Configurazione di Cisco Secure UNIX e Secure ID (client SDI)

Sommario

Introduzione

Per implementare la configurazione descritta in questo documento, è necessaria una versione di Cisco Secure che supporti il Secure ID di Security Dynamics Incorporated (SDI).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Installazione di un client SDI (Secure ID) su un computer Cisco Secure UNIX

Nota: Secure ID viene in genere installato prima di Cisco Secure UNIX (CSUnix). Queste istruzioni descrivono come installare il client SDI dopo l'installazione di CSUnix.

1. Sul server SDI, eseguire **sdadmin**. Comunicare al server SDI che il computer CSUnix è un client e specificare che gli utenti SDI in questione vengono attivati sul client CSUnix.
2. Utilizzare il comando **nslookup** #.#.#.# o **nslookup** <nomehost> per assicurarsi che il client CSUnix e il server SDI siano in grado di eseguire la ricerca diretta e inversa l'uno dell'altro.
3. Copiare il file /etc/sdace.txt del server SDI nel file /etc/sdace.txt del client CSUnix.
4. Copiare il file sdconf.rec del server SDI sul client CSUnix; il file può trovarsi in qualsiasi punto del client CSUnix. Tuttavia, se il file viene inserito nella stessa struttura di directory sul client CSUnix come sul server SDI, non è necessario modificare sdace.txt.
5. /etc/sdace.txt o VAR_ACE devono puntare al percorso in cui si trova il file sdconf.rec. Per verificare questa condizione, eseguire cat /etc/sdace.txt o controllare l'output di env per assicurarsi che VAR_ACE sia definito nel profilo della radice come avvio della radice.
6. Eseguire il backup del file CSU.cfg del client CSUnix, quindi modificare la sezione AUTHEN config_external_auto_symbols con le seguenti
   righe:

```
AUTHEN config_external_authen_symbols = {
  {
    "./libskey.so",
    "skey"
  }
       ,
{
   "./libsdi.so",
   "sdi"
}
       ,
{
  "./libpap.so",
  "pap"
}
       ,
{
  "./libchap.so",
  "chap"
}
```

Note: A "," is required before and after these lines if preceeded or followed by another option "AUTHEN config_external_authen_symbols" section in the **CSU.cfg** file. The "," is *not* required when these lines appear as the last lines of the "AUTHEN config_external_authen_symbols" section of the **CSU.cfg** file.

7. Riciclare CSUnix eseguendo **K80CiscoSecure** e **S80CiscoSecure**.
8. Se $BASE/utils/psg indica che il processo Cisco Secure AAA Server era attivo prima della modifica del file CSU.cfg ma non dopo, sono stati commessi errori nella revisione del file CSU.cfg. Ripristinare il file CSU.cfg originale e provare di nuovo ad apportare le modifiche indicate al punto 6.

Test iniziale di Secure ID e CSUnix

Per verificare Secure ID e CSUnix, attenersi alla seguente procedura:

1. Accertarsi che un utente non SDI possa connettersi al router in modalità Telnet e ricevere l'autenticazione da CSUnix. Se non funziona, l'interfaccia SDI non funziona.
2. Verificare l'autenticazione SDI di base nel router ed eseguire questo comando:

   ```
   aaa new-model

   aaa authentication login default tacacs+ none
   ```

   Nota: si presume che i comandi **tacacs-server** siano già attivi sul router.
3. Aggiungere un utente SDI dalla riga di comando di CSUnix per immettere questo comando

   ```
   $BASE/CLI/AddProfile -p 9900 -u sdi_user -pw sdi
   ```

4. Provare ad eseguire l'autenticazione come utente. . Se l'utente funziona, l'interfaccia SDI è operativa ed è possibile aggiungere ulteriori informazioni ai profili utente.
5. Gli utenti SDI possono essere testati con il profilo utente sconosciuto in CSUnix. (Non è necessario che gli utenti siano elencati in modo esplicito in CSUnix se vengono trasmessi a SDI e hanno tutti lo stesso profilo). Se esiste già un profilo utente sconosciuto, eliminarlo tramite questo comando:

   ```
   $BASE/CLI/DeleteProfile -p 9900 -u unknown_user
   ```

6. Utilizzare questo comando per aggiungere un altro profilo utente sconosciuto:

   ```
   $BASE/CLI/AddProfile -p 9900 -u unknown_user -pw sdi
   ```

   Questo comando passa tutti gli utenti sconosciuti a SDI.

