Konfigurieren des Cisco Routers für die Wählauthentifizierung mithilfe von TACACS+

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie einen Cisco Router für die Wählauthentifizierung mit dem unter UNIX ausgeführten TACACS+ konfigurieren. TACACS+ bietet nicht so viele Funktionen wie das kommerziell verfügbare Cisco Secure ACS für Windows oder Cisco Secure ACS für UNIX.

Die zuvor von Cisco Systems bereitgestellte TACACS+-Software wurde eingestellt und wird von Cisco Systems nicht mehr unterstützt.

Heute können Sie viele verfügbare Freeware-Versionen von TACACS+ finden, wenn Sie in Ihrer Internet-Suchmaschine nach "TACACS+ Freeware" suchen. Cisco empfiehlt keine spezielle Implementierung von TACACS+-Freeware.

Der Cisco Secure Access Control Server (ACS) kann über reguläre Vertriebs- und Vertriebskanäle von Cisco weltweit erworben werden. Cisco Secure ACS für Windows umfasst alle erforderlichen Komponenten für eine unabhängige Installation auf einer Microsoft Windows-Workstation. Die Cisco Secure ACS Solution Engine wird mit einer vorinstallierten Cisco Secure ACS-Softwarelizenz geliefert. Produktnummern finden Sie im Cisco Secure ACS 4.0-Produktbulletin. Besuchen Sie die Cisco Bestellseite (nur registrierte Kunden), um eine Bestellung aufzugeben.

Hinweis: Sie benötigen ein CCO-Konto mit einem zugehörigen Servicevertrag, um die 90-tägige

Testversion für Cisco Secure ACS für Windows zu erhalten (nur registrierte Kunden).

Die Router-Konfiguration in diesem Dokument wurde auf einem Router entwickelt, auf dem die Cisco IOS® Software, Version 11.3.3, ausgeführt wird. Cisco IOS Software-Versionen 12.0.5.T und höher verwenden **Gruppentakacs+** anstelle von **tacacs+**. Anweisungen wie **aaa authentication login default tacacs+ enable** erscheinen als **aaa authentication login default group tacacs+ enable**.

Sie können die TACACS+-Freeware und das Benutzerhandbuch über anonymous ftp auf ftp-eng.cisco.com im Verzeichnis /pub/tacacs herunterladen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfigurationen

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

In diesem Dokument werden folgende Konfigurationen verwendet:

- Routerkonfiguration
- TACACS+-Konfigurationsdatei für Freeware Server

Routerkonfiguration

```
!
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication ppp default if-needed tacacs+
aaa authorization exec default tacacs+ if-authenticated
aaa authorization commands 1 default tacacs+ if-
authenticated
aaa authorization commands 15 default tacacs+ if-
authenticated
aaa authorization network default tacacs+
enable password ww
```

```
!
chat-script default "" at&fls0=1&h1&r2&c1&d2&b1e0q2 OK
!
interface Ethernet0
 ip address 10.6.1.200 255.255.255.0
!
 !--- Challenge Handshake Authentication Protocol !---
(CHAP/PPP) authentication user. interface Async1 ip
unnumbered Ethernet0 encapsulation ppp async mode
dedicated peer default ip address pool async no cdp
enable ppp authentication chap ! !--- Password
Authentication Protocol (PAP/PPP) authentication user.
interface Async2 ip unnumbered Ethernet0 encapsulation
ppp async mode dedicated peer default ip address pool
async no cdp enable ppp authentication pap ! !---
Authentication user with autocommand PPP. interface
Async3 ip unnumbered Ethernet0 encapsulation ppp async
mode interactive peer default ip address pool async no
cdp enable ! ip local pool async 10.6.100.101
10.6.100.103 tacacs-server host 171.68.118.101 tacacs-
server timeout 10 tacacs-server key cisco ! line 1
session-timeout 20 exec-timeout 120 0 autoselect during-
login script startup default script reset default modem
Dialin transport input all stopbits 1 rxspeed 115200
txspeed 115200 flowcontrol hardware ! line 2 session-
timeout 20 exec-timeout 120 0 autoselect during-login
script startup default script reset default modem Dialin
transport input all stopbits 1 rxspeed 115200 txspeed
115200 flowcontrol hardware ! line 3 session-timeout 20
exec-timeout 120 0 autoselect during-login autoselect
ppp script startup default script reset default modem
Dialin autocommand ppp transport input all stopbits 1
rxspeed 115200 txspeed 115200 flowcontrol hardware ! end
```

TACACS+-Konfigurationsdatei für Freeware Server

```
!--- Handshake with router !--- AS needs 'tacacs-server
key cisco'. key = "cisco" !--- User who can Telnet in to
configure. user = admin { default service = permit login
= cleartext "admin" } !--- CHAP/PPP authentication line
1 - !--- password must be cleartext per CHAP
specifications. user = chapuser { chap = cleartext
"chapuser" service = ppp protocol = ip { default
attribute = permit } } !--- PPP/PAP authentication line
2. user = papuser { login = file /etc/passwd service =
ppp protocol = ip { default attribute = permit } } !---
Authentication user line 3. user = authauto { login =
file /etc/passwd service = ppp protocol = ip { default
attribute = permit } }
```

Microsoft Windows-Setup

Microsoft Windows Setup für Benutzer 1 und 2

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Schrittweise Anleitung

Führen Sie diese Schritte aus.

