Konfigurieren des Cisco VPN 500-Konzentrators und Implementieren der IPSec-VPN-Verbindung im Hauptmodus (LAN-to-LAN)

Inhalt

Einführung

In diesem Dokument wird die Erstkonfiguration des Cisco VPN 500 Concentrator erläutert. Außerdem wird veranschaulicht, wie die Verbindung mit dem Netzwerk über IP hergestellt wird und wie IPSec-Hauptmodus-LAN-zu-LAN-VPN-Verbindungen bereitgestellt werden.

Sie können den VPN Concentrator in einer der beiden Konfigurationen installieren, je nachdem, wo Sie ihn mit dem Netzwerk in Verbindung mit einer Firewall verbinden. Der VPN Concentrator verfügt über zwei Ethernet-Ports, von denen einer (Ethernet 1) nur IPSec-Datenverkehr leitet. 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 VPN-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 besonderen Voraussetzungen.

Verwendete Komponenten

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

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

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 des VPN Concentrator 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 mit dem VPN-Concentrator abzuschließen. Sie können auch eine Konfigurationsdatei in einem entsprechenden Texteditor generieren und über TFTP an den VPN Concentrator 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 Aufforderungen. Die Abfolge der Aufforderungen sollte wie im folgenden Beispiel 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.

Konfigurieren von Ethernet 1-Port

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

Konfigurieren des IPSec-Gateways

Das IPSec-Gateway steuert, wo der VPN Concentrator den gesamten IPSec- oder getunnelten Datenverkehr sendet. Dies ist unabhängig von der Standardroute, die Sie später konfigurieren. Geben Sie zunächst den Befehl **configure** ein, und antworten Sie auf Eingabeaufforderungen mit Ihren Systeminformationen. Die Abfolge der Aufforderungen sollte dem Beispiel unten entsprechen.

```
* 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#
```

Hinweis: In Version 6.x und höher wurde der Befehl **ipsecgateway** in den Befehl **vpngateway** geändert.

Konfigurieren wir nun die IKE-Richtlinie (Internet Key Exchange).

Konfigurieren der IKE-Richtlinie

Die ISAKMP/IKE-Parameter (Internet Security Association Key Management Protocol) steuern, wie der VPN-Konzentrator und der Client sich 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 Concentrator und der VPN Client einzelne Tunnelsitzungen verarbeiten. Phase 2 IKE-Verhandlungsparameter für den VPN-Konzentrator und den VPN-Client werden im Gerät [VPN-Gruppe <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 VPN-Client fest. Dieses Schlüsselwort kann in diesem Abschnitt mehrfach vorkommen. In diesem Fall schlägt der VPN Concentrator alle angegebenen Schutzsuiten vor. Der VPN-Client akzeptiert eine der Optionen für die Aushandlung. Das erste Element jeder Option, MD5 (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. Ein Beispiel ist unten dargestellt.

```
* 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 Sie die Grundlagen konfiguriert haben, ist es an der Zeit, die Tunnel- und IP-Kommunikationsparameter zu definieren.

Konfiguration zwischen Standorten im Hauptmodus

Um den VPN Concentrator für die Unterstützung von LAN-zu-LAN-Verbindungen zu konfigurieren, müssen Sie die Tunnelkonfiguration sowie die im Tunnel zu verwendenden IP-Kommunikationsparameter definieren. Dies erfolgt in zwei Abschnitten: [Tunnel Partner VPN x] und [IP VPN x]. Für jede beliebige standortübergreifende Konfiguration muss das *x*, das in diesen beiden Abschnitten definiert ist, übereinstimmen, damit die Tunnelkonfiguration der Protokollkonfiguration ordnungsgemäß zugeordnet wird.

Schauen wir uns die einzelnen Abschnitte genauer an.

Konfigurieren des Abschnitts "Tunnel Partner"

Im Tunnelpartnerabschnitt müssen mindestens die folgenden acht Parameter definiert werden.

- Transformation
- Partner
- KeyManage
- SharedKey
- Modus
- Lokaler Zugriff
- Peer

- BindTo

Transformation

Das Transform-Schlüsselwort legt die für IKE-Clientsitzungen verwendeten Schutztypen und Algorithmen fest. Jede diesem Parameter zugeordnete Option ist ein Schutzelement, das Authentifizierungs- und Verschlüsselungsparameter angibt. Der Transform-Parameter kann in diesem Abschnitt mehrmals angezeigt werden. In diesem Fall schlägt der VPN Concentrator 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.

Die Optionen für das Transform-Schlüsselwort lauten wie folgt.

```
[ 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 steht für Encapsulating Security Payload, und AH steht für Authentication Header. Beide Header werden zum Verschlüsseln und Authentifizieren von Paketen verwendet. 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. SHA ist der Secure Hash Algorithm, der als etwas sicherer gilt als MD5.

ESP(MD5,DES) ist die Standardeinstellung und wird für die meisten Konfigurationen empfohlen. ESP(MD5) und ESP(SHA) verwenden ESP zur Authentifizierung von Paketen (ohne Verschlüsselung). AH(MD5) und AH(SHA) verwenden AH, um Pakete zu authentifizieren. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES) und AH(SHA)+ESP(3DES) authentifizieren mithilfe von AH Pakete und ESP Pakete.

Partner

Das Partner-Schlüsselwort definiert die IP-Adresse des anderen Tunnelterminators in der Tunnelpartnerschaft. Diese Nummer muss eine öffentliche, routbare IP-Adresse sein, mit der der lokale VPN Concentrator eine IPSec-Verbindung herstellen kann.

