ASA Anyconnect VPN e autorização de OpenLDAP com exemplo de configuração feito sob encomenda do esquema e dos Certificados

Índice

Introdução

Este documento descreve como configurar OpenLDAP com esquema feito sob encomenda para apoiar atributos por usuário para o Cliente de mobilidade Cisco AnyConnect Secure que conecta a Cisco uma ferramenta de segurança adaptável (ASA). A configuração ASA é bastante básica porque todos os atributos de usuário são recuperados do server de OpenLDAP. Igualmente são descritas neste documento as diferenças na autenticação LDAP e na autorização quando usadas junto com Certificados.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Versão ASA 8.4 de Cisco e mais atrasado
- Versão 2.4.30 de OpenLDAP

Configurar

Configuração básica de OpenLDAP

Etapa 1. Configurar o server.

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

o arquivo ldap.conf é usado para ajustar os padrões do nível de sistema que podem ser usados pelo cliente local do ldap.

Nota: Embora você não seja exigido estabelecer padrões do nível de sistema, podem ajudar a testar e pesquisar defeitos o mais servier quando você executa um cliente local do ldap.

/etc/openldap/ldap.conf:

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

o arquivo slapd.conf é usado para a configuração do servidor de OpenLDAP. Os arquivos do esquema do padrão incluem definições amplamente utilizadas LDAP. Por exemplo, os personis do nome de classe do objeto definidos no core.schema arquivam. Os usos desta configuração que esquema comum e definem 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.

A fim verificar que OpenLDAP básico trabalha, execute esta configuração:

```
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 3. Adicionar registros ao base de dados.

Uma vez que você hve testou e configurou everthing corretamente, adicionar registros ao base de dados. A fim adicionar recipientes básicos para usuários e grupos, execute esta configuração:

```
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
```

Esquema feito sob encomenda de Openldap

Agora que a configuração básica trabalha, você pode adicionar o esquema feito sob encomenda. Neste exemplo de configuração, um novo tipo de objeto *CiscoPerson* nomeado classe é criado e estes atributos são criados e usados nesta classe de objeto:

- CiscoBanner
- CiscoACLin
- CiscoDomain
- CiscoDNS
- CiscoIPAddress
- CiscoIPNetmask
- CiscoSplitACL
- CiscoSplitTunnelPolicy
- CiscoGroupPolicy

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

```
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
```

Notas importantes

- Use a empresa privada OID para sua empresa. Todos os OID querem o wor, mas o melhor prática é usar os OID atribuídos pelo IANA. Esse configurado no este exemplos começa de 1.3.6.1.4.1.9 (que é reservado por Cisco: http://www.iana.org/assignments/enterprise-numbers).
- O seguinte OID (500.1.1-500.1.9) foi usado parte de para não interferir diretamente na árvore principal de Cisco OID ("1.3.6.1.4.1.9").
- Este base de dados usa a classe de objeto da *pessoa* definida no esquema/core.ldif. Que o objeto é do tipo e de registros SUPERIORES pode incluir somente um tal atributo (que é porque a classe de CiscoPersonobject é do tipo auxiliar).
- A classe do objeto nomeada *CiscoPerson* deve incluir o SN ou o CN e pode incluir alguns dos atributos de Cisco do costume definidos mais cedo. Note que pode igualmente incluir todos os outros atributos definidos em outros esquemas (tais como o *userPassword* ou o *telephoneNumber*).
- Recorde que cada objeto deve ter um número diferente OID.
- Os atributos feitos sob encomenda são não diferenciando maiúsculas e minúsculas e do tipo da *corda* com a codificação de UTF-8 e os caráteres 128 máximos (definidos pela SINTAXE).

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. Serviços do reinício.

```
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 4. Adicionar um novo usuário com todos os atributos feitos sob encomenda.

Neste exemplo, o usuário pertence aos objetos múltiplos dos objectClass, e herda atributos de todo. Com este processo é fácil adicionar o esquema adicional ou os atributos sem mudanças aos registros de base de dados existente.

```
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. Ajuste a senha para o usuário.

