El uso ASA del atributo LDAP asocia el ejemplo de configuración

Contenido

Introducción

Este documento describe cómo utilizar las correspondencias del atributo del Lightweight Directory Access Protocol (LDAP) para configurar las directivas dinámicas granulares de Accesss en un dispositivo de seguridad adaptante (ASA).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Secure Sockets Layer VPN (SSL VPN) en el ® del Cisco IOS
- Autenticación Idap 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 IP. Los servicios de directorio desempeñan un papel importante en el desarrollo del intranet y de las aplicaciones de Internet porque permiten la información sobre los usuarios, los sistemas, las redes, los servicios, y las aplicaciones que se compartirán en la red.

Con frecuencia, los administradores quieren proporcionar a los usuarios VPN diversos permisos de acceso o contenido WebVPN. Esto puede ser hecha si usted configura diversas políticas del VPN en el servidor VPN y asigna estos directiva-conjuntos a cada usuario basado en sus credenciales. Mientras que esto se puede hacer 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 **memberOf del** atributo del Active Directory (AD), al atributo de la IETF-Radio-**clase** que es entendido por la cabecera VPN.

En el Cisco IOS, la misma cosa puede ser alcanzada si usted configura a diversos grupos de políticas bajo contexto del WebVPN y utiliza las correspondencias del atributo del LDAP para determinar que asignarán el grupo de políticas el usuario según lo descrito en el documento.

Vea la 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.

En el ASA, esto se alcanza regularmente con la asignación de diversas directivas del grupo a diversos usuarios. Cuando está en uso la autenticación LDAP, esto se puede conseguir automáticamente con una correspondencia de atributo LDAP. Para utilizar el LDAP para asignar una directiva del grupo a un usuario, usted debe asociar un atributo LDAP, tal como el **memberOf del** atributo AD al atributo de la Grupo-**directiva** que es entendido por el ASA. La asignación del atributo se establece una vez, usted debe asociar el valor de atributo configurado en el servidor LDAP al nombre de una directiva del grupo en el ASA.

> Nota: El atributo del **memberOf** corresponde al grupo que el usuario es una parte de en el Active Directory. Es posible que un usuario sea un miembro de más de un grupo en el Active Directory. Esto hace los atributos múltiples del **memberOf** ser enviada por el servidor, pero el ASA puede hacer juego solamente un atributo a una directiva del grupo.

FAQ

Q. ¿Hay un límite de configuración en el número de ldap-atributo-correspondencias para el ASA?

R. No, allí no es ningún límite. las ldap-atributo-correspondencias se afectan un aparato dinámicamente durante la sesión de acceso remoto VPN que utiliza la autenticación ldap/la autorización.

Q. ¿Hay un límite en los números de atributos que se puedan asociar por el ldap-atributo-mapa?

R. Ningunos límites de configuración.

Q. ¿Hay una restricción en cuántos servidores LDAP a quienes un ldap-atributo-mapa específico puede ser aplicado?

R. Ninguna restricción. El código LDAP verifica solamente que el nombre del ldap-atributo-mapa sea válido.

Q. ¿Hay limitaciones con las ldap-atributo-correspondencias y atributos muti-valorados como el memberOf AD?

R. Sí. Aquí, solamente se explica el AD, pero se aplica a cualquier servidor LDAP que utilice los atributos del multi-valor para las decisiones de políticas. El ldap-atributo-mapa tiene una limitación con los atributos polivalentes como el memberOf AD. Si un usuario es un memberOf de varios grupos AD (que es común) y el ldap-atributo-mapa hace juego más de uno de ellos, el valor asociado será elegido basó en la alfabetización de las entradas correspondidas con. Puesto que

este comportamiento no es obvio o intuitivo, es importante tener conocimiento claro sobre cómo trabaja.

Resumen Si la sincronización LDAP da lugar a los valores múltiples para un atributo, el valor de atributo final será elegido como sigue:

- Primero, seleccione los valores con el número más pequeño de caracteres.
- Si esto da lugar a más de un valor, elija el valor que es el más bajo del orden alfabético.

