Beheben von häufigen Problemen bei L2L und RAS-IPsec-VPN

Inhalt

Einleitung

In diesem Dokument werden die häufigsten Lösungen für IPsec-VPN-Probleme beschrieben.

Hintergrundinformationen

Die hier beschriebenen Lösungen sind direkt auf Serviceanfragen zurückzuführen, die vom technischen Support von Cisco bearbeitet wurden.

Viele dieser Lösungen werden vor der detaillierten Fehlerbehebung einer IPsec-VPN-Verbindung implementiert.

In diesem Dokument finden Sie eine Zusammenfassung der gängigen Verfahren, die Sie vor Beginn der Fehlerbehebung bei einer Verbindung ausprobieren müssen.

Obwohl die Konfigurationsbeispiele in diesem Dokument für die Verwendung auf Routern und Security Appliances vorgesehen sind, gelten fast alle diese Konzepte auch für VPN 3000.

Eine Erläuterung der gängigen Debug-Befehle zur Behebung von IPsec-Problemen mit der Cisco IOS®-Software und finden Sie unter IP Security Troubleshooting - Understanding and Using debug Commands .

Hinweis: ASA leitet Multicast-Datenverkehr nicht über IPsec-VPN-Tunnel weiter.

Warnung: Viele der in diesem Dokument vorgestellten Lösungen können zu einem vorübergehenden Verlust der gesamten IPsec-VPN-Verbindung auf einem Gerät führen.

Es wird empfohlen, diese Lösungen mit Vorsicht und in Übereinstimmung mit Ihrer Änderungskontrollrichtlinie zu implementieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt die Kenntnis der IPsec-VPN-Konfiguration auf folgenden Cisco Geräten:

- Cisco Adaptive Security Appliance der ASA 5500-Serie
- Cisco IOS® Router

Verwendete Komponenten

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

- Cisco Adaptive Security Appliance der ASA 5500-Serie
- Cisco IOS®

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.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Convention.

IPsec-VPN-Konfiguration funktioniert nicht

Problem

Eine kürzlich konfigurierte oder geänderte IPsec-VPN-Lösung funktioniert nicht.

Eine aktuelle IPsec-VPN-Konfiguration funktioniert nicht mehr.

Lösungen

Dieser Abschnitt enthält Lösungen für die häufigsten IPsec-VPN-Probleme.

Obwohl sie nicht in einer bestimmten Reihenfolge aufgeführt sind, können diese Lösungen als Checkliste verwendet werden, um sie zu überprüfen oder zu testen, bevor Sie eine gründliche Sanierung einleiten.

Alle diese Lösungen stammen direkt aus TAC-Serviceanfragen und haben eine Reihe von Problemen gelöst.

- NAT-Traversal aktivieren (RA-VPN-Problem Nr. 1)
- Ordnungsgemäßer Verbindungstest
- Aktivieren von ISAKMP
- Aktivieren/Deaktivieren von PFS
- Löschen alter oder vorhandener Sicherheitszuordnungen (Tunnel)
- Überprüfen der ISAKMP-Lebensdauer
- Aktivieren oder Deaktivieren von ISAKMP Keepalives
- Erneute Eingabe oder Wiederherstellung von Pre-Shared-Keys
- Nicht übereinstimmender Pre-Shared Key
- Entfernen und erneutes Anwenden von Krypto-Zuordnungen
- Stellen Sie sicher, dass die sysopt-Befehle vorhanden sind (nur /ASA).
- Überprüfen der ISAKMP-Identität

- Überprüfen des Leerlauf-/Sitzungs-Timeouts
- Überprüfen Sie, ob die ACLs korrekt sind und an die Krypto-Zuordnung gebunden sind
- Überprüfen der ISAKMP-Richtlinien
- Überprüfen, ob das Routing korrekt ist
- Überprüfen, ob die Transformationsgruppe korrekt ist
- Überprüfen Sie die Sequenznummern und den Namen der Krypto-Zuordnung
- Überprüfen, ob die Peer-IP-Adresse korrekt ist
- Überprüfen der Tunnelgruppe und der Gruppennamen
- Deaktivieren von XAUTH für L2L-Peers
- Erschöpfung des VPN-Pools
- Probleme mit der Latenz für VPN-Client-Datenverkehr

Hinweis: Einige der Befehle in diesen Abschnitten wurden aus Platzgründen um eine zweite Zeile erweitert.

NAT-Traversal aktivieren (RA-VPN-Problem Nr. 1)

NAT-Traversal (oder NAT-T) ermöglicht die Weiterleitung von VPN-Datenverkehr über NAT- oder PAT-Geräte, z. B. einen Linksys SOHO-Router.

Wenn NAT-T nicht aktiviert ist, stellen Benutzer des VPN-Clients häufig eine problemlose Verbindung mit der ASA her, können jedoch nicht auf das interne Netzwerk hinter der Sicherheits-Appliance zugreifen.

Wenn Sie NAT-T nicht im NAT/PAT-Gerät aktivieren, können Sie die Fehlermeldung **`Regelmäßige Übersetzung konnte für Protokoll 50 src innerhalb:10.0.1.26 dst außerhalb:10.9.69.4`**in ASA empfangen.

Wenn Sie sich nicht gleichzeitig über dieselbe IP-Adresse anmelden können, wird **`die sichere VPN-Verbindung vom Client lokal beendet. Grund 412: Der Remote-Peer antwortet nicht mehr.`**Fehlermeldung wird angezeigt.

Aktivieren Sie NAT-T im Headend-VPN-Gerät, um diesen Fehler zu beheben.

Hinweis: Ab Version 12.2(13)T der Cisco IOS® Software ist NAT-T in Cisco IOS® standardmäßig aktiviert.

Folgende Befehle dienen zum Aktivieren von NAT-T auf einer Cisco Security-Appliance. Die zwanzig (20) in diesem Beispiel ist die Keepalive-Zeit (Standard).

ASA

<#root>

```
securityappliance(config)#
```

```
crypto isakmp nat-traversal 20
```

Die Clients müssen ebenfalls geändert werden, damit dies funktioniert.

Navigieren Sie im Cisco VPN Client **zuVerbindungseinträge**, und **klicken Sie auf Ändern**. Es öffnet sich ein neues Fenster, in dem Sie die Registerkarte Transport auswählen müssen.

Klicken Sie auf dieser Registerkarte **auf Transparentes** Tunneling **aktivieren** und **das** Optionsfeld **IPSec over UDP (NAT/PAT**). Klicken Sie dann auf Save, und testen Sie die Verbindung.

Es ist wichtig, UDP 4500 für NAT-T-, UDP 500- und ESP-Ports durch die Konfiguration einer ACL zuzulassen, da die ASA als NAT-Gerät fungiert.

Weitere Informationen zur ACL-Konfiguration in ASA finden Sie unter Konfigurieren eines IPsec-Tunnels über eine Firewall mit NAT.

Ordnungsgemäßer Verbindungstest

Im Idealfall wird die VPN-Konnektivität von Geräten hinter den Endgeräten getestet, die die Verschlüsselung durchführen. Viele Benutzer testen jedoch die VPN-Konnektivität mit dem Befehl pingauf den Geräten, die die Verschlüsselung durchführen.

Obwohl das Ping für diesen Zweck im Allgemeinen funktioniert, ist es wichtig, dass Sie Ihr Ping von der richtigen Schnittstelle beziehen.

Wenn die Quelle falsch ist, kann es den Anschein haben, dass die VPN-Verbindung ausgefallen ist, wenn sie wirklich funktioniert. Dies ist ein Beispiel:

Krypto-ACL von Router A

```
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
```

Krypto-ACL von Router B

```
access-list 110 permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
```

In dieser Situation muss der PingPing vom internen Netzwerk hinter einem der beiden Router bezogen werden. Dies liegt daran, dass die Krypto-ACLs nur für die Verschlüsselung des Datenverkehrs mit diesen Quelladressen konfiguriert sind.

Die von den externen Schnittstellen der beiden Router eingehenden Anrufe werden nicht verschlüsselt. Verwenden Sie die erweiterten Optionen des Befehls pingim privilegierten EXEC-Modus, um einen Ping von der internen Schnittstelle eines Routers zu beziehen:

<#root>

```
routerA#
ping
Protocol [ip]:
```

```
Target IP address: 192.168.200.10

Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: 192.168.100.1

Type of service [0]:
Set DF bit in IP header? [no]:
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, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:

Packet sent with a source address of 192.168.100.1

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = ½/4 ms
```

Stellen Sie sich vor, die Router in diesem **Diagramm** wurden durch ASA Security Appliances ersetzt. **Theping**, das zum Testen der Konnektivität verwendet wird, kann auch über die interne Schnittstelle mit dem InsideKeyword bezogen werden:

```
<#root>

securityappliance#

ping inside 192.168.200.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Es wird nicht empfohlen, die interne Schnittstelle einer Sicherheits-Appliance mit Ihrem Ping **anzuvisieren**.

Wenn Sie die interne Schnittstelle mit **Ihrem Ping** als Ziel festlegen müssen, müssen Sie den **Management**-Zugriff für diese Schnittstelle **aktivieren**, da die Appliance andernfalls nicht antwortet.

```
<#root>

securityappliance(config)#

management-access inside
```

Wenn ein Problem mit der Verbindung besteht, funktioniert auch Phase eins (1) des VPN nicht.

Wenn die Verbindung auf der ASA fehlschlägt, ist die SA-Ausgabe ähnlich wie in diesem Beispiel, das auf eine mögliche falsche Krypto-Peer-Konfiguration und/oder eine falsche ISAKMP-Vorschlagskonfiguration hinweist:

<#root>

```
Router#
```

show crypto isakmp sa

```
1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_WAIT_MSG2
```

Der Status kann zwischen **MM_WAIT_MSG2** und **MM_WAIT_MSG5** liegen, was bedeutet, dass der betreffende Statusaustausch im **Hauptmodus (MM)** fehlschlägt.

Die Ausgabe von **Crypto SA** bei eingeschalteter Phase 1 ähnelt diesem Beispiel:

<#root>

```
Router#
```

show crypto isakmp sa

```
1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

Aktivieren von ISAKMP

Wenn es keinen Hinweis darauf gibt, dass ein IPsec-VPN-Tunnel funktioniert, wurde ISAKMP möglicherweise nicht aktiviert. Stellen Sie sicher, dass Sie ISAKMP auf Ihren Geräten aktiviert haben.

Verwenden Sie einen der folgenden Befehle, um ISAKMP auf Ihren Geräten zu aktivieren:

Cisco IOS®

<#root>

```
router(config)#
```

crypto isakmp enable

Cisco ASA (ersetzt durch die gewünschte Benutzeroberfläche)

<#root>

```
securityappliance(config)#
```

crypto isakmp enable outside

Sie können auch folgenden Fehler erhalten, wenn Sie ISAKMP auf der externen Schnittstelle aktivieren:

```
UDP: ERROR - socket <unknown> 62465 in used
ERROR: IkeReceiverInit, unable to bind to port
```

Die Ursache des Fehlers kann darin bestehen, dass der Client hinter der ASA PAT an den UDP-Port 500 überträgt, bevor isakmp auf der Schnittstelle aktiviert werden kann. Sobald die PAT-Übersetzung entfernt wurde (clear xlate), kann ISAKMP aktiviert werden.

Stellen Sie sicher, dass die UDP 500- und 4500-Portnummern für die Aushandlung von ISAKMP-Verbindungen mit dem Peer reserviert sind.

Wenn ISAKMP auf der Schnittstelle nicht aktiviert ist, zeigt der VPN-Client eine Fehlermeldung ähnlich der folgenden an:

```
Secure VPN connection terminated locally by client.
Reason 412: The remote peer is no longer responding
```

Um diesen Fehler zu beheben, aktivieren Sie ISAKMP auf der Kryptografieschnittstelle des VPN-Gateways.

Aktivieren/Deaktivieren von PFS

Bei IPsec-Verhandlungen stellt Perfect Forward Secrecy (PFS) sicher, dass jeder neue kryptografische Schlüssel unabhängig von einem vorherigen Schlüssel ist.

Aktivieren oder deaktivieren Sie PFS auf beiden Tunnel-Peers. Andernfalls wird der LAN-to-LAN (L2L) IPsec-Tunnel auf dem ASA-/Cisco IOS®-Router nicht eingerichtet.

Perfect Forward Secrecy (PFS) ist ein proprietäres System von Cisco und wird auf Geräten von Drittanbietern nicht unterstützt.

ASA:

PFS ist standardmäßig deaktiviert. Um PFS zu aktivieren, verwenden Sie den Befehl epfsmit dem Schlüsselwort enable im Konfigurationsmodus für Gruppenrichtlinien. Um PFS zu deaktivieren, geben Sie das Schlüsselwort â€ždisableâ€œ ein.

<#root>

```
hostname(config-group-policy)#
```

pfs {enable | disable}

Um das PFS-Attribut aus der Konfiguration zu entfernen, geben Sie die Form **no** dieses Befehls ein.

Eine Gruppenrichtlinie kann einen Wert für PFS von einer anderen Gruppenrichtlinie erben. Geben Sie die Form **no** dieses Befehls ein, um die Übertragung eines Werts zu verhindern.

<#root>

```
hostname(config-group-policy)#
```

no pfs

Cisco IOS® Router:

Um anzugeben, dass IPsec PFS anfordern muss, wenn neue **Sicherheitszuordnungen** für diesen Crypto Map-Eintrag angefordert werden, verwenden Sie den Befehl **set** pfsim Konfigurationsmodus für die Crypto Map.

Um festzulegen, dass IPsec PFS benötigt, wenn es Anforderungen für neue **Sicherheitszuordnungen** empfängt, verwenden Sie **den Befehl set** pfsim Konfigurationsmodus für die Kryptografiezuordnung.

