Configuring a Cisco VPN 5000 Concentrator with External Authentication to a Microsoft Windows 2000 IAS RADIUS Server

Document ID: 12491

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

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Cisco VPN 5000 Concentrator Configuration
Configure the Microsoft Windows 2000 IAS RADIUS Server
Verify the Result
Configure the VPN Client
Concentrator Logs
Troubleshoot
Related Information
Introduction

This document describes the procedures used to configure a Cisco VPN 5000 Concentrator with external authentication to a Microsoft Windows 2000 Internet Authentication Server (IAS) with RADIUS.

Note: Challenge Handshake Authentication Protocol (CHAP) does not work. Use only Password Authentication Protocol (PAP). Refer to Cisco bug ID CSCdt96941 (registered customers only) for further details.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on this software version:

Cisco VPN 5000 Concentrator Software Version 6.0.16.0001

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.

Cisco VPN 5000 Concentrator Configuration

VPN5001_4B9CBA80

| VPN5001_4B9CBA80> show co Enter Password: | onfig |
|--|---|
| Edited Configuration not | Present, using Running |
| [General] EthernetAddress DeviceType ConfiguredOn ConfiguredFrom EnablePassword Password | <pre>= 00:02:4b:9c:ba:80 = VPN 5001 Concentrator = Timeserver not configured = Command Line, from Console = =</pre> |
| [IP Ethernet 0] Mode SubnetMask IPAddress | = Routed = 255.255.255.0 = 172.18.124.223 |
| [IP Ethernet 1] Mode | = Off |
| [IKE Policy] Protection | = MD5_DES_G1 |
| [VPN Group "rtp-group" BindTo Transform LocalIPNet MaxConnections IPNet | <pre>] = "ethernet0" = esp(md5,des) = 10.1.1.0/24 = 10 = 0.0.0.0/0</pre> |
| BindTo ChallengeType PAPAuthSecret PrimAddress Secret UseChap16 Authentication | <pre>= "ethernet0" = PAP = "pappassword" = "172.18.124.108" = "radiuspassword" = Off = On</pre> |
| [Logging] Level Enabled Configuration size is 100 | = 7 = On 65 out of 65500 bytes. |
| VPN5001_4B9CBA80# | |

Configure the Microsoft Windows 2000 IAS RADIUS Server

These steps guide you through a simple Microsoft Windows 2000 IAS RADIUS server configuration.

1. Under the Microsoft Windows 2000 IAS properties, select Clients and create a new client.

In this example, an entry named VPN5000 is created. The IP address of the Cisco VPN 5000 Concentrator is 172.18.124.223. Under the Client–Vendor drop–down box, select **Cisco**. The shared secret is the secret in the [RADIUS] section of the VPN Concentrator configuration.

| VPN5000 Properties |
|--|
| Settings |
| Friendly name for client: |
| VPN5000 |
| Client address |
| Address (IP or DNS): |
| 172.18.124.223 |
| Verify |
| Client-Vendor: Cisco |
| Client must always send the signature attribute in the request |
| Shared secret: |
| Confirm shared secret: |
| |
| |
| OK Cancel Apply |

2. Under the properties of the Remote Access Policy, select **Grant remote access permission** under the "If a user matches the conditions" section and then click **Edit Profile**.

| ow access if dia | al-in permissior | n is enable | d Properties | ? |
|------------------------------|---------------------|----------------|-------------------|-------------------------------|
| Settings | | | | |
| Policy name: | Allow acc | ess if dial-in | permission is ena | abled |
| Specify the cond | ditions to match: | | | |
| Day-And-Time-F | Restrictions match | es ''Sun 00: | 00-24:00; Mon 0 | 0:00-24:00; 1 |
| | | | | |
| | | | | |
| | | | | inininininii i - 1 |
| | | | | • |
| Add 1 | Bemove | Edit | -1 | |
| | Themove | | | |
| ⊢ If a user match | ies the conditions | | | |
| Grant rem | ote access permis | sion | | |
| C Domuson | ata agagga pormia | aian | | |
| Deny rem | ote access pennis | sion | | |
| Access w | ill be granted with | the profile y | ou specify, unles | s access |
| is overnuc | ien on a pei-usei i | Jasis. | | |
| | | | | |
| Edit Profile | | | | |
| а — т | | | | |
| | | | | |
| | 1.0 | 141 | | |
| | | OK L | Cancel | () oplu |

