Exemplo de Configuração de ASA Anyconnect VPN e OpenLDAP Authorization com Esquema Personalizado e Certificados

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Configurar](#)
[Configuração básica do OpenLDAP](#)
[Esquema Openldap Personalizado](#)
[Configuração do ASA](#)
[Verificar](#)
[Testar acesso VPN](#)
[Debugs](#)
[Autenticação e autorização separados do ASA](#)
[Atributos ASA do LDAP e do grupo local](#)
[ASA e LDAP com autenticação de certificado](#)
[Debugs](#)
[Autenticação secundária](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar o OpenLDAP com esquema personalizado para suportar atributos por usuário para o Cisco Anyconnect Secure Mobility Client que se conecta a um Cisco Adaptive Security Appliance (ASA). A configuração do ASA é bem básica, pois todos os atributos do usuário são recuperados do servidor OpenLDAP. Também são descritas neste documento as diferenças na autenticação e autorização LDAP quando usadas juntamente com os certificados.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico sobre a configuração do Linux
- Conhecimento básico sobre a configuração do ASA CLI

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Cisco ASA versão 8.4 e posterior
- OpenLDAP versão 2.4.30

Configurar

Configuração básica do OpenLDAP

Etapa 1. Configure o servidor.

Este exemplo usa a árvore ldap test-cisco.com.

O arquivo ldap.conf é usado para definir padrões de nível de sistema que podem ser usados pelo cliente ldap local.

Note: Embora você não seja obrigado a configurar padrões no nível do sistema, eles podem ajudar a testar e solucionar problemas do servidor quando você executa um cliente ldap local.

/etc/openldap/ldap.conf:

```
BASE   dc=test-cisco,dc=com
```

o arquivo slapd.conf é usado para a configuração do servidor OpenLDAP. Os arquivos de esquema padrão incluem definições LDAP amplamente usadas. Por exemplo, a *pessoa* do nome da classe de objeto é definida no arquivo core.schema. Essa configuração usa esse esquema comum e define seu próprio esquema para atributos específicos da Cisco.

/etc/openldap/slapd.conf:

```
include         /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/openldap.schema
include /etc/openldap/schema/nis.schema

# Defines backend database type and redirects all # queries with specified suffix to that
database
database hdb
suffix "dc=test-cisco,dc=com"
checkpoint 32 30

# Rootdn will be used to perform all administrative tasks.
rootdn          "cn=Manager,dc=test-cisco,dc=com"

# Cleartext passwords, especially for the rootdn, should be avoid.
rootpw          secret

directory /var/lib/openldap-data
index objectClass eq
```

Etapa 2. Verifique a configuração LDAP.

Para verificar se o OpenLDAP básico funciona, execute esta configuração:

```
pluton openldap # /etc/init.d/slapd start
* Starting ldap-server [ ok ]
pluton openldap # ps ax | grep openldap
27562 ? Ssl 0:00 /usr/lib64/openldap/slapd -u ldap -g ldap -f
/etc/openldap/slapd.conf -h ldaps:// ldap:// ldapi://var/run/openldap/slapd.sock

pluton openldap # netstat -atcpn | grep slapd
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 0.0.0.0:636 0.0.0.0:* LISTEN 27562/slapd
tcp 0 0 0.0.0.0:389 0.0.0.0:* LISTEN 27562/slapd

pluton # ldapsearch -h 192.168.10.1 -D "CN=Manager,DC=test-cisco,DC=com" -w secret
# extended LDIF
#
# LDAPv3
# base <dc=test-cisco,dc=com> (default) with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# search result
search: 2
result: 32 No such object

# numResponses: 1
```

Etapa 3. Adicione registros ao banco de dados.

Depois de testar e configurar tudo corretamente, adicione registros ao banco de dados. Para adicionar contêineres básicos para usuários e grupos, execute esta configuração:

```
pluton # cat root.ldiff
dn: dc=test-cisco,dc=com
objectclass: dcObject
objectclass: organization
o: test-cisco.com
dc: test-cisco

dn: ou=People,dc=test-cisco,dc=com
objectClass: organizationalUnit
objectClass: top
ou: People

dn: ou=Groups,dc=test-cisco,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Groups

pluton # ldapadd -h 192.168.10.1 -D "CN=Manager,DC=test-cisco,DC=com"
-w secret -x -f root.ldiff
adding new entry "dc=test-cisco,dc=com"
adding new entry "ou=People,dc=test-cisco,dc=com"
adding new entry "ou=Groups,dc=test-cisco,dc=com"

pluton # ldapsearch -h 192.168.10.1 -D "CN=Manager,DC=test-cisco,DC=com" -w secret
# extended LDIF
#
# LDAPv3
# base <dc=test-cisco,dc=com> (default) with scope subtree
# filter: (objectclass=*)
```

```
# requesting: ALL
#

# test-cisco.com
dn: dc=test-cisco,dc=com
objectClass: dcObject
objectClass: organization
o: test-cisco.com
dc: test-cisco

# People, test-cisco.com
dn: ou=People,dc=test-cisco,dc=com
objectClass: organizationalUnit
objectClass: top
ou: People

# Groups, test-cisco.com
dn: ou=Groups,dc=test-cisco,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Groups

# search result
search: 2
result: 0 Success

# numResponses: 4
# numEntries: 3
```

Esquema Openldap Personalizado

Agora que a configuração básica funciona, você pode adicionar um esquema personalizado. Neste exemplo de configuração, um novo tipo de classe de objeto chamada *CiscoPerson* é criado e esses atributos são criados e usados nesta classe de objeto:

- CiscoBanner
- CiscoACLin
- CiscoDomain
- CiscoDNS
- EndereçoIPdaCisco
- máscaraIPNCisco
- CiscoSplitACL
- CiscoSplitTunnelPolicy
- PolíticaGrupoCisco