```
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 6. Verifique a configuração.

```
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"
```

Configuração ASA

Etapa 1. Configurar a relação e o certificado.

```
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 2. Gerencia um certificado auto-assinado.

```
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 3. Permita o WebVPN na interface externa.

```
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 4. Rache a configuração ACL.

O nome ACL é retornado por OpenLDAP:

```
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. Crie um nome de grupo de túneis que use a grupo-política do padrão (DfltAccessPolicy).

Os usuários com o atributo específico LDAP (*CiscoGroupPolicy*) são traçados a uma outra política: POLICY1

```
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"
```

A configuração de AAA-server ASA usa o mapa de atributos do ldap traçando dos atributos retornados por OpenLDAP aos atributos que podem ser interpretados pelo ASA para usuários de Anyconnect.

```
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 6. Permita o servidor ldap para a autenticação para o grupo de túneis especificado.

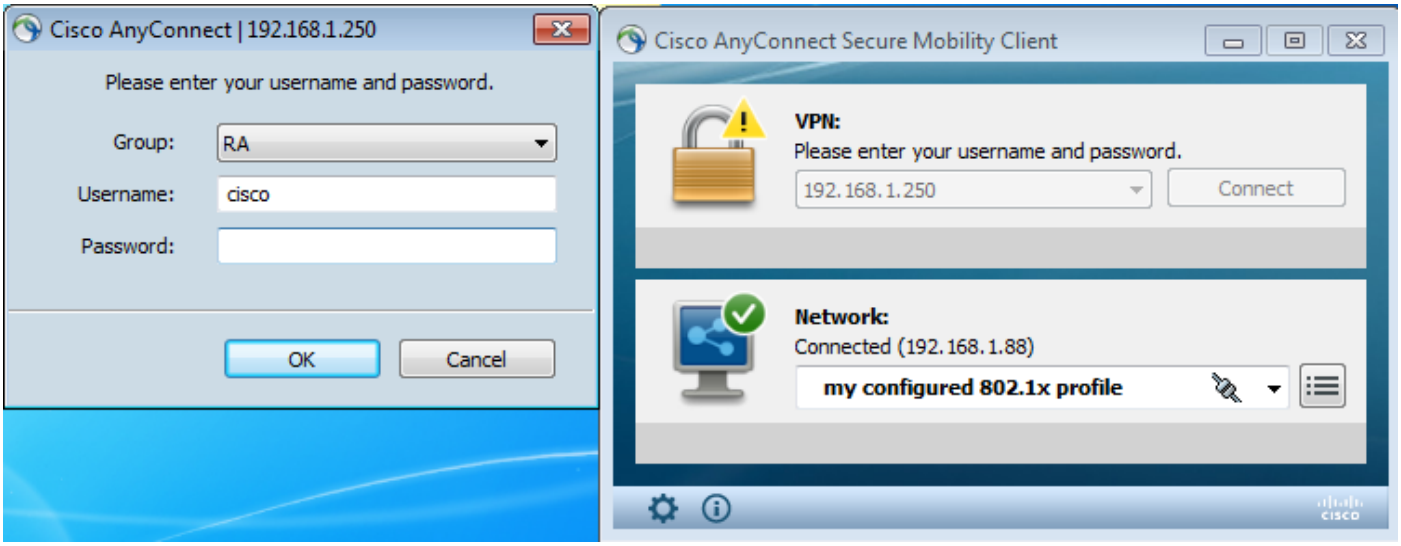
```
pluton # cat users.ldiff
# User account
dn: uid=cisco,ou=people,dc=test-cisco,dc=com
cn: John Smith
givenName: John
sn: cisco
uid: cisco
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/cisco
