Cisco Secure UNIX 및 Secure ID(SDI 클라이언트) 구성

목차

소개

이 문서에서 구성을 구현하려면 SDI(Security Dynamics Incorporated)의 보안 ID를 지원하는 Cisco Secure 버전이 필요합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

Cisco Secure UNIX 시스템에 SDI 클라이언트(보안 ID) 설치

참고: 보안 ID는 일반적으로 Cisco CSUnix(Secure UNIX)를 설치하기 전에 설치됩니다.다음 지침은 CSUnix가 설치된 후 SDI 클라이언트를 설치하는 방법에 대해 설명합니다.

1. SDI 서버에서 sdadmin을 **실행합니다**.SDI 서버에 CSUnix 시스템이 클라이언트임을 알리고 해당 SDI 사용자가 CSUnix 클라이언트에서 활성화되도록 지정합니다.
2. nslookup #.#.#.# 또는 nslookup <hostname> 명령을 사용하여 CSUnix 클라이언트 및 SDI 서버가 서로 정방향 및 역방향 조회를 수행할 수 있는지 확인합니다.
3. SDI 서버의 /etc/sdace.txt 파일을 CSUnix 클라이언트 /etc/sdace.txt 파일에 복사합니다.
4. SDI 서버의 sdconf.rec 파일을 CSUnix 클라이언트에 복사합니다.이 파일은 CSUnix 클라이언트의 모든 위치에 있을 수 있습니다.그러나 CSUnix 클라이언트가 SDI 서버에 있는 것과 동일한 디렉토리 구조에 배치된 경우 sdace.txt를 수정할 필요가 없습니다.
5. /etc/sdace.txt 또는 VAR_ACE는 sdconf.rec 파일이 있는 경로를 가리켜야 합니다.이를 확인하려면 cat /etc/sdace.txt을 실행하거나 env의 출력을 확인하여 루트가 시작될 때 루트 프로필에 VAR_ACE가 정의되어 있는지 확인합니다.
6. CSUnix 클라이언트의 CSU.cfg를 백업한 다음 AUTHEN config_external_authen_symbols 섹션을 다음 행으로 수정합니다

```
.
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. K80CiscoSecure 및 **S80CiscoSecure**를 실행하여 CSUnix를 **재활용합니다**.
8. $BASE/utils/psg에서 CSU.cfg 파일을 수정하기 전에 Cisco Secure AAA Server 프로세스 프로세스가 활성 상태였지만 이후 수정되지 않은 경우 CSU.cfg 파일 수정 버전에서 오류가 발생했습니다.원래 CSU.cfg 파일을 복원한 후 6단계에서 변경된 내용을 다시 설명하십시오.

보안 ID 및 CSUnix의 초기 테스트

Secure ID 및 CSUnix를 테스트하려면 다음 단계를 수행합니다.

1. 비 SDI 사용자가 라우터에 텔넷하고 CSUnix로 인증할 수 있는지 확인합니다.그렇지 않으면

SDI가 작동하지 않습니다.

2. 라우터에서 기본 SDI 인증을 테스트하고 다음 명령을 실행합니다.

```
aaa new-model

aaa authentication login default tacacs+ none
```

참고: 이 경우 라우터에서 **tacacs-server** 명령이 이미 활성화되어 있는 것으로 가정합니다.

3. CSUnix 명령행에서 SDI 사용자를 추가하여 이 명령을 입력합니다.

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

4. 사용자로 인증해 보십시오..해당 사용자가 작동하는 경우 SDI가 작동하며 사용자 프로필에 추가 정보를 추가할 수 있습니다.
5. CSUnix에서 unknown_user 프로필로 SDI 사용자를 테스트할 수 있습니다.(사용자가 모두 SDI에 전달되고 모든 사용자가 동일한 프로필을 가진 경우 CSUnix에 명시적으로 나열할 필요가 없습니다.) 알 수 없는 사용자 프로필이 이미 있는 경우 이 명령의 도움말을 사용하여 이를 삭제합니다.

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

6. 이 명령을 사용하여 알 수 없는 다른 사용자 프로필을 추가합니다.

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

이 명령은 알려지지 않은 모든 사용자를 SDI로 전달합니다.

보안 ID 및 CSUnix:TACACS+ 프로필

1. SDI 없이 초기 테스트를 수행합니다.로그인 인증, CHAP(Challenge Handshake Authentication Protocol) 및 PAP(Password Authentication Protocol)를 위한 SDI 비밀번호 없이 이 사용자 프로파일이 작동하지 않을 경우 SDI 비밀번호와 함께 작동하지 않습니다.

