Cisco VPN 3000 コンセントレータに関する FAQ

内容

概要

このドキュメントでは、Cisco VPN 3000 シリーズ コンセントレータに関してよく寄せられる質問 (FAQ) への回答を示します。

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

全般

Q.エラーメッセージ「Lost Service」は何を意味しますか。

A. VPNコンセントレータとVPN Clientの間に一定期間送信されたトラフィックがない場合は、ピアが存在することを確認するために、Dead Peer Detection(DPD)パケットがVPNコンセントレータからVPN Clientに送信されます。VPN クライアントが VPN コンセントレータに応答しないような 2 ピア間での接続上の問題がある場合、VPN コンセントレータは一定期間 DPD パケットを送信し続けます。れにより、その間に応答を受け取らないと、トンネルが終了されてエラーが生成されます。Cisco Bug ID CSCdz45586(サポート契約が必要)を参照してください。

エラーは次のようになります。

```
SEV=4 AUTH/28 RPT=381 XXX.XXX.XXX.XX User [SomeUser] disconnected:
Duration: HH:MM:SS Bytes xmt: 19560 Bytes rcv: 17704 Reason:
Lost Service YYYY/MM/DD HH:MM:SS XXX.XXX.XXX.XXX
syslog notice
45549 MM/DD/YYYY HH:MM:SS SEV=4 IKE/123 RPT=XXX.XXX.XXX.XXX
Group [SomeDefault] User [SomeUser]
IKE lost contact with remote peer, deleting connection (keepalive type: DPD)
```

原因：リモート IKE ピアが予測時間枠内でキープアライブに応答しなかったため、IKE ピアへの接続が削除されました。メッセージには、使用されたキープアライブ メカニズムが含まれています。この問題は、アクティブなトンネル セッション中にパブリック インターフェイスが接続解除されている場合にのみ再現可能です。ネットワーク接続の潜在的な問題の根本原因を特定するために、これらのイベントが生成されるので、顧客はネットワーク接続を監視する必要があります。

問題の発生したクライアント PC で %System Root%\Program Files\Cisco Systems\VPN

Client\Profiles に移動して、IKE キープアライブをディセーブルにし、接続用に PCF ファイル（該当する場合）を編集します。

'ForceKeepAlives=0'（デフォルト）を 'ForceKeepAlives=1' に変更します。

問題が続く場合、Cisco テクニカルサポートでサービスリクエストをオープンし、問題が発生した際の VPN コンセントレータのログおよびクライアントの「Log Viewer」を提供してください。

Q. EMQ1キューで検出されたエラーメッセージ「q_send failures detected」は何を意味するのですか。

A.このエラーメッセージは、バッファ内のデバッグイベントや情報が多すぎる場合に表示されます。これにより少数のイベント メッセージが失われる可能性がある以外、悪影響はありません。メッセージを防ぐのに必要な最小の数にイベントを減らすようにしてください。

Q. VPNコンセントレータの設定では、削除したグループがまだ表示されます。これを削除するにはどうすればよいのですか。

A.構成をテキストエディタ（メモ帳など）にコピーし、**[ipaddrgrouppool #.0]で示される影響を受けるグループ情報を手動で編集または削除します。**設定を保存し、VPN コンセントレータにアップロードしてください。次に例を示します。

```
!--- Change to 14.1 or any other number that is not in use !--- any number other than 0).
[ipaddrgrouppool 14.0] rowstatus=1 rangename= startaddr=172.18.124.1 endaddr=172.18.124.2
```

Q.複数のプライマリSDIサーバを使用することはできますか。

A. VPN 3000コンセントレータは、一度に1つのノードシークレットファイルしかダウンロードできません。SDI バージョン 5.0 よりも前では、複数の SDI サーバを追加できますが、すべてのサーバで同じノード シークレット ファイルを共有する必要があります（プライマリおよびバックアップ サーバとして考えてください）。 SDI バージョン 5.0 で入力できるのは、1 つのプライマリ SDI サーバ（バックアップ サーバはノード シークレット ファイルにリストされる）とレプリカ サーバだけです。