Etapa 1. Crie o novo esquema em cisco.schema.

```
pluton openldap # pwd
/etc/openldap
pluton openldap # cat schema/cisco.schema

attributetype ( 1.3.6.1.4.1.9.500.1.1
 NAME 'CiscoBanner'
 DESC 'Banner Name for VPN users'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 ORDERING caseIgnoreOrderingMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128}
 SINGLE-VALUE )
```

```
attributetype ( 1.3.6.1.4.1.9.500.1.2
 NAME 'CiscoACLin'
 DESC 'ACL in for VPN users'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 ORDERING caseIgnoreOrderingMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128}
 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.9.500.1.3
 NAME 'CiscoDomain'
 DESC 'Domain for VPN users'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 ORDERING caseIgnoreOrderingMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128}
 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.9.500.1.4
 NAME 'CiscoDNS'
 DESC 'DNS server for VPN users'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 ORDERING caseIgnoreOrderingMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128}
 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.9.500.1.5
 NAME 'CiscoIPAddress'
 DESC 'Address for VPN user'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 ORDERING caseIgnoreOrderingMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128}
 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.9.500.1.6
 NAME 'CiscoIPNetmask'
 DESC 'Address for VPN user'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 ORDERING caseIgnoreOrderingMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128}
 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.9.500.1.7
 NAME 'CiscoSplitACL'
 DESC 'Split tunnel list for VPN users'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 ORDERING caseIgnoreOrderingMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128}
 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.9.500.1.8
 NAME 'CiscoSplitTunnelPolicy'
 DESC 'Split tunnel policy for VPN users'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 ORDERING caseIgnoreOrderingMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128}
 SINGLE-VALUE )
```

```
attributetype ( 1.3.6.1.4.1.9.500.1.9
 NAME 'CiscoGroupPolicy'
 DESC 'Group policy for VPN users'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 ORDERING caseIgnoreOrderingMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128}
 SINGLE-VALUE )

objectclass ( 1.3.6.1.4.1.9.500.2.1 NAME 'CiscoPerson'
       DESC 'My cisco person'
       AUXILIARY
       MUST ( sn $ cn )
       MAY ( userPassword $ telephoneNumber $ seeAlso
$ description $ CiscoBanner $ CiscoACLin $ CiscoDomain
$ CiscoDNS $ CiscoIPAddress $ CiscoIPNetmask $ CiscoSplitACL
$ CiscoSplitTunnelPolicy $ CiscoGroupPolicy ) )
```

Notas importantes

- Use OIDs corporativas privadas para sua empresa. Qualquer OID funciona, mas a melhor prática é usar os OIDs atribuídos pela IANA. O configurado neste exemplo começa em 1.3.6.1.4.1.9 (reservado pela Cisco: http://www.iana.org/assignments/enterprise-numbers).
- A seguinte parte do OID (500.1.1-500.1.9) foi usada para não interferir diretamente na árvore principal do OID da Cisco ("1.3.6.1.4.1.9").
- Este banco de dados usa a classe de objeto *Pessoa* definida em schema/core.ldif. Esse objeto é do tipo TOP e os registros podem incluir apenas um desses atributos (por isso a classe de objeto *CiscoPerson* é do tipo Auxiliar).
- A classe de objeto chamada *CiscoPerson* deve incluir SN ou CN e pode incluir qualquer um dos atributos personalizados da Cisco definidos anteriormente. Observe que também pode incluir quaisquer outros atributos definidos em outros esquemas (como *userPassword* ou *phoneNumber*).
- Lembre-se de que cada objeto deve ter um número OID diferente.
- Os atributos personalizados não diferenciam maiúsculas de minúsculas e do tipo de *string* com codificação UTF-8 e máximo de 128 caracteres (definido pela SYNTAX).

Etapa 2. Inclua o esquema em sldap.conf.

```
pluton openldap # cat slapd.conf | grep include
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/openldap.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/cisco.schema
```

Etapa 3. Reiniciar Serviços.

```
puton openldap # /etc/init.d/slapd restart
 * Stopping ldap-server                              [ ok ]
 * Starting ldap-server                              [ ok ]
```

Etapa 4. Adicione um novo usuário com todos os atributos personalizados.

Neste exemplo, o usuário pertence a vários objetos objectClass e herda atributos de todos eles.

Com esse processo, é fácil adicionar um esquema ou atributos adicionais sem alterações nos registros de banco de dados existentes.

```
pluton # cat users.ldiff
# User account
dn: uid=cisco,ou=people,dc=test-cisco,dc=com
cn: John Smith
givenName: John
sn: cisco
uid: cisco
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/cisco
mail: jsmith@dev.local
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: CiscoPerson
loginShell: /bin/bash
userPassword: {CRYPT}*
CiscoBanner: This is banner 1
CiscoIPAddress: 10.1.1.1
CiscoIPNetmask: 255.255.255.128
CiscoDomain: domain1.com
CiscoDNS: 10.6.6.6
CiscoACLin: ip:inacl#1=permit ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0
CiscoSplitACL: ACL1
CiscoSplitTunnelPolicy: 1
CiscoGroupPolicy: POLICY1

pluton # ldapadd -h 192.168.10.1 -D "CN=Manager,DC=test-cisco,DC=com"
-w secret -x -f users.ldiff
adding new entry "uid=cisco,ou=people,dc=test-cisco,dc=com"
```

Etapa 5. Defina a senha para o usuário.

```
pluton moje # ldappasswd -h 192.168.10.1 -D "CN=Manager,DC=test-cisco,DC=com"
-w secret -x uid=cisco,ou=people,dc=test-cisco,dc=com -s pass1
```

Etapa 6. Verificar a configuração.

```
pluton # ldapsearch -h 192.168.10.1 -D "CN=Manager,DC=test-cisco,DC=com"
-w secret -b uid=cisco,ou=people,dc=test-cisco,dc=com
# extended LDIF
#
# LDAPv3
# base <uid=cisco,ou=people,dc=test-cisco,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# cisco, People, test-cisco.com
dn: uid=cisco,ou=People,dc=test-cisco,dc=com
cn: John Smith
givenName: John
sn: cisco
uid: cisco
```

```
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/cisco
mail: jsmith@dev.local
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: CiscoPerson
loginShell: /bin/bash
userPassword:: e0NSWVBUfSo=
CiscoBanner: This is banner 1
CiscoIPAddress: 10.1.1.1
CiscoIPNetmask: 255.255.255.128
CiscoDomain: domain1.com
CiscoDNS: 10.6.6.6
CiscoACLin: ip:inacl#1=permit ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.
 0
CiscoSplitACL: ACL1
CiscoSplitTunnelPolicy: 1
CiscoGroupPolicy: POLICY1
userPassword:: e1NTSEF9NXM4MUZtaS85YUcvV2ZQU3kzbEdtdzFPUkk0bHl3V0M=

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Configuração do ASA

Etapa 1. Configure a interface e o certificado.

