Configurazione e debug di Cisco Secure 2.x TACACS+

Sommario

Introduzione
Prerequisiti
Requisiti
Convenzioni
Configurazione di Cisco Secure
Impostazione dell'autenticazione
Configurazione
Aggiunta dell'autorizzazione
Aggiunta di accounting
Aggiunta di utenti remoti
Verifica
Risoluzione dei problemi
Server
Router
File Cisco Secure Users
Informazioni correlate

Introduzione

Questo documento aiuta il primo utente Cisco Secure 2.x nella configurazione e nel debug di una configurazione Cisco Secure TACACS+. Non è una descrizione completa delle funzionalità di Cisco Secure.

Per informazioni più complete sul software server e sulla configurazione dell'utente, consultare la documentazione di Cisco Secure. Per ulteriori informazioni sui comandi del router, consultare la documentazione del software Cisco IOS per la versione appropriata.

Prerequisiti

Requisiti

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure ACS 2.x e versioni successive
- Software Cisco IOS® versione 11.3.3 e successive

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione di Cisco Secure

Attenersi alla seguente procedura:

1. Per installare il codice Cisco Secure sul server UNIX, attenersi alle istruzioni fornite con il software.
2. Per confermare che il prodotto si arresta e si avvia, immettere `cd in /etc/rc0.d` e come root eseguire `./K80Cisco Secure` (per arrestare i daemon).Immettere `cd in /etc/rc2.d` e come root eseguire `./S80Cisco Secure` (per avviare i daemon).All'avvio dovrebbero essere visualizzati messaggi quali:
   ```
   Cisco Secure starting Processes: Fast Track Admin, FastTrack Server (Delayed Start),
   DBServer, AAA Server
   ```
   Eseguire `$BASE/utils/psg` per accertarsi che almeno uno dei singoli processi sia in esecuzione, ad esempio SQLAnywhere o un altro modulo di gestione di database, il processo server di database Cisco Secure, il server Web Netscape, l'amministratore Web Netscape, il server Web Acme, il processo Cisco Secure AAA o il processo di riavvio automatico.
3. Per essere certi di trovarsi nelle directory appropriate, impostare le variabili di ambiente e i percorsi nell'ambiente shell. c-shell è usato qui.**$BASE** è la directory in cui è installato Cisco Secure, scelta durante l'installazione. Contiene directory quali DOCS, DBServer, CSU e così via.In questo esempio, si presuppone l'installazione in /opt/CSCOacs, ma questa condizione può variare a seconda del sistema:
   ```
   setenv $BASE   /opt/CSCOacs
   ```
   $SQLANY è la directory in cui viene installato il database Cisco Secure predefinito, scelto durante l'installazione. Se è stato utilizzato il database predefinito fornito con il prodotto, SQLAnywhere, contiene directory quali database, doc e così via.In questo esempio, si presuppone l'installazione in /opt/CSCOacs/SYBSsa50, ma può variare a seconda del sistema.
   ```
   setenv $SQLANY /opt/CSCOacs/SYBSsa50
   ```
   Aggiungere percorsi nell'ambiente shell per:
   ```
   $BASE/utils
   $BASE/bin
   $BASE/CSU
   $BASE/ns-home/admserv
   $BASE/Ns-home/bin/httpd
   $SQLANY/bin
   ```
4. CD in $BASE/config**CSU.cfg** è il control file Cisco Secure server. Crea una copia di backup del file.In questo file, `LIST config_license_key` mostra la chiave di licenza ricevuta durante la procedura di licenza se è stato acquistato il software; se si tratta di una licenza di prova a 4 porte, è possibile escludere questa riga.La sezione **NAS config_nas_config** può contenere un server di accesso alla rete (NAS) o un router predefinito oppure il server NAS immesso durante l'installazione. Ai fini del debug in questo esempio, è possibile consentire a *qualsiasi* server NAS di comunicare con il server Cisco Secure *senza* una chiave. Ad esempio, rimuovere il nome del NAS e la chiave dalle righe che contengono `/* nome NAS può andare qui */`" e */*NAS/Cisco Secure secret key */*. L'unica *stanza* in quell'area recita:

```
NAS config_nas_config = {
  {
    "",          /* NAS name can go here */
    "",              /* NAS/Cisco Secure secret key */
    "",                          /* message_catalogue_filename */
    1,                           /* username retries */
    2,                           /* password retries */
    1                            /* trusted NAS for SENDPASS */
  }
};

AUTHEN config_external_authen_symbols = {
```

In questo modo, si comunica a Cisco Secure che può comunicare con tutti i NAS senza scambio di chiavi.