Q. 「SSL certificate will expire in 28 days」という表示されます。どうすればよいでしょうか。

A.このメッセージは、Secure Socket Layer(SSL)証明書が28日後に期限切れになることを示しています。この認証は、HTTPS で Web 管理をブラウズする際に使用されます。認証をデフォルト設定のままにするか、さまざまなオプションを設定してから新しい認証を生成できます。これを行**うには、[Configuration] > [System] > [Management Protocols] > [SSL]**を選択します。**[Administration] > [Certificate Management]を選択し**、**[Generate]をクリック**して証明書を更新します。

VPNコンセントレータのセキュリティに懸念があり、不正アクセスを防止する場合は、**Configuration > Policy Management > Traffic Management > Filters**の順に選択して、パブリックインターフェイスでHTTPまたはHTTPSを無効にします。HTTP または HTTPS により、インターネット経由で VPN コンセントレータにアクセスする必要がある場合、Administration > Access Rights > Access Control List を選択して、送信元アドレスに基づいてアクセスを指定できます。

詳細については、ウィンドウの右上にあるヘルプ メニューを使用してください。

Q.内部ユーザデータベースのユーザ情報を表示するにはどうすればよいのですか。コンフィギュレーション ファイルを参照しても表示されません。

A. [Administration] > [Access Rights] > [Access Settings]の順に選択し、[Config File Encryption=None]を選択し、設定を保存してユーザとパスワードを表示します。特定のユーザを検索できます。

Q.内部データベースに保存できるユーザ数はいくつですか。

A.ユーザの数はバージョンによって異なり、ご使用のVPN 3000コンセントレータリリースのユーザガイドのConfiguration > User Managementセクションで指定されます。VPN 3000リリース2.2 ~ 2.5.2では、合計100のユーザまたはグループ（ユーザとグループの合計が100以下）が可能です。VPN 3000リリース3.0以降では、3005および3015コンセントレータの数は10のままです。VPN 3030および3020コンセントレータの場合は500、VPN 3060または3080コンセントレータの場合は1000です。また、外部認証サーバを使用すると、拡張性と管理性が向上します。

Q.トンネルデフォルトゲートウェイとデフォルトゲートウェイの違いは何ですか。

A. VPN 3000コンセントレータは、トンネルデフォルトゲートウェイを使用して、プライベートネットワーク（通常は内部ルータ）内のトンネルユーザをルーティングします。 VPN コンセントレータは、デフォルト ゲートウェイを使用して、インターネット（通常は外部ルータ）にパケットをルーティングします。

Q. VPN 3000コンセントレータを、アクセスコントロールリストを実行しているファイアウォールまたはルータの背後に配置する場合、どのポートとプロトコルの通過を許可する必要がありますか。

A.この図は、ポートとプロトコルを示しています。

サービス	プロトコル番号	送信元ポート	宛先ポート
PPTP 制御接続	6（TCP）	1023	1723
PPTP トンネル カプセル化	47（GRE）	N/A	N/A
ISAKMP/IPSec キー管理	17（UDP）	500	500
IPSec トンネル カプセル化	50（ESP）	N/A	N/A
IPSec NAT 透過性	17（UDP）	10000（デフォルト）	10000（デフォルト）

注：ネットワークアドレス変換(NAT)透過ポートは、4001 ~ 49151の範囲の任意の値に設定でき

ます。バージョン 3.5 以降で IPSec over TCP を設定するには、Configuration > System > Tunneling Protocols > IPSec > IPSec over TCP の順に進みます。最大 10 個の TCP ポート（1～65535）をコンマで区切って入力できます。 このオプションを設定する場合は、これらのポートが、アクセス コントロール リストを実行しているファイアウォールまたはルータで許可されていることを確認してください。

