De Cisco VPN 5000 Concentrator configureren en IPSec Main-mode LAN-to-LAN VPN-connectiviteit implementeren

Inhoud

Inleiding

Dit document verklaart de eerste configuratie van Cisco VPN 5000 Concentrator en toont aan hoe u een verbinding kunt maken met het netwerk via IP en hoe u IPSec Main-Mode LAN-to-LAN VPN-connectiviteit kunt bieden.

U kunt de VPN Concentrator in twee configuraties installeren, afhankelijk van de plaats waar u de Concentrator met het netwerk verbindt in relatie tot een firewall. VPN 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 ook de VPN Concentrator achter de firewall op het beschermde LAN installeren 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 voorwaarden 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 apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de potentiële impact van om het even welke opdracht begrijpt alvorens het te gebruiken.

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 VPN Concentrator aan te sluiten en de eindsoftware te gebruiken om het IP adres op de Ethernet 0 poort te configureren. Na het configureren van het IP-adres op Ethernet 0 poort kunt u telnet gebruiken om verbinding te maken met VPN Concentrator om de configuratie te voltooien. U kunt ook een configuratiebestand in een geschikte teksteditor genereren en het naar de VPN-centrator sturen met behulp van 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 gereageerd, geeft u de opdracht ip **Ethernet 0** aan, waarmee u reageert op de aanwijzingen met uw systeeminformatie. De volgorde van de aanwijzingen moet er als het volgende voorbeeld 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 en 1 poort configureren

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

Voer de opdrachten **ip Ethernet 1 in** die reageren op aanwijzingen met uw systeeminformatie. De volgorde van de aanwijzingen moet er als het volgende voorbeeld 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 ]#
```

U moet nu de IPSec-gateway configureren.

De IPSec-gateway configureren

De IPec gateway controleert waar de VPN Concentrator al het IPSec-verkeer of het tunnelverkeer verstuurt. Dit is onafhankelijk van de standaardroute die u later vormt. Start door de opdracht **Configuration General in te** voeren, die reageert op aanwijzingen met uw systeeminformatie. De volgorde van de aanwijzingen moet eruit zien zoals hieronder wordt getoond.

```
* 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#
```

Opmerking: In releases 6.x en later is de **ipsecgateway-**opdracht gewijzigd in de **VPN-gateway-**opdracht.

Laten we nu het Internet Key Exchange (IKE)-beleid configureren.

Het IKE-beleid configureren

De ISAKMP/IKE-parameters van Internet Security Association Key Management Protocol (ISAKMP) controleren hoe de VPN Concentrator en de client elkaar identificeren en authenticeren om tunnelsessies op te zetten. Deze initiële onderhandeling wordt fase 1 genoemd. Fase 1 parameters zijn mondiaal aan 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 VPN client afzonderlijke tunnelsessies behandelen. Fase 2 IKE-onderhandelingsparameters voor de VPN-Concentrator en de VPN-client worden ingesteld in het apparaat [VPN Group <Name>].

De syntaxis voor IKE-beleid 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 VPN Concentrator en de client van VPN. Dit sleutelwoord kan meerdere keren binnen deze sectie verschijnen, in welk geval de VPN Concentrator alle gespecificeerde veiligheidspakken voorstelt. De VPN-client accepteert een van de opties voor de onderhandeling. Het eerste deel van elke optie, MD5 (Message Digest 5), is het authenticatiemechanisme dat 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. Hieronder wordt een voorbeeld gegeven.

```
* 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 u de basislijnen hebt ingesteld, is het tijd om de tunnels en IP communicatieparameters te definiëren.

Main-mode site-to-site configuratie

Om de VPN-Concentrator te configureren ter ondersteuning van LAN-to-LAN verbindingen, moet u de tunnelconfiguratie definiëren, evenals de IP-communicatieparameters die in de tunnel worden gebruikt. U doet dit in twee delen, de sectie [Tunnel partner VPN x] en de sectie [IP VPN x]. Voor elke configuratie van de site-to-site moet de *x* die in deze twee secties is gedefinieerd overeenkomen, zodat de tunnelconfiguratie correct gekoppeld is aan de protocolconfiguratie.

Laten we elk van deze delen in detail bekijken.

De tunnelpartner configureren

In de tunnelpartner sectie moet je minstens de volgende acht parameters definiëren.

- omzetten
- Partnerpartner
- Sleutel beheren
- GedeeldKey
- Modus
- Lokale toegang
- Peer
- BindTo

omzetten

Het sleutelwoord van het Omzetten specificeert de beveiligingstypen en algoritmen die voor IKE clientsessies worden gebruikt. Elke optie die met deze parameter is verbonden is een beschermingsstuk dat authenticatie- en encryptieparameters specificeert. De parameter Omzetten kan meerdere malen binnen deze sectie verschijnen, in welk geval de VPN-Concentrator de gespecificeerde beschermingsstukken voorstelt in de volgorde waarin ze worden geparseerd, totdat een door de client is geaccepteerd voor gebruik tijdens de sessie. In de meeste gevallen is slechts één sleutelwoord van het Omzetten nodig.

De opties voor het sleutelwoord van het transformeren zijn als volgt.

```
[ 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 staat voor het insluiten van Security Payload en AH staat voor verificatieheader. Beide kopregels worden gebruikt om pakketten te versleutelen en te authentiseren. 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 bericht-digest 5 hash-algoritme. SHA is het Secure Hash Algorithm, dat als iets veiliger wordt beschouwd dan MD5.

ESP (MD5, DES) is de standaardinstelling en wordt voor de meeste instellingen aanbevolen. ESP (MD5) en ESP (SHA) gebruiken ESP om IP-pakketten (zonder encryptie) te authentiseren. AH (MD5) en AH (SHA) gebruiken AH om pakketten te echt te maken. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES) en AH(SHA)+ESP(3DES) gebruiken AH om pakketten te controleren en ESP te versleutelen.

Partnerpartner

Het sleutelwoord van de partner definieert het IP adres van de andere tunnelterminator in het tunnelpartnerschap. Dit nummer moet een openbaar, routabel IP-adres zijn waarmee de lokale VPN-centrator een IPSec-verbinding kan maken.

Sleutel beheren

Het sleutelwoord KeyManager definieert hoe de twee VPN Concentrators in een tunnelpartnerschap bepalen welk apparaat de tunnel initieert en welk type van tunnelvestiging te volgen procedure. De opties zijn automatisch, initiëren, reageren en handmatig. U kunt de eerste drie opties gebruiken om IKE-tunnels te configureren en het sleutelwoord Handmatig om tunnels met een vaste encryptie te configureren. Dit document beslaat niet hoe u tunnels met vaste encryptie moet configureren. Auto specificeert dat de tunnelpartner zowel verzoeken om tunnelinstellingen kan initiëren als beantwoorden. Initiate specificeert dat de tunnelpartner alleen verzoeken van tunnelinstellingen verstuurt, het reageert er niet op. Respond geeft aan dat tunnelpartner reageert op verzoeken om tunnelinstellingen, maar start ze nooit.

GedeeldKey

Het SharedKey sleutelwoord wordt gebruikt als het IKE gedeeld geheim. U moet dezelfde SharedKey waarde op beide tunnelpartners instellen.

Modus

Het sleutelwoord van de Modus definieert het IKE-onderhandelingsprotocol. De standaardinstelling is agressief, zodat om de VPN Concentrator voor interoperabiliteitsmodus in te stellen, moet u het sleutelwoord in de modus op hoofdpersoon instellen.

Lokale toegang

LocalAccess definieert IP-nummers die door de tunnel toegankelijk zijn, van een host-masker naar een standaardroute. Het trefwoord LocalProto definieert welke IP-protocolnummers toegankelijk zijn via de tunnel, zoals ICMP(1), TCP(6), UDP(17) enzovoort. Als u alle IP nummers wilt doorgeven, dient u LocalProto=0 in te stellen. LocalPort bepaalt welke poortnummers door de tunnel kunnen worden bereikt. Zowel LocalProto als LocalPort is standaard op 0 of all-access.

Peer

Het sleutelwoord van Peer specificeert welke subnetten door een tunnel worden gevonden. PeerProto specificeert welke protocollen zijn toegestaan door het afstandstunneleindpunt, en PeerPort-sets welke poortnummers toegankelijk zijn aan het andere uiteinde van de tunnel.

BindTo

BindTo specificeert welke Ethernet poort site-to-site verbindingen beëindigt. U dient deze parameter altijd op Ethernet 1 in te stellen, behalve wanneer de VPN Concentrator in één poort-mode actief is.

De parameters configureren

Om deze parameters te configureren voert u de **configuratie Tunnel partner VPN 1** opdracht in, waarmee u reageert op aanwijzingen met uw systeeminformatie.

De volgorde van de aanwijzingen moet er als voorbeeld hieronder uitzien.

```
*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.
```

Nu is het tijd om de IP sectie te configureren.

De IP-sectie configureren

U kunt genummerde of ongenummerde verbindingen (zoals in IP configuratie op WAN

verbindingen) gebruiken in het IP configuratie gedeelte van elk tunnelpartnerschap. Hier gebruikten we ongenummerd.

De minimum configuratie voor een ongenummerde site-to-site verbinding vereist twee verklaringen: genummerd=vals en mode=routed. Start door de opdrachten **ip vpn 1 in te** voeren en reageer als volgt op de aanwijzingen van het systeem.

```
*[ 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
```

Nu is het tijd om een standaardroute in te stellen.

De standaardroute configureren (TCP/IP-routeswitch)

U dient een standaardroute te configureren die de VPN-centrator kan gebruiken om al het TCP/IP-verkeer te verzenden dat bestemd is voor netwerken anders dan het netwerk of de netwerken waarmee het direct verbonden is, of waarvoor het dynamische routes heeft. De standaardroute wijst terug naar alle netwerken die op de interne poort zijn gevonden. U hebt de Invoerpoort al ingesteld om IPSec-verkeer naar en van het internet te verzenden met behulp van de IPSec Gateway-parameter. 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 voorbeeld hieronder 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#
```

Voltooien

De 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 **ENTER**. Schakel de VPN-centrator tijdens het opstarten niet uit. Nadat de concentrator is herstart, kunnen gebruikers verbinding maken met de VPN-clientsoftware van de concentrator.

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 telnet op de VPN-centrator bent aangesloten, is de bovenstaande uitvoer volledig zichtbaar. 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 VPN 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