Beleidsgroeptoewijzing voor AnyConnect-clients die LDAP gebruiken op Cisco IOS-headends Configuration-voorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u lichtgewicht Directory Access Protocol (LDAP)-kaarten kunt configureren om automatisch het juiste VPN-beleid aan een gebruiker toe te wijzen, op basis van hun referenties.

> **Opmerking:** Ondersteuning voor LDAP-verificatie voor Secure Socket Layer VPN-gebruikers (SSL VPN) die verbinding maken met een Cisco IOS® head-end wordt gevolgd door Cisco bug ID CSCuj20940. Totdat ondersteuning officieel wordt toegevoegd, is LDAP-ondersteuning de beste inspanning.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SSL VPN op Cisco IOS
- LDAP-verificatie op Cisco IOS
- Map-services

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CISCO 881-SEC-K9
- Cisco IOS-software, C880-software (C880/DATA-UNIVERSALK9-M), versie 15.1(4)M, RELEASE-SOFTWARE (FC1)

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.

Achtergrondinformatie

De LDAP is een open, leverancierneutraal, industrieel standaardtoepassingsprotocol om gedistribueerde telefoongids informatiediensten via een IP-netwerk (Internet Protocol) te kunnen gebruiken en onderhouden. Intranet en internettoepassingen spelen een belangrijke rol bij de ontwikkeling van intranet en internettoepassingen, aangezien zij het mogelijk maken informatie over gebruikers, systemen, netwerken, diensten en toepassingen in het gehele netwerk te delen.

Frequent willen de beheerders VPN-gebruikers andere toegangsrechten of WebVPN-inhoud geven. Dit kan worden voltooid met de configuratie van verschillende VPN-beleidsmaatregelen op de VPN-server en de toewijzing van deze beleidssets aan elke gebruiker, afhankelijk van hun aanmeldingsgegevens. Hoewel dit handmatig kan worden voltooid, is het efficiënter het proces te automatiseren met Directory Services. Om LDAP te gebruiken om een groepsbeleid aan een gebruiker toe te wijzen, moet u een map configureren die een LDAP-eigenschap zoals de AD-eigenschap (Active Directory) in kaart brengt aan een eigenschap die wordt begrepen door het VPN-head-end.

Op de adaptieve security applicatie (ASA) wordt dit regelmatig bereikt door de toewijzing van verschillende groepsbeleid aan verschillende gebruikers met een LBP-attributenkaart zoals getoond in ASA Use of LDAP Attribution Maps Configuratievoorbeeld.

Op Cisco IOS kan hetzelfde worden bereikt met de configuratie van verschillende beleidsgroepen onder de WebeVPN-context en het gebruik van LDAP-attributiekaarten om te bepalen welke beleidsgroep de gebruiker zal worden toegewezen. Op Cisco IOS head-ends, wordt de eigenschap "lid van" AD in kaart gebracht aan de veelzijdige groep van de eigenschap verificatie, autorisatie en accounting (AAA). Zie LDAP op IOS-apparaten met behulp van het Configuratievoorbeeld van Dynamische toeslagen voor meer informatie over de standaardkarakteristieken. Maar voor SSL VPN zijn er twee relevante AAA-afbeeldingen:

