Configuración Cisco Secure UNIX e Secure ID (Cliente SDI)

Contenido

Introducción

Para implementar la configuración en este documento, usted necesita cualquier versión segura de Cisco que soporte Secure ID s del Security Dynamics Incorporated (SDI) '.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Instalación de un cliente SDI (ID segura) en una máquina con Cisco Secure UNIX

Nota: El Secure ID está instalado generalmente antes de que Cisco UNIX seguro (CSUnix) haya estado instalado. Estas instrucciones describen cómo instalar al cliente SDI después de que CSUnix haya estado instalado.

1. En el servidor SDI, ejecute el **sdadmin**. Diga al servidor SDI que la máquina de CSUnix es un cliente y especifique que activan a los usuarios de SDI en la pregunta en el cliente de CSUnix.
2. Utilice el **nslookup** #.#.#.# o el **comando nslookup <hostname>** de aseegurarse al cliente de CSUnix y el servidor SDI puede hacer adelante y búsqueda inversa de uno a.
3. Copie el archivo de /etc/sdace.txt del servidor SDI al archivo de /etc/sdace.txt del cliente de CSUnix.
4. Copie el archivo sdconf.rec del servidor SDI al cliente de CSUnix; este archivo puede residir dondequiera en el cliente de CSUnix. Sin embargo, si se coloca en la misma estructura de directorios en el cliente de CSUnix que era en el servidor SDI, sdace.txt no tiene que ser modificado.
5. O /etc/sdace.txt o VAR_ACE debe señalar a la trayectoria en donde se localiza el archivo sdconf.rec. Para verificar esto, funcione con el gato /etc/sdace.txt, o marque la salida del ENV para estar seguro que VAR_ACE está definido en el perfil de la raíz mientras que la raíz comienza.
6. Sostenga el CSU.cfg del cliente de CSUnix, después modifique la sección de los config_external_authen_symbols AUTHEN con estas líneas:

```
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. Recicle CSUnix por la ejecución de **K80CiscoSecure** y de **S80CiscoSecure**.
8. Si $BASE/utils/psg muestra que Cisco asegura el proceso del proceso de servidor de AAA

era activo antes de que el archivo CSU.cfg fuera modificado pero no luego, después los errores fueron hechos en la revisión del archivo CSU.cfg. Restablezca el archivo CSU.cfg original e intente realizar los cambios delineados en el paso 6 otra vez.

Pruebas iniciales del Secure ID y csunix

Para probar Secure ID y csunix, realice estos pasos:

1. Aseegurese que usuario no SDI puede Telnet al router y ser autenticado con CSUnix. Si esto no trabaja, el SDI no trabajará.
2. Pruebe básico Autenticación SDI en el router y funcione con este comando:

   ```
   aaa new-model

   aaa authentication login default tacacs+ none
   ```

   Nota: Esto asume que los **comandos tacacs-server** son ya activos en el router.
3. Agregue a un usuario de SDI de la línea de comando csunix para ingresar este comando

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

4. Intente autenticar como usuario. Si ese usuario trabaja, SDI está funcionando, y usted puede agregar la información adicional a los perfiles del usuario.
5. Los usuarios de SDI pueden ser probados con el perfil del unknown_user en CSUnix. (Los usuarios no tienen que ser enumerados explícitamente en CSUnix si ellos que pasan todos apagado al SDI y todos tienen el mismo perfil.) Si hay un perfil de usuario desconocido ya exista, borrelo con la ayuda de este comando:

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

6. Utilice este comando de agregar otro perfil de usuario desconocido:

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

   Este comando pasa de todos los usuarios desconocidos al SDI.

Secure ID y csunix: Perfil de TACACS+

1. Realice una prueba inicial sin el SDI. Si este perfil del usuario no trabaja sin una contraseña SDI para la autenticación de inicio de sesión, el Challenge Handshake Authentication Protocol (CHAP), y el protocolo password authentication (PAP), no trabajará con una contraseña 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 vez que el perfil trabaja, agregue el “sdi” al perfil en lugar de “claro” tal y como se muestra en de este ejemplo:

```
# ./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 {
}
}

}
```

Cómo funciona el perfil

Este perfil permite que el usuario inicie sesión con estas combinaciones:

- Telnet al router y al SDI del uso. (Esto asume que han ejecutado al **comando aaa authentication login default tacacs+** en el router.)
- Conexión PPP del dial-up networking y PAP. (Esto asume que han ejecutado a los **comandos aaa authentication ppp default if-needed tacacs y ppp authen pap** en el router).**Nota:** En el PC, en el dial-up networking, aseegurese el “Accept any authentication incluyendo el texto claro” se marca. Antes de marcar, ingrese una de estas Combinaciones de nombre de usuario/contraseña en la ventana de terminal:

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

username: cse
password: code+card
```

