Configuration du concentrateur Cisco VPN 5000 et implémentation d'une connectivité VPN IPSec LAN à LAN en mode principal

Contenu

Introduction

Ce document explique la configuration initiale du concentrateur de Cisco VPN 5000 et explique comment se connecter au réseau utilisant l'IP et comment offrir la connectivité VPN d'entre réseaux locaux de Principal-mode d'IPSec.

Vous pouvez installer le concentrateur VPN dans l'un ou l'autre de deux configurations, selon où vous le connectez au réseau par rapport à un Pare-feu. Le concentrateur VPN a deux ports Ethernet, l'un d'entre eux (le trafic d'IPSec de passages d'Ethernets 1) seulement. L'autre port (Ethernet 0) conduit tout le trafic IP. Si vous prévoyez d'installer le concentrateur VPN parallèlement au Pare-feu, vous devez utiliser les deux ports de sorte que l'Ethernet 0 fasse face au RÉSEAU LOCAL protégé, et l'Ethernet 1 fasse face à l'Internet par le routeur de passerelle Internet du réseau. Vous pouvez également installer le concentrateur VPN derrière le Pare-feu sur le RÉSEAU LOCAL protégé et le connecter par le port d'Ethernet 0, de sorte que le trafic d'IPSec passant entre l'Internet et le concentrateur soit traversé le Pare-feu.

Conditions préalables

Exigences

Aucune condition préalable spécifique n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur le concentrateur de Cisco VPN 5000.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration de base de Connectivité

Le moyen le plus simple d'établir la connexion réseau de base est de connecter un câble série au port de console sur le concentrateur VPN et d'employer le logiciel de terminal pour configurer l'adresse IP sur le port d'Ethernet 0. Après avoir configuré l'adresse IP sur le port d'Ethernet 0, vous pouvez employer le telnet pour se connecter au concentrateur VPN pour se terminer la configuration. Vous pouvez également générer un fichier de configuration dans un éditeur de texte compétent, et l'envoyez au concentrateur VPN utilisant le TFTP.

Utilisant le logiciel de terminal par le port de console, vous êtes au commencement incité pour un mot de passe. Utilisez le mot de passe « letmein. » Après avoir répondu avec le mot de passe, émettez les **Ethernets d'IP de configurer 0** commandes, répondant aux demandes avec vos informations système. L'ordre des demandes devrait ressembler à l'exemple suivant.

```
*[ IP Ethernet 0 ]# configure ip ethernet 0
      Section 'ip ethernet 0' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IP Ethernet 0 ]# ipaddress=192.168.233.1
      *[ IP Ethernet 0 ]# subnetmask=255.255.255.0
      *[ IP Ethernet 0 ]# ipbroadcast=192.168.233.255
      *[ IP Ethernet 0 ]# mode=routed
      *[ IP Ethernet 0 ]#
```

Maintenant vous êtes prêt à configurer le port d'Ethernet 1.

Configurer le port d'Ethernet 1

Les informations d'adressage TCP/IP sur le port d'Ethernet 1 sont les externes, adresse TCP/IP d'Internet-routable que vous avez assignée pour le concentrateur VPN. Évitez d'utiliser une adresse dans le même réseau TCP/IP que des Ethernet 0, car ceci désactivera le TCP/IP dans le concentrateur.

Sélectionnez les commandes des **Ethernets 1 d'IP de configurer**, répondant aux demandes avec vos informations système. L'ordre des demandes devrait ressembler à l'exemple suivant.

```
*[ IP Ethernet 0 ]# configure ip ethernet 1
      Section 'ip ethernet 1' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IP Ethernet 1 ]# ipaddress=206.45.55.1
      *[ IP Ethernet 1 ]# subnetmask=255.255.255.0
      *[ IP Ethernet 1 ]# ipbroadcast=206.45.55.255
      *[ IP Ethernet 1 ]# mode=routed
      *[ IP Ethernet 1 ]#
```

Maintenant vous devez configurer la passerelle d'IPSec.

Configurer la passerelle d'IPSec

Les contrôles de passerelle d'IPSec où le concentrateur VPN envoie tout l'IPSec, ou percé un tunnel, le trafic. C'est indépendant du default route que vous configurez plus tard. Début en écrivant la commande **générale de configurer**, répondant aux demandes avec vos informations système. L'ordre des demandes devrait ressembler à l'exemple présenté ci-dessous.

```
* IntraPort2+_A56CB700# configure general
      Section 'general' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
       =
      To find a list of valid keywords and additional help enter "?"
      *[ General ]# ipsecgateway=206.45.55.2
      *[ General ]# exit
      Leaving section editor.
      * IntraPort2+_A56CB700#
```

Remarque: Dans des versions 6.x et ultérieures, la commande **ipsecgateway** a été changée à la commande **vpngateway**.