3. Click the Authentication tab and ensure that only **Unencrypted Authentication (PAP, SPAP)** is selected.

| Dial-in Profile | |
|---|--------------------------|
| Dial-in Constraints IP |] Multilink |
| Authentication Encryption | Advanced |
| Check the authentication methods which are allo | wed for this connection |
| | med for this connection. |
| | ina a Parton |
| Select the EAP type which is acceptable for thi | s policy. |
| MD5-Challenge | Configure |
| Microsoft Encrypted Authentication version | 2 (MS-CHAP v2) |
| | |
| Microsoft Encrypted Authentication (MS-CF | (AP) |
| Encrypted Authentication (CHAP) | |
| ✓ Unencrypted Authentication (PAP_SPAP) | |
| | |
| | |
| - Unauthenticated Access | |
| - Allow remote PPP clients to connect without | ut negotiating |
| any authentication method. | |
| | |
| | |
| Οκ | Cancel Acolu |
| OK | Cancer Apply |

4. Select the Advanced tab, click Add and select Vendor–Specific.

| | Encig | ption Advanced | d 1 | | |
|---|--------------|--|--|---|--|
| pecify additional connection coess Server. arameters: | n attributes | to be returned to the Remote Add Attributes | | <u>?</u> | |
| Name | Vendo | To add an attribute to the Pro RADIUS attributes: | file, select the attribut | e and click Add. | |
| | | Name Reply-Message | RADIUS Standard | Description Message to be displayed to user when authenticati | |
| | | Service-Type RADIUS Star Tunnel-Assignment-ID RADIUS Star Tunnel-Clent-Auth-ID RADIUS Star | | I Type of service user has requested Tunnel to which a session is to be assigned Name used by the tunnel initiator during the authen | |
| | | Tunnel-Dient-Endpt Tunnel-Medium-Type Tunnel-Password Tunnel-Password | RADIUS Standard RADIUS Standard RADIUS Standard RADIUS Standard | IP address of the initiator end of the tunnel Transport medium to use when creating a tunnel to Password for authenticating to a remote server Relative rederence assigned to each tunnel when | |
| Add Remove | | Tunnel-Pvt-Group-ID Tunnel-Server-Auth-ID Tunnel-Server-Endpt Tunnel-Terre | RADIUS Standard RADIUS Standard RADIUS Standard RADIUS Standard | Group ID for a particular tunneled session Name used by the tunnel terminator during the auth IP address of the server end of the tunnel Tunneling protocols to be used. | |
| | | Vendor-Specific Cisco-AV-Pair USB-&CCM-Tune | RADIUS Standard Cisco | Used to support proprietary NAS features Cisco AV Pair VSA Description and available | |
| | | USR-AT-Call-Input-Filter USR-AT-Call-Output-Filter USR-AT-Input-Filter | U.S. Robotics, I U.S. Robotics, I U.S. Robotics, I | Description not available Description not available Description not available | |
| | OK | USR-AT-Output-Filter USR-AT-RTMP-Input-Filter | U.S. Robotics, I U.S. Robotics, I | Description not available Description not available | |

5. Under the Multivalued Attribute Information dialog box for the Vendor–Specific attribute, click **Add** in order to go to the Vendor–Specific Attribute Information dialog box. Select **Enter Vendor Code** and enter **255** in the adjacent box. Next, select **Yes. It conforms** and click **Configure Attribute**.