5. Se si desidera visualizzare le informazioni di debug in /var/log/csuslog, è necessario inserire una riga nella sezione superiore di CSU.cfg, che indica al server la quantità di debug da eseguire. 0X7FFFFFFF aggiunge tutte le operazioni di debug possibili. Aggiungere o modificare la riga di conseguenza:
   ```
   NUMBER config_logging_configuration = 0x7FFFFFFF;
   ```
   Questa riga aggiuntiva invia le informazioni di debug a local0:
   ```
   NUMBER config_system_logging_level = 0x80;
   ```
   Inoltre, aggiungere questa voce per modificare il file /etc/syslog.conf:
   ```
   local0.debug /var/log/csuslog
   ```
   Quindi riciclare il syslogd per rileggere:
   ```
   kill -HUP `cat /etc/syslog.pid`
   ```
   Riciclare il server Cisco Secure:
   ```
   /etc/rc0.d/K80Cisco Secure
   /etc/rc2.d/S80Cisco Secure
   ```
   Dovrebbe ancora iniziare.
6. Èpossibile utilizzare il browser per aggiungere utenti, gruppi e così via oppure l'utilità CSimport. Gli utenti di esempio nel file flat alla fine di questo documento possono essere spostati facilmente nel database utilizzando CSimport. Questi utenti funzioneranno per scopi di test e sarà possibile eliminarli una volta che si ottengono i propri utenti in. Una volta importati, gli utenti possono essere visualizzati tramite la GUI.Se decidete di utilizzare CSimport:
   ```
   CD $BASE/utils
   ```
   Inserire i profili utente e di gruppo alla fine di questo documento in un file, ad esempio in qualsiasi punto del sistema, quindi dalla directory $BASE/utils, con i daemon in esecuzione, ad esempio /etc/rc2.d/S80Cisco Secure e come utente root, eseguire CSimport con l'opzione di test (-t):
   ```
   ./CSimport -t -p <path_to_file> -s <name_of_file>
   ```
   In questo modo viene verificata la sintassi per gli utenti. dovresti ricevere messaggi come:
   ```
   Secure config home directory is: /opt/CSCOacs/config/CSConfig.ini
   hostname = berry and port = 9900 and clientid = 100
   /home/ddunlap/csecure/upgrade.log exists, do you want to write over 'yes' or 'no' ?
   yes
   Sorting profiles...
   Done sorting 21 profiles!
   Running the database import test...
   ```
   Non dovresti ricevere messaggi come:
   ```
   Error at line 2: password = "adminusr"
   Couldn't repair and continue parse
   ```
   Se si sono verificati errori, esaminare il file upgrade.log per verificare che i profili siano stati estratti. Una volta corretti gli errori, dalla directory $BASE/utils, con i daemon in esecuzione (/etc/rc2.d/S80Cisco Secure) e come utente root, eseguire CSimport con l'opzione commit (-

c) per spostare gli utenti nel database:
`./CSimport -c -p <path_to_file> -s <name_of_file>`
Anche in questo caso non dovrebbero essere presenti errori sullo schermo o nel file upgrade.log.

7. I browser supportati sono elencati nel suggerimento tecnico Cisco Secure Compatibility. Dal browser del PC, selezionare la casella Cisco Secure/Solaris **http://#.#.#.#/cs** dove **#.#.#.#** è l'indirizzo IP del server Cisco Secure/Solaris.Nella schermata visualizzata, per l'utente immettere **superuser** e per la password immettere **changeme**. Non modificare la password. Se si utilizza CSimport nel passaggio precedente, è possibile visualizzare gli utenti/gruppi aggiunti oppure fare clic sul blocco Sfoglia per **disattivare** e aggiungere manualmente utenti e gruppi tramite la GUI.

