Konfigurieren eines Secure Sockets Layer Virtual Private Network

Überblick

Ein Secure Sockets Layer Virtual Private Network (SSL VPN) sorgt für sichere Verbindungen zu Netzwerkressourcen über das öffentliche Internet. Dabei wird das Hypertext Transfer Protocol Secure (HTTPS) verwendet. Über ein SSL VPN können Benutzer sichere Remotezugriffs-Sitzungen von nahezu allen Internet-Browsern herstellen. SSL arbeitet auf einer Ebene zwischen der Transmission Control Protocol (TCP)-Ebene und den Protokollen auf Anwendungsebene. SSL nutzt den TCP-Port 443, der normalerweise sowohl an der lokalen als auch an der Remote-Firewall geöffnet ist. So können Remote-Benutzer leicht und sicher auf entfernte Netzwerkressourcen zugreifen.

Mit der SSL VPN-Lösung können die Netzwerkressourcen auf flexible und äußerst sichere Weise auf nahezu alle Remote-Benutzer erweitert werden, die Zugriff auf das Internet und einen Webbrowser haben. Durch die Verwendung eines standardmäßigen webbasierten Zugriffs werden die Kosten für den Desktop-Support reduziert und die Verwaltung vereinfacht.

Beschriebene Produkte

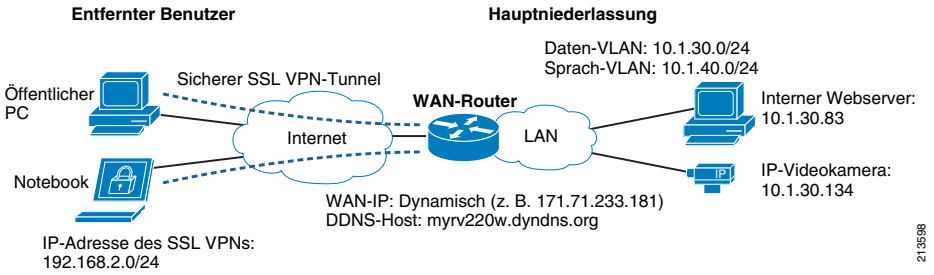
- Cisco RV220W Wireless-N Netzwerksicherheits-Firewall-Router – Unterstützt standardmäßig fünf SSL VPN-Verbindungen gleichzeitig

Netzwerktopologie

Abbildung 1 zeigt eine Beispiel-Implementierung für ein SSL VPN mit einem Cisco Small Business-Router der Serie RV220. Entfernte Internetbenutzer stellen über einen sicheren SSL VPN-Tunnel eine Verbindung zum SSL VPN her und können dann auf interne Server und Netzwerkressourcen zugreifen. Diese sind in der Regel durch eine Firewall, die auf dem Cisco WAN-Router ausgeführt wird, vor einem öffentlichen Zugriff geschützt.

Der Cisco WAN-Router stellt darüber hinaus Routing-Funktionen zwischen unterschiedlichen VLANs zur Verfügung, darunter das Daten-VLAN (30), das Sprach-VLAN (40) und das Verwaltungs-VLAN (60). Im vorliegenden Beispiel umfasst das Daten-VLAN einen internen Webserver (*10.1.30.83*) und eine IP-Videokamera (1*0.1.30.134*).

Abbildung 1 SSL VPN mit einem Cisco Small Business-Router der Serie RV220



Hauptmerkmale

- **SSL VPN-Tunnel-Modus** – Der SSL VPN-Tunnel-Modus überträgt Daten auf Netzwerk- (IP)-Ebene und kann deshalb alle IP-basierten Anwendungen unterstützen. Zum Aktivieren des Tunnel-Modus müssen Sie auf einen Link auf der Portal-Seite klicken, um den SSL VPN-Client für den Tunnel-Modus vom SSL VPN-Server herunterzuladen. Sie können die Client-Software vom entfernten Laptop oder PC entfernen, wenn die SSL VPN-Sitzung beendet ist, oder sie installiert lassen.
- **SSL VPN-Port Forwarding (ohne Tunnel)** – Beim SSL VPN-Port Forwarding-Modus werden Daten auf Anwendungsebene weitergeleitet. Dabei werden spezifische TCP-Ports wie der TCP-Port 80, 25 usw. verwendet. In diesem Modus ist der Remotezugriff auf TCP-basierte Anwendungen möglich, die bekannte feste Ports verwenden, z. B. Post Office Protocol 3 (POP3), Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP), Telnet und Secure Shell (SSH). Dieser Modus kann nicht für Anwendungen genutzt werden, die dynamisch zugewiesene Ports verwenden, z. B. FTP. Sie können auf einen Link auf der SSL VPN-Portalseite klicken, um den Port Forwarding-Client herunterzuladen. Die Konfiguration des SSL VPN-Servers umfasst eine Reihe spezifischer Server wie Web- und E-Mail-Server, auf die Benutzer Zugriff haben.