```
# ./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. 프로파일이 작동하면 다음 예와 같이 "clear" 대신 프로파일에 "sdi"를 추가합니다.

```
# ./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 {
}
}

}
```

프로파일 작동 방식

이 프로파일을 사용하여 사용자가 다음 조합으로 로그인할 수 있습니다.

- 라우터에 텔넷하고 SDI를 사용합니다. 이 경우 **aaa authentication login default tacacs+** 명령이 라우터에서 실행되었다고 가정합니다.
- 전화 접속 네트워킹 PPP 연결 및 PAP(**aaa authentication ppp default if-needed tacacs** 및 **ppp authen pap** 명령이 라우터에서 실행되었다고 가정합니다.)**참고:** PC의 Dial-Up Networking(전화 접속 네트워킹)에서 "Accept any authentication with clear text(일반 텍스트를 포함한 모든 인증 수락)"가 선택되어 있는지 확인합니다.다이얼하기 전에 터미널 창에 다음 사용자 이름/비밀번호 조합 중 하나를 입력합니다.
```
username: cse*code+card
password: pap (must agree with profile)

username: cse
password: code+card
```
- 전화 접속 네트워킹 PPP 연결 및 CHAP. (**필요한 경우 aaa authentication ppp default if-needed tacacs** 및 **ppp** authen chap 명령이 라우터에서 실행된 것으로 가정합니다.)**참고:** PC의 Dial-Up Networking(전화 접속 네트워킹)에서 "Accept any authentication with clear text(일반 텍스트 포함 모든 인증 수락)" 또는 "Accept only encrypted authentication(암호화된 인증만 수락)"을 선택해야 합니다.다이얼하기 전에 터미널 창에 다음 사용자 이름과 암호를 입력합니다.
```
username: cse*code+card
password: chap (must agree with profile)
```

작동하지 않는 CSUnix TACACS+ 비밀번호 조합

이러한 조합은 다음과 같은 CSUnix 디버그 오류를 생성합니다.

- CHAP 및 비밀번호 필드에 "일반 텍스트" 비밀번호가 없습니다.사용자는 "cleartext" 비밀번호 대신 `code+card`를 입력합니다.CHAP의 RFC 1994에는 일반 텍스트 암호 스토리지가 필요합니다.

```
username: cse
password: code+card

CiscoSecure INFO - User cse, No tokencard password received
CiscoSecure NOTICE - Authentication - Incorrect password;
```
- CHAP 및 잘못된 CHAP 암호입니다.

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

(사용자가 SDI로 전송되고 SDI가 사용자를 통과하지만 CHAP 암호가 잘못되어 CSUnix가 사용

자에게 실패합니다.)

```
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 및 잘못된 PAP 암호입니다.

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

(사용자가 SDI로 전송되고 SDI가 사용자를 통과하지만 CHAP 암호가 잘못되어 CSUnix가 사용자에게 실패합니다.)

```
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;
```

CSUnix TACACS+ SDI 샘플 프로파일 디버깅

- 사용자는 CHAP 및 로그인 인증을 수행해야 합니다.PAP가 실패합니다.

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

- 사용자는 PAP 및 로그인 인증을 수행해야 합니다.CHAP에 장애가 발생했습니다.

