

Fehlerbehebung bei IPsec-Tunneln und häufigen Problemen auf der Kontrollebene mit Paketerfassungen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Nützliche Tools](#)

[Konfigurieren von Aufzeichnungen auf dem IOS XE-Router](#)

[Analysieren der Tunneleinrichtung mit Paketerfassungen](#)

[Transaktion, wenn NAT dazwischen liegt](#)

[Häufige Probleme auf der Kontrollebene](#)

[Konfigurationskonflikt](#)

[Erneute Übertragungen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Paketerfassungen und andere Tools bei Problemen auf Steuerungsebene helfen, wenn Site-to-Site-VPN auf Cisco IOS® XE-Routern ausgehandelt wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der Konfiguration der Cisco IOS® CLI
- Grundlegende Kenntnisse über IKEv2 und IPsec

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- CSR1000V - Cisco IOS XE Software mit Version 16.12.0

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.

Hintergrundinformationen

Die Paketerfassung ist ein leistungsstarkes Tool, mit dem Sie überprüfen können, ob Pakete zwischen VPN-Peer-Geräten gesendet/empfangen werden. Sie bestätigen auch, ob das Verhalten, das bei IPsec-Debugs beobachtet wurde, mit der Ausgabe übereinstimmt, die bei den Erfassungen erfasst wurde, da die Debugs eine logische Interpretation sind und die Erfassung die physische Interaktion zwischen den Peers darstellt. Daher können Sie Verbindungsprobleme bestätigen oder verwerfen.

Nützliche Tools

Es gibt nützliche Tools, die Ihnen helfen, die Aufnahmen zu konfigurieren, die Ausgabe zu extrahieren und weiter zu analysieren. Einige davon sind:

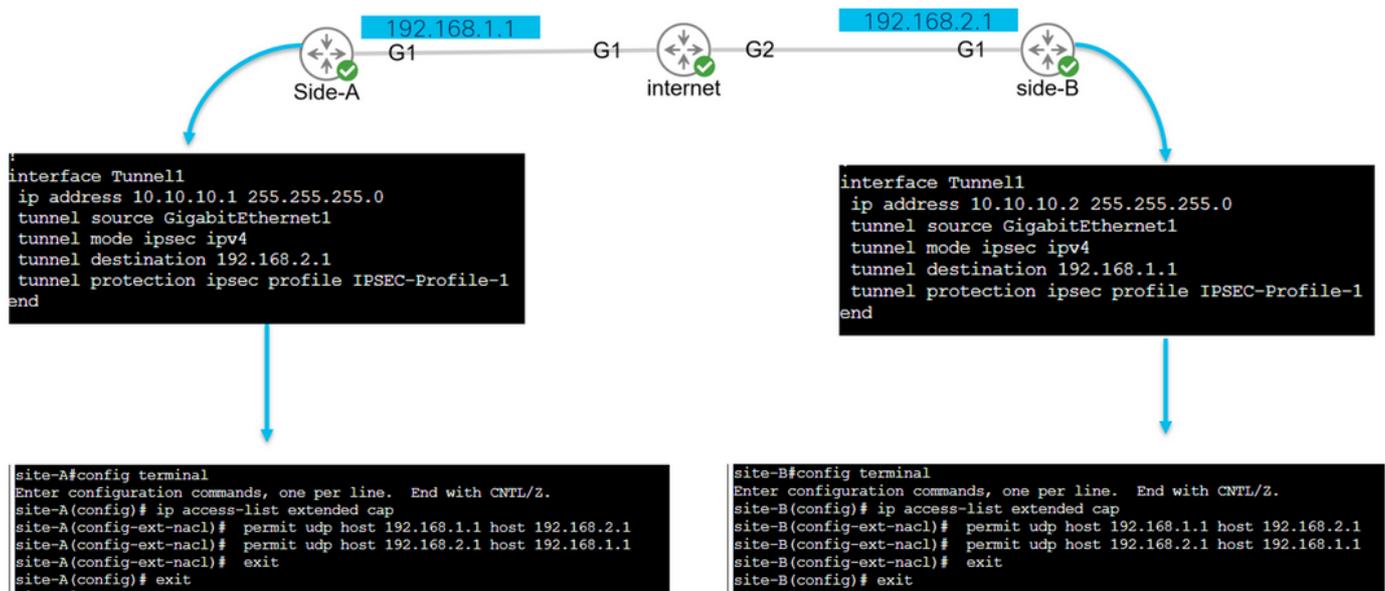
- Wireshark: Dies ist ein bekannter und häufig verwendeter Open-Source-Paketanalysator.
- Überwachungsaufzeichnungen: Die Cisco IOS XE-Funktion auf Routern unterstützt Sie beim Erfassen von Aufnahmen und liefert Ihnen eine ungefähre Ausgabe des Datenverkehrsflusses, der Protokollsammlung und der Zeitstempel.

