Guida alla progettazione e all'implementazione di TokenCaching

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Convenzioni
Configurazione
Esempio di rete
Configurazioni
Configurazione di nome utente e password
Configurazione di TokenCaching sulle finestre di Cisco Secure ACS
Configurazione di TokenCaching in Cisco Secure ACS UNIX
Verifica
Risoluzione dei problemi
Debug TokenCaching su Cisco Secure ACS UNIX
Informazioni correlate

Introduzione

Lo scopo di questo documento è discutere la configurazione e la risoluzione dei problemi di TokenCaching. Le sessioni PPP (Point-to-Point Protocol) per gli utenti della scheda di terminale ISDN (TA) vengono in genere terminate nel PC dell'utente. Ciò consente all'utente di controllare la sessione PPP nello stesso modo di una connessione di accesso remoto asincrona (modem), ovvero connettere e disconnettere la sessione in base alle esigenze. In questo modo, l'utente può utilizzare il protocollo PAP (Password Authentication Protocol) per immettere la password per il trasporto (OTP).

Tuttavia, se il secondo canale B è progettato per l'accensione automatica, all'utente deve essere richiesto di inserire un nuovo OTP per il secondo canale B. Il software PPP per PC non raccoglie il secondo OTP. Al contrario, il software tenta di utilizzare la stessa password utilizzata per il canale B primario. Il server Token Card nega il riutilizzo di un OTP in base alla progettazione. CiscoSecure ACS per UNIX (versione 2.2 e successive) e CiscoSecure ACS per Windows (versione 2.1 e successive) eseguono TokenCaching per supportare l'uso della stessa OTP sul secondo canale B. Questa opzione richiede che il server di autenticazione, autorizzazione e accounting (AAA) gestisca le informazioni sullo stato relative alla connessione dell'utente token.

per ulteriori informazioni, fare riferimento a Supporto delle password monouso sull'ISDN.

Prerequisiti

Requisiti

In questo documento si presume che questi elementi siano già stati configurati correttamente:

- Modem di accesso remoto che funziona correttamente.
- Il server di accesso alla rete (NAS) è configurato correttamente, con il server AAA che punta a Cisco Secure ACS UNIX o ACS Windows.
- ACE/SDI è già configurato con Cisco Secure ACS UNIX o ACS Windows e funziona correttamente.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure ACS Unix 2.2 o successivo
- Cisco Secure ACS Windows 2.1 o versione successiva

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione

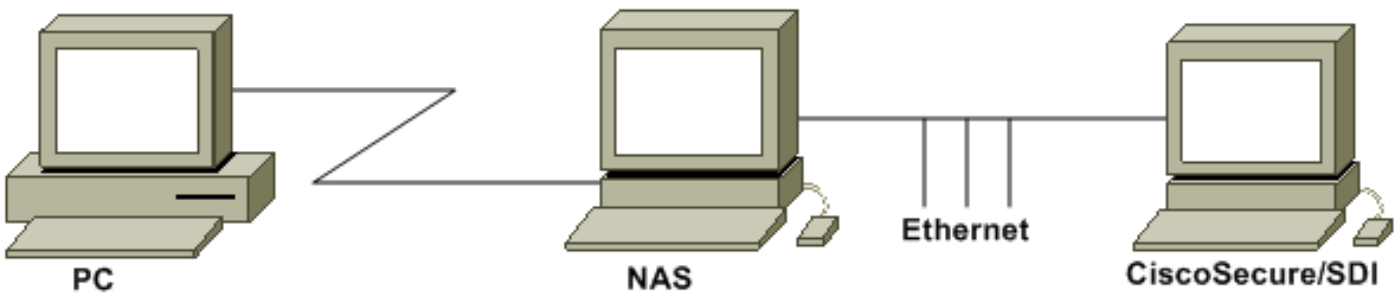
In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:

Un PC effettua la connessione a un NAS e al modem ISDN ed è configurato per il comando **ppp multilink**.



Configurazioni

Nel documento vengono usate queste configurazioni:

- Configurazione di nome utente e password
- Configurazione di TokenCaching sulle finestre di Cisco Secure ACS
- Configurazione di TokenCaching in Cisco Secure ACS UNIX

Configurazione di nome utente e password

In questo documento, il server NAS utilizza il protocollo CHAP (Challenge Handshake Authentication Protocol) per la sessione PPP insieme alla password monouso SDI. Se si utilizza la protezione CHAP, immettere la password nel formato seguente:

- **username** - fadi*pin+code (notare * nel nome utente)
- **password**—chappassword

Un esempio è: username = fadi, chap password = cisco, pin = 1234 e il codice visualizzato sul token è 987654. Pertanto, l'utente immette quanto segue:

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

Nota: se Cisco Secure e il server NAS sono stati configurati per PAP, il nome utente e il token possono essere immessi come segue:

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

O:

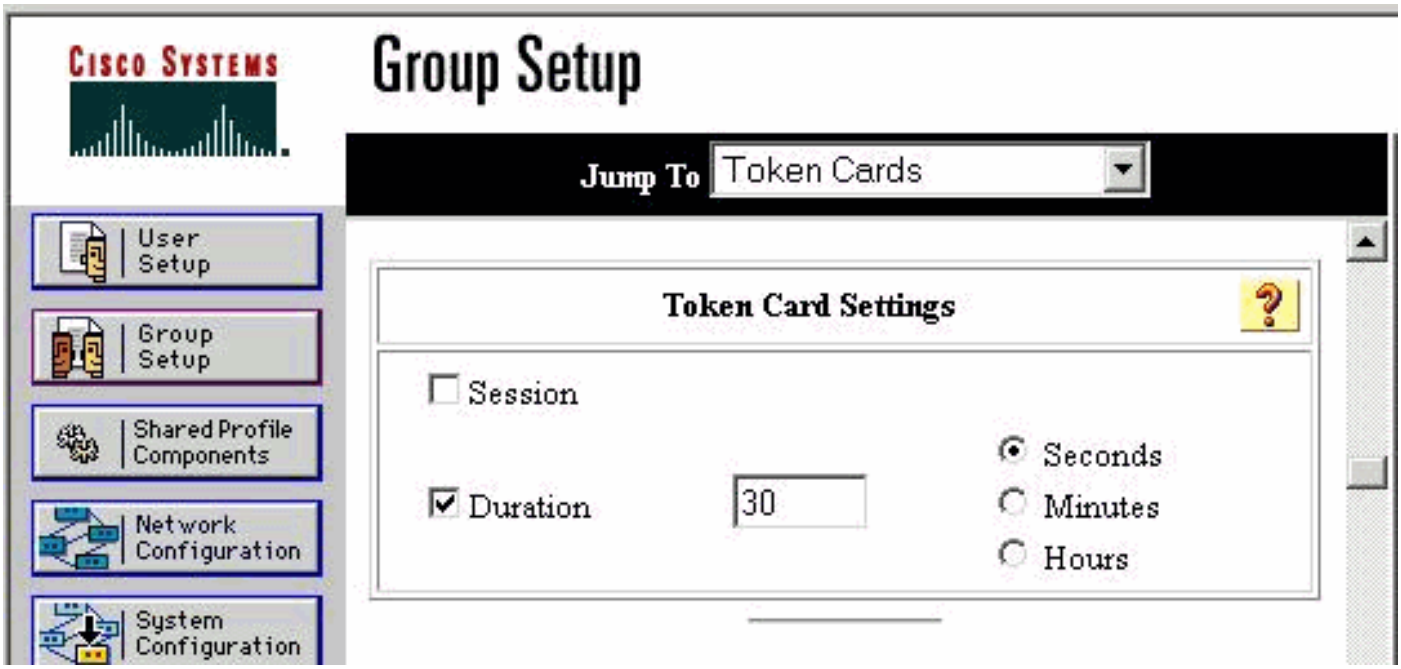
- **username**: username
- **password**—pin+code

Configurazione di TokenCaching sulle finestre di Cisco Secure ACS

L'utente o il gruppo CiscoSecure ACS Windows è configurato come di consueto, con PPP IP e PPP LCP selezionati se si usa TACACS+. Se si utilizza RADIUS, è necessario configurare i seguenti elementi:

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

Inoltre, è possibile controllare i parametri TokenCaching per il gruppo, come mostrato nell'esempio seguente:



Configurazione di TokenCaching in Cisco Secure ACS UNIX

Sono disponibili quattro attributi TokenCaching. L'attributo config_token_cache_absolute_timeout (in secondi) è impostato nel file $install_directory/config/CSU.cfg. Gli altri tre attributi (set server token-caching, set server token-caching-expire-method e set server token-caching-timeout) sono impostati nei profili utente o di gruppo. Per questo documento, l'attributo globale config_token_cache_absolute_timeout è impostato su questo nel file $install_directory/config/CSU.cfg:

```
NUMBER config_token_cache_absolute_timeout = 300;
```

I profili degli attributi TokenCaching del server utente e del server di gruppo sono configurati come mostrato nell'esempio seguente:

```
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 } } }
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Debug TokenCaching su Cisco Secure ACS UNIX

Questo registro CiscoSecure UNIX mostra un'autenticazione riuscita con TokenCaching quando l'autenticazione viene eseguita su due canali BRI:

```
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
```

Informazioni correlate

- Consigli, risposte e avvisi sulla sicurezza Cisco
- Pagina di supporto dei prodotti Cisco Secure UNIX
- Pagina di supporto dei prodotti Cisco Secure ACS per Windows
- Documentazione e supporto tecnico – Cisco Systems