Um anzugeben, dass IPsec kein PFS anfordern darf, verwenden Sie â€žnoâ€œ-Form des Befehls. Standardmäßig wird PFS nicht angefordert. Wenn mit diesem Befehl keine Gruppe angegeben wird, wird group1 als Standardwert verwendet.

```
set pfs [group1 | group2]
no set pfs
```

Für den Befehl set pfs:

- group1: Gibt an, dass IPsec die Diffie-Hellman-Primzahlmodulgruppe mit 768 Bit verwenden muss, wenn der neue Diffie-Hellman-Austausch durchgeführt wird.
- group2: Gibt an, dass IPsec die Diffie-Hellman-Primzahlmodulgruppe mit 1024 Bit verwenden muss, wenn der neue Diffie-Hellman-Austausch durchgeführt wird.

Beispiel:

<#root>

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#
```

set pfs group2

Alte oder aktuelle Sicherheitszuordnungen (Tunnel) löschen

Wenn diese Fehlermeldung auf dem Cisco IOS®®-Router auftritt, besteht das Problem darin, dass die SA entweder abgelaufen ist oder gelöscht wurde.

Das Remote-Tunnel-Endgerät weiß nicht, dass es die abgelaufene Sicherheitszuordnung verwendet, um ein Paket zu senden (kein SA-Aufbaupaket).

Wenn eine neue Sicherheitszuordnung eingerichtet wurde, wird die Kommunikation fortgesetzt. Initiieren

Sie also den interessanten Datenverkehr über den Tunnel, um eine neue Sicherheitszuordnung zu erstellen und den Tunnel neu aufzubauen.

<#root>

%CRYPTO-4-IKMP_NO_SA: IKE message from x.x.x.x has no SA

Wenn Sie die Sicherheitszuordnungen für ISAKMP (Phase I) und IPsec (Phase II) löschen, ist dies die einfachste und häufig beste Lösung zur Lösung von IPsec-VPN-Problemen.

Wenn Sie Sicherheitszuordnungen löschen, können Sie häufig eine Vielzahl von Fehlermeldungen und seltsamen Verhaltensweisen beheben, ohne dass eine Fehlerbehebung erforderlich ist.

Diese Technik kann zwar problemlos in jeder Situation verwendet werden, es ist jedoch fast immer erforderlich, Sicherheitszuordnungen zu löschen, nachdem Sie eine aktuelle IPsec-VPN-Konfiguration geändert oder hinzugefügt haben.

Darüber hinaus ist es zwar möglich, nur bestimmte Sicherheitszuordnungen zu löschen, aber der größte Nutzen kann durch das globale Löschen von Sicherheitszuordnungen auf dem Gerät erzielt werden.

Sobald die Sicherheitszuordnungen gelöscht wurden, kann es erforderlich sein, Datenverkehr über den Tunnel zu senden, um diese wiederherzustellen.

Warnung: Wenn Sie nicht angeben, welche Sicherheitszuordnungen gelöscht werden sollen, können die hier aufgeführten Befehle alle Sicherheitszuordnungen auf dem Gerät löschen. Gehen Sie vorsichtig vor, wenn andere IPsec-VPN-Tunnel verwendet werden.

1. Sehen Sie sich die Sicherheitszuordnungen an, bevor Sie sie löschen

    a. **Cisco IOS®**

    <#root>

    router#

    show crypto isakmp sa

    router#

    show crypto ipsec sa

    b. **Cisco ASA Security Appliances**

    <#root>

    securityappliance#

    show crypto isakmp sa

    securityappliance#

    show crypto ipsec sa

2. Löschen Sie die Sicherheitszuordnungen. Jeder Befehl kann wie fett dargestellt oder mit den angezeigten Optionen eingegeben werden.

a. **Cisco IOS®**

a. **ISAKMP (Phase I)**

<#root>

```
router#
clear crypto isakmp
 ?
  <0 - 32766>  connection id of SA
  <cr>
```

b. **IPsec (Phase II)**

<#root>

```
router#
clear crypto sa
 ?
  counters  Reset the SA counters
  map       Clear all SAs for a given crypto map
  peer      Clear all SAs for a given crypto peer
  spi       Clear SA by SPI
  <cr>
```

b. **Cisco ASA Security Appliances**

a. **ISAKMP (Phase I)**

<#root>

```
securityappliance#
clear crypto isakmp sa
```

b. **IPsec (Phase II)**

<#root>

```
security appliance#
clear crypto ipsec sa
 ?
```

```
counters  Clear IPsec SA counters
entry     Clear IPsec SAs by entry
map       Clear IPsec SAs by map
peer      Clear IPsec SA by peer
<cr>
```

Überprüfen der ISAKMP-Lebensdauer

Wenn Benutzer häufig über den L2L-Tunnel getrennt werden, kann das Problem die geringere Lebensdauer sein, die in der ISAKMP-Sicherheitszuordnung konfiguriert ist.

Wenn während der ISAKMP-Lebensdauer eine Diskrepanz auftritt, können Sie den %**ASA-5-713092: Group = x.x.x.x, IP = x.x.x.x, Failure during phase 1 rekey try due to** collisionerror message in /ASA empfangen.

Der Standardwert ist 86400 Sekunden (24 Stunden). In der Regel bietet eine kürzere Lebensdauer sicherere ISAKMP-Verhandlungen (bis zu einem bestimmten Punkt), aber mit einer kürzeren Lebensdauer richtet die Security-Appliance zukünftige IPsec-Sicherheitszuordnungen schneller ein.

Eine Übereinstimmung wird hergestellt, wenn beide Richtlinien der beiden Peers dieselben Werte für Verschlüsselung, Hash, Authentifizierung und Diffie-Hellman-Parameter enthalten und wenn die Richtlinie des Remote-Peers eine Lebensdauer angibt, die kleiner oder gleich der Lebensdauer in der verglichenen Richtlinie ist.

Wenn die Lebensdauern nicht identisch sind, wird die kürzere Lebensdauer â€“ gemäß der Richtlinie der Remote-Gegenstelle â€“ verwendet. Wenn keine akzeptable Übereinstimmung gefunden wird, lehnt die IKE die Aushandlung ab, und die IKE-Sicherheitszuordnung wird nicht eingerichtet.

Geben Sie die Lebensdauer der Sicherheitszuordnung an. In diesem Beispiel wird eine Lebensdauer von 4 Stunden (14400 Sekunden) festgelegt. Der Standardwert ist 86400 Sekunden (24 Stunden).

ASA

<#root>

```
hostname(config)#
```

isakmp policy 2 lifetime 14400

Cisco IOS® Router

<#root>

```
R2(config)#
```

crypto isakmp policy 10

```
R2(config-isakmp)#
```

lifetime 86400

Wenn die maximale konfigurierte Lebensdauer überschritten wird, wird beim Beenden der VPN-Verbindung folgende Fehlermeldung angezeigt:

Secure VPN Connection terminated locally by the Client. Grund 426: Die konfigurierte maximale Lebensdauer wurde überschritten.

Um diese Fehlermeldung zu beheben, setzen Sie denLifetimevalue auf null (0), um die Lebensdauer einer IKE-Sicherheitszuordnung auf unendlich zu setzen. Das VPN ist immer verbunden und wird nicht beendet.

```
hostname(config)#isakmp policy 2 lifetime 0
```

Sie können auch **die erneute Auslieferung in der Gruppenrichtlinie deaktivieren**, um das Problem zu beheben.

Aktivieren oder Deaktivieren von ISAKMP Keepalives

Wenn Sie ISAKMP-Keepalives konfigurieren, wird verhindert, dass LAN-zu-LAN- oder RAS-VPNs sporadisch verworfen werden. Dies umfasst auch VPN-Clients, Tunnel und die nach einer Zeit der Inaktivität verworfenen Tunnel.

Mit dieser Funktion kann der Tunnel-Endpunkt die fortlaufende Anwesenheit eines Remote-Peers überwachen und seine eigene Anwesenheit diesem Peer melden.

Wenn der Peer nicht mehr reagiert, trennt der Endpunkt die Verbindung.

Damit ISAKMP-Keepalives funktionieren, müssen beide VPN-Endpunkte diese unterstützen.

Konfigurieren Sie ISAKMP-Keepalives in Cisco IOS® mit dem folgenden Befehl:

<#root>

```
router(config)#
```

```
crypto isakmp keepalive 15
```

Verwenden Sie diese Befehle, um ISAKMP-Keepalives auf den **ASA Security Appliances** zu konfigurieren:

Cisco ASA für die Tunnelgruppe mit der Bezeichnung**10.165.205.222**

<#root>

```
securityappliance(config)#
```

```
tunnel-group 10.165.205.222
   ipsec-attributes
```

```
securityappliance(config-tunnel-ipsec)#
```

```
isakmp keepalive
   threshold 15 retry 10
```

In einigen Fällen müssen Sie diese Funktion deaktivieren, um das Problem zu beheben, z. B. wenn sich der VPN-Client hinter einer Firewall befindet, die DPD-Pakete verhindert.

Cisco ASA, für die Tunnel-Gruppe mit der Bezeichnung**10.165.205.222**

Deaktivieren Sie die IKE-Keepalive-Verarbeitung, die standardmäßig aktiviert ist.

```
<#root>

securityappliance(config)#

tunnel-group 10.165.205.222
   ipsec-attributes


securityappliance(config-tunnel-ipsec)#

isakmp keepalive


disable
```

Deaktivieren Sie Keepalive für Cisco VPN Client 4.x

Navigieren Sie zu %**System Root% > Program Files > Cisco Systems > VPN Client > Profilesauf** dem Client-PC, auf dem das Problem auftritt, um IKE Keepalive zu deaktivieren, und bearbeiten Sie ggf. **die PCF-Datei** für die Verbindung.

Ändern Sie **ForceKeepAlives=0** (Standard**) in ForceKeepAlives=1**.

Keepalives sind proprietäre Produkte von Cisco und werden nicht von Drittanbietergeräten unterstützt.

Erneute Eingabe oder Wiederherstellung von Pre-Shared-Keys

In vielen Fällen kann ein einfacher Tippfehler schuld sein, wenn ein IPsec VPN-Tunnel nicht funktioniert. Auf der Security-Appliance werden beispielsweise Pre-Shared Keys verborgen, sobald sie eingegeben wurden.

Diese Verschleierung macht es unmöglich zu erkennen, ob eine Taste falsch ist. Vergewissern Sie sich, dass Sie alle Pre-Shared Keys auf jedem VPN-Endpunkt korrekt eingegeben haben.

Geben Sie einen Schlüssel erneut ein, um sicherzustellen, dass er korrekt ist. Dies ist eine einfache Lösung, mit der Sie eine gründliche Fehlerbehebung vermeiden können.

Überprüfen Sie in Remote Access VPN, ob der gültige Gruppenname und der Pre-Shared Key im Cisco VPN Client eingegeben wurden.

Dieser Fehler tritt auf, wenn der Gruppenname oder der vorinstallierte Schlüssel nicht zwischen dem VPN-Client und dem Headend-Gerät übereinstimmen.

```
 1 12:41:51.900 02/18/06 Sev=Warning/3 IKE/0xE3000056
 The received HASH payload cannot be verified
 2 12:41:51.900 02/18/06 Sev=Warning/2 IKE/0xE300007D
Hash verification failed
3      14:37:50.562  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
4      14:37:50.593  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
5      14:44:15.937  10/05/06  Sev=Warning/2 IKE/0xA3000067
Received Unexpected InitialContact Notify (PLMgrNotify:888)
6      14:44:36.578  10/05/06  Sev=Warning/3 IKE/0xE3000056
The received HASH payload cannot be verified
7      14:44:36.593  10/05/06  Sev=Warning/2 IKE/0xE300007D
Hash verification failed... possibly be configured with invalid group password.
8      14:44:36.609  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
9      14:44:36.640  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
```

Warnung: Wenn Sie krypto-bezogene Befehle entfernen, führt dies wahrscheinlich zum Ausfall eines oder aller Ihrer VPN-Tunnel. Verwenden Sie diese Befehle mit Vorsicht, und lesen Sie die Änderungskontrollrichtlinie Ihres Unternehmens, bevor Sie kryptographische Befehle entfernen.

Verwenden Sie diese Befehle, um den pre-shared-keysecretkey für den Peer10.**0.0.1**oder die groupVPNgroupin Cisco IOS® zu entfernen und erneut einzugeben:

Cisco LAN-zu-LAN-VPN

<#root>

```
router(config)#
```

no crypto isakmp key secretkey
address 10.0.0.1

```
router(config)#
```

crypto isakmp key secretkey
address 10.0.0.1

Cisco Remote Access-VPN

<#root>

```
router(config)#
```

crypto isakmp client configuration
group vpngroup

```
router(config-isakmp-group)#
```

no key secretkey

```
router(config-isakmp-group)#
```

key secretkey

Verwenden Sie diese Befehle, um den pre-shared-keysecretkey für den Peer10.**0.0.1**auf /ASA Security Appliances zu entfernen und erneut einzugeben:

Cisco 6.x

<#root>

```
(config)#
```

```
no isakmp key secretkey address 10.0.0.1
```

```
(config)#
```

```
isakmp key secretkey address 10.0.0.1
```

Cisco /ASA 7.x und höher

<#root>

```
securityappliance(config)#
```

```
tunnel-group 10.0.0.1
   ipsec-attributes
```

```
securityappliance(config-tunnel-ipsec)#
```

```
no ikev1 pre-shared-key
```

```
securityappliance(config-tunnel-ipsec)#
```

```
ikev1
```

```
pre-shared-key
   secretkey
```

Nicht übereinstimmender Pre-Shared Key

Die Initiierung des VPN-Tunnels wird getrennt. Dieses Problem tritt auf, weil der Pre-Shared Key während der Phase-I-Verhandlungen falsch zugeordnet wurde.

Die Nachricht **MM_WAIT_MSG_6** im Befehl **crypto isakmp** gibt einen falsch zugeordneten Pre-Shared Key an, wie in diesem Beispiel gezeigt:

<#root>

```
ASA#
```

```
show crypto isakmp sa
```

```
Active SA: 1
Rekey SA: 0 (A tunnel reports 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

```
1         IKE Peer: 10.7.13.20
             Type : L2L                                Role : initiator
             Rekey : no                                State :

MM_WAIT_MSG_6
```

Um dieses Problem zu beheben, geben Sie den vorinstallierten Schlüssel in beiden Appliances erneut ein. Der vorinstallierte Schlüssel muss eindeutig und zugeordnet sein. Weitere Informationen finden Sie unter Vorinstallierte Schlüssel erneut eingeben oder wiederherstellen.

