O uso ASA do atributo LDAP traça o exemplo de configuração

Índice

Introdução

Este documento descreve como usar mapas do atributo do Lightweight Directory Access Protocol (LDAP) a fim configurar políticas dinâmicas granuladas de Accesss em uma ferramenta de segurança adaptável (ASA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Secure sockets layer VPN (SSL VPN) no ® do 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
- Cisco IOS Software, software C880 (C880DATA-UNIVERSALK9-M), versão 15.1(4)M, SOFTWARE DE VERSÃO (fc1)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O LDAP é um protocolo do aplicativo aberto, vendedor-neutro, do padrão para indústria para alcançar e manter serviços de informação de diretório distribuídos sobre uma rede IP. Os serviços de diretório jogam um papel importante no desenvolvimento do intranet e dos aplicativos de Internet porque permitem a informação sobre usuários, sistemas, redes, serviços, e aplicativos ser compartilhado durante todo a rede.

Frequentemente, os administradores querem fornecer aos usuários VPN diferentes permissões de acesso ou conteúdo WebVPN. Isto pode ser feito se você configura políticas de VPN diferentes no servidor de VPN e atribui estes política-grupos a cada usuário baseado em suas credenciais. Quando isto puder ser feito manualmente, é mais eficiente para automatizar o processo com serviços de diretório. A fim usar o LDAP para atribuir uma política do grupo a um usuário, você precisa de configurar um mapa que trace um atributo LDAP, tal como o **memberOf do** atributo do diretório ativo (AD), ao atributo da IETF-Raio-**classe** que é compreendido pelo fim de cabeçalho de VPN.

No Cisco IOS, a mesma coisa pode ser conseguida se você configura grupos de política diferentes sob o contexto WebVPN e usa mapas do atributo LDAP a fim determinar que grupo de política o usuário estará atribuído como descrito no documento. Veja a atribuição do grupo de política para os clientes de AnyConnect que usam o LDAP no exemplo de configuração dos finais do cabeçalho do Cisco IOS.

No ASA, isto é conseguido regularmente com a atribuição de políticas diferentes do grupo aos usuários diferentes. Quando a autenticação LDAP está em uso, esta pode ser obtida

automaticamente com um mapa do atributos LDAP. A fim usar o LDAP para atribuir uma política do grupo a um usuário, você deve traçar um atributo LDAP, tal como o **memberOf do** atributo AD ao atributo da Grupo-**política** que é compreendido pelo ASA. O mapeamento do atributo é estabelecido uma vez, você deve traçar o valor de atributo configurado no servidor ldap ao nome de uma política do grupo no ASA.

> Nota: O atributo do **memberOf** corresponde ao grupo que o usuário é um a parte de no diretório ativo. É possível para um usuário ser um membro de mais de um grupo no diretório ativo. Isto faz com que os atributos múltiplos do **memberOf** sejam enviados pelo server, mas o ASA pode somente combinar um atributo a uma política do grupo.

FAQ

Q. Há um limite de configuração no número de LDAP-atributo-mapas para o ASA?

R. Não, lá não é nenhum limite. os LDAP-atributo-mapas são atribuídos dinamicamente durante a sessão de acesso remota VPN que usa a autenticação LDAP/autorização.

Q. Há um limite nos números de atributos que podem ser traçados pelo LDAP-atributo-mapa?

R. Nenhuns limites de configuração.

Q. Há uma limitação em quantos servidores ldap a que um LDAP-atributo-mapa específico pode ser aplicado?

R. Nenhuma limitação. O código LDAP verifica somente que o nome do LDAP-atributo-mapa é válido.

Q. Há umas limitações com LDAP-atributo-mapas e uns atributos muti-avaliados como o memberOf AD?

R. Sim. Aqui, somente o AD é explicado, mas aplica-se a todo o servidor ldap que usar atributos do multi-valor para decisões de política. O ldap-atributo-mapa tem uma limitação com atributos multi-avaliados como o memberOf AD. Se um usuário é um memberOf de diversos grupos AD (que é comum) e o LDAP-atributo-mapa combina mais de um deles, o valor traçado será escolhido baseou no alphabetization das entradas combinadas. Desde que este comportamento não é óbvio ou intuitivo, é importante ter o conhecimento claro sobre como trabalha.

