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 Cisco VPN 5000 et explique comment se connecter au réseau à l'aide d'IP et comment offrir une connectivité VPN IPSec LAN-à-LAN en mode principal.

Vous pouvez installer le concentrateur VPN dans l'une ou l'autre des deux configurations, selon l'endroit où vous le connectez au réseau par rapport à un pare-feu. Le concentrateur VPN possède deux ports Ethernet, dont un (Ethernet 1) transmet uniquement le trafic IPSec. L'autre port (Ethernet 0) achemine tout le trafic IP. Si vous prévoyez d'installer le concentrateur VPN en parallèle avec le pare-feu, vous devez utiliser les deux ports pour qu'Ethernet 0 fasse face au LAN protégé et Ethernet 1 fasse face à Internet via le routeur de passerelle Internet du réseau. Vous pouvez également installer le concentrateur VPN derrière le pare-feu sur le LAN protégé et le connecter via le port Ethernet 0, de sorte que le trafic IPSec passant entre Internet et le concentrateur passe par le pare-feu.

Conditions préalables

Conditions requises

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

Components Used

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

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configuration de la connectivité de base

Le moyen le plus simple d'établir une connectivité réseau de base consiste à connecter un câble série au port de console du concentrateur VPN et à utiliser le logiciel de terminal pour configurer l'adresse IP sur le port Ethernet 0. Après avoir configuré l'adresse IP sur le port Ethernet 0, vous pouvez utiliser Telnet pour vous connecter au concentrateur VPN afin de terminer la configuration. Vous pouvez également générer un fichier de configuration dans un éditeur de texte approprié et l'envoyer au concentrateur VPN à l'aide du protocole TFTP.

Àl'aide du logiciel de terminal via le port de console, vous êtes d'abord invité à saisir un mot de passe. Utilisez le mot de passe « letmein ». Après avoir répondu avec le mot de passe, exécutez la commande **configure ip ethernet 0**, en répondant aux invites avec vos informations système. La séquence d'invites doit 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 ]#
```

Vous êtes maintenant prêt à configurer le port Ethernet 1.

Configuration d'un port Ethernet 1

Les informations d'adressage TCP/IP sur le port Ethernet 1 sont l'adresse TCP/IP externe routable sur Internet que vous avez attribuée au concentrateur VPN. Évitez d'utiliser une adresse dans le même réseau TCP/IP qu'Ethernet 0, car cela désactivera TCP/IP dans le concentrateur.

Entrez les commandes **configure ip ethernet 1**, en réponse aux invites avec vos informations système. La séquence d'invites doit 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 ]#
```

Vous devez maintenant configurer la passerelle IPSec.

Configuration de la passerelle IPSec

La passerelle IPSec contrôle l'emplacement où le concentrateur VPN envoie tout le trafic IPSec, ou tunnelisé. Ceci est indépendant de la route par défaut que vous configurez ultérieurement. Commencez par entrer la commande **configure general**, en répondant aux invites avec vos informations système. La séquence des invites doit ressembler à l'exemple 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 les versions 6.x et ultérieures, la commande **ipsecgateway** a été remplacée par la commande **vpngateway**.

Maintenant, configurons la stratégie IKE (Internet Key Exchange).

Configuration de la stratégie IKE

Les paramètres ISAKMP (Internet Security Association Key Management Protocol)/IKE contrôlent la manière dont le concentrateur VPN et le client s'identifient et s'authentifient mutuellement pour établir des sessions de tunnel. Cette négociation initiale est appelée phase 1. Les paramètres de phase 1 sont globaux pour le périphérique et ne sont pas associés à une interface particulière. Les mots clés reconnus dans cette section sont décrits ci-dessous. Les paramètres de négociation de phase 1 pour les tunnels LAN à LAN peuvent être définis dans la section [Tunnel Partner <ID de section>]. La négociation IKE de phase 2 contrôle la manière dont le concentrateur VPN et le client VPN gèrent les sessions de tunnel individuelles. Les paramètres de négociation IKE de phase 2 pour le concentrateur VPN et le client VPN sont définis dans le périphérique [VPN Group <Name>].

