ASA IPsec- und IKE-Debugs (IKEv1-Hauptmodus) Fehlerbehebung TechNote

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Kernproblem
Szenario
Verwendete Debugbefehle
ASA-Konfiguration
Debuggen
Zugehörige Informationen

Einführung

In diesem Dokument werden die Debugging auf der Adaptive Security Appliance (ASA) beschrieben, wenn sowohl der Hauptmodus als auch der Pre-Shared Key (PSK) verwendet werden. Die Übersetzung bestimmter Debugzeilen in die Konfiguration wird ebenfalls behandelt.

Zu den Themen, die in diesem Dokument nicht behandelt werden, gehören die Weiterleitung des Datenverkehrs nach der Tunneleinrichtung und grundlegende Konzepte von IPsec oder Internet Key Exchange (IKE).

Voraussetzungen

Anforderungen

Die Leser dieses Dokuments sollten diese Themen kennen.

- PSK
- IKE

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Hardware- und Softwareversionen:

- Cisco ASA 9.3.2
- Router mit Cisco IOS® 12.4T

Kernproblem

IKE- und IPsec-Debuggen sind manchmal kryptisch, aber Sie können sie verwenden, um zu verstehen, wo sich ein IPsec-VPN-Tunnelerstellungsproblem befindet.

Szenario

Der Hauptmodus wird in der Regel zwischen LAN-zu-LAN-Tunneln oder, im Falle des Remote-Zugriffs (EzVPN), bei der Verwendung von Zertifikaten für die Authentifizierung verwendet.

Die Debug-Versionen stammen von zwei ASAs, die die Software Version 9.3.2 ausführen. Die beiden Geräte bilden einen LAN-zu-LAN-Tunnel.

Es werden zwei Hauptszenarien beschrieben:

- ASA als Initiator von IKE
- ASA als Verantwortlicher für IKE

Verwendete Debugbefehle

debug crypto ikev1 127

debug crypto ipsec 127

ASA-Konfiguration

IPsec-Konfiguration:

```
crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac
crypto map MAP 10 match address VPN
crypto map MAP 10 set peer 10.0.0.2
crypto map MAP 10 set transform-set TRANSFORM
crypto map MAP 10 set reverse-route
crypto map MAP interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
tunnel-group 10.0.0.2 type ipsec-l2l
tunnel-group 10.0.0.2 ipsec-attributes
 pre-shared-key cisco
access-list VPN extended permit tcp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
```

IP-Konfiguration:

```
ciscoasa#

show ip
```

```
System IP Addresses:
Interface                  Name      IP address      Subnet mask      Method
GigabitEthernet0/0       inside     192.168.1.1     255.255.255.0   manual
GigabitEthernet0/1       outside   10.0.0.1          255.255.255.0   manual
Current IP Addresses:
Interface                  Name       IP address      Subnet mask      Method
GigabitEthernet0/0       inside     192.168.1.1    255.255.255.0   manual
GigabitEthernet0/1       outside   10.0.0.1          255.255.255.0   manual
```

NAT-Konfiguration:

```
object network INSIDE-RANGE
 subnet 192.168.1.0 255.255.255.0 object network FOREIGN_NETWORK
 subnet 192.168.2.0 255.255.255
nat (inside,outside) source static INSIDE-RANGE INSIDE-RANGE destination static
FOREIGN_NETWORK FOREIGN_NETWORK no-proxy-arp route-lookup
```

Debuggen

Beschreibung der Initiator-Nachricht	Debugger	Beschreibung der Responder-Nachricht
Der Hauptmodus wechselt. Es wurden keine Richtlinien freigegeben, und die Peers befinden sich noch in MM_NO_STATE. Als Initiator beginnt die ASA, die Payload zu erstellen.	[IKEv1-DEBUG]: Pitcher: eine Schlüsselempfangende Nachricht empfangen hat, spi 0x0 IPSEC(crypto_map_check)-3: Suchen Sie nach einer Crypto Map mit 5-Tupel: Port=1, saddr=192.168.1.2, sport=2816, daddr=192.168.2.1, dport=2816 IPSEC(crypto_map_check)-3: Überprüfen der Crypto Map MAP 10: Übereinstimmung. [IKEv1]: IP = 10.0.0.2, IKE-Initiator: Neue Phase 1, Intf inside, IKE-Peer 10.0.0.2, lokale Proxyadresse 192.168.1.0, Remote-Proxyadresse 192.168.2.0, Crypto Map (MAP)	
MM1 konstruieren Dieser Prozess wirdEnthält iErster Vorschlag für IKE und sUnterstützte NAT-T-Anbieter.	[IKEv1-DEBUG]: IP = 10.0.0.2, Erstellung der **ISAKMP SA-Payload** [IKEv1 DEBUG]: IP = 10.0.0.2, Erstellung der NAT-Traversal VID über 02-Nutzlast [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellung der NAT-Traversal VID über 03-Nutzlast [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellung der NAT-Traversal VID über RFC-Nutzlast [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellen einer Fragmentierung VID + Payload erweiterter Funktionen	
MM1 senden	[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=0) mit Payloads: HDR + SA (1) + ANBIETER (13) + ANBIETER (13) + ANBIETER (13) + ANBIETER (13) + KEINE (0) Gesamtlänge: 168	
	========== ========>	
	[IKEv1]: IP = 10.0.0.2, IKE_DECODE EMPFANGENE Nachricht (msgid=0) mit Payloads: HDR + SA (1) + ANBIETER (13) + ANBIETER (13) + ANBIETER (13) + ANBIETER (13) + KEINE (0) Gesamtlänge: 164	MM1 wurde vom Initiator empfangen.
	[IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der SA-Nutzlast [IKEv1-DEBUG]: IP = 10.0.0.2, Oakley-Vorschlag zulässig [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der VID-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, empfangene NAT-Traversal-RFC-VID [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der VID-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der VID-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, empfangene NAT-Traversal über 03 VID [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der VID-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, NAT-Traversal empfangen über 20 VID [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der IKE SA-Nutzlast [IKEv1-DEBUG]: IP = 10.0.0.2, IKE SA Proposal # 1, Transform # 1 Acceptable Matches Global IKE Entry # 2	Prozess MM1. Der Vergleich von ISAKMP/IKE-Richtlinien beginnt. Der Remote-Peer gibt an, dass er NAT-T verwenden kann. Verwandte Konfiguration: *crypto isakmp-Richtlinie 10 Authentifizierung Pre-Share Verschlüsselung 3des*

