Ejemplo de Configuración de Integración SSO de WebVPN con Delegación Limitada Kerberos

Contenido

Introducción

Este documento describe cómo configurar y resolver problemas de WebVPN Single Sign On (SSO) para aplicaciones protegidas por Kerberos.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos básicos sobre estos temas:

- Configuración CLI de Cisco Adaptive Security Appliance (ASA) y configuración VPN de capa de socket seguro (SSL)
- Servicios Kerberos

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Software Cisco ASA, versión 9.0 y posterior
- Cliente de Microsoft Windows 7
- Microsoft Windows 2003 Server y posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Kerberos es un protocolo de autenticación de red que permite a las entidades de red autenticarse entre sí de forma segura. Utiliza un tercero de confianza, el Centro de distribución de claves (KDC), que concede entradas a las entidades de red. Estas notificaciones son utilizadas por las entidades para verificar y confirmar el acceso al servicio solicitado.

Es posible configurar WebVPN SSO para las aplicaciones protegidas por Kerberos con la función Cisco ASA llamada Delegación restringida de Kerberos (KCD). Con esta función, ASA puede solicitar entradas Kerberos en nombre del usuario del portal WebVPN, mientras accede a las aplicaciones protegidas por Kerberos.

Cuando accede a estas aplicaciones a través del portal WebVPN, ya no necesita proporcionar ninguna credencial; en su lugar, se utiliza la cuenta que se utilizó para iniciar sesión en el portal WebVPN.

Refiérase a la sección Cómo Funciona KCD de la Guía de Configuración de ASA para obtener más información.

Interacción Kerberos con ASA

Para WebVPN, el ASA debe solicitar las notificaciones en nombre del usuario (porque el usuario del portal WebVPN sólo tiene acceso al portal, no al servicio Kerberos). Para ello, ASA utiliza extensiones Kerberos para Delegación restringida. Aquí está el flujo:

1. ASA se une al dominio y obtiene un ticket (Ticket1) para una cuenta de computadora con credenciales configuradas en ASA (**comando kcd-server**). Este ticket se utiliza en los siguientes pasos para el acceso a los servicios Kerberos.

2. El usuario hace clic en el enlace del portal WebVPN para la aplicación protegida por Kerberos.

3. ASA solicita (**TGS-REQ**) un billete para la cuenta de computadora con su nombre de host como principal. Esta solicitud incluye el campo **PA-TGS-REQ** con **PA-FOR-USER** con el nombre de usuario principal como el nombre de usuario del portal WebVPN, que es **cisco** en este escenario. El ticket para el servicio Kerberos del Paso 1 se utiliza para la autenticación

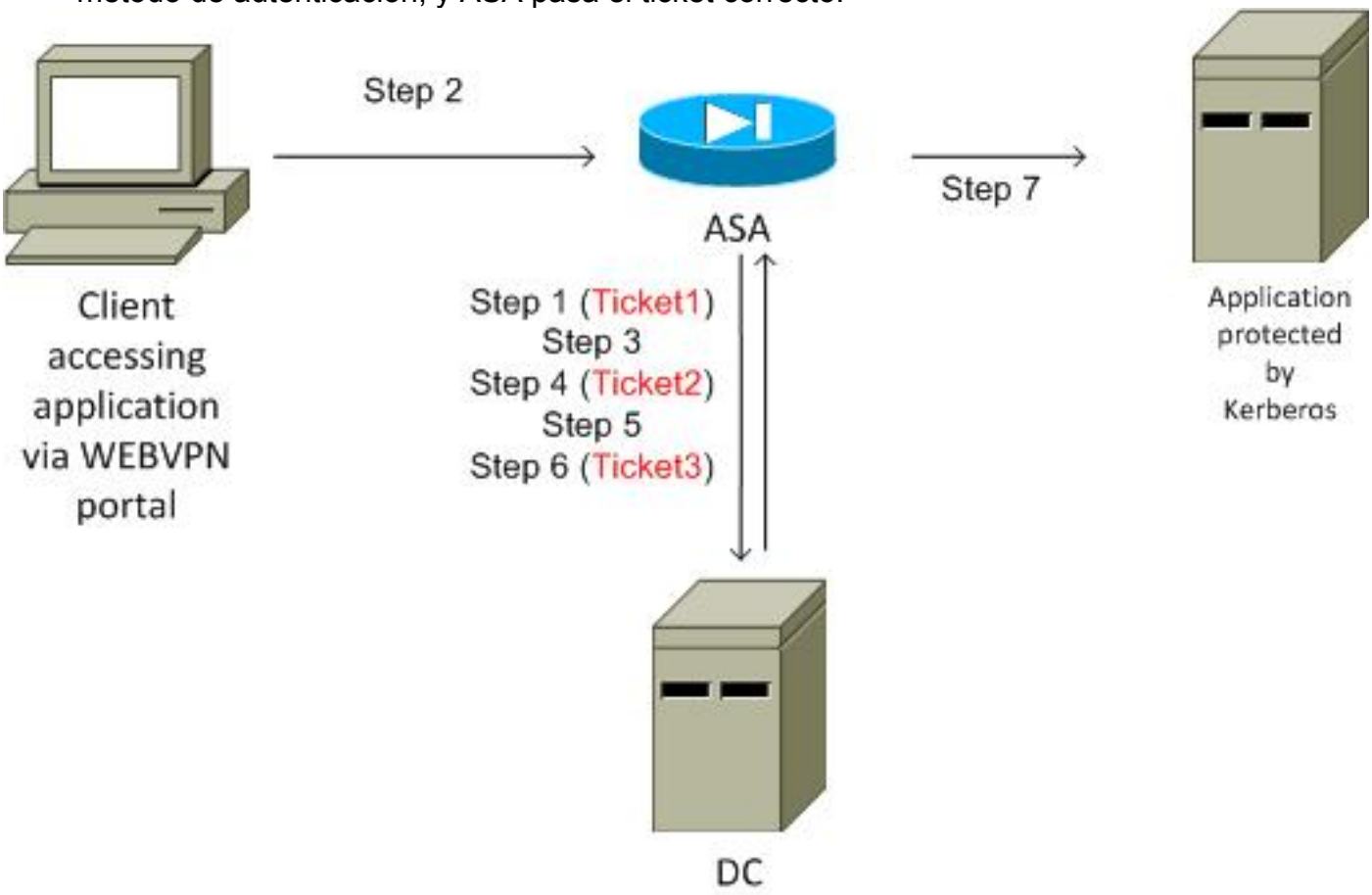
(delegación correcta).

4. Como respuesta, ASA recibe un ticket suplantado (Ticket2) en nombre del usuario de WebVPN (**TGS_REP**) para la cuenta de computadora. Este ticket se utiliza para solicitar los tickets de aplicación en nombre de este usuario WebVPN.

5. ASA inicia otra solicitud (**TGS_REQ**) para obtener el ticket para la aplicación (**HTTP/test.kra-sec.cisco.com**). Esta solicitud utiliza de nuevo el campo **PA-TGS-REQ**, esta vez **sin el** campo **PA-FOR-USER**, pero con el ticket suplantado recibido en el Paso 4.

6. Se devuelve la respuesta (**TGS_REQ**) con el ticket suplantado (Ticket3) para la solicitud.

7. El ASA utiliza este ticket de forma transparente para acceder al servicio protegido, y el usuario WebVPN no necesita ingresar ninguna credencial. Para la aplicación HTTP, se utiliza el mecanismo Simple and Protected GSS-API Negotiation (SPNEGO) para negociar el método de autenticación, y ASA pasa el ticket correcto.



