Настройка Cisco Secure UNIX и Secure ID (клиент SDI)

Содержание

Введение

Для реализации конфигурации в этом документе вам нужна любая версия Cisco Secure, которая поддерживает Security Dynamics Incorporated (SDI) Безопасный ID.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Установка клиента SDI (безопасного идентификатора) на машинах Cisco Secure UNIX

Примечание: Безопасный ID обычно устанавливается, прежде чем Cisco Secure UNIX (CSUnix) был установлен. Эти инструкции описывают, как установить SDI - клиента после того, как был установлен CSUnix.

1. На сервере SDI выполните **sdadmin**. Скажите серверу SDI, что машина CSUnix является клиентом, и укажите, что рассматриваемые пользователи SDI активированы на клиенте CSUnix.
2. Используйте **nslookup** #.#.#.# или команда <hostname> **nslookup** для проверки, клиент CSUnix и сервер SDI могут сделать вперед и обратный просмотр друг друга.
3. Скопируйте/etc/sdace.txt файл сервера SDI клиенту CSUnix/etc/sdace.txt файл.
4. Скопируйте sdconf.rec файл сервера SDI клиенту CSUnix; этот файл может находиться где угодно на клиенте CSUnix. Однако, если это размещено в ту же структуру каталогов на клиенте CSUnix, как это было на сервере SDI, sdace.txt не должен модифицироваться.
5. Или/etc/sdace.txt или VAR_ACE должны указать к пути, где расположен sdconf.rec файл. Для проверки этого выполните кошку/etc/sdace.txt или проверьте выходные данные ENV, чтобы быть уверенными, что VAR_ACE определен в профиле root, поскольку запускается root.
6. Резервное копирование CSU.cfg клиента CSUnix, затем модифицируйте AUTHEN config_external_authen_symbols раздел с этими линиями:

```
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. Переработайте CSUnix выполнением **K80CiscoSecure** и **S80CiscoSecure**.
8. Если $BASE/utils/psg показывает, что процесс Процесса AAA-сервера Cisco Secure был активен, прежде чем файл CSU.cfg модифицировался, но не впоследствии, то ошибки

были сделаны в пересмотре файла CSU.cfg. Восстановите исходный файл CSU.cfg и попытайтесь делать изменения выделенными в шаге 6 снова.

Начальное тестирование безопасного ID и CSUnix

Для тестирования Безопасного ID и CSUnix выполните эти шаги:

1. Удостоверьтесь, что отличный от SDI пользователь может Telnet к маршрутизатору и аутентифицироваться с CSUnix. Если это не будет работать, то SDI не будет работать.
2. Протестируйте основную аутентификацию SDI в маршрутизаторе и выполните эту команду:
   `aaa new-model aaa authentication login default tacacs+ none` **Примечание:** Это предполагает, что **команды tacacs-server** уже активны в маршрутизаторе.
3. Добавьте пользователя SDI из командной строки CSUnix для ввода этой команды
   `$BASE/CLI/AddProfile -p 9900 -u` *`sdi_user`* **`-pw sdi`**
4. Попытайтесь аутентифицироваться как пользователь.. Если тот пользователь работает, SDI isoperational, и можно добавить дополнительные сведения к профилям пользователей.
5. Пользователи SDI могут быть протестированы с профилем unknown_user в CSUnix. (Пользователи не должны быть явно перечислены в CSUnix, если они все выданы к SDI, и у всех есть тот же профиль.), Если существует неизвестный профиль пользователя уже, существуют, удаляют его с помощью этой команды:
   `$BASE/CLI/DeleteProfile -p 9900 -u unknown_user`
6. Используйте эту команду для добавления другого неизвестного профиля пользователя:
   `$BASE/CLI/AddProfile -p 9900 -u unknown_user -pw sdi` Эта команда выдает всех неизвестных пользователей к SDI.

Безопасный ID и CSUnix: Профиль TACACS+

1. Выполните начальный тест без SDI. Если этот профиль пользователя не будет работать без пароля SDI для login authentication, Протокола аутентификации по квитированию вызова (CHAP) и Протокола аутентификации пароля (PAP), то это не будет работать с паролем 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. Как только профиль работает, добавьте "СОИ" к профилю вместо "ясного" как показано в данном примере:
```
# ./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 { } } }
```

Принципы работы профиля

Этот профиль позволяет пользователю входить с этими комбинациями:

- Telnet к маршрутизатору и SDI использования (Это предполагает, что **tacacs aaa authentication login default +** команда был выполнен на маршрутизаторе.)
- Удаленный доступ к сети по протоколу двухточечного соединения и протокол аутентификации пароля. (Это предполагает, что **система TACACS по умалчанию (при необходимости) aaa authentication ppp** и **команды ppp authen pap** были выполнены на маршрутизаторе).**Примечание:** На ПК, в Удаленном доступе к сети, удостоверяются, "Accept any authentication включая открытый текст", проверен. Перед набором номера введите одно из этих сочетаний имени пользователя и пароля в окне терминала:`username: cse*code+card`
`password: pap (must agree with profile)`

`username: cse`
`password: code+card`
- PPP - подключение удаленного доступа к сети и CHAP. (Это предполагает, что **система TACACS по умалчанию (при необходимости) aaa authentication ppp** и **команды ppp authen chap** были выполнены на маршрутизаторе).**Примечание:** На ПК, в Удаленном доступе к сети, или "Accept any authentication включая открытый текст" или, "Признают, что только должна быть проверена зашифрованная проверка подлинности". Перед набором номера введите это имя пользователя и пароль в окно терминала:`username: cse*code+card`
`password: chap (must agree with profile)`

TACACS CSUnix + Комбинации пароля, которые не Работают

Эти комбинации производят их debug errors CSUnix:

- CHAP и никакой пароль "открытого текста" в поле Password. Пользователь вводит `code+card` вместо пароля "открытого текста". RFC 1994 на CHAP требует хранилища незашифрованного пароля.
`username: cse password: code+card` `CiscoSecure INFO - User cse, No tokencard password received CiscoSecure NOTICE - Authentication - Incorrect password;`
- CHAP и плохой пароль CHAP.
`username: cse*code+card password: wrong chap password` (Пользователь исчезает к SDI, и SDI передает пользователя, но CSUnix отказывает пользователя, потому что пароль CHAP плох.)`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 и плохой пароль PAP.

username: cse*code+card password: wrong pap password (Пользователь исчезает к SDI, и SDI передает пользователя, но CSUnix отказывает пользователя, потому что пароль CHAP плох.)

