Risoluzione dei problemi relativi ai tunnel IPsec e ai Control-Plane comuni con le acquisizioni dei pacchetti

Sommario

Introduzione

Questo documento descrive come acquisire pacchetti, altri strumenti, aiutano con problemi del control plane quando viene negoziata la VPN da sito a sito sui router Cisco IOS® XE.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base della configurazione della CLI di Cisco IOS®.
- Conoscenze base di IKEv2 e IPsec.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- CSR1000V - Software Cisco IOS XE con versione 16.12.0.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Premesse

Le acquisizioni dei pacchetti sono uno strumento potente per verificare se i pacchetti vengono inviati/ricevuti tra dispositivi peer VPN. Confermano inoltre se il comportamento rilevato con i debug IPsec è allineato all'output raccolto sulle acquisizioni poiché i debug sono un'interpretazione logica e l'acquisizione rappresenta l'interazione fisica tra peer. Per questo motivo, è possibile confermare o eliminare i problemi di connettività.

Strumenti utili

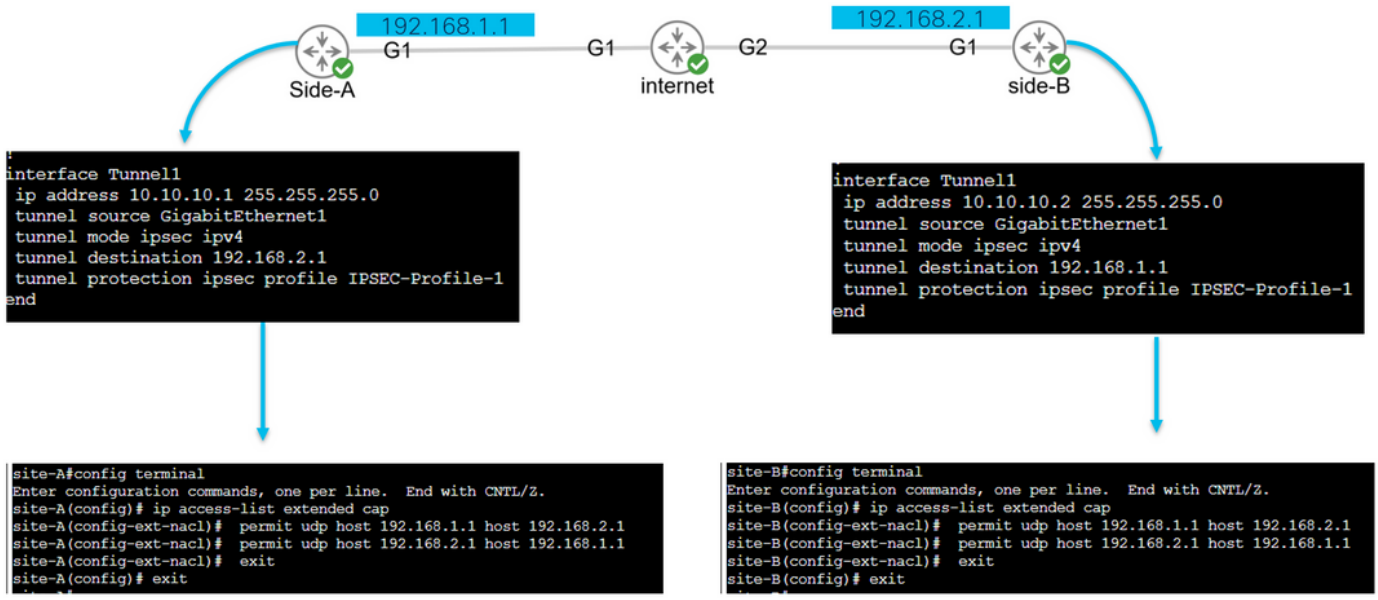
Sono disponibili strumenti utili che consentono di configurare le acquisizioni, estrarre l'output e analizzarlo ulteriormente. Alcuni di essi sono:

- Wireshark: questo è un analizzatore di pacchetti open-source conosciuto e usato.
- Acquisizioni monitor: funzionalità Cisco IOS XE sui router che consente di raccogliere le acquisizioni e di fornire un output leggero dell'aspetto del flusso di traffico, del protocollo raccolto e dei relativi timestamp.