Utilice los ejemplos de caso

El Directorio-LDAP activo vuelve estos casos de cuatro memberOf para una autenticación de usuario o un pedido de autorización:

```
memberOf: value = CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com
memberOf: value = CN=Cisco-Eng,CN=Users,DC=stbu,OU=cisco,DC=com
memberOf: value = CN=Employees,CN=Users,OU=stbu,DC=cisco,DC=com
memberOf: value = CN=Engineering,CN=Users,OU=stbu,DC=cisco,DC=com
```

LDAP-MAP #1: Asuma que este ldap-atributo-mapa está configurado para asociar diversas grupo-directivas ASA basadas en la configuración del memberOf:

```
ldap attribute-map Class
map-name memberOf Group-Policy
map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup4
map-value memberOf CN=cisco-Eng,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup3
map-value memberOf CN=Employees,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup2
map-value memberOf CN=Engineering,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup1
```

En este caso, las coincidencias ocurrirán en los cuatro valores de directiva del grupo (ASAGroup1 - ASAGroup4). Sin embargo, la conexión será asignada a la grupo-directiva ASAGroup1 porque ocurre primero en el orden alfabético.

LDAP-MAP #2: Este ldap-atributo-mapa es lo mismo, a menos que el primer memberOf no tenga un mapa-valor explícito asignado (ningún ASAGroup4). Observe que cuando no hay mapa-valor explícito definido, el texto del atributo recibido del LDAP está utilizado.

```
ldap attribute-map Class
map-name memberOf Group-Policy
map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com
map-value memberOf CN=cisco-Eng,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup3
map-value memberOf CN=Employees,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup2
map-value memberOf CN=Engineering,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup1
```

Como en el caso anterior, las coincidencias ocurren en las cuatro entradas. En este caso, puesto que no se proporciona ningún valor asociado para la entrada APP-SSL-VPN, el valor asociado omitirá los administradores CN=APP-SSL-VPN, cn=Users, OU=stbu, dc=cisco, dc=com. Puesto que CN=APP-SSL-VPN aparece primero en la orden aphabetical, APP-SSL-VPN será seleccionado como el valor de directiva.

Refiera al Id. de bug Cisco CSCub64284 para más información. Refiera al PIX/ASA 8.0: Utilice la autenticación ldap para asignar una directiva del grupo en el login, que muestra un caso simple LDAP con el memberOf que pudo trabajar en su despliegue determinado.

Workaround/opciones de la mejor práctica

1. Utilice la directiva del acceso dinámico (el DAP) - El DAP no tiene esta limitación de analizar los atributos polivalentes (como el memberOf); pero el DAP no puede fijar actualmente una grupo-directiva dentro de sí mismo. Esto significa que la sesión tendría que ser dividida en segmentos correctamente vía los métodos de la asociación del grupo de túnel/grupo-directiva. En el futuro, el DAP tendrá la capacidad para fijar cualquier atributo del authorizaiton, incluyendo la grupo-directiva, (Id. de bug Cisco CSCsi54718), así que la necesidad de un para este propósito del ldap-atributo-mapa no será requerida eventual.

2. Como una alternativa y si el escenario de instrumentación la permite, siempre que usted deba utilizar un ldap-atributo-mapa para fijar el atributo de clase, usted posibles podría también utilizar un atributo de un solo valor (como el departamento) que representa su diferenciación del grupo en el AD.

   Nota: En un memberOf DN tal como “CN=Engineering, OU=Office1, dc=cisco, dc=com”, usted puede tomar solamente la decisión en el primer DN, que es CN=Engineering, no la unidad organizativa (OU). Hay una mejora a poder capaz filtrar en cualquier campo DN.

Configuración - Casos del uso de la muestra

> Nota: Cada ejemplo descrito en esta sección es una configuración independiente, pero puede ser mezclado y correspondido con con uno a para producir la política de acceso deseada.

> Consejo: Los nombres y los valores del atributo son con diferenciación entre mayúsculas y minúsculas. Si no ocurre la asignación correctamente, esté seguro que el deletreo y la capitalización correctos se ha utilizado en la correspondencia del atributo LDAP para los nombres y los valores del atributo de Cisco y LDAP.