Configurar

Topología

Dominio: kra-sec.cisco.com (10.211.0.221 o 10.211.0.216)

Aplicación Internet Information Services (IIS) 7: test.kra-sec.cisco.com (10.211.0.223)

Controlador de dominio (DC): dc.kra-sec.cisco.com (10.211.0.221 o 10.211.0.216) - Windows2008

ASA: 10.211.0.162

Nombre de usuario/contraseña de WebVPN: Cisco/Cisco

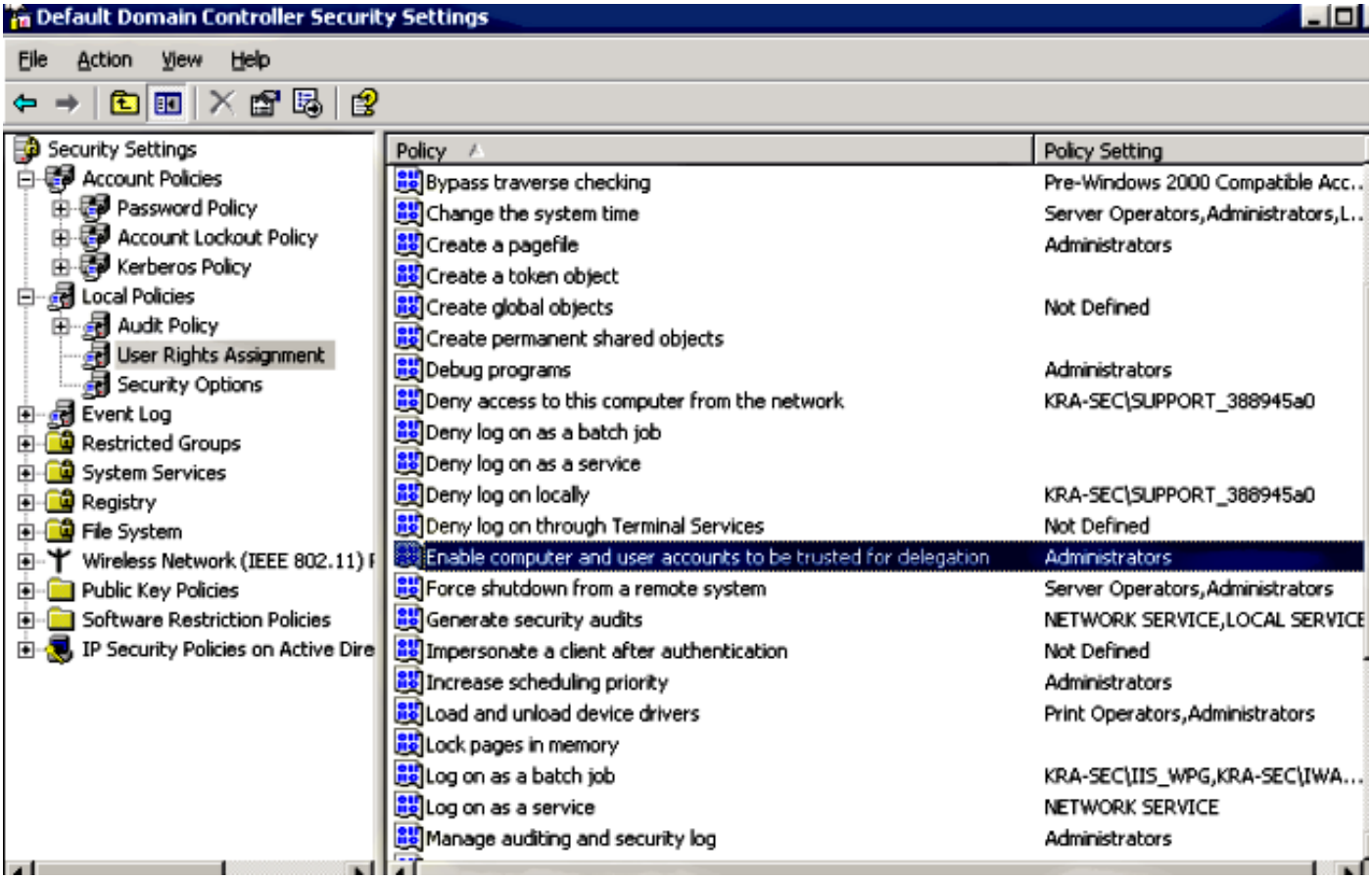
Archivo adjunto: asa-Join.pcap (unirse correctamente al dominio)

Archivo adjunto: asa-kerberos-bad.pcap (solicitud de servicio)

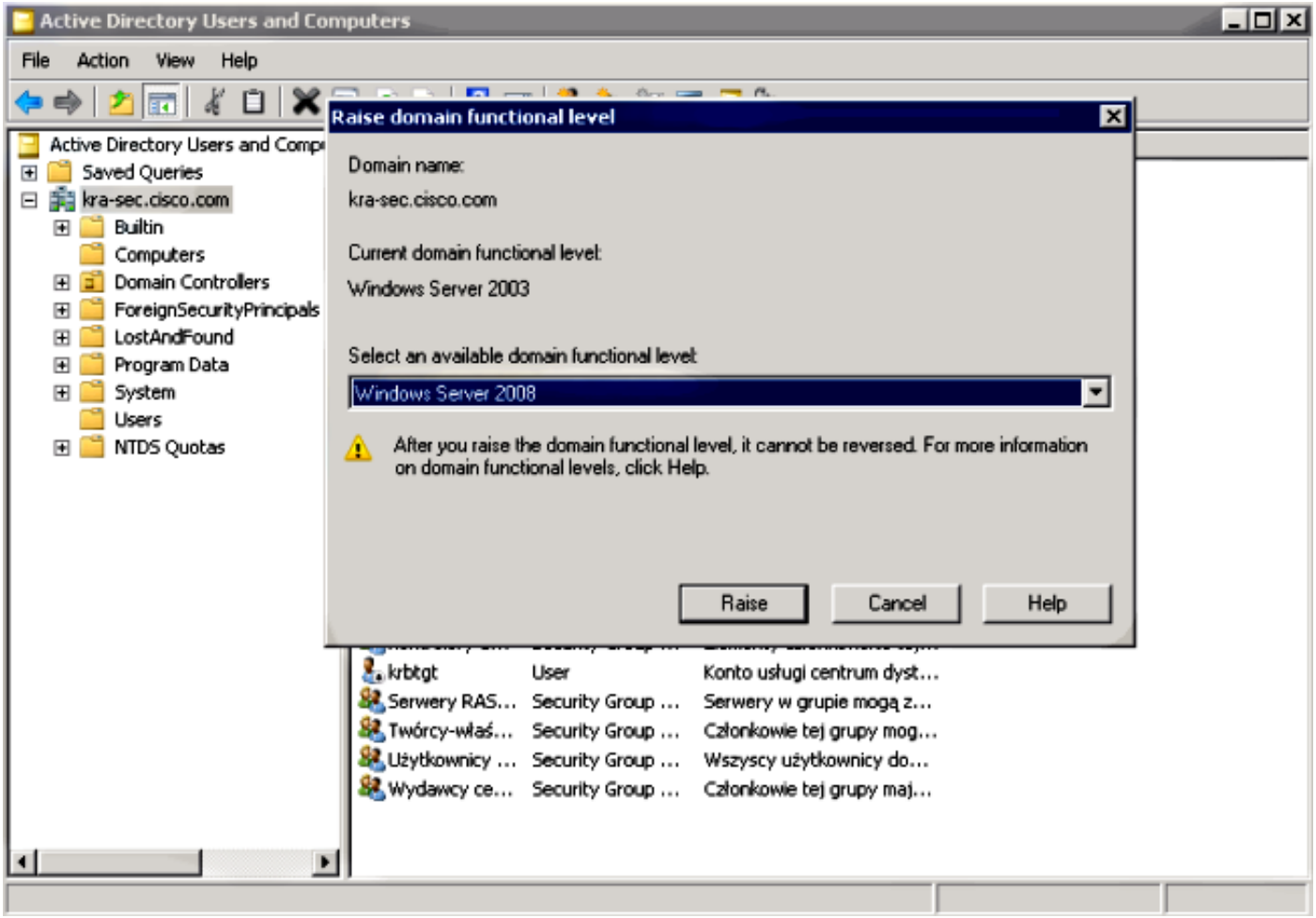
Configuración del controlador de dominio y la aplicación

Configuración de dominio

Se supone que ya existe una aplicación IIS7 funcional protegida por Kerberos (si no, lea la sección Requisitos previos). Debe comprobar la configuración de las delegaciones de los usuarios:



Asegúrese de que el nivel de dominio funcional se eleve a Windows Server 2003 (al menos). El valor predeterminado es Windows Server 2000:



Establecer el nombre principal de servicio (SPN)

