Руководство по разработке и реализации TokenCaching

Содержание

Введение

Область этого документа должна обсудить настройку и устранение неполадок TokenCaching. Сеансы Протокола PPP для адаптера терминала ISDN (TA) пользователи, как правило, завершаются в пользовательском ПК. Это позволяет пользователю управлять сеансом PPP таким же образом как асинксом (модем) подключение удаленного доступа, что означает подключение, и разъедините сеанс по мере необходимости. Это разрешает пользователю использовать Протокол аутентификации пароля (PAP) для ввода одноразового пароля (OTP) для транспорта.

Однако, если второй канал B разработан для подъема автоматически, пользователю нужно предложить для нового OTP для второго канала B. Программное обеспечение для PPP ПК не собирает второй OTP. Вместо этого программное обеспечение пытается использовать тот же пароль, используемый для основного канала B. Сервер Token Card запрещает повторное использование OTP дизайном. CiscoSecure ACS для UNIX (версия 2.2 и позднее) и CiscoSecure ACS для Windows (2.1 и позже) выполняют TokenCaching для поддержки использования того же OTP на втором канале B. Эта опция требует, чтобы аутентификация, авторизация и учет (AAA) поддержала информацию о состоянии о соединении пользователя с маркерным доступом.

См. Поддержку Разовых паролей для ISDN для получения дополнительной информации.

Предварительные условия

Требования

Этот документ предполагает, что вам уже настроили их правильно:

- Модем коммутируемой линии передачи, который работает должным образом.
- Сервер доступа к сети (NAS) настроил должным образом с AAA, который указывает к CiscoSecure ACS UNIX или Окнам ACS.
- ACE/SDI уже является настройкой с CiscoSecure ACS UNIX или Окнами ACS, и работает должным образом.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- CiscoSecure ACS UNIX 2.2 или позже
- Windows 2.1 CiscoSecure ACS или позже

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Настройка

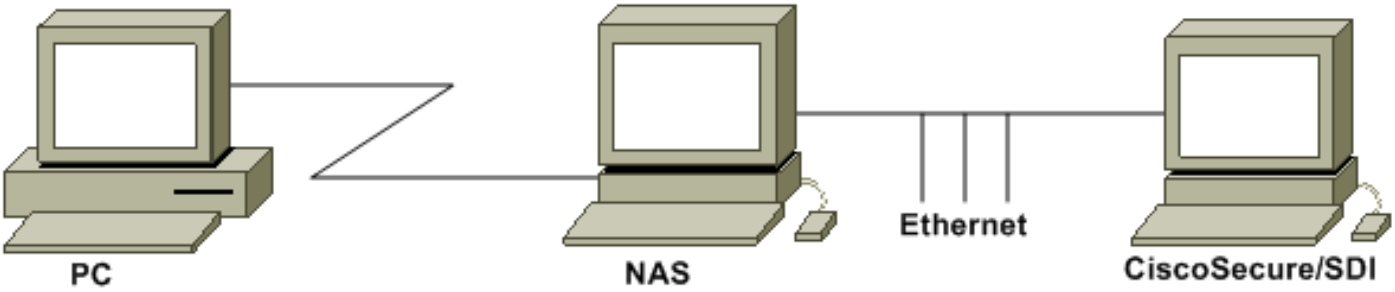
В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:

ПК набирает в NAS и Модем ISDN, и настроен для **команды ppp multilink**.



Конфигурации

Эти конфигурации используются в данном документе:

- Настройте ввод имени пользователя и пароля
- Настройте TokenCaching на Windows CiscoSecure ACS
- Настройте TokenCaching в CiscoSecure ACS UNIX

Настройте ввод имени пользователя и пароля

В этом документе NAS использует Протокол аутентификации по квитированию вызова (CHAP) для сеанса PPP наряду с разовым паролем SDI. При использовании CHAP, вводите пароль в этой форме:

- **имя пользователя** — fadi*pin+code (обращают внимание * в имени пользователя),
- **пароль** — chappassword

Пример этого: имя пользователя = fadi, пароль парня = Cisco, прикрепляет = 1234, и код, который показывает на маркере, 987654. Поэтому пользователь вводит это:

- **имя пользователя** — fadi*1234987654
- **password cisco**

Примечание: Если CiscoSecure и NAS были настроены для PAP, имя пользователя и маркер могут быть введены как это:

- **имя пользователя** — username*pin+code
- **password**

Или:

