

Certificate DN Group Matching Configuration on the Cisco VPN 3000 Concentrator

Document ID: 26324

Introduction

Before You Begin

Conventions

Prerequisites

Components Used

Network Diagram

Configure the Certificate DN Group Matching Feature

Step-by-Step Instructions to Configure the VPN 3000 Concentrator

VPN Client Certificate

Verify

Troubleshoot

Related Information

Introduction

This document demonstrates how to configure the Certificate Distinguished Name (DN) Group Matching feature introduced in Cisco VPN 3000 Concentrator version 3.6.

Prior to version 3.6, the VPN 3000 Concentrator tried to match the Organizational Unit (OU) field in the remote VPN identity certificate with a locally configured VPN group name, when RSA signatures were used as the Internet Key Exchange (IKE) authentication method. The Certificate DN Group Matching feature provides users more flexibility to map VPN users to different VPN groups defined on the concentrators, using different fields in the certificate.

Before You Begin

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Prerequisites

To learn more about the basic configuration steps for enrolling Cisco VPN Clients and VPN 3000 Concentrators to a Certification Authentication (CA) server, and how to set up a remote-access VPN tunnel between client and concentrators using certificates, refer to:

- Configuring the VPN Client 3.0.x to Get a Digital Certificate
- Configuring the VPN 3000 Concentrator to Communicate with the VPN Client Using Certificates
- Configuring the Cisco VPN 3000 Concentrator 3.5.x to Get a Digital Certificate Using SCEP

Components Used

The information in this document is based on these software and hardware versions:

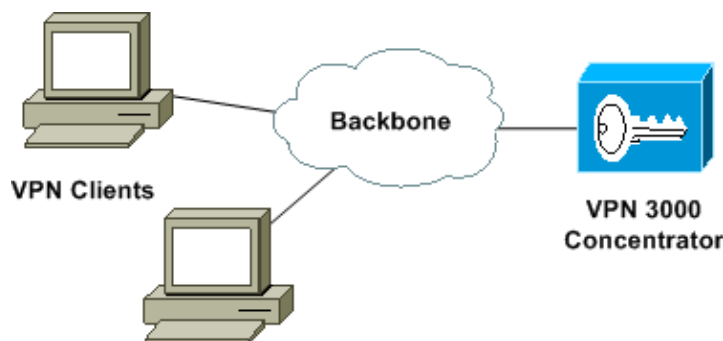
- Cisco VPN 3000 Concentrator version 3.6

- Cisco VPN Client version 3.6
- Microsoft CA server running on Microsoft Windows 2000 server

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Network Diagram

This document uses this network setup:



Configure the Certificate DN Group Matching Feature

This section demonstrates how to configure the Certificate DN Group Matching policies and rules to map VPN Clients to VPN groups defined locally on VPN Concentrators.

This is the certificate matching policy that is defined on the VPN Concentrators:

- VPN users from the San Jose Technical Assistance Center (TAC) VPN team are mapped to a VPN group called "SJVPNusers."
- VPN users from the Research Triangle Park (RTP) TAC VPN team are mapped to a VPN group called "RTPVPNusers."
- All other VPN users with valid certificates are mapped to a VPN group called "OtherVPNusers."

To create VPN groups on VPN Concentrators for remote VPN Clients using certificates, refer to the links in the Prerequisites section.

Step-by-Step Instructions to Configure the VPN 3000 Concentrator

Define the Certificate DN Group Matching Policy

The Certificate DN Group Matching rules are checked first when the VPN Concentrator verifies the VPN Client certificate to see if there is a match. If there is a match, the VPN user is mapped to the corresponding VPN group. Otherwise, the VPN user is mapped to the default group (in this example, "OtherVPNusers").

Configuration | Policy Management | Certificate Group Matching | Policy

Configure the policy for certificate group matching. The VPN Concentrator processes the policies in the order listed below until it finds a match.

Match Group from Rules Check to use configured rules to match a certificate to a group.

Obtain Group from OU Check to use the certificate OU field to determine the group.

Default to Group Check to use a default group for certificate users. Choose the default group from the drop down menu.

Define the Certificate DN Group Matching Rules

To define the Certificate DN Group Matching rules, complete these steps:

1. Go to **Configuration > Policy Management > Certificate Group Matching > Rules > Add** to define the first rule.

In the examples, VPN users from the San Jose TAC VPN team are mapped to a VPN group called "SJVPNusers."