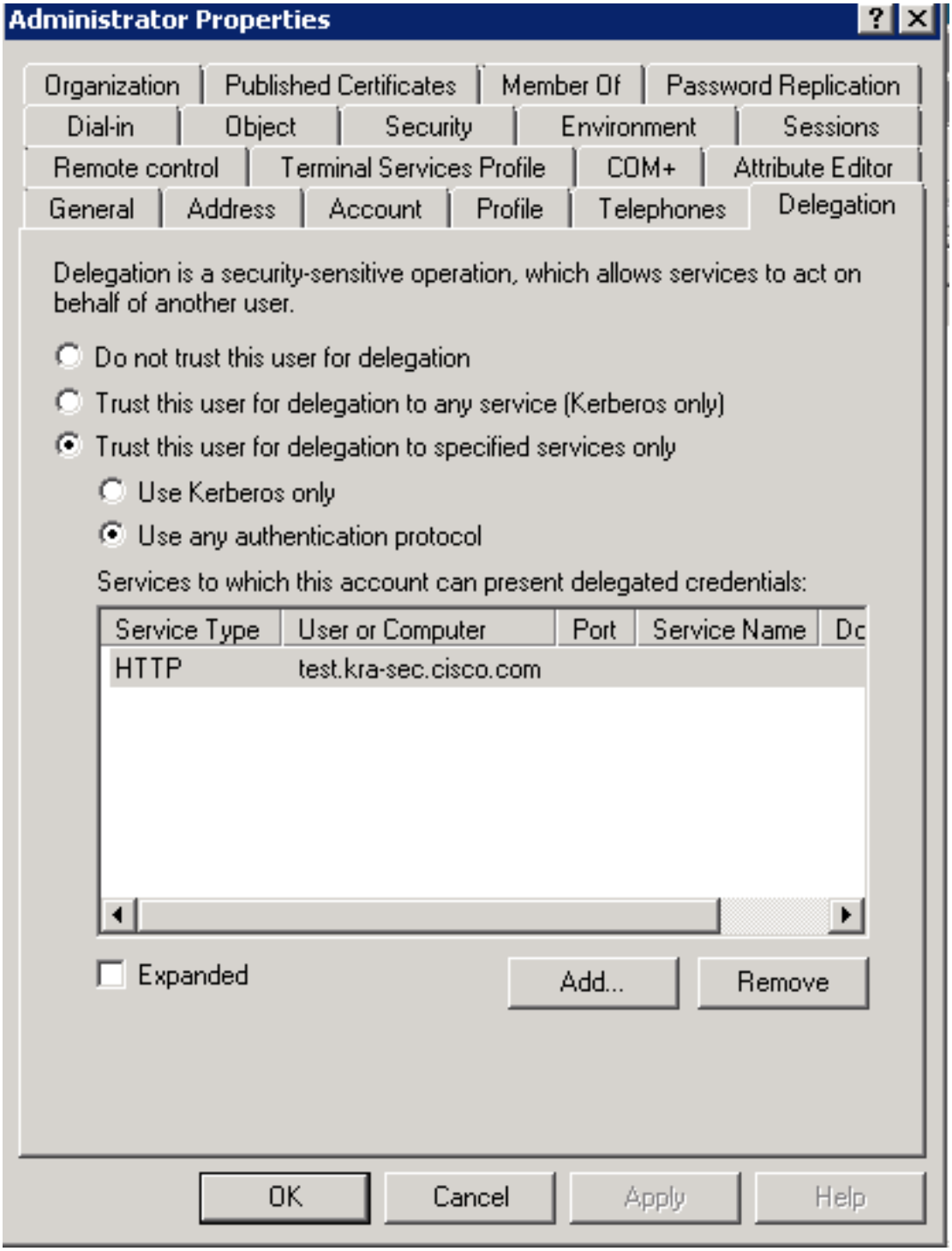
Debe configurar cualquier cuenta en AD con la delegación correcta. Se utiliza una cuenta de administrador. Cuando ASA utiliza esa cuenta, puede solicitar un ticket en nombre de otro usuario (Delegación restringida) para el servicio específico (aplicación HTTP). Para que esto ocurra, se debe crear la delegación correcta para la aplicación/servicio.

Para hacer esta delegación a través de la CLI con **setspan.exe**, que forma parte de las Herramientas de soporte de Windows Server 2003 Service Pack 1, ingrese este comando:

```
setspn.exe -A HTTP/test.kra-sec.cisco.com kra-sec.cisco.com\Administrator
```

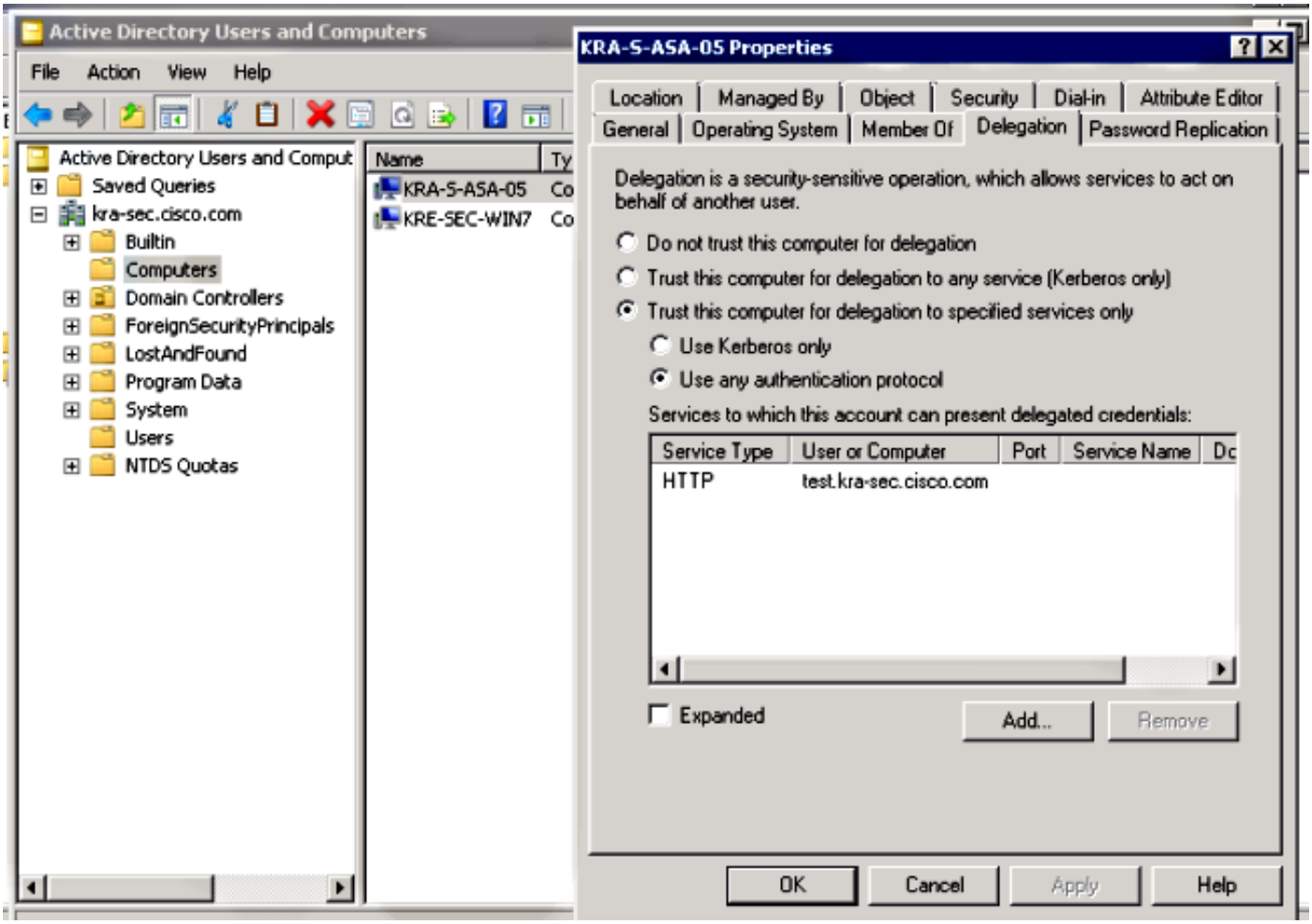
Esto indica que el nombre de usuario **Administrator** es la cuenta de confianza para la delegación del servicio HTTP en **test.kra-sec.cisco.com**.

El comando **SPN** también es necesario para activar la **ficha Delegación** para ese usuario. Cuando ingrese el comando, aparecerá la ficha Delegación para el administrador. Es importante habilitar "Usar cualquier protocolo de autenticación" porque "Usar sólo Kerberos" no admite la extensión de delegación restringida.



En la ficha **General**, también es posible inhabilitar la autenticación previa Kerberos. Sin embargo, esto no se aconseja, porque esta función se utiliza para proteger el DC contra los ataques de repetición. El ASA puede funcionar correctamente con la autenticación previa.

