Pour les PME

Configuration du réseau privé virtuel (VPN) SSL (Secure Sockets Layer)

Présentation

Un réseau privé virtuel Secure Sockets Layer (VPN SSL) fournit une connexion sécurisée aux ressources réseau sur l'Internet public, à l'aide du protocole HTTPS (Hypertext Transfer Protocol Secure). Un VPN SSL permet aux utilisateurs d'établir des sessions d'accès à distance sécurisées depuis quasiment n'importe quel navigateur connecté à Internet. Le protocole SSL fonctionne sur une couche qui se trouve entre la couche TCP (Transmission Control Protocol) et la couche Application. Le protocole SSL utilise le port TCP 443, qui est généralement ouvert sur le pare-feu local et le pare-feu distant, qui permet aux utilisateurs distants d'accéder à des ressources réseau à distance, facilement et en toute sécurité.

La solution VPN SSL offre une méthode flexible et hautement sécurisée permettant de déployer des ressources réseau à quasiment n'importe quel utilisateur distant ayant accès à Internet et à un navigateur Web. À l'aide de l'accès Web standard, cette solution réduit les coûts d'assistance des PC de bureau et la complexité de la gestion.

Produits proposés

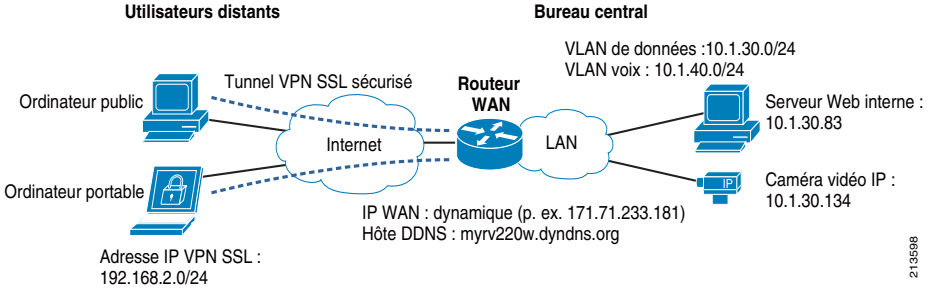
- Routeur pare-feu de sécurité réseau Cisco RV220W Wireless-N : prend en charge cinq connexions VPN SSL simultanées par défaut.

Topologie du réseau

La Figure 1 illustre un exemple de mise en œuvre de VPN SSL avec un routeur Cisco Small Business RV220. Les utilisateurs Internet distants se connectent au routeur VPN SSL via un tunnel VPN SSL sécurisé et peuvent ensuite accéder aux serveurs et ressources réseau internes, qui sont en général protégés de l'accès public par un pare-feu exécuté sur le routeur WAN Cisco.

Le routeur WAN Cisco fournit également le routage entre les différents VLAN, dont le VLAN de données (30), le VLAN voix (40) et le VLAN de gestion (60). Dans cet exemple, un serveur Web interne (*10.1.30.83*) et une caméra vidéo IP (1*0.1.30.134*) sont placés dans le VLAN de données.

Figure 1 **VPN SSL avec un routeur Cisco Small Business RV220**



Principales caractéristiques

- **Mode Tunnel VPN SSL** : le mode de tunnel VPN SSL transfère les données de la couche réseau (IP), et peut donc prendre en charge toutes les applications IP. Pour activer le mode de tunnel, cliquez sur un lien de la page du portail pour télécharger le client VPN SSL du mode de tunnel à partir du serveur VPN SSL. Vous pouvez supprimer le logiciel client de l'ordinateur, portable ou de bureau, distant une fois la session VPN SSL interrompue, ou le laisser installé.
- **Transfert de port VPN SSL (sans tunnel)** : le mode Transfert de port VPN SSL transfère les données de la couche application, à l'aide de ports TCP spécifiques, tels que les ports TCP 80 et 25. Ce mode permet d'accéder à distance aux applications TCP qui utilisent des ports fixes connus, par exemple les protocoles POP3 (Post Office Protocol version 3), IMAP (Internet Message Access Protocol), SMTP (Simple Mail Transfer Protocol), Telnet et SSH (Secure Shell). Ce mode ne peut pas être utilisé pour les applications qui utilisent des ports attribués dynamiquement, comme FTP. Vous pouvez cliquer sur un lien de la page du portail VPN SSL pour télécharger le client de transfert de port. La configuration du serveur VPN SSL comprend une liste de serveurs spécifiques, tels que des serveurs Web et des serveurs de messagerie électronique, auxquels les utilisateurs ont accès.