Entfernen und erneutes Anwenden von Krypto-Zuordnungen

Wenn Sie Sicherheitszuordnungen löschen und ein IPsec-VPN-Problem nicht lösen, entfernen Sie die entsprechende Crypto Map, und wenden Sie sie erneut an, um eine Vielzahl von Problemen zu beheben, zu denen das zeitweilige Verwerfen des VPN-Tunnels und das Ausfallen einiger VPN-Standorte gehören.

Warnung: Wenn Sie eine Crypto Map von einer Schnittstelle entfernen, werden alle dieser Crypto Map zugeordneten IPsec-Tunnel deaktiviert. Gehen Sie vorsichtig mit diesen Schritten vor, und berücksichtigen Sie die Änderungskontrollrichtlinie Ihres Unternehmens, bevor Sie fortfahren.

Verwenden Sie diese Befehle, um eine Crypto Map in Cisco IOS® zu entfernen und zu ersetzen:

Beginnen Sie mit dem Entfernen der Krypto-Zuordnung von der Schnittstelle. Verwenden Sie die Form no des Befehls **crypto** map.

```
<#root>

router(config-if)#

no crypto map mymap
```

Verwenden Sie weiterhin das Formular, um eine vollständige Crypto Map zu entfernen.

```
<#root>

router(config)#

no crypto map mymap 10
```

Ersetzen Sie die Krypto-Zuordnung auf der Schnittstelle Ethernet0/0 für den Peer 10.0.0.1. Dieses Beispiel zeigt die mindestens erforderliche Konfiguration der Krypto-Zuordnung:

```
<#root>

router(config)#

crypto map mymap 10 ipsec-isakmp

router(config-crypto-map)#

match address 101
```

```
router(config-crypto-map)#
set transform-set mySET
router(config-crypto-map)#
set peer 10.0.0.1
router(config-crypto-map)#
exit
router(config)#
interface ethernet0/0
router(config-if)#
crypto map mymap
```

Verwenden Sie diese Befehle, um eine Crypto Map auf der ASA zu entfernen und zu ersetzen:

Beginnen Sie mit dem Entfernen der Krypto-Zuordnung von der Schnittstelle. Verwenden Sie die Form no des Befehls **crypto** map.

```
<#root>
securityappliance(config)#
no crypto map mymap interface outside
```

Fahren Sie mit dem Entfernen der anderen Crypto Map-Befehle fort.

```
<#root>
securityappliance(config)#
no crypto map mymap 10 match
   address 101
securityappliance(config)#
no crypto map mymap set
   transform-set mySET
securityappliance(config)#
no crypto map mymap set
   peer 10.0.0.1
```

Ersetzen Sie die Krypto-Zuordnung für den Peer 10.0.0.1. Dieses Beispiel zeigt die mindestens erforderliche Konfiguration der Krypto-Zuordnung:

```
<#root>
securityappliance(config)#
```

```
crypto map mymap 10 ipsec-isakmp

securityappliance(config)#

crypto map mymap 10
   match address 101

securityappliance(config)#

crypto map mymap 10 set
   transform-set mySET

securityappliance(config)#

crypto map mymap 10 set
   peer 10.0.0.1

securityappliance(config)#

crypto map mymap interface outside
```

Wenn Sie die Crypto Map entfernen und erneut anwenden, wird auch das Verbindungsproblem behoben, wenn die IP-Adresse des Headends geändert wurde.

Stellen Sie sicher, dass sysopt-Befehle vorhanden sind (nur ASA).

Der Befehl **sysopt connection permit-ipsecandsysopt connection permit-**vpnallow-Pakete aus einem IPsec-Tunnel und deren Payloads, um die Schnittstellen-ACLs auf der Sicherheits-Appliance zu umgehen.

IPsec-Tunnel, die auf der Security-Appliance terminiert sind, fallen wahrscheinlich aus, wenn einer dieser Befehle nicht aktiviert ist.

In Security Appliance Software Version 7.0 und früher lautet der entsprechende Befehl sysopt für diese Situation **issysopt connection permit-ipsec**.

In Security Appliance Software Version 7.1(1) und höher lautet der entsprechende Befehl sysopt für diese Situation **issysopt connection permit-vpn**.

In 6.x ist diese Funktion standardmäßig deaktiviert. Bei /ASA 7.0(1) und höheren Versionen ist diese Funktion standardmäßig aktiviert. Verwenden Sie diese Befehle zum Anzeigen, um festzustellen, ob der entsprechendeSystemsoptbefehl auf Ihrem Gerät aktiviert ist:

Cisco ASA

<#root>

```
securityappliance#

show running-config all sysopt

no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret

sysopt connection permit-vpn
```

```
!--- sysopt connection permit-vpn is enabled !--- This device is running 7.2(2)
```

Verwenden Sie die folgenden Befehle, um den Befehl correctSysoptfür Ihr Gerät zu aktivieren:

Cisco ASA

<#root>

```
securityappliance(config)#
```

sysopt connection permit-vpn

Wenn Sie den Befehl **ysopt** connection nicht verwenden möchten, lassen Sie den erforderlichen interessanten Datenverkehr explizit von der Quelle zum Ziel zu.

Beispiel: Von Remote zu lokalem LAN des Remote-Geräts und "UDP-Port 500" für externe Schnittstelle des Remote-Geräts zu externer Schnittstelle des lokalen Geräts in externer ACL.

Überprüfen der ISAKMP-Identität

Wenn der IPsec-VPN-Tunnel innerhalb der IKE-Aushandlung ausgefallen ist, kann der Fehler entweder auf die oder die Unfähigkeit des Peers zurückzuführen sein, die Identität des Peers zu erkennen.

Wenn zwei Peers IKE verwenden, um IPsec-Sicherheitszuordnungen herzustellen, sendet jeder Peer seine ISAKMP-Identität an den Remote-Peer.

Er sendet entweder seine IP-Adresse oder seinen Hostnamen, je nachdem, wie jede ISAKMP-Identität festgelegt ist.

Standardmäßig ist die ISAKMP-Identität der Firewall-Einheit auf die IP-Adresse festgelegt.

In der Regel sollten Sie die Security-Appliance und die Identitäten der Peers auf die gleiche Weise festlegen, um einen IKE-Aushandlungsfehler zu vermeiden.

Um die an den Peer zu sendende Phase-2-ID festzulegen, verwenden Sie den Befehl **eisakmp** identity im globalen Konfigurationsmodus.

```
crypto isakmp identity address

!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with pre-shared key as authentication type
```

ODER

```
crypto isakmp identity auto
```

```
!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with ISAKMP negotiation by connection type
```

ODER

```
crypto isakmp identity hostname

!--- Uses the fully-qualified domain name of !--- the host exchange ISAKMP identity information (default
```

Nach einer Verlagerung der Konfiguration von auf ASA mit dem ASA-Konfigurations-Migrations-Tool kommt der VPN-Tunnel nicht zum Einsatz. Die folgenden Meldungen werden im Protokoll angezeigt:

[IKEv1]: Gruppe = x.x.x.x, IP = x.x.x.x, Stale PeerTblEntry gefunden, wird entfernt!

[IKEv1]: Gruppe = x.x.x.x, IP = x.x.x.x, Entfernen des Peers aus der Korrelatortabelle fehlgeschlagen, keine Übereinstimmung!

[IKEv1]: Gruppe = x.x.x.x, IP = x.x.x.x, construct_ipsec_delete(): Kein SPI zur Identifizierung von Phase 2 SA!

[IKEv1]: Gruppe = x.x.x.x, IP = x.x.x.x, Entfernen des Peers aus der Korrelatortabelle fehlgeschlagen, keine Übereinstimmung!

Überprüfen des Leerlauf-/Sitzungs-Timeouts

Wenn der Leerlauf-Timeout auf 30 Minuten (Standard) festgelegt ist, bedeutet dies, dass der Tunnel nach 30 Minuten ohne Datenverkehr verworfen wird.

Die Verbindung des VPN-Clients wird nach 30 Minuten getrennt, unabhängig vom Timeout-Parameter bei Inaktivität, und es wird **der Fehler PEER_DELETE-IKE_DELETE**_UNSPECIFIED festgestellt.

Konfigurieren Sie die Zeitüberschreitung und die Sitzungszeitüberschreitung so, dass der Tunnel **immer unterstützt wird**, sodass der Tunnel nie verworfen wird, auch wenn Geräte von Drittanbietern verwendet werden.

ASA

Geben Sie den Befehl **vpn-idle-**timeout im Konfigurationsmodus für Gruppenrichtlinien oder im Konfigurationsmodus für den Benutzernamen ein, um die Zeitüberschreitung für den Benutzer zu konfigurieren:

<#root>

```
hostname(config)#
```

group-policy DfltGrpPolicy attributes

```
hostname(config-group-policy)#
```

vpn-idle-timeout none

Konfigurieren Sie mit dem Befehl **vpn-session-**timeout im Konfigurationsmodus für Gruppenrichtlinien oder im Konfigurationsmodus für Benutzernamen die maximale Dauer für VPN-Verbindungen:

<#root>

```
hostname(config)#
```

```
group-policy DfltGrpPolicy attributes
```

```
hostname(config-group-policy)#
```

```
vpn-session-timeout none
```

Wenn Sie **unnel-**all konfiguriert haben, müssen Sie **configure-**timeout nicht konfigurieren, denn selbst wenn Sie VPN-idle-Timeout konfigurieren, funktioniert es nicht, da der gesamte Datenverkehr durch den Tunnel fließt (da tunnel-all konfiguriert ist).

Daher ist der interessante Datenverkehr (oder sogar der vom PC generierte Datenverkehr) interessant und lässt keine Idle-Timeout-Funktion zu.

Cisco IOS® Router

Verwenden Sie **den Befehl rypto ipsec security-association idle-**timecim globalen Konfigurationsmodus oder crypto map configuration mode, um den IPsec-SA idle-Timer zu konfigurieren.

IPsec-Leerlaufzeitgeber für Sicherheitszuordnungen sind standardmäßig deaktiviert.

<#root>

```
crypto ipsec security-association idle-time
```

```
seconds
```

Die Zeit wird in Sekunden gemessen, nach deren Ablauf der Inaktivitäts-Timer einem inaktiven Peer die Aufrechterhaltung einer Sicherheitszuordnung ermöglicht. Gültige Werte für das Sekunden-Argument liegen zwischen 60 und 86400.

Überprüfen, ob die ACLs korrekt und an die Krypto-Zuordnung gebunden sind

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 definiert, welchen Datenverkehr verschlüsselt werden soll. Dazu gehört eine Krypto-ACL in einer LAN-zu-LAN-Konfiguration oder eine Split-Tunnel-ACL in einer RAS-Konfiguration.

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

Binden Sie die Krypto-ACL mit der Crypto Map mit dem Befehl **crypto map match address** im globalen Konfigurationsmodus an.

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

Die folgende Liste enthält einfache Dinge, die Sie überprüfen sollten, 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.

Stellen Sie sicher, dass Ihr Gerät für die Verwendung der NAT-Ausnahme-ACL konfiguriert ist. Auf einem Router bedeutet dies, dass Sie den Befehl **route-**map verwenden.

Auf der ASA bedeutet dies, dass Sie den Befehl **at (0)**verwenden. Eine NAT-Ausnahme-ACL ist für LAN-zu-LAN- und RAS-Konfigurationen erforderlich.

Hier ist ein Cisco IOS®-Router so konfiguriert, dass er Datenverkehr ausnimmt, der zwischen **192.168.100.0 /24** und **192.168.200.0 /24**oder **192.168.1.0 /2** gesendet wird. 4 von NAT. Datenverkehr, der für einen anderen Standort bestimmt ist, unterliegt NAT-Overload:

```
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.1.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255 any

route-map nonat permit 10
  match ip address 110

ip nat inside source route-map nonat interface FastEthernet0/0 overload
```

NAT-Befreiungszugriffskontrolllisten funktionieren nur mit der IP-Adresse oder den IP-Netzwerken, wie in den oben genannten Beispielen (Zugriffsliste noNAT), und müssen mit den Crypto Map-Zugriffskontrolllisten identisch sein.

Die Zugriffskontrolllisten für die NAT-Ausnahme funktionieren nicht mit den Portnummern (z. B. 23, 25 usw.).

In einer VoIP-Umgebung, in der die Sprachanrufe zwischen Netzwerken über das VPN übertragen werden, funktionieren die Sprachanrufe nicht, wenn die NAT 0-ACLs nicht ordnungsgemäß konfiguriert sind.

Vor der Fehlerbehebung wird empfohlen, den VPN-Verbindungsstatus zu überprüfen, da das Problem bei einer falschen Konfiguration von NAT-ausgenommenen ACLs auftreten kann.

Die Fehlermeldung wird angezeigt, wenn bei den Zugriffskontrolllisten für die NAT-Ausnahme (NAT 0) eine Fehlkonfiguration vorliegt.

```
%ASA-3-305005: No translation group found for
udp src Outside:x.x.x.x/p dst Inside:y.y.y.y/p
```

Falsches Beispiel:

<#root>

```
access-list noNAT extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
```

eq 25

Wenn die NAT-Ausnahme (NAT 0) nicht funktioniert, versuchen Sie, sie zu entfernen, und geben Sie **den NAT 0**-Befehl aus, damit sie funktioniert.

Stellen Sie sicher, dass Ihre ACLs nicht rückwärts sind und dass sie den richtigen Typ haben.

Krypto- und NAT-Ausnahme-ACLs für LAN-zu-LAN-Konfigurationen müssen aus der Perspektive des Geräts geschrieben sein, auf dem die ACL konfiguriert ist.

Das bedeutet, dass die ACLs einander spiegeln müssen. In diesem Beispiel wird ein LAN-zu-LAN-Tunnel zwischen **192.168.100.0 /24** und **192.168.200.0 /24** eingerichtet.