Permettez-maintenant nous configurent la stratégie d'Échange de clés Internet (IKE).

Configurer la stratégie IKE

Le contrôle de paramètres de protocole de gestion de clés d'association de sécurité internet (ISAKMP) /IKE comment le concentrateur VPN et le client identifient et s'authentifient pour établir des sessions de tunnel. Cette première négociation est mentionnée car phase les paramètres de 1. Phase 1 sont globaux au périphérique et ne sont pas associés avec une interface spécifique. Les mots clé identifiés dans cette section sont décrits ci-dessous. Des paramètres de négociation de Phase 1 pour des tunnels entre réseaux locaux peuvent être placés dans [<Section ID> de partenaire de tunnel] la section. Contrôles de négociation d'IKE de Phase 2 comment le concentrateur VPN et le client vpn manipulent différentes sessions de tunnel. Des paramètres de négociation d'IKE de Phase 2 pour le concentrateur VPN et le client vpn sont placés dans [le périphérique de <Name> de groupe VPN].

La syntaxe pour la stratégie IKE est comme suit.

```
Protection = [ MD5_DES_G1 | MD5_DES_G2 | SHA_DES_G1 | SHA_DES_G2 ]
```

Le mot clé de protection spécifie une suite de protection pour la négociation ISAKMP/IKE entre le

concentrateur VPN et le client vpn. Ce mot clé peut apparaître de plusieurs périodes dans cette section, dans ce cas le concentrateur VPN propose toutes les suites spécifiées de protection. Le client vpn reçoit une des options pour la négociation. La première partie de chaque option, MD5 (le condensé de message 5), est l'algorithme d'authentification utilisé pour la négociation. Le SHA signifie le Secure Hash Algorithm, qui est considéré plus sécurisé que le MD5. La deuxième partie de chaque option est l'algorithme de chiffrement. DES (norme de chiffrement de données) emploie une clé 56-bit pour brouiller les données. La troisième partie de chaque option est le groupe de Diffie-Hellman, utilisé pour l'échange clé. Puisque de plus grands nombres sont utilisés par l'algorithme du groupe 2 (G2), il est plus sécurisé que le groupe 1 (G1).

Pour commencer la configuration, sélectionnez la commande de **stratégie IKE de configurer**, répondant aux demandes avec vos informations système. Un exemple est affiché ci-dessous.

```
* IntraPort2+_A56CB700# configure IKE Policy
      Section 'IKE Policy' was not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IKE Policy ] Protection = MD5_DES_G1
      *[ IKE Policy ] exit
      Leaving section editor.
      * IntraPort2+_A56CB700#
```

Maintenant que vous avez configuré les fondements, il est temps de définir le tunnel et les paramètres de communication IP.

Configuration de site à site de Principal-mode

Pour configurer le concentrateur VPN pour prendre en charge des connexions entre réseaux locaux, vous devez définir la configuration de tunnel, aussi bien que les paramètres de communication IP à utiliser dans le tunnel. Vous ferez ceci dans deux sections, [partenaire de tunnel VPN X] la section, et [IP VPN X] la section. Pour n'importe quelle configuration donnée de site à site, le *x* défini dans ces deux sections doit s'assortir, de sorte que la configuration de tunnel soit correctement associée avec la configuration de protocole.

Regardons en détail chacune de ces sections.

Configurer la partie partenaire du tunnel

Dans la partie partenaire du tunnel, vous devez définir au moins les huit paramètres suivants.

- Transformez
- Partenaire
- KeyManage
- SharedKey
- **Mode**
- LocalAccess
- Pair
- BindTo

Transformez

Le mot clé de transformation spécifie les types et les algorithmes de protection utilisés pour des sessions de client d'IKE. Chaque option associée avec ce paramètre est une partie de protection qui spécifie l'authentification et les paramètres de chiffrement. Le paramètre de transformation peut apparaître de plusieurs périodes dans cette section, dans ce cas le concentrateur VPN propose les parties spécifiées de protection dans la commande qu'ils sont analysés, jusqu'à ce qu'une soit reçue par le client pour l'usage pendant la session. Dans la plupart des cas, seulement un transforment le mot clé est nécessaire.

