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

Inhalt

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

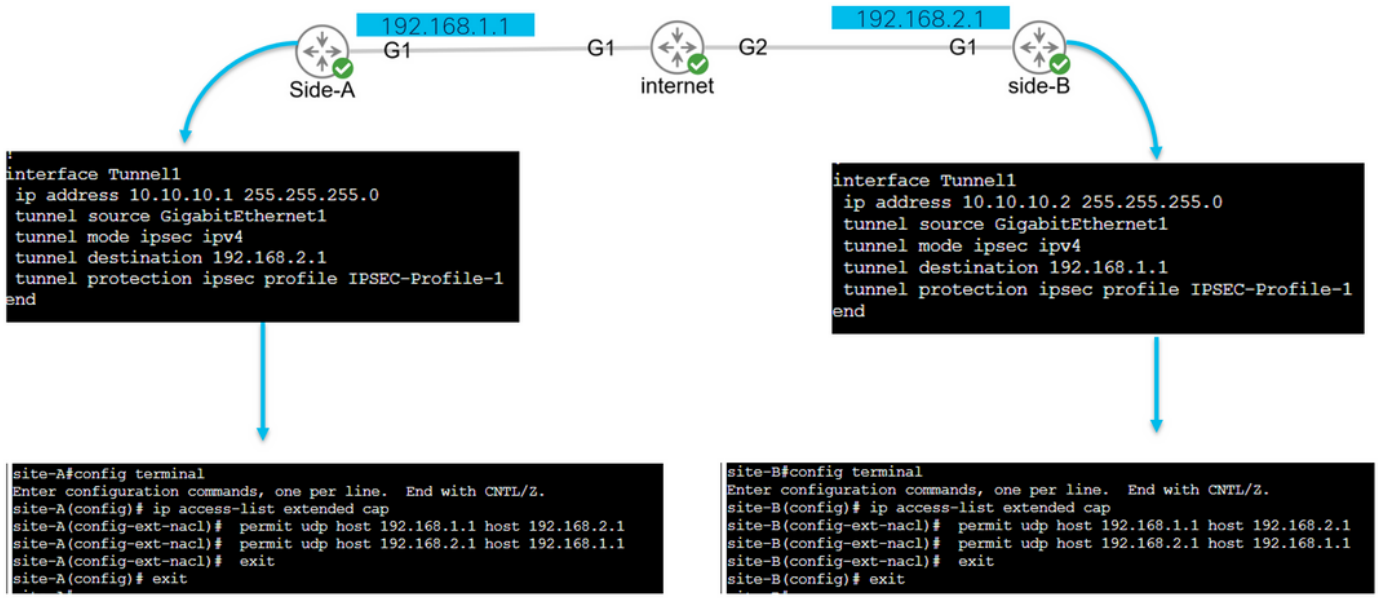
Es gibt nützliche Tools, die Ihnen helfen, die Aufnahmen zu konfigurieren, die Ausgabe zu extrahieren und weiter zu analysieren. Einige davon sind:

- 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

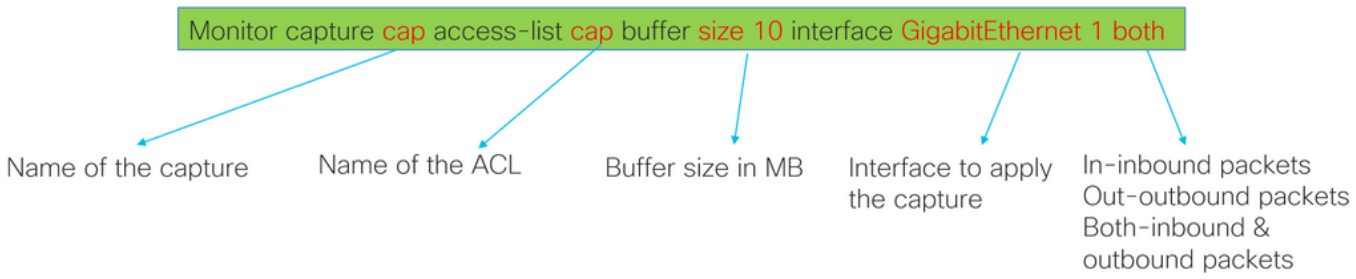
Bei der Erfassung wird eine erweiterte Zugriffsliste (ACL) verwendet, die den zu erfassenden Datenverkehrstyp sowie die Quell- und Zieladressen der VPN-Peers oder Segmente des interessanten Datenverkehrs definiert. Bei einer Tunnelaushandlung werden der UDP-Port 500 und der Port 4500 verwendet, wenn 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.

