Fehlerbehebung bei IOS IKEv2-Debuggern für Site-to-Site-VPN mit PSKs

Inhalt

Einleitung

Dieses Dokument beschreibt Internet Key Exchange Version 2 (IKEv2)-Debugging-Vorgänge unter Cisco IOS® bei Verwendung eines nicht freigegebenen Schlüssels (Unshared Key, PSK).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse des Paketaustauschs für IKEv2 verfügen. Weitere Informationen finden Sie unter Debuggen auf IKEv2-Paketaustausch- und Protokollebene.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Internet Key Exchange Version 2 (IKEv2)
- Cisco IOS 15.1(1)T oder spätere Version

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

Dieses Dokument enthält Informationen zur Übersetzung bestimmter Debugzeilen in einer Konfiguration.

Kernproblem

Der Paketaustausch in IKEv2 unterscheidet sich grundlegend vom Paketaustausch in IKEv1. In IKEv1 gab es einen klar abgegrenzten Phase-1-Austausch, der aus sechs (6) Paketen bestand, gefolgt von einem Phase-2-Austausch, der aus drei (3) Paketen bestand. Der IKEv2-Austausch ist variabel. Weitere Informationen zu den Unterschieden und eine Erläuterung des Paketaustauschs finden Sie unter Debuggen auf IKEv2-Paket- und Protokollebene.

Router-Konfiguration

In diesem Abschnitt werden die in diesem Dokument verwendeten Konfigurationen aufgeführt.

Router 1

```
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
 ip address 172.16.0.101 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.2
 tunnel protection ipsec profile phse2-prof
!
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0

crypto ikev2 proposal PHASE1-prop
 encryption 3des aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 policy site-pol
 proposal PHASE1-prop
!
crypto ikev2 keyring KEYRNG
 peer peer1
  address 10.0.0.2 255.255.255.0
  hostname host1
  pre-shared-key local cisco
  pre-shared-key remote cisco
 !
crypto ikev2 profile IKEV2-SETUP
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRNG
 lifetime 120
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
```

```
crypto ipsec profile phse2-prof
 set transform-set TS
 set ikev2-profile IKEV2-SETUP
!
ip route 0.0.0.0 0.0.0.0 10.0.0.2
ip route 192.168.2.1 255.255.255.255 Tunnel0
```

Router 2

```
crypto ikev2 proposal PHASE1-prop
 encryption 3des aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 keyring KEYRNG
 peer peer2
  address 10.0.0.1 255.255.255.0
  hostname host2
  pre-shared-key local cisco
  pre-shared-key remote cisco
 !
crypto ikev2 profile IKEV2-SETUP
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRNG
 lifetime 120
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
!
crypto ipsec profile phse2-prof
 set transform-set TS
 set ikev2-profile IKEV2-SETUP
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.0.2 255.255.255.0
!
interface Tunnel0
 ip address 172.16.0.102 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.1
 tunnel protection ipsec profile phse2-prof
!
ip route 0.0.0.0 0.0.0.0 10.0.0.1
ip route 192.168.1.1 255.255.255.255 Tunnel0
```

Fehlerbehebung

Router-Fehlerbehebung

Die folgenden Debug-Befehle werden in diesem Dokument verwendet:

```
deb crypto ikev2 packet
deb crypto ikev2 internal
```

Router 1 (Initiator) - Beschreibung der Nachricht	**Fehlerbehebung**	**Re Besc**
Router 1 empfängt ein Paket, das mit der Crypto-ACL für Peer-ASA 10.0.0.2 übereinstimmt. Initiiert SA-Erstellung	* 11. November 20:28:34.03: IKEv2:Paket vom Verteiler erhalten * 11. November 20:28:34.03: IKEv2:Verarbeiten eines Elements aus der Paket-Warteschlange * 11. November 19:30:34.811: IKEv2:% Erhalten des vorinstallierten Schlüssels nach Adresse 10.0.0.2 *11. November 19:30:34.811: IKEv2:Adding Proposal PHASE1-prop to toolkit policyle * 11. November 19:30:34.811: IKEv2:(1): Auswahl des IKE-Profils "IKEV2-SETUP" *Nov 11 19:30:34.811: IKEv2:New ikev2 wie Anfrage zugelassen *11. November 19:30:34.811: IKEv2:Steigerung der Anzahl ausgehender Verhandlungen um eins	
Das erste Nachrichtenpaar ist der IKE_SA_INIT-Austausch. Diese Nachrichten handeln kryptografische Algorithmen aus, tauschen Unzen aus und führen einen Diffie-Hellman-Austausch durch. **Relevante Konfiguration:** `crypto ikev2 vorschlag PHASE1-prop verschlüsselung 3des aes-cbc-128 integrität sha1 gruppe 2crypto ikev2 keyring KEYRNG peer1 address 10.0.0.2 255.255.255.0 hostname host1 preshared-key local cisco preshared-key remote cisco`	*11. November 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: IDLE Ereignis: EV_INIT_SA *11. November 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Ereignis: EV_GET_IKE_POLICY * 11. November 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event **EV_SET_POLICY** * 11. November 19:30:34.811: IKEv2:(SA-ID = 1):Festlegen konfigurierter Richtlinien *11. November 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Ereignis: EV_CHK_AUTH4PKI * 11. November 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Event **EV_GEN_DH_KEY** *11. November 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Ereignis: EV_NO_EVENT *11. November 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Ereignis: EV_OK_RECD_DH_PUBKEY_RESP *11. November 19:30:34.811: IKEv2:(SA-ID = 1):Aktion: Action_Null *11. November 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Ereignis: EV_GET_CONFIG_MODE *11. November 19:30:34.811: IKEv2:IKEv2-Initiator - keine Konfigurationsdaten zum Senden in IKE_SA_INIT-Exchange *11. November 19:30:34.811: IKEv2:Keine Konfigurationsdaten zum Senden	

	an Toolkit: *11. November 19:30:34.811: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=0000000000000000 (I) MsgID = 00000000 CurState: I_BLD_INIT Ereignis: EV_BLD_MSG *11. November 19:30:34.811: IKEv2:Aufbau anbieterspezifischer Payload: LÖSCHEN-GRUND *11. November 19:30:34.811: IKEv2:Aufbau anbieterspezifischer Payload: (BENUTZERDEFINIERT) *11. November 19:30:34.811: IKEv2:Construct Notify Payload: NAT_DETECTION_SOURCE_IP *11. November 19:30:34.811: IKEv2:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP	
Initiator erstellt IKE_INIT_SA-Paket. Es enthält: ISAKMP-Header (SPI/Version/Flags), SAi1 (kryptografischer Algorithmus, der vom IKE-Initiator unterstützt wird), KEi (öffentlicher DH-Schlüsselwert des Initiators) und N (Initiator Nonce).	*11. November 19:30:34.811: **IKEv2:(SA ID = 1)**:Nächste Nutzlast: SA, Version: 2.0 Austauschtyp: **IKE_SA_INIT,** Flags: **INITIATOR** Nachrichtenkennung: 0, Länge: 344 Payload-Inhalte: **SA** Nächste Nutzlast: KE, reserviert: 0x0, Länge: 56 letztes Angebot: 0x0, reserviert: 0x0, Länge: 52 Vorschlag: 1, Protokoll-ID: IKE, SPI-Größe: 0, #trans: 5 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 1, reserviert: 0x0, ID: 3DES letzte Transformation: 0x3, reserviert: 0x0: Länge: 12 Typ: 1, reserviert: 0x0, ID: AES-CBC letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 2, reserviert: 0x0, ID: SHA1 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 3, reserviert: 0x0, ID: SHA96 letzte Transformation: 0x0, reserviert: 0x0: Länge: 8 Typ: 4, reserviert: 0x0, ID: DH_GROUP_1024_MODP/Gruppe 2 **KE** Nächste Nutzlast: N, reserviert: 0x0, Länge: 136 DH-Gruppe: 2, Reserviert: 0x0 N Nächste Nutzlast: VID, reserviert: 0x0, Länge: 24 VID Nächste Nutzlast: VID, reserviert: 0x0, Länge: 23 VID Nächste Nutzlast: NOTIFY, reserviert: 0x0, Länge: 21 NOTIFY(NAT_DETECTION_SOURCE_IP) Nächste Nutzlast: NOTIFY, reserviert: 0x0, Länge: 28 Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Nächste Nutzlast: KEINE, reserviert: 0x0, Länge: 28 Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: NAT_DETECTION_DESTINATION_IP	
----------Initiator hat IKE_INIT_SA ----------> gesende		
	*11. November 19:30:34.814: IKEv2:Paket vom Verteiler erhalten *11. November 19:30:34.814: IKEv2:Verarbeiten eines Elements aus der Paket-Warteschlange *Nov 11 19:30:34.814: IKEv2:New ikev2 wie Anfrage zugelassen *11. November 19:30:34.814: IKEv2:Erhöhung der eingehenden Verhandlungsanzahl um eins	Resp IKE_
	*Nov 11 19:30:34.814: IKEv2:Nächste Nutzlast: SA, Version: 2.0	Der SA- Peer.