KeyManage

Das KeyManage-Schlüsselwort definiert, wie die beiden VPN-Concentrators in einer Tunnelpartnerschaft bestimmen, welches Gerät den Tunnel initiiert und welche Art von Tunnelerstellungsverfahren zu befolgen ist. Die Optionen sind Auto (Automatisch), Initiate (Initiieren), Response (Antworten) und Manual (Manuell). Sie können die ersten drei Optionen verwenden, um IKE-Tunnel zu konfigurieren, und das Schlüsselwort Manual, um festkonfigurierte Verschlüsselungstunnel zu konfigurieren. In diesem Dokument wird nicht erläutert, wie Tunnel mit fester Verschlüsselung konfiguriert werden. Auto gibt an, dass der Tunnel-Partner sowohl Tunnel-Setup-Anfragen initiieren als auch darauf reagieren kann. Initiate gibt an, dass der Tunnelpartner nur Tunneleinrichtungsanfragen sendet, aber nicht darauf reagiert. Die Antwort gibt an, dass Tunnelpartner auf Anfragen zur Einrichtung von Tunneln reagieren, diese jedoch nie initiieren.

SharedKey

Das SharedKey-Schlüsselwort wird als IKE Shared geheim verwendet. Sie müssen für beide Tunnelpartner denselben SharedKey-Wert festlegen.

Modus

Das Mode-Schlüsselwort definiert das IKE-Verhandlungsprotokoll. Die Standardeinstellung ist Aggressive (Aggressiv). Um den VPN Concentrator für den Interoperabilitätsmodus festzulegen, müssen Sie das Mode-Schlüsselwort auf Main (Hauptmodus) festlegen.

Lokaler Zugriff

LocalAccess definiert IP-Nummern, auf die über den Tunnel zugegriffen werden kann, von einer Hostmaske bis hin zu einer Standardroute. Das LocalProto-Schlüsselwort definiert, auf welche IP-Protokollnummern über den Tunnel zugegriffen werden kann, z. B. ICMP(1), TCP(6), UDP(17) usw. Wenn Sie alle IP-Nummern übergeben möchten, sollten Sie LocalProto=0 festlegen. LocalPort bestimmt, welche Portnummern durch den Tunnel erreicht werden können. Sowohl LocalProto als auch LocalPort setzen die Standardeinstellung auf 0 oder den Allzugriff.

Peer

Das Peer-Schlüsselwort gibt an, welche Subnetze durch einen Tunnel gefunden werden. PeerProto legt fest, welche Protokolle durch den Endpunkt des Remote-Tunnels zugelassen werden, und PeerPort legt fest, auf welche Portnummern am anderen Ende des Tunnels zugegriffen werden kann.

BindTo

BindTo gibt an, welcher Ethernet-Port Site-to-Site-Verbindungen terminiert. Sie sollten diesen Parameter immer auf Ethernet 1 setzen, außer wenn der VPN-Konzentrator im Single-Port-Modus ausgeführt wird.

Konfigurieren der Parameter

Um diese Parameter zu konfigurieren, geben Sie den Befehl **configure Tunnel Partner VPN 1** ein, und antworten Sie auf Eingabeaufforderungen mit Ihren Systeminformationen.

Die Abfolge der Aufforderungen sollte wie im Beispiel unten aussehen.

```
*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.
```

Jetzt ist es an der Zeit, den IP-Abschnitt zu konfigurieren.

Konfigurieren des IP-Abschnitts

Sie können nummerierte oder unnummerierte Verbindungen (wie in der IP-Konfiguration für WAN-Verbindungen) im IP-Konfigurationsabschnitt jeder Tunnelpartnerschaft verwenden. Hier haben wir unnummeriert verwendet.

Die Mindestkonfiguration für eine nicht nummerierte Site-to-Site-Verbindung erfordert zwei Anweisungen: numbered=false und mode=geroutet. Geben Sie zunächst die Befehle **configure ip vpn 1 ein**, und beantworten Sie die Systemaufforderungen wie folgt.

```
*[ 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
```

Jetzt ist es an der Zeit, eine Standardroute einzurichten.

Konfigurieren der Standardroute (TCP/IP-Routentabelle)

Sie müssen eine Standardroute konfigurieren, die der VPN Concentrator verwenden kann, um den gesamten TCP/IP-Datenverkehr zu senden, der für Netzwerke bestimmt ist, die nicht mit dem Netzwerk verbunden sind, mit dem er direkt verbunden ist, oder für die er dynamische Routen hat. Die Standardroute verweist zurück auf alle Netzwerke, die auf dem internen Port gefunden wurden. Sie haben den Intraport bereits so konfiguriert, dass er IPSec-Datenverkehr mit dem IPSec-Gateway-Parameter an das Internet und aus dem Internet sendet. 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 im Beispiel unten 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#
```

Abschließen

Der letzte Schritt besteht darin, die Konfiguration zu speichern. 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 während des Startvorgangs den VPN-Konzentrator nicht aus. Nachdem der Konzentrator neu gestartet wurde, können sich Benutzer über die VPN Client-Software des Konzentrators verbinden.

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 VPN-Concentrator verbunden sind, wird nur die oben angegebene Ausgabe angezeigt. Wenn Sie über eine Konsole verbunden sind, sehen Sie die Ausgabe ähnlich der folgenden, nur viel länger. Am Ende dieser Ausgabe gibt der VPN Concentrator "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