Hinweis: Die PC-Konfiguration kann je nach verwendeter Betriebssystemversion leicht abweichen.

1. Wählen Sie **Start > Programme > Zubehör > DFÜ-Netzwerk**, um das Fenster DFÜ-Netzwerk zu öffnen.
2. Wählen Sie **Neue Verbindung herstellen** aus dem Menü Verbindungen, und geben Sie einen Namen für die Verbindung ein.
3. Geben Sie die modemspezifischen Informationen ein, und klicken Sie auf **Konfigurieren**.
4. Wählen Sie auf der Seite Allgemeine Eigenschaften die höchste Geschwindigkeit Ihres Modems aus, aber überprüfen Sie nicht die Option **Nur Verbindung mit dieser Geschwindigkeit**... Box.
5. Verwenden Sie auf der Seite Konfigurieren/Verbindungseigenschaften 8 Datenbits, keine Parität und 1 Stoppbit. Zu verwendende Anrufvoreinstellungen sind **Warten auf Wählton vor dem Wählen** und **Abbrechen des Anrufs, wenn der Anruf nach 200 Sekunden nicht verbunden ist**.
6. Klicken Sie auf der Seite Verbindung auf **Erweitert**. Wählen Sie in den erweiterten Verbindungseinstellungen nur **Hardware Flow Control** and **Modulation Type Standard**.Auf der Eigenschaftenseite Konfigurieren/Optionen sollte nur das Kontrollkästchen unter Statussteuerung aktiviert werden.
7. Klicken Sie auf **OK** und dann auf **Weiter**.
8. Geben Sie die Telefonnummer des Ziels ein, klicken Sie erneut auf **Weiter** und dann auf **Fertig stellen**.
9. Wenn das neue Verbindungssymbol angezeigt wird, klicken Sie mit der rechten Maustaste darauf, und wählen Sie **Eigenschaften > Servertyp aus**.
10. Wählen Sie **PPP:WINDOWS 95, WINDOWS NT 3.5, Internet** aus, und aktivieren Sie keine erweiterten Optionen.
11. Aktivieren Sie **TCP/IP** unter Zulässige Netzwerkprotokolle.
12. Wählen Sie unter TCP/IP-Einstellungen... die Option **Server assigned IP address**, **Server assigned name server address**, und **Use default gateway on remote network (Standard-Gateway im Remote-Netzwerk verwenden) aus,** und klicken Sie dann auf **OK**.
13. Wenn der Benutzer auf das Symbol doppelklickt, um das Fenster Connect To (Verbindung herstellen) anzuzeigen, um eine Nummer zu wählen, muss der Benutzer die Felder User Name (Benutzername) und Password (Kennwort) eingeben und dann auf **Connect (Verbinden)** klicken.

Microsoft Windows-Setup für Benutzer 3

Die Konfiguration für Benutzer 3 (Authentifizierungsbenutzer mit autocommand PPP) ist mit der für Benutzer 1 und 2 identisch, mit den folgenden Ausnahmen:

- Aktivieren Sie auf der Seite Eigenschaften von Konfigurieren/Optionen (Schritt 6) die Option **Terminalfenster nach dem Wählen öffnen**.
- Wenn der Benutzer auf das Symbol doppelklickt, um das Fenster Connect To (Verbindung mit) zu wählen (Schritt 13), füllt der Benutzer die Felder User name (Benutzername) und Password (Kennwort) nicht aus. Der Benutzer klickt auf **Verbinden**. Nachdem die Verbindung zum Router hergestellt wurde, geben Sie im schwarzen Fenster den Benutzernamen und das Kennwort ein. Nach der Authentifizierung drückt der Benutzer **Continue (F7)**.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Router

Weitere Informationen zu Debug-Befehlen finden Sie vor dem Ausgeben von **Debug-**Befehlen unter Wichtige Informationen.

- **terminal monitor** (Terminalmonitor): Zeigt die Ausgabe des Befehls debug sowie Systemfehlermeldungen für das aktuelle Terminal und die aktuelle Sitzung an.
- **debug ppp negotiation**: Zeigt PPP-Pakete an, die während des PPP-Startvorgangs gesendet werden, wobei PPP-Optionen ausgehandelt werden.
- **debug ppp packet**: Zeigt PPP-Pakete an, die gesendet und empfangen werden. (Dieser Befehl zeigt Low-Level Packet Dumps an.)
- **debug ppp chap**: Zeigt Informationen darüber an, ob ein Client die Authentifizierung besteht (für Cisco IOS Software Releases vor 11.2).
- **debug aaa authentication**: Zeigt Informationen zur AAA-/TACACS+-Authentifizierung (Authentication, Authorization, Accounting) und TACACS+-Authentifizierung an.
- **debug aaa autorization**: Zeigt Informationen zur AAA/TACACS+-Autorisierung an.

Server

Hinweis: Hierbei wird der Servercode der Cisco TACACS+-Freeware vorausgesetzt.

```
tac_plus_executable -C config.file -d 16
  tail -f /var/tmp/tac_plus.log
```

Zugehörige Informationen

- Support-Seite für TACACS+
- TACACS+ in der IOS-Dokumentation
- Cisco Secure Access Control-Server
- Einrichten und Debuggen von CiscoSecure 2.x TACACS+
- Technischer Support und Dokumentation - Cisco Systems