	Austauschtyp: IKE_SA_INIT, Flags: INITIATOR Nachrichten-ID: 0, Länge: 344 Payload-Inhalte: SA Nächste Nutzlast: KE, reserviert: 0x0, Länge: 56 letztes Angebot: 0x0, reserviert: 0x0, Länge: 52 Vorschlag: 1, Protokoll-ID: IKE, SPI-Größe: 0, #trans: 5 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 1, reserviert: 0x0, ID: 3DES letzte Transformation: 0x3, reserviert: 0x0: Länge: 12 Typ: 1, reserviert: 0x0, ID: AES-CBC letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 2, reserviert: 0x0, ID: SHA1 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 3, reserviert: 0x0, ID: SHA96 letzte Transformation: 0x0, reserviert: 0x0: Länge: 8 Typ: 4, reserviert: 0x0, ID: DH_GROUP_1024_MODP/Gruppe 2 KE Nächste Nutzlast: N, reserviert: 0x0, Länge: 136 DH-Gruppe: 2, Reserviert: 0x0 N Nächste Nutzlast: VID, reserviert: 0x0, Länge: 24 * 11. November 19:30:34.814: IKEv2:Analyse anbieterspezifische Payload: CISCO-DELETE-REASON VID Nächste Payload: VID, reserviert: 0x0, Länge: 23 *11. November 19:30:34.814: IKEv2:Analyse anbieterspezifischer Payload: (CUSTOM) VID Nächste Payload: NOTIFY, reserviert: 0x0, Länge: 21 *11. November 19:30:34.814: IKEv2:Parse Notify Payload: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP) Nächste Payload: NOTIFY, reserviert: 0x0, Länge: 28 Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: NAT_DETECTION_SOURCE_IP *11. November 19:30:34.814: IKEv2:Parse Notify Payload: NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Nächste Payload: KEINE, reserviert: 0x0, Länge: 28 Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: NAT_DETECTION_DESTINATION_IP	
	*11. November 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: IDLE-Ereignis:**EV_RECV_INIT** *11. November 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: R_INIT-Ereignis:**EV_VERIFY_MSG** *11. November 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: R_INIT Ereignis:**EV_INSERT_SA** *11. November 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: R_INIT-Ereignis:**EV_GET_IKE_POLICY** *11. November 19:30:34.814: IKEv2:Standardangebot zur Toolkit-Richtlinie hinzufügen	Der I veran Nach Cryp Initia berec Gehe berec von d diese werd Nach Head Nach

*11. November 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: R_INIT-Ereignis:**EV_PROC_MSG**
*11. November 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: R_INIT-Ereignis: EV_DETECT_NAT
*11. November 19:30:34.814: IKEv2:(SA-ID = 1):Prozess-NAT-Erkennungsbenachrichtigung
* 11. November 19:30:34.814: IKEv2:(SA-ID = 1):Verarbeitung von NAT-Erkennungsbenachrichtigung
*11. November 19:30:34.814: IKEv2:(SA-ID = 1):Remote-Adresse zugeordnet
* 11. November 19:30:34.814: IKEv2:(SA-ID = 1):Verarbeitung der Benachrichtigung über nat-Erkennung
*11. November 19:30:34.814: IKEv2:(SA-ID = 1):Lokale Adresse zugeordnet
*11. November 19:30:34.814: IKEv2:(SA-ID = 1):Kein NAT gefunden
*11. November 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: R_INIT-Ereignis: EV_CHK_CONFIG_MODE
*11. November 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: R_BLD_INIT-Ereignis: EV_SET_POLICY
*11.11.19:30:34.814: IKEv2:(SA-ID = 1):**Festlegen konfigurierter Richtlinien**
*11. November 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: R_BLD_INIT-Ereignis: EV_CHK_AUTH4PKI
*11. November 19:30:34.814: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: R_BLD_INIT-Ereignis: EV_PKI_SESH_OPEN
*11. November 19:30:34.814: IKEv2:(SA-ID = 1):PKI-Sitzung wird geöffnet
*11. November 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Zustand: R_BLD_INIT Ereignis:**EV_GEN_DH_KEY**
*11. November 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: R_BLD_INIT-Ereignis: EV_NO_EVENT
*11. November 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Zustand: R_BLD_INIT Ereignis:**EV_OK_RECD_DH_PUBKEY_RESP**
*11. November 19:30:34.815: IKEv2:(SA-ID = 1):Aktion: Action_Null
*11. November 19:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Zustand: R_BLD_INIT Ereignis:**EV_GEN_DH_SECRET**
*11. November 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: R_BLD_INIT-Ereignis: EV_NO_EVENT
* 11.11. 19:30:34.822: IKEv2:% **Erhalten des vorinstallierten Schlüssels nach Adresse 10.0.0.1**
*11. November 19:30:34.822: IKEv2:Standardangebot zur Toolkit-Richtlinie hinzufügen
* 11. November 19:30:34.822: IKEv2:(2): Auswahl des IKE-Profils "IKEV2-

vers
authe
Vers
Integ
Schlü
SKE
heiße
(Vers
(Autl
wird
Able
Schlü
CHIL
für je
separ
berec

Relev
Konf
ikev2
encry
128
2 cry
KEYRI
10.0
hostn
key
share

	SETUP" *11. November 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Zustand: R_BLD_INIT Ereignis: EV_OK_RECD_DH_SECRET_RESP *11. November 19:30:34.822: IKEv2:(SA-ID = 1):Aktion: Action_Null *11. November 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: R_BLD_INIT-Ereignis:**EV_GEN_SKEYID** *11.11.1930:34.822: IKEv2:(SA-ID = 1):**Schlüsselkennung generieren** *11. November 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: R_BLD_INIT-Ereignis: EV_GET_CONFIG_MODE * 11. November 19:30:34.822: IKEv2:IKEv2-Responder - keine Konfigurationsdaten zum Senden in IKE_SA_INIT-Exchange *11. November 19:30:34.822: IKEv2:Keine Konfigurationsdaten zum Senden an Toolkit: *11. November 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: R_BLD_INIT-Ereignis: EV_BLD_MSG *11. November 19:30:34.822: IKEv2:Aufbau anbieterspezifischer Payload: LÖSCHEN-GRUND *11. November 19:30:34.822: IKEv2:Aufbau anbieterspezifischer Payload: (BENUTZERDEFINIERT) *11. November 19:30:34.822: IKEv2:Construct Notify Payload: NAT_DETECTION_SOURCE_IP *11. November 19:30:34.822: IKEv2:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP *11. November 19:30:34.822: IKEv2:Construct Notify Payload: HTTP_CERT_LOOKUP_SUPPORTED	
	*11. November 19:30:34.822: IKEv2:(SA ID = 1):Nächste Nutzlast: SA, Version: 2.0 Austauschtyp: **IKE_SA_INIT,** Flags: **RESPONDER MSG-RESPONSE** Nachrichtenkennung: 0, Länge: 449 Payload-Inhalte: **SA** Nächste Nutzlast: KE, reserviert: 0x0, Länge: 48 letztes Angebot: 0x0, reserviert: 0x0, Länge: 44 Angebot: 1, Protokoll-ID: IKE, SPI-Größe: 0, #trans: 4 letzte Transformation: 0x3, reserviert: 0x0: Länge: 12 Typ: 1, reserviert: 0x0, ID: AES-CBC letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 2, reserviert: 0x0, ID: SHA1 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 3, reserviert: 0x0, ID: SHA96 letzte Transformation: 0x0, reserviert: 0x0: Länge: 8 Typ: 4, reserviert: 0x0, ID: DH_GROUP_1024_MODP/Gruppe 2 **KE** Nächste Nutzlast: N, reserviert: 0x0, Länge: 136 DH-Gruppe: 2, Reserviert: 0x0 **N** Nächste Nutzlast: VID, reserviert: 0x0, Länge: 24 VID Nächste Nutzlast: VID, reserviert: 0x0, Länge: 23 VID Nächste Nutzlast: NOTIFY, reserviert: 0x0, Länge: 21 NOTIFY(NAT_DETECTION_SOURCE_IP) Nächste Nutzlast: NOTIFY,	Rout Resp IKE_ die v wird. ISAK (SPI/ (kryp Algo Resp KEr(Schli Resp Nonc