		Hash-Sha *Gruppe 2* *Lebensdauer 86400* Erstellen MM2. In dieser Nachricht wählt der Befragte aus, welche isakmp-Richtlinieneinstellungen verwendet werden sollen. Außerdem werden die zu verwendenden NAT-T-Versionen angekündigt.
	[IKEv1-DEBUG]: IP = 10.0.0.2, Erstellung der ISAKMP SA-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellung der NAT-Traversal VID über 02-Nutzlast [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellen einer Fragmentierung VID + Payload erweiterter Funktionen	
	[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=0) mit Payloads: HDR + SA (1) + ANBIETER (13) + ANBIETER (13) + KEINE (0) Gesamtlänge: 128	MM2 senden
	<==========	
MM2 vom Responder empfangen.	[IKEv1]: IP = 10.0.0.2, IKE_DECODE EMPFANGENE Nachricht (msgid=0) mit Payloads: HDR + SA (1) + ANBIETER (13) + KEINE (0) Gesamtlänge: 104	
Prozess MM2.	[IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der SA-Nutzlast [IKEv1-DEBUG]: IP = 10.0.0.2, Oakley-Vorschlag zulässig [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der VID-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, empfangene NAT-Traversal-RFC-VID 30. November 10:38:29 [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellen von ke-Payload 30. November 10:38:29 [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellen einer einmaligen Payload 30. November 10:38:29 [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellen der Cisco Unity VID-Payload 30. November 10:38:29 [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellen der Xauth V6 VID-Nutzlast	
Bauen Sie MM3. Dieser Prozess wirdEnthältNAT Discovery-Payloads, Diffie- Hellman (DH) Key Exchange (KE)-Payloads (i)Nitator umfasst g, p und A auf Responder) und DPD-Unterstützung.	30. November 10:38:29 [IKEv1-DEBUG]: IP = 10.0.0.2, IOS-VID senden 30. November 10:38:29 [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellen von ASA-Spoofing IOS Vendor ID-Payload (Version: 1.0.0, Funktionen: 2000001) 30. November 10:38:29 [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellen der VID-Payload 30. November 10:38:29 [IKEv1-DEBUG]: IP = 10.0.0.2, Altiga/Cisco VPN3000/Cisco ASA GW VID senden 30. November 10:38:29 [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellung der NAT-Discovery-Payload 30. November 10:38:29 [IKEv1-DEBUG]: IP = 10.0.0.2, Computing NAT Discovery Hash 30. November 10:38:29 [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellung der NAT-Discovery-Payload 30. November 10:38:29 [IKEv1-DEBUG]: IP = 10.0.0.2, Computing NAT Discovery Hash	
MM3 senden	[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=0) mit Payloads: HDR + KE (4) + NONCE (10) + ANBIETER (13) + ANBIETER (13) + ANBIETER (13) + ANBIETER (13) + NAT-D (20) + NAT-D (20) + KEINE (0) Gesamtlänge: 304	
	==========MM3==========>	
	[IKEv1]: IP = 10.0.0.2, IKE_DECODE EMPFANGENE Nachricht (msgid=0) mit Payloads: HDR + KE (4) + NONCE (10) + ANBIETER (13) + ANBIETER (13) + ANBIETER (13) + NAT-D (130) + NAT-D (130) + KEINE (0) Gesamtlänge: 284	MM3 wird vom Initiator empfangen.
	[IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung ke-Payload	Prozess MM3.
	[IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung von ISA_KE-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung bei einmaliger Nutzlast [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der VID-Payload	Von NAT-D Payloads kann der Responder ermitteln, ob die Der