1. Aplicación de políticas de los atributos basados en el usuario

Cualquier atributo estándar LDAP se puede asociar a un atributo específico del vendedor bien conocido del dispositivo (VSA). Uno o más atributos LDAP se pueden asociar a uno o más atributos de Cisco LDAP. Para una lista completa de Cisco LDAP VSA, refiera los atributos soportados de Cisco para la autorización LDAP. Este ejemplo muestra cómo aplicar un banner para el user1 LDAP. El user1 puede ser cualquier tipo del Acceso Remoto VPN: IPSec, SVC, o clientless del WebVPN. Este ejemplo utiliza las propiedades/general/atributo/campo de la oficina para aplicar el Banner1.

> Nota: Usted podría utilizar el atributo/el campo del departamento AD para asociar a Cisco la IETF-Radio-clase VSA para aplicar las directivas ASA/PIX de una grupo-directiva. Hay ejemplos de esto más adelante en el documento.

La atributo-asignación LDAP (para Microsoft AD y Sun) se soporta a partir de la versión 7.1.x del PIX/ASA. Cualquier atributo Microsoft/AD se puede asociar a un atributo de Cisco. Aquí está el procedimiento para realizar esto:

1. En el servidor AD/LDAP:Seleccione el user1.Click derecho **> propiedades**.Seleccione una lengueta para ser utilizado para fijar un atributo (ejemplo. Ficha general).Seleccione un campo/un atributo, por ejemplo el campo de la “oficina”, para ser utilizado para hacer cumplir el tiempo-rango, y ingrese el texto del banner (ejemplo, recepción al LDAP!!!!). La configuración de la “oficina” en el GUI se salva en el atributo “physicalDeliveryOfficeName” AD/LDAP.

2. En el ASA, para crear una tabla de correspondencia del atributo LDAP, asocie el atributo “physicalDeliveryOfficeName” AD/LDAP al atributo el "Banner1" ASA:
```
B200-54(config)# show run ldap
ldap attribute-map Banner
map-name physicalDeliveryOfficeName Banner1
```

3. Asocie la correspondencia del atributo LDAP a la entrada del AAA-servidor:
```
B200-54(config-time-range)# show runn aaa-server microsoft
aaa-server microsoft protocol ldap
aaa-server microsoft host audi-qa.frdevtestad.local
ldap-base-dn dc=frdevtestad,dc=local
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password hello
ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
ldap-attribute-map Banner
```

4. Establezca a la sesión de acceso remoto y verifiquela que el banner la “recepción al LDAP!!!!” se presenta al usuario de VPN.

2. Coloque a los usuarios LDAP en una Grupo-directiva específica - Ejemplo genérico

Este ejemplo demuestra la autenticación del user1 en el servidor AD-LDAP y extrae el valor de campo del departamento así que puede ser asociado ASA/PIX a una grupo-directiva de la cual las directivas sean aplicadas.

1. En el servidor AD/LDAP:Seleccione el user1.Click derecho **> propiedades**.Seleccione una lengueta para ser utilizado para fijar un atributo (ejemplo. Lengueta de la organización).Seleccione un campo/un atributo, por ejemplo “departamento”, para ser utilizado para hacer cumplir una grupo-directiva, y ingrese el valor de la grupo-directiva (Group-Policy1) en ASA/PIX. La configuración del “departamento” en el GUI se salva en el atributo “departamento” AD/LDAP.

2. Defina una tabla del ldap-atributo-mapa.
```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department Group-Policy
5520-1(config)#
```

   Nota: Como resultado de la implementación del Id. de bug Cisco CSCsv43552, un nuevo atributo del ldap-atributo-mapa, Grupo-directiva, fue introducido para substituir la IETF-Radio-clase. El CLI en la Versión de ASA 8.2 soporta la palabra clave de la IETF-Radio-clase como opción válida en los comandos del nombre de asignación y del mapa-valor para leer un archivo de configuración 8.0 (escenario de la actualización del software). El código

adaptante del Administrador de dispositivos de seguridad (ASDM) se ha puesto al día ya para visualizar no más la IETF-Radio-clase como opción cuando usted configura una entrada de mapeo del atributo. Además, el ASDM pondrá el atributo de la IETF-Radio-clase en escrito (si está leído adentro en los 8.0 config) como el atributo de la Grupo-directiva.

