Fehlerbehebung bei SD-WAN cEdge IPsec Anti Replay-Fehlern

Inhalt

Einleitung

In diesem Dokument wird das IPsec-Anti-Replay-Verhalten in SD-WAN IPsec für Edge-Router und die Fehlerbehebung bei Anti-Replay-Problemen beschrieben.

Voraussetzungen

Anforderungen

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

- Cisco Software-defined Wide Area Network (SD-WAN)
- Internetprotokollsicherheit (IPsec)

Verwendete Komponenten

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

- C8000V Version17.06.01
- ASR1001-X Version 17.06.03a
- vManage Version 20.7.1

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 verstehen.

Hintergrundinformationen

Die IPsec-Authentifizierung bietet integrierten Anti-Replay-Schutz gegen alte oder duplizierte IPsec-Pakete, wobei die Sequenznummer im ESP-Header auf dem Empfänger überprüft wird. Das Verwerfen von Anti-Replay-Paketen ist eines der häufigsten Probleme mit IPsec auf Datenebene, da Pakete außerhalb des Anti-Replay-Fensters in ungeordneter Reihenfolge zugestellt wurden. Eine allgemeine Vorgehensweise zur Fehlerbehebung bei IPsec-Anti-Replay-Drops finden Sie in IPsec-Anti-Replay-Check-Failures, und die allgemeine Technik gilt auch für SD-WAN. Zwischen den in der Cisco SD-WAN-Lösung verwendeten herkömmlichen IPsec und IPsec bestehen jedoch einige Implementierungsunterschiede. In diesem Artikel werden diese Unterschiede und der Ansatz für cEdge-Plattformen mit Cisco IOS ®XE erläutert.

Überlegungen zur SD-WAN-Wiedergabeerkennung

Gruppenschlüssel und paarweiser Schlüssel

Im Gegensatz zu herkömmlichen IPsec-Verbindungen, bei denen IPsec-SAs unter Verwendung des IKE-Protokolls zwischen zwei Peers ausgehandelt werden, verwendet das SD-WAN ein Gruppenschlüsselkonzept. Bei diesem Modell generiert ein SD-WAN-Edge-Gerät periodisch eine eingehende SA der Datenebene pro TLOC und sendet diese SAs an den vSmart-Controller, der die SA wiederum an die übrigen Edge-Geräte im SD-WAN-Netzwerk weiterleitet. Eine ausführlichere Beschreibung der Vorgänge auf SD-WAN-Datenebene finden Sie unter Übersicht über die Sicherheit auf SD-WAN-Datenebene.

> **Hinweis**: Seit Cisco IOS ® XE. 6.12.1a/SD-WAN 19.2, IPsec-Schlüssel für paarweise Verbindungen werden unterstützt. Siehe Übersicht über paarweise IPsec-Schlüssel. Mit Pairwise-Schlüsseln funktioniert der IPsec-Anti-Replay-Schutz genau wie herkömmliche IPsec. Dieser Artikel konzentriert sich in erster Linie auf Replay-Check mit der Verwendung der Gruppe Schlüsselmodell.

Kodierter SPI

Im IPsec-ESP-Header ist der SPI (Security Parameter Index, Sicherheitsparameterindex) ein 32-Bit-Wert, den der Empfänger verwendet, um die SA zu identifizieren, mit der ein eingehendes Paket entschlüsselt wird. Mit SD-WAN kann dieser eingehende SPI mit **show crypto ipsec sa** identifiziert werden:

```
cedge-2#show crypto ipsec sa | se inbound
     inbound esp sas:
      spi: 0x123(291)
        transform: esp-gcm 256 ,
        in use settings ={Transport UDP-Encaps, esn}
        conn id: 2083, flow_id: CSR:83, sibling_flags FFFFFFFF80000008, crypto map: Tunnel1-
vesen-head-0
        sa timing: remaining key lifetime 9410 days, 4 hours, 6 mins
        Kilobyte Volume Rekey has been disabled
```

```
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

Hinweis: Auch wenn der eingehende SPI für alle Tunnel identisch ist, verfügt der Empfänger für jedes Peer-Edge-Gerät über eine andere SA und das entsprechende Wiedergabefenster-Objekt, die mit der SA verknüpft sind, da die SA durch die Quelle, die Ziel-IP-Adresse, die Quelle, die Ziel-Ports, 4-Tupel und die SPI-Nummer identifiziert wird. Jeder Peer hat also sein eigenes Anti-Replay-Fensterobjekt.

Beachten Sie, dass sich der SPI-Wert im vom Peer-Gerät gesendeten Paket von der vorherigen Ausgabe unterscheidet. Hier ist ein Beispiel aus der Paketverfolgungs-Ausgabe, bei der die Paketkopieoption aktiviert ist:

```
Packet Copy In
  45000102 0cc64000 ff111c5e ac127cd0 ac127cd1 3062303a 00eea51b 04000123
  00000138 78014444 f40d7445 3308bf7a e2c2d4a3 73f05304 546871af 8d4e6b9f
```

Der tatsächliche SPI im ESP-Header ist **0x04000123.** Der Grund hierfür ist, dass die ersten Bits im SPI für SD-WAN mit zusätzlichen Informationen codiert werden und nur die niedrigen Bits des SPI-Feldes dem eigentlichen SPI zugeordnet werden.

Traditionelle IPsec:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Security Parameters Index (SPI)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

SD-WAN:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  CTR  | MSNS|         Security Parameters Index (SPI)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Hierbei gilt:

- **CTR** (die ersten 4 Bit, Bit 0-3) - Control Bits, mit denen der spezifische Typ von Steuerungspaketen angegeben wird. Beispielsweise wird das Steuerbit 0x80000000 für BFD verwendet.
- **MSNS** (nächste 3 Bit, Bit 4-6) - Multiple Sequence Number Space Index (Index des Speicherplatzes für mehrere Sequenznummern) Dieser wird verwendet, um den richtigen Sequenzzähler im Sequenzzählerarray zu finden, um die Wiedergabe für das gegebene Paket zu überprüfen. Bei SD-WAN können mit dem 3-Bit-MSNS 8 verschiedene Datenverkehrsklassen einem eigenen Sequenznummernraum zugeordnet werden. Dies impliziert, dass der effektive SPI-Wert, der für die SA-Auswahl verwendet werden kann, die reduzierte niedrige Ordnung von 25 Bit vom vollen 32-Bit-Wert des Felds ist.

Platz für mehrere Sequenznummern für QoS

Häufig werden IPsec-Wiedergabefehler in einer Umgebung beobachtet, in der Pakete aufgrund von QoS (z. B. LLQ) nicht in der richtigen Reihenfolge zugestellt werden, da QoS immer nach der IPsec-Verschlüsselung und -Kapselung ausgeführt wird. Die Multiple Sequence Number Space-Lösung löst dieses Problem durch die Verwendung mehrerer Sequenznummernräume, die unterschiedlichen QoS-Verkehrsklassen für eine bestimmte Sicherheitszuordnung zugeordnet sind. Der unterschiedliche Sequenznummernraum wird durch die MSNS-Bits indiziert, die im ESP-Paket-SPI-Feld wie dargestellt codiert sind. Eine ausführlichere Beschreibung finden Sie unter IPsec Anti Replay Mechanism for QoS.

Wie bereits erwähnt, impliziert diese Implementierung mit mehreren Sequenznummern, dass der effektive SPI-Wert, der für die SA-Auswahl verwendet werden kann, die reduzierte niedrige Ordnung von 25 Bits ist. Eine weitere praktische Überlegung bei der Konfiguration der Wiedergabefenstergröße mit dieser Implementierung besteht darin, dass die konfigurierte Wiedergabefenstergröße für das aggregierte Wiedergabefenster gilt, sodass die effektive Wiedergabefenstergröße für jeden Sequenznummernraum 1/8 des aggregierten Fensters beträgt.

Konfigurationsbeispiel:

```
config-t
Security
IPsec
replay-window 1024
Commit
```

> **Hinweis**: Die effektive Größe des Wiedergabefensters für jeden Sequenznummernraum beträgt 1024/8 = 128!

> **Hinweis**: Seit dem Cisco IOS ®XE. 17.2.1 wurde die Gesamtgröße des Wiedergabefensters auf 8192 erhöht, sodass für jeden Sequenznummernraum ein maximales Wiedergabefenster von 8192/8 = 1024 Pakete festgelegt werden kann.

Auf einem cEdge-Gerät kann die letzte für jeden Sequenznummernbereich empfangene Sequenznummer aus der Ausgabe des IPsec-Datenplans **show crypto ipsec sa peer x.x.x.x** abgerufen werden:

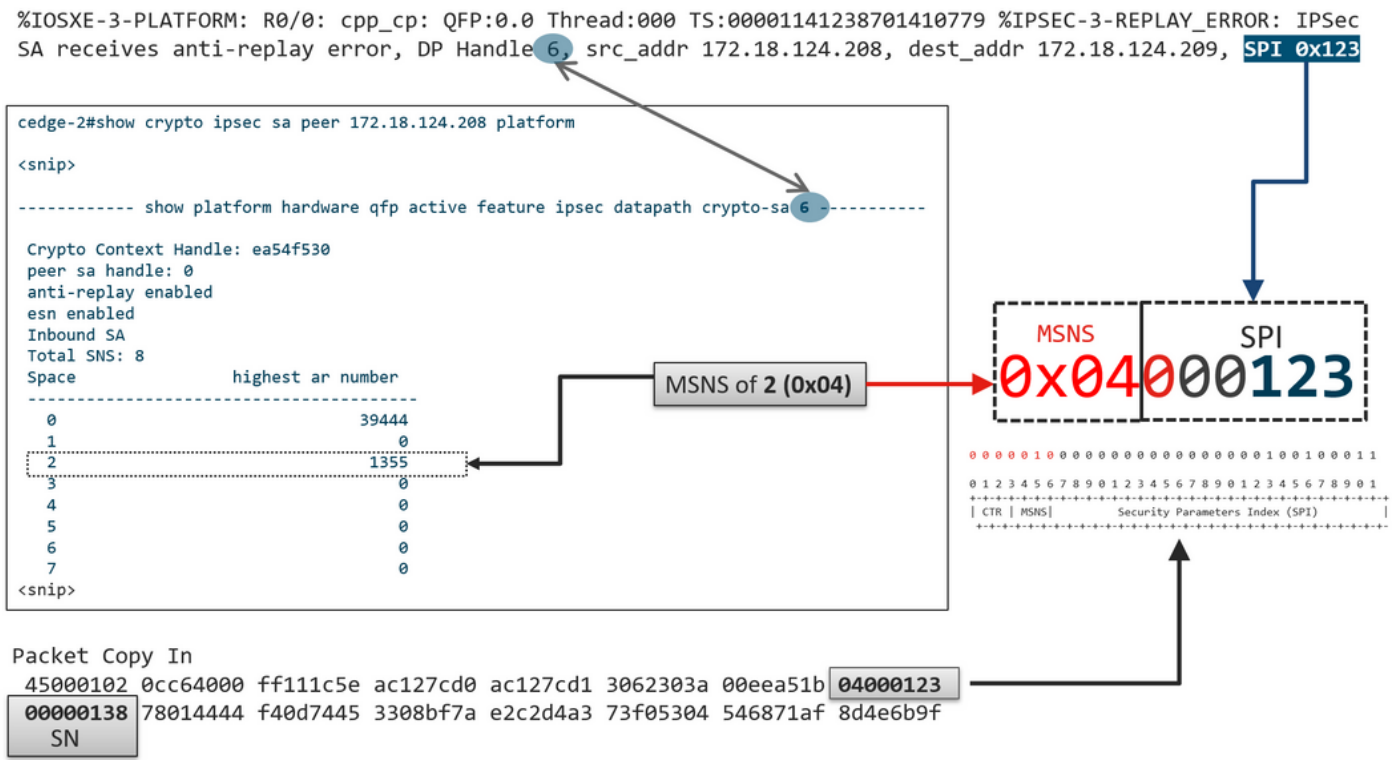
```
cedge-2#show crypto ipsec sa peer 172.18.124.208 platform

<snip>

------------------ show platform hardware qfp active feature ipsec datapath crypto-sa 5 --------
----------

 Crypto Context Handle: ea54f530
 peer sa handle: 0
 anti-replay enabled
 esn enabled
 Inbound SA
 Total SNS: 8
 Space                highest ar number
 ---------------------------------------
   0                              39444
   1                                  0
   2                               1355
   3                                  0
```

```
   4                                   0
   5                                   0
   6                                   0
   7                                   0
<snip>
```

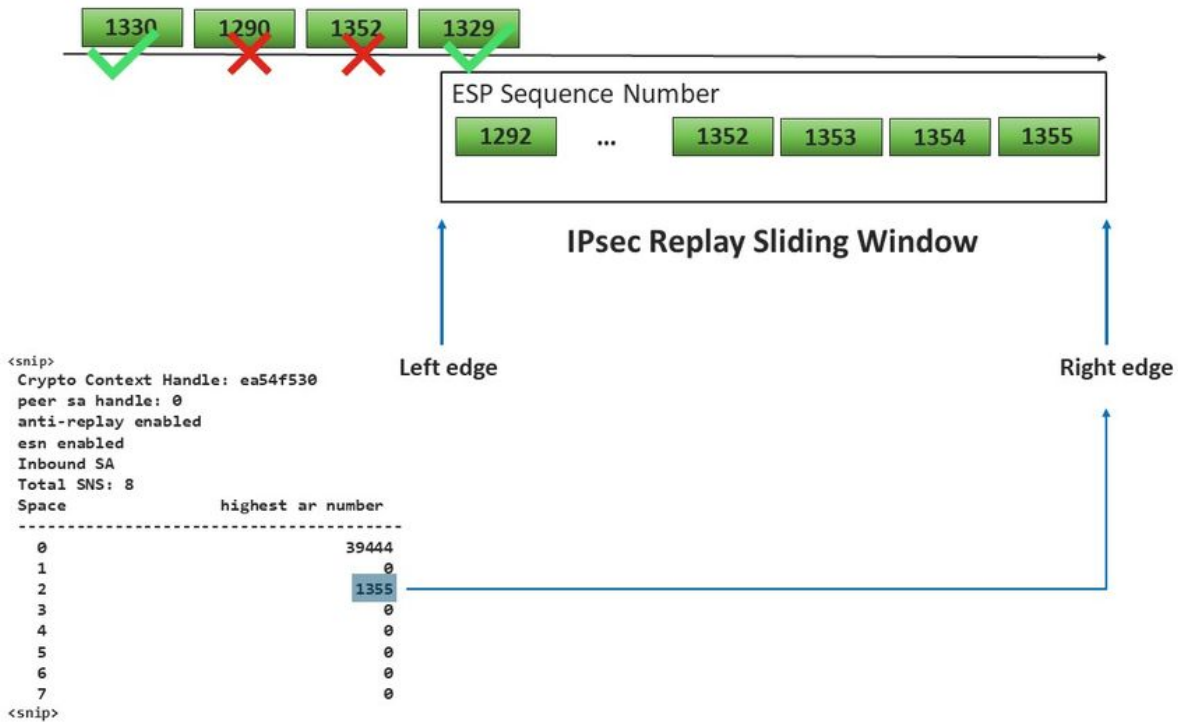
Im Beispiel ist das höchste Anti-Replay-Fenster (rechter Rand des Anti-Replay-Gleitfensters) für MSNS von 0 (**0x00**) der Wert **3944** und für MSNS von **2 (0x04)** der Wert **1335. Mit diesen Zählern wird überprüft, ob die Sequenznummer des Wiedergabefensters für Pakete im gleichen Sequenznummernbereich.**

> **Hinweis**: Es bestehen Implementierungsunterschiede zwischen der ASR1k-Plattform und den übrigen Cisco IOS ®XE Routing-Plattformen (ISR4k, ISR1k, CSR1kv). Infolgedessen gibt es einige Diskrepanzen in Bezug auf die show-Befehle und ihre Ausgabe für diese Plattformen.

Es ist möglich, die Anti-Replay-Fehler und die Ausgänge zeigen korrelieren, um den SPI und den Sequenznummernindex zu finden, wie im Bild gezeigt.



Mit den vorherigen Informationen erhalten die rechte Kante (Top-Fenster) und das Schiebefenster sieht aus, wie im Bild gezeigt.



Befehle zur Sicherstellung der Effektivität des konfigurierten Wiedergabefensters

Anders als bei regulären IPsec (nicht SD-WAN) wird der Befehl rekey für das Anti-Replay-Fenster nicht wirksam.

```
request platform software sdwan security ipsec-rekey
```

Mit diesen Befehlen wird das konfigurierte Wiedergabefenster aktiviert:

> **Warnung**: Stellen Sie sicher, dass Sie die potenziellen Auswirkungen von Befehlen kennen, die sich auf die Steuerverbindungen und die Datenebene auswirken.

```
clear sdwan control connection
```

Oder

```
request platform software sdwan port_hop <color>
```

Oder

```
Interface Tunnelx
shutdown/ no shutdown
```

Fehlerbehebung bei Wiedergabe-Löschvorgängen

Fehlerbehebung bei der Datensammlung

Damit die IPsec-Anti-Replay-Funktion nicht ausgeführt wird, ist es wichtig, die Bedingungen und potenziellen Auslöser des Problems zu kennen. Sammeln Sie mindestens die Informationen für, um den Kontext bereitzustellen:

- Geräteinformationen für Absender und Empfänger der Wiedergabepakete werden verworfen und umfassen Gerätetyp, cEdge im Vergleich zu vEdge, Softwareversion und Konfiguration.
- Problemverlauf: Wie lange ist die Bereitstellung bereits verfügbar? Wann begann das Problem? Alle aktuellen Änderungen am Netzwerk oder an den Datenverkehrsbedingungen.
- Jedes Muster auf die Wiedergabe fällt, zum Beispiel., ist es sporadisch oder konstant? Die Zeit des Problems und/oder des bedeutenden Ereignisses, zum Beispiel, passiert es nur während der hohen Verkehrsspitzen Produktionsstunden, oder nur während rekey, und so weiter?

Fahren Sie mit dem Fehlerbehebungs-Workflow fort, nachdem Sie die vorherigen Informationen gesammelt haben.

Workflow-Fehlerbehebung

Der allgemeine Ansatz zur Fehlerbehebung bei IPsec-Wiederholungsproblemen entspricht dem für herkömmliche IPsec, wobei der Pro-Peer-SA-Sequenzbereich und der Multiple Sequence Number Space wie erläutert berücksichtigt werden. Gehen Sie dann wie folgt vor:

Schritt 1: Identifizieren Sie zuerst den Peer für die Wiederholung und die Abwurfrate aus dem Syslog. Sammeln Sie für Drop-Statistiken immer mehrere Zeitstempel-Snapshots der Ausgabe, sodass die Drop-Rate quantifiziert werden kann:

```
*Feb 19 21:28:25.006: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000
TS:00001141238701410779 %IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 6,
src_addr 172.18.124.208, dest_addr 172.18.124.209, SPI 0x123

cedge-2#show platform hardware qfp active feature ipsec datapath drops
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
No time source, *11:25:53.524 EDT Wed Feb 26 2020
----------------------------------------------------------------------
Drop Type  Name                                          Packets
----------------------------------------------------------------------
        4  IN_US_V4_PKT_SA_NOT_FOUND_SPI                          30
       19  IN_CD_SW_IPSEC_ANTI_REPLAY_FAIL                        41
```

> **Hinweis**: Gelegentliche Replay-Drops aufgrund einer Neuordnung der Paketübermittlung im Netzwerk sind nicht ungewöhnlich, aber persistente Replay-Drops wirken sich auf den Service aus und können untersucht werden.

Schritt 2a: Bei relativ geringer Datenverkehrsrate sollten Sie eine Paketverfolgung durchführen, bei der die Bedingung auf die Peer-IPv4-Adresse mit der Option **"Copy Packet"** gesetzt wurde, und die Sequenznummern für das verworfene Paket mit der rechten Kante des aktuellen Wiedergabefensters und den Sequenznummern in den benachbarten Paketen vergleichen, um zu überprüfen, ob es sich tatsächlich um doppelte Pakete oder Pakete außerhalb des Wiedergabefensters handelt.

Schritt 2b. Für hohe Datenverkehrsraten ohne vorhersehbaren Trigger müssen Sie eine EPC-Erfassung mit zirkulärem Puffer und EEM konfigurieren, um die Erfassung zu stoppen, wenn Wiedergabefehler erkannt werden. Da EEM ab Version 19.3 von vManage derzeit nicht unterstützt wird, impliziert dies, dass sich cEdge bei der Durchführung dieser Fehlerbehebungsaufgabe im CLI-Modus befinden muss.

Schritt 3: Sammeln Sie die **Show crypto ipsec als Peer-x.x.x.x-Plattform** auf dem Empfänger idealerweise gleichzeitig mit der Paketerfassung oder der Paketverfolgung. Dieser Befehl enthält die Echtzeitinformationen zum Replay-Fenster des Datenflugs für die eingehende und ausgehende SA.

Schritt 4: Wenn das verworfene Paket tatsächlich nicht in der richtigen Reihenfolge ist, nehmen Sie gleichzeitig Aufnahmen vom Absender und vom Empfänger vor, um festzustellen, ob das Problem bei der Quelle oder der zugrunde liegenden Netzwerkzustellungsschicht liegt.

Schritt 5: Wenn die Pakete verworfen werden, obwohl sie weder doppelt vorhanden sind noch sich außerhalb des Wiedergabefensters befinden, ist dies in der Regel ein Hinweis auf ein Softwareproblem auf dem Empfänger.

Beispiel zur Fehlerbehebung für ASR1001-x

Problembeschreibung:

HW: ASR 1001-X
SW: 17.6.03a

Mehrere Anti-Replay-Fehler werden für den Session-Peer 10.62.33.91 empfangen. Daher flattert die BFD-Sitzung ständig, und der Datenverkehr zwischen diesen beiden Standorten ist betroffen.

```
Jul 26 20:31:20.879: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:027 TS:00000093139972173042
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 22, src_addr 10.62.33.91,
dest_addr 10.62.63.251, SPI 0x106
Jul 26 20:32:23.567: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:009 TS:00000093202660128696
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 22, src_addr 10.62.33.91,
dest_addr 10.62.63.251, SPI 0x106
Jul 26 20:33:33.939: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:051 TS:00000093273031417384
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 22, src_addr 10.62.33.91,
dest_addr 10.62.63.251, SPI 0x106
Jul 26 20:34:34.407: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:020 TS:00000093333499638628
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 22, src_addr 10.62.33.91,
dest_addr 10.62.63.251, SPI 0x106
```

Schritt 1: Check Configured Anti Replay-Fenster ist 8192.

```
cEdge#sh sdwan security-info
security-info authentication-type deprecated
security-info rekey 86400
 security-info replay-window 8192
security-info encryption-supported "AES_GCM_256 (and AES_256_CBC for multicast)"
security-info fips-mode Disabled
security-info pairwise-keying Disabled
security-info pwk-sym-rekey Enabled
```

```
security-info extended-ar-window Disabled
security-info integrity-type "ip-udp-esp esp"
```

> **Hinweis**: Die effektive Größe des Wiedergabefensters für jeden Sequenznummernraum muss in diesem Beispiel 8192/8= 1024 sein.

Schritt 2: Überprüfen Sie die effektive Größe des Wiedergabefensters für Peer 10.62.33.91, um den konfigurierten Wert zu vergleichen und zu bestätigen.

```
show crypto ipsec sa peer 10.62.33.91 platform
<snip>
------------------ show platform hardware qfp active feature ipsec sa 22 ------------------
<snip>
------------------ show platform software ipsec fp active encryption-processor 0 context
c441ff4c ------------------
<snip>
       window size: 64                  <-- Effective Window Size
window base(ESN): 0
Multi-SNS window_top
---------------------------------
index: 0, win_top: 0x00000000010dc0
index: 1, win_top: 0000000000000000
index: 2, win_top: 0x00000000b65f00
index: 3, win_top: 0000000000000000
index: 4, win_top: 0000000000000000
index: 5, win_top: 0000000000000000
index: 6, win_top: 0000000000000000
index: 7, win_top: 0000000000000000
traffic hard limit: 12876354284605669376
byte count: 0
packet count: 11378618
```

Die Fehlermeldung **Fenstergröße: 64** in der Ausgabe nicht mit dem konfigurierten Wiedergabefenster übereinstimmt **8192 (8192/08 = 1024)**, was bedeutet, dass der Befehl selbst dann nicht wirksam wurde, wenn er konfiguriert wurde.

> **Hinweis**: Das effektive Wiedergabefenster wird nur auf den ASR-Plattformen angezeigt. Um sicherzustellen, dass die tatsächliche Größe des Anti-Replay-Fensters mit der konfigurierten Größe übereinstimmt, wenden Sie einen der Befehle im Abschnitt an, um die Effektivität des konfigurierten Replay-Fensters zu ermitteln.

Schritt 3: gleichzeitige Konfiguration und Aktivierung der Paketablaufverfolgung und Überwachungserfassung (optional) für eingehenden Datenverkehr von der Sitzungsquelle: 10.62.33.91, Ziel: 10.62.63.251

```
cEdge#debug platform packet-trace packet 2048 circular fia-trace data-size 2048
cEdge#debug platform packet-trace copy packet both size 2048 L3
cEdge#debug platform condition ipv4 10.62.33.91/32 in
cEdge#debug plat cond start
```

Schritt 4: Zusammenfassung der Paketverfolgung erfassen:

```
cEdge#show platform packet summay
```

Schritt 5: Erweitern Sie einige gelöschte (IpsecInput) Pakete, die erfasst wurden.

(IPSecInput) Paketverluste:

```
cEdge#sh platform pack pack 816
Packet: 816 CBUG ID: 973582
Summary
Input : TenGigabitEthernet0/0/0.972
Output : TenGigabitEthernet0/0/0.972
State : DROP 56 (IpsecInput)
Timestamp
Start : 97495234494754 ns (07/26/2022 21:43:56.25110 UTC)
Stop : 97495234610186 ns (07/26/2022 21:43:56.25225 UTC)
Path Trace
Feature: IPV4(Input)
Input : TenGigabitEthernet0/0/0.972
Output : <unknown>
Source : 10.62.33.91
Destination : 10.62.63.251
Protocol : 17 (UDP)
SrcPort : 12367
DstPort : 12347
<snip>

Packet Copy In
45000072 ab314000 fd115c77 0a3e215b 0a3e3ffb 304f303b 005e0000 04000106
00b6dfed 00000000 d0a60d5b 6161b06e 453d0e3d 5ab694ce 5311bbb6 640ecd68
7ceb2726 80e39efd 70e5549e 57b24820 fb963be5 76d01ff8 273559b0 32382ab4
c601d886 da1b3b94 7a2826e2 ead8f308 c464
```

```
817 DROP:
------------------------------
Packet: 817
<snip>
Packet Copy In
45000072 ab314000 fd115c77 0a3e215b 0a3e3ffb 304f303b 005e0000 04000106
00b6dfec 00000000 cc72d5dd ef73fe25 2440bed6 31378b78 3c506ee5 98e3dba4
bc9e6aa0 50ea98f6 7dee25c8 c1579ce0 1212290c 650f5947 57b9bc04 97c7996c
d4dbf3e6 25b33684 a7129b67 141a5e73 8736
```

SD-WAN nutzt UDP-gekapselten ESP:

- Der UDP-Header ist 304f303b 00770000.
- Der nächste SPI (**04000106**)
- Daher ist **00b6e00d** die Sicherheitsnummer (Security Number, SN).
- Der MSNS-Index beträgt **2** (**x0400106**) aufgrund von 32-Bit-SPI (**0 0 0 0 1 0** 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 1 0 0 0 1 1).

Schritt 6: Überprüfen des MSNS-Index

```
show crypto ipsec sa peer 10.62.33.91 platform
<snip>
------------------ show platform hardware qfp active feature ipsec sa 22 ------------------
<snip>
------------------ show platform software ipsec fp active encryption-processor 0 context
c441ff4c ------------------
<snip>
       window size: 64
window base(ESN): 0
Multi-SNS window_top
----------------------------------
index: 0, win_top: 0x00000000010dc0
index: 1, win_top: 0000000000000000
  index: 2, win_top: 0x00000000b65f00
index: 3, win_top: 0000000000000000
index: 4, win_top: 0000000000000000
index: 5, win_top: 0000000000000000
index: 6, win_top: 0000000000000000
index: 7, win_top: 0000000000000000
traffic hard limit: 12876354284605669376
byte count: 0
packet count: 11378618
```

Das höchste Anti-Replay-Fenster (rechter Rand des Anti-Replay-Gleitfensters) für MSNS von 2 (0x04) ist **0b65f00.**

Schritt 7. Erweitern einiger weitergeleiteter (FWD) erfasster Pakete

Weitergeleitete Pakete:

```
Packet: 838
<snip>
Packet Copy In
4564008e ab044000 fd115c24 0a3e215b 0a3e3ffb 304f303b 007a0000 04000106
 00b6e015 00000000 088bbd6a f4e4b35f b131143f ef1f91eb 659149f7 dbe6b025
```

```
be7fbfd0 5fad1c71 014321f1 3e0d38f2 cc8d0e5f 1494e4fa 097c7723 dfc7ceef
4a14f444 abcc1777 0bb9337f cd70c1da 01fc5262 848b657c 3a834680 b07b7092
81f07310 4eacd656 ed36894a e468
```

Paket: 837

```
Packet: 837
<snip>
Packet Copy In
4564008e ab044000 fd115c24 0a3e215b 0a3e3ffb 304f303b 007a0000 04000106
00b6e014 00000000 76b2a256 8e835507 13d14430 ae16d62c c152cdfd 2657c20c
01d7ce1d b3dfa451 a2cbf6e9 32f267f9 e10e9dec 395a0f9e 38589adb aad8dfb8
a3b72c8d a96f2dce 2a1557ab 67959b6e 94bbbb0a cfc4fc9e 391888da af0e492c
80bebb0e 9d7365a4 153117a6 4089
```

Schritt 8: Sammeln Sie Informationen zu den Sequenznummern mehrerer weitergeleiteter Pakete (FWD) vor, nach und nach dem Verwerfen, und rufen Sie diese ab.

```
FWD:
839 PKT: 00b6e003 FWD
838 PKT: 00b6e001 FWD
837 PKT: 00b6e000 FWD
815 PKT: 00b6e044 FWD
814 PKT: 00b6dfe8 FWD
813 PKT: 00b6e00d FWD

DROP:
816 PKT: 00b6dfed DROP
817 PKT: 00b6dfec DROP
818 PKT: 00b6dfeb DROP
819 PKT: 00b6dfe9 DROP
820 PKT: 00b6dfea DROP
```

Schritt 9. Konvertieren Sie die SN in Dezimalzahlen, und ordnen Sie sie in einfache Berechnung um:

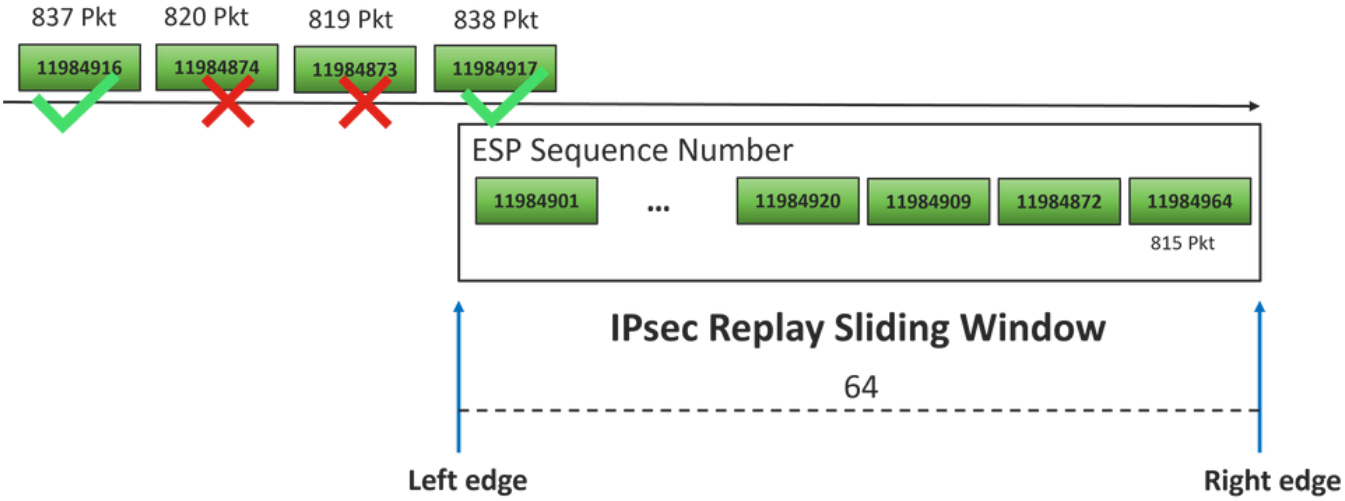
```
REORDERED:
813 PKT: 00b6e00d FWD --- Decimal: 11984909
814 PKT: 00b6dfe8 FWD --- Decimal: 11984872
815 PKT: 00b6e044 FWD --- Decimal: 11984964 ***** Highest Value
816 PKT: 00b6dfed DROP--- Decimal: 11984877
817 PKT: 00b6dfec DROP--- Decimal: 11984876
818 PKT: 00b6dfeb DROP--- Decimal: 11984875
819 PKT: 00b6dfe9 DROP--- Decimal: 11984873
820 PKT: 00b6dfea DROP--- Decimal: 11984874
<snip>
837 PKT: 00b6e014 FWD --- Decimal: 11984916
838 PKT: 00b6e015 FWD --- Decimal: 11984917
839 PKT: 00b6e016 FWD --- Decimal: 11984918
```

> **Hinweis**: Wenn die Sequenznummer größer als die höchste Sequenznummer im Fenster ist, wird die Integrität des Pakets überprüft. Wenn das Paket die Integritätsprüfung besteht, wird das Schieberegler nach rechts verschoben.

Schritt 10. Konvertieren Sie die SN in Dezimalzahlen, und ordnen Sie sie in einfache Berechnung um:

```
Difference:

815 PKT: Decimal: 11984964 ***** Highest Value
-------------------------------------
815(Highest) - X PKT = Diff
-------------------------------------
816 PKT: 11984964 - 11984877 = 87 DROP
817 PKT: 11984964 - 11984876 = 88 DROP
818 PKT: 11984964 - 11984875 = 89 DROP
819 PKT: 11984964 - 11984873 = 91 DROP
820 PKT: 11984964 - 11984874 = 90 DROP
<snip>
837 PKT: 11984964 - 11984916 = 48 FWD
838 PKT: 11984964 - 11984917 = 47 FWD
839 PKT: 11984964 - 11984918 = 45 FWD
```

Für dieses Beispiel ist es möglich, das Schiebefenster mit der **Fenstergröße 64** und dem **rechten Rand11984964** wie im Bild dargestellt **zu** visualisieren.



Die empfangene Sequenznummer für verworfene Pakete liegt weit vor dem rechten Rand des Wiedergabefensters für diesen Sequenzbereich.

Lösung

Da die Fenstergröße noch im vorherigen Wert 64 liegt (siehe Schritt 2), muss einer der Befehle im Abschnitt Befehle zum Erzielen der Effektivität des konfigurierten Wiedergabefensters angewendet werden, damit die Fenstergröße 1024 wirksam wird.

Zusätzliches Wireshark-Erfassungstool

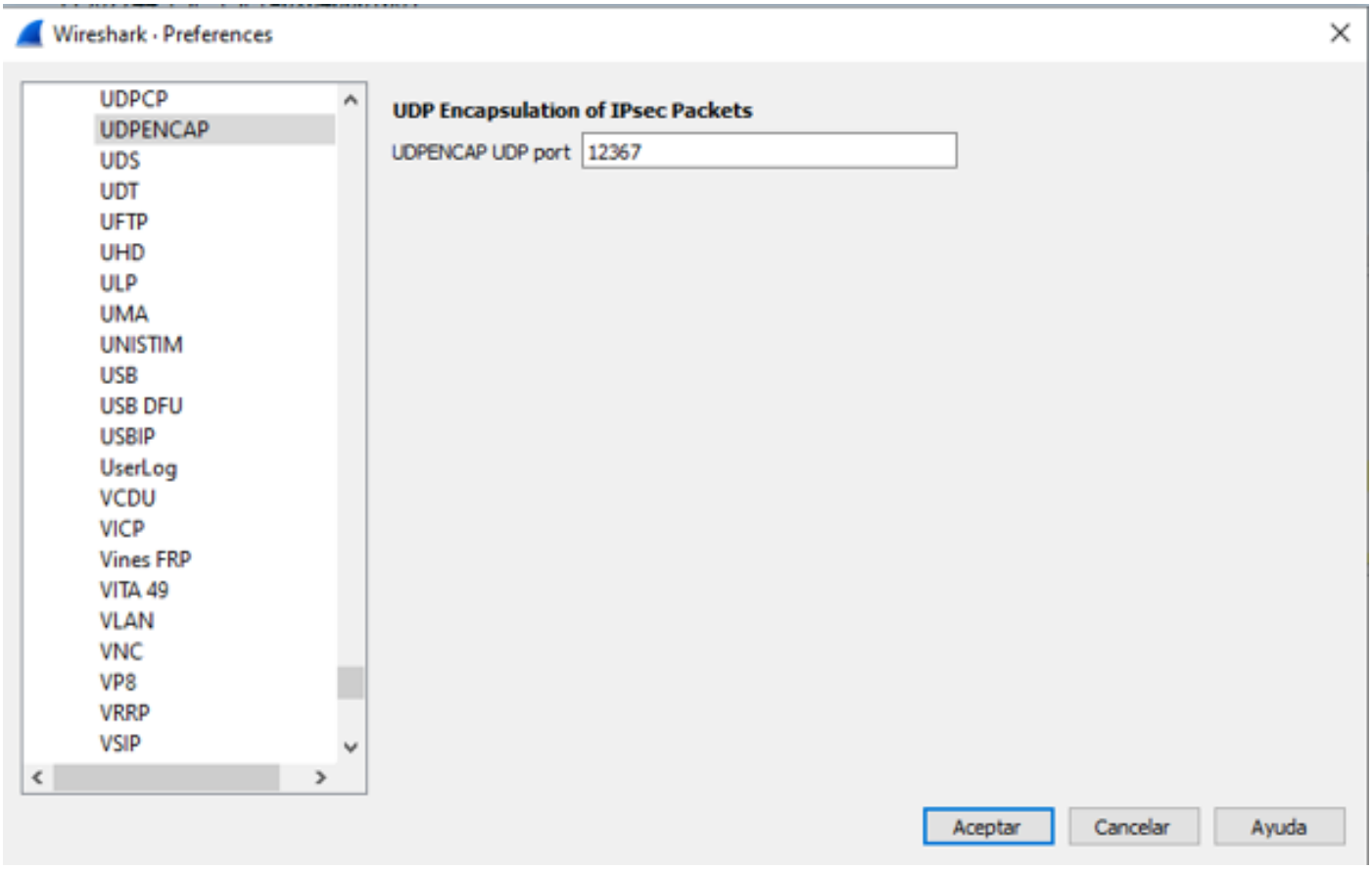
Ein weiteres nützliches Tool zur Korrelation von ESP-SPI und Sequenznummer ist die Wireshark-Software.

> **Hinweis**: Es ist wichtig, die Paketerfassung zu sammeln, wenn das Problem auftritt, und wenn es gleichzeitig möglich ist, die Ablaufverfolgung wie oben beschrieben zu sammeln.

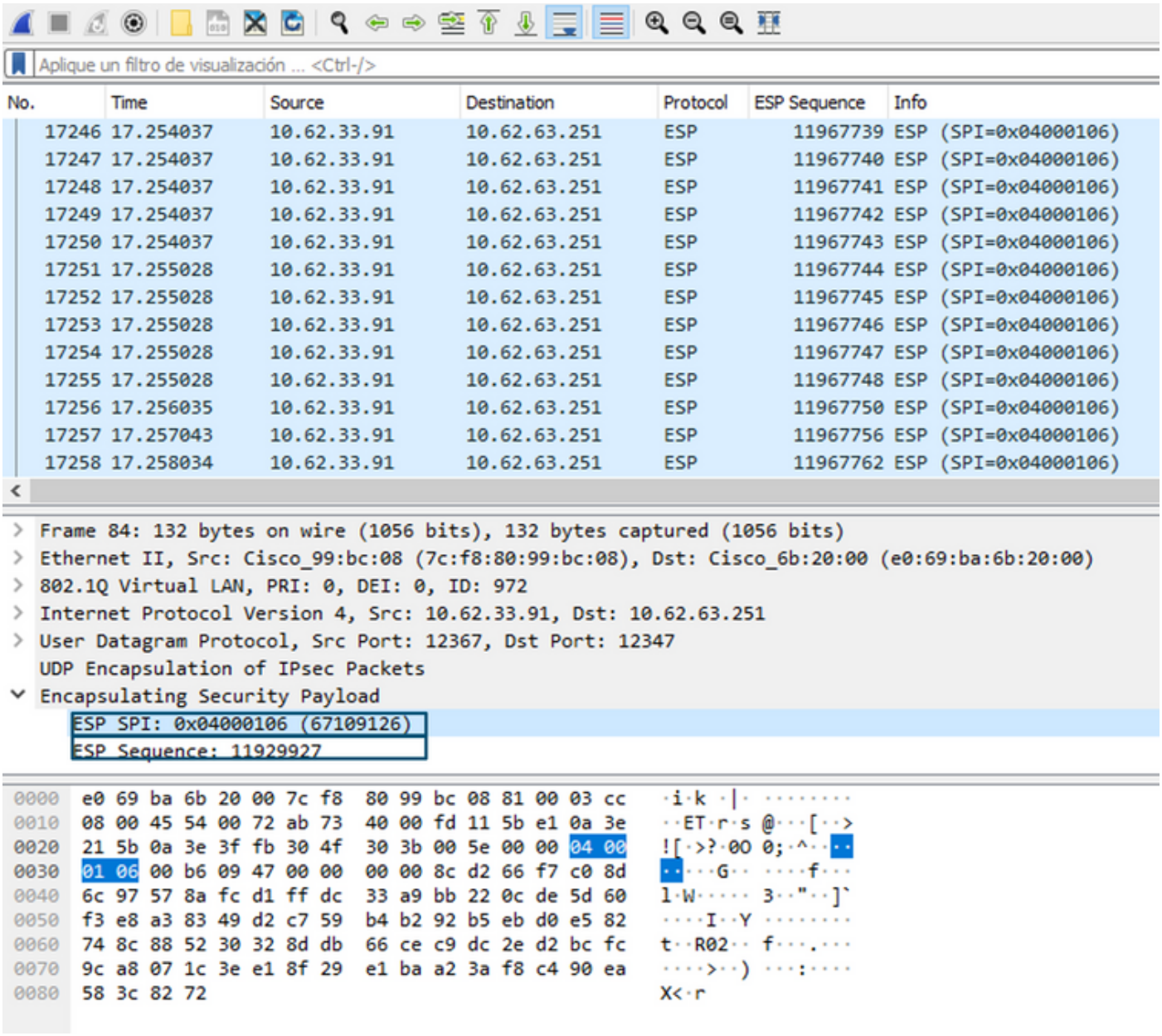
Konfigurieren Sie die Paketerfassung für die eingehende Richtung, und exportieren Sie sie in eine pcap-Datei.

```
monitor caputure CAP match ipv4 host 10.62.33.91 host 10.62.63.251 buffer size 20 inter
TenGigabitEthernet0/0/0 in
monitor caputure CAP star
monitor caputure CAP stop
monitor caputure CAP export bootflash:Anti-replay.pca
```

Wenn die pcap-Architektur in Wireshark geöffnet wird, können Sie, um die ESP-SPI- und Sequenznummer anzuzeigen, ein Paket erweitern, mit der rechten Maustaste klicken und die **Protokolleinstellungen** auswählen, nach **UDPENCAP** suchen und den Standardport in den SD-WAN-Port (Quellport) ändern, wie im Bild dargestellt.



Nachdem UDPENCAP mit dem richtigen Port installiert wurde, werden die ESP-Informationen jetzt angezeigt, wie im Bild gezeigt.



Zugehörige Informationen

- TechZone-Artikel zu IPsec-Anti-Replay-Überprüfungsfehlern
- IPsec-Anti-Replay-Fenster erweitern und deaktivieren
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

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