Impostazione dell'autenticazione

Nota: questa configurazione del router è stata sviluppata su un router con software Cisco IOS versione 11.3.3. Il software Cisco IOS versione 12.0.5.T e successive mostra i **TACACS di gruppo** anziché i **TACACS**.

A questo punto, configurare il router.

1. Arrestare Cisco Secure durante la configurazione del router.
`/etc/rc0.d/K80Cisco Secure to stop the daemons.`
2. Sul router, avviare la configurazione di TACACS+. Immettere enable mode e digitare `conf t` prima del set di comandi. Questa sintassi garantisce che non si sia bloccati dal router *inizialmente* purché Cisco Secure non sia in esecuzione. Immettere `ps -ef | grep Secure` per verificare che Cisco Secure non sia in esecuzione e terminare il processo -9 se è:

```
!--- Turn on TACACS+ aaa new-model enable password whatever !--- These are lists of
authentication methods, !--- that is, vtymethod and conmethod are !--- names of lists, and
the methods listed on the !--- same lines are the methods in the order to be !--- tried. As
used here, if authentication !--- fails due to Cisco Secure not being started, !--- the
enable password is accepted !--- because it is in each list. aaa authentication login
vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable !--- Point the
router to the server, that is, !--- #.#.#.# is the server IP address. tacacs-server host
#.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !---
during debugging. exec-timeout 0 0 login authentication conmethod line vty 0 4 password
whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0
0 login authentication vtymethod
```

3. Prima di continuare, verificare che sia ancora possibile accedere al router con Telnet e tramite la porta della console. Poiché Cisco Secure non è in esecuzione, la password di abilitazione deve essere accettata.**Attenzione:** mantenere attiva la sessione della porta console e rimanere in modalità abilitazione; questa sessione non deve scadere. A questo punto si inizia a limitare l'accesso al router e si deve essere in grado di apportare modifiche alla configurazione senza bloccarsi.Per verificare l'interazione tra server e router sul router, eseguire questi comandi:
```
terminal monitor
debug aaa authentication
```
4. Come root, avviare Cisco Secure sul server:
`/etc/rc2.d/S80Cisco Secure`
In questo modo vengono avviati i processi, ma si desidera abilitare un numero di debug maggiore di quello configurato in S80Cisco Secure, in modo da:
`ps -ef | grep Cisco Secure`

```
kill -9 <pid_of CS_process>

CD $BASE/CSU
./Cisco Secure -cx -f $BASE/config/CSU.cfg to start the Cisco Secure process with debugging
```

Con l'opzione `-x`, Cisco Secure viene eseguito in primo piano in modo da consentire l'interazione tra router e server. Non dovrebbero essere visualizzati messaggi di errore. Il processo Cisco Secure deve iniziare e terminare qui a causa dell'opzione -x.

5. Da un'altra finestra, verificare che Cisco Secure sia stato avviato. Immettere `ps -ef` e cercare il processo Cisco Secure.
6. Gli utenti Telnet (vty) devono ora eseguire l'autenticazione tramite Cisco Secure. Con il debug sul router, eseguire Telnet nel router da un'altra parte della rete. Il router deve generare un prompt con nome utente e password. Dovrebbe essere possibile accedere al router con le seguenti combinazioni di ID utente e password:
   ```
   adminusr/adminusr
   operator/oper
   desusr/encrypt
   ```
   Osservare il server e il router in cui dovrebbe essere visualizzata l'interazione, ovvero il messaggio inviato dove, le risposte e le richieste e così via. Correggere eventuali problemi prima di continuare.
7. Se si desidera che gli utenti eseguano l'autenticazione tramite Cisco Secure per accedere alla modalità di abilitazione, verificare che la sessione della porta della console sia ancora attiva e aggiungere questo comando al router:

   ```
   !--- For enable mode, list 'default' looks to Cisco Secure !--- then enable password if Cisco Secure is not running. aaa authentication enable default tacacs+ enable
   ```
8. A questo punto, è necessario eseguire l'**abilitazione** tramite Cisco Secure. Con il debug sul router, eseguire Telnet nel router da un'altra parte della rete. Quando il router chiede un nome utente/password, rispondere con l'`operatore/operatore operativo`.Quando l'operatore utente tenta di accedere alla modalità di abilitazione (livello di privilegio 15), è richiesta la password "cisco". Senza l'istruzione del livello di privilegio (o il daemon Cisco Secure non attivo), gli altri utenti non potranno accedere alla modalità di abilitazione.Guarda il server e il router dove dovrebbe essere visualizzata l'interazione Cisco Secure, ad esempio, cosa viene inviato dove, risposte e richieste e così via. Correggere eventuali problemi prima di continuare.
9. Disattivare il processo Cisco Secure sul server mentre è ancora connesso alla porta della console per essere certi che gli utenti possano ancora accedere al router se Cisco Secure non è attivo:
   ```
   'ps -ef' and look for Cisco Secure process
   kill -9 pid_of_Cisco Secure
   ```
   Ripetere la procedura Telnet e abilitare la procedura precedente. Il router deve rendersi conto che il processo Cisco Secure non risponde e consente agli utenti di accedere e abilitare il sistema con le password di abilitazione predefinite.
10. Riattivare il server Cisco Secure e stabilire una sessione Telnet con il router, che deve autenticarsi tramite Cisco Secure, tramite ID utente/password **operatore/operatore** per verificare la presenza di autenticazioni degli utenti della porta della console tramite Cisco Secure. Rimanere collegati al router e in modalità abilitazione finché non si è certi di poter accedere al router tramite la porta della console, ad esempio uscire dalla connessione originale al router tramite la porta della console, quindi riconnettersi alla porta della console. L'autenticazione della porta console per accedere con le precedenti combinazioni di ID utente e password deve essere ora eseguita tramite Cisco Secure. Ad esempio, **per abilitare** il **comando** userid/password **operator/**oper e la password **cisco** devono essere

usati.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Aggiunta dell'autorizzazione

L'aggiunta dell'autorizzazione è facoltativa.

Per impostazione predefinita, sul router sono disponibili tre livelli di comando:

- Livello di privilegio 0: disabilitazione, abilitazione dell'uscita, guida e disconnessione
- Livello di privilegio 1: livello normale su Telnet e prompt `router>`
- Livello di privilegio 15: livello di abilitazione e prompt `router#`

Poiché i comandi disponibili dipendono dal set di funzionalità di Cisco IOS, dalla versione del software Cisco IOS, dal modello di router e così via, non è disponibile un elenco completo di tutti i comandi dei livelli 1 e 15. Ad esempio, **show ipx route** non è presente in un set di funzionalità solo IP, **show ip nat trans** non è nel software Cisco IOS versione 10.2.X perché NAT non è stato introdotto in quel momento e **show environment** non è presente nei modelli di router senza alimentazione e monitoraggio della temperatura.

I comandi disponibili in un particolare router a un particolare livello possono essere immessi nel campo **?** al prompt nel router quando si trova a quel livello di privilegio.

L'autorizzazione della porta console non è stata aggiunta come funzionalità finché non è stato implementato CSCdi82030. Per impostazione predefinita, l'autorizzazione della porta console è disattivata per ridurre la probabilità di essere bloccata accidentalmente dal router. Se un utente ha accesso fisico al router tramite la console, l'autorizzazione della porta della console non è molto efficace. Tuttavia, l'autorizzazione della porta della console può essere attivata nella **riga di** comando **con 0** in un'immagine Cisco IOS in cui CSCdi82030 è stato implementato con il comando **authorization exec default|WORD**.

Attenersi alla seguente procedura:

1. Il router può essere configurato per autorizzare i comandi tramite Cisco Secure a tutti i livelli o ad alcuni livelli. Questa configurazione del router consente a tutti gli utenti di impostare l'autorizzazione per comando sul server. È possibile autorizzare tutti i comandi tramite Cisco Secure, ma se il server non è attivo, non è necessaria alcuna autorizzazione, da cui `nessuna` autorizzazione.Con il Cisco Secure server spento, immettere questi comandi:Immettere questo comando per rimuovere il requisito per cui è consentita l'autenticazione tramite Cisco Secure:
   ```
   no aaa authentication enable default tacacs+ none
   ```
   Immettere questi comandi per richiedere l'autorizzazione dei comandi tramite Cisco Secure:
   ```
   aaa authorization commands 0 default tacacs+ none
   aaa authorization commands 1 default tacacs+ none
   aaa authorization commands 15 default tacacs+ none
   ```