3. Defina la grupo-directiva Group_policy1 en el dispositivo y los atributos de la política requeridos.

4. Establezca el túnel de acceso remoto VPN y verifiquelo que la sesión hereda los atributos de Group-Policy1 (y cualquier otros atributos aplicables de la grupo-directiva predeterminada).

   Nota: Agregue más atributos a la correspondencia como sea necesario. Este ejemplo muestra solamente el mínimo para controlar esta función específica (coloque a un usuario en una grupo-directiva 7.1.x del específico ASA/PIX). El tercer ejemplo muestra este tipo de correspondencia.

Configure una Grupo-directiva NOACCESS

Usted puede crear una grupo-directiva NOACCESS para negar la conexión VPN cuando el usuario no es grupos uces de los de la parte de LDAP. Estos fragmentos de la configuración se muestran para su referencia:

```
group-policy NOACCESS internal
group-policy NOACCESS attributes
vpn-simultaneous-logins 0
vpn-tunnel-protocol IPSec webvpn
```

Usted debe aplicar esta directiva del grupo como directiva del grupo predeterminado al grupo de túnel. Esto permite los usuarios que consiguen una asignación de la correspondencia del atributo LDAP, por ejemplo los que pertenezcan a un grupo deseado LDAP, para conseguir sus directivas deseadas del grupo y a los usuarios que no consiguen ninguna asignación, por ejemplo los que no pertenezcan a los grupos deseados uces de los LDAP, para conseguir la grupo-directiva NOACCESS del grupo de túnel, que bloquea el acceso para ellos.

Consejo: Puesto que el atributo de los VPN-simultáneo-logines se fija a 0 aquí, debe ser definido explícitamente en el resto de grupo-directivas también; si no, será heredado de la grupo-directiva predeterminada para ese grupo de túnel, que en este caso es la directiva NOACCESS.

3. Aplicación de políticas basada en el grupo de los atributos - Ejemplo

Nota: La implementación/el arreglo del Id. de bug Cisco CSCse08736 se requiere, así que el ASA debe funcionar con por lo menos la versión 7.2.2.

1. En el servidor AD-LDAP, los usuarios de directorio activo y computadora, configuran un registro del usuario (VPNUserGroup) que represente a un grupo donde se configuran los atributos VPN.

2. En el servidor AD-LDAP, los usuarios de directorio activo y computadora, definen cada

campo del departamento de registro del usuario para señalar al registro de grupos (VPNUserGroup) en el paso 1. El Nombre de usuario en este ejemplo es **web1**.

Nota: El atributo del departamento AD fue utilizado solamente porque el “departamento” refiere lógicamente a la grupo-directiva. En la realidad, cualquier campo podía ser utilizado. El requisito es que este campo tiene que asociar a la Grupo-directiva del atributo del Cisco VPN tal y como se muestra en de este ejemplo.

3. Defina una tabla del ldap-atributo-mapa:

```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department IETF-Radius-Class
map-name description\Banner1
map-name physicalDeliveryOfficeName IETF-Radius-Session-Timeout
5520-1(config)#
```

La descripción y la oficina de dos atributos AD-LDAP (representadas por la descripción y PhysicalDeliveryOfficeName de los nombres AD) son los atributos del registro de grupos (para VPNUSerGroup) que las correspondencias al Cisco VPN atribuyen Banner1 y el IETF-Radio-Sesión-descanso.

El atributo del departamento está para que el registro del usuario asocie al nombre de la grupo-directiva externa en el ASA (VPNUSer), que entonces asocia de nuevo al expediente de VPNuserGroup en el servidor AD-LDAP, donde se definen los atributos.

Nota: El atributo de Cisco (Grupo-directiva) se debe definir en el ldap-atributo-mapa. Su AD-atributo asociado puede ser cualquier atributo settable AD. Este ejemplo utiliza el departamento porque es la mayoría del nombre lógico que refiere a la grupo-directiva.

