WebVPN SO-integratie met beperkt doordat Kerberos het Configuratievoorbeeld van een delegatie hanteert

Inhoud

Inleiding

Dit document beschrijft hoe u WebexVPN Single Sign On (SSO) kunt configureren en oplossen voor toepassingen die door Kerberos worden beschermd.

Voorwaarden

Vereisten

Cisco raadt u aan basiskennis van deze onderwerpen te hebben:

- Cisco adaptieve security applicatie (ASA) CLI-configuratie en Secure Socket Layer (SSL) VPN-configuratie

- Kerberos-services

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Cisco ASA-software, versie 9.0 en hoger
- Microsoft Windows 7-client
- Microsoft Windows 2003-server en later

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.

Achtergrondinformatie

Kerberos is een protocol voor netwerkverificatie dat netwerkentiteiten in staat stelt om op veilige wijze aan elkaar authentiek te verklaren. Het maakt gebruik van een vertrouwde derde, het Key Distribution Center (KDC), die tickets verstrekt aan de netwerkentiteiten. Deze tickets worden door de entiteiten gebruikt om de toegang tot de gevraagde dienst te verifiëren en te bevestigen.

Het is mogelijk om WebVPN SSO te configureren voor toepassingen die door Kerberos worden beschermd met de Cisco ASA optie Kerberos Beperkte Delegatie (KCD) genaamd. Met deze optie kan de ASA Kerberos-tickets aanvragen namens de WebVPN-poortgebruiker, terwijl hij toegang heeft tot toepassingen die door Kerberos worden beschermd.

Wanneer u zulke toepassingen via het WebVPN-portaal opzoekt, hoeft u geen aanmeldingsgegevens meer te verstrekken. in plaats daarvan wordt de account gebruikt die u in het WebVPN-portaal wilt loggen.

Raadpleeg het gedeelte Understanding How KCD Works van de ASA configuratie gids voor meer informatie.

Interactie van Kerberos met de ASA

Voor WebVPN moet de ASA kaartjes in naam van de gebruiker aanvragen (omdat de gebruiker van het portaal WebVPN slechts toegang tot het portaal heeft, niet de dienst Kerberos). Daartoe maakt de ASA gebruik van Kerberos-uitbreidingen voor beperkte delegatie. Hier is de stroom:

1. De ASA doet mee aan het domein en verkrijgt een ticket (Ticket1) voor een computeraccount met aanmeldingsgegevens ingesteld op ASA (**kcd-server** opdracht). Dit ticket wordt in de volgende stappen gebruikt voor de toegang tot Kerberos-diensten.

2. De gebruiker klikt op de WebVPN poortlink voor de door Kerberos beschermde toepassing.

3. De ASA vraagt (**TGS-REQ**) een ticket naar de computerrekening met zijn hostname als aangever. Dit verzoek omvat het veld **PA-TGS-REQ** met **PA-FOR-USER** met de naam van

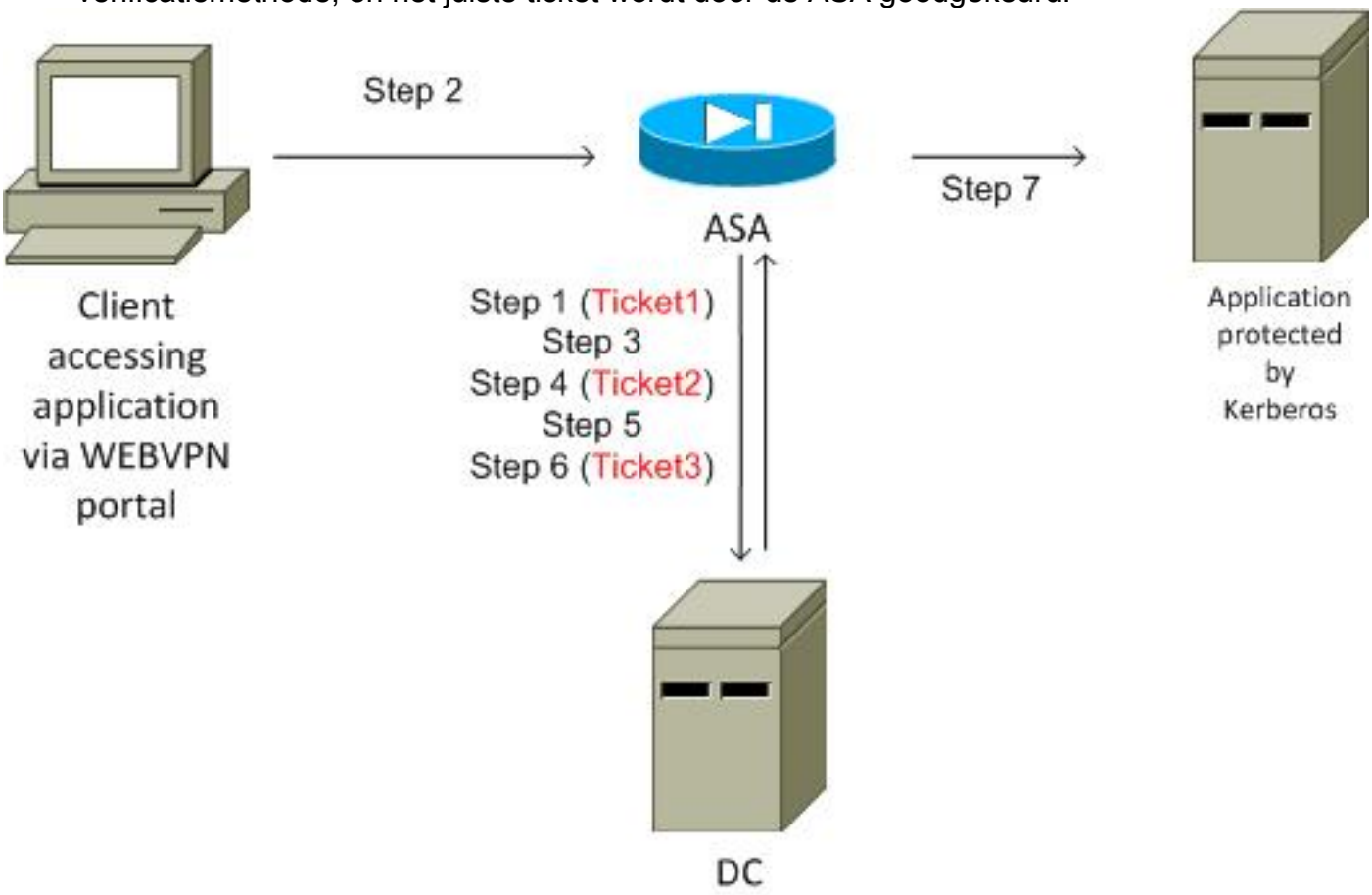
de gebruikersnaam voor het WebVPN-portal, **cisco** in dit scenario. Het ticket voor de Kerberos-service uit stap 1 wordt gebruikt voor de echtheidscontrole (correcte delegatie).

4. Als antwoord hierop ontvangt de ASA een gepersonaliseerd ticket (Ticket2) namens de WebVPN-gebruiker (**TGS_REP**) voor de computeraccount. Dit ticket wordt gebruikt om toepassingskaartjes te vragen namens deze WebVPN-gebruiker.