```
interface GigabitEthernet0
 nameif inside
 security-level 100
 ip address 192.168.11.250 255.255.255.0
!
interface GigabitEthernet1
 nameif outside
 security-level 0
 ip address 192.168.1.250 255.255.255.0

crypto ca trustpoint CA
 keypair CA
 crl configure
crypto ca certificate chain CA
 certificate ca 00cf946de20d0ce6d9
   30820223 3082018c 020900cf 946de20d 0ce6d930 0d06092a 864886f7 0d010105
   05003056 310b3009 06035504 06130250 4c310c30 0a060355 04080c03 4d617a31
   0f300d06 03550407 0c065761 72736177 310c300a 06035504 0a0c0354 4143310c
   300a0603 55040b0c 03524143 310c300a 06035504 030c0354 4143301e 170d3132
   31313136 30383131 32365a17 0d313331 31313630 38313132 365a3056 310b3009
   06035504 06130250 4c310c30 0a060355 04080c03 4d617a31 0f300d06 03550407
   0c065761 72736177 310c300a 06035504 0a0c0354 4143310c 300a0603 55040b0c
   03524143 310c300a 06035504 030c0354 41433081 9f300d06 092a8648 86f70d01
   01010500 03818d00 30818902 818100d0 68af1ef6 9b256071 d39c8d25 4fb9f391
   5a96e8e0 1ac424d5 fc9cf460 f09e181e f1487525 d982f3ae 29384ca8 13d5290d
   a360e796 0224dce5 ffc0767e 6f54b991 967b54a4 4b3aa59e c2a69310 550029fb
```

```
   cb1c3f45 3fb15d15 0d507b09 52b02a17 6189d591 87d42617 1d93b683 4d685005
   34788fd0 2a899ca4 926e7318 1f914102 03010001 300d0609 2a864886 f70d0101
   05050003 81810046 8c58cddb dfd6932b 9260af40 ebc63465 1f18a374 f5b7865c
   a21b22f3 a07ebf57 d64312b7 57543c91 edc4088d 3c7b3c75 e3f29b8d b7e04e01
   4dc2cb89 6935e07c 3518ad97 96e50aae 52e89265 92bb1aad a85656dc 931e2006
   af4042a0 09826d29 88ca972e 5442e0c3 8c957978 4a15e5d9 cac5a12c b0604df4
   97438706 c973a5
 quit
 certificate 00fe9c3d61e131cd9e
   30820225 3082018e 020900fe 9c3d61e1 31cd9e30 0d06092a 864886f7 0d010105
   05003056 310b3009 06035504 06130250 4c310c30 0a060355 04080c03 4d617a31
   0f300d06 03550407 0c065761 72736177 310c300a 06035504 0a0c0354 4143310c
   300a0603 55040b0c 03524143 310c300a 06035504 030c0354 4143301e 170d3132
   31313136 31303336 31325a17 0d313331 31313631 30333631 325a3058 310b3009
   06035504 06130250 4c310c30 0a060355 04080c03 4d617a31 11300f06 03550407
   0c085761 72737a61 7761310c 300a0603 55040a0c 03414353 310c300a 06035504
   0b0c0341 4353310c 300a0603 5504030c 03414353 30819f30 0d06092a 864886f7
   0d010101 05000381 8d003081 89028181 00d15ee2 0f14597a 0703204b 22a2c5cc
   34c0967e 74bb087c b16bc462 d1e4f99d 3d40bd19 5b80845e 08f2cccb e2ca0d01
   aa6fe4f4 df287598 45956110 d3c66465 668ae4d2 8a9583e8 7a652685 19b25dfa
   fce7b84e e1780dd0 1cd3d71e 0926db1a 74354b11 c5b976e0 07e7dd01 0b4115f0
   662874c3 2ed5f87e 170b3baa f266f650 2f020301 0001300d 06092a86 4886f70d
   01010505 00038181 00987d8e acfa9cac ab9dbb52 5bb61992 975e4bbe e9c28426
   1dc3dd1e 87abd839 fa3a937d b1aebcc4 fdc549a2 010b83f3 aa0e12b3 f03a4f49
   d8e6fdea 61776ae5 17daf7e4 6baf810d 37c24784 bd71429b dc0494c0 84a020ff
   1be0c903 a055f634 1e29b6ea 7d7f3280 f161a86c 50d40b6c c24bc8b0 493c0918
   8a185e05 1b52d8b0 0e
 quit
```

Etapa 2. Gerar um certificado autoassinado.

```
crypto ca trustpoint CA
enrollment self
crypto ca enroll CA
```

Etapa 3. Ative o WebVPN na interface externa.

```
ssl trust-point CA
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.01065-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
```

Etapa 4. Divida a configuração da ACL.

O nome da ACL é retornado pelo OpenLDAP:

```
access-list ACL1 standard permit 10.7.7.0 255.255.255.0
```

Etapa 5. Crie um nome de grupo de túnel que use a política de grupo padrão (DfltAccessPolicy).

Os usuários com o atributo LDAP específico (*CiscoGroupPolicy*) são mapeados para outra política: POLÍTICA1

```
group-policy DfltAccessPolicy internal
group-policy DfltAccessPolicy attributes
```

```
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless

group-policy POLICY1 internal
group-policy POLICY1 attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless

tunnel-group RA type remote-access
tunnel-group RA general-attributes
tunnel-group RA webvpn-attributes
 group-alias RA enable
 without-csd
```

A configuração do servidor Aaa do ASA usa o mapa de atributos ldap para mapear de atributos retornados pelo OpenLDAP para atributos que podem ser interpretados pelo ASA para usuários do Anyconnect.

