Erstmaliges Einrichten des Cisco VPN 500 Concentrator und für den Remote-Client-Zugriff

Inhalt

Einführung

In diesem Leitfaden wird die anfängliche Konfiguration des Cisco VPN 500 Concentrator beschrieben. Es wird erläutert, wie dieser so konfiguriert wird, dass er über IP eine Verbindung zum Netzwerk herstellt und Remoteclient-Verbindungen bereitstellt.

Sie können den Konzentrator in einer von zwei Konfigurationen installieren, je nachdem, wo Sie ihn mit dem Netzwerk in Verbindung mit einer Firewall verbinden. Der Konzentrator verfügt über zwei Ethernet-Ports, von denen einer (Ethernet 1) nur IPSec-Datenverkehr weiterleitet. Der andere Port (Ethernet 0) leitet den gesamten IP-Datenverkehr weiter. Wenn Sie planen, den VPN-Konzentrator parallel zur Firewall zu installieren, müssen Sie beide Ports verwenden, sodass Ethernet 0 mit dem geschützten LAN verbunden ist und Ethernet 1 mit dem Internet über den Internet-Gateway-Router des Netzwerks verbunden ist. Sie können auch den Konzentrator hinter der Firewall im geschützten LAN installieren und ihn über den Ethernet 0-Port verbinden, sodass der IPSec-Datenverkehr zwischen dem Internet und dem Konzentrator über die Firewall geleitet wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco VPN 500 Concentrator.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Grundlegende Verbindungskonfiguration

Die einfachste Methode zum Herstellen einer grundlegenden Netzwerkverbindung besteht darin, ein serielles Kabel an den Konsolenport am Konzentrator anzuschließen und die IP-Adresse am Ethernet 0-Port mithilfe einer Terminalsoftware zu konfigurieren. Nachdem Sie die IP-Adresse auf dem Ethernet 0-Port konfiguriert haben, können Sie Telnet verwenden, um die Konfiguration abzuschließen. Sie können auch eine Konfigurationsdatei in einem entsprechenden Texteditor generieren und mit TFTP an den Konzentrator senden.

Bei Verwendung von Terminalsoftware über den Konsolenport werden Sie zunächst zur Eingabe eines Kennworts aufgefordert. Verwenden Sie das Kennwort "letmein". Nachdem Sie mit dem Kennwort geantwortet haben, geben Sie den Befehl **configure ip Ethernet 0** ein, und antworten Sie mit Ihren Systeminformationen auf Eingabeaufforderungen. Die Abfolge der Aufforderungen sollte wie folgt aussehen:

```
*[ 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 ]#
```

Jetzt können Sie den Ethernet 1-Port konfigurieren.

Ethernet 1-Port

Die TCP/IP-Adressinformationen am Ethernet 1-Port sind die externe, über das Internet routbare TCP/IP-Adresse, die Sie dem Konzentrator zugewiesen haben. Verwenden Sie keine Adresse im selben TCP/IP-Netzwerk wie Ethernet 0, da TCP/IP im VPN-Konzentrator deaktiviert wird.

Geben Sie die Befehle **configure ip ethernet 1** ein, und antworten Sie auf Eingabeaufforderungen mit Ihren Systeminformationen. Die Abfolge der Aufforderungen sollte wie folgt aussehen:

```
*[ 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 ]#
```

Jetzt müssen Sie die Standardroute konfigurieren.

Standardroute

Sie müssen eine Standardroute konfigurieren, die der Konzentrator verwenden kann, um den gesamten TCP/IP-Datenverkehr zu senden, der für Netzwerke bestimmt ist, die nicht direkt mit dem Netzwerk verbunden sind oder für die dynamische Routen bestehen. Die Standardroute verweist zurück auf alle Netzwerke, die auf dem internen Port gefunden wurden. Später konfigurieren Sie den Intraport so, dass IPSec-Datenverkehr über den IPSec-Gateway-Parameter an das Internet und aus dem Internet gesendet wird. Um die Standardroute-Konfiguration zu starten, geben Sie den Befehl edit config ip static ein, und antworten Sie auf Aufforderungen mit Ihren Systeminformationen. Die Abfolge der Aufforderungen sollte wie folgt aussehen:

```
*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#
```

Jetzt müssen Sie das IPSec-Gateway konfigurieren.

