アクセラレーション カードはありますか？

A.59

あります。Cisco VPN 3015 コンセントレータを Cisco VPN 3030-E または 3060-E コンセントレータに変換するためのアップグレードパッケージが用意されています。

Q.60

IPSec では、専用ソフトウェア クライアント、ハードウェア、一般的なソフトウェア クライアントのうち、どのクライアント接続が望ましいですか？どれを使用しても大きな違いはないのですか？

A.60

ユーザのニーズによって異なります。Cisco IPSec VPN クライアントは、Cisco VPN 3000 コンセントレータ、Cisco PIX セキュリティ アプライアンス、Cisco IOS® IPSec VPN ルータとともに使用する場合に最適な機能を提供するように設計されています。

Q.61

現在 Cisco VPN 3005 コンセントレータを使用しており、同時に 20 セッション（以下）の Web トラフィックを想定しています。32 MB の RAM で十分でしょうか？

A.61

機能すると思われませんが、最大メモリの搭載を推奨します。

Q.62

クラスタ化と負荷分散には Cisco VPN 3000 コンセントレータ ソフトウェア v4.1 が必要ですか？

A.62

負荷分散の機能自体は何年も前から利用できます。Cisco VPN 3000 コンセントレータ ソフトウェア v4.1 では、SSL-VPN における負荷分散が可能になりました。

Q.63

一定時間非アクティブ状態のユーザ接続をタイムアウトにできますか？

A.63

できます。最大値を設定できる接続タイマーと非アクティブ タイマーを使用できます。

Q.64

VPN リモート サイトを構築する場合の推奨シスコ製ハードウェア（DSL ルータ、ローエンドの Cisco PIX セキュリティ アプライアンスなど）を教えてください。

A.64

シスコの機器の利点は、あらゆる環境に対応できることです。リモート サイトで DSL 接続にシスコ製 WAN ルータを使用している場合、VPN 接続にも問題なくそのルータを使用できます。リモート サイトに強力なファイアウォールを提供する Cisco PIX セキュリティ アプライアンスは、強力な VPN 機能も備えています。

Q.65

Cisco VPN 3000 コンセントレータ ソフトウェア v4.1 は、Cisco VPN 3005 コンセントレータにインストールできますか？

A.65

できます。

Q.66

他のファイアウォールを通じて SSL-VPN ソリューションへのトンネルを確立すると何か問題が生じますか？

A.66

一般的に Web トラフィックに必要なポートはファイアウォール上でオープンされ、SSL-VPN は同じポートを使用します。したがって、問題は生じないはずで

Q.67

Cisco Secure Access Control Server (ACS) は Cisco VPN 3000 コンセントレータ シリーズに追加された新機能と、どのように作用しあうのですか？

A.67

Cisco ACS を使用すると、RADIUS やユーザ接続に適用される ACL を利用し、SSL-VPN を通じて接続するユーザを認証できます。

Q.68

SSL-VPN 用に新しい VPN グループを作成する必要がありますか？それとも IPSec で使用している VPN グループを使用できますか？

A.68

SSL-VPN ユーザにも既存のグループ構造を使用できます。

Q.69

Cisco VPN 3000 コンセントレータ サービス アプリケーションに非標準の TCP ポートを使用できますか（TCP1111 を使用するアプリケーションがあります）？

A.69

使用できます。スタティック TCP ポートを使用すれば、TCP ポート転送によって機能させることができます。

Q.70

32 MB の RAM を搭載した Cisco 3005 VPN コンセントレータを使用しています。Cisco VPN 3000 コンセントレータ ソフトウェア v4.1 にアップグレードするには RAM を追加する必要がありますか？



あらゆる環境に対応できるリモート アクセス：

IPSec と SSL-VPN を使用すれば、すべてのユーザにネットワークを拡大できます。

A.70

Cisco 3005 VPN コンセントレータで WebVPN を使用する場合は 64 MB の RAM を推奨します。ただし、ユーザ数が少なければ 32 MB メモリでも機能します。

Q.71

アクセス ポイント からダイナミック VLAN 上のワイヤレス VPN クライアントを設定する場合は、値の割り当てに RADIUS サーバを使用するのですか？ そうであるなら、VPN 終端ポイント（コンセントレータまたはルータ）はこれらの値を単に通過させるだけですか？

A.71

ワイヤレス クライアントを割り当てて動的 VLAN を設定したあと、VLAN を設定する必要があります。その後、VPN トンネルがその VPN ゲートウェイを終端します。

Q.72

Cisco VPN 3000 コンセントレータの各モデルは、トンネル数やパフォーマンスが違うだけで、その他の機能は同じなのですか？

A.72

Cisco VPN 3000 コンセントレータ シリーズの基本的な機能はどれも同じです。

Q.73

Java アプレットが証明されているのはどの Java Virtual Machine ですか？

A.73

Sun Java v1.4 以上の使用を推奨します。

Q.74

SSL-VPN は、複数の Web アプリケーション（HTTP または HTTPS に基づくもの）をサポートできますか？

A.74

できます。

Q.75

Cisco VPN 3000 コンセントレータ ソフトウェア v4.1 をインストールすると、Cisco VPN 3005 コンセントレータのトンネル数の上限は 100 から 200 になりますか？