Come configurare le acquisizioni sul router IOS XE

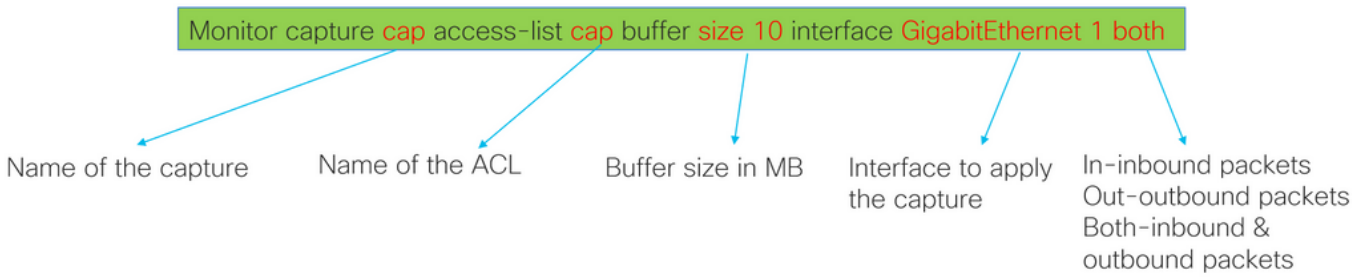
Un'acquisizione utilizza un elenco degli accessi esteso (ACL) che definisce il tipo di traffico da raccogliere, nonché gli indirizzi di origine e di destinazione dei peer VPN o dei segmenti del traffico interessato. Una negoziazione del tunnel utilizza la porta UDP 500 e la porta 4500 se NAT-T è abilitato lungo il percorso. Una volta completata la negoziazione e stabilito il tunnel, il traffico interessato utilizza il protocollo IP 50 (ESP) o UDP 4500 se NAT-T è abilitato.

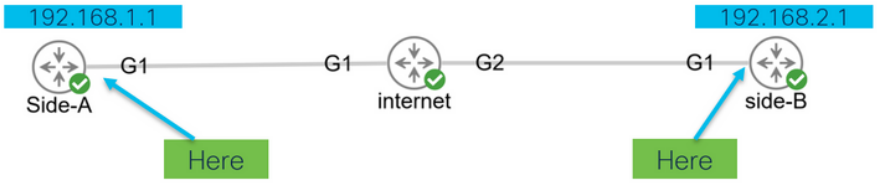
Per risolvere i problemi relativi al control plane, è necessario utilizzare gli indirizzi IP dei peer VPN per acquisire le modalità di negoziazione del tunnel.




```
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
```

L'ACL configurato viene usato per limitare il traffico acquisito e viene posizionato sull'interfaccia usata per negoziare il tunnel.






```
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
```

Una volta configurata l'acquisizione, è possibile modificarla in modo da arrestarla, cancellarla o estrarre il traffico raccolto con i comandi successivi:

- Controllare le informazioni generali sull'acquisizione: show monitor capture
- Avvia/arresta la cattura: avvio/arresto del cappuccio di cattura del monitor
- Verificare che l'acquisizione stia raccogliendo pacchetti: show monitor capture cap buffer
- Visualizza un breve output del traffico: show monitor capture cap buffer brief
- Cancella l'acquisizione: cancella il coperchio di acquisizione del monitor
- Estrarre l'output di acquisizione:
  - dump buff cap monitor
  - monitor capture cap export bootflash:capture.pcap

Analisi della definizione del tunnel con le acquisizioni dei pacchetti

Come accennato in precedenza, per negoziare il tunnel IPSec, i pacchetti vengono inviati su UDP con la porta 500 e la porta 4500 se NAT-T è abilitato. Nelle acquisizioni, è possibile ottenere più informazioni dai pacchetti, ad esempio la fase in fase di negoziazione (fase 1 o fase 2), il ruolo di ciascun dispositivo (iniziatore o risponditore) o i valori SPI appena creati.