Conseils de conception

- **Adresse IP WAN et DDNS** : les utilisateurs distants doivent accéder à l'interface WAN du routeur VPN SSL par l'Internet public, une adresse IP WAN statique est donc préférable. Si l'adresse IP WAN est reçue dynamiquement du fournisseur de services Internet (ISP), configurez le service DDNS (Dynamic Domain Name Service) et utilisez le nom d'hôte du routeur pour accéder au routeur VPN SSL.
- **Mode Tunnel ou Transfert de port** : le mode Tunnel est recommandé pour les PME car il fournit la meilleure fonctionnalité, bien que l'autre mode puisse être utilisé le cas échéant pour répondre aux exigences d'un déploiement spécifique.
- **Chiffrement et certificat** : un VPN SSL utilise un certificat numérique côté serveur pour le chiffrement. Il utilise le niveau de chiffrement le plus élevé qui puisse être négocié avec le navigateur Web client. Le routeur VPN SSL peut générer son propre certificat (*certificat autosigné*). Il peut également importer un certificat numérique si l'organisation en a déjà émis un.
- **Authentification des utilisateurs VPN** : plusieurs méthodes d'authentification des utilisateurs sont prises en charge dans une mise en œuvre VPN SSL. L'utilisation de la base de données des utilisateurs locale est une méthode simple qui nécessite l'ajout manuel de chaque utilisateur et de son mot de passe à la base de données. Le VPN SSL prend également en charge l'utilisation de serveurs d'authentification externes, tels que RADIUS, NT Domain ou Active Directory, pour tirer profit de l'infrastructure de gestion du réseau informatique existante.
- **Adresse IP du client VPN** : une adresse réseau distincte doit être attribuée comme adresse IP du client VPN SSL. Cet exemple utilise *192.168.2.0/24* comme adresse IP du client SSL.
- **Split tunneling** : le Split tunneling peut être activé de sorte que seul le trafic destiné au serveur VPN soit chiffré et transmis par le tunnel VPN SSL, pour réduire la charge côté serveur VPN et pour augmenter les performances du réseau.

Configuration d'un VPN SSL sur un routeur Cisco Small Business RV220W

Liste de contrôle de préconfiguration

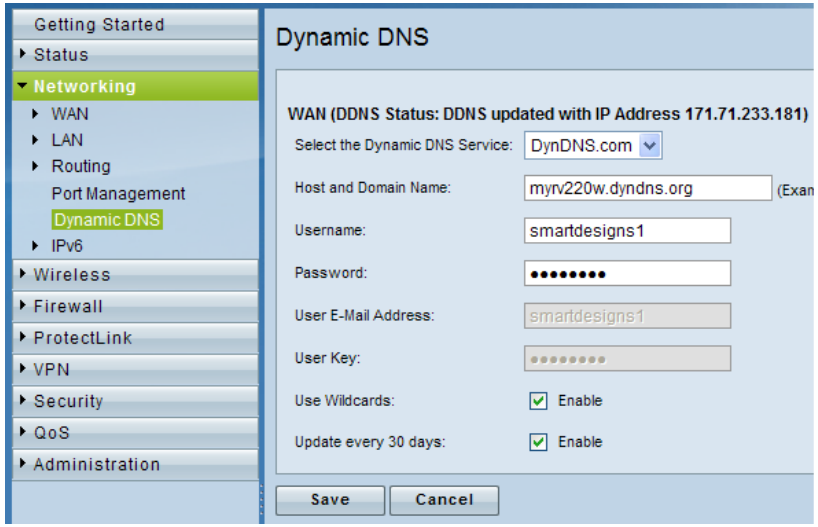
Reportez-vous au Guide de l'administrateur du routeur RV220W pour terminer la configuration initiale du routeur RV220W.

1. Vérifiez que les connexions Internet du routeur WAN sont actives. La traduction d'adresses réseau (NAT) et un pare-feu doivent également être activés.
2. Vérifiez le bon fonctionnement de la connectivité locale entre le routeur, le commutateur et les périphériques IP locaux. Les VLAN de données, voix et de gestion sur le routeur RV et les commutateurs doivent être configurés correctement. Le routage entre VLAN et la jonction doivent fonctionner sur chaque VLAN. Le service DHCP de chaque VLAN doit être fonctionnel.
3. Vérifiez le bon fonctionnement de la connectivité des ordinateurs, serveurs et autres périphériques internes avec le commutateur local ou les ports de commutation du routeur RV. Vérifiez que les ordinateurs et les serveurs peuvent communiquer entre eux et accéder à l'Internet public.
4. Connectez et configurez un serveur Web interne et une caméra IP WVC210 sur le VLAN de données (sur le site du bureau central dans cet exemple).

Activation du service DDNS (facultatif)

Si une adresse IP WAN statique est utilisée, ou que le service DDNS sur le routeur WAN est déjà configuré, ignorez cette étape. Lorsque l'interface WAN reçoit une adresse IP dynamique du fournisseur de services, le service DDNS peut être utilisé pour que le client accède au serveur VPN SSL à l'aide d'un nom d'hôte. Accédez à **Networking** > **Dynamic DNS** pour configurer les paramètres DDNS (voir Figure 2). Pour obtenir plus de détails, reportez-vous au document Conseils avancés : Activation de l'accès public WAN avec DDNS et le transfert de port.

Figure 2 Page Dynamic DNS

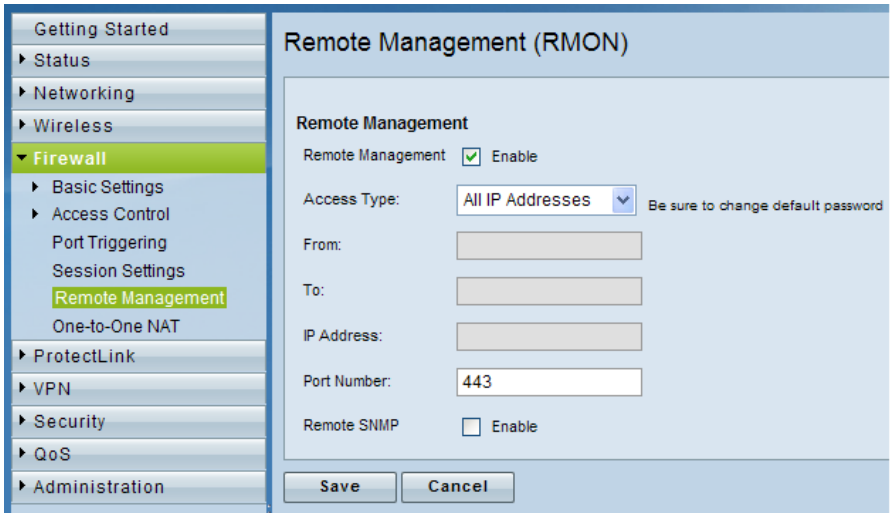


Activation de la gestion à distance

La gestion à distance doit être activée sur le routeur Cisco RV220W avant que le VPN SSL puisse être mis en œuvre. La gestion à distance permet aux utilisateurs distants de se connecter à l'interface WAN du routeur à l'aide du protocole HTTPS. Il s'agit d'une condition prérequise pour le VPN SSL.

