Analyse und Verwendung von Debugbefehlen zur Fehlerbehebung bei IPsec

Inhalt

Einleitung

In diesem Dokument werden die gängigenDebug-Befehle zur Behebung von IPsec-Problemen mit der Cisco IOS®-Software und mit PIX/ASA beschrieben.

Hintergrundinformationen

Unter Häufigste Lösungen zur Fehlerbehebung von IPsec-VPNs für L2L und Remote-Zugriff finden Sie Informationen zu den häufigsten Lösungen für IPsec-VPN-Probleme.

Es enthält eine Checkliste gängiger Verfahren, die Sie ausprobieren können, bevor Sie mit der Fehlerbehebung beginnen und den technischen Support von Cisco anrufen.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass Sie IPsec konfiguriert haben. Weitere Informationen finden Sie unter IPSec Negotiation/IKE-Protokolle.

Verwendete Komponenten

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.

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

- **Cisco IOS® Software**IPsec-Feature-Set56i - Kennzeichnet Single **Data Encryption Standard (DES)** (für Cisco IOS® Software Version 11.2 und höher).k2 - Zeigt die Triple-DES-Funktion an (für Cisco IOS® Software, Version 12.0 und höher). Triple DES ist ab der Cisco Serie 2600 erhältlich.
- **PIX** - V5.0 und höher, für deren Aktivierung ein einzelner oder drei DES-Lizenzschlüssel erforderlich sind.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Cisco IOS® Software-Debugs

In den Themen in diesem Abschnitt werden die Debugbefehle der Cisco IOS®-Software beschrieben. Weitere Informationen finden Sie unter IPSec Negotiation/IKE-Protokolle.

show crypto isakmp sa

Dieser Befehl zeigt die **Internet Security Association Management Protocol (ISAKMP) Security Associations (SAs)** zwischen Peers erstellt.

```
dst      src        state     conn-id     slot
10.1.0.2  10.1.0.1   QM_IDLE    1           0
```

show crypto ipsec sa

Dieser Befehl zeigt IPsec-SAs an, die zwischen Peers erstellt wurden. Der verschlüsselte Tunnel wird zwischen 10.1.0.1 und 10.1.0.2 für den Datenverkehr zwischen den Netzwerken 10.1.0.0 und 10.1.1.0 erstellt.

Sie können die beiden **Encapsulating Security Payload (ESP)** Eingehende und ausgehende Sicherheitszuordnungen. Der Authentifizierungsheader (AH) wird nicht verwendet, da keine AH-SAs vorhanden sind.

Diese Ausgabe zeigt ein Beispiel für **show crypto ipsec sa** aus.

```
interface: FastEthernet0
  Crypto map tag: test, local addr. 10.1.0.1
 local  ident (addr/mask/prot/port): (10.1.0.0/255.255.255.0/0/0)
 remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
 current_peer: 10.1.0.2
   PERMIT, flags={origin_is_acl,}
  #pkts encaps: 7767918, #pkts encrypt: 7767918, #pkts digest 7767918
  #pkts decaps: 7760382, #pkts decrypt: 7760382, #pkts verify 7760382
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0,
  #pkts decompress failed: 0, #send errors 1, #recv errors 0
   local crypto endpt.: 10.1.0.1, remote crypto endpt.: 10.1.0.2
   path mtu 1500, media mtu 1500
   current outbound spi: 3D3
   inbound esp sas:
    spi: 0x136A010F(325714191)
      transform: esp-3des esp-md5-hmac ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 3442, flow_id: 1443, crypto map: test
      sa timing: remaining key lifetime (k/sec): (4608000/52)
      IV size: 8 bytes
      replay detection support: Y
   inbound ah sas:
   inbound pcp sas:
```

```
inbound pcp sas:
outbound esp sas:
   spi: 0x3D3(979)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 3443, flow_id: 1444, crypto map: test
    sa timing: remaining key lifetime (k/sec): (4608000/52)
    IV size: 8 bytes
    replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

show crypto engine connection active

Dieser Befehl zeigt die einzelnen SAs der Phase 2 und die Menge des gesendeten Datenverkehrs an.

Weil Phase 2 **Security Associations (SAs)** unidirektional sind, zeigt jede SA den Datenverkehr nur in eine Richtung an (Verschlüsselungen sind ausgehend, Entschlüsselungen eingehend).

debuggen crypto isakmp

Diese Ausgabe zeigt ein Beispiel für **debug crypto isakmp** aus.

```
processing SA payload. message ID = 0
Checking ISAKMP transform against priority 1 policy
encryption DES-CBC
      hash SHA
default group 2
auth pre-share
life type in seconds
life duration (basic) of 240
atts are acceptable. Next payload is 0
processing KE payload. message ID = 0
processing NONCE payload. message ID = 0
processing ID payload. message ID = 0
SKEYID state generated
processing HASH payload. message ID = 0
SA has been authenticated
processing SA payload. message ID = 800032287
```

debuggen crypto ipsec

Dieser Befehl zeigt die Quelle und das Ziel von IPsec-Tunnelendpunkten an. **Src_proxy** und **dest_proxy** sind die Client-Subnetze.

Zwei **sa created** -Nachrichten werden mit einer Eins in jede Richtung angezeigt. (Es werden vier Meldungen angezeigt, wenn Sie ESP und AH durchführen.)

Diese Ausgabe zeigt ein Beispiel für **debug crypto ipsec** aus.

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
```

```
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 10.1.0.2, src=10.1.0.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 10.1.0.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 10.1.0.2 to 10.1.0.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 10.1.0.2 to 10.1.0.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 10.1.0.2, src=10.1.0.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 10.1.0.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src=10.1.0.2, dest= 10.1.0.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 10.1.0.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
      (sa) sa_dest= 10.1.0.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 10.1.0.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

Beispiel-Fehlermeldungen

Diese Beispielfehlermeldungen wurden aus den hier aufgeführten **Debug**-Befehlen generiert:

- **debug crypto ipsec**
- **debug crypto isakmp**
- **debug crypt engine**

Wiederholungsprüfung fehlgeschlagen

Diese Ausgabe zeigt ein Beispiel für **Replay Check Failed** fehler:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed connection id=#.
```

Dieser Fehler ist das Ergebnis einer Neuordnung des Übertragungsmediums (insbesondere wenn parallele Pfade vorhanden sind) oder ungleicher Paketpfade, die innerhalb von Cisco IOS® für große und kleine Pakete sowie unter Last verarbeitet werden.

