Konfigurieren Sie die AnyConnect LDAP-Zuordnung auf Firepower Threat Defense (FTD).

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Konfiguration im FTD Überprüfen Fehlerbehebung

Einführung

Dieses Dokument enthält ein Konfigurationsbeispiel für die LDAP-Zuordnung (Lightweight Directory Access Protocol) für AnyConnect-Benutzer in FirePOWER Threat Defense (FTD) mithilfe einer FirePOWER Management Center (FMC)-FlexConfig-Richtlinie. Diese Konfiguration ermöglicht bestimmten Benutzern, die einer Active Directory-Gruppe (AD) angehören, eine VPN-Verbindung (Virtual Private Network) einzurichten. Benutzer aus verschiedenen AD-Gruppen, die nicht auf der Karte definiert sind, können sich nicht mit demselben Profil verbinden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse zu folgenden Themen verfügen:

- AD-Bereichskonfiguration auf FMC
- Windows Active Directory
- AnyConnect (SSLVPN)-Konfiguration auf FMC
- Grundkenntnisse der FlexConfig-Objekte auf FMC

Verwendete Komponenten

- FirePower Manager Center (FMC), Version 6.2.3 und 6.5.0
- FirePower Threat Defense (FTD), Version 6.2.3 und 6.5.0
- Windows Server mit Active Directory

Konfigurieren

Konfiguration im FTD

In diesem Beispiel verwenden Benutzer, die zu AD Group1 gehören, eine Tunnel-All-Konfiguration, und Benutzer, die zu AD Group2 gehören, haben eingeschränkten Zugriff auf bestimmte Hosts. Alle anderen Benutzer, die nicht zu diesen Gruppen gehören, können nicht authentifiziert werden.

Schritt 1: Konfigurieren Sie AnyConnect mithilfe der LDAP-Authentifizierung, und stellen Sie die Änderungen bereit. Ein Beispiel finden Sie in <u>diesem Leitfaden</u>.

Schritt 2: Navigieren Sie zu Geräte > Remotezugriff > AnyConnect-Richtlinie bearbeiten > Erweitert > Gruppenrichtlinien.

Schritt 3: Erstellen Sie drei verschiedene Gruppenrichtlinien:

• Gruppe1 mit Split Tunneling-Konfiguration auf **Zulassen des gesamten Datenverkehrs über Tunnel**.

escription:	e:*	Group1				
General AnyConnect Advanced PN Protocols IPv4 Split Tunneling: Allow all traffic over tunnel Address Pools anner IPv6 Split Tunneling: Allow all traffic over tunnel NS/WINS Split Tunnel Network List Type: Standard Access List: Standard Access List: plit Tunneling Standard Access List: Split Split DNS Request Split Tunneling DNS Requests: Send DNS requests as per split tunnel policy Domain List: Its: Send DNS requests as per split tunnel policy	ription:					
PN Protocols IPv4 Split Tunneling: Allow all traffic over tunnel Address Pools IPv6 Split Tunneling: Allow all traffic over tunnel IPv6 Split Tunnel Network List Type: Standard Access List: Standard Access List: Dilt Tunneling Standard Access List: Split DNS Request Split Tunneling DNS Requests: Send DNS requests as per split tunnel policy Domain List: Image: Standard Access List: Send DNS requests as per split tunnel policy	aneral AnyC	Connect	Advanced			
Address Pools IPv6 Split Tunneling: Allow all traffic over tunnel NS/WINS Split Tunnel Network List Type: Standard Access List: Split Dit Tunneling Standard Access List: Split Split DNS Request Split Tunneling DNS Requests: Send DNS requests as per split tunnel policy Domain List: Interference Send DNS requests as per split tunnel policy	Protocols		IPv4 Split Tunneling:	Allow all traffic over tunnel	*	
NS/WINS Split Tunnel Network List Type: Standard Access List Cextended Access Standard Access List: Split DNS Request Split Tunneling DNS Requests: Send DNS requests as per split tunnel policy Domain List:	adress Pools ner		IPv6 Split Tunneling:	Allow all traffic over tunnel	*	
olit Tunneling Standard Access List: Split DNS Request Split Tunneling DNS Requests: Send DNS requests as per split tunnel policy Domain List: Image: Comparing the second	/WINS		Split Tunnel Network List Type:	Standard Access List O Extended Access L	ist	
DNS Request Split Tunneling DNS Requests: Domain List:	t Tunneling		Standard Access List:	Split	~	
DNS Requests: Send DNS requests as per split tunnel policy Domain List:			DNS Request Split Tunneling			
Domain List:			DNS Requests:	Send DNS requests as per split tunnel policy	~	
			Domain List:			

• Gruppe2 mit Split Tunneling-Konfiguration auf Split.