Tipps zur Ausführung

- **WAN-IP-Adresse und DDNS** – Remote-Benutzer müssen über das öffentliche Internet auf die WAN-Schnittstelle des SSL VPN-Routers zugreifen, sodass eine statische WAN-IP-Adresse bevorzugt wird. Wenn die WAN-IP-Adresse dynamisch vom Internet Service Provider (ISP) empfangen wird, konfigurieren Sie den Dynamic Domain Name Service (DDNS)-Dienst, und verwenden Sie den Hostnamen des Routers für den Zugriff auf den SSL VPN-Router.
- **Tunnel- oder Port Forwarding-Modus** – Der Tunnelmodus ist die empfohlene Option für kleine und mittlere Unternehmen, da dieser Modus die meisten Funktionen bietet. Sie können bei Bedarf allerdings auch den anderen Modus verwenden, um die Anforderungen einer spezifischen Bereitstellung zu erfüllen.
- **Verschlüsselung und Zertifikat** – Ein SSL VPN nutzt ein serverseitiges digitales Zertifikat für die Verschlüsselung. Dieses verwendet den höchsten Verschlüsselungsgrad, der mit dem Webbrowser des Clients ausgehandelt werden kann. Der SSL VPN-Router kann sein eigenes Zertifikat generieren (*selbst unterzeichnetes Zertifikat*). Darüber hinaus kann er ein vorhandenes digitales Zertifikat importieren, wenn das Unternehmen dieses bereits ausgegeben hat.
- **VPN-Benutzerauthentifizierung** – Bei einer SSL VPN-Implementierung werden eine Reihe unterschiedlicher Verfahren zur Benutzerauthentifizierung unterstützt. Die Verwendung der lokalen Benutzerdatenbank stellt eine einfache Methode dar. Dabei müssen Sie jeden Benutzer und jedes Kennwort manuell zur Datenbank hinzufügen. Das SSL VPN unterstützt darüber hinaus die Verwendung externer Authentifizierungsserver wie RADIUS, NT Domain oder Active Directory. So kann die vorhandene IT-Infrastruktur zur Netzwerkverwaltung verwendet werden.
- **IP-Adresse des VPN-Clients** – Der IP-Adresse des SSL VPN-Clients sollte eine separate Netzwerkadresse zugeordnet werden. Im vorliegenden Beispiel wird *192.168.2.0/24* als IP-Adresse des SSL VPN-Clients verwendet.
- **Split-Tunneling** – Split-Tunneling kann aktiviert werden, damit nur der Verkehr zum VPN-Server verschlüsselt und über den SSL VPN-Tunnel weitergeleitet wird. So wird die Last auf der VPN-Server-Seite reduziert und die Netzwerkleistung erhöht.

Konfigurieren eines SSL VPNs auf einem Cisco Small Business-Router der Serie RV220W

Checkliste für die Vorkonfiguration

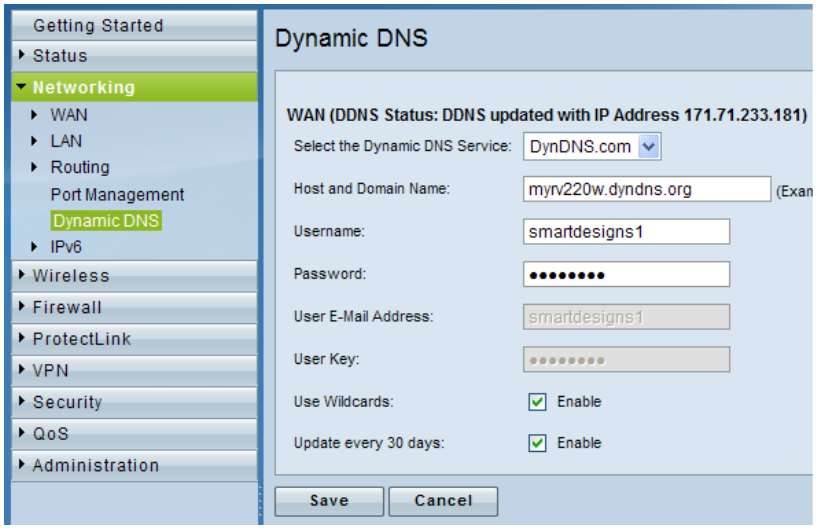
Weitere Informationen zum Abschließen der ursprünglichen Konfiguration des Routers der Serie RV220W finden Sie im RV220W Administrator Guide.

1. Stellen Sie sicher, dass der WAN-Router über aktive Internet-Verbindungen verfügt. Die Network Address Translation (NAT) und eine Firewall sollten aktiviert sein.
2. Stellen Sie die LAN-Konnektivität zwischen dem Router, dem Switch und den lokalen IP-Geräten sicher. Die Daten-, Sprach- und Verwaltungs-VLANs auf dem RV-Router und den Switches müssen ordnungsgemäß konfiguriert sein. Die VLAN-weiten Routing- und Trunking-Funktionen für die einzelnen VLANs müssen funktionsfähig sein. Außerdem muss der DHCP-Dienst für jedes VLAN funktionsfähig sein.
3. Stellen Sie sicher, dass die internen PCs, Server und anderen IP-Geräte mit dem LAN-Switch oder den Switch-Ports des RV-Routers verbunden sind. Vergewissern Sie sich, dass die PCs und Server miteinander kommunizieren und auf das öffentliche Internet zugreifen können.
4. Stellen Sie eine Verbindung mit einem internen Webserver und einer WVC210-IP-Kamera im Daten-VLAN her (z. B. in der Hauptniederlassung im vorliegenden Beispiel), und richten Sie diese ein.

Aktivieren des DDNS (Optional)

Wenn eine statische WAN-IP-Adresse verwendet wird, oder der DDNS-Dienst auf dem WAN-Router bereits konfiguriert ist, überspringen Sie diesen Schritt. Wenn die WAN-Schnittstelle eine dynamische IP-Adresse vom Service Provider erhält, kann DDNS für den Client verwendet werden, damit dieser mithilfe eines Hostnamens auf den SSL VPN-Server zugreifen kann. Gehen Sie zu **Networking** > **Dynamic DNS**, um die DDNS-Einstellungen zu konfigurieren (siehe Abbildung 2). Weitere Einzelheiten finden Sie in Smart Tips: Enabling WAN Public Access with DDNS and Port Forwarding.