Secure ID e CSUnix: Profilo TACACS+

1. Eseguire un test iniziale senza SDI. Se questo profilo utente non funziona senza una password SDI per l'autenticazione di accesso, il protocollo CHAP (Challenge Handshake Authentication Protocol) e il protocollo PAP (Password Authentication Protocol), non funzionerà con una password SDI:

   ```
   # ./ViewProfile -p 9900 -u cse
   User Profile Information
   user = cse{
   password = chap "chappwd"
   password = pap "pappwd"
   password = clear,"clearpwd"
   default service=permit
   service=shell {
   }
   service=ppp {
   protocol=lcp {
   }
   protocol=ip {
   }
   }
   }
   ```

2. Una volta che il profilo funziona, aggiungere "sdi" al profilo anziché "clear" come mostrato nell'esempio:

```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
password = chap "chappwd"
password = pap "pappwd"
password = sdi
default service=permit
service=shell {
}
service=ppp {
protocol=lcp {
}
protocol=ip {
}
}

}
```

Funzionamento del profilo

Questo profilo consente all'utente di accedere con queste combinazioni:

- Telnet su router e uso di SDI. (Si presume che il comando **aaa authentication login default tacacs+** sia stato eseguito sul router.)
- Connessione remota PPP e PAP. (Questa operazione presuppone che sul router siano stati eseguiti i comandi **aaa authentication ppp predefinito se necessario** e **ppp autthen pap**).**Nota:** Sul PC, in Accesso remoto, verificare che sia selezionata l'opzione "Accetta qualsiasi autenticazione, incluso testo non crittografato". Prima di comporre il numero, immettere una delle seguenti combinazioni di nome utente e password nella finestra del terminale:
```
username: cse*code+card
password: pap (must agree with profile)

username: cse
password: code+card
```
- Connessione remota PPP e CHAP. (Si presume che sul router siano stati eseguiti i comandi **aaa authentication ppp default if-needed tacacs** e **ppp autthen chap**).**Nota:** nel PC, in Accesso remoto, è necessario selezionare "Accetta qualsiasi autenticazione, incluso testo non crittografato" o "Accetta solo autenticazione crittografata". Prima di comporre il numero, immettere il nome utente e la password nella finestra del terminale:
```
username: cse*code+card
password: chap (must agree with profile)
```

Combinazioni di password CSUnix TACACS+ non funzionanti

Le seguenti combinazioni producono i seguenti errori di debug di CSUnix:

- CHAP e nessuna password "non crittografata" nel campo della password. L'utente immette `code+card` invece della password "cleartext". La RFC 1994 sulla protezione CHAP richiede la memorizzazione di password non crittografate.

```
username: cse
password: code+card

CiscoSecure INFO - User cse, No tokencard password received
CiscoSecure NOTICE - Authentication - Incorrect password;
```

- CHAP e password CHAP non valida.

```
username: cse*code+card
password: wrong chap password
```

(L'utente passa a SDI, mentre SDI passa l'utente, ma CSUnix non riesce a farlo perché la password CHAP è errata.)

```
CiscoSecure INFO - The character * was found in username:
   username=cse,passcode=1234755962
CiscoSecure INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
CiscoSecure INFO - sdi_verify: cse authenticated by ACE Srvr
CiscoSecure INFO - sdi: cse free external_data memory,state=GET_PASSCODE
CiscoSecure INFO - sdi_verify: rtn 1
CiscoSecure NOTICE - Authentication - Incorrect password;
```

- PAP e una password PAP non valida.

```
username: cse*code+card
password: wrong pap password
```