Konfigurieren von Aufzeichnungen auf dem IOS XE-Router



Bei der Erfassung wird eine erweiterte Zugriffsliste (ACL) verwendet, die den zu erfassenden Datenverkehrstyp sowie die Quell- und Zieladressen der VPN-Peers oder Segmente des interessanten Datenverkehrs definiert. Bei einer Tunnelaushandlung werden der UDP-Port 500 und der Port 4500 verwendet, wenn NAT-T entlang des Pfads aktiviert ist. Wenn die Aushandlung abgeschlossen und der Tunnel eingerichtet ist, verwendet der interessante Datenverkehr das IP-Protokoll 50 (ESP) oder UDP 4500, wenn NAT-T aktiviert ist.

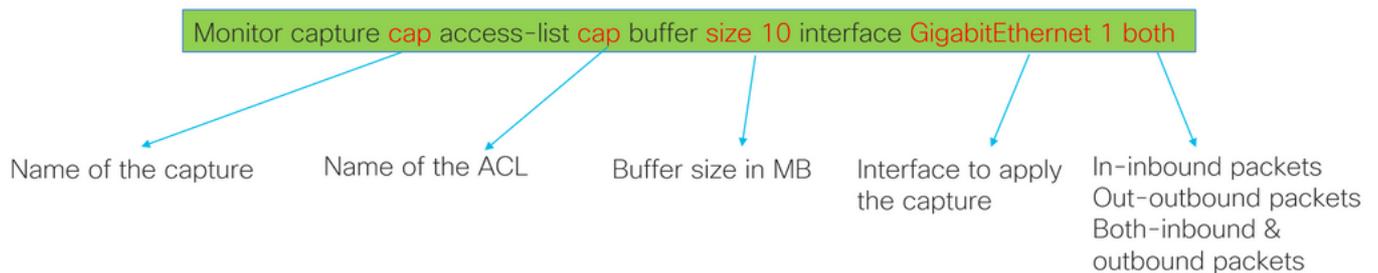
Um Probleme im Zusammenhang mit der Kontrollebene zu beheben, müssen die IP-Adressen der VPN-Peers zur Erfassung der Tunnelverhandlung verwendet werden.



```

config terminal
ip access-list extended <ACL name>
permit udp host <local address> host <peer address>
permit udp host <peer address> host <source address>
exit
exit
  
```

Die konfigurierte ACL wird verwendet, um den erfassten Datenverkehr einzuschränken, und auf der Schnittstelle platziert, über die der Tunnel ausgehandelt wird.





```
monitor capture cap access-list cap buffer size 10 interface GigabitEthernet1 both
monitor capture cap start
```

```
monitor capture cap access-list cap buffer size 10 interface GigabitEthernet1 both
monitor capture cap start
```

```
Status Information for Capture cap
Target Type:
Interface: GigabitEthernet1, Direction: BOTH
Status : Active
Filter Details:
Access-list: cap
Buffer Details:
Buffer Type: LINEAR (default)
Buffer Size (in MB): 10
Limit Details:
Number of Packets to capture: 0 (no limit)
Packet Capture duration: 0 (no limit)
Packet Size to capture: 0 (no limit)
Maximum number of packets to capture per second: 1000
Packet sampling rate: 0 (no sampling)
site-A#
```

```
Status Information for Capture cap
Target Type:
Interface: GigabitEthernet1, Direction: BOTH
Status : Active
Filter Details:
Access-list: cap
Buffer Details:
Buffer Type: LINEAR (default)
Buffer Size (in MB): 10
Limit Details:
Number of Packets to capture: 0 (no limit)
Packet Capture duration: 0 (no limit)
Packet Size to capture: 0 (no limit)
Maximum number of packets to capture per second: 1000
Packet sampling rate: 0 (no sampling)
site-B#
```

monitor capture <capture name> access-list <ACL name> buffer size <custom buffer size in MB> interface

Sobald die Erfassung konfiguriert ist, kann sie manipuliert werden, um sie zu stoppen, zu löschen oder den mit den folgenden Befehlen gesammelten Datenverkehr zu extrahieren:

- Allgemeine Erfassungsinformationen überprüfen: Überwachungserfassung anzeigen
- Starten/Stoppen der Erfassung: Start/Stop der Monitorerfassung
- Überprüfen Sie, ob die Erfassung Pakete sammelt: show monitor capture cap buffer
- Siehe eine kurze Ausgabe des Datenverkehrs: show monitor capture cap buffer brief
- Erfassung löschen: Überwachungserfassungskappe leeren
- Extrahieren Sie die Erfassungsausgabe:
 - Stopfbuchse für Monitordeckel
 - Monitor, Caption, Export, bootflash:capture.pcap