Q. VPNコンセントレータを工場出荷時のデフォルトに戻すにはどうすればよいのですか。

A. [ファイル管理]画面で、「config」ファイルを削除して再起動します。このファイルを誤って削除した場合、バックアップ コピー「config.bak」が残っています。

Q.管理認証にTACACS+を使用できますか。また、使用する場合はどのような点に注意すればよいのですか。

A.はい。VPN 3000コンセントレータリリース3.0以降では、管理認証にTACACS+を使用できます。TACACS+ の設定が完了したら、ログ アウトする前に必ず認証をテストしてください。TACACS+ の設定が誤っているとロック アウトされる可能性があります。そうなると、コンソール ポートからログインして、TACACS+ を無効にして問題を解決する必要があります。

Q.管理パスワードを忘れた場合はどうすればよいのですか。

A. バージョン2.5.1以降では、PCを次のように設定したストレートRS-232シリアルケーブルを使用して、PCをVPNコンセントレータのコンソールポートに接続します。

- 9600 ビット/秒
- 8 データ ビット
- パリティなし
- 1 ストップ ビット
- ハードウェア フロー制御オン
- VT100 エミュレーション

VPN コンセントレータをリブートします。診断チェックが完了すると、コンソールに 3 個のドット（...）のみの行が表示されます。これらのドットが表示されたら、3 秒以内に Ctrl+C キーを押します。システム パスワードをデフォルトにリセットするためのメニューが表示されます。

Q.グループ名とグループパスワードの目的は何ですか。

A.グループ名とグループパスワードは、ハッシュの作成に使用され、そのハッシュはセキュリティアソシエーションの作成に使用されます。

Q. VPNコンセントレータは、トンネルユーザの代わりにARPをプロキシしますか。

A.はい。

Q. VPN 3000コンセントレータは、ネットワークファイアウォールに対してどこに配置すればよいのですか。

A. VPN 3000コンセントレータは、ファイアウォールの手前、背後、平行、非武装地帯(DMZ)に配置できます。同じ Virtual LAN（VLAN; 仮想 LAN）内にパブリック インターフェイスとプライベート インターフェイスを持つことはお勧めできません。

Q. Cisco VPN 3000コンセントレータでプロキシARPを無効にする方法はありますか。

A. Proxy Address Resolution Protocol(ARP)は、Cisco VPN 3000コンセントレータでは無効にできません。

Q. VPN 3000コンセントレータに関するバグはどこで発見できますか。

A.バグ検索ツール(サポート契約が必要)を使用して、バグに関する詳細情報を検索することができます。

Q. VPN 3000コンセントレータの設定例はどこで入手できますか。

A. VPN 3000コンセントレータのマニュアルに加えて、Cisco VPN 3000 Series Concentrator Support Pageに、より多くの設定例が掲載されています。

Q.特定のイベントに対してより良いデバッグを得るためにロギングを増やすにはどうすればよいのですか。

A. [Configuration] > [System] > [Events] > [Classes]に移動し、より良いデバッグを得るために特定のイベント（IPsecやPPTPなど）を設定できます。デバッグを有効にするとパフォーマンスが低下するおそれがあるため、デバッグを有効にするのはトラブルシューティングを実施している間のみにしてください。IPSec のデバッグ時には、IKE、IKEDBG、IPSEC、IPSECDBG、AUTH、および AUTHDBG を有効にします。証明書を使用している場合は、CERT クラスをリストに追加してください。

Q. VPN 3000コンセントレータへのトラフィックをモニタするにはどうすればよいのですか。

A. VPN 3000コンセントレータに付属のHTMLインターフェイスでは、[Monitoring] > [Sessions]の下に基本的なモニタリング機能があります。また、任意の SNMP マネージャを使用して、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）経由で VPN 3000 コンセントレータを監視できます。あるいは、Cisco VPN/Security Management Solution（VMS; VPN/セキュリティ管理ソリューション）を購入できます。 Cisco VMS により、VPN 3000 コンセントレータ シリーズを配備して、IPSec、L2TP、および PPTP に基づくリモート アクセスとサイトツーサイト VPN の詳細なモニタリングを行う必要がある場合に役立つ重要な機能が提供されます。VMS の詳細については、『VPN セキュリティ マネジメント ソリューション』を参照してください。