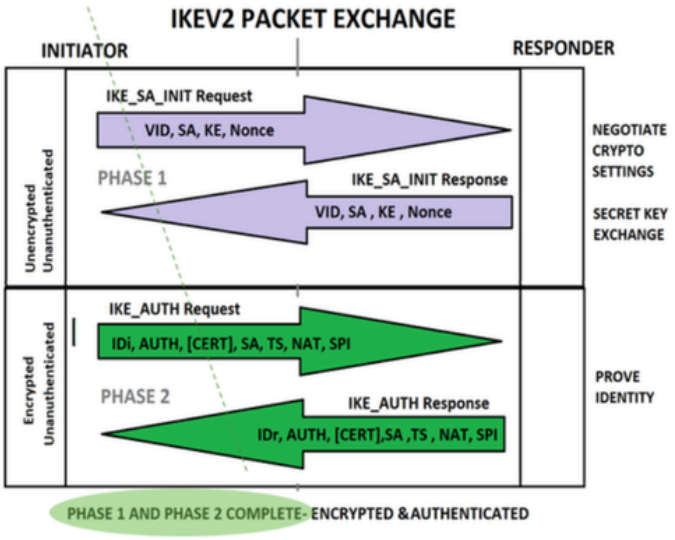
UDP 500/4500 packets seen.

Initiator and responder roles.

SPI values created.

Phase 1 in clear text.