| Multivalued Attribute Information | Vendor-Specific Attribute Information |
|--|---|
| Attribute name: | Attribute name: |
| Vendor-Specific | Vendor-Specific |
| Attribute number: | Specify network access server vendor. |
| 26 | C Select from list RADIUS Standard |
| Attribute format: | Enter Vendor Code: 255 |
| OctetString | |
| Attribute values: | Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes. |
| Vendor Value Move Up Move Down Add Bemove Edit | Yes. It conforms. No. It does not conform. Configure Athibute OK Cancel |
| OK. Cancel | |

6. Under the Configure VSA (RFC compliant) dialog box, enter **4** for the Vendor–assigned attribute number, enter **String** for the Attribute format, and enter **rtp–group** (name of the VPN Group in the Cisco VPN 5000 Concentrator) for the Attribute value. Click **OK** and repeat step 5.

| onfigure VSA (RFC compliant) | | ? × |
|-----------------------------------|--|-----|
| Vendor-assigned attribute number: | | |
| 4 | | |
| Attribute format: | | |
| String | | • |
| Attribute value: | | |
| rtp-group | | |

7. Under the Configure VSA (RFC compliant) dialog box, enter **4** for the Vendor–assigned attribute number, enter **String** for the Attribute format, and enter **cisco123** (the client shared secret) for the Attribute value. Click **OK**.

| Configure VSA (RFC compliant) | | ? × |
|-----------------------------------|------|-------|
| Vendor-assigned attribute number: | | |
| 5 | | |
| Attribute format: | | |
| String | | • |
| Attribute value: | | |
| cisco123 | | |
| cisco123 | | |
| s | | |
| | ОК С | ancel |
| | | |

8. You see that the Vendor–Specific attribute contains two values (group and VPN password).

| t Dial-in Profile | | ? |
|---|---------------------------|---------------------|
| Dial-in Constraints | I IP | Multilink |
| Authentication | Encryption | Advanced |
| Specify additional connectio Access Server. Parameters: | n attributes to be return | ned to the Remote |
| Name | Vendor | Value |
| Vendor-Specific | RADIUS Standard | rtp-group, cisco123 |
| <pre></pre> | | F |
| Add Remov | e Edit | |
| | | |
| | | |
| | | 2 2 1 2 2 |

Under your user properties, click the Dial-in tab and ensure that Control access through Remote Access Policy is selected.

| mar Properties | ? |
|---|------------------|
| General Member Of Profile Dial-in | |
| Remote Access Permission (Dial-in or VPN) | |
| C Allow access | |
| C Deny access | |
| Control access through Remote Access F | Policy |
| Verify Caller-ID: | |
| Callback Options | |
| No Callback | |
| C Set by Caller (Routing and Remote Acces | ss Service only) |
| Always Callback to: | |
| Assign a Static IP Address | |
| Apply Static Routes | |
| Define routes to enable for this Dial-in connection. | Static Routes |
| | |
| OK | Cancel Apply |

Verify the Result

This section provides information you can use in order to confirm your configuration works properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only), which allows you to view an analysis of **show** command output.

- **show radius statistics** Displays packet statistics for communication between the VPN Concentrator and the default RADIUS server identified by the RADIUS section.
- show radius config Shows the current settings for RADIUS parameters.

This is the output of the **show radius statistics** command.

VPN5001_4B9CBA80>show radius statistics

| RADIUS Stats | | |
|--|-----------------------|----------------------|
| Accounting | Primary | Secondary |
| Requests | 0 | na |
| Responses | 0 | na |
| Retransmissions | 0 | na |
| Bad Authenticators | 0 | na |
| Malformed Responses | 0 | na |
| Packets Dropped | 0 | na |
| Pending Requests | 0 | na |
| Timeouts | 0 | na |
| Unknown Types | 0 | na |
| | | |
| Authentication | Primary | Secondary |
| Requests | 3 | na |
| Accepts | 3 | na |
| Rejects | 0 | na |
| Challenges | 0 | na |
| Retransmissions | 0 | na |
| Bad Authenticators | | |
| | 0 | na |
| Malformed Responses | 0 0 | na na |
| Malformed Responses Packets Dropped | 0 0 0 | na na na |
| Malformed Responses Packets Dropped Pending Requests | 0 0 0 0 | na na na na |
| Malformed Responses Packets Dropped Pending Requests Timeouts | 0 0 0 0 0 | na na na na |