2. Check the **Enable** box to enable the rule.
3. Specify the group to which the rule applies (in this case, "SJVPNusers").
4. Define the first criteria. Select from the **Distinguished Name** and **Operator** pull-down menus, and fill in the Value field (in this example, look for any instance of "San Jose" contained in the State/Province field in the certificate DN).

Configuration | Policy Management | Certificate Group Matching | Rules | Add

Create a new rule for certificate group matching from the fields below. A rule contains a group name and matching criteria that define the group. The VPN Concentrator checks the information in the certificate against these criteria; all the criteria must match the certificate to establish the group.

Note that the Value string must be enclosed in double quotes. These quotes are added automatically.

You can also create a rule by entering its text directly in the **Matching Criterion** box. If you create a rule in this way, separate the components with commas. Also, be sure to add double quotes around the value. If the value itself contains double quotes, replace them with two double quotes. For example, enter the value "Tech" Eng as: ""Tech"" Eng". An example of a matching criterion is: OU="Engineering",ISSUER-O="Cisco"

Enable Check to enable the rule.

Group Select the group to which this rule applies.

Distinguished Name	Operator	Value
<input type="text" value="Subject"/>	<input type="text" value="State/Province (SP)"/>	<input type="text" value="Contains (*)"/>
		<input type="text" value="San Jose"/> <input type="button" value="Append"/>

Matching Criterion

5. Click **Append** to update the Matching Criterion field. Click **Add** to continue.

Configuration | Policy Management | Certificate Group Matching | Rules | Add

Create a new rule for certificate group matching from the fields below. A rule contains a group name and matching criteria that define the group. The VPN Concentrator checks the information in the certificate against these criteria; all the criteria must match the certificate to establish the group.

Note that the Value string must be enclosed in double quotes. These quotes are added automatically.

You can also create a rule by entering its text directly in the **Matching Criterion** box. If you create a rule in this way, separate the components with commas. Also, be sure to add double quotes around the value. If the value itself contains double quotes, replace them with two double quotes. For example, enter the value *Tech Eng* as: `""Tech"" Eng`. An example of a matching criterion is: `OU="Engineering",ISSUER-O="Cisco"`

Enable Check to enable the rule.

Group Select the group to which this rule applies.

Distinguished Name	Operator	Value
<input type="text" value="Subject"/> <input type="text" value="CommonName (CN)"/>	<input type="text" value="Equals (-)"/>	<input type="text"/>

Matching Criterion

- Again, while using the same Group within the same Rule, append OU = Equals(*) TACVPN in the rule. Click **Add**.

Configuration | Policy Management | Certificate Group Matching | Rules | Add

Create a new rule for certificate group matching from the fields below. A rule contains a group name and matching criteria that define the group. The VPN Concentrator checks the information in the certificate against these criteria; all the criteria must match the certificate to establish the group.

Note that the Value string must be enclosed in double quotes. These quotes are added automatically.

You can also create a rule by entering its text directly in the **Matching Criterion** box. If you create a rule in this way, separate the components with commas. Also, be sure to add double quotes around the value. If the value itself contains double quotes, replace them with two double quotes. For example, enter the value *Tech Eng* as: `""Tech"" Eng`. An example of a matching criterion is: `OU="Engineering",ISSUER-O="Cisco"`

