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

Inhalt

Einführung Kernproblem Szenario Verwendete Debug-Befehle ASA-Konfiguration Debuggen Tunnelüberprüfung ISAKMP IPsec Zugehörige Informationen

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 <u>zu Debug-Befehlen</u> vor der Verwendung von **Debug-**Befehlen finden Sie unter <u>Wichtige Informationen</u>.

Beschreibung der Servernachricht		Debugger	
	49711:28:30.28908/24/1	2Sev=Info/6IKE/0x630003B	ĪD
	Verbindungsversuch mit	64.102.156.88.	a
	49811:28:30.29708/24/1	2Sev=Debug/7IKE/0x6300076	Ď
	NAV Trace->SA:I Cooki	e=D56197780D7BE3E5	-
	R Cookie=00000000000	00000CurState:	_
	AM INITIALEvent: EV II	NITIATOR	
	49911:28:30.29708/24/1	2Sev=Info/4IKE/0x6300001	U
	Beginn der IKE Phase 1-	Verhandlung	a
	50011:28:30.29708/24/1	2Sev=Debug/7IKE/0x6300076	_
	NAV Trace->SA:L Cookie	e=D56197780D7BE3E5	_
	R Cookie=00000000000	00000CurState	_
	AM SND MSG1Veranst	altung: EV GEN DHKEY	
	50111.28.30 30408/24/1	2Sev=Debug/7IKF/0x6300076	
	NAV Trace->SA:L Cooki	e=D56197780D7BE3E5	
	R Cookie=00000000000	00000CurState	
	AM SND MSG1Veranst	altung: EV BLD MSG	
	50211.28.30 30408/24/1	2Sev=Debug/7IKE/0x6300076	
	NAV Trace->SA:L Cooki	e=D56197780D7BE3E5	
	B Cookie=00000000000	00000CurState	
	AM SND MSG1Veranst	altung: EV START RETRY TMR	
	50311.28.30 30408/24/1	2Sev=Debug/7IKE/0x6300076	
	NAV Trace->SA:L Cooki	=D56197780D7BE3E5	
	B Cookie=00000000000	00000CurState	
	AM SND MSG1Veranst	altung: EV_SND_MSG	
	50/11:28:30 30/08/2//1	$2S_{ev} = \ln f_0 / 4 K E / 0 \times 6300013$	
	SENDEN >>> ISAKMP (AK AG (SA KE NON ID VID(Xauth)	
	VID(dpd), VID(Frag), VIE	(Nat-T), VID(Unity)) an 64,102,156.88	
	<======================================	==== Aggressive Nachricht 1 (AM1)	忄
	==	==========	
Empfangen von AM1 vom Client	24. August 11:31:03	50611:28:30.3308/24/12Sev=Debug/7I	
	[IKEv1]IP =	KE/0x6300076	S
	64.102.156.87,	NAV Trace-	
	EMPFANGENE	>SA:I_Cookie=D56197780D7BE3E5	
	IKE_DECODE-Nachricht	R_Cookie=000000000000000000CurSta	ι
	(msgid=0) mit Payloads:	te:	
	HDR + SA (1) + KE (4)	AM_WAIT_MSG2Veranstaltung:	
	+ NEIN (10) + ID (5) +	EV_NO_EVENT	
	ANBIETER (13) +		
	KEINE (0)		
	Gesamtlänge: 849		
Prozess AM1. Vergleichen Sie	24. Aug. 11:31:03 [IKEv1	DEBUG]IP = 64.102.156.87,	1

ſ	ampfangana Angahata und	Wararhaitung SA Dayland
	I ransformationen mit bereits für	[24. August 11:31:03 [IKEV1 DEBUG]IP = 64.102.156.87,
	Ubereinstimmungen konfigurierten	Verarbeitung der ke-Payload
	Angeboten.	24. August 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87,
	Relevante Konfiguration:	Verarbeitung der ISA_KE-Payload
	ISAKMP ist auf der Schnittstelle	24. August 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87,
	aktiviert, und es wird mindestens	Verarbeitung einmaliger Nutzlast
	eine Richtlinie definiert, die dem	24. Aug. 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87.
	entspricht was der Client gesendet	Processing ID Payload
	hat	24 August 11:31:03 [IKEv1 DEBUG]IP = 64 102 156 87
	nat.	Verarbeitung der VID-Nutzlast
	arimto igalemn onable	$\frac{1}{24} = \frac{1}{24} $
	outside	24. Aug. 11.31.03 [IKEVI DEDUG]IP = 04.102.130.07, VID
	crvpto isakmp policy	
	10	24. August 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87,
	authentication pre-	Verarbeitung der VID-Nutzlast
	share	24. August 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87,
	encryption aes	empfangene DPD-VID
	hash sha	24. August 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87,
	group 2	Verarbeitung der VID-Nutzlast
	lifetime 86400	24 August 11:31:03 [IKEv1 DEBUG]IP = 64 102 156 87
	l'unneigruppe, die mit dem	empfangene Fragmentierungs_VID
	vorhandenen Identitätsnamen	$24 \text{August } 11:31:03 \text{ [IKEy1 DEBLC]ID} = 64 \ 102 \ 156 \ 87 \ \text{IKE}$
	übereinstimmt:	24. August 11.51.05 [INEVI DEDOG]IF = 04.102.150.07, INE-
	tunnel-group EZ type	
	remote-access	[24. August 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87,
	tunnel-group EZ	Verarbeitung der VID-Nutzlast
	general-attributes	24. Aug. 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, NAT-
	FZ	Traversal ver 02 VID erhalten
	tunnel-group EZ ipsec-	24. August 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87,
	attributes	Verarbeitung der VID-Nutzlast
	pre-shared-key cisco	24. Aug. 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87.
		empfangene Cisco Unity Client-VID
		24 Aug = 11.31.03 [IKEv1]]P = 64.102.156.87 Verbindung
		landete auf tunnel, group insec
		24 Aug. 11:31:03 [[KEv1 DEB] G]Gruppo - insoc IP -
		64 102 156 97 Vererbeitung IKE SA Devloed
		24. August 11:31:03 [IKEV1]Fenier in Phase 1:Nicht
		ubereinstimmende 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
		ühereinstimmende Attributtynen für Klassenbeschreibung Rov'd:
		Crunne 20 fa'd: Crunne 5
		101 uppe 2019 u. Oluppe 3
		upereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd:
		Gruppe 2Ctg'd: Gruppe 5
		24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht
		übereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd:
1	1	

	Gruppe 2Cfg'd: Gruppe 5
	24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht
	übereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd:
	Gruppe 2Cfa'd: Gruppe 5
	24 August 11:31:03 [IKEv1]Eehler in Phase 1:Nicht
	übereinstimmende Attributtypen für Klassenbeschreibung Rcv'd
	Gruppe 2Cfg/d: Gruppe 5
	24 August 11:21:02 [IKEv1]Eabler in Dhase 1:Night
	24. August 11.51.05 [INEVI]Femer III Fildse 1.Nicht
	ubereinsummende Aunbultypen für Klassenbeschreibung:Rcv d:
	Gruppe 2Ctg'd: Gruppe 5
	24. August 11:31:03 [IKEv1]Fehler in Phase 1:Nicht
	lübereinstimmende Attributtypen für Klassenbeschreibung:Rcv'd:
	Gruppe 2Ctg'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 2Cfo'd' Gruppe 5
	24 August 11:31:03 [IKEv1]Eehler in Phase 1:Nicht
	übereinstimmende Attributtynen für Klassenbeschreibung:Rcv'd:
	Gruppe 2Cfd/d: Gruppe 5
	24 August 11:21:02 [IKEv1]Eabler in Dhase 1:Night
	übereinstimmende Attributtypen für Klassenbeschreibung: Deu'd:
	Cruppe 20fe/d: Cruppe 5
	Gruppe 2Cig d. Gruppe 5
	24. August 11.31.03 [IKEVI]Fenier in Phase 1. Nicht
	ubereinstimmende 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	24. Aug. 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP =
umfasst:	64.102.156.87, Erstellen der ISAKMP SA-Payload
- gewählte Richtlinien	24. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP =
Diffie-Hellman (DH)	64.102.156.87, Erstellen von ke-Payload
- Responder-ID	24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP =
- Autor	64.102.156.87, Erstellen von einmaliger Nutzlast
- Network Address Translation	24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP =
(NAT)-Erkennungs-Pavload	64.102.156.87. Erstellen von Schlüsseln für Responder.
	24 August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec. IP =
	64 102 156 87 Frstellen der ID-Nutzlast
	24 August 11:31:03 [IKEv1 DEBUG]Group = insec IP =
	64 102 156 87 Erstellen von Hash-Payload
	24 Aug. 11:31:03 [IKEv1 DEBLIG]Gruppe = insec. IP =
	$164 \ 102 \ 156 \ 87 \ Computing-Hash für ISAKMP$
	24 Aug 11:31:03 [[KEy4 DEP1G]Group = incom [D =
	64 102 156 87 Erstellen der Ciese Unity VID Devlagd
	24. Aug. 11.31.03 NEV DEDOG Gluppe = psec, P = 64.403.456.97 Free to 64.456.97 Free to Free to 64.456.97 Free to 64.456.97 Free to F
	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-Pavload	
	24 Aug 11:31:03 [IKEv1 DEBUG]Group = ipsec IP =	
	64 102 156 87 Erstellen der NAT-Discovery-Payload	
	24 Aug 11:31:03 [[KEy1 DEB]]G[Group = insec []B =	
	24. Aug. 11.51.05 [IKEVI DEDOG]Gloup = Ipsec, IF =	
	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 = insec. IP =	
	64 102 156 87 Erstellen der VID-Payload	
	24. August 11:21:02 [IKEv1 DEPLIC]Crupps = incos ID =	
	24. August 11.31.05 [IKEVI DEBOG]Gluppe – Ipsec, IP –	
	104.102.156.87, Altiga/CISCO VPN3000 senden/CISCO ASA GVV-	
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) +	
	ANBIÉTER (13) + ANBIÈTER (13) + ANBIETER (13) + NAT-D	
	(130) + NAT-D (130) + ANBIETER (1) 3) + ANBIETER (13) +	
	KEINE(0) Gesamtlänge: 444	
	======================================	╢╴
	\square ====================================	
	=======>	
	======================================	
	======================================	A
	======================================	 A
	======================================	A
	======================================	A
	======================================	A
	======================================	A
	======================================	
	======================================	
	======================================	
	======================================	
	======================================	
	======================================	
	======================================	
	=================================	
	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 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 NAT-T	
	====================================	
	====================================	
	======> 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 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:	
	======> 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 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_SKEVID	
	======> 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 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 51411:28:30.41208/24/12Sev=Debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Veranstaltung: EV_GEN_SKEYID 51471:29:20.42209/24/42Sev=Debug/7IKE/0x6200076	