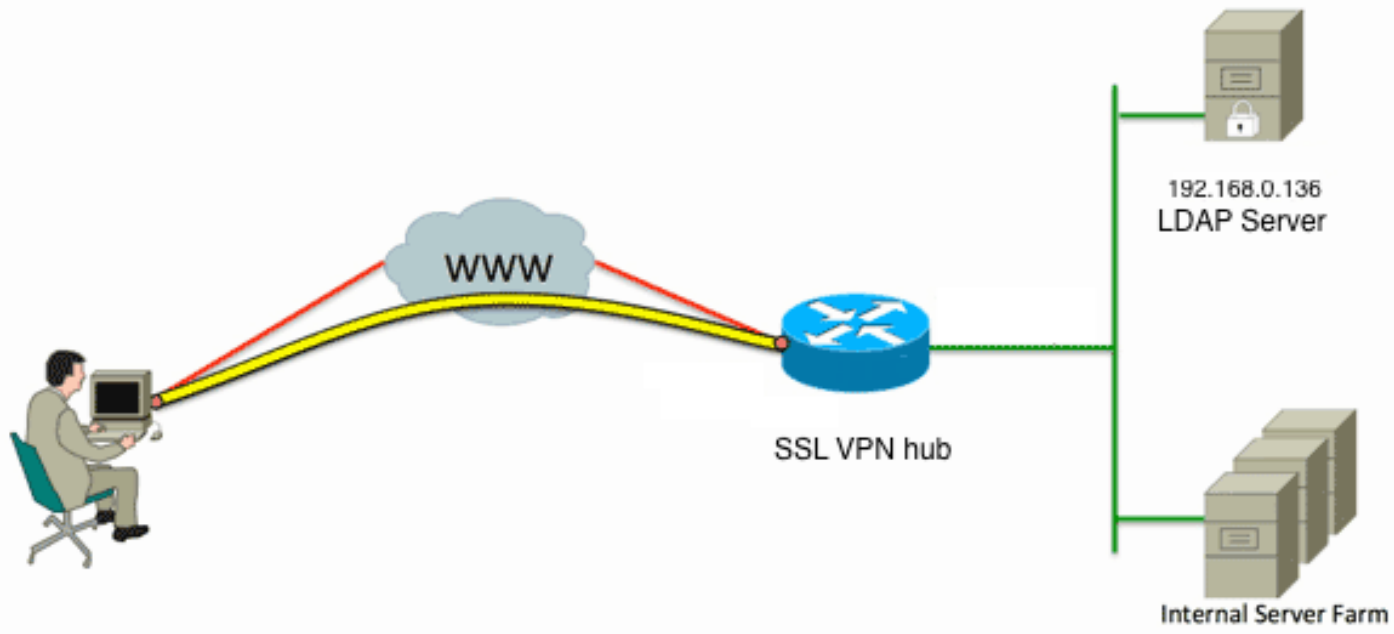
Naam van AAA-kenmerk	SSL VPN-relevantie
gebruikersgroep VPN	kaarten naar de beleidsgroep gedefinieerd in de WebeVPN-context
internetcontext	kaarten naar de eigenlijke WebVPN-context zelf

Daarom moet de LDAP-attributenkaart de desbetreffende LDAP-eigenschap aan een van deze twee AAA-eigenschappen in kaart brengen.

Configureren

Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram



Deze configuratie maakt gebruik van een LDAP-attributenkaart om de LDAP-eigenschap "lidOf" aan de AAA-gebruiker-vpn-groep in kaart te brengen.

1. Configureer de verificatiemethode en de AAA-servergroep.
```
aaa new-model
!
!
aaa group server ldap AD
 server DC1
!
aaa authentication login default local
aaa authentication login vpn local
aaa authentication login AD group ldap local
aaa authorization exec default local
```
2. Configuratie van een lidaf-attributenkaart.
```
ldap attribute-map ADMAP
 map type memberOf user-vpn-group
```
3. Configuratie van de LDAP server die verwijst naar de vorige LDAP attributenkaart.
```
ldap server DC1
 ipv4 192.168.0.136
 attribute map ADMAP
 bind authenticate root-dn CN=Cisco Systems,OU=Service Accounts,DC=chillsthrills,
DC=local password 7 <removed>
 base-dn DC=chillsthrills,DC=local
```
4. Configureer de router om als een WebVPN-server op te treden. In dit voorbeeld, omdat de eigenschap "lidOf" in kaart zal worden gebracht aan de eigenschap "user-VPN-group", wordt één enkele WebeVPN-context geconfigureerd met meerdere beleidsgroepen die een "NOACCESS"-beleid omvatten. Deze beleidsgroep is voor gebruikers die geen overeenkomende waarde "lidOf" hebben.
```
ip local pool vpnpool 192.168.200.200 192.168.200.250
!
```

```
webvpn gateway gateway_1
 hostname vpn
 ip address 173.11.196.220 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-2564112419
 logging enable
 inservice
 !
webvpn install svc flash:/webvpn/anyconnect-win-2.5.2019-k9.pkg sequence 1
 !
webvpn install csd flash:/webvpn/sdesktop.pkg
 !
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
  hide-url-bar
  timeout idle 60
  timeout session 1
 !
 !
 policy group CN=T,OU=MyBusiness,DC=chillsthrills,DC=local
  functions svc-enabled
  banner "special access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
   svc split include 192.168.0.0 255.255.255.0
   svc split include 10.10.10.0 255.255.255.0
   svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

Caveats

1. Als de gebruiker een "lidOf" meerdere groepen is, wordt de eerste "lidOf" waarde gebruikt door de router.
2. Wat vreemd is in deze configuratie is dat de naam van de beleidsgroep een exacte match moet zijn voor de **volledige** string die geduwd wordt door de LDAP server voor de "lidOf waarde". Gewoonlijk gebruiken beheerders kortere en relevantere namen voor de beleidsgroep, zoals VPNACCESS, maar afgezien van het cosmetische vraagstuk kan dit leiden tot een groter probleem. Het is niet ongewoon dat de string "lidOf" aanzienlijk groter is dan wat in dit voorbeeld gebruikt is. Denk bijvoorbeeld aan dit debug-bericht:
   ```
   004090: Aug 23 08:26:57.235 PCTime: %SSLVPN-6-INVALID_RADIUS_CONFIGURATION:
   Radius configured group policy "CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,
   DC=chillsthrills,DC=local" does not exist
   ```
   Dit toont duidelijk aan dat de string die van AD wordt ontvangen, is:
   ```
   "CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,DC=chillsthrills,DC=local"
   ```

Aangezien een dergelijk beleidsgroep echter niet is gedefinieerd, als de beheerder probeert om zo'n groepsbeleid te configureren, levert dit een fout op omdat Cisco IOS een limiet heeft op het aantal tekens in de naam van de beleidsgroep:

```
HOURTR1(config-webvpn-context)#webvpn context VPNACCESS
HOURTR1(config-webvpn-context)# policy group "CN=VPNACCESS,OU=Security Groups,
OU=MyBusiness,DC=chillsthrills,DC=local"
Error: group policy name cannot exceed 63 characters
```

In dergelijke situaties zijn er twee mogelijke oplossingen:

1. Gebruik een andere LDAP eigenschap, zoals "departement".Denk aan deze LDAP attributenkaart:

   ```
   ldap attribute-map ADMAP
    map type department user-vpn-group
   ```

   In dit geval kan de waarde van de eigenschap departement voor een gebruiker worden ingesteld op een waarde zoals VPN ACCESS en is de configuratie van WebVPN een beetje eenvoudiger:

   ```
   webvpn context VPNACCESS
    secondary-color white
    title-color #669999
    text-color black
    ssl authenticate verify all
    !
    policy group NOACCESS
     banner "Access denied per user group restrictions in Active Directory.
   Please contact your system administrator or manager to request access."
    !
    policy group VPNACCESS
     functions svc-enabled
     banner "access-granted"
     svc address-pool "vpnpool"
     svc default-domain "cisco.com"
     svc keep-client-installed
     svc rekey method new-tunnel
     svc split dns "cisco.com"
     svc split include 192.168.0.0 255.255.255.0
     svc split include 10.10.10.0 255.255.255.0
     svc split include 172.16.254.0 255.255.255.0
     svc dns-server primary 192.168.0.136
    default-group-policy NOACCESS
    aaa authentication list AD
    gateway gateway_1
    inservice
   !
   end
   ```

2. Gebruik het DN-to-string sleutelwoord in de LDAP attributenkaart.Als de vorige workround niet geschikt is dan kan de beheerder het dn-to-string sleutelwoord in de LDAP attribuut map gebruiken om alleen de Common Name (CN) waarde uit de "LidOf" string te halen. In dit scenario zou de LDAP-attributenkaart zijn:

   ```
   ldap attribute-map ADMAP
    map type memberOf user-vpn-group format dn-to-string
   ```

   En de configuratie van WebVPN zou zijn:

   ```
   webvpn context VPNACCESS
    secondary-color white
    title-color #669999
    text-color black
    ssl authenticate verify all
    !
    policy group NOACCESS
     banner "Access denied per user group restrictions in Active Directory.
   ```

```
Please contact your system administrator or manager to request access."
 !
 policy group VPNACCESS
  functions svc-enabled
  banner "access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
  svc split include 192.168.0.0 255.255.255.0
  svc split include 10.10.10.0 255.255.255.0
  svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

Opmerking: Anders dan in ASA's, waar u de opdracht **plattewaarde** kunt gebruiken onder een attributenkaart om de waarde te koppelen van de LDAP server aan een andere lokaal significante waarde, hebben Cisco IOS head-ends deze optie niet en zijn daarom niet zo flexibel. Cisco bug-ID CSCts31840 is ingediend om dit aan te pakken.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met **show.** Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

- **ldap-eigenschappen tonen**
- **ldap server all tonen**

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Opmerking: Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**

Om de LDAP-attributenafbeelding te verhelpen, stelt u deze defecten in:

- **streep ldap**
- **debug ldap**
- **debug van verificatie**
- **debug AAA-autorisatie**