Krypto-ACL von Router A

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
```

Krypto-ACL von Router B

```
access-list 110 permit ip 192.168.200.0 0.0.0.255
   192.168.100.0 0.0.0.255
```

Das Konzept ist hier zwar nicht abgebildet, bezieht sich jedoch auf die ASA Security Appliances.

Bei ASA müssen Split-Tunnel-ACLs für Remote-Zugriffskonfigurationen Standard-Zugriffslisten sein, die Datenverkehr zu dem Netzwerk zulassen, auf das die VPN-Clients Zugriff benötigen.

Cisco IOS® Router können erweiterte ACLs für Split-Tunnel verwenden. In der erweiterten Zugriffsliste ist die Verwendung von**'any'**an der Quelle in der Split-Tunnel-ACL ähnlich wie die Deaktivierung des Split-Tunnels.

Verwenden Sie für Split-Tunnel nur die Quellnetzwerke in der erweiterten ACL.

Richtiges Beispiel:

<#root>

```
access-list 140 permit ip
```

10.1.0.0 0.0.255.255

```
 10.18.0.0 0.0.255.255
```

Falsches Beispiel:

<#root>

```
access-list 140 permit ip
```

```
any
```

```
 10.18.0.0 0.0.255.255
```

Cisco IOS®

<#root>

```
router(config)#
```

```
access-list 10 permit ip 192.168.100.0
```

```
router(config)#
```

```
crypto isakmp client configuration group MYGROUP
```

```
router(config-isakmp-group)#
```

```
acl 10
```

Cisco ASA

<#root>

```
securityappliance(config)#
```

```
access-list 10 standard
   permit 192.168.100.0 255.255.255.0
```

```
securityappliance(config)#
```

```
group-policy MYPOLICY internal
```

```
securityappliance(config)#
```

```
group-policy MYPOLICY attributes
```

```
securityappliance(config-group-policy)#
```

```
split-tunnel-policy
   tunnelspecified
```

```
securityappliance(config-group-policy)#
```

```
split-tunnel-network-list
   value 10
```

NAT-Ausnahme-Konfiguration in ASA-Version 8.3 für Site-to-Site-VPN-Tunnel:

Zwischen HOASA und BOASA muss mit beiden ASAs mit Version 8.3 ein Site-to-Site-VPN eingerichtet werden. Die NAT-Ausnahme-Konfiguration auf HOASA sieht ungefähr so aus:

```
object network obj-local
subnet 192.168.100.0 255.255.255.0
object network obj-remote
subnet 192.168.200.0 255.255.255.0
nat (inside,outside) 1 source static obj-local obj-local destination static obj-remote objremote
```

Überprüfen der ISAKMP-Richtlinien

Wenn der IPsec-Tunnel nicht aktiv ist, überprüfen Sie, ob die ISAKMP-Richtlinien mit den Remote-Peers übereinstimmen. Diese ISAKMP-Richtlinie gilt sowohl für das Site-to-Site- (L2L-) als auch für das Remote-IPsec-VPN.

Wenn die Cisco VPN-Clients oder das Site-to-Site-VPN den Tunnel mit dem Remote-Endgerät nicht herstellen können, stellen Sie sicher, **dass die beiden Peers die gleichen Werte für Verschlüsselung, Hash, Authentifizierung und Diffie-Hellman-Parameter enthalten.**

Überprüfen Sie, ob die Remote-Peer-Richtlinie eine Lebensdauer angibt, die kleiner oder gleich der Lebensdauer in der Richtlinie ist, die der Initiator gesendet hat.

Wenn die Lebensdauern nicht identisch sind, verwendet die Security-Appliance die kürzere Lebensdauer. Wenn keine akzeptable Übereinstimmung vorhanden ist, lehnt ISAKMP die Aushandlung ab, und die Sicherheitszuordnung wird nicht eingerichtet.

```
"Error: Unable to remove Peer TblEntry, Removing peer from peer table
failed, no match!"
```

Die ausführliche Protokollmeldung sieht so aus:

```
4|Mar 24 2010 10:21:50|713903: IP = X.X.X.X, Error: Unable to remove PeerTblEntry
3|Mar 24 2010 10:21:50|713902: IP = X.X.X.X, Removing peer from peer table failed,
no match!
3|Mar 24 2010 10:21:50|713048: IP = X.X.X.X, Error processing payload: Payload ID: 1
4|Mar 24 2010 10:21:49|713903: IP = X.X.X.X, Information Exchange processing failed
5|Mar 24 2010 10:21:49|713904: IP = X.X.X.X, Received an un-encrypted
NO_PROPOSAL_CHOSEN notify message, drop
```

Diese Meldung wird in der Regel aufgrund falsch übereinstimmender ISAKMP-Richtlinien oder einer fehlenden NAT 0-Anweisung angezeigt.

Darüber hinaus wird folgende Meldung angezeigt:

```
Error Message    %ASA-6-713219: Queueing KEY-ACQUIRE messages to be processed when
P1 SA is complete.
```

Diese Meldung zeigt an, dass sich Phase-2-Nachrichten nach Abschluss von Phase 1 in der Warteschlange befinden. Diese Fehlermeldung ist auf einen der folgenden Gründe zurückzuführen:

- Nicht übereinstimmende Phase auf einem der Peers
- ACL blockiert die Peers vor Abschluss von Phase 1

Diese Meldung wird in der Regel angezeigt, nachdem **`die Meldung Removing peer from peer table failed, no match!`**error (Peer aus Peertabelle entfernen) **`fehlgeschlagen`** ist.

Wenn der Cisco VPN-Client keine Verbindung zum Headend-Gerät herstellen kann, liegt das Problem möglicherweise an der Nichtübereinstimmung der ISAKMP-Richtlinie. Das Headend-Gerät muss mit einem der IKE-Angebote des Cisco VPN Client übereinstimmen.

Für die ISAKMP-Richtlinie und den IPsec-Transformationssatz, die auf der ASA verwendet werden, kann der Cisco VPN-Client keine Richtlinie mit einer Kombination aus DES und SHA verwenden.

Wenn Sie DES verwenden, müssen Sie MD5 für den Hash-Algorithmus verwenden, oder Sie können die anderen Kombinationen verwenden: 3DES mit SHA und 3DES mit MD5.

Überprüfen, ob das Routing korrekt ist

Stellen Sie sicher, dass Ihre Verschlüsselungsgeräte wie Router und ASA Security Appliances über die richtigen Routing-Informationen zum Senden von Datenverkehr über den VPN-Tunnel verfügen.

Wenn sich hinter Ihrem Gateway weitere Router befinden, müssen Sie sicherstellen, dass diese Router wissen, wie der Tunnel zu erreichen ist und welche Netzwerke sich auf der anderen Seite befinden.

Eine wichtige Komponente des Routings in einer VPN-Bereitstellung ist Reverse Route Injection (RRI).

RRI fügt dynamische Einträge für Remote-Netzwerke oder VPN-Clients in die Routing-Tabelle eines VPN-Gateways ein.

Diese Routen sind für das Gerät, auf dem sie installiert sind, sowie für andere Geräte im Netzwerk nützlich, da von RRI installierte Routen über ein Routing-Protokoll wie EIGRP oder OSPF neu verteilt werden können.

In einer LAN-zu-LAN-Konfiguration ist es wichtig, dass jeder Endpunkt eine oder mehrere Routen zu den Netzwerken hat, für die der Datenverkehr verschlüsselt werden soll.

In diesem Beispiel muss Router A Routen zu den Netzwerken hinter Router B über 10.89.129.2 haben. Router B muss eine ähnliche Route wie 192.168.100.0 /24 haben:

Die erste Möglichkeit, um sicherzustellen, dass jeder Router die entsprechenden Routen kennt, besteht darin, statische Routen für jedes Zielnetzwerk zu konfigurieren. Router A kann beispielsweise die folgenden Routenanweisungen konfigurieren:

```
ip route 0.0.0.0 0.0.0.0 172.22.1.1
ip route 192.168.200.0 255.255.255.0 10.89.129.2
ip route 192.168.210.0 255.255.255.0 10.89.129.2
```

```
ip route 192.168.220.0 255.255.255.0 10.89.129.2
ip route 192.168.230.0 255.255.255.0 10.89.129.2
```

Wenn Router A durch eine ASA ersetzt wurde, kann die Konfiguration wie folgt aussehen:

```
route outside 0.0.0.0 0.0.0.0 172.22.1.1
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
```

Wenn hinter jedem Endpunkt eine große Anzahl von Netzwerken vorhanden ist, wird die Aufrechterhaltung der Konfiguration statischer Routen schwierig.

Stattdessen wird empfohlen, dass Sie Reverse Route Injection wie beschrieben verwenden. RRI fügt Routen für alle in der Krypto-ACL aufgeführten Remote-Netzwerke in die Routing-Tabelle ein.

Die Krypto-ACL und die Krypto-Zuordnung von Router A können beispielsweise wie folgt aussehen:

<#root>

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.210.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.220.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.230.0 0.0.0.255

crypto map myMAP 10 ipsec-isakmp
 set peer 10.89.129.2
```

reverse-route

```
 set transform-set mySET
 match address 110
```

Wenn Router A durch eine ASA ersetzt wurde, kann die Konfiguration wie folgt aussehen:

<#root>

```
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.210.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.220.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.230.0 255.255.255.0
```

```
crypto map myMAP 10 match address cryptoACL
crypto map myMAP 10 set peer 10.89.129.2
crypto map myMAP 10 set transform-set mySET
```

`crypto map mymap 10 set reverse-route`

In einer RAS-Konfiguration sind Routing-Änderungen nicht immer erforderlich.

Wenn jedoch weitere Router hinter dem VPN-Gateway-Router oder der Security-Appliance vorhanden sind, müssen diese den Pfad zu den VPN-Clients lernen.

In diesem Beispiel wird davon ausgegangen, dass den VPN-Clients bei der Verbindung Adressen im Bereich von **10.0.0.0 /24** zugewiesen werden.

Wenn zwischen dem Gateway und den anderen Routern kein Routing-Protokoll verwendet wird, können statische Routen auf Routern wie Router 2 verwendet werden:

```
ip route 10.0.0.0 255.255.255.0 192.168.100.1
```

Wenn zwischen dem Gateway und anderen Routern ein Routing-Protokoll wie EIGRP oder OSPF verwendet wird, wird empfohlen, Reverse Route Injection wie beschrieben zu verwenden.

RRI fügt Routen für den VPN-Client automatisch zur Routing-Tabelle des Gateways hinzu. Diese Routen können dann an die anderen Router im Netzwerk verteilt werden.

Cisco IOS® Router:

<#root>

```
crypto dynamic-map dynMAP 10
 set transform-set mySET
```

`reverse-route`

```
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

Cisco ASA Security Appliance:

<#root>

```
crypto dynamic-map dynMAP 10 set transform-set mySET
```

`crypto dynamic-map dynMAP 10 set reverse-route`

```
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

Das Routing-Problem tritt auf, wenn sich der Pool der den VPN-Clients zugewiesenen IP-Adressen mit den

internen Netzwerken des Headend-Geräts überschneidet. Weitere Informationen finden Sie unter Überlappende private Netzwerke .

Überprüfen, ob die Transformationsgruppe korrekt ist

Stellen Sie sicher, dass die IPsec-Verschlüsselungs- und Hash-Algorithmen, die von der Transformationsgruppe an beiden Enden verwendet werden sollen, identisch sind.

Weitere Informationen finden Sie im Abschnitt "Befehlsreferenz" der Cisco Security Appliance-Konfigurationsanleitung.

Für die ISAKMP-Richtlinie und den IPsec-Transformationssatz, die auf der ASA verwendet werden, kann der Cisco VPN-Client keine Richtlinie mit einer Kombination aus DES und SHA verwenden.

Wenn Sie DES verwenden, müssen Sie MD5 für den Hash-Algorithmus verwenden, oder Sie können die anderen Kombinationen verwenden: 3DES mit SHA und 3DES mit MD5.

Überprüfen der Sequenznummern und des Namens der Krypto-Zuordnung sowie der Anwendung der Krypto-Zuordnung in der richtigen Schnittstelle, an der der IPsec-Tunnel beginnt/endet

Wenn statische und dynamische Peers auf derselben Krypto-Zuordnung konfiguriert sind, ist die Reihenfolge der Krypto-Zuordnungseinträge sehr wichtig.

Die Sequenznummer des dynamischen Crypto Map-**Eintrags muss** höher sein als die aller anderen statischen Crypto Map-Einträge.

Wenn die statischen Einträge höher nummeriert sind als der dynamische Eintrag, schlagen Verbindungen mit diesen Peers fehl und die dargestellten Debugs werden angezeigt.

```
IKEv1]: Group = x.x.x.x, IP = x.x.x.x, QM FSM error (P2 struct &0x49ba5a0, mess id 0xcd600011)!
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!
```

Für jede Schnittstelle in der Security Appliance ist nur eine dynamische Crypto-Map zulässig.

Hier ein Beispiel für eine richtig nummerierte Krypto-Zuordnung, die einen statischen und einen dynamischen Eintrag enthält. Beachten Sie, dass der dynamische Eintrag die höchste Sequenznummer hat und noch Platz für weitere statische Einträge vorhanden ist:

<#root>

```
crypto dynamic-map cisco 20 set transform-set myset
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 172.16.77.10
crypto map mymap 10 set transform-set myset
crypto map mymap interface outside
```

crypto map mymap 60000 ipsec-isakmp dynamic ciscothe

Bei Crypto Map-Namen wird die Groß- und Kleinschreibung berücksichtigt.

Diese Fehlermeldung wird auch angezeigt, wenn die dynamische Crypto-Man-Sequenz nicht korrekt ist, was dazu führt, dass der Peer die falsche Crypto-Map trifft.

Dies wird auch durch eine nicht übereinstimmende Krypto-Zugriffsliste verursacht, die den interessanten Datenverkehr definiert: %**ASA-3-713042: IKE Initiator kann die Richtlinie nicht finden:**

Wenn mehrere VPN-Tunnel an derselben Schnittstelle terminiert werden sollen, erstellen Sie eine Crypto Map mit demselben Namen (pro Schnittstelle ist nur eine Crypto Map zulässig), jedoch mit einer anderen Sequenznummer.

Dies gilt für den Router und die ASA.