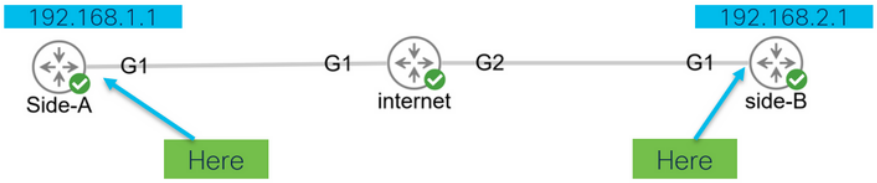
Um Probleme im Zusammenhang mit der Kontrollebene zu beheben, müssen die IP-Adressen der VPN-Peers zur Erfassung der Tunnelverhandlung verwendet werden.




```
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
```

```
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#
```

```
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-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/Stopp 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 Tunneleinrichtung 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.

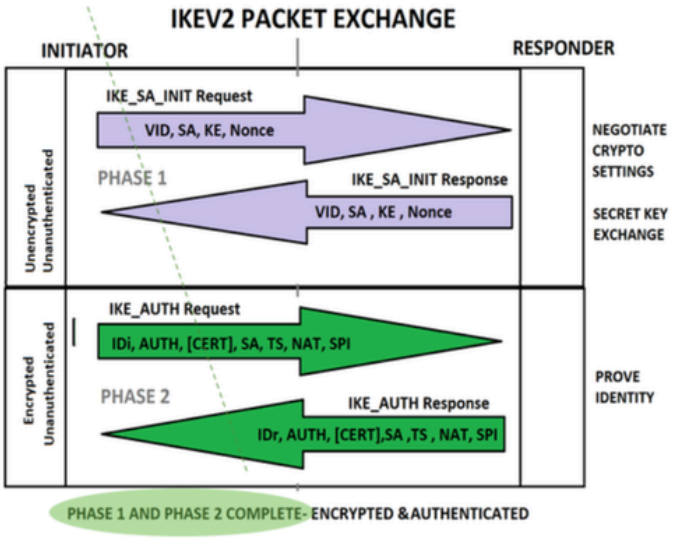
UDP 500/4500 packets seen.

Initiator and responder roles.

SPI values created.

Phase 1 in clear text.

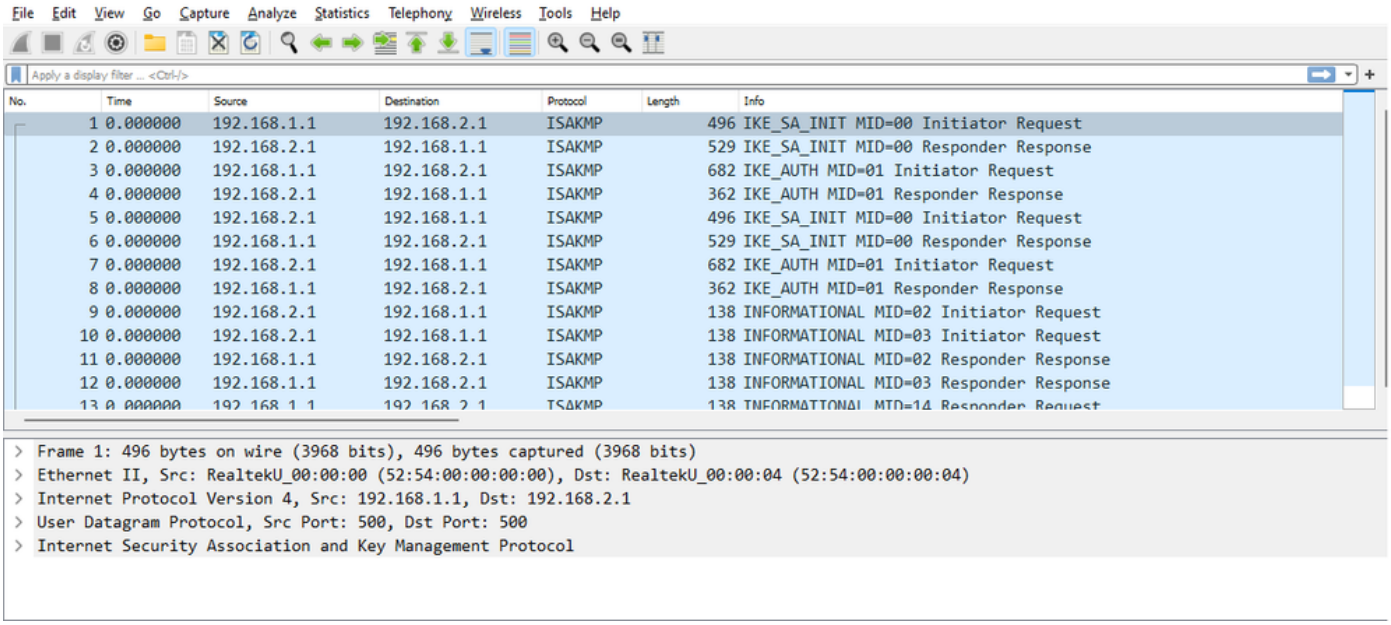
Phase 2 encrypted



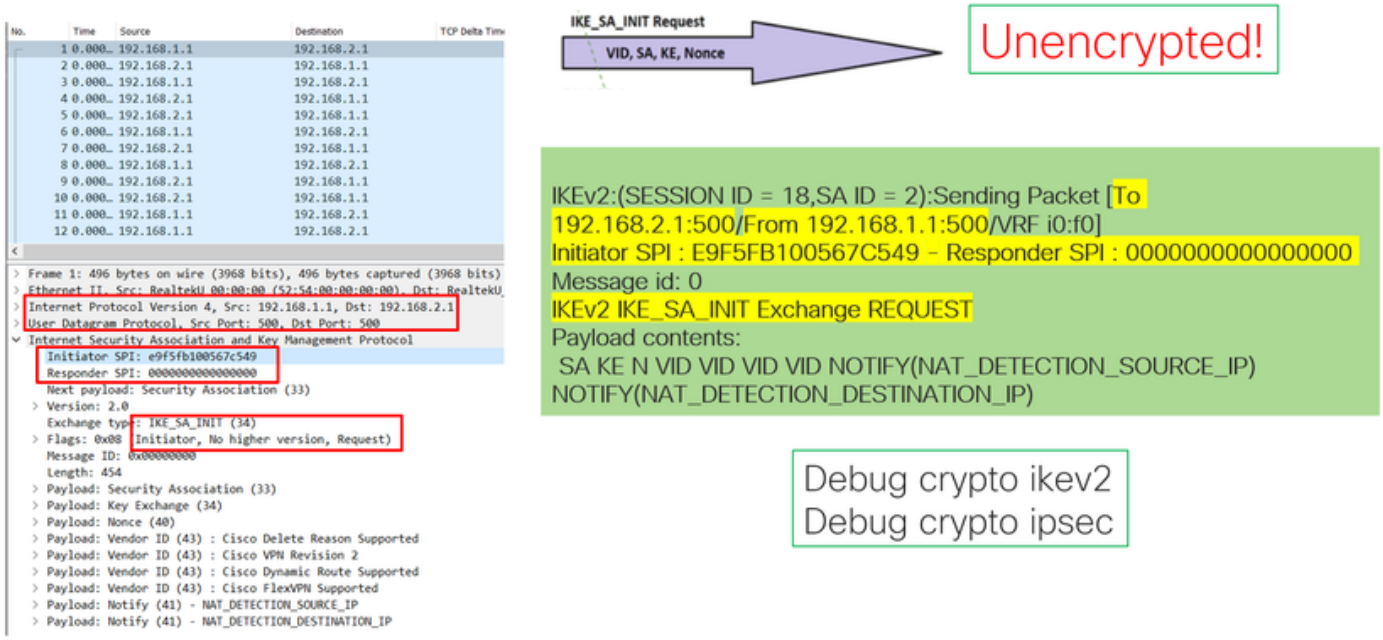
Die kurze Ausgabe der Erfassung durch den Router zeigt die Interaktion zwischen den Peers an und sendet UDP-Pakete.