IPSec-Gateway

Das IPSec-Gateway steuert, wo der Konzentrator den gesamten IPSec- oder getunnelten Datenverkehr sendet. Dies ist unabhängig von der Standardroute, die Sie gerade konfiguriert haben. Geben Sie zunächst den Befehl **configure** ein, und antworten Sie auf Eingabeaufforderungen mit Ihren Systeminformationen. Die Abfolge der Aufforderungen sollte wie folgt aussehen:

```
* 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#
```

Konfigurieren Sie anschließend die IKE-Richtlinie.

IKE-Richtlinie

Legen Sie die ISAKMP/IKE-Parameter (Internet Security Association Key Management Protocol/Internet Key Exchange) für den Konzentrator fest. Diese Einstellungen steuern, wie der Konzentrator und der Client einander identifizieren und authentifizieren, um Tunnelsitzungen einzurichten. Diese erste Aushandlung wird als Phase 1 bezeichnet. Phase-1-Parameter sind für das Gerät global und nicht mit einer bestimmten Schnittstelle verknüpft. Die in diesem Abschnitt erkannten Schlüsselwörter werden nachfolgend beschrieben. Phase-1-Verhandlungsparameter für LAN-zu-LAN-Tunnel können im Abschnitt [Tunnel-Partner <Abschnitt-ID>] festgelegt werden.

In Phase 2 der IKE-Aushandlung wird gesteuert, wie der VPN-Konzentrator und der Client einzelne Tunnelsitzungen behandeln. Phase 2 IKE-Verhandlungsparameter für den VPN-Konzentrator und den Client werden im Gerät [VPN Group <Name>] festgelegt.

Die Syntax für IKE-Richtlinien lautet wie folgt:

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

Das protection-Schlüsselwort legt eine Schutzsuite für die ISAKMP/IKE-Aushandlung zwischen dem VPN-Concentrator und dem Client fest. Dieses Schlüsselwort kann in diesem Abschnitt mehrfach vorkommen. In diesem Fall schlägt der Konzentrator alle angegebenen Schutzsuiten vor. Der Client akzeptiert eine der Optionen für die Aushandlung. Das erste Element jeder Option, MD-5 (Message-Digest 5), ist der für die Aushandlung verwendete Authentifizierungsalgorithmus. SHA steht für Secure Hash Algorithm, der als sicherer gilt als MD5. Der zweite Teil jeder Option ist der Verschlüsselungsalgorithmus. DES (Data Encryption Standard) verwendet einen 56-Bit-Schlüssel, um die Daten zu verschlüsseln. Das dritte Element jeder Option ist die Diffie-Hellman-Gruppe, die für den Schlüsselaustausch verwendet wird. Da der Algorithmus der Gruppe 2 (G2) größere Zahlen verwendet, ist er sicherer als der Algorithmus der Gruppe 1 (G1).

Um die Konfiguration zu starten, geben Sie den Befehl **configure IKE policy (IKE-Richtlinie konfigurieren**) ein, und antworten Sie auf die Aufforderungen mit Ihren Systeminformationen.

```
* 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#
```

Nachdem die Grundlagen konfiguriert sind, geben Sie die Gruppenparameter ein.

VPN-Gruppenkonfiguration

Beachten Sie bei der Eingabe von Gruppenparametern, dass der VPN-Gruppenname keine Leerzeichen enthalten darf, auch wenn Sie mit dem Befehlszeilenparser Leerzeichen im VPN-Gruppennamen eingeben können. Der VPN-Gruppenname kann Buchstaben, Zahlen, Bindestriche und Unterstriche enthalten.

Für den IP-Betrieb sind in jeder VPN-Gruppe vier grundlegende Parameter erforderlich:

- Maximale Verbindungen
- StartIPaddress oder LocalIPNet
- Transformation
- IPNet

Der Parameter "Maxconnections" ist die maximale Anzahl gleichzeitiger Client-Sitzungen, die in dieser bestimmten VPN-Gruppenkonfiguration zulässig ist. Beachten Sie diese Nummer, da sie zusammen mit dem StartIPAddress-Parameter oder dem LocalIPNet-Parameter verwendet wird.

Der VPN Concentrator weist Remote-Clients IP-Adressen durch zwei verschiedene Schemata zu: StartIPAddress und LocalIPNet. StartIPAddress weist IP-Nummern aus dem mit Ethernet 0 verbundenen Subnetz und Proxy-Arps für die angeschlossenen Clients zu. LocalIPNet weist Remote-Clients IP-Nummern von einem Subnetz zu, das für die VPN-Clients eindeutig ist. Das übrige Netzwerk muss über statisches oder dynamisches Routing auf das Vorhandensein des VPN-Subnetzes aufmerksam gemacht werden. StartIPAddress bietet eine einfachere Konfiguration, kann jedoch die Größe des Adressbereichs einschränken. LocalIPNet bietet mehr Flexibilität bei der Adressierung von Remote-Benutzern, erfordert jedoch etwas mehr Arbeit bei der Konfiguration des erforderlichen Routings.

