Konfigurieren von Cisco Secure UNIX und Secure ID (SDI-Client)

Inhalt

Einführung

Zur Implementierung der Konfiguration in diesem Dokument benötigen Sie eine Cisco Secure-Version, die die Secure ID von Security Dynamics Incorporated (SDI) unterstützt.

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 in den Cisco Technical Tips Conventions.

Installieren eines SDI-Clients (Secure ID) auf einem Cisco Secure UNIX-System

Hinweis: Die sichere ID wird normalerweise installiert, bevor Cisco Secure UNIX (CSUnix) installiert wurde. In diesen Anweisungen wird beschrieben, wie der SDI-Client nach der Installation von CSUnix installiert wird.

1. Führen Sie auf dem SDI-Server **sdadmin aus**. Teilen Sie dem SDI-Server mit, dass der CSUnix-Rechner ein Client ist, und geben Sie an, dass die betreffenden SDI-Benutzer auf dem CSUnix-Client aktiviert sind.
2. Verwenden Sie den Befehl **nslookup** #.#.#.# oder **nslookup** <hostname>, um sicherzustellen, dass der CSUnix-Client und der SDI-Server die gegenseitige Vorwärts- und Rückwärtssuche durchführen können.
3. Kopieren Sie die Datei des SDI-Servers /etc/sdace.txt in die Datei CSUnix client /etc/sdace.txt.
4. Kopieren Sie die Datei "sdconf.rec" des SDI-Servers in den CSUnix-Client. Diese Datei kann sich an einer beliebigen Stelle auf dem CSUnix-Client befinden. Wenn sie jedoch in derselben Verzeichnisstruktur auf dem CSUnix-Client wie auf dem SDI-Server platziert wird, muss sdace.txt nicht geändert werden.
5. Entweder /etc/sdace.txt oder VAR_ACE müssen auf den Pfad zeigen, in dem sich die Datei sdconf.rec befindet. Um dies zu überprüfen, führen Sie cat /etc/sdace.txt aus, oder überprüfen Sie die Ausgabe von env, um sicherzustellen, dass VAR_ACE im Root-Profil als Root-Start definiert ist.
6. Sichern Sie die CSU.cfg-Datei des CSUnix-Clients, und ändern Sie dann den Abschnitt AUTHEN config_external_authen_symbole mit den folgenden Zeilen:

```
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. CSUnix durch die Ausführung von **K80CiscoSecure** und **S80CiscoSecure** wiederverwerten.
8. Wenn $BASE/utils/psg anzeigt, dass der Cisco Secure AAA Server Process aktiv war, bevor die CSU.cfg-Datei geändert wurde, aber nicht danach, dann wurden Fehler in der Version

der CSU.cfg-Datei gemacht. Stellen Sie die ursprüngliche CSU.cfg-Datei wieder her, und versuchen Sie, die in Schritt 6 beschriebenen Änderungen erneut durchzuführen.

Anfängliche Tests der Secure ID und CSUnix

So testen Sie die sichere ID und CSUnix:

1. Stellen Sie sicher, dass ein Nicht-SDI-Benutzer Telnet zum Router nutzen und mit CSUnix authentifiziert werden kann. Wenn dies nicht funktioniert, funktioniert SDI nicht.
2. Testen Sie die grundlegende SDI-Authentifizierung im Router, und führen Sie den folgenden Befehl aus:

   ```
   aaa new-model

