TokenCaching 설계 및 구현 가이드

목차

소개

이 문서의 범위는 TokenCaching의 설정 및 문제 해결에 대해 설명합니다. ISDN 터미널 어댑터(TA) 사용자의 PPP(Point-to-Point Protocol) 세션은 일반적으로 사용자 PC에서 종료됩니다. 이를 통해 사용자는 비동기(모뎀) 전화 접속 연결과 동일한 방식으로 PPP 세션을 제어할 수 있습니다. 즉, 필요에 따라 세션을 연결하고 연결을 끊습니다. 이렇게 하면 사용자가 PAP(Password Authentication Protocol)를 사용하여 전송을 위한 OTP(일회용 비밀번호)를 입력할 수 있습니다.

그러나, 제 2 B 채널이 자동으로 올라오도록 설계된 경우, 사용자는 제 2 B 채널에 대한 새로운 OTP를 요구해야 한다. PC PPP 소프트웨어는 두 번째 OTP를 수집하지 않습니다. 대신 소프트웨어는 기본 B 채널에 사용된 것과 동일한 비밀번호를 사용하려고 시도합니다. 토큰 카드 서버는 OTP 재사용을 거부합니다. UNIX용 CiscoSecure ACS(버전 2.2 이상) 및 Windows용 CiscoSecure ACS(2.1 이상)는 두 번째 B 채널에서 동일한 OTP 사용을 지원하기 위해 TokenCaching을 수행합니다. 이 옵션을 사용하려면 AAA(authentication, authorization, and accounting) 서버에서 토큰 사용자 연결에 대한 상태 정보를 유지 관리해야 합니다.

자세한 내용은 ISDN에서 일회용 비밀번호 지원을 참조하십시오.

사전 요구 사항

요구 사항

이 문서에서는 사용자가 이미 올바르게 구성되었다고 가정합니다.

- 정상적으로 작동하는 전화 접속 모뎀입니다.
- CiscoSecure ACS UNIX 또는 ACS Windows를 가리키는 AAA와 함께 NAS(Network Access Server)가 올바르게 구성되었습니다.
- ACE/SDI는 이미 CiscoSecure ACS UNIX 또는 ACS Windows로 설정되어 있으며 제대로 작동합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CiscoSecure ACS Unix 2.2 이상
- CiscoSecure ACS Windows 2.1 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

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

구성

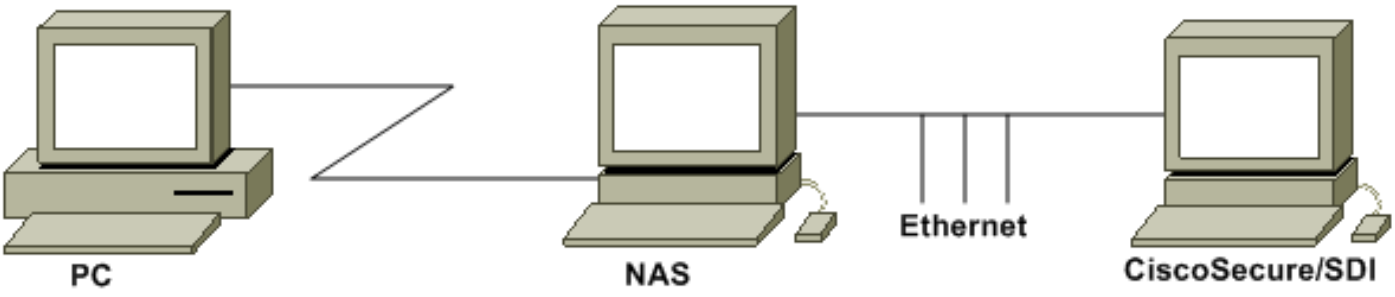
이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 명령 조회 도구(등록된 고객만 해당)를 사용하십시오.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.

PC는 NAS 및 ISDN 모뎀으로 다이얼하며 ppp multilink 명령에 대해 구성됩니다.



설정

이 문서에서는 다음 설정을 사용합니다.

사용자 이름 및 비밀번호 입력 구성

이 문서에서 NAS는 SDI 일회용 비밀번호와 함께 PPP 세션에 CHAP(Challenge Handshake Authentication Protocol)를 사용합니다. CHAP를 사용하는 경우 다음 형식으로 암호를 입력하십시오.

- username - fadi*pin+code(사용자 이름에 *가 있음)
- password - chappassword

예를 들면 사용자 이름 = fadi, chap 비밀번호 = cisco, pin = 1234이며, 토큰에 표시되는 코드는 987654입니다. 따라서 사용자는 다음을 입력합니다.

- username—fadi*1234987654
- password - cisco

참고: CiscoSecure 및 NAS가 PAP에 대해 구성된 경우 사용자 이름 및 토큰을 다음과 같이 입력할 수 있습니다.