Étape 1 Pour activer la gestion à distance, accédez à **Firewall > Remote Management** et définissez Access Type sur *All IP Address,* car les adresses IP du client sont principalement inconnues, et conservez le numéro de port 443, qui est la valeur par défaut pour le protocole HTTPS. (Reportez-vous à la Figure 3.)

Figure 3 Activation de la gestion à distance

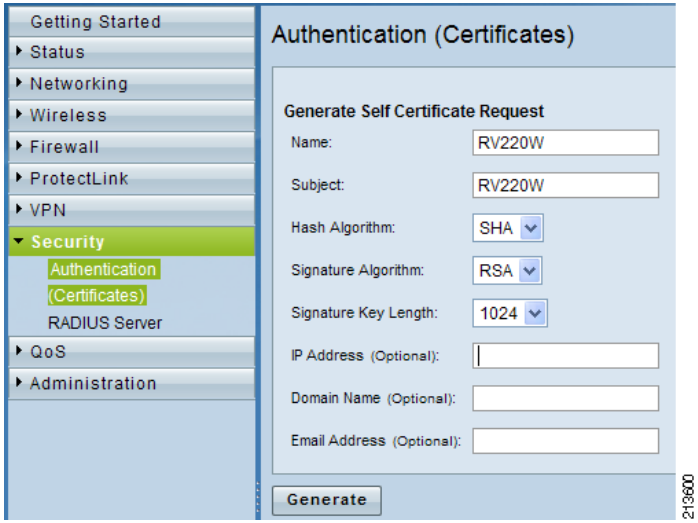


Étape 2 Accédez à **Security > Authentication (Certificates)**. (Reportez-vous à la Figure 4.)

Étape 3 Dans l'écran Generate Self Certificate Request, cliquez sur **Generate Certificate** pour ajouter un certificat numérique personnalisé.

Un certificat numérique est utilisé par le protocole HTTPS pour l'authentification et le chiffrement.

Figure 4 Génération d'une requête d'autocertificat



Configuration de groupes et utilisateurs VPN SSL

Les utilisateurs et groupes SSLVPN doivent être créés pour l'authentification du VPN SSL. Dans cet exemple, les utilisateurs du VPN SSL sont créés dans la base de données locale RV220W, dans le groupe SSLVPN par défaut.

Étape 1 Pour modifier le mot de passe par défaut de l'administrateur, accédez à **Administration > Password Complexity** pour activer **enforce Password Complexity**.

Étape 2 Accédez à **Administration > Users > Users** pour modifier le mot de passe par défaut des utilisateurs administrateurs**.**

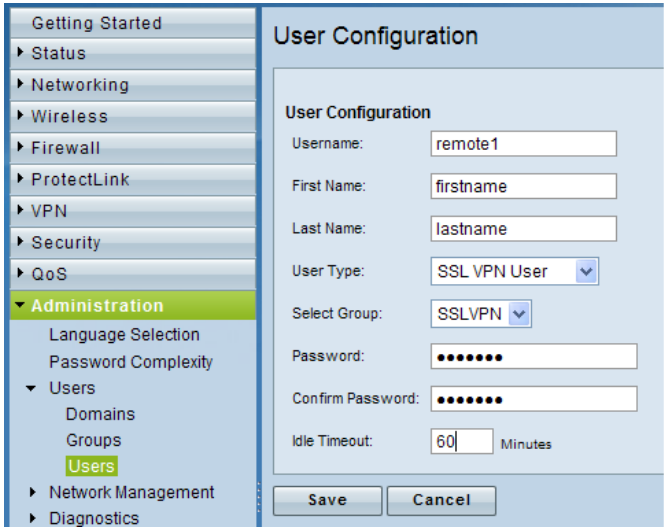
Étape 3 Accédez à **Administration > Users > Users** pour ajouter des utilisateurs VPN SSL. Un groupe SSLVPN par défaut existe déjà. Cliquez sur **Add** pour afficher une nouvelle page User Configuration.

Étape 4 Dans la page User Configuration (voir Figure 5), procédez comme suit :

a. Saisissez le nom d'utilisateur, le prénom et le nom, sélectionnez SSL VPN User comme type d'utilisateur, sélectionnez SSLVPN comme groupe, puis saisissez le mot de passe et le délai d'inactivité.

b. Cliquez sur Save.

Figure 5 Page User Configuration



Étape 5 Ajoutez d'autres utilisateurs VPN SSL au même groupe, en suivant l'étape 3.