	[IKEv1-DEBUG]: IP = 10.0.0.2, empfangene DPD-VID [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der VID-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der IOS/PIX Vendor ID-Payload (Version: 1.0.0, Funktionen: 00000f6f) [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der VID-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, empfangene xauth v6-VID [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der NAT-Discovery-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, Computing NAT Discovery Hash [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der NAT-Discovery-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, Computing NAT Discovery Hash [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellen von ke-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellen einer einmaligen Payload	Initiator ist hinter NAT und wenn der Der Responder ist hinter NAT. Der Payload-Responder erhält vom DH KE Werte von p, g und A.
	[IKEv1-DEBUG]: IP = 10.0.0.2, Erstellen der Cisco Unity VID-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellen einer Xauth V6 VID-Nutzlast [IKEv1-DEBUG]: IP = 10.0.0.2, IOS-VID senden [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellen von ASA-Spoofing IOS Vendor ID-Payload (Version: 1.0.0, Funktionen: 2000001) [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellen der VID-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, Altiga senden/Cisco VPN3000/Cisco ASA GW VID [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellung der NAT-Discovery-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, Computing NAT Discovery Hash [IKEv1-DEBUG]: IP = 10.0.0.2, Erstellung der NAT-Discovery-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, Computing NAT Discovery Hash	Bauen Sie MM4. Dieser Prozess wirdEnthält NAT Discovery Payload, DH KE rEsponder erzeugt "B" und "s" (sendet "B" an Initiator) und DPD-VID
	[IKEv1]: IP = 10.0.0.2, Verbindung landete auf tunnel_group 10.0.0.2 [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Erstellen von Schlüsseln für Responder ...	Der Peer ist mit der L2L-Tunnelgruppe 10.0.0.2 verknüpft, und die Verschlüsselungs- und Hashschlüssel werden aus den obigen "s" und dem Pre-Shared-Key generiert.
	[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=0) mit Payloads: HDR + KE (4) + NONCE (10) + ANBIETER (13) + ANBIETER (13) + ANBIETER (13) + ANBIETER (13) + NAT-D (130) + NAT-D (130) + KEINE (0) Gesamtlänge: 304 <========== ==========	MM4 senden
MM4 erhalten vom Responder.	[IKEv1]: IP = 10.0.0.2, IKE_DECODE EMPFANGENE Nachricht (msgid=0) mit Payloads: HDR + KE (4) + NONCE (10) + ANBIETER (13) + ANBIETER (13) + ANBIETER (13) + ANBIETER (13) + NAT-D (20) + NAT-D (20) + KEINE (0) Gesamtlänge: 304	
Prozess MM4. Über die NAT-D-Payloads kann der Initiator jetzt bestimmen, ob die Der Initiator ist hinter NAT und wenn der Der Responder ist hinter NAT.	[IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung wie Payload [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung von ISA_KE-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung bei einmaliger Nutzlast [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der VID-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, empfangene Cisco Unity Client-VID [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der VID-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, empfangene DPD-VID [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der VID-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der IOS/PIX Vendor ID-Payload (Version: 1.0.0, Funktionen: 00000f7f)	
Von DH KE, iDer Initiator erhält "B" und kann jetzt "s" generieren.	[IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der VID-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, empfangene xauth v6-VID [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der NAT-Discovery-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, Computing NAT Discovery Hash [IKEv1-DEBUG]: IP = 10.0.0.2, Verarbeitung der NAT-Discovery-Payload [IKEv1-DEBUG]: IP = 10.0.0.2, Computing NAT Discovery Hash	
Der Peer ist mit der L2L-Tunnelgruppe 10.0.0.2 verknüpft, und der Initiator generiert	[IKEv1]: IP = 10.0.0.2, Verbindung landete auf tunnel_group 10.0.0.2 [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Generieren von Schlüsseln für Initiator..	

Verschlüsselungs- und Hashschlüssel, indem er oben "s" und den Pre-Shared-Key verwendet.			
Bauen Sie MM5. Verwandte Konfiguration: crypto isakmp identity auto	[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Erstellen der ID-Nutzlast [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Erstellen der Hash-Payload [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Computing-Hash für ISAKMP [IKEv1-DEBUG]: IP = 10.0.0.2, Constructing IOS Keep Alive Payload: vorschlag=32767/32767 Sek. [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Erstellung der dpd-Vid-Nutzlast		
Senden MM5.	[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=0) mit Payloads: HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +ANBIETER (13) + KEINE (0) Gesamtlänge: 96 ========== =====>		
Der Responder liegt nicht hinter einer NAT. Kein NAT-T erforderlich.	[IKEv1]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Automatischer NAT-Erkennungsstatus: Das Remote-Ende befindet sich NICHT hinter einem NAT-Gerät Dieses Ende liegt NICHT hinter einem NAT-Gerät.	[IKEv1]: IP = 10.0.0.2, IKE_DECODE EMPFANGENE Nachricht (msgid=0) mit Payloads: HDR + ID (5) + HASH (8) + KEINE (0) Gesamtlänge: 64	MM5 erhalten vom Initiator. Dieser Prozess wirdEnthält rRemote Peer Identity (ID) und cAnschlusslandung auf einer bestimmten Tunnelgruppe.
		[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Verarbeitungs-ID-Payload [IKEv1-DECODE]: Gruppe = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR-ID erhalten 10.0.0.2 [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Verarbeitung der Hash-Payload [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Computing-Hash für ISAKMP [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Verarbeitung benachrichtigt Payload [IKEv1]: Gruppe = 10.0.0.2, IP = 10.0.0.2,Automatische NAT [IKEv1]: IP = 10.0.0.2, Verbindung landete auf tunnel_group 10.0.0.2	Verarbeiten Sie MM5. Die Authentifizierung mit vorinstallierten Schlüsseln beginnt jetzt. Die Authentifizierung erfolgt auf beiden Peers. Daher werden zwei Gruppen entsprechender Authentifizierungspro zesse angezeigt. Verwandte Konfiguration: Tunnelgruppe 10.0.0.2 Typ ipsec-l2l
	Erkennungsstatus: Das Remote-Ende befindet sich NICHT hinter einem NAT-Gerät Dieses Ende liegt NICHT hinter einem NAT-Gerät.		Nein In diesem Fall ist NAT-T erforderlich.
	[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Erstellen der ID-Nutzlast [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Erstellen der Hash-Payload [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Computing-Hash für ISAKMP [IKEv1-DEBUG]: IP = 10.0.0.2, Constructing IOS Keep Alive Payload: vorschlag=32767/32767 Sek. [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Erstellung der dpd-Vid-Nutzlast		Konfigurieren Sie MM6. Identität senden umfasst neu gestartete Zeiten und Identität, die an Remote-Peer gesendet werden.
	[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=0) mit Payloads: HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128)		MM6 senden.

