Exemplo de Configuração de 802.1x EAP-TLS com Comparação de Certificado Binário de Perfis AD e NAM

Contents

Introduction

Este documento descreve a configuração 802.1x com Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) e Access Control System (ACS), pois eles executam uma comparação de certificado binário entre um certificado de cliente fornecido pelo requerente e o mesmo certificado mantido no Microsoft Ative Diretory (AD). O perfil do AnyConnect Network Access Manager (NAM) é usado para personalização. A configuração de todos os componentes é apresentada neste documento, juntamente com cenários para solucionar problemas de configuração.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Topologia

- Suplicante 802.1x - Windows 7 com Cisco AnyConnect Secure Mobility Client versão 3.1.01065 (módulo NAM)
- Autenticador 802.1x - switch 2960
- Servidor de autenticação 802.1x - ACS versão 5.4
- ACS integrado ao Microsoft AD - Controlador de domínio - Windows 2008 Server

Detalhes da topologia

- ACS - 192.168.10.152
- 2960 - 192.168.10.10 (e0/0 - suplicante conectado)
- DC - 192.168.10.101
- Windows 7 - DHCP

Fluxo

A estação do Windows 7 tem o AnyConnect NAM instalado, que é usado como um suplicante para autenticar no servidor ACS com o método EAP-TLS. O switch com 802.1x atua como autenticador. O certificado do usuário é verificado pelo ACS e a autorização da política aplica políticas baseadas no Nome Comum (CN) do certificado. Além disso, o ACS obtém o certificado do usuário do AD e executa uma comparação binária com o certificado fornecido pelo requerente.

Configuração do Switch

O switch tem uma configuração básica. Por padrão, a porta está em quarentena na VLAN 666. Essa VLAN tem acesso restrito. Depois que o usuário é autorizado, a porta VLAN é reconfigurada.

```
aaa authentication login default group radius local
aaa authentication dot1x default group radius
aaa authorization network default group radius
dot1x system-auth-control

interface Ethernet0/0
switchport access vlan 666
switchport mode access
ip device tracking maximum 10
duplex auto
authentication event fail action next-method
authentication order dot1x mab
authentication port-control auto
dot1x pae authenticator
end

radius-server host 192.168.10.152 auth-port 1645 acct-port 1646 key cisco
```

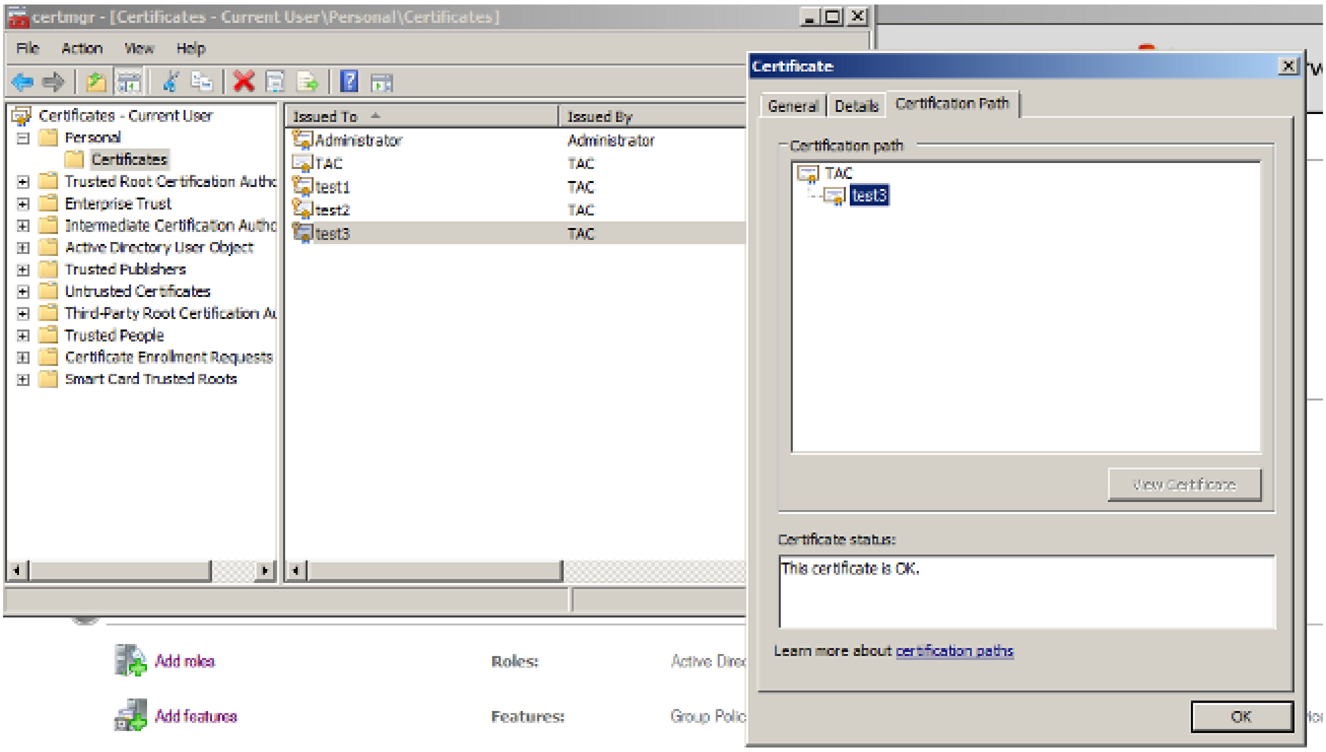
Preparação do certificado

Para EAP-TLS, é necessário um certificado para o requerente e para o servidor de autenticação. Este exemplo é baseado em certificados gerados pelo OpenSSL. A Autoridade de Certificação da Microsoft (AC) pode ser usada para simplificar a implantação em redes corporativas.

1. Para gerar a CA, digite estes comandos:
   ```
   openssl genrsa -des3 -out ca.key 1024
   openssl req -new -key ca.key -out ca.csr
   cp ca.key ca.key.org
   openssl rsa -in ca.key.org -out ca.key
   openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt
   ```
   O certificado CA é mantido no arquivo ca.crt e na chave privada (e desprotegida) no arquivo ca.key.
2. Gerar três certificados de usuário e um certificado para ACS, todos assinados por essa CA: CN=teste1CN=teste2CN=teste3CN=acs54O script para gerar um único certificado assinado pela CA da Cisco é:
   ```
   openssl genrsa -des3 -out server.key 1024
   openssl req -new -key server.key -out server.csr

   cp server.key server.key.org
   openssl rsa -in server.key.org -out server.key

   openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial
   -out server.crt -days 365
   openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
   -certfile ca.crt
   ```
   A chave privada está no arquivo server.key e o certificado está no arquivo server.crt. A versão pkcs12 está no arquivo server.pfx.
3. Clique duas vezes em cada certificado (arquivo .pfx) para importá-lo para o Controlador de domínio. No Controlador de Domínio, todos os três certificados devem ser confiáveis.



Issued To	Issued By
Administrator	Administrator
TAC	TAC
test1	TAC
test2	TAC
test3	TAC

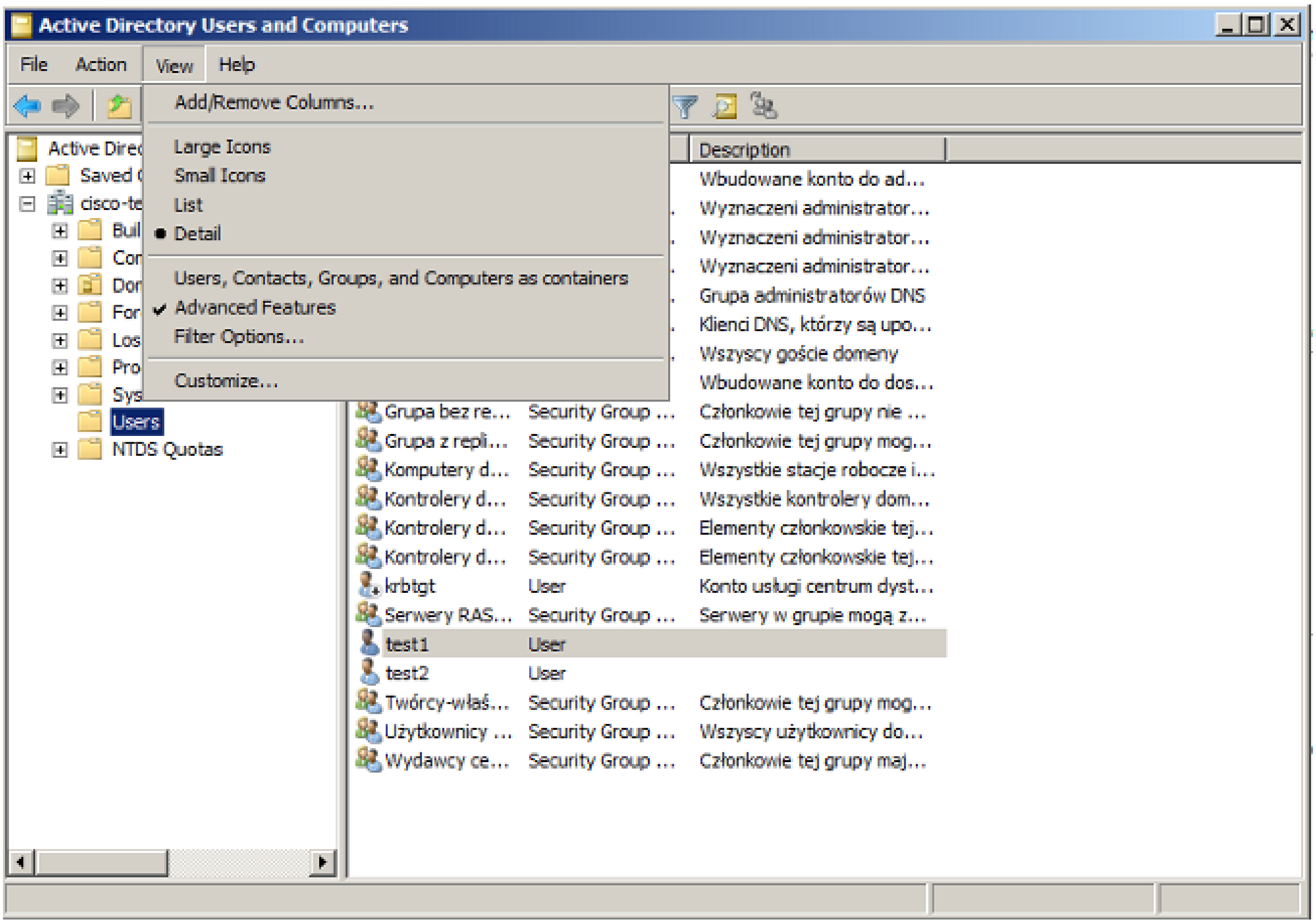
This certificate is OK.

