Exemplo de configuração de atribuição de grupo de política para clientes AnyConnect que usam LDAP em headends do Cisco IOS

Contents

Introduction

Este documento descreve como configurar mapas de atributos do Lightweight Diretory Access Protocol (LDAP) para atribuir automaticamente a política de VPN correta a um usuário com base em suas credenciais.

> **Note**: O suporte para autenticação LDAP para usuários de SSL VPN (Secure Sockets Layer VPN) que se conectam a um headend do Cisco IOS® é rastreado pelo bug da Cisco ID CSCuj20940. Até que o suporte seja oficialmente adicionado, o suporte LDAP é o melhor esforço.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- VPN SSL no Cisco IOS
- Autenticação LDAP no Cisco IOS
- Serviços de diretório

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- CISCO881-SEC-K9
- Software Cisco IOS, software C880 (C880DATA-UNIVERSALK9-M), versão 15.1(4)M, SOFTWARE DE VERSÃO (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.

Informações de Apoio

O LDAP é um protocolo de aplicativo padrão do setor aberto, neutro em relação ao fornecedor, para acessar e manter serviços de informações de diretório distribuído em uma rede IP (Internet Protocol). Os serviços de diretório desempenham um papel importante no desenvolvimento de aplicativos de intranet e Internet, pois permitem o compartilhamento de informações sobre usuários, sistemas, redes, serviços e aplicativos em toda a rede.

Frequentemente, os administradores querem fornecer aos usuários VPN diferentes permissões de acesso ou conteúdo WebVPN. Isso pode ser concluído com a configuração de diferentes políticas de VPN no servidor VPN e a atribuição desses conjuntos de políticas a cada usuário, dependendo de suas credenciais. Embora isso possa ser concluído manualmente, é mais eficiente automatizar o processo com os Serviços de Diretório. Para usar o LDAP para atribuir uma política de grupo a um usuário, você precisa configurar um mapa que mapeie um atributo LDAP como o atributo "memberOf" do Ative Diretory (AD) para um atributo compreendido pelo headend da VPN.

No Adaptive Security Appliance (ASA), isso é obtido regularmente através da atribuição de diferentes políticas de grupo a diferentes usuários com um mapa de atributos LDAP, como mostrado no Exemplo de Configuração de Mapas de Atributos LDAP do ASA.

No Cisco IOS, a mesma coisa pode ser alcançada com a configuração de diferentes grupos de política no contexto WebVPN e com o uso de mapas de atributos LDAP para determinar qual grupo de política o usuário será atribuído. Nos headends do Cisco IOS, o atributo "memberOf" do AD é mapeado para o grupo-suplicante de atributo Authentication, Authorization, and Accounting (AAA). Para obter mais detalhes sobre os mapeamentos de atributos padrão, consulte Exemplo de Configuração de Mapas de Atributos Dinâmicos de LDAP em Dispositivos IOS. No entanto, para SSL VPN, há dois mapeamentos de atributos AAA relevantes:

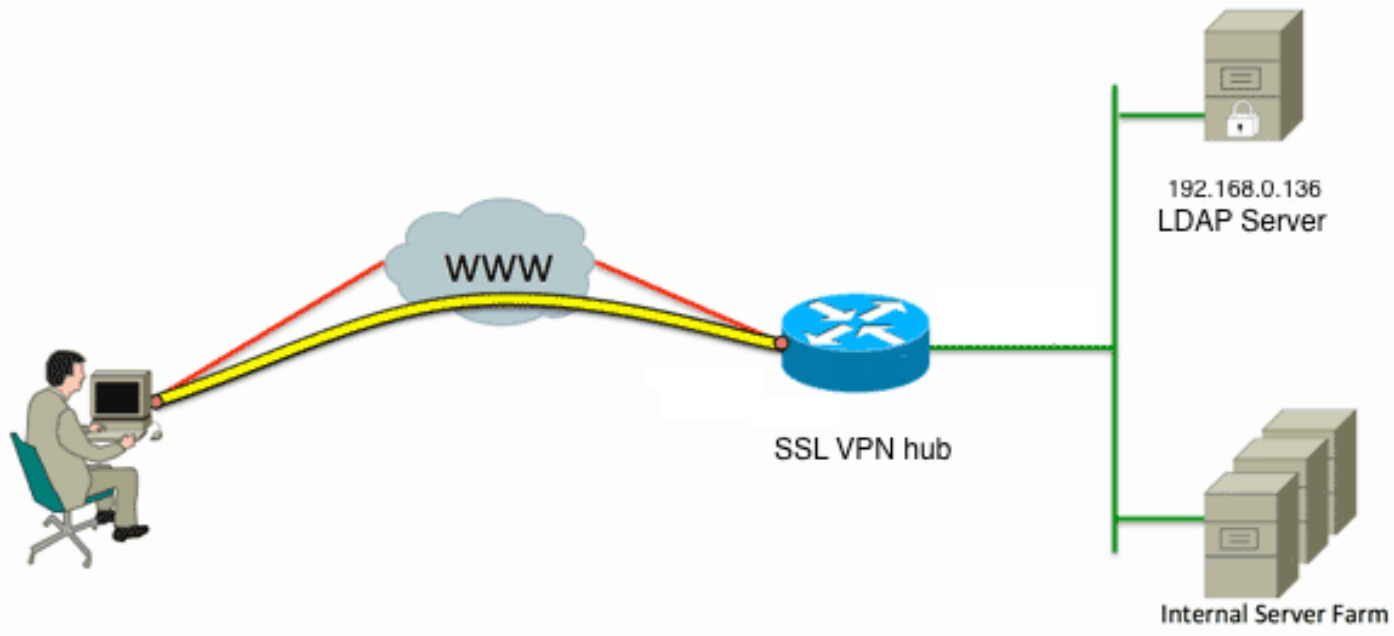
Nome do atributo AAA	Relevância de VPN SSL
user-vpn-group	mapeia para o grupo de políticas definido no contexto WebVPN
contexto de webvpn	mapeia para o próprio contexto WebVPN real

