

Cisco VPN Client User and Group Attribute Processing on the VPN 3000 Concentrator

Document ID: 14115

Introduction

Prerequisites

Requirements

Components Used

Conventions

VPN Client Connects to a VPN 3000 Concentrator

Authenticate Groups and Users Externally through RADIUS

How the VPN 3000 Concentrator Uses User and Group Attributes

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document describes how Cisco VPN Clients are authenticated on the VPN Concentrator and how the Cisco VPN 3000 Concentrator uses User and Group attributes.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco VPN 3000 Concentrator.

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

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

VPN Client Connects to a VPN 3000 Concentrator

When a VPN Client connects to a VPN 3000 Concentrator, up to four authentications can take place.

1. The Group is authenticated. (This is often called the "Tunnel Group.")
2. The User is authenticated.
3. (Optional) If the User is part of another Group, this Group is authenticated next. If the user does not belong to another Group or the Tunnel Group, then the user defaults to the Base Group and this step does NOT occur.

4. The "Tunnel Group" from Step 1 is authenticated again. (This is done in case the "Group Lock" feature is used. This feature is available in version 2.1 or later.)

This is an example of the events you see in the Event Log for a VPN Client authenticated via the Internal Database ("testuser" is part of the Group "Engineering").

```
1 12/09/1999 11:03:46.470 SEV=6 AUTH/4 RPT=6491 80.50.0.4
Authentication successful: handle = 642, server = Internal, user = Tunnel_Group
2 12/09/1999 11:03:52.100 SEV=6 AUTH/4 RPT=6492 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = testuser
3 12/09/1999 11:03:52.200 SEV=6 AUTH/4 RPT=6493 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = Engineering
4 12/09/1999 11:03:52.310 SEV=6 AUTH/4 RPT=6494 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = Tunnel_Group
```

Note: To see these Events, you must configure the Auth Event Class with severity 1–6 in **Configuration > System > Events > Classes**.

Group Lock Feature – If the Group Lock feature is enabled on the Group – Tunnel_Group, then the User must be part of Tunnel_Group to connect. In the previous example, you see all the same Events, but "testuser" does not connect because they are part of the Group – Engineering and not part of the Group – Tunnel_Group. You also see this Event:

```
5 12/09/1999 11:35:08.760 SEV=4 IKE/60 RPT=1 80.50.0.4
User [ testuser ]
User (testuser) not member of group (Tunnel_Group), authentication failed.
```

For additional information about the Group Lock feature and a sample configuration, refer to Locking Users into a VPN 3000 Concentrator Group Using a RADIUS Server.

Authenticate Groups and Users Externally through RADIUS

The VPN 3000 Concentrator can also be configured to authenticate Users and Groups externally through a RADIUS server. This still requires the names of the Groups to be configured on the VPN Concentrator, but the Group Type is configured as "External."

- External Groups can return Cisco/Altiga attributes if the RADIUS server supports Vendor Specific Attributes (VSAs).
- Any Cisco/Altiga attributes NOT returned by RADIUS default to the values in the Base Group.
- If the RADIUS server does NOT support VSAs, then ALL attributes default to the Base Group attributes.

Note: A RADIUS server treats Group names no differently than User names. A Group on a RADIUS server is configured just like a standard User.

These steps outline what happens when an IPSec Client connects to the VPN 3000 Concentrator if both Users and Groups are authenticated externally. Similar the internal case, up to four authentications can take place.

1. The Group is authenticated via RADIUS. The RADIUS server can return many attributes for the group or none at all. At a minimum, the RADIUS server needs to return the Cisco/Altiga attribute "IPSec Authentication = RADIUS" to tell the VPN Concentrator how to authenticate the User. If not, the Base Group's IPSec Authentication method needs to be set to "RADIUS."
2. The User is authenticated via RADIUS. The RADIUS server can return many attributes for the user or none at all. If the RADIUS server returns the attribute CLASS (standard RADIUS attribute #25), the

VPN 3000 Concentrator uses that attribute as a Group name and moves to Step 3, or else it goes to Step 4.

3. The user's Group is authenticated next via RADIUS. The RADIUS server can return many attributes for the group or none at all.
4. The "Tunnel Group" from Step 1 is authenticated again via RADIUS. The authentication subsystem must authenticate the Tunnel Group again because it has not stored the attributes (if any) from the authentication in Step 1. This is done in case the "Group Lock" feature is used.

How the VPN 3000 Concentrator Uses User and Group Attributes

After the VPN 3000 Concentrator has authenticated the User and Group(s), it must organize the attributes it has received. The VPN Concentrator uses the attributes in this order of preference. It does not matter if the authentication was done internally or externally:

1. **User attributes** These take precedence over all others.
2. **Group attributes** Any attributes missing from the User attributes are filled in by the Group attributes. Any that are the same are overridden by the User attributes.
3. **Tunnel Group attributes** Any attributes missing from the User or Group attributes are filled in by the Tunnel Group attributes. Any that are the same are overridden by the User attributes.
4. **Base Group attributes** Any attributes missing from the User, Group, or Tunnel Group attributes are filled in by the Base Group attributes.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

Related Information

- [Cisco VPN 3000 Series Concentrator Support Page](#)
- [Cisco VPN Client Support Page](#)
- [IPSec Support Page](#)
- [RADIUS Support Page](#)
- [RADIUS in IOS Documentation](#)
- [Requests for Comments \(RFCs\)](#)
- [Technical Support – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 11, 2007

Document ID: 14115