Q. Cisco VPN 3000コンセントレータシリーズには統合ファイアウォールがありますか。その場合、どんな機能がサポートされますか。

A.このシリーズには、ステートレスポート/フィルタリング機能とNATが統合されていますが、シスコでは、企業のファイアウォールにCisco Secure PIX Firewallなどのデバイスを使用することを推奨しています。

Q. Cisco VPN 3000コンセントレータシリーズでは、どのようなルーティングオプションとVPNプロトコルがサポートされていますか。

A.シリーズでは、次のルーティングオプションがサポートされています。

- Routing Information Protocol（RIP）
- RIP2
- Open Shortest Path First（OSPF）
- スタティック ルート
- Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）

サポートされている VPN プロトコルには、Point-to-Point Tunneling Protocol（PPTP）、L2TP、L2TP/IPSec、および IPSec などがあります。これらはすべて、VPN 3000 とエンド クライアントとの間に NAT デバイスがある場合とない場合の両方に対応しています。NAT を介した IPSec は NAT 透過性と呼ばれます。

Q. Cisco VPN 3000コンセントレータシリーズでは、クライアントPCに対してどのような認証メカニズム/システムがサポートされていますか。

A. NTドメイン、RADIUSまたはRADIUSプロキシ、RSA Security SecurID(SDI)、デジタル証明書、および内部認証がサポートされています。

Q. VPN 3000コンセントレータを通過するユーザに対して、スタティックなネットワークアドレス変換(NAT)を実行できますか。

A. Port Address Translation（PAT；ポートアドレス変換）は、外出するユーザにのみ実行できます。VPN 3000 コンセントレータでは、スタティック NAT は実行できません。

Q. VPN 3000コンセントレータを介して、特定のPoint-to-Point Tunneling Protocol(PPTP)またはIPsecユーザにスタティックIPアドレスを割り当てるにはどうすればよいのですか。

A.このリストでは、スタティックIPアドレスを割り当てる方法について説明します。

- **PPTPユーザ**IP Address Management セクションで、your pool オプションまたは Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル）オプションを選択して、Use Client Address オプションをチェックします。次に、ユーザと、VPN 3000 コンセントレータにおける IP アドレスを定義します。このユーザが接続するときは常に、VPN コンセントレータに設定された IP アドレスが付与されます。
- **IPsecユーザ**IP Address Management セクションで、your pool オプションまたは DHCP オプションを選択して、Use Address from Authentication Server オプションをチェックします。次に、ユーザと、VPN 3000 コンセントレータにおける IP アドレスを定義します。このユーザが接続するときは常に、VPN コンセントレータに設定された IP アドレスが付与されます。同じグループまたは他のグループに属する他のユーザはすべて、グローバル プールまたは DHCP から IP アドレスを付与されます。Cisco VPN 3000 コンセントレータ ソフトウェア バージョン 3.0 以降には、グループ単位でアドレス プールを設定するオプションがあります。この機能は、特定のユーザにスタティック IP アドレスを割り当てる場合にも役立ちます。あるグループにプールを設定した場合、固定 IP を持つユーザにはそのユーザ専用に割り当てられた IP アドレスが付与され、同じグループの他のメンバにはグループ プールから IP アド

レスが付与されます。これが適用されるのは、認証サーバとして VPN コンセントレータを使用する場合のみです。

注：外部認証サーバを使用する場合は、外部サーバを使用してアドレスを正しく割り当てる必要があります。

Q. MicrosoftのPPTP製品とVPN 3000コンセントレータの互換性に関する既知の問題は何ですか。

A.この情報は、VPN 3000シリーズコンセントレータソフトウェアリリース3.5以降に基づいています。VPN 3000シリーズコンセントレータ、モデル3005、3015、3020、3030、3060、3080。および Microsoft オペレーティング システム Windows 95 以降に基づいています。