Resumo: Se o mapeamento LDAP conduz aos valores múltiplos para um atributo, o valor de atributo final estará escolhido como segue:

- Primeiramente, selecione os valores com o número o menor de caráteres.
- Se isto conduz a mais de um valor, escolha o valor que é o mais baixo em ordem alfabética.

Use exemplos de caso

O Diretório-LDAP ativo retorna estes exemplos de quatro memberOf para uma autenticação de usuário ou um pedido de autorização:

```
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: Supõe que este LDAP-atributo-mapa está configurado para traçar as grupo-políticas diferentes ASA baseadas no ajuste do 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
```

Neste caso, os fósforos ocorrerão em todos os quatro valores de política do grupo (ASAGroup1 - ASAGroup4). Contudo, a conexão será atribuída à grupo-política ASAGroup1 porque ocorre primeiramente em ordem alfabética.

LDAP-MAP #2: Este LDAP-atributo-mapa é o mesmo, a não ser que o primeiro memberOf não tenha um mapa-valor explícito atribuído (nenhum ASAGroup4). Note que quando não houver nenhum mapa-valor explícito definido, o texto do atributo recebido do LDAP está usado.

```
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 no caso precedente, os fósforos ocorrem em todas as quatro entradas. Neste caso, desde que nenhum valor traçado é fornecido para a entrada APP-SSL-VPN, o valor traçado optará gerentes CN=APP-SSL-VPN, cn=Users, OU=stbu, dc=cisco, dc=com. Desde que CN=APP-SSL-VPN aparece primeiramente na ordem aphabetical, APP-SSL-VPN será selecionado como o valor de política.

Refira a identificação de bug Cisco CSCub64284 para mais informação. Refira PIX/ASA 8.0: Use a autenticação LDAP para atribuir uma política do grupo no início de uma sessão, que mostra um exemplo simples LDAP com memberOf que pôde trabalhar em seu desenvolvimento particular.

Workaround/opções do melhor prática

1. Use a política do acesso dinâmico (o DAP) - O DAP não tem esta limitação de analisar gramaticalmente atributos multi-avaliados (como o memberOf); mas o DAP atualmente não pode ajustar uma grupo-política de dentro dse. Isto significa que a sessão teria que ser segmentada corretamente através dos métodos da associação do grupo de túneis/política. No futuro, o DAP terá a capacidade de ajustar todo o atributo do authorizaiton, incluindo a grupo-política, (identificação de bug Cisco CSCsi54718), assim que a necessidade para um LDAP-atributo-mapa não será exigida por esse motivo eventualmente.

2. Como uma alternativa e se o cenário de distribuição a permite, sempre que você deve usar um LDAP-atributo-mapa para ajustar o atributo de classe, você possíveis poderia igualmente usar um atributo único-avaliado (como o departamento) que representa sua diferenciação do grupo no AD.

   Nota: Em um memberOf DN tal como “CN=Engineering, OU=Office1, dc=cisco, dc=com”, você pode somente fazer a decisão no primeiro DN, que é CN=Engineering, não a unidade organizacional (OU). Há um realce a poder capaz filtrar em todo o campo DN.

Configurar - Prove caixas do uso

Nota: Cada exemplo descrito nesta seção é uma configuração independente, mas pode ser misturado e combinado um com o otro para produzir a política de acesso desejada.

Dica: Os nomes e os valores do atributo são diferenciando maiúsculas e minúsculas. Se o mapeamento não ocorre corretamente, esteja certo que a soletração e a capitalização corretas estiveram usadas no mapa do atributo LDAP para Cisco e valores do atributo LDAP nomes e.

1. Reforço de política dos atributos baseado em usuário

Todo o atributo do padrão LDAP pode ser traçado a um atributo específico do vendedor conhecido do dispositivo (VSA). Uns ou vários atributos LDAP podem ser traçados a uns ou vários atributos de Cisco LDAP. Para uma lista completa de Cisco LDAP VSA, consulte atributos apoiados de Cisco para a autorização LDAP. Este exemplo mostra como reforçar uma bandeira para o usuário1 LDAP. O usuário1 pode ser qualquer tipo do Acesso remoto VPN: IPsec, sem clientes SVC, ou WebVPN. Este exemplo usa as propriedades/general/atributo/campo do escritório para reforçar o Banner1.

Nota: Você poderia usar o atributo/campo do departamento AD para traçar a Cisco a IETF-Raio-classe VSA a fim reforçar políticas de uma grupo-política ASA/PIX. Há uns exemplos deste mais tarde no documento.

O atributo-mapeamento LDAP (para Microsoft AD e Sun) é apoiado até à data da versão 7.1.x PIX/ASA. Todo o atributo Microsoft/AD pode ser traçado a um atributo de Cisco. Está aqui o procedimento para executar isto:

1. No server AD/LDAP:Selecione o usuário1.Clicar com o botão direito **>** **propriedades**.Selecione uma aba para ser usado a fim ajustar um atributo (exemplo. Tab geral).Selecione um campo/atributo, por exemplo o campo do “escritório”, para ser usado a fim reforçar a tempo-escala, e incorpore o texto da bandeira (exemplo, boa vinda ao LDAP!!!!). A configuração do “escritório” no GUI é armazenada no atributo “physicalDeliveryOfficeName” AD/LDAP.

2. No ASA, a fim criar uma tabela de mapeamento do atributo LDAP, trace o atributo

“physicalDeliveryOfficeName” AD/LDAP ao atributo "Banner1" ASA:

```
B200-54(config)# show run ldap
ldap attribute-map Banner
map-name physicalDeliveryOfficeName Banner1
```

3. Associe o mapa do atributo LDAP à entrada do AAA-server:

```
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. Estabeleça a sessão de acesso remota e verifique que a bandeira a “boa vinda ao LDAP!!!!” é apresentado ao usuário VPN.

2. Coloque usuários LDAP em uma Grupo-política específica - Exemplo Genérico

Este exemplo demonstra a autenticação do usuário1 no server AD-LDAP e recupera o valor de campo do departamento assim que pode ser traçado a uma grupo-política ASA/PIX de que as políticas serão reforçadas.

1. No server AD/LDAP:Selecione o usuário1.Clicar com o botão direito **>** **propriedades**.Selecione uma aba para ser usado a fim ajustar um atributo (exemplo. Aba da organização).Selecione um campo/atributo, por exemplo “departamento”, para ser usado a fim reforçar uma grupo-política, e incorpore o valor da grupo-política (Group-Policy1) no ASA/PIX. A configuração do “departamento” no GUI é armazenada no atributo “departamento” AD/LDAP.

2. Defina uma tabela do LDAP-atributo-mapa.

```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department Group-Policy
5520-1(config)#
```

   Nota: Em consequência da aplicação da identificação de bug Cisco CSCsv43552, um atributo novo do LDAP-atributo-mapa, Grupo-política, foi introduzido a fim substituir a IETF-Raio-classe. O CLI na versão ASA 8.2 apoia a palavra-chave da IETF-Raio-classe como uma escolha válida nos comandos do nome de mapa e do mapa-valor a fim ler um arquivo de configuração 8.0 (encenação do upgrade de software). O código adaptável do Security Device Manager (ASDM) tem sido atualizado já para indicar já não a IETF-Raio-classe como uma escolha quando você configura uma entrada de mapa do atributo. Adicionalmente, o ASDM escreverá para fora o atributo da IETF-Raio-classe (se lido dentro de uma configuração 8.0) como o atributo da Grupo-política.

3. Defina a grupo-política Group_policy1 no dispositivo e nos atributos de política exigidos.

4. Estabeleça o túnel de acesso remoto VPN e verifique que a sessão herda os atributos de Group-Policy1 (e alguns outros atributos aplicáveis da grupo-política do padrão).

Nota: Adicionar mais atributos ao mapa como necessário. Este exemplo mostra somente o mínimo para controlar esta função específica (coloque um usuário em uma grupo-política específica ASA/PIX 7.1.x). O terceiro exemplo mostra este tipo de mapa.

Configurar uma Grupo-política NOACCESS

Você pode criar uma grupo-política NOACCESS a fim negar a conexão de VPN quando o usuário não é parte de alguns dos grupos LDAP. Este snippet de configuração é mostrado para sua referência:

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

Você deve aplicar esta política do grupo como uma política do grupo padrão ao grupo de túneis. Isto permite os usuários que obtêm um mapeamento do mapa do atributo LDAP, por exemplo aqueles que pertencem a um grupo desejado LDAP, para obter suas políticas desejadas do grupo e os usuários que não obtêm nenhum mapeamento, por exemplo aqueles que não pertencem a alguns dos grupos desejados LDAP, para obter a grupo-política NOACCESS do grupo de túneis, que obstrui o acesso para eles.