Este procedimiento también se aplica con delegación para la cuenta de computadora (el ASA se introduce en el dominio como una computadora para establecer una relación de "confianza"):



Configuración en ASA

```
interface Vlan211
 nameif inside
 security-level 100
 ip address 10.211.0.162 255.255.255.0

hostname KRA-S-ASA-05
domain-name kra-sec.cisco.com

dns domain-lookup inside
dns server-group DNS-GROUP
 name-server 10.211.0.221
domain-name kra-sec.cisco.com

aaa-server KerberosGroup protocol kerberos
aaa-server KerberosGroup (inside) host 10.211.0.221
 kerberos-realm KRA-SEC.CISCO.COM

webvpn
 enable outside
 enable inside
  kcd-server KerberosGroup username Administrator password *****

group-policy G1 internal
group-policy G1 attributes
 WebVPN
   url-list value KerberosProtected
username cisco password 3USUcOPFUiMCO4Jk encrypted
```

```
tunnel-group WEB type remote-access
tunnel-group WEB general-attributes
 default-group-policy G1
tunnel-group WEB webvpn-attributes
 group-alias WEB enable
 dns-group DNS-GROUP
```

Verificación

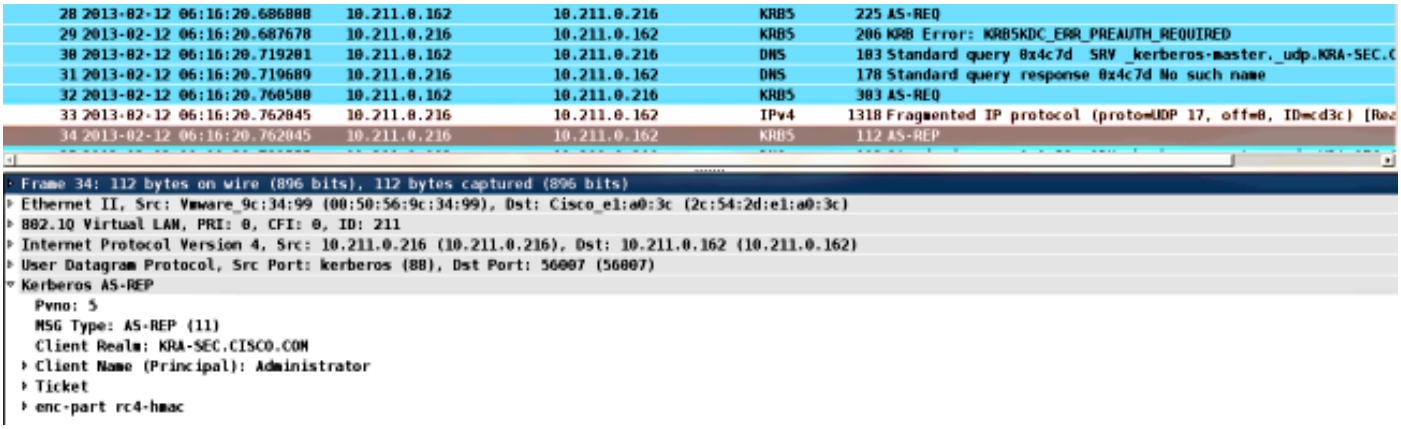
ASA se une al dominio

Después de que se utilice el comando **kcd-server**, ASA intenta unirse al dominio:

```
********** START: KERBEROS PACKET DECODE ************
Kerberos: Message type KRB_AS_REQ
Kerberos: Option forwardable
Kerberos: Client Name KRA-S-ASA-05$
Kerberos: Client Realm KRA-SEC.CISCO.COM
Kerberos: Server Name krbtgt
Kerberos: Start time 0
Kerberos: End time -878674400
Kerberos: Renew until time -878667552
Kerberos: Nonce 0xa9db408e
Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type des-cbc-md5
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4
Kerberos: Encryption type des3-cbc-sha1
********** END: KERBEROS PACKET DECODE ************
In kerberos_recv_msg
In KCD_self_tkt_process_response
********** START: KERBEROS PACKET DECODE ************
Kerberos: Message type KRB_ERROR
Kerberos: Error type: Additional pre-authentication required, -1765328359
(0x96c73a19)
Kerberos: Encrypt Type: 23 (rc4-hmac-md5)
Salt: "" Salttype: 0
Kerberos: Encrypt Type: 3 (des-cbc-md5)
Salt: "KRA-SEC.CISCO.COMhostkra-s-asa-05.kra-sec.cisco.com" Salttype: 0
Kerberos: Encrypt Type: 1 (des-cbc-crc)
Salt: "KRA-SEC.CISCO.COMhostkra-s-asa-05.kra-sec.cisco.com" Salttype: 0
Kerberos: Preauthentication type unknown
Kerberos: Preauthentication type encrypt timestamp
Kerberos: Preauthentication type unknown
Kerberos: Preauthentication type unknown
Kerberos: Server time 1360917305
Kerberos: Realm KRA-SEC.CISCO.COM
Kerberos: Server Name krbtgt
********** END: KERBEROS PACKET DECODE ************
Attempting to parse the error response from KCD server.
Kerberos library reports: "Additional pre-authentication required"
In kerberos_send_request
********** START: KERBEROS PACKET DECODE ************
Kerberos: Message type KRB_AS_REQ
Kerberos: Preauthentication type encrypt timestamp
Kerberos: Option forwardable
Kerberos: Client Name KRA-S-ASA-05$
Kerberos: Client Realm KRA-SEC.CISCO.COM
```

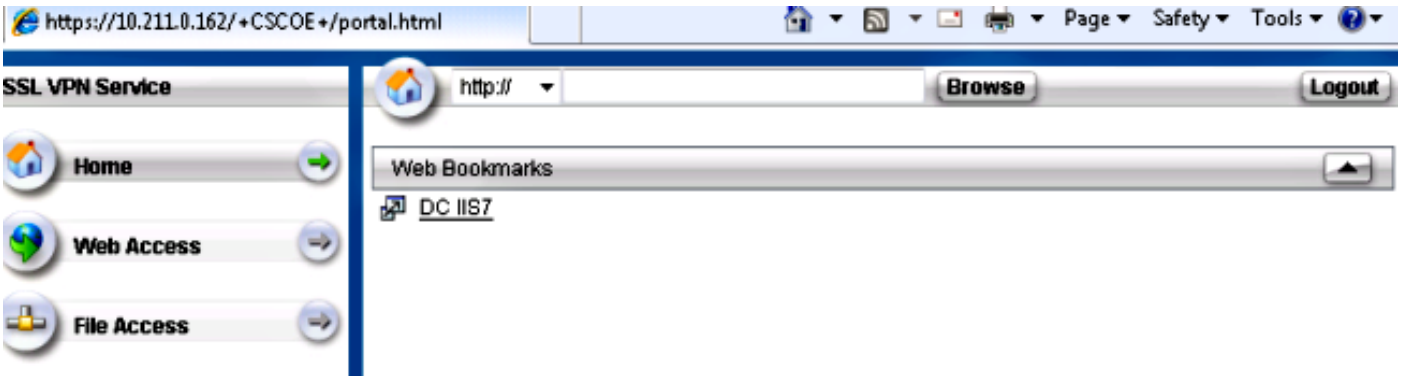
```
Kerberos: Server Name krbtgt
Kerberos: Start time 0
Kerberos: End time -878667256
Kerberos: Renew until time -878672192
Kerberos: Nonce 0xa9db408e
Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type des-cbc-md5
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4
Kerberos: Encryption type des3-cbc-sha1
********** END: KERBEROS PACKET DECODE ************
In kerberos_recv_msg
In KCD_self_tkt_process_response
********** START: KERBEROS PACKET DECODE ************
Kerberos: Message type KRB_AS_REP
Kerberos: Client Name KRA-S-ASA-05$
Kerberos: Client Realm KRA-SEC.CISCO.COM
********** END: KERBEROS PACKET DECODE ************
INFO: Successfully stored self-ticket in cache a6588e0
KCD self-ticket retrieval succeeded.
In kerberos_close_connection
remove_req 0xcc09ad18 session 0x1 id 0
free_kip 0xcc09ad18
kerberos: work queue empty
```

El ASA puede unirse correctamente al dominio. Después de la autenticación correcta, el ASA recibe un ticket para el principal: Administrador en el paquete **AS_REP** (Ticket1 descrito en el Paso 1).

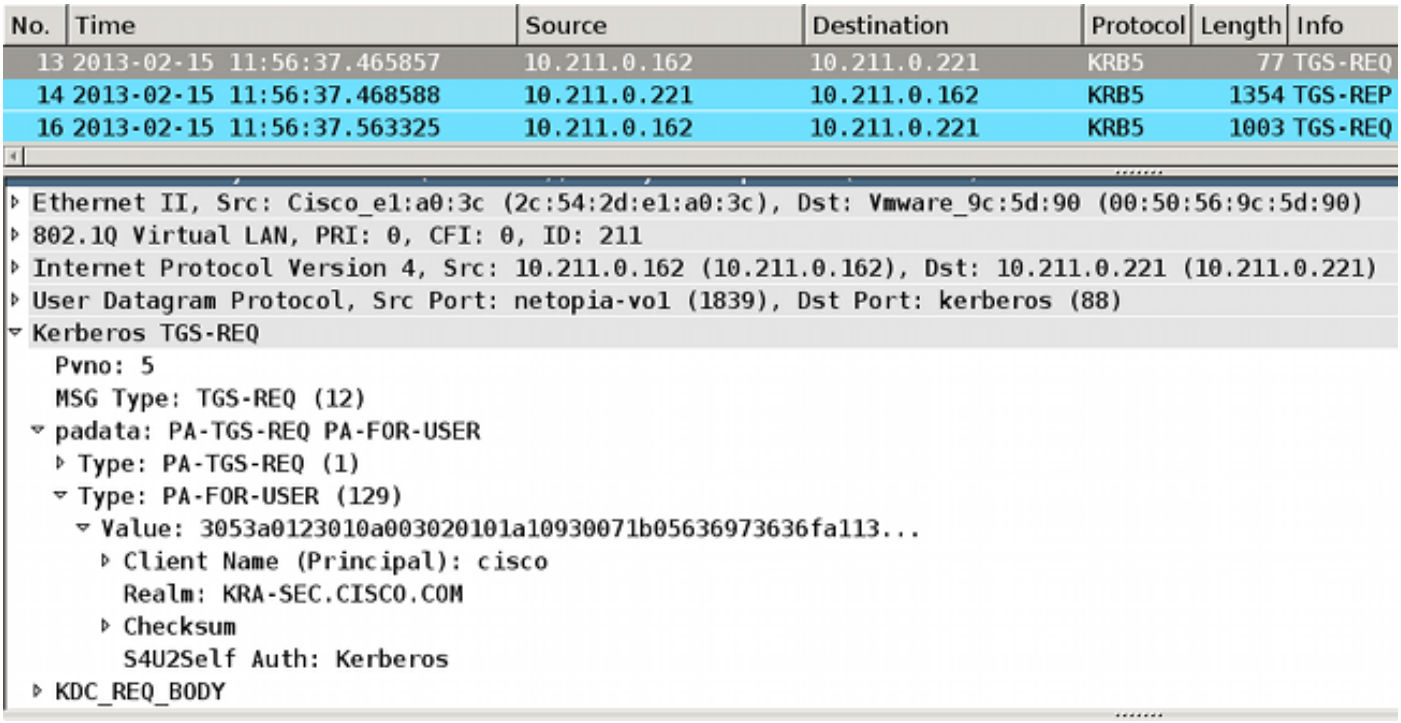


Solicitud del servicio

El usuario hace clic en el enlace WebVPN:

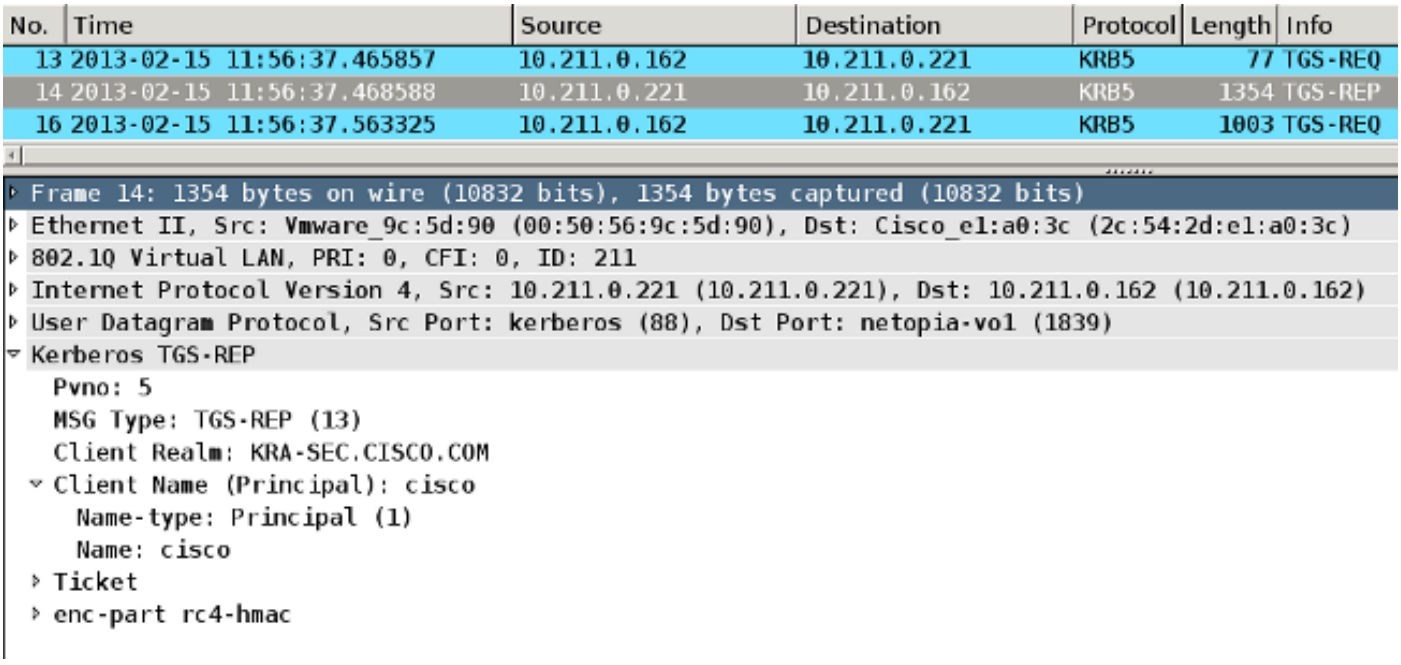


ASA envía el **TGS_REQ** para un ticket suplantado con el ticket recibido en el paquete **AS_REP**:



Nota: El valor **PA-FOR-USER** es **cisco** (usuario WebVPN). **PA-TGS-REQ** contiene el ticket recibido para la solicitud de servicio Kerberos (el nombre de host ASA es el principal).

ASA obtiene una respuesta correcta con el ticket suplantado para el usuario **cisco** (Ticket2 descrito en el Paso 4):



Esta es la solicitud del ticket para el servicio HTTP (algunas depuraciones se omiten para mayor claridad):

```
KRA-S-ASA-05# show WebVPN kcd
Kerberos Realm: TEST-CISCO.COM
Domain Join   : Complete

find_spn_in_url(): URL - /
build_host_spn(): host - test.kra-sec.cisco.com
```

```
build_host_spn(): SPN - HTTP/test.kra-sec.cisco.com
KCD_unicorn_get_cred(): Attempting to retrieve required KCD tickets.
In KCD_check_cache_validity, Checking cache validity for type KCD service
ticket cache name:  and spn HTTP/test.kra-sec.cisco.com.
In kerberos_cache_open: KCD opening cache .
Cache doesn't exist!
In KCD_check_cache_validity, Checking cache validity for type KCD self ticket
cache name: a6ad760 and spn N/A.
In kerberos_cache_open: KCD opening cache a6ad760.
Credential is valid.
In KCD_check_cache_validity, Checking cache validity for type KCD impersonate
ticket cache name:  and spn N/A.
In kerberos_cache_open: KCD opening cache .
Cache doesn't exist!
KCD requesting impersonate ticket retrieval for:
        user     : cisco
       in_cache : a6ad760
       out_cache: adab04f8I
Successfully queued up AAA request to retrieve KCD tickets.
kerberos mkreq: 0x4
kip_lookup_by_sessID: kip with id 4 not found
alloc_kip 0xaceaf560
   new request 0x4 --> 1 (0xaceaf560)
add_req 0xaceaf560 session 0x4 id 1
In KCD_cred_tkt_build_request
In kerberos_cache_open: KCD opening cache a6ad760.
KCD_cred_tkt_build_request: using KRA-S-ASA-05 for principal name
In kerberos_open_connection
In kerberos_send_request

********** START: KERBEROS PACKET DECODE ************
Kerberos: Message type KRB_TGS_REQ
Kerberos: Preauthentication type ap request
Kerberos: Preauthentication type unknown
Kerberos: Option forwardable
Kerberos: Option renewable
Kerberos: Client Realm KRA-SEC.CISCO.COM
Kerberos: Server Name KRA-S-ASA-05
Kerberos: Start time 0
Kerberos: End time -1381294376
Kerberos: Renew until time 0
Kerberos: Nonce 0xe9d5fd7f
Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type des3-cbc-sha
Kerberos: Encryption type des-cbc-md5
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4
********** END: KERBEROS PACKET DECODE ************
In kerberos_recv_msg
In KCD_cred_tkt_process_response

********** START: KERBEROS PACKET DECODE ************
Kerberos: Message type KRB_TGS_REP
Kerberos: Client Name cisco
Kerberos: Client Realm KRA-SEC.CISCO.COM
********** END: KERBEROS PACKET DECODE ************
KCD_unicorn_callback(): called with status: 1.
Successfully retrieved impersonate ticket for user: cisco
KCD callback requesting service ticket retrieval for:
       user     :
       in_cache : a6ad760
       out_cache: adab04f8S
       DC_cache : adab04f8I
       SPN      : HTTP/test.kra-sec.cisco.com
```

```
Successfully queued up AAA request from callback to retrieve KCD tickets.
In kerberos_close_connection
remove_req 0xaceaf560 session 0x4 id 1
free_kip 0xaceaf560
kerberos mkreq: 0x5
kip_lookup_by_sessID: kip with id 5 not found
alloc_kip 0xaceaf560
   new request 0x5 --> 2 (0xaceaf560)
add_req 0xaceaf560 session 0x5 id 2
In KCD_cred_tkt_build_request
In kerberos_cache_open: KCD opening cache a6ad760.
In kerberos_cache_open: KCD opening cache adab04f8I.
In kerberos_open_connection
In kerberos_send_request

********** START: KERBEROS PACKET DECODE ************
Kerberos: Message type KRB_TGS_REQ
Kerberos: Preauthentication type ap request
Kerberos: Option forwardable
Kerberos: Option renewable
Kerberos: Client Realm KRA-SEC.CISCO.COM
Kerberos: Server Name HTTP
Kerberos: Start time 0
Kerberos: End time -1381285944
Kerberos: Renew until time 0
Kerberos: Nonce 0x750cf5ac
Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type des3-cbc-sha
Kerberos: Encryption type des-cbc-md5
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4
********** END: KERBEROS PACKET DECODE ************
In kerberos_recv_msg
In KCD_cred_tkt_process_response

********** START: KERBEROS PACKET DECODE ************
Kerberos: Message type KRB_TGS_REP
Kerberos: Client Name cisco
Kerberos: Client Realm KRA-SEC.CISCO.COM
********** END: KERBEROS PACKET DECODE ************
KCD_unicorn_callback(): called with status: 1.
Successfully retrieved service ticket
for user cisco, spn HTTP/test.kra-sec.cisco.com
In kerberos_close_connection
remove_req 0xaceaf560 session 0x5 id 2
free_kip 0xaceaf560
kerberos: work queue empty
ucte_krb_authenticate_connection(): ctx - 0xad045dd0, proto - http,
host - test.kra-sec.cisco.com
In kerberos_cache_open: KCD opening cache adab04f8S.
Source: cisco@KRA-SEC.CISCO.COM
Target: HTTP/test.kra-sec.cisco.com@KRA-SEC.CISCO.COM
```

El ASA recibe el ticket suplantado correcto para el servicio HTTP (Ticket3 descrito en el Paso 6).

Ambos billetes pueden verificarse. El primero es el ticket suplantado para el usuario **cisco**, que se utiliza para solicitar y recibir el segundo ticket para el servicio HTTP al que se accede:

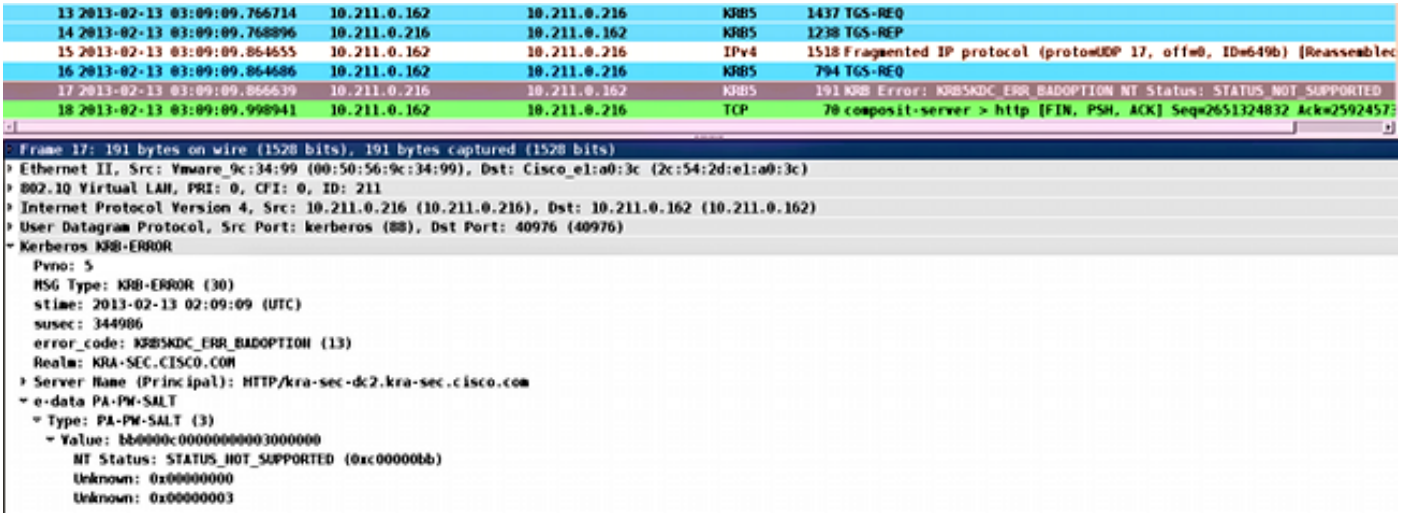
```
KRA-S-ASA-05(config)# show aaa kerberos
Default Principal: cisco@KRA-SEC.CISCO.COM
Valid Starting       Expires              Service Principal
19:38:10 CEST Oct 2 2013 05:37:33 CEST Oct 3 2013 KRA-S-ASA-05@KRA-SEC.CISCO.COM
```

```
Default Principal: cisco@KRA-SEC.CISCO.COM
Valid Starting       Expires              Service Principal
19:38:10 CEST Oct 2 2013 05:37:33 CEST Oct 3 2013
HTTP/test.kra-sec.cisco.com@KRA-SEC.CISCO.COM
```

Este ticket HTTP (Ticket3) se utiliza para el acceso HTTP (con SPNEGO) y el usuario no necesita proporcionar ninguna credencial.

Troubleshoot

A veces puede que se encuentre con un problema de delegación incorrecta. Por ejemplo, ASA utiliza un ticket para solicitar el servicio **HTTP/test.kra-sec.cisco.com** (Paso 5), pero la respuesta es **KRB-ERROR** con **ERR_BADOPTION**:



Este es un problema típico que se produce cuando la delegación no está configurada correctamente. ASA informa que **"KDC no puede cumplir con la opción solicitada"**:

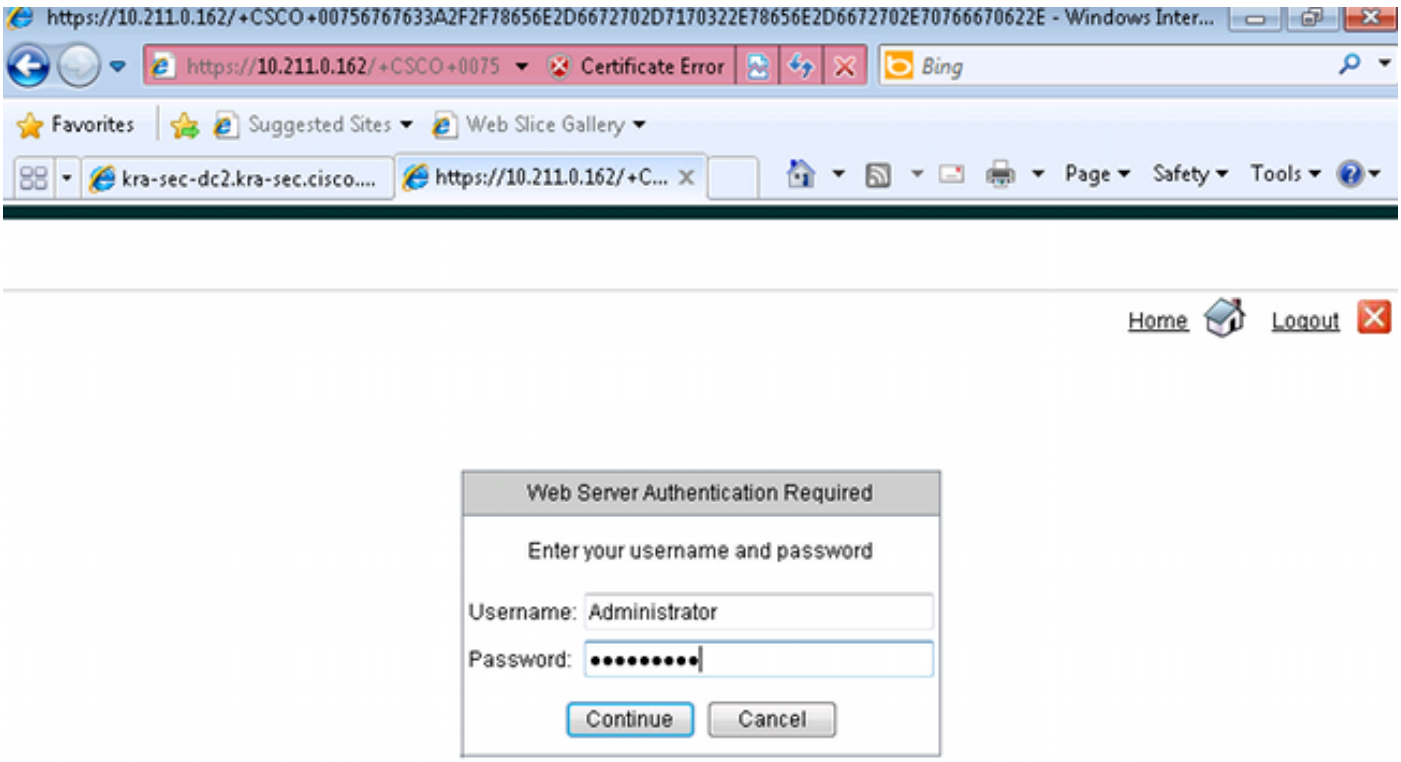
```
KRA-S-ASA-05# ucte_krb_get_auth_cred(): ctx = 0xcc4b5390,
WebVPN_session = 0xc919a260, protocol = 1
find_spn_in_url(): URL - /
build_host_spn(): host - test.kra-sec.cisco.com
build_host_spn(): SPN - HTTP/test.kra-sec.cisco.com
KCD_unicorn_get_cred(): Attempting to retrieve required KCD tickets.
In KCD_check_cache_validity, Checking cache validity for type KCD service ticket
cache name: and spn HTTP/test.kra-sec.cisco.com.
In kerberos_cache_open: KCD opening cache .
Cache doesn't exist!
In KCD_check_cache_validity, Checking cache validity for type KCD self ticket
cache name: a6588e0 and spn N/A.
In kerberos_cache_open: KCD opening cache a6588e0.
Credential is valid.
In KCD_check_cache_validity, Checking cache validity for type KCD impersonate
ticket cache name: and spn N/A.
In kerberos_cache_open: KCD opening cache .
Cache doesn't exist!
KCD requesting impersonate ticket retrieval for:
user : cisco
in_cache : a6588e0
out_cache: c919a260I
Successfully queued up AAA request to retrieve KCD tickets.
kerberos mkreq: 0x4
```

```
kip_lookup_by_sessID: kip with id 4 not found
alloc_kip 0xcc09ad18
new request 0x4 --> 1 (0xcc09ad18)
add_req 0xcc09ad18 session 0x4 id 1
In KCD_cred_tkt_build_request
In kerberos_cache_open: KCD opening cache a6588e0.
KCD_cred_tkt_build_request: using KRA-S-ASA-05$ for principal name
In kerberos_open_connection
In kerberos_send_request
********** START: KERBEROS PACKET DECODE ************
Kerberos: Message type KRB_TGS_REQ
Kerberos: Preauthentication type ap request
Kerberos: Preauthentication type unknown
Kerberos: Option forwardable
Kerberos: Option renewable
Kerberos: Client Realm KRA-SEC.CISCO.COM
Kerberos: Server Name KRA-S-ASA-05$
Kerberos: Start time 0
Kerberos: End time -856104128
Kerberos: Renew until time 0
Kerberos: Nonce 0xb086e4a5
Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type des3-cbc-sha
Kerberos: Encryption type des-cbc-md5
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4
********** END: KERBEROS PACKET DECODE ************
In kerberos_recv_msg
In KCD_cred_tkt_process_response
********** START: KERBEROS PACKET DECODE ************
Kerberos: Message type KRB_TGS_REP
Kerberos: Client Name cisco
Kerberos: Client Realm KRA-SEC.CISCO.COM
********** END: KERBEROS PACKET DECODE ************
KCD_unicorn_callback(): called with status: 1.
Successfully retrieved impersonate ticket for user: cisco
KCD callback requesting service ticket retrieval for:
user :
in_cache : a6588e0
out_cache: c919a260S
DC_cache : c919a260I
SPN : HTTP/test.kra-sec.cisco.com
Successfully queued up AAA request from callback to retrieve KCD tickets.
In kerberos_close_connection
remove_req 0xcc09ad18 session 0x4 id 1
free_kip 0xcc09ad18
kerberos mkreq: 0x5
kip_lookup_by_sessID: kip with id 5 not found
alloc_kip 0xcc09ad18
new request 0x5 --> 2 (0xcc09ad18)
add_req 0xcc09ad18 session 0x5 id 2
In KCD_cred_tkt_build_request
In kerberos_cache_open: KCD opening cache a6588e0.
In kerberos_cache_open: KCD opening cache c919a260I.
In kerberos_open_connection
In kerberos_send_request
********** START: KERBEROS PACKET DECODE ************
Kerberos: Message type KRB_TGS_REQ
Kerberos: Preauthentication type ap request
Kerberos: Option forwardable
Kerberos: Option renewable
Kerberos: Client Realm KRA-SEC.CISCO.COM
Kerberos: Server Name HTTP
Kerberos: Start time 0
```

```
Kerberos: End time -856104568
Kerberos: Renew until time 0
Kerberos: Nonce 0xf84c9385
Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type des3-cbc-sha
Kerberos: Encryption type des-cbc-md5
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4
********** END: KERBEROS PACKET DECODE ************
In kerberos_recv_msg
In KCD_cred_tkt_process_response
********** START: KERBEROS PACKET DECODE ************
Kerberos: Message type KRB_ERROR
Kerberos: Error type: KDC can't fulfill requested option, -1765328371
(0x96c73a0d)
Kerberos: Server time 1360917437
Kerberos: Realm KRA-SEC.CISCO.COM
Kerberos: Server Name HTTP
********** END: KERBEROS PACKET DECODE ************
Kerberos library reports: "KDC can't fulfill requested option"
KCD_unicorn_callback(): called with status: -3.
KCD callback called with AAA error -3.
In kerberos_close_connection
remove_req 0xcc09ad18 session 0x5 id 2
free_kip 0xcc09ad18
kerberos: work queue empty
```

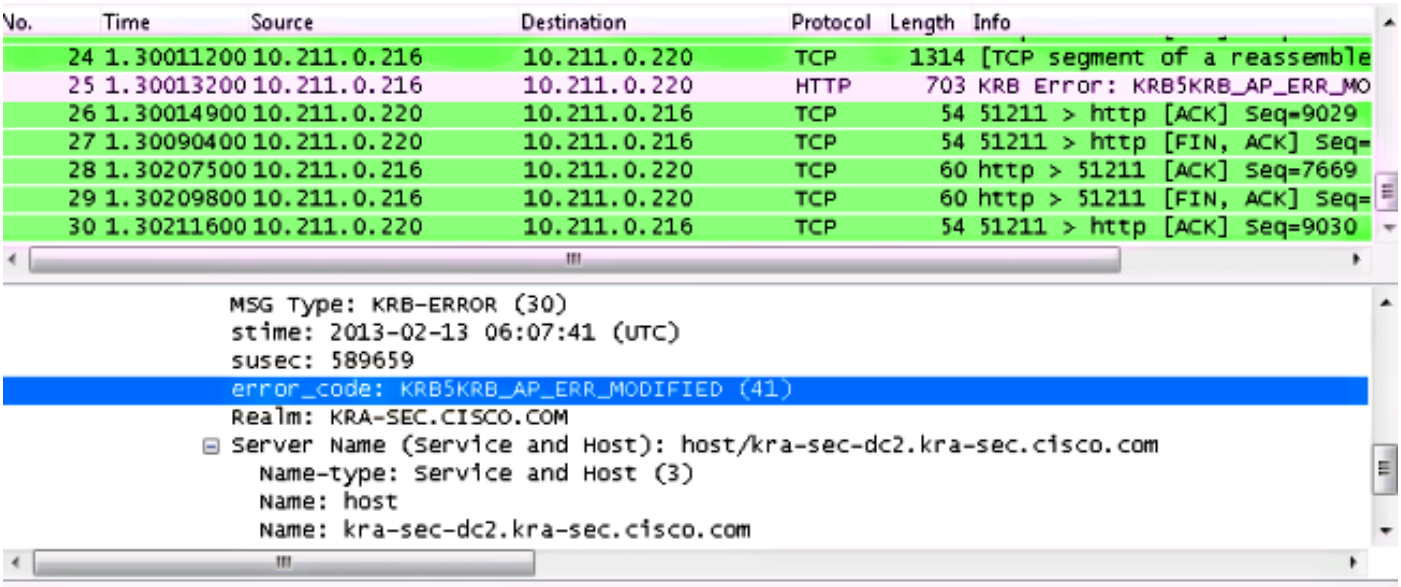
Este es básicamente el mismo problema que se describe en las capturas - la falla es **en TGS_REQ con BAD_OPTION**.

