

Cisco VPN 5000 Concentrator: Migrating from STEP to IKE Clients

Document ID: 14112

Cisco has announced the end of sales for the Cisco VPN 5000 Series Concentrators. For more information, refer to the End-of-Sales Announcement.

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Transition Clients and Server Code

- Add the IKE Policy Section
- Update the VPN Group
- Update the Cisco VPN 5000 Concentrator's Internal User Database
- Update a RADIUS User Database
- Client Changes
- Software Versions

Related Information

Introduction

When the VPN 5000 Concentrator was a Compatible Systems product, the concentrator used a proprietary encryption methodology called STEP. Currently, in software versions 4.2.x, the Cisco VPN 5000 Concentrator supports Internet Key Exchange (IKE) clients. This document explains how to migrate from the earlier STEP (versions 2.x) Microsoft Windows clients to the new IKE clients.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- Cisco VPN 5000 Concentrator 4.x, 5.x and 6.x
- Cisco VPN 5000 Manager 5.3 or later

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.

Transition Clients and Server Code

Note: If you are not upgrading any of your users to the 4.x clients, no configuration changes are needed.

Transitioning VPN users from STEP to IKE involves only a few changes. The changes are based on how your authentication is currently performed. Users can migrate as they install the 4.x client, so 2.x and 4.x users can use the same group configuration concurrently.

Two of the existing Cisco VPN 5000 Concentrator server configuration sections have been renamed. The [STEP Client] keyword is now called the [VPN Group] keyword, and the [STEP Users] keyword is now the [VPN Users] keyword.

Add the IKE Policy Section

A new configuration section, [IKE Policy], has been added. You need to either add that section manually (using the command line) or use Cisco VPN 5000 Manager 5.3 or later. The command line prompts you to use the new section names (overwriting the old), and Cisco VPN 5000 Manager automatically changes the section names from the old to the new. After you upgrade the VPN Concentrator server, if the Manager does not display the **IKE Policy** section in the **Global** section, delete the VPN Concentrator server's entry from the Manager Device View database and then add it again. This resets the attribute bits and lets Manager know that the VPN Concentrator server is now IKE-capable.

The only keyword available in the [IKE Policy] section is **Protection**. The Protection keyword specifies a protection suite for the ISAKMP/IKE negotiation between the VPN Concentrator server and client. This keyword can appear multiple times within this section. If this is the case, the VPN Concentrator server proposes all of the specified protection suites. The VPN Concentrator client then accepts one of the options for the negotiation. There are four possible protections:

- MD5_DES_G1
- MD5_DES_G2
- SHA_DES_G1
- SHA_DES_G2

The first part of each option is the authentication algorithm to be used for the negotiation: MD5 or SHA. MD5 is the message-digest 5 hash algorithm. SHA is the Secure Hash Algorithm, which is considered to be more secure than MD5. The second part is the encryption algorithm, Data Encryption Standard (DES), which uses a 56-bit key to scramble the data. The third part is the Diffie-Hellman group to be used for key exchange. Because larger numbers are used by the Group 2 (G2) algorithm, it is more secure than Group 1 (G1).

Update the VPN Group

The server software provides backwards compatibility in a very smooth manner; it allows the same user ID to use either the 4.x or the 2.x client. You need to add the **Transform = x** keyword/value pair in the VPN Concentrator's [VPN Group], in addition to adding the [IKE Policy] section. The 2.x client ignores these attributes and the 4.x client uses them, so both work.