- username—username*pin+code
- 암호—

또는:

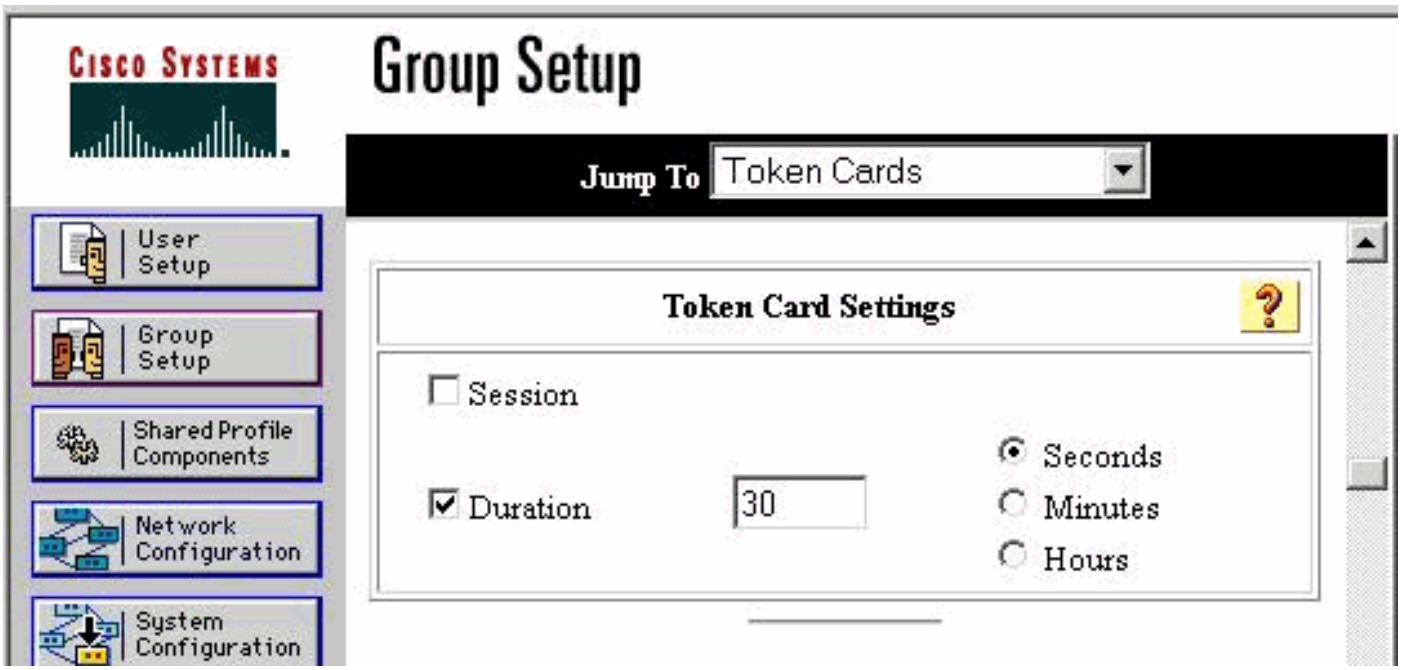
- username—사용자 이름
- password - pin+code

CiscoSecure ACS Windows에서 TokenCaching 구성

CiscoSecure ACS Windows 사용자 또는 그룹은 TACACS+를 사용하는 경우 PPP IP 및 PPP LCP를 확인하여 정상적으로 설정됩니다. RADIUS를 사용하는 경우 다음을 구성해야 합니다.

- 속성 6 = Service_Type = 프레임
- 속성 7 = Framed_Protocol = PPP

또한 다음 예제와 같이 그룹에 대해 TokenCaching 매개변수를 확인할 수 있습니다.



CiscoSecure ACS UNIX에서 토큰 캐싱 구성

TokenCaching 특성에는 네 가지가 있습니다. config_token_cache_absolute_timeout(초) 특성은 $install_directory/config/CSU.cfg 파일에 설정됩니다. 다른 세 가지 특성(set server token-caching, set server token-caching-expire-method, set server token-caching-timeout)은 사용자 또는 그룹 프로필에 설정됩니다. 이 문서의 경우 전역 특성 config_token_cache_absolute_timeout은 $install_directory/config/CSU.cfg 파일에서 이 값으로 설정됩니다.

```
NUMBER config_token_cache_absolute_timeout = 300;
```

사용자 및 그룹 서버 TokenCaching 특성 프로필은 다음 예와 같이 구성됩니다.

