令牌缓存设计和实施指南

目录

简介

范围本文是讨论设置和排除故障令牌缓存。ISDN终端适配器(TA)用户的点对点协议(PPP)会话典型地终止在用户PC。这允许用户控制PPP会话与异步(调制解调器)拨号连接同样，含义联络并且断开会话当必要时。这允许用户使用密码认证协议为了进入传输的一次性密码(OTP)。

然而，如果第二条B信道设计自动地出现，必须提示用户输入第二条B信道的一新的OTP。PC PPP软件不收集第二OTP。反而，软件设法使用用于主要的B信道的同一个密码。令牌卡服务器故意地拒绝OTP的重新使用。CiscoSecure ACS for UNIX (版本2.2和以后版本)和CiscoSecure ACS Windows版(2.1及以后)执行令牌缓存为了支持使用在第二条B信道的同样OTP。此选项要求验证、授权和统计(AAA)服务器维护关于令牌用户的连接的状态信息。

参考的支持的ISDN上的一次性密码欲知更多信息。

先决条件

要求

本文假设，您已经安排这些正确地配置：

- 适当地运作的拨号调制解调器。
- 指向CiscoSecure ACS UNIX或ACS Windows的网络接入服务器(NAS)适当地配置，与AAA。
- ACE/SDI已经设置CiscoSecure ACS UNIX或ACS Windows，并且适当地工作。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CiscoSecure ACS UNIX 2.2或以上
- CiscoSecure ACS Windows 2.1或以上版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

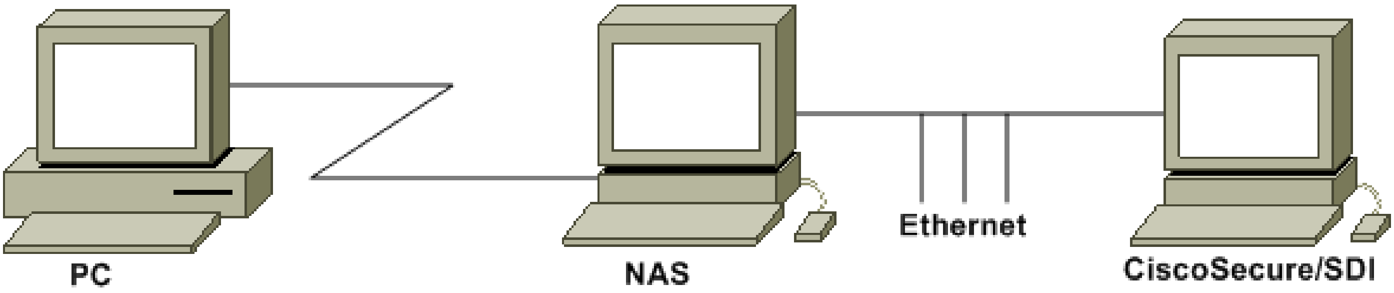
本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