- **Windows 95 Dial-Up Networking (DUN) 1.2**DUN 1.2では、Microsoft Point-to-Point Encryption (MPPE)はサポートされていません。MPPEを使用して接続するには、Windows 95 DUN 1.3をインストールしてください。Microsoft DUN 1.3アップグレードはMicrosoftのWebサイトからダウンロードできま す。
- **Windows NT 4.0**Windows NT は、VPN コンセントレータへの Point-to-Point Tunneling Protocol (PPTP) 接続について完全にサポートされています。Service Pack 3 (SP3) 以降が必要です。SP3 を実行する場合は、PPTP パフォーマンスおよびセキュリティ パッチをインストールする必要があります。Microsoft PPTP Performance and Security Upgrade for WinNT 4.0 に関する情報は、Microsoft の Web サイトを参照してください。128 ビット Service Pack 5 は MPPE キーを正しく処理しないため、PPTP によるデータの送信が失敗するおそれがあります。これが発生した場合は、イベント ログに次のメッセージが表示されます。

  ```
  103 12/09/1999 09:08:01.550 SEV=6 PPP/4 RPT=3 80.50.0.4
  User [ testuser ]
  disconnected. Experiencing excessive packet decrypt failure.
  ```

  この問題を解決するには、『How to obtain the latest Windows NT Service Pack 6a and Windows NT 4.0 Service Pack 6a Available』のアップグレードをダウンロードしてください。詳細については、Microsoftの記事「MPPE Keys Not Handled Correctly for a 128-Bit MS-CHAP Request 」を参照してください。

Q. VPN 3000コンセントレータで許可されるフィルタの最大数はいくつですか。

A. VPN 30xxユニット (3030または3060であっても) に追加できるフィルタの最大数は100に修正されています。Cisco Bug ID CSCdw86558 (サポート契約が必要) を参照してください。

Q. VPNコンセントレータの30xx回線のルートの最大数はいくつですか。

A.ルートの最大数は次のとおりです。

- 以前、VPN 3005 コンセントレータで保持されていたルートは最大で 200。現在では、この数字は 350 ルートに増加しています。詳細については、Cisco Bug ID CSCeb35779 (サポート契約が必要) を参照してください。
- VPN 3030 コンセントレータでは、最大 10,000 のルートがテストされている。
- VPN 3030、3060、および3080コンセントレータのルーティングテーブルの制限は、各デバイスで使用可能なリソース/メモリに比例します。
- VPN 3015 コンセントレータには、最大制限が事前定義されていない。これは、Routing Information Protocol (RIP; ルーティング情報プロトコル) および Open Shortest Path

First（OSPF）プロトコルについても当てはまります。
- VPN 3020 コンセントレータ：Microsoft の制限により、Windows XP の PC では Classless Static Route（CSR）を大量に受け取ることはできない。 VPN 3000 コンセントレータでは、設定により DHCP INFORM メッセージ応答に挿入される CSR の数が制限されます。VPN 3000 コンセントレータでは、クラスにより、ルートの数を 28 ～ 42 に制限します。

Q. VPN 3000コンセントレータのインターフェイス統計情報を完全にクリアするにはどうすればよいのですか。

A. [Monitoring] > [Statistics] > [MIB-II] > [Ethernet]の順に選択し、統計情報をリセットして現在のセッションの統計情報をクリアします。これでは統計情報が完全にティアダウンされない点に注意してください。（監視目的のリセットに対して）統計情報を実際にリセットするには、リブートする必要があります。

Q. VPNコンセントレータでNetwork Time Protocol(NTP)通信を行うにはどのポートを許可すればよいのですか。

A. TCPおよびUDPポート123を許可します。

Q. UDPポート625xxにはどのような機能がありますか。

A.ポートは、実際のshim / Deterministic NDIS Extender (DNE)とPCのTCP / IPスタックの間のVPN Client通信に使用され、内部開発専用です。たとえば、ポート 62515 は、VPN Client により VPN Client ログに情報を送信する目的で使用されます。その他のポートの機能を次に示します。