Auf ähnliche Weise finden Sie weitere Informationen zur Konfiguration der Crypto Map sowohl für das L2L- als auch für das Remote Access VPN-Szenario unter ASA: Add a New Tunnel or Remote Access to an Existing L2L VPN - Cisco.

Überprüfen, ob die Peer-IP-Adresse korrekt ist

Erstellen und verwalten Sie die Datenbank mit verbindungsspezifischen Datensätzen für IPsec.

Geben Sie für eine LAN-to-LAN (L2L)-IPsec-VPN-Konfiguration der ASA Security Appliance den **<name>**der Tunnelgruppe als **Remote-Peer-IP-Adresse (**Remote-Tunnelende) in **der Tunnelgruppe <name> den Befehl ipsec-l2** ein.

Die Peer-IP-Adresse muss mit dem Namen der **Intunnel-Gruppe** und **den BefehlenCrypto map set address**übereinstimmen.

Während Sie das VPN mit ASDM konfigurieren, wurde der Tunnelgruppenname automatisch mit der richtigen Peer-IP-Adresse generiert.

Wenn die Peer-IP-Adresse nicht richtig konfiguriert ist, können die Protokolle diese Meldung enthalten. Dies kann durch eine ordnungsgemäße Konfiguration der **Peer-IP-Adresse** aufgelöst werden.

```
[IKEv1]: Group = DefaultL2LGroup, IP = x.x.x.x,
ERROR, had problems decrypting packet, probably due to mismatched pre-shared key. Aborting
```

Wenn die Peer-IP-Adresse in der ASA-Verschlüsselungskonfiguration nicht richtig konfiguriert wurde, kann die ASA den VPN-Tunnel nicht herstellen und hängt nur in *der* Phase *MM_WAIT_MSG4*.

Um dieses Problem zu beheben, korrigieren Sie die IP-Adresse des Peers in der Konfiguration.

Hier ist die Ausgabe des Befehls **show crypto isakmp** sacommand when the VPN tunnel hangs at in the MM_WAIT_MSG4 state.

<#root>

```
hostname#
```

show crypto isakmp sa

```
1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
```

```
    Rekey   : no              State   : MM_WAIT_MSG4
```

Überprüfen der Tunnelgruppe und der Gruppennamen

```
%ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by
tunnel-group and group-policy
```

Die Meldung wird angezeigt, wenn ein Tunnel verworfen wird, da sich der in der Gruppenrichtlinie angegebene zulässige Tunnel von dem zulässigen Tunnel in der Tunnelgruppenkonfiguration unterscheidet.

<#root>

```
group-policy hf_group_policy attributes
  vpn-tunnel-protocol l2tp-ipsec

username hfremote attributes
  vpn-tunnel-protocol l2tp-ipsec
```

Both lines read:

```
  vpn-tunnel-protocol ipsec l2tp-ipsec
```

Aktivieren Sie IPSec in der Standard-Gruppenrichtlinie für die bereits vorhandenen Protokolle in der Standard-Gruppenrichtlinie.

```
group-policy DfltGrpPolicy attributes
   vpn-tunnel-protocol L2TP-IPSec IPSec webvpn
```

Deaktivieren von XAUTH für L2L-Peers

Wenn ein LAN-zu-LAN-Tunnel und ein Remote Access-VPN-Tunnel auf derselben Crypto Map konfiguriert sind, wird der LAN-zu-LAN-Peer aufgefordert, XAUTH-Informationen einzugeben, und der LAN-zu-LAN-Tunnel schlägt mit "***CONF_XAUTH"*** in der Ausgabe des Befehls **How crypto isakmp** sacommand fehl.

Hier ist ein Beispiel für die Ausgabe der Sicherheitszuordnung:

<#root>

```
Router#
```

show crypto isakmp sa

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id  slot  status
X.X.X.X         Y.Y.Y.Y         CONF_XAUTH       10223    0   ACTIVE
```

```
X.X.X.X         Z.Z.Z.Z         CONF_XAUTH       10197    0   ACTIVE
```

Dieses Problem betrifft nur Cisco IOS®, ASA hingegen ist von diesem Problem nicht betroffen, da es Tunnelgruppen verwendet.

Verwenden Sie **das** Schlüsselwort **o-**xauth, wenn Sie den isakmp-Schlüssel eingeben, damit das Gerät den Peer nicht zur Eingabe von XAUTH-Informationen (Benutzername und Kennwort) auffordert.

Dieses Schlüsselwort deaktiviert XAUTH für statische IPsec-Peers. Geben Sie einen ähnlichen Befehl auf dem Gerät ein, auf dem L2L- und RA-VPN auf derselben Krypto-Zuordnung konfiguriert sind:

```
<#root>

router(config)#

crypto isakmp key cisco123 address
   172.22.1.164 no-xauth
```

In einem Szenario, in dem die ASA als Easy VPN-Server fungiert, kann der Easy VPN-Client aufgrund des Xauth-Problems keine Verbindung zum Headend herstellen.

Deaktivieren Sie die Benutzerauthentifizierung im ASA-Gerät, um das Problem wie folgt zu beheben:

```
<#root>

ASA(config)#

tunnel-group example-group type ipsec-ra

ASA(config)#

tunnel-group example-group ipsec-attributes

ASA(config-tunnel-ipsec)#

isakmp ikev1-user-authentication none
```

Weitere Informationen über den Befehl **sakmp ikev1-user-**authentication finden Sie im Abschnitt **Miscellaneousdieses Dokuments**.

Erschöpfung des VPN-Pools

Wenn der dem VPN-Pool zugewiesene Bereich von IP-Adressen nicht ausreicht, können Sie die Verfügbarkeit von IP-Adressen auf zwei Arten erweitern:

1. Entfernen Sie den vorhandenen Bereich, und definieren Sie den neuen. Hier ein Beispiel:

```
<#root>

CiscoASA(config)#

no ip local pool testvpnpool 10.76.41.1-10.76.41.254
```

```
CiscoASA(config)#
ip local pool testvpnpool 10.76.41.1-10.76.42.254
```

2. Wenn dem VPN-Pool nicht zusammenhängende Subnetze hinzugefügt werden sollen, können Sie zwei separate VPN-Pools definieren und diese dann in der Reihenfolge unter den â€žTunnelgruppen-Attributenâ€œ angeben. Hier ein Beispiel:

```
<#root>
CiscoASA(config)#
ip local pool testvpnpoolAB 10.76.41.1-10.76.42.254
CiscoASA(config)#
ip local pool testvpnpoolCD 10.76.45.1-10.76.45.254
CiscoASA(config)#
tunnel-group test type remote-access
CiscoASA(config)#
tunnel-group test general-attributes
CiscoASA(config-tunnel-general)#
address-pool (inside) testvpnpoolAB testvpnpoolCD
CiscoASA(config-tunnel-general)#
exit
```

Die Reihenfolge, in der Sie die Pools angeben, ist sehr wichtig, da die ASA Adressen aus diesen Pools in der Reihenfolge zuordnet, in der die Pools in diesem Befehl angezeigt werden.

Die Adresspooleinstellungen im Befehl group-policy address-pools überschreiben immer die lokalen Pooleinstellungen im Befehl tunnel-group address-pool.

Probleme mit der Latenz für VPN-Client-Datenverkehr

Wenn bei einer VPN-Verbindung Latenzprobleme auftreten, überprüfen Sie diese Bedingungen, um dieses Problem zu beheben:

1. Überprüfen Sie, ob die MSS des Pakets weiter reduziert werden kann.
2. Wenn IPsec/tcp anstelle von IPsec/udp verwendet wird, konfigurieren Sie "erve-vpn-flow".
3. Laden Sie die Cisco ASA neu.

VPN-Clients können keine Verbindung mit ASA herstellen

Problem

Cisco VPN-Clients können sich nicht authentifizieren, wenn X-auth mit dem Radius-Server verwendet wird.

Lösung

Das Problem kann sein, dass die Zeit für xauth überschritten wird. Erhöhen Sie den Timeout-Wert für den AAA-Server, um dieses Problem zu beheben.

Beispiele:

<#root>

```
Hostname(config)#
aaa-server test protocol radius

hostname(config-aaa-server-group)#
aaa-server test host 10.2.3.4

hostname(config-aaa-server-host)#
timeout 10
```

Problem

Cisco VPN-Clients können sich nicht authentifizieren, wenn X-auth mit dem Radius-Server verwendet wird.

Lösung

Stellen Sie zunächst sicher, dass die Authentifizierung ordnungsgemäß funktioniert. Um das Problem einzugrenzen, überprüfen Sie zunächst die Authentifizierung mit der lokalen Datenbank auf der ASA.

```
tunnel-group tggroup general-attributes
              authentication-server-group none
              authentication-server-group LOCAL
        exit
```

Wenn das funktioniert, dann ist das Problem auf die Radius-Serverkonfiguration zurückzuführen.

Überprüfen Sie die Konnektivität des Radius-Servers von der ASA. Wenn der Ping-Test ohne Probleme funktioniert, überprüfen Sie die Radius-bezogene Konfiguration auf der ASA und die Datenbankkonfiguration auf dem Radius-Server.

Sie können den Befehl **debug** radius verwenden, um radiusbezogene Probleme zu beheben. Informationen zur **Beispieldebug**-Radiusausgabe finden Sie unter **dieser Beispielausgabe**.

Bevor Sie den Befehl debugauf dem ASA-Gerät verwenden, lesen Sie die Dokumentation:**Warnmeldung**.

VPN-Client unterbricht die Verbindung häufig beim ersten Versuch oder â€žSecurity VPN Connection terminated by peer.

Grund 433." oder "Sichere VPN-Verbindung durch Peer beendet Grund 433:(Grund nicht durch Peer angegeben)"

Problem

Benutzer von Cisco VPN-Clients erhalten diesen Fehler, wenn sie versuchen, eine Verbindung zum Head-End-VPN-Gerät herzustellen.

VPN-Client lässt Verbindung beim ersten Versuch häufig verloren

Die Sicherheits-VPN-Verbindung wurde vom Peer beendet. Grund 433.

Sichere VPN-Verbindung durch Peer beendet. Grund 433:(Grund nicht durch Peer angegeben)

Versucht, eine Netzwerk- oder Broadcast-IP-Adresse zuzuweisen, wobei (x.x.x.x) aus dem Pool entfernt wurde

Lösung 1

Das Problem kann bei der Zuweisung des IP-Pools durch die ASA, den Radius-Server, den DHCP-Server oder den Radius-Server auftreten, der als DHCP-Server fungiert.

Verwenden Sie den Befehl **debug** cryptocommand, um die Richtigkeit der Netzmaske und der IP-Adressen zu überprüfen. Stellen Sie außerdem sicher, dass der Pool die Netzwerkadresse und die Broadcast-Adresse nicht enthält.

Radius-Server müssen in der Lage sein, den Clients die richtigen IP-Adressen zuzuweisen.

Lösung 2

Dieses Problem tritt auch auf, weil die erweiterte Authentifizierung fehlschlägt. Sie müssen den AAA-Server überprüfen, um diesen Fehler zu beheben.

Überprüfen Sie das Kennwort für die Serverauthentifizierung auf Server und Client. Laden Sie den AAA-Server neu, um dieses Problem zu beheben.

Lösung 3

Eine weitere Problemumgehung für dieses Problem ist die Deaktivierung der Bedrohungserkennungsfunktion.

In Zeiten, in denen mehrere Neuübertragungen für verschiedene unvollständige **Sicherheitszuordnungen (SAs)** erfolgen, geht die ASA mit aktivierter Bedrohungserkennungsfunktion davon aus, dass ein Scan-Angriff stattgefunden hat und die VPN-Ports als Haupttäter markiert sind.

Versuchen Sie, die Bedrohungserkennungsfunktion zu deaktivieren, da sie den Prozessor der ASA sehr stark auslasten kann. Verwenden Sie folgende Befehle, um die Bedrohungserkennung zu deaktivieren:

```
no threat-detection basic-threat
no threat-detection scanning-threat shun
no threat-detection statistics
no threat-detection rate
```

Dies kann als Problemumgehung verwendet werden, um zu überprüfen, ob dadurch das eigentliche Problem behoben wird.

Vergewissern Sie sich, dass durch die Deaktivierung der Bedrohungserkennung auf der Cisco ASA mehrere Sicherheitsfunktionen beeinträchtigt werden, wie z. B. die Minimierung der **Scanversuche,** der **DoS mit ungültigem SPI,** Pakete, die die **Anwendungsinspektion** nicht bestehen, und **unvollständige Sitzungen**.

Lösung 4

Dieses Problem tritt auch auf, wenn ein Transformationssatz nicht ordnungsgemäß konfiguriert ist. Eine ordnungsgemäße Konfiguration des Transformationssatzes behebt das Problem.

Remote-Zugriffs- und EZVPN-Benutzer stellen eine Verbindung zu VPN her, können aber nicht auf externe Ressourcen zugreifen

Problem

Benutzer mit Remote-Zugriff haben nach der Verbindung mit dem VPN keine Internetverbindung.

Benutzer mit Remote-Zugriff können nicht auf Ressourcen zugreifen, die sich hinter anderen VPNs auf demselben Gerät befinden.

Benutzer mit Remote-Zugriff können nur auf das lokale Netzwerk zugreifen.

Lösungen

Versuchen Sie diese Lösungen, um das Problem zu beheben:

- Kein Zugriff auf die Server in der DMZ möglich
- VPN-Clients können DNS nicht auflösen
- Split-Tunnel: Kein Zugriff auf das Internet oder ausgeschlossene Netzwerke möglich
- Lokaler LAN-Zugang
- Überlappende private Netzwerke

Kein Zugriff auf die Server in der DMZ möglich

Sobald der VPN-Client im IPsec-Tunnel mit dem VPN-Headend-Gerät (ASA/Cisco IOS® Router) eingerichtet ist, können die VPN-Client-Benutzer auf die INSIDE-Netzwerkressourcen (10.10.10.0/24) zugreifen, jedoch nicht auf das DMZ-Netzwerk (10.1.1.0/24).

Diagramm

Überprüfen Sie, ob die Konfiguration â€žSplit Tunnel, NO NATâ€œ im Headend-Gerät hinzugefügt wurde, um auf die Ressourcen im DMZ-Netzwerk zuzugreifen.

Beispiel:

ASA-Konfiguration:

Die folgende Konfiguration zeigt, wie die NAT-Ausnahme für das DMZ-Netzwerk konfiguriert wird, damit die VPN-Benutzer auf das DMZ-Netzwerk zugreifen können:

```
object network obj-dmz
subnet 10.1.1.0 255.255.255.0
object network obj-vpnpool
subnet 192.168.1.0 255.255.255.0
nat (inside,dmz) 1 source static obj-dmz obj-dmz destination static obj-vpnpool obj-vpnpool
```

Nachdem Sie einen neuen Eintrag für die NAT-Konfiguration hinzugefügt haben, löschen Sie die NAT-Übersetzung.