		+ANBIETER (13) + KEINE (0) Gesamtlänge: 96 <========== ==========	
			Phase 1 abgeschlossen. Starten Sie isakmp rekey timer. Verwandte Konfiguration: crypto isakmp-Richtlinie 10 Authentifizierung Pre-Share Verschlüsselung 3des Hash-Sha Gruppe 2 Lebensdauer 86400 ciscoasa# sh führt alle crypto isakmp aus crypto isakmp identity auto
MM6 erhalten vom Responder.	[IKEv1]: IP = 10.0.0.2, IKE_DECODE EMPFANGENE Nachricht (msgid=0) mit Payloads: HDR + ID (5) + HASH (8) + KEINE (0) Gesamtlänge: 64	[IKEv1]: Gruppe = 10.0.0.2, IP = 10.0.0.2, PHASE 1 ABGESCHLOSSEN [IKEv1]: IP = 10.0.0.2, Keep-Alive-Typ für diese Verbindung: DPD [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Start P1 rekey Timer: 64800 Sekunden.	
Prozess MM6. Dieser Prozess wirdEnthält rE-Mail-Identität gesendet von Peer und fdie endgültige Entscheidung bezüglich der auszuwählenden Tunnelgruppe.	[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Verarbeitungs-ID-Payload [IKEv1-DECODE]: Gruppe = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR-ID erhalten 10.0.0.2 [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Verarbeitung der Hash-Payload [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Computing-Hash für ISAKMP [IKEv1]: IP = 10.0.0.2, Verbindung landete auf tunnel_group 10.0.0.2 [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Oakley beginnt Quick Mode [IKEv1-DECODE]: Gruppe = 10.0.0.2, IP = 10.0.0.2, IKE-Initiator, der QM startet: msg id = 7b80c2b0		
Phase 1 abgeschlossen. Starten Sie den ISAKMP-rekey-Timer. Verwandte cKonfiguration: Tunnelgruppe 10.0.0.2 Typ ipsec-l2l Tunnelgruppe 10.0.0.2 ipsec-Attribute Pre-Shared Key Cisco	[IKEv1]: Gruppe = 10.0.0.2, IP = 10.0.0.2, PHASE 1 ABGESCHLOSSEN [IKEv1]: IP = 10.0.0.2, Keep-Alive-Typ für diese Verbindung: DPD Die DPD wurde ausgehandelt, und Phase 1 ist nun abgeschlossen. [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Start P1 rekey Timer: 82080 Sekunden.		
Phase 2 (Quick Mode) wird gestartet.	IPSEC: Neue embryonale SA erstellt bei 0x53FC3C00, SCB: 0x53F90A00, Richtung: eingehend SPI: 0xFD2D851F Sitzungs-ID: 0x00006000 VPIF-Nummer: 0x0000003 Tunneltyp: l2l Protokoll: esp Lebensdauer: 240 Sekunden		
Erstellen Sie QM1. Dieser Prozess umfasst Proxy-IDs und IPSek. Richtlinien. Verwandte Konfiguration: crypto ipsec-	[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, IKE hat SPI von der Key-Engine erhalten: SPI = 0xfd2d851f [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Oakley Constructing Quick Mode [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Erstellen einer leeren Hash-Payload [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Erstellung der IPSec SA-Nutzlast		

[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Erstellen von IPSec einmal Payload

[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Erstellen der Proxy-ID

[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Proxy-ID-Übertragung: Lokales Subnetz: 192.168.1.0 Maske 255.255.255.0 Protocol 1 Port 0 Remote-Subnetz: 192.168.2.0 Maske 255.255.255.0 Protokoll 1 Port 0

Das lokale Subnetz (192.168.1.0/24) und das erwartete Remote-Subnetz (192.168.2.0/24) werden gesendet.

[IKEv1-DECODE]: Gruppe = 10.0.0.2, IP = 10.0.0.2, IKE-Initiator, der den ersten Kontakt sendet

[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Erstellen der qm-Hash-Nutzlast

[IKEv1-DECODE]: Gruppe = 10.0.0.2, IP = 10.0.0.2, IKE-Initiator sendet 1st QM-Pkt: msg id = 7b80c2b0

Transformationssatz TRANSFORM esp-aes esp-sha-hmac access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0

[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=7b80c2b0) mit Payloads: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + KEINE (0) Gesamtlänge: 200

Senden QM1.

==========QM1==========

[IKEv1-DECODE]: IP = 10.0.0.2, IKE Responder startet QM: msg id = 52481cf5

[IKEv1]: IP = 10.0.0.2, IKE_DECODE EMPFANGENE Nachricht (msgid=52481cf5) mit Payloads: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + KEINE (0) Gesamtlänge: 172

QM1 wird vom Initiator empfangen. Responder startet Phase 2 (QM).

[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Verarbeitung der Hash-Payload

[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Verarbeitung SA-Nutzlast

[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Verarbeitung bei einmaliger Nutzlast

[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Verarbeitungs-ID-Payload

QM1 verarbeiten. Dieser Prozess Remote-Proxys mit lokalen und wählt akzeptable IP ausSek. Policy. Verwandte Konfiguration: crypto ipsec Transformationssatz TRANSFORM esp-aes esp-sha-hmac access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0 crypto map MAP 10-Match-Adresse VPN

[IKEv1-DECODE]: Gruppe = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID erhalten—192.168.2.0—255.255.255.0[IKEv1]: Gruppe = 10.0.0.2, IP = 10.0.0.2, empfangene Remote-IP-Proxy-Subnetzdaten in ID-Payload: Adresse 192.168.2.0, Maske 255.255.255.0, Protokoll 1, Port 0

[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Verarbeitungs-ID-Payload

[IKEv1-DECODE]: Gruppe = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID erhalten—192.168.1.0—255.255.255.0

[IKEv1]: Gruppe = 10.0.0.2, IP = 10.0.0.2, empfangene lokale IP-Proxy-Subnetzdaten in ID-Payload: Adresse 192.168.1.0, Maske 255.255.255.0, Protokoll 1, Port 0

Die Remote- und lokalen Subnetze (192.168.2.0/24 und 192.168.1.0/24) werden empfangen.

