Affectation de policy group pour les clients d'AnyConnect qui utilisent le LDAP sur l'exemple de configuration de Headends de Cisco IOS

Contenu

Introduction

Ce document décrit comment configurer des cartes d'attribut de Protocole LDAP (Lightweight Directory Access Protocol) pour assigner automatiquement la règle VPN correcte à un utilisateur basé sur leurs qualifications.

> **Note**: Le soutien de l'authentification LDAP pour les utilisateurs de Secure Sockets Layer VPN (VPN SSL) qui connectent au Cisco IOS® un headend est dépisté par l'ID de bogue Cisco CSCuj20940. Jusqu'à ce que le support soit officiellement ajouté, le support de LDAP est le meilleur effort.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- VPN SSL sur le Cisco IOS
- Authentification LDAP sur le Cisco IOS
- Services d'annuaire

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CISCO881-SEC-K9
- Logiciel de Cisco IOS, logiciel C880 (C880DATA-UNIVERSALK9-M), version 15.1(4)M, LOGICIEL de VERSION (fc1)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Le LDAP est un protocole de l'application ouvert, constructeur-neutre, industriellement compatible pour accéder à et mettre à jour des services d'informations distribués de répertoire au-dessus d'un réseau de Procotole IP (Internet Protocol). Les services d'annuaire jouent un important rôle dans le développement de l'intranet et des applications Web pendant qu'ils permettent partager des informations sur des utilisateurs, des systèmes, des réseaux, des services, et des applications dans tout le réseau.

Fréquemment, les administrateurs veulent fournir à des utilisateurs VPN différentes autorisations d'accès ou de contenu WebVPN. Ceci peut être terminé avec la configuration de différentes règles VPN sur le serveur VPN et l'attribution de ces stratégie-positionnements à chaque personne à charge d'utilisateur sur leurs qualifications. Tandis que ceci peut être terminé manuellement, il est plus efficace d'automatiser le processus avec des services d'annuaire. Afin d'employer le LDAP pour assigner une stratégie de groupe à un utilisateur, vous devez configurer une carte qui trace un attribut de LDAP tel que l'attribut « memberOf » de Répertoire actif (AD) à un attribut qui est compris par le headend VPN.

Sur l'appliance de sécurité adaptable (ASA) ceci est régulièrement réalisé par l'attribution de différentes stratégies de groupe à différents utilisateurs avec une carte d'attribut de LDAP suivant les indications de l'utilisation ASA de l'exemple de configuration de cartes d'attribut de LDAP.

Sur le Cisco IOS la même chose peut être réalisée avec la configuration de différents policy group sous le contexte de webvpn et l'utilisation des cartes d'attribut de LDAP afin de déterminer quel policy group l'utilisateur sera assigné. Sur des headends de Cisco IOS, l'attribut d'AD de « memberOf » est tracé au suppliant-groupe d'attribut d'Authentification, autorisation et comptabilité (AAA). Pour plus de détails sur les mappages d'attribut par défaut, voir le LDAP sur des périphériques IOS utilisant l'exemple dynamique de configuration de cartes d'attribut.
Cependant pour le VPN SSL, il y a deux mappages appropriés d'aaa attribute :

Nom d'aaa attribute	Pertinence de VPN SSL
utilisateur-VPN-groupe	cartes au policy group défini sous le contexte de webvpn
webvpn-contexte	cartes au contexte réel de webvpn elle-même

Par conséquent la carte d'attribut de LDAP doit tracer l'attribut approprié de LDAP à l'un ou l'autre un de ces deux attributs d'AAA.

Configurez

Note: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Cette configuration emploie une carte d'attribut de LDAP afin de tracer l'attribut de LDAP de « memberOf » au l'utilisateur-VPN-groupe d'aaa attribute.

1. Configurez la méthode d'authentification et le Groupe de serveurs AAA.
```
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. Configurez une carte d'attribut de LDAP.
```
ldap attribute-map ADMAP
 map type memberOf user-vpn-group
```
3. Configurez le serveur LDAP qui met en référence la carte précédente d'attribut de LDAP.
```
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. Configurez le routeur pour agir en tant que serveur de webvpn. Dans cet exemple, puisque l'attribut de « memberOf » sera tracé à l'attribut de « utilisateur-VPN-groupe », un contexte simple de webvpn est configuré avec les plusieurs policy group qui incluent une stratégie « NOACCESS ». Ce policy group est pour les utilisateurs qui n'ont pas une valeur assortie de « memberOf ».
```
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
```

Mises en garde

1. Si l'utilisateur est de plusieurs groupes d'un « memberOf », la première valeur de « memberOf » est utilisée par le routeur.
2. Ce qui est impair dans cette configuration est que le nom du policy group doit être un précis - correspondance pour la chaîne **complète** poussée par le serveur LDAP pour la « valeur de memberOf ». Habituellement les administrateurs utilisent des noms plus courts et plus appropriés pour le policy group, tel que VPNACCESS, mais indépendamment de la question cosmétique ceci peut mener à un plus grand problème. Il n'est pas rare que la chaîne d'attribut de « memberOf » soit considérablement plus grand que ce qui a été utilisé dans cet exemple. Par exemple, considérez ce message de débogage :

```
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
```

Il prouve clairement que la chaîne reçue de l'AD est :

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

Cependant, puisqu'il n'y a aucun un tel policy group défini, si les essais d'administrateur pour configurer une telle stratégie de groupe il a comme conséquence une erreur parce que le Cisco IOS a une limite sur le nombre de caractères dans le nom de policy group :

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

Dans de telles situations il y a deux contournements possibles :

1. Utilisez un attribut différent de LDAP, tel que le « service ».Considérez cette carte d'attribut de LDAP :

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

   Dans ce cas la valeur de l'attribut de service pour un utilisateur peut être placée à une valeur telle que VPNACCESS et la configuration de webvpn est un peu plus simple :

   ```
   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. Utilisez le mot clé de Dn-à-chaîne dans la carte d'attribut de LDAP.Si le contournement précédent n'est pas approprié puis l'administrateur peut employer le mot clé de dn-à-chaîne dans la carte d'attribut de LDAP afin d'extraire juste la valeur commune du nom (NC) de la chaîne de « memberOf ». Dans ce scénario la carte d'attribut de LDAP serait :

```
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
```

Et la configuration de webvpn serait :

```
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
```

Note: À la différence de dans des ASA où vous pouvez employer la commande de **valeur de carte** sous une carte d'attribut afin d'apparier la valeur reçue du serveur LDAP à une autre localement - la valeur significative, des headends de Cisco IOS n'ont pas cette option et sont donc pas comme flexible. L'ID de bogue Cisco CSCts31840 a été classé afin d'adresser ceci.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

- **attributs de show ldap**
- **serveur tout de show ldap**

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Note: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Afin de dépanner le mappage d'attribut de LDAP, activez ces derniers met au point :

- **mettez au point le LDAP tout**
- **mettez au point l'événement de LDAP**
- **debug aaa authentication**
- **debug aaa authorization**