O mesmo processo pode ser seguido no Windows 7 (suplicante) ou usar o Ative Diretory para enviar os certificados do usuário.

Configuração do controlador de domínio

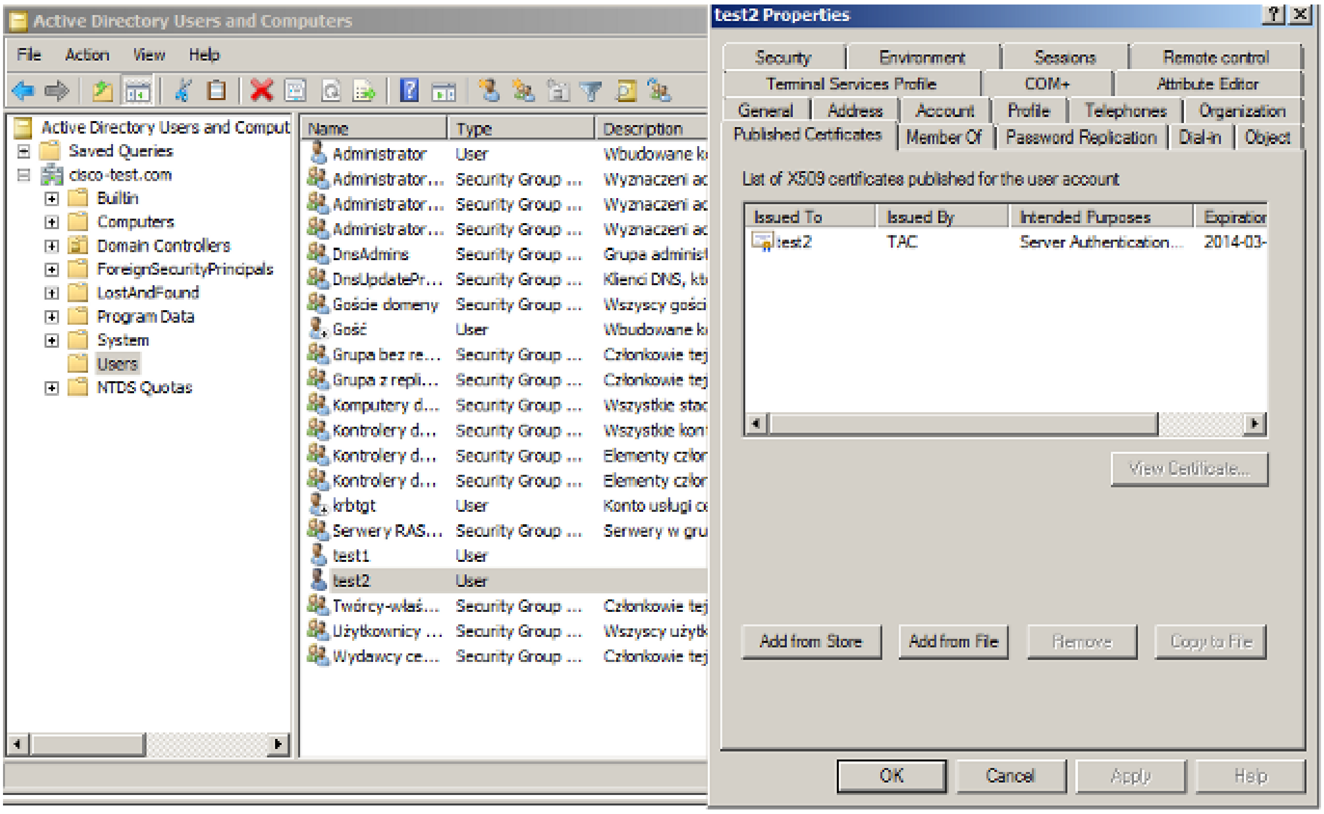
Énecessário mapear o certificado específico para o usuário específico no AD.

1. Em Usuários e Computadores do Ative Diretory, navegue até a pasta **Usuários**.
2. No menu Exibir, escolha **Recursos avançados**.



		Description
		Wbudowane konto do ad...
		Wyznaczeni administrator...
		Wyznaczeni administrator...
		Wyznaczeni administrator...
		Grupa administratorów DNS
		Klienci DNS, którzy są upo...
		Wszyscy goście domeny
		Wbudowane konto do dos...
Grupa bez re...	Security Group ...	Członkowie tej grupy nie ...
Grupa z repli...	Security Group ...	Członkowie tej grupy mog...
Komputery d...	Security Group ...	Wszystkie stacje robocze i...
Kontrolery d...	Security Group ...	Wszystkie kontrolery dom...
Kontrolery d...	Security Group ...	Elementy członkowskie tej...
Kontrolery d...	Security Group ...	Elementy członkowskie tej...
krbtgt	User	Konto usługi centrum dyst...
Serwery RAS...	Security Group ...	Serwery w grupie mogą z...
test1	User	
test2	User	
Twórcy-właś...	Security Group ...	Członkowie tej grupy mog...
Użytkownicy ...	Security Group ...	Wszyscy użytkownicy do...
Wydawcy ce...	Security Group ...	Członkowie tej grupy maj...

3. Adicione estes usuários: teste1teste 2teste 3**Note**: A senha não é importante.
4. Na janela Propriedades, escolha a guia **Certificados Publicados**. Escolha o certificado específico para o teste. Por exemplo, para test1, o CN do usuário é test1.**Note**: Não use o Mapeamento de nomes (clique com o botão direito do mouse no nome de usuário). É usado para serviços
diferentes.



Name	Type	Description
Administrator	User	Wbudowane k
Administrator...	Security Group ...	Wyznaczeni ac
Administrator...	Security Group ...	Wyznaczeni ac
Administrator...	Security Group ...	Wyznaczeni ac
DnsAdmins	Security Group ...	Grupa adminis
DnsUpdatePr...	Security Group ...	Klienci DNS, kt
Goście domeny	Security Group ...	Wszyscy gości
Gość	User	Wbudowane k
Grupa bez re...	Security Group ...	Członkowie tej
Grupa z repli...	Security Group ...	Członkowie tej
Komputery d...	Security Group ...	Wszystkie stac
Kontrolery d...	Security Group ...	Wszystkie kon
Kontrolery d...	Security Group ...	Elementy człor
Kontrolery d...	Security Group ...	Elementy człor
krbtgt	User	Konto usługi ce
Serwery RAS...	Security Group ...	Serwery w gru
test1	User	
test2	User	
Twórcy-właś...	Security Group ...	Członkowie tej
Użytkownicy ...	Security Group ...	Wszyscy użytk
Wydawcy ce...	Security Group ...	Członkowie tej

List of X509 certificates published for the user account

Issued To	Issued By	Intended Purposes	Expiratior
test2	TAC	Server Authentication...	2014-03-

Neste estágio, o certificado é vinculado a um usuário específico no AD. Isso pode ser verificado com o uso de ldapsearch:

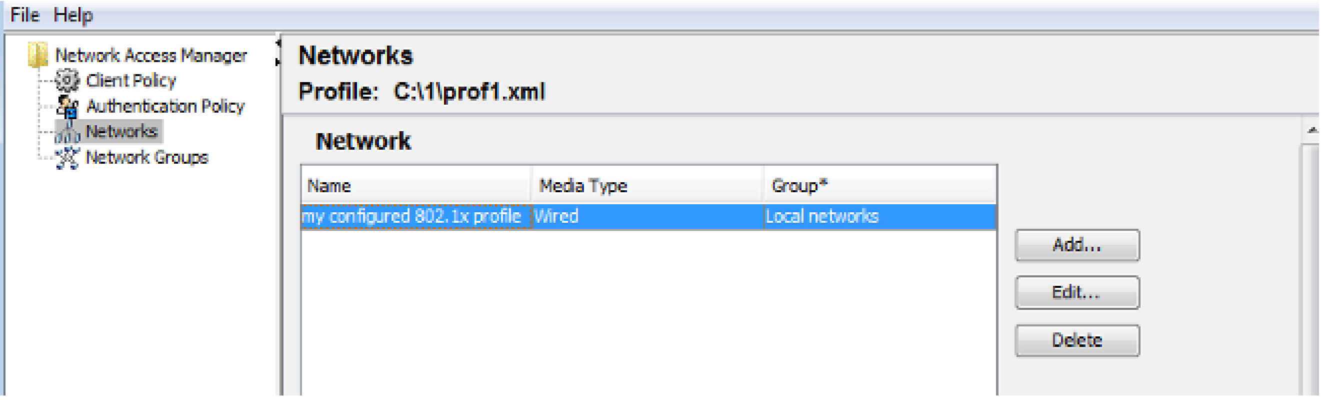
```
ldapsearch -h 192.168.10.101 -D "CN=Administrator,CN=Users,DC=cisco-test,DC=com" -w
Adminpass -b "DC=cisco-test,DC=com"
```