   aaa authentication login default tacacs+ none
   ```

   Hinweis: Hierbei wird davon ausgegangen, dass die **takacs-server-**Befehle bereits im Router aktiv sind.
3. Hinzufügen eines SDI-Benutzers über die CSUnix-Befehlszeile, um diesen Befehl einzugeben

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

4. Versuchen Sie, sich als Benutzer zu authentifizieren. . Wenn dieser Benutzer arbeitet, ist SDI betriebsbereit, und Sie können den Benutzerprofilen zusätzliche Informationen hinzufügen.
5. SDI-Benutzer können mit dem unbekannten_Benutzerprofil in CSUnix getestet werden. (Benutzer müssen nicht explizit in CSUnix aufgeführt werden, wenn sie alle an SDI übergeben werden und alle dasselbe Profil haben.) Wenn bereits ein unbekanntes Benutzerprofil vorhanden ist, löschen Sie es mithilfe des folgenden Befehls:

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

6. Verwenden Sie diesen Befehl, um ein anderes unbekanntes Benutzerprofil hinzuzufügen:

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

   Dieser Befehl leitet alle unbekannten Benutzer an SDI weiter.

Sichere ID und CSUnix: TACACS+-Profil

1. Führen Sie einen ersten Test ohne SDI durch. Wenn dieses Benutzerprofil ohne SDI-Kennwort für die Anmeldeauthentifizierung, das Challenge Handshake Authentication Protocol (CHAP) und das Password Authentication Protocol (PAP) nicht funktioniert, funktioniert es nicht mit einem SDI-Kennwort:

   ```
   # ./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. Wenn das Profil funktioniert, fügen Sie dem Profil "sdi" anstelle von "clear" hinzu, wie in diesem Beispiel gezeigt:

```
# ./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 {
}
}

}
```

Funktionsweise des Profils

Dieses Profil ermöglicht dem Benutzer, sich mit folgenden Kombinationen anzumelden:

- Telnet zum Router und SDI. (Dabei wird davon ausgegangen, dass der Befehl **aaa authentication login default tacacs+** auf dem Router ausgeführt wurde.)
- PPP-Einwahlverbindung und PAP für das Netzwerk. (Dabei wird davon ausgegangen, dass die **AAA-Standard-Authentifizierungs-PPP-Standardbefehle (falls erforderlich) für Takaks** und **ppp-Authentifizierungspopp-**Befehle auf dem Router ausgeführt wurden.)**Hinweis:** Stellen Sie sicher, dass auf dem PC in DFÜ-Netzwerk die Option "Authentifizierung einschließlich Klartext akzeptieren" aktiviert ist. Geben Sie vor dem Wählen eine der folgenden Kombinationen aus Benutzername und Kennwort im Terminalfenster ein:

```
username: cse*code+card
password: pap (must agree with profile)

username: cse
password: code+card
```

- PPP-Einwahlverbindung und CHAP für das Netzwerk. (Dabei wird davon ausgegangen, dass die **AAA-Standard-Authentifizierungs-PPP-Standardbefehle (falls erforderlich) für Takaks** und **ppp-Authentifizierungs-chap-**Befehle auf dem Router ausgeführt wurden.)**Hinweis:** Auf dem PC muss im Wählnetzwerk entweder "Annehmen einer Authentifizierung einschließlich Klartext" oder "Nur verschlüsselte Authentifizierung akzeptieren" aktiviert werden. Geben Sie vor dem Wählen den folgenden Benutzernamen und das Kennwort im Terminalfenster ein:

```
username: cse*code+card
password: chap (must agree with profile)
```

CSUnix TACACS+-Kennwortkombinationen, die nicht funktionieren

Diese Kombinationen führen zu folgenden CSUnix-Debugfehlern:

- CHAP und kein "Klartext"-Kennwort im Kennwortfeld. Der Benutzer gibt `Code+Card` anstelle des Kennworts "clear text" ein. RFC 1994 auf CHAP erfordert eine Kennwortspeicherung mit Klartext.

  username: cse
  password: code+card

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

- CHAP und ein falsches CHAP-Kennwort.

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

  (Der Benutzer wird an SDI weitergeleitet, und SDI übergibt den Benutzer, CSUnix schlägt jedoch fehl, da das CHAP-Kennwort falsch ist.)

  ```
  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 und ein falsches PAP-Kennwort.

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

  (Der Benutzer wird an SDI weitergeleitet, und SDI übergibt den Benutzer, CSUnix schlägt jedoch fehl, da das CHAP-Kennwort falsch ist.)

  ```
  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;
  ```

Debuggen von CSUnix-TACACS+-SDI-Beispielprofilen

- Der Benutzer muss CHAP- und Anmeldeauthentifizierung durchführen. PAP schlägt fehl.

  ```
  # ./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 {
  }
  }
  ```

- Der Benutzer muss eine PAP- und Anmeldeauthentifizierung durchführen. CHAP schlägt fehl.

