Configuration de Cisco Secure UNIX et de Secure ID (client SDI)

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Installer un client de SDI (ID sécurisé) sur un ordinateur de Cisco Secure UNIX
Test initial de l'ID et du CSUnix sécurisés
ID sécurisé et CSUnix : Profil TACACS+
Comment le profil fonctionne
Combinaisons de mot de passe de CSUnix TACACS+ qui ne fonctionnent pas
Exemples de profil de SDI de débogage CSUnix TACACS+
RAYON de CSUnix
Authentification de connexion avec CSUnix et RAYON
PPP et authentification PAP avec CSUnix et RAYON
Connexion PPP commutée de réseau et PAP
Debug et conseils de vérification
RAYON Cisco Secure, PPP, et PAP
ID sécurisé et CSUnix
Informations connexes

Introduction

Pour implémenter la configuration dans ce document, vous avez besoin de n'importe quelle version Cisco Secure qui prend en charge ID sécurisé s incorporé par dynamics de Sécurité (SDI) le '.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Installer un client de SDI (ID sécurisé) sur un ordinateur de Cisco Secure UNIX

Remarque: L'ID sécurisé est habituellement installé avant que Cisco Secure UNIX (CSUnix) ait été installé. Ces instructions décrivent comment installer le client de SDI après que CSUnix ait été installé.

1. Sur le serveur de SDI, exécutez le **sdadmin**. Dites le serveur de SDI que l'ordinateur de CSUnix est un client et le spécifiez que les utilisateurs de SDI en question sont lancés sur le client de CSUnix.
2. Utilisez le **nslookup** #.#.#.# ou la commande de <hostname> de **nslookup** de s'assurer que le client de CSUnix et le serveur de SDI peuvent faire la consultation en avant et inverse de l'un l'autre.
3. Copiez le fichier de /etc/sdace.txt du serveur de SDI sur le fichier de /etc/sdace.txt de client de CSUnix.
4. Copiez le fichier sdconf.rec du serveur de SDI sur le client de CSUnix ; ce fichier peut résider n'importe où sur le client de CSUnix. Cependant, s'il est placé dans la même structure de répertoire sur le client de CSUnix comme il était sur le serveur de SDI, sdace.txt ne doit pas être modifié.
5. /etc/sdace.txt ou VAR_ACE doit indiquer le chemin où le fichier sdconf.rec se trouve. Pour vérifier ceci, exécutez le cat /etc/sdace.txt, ou vérifiez la sortie de l'ENV pour être sûr que VAR_ACE est défini dans le profil de la racine comme débuts de racine.
6. Sauvegardez le CSU.cfg du client de CSUnix, puis modifiez la section de config_external_authen_symbols AUTHEN avec ces lignes :
7. Réutilisez CSUnix par l'exécution de **K80CiscoSecure** et de **S80CiscoSecure**.
8. Si $BASE/utils/psg prouve que le procédé Cisco Secure de processus de serveur d'AAA était en activité avant que le fichier CSU.cfg ait été modifié mais pas après, alors des erreurs ont été faites dans la révision du fichier CSU.cfg. Restaurez le fichier CSU.cfg et l'essai d'origine pour apporter les modifications tracées les grandes lignes dans l'étape 6 de nouveau.

Test initial de l'ID et du CSUnix sécurisés

Pour tester l'ID sécurisé et le CSUnix, exécutez ces étapes :

1. Assurez-vous qu'un utilisateur de non-SDI peut telnet au routeur et être authentifié avec CSUnix. Si ceci ne fonctionne pas, le SDI ne fonctionnera pas.
2. Testez l'authentification de base de SDI dans le routeur et exécutez cette commande : `aaa new-model aaa authentication login default tacacs+ none` **Remarque:** Ceci suppose que les ordres de **serveur TACACS** sont déjà en activité dans le routeur.
3. Ajoutez un utilisateur de SDI de la ligne de commande de CSUnix pour sélectionner cette commande
   `$BASE/CLI/AddProfile -p 9900 -u sdi_user -pw sdi`