Os resultados de exemplo para o teste2 são os seguintes:

```
# test2, Users, cisco-test.com
dn: CN=test2,CN=Users,DC=cisco-test,DC=com
..................
userCertificate:: MIICuDCCAiGgAwIBAgIJAP6cPWHhMc2yMA0GCSqGSIb3DQEBBQUAMFYxCzAJ
BgNVBAYTAlBMMQwwCgYDVQQIDANNYXoxDzANBgNVBAcMBldhcnNhdzEMMAoGA1UECgwDVEFDMQwwC
gYDVQQLDANSQUMxDDAKBgNVBAMMA1RBQzAeFw0xMzAzMDYxMjUzMjdaFw0xNDAzMDYxMjUzMjdaMF
oxCzAJBgNVBAYTAlBMMQswCQYDVQQIDAJQTDEPMA0GA1UEBwwGS3Jha293MQ4wDAYDVQQKDAVDaXN
jbzENMAsGA1UECwwEQ29yZTEOMAwGA1UEAwwFdGVzdDIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMFQZywrGTQKL+LeI19ovNavCFSG2zt2HGs8qGPrf/h3o4IIvU+nN6aZPdkTdsjiuCeav8HYD
aRznaK1LURt1PeGtHlcTgcGZ1MwIGptimzG+h234GmPU59k4XSVQixARCDpMH8IBR9zOSWQLXe+kR
iZpXC444eKOh6wO/+yWb4bAgMBAAGjgYkwgYYwCwYDVR0PBAQDAgTwMHcGA1UdJQRwMG4GCCsGAQU
FBwMBBggrBgEFBQcDAgYKKwYBBAGCNwoDBAYLKwYBBAGCNwoDBAEGCCsGAQUFBwMBBggrBgEFBQgC
FQYKKwYBBAGCNwoDAQYKKwYBBAGCNxQCAQYJKwYBBAGCNxUGBggrBgEFBQcDAjANBgkqhkiG9w0BA
QUFAAOBgQCuXwAgcYqLNm6gEDTWm/OWmTFjPyA5KSDB76yVqZwr11ch7eZiNSmCtH7Pn+VILagf9o
tiFl5ttk9KX6tIvbeEC4X/mQVgAB3HuJH5sL1n/k2H10XCXKfMqMGrtsZrA64tMCcCeZRoxfAO94n
PulwF4nkcnu1xO/B7x+LpcjxjhQ==
```

Configuração do requerente

1. Instale este editor de perfil, anyconnect-profileeditor-win-3.1.00495-k9.exe.
2. Abra o Editor de perfis do Network Access Manager e configure o perfil específico.
3. Crie uma rede com fio específica.



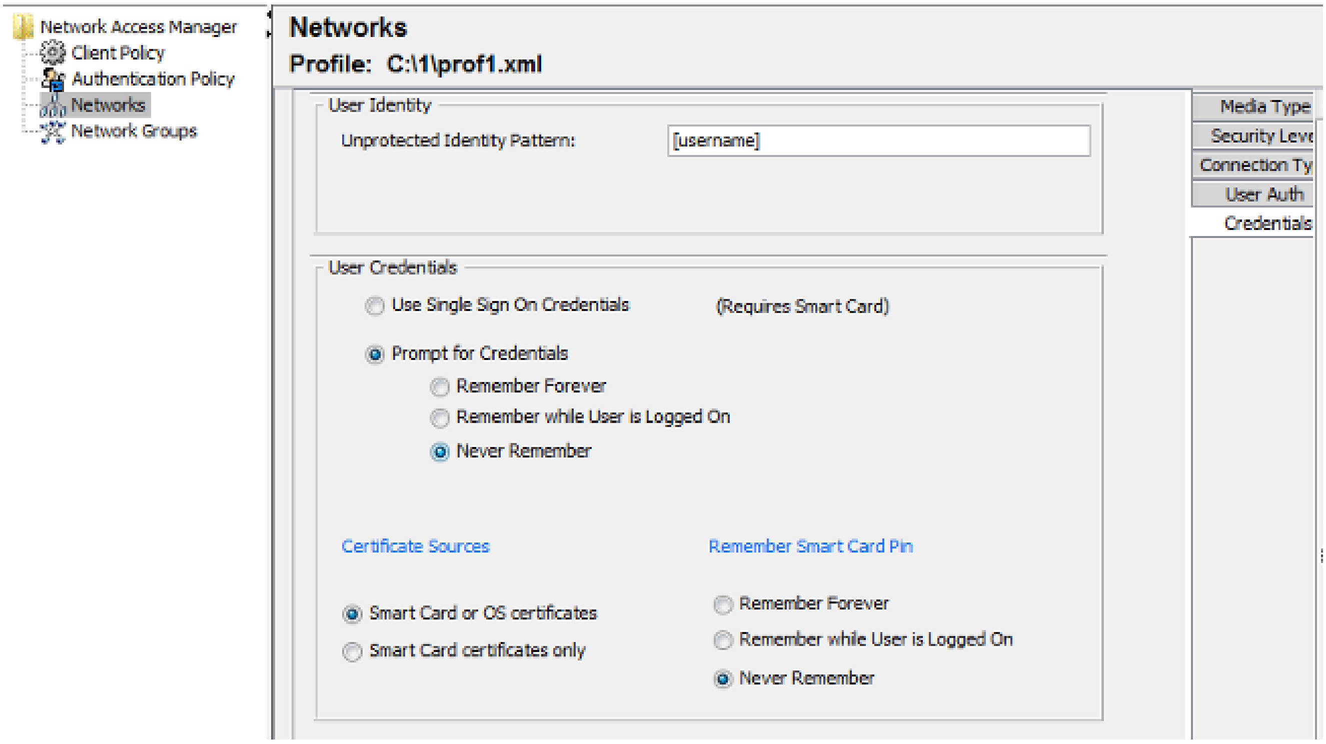
Networks

Profile: C:\1\prof1.xml

Network

Name	Media Type	Group*
my configured 802.1x profile	Wired	Local networks

Neste estágio, é muito importante dar ao usuário a opção de usar o certificado em cada autenticação. Não armazene essa opção em cache. Além disso, use o 'nome de usuário' como a id desprotegida. É importante lembrar que ela não é a mesma id usada pelo ACS para consultar o AD para o certificado. Essa id será configurada no ACS.



Networks

Profile: C:\1\prof1.xml

User Identity

Unprotected Identity Pattern: [username]

User Credentials

○ Use Single Sign On Credentials (Requires Smart Card)

● Prompt for Credentials

○ Remember Forever

○ Remember while User is Logged On

● Never Remember

Certificate Sources

● Smart Card or OS certificates

○ Smart Card certificates only

Remember Smart Card Pin

○ Remember Forever

○ Remember while User is Logged On

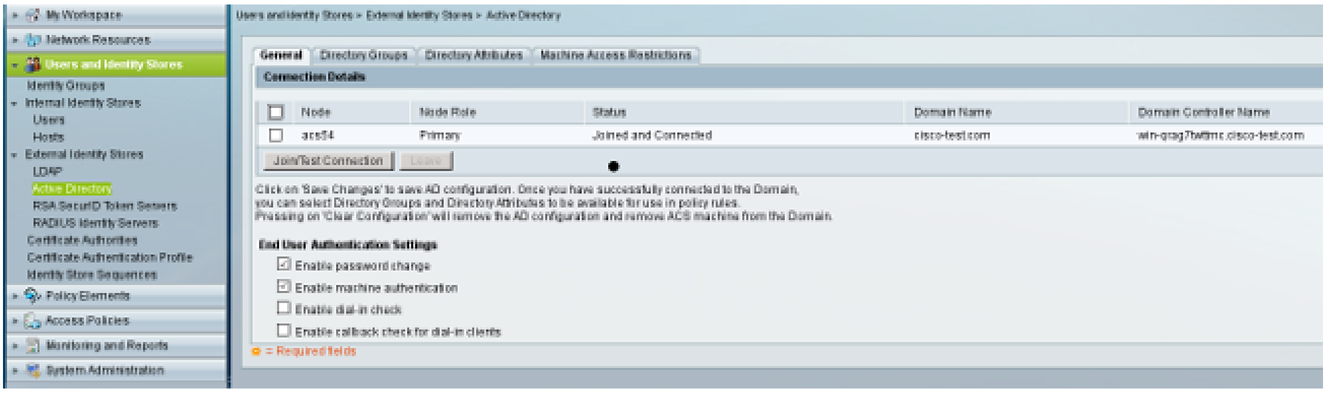
● Never Remember

4. Salve o arquivo .xml como c:\Users\All Users\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml.
5. Reinicie o serviço Cisco AnyConnect NAM.

Este exemplo mostrou uma implantação de perfil manual. O AD pode ser usado para implantar esse arquivo para todos os usuários. Além disso, o ASA pode ser usado para provisionar o perfil quando integrado a VPNs.

Configuração do ACS

1. Junte-se ao domínio do AD.



Users and Identity Stores > External Identity Stores > Active Directory

Connection Details

□	Node	Node Role	Status	Domain Name	Domain Controller Name
□	acs54	Primary	Joined and Connected	cisco-test.com	win-grag7bwmc.cisco-test.com

Click on 'Save Changes' to save AD configuration. Once you have successfully connected to the Domain, you can select Directory Groups and Directory Attributes to be available for use in policy rules.
Pressing on 'Clear Configuration' will remove the AD configuration and remove ACS machine from the Domain.

