사용자 지정 스키마 및 인증서를 사용한 ASA Anyconnect VPN 및 OpenLDAP 권한 부여 구성 예

목차

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance)에 연결되는 Cisco AnyConnect Secure Mobility Client에 대한 사용자별 특성을 지원하도록 사용자 지정 스키마로 OpenLDAP을 구성하는 방법에 대해 설명합니다. 모든 사용자 특성이 OpenLDAP 서버에서 검색되므로 ASA 컨피그레이션은 매우 기본적입니다.이 문서에서 설명하는 것은 인증서와 함께 사용할 때 LDAP 인증 및 권한 부여의 차이점입니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Linux 구성에 대한 기본 지식
- ASA CLI 컨피그레이션에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco ASA 버전 8.4 이상
- OpenLDAP 버전 2.4.30

구성

기본 OpenLDAP 컨피그레이션

1단계. 서버를 구성합니다.

이 예에서는 test-cisco.com ldap 트리를 사용합니다.

ldap.conf 파일은 로컬 ldap 클라이언트에서 사용할 수 있는 시스템 수준 기본값을 설정하는 데 사용됩니다.

참고:시스템 레벨 기본값을 설정할 필요는 없지만, 로컬 ldap 클라이언트를 실행할 때 이를 통해 서비스를 테스트하고 문제를 해결할 수 있습니다.

/etc/openldap/ldap.conf:

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

slapd.conf 파일은 OpenLDAP 서버 컨피그레이션에 사용됩니다.기본 스키마 파일에는 널리 사용되는 LDAP 정의가 포함됩니다.예를 들어, object 클래스 이름 person은 core.schema 파일에 정의됩니다.이 컨피그레이션에서는 해당 공통 스키마를 사용하고 Cisco별 특성에 대한 고유의 스키마를 정의합니다.

/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
```

2단계. LDAP 컨피그레이션을 확인합니다.

기본 OpenLDAP가 작동하는지 확인하려면 다음 컨피그레이션을 실행합니다.

```
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
```

3단계. 데이터베이스에 레코드를 추가합니다.

모든 항목을 올바르게 테스트하고 구성했으면 데이터베이스에 레코드를 추가합니다. 사용자 및 그룹의 기본 컨테이너를 추가하려면 다음 구성을 실행합니다.

```
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
```

사용자 지정 Openldap 스키마

기본 컨피그레이션이 작동하므로 사용자 지정 스키마를 추가할 수 있습니다.이 컨피그레이션 예에서는 CiscoPerson이라는 새 객체 클래스 유형*이* 생성되고 이 속성이 생성되어 이 객체 클래스에서 사용됩니다.

- Cisco배너
- CiscoACL인
- Cisco 도메인
- CiscoDNS
- CiscoIPA주소
- CiscoIPN넷마스크
- CiscoSplitACL
- Cisco스플릿 터널 정책
- Cisco 그룹 정책

1단계. cisco.schema에 새 스키마를 생성합니다.

```
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 ) )
```

중요 참고 사항

- 회사에 프라이빗 엔터프라이즈 OID를 사용합니다.모든 OID는 작동하지만 IANA에서 할당한 OID를 사용하는 것이 좋습니다.이 예에서 구성된 항목은 1.3.6.1.4.1.9(Cisco에서 예약함)부터 시작합니다.http://www.iana.org/assignments/enterprise-numbers)
- OID의 다음 부분(500.1.1-500.1.9)은 Cisco OID의 기본 트리("1.3.6.1.4.1.9")에서 직접 간섭하지 않는 데 사용되었습니다.
- 이 데이터베이스는 schema/core.ldif에 정의된 *Person* 객체 클래스를 사용합니다.해당 개체는 TOP 유형이며 레코드는 이러한 특성을 하나만 포함할 수 있습니다(*CiscoPerson* 객체 클래스가 Auxiliary 유형인 이유).
- *CiscoPerson*이라는 개체 클래스는 SN 또는 CN을 포함해야 하며 이전에 정의된 사용자 지정 Cisco 특성을 포함할 수 있습니다.또한 다른 스키마(예: userPassword 또는 telephoneNumber)에 정의된 다른 속성을 포함할 수 있습니다.
- 각 객체에는 다른 OID 번호가 있어야 합니다.
- 사용자 지정 특성은 대/소문자를 구분하지 않으며 UTF-8 인코딩 및 최대 128자(SYNTAX에 의해 정의됨)를 사용하는 *문자열* 유형입니다.

2단계. sldap.conf에 스키마를 포함합니다.

