Configuration, initiale et pour l'accès client à distance, du concentrateur Cisco VPN 5000

Contenu

Introduction

Ce guide explique la configuration initiale du concentrateur Cisco VPN 5000, en particulier comment le configurer pour se connecter au réseau à l'aide d'IP et offrir une connectivité client à distance.

Vous pouvez installer le concentrateur 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 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 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 spécification déterminée n'est requise pour ce document.

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

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 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 afin de terminer la configuration. Vous pouvez également générer un fichier de configuration dans un éditeur de texte approprié et l'envoyer au concentrateur 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 les informations système. La séquence des invites doit ressembler à ceci :

```
*[ 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.

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. Évitez d'utiliser une adresse dans le même réseau TCP/IP qu'Ethernet 0, car cela désactivera TCP/IP dans le concentrateur VPN.

Entrez les commandes **configure ip ethernet 1**, en réponse aux invites avec vos informations système. La séquence des invites doit ressembler à ceci :

```
*[ 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 route par défaut.

Route par défaut

Vous devez configurer une route par défaut que le concentrateur 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. Plus tard, vous configurerez l'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 des invites doit ressembler à ceci :

```
*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#
```

Vous devez maintenant configurer la passerelle IPSec.

Passerelle IPSec

La passerelle IPSec contrôle l'emplacement où le concentrateur envoie tout le trafic IPSec, ou tunnelisé. Ceci est indépendant de la route par défaut que vous venez de configurer. Commencez par entrer la commande **configure general**, en répondant aux invites avec vos informations système. La séquence des invites doit ressembler à ceci :

```
* 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#
```

Configurez ensuite la stratégie IKE.

Stratégie IKE

Définissez les paramètres ISAKMP/IKE (Internet Security Association Key Management Protocol/Internet Key Exchange) du concentrateur. Ces paramètres contrôlent la manière dont le concentrateur et le client s'identifient et s'authentifient mutuellement afin d'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>].

Phase 2 La négociation IKE contrôle la manière dont le concentrateur VPN et le client gèrent les sessions de tunnel individuelles. Les paramètres de négociation IKE de phase 2 pour le concentrateur VPN et le client 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. Ce mot clé peut apparaître plusieurs fois dans cette section, auquel cas le concentrateur propose toutes les suites de protection spécifiées. Le client accepte l'une des options de la négociation. La première partie de chaque option, MD-5 (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.

```
* 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 les éléments de base sont configurés, saisissez les paramètres de groupe.

Configuration du groupe VPN

Lorsque vous saisissez des paramètres de groupe, n'oubliez pas que le nom du groupe VPN ne doit pas contenir d'espaces, même si l'analyseur de ligne de commande vous permet d'entrer des espaces dans le nom du groupe VPN. Le nom du groupe VPN peut contenir des lettres, des chiffres, des tirets et des traits de soulignement.

Quatre paramètres de base sont requis dans chaque groupe VPN pour le fonctionnement IP :

- Maxconnections
- StartIPaddress ou LocalIPNet
- Transformation
- IPNet

Le paramètre Maxconnections est le nombre maximal de sessions client simultanées autorisées dans cette configuration de groupe VPN particulière. Gardez ce numéro à l'esprit, car il fonctionne avec le paramètre StartIPAddress ou LocalIPNet.

Le concentrateur VPN attribue des adresses IP à des clients distants par deux schémas différents, StartIPAddress et LocalIPNet. StartIPAddress attribue des numéros IP du sous-réseau connecté à Ethernet 0 et des proxy-arps aux clients connectés. LocalIPNet attribue des numéros IP à des clients distants à partir d'un sous-réseau unique aux clients VPN et exige que le reste du réseau soit informé de l'existence du sous-réseau VPN par le biais d'un routage statique ou dynamique. StartIPAddress facilite la configuration, mais peut limiter la taille de l'espace d'adressage. LocalIPNet offre une plus grande souplesse d'adressage pour les utilisateurs distants, mais nécessite un peu plus de travail pour configurer le routage nécessaire.

Pour StartIPAddress, utilisez la première adresse IP attribuée à une session de tunnel client entrante. Dans une configuration de base, il doit s'agir d'une adresse IP sur le réseau TCP/IP interne (le même réseau que le port Ethernet 0). Dans notre exemple ci-dessous, l'adresse 192.168.233.50 est affectée à la première session client, 192.168.233.51 est affectée à la prochaine session client simultanée, etc. Nous avons attribué une valeur Maxconnections de 30, ce qui signifie que nous devons avoir un bloc de 30 adresses IP inutilisées (y compris les serveurs DHCP si vous en avez) commençant par 192.168.233.50 et se terminant par 192.168.233.79. Évitez le chevauchement des adresses IP utilisées dans différentes configurations de groupe VPN.

LocalIPNet attribue des adresses IP à des clients distants à partir d'un sous-réseau qui doit être inutilisé ailleurs sur le réseau local. Par exemple, si vous spécifiez le paramètre LocalIPNet=182.168.1.0/24 dans la configuration du groupe VPN, le concentrateur attribue des adresses IP aux clients commençant par 192.168.1.1. Par conséquent, vous devez affecter « Maxconnections=254 », car le concentrateur ne tiendra pas compte des limites de sous-réseau lors de l'attribution de numéros IP à l'aide de LocalIPNet.

Le mot clé Transform spécifie les types de protection et les algorithmes que le concentrateur utilise pour les sessions client IKE. Les options sont les suivantes :