Analysieren der Tunnleinrichtung mit Paketerfassungen

Wie bereits erwähnt, werden zur Aushandlung des IPSec-Tunnels Pakete über UDP mit Port 500 und Port 4500 gesendet, wenn NAT-T aktiviert ist. Bei der Erfassung können mehr Informationen aus den Paketen angezeigt werden, z. B. die Phase, die ausgehandelt wird (Phase 1 oder Phase 2), die Rolle jedes Geräts (Initiator oder Responder) oder die SPI-Werte, die gerade erstellt wurden.

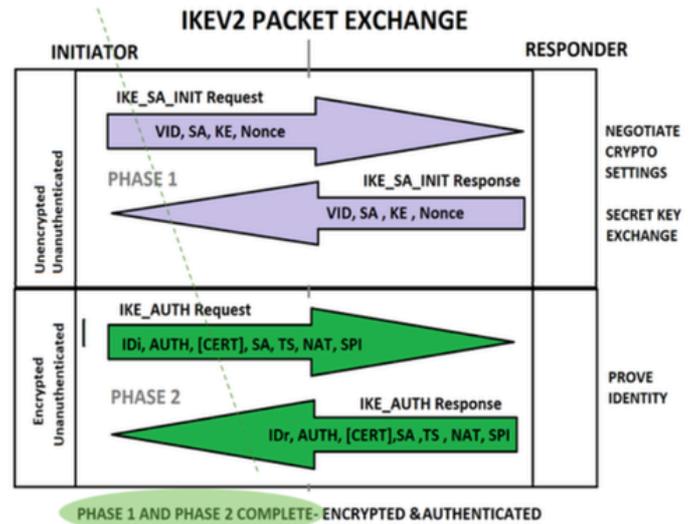
UDP 500/4500 packets seen.

Initiator and responder roles.

SPI values created.

Phase 1 in clear text.

Phase 2 encrypted



Die kurze Ausgabe der Erfassung durch den Router zeigt die Interaktion zwischen den Peers an und sendet UDP-Pakete.

```
site-A#show monitor cap cap buffer brief
```

#	size	timestamp	source	direction	destination	dscp	protocol
0	496	0.000000	192.168.1.1	->	192.168.2.1	48 CS6	UDP
1	529	0.011992	192.168.2.1	->	192.168.1.1	48 CS6	UDP
2	682	0.026991	192.168.1.1	->	192.168.2.1	48 CS6	UDP
3	362	0.035993	192.168.2.1	->	192.168.1.1	48 CS6	UDP
4	496	0.579016	192.168.2.1	->	192.168.1.1	48 CS6	UDP
5	529	0.593023	192.168.1.1	->	192.168.2.1	48 CS6	UDP
6	682	0.610020	192.168.2.1	->	192.168.1.1	48 CS6	UDP
7	362	0.616017	192.168.1.1	->	192.168.2.1	48 CS6	UDP
8	138	0.638019	192.168.2.1	->	192.168.1.1	48 CS6	UDP
9	138	0.638019	192.168.2.1	->	192.168.1.1	48 CS6	UDP
10	138	0.641009	192.168.1.1	->	192.168.2.1	48 CS6	UDP
11	138	0.655016	192.168.1.1	->	192.168.2.1	48 CS6	UDP

Nachdem der Dump extrahiert und die pcap-Datei vom Router exportiert wurde, können weitere Informationen aus den Paketen mithilfe von Wireshark angezeigt werden.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.1	192.168.2.1	ISAKMP	496	IKE_SA_INIT MID=00 Initiator Request
2	0.000000	192.168.2.1	192.168.1.1	ISAKMP	529	IKE_SA_INIT MID=00 Responder Response
3	0.000000	192.168.1.1	192.168.2.1	ISAKMP	682	IKE_AUTH MID=01 Initiator Request
4	0.000000	192.168.2.1	192.168.1.1	ISAKMP	362	IKE_AUTH MID=01 Responder Response
5	0.000000	192.168.2.1	192.168.1.1	ISAKMP	496	IKE_SA_INIT MID=00 Initiator Request
6	0.000000	192.168.1.1	192.168.2.1	ISAKMP	529	IKE_SA_INIT MID=00 Responder Response
7	0.000000	192.168.2.1	192.168.1.1	ISAKMP	682	IKE_AUTH MID=01 Initiator Request
8	0.000000	192.168.1.1	192.168.2.1	ISAKMP	362	IKE_AUTH MID=01 Responder Response
9	0.000000	192.168.2.1	192.168.1.1	ISAKMP	138	INFORMATIONAL MID=02 Initiator Request
10	0.000000	192.168.2.1	192.168.1.1	ISAKMP	138	INFORMATIONAL MID=03 Initiator Request
11	0.000000	192.168.1.1	192.168.2.1	ISAKMP	138	INFORMATIONAL MID=02 Responder Response
12	0.000000	192.168.1.1	192.168.2.1	ISAKMP	138	INFORMATIONAL MID=03 Responder Response
13	0.000000	192.168.1.1	192.168.2.1	ISAKMP	138	INFORMATIONAL MID=14 Responder Request