VPN5001_4B9CBA80>

This is the output of the show radius config command.

| RADIUS | | State | UDP | CHAP16 | |
|-------------|--------|-----------|--------|--------|------------|
| Authenticat | ion | On | 1812 | No | |
| Accounting | | Off | 1813 | n/a | |
| Secret | | 'radiusp | asswoi | rd ' | |
| Server | IP add | lress | Atte | empts | AcctSecret |
| Primary | 172.18 | 3.124.108 | 3 | 5 | n/a |
| Secondary | Off | | | | |

Configure the VPN Client

This procedure guides you through the configuration of the VPN Client.

1. From the VPN Client dialog box, select the Configuration tab. Next, from the VPN Client–Prompt for Secret dialog box, enter the shared secret under the VPN Server. The VPN Client shared secret is the value entered for the VPN password of attribute 5 in the VPN Concentrator.

| omar 172.18.124.215 Manual omar 172.18.124.223 Shared Key Edit VPN Client - Prompt for Secret Login Name: omar OK VPN Server: 172.18.124.223 Cancel Shared Secret: | ime | Partner | Login Met | hod | Add |
|---|-----------|----------|-------------------------------------|-----|----------|
| VPN Client - Prompt for Secret Edit Login Name: omar VPN Server: 172.18.124.223 Cancel | omar | 172.18.1 | 124.215 Manual 124.222 Shared Ka | | Remove |
| VPN Client - Prompt for Secret Login Name: omar VPN Server: 172.18.124.223 Shared Secret: Cancel | omar | 172.10. | 124.223 Shaled Ke | y | Edit |
| | Charad C. | сı. | 172.10.124.220 | | Lancel |
| | Shaleu St | 30181. | 4 | -11 | |
| | | | | | Advanced |
| Advanced | | | | | |
| Advanced. | | | | | |

2. After you enter the shared secret, you are prompted for a password and authentication secret. The password is your RADIUS password for that user, and the authentication secret is the PAP authentication secret in the [RADIUS] section of the VPN Concentrator.

| VPN Client | | × |
|---------------|--|----------|
| Configuration | Logging General Certificates About | |
| Login Cont | iguration | |
| Name | Partner Login Method | Add |
| omar Pomar | 172.18.124.215 Manual 172.18.124.223 Shared Key | Remove |
| | | Edit |
| RADIUS | Login | × |
| Passwo | rd: | ок |
| Authen | tication Secret: | Cancel |
| - | | |
| | | |
| • | | Advanced |
| C Auto-Conne | ect to Default when Opened | |
| Auto-Conne | ect to Default before Logon | |
| Connecting u | ser omar to 172.18.124.223 | |
| | Hide Exit | |

Concentrator Logs

| Notice | 4080.11 seconds New IKE connection: [172.18.124.108]:1195:omar |
|--------|---|
| Debug | 4080.15 seconds Sending RADIUS PAP challenge to omar at 172.18.124.108 |
| Debug | 4087.52 seconds Received RADIUS PAP response from omar at 172.18.124.108, contact |
| Notice | 4088.8 seconds VPN 0:3 opened for omar from 172.18.124.108. |
| Debug | 4088.8 seconds Client's local broadcast address = 172.18.124.255 |
| Notice | 4088.8 seconds User assigned IP address 10.1.1.1 |
| Info | 4094.49 seconds Command loop started from 10.1.1.1 on PTY2 |

Troubleshoot

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

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

```
Contacts & Feedback | Help | Site Map
```

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.