```
# ./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

Diese Abschnitte enthalten CSUnix-RADIUS-Prozeduren.

Anmeldeauthentifizierung mit CSUnix und RADIUS

So testen Sie die Authentifizierung:

1. Führen Sie einen ersten Test ohne SDI durch. Wenn dieses Benutzerprofil ohne ein SDI-Kennwort für die Anmeldeauthentifizierung nicht funktioniert, funktioniert es nicht mit einem SDI-Kennwort:

```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2="whatever" } reply_attributes= { 6=6 } } }
```

2. Sobald dieses Profil funktioniert, ersetzen Sie "any" durch "sdi" (was auch immer ist), wie in diesem Beispiel gezeigt:

```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2=sdi } reply_attributes= { 6=6 } } }
```

PPP- und PAP-Authentifizierung mit CSUnix und RADIUS

So testen Sie die Authentifizierung:

Hinweis: PPP CHAP-Authentifizierung mit CSUnix und RADIUS wird nicht unterstützt.

1. Führen Sie einen ersten Test ohne SDI durch. Wenn dieses Benutzerprofil ohne ein SDI-Kennwort für die PPP/PAP-Authentifizierung und den dedizierten asynchronen Modus nicht funktioniert, funktioniert es nicht mit einem SDI-Kennwort:

```
# ./ViewProfile -p 9900 -u cse
```

```
user = cse {
password = pap "pappass"
radius=Cisco {
check_items = {
}
reply_attributes= {
6=2
7=1
}
}
}
```

2. Wenn das obige Profil funktioniert, fügen Sie dem Profil **password = sdi** hinzu und fügen Sie das Attribut **200=1** hinzu, wie in diesem Beispiel gezeigt (dies setzt Cisco_Token_Immediate auf 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. Stellen Sie im Abschnitt "**Erweiterte Benutzeroberfläche**, Server" **sicher, dass "Token-Caching aktivieren"** eingestellt ist. Dies kann über die Befehlszeilenschnittstelle (CLI) bestätigt werden mit:

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

Einwählnetzwerk PPP-Verbindung und PAP

Es wird davon ausgegangen, dass **bei Bedarf Taks** und **PAP-PAP**-Befehle **mit PPP-Authentifizierung** auf dem Router **als Standard-Authentifizierungs-PPP** ausgeführt wurden. Geben Sie vor dem Wählen im Terminalfenster diesen Benutzernamen und das Kennwort ein.

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

Hinweis: Stellen Sie sicher, dass auf dem PC in DFÜ-Netzwerk die Option "Authentifizierung einschließlich Klartext akzeptieren" aktiviert ist.

Tipps zu Debuggen und Überprüfung

Diese Abschnitte enthalten Tipps für das Debuggen und die Überprüfung.

Cisco Secure RADIUS, PPP und PAP

Dies ist ein Beispiel für ein gutes Debuggen:

```
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)
```

Sichere ID und CSUnix

Das Debuggen wird in der Datei gespeichert, die in /etc/syslog.conf für local0.debug angegeben ist.

Keine Benutzer können sich authentifizieren - SDI oder auf andere Weise:

Nachdem Sie die sichere ID hinzugefügt haben, stellen Sie sicher, dass beim Ändern der CSU.cfg-Datei keine Fehler aufgetreten sind. Korrigieren Sie die CSU.cfg-Datei, oder kehren Sie zur Backup-CSU.cfg-Datei zurück.

Dies ist ein Beispiel für ein gutes Debuggen:

```
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
```

Dies ist ein Beispiel für ein fehlerhaftes Debuggen:

CSUnix findet das Benutzerprofil und sendet es an den SDI-Server, aber der SDI-Server versagt den Benutzer, weil der Passcode fehlerhaft ist.

```
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;
```

Dies ist ein Beispiel, das zeigt, dass der ACE-Server ausgefallen ist:

Geben Sie **./ACSERVER stop** auf dem SDI-Server ein. Der Benutzer erhält die Meldung "PASSCODE eingeben" nicht.

```
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
```

Zugehörige Informationen

- Support-Seite für Cisco Secure ACS für UNIX
- Problemhinweise zu Cisco Secure ACS für UNIX
- Technischer Support - Cisco Systems