Dica: Desde que o atributo dos VPN-simultâneo-inícios de uma sessão é ajustado a 0 aqui, deve explicitamente ser definido em todas as grupo-políticas restantes também; se não, será herdado da grupo-política do padrão para esse grupo de túneis, que é neste caso a política NOACCESS.

3. Reforço de política Grupo-baseado dos atributos - Exemplo

Nota: A aplicação/reparo da identificação de bug Cisco CSCse08736 é exigida, assim que o ASA deve executar pelo menos a versão 7.2.2.

1. No server AD-LDAP, os usuários e os computadores de diretório ativo, estabelecem um registro de usuário (VPNUserGroup) que representasse um grupo onde os atributos VPN fossem configurados.

2. No server AD-LDAP, os usuários e os computadores de diretório ativo, definem cada campo do departamento de registro de usuário para apontar ao registro de grupo (VPNUserGroup) em etapa 1. O nome de usuário neste exemplo é **web1**.

   Nota: O atributo do departamento AD foi usado somente porque logicamente o “departamento” refere a grupo-política. Na realidade, todo o campo podia ser usado. A exigência é que este campo tem que traçar à Grupo-política do atributo de Cisco VPN segundo as indicações deste exemplo.

3. Defina uma tabela do 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)#
```

A descrição e o escritório de dois atributos AD-LDAP (representados pela descrição e pelo PhysicalDeliveryOfficeName dos nomes AD) são os atributos do registro de grupo (para VPNUSerGroup) que os mapas a Cisco VPN atribuem Banner1 e IETF-Raio-Sessão-intervalo.

O atributo do departamento é para que o registro de usuário trace ao nome da grupo-política externo no ASA (VPNUSer), que traça então de volta ao registro de VPNuserGroup no server AD-LDAP, onde os atributos são definidos.

Nota: Cisco atribui (Grupo-política) deve ser definido no LDAP-atributo-mapa. Seu AD-atributo traçado pode ser todo o atributo settable AD. Este exemplo usa o departamento porque é a maioria de nome lógico que refere a grupo-política.

4. Configurar o AAA-server com o nome do LDAP-atributo-mapa a ser usado para operações da autenticação LDAP, da autorização, e da contabilidade (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 um grupo de túneis com com autenticação LDAP ou autorização LDAP.

Exemplo com autenticação LDAP. Executa a autenticação + reforço de política do atributo (da autorização) se os atributos são definidos.