A.75

はい。Cisco VPN 3000 コンセントレータ ソフトウェア v4.1 によってトンネル数は 200 に増えます。

Q.76

WebVPN を使用した Windows のリモート デスクトップ (Terminal Server) 接続を行うために何か特別な要件はありますか？

A.76

Windows Terminal Service (Cisco RADIUS Data Proxy) をサポートするには、ポート 転送 Java アプレットを使用する必要があります。

Q.77

500 の SSL-VPN 接続によって同じコンセントレータ上の IPSec VPN 接続の上限は減少しますか？ そうだとしたら、どの程度減少するのですか？

A.77

減少します。SSL-VPN と IPSec の接続はそのコンセントレータ内のリソースを消費します。SSL-VPN 接続が追加されると、サポートできる IPSec 接続の数は減ります。

Q.78

アップグレードしていない Cisco 3005 VPN コンセントレータ (64 MB メモリ搭載) シャーシで同時に処理できるユーザ数はいくつですか？

A.78

75 の WebVPN ユーザまたは 200 の IPSec ユーザを処理できます。

Q.79

すべてのクライアント / サーバがポート 1352 を使用する場合、どうすれば WebVPN を通じて複数の Notes サーバにアクセスできますか？

A.79

ポート 転送によってホスト名を対応付ければ、複数の Notes サーバで同時に同じ TCP ポート (1352) を使用できます。

Q.80

ポイント アンド クリック式の管理機能は企業ネットワークの管理ソリューションとして使用するものですか？ それとも個々の VPN コンセントレータを管理するためのソリューションですか？

A.80

VPN Manager はデバイスを設定し、中央集中型でリモート ゲートウェイや VPN クライアントに新しい VPN ポリシーを適用します。これは全社規模で行われます。

Q.81

Cisco VPN 3000 コンセントレータ シリーズの外部インターフェイスからの管理アクセスはどのように制御するのですか？

A.81

いくつかの方法があります。最も安全なのは、コンセントレータへの IPSec 接続を確立し、管理証明書を使用してデバイスを管理する方法です。

Q.82

アプリケーションやサーバなどの制限に関する設定は、WebVPN クライアントとアクセス コンセントレータのどちらで行うのですか？

A.82

アクセス制御は、エンドユーザではなくコンセントレータの管理者が設定します。



あらゆる環境に対応できるリモート アクセス :

IPSec と SSL-VPN を使用すれば、すべてのユーザにネットワークを拡大できます。

- Q.83**
SSL-VPN を通じた接続に使用可能なポートを制限できますか？
- A.83**
できます。WebVPN を使用して、アクセスできる Web サーバと TCP ベース サービスを制限できます。
- Q.84**
Cisco VPN 3000 コンセントレータに適した SSL-VPN アクセラレーションはありますか？
- A.84**
あります。Cisco 3000 コンセントレータに SEP-E アクセラレーション カードを搭載すると、SSL-VPN 暗号化機能がサポートされます。
- Q.85**
ホテルから IPSec を通じて VPN 接続を確立しようとするとう問題が生じます。SSL-VPN によってこの問題を解決できますか？
- A.85**
ほとんどのユーザはホテルから問題なく IPSec 接続を確立していません。特に TCP または UDP のトンネリング オプションを使用すればたいていの場合問題は生じません。その他のセキュア Web サーバにアクセスできるのであれば、SSL-VPN 接続だけが利用できないということは起こらないはずで
- Q.86**
Cisco PIX 515 セキュリティ アプライアンスを使用して IPSec VPN を稼働しています。自宅の DSL 回線を通じてリモート ユーザを追加し、その E メールや個人的なファイルを安全に送信することはできますか？
- A.86**
できます。Cisco PIX 515 セキュリティ アプライアンスはリモート アクセスの IPSec 接続をサポートしています。Cisco IPSec クライアント (無料) があれば、自宅からでもブロードバンド接続を使用して Cisco PIX 515 セキュリティ アプライアンスに安全に接続し、自分のデータ、ファイル、およびアプリケーションにアクセスできます。
- Q.87**
SSL を通じたトンネルにはどのようなプロトコルを使用できますか？
- A.87**
WebVPN の当初のリリースでは、Web サービス (HTTP および HTTPS)、Windows File Share (共通のインターネット ファイルサーバ)、およびポート転送アプレットを使用する TCP ベースのアプリケーション (ほとんどの E メール オプションが含まれる) へのアクセスがサポートされます。
- Q.88**
企業へのトラフィックがすでに暗号化されている場合でもなぜ SSL-VPN が必要なのですか？
- A.88**
SSL-VPN の主要な利点は、VPN クライアント ソフトウェアがなくても、サポート対象のブラウザから企業ネットワークに安全にアクセスできることです。ただし、すべてのアプリケーションが Web 対応とは限らないため、SSL ベースの VPN には使用できないアプリケーションもあります。
- Q.89**
Cisco VPN 3005 コンセントレータのスループットは 4 Mbps です。各ユーザに一定量のスループットが確保されているのですか？ それとも先着順方式なのですか？
- A.89**
コンセントレータの帯域管理機能によって、ユーザ単位でレートを制限することも、先着順方式にすることもできます。
- Q.90**
同じデバイス上で IPSec と SSL-VPN の接続を両方使用できますか？
- A.90**
できます。Cisco VPN 3000 コンセントレータ シリーズでは、1 つのデバイスおよび管理フレームワークで IPSec と SSL-VPN の両方の接続が可能です。要求に応じて適切な技術を選択できます。
- Q.91**
ユーザは複数のグループに属することができますか？
- A.91**
グループによってユーザのアクセス権が定義されます。したがって、ユーザは 1 つのコンセントレータ グループのみに属している必要があります。
- Q.92**
動的な負荷分散、クラスタ化、各種ユーザ認証などの IPSec 機能は、WebVPN でも使用できますか？
- A.92**
できます。WebVPN は、負荷分散、複数デバイスのクラスタ化による必要に応じた拡張、耐障害性、および Cisco VPN 3000 コンセントレータ シリーズがサポートしているすべてのユーザ認証方式 (OTP、RADIUS、NT Domain、Active Directory、SDI、デジタル証明書など) をサポートしています。
- Q.93**
シスコの SSL-VPN 製品では、特定のアプリケーション、サーバ、URL へのユーザのアクセスを制限することは可能ですか？
- A.93**
可能です。WebVPN を通じてユーザ グループに対してきめ細かいアクセス制御が可能です。個々のユーザ グループの要求に応じてアクセスをカスタマイズできます。
- Q.94**
WebVPN はどのように管理するのですか？