> Frame 1: 496 bytes on wire (3968 bits), 496 bytes captured (3968 bits)
 > Ethernet II, Src: RealtekU_00:00:00 (52:54:00:00:00:00), Dst: RealtekU_00:00:04 (52:54:00:00:00:04)
 > Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.2.1
 > User Datagram Protocol, Src Port: 500, Dst Port: 500
 > Internet Security Association and Key Management Protocol

Im Internet Protocol-Abschnitt des ersten gesendeten IKE_SA_INIT Exchange-Pakets befinden sich die Quell- und Zieladressen des UDP-Pakets. Im Bereich User Datagram Protocol werden die verwendeten Ports und im Bereich Internet Security Association and Key Management Protocol die Version des Protokolls, die Art der ausgetauschten Nachricht und die Rolle des Gerats sowie der erstellte SPI angezeigt. Beim Sammeln von IKEv2-Debugging-Meldungen werden die gleichen Informationen in den Debug-Protokollen angezeigt.

No.	Time	Source	Destination	TCP Delta Time
1	0.000	192.168.1.1	192.168.2.1	
2	0.000	192.168.2.1	192.168.1.1	
3	0.000	192.168.1.1	192.168.2.1	
4	0.000	192.168.2.1	192.168.1.1	
5	0.000	192.168.2.1	192.168.1.1	
6	0.000	192.168.1.1	192.168.2.1	
7	0.000	192.168.2.1	192.168.1.1	
8	0.000	192.168.1.1	192.168.2.1	
9	0.000	192.168.2.1	192.168.1.1	
10	0.000	192.168.2.1	192.168.1.1	
11	0.000	192.168.1.1	192.168.2.1	
12	0.000	192.168.1.1	192.168.2.1	

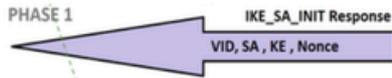
> Frame 1: 496 bytes on wire (3968 bits), 496 bytes captured (3968 bits)
 > Ethernet II, Src: RealtekU_00:00:00 (52:54:00:00:00:00), Dst: RealtekU_00:00:04 (52:54:00:00:00:04)
 > Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.2.1
 > User Datagram Protocol, Src Port: 500, Dst Port: 500
 > Internet Security Association and Key Management Protocol
 Initiator SPI: e9f5fb100567c549
 Responder SPI: 0000000000000000
 Next payload: Security Association (33)
 Version: 2.0
 Exchange type: IKE_SA_INIT (34)
 Flags: 0x08 Initiator, No higher version, Request
 Message ID: 0x00000000
 Length: 454
 > Payload: Security Association (33)
 > Payload: Key Exchange (34)
 > Payload: Nonce (40)
 > Payload: Vendor ID (43) : Cisco Delete Reason Supported
 > Payload: Vendor ID (43) : Cisco VPN Revision 2
 > Payload: Vendor ID (43) : Cisco Dynamic Route Supported
 > Payload: Vendor ID (43) : Cisco FlexVPN Supported
 > Payload: Notify (41) - NAT_DETECTION_SOURCE_IP
 > Payload: Notify (41) - NAT_DETECTION_DESTINATION_IP



```

IKEv2:(SESSION ID = 18,SA ID = 2):Sending Packet [To
192.168.2.1:500/From 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 0000000000000000
Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP)
NOTIFY(NAT_DETECTION_DESTINATION_IP)
  
