Richtliniengruppenzuweisung für AnyConnect-Clients, die LDAP auf Cisco IOS-Headends verwenden - Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie LDAP-Attributzuordnungen (Lightweight Directory Access Protocol) konfigurieren, um einem Benutzer anhand seiner Anmeldeinformationen automatisch die richtige VPN-Richtlinie zuzuweisen.

> **Hinweis**: Die Unterstützung der LDAP-Authentifizierung für SSL VPN-Benutzer (Secure Sockets Layer VPN), die eine Verbindung zu einem Cisco IOS® Headend herstellen, wird durch die Cisco Bug-ID CSCuj20940 nachverfolgt. Bis die Unterstützung offiziell hinzugefügt wird, ist die LDAP-Unterstützung der beste Schritt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- SSL VPN auf Cisco IOS
- LDAP-Authentifizierung auf Cisco IOS
- Verzeichnisdienste

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- CISCO881-SEC-K9
- Cisco IOS-Software, C880-Software (C880DATA-UNIVERSALK9-M), Version 15.1(4)M, RELEASE-SOFTWARE (fc1)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Das LDAP ist ein offenes, anbieterunabhängiges, dem Industriestandard entsprechendes Anwendungsprotokoll für den Zugriff auf verteilte Verzeichnisinformationsdienste über ein IP-Netzwerk. Verzeichnisdienste spielen eine wichtige Rolle bei der Entwicklung von Intranet- und Internetanwendungen, da sie den Austausch von Informationen über Benutzer, Systeme, Netzwerke, Dienste und Anwendungen im gesamten Netzwerk ermöglichen.

Häufig möchten Administratoren VPN-Benutzern unterschiedliche Zugriffsberechtigungen oder WebVPN-Inhalte bereitstellen. Dies kann durch die Konfiguration verschiedener VPN-Richtlinien auf dem VPN-Server und die Zuweisung dieser Richtlinien an jeden Benutzer, abhängig von dessen Anmeldeinformationen, ergänzt werden. Obwohl dies manuell durchgeführt werden kann, ist es effizienter, den Prozess mit Verzeichnisdiensten zu automatisieren. Damit LDAP einem Benutzer eine Gruppenrichtlinie zuweist, müssen Sie eine Zuordnung konfigurieren, die einem vom VPN-Headend verständlichen Attribut ein LDAP-Attribut wie das Active Directory (AD)-Attribut "memberOf" zuordnet.

Auf der Adaptive Security Appliance (ASA) wird dies regelmäßig durch die Zuweisung unterschiedlicher Gruppenrichtlinien für verschiedene Benutzer mit einer LDAP-Attributzuordnung erreicht, wie in ASA-Konfigurationsbeispiel zur Verwendung von LDAP-Attributzuordnungen gezeigt.

Auf dem Cisco IOS kann dasselbe mit der Konfiguration verschiedener Richtliniengruppen im WebVPN-Kontext und der Verwendung von LDAP-Attributzuordnungen erreicht werden, um festzulegen, welcher Richtliniengruppe der Benutzer zugewiesen wird. Bei Cisco IOS-Headends wird das "memberOf" AD-Attribut der Supplicant-Gruppe für das Authentication, Authorization, and Accounting (AAA)-Attribut zugeordnet. Weitere Informationen zu den standardmäßigen Attributzuordnungen finden Sie unter Konfigurationsbeispiel LDAP auf IOS-Geräten mit dynamischen Attributzuordnungen. Für SSL VPN gibt es jedoch zwei relevante AAA-Attributzuordnungen:

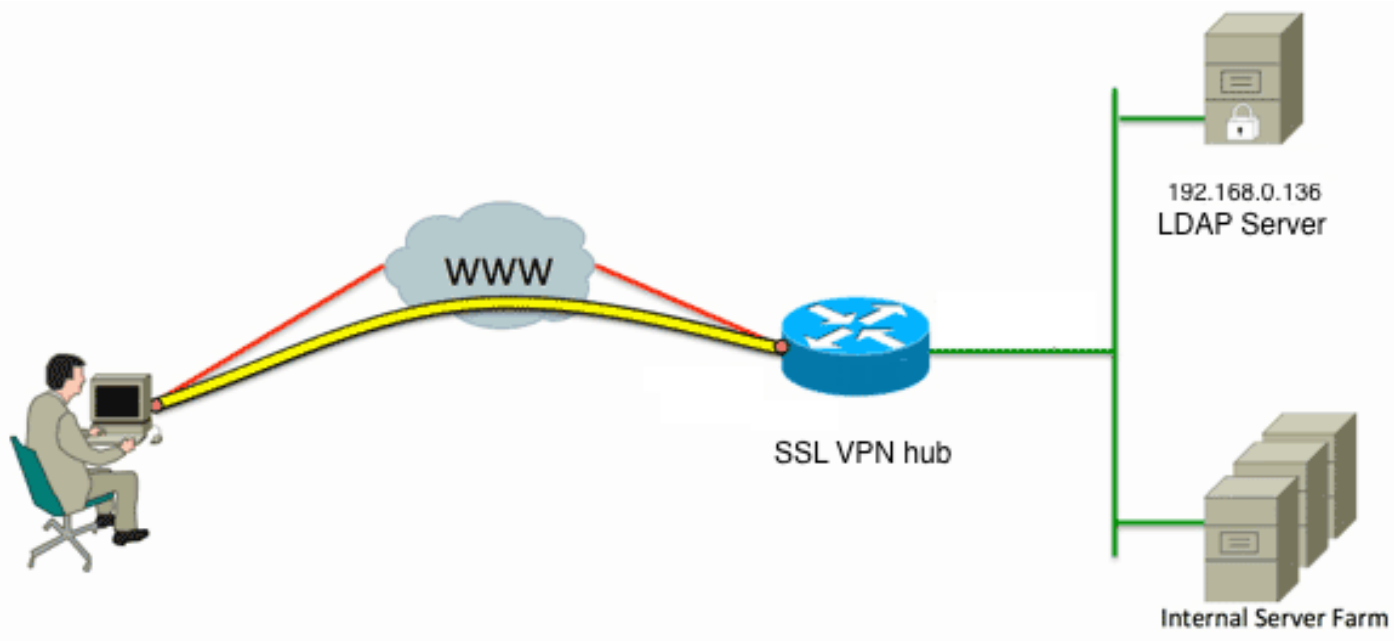
AAA-Attributname	SSL VPN-Relevanz
Benutzer-VPN-Gruppe	der im WebVPN-Kontext definierten Richtliniengruppe zugeordnet
webvpn-Kontext	wird dem tatsächlichen WebVPN-Kontext selbst zugeordnet