End User Authentication Settings

☑ Enable password change

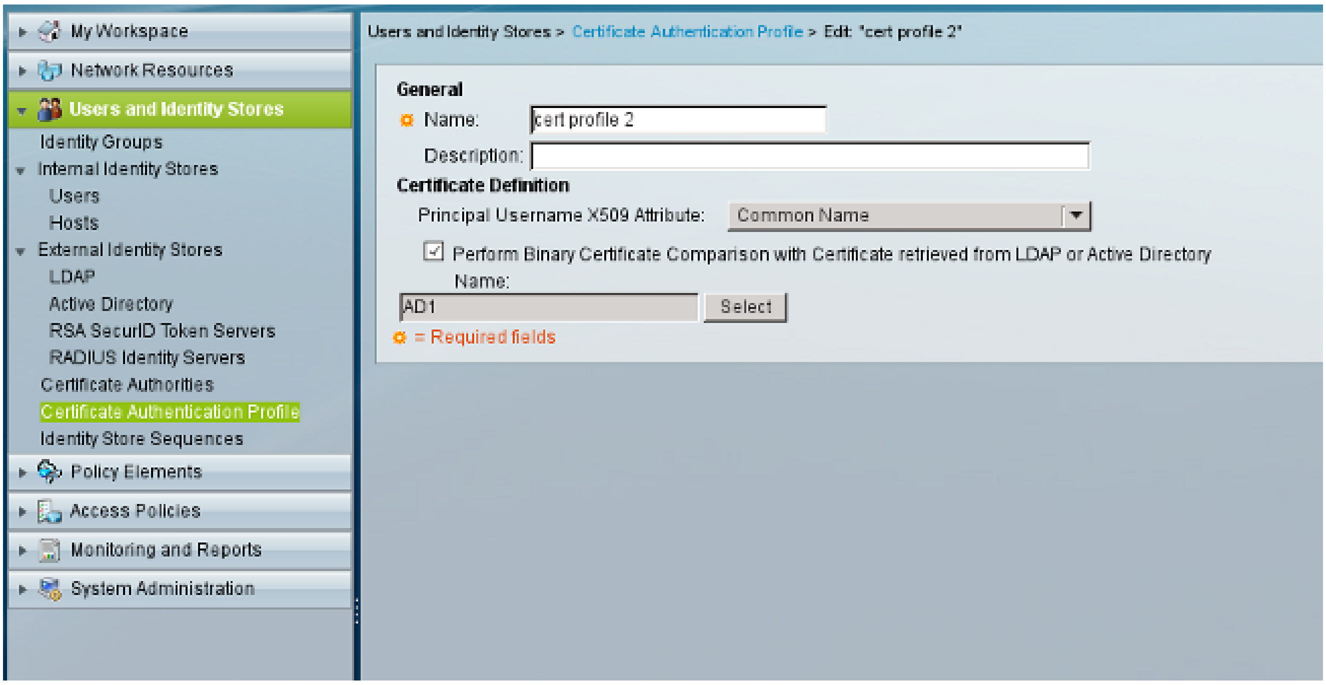
☑ Enable machine authentication

□ Enable dial-in check

□ Enable callback check for dial-in clients

● = Required fields

O ACS corresponde nomes de usuário do AD com o uso do campo CN do certificado recebido do requerente (nesse caso, é test1, test2 ou test3). A comparação binária também está habilitada. Isso força o ACS a obter o certificado do usuário do AD e o compara com o mesmo certificado recebido pelo requerente. Se não corresponder, a autenticação falhará.



Users and Identity Stores > Certificate Authentication Profile > Edit: "cert profile 2"

General

Name: cert profile 2

Description:

Certificate Definition

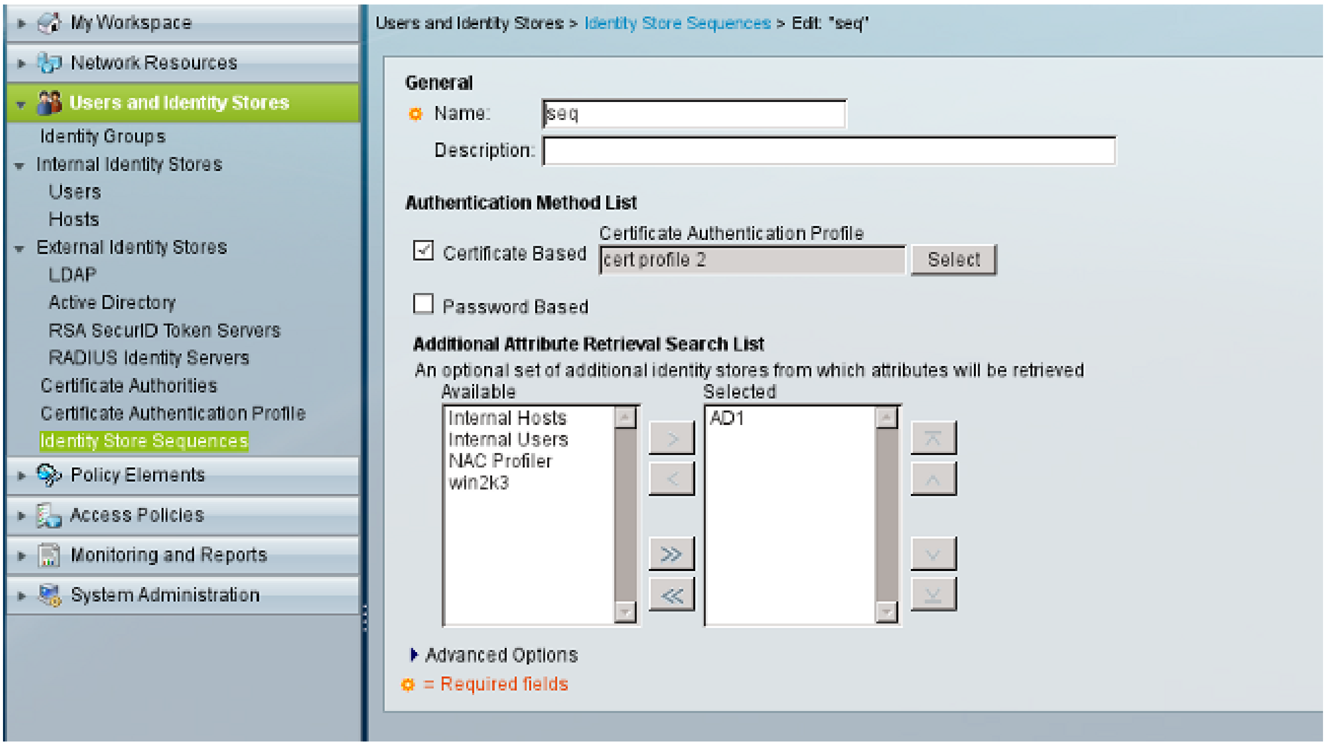
Principal Username X509 Attribute: Common Name

☑ Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory

Name: AD1

= Required fields

2. Configure as Sequências do Repositório de Identidades, que usa AD para autenticação baseada em certificado junto com o perfil de certificado.



Users and Identity Stores > Identity Store Sequences > Edit: "seq"

General

Name: seq

Description:

Authentication Method List

☑ Certificate Based — Certificate Authentication Profile: cert profile 2

□ Password Based

Additional Attribute Retrieval Search List

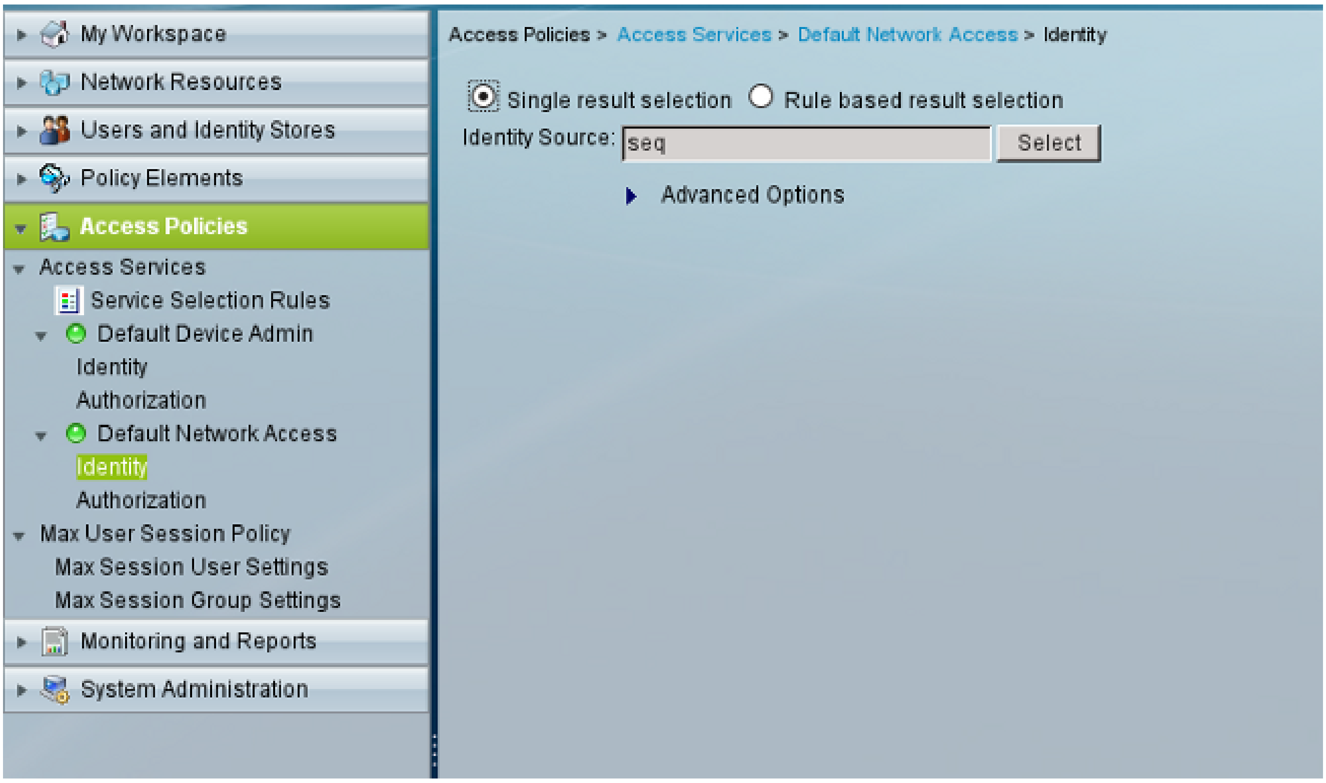
An optional set of additional identity stores from which attributes will be retrieved

Available: Internal Hosts, Internal Users, NAC Profiler, win2k3

Selected: AD1

= Required fields

Isso é usado como a origem da identidade na política de identidade RADIUS.