Portanto, o mapa de atributos LDAP precisa mapear o atributo LDAP relevante para um desses dois atributos AAA.

Configurar

Note: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede



Essa configuração usa um mapa de atributos LDAP para mapear o atributo LDAP "memberOf" para o atributo AAA user-vpn-group.

1. Configure o método de autenticação e o 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 um mapa de atributos LDAP.
```
ldap attribute-map ADMAP
 map type memberOf user-vpn-group
```
3. Configure o servidor LDAP que faz referência ao 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 o roteador para atuar como um servidor WebVPN. Neste exemplo, como o atributo "memberOf" será mapeado para o atributo "user-vpn-group", um único contexto WebVPN é configurado com vários grupos de política que incluem uma política "NOACCESS". Este grupo de política é para usuários que não têm um valor "memberOf" correspondente.
```
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
```

Caveats

1. Se o usuário for um "memberOf" de vários grupos, o primeiro valor "memberOf" será usado pelo roteador.
2. O que é estranho nesta configuração é que o nome do grupo de política tem de ser uma correspondência exata para a cadeia **completa** enviada pelo servidor LDAP para o "memberOf value". Geralmente, os administradores usam nomes mais curtos e relevantes para o grupo de políticas, como VPNACCESS, mas, além do problema cosmético, isso pode levar a um problema maior. Não é raro que a string do atributo "memberOf" seja consideravelmente maior do que a usada neste exemplo. Por exemplo, considere esta mensagem de depuração:

```
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
```

Mostra claramente que a cadeia de caracteres recebida do AD é:

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

No entanto, como esse grupo de políticas não está definido, se o administrador tentar configurar tal política de grupo, isso resultará em um erro, pois o Cisco IOS tem um limite no número de caracteres no nome do 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
```

Nessas situações, há duas soluções possíveis:

1. Use um atributo LDAP diferente, como "departamento".Considere este mapa de atributos LDAP:

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

   Nesse caso, o valor do atributo de departamento de um usuário pode ser definido como um valor como VPNACCESS e a configuração da WebVPN é um pouco mais simples:

   ```
   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. Use a palavra-chave DN-to-string no mapa de atributos LDAP.Se a solução alternativa anterior não for adequada, o administrador poderá usar a palavra-chave dn-to-string no mapa de atributos LDAP para extrair apenas o valor de Common Name (CN) da string "memberOf". Neste cenário, o mapa de atributos LDAP seria:

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

   E a configuração da WebVPN seria:

   ```
   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: Ao contrário dos ASAs em que você pode usar o comando **map value** em um mapa de atributo para corresponder o valor recebido do servidor LDAP a algum outro valor localmente significativo, os headends do Cisco IOS não têm essa opção e, portanto, não são tão flexíveis. O bug da Cisco ID CSCts31840 foi arquivado para resolver isso.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

- **show ldap attribute**
- **show ldap server all**

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Note: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug.**

Para solucionar problemas do mapeamento de atributos LDAP, habilite estas depurações:

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