	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/7IKF/0x6300076	
	NAV Trace->SA:L Cookie=D56197780D7BE3E5	
	P. Cookio=18301D2DE710ED40CurState:	
	AM WAIT MSC2)/oropotalturg: EV CBVDTO ACTIVE	
	52011:28:30.42208/24/12Sev=Debug//IKE/0x6300076	A
	NAV Trace->SA:I_Cookie=D5619/780D7BE3E5	b
	R_Cookie=1B301D2DE710EDA0CurState:	Z
	AM_SND_MSG3Ereignis: EV_BLD_MSG	d
	52111:28:30.42208/24/12Sev=Debug/8IKE/0x6300001	E
	IOS-Anbieter-ID-Aufbau gestartet	
	52211:28:30.42208/24/12Sev=Info/6IKE/0x6300001	
	IOS-Anbieter-ID-Aufbau erfolgreich	
L	52311.28.30 /2308/2//12Sev=Debug/7lkE/0v6300076	
	NAV Trace->SAIL Cookio-D56107780D7E2E5	
	D. Cookie=4D204D2DE740ED40CurrChates	
	R_COOKIE=1B301D2DE/10EDAUCUrState:	
	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	
	<pre><====================================</pre>	
	=======================================	
Empfangen von AM3 vom Client.	======================================	
Empfangen von AM3 vom Client.	======================================	
Empfangen von AM3 vom Client.	======================================	
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	
Empfangen von AM3 vom Client.	======================================	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten	======================================	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit die	24. August 11:31:03 [IKEv1]IP = 64.102.156.87, EMPFANGENEIKE_DECODE-Nachricht (msgid=0) mit Payloads: HDR + HASH(8) + NOTIFY (11) + NAT-D (130) + NAT-D (130) + ANBIETER(13) + ANBIETER (13) + KEINE (0) Gesamtlänge: 16824. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP =64.102.156.87, Verarbeitung von Hash-Payload24. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP =	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die	24. August 11:31:03 [IKEv1]IP = 64.102.156.87, EMPFANGENEIKE_DECODE-Nachricht (msgid=0) mit Payloads: HDR + HASH(8) + NOTIFY (11) + NAT-D (130) + NAT-D (130) + ANBIETER(13) + ANBIETER (13) + KEINE (0) Gesamtlänge: 16824. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP =64.102.156.87, Verarbeitung von Hash-Payload24. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP =64.102.156.87, Verarbeitung von Hash-Payload24. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP =64.102.156.87, Verarbeitung von Hash-Payload	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu	==================================	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu starten.	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 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, Computing-Hash für ISAKMP	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu starten.	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 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	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu starten.	==================================	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu starten.	==================================	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu starten.	==================================	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu starten.	==================================	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu starten.	==================================	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu starten.	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 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, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = 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	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu starten.	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 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. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = 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. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung der NAT-Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung der NAT-Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung der NAT-Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung der NAT-Discovery-Payload	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu starten.	24. August 11:31:03 [IKEv1]IP = 64.102.156.87, EMPFANGENEIKE_DECODE-Nachricht (msgid=0) mit Payloads: HDR + HASH(8) + NOTIFY (11) + NAT-D (130) + NAT-D (130) + ANBIETER(13) + ANBIETER (13) + KEINE (0) Gesamtlänge: 16824. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP =64.102.156.87, Verarbeitung von Hash-Payload24. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP =64.102.156.87, Computing-Hash für ISAKMP24. Aug. 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP =64.102.156.87, Verarbeitung der Benachrichtigungs-Payload24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP =64.102.156.87, Verarbeitung der NAT-Discovery-Payload24. Aug. 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP =64.102.156.87, Verarbeitung der NAT-Discovery-Payload24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP =64.102.156.87, Computing NAT Discovery Hash24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP =64.102.156.87, Verarbeitung der NAT-Discovery-Payload24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP =64.102.156.87, Computing NAT Discovery Hash24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP =64.102.156.87, Verarbeitung der NAT-Discovery-Payload24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP =64.102.156.87, Verarbeitung der NAT-Discovery-Payload24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP =64.102.156.87, Verarbeitung der NAT-Discovery-Payload24. Aug. 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP =64.102.156.87, Computing NAT Discovery Hash	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu starten.	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 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. August 11:31:03 [IKEv1 DEBUG]Gruppe = 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. August 11:31:03 [IKEv1 DEBUG]Gruppe = 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. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Computing NAT Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Computing NAT Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Computing NAT Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Computing NAT Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Computing NAT Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP =	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu starten.	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 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. August 11:31:03 [IKEv1 DEBUG]Gruppe = 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. August 11:31:03 [IKEv1 DEBUG]Gruppe = 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. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung der NAT-Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung der NAT-Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung der NAT-Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung von VID-Payload	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu starten.	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 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. August 11:31:03 [IKEv1 DEBUG]Grupp = 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. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Verarbeitung von VID-Payload 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Verarbeitung von VID-Payload	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu starten.	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 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. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Verarbeitung der NAT-Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Verarbeitung der NAT-Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Verarbeitung der NAT-Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Verarbeitung der NAT-Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Verarbeitung von VID-Payload 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Verarbeitung von VID-Payload 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Verarbeitung von VID-Payload 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Verarbeitung von VID-Payload 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Verarbeitung von VID-Payload	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu starten.	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 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. August 11:31:03 [IKEv1 DEBUG]Gruppe = 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. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung der NAT-Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung der NAT-Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Verarbeitung der NAT-Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = 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]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, Processing IOS/PIX Vendor ID Payload (Version 10.0. Euclifonene: (00002408)	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu starten.	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 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. August 11:31:03 [IKEv1 DEBUG]Gruppe = 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. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Gruppe = 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]Gruppe = ipsec, IP = 64.102.156.87, Processing IOS/PIX Vendor ID Payload (Version 1.0.0, Funktionen: 00000408) 24. August 14:21:02 [IKEv1 DEBUG]Gruppe = ipsec, IP =	
Empfangen von AM3 vom Client. Prozess AM 3. NAT-Traversal (NAT-T) bestätigen Beide Seiten sind nun bereit, die Datenverkehrsverschlüsselung zu starten.	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 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. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Verarbeitung der NAT-Discovery-Payload 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Computing NAT Discovery Hash 24. August 11:31:03 [IKEv1 DEBUG]Grupp = ipsec, IP = 64.102.156.87, Verarbeitung von VID-Payload 24. August 11:31:03 [IKEv1 DEBUG]Grupp = 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]Grupp = ipsec, IP =	

	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 device Dieses Endgerät	
	befindet sich NICHT hinter einem NAT-Gerät	
Initiioron Cio Dhaga 1 5 (XALITH)		╣┝═
Initileren Sie Phase 1.5 (XAUTH),	124. Aug. 11:31:03 [IKEV1 DEBUG]Group = Ipsec, IP =	
und fordern Sie	64.102.156.87, Erstellen einer leeren Hasn-Payload	
Benutzeranmeldeinformationen an.	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	
	======================================	1
	=========>	
	53511:28:30 43008/24/12Sev=Info/4IKE/0x6300014	Ā
	EMPEANG << ISAKMP OAK TRANS *(HASH ATTR) ab	
	64 102 156 88	
	53611:28:30 43108/24/12Sov=Decode/111KE/0x6300001	
	Source 11.20.30.43100/24/1236v-Decode/111KE/0x0300001	
	Responder COOKIE: 1B301D2DE710EDA0	
	Nachste 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 Pavload: Keine	
	Reserviert: 00	
	Pavload-Länge: 20	
	Typ ISAKMP CEG REQUEST	
	Reserviert: 00	
	Kennung: 0000	
	XALITH-Typ: Allgemein	
	XAUTH-Reputzername: (leer)	
	XAUTH Benutzerkennwert: (leer)	
	52711-29:20 42108/24/12Sov=Dobug/7IKE/0x6200076	
	155711.20.50.45100/24/1256V-Debug/TIRE/000500070	
		ļĻ
	153811:28:30.43108/24/12Sev=Debug//IKE/0x63000/6	ll.
	NAV Irace->TM:MsgID=FB709D4DCurState:	llr
	IM_PCS_XAUTH_REQEvent: EV_INIT_XAUTH	T
	53911:28:30.43108/24/12 Sev=Debug/7IKE/0x6300076	B
	NAV Trace->TM:MsgID=FB709D4DCurState:	d
	TM_PCS_XAUTH_REQEvent: EV_START_RETRY_TMR	a

	54011:28:30.43208/24/12Sev=Debug/7IKE/0x6300076	г
	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	
	54211.28:36 41508/24/12Sev=Debug/7IKE/0x6300076	抗
	NAV Trace->TM·MsoID=EB709D4DCurState	
	TM WAIT AUSEREvent EV SND MSG	
	54211:28:26 41508/24/128 ov = lpfo/41/KE/0x6200012	
	SENDEN >>> ISAKMD OAK TDANS */UASH ATTD) his	
	SENDEN ISANINF OAN TRAINS (HASH, ATTR) DIS	
	04.102.100.00	Ċ
	54411.28.30.41508/24/12Sev=Decode/111KE/0x0300001	
		ľ
	Initiator COOKIE:D56197780D7BE3E5	
	Responder COOKIE:1B301D2DE/10EDA0	(
	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 Pavload: Keine	
	Reserviert: 00	
	Pavload-I änge: 33	
	Typ: ISAKMP CEG REPLY	
	Reserviert: 00	
	Kennung: 0000	
	XALITH-Typ: Allgemein	
	XALITH-Benutzername: (Daten werden nicht angezeigt)	
	XAUTH-Benutzerkennwort: (Daten werden nicht angezeigt)	
		╢╴
Emplangen von	24. August 11.31.09 [INEVI]IP = 04.102.150.87, EMPFANGENE	
Benutzeranmeideinformationen.		
	+ HASH(8) + ATTR(14) + KEINE(0)	
	Gesamtlange: 85	
	24. Aug. 11:31:09 [IKEv1 DEBUG]Group = ipsec, IP =	
	64.102.156.87, process_attr(): Geben Sie ein!	
Verarbeitung von	24. August 11:31:09 [IKEv1 DEBUG]Gruppe = ipsec, IP =	
Benutzeranmeldeinformationen.	64.102.156.87, Processing MODE_CFG Reply-Attribute.	
Überprüfen Sie die	24. August 11:31:09 [IKEv1 DEBUG]Gruppe = ipsec,	
Anmeldeinformationen, und	Benutzername = user1, IP = 64.102.156.87,	
generieren Sie die	IKEGetUserAttributes: Primäres DNS = 192.168.1.99	
Moduskonfigurationsnutzlast.	24. August 11:31:09 [IKEv1 DEBUG]Gruppe = ipsec,	
Relevante Konfiguration:	Benutzername = user1, IP = 64.102.156.87,	
		_