Abbildung 2 Seite „Dynamic DNS“

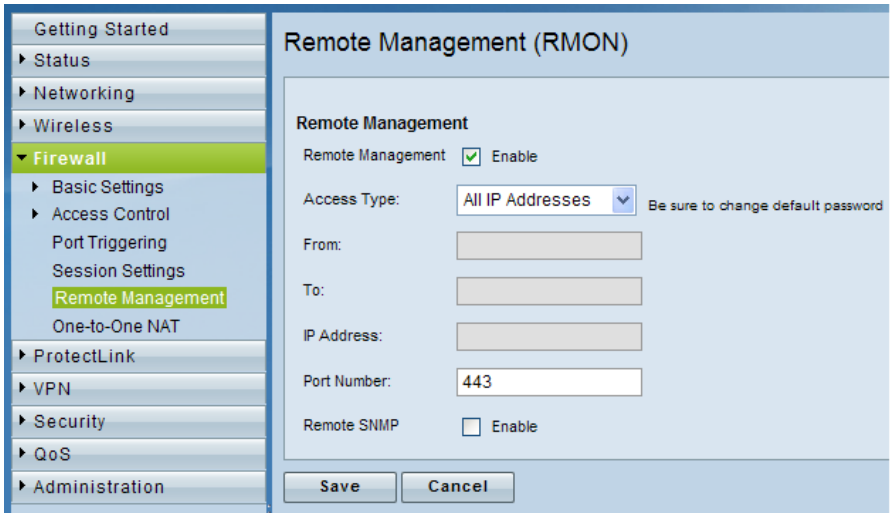


Aktivieren der Remoteverwaltung

Bevor ein SSL VPN implementiert werden kann, muss die Remoteverwaltung auf dem Cisco Router der Serie RV220W aktiviert werden. Dank der Remoteverwaltung können Remote-Benutzer mithilfe des HTTPS-Protokolls eine Verbindung zur WAN-Schnittstelle des Routers herstellen. Dies ist eine Voraussetzung für das SSL VPN.

Schritt 1 Um die Remoteverwaltung zu aktivieren, gehen Sie zu **Firewall > Remote Management,** und legen Sie als „Access Type“ die Einstellung *All IP Address,* fest, da die IP-Adressen vom Client größtenteils unbekannt sind. Behalten Sie die Portnummer 443 bei. Dies ist die Standardnummer für das HTTPS-Protokoll. (Siehe Abbildung 3).

Abbildung 3 Aktivieren der Remoteverwaltung

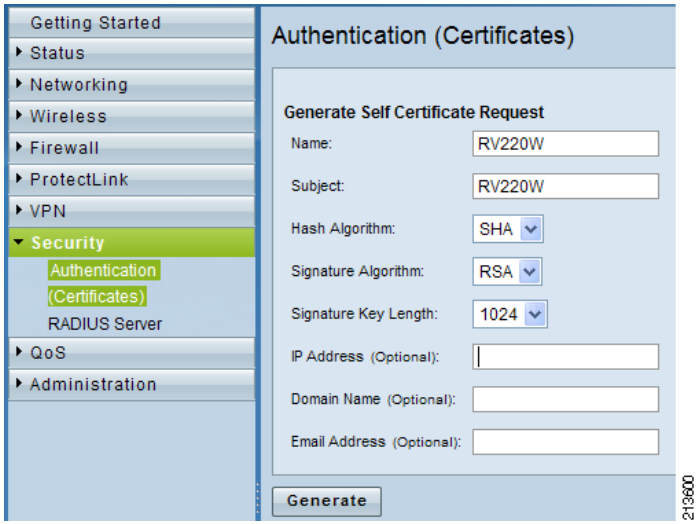


Schritt 2 Gehen Sie zu **Security > Authentication (Certificates)**. (Siehe Abbildung 4.)

Schritt 3 Klicken Sie im Bildschirm „Generate Self Certificate Request“ auf **Generate Certificate**, um ein benutzerdefiniertes digitales Zertifikat hinzuzufügen.

Das digitale Zertifikat wird vom HTTPS-Protokoll für die Authentifizierung und Verschlüsselung benutzt.

Abbildung 4 Generieren einer Anforderung für ein eigenes Zertifikat



Konfigurieren von SSL VPN-Gruppen und -Benutzern

Für die SSL VPN-Authentifizierung müssen SSL VPN-Benutzer und -Gruppen erstellt werden. Im vorliegenden Beispiel werden mithilfe der Standard-SSL VPN-Gruppe die SSL VPN-Benutzer in der lokalen RV220W-Datenbank erstellt.

Schritt 1 Zum Ändern des Standard-Administrator-Kennworts gehen Sie zu **Administration > Password Complexity**, um **enforce Password Complexity** zu aktivieren.

Schritt 2 Gehen Sie zu **Administration > Users > Users**, um das Standard-Kennwort für Administrator-Benutzer zu ändern.

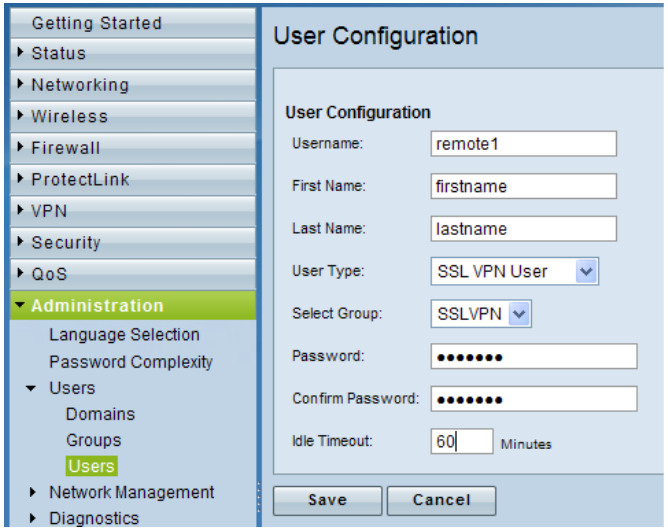
Schritt 3 Gehen Sie zu **Administration > Users > Users**, um neue SSL VPN-Benutzer hinzuzufügen. Eine Standard SSL VPN-Gruppe ist bereits vorhanden. Klicken Sie auf **Add**, um eine neue Seite für die Benutzerkonfiguration anzuzeigen.

Schritt 4 Gehen Sie auf der Seite „User Configuration“ (siehe Abbildung 5) wie folgt vor:

a. Geben Sie den Benutzernamen (Vor- und Nachname) ein, wählen Sie als Benutzertyp SSL VPN User und als Gruppe SSLVPN aus, und geben Sie dann das Kennwort (Password) und den Wert für das Leerlauf-Timeout (Idle Timeout) ein.

b. Klicken Sie auf Speichern.

Abbildung 5 Seite „User Configuration“



Schritt 5 Fügen Sie, wie in Schritt 3 beschrieben, der gleichen Gruppe weitere SSL VPN-Benutzer hinzu.