4. Essayez d'authentifier en tant qu'utilisateur. Si cet utilisateur travaille, l'isoperational de SDI, et vous pouvez ajouter les informations complémentaires aux profils utilisateurs.
5. Des utilisateurs de SDI peuvent être examinés avec le profil d'unknown_user dans CSUnix. (Des utilisateurs ne doivent pas être explicitement répertoriés dans CSUnix s'ils que tous sont passés hors fonction au SDI et tous ont le même profil.) S'il y a un profil utilisateur inconnu déjà existez, supprimez-le avec l'aide de cette commande :
   `$BASE/CLI/DeleteProfile -p 9900 -u unknown_user`
6. Utilisez cette commande d'ajouter un autre profil utilisateur inconnu :
   `$BASE/CLI/AddProfile -p 9900 -u unknown_user -pw sdi` Cette commande passe outre de tous les utilisateurs inconnus au SDI.

ID sécurisé et CSUnix : Profil TACACS+

1. Réalisez un premier essai sans SDI. Si ce profil utilisateur ne fonctionne pas sans mot de passe de SDI pour l'authentification de connexion, le protocole d'authentification CHAP (Challenge Handshake Authentication Protocol), et le Password Authentication Protocol (PAP), cela ne fonctionnera pas avec un mot de passe de 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. Une fois que le profil fonctionne, ajoutez le « SDI » au profil au lieu de « clair » suivant les indications de cet exemple :
```
# ./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 { } } }
```

Comment le profil fonctionne

Ce profil permet à l'utilisateur pour ouvrir une session avec ces combinaisons :

- Telnet au routeur et au SDI d'utilisation. (Ceci suppose que la commande de l'**aaa authentication login default tacacs+** a été exécutée sur le routeur.)
- Connexion PPP commutée de réseau et PAP. (Ceci suppose que les **tacacs** et le **ppp si-nécessaires de par défaut d'aaa authentication ppp authen des** commandes **PAP** ont été exécutés sur le routeur).**Remarque:** Sur le PC, dans le réseau commuté, assurez-vous que « recevoir n'importe quelle authentification comprenant le texte clair » est vérifié. Avant la composition, écrivez une de ces combinaisons de nom d'utilisateur/mot de passe dans le

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

username: cse
password: code+card
```

- Connexion PPP et CHAP commutés de réseau. (Ceci suppose que les **tacacs** et le **ppp si-nécessaires de par défaut d'aaa authentication ppp authen le CHAP que des** commandes ont été exécutées sur le routeur).**Remarque:** Sur le PC, dans le réseau commuté, ou « recevez n'importe quelle authentification comprenant le texte clair » ou « recevez seulement l'authentification chiffrée » doit être vérifié. Avant la composition, écrivez ce nom d'utilisateur et mot de passe dans le terminal window :
```
username: cse*code+card
password: chap (must agree with profile)
```

Combinaisons de mot de passe de CSUnix TACACS+ qui ne fonctionnent pas

Ces combinaisons produisent ce debug errors de CSUnix :

- GERCEZ et non mot de passe de « libellé » dans le domaine de mot de passe. L'utilisateur écrit `code+card` au lieu du mot de passe de « libellé ». RFC 1994 sur le CHAP exige la mémoire de mot de passe des textes clairs.
```
username: cse password: code+card CiscoSecure INFO - User cse, No tokencard password
received CiscoSecure NOTICE - Authentication - Incorrect password;
```
- CHAP et un mauvais mot de passe CHAP.
username: cse*code+card password: wrong chap password (L'utilisateur passe hors fonction au SDI, et le SDI passe l'utilisateur, mais CSUnix échoue l'utilisateur parce que le mot de passe CHAP est mauvais.)
```
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 et un mauvais mot de passe PAP.
username: cse*code+card password: wrong pap password (L'utilisateur passe hors fonction au SDI, et le SDI passe l'utilisateur, mais CSUnix échoue l'utilisateur parce que le mot de passe CHAP est mauvais.)
```
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;
```

Exemples de profil de SDI de débogage CSUnix TACACS+

- Les besoins de l'utilisateur de faire le CHAP et l'authentification de connexion ; Le PAP échoue.
```
# ./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 {
}
}
```

- Les besoins de l'utilisateur de faire le PAP et l'authentification de connexion ; Le CHAP échoue.
```
# ./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 {
}
}
}
```

RAYON de CSUnix

Ces sections contiennent des procédures de RAYON de CSUnix.

