Cisco Secure UNIX en Secure ID (SDI-client) configureren

Inhoud

Inleiding

Om de configuratie in dit document uit te voeren, hebt u een Cisco Secure versie nodig die de Secure ID van Security Dynamics Geïntegreerde (SDI) ondersteunt.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Een SDI-client (Secure ID) installeren op een Cisco Secure UNIX-machine

Opmerking: Secure ID is meestal geïnstalleerd voordat Cisco Secure UNIX (CSUnix) is geïnstalleerd. Deze instructies beschrijven hoe de SDI-client moet worden geïnstalleerd nadat CSUnix is geïnstalleerd.

1. Start **sdadmin** op de SDI-server. Vertel de SDI-server dat de CSUnix-machine een client is en specificeer dat de SDI-gebruikers in kwestie op de CSUnix-client zijn geactiveerd.
2. Gebruik de opdracht **nslookup** #.#.# of **nslookup** <hostname> om ervoor te zorgen dat de CSUnix-client en de SDI-server vooruit kunnen kijken en elkaars raadpleging kunnen omkeren.
3. Kopieer het /etc/sdace.txt-bestand van de SDI-server naar het /etc/sdace.txt-bestand van de CSUnix-client.
4. Kopieert het sdconf.rec-bestand van de SDI-server naar de CSUnix-client; dit bestand kan overal op de CSUnix-client worden geplaatst. Als deze echter in dezelfde directory structuur op de CSUnix-client is geplaatst als op de SDI-server, hoeft sdace.txt niet te worden aangepast.
5. Ofwel /etc/sdace.txt of VAR_ACE moet naar het pad wijzen waar het sdconf.rec-bestand zich bevindt. Om dit te verifiëren, open kat /etc/sdace.txt, of controleer de output van env om er zeker van te zijn dat VAR_ACE in het profiel van de wortel wordt gedefinieerd zoals de wortel begint.
6. back-up van CSUnix client s CSU.cfg en wijzig vervolgens de sectie AUTHEN COMPONENT_foreign_authen_symbolen met deze lijnen:

```
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 recyclen door uitvoering van **K80Cisco Secure** en **S80Cisco** Secure.
8. Als $BASE/utils/psg toont dat het Cisco Secure AAA-serverproces actief was voordat het CSU.cfg-bestand werd gewijzigd maar niet daarna, zijn er fouten gemaakt in de herziening van het CSU.cfg-bestand. Herstelt het oorspronkelijke CSU.cfg-bestand en probeer de in

stap 6 beschreven wijzigingen opnieuw aan te brengen.

Eerste test van de beveiligde ID en CSUnix

Voer de volgende stappen uit om beveiligde ID en CSUnix te testen:

1. Zorg ervoor dat een niet-SDI gebruiker telnet aan de router kan en met CSUnix voor authentiek kan worden verklaard. Als dit niet werkt zal SDI niet werken.
2. Test basisauthenticatie SDI in de router en voer deze opdracht uit:

   ```
   aaa new-model

   aaa authentication login default tacacs+ none
   ```

   Opmerking: Dit veronderstelt dat de opdrachten **van de tacacs-server** al actief zijn in de router.
3. Voeg een SDI-gebruiker toe van de CSUnix-opdrachtregel om deze opdracht in te voeren

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

4. Probeer als een gebruiker te authenticeren. . Als die gebruiker werkt, is SDI operationeel en u kunt extra informatie aan de gebruikersprofielen toevoegen.
5. SDI-gebruikers kunnen worden getest met het onbekende_gebruikersprofiel in CSUnix. (De gebruikers hoeven niet expliciet in CSUnix te worden vermeld als ze allemaal worden doorgegeven aan SDI en allemaal hetzelfde profiel hebben.) Als er al een onbekend gebruikersprofiel bestaat, verwijdert u het profiel met de hulp van deze opdracht:

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

6. Gebruik deze opdracht om een ander onbekend gebruikersprofiel toe te voegen:

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

   Deze opdracht geeft alle onbekende gebruikers door aan SDI.

Beveiligde ID en CSUnix: Profiel van TACACS+

1. Voer een initiële test uit zonder SDI. Als dit gebruikersprofiel niet werkt zonder een SDI-wachtwoord voor inlogverificatie, Challenge Handshake Authentication Protocol (CHAP) en Password Authentication Protocol (PAP), werkt het niet met een SDI-wachtwoord:

   ```
   # ./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. Wanneer het profiel eenmaal werkt, voegt u "SDI" toe aan het profiel in plaats van "helder" zoals in dit voorbeeld wordt getoond:

```
# ./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 {
}
}

}
```

Hoe het profiel werkt

Met dit profiel kan de gebruiker inloggen met deze combinaties:

- Telnet aan de router en gebruik SDI. (Dit veronderstelt dat de standaard **tacacs+** opdracht **van de** authenticatie op de router is uitgevoerd.)
- Dial-up netwerk PPP verbinding en PAP. (Dit veronderstelt dat de **standaard** van de **AAA authenticatie ppp indien-nodig tacacs** en **ppp** copyright bevelen op de router zijn uitgevoerd).**Opmerking:** Controleer op de pc in een inbelnetwerk of "Een verificatie inclusief duidelijke tekst accepteren" is ingeschakeld. Voer in het eindvenster een van deze combinaties van gebruikersnaam en wachtwoord in voordat u een keuze maakt:

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

username: cse
password: code+card
```

- Dial-up netwerk PPP verbinding en CHAP. (Dit veronderstelt dat de **standaard** van de **AAA authenticatie ppp indien-nodig tacacs** en **ppp** copyright bevelen op de router zijn uitgevoerd).**Opmerking:** Op de PC, in Dial-Up Network, moet "Accept any Authentication including clear text" of "Accept only Encryption" zijn gecontroleerd. Voordat u het programma selecteert, voert u deze gebruikersnaam en het wachtwoord in het terminalvenster in:

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

CSUnix TACACS+ wachtwoordcombinaties die niet werken

Deze combinaties produceren deze CSUnix debug:

- CHAP en geen "cleartext" wachtwoord in het wachtwoordveld. De gebruiker voert `code+card in` in in plaats van het wachtwoord voor het vrijgeven van de tekst. RFC 1994 op CHAP vereist een heldere opslag van tekstwachtwoorden.

```
username: cse
password: code+card

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

- CHAP en een slecht CHAP wachtwoord.

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

(De gebruiker gaat over naar SDI en SDI geeft de gebruiker door, maar CSUnix mislukt de gebruiker omdat het wachtwoord CHAP slecht is.)

```
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 en een slecht PAP-wachtwoord.

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

(De gebruiker gaat over naar SDI en SDI geeft de gebruiker door, maar CSUnix mislukt de gebruiker omdat het wachtwoord CHAP slecht is.)

```
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;
```

Aanhoudende CSUnix TACACS+ SDI-voorbeeldbestanden

- De gebruiker moet CHAP en inlogverificatie uitvoeren. PAP mislukt.

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

- De gebruiker moet PAP- en inlogverificatie uitvoeren. CHAP faalt.

```
# ./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

Deze secties bevatten RADIUS-procedures van CSUnix.

Login-verificatie met CSUnix en RADIUS

Voer deze stappen uit om de authenticatie te testen:

1. Voer een initiële test uit zonder SDI. Als dit gebruikersprofiel niet werkt zonder een SDI-wachtwoord voor inlogverificatie, werkt het niet met een SDI-wachtwoord:
```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2="whatever" } reply_attributes= { 6=6 } } }
```
2. Als dit profiel eenmaal werkt, vervang "wat" door "wat" zoals in dit voorbeeld wordt getoond:
```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2=sdi } reply_attributes= { 6=6 } } }
```

PPP- en PAP-verificatie met CSUnix en RADIUS

Voer deze stappen uit om de authenticatie te testen:

Opmerking: PPP CHAP-verificatie met CSUnix en RADIUS wordt niet ondersteund.

1. Voer een initiële test uit zonder SDI. Als dit gebruikersprofiel niet werkt zonder een SDI-wachtwoord voor PPP/PAP-verificatie en "async mode toegewijd", werkt het niet met een SDI-wachtwoord:
```
# ./ViewProfile -p 9900 -u cse

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

```
}
}
```

2. Zodra het bovenstaande profiel werkt, voegt u **het wachtwoord toe = sdi** aan het profiel en voegt u attribuut **200=1 toe** zoals in dit voorbeeld (dit stelt Cisco_Token_Immediate in om ja.):

```
# ./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. In de "**Geavanceerde GUI**, server sectie" **moet "Token Caching inschakelen**" worden ingesteld. Dit kan worden bevestigd vanuit de opdrachtregel interface (CLI) met:

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

Netwerkverbinding en -PAP met snelkiezer

Het wordt verondersteld dat **de a** authenticatie ppp standaard indien-**noodzakelijke tacacs** en **PPP auen PAP** opdrachten op de router zijn uitgevoerd. Voer deze gebruikersnaam en het wachtwoord in in het terminalvenster voordat u inbel.:

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

Opmerking: Controleer op de PC in het inbelnetwerk of "Een verificatie inclusief duidelijke tekst accepteren" is ingeschakeld.

Tips voor detectie en verificatie

Deze secties bevatten tips voor debug en verificatie.

Cisco Secure RADIUS, PPP en PAP

Dit is een voorbeeld van een goed debug:

```
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)
```

Beveiligde ID en CSUnix

Het debug wordt opgeslagen in het bestand dat in /etc/syslog.conf voor local0.debug is gespecificeerd.

Geen gebruikers kunnen - SDI of anderszins:

Controleer na het toevoegen van de Secure ID of er geen fouten zijn gemaakt tijdens het wijzigen van het CSU.cfg-bestand. Bevestig het CSU.cfg-bestand of voer terug naar het CSU.cfg-bestand.

Dit is een voorbeeld van een goed debug:

```
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
```

Dit is een voorbeeld van een slecht debug:

CSUnix vindt het gebruikersprofiel en stuurt het naar de SDI server, maar de SDI server mislukt de gebruiker omdat de wachtcode slecht is.

```
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;
```

Dit is een voorbeeld waaruit blijkt dat de ACE-server is uitgevallen:

Voer **een reservekopie-/**reservetender in op de SDI-server. De gebruiker krijgt het bericht "PASSCODE invoeren" niet.

```
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
```

Gerelateerde informatie

- Cisco Secure ACS voor UNIX-ondersteuningspagina
- Veldmeldingen voor Cisco Secure ACS voor UNIX
- Technische ondersteuning - Cisco-systemen