5. De ASA initieert een ander verzoek (**TGS_REQ**) om het kaartje voor de toepassing te verkrijgen (**HTTP/test.kra-sec.cisco.com**). Dit verzoek gebruikt opnieuw het veld **PA-TGS-REQ**, dit keer **zonder het** veld **PA-FOR-USER**, maar met het gepersonaliseerde ticket dat in Stap 4 wordt ontvangen.

6. De reactie (**TGS_REQ**) op de aanvraag met het toegangsbewijs (Ticket3) wordt teruggegeven.

7. Dit ticket wordt op transparante wijze gebruikt door de ASA om toegang te krijgen tot de beschermde service. De WebVPN-gebruiker hoeft geen aanmeldingsgegevens in te voeren. Voor de HTTP-toepassing wordt het Simple and Protected GSS-API onderhandelingsmechanisme (SPNEGO) gebruikt om te onderhandelen over de verificatiemethode, en het juiste ticket wordt door de ASA goedgekeurd.



Configureren

Topologie

Domain: kra-sec.cisco.com (10.211.0.221 of 10.211.0.216)

Op de toepassing Internet Information Services (IS) 7: test.kra-sec.cisco.com (10.21.0.223)

Domain Controller (DC): dc.kra-sec.cisco.com (10.211.0.221 of 10.211.0.216) - Windows2008

ASA: 10.211.0.162

Gebruikersnaam/wachtwoord voor Webex VPN: Cisco/cisco

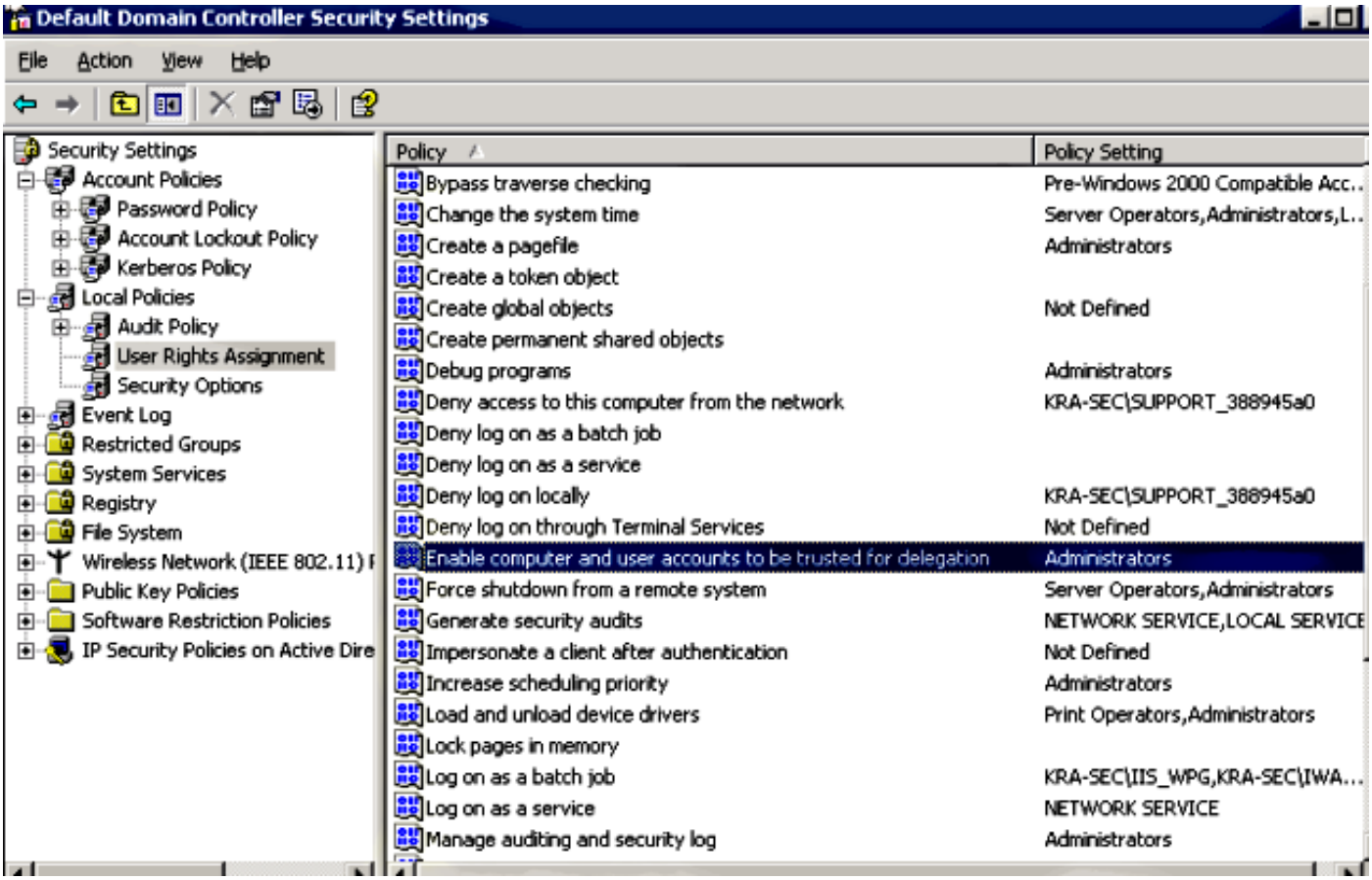
Bijgevoegd bestand: asa-seed.pcap (succesvol doen aan het domein)

Bijgevoegd bestand: asa-kerberos-bad.pcap (verzoek om service)

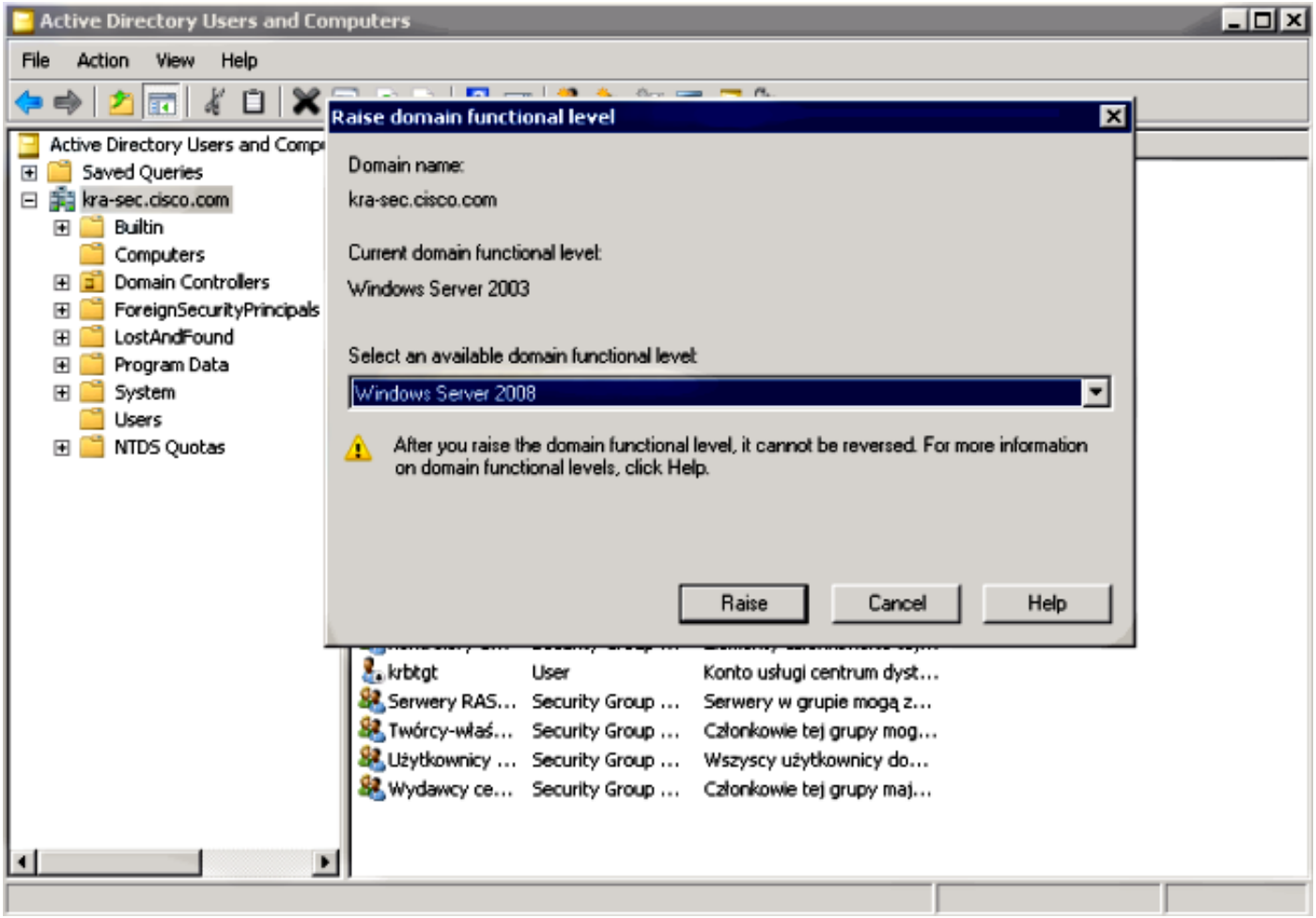
Domain Controller- en toepassingsconfiguratie

Domain Settings

Er wordt aangenomen dat er al een functionele IS7-toepassing is die door Kerberos wordt beschermd (indien niet, lees de sectie Voorwaarden). U moet de instellingen voor de delegaties van de gebruikers controleren:



Zorg ervoor dat het functionele domeinniveau is verhoogd naar Windows Server 2003 (ten minste). De standaardinstelling is Windows Server 2000:



Instellen van de hoofdnaam van de service (SPN)

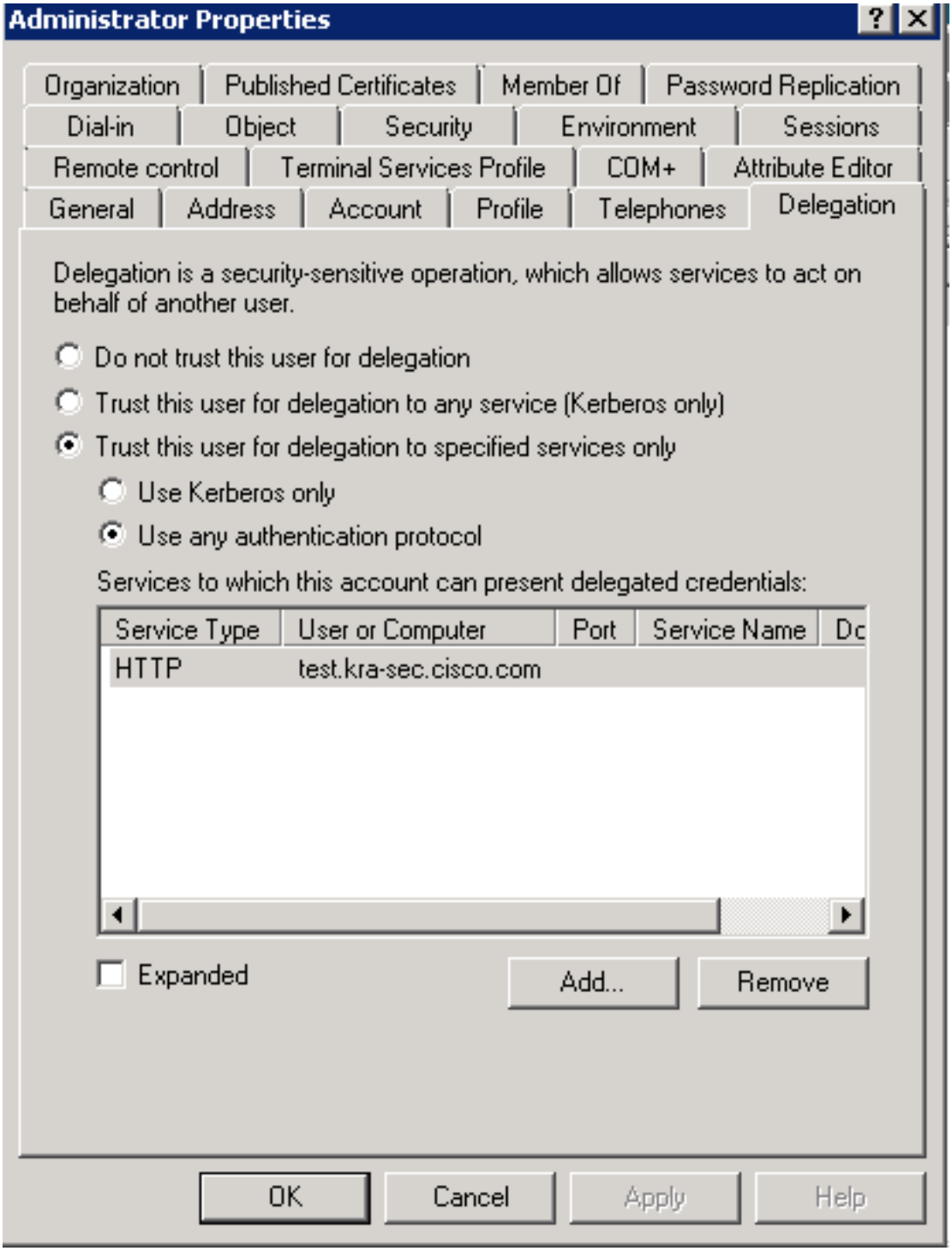
U moet alle rekeningen op de AD met de juiste delegatie configureren. Er wordt een Administrator-account gebruikt. Wanneer de ASA die rekening gebruikt, kan zij een ticket aanvragen namens een andere gebruiker (beperkte delegatie) voor de specifieke dienst (HTTP-toepassing). Om dit mogelijk te maken, moet de juiste delegatie voor de aanvraag/dienst worden ingesteld.

Om deze delegatie via het CLI te kunnen maken met het **setspn.exe**, dat een onderdeel is van de Windows Server 2003 Service Pack 1 Support Tools, voert u deze opdracht in:

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

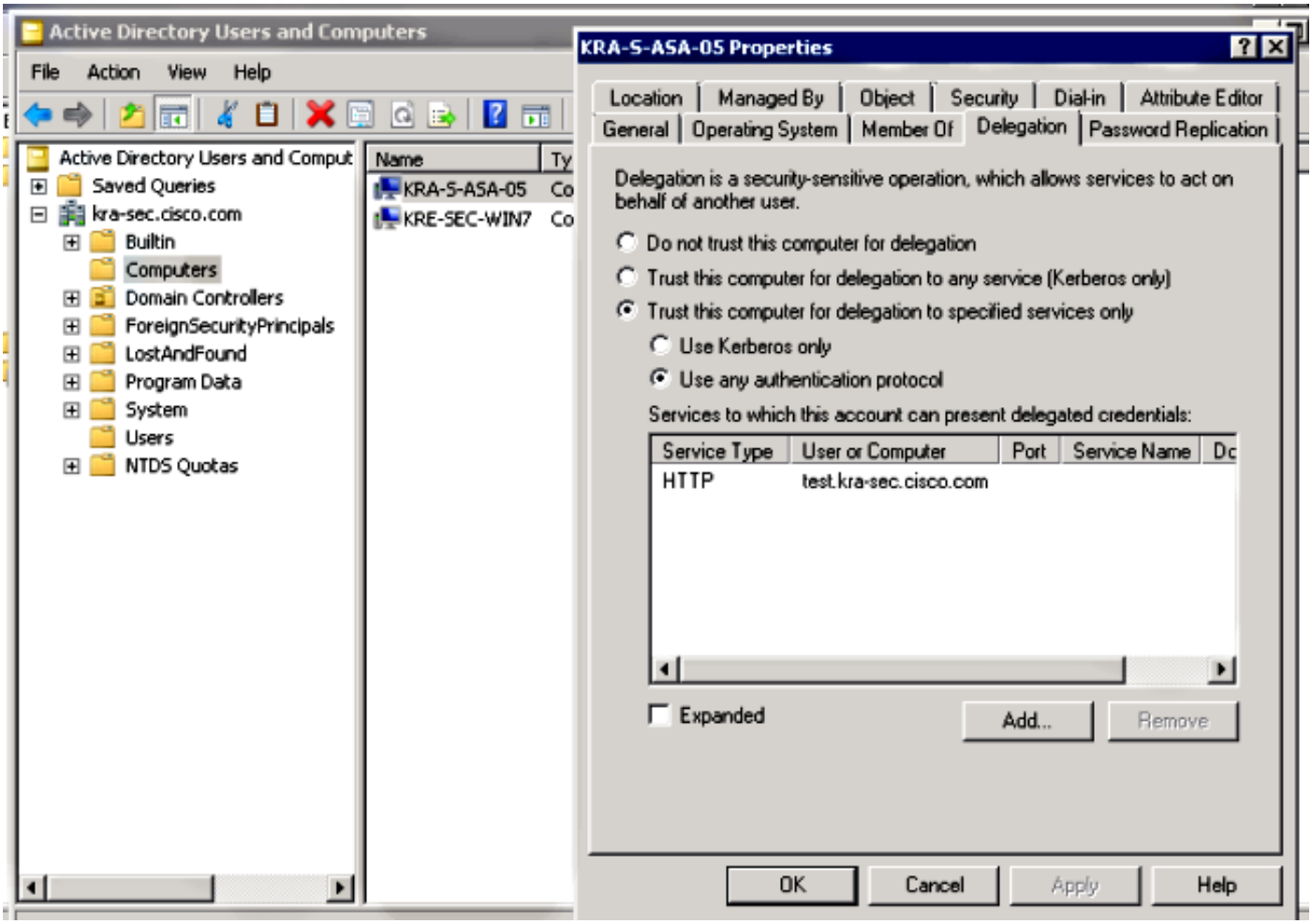
Dit geeft aan dat de gebruikersnaam voor de **beheerder** de betrouwbare account is voor de delegatie van de HTTP-service op **test.kra-sec.cisco.com**.

De **SPN**-opdracht is ook nodig om het tabblad **Delegatie** voor deze gebruiker te activeren. Zodra u de opdracht hebt ingevoerd, verschijnt het tabblad Delegatie voor de beheerder. Het is belangrijk om "elk authentificatieprotocol te gebruiken" omdat "uitsluitend Kerberos gebruiken" de uitbreiding van de beperkte delegatie niet ondersteunt.



Op het **tabblad General** is het ook mogelijk de Kerberos-voorverificatie uit te schakelen. Dit wordt echter niet aangeraden, omdat deze functie wordt gebruikt om de DC te beschermen tegen aanvallen met wederspelen. De ASA kan correct werken met pre-authenticatie.

Deze procedure is ook van toepassing met delegatie voor de computerrekening (de ASA wordt als computer in het domein gebracht om een "vertrouwensrelatie" tot stand te brengen):



Configuratie van de 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
```

Verifiëren

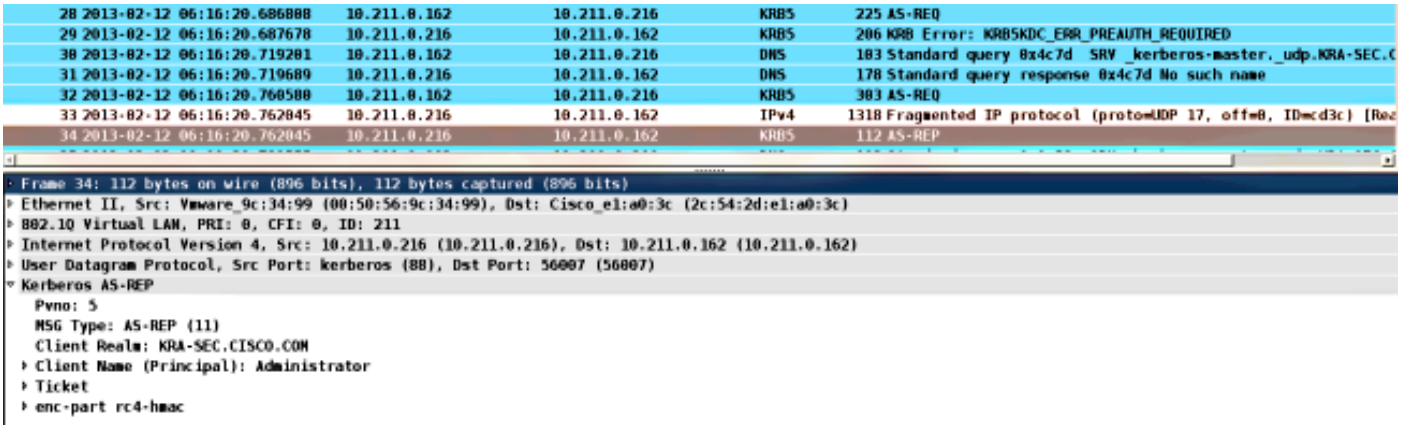
ASA treedt toe tot het domein

Nadat de opdracht **kcd-server** is gebruikt, probeert de ASA zich aan te sluiten bij het domein:

```
********** 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
```

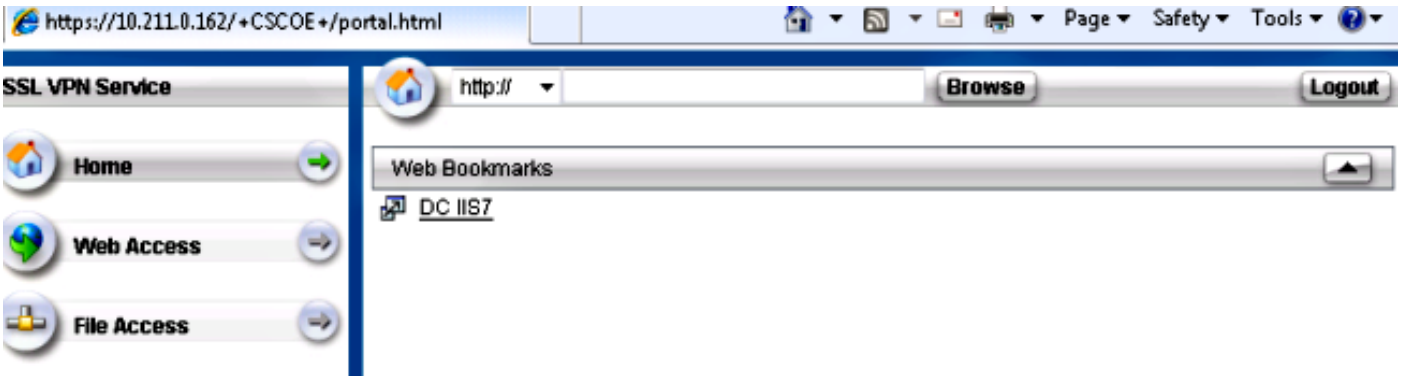
```
Kerberos: Server Name krbtgt
Kerberos: Start time 0
Kerberos: End time -878667256
Kerberos: Renew until time -878672192
Kerberos: Nonce 0xa9db408e
Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type des-cbc-md5
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4
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
```

De ASA kan zich met succes bij het domein aansluiten. Na de juiste echtheidscontrole ontvangt de ASA een ticket voor de aangever: Administrator in **AS_REP** pakje (Ticket1 beschreven in Stap 1).



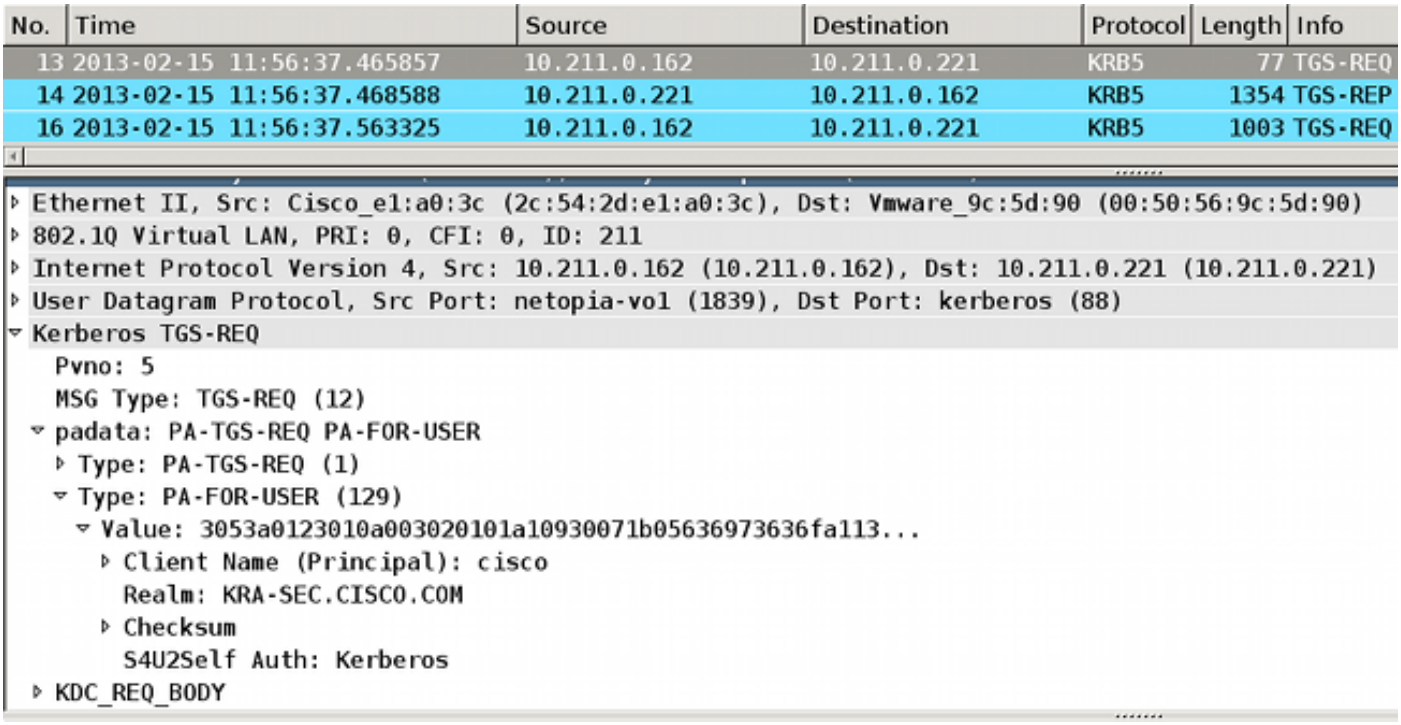
Aanvraag van de dienst

De gebruiker klikt op de link WebVPN:



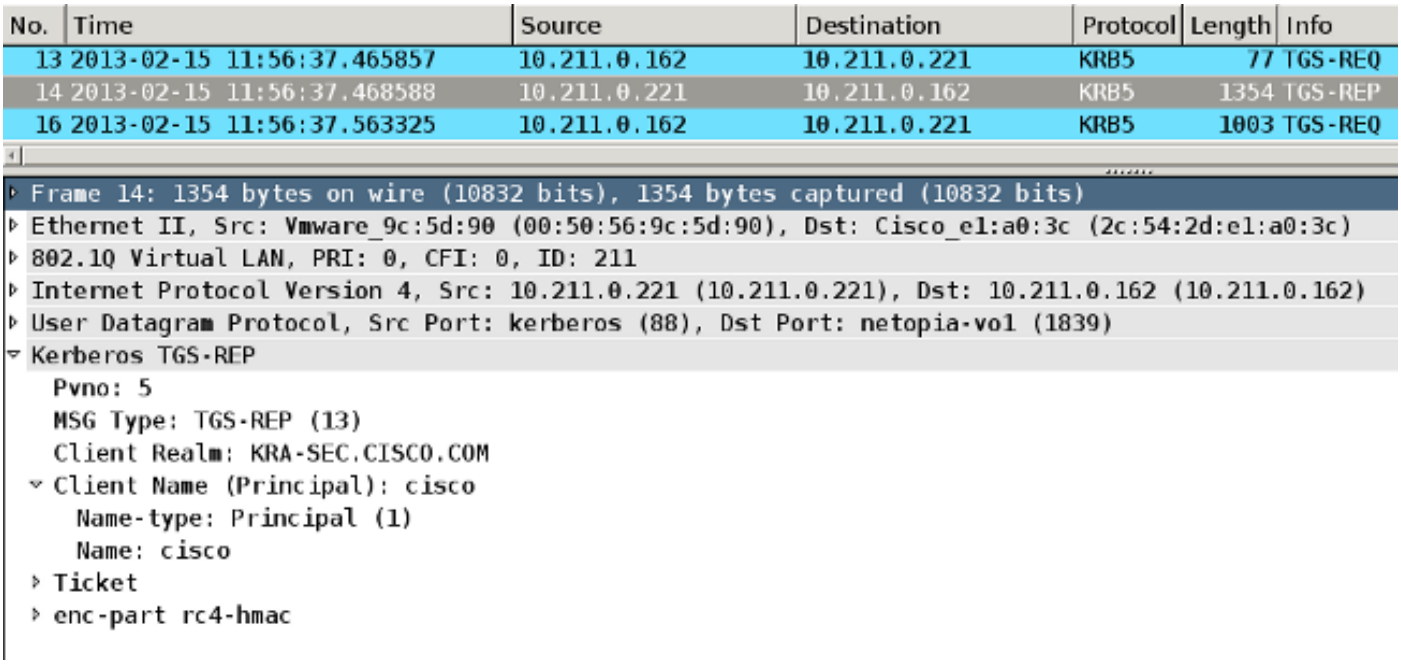
De ASA verstuurt de **TGS_REQ** voor een toegangsbewijs met het ticket dat in het **AS_REP**-pakket

wordt ontvangen:



> **Opmerking:** De **PA-FOR-USER** waarde is **cisco** (WebVPN-gebruiker). **PA-TGS-REQ** bevat het ticket dat wordt ontvangen voor het Kerberos Service- verzoek (de ASA hostname is de opdrachtgever).

De ASA krijgt een juiste reactie met het gepersonaliseerde ticket voor **Cisco**-gebruiker (Ticket2 beschreven in Stap 4):



Hier is het verzoek om het ticket voor de HTTP-service (sommige defecten zijn weggelaten voor de duidelijkheid):

```
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 ticket**s.
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
```

De ASA ontvangt het juiste gepersonaliseerde ticket voor de HTTP-service (Ticket3 beschreven in Stap 6).

Beide tickets kunnen worden geverifieerd. Het eerste is het gepersonaliseerde ticket voor de gebruiker **cisco**, dat wordt gebruikt om het tweede ticket te vragen en te ontvangen voor de HTTP-service die benaderd wordt:

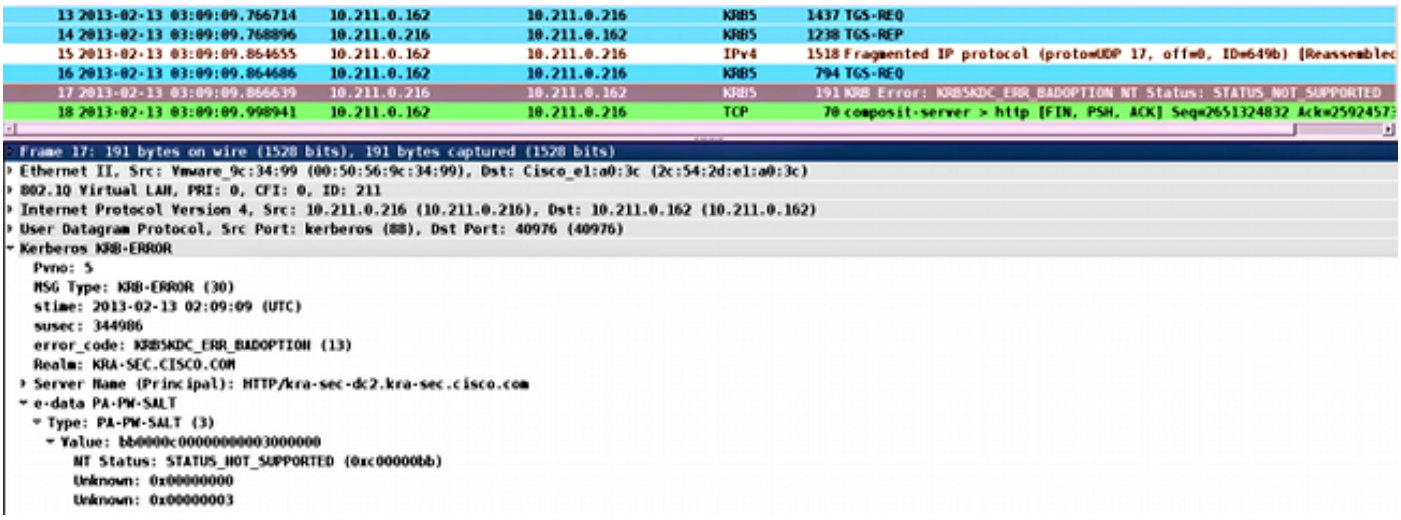
```
KRA-S-ASA-05(config)# show aaa kerberos
Default Principal: cisco@KRA-SEC.CISCO.COM
Valid Starting       Expires              Service Principal
19:38:10 CEST Oct 2 2013 05:37:33 CEST Oct 3 2013 KRA-S-ASA-05@KRA-SEC.CISCO.COM

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
```

Dit HTTP-ticket (Ticket3) wordt gebruikt voor HTTP-toegang (met SPNEGO) en de gebruiker hoeft geen aanmeldingsgegevens te leveren.

Problemen oplossen

Soms krijgt u te maken met een probleem van onjuiste delegatie. ASA gebruikt bijvoorbeeld een ticket om de service **HTTP/test.kra-sec.cisco.com** aan te vragen (stap 5), maar de reactie is **KRB-FOUT** met **ERR_BADOPTION**:



Dit is een typisch probleem dat zich voordoet wanneer de delegatie niet correct is ingesteld. De ASA meldt dat **"KDC niet kan voldoen aan de gevraagde optie"**:

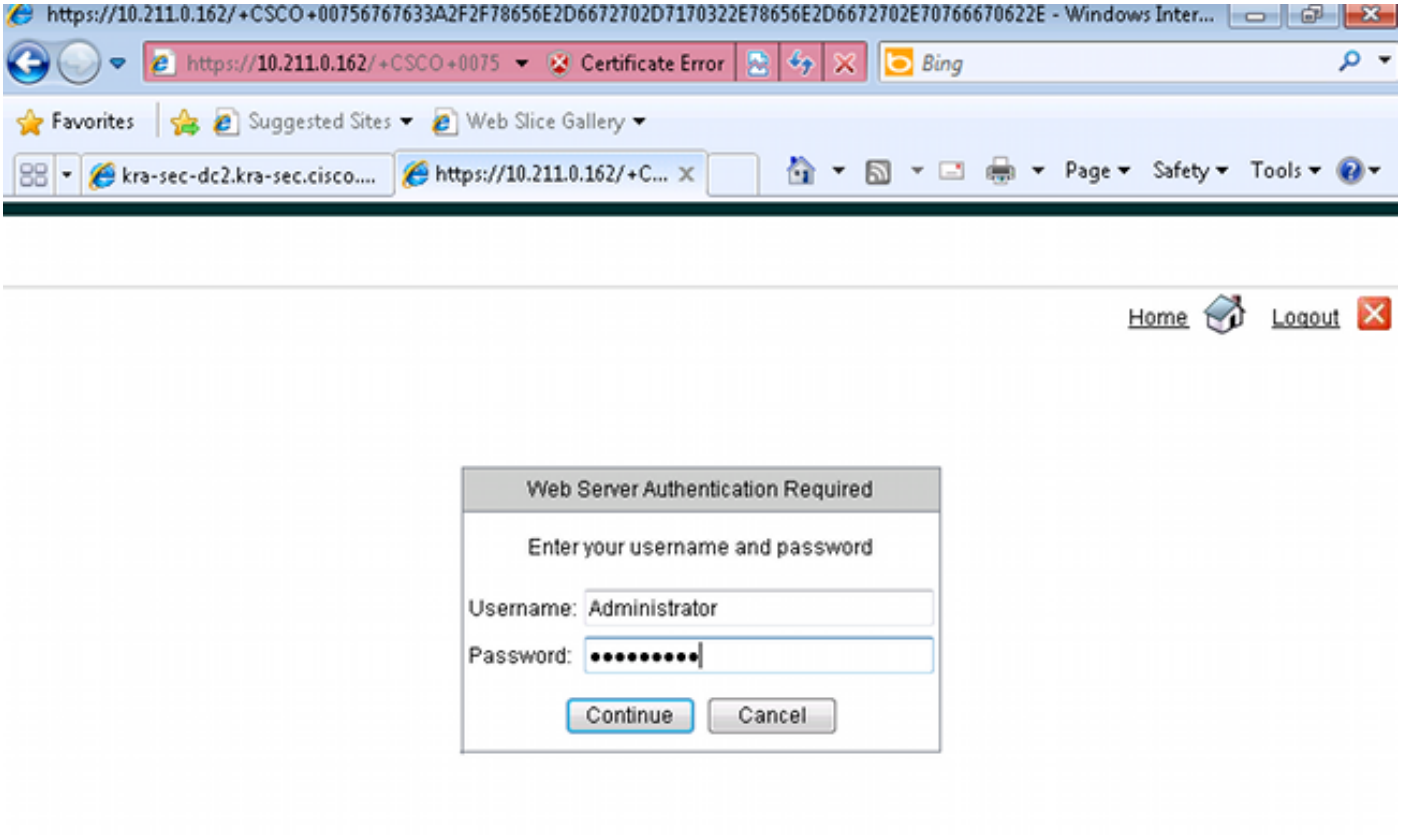
```
KRA-S-ASA-05# ucte_krb_get_auth_cred(): ctx = 0xcc4b5390,
WebVPN_session = 0xc919a260, protocol = 1
find_spn_in_url(): URL - /
build_host_spn(): host - test.kra-sec.cisco.com
build_host_spn(): SPN - HTTP/test.kra-sec.cisco.com
KCD_unicorn_get_cred(): Attempting to retrieve required KCD tickets.
In 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

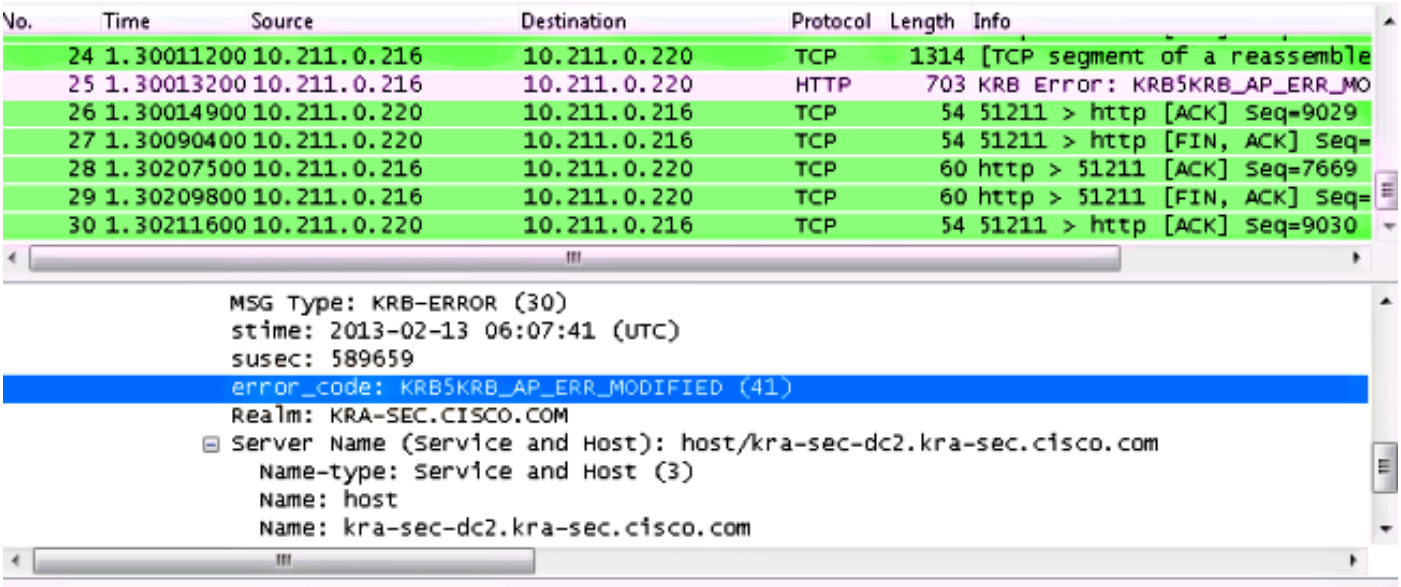
```
Kerberos: Option forwardable
Kerberos: Option renewable
Kerberos: Client Realm KRA-SEC.CISCO.COM
Kerberos: Server Name HTTP
Kerberos: Start time 0
Kerberos: End time -856104568
Kerberos: Renew until time 0
Kerberos: Nonce 0xf84c9385
Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type 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
```

Dit is in principe hetzelfde probleem dat wordt beschreven in de opnames. De mislukking is **bij TGS_REQ met BAD_OPTION**.

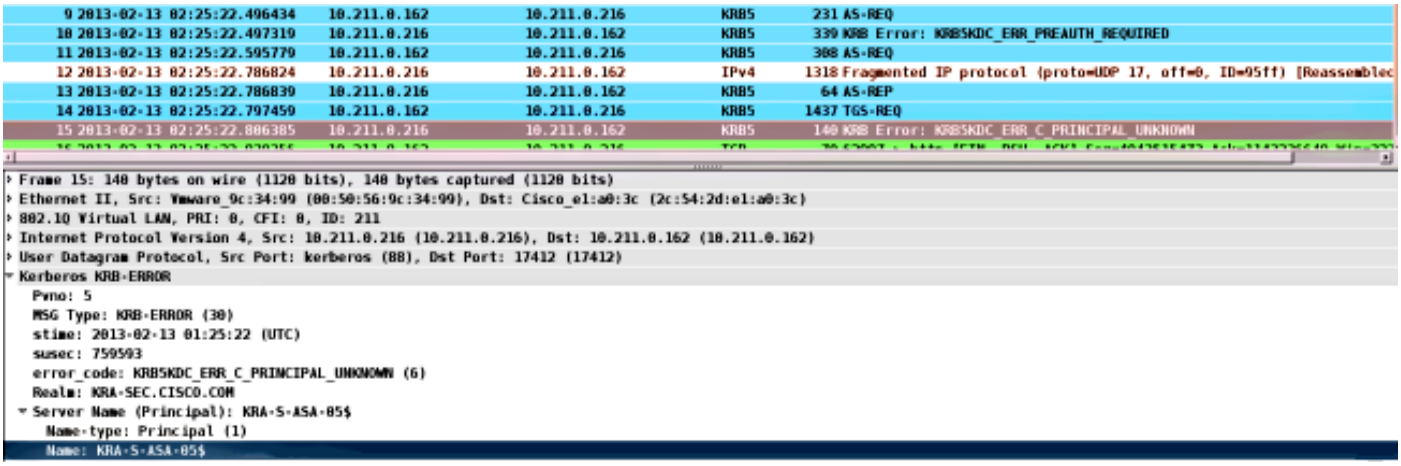
Als de reactie **Succes** is, dan ontvangt ASA een kaartje voor de **HTTP/test.kra-sec.cisco.com** dienst, die voor **SPNEGO** onderhandeling wordt gebruikt. Maar vanwege deze fout is er onderhandeld over de **NT LAN Manager (NTLM)** en de gebruiker moet aanmeldingsgegevens verstrekken:



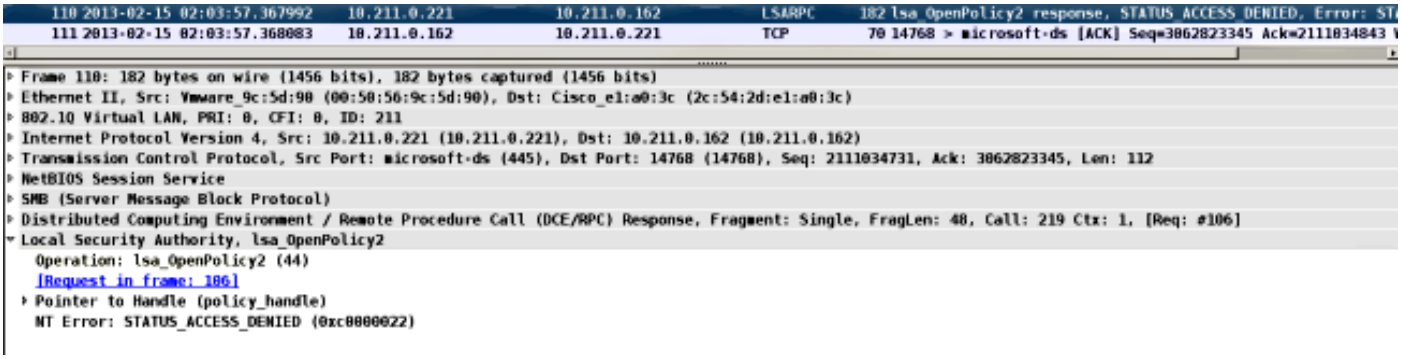
Zorg ervoor dat de SPN slechts voor één account is geregistreerd (script uit vorig artikel). Wanneer u deze fout ontvangt, betekent **KRB_AP_ERR_MODIFIED**, dat gewoonlijk dat de **SPN** niet geregistreerd is voor de juiste account. Het moet worden geregistreerd voor de rekening die wordt gebruikt om de toepassing te kunnen uitvoeren (applicatie op IS).



Wanneer u deze fout ontvangt, **betekent KRB_ERR_C_PRINCIPAL_UNKNOWN**, dat er geen gebruiker op de DC is (WebVPN-gebruiker: **cisco**).



U zou dit probleem kunnen tegenkomen wanneer u zich bij het domein aansluit. ASA ontvangt **AS-REP**, maar faalt op **LSA** niveau met de fout: **STATUS_ACCESS_DENIED**:



Om dit probleem op te lossen, moet u pre-verificatie op de DC voor die gebruiker (**beheerder**) inschakelen/uitschakelen.

Hier zijn een paar andere problemen die u zou kunnen tegenkomen:

- Er kunnen problemen zijn als je je bij het domein aansluit. Als de DC-server meerdere Network Interface Controller-adapters (NIC) heeft (meerdere IP-adressen), zorg er dan voor dat de ASA toegang heeft tot alle adapters om zich aan te sluiten bij het domein (willekeurig gekozen door de client op basis van de DNS-respons (Domain Name Server)).

- Stel **SPN** niet in als de **HOST/dc.kra-sec.cisco.com** voor de **Administrator-**account. Het is mogelijk om verbinding met de DC te verliezen vanwege die instelling.

- Nadat de ASA zich bij het domein aansluit, is het mogelijk om te verifiëren dat de correcte computeraccount op de DC (ASA hostname) wordt gecreëerd. Zorg ervoor dat de gebruiker de juiste rechten heeft om computerrekeningen toe te voegen (in dit voorbeeld heeft de **beheerder** de juiste rechten).

- Onthoud de juiste **NTP-**configuratie **(Network Time Protocol)** op de ASA. Standaard accepteert de DC een klokscheefheid van vijf minuten. Die timer kan op de DC worden gewijzigd.

- Controleer de connectiviteit van Kerberos voor het kleine pakket **UDP/88** wordt gebruikt. Na de fout van de DC, **KRB5KDC_ERR_RESPONSE_TOO_BIG**, de switches van de client naar **TCP/88**. Het is mogelijk om de Windows client te dwingen **TCP/88** te gebruiken, maar **ASA zal**

UDP standaard gebruiken.

- DC: als je beleid verandert , vergeet dan **gpupdate / force** .
- ASA: verificatie met de **test aaa** opdracht, maar vergeet niet dat het slechts een eenvoudige echtheidscontrole is.
- Om een probleemoplossing op de DC-site te voorkomen, is het handig om Kerberos-debugs in te schakelen: Hoe kunt u Kerberos-eventvastlegging inschakelen.

Cisco-id's voor bugs

Hier is een lijst met relevante Cisco bug-ID's:

- Cisco bug-ID CSCsi3224 - ASA switch niet op TCP na ontvangst van Kerberos-foutcode 52
- Cisco bug-ID CSCtd92673 - Kerberos-verificatie mislukt met pre-auth-enabled
- Cisco bug-ID CSCuj19601 - ASA WebVPN KCD - die alleen na het herstarten van de SOFTWARE probeert verbinding te maken met AD
- Cisco bug-ID CSC32106 - ASA KCD is kapot vanaf 8.4.5

Gerelateerde informatie

- Over beperkte delegatie van Kerberos
- Het begrijpen van hoe KCD werkt
- PIX/ASA : Groepen van Kerberos-verificatie en LDAP-licentieservers voor VPN-clientgebruikers via het configuratievoorbeeld ASDM/CLI
- Cisco ASA Series handleiding
- KDC_ERR_BADOPTION bij pogingen tot beperkte delegatie
- Hoe Kerberos te dwingen TCP in plaats van UDP in Windows te gebruiken
- Technische ondersteuning en documentatie – Cisco Systems