```
Clear xlate
Clear local
```

Überprüfung:

Wenn der Tunnel eingerichtet wurde, wechseln Sie zum **Cisco VPN Client, und wählen Sie Status > Route Details (Status > Routendetails),** um zu überprüfen, ob die sicheren Routen sowohl für das DMZ- als auch für das INSIDE-Netzwerk angezeigt werden.

Informationen zum Hinzufügen eines neuen VPN-Tunnels oder eines Remotezugriffs zu einem vorhandenen L2L-VPN - Cisco zu einer bereits vorhandenen L2L-VPN-Konfiguration, finden Sie unter ASA: Add a New Tunnel or Remote Access to a Existing L2L VPN - Cisco.

Im ASA-Konfigurationsbeispiel für Split-Tunneling für VPN-Clients zulassen finden Sie schrittweise Anleitungen dazu, wie VPN-Clients Zugriff auf das Internet erhalten, während sie in eine **Cisco Adaptive Security Appliance (ASA) der Serie 5500** getunnelt **werden**.

VPN-Clients können DNS nicht auflösen

Wenn der Tunnel eingerichtet wurde und die VPN-Clients den DNS nicht auflösen können, kann das Problem die DNS-Serverkonfiguration im Headend-Gerät (ASA) sein.

Überprüfen Sie außerdem die Verbindung zwischen den VPN-Clients und dem DNS-Server. Die Konfiguration des DNS-Servers muss unter der Gruppenrichtlinie konfiguriert und unter der Gruppenrichtlinie in den allgemeinen Tunnelgruppenattributen angewendet werden. Beispiel:

<#root>

```
!--- Create the group policy named vpn3000 and !--- specify the DNS server IP address(172.16.1.1) !--- a
```

```
group-policy vpn3000 internal
group-policy vpn3000 attributes
 dns-server value 172.16.1.1
 default-domain value cisco.com
```

```
!--- Associate the group policy(vpn3000) to the tunnel group !--- with the default-group-policy.

tunnel-group vpn3000 general-attributes
 default-group-policy vpn3000
```

VPN-Clients können keine internen Server nach Namen verbinden

Der VPN-Client kann die Hosts oder Server des Remote- oder Headend-internen Netzwerks nicht namentlich anpingen. Sie müssen â€žsplit-dns configureâ€œ auf der ASA aktivieren, um dieses Problem zu beheben.

Split-Tunnel: Kein Zugriff auf das Internet oder ausgeschlossene Netzwerke möglich

Mithilfe des Split-Tunnels können Remote-Access-IPsec-Clients Pakete bedingt verschlüsselt über den IPsec-Tunnel oder in Klartextform entschlüsselt an eine Netzwerkschnittstelle weiterleiten, wo sie an ein endgültiges Ziel weitergeleitet werden.

Split-tunnel ist standardmäßig deaktiviert, wodurchTunnel-Datenverkehr blockiert wird.

```
split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}
```

Die Option **excludeSpecified** wird nur für Cisco VPN Clients unterstützt, nicht EZVPN Clients.

```
ciscoasa(config-group-policy)#split-tunnel-policy excludespecified
```

Detaillierte Konfigurationsbeispiele für Split-Tunnel finden Sie in den folgenden Dokumenten:

- ASA: Split-Tunneling für VPN-Clients auf ASA-Konfigurationsbeispiel zulassen
- Konfigurationsbeispiel: Router ermöglicht VPN-Clients, IPsec und Internet mit Split-Tunneling zu verbinden

Haarnadellösung

Diese Funktion ist für VPN-Datenverkehr nützlich, der über eine Schnittstelle eingeht, dann aber über dieselbe Schnittstelle weitergeleitet wird.

Beispielsweise muss in einem Hub-and-Spoke-VPN-Netzwerk, in dem die Sicherheits-Appliance der Hub ist und Remote-VPN-Netzwerke Spokes sind, der Datenverkehr **zwischen Spoke-to-Spoke**-Kommunikation in die Sicherheits-Appliance und dann wieder nach der anderen Spoke fließen.

Verwenden Sie **dieselbe** Sicherheitsdatenverkehrskonfiguration, um den Datenverkehr in dieselbe Schnittstelle ein- und auszuführen.

<#root>

```
securityappliance(config)#
```

```
same-security-traffic permit intra-interface
```

Lokaler LAN-Zugang

Benutzer mit Remote-Zugriff stellen eine Verbindung zum VPN her und können sich nur mit dem lokalen Netzwerk verbinden.

Ein ausführlicheres Konfigurationsbeispiel finden Sie unter ASA: Allow local LAN access for VPN clients.

Überlappende private Netzwerke

Problem

Wenn Sie nach dem Tunnelaufbau nicht auf das interne Netzwerk zugreifen können, überprüfen Sie die IP-Adresse des VPN-Clients, die sich mit dem internen Netzwerk hinter dem Headend-Gerät überschneidet.

Lösung

Überprüfen Sie, ob sich die IP-Adressen im Pool, die den VPN-Clients, dem internen Netzwerk des Headend-Geräts und dem internen Netzwerk des VPN-Clients zugewiesen werden sollen, in unterschiedlichen Netzwerken befinden.

Sie können dasselbe Hauptnetzwerk verschiedenen Subnetzen zuweisen, aber manchmal treten Routing-Probleme auf.

Weitere Beispiele finden Sie unter Diagramm und Beispiel für den Abschnitt Die Server können nicht auf die DMZ zugreifen.

Keine Verbindung mit mehr als drei VPN-Client-Benutzern möglich

Problem

Nur drei VPN-Clients können eine Verbindung mit ASA/ herstellen; die Verbindung für den vierten Client fällt aus. Dabei wird folgende Fehlermeldung angezeigt:

```
Secure VPN Connection terminated locally by the client.
     Reason 413: User Authentication failed.
```

```
tunnel rejected; the maximum tunnel count has been reached
```

Lösungen

In den meisten Fällen hängt dieses Problem mit einer Einstellung für die gleichzeitige Anmeldung innerhalb der Gruppenrichtlinie und dem maximalen Sitzungslimit zusammen.

Versuchen Sie diese Lösungen, um das Problem zu beheben:

- Konfigurieren gleichzeitiger Anmeldungen
- Konfigurieren der ASA mit der CLI
- Konfigurieren

Konfigurieren gleichzeitiger Anmeldungen

Wenn das Kontrollkästchen Vererbung in ASDM aktiviert ist, ist nur die Standardanzahl gleichzeitiger Anmeldungen für den Benutzer zulässig. Der Standardwert für gleichzeitige Anmeldungen ist drei (3).

Um dieses Problem zu beheben, erhöhen Sie den Wert für gleichzeitige Anmeldungen.

1. Starten Sie ASDM, und navigieren Sie dann **zuConfiguration > VPN > Group Policy**.
2. Wählen Sie die entsprechende Gruppe aus, und klicken Sie auf die Schaltfläche Bearbeiten.
3. Deaktivieren Sie auf der Registerkarte Allgemein das Kontrollkästchen Vererbung **fürSimultane Anmeldungen unter Verbindungseinstellungen**. Wählen Sie einen geeigneten Wert im Feld aus.

   Der Mindestwert für dieses Feld ist Null (0). Dadurch wird die Anmeldung deaktiviert und der Benutzerzugriff verhindert.

   Wenn Sie sich mit demselben Benutzerkonto von einem anderen PC aus anmelden, wird die aktuelle Sitzung (die Verbindung, die von einem anderen PC mit demselben Benutzerkonto hergestellt wurde) beendet, und die neue Sitzung wird eingerichtet.

Dies ist das Standardverhalten und unabhängig von gleichzeitigen VPN-Anmeldungen.

Konfigurieren der ASA mit der CLI

Führen Sie diese Schritte aus, um die gewünschte Anzahl gleichzeitiger Anmeldungen zu konfigurieren. In diesem Beispiel wurde zwanzig (20) als Sollwert gewählt.

<#root>

```
ciscoasa(config)#
```

group-policy Bryan attributes

```
ciscoasa(config-group-policy)#
```

vpn-simultaneous-logins 20

Weitere Informationen zu diesem Befehl finden Sie unter Cisco Security Appliance Command Reference.

Verwenden Sie im globalen Konfigurationsmodus den Befehl **vpn-sessiondb max-session-**limit, um die Anzahl der VPN-Sitzungen auf einen Wert zu begrenzen, der unter dem Wert liegt, den die Security Appliance zulässt.

Verwenden Sie die Version dieses Befehls, um die Sitzungsbeschränkung zu entfernen. Verwenden Sie den Befehl erneut, um die aktuelle Einstellung zu überschreiben.

```
vpn-sessiondb max-session-limit {session-limit}
```

Dieses Beispiel zeigt, wie Sie einen maximalen VPN-Sitzungsgrenzwert von 450 festlegen:

<#root>

```
hostname#
```

vpn-sessiondb max-session-limit 450

Konfigurieren

Fehlermeldung

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

Lösung

Gehen Sie wie folgt vor, um die gewünschte Anzahl gleichzeitiger Anmeldungen zu konfigurieren. Sie können auch versuchen, die Anzahl gleichzeitiger Anmeldungen für diese Sicherheitszuordnung auf 5 festzulegen:

Wählen Sie Configuration > User Management > Groups > Modify 10.19.187.229 > General > Simultaneous Logins (Konfiguration > Benutzerverwaltung > Gruppen > Ändern 10.19.187.229 > General > Simultaneous Logins), und ändern Sie die Anzahl der Anmeldungen auf**5**.

Die Sitzung oder eine Anwendung kann nicht initiiert werden, und die Übertragung nach dem Tunnelaufbau ist langsam

Problem

Nach der Einrichtung des IPsec-Tunnels wird die Anwendung oder die Sitzung nicht über den gesamten Tunnel hinweg initiiert.

Lösungen

Verwenden Sie den Befehl ping, um das Netzwerk zu überprüfen oder zu ermitteln, ob der Anwendungsserver von Ihrem Netzwerk aus erreichbar ist.

Es kann ein Problem mit der maximalen Segmentgröße (MSS) für transiente Pakete auftreten, die einen Router oder ein /ASA-Gerät durchlaufen, insbesondere TCP-Segmente mit dem SYN-Bit-Set.

Cisco IOS® Router - Ändern des MSS-Werts in der externen Schnittstelle

(Tunnelendschnittstelle) des Routers

Führen Sie folgende Befehle aus, um den MSS-Wert an der externen Schnittstelle (Tunnel End Interface) des Routers zu ändern:

<#root>

```
Router>
enable

Router#
configure terminal
Router(config)#
interface ethernet0/1

Router(config-if)#ip tcp adjust-mss 1300
Router(config-if)#
end
```

Folgende Meldungen zeigen die Debug-Ausgabe für TCP MSS an:

<#root>

```
Router#debug ip tcp transactions

Sep 5 18:42:46.247: TCP0: state was LISTEN -> SYNRCVD [23 -> 10.0.1.1(38437)]
Sep 5 18:42:46.247: TCP: tcb 32290C0 connection to 10.0.1.1:38437, peer MSS 1300, MSS is
1300
Sep 5 18:42:46.247: TCP: sending SYN, seq 580539401, ack 6015751
Sep 5 18:42:46.247: TCP0: Connection to 10.0.1.1:38437, advertising MSS 1300
Sep 5 18:42:46.251: TCP0: state was SYNRCVD -> ESTAB [23 -> 10.0.1.1(38437)]
```

Die MSS wird auf dem Router wie konfiguriert auf 1300 eingestellt.

Weitere Informationen finden Sie unter ASA und Cisco IOS®: VPN Fragmentation.

ASA - Weitere Informationen finden Sie in der Dokumentation zu /ASA

Es ist nicht möglich, ordnungsgemäß auf das Internet zuzugreifen oder die Übertragung durch den Tunnel zu verlangsamen, da dies zu einer MTU-Größenfehlermeldung und MSS-Problemen führt.

Lesen Sie dieses Dokument, um das Problem zu beheben:

- ASA und Cisco IOS®: VPN-Fragmentierung

VPN-Tunnel kann von ASA nicht initiiert werden

Problem

Sie können den VPN-Tunnel nicht von der ASA-Schnittstelle initiieren. Nach der Tunneleinrichtung kann der Remote-End-/VPN-Client keinen Ping an die interne ASA-Schnittstelle im VPN-Tunnel senden.

Beispielsweise kann der pn-Client keine SSH- oder HTTP-Verbindung zu ASAs innerhalb der Schnittstelle über einen VPN-Tunnel initiieren.

Lösung

Die interne Schnittstelle des kann nur dann vom anderen Ende des Tunnels angepingt werden, wenn der Befehl **management-**access im globalen Konfigurationsmodus konfiguriert wird.

<#root>

```
ASA-02(config)#
```

management-access inside

```
ASA-02(config)#
```

show management-access

```
management-access inside
```

Dieser Befehl unterstützt auch die SSH-Initiierung oder die HTTP-Verbindung zur internen Schnittstelle der ASA über einen VPN-Tunnel.

Diese Informationen gelten auch für die DMZ-Schnittstelle. Wenn Sie beispielsweise einen Ping an die DMZ-Schnittstelle von /ASA senden oder einen Tunnel von der DMZ-Schnittstelle aus initiieren möchten, ist der Befehl **management-access** DMZ erforderlich.

<#root>