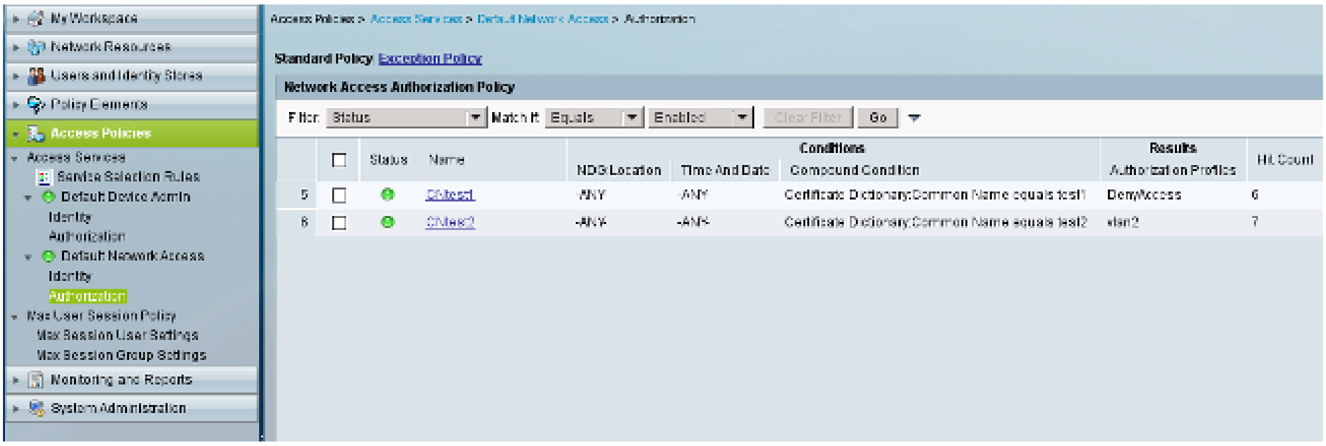


Access Policies > Access Services > Default Network Access > Identity

● Single result selection ○ Rule based result selection

Identity Source: seq

3. Configure duas políticas de autorização. A primeira política é usada para test1 e nega acesso a esse usuário. A segunda política é usada para o teste 2 e permite acesso com o perfil da
VLAN2.



Access Policies > Access Services > Default Network Access > Authorization

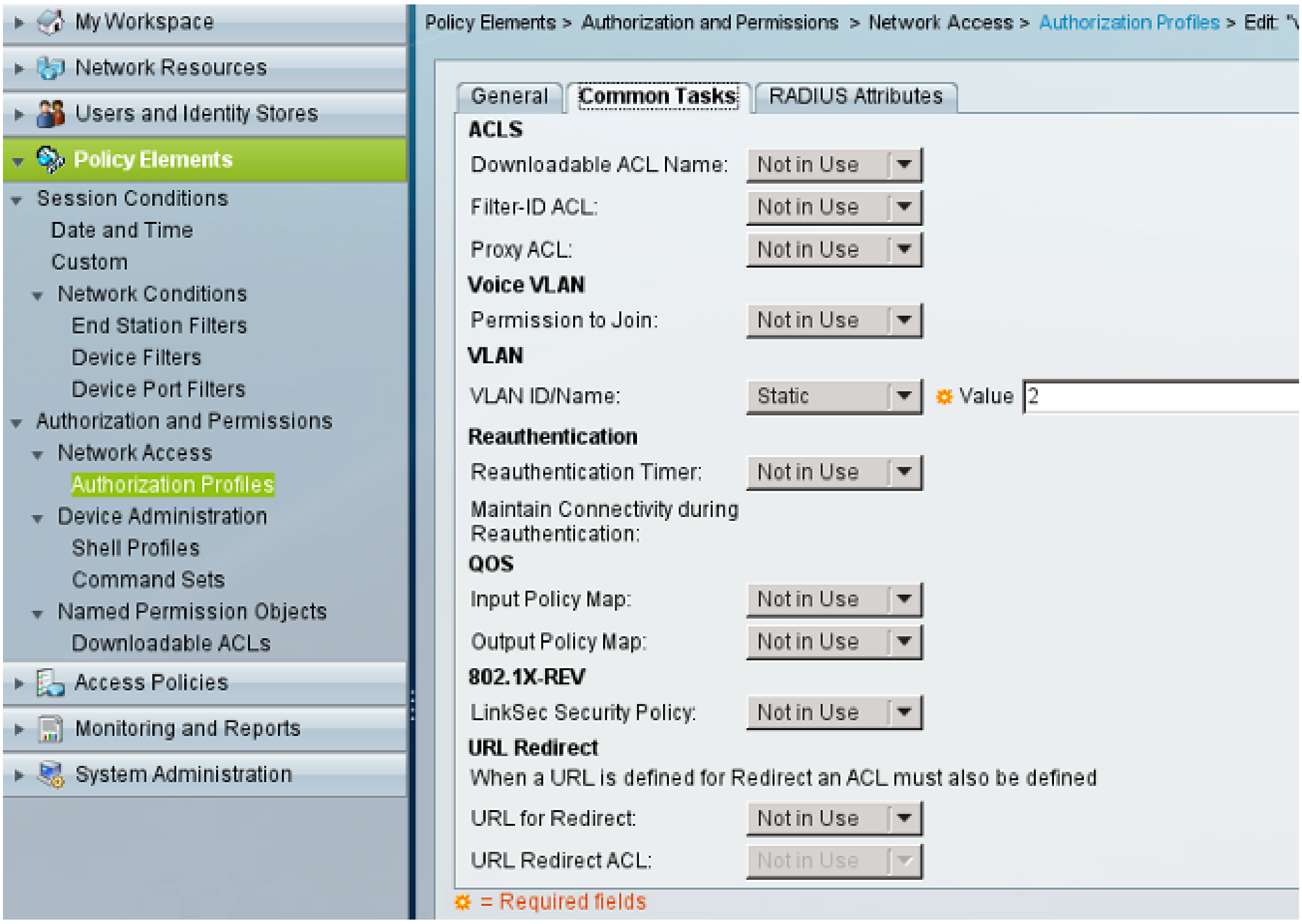
Standard Policy Exception Policy

Network Access Authorization Policy

Filter: Status Match if: Equals Enabled

				Conditions			Results	
	□	Status	Name	NDG:Location	Time And Date	Compound Condition	Authorization Profiles	Hit Count
5	□	●	CNtest1	-ANY-	-ANY-	Certificate Dictionary:Common Name equals test1	DenyAccess	6
6	□	●	CNtest2	-ANY-	-ANY-	Certificate Dictionary:Common Name equals test2	vlan2	7

VLAN2 é o perfil de autorização que retorna atributos RADIUS que vinculam o usuário à VLAN2 no
switch.



Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "\

ACLS

Downloadable ACL Name: Not in Use

Filter-ID ACL: Not in Use

Proxy ACL: Not in Use

Voice VLAN

Permission to Join: Not in Use

VLAN

VLAN ID/Name: Static ✱ Value 2

Reauthentication

Reauthentication Timer: Not in Use

Maintain Connectivity during Reauthentication:

QOS

Input Policy Map: Not in Use

Output Policy Map: Not in Use

802.1X-REV

LinkSec Security Policy: Not in Use

URL Redirect

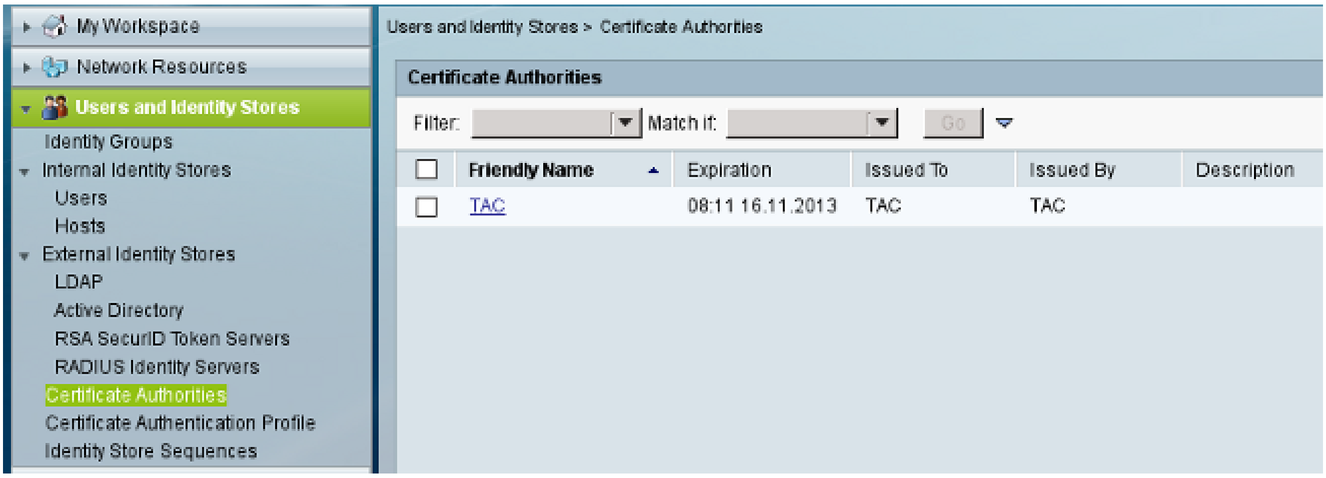
When a URL is defined for Redirect an ACL must also be defined