```
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
```

3단계. 서비스를 다시 시작합니다.

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

4단계. 모든 사용자 지정 특성을 가진 새 사용자를 추가합니다.

이 예제에서는 사용자가 여러 objectClass 개체에 속하며 모든 개체에서 특성을 상속합니다.이 프로세스를 사용하면 기존 데이터베이스 레코드를 변경하지 않고도 스키마 또는 속성을 쉽게 추가할 수

있습니다.

```
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"
```

5단계. 사용자의 비밀번호를 설정합니다.

```
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
```

6단계. 컨피그레이션을 확인합니다.

```
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
```

ASA 컨피그레이션

1단계. 인터페이스 및 인증서를 구성합니다.

```
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
```

2단계. 자체 서명 인증서를 생성합니다.

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

3단계. 외부 인터페이스에서 WebVPN을 활성화합니다.

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

4단계. ACL 컨피그레이션을 분할합니다.

ACL 이름은 OpenLDAP에 의해 반환됩니다.

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

5단계. 기본 그룹 정책(DfltAccessPolicy)을 사용하는 터널 그룹 이름을 생성합니다.

특정 LDAP 특성(*CiscoGroupPolicy*)이 있는 사용자는 다른 정책에 매핑됩니다.정책1

```
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
```

ASA aaa-server 컨피그레이션은 OpenLDAP에서 반환한 특성에서 Anyconnect 사용자를 위해 ASA에서 해석할 수 있는 특성으로 매핑하기 위해 ldap attribute-map을 사용합니다.

