Asignación del grupo de políticas para los clientes de AnyConnect que utilizan el LDAP en el ejemplo de configuración de los Headends del Cisco IOS

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Antecedentes
Configurar
Diagrama de la red
Advertencias
Verificación
Troubleshooting

Introducción

Este documento describe cómo configurar las correspondencias del atributo del Lightweight Directory Access Protocol (LDAP) para asignar automáticamente la política del VPN correcta a un usuario basado en sus credenciales.

> **Note**: El soporte para la autenticación ldap para los usuarios de Secure Sockets Layer VPN (SSL VPN) que conectan con un headend del ® del Cisco IOS es seguido por el Id. de bug Cisco CSCuj20940. Hasta que el soporte se agregue oficialmente, el soporte LDAP es el mejor esfuerzo.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- SSL VPN en el Cisco IOS
- Autenticación ldap en el Cisco IOS

- Servicios de directorio

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CISCO881-SEC-K9
- Cisco IOS Software, software C880 (C880DATA-UNIVERSALK9-M), versión 15.1(4)M, SOFTWARE DE LA VERSIÓN (fc1)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

El LDAP es un Application Protocol abierto, vendedor-neutral, del estándar de la industria para acceder y para mantener los servicios informativos de información del directorio distribuidos sobre una red del Internet Protocol (IP). Los servicios de directorio desempeñan un papel importante en el desarrollo del intranet y de las aplicaciones de Internet mientras que permiten la distribución de la información sobre los usuarios, los sistemas, las redes, los servicios, y las aplicaciones en la red.

Con frecuencia, los administradores quieren proporcionar a los usuarios VPN diversos permisos de acceso o contenido WebVPN. Esto se puede completar con la configuración de diversas políticas del VPN en el servidor VPN y de la asignación de estos directiva-conjuntos a cada dependen del usuario sobre sus credenciales. Mientras que esto se puede completar manualmente, es más eficiente automatizar el proceso con los servicios de directorio. Para utilizar el LDAP para asignar una directiva del grupo a un usuario, usted necesita configurar una correspondencia que asocie un atributo LDAP tal como el atributo “memberOf” del Active Directory (AD) a un atributo que sea entendido por la cabecera VPN.

En el dispositivo de seguridad adaptante (ASA) esto se alcanza regularmente con la asignación de diversas directivas del grupo a diversos usuarios con una correspondencia del atributo LDAP tal y como se muestra en del uso ASA del ejemplo de configuración de las correspondencias del atributo LDAP.

En el Cisco IOS la misma cosa se puede alcanzar con la configuración de diversos grupos de políticas bajo contexto del WebVPN y el uso de las correspondencias del atributo del LDAP para determinar que asignarán el grupo de políticas el usuario. En los headends del Cisco IOS, el atributo AD del “memberOf” se asocia al supplicant-grupo del atributo del Authentication, Authorization, and Accounting (AAA). Para más detalles en las asignaciones del atributo predeterminado, vea el LDAP en los dispositivos IOS usando el ejemplo de configuración dinámico de las correspondencias del atributo. Sin embargo para SSL VPN, hay dos asignaciones relevantes del atributo AAA:

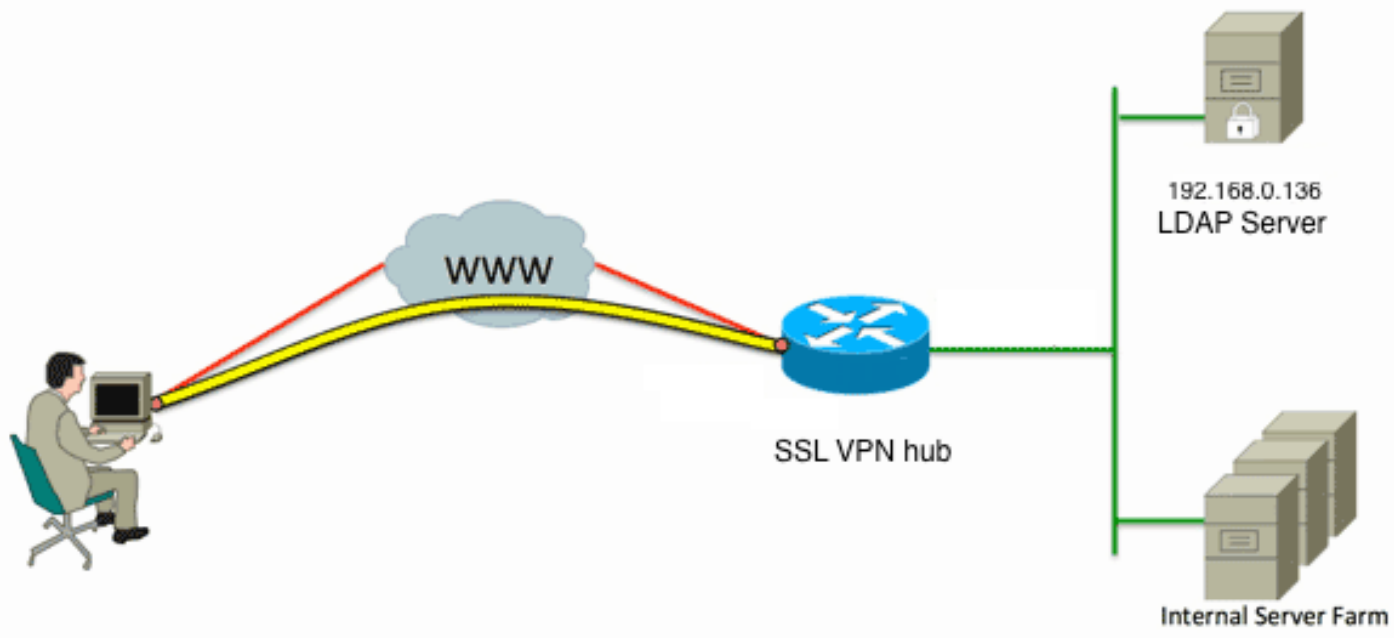
Nombre del atributo AAA	Importancia SSL VPN
usuario-VPN-grupo	correspondencias al grupo de políticas definido bajo contexto del WebVPN
WebVPN-contexto	correspondencias al contexto real del WebVPN sí mismo