mail: jsmith@dev.local
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: 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"
```

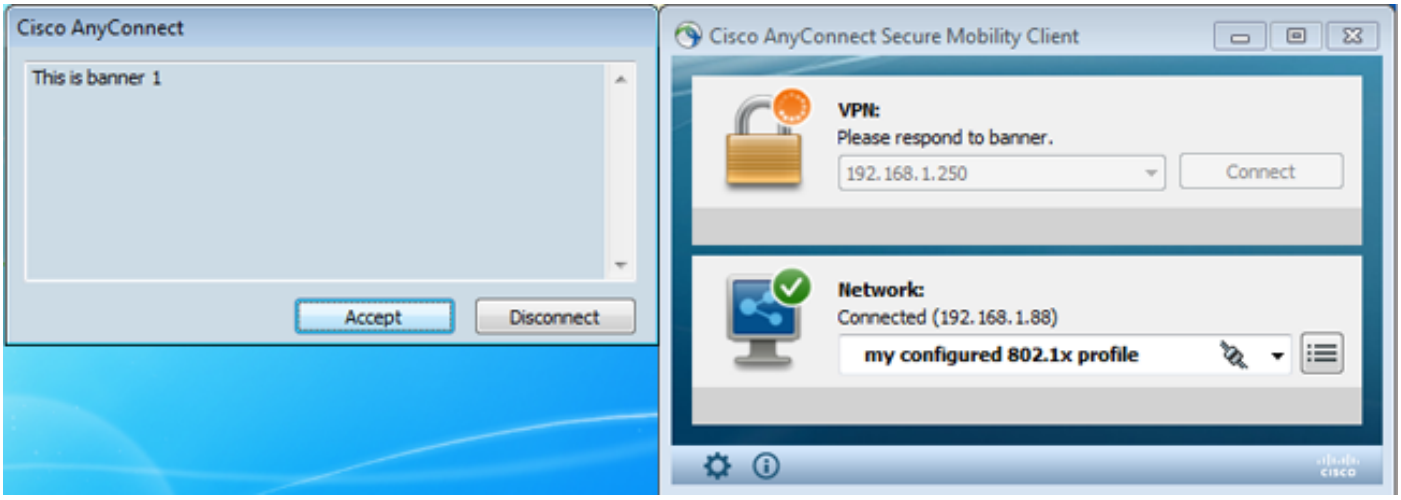
Verificar

Teste o acesso VPN

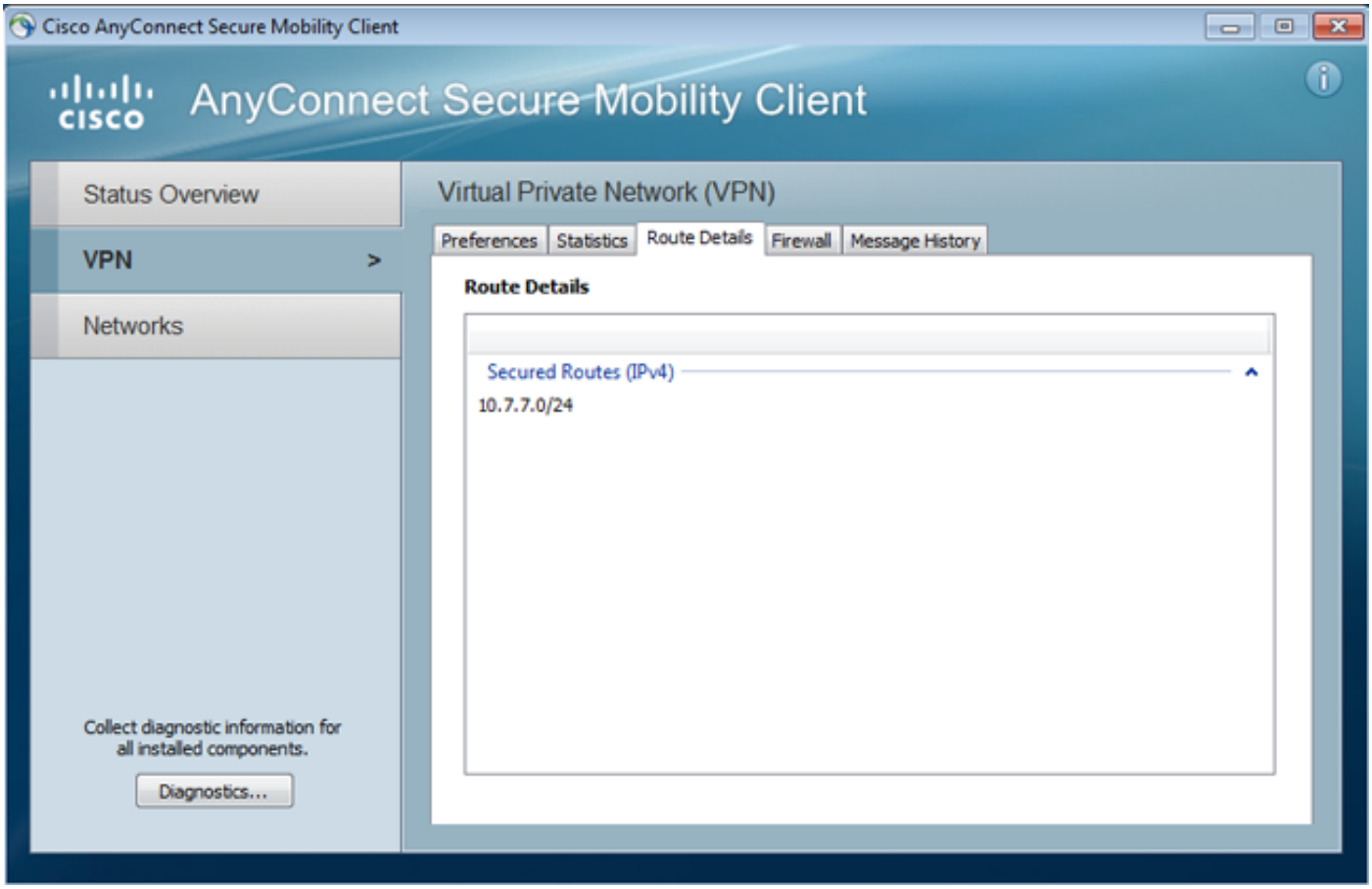
Anyconnect é configurado para conectar a 192.168.1.250. O início de uma sessão é username *Cisco* e senha *pass1*.



Após a autenticação a bandeira correta é usada.



A separação correta ACL é enviada (ACL1 definido no ASA).



A relação de Anyconnect é configurada com IP: 10.1.1.1 e netmask 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 o IP: 10.1.1.1 e é atribuído para agrupar a política *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:
```