```
ldap attribute-map LDAP-MAP
 map-name  CiscoACLin Cisco-AV-Pair
 map-name  CiscoBanner Banner1
 map-name  CiscoDNS Primary-DNS
 map-name  CiscoDomain IPSec-Default-Domain
 map-name  CiscoGroupPolicy IETF-Radius-Class
 map-name  CiscoIPAddress IETF-Radius-Framed-IP-Address
 map-name  CiscoIPNetmask IETF-Radius-Framed-IP-Netmask
 map-name  CiscoSplitACL IPSec-Split-Tunnel-List
 map-name  CiscoSplitTunnelPolicy IPSec-Split-Tunneling-Policy

aaa-server LDAP protocol ldap
aaa-server LDAP (inside) host 192.168.11.10
 ldap-base-dn DC=test-cisco,DC=com
 ldap-scope subtree
 ldap-naming-attribute uid
 ldap-login-password secret
 ldap-login-dn CN=Manager,DC=test-cisco,DC=com
 server-type openldap
 ldap-attribute-map LDAP-MA
```

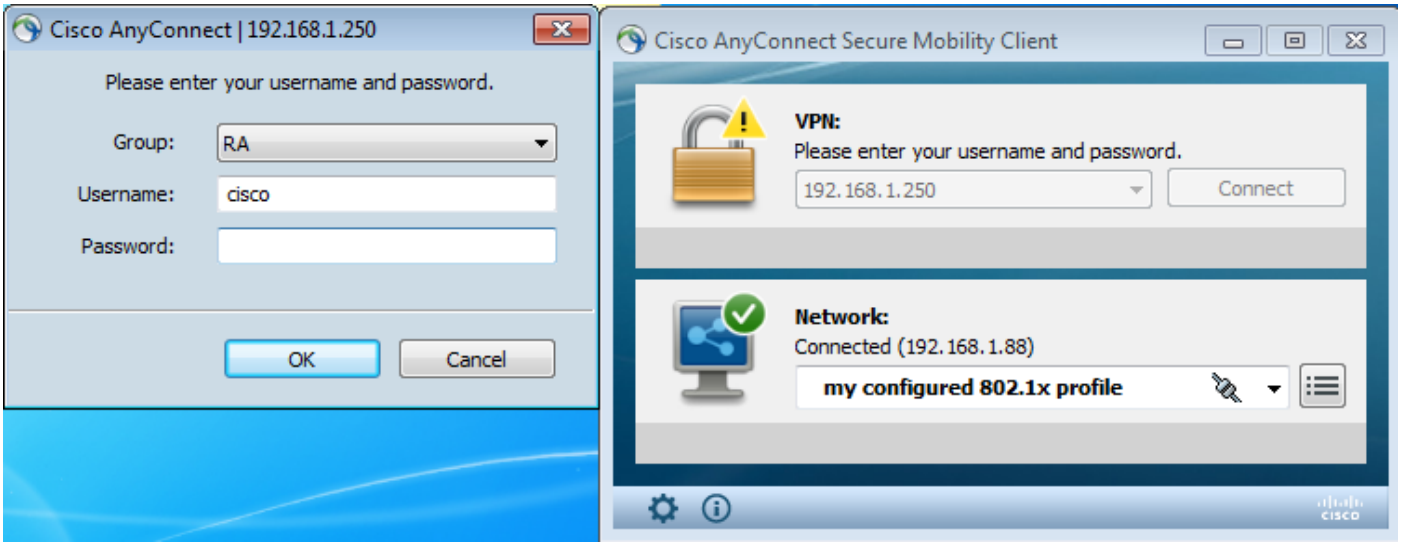
Etapa 6. Ative o servidor LDAP para autenticação para o grupo de túneis especificado.