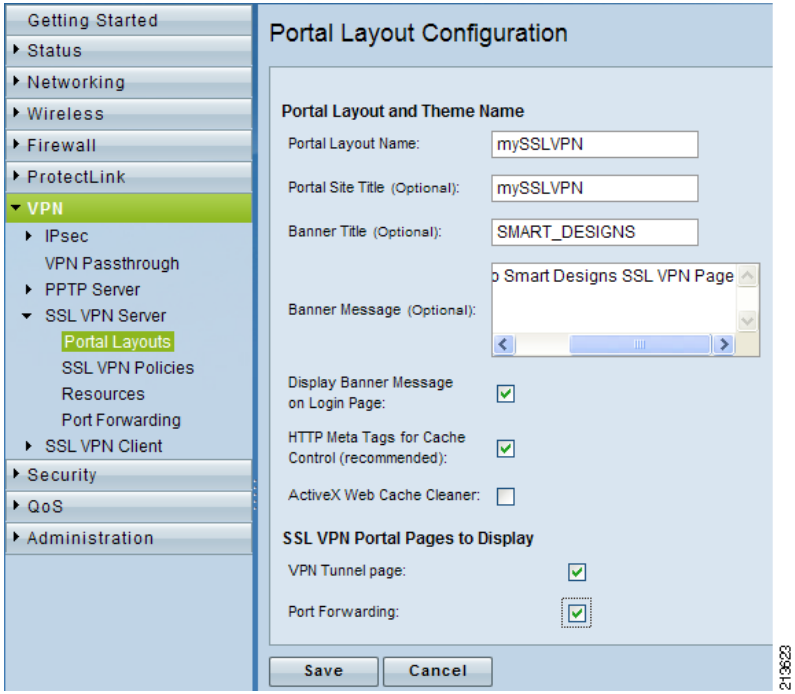
Anpassen der Portalseite für den SSL VPN-Server (optional)

Der SSL VPN-Server wird standardmäßig nach der Aktivierung der Remoteverwaltung aktiviert. Auf dem Cisco RV220W-Router ist bereits eine Standard SSL-Portalseite konfiguriert. Eine neue Portalseite kann hinzugefügt oder die Standardseite kann geändert werden. Gehen Sie dazu wie folgt vor.

Schritt 1 Gehen Sie zu **VPN > SSL VPN Server > Portal Layouts,** und klicken Sie auf **Add**.

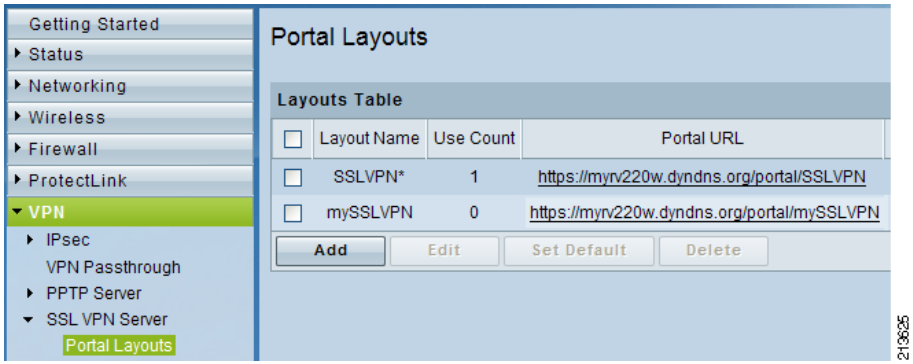
Schritt 2 Passen Sie den Seitennamen, den Titel, die Banner-Überschrift und die Symbole an. (Siehe Abbildung 6).

Abbildung 6 Seite „Portal Layout Configuration“



Schritt 3 Gehen Sie zu **VPN > SSL VPN Server > Portal Layouts**, um eine Zusammenfassung und die URL anzuzeigen.

Abbildung 7 Fenster „Portal Layouts“



Hinzufügen von SSL VPN-Richtlinien (optional)

SSL VPN-Richtlinien sind nützlich, wenn Sie den Zugriff auf spezifische Netzwerk-Ressourcen, IP-Adressen oder IP-Netzwerke zulassen oder verweigern möchten. Sie können auf Benutzer- oder Gruppenebene oder global definiert werden. Standardmäßig wird eine globale PERMIT-Richtlinie (nicht gezeigt) für alle Adressen und alle Services/Ports konfiguriert.

Die spezifischste Richtlinie für einen bestimmten Besitzer hat Vorrang vor weniger spezifischen Richtlinien. Wenn keine Richtlinien für einen Benutzer konfiguriert sind, werden die damit verknüpften Gruppenrichtlinien angewandt. Sind für die Gruppe ebenfalls keine Richtlinien konfiguriert, werden die globalen Richtlinien angewandt.

Schritt 1 Gehe Sie zu **VPN > SSL VPN Server > SSL VPN Policies**, und klicken Sie auf **Add**.

Schritt 2 Aktivieren Sie auf der Seite „SSL VPN Policy Configuration Page“ (siehe Abbildung 8) die Richtlinie für die Ebene „Global“, „Group“ oder „User“. Wählen Sie dort die jeweilige Gruppe oder den Benutzer aus.

Eine Richtlinie kann auf eine spezifische IP-Adresse oder ein spezifisches IP-Netzwerk, alle IP-Adressen oder eine Netzwerkquelle (ein vordefinierter Dienst auf der Basis einer IP- oder Netzwerk-Adresse und eines Port-Bereichs) angewendet werden.

Schritt 3 Legen Sie einen Port-Bereich oder eine Port-Nummer fest, wählen Sie den Service aus (Tunnel- oder Port Forwarding oder beide), und wählen Sie als Berechtigung *permit* oder *deny* aus.

Abbildung 8 zeigt eine hinzugefügte Richtlinie, die den SSL VPN-Zugriff für die IP-Kamera 10.1.30.134 zulässt, während Abbildung 9 anzeigt, dass der Zugriff für alle anderen verweigert wird. Befolgen Sie dieselben Schritte, um den Zugriff auf den internen Webserver 10.1.30.83 zuzulassen.