La syntaxe de la stratégie IKE est la suivante.

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

Le mot clé protection spécifie une suite de protection pour la négociation ISAKMP/IKE entre le concentrateur VPN et le client VPN. Ce mot clé peut apparaître plusieurs fois dans cette section, auquel cas le concentrateur VPN propose toutes les suites de protection spécifiées. Le client VPN accepte l'une des options de la négociation. La première partie de chaque option, MD5 (Message

Digest 5), est l'algorithme d'authentification utilisé pour la négociation. SHA signifie Secure Hash Algorithm, qui est considéré comme plus sécurisé que MD5. La deuxième partie de chaque option est l'algorithme de chiffrement. DES (Data Encryption Standard) utilise une clé de 56 bits pour brouiller les données. Le troisième élément de chaque option est le groupe Diffie-Hellman, utilisé pour l'échange de clés. Comme les nombres plus importants sont utilisés par l'algorithme de groupe 2 (G2), il est plus sécurisé que le groupe 1 (G1).

Pour démarrer la configuration, entrez la commande **configure IKE policy**, en réponse aux invites avec les informations système. Un exemple est présenté 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 paramètres de base, il est temps de définir les paramètres de communication du tunnel et IP.

Configuration site à site en mode principal

Pour configurer le concentrateur VPN afin qu'il prenne en charge les connexions LAN à LAN, vous devez définir la configuration du tunnel, ainsi que les paramètres de communication IP à utiliser dans le tunnel. Vous allez effectuer cette opération en deux sections, la section [Tunnel Partner VPN x] et la section [IP VPN x]. Pour toute configuration site à site donnée, la *x* définie dans ces deux sections doit correspondre, de sorte que la configuration du tunnel soit correctement associée à la configuration du protocole.

Regardons chacune de ces sections en détail.

Configuration de la section Tunnel Partner

Dans la section des partenaires de tunnel, vous devez définir au moins les huit paramètres suivants.

- Transformation
- Partenaire
- KeyManage
- CléPartagée
- Mode
- Accès local
- Homologue
- LierÀ

Transformation

Le mot clé Transform spécifie les types de protection et les algorithmes utilisés pour les sessions

client IKE. Chaque option associée à ce paramètre est une pièce de protection qui spécifie les paramètres d'authentification et de chiffrement. Le paramètre Transform peut apparaître plusieurs fois dans cette section, auquel cas le concentrateur VPN propose les éléments de protection spécifiés dans l'ordre dans lequel ils sont analysés, jusqu'à ce qu'un élément soit accepté par le client pour utilisation pendant la session. Dans la plupart des cas, un seul mot clé Transform est nécessaire.

Les options du mot clé Transform sont les suivantes.

```
[ 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) ]
```

ESP signifie Encapsulating Security Payload et AH signifie Authentication Header. Ces deux en-têtes sont utilisés pour chiffrer et authentifier les paquets. DES (Data Encryption Standard) utilise une clé de 56 bits pour brouiller les données. 3DES utilise trois clés différentes et trois applications de l'algorithme DES pour brouiller les données. MD5 est l'algorithme de hachage Message-Digest 5. SHA est l'algorithme de hachage sécurisé, considéré comme un peu plus sécurisé que MD5.

ESP(MD5,DES) est le paramètre par défaut et est recommandé pour la plupart des configurations. ESP(MD5) et ESP(SHA) utilisent ESP pour authentifier les paquets (sans chiffrement). AH(MD5) et AH(SHA) utilisent AH pour authentifier les paquets. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES) et AH(SHA)+ESP(3DES) utilisent AH pour authentifier les paquets et ESP pour chiffrer les paquets.

Partenaire

Le mot clé Partner définit l'adresse IP de l'autre terminateur de tunnel dans le partenariat de tunnel. Ce numéro doit être une adresse IP publique routable avec laquelle le concentrateur VPN local peut créer une connexion IPSec.