```
tunnel-group RA general-attributes
 authentication-server-group LDAP
```

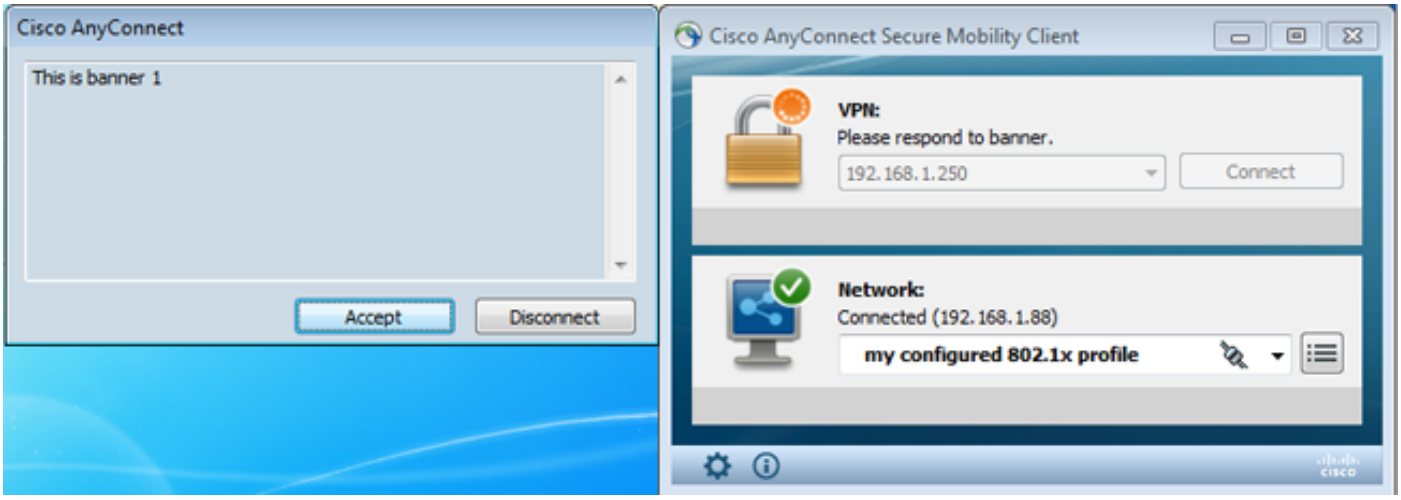
Verificar

Testar acesso VPN

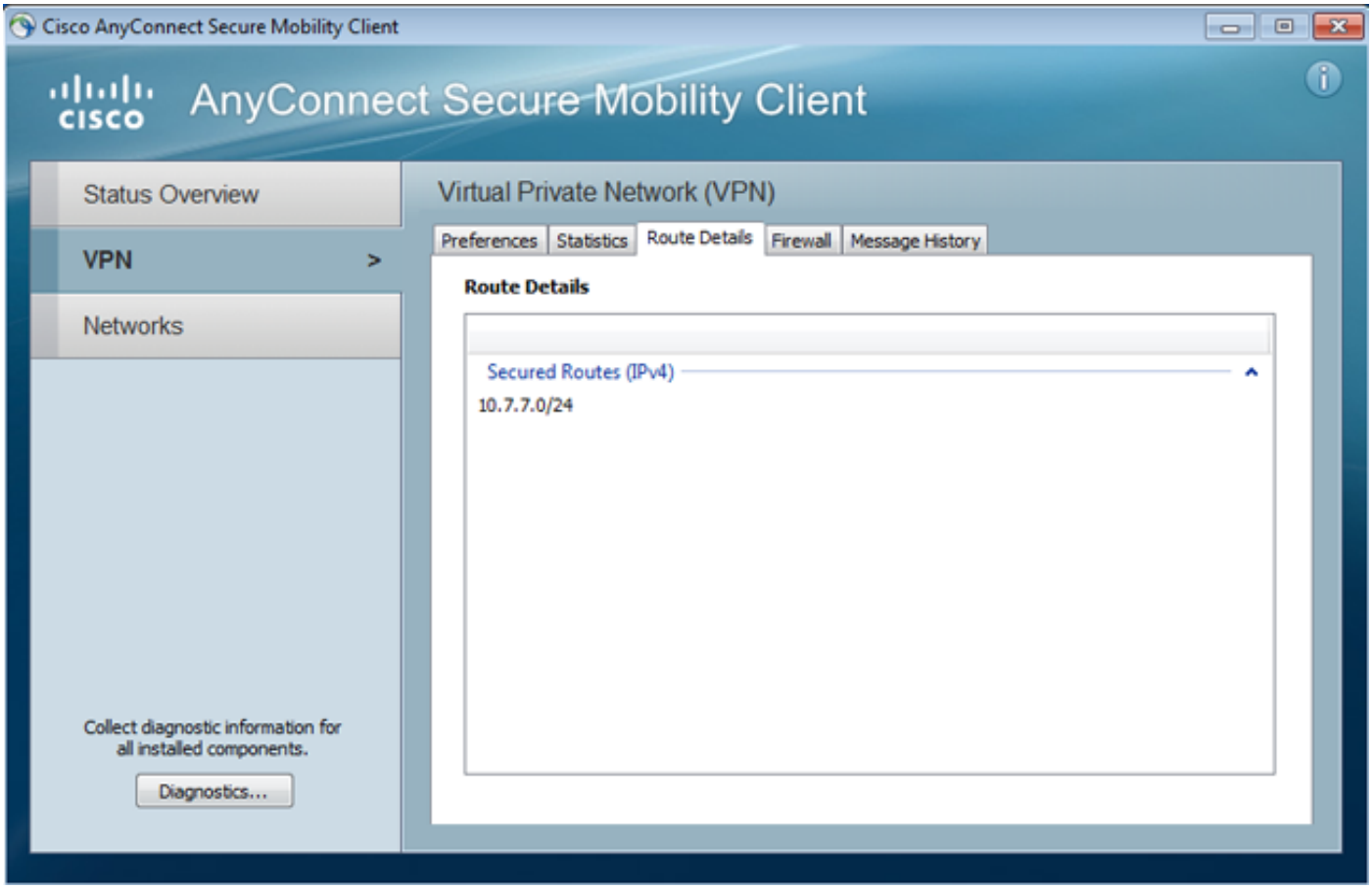
O Anyconnect está configurado para se conectar a 192.168.1.250. O login é nome de usuário *cisco* e senha *pass1*.



Após a autenticação, o banner correto é usado.



A ACL dividida correta é enviada (ACL1 definida no ASA).



A interface do Anyconnect é configurada com IP: 10.1.1.1 e máscara de rede 255.255.255.128. O domínio é domain1.com e o servidor DNS é 10.6.6.6.

```
Ethernet adapter Połączenie lokalne 2:

   Connection-specific DNS Suffix  . : domain1.com
   Description . . . . . . . . . . . : Cisco AnyConnect Secure Mobility Client V
irtual Miniport Adapter for Windows x64
   Physical Address. . . . . . . . . : 00-05-9A-3C-7A-00
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2015:d34b:e3a8:1787%14(Preferred)
   Link-local IPv6 Address . . . . . : fe80::3a02:5a4a:4b9b:ddf2%14(Preferred)
   Link-local IPv6 Address . . . . . : fe80::4fd8:3523:c111:ad1d%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.1.1.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.128
   Default Gateway . . . . . . . . . : ::
   DNS Servers . . . . . . . . . . . : 10.6.6.6
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

No ASA, o usuário *cisco* recebeu IP: 10.1.1.1 e é atribuído à política de grupo *POLICY1*.

```
ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : cisco                  Index        : 29
Assigned IP  : 10.1.1.1               Public IP    : 192.168.1.88
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : RC4                    Hashing      : none SHA1
Bytes Tx     : 10212                  Bytes Rx     : 856
Pkts Tx      : 8                      Pkts Rx      : 2
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : POLICY1                Tunnel Group : RA
Login Time   : 10:18:25 UTC Thu Apr 4 2013
Duration     : 0h:00m:17s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
```

```
VLAN Mapping : N/A                    VLAN         : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1

AnyConnect-Parent:
 Tunnel ID    : 29.1
 Public IP    : 192.168.1.88
 Encryption   : none                   TCP Src Port : 49262
 TCP Dst Port : 443                    Auth Mode    : userPassword
 Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
 Client Type  : AnyConnect
 Client Ver   : 3.1.01065
 Bytes Tx     : 5106                   Bytes Rx     : 788
 Pkts Tx      : 4                      Pkts Rx      : 1
 Pkts Tx Drop : 0                      Pkts Rx Drop : 0

SSL-Tunnel:
 Tunnel ID    : 29.2
 Assigned IP  : 10.1.1.1               Public IP    : 192.168.1.88
 Encryption   : RC4                    Hashing      : SHA1
 Encapsulation: TLSv1.0                TCP Src Port : 49265
 TCP Dst Port : 443                    Auth Mode    : userPassword
 Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
 Client Type  : SSL VPN Client
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.01065
 Bytes Tx     : 5106                   Bytes Rx     : 68
 Pkts Tx      : 4                      Pkts Rx      : 1
 Pkts Tx Drop : 0                      Pkts Rx Drop : 0
 Filter Name  : AAA-user-cisco-E0CF3C05

NAC:
 Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
 SQ Int (T)   : 0 Seconds              EoU Age(T)   : 17 Seconds
 Hold Left (T): 0 Seconds              Posture Token:
```

