De Cisco VPN 5000 Concentrator aanvankelijk instellen en voor toegang tot externe client

Inhoud

Inleiding

Deze handleiding legt de eerste configuratie van Cisco VPN 5000 Concentrator uit, specifiek hoe u deze kunt configureren om verbinding te maken met het netwerk via IP, en biedt connectiviteit op afstand aan.

U kunt de concentrator in een van beide configuraties installeren, afhankelijk van de plaats waar u de concentrator met het netwerk verbindt in relatie tot een firewall. De concentrator heeft twee Ethernet poorten, waarvan (Ethernet 1) alleen IPSec-verkeer doorgeeft. De andere haven (Ethernet 0) routeert al IP verkeer. Als u van plan bent om de VPN Concentrator parallel met de firewall te installeren, moet u beide poorten gebruiken zodat Ethernet 0 interfaces op het beschermde LAN, en Ethernet 1 gezichten op het internet door de Internet gateway router van het netwerk. U kunt de concentrator achter de firewall ook installeren op het beschermde LAN en deze via de Ethernet 0-poort aansluiten, zodat het IPSec-verkeer dat tussen het internet en de concentrator verloopt, door de firewall wordt doorgegeven.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco VPN 5000 Concentrator.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Configuratie van basisverbindingen

De makkelijkste manier om basisnetwerkconnectiviteit in te stellen is een seriekabel aan de troostpoort op de concentrator aan te sluiten en eindsoftware te gebruiken om het IP adres op Ethernet 0 haven te vormen. Na het configureren van het IP-adres op Ethernet 0 poort kunt u telnet gebruiken om verbinding te maken met de concentrator om de configuratie te voltooien. U kunt ook een configuratiebestand in een geschikte teksteditor genereren en het naar de concentrator sturen met TFTP.

Gebruikend van eindsoftware door de console poort wordt u aanvankelijk gevraagd om een wachtwoord. Gebruik het wachtwoord "achterlaten". Nadat u met het wachtwoord hebt geantwoord, geeft u de **configuratie ip Ethernet 0** opdracht uit, in antwoord op aanwijzingen met uw systeeminformatie. De volgorde van de aanwijzingen moet er als volgt uitzien:

```
*[ 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 ]#
```

Nu bent u klaar om de Ethernet 1 poort te configureren.

Ethernet 1 poort

De TCP/IP adresserende informatie op de Ethernet 1 poort is het externe, Internet-routeerbare TCP/IP adres dat u voor de concentrator hebt toegewezen. Gebruik geen adres in hetzelfde TCP/IP-netwerk als Ethernet 0, omdat dit TCP/IP in de VPN-centrator uitschakelt.

Voer de opdrachten **ip Ethernet 1 in** die reageren op aanwijzingen met uw systeeminformatie. De volgorde van de aanwijzingen moet er als volgt uitzien:

```
*[ 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 ]#
```

Nu moet u de standaardroute configureren.

Standaard route

U dient een standaardroute te configureren die de concentrator kan gebruiken om al het TCP/IP-verkeer te verzenden dat bestemd is voor netwerken anders dan het netwerk of de netwerken waartoe het direct is aangesloten, of voor welke dynamische routes het heeft. De standaardroute wijst terug naar alle netwerken die op de interne poort zijn gevonden. Later, zult u het Intraport vormen om IPSec verkeer naar en van het Internet te verzenden met behulp van de parameter van de Gateway van IPSec. Om de standaardrouteconfiguratie te starten, voer het bestand van de configuratie ip uit, dat reageert op aanwijzingen met uw systeeminformatie. De volgorde van de aanwijzingen moet er als volgt uitzien:

```
*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#
```

Nu moet u de gateway van IPSec configureren.

