Windows オペレーティングシステムの Cisco QuickVPN インストールのヒント

Quick VPNのインストールのヒントを紹介するビデオについては、 <u>http://youtu.be/hHu2z6A78N8</u>を参照してください。

目的

Cisco QuickVPNは、ネットワークへのリモートアクセス用に設計された無料のソフトウェ アです。PCへのインストールが簡単で、管理が簡単です。QuickVPNは、Windowsオペレー ティングシステム(32ビット版と64ビット版の両方)と互換性があります。QuickVPNが正 しく動作するためには、一連の要件をチェックして、ネットワークとのVPN接続を確認する 必要があります。

この記事では、QuickVPN を適切に実行するための要件とヒントを示し、QuickVPN がネットワークにアクセスする方法について説明します。

適用可能なデバイス

- RV215W
- RV110W
- · RV180/RV180W
- RV120W
- RV220W
- RV016
- · RV042/RV042G
- · RV082
- · RVS4000
- · SA520/SA520W
- SA540
- WRV200
- WRV210
- · WRVS4400N
- Windows XP、Windows Vista、Windows 7

QuickVPNプロセス

次に、QuickVPNがコンピュータでどのように動作するか、およびQuickVPNを実行する前 に要件を満たすことが重要である理由について説明します。

1.クライアントはSSL(Secure Socket Layer)を使用してルータに接続します。接続はポート 番号443または60443(ルータのVPN設定に応じて)を使用し、証明書を検索します。詳細 については、「<u>ルータの要件</u>」のセクションを参照してください。

注:証明書を使用する場合は、証明書がコンピュータに保存されていることを確認してくだ さい。そうでない場合は、証明書の警告メッセージが表示されたときに証明書を使用しない 場合は、Noをクリックします。

2.クライアントのユーザ名とパスワードはルータによって認証されます。ユーザが認証され ると、IPSecトンネルが確立されます。

注:VPNにログインできない場合は、エラーメッセージが表示されます。

3.クライアントは、ICMPエコー要求パケットをルータの内部IPアドレスに送信します。ル ータはICMPエコー応答パケットで応答します。この目的は、両端の間に接続を確立するこ とです。このため、ICMPの適切な要件を設定するために(ご使用のオペレーティングシス テムに応じて)確認する必要があります。詳細については、「<u>Windows Vistaまたは</u> <u>Windows 7オペレーティングシステムの要件</u>」の項を参照してください。

注:接続が失敗すると、「Remote Gateway Not Responding」エラーメッセージが表示されます。

ルータの要件

スモールビジネス向けルータが満たす必要がある要件のリストを次に示します。

・ポート443および60443に対してリモート管理を有効にする必要があります。

・ユーザはVPNトンネルを作成して有効にする必要があります。

・ユーザー名とパスワードは大文字と小文字の区別があり、接続の両端で一致している必 要があります。

・各ユーザーアカウントに許可される接続は1つだけです。

・ローカルネットワークサブネットはリモートネットワークサブネットと異なっている必 要があります。

・証明書を使用している場合は、証明書ファイルをコンピュータのQuickVPN Clientフォル ダに保存する必要があります。

Windows Vista/Windows 7オペレーティングシステムの要件

ステップ 1:コンピュータにWindows Vistaがインストールされている場合は、Windows 7のService Pack 2またはVista Service Pack 2の互換性がインストールされている必要があ ります。これを確認するには、Start > Computer System Propertiesの順に選択します。コン ピュータにWindows 7がインストールされている場合は、この手順をスキップしてください 。

注: Windows Vistaの場合、Service Packがインストールされていない場合は、Start > All Programs > Windows Updateの順に選択してシステムを更新してください。



ステップ 2: Windowsファイアウォールを有効にする必要があります。これを確認するには、Start > Control Panel > System and Security > Windows Firewallの順に選択します。



ステップ 3: ICMP(Internet Control Message Protocol)パケット転送を許可するルールを作 成する必要があります。これを行うには、Start > Control Panel > System and Security > Windows Firewall > Advanced Settingsの順に選択します。Windows Firewall with Advanced Securityウィンドウが開きます。