あらゆる環境に対応できるリモート アクセス：

IPSec と SSL-VPN を使用すれば、すべてのユーザにネットワークを拡大できます。

A.94

Cisco VPN 3000 コンセントレータの WebVPN 用管理インターフェイスは、IPSec 機能の設定用に組み込まれている HTML ベースのインターフェイスと同じです。WebVPN の機能は、わずかな追加オプションで構成されており、簡単に設定できます。

Q.95

外部インターフェイス（インターネット）から Cisco VPN 3000 コンセントレータへの Web アクセスを停止し、かつ内部ネットワークからのアクセスは許可する方法はありますか？

A.95

管理アクセスと WebVPN アクセスのいずれもインターフェイス単位で制御できます。たとえば、コンセントレータの内部インターフェイスからの管理アクセスのみを許可することが可能です。

Q.96

IPSec over TCP と IPSec over UDP には何か違いがありますか？

A.96

ファイアウォール、または NAT および Port Address Translation (PAT; ポート アドレス変換) 環境でどちらのオプションも選択できます。IPSec/TCP はシスコ独自のプロトコルですが、UDP は現在 IETF のドラフト標準です。IPSec/TCP は、Extended Services Platform (Protocol 50) や UDP では許可されない環境で役立ちます。

Q.97

VPN トンネルを通じてログイン スクリプトを開始することは可能ですか？

A.97

IPSec クライアントの場合、START BEFORE LOGIN または FORCE NETWORKLOGIN オプションでログイン スクリプトを開始できます。

Q.98

SSL-VPN を使用するには Cisco VPN 3000 コンセントレータに証明書を実インストールすることが必要ですか？

A.98

必要です。ブラウザベースのアクセスには証明書が必要です。出荷時には自己署名証明書が付いています。信頼できる証明書をインストールすることもできます。

Q.99

リモート アクセス用に SSL がサポートされているのに、なぜ IPSec が必要なのですか？

A.99

この 2 つの技術は補完的に作用します。SSL は、限定されたアプリケーションへのアクセスに関して、ユーザが安全に接続できるようにします。IPSec は、IP テレフォニーやビデオを含め、実質的にあらゆるアプリケーションへのアクセスを保護します。

Q.100

IPSec を使用して常にネットワークにアクセスしたいと考えています。外出時に社外のマシンから、別のアカウントをセットアップせずに、SSL を使用して会社のネットワークにアクセスできますか？

A.100

できます。これは IPSec と SSL の技術を補完的に使用する典型的な例です。ご使用のユーザ証明書とアクセス権を変更せずに使えます。



自己防衛型ネットワークは人的な攻撃やミスからの保護を提供します。

シスコの統合セキュリティ アプローチについての詳細は、
以下をご覧ください。

<http://www.cisco.com/jp/powernow/security/>

Copyright, 2005 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, Cisco Systems のロゴ、Cisco IOS, Cisco PIX、および SmartNET は、米国および一部の国における Cisco Systems, Inc. または関連会社の登録商標または商標です。この文書または Web サイトで言及している他の商標はいずれも、それぞれの所有者のもので、「パートナー」という用語を使用している場合、シスコシステムズと他社とのパートナー関係を意味するものではありません。(0401R)

CISCO SYSTEMS



THIS IS THE POWER OF THE NETWORK. NOW