4. Configure el AAA-servidor con el nombre del ldap-atributo-mapa que se utilizará para las operaciones de la autenticación ldap, de la autorización, y de las estadísticas (AAA):

```
5520-1(config)# show runn aaa-server LDAP-AD11
aaa-server LDAP-AD11 protocol ldap
aaa-server LDAP-AD11 host 90.148.1.11
ldap-base-dn cn=Users,dc=nelson,dc=cisco,dc=com
ldap-scope onelevel
ldap-naming-attribute sAMAccountName
ldap-login-password altiga
ldap-login-dn cn=Administrator,cn=Users,dc=nelson,dc=cisco,dc=com
ldap-attribute-map Our-AD-Map
5520-1(config)#
```

5. Defina a un grupo de túnel con con la autenticación ldap o la autorización LDAP.

Ejemplo con la autenticación ldap. Realiza la autenticación + aplicación de políticas del atributo (de la autorización) si se definen los atributos.

```
5520-1(config)# show runn tunnel-group
remoteAccessLDAPTunnelGroup
tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
authentication-server-group LDAP-AD11
accounting-server-group RadiusACS28
```

5520-1(config)#Ejemplo con la autorización LDAP. Configuración usada para usar los Certificados digitales.

```
5520-1(config)# show runn tunnel-group
remoteAccessLDAPTunnelGroup
tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
authentication-server-group none
authorization-server-group LDAP-AD11
accounting-server-group RadiusACS28
authorization-required
authorization-dn-attributes ea
5520-1(config)#
```

6. Defina una grupo-directiva externa. El nombre de la grupo-directiva es el valor del registro del usuario AD-LDAP que representa el grupo (VPNUserGroup).

```
5520-1(config)# show runn group-policy VPNUserGroup
group-policy VPNUserGroup external server-group LDAP-AD11
5520-1(config)#
```

7. Establezca el túnel y verifiquelo que los atributos están aplicados. En este caso, el banner y el Sesión-descanso se aplica del expediente de VPNuserGroup en el AD.

4. La aplicación del Active Directory de “asigna un IP Address estático” para el IPSec y los túneles de SVC

El atributo AD es msRADIUSFramedIPAddress. El atributo se configura en las propiedades del usuario AD, dial-in tab, “asigna un IP Address estático”.

Éstos son los pasos:

1. En el servidor AD, bajo propiedades del usuario, el dial-in tab, “asigna un IP Address estático”, ingresa el valor del IP Address para asignar a la sesión IPsec/SVC (10.20.30.6).

2. En el ASA cree un ldap-atributo-mapa con esta asignación:

```
5540-1# show running-config ldap
ldap attribute-map Assign-IP
map-name msRADIUSFrameIPAdddress IETF-Radius-Framed-IP-Address
5540-1#
```

3. En el ASA, verifique el VPN-direccionamiento-assigment se configura para incluir el “VPN-addr-asignar-AAA”:

```
5520-1(config)# show runn all vpn-addr-assign
vpn-addr-assign aaa
no vpn-addr-assign dhcp
vpn-addr-assign local
5520-1(config)#
```

4. Establezca las sesiones remotas de la autoridad IPsec/SVC (RA) y verifique con “el telecontrol de VPN-sessiondb de la demostración|svc” que “IP asignada el” campo está correcto (10.20.30.6).

5. La aplicación del Active Directory del “dial-in del Permiso de acceso remoto, permite/niega el acceso”

Soporta todas las sesiones remotas VPN Acccess: IPSec, WebVPN, y SVC. Permita el acceso tiene un valor de VERDAD. Niegue Acccess tiene un valor de FALSO. El nombre del atributo AD es msNPAllowDialin.

Este ejemplo demuestra la creación de un ldap-atributo-mapa que utilice los protocolos de túneles de Cisco para crear permita el acceso (VERDAD) y niega las condiciones (FALSAS). Por ejemplo, si usted asocia el IPSec tunnel-protocol=L2TPover (8), usted puede crear una condición FALSA si usted intenta aplicar el acceso para el WebVPN y el IPSec. La lógica reversa se aplica también.

Éstos son los pasos:

1. En las propiedades del user1 del servidor AD, el dial-in, selecciona el apropiado permite el acceso o niega el acceso para cada usuario.

   Nota: Si usted selecciona la tercera opción “acceso del control con la política de acceso remoto,” no se vuelve ningún valor del servidor AD, tan los permisos se aplican que se basan en la configuración de las grupo-directivas internas ASA/PIX.

