Diseño TokenCaching y Guía de instalación

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Configurar](#)
[Diagrama de la red](#)
[Configuraciones](#)
[Entrada del nombre de usuario y contraseña de la configuración](#)
[TokenCaching de la configuración en el CiscoSecure ACS Windows](#)
[TokenCaching de la configuración en el CiscoSecure ACS UNIX](#)
[Verificación](#)
[Troubleshooting](#)
[TokenCaching del debug en el CiscoSecure ACS UNIX](#)
[Información Relacionada](#)

Introducción

El alcance de este documento es discutir la configuración y el Troubleshooting del TokenCaching. Las sesiones del Point-to-Point Protocol (PPP) para los usuarios del adaptador de terminal ISDN (TA) se terminan típicamente en el usuario PC. Esto permite que el usuario controle a la sesión PPP de la misma manera que una conexión de marcación manual del async (módem), que significa conecta y desconecta la sesión según las necesidades. Esto permite que el usuario utilice el protocolo password authentication (PAP) para ingresar el contraseña que se puede utilizar una sola vez (OTP) para el transporte.

Sin embargo, si el segundo canal B se diseña para subir automáticamente, el usuario debe ser indicado para un nuevo OTP para el segundo canal B. El software PPP PC no recoge el segundo OTP. En lugar, el software intenta utilizar la misma contraseña usada para el canal B primario. El servidor de placa Token niega la reutilización de un OTP por el diseño. El ACS Secure de Cisco para UNIX (versión 2.2 y versiones posteriores) y el CiscoSecure ACS for Windows (2.1 y posterior) realizan el TokenCaching para soportar el uso del mismo OTP en el segundo canal B. Esta opción requiere el servidor del Authentication, Authorization, and Accounting (AAA) mantener la información del estado sobre la conexión del usuario de Token.

Refiera a soportar las contraseñas de uso único en ISDN para más información.

prerrequisitos

Requisitos

Este documento asume que usted hace ya éstos configurar correctamente:

- Un módem de marcación manual que funciona correctamente.
- El servidor de acceso a la red (NAS) configurado correctamente, con el AAA que señala al CiscoSecure ACS UNIX o a las ventanas ACS.
- El ACE/SDI se pone ya con el CiscoSecure ACS UNIX o las ventanas ACS, y trabaja correctamente.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CiscoSecure ACS UNIX 2.2 o más adelante
- 2.1 de Windows del CiscoSecure ACS o más adelante

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configurar

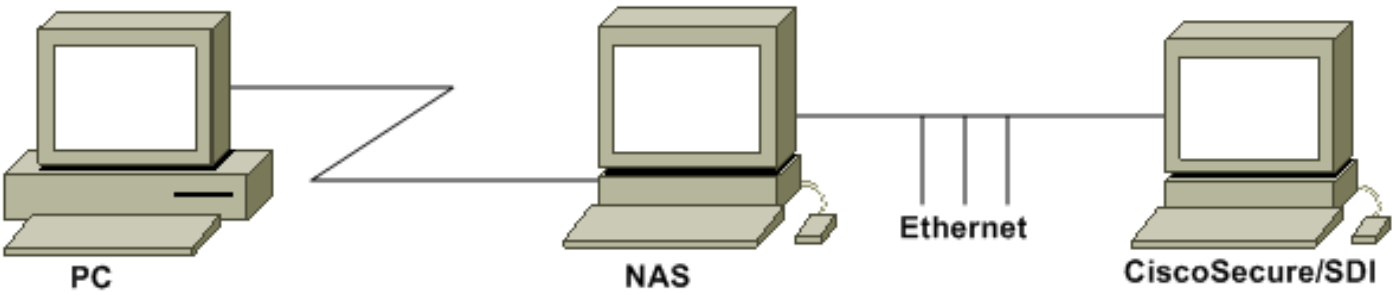
En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Un PC marca en un NAS y el módem ISDN, y se configura para el **comando ppp multilink**.



Configuraciones

En este documento, se utilizan estas configuraciones:

- Entrada del nombre de usuario y contraseña de la configuración
- TokenCaching de la configuración en el CiscoSecure ACS Windows
- TokenCaching de la configuración en el CiscoSecure ACS UNIX

Entrada del nombre de usuario y contraseña de la configuración

En este documento, el NAS utiliza el Challenge Handshake Authentication Protocol (CHAP) para la sesión PPP junto con la contraseña de USO único del SDI. Si usted utiliza la GRIETA, ingrese la contraseña en esta forma:

- **nombre de usuario** — fadi*pin+code (observe * en el nombre de usuario)
- **contraseña** — chappassword

Un ejemplo de esto es: el nombre de usuario = el fadi, la contraseña de la grieta = Cisco, pin = 1234, y el código que muestra en el token es 987654. Por lo tanto, el usuario ingresa esto:

- **nombre de usuario** — fadi*1234987654
- **palabra clave Cisco**

Nota: Si el CiscoSecure y el NAS fueron configurados para el PAP, el nombre de usuario y el token se pueden ingresar como esto:

- **nombre de usuario** — username*pin+code
- **contraseña**—

O:

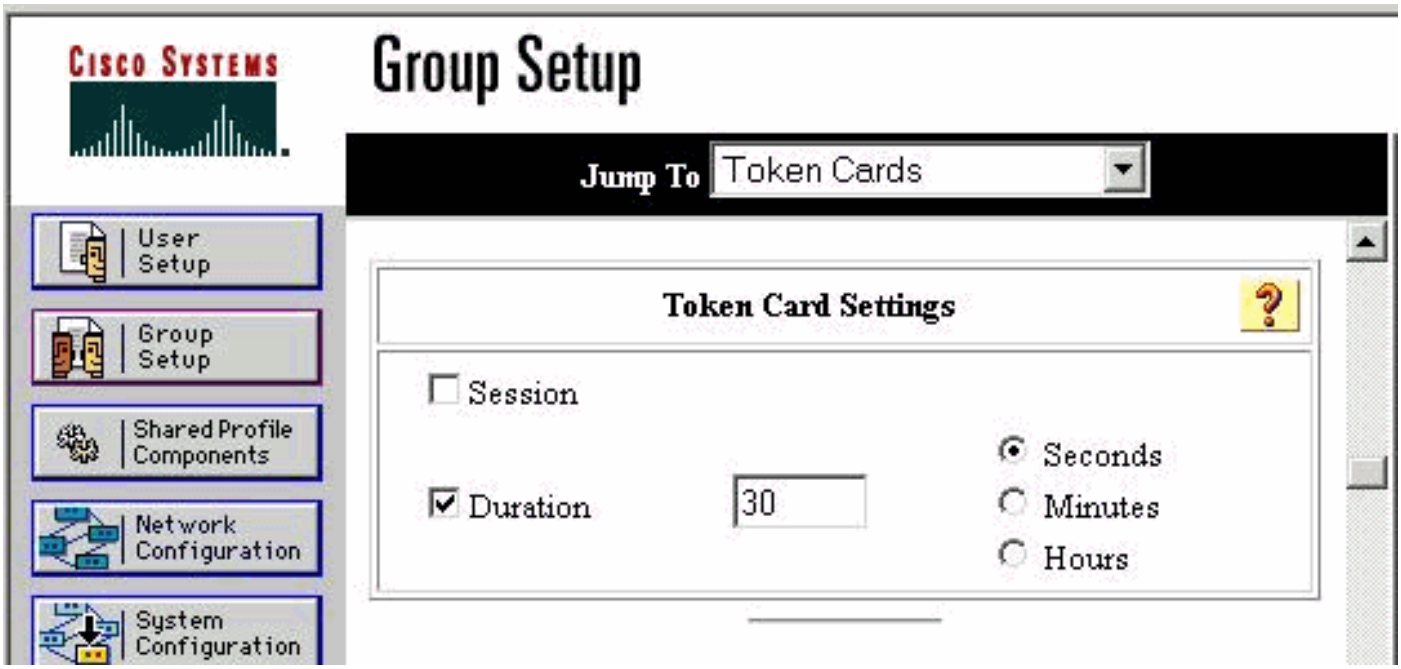
- **nombre de usuario nombre de usuario**
- **contraseña** — pin+code

TokenCaching de la configuración en el CiscoSecure ACS Windows

Configuran al usuario de Windows o al grupo del CiscoSecure ACS como de costumbre, con IP y PPP LCP PPP marcados si usted utiliza el TACACS+. Si usted utiliza el RADIUS, éstos deben ser configurados:

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

Además, los parámetros del TokenCaching se pueden marcar para saber si hay el grupo tal y como se muestra en de este ejemplo:



TokenCaching de la configuración en el CiscoSecure ACS UNIX

Hay cuatro atributos del TokenCaching. El atributo del config_token_cache_absolute_timeout (en los segundos) se fija en el archivo $install_directory/config/CSU.cfg. Los otros tres atributos (set server token-caching, set server token-caching-expire-method, y set server token-caching-timeout) se fijan en el usuario o los perfiles del grupo. Para este documento, el global attribute config_token_cache_absolute_timeout se fija a esto en el archivo $install_directory/config/CSU.cfg:

```
NUMBER config_token_cache_absolute_timeout = 300;
```

Los perfiles del atributo del TokenCaching del usuario y del servidor del grupo se configuran tal y como se muestra en de este ejemplo:

```
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 } } }
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

TokenCaching del debug en el CiscoSecure ACS UNIX

Este registro del CiscoSecure UNIX muestra una autenticación satisfactoria con el TokenCaching, cuando la autenticación ocurre en dos canales 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
```

Información Relacionada

- Cisco Security Advisory, respuestas, y avisos
- Páginas de soporte del producto de UNIX CiscoSecure
- Página de soporte de producto CiscoSecure ACS para Windows
- Soporte Técnico y Documentación - Cisco Systems