PC拨号到NAS和ISDN调制解调器和为**ppp multilink命令**配置。



配置

本文档使用以下配置：

- 配置用户名和密码输入
- 配置在CiscoSecure ACS Windows的令牌缓存
- 配置在CiscoSecure ACS UNIX的令牌缓存

配置用户名和密码输入

在本文中， NAS使用质询握手验证协议(CHAP) PPP会话与SDI一次性密码一起。如果使用CHAP，请输入密码以此形式：

- **用户名**— fadi*pin+code (请注释*在用户名)
- **密码**— chappassword

此的示例是：username= fadi、chap密码= cisco，管脚= 1234和在标记显示的代码是987654。所以，用户输入此：

- **用户名**— fadi*1234987654
- **密码**— cisco

注意： 如果CiscoSecure和NAS为PAP配置，用户名和标记可以被输入作为此：

- **用户名**— username*pin+code
- **密码**—

或者：

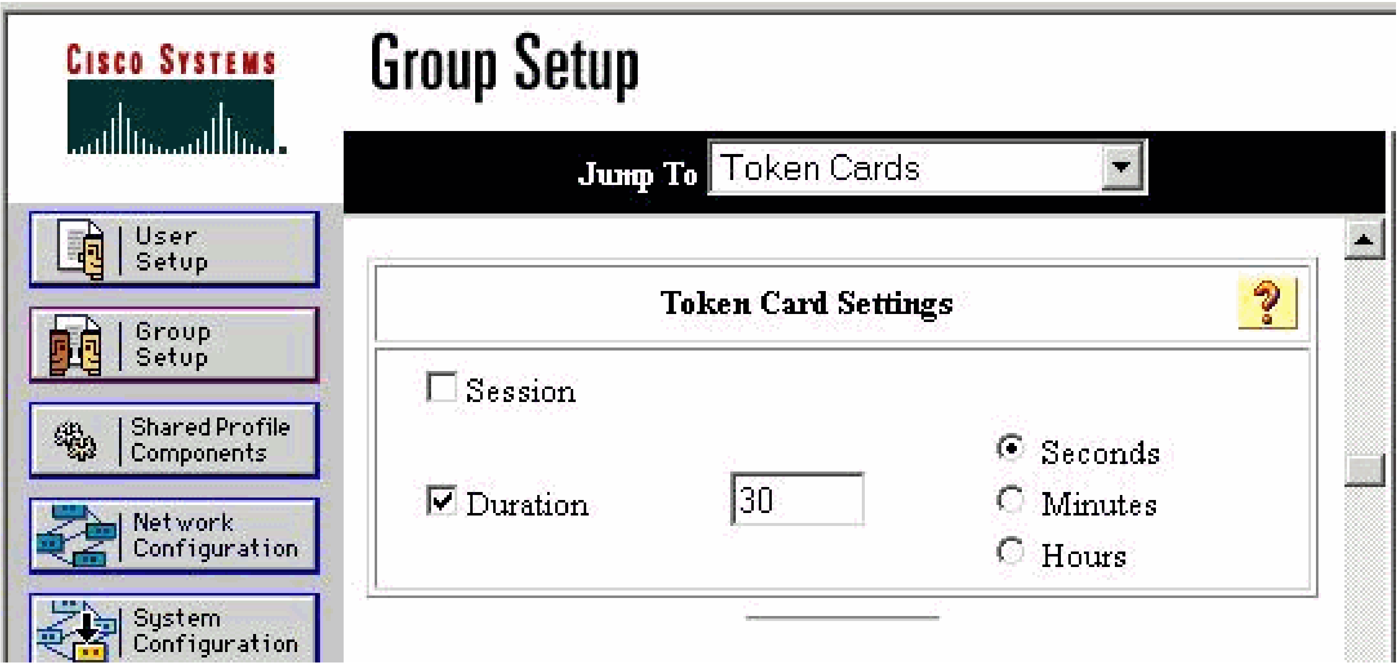
- **用户名用户名**
- **密码**— pin+code

配置在CiscoSecure ACS Windows的令牌缓存

CiscoSecure ACS Windows用户或组照常设置，被检查的PPP IP和PPP LCP是否使用TACACS+。如果使用RADIUS，必须配置这些：

- 属性6 = **Service_Type =Framed**
- 属性7 = **Framed_Protocol = PPP**

另外，如此示例所显示，令牌缓存参数可以被检查组：



Jump To Token Cards

Token Card Settings

□ Session

☑ Duration 30 ● Seconds ○ Minutes ○ Hours

配置在CiscoSecure ACS UNIX的令牌缓存

有四个令牌缓存属性。config_token_cache_absolute_timeout (以秒钟)属性在$install_directory/config/CSU.cfg文件设置。其他三个属性(set server token-caching、set server token-caching-expire-method和set server token-caching-timeout)在用户或组配置文件设置。对于本文， global attribute config_token_cache_absolute_timeout设置对此在$install_directory/config/CSU.cfg文件：

```
NUMBER config_token_cache_absolute_timeout = 300;
```

如此示例所显示，用户和组服务器令牌缓存属性配置文件配置：

```
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 } } }
```

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

在CiscoSecure ACS UNIX的调试令牌缓存

当验证在两个BRI信道时，出现此CiscoSecure UNIX日志显示与令牌缓存的一成功认证：

```
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 13:44:31 cholera CiscoSecure: DEBUG - Expiring Cisco Token Cache
Entry Jun 14 13:45:03 cholera CiscoSecure: DEBUG - Cisco Cached Tokens : 0
```

相关信息

- Cisco安全建议、答复和通知
- CiscoSecure UNIX产品支持页
- CiscoSecure ACS Windows版产品支持页

- 技术支持和文档 - Cisco Systems