IPsec-gateway

De gateway van IPSec controleert waar de concentrator al het IPSec- of tunnelverkeer verstuurt. Dit is onafhankelijk van de standaard route die u zojuist hebt ingesteld. Start door de opdracht **Configuration General in te** voeren, die reageert op aanwijzingen met uw systeeminformatie. De volgorde van de aanwijzingen moet er als volgt uitzien:

```
* 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#
```

Stel vervolgens het IKE-beleid in.

IKE-beleid

Stel de parameters van de Internet Security Association Key Management Protocol/Internet Key Exchange (ISAKMP/IKE) in voor de concentrator. Deze instellingen controleren hoe de concentrator en de client elkaar identificeren en authentiek verklaren om tunnelsessies op te zetten. Deze initiële onderhandeling wordt fase 1 genoemd. Fase 1-parameters zijn globaal ten opzichte van het apparaat en worden niet geassocieerd met een bepaalde interface. Trefwoorden die in dit gedeelte zijn herkend, worden hieronder beschreven. Fase 1 onderhandelingsparameters voor LAN-to-LAN tunnels kunnen worden ingesteld in het gedeelte [Tunnel partner <Section ID>].

Fase 2 IKE onderhandeling controleert hoe de VPN Concentrator en de client afzonderlijke tunnelsessies behandelen. Fase 2 IKE-onderhandelingsparameters voor VPN-concentratie en -client worden ingesteld in het apparaat [VPN Group <Name>]

De syntaxis voor IKE Policy is als volgt:

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

Het sleutelwoord van de bescherming specificeert een beschermingsreeks voor de onderhandeling van ISAKMP/IKE tussen de Concentrator en de cliënt van VPN. Dit sleutelwoord kan meerdere keren binnen deze sectie verschijnen, in welk geval de concentrator alle gespecificeerde veiligheidskoffers voorstelt. De klant accepteert een van de opties voor de onderhandeling. Het eerste stuk van elke optie, MD-5 (berichtverwant 5), is de authenticatie algoritme die voor de onderhandeling wordt gebruikt. SHA staat voor Secure Hash Algorithm, dat als veiliger wordt beschouwd dan MD5. Het tweede deel van elke optie is het encryptiealgoritme. DES (Data Encryption Standard) gebruikt een 56-bits toets om de gegevens te versleutelen. Het derde deel van elke optie is de Diffie-Hellman groep, gebruikt voor belangrijke uitwisseling. Omdat grotere getallen door het G2 (Group 2) algoritme worden gebruikt, is het veiliger dan Groep 1 (G1).

Om de configuratie te starten dient u de opdracht **IKE-beleid** te **configureren** en te reageren op de aanwijzingen met uw systeeminformatie.

```
* 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#
```

Nu de basis is ingesteld, voert u groepparameters in.

VPN-groepsconfiguratie

Wanneer u groepparameters invoert, bedenk dan dat de naam van de VPN-groep geen spaties moet bevatten, ook al staat de opdrachtregel parser u toe om spaties in de naam van de VPN-groep in te voeren. De naam van de VPN-groep kan letters, getallen, streepjes en onderscores bevatten.

Er zijn vier basisparameters die in elke VPN-groep voor IP-handeling vereist zijn:

- Maximum aantal verbindingen
- Start IP-adres of LocalIPet
- omzetten
- IPNet

De Max. connecties parameter is het maximale aantal gelijktijdige client sessies toegestaan in deze VPN Group configuratie. Houd dit aantal in gedachten, aangezien het in combinatie met de StartIPAAddress of LocalIPNet parameter werkt.

De VPN Concentrator wijst IP-adressen aan externe klanten toe door twee verschillende schema's, StartIPA-adres en LocalIPNet. StartIPA-adres wijst IP-nummers toe van het net dat is aangesloten op Ethernet 0 en proxy-arps voor de aangesloten klanten. LocalIPNet wijst IP-nummers toe aan externe klanten van een netwerk dat uniek is aan de VPN-clients en vereist dat de rest van het netwerk bewust wordt gemaakt van het bestaan van VPN-bit via statische of dynamische routing. StartIPA-adres biedt een makkelijke configuratie, maar kan de grootte van de adresruimte beperken. LocalIPNet biedt een grotere flexibiliteit van het richten voor verre gebruikers, maar vereist iets meer werk om de noodzakelijke routing te configureren.