```
site-A#show monitor cap cap buffer brief
 ------------------------------------------------------------------------------
 #   size   timestamp     source               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.

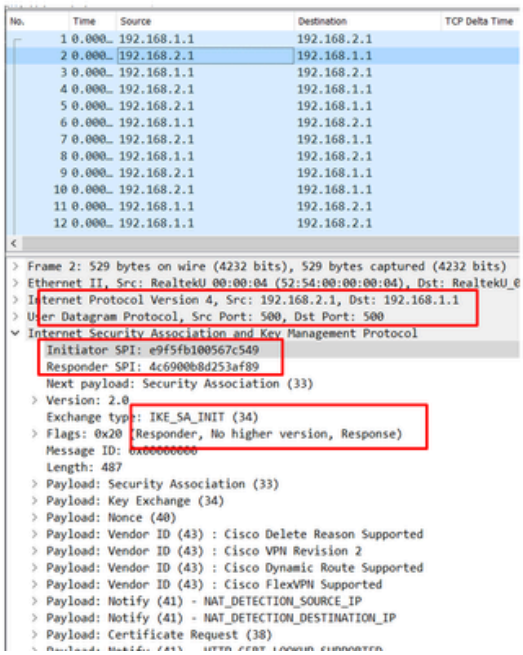


Im Internet Protocol-Abschnitt des ersten gesendeten IKE_SA_INIT Exchange-Pakets befinden sich die Quell- und Zieladressen des UDP-Pakets. Im Bereich User Datagram Protocol werden die verwendeten Ports und im Bereich Internet Security Association and Key Management Protocol die Version des Protokolls,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



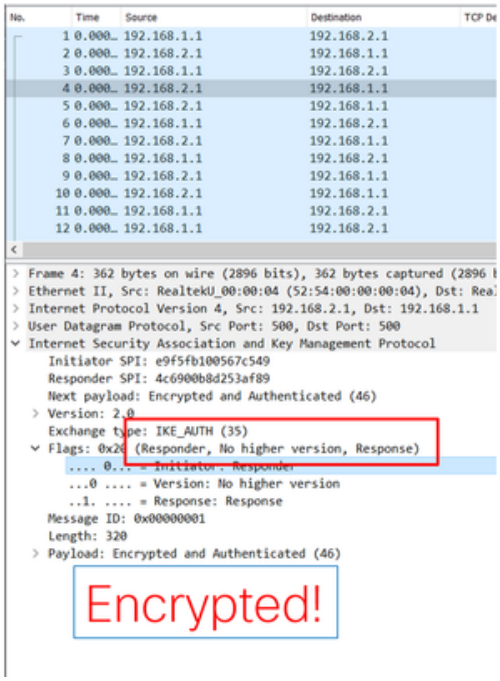
IKEv2:(SESSION ID = 18,SA ID = 2):Received Packet [From 192.168.2.1:500/To 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE
Payload contents:
SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP)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

Unencrypted!



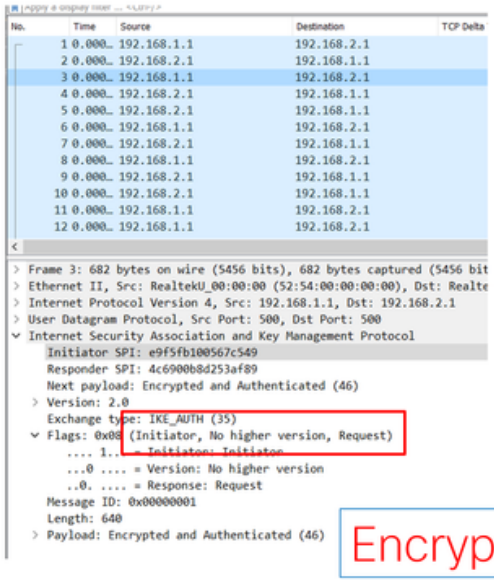
Wenn die IKE_AUTH-Exchange-Aushandlung stattfindet, wird die Nutzlast verschlüsselt, es werden jedoch einige Informationen über die Aushandlung angezeigt, z. B. der zuvor erstellte SPI und die Art der ausgeführten Transaktion.

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



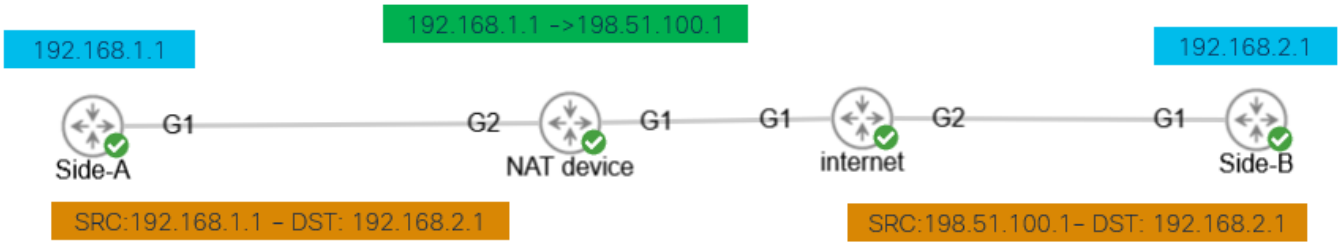
Encrypted!