	KEGetUserAttributes: Sekundärer DNS = gelöscht	
username cisco	24. August 11:31:09 [IKEv1 DEBUG]Gruppe = ipsec,	
password cisco	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 = ivoungta-	
	labdomain cisco com	
	21 August 11:31:00 [[KEv1 DEB]]G]Gruppe = insec	
	$P_{\text{abstrace}} = P_{\text{abstrace}} = P_{\text{abstracee}} = P_{\text{abstracee}} = P_{\text{abstrace}} = P_{\text{abstrace}} = P_{abs$	
	Benutzemame – useri, IF – 04.102.150.07,	
	IKEGelUserAllinbules: IP-Komphinierung = deakliviert	
	24. August 11:31:09 [IKEV1 DEB0G]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,	
	<pre>IKEGetUserAttributes: Browserproxy-Einstellung = keine</pre>	
	Anderung 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,	٦
	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 gm-	
	Hash-Pavload	
	24 August 11:31:09 [[KEv1]]P = 64 102 156 87 [KE DECODE-	
	SENDING-Nachricht (msgid=5b6910ff) mit Pavloads: HDR +	
	HASH(8) + ATTR(14) + KEINE(0) Gesantlänge: 64	
		4
	54511:28:36.41608/24/12Sev=Debug/7KE/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	

	ISAKMP-Header	
	Initiator COOKIE:D56197780D7BE3E5	
	Responder COOKIE:1B301D2DE710EDA0	
	Nächste Pavload: Hash	
	Ver. (Hex):10	
	Exchange-Typ: Transaktion	
	Elags (Verschlüsselung)	
	MessageID(Hex):5B6910FF	
	Länge: 76	
	Pavload-Hash	
	Nächste Pavload: Attribute	
	Reserviert: 00	
	Pavload-Länge: 24	
	Daten (in Hex):	
	7DCE47827164108731630BEB7505E604C0DEE85	
	Povload Attributo	
	Nächste Devlaad: Keine	
	Deservicet 00	
	Reservent. 00	
	Typ: ISAKMP_CFG_SET	
	XAUTH-Status: Pass	
	55011:28:36.42508/24/12Sev=Debug//IKE/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	A
	SENDEN >>> ISAKMP OAK TRANS *(HASH, ATTR) bis	
	64.102.156.88	
	<===================================	Ī
Empfangen und Verarbeiten von	24. August 11:31:09 [IKEv1]IP = 64.102.156.87. EMPFANGENE	╡┣╴
ACK. Keine Antwort vom Server	IKE DECODE-Nachricht (msgid=5b6910ff) mit Pavloads: 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 = insec	
	Benutzername = Benutzer1 IP = 64 102 156 87 Verarbeitung	
	der ofg ACK-Attribute	
	55511:28:36 / 2608/2//12Sev=Debug/7IKE/0x6300076	
	NΔV Trace->TM·MedID=5R6010EECurState	
	TM XALITH DONEvent	
	55611.28.36 42608/24/12Sav=Dabua/71KE/0x6200076	d
	NAV Trace STM: MedD-5860105500070	lo lo
	TM VALITE DONEWOOT EV NO EVENT	
	55711:29:26 42608/24/128 av=Dabua/7///E/0v6200076	
	100/11.20.00.42000/24/125ev=Debug//1KE/0x03000/0	
	IINAV TTACE-ZTWINSGID=FB709D4DCUrState:	

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->SAIL Cookie=D56197780D7BE3E5	
R Cookie=1B301D2DE710EDA0CurState	
CMN XAUTH PROGEvent EV XAUTH DONE SUC	
56111:28:38 /0608/2//12Sev=Debug/8lKE/0x63000/C	
Starten des DPD-Timers für IKE SA	
(1 Cooking - D56107780 D7RE2E5)	
$(1_{COOKie} = D_{COOKie} = D_{COOKie} = 1_{COOKie}$	
$R_{OOKIE-1D301D2DE710EDA0}$ sa->siale - 1, sa-	
$ ^{2}upu.care_ireq(insec) = 5000$	
50211.28.38.40008/24/125ev=Debug//INE/0x0300076	
56311:28:38.40608/24/12Sev=Debug//IKE/0x6300076	
NAV Trace->SA:I_Cookie=D5619/780D/BE3E5	
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	S
NAV Trace->TM:MsgID=84B4B653CurState:	k
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 Pavload: Hash	
Ver (Hev):10	
Exchange-Typ: Transaktion	
Elage (Vorschlüssolung)	
MoscogolD/Hox):94R4R653	
IIVIESSAYEID(TIEX).040400000	
Payload-Hash	
Nachste Payload: Attribute	
Reserviert: 00	

			—
	Payload-Lange: 24		l
	Daten (in Hex):		l
	81BFBF6721A744A815D	069A315EF4AAA571D6B687	
	Payload-Attribute		l
	Nächste Payload: Keine		l
	Reserviert: 00		l
	Payload-Länge: 131		
	Typ: ISAKMP_CFG_REC	QUEST	l
	Reserviert: 00		
	Kennung: 0000		l
	IPv4-Adresse: (leer)		l
	IPv4-Netzmaske: (leer)		l
	IPv4-DNS: (leer)		l
	IPv4-NBNS (WINS): (lee	r)	Ì
	Ablaufdatum der Adresse) (leer)	l
	Cisco Erweiterung: Bann	er: (leer)	l
	Cisco Erweiterung: PWD	speichern: (leer)	Ì
	Cisco Enveiterung: Stan	lard-Domänenname: (leer)	l
	Cisco Envoitorung: Aufto	ilon: (loor)	Ì
	Cisco Envoitorung: DNS	Nomen auffeilen: (leer)	Ì
	Cisco Erweiterung: DNS-		l
	CISCO Erweiterung. PFS.	(leer)	l
			l
	Cisco Erweiterung: Backi	up-Server: (leer)	l
	Cisco Erweiterung: Entre	rnen der Smartcard: (leer)	l
	Anwendungsversion: Cis	co Systems VPN Client	l
	5.0.07.0290:WinNT		l
	Cisco Erweiterung: Firew	/all-Typ: (leer)	l
	Cisco Erweiterung: Dyna	mischer DNS-Hostname: ATBASU-	l
	LABBOX		
	<=========	==== Mode-config-Anforderung	-
	==	==============	l
Anforderung für die	24. Aug. 11:31:11	57011:28:38.62808/24/12Sev=	٧
Empfangsmodus-Konfiguration.	[IKEv1]IP	Debug/7IKE/0x6300076	S
	= 64.102.156.87.	NAV Trace-	
	EMPFANGENE	>TM:MsgID=84B4B653CurState:	l
	IKE DECODE-Nachricht	TM WAIT MODECEGREPI YEvent	l
	(msgid=84b4b653) mit	EV NO EVENT	l
	Pavloads: HDR + HASH		l
	$(8) + \Delta TTR (14) +$		
	(0) (1)		l
	Cosamtlängo: 183		l
			l
	[IKEVI DEBOG]Group =		l
	ipsec, Username =		
			l
	64.102.156.87,		l
	process_attr(): Geben		l
	Sie ein!		
Prozess-Konfigurationsanforderung.	24. August 11:31:11 [IKE	v1 DEBUG]Gruppe = ipsec,	
Viele dieser Werte werden	Benutzername = user1, I	P = 64.102.156.87, Verarbeiten der	Ì
normalerweise in der	Attribute cfg Request		
Gruppenrichtlinie konfiguriert. Da	24. August 11:31:11 [IKE	v1 DEBUG]Gruppe = ipsec,	
	-		