Verwenden Sie für StartIPAddress die erste IP-Adresse, die einer eingehenden Client-Tunnel-Sitzung zugewiesen ist. In einer grundlegenden Konfigurationseinrichtung sollte es sich um eine IP-Adresse im internen TCP/IP-Netzwerk (das gleiche Netzwerk wie der Ethernet 0-Port) handeln. In unserem Beispiel unten wird der ersten Clientsitzung die Adresse 192.168.233.50 zugewiesen, der nächsten gleichzeitigen Clientsitzung wird 192.168.233.51 usw. zugewiesen. Wir haben einen Wert für maximale Verbindungen von 30 zugewiesen. Das bedeutet, dass wir einen Block von 30 ungenutzten IP-Adressen (einschließlich DHCP-Server, falls vorhanden) benötigen, der mit 192.168.233.50 beginnt und mit 192.168.233.79 endet. Vermeiden Sie Überschneidungen bei den IP-Adressen, die in verschiedenen VPN-Gruppen-Konfigurationen verwendet werden.

LocalIPNet weist Remote-Clients IP-Adressen aus einem Subnetz zu, das an anderer Stelle im LAN nicht verwendet werden darf. Wenn Sie beispielsweise in der VPN-Gruppenkonfiguration den Parameter "LocalIPNet=182.168.1.0/24" angeben, weist der Konzentrator Clients ab 192.168.1.1 IP-Adressen zu. Daher müssen Sie "Maxconnections=254" zuweisen, da der Konzentrator bei der Zuweisung von IP-Nummern mit LocalIPNet keine Subnetzgrenzen beachtet.

Das Transform-Schlüsselwort legt die Schutztypen und Algorithmen fest, die der Konzentrator für IKE-Clientsitzungen verwendet. Folgende Optionen sind verfügbar:

```
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) ]
```

Jede Option ist ein Schutzelement, das Authentifizierungs- und Verschlüsselungsparameter angibt. Dieses Schlüsselwort kann in diesem Abschnitt mehrmals vorkommen. In diesem Fall schlägt der Konzentrator die angegebenen Schutzelemente in der Reihenfolge vor, in der sie analysiert werden, bis sie vom Client zur Verwendung während der Sitzung akzeptiert werden. In den meisten Fällen wird nur ein Transform-Schlüsselwort benötigt.

ESP(SHA, DES), ESP(SHA, 3DES), ESP(MD5, DES) und ESP(MD5, 3DES) bezeichnen den ESP-Header (Encapsulating Security Payload) zum Verschlüsseln und Authentifizieren von Paketen. DES (Data Encryption Standard) verwendet einen 56-Bit-Schlüssel, um die Daten zu verschlüsseln. 3DES verwendet drei verschiedene Schlüssel und drei Anwendungen des DES-Algorithmus, um die Daten zu verschlüsseln. MD5 ist der Message-Digest-5-Hash-Algorithmus, und SHA ist der Secure Hash Algorithm, der als etwas sicherer gilt als MD5.

ESP(MD5,DES) ist die Standardeinstellung und wird für die meisten Installationen empfohlen. ESP(MD5) und ESP(SHA) authentifizieren mithilfe des ESP-Headers Pakete ohne Verschlüsselung. AH(MD5) und AH(SHA) authentifizieren mithilfe des Authentifizierungs-Headers (AH) Pakete. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES) und AH(SHA)+ESP(3DES) authentifizieren mithilfe des Authentifizierungs-Headers Pakete und des ESP-Headers Pakete.

Hinweis: Die Mac OS Client-Software unterstützt die AH-Option nicht. Sie sollten mindestens eine ESP-Option angeben, wenn Sie die Mac OS-Client-Software verwenden.

Das IPNet-Feld ist wichtig, da es steuert, wohin die Concentrator-Clients gehen können. Die Werte, die Sie in diesem Feld eingeben, bestimmen, welcher TCP/IP-Datenverkehr getunnelt wird, oder häufiger, wo ein Client, der zu dieser VPN-Gruppe gehört, in Ihrem Netzwerk navigieren kann.