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



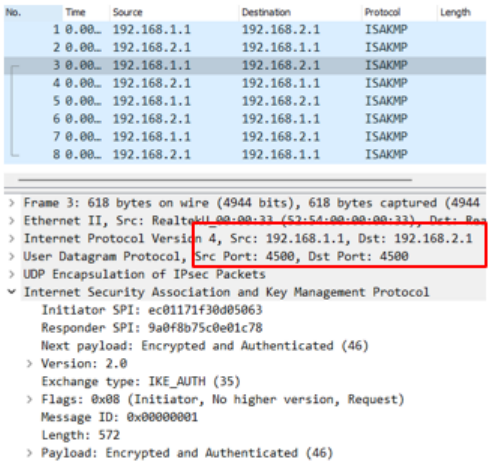
IKEv2:(SESSION ID = 18,SA ID = 2):Sending Packet [To 192.168.2.1:500/From 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:
ENCR

Transaktion, wenn NAT dazwischen liegt



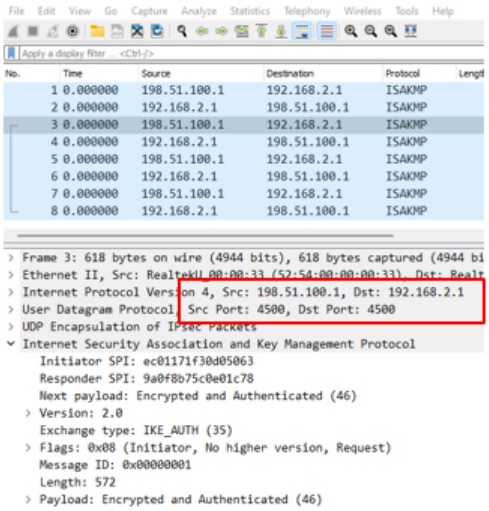
Eine weitere Funktion, die erkennbar ist, wenn die Tunnelaushandlung stattfindet, ist die Nat-Transversal-Funktion. Wenn ein zwischengeschaltetes Gerät eine oder beide für den Tunnel verwendete Adressen nutzt, ändern die Geräte den UDP-Port von 500 auf 4500, wenn Phase 2 (IKE_AUTH-Austausch) ausgehandelt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

Aufnahme von Seite A:



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:




```
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:
```