Gebruik voor StartIPAAddress het eerste IP-adres dat is toegewezen aan een inkomende tunnelsessie. In een basisconfiguratie instelling moet dit een IP-adres op het interne TCP/IP-netwerk zijn (hetzelfde netwerk als de Ethernet 0-poort). In ons voorbeeld hieronder, wordt de eerste clientsessie toegewezen aan het adres 192.168.233.50, de volgende gelijktijdige clientsessie toegewezen aan 192.168.233.51, enzovoort. We hebben een maximale waarde van 30 toegewezen, wat betekent dat we een blok van 30 ongebruikte IP-adressen (inclusief DHCP-servers als u er een hebt) moeten hebben beginnend met 192.168.233.50 en eindigend met 192.168.233.79. Vermijd overlapping van de IP-adressen die in verschillende VPN-groepsconfiguraties worden gebruikt.

LocalIPNet wijst IP adressen aan verre klanten van een voorwerp toe die elders op LAN ongebruikt moeten zijn. Bijvoorbeeld, als u de parameter "LocalIPNet=182.168.1.0/24" in de VPN groepsconfiguratie specificeert, wijst de concentrator IP adressen aan klanten toe die met 192.168.1.1 beginnen. Daarom moet u "Maxconnecties=254" toewijzen, aangezien de concentrator geen subgrenzen zal hechten wanneer IP-nummers worden toegewezen met LocalIPNet.

Het sleutelwoord van het Omzetten specificeert de beveiligingstypen en algoritmen die de concentrator voor IKE clientsessies gebruikt. De opties zijn als volgt:

```
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) ]
```

Elke optie is een beschermingsstuk dat verificatie- en encryptieparameters specificeert. Dit sleutelwoord kan meerdere keren binnen deze sectie verschijnen, in welk geval de concentrator de gespecificeerde beschermingsstukken voorstelt in de volgorde waarin ze worden geparsed, totdat een door de cliënt voor gebruik tijdens de sessie wordt geaccepteerd. In de meeste gevallen is slechts één sleutelwoord van het Omzetten nodig.

ESP (SHA, DES), ESP (SHA, 3DES), ESP (MD5, DES) en ESP (MD5,3DES) geven de Encapsulating Security Payload (ESP)-header aan om pakketten te versleutelen en te authenticeren. DES (Data Encryption Standard) gebruikt een 56-bits toets om de gegevens te versleutelen. 3DES gebruikt drie verschillende toetsen en drie applicaties van het DES-algoritme om de gegevens te scrammelen. MD5 is het Messaging-digest 5 hash-algoritme en SHA is het Secure Hash Algorithm, dat wat veiliger wordt geacht dan MD5.

ESP (MD5,DES) is de standaardinstelling en wordt voor de meeste installaties aanbevolen. ESP (MD5) en ESP (SHA) gebruiken de ESP-header om pakketten zonder encryptie te authenticeren. AH (MD5) en AH(SHA) gebruiken de verificatieheader (AH) voor verificatie van pakketten. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES) en AH(SHA)+ESP(3DES) gebruiken de verificatieheader om pakketten te authenticeren en de ESP-header om pakketten te versleutelen.

Opmerking: De Mac OS Client-software ondersteunt de AH-optie niet. U dient minimaal één ESP-optie in te stellen als u de Mac OS-clientsoftware gebruikt.

Het IPNet-veld is belangrijk, omdat het de klanten van de concentrator controleert waar ze kunnen gaan. De waarden die u in dit veld invoert, bepalen wat TCP/IP-verkeer wordt getunneerd of, meer algemeen, wanneer een client die tot deze VPN-groep behoort, op uw netwerk kan gaan.

