Ejemplo de Configuración de Asignación de Grupos de Políticas para Clientes de AnyConnect que Utilizan LDAP en Encabezados de Cisco IOS

Contenido

Introducción

Este documento describe cómo configurar mapas de atributos LDAP (protocolo ligero de acceso a directorios) para asignar automáticamente la política VPN correcta a un usuario en función de sus credenciales.

> **Nota:** El ID de bug de Cisco CSCuj20940 realiza un seguimiento del soporte para la autenticación LDAP para los usuarios de VPN de capa de conexión segura (SSL VPN) que se conectan a una cabecera Cisco IOS®. Hasta que se agregue oficialmente el soporte, el soporte LDAP es el mejor esfuerzo.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- VPN SSL en Cisco IOS
- Autenticación LDAP en 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
- Software Cisco IOS, software C880 (C880DATA-UNIVERSALK9-M), versión 15.1(4)M, SOFTWARE DE VERSIÓN (fc1)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

El LDAP es un protocolo de aplicaciones abierto, neutral con respecto al proveedor y estándar del sector para acceder y mantener servicios de información de directorios distribuidos a través de una red de protocolo de Internet (IP). Los servicios de directorio desempeñan un papel importante en el desarrollo de aplicaciones de intranet e Internet, ya que permiten compartir información sobre usuarios, sistemas, redes, servicios y aplicaciones en toda 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 diferentes políticas VPN en el servidor VPN y la asignación de estos conjuntos de políticas a cada usuario según sus credenciales. Aunque esto se puede completar manualmente, es más eficiente automatizar el proceso con los Servicios de directorio. Para utilizar LDAP para asignar una política de grupo a un usuario, debe configurar un mapa que mapee un atributo LDAP como el atributo de Active Directory (AD) "memberOf" a un atributo que entienda la cabecera VPN.

En Adaptive Security Appliance (ASA) esto se logra regularmente mediante la asignación de diferentes políticas de grupo a diferentes usuarios con un mapa de atributos LDAP, como se muestra en Ejemplo de Configuración de Uso de Mapas de Atributo LDAP.

En el IOS de Cisco se puede lograr lo mismo con la configuración de diferentes grupos de políticas bajo el contexto WebVPN y el uso de mapas de atributos LDAP para determinar qué grupo de políticas se asignará al usuario. En las cabeceras de Cisco IOS, el atributo AD "memberOf" se asigna al grupo de suplicantes del atributo Authentication, Authorization and Accounting (AAA). Para obtener más detalles sobre las asignaciones de atributos predeterminadas, vea Ejemplo de Configuración de LDAP en Dispositivos IOS Usando Mapas de Atributo Dinámicos. Sin embargo, para SSL VPN, hay dos asignaciones de atributos AAA relevantes:

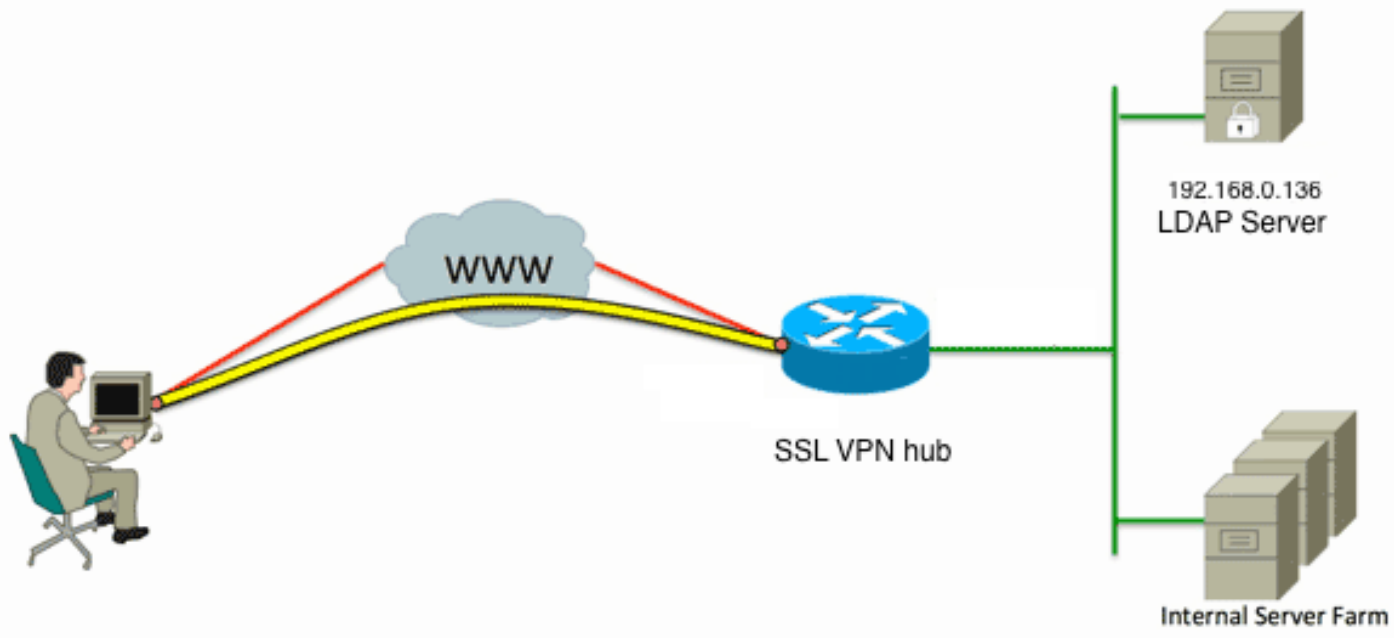
Nombre de atributo AAA	Relevancia de SSL VPN
user-vpn-group	se asigna al grupo de políticas definido en el contexto WebVPN
webvpn-context	se asigna al contexto real de WebVPN