```

Debug crypto ikev2
 Debug crypto ipsec



No.	Time	Source	Destination	TCP Delta Time
1	0.000	192.168.1.1	192.168.2.1	
2	0.000	192.168.2.1	192.168.1.1	
3	0.000	192.168.1.1	192.168.2.1	
4	0.000	192.168.2.1	192.168.1.1	
5	0.000	192.168.2.1	192.168.1.1	
6	0.000	192.168.1.1	192.168.2.1	
7	0.000	192.168.2.1	192.168.1.1	
8	0.000	192.168.1.1	192.168.2.1	
9	0.000	192.168.2.1	192.168.1.1	
10	0.000	192.168.2.1	192.168.1.1	
11	0.000	192.168.1.1	192.168.2.1	
12	0.000	192.168.1.1	192.168.2.1	

```

Frame 2: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits)
> Ethernet II, Src: RealtekU_00:00:04 (52:54:00:00:04), Dst: RealtekU_0
> Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 500, Dst Port: 500
  > Internet Security Association and Key Management Protocol
    Initiator SPI: e9f5fb100567c549
    Responder SPI: 4c6900b8d253af89
    Next payload: Security Association (33)
  > Version: 2.0
  > Exchange type: IKE_SA_INIT (34)
  > Flags: 0x20 (Responder, No higher version, Response)
  > Message ID: 0x00000000
  > Length: 487
  > Payload: Security Association (33)
  > Payload: Key Exchange (34)
  > Payload: Nonce (40)
  > Payload: Vendor ID (43) : Cisco Delete Reason Supported
  > Payload: Vendor ID (43) : Cisco VPN Revision 2
  > Payload: Vendor ID (43) : Cisco Dynamic Route Supported
  > Payload: Vendor ID (43) : Cisco FlexVPN Supported
  > Payload: Notify (41) - NAT_DETECTION_SOURCE_IP
  > Payload: Notify (41) - NAT_DETECTION_DESTINATION_IP
  > Payload: Certificate Request (38)
  
```

IKEv2:(SESSION ID = 18,SA ID = 2):Received Packet [From 192.168.2.1:500/To 192.168.1.1:500/VRF i0:f0]
 Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
 Message id: 0
 IKEv2 IKE_SA_INIT Exchange RESPONSE
 Payload contents:
 SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP)
 NOTIFY(NAT_DETECTION_DESTINATION_IP) CERTREQ
 NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)

Unencrypted!

Wenn die IKE_AUTH-Exchange-Aushandlung stattfindet, wird die Nutzlast verschlüsselt, es werden jedoch einige Informationen über die Aushandlung angezeigt, z. B. der zuvor erstellte SPI und die Art der ausgeführten Transaktion.



No.	Time	Source	Destination	TCP Delta Time
1	0.000	192.168.1.1	192.168.2.1	
2	0.000	192.168.2.1	192.168.1.1	
3	0.000	192.168.1.1	192.168.2.1	
4	0.000	192.168.2.1	192.168.1.1	
5	0.000	192.168.2.1	192.168.1.1	
6	0.000	192.168.1.1	192.168.2.1	
7	0.000	192.168.2.1	192.168.1.1	
8	0.000	192.168.1.1	192.168.2.1	
9	0.000	192.168.2.1	192.168.1.1	
10	0.000	192.168.2.1	192.168.1.1	
11	0.000	192.168.1.1	192.168.2.1	
12	0.000	192.168.1.1	192.168.2.1	

```

Frame 4: 362 bytes on wire (2896 bits), 362 bytes captured (2896 b
> Ethernet II, Src: RealtekU_00:00:04 (52:54:00:00:04), Dst: Real
> Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 500, Dst Port: 500
  > Internet Security Association and Key Management Protocol
    Initiator SPI: e9f5fb100567c549
    Responder SPI: 4c6900b8d253af89
    Next payload: Encrypted and Authenticated (46)
  > Version: 2.0
  > Exchange type: IKE_AUTH (35)
  > Flags: 0x20 (Responder, No higher version, Response)
  > ... 0... = Initiator: Responder
  > ...0... = Version: No higher version
  > ...1... = Response: Response
  > Message ID: 0x00000001
  > Length: 320
  > Payload: Encrypted and Authenticated (46)
  
```

IKEv2:(SESSION ID = 18,SA ID = 2):Received Packet [From 192.168.2.1:500/To 192.168.1.1:500/VRF i0:f0]
 Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
 Message id: 1
 IKEv2 IKE_AUTH Exchange RESPONSE

Encrypted!

Sobald das letzte IKE_AUTH-Exchange-Paket empfangen wurde, ist die Tunnelaushandlung abgeschlossen.