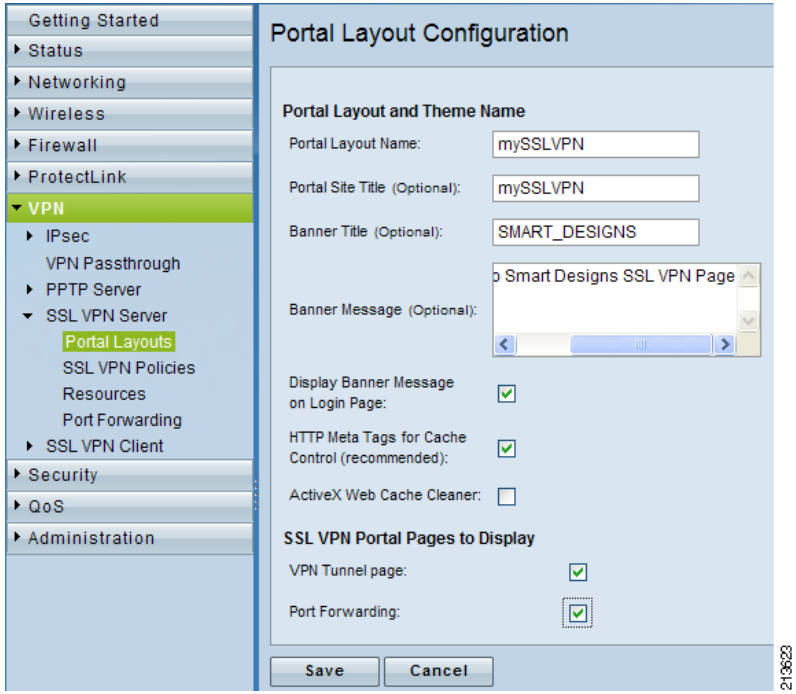
Personnalisation de la page du portail du serveur VPN SSL (facultatif)

Le serveur VPN SSL est activé par défaut une fois la gestion à distance activée. Une page de portail SSL par défaut est déjà configurée sur le routeur Cisco RV220W. Une nouvelle page de portail peut être ajoutée ou la page par défaut peut être modifiée en procédant comme suit.

Étape 1 Accédez à **VPN > SSL VPN Server > Portal Layouts**, puis cliquez sur **Add**.

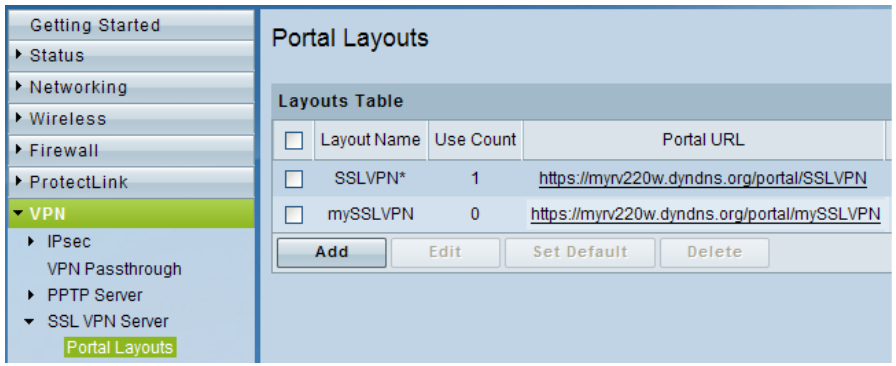
Étape 2 Personnalisez le nom de la page, le titre, le message de la bannière et les icônes. (Reportez-vous à la Figure 6.)

Figure 6 Page Portal Layout Configuration



Étape 3 Accédez à **VPN > SSL VPN Server > Portal Layouts** pour afficher un récapitulatif et une adresse URL.

Figure 7 Fenêtre Portal Layouts



Ajout de stratégies VPN SSL (facultatif)

Les stratégies VPN SSL permettent d'octroyer ou de refuser l'accès à des ressources réseau, adresses IP ou réseaux IP spécifiques. Elles peuvent être définies au niveau de l'utilisateur, du groupe ou au niveau global. Par défaut, une stratégie PERMIT globale (non affichée) est configurée sur toutes les adresses et sur tous les services/ports.

La stratégie la plus spécifique est prioritaire sur les stratégies moins spécifiques d'un propriétaire donné. Si les stratégies d'un utilisateur ne sont pas configurées, les stratégies de groupe associées sont appliquées. Si aucune stratégie n'est configurée pour le groupe, les stratégies globales sont appliquées.

Étape 1 Accédez à **VPN > SSL VPN Server > SSL VPN Policies**, puis cliquez sur **Add**.

Étape 2 Dans la page SSL VPN Policy Configuration (voir Figure 8), activez la stratégie pour le niveau Global, Group ou User, puis sélectionnez le groupe ou l'utilisateur correspondant.

Une stratégie peut être appliquée à une adresse IP ou un réseau IP spécifique, à toutes les adresses IP, ou à une source réseau (service prédéfini basé sur une adresse IP ou adresse réseau, ou une plage de ports).

Étape 3 Spécifiez une plage de ports ou un numéro de port, sélectionnez le service (Tunnel ou Transfert de port, ou les deux), et sélectionnez l'autorisation *permit* ou *deny*.

La Figure 8 illustre une stratégie ajoutée pour octroyer l'accès VPN SSL à la caméra IP 10.1.30.134, alors que la Figure 9 illustre que tous les autres se voient refuser l'accès. Suivez les mêmes étapes pour octroyer l'accès au serveur Web interne 10.1.30.83.

