

Shell Command Authorization on Juniper Router with ACS Configuration Example

Document ID: 110895

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Configure

- TACACS+ Configurations

Related Information

Introduction

This document provides a sample configuration on Shell Command Authorization sets in Cisco Secure Access Control Server (ACS) for Juniper Router, a third party vendor, with TACACS+.

Refer to Setting Juniper RADIUS Parameters for a User in order to configure and enable Juniper RADIUS attributes to apply as an authorization for the current user.

Prerequisites

Requirements

This document assumes that the basic configurations are set in both AAA clients and ACS.

1. In ACS, choose **Interface Configuration > Advanced Options**.
2. Ensure that the **Per-user TACACS+/RADIUS Attributes** check box is checked.

Components Used

The information in this document is based on the Cisco Secure Access Control Server (ACS) that runs the software version 4.1.

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

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

TACACS+ Configurations

Command authorization sets provide a central mechanism to control the authorization of each command that is issued on any given network device. This feature greatly enhances the scalability and manageability required to set authorization restrictions.

Juniper Command Authorization Sets require that the TACACS+ command authorization request identify the service as **junos-exec**.

In order to configure and enable Juniper attributes to apply as an authorization for the current user, complete these steps:

1. Add the Juniper routers under **Network Configuration > AAA clients > Add Entry** with **TACACS+ (CISCO IOS)** as the authentication protocol and with the correct **ip address** where they source their requests and the matching **shared-secret key**.

The screenshot shows the Cisco Systems Network Configuration interface. The left sidebar contains a navigation menu with the following items: User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted with a red box), System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled 'Add AAA Client' and contains the following fields and options:

- AAA Client Hostname: Juniper
- AAA Client IP Address: 1.1.1.1
- Key: Junos
- Authenticate Using: TACACS+ (Cisco IOS) (highlighted with a red box)
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

At the bottom of the form are three buttons: Submit, Submit + Restart, and Cancel.

2. Choose **Interface Configuration > TACACS+ (CISCO IOS)**. Under New Services, enable the **junos-exec** services either per user, per group or both. It is recommended to do this per user if you want to allow different values on a per user basis (X, Y, Z, XY).