Si la respuesta es **Success**, el ASA recibe un ticket para el servicio **HTTP/test.kra-sec.cisco.com**, que se utiliza para la negociación **SPNEGO**. Sin embargo, debido a la falla, se negocia **NT LAN Manager (NTLM)** y el usuario debe proporcionar credenciales:

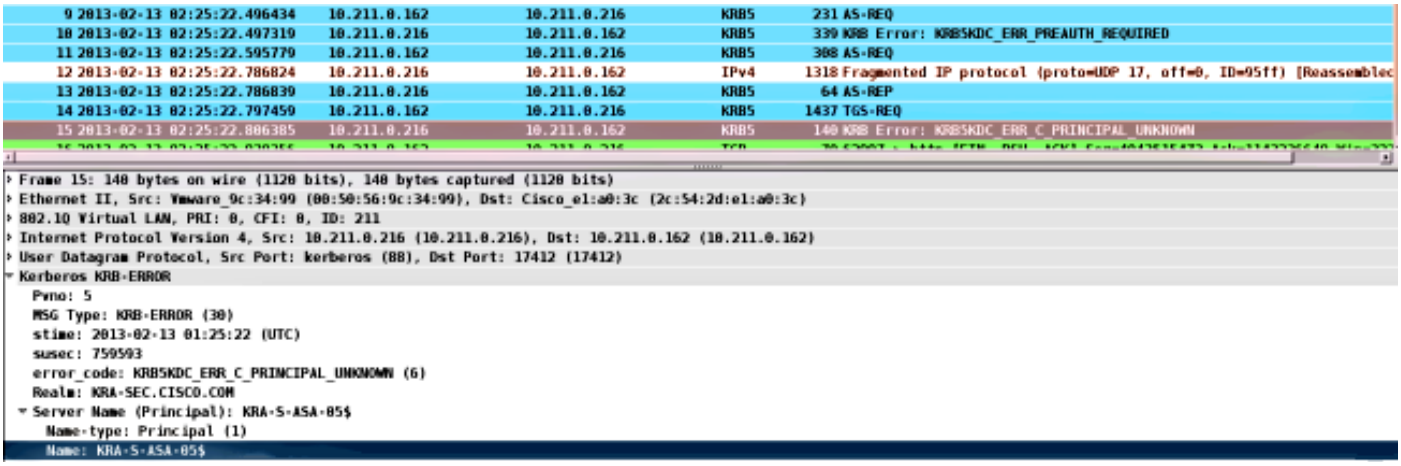


Asegúrese de que el SPN esté registrado sólo para una cuenta (script del artículo anterior). Cuando recibe este error, **KRB_AP_ERR_MODIFIED**, generalmente significa que el **SPN** no está

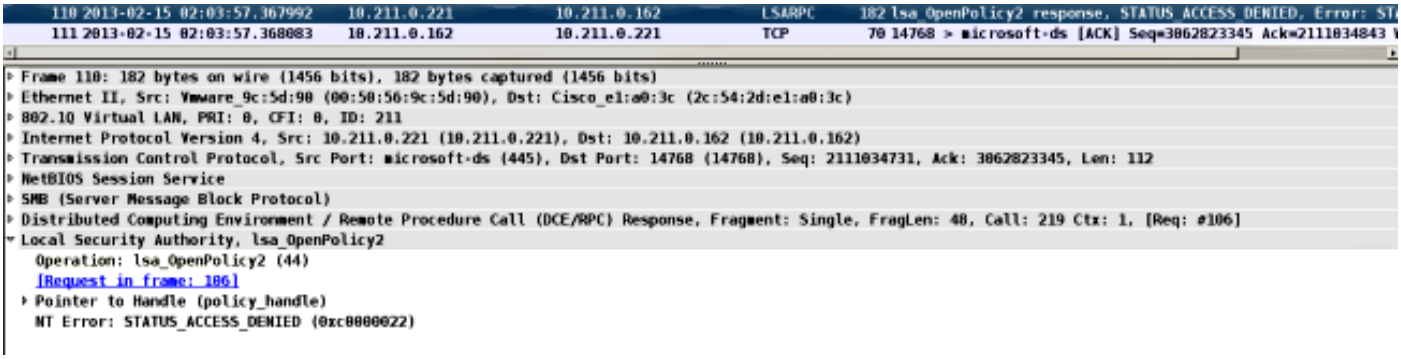
registrado para la cuenta correcta. Se debe registrar para la cuenta que se utiliza para ejecutar la aplicación (conjunto de aplicaciones en IIS).



Cuando recibe este error, **KRB_ERR_C_PRINCIPAL_UNKNOWN**, significa que no hay ningún usuario en el DC (usuario WebVPN: **cisco**).



Es posible que encuentre este problema cuando se una al dominio. El ASA recibe **AS-REP**, pero falla en el **nivel LSA** con el error: **STATUS_ACCESS_DENIED**:



Para solucionar este problema, debe habilitar/inhabilitar la autenticación previa en el DC para ese usuario (**Administrador**).

Estos son algunos otros problemas con los que podría encontrar:

- Puede haber problemas cuando se une al dominio. Si el servidor DC tiene varios adaptadores de controlador de interfaz de red (NIC) (varias direcciones IP), asegúrese de que el ASA pueda acceder a todos ellos para unirse al dominio (elegido aleatoriamente por el cliente según la respuesta de servidor de nombres de dominio (DNS)).

- No configure **SPN** como **HOST/dc.kra-sec.cisco.com** para la cuenta **Administrator**. Es posible perder la conectividad con el DC debido a esa configuración.

- Después de que ASA se una al dominio, es posible verificar que la cuenta de computadora correcta se crea en el DC (nombre de host ASA). Asegúrese de que el usuario tenga los permisos correctos para agregar cuentas de equipo (en este ejemplo, el **administrador** tiene los permisos correctos).

- Recuerde la correcta configuración del **protocolo de tiempo de red (NTP)** en el ASA. De forma predeterminada, el DC acepta un desplazamiento del reloj de cinco minutos. Ese temporizador se puede cambiar en el DC.

- Verifique la conectividad Kerberos para el paquete pequeño **UDP/88** se utiliza. Después del error del DC, **KRB5KDC_ERR_RESPONSE_TOO_BIG**, el cliente cambia a **TCP/88**. Es posible forzar al cliente de Windows a utilizar **TCP/88**, pero **ASA utilizará UDP de forma predeterminada**.

- DC: cuando realice cambios en la política, recuerde **gpupdate /force**.

- ASA: prueba la autenticación con el comando **test aaa**, pero recuerde que es sólo una autenticación simple.

- Para resolver problemas en el sitio DC, es útil habilitar depuraciones Kerberos: Cómo habilitar el registro de eventos Kerberos.

ID de bug de Cisco

Esta es una lista de ID de bug relevantes de Cisco:

- ID de bug Cisco CSCsi32224 : ASA no cambia a TCP después de recibir el código de error Kerberos 52
- Id. de bug Cisco CSCtd92673 - La autenticación Kerberos falla con la autenticación previa habilitada
- El ID de bug Cisco CSCuj19601 - ASA Webvpn KCD - intenta unirse a AD solamente después del reinicio
- Id. de bug Cisco CSCuh32106 - ASA KCD se rompe en 8.4.5 en adelante

Información Relacionada

- Acerca de la delegación restringida Kerberos
- Cómo funciona KCD
- PIX/ASA: Ejemplo de Configuración de Grupos de Servidores de Autenticación Kerberos y

Autorización LDAP para Usuarios de Cliente VPN a través de ASDM/CLI

- Referencia de Comandos de Cisco ASA Series
- KDC_ERR_BADOPTION cuando intenta restringir la delegación
- Cómo obligar a Kerberos a utilizar TCP en lugar de UDP en Windows
- Soporte Técnico y Documentación - Cisco Systems