Authentification de connexion avec CSUnix et RAYON

Exécutez ces étapes au test d'authentification :

1. Réalisez un premier essai sans SDI. Si ce profil utilisateur ne fonctionne pas sans mot de passe de SDI pour l'authentification de connexion, cela ne fonctionnera pas avec un mot de passe de SDI :
```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2="whatever" } reply_attributes= { 6=6 } } }
```
2. Une fois que ce profil fonctionne, remplacez « quoi que » avec le « SDI » suivant les indications de cet exemple :
```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2=sdi } reply_attributes= { 6=6 } } }
```

PPP et authentification PAP avec CSUnix et RAYON

Exécutez ces étapes au test d'authentification :

Remarque: L'authentification de PPP CHAP avec CSUnix et RAYON n'est pas prise en charge.

1. Réalisez un premier essai sans SDI. Si ce profil utilisateur ne fonctionne pas sans mot de passe de SDI pour l'authentification et le « async mode dedicated PPP/PAP, » cela ne fonctionnera pas avec un mot de passe de SDI :`# ./ViewProfile -p 9900 -u cse`

   ```
   user = cse {
   password = pap "pappass"
   radius=Cisco {
   check_items = {
   }
   reply_attributes= {
   6=2
   7=1
   }
   }
   }
   ```
2. Une fois les travaux ci-dessus de profil, ajoutent le **mot de passe = le SDI au** profil et ajoutent l'attribut **200=1** suivant les indications de cet exemple (ceci place Cisco_Token_Immediate à l'oui.) :`# ./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. Dans « **a avancé le GUI**, section Serveur, » **s'assurent que « la mise en cache symbolique d'enable** » est placée. Ceci peut être confirmé de l'interface de ligne de commande (CLI) avec :`$BASE/CLI/ViewProfile -p 9900 -u SERVER.#.#.#.#`
   `!--- Where #.#.#.# is the IP address of the CSUnix server.` `TokenCachingEnabled="yes"`

Connexion PPP commutée de réseau et PAP

On le suppose que les **tacacs si-nécessaires par défaut** et le **PPP d'aaa authentication ppp authen des** commandes **PAP** ont été exécutés sur le routeur. Écrivez ce nom d'utilisateur et mot de passe dans le terminal window avant que vous composiez. :

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

Remarque: Sur le PC, dans le réseau commuté, assurez-vous que « recevoir n'importe quelle authentification comprenant le texte clair » est vérifié.

Debug et conseils de vérification

Ces sections contiennent des conseils pour mettent au point et des conseils de vérification.

RAYON Cisco Secure, PPP, et PAP

C'est un exemple d'un bon mettent au point :

```
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)
```

ID sécurisé et CSUnix

Le débogage est enregistré dans le fichier spécifié dans /etc/syslog.conf pour local0.debug.

Aucun utilisateur ne peut authentifier - SDI ou autrement :

Après que vous ajoutiez l'ID sécurisé, assurez-vous qu'aucune erreur n'a été faite quand vous modifiez le fichier CSU.cfg. Réparez le fichier CSU.cfg ou retournez au fichier CSU.cfg de sauvegarde.

C'est un exemple d'un bon mettent au point :

```
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
```

C'est un exemple d'un mauvais mettent au point :

CSUnix trouve le profil utilisateur et l'envoie au serveur de SDI, mais le serveur de SDI échoue l'utilisateur parce que le code de passage est mauvais.

```
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;
```

C'est une exposition d'exemple que le serveur d'Ace est en panne :

Écrivez l'**arrêt de ./aceserver** sur le serveur de SDI. L'utilisateur ne reçoit pas le message « écrivent CODE DE PASSAGE ».

```
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
```

Informations connexes

- Cisco Secure ACS pour la page de support UNIX
- Notes de terrain pour le Cisco Secure ACS pour l'UNIX
- Support technique - Cisco Systems