RADIUS, TACACS+, and Cisco Secure Domain Stripping

Document ID: 10148

Contents

Introduction

In some situations, a username with an "@" sign (username@website.com) is sent to Cisco IOS® Software. When this happens, there is a need to strip the domain name off of an incoming user. In such cases, this may be done using either directed–requests on the router or Cisco Secure software on the server.

Before You Begin

Conventions

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

Prerequisites

There are no specific prerequisites for this document.

Components Used

This document is not restricted to specific software and hardware versions.

RADIUS Domain Stripping

In this sample configuration, assume you are configuring a router that hosts a domain called *website.com*. Your RADIUS server has an IP address of 10.1.1.1.

```
ip host website.com 10.1.1.1
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server directed-request
```

Note: The **radius–server directed–request** command was introduced in Cisco IOS® Software Release 12.0(2)T.

With this configuration, when a person named *user@website.com* needs to be authenticated, the **directed–request** code tries to resolve the domain name to an IP address. In this case, website.com resolves to the IP address 10.1.1.1 because of the local **ip host** statement. The router then looks up the **radius–server host** line for the IP address that was resolved, and sends the authentication request for username *user* to the RADIUS server.

TACACS+ Domain Stripping

You can perform the same process for TACACS+ with these commands:

```
ip host website.com 10.1.1.1
tacacs-server host 10.1.1.1
tacacs-server directed-request
```

Cisco Secure ACS for Windows Domain Stripping

If you need to strip the domain from user@website.com, configure Cisco Secure NT to authenticate the username as user only by completing these steps:

1. Go to **Interface Configuration > Advanced Options**, select **Distributed System Settings**, and click **Submit**.

   In addition, if the stripped user is to go to a server other than this one, complete the following steps:

   a. Go to **Network Configuration > Network Device Groups > Add Entry** to add an authentication, authorization, and accounting (AAA) server.
   b. Go to **Network Configuration > Network Device Groups** on the target and configure the source.
2. On the source, go to **Network Configuration > Distribution Table > Add Entry**. Configure the settings as follows:

   ♦ In the field for **Character String**, type the domain name (@website.com).
   ♦ From the **Position** pull–down menu, choose Suffix. (Note that Prefix is also applicable in some cases.)
   ♦ From the **Strip** pull–down menu, choose Yes.
   ♦ Move the server from the **AAA Server** list to the **Forward To** list. If the stripped name is to go from source to source (meaning that the source and target are the same), the source would be the server to "forward to." If the stripped name is to go from source to a different target, then the target would be the server to "forward to."
3. Click **Submit** to save the settings.

Cisco Secure UNIX Domain Stripping

On the **AAA > Domain** web page for the home gateway access control server, specify these settings:

• Domain Name: website.com
• Delimiter: @
• Domain Name Position: After
• Domain Type: Remote

Related Information

- **Remote Authentication Dial−In User Service (RADIUS)**
- **Terminal Access Controller Access Control System (TACACS+)**
- **Requests for Comments (RFCs)** ⬀
- **Technical Support – Cisco Systems**

Updated: Jan 17, 2006   Document ID: 10148