TokenCaching, ontwerp- en implementatiegids

Inhoud

Inleiding

Het bereik van dit document is om de installatie en probleemoplossing van TokenCaching te bespreken. Point-to-Point Protocol (PPP)-sessies voor ISDN-terminalgebruikers (TA) worden doorgaans beëindigd op de PC van de gebruiker. Dit staat de gebruiker toe om de PPP zitting op dezelfde manier als een async (modem) dialup te controleren, wat betekent de sessie zoals nodig aan te sluiten en los te koppelen. Dit maakt het de gebruiker mogelijk om Wachtwoord Verificatieprotocol (PAP) te gebruiken om het eenmalige wachtwoord (OTP) voor transport in te voeren.

Als het tweede B-kanaal echter automatisch is ontworpen, moet de gebruiker om een nieuwe OTP voor het tweede B-kanaal worden gevraagd. PC PPP-software verzamelt niet de tweede OTP. In plaats daarvan probeert de software hetzelfde wachtwoord te gebruiken dat wordt gebruikt voor het primaire B-kanaal. De Token Card-server ontkent het hergebruik van een OTP door ontwerp. Cisco Secure ACS voor UNIX (versie 2.2 en hoger) en Cisco Secure ACS voor Windows (2.1 en hoger) voeren TokenCaching uit om het gebruik van dezelfde OTP op het tweede B-kanaal te ondersteunen. Deze optie vereist de authenticatie, autorisatie en accounting (AAA) server om staatsinformatie over de verbinding van de token gebruiker te bewaren.

Raadpleeg Ondersteunende eenmalige wachtwoorden op ISDN voor meer informatie.

Voorwaarden

Vereisten

In dit document wordt ervan uitgegaan dat u deze reeds correct hebt ingesteld:

- Een DICOM-modem die correct werkt.
- De Network Access Server (NAS) is correct ingesteld met AAA dat wijst op Cisco Secure ACS UNIX- of ACS-Windows.
- ACE/SDI is al ingesteld met Cisco Secure ACS UNIX of ACS Windows en werkt correct.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure ACS Unix 2.2 of hoger
- Cisco Secure ACS Windows 2.1 of hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Configureren

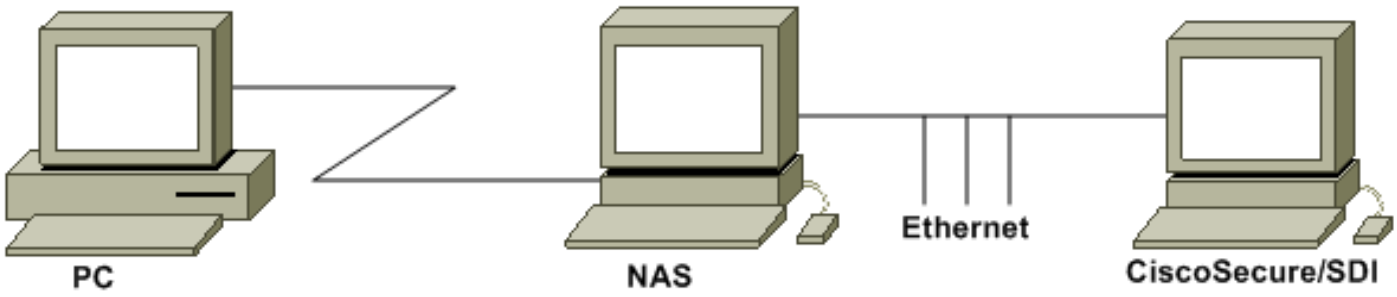
Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:

Een PC Keert in een NAS en de ISDN modem, en wordt gevormd voor de **ppp multilink** opdracht.



Configuraties

Dit document gebruikt deze configuraties:

- Gebruikersnaam en Wachtwoord invoeren
- TokenCken configureren op Cisco Secure ACS Windows
- TokenCken configureren in Cisco Secure ACS UNIX

Gebruikersnaam en Wachtwoord invoeren

In dit document gebruikt NAS Challenge Handshake Authentication Protocol (CHAP) voor de PPP-sessie samen met het eenmalige wachtwoord van SDI. Als u CHAP gebruikt, voer dan het wachtwoord in dit formulier in:

- **gebruikersnaam**—fadi*pin+code (let op de * in de gebruikersnaam)
- **wachtwoord**—wachtwoord

Een voorbeeld hiervan is: gebruikersnaam = fadi, kettingwachtwoord = cisco, pin = 1234, en de code die op het token verschijnt, is 987654. Daarom voert de gebruiker dit in:

- **Gebruikersnaam**—fadi*1234987654
- **wachtwoord**—cisco

Opmerking: Als CiscoSecure en NAS voor PAP zijn geconfigureerd, kunnen de gebruikersnaam en het token als volgt worden ingevoerd:

- **Gebruikersnaam**—gebruikersnaam*pin+code
- **wachtwoord**—

Of:

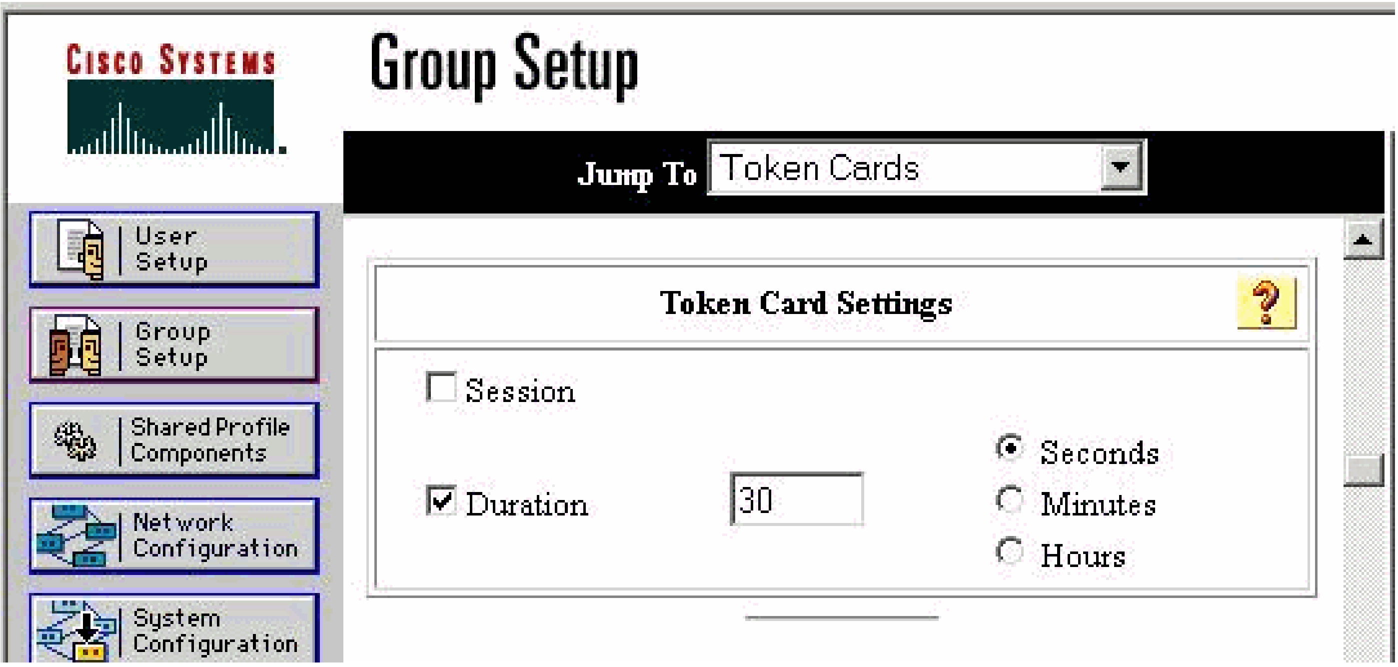
- **gebruikersnaam** - gebruikersnaam
- **wachtwoord**—pins+code

TokenCken configureren op Cisco Secure ACS Windows

De Cisco Secure ACS Windows-gebruiker of -groep is zoals gebruikelijk ingesteld met PPP IP en PPP LCP ingeschakeld als u TACACS+ gebruikt. Als u RADIUS gebruikt, moeten deze worden geconfigureerd:

- Eigenschappen 6 = **Service_Type = geframed**
- Eigenschappen 7 = **Framed_Protocol = PPP**

Daarnaast kunnen de parameters TokenCaching voor de groep worden gecontroleerd zoals in dit voorbeeld:



TokenCken configureren in Cisco Secure ACS UNIX

Er zijn vier TokenCaching-eigenschappen. De van de waarde. De andere drie eigenschappen (set server token-caching, set server token-caching-expiratiemethode en set server token-caching-timeout) worden in de gebruiker- of groepsprofielen ingesteld. Voor dit document wordt de global attributenconfiguratie_token_cache_absoluut_timeout op dit tijdstip ingesteld in het $install_directory/config/CSU.cfg bestand:

```
NUMBER config_token_cache_absolute_timeout = 300;
```

De gebruikersprofielen en de profielen van de groepserver TokenCaching worden ingesteld zoals in dit voorbeeld:

```
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 } } }
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Debug Token Caching op Cisco Secure ACS UNIX

Dit Cisco Secure UNIX-logbestand toont een succesvolle verificatie met TokenCaching, wanneer verificatie plaatsvindt op twee BRI-kanalen:

```
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

Gerelateerde informatie

- Cisco Security Advisories, antwoorden en kennisgevingen
- Cisco Secure UNIX-productondersteuningspagina
- Cisco Secure ACS voor Windows-productondersteuningspagina
- Technische ondersteuning en documentatie – Cisco Systems