ASA IPsec- und IKE-Debugs (IKEv1 Aggressive Mode) Fehlerbehebung - Technische Hinweise

Inhalt

Einführung

In diesem Dokument werden die Debugging auf der Cisco Adaptive Security Appliance (ASA) beschrieben, wenn sowohl aggressiver Modus als auch Pre-Shared Key (PSK) verwendet werden. Die Übersetzung bestimmter Debugzeilen in die Konfiguration wird ebenfalls behandelt. Cisco empfiehlt, über grundlegende Kenntnisse in den Bereichen IPsec und Internet Key Exchange (IKE) zu verfügen.

In diesem Dokument wird der weitergeleitete Datenverkehr nach der Einrichtung des Tunnels nicht behandelt.

Kernproblem

IKE- und IPsec-Debuggen sind manchmal kryptisch, aber Sie können sie verwenden, um Probleme bei der Einrichtung von IPsec-VPN-Tunneln zu verstehen.

Szenario

Der aggressive Modus wird in der Regel für Easy VPN (EzVPN) mit Software- (Cisco VPN-Client) und Hardware-Clients (Cisco ASA 5505 Adaptive Security Appliance oder Cisco IOS) verwendet? Software-Router), jedoch nur bei Verwendung eines vorinstallierten Schlüssels. Im Gegensatz zum Hauptmodus besteht der aggressive Modus aus drei Nachrichten.

Die Debug-Software stammt von einer ASA, die die Softwareversion 8.3.2 ausführt und als

EzVPN-Server fungiert. Der EzVPN-Client ist ein Software-Client.

Verwendete Debug-Befehle

Dies sind die in diesem Dokument verwendeten Debugbefehle:

```
debug crypto isakmp 127
debug crypto ipsec 127
```

ASA-Konfiguration

Die ASA-Konfiguration in diesem Beispiel ist ausschließlich auf grundlegende Anforderungen ausgelegt. Es werden keine externen Server verwendet.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.48.67.14 255.255.254.0

crypto ipsec transform-set TRA esp-aes esp-sha-hmac

crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000

crypto dynamic-map DYN 10 set transform-set TRA
crypto dynamic-map DYN 10 set reverse-route

crypto map MAP 65000 ipsec-isakmp dynamic DYN
crypto map MAP interface outside
crypto isakmp enable outside

crypto isakmp policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
lifetime 86400

username cisco password  cisco
username cisco attributes
vpn-framed-ip-address 192.168.1.100 255.255.255.0

tunnel-group EZ type remote-access
tunnel-group EZ general-attributes
 default-group-policy EZ
tunnel-group EZ ipsec-attributes
 pre-shared-key *****