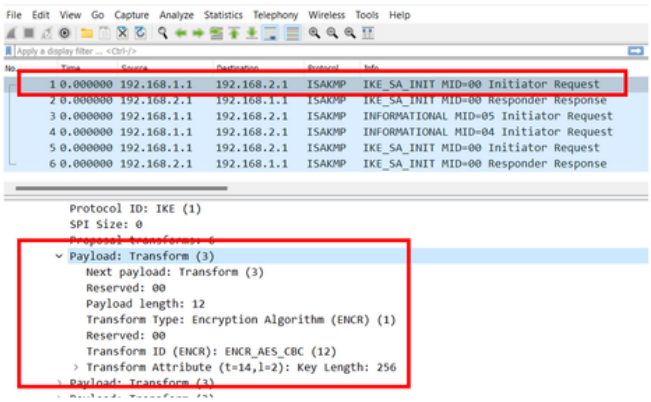
Häufige Probleme auf der Kontrollebene

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

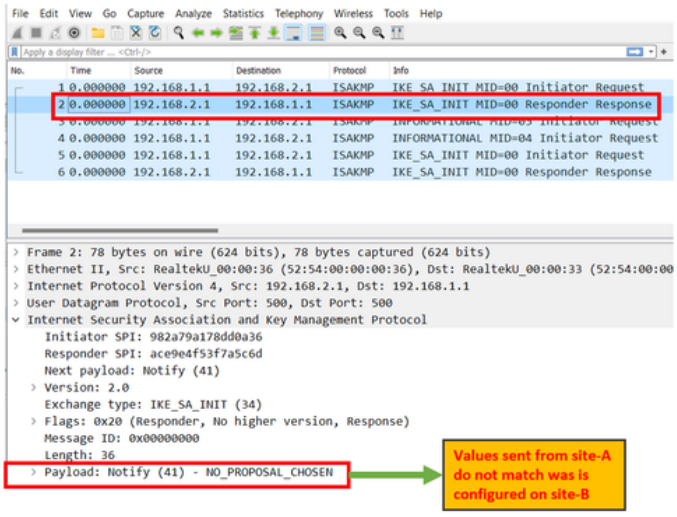
Konfigurationskonflikt

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



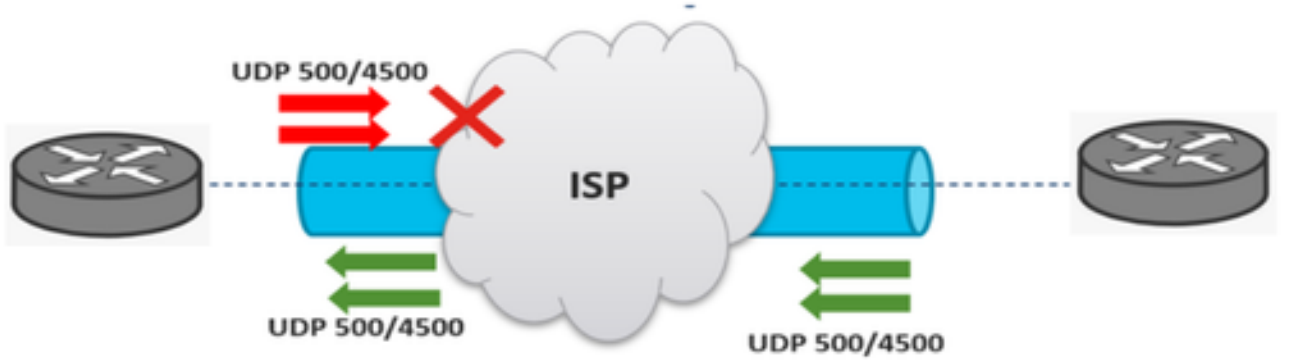
Side-B

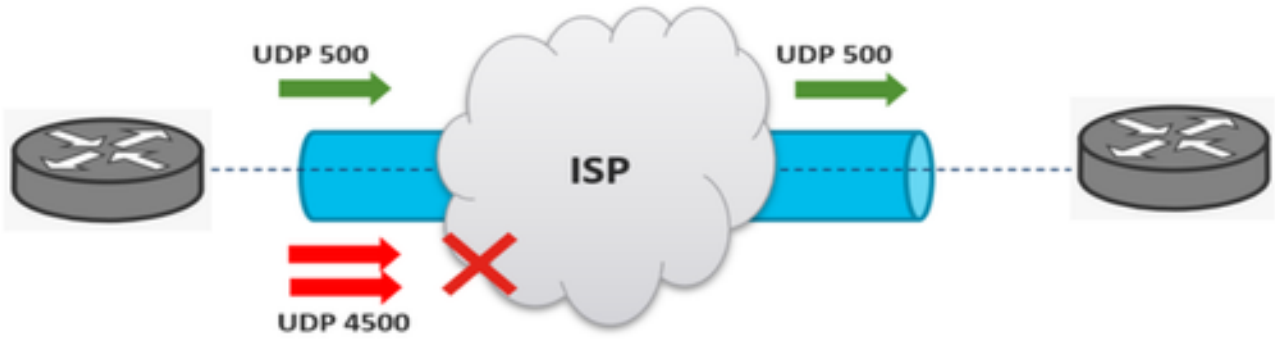


Erneute Übertragungen

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.

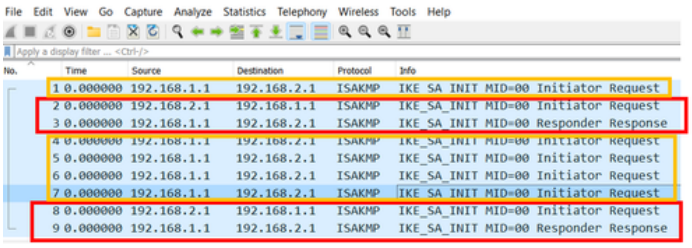
Durch die Erfassung auf beiden Seiten des Tunnels kann ermittelt werden, was den Verkehr möglicherweise blockieren könnte und in welche Richtung er betroffen ist.

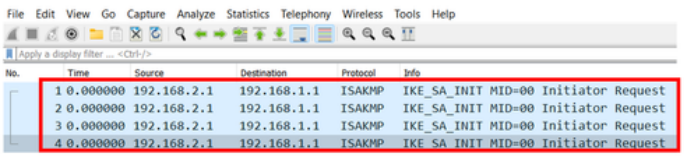




Side-A

Side-B





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.