[IKEv1]: Gruppe = 10.0.0.2, IP = 10.0.0.2, QM IsRekeyed old sa not found by addr

[IKEv1]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Prüfung der statischen Crypto Map, Überprüfung der Karte = MAP, seq = 10...

[IKEv1]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Prüfung der statischen Crypto Map, Zuordnung MAP, seq = 10 ist eine erfolgreiche Übereinstimmung

[IKEv1]: Gruppe = 10.0.0.2, IP = 10.0.0.2, IKE-Remote-Peer für Crypto Map konfiguriert: MAP

Ein entsprechender statischer Kryptoeintrag wird gesucht und gefunden.

	[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Verarbeitung der IPSec SA-Nutzlast [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, IPSec SA Proposal # 1, Transform # 1 Acceptable Matches Global IPSec SA entry # 10 [IKEv1]: Gruppe = 10.0.0.2, IP = 10.0.0.2, IKE: SPI wird angefordert! IPSEC: Neue embryonale SA erstellt bei 0x53FC3698, SCB: 0x53FC2998, Richtung: eingehend SPI: 0x1698CAC7 Sitzungs-ID: 0x00004000 VPIF-Nummer: 0x0000003 Tunneltyp: l2l Protokoll: esp Lebensdauer: 240 Sekunden [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, IKE hat SPI von der Key-Engine erhalten: SPI = 0x1698cac7 [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Oakley Erstellen des Schnellmodus [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Erstellen einer leeren Hash-Payload [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Erstellung der IPSec SA-Nutzlast [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Erstellen von IPSec einmal Payload [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Erstellen der Proxy-ID [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Proxy-ID-Übertragung: Remote-Subnetz: 192.168.2.0 Maske 255.255.255.0 Protokoll 1 Port 0 Lokales Subnetz: 192.168.1.0 Maske 255.255.255.0 Protocol 1 Port 0 [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Erstellen der qm-Hash-Nutzlast [IKEv1-DECODE]: Gruppe = 10.0.0.2, IP = 10.0.0.2, IKE-Responder sendet 2nd QM pkt: msg-ID = 52481cf5 [IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=52481cf5) mit Payloads: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + KEINE (0) Gesamtlänge: 172	Erstellen Sie QM2. Dieser Prozess wirdBeinhaltet cBestätigung von Proxy-Identitäten, Tunneltyp und Die Überprüfung wird für gespiegelte Krypto-ACLs durchgeführt.
	<========== ========= [IKEv1]: IP = 10.0.0.2, IKE_DECODE EMPFANGENE Nachricht (msgid=7b80c2b0) mit Payloads: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + KEINE (0) Gesamtlänge: 200	Senden Sie QM2.
QM2 vom Responder empfangen.	[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Verarbeitung der Hash-Payload [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Verarbeitung SA-Nutzlast [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Verarbeitung bei einmaliger Nutzlast [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Verarbeitungs-ID-Payload	
QM2 verarbeiten. In diesem Prozess rRemote End sendet Parameter und Die kürzeste vorgeschlagene Lebensdauer für Phase 2 wird ausgewählt.	[IKEv1-DECODE]: Gruppe = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID erhalten—192.168.1.0—255.255.255.0 [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Verarbeitungs-ID-Payload [IKEv1-DECODE]: Gruppe = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID erhalten—192.168.2.0—255.255.255.0 [IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Verarbeitung benachrichtigt Payload [IKEv1-DECODE]: Responder Lifetime-Decodierung folgt (outb SPI[4]|attribute): [IKEv1-DECODE]: 0000: DDE50931 80010001 00020004 00000E10 ...1..... [IKEv1]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Responder Forcing Wechsel der IPSec-Neueingabe von 28.800 auf 3600 Sekunden basierend auf der Reaktion des Peers ändert die ASA bestimmte IPSEC-Attribute. In diesem Fall ist das rekey-Intervall	

[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Laden aller IPSEC-SAs
[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Generating Quick Mode Key!

Entsprechende Crypto Map "MAP" und Eintrag 10 gefunden und mit der Zugriffsliste "VPN" abgeglichen.

[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, NP-Verschlüsselungsregel sucht nach Crypto Map MAP 10-konformen ACL-VPNs: zurückgegeben cs_id=53f11198; Regel=53f11a90