(L'utente passa a SDI, mentre SDI passa l'utente, ma CSUnix non riesce a farlo perché la password CHAP è errata.)

```
CiscoSecure INFO - 52 User Profiles and 8 Group Profiles loaded into Cache.
CiscoSecure INFO - The character * was found in username:
   username=cse,passcode=1234651500
CiscoSecure INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
CiscoSecure INFO - sdi_verify: cse authenticated by ACE Srvr
CiscoSecure INFO - sdi: cse free external_data memory,state=GET_PASSCODE
CiscoSecure INFO - sdi_verify: rtn 1
CiscoSecure NOTICE - Authentication - Incorrect password;
```

Debug dei profili di esempio CSUnix TACACS+ SDI

- L'utente deve eseguire l'autenticazione CHAP e di accesso; Il protocollo PAP non riesce.

```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
password = chap "********"
password = sdi
default service=permit
service=shell {
}
service=ppp {
protocol=lcp {
}
protocol=ip {
}
}
```

- L'utente deve eseguire l'autenticazione PAP e di accesso; Errore CHAP.

```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
member = admin
password = pap "********"
password = sdi
default service=permit
service=shell {
}
service=ppp {
protocol=lcp {
```

```
}
protocol=ip {
}
}
}
```

CSUnix RADIUS

Queste sezioni contengono le procedure RADIUS CSUnix.

Autenticazione di accesso con CSUnix e RADIUS

Per verificare l'autenticazione, effettuare le seguenti operazioni:

1. Eseguire un test iniziale senza SDI. Se questo profilo utente non funziona senza una password SDI per l'autenticazione di accesso, non funzionerà con una password SDI:
```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2="whatever" } reply_attributes= { 6=6 } } }
```
2. Una volta che il profilo funziona, sostituire "any" (qualsiasi) con "sdi" (sdi), come mostrato nell'esempio:
```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2=sdi } reply_attributes= { 6=6 } } }
```

Autenticazione PPP e PAP con CSUnix e RADIUS

Per verificare l'autenticazione, effettuare le seguenti operazioni:

Nota: l'autenticazione CHAP PPP con CSUnix e RADIUS non è supportata.

1. Eseguire un test iniziale senza SDI. Se il profilo utente non funziona senza una password SDI per l'autenticazione PPP/PAP e la "modalità asincrona dedicata", non funzionerà con una password SDI:
```
# ./ViewProfile -p 9900 -u cse

user = cse {
password = pap "pappass"
radius=Cisco {
check_items = {
}
reply_attributes= {
6=2
7=1
}
}
}
```
2. Quando il profilo funziona, aggiungere **password = sdi** al profilo e l'attributo **200=1** come mostrato nell'esempio (Cisco_Token_Immediate viene impostato su yes):

```
# ./ViewProfile -p 9900 -u cse
user = cse {
password = pap "pappass"
password = sdi
radius=Cisco {
check_items = {
200=1
}
reply_attributes= {
6=2
7=1
}
}
}
```

3. Nella sezione "**Advanced GUI**, server" **verificare che "Enable Token Caching**" sia impostato. È possibile verificare questa condizione dall'interfaccia della riga di comando (CLI) con:

```
$BASE/CLI/ViewProfile -p 9900 -u SERVER.#.#.#.#
!--- Where #.#.#.# is the IP address of the CSUnix server. TokenCachingEnabled="yes"
```

Connessione remota PPP e PAP

Si presume che **aaa authentication ppp** sia stato eseguito sul router **se necessario tacacs** e comandi **PPP autent PAP**. Immettere il nome utente e la password nella finestra del terminale prima di comporre il numero.

```
username: cse
password: code+card
```

Nota: sul PC, in Accesso remoto, verificare che sia selezionata l'opzione "Accetta qualsiasi autenticazione, incluso testo non crittografato".

Suggerimenti per il debug e la verifica

Nelle sezioni seguenti vengono forniti suggerimenti per il debug e la verifica.