Cisco empfiehlt, das interne Netzwerk zu konfigurieren (in diesem Beispiel 192.168.233.0/24), sodass der gesamte Datenverkehr von einem Client, der zum internen Netzwerk führt, über den Tunnel gesendet wird und daher authentifiziert und verschlüsselt ist (wenn Sie die Verschlüsselung aktivieren). In diesem Szenario wird kein anderer Datenverkehr getunnelt. Stattdessen wird es normal geroutet. Sie können mehrere Einträge haben, einschließlich Einzel- oder Hostadressen. Das Format ist die Adresse (in unserem Beispiel die Netzwerkadresse 192.168.233.0) und anschließend die Maske, die dieser Adresse zugeordnet ist (Bit/24, eine Maske der Klasse C).

Starten Sie diesen Teil der Konfiguration, indem Sie den Befehl **configure VPN group basic-user** eingeben und dann auf die Aufforderungen mit Ihren Systeminformationen antworten. Hier ein Beispiel für die gesamte Konfigurationssequenz:

```
*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#
```

Im nächsten Schritt wird die Datenbank des Benutzers definiert.

VPN-Benutzerkonfiguration

In diesem Abschnitt der Konfiguration definieren Sie die VPN-Benutzerdatenbank. Jede Leitung definiert einen VPN-Benutzer zusammen mit der Konfiguration und dem Kennwort der VPN-Gruppe dieses Benutzers. Mehrzeilige Einträge müssen Zeilenumbrüche aufweisen, die mit einem umgekehrten Schrägstrich enden. Zeilenumbrüche, die in doppelte Anführungszeichen eingebettet sind, bleiben jedoch erhalten.

Wenn ein VPN-Client eine Tunnelsitzung startet, wird der Benutzername des Clients an das Gerät übertragen. Wenn das Gerät den Benutzer in diesem Abschnitt findet, verwendet es die Informationen im Eintrag, um den Tunnel einzurichten. (Sie können auch einen RADIUS-Server für die Authentifizierung von VPN-Benutzern verwenden). Wenn das Gerät den Benutzernamen nicht findet und Sie keinen RADIUS-Server für die Authentifizierung konfiguriert haben, wird die Tunnelsitzung nicht geöffnet, und es wird ein Fehler an den Client zurückgegeben.

Starten Sie die Konfiguration, indem Sie den Befehl **Edit config VPN users** eingeben. Sehen wir uns ein Beispiel an, in dem der VPN-Gruppe ein Benutzer mit dem Namen "User1" (Benutzer1) hinzugefügt wird.

```
*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#
```

Der SharedKey dieses Benutzers ist "gebrannt". Bei allen diesen Konfigurationswerten wird die Groß- und Kleinschreibung beachtet. Wenn Sie "User1" konfigurieren, muss der Benutzer "User1" in die Client-Software eingeben. Die Eingabe von "user1" führt zu einer ungültigen oder nicht autorisierten Benutzerfehlermeldung. Sie können weiterhin Benutzer eingeben, statt den Editor zu verlassen. Denken Sie jedoch daran, dass Sie einen Punkt eingeben müssen, um den Editor zu verlassen. Andernfalls kann es zu ungültigen Einträgen in der Konfiguration kommen.

Abschließen

Der letzte Schritt ist das Speichern der Konfiguration. Wenn Sie gefragt werden, ob Sie sicher sind, dass Sie die Konfiguration herunterladen und das Gerät neu starten möchten, geben Sie y ein, und drücken Sie die Eingabetaste. Schalten Sie den Konzentrator beim Booten nicht aus. Nachdem der Konzentrator neu gestartet wurde, können Benutzer die Verbindung über die Concentrator VPN Client-Software herstellen.

Um die Konfiguration zu speichern, geben Sie den Befehl **save** wie folgt ein:

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

Wenn Sie über Telnet mit dem Konzentrator verbunden sind, wird Ihnen nur die oben angegebene Ausgabe angezeigt. Wenn Sie über eine Konsole verbunden sind, wird die Ausgabe ähnlich der folgenden angezeigt, nur viel länger. Am Ende dieser Ausgabe gibt der Konzentrator "Hello Console.." zurück. und fordert ein Kennwort an. So weißt du, dass du fertig bist.

```
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....
```

Zugehörige Informationen

- Cisco VPN Concentrators der Serie 5000 - Ankündigung des Vertriebsendes
- Support-Seite für Cisco VPN 500 Concentrator
- Support-Seite für Cisco VPN 5000-Client
- IPsec-Support-Seite
- Technischer Support und Dokumentation - Cisco Systems