Abbildung 8 Zulassen des SSL VPN-Zugriffs

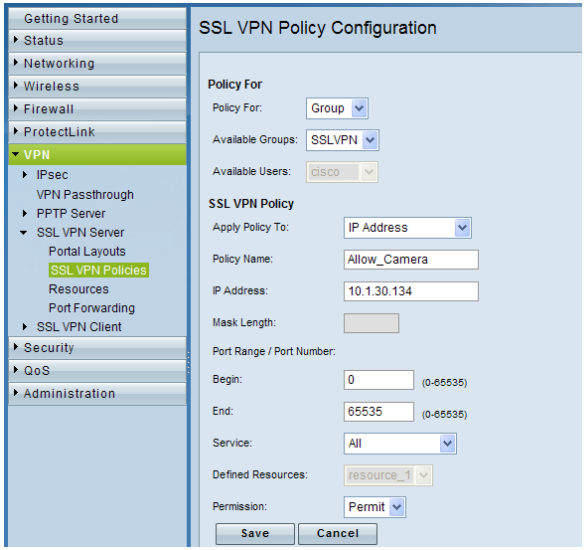
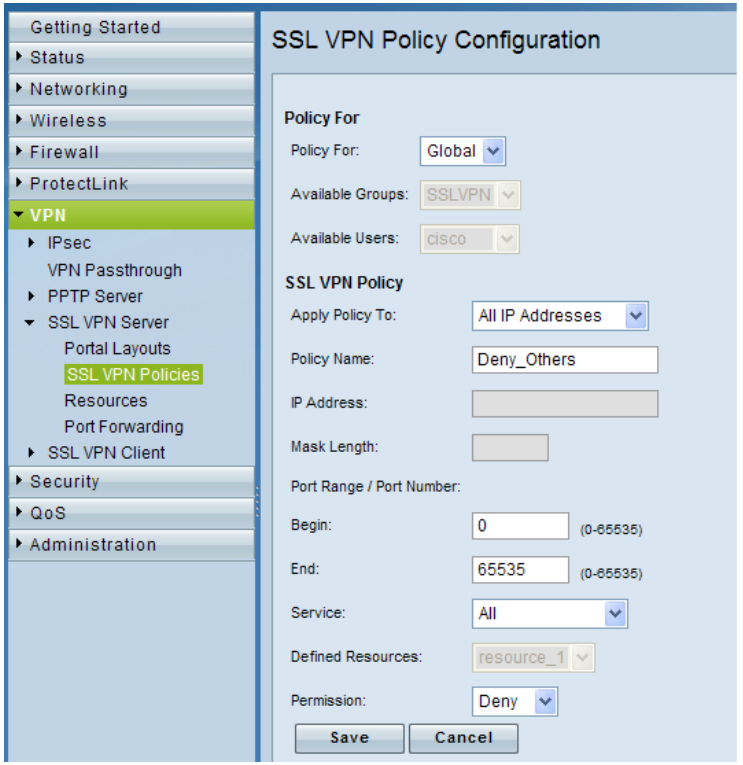


Abbildung 9 Verweigern des SSL VPN-Zugriffs



Nach der Durchführung der oben beschriebenen Schritte ist die SSL VPN-Serverkonfiguration für den Tunnelmodus abgeschlossen. Der Port Forwarding-Modus kann ebenfalls als weitere Option konfiguriert werden, wie im nächsten Abschnitt gezeigt.

Konfigurieren des SSL VPN-Port Forwarding-Modus (optional)

Obwohl der SSL VPN-Tunnelmodus dringend empfohlen wird, kann unter bestimmten Bedingungen auch der SSL-Port Forwarding-Modus konfiguriert werden.

Schritt 1 Gehen Sie zu **VPN > SSL VPN Server > Port Forwarding**, um die IP-Adresse und den TCP-Port des lokalen Servers hinzuzufügen.

In den in Abbildung 10 und Abbildung 11 gezeigten Beispielen werden die HTTP- und HTTPS-Ports für den lokalen Webserver 10.1.30.83 hinzugefügt.

Abbildung 10 Bildschirm „Port Forwarding“ (1)

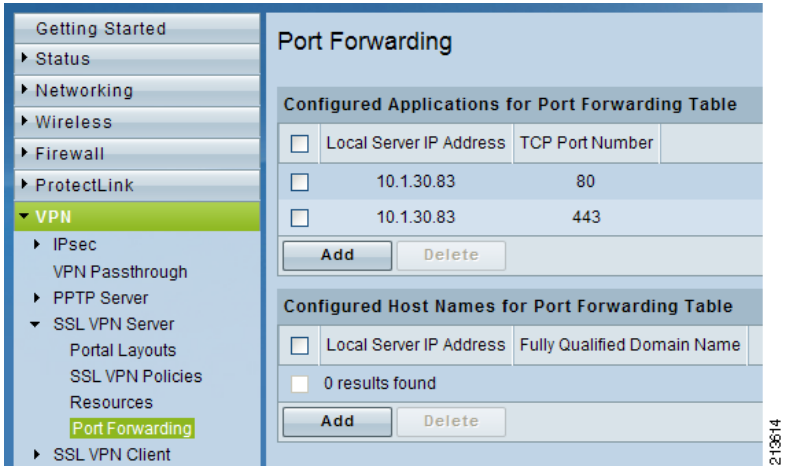


Abbildung 11 Bildschirm „Port Forwarding“ (2)