Por lo tanto, el mapa del atributo LDAP necesita asignar el atributo LDAP relevante a cualquiera de estos dos atributos AAA.

Configurar

> **Nota:** 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 un mapa de atributos LDAP para mapear el atributo LDAP "memberOf" al atributo AAA user-vpn-group.

1. Configure el método de autenticación y el 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 un mapa de atributos LDAP.
```
ldap attribute-map ADMAP
 map type memberOf user-vpn-group
```
3. Configure el servidor LDAP que hace referencia al mapa de atributos LDAP anterior.
```
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 el router para que actúe como servidor WebVPN. En este ejemplo, dado que el atributo "memberOf" se asignará al atributo "user-vpn-group", se configura un único contexto WebVPN con varios grupos de políticas que incluyen una política "NOACCESS". Este grupo de políticas es para usuarios que no tienen un valor "memberOf" coincidente.

```
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 un "miembroDe" varios grupos, el router utiliza el primer valor "miembroDe".
2. Lo que es extraño en esta configuración es que el nombre del grupo de políticas debe ser una coincidencia exacta para la cadena **completa** enviada por el servidor LDAP para el "memberOf value". Por lo general, los administradores utilizan nombres más cortos y relevantes para el grupo de políticas, como VPNACCESS, pero aparte del problema superficial, esto puede provocar un problema mayor. No es raro que la cadena de atributo "memberOf" sea considerablemente mayor que la que se ha utilizado en este ejemplo. Por ejemplo, considere este mensaje de depuración:

```
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
```

Muestra claramente que la cadena recibida de AD es:

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

Sin embargo, dado que no hay tal grupo de políticas definido, si el administrador intenta configurar tal política de grupo, se produce un error porque Cisco IOS tiene un límite en el número de caracteres en el nombre del grupo de políticas:

```
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
```

En esas situaciones hay dos posibles soluciones:

1. Utilice un atributo LDAP diferente, como "departamento".Considere este mapa de atributos LDAP:

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

   En este caso, el valor del atributo de departamento para un usuario se puede establecer en un valor como VPNACCESS y la configuración de WebVPN es un poco 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 DN-to-string en el mapa de atributos LDAP.Si la solución alternativa anterior no es adecuada, el administrador puede utilizar la palabra clave dn-to-string en el mapa de atributos LDAP para extraer sólo el valor Common Name (CN) de la cadena "memberOf". En este escenario, el mapa de atributos LDAP sería:

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

   Y la configuración de 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
```

Nota: A diferencia de los ASA donde puede utilizar el comando **map value** bajo un mapa de atributos para hacer coincidir el valor recibido del servidor LDAP con algún otro valor significativo localmente, los encabezados de Cisco IOS no tienen esta opción y, por lo tanto, no son tan flexibles. Se ha registrado el ID de bug Cisco CSCts31840 para abordar esto.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

- **show ldap atributos**
- **show ldap server all**

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

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

Para resolver el problema de asignación de atributos LDAP, habilite estos debugs:

- **debug ldap all**
- **debug ldap event**
- **debug aaa authentication**
- **debug aaa authorization**