- 62514：Cisco Systems, Inc. VPN Service から Cisco Systems IPSec ドライバへ
- 62515：Cisco Systems IPSec ドライバから Cisco Systems, Inc. VPN Service へ
- 62516：Cisco Systems, Inc. VPN Service から XAUTH へ
- 62517：XAUTH から Cisco Systems, Inc. VPN Service へ
- 62518：Cisco Systems, Inc. VPN Service から CLI へ
- 62519：CLI から Cisco Systems, Inc. VPN Service へ
- 62520：Cisco Systems, Inc. VPN Service から UI へ
- 62521：UI から Cisco Systems, Inc. VPN Service へ
- 62522：ログ メッセージ
- 62523：Connection Manager から Cisco Systems, Inc. VPN Service へ
- 62524：PPPTool から Cisco Systems, Inc. VPN Service へ

Q. WebVPNフローティングバーを削除できますか。

A. WebVPNセッションの確立中は、フローティングツールバーを削除したり、フローティングツールバーのロードを回避したりすることはできません。この理由は、このウィンドウを閉じる際にセッションがただちに終了し、再度ログインを試みる際にウィンドウが再びロードされるためです。これは、WebVPN セッションの元々の設計です。メイン ウィンドウを閉じることができますが、フローティング ウィンドウを閉じることはできません。

[ソフトウェア（Software）]

Q. WebVPNはOutlook Web Access(OWA)2003をサポートしていますか。

A. VPN 3000コンセントレータでのWebVPNに対するOWA 2003のサポートは、バージョン4.1.7のダウンロードで利用できます(サポート契約が必要)。

Q. VPN 3000コンセントレータの最新のソフトウェアリビジョンはどこで入手できますか。

A.**すべての**Cisco VPN 3000コンセントレータには最新のコードが付属していますが、ユーザはダウンロード(サポート契約が必要です)を確認して、最新のソフトウェアが利用可能かどうかを確認できます。

VPN 3000 コンセントレータの最新のドキュメンテーションは、『Cisco VPN 3000 シリーズ コンセントレータ』ドキュメンテーション ページを参照してください。

Q. VPN 3000コンセントレータをアップグレードするにはTFTPサーバが必要ですか。ボックスをアップグレードするための代替方法がありますか。

A. TFTPの使用に加え、最新のソフトウェアをハードドライブにダウンロードして、VPNコンセントレータをアップグレードできます。次に、ソフトウェアが配置されたシステムのブラウザで Administration > Software Update の順に進み、ファイルを開く場合と同じ要領で、ハード ドライブにダウンロードしたファイルを探します。 ダウンロードしたファイルが見つかったら、Upload タブを選択します。

Q. 「k9」は最新のコード名(「vpn3000-3.0.4.Rel-k9.bin」など)で何を意味するのですか。

A.**イメージ**名の「k9」の指定は、最初に使用された3DESの指定(vpn3000-2.5.2.F-3des.binなど)に置き換えられました。 したがって「k9」は、これが 3DES イメージであることを意味します。

Q.すべてのユーザに対して、IPsecグループの下の[Data Compression]オプションを使用する必要がありますか。

A.**データ圧縮**により、各ユーザセッションのメモリ要件とCPU使用率が増加し、その結果、VPNコンセントレータの全体的なスループットが低下します。そのため Cisco では、グループの全メンバがモデムで接続するリモート ユーザである場合に限り、データ圧縮を有効にすることをお勧めします。グループの中にブロードバンドを通じて接続するメンバがいる場合は、そのグループのデータ圧縮は有効にしないでください。その代わりにグループを 2 つに分け、1 つをモデム ユーザ、もう 1 つをブロードバンド ユーザにしてください。モデム ユーザのグループに対してのみデータ圧縮を有効にしてください。

その他の高度な機能

Q. LAN-to-LAN接続ではロードバランシングは機能しますか。

A.**ロードバランシング**は、Cisco VPN Software Client（リリース3.0以降）で開始されたリモート セッションでのみ有効です。 他のすべてのクライアント（PPTP、L2TP）と LAN-to-LAN 接続は、ロード バランシングが有効に設定されている VPN コンセントレータに接続できますが、ロード バランシングには参加できません。