Konfigurieren des WAN-Routers zum Anpassen des SSL VPN-Clients

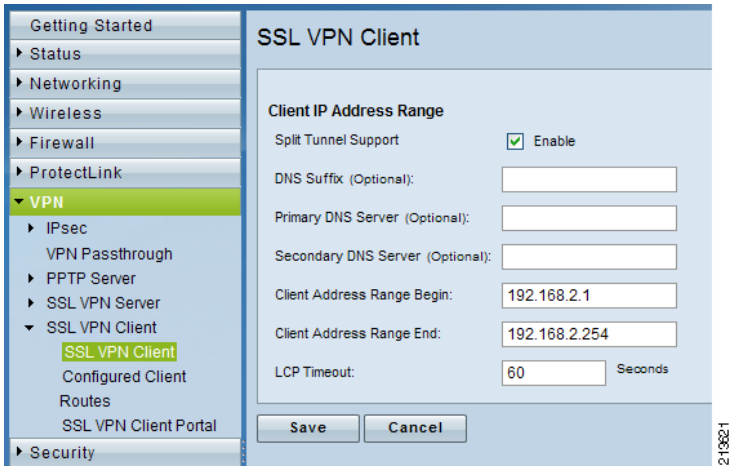
Der IP-Adresspool des SSL VPN-Client kann geändert werden. Die Standard-Netzwerkadresse für den SSL VPN-Client lautet 192.168.254.0. Split-Tunneling kann auch auf dem SSL VPN-Client aktiviert werden, sodass nur der Datenverkehr zur Hauptniederlassung (10.1.30.0/24) über den SSL VPN-Tunnel weitergeleitet wird.

Schritt 1 Um die IP-Adresse des SSL VPN-Clients zu ändern, gehen Sie zu **VPN > SSL VPN Client > SSL VPN Client**, und ändern Sie den Anfangs- und Endbereich für die Client-Adresse.

In diesem Beispiel wird die Client-IP-Adresse in *192.168.2.0* geändert.

Schritt 2 Aktivieren Sie **Split Tunnel Support**. (Siehe Abbildung 12).

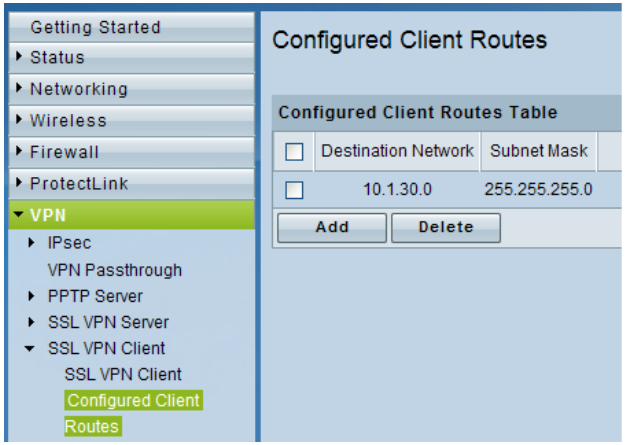
Abbildung 12 Seite „SSL VPN Client“



Schritt 3 Gehen Sie zu **to VPN > SSL VPN Client > Configured Client Routes**, um die Routen für den Client hinzuzufügen. (Siehe Abbildung 13).

Im vorliegenden Beispiel wird die IP-Adresse des Daten-VLAN (10.1.30.0/24) zur Tabelle mit den Client-Routen hinzugefügt.

Abbildung 13 Seite „Configured Client Routes“



Verwenden des SSL VPN-Clients auf PCs/Laptops

Verwenden des SSL VPN-Clients im Tunnelmodus

Schritt 1 Öffnen Sie im Webbrowser eines mit dem Internet verbundenen Client-PCs oder -Laptops die SSL VPN-Portalseite des Cisco Routers der Serie RV220W. Verwenden Sie hierzu entweder die IP-Adresse oder den DDNS-Hostnamen.

Die URL für die jeweilige Portalseite ist unter **VPN > SSL VPN Server > Portal Layouts** aufgeführt. Zum Beispiel:

`HTTPS://myrv220w.dyndns.org/portal/SSLVPN`

Hinweis Webbrowser müssen so konfiguriert sein, dass nicht signierte Active X-Steuerelemente für die vertrauenswürdige Site ausgeführt werden, um auf Portalseite des SSL VPN-Clients zuzugreifen. Ausführliche Anweisungen hierzu finden Sie unter https://supportforums.cisco.com/docs/DOC-9376.

Schritt 2 Wenn die Anmeldeseite angezeigt wird, melden Sie sich mit einer zuvor vom Administrator erstellten SSL VPN-Benutzer-ID und einem zuvor erstellten Kennwort an.

Nach der erfolgreichen Anmeldung wird die SSL VPN-Portalseite angezeigt.

Schritt 3 Gehen Sie zur Seite „VPN Tunnel“, und klicken Sie auf das Symbol  . (Siehe Abbildung 14.)

Für den Internet Explorer-Browser muss ActiveX installiert sein. Wenn eine Sicherheitswarnung beim IE angezeigt wird, klicken Sie auf **Install** (siehe Abbildung 15).

Abbildung 14 Seite „VPN Tunnel“

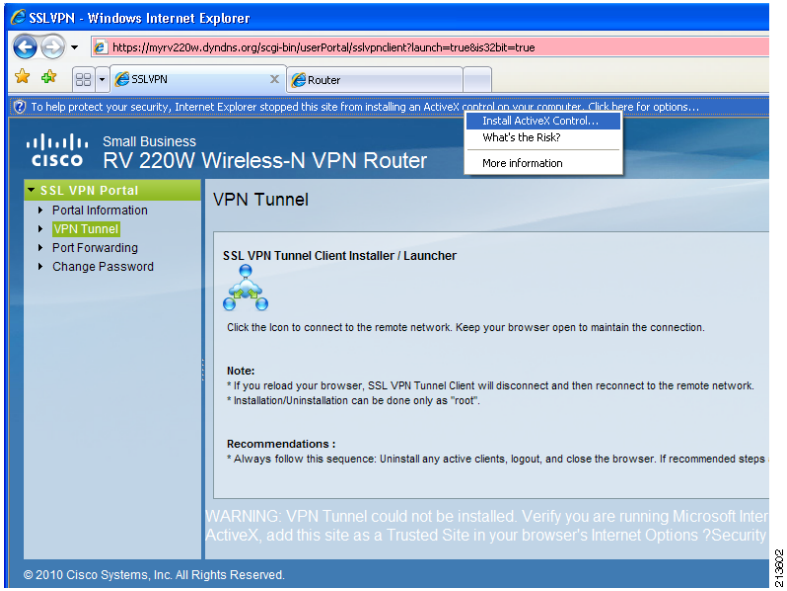
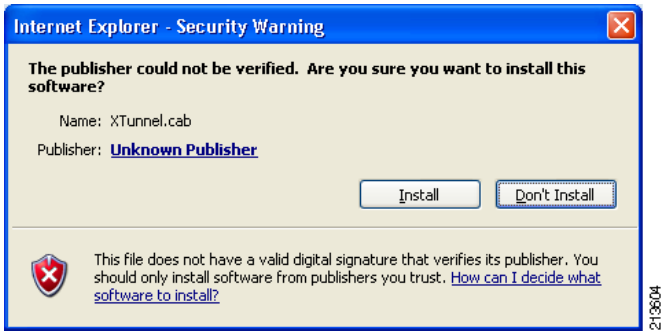