```
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)#Exemplo com autorização LDAP. Configuração usada usando Certificados digitais.

```
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 uma grupo-política externo. O nome da grupo-política é o valor do registro de usuário AD-LDAP que representa o grupo (VPNUserGroup).

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

7. Estabeleça o túnel e verifique que os atributos estão reforçados. Neste caso, a bandeira e o Sessão-intervalo são reforçados do registro de VPNuserGroup no AD.

4. A aplicação do diretório ativo de “atribui um endereço IP estático” para o IPsec e os túneis SVC

O atributo AD é msRADIUSFramedIPAddress. O atributo é configurado em propriedades de usuário AD, guia de discagem de entrada, “atribui um endereço IP estático”.

Aqui estão as etapas:

1. No server AD, sob propriedades de usuário, o guia de discagem de entrada, “atribui um endereço IP estático”, incorpora o valor do endereço IP de Um ou Mais Servidores Cisco ICM NT a fim atribuir à sessão IPsec/SVC (10.20.30.6).

2. No ASA crie um LDAP-atributo-mapa com este mapeamento:

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

3. No ASA, verifique que o VPN-endereço-assigment está configurado para incluir o “VPN-ADDR-atribuir-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. Estabeleça as sessões remotas da autoridade IPsec/SVC (RA) e verifique com da “o telecontrole mostra VPN-sessiondb|svc” que campo “do IP atribuído o” está correto (10.20.30.6).

5. A aplicação do diretório ativo da “do discado permissão de acesso remoto, permite/nega o acesso”

Apoia todas as sessões remotas VPN Acccess: IPsec, WebVPN, e SVC. Permita o acesso tem um valor de VERDADEIRO. Negue Acccess tem um valor de FALSO. O nome do atributo AD é msNPAllowDialin.

Este exemplo demonstra a criação de um LDAP-atributo-mapa que use os protocolos de tunelamento de Cisco para criar permita o acesso (VERDADEIRO) e nega circunstâncias

(FALSAS). Por exemplo, se você traça o IPsec tunnel-protocol=L2TPover (8), você pode criar uma condição FALSA se você tenta reforçar o acesso para o WebVPN e o IPsec. A lógica reversa aplica-se demasiado.

Aqui estão as etapas:

1. Nas propriedades do usuário1 do server AD, o discado, seleciona o apropriado permite o acesso ou nega o acesso para cada usuário.

   Nota: Se você seleciona a terceira opção do “acesso controle com a política de acesso remoto,” nenhum valor está retornado do server AD, assim as permissões que são reforçadas são baseadas no ajuste das grupo-políticas internas ASA/PIX.

2. No ASA, crie um LDAP-atributo-mapa com este mapeamento:

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

   Nota: Adicionar mais atributos ao mapa como necessário. Este exemplo mostra somente o mínimo para controlar esta função específica (permita ou negue o acesso baseado no ajuste do discado).

   Que o LDAP-atributo-mapa significa ou reforça?

   msNPAllowDialin 8 FALSOS do mapa-valor

   Negue o acesso para um usuário1. A condição FALSA do valor traça ao protocolo de túnel L2TPoverIPsec, (valor 8).

   Permita o acesso para user2. A condição do valor verdadeiro traça ao protocolo de túnel WebVPN + IPsec, (valor 20).

   Um WebVPN/usuário de IPsec, authenticaticated como o usuário1 no AD, falharia devido à má combinação do protocolo de túnel.

   Um L2TPoverIPsec, authenticaticated como o usuário1 no AD, falharia devido à regra da negação.

   Um WebVPN/usuário de IPsec, authenticaticated como user2 no AD, sucederia (permita a regra + protocolo de túnel combinado).

   Um L2TPoverIPsec, authenticaticated como user2 no AD, falharia devido à má combinação do protocolo de túnel.
   Apoio para o protocolo de túnel, como definido no RFCs 2867 e em 2868.

6. Aplicação do diretório ativo do “membro” da sociedade /Group para permitir ou

negar o acesso

Este caso é estreitamente relacionado encaixotar 5, prevê um fluxo mais lógico, e é o método recomendada, desde que estabelece a verificação da membrasia do clube como uma circunstância.

1. Configurar o usuário AD para ser “membro” de um grupo específico. Use um nome que o coloque na parte superior da grupo-hierarquia (ASA-VPN-consultantes). Em AD-LDAP, a membrasia do clube é definida pelo atributo “memberOf” AD.

   É importante que o grupo esteja na parte superior da lista, desde que você pode atualmente somente aplicar as regras à primeira corda do “memberOf” do grupo. Na liberação 7.3, você poderá executar a filtração e a aplicação do grupo múltiplo.
2. No ASA, crie um LDAP-atributo-mapa com o o mapeamento mínimo:

   ```
   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: Adicionar mais atributos ao mapa como necessário. Este os exemplos mostram somente o mínimo para controlar esta função específica (permita ou negue o acesso baseado na membrasia do clube).

   Que o LDAP-atributo-mapa significa ou reforça?

   User=joe_consultant, parte do AD, que é membro do grupo “ASA-VPN-consultantes” AD estará permitido o acesso somente se o usuário usa o IPsec (tunnel-protocol=4=IPSec).

   User=joe_consultant, parte de AD, falhará o acesso VPN durante todo o outro cliente de acesso remoto (PPTP/L2TP, L2TP/IPSec, WebVPN/SVC, e assim por diante).

   User=bill_the_hacker não será permitido dentro desde que o usuário não tem nenhuma sociedade AD.

7. A aplicação do diretório ativo do “de horas fazer logon/hora ordena”

Este caso do uso descreve como estabelecer e reforçar as regras do Time Of Day em AD/LDAP.

Está aqui o procedimento para fazer isto:

1. No server AD/LDAP:Selecione o usuário.Clicar com o botão direito **> propriedades**.Selecione uma aba para ser usado a fim ajustar um atributo (exemplo. Tab geral).Selecione um campo/atributo, por exemplo o campo do “escritório”, para ser usado a fim reforçar a tempo-escala, e dê entrada com o nome da tempo-escala (por exemplo, Boston). A configuração do “escritório” no GUI é armazenada no atributo “physicalDeliveryOfficeName” AD/LDAP.