Edit Group Policy

Name:*	Group2				
Description:					
General	AnyConnect	Advanced			
VPN Protoco	bls	IPv4 Split Tunneling:	Tunnel networks specified below	~	
IP Address F Banner	Pools	IPv6 Split Tunneling:	Allow all traffic over tunnel	~	
DNS/WINS		Split Tunnel Network List Type:	Standard Access List Extended Access L	ist	
Split Tunnel	ing	Standard Access List:	Split	~	0
		DNS Request Split Tunneling DNS Requests: Domain List:	Send DNS requests as per split tunnel policy	*	
			Save	Ca	ncel

• NOACCESS-Gruppe für Benutzer, die keiner der vorherigen Gruppen angehören. Das Feld **Simultane Anmeldung pro Benutzer** muss auf 0 gesetzt sein.

Edit Group Policy			? ×
Name:* NOACC	ESS		
Description:			
General AnyConnect	Advanced		
Traffic Filter	Access Hours:		✓ ②
Session Settings	Simultaneous Login Per User:	0	(Range 0-2147483647)
	Connection Time		
	Max Connection Time:		Minutes (Range 1-4473924)
	Alert Interval:	1	Minutes (Range 1-30)
	Idle Time		
	Idle Timeout:	30	Minutes (Range 1-35791394)
	Alert Interval:	1	Minutes (Range 1-30)
			Save Cancel

Schritt 4: Weisen Sie dem Verbindungsprofil die NOACCESS-Gruppenrichtlinie zu.

Edit Connection Profile

Connection Profile:"	AnyConnec	t	
Group Policy:*	NOACCESS Edit Group P	olicy 🖉	
Client Address Assign	ment A/	A Aliases	
IP Address for the remot 'Client Address Assignme	te clients can ent Policy' in	be assigned from local IP Address pools/DHCP Servers/AAA Servers. C the Advanced tab to define the assignment criteria.	onfigure the
Address Pools:			0-
Name		IP Address Range	
SSL		10.10.10.1-10.10.10.10	a 🖉 🖬
DHCP Servers:			Ø
Name		DHCP Server IP Address	
Ocnfigure device overri	ides in the add	ress pool object to avoid IP address conflicts in case of object is shared acros	s multiple devices
		Save	Cancel

Schritt 5: Navigieren Sie zu Objekt > Objektmanagement > FlexConfig > FlexConfig Object > Add FlexConfig Object.

Schritt 6: Fügen Sie die erforderlichen memberOf-Werte hinzu, die für die LDAP-Attributzuordnungskonfiguration erforderlich sind. Um die Gruppen-DN vom Server abzurufen, können Sie den Befehl "dsquery samid-group <group-name>" verwenden.

Die Bereitstellung muss als einmal festgelegt werden und als Prepend eingeben.

Tipp: Attributnamen und -werte sind Groß- und Kleinschreibung untergeordnet. Wenn die Zuordnung nicht ordnungsgemäß erfolgt, stellen Sie sicher, dass in der LDAP-Attributzuordnung die richtige Schreibweise und Groß- und Kleinschreibung für die Namen und Werte der Cisco und LDAP-Attribute verwendet wurde.

dit FlexConfig	g Object						? >
Name:	LDAPattributeMAP						
Description:							
🛆 Copy-pastin	g any rich text might introdu	ce line breaks while ge	enerating CLI. Please verif	y the CLI before deployme	int.		
🔾 Insert 🔹	1×				Deployment:	Once ᅌ	Type: Prepend ᅌ
map-value map-value	e <u>memberOf</u> "CN=g1 e <u>memberOf</u> "CN=g1	roup1, <u>CN</u> =User roup2, <u>CN</u> =User	s,DC= <u>cisco</u> ,DC=c s,DC= <u>cisco</u> ,DC=c	com" Group1 com" Group2			
Variables		Dimension	Default Value	Property (Typ.	Override	Description	
		Chickson	No records t	o display			
						- Fa	Capital

Schritt 7: Andere erstellen FlexConfig-Objekt mit dem Namen AAAserverLDAPmapping. Dieses Objekt fügt die Attributzuordnung der AAA-Serverkonfiguration zu.

Die Bereitstellungswerte müssen als *Everytime* festgelegt werden und als *Append* eingeben.

Add FlexConfig Object

Name:	AAAserverLDAPmapping						
Description:							
🛆 Copy-pasting	any rich text might introduce	line breaks while ge	enerating CLI. Please verif	y the CLI before deploym	ent.		
🔾 Insert 🔹	e X				Deployment:	Everytime ᅌ	Type: Append ᅌ
aaa-server ldap-attr	LDAP host 192.16 ibute-map MAP	8.109.29					
Variables							
Name		Dimension	Default Value	Property (Typ	Override	Description	
			No records t	o display			
				/			
						Sa	ve Cancel

Schritt 8: Navigieren Sie zu Geräte > FlexConfig > Edit current FlexConfig. Stellen Sie sicher, dass die Reihenfolge der FlexConfig-Objekte in der FlexConfig-Richtlinie zuerst das LDAP-Attribut Map FlexConfig-Objekt gefolgt vom AAA-Server-Objekt ist.

Schritt 9: Stellen Sie die Konfiguration auf dem Gerät bereit, um diese Konfiguration an das verwaltete Gerät zu senden.

Um einen zusätzlichen Eintrag in der LDAP-Zuordnung hinzuzufügen, ändern Sie das vorhandene FlexConfig LDAPAtributeMAP-Objekt, sodass NUR der neue Zuordnungswert enthalten ist.

Edit FlexConfig Object							
Name:	LDAPattributeMAP						
Description:							
🛆 Copy-pastin	g any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.						
🔾 Insert 🗸		Deployment:	Once ᅌ	Type:	Prepend ᅌ		
<pre>ldap attribute-map MAP map-value memberOf "CN=group3, CN=Users, DC=cisco, DC=com" Group3</pre>							

Überprüfen

Stellen Sie eine Verbindung zur FTD-CLISH her, und geben Sie diese Befehle aus, um sicherzustellen, dass die Benutzer in den definierten Gruppen eine Verbindung herstellen können.

```
> show vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect
```

```
Index : 25
Public IP : 192.168.109.80
           : ciscol
Username
Assigned IP : 10.10.10.1
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
           : AnyConnect Premium
License
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing : AnyCon
Bytes Tx : 15820
           : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
                                   Bytes Rx : 160
Group Policy : Group1
                                   Tunnel Group : AnyConnect
Login Time : 16:02:45 UTC Tue Oct 9 2018
Duration : 0h:00m:38s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                   VLAN : none
Audt Sess ID : 0000000000190005bbcd125
Security Grp : none
                                   Tunnel Zone : 0
```

> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : cisco2 Index : 26 Public IP Assigned IP : 11.11.11.1 : 192.168.109.80 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256 Hashing: AnyConnect-Parent: (1)noneSSL-Tunnel: (1)SHA384DTLS-Tunnel: (1)SHA1Bytes Tx: 15820Bytes Rx: 442 Group Policy : Group2 Tunnel Group : AnyConnect Login Time : 16:04:12 UTC Tue Oct 9 2018 Duration : 0h:00m:14s Inactivity : 0h:00m:00s VLAN Mapping : N/A : none VLAN Audt Sess ID : 00000000001a0005bbcd17c Security Grp : none Tunnel Zone : 0

Fehlerbehebung

Debugger:

Um die LDAP-Transaktion zu überprüfen, können Sie diese Debugbefehle verwenden.

> system support diagnostic-cli
debug ldap 250
debug aaa common 250
Dies sind Beispiele für die erfolgreiche Ausgabe für jeden Debugbefehl.

firepower# debug ldap 250 debug ldap enabled at level 250 firepower# [49] Session Start [49] New request Session, context 0x00002aaad332f100, reqType = Authentication [49] Fiber started [49] Creating LDAP context with uri=ldap://192.168.109.29:389

```
[49] Connect to LDAP server: ldap://192.168.109.29:389, status = Successful
[49] supportedLDAPVersion: value = 3
[49] supportedLDAPVersion: value = 2
[49] LDAP server 192.168.109.29 is Active directory
[49] Binding as AdminFTD
[49] Performing Simple authentication for AdminFTD to 192.168.109.29
[49] LDAP Search:
       Base DN = [DC=cisco,DC=com]
       Filter = [samaccountname=cisco1]
       Scope = [SUBTREE]
[49] User DN = [CN=cisco1, CN=Users, DC=cisco, DC=com]
[49] Talking to Active Directory server 192.168.109.29
[49] Reading password policy for ciscol, dn:CN=ciscol,CN=Users,DC=cisco,DC=com
[49] Read bad password count 1
[49] Binding as ciscol
[49] Performing Simple authentication for ciscol to 192.168.109.29
[49] Processing LDAP response for user ciscol
[49] Message (ciscol):
[49] Authentication successful for ciscol to 192.168.109.29
[49] Retrieved User Attributes:
[49]
      objectClass: value = top
       objectClass: value = person
[49]
[49]
      objectClass: value = organizationalPerson
      objectClass: value = user
[49]
[49]
      cn: value = ciscol
[49]
      givenName: value = ciscol
      distinguishedName: value = CN=cisco1,CN=Users,DC=cisco,DC=com
[49]
[49]
      instanceType: value = 4
[49]
       whenCreated: value = 20181009153032.0Z
[49]
       whenChanged: value = 20181009154032.0Z
[49]
      displayName: value = ciscol
      uSNCreated: value = 856333
[49]
[49] memberOf: value = CN=group1,CN=Users,DC=cisco,DC=com
[49]
               mapped to Group-Policy: value = Group1
               mapped to LDAP-Class: value = Group1
[49]
[49]
      uSNChanged: value = 856372
       name: value = ciscol
[49]
[49]
      objectGUID: value = .K.'..3N....Q...
[49]
      userAccountControl: value = 66048
[49]
      badPwdCount: value = 1
[49]
      codePage: value = 0
       countryCode: value = 0
[49]
      badPasswordTime: value = 131835752510299209
[49]
[49]
       lastLogoff: value = 0
      lastLogon: value = 131835733331105504
[49]
      pwdLastSet: value = 131835726324409149
[49]
[49]
      primaryGroupID: value = 513
[49]
      objectSid: value = .....El.E.G..9..@s...
      adminCount: value = 1
[49]
[49]
       accountExpires: value = 9223372036854775807
[49]
       logonCount: value = 0
      sAMAccountName: value = ciscol
[49]
[49]
      sAMAccountType: value = 805306368
[49]
      userPrincipalName: value = ciscol@cisco.com
[49]
       objectCategory: value = CN=Person, CN=Schema, CN=Configuration, DC=cisco, DC=com
       dSCorePropagationData: value = 20181009153316.0Z
[49]
       dSCorePropagationData: value = 16010101000000.0Z
[49]
       lastLogonTimestamp: value = 131835732321783732
[49]
[49] Fiber exit Tx=551 bytes Rx=2628 bytes, status=1
[49] Session End
```

firepower# debug aaa common 250

debug aaa common enabled at level 250

```
firepower# AAA API: In aaa_open
AAA session opened: handle = 31
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(0x00002b4ad7423b20) received message type 0
[31] AAA FSM: In AAA_StartAAATransaction
[31] AAA FSM: In AAA_InitTransaction
Initiating authentication to primary server (Svr Grp: LDAP-29)
_____
[31] AAA FSM: In AAA_BindServer
[31] AAA_BindServer: Using server: 192.168.109.29
[31] AAA FSM: In AAA_SendMsg
User: ciscol
Resp:
callback_aaa_task: status = 1, msg =
[31] AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 31, pAcb = 0x00002aaad352bc80
AAA task: aaa_process_msg(0x00002b4ad7423b20) received message type 1
[31] AAA FSM: In AAA_ProcSvrResp
Back End response:
_____
Authentication Status: 1 (ACCEPT)
[31] AAA FSM: In AAA_NextFunction
AAA NextFunction: i fsm state = IFSM PRIM AUTHENTICATE, auth status = ACCEPT
AAA_NextFunction: authen svr = LDAP-29, author svr = <none>, user pol = Group1, tunn pol =
NOACCESS
AAA NextFunction: New i fsm state = IFSM USER GRP POLICY,
[31] AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(Group1)
Got server ID 0 for group policy DB
Initiating user group policy lookup (Svr Grp: GROUP_POLICY_DB)
_____
[31] AAA FSM: In AAA_BindServer
[31] AAA_BindServer: Using server: <Internal Server>
[31] AAA FSM: In AAA_SendMsg
User: Group1
Resp:
grp_policy_ioctl(0x00002b4ad31fd460, 114698, 0x00002b4ad7423430)
grp_policy_ioctl: Looking up Group1
callback_aaa_task: status = 1, msg =
[31] AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 31, pAcb = 0x00002aaad352bc80
AAA task: aaa_process_msg(0x00002b4ad7423b20) received message type 1
[31] AAA FSM: In AAA_ProcSvrResp
Back End response:
_____
User Group Policy Status: 1 (ACCEPT)
[31] AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_USER_GRP_POLICY, auth_status = ACCEPT
AAA_NextFunction: New i_fsm_state = IFSM_TUNN_GRP_POLICY,
[31] AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(NOACCESS)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp: GROUP_POLICY_DB)
    _____
[31] AAA FSM: In AAA_BindServer
```

[31] AAA_BindServer: Using server: <Internal Server>

```
[31] AAA FSM: In AAA_SendMsq
User: NOACCESS
Resp:
grp_policy_ioctl(0x00002b4ad31fd460, 114698, 0x00002b4ad7423430)
grp_policy_ioctl: Looking up NOACCESS
callback_aaa_task: status = 1, msg =
[31] AAA FSM: In aaa_backend_callback
aaa backend callback: Handle = 31, pAcb = 0x00002aaad352bc80
AAA task: aaa_process_msg(0x00002b4ad7423b20) received message type 1
[31] AAA FSM: In AAA_ProcSvrResp
Back End response:
_____
Tunnel Group Policy Status: 1 (ACCEPT)
[31] AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY, auth_status = ACCEPT
dACL processing skipped: no ATTR_FILTER_ID found
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
[31] AAA FSM: In AAA_ProcessFinal
Checking simultaneous login restriction (max allowance=3) for user ciscol
Class attribute created from LDAP-Class attribute
[31] AAA FSM: In AAA Callback
user attributes:
 1
     User-Name(1)
                      6 "ciscol"
      User-Password(2) 13 (hidden)
 2
 3
      Group-Policy(4121)
                           6 "Group1"
      AAA-AVP-Table(4243) 1639 "g[06][00][00]$[00][00][00]x[01][00][00][8F][01][00][00]"
 4
 5
      DAP class attribute required(20510)
                                            4
                                                1
 6
      LDAP-Class(20520) 7 "Group1[00]"
User Access-Lists:
user_acl[0] = NULL
user_acl[1] = NULL
user policy attributes:
                                              <--- Group-Policy Configuration (Group1)</pre>
     Filter-Id(11) 8
                            ....
 1
      Session-Timeout(27)
                             4
 2
                                  0
      Idle-Timeout(28) 4 30
 3
      Simultaneous-Logins(4098) 4
 4
                                        3
 5
      Primary-DNS(4101) 4 IP: 0.0.0.0
                            4 IP: 0.0.0.0
 6
      Secondary-DNS(4102)
 7
                           4 IP: 0.0.0.0
      Primary-WINS(4103)
      Secondary-WINS(4104)
                             4 IP: 0.0.0.0
 8
 9
      Tunnelling-Protocol(4107)
                                  4
                                       96
      Banner(4111) 0 0x00002aaad49daa38
10
                                               ** Unresolved Attribute **
      Split-Tunnel-Inclusion-List(4123) 8
                                               ....
11
      Default-Domain-Name(4124) 0 0x00002aaad49daa41 ** Unresolved Attribute **
12
      Secondary-Domain-Name-List(4125) 0 0x00002aaad49daa42 ** Unresolved Attribute
13
* *
14
      Split-Tunneling-Policy(4151)
                                  4
                                           0
       Group-giaddr(4157) 4 IP: 0.0.0.0
15
16
       WebVPN SVC Keepalive interval(4203) 4
                                                20
17
       WebVPN SVC Client DPD period(4204)
                                           4 30
18
      WebVPN SVC Gateway DPD period(4205)
                                           4
                                                30
19
       WebVPN SVC Rekey period(4206)
                                    4
                                           0
       WebVPN SVC Rekey method(4207)
                                      4
20
                                           0
                                    4
       WebVPN SVC Compression(4208)
 21
                                          0
       WebVPN SVC Firewall Rule(4211)
                                      17
                                          "public#,private#,"
 22
 23
       WebVPN SVC DTLS Compression(4213)
                                          4
                                             0
 24
      WebVPN SVC DTLS enable(4219) 4
                                         1
 25
      WebVPN SVC MTU(4221) 4 1406
      CVC-Modules(4223) 4 "dart"
 26
      CVC-Profile(4224) 11 "FTD03#user,"
 27
      CVC-Ask(4227) 4 2
 28
```

```
29
     CVC-Ask-Timeout(4228) 4
                            0
     VLAN ID(4236) 4
30
                        0
31
     WebVPN Idle timeout alert interval(4244)
                                       4 1
     WebVPN Session timeout alert interval(4245) 4 1
32
33
     List of address pools to assign addresses from(4313) 3
                                                     "SSL"
     SVC ignore DF bit(4326) 4 0
34
35
     Configure the behaviour of DNS queries by the client when Split tunneling is
enabled(4328) 4 0
                         Primary-IPv6-DNS(4329)
36
Client Bypass Protocol(4331) 4 0
    IPv6-Split-Tunneling-Policy(4332) 4
                                       0
39
User Policy Access-Lists:
user_acl[0] = NULL
user_acl[1] = NULL
tunnel policy attributes:
                                                <--- Default Group-Policy
attributes (NOACCESS)
                       ....
 1 Filter-Id(11) 8
 2
     Session-Timeout(27)
                       4
                            0
    Idle-Timeout(28) 4 30
 3
    Simultaneous-Logins(4098) 4
 4
                                 0
 5
    Primary-DNS(4101) 4 IP: 0.0.0.0
 6
    Secondary-DNS(4102)
                       4 IP: 0.0.0.0
 7
    Primary-WINS(4103)
                       4 IP: 0.0.0.0
    Secondary-WINS(4104) 4 IP: 0.0.0.0
 8
 9
     Tunnelling-Protocol(4107)
                            4
                                96
     Banner(4111) 0 0x00002aaad2580328 ** Unresolved Attribute **
10
                       8 "NOACCESS"
11
     Group-Policy(4121)
12
     Split-Tunnel-Inclusion-List(4123) 8
                                       .....
     Default-Domain-Name(4124) 0 0x00002aaad2580331 ** Unresolved Attribute **
13
     Secondary-Domain-Name-List(4125) 0 0x00002aaad2580332 ** Unresolved Attribute
14
* *
15
     Split-Tunneling-Policy(4151)
                               4 0
     Group-giaddr(4157) 4 IP: 0.0.0.0
16
17
     WebVPN SVC Keepalive interval(4203) 4
                                         20
     WebVPN SVC Client DPD period(4204)
18
                                    4
                                        30
19
     WebVPN SVC Gateway DPD period(4205)
                                    4
                                        30
20
     WebVPN SVC Rekey period(4206) 4
                                    0
21
     WebVPN SVC Rekey method(4207)
                                4 0
                               4 0
22
     WebVPN SVC Compression(4208)
     WebVPN SVC Firewall Rule(4211)
                               17 "public#,private#,"
23
                                   4
     WebVPN SVC DTLS Compression(4213)
24
                                      0
25
     WebVPN SVC DTLS enable(4219) 4
                                    1
26
     WebVPN SVC MTU(4221) 4 1406
     CVC-Modules(4223) 4 "dart"
CVC-Profile(4224) 11 "FTD03#user,"
27
28
     CVC-Ask(4227) 4 2
29
     CVC-Ask-Timeout(4228)
                        4 0
30
     VLAN ID(4236) 4 0
31
     WebVPN Idle timeout alert interval(4244)
32
                                         4
33
     WebVPN Session timeout alert interval(4245) 4 1
34
     SVC ignore DF bit(4326) 4 0
35
     Configure the behaviour of DNS queries by the client when Split tunneling is
enabled(4328) 4 0
   Primary-IPv6-DNS(4329)
                         36
Client Bypass Protocol(4331) 4 0
39
   IPv6-Split-Tunneling-Policy(4332) 4
                                       0
Tunnel Policy Access-Lists:
user_acl[0] = NULL
user_acl[1] = NULL
```

Auth Status = ACCEPT
aaai_internal_cb: handle is 31, pAcb is 0x00002aaad352bc80, pAcb->tq.tqh_first is
0x000000000000
AAA API: In aaa_close
Checking simultaneous login restriction (max allowance=3) for user ciscol
AAA task: aaa_process_msg(0x00002b4ad7423b20) received message type 2
In aaai_close_session (31)
AAA API: In aaa_send_acct_start