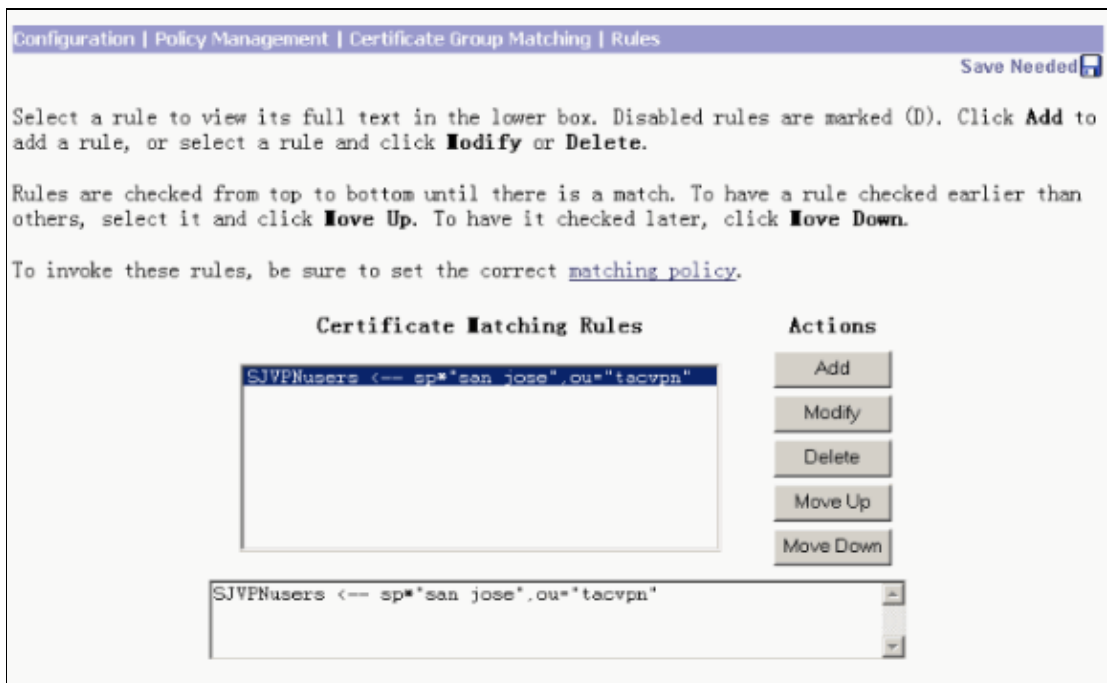
Enable Check to enable the rule.

Group Select the group to which this rule applies.

Distinguished Name	Operator	Value
<input type="text" value="Subject"/> <input type="text" value="Organizational Unit (OU)"/>	<input type="text" value="Equals (-)"/>	<input type="text" value="TACVPN"/>

Matching Criterion

- Verify the first rule by selecting the rule in the Certificate Matching Rules list. The corresponding rule parameters are displayed in the field below.



8. Follow the same procedure to define the remaining rules.

In the next example, the second rule maps VPN users from the RTP TAC VPN team to a VPN group called "RTPVPNusers."



VPN Client Certificate

This is what the DN might look like in a VPN Client certificate. The Certificate Group Matching rule, defined above, uses "OU" and "ST" in the subject DN.



Verify

This section provides information you can use to confirm that your configuration is working properly.

This is the event log collected on the VPN Concentrator during a successful IKE negotiation. In this case, a VPN user from RTP is trying to connect to the concentrator using certificates. The DN of the VPN Client certificate has OU = TACVPN and ST = RTP,NC.

According to the event log, the VPN Concentrator first checks the Certificate DN Group Matching rules one by one, according to the order defined. When there is a match, the VPN Client is mapped to the corresponding VPN group (in this example, RTPVPNusers).

```
3 08/15/2002 15:19:57.770 SEV=5 IKE/21 RPT=18 171.69.89.90
No Group found by matching IP Address of Cert peer 171.69.89.90

4 08/15/2002 15:19:57.770 SEV=5 CERT/110 RPT=21
Group match for cert peer 171.69.89.90 failed using rule
sp*"san jose",ou="tacvpn"

6 08/15/2002 15:19:57.770 SEV=5 CERT/110 RPT=22
Group match for cert peer 171.69.89.90 succeeded using rule
SP*"rtp",ou="tacvpn"

7 08/15/2002 15:19:57.770 SEV=5 CERT/105 RPT=10
Group [RTPVPNusers] found for cert peer 171.69.89.90 by group match rule
SP*"rtp",ou="tacvpn"

9 08/15/2002 15:19:57.880 SEV=5 IKE/79 RPT=9 171.69.89.90
Group [RTPVPNusers]
Validation of certificate successful
(CN=RTPvpuser1, SN=0EDA5052000000000039)

11 08/15/2002 15:20:06.180 SEV=4 IKE/52 RPT=6 171.69.89.90
Group [RTPVPNusers] User [rtpvpuser1]
User (rtpvpuser1) authenticated.

12 08/15/2002 15:20:06.200 SEV=6 IKE/130 RPT=7 171.69.89.90
Group [RTPVPNusers] User [rtpvpuser1]
Received unsupported transaction mode attribute: 5
```