Figure 8 Octroi de l'accès VPN SSL

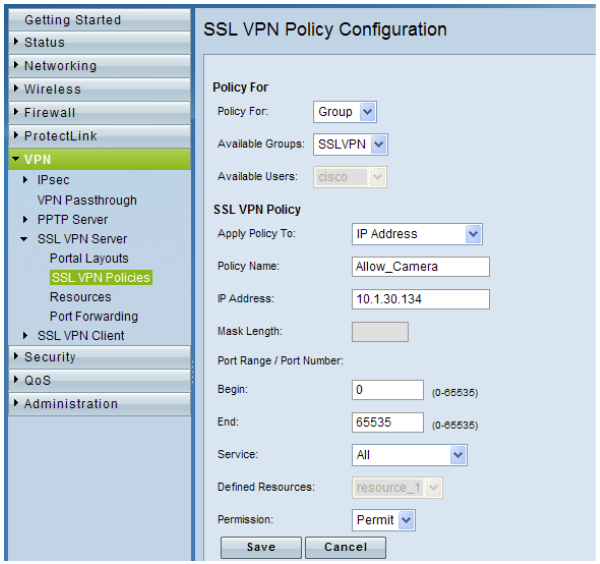
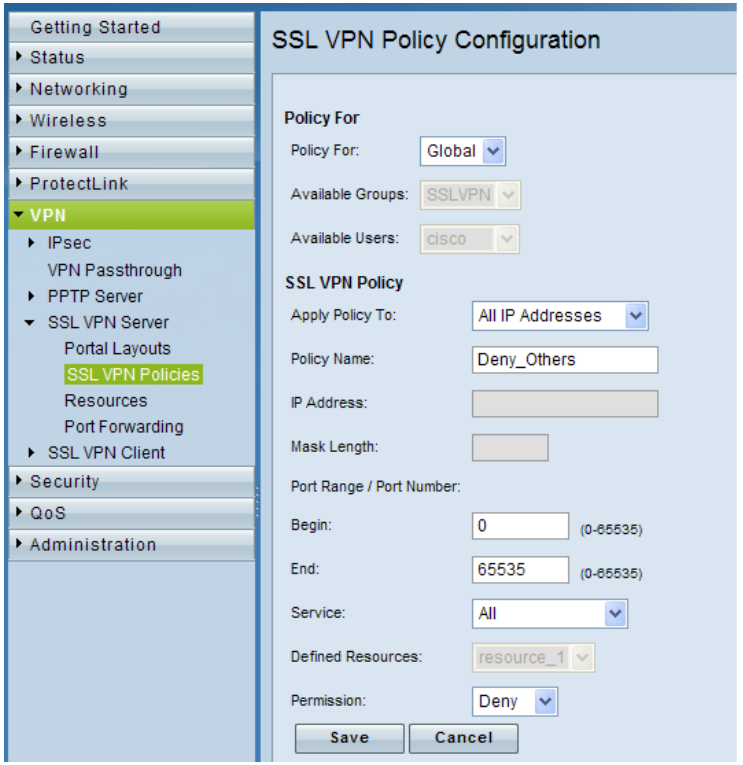


Figure 9 Refus de l'accès VPN SSL



Une fois la procédure ci-dessus terminée, la configuration du serveur VPN SSL en mode Tunnel est terminée. Le transfert de port peut également être configuré, comme le décrit la section suivante.

Configuration du transfert de port VPN SSL (facultatif)

Bien que le mode Tunnel VPN SSL soit fortement recommandé, le transfert de port SSL peut également être configuré et utilisé dans certaines conditions.

Étape 1 Accédez à **VPN > SSL VPN Server > Port Forwarding** pour ajouter l'adresse IP du serveur local et son port TCP.

Les exemples illustrés dans la Figure 10 et la Figure 11 ajoutent les ports HTTP et HTTPS pour le serveur Web local 10.1.30.83.

Figure 10 Écran Port Forwarding (1)

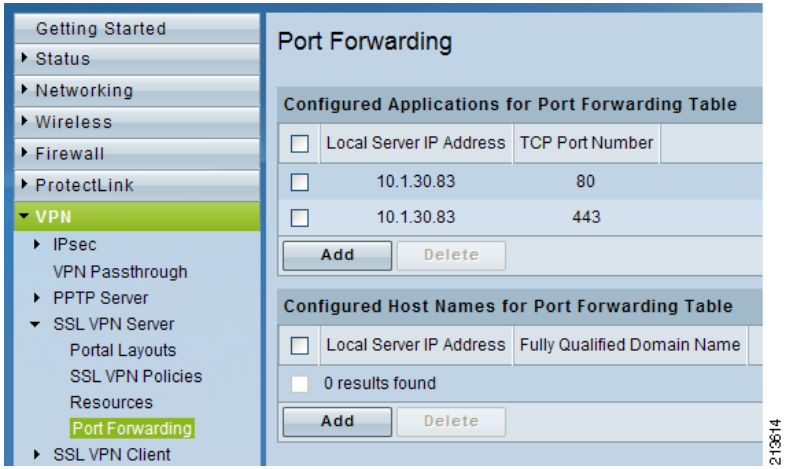


Figure 11 Écran Port Forwarding (2)