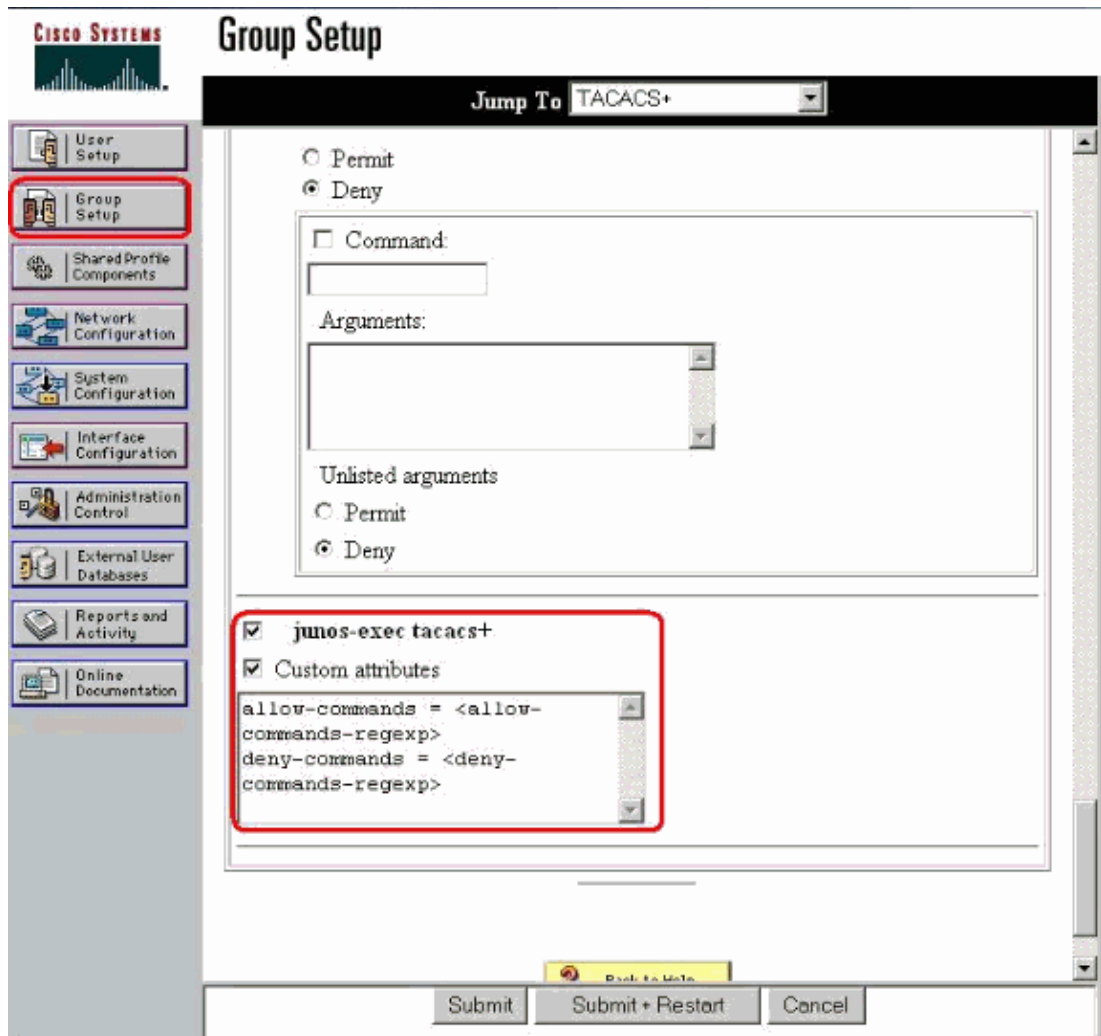
The screenshot shows the Cisco Systems Interface Configuration window. On the left is a navigation pane with the following items: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration (highlighted with a red box), Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "Interface Configuration" and contains several sections:

- A list of protocols with checkboxes: PPP IP (checked), PPP IPX, PPP Multilink, PPP Apple Talk, PPP VPDN, PPP LCP, ARAP, Shell (exec) (checked and circled in red), PIX Shell (pixshell), and SLIP.
- A section titled "New Services" with a table:

	Service	Protocol
<input checked="" type="checkbox"/>	junos-exec	tacacs+
<input type="checkbox"/>		
- A section titled "Advanced Configuration Options" with a help icon (yellow question mark) and the following options:
 - Advanced TACACS+ Features (circled in red)
 - Display a Time-of-Day access grid for every TACACS+ service where you can override the default Time-of-Day settings
 - Display a window for each service selected in which you can enter customized TACACS+ attributes
 - Display enable default (Undefined) service configuration

At the bottom of the window are "Submit" and "Cancel" buttons.

3. Go to the group/user setup and find this newly created service under **TACACS+** settings. Check the option for **junos-exec** and the option for **Custom Attributes**. Enter the values of this service for each user per this image:



For X user account you will need to enter the following attributes:

```
local-user-name = sales
allow-commands = "configure"
deny-commands = "shutdown"
```

For Y user account you will need to enter:

```
local-user-name = sales
allow-commands = "(request system) | (show rip neighbor)"
deny-commands = "<^clear"
```

For Z user account:

```
local-user-name = engineering
allow-commands = "monitor | help | show | ping | traceroute"
deny-commands = "configure"
```

Finally, for XY user account:

```
local-user-name = engineering
allow-commands = "show bgp neighbor"
deny-commands = "telnet | ssh"
```

Related Information

- **User Guide for Cisco Secure Access Control Server 4.1**
 - **Technical Support & Documentation – Cisco Systems**
-

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

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 21, 2009

Document ID: 110895