```
Transform = [ 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) ]
```

Chaque option est un élément de protection qui spécifie les paramètres d'authentification et de chiffrement. Ce mot-clé peut apparaître plusieurs fois dans cette section, auquel cas le concentrateur propose les pièces de protection spécifiées dans l'ordre dans lequel elles sont analysées, jusqu'à ce qu'une soit acceptée par le client pour utilisation pendant la session. Dans la plupart des cas, un seul mot clé Transform est nécessaire.

ESP(SHA, DES), ESP(SHA, 3DES), ESP(MD5, DES) et ESP(MD5, 3DES) désignent l'en-tête ESP (Encapsulating Security Payload) 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 de message-digest 5 et 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 installations. ESP(MD5) et ESP(SHA) utilisent l'en-tête ESP pour authentifier les paquets sans chiffrement. AH(MD5) et AH(SHA) utilisent l'en-tête d'authentification (AH) pour authentifier les paquets. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES) et AH(SHA)+ESP(3DES) utilisent l'en-tête d'authentification pour authentifier les paquets et l'en-tête ESP pour chiffrer les paquets.

Remarque : Le logiciel client Mac OS ne prend pas en charge l'option AH. Vous devez spécifier au moins une option ESP si vous utilisez le logiciel client Mac OS.

Le champ IPNet est important, car il contrôle l'emplacement des clients du concentrateur. Les valeurs que vous entrez dans ce champ déterminent le trafic TCP/IP tunnelisé, ou plus généralement, l'emplacement où un client appartenant à ce groupe VPN peut se rendre sur votre réseau.

Cisco recommande de configurer le réseau interne (dans cet exemple, 192.168.233.0/24), de sorte que tout le trafic d'un client se dirigeant vers le réseau interne soit envoyé via le tunnel, et donc authentifié et chiffré (si vous activez le chiffrement). Dans ce scénario, aucun autre trafic n'est tunnelisé ; au lieu de cela, il est routé normalement. Vous pouvez avoir plusieurs entrées, y compris des adresses d'hôte ou uniques. Le format est l'adresse (dans notre exemple, l'adresse réseau 192.168.233.0), puis le masque associé à cette adresse en bits (/24, qui est un masque de classe C).

Démarrez cette partie de la configuration en entrant la commande **configure VPN group basic-user**, puis répondez aux invites avec vos informations système. Voici un exemple de toute la séquence de configuration :

```
*IntraPort2+_A56CB700# configure VPN group basic-user
      Section 'VPN Group basic-user' 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 "?"
      *[ VPN Group "basic-user" ]# startipaddress=192.168.233.50
                                 or
      *[ VPN Group "basic-user" ]# localipnet=192.168.234.0/24
      *[ VPN Group "basic-user" ]# maxconnections=30
      *[ VPN Group "basic-user" ]# Transform=ESP(SHA,DES)
      *[ VPN Group "basic-user" ]# ipnet=192.168.233.0/24
      *[ VPN Group "basic-user" ]# exit
      Leaving section editor.
      *IntraPort2_A51EB700#
```

L'étape suivante consiste à définir la base de données de l'utilisateur.

Configuration utilisateur VPN

Dans cette section de la configuration, vous définissez la base de données des utilisateurs VPN. Chaque ligne définit un utilisateur VPN ainsi que la configuration et le mot de passe du groupe VPN de cet utilisateur. Les sauts de ligne des entrées multilignes doivent se terminer par une barre oblique inverse. Cependant, les sauts de ligne entre guillemets doubles sont conservés.

Lorsqu'un client VPN démarre une session de tunnel, le nom d'utilisateur du client est transmis au périphérique. Si le périphérique trouve l'utilisateur dans cette section, il utilise les informations de

l'entrée pour configurer le tunnel. (Vous pouvez également utiliser un serveur RADIUS pour l'authentification des utilisateurs VPN). Si le périphérique ne trouve pas le nom d'utilisateur et que vous n'avez pas configuré de serveur RADIUS pour effectuer l'authentification, la session de tunnel n'est pas ouverte et une erreur est renvoyée au client.

Démarrez la configuration en entrant la commande **edit config VPN users**. Examinons un exemple qui ajoute un utilisateur nommé « User1 » au groupe VPN « basic-user ».

```
*IntraPort2+_A56CB700# edit config VPN users
      Section 'VPN users' not found in the config.
      Do you want to add it to the config? y
      <Name> <Config> <SharedKey>
      Editing "[ VPN Users ]"...
      1: [ VPN Users ]
      End of buffer
      Edit [ VPN Users ]> append 1
      Enter lines at the prompt. To terminate input, enter
      a . on a line all by itself.
      Append> User1 Config="basic-user" SharedKey="Burnt"
      Append> .
      Edit [ VPN Users ]> exit
      Saving section...
      Checking syntax...
      Section checked successfully.
      *IntraPort2+_A56CB700#
```

SharedKey de cet utilisateur est « Burnt ». Toutes ces valeurs de configuration sont sensibles à la casse ; si vous configurez « User1 », l'utilisateur doit entrer « User1 » dans le logiciel client. La saisie de « user1 » entraîne un message d'erreur utilisateur non valide ou non autorisé. Vous pouvez continuer à entrer des utilisateurs au lieu de quitter l'éditeur, mais n'oubliez pas que vous devez entrer un point pour quitter l'éditeur. Si vous ne le faites pas, les entrées de la configuration peuvent être incorrectes.

Fin

Votre 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 la touche Entrée. N'éteignez pas le concentrateur 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 à l'aide de Telnet, la sortie ci-dessus est tout ce que vous verrez. Si vous êtes connecté via une console, la sortie s'affiche comme suit, mais beaucoup plus longtemps. À la fin de cette sortie, le concentrateur 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