Cisco raadt aan het interne netwerk te configureren (in dit voorbeeld 192.168.233.0/24), zodat al het verkeer van een client naar het interne netwerk verzonden wordt door de tunnel en daarom geauthentiseerd en versleuteld (als u encryptie toestaat). In dit scenario wordt geen ander verkeer getunneld; in plaats daarvan wordt het normaal gerouteerd . U kunt meerdere items hebben, waaronder één- of host-adressen. Het formaat is het adres (in ons voorbeeld, het netwerkadres 192.168.233.0) en dan het masker verbonden met dat adres in bits (/24, dat een masker van Klasse C is).

Start dit deel van de configuratie door de opdracht **basisgebruiker** van **de VPN-groep** in te voeren en reageer vervolgens op de aanwijzingen met uw systeeminformatie. Hier is een voorbeeld van de hele configuratie sequentie:

```
*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#
```

De volgende stap is het definiëren van de database van de gebruiker.

VPN-gebruikersconfiguratie

In deze sectie van de configuratie, definieert u de VPN-gebruikersdatabase. Elke regel definieert

een VPN-gebruiker in combinatie met de VPN-groepsconfiguratie en het wachtwoord van de gebruiker. Toevoegingen van meerdere regels moeten lijneinden hebben die met een backslash eindigen. Regeleinden die zijn omgeven door een dubbele aanhalingstekens, blijven echter behouden.

Wanneer een VPN-client een tunnelsessie begint, wordt de gebruikersnaam van de client naar het apparaat verzonden. Als het apparaat de gebruiker in deze sectie vindt, gebruikt het de informatie in de ingang om de tunnel in te stellen. (U kunt ook een RADIUS-server gebruiken voor verificatie van VPN-gebruikers). Als het apparaat de gebruikersnaam niet vindt en u geen RADIUS-server hebt ingesteld om de verificatie uit te voeren, wordt de tunnelsessie niet geopend en wordt een fout teruggegeven aan de client.

Start de configuratie door de opdracht **VPN-gebruikers** te **bewerken**. Laten we naar een voorbeeld kijken dat een gebruiker met de naam "User1" aan de VPN-groep toevoegt.

```
*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 van deze gebruiker is "Burnt". Al deze configuratiewaarden zijn hoofdlettergevoelig; als u "User1" configureren moet de gebruiker "User1" in de clientsoftware invoeren. Het invoeren van "user1" levert een ongeldig of onbevoegd gebruikersfoutbericht op. U kunt gebruikers blijven invoeren in plaats van de editor te verlaten, maar vergeet niet dat u een periode moet opgeven om de editor te verlaten. Wanneer u dit niet doet, kan dit leiden tot ongeldige items in de configuratie.

Voltooien

Je laatste stap is het opslaan van de configuratie. Op de vraag of u zeker bent dat u de configuratie wilt downloaden en het apparaat opnieuw wilt starten, typt u y en drukt u op de toets ENTER. Schakel de concentrator tijdens het opstarten niet uit. Nadat de concentrator is herstart, kunnen gebruikers verbinding maken met de concentrator VPN-clientsoftware.

U kunt de configuratie als volgt opslaan door de opdracht **op te slaan**:

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

Als u met de concentrator via telnet bent verbonden, wordt de bovenstaande uitvoer volledig weergegeven. Als u door een console wordt aangesloten, zult u uitvoer gelijkend op het volgende zien, slechts veel langer. Aan het eind van deze output keert de concentrator "Hallo console..."

terug. en vraagt om een wachtwoord. Zo weet je dat je klaar bent.

```
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....
```

Gerelateerde informatie

- Cisco VPN 5000 Series Concentrators end-of-sale aankondiging
- Ondersteuning van Cisco VPN 5000 Concentrator-pagina
- Cisco VPN 5000 clientondersteuningspagina
- Ondersteuning van IPsec
- Technische ondersteuning en documentatie – Cisco Systems