2. En el ASA, cree un ldap-atributo-mapa con esta asignación:

   ```
   ldap attribute-map LDAP-MAP
   map-name msNPAllowDialin Tunneling-Protocols
   map-value msNPAllowDialin FALSE 8
   map-value msNPAllowDialin TRUE 20
   5540-1#
   ```

   Nota: Agregue más atributos a la correspondencia como sea necesario. Este ejemplo muestra solamente el mínimo para controlar esta función específica (permita o niegue el acceso basado en la configuración del dial-in).

   ¿Qué el ldap-atributo-mapa significa o aplica?

   msNPAllowDialin 8 FALSOS del mapa-valor

   Niegue el acceso para un user1. La condición FALSA del valor asocia al Tunnel Protocol L2TPoverIPsec, (el valor 8).

   Permita el acceso para user2. La condición del valor verdadero asocia al Tunnel Protocol el WebVPN + el IPSec, (valor 20).

   Un WebVPN/usuario IPsec, authenticaticated como user1 en el AD, fallaría debido a la discordancía del Tunnel Protocol.

   Un L2TPoverIPsec, authenticaticated como user1 en el AD, fallaría debido a la regla de la negación.

   Un WebVPN/usuario IPsec, authenticaticated como user2 en el AD, tendría éxito (permita la

regla + Tunnel Protocol correspondido con).

Un L2TPoverIPsec, authenticaticated como user2 en el AD, fallaría debido a la discordancía del Tunnel Protocol.
Soporte para el Tunnel Protocol, según lo definido en el RFCs 2867 y 2868.

6. Aplicación del Active Directory del “miembro” de la calidad de miembro /Group para permitir o para negar el acceso

Este caso está estrechamente vinculado encajonar 5, prevé un flujo más lógico, y es el método recomendado, puesto que establece el control de la membresía del grupo como condición.

1. Configure al usuario AD para ser “miembro” de un grupo específico. Utilice un nombre que lo coloque en la cima de la grupo-jerarquía (ASA-VPN-consultores). En AD-LDAP, la membresía del grupo es definida por el atributo “memberOf” AD.

   Es importante que el grupo esté en la cima de la lista, puesto que usted puede aplicar actualmente solamente las reglas a la primera cadena del “memberOf” del grupo. En la versión 7.3, usted podrá realizar la filtración y la aplicación de los múltiples grupos.
2. En el ASA, cree un ldap-atributo-mapa con el asignación mínima:

   ```
   ldap attribute-map LDAP-MAP
   map-name memberOf Tunneling-Protocols
   map-value memberOf cn=ASA-VPN-Consultants,cn=Users,dc=abcd,dc=com 4

   5540-1#
   ```

   Nota: Agregue más atributos a la correspondencia como sea necesario. Este los ejemplos muestran solamente el mínimo para controlar esta función específica (permita o niegue el acceso basado en la membresía del grupo).

   ¿Qué el ldap-atributo-mapa significa o aplica?

   User=joe_consultant, la parte de AD, que es miembro del grupo “ASA-VPN-consultores” AD no será prohibido el acceso solamente si el usuario utiliza el IPSec (tunnel-protocol=4=IPSec).

   User=joe_consultant, la parte de AD, fallará el acceso VPN durante cualquier otro cliente de acceso remoto (PPTP/L2TP, L2TP/IPSec, WebVPN/SVC, y así sucesivamente).

   User=bill_the_hacker no será permitido adentro puesto que el usuario no tiene ninguna calidad de miembro AD.

7. La aplicación del Active Directory de las “horas de inicio de sesión/hora gobierna”

Este caso del uso describe cómo configurar y aplicar las reglas del Time Of Day en AD/LDAP.

Aquí está el procedimiento para hacer esto:

1. En el servidor AD/LDAP:Seleccione al usuario.Click derecho **> propiedades**.Seleccione una lengueta para ser utilizado para fijar un atributo (ejemplo. Ficha general).Seleccione un campo/un atributo, por ejemplo el campo de la “oficina”, para ser utilizado para hacer cumplir el tiempo-rango, y ingrese el nombre del tiempo-rango (por ejemplo, Boston). La configuración de la “oficina” en el GUI se salva en el atributo “physicalDeliveryOfficeName” AD/LDAP.

2. En el ASA

   Cree una tabla de correspondencia del atributo LDAP.Asocie el atributo “physicalDeliveryOfficeName” AD/LDAP al atributo “horas de acceso” ASA.