URL for Redirect: Not in Use

URL Redirect ACL: Not in Use

✱ = Required fields

4. Instale o certificado CA no ACS.

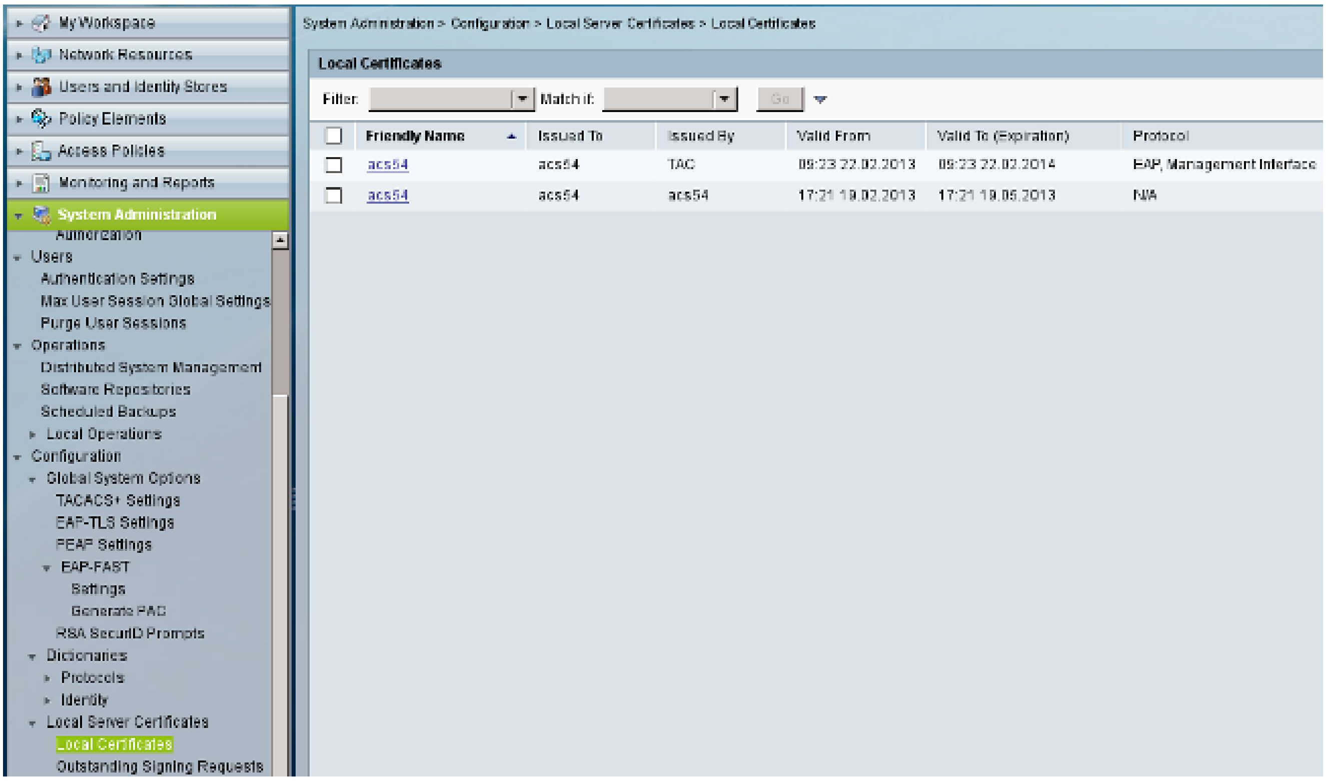


Users and Identity Stores > Certificate Authorities

Certificate Authorities

	Friendly Name	Expiration	Issued To	Issued By	Description
□	TAC	08:11 16.11.2013	TAC	TAC	

5. Gerar e instalar o certificado (para uso do Extensible Authentication Protocol) assinado pela CA da Cisco para ACS.



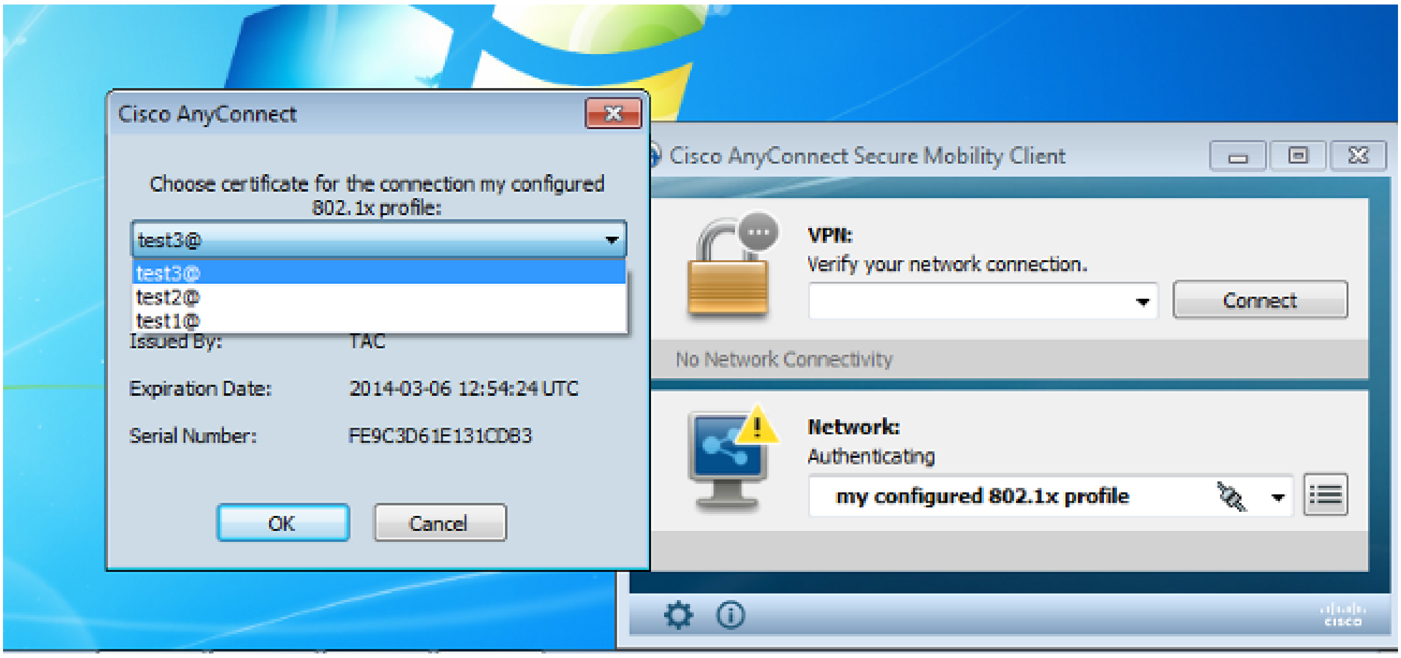
System Administration > Configuration > Local Server Certificates > Local Certificates

Local Certificates

□	Friendly Name	Issued To	Issued By	Valid From	Valid To (Expiration)	Protocol
□	acs54	acs54	TAC	09:23 22.02.2013	09:23 22.02.2014	EAP, Management Interface
□	acs54	acs54	acs54	17:21 19.02.2013	17:21 19.05.2013	N/A

Verificar

Éuma boa prática desativar o serviço 802.1x nativo no suplicante do Windows 7, pois o AnyConnect NAM é usado. Com o perfil configurado, o cliente tem permissão para selecionar um certificado específico.



Choose certificate for the connection my configured 802.1x profile:

test3@

test3@
test2@
test1@

Issued By: TAC

Expiration Date: 2014-03-06 12:54:24 UTC

Serial Number: FE9C3D61E131CDB3

VPN:
Verify your network connection.

No Network Connectivity

Network:
Authenticating

my configured 802.1x profile

Quando o certificado test2 é usado, o switch recebe uma resposta de sucesso junto com os atributos RADIUS.

```
00:02:51: %DOT1X-5-SUCCESS: Authentication successful for client
(0800.277f.5f64) on Interface Et0/0
00:02:51: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x'
for client (0800.277f.5f64) on Interface Et0/0
```