group-policy EZ internal
group-policy EZ attributes
 password-storage enable
 dns-server value 192.168.1.99
 vpn-tunnel-protocol ikev1
 split-tunnel-policy tunnelall
 split-tunnel-network-list value split
 default-domain value jyoungta-labdomain.cisco.com
```

Debuggen

Hinweis: Weitere Informationen zu Debug-Befehlen vor der Verwendung von **Debug-**Befehlen finden Sie unter Wichtige Informationen.

Beschreibung der Servernachricht	Debugger		C
	49711:28:30.28908/24/12Sev=Info/6IKE/0x630003B Verbindungsversuch mit 64.102.156.88. 49811:28:30.29708/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_INITIALEvent: EV_INITIATOR 49911:28:30.29708/24/12Sev=Info/4IKE/0x6300001 Beginn der IKE Phase 1-Verhandlung 50011:28:30.29708/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Veranstaltung: EV_GEN_DHKEY 50111:28:30.30408/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Veranstaltung: EV_BLD_MSG 50211:28:30.30408/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Veranstaltung: EV_START_RETRY_TMR 50311:28:30.30408/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Veranstaltung: EV_SND_MSG		D ge D - - vo U ar - - -
	50411:28:30.30408/24/12Sev=Info/4IKE/0x6300013 SENDEN >>> ISAKMP OAK AG (SA, KE, NON, ID, VID(Xauth), VID(dpd), VID(Frag), VID(Nat-T), VID(Unity)) an 64.102.156,88		A
	<================ Aggressive Nachricht 1 (AM1) ================		
Empfangen von AM1 vom Client	24. August 11:31:03 [IKEv1]IP = 64.102.156.87, EMPFANGENE IKE_DECODE-Nachricht (msgid=0) mit Payloads: HDR + SA (1) + KE (4) + NEIN (10) + ID (5) + ANBIETER (13) + ANBIETER (13) + ANBIETER (13) + ANBIETER (13) + ANBIETER (13) + KEINE (0) Gesamtlänge: 849	50611:28:30.3308/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=00000000000000000CurState: AM_WAIT_MSG2Veranstaltung: EV_NO_EVENT	W S
Prozess AM1. Vergleichen Sie	24. Aug. 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87,		

empfangene Angebote und Transformationen mit bereits für Übereinstimmungen konfigurierten Angeboten.
Relevante Konfiguration:
ISAKMP ist auf der Schnittstelle aktiviert, und es wird mindestens eine Richtlinie definiert, die dem entspricht, was der Client gesendet hat:
 	
`crypto isakmp enable outside`
`crypto isakmp policy 10`
`authentication pre-share`
`encryption aes`
`hash sha`
`group 2`
`lifetime 86400`
Tunnelgruppe, die mit dem vorhandenen Identitätsnamen übereinstimmt:
 	
`tunnel-group EZ type remote-access`
`tunnel-group EZ general-attributes`
`default-group-policy EZ`
`tunnel-group EZ ipsec-attributes`
`pre-shared-key cisco`
	Verarbeitung SA-Payload
	24. August 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Verarbeitung der ke-Payload
	24. August 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Verarbeitung der ISA_KE-Payload
	24. August 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Verarbeitung einmaliger Nutzlast
	24. Aug. 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Processing ID Payload
	24. August 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Verarbeitung der VID-Nutzlast
	24. Aug. 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, VID "xauth v6" empfangen
	24. August 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Verarbeitung der VID-Nutzlast
	24. August 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, empfangene DPD-VID
	24. August 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Verarbeitung der VID-Nutzlast
	24. August 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, empfangene Fragmentierungs-VID
	24. August 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, IKE-Peer enthielt IKE-Fragmentierungsfähigkeitsflags: Hauptmodus:TrueAggressive-Modus:False
	24. August 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Verarbeitung der VID-Nutzlast
	24. Aug. 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, NAT-Traversal ver 02 VID erhalten
	24. August 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Verarbeitung der VID-Nutzlast
	24. Aug. 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, empfangene Cisco Unity Client-VID
	24. Aug. 11:31:03 [IKEv1]IP = 64.102.156.87, Verbindung landete auf tunnel_group ipsec
	24. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung IKE SA-Payload
	24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht übereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd: Gruppe 2Cfg'd: Gruppe 5
	24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht übereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd: Gruppe 2Cfg'd: Gruppe 5
	24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht übereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd: Gruppe 2Cfg'd: Gruppe 5
	24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht übereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd: Gruppe 2Cfg'd: Gruppe 5
	24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht übereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd: Gruppe 2Cfg'd: Gruppe 5
	24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht übereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd:	

	Gruppe 2Cfg'd: Gruppe 5 24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht übereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd: Gruppe 2Cfg'd: Gruppe 5 24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht übereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd: Gruppe 2Cfg'd: Gruppe 5 24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht übereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd: Gruppe 2Cfg'd: Gruppe 5 24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht übereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd: Gruppe 2Cfg'd: Gruppe 5 24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht übereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd: Gruppe 2Cfg'd: Gruppe 5 24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht übereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd: Gruppe 2Cfg'd: Gruppe 5 24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht übereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd: Gruppe 2Cfg'd: Gruppe 5 24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht übereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd: Gruppe 2Cfg'd: Gruppe 5 24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht übereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd: Gruppe 2Cfg'd: Gruppe 5 24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht übereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd: Gruppe 2Cfg'd: Gruppe 5 24. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, IKE SA-Vorschlag Nr. 1, Umwandeln Nr. 5 (annehmbar) stimmt mit globalem IKE-Eintrag Nr. 1 überein	
AM2 erstellen Dieser Prozess umfasst: - gewählte Richtlinien Diffie-Hellman (DH) - Responder-ID - Autor - Network Address Translation (NAT)-Erkennungs-Payload	24. Aug. 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Erstellen der ISAKMP SA-Payload 24. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Erstellen von ke-Payload 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Erstellen von einmaliger Nutzlast 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Erstellen von Schlüsseln für Responder.. 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Erstellen der ID-Nutzlast 24. August 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Erstellen von Hash-Payload 24. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Computing-Hash für ISAKMP 24. Aug. 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Erstellen der Cisco Unity VID-Payload 24. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Erstellen der Xauth V6 VID-Nutzlast 24. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP =	

	64.102.156.87, Erstellen der dpd-VID-Payload 24. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Erstellen der NAT-Traversal VID ver 02-Payload 24. Aug. 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Erstellen der NAT-Discovery-Payload 24. Aug. 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. Aug. 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Erstellen der NAT-Discovery-Payload 24. Aug. 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. Aug. 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Erstellen von Fragmentierung VID + Payload mit erweiterten Funktionen 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Erstellen der VID-Payload 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Altiga/Cisco VPN3000 senden/Cisco ASA GW-VID	
AM2 senden.	24. August 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE-SENDING-Nachricht (msgid=0) mit Payloads: HDR + SA (1) + KE (4) + NEIN (10) + ID (5) + HASH (8) + ANBIETER (13) + ANBIETER (13) + ANBIETER (13) + ANBIETER (13) + NAT-D (130) + NAT-D (130) + ANBIETER (1) 3) + ANBIETER (13) + KEINE (0) Gesamtlänge: 444	
	========== Aggressive Nachricht 2 (AM2) ==========>	
	50711:28:30.40208/24/12Sev=Info/5IKE/0x630002F Empfangenes ISAKMP-Paket: peer = 64.102.156.8 50811:28:30.40308/24/12Sev=Info/4IKE/0x6300014 EMPFANG << ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID(Unity), VID(Xauth), VID(dpd), VID(Nat-T), NAT-D, NAT-D, VID(Frag), VID(?)) ab 64.102.156 88 51011:28:30.41208/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Veranstaltung: EV_RCVD_MSG	A
	5111:28:30.41208/24/12Sev=Info/5IKE/0x6300001 Peer ist ein Cisco Unity-konformer Peer 51211:28:30.41208/24/12Sev=Info/5IKE/0x6300001 Peer unterstützt XAUTH 51311:28:30.41208/24/12Sev=Info/5IKE/0x6300001 Peer unterstützt DPD 51411:28:30.41208/24/12Sev=Info/5IKE/0x6300001 Peer unterstützt NAT-T 51511:28:30.41208/24/12Sev=Info/5IKE/0x6300001 Peer unterstützt IKE-Fragmentierungs-Payloads 51611:28:30.41208/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Veranstaltung: EV_GEN_SKEYID 51711:28:30.42208/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5	P

	R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Veranstaltung: EV_AUTHENTICATE_PEER 51811:28:30.42208/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Veranstaltung: EV_ADJUST_PORT 51911:28:30.42208/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Veranstaltung: EV_CRYPTO_ACTIVE	
	52011:28:30.42208/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_SND_MSG3Ereignis: EV_BLD_MSG 52111:28:30.42208/24/12Sev=Debug/8IKE/0x6300001 IOS-Anbieter-ID-Aufbau gestartet 52211:28:30.42208/24/12Sev=Info/6IKE/0x6300001 IOS-Anbieter-ID-Aufbau erfolgreich	A be Z di D
	52311:28:30.42308/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_SND_MSG3Ereignis: EV_SND_MSG 52411:28:30.42308/24/12Sev=Info/4IKE/0x6300013 SENDEN >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT, NAT-D, NAT-D, VID(?), VID(Unity)) an 64.102.156.88	A
	<================ Aggressive Nachricht 3 (AM3) ================	
Empfangen von AM3 vom Client.	24. August 11:31:03 [IKEv1]IP = 64.102.156.87, EMPFANGENE IKE_DECODE-Nachricht (msgid=0) mit Payloads: HDR + HASH (8) + NOTIFY (11) + NAT-D (130) + NAT-D (130) + ANBIETER (13) + ANBIETER (13) + KEINE (0) Gesamtlänge: 168	
Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu starten.	24. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung von Hash-Payload 24. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Computing-Hash für ISAKMP 24. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung der Benachrichtigungs-Payload 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung der NAT-Discovery-Payload 24. Aug. 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung der NAT-Discovery-Payload 24. Aug. 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung von VID-Payload 24. August 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Processing IOS/PIX Vendor ID Payload (Version: 1.0.0, Funktionen: 00000408) 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung von VID-Payload	

	24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, empfangener Cisco Unity Client-VID 24. Aug. 11:31:03 [IKEv1]Group = ipsec, IP = 64.102.156.87, Automatische NAT-Erkennung Status:Remote EndISBehind a NAT deviceDieses Endgerät befindet sich NICHT hinter einem NAT-Gerät	
Initiieren Sie Phase 1.5 (XAUTH), und fordern Sie Benutzeranmeldeinformationen an.	24. Aug. 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Erstellen einer leeren Hash-Payload 24. Aug. 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Erstellen von qm-Hash-Payload 24. August 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE-SENDING-Nachricht (msgid=fb709d4d) mit Payloads: HDR + HASH (8) + ATTR (14) + KEINE (0) Gesamtlänge: 72	
	========== XAuth - Anfrage für Anmeldedaten ==========>	
	53511:28:30.43008/24/12Sev=Info/4IKE/0x6300014 EMPFANG << ISAKMP OAK TRANS *(HASH, ATTR) ab 64.102.156.88 53611:28:30.43108/24/12Sev=Decode/11IKE/0x6300001 ISAKMP-Header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Nächste Payload: Hash Ver. (Hex):10 Exchange-Typ: Transaktion Flags:(Verschlüsselung) MessageID(Hex):FB709D4D Länge: 76 Payload-Hash Nächste Payload: Attribute Reserviert: 00 Payload-Länge: 24 Daten (in Hex): C779D5CBC5C75E3576C478A15A7CAB8A83A232D0 Payload-Attribute Nächste Payload: Keine Reserviert: 00 Payload-Länge: 20 Typ: ISAKMP_CFG_REQUEST Reserviert: 00 Kennung: 0000 XAUTH-Typ: Allgemein XAUTH-Benutzername: (leer) XAUTH-Benutzerkennwort: (leer) 53711:28:30.43108/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_INITIALEvent: EV_RCVD_MSG	A er ze B
	53811:28:30.43108/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_PCS_XAUTH_REQEvent: EV_INIT_XAUTH 53911:28:30.43108/24/12 Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_PCS_XAUTH_REQEvent: EV_START_RETRY_TMR	In In Ti B de au

	54011:28:30.43208/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_NO_EVENT 541 11:28:36.41508/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_RCVD_USER_INPUT	au
	54211:28:36.41508/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_SND_MSG 54311:28:36.41508/24/12Sev=Info/4IKE/0x6300013 SENDEN >>> ISAKMP OAK TRANS *(HASH, ATTR) bis 64.102.156.88 54411:28:36.41508/24/12Sev=Decode/11IKE/0x6300001 ISAKMP-Header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Nächste Payload: Hash Ver. (Hex):10 Exchange-Typ: Transaktion Flags:(Verschlüsselung) MessageID(Hex):FB709D4D Länge: 85 Payload-Hash Nächste Payload: Attribute Reserviert: 00 Payload-Länge: 24 Daten (in Hex): 1A3645155BE9A81CB80FCDB5F7F24E03FF8239F5 Payload-Attribute Nächste Payload: Keine Reserviert: 00 Payload-Länge: 33 Typ: ISAKMP_CFG_REPLY Reserviert: 00 Kennung: 0000 XAUTH-Typ: Allgemein XAUTH-Benutzername: (Daten werden nicht angezeigt) XAUTH-Benutzerkennwort: (Daten werden nicht angezeigt)	W en B ar N au B A de (v
	<========== Xauth - Benutzeranmeldedaten ==========	
Empfangen von Benutzeranmeldeinformationen.	24. August 11:31:09 [IKEv1]IP = 64.102.156.87, EMPFANGENE IKE_DECODE-Nachricht (msgid=fb709d4d) mit Payloads: HDR + HASH (8) + ATTR (14) + KEINE (0) Gesamtlänge: 85 24. Aug. 11:31:09 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, process_attr(): Geben Sie ein!	
Verarbeitung von Benutzeranmeldeinformationen. Überprüfen Sie die Anmeldeinformationen, und generieren Sie die Moduskonfigurationsnutzlast. Relevante Konfiguration:	24. August 11:31:09 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Processing MODE_CFG Reply-Attribute. 24. August 11:31:09 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, IKEGetUserAttributes: Primäres DNS = 192.168.1.99 24. August 11:31:09 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87,	

username cisco password cisco	IKEGetUserAttributes: Sekundärer DNS = gelöscht 24. August 11:31:09 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, IKEGetUserAttributes: Primäres WINS = gelöscht 24. August 11:31:09 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, IKEGetUserAttributes: Sekundäres WINS = gelöscht 24. August 11:31:09 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, IKEGetUserAttributes: Split-Tunneling-Liste = Split 24. August 11:31:09 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, IKEGetUserAttributes: Standard-Domäne = jyoungta-labdomain.cisco.com 24. August 11:31:09 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, IKEGetUserAttributes: IP-Komprimierung = deaktiviert 24. August 11:31:09 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, IKEGetUserAttributes: Split Tunneling-Richtlinie = deaktiviert 24. August 11:31:09 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, IKEGetUserAttributes: Browserproxy-Einstellung = keine Änderung vornehmen 24. August 11:31:09 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, IKEGetUserAttributes: Browser-Proxy-Umgehung Local = Deaktivieren 24. August 11:31:09 [IKEv1]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Benutzer (user1) authentifiziert.	
xuath result senden.	24. August 11:31:09 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Erstellen einer leeren Hash-Nutzlast 24. August 11:31:09 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Erstellen der qm-Hash-Payload 24. August 11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE-SENDING-Nachricht (msgid=5b6910ff) mit Payloads: HDR + HASH (8) + ATTR (14) + KEINE (0) Gesamtlänge: 64	
	========== XAuth - Autorisierungsergebnis ==========>	
	54511:28:36.41608/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_XAUTHREQ_DONE 54611:28:36.41608/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_NO_EVENT 54711:28:36.42408/24/12Sev=Info/5IKE/0x630002F Empfangenes ISAKMP-Paket: peer = 64.102.156.88 54811:28:36.42408/24/12Sev=Info/4IKE/0x6300014 EMPFANG << ISAKMP OAK TRANS *(HASH, ATTR) ab 64.102.156.88 54911:28:36.42508/24/12Sev=Decode/11IKE/0x6300001	A P

	ISAKMP-Header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Nächste Payload: Hash Ver. (Hex):10 Exchange-Typ: Transaktion Flags:(Verschlüsselung) MessageID(Hex):5B6910FF Länge: 76 Payload-Hash Nächste Payload: Attribute Reserviert: 00 Payload-Länge: 24 Daten (in Hex): 7DCF47827164198731639BFB7595F694C9DFE85 Payload-Attribute Nächste Payload: Keine Reserviert: 00 Payload-Länge: 12 Typ: ISAKMP_CFG_SET Reserviert: 00 Kennung: 0000 XAUTH-Status: Pass 55011:28:36.42508/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_INITIALEvent: EV_RCVD_MSG 55111:28:36.42508/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_PCS_XAUTH_SETEvent: EV_INIT_XAUTH 55211:28:36.42508/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_PCS_XAUTH_SETEvent: EV_CHK_AUTH_RESULT	
	55311:28:36.42508/24/12Sev=Info/4IKE/0x6300013 SENDEN >>> ISAKMP OAK TRANS *(HASH, ATTR) bis 64.102.156.88	A
	<========== XAUTH - Bestätigung ==========	
Empfangen und Verarbeiten von ACK; Keine Antwort vom Server.	24. August 11:31:09 [IKEv1]IP = 64.102.156.87, EMPFANGENE IKE_DECODE-Nachricht (msgid=5b6910ff) mit Payloads: HDR + HASH (8) + ATTR (14) + KEINE (0) Gesamtlänge: 60 24. August 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, process_attr(): Geben Sie ein! 24. Aug. 11:31:09 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Verarbeitung der cfg ACK-Attribute	
	55511:28:36.42608/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_XAUTH_DONEvent: EV_XAUTH_DONE_SUC 55611:28:36.42608/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_XAUTH_DONEvent: EV_NO_EVENT 55711:28:36.42608/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState:	G M E a S

	TM_XAUTHREQ_DONEEvent: EV_TERM_REQUEST 55811:28:36.42608/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_FREEEvent: EV_ENTFERNEN 55911:28:36.42608/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_FREEEvent: EV_NO_EVENT 56011:28:36.42608/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_XAUTH_PROGEvent: EV_XAUTH_DONE_SUC 56111:28:38.40608/24/12Sev=Debug/8IKE/0x630004C Starten des DPD-Timers für IKE SA (I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0) sa->state = 1, sa->dpd.care_freq(mSec) = 5000 56211:28:38.40608/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_INIT_MODECFG 56311:28:38.40608/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_NO_EVENT 56411:28:38.40608/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=84B4B653CurState: TM_INITIALEvent: EV_INIT_MODECFG 56511:28:38.40808/24/12Sev=Info/5IKE/0x630005E Client sendet Firewall-Anfrage an Konzentrator 56611:28:38.40908/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_START_RETRY_TMR	
	56711:28:38.40908/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_SND_MSG 56811:28:38.40908/24/12Sev=Info/4IKE/0x6300013 SENDEN >>> ISAKMP OAK TRANS *(HASH, ATTR) bis 64.102.156.88 56911:28:38.62708/24/12Sev=Decode/11IKE/0x6300001 ISAKMP-Header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Nächste Payload: Hash Ver. (Hex):10 Exchange-Typ: Transaktion Flags:(Verschlüsselung) MessageID(Hex):84B4B653 Länge: 183 Payload-Hash Nächste Payload: Attribute Reserviert: 00	S K

	Payload-Länge: 24 Daten (in Hex): 81BFBF6721A744A815D69A315EF4AAA571D6B687 Payload-Attribute Nächste Payload: Keine Reserviert: 00 Payload-Länge: 131 Typ: ISAKMP_CFG_REQUEST Reserviert: 00 Kennung: 0000 IPv4-Adresse: (leer) IPv4-Netzmaske: (leer) IPv4-DNS: (leer) IPv4-NBNS (WINS): (leer) Ablaufdatum der Adresse: (leer) Cisco Erweiterung: Banner: (leer) Cisco Erweiterung: PWD speichern: (leer) Cisco Erweiterung: Standard-Domänenname: (leer) Cisco Erweiterung: Aufteilen: (leer) Cisco Erweiterung: DNS-Namen aufteilen: (leer) Cisco Erweiterung: PFS: (leer) Unbekannt: (leer) Cisco Erweiterung: Backup-Server: (leer) Cisco Erweiterung: Entfernen der Smartcard: (leer) Anwendungsversion: Cisco Systems VPN Client 5.0.07.0290:WinNT Cisco Erweiterung: Firewall-Typ: (leer) Cisco Erweiterung: Dynamischer DNS-Hostname: ATBASU-LABBOX		
	<========== Mode-config-Anforderung ==========		
Anforderung für die Empfangsmodus-Konfiguration.	24. Aug. 11:31:11 [IKEv1]IP = 64.102.156.87, EMPFANGENE IKE_DECODE-Nachricht (msgid=84b4b653) mit Payloads: HDR + HASH (8) + ATTR (14) + KEINE (0) Gesamtlänge: 183 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, process_attr(): Geben Sie ein!	57011:28:38.62808/24/12Sev= Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=84B4B653CurState: TM_WAIT_MODECFGREPLYEvent: EV_NO_EVENT	W S
Prozess-Konfigurationsanforderung. Viele dieser Werte werden normalerweise in der Gruppenrichtlinie konfiguriert. Da	24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Verarbeiten der Attribute cfg Request 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec,		

der Server in diesem Beispiel jedoch über eine sehr einfache Konfiguration verfügt, werden sie hier nicht angezeigt.	Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG: Erhaltene Anfrage für IPv4-Adresse! 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG: Empfangene Anfrage für die IPv4-Netzmaske! 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG: Empfangene Anfrage für DNS-Serveradresse! 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG: Erhaltene Anfrage für WINS-Serveradresse! 24. August 11:31:11 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Received unsupported transaction mode attribute: 5 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG: Anfrage für Banner erhalten! 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG: Empfangene Anfrage für die PW-Einstellung speichern! 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG: Empfangene Anfrage für Standard Domain Name! 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG: Empfangene Anfrage für Split Tunnel List! 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG: Empfangene Anforderung für Split DNS! 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG: Empfangene Anfrage für PFS-Einstellung! 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG: Empfangene Anfrage für Client Browser Proxy Setting! 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG: Empfangene Anfrage für Backup-IP-sec-Peer-Liste! 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG: Empfangene Anforderung für die Client Smartcard Removal Disconnect-Einstellung! 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG: Anfrage für Anwendungsversion erhalten! 24. Aug. 11:31:11 [IKEv1]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Client-Typ: WinNTClient-Anwendungsversion: 5 07 0290 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG: Anfrage für FWTYPE erhalten! 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG:

	Die empfangene Anfrage für den DHCP-Hostnamen für DDNS lautet: ATBASU-LABBOX!	
Erstellen Sie eine mode-config-Antwort mit allen konfigurierten Werten. Relevante Konfiguration: In diesem Fall wird dem Benutzer immer die gleiche IP zugewiesen. username cisco attributes **vpn-framed-ip-** **address 192.168.1.100** **255.255.255.0** group-policy EZ internal group-policy EZ attributes password-storage enabledns-server value 192.168.1.129 vpn-tunnel-protocol ikev1 split-tunnel-policy tunnelall split-tunnel-network- list value split default- domain value jyoungta- labdomain.cisco.com	24. Aug. 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, IP-Adresse (192.168.1.100) vor dem Initiieren von Modus-Cfg (XAuth) aktiviert) 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Senden der Subnetzmaske (255.255.255.0) an den Remote-Client 24. August 11:31:11 [IKEv1]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Zugewiesene private IP-Adresse 192.168.1.100 für Remote-Benutzer 24. Aug. 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Erstellen einer leeren Hash-Payload 24. Aug. 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, construct_cfg_set: Standard-Domäne = jyoungta-labdomain.cisco.com 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Clientbrowser-Proxy-Attribute senden! 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Browser-Proxy auf "No-Modify" (Kein Ändern) eingestellt. Browser-Proxy-Daten werden NICHT in die mode-cfg-Antwort aufgenommen. 24. Aug. 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Cisco Smartcard-Entfernung aktivieren! 24. Aug. 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Erstellen von qm-Hash-Payload	
Antwort "mode-config" senden.	24. August 11:31:11 [IKEv1]IP = 64.102.156.87, IKE_DECODE-SENDING-Nachricht (msgid=84b4b653) mit Payloads: HDR + HASH (8) + ATTR (14) + KEINE (0) Gesamtlänge: 215	
	============== Mode-config-Antwort ==========>	
	57111:28:38.63808/24/12Sev=Info/5IKE/0x630002F Empfangenes ISAKMP-Paket: peer = 64.102.156.88 57211:28:38.63808/24/12Sev=Info/4IKE/0x6300014 EMPFANG << ISAKMP OAK TRANS *(HASH, ATTR) ab 64.102.156.88 57311:28:38.63908/24/12Sev=Decode/11IKE/0x6300001 ISAKMP-Header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Nächste Payload: Hash Ver. (Hex):10 Exchange-Typ: Transaktion Flags:(Verschlüsselung) MessageID(Hex):84B4B653 Länge: 220 Payload-Hash Nächste Payload: Attribute Reserviert: 00 Payload-Länge: 24 Daten (in Hex):	E P M

	6DE2E70ACF6B185846BC62E590C00A66745D14D Payload-Attribute Nächste Payload: Keine Reserviert: 00 Payload-Länge: 163 Typ: ISAKMP_CFG_REPLY Reserviert: 00 Kennung: 0000 IPv4-Adresse: 192.168.1.100 IPv4-Netzmaske: 255.255.255,0 IPv4-DNS: 192.168.1.99 Cisco Erweiterung: PWD speichern: Nein Cisco Erweiterung: Standard-Domänenname: jyoungta-labdomain.cisco.com Cisco Erweiterung: PFS: Nein Anwendungsversion: Cisco Systems, Inc ASA5505 Version 8.4(4)1 von Entwicklern auf Thu 14-Jun-12 11:20 Cisco Erweiterung: Entfernen der Smartcard: Ja		
Phase 1 wird auf dem Server abgeschlossen. Initiieren Sie den Quick Mode (QM)-Prozess.	24. August 11:31:13 [IKEv1 DECODE]IP = 64.102.156.87, IKE Responder startet QM: msg id = 0e83792e 24. Aug. 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Schnellmodusverarbeitung verzögert, Cert/Trans Exchange/RM DSID in Verarbeitung 24. Aug. 11:31:13 [IKEv1]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Gratuitous ARP wird für 192.168.1.100 gesendet 24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Resume Quick Mode Processing, Cert/Trans Exch/RM DSID abgeschlossen 24. August 11:31:13 [IKEv1]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, PHASE 1 ABGESCHLOSSEN	57411:28:38.63908/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=84B4B653CurState: TM_WAIT_MODECFGREPLYEvent: EV_RCVD_MSG 57511:28:38.63908/24/12Sev=Info/5IKE/0x6300010 MODE_CFG_REPLY: Attribut = INTERNAL_IPV4_ADDRESS: Wert = 192.168.1.100 57611:28:38.63908/24/12Sev=Info/5IKE/0x6300010 MODE_CFG_REPLY: Attribut = INTERNAL_IPV4_NETMASK, Wert = 255.255.255.0 57711:28:38.63908/24/12Sev=Info/5IKE/0x6300010 MODE_CFG_REPLY: Attribut = INTERNAL_IPV4_DNS(1): , Wert = 192.168.1.99 57811:28:38.63908/24/12Sev=Info/5IKE/0x630000D MODE_CFG_REPLY: Attribut = MODECFG_UNITY_SAVEPWD: , value = 0x00000000 57911:28:38.63908/24/12Sev=Info/5IKE/0x630000E MODE_CFG_REPLY: Attribut = MODECFG_UNITY_DEFDOMAIN: , value = jyoungta-labdomain.cisco.com 58011:28:38.63908/24/12Sev=Info/5IKE/0x630000D MODE_CFG_REPLY: Attribut =	V k e

		MODECFG_UNITY_PFS: , value = 0x00000000 58111:28:38.63908/24/12Sev=Info/5IKE/0x630000E MODE_CFG_REPLY: Attribut = APPLICATION_VERSION, value = Cisco Systems, Inc ASA5505 Version 8.4(4)1, erstellt von Builder on Thu 14-Jun-12 11:20 58211:28:38.63908/24/12Sev=Info/5IKE/0x630000D MODE_CFG_REPLY: Attribut = MODECFG_UNITY_SMARTCARD_REMOVAL_DISCONNECT: , value = 0x00000001 58311:28:38.63908/24/12Sev=Info/5IKE/0x630000D MODE_CFG_REPLY: Attribut = Empfangen und Verwenden von NAT-T Portnummer , Wert = 0x00001194 58411:28:39.36708/24/12Sev=Debug/9IKE/0x6300093 Wert für ini-Parameter EnableDNSRedirection ist 1 58511:28:39.36708/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->TM:MsgID=84B4B653CurState: TM_MODECFG_DONEEvent: EV_MODECFG_DONE_SUC
Erstellen und Senden von DPD für den Client	24. August 11:31:13 [IKEv1]IP = 64.102.156.87, Keep-Alive-Typ für diese Verbindung: DPD 24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Start P1 rekey timer: 82080 Sekunden. 24. Aug. 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Benachrichtigung senden 24. Aug. 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Erstellen einer leeren Hash-Payload 24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Erstellen der qm-Hash-Payload 24. August 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE-SENDING-Nachricht (msgid=be8f7821) mit Payloads: HDR + HASH (8) + NOTIFY (11) + KEINE (0) Gesamtlänge: 92	
	========== DPD (Dead Peer Detection) ==========>	
	58811:28:39.79508/24/12Sev=Debug/7IKE/0x6300015 intf_data: lcl=0x0501A8C0, mask=0x00FFFF, bcast=0xFF01A8C0, bcast_vra=0xFF07070A 58911:28:39.79508/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5	

	R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_INIT_P2 59011:28:39.79508/24/12Sev=Info/4IKE/0x6300056 Eine Schlüsselanfrage vom Treiber erhalten: Lokale IP = 192.168.1.100, GW IP = 64.102.156.88, Remote IP = 0,0.0,0 59111:28:39.79508/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_ACTIVEEvent: EV_NO_EVENT 59211:28:39.79508/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->QM:MsgID=0E83792ECurState: QM_INITIALEvent: EV_INITIATOR 59311:28:39.79508/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->QM:MsgID=0E83792ECurState: QM_BLD_MSG1Ereignis: EV_CHK_PFS 59411:28:39.79608/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->QM:MsgID=0E83792ECurState: QM_BLD_MSG1Ereignis: EV_BLD_MSG 59511:28:39.79608/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->QM:MsgID=0E83792ECurState: QM_SND_MSG1Ereignis: EV_START_RETRY_TMR	C V P - - -
	59611:28:39.79608/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->QM:MsgID=0E83792ECurState: QM_SND_MSG1Ereignis: EV_SND_MSG 59711:28:39.79608/24/12Sev=Info/4IKE/0x6300013 SENDEN >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) an 64.102.156,88	S
	<========== Schnellmodus-Meldung 1 (QM1) ==========	
Empfangen von QM1.	24. August 11:31:13 [IKEv1]IP = 64.102.156.87, EMPFANGENE IKE_DECODE-Nachricht (msgid=e83792e) mit Payloads: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + KEINE (0) Gesamtlänge: 1026	
QM1 verarbeiten. Relevante Konfiguration: `crypto dynamic-map DYN 10 set transform-set TRA`	24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Verarbeitung von Hash-Payload 24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Verarbeitung der SA-Nutzlast 24. Aug. 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Verarbeitung von einmaliger Nutzlast 24. Aug. 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Verarbeitungs-ID-Payload 24. Aug. 11:31:13 [IKEv1 DECODE]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, ID_IPV4_ADDR-ID erhalten 192.168.1.100 24. August 11:31:13 [IKEv1]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, empfangene Remote-Proxy-Host-Daten in ID-Payload:Adresse 192.168.1.100, Protokoll 0, Port 0 24. Aug. 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec,	

	Benutzername = Benutzer1, IP = 64.102.156.87, Verarbeitungs-ID-Payload 24. Aug. 11:31:13 [IKEv1 DECODE]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, ID_IPV4_ADDR_SUBNET ID received—0.0.0.0—0.0.0.0 24. August 11:31:13 [IKEv1]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, empfangene lokale IP-Proxy-Subnetzdaten in ID-Payload:Adresse 0.0.0,0, Maske 0.0.0, Protokoll 0, Port 0 24. August 11:31:13 [IKEv1]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, QM IsRekeyed old as not found by addr 24. August 11:31:13 [IKEv1]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Prüfung der statischen Crypto Map, Überprüfung Map = out-map, seq = 10.. 24. Aug. 11:31:13 [IKEv1]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Statische Kryptozuordnung Nach Übergabe prüfen: Crypto Map Eintrag unvollständig! 24. Aug. 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, wobei nur der durch NAT-Traversal definierte UDP-gekapselte-Tunnel- und UDP-gekapselte-Transportmodus ausgewählt wird 24. Aug. 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, wobei nur der durch NAT-Traversal definierte UDP-gekapselte-Tunnel- und UDP-gekapselte-Transportmodus ausgewählt wird 24. Aug. 11:31:13 [IKEv1]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, IKE-Remote-Peer konfiguriert für Crypto Map: Out-of-dyn-Map 24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Verarbeitung der IPSec SA-Nutzlast

Erstellen Sie QM2.
Relevante Konfiguration:
 	
`tunnel-group EZ`
`type` **`remote-access`** *`!`*
`(tunnel type ra = tunnel type remote-access)`
`crypto ipsec transform-set TRA` **`esp-aes esp-sha-hmac`**
`crypto ipsec security-association` **`lifetime seconds 28800`**
`crypto ipsec security-association lifetime kilobytes 4608000`
`crypto dynamic-map DYN 10 set transform-set TRA`
`crypto map MAP 65000 ipsec-isakmp dynamic DYN`
`crypto map MAP interface outside`
	24. Aug. 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, IPSec SA-Angebot Nr. 12, Umwandeln Nr. 1 akzeptabelEntspricht dem globalen IPSec SA-Eintrag Nr. 10
	24. August 11:31:13 [IKEv1]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, IKE: SPI wird angefordert!
	IPSEC: Neue embryonale SA erstellt @ 0xcfdffc90, SCB: 0xCFDFFB58, Richtung: eingehend
	SPI: 0x9E18ACB2
	Sitzungs-ID: 0x00138000
	VPIF-Nummer: 0x0000004
	Tunneltyp: rz
	Protokoll: esp
	Lebensdauer: 240 Sekunden
	24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, IKE hat SPI von der Schlüsselengine erhalten: SPI = 0x9e18acb2
	24. Aug. 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, oakley-Konstruktor Quick-Modus
	24. Aug. 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username =

	user1, IP = 64.102.156.87, Erstellen einer leeren Hash-Payload 24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Erstellen der IPSec SA-Nutzlast 24. Aug. 11:31:13 [IKEv1]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Überschreiben der IPSec-Neueinstellungsdauer des Initiators von 2147483 auf 86400 Sekunden 24. Aug. 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Erstellen der IPSec-EinmalPayload 24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Erstellen der Proxy-ID 24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Proxy-ID senden: Remote-Host: 192.168.1.100Protokoll, 0 Ports, 0 Lokales Subnetz: 0.0.0.0mask 0.0.0.0 Protocol: 0 Port 0 24. Aug. 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Senden der LIFETIME-ANTWORT an Initiator 24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Erstellen der qm-Hash-Payload	
Senden Sie QM2.	24. Aug. 11:31:13 [IKEv1 DECODE]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, IKE-Responder sendet 2nd QM pkt: msg id = 0e83792e 24. August 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE-SENDING-Nachricht (msgid=e83792e) mit Payloads: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + KEINE (0) Gesamtlänge: 184	
	========== Quick Mode Message 2 (QM2) ==========>	
	60811:28:39,96208/24/12Sev=Info/4IKE/0x6300014 EMPFANG << ISAKMP OAK QM *(HASH, SA, NON, ID, ID, BENACHRICHTIGUNG:STATUS_RESP_LIFETIME) von 64.102.156.88	E
	60911:28:39,96408/24/12Sev=Decode/11IKE/0x6300001 ISAKMP-Header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Nächste Payload: Hash Ver. (Hex):10 Exchange Type (Exchange-Typ): Quick Mode Flags:(Verschlüsselung) MessageID(Hex):E83792E Länge: 188 Payload-Hash Nächste Payload: Security Association Reserviert: 00 Payload-Länge: 24 Daten (in Hex):	P P A

	CABF38A62C9B88D1691E81F3857D6189534B2EC0 Payload Security Association Nächste Payload: Nonce Reserviert: 00 Payload-Länge: 52 DOI: IPsec Lage: (SIT_IDENTITY_ONLY) Payload-Angebot Nächste Payload: Keine Reserviert: 00 Payload-Länge: 40 Angebotsnr.: 1 Protokoll-ID: PROTO_IPSEC_ESP SPI-Größe: 4 Anzahl der Umwandlungen: 1 SPI: 9E18ACB2 Payload-Umwandlung Nächste Payload: Keine Reserviert: 00 Payload-Länge: 28 Umwandlungsnr.: 1 Transform-ID: ESP_3DES Reserviert2: 0000 Art des Lebenszyklus: Sekunden Lebensdauer (Hex): 0020C49B Kapselungsmodus: UDP-Tunnel Authentifizierungsalgorithmus: SHA1 Payload Nonce Nächste Payload: Identifikation Reserviert: 00 Payload-Länge: 24 Daten (in Hex): 3A079B75DA512473706F235EA3FCA61F1D15D4CD Payload-Identifizierung Nächste Payload: Identifikation Reserviert: 00 Payload-Länge: 12 ID-Typ: IPv4-Adresse Protokoll-ID (UDP/TCP usw.): 0 Port: 0 ID-Daten und -Doppelpunkt; 192.168.1.100 Payload-Identifizierung Nächste Payload: Benachrichtigung Reserviert: 00 Payload-Länge: 16 ID-Typ: IPv4-Subnetz Protokoll-ID (UDP/TCP usw.): 0 Port: 0 ID-Daten und -Doppelpunkt; 0.0.0.0/0.0.0.0 Payload-Benachrichtigung Nächste Payload: Keine

	Reserviert: 00 Payload-Länge: 28 DOI: IPsec Protokoll-ID: PROTO_IPSEC_ESP SPI-Größe: 4 Benachrichtigungstyp: STATUS_RESP_LIFETIME SPI: 9E18ACB2 Daten & Kolon; Art des Lebenszyklus: Sekunden Lebensdauer (Hex): 00015180	
	61011:28:39.96508/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->QM:MsgID=0E83792ECurState: QM_WAIT_MSG2Ereignis: EV_RCVD_MSG 61111:28:39,96508/24/12Sev=Info/5IKE/0x6300045 RESPONDER-LIFETIME notify hat einen Wert von 86400 Sekunden 61211:28:39.96508/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->QM:MsgID=0E83792ECurState: QM_WAIT_MSG2Ereignis: EV_CHK_PFS 61311:28:39.96508/24/12Sev=Debug/7IKE/0x6300076	Q
	NAV Trace->QM:MsgID=0E83792ECurState: QM_BLD_MSG3Ereignis: EV_BLD_MSG 61411:28:39.96508/24/12Sev=Debug/7IKE/0x6300076 ISAKMP-Header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Nächste Payload: Hash Ver. (Hex):10 Exchange Type (Exchange-Typ): Quick Mode Flags:(Verschlüsselung) MessageID(Hex):E83792E Länge: 52 Payload-Hash Nächste Payload: Keine Reserviert: 00 Payload-Länge: 24 Daten (in Hex): CDDC20D91EB4B568C826D6A5770A5CF020141236	E E w be
	61511:28:39.96508/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->QM:MsgID=0E83792ECurState: QM_SND_MSG3Ereignis: EV_SND_MSG 61611:28:39,96508/24/12Sev=Info/4IKE/0x6300013 SENDEN >>> ISAKMP OAK QM *(HASH) an 64.102.156.88	Q be ur
	<========== Quick Mode Message 3 (QM3) ==========	
Empfangen von QM3.	24. August 11:31:13 [IKEv1]IP = 64.102.156.87, EMPFANGENE IKE_DECODE-Nachricht (msgid=e83792e) mit Payloads: HDR + HASH (8) + KEINE (0) Gesamtlänge: 52	
QM3 verarbeiten. Erstellen Sie die ein- und ausgehenden Security-Parameterindizes (SPIs).	24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Verarbeitung von Hash-Payload	

Hinzufügen einer statischen Route für den Host Relevante Konfiguration: crypto ipsec transform-set TRA esp-aes esp-sha-hmac crypto ipsec security-association lifetime seconds 28800 crypto ipsec security-association lifetime kilobytes 4608000 crypto dynamic-map DYN 10 set transform-set TRA crypto dynamic-map DYN 10 **set reverse-route**	24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Laden aller IPSEC SAs 24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Generating Quick Mode Key! 24. Aug. 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, NP-Verschlüsselungsregel sucht nach der unverschlüsselten Zuordnung 10 übereinstimmender ACL Unbekannt: zurückgesendet cs_id=cc107410; Regel=00000000 24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Generating Quick Mode Key! IPSEC: Neue embryonale SA erstellt @ 0xccc9ed60, SCB: 0xCF7F59E0, Richtung: ausgehend SPI: 0 x C055290 A Sitzungs-ID: 0x00138000 VPIF-Nummer: 0x0000004 Tunneltyp: rz Protokoll: esp Lebensdauer: 240 Sekunden IPSEC: Abgeschlossenes Host-OBSA-Update, SPI 0xC05290A IPSEC: Erstellen von ausgehenden VPN-Kontexten, SPI 0xC05290A Flaggen: 0x0000025 SA: 0xccc9ed60 SPI: 0 x C055290 A MTU: 1500 Byte VCID: 0x0000000 Peer: 0x0000000 SCB: 0xA5922B6B Kanal: 0xc82afb60 IPSEC: Abgeschlossener ausgehender VPN-Kontext, SPI 0xC05290A VPN-Handle: 0 x 0015909c IPSEC: Neue ausgehende Verschlüsselungsregel, SPI 0xC05290A Src-Adresse: 0,0 0,0 SRC-Maske: 0,0 0,0 Ziel-Adresse: 192.168.1.100 DART-Maske: 255 255 255 255 255 Src-Ports Obere: 0 Unteres: 0 Op: ignorieren Dst-Ports Obere: 0 Unteres: 0 Op: ignorieren Protokoll: 0

	Protokoll verwenden: falsch SPI: 0x0000000 SPI verwenden: falsch IPSEC: Abgeschlossene Verschlüsselungsregel für ausgehenden Datenverkehr, SPI 0xC05290A Regel-ID: 0xcb47a710 IPSEC: Neue Regel für die Genehmigung ausgehender Anrufe, SPI 0xC055290A Src-Adresse: 64 102 156 88 SRC-Maske: 255 255 255 255 255 Ziel-Adresse: 64 102 156 87 DART-Maske: 255 255 255 255 255 Src-Ports Obere: 4500 Unteres: 4500 Op: gleich Dst-Ports Obere: 58506 Unteres: 58506 Op: gleich Protokoll: 17 Protokoll verwenden: wahr SPI: 0x0000000 SPI verwenden: falsch IPSEC: Abgeschlossene Regel für die Genehmigung ausgehender Anrufe, SPI 0xC05290A Regel-ID: 0xcdf3cfa0 24. Aug. 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, NP-Verschlüsselungsregel sucht nach der unverschlüsselten Zuordnung 10 übereinstimmender ACL Unbekannt: zurückgesendet cs_id=cc107410; Regel=00000000 24. Aug. 11:31:13 [IKEv1]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Sicherheitsverhandlungen abgeschlossen für Benutzer (user1)Responder, Eingehender SPI = 0x9e18acb2, Ausgehend SPI = 0xc055290a 24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, IKE KEY_ADD-Nachricht für SA erhalten: SPI = 0xc055290a IPSEC: Abgeschlossenes Host-IBSA-Update, SPI 0x9E18ACB2 IPSEC: Erstellen eines eingehenden VPN-Kontexts, SPI 0x9E18ACB2 Flaggen: 0x0000026 SA: 0xcfdffc90 SPI: 0x9E18ACB2 MTU: 0 Byte VCID: 0x0000000 Peer: 0 x 0015909C SCB: 0xA5672481 Kanal: 0xc82afb60 IPSEC: Abgeschlossener eingehender VPN-Kontext, SPI

	0x9E18ACB2 VPN-Handle: 0 x 0016219c IPSEC: Aktualisierung des ausgehenden VPN-Kontexts 0x0015909C, SPI 0xC055290A Flaggen: 0x0000025 SA: 0xccc9ed60 SPI: 0 x C055290 A MTU: 1500 Byte VCID: 0x0000000 Peer: 0 x 0016219C SCB: 0xA5922B6B Kanal: 0xc82afb60 IPSEC: Abgeschlossener ausgehender VPN-Kontext, SPI 0xC05290A VPN-Handle: 0 x 0015909c IPSEC: Abgeschlossene innere Regel für ausgehenden Datenverkehr, SPI 0xC05290A Regel-ID: 0xcb47a710 IPSEC: Ausgehende SPD-Regel, SPI 0xC05290A Regel-ID: 0xcdf3cfa0 IPSEC: Neue Regel für eingehenden Tunnelfluss, SPI 0x9E18ACB2 Src-Adresse: 192.168.1.100 SRC-Maske: 255 255 255 255 255 Ziel-Adresse: 0,0 0,0 DART-Maske: 0,0 0,0 Src-Ports Obere: 0 Unteres: 0 Op: ignorieren Dst-Ports Obere: 0 Unteres: 0 Op: ignorieren Protokoll: 0 Protokoll verwenden: falsch SPI: 0x0000000 SPI verwenden: falsch IPSEC: Abgeschlossene eingehende Tunnelflussregel, SPI 0x9E18ACB2 Regel-ID: 0xcdf15270 IPSEC: Neue Entschlüsselungsregel für eingehenden Datenverkehr, SPI 0x9E18ACB2 Src-Adresse: 64 102 156 87 SRC-Maske: 255 255 255 255 255 Ziel-Adresse: 64 102 156 88 DART-Maske: 255 255 255 255 255 Src-Ports Obere: 58506 Unteres: 58506 Op: gleich Dst-Ports Obere: 4500

	Unteres: 4500 Op: gleich Protokoll: 17 Protokoll verwenden: wahr SPI: 0x0000000 SPI verwenden: falsch IPSEC: Abgeschlossene Entschlüsselungsregel für eingehenden Datenverkehr, SPI 0x9E18ACB2 Regel-ID: 0xce03c2f8 IPSEC: Neue Zulassungsregel für eingehenden Datenverkehr, SPI 0x9E18ACB2 Src-Adresse: 64 102 156 87 SRC-Maske: 255 255 255 255 255 Ziel-Adresse: 64 102 156 88 DART-Maske: 255 255 255 255 255 Src-Ports Obere: 58506 Unteres: 58506 Op: gleich Dst-Ports Obere: 4500 Unteres: 4500 Op: gleich Protokoll: 17 Protokoll verwenden: wahr SPI: 0x0000000 SPI verwenden: falsch IPSEC: Abgeschlossene Zulassungsregel für eingehenden Datenverkehr, SPI 0x9E18ACB2 Regel-ID: 0xcf6f58c0 24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Pitcher: Empfangene KEY_UPDATE, spi 0x9e18acb2 24. Aug. 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Start P2 rekey Timer: 82080 Sekunden. 24. August 11:31:13 [IKEv1]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Hinzufügen einer statischen Route für Client-Adresse: 192.168.1.100
Phase 2 abgeschlossen. Beide Seiten verschlüsseln und entschlüsseln jetzt.	24. August 11:31:13 [IKEv1]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, PHASE 2 ABGESCHLOSSEN (msgid=0e83792e)
Für Hardware-Clients wird eine weitere Nachricht empfangen, in der der Client Informationen über sich selbst sendet. Wenn Sie genau hinschauen, sollten Sie den Hostnamen des EzVPN-Clients, die auf dem Client ausgeführte Software sowie den Standort und den Namen der Software finden	24. August 11:31:13 [IKEv1]: IP = 10.48.66.23, IKE_DECODE EMPFANGENE Nachricht (msgid=91facca9) mit Payloads: HDR + HASH (8) + NOTIFY (11) + KEINE (0) Gesamtlänge: 184 24. August 11:31:13 [IKEv1 DEBUG]: Gruppe = EZ, Benutzername = cisco, IP = 10,48,66,23, Verarbeitung von Hash-Payload 24. August 11:31:13 [IKEv1 DEBUG]: Gruppe = EZ, Benutzername = cisco, IP = 10,48,66,23, Verarbeitung der Benachrichtigungs-Payload 24. Aug. 11:31:13 [IKEv1 DECODE]: OBSOLETE-BESCHREIBER - INDEX 1

	24. Aug. 11:31:13 [IKEv1 DECODE]: 0000: 0000000 7534000 B 62736E73 2D383731 ....u4.**bsns-871** 0010: 2D332E75 32000943 6973636F 20383731 **-3**.u2..**Cisco 871** 0020: 7535000B 46484B30 39343431 32513675 u5.FHK094412Q6u 0030: 36000932 32383538 39353638 75390009 6.228589568u9.. 0040: 31343532 31363331 32753300 2B666C61 145216312u3.+**fla** 0050: 73683A63 3837302D 61647669 70736572 **sh:c870-advipser** 0060: 76696365 736B392D 6D7A2E31 32342D32 **vicesk9-mz.124-2** 0070: 302E5435 2E62696E **0,T5,bin** 24. August 11:31:13 [IKEv1 DEBUG]: Gruppe = EZ, Benutzername = cisco, IP = 10.48.66.23, Verarbeitung PSK Hash 24. August 11:31:13 [IKEv1]: Gruppe = EZ, Benutzername = cisco, IP = 192.168.1.100, inkonsistente PSK-Hash-Größe 24. August 11:31:13 [IKEv1 DEBUG]: Gruppe = EZ, Benutzername = cisco, IP = 10.48.66.23, PSK-Hash-Verifizierung fehlgeschlagen!

Tunnelüberprüfung

ISAKMP

Die Ausgabe des Befehls **sh cry isa sa det** lautet:

```
 Active SA: 1
 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 10.48.66.23
 Type : user Role : responder
 Rekey : no State : AM_ACTIVE
 Encrypt : aes Hash : SHA
 Auth : preshared Lifetime: 86400
 Lifetime Remaining: 86387
 AM_ACTIVE - aggressive mode is active.
```

IPsec

Da das Internet Control Message Protocol (ICMP) zum Auslösen des Tunnels verwendet wird, ist nur eine IPsec-SA aktiv. Protokoll 1 ist ICMP. Beachten Sie, dass sich die SPI-Werte von den Werten unterscheiden, die im Debuggen ausgehandelt werden. Dies ist in der Tat der gleiche Tunnel nach der Phase-2-Wiederkehr.

Die Ausgabe des Befehls **sh crypto ipsec sa** lautet:

```
interface: outside
 Crypto map tag: DYN, seq num: 10, local addr: 10.48.67.14

 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
 remote ident (addr/mask/prot/port): (192.168.1.100/255.255.255.255/0/0)
 current_peer: 10.48.66.23, username: cisco
 dynamic allocated peer ip: 192.168.1.100

 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
 #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
 #send errors: 0, #recv errors: 0

 local crypto endpt.: 10.48.67.14/0, remote crypto endpt.: 10.48.66.23/0
 path mtu 1500, ipsec overhead 74, media mtu 1500
 current outbound spi: C4B9A77C
 current inbound spi : EA2B6B15

 inbound esp sas:
 spi: 0xEA2B6B15 (3928714005)
 transform: esp-aes esp-sha-hmac no compression
 in use settings ={RA, Tunnel, }
 slot: 0, conn_id: 425984, crypto-map: DYN
 sa timing: remaining key lifetime (sec): 28714
 IV size: 16 bytes
 replay detection support: Y
 Anti replay bitmap:
 0x00000000 0x0000003F
 outbound esp sas:
 spi: 0xC4B9A77C (3300501372)
 transform: esp-aes esp-sha-hmac no compression
 in use settings ={RA, Tunnel, }
 slot: 0, conn_id: 425984, crypto-map: DYN
 sa timing: remaining key lifetime (sec): 28714
 IV size: 16 bytes
 replay detection support: Y
 Anti replay bitmap:
 0x00000000 0x00000001
```

Zugehörige Informationen

- Wikipedia-Artikel zu IPsec
- IPsec-Fehlerbehebung: Verwenden von Debugbefehlen
- Technischer Support und Dokumentation - Cisco Systems