   Ejemplo:

   ```
   B200-54(config-time-range)# show run ldap
   ldap attribute-map TimeOfDay
   map-name physicalDeliveryOfficeName Access-Hours
   ```

3. En el ASA, asocie la correspondencia del atributo LDAP a la entrada del AAA-servidor:

   ```
   B200-54(config-time-range)# show runn aaa-server microsoft
   aaa-server microsoft protocol ldap
   aaa-server microsoft host audi-qa.frdevtestad.local
   ldap-base-dn dc=frdevtestad,dc=local
   ldap-scope subtree
   ldap-naming-attribute sAMAccountName
   ldap-login-password hello
   ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
   ldap-attribute-map TimeOfDay
   ```

4. En el ASA, cree un objeto del tiempo-rango que tenga el valor del nombre que se asigna al usuario (valor de la oficina en el paso 1):`B200-54(config-time-range)# show runn time-range`
   ```
   !
   time-range Boston
   periodic weekdays 8:00 to 17:00
   !
   ```

5. Establezca a la sesión de acceso remoto VPN:

   La sesión debe tener éxito si dentro del tiempo-rango.La sesión debe fallar si fuera del tiempo-rango.

8. Utilice la configuración del ldap-mapa para asociar a un usuario en una Grupo-directiva específica y para utilizar el comando del autorización-servidor-grupo, en el caso de la Autenticación doble

1. En este escenario, se utiliza la Autenticación doble. El primer servidor de autenticación usado es RADIUS y la segunda autenticación separa utilizado es servidor LDAP.

   Configure el servidor LDAP así como al servidor de RADIUS. Aquí tiene un ejemplo:

   ```
   ASA5585-S10-K9# show runn aaa-server
   ```

```
aaa-server test-ldap protocol ldap
aaa-server test-ldap (out) host 10.201.246.130
 ldap-base-dn cn=users, dc=htts-sec, dc=com
 ldap-login-password *****
 ldap-login-dn cn=Administrator, cn=Users, dc=htts-sec, dc=com
 server-type microsoft
 ldap-attribute-map Test-Safenet-MAP
aaa-server test-rad protocol radius
aaa-server test-rad (out) host 10.201.249.102
 key *****
```

Definine la correspondencia del atributo LDAP. Aquí tiene un ejemplo:

```
ASA5585-S10-K9# show runn ldap
ldap attribute-map Test-Safenet-MAP
map-name memberOf IETF-Radius-Class
map-value memberOf "CN=DHCP Users,CN=Users,DC=htts-sec,DC=com" Test-Policy-Safenet
```

Defina al grupo de túnel y asocie el RADIUS y al servidor LDAP para la autenticación. Aquí tiene un ejemplo:

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

Vea la grupo-directiva que se utiliza en la configuración del grupo de túnel:

```
ASA5585-S10-K9# show runn group-policy
group-policy NoAccess internal
group-policy NoAccess attributes
wins-server none
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 0
default-domain none
group-policy Test-Policy-Safenet internal
group-policy Test-Policy-Safenet attributes
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 15
vpn-idle-timeout 30
vpn-tunnel-protocol ikev1 ssl-client ssl-clientless
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Safenet-Group-Policy-SplitAcl
default-domain none
```

Con esta configuración, no colocaron a los usuarios de AnyConnect que fueron asociados correctamente con el uso de los atributos LDAP en la grupo-directiva, Prueba-directiva-Safenet. En lugar, los todavía colocaron en la grupo-directiva predeterminada, en este caso NoAccess.

Vea el snippet de los debugs (ldap 255 del debug) y de los Syslog en informativo llano:

```
---------------------------------------------------------------------------
```

```
memberOf: value = CN=DHCP Users,CN=Users,DC=htts-sec,DC=com

[47]                        mapped to IETF-Radius-Class: value = Test-Policy-Safenet

[47]                        mapped to LDAP-Class: value = Test-Policy-Safenet

--------------------------------------------------------------------------------

Syslogs :

%ASA-6-113004: AAA user authentication Successful : server = 10.201.246.130 : user =
test123

%ASA-6-113003: AAA group policy for user test123 is being set to Test-Policy-Safenet

%ASA-6-113011: AAA retrieved user specific group policy (Test-Policy-Safenet) for user =
test123

%ASA-6-113009: AAA retrieved default group policy (NoAccess) for user = test123

%ASA-6-113013: AAA unable to complete the request Error : reason = Simultaneous logins
exceeded for user : user = test123

%ASA-6-716039: Group <DfltGrpPolicy> User <test123> IP <10.116.122.154> Authentication:
rejected, Session Type: WebVPN.
```