No.	Time	Source	Destination	TCP Delta
1	0.000	192.168.1.1	192.168.2.1	
2	0.000	192.168.2.1	192.168.1.1	
3	0.000	192.168.1.1	192.168.2.1	
4	0.000	192.168.2.1	192.168.1.1	
5	0.000	192.168.2.1	192.168.1.1	
6	0.000	192.168.1.1	192.168.2.1	
7	0.000	192.168.2.1	192.168.1.1	
8	0.000	192.168.1.1	192.168.2.1	
9	0.000	192.168.2.1	192.168.1.1	
10	0.000	192.168.2.1	192.168.1.1	
11	0.000	192.168.1.1	192.168.2.1	
12	0.000	192.168.1.1	192.168.2.1	


```

> Frame 3: 682 bytes on wire (5456 bits), 682 bytes captured (5456 bit
> Ethernet II, Src: RealtekU_00:00:00 (52:54:00:00:00:00), Dst: Realte
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.2.1
> User Datagram Protocol, Src Port: 500, Dst Port: 500
> Internet Security Association and Key Management Protocol
  Initiator SPI: e9f5fb100567c549
  Responder SPI: 4c6900b8d253af89
  Next payload: Encrypted and Authenticated (46)
  > Version: 2.0
  > Exchange type: IKE_AUTH (35)
  > Flags: 0x00 (Initiator, No higher version, Request)
    .... 1. .... = Initiator: Initiator
    .... 1. .... = Version: No higher version
    .... 0. .... = Response: Request
  Message ID: 0x00000001
  Length: 640
  > Payload: Encrypted and Authenticated (46)

```



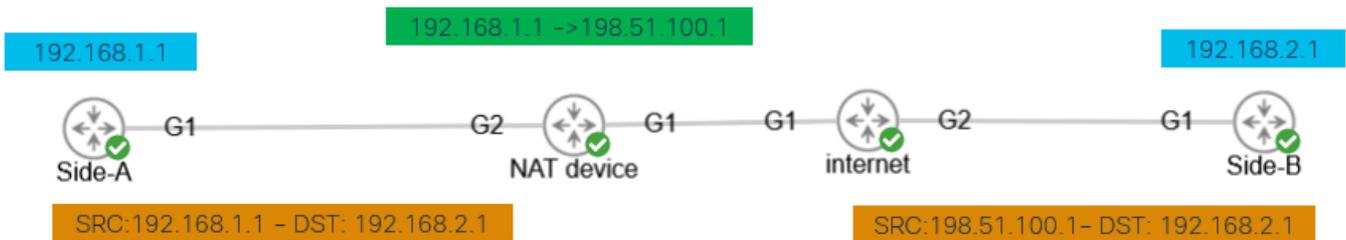
```

IKEv2:(SESSION ID = 18,SA ID = 2):Sending Packet [To
192.168.2.1:500/From 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:
ENCR

```

Encrypted!

Transaktion, wenn NAT dazwischen liegt



Eine weitere Funktion, die erkennbar ist, wenn die Tunnelaushandlung stattfindet, ist die Nat-Transversal-Funktion. Wenn ein zwischengeschaltetes Gerät eine oder beide für den Tunnel verwendete Adressen nutzt, ändern die Geräte den UDP-Port von 500 auf 4500, wenn Phase 2 (IKE_AUTH-Austausch) ausgehandelt wird.

Aufnahme von Seite A:

No.	Time	Source	Destination	Protocol	Length
1	0.00	192.168.1.1	192.168.2.1	ISAKMP	
2	0.00	192.168.2.1	192.168.1.1	ISAKMP	
3	0.00	192.168.1.1	192.168.2.1	ISAKMP	
4	0.00	192.168.2.1	192.168.1.1	ISAKMP	
5	0.00	192.168.1.1	192.168.2.1	ISAKMP	
6	0.00	192.168.2.1	192.168.1.1	ISAKMP	
7	0.00	192.168.1.1	192.168.2.1	ISAKMP	
8	0.00	192.168.2.1	192.168.1.1	ISAKMP	


```

> Frame 3: 618 bytes on wire (4944 bits), 618 bytes captured (4944
> Ethernet II, Src: RealtekU_00:00:33 (52:54:00:00:00:33), Dst: Rea
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.2.1
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
> UDP Encapsulation of IPsec Packets
> Internet Security Association and Key Management Protocol
  Initiator SPI: ec01171f30d05063
  Responder SPI: 9a0f8b75c0e01c78
  Next payload: Encrypted and Authenticated (46)
  > Version: 2.0
  > Exchange type: IKE_AUTH (35)
  > Flags: 0x00 (Initiator, No higher version, Request)
  Message ID: 0x00000001
  Length: 572
  > Payload: Encrypted and Authenticated (46)

```

```

IKEv2:(SESSION ID = 10,SA ID = 1):Received Packet [From
192.168.1.1:4500/To 192.168.2.1:4500/VRF i0:f0]
Initiator SPI : EC01171F30D05063 - Responder SPI : 9A0F8B75C0E01C78
Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
-----
IKEv2:(SESSION ID = 10,SA ID = 1):Stopping timer to wait for auth message
IKEv2:(SESSION ID = 10,SA ID = 1):Checking NAT discovery
IKEv2:(SESSION ID = 10,SA ID = 1):NAT INSIDE found
IKEv2:(SESSION ID = 10,SA ID = 1):NAT detected float to init port 4500,
resp port 4500