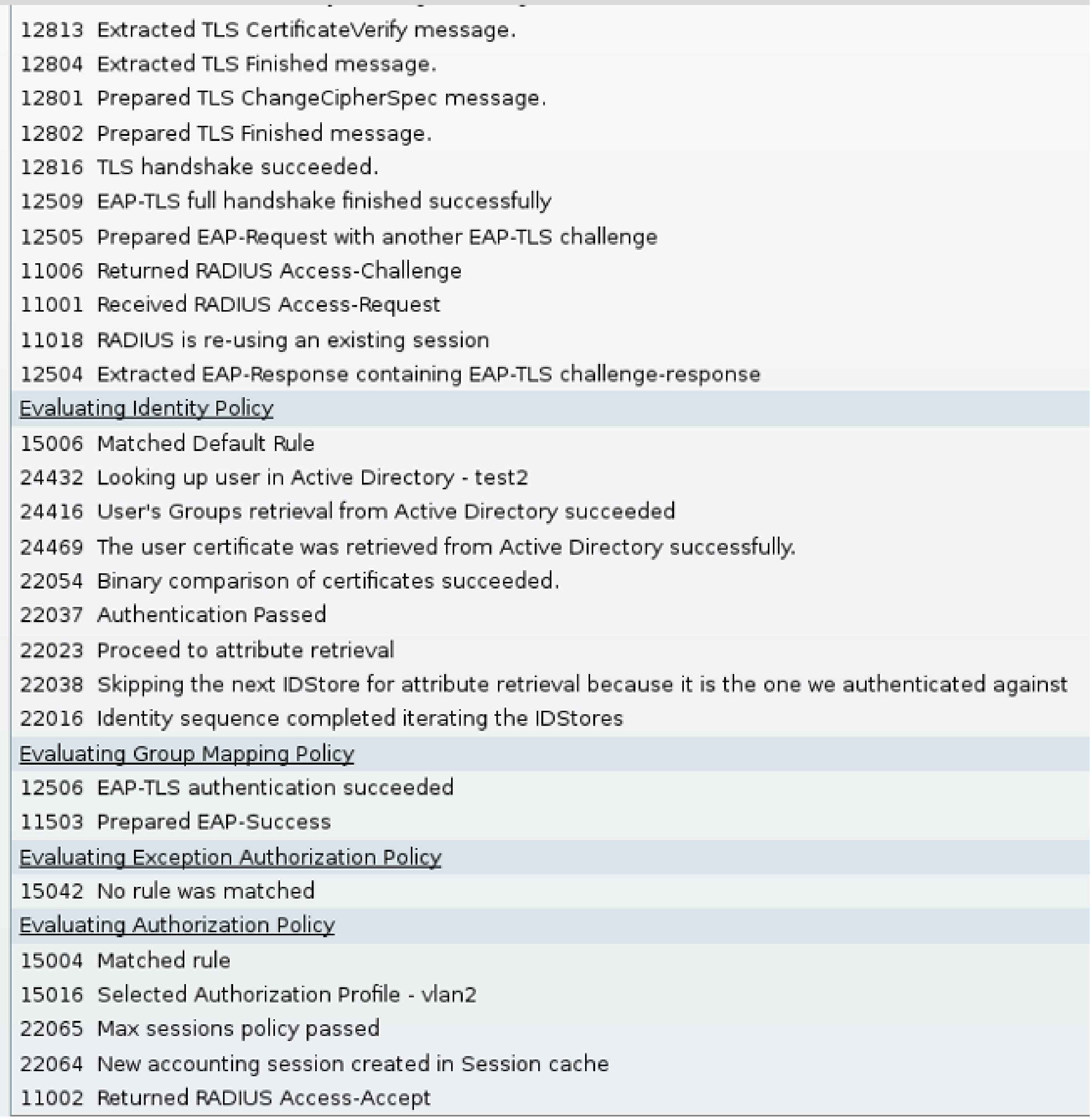
```
switch#
00:02:51: %EPM-6-POLICY_REQ: IP=0.0.0.0| MAC=0800.277f.5f64|
       AUDITSESID=C0A80A0A00000001000215F0| AUTHTYPE=DOT1X|
       EVENT=APPLY

switch#show authentication sessions interface e0/0
           Interface:  Ethernet0/0
          MAC Address:  0800.277f.5f64
           IP Address:  Unknown
           User-Name:  test2
           Status:  Authz Success
           Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  2
      Session timeout:  N/A
         Idle timeout:  N/A
   Common Session ID:  C0A80A0A00000001000215F0
      Acct Session ID:  0x00000005
           Handle:  0xE8000002

Runnable methods list:
      Method   State
      dot1x    Authc Succes
```

Observe que a VLAN 2 foi atribuída. É possível adicionar outros atributos RADIUS a esse perfil de autorização no ACS (como a lista de controle de acesso avançado ou os temporizadores de reautorização).

Os registros no ACS são os seguintes:

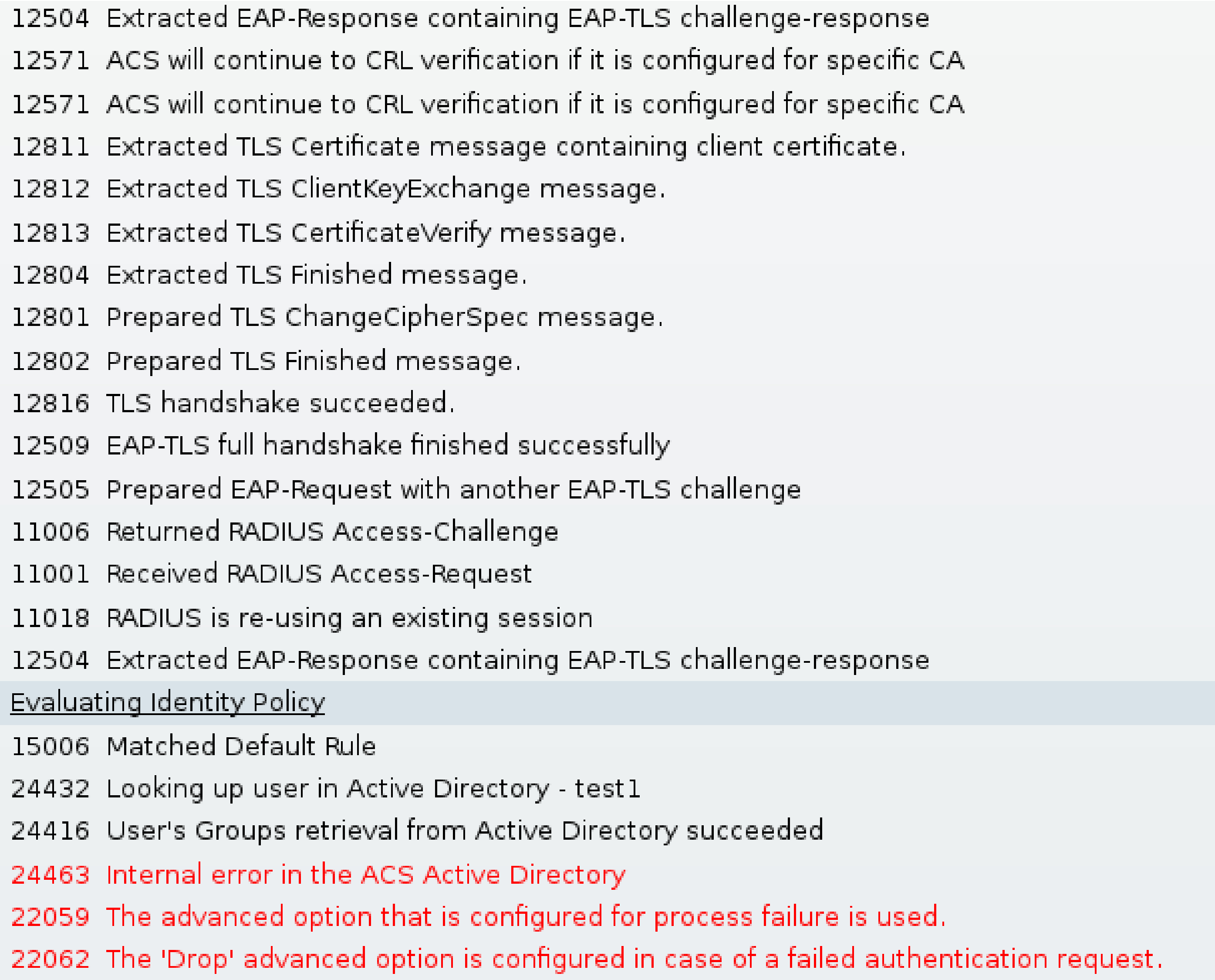


```
12813  Extracted TLS CertificateVerify message.
12804  Extracted TLS Finished message.
12801  Prepared TLS ChangeCipherSpec message.
12802  Prepared TLS Finished message.
12816  TLS handshake succeeded.
12509  EAP-TLS full handshake finished successfully
12505  Prepared EAP-Request with another EAP-TLS challenge
11006  Returned RADIUS Access-Challenge
11001  Received RADIUS Access-Request
11018  RADIUS is re-using an existing session
12504  Extracted EAP-Response containing EAP-TLS challenge-response
Evaluating Identity Policy
15006  Matched Default Rule
24432  Looking up user in Active Directory - test2
24416  User's Groups retrieval from Active Directory succeeded
24469  The user certificate was retrieved from Active Directory successfully.
22054  Binary comparison of certificates succeeded.
22037  Authentication Passed
22023  Proceed to attribute retrieval
22038  Skipping the next IDStore for attribute retrieval because it is the one we authenticated against
22016  Identity sequence completed iterating the IDStores
Evaluating Group Mapping Policy
12506  EAP-TLS authentication succeeded
11503  Prepared EAP-Success
Evaluating Exception Authorization Policy
15042  No rule was matched
Evaluating Authorization Policy
15004  Matched rule
15016  Selected Authorization Profile - vlan2
22065  Max sessions policy passed
22064  New accounting session created in Session cache
11002  Returned RADIUS Access-Accept
```