Abbildung 15 Sicherheitswarnung:



Nach dem Installieren des ActiveX-Plug-Ins wird ein SSL VPN-Tunnel erstellt. Wenn die Verbindung hergestellt wurde, wird das Symbol für den SSL VPN-Client in der Taskleiste angezeigt.

Schritt 4 Klicken Sie mit der rechten Maustaste auf das Symbol in der Taskleiste, und wählen Sie **Cisco-SSLVPN-Tunnel Status** aus, um den Status anzuzeigen (siehe Abbildung 16).

Abbildung 16 Cisco-SSLVPN-Tunnel Status

Im Popup-Bildschirm werden der SSL VPN-Status, die Dauer, die IP-Adresse und die Aktivität angezeigt, wie in Abbildung 17und Abbildung 18 dargestellt.

Abbildung 17 Popup-Bildschirm für den Status

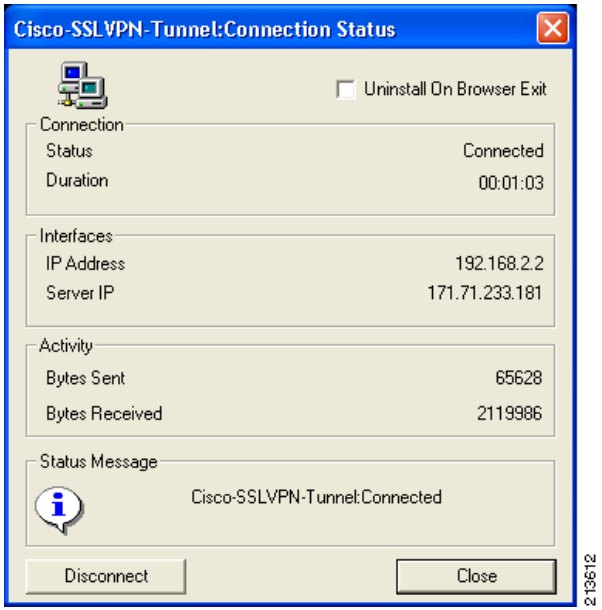
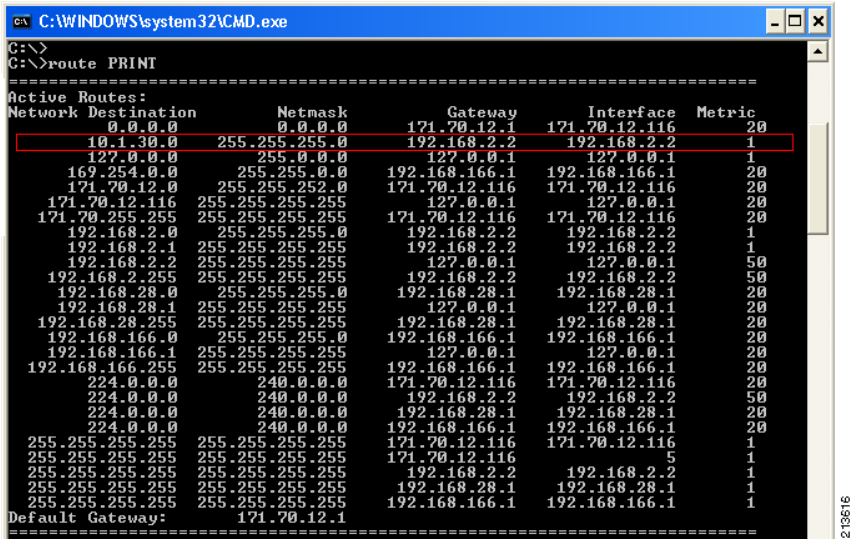


Abbildung 18 Bildschirm für die SSL VPN-Aktivität



Schritt 5 Starten Sie auf dem Client-PC einen Webbrowser, um die internen Webserver oder das IP-Gerät im Netzwerk der Hauptniederlassung anzuzeigen.

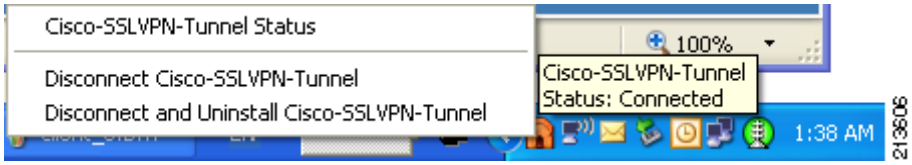
Gehen Sie für dieses Beispiel zu http://10.1.30.134, um das Video von der IP-Kamera anzuzeigen, oder zu http://10.1.30.83, um den internen Webserver anzuzeigen.

Schritt 6 Geben Sie auf dem Client-PC im Eingabeaufforderungsmodus **route PRINT** ein.

Daraufhin sollte die Route zum Netzwerk 10.1.30.0 angezeigt werden.

Schritt 7 Wenn Sie die Verbindung mit dem SSL VPN trennen möchten, klicken Sie mit der rechten Maustaste auf das Symbol in der Taskleiste, und wählen Sie **Disconnect Cisco-SSLVPN-Tunnel** aus. Wählen Sie auf dem öffentlichen PC **Disconnect and Uninstall Cisco-SSLVPN-Tunnel** aus, um auch das Plug-In zu deinstallieren. (Siehe Abbildung 19).