For example, if your entry looks like this:

```
[ VPN Group ]
```

```
BindTo          = Ethernet 0
MaxConnections  = 45
KeepAliveInterval = 60
InactivityTimeout = 0
EncryptMethod   = fixed
StartIPAddress  = 200.200.200.50
Ipnet           = 200.200.200.0/24
```

You can change it so that you can use IKE clients as well:

```
[ VPN Group ]
BindTo          = Ethernet 0
MaxConnections  = 45
KeepAliveInterval = 60
InactivityTimeout = 0
EncryptMethod   = fixed
StartIPAddress  = 200.200.200.50
Ipnet           = 200.200.200.0/24
Transform       = ESP(SHA,DES)
```

Update the Cisco VPN 5000 Concentrator's Internal User Database

IKE users can be migrated as they install the client. If you use the internal server database, you need to add a **Sharedkey=** attribute to each user's [VPN Users] entry. For example, assume your entry looked like this:

```
[ VPN Users ]
loren Config="VPN1" Auth="letmein" Encrypt="letmein"
```

To change your entry so that you can use an IKE client as well, add the Sharedkey= attribute as demonstrated here:

```
[ VPN Users ]
loren Config="VPN1" SharedKey="letmein" Auth="letmein" Encrypt="letmein"
```

Update a RADIUS User Database

The server software provides backwards compatibility in a very smooth manner. It allows the same user ID to use either the 4.x or the 2.x client. You are not required to modify the RADIUS user profile. The RADIUS attributes that you entered are still used with IKE.

Cisco Secure RADIUS

For instructions on configuring Cisco Secure to work with the VPN 5000 Concentrator, refer to:

- How to Authenticate VPN 5000 Client to the VPN 5000 Concentrator with Cisco Secure NT 2.5 (RADIUS)
- Configuring the Cisco VPN 5000 Client to the Cisco VPN 5000 Concentrator with Cisco Secure UNIX (RADIUS) Authentication

Funk RADIUS

This is a Funk RADIUS entry for a VPN account:

```
loren User Type:Set password = Unix-PW
Compatible-VPN-Password = "letmein"
Compatible-VPN-GroupInfo = "VPN1"
```

In the attributes defined, the Compatible-VPN-Password is the shared secret. The shared secret is used to create the keys for packet authentication and encryption. It does not replace the RADIUS authentication. As with the 2.x client, if RADIUS is used for authentication, the user must enter a RADIUS password. The Compatible-GroupInfo is the [VPN Group]. Except for the shared secret, there is no difference compared to what you did with the 2.x client.

Merit RADIUS

This is a Merit RADIUS entry for a VPN account:

```
loren Authentication-Type = "letmein"  
Tunnel-Password = "letmein"  
Connect-Info = "VPN1"
```

In the defined attributes, the Tunnel-Password is the shared secret and the Connect-Info is the [VPN Group]. Since Authentication-Type is Unix-PW, the RADIUS password is the same one that you use when you log into your hosts as "loren." Except for the shared secret, there is no difference compared to what you did with the 2.x client.

Client Changes

There are no fields for authentication/encryption information in the 4.x clients. Instead of entering authentication and encryption information in the Connection Configuration screen, the user is prompted for the shared secret when he attempts to establish a connection. This improves security because secrets are not stored on the PC.

The administrator can enable storage of secrets on the server, but is off by default. This is done with the SaveSecrets keyword, which is located in the [VPN Group] section.

If the server determines that the user is a RADIUS user (it does this by looking in its internal user database and not finding a user entry), it prompts the user for her RADIUS password. The RADIUS transaction takes place, with the RADIUS server sending the Tunnel-Password back to the VPN Concentrator, which validates it against the shared secret. If you are not using RADIUS, the user is prompted only for the SharedKey. The VPN Concentrator server then uses that value to generate authentication and encryption keys for the data stream.

Software Versions

The new IKE clients work with the Cisco VPN 5000 Concentrator Server 5.x and 6.x, but they do not work with 4.x code or earlier versions. It is highly recommended that you migrate to the new IKE clients and that you run the latest version of VPN Concentrator software. To download this software, go to the VPN Software Center Downloads (registered customers only) page.

Related Information

- [Cisco VPN 5000 Series Concentrators End-of-Sales Announcement](#)
 - [Cisco VPN 5000 Concentrator Support Page](#)
 - [Cisco VPN 5000 Client Support Page](#)
 - [IPSec Support Page](#)
 - [Technical Support – Cisco Systems](#)
-