```

Aufnahme von Seite B:

No.	Time	Source	Destination	Protocol	Length
1	0.000000	198.51.100.1	192.168.2.1	ISAKMP	
2	0.000000	192.168.2.1	198.51.100.1	ISAKMP	
3	0.000000	198.51.100.1	192.168.2.1	ISAKMP	
4	0.000000	192.168.2.1	198.51.100.1	ISAKMP	
5	0.000000	198.51.100.1	192.168.2.1	ISAKMP	
6	0.000000	192.168.2.1	198.51.100.1	ISAKMP	
7	0.000000	198.51.100.1	192.168.2.1	ISAKMP	
8	0.000000	192.168.2.1	198.51.100.1	ISAKMP	

```

> Frame 3: 618 bytes on wire (4944 bits), 618 bytes captured (4944 b)
> Ethernet II, Src: RealtekU_00:00:33 (52:54:00:00:33), Dst: Real
> Internet Protocol Version 4, Src: 198.51.100.1, Dst: 192.168.2.1
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
> UDP Encapsulation of IPsec Packets
> Internet Security Association and Key Management Protocol
  Initiator SPI: ec01171f30d05063
  Responder SPI: 9a0f8b75c0e01c78
  Next payload: Encrypted and Authenticated (46)
  > Version: 2.0
  > Exchange type: IKE_AUTH (35)
  > Flags: 0x08 (Initiator, No higher version, Request)
  > Message ID: 0x00000001
  > Length: 572
  > Payload: Encrypted and Authenticated (46)

```

IKEv2:(SESSION ID = 11,SA ID = 1):Sending Packet [To 192.168.2.1:4500/From 198.51.100.1:4500/VRF i0:f0]
 Initiator SPI : EC01171F30D05063 - Responder SPI : 9A0F8B75C0E01C78
 Message id: 1
 IKEv2 IKE_AUTH Exchange REQUEST
 Payload contents:

Häufige Probleme auf der Kontrollebene

Lokale oder externe Faktoren können die Tunnelaushandlung beeinflussen und mit Erfassungen identifiziert werden. Die nächsten Szenarien sind die gängigsten.

Konfigurationskonflikt

Dieses Szenario lässt sich durch Betrachtung der Gerätekonfiguration in Phase 1 und Phase 2 lösen. Es kann jedoch Szenarien geben, in denen kein Zugriff auf das Remote-End möglich ist. Hilft bei der Identifizierung des Geräts, das ein NO_PROPOSAL_CHOSEN innerhalb der Pakete in Phase 1 oder 2 sendet. Diese Antwort weist darauf hin, dass möglicherweise ein Problem mit der Konfiguration besteht und welche Phase angepasst werden muss.

Side-A

Side-B

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
2	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Responder Response
3	0.000000	192.168.1.1	192.168.2.1	ISAKMP	INFORMATIONAL MID=05 Initiator Request
4	0.000000	192.168.1.1	192.168.2.1	ISAKMP	INFORMATIONAL MID=04 Initiator Request
5	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
6	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Responder Response

```

Protocol ID: IKE (1)
SPI Size: 0
Proposed Transform: 4
Payload: Transform (3)
  Next payload: Transform (3)
  Reserved: 00
  Payload length: 12
  Transform Type: Encryption Algorithm (ENCR) (1)
  Reserved: 00
  Transform ID (ENCR): ENCR_AES_CBC (12)
  > Transform Attribute (t=14,l=2): Key Length: 256
  > Payload: Transform (3)