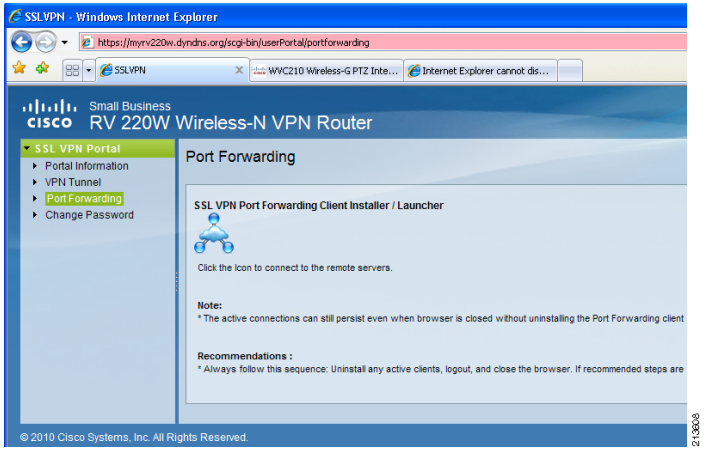
Abbildung 19 Trennen der Verbindung zum SSL VPN



Verwenden des SSL VPN-Clients im Port Forwarding-Modus (optional)

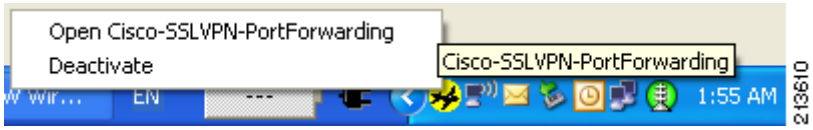
Schritt 1 Wenn das SSL VPN so eingerichtet ist, dass der Port Forwarding-Modus verwendet wird, öffnen Sie von der Portalseite des SSL VPN-Clients aus die Seite „Port Forwarding“ (siehe Abbildung 20), und klicken Sie auf das Symbol zum Installieren des Port Forwarding-Clients.

Abbildung 20 Seite „Port Forwarding“



Nach der Installation wird das Symbol für den SSL VPN-Port Forwarding-Modus in der Taskleiste angezeigt, wie in Abbildung 21 dargestellt.

Abbildung 21 Symbol für den SSL VPN-Port Forwarding-Modus



Schritt 2 Öffnen Sie in einem Browser *http://10.1.30.83*.

Die interne Webseite wird angezeigt.

Schritt 3 Klicken Sie mit der rechten Maustaste auf die Taskleiste, um das Statusfenster zu öffnen (siehe Abbildung 22), das auch die bestehenden Verbindungen anzeigt.

Abbildung 22 Statusfenster

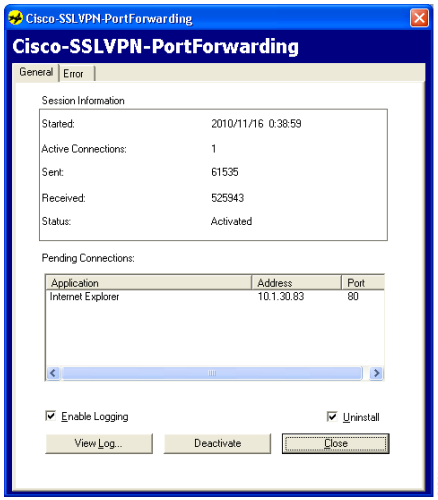
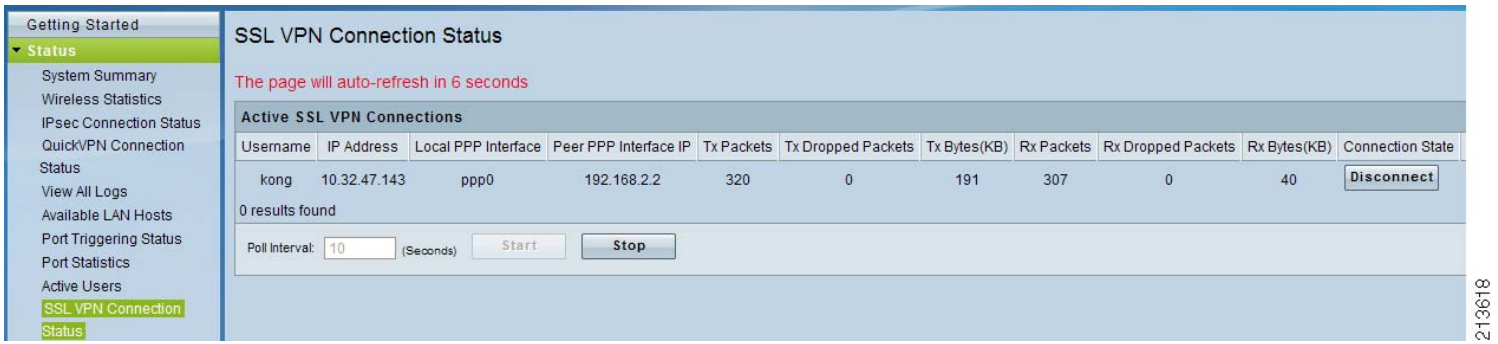


Abbildung 23 Bildschirm „SSL VPN Connection Status“



Schritt 4 Klicken Sie mit der rechten Maustaste auf das Symbol in der Taskleiste  , und wählen Sie **Deactivate** aus, um den SSL VPN-Port Forwarding-Modus zu beenden.

Überwachen aller SSL VPN-Verbindungen auf dem Server

Administratoren können den Bildschirm **Status > SSL VPN Connection Status** öffnen, um den Status aller aktiven SSL VPN-Clients anzuzeigen, wie in Abbildung 23 dargestellt. Klicken Sie auf **Disconnect**, um die einzelnen Verbindungen zu beenden.

Cisco und das Cisco Logo sind Marken von Cisco Systems, Inc. und/oder von Partnerunternehmen in den Vereinigten Staaten und anderen Ländern. Eine Liste der Cisco Marken finden Sie unter www.cisco.com/go/trademarks. Die genannten Marken anderer Anbieter sind Eigentum der jeweiligen Inhaber. Die Verwendung des Begriffs „Partner“ impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und anderen Unternehmen. (1005R)