2. Mentre il server Cisco Secure è in esecuzione, collegarsi in modalità Telnet al router con ID utente/password **loneuser/lonepwd**. L'utente non deve essere in grado di eseguire altri comandi oltre a:
   ```
   show version
   ping <anything>
   logout
   ```
   Gli utenti precedenti, **adminusr/adminusr**, **operator/oper**, **desusr/encrypt**, dovrebbero essere ancora in grado di eseguire tutti i comandi in base al `servizio predefinito = allow`. In caso di problemi con il processo, accedere alla modalità di abilitazione sul router e attivare il debug di autorizzazione con questo comando:
   ```
   terminal monitor
   debug aaa authorization
   ```
   Guarda il server e il router dove dovrebbe essere visualizzata l'interazione Cisco Secure, ad esempio, cosa viene inviato dove, risposte e richieste e così via. Correggere eventuali problemi prima di continuare.
3. Il router può essere configurato per autorizzare le sessioni di esecuzione tramite Cisco Secure. Il comando **aaa authorization exec default tacacs+ none** istituisce l'autorizzazione TACACS+ per le sessioni exec.L'applicazione di questa proprietà influisce sul tempo/ora degli utenti, su **telnet/telnet**, **todam/todam**, **todpm/todpm** e **somerouters/somerouters**. Dopo aver aggiunto il comando al router e aver impostato Telnet sul router come **ora** utente, una sessione di esecuzione rimane aperta per un minuto (set timeout = 1). L'utente **telnet/telnet** accede al router ma viene immediatamente inviato all'altro indirizzo (set autocmd = "telnet 171.68.118.102"). È possibile che gli utenti **todam/todam** e **todpm/todpm** siano o non siano in grado di accedere al router, a seconda dell'ora del giorno in cui si trova durante il test. L'utente **somerouters** può connettersi solo in modalità Telnet al router koala.rtp.cisco.com dalla rete 10.31.1.x. Cisco Secure cerca di risolvere il nome del router. Se si utilizza l'indirizzo IP 10.31.1.5, è valido se la risoluzione non ha luogo e se si utilizza il nome koala, è valido se la risoluzione è tramite.

Aggiunta di accounting

L'aggiunta dell'accounting è facoltativa.

1. L'accounting non viene eseguito a meno che non sia stato configurato nel router, se il router esegue il software Cisco IOS versione successiva al software Cisco IOS versione 11.0. È possibile abilitare l'accounting sul router:
   ```
   aaa accounting exec default start-stop tacacs+
   aaa accounting connection default start-stop tacacs+
   aaa accounting network default start-stop tacacs+
   aaa accounting system default start-stop tacacs+
   ```
   Nota: l'accounting dei comandi è stato interrotto nell'ID bug Cisco CSCdi44140, ma se si utilizza un'immagine in cui questo problema è risolto, è possibile abilitare anche l'accounting dei comandi.
2. Aggiungi debug record di accounting sul router:
   ```
   terminal monitor
   debug aaa accounting
   ```
3. Il debug sulla console dovrebbe mostrare i record di accounting che entrano nel server quando gli utenti si collegano.
4. Per recuperare i record di accounting come radice:
   ```
   CD $BASE/utils/bin
   ./AcctExport <filename> no_truncate
   ```

`no_truncate` indica che i dati vengono conservati nel database.