[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Generating Quick Mode Key!
IPSEC: Neue embryonale SA erstellt bei 0x53FC3698,
SCB: 0x53F910F0,
Richtung: ausgehend
SPI: 0xDDE50931
Sitzungs-ID: 0x00006000
VPIF-Nummer: 0x0000003
Tunneltyp: l2l
Protokoll: esp
Lebensdauer: 240 Sekunden
IPSEC: Abgeschlossenes Host-OBSA-Update, SPI 0xDDE50931
IPSEC: Erstellen eines ausgehenden VPN-Kontexts, SPI 0xDDE50931
Flaggen: 0x0000005
SA: 0x53FC3698
SPI: 0xDDE50931
MTU: 1500 Byte
VCID: 0x0000000
Peer: 0x0000000
SCB: 0 x 01 CF218F
Kanal: 0x4C69CB80
IPSEC: Abgeschlossener ausgehender VPN-Kontext, SPI 0xDDE50931
VPN-Handle: 0x000161A4
IPSEC: Neue Verschlüsselungsregel für ausgehenden Datenverkehr, SPI 0xDDE50931
Src-Adresse: 192.168.1.0
Src-Maske: 255.255.255,0
Dst-Adresse: 192.168.2.0
Dst-Maske: 255.255.255,0
RC-Ports
Obere: 0
Unteres: 0
Op: ignorieren
Dst-Ports
Obere: 0
Unteres: 0
Op: ignorieren
Protokoll: 1
Protokoll verwenden: wahr
SPI: 0x0000000
SPI verwenden: falsch
IPSEC: Abgeschlossene Verschlüsselungsregel für ausgehenden Datenverkehr, SPI 0xDDE50931
Regel-ID: 0x53FC3AD8
IPSEC: Neue Regel für die Genehmigung ausgehender Anrufe, SPI 0xDDE50931
Src-Adresse: 10.0.0.1
Src-Maske: 255 255 255 255 255
Dst-Adresse: 10.0.0.2
Dst-Maske: 255 255 255 255 255
RC-Ports
Obere: 0
Unteres: 0
Op: ignorieren
Dst-Ports

Die Appliance hat die SPIs 0xfd2d851f und 0xdde50931f für eingehenden bzw. ausgehenden Datenverkehr generiert.

Obere: 0
Unteres: 0
Op: ignorieren
Protokoll: 50
Protokoll verwenden: wahr
SPI: 0xDDE50931
SPI verwenden: wahr
IPSEC: Abgeschlossene Regel für die Genehmigung ausgehender Anrufe, SPI 0xDDE50931
Regel-ID: 0 x 53F91538
[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, NP-Verschlüsselungsregel sucht nach Crypto Map MAP 10-konformen ACL-VPNs: zurückgegeben cs_id=53f11198; Regel=53f11a90
[IKEv1]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Sicherheitsverhandlung abgeschlossen für Initiator der LAN-to-LAN-Gruppe (10.0.0.2), eingehender SPI = 0xfd2d851f, ausgehender SPI = 0xde50931
IPSEC: Abgeschlossenes Host-IBSA-Update, SPI 0xFD2D851F
IPSEC: Erstellen eines eingehenden VPN-Kontexts, SPI 0xFD2D851F
Flaggen: 0x0000006
SA: 0x53FC3C00
SPI: 0xFD2D851F
MTU: 0 Byte
VCID: 0x0000000
Peer: 0x000161A4
SCB: 0x01CEA8EF
Kanal: 0x4C69CB80
IPSEC: Abgeschlossener eingehender VPN-Kontext, SPI 0xFD2D851F
VPN-Handle: 0 x 00018BBC
IPSEC: Aktualisierung des ausgehenden VPN-Kontexts 0x000161A4, SPI 0xDDE50931
Flaggen: 0x0000005
SA: 0x53FC3698
SPI: 0xDDE50931
MTU: 1500 Byte
VCID: 0x0000000
Peer: 0 x 00018BBC
SCB: 0 x 01 CF218F
Kanal: 0x4C69CB80

Erstellen Sie QM3. Bestätigen alle SPIs, die für den Remote-Peer erstellt wurden.

IPSEC: Abgeschlossener ausgehender VPN-Kontext, SPI 0xDDE50931
VPN-Handle: 0x000161A4
IPSEC: Ausgehende innere Regel, SPI 0xDDE50931
Regel-ID: 0x53FC3AD8
IPSEC: Ausgehende SPD-Regel, SPI 0xDDE50931
Regel-ID: 0 x 53F91538
IPSEC: Neue Regel für eingehenden Tunnelfluss, SPI 0xFD2D851F
Src-Adresse: 192.168.2.0
Src-Maske: 255.255.255,0
Dst-Adresse: 192.168.1.0
Dst-Maske: 255.255.255,0
RC-Ports
Obere: 0
Unteres: 0
Op: ignorieren
Dst-Ports
Obere: 0
Unteres: 0
Op: ignorieren
Protokoll: 1
Protokoll verwenden: wahr
SPI: 0x0000000
SPI verwenden: falsch
IPSEC: Abgeschlossene Regel für eingehenden Tunnelfluss, SPI 0xFD2D851F
Regel-ID: 0x53F91970

IPSEC: Neue Entschlüsselungsregel für eingehenden Datenverkehr, SPI 0xFD2D851F
Src-Adresse: 10.0.0.2
Src-Maske: 255 255 255 255 255
Dst-Adresse: 10.0.0.1
Dst-Maske: 255 255 255 255 255
RC-Ports
Obere: 0
Unteres: 0
Op: ignorieren
Dst-Ports
Obere: 0
Unteres: 0
Op: ignorieren
Protokoll: 50
Protokoll verwenden: wahr
SPI: 0xFD2D851F
SPI verwenden: wahr
IPSEC: Abgeschlossene Entschlüsselungsregel für eingehenden Datenverkehr, SPI 0xFD2D851F
Regel-ID: 0 x 53F91A08
IPSEC: Neue Zulassungsregel für eingehenden Datenverkehr, SPI 0xFD2D851F
Src-Adresse: 10.0.0.2
Src-Maske: 255 255 255 255 255
Dst-Adresse: 10.0.0.1
Dst-Maske: 255 255 255 255 255
RC-Ports
Obere: 0
Unteres: 0
Op: ignorieren
Dst-Ports
Obere: 0
Unteres: 0
Op: ignorieren
Protokoll: 50
Protokoll verwenden: wahr
SPI: 0xFD2D851F
SPI verwenden: wahr
IPSEC: Abgeschlossene Zulassungsregel für eingehenden Datenverkehr, SPI 0xFD2D851F
Regel-ID: 0x53F91AA0