Les options pour le mot clé de transformation sont comme suit.

```
[ ESP(SHA,DES) | ESP(SHA,3DES) | ESP(MD5,DES) | ESP(MD5,3DES) | ESP(MD5) |
ESP(SHA) | AH(MD5) | AH(SHA) |AH(MD5)+ESP(DES) | AH(MD5)+ESP(3DES) |
AH(SHA)+ESP(DES) | AH(SHA)+ESP(3DES) ]
```

L'ESP signifie encapsuler la charge utile de Sécurité et OH signifie l'en-tête d'authentification. Ces deux en-têtes sont utilisées pour chiffrer et authentifier des paquets. DES (norme de chiffrement de données) emploie une clé 56-bit pour brouiller les données. 3DES emploie trois clés différentes et trois applications de l'algorithme DES pour brouiller les données. Le MD5 est l'algorithme de hachage du message-digest 5. Le SHA est le Secure Hash Algorithm, qui est considéré en quelque sorte plus sécurisé que le MD5.

ESP(MD5,DES) est la valeur par défaut, et est recommandé pour la plupart des installations. L'ESP d'utilisation d'ESP(MD5) et ESP(SHA) pour authentifier des paquets (sans le cryptage). Utilisation d'AH(MD5) et AH(SHA) OH d'authentifier des paquets. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES), et AH(SHA)+ESP(3DES) utilisation OH d'authentifier des paquets et l'ESP pour chiffrer des paquets.

Partenaire

Le mot clé de partenaire définit l'adresse IP de l'autre Terminator de tunnel dans le partenariat de tunnel. Ce nombre doit être une adresse IP publique et routable avec laquelle le concentrateur des gens du pays VPN peut créer une connexion d'IPSec.

KeyManage

Le mot clé de KeyManage définit comment les deux concentrateurs VPN dans un partenariat de tunnel déterminent quel périphérique initie le tunnel et quel type de procédure d'établissement de tunnel à suivre. Les options sont automatiques, initié, répondent, et manuel. Vous pouvez utiliser les trois premières options de configurer des tunnels d'IKE, et le mot clé manuel pour configurer des tunnels de réparer-cryptage. Ce document ne couvre pas comment configurer des tunnels de réparer-cryptage. L'automatique spécifie que le partenaire de tunnel peut initier et répondre pour percer un tunnel des demandes de configuration. L'initié spécifie que le partenaire de tunnel envoie seulement des demandes de configuration de tunnel, il ne répond pas à elles. Répondez les spécifie que le partenaire de tunnel répond des demandes de tunnel-installation, mais n'initie jamais.

SharedKey

Le mot clé de SharedKey est utilisé comme secret partagé par IKE. Vous devez placer la même valeur de SharedKey sur les deux partenaires de tunnel.

Mode

Le mot clé mode définit le protocole de négociation d'IKE. La valeur par défaut est agressive, ainsi pour placer le concentrateur VPN pour le mode d'Interopérabilité, vous devez placer le mot clé mode à la canalisation.

LocalAccess

LocalAccess définit les numéros IP qui peuvent être accédés à par le tunnel, d'un masque d'hôte à un default route. Le mot clé de LocalProto définit que des nombres de protocole IP peuvent être accédé à par le tunnel, tel qu'ICMP(1), TCP(6), UDP(17), et ainsi de suite. Si vous voulez passer tous les numéros IP, alors vous devriez placer LocalProto=0. LocalPort détermine quels numéros de port peuvent être accédés par le tunnel. LocalProto et LocalPort se transfèrent sur 0, ou tout-Access.

Pair

Le mot clé de pair spécifie quels sous-réseaux sont trouvés par un tunnel. PeerProto spécifie quels protocoles sont permis par le périphérique du tunnel distant, et PeerPort place quels numéros de port peuvent être accédés à l'autre bout du tunnel.

BindTo

BindTo spécifie quel port Ethernet termine des connexions de site à site. Vous devriez toujours placer ce paramètre aux Ethernet 1, excepté quand le concentrateur VPN s'exécute en mode de port unique.

Configurer les paramètres

Pour configurer ces paramètres, sélectionnez la commande du **partenaire de tunnel VPN 1 de configurer**, répondant aux demandes avec vos informations système.