Daher muss die LDAP-Attributzuordnung das entsprechende LDAP-Attribut einem der beiden AAA-Attribute zuordnen.

Konfigurieren

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm



Diese Konfiguration verwendet eine LDAP-Attributzuordnung, um das "memberOf"-LDAP-Attribut der AAA-Attribut-user-vpn-group zuzuordnen.

1. Konfigurieren Sie die Authentifizierungsmethode und die AAA-Servergruppe.
```
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. Konfigurieren einer LDAP-Attributzuordnung
```
ldap attribute-map ADMAP
 map type memberOf user-vpn-group
```
3. Konfigurieren Sie den LDAP-Server, der auf die vorherige LDAP-Attributzuordnung verweist.
```
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. Konfigurieren Sie den Router so, dass er als WebVPN-Server fungiert. Da in diesem Beispiel das Attribut "memberOf" dem Attribut "user-vpn-group" zugeordnet wird, wird ein einzelner WebVPN-Kontext mit mehreren Richtliniengruppen konfiguriert, die eine Richtlinie für

"NOACCESS" enthalten. Diese Richtliniengruppe ist für Benutzer bestimmt, die keinen übereinstimmenden "memberOf"-Wert haben.

```
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
```

Einsprüche

1. Wenn der Benutzer ein "memberOf"-Objekt aus mehreren Gruppen ist, wird der erste "memberOf"-Wert vom Router verwendet.
2. In dieser Konfiguration ist es merkwürdig, dass der Name der Richtliniengruppe genau der **vollständigen** Zeichenfolge entsprechen muss, die vom LDAP-Server für den "memberOf value" übertragen wird. In der Regel verwenden Administratoren kürzere und relevantere Namen für die Richtliniengruppe, z. B. VPNACCESS, aber abgesehen von der kosmetischen Frage kann dies zu einem größeren Problem führen. Es ist nicht ungewöhnlich, dass die Attribut-Zeichenfolge "memberOf" deutlich größer ist als die, die in diesem Beispiel

verwendet wird. Betrachten Sie z. B. folgende Debugmeldung:

```
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
```

Es zeigt deutlich, dass die Zeichenfolge, die von AD empfangen wird, folgende ist:

```
"CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,DC=chillsthrills,DC=local"
```

Da jedoch keine solche Richtliniengruppe definiert ist, führt der Administrator beim Versuch, eine solche Gruppenrichtlinie zu konfigurieren, zu einem Fehler, da Cisco IOS die Anzahl der Zeichen im Richtliniengruppen-Namen beschränkt:

```
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 solchen Situationen gibt es zwei mögliche Problemumgehungen:

1. Verwenden Sie ein anderes LDAP-Attribut, z. B. "Department" (Abteilung).Betrachten Sie die folgende LDAP-Attributzuordnung:

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

   In diesem Fall kann der Wert des Abteilungsattributs für einen Benutzer auf einen Wert wie VPNACCESS gesetzt werden, und die WebVPN-Konfiguration ist etwas einfacher:

   ```
   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. Verwenden Sie das Schlüsselwort DN-zu-String in der LDAP-Attributzuordnung.Wenn die vorherige Problemumgehung nicht geeignet ist, kann der Administrator in der LDAP-Attributübersicht das Schlüsselwort dn-to-String verwenden, um nur den CN-Wert aus der Zeichenfolge "memberOf" zu extrahieren. In diesem Szenario wäre die LDAP-Attributzuordnung:

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

   Die WebVPN-Konfiguration sieht wie folgt aus:

   ```
   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
```

Hinweis: Anders als bei ASAs, bei denen der Befehl **map value** unter einer Attributzuordnung verwendet werden kann, um den vom LDAP-Server erhaltenen Wert einem anderen lokal relevanten Wert zuzuordnen, haben Cisco IOS-Headends diese Option nicht und sind daher nicht so flexibel. Cisco Bug ID CSCts31840 wurde zur Behebung dieses Problems abgelegt.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

- **LDAP-Attribute anzeigen**
- **ldap server all anzeigen**

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Hinweis: Weitere Informationen zu Debug-Befehlen vor der Verwendung von **Debug-**Befehlen finden Sie unter Wichtige Informationen.

Aktivieren Sie zur Fehlerbehebung bei der LDAP-Attributzuordnung folgende Debugging-

Optionen:

- debuggen ldap all
- debuggen ldap-Ereignis
- debuggen aaa authentication
- debuggen aaa autorisierung