Ändern Sie den Transformationssatz, um dies widerzuspiegeln. Die Fehlermeldung **reply check** wird nur angezeigt, wenn **transform-set esp-md5-hmac** ist aktiviert. Um diese Fehlermeldung zu unterdrücken, deaktivieren Sie **esp-md5-hmac** und nur Verschlüsselung.

Weitere Informationen finden Sie unter Cisco bug IDCSCdp19680 (nur registrierte Kunden) .

QM-FSM-Fehler

Der IPsec L2L VPN-Tunnel wird nicht auf der PIX-Firewall oder der ASA angezeigt, und die QM-FSM-Fehlermeldung wird angezeigt.

Ein möglicher Grund sind die Proxy-Identitäten, z. B. ungewöhnlicher Datenverkehr, **Access Control List (ACL)**, oder die Krypto-ACL nicht auf beiden Seiten übereinstimmen.

Überprüfen Sie die Konfiguration auf beiden Geräten, und stellen Sie sicher, dass die Krypto-ACLs übereinstimmen.

Ein weiterer möglicher Grund ist die fehlende Übereinstimmung der Transformationssatzparameter. Vergewissern Sie sich, dass die VPN-Gateways auf beiden Seiten denselben Transformationssatz mit denselben Parametern verwenden.

Ungültige lokale Adresse

Diese Ausgabe zeigt ein Beispiel für die Fehlermeldung:

```
IPSEC(validate_proposal): invalid local address 10.2.0.2
ISAKMP (0:3): atts not acceptable. Next payload is 0
ISAKMP (0:3): SA not acceptable!
```

Diese Fehlermeldung wird auf eines der beiden häufigsten Probleme zurückgeführt:

- Die Fehlermeldung **crypto map map-name local-address interface-id** veranlasst, dass der Router eine falsche Adresse als Identität verwendet, da er den Router zwingt, eine bestimmte Adresse zu verwenden.
- **Crypto map** wird auf die falsche Schnittstelle angewendet oder überhaupt nicht. Überprüfen Sie die Konfiguration, um sicherzustellen, dass die Crypto Map auf die richtige Schnittstelle angewendet wird.

IKE-Nachricht von X.X.X.X hat die Sanitätsprüfung nicht bestanden oder ist fehlerhaft

Dieser **Debugfehler** wird angezeigt, wenn die vorinstallierten Schlüssel auf den Peers nicht übereinstimmen. Um dieses Problem zu beheben, überprüfen Sie die Pre-Shared Keys auf beiden Seiten.

```
1d00H:%CRPTO-4-IKMP_BAD_MESSAGE: IKE message from 198.51.100.1 failed its
 sanity check or is malformed
```

Fehler im Hauptmodus mit Peer

Dies ist ein Beispiel für die **Main Mode** fehl. Der Ausfall des Hauptmodus deutet darauf hin, dass die

Phase-1-Richtlinie nicht auf beiden Seiten übereinstimmt.

```
1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0
1d00h: ISAKMP (0:1); no offers accepted!
1d00h: ISAKMP (0:1): SA not acceptable!
1d00h: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with
peer at 198.51.100.1
```

Der Befehl **show crypto isakmp sa** gibt an, dass die ISAKMP-SAs **MM_NO_STATE**. Dies bedeutet auch, dass der Hauptmodus ausgefallen ist.

```
dst      src        state     conn-id     slot
10.1.1.2  10.1.1.1   MM_NO_STATE    1           0
```

Überprüfen Sie, ob die Phase-1-Richtlinie auf beiden Peers angewendet wird, und stellen Sie sicher, dass alle Attribute übereinstimmen.

```
Encryption DES or 3DES
Hash MD5 or SHA
Diffie-Hellman Group 1 or 2
Authentication {rsa-sig | rsa-encr | pre-share
```

Nicht unterstützte Proxy-Identitäten

Diese Meldung wird in Debugs angezeigt, wenn die Zugriffsliste für IPsec-Datenverkehr nicht übereinstimmt.

```
1d00h: IPSec(validate_transform_proposal): proxy identities not supported
1d00h: ISAKMP: IPSec policy invalidated proposal
1d00h: ISAKMP (0:2): SA not acceptable!
```

Die Zugriffslisten jedes Peers müssen einander spiegeln (alle Einträge müssen umkehrbar sein). Dieses Beispiel veranschaulicht diesen Punkt.

```
Peer A
access-list 150 permit ip 172.21.113.0 0.0.0.255 172.21.114.0 0.0.0.255
access-list 150 permit ip host 10.2.0.8 host 172.21.114.123
Peer B
access-list 150 permit ip 172.21.114.0 0.0.0.255 172.21.113.0 0.0.0.255
access-list 150 permit ip host 172.21.114.123 host 10.2.0.8
```

Angebot umwandeln wird nicht unterstützt

Diese Meldung wird angezeigt, wenn Phase 2 (IPsec) nicht auf beiden Seiten übereinstimmt. Dies tritt am häufigsten auf, wenn eine Diskrepanz oder eine Inkompatibilität im Transformationssatz vorliegt.

```
1d00h: IPSec (validate_proposal): transform proposal
   (port 3, trans 2, hmac_alg 2) not supported
1d00h: ISAKMP (0:2) : atts not acceptable. Next payload is 0
1d00h: ISAKMP (0:2) SA not acceptable
```

Überprüfen Sie, ob der Transformationssatz auf beiden Seiten übereinstimmt:

```
crypto ipsec transform-set transform-set-name transform1
```

```
[transform2 [transform3]]
? ah-md5-hmac
? ah-sha-hmac
? esp-des
? esp-des and esp-md5-hmac
? esp-des and esp-sha-hmac
? esp-3des and esp-md5-hmac
? esp-3des and esp-sha-hmac
? comp-lzs
```

Keine Zertifizierung und keine Schlüssel mit Remote-Peer

Diese Nachricht zeigt an, dass die auf dem Router konfigurierte Peer-Adresse falsch ist oder geändert wurde. Überprüfen Sie, ob die Peer-Adresse korrekt ist und ob die Adresse erreicht werden kann.

```
1d00h: ISAKMP: No cert, and no keys (public or pre-shared) with
remote peer 198.51.100.2
```

Peer-Adresse X.X.X.X nicht gefunden

Diese Fehlermeldung wird normal mit dem **VPN 3000 Concentrator** fehl **Message: No proposal chosen(14)**. Dies liegt daran, dass es sich bei den Verbindungen um Host-zu-Host-Verbindungen handelt.

Die IPsec-Vorschläge befinden sich in einer Reihenfolge, in der der für den Router ausgewählte Vorschlag mit der Zugriffsliste übereinstimmt, nicht jedoch mit dem Peer.

Die Zugriffsliste verfügt über ein größeres Netzwerk mit dem Host, der den Datenverkehr schneidet. Um dies zu korrigieren, machen Sie zunächst den Vorschlag für diese Verbindung zwischen Konzentrator und Router.

Auf diese Weise kann der Host zuerst zugeordnet werden.

```
20:44:44: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.0.2.15, src=198.51.100.6,
    dest_proxy= 10.0.0.76/255.255.255.255/0/0 (type=1),
    src_proxy= 198.51.100.23/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
20:44:44: IPSEC(validate_transform_proposal):
   peer address 198.51.100.6 not found
```

IPsec-Paket hat ungültigen SPI

Diese Ausgabe ist ein Beispiel für die Fehlermeldung:

```
%PIX|ASA-4-402101: decaps: recd IPSEC packet has
invalid spi for destaddr=dest_address, prot=protocol, spi=number
```

Das empfangene IPsec-Paket gibt eine **Security Parameters Index (SPI)** die nicht im **Security Associations Database (SADB)**. Dies kann aus folgenden Gründen eine vorübergehende Bedingung sein:

- Leichte Unterschiede bei der Alterung von **Security Sssociations (SAs)** zwischen den IPsec-Peers
- Die lokalen SAs wurden gelöscht.

- Vom IPsec-Peer gesendete falsche Pakete

Dies ist möglicherweise ein Angriff.

Empfohlene Aktion: Der Peer bestätigt möglicherweise nicht, dass die lokalen SAs gelöscht wurden. Wenn vom lokalen Router eine neue Verbindung hergestellt wird, können die beiden Peers die Verbindung erfolgreich wiederherstellen.

Andernfalls, wenn das Problem länger als einen kurzen Zeitraum auftritt, versuchen Sie entweder, eine neue Verbindung herzustellen, oder wenden Sie sich an den Administrator dieses Peers.

IPSEC(initialize_sas): Ungültige Proxy-IDs

Der Fehler **21:57:57: IPSEC(initialize_sas): invalid proxy IDs** gibt an, dass die empfangene Proxy-Identität nicht mit der konfigurierten Proxy-Identität gemäß Zugriffsliste übereinstimmt.

Um sicherzustellen, dass beide übereinstimmen, überprüfen Sie die Ausgabe des Befehls **debug**.

In der Ausgabe des Befehls **debug** der Vorschlagsanforderung stimmt die Zugriffsliste 103 permit ip 10.1.1.0 0.0.0.255 10.1.0.0 0.0.0.255 nicht überein.

Die Zugriffsliste ist einerseits netzwerkspezifisch und andererseits hostspezifisch.

```
21:57:57: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.0.2.1, src=192.0.2.2,
    dest_proxy= 10.1.1.1/255.255.255.0/0/0 (type=4),
    src_proxy= 10.2.0.1/255.255.255.0/0/0 (type=4)
```

Reserviert, nicht Null bei Payload 5

Das bedeutet, dass die ISAKMP-Schlüssel nicht übereinstimmen. Erneute Eingabe/Zurücksetzen, um die Genauigkeit zu gewährleisten.

Der angebotene Hash-Algorithmus stimmt nicht mit der Richtlinie überein.

Wenn die konfigurierten ISAKMP-Richtlinien nicht mit der vorgeschlagenen Richtlinie des Remote-Peers übereinstimmen, versucht der Router, die Standardrichtlinie von 65535 zu verwenden.

Wenn diese beiden Werte nicht übereinstimmen, schlägt die ISAKMP-Aushandlung fehl.

Ein Benutzer empfängt entweder **Hash algorithm offered does not match policy!** Oder **Encryption algorithm offered does not match policy!** Fehlermeldung auf den Routern.

```
=RouterA=
3d01h: ISAKMP (0:1): processing SA payload. message ID = 0
3d01h: ISAKMP (0:1): found peer pre-shared key matched 203.0.113.22
ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:1): Hash algorithm offered does not match policy!
```

```
ISAKMP (0:1): atts are not acceptable. Next payload is 0
=RouterB=
ISAKMP (0:1): Checking ISAKMP transform 1 against priority 65535 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 0
ISAKMP (0:1): no offers accepted!
ISAKMP (0:1): phase 1 SA not acceptable!
```

HMAC-Überprüfung fehlgeschlagen

Diese Fehlermeldung wird angezeigt, wenn bei der Überprüfung der **Hash Message Authentication Code** auf dem IPsec-Paket. Dies geschieht normalerweise, wenn das Paket in irgendeiner Weise beschädigt ist.

```
Sep 22 11:02:39 203.0.113.16 2435:
Sep 22 11:02:39: %MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure
Sep 22 11:02:39 203.0.113.16 2436:
Sep 22 11:02:39: %MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000,
                 PktEngReturn_MACMiscompare
```

Wenn diese Fehlermeldung gelegentlich auftritt, können Sie sie ignorieren. Wenn dies jedoch häufiger geschieht, müssen Sie die Quelle der Beschädigung des Pakets untersuchen. Dies kann auf einen Fehler im Crypto Accelerator zurückzuführen sein.

Remote-Peer antwortet nicht

Diese Fehlermeldung wird angezeigt, wenn beim Transformationssatz eine Ungleichheit auftritt. Stellen Sie sicher, dass die zugeordneten Transformationssätze auf beiden Peers konfiguriert sind.

Alle IPSec-SA-Angebote als inakzeptabel eingestuft

Diese Fehlermeldung tritt auf, wenn die IPSec-Parameter der Phase 2 zwischen dem lokalen und dem Remote-Standort nicht übereinstimmen.

Um dieses Problem zu beheben, geben Sie die gleichen Parameter im Transformationssatz an, sodass sie übereinstimmen und ein erfolgreiches VPN eingerichtet wird.

Fehler bei Paketverschlüsselung/-entschlüsselung

Diese Ausgabe ist ein Beispiel für die Fehlermeldung:

```
HW_VPN-1-HPRXERR: Virtual Private Network (VPN) Module0/2: Packet Encryption/Decryption
error, status=4615
```

Diese Fehlermeldung kann einen der folgenden Gründe haben:

- Fragmentierung - Fragmentierte Kryptopakete werden per Prozess-Switching übertragen, sodass die schnell geschalteten Pakete vor den verarbeiteten Paketen an die VPN-Karte gesendet werden.

Werden genügend schnell geschaltete Pakete vor den prozessgeschalteten Paketen verarbeitet, wird die ESP- oder AH-Sequenznummer für das prozessgeschaltete Paket veraltet, und wenn das Paket bei der VPN-Karte ankommt, befindet sich seine Sequenznummer außerhalb des Wiedergabefensters.

Dies verursacht entweder AH- oder ESP-Sequenzzahlfehler (4615 bzw. 4612), je nachdem, welche Kapselung Sie verwenden.

- Veraltete Cacheeinträge — Eine weitere mögliche Ursache ist, dass ein Fast-Switch-Cacheeintrag veraltet wird und das erste Paket mit einem Cachefehler prozessvertauscht wird.

Problemumgehungen

1. Deaktivieren Sie alle Authentifizierungstypen im 3DES-Transformationssatz, und verwenden Sie ESP-DES/3DES. Dadurch wird der Authentifizierungs-/Anti-Replay-Schutz effektiv deaktiviert, wodurch (wiederum) Paketverluste aufgrund von ungeordnetem (gemischtem) IPsec-Datenverkehr vermieden werden. **%HW_VPN-1-HPRXERR: Hardware VPN0/2: Packet Encryption/Decryption error, status=4615.**
2. Eine Problemumgehung, die für den hier erwähnten Grund gilt, besteht darin, die **Maximum Transmission Unit (MTU)** Größe eingehender Streams auf weniger als 1.400 Byte. Geben Sie den folgenden Befehl ein, um die maximale MTU-Größe (Transmission Unit) eingehender Streams auf weniger als 1.400 Byte festzulegen:
   ```
   ip tcp adjust-mss 1300
   ```
3. Deaktivieren Sie die AIM-Karte.
4. Deaktivieren Sie Fast/CEF-Switching an den Router-Schnittstellen. Um Fast Switching zu entfernen, verwenden Sie diese Befehle im Schnittstellenkonfigurationsmodus:
   ```
   no ip route-cache
   ```

Fehler beim Empfang von Paketen aufgrund eines Fehlers der ESP-Sequenz

Hier ein Beispiel der Fehlermeldung:

```
%C1700_EM-1-ERROR: packet-rx error: ESP sequence fail
```

Diese Fehlermeldung weist in der Regel auf eine der folgenden möglichen Bedingungen hin:

- Die verschlüsselten IPsec-Pakete werden aufgrund eines falsch konfigurierten QoS-Mechanismus vom verschlüsselnden Router aus der richtigen Reihenfolge weitergeleitet.
- Die vom Entschlüsselungsrouter empfangenen IPsec-Pakete sind aufgrund einer Paketneuordnung an einem zwischengeschalteten Gerät außer Betrieb.
- Das empfangene IPsec-Paket ist fragmentiert und muss vor der Authentifizierungsprüfung und -entschlüsselung erneut zusammengesetzt werden.

Problemumgehung

1. Deaktivieren Sie QoS für den IPsec-Datenverkehr auf den verschlüsselnden oder zwischengeschalteten Routern.

2. Aktivieren Sie die IPsec-Vorabfragmentierung auf dem Verschlüsselungsrouter.
   ```
   Router(config-if)#crypto ipsec fragmentation before-encryption
   ```

3. Stellen Sie den MTU-Wert auf eine Größe ein, die nicht fragmentiert werden muss.
   ```
   Router(config)#interface type [slot_#/]port_#


   Router(config-if)#ip mtu MTU_size_in_bytes
   ```

4. Aktualisieren Sie das Cisco IOS®-Image auf das neueste verfügbare Stable-Image in diesem Zug.

Wenn die MTU-Größe auf einem Router geändert wird, werden alle an dieser Schnittstelle terminierten Tunnel deaktiviert.

Planen Sie, diese Problemumgehung während einer geplanten Ausfallzeit durchzuführen.

Fehler beim Einrichten des VPN-Tunnels auf dem Router der Serie 7600

Dieser Fehler tritt auf, wenn Sie versuchen, einen VPN-Tunnel auf Routern der Serie 7600 einzurichten:

```
crypto_engine_select_crypto_engine: can't handle any more
```

Dieser Fehler tritt auf, da die Softwareverschlüsselung auf Routern der Serie 7600 nicht unterstützt wird. Router der 7600-Serie unterstützen keine IPsec-Tunnelterminierung ohne IPsec-SPA-Hardware. VPN wird bei 7600-Routern nur mit einer IPSEC-SPA-Karte unterstützt.

PIX-Debugger

show crypto isakmp sa

Dieser Befehl zeigt die ISAKMP-SAs zwischen Peers an.

```
dst      src        state     conn-id     slot
10.1.0.2  10.1.0.1   QM_IDLE    1           0
```

In derHow crypto isakmp saoutput muss der Status immer **QM_IDLE lauten**. Wenn der Status **MM_KEY_EXCH** lautet, bedeutet dies, dass entweder der konfigurierte vorinstallierte Schlüssel nicht richtig ist oder die Peer-IP-Adressen unterschiedlich sind.

```
PIX(config)#show crypto isakmp sa
Total     : 2
Embryonic : 1
        dst               src        state     pending     created
 192.168.254.250   10.177.243.187    MM_KEY_EXCH   0           0
```

Sie können dies korrigieren, wenn Sie die richtige IP-Adresse oder den vorinstallierten Schlüssel konfigurieren.

show crypto ipsec sa

Dieser Befehl zeigt IPsec-SAs an, die zwischen Peers erstellt wurden. Für den Datenverkehr zwischen den Netzwerken 10.1.0.0 und 10.1.1.0 wird ein verschlüsselter Tunnel zwischen 10.1.0.1 und 10.1.0.2 erstellt.

Die beiden integrierten ESP-SAs sind eingehend und ausgehend zu sehen. AH wird nicht verwendet, da es keine AH-SAs gibt.

Ein Beispiel für **show crypto ipsec sa** wird in dieser Ausgabe angezeigt.

```
interface: outside
    Crypto map tag: vpn, local addr. 10.1.0.1
   local  ident (addr/mask/prot/port): (10.1.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.1.0.2/255.255.255.255/0/0)
   current_peer: 10.2.1.1
   dynamic allocated peer ip: 10.1.0.2
     PERMIT, flags={}
    #pkts encaps: 345, #pkts encrypt: 345, #pkts digest 0
    #pkts decaps: 366, #pkts decrypt: 366, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0
     local crypto endpt.: 10.1.0.1, remote crypto endpt.: 10.1.0.2
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 9a46ecae
     inbound esp sas:
      spi: 0x50b98b5(84646069)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (460800/21)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x9a46ecae(2588339374)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (460800/21)
        IV size: 8 bytes
        replay detection support: Y
    outbound ah sas:
```

debuggen crypto isakmp

Dieser Befehl zeigt Debuginformationen über IPsec-Verbindungen und den ersten Satz von Attributen an, die aufgrund von Inkompatibilitäten auf beiden Seiten abgelehnt wurden.

Der zweite Versuch, eine Übereinstimmung herzustellen (3DES anstelle von DES und **Secure Hash Algorithm (SHA)** ist akzeptabel und die ISAKMP SA wurde erstellt.

Dieses Debugging wird auch von einem DFÜ-Client durchgeführt, der eine IP-Adresse (10.32.8.1) aus einem lokalen Pool akzeptiert. Sobald die ISAKMP-SAs erstellt wurden, werden die IPsec-Attribute ausgehandelt und als akzeptabel eingestuft.

Der PIX richtet dann die IPsec-SAs wie hier dargestellt ein. Diese Ausgabe zeigt ein Beispiel für **debug crypto isakmp** aus.

```
crypto_isakmp_process_block: src 10.1.0.1, dest 10.1.0.2
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0): atts are acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP: Created a peer node for 10.1.0.2
OAK_QM exchange
ISAKMP (0:0): Need config/address
ISAKMP (0:0): initiating peer config to 10.1.0.2. ID = 2607270170 (0x9b67c91a)
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.1.0.2, dest 10.1.0.1
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.1.0.2.
   message ID = 2156506360
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0): peer accepted the address!
ISAKMP (0:0): processing saved QM.
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 818324052
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
IPSEC(validate_proposal): transform proposal
   (prot 3, trans 2, hmac_alg 1) not supported
ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPSec proposal 2
ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP (0): atts are acceptable.
ISAKMP (0): processing NONCE payload. message ID = 818324052
ISAKMP (0): processing ID payload. message ID = 81
ISAKMP (0): ID_IPV4_ADDR src 10.32.8.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 81
ISAKMP (0): ID_IPV4_ADDR dst 10.1.0.1 prot 0 port 0
INITIAL_CONTACTIPSEC(key_engine): got a queue event...
```

debuggen crypto ipsec

Dieser Befehl zeigt **Debuginformationen** über IPsec-Verbindungen an.

```
IPSEC(key_engine): got a queue event...
```

```
IPSEC(spi_response): getting spi 0xd532efbd(3576885181) for SA
        from  10.1.0.2  to  10.1.0.1  for prot 3
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.1.0.2, dest 10.1.0.1
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
        inbound SA from  10.1.0.2  to  10.1.0.1
           (proxy 10.32.8.1 to  10.1.0.1.)
        has spi 3576885181 and conn_id 2 and flags 4
        outbound SA from  10.1.0.1  to  10.1.0.2
           (proxy 10.1.0.1 to 10.32.8.1)
        has spi 2749108168 and conn_id 1 and flags 4IPSEC(key_engine):
           got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 10.1.0.1, src=10.1.0.2,
    dest_proxy= 10.1.0.1/0.0.0.0/0/0 (type=1),
    src_proxy= 10.32.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xd532efbd(3576885181), conn_id= 2, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src=10.1.0.1, dest= 10.1.0.2,
    src_proxy= 10.1.0.1/0.0.0.0/0/0 (type=1),
    dest_proxy= 10.32.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xa3dc0fc8(2749108168), conn_id= 1, keysize= 0, flags= 0x4
return status is IKMP_NO_ERROR
```

Häufige Probleme mit dem Router-zu-VPN-Client

Kein Zugriff auf Subnetze außerhalb des VPN-Tunnels möglich: Split-Tunnel

In dieser Ausgabe der Beispielrouterkonfiguration wird veranschaulicht, wie ein Split-Tunnel für die VPN-Verbindungen aktiviert wird.

Die Fehlermeldung **split tunnel** wird der Gruppe zugeordnet, wie im **crypto isakmp client configuration group hw-client-groupname** aus.

Dies ermöglicht **Cisco VPN Client** den Router für den Zugriff auf ein zusätzliches Subnetz zu verwenden, das nicht Teil des VPN-Tunnels ist.

Dies geschieht ohne Kompromisse bei der Sicherheit der IPsec-Verbindung. Der Tunnel wird im Netzwerk 192.0.2.18 gebildet.

Der Datenverkehr fließt unverschlüsselt zu Geräten, die nicht im **access list 150** wie das Internet.

```
!
crypto isakmp client configuration group hw-client-groupname
 key hw-client-password
 dns 192.0.2.20 198.51.100.21
 wins 192.0.2.22 192.0.2.23
 domain cisco.com
 pool dynpool
 acl 150
!
```

```
!
access-list 150 permit ip 192.0.2.18 0.0.0.127 any
!
```

Häufige Probleme mit dem PIX-zu-VPN-Client

Die Themen in diesem Abschnitt behandeln häufige Probleme, die Sie bei der Konfiguration von PIX zu IPsec mithilfe von VPN Client 3.x haben. Die Beispielkonfigurationen für PIX basieren auf Version 6.x.

Der Datenverkehr fließt nicht, nachdem der Tunnel eingerichtet wurde: Ping im Netzwerk hinter PIX nicht möglich

Dieses Problem tritt häufig beim Routing auf. Stellen Sie sicher, dass der PIX über eine Route für interne Netzwerke verfügt, die nicht direkt mit demselben Subnetz verbunden sind.

Außerdem muss das interne Netzwerk über eine Route zurück zum PIX für die Adressen im Client-Adresspool verfügen.

Diese Ausgabe zeigt ein Beispiel.

```
!--- Address of PIX inside interface.

ip address inside 10.1.1.1 255.255.255.240

!--- Route to the networks that are on the inside segment. !--- The next hop is the router on
the inside.

route inside 172.16.0.0 255.255.0.0 10.1.1.2 1

 !--- Pool of addresses defined on PIX from which it assigns !--- addresses to the VPN Client
for the IPsec session.

ip local pool mypool 10.1.2.1-10.1.2.254

!--- On the internal router, if the default gateway is not !--- the PIX inside interface, then
the router needs to have route !--- for 10.1.2.0/24 network with next hop as the PIX inside
interface !.

ip route 10.1.2.0 255.255.255.0 10.1.1.1
```

Nach dem Tunnel kann der Benutzer nicht mehr im Internet surfen: Split-Tunnel

Der häufigste Grund für dieses Problem ist, dass der gesamte Datenverkehr beim IPsec-Tunnel vom VPN-Client zum PIX über den Tunnel an die PIX-Firewall gesendet wird.

Die PIX-Funktion verhindert, dass Datenverkehr an die Schnittstelle zurückgesendet wird, an der er empfangen wurde. Der für das Internet bestimmte Datenverkehr funktioniert daher nicht.

Um dieses Problem zu beheben, verwenden Sie die **split tunnel** aus. Die Idee hinter diesem Fix ist, dass nur einer bestimmten Verkehr durch den Tunnel sendet und der Rest des Verkehrs direkt zum Internet geht, nicht durch den Tunnel.

```
vpngroup vpn3000 split-tunnel 90
access-list 90 permit ip 10.1.1.0 255.255.255.0 10.1.2.0 255.255.255.0
```

```
access-list 90 permit ip 172.16.0.0 255.255.0.0 10.1.2.0 255.255.255.0
```

Die Fehlermeldung **vpngroup vpn3000 split-tunnel 90** aktiviert den Split-Tunnel mit **access-list number 90**.

Die Fehlermeldung **access-list number 90** legt fest, welcher Datenverkehr durch den Tunnel fließt. Der Rest wird am Ende der Zugriffsliste abgelehnt.

Die Zugriffsliste muss identisch sein, um abgelehnt zu werden. **Network Address Translation (NAT)** auf PIX.

Nach dem Tunnelstart funktionieren bestimmte Anwendungen nicht mehr: MTU-Anpassung auf Client

Nachdem der Tunnel eingerichtet wurde, können Sie zwar die Computer im Netzwerk hinter der PIX-Firewall pingen, bestimmte Anwendungen wie Microsoft jedoch nicht verwenden. **Outlook**.

Ein häufiges Problem ist die maximale Übertragungseinheit (MTU) der Pakete. Der IPsec-Header kann bis zu 50 bis 60 Byte lang sein und dem ursprünglichen Paket hinzugefügt werden.

Wenn die Größe des Pakets 1500 übersteigt (dies ist der Standard für das Internet), müssen die Geräte es fragmentieren. Nachdem der IPsec-Header hinzugefügt wurde, ist die Größe immer noch unter 1496, dem Maximum für IPsec.

Die Fehlermeldung **show interface** zeigt die MTU dieser Schnittstelle auf den zugänglichen Routern oder auf den Routern in Ihrem eigenen Gebäude an.

Um die MTU des gesamten Pfades von der Quelle bis zum Ziel zu bestimmen, werden die Datagramme unterschiedlicher Größe zusammen mit dem **Do Not Fragment (DF)** Bit so festgelegt, dass diese Fehlermeldung an die Quelle zurückgesendet wird, wenn das gesendete Datagramm größer als die MTU ist:

```
frag. needed and DF set
```

Diese Ausgabe zeigt ein Beispiel für das Ermitteln der MTU des Pfads zwischen den Hosts mit den IP-Adressen 10.1.1.2 und 172.16.1.56.

```
Router#debug ip icmp
ICMP packet debugging is on


!--- Perform an extended ping.

Router#ping
Protocol [ip]:
Target IP address: 172.16.1.56
Repeat count [5]:
Datagram size [100]: 1550
Timeout in seconds [2]:


!--- Make sure you enter y for extended commands.

Extended commands [n]: y
Source address or interface: 10.1.1.2
Type of service [0]:
```

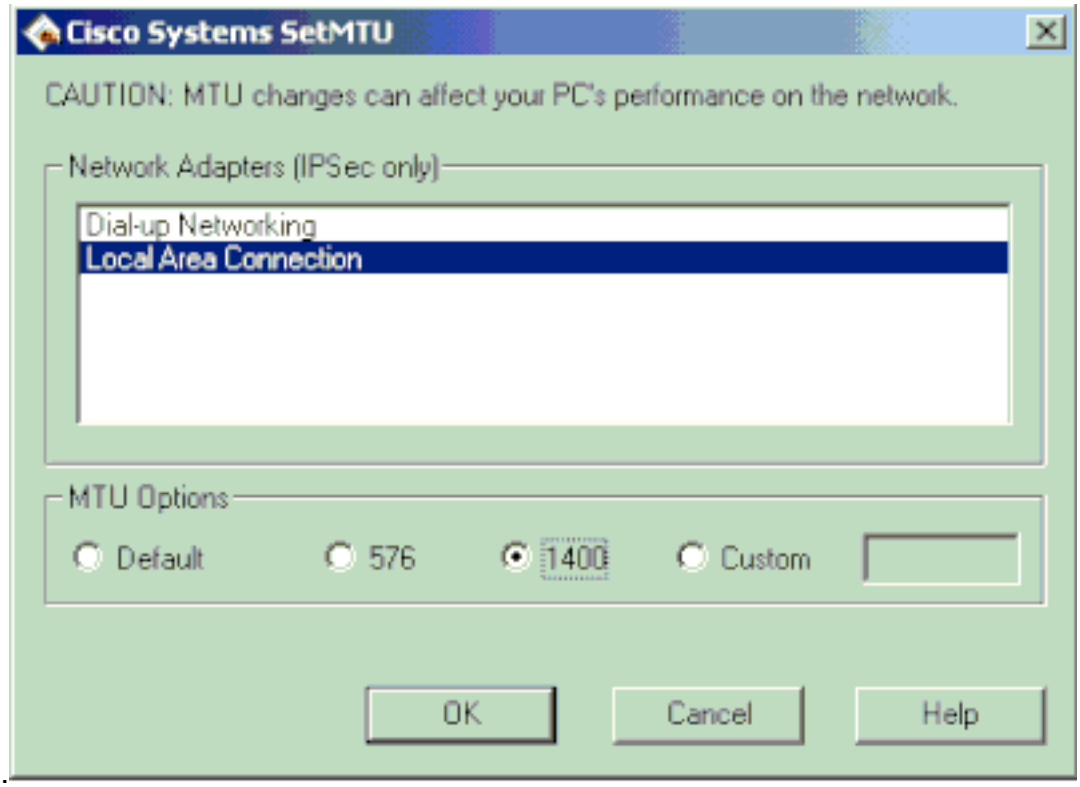
```
!--- Set the DF bit as shown.


Set DF bit in IP header? [no]: y
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1550-byte ICMP Echos to 172.16.1.56, timeout is 2 seconds:

2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
Success rate is 0 percent (0/5)


!--- Reduce the datagram size further and perform extended ping again.

Router#ping
Protocol [ip]:
Target IP address: 172.16.1.56
Repeat count [5]:
Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.2
Type of service [0]:
Set DF bit in IP header? [no]: y
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 172.16.1.56, timeout is 2 seconds:
!!!!!
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2

Success rate is 100 percent (5/5), round-trip min/avg/max = 380/383/384 ms
```

Der VPN-Client verfügt über ein Dienstprogramm zur MTU-Anpassung, mit dem der Benutzer die MTU für den Cisco VPN-Client anpassen kann.

Bei PPP over Ethernet (PPPoE)-Client-Benutzern muss die MTU für den PPPoE-Adapter angepasst werden.

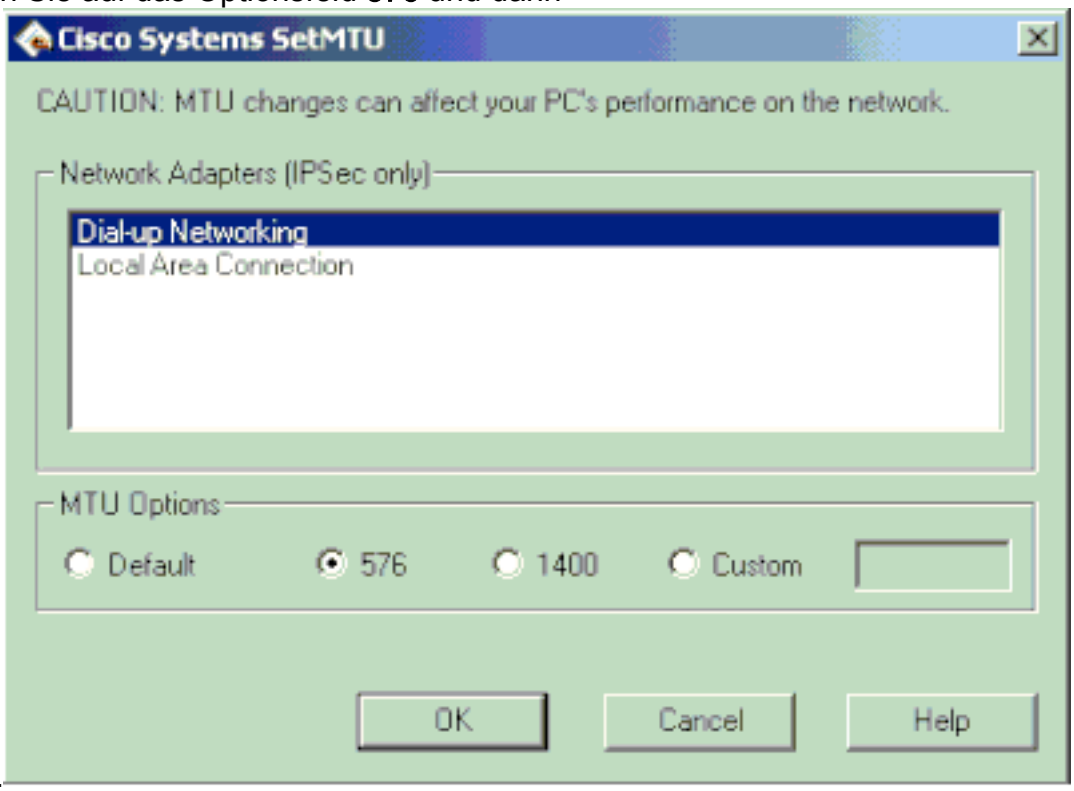
Führen Sie diese Schritte aus, um das MTU-Dienstprogramm für den VPN-Client anzupassen.

1. Auswählen **Start > Programs > Cisco System VPN Client > Set MTU**.
2. Auswählen **Local Area Connection**, und klicken Sie dann auf das Optionsfeld 1400.
3. Klicken Sie auf



OK.

4. Wiederholen Sie Schritt 1, und wählen Sie **Dial-up Networking**.
5. Klicken Sie auf das Optionsfeld **576** und dann



auf**OK**.

Verpasst den Befehl sysopt

Verwenden Sie **sysopt connection permit-ipsec** in IPsec-Konfigurationen auf dem PIX, um zu ermöglichen, dass IPsec-Datenverkehr die PIX-Firewall passiert, ohne **conduit** Oder **access-list** Befehlen.

Jede eingehende Sitzung muss standardmäßig explizit von einem **conduit** Oder **access-list** -Anweisung. Bei IPsec-geschütztem Datenverkehr kann die sekundäre Zugriffslistenüberprüfung redundant sein.

Damit eingehende Sitzungen mit IPsec-Authentifizierung/Verschlüsselung immer zugelassen werden, verwenden Sie die **sysopt connection permit-ipsec** aus.

Überprüfen von Zugriffskontrolllisten (ACLs)

In einer typischen IPsec-VPN-Konfiguration werden zwei Zugriffslisten verwendet.

Eine Zugriffsliste wird verwendet, um Datenverkehr, der für den VPN-Tunnel bestimmt ist, vom NAT-Prozess auszuschließen.

Die andere Zugriffsliste legt fest, welcher Datenverkehr verschlüsselt werden soll. Dies umfasst eine Krypto-ACL in einer LAN-zu-LAN-Konfiguration oder eine Split-Tunnel-ACL in einer Remote-Zugriffskonfiguration.

Wenn diese ACLs nicht richtig konfiguriert sind oder verpasst werden, fließt der Datenverkehr möglicherweise nur in eine Richtung durch den VPN-Tunnel, oder er wurde überhaupt nicht über den Tunnel gesendet.

Stellen Sie sicher, dass Sie alle erforderlichen Zugriffslisten konfiguriert haben, um Ihre IPsec-VPN-Konfiguration abzuschließen, und dass diese Zugriffslisten den richtigen Datenverkehr definieren.

Diese Liste enthält Elemente, die überprüft werden müssen, wenn Sie vermuten, dass eine ACL die Ursache von Problemen mit Ihrem IPsec-VPN ist.

- Stellen Sie sicher, dass Ihre NAT-Ausnahme und Krypto-ACLs den richtigen Datenverkehr angeben.
- Wenn Sie mehrere VPN-Tunnel und mehrere Krypto-ACLs haben, stellen Sie sicher, dass sich diese ACLs nicht überschneiden.
- Verwenden Sie ACLs nicht doppelt. Verwenden Sie zwei unterschiedliche Zugriffslisten, auch wenn Ihre NAT-Ausnahme-ACL und Ihre Krypto-ACL denselben Datenverkehr angeben.
- Stellen Sie sicher, dass Ihr Gerät für die Verwendung der NAT-Ausnahme-ACL konfiguriert ist. Das heißt, verwenden Sie die **route-map** Befehl auf dem Router; die **nat (0)** auf dem PIX oder ASA. Eine NAT-Ausnahme-ACL ist für LAN-zu-LAN- und RAS-Konfigurationen erforderlich.

Weitere Informationen zum Überprüfen der ACL-Anweisungen finden Sie unter Verify that ACLs are Corrected in Most Common L2L and Remote Access IPsec VPN Troubleshooting Solutions.

Zugehörige Informationen

- Support-Seite für IPsec-Aushandlung/IKE-Protokoll
- PIX-Support-Seite
- Technische Hinweise
- Technischer Support und Dokumentation für Cisco Systeme

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.