Configuration du routeur WAN pour personnaliser le client VPN SSL

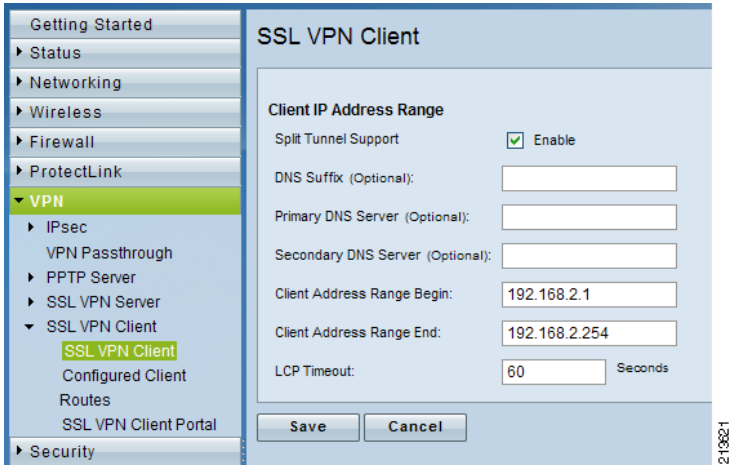
Vous pouvez modifier le pool d'adresses IP du client VPN SSL. L'adresse réseau par défaut pour le client VPN SSL est 192.168.254.0. Le split tunneling peut également être activé sur le client VPN SSL de sorte que seul le trafic destiné au bureau central (10.1.30.0/24) est transmis par le tunnel VPN SSL.

Étape 1 Pour modifier l'adresse IP du client VPN SSL, accédez à **VPN > SSL VPN Client > SSL VPN Client** et modifiez les valeurs de début et de fin de la plage pour l'adresse client.

Dans cet exemple, l'adresse IP du client est remplacée par *192.168.2.0*.

Étape 2 Activez **Split Tunnel Support**. (Reportez-vous à la Figure 12.)

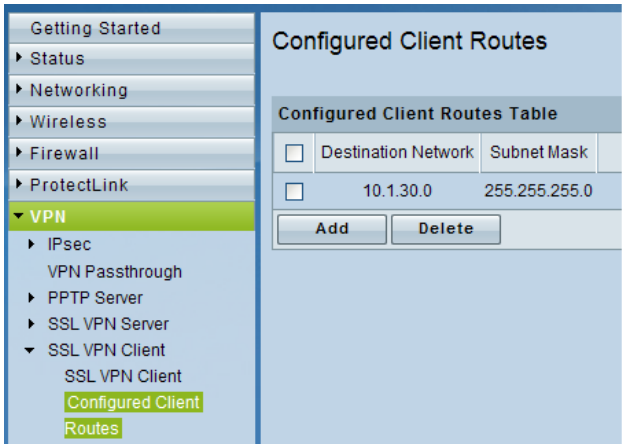
Figure 12 Page SSL VPN Client



Étape 3 Accédez à **VPN > SSL VPN Client > Configured Client Routes** pour ajouter le routage du client. (Reportez-vous à la Figure 13.)

Dans cet exemple, l'adresse IP du VLAN de données, 10.1.30.0/24, est ajoutée à la table de routage du client.

Figure 13 Page Configured Client Routes



Utilisation du client VPN SSL sur un ordinateur

Utilisation du client VPN SSL en mode Tunnel

Étape 1 Sur l'ordinateur client connecté à Internet, ouvrez un navigateur Web et accédez à la page du portail VPN SSL du routeur Cisco RV220W, avec l'adresse IP ou le nom d'hôte DDNS.

Les adresses URL de toutes les pages du portail sont répertoriées sous **VPN > SSL VPN Server > Portal Layouts**. Par exemple :

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

Remarque Les navigateurs Web doivent être configurés pour exécuter des contrôles Active X non signés sur le site approuvé pour accéder à la page du portail du client VPN SSL. Pour obtenir des instructions détaillées, reportez-vous à https://supportforums.cisco.com/docs/DOC-9376.

Étape 2 Lorsque la page de connexion s'affiche, connectez-vous à l'aide de l'ID utilisateur VPN SSL et du mot de passe préalablement créés par l'administrateur.

Une fois la connexion établie, la page du portail VPN SSL s'affiche.

Étape 3 Accédez à la page VPN Tunnel et cliquez sur l'icône  . (Reportez-vous à la Figure 14.)

Pour Internet Explorer, ActiveX doit être installé. Cliquez sur **Installer** si Internet Explorer affiche un avertissement de sécurité (voir Figure 15).

Figure 14 Page VPN Tunnel

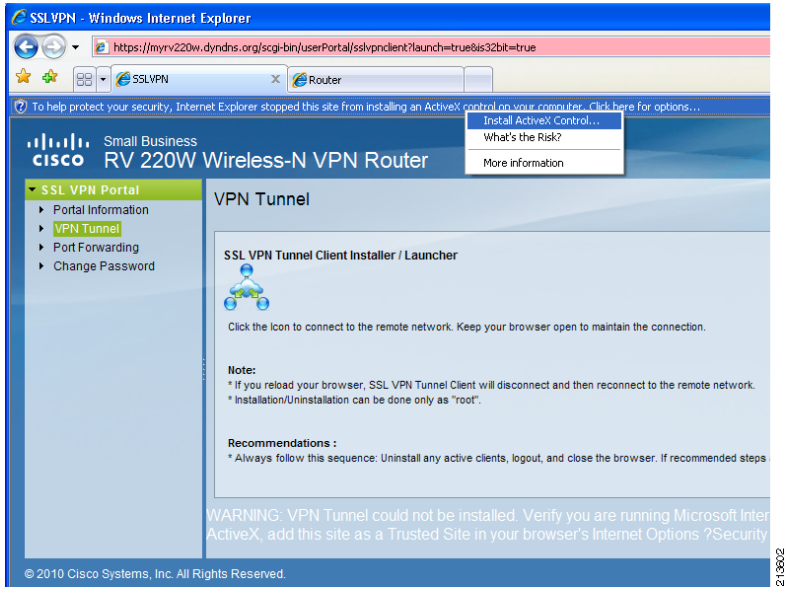
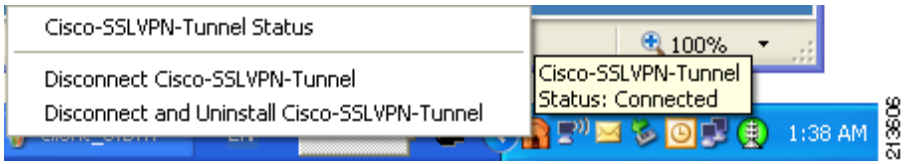


Figure 15 Avertissement de sécurité

Une fois le plugin ActiveX installé, un tunnel VPN SSL est établi. La barre d'état du client VPN SSL s'affiche une fois la connexion établie.

Étape 4 Cliquez avec le bouton droit sur la barre d'état et sélectionnez **Cisco-SSLVPN-Tunnel Status** pour afficher l'état (voir Figure 16).

Figure 16 État de Cisco-SSLVPN-Tunnel



La fenêtre contextuelle indique l'état du VPN SSL, la durée, l'adresse IP et l'activité, comme l'illustrent la Figure 17 et la Figure 18.

Figure 17 Fenêtre contextuelle d'état

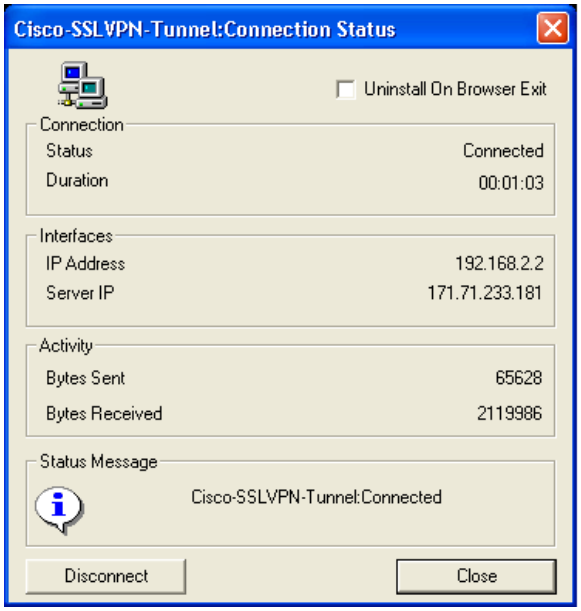
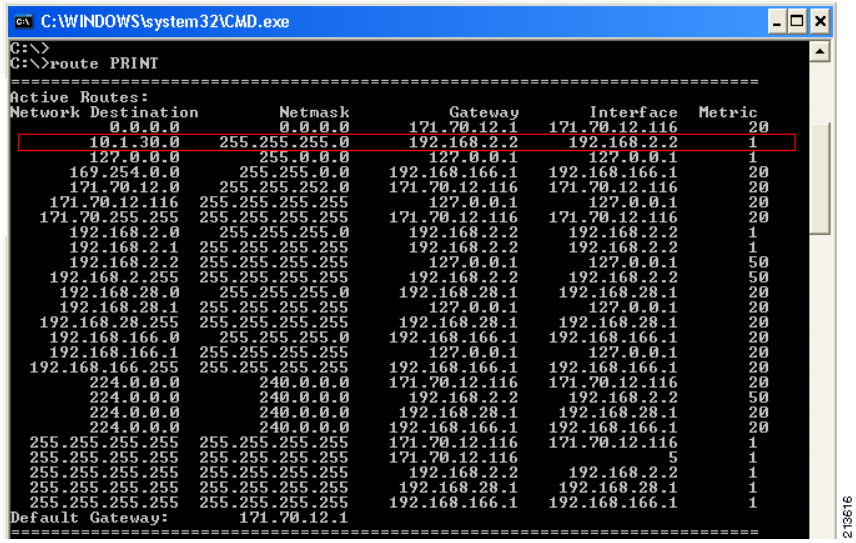


Figure 18 Écran SSL VPN Activity



Étape 5 Sur l'ordinateur client, lancez un navigateur Web pour accéder aux serveurs Web internes ou à un périphérique IP du réseau du bureau central.

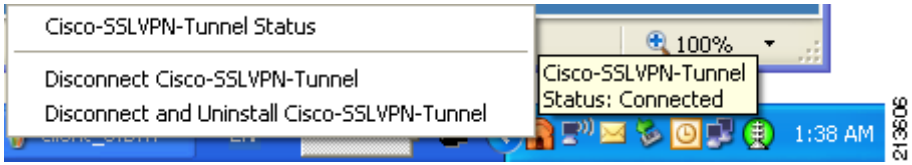
Dans cet exemple, accédez à http://10.1.30.134 pour afficher la vidéo d'une caméra IP ou à http://10.1.30.83 pour accéder au serveur Web interne.

Étape 6 Sur l'ordinateur client, saisissez **route PRINT** à l'invite de commande.

L'itinéraire d'accès au réseau 10.1.30.0 doit être indiqué.

Étape 7 Pour déconnecter le VPN SSL, cliquez avec le bouton droit sur l'icône dans la barre d'état système et sélectionnez **Disconnect Cisco-SSLVPN-Tunnel**. Sur l'ordinateur public, sélectionnez **Disconnect and Uninstall Cisco-SSLVPN-Tunnel** pour aussi désinstaller le plugin. (Reportez-vous à la Figure 19.)