der Server in diesem Beispiel	Benutzername = Benutzer1, IP = 64.102.156.87, MODE CFG:
iedoch über eine sehr einfache	Erhaltene Anfrage für IPv4-Adresse!
Konfiguration verfügt, werden sie	24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec.
hier nicht angezeigt	Benutzername = Benutzer1 IP = 64 102 156 87 MODE CEG
	Empfangene Anfrage für die IPv4-Netzmaske!
	24 August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec
	Benutzername = Benutzer1 IP = 64 102 156 87 MODE CEG:
	Empfangene Anfrage für DNS-Serveradressel
	24 August 11:31:11 [[KEy1 DEB] [G]Gruppe = insec
	Bonutzornamo - Bonutzor1 JP - 64 102 156 87 MODE CEC:
	Erbaltono Anfrago für WINS Sonvoradrossol
	24 August 11:21:11 [[KEy1]Croup = income Linerrame = upor1
	ID = 64,102,156,87 Bosoived unsupported transaction mode
	attributes 5
	[24. August 11:31:11 [IKEVI DEBUG]Gluppe = Ipsec,
	Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG:
	24. August 11:31:11 [IKEV1 DEBUG]Gruppe = ipsec,
	Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG:
	Emptangene Antrage für die PW-Einstellung speichern!
	24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec,
	Benutzername = Benutzer1, IP = 64.102.156.87, MODE_CFG:
	Emptangene Antrage 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:
	Emptangene Antorderung 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 Iautet: ATBASU-LABBOXI Erstellen Sie eine mode-config- Antwort mit allen konfigurieten 24. Aug. 11:31:11 [IKEV1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, SPAdresse (H20.156.87, Senden der Subnetzmaske (252.252.250.0) an den Remote-Client 24. August 11:31:11 [IKEV1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Senden der Subnetzmaske (252.252.250.0) an den Remote-Client 24. August 11:31:11 [IKEV1 DEBUG]Gruppe = ipsec, Benutzername = Benutzername = Benutzer1, IP = 64.102.156.87, Senden der Subnetzmaske (252.252.250.0) an den Remote-Client 24. August 11:31:11 [IKEV1 DEBUG]Gruppe = ipsec, Username = Benutzern.IP = 64.102.156.87, Zugewiesene private IP-Adresse differentiation in Cisco. Com 25.353.35.0 user1, IP = 64.102.156.87, Stellen einer Hash-Payload 24. August 11:31:11 [IKEV1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Riename = iyoungta-labdomain.cisco.com 24. August 11:31:11 [IKEV1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Browser-Proxy auf "No-Modify" (Kein Andern) eingestellt. Browser-Proxy auf "No-Modify			
Erstellen Sie eine mode-config- Antwort mit allen konfigurieten 24. Aug. 11:31:11 [IKEV1 DEBUG]Gruppe = ipsec. Benutzername = Benutzer1, IP = 64.102.156.87, IP-Adresse (IP2.168.1.100) vor dem Initizen von Modus-Cfg (XAuth) aktivieri) In diesen Fall wird dem Benutzer immer die gleiche IP zugewiesen. Senutzername = Benutzer1, IP = 64.102.156.87, Senutzername = Benutzername = Benutzer1, IP = 64.102.156.87, Senutzername = Benutzername = Benutzer1, IP = 64.102.156.87, Senutzername = Benutzer1, IP = 64.102.156.87, Zugewiesene private IP-Adresse (JS 2.58.1.100) S55.255.255.255.255.255.255.255.255.255.		Die empfangene Anfrage für den DHCP-Hostnamen für DDNS lautet: ATBASU-LABBOX!	
Antwort mit allen konfigurierten Werten. Relevante Konfiguration: In diesem Fall wird dem Benutzer immer die gleiche IP zugewiesen. Benutzername = Benutzer, 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 = benutzer, IP = 64.102.156.87, Clean der Subnetzmaske (255.255.25) an den Remote-Client 24. August 11:31:11 [IKEV1]Gruppe = ipsec, Benutzername = benutzer, IP, = 64.102.156.87, Cugewiesene private IP-Adresse 192.168.1.100 für Remote-Benutzer 24. August 11:31:11 [IKEV1 DEBUG]Gruppe = ipsec, Username = user1, IP = 64.102.156.87, construct ofg. sec, Username = user1, IP = 64.102.156.87, Construct ofg. sec, Username = 24. August 11:31:11 [IKEV1 DEBUG]Gruppe = ipsec, Benutzername = lesent, 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, Clientbrowser- Proxy-Attribute senden! 24. August 11:31:11 [IKEV1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, 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, Clientbrowser- Proxy-Attribute senden! 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 = user1, IP = 64.102.156.87, Cliesco Smantzard- Entfernung aktivieren! 24. August 11:31:11 [IKEV1]DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Cliesco Smantzard- Entfernung aktivieren! 24. August 11:31:11 [IKEV1]DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Cliesco Smantzard- Entfernung aktivieren! 24. August 11:31:11 [IKEV1]DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Cliesco Smantzard- Entfernung aktivieren! 24. August 11:31:11 [IKEV1]DEBUG]Gruppe = ipsec, Benutzername = user1,	Frstellen Sie eine mode-config-	24 Aug 11:31:11 [IKEv1 DEBUG]Gruppe = insec	
Werten. (192.168.1.100) vor dem Initiieren von Modus-Cfg (XAuth) Relevante Konfiguration: (192.168.1.100) vor dem Initiieren von Modus-Cfg (XAuth) aktiviert) (192.168.1.00) vor dem Initiieren von Modus-Cfg (XAuth) aktiviert) (192.168.100) vor dem Initiieren von Modus-Cfg (Xauth) aktiviert)	Antwort mit allen konfigurierten	Benutzername = Benutzer1 IP = 64 102 156 87 IP-Adresse	
Refevante Konfiguration: In diesem Fall wird dem Benutzer In diesem Fall wird dem Benutzer 24. August 11:31:11 [IKEV1 DEBUG]Gruppe = ipsec, Benutzername Clasco SubnetZmaske (255:255:0) an den Remote-Client 24. August 11:31:11 [IKEV1 DEBUG]Group = ipsec, Benutzername = S5:25:35:35:0 24. August 11:31:11 [IKEV1 DEBUG]Group = ipsec, Username = 9roup-policy mz 24. August 11:31:11 [IKEV1 DEBUG]Group = ipsec, Username = 9roup-policy mz 24. August 11:31:11 [IKEV1 DEBUG]Group = ipsec, Username = 9roup-policy mz 24. August 11:31:11 [IKEV1 DEBUG]Group = ipsec, 9roup-policy mz 24. August 11:31:11 [IKEV1 DEBUG]Group = ipsec, 9roup-policy mz 24. August 11:31:11 [IKEV1 DEBUG]Group = ipsec, 9roup-tunel-portocol. 24. August 11:31:11 [IKEV1 DEBUG]Group = ipsec, 1abdemain. ciaco.com <td>Werten</td> <td>(192 168 1 100) vor dem Initijeren von Modus-Cfg (XAuth)</td> <td></td>	Werten	(192 168 1 100) vor dem Initijeren von Modus-Cfg (XAuth)	
In diesem Fall wird dem Benutzer immer die gleiche IP zugewiesen. 24. August 11:31:11 [IKEV1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Senden der Stubetzmaske (255.255.250) an den Remote-Client username cisco attributes ypn-framed-lp- address 192.168.1.100 24. August 11:31:11 [IKEV1 DEBUG]Group = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Cugewiesene private IP-Adresse 192.168.1.100 für Remote-Benutzer 25.255.255.05 group-policy mz interval group-policy mz attributes 24. Aug.11:31:11 [IKEV1 DEBUG]Group = ipsec, Username = group-policy mz attributes 24.3.21.21 11:31:11 [IKEV1 DEBUG]Group = ipsec, Username = group-policy mz attributes 24. Aug.11:31:11 [IKEV1 DEBUG]Group = ipsec, Username = group-policy mz attributes 25.108.1.129 P = 64.102.156.87, Construct_cfg_set.Standard-Domäne group-policy mz attributes 24. August 11:31:11 [IKEV1 DEBUG]Groupe = ipsec, genutzemame = user1, IP = 64.102.156.87, Clientbrowser- Proxy-Attribute senden! 24. August 11:31:11 [IKEV1 DEBUG]Groupe = ipsec, genutzemame = user1, IP = 64.102.156.87, Clientbrowser- Proxy-Attribute senden! 24. August 11:31:11 [IKEV1 DEBUG]Groupe = ipsec, Benutzername = user1, IP = 64.102.156.87, Clientbrowser- Proxy-Attribute senden! 24. August 11:31:11 [IKEV1 DEBUG]Groupe = ipsec, Benutzername = user1, IP = 64.102.156.87, Clientbrowser- Proxy-Attributes 25.21:23.236.3300/24/24/24/24/24/24/24/24/24/24/24/24/24/	Relevante Konfiguration:	aktiviert)	
Immer die gleiche IP zugewiesen. En utzername = Benutzer1, IP = 64, 102, 156, 87, Senden der Subnetzmaske (255, 255, 05, 0) an den Remote-Client 44. August 113:111 [IKEVI DEBUG]Group = ipsec, Username = Benutzer1, IP = 64, 102, 156, 87, Zugewiesene private IP-Adresse 192, 168, 1.100 für Remote-Benutzer 44. Aug. 113:111 [IKEVI DEBUG]Group = ipsec, Username = user1, IP = 64, 102, 156, 87, Construct, cig, set: Standard-Domäne = jyoungta-labdomain.cisco.com 24. August 11:31:11 [IKEVI DEBUG]Group = ipsec, Benutzername = user1, IP = 64, 102, 156, 87, Clientbrowser- Proxy-Attribute senden! vanisht value 23. 168, 1.129 Pa 64, 102, 156, 87, construct, cig, set: Standard-Domäne = jyoungta-labdomain.cisco.com 24. August 11:31:11 [IKEVI DEBUG]Groupe = ipsec, Benutzername = user1, IP = 64, 102, 156, 87, Clientbrowser- Proxy-Attribute senden! vanisht value 24. August 11:31:11 [IKEVI DEBUG]Groupe = ipsec, Benutzername = user1, IP = 64, 102, 156, 87, Clientbrowser- Proxy-Attribute senden! vanisht value 24. August 11:31:11 [IKEVI DEBUG]Groupe = ipsec, Benutzername = user1, IP = 64, 102, 156, 87, Cisco Smartcard- Entfernung aktivieren! 24. Aug. 11:31:11 [IKEVI DEBUG]Groupe = ipsec, Benutzername = user1, IP = 64, 102, 156, 87, Cisco Smartcard- Entfernung aktivieren! 24. August 11:31:11 [IKEVI DEBUG]Group = ipsec, Username = user1, IP = 64, 102, 156, 87, Erstellen von qm-Hash-Payload Antwort "mode-config" senden. 24. August 11:31:11 [IKEVI DEBUG]Group = ipsec, Benutzername = User1, IP = 64, 102, 156, 87, Cisco Smartcard- Entfernung aktivieren! 24. August 11:31:11 [KEVI DEBUG]Group = ipsec, Benutzername = User1, IP = 64, 102, 156, 88, Fistellen von qm-Hash-Payload Antwort "mode-config" senden. 24. August 11:31:11 [KEVI DEBUG]Group = ipsec, Benutzername = User1, IP = 64, 102,	In diesem Fall wird dem Benutzer	24 August 11:31:11 [[KEv1 DEB] [G]Gruppe = insec	
Initiate of egicite in 20gewiesen: Subnetzmaske (255.255.255.0) an den Remote-Client username cisco 24. August 11:31:11 [IKEv1]Gruppe = ipsec, Benutzername = grup-standel-3p- address 192.168.1.100 storestand 24. August 11:31:11 [IKEv1]Gruppe = ipsec, Benutzername = grup-policy Ex usern, IP = 64.102.156.87, Construct_cfg_set: Standard-Domäne = uscorp-olicy Fx user1, IP = 64.102.156.87, construct_cfg_set: Standard-Domäne = usernal protocol 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, construct_cfg_set: Standard-Domäne = user1, IP = 64.102.156.87, Clientbrowser- Pro-tune1-policy Enutzername = Benutzer1, IP = 64.102.156.87, Clientbrowser- Provy-Attribute sendeni 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Cisco Smartcard- Ist value spit default- 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, Benutzername = user1, IP = 64.102.156.87, Cisco Smartcard- Internal-network- 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, Benutzername = user1, IP = 64.102.156.87, Cisco Smartcard- Internal-network- 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, Strintizername = user1, IP = 64.102.156.87, Cisco Smartcard- Entferming aktivieren! 24	immor dio gloicho IP zugowioson	Boputzornamo - Boputzor1 $IP = 64,102,156,87$ Sondon dor	
username cisco 24. August 11:31:11 [IKEv1]Gruppe = ipsec, Benutzername = str:buce Benutzer1, IP = 64.102.156.87, Zugewiesene private IP-Adresse address 192.168.1.100 24. Aug. 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Erstellen einer leeren Hash-Payload iternal 24. Aug. 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Cristellen einer leeren Hash-Payload iternal 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Construct_cfg_set: Standard-Domäne ipyongta-bedomain.cisco.com 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, enutzername = user1, IP = 64.102.156.87, Browser-Proxy gilt-tumel-policy 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, ummelail 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, gilt-tumel-policy 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, ummelail 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, gilt-tumel-policy 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, ummelail 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, gilt-tumel-policy 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, ummelail 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, seconder Config" senden. </td <td>inniner die gleiche if Zugewiesen.</td> <td>Subnetzmaske (255.255.255.0) an den Remote-Client</td> <td></td>	inniner die gleiche if Zugewiesen.	Subnetzmaske (255.255.255.0) an den Remote-Client	
attributes Benutzer1, IP = 64.102.156.87, Zugewiesene private IP-Adresse address 192.168.1.100 Ya. Aug. 11:31:11 [IKEV1 DEBUG]Group = ipsec, Username = group-policy HZ user1, IP = 64.102.156.87, Construct_ofg_set: Standard-Domäne attributes user1, IP = 64.102.156.87, construct_ofg_set: Standard-Domäne paseword-storage 24. Aug. 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, construct_ofg_set: Standard-Domäne = youngta-abdomain.cisco.com 24. August 11:31:11 [IKEv1 DEBUG]Grouppe = ipsec, galt14.119 Proxy-Attribute senden! kev1 Benutzername = user1, IP = 64.102.156.87, Browser-Proxy-Daten worden Naho 24. August 11:31:11 [IKEv1 DEBUG]Grouppe = ipsec, goungta- Benutzername = Benutzer1, IP = 64.102.156.87, Browser-Proxy-Daten worden Naho 24. August 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, goungta- Benutzername = user1, IP = 64.102.156.87, Cisco Smartcard- Internant value 24. August 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, goungta- 24. August 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, goungta- Benutzername = user1, IP = 64.102.156.87, Cisco Smartcard- Entferning atkivieren! 24. August 11:31:11 [IKEv1 DEBUG]Groupe = ipsec, goungta- Standard-	username cisco	24. August 11:31:11 [IKEv1]Gruppe = ipsec, Benutzername =	
vpn-framed-ip- address 12: 168.1.100 192.168.1.100 für Remote-Benutzer 255.255.0 192.168.1.100 für Remote-Benutzer 24. Aug. 11:31:11 [IKEV1 DEBUG]Group = ipsec, Username = uscrt, IP = 64.102.156.87, Erstellen einer leeren Hash-Payload 24. Aug. 11:31:11 [IKEV1 DEBUG]Group = ipsec, Username = usert, IP = 64.102.156.87, construct_cfg_st: Standard-Domäne = jyoungta-labdomain.cisco.com 24. August 11:31:11 [IKEV1 DEBUG]Groupe = ipsec, enableds-server vulue 12.168.1.129 1901t-tume1-policy tumnelall opilt-tume1-policy tumnelall opilt-tume1-policy tumnelall 201t-tume1-policy tumnelall opilt-tume1-policy tumnelall 201t-tume1-policy tumnelall 201t-tume1-policy tumnelall 201t-tume1-policy tumnelall 201t-tume1-policy tumnelall 201t-tume1-policy tumnelall 201t-tume1-policy tumnelall 201t-tume1-policy tumnelall 201t-tume1-policy tumnelan.cisco.com 24. Aug. 11:31:11 [IKEV1 DEBUG]Group = 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, Cisco Smartcard- Entfernung aktivieren! 24. Aug. 11:31:11 [IKEV1 DEBUG]Group = ipsec, Username = 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,	attributes	Benutzer1, IP = 64.102.156.87, Zugewiesene private IP-Adresse	
address 192.185.1100 24. Aug. 11:31:11 [IKEV1 DEBUG]Group = ipsec, Username = group-policy EZ user1, IP = 64.102.156.87, Erstellen einer leeren Hash-Payload attributes = jyoungta-labdomain.cisco.com analedms-protocol 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 analedms-protocol law pilt-tunnel-protocol law pilt-tunnel-inetwork- late value grid default- domain value givoungta- labdomain.cisco.com labdomain.cisco.com Antwort "mode-config" senden. 24. August 11:31:11 [IKEV1 DEBUG]Group = ipsec, genutzername = user1, IP = 64.102.156.87, IKE_DECODE- SENDING-Nachricht (msgid=84dxb653) mit Payload Antwort "mode-config" senden. 24. August 11:31:11 [IKEV1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKE_DECODE- SENDING-Nachricht (msgid=84dxb653) mit Payload Antwort "mode-config" senden. 24. August 11:31:11 [KEV1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Erstellen von qm-Hash-Payload Antwort "mode	vpn-framed-ip-	192.168.1.100 für Remote-Benutzer	
user1, P = 64.102.156.87, Erstellen einer leeren Hash-Payload urour-policy Ez attributes password-storage enabladne-server value 12.16.1.129 vpn-tumel-policy prit-tumel-policy prit-tumel-network- ista ista prit-tumel-network- ista ista prit-tumel-network- ista i	address 192.168.1.100	24. Aug. 11:31:11 [IKEv1 DEBUG]Group = ipsec. Username =	
Internal 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 1st_tilutes persword-storage 24. Aug. 11:31:11 [IKEv1 DEBUG]Groupp = ipsec, Benutzername = user1, IP = 64.102.156.87, Clientbrowser- Proxy-Attribute senden! 24. Aug. 11:31:11 [IKEv1 DEBUG]Groupp = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Browser-Proxy auf "No-Modify" (Kein Andern) eingestellt. Browser-Proxy-Daten werden NICHT in die mode-cfg-Antwort aufgenommen. 24. Aug. 11:31:11 [IKEv1 DEBUG]Groupp = ipsec, Benutzername = user1, IP = 64.102.156.87, Cisco Smartcard- Enffernung aktivieren! 24. Aug. 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Cisco Smartcard- Enffernung aktivieren! 24. Aug. 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Cisco Smartcard- Enffernung aktivieren! 24. Aug. 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Cisco Smartcard- Enffernung aktivieren! 24. Aug. 11:31:11 [IKEv1]DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Cisco Smartcard- Enffernung aktivieren! 257111:28:38.63808/24/12Sev=Info/5/IKE/0Xc630002F Empfangenes ISAKMP-Paket: peer = 64.102.156.88 S7311:28:38.63808/24/12Sev=Info/5/IKE/0Xc6300001 ISAKMP-Header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:13301D2DE710EDA0 Nächste Payload: Hash Ver. (Hex):10 ExAnge : 2yload-Hash Nächste Payload: Attribute Re	group-policy EZ	user1. IP = 64.102.156.87. Erstellen einer leeren Hash-Pavload	
group-policy E2 distributes password-storage enabledras-server value 132.166.1129 vpn-tunnel-protocol likevi aplit-tunnel-policy tunnetall aplit-tunnel-network- list value split default- domain.cisco.com 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Cilentbrowser- Proxy-Attributes senden! 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Browser-Proxy auf "No-Modify" (Kein Ändern) eingestell. 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]Grupp = ipsec, Username = user1, IP = 64.102.156.87, Erstellen von gm-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	internal	24. Aug. 11:31:11 [IKEv1 DEBUG]Group = ipsec. Username =	
attributes password-storage enabledna-server value 132.168.1.129 wp-tume1-protocol iker1 aplit-tume1-policy tume1all aplit-tume1-policy tume1all aplit-tume1-network- labdomain.cisco.com 24. August 11:31:11 [IKEV1 DEBUG]Gruppe = ipsec, Benutzername = user1, 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. August 11:31:11 [IKEV1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Cisco Smartcard- Entfernung aktivieren! 24. August 11:31:11 [IKEV1 DEBUG]Grupp = ipsec, Username = user1, IP = 64.102.156.87, Cisco Smartcard- Entfernung aktivieren! 24. August 11:31:11 [IKEV1]DEBUG]Grupp = ipsec, Username = user1, IP = 64.102.156.87, IKE_DECODE- SENDING-Nachricht (msgid=84b4b653) mit Payloads: HDR + HASH (8) + ATTR (14) + KEINE (0) Gesamtlänge: 215	group-policy EZ	user1 IP = 64 102 156 87 construct cfg set Standard-Domäne	
password-storage 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, 192.168.1.129 Benutzername = user1, IP = 64.102.156.87, Clientbrowser- vpn-tunnel-protocol Proxy-Attribute senden! 1kori 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, split-tunnel-protocol Benutzername = Benutzer1, IP = 64.102.156.87, Clientbrowser- ikori Split-tunnel-network- ist value split default- Worden NICHT in die mode-cfg-Antwort aufgenommen. 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Cisco Smartcard- Iabdonain.cisco.com Benutzername = user1, IP = 64.102.156.87, Cisco Smartcard- Infernung aktivieren! 24. August 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 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKE_DECODE- SENDING-Nachricht (msgid=84b4b653) mit Payloads: HDR + HASH (8) + ATTR (14) + KEINE (0) Gesamtlange: 215 Image: SAKMP-Paket: peer = 64.102.156.88 57211:28:38.63808/24/12Sev=Info/sIKE/0x630002F Empfangenes ISAKMP-Paket: peer = 64.102.156.88 57311:28:38.63808/24/12Sev=Info/sIKE/0x630001 ISAKMP-Header Initiator COOKIE:IB301D2DE710EDA0 Nächste Payload: Hash<	attributes	= ivoungta-labdomain cisco com	
Pinable of Server Value Demogram = user1, IP = 64.102.156.87, Clientbrowser- Vpn-tunnel-protocol Servizername = user1, IP = 64.102.156.87, Clientbrowser- Proxy-Attribute senden! 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Browser-Proxy auf "No-Modify" (Kein Ändern) eingestellt. Browser-Proxy-Daten Virus alue 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, Cisco Smartcard- Labdomain.cisco.com 24. August 11:31:11 [IKEv1 DEBUG]Groupp = ipsec, Matwort "mode-config" senden. 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, Senutzername = user1, IP = 64.102.156.87, IKE_DECODE- SENDING-Nachricht (msgid=84b4b653) mit Payload Antwort "mode-config" senden. 24. August 11:31:11 [IKEv1]DEBUG]Group = ipsec, Sort11:28:38.63808/24/12Sev=Info/SIKE/0x630002F E Empfragenes ISAKMP-Paket: peer = 64.102.156.88 57211:28:38.63808/24/12Sev=Info/SIKE/0x6300014 EMPFANG << ISAKMP OAK TRANS *(HASH, ATTR) ab	password-storage	24 August 11:31:11 [[KEv1 DEB] [G]Gruppe = ipsec	
Image: State Stat	enabledns-server value	Benutzername = user1 $IP = 64 \ 102 \ 156 \ 87 \ Clientbrowser-$	
izev1 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, gplit-tunnel-network- Benutzername = Benutzer1, IP = 64.102.156.87, Browser-Proxy-Daten werden NICHT in die mode-cfg-Antwort aufgenommen. 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, gpuit-tunnel-network- Benutzername = user1, IP = 64.102.156.87, Cisco Smartcard- labdomain.cisco.com Enternung aktivieren! 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, Benutzername = user1, IP = 64.102.156.87, Cisco Smartcard- Antwort "mode-config" senden. 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, SENDING-Nachricht (msgid=84b4b653) mit Payload 24. August 11:31:11 [IKEv1 DEBUG]Group = ipsec, SENDING-Nachricht (msgid=84b4b653) mit Payloads: HDR + HASH (8) + ATTR (14) + KEINE (0) Gesamtlänge: 215 SENDING-Nachricht (msgid=84b4b653) mit Payloads: HDR + HASH (8) + ATTR (14) + KEINE (0) Gesamtlänge: 215 SENDING-Nachricht (msgid=84b4b653) mit Payloads: HDR + HASH (8) + ATTR (14) + KEINE (0) Gesamtlänge: 215 SENDING-Nachricht (msgid=84b4b653) Fort11:28:38.63808/24/12Sev=Info/5IKE/0x630002F E Empfangenes ISAKMP-Paket: peer = 64.102.156.88 Fort11:28:38.63808/24/12Sev=Info/4IKE/0x6300001 N SAKMP-Header Initiator COOKIE:D56197780D7BE3E5 Responder COOKIE:D56197780D7BE3E5 Responder COOKIE:D56197780D7BE3E5 Responder COOKIE:D56197780D7BE3	vpn-tunnel-protocol	Proxy-Attribute senden!	
aplit-tunnel-policy tunnelall split-tunnel-network- list value split default- domain value iyoungta- labdonain.cisco.com Antwort "mode-config" senden. 24. August 11:31:11 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = user1, IP = 64.102.156.87, 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, Istes Benutzername = user1, IP = 64.102.156.87, IKE_DECODE- SENDING-Nachricht (msgid=84b4b653) mit Payloads: HDR + HASH (8) + ATTR (14) + KEINE (0) Gesamtlänge: 215 Image: Senden. 24. August 11:33:111 [IKEV1 DEBUG]Group = ipsec, Stritt:28:38.63808/24/12Sev=Info/5IKE/0x630002F Empfangenes ISAKMP-Paket: peer = 64.102.156.88 S7211:28:38.63808/24/12Sev=Info/5IKE/0x6300001 ISAKMP-Paket: peer = 64.102.156.88 S7311:28:38.63908/24/12Sev=Decode/11IKE/0x6300001 ISAKMP-Paket: peer = 64.102.156.88 S7311:28:38.63908/24/12Sev=Decode/11IKE/0x6300001 ISAKMP-Paket: peer = 64.102.156.81 Pintiator COOKIE:D56197780D7BE3E5 Responder COOKIE:1B301D2DE710EDA0 Nächste Payload: H	ikev1	21 August 11:31:11 [[KEv1 DEB]]G]Gruppe = insec	
tunnelall Definitions = Definited = Definited = Definited = Definitions = Definitions = Definiti	split-tunnel-policy	Benutzername = Benutzer1 $IP = 61.102.156.87$ Browser-Proxy	
split-tunnel-network- list value split default- domain value jyoungta- labdomain.cisco.com Antwort "mode-config" senden. 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. Aug.11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Erstellen von qm-Hash-Payload 24. Aug.11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Erstellen von qm-Hash-Payload 24. Aug.11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKE_DECODE- SENDING-Nachricht (msgid=84b4b653) mit Payloads: HDR + HASH (8) + ATTR (14) + KEINE (0) Gesamtlänge: 215 ====================================	tunnelall	auf "No Modify" (Koin Ändern) eingestellt Browser Proxy Daten	
Itst value spirt deraute- domain value dyoungta- labdomain.cisco.com 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]Gruppe = 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 Image: senden in the induce config-Antwort ====================================	split-tunnel-network-	wordon NICHT in dia mada cfa Antwort aufaanamman	
Jabdomain.cisco.com 24. Adg. 11.31.11 [IKEV1 DEBOGISIUPpe = 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) Gesamtänge: 215 Image: team in the image is the imag	domain value	24 Aug. 11:31:11 [[KEy1 DERLIC]Gruppo = incoc	
Tabdomain.cisco.com Bendizernane = user1, IP = 04.102.136.87, Cisco Sinancalo 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. Aug. 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 Image: Sender in the intervent of	ivoungta-	24. Aug. 11.31.11 [IKEVI DEBOG]Gluppe – Ipsec,	
24. Aug. 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Erstellen von qm-Hash-PayloadAntwort "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 EXEMPTION: 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: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):	labdomain.cisco.com	Entformung aktivioren	
24. Adg. 11.31.11 [IKEV1 DEOG]GIOUG - ipsec, osemanie - 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 ====================================		Entiemung aktivieren:	
Idself 1, IP - 64.102.136.37, IEstelleri von qhi-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 ==================================		24. Aug. 11.31.11 [IKEVI DEBOG]GIOUP - Ipsec, Osername -	
Antwort "mode-contig" senden. 24. August 11:31:11 [IREVIIP = 64.102.156.87, IRE_DECODE-SENDING-Nachricht (msgid=84b4b653) mit Payloads: HDR + HASH (8) + ATTR (14) + KEINE (0) Gesamtlänge: 215 Image: senden. Image: senden. Image: senden. Image.			
SENDING-Nachricht (msgld=84b4b653) mit Payloads: HDR + HASH (8) + ATTR (14) + KEINE (0) Gesamtlänge: 215 ====================================	Antwort "mode-config" senden.	24. August 11:31:11 [IKEV1]IP = $64.102.156.87$, IKE_DECODE-	
HASH (8) + ATTR (14) + KEINE (0) Gesamtiange: 215 ====================================		SENDING-Nachricht (msgid=84040653) mit Payloads: HDR +	
Image: construct construction image: construction Signal Construction Signal Const		HASH (8) + ATTR (14) + KEINE (0) Gesamtiange: 215	
57111:28:38.63808/24/12Sev=Info/5IKE/0x630002F E Empfangenes ISAKMP-Paket: peer = 64.102.156.88 F 57211:28:38.63808/24/12Sev=Info/4IKE/0x6300014 M 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):			
Empfangenes ISAKMP-Paket: peer = 64.102.156.8857211:28:38.63808/24/12Sev=Info/4IKE/0x6300014EMPFANG << ISAKMP OAK TRANS *(HASH, ATTR) ab		57111:28:38.63808/24/12Sev=Info/5IKE/0x630002F	E
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):		Empfangenes ISAKMP-Paket: peer = 64.102.156.88	P
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):		57211:28:38.63808/24/12Sev=Info/4IKE/0x6300014	N
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):		EMPFANG << ISAKMP OAK TRANS *(HASH, ATTR) ab	
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):		64.102.156.88	
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):		57311:28:38.63908/24/12Sev=Decode/11IKE/0x6300001	
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):		ISAKMP-Header	
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):		Initiator COOKIE:D56197780D7BE3E5	
Nächste Payload: Hash Ver. (Hex):10 Exchange-Typ: Transaktion Flags:(Verschlüsselung) MessagelD(Hex):84B4B653 Länge: 220 Payload-Hash Nächste Payload: Attribute Reserviert: 00 Payload-Länge: 24 Daten (in Hex):		Responder COOKIE:1B301D2DE710EDA0	
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):		Nächste Payload: Hash	
Exchange-Typ: Transaktion Flags:(Verschlüsselung) MessageID(Hex):84B4B653 Länge: 220 Payload-Hash Nächste Payload: Attribute Reserviert: 00 Payload-Länge: 24 Daten (in Hex):		Ver. (Hex):10	
Flags:(Verschlüsselung) MessageID(Hex):84B4B653 Länge: 220 Payload-Hash Nächste Payload: Attribute Reserviert: 00 Payload-Länge: 24 Daten (in Hex):		Exchange-Typ: Transaktion	
MessageID(Hex):84B4B653 Länge: 220 Payload-Hash Nächste Payload: Attribute Reserviert: 00 Payload-Länge: 24 Daten (in Hex):		Flags:(Verschlüsselung)	
Länge: 220 Payload-Hash Nächste Payload: Attribute Reserviert: 00 Payload-Länge: 24 Daten (in Hex):		MessageID(Hex):84B4B653	
Payload-Hash Nächste Payload: Attribute Reserviert: 00 Payload-Länge: 24 Daten (in Hex):		Länge: 220	
Nächste Payload: Attribute Reserviert: 00 Payload-Länge: 24 Daten (in Hex):		Payload-Hash	
Reserviert: 00 Payload-Länge: 24 Daten (in Hex):		Nächste Payload: Attribute	
Payload-Länge: 24 Daten (in Hex):		Reserviert: 00	
Daten (in Hex):		Payload-Länge: 24	
		Daten (in Hex):	