Além disso, a lista de acesso dinâmico está instalada para esse usuário:

```
ASA# show access-list AAA-user-cisco-E0CF3C05
access-list AAA-user-cisco-E0CF3C05; 1 elements; name hash: 0xf9b6b75c (dynamic)
access-list AAA-user-cisco-E0CF3C05 line 1 extended permit
ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0
(hitcnt=0) 0xf8010475
```

Debugs

Depois de habilitar as depurações, você pode acompanhar cada etapa da sessão WebVPN.

Este exemplo mostra a autenticação LDAP junto com a recuperação de atributo:

```
ASA# show debug
debug ldap  enabled at level 255
debug webvpn anyconnect enabled at level 254
ASA#
[63] Session Start
[63] New request Session, context 0xbbe10120, reqType = Authentication
[63] Fiber started
[63] Creating LDAP context with uri=ldap://192.168.11.10:389
[63] Connect to LDAP server: ldap://192.168.11.10:389, status = Successful
[63] supportedLDAPVersion: value = 3
[63] Binding as Manager
```

```
[63] Performing Simple authentication for Manager to 192.168.11.10
[63] LDAP Search:
       Base DN = [DC=test-cisco,DC=com]
       Filter  = [uid=cisco]
       Scope   = [SUBTREE]
[63] User DN = [uid=cisco,ou=People,dc=test-cisco,dc=com]
[63] Server type for 192.168.11.10 unknown - no password policy
[63] Binding as cisco
[63] Performing Simple authentication for cisco to 192.168.11.10
[63] Processing LDAP response for user cisco
[63] Authentication successful for cisco to 192.168.11.10
[63] Retrieved User Attributes:
[63]    cn: value = John Smith
[63]    givenName: value = John
[63]    sn: value = cisco
[63]    uid: value = cisco
[63]    uidNumber: value = 10000
[63]    gidNumber: value = 10000
[63]    homeDirectory: value = /home/cisco
[63]    mail: value = jsmith@dev.local
[63]    objectClass: value = top
[63]    objectClass: value = posixAccount
[63]    objectClass: value = shadowAccount
[63]    objectClass: value = inetOrgPerson
[63]    objectClass: value = organizationalPerson
[63]    objectClass: value = person
[63]    objectClass: value = CiscoPerson
[63]    loginShell: value = /bin/bash
```

Importante! Os atributos LDAP personalizados são mapeados para atributos do ASA conforme definido no mapa de atributos do ldap:

```
[63]    CiscoBanner: value = This is banner 1
[63]            mapped to Banner1: value = This is banner 1
[63]    CiscoIPAddress: value = 10.1.1.1
[63]            mapped to IETF-Radius-Framed-IP-Address: value = 10.1.1.1
[63]    CiscoIPNetmask: value = 255.255.255.128
[63]            mapped to IETF-Radius-Framed-IP-Netmask: value = 255.255.255.128
[63]    CiscoDomain: value = domain1.com
[63]            mapped to IPSec-Default-Domain: value = domain1.com
[63]    CiscoDNS: value = 10.6.6.6
[63]            mapped to Primary-DNS: value = 10.6.6.6
[63]    CiscoACLin: value = ip:inacl#1=permit
ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0
[63]            mapped to Cisco-AV-Pair: value = ip:inacl#1=permit
ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0
[63]    CiscoSplitACL: value = ACL1
[63]            mapped to IPSec-Split-Tunnel-List: value = ACL1
[63]    CiscoSplitTunnelPolicy: value = 1
[63]            mapped to IPSec-Split-Tunneling-Policy: value = 1
[63]    CiscoGroupPolicy: value = POLICY1
[63]            mapped to IETF-Radius-Class: value = POLICY1
[63]            mapped to LDAP-Class: value = POLICY1
[63]    userPassword: value = {SSHA}5s81Fmi/9aG/WfPSy3lGmw1ORI4lywWC
[63] ATTR_CISCO_AV_PAIR attribute contains 68 bytes
[63] Fiber exit Tx=315 bytes Rx=907 bytes, status=1
[63] Session End
```

A sessão LDAP foi concluída. Agora, o ASA processa e aplica esses atributos.

A ACL dinâmica é criada (com base na entrada ACE no Cisco-AV-Pair):

```
webvpn_svc_parse_acl: processing ACL: name: 'AAA-user-cisco-E0CF3C05',
list: YES, id -1
webvpn_svc_parse_acl: before add: acl_id: -1, acl_name: AAA-user-cisco-E0CF3C05
webvpn_svc_parse_acl: after add: acl_id: 5, acl_name: AAA-user-cisco-E0CF3C05,
refcnt: 1
```