```
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;
```

Отладка TACACS CSUnix + образцы профиля SDI

- Пользователь должен сделать CHAP и login authentication; сбои PAP.

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

- Пользователь должен сделать PAP и login authentication; сбои 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

Эти разделы содержат процедуры CSUnix RADIUS.

Login Authentication с CSUnix и RADIUS

Выполните эти шаги в тестовую аутентификацию:

1. Выполните начальный тест без SDI. Если этот профиль пользователя не будет работать без пароля SDI для login authentication, то он не будет работать с паролем

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

2. Как только этот профиль работает, замените "что" "СОИ" как показано в данном примере:
```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2=sdi } reply_attributes= { 6=6 } } }
```

PPP и аутентификация PAP с CSUnix и RADIUS

Выполните эти шаги в тестовую аутентификацию:

Примечание: Проверка подлинности CHAP PPP с CSUnix и RADIUS не поддерживается.

1. Выполните начальный тест без SDI. Если этот профиль пользователя не будет работать без пароля SDI для аутентификации PPP/PAP и "async mode dedicated", то это не будет работать с паролем SDI:
```
# ./ViewProfile -p 9900 -u cse

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

2. Как только вышеупомянутый профиль работает, добавьте **пароль = СОИ** к профилю и добавьте атрибут **200=1** как показано в данном примере (это устанавливает Cisco_Token_Immediate в да.):
```
# ./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. В "**Расширенном ГИПе** установлен раздел сервера", **удостоверяются "Enable Token Caching"**. Это может быть подтверждено от интерфейса командной строки (CLI)
```
C:$BASE/CLI/ViewProfile -p 9900 -u SERVER.#.#.#.#
!--- Where #.#.#.# is the IP address of the CSUnix server. TokenCachingEnabled="yes"
```

Удаленный доступ к сети по протоколу двухточечного соединения и протокол

аутентификации пароля

Предполагается, что **система TACACS по умалчанию (при необходимости) aaa authentication ppp** и **команды PPP authen PAP** были выполнены на маршрутизаторе. Введите это имя пользователя и пароль в окно терминала перед набором номера.:

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

Примечание: На ПК, в Удаленном доступе к сети, удостоверяются, "Accept any authentication включая открытый текст", проверен.

Советы по отладке и проверке

Эти разделы содержат советы для советов отладки и проверки.

Cisco Secure RADIUS, PPP и PAP

Это - пример хорошей отладки:

```
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)
```

Безопасный ID и CSUnix

Отладка сохранена в файле, заданном в/etc/syslog.conf для local0. .debug.

Никакие пользователи не могут аутентифицироваться - SDI или иначе:

После добавления Безопасного ID удостоверьтесь, что никакие ошибки не были сделаны при изменении файла CSU.cfg. Исправьте файл CSU.cfg или вернитесь к резервному файлу CSU.cfg.

Это - пример хорошей отладки:

```
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
```

Это - пример неудачной отладки:

CSUnix находит профиль пользователя и передает его к серверу SDI, но сервер SDI отказывает пользователя, потому что код доступа плох.

```
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;
```

Это - пример, показывают, что Первоклассный сервер не работает:

Введите./aceserver останавливаются на сервере SDI. Пользователь не добирается, "Вводят КОД ДОСТУПА" сообщение.

```
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
```

Дополнительные сведения

- Страница поддержки Cisco Secure ACS для UNIX
- Уведомления о дефектах для Cisco Secure ACS для UNIX
- Техническая поддержка - Cisco Systems