2. No ASA

Crie uma tabela de mapeamento do atributo LDAP.Trace o atributo “physicalDeliveryOfficeName” AD/LDAP ao atributo “horas do acesso” ASA.

Exemplo:

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

3. No ASA, associe o mapa do atributo LDAP à entrada do AAA-server:

```
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. No ASA, crie um objeto da tempo-escala que tenha o valor do nome que é atribuído ao usuário (valor do escritório em etapa 1):`B200-54(config-time-range)# show runn time-range`

```
!
time-range Boston
periodic weekdays 8:00 to 17:00
!
```

5. Estabeleça a sessão de acesso remota VPN:

   A sessão deve suceder se dentro da tempo-escala.A sessão deve falhar se fora da tempo-escala.

8. Use a configuração do LDAP-mapa para traçar um usuário em uma Grupo-política específica e para usar o comando do autorização-server-grupo, no caso da Autenticação dupla

1. Nesta encenação, a Autenticação dupla é usada. O primeiro Authentication Server usado é RAIO e a segunda autenticação separa usado é um servidor ldap.

   Configurar o servidor ldap assim como o servidor Radius. Aqui está um exemplo:

```
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 o mapa de atributos LDAP. Aqui está um exemplo:

```
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 o grupo de túneis e associe o RAIO e o servidor ldap para a autenticação. Aqui está um exemplo:

```
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
```

Veja a grupo-política que é usada na configuração do grupo de túneis:

```
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
```

Com esta configuração, os usuários de AnyConnect que foram traçados corretamente com o uso de atributos LDAP não foram colocados na grupo-política, Teste-política-Safenet. Em lugar de, foram colocados ainda na grupo-política do padrão, neste caso NoAccess.

Veja que o snippet do debuga (debugar o ldap 255) e Syslog em informativo nivelado:

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

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.
```

A falha da mostra destes Syslog como o usuário era dada a grupo-política de NoAccess que teve o simultâneo-início de uma sessão ajustado a 0 mesmo que os Syslog dissessem que recuperou uma grupo-política do específico do usuário.

A fim ter o usuário atribuído na grupo-política, com base no LDAP-mapa, você deve ter este comando: **autorização-server-grupo teste-LDAP** (neste caso, o teste-**LDAP** é o nome de servidor ldap). Aqui está um exemplo:

```
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. Agora, se o primeiro Authentication Server (RAIO, neste exemplo) enviou os atributos específicas de usuário, por exemplo o atributo da IEFT-classe, nesse caso, o usuário será traçado à grupo-política enviada pelo RAIO. Assim mesmo que o servidor secundário tenha um mapa LDAP configurado e os atributos LDAP do usuário tracem o usuário a uma grupo-política diferente, a grupo-política enviada pelo primeiro Authentication Server será reforçada.

   A fim ter o usuário coloque em uma grupo-política baseada no atributo do mapa LDAP, você deve especificar este comando sob o grupo de túneis: **autorização-server-grupo teste-LDAP**.

3. Se o primeiro Authentication Server é o SDI ou o OTP, que não podem passar o atributo específica de usuário, a seguir o usuário cairia na grupo-política do padrão do grupo de túneis. Neste caso, NoAccess mesmo que o mapeamento LDAP esteja correto.

   Neste caso, você igualmente precisaria o comando, o autorização-server-**grupo teste-LDAP**, sob o grupo de túneis para que o usuário seja colocado na grupo-política correta.

4. Se ambos os server são o mesmos RAIO ou servidores ldap, a seguir você não precisa o comando do autorização-server-**grupo** para que o fechamento da grupo-política trabalhe.

Verificar

```
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 seção para fazer o troubleshooting da sua configuração.

Debugar a transação LDAP

Estes debugam podem ser usados a fim ajudar a isolar edições com a configuração DAP:

- **debugar o ldap 255**
- **debugar o traço do dap**
- **debug aaa authentication**

O ASA não pode autenticar usuários do servidor ldap

Caso que o ASA não pode autenticar os usuários do LDAP servem, são aqui alguma amostra debugam:

```
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
```

Destes debuga, ou o formato do início de uma sessão DN LDAP está incorreto ou a senha está

incorreta assim que verifique ambos a fim resolver a edição.