A sessão WebVPN prossegue:

```
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 192.168.1.250'
Processing CSTP header line: 'Host: 192.168.1.250'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 3.1.01065'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent
for Windows 3.1.01065'
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 3.1.01065'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=1476503744@122880@
1365070898@908F356D1C1F4CDF1138088854AF0E480FDCB1BD'
Processing CSTP header line: 'Cookie: webvpn=1476503744@122880@
1365070898@908F356D1C1F4CDF1138088854AF0E480FDCB1BD'
Found WebVPN cookie: 'webvpn=1476503744@122880@
1365070898@908F356D1C1F4CDF1138088854AF0E480FDCB1BD'
WebVPN Cookie: 'webvpn=1476503744@122880@1365070898@
908F356D1C1F4CDF1138088854AF0E480FDCB1BD'
IPADDR: '1476503744', INDEX: '122880', LOGIN: '1365070898'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
Setting version to '1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: admin-Komputer'
Processing CSTP header line: 'X-CSTP-Hostname: admin-Komputer'
Setting hostname to: 'admin-Komputer'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1367'
Processing CSTP header line: 'X-CSTP-MTU: 1367'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv6,IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv6,IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Local-Address-IP4: 192.168.1.88'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Base-MTU: 1468'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Remote-Address-IP4: 192.168.1.250'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Full-IPv6-Capability: true'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: F5ADDD0151261404504FC3B165C3B68A90E51
A1C8EB7EA9B2FE70F1EB8E10929FFD79650B07E218EC8774678CDE1FB5E'
Processing CSTP header line: 'X-DTLS-Master-Secret: F5ADDD015126140450
4FC3B165C3B68A90E51A1C8EB7EA9B2FE70F1EB8E10929FFD79650B07E2
18EC8774678CDE1FB5E'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:
DES-CBC3-SHA:DES-CBC-SHA'
webvpn_cstp_parse_request_field()
```

```
...input: 'X-DTLS-Accept-Encoding: lzs'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: lzs,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol:
Copyright (c) 2004 Cisco Systems, Inc.'
```

Em seguida, a atribuição de endereço ocorre. Observe que não há nenhum pool de IP definido no ASA. Se o LDAP não retornar o atributo *CiscoIPAddress* (que é mapeado para *IETF-Radius-Framed-IP-Address* e usado para atribuição de endereço IP), a configuração falhará nesse estágio.

```
Validating address: 10.1.1.1
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 10.1.1.1/255.255.255.128
webvpn_cstp_accept_ipv6_address: No IPv6 Address
CSTP state = HAVE_ADDRESS
```

A sessão WebVPN é concluída:

```
SVC: NP setup
np_svc_create_session(0x1E000, 0xb5eafa80, TRUE)
webvpn_svc_np_setup
SVC ACL Name: AAA-user-cisco-E0CF3C05
SVC ACL ID: 5
SVC ACL ID: 5
vpn_put_uauth success!
SVC IPv6 ACL Name: NULL
SVC IPv6 ACL ID: -1
SVC: adding to sessmgmt
SVC: Sending response
Sending X-CSTP-FW-RULE msgs: Start
Sending X-CSTP-FW-RULE msgs: Done
Sending X-CSTP-Quarantine: false
Sending X-CSTP-Disable-Always-On-VPN: false
Unable to initiate NAC, NAC might not be enabled or invalid policy
CSTP state = CONNECTED
```

Autenticação e autorização separados do ASA

Às vezes, é melhor separar a autenticação e o processo de autorização. Por exemplo, use a autenticação de senha para usuários definidos localmente; em seguida, após a autenticação local bem-sucedida, recupere todos os atributos de usuário do servidor LDAP:

```
username cisco password cisco
tunnel-group RA general-attributes
authentication-server-group LOCAL
 authorization-server-group LDAP
```

A diferença está na sessão LDAP. No exemplo anterior, ASA:

- vinculado ao OpenLDAP com credenciais de gerente,
- pesquisou o usuário *cisco*, e

- vinculado (autenticação simples) ao OpenLDAP com credenciais Cisco.

Atualmente, com autorização LDAP, a terceira etapa não é mais necessária, pois o usuário já foi autenticado pelo banco de dados local.

Cenários mais comuns envolvem o uso de tokens RSA para processo de autenticação e atributos LDAP/AD para autorização.

Atributos ASA do LDAP e do grupo local

Éimportante entender a diferença entre os atributos LDAP e RADIUS.

Quando você usa LDAP, o ASA não permite mapeamento para nenhum atributo *radius*. Por exemplo, quando você usa o RADIUS, é possível retornar o atributo 217 *do par* do *cisco av* (pools de endereços). Esse atributo define um pool de endereços IP configurados localmente que são usados para atribuir endereços IP.

Com o mapeamento LDAP, é impossível usar esse atributo *cisco-av-pair* específico. O atributo *cisco-av-pair* com mapeamento LDAP pode ser usado somente para especificar diferentes tipos de ACLs.

Essas limitações no LDAP impedem que ele seja tão flexível quanto o RADIUS. Para trabalhar em nuvem, essa política de grupo definida localmente pode ser criada no ASA com atributos que não podem ser mapeados do ldap (como pools de endereços). Depois que o usuário LDAP é autenticado, ele é atribuído a essa política de grupo (no nosso exemplo POLICY1) e aos atributos não específicos do usuário recuperados da política de grupo.

A lista completa de atributos suportada pelo mapeamento LDAP pode ser encontrada neste documento: Guia de configuração do Cisco ASA 5500 Series usando CLI, 8.4 e 8.6

Você pode comparar com a lista completa de atributos do RADIUS VPN3000 suportados pelo ASA; consulte este documento: Guia de configuração do Cisco ASA 5500 Series usando CLI, 8.4 e 8.6

Consulte este documento para obter uma lista completa de atributos IETF RADIUS suportados pelo ASA: Guia de configuração do Cisco ASA 5500 Series usando CLI, 8.4 e 8.6

ASA e LDAP com autenticação de certificado

O ASA não oferece suporte à recuperação de atributo de certificado LDAP e à comparação binária com o certificado fornecido pelo Anyconnect. Essa funcionalidade é reservada para Cisco ACS ou ISE (e somente para suplicantes 802.1x) porque a autenticação VPN é encerrada em um dispositivo de acesso à rede (NAD).

Há outra solução. Quando a autenticação do usuário usa certificados, o ASA executa a validação do certificado e pode recuperar atributos LDAP com base em campos específicos do certificado (por exemplo, CN):

```
tunnel-group RA general-attributes
authorization-server-group LDAP
username-from-certificate CN
```

```
authorization-required
tunnel-group RA webvpn-attributes
 authentication certificate
```

Depois que o certificado do usuário é validado pelo ASA, a autorização LDAP é executada e os atributos do usuário (do campo CN) são recuperados e aplicados.

