

Advanced TACACS+ for Dialup Clients

Document ID: 10362

Introduction

Prerequisites

Requirements

Components Used

Conventions

Configure

Network Diagram

Configurations

Verify

Troubleshoot

Troubleshooting Commands

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document provides a sample configuration for dialup clients that use Terminal Access Controller Access Control System (TACACS+).

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Make sure dial-in works.
- When the modem can connect and authenticate locally, turn on TACACS+.
- Finally, test authentication to ensure that you can connect and authenticate through TACACS+, and turn on authorization.

Components Used

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

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 Cisco Technical Tips Conventions for more information on document conventions.

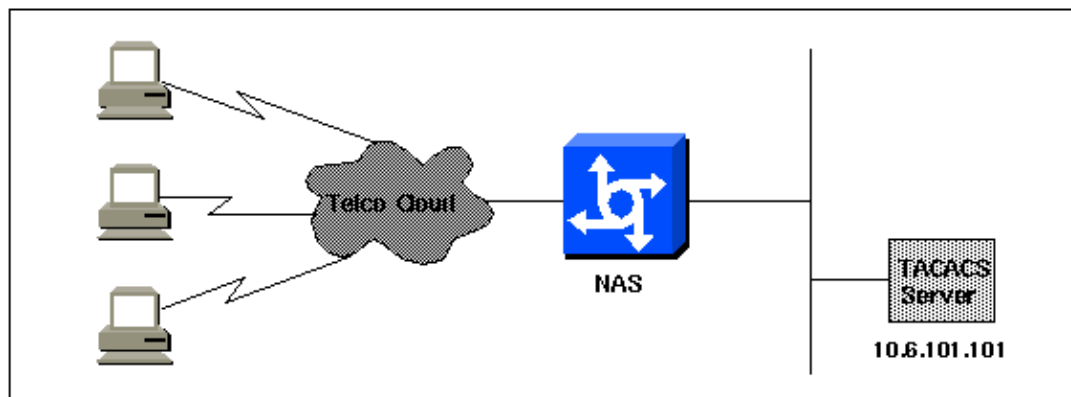
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only).

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- NAS
- TACACS+ Configuration File (freeware version)

```

                                     NAS
-----
version 11.2
service timestamps debug datetime msec
service timestamps log uptime
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname Cisco3640
!
aaa new-model
aaa authentication login default tacacs local
aaa authentication login consoleport none
aaa authentication ppp default if-needed tacacs
aaa authorization network tacacs

!--- You require this for static IP address assignment.

!
enable password cisco
!
username cisco password letmein
!
interface Ethernet0
```

```

ip address 10.29.1.3 255.255.255.0
!
Interface Group-Async1
ip unnumbered Ethernet0
encapsulation ppp
async mode interactive
peer default ip address pool async
no cdp enable
ppp authentication chap
group-range 1 16
!
access-list 101 deny icmp any any
access-list 101 permit ip any any
!
ip local pool async 10.6.100.101 10.6.100.103
tacacs-server host 10.6.101.101
tacacs-server key cisco
!
line con 0
login authentication consoleport

!--- This is to always allow console port access.

!
line 1 16
autoselect ppp
autoselect during-login
modem Dialin
transport input all
stopbits 1
rxspeed 115200
txspeed 115200
flowcontrol hardware
!
line aux 0
!
line vty 0 4
!
end

```

TACACS+ Configuration File (freeware version)

```

!--- Superuser (similar to an admin) who can perform all operations,
!--- whose 'default service = permit', and has a password that allows
!--- for connections in any mode.

user = Russ
{
  global = cleartext 'bar'
  default service = permit
}

!--- Normal PPP user who receives an IP address from the router.

user = Jason
{
  chap = cleartext 'letmein'
  service = ppp protocol = ip {}
}

!--- Statically assign IP address.

```

```

user = Laura
{
  chap = cleartext 'letmein'
  service = ppp protocol = ip
    {
      addr = 10.1.1.104
    }
}

!--- Only permit EXEC connections, at a privilege level of 1,
!--- and only allow telnets to host on the 171.68.200.0 network.
!--- Allow all show commands. Also assign and access list #101.

#
user = Tito {
  login = cleartext bar
  service = exec
    {
      priv-lvl = 1
      acl = 101
    }
  cmd = telnet
    {
      # permit
      permit 171\.68\.200\.[0-9]+
    }
  cmd = show {
    permit .*
  }
}

```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug ppp negotiation** checks whether a client passes PPP negotiation when you check for address negotiation.
- **debug ppp authentication** checks whether a client passes authentication. If you use a version earlier than Cisco IOS® Software Release 11.2, use the **debug ppp chap** command instead.
- **debug ppp error** displays protocol errors and error statistics associated with PPP connection negotiation and operation.
- **debug aaa authentication** verifies the method used to authenticate (must be TACACS, unless the TACACS server is down), and checks whether or not the users pass authentication.
- **debug aaa authorization** verifies the method used for authorization, and checks whether or not the

users pass it.

- **debug tacacs** enables you to see the messages sent to the server.

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 Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- **Technical Support & Documentation – Cisco Systems**
-

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

Updated: Jul 23, 2007

Document ID: 10362