Também, a lista de acesso dinâmica é 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 que você permite debuga, você pode seguir cada etapa da sessão de VPN da Web.

Este exemplo mostra a autenticação LDAP junto com a recuperação do 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 do costume LDAP são traçados aos atributos ASA como 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 é terminada. Agora, o ASA processa e aplica aqueles atributos.

O ACL dinâmico é criado (baseado no ACE a entrada 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
```

Os rendimentos da sessão de VPN da Web:

```
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. A observação lá não é nenhum IP pool definido no ASA. Se o LDAP não retorna o atributo de *CiscoIPAddress* (que é IETF-Raio-Framed-IP-*endereço* traçado e usado para a atribuição do endereço IP de Um ou Mais Servidores Cisco ICM NT), a configuração falharia nesta fase.

```
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 de VPN da Web termina:

```
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
```

Authentication e autorização separada ASA

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

```
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
```

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

- ativado a OpenLDAP com credenciais do gerente,
- busca executada para o usuário *Cisco*, e
- ativado (autenticação simples) a OpenLDAP com credenciais de Cisco.

Atualmente, com autorização LDAP, a terceira etapa é já não necessária, desde que o usuário tem sido autenticado já através do base de dados local.

Mais cenários comuns envolvem o uso de tokens RSA para o processo de autenticação e de atributos LDAP/AD para a autorização.

Atributos ASA do LDAP e do grupo local

Éimportante compreender a diferença entre atributos LDAP e atributos RADIUS.

Quando você usa o LDAP, o ASA não reserva traçar a nenhum *atributo RADIUS*. Por exemplo, quando você usa o RAIO, é possível retornar o atributo 217 do *Cisco-av-pair* (poois de endereços). Esse atributo define localmente um conjunto configurado de endereços IP de Um ou Mais Servidores Cisco ICM NT que são usados para atribuir endereços IP de Um ou Mais Servidores Cisco ICM NT.

Com mapeamento LDAP, é impossível usar-se que atributo específico do *Cisco-av-pair*. O atributo do *Cisco-av-pair* com mapeamento LDAP pode ser usado para especificar somente tipos diferentes de ACL.

Estas limitações no LDAP impedem que seja tão flexível quanto o raio. Ao workaroud esta localmente política do grupo definido pode ser criada no ASA com os atributos que não podem ser traçados do ldap (como poois de endereços). Uma vez que o usuário LDAP é autenticado, estão atribuídos a essa política do grupo (em nosso exemplo POLICY1) e o não específica de usuário atribui reretrieved da grupo-política.

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

Você pode comparar ao máximo a lista de atributos do RAIO VPN3000 apoiados pelo ASA; refira este documento: Manual de configuração do 5500 Series de Cisco ASA usando o CLI, os 8.4 e os 8.6

Refira este documento para uma lista completa dos atributos do RAIO IETF apoiados pelo ASA: Manual de configuração do 5500 Series de Cisco ASA usando o CLI, os 8.4 e os 8.6

ASA e LDAP com certificado de autenticação

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

Há um outro soluction. Quando a autenticação de usuário usa Certificados, o ASA executa a validação certificada e pode recuperar os atributos LDAP baseados em campos específicos do certificado (por exemplo, CN):

```
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
```

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

Debugs

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

O mapeamento do certificado é configurado para traçar esse certificado ao grupo de túneis RA:

```
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
```

Validação certificada e mapeamento:

```
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 3Apr 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-6-717028: Certificate chain was successfully validated with
revocation status check.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 username do certificado e da autorização usando o 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 been requested**. [Request 53]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 been requested**. [Request 53]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-6-113004: **AAA user authorization Successful : server = 192.168.11.10 : user = test1**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-6-113004: **AAA user authorization Successful : server = 192.168.11.10 : user = test1**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-6-113004: **AAA user authorization Successful : server = 192.168.11.10 : user = test1**

Atribui a recuperação 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**

Cisco traçou attibutes:

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 = test1Apr 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 = RAApr 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: DfltAccessPolicyApr 09 2013 17:31:32: %ASA-6-113039:
Group <POLICY1> User <test1> IP <192.168.1.88> AnyConnect parent session started.Apr 09 2013
17:31:32: %ASA-6-113039: Group <POLICY1> User <test1> IP <192.168.1.88> AnyConnect parent
session started.
```

Autenticação secundária

Se a autenticação de dois fatores é exigida, é possível usar a senha simbólica junto com a autenticação LDAP e a autorização:

```
Apr 09 2013 17:31:32: %ASA-6-113039: Group <POLICY1> User <test1> IP <192.168.1.88> AnyConnect
parent session started.
```

Então, o usuário deve fornecer um nome de usuário e senha do RSA (algo o usuário tem — um token), junto com username LDAP/senha (algo que o usuário sabe). É igualmente possível usar um username do certificado para a autenticação secundária. Para obter mais informações sobre da Autenticação dupla, refira o manual de configuração do 5500 Series de Cisco ASA usando o CLI, os 8.4 e os 8.6.

Informações Relacionadas

- Manual de configuração do 5500 Series de Cisco ASA usando o CLI, os 8.4 e os 8.6
- O guia de administrador do software 2.4 de OpenLDAP
- Números de empresa privada
- Suporte Técnico e Documentação - Cisco Systems