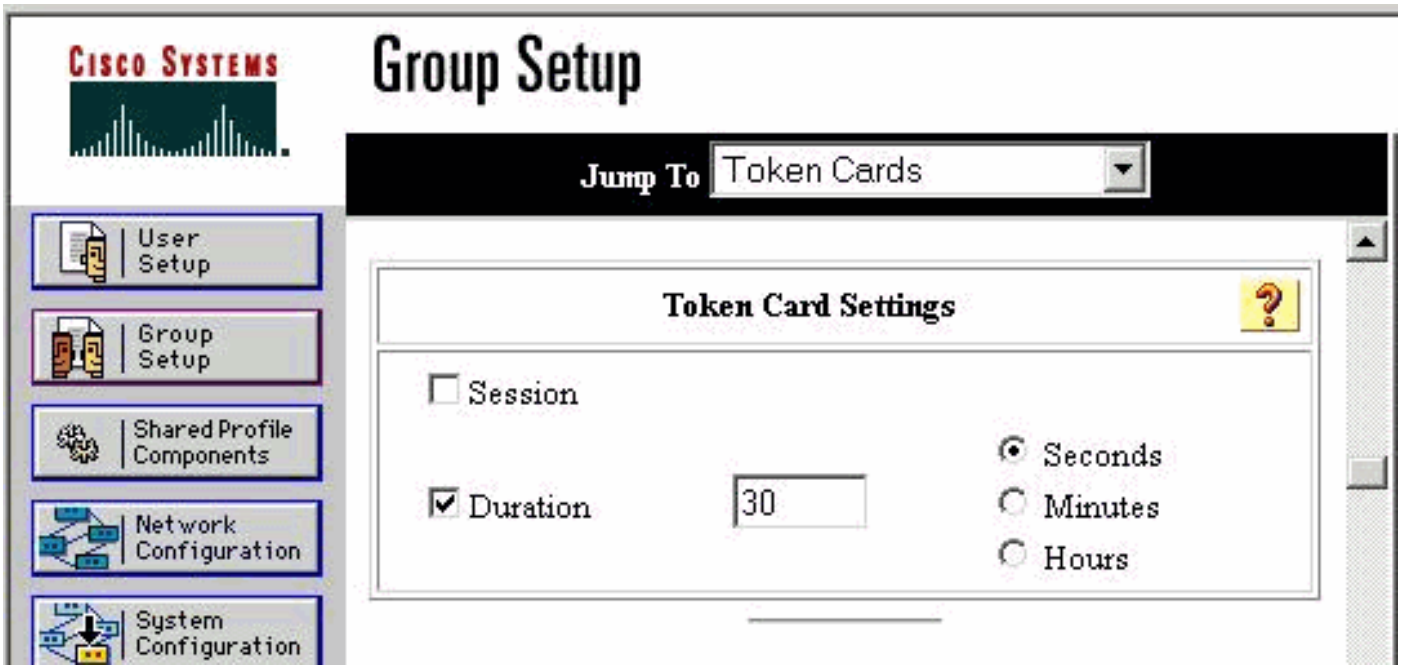
- **имя пользователя** — имя пользователя
- **пароль** — pin+code

Настройте TokenCaching на Windows CiscoSecure ACS

Пользователь Windows CiscoSecure ACS или группа установлены, как обычно, с IP PPP, и LCP PPP проверил, используете ли вы TACACS +. При использовании RADIUS они должны быть настроены:

- Припишите 6 = **Service_Type = обрамленный**
- Припишите 7 = **Framed_Protocol = PPP**

Кроме того, параметры TokenCaching могут быть проверены для группы как показано в данном примере:



Настройте TokenCaching в CiscoSecure ACS UNIX

Существует четыре атрибута TokenCaching. config_token_cache_absolute_timeout (в секундах) атрибут установлен в файле $install_directory/config/CSU.cfg. Другие три атрибута (кэширование маркера сервера набора, сервер набора token-caching-expire-method, и таймаут кэширования маркера сервера набора) установлены в пользователе или профилях группы. Для этого документа global attribute config_token_cache_absolute_timeout установлен в это в файле $install_directory/config/CSU.cfg:

```
NUMBER config_token_cache_absolute_timeout = 300;
```

Пользователь и профили атрибута TokenCaching сервера группы настроены как показано в данном примере:

```
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 } } }
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

TokenCaching отладки на CiscoSecure ACS UNIX

Когда аутентификация происходит на двух каналах BRI, этот журнал CiscoSecure UNIX показывает успешную аутентификацию с TokenCaching:

```
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
```

Дополнительные сведения

- Информационные сообщения Cisco Security, ответы и предупреждения
- Страница поддержки продукта Cisco Secure UNIX
- Страница поддержки продукта CiscoSecure ACS для Windows
- Cisco Systems – техническая поддержка и документация