Debugs

O certificado de usuário foi usado: cn=test1,ou=Security,o=Cisco,l=Cracóvia,st=PL,c=PL

O mapeamento de certificado está configurado para mapear esse certificado para o grupo de túneis RA:

```
crypto ca certificate map MAP-RA 10
 issuer-name co tac
webvpn
certificate-group-map MAP-RA 10 RA
```

Validação e mapeamento do certificado:

```
ASA# show debug
debug ldap  enabled at level 255
debug webvpn anyconnect enabled at level 254
debug crypto ca enabled at level 3
debug crypto ca messages enabled at level 3
debug crypto ca transactions enabled at level 3

Apr 09 2013 17:31:32: %ASA-7-717025: Validating certificate chain containing 1 certificate(s).

Apr 09 2013 17:31:32: %ASA-7-717029: Identified client certificate within certificate chain.
serial number: 00FE9C3D61E131CDB1, subject name:
cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,c=PL.

Apr 09 2013 17:31:32: %ASA-6-717022: Certificate was successfully validated. Certificate is
resident and trusted, serial number: 00FE9C3D61E131CDB1, subject name:
cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,c=PL.

Apr 09 2013 17:31:32: %ASA-6-717028: Certificate chain was successfully validated with
revocation status check.

Apr 09 2013 17:31:32: %ASA-6-725002: Device completed SSL handshake with client
outside:192.168.1.88/49179

Apr 09 2013 17:31:32: %ASA-7-717036: Looking for a tunnel group match based on certificate maps
for peer certificate with serial number: 00FE9C3D61E131CDB1, subject name:
cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,c=PL, issuer_name:
cn=TAC,ou=RAC,o=TAC,l=Warsaw,st=Maz,c=PL.

Apr 09 2013 17:31:32: %ASA-7-717038: Tunnel group match found. Tunnel Group: RA, Peer
certificate: serial number: 00FE9C3D61E131CDB1, subject name:
cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,c=PL, issuer_name:
cn=TAC,ou=RAC,o=TAC,l=Warsaw,st=Maz,c=PL.
```

Extração do nome de usuário do certificado e autorização usando LDAP:

```
Apr 09 2013 17:31:32: %ASA-7-113028: Extraction of username from VPN client certificate has been
requested.  [Request 53]
```

```
Apr 09 2013 17:31:32: %ASA-7-113028: Extraction of username from VPN client certificate has
started.  [Request 53]

Apr 09 2013 17:31:32: %ASA-7-113028: Extraction of username from VPN client certificate has
finished successfully.  [Request 53]

Apr 09 2013 17:31:32: %ASA-7-113028: Extraction of username from VPN client certificate has
completed.  [Request 53]

Apr 09 2013 17:31:32: %ASA-6-302013: Built outbound TCP connection 286 for
inside:192.168.11.10/389 (192.168.11.10/389) to identity:192.168.11.250/33383
(192.168.11.250/33383)

Apr 09 2013 17:31:32: %ASA-6-113004: AAA user authorization Successful : server =  192.168.11.10
: user = test1

Apr 09 2013 17:31:32: %ASA-6-113003: AAA group policy for user test1 is being set to POLICY1

Apr 09 2013 17:31:32: %ASA-6-113011: AAA retrieved user specific group policy (POLICY1) for user
= test1

Apr 09 2013 17:31:32: %ASA-6-113009: AAA retrieved default group policy (MY) for user = test1

Apr 09 2013 17:31:32: %ASA-6-113008: AAA transaction status ACCEPT : user = test1
```

Recuperação de atributos do LDAP:

```
Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.cn = John Smith

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.givenName = John

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.sn = test1

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.uid = test1

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.uidNumber = 10000

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.gidNumber = 10000

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.homeDirectory = /home/cisco

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.mail = jsmith@dev.local

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.objectClass.1 = top

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.objectClass.2 = posixAccount

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
```

```
aaa.ldap.objectClass.3 = shadowAccount

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.objectClass.4 = inetOrgPerson

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.objectClass.5 = organizationalPerson

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.objectClass.6 = person

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.objectClass.7 = CiscoPerson

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.loginShell = /bin/bash

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.userPassword = {CRYPT}*

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.CiscoBanner = This is banner 1

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.CiscoIPAddress = 10.1.1.1

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.CiscoIPNetmask = 255.255.255.128

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.CiscoDomain = domain1.com

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.CiscoDNS = 10.6.6.6

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.CiscoACLin = ip:inacl#1=permit ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.CiscoSplitACL = ACL1

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.CiscoSplitTunnelPolicy = 1

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.ldap.CiscoGroupPolicy = POLICY1
```

Atributos mapeados da Cisco:

```
Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.cisco.grouppolicy = POLICY1

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.cisco.ipaddress = 10.1.1.1

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.cisco.username = test1

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
```

```
aaa.cisco.username1 = test1

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.cisco.username2 =

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.cisco.tunnelgroup = RA

Apr 09 2013 17:31:32: %ASA-6-734001: DAP: User test1, Addr 192.168.1.88, Connection AnyConnect:
The following DAP records were selected for this connection: DfltAccessPolicy

Apr 09 2013 17:31:32: %ASA-6-113039: Group
```

.

Autenticação secundária

Se a autenticação de dois fatores for necessária, será possível usar a senha do token junto com a autenticação e autorização LDAP:

```
tunnel-group RA general-attributes
 authentication-server-group RSA
secondary-authentication-server-group LDAP
 authorization-server-group LDAP
tunnel-group RA webvpn-attributes
 authentication aaa
```

Em seguida, o usuário deve fornecer um nome de usuário e uma senha RSA (algo que o usuário tem — um token), juntamente com o nome de usuário/senha LDAP (algo que o usuário sabe). Também é possível usar um nome de usuário do certificado para autenticação secundária. Para obter mais informações sobre autenticação dupla, consulte o Guia de Configuração do Cisco ASA 5500 Series usando CLI, 8.4 e 8.6.

Informações Relacionadas

- Guia de configuração do Cisco ASA 5500 Series usando CLI, 8.4 e 8.6
- Guia do administrador do software OpenLDAP 2.4
- Números da empresa privada
- Suporte Técnico e Documentação - Cisco Systems