Cisco VPN-clientgebruiker en -groepskenmerk Verwerking op de VPN 3000-centrator

Inhoud

Inleiding

Dit document beschrijft hoe Cisco VPN-clients zijn geauthentiseerd op de VPN-centrator en hoe Cisco VPN 3000 Concentrator gebruikers en groepskenmerken gebruikt.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco VPN 3000 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.

VPN-client verbindingen met een VPN 3000 Concentrator

Wanneer een VPN-client is verbonden met een VPN 3000 Concentrator, kunnen maximaal vier authenticaties plaatsvinden.

1. De groep is authentiek. (Deze wordt vaak de "Tunnel Group" genoemd.)
2. De gebruiker is authentiek.
3. (Optioneel) Als de gebruiker deel uitmaakt van een andere groep, is deze groep als volgende geauthentiseerd. Als de gebruiker niet tot een andere groep of de Tunnel Groep behoort, dan blijft de gebruiker standaard naar de Base Group en gebeurt deze stap NIET.
4. De "Tunnel Groep" van Stap 1 is opnieuw echt gemaakt. (Dit gebeurt wanneer de optie "Groepsslot" wordt gebruikt. Deze optie is beschikbaar in versie 2.1 of hoger.)

Dit is een voorbeeld van de gebeurtenissen die u in het logbestand van de gebeurtenis ziet voor een VPN-client die via de interne database is geauthentiseerd ("testgebruiker" maakt deel uit van de groep "Engineering").

```
1 12/09/1999 11:03:46.470 SEV=6 AUTH/4 RPT=6491 80.50.0.4
Authentication successful: handle = 642, server = Internal, user = Tunnel_Group
2 12/09/1999 11:03:52.100 SEV=6 AUTH/4 RPT=6492 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = testuser
3 12/09/1999 11:03:52.200 SEV=6 AUTH/4 RPT=6493 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = Engineering
4 12/09/1999 11:03:52.310 SEV=6 AUTH/4 RPT=6494 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = Tunnel_Group
```

Opmerking: Om deze gebeurtenissen te zien, moet u de klasse Auth Event Class met ernst 1-6 in **Configuration > System > Events > Classes** configureren.

Functie voor groepsvergrendeling - Als de optie Groepsslot is ingeschakeld op de Group - Tunnel_Group, dan moet de gebruiker onderdeel zijn van Tunnel_Group voor verbinding. In het vorige voorbeeld, zie je alle zelfde gebeurtenissen maar "testuser" maakt geen verbinding omdat ze deel uitmaken van de Groep - Engineering en geen deel uitmaken van de Groep - Tunnel_Group. U ziet ook deze gebeurtenis:

```
5 12/09/1999 11:35:08.760 SEV=4 IKE/60 RPT=1 80.50.0.4
User [ testuser ]
User (testuser) not member of group (Tunnel_Group), authentication failed.
```

Raadpleeg voor meer informatie over de optie Groepsslot en een voorbeeldconfiguratie de gebruikers insluiten in een VPN 3000 Concentrator-groep die een RADIUS-server gebruikt.

Authenticeer groepen en gebruikers extern via RADIUS

De VPN 3000 Concentrator kan ook worden geconfigureerd om gebruikers en groepen extern door een RADIUS-server te authentiseren. Dit vereist nog steeds dat de namen van de groepen op de VPN Concentrator worden geconfigureerd, maar het groepstype is ingesteld als "Extern".

- Externe groepen kunnen de eigenschappen Cisco/Altiga teruggeven als de RADIUS-server leverancierspecifieke kenmerken (VSA's) ondersteunt.
- Alle eigenschappen van Cisco/Altiga die NIET door RADIUS worden teruggegeven aan de waarden in de Base Group.
- Als de RADIUS-server GEEN VSA's ondersteunt, worden alle eigenschappen standaard toegewezen aan de Base Group-eigenschappen.

Opmerking: Een RADIUS-server behandelt groepsnamen niet anders dan gebruikersnamen. Een

groep op een RADIUS-server is net zo ingesteld als een standaardgebruiker.

Deze stappen schetsen wat er gebeurt wanneer een IPSec-client wordt aangesloten op VPN 3000 Concentrator als zowel gebruikers als groepen extern voor authentiek zijn verklaard. Overeenkomstig het interne geval kunnen maximaal vier authenticaties plaatsvinden.

1. De groep is via RADIUS authentiek. De RADIUS-server kan veel eigenschappen voor de groep teruggeven of helemaal geen. De RADIUS-server moet minimaal de Cisco/Altiga-eigenschap "IPSec-verificatie = RADIUS" retourneren om de VPN-centrator te vertellen hoe de gebruiker echt kan worden gemaakt. Als dit niet het geval is, moet de IPSec-verificatiemethode van de Base Group op "RADIUS" worden ingesteld.
2. De gebruiker is via RADIUS authentiek. De RADIUS-server kan veel eigenschappen voor de gebruiker of helemaal geen eigenschappen teruggeven. Als de RADIUS-server de eigenschap CLASS (standaard RADIUS-kenmerk #25) retourneert, gebruikt de VPN 3000 Concentrator die de eigenschap toeschrijft als een groepsnaam en naar Stap 3 verplaatst, of anders gaat het naar Stap 4.
3. De gebruikersgroep is nadien geauthentificeerd via RADIUS. De RADIUS-server kan veel eigenschappen voor de groep teruggeven of helemaal geen.
4. De "Tunnel Group" uit Stap 1 is opnieuw geauthentiseerd via RADIUS. Het subsysteem voor echtheidscontrole moet de tunnelgroep opnieuw authentificeren omdat het de eigenschappen (indien van toepassing) van de authenticatie in stap 1 niet heeft opgeslagen. Dit gebeurt voor het geval de functie "Groepsslot" wordt gebruikt.

Hoe de VPN 3000 Concentrator gebruiker- en groepskenmerken gebruikt

Nadat de VPN 3000 Concentrator de gebruiker en de groep(en) voor authentiek heeft verklaard, moet hij de eigenschappen organiseren die hij heeft ontvangen. De VPN Concentrator gebruikt de eigenschappen in deze volgorde van voorkeur. Het doet er niet toe of de authenticatie intern of extern werd uitgevoerd:

1. **Eigenschappen van gebruikers**—Deze hebben voorrang op alle anderen.
2. Eigenschappen **van de groep** - Alle eigenschappen die ontbreken van de eigenschappen van de Gebruiker worden ingevuld door de eigenschappen van de Groep. Alle eigenschappen die hetzelfde zijn, worden gecorrigeerd door de gebruikerseigenschappen.
3. **Eigenschappen van de Tunnelgroep** - Alle eigenschappen die ontbreken van de eigenschappen van de Gebruiker of de Groep worden ingevuld door de eigenschappen van de Tunnelgroep. Alle eigenschappen die hetzelfde zijn, worden gecorrigeerd door de gebruikerseigenschappen.
4. **Eigenschappen van de basisgroep** - Om het even welke eigenschappen die van de Gebruiker, de Groep, of de eigenschappen van de Tunnelgroep missen worden ingevuld door de eigenschappen van de Basisgroep.

Gerelateerde informatie

- Ondersteuning van Cisco VPN 3000 Series Concentrator-pagina
- Cisco VPN-clientondersteuningspagina

- IPsec-ondersteuningspagina
- RADIUS-ondersteuningspagina
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning - Cisco-systemen