Aggiunta di utenti remoti

Attenersi alla seguente procedura:

1. Accertarsi che le altre funzioni di Cisco Secure funzionino prima di aggiungere utenti remoti. Se il server Cisco Secure e il modem non funzionano prima di questo punto, non funzioneranno dopo questo punto.
2. Aggiungere questo comando alla configurazione del router:
   ```
   aaa authentication ppp default if-needed tacacs+
   aaa authentication login default tacacs+ enable
   aaa authorization network default tacacs+
   chat-script default "" at&fls0=1&h1&r2&c1&d2&b1e0q2 OK
   ```
   Le configurazioni di interfaccia sono diverse, a seconda di come viene eseguita l'autenticazione, ma nell'esempio riportato vengono utilizzate le linee di connessione remota con le configurazioni seguenti:
   ```
   interface Ethernet 0
   ip address 10.6.1.200 255.255.255.0
   ! !--- 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 ! !--- 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 ! !--- login 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
   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 ! access-list 101 deny icmp any any
   ```
3. Dal file utente di Cisco Secure:chapuser—CHAP/PPP—l'utente chiama sulla linea 1; l'indirizzo viene assegnato dal **pool di indirizzi ip asincrono predefinito peer e dal pool locale ip async 10.6.100.101 10.6.100.103** sul routerchapaddr—CHAP/PPP—l'utente chiama sulla linea 1; l'indirizzo 10.29.1.99 è assegnato dal serverchapacl—CHAP/PPP—l'utente chiama sulla linea 1; l'indirizzo 10.29.1.100 viene assegnato dal server e viene applicato l'elenco degli accessi in entrata 101 (da definire sul router)papuser—PAP/PPP— user dial in on line 2; l'indirizzo viene assegnato dal **pool di indirizzi ip asincrono predefinito peer e dal pool locale ip async 10.6.100.101 10.6.100.103** sul routerpapaddr—PAP/PPP—l'utente digita sulla linea 2; l'indirizzo 10.29.1.98 è assegnato dal serverpapacl—PAP/PPP—l'utente chiama sulla linea 2; l'indirizzo 10.29.1.100 viene assegnato dal server e viene applicato l'elenco degli accessi in entrata 101, che deve essere definito sul routerloginauto—l'utente chiama la linea 3; l'autenticazione di accesso con il comando automatico in linea forza la connessione PPP all'utente e assegna l'indirizzo dal pool
4. Installazione di Microsoft Windows per tutti gli utenti ad eccezione di user loginautoScegliere **Start > Programmi > Accessori > Connessione remota**.Scegliete **Connessioni > Crea nuova connessione**. Digitare un nome per la connessione.Immettere le informazioni specifiche del modem. In **Configurazione > Generale**, scegliere la velocità più alta del modem, ma non selezionare la casella sottostante.In **Configura > Connessione**, utilizzare 8 bit di dati, nessuna parità e 1 bit di stop. Le preferenze di chiamata sono **Attendi il segnale prima di**

comporre il numero e **Annulla la chiamata se non si è connessi dopo 200 secondi**.In Avanzate, scegliere solo **Controllo flusso hardware** e **Tipo modulazione standard**.In **Configura > Opzioni**, non controllare nulla se non sotto il controllo dello stato. Fare clic su **OK**.Nella finestra Avanti immettere il numero di telefono della destinazione, fare clic su **Avanti** e quindi su **Fine**.Una volta visualizzata l'icona della nuova connessione, fare clic con il pulsante destro del mouse su di essa e scegliere **Proprietà**, quindi fare clic su **Tipo server**.Scegliere **PPP:WINDOWS 95, WINDOWS NT 3.5, Internet** e non selezionare alcuna opzione avanzata.In Protocolli di rete consentiti, selezionare almeno **TCP/IP**.In Impostazioni TCP/IP scegliere **Indirizzo IP assegnato dal server**, **Indirizzi server dei nomi assegnati dal server** e **Usa gateway predefinito nella rete remota**. Fare clic su **OK**.Quando si fa doppio clic sull'icona per visualizzare la finestra Connetti a per comporre il numero, è necessario compilare i campi Nome utente e Password, quindi fare clic sul pulsante **Connetti**.

5. Installazione di Microsoft Windows 95 per l'accesso utente automaticoLa configurazione per l'utente loginauto, l'utente di autenticazione con autocommand PPP, è la stessa degli altri utenti tranne che nella finestra **Configura > Opzioni**. Selezionare **Visualizza la finestra del terminale dopo la composizione**.Quando si fa doppio clic sull'icona per visualizzare la finestra Connetti a, non è possibile compilare i campi Nome utente e Password. Fare clic su **Connect** (Connetti). Una volta stabilita la connessione al router, immettere il nome utente e la password nella finestra nera visualizzata.Dopo l'autenticazione, fare clic su **Continua(F7)**.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Server

```
./Cisco Secure -cx -f $BASE/CSU $BASE/config/CSU.cfg
```

Router

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**. Per ulteriori informazioni su comandi specifici, vedere la guida di riferimento dei comandi di debug di Cisco IOS.