	6DE2E70ACF6B185846	BC62E590C00A66745D14D	
	Payload-Attribute		
	Nächste Payload: Keine		
	Reserviert: 00		
	Payload-Länge: 163		
	Typ: ISAKMP_CFG_REF	PLY	
	Reserviert: 00		
	Kennung: 0000		
	IPv4-Adresse: 192.168.1	.100	
	IPv4-Netzmaske: 255.25	5.255.0	
	IPv4-DNS: 192.168.1.99	,-	
	Cisco Erweiterung: PWD	speichern: Nein	
	Cisco Erweiterung: Stand	dard-Domänenname:	
	ivoungta-labdomain.cisco	D.COM	
	Cisco Erweiterung: PES:	Nein	
	Anwendungsversion: Cis	co Systems Inc ASA5505 Version	
	8 4(4)1 von Entwicklern	auf Thu 14-Jun-12 11:20	
	Cisco Erweiterung: Entfe	rnen der Smartcard: Ja	
Phase 1 wird auf dem Server	24 August 11:31:13	57/11.28.3863008/21/12Sev=	
abaasablassan Initijaran Sia dan		Dobug/71KE/0x6200076	
Augeschlossen. Indieren Sie den	[[KEV] DECODE][F =		r
	Deepender startet OM:	TM/MagID=94D4D652CurState	e
	msy ld = 0e83792e		
	24. Aug. 11:31:13	EV_RCVD_WSG	
		57511:28:38.63908/24/125ev=	
	= Ipsec, Benutzername		
	= Benutzer1, IP =		
	64.102.156.87,	INTERNAL_IPV4_ADDRESS:	
	Schnellmodusverarbeitu	Wert = 192.168.1.100	
	Ing verzogert, Cert/Trans	5/611:28:38.63908/24/12Sev=Info/5IK	
	Exchange/RM DSID in	E/0x6300010	
	Verarbeitung	MODE_CFG_REPLY: Attribut =	
	24. Aug. 11:31:13	INTERNAL_IPV4_NETMASK,	
	[IKEv1]Gruppe = ipsec,	Wert = 255.255.255.0	
	Benutzername =	57711:28:38.63908/24/12Sev=	
	Benutzer1, IP =	Info/5IKE/0x6300010	
	64.102.156.87,	MODE_CFG_REPLY: Attribut =	
	Gratuitous ARP wird für	INTERNAL_IPV4_DNS(1): ,	
	192.168.1.100 gesendet	Wert = 192.168.1.99	
	24. August 11:31:13	57811:28:38.63908/24/12Sev=Info/5IK	
	[[IKEv1 DEBUG]Gruppe	E/0x630000D	
	= ipsec, Benutzername	MODE_CFG_REPLY: Attribut =	
	= Benutzer1, IP =	MODECFG_UNITY_SAVEPWD: ,	
	64.102.156.87, Resume	value = 0x0000000	
	Quick Mode Processing,	57911:28:38.63908/24/12Sev=Info/5IK	
	Cert/Trans Exch/RM	E/0x630000E	
	DSID abgeschlossen	MODE_CFG_REPLY: Attribut =	
	24. August 11:31:13	MODECFG_UNITY_DEFDOMAIN: ,	
	[IKEv1]Gruppe = ipsec,	value = jyoungta-	
	Benutzername =	labdomain.cisco.com	
	Benutzer1, IP =	58011:28:38.63908/24/12Sev=	
	64.102.156.87, PHASE	Info/5IKE/0x630000D	
	1 ABGESCHLOSSEN	MODE_CFG_REPLY: Attribut =	
1	11		11

	MODECFG_UNITY_PFS: , value =	
	0x0000000	
	58111:28:38.63908/24/12Sev=Info/5IK	
	F/0x630000F	
	MODE CEG REPLY: Attribut =	
	AFFEICATION_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 RE	
	MOVAL DISCONNECT: value =	
	0x0000001	
	58311·28·38 63908/24/12Sev=	
	Info/5IKE/0x630000D	
	MODE CEG REPLY: Attribut =	
	Empfangen und Verwenden von NAT T	
	Borthummer Wort = 0x00001104	
	58411:28:39.30708/24/12SeV=	
	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	24. August 11:31:13 [IKEv1]IP = 64.102.156.87. Keep-Alive-Tvp	iF
den Client	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	
	$24 \text{ Aug} = 11\cdot31\cdot13 \text{ [IKEV1 DEBLIG]Gruppe = insec}$	
	Benutzername = Benutzer1 $IP = 64,102,156,87$	
	Benachrichtigung condon	
	24 Aug. 11/21/12 IVEv/ DEPUCICroup = incore Ucorname =	
	24. Aug. 11.51.15 [INEVI DEBOG]GIOUP - Ipsec, Userhame -	
	User1, IP = 64.102.156.87, Erstellen einer leeren Hasn-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)	1
	=======>	
	58811:28:39.79508/24/12Sev=Debug/7IKE/0x6300015	
	intf_data: lcl=0x0501A8C0, mask=0x00FFFF.	S
	bcast=0xFF01A8C0, bcast_vra=0xFF07070A	llu
	58911:28:39.79508/24/12Sev=Debua/7IKE/0x6300076	_
	NAV Trace->SA:L Cookie=D56197780D7BF3F5	_

	R_Cookie=1B301D2DE710EDA0CurState:	C
	CMN_MODECFG_PROGEvent: EV_INIT_P2	V
	59011:28:39.79508/24/12Sev=Info/4IKE/0x6300056	F
	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:L Cookie=D56197780D7BE3E5	
	R Cookie=1B301D2DE710EDA0CurState	
	CMN_ACTIVEEvent: EV_NO_EVENT	
	50211:28:30 70508/21/12Sev=Debug/7IKE/0x6300076	
	NAV Trace->OM·McalD=0E83702ECurState: OM_INITIALEvent:	
	EV_INITIATOR 60211:29:20 70609/24/128 ov=Dobug/71//E/0x6200076	
	59311.20.39.79500/24/125ev=Debug/71KE/0x0500070	
	NAV Trace->QM:MSgID=0E83792ECurState:	
	59411:28:39./9608/24/12Sev=Debug//IKE/0x63000/6	
	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	
	59611:28:39.79608/24/12Sev=Debug/7IKE/0x6300076	S
	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	
	<pre><====================================</pre>	眝
	=======================================	
Empfangen von QM1.	24. August 11:31:13 [IKEv1]IP = 64.102.156.87. EMPFANGENE	眝
	IKE DECODE-Nachricht (msgid=e83792e) mit Payloads: HDR +	
	HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + KEINE (0)	
	Gesamtlänge: 1026	
OM1 verarbeiten	24 August 11:31:13 [[KEy1 DEBLIC]Gruppo = insoc	╬
Relevante Konfiguration:	$P_{\text{August 11.51.15}} [IKEVI DEDOG]Gluppe = lpsec,$	
Relevante Koniguration.	Denuizemanie – Denuizer I, IP – 04. 102. 150.07, Veraibeilung	
aremto demonia mon		
DYN 10 set transform-	24. August 11.31.13 [INEVI DEDOG]GIuppe – Ipsec,	
set TRA	Benulzername = Benulzer1, IP = 64.102.156.87, Verarbeilung	
DCC 11/11		
	24. Aug. 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec,	
	24. Aug. 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec, Benutzername = Benutzer1, IP = 64.102.156.87, Verarbeitung	
	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, Verarbeitung von einmaliger Nutzlast 24. Aug. 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec,	
	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-	
	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 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,	
	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,	
	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	
	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. 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 =	
	 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- 	
	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	

	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-Pavload Adresse 0.0.0.0 Maske 0.0.0
	Protokoll 0. Port 0
	24 August 11:31:13 [[KEv1]Gruppo = insoc. Bonutzornamo =
	24. August 11.51.15 [IKLV1]Gruppe – ipsec, Denuizemanie –
	user I, IF – 04.102.130.07, QIVI ISREKEYEU Olu as hol lound by
	24. August 11:31:13 [IKEV1]Gruppe = Ipsec, Benutzername =
	user1, IP = 64.102.156.87, Prutung der statischen Crypto Map,
	Uberprüfung Map = out-map, seq = 10
	24. Aug. 11:31:13 [IKEv1]Gruppe = ipsec, Benutzername =
	Benutzer1, IP = 64.102.156.87, Statische Kryptozuordnung Nach
	Ubergabe 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 = insec. 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 = insec
	Benutzername = user1 IP = 64 102 156 87 Verarbeitung der
	IPSec SA-Nutzlast
Erstellen Sie OM2	24 Aug. 11:31:13 [IKEv1 DEBLIG]Gruppe = insec
Polovanto Konfiguration:	Bonutzornamo - Bonutzor1 $IP = 64,102,156,87, IPSoc, SA$
	Angebet Nr. 12, Umwandeln Nr. 1 akzentabelEntenricht dem
tuppol-group F7	Algebol Nr. 12, Oniwandelli Nr. 1 akzeptabelentspricht den
tvpe remote-access !	24 August 11:21:12 [IKEv1]Crupps = ipage Reputzerneme =
(tunnel type ra = tunnel	Poputator1 ID = 64 102 156 87 IKE: SDI wird opgeferdert
type remote-access)	Defiuizer 1, IP – 64. 102. 156.67, IKE. SPI wird angelordert!
crypto ipsec transform-	IPSEC. Neue emplyonale SA erstellit @ 0xciditc90,
set TRA esp-aes esp-	
sna-nmac	
association lifetime	Sitzungs-ID: 0x00138000
seconds 28800	
crypto ipsec security-	l unneityp: rz
association lifetime	Protokoll: esp
kilobytes 4608000	Lebensdauer: 240 Sekunden
DYN 10 set transform-	24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec,
set TRA	Benutzername = Benutzer1, IP = 64.102.156.87, IKE hat SPI von
crypto map MAP 65000	der Schlüsselengine erhalten: SPI = 0x9e18acb2
ipsec-isakmp dynamic	24. Aug. 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec,
DYN	Benutzername = Benutzer1, IP = 64.102.156.87, oakley-
crypto map MAP	Konstruktor Quick-Modus
Interlace outside	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 = insec Benutzername =	
	$Benutzer1 IP = 61 102 156 87 Ilberschreiben der IPSec_$	
	Neucinetellungedeuer des Initieters von 2147492 auf 96400	
	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 = insec	
	Benutzername = user1 $IP = 64 \ 102 \ 156 \ 87$ Erstellen der Prov	
	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 JP = 64 102 156 87 Senden der	
	LIEFTIME-ANTWORT an Initiator	
	24 August 11:21:12 [IKEy1 DEBUG] Given points of the second	
	24. August 11.51.15 [IKEVI DEDOG]Gluppe – 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 Pavloads, HDR +	
	HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIEY	
	(11) + KEINE (0) Gesantlänge: 184	
		╬
	60811:28:39,96208/24/12Sev=Info/4IKE/0x6300014	E
	EMPFANG << ISAKMP OAK QM *(HASH, SA, NON, ID, ID,	
	BENACHRICHTIGUNG:STATUS_RESP_LIFETIME) von	
	64.102.156.88	
	60911:28:39,96408/24/12Sev=Decode/11IKE/0x6300001	ΪP
	ISAKMP-Header	_P
	Initiator COOKIE D56197780D7BE3E5	۱'n
		