<#root>

```
Group Profile:

Group Profile Information
group = sdi{
profile_id = 42
profile_cycle = 5
default service=permit
set server token-caching=enable
set server token-caching-expire-method=timeout
set server token-caching-timeout=30
set server max-failed-login-count=1000

}

User Profile:

user = fadi{
profile_id = 20
```

```
set server current-failed-logins = 0
profile_cycle = 168
member = sdi
profile_status = enabled
password = chap "********"
password = sdi
password = pap "********"
password = clear "********"
default service=permit
set server max-failed-login-count=1000

!--- The TACACS+ section of the profile.

service=ppp {
default protocol=permit
protocol=ip {
set addr=1.1.1.1
}
protocol=lcp {
}

!--- This allows the user to use the

ppp multilink

 command.

protocol=multilink {
}
}
service=shell {
default attribute=permit
}

!--- The RADIUS section of the profile.

radius=Cisco12.05 {
check_items= {
200=0
}
}

}
```

다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

CiscoSecure ACS UNIX에서 토큰 캐싱 디버그

이 CiscoSecure UNIX 로그는 2개의 BRI 채널에서 인증이 발생할 때 TokenCaching을 통한 성공적

인 인증을 보여줍니다.

```
Jun 14 13:44:29 cholera CiscoSecure: DEBUG - AUTHENTICATION START request
          (e7079cae)

!--- Detects the * in the username.

Jun 14 13:44:29 cholera CiscoSecure: INFO - The character * was found
          in username: username=fadi,passcode=3435598216

!--- Initializes ACE modules in CiscoSecure.

Jun 14 13:44:29 cholera CiscoSecure: DEBUG - sdi_challenge response timeout 5
Jun 14 13:44:29 cholera CiscoSecure: DEBUG - AceInit()
Jun 14 13:44:29 cholera CiscoSecure: DEBUG - AceInit(17477), ace rc=150,
          ed=1039800
Jun 14 13:44:29 cholera CiscoSecure: DEBUG -   acsWaitForSingleObject
          (17477) begin
Jun 14 13:44:29 cholera CiscoSecure: DEBUG -   aceCB(17477)
Jun 14 13:44:29 cholera CiscoSecure: DEBUG -   aceCB(17477) AceGetUserData,
           ace rc=1, ed=1039800
Jun 14 13:44:29 cholera CiscoSecure: DEBUG -   aceCB(17477):
           AceGetAuthenticationStatus, ace rc=1, acm rc=0
Jun 14 13:44:29 cholera CiscoSecure: DEBUG -   aceCB(17477): return
Jun 14 13:44:29 cholera CiscoSecure: DEBUG -   acsWaitForSingleObject(0) (17477)
Jun 14 13:44:29 cholera CiscoSecure: DEBUG -   acsWaitForSingleObject
           (17477) end, rc=0
Jun 14 13:44:29 cholera CiscoSecure: DEBUG - AceInit(17477), continue, acm rc=0
Jun 14 13:44:29 cholera CiscoSecure: DEBUG - AceSetUsername(17477),
           username=fadi
Jun 14 13:44:29 cholera CiscoSecure: DEBUG - AceSetUsername(17477), ace rc=1
Jun 14 13:44:29 cholera CiscoSecure: INFO - sdi_challenge(17477): rtn 1,
           state=GET_PASSCODE, user=fadi
Jun 14 13:44:29 cholera CiscoSecure: DEBUG - Token Caching. timeout_value is: 30
Jun 14 13:44:29 cholera CiscoSecure: DEBUG - Token Caching.
           timeout enabled value: 30
Jun 14 13:44:29 cholera CiscoSecure: DEBUG - profile_valid_tcaching TRUE ending.
Jun 14 13:44:29 cholera CiscoSecure: DEBUG - Token Caching.  MISS.
Jun 14 13:44:29 cholera CiscoSecure: DEBUG - AceSetPasscode(17477),
           passcode=3435598216
Jun 14 13:44:29 cholera CiscoSecure: DEBUG - AceSetPasscode(17477), ace rc=1

!--- Checks credentials with ACE server.

Jun 14 13:44:29 cholera CiscoSecure: DEBUG - AceCheck(17477)
Jun 14 13:44:29 cholera CiscoSecure: DEBUG - AceCheck(17477), ace rc=150
Jun 14 13:44:29 cholera CiscoSecure: DEBUG -   acsWaitForSingleObject
          (17477) begin
Jun 14 13:44:31 cholera CiscoSecure: DEBUG -   aceCB(17477)
Jun 14 13:44:31 cholera CiscoSecure: DEBUG -   aceCB(17477) AceGetUserData,
           ace rc=1, ed=1039800
Jun 14 13:44:31 cholera CiscoSecure: DEBUG -   aceCB(17477):
           AceGetAuthenticationStatus, ace rc=1, acm rc=0
Jun 14 13:44:31 cholera CiscoSecure: DEBUG -   aceCB(17477): return
Jun 14 13:44:31 cholera CiscoSecure: DEBUG -   acsWaitForSingleObject(0) (17477)
Jun 14 13:44:31 cholera CiscoSecure: DEBUG -   acsWaitForSingleObject (17477) end,
           rc=0
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - AceCheck(17477), continue, acm rc=0