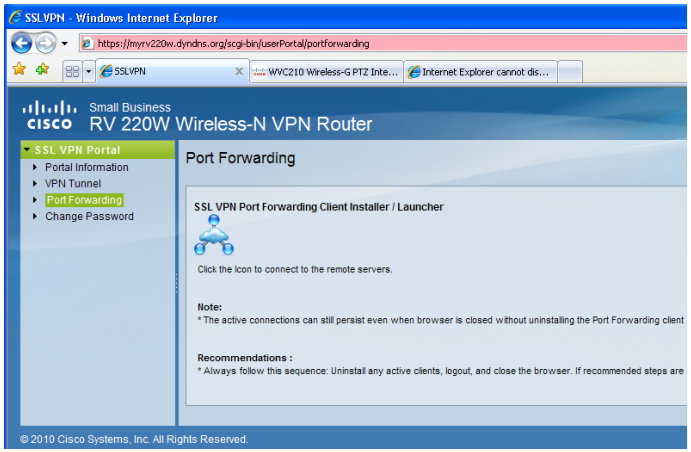
Figure 19 Déconnexion du VPN SSL



Utilisation du client VPN SSL en mode Transfert de port (facultatif)

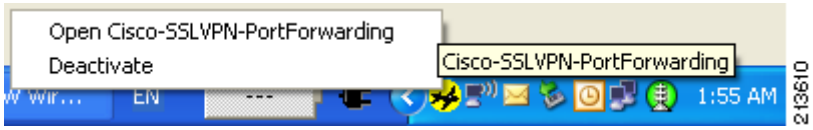
Étape 1 Si le VPN SSL est défini pour utiliser le mode Transfert de port, accédez à la page Port Forwarding à partir de la page du portail du client VPN SSL (voir Figure 20) et cliquez sur l'icône pour installer le client de transfert de port.

Figure 20 Page Port Forwarding



Après l'installation, l'icône de transfert de port SSL apparaît dans la barre d'état, comme l'illustre la Figure 21.

Figure 21 Icône du transfert de port SSL



Étape 2 Uitlisez un navigateur pour accéder à *http://10.1.30.83*.

La page Web interne s'affiche.

Étape 3 Cliquez avec le bouton droit sur la barre d'état pour ouvrir la fenêtre d'état (voir Figure 22), qui indique également les connexions en attente.

Figure 22 Fenêtre d'état

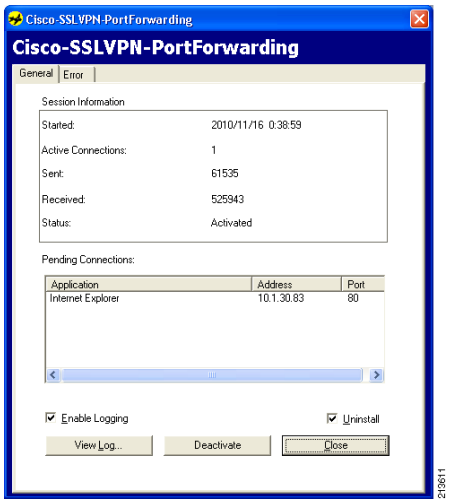
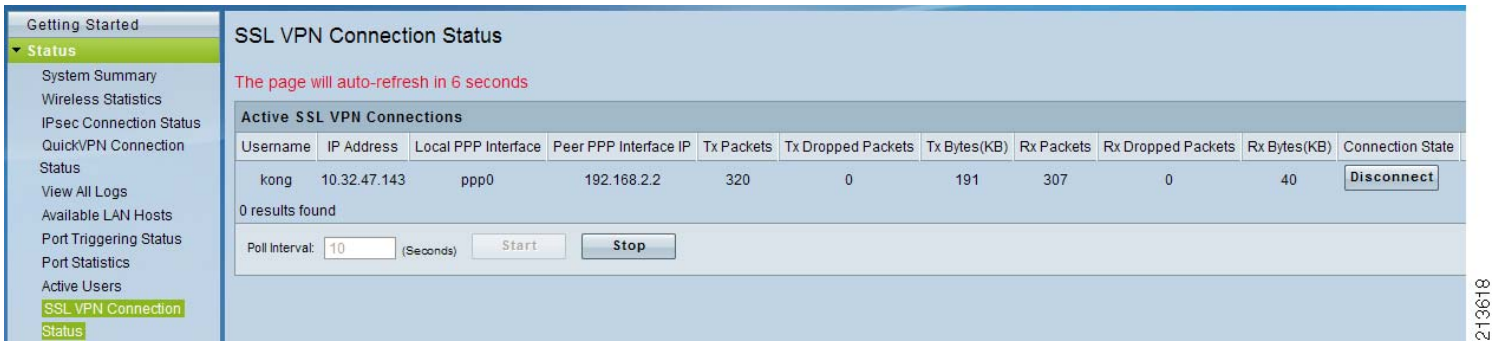


Figure 23 Écran SSL VPN Connection Status



Étape 4 Cliquez avec le bouton droit sur l'icône de la barre d'état  et sélectionnez **Deactivate** pour quitter le mode de transfert de port VPN SSL.

Surveillance de toutes les connexions VPN SSL sur le serveur

Les administrateurs peuvent accéder à Status > SSL VPN Connection Status pour consulter l'état de tous les clients VPN SSL actifs, comme l'illustre la Figure 23. Cliquez sur Disconnect pour interrompre chaque connexion.

Cisco et le logo Cisco sont des marques déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays. Vous trouverez la liste des marques commerciales de Cisco sur la page Web www.cisco.com/go/trademarks. Les autres marques commerciales mentionnées dans les présentes sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et toute autre entreprise. (1005R)