KeyManage

Le mot clé KeyManage définit comment les deux concentrateurs VPN d'un partenariat de tunnel déterminent quel périphérique lance le tunnel et quel type de procédure d'établissement de tunnel suivre. Les options disponibles sont Auto, Initiate, Respond et Manual. Vous pouvez utiliser les trois premières options pour configurer les tunnels IKE et le mot clé Manual pour configurer les tunnels à chiffrement fixe. Ce document ne décrit pas comment configurer des tunnels à chiffrement fixe. Auto indique que le partenaire de tunnel peut à la fois initier et répondre aux demandes de configuration de tunnel. Initiate spécifie que le partenaire de tunnel envoie uniquement des demandes de configuration de tunnel, il ne leur répond pas. Respond spécifie que le partenaire de tunnel doit répondre aux demandes de configuration de tunnel, mais ne les initie jamais.

CléPartagée

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

Mode

Le mot clé Mode définit le protocole de négociation IKE. Le paramètre par défaut est Aggressive. Par conséquent, pour définir le concentrateur VPN en mode d'interopérabilité, vous devez définir le mot clé Mode sur Main.

Accès local

LocalAccess définit les numéros IP accessibles via le tunnel, d'un masque d'hôte à une route par défaut. Le mot clé LocalProto définit les numéros de protocole IP accessibles via le tunnel, tels que ICMP(1), TCP(6), UDP(17), etc. Si vous souhaitez passer tous les numéros IP, vous devez définir LocalProto=0. LocalPort détermine quels numéros de port peuvent être atteints via le tunnel. LocalProto et LocalPort ont la valeur par défaut 0, ou tout accès.

Homologue

Le mot clé Peer spécifie les sous-réseaux qui sont trouvés via un tunnel. PeerProto spécifie quels protocoles sont autorisés via le point de terminaison du tunnel distant, et PeerPort définit quels numéros de port sont accessibles à l'autre extrémité du tunnel.

LierÀ

BindTo spécifie quel port Ethernet termine les connexions de site à site. Vous devez toujours définir ce paramètre sur Ethernet 1, sauf lorsque le concentrateur VPN fonctionne en mode monoport.

Configuration des paramètres

Pour configurer ces paramètres, entrez la commande **configure Tunnel Partner VPN 1**, en réponse aux invites avec vos informations système.

La séquence d'invites doit 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.
```

Il est maintenant temps de configurer la section IP.

Configuration de la section IP

Vous pouvez utiliser des connexions numérotées ou non numérotées (comme dans la

configuration IP sur les 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 de site à site non numérotée nécessite deux instructions : numbered=false et mode=routé. Commencez par entrer les commandes **configure ip vpn 1** et répondez aux invites système 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
```

Il est maintenant temps de configurer une route par défaut.

Configuration de la route par défaut (table de routage TCP/IP)

Vous devez configurer une route par défaut que le concentrateur VPN peut utiliser pour envoyer tout le trafic TCP/IP destiné à des réseaux autres que les réseaux auxquels il est directement connecté ou pour lesquels il dispose de routes dynamiques. La route par défaut renvoie à tous les réseaux trouvés sur le port interne. Vous avez déjà configuré Intraport pour envoyer le trafic IPSec vers et depuis Internet à l'aide du paramètre de passerelle IPSec. Pour démarrer la configuration de route par défaut, entrez la commande edit config ip static, en répondant aux invites avec les informations système. La séquence d'invites doit 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#
```

Fin

La dernière étape consiste à enregistrer la configuration. Lorsque vous êtes invité à télécharger la configuration et à redémarrer le périphérique, tapez **y** et appuyez sur **Entrée**. N'éteignez pas le concentrateur VPN pendant le processus de démarrage. Une fois le concentrateur redémarré, les utilisateurs peuvent se connecter à l'aide du logiciel client VPN du concentrateur.

Pour enregistrer la configuration, entrez la commande **save**, comme suit.

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

Si vous êtes connecté au concentrateur VPN à l'aide de Telnet, le résultat ci-dessus est tout ce que vous verrez. Si vous êtes connecté via une console, la sortie s'affichera comme suit, beaucoup plus longtemps. À la fin de ce résultat, le concentrateur VPN retourne « Hello Console... ». et demande un mot de passe. C'est comme ça que tu sais que tu as fini.

```
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 commercialisation des concentrateurs Cisco VPN 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