TokenCaching の設計および実装ガイド

目次

概要

このドキュメントでは、TokenCaching のセットアップとトラブルシューティングについて説明します。 ISDN ターミナル アダプタ（TA）ユーザのポイントツーポイント プロトコル（PPP）セッションは、通常ユーザの PC で終了します。 このため、ユーザは非同期（モデム）のダイヤルアップ接続の場合と同じ方法で PPP のセッションを制御できます。つまり、必要に応じて、セッションの接続および接続解除ができます。 このため、ユーザはパスワード認証プロトコル（PAP）を使用して、転送用のワンタイム パスワード（OTP）を入力することができます。

ただし、第 2 Bチャネルが自動的にアップするように設計されていればユーザは第 2 Bチャネルの新しい OTP のためにプロンプト表示する必要があります。 PC PPP ソフトウェアは第 2 OTP を集めません。 その代り、ソフトウェアはプライマリ Bチャネルに使用する同じパスワードを使用するために試みます。 トークンカードサーバは OTP の再使用を意図的に否定します。 CiscoSecure ACS（バージョン 2.2 および それ以降） for UNIX および CiscoSecure ACS for Windows（2.1 およびそれ以降）は第 2 Bチャネルの同じ OTP の使用をサポートするために TokenCaching を行います。 このオプションは認証、許可、アカウンティング（AAA）サーバがトークンユーザの接続についてのステート情報を維持するように要求します。

詳細については[サポート ISDN の ワンタイム パスワードを]参照して下さい。

前提条件

要件

この資料は既にこれらを正しく設定してもらっていると仮定します:

- きちんと動作するダイヤルアップモデム。
- CiscoSecure ACS UNIX か ACS Windows を指す AAA で、正しく設定される VPDN ダイヤルインのネットワーク アクセス サーバ（NAS）（NAS）。
- ACE/SDI は CiscoSecure ACS UNIX か ACS Windows によって既に設定され、きちんとはたらきます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- CiscoSecure ACS UNIX 2.2 またはそれ以降
- CiscoSecure ACS Windows 2.1 またはそれ以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

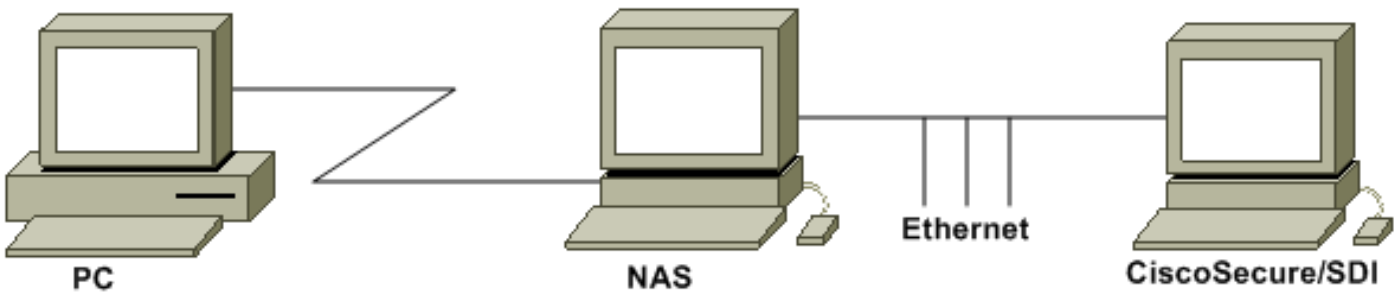
この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

PC は NAS および ISDN モデムにダイアルインし、**ppp multilink コマンド**のために設定されます。



設定

このドキュメントでは、次の設定を使用します。

- 設定 ユーザ名 および パスワード 入力
- CiscoSecure ACS Windows の設定 TokenCaching
- CiscoSecure ACS UNIX の設定 TokenCaching

設定 ユーザ名 および パスワード 入力

この資料では、NAS は SDI ワンタイムパスワードと共に PPP セッションのために Challenge Handshake Authentication Protocol（CHAP）を使用します。 CHAP を使用する場合、この形式でパスワードを入力して下さい:

- **username** — fadi*pin+code（*ユーザ名の…注意して下さい）
- **password** — chappassword

これの例は次のとおりです: ユーザ名 = fadi、chap パスワード = cisco は、ピン = 1234、およびトークンで示すコード 987654 です。 従って、ユーザはこれを入力します:

- **username** — fadi*1234987654
- **password** — cisco

注: CiscoSecure および NAS が PAP のために設定された場合、ユーザ名およびトークンはこれとして入力することができます:

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

または

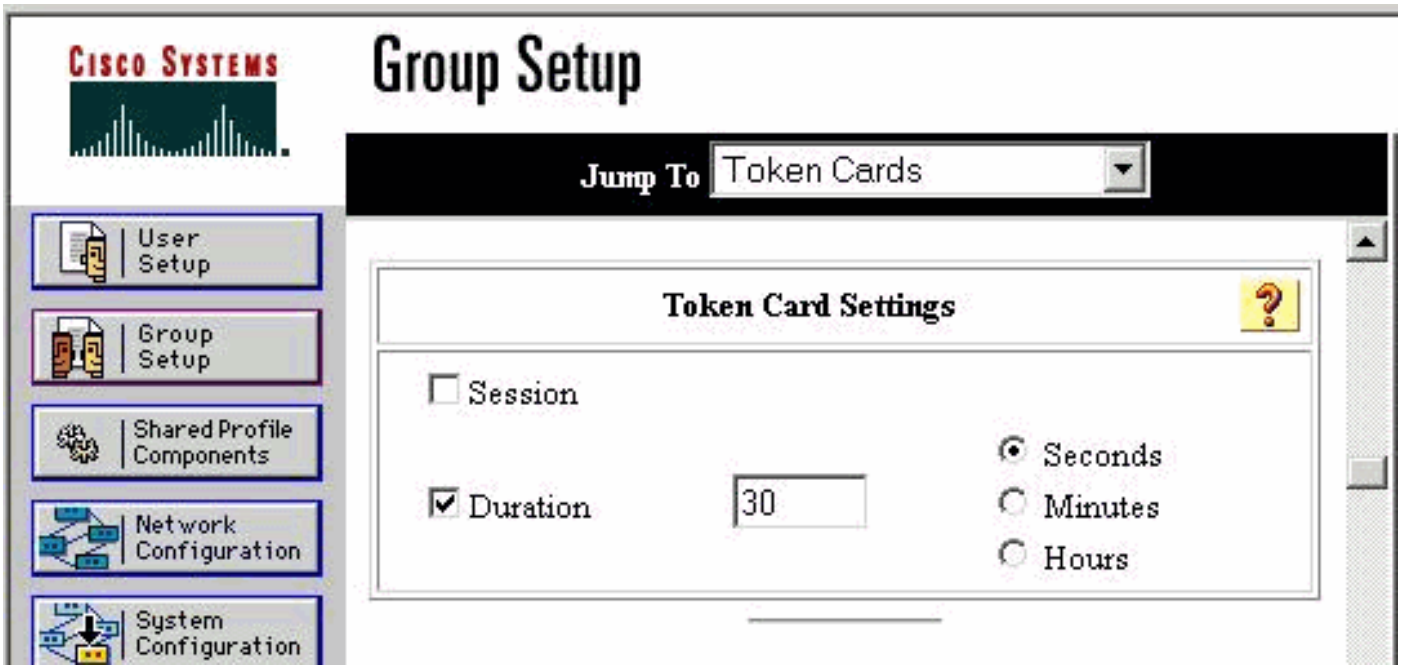
- **username username**
- **password** — pin+code

CiscoSecure ACS Windows の設定 TokenCaching

TACACS+ を使用する場合 CiscoSecure ACS Windows ユーザかグループはチェックされて PPP IP および PPP LCP が、いつも通り設定されます。 RADIUS を使用する場合、これらは設定する必要があります:

- アトリビュート 6 = **Service_Type = フレーム化される**
- アトリビュート 7 = **Framed_Protocol = PPP**

さらに、TokenCaching パラメータはこの例に示すようにグループがあるように確認することができます:



CiscoSecure ACS UNIX の設定 TokenCaching

TokenCaching 4 つの属性があります。 config_token_cache_absolute_timeout （秒で）アトリビュートは $install_directory/config/CSU.cfg ファイルで設定 されます。 他の 3 つの属性（set server token-caching、set server token-caching-expire-method および set server token-caching-timeout）はユーザかグループ プロファイルで設定 されます。 この資料に関しては、global attribute config_token_cache_absolute_timeout は $install_directory/config/CSU.cfg ファイルでこれに設定 されます:

```
NUMBER config_token_cache_absolute_timeout = 300;
```

ユーザおよびグループ サーバ TokenCaching アトリビュート プロファイルはこの例に示すように設定されます:

```
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 } } }
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

CiscoSecure ACS UNIX のデバッグ TokenCaching

この CiscoSecure UNIX ログは認証が 2 つの BRI チャネルで行われるとき、TokenCaching の認証の成功を示します:

```
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
```

関連情報

- Cisco セキュリティ アドバイザリー、応答および通告
- CiscoSecure UNIX 製品に関するサポートページ
- CiscoSecure ACS for Windows 製品に関するサポートページ
- テクニカルサポートとドキュメント - Cisco Systems