- Conexión PPP y GRIETA del dial-up networking. (Esto asume que han ejecutado a los **comandos aaa authentication ppp default if-needed tacacs y ppp authen chap** en el router).**Nota:** En el PC, en el dial-up networking, o el “Accept any authentication incluyendo el texto claro” o “valida solamente la autenticación encriptada” debe ser marcado. Antes de marcar, ingrese este nombre de usuario y contraseña en la ventana de terminal:

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

Combinaciones de la contraseña de CSUnix TACACS+ que no trabajan

Estas combinaciones producen estos errores del debug de CSUnix:

- AGRIETE y no contraseña del “texto claro” en el campo de contraseña. El usuario ingresa el

`code+card` en vez de la contraseña del “texto claro”. El RFC 1994 en la GRIETA requiere el almacenamiento de la contraseña de texto sin cifrar.

```
username: cse
password: code+card

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

- GRIETA y una mala contraseña de la GRIETA.

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

(El usuario pasa apagado al SDI, y el SDI pasa al usuario, pero CSUnix falla al usuario porque la contraseña de la GRIETA es mala.)

```
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 y una mala contraseña PAP.

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

(El usuario pasa apagado al SDI, y el SDI pasa al usuario, pero CSUnix falla al usuario porque la contraseña de la GRIETA es mala.)

```
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;
```

Hacer el debug de los ejemplos de perfil del SDI de CSUnix TACACS+

- El usuario necesita hacer la GRIETA y la autenticación de inicio de sesión; El PAP falla.

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

- El usuario necesita hacer el PAP y la autenticación de inicio de sesión; La GRIETA falla.

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

RADIUS CSUnix

Estas secciones contienen RADIUS CSUnix los procedimientos.

Autenticación de inicio de sesión con CSUnix y el RADIUS

Realice estos pasos a la prueba de la autentificación:

1. Realice una prueba inicial sin el SDI. Si este perfil del usuario no trabaja sin una contraseña SDI para la autenticación de inicio de sesión, no trabajará con una contraseña SDI:
```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2="whatever" } reply_attributes= { 6=6 } } }
```
2. Una vez que este perfil trabaja, substituya “sea cual sea” con el “sdi” tal y como se muestra en de este ejemplo:
```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2=sdi } reply_attributes= { 6=6 } } }
```

PPP y autenticación PAP con CSUnix y el RADIUS

Realice estos pasos a la prueba de la autentificación:

Nota: La autenticación CHAP de PPP con CSUnix y el RADIUS no se soporta.

1. Realice una prueba inicial sin el SDI. Si este perfil del usuario no trabaja sin una contraseña SDI para la autenticación PPP/PAP y el “modo asincrónico dedicado,” no trabajará con una contraseña SDI:
```
# ./ViewProfile -p 9900 -u cse

user = cse {
password = pap "pappass"
radius=Cisco {
check_items = {
}
reply_attributes= {
```

```
6=2
7=1
}
}
}
```

2. Una vez los trabajos antedichos del perfil, agregan la **contraseña = el sdi al** perfil y agregan el atributo **200=1** tal y como se muestra en de este ejemplo (éste fija Cisco_Token_Immediate al sí.):

```
# ./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. En el "**GUI avanzado**, se fija la sección del servidor," **se aseegura el "Habilitar almacenamiento de token en caché"**. Esto se puede confirmar del comando line interface(cli) con:

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

Conexión PPP de interconexión de redes de marcación manual y PAP

Se asume que han ejecutado a los **comandos aaa authentication ppp default if-needed tacacs y PPP authen PAP** en el router. Ingrese este nombre de usuario y contraseña en la ventana de terminal antes de que usted marque.:

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

Nota: En el PC, en el dial-up networking, aseegurese el "Accept any authentication incluyendo el texto claro" se marca.

Consejos sobre Depuración y Verificación

Estas secciones contienen las extremidades para las extremidades del debug y verificación.

Cisco Secure RADIUS, PPP, y PAP

Éste es un ejemplo de un debug correcta:

```
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 y csunix

El debug se salva en el archivo especificado en /etc/syslog.conf para local0.debug.

Ningunos usuarios pueden autenticar - SDI o de otra manera:

Después de que usted agregue el Secure ID, aseegurese que no se hizo ningunos errores cuando usted modifica el archivo CSU.cfg. Repare el archivo CSU.cfg o invierta al archivo CSU.cfg de reserva.

Éste es un ejemplo de un debug correcta:

```
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
```

Éste es un ejemplo de un debug inadecuada:

CSUnix encuentra el perfil del usuario y lo envía al servidor SDI, pero el servidor SDI falla al usuario porque la contraseña es mala.

```
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;
```

Esto es una demostración del ejemplo que el servidor de Ace está abajo:

Ingrese la **parada de ./aceserver** en el servidor SDI. El usuario no consigue el mensaje "Ingresar clave".

```
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
```

Información Relacionada

- Página de soporte de Cisco Secure ACS para Windows
- Field Notice para el Cisco Secure ACS para UNIX
- Soporte Técnico - Cisco Systems