```
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
```

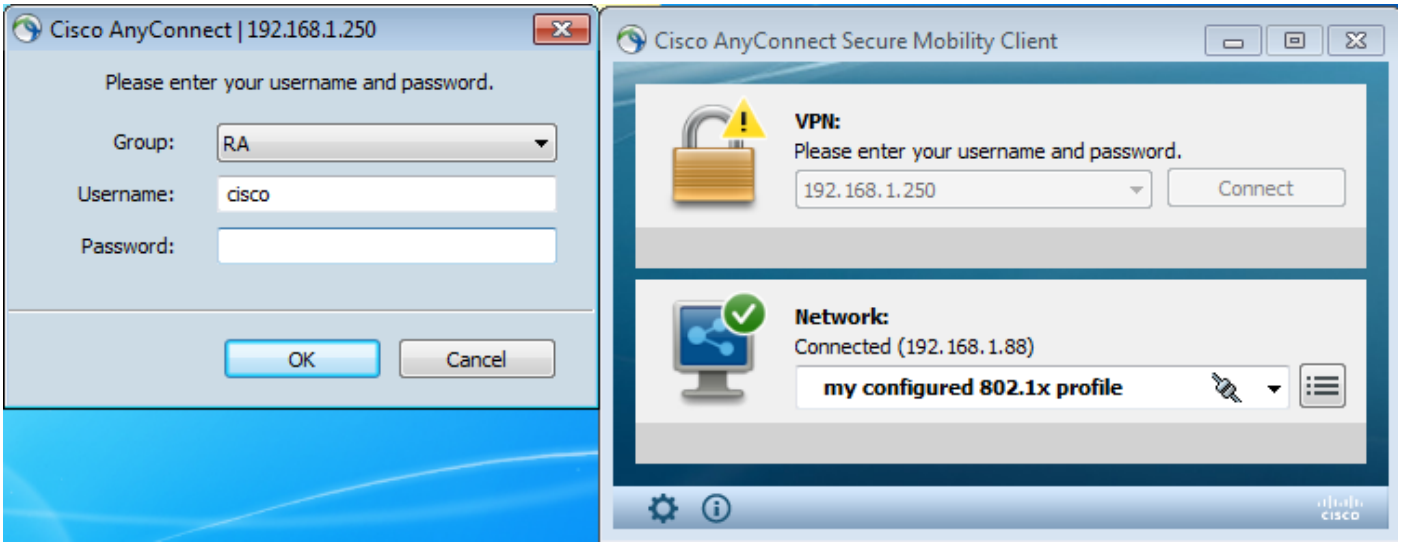
6단계. 지정된 터널 그룹에 대한 인증을 위해 LDAP 서버를 활성화합니다.

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

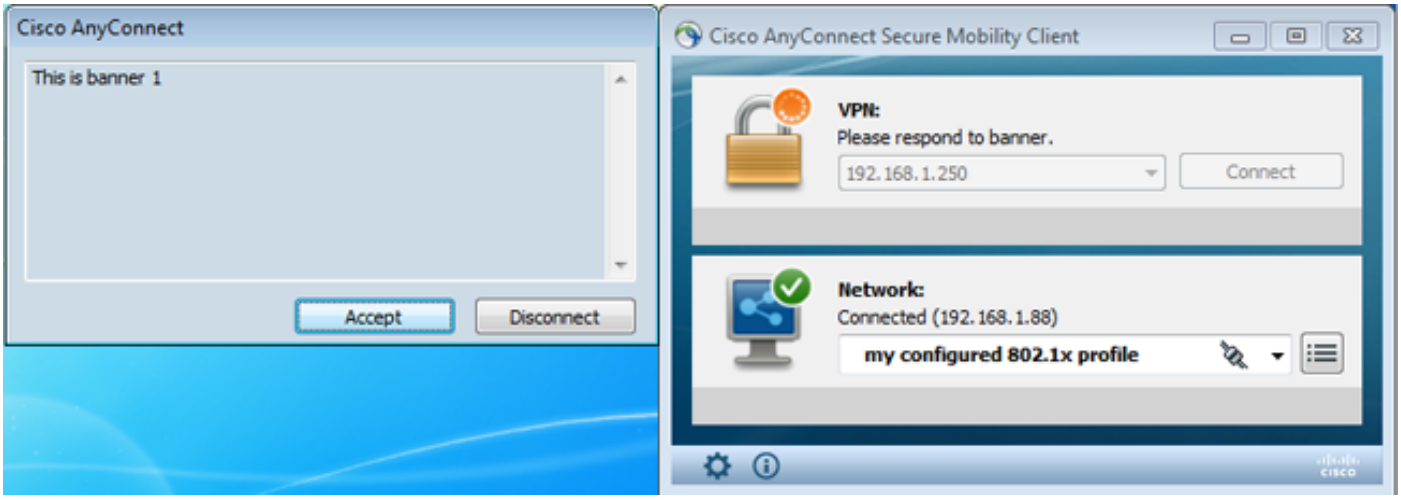
다음을 확인합니다.

VPN 액세스 테스트

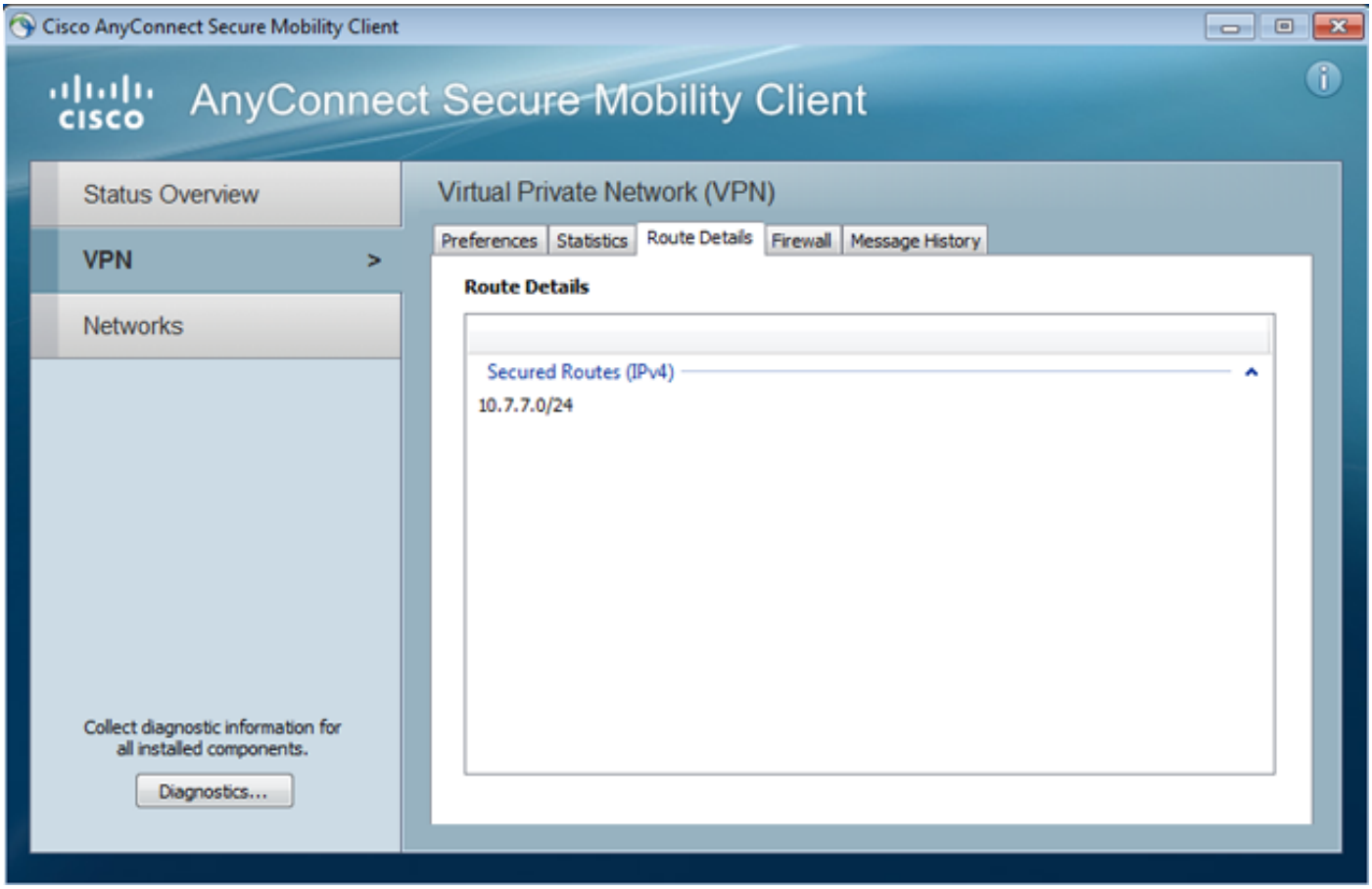
AnyConnect는 192.168.1.250에 연결하도록 구성되어 있습니다. 로그인은 사용자 이름 *cisco* 및 비밀번호 *pass1입니다*.



인증 후 올바른 배너가 사용됩니다.



올바른 스플릿 ACL이 전송됩니다(ASA에 정의된 ACL1).



Anyconnect 인터페이스는 IP로 구성됩니다.10.1.1.1 및 netmask 255.255.255.128. 도메인은 domain1.com이고 DNS 서버는 10.6.6.6입니다.

```
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
```

ASA에서 사용자 *cisco*가 IP를 수신했습니다.10.1.1.1 및 이(가) 그룹 정책 POLICY*1에 할당됩니다*.

```
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:
```

또한 해당 사용자에 대해 동적 액세스 목록이 설치됩니다.

```
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
```

디버깅

디버그를 활성화한 후 WebVPN 세션의 각 단계를 추적할 수 있습니다.

다음 예에서는 특성 검색과 함께 LDAP 인증을 보여줍니다.

```
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
```

중요!사용자 지정 LDAP 특성은 ldap 특성 맵에 정의된 대로 ASA 특성에 매핑됩니다.

```
[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
```

LDAP 세션이 완료되었습니다.이제 ASA는 이러한 특성을 처리하고 적용합니다.

동적 ACL이 생성됩니다(Cisco-AV-Pair의 ACE에 따라).

```
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
```

WebVPN 세션이 진행됩니다.

```
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.'
```

다음으로 주소 할당이 발생합니다.ASA에 정의된 IP 풀이 없습니다.LDAP가 *CiscoIPAddress* 특성(IETF-*Radius-Framed-IP-Address에 매핑되고* IP 주소 할당에 사용됨)을 반환하지 않을 경우 이 단계에서 컨피그레이션이 실패합니다.

```
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
```

WebVPN 세션이 완료됩니다.

```
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
```

ASA 별도의 인증 및 권한 부여

인증 및 권한 부여 프로세스를 분리하는 것이 더 나은 경우도 있습니다.예를 들어, 로컬로 정의된 사용자에 대해 비밀번호 인증을 사용합니다.로컬 인증이 성공한 후 LDAP 서버에서 모든 사용자 특성을 검색합니다.

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

차이점은 LDAP 세션입니다.이전 예에서 ASA는 다음과 같습니다.

- 관리자 자격 증명을 사용하여 OpenLDAP에 바인딩,
- 사용자 *cisco*를 검색하고
- Cisco 자격 증명을 사용하여 OpenLDAP에 바인딩(단순 인증)

현재 LDAP 권한 부여를 사용하면 사용자가 이미 로컬 데이터베이스를 통해 인증되었으므로 세 번

째 단계가 더 이상 필요하지 않습니다.

인증 프로세스에 RSA 토큰을 사용하고 권한 부여를 위해 LDAP/AD 특성을 사용하는 경우가 더 많습니다.

LDAP 및 로컬 그룹의 ASA 특성

LDAP 특성과 RADIUS 특성의 차이를 이해하는 것이 중요합니다.

LDAP를 사용하는 경우 ASA는 어떤 *radius* 특성에 매핑하는 것을 허용하지 않습니다.예를 들어 RADIUS를 사용할 경우 *cisco-av-pair* 특성 217(Address-Pools)을 반환할 수 있습니다. 이 특성은 IP 주소를 할당하는 데 사용되는 로컬에서 구성된 IP 주소 풀을 정의합니다.

LDAP 매핑에서는 특정 *cisco-av-pair* 특성을 사용할 수 없습니다.LDAP 매핑이 *있는* *cisco-av-pair* 특성은 서로 다른 유형의 ACL을 지정하는 데만 사용할 수 있습니다.

LDAP의 이러한 제한 때문에 RADIUS만큼 유연하지 않습니다.이 로컬로 정의된 그룹 정책을 ASA에서 생성할 수 있으며, 이 특성은 ldap(예: 주소 풀)에서 매핑할 수 없습니다. LDAP 사용자가 인증되면 해당 그룹 정책(예: POLICY1)에 할당되고 그룹 정책에서 재검색되는 사용자별 특성이 아닌 것입니다.

LDAP 매핑에서 지원되는 전체 특성 목록은 다음 문서에서 확인할 수 있습니다. CLI, 8.4 및 8.6을 사용하는 Cisco ASA 5500 Series 컨피그레이션 가이드

ASA에서 지원하는 RADIUS VPN3000 특성의 전체 목록과 비교할 수 있습니다.다음 문서를 참조하십시오.CLI, 8.4 및 8.6을 사용하는 Cisco ASA 5500 Series 컨피그레이션 가이드

ASA에서 지원하는 RADIUS IETF 특성의 전체 목록은 다음 문서를 참조하십시오.CLI, 8.4 및 8.6을 사용하는 Cisco ASA 5500 Series 컨피그레이션 가이드

인증서 인증을 사용하는 ASA 및 LDAP

ASA는 Anyconnect에서 제공하는 인증서와 LDAP 인증서 특성 검색 및 이진 비교를 지원하지 않습니다.이 기능은 NAD(네트워크 액세스 디바이스)에서 VPN 인증이 종료되므로 Cisco ACS 또는 ISE(802.1x 신청자만 해당)에 예약됩니다.

또 다른 해결책이 있습니다.사용자 인증이 인증서를 사용하는 경우 ASA는 인증서 검증을 수행하고 인증서의 특정 필드(예: CN)를 기반으로 LDAP 특성을 검색할 수 있습니다.

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

ASA에서 사용자 인증서를 검증하면 LDAP 권한 부여가 수행되고 사용자 특성(CN 필드에서)이 검색되고 적용됩니다.

디버깅

사용자 인증서가 사용됨:cn=test1,ou=보안,o=Cisco,l=Krakow,st=PL,c=PL

인증서 매핑은 해당 인증서를 RA 터널 그룹에 매핑하도록 구성됩니다.

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

인증서 검증 및 매핑:

```
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.
```

LDAP를 사용하여 인증서 및 권한 부여에서 사용자 이름 추출:

```
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
```

LDAP에서 특성 검색:

```
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 매핑된 특성:

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
```

.

보조 인증

2단계 인증이 필요한 경우 LDAP 인증 및 권한 부여와 함께 토큰 비밀번호를 사용할 수 있습니다.

```
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
```

그런 다음 사용자는 LDAP 사용자 이름/비밀번호(사용자가 알고 있는 것)와 함께 RSA에서 사용자 이름 및 비밀번호(사용자가 가지고 있는 토큰)를 제공해야 합니다. 보조 인증을 위해 인증서의 사용자 이름을 사용할 수도 있습니다.이중 인증에 대한 자세한 내용은 CLI, 8.4 및 8.6을 사용하는 Cisco ASA 5500 Series 컨피그레이션 가이드를 참조하십시오.

관련 정보

- CLI, 8.4 및 8.6을 사용하는 Cisco ASA 5500 Series 컨피그레이션 가이드
- OpenLDAP 소프트웨어 2.4 관리자 가이드
- 개인 기업 번호
- 기술 지원 및 문서 – Cisco Systems