Cisco Secure RADIUS, PPP e PAP

Questo è un esempio di debug corretto:

```
CiscoSecure DEBUG - RADIUS ; Outgoing Accept Packet id=133 (10.31.1.6)
    User-Service-Type = Framed-User
    Framed-Protocol = PPP
CiscoSecure DEBUG - RADIUS ; Request from host a1f0106 nas (10.31.1.6)
    code=1 id=134 length=73
CiscoSecure DEBUG - RADIUS ; Incoming Packet id=134 (10.31.1.6)
    Client-Id = 10.31.1.6
    Client-Port-Id = 1
    NAS-Port-Type = Async
    User-Name = "cse"
    Password = "?\235\306"
    User-Service-Type = Framed-User
    Framed-Protocol = PPP
CiscoSecure DEBUG - RADIUS ; Authenticate (10.31.1.6)
CiscoSecure DEBUG - RADIUS ; checkList: ASCEND_TOKEN_IMMEDIATE = 1
CiscoSecure DEBUG - RADIUS ; User PASSWORD type is Special
CiscoSecure DEBUG - RADIUS ; authPapPwd (10.31.1.6)
```

```
CiscoSecure INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
CiscoSecure DEBUG - profile_valid_tcaching FALSE ending.
CiscoSecure DEBUG - Token Caching.  IGNORE.
CiscoSecure INFO - sdi_verify: cse authenticated by ACE Srvr
CiscoSecure INFO - sdi: cse free external_data memory,state=GET_PASSCODE
CiscoSecure INFO - sdi_verify: rtn 1
CiscoSecure DEBUG - RADIUS ; Sending Ack of id 134 to a1f0106 (10.31.1.6)
```

Secure ID e CSUnix

Il debug viene memorizzato nel file specificato in /etc/syslog.conf per local0.debug.

Nessun utente può autenticarsi - SDI o altro:

Dopo aver aggiunto l'ID di protezione, accertarsi che non siano stati commessi errori durante la modifica del file CSU.cfg. Correggere il file CSU.cfg o ripristinare il file di backup CSU.cfg.

Questo è un esempio di debug corretto:

```
Dec 13 11:24:22 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
Dec 13 11:24:22 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
Dec 13 11:24:31 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_verify: cse authenticated by ACE Srvr
Dec 13 11:24:31 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_verify: cse authenticated by ACE Srvr
Dec 13 11:24:31 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi: cse free external_data memory,state=GET_PASSCODE
Dec 13 11:24:31 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi: cse free external_data memory,state=GET_PASSCODE
Dec 13 11:24:31 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_verify: rtn 1
Dec 13 11:24:31 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_verify: rtn 1
```

Questo è un esempio di debug errato:

CSUnix trova il profilo utente e lo invia al server SDI, ma il server SDI non riesce a individuare l'utente perché il passcode è errato.

```
Dec 13 11:26:22 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
Dec 13 11:26:22 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
   WARNING - sdi_verify: cse denied access by ACE Srvr
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
   WARNING - sdi_verify: cse denied access by ACE Srvr
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi: cse free external_data memory,state=GET_PASSCODE
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi: cse free external_data memory,state=GET_PASSCODE
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_verify: rtn 0
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_verify: rtn 0
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
   NOTICE - Authentication - Incorrect password;
```

```
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
   NOTICE - Authentication - Incorrect password;
```

Di seguito è riportato un esempio di server Ace inattivo:

Immettere **./aceserver stop** sul server SDI. L'utente non riceve il messaggio "Enter PASSCODE".

```
Dec 13 11:33:42 rtp-evergreen.rtp.cisco.com CiscoSecure:
   ERROR - sdi_challenge error: sd_init failed cli/srvr comm init (cse)
Dec 13 11:33:42 rtp-evergreen.rtp.cisco.com CiscoSecure:
   ERROR - sdi_challenge error: sd_init failed cli/srvr comm init (cse)
Dec 13 11:33:42 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi: cse free external_data memory,state=RESET
Dec 13 11:33:42 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi: cse free external_data memory,state=RESET
```

Informazioni correlate

- Pagina di supporto di Cisco Secure ACS per UNIX
- Notifiche sul campo per Cisco Secure ACS per UNIX
- Supporto tecnico – Cisco Systems