L'ordre des demandes devrait ressembler à l'exemple ci-dessous.

```
*IntraPort2+_A56CB700# configure Tunnel Partner VPN 1
      Section ?config Tunnel Partner VPN 1? not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
       =
      To find a list of valid keywords and additional help enter "?"
      *[ Tunnel Partner VPN 1 ]# transform=ESP(MD5,DES)
      *[ Tunnel Partner VPN 1 ]# sharedkey=letmein
      *[ Tunnel Partner VPN 1 ]# partner=208.203.136.10
      *[ Tunnel Partner VPN 1 ]# mode=main
      *[ Tunnel Partner VPN 1 ]# peer=10.0.0.0/8
      *[ Tunnel Partner VPN 1 ]# localaccess=192.168.233.0/24
      *[ Tunnel Partner VPN 1 ]# bindto=Ethernet 1
      *[ Tunnel Partner VPN 1 ]# exit
      Leaving section editor.
```

Maintenant il est temps de configurer la section IP.

Configurer la section IP

Vous pouvez utiliser les connexions numérotées ou non-numérotées (comme en configuration IP sur des connexions WAN) dans la section de configuration IP de chaque partenariat de tunnel. Ici, nous avons utilisé non-numéroté.

La configuration minimale pour une connexion non-numérotée de site à site exige deux déclarations : numbered=false et mode=routed. Commencez par écrire les commandes du **vpn 1 d'IP de configurer**, et répondez aux systèmes invite comme suit.

```
*[ IP Ethernet 0 ]# configure ip vpn 1
      Section ?IP VPN 1? not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IP VPN 1 ]# mode=routed
      *[ IP VPN 1 ]# numbered=false
```

Maintenant il est temps d'installer un default route.

Configurant le default route (table de routage TCP/IP)

Vous devez configurer un default route que le concentrateur VPN peut employer pour envoyer tout le trafic TCP/IP destiné pour des réseaux autres que les réseaux auxquels on le connecte directement, ou pour ce qu'il a les artères dynamiques. Le default route redésigne tous les réseaux trouvés sur le port interne. Vous avez déjà configuré l'Intraport pour envoyer le trafic d'IPSec à et de l'Internet utilisant le paramètre de passerelle d'IPSec. Pour commencer la configuration de default route, sélectionnez la commande statique d'IP de config d'éditer, répondant aux demandes avec vos informations système. L'ordre des demandes devrait ressembler à l'exemple ci-dessous.

```
*IntraPort2+_A56CB700# edit config ip static
      Section 'ip static' not found in the config.
      Do you want to add it to the config? y
      Configuration lines in this section have the following format:
      <Destination> <Mask> <Gateway> <Metric> [<Redist=(RIP|none)>]
      Editing "[ IP Static ]"...
      1: [ IP Static ]
      End of buffer
      Edit [ IP Static ]> append 1
      Enter lines at the prompt. To terminate input, enter
      a . on a line all by itself.
      Append> 0.0.0.0 0.0.0.0 192.168.233.2 1
      Append> .
      Edit [ IP Static ]> exit
      Saving section...
      Checking syntax...
      Section checked successfully.
      *IntraPort2+_A56CB700#
```

Terminer

La dernière étape est de sauvegarder la configuration. Une fois demandé si vous êtes sûr que

vous voulez télécharger la configuration et redémarrer le périphérique, le type **y** et appuient sur **entrent**. N'arrêtez pas le concentrateur VPN pendant le processus de démarrage. Après que le concentrateur ait redémarré, les utilisateurs peuvent se connecter utilisant le logiciel de client VPN du concentrateur.

Pour sauvegarder la configuration, sélectionnez la commande de **sauvegarde**, comme suit.

```
*IntraPort2+_A56CB700# save
      Save configuration to flash and restart device? y
```

Si vous êtes connecté au concentrateur VPN utilisant le telnet, la sortie ci-dessus est toute que vous verrez. Si vous êtes connecté par une console, vous verrez la sortie semblable au suivant, seulement beaucoup plus long. À l'extrémité de cette sortie, le concentrateur VPN renvoie « bonjour la console… » et demande un mot de passe. C'est comment vous savez que vous êtes de finition.

```
Codesize => 0 pfree => 462
      Updating Config variables...
      Adding section '[ General ]' to config
      Adding -- ConfiguredFrom = Command Line, from Console
      Adding -- ConfiguredOn = Timeserver not configured
      Adding -- DeviceType = IntraPort2
      Adding -- SoftwareVersion = IntraPort2 V4.5
      Adding -- EthernetAddress = 00:00:a5:6c:b7:00
      Not starting command loop: restart in progress.
      Rewriting Flash....
```

Informations connexes

- Annonce de fin de ventes de Concentrateur VPN de la gamme Cisco 5000
- Page d'assistance du concentrateur VPN Cisco 5000
- Page d'assistance du client VPN 5000 de Cisco
- Page d'assistance IPsec
- Support et documentation techniques - Cisco Systems