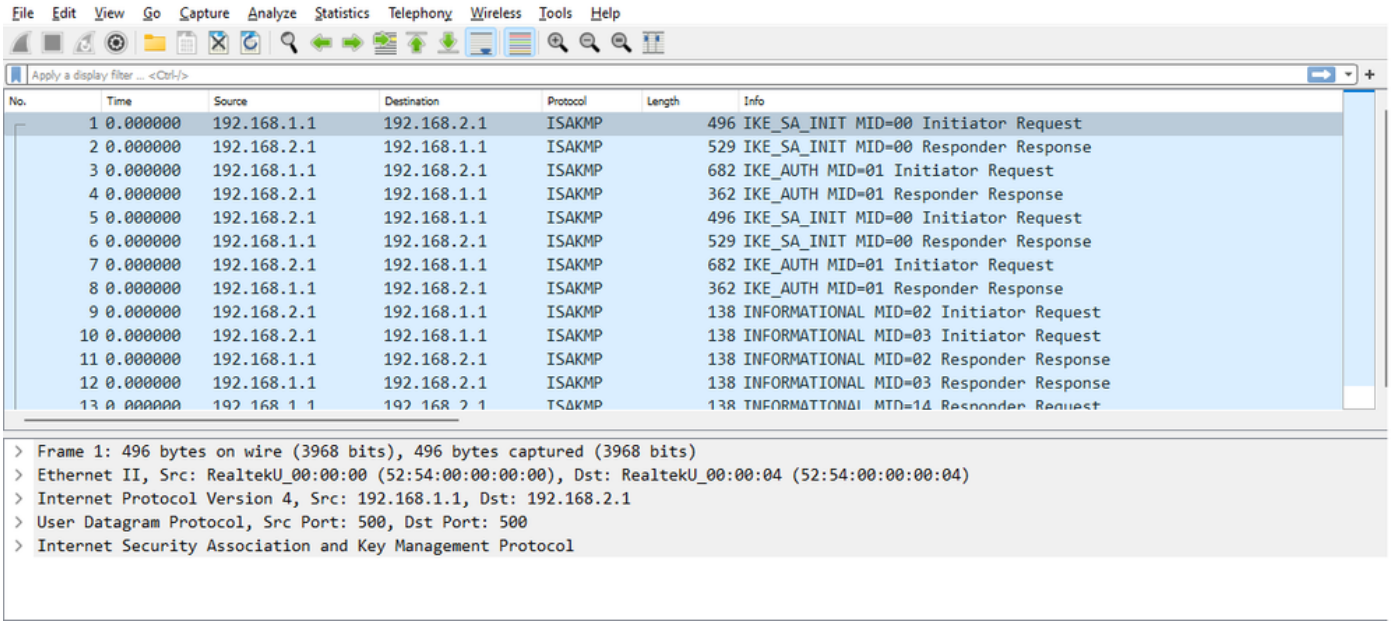
Phase 2 encrypted



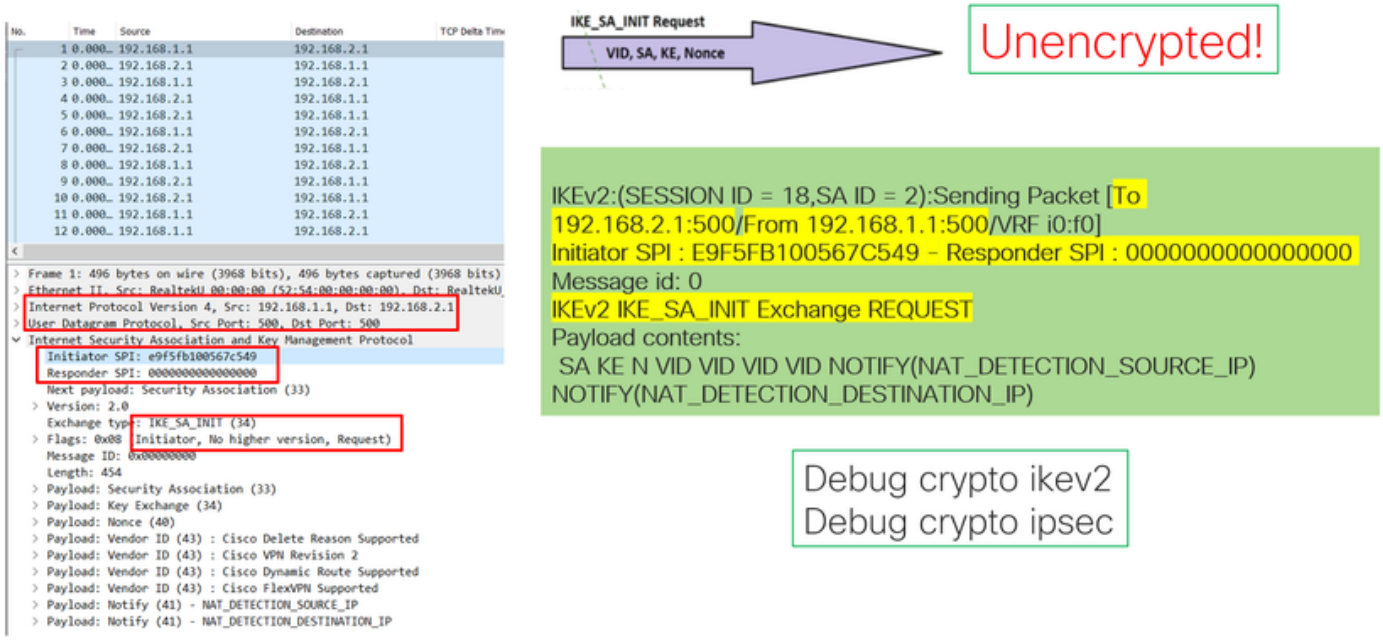
Mostrando il breve output della cattura dal router, viene rilevata l'interazione tra i peer e vengono inviati pacchetti UDP.

```
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
```

Dopo aver estratto il dump e aver esportato il file pcap dal router, è possibile visualizzare ulteriori informazioni dai pacchetti utilizzando wireshark.

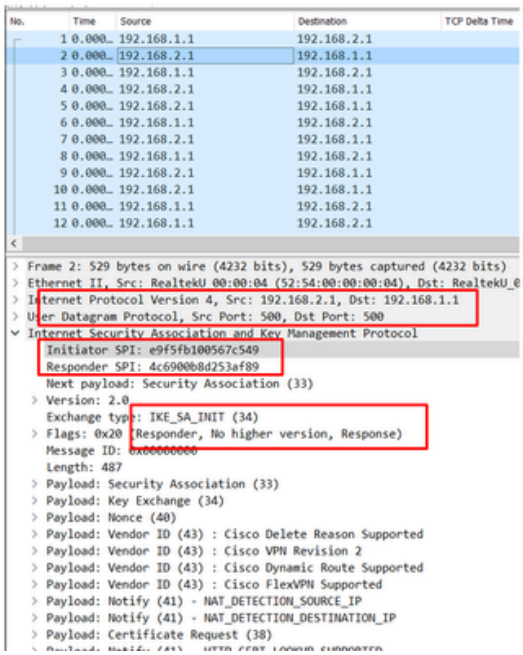


Nella sezione Internet Protocol del primo pacchetto di scambio IKE_SA_INIT inviato, vengono individuati gli indirizzi di origine e di destinazione del pacchetto UDP. Nella sezione User Datagram Protocol sono visualizzate le porte utilizzate e la sezione Internet Security Association and Key Management Protocol la versione del protocollo, il tipo di messaggio scambiato e il ruolo del dispositivo, nonché l'indice SPI creato. Quando si raccolgono i debug IKEv2, le stesse informazioni vengono presentate nei log di debug.



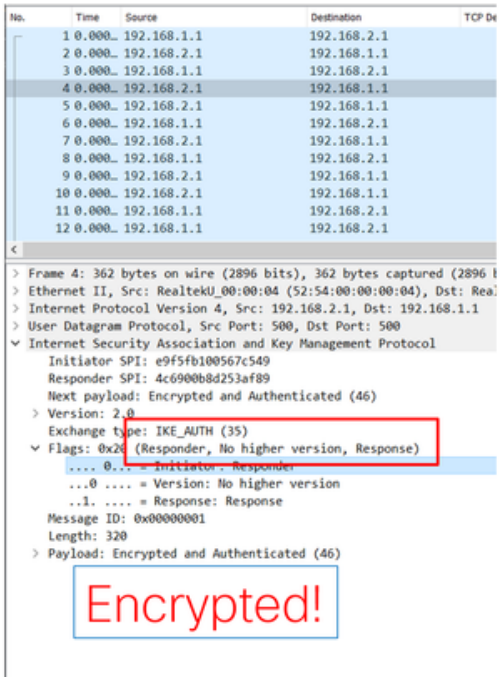
IKEv2:(SESSION ID = 18,SA ID = 2):Received Packet [From 192.168.2.1:500/To 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE
Payload contents:
SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP)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

Unencrypted!



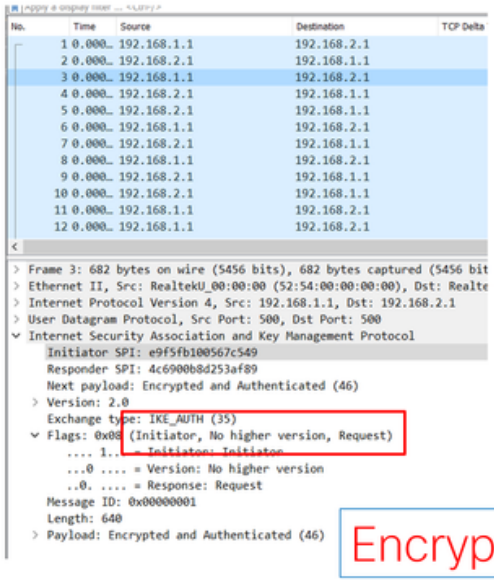
Quando viene eseguita la negoziazione di Exchange IKE_AUTH, il payload è crittografato ma alcune informazioni sulla negoziazione sono visibili, ad esempio l'indice SPI creato in precedenza e il tipo di transazione da eseguire.

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



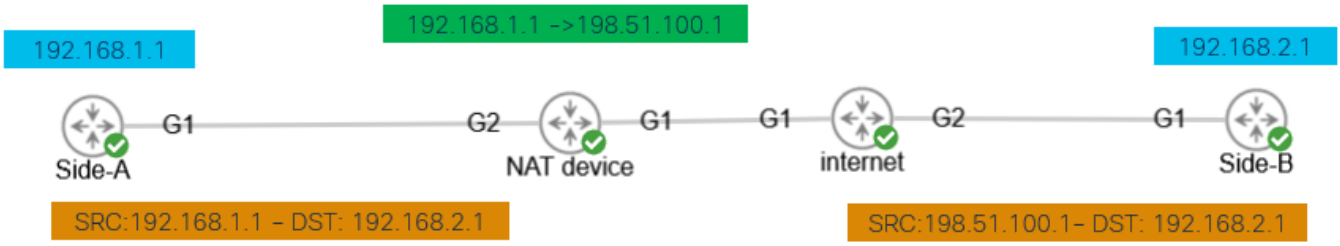
Encrypted!

Dopo aver ricevuto l'ultimo pacchetto di scambio IKE_AUTH, la negoziazione del tunnel è completata.



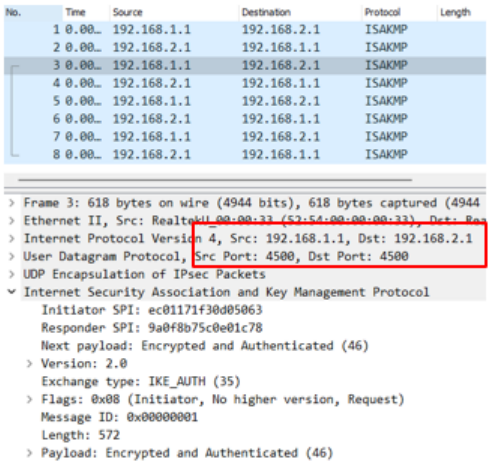
IKEv2:(SESSION ID = 18,SA ID = 2):Sending Packet [To 192.168.2.1:500/From 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:
ENCR

Transazione se NAT è compreso tra



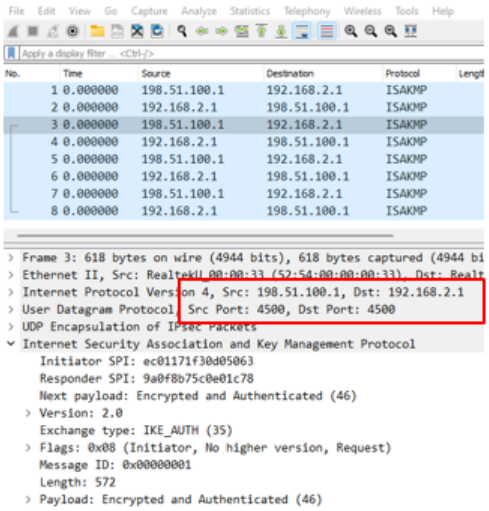
La funzionalità Nat-Transversal è un'altra funzionalità che può essere rilevata quando viene eseguita la negoziazione del tunnel. Se un dispositivo intermedio specifica uno o entrambi gli indirizzi utilizzati per il tunnel, i dispositivi modificano la porta UDP da 500 a 4500 durante la negoziazione della fase 2 (IKE_AUTH Exchange).

Acquisizione sul lato 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

Acquisizione sul lato 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:
```

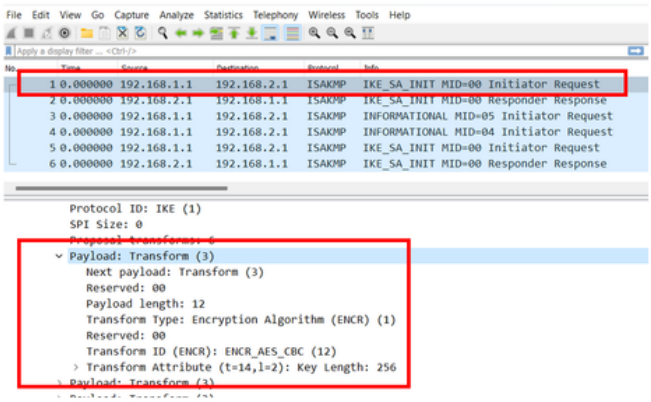
Problemi comuni relativi al Control Plane

La negoziazione del tunnel potrebbe essere influenzata da fattori locali o esterni che possono essere identificati anche con le acquisizioni. Gli scenari successivi sono i più comuni.

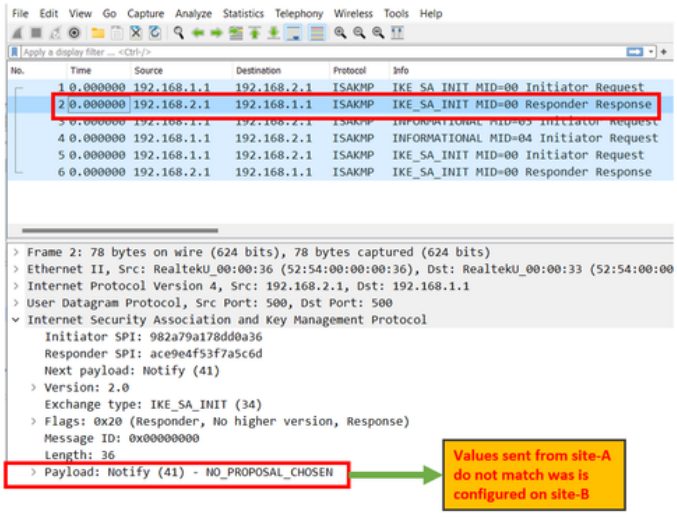
Configurazione non corrispondente

Questo scenario può essere risolto esaminando la configurazione di ogni dispositivo di fase 1 e 2. Tuttavia, potrebbero verificarsi scenari in cui non è possibile accedere all'estremità remota. Cattura l'aiuto identificando quale dispositivo invia un NO_PROPOS_CHOSEN all'interno dei pacchetti nella fase 1 o 2. Questa risposta indica che la configurazione può presentare dei problemi e quale fase deve essere modificata.

Side-A



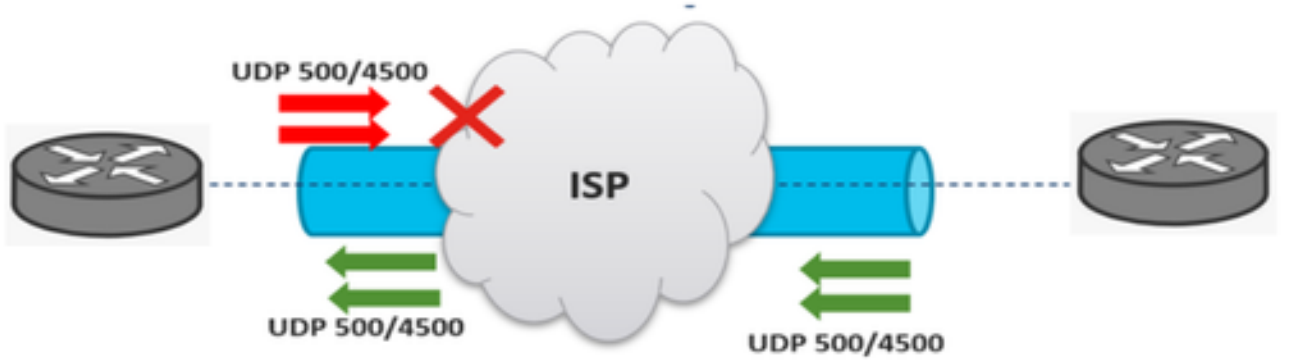
Side-B

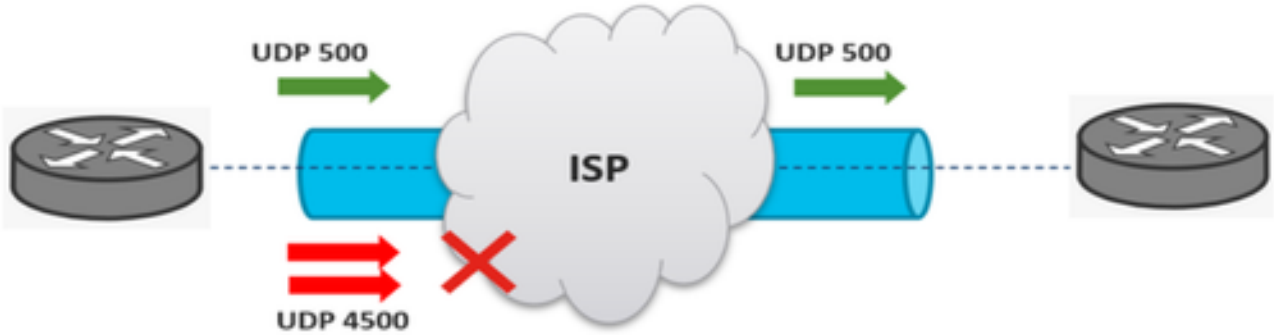


Ritrasmissioni

La negoziazione di un tunnel IPSec può avere esito negativo perché i pacchetti di negoziazione vengono scartati lungo il percorso tra i dispositivi terminali. I pacchetti scartati possono essere pacchetti di fase 1 o 2. In questo caso, il dispositivo che prevede un pacchetto di risposta trasmette nuovamente l'ultimo pacchetto e, se non c'è risposta dopo 5 tentativi, il tunnel viene concluso e riavviato dall'inizio.

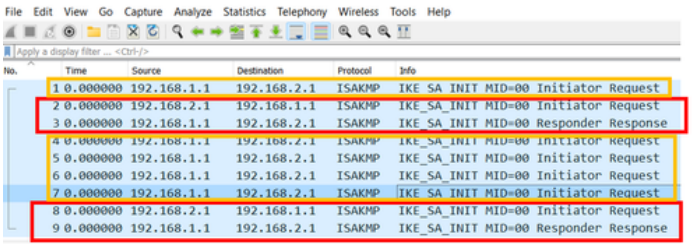
Le clip su entrambi i lati del tunnel aiutano a identificare cosa potrebbe bloccare il traffico e in quale direzione questo viene influenzato.

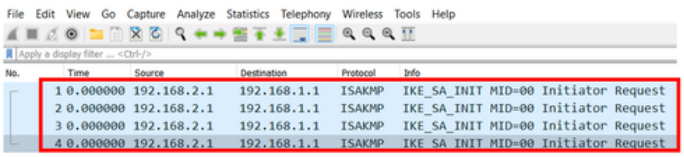




Side-A

Side-B





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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).