QM3 senden

[IKEv1-DECODE]: Gruppe = 10.0.0.2, IP = 10.0.0.2, IKE-Initiator sendet 3rd QM pkt: msg id = 7b80c2b0

==========QM3==========>

[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=7b80c2b0) mit Payloads: HDR + HASH (8) + KEINE (0) Gesamtlänge: 76

Phase 2 abgeschlossen.
Der Initiator ist nun bereit, Pakete mit diesen SPI-Werten zu verschlüsseln und zu entschlüsseln.

[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, IKE hat eine KEY_ADD-msg für SA: SPI = 0xdde50931
[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Pitcher: Empfangene KEY_UPDATE, spi 0xfd2d851f
[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Start P2 rekey Timer: 3060 Sekunden.
[IKEv1]: Gruppe = 10.0.0.2, IP = 10.0.0.2, PHASE 2 ABGESCHLOSSEN (msgid=7b80c2b0)

[IKEv1]: IP = 10.0.0.2, IKE_DECODE EMPFANGENE Nachricht (msgid=52481cf5) mit Payloads: HDR + HASH (8) + KEINE (0) Gesamtlänge: 52

QM3 wurde vom Initiator empfangen.

[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Verarbeitung der Hash-Payload

QM3 verarbeiten.

[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Laden aller IPSEC-SAs

Für die Daten-SAs werden

[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Generating Quick Mode Key!

Verschlüsselungsschlüssel generiert.

[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, NP-

Während dieses

Verschlüsselungsregel sucht nach Crypto Map MAP 10-konformen ACL-VPNs: zurückgegeben cs_id=53f11198; Rule=53f11a90
[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Generating Quick Mode Key!
IPSEC: Neue embryonale SA erstellt bei 0x53F18B00,
SCB: 0x53F8A1C0,
Richtung: ausgehend
SPI: 0xDB680406
Sitzungs-ID: 0x00004000
VPIF-Nummer: 0x0000003
Tunneltyp: l2l
Protokoll: esp
Lebensdauer: 240 Sekunden
IPSEC: Abgeschlossenes Host-OBSA-Update, SPI 0xDB680406
IPSEC: Erstellen des ausgehenden VPN-Kontexts, SPI 0xDB680406
Flaggen: 0x0000005
SA: 0 x 53 F18 B00
SPI: 0xDB680406
MTU: 1500 Byte
VCID: 0x0000000
Peer: 0x0000000
SCB: 0 x 005E4849
Kanal: 0x4C69CB80
IPSEC: Abgeschlossener ausgehender VPN-Kontext, SPI 0xDB680406
VPN-Handle: 0x0000E9B4
IPSEC: Neue Verschlüsselungsregel für ausgehenden Datenverkehr, SPI 0xDB680406
Src-Adresse: 192.168.1.0
Src-Maske: 255.255.255,0
Dst-Adresse: 192.168.2.0
Dst-Maske: 255.255.255,0
RC-Ports
Obere: 0
Unteres: 0
Op: ignorieren
Dst-Ports
Obere: 0
Unteres: 0
Op: ignorieren
Protokoll: 1
Protokoll verwenden: wahr
SPI: 0x0000000
SPI verwenden: falsch
IPSEC: Abgeschlossene Verschlüsselungsregel für ausgehenden Datenverkehr, SPI 0xDB680406
Regel-ID: 0x53F89160
IPSEC: Neue Regel für die Genehmigung ausgehender Anrufe, SPI 0xDB680406
Src-Adresse: 10.0.0.1
Src-Maske: 255 255 255 255 255
Dst-Adresse: 10.0.0.2
Dst-Maske: 255 255 255 255 255
RC-Ports
Obere: 0
Unteres: 0
Op: ignorieren
Dst-Ports
Obere: 0
Unteres: 0
Op: ignorieren
Protokoll: 50
Protokoll verwenden: wahr
SPI: 0xDB680406
SPI verwenden: wahr

Prozesses SPIs werden so eingerichtet, dass Datenverkehr weitergeleitet wird.