	reserviert: 0x0, Länge: 28 Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Nächste Nutzlast: CERTREQ, reserviert: 0x0, Länge: 28 Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: NAT_DETECTION_DESTINATION_IP CERTREQ Nächste Nutzlast: NOTIFY, reserviert: 0x0, Länge: 105 Zertifikatcodierung Hash und URL von PKIX NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) Nächste Nutzlast: KEINE, reserviert: 0x0, Länge: 8 Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: HTTP_CERT_LOOKUP_SUPPORTED		
	*11. November 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: INIT_DONE-Ereignis: EV_DONE * 11. November 19:30:34.822: IKEv2:(SA-ID = 1):Cisco DeleteReason Notify ist aktiviert *11. November 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: INIT_DONE-Ereignis: EV_CHK4_ROLE *11. November 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: INIT_DONE-Ereignis**: EV_START_TMR** *11. November 19:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 Cur Status: R_WAIT_AUTH-Ereignis: EV_NO_EVENT * 11. November 19:30:34.822: IKEv2:**Neues ikev2, wie Anfrage zugelassen** * 11. November 19:30:34.822: IKEv2:**Erhöhung der Anzahl ausgehender Verhandlungen um eins**		Rout Resp Rout
<----------Responder hat IKE_INIT_SA gesendet ----------			
Router 1 empfängt das IKE_SA_INIT-Antwortpaket von Router 2.	*11. November 19:30:34.823: IKEv2:Paket vom Verteiler erhalten *11. November 19:30:34.823: IKEv2:Paket vom Verteiler erhalten *11. November 19:30:34.823: IKEv2:Verarbeiten eines Elements aus der Paket-Warteschlange	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE Ereignis:**EV_START_TMR**	Der I Time
Router1 verifiziert und verarbeitet die Antwort: (1) Der geheime DH-Schlüssel des Initiators wird berechnet, und (2) die Schlüsselkennung des Initiators wird ebenfalls generiert.	*11. November 19:30:34.823: IKEv2:(SA ID = 1):Nächste Nutzlast: SA, Version: 2.0 Austauschtyp: IKE_SA_INIT, Flags: **RESPONDER MSG-RESPONSE** Nachrichten-ID: 0, Länge: 449 Payload-Inhalte: **SA** Nächste Nutzlast: KE, reserviert: 0x0, Länge: 48 letztes Angebot: 0x0, reserviert: 0x0, Länge: 44 Angebot: 1, Protokoll-ID: IKE, SPI-Größe: 0, #trans: 4 letzte		

Transformation: 0x3, reserviert: 0x0: Länge: 12
Typ: 1, reserviert: 0x0, ID: AES-CBC
letzte Transformation: 0x3, reserviert: 0x0: Länge: 8
Typ: 2, reserviert: 0x0, ID: SHA1
letzte Transformation: 0x3, reserviert: 0x0: Länge: 8
Typ: 3, reserviert: 0x0, ID: SHA96
letzte Transformation: 0x0, reserviert: 0x0: Länge: 8
Typ: 4, reserviert: 0x0, ID: DH_GROUP_1024_MODP/Gruppe 2
KE Nächste Nutzlast: N, reserviert: 0x0, Länge: 136
DH-Gruppe: 2, Reserviert: 0x0
N Nächste Nutzlast: VID, reserviert: 0x0, Länge: 24

*11. November 19:30:34.823: IKEv2:Analyse anbieterspezifische Payload: CISCO-DELETE-REASON VID Nächste Payload: VID, reserviert: 0x0, Länge: 23

*11. November 19:30:34.823: IKEv2:Analyse anbieterspezifischer Payload: (CUSTOM) VID Nächste Payload: NOTIFY, reserviert: 0x0, Länge: 21

*11. November 19:30:34.823: IKEv2:Parse Notify Payload: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP) Nächste Payload: NOTIFY, reserviert: 0x0, Länge: 28
Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: NAT_DETECTION_SOURCE_IP

*11. November 19:30:34.824: IKEv2:Parse Notify Payload: NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Nächste Payload: CERTREQ, reserviert: 0x0, Länge: 28
Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: NAT_DETECTION_DESTINATION_IP
CERTREQ Nächste Nutzlast: NOTIFY, reserviert: 0x0, Länge: 105
Zertifikatcodierung Hash und URL von PKIX

*11. November 19:30:34.824: IKEv2:Parse Notify Payload: HTTP_CERT_LOOKUP_SUPPORTED NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) Nächste Payload: KEINE, reserviert: 0x0, Länge: 8
Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: HTTP_CERT_LOOKUP_SUPPORTED

*11. November 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Status: I_WAIT_INIT-Ereignis: EV_RECV_INIT
* 11. November 19:30:34.824: IKEv2:(SA-ID = 1):IKE_SA_INIT-Nachricht wird verarbeitet
*11. November 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Status: I_PROC_INIT Ereignis: EV_CHK4_NOTIFY
*11. November 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Status: I_PROC_INIT-Ereignis: EV_VERIFY_MSG

*11. November 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Status: I_PROC_INIT-Ereignis: EV_PROC_MSG
*11. November 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Status: I_PROC_INIT-Ereignis: EV_DETECT_NAT
*11. November 19:30:34.824: IKEv2:(SA-ID = 1):Prozess-NAT-Erkennungsbenachrichtigung
* 11. November 19:30:34.824: IKEv2:(SA-ID = 1):Verarbeitung von NAT-Erkennungsbenachrichtigung
*11. November 19:30:34.824: IKEv2:(SA-ID = 1):Remote-Adresse zugeordnet
* 11. November 19:30:34.824: IKEv2:(SA-ID = 1):Verarbeitung der Benachrichtigung über nat-Erkennung
*11. November 19:30:34.824: IKEv2:(SA-ID = 1):Lokale Adresse zugeordnet
*11. November 19:30:34.824: IKEv2:(SA-ID = 1):Kein NAT gefunden
*11. November 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Status: I_PROC_INIT-Ereignis: EV_CHK_NAT_T
*11. November 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Zustand: I_PROC_INIT Ereignis: EV_CHK_CONFIG_MODE
*11. November 19:30:34.824: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Status: INIT_DONE-Ereignis**: EV_GEN_DH_SECRET**
*11. November 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Status: INIT_DONE-Ereignis: EV_NO_EVENT
*11. November 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Status: INIT_DONE-Ereignis: EV_OK_RECD_DH_SECRET_RESP
*11. November 19:30:34.831: IKEv2:(SA-ID = 1):Aktion: Action_Null
*11. November 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Status: INIT_DONE-Ereignis:**EV_GEN_SKEYID**
*11.11.1930:34.831: IKEv2:(SA-ID = 1):**Schlüsselkennung generieren**
*11. November 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Status: INIT_DONE-Ereignis: EV_DONE
* 11. November 19:30:34.831: IKEv2:(SA-ID = 1):Cisco DeleteReason Notify ist aktiviert
*11. November 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Status: INIT_DONE-Ereignis: EV_CHK4_ROLE
*11. November 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Status: I_BLD_AUTH-Ereignis: EV_GET_CONFIG_MODE
*11. November 19:30:34.831: IKEv2:Konfigurationsdaten werden an Toolkit gesendet
*11. November 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Status: I_BLD_AUTH-Ereignis: EV_CHK_EAP

Der Initiator startet den IKE_AUTH-Austausch und generiert die Authentifizierungsnutzlast. Das IKE_AUTH-Paket enthält: ISAKMP-Header (SPI/Version/Flags), IDi (Initiator-Identität), AUTH-Nutzlast, SAi2 (initiiert das SA ähnlich dem Phase-2-Transformationssatzaustausch in IKEv1) und TSi und TSr (Initiator- und Responder-Datenverkehrsauswahl). Sie enthalten die Quell- und Zieladresse des Initiators bzw. des Responders für die Weiterleitung/den Empfang von verschlüsseltem Datenverkehr. Der Adressbereich gibt an, dass der gesamte Datenverkehr zu und von diesem Bereich getunnelt wird. Wenn der Vorschlag für den Beantworter akzeptabel ist, sendet er identische TS-Payloads zurück. Die erste CHILD_SA wird für das Proxy_ID-Paar erstellt, das mit dem Triggerpaket übereinstimmt. **Relevante Konfiguration:** `crypto ipsec transform-set TS esp-3des esp-sha-hmac crypto ipsec profile phse2-prof set transformation-set TS set ikev2-profile IKEV2-SETUP`	*11. November 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Status: I_BLD_AUTH-Ereignis:**EV_GEN_AUTH** *11. November 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Status: I_BLD_AUTH-Ereignis: EV_CHK_AUTH_TYPE *11. November 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Status: I_BLD_AUTH-Ereignis: EV_OK_AUTH_GEN *11. November 19:30:34.831: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 Cur Status: I_BLD_AUTH-Ereignis: EV_SEND_AUTH *11. November 19:30:34.831: IKEv2:Aufbau anbieterspezifischer Payload: CISCO-GRANITE *11. November 19:30:34.831: IKEv2:Construct Notify Payload: INITIAL_CONTACT *11. November 19:30:34.831: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE *11. November 19:30:34.831: IKEv2:Construct Notify Payload: ESP_TFC_NO_SUPPORT *11. November 19:30:34.831: IKEv2:Construct Notify Payload: NON_FIRST_FRAGS **Payload-Inhalte:** VID Nächste Nutzlast: IDi, reserviert: 0x0, Länge: 20 **IDi** Nächste Nutzlast: AUTH, reserviert: 0x0, Länge: 12 ID-Typ: IPv4-Adresse, Reserviert: 0x0 0x0 **AUTH** Nächste Nutzlast: CFG, reserviert: 0x0, Länge: 28 Auth-Methode PSK, reserviert: 0x0, reserviert: 0x0 **CFG** Nächste Nutzlast: SA, reserviert: 0x0, Länge: 309 cfg type: CFG_REQUEST, reserviert: 0x0, reserviert: 0x0 *11.11.19:30:34.831: SA Nächste Nutzlast: **TSi**, reserviert: 0x0, Länge: 40 letztes Angebot: 0x0, reserviert: 0x0, Länge: 36 Vorschlag: 1, Protokoll-ID: ESP, SPI-Größe: 4, #trans: 3 Letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 1, reserviert: 0x0, ID: 3DES letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 3, reserviert: 0x0, ID: SHA96 letzte Transformation: 0x0, reserviert: 0x0: Länge: 8 Typ: 5, reserviert: 0x0, ID: ESN nicht verwenden **TSi** Nächste Nutzlast: TSr, reserviert: 0x0, Länge: 24 Anzahl der TSs: 1, reserviert 0x0, reserviert 0x0 TS-Typ: TS_IPV4_ADDR_RANGE, Proto-ID: 0, Länge: 16 Anfangsport: 0, Endport: 65535 start addr: 0.0.0.0, end addr: 255.255.255.255 **TSr** Nächste Nutzlast: NOTIFY, reserviert: 0x0, Länge: 24 Anzahl der TSs: 1, reserviert 0x0, reserviert 0x0 TS-Typ: TS_IPV4_ADDR_RANGE, Proto-ID: 0, Länge: 16 Anfangsport: 0, Endport: 65535 start addr: 0.0.0.0, end addr: 255.255.255.255 NOTIFY(INITIAL_CONTACT) Nächste Nutzlast: NOTIFY, reserviert: 0x0, Länge: 8

Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: INITIAL_CONTACT
NOTIFY(SET_WINDOW_SIZE) Nächste Nutzlast: NOTIFY, reserviert: 0x0, Länge: 12
Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: SET_WINDOW_SIZE
NOTIFY(ESP_TFC_NO_SUPPORT) Nächste Nutzlast: NOTIFY, reserviert: 0x0, Länge: 8
Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: ESP_TFC_NO_SUPPORT
NOTIFY(NON_FIRST_FRAGS) Nächste Nutzlast: KEINE, reserviert: 0x0, Länge: 8
Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: NON_FIRST_FRAGS

*11. November 19:30:34.832: IKEv2:(SA ID = 1):Nächste Nutzlast: ENCR, Version: 2.0 Austauschtyp: **IKE_AUTH**, Flaggen: **INITIATOR**
Nachrichten-ID: 1, Länge: 556
Payload-Inhalte:
ENCR Nächste Nutzlast: VID, reserviert: 0x0, Länge: 528

*11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00 00001 **CurState: I_WAIT_AUTH** Ereignis: EV_NO_EVENT

----------Initiator hat IKE_AUTH ----------> gesend

*11. November 19:30:34.832: IKEv2:Paket vom Verteiler erhalten
*11. November 19:30:34.832: IKEv2:Verarbeiten eines Elements aus der Paket-Warteschlange
*11. November 19:30:34.832: IKEv2:(SA-ID = 1):Anfrage hat mess_id 1; erwartet werden 1 bis 1
*11. November 19:30:34.832: **IKEv2:(SA ID = 1)**:Nächste Nutzlast: ENCR, Version: 2.0 Austauschtyp: **IKE_AUTH**, Flaggen: **INITIATOR**
Nachrichtenkennung: 1, Länge: 556
Payload-Inhalte:
*11. November 19:30:34.832: IKEv2:Analyse anbieterspezifischer Payload: (CUSTOM) VID Nächste Payload: IDi, reserviert: 0x0, Länge: 20
IDi Nächste Nutzlast: AUTH, reserviert: 0x0, Länge: 12
ID-Typ: IPv4-Adresse, Reserviert: 0x0 0x0
AUTH Nächste Nutzlast: CFG, reserviert: 0x0, Länge: 28
Auth-Methode PSK, reserviert: 0x0, reserviert: 0x0
CFG Nächste Nutzlast: SA, reserviert: 0x0, Länge: 309
cfg type: CFG_REQUEST, reserviert: 0x0, reserviert: 0x0
* 11. November 19:30:34.832: Attributtyp: interner IP4 DNS, Länge: 0
* 11. November 19:30:34.832: Attributtyp: interner IP4 DNS, Länge: 0
*11. November 19:30:34.832: Attributtyp: intern IP4 NBNS, Länge: 0
*11. November 19:30:34.832: Attributtyp: intern IP4 NBNS, Länge: 0
* 11. November 19:30:34.832: Attributtyp: internes IP4-Subnetz, Länge: 0
*Nov 11 19:30:34.832: Attributtyp: Anwendungsversion, Länge: 257
Attributtyp: Unbekannt - 28675, Länge: 0
*Nov 11 19:30:34.832: Attributtyp: Unbekannt - 28672, Länge: 0
*Nov 11 19:30:34.832: Attributtyp: Unbekannt - 28692, Länge: 0
*Nov 11 19:30:34.832: Attributtyp: Unbekannt - 28681, Länge: 0
*Nov 11 19:30:34.832: Attributtyp: Unbekannt - 28674, Länge: 0
* Nov 11 19:30:34.832: **SA** Nächste Nutzlast: TSi, reserviert: 0x0, Länge: 40
letztes Angebot: 0x0, reserviert: 0x0, Länge: 36

Rout
verif
empf
Auth

Rele
cryp
vors
esp
256
integ

	Vorschlag: 1, Protokoll-ID: ESP, SPI-Größe: 4, #trans: 3 Letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 1, reserviert: 0x0, ID: 3DES letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 3, reserviert: 0x0, ID: SHA96 letzte Transformation: 0x0, reserviert: 0x0: Länge: 8 Typ: 5, reserviert: 0x0, ID: ESN nicht verwenden **TSi** Nächste Nutzlast: TSr, reserviert: 0x0, Länge: 24 Anzahl der TSs: 1, reserviert 0x0, reserviert 0x0 TS-Typ: TS_IPV4_ADDR_RANGE, Proto-ID: 0, Länge: 16 Anfangsport: 0, Endport: 65535 start addr: 0.0.0.0, end addr: 255.255.255.255 **TSr** Nächste Nutzlast: NOTIFY, reserviert: 0x0, Länge: 24 Anzahl der TSs: 1, reserviert 0x0, reserviert 0x0 TS-Typ: TS_IPV4_ADDR_RANGE, Proto-ID: 0, Länge: 16 Anfangsport: 0, Endport: 65535 start addr: 0.0.0.0, end addr: 255.255.255.255	
	*11. November 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_WAIT_AUTH-Ereignis: EV_RECV_AUTH *11. November 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_WAIT_AUTH-Ereignis: EV_CHK_NAT_T *11. November 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_WAIT_AUTH-Ereignis: EV_PROC_ID *11. November 19:30:34.832: IKEv2:(SA ID = 1):Es wurden gültige Parameter in Prozess-ID empfangen. *11. November 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_WAIT_AUTH-Ereignis: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL *11. November 19:30:34.832: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_WAIT_AUTH-Ereignis: EV_GET_POLICY_BY_PEERID * 11. November 19:30:34.833: IKEv2:(1): Auswahl des IKE-Profils "IKEV2-SETUP" * 11. November 19:30:34.833: IKEv2:% Erhalten des vorinstallierten Schlüssels nach Adresse 10.0.0.1 * 11. November 19:30:34.833: IKEv2:% Erhalten des vorinstallierten Schlüssels nach Adresse 10.0.0.1 *11. November 19:30:34.833: IKEv2:Standardangebot zur Toolkit-Richtlinie hinzufügen *11. November 19:30:34.833: IKEv2:(SA-ID = 1):Verwenden des IKEv2-Profils "IKEV2-SETUP" *11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_WAIT_AUTH-Ereignis: EV_SET_POLICY * 11. November 19:30:34.833: IKEv2:(SA-ID = 1):Festlegen konfigurierter Richtlinien	Rout auf d das v wurd enthä (SPI/ IDr.(AUT SAr2 dem Trans in IK TSr(Traff entha Ziela bzw. Weit von v Date Adre der g und v getun Para ident empf

*11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_WAIT_AUTH-Ereignis: EV_VERIFY_POLICY_BY_PEERID
*11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_WAIT_AUTH-Ereignis: EV_CHK_AUTH4EAP
*11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_WAIT_AUTH-Ereignis: EV_CHK_POLREQEAP
*11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_VERIFY_AUTH-Ereignis: EV_CHK_AUTH_TYPE
*11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_VERIFY_AUTH-Ereignis: EV_GET_PRESHR_KEY
*11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_VERIFY_AUTH-Ereignis: EV_VERIFY_AUTH
*11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_VERIFY_AUTH-Ereignis: EV_CHK4_IC
*11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_VERIFY_AUTH-Ereignis: EV_CHK_REDIRECT
* 11. November 19:30:34.833: IKEv2:(SA-ID = 1):Eine Umleitungsprüfung ist nicht erforderlich. Sie wird übersprungen.
*11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_VERIFY_AUTH-Ereignis: EV_NOTIFY_AUTH_DONE
*11. November 19:30:34.833: IKEv2:AAA-Gruppenautorisierung ist nicht konfiguriert
*11. November 19:30:34.833: IKEv2:AAA-Benutzerautorisierung ist nicht konfiguriert
*11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_VERIFY_AUTH-Ereignis: EV_CHK_CONFIG_MODE
*11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_VERIFY_AUTH-Ereignis: EV_SET_RECD_CONFIG_MODE
*11. November 19:30:34.833: IKEv2:Empfangene Konfigurationsdaten aus Toolkit:
*11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_VERIFY_AUTH-Ereignis: EV_PROC_SA_TS
*11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_VERIFY_AUTH-Ereignis: EV_GET_CONFIG_MODE

	*11. November 19:30:34.833: IKEv2:Fehler beim Erstellen der Konfigurationsantwort *11. November 19:30:34.833: IKEv2:Keine Konfigurationsdaten zum Senden an Toolkit: *11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_BLD_AUTH-Ereignis: EV_MY_AUTH_METHOD *11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_BLD_AUTH-Ereignis: EV_GET_PRESHR_KEY *11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_BLD_AUTH-Ereignis: EV_GEN_AUTH *11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_BLD_AUTH-Ereignis: EV_CHK4_SIGN *11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_BLD_AUTH-Ereignis: EV_OK_AUTH_GEN *11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: R_BLD_AUTH-Ereignis: EV_SEND_AUTH *11. November 19:30:34.833: IKEv2:Aufbau anbieterspezifischer Payload: CISCO-GRANITE *11. November 19:30:34.833: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE *11. November 19:30:34.833: IKEv2:Construct Notify Payload: ESP_TFC_NO_SUPPORT *11. November 19:30:34.833: IKEv2:Construct Notify Payload: NON_FIRST_FRAGS	
	*11. November 19:30:34.833: IKEv2:(SA ID = 1):Nächste Nutzlast: ENCR, Version: 2.0 Austauschtyp: **IKE_AUTH**, Flags: **RESPONDER MSG-RESPONSE** Nachrichtenkennung: 1, Länge: 252 Payload-Inhalte: **ENCR** Nächste Nutzlast: VID, reserviert: 0x0, Länge: 224 *11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: AUTH_DONE-Ereignis: EV_OK *11. November 19:30:34.833: IKEv2:(SA-ID = 1):Aktion: Action_Null *11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: AUTH_DONE-Ereignis: EV_PKI_SESH_CLOSE *11. November 19:30:34.833: IKEv2:(SA ID = 1):PKI-Sitzung wird geschlossen *11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: AUTH_DONE-Ereignis: EV_UPDATE_CAC_STATS *11. November 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: AUTH_DONE-Ereignis:**EV_INSERT_IKE** *11. November 19:30:34.834: IKEv2:Store mib index ikev2 1, platform 60	Der I Antw

	*11. November 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: AUTH_DONE-Ereignis: EV_GEN_LOAD_IPSEC *11. November 19:30:34.834: IKEv2:(SA-ID = 1):Asynchrone Anforderung in Warteschlange gestellt *11. November 19:30:34.834: IKEv2:(SA-ID = 1): *11. November 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: **AUTH_DONE** Ereignis: EV_NO_EVENT		
<----------Responder hat IKE_AUTH---------- gesend			
Initiator erhält Antwort von Responder.	*11. November 19:30:34.834: IKEv2:Paket vom Verteiler erhalten *11. November 19:30:34.834: IKEv2:Verarbeiten eines Elements aus der Paket-Warteschlange	*11. November 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: AUTH_DONE-Ereignis: EV_OK_RECD_LOAD_IPSEC *11. November 19:30:34.840: IKEv2:(SA-ID = 1):Aktion: Action_Null *11. November 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: AUTH_DONE-Ereignis: EV_START_ACCT *11. November 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: AUTH_DONE-Ereignis: EV_CHECK_DUPE *11. November 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: AUTH_DONE-Ereignis: EV_CHK4_ROLE	Der I Eintr
Router 1 überprüft und verarbeitet die Authentifizierungsdaten in diesem Paket. Router 1 fügt diese SA dann in seine SAD ein.	*11. November 19:30:34.834: IKEv2:(SA ID = 1):Nächste Nutzlast: ENCR, Version: 2.0 Austauschtyp: **IKE_AUTH**, Flags: **RESPONDER MSG-RESPONSE** Nachrichtenkennung: 1, Länge: 252 **Payload-Inhalte:** * 11. November 19:30:34.834: IKEv2:Analyse anbieterspezifischer Payload: (CUSTOM) VID Nächste Payload: IDr., reserviert: 0x0, Länge: 20 **IDr.** Nächste Nutzlast: AUTH, reserviert: 0x0, Länge: 12		

ID-Typ: IPv4-Adresse, Reserviert: 0x0 0x0
AUTH Nächste Nutzlast: SA, reserviert: 0x0, Länge: 28
Auth-Methode PSK, reserviert: 0x0, reserviert: 0x0
SA Nächste Nutzlast: TSi, reserviert: 0x0, Länge: 40
letztes Angebot: 0x0, reserviert: 0x0, Länge: 36
Vorschlag: 1, Protokoll-ID: ESP, SPI-Größe: 4, #trans: 3 Letzte Transformation: 0x3, reserviert: 0x0: Länge: 8
Typ: 1, reserviert: 0x0, ID: 3DES
letzte Transformation: 0x3, reserviert: 0x0: Länge: 8
Typ: 3, reserviert: 0x0, ID: SHA96
letzte Transformation: 0x0, reserviert: 0x0: Länge: 8
Typ: 5, reserviert: 0x0, ID: ESN nicht verwenden
TSi Nächste Nutzlast: TSr, reserviert: 0x0, Länge: 24
Anzahl der TSs: 1, reserviert 0x0, reserviert 0x0
TS-Typ: TS_IPV4_ADDR_RANGE, Proto-ID: 0, Länge: 16
Anfangsport: 0, Endport: 65535
start addr: 0.0.0.0, end addr: 255.255.255.255
TSr Nächste Nutzlast: NOTIFY, reserviert: 0x0, Länge: 24
Anzahl der TSs: 1, reserviert 0x0, reserviert 0x0
TS-Typ: TS_IPV4_ADDR_RANGE, Proto-ID: 0, Länge: 16
Anfangsport: 0, Endport: 65535
start addr: 0.0.0.0, end addr: 255.255.255.255

*Nov 11 19:30:34.834: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE) Nächste Payload: NOTIFY, reserviert: 0x0, Länge: 12
Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: SET_WINDOW_SIZE

*Nov 11 19:30:34.834: IKEv2:Parse Notify Payload: ESP_TFC_NO_SUPPORT NOTIFY(ESP_TFC_NO_SUPPORT) Nächste Payload: NOTIFY, reserviert: 0x0, Länge: 8
Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: ESP_TFC_NO_SUPPORT

*Nov 11 19:30:34.834: IKEv2:Parse Notify Payload: NON_FIRST_FRAGS NOTIFY(NON_FIRST_FRAGS) Nächste Payload: NONE, reserviert: 0x0, Länge: 8
Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: NON_FIRST_FRAGS

*11. November 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: I_WAIT_AUTH-Ereignis:**EV_RECV_AUTH**
*11. November 19:30:34.834: IKEv2:(SA-ID = 1):Aktion: Action_Null
*11. November 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: I_PROC_AUTH-Ereignis: EV_CHK4_NOTIFY
*11. November 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: I_PROC_AUTH-Ereignis:**EV_PROC_MSG**
*11. November 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: I_PROC_AUTH-Ereignis: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL

*11. November 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: I_PROC_AUTH-Ereignis: EV_GET_POLICY_BY_PEERID
*11. November 19:30:34.834: IKEv2:Adding Proposal PHASE1-prop to toolkit policy
*11. November 19:30:34.834: IKEv2:(SA-ID = 1):Verwenden des IKEv2-Profils "IKEV2-SETUP"
*11. November 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: I_PROC_AUTH-Ereignis: EV_VERIFY_POLICY_BY_PEERID
*11. November 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: I_PROC_AUTH-Ereignis: EV_CHK_AUTH_TYPE
*11. November 19:30:34.834: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: I_PROC_AUTH-Ereignis: EV_GET_PRESHR_KEY
*11. November 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: I_PROC_AUTH-Ereignis:**EV_VERIFY_AUTH**
*11. November 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: I_PROC_AUTH-Ereignis: EV_CHK_EAP
*11. November 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: I_PROC_AUTH-Ereignis:**EV_NOTIFY_AUTH_DONE**
*11. November 19:30:34.835: IKEv2:AAA-Gruppenautorisierung ist nicht konfiguriert
*11. November 19:30:34.835: IKEv2:AAA-Benutzerautorisierung ist nicht konfiguriert
*11. November 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: I_PROC_AUTH-Ereignis: EV_CHK_CONFIG_MODE
*11. November 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: I_PROC_AUTH-Ereignis: EV_CHK4_IC
*11. November 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: I_PROC_AUTH-Ereignis: EV_CHK_IKE_ONLY
*11. November 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: I_PROC_AUTH-Ereignis: EV_PROC_SA_TS
*11. November 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: AUTH_DONE-Ereignis: EV_OK
*11. November 19:30:34.835: IKEv2:(SA-ID = 1):Aktion: Action_Null
*11. November 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: AUTH_DONE-Ereignis: EV_PKI_SESH_CLOSE
*11. November 19:30:34.835: IKEv2:(SA ID = 1):PKI-Sitzung wird geschlossen

	*11. November 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: AUTH_DONE-Ereignis: EV_UPDATE_CAC_STATS *11. November 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: AUTH_DONE-Ereignis: EV_INSERT_IKE *11. November 19:30:34.835: IKEv2:Store mib index ikev2 1, platform 60 *11. November 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: AUTH_DONE-Ereignis: EV_GEN_LOAD_IPSEC *11. November 19:30:34.835: IKEv2:(SA-ID = 1):Asynchrone Anforderung in Warteschlange gestellt *11. November 19:30:34.835: IKEv2:(SA-ID = 1): *11. November 19:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: AUTH_DONE-Ereignis: EV_NO_EVENT *11. November 19:30:34.835: IKEv2:KMI-Nachricht 8 verbraucht. Keine Maßnahmen ergriffen. *11. November 19:30:34.835: IKEv2:KMI-Nachricht 12 verbraucht. Keine Maßnahmen ergriffen. *11. November 19:30:34.835: IKEv2:Keine Daten zum Senden im Modus-Konfigurationssatz. *11. November 19:30:34.841: IKEv2:IDENT-Handle 0x80000002 hinzugefügt, verknüpft mit SPI 0x9506D414 für Sitzung 8 *11. November 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: AUTH_DONE-Ereignis: EV_OK_RECD_LOAD_IPSEC *11. November 19:30:34.841: IKEv2:(SA-ID = 1):Aktion: Action_Null *11. November 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: AUTH_DONE-Ereignis: EV_START_ACCT *11. November 19:30:34.841: IKEv2:(SA-ID = 1):Abrechnung nicht erforderlich *11. November 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: AUTH_DONE-Ereignis: EV_CHECK_DUPE *11. November 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: **AUTH_DONE** Ereignis: EV_CHK4_ROLE		
Der Tunnel ist auf dem Initiator aktiv, und der Status *zeigt READY an*.	*11. November 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: BEREITvent: EV_CHK_IKE_ONLY *11. November 19:30:34.841: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B	*****11. November 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: **READY**-Ereignis: EV_R_OK *11. November 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BD5A59F0B	Tunn Resp Tunn vor d

	R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Cur Status: READY-Ereignis: EV_I_OK	R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Cur Status: READY-Veranstaltung: EV_NO_EVENT	

CHILD_SA-Debugger

Dieser Austausch besteht aus einem einzelnen Anforderung/Antwort-Paar und wurde in IKEv1 als Phase-2-Austausch bezeichnet. Sie kann von beiden Seiten der IKE_SA initiiert werden, nachdem die ersten Austauschvorgänge abgeschlossen sind.

Router 1 CHILD_SA - Beschreibung der Nachricht	Fehlerbehebung	Router 2 CHILD_SA - Beschreibung der Nachricht
Router 1 initiiert den CHILD_SA-Austausch. Dies ist die CREATE_CHILD_SA-Anforderung. Das Paket CHILD_SA enthält normalerweise: • SA HDR (Version.Flags/Austauschtyp) • Nonce Ni (optional): Wenn der CHILD_SA als Teil des ersten Austauschs erstellt wird, darf eine zweite KE-Nutzlast und nonce nicht gesendet werden) • SA-Payload • KEi (Key-optional): Die CREATE_CHILD_SA-Anfrage kann optional eine KE-Nutzlast für einen zusätzlichen DH-Austausch enthalten, um stärkere Garantien der Weiterleitungsgeheimnis für die CHILD_SA zu ermöglichen. Wenn die SA-Angebote unterschiedliche DH-Gruppen enthalten, muss KEi ein Element der Gruppe sein, die der Initiator vom Responder zu akzeptieren erwartet. Wenn er falsch erraten wird, schlägt der CREATE_CHILD_SA-Austausch fehl, und er kann es mit einer anderen KEi erneut versuchen. • N(Payload benachrichtigen - optional). Über die Benachrichtigungsnutzlast werden Informationsdaten, z. B. Fehlerbedingungen und Statusübergänge, an einen IKE-	*11. November 19:31:35.873: IKEv2:Paket vom Verteiler erhalten *11. November 19:31:35.873: IKEv2:Verarbeiten eines Elements aus der Paket-Warteschlange *11. November 19:31:35.873: IKEv2:(SA-ID = 2):Anfrage hat mess_id 3; erwartet werden 3 bis 7 *11. November 19:31:35.873: IKEv2:(SA ID = 2):Nächste Nutzlast: ENCR, Version: 2.0 **Austauschtyp: CREATE_CHILD_SA**, Markierungen: **INITIATOR** Nachrichten-ID: 3, Länge: 396 Payload-Inhalte: **SA** Nächste Nutzlast: N, reserviert: 0x0, Länge: 152 letztes Angebot: 0x0, reserviert: 0x0, Länge: 148 Angebot: 1, Protokoll-ID: IKE, SPI-Größe: 8, #trans: 15 letzte Transformation: 0x3, reserviert: 0x0: Länge: 12 Typ: 1, reserviert: 0x0, ID: AES-CBC letzte Transformation: 0x3, reserviert: 0x0: Länge: 12 Typ: 1, reserviert: 0x0, ID: AES-CBC letzte Transformation: 0x3, reserviert: 0x0: Länge: 12 Typ: 1, reserviert: 0x0, ID: AES-CBC letzte Transformation: 0x3, reserviert: 0x0: Länge: 8	

Peer übertragen. Eine Notify Payload kann in einer Antwortnachricht (in der Regel gibt sie an, warum eine Anforderung abgelehnt wurde), in einem INFORMATIONSAUSTAUSCH (um einen Fehler nicht in einer IKE-Anforderung zu melden) oder in einer anderen Nachricht erscheinen, um die Absenderfunktionen anzugeben oder die Bedeutung der Anforderung zu ändern.Wenn dieser CREATE_CHILD_SA-Austausch eine vorhandene SA mit Ausnahme der IKE_SA erneut eingibt, MUSS die führende N Payload vom Typ REKEY_SA SA wird neu codiert. Wenn dieser CREATE_CHILD_SA-Austausch keine bestehende SA wiederholt, MUSS die N-Nutzlast weggelassen werden.	Typ: 2, reserviert: 0x0, ID: SHA512 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 2, reserviert: 0x0, ID: SHA384 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 2, reserviert: 0x0, ID: SHA256 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 2, reserviert: 0x0, ID: SHA1 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 2, reserviert: 0x0, ID: MD5 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 3, reserviert: 0x0, ID: SHA512 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 3, reserviert: 0x0, ID: SHA384 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 3, reserviert: 0x0, ID: SHA256 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 3, reserviert: 0x0, ID: SHA96 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 3, reserviert: 0x0, ID: MD596 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 4, reserviert: 0x0, ID: DH_GROUP_1536_MODP/Gruppe 5 letzte Transformation: 0x0, reserviert: 0x0: Länge: 8 Typ: 4, reserviert: 0x0, ID: DH_GROUP_1024_MODP/Gruppe 2 **N** Nächste Nutzlast: KE, reserviert: 0x0, Länge: 24 **KE** Nächste Nutzlast: NOTIFY, reserviert: 0x0, Länge: 136 DH-Gruppe: 2, Reserviert: 0x0 *Nov 11 19:31:35.874: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE **NOTIFY(**SET_WINDOW_SIZE) Nächste Payload: NONE, reserviert: 0x0, Länge: 12 Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: SET_WINDOW_SIZE *11. November 19:31:35.874: IKEv2:(**SA ID = 2**):SM Trace-> SA:	

	I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CID urState: READY-Ereignis: **EV_RECV_CREATE_CHILD** *11. November 19:31:35.874: IKEv2:(SA-ID = 2):Aktion: Action_Null *11. November 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHR ILD_R_INIT-Ereignis: EV_RECV_CREATE_CHILD *11. November 19:31:35.874: IKEv2:(SA-ID = 2):Aktion: Action_Null *11. November 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHR ILD_R_INIT-Ereignis: EV_VERIFY_MSG *11. November 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHR ILD_R_INIT-Ereignis: EV_CHK_CC_TYPE *11. November 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_IKE-Veranstaltung: **EV_REKEY_IKESA** *11. November 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHR ILD_R_IKE-Ereignis: EV_GET_IKE_POLICY *11.11.19:31:35.874: IKEv2:% **Erhalten des vorinstallierten Schlüssels nach Adresse 10.0.0.2** * 11. November 19:31:35.874: IKEv2:% Erhalten des vorinstallierten Schlüssels nach Adresse 10.0.0.2 *11. November 19:31:35.874:	

	IKEv2:Adding Proposal PHASE1-prop to toolkit policy *11. November 19:31:35.874: IKEv2:(SA-ID = 2):Verwenden des IKEv2-Profils "IKEV2-SETUP" *11. November 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHR ILD_R_IKE-Ereignis: EV_PROC_MSG *11. November 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHR ILD_R_IKE-Ereignis: EV_SET_POLICY * 11.11.1931:35.874: IKEv2:(SA-ID = 2):**Festlegen konfigurierter Richtlinien** *11. November 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHR ILD_R_BLD_MSG-Ereignis: EV_GEN_DH_KEY *11. November 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHR ILD_R_BLD_MSG-Ereignis: EV_NO_EVENT *11. November 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHR ILD_R_BLD_MSG-Ereignis: EV_OK_RECD_DH_PUBKEY_RESP *11. November 19:31:35.874: IKEv2:(SA-ID = 2):Aktion: Action_Null *11. November 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG-Ereignis:**EV_GEN_DH_SECRET**	

*11. November 19:31:35.881:
IKEv2:(SA ID = 2):SM Trace-> SA:
I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R)
MsgID = 00000003 CurState: CHR
ILD_R_BLD_MSG-Ereignis:
EV_NO_EVENT
*11. November 19:31:35.882:
IKEv2:(SA ID = 2):SM Trace-> SA:
I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R)
MsgID = 00000003 CurState: CHR
ILD_R_BLD_MSG-Ereignis:
EV_OK_RECD_DH_SECRET_RESP
*11. November 19:31:35.882:
IKEv2:(SA-ID = 2):Aktion:
Action_Null
*11. November 19:31:35.882:
IKEv2:(SA ID = 2):SM Trace-> SA:
I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (R)
MsgID = 00000003 CurState: CHR
ILD_R_BLD_MSG-Ereignis:
EV_BLD_MSG
* 11. Nov. 19:31:35.882:
IKEv2:ConstructNotify Payload:
SET_WINDOW_SIZE
Payload-Inhalte:
SA Nächste Nutzlast: N, reserviert:
0x0, Länge: 56
letztes Angebot: 0x0, reserviert: 0x0,
Länge: 52
Angebot: 1, Protokoll-ID: IKE, SPI-
Größe: 8, #trans: 4 letzte
Transformation: 0x3, reserviert: 0x0:
Länge: 12
Typ: 1, reserviert: 0x0, ID: AES-
CBC
letzte Transformation: 0x3,
reserviert: 0x0: Länge: 8
Typ: 2, reserviert: 0x0, ID: SHA1
letzte Transformation: 0x3,
reserviert: 0x0: Länge: 8
Typ: 3, reserviert: 0x0, ID: SHA96
letzte Transformation: 0x0,
reserviert: 0x0: Länge: 8
Typ: 4, reserviert: 0x0, ID:
DH_GROUP_1024_MODP/Gruppe 2
N Nächste Nutzlast: KE, reserviert:
0x0, Länge: 24
KE Nächste Nutzlast: NOTIFY,
reserviert: 0x0, Länge: 136
DH-Gruppe: 2, Reserviert: 0x0

	NOTIFY(SET_WINDOW_SIZE) Nächste Nutzlast: KEINE, reserviert: 0x0, Länge: 12 Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: SET_WINDOW_SIZE	
	*11. November 19:31:35.869: IKEv2:(**SA ID = 2**):Nächste Nutzlast: ENCR, Version: 2.0 Austauschtyp: **CREATE_CHILD_SA**, Flags: **INITIATOR** Nachrichten-ID: 2, Länge: 460 Payload-Inhalte: ENCR Nächste Nutzlast: SA, reserviert: 0x0, Länge: 432 *11. November 19:31:35.873: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE Payload-Inhalte: **SA** Nächste Nutzlast: N, reserviert: 0x0, Länge: 152 letztes Angebot: 0x0, reserviert: 0x0, Länge: 148 Angebot: 1, Protokoll-ID: IKE, SPI-Größe: 8, #trans: 15 letzte Transformation: 0x3, reserviert: 0x0: Länge: 12 Typ: 1, reserviert: 0x0, ID: AES-CBC letzte Transformation: 0x3, reserviert: 0x0: Länge: 12 Typ: 1, reserviert: 0x0, ID: AES-CBC letzte Transformation: 0x3, reserviert: 0x0: Länge: 12 Typ: 1, reserviert: 0x0, ID: AES-CBC letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 2, reserviert: 0x0, ID: SHA512 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 2, reserviert: 0x0, ID: SHA384 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 2, reserviert: 0x0, ID: SHA256 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 2, reserviert: 0x0, ID: SHA1 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 2, reserviert: 0x0, ID: MD5 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8	Dieses Paket wird von Router 2 empfangen.

	Typ: 3, reserviert: 0x0, ID: SHA512 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 3, reserviert: 0x0, ID: SHA384 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 3, reserviert: 0x0, ID: SHA256 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 3, reserviert: 0x0, ID: SHA96 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 3, reserviert: 0x0, ID: MD596 letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 4, reserviert: 0x0, ID: DH_GROUP_1536_MODP/Gruppe 5 letzte Transformation: 0x0, reserviert: 0x0: Länge: 8 Typ: 4, reserviert: 0x0, ID: DH_GROUP_1024_MODP/Gruppe 2 **N** Nächste Nutzlast: KE, reserviert: 0x0, Länge: 24 **KE** Nächste Nutzlast: NOTIFY, reserviert: 0x0, Länge: 136 DH-Gruppe: 2, Reserviert: 0x0 **NOTIFY**(SET_WINDOW_SIZE) Nächste Nutzlast: KEINE, reserviert: 0x0, Länge: 12 Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: SET_WINDOW_SIZE	
	*11. November 19:31:35.882: IKEv2:(**SA ID = 2**):Nächste Nutzlast: ENCR, Version: 2.0 Austauschtyp: **CREATE_CHILD_SA,** Flags: **RESPONDER MSG-RESPONSE** Nachrichtenkennung: 3, Länge: 300 Payload-Inhalte: **SA** Nächste Nutzlast: N, reserviert: 0x0, Länge: 56 letztes Angebot: 0x0, reserviert: 0x0, Länge: 52 Angebot: 1, Protokoll-ID: IKE, SPI-Größe: 8, #trans: 4 letzte Transformation: 0x3, reserviert: 0x0: Länge: 12 Typ: 1, reserviert: 0x0, ID: AES-CBC letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 2, reserviert: 0x0, ID: SHA1	Router 2 erstellt nun die Antwort für den CHILD_SA-Austausch. Dies ist die CREATE_CHILD_SA Antwort. Das Paket CHILD_SA enthält normalerweise: • SA HDR (Version.Flags/Austauschty • Nonce Ni(optional): Wenn der CHILD_SA als Teil des ersten Austauschs erstellt wird, darf eine zweite KE-Nutzlast und nonce nicht gesendet werden. • SA-Payload • KEi (Key-optional): Die CREATE_CHILD_SA-Anfrage kann optional eine KE-Nutzlast für einen zusätzlichen DH-Austausch enthalten, um stärkere

	letzte Transformation: 0x3, reserviert: 0x0: Länge: 8 Typ: 3, reserviert: 0x0, ID: SHA96 letzte Transformation: 0x0, reserviert: 0x0: Länge: 8 Typ: 4, reserviert: 0x0, ID: DH_GROUP_1024_MODP/Gruppe 2 **N** Nächste Nutzlast: KE, reserviert: 0x0, Länge: 24 **KE** Nächste Nutzlast: NOTIFY, reserviert: 0x0, Länge: 136 DH-Gruppe: 2, Reserviert: 0x0 *Nov 11 19:31:35.882: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE **NOTIFY(**SET_WINDOW_SIZE) Nächste Payload: NONE, reserviert: 0x0, Länge: 12 Sicherheitsprotokoll-ID: IKE, SPI-Größe: 0, Typ: SET_WINDOW_SIZE *11. November 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: **CHILD_I_WAIT-**Ereignis: **EV_RECV_CREATE_CHILD** *11. November 19:31:35.882: IKEv2:(SA-ID = 2):Aktion: Action_Null *11. November 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: **CHILD_I_PROC-**Ereignis: EV_CHK4_NOTIFY *11. November 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHILD_I_PROC-Ereignis: **EV_VERIFY_MSG** *11. November 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHR ILD_I_PROC-Ereignis: EV_PROC_MSG	Garantien der Weiterleitungsgeheimnis für die CHILD_SA zu ermöglichen. Wenn die SA-Angebote unterschiedliche DH-Gruppen enthalten, mus KEi ein Element der Gruppe sein, die der Initiator vom Responder zu akzeptieren erwartet. Wenn sie falsch vermutet, schlägt der CREATE_CHILD_SA-Austausch fehl und muss mi einer anderen KEi erneut versuchen. • N (Notify payload-optional) Über Notify Payload werden Informationsdaten wie Fehlerbedingungen und Statusübergänge an einen IKE-Peer übertragen. Eine Notify Payload kann in eine Antwortnachricht (in der Regel wird angegeben, warum eine Anforderung abgelehnt wurde), in einem Informationsaustausch (zum Melden eines Fehlers, der nicht in einer IKE-Anforderung enthalten ist) oder in einer anderen Nachricht erscheinen, um di Absenderfunktionen anzugeben oder die Bedeutung der Anforderung zu ändern. Wenn dieser CREATE_CHILD_SA-Austausch eine vorhandene SA mit Ausnahme der IKE_SA neu einspielt, muss die führende N-Nutzlast vor Typ REKEY_SA die SA identifizieren, die neu einprogrammiert wird. Wen dieser CREATE_CHILD_SA-Austausch keine vorhanden SA wiederholt, muss die N-Nutzlast weggelassen werden. Router 2 sendet die Antwort aus und schließt die Aktivierung der neuen CHILD SA ab.

	*11. November 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHR ILD_I_PROC-Ereignis: EV_CHK4_PFS *11. November 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHR ILD_I_PROC-Ereignis: EV_GEN_DH_SECRET *11. November 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHR ILD_I_PROC-Ereignis: EV_NO_EVENT *11. November 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHR ILD_I_PROC-Ereignis: EV_OK_RECD_DH_SECRET_RESP *11. November 19:31:35.890: IKEv2:(SA-ID = 2):Aktion: Action_Null *11. November 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHR ILD_I_PROC-Ereignis: EV_CHK_IKE_REKEY *11. November 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHR ILD_I_PROC-Ereignis: EV_GEN_SKEYID * 11. November 19:31:35.890: IKEv2:(SA-ID = 2):Schlüsselkennung generieren *11. November 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState:	

	CHILD_I_DONE Ereignis: **EV_ACTIVATE_NEW_SA** *11. November 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHR ILD_I_DONE-Ereignis: EV_UPDATE_CAC_STATS *11. November 19:31:35.890: IKEv2:New ikev2 as request activated *11. November 19:31:35.890: IKEv2: Zählung für ausgehende Verhandlungen konnte nicht verringert werden *11. November 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHR ILD_I_DONE-Ereignis: EV_CHECK_DUPE *11. November 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: CHR ILD_I_DONE-Ereignis: EV_OK *11. November 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: EXE IT-Veranstaltung: EV_CHK_PENDING *11. November 19:31:35.890: IKEv2:(SA ID = 2):Verarbeitete Antwort mit der Nachrichten-ID 3. Anforderungen können zwischen 4 und 8 gesendet werden *11. November 19:31:35.890: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000 00003 **CurState: EXIT**-Ereignis: EV_NO_EVENT	
Router 1 empfängt das Antwortpaket von Router 2 und schließt die Aktivierung von CHILD_SA ab.	*11. November 19:31:35.882: IKEv2:(SA ID = 2):Nächste Nutzlast: ENCR, Version: 2.0 Austauschtyp: **CREATE_CHILD_SA**, Flags: **RESPONDER MSG-RESPONSE** Meldungs-ID: 3, Länge: 300	

	Payload-Inhalte: ENCR Nächste Nutzlast: SA, reserviert: 0x0, Länge: 272 *11. November 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_BLD_MSG-Ereignis:**EV_CHK_IKE_REKEY** *11. November 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHR ILD_R_BLD_MSG-Ereignis: EV_GEN_SKEYID *11.11.1931:35.882: IKEv2:(SA-ID = 2):**Schlüsselkennung generieren** *11. November 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHILD_R_DONE-Ereignis**:EV_ACTIVATE_NEW_SA** *11. November 19:31:35.882: IKEv2:Store mib index ikev2 3, platform 62 *11. November 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHR ILD_R_DONE-Ereignis: EV_UPDATE_CAC_STATS *11. November 19:31:35.882: IKEv2:New ikev2 as request activated *11. November 19:31:35.882: IKEv2: Zählung für eingehende Verhandlungen konnte nicht verringert werden *11. November 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: **CHILD_R_DONE**-Ereignis: EV_CHECK_DUPE *11. November 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6	

	R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHR ILD_R_DONE-Ereignis: EV_OK *11. November 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: CHR ILD_R_DONE-Ereignis: EV_START_DEL_NEG_TMR *11. November 19:31:35.882: IKEv2:(SA-ID = 2):Aktion: Action_Null *11. November 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: EXE IT-Veranstaltung: EV_CHK_PENDING * 11. November 19:31:35.882: IKEv2:(SA ID = 2):Gesendete Antwort mit Nachrichten-ID 3. Anfragen können zwischen 4 und 8 angenommen werden. *11. November 19:31:35.882: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000 00003 **CurState: EXIT**-Ereignis: EV_NO_EVENT	

Tunnelüberprüfung

ISAKMP

Command

<#root>

show crypto ikev2 sa detailed

Router 1-Ausgabe

<#root>

Router1#

show crypto ikev2 sa detailed

```
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote             fvrf/ivrf         Status
1         10.0.0.1/500          10.0.0.2/500       none/none         READY
      Encr: AES-CBC, keysize: 128,
         Hash: SHA96, DH Grp:2,
         Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 120/10 sec
      CE id: 1006, Session-id: 4
      Status Description: Negotiation done
      Local spi: E58F925107F8B73F     Remote spi: AFD098F4147869DA
      Local id: 10.0.0.1
      Remote id: 10.0.0.2
      Local req msg id:  2       Remote req msg id:  0
      Local next msg id: 2       Remote next msg id: 0
      Local req queued:  2       Remote req queued:  0
      Local window:      5       Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes
```

Router 2-Ausgabe

<#root>

```
Router2#
```

show crypto ikev2 sa detailed

```
 IPv4 Crypto IKEv2  SA

Tunnel-id Local           Remote              fvrf/ivrf          Status
2         10.0.0.2/500    10.0.0.1/500        none/none          READY
      Encr: AES-CBC, keysize: 128, Hash: SHA96,
         DH Grp:2, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 120/37 sec
      CE id: 1006, Session-id: 4
      Status Description: Negotiation done
      Local spi: AFD098F4147869DA       Remote spi: E58F925107F8B73F
      Local id: 10.0.0.2
      Remote id: 10.0.0.1
      Local req msg id:  0              Remote req msg id:  2
      Local next msg id: 0              Remote next msg id: 2
      Local req queued:  0              Remote req queued:  2
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : No
```

IPsec

Command

<#root>

show crypto ipsec sa

> **Hinweis:** In dieser Ausgabe wird der PFS-DH-Gruppenwert im Gegensatz zu IKEv1 während der ersten Tunnelaushandlung als "PFS (Y/N): N, DH-Gruppe: none" angezeigt. Nach einem erneuten Abgleich werden jedoch die richtigen Werte angezeigt. Dies ist kein Bug, obwohl das Verhalten in Cisco Bug-ID CSCug67056 beschrieben wird. (Nur registrierte Cisco Benutzer können auf interne Cisco Tools oder Informationen zugreifen.)
> Der Unterschied zwischen IKEv1 und IKEv2 besteht darin, dass in letzterem die untergeordneten SAs als Teil des AUTH-Austauschs selbst erstellt werden. Die unter der Crypto Map konfigurierte DH-Gruppe wird nur während des erneuten Schlüsselvorgangs verwendet. Daher würden Sie bis zum ersten rekey 'PFS (Y/N): N, DH-Gruppe: none' sehen.
> Bei IKEv1 wird ein anderes Verhalten angezeigt, da die Erstellung der untergeordneten SA im Schnellmodus erfolgt und die CREATE_CHILD_SA-Nachricht über eine Bestimmung verfügt, die die Schlüsselaustausch-Nutzlast enthält, die die DH-Parameter zur Ableitung eines neuen gemeinsamen geheimen Schlüssels angibt.

Router 1-Ausgabe

<#root>

```
Router1#
```

show crypto ipsec sa

```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0,
         local addr 10.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port):
         (0.0.0.0/0.0.0.0/256/0)
   remote ident (addr/mask/prot/port):
         (0.0.0.0/0.0.0.0/256/0)
   current_peer 10.0.0.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt:
         10, #pkts digest: 10
    #pkts decaps: 10, #pkts decrypt:
         10, #pkts verify: 10
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.0.0.1,
         remote crypto endpt.: 10.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0xF6083ADD(4127734493)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x6B74CB79(1802816377)
        transform: esp-3des esp-sha-hmac ,
```

```
        in use settings ={Tunnel, }
        conn id: 18, flow_id: SW:18,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec):
         (4276853/3592)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xF6083ADD(4127734493)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 17, flow_id: SW:17,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key
         lifetime (k/sec): (4276853/3592)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

Router 2-Ausgabe

<#root>

```
Router2#
```

`show crypto ipsec sa`

```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 10.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
   current_peer 10.0.0.1 port 500
     PERMIT, flags={origin_is_acl,}
    #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: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.0.0.2,
         remote crypto endpt.: 10.0.0.1
     path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0x6B74CB79(1802816377)
```

```
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xF6083ADD(4127734493)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 17, flow_id: SW:17,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime
         (k/sec): (4347479/3584)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x6B74CB79(1802816377)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 18, flow_id: SW:18,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key
         lifetime (k/sec): (4347479/3584)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

Sie können auch die Ausgabe des Befehls **show crypto session** auf beiden Routern überprüfen. Diese Ausgabe zeigt den Tunnelsitzungsstatus als UP-ACTIVE an.

<#root>

```
Router1#
```

show crypto session

```
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.2 port 500
  IKEv2 SA: local 10.0.0.1/500 remote 10.0.0.2/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map

Router2#
```

show cry session

```
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.1 port 500
  IKEv2 SA: local 10.0.0.2/500 remote 10.0.0.1/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

Zugehörige Informationen

- **Debuggen auf IKEv2-Paket- und Protokollebene**
- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.