Windows Firewall wit	th Advanced Security		
File Action View	Help		
Windows Firewall w Inbound Rules Outbound Rules Connection S Monitoring	New Rule Filter by Profile Filter by State Filter by Group View Refresh Export List	 Rules TCP-In) JDP-In) Desktop Soft Desktop Soft Desktop Soft Desktop Soft Desktop Soft Desktop Soft 	Actions Inbound Rules • Inbound Rules
<	Help	vice our service our Service	P Help

ステップ 4:Inbound Rulesで右クリックして、New Ruleを選択します。「新規インバウン ド規則ウィザード」ページが開きます。

Prew Inbound Rule Wizard	1
Rule Type Select the type of firewall rule to	create.
Steps: Program Protocol and Ports Scope Action Profile Name	What type of rule would you like to create? Program Rule that controls connections for a program. Predefined: Connect to a Network Projector Rule that controls connections for a Windows experience. (a Custor) Custor rule. Leam more about rule types (a Back Next > Cancel)

ステップ 5:カスタムルールを作成するには、Customをクリックします。

Mew Inbound Rule Wizar	ł				
Protocol and Ports Specify the protocols and ports	to which this rule applies.				
Steps: Rule Type Program	To which ports and protocols does this rule apply?				
Protocol and Ports	Protocol type:	ICMPv4			
ScopeAction	Protocol number:	Any Custom HOPOPT			
ProfileName	Local port:	ICMPv4 IGMP TCP UDP IPv6			
	Remote port:	IPv6-Route IPv6-Frag GRE ICMPv6 IPv6-NoNot IPv6-Opts			
	Internet Control Message (ICMP) settings:	VRRP PGM L2TP			
	Learn more about protoco	I and ports			
	< Ba	ck Next > Cancel			

手順 6 : Protocol Typeドロップダウンリストで、ICMPv4を選択します。

注:その他のフィールドは、デフォルト設定のままにしておくことができます。

Prew Inbound Rule Wizard	
Name Specify the name and description	of this rule.
Steps: Program Protocol and Ports Scope Action Profile Name	Name: ICMP Echo Request Description (optional):
	< Back Finish Cancel

手順7:Nameフィールドに、このルールを説明する名前を入力します。

ステップ 8 : [Finish] をクリックします。

ステップ 9: IPSecサービスを実行している必要があります。これを確認するには、Startを クリックし、Search Programs and Filesフィールドにmsconfigと入力します。System Configurationウィンドウが開きます。

ľ				System C	Configura	ation		
General	Boot	Services	Startup T	ools				
	up select Iormal st .oad all d Nagnostic .oad bas	tion artup device drive c startup ic devices a	rs and servic nd services o	es nly				
• s	elective Loa Loa Use	startup d system se d startup it e original bo	ervices ems ot configurat	on				
					OK	Cancel	Apply	Help

ステップ 10: Servicesタブをクリックして、IPSec Policy Agentが有効になっていることを 確認します。有効になっていない場合は、IPSec Policy Agentチェックボックスをオンにし て、IPSecサービスを許可します。

		Date Disabled		
Microsoft Corporation	Stopped			
Microsoft Corporation	Runnina			
Microsoft Corporation	Running			
Microsoft Corporation	Running			
Microsoft Corporation	Stopped			
Microsoft Corporation	Stopped			
Microsoft Corporation	Stopped		12-	
Microsoft Corporation	Stopped			
Microsoft Corporation	Running			
Microsoft Corporation	Stopped			
Microsoft Corporation	Running			
Microsoft Corporation	Runnina		~	
s may not be disabled.	Enable all Disable		e all	
	Microsoft Corporation Microsoft Corporation	Microsoft Corporation Running Microsoft Corporation Running Microsoft Corporation Running Microsoft Corporation Running Microsoft Corporation Stopped Microsoft Corporation Running Microsoft Corporation Running	Microsoft Corporation Running Microsoft Corporation Running Microsoft Corporation Running Microsoft Corporation Running Microsoft Corporation Stopped Microsoft Corporation Running Microsoft Corporation Run	

ステップ 11[Apply] をクリックして設定を保存します。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。