IPSEC: Abgeschlossene Regel für die Genehmigung ausgehender Anrufe, SPI 0xDB680406
Regel-ID: 0 x 53E47E88
[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, NP-Verschlüsselungsregel sucht nach Crypto Map MAP 10-konformen ACL-VPNs: zurückgegeben cs_id=53f11198; Regel=53f11a90
[IKEv1]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Sicherheitsverhandlung abgeschlossen für LAN-to-LAN Group (10.0.0.2) Responder, eingehender SPI = 0x1698cac7, ausgehender SPI = 0xdb680406
[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, IKE hat eine KEY_ADD-msg für SA: SPI = 0xdb680406
IPSEC: Abgeschlossenes Host-IBSA-Update, SPI 0x1698CAC7
IPSEC: Erstellen eines eingehenden VPN-Kontexts, SPI 0x1698CAC7
Flaggen: 0x0000006
SA: 0x53FC3698
SPI: 0x1698CAC7
MTU: 0 Byte
VCID: 0x0000000
Peer: 0x0000E9B4
SCB: 0x005DAE51
Kanal: 0x4C69CB80
IPSEC: Abgeschlossener eingehender VPN-Kontext, SPI 0x1698CAC7
VPN-Handle: 0x00011A8C
IPSEC: Aktualisieren des ausgehenden VPN-Kontexts 0x000 E9B4, SPI 0xDB680406
Flaggen: 0x0000005
SA: 0 x 53 F18 B00
SPI: 0xDB680406
MTU: 1500 Byte
VCID: 0x0000000
Peer: 0x00011A8C
SCB: 0 x 005E4849
Kanal: 0x4C69CB80
IPSEC: Abgeschlossener ausgehender VPN-Kontext, SPI 0xDB680406
VPN-Handle: 0x0000E9B4
IPSEC: Ausgehende interne Regel, SPI 0xDB680406
Regel-ID: 0x53F89160
IPSEC: Ausgehende äußere SPD-Regel, SPI 0xDB680406
Regel-ID: 0 x 53E47E88
IPSEC: Neue Regel für eingehenden Tunnelfluss, SPI 0x1698CAC7
Src-Adresse: 192.168.2.0
Src-Maske: 255.255.255,0
Dst-Adresse: 192.168.1.0
Dst-Maske: 255.255.255,0
RC-Ports
Obere: 0
Unteres: 0
Op: ignorieren
Dst-Ports
Obere: 0
Unteres: 0
Op: ignorieren
Protokoll: 1
Protokoll verwenden: wahr
SPI: 0x0000000
SPI verwenden: falsch
IPSEC: Abgeschlossene Regel für eingehenden Tunnelfluss, SPI 0x1698CAC7
Regel-ID: 0x53FC3E80
IPSEC: Neue Entschlüsselungsregel für eingehenden Datenverkehr, SPI 0x1698CAC7
Src-Adresse: 10.0.0.2
Src-Maske: 255 255 255 255 255
Dst-Adresse: 10.0.0.1

SPIs werden den Daten-SAs zugewiesen.

Dst-Maske: 255 255 255 255 255 RC-Ports Obere: 0 Unteres: 0 Op: ignorieren Dst-Ports Obere: 0 Unteres: 0 Op: ignorieren Protokoll: 50 Protokoll verwenden: wahr SPI: 0x1698CAC7 SPI verwenden: wahr IPSEC: Abgeschlossene Entschlüsselungsregel für eingehenden Datenverkehr, SPI 0x1698CAC7 Regel-ID: 0x53FC3F18 IPSEC: Neue Regel für die Zulassung eingehender Anrufe, SPI 0x1698CAC7 Src-Adresse: 10.0.0.2 Src-Maske: 255 255 255 255 255 Dst-Adresse: 10.0.0.1 Dst-Maske: 255 255 255 255 255 RC-Ports Obere: 0 Unteres: 0 Op: ignorieren Dst-Ports Obere: 0 Unteres: 0 Op: ignorieren Protokoll: 50 Protokoll verwenden: wahr SPI: 0x1698CAC7 SPI verwenden: wahr IPSEC: Abgeschlossene Regel für eingehende Zulassen, SPI 0x1698CAC7 Regel-ID: 0x53F8AEA8	
[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Pitcher: erhalten KEY_UPDATE, spi 0x1698cac7	
[IKEv1-DEBUG]: Gruppe = 10.0.0.2, IP = 10.0.0.2, Start P2 rekey Timer: 3060 Sekunden.	Starten Sie IPsec erneut.
[IKEv1]: Gruppe = 10.0.0.2, IP = 10.0.0.2, PHASE 2 ABGESCHLOSSEN (msgid=52481cf5)	Phase 2 abgeschlossen. Sowohl der Responder als auch der Initiator können Datenverkehr verschlüsseln/entschlüsseln.

Tunnelüberprüfung

Hinweis: Da zum Auslösen des Tunnels ICMP verwendet wird, ist nur eine IPSec SA aktiv. Protokoll 1 = ICMP.

show crypto ipsec sa

```
interface: outside
  Crypto map tag: MAP, seq num: 10, local addr: 10.0.0.1
   access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
   local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/
```

1

```
/0)
   remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/
```

1

```
/0)
   current_peer: 10.0.0.2
   #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
   #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 4, #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.: 10.0.0.1/0, remote crypto endpt.: 10.0.0.2/0
   path mtu 1500, ipsec overhead 74, media mtu 1500
   current outbound spi: DB680406
   current inbound spi : 1698CAC7
  inbound esp sas:
   spi: 0x
```

1698CAC7

```
 (379112135)
      transform: esp-aes esp-sha-hmac no compression
      in use settings ={L2L, Tunnel, }
      slot: 0, conn_id: 16384, crypto-map: MAP
      sa timing: remaining key lifetime (kB/sec): (3914999/3326)
      IV size: 16 bytes
      replay detection support: Y
      Anti replay bitmap:
       0x00000000 0x0000001F
  outbound esp sas:
   spi: 0xDB680406 (3681027078)
      transform: esp-aes esp-sha-hmac no compression
      in use settings ={L2L, Tunnel, }
      slot: 0, conn_id: 16384, crypto-map: MAP
      sa timing: remaining key lifetime (kB/sec): (3914999/3326)
      IV size: 16 bytes
      replay detection support: Y
      Anti replay bitmap:
      0x00000000 0x00000001
```

show crypto isakmp sa

```
  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: 10.0.0.2
   Type    :
```

L2L

```
             Role    :
```

responder

```
   Rekey   : no              State   :
```

MM_ACTIVE

Zugehörige Informationen

- Ein guter Ausgangspunkt ist Wikipedia-Artikel zu IPSec. Standard und Referenzen enthalten viele nützliche Informationen
- IPsec-Fehlerbehebung: Verwenden von Debugbefehlen
- Technischer Support und Dokumentation - Cisco Systems