Q.コンフィギュレーションファイルからパスワードを復号化するにはどうすればよいのですか。

A. [Configuration] > [System] > [Management Protocols] > [XML]の順に選択して、[administration]に移動します |ファイル管理XML形式を選択します。パスワードを表示するには、同じ名前または異なる名前を使用し、ファイルを開きます。

Q. Virtual Router Redundancy Protocol(VRRP)とロードバランシングを併用できますか。

A. VRRPではロードバランシングを使用できません。VRRP コンフィギュレーションでは、アクティブな VPN コンセントレータが故障しない限り、バックアップ デバイスはアイドルのままです。ロードバランシング設定では、アイドルデバイスはありません。

Q.すべてのリモートアクセスクライアントVPNトラフィックは、企業またはサービスプロバイダーのVPNコンセントレータへの暗号化トンネルを通過する必要がありますか。たとえば、他のサイトへ普通の Web アクセスを実行する場合に、ISP のインターネット接続を通じて直接、オープンにアクセスすることはできますか。

A.はい。この概念は「スプリット トンネリング」と呼ばれます。 スプリット トンネリングでは、暗号化されたトンネルを通じて企業リソースに安全にアクセスできると同時に、ISP のリソースを通じてインターネットに直接アクセスできます（Web アクセスのパスから企業ネットワークが除去されます）。 Cisco VPN 3000 コンセントレータ シリーズは、Cisco VPN Client と VPN 3002 Hardware Client の両方に対してスプリット トンネリングをサポートしています。セキュリティ強化のため、この機能を制御できるのはユーザではなく、VPN コンセントレータの管理者になります。

Q.スプリットトンネリングを使用しても安全ですか。

A.スプリットトンネリングを使用すると、VPNトンネルを介して接続している間にインターネットを参照する便利さが得られます。しかし、企業ネットワークに接続された VPN ユーザが攻撃を受けやすい状況にある場合は危険が生じます。この場合は、各ユーザがパーソナル ファイアウォールを使用することをお勧めします。特定の VPN Client バージョンのリリース ノートに、パーソナル ファイアウォールとの相互運用性に関する情報が記載されています。

Q. Cisco VPN 3000コンセントレータでは、ロードバランシングはどのように機能するのですか。

A.負荷は、アクティブな接続から導き出されたパーセンテージを、設定された最大接続で割って計算されます。ディレクタは、すべての管理LAN-to-LANセッションを維持し、他のすべてのクラスタメンバーのロードを計算し、すべてのクライアントのリダイレクトを処理するという追加（固有）の負荷を負うため、常に負荷が最小になります。

新しく設定された機能クラスタでは、接続が確立される前に、ダイレクタの負荷は約1 %です。したがって、ディレクタは、バックアップの負荷のパーセンテージがディレクタの負荷のパーセンテージよりも大きくなるまで、バックアップコンセントレータに接続をリダイレクトします。たとえば、「アイドル」状態の2台のVPN 3030コンセントレータでは、ダイレクタの負荷が1 %になります。セカンダリには、ダイレクタが接続を受け入れる前に、30個の接続（2 %の負荷）が与えられます。

ディレクタが接続を受け入れることを確認するには、[Configuration] > [System] > [General] > [Sessions]に移動し、接続の最大数を意図的に少ない数に減らして、バックアップVPNコンセントレータにかかる負荷を迅速に増加させます。

Q. VPNモニタで追跡できるヘッドエンドデバイスはいくつですか。

A. VPNモニタは20台のヘッドエンドデバイスを追跡できます。ハブアンドスポーク シナリオでは、リモート サイトからの接続はヘッドエンドで監視されます。情報はハブ ルータ上で追跡できるため、リモート サイトおよびユーザをすべて監視する必要はありません。これらのヘッドエンド デバイスでは、最大 20,000 人のリモート ユーザまたは 2,500 のリモート サイトをサポートできます。スポーク サイトに向かうデュアルホーム VPN デバイスは、監視できる最大 20 台のデバイスのうちの 2 台としてカウントされます。

関連情報

- Cisco VPN 3000 コンセントレータに関するサポートページ
- Cisco VPN 3000 クライアントに関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems