Cisco VPN 3000 Concentrator FAQ

Inhoud

[Inleiding](#)
[Algemeen](#)
[Software](#)
[Overige geavanceerde functies](#)
[Gerelateerde informatie](#)

Inleiding

Dit document beantwoordt dikwijls gestelde vragen (FAQ's) over Cisco VPN 3000 Series Concentrator.

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Algemeen

Q. Wat betekent de foutmelding "`Lost Service`"?

A. Als er geen verkeer gedurende een periode tussen de VPN-centrator en de VPN-client is verstuurd, wordt er een DPD-pakket (Dead Peer Detectie) verzonden van de VPN-concentrator naar de VPN-client om er zeker van te zijn dat de peer er nog is. Als er een aansluitingsprobleem is tussen de twee peers waarin de VPN-client niet reageert op de VPN-centrator, blijft de VPN-Concentrator DPD-pakketten over een tijdsperiode verzenden. Dit beëindigt de tunnel en genereert de fout als deze gedurende die tijd geen respons ontvangt. Raadpleeg Cisco bug-ID CSCdz4586 (ondersteuningscontract vereist).

De fout moet er zo uitzien:

```
SEV=4 AUTH/28 RPT=381 XXX.XXX.XXX.XX User [SomeUser] disconnected:
Duration: HH:MM:SS Bytes xmt: 19560 Bytes rcv: 17704 Reason:
Lost Service YYYY/MM/DD HH:MM:SS XXX.XXX.XXX.XXX
syslog notice
45549 MM/DD/YYYY HH:MM:SS SEV=4 IKE/123 RPT=XXX.XXX.XXX.XXX
Group [SomeDefault] User [SomeUser]
IKE lost contact with remote peer, deleting connection (keepalive type: DPD)
```

Oorzaak: De externe IKE-peer heeft niet gereageerd op keepalives binnen het verwachte venster van tijd, zodat de verbinding met de IKE-peer werd verwijderd. De boodschap omvat het gebruikte bewaarde mechanisme. Dit probleem kan alleen worden gereproduceerd als de publieke interface tijdens een actieve tunnelsessie is losgekoppeld. De klant moet hun netwerkconnectiviteit controleren aangezien deze gebeurtenissen worden gegenereerd om de grondoorzaak van hun potentiële probleem(en) van de netwerkconnectiviteit aan te wijzen.

Uitschakelen van IKE in stand-houden door naar **%System Root%\Program Files\Cisco Systems\VPN Client\Profiles** op de pc van de client die de kwestie ervaart en het **PCF-bestand** (indien van toepassing) voor de verbinding bewerken.

Verander 'ForceHoudAlife=0' (standaard) in '**ForceHoudAlife=1**'.

Als het probleem zich blijft voordoen, opent u een serviceaanvraag met Cisco Technical Support en specificeert u de logbestanden van de client "Log Viewer" en de VPN-centrator wanneer het probleem zich voordoet.

Q. Wat betekenen de foutmelding "`q_send`" die is gedetecteerd voor de EMQ1 wachtrij?

A. Deze foutmelding wordt weergegeven wanneer de buffer te veel debug-gebeurtenissen / informatie bevat. Het heeft geen enkel negatief effect anders dan mogelijk het verliezen van een paar berichten. Probeer de gebeurtenissen te beperken tot het minimumaantal dat nodig is om het bericht te voorkomen.

Q. Mijn verwijderde groep toont nog steeds in de VPN Concentrator-configuratie. Hoe verwijder ik dit?

A. Kopieer de configuratie naar een teksteditor (zoals Kladblok) en bewerk of verwijder handmatig de betreffende groepsinformatie die wordt aangegeven door **[ipadgroup pool #.0]**. Sla de configuratie op en uploaden deze naar de VPN-centrator. Hier wordt een voorbeeld getoond.

```
!--- Change to 14.1 or any other number that is not in use !--- any number other than 0).
[ipaddrgrouppool 14.0] rowstatus=1 rangename= startaddr=172.18.124.1 endaddr=172.18.124.2
```

Is het mogelijk meerdere primaire SDI-servers te hebben?

A. De VPN 3000 Concentrators kunnen slechts één knooppunt per keer downloaden. In SDI Versie pre-5.0 kunt u meerdere SDI-servers toevoegen, maar ze moeten allemaal hetzelfde knooppunt-geheime bestand delen (denk eraan als de primaire en reserveservers). In SDI versie 5.0 kunt u alleen de één primaire SDI-server invoeren (de reserveservers zijn opgenomen in het knooppunt-geheim bestand) en replica-servers.

Q. Ik krijg een "`SSL certificaat zal binnen 28 dagen verlopen`". Wat moet ik doen?

A. Het bericht geeft aan dat uw Secure Socket Layer (SSL)-certificaat over 28 dagen vervalt. Dit certificaat wordt gebruikt om via HTTPS naar het webbeheer te bladeren. U kunt het certificaat verlaten met de standaardinstellingen, of u kunt verschillende opties configureren voordat u het nieuwe certificaat genereert. Selecteer **Configuration > System > Management Protocols > SSL** om dit te doen. Selecteer **Beheer > certificaatbeheer** en klik op **Generate** om het certificaat te vernieuwen.

Als u zich zorgen maakt over beveiliging van uw VPN-Concentrator en u onbevoegde toegang wilt voorkomen, moet u HTTP en/of HTTPS op de openbare interface uitschakelen door te gaan naar **Configuration > Policy Management > Traffic Management > Filters**. Als u via HTTP of HTTPS naar uw VPN-centrator wilt gaan, kunt u op basis van bronadres toegang instellen via **Administratie > Toegangsrechten > Toegangscontrolelijst**. U kunt het Help-menu in de rechterbovenhoek van het venster gebruiken om meer informatie te krijgen.

Q. Hoe kan ik de gebruikersinformatie in de interne gebruikersdatabase bekijken? Het is niet zichtbaar wanneer ik in het configuratiebestand kijk.

A. Selecteer **Beheer > Toegangsrechten > Toegangsinstellingen**, kies **Encryptie van bestand=**geen, en bewaar de configuratie van gebruikers en wachtwoorden. U dient naar de specifieke gebruiker te kunnen zoeken.

Q. Hoeveel gebruikers kunnen de interne database opslaan?

A. Het aantal gebruikers is versie-afhankelijk en gespecificeerd in het gedeelte **Configuration > User Management** van de Gebruikersgids voor uw VPN-centrator 3000-release. In totaal zijn 100 gebruikers of groepen (de som van gebruikers en groepen moet 100 of minder bedragen) mogelijk in VPN 3000 releases 2.2 tot 2.5.2. In VPN 3000 releases 3.0 en later blijft het nummer voor de 3005- en 3015-concentrators 100. Voor de VPN-technologie. VPN 3030 en 3020 Concentrator is het nummer 500, voor VPN 3060 of 3080 Concentrators is het nummer 1000. Ook verbetert het gebruik van een externe authenticatieserver de schaalbaarheid en beheerbaarheid.

Wat is het verschil tussen de standaardgateway van de tunnel en de standaardgateway?

A. De VPN 3000 Concentrator gebruikt de tunnel standaardgateway om de getunnelde gebruikers binnen het privé netwerk te leiden (gewoonlijk de binnenrouter). De VPN Concentrator gebruikt de standaardgateway om pakketten naar het internet (meestal de externe router) te leiden.

Q. Als ik mijn VPN 3000 Concentrator achter een firewall of router plaats die toegangscontrolelijsten runt, welke poorten en protocollen moet ik doorgeven?

A. Deze grafiek maakt een lijst van poorten en protocollen.

Service	Protocolnummer	Bronpoort	Doelpoort
PPTP-beheerverbinding	6 (TCP)	1023	1723
PPTP-tunnelinsluiting	47 (GRE)	N.v.t.	N.v.t.
ISAKMP/IPSec-sleutelbeheer	17 (UDP)	500	500
IPsec-tunnelinsluiting	50 (ESP)	N.v.t.	N.v.t.
IPsec NAT-transparantie	17 (UDP)	10000 (standaard)	10000 (standaard)

Opmerking: De poort naar netwerkadresomzetting (NAT) (Transparency) is configureerbaar voor elke waarde in het bereik van 4001 tot en met 49151. In versies 3.5 of hoger kunt u IPsec over TCP configureren door naar **Configuration > System > Tunneling Protocols > IPSec > IPSec over TCP te** gaan. U kunt maximaal 10 komma-gescheiden TCP-poorten (1-6535) invoeren. Als deze optie is ingesteld, zorg er dan voor dat deze poorten zijn toegestaan in uw firewall of router die toegangscontrolelijsten uitvoert.

Vraag. Hoe kan ik de VPN Concentrator weer in de fabriek zetten?

A. Verwijder het "Configuration"-bestand van het bestandsbeheer en herstart het. Als dit bestand per ongeluk wordt verwijderd, wordt een reservekopie, "fig.bak" bewaard.

Kan ik TACACS+ gebruiken voor administratieve authenticatie? Wat moet ik in gedachten houden als ik het doe?

A. Ja, vanaf VPN 3000 Concentrator release 3.0 kunt u een TACACS+ gebruiken voor administratieve verificatie. Nadat u TACACS+ hebt ingesteld, controleert u of u de verificatie controleert voordat u uitlogt. Onjuiste configuratie van TACACS+ kan u uitsluiten. Dit vereist een console poortinlognaam om TACACS+ uit te schakelen en het probleem te corrigeren.

Wat doe ik als het administratieve wachtwoord wordt vergeten?

A. Sluit in versies 2.5.1 en hoger een pc aan op de console-poort van de VPN Concentrator met behulp van een rechte RS-232 seriekabel met de PC die is ingesteld voor:

- 9600 bits per seconde
- 8 gegevensbits
- geen pariteit
- 1 stopcontact
- controle van de hardwarestroom op
- VT100-emulatie

Herstart de VPN-centrator. Nadat de diagnostische controle is voltooid, verschijnt een lijn met drie punten (...) op de console. Druk op **CTRL-C** binnen drie seconden nadat deze punten verschijnen. De standaardinstellingen van een menu waarmee u de wachtwoorden van het systeem opnieuw kunt instellen.

V. Wat is het doel van de groepsnaam en het groepswachtwoord?

A. De groepsnaam en het groepswachtwoord worden gebruikt om een hash te maken die dan wordt gebruikt om een veiligheidsassociatie te maken.

V. Volgt de VPN Concentrator ARP namens verbonden gebruikers?

A. Ja.

Q. Waar plaats ik de VPN 3000 Concentrator in mijn netwerkfirewall?

A. De VPN 3000 Concentrator kan voor, achter, parallel met of in de gedemilitariseerde zone (DMZ) van een firewall worden geplaatst. Het is niet raadzaam de openbare en privé interfaces in hetzelfde virtuele LAN (VLAN) te hebben.

Q. Is er een manier om proxy ARP uit te schakelen op Cisco VPN 3000 Concentrator?

A. Proxy-protocol voor adresoplossing (ARP) kan niet worden uitgeschakeld aan de Cisco VPN-Concentrator 3000.

Q. Waar kan ik insecten tegen de VPN 3000 Concentrator vinden?

A. Gebruikers kunnen de bugs zoekfunctie (ondersteuningscontract vereist) gebruiken om

gedetailleerde informatie over bugs te vinden.

Q. Waar kan ik configuratievoorbeelden voor de VPN 3000 Concentrator vinden?

A. Naast de documentatie van VPN 3000 Concentrator, kunnen er meer configuratievoorbeelden worden gevonden in de ondersteuningspagina van Cisco VPN 3000 Series Concentrator.

Vraag. Hoe kan ik de houtkap vergroten om betere sites te krijgen voor specifieke gebeurtenissen?

A. U kunt naar **Configuration > System > Events > Classes** gaan en de specifieke gebeurtenissen (zoals IPsec of PPTP) configureren om een beter profiel te krijgen. Debugging moet alleen worden ingeschakeld voor de duur van de procedure voor het opsporen en verhelpen van problemen, omdat deze procedure een verslechtering van de prestaties kan veroorzaken. Schakel voor IPsec debug IKE, IKEDBG, IPSEC, IPSECDBG, AUTH en AUTHDBG in. Als u certificaten gebruikt, voegt u de CERT-klasse toe aan de lijst.

V. Hoe kan ik het verkeer naar de VPN 3000 Concentrator bewaken?

A. De HTML-interface die bij de VPN 3000 Concentrator wordt geleverd, maakt het mogelijk om elementaire bewakingsfuncties te gebruiken als u **Monitoring > Sessies** bekijkt. De VPN 3000 Concentrator kan ook worden gemonitord via Simple Network Management Protocol (SNMP) met een SNMP-beheerder naar keuze. U kunt ook Cisco VPN/Security Management Solutions (VMS) aanschaffen. Cisco VMS biedt belangrijke functionaliteit om u te helpen als u de VPN 3000 Concentrator Series implementeert en diepgaande controle van externe toegang en site-to-site VPNs vereist, gebaseerd op IPsec, L2TP en PPTP. Raadpleeg de VPN Security Management Solutions voor meer informatie over VMS.

Q. Heeft Cisco VPN 3000 Concentrator Series een geïntegreerde firewall? Zo ja, welke functies worden ondersteund?

A. Terwijl de serie stateless poort/filtreermogelijkheden en NAT heeft geïntegreerd, stelt Cisco u voor om een apparaat als de Cisco Secure PIX-firewall voor de firewall van het bedrijf te gebruiken.

Q. Welke routeopties en VPN-protocollen worden ondersteund door Cisco VPN 3000 Concentrator Series?

A. De serie steunt deze routeopties:

- Routing Information Protocol (RIP)
- RIP2
- Open kortste pad eerst (OSPF)
- statische routes
- Virtual Router Redundancy Protocol (VRRP)

Ondersteunde VPN-protocollen omvatten Point-to-Point Tunneling Protocol (PPTP), L2TP, L2TP/IPsec en IPsec met of zonder NAT-apparaat tussen VPN 3000 en de eindclient. IPsec door NAT is bekend als NAT Transparency.

Q. Welke verificatiemechanismen / systemen ondersteunt Cisco VPN 3000 Concentrator Series voor client-pc's?

A. NT Domain, RADIUS of RADIUS-proxy, RSA Security Security SECurID (SDI), Digitale Certificaten en interne authenticatie worden ondersteund.

Q. Kan ik statische Netwerkadresomzetting (NAT) doen voor gebruikers die door de VPN-Concentrator 3000 gaan?

A. U kunt alleen Port Address Translation (PAT) voor alle gebruikers die uitgaan. U kunt geen statische NAT uitvoeren op de VPN 3000-centrator.

Q. Hoe kan ik een statisch IP-adres toewijzen aan een specifiek Point-to-Point Tunneling Protocol (PPTP) of IPsec-gebruiker via de VPN 3000 Concentrator?

A. Deze lijst legt uit hoe u statische IP-adressen toe kunt wijzen:

- **PPTP-gebruikers**Controleer in het gedeelte IP-adresbeheer de optie **Clientadres** gebruiken in combinatie met de opties voor de configuratie van uw pool of Dynamic Host Configuration Protocol (DHCP). Bepaal vervolgens de gebruiker en het IP-adres in de VPN 3000 Concentrator. Deze gebruiker krijgt altijd het IP-adres dat in de VPN-centrator is ingesteld bij het aansluiten.
- **Gebruikers van IPsec**In het gedeelte IP-adresbeheer kunt u, naast de opties op uw pool of DHCP, het **gebruikersadres** controleren **vanaf de** optie **Verificatieserver**. Bepaal vervolgens de gebruiker en het IP-adres in de VPN 3000 Concentrator. Deze gebruiker krijgt altijd het IP-adres dat in de VPN-centrator is ingesteld bij het aansluiten. Alle anderen die tot dezelfde groep of andere groepen behoren, krijgen een IP-adres uit de wereldwijde pool of DHCP.Met de Cisco VPN 3000 Concentrator-softwareversie 3.0 en hoger hebt u de optie om een adrespool op groepsbasis te configureren. Deze optie kan u helpen om ook een statisch IP-adres aan een specifieke gebruiker toe te wijzen. Als u een pool voor een groep vormt, krijgt de gebruiker met statische IP het IP-adres dat aan hen is toegewezen en krijgen andere leden van dezelfde groep IP-adressen van de groep. Dit is alleen van toepassing wanneer u de VPN-Concentrator als verificatieserver gebruikt.

Opmerking: Als u een externe authenticatieserver gebruikt, moet u de externe server gebruiken om de adressen correct toe te wijzen.

Q. Wat zijn een aantal bekende compatibiliteitsproblemen met de PPTP-producten van Microsoft en de VPN 3000-centrator?

A. Deze informatie is gebaseerd op VPN 3000 Series Concentrator-softwarerelease 3.5 en hoger; VPN 3000 Series concentrators, modellen 3005, 3015, 3020, 3030, 3060, 3080; en Microsoft besturingssystemen Windows 95 en hoger.

- **Windows 95 Inbelnetwerken (DUN) 1.2**Microsoft Point-to-Point Encryption (MPPE) wordt niet ondersteund onder DUN 1.2. Om verbinding te maken met MPPE, installeert u Windows 95 DUN 1.3. U kunt de Microsoft DUN 1.3-upgrade downloaden van de Microsoft website.
- **Windows NT 4.0**Windows NT wordt volledig ondersteund voor Point-to-Point Tunneling Protocol (PPTP)-verbindingen naar de VPN-centrator. Service Pack 3 (SP3) of hoger is

vereist. Als u SP3 draait, dient u de PPTP Performance and Security patches te installeren. Raadpleeg de Microsoft-website voor informatie over de Microsoft PPTP-prestaties en beveiligingsupgrade voor WinNT 4.0 .Merk op dat de 128-bits Service Pack 5 de MPPE-toetsen niet correct hanteert en PPTP kan er niet in slagen gegevens door te geven. Wanneer dit voorkomt, toont het eventlogbestand dit bericht:

```
103 12/09/1999 09:08:01.550 SEV=6 PPP/4 RPT=3 80.50.0.4
User [ testuser ]
disconnected. Experiencing excessive packet decrypt failure.
```

Download de upgrade om dit probleem op te lossen Hoe u het nieuwste Windows NT Service Pack 6a en Windows NT 4.0 Service Pack 6a beschikbaar kunt verkrijgen. Raadpleeg de Microsoft artikel MPPE-toetsen niet correct verwerkt voor een 128-bits MS-CHAP-verzoek voor meer informatie.

Q. Wat is het maximum aantal filters dat op een VPN 3000 Concentrator is toegestaan?

A. Het maximale aantal filters dat u op een VPN 30xx-eenheid kunt toevoegen (zelfs een 3030 of 3060) is ingesteld op 100. Gebruikers kunnen aanvullende informatie over dit probleem vinden door Cisco bug-ID CSCdw8658 (Ondersteuningscontract vereist) te bekijken.

Q. Wat is het maximum aantal routes in de 30xx lijn van VPN Concentrators?

A. Het maximale aantal routes is:

- De VPN 3005 Concentrator had voorheen maximaal 200 routes. Dit aantal is nu gestegen tot 350 routes. Raadpleeg Cisco bug-ID CSCeb3579 (ondersteuningscontract vereist) voor meer informatie.
- De VPN 3030 Concentrator is getest op maximaal 10.000 routes.
- De routeringstabellimiet op VPN 3030, 3060 en 3080 Concentrators is evenredig met de beschikbare bronnen/geheugen in elk apparaat.
- De VPN 3015-Concentrator heeft geen vooraf bepaalde maximumgrens. Dit geldt voor Routing Information Protocol (RIP) en Open Shortest Path First (OSPF)-protocol.
- VPN 3020 Concentrator - vanwege een Microsoft limitering zijn Windows XP-pc's niet in staat om een groot aantal klasloze statische routers (CSR) te ontvangen. De VPN 3000 Concentrator beperkt het aantal CSR's dat in een DHCP-berichtreactie wordt ingevoegd wanneer deze is geconfigureerd. De VPN 3000 Concentrator beperkt het aantal routes tot 28-42, afhankelijk van de klasse.

V. Hoe kan ik de interfacestatistieken op de VPN 3000 Concentrator volledig wissen?

A. Selecteer **Monitoring > Statistieken > MIB-II > Ethernet** en stel de statistieken opnieuw in om de statistieken voor de huidige sessie te wissen. Onthoud dat dit de statistieken niet helemaal duidelijk maakt. U moet opnieuw opstarten om de statistieken daadwerkelijk te herstellen (in plaats van de instelling voor bewakingsdoeleinden).

Q. Welke poorten moet ik op VPN Concentrator voor Network Time Protocol (NTP) toestaan?

A. Sta TCP- en UDP-poort 123 toe.

Q. Wat zijn de functies van UDP-poorten 625xx?

A. De poorten worden gebruikt voor de VPN-clientcommunicatie tussen de eigenlijke shim/deterministische NDIS extender (DNE) en de TCP/IP-stack van de PC, en zijn alleen bedoeld voor intern ontwikkelingsgebruik. Port 62515 wordt bijvoorbeeld door de VPN-client gebruikt voor het verzenden van informatie naar het VPN-clientlogbestand. Andere poortfuncties worden hier weergegeven.

- 62514 - Cisco Systems, Inc. VPN-service voor Cisco Systems IPsec-stuurprogramma
- 62515 - Cisco Systems IPsec-stuurprogramma voor Cisco Systems, Inc. VPN-service
- 62516 - Cisco Systems, Inc. VPN-service naar XAUTH
- 62517 - XAUTH to Cisco Systems, Inc. VPN-service
- 62518 - Cisco Systems, Inc. VPN-service met CLI
- 62519 - CLI naar Cisco Systems, Inc VPN-service
- 62520 - Cisco Systems, Inc. VPN-service naar UI
- 62521 - UI naar Cisco Systems, Inc. VPN-service
- 6252 - Log berichten
- 6252 - Connection Manager naar Cisco Systems, Inc. VPN-service
- 62524 - Pool voor Cisco Systems, Inc. VPN-service

Kan ik de WebVPN-zwevende balk verwijderen?

A. U kunt de drijvende werkbalk niet verwijderen en evenmin de drijvende werkbalk laden terwijl u de WebVPN-sessie hebt ingesteld. Wanneer u dit venster sluit, wordt de sessie onmiddellijk beëindigd en wanneer u opnieuw probeert in te loggen, wordt het venster opnieuw geladen. Dit is de manier waarop de WebVPN sessies oorspronkelijk ontworpen werden. U kunt het hoofdvenster sluiten maar het is niet mogelijk het drijvende venster te sluiten.

Software

Q. steunt WebVPN Outlook Web Access (OWA) 2003?

A. Ondersteuning van OWA 2003 voor WebVPN op de VPN 3000 Concentrator is nu beschikbaar bij downloads van versie 4.1.7 (ondersteuningscontract vereist).

Q. Waar kan ik de nieuwste softwareherzieningen voor de VPN 3000 Concentrator krijgen?

A. Alle Cisco VPN 3000 Concentrators verzenden met de meest recente code, maar gebruikers kunnen de downloads controleren (ondersteuningscontract vereist) om te zien of er meer huidige software beschikbaar is.

Raadpleeg de documentpagina van Cisco VPN 3000 Series Concentrator voor de laatste documentatie op de VPN 3000 Concentrator.

Q. heb ik een TFTP server nodig om de VPN 3000 Concentrator te verbeteren? Is

er een andere manier om het vak te verbeteren?

A. Naast het gebruik van TFTP kunt u de VPN-centrator upgraden door de laatste software op uw vaste schijf te downloaden. Vervolgens gaat u, vanaf een browser van het systeem waar de software zich bevindt, naar **Administration > Software Update** en zoekt u de gedownload software op uw harde schijf (net zoals het openen van een bestand). Selecteer in het tabblad **Upload**.

Wat betekent "k9" in de laatste codenamen (zoals in "vpn3000-3.0.4.Rel-k9.bin")?

A. De "k9"-benaming voor de beeldnaam heeft de oorspronkelijk gebruikte 3DES-benaming vervangen (bijvoorbeeld vpn3000-2.5.2.F-3des.bin). Aldus betekent "k9" nu dat dit een 3DES-afbeelding is.

Vraag. Moet ik de optie Gegevenscompressie onder de IPsec groep voor al mijn gebruikers gebruiken?

A. Gegevenscompressie verhoogt de geheugenvereisten en het CPU-gebruik voor elke gebruikerssessie en verlaagt bijgevolg de totale doorvoersnelheid van de VPN-centrator. Om deze reden, adviseert Cisco u om gegevenscompressie slechts toe te staan als elk lid van de groep een verre gebruiker is die met een modem verbonden is. Als een lid van de groep via breedband verbinding maakt, schakelt u geen gegevenscompressie voor de groep in. In plaats daarvan verdeel de groep in twee groepen, één voor modemgebruikers en één voor breedbandgebruikers. Gegevenscompressie alleen inschakelen voor de groep modemgebruikers.

Overige geavanceerde functies

Q. Werkt het in evenwicht brengen van de lading met LAN-to-LAN verbindingen?

A. Taakverdeling is alleen effectief op externe sessies die worden geïnitieerd met de Cisco VPN-softwareclient (release 3.0 en hoger). Alle andere klanten (PPTP, L2TP) en LAN-to-LAN verbindingen kunnen met een VPN Concentrator verbinden op welke lading-balanceren is ingeschakeld, maar zij kunnen niet deelnemen aan de taakverdeling.

Q. Hoe decrypteer ik de wachtwoorden van het configuratiebestand?

A. Ga naar **Configuration > System > Management Protocols > XML** en dan naar **administratie | File management select XML formaat**. Gebruik dezelfde naam of een andere naam en open het bestand om de wachtwoorden te bekijken.

Q. Kan ik het Virtual Router Redundancy Protocol (VRRP) en het taakverdeling samen gebruiken?

A. U kunt geen load-balanceren met VRRP gebruiken. In een VRRP-configuratie blijft het reservestation leeg tenzij de actieve VPN-Concentrator faalt. In een belasting-uitbalanceerconfiguratie zijn er geen losse apparaten.

Q. Moet al het externe VPN-verkeer van de toegangsclient door een versleutelde tunnel naar de VPN-centrator bij de onderneming of de serviceprovider? Kan

bijvoorbeeld gewoon web toegang tot andere sites open gaan, rechtstreeks via de internetverbinding van de ISP?

A. Ja. Dit concept staat bekend als "split tunneling." Split-tunneling maakt beveiligde toegang tot bedrijfsmiddelen mogelijk via een versleutelde tunnel en maakt internettoegang rechtstreeks mogelijk via de bronnen van de ISP (dit heft het bedrijfsnetwerk uit het pad voor webtoegang). De Cisco VPN 3000 Concentrator Series aan zowel Cisco VPN-client als de VPN 3002 Hardware-client kan splitsingen ondersteunen. Voor extra veiligheid, wordt deze optie bestuurd door de beheerder van de VPN Concentrator en niet door de gebruiker.

V. Is het veilig om gesplitste tunneling te gebruiken?

A. Split-tunneling biedt u het gemak om door het internet te bladeren terwijl u via de VPN-tunnel bent verbonden. Maar het vormt wel een risico voor ons als de VPN-gebruiker die aangesloten is op het netwerk kwetsbaar is voor aanvallen. Het wordt aanbevolen dat de gebruikers in dat geval een persoonlijke firewall gebruiken. De release notities voor een bepaalde VPN-clientversie bespreken interoperabiliteit met persoonlijke firewalls.

Q. Hoe werkt het in evenwicht brengen van lading aan de Cisco VPN 3000 Concentrator?

A. De lading wordt berekend als een percentage afgeleid van de actieve verbindingen gedeeld door de maximum geconfigureerde verbindingen. De regisseur probeert altijd de minste lading te hebben omdat het met de extra (inherente) lading van het onderhouden van alle administratieve LAN-to-LAN sessies belast wordt, het berekenen van alle andere lading van de clusterlid, en het is verantwoordelijk voor alle client-omleidingen.

Voor een nieuw geconfigureerd functioneel cluster heeft de regisseur ongeveer 1% lading voordat er verbindingen zijn ingesteld. Daarom richt de regisseur verbindingen op de reserveconcentrator terug tot het percentage van lading op de back-up hoger is dan het percentage van lading op de regisseur. Gegeven twee VPN 3030 Concentrators in onbelaste staten heeft de regisseur bijvoorbeeld een lading van 1 procent. Het secundaire systeem krijgt 30 verbindingen (2 procent lading) voordat de regisseur verbindingen accepteert.

Om te controleren of de regisseur verbindingen accepteert, gaat u naar **Configuration > System > General > Sessions** en verlaagt u het maximale aantal verbindingen naar een kunstmatig laag aantal om snel de lading op de back-up VPN Concentrator te verhogen.

Q. Hoeveel head-end apparaten kunnen de VPN monitor volgen?

A. De VPN Monitor kan 20 head-end apparaten volgen. In een scenario dat helemaal op de voorgrond staat, worden de verbindingen van afgelegen sites in het oog gehouden. Er is geen behoefte om alle verre plaatsen en gebruikers te controleren aangezien die informatie op de hub router kan worden getraceerd. Deze head-end apparaten kunnen tot 20.000 externe gebruikers of 2.500 afgelegen sites ondersteunen. Een apparaat van dubbel-gehomed VPN dat naar de gesproken plaatsen uitgaat telt als twee van de 20 maximum apparaten die kunnen worden gecontroleerd.

Gerelateerde informatie

- Ondersteuning van Cisco VPN 3000 Concentrator-pagina
- Cisco VPN 3000 clientondersteuningspagina
- Technische ondersteuning en documentatie – Cisco Systems