Jun 14 13:44:31 cholera CiscoSecure: INFO - sdi_verify(17477):
           fadi authenticated by ACE Srvr
```

```
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - AceClose(17477)
Jun 14 13:44:31 cholera CiscoSecure: INFO - sdi(17477):
          fadi free external_data memory, state=GET_PASSCODE

!--- The TokenCaching timeout is set to 30 seconds.

Jun 14 13:44:31 cholera CiscoSecure: DEBUG - Token Caching. timeout_value is: 30
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - Token Caching.
          timeout enabled value: 30
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - profile_valid_tcaching TRUE ending.

!--- The TokenCaching takes place.

Jun 14 13:44:31 cholera CiscoSecure: DEBUG - cache_insert
          (key<4>, val<10><3435598216>, port_type<3>)

Jun 14 13:44:31 cholera CiscoSecure: DEBUG - Cisco Cached Tokens : 1
Jun 14 13:44:31 cholera CiscoSecure: INFO - sdi_verify(17477): rtn 1
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - Authentication - LOGIN successful;
          [NAS=lynch.cisco.com, Port=BRI0:1, User=fadi, Priv=1]

!--- The authentication of the second BRI channel begins.

Jun 14 13:44:31 cholera CiscoSecure: DEBUG - AUTHENTICATION START request (76f91a6c)
Jun 14 13:44:31 cholera CiscoSecure: INFO - The character * was found in username:
          username=fadi,passcode=3435598216
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - sdi_challenge response timeout 5
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - AceInit()
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - AceInit(29111), ace rc=150, ed=1039984
Jun 14 13:44:31 cholera CiscoSecure: DEBUG -   acsWaitForSingleObject (29111) begin
Jun 14 13:44:31 cholera CiscoSecure: DEBUG -   aceCB(29111)
Jun 14 13:44:31 cholera CiscoSecure: DEBUG -   aceCB(29111) AceGetUserData, ace rc=1,
          ed=1039984
Jun 14 13:44:31 cholera CiscoSecure: DEBUG -   aceCB(29111): AceGetAuthenticationStatus,
          ace rc=1, acm rc=0
Jun 14 13:44:31 cholera CiscoSecure: DEBUG -   aceCB(29111): return
Jun 14 13:44:31 cholera CiscoSecure: DEBUG -   acsWaitForSingleObject(0) (29111)
Jun 14 13:44:31 cholera CiscoSecure: DEBUG -   acsWaitForSingleObject (29111) end, rc=0
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - AceInit(29111), continue, acm rc=0
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - AceSetUsername(29111), username=fadi
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - AceSetUsername(29111), ace rc=1
Jun 14 13:44:31 cholera CiscoSecure: INFO - sdi_challenge(29111): rtn 1,
          state=GET_PASSCODE, user=fadi
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - Token Caching. timeout_value is: 30
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - Token Caching. timeout enabled value: 30
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - profile_valid_tcaching TRUE ending.

!--- Checks with the cached token for the user "fadi".

Jun 14 13:44:31 cholera CiscoSecure: DEBUG - Token Caching. USER       : fadi
Jun 14 13:44:31 cholera CiscoSecure: DEBUG -                PASSWORD   : 3435598216 len: 10
Jun 14 13:44:31 cholera CiscoSecure: DEBUG -                hashval_str: 3435598216 len: 10
Jun 14 13:44:31 cholera CiscoSecure: DEBUG -                port_type  : BRI len: 3
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - Token Caching. HIT.
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - AceClose(29111)
Jun 14 13:44:31 cholera CiscoSecure: INFO - sdi(29111): fadi free external_data memory,
          state=GET_PASSCODE
Jun 14 13:44:31 cholera CiscoSecure: INFO - sdi_verify(29111): rtn 1
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - Authentication - LOGIN successful;
          [NAS=lynch.cisco.com, Port=BRI0:2, User=fadi, Priv=1]

!--- After 30 seconds the cached token expires.
```

```
Jun 14 13:45:03 cholera CiscoSecure: DEBUG - Expiring Cisco Token Cache Entry
Jun 14 13:45:03 cholera CiscoSecure: DEBUG - Cisco Cached Tokens : 0
```

관련 정보

- Cisco 보안 자문, 응답 및 공지
- CiscoSecure UNIX 제품 지원 페이지
- Windows용 CiscoSecure ACS 제품 지원 페이지
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.