	Nächste Devlaad: Heeh	
	Nachsie Payloau. Hash	
	Exchange Type (Exchange-Typ): Quick Mode	
	Flags:(Verschlüsselung)	
	MessageID(Hex):E83792E	
	Länge: 188	
	Payload-Hash	
	Nächste Payload: Security Association	
	Reserviert: 00	
	Payload-Länge: 24	
	Datan (in Hay):	

CABF38A62C9B88D1691E81F3857D6189534B2EC0
Payload Security Association
Nächste Payload: Nonce
Reserviert: 00
Pavload-Länge: 52
DOI: IPsec
l age: (SIT IDENTITY ONLY)
Pavload-Angebot
Nächste Pavload: Keine
Reserviert: 00
Payload Länge: 40
Angebetenr : 1
PTOLOKOII-ID. PROTO_IPSEC_ESP
SPI-Groise: 4
Anzani 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
Pavload Nonce
Nächste Pavload: Identifikation
Reserviert: 00
Pavload-I änge: 24
Daten (in Hex):
3A079B75DA512473706E235EA3ECA61E1D15D4CD
Pavload-Identifizierung
Nächste Pavload: Identifikation
Posonyiort: 00
Pavload-Länge: 12
ID_Typ: IDv4_Adresse
Protokoll ID (IDP/TCP upw.): 0
Dart 0
Poll. U
Devide ed. Identificierum r
Payload-Identifizierung
Nachste 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	C
	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	
	NAV Trace->QM:MsgID=0E83792ECurState:	İE
	QM_BLD_MSG3Ereignis: EV_BLD_MSG	E
	61411:28:39.96508/24/12Sev=Debug/7IKE/0x6300076	w
	ISAKMP-Header	b
	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	
	61511:28:39.96508/24/12Sev=Debug/7IKE/0x6300076	C
	NAV Trace->QM:MsgID=0E83792ECurState:	b
	QM_SND_MSG3Ereignis: EV_SND_MSG	u
	61611:28:39,96508/24/12Sev=Info/4IKE/0x6300013	
	SENDEN >>> ISAKMP OAK QM *(HASH) an 64.102.156.88	
	<============ Quick Mode Message 3 (QM3)	i
Empfangen von QM3.	24. August 11:31:13 [IKEv1]IP = 64.102.156.87, EMPFANGENE	iF
	IKE_DECODE-Nachricht (msgid=e83792e) mit Pavloads: HDR +	
	HASH (8) + KEINE (0) Gesamtlänge: 52	
QM3 verarbeiten. Erstellen Sie die	24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec.	悁
ein- und ausgehenden Security-	Benutzername = Benutzer1. IP = 64.102.156.87. Verarbeitung	
		11
Parameterindizes (SPIs).	von Hash-Payload	

Hinzufügen einer statischen Route	24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec,
für den Host	Benutzername = Benutzer1, IP = 64.102.156.87, Laden aller
Relevante Konfiguration:	IPSEC SAs
3	24 August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec
crvpto ipsec transform-	Benutzername = user1 $IP = 64 102 156 87$ Generating Ouick
set TRA esp-aes esp-	Mode Keyl
sha-hmac	24 Aug = 11:21:12 [IKEy1 DEPLIC] Cruppo = ipago
crypto ipsec security-	24. Aug. 11.31.13 [INEVI DEBUG]Gluppe – Ipsec,
association lifetime	Benutzername = Benutzer1, IP = 64.102.156.87, NP-
seconds 28800	Verschlusselungsregel sucht nach der unverschlusselten
crypto ipsec security-	Zuordnung 10 übereinstimmender ACL Unbekannt:
association lifetime	zurückgesendet
kilopytes 4608000	cs_id=cc107410; Regel=00000000
DYN 10 set transform-	24. August 11:31:13 [IKEv1 DEBUG]Gruppe = ipsec,
set TRA	Benutzername = user1. IP = 64.102.156.87. Generating Quick
crypto dynamic-map	Mode Kev!
DYN 10 set reverse-	IPSEC: Neue embryonale SA erstellt @ 0xccc9ed60
route	$SCB: 0_{V}CE7E50E0$
	Diehtung: eusgehand
	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
	Elaggen: $0x0000025$
	SA: 0xcc9ed60
	SPI: $0 \times C055290$ A
	MTU: 1500 Byte
	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 Porte
	Obere: 0
	Dst-Ports
	Obere: 0
	Unteres: 0
	Op: ignorieren
	Protokoll: 0
11	

Protokoll verwenden: falsch
SPI: 0x000000
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 Darts
Obere: 4500
Uptere. 4500
Op: gleich
Dst-Ports
Obere: 58506
Unteres: 58506
Op: gleich
Protokoll: 17
Protokoll verwenden: wahr
SPI: 0x000000
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
c_{s} id= $c_{s}107410$; $P_{oracl}=0000000$
24 Aug 11:21:12 [[KEy1]Cruppo = incoc Boputzornomo =
24. Aug. 11.51.15 [IKEV1]Gluppe – Ipsec, Benutzerhandungen
benutzer 1, IF – 04. 102. 150.07, Sichementsverhandungen
abgeschlossen für Benutzer (user 1)Responder, Eingenender SPI
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: 0x000000
Peer: 0 x 0015909C
SCB: 0xA5672481
Kanal [,] 0xc82afb60
IPSEC: Abgeschlossener eingehender \/PNI_Kontext_SPI
n oro. Abyesoniossenei eingenendei vriv-nonieki, ori

0x9F18ACB2
VPN-Handle: 0 x 0016219c
IPSEC: Aktualisierung des ausgehenden VPN-Kontexts
Elagon: $0x000025$
SPI: 0 X C005290 A
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
Src Adrosco: 102 168 1 100
SIC-AULESSE. 192.100.1.100
SRC-IVIASKE. 200 200 200 200 200
Ziel-Adresse: 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 [.] 0x000000
SPI verwenden: falsch
IPSEC: Abgeschlossene eingebende Tunnelflussregel, SPI
Dage ID: 0xedf15270
Regerind. Uxcui 15270
Datenverkenr, SPI UX9E18ACB2
Src-Adresse: 64 102 156 87
SRC-Maske: 255 255 255 255 255
Ziel-Adresse: 64 102 156 88
DAR I - 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: 0x000000
	SPI verwenden: falsch
	IPSEC: Abgeschlossene Entschlüsselungsregel für eingehenden
	Datenverkehr SPI 0x9F18ACB2
	Regel-ID: 0xce03c2f8
	IPSEC: Neue Zulassungsregel für eingehenden Datenverkehr
	SPI 0x9F18ACB2
	$Src_Adresse' 64 102 156 87$
	SRC-Maske: 255 255 255 255 255
	Ziel-Adresse: 64 102 156 88
	DAPT Macka: 255 255 255 255 255
	Sro Dorto
	Obere: 58506
	Upteres: 58506
	On eleich
	Op: gleich
	DSI-POILS
	Unteres: 4500
	Protokoli: 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	24. August 11:31:13 [IKEv1]Gruppe = ipsec, Benutzername =
Seiten verschlüsseln und	Benutzer1, IP = 64.102.156.87, PHASE 2 ABGESCHLOSSEN
entschlüsseln jetzt.	(msgid=0e83792e)
Für Hardware-Clients wird eine	24. August 11:31:13 [IKEv1]: IP = 10.48.66.23, IKE DECODE
weitere Nachricht empfangen, in	EMPFANGENE Nachricht (msgid=91facca9) mit Payloads: HDR
der der Client Informationen über	+ HASH (8) + NOTIFY (11) + KEINE (0) Gesamtlänge: 184
sich selbst sendet. Wenn Sie genau	24. August 11:31:13 [IKEv1 DEBUG]: Gruppe = EZ.
hinschauen, sollten Sie den	Benutzername = cisco, IP = 10,48,66,23, Verarbeitung von
Hostnamen des EzVPN-Clients die	Hash-Payload
auf dem Client ausgeführte	24. August 11:31:13 [IKEv1 DEBUG]: Gruppe = EZ.
Software sowie den Standort und	Benutzername = cisco. IP = 10.48.66.23. Verarbeitung der
den Namen der Software finden	Benachrichtigungs-Payload
	24. Aug. 11:31:13 [IKEv1 DECODE]: OBSOLETE-
	BESCHREIBER - INDEX 1
L	

24. Aug. 11:31:13 [IKEv1 DECODE]: 0000: 0000000 7534000 B
62736E73 2D383731
u4.bsns-871
0010: 2D332E75 32000943 6973636F 20383731 -3.u2Cisco
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) 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: 0x0000000 0x000003F 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: 0x0000000 0x0000001

Zugehörige Informationen

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