Daban el error de la demostración de estos Syslog como el usuario la grupo-directiva de NoAccess que tenía simultáneo-login fijado a 0 aunque los Syslog lo dicen extrajeron una grupo-directiva del específico del usuario.

Para tener el usuario asignado en la grupo-directiva, sobre la base del LDAP-mapa, usted debe tener este comando: **prueba-ldap del autorización-servidor-grupo** (en este caso, el prueba-**ldap** es el nombre de servidor LDAP). Aquí tiene un ejemplo:

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
authorization-server-group test-ldap
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

2. Ahora, si el primer servidor de autenticación (RADIUS, en este ejemplo) envió los atributos específicos del usuario, por ejemplo el atributo de la IEFT-clase, en ese caso, el usuario será asociado a la grupo-directiva enviada por el RADIUS. Tan aunque el servidor secundario hace una correspondencia LDAP configurar y los atributos LDAP del usuario asocian al usuario a una diversa grupo-directiva, la grupo-directiva enviada por el primer servidor de autenticación será aplicada.

   Para tener el usuario coloque en una grupo-directiva basada en el atributo de la correspondencia LDAP, usted debe especificar este comando bajo grupo de túnel: **prueba-**

ldap del autorización-servidor-grupo.

3. Si el primer servidor de autenticación es el SDI o el OTP, que no pueden pasar el atributo específico del usuario, después el usuario caería en la grupo-directiva predeterminada del grupo de túnel. En este caso, NoAccess aunque la sincronización LDAP está correcta.

   En este caso, usted también necesitaría el comando, prueba-**ldap del autorización-servidor-grupo**, bajo grupo de túnel para que el usuario sea colocado en la grupo-directiva correcta.

4. Si ambos servidores son el mismo RADIUS o servidores LDAP, después usted no necesita el comando del autorización-servidor-**grupo** para que el bloqueo de la grupo-directiva trabaje.

Verificación

```
ASA5585-S10-K9# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : test123                  Index        : 2
Assigned IP  : 10.34.63.1             Public IP    : 10.116.122.154
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : 3DES 3DES 3DES         Hashing      : SHA1 SHA1 SHA1
Bytes Tx     : 14042                  Bytes Rx     : 8872
Group Policy : Test-Policy-Safenet    Tunnel Group : Test_Safenet
Login Time   : 10:45:28 UTC Fri Sep 12 2014
Duration     : 0h:01m:12s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

Troubleshooting

Use esta sección para resolver problemas su configuración.

Haga el debug de la transacción LDAP

Estos debugs se pueden utilizar para ayudar a aislar los problemas con la configuración DAP:

- ldap 255 del debug
- traza del dap del debug
- debug aaa authentication

El ASA no puede autenticar a los usuarios del servidor LDAP

En caso de que el ASA no pueda autenticar los usuarios del LDAP sirven, aquí son algunos debugs de la muestra:

```
ldap 255 output:[1555805] Session Start[1555805] New request Session, context
0xcd66c028, reqType = 1[1555805]
```

```
Fiber started[1555805] Creating LDAP context with uri=ldaps://172.30.74.70:636
[1555805] Connect to LDAP server:
ldaps://172.30.74.70:636, status = Successful[1555805] supportedLDAPVersion:
value = 3[1555805]
supportedLDAPVersion: value = 2[1555805] Binding as administrator[1555805]
Performing Simple
authentication for sysservices to 172.30.74.70[1555805] Simple authentication
for sysservices returned code (49)
Invalid credentials[1555805] Failed to bind as administrator returned code
(-1) Can't contact LDAP server[1555805]
Fiber exit Tx=222 bytes Rx=605 bytes, status=-2[1555805] Session End
```

De estos debugs, o el formato del login DN LDAP es incorrecto o la contraseña es incorrecta así que verifique ambos para resolver el problema.