```

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
2	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Responder Response
3	0.000000	192.168.1.1	192.168.2.1	ISAKMP	INFORMATIONAL MID=05 Initiator Request
4	0.000000	192.168.1.1	192.168.2.1	ISAKMP	INFORMATIONAL MID=04 Initiator Request
5	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
6	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Responder Response

```

> Frame 2: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
> Ethernet II, Src: RealtekU_00:00:36 (52:54:00:00:36), Dst: RealtekU_00:00:33 (52:54:00:00:33)
> Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 500, Dst Port: 500
> Internet Security Association and Key Management Protocol
  Initiator SPI: 982a79a178dd0a36
  Responder SPI: ace9e4f3f7a5c6d
  Next payload: Notify (41)
  > Version: 2.0
  > Exchange type: IKE_SA_INIT (34)
  > Flags: 0x20 (Responder, No higher version, Response)
  > Message ID: 0x00000000
  > Length: 36
  > Payload: Notify (41) - NO_PROPOSAL_CHOSEN

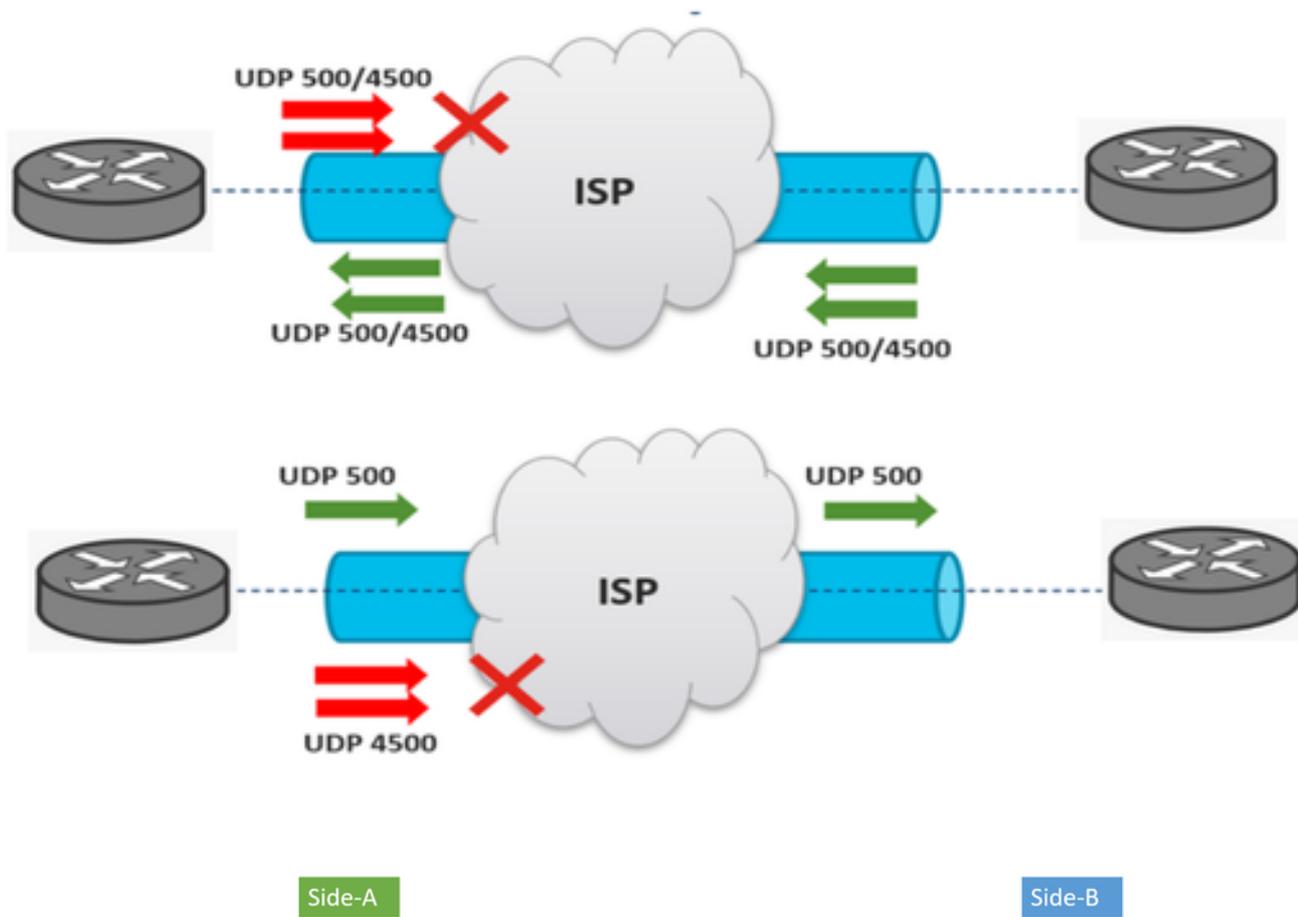
```

Values sent from site-A do not match as is configured on site-B

Erneute Übertragungen

Eine IPSec-Tunnelaushandlung kann fehlschlagen, weil die Aushandlungspakete entlang des Pfads zwischen den Endgeräten verworfen werden. Bei den verworfenen Paketen kann es sich um Phase-1- oder Phase-2-Pakete handeln. Wenn dies der Fall ist, sendet das Gerät, das ein Antwortpaket erwartet, das letzte Paket erneut. Wenn es nach 5 Versuchen keine Antwort gibt, wird der Tunnel beendet und von Anfang an neu gestartet.

Durch die Erfassung auf beiden Seiten des Tunnels kann ermittelt werden, was den Verkehr möglicherweise blockieren könnte und in welche Richtung er betroffen ist.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
2	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
3	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Responder Response
4	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
5	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
6	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
7	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
8	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
9	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Responder Response

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
2	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
3	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
4	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request

A device or service in between is blocking UDP packets that come from side-A

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.