Por lo tanto la correspondencia del atributo LDAP necesita asociar el atributo relevante LDAP a cualquiera uno de estos dos atributos AAA.

Configurar

> **Note**: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red



Esta configuración utiliza una correspondencia del atributo LDAP para asociar el atributo LDAP del “memberOf” al usuario-VPN-grupo del atributo AAA.

1. Configure el método de autentificación y al Grupo de servidores 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. Configure una correspondencia del atributo LDAP.

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

3. Configure al servidor LDAP que se refiere a la correspondencia anterior del atributo 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. Configure al router para actuar como servidor WebVPN. En este ejemplo, puesto que el atributo del “memberOf” será asociado al atributo del “usuario-VPN-grupo”, un solo contexto del WebVPN se configura con los grupos de políticas múltiples que incluyen una directiva “NOACCESS”. Este grupo de políticas está para los usuarios que no tienen un valor del “memberOf que corresponde con”.

```
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
```

Advertencias

1. Si el usuario es múltiples grupos de un “memberOf”, el primer valor del “memberOf” es utilizado por el router.
2. Cuál es impar en esta configuración es que el nombre del grupo de políticas tiene que ser un exacto - coincidencia para la cadena **completa** avanzada por el servidor LDAP para el “valor del memberOf”. Los administradores utilizan generalmente nombres más cortos y más

relevantes para el grupo de políticas, tal como VPNACCESS, pero aparte del problema estético éste puede llevar a un problema más grande. No es infrecuente que la cadena del atributo del “memberOf” sea considerablemente más grande que lo que se ha utilizado en este ejemplo. Por ejemplo, considere este mensaje del debug:

```
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
```

Muestra claramente que es la cadena recibida del AD:

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

Sin embargo, puesto que no hay tal grupo de políticas definido, si el administrador intenta configurar tal directiva del grupo da lugar a un error porque el Cisco IOS tiene un límite en el número de caracteres en el nombre de grupo de políticas:

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

En tales situaciones hay dos soluciones alternativas posibles:

1. Utilice un diverso atributo LDAP, tal como “departamento”.Considere esta correspondencia del atributo LDAP:

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

En este caso el valor del atributo del departamento para un usuario se puede fijar a un valor tal como VPNACCESS y la configuración del WebVPN es un bit más 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. Utilice la palabra clave de la DN-a-cadena en la correspondencia del atributo LDAP.Si la solución alternativa anterior no es conveniente entonces el administrador puede utilizar la palabra clave de la dn-a-cadena en la correspondencia del atributo LDAP para extraer apenas el valor del Common Name (CN) de la cadena del “memberOf”. En este escenario la correspondencia del atributo LDAP sería:

```
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
```

Y la configuración del WebVPN sería:

```
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: A diferencia en de los ASA donde usted puede utilizar el **comando value de la correspondencia** bajo una correspondencia del atributo para hacer juego el valor recibido del servidor LDAP a algún otro localmente - el valor significativo, los headends del Cisco IOS no tiene esta opción y está por lo tanto no como flexible. El Id. de bug Cisco CSCts31840 se ha clasifiado para dirigir esto.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

- **muestre los atributos del ldap**
- **muestre al servidor LDAP todo**

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

Note: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Para resolver problemas la asignación del atributo LDAP, habilite estos debugs:

- **haga el debug del ldap todo**
- **haga el debug del evento del ldap**
- **debug aaa authentication**
- **debug aaa authorization**