Troubleshoot

Configurações de hora inválidas no ACS

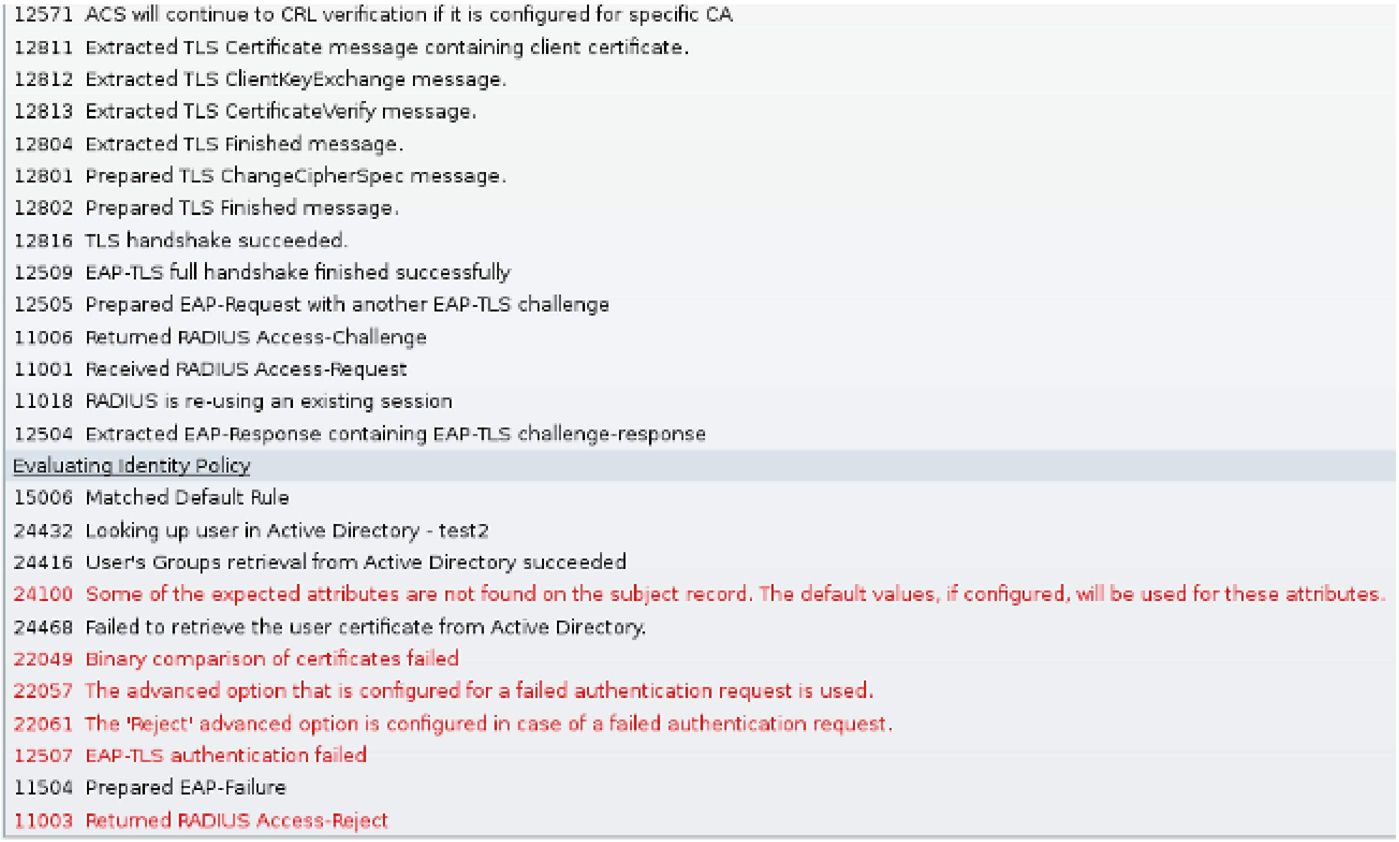
Erro possível - erro interno no Ative Diretory do ACS



```
12504  Extracted EAP-Response containing EAP-TLS challenge-response
12571  ACS will continue to CRL verification if it is configured for specific CA
12571  ACS will continue to CRL verification if it is configured for specific CA
12811  Extracted TLS Certificate message containing client certificate.
12812  Extracted TLS ClientKeyExchange message.
12813  Extracted TLS CertificateVerify message.
12804  Extracted TLS Finished message.
12801  Prepared TLS ChangeCipherSpec message.
12802  Prepared TLS Finished message.
12816  TLS handshake succeeded.
12509  EAP-TLS full handshake finished successfully
12505  Prepared EAP-Request with another EAP-TLS challenge
11006  Returned RADIUS Access-Challenge
11001  Received RADIUS Access-Request
11018  RADIUS is re-using an existing session
12504  Extracted EAP-Response containing EAP-TLS challenge-response
Evaluating Identity Policy
15006  Matched Default Rule
24432  Looking up user in Active Directory - test1
24416  User's Groups retrieval from Active Directory succeeded
24463  Internal error in the ACS Active Directory
22059  The advanced option that is configured for process failure is used.
22062  The 'Drop' advanced option is configured in case of a failed authentication request.
```

Nenhum certificado configurado e vinculado no AD DC

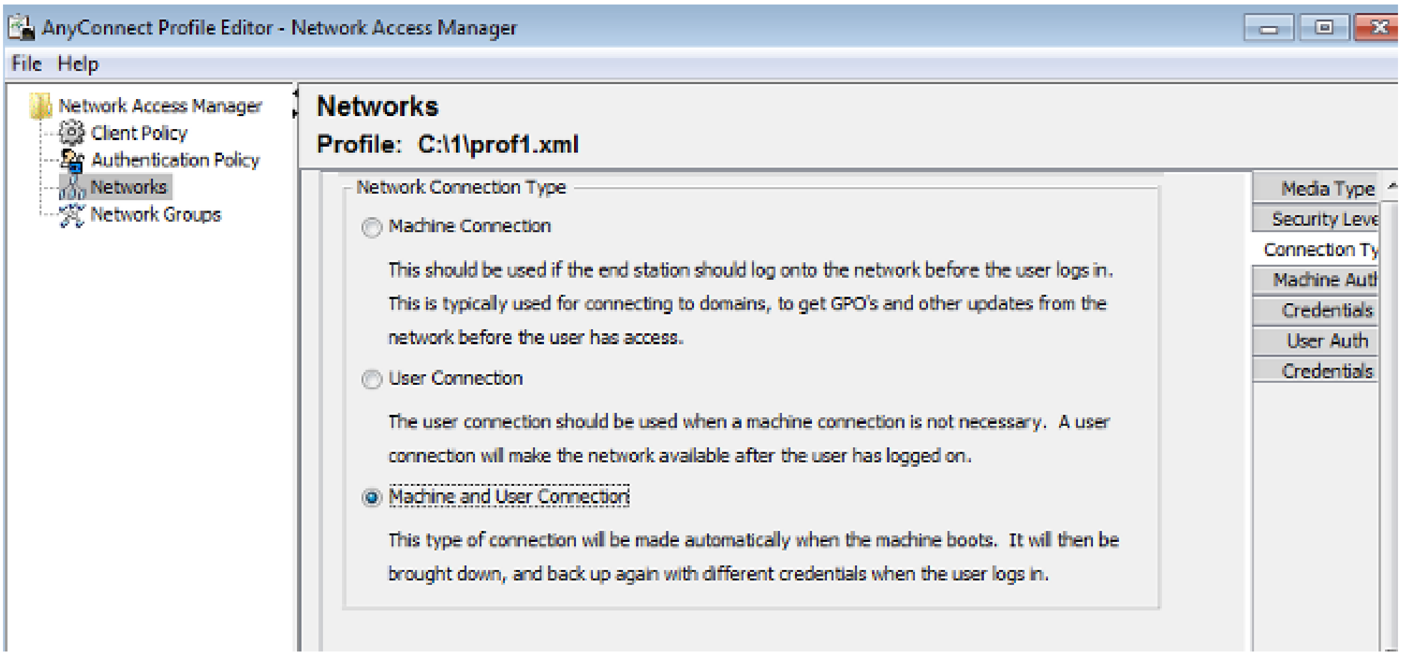
Erro possível - falha ao recuperar o certificado de usuário do Ative Diretory



```
12571  ACS will continue to CRL verification if it is configured for specific CA
12811  Extracted TLS Certificate message containing client certificate.
12812  Extracted TLS ClientKeyExchange message.
12813  Extracted TLS CertificateVerify message.
12804  Extracted TLS Finished message.
12801  Prepared TLS ChangeCipherSpec message.
12802  Prepared TLS Finished message.
12816  TLS handshake succeeded.
12509  EAP-TLS full handshake finished successfully
12505  Prepared EAP-Request with another EAP-TLS challenge
11006  Returned RADIUS Access-Challenge
11001  Received RADIUS Access-Request
11018  RADIUS is re-using an existing session
12504  Extracted EAP-Response containing EAP-TLS challenge-response
Evaluating Identity Policy
15006  Matched Default Rule
24432  Looking up user in Active Directory - test2
24416  User's Groups retrieval from Active Directory succeeded
24100  Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.
24468  Failed to retrieve the user certificate from Active Directory.
22049  Binary comparison of certificates failed
22057  The advanced option that is configured for a failed authentication request is used.
22061  The 'Reject' advanced option is configured in case of a failed authentication request.
12507  EAP-TLS authentication failed
11504  Prepared EAP-Failure
11003  Returned RADIUS Access-Reject
```

Personalização do perfil NAM

Nas redes corporativas, recomenda-se autenticar com o uso de certificados de máquina e de usuário.Nesse cenário, recomenda-se usar o modo 802.1x aberto no switch com VLAN restrita. Após a reinicialização da máquina para 802.1x, a primeira sessão de autenticação é iniciada e autenticada com o uso do certificado da máquina do AD. Depois que o usuário fornecer credenciais e fizer logon no domínio, a segunda sessão de autenticação será iniciada com o certificado do usuário. O usuário é colocado na VLAN correta (confiável) com acesso total à rede. Ele é bem integrado ao Identity Services Engine (ISE).



Networks

Profile: C:\1\prof1.xml

Network Connection Type

○ Machine Connection

This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

○ User Connection

The user connection should be used when a machine connection is not necessary. A user connection will make the network available after the user has logged on.

● Machine and User Connection

This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

Em seguida, é possível configurar autenticações separadas das guias Autenticação da máquina e

Autenticação do usuário.

Se o modo 802.1x aberto não for aceitável no switch, é possível usar o modo 802.1x antes que o recurso de logon seja configurado na Política do cliente.

Informações Relacionadas

- Guia do usuário do Cisco Secure Access Control System 5.3
- Guia do administrador do Cisco AnyConnect Secure Mobility Client, versão 3.0
- AnyConnect Secure Mobility Client 3.0: Gerenciador de acesso à rede e Editor de perfis no Windows
- Suporte Técnico e Documentação - Cisco Systems