14 08/15/2002 15:20:06.200 SEV=5 IKE/184 RPT=7 171.69.89.90
Group [RTPVPNusers] User [rtvpvnpuser1]
Client OS: WinNT
Client Application Version: 3.6 (Rel)

16 08/15/2002 15:20:06.240 SEV=4 IKE/119 RPT=14 171.69.89.90
Group [RTPVPNusers] User [rtvpvnpuser1]
PHASE 1 COMPLETED

17 08/15/2002 15:20:06.240 SEV=6 IKE/121 RPT=14 171.69.89.90
Keep-alive type for this connection: DPD

18 08/15/2002 15:20:06.240 SEV=4 AUTH/22 RPT=42
User rtvpvnpuser1 connected

19 08/15/2002 15:20:06.240 SEV=5 IKE/25 RPT=13 171.69.89.90
Group [RTPVPNusers] User [rtvpvnpuser1]
Received remote Proxy Host data in ID Payload:
Address 10.10.10.1, Protocol 0, Port 0

22 08/15/2002 15:20:06.240 SEV=5 IKE/24 RPT=7 171.69.89.90
Group [RTPVPNusers] User [rtvpvnpuser1]
Received local Proxy Host data in ID Payload:
Address 172.16.172.36, Protocol 0, Port 0

25 08/15/2002 15:20:06.240 SEV=5 IKE/66 RPT=13 171.69.89.90
Group [RTPVPNusers] User [rtvpvnpuser1]
IKE Remote Peer configured for SA: ESP-3DES-MD5

27 08/15/2002 15:20:06.240 SEV=5 IKE/75 RPT=13 171.69.89.90
Group [RTPVPNusers] User [rtvpvnpuser1]
Overriding Initiator's IPsec rekeying duration from 2147483 to 28800 seconds

29 08/15/2002 15:20:06.240 SEV=5 IKE/25 RPT=14 171.69.89.90
Group [RTPVPNusers] User [rtvpvnpuser1]
Received remote Proxy Host data in ID Payload:
Address 10.10.10.1, Protocol 0, Port 0

32 08/15/2002 15:20:06.240 SEV=5 IKE/34 RPT=7 171.69.89.90
Group [RTPVPNusers] User [rtvpvnpuser1]
Received local IP Proxy Subnet data in ID Payload:
Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0

35 08/15/2002 15:20:06.240 SEV=5 IKE/66 RPT=14 171.69.89.90
Group [RTPVPNusers] User [rtvpvnpuser1]
IKE Remote Peer configured for SA: ESP-3DES-MD5

37 08/15/2002 15:20:06.240 SEV=5 IKE/75 RPT=14 171.69.89.90
Group [RTPVPNusers] User [rtvpvnpuser1]
Overriding Initiator's IPsec rekeying duration from 2147483 to 28800 seconds

39 08/15/2002 15:20:06.250 SEV=4 IKE/49 RPT=16 171.69.89.90
Group [RTPVPNusers] User [rtvpvnpuser1]
Security negotiation complete for User (rtvpvnpuser1)
Responder, Inbound SPI = 0x38d81ab3, Outbound SPI = 0xc5d0d0e8

42 08/15/2002 15:20:06.250 SEV=4 IKE/120 RPT=16 171.69.89.90
Group [RTPVPNusers] User [rtvpvnpuser1]
PHASE 2 COMPLETED (msgid=d26e17a6)

43 08/15/2002 15:20:06.400 SEV=4 IKE/49 RPT=17 171.69.89.90
Group [RTPVPNusers] User [rtvpvnpuser1]
Security negotiation complete for User (rtvpvnpuser1)
Responder, Inbound SPI = 0x174f4c9a, Outbound SPI = 0x68654776

46 08/15/2002 15:20:06.400 SEV=4 IKE/120 RPT=17 171.69.89.90
Group [RTPVPNusers] User [rtvpnuser1]
PHASE 2 COMPLETED (msgid=92e0a081)

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- [Cisco VPN 3000 Concentrator Support Page](#)
 - [Cisco VPN 3000 Client Support Page](#)
 - [IPSec Support Page](#)
 - [Technical Support Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 19, 2006

Document ID: 26324