```
# ./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

이 섹션에는 CSUnix RADIUS 절차가 포함되어 있습니다.

CSUnix 및 RADIUS로 로그인 인증

인증을 테스트하려면 다음 단계를 수행합니다.

1. SDI 없이 초기 테스트를 수행합니다.로그인 인증을 위한 SDI 비밀번호 없이 이 사용자 프로파일이 작동하지 않을 경우 SDI 비밀번호로 작동하지 않습니다.
```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2="whatever" } reply_attributes= { 6=6 } } }
```
2. 이 프로파일이 작동되면 다음 예에 표시된 대로 "anything"을 "sdi"로 바꿉니다.
```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2=sdi } reply_attributes= { 6=6 } } }
```

CSUnix 및 RADIUS를 사용한 PPP 및 PAP 인증

인증을 테스트하려면 다음 단계를 수행합니다.

참고: CSUnix 및 RADIUS를 사용한 PPP CHAP 인증은 지원되지 않습니다.

1. SDI 없이 초기 테스트를 수행합니다.이 사용자 프로파일이 PPP/PAP 인증을 위한 SDI 비밀번호 및 "async mode dedicated"가 없으면 SDI 비밀번호로 작동하지 않습니다.
```
# ./ViewProfile -p 9900 -u cse

user = cse {
password = pap "pappass"
radius=Cisco {
check_items = {
}
reply_attributes= {
6=2
7=1
}
}
}
```
2. 위 프로파일이 작동하면 **password = sdi**를 프로파일에 추가하고 이 예와 같이 특성 **200=1**을 추가합니다(Cisco_Token_Immediate를 yes로 설정).
```
# ./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. "**Advanced GUI**, server 섹션"에서 "**Enable Token Caching(토큰 캐싱 활성화)**"이 설정되어 있는지 확인합니다.CLI(Command Line Interface)에서 확인할 수 있는 기능은 다음과 같습니다.

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

전화 접속 네트워킹 PPP 연결 및 PAP

aaa authentication ppp default if-needed tacacs 및 **PPP autothen PAP** 명령이 라우터에서 실행된 것으로 가정합니다.전화를 걸기 전에 터미널 창에 이 사용자 이름과 암호를 입력합니다.

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

참고: PC의 Dial-Up Networking(전화 접속 네트워킹)에서 "Accept any authentication with clear text(일반 텍스트 포함 모든 인증 수락)"가 선택되어 있는지 확인합니다.

디버그 및 확인 팁

이 섹션에는 디버그 및 확인 팁에 대한 팁이 포함되어 있습니다.

Cisco Secure RADIUS, PPP 및 PAP

다음은 올바른 디버그의 예입니다.

```
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)
```

보안 ID 및 CSUnix

디버그는 local0.debug에 대해 /etc/syslog.conf에 지정된 파일에 저장됩니다.

어떤 사용자도 인증할 수 없음 - SDI 또는 기타:

보안 ID를 추가한 후 CSU.cfg 파일을 수정할 때 오류가 발생하지 않았는지 확인합니다.CSU.cfg 파일을 수정하거나 백업 CSU.cfg 파일로 되돌립니다.

다음은 올바른 디버그의 예입니다.

```
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
```

다음은 잘못된 디버그의 예입니다.

CSUnix는 사용자 프로필을 찾아 SDI 서버에 전송하지만, 패스코드가 잘못되어 SDI 서버가 사용자에게 실패합니다.

```
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;
```

다음은 Ace 서버가 다운되었음을 보여주는 예입니다.

SDI 서버에./aceserver stop을 입력합니다.사용자는 "Enter PASSCODE" 메시지를 받지 않습니다.

```
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
```

관련 정보

- UNIX용 Cisco Secure ACS 지원 페이지
- UNIX용 Cisco Secure ACS에 대한 필드 알림
- Technical Support - Cisco Systems