- **terminal monitor**: visualizza l'output del comando **debug** e i messaggi di errore del terminale e della sessione correnti.
- **debug ppp negotiation**: visualizza i pacchetti PPP trasmessi durante l'avvio di PPP, in cui le opzioni PPP vengono negoziate.
- **debug ppp packet**: visualizza i pacchetti PPP che vengono inviati e ricevuti. Con questo

comando vengono visualizzati i dump di pacchetti di basso livello.

- **debug ppp chap**: visualizza le informazioni sul traffico e gli scambi in una rete interna che implementa il protocollo CHAP (Challenge Authentication Protocol).
- **debug aaa authentication**: visualizza i metodi di autenticazione utilizzati e i relativi risultati.
- **debug aaa authorization**: vedere quali metodi di autorizzazione vengono utilizzati e quali sono i risultati di tali metodi.

File Cisco Secure Users

```
group = admin {
        password = clear "adminpwd"
        service = shell {
                default cmd = permit
                default attribute = permit
        }
}

group = oper {
        password = clear "oper"
        privilege = clear "cisco" 15
        service = shell {
                default cmd = permit
                default attribute = permit
        }
}

user = adminusr {
        password = clear "adminusr"
        default service = permit
        }

user = desusr {
        password = des "QjnXYd1kd7ePk"
        default service = permit
        }

user = operator {
        member = oper
        default service = permit
        }

user = time {
        default service = permit
        password = clear "time"
        service = shell  {
                set timeout = 1
                default cmd = permit
                default attribute = permit
        }
}

user = todam {
        password = clear "todam"
        service = shell  {
                default cmd = permit
                default attribute = permit
                time = Any 0600 - 1200
        }
        }
```

```
user = todpm {
        password = clear "todpm"
        service = shell  {
                default cmd = permit
                default attribute = permit
                time = Any 1200 - 2359
        }
        }

user = telnet {
        password = clear "telnet"
        service = shell  {
                set autocmd = "telnet 171.68.118.102"
                        }
        }

user = limit_lifetime {
        password = clear "cisco" from
        "2 may 2001" until
        "4 may 2001"
        }

user = loneusr {
        password = clear "lonepwd"
        service = shell  {
                cmd = show {
                permit "ver"
                }
                cmd = ping {
                permit "."
                }
                cmd = logout {
                permit "."
                }
        }
}

user = chapuser {
        default service = permit
        password = chap "chapuser"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                }
        }
}

user = chapaddr {
        password = chap "chapaddr"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        set addr = 10.29.1.99
                }
        }
}

user = chapacl {
        default service = permit
        password = chap "chapacl"
        service = ppp {
```

```
                protocol = lcp {
                        }
                protocol = ip {
                        set inacl = 101
                        set addr = 10.29.1.100
                }
        }
}

user = papuser {
        default service = permit
        password = pap "papuser"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                }
        }
}

user = papaddr {
        default service = permit
        password = pap "papaddr"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        set addr = 10.29.1.98
                }
        }
}

user = papacl {
        default service = permit
        password = chap "papacl"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        set inacl = 101
                        set addr = 10.29.1.100
                }
        }
}

user = loginauto {
        default service = permit
        password = clear "loginauto"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        }
        }
 }

user = somerouters {
   password = clear "somerouters"
   allow koala ".*" "10\.31\.1\.*"
   allow koala.rtp.cisco.com ".*" "10\.31\.1\.*"
   allow 10.31.1.5 ".*" "10\.31\.1\.*"
   refuse ".*" ".*" ".*"
   service=shell {
   default cmd=permit
```

```
default attribute=permit
}
}
```

Informazioni correlate

- Supporto dei prodotti Cisco Secure ACS per UNIX
- Avvisi sui prodotti per la sicurezza (incluso Cisco Secure UNIX)