```
ASA-02(config)#
```

management-access DMZ

Wenn der VPN-Client keine Verbindung herstellen kann, stellen Sie sicher, dass die ESP- und UDP-Ports offen sind.

Wenn diese Ports jedoch nicht geöffnet sind, versuchen Sie, über TCP 10000 eine Verbindung herzustellen. Wählen Sie dazu diesen Port unter dem VPN-Client-Verbindungseintrag aus.

Klicken Sie mit der rechten **Maustaste aufÄndern > Registerkarte Transport > IPsec über TCP**.

Datenverkehr kann nicht über VPN-Tunnel weitergeleitet werden

Problem

Sie können keinen Datenverkehr über einen VPN-Tunnel weiterleiten.

Lösung

Dieses Problem kann auch auftreten, wenn die ESP-Pakete blockiert werden. Um dieses Problem zu beheben, konfigurieren Sie den VPN-Tunnel neu.

Dieses Problem kann auftreten, wenn Daten nicht verschlüsselt, sondern nur über den VPN-Tunnel entschlüsselt werden, wie in der folgenden Ausgabe gezeigt:

<#root>

```
ASA# sh crypto ipsec sa peer x.x.x.x
peer address: y.y.y.y
    Crypto map tag: IPSec_map, seq num: 37, local addr: x.x.x.x
      access-list test permit ip host xx.xx.xx.xx host yy.yy.yy.yy
      local ident (addr/mask/prot/port): (xx.xx.xx.xx/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port): (yy.yy.yy.yy/255.255.255.255/0/0)
      current_peer: y.y.y.y


 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 393, #pkts decrypt: 393, #pkts verify: 393

      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0
```

Um dieses Problem zu beheben, überprüfen Sie die folgenden Bedingungen:

1. Ob die Krypto-Zugriffslisten mit der Gegenstelle übereinstimmen und NAT 0-Zugriffslisten korrekt sind.

2. Wenn das Routing korrekt ist und der Datenverkehr die externe Schnittstelle erreicht, die den Datenverkehr innerhalb der Schnittstelle weiterleitet. Die Beispielausgabe zeigt, dass die Entschlüsselung erfolgt, die Verschlüsselung aber nicht.

3. Wenn der Befehl ysopt permit connection-vpn auf der ASA konfiguriert wurde. Wenn dieser Befehl nicht konfiguriert ist, können Sie ihn konfigurieren, da er es der ASA ermöglicht, den verschlüsselten/VPN-Datenverkehr von der ACL-Überprüfung der Schnittstelle auszunehmen.

Konfigurieren des Backup-Peers für den VPN-Tunnel auf derselben Crypto Map

Problem

Sie möchten mehrere Backup-Peers für einen einzelnen VPN-Tunnel verwenden.

Lösung

Die Konfiguration mehrerer Peers entspricht der Bereitstellung einer Fallbackliste. Für jeden Tunnel versucht die Security-Appliance, mit dem ersten Peer in der Liste zu verhandeln.

Wenn dieser Peer nicht antwortet, arbeitet sich die Security-Appliance in der Liste nach unten, bis entweder ein Peer antwortet oder keine weiteren Peers in der Liste vorhanden sind.

Auf der ASA ist bereits eine Crypto Map als primärer Peer konfiguriert. Der sekundäre Peer könnte nach dem primären hinzugefügt werden.

Diese Beispielkonfiguration zeigt den primären Peer als X.X.X.X. und den Backup-Peer als Y.Y.Y.Y. an:

<#root>

ASA(config)#

crypto map mymap 10 set peer X.X.X.X Y.Y.Y.Y

Deaktivieren/Neustarten des VPN-Tunnels

Problem

Um den VPN-Tunnel vorübergehend zu deaktivieren und den Dienst neu zu starten, führen Sie das in diesem Abschnitt beschriebene Verfahren aus.

Lösung

Verwenden Sie **den Befehl crypto map** interfacecommand im globalen Konfigurationsmodus, um eine zuvor definierte Crypto Map für eine Schnittstelle zu entfernen.

Verwenden Sie die enoform dieses Befehls, um den Crypto Map-Satz von der Schnittstelle zu entfernen.

<#root>

hostname(config)#

no crypto map

map-name

interface

interface-name

Dieser Befehl entfernt eine Krypto-Zuordnung zu einer aktiven Security-Appliance-Schnittstelle und macht den IPsec-VPN-Tunnel auf dieser Schnittstelle inaktiv.

Um den IPsec-Tunnel auf einer Schnittstelle neu zu starten, müssen Sie einer Schnittstelle einen Krypto-Zuordnungssatz zuweisen, bevor diese Schnittstelle IPsec-Dienste bereitstellen kann.

<#root>

```
hostname(config)#
```

crypto map

map-name

interface

interface-name

Einige Tunnel nicht verschlüsselt

Problem

Wenn eine große Anzahl von Tunneln auf dem VPN-Gateway konfiguriert ist, leiten einige Tunnel den Datenverkehr nicht weiter. Die ASA empfängt keine verschlüsselten Pakete für diese Tunnel.

Lösung

Dieses Problem tritt auf, weil die ASA die verschlüsselten Pakete nicht durch die Tunnel weiterleitet. In der ASP-Tabelle werden doppelte Verschlüsselungsregeln erstellt.

Fehler:- %ASA-5-713904: Gruppe = DefaultRAGroup, IP = x.x.x.x, ... Nicht unterstützter Transaktionsmodus Version 2.Tunnel beendet.

Problem

%**ASA-5-713904: Group = DefaultRAGroup, IP = 192.0.2.0,... nicht unterstützter Transaktionsmodus v2 version.Tunnel terminatederror** Meldung wird angezeigt.

Lösung

Der Grund für `die` Fehlermeldung `Transaction Mode v2` ist, dass ASA nur IKE Mode Config V6 und nicht die alte Version des V2-Modus unterstützt.

Verwenden Sie die Version IKE Mode Config V6, um diesen Fehler zu beheben.

Fehler:- %ASA-6-722036: Gruppe Client-Gruppe Benutzer xxxx IP x.x.x.x Übertragen eines großen Pakets 1220 (Schwellenwert 1206)

Problem

Die Fehlermeldung **%ASA-6-722036: Group < client-group > User < xxxx > IP < x.x.x.x> Transmitting large packet 1220 (threshold 1206)** wird in den Protokollen von ASA angezeigt.

Was bedeutet dieses Protokoll und wie wird dieses Problem behoben?

Lösung

Diese Protokollmeldung besagt, dass ein großes Paket an den Client gesendet wurde. Die Quelle des Pakets kennt die MTU des Clients nicht.

Dies kann auch auf die Komprimierung nicht komprimierbarer Daten zurückzuführen sein. Die Problemumgehung besteht darin, die SVC-Komprimierung mit dem Befehl **vc komprimierung** nonecommand abzuschalten, wodurch das Problem behoben wird.

Fehlermeldung, wenn QoS an einem Ende des VPN-Tunnels aktiviert ist

Problem

Wenn Sie QoS an einem Ende des VPN-Tunnels aktiviert haben, wird folgende Fehlermeldung angezeigt:

```
IPSEC: Received an ESP packet (SPI= 0xDB6E5A60, sequence number= 0x7F9F) from
10.18.7.11 (user= ghufhi) to 172.16.29.23 that failed anti-replay check
```

Lösung

Diese Meldung wird normalerweise angezeigt, wenn ein Ende des Tunnels QoS durchführt. Dies geschieht, wenn ein Paket als außer Betrieb erkannt wird.

Sie können QoS deaktivieren, um dies zu stoppen, aber es kann ignoriert werden, solange der Datenverkehr den Tunnel passieren kann.

WARNUNG: Crypto Map-Eintrag unvollständig

Problem

Wenn Sie den Befehl **crypto map mymap 20 ipsec**-isakmpausführen, wird folgender Fehler angezeigt:

```
WARNUNG: Crypto Map-Eintrag unvollständig
```

Beispiele:

<#root>

```
ciscoasa(config)#
```

```
crypto map mymap 20 ipsec-isakmp
```

```
WARNING: crypto map entry incomplete
```

Lösung

Dies ist eine übliche Warnung, wenn Sie eine neue Crypto Map definieren. Eine Erinnerung, dass Parameter wie access-list (match address), transform set und peer address konfiguriert werden müssen, bevor sie funktionieren können.

Es ist auch normal, dass die erste Zeile, die Sie zum Definieren der Krypto-Zuordnung eingeben, in der Konfiguration nicht angezeigt wird.

Fehler:- %ASA-4-400024: IDS:2151 Großes ICMP-Paket von einer zu einer Schnittstelle außerhalb

Problem

Ein großes Ping-Paket kann nicht über den VPN-Tunnel weitergeleitet werden. Wenn wir versuchen, große Ping-Pakete weiterzuleiten, erhalten wir den Fehler %**`ASA-4-400024: IDS:2151 Large ICMP packet from to on interface outside.`**

Lösung

Deaktivieren Sie die Signaturen 2150 und 2151, um dieses Problem zu beheben. Sobald die Signaturen deaktiviert sind, funktioniert der Ping-Test.

Verwenden Sie folgende Befehle, um die Signaturen zu deaktivieren:

ASA(config)#**ip audit signature 2151 disable**

ASA(config)#**ip audit signature 2150 disable**

Fehler:- %ASA-4-402119: IPSEC: Es wurde ein Protokollpaket (SPI=spi, Sequenznummer= seq_num) von remote_IP (Benutzername) an local_IP empfangen, bei dem die Anti-Replay-Prüfung fehlgeschlagen ist.

Problem

Ich habe in den Protokollmeldungen der ASA folgenden Fehler erhalten:

`Fehler:- %|ASA-4-402119: IPSEC: Es wurde ein Protokollpaket (SPI=spi, Sequenznummer= seq_num) von remote_IP (Benutzername) an local_IP empfangen, bei dem die Anti-Replay-Prüfung fehlgeschlagen ist.`

Lösung

Um diesen Fehler zu beheben, verwenden Sie **den Befehl rypto ipsec security-association replay window-**size, um die Fenstergröße zu variieren.

<#root>

`hostname(config)#`

`crypto ipsec security-association replay window-size 1024`

Cisco empfiehlt die Verwendung der vollen Fenstergröße 1024, um alle Anti-Replay-Probleme zu beseitigen.

Fehlermeldung - %ASA-4-407001: Datenverkehr für lokale Host-Schnittstelle ablehnen_name:inside_address, Lizenzgrenzwert der Anzahl überschritten

Problem

Nur wenige Hosts können sich nicht mit dem Internet verbinden, und im Syslog wird folgende Fehlermeldung angezeigt:

Fehlermeldung - %ASA-4-407001: Datenverkehr für lokale Host-Schnittstelle ablehnen_name:inside_address, Lizenzgrenzwert der Anzahl überschritten

Lösung

Diese Fehlermeldung wird angezeigt, wenn die Anzahl der Benutzer das Benutzerlimit der verwendeten Lizenz überschreitet. Dieser Fehler kann durch ein Upgrade der Lizenz auf eine höhere Anzahl von Benutzern behoben werden.

Die Benutzerlizenz kann je nach Bedarf 50, 100 oder eine unbegrenzte Zahl von Benutzern enthalten.

Fehlermeldung: %VPN_HW-4-PACKET_ERROR:

Problem

`Die Fehlermeldung - %VPN_HW-4-PACKET_ERROR:`error message zeigt an, dass die vom Router empfangenen ESP-Pakete mit HMAC nicht übereinstimmen. Dieser Fehler kann durch folgende Probleme verursacht werden:

- VPN-H/W-Modul defekt
- Beschädigtes ESP-Paket

Lösung

Gehen Sie folgendermaßen vor, um dieses Problem zu beheben:

- Ignorieren Sie die Fehlermeldungen, es sei denn, der Datenverkehr ist unterbrochen.
- Wenn der Datenverkehr unterbrochen wird, ersetzen Sie das Modul.

Fehlermeldung: Befehl abgelehnt: Löschen Sie zuerst die Kryptografieverbindung zwischen VLAN XXXX und XXXX.

Problem

Diese Fehlermeldung wird angezeigt, wenn Sie versuchen, dem Trunk-Port eines Switches ein zulässiges

VLAN hinzuzufügen:`Befehl abgelehnt: Löschen Sie zuerst die Krypto-Verbindung zwischen VLAN XXXX und VLAN XXXX..`

Der WAN-Edge-Trunk kann nicht so geändert werden, dass er zusätzliche VLANs ermöglicht. Das heißt, Sie können dem IPSEC-**VPN**-SPA-Trunk keine VLANs hinzufügen.

Dieser Befehl wird abgelehnt, da er zu einem VLAN mit verschlüsselter Verbindung führt, das zur Liste der zulässigen VLANs gehört, was eine potenzielle IPSec-Sicherheitsverletzung darstellt.

Beachten Sie, dass dieses Verhalten für alle Trunk-Ports gilt.

Lösung

Verwenden Sie anstelle des Befehls `no switchport trunk allowed vlan (vlanlist)` den Befehl `witchport trunk allowed vlan` non-ecommand oder den Befehl "`switchport trunk allowed vlan remove (vlanlist)`".

Fehlermeldung - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Verworfenes Paket - Ungültige Fensterskalierungsoption für Sitzung x.x.x.x:27331 bis x.x.x.x:23 [Initiator(Flag 0, Faktor 0) Responder (Flag 1, Faktor 2)]

Problem

Dieser Fehler tritt auf, wenn Sie versuchen, eine Telnet-Verbindung von einem Gerät am anderen Ende eines VPN-Tunnels oder über den Router selbst herzustellen:

`Fehlermeldung - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Verworfenes Paket - Ungültige Fensterskalierungsoption für Sitzung x.x.x.x:27331 bis x.x.x.x:23 [Initiator(Flag 0, Faktor 0) Responder (Flag 1, Faktor 2)]`

Lösung

Die Benutzerlizenz kann je nach Bedarf 50, 100 oder eine unbegrenzte Zahl von Benutzern enthalten. Eine Fensterskala-Funktion wurde hinzugefügt, um eine schnelle Übertragung von Daten über lange Fett-Netzwerke (LFN) zu ermöglichen.

Dies sind in der Regel Verbindungen mit sehr hoher Bandbreite, aber auch hoher Latenz.

Netzwerke mit Satellitenverbindungen sind ein Beispiel für ein LFN, da Satellitenverbindungen immer hohe Ausbreitungsverzögerungen, aber typischerweise eine hohe Bandbreite aufweisen.

Um die Fensterskalierungsfunktion zur Unterstützung von LFNs zu aktivieren, muss die TCP-Fenstergröße mehr als 65.535 betragen. Diese Fehlermeldung kann behoben werden, wenn Sie die TCP-Fenstergröße auf mehr als 65.535 erhöhen.

%ASA-5-305013: Asymmetrische NAT-Regeln wurden für Vorwärts- und Rückwärtsrichtung abgeglichen. Please update this issue flows

Problem

Diese Fehlermeldung wird angezeigt, sobald der VPN-Tunnel aktiviert wird:

%ASA-5-305013: Asymmetrische NAT-Regeln wurden für Vorwärts- und Rückwärtsrichtung abgeglichen. Please update this issue flows

Lösung

Um dieses Problem zu beheben, wenn es sich nicht auf derselben Schnittstelle wie der Host mit NAT befindet, verwenden Sie die zugeordnete Adresse anstelle der tatsächlichen Adresse, um eine Verbindung mit dem Host herzustellen.

Aktivieren Sie außerdem den Befehl einspect, wenn die Anwendung die IP-Adresse einbettet.

%ASA-5-713068: Nicht routinemäßig empfangene Benachrichtigungsmeldung: notify_type

Problem

Diese Fehlermeldung wird angezeigt, wenn der VPN-Tunnel nicht gestartet werden kann:

%ASA-5-713068: Nicht routinemäßig empfangene Benachrichtigungsmeldung: notify_type

Lösung

Diese Meldung wird aufgrund einer Fehlkonfiguration angezeigt (d. h. wenn die Richtlinien oder ACLs auf Peers nicht identisch konfiguriert sind).

Sobald die Richtlinien und ACLs übereinstimmen, wird der Tunnel problemlos hergestellt.

%ASA-5-720012: (VPN-sekundär) IPSec-Failover-Laufzeitdaten konnten auf der Standby-Einheit nicht aktualisiert werden (oder) %ASA-6-720012: (VPN-Einheit) IPsec-Failover-Laufzeitdaten konnten auf der Standby-Einheit nicht aktualisiert werden

Problem

Eine der folgenden Fehlermeldungen wird angezeigt, wenn Sie versuchen, die Cisco Adaptive Security Appliance (ASA) zu aktualisieren:

%ASA-5-720012: (VPN-Sekundär) Fehler beim Aktualisieren der IPSec-Failover-Laufzeitdaten auf der Standby-Einheit.

%ASA-6-720012: (VPN-Einheit) Fehler beim Aktualisieren der IPsec-Failover-Laufzeitdaten auf der Standby-Einheit.

Lösung

Diese Fehlermeldungen dienen lediglich der Information und haben keine Auswirkungen auf die

Funktionalität von ASA oder VPN.

Diese Meldungen werden angezeigt, wenn das VPN-Failover-Subsystem die IPsec-bezogenen Laufzeitdaten nicht aktualisieren kann, da der zugehörige IPsec-Tunnel auf der Standby-Einheit gelöscht wurde.

Um diese zu beheben, geben Sie **den** Befehl wr standby auf dem aktiven Gerät ein.

Fehler:- %ASA-3-713063: IKE-Peer-Adresse nicht für Ziel 0.0.0.0 konfiguriert

Problem

Die Fehlermeldung **`%ASA-3-713063: IKE-Peer-Adresse nicht für Ziel 0.0.0.0 konfiguriert`** wird angezeigt, und der Tunnel wird nicht hochgefahren.

Lösung

Diese Meldung wird angezeigt, wenn die IKE-Peer-Adresse nicht für einen L2L-Tunnel konfiguriert ist.

Dieser Fehler kann behoben werden, wenn Sie die Sequenznummer der Crypto Map ändern, die Crypto Map entfernen und erneut anwenden.

Fehler: %ASA-3-752006: Tunnel Manager konnte keine KEY_ACQUIRE-Nachricht versenden.

Problem

`%ASA-3-752006: Tunnel Manager konnte keine KEY_ACQUIRE-Nachricht versenden.Wahrscheinliche Fehlkonfiguration der Crypto Map oder der Tunnel-Gruppe."`Fehlermeldung wird auf der Cisco ASA protokolliert.

Lösung

Diese Fehlermeldung kann durch eine falsche Konfiguration der Krypto-Zuordnung oder der Tunnel-Gruppe verursacht werden. Stellen Sie sicher, dass beide richtig konfiguriert sind. Weitere Informationen zu dieser Fehlermeldung finden Sie unter Fehler 752006 .

Hier einige Korrekturmaßnahmen:

- Entfernen Sie die Krypto-ACL (z. B. der dynamischen Zuordnung zugewiesen).
- Entfernen Sie nicht verwendete IKEv2-bezogene Konfigurationen, falls vorhanden.
- Überprüfen Sie, ob die Krypto-ACL übereinstimmt.
- Entfernen Sie doppelte Einträge in der Zugriffsliste, falls vorhanden.

Fehler: %ASA-4-402116: IPSEC: Es wurde ein ESP-Paket (SPI= 0x99554D4E, Sequenznummer= 0x9E) von XX.XX.XX.XX (user= XX.XX.XX.XX) an YY.YY.YY.YY empfangen.

In einer LAN-zu-LAN-VPN-Tunnel-Einrichtung wird folgender Fehler auf einem ASA-Ende empfangen:

```
Das entkapselte innere Paket stimmt nicht mit der ausgehandelten Richtlinie in der SA überein.

Das Paket gibt als Ziel 10.32.77.67, als Quelle 10.105.30.1 und als Protokoll icmp an.

Die Sicherheitszuordnung legt ihren lokalen Proxy als 10.32.77.67/255.255.255.255/ip/0 und ihren Remote-Proxy als 10.105.42.192/255.255.255.224/ip/0 fest.
```

Lösung

Sie müssen die interessanten Zugriffslisten an beiden Enden des VPN-Tunnels überprüfen. Beide müssen als exakte Spiegelbilder übereinstimmen.

Failed to launch 64-bit VA installer to enable the virtual adapter due to error 0xffffffff

Problem

`Der Fehler beim Starten des 64-Bit-VA-Installationsprogramms zum Aktivieren des virtuellen Adapters aufgrund des Fehlers "0xfffffflog"` wird empfangen, wenn AnyConnect keine Verbindung herstellen kann.

Lösung

Gehen Sie folgendermaßen vor, um dieses Problem zu beheben:

1. Gehen Sie **zuSystem > Internet Communication Management > Internet Communication** settings, und stellen Sie sicher**, dassDeaktivierung von Automatic Root Certificates** Update vorhanden ist.
2. Wenn sie deaktiviert ist, deaktivieren Sie den **gesamten administrativen** Vorlagenteil des Gruppenrichtlinienobjekts, das dem betroffenen Computer zugewiesen ist, und führen Sie den Test erneut aus.

Weitere Informationen finden Sie unter Automatische Aktualisierung der Stammzertifikate deaktivieren.

Der Cisco VPN-Client funktioniert unter Windows 7 nicht mit der Datenkarte

Problem

Der Cisco VPN-Client funktioniert unter Windows 7 nicht mit der Datenkarte.

Lösung

Der auf Windows 7 installierte Cisco VPN-Client funktioniert nicht mit 3G-Verbindungen, da Datenkarten auf VPN-Clients auf einem Windows 7-Computer nicht unterstützt werden.

Warnung: "VPN-Funktionalität funktioniert möglicherweise

überhaupt nicht"

Problem

Bei Versuchen, isakmp auf der externen Schnittstelle von ASA zu aktivieren, wird diese Warnmeldung empfangen:

```
ASA(config)# crypto isakmp enable outside
WARNING, system is running low on memory.  Performance may start to degrade.
VPN functionality may not work at all.
```

Greifen Sie in diesem Fall über ssh auf die ASA zu. HTTPS wird beendet und andere SSL-Clients sind ebenfalls betroffen.

Lösung

Dieses Problem ist auf Speicheranforderungen verschiedener Module wie Logger und Krypto zurückzuführen.

Stellen Sie sicher, dass Sie nicht über den Befehl **log queue 0**verfügen. Die Warteschlangengröße wird auf 8192 festgelegt, und die Speicherzuweisung wird erhöht.

Bei Plattformen wie ASA5505 und ASA5510 ist diese Speicherzuweisung tendenziell auf andere Module beschränkt, für die nur wenig Speicher zur Verfügung steht.

IPSec-Padding-Fehler

Problem

Folgende Fehlermeldung wird angezeigt:

```
%ASA-3-402130: CRYPTO: Received an ESP packet (SPI =
     0xXXXXXXX, sequence number= 0xXXXX) from x.x.x.x (user= user) to y.y.y.y with
     incorrect IPsec padding
```

Lösung

Das Problem tritt auf, weil das IPSec-VPN ohne Hash-Algorithmus aushandelt. Paket-Hash stellt die Integritätsprüfung für den ESP-Kanal sicher.

Aus diesem Grund werden fehlerhafte Pakete ohne Hash von der Cisco ASA unerkannt akzeptiert und versucht, diese Pakete zu entschlüsseln.

Da diese Pakete jedoch fehlerhaft sind, findet die ASA Fehler bei der Paketentschlüsselung. Dies verursacht die Padding-Fehlermeldungen, die angezeigt werden.

Es wird empfohlen, einen Hash-Algorithmus in den Transformationssatz für das VPN aufzunehmen und

sicherzustellen, dass die Verbindung zwischen den Peers minimale Paketfehler aufweist.

Der VPN-Tunnel wird alle 18 Stunden getrennt

Problem

Der VPN-Tunnel wird alle 18 Stunden getrennt, obwohl die Lebensdauer auf 24 Stunden festgelegt ist.

Lösung

Die Lebensdauer ist die maximale Zeit, die die SA für rekey verwendet werden kann. Der Wert, den Sie in der Konfiguration als Lebensdauer eingeben, stimmt nicht mit der Schlüssel-Neuerstellungszeit der Sicherheitszuordnung überein.

Daher ist es notwendig, eine neue Sicherheitszuordnung (oder ein Sicherheitszuordnungs-Paar im Fall von IPsec) auszuhandeln, bevor die aktuelle abläuft.

Die Schlüssel-Neuerstellungszeit muss immer kleiner als die Lebensdauer sein, um mehrere Versuche zu ermöglichen, falls der erste Versuch der Schlüssel-Neuerstellung fehlschlägt.

Die RFCs legen nicht fest, wie die Schlüssel-Neuerstellungszeit berechnet werden soll. Dies liegt im Ermessen der Implementierer.

Daher variiert die Zeit je nach Plattform. Einige Implementierungen können einen Zufallsfaktor verwenden, um den Timer für die Schlüssel-Neuerstellung zu berechnen.

Wenn die ASA beispielsweise den Tunnel initiiert, ist es normal, dass die Schlüsselneuzuweisung mit 64800 Sekunden = 75 % von 86400 erfolgt.

Wenn der Router initiiert, kann die ASA länger warten, um dem Peer mehr Zeit zu geben, die Schlüssel-Neuerstellung zu initiieren.

Daher ist es normal, dass die VPN-Sitzung alle 18 Stunden getrennt wird, um einen anderen Schlüssel für die VPN-Aushandlung zu verwenden. Dies darf keine VPN-Ausfälle oder Probleme verursachen.

Der Datenverkehrsfluss wird nicht aufrechterhalten, nachdem der LAN-zu-LAN-Tunnel neu ausgehandelt wurde

Problem

Der Datenverkehrsfluss wird nicht aufrechterhalten, nachdem der LAN-zu-LAN-Tunnel neu ausgehandelt wurde.

Lösung

Die ASA überwacht alle Verbindungen, die sie passieren, und behält einen Eintrag in der Statustabelle gemäß der Funktion für die Anwendungsinspektion bei.

Die Details des verschlüsselten Datenverkehrs, der das VPN passiert, werden in Form einer Sicherheitszuordnungs-Datenbank verwaltet. Bei LAN-zu-LAN-VPN-Verbindungen werden zwei verschiedene Datenströme verwaltet.

Einer davon ist der verschlüsselte Datenverkehr zwischen den VPN-Gateways. Der andere ist der Datenstrom zwischen der Netzwerkressource hinter dem VPN-Gateway und dem Endbenutzer hinter dem anderen Ende.

Wenn das VPN beendet wird, werden die Flow-Details für diese bestimmte Sicherheitszuordnung gelöscht.

Der von der ASA für diese TCP-Verbindung verwaltete Eintrag in der Statustabelle veraltet jedoch aufgrund fehlender Aktivität, was den Download behindert.

Das bedeutet, dass die ASA die TCP-Verbindung für diesen bestimmten Datenfluss beibehält, während die Benutzeranwendung beendet wird.

Die TCP-Verbindungen gehen jedoch verloren und werden nach Ablauf des TCP-Idle-Timers möglicherweise zu einem Timeout.

Dieses Problem wurde mit der Einführung der Funktion "**Persistent IPSec Tunneled Flows"** gelöst.

Ein neuer Befehl, sysopt connection preserve-vpn-flows, wurde in die Cisco ASA integriert, um die Status-Tabelleninformationen bei der Neuverhandlung des VPN-Tunnels beizubehalten.

Dieser Befehl ist standardmäßig deaktiviert. Um dies zu aktivieren, pflegt die Cisco ASA die Informationen der TCP-Statustabelle, wenn sich das L2L-VPN von der Unterbrechung erholt und den Tunnel wieder herstellt.

Eine Fehlermeldung besagt, dass die Bandbreite für die Kryptofunktion erreicht wurde

Problem

Auf dem Router der 2900-Serie wird folgende Fehlermeldung angezeigt:

`Fehler: 20.03. 10:51:29: %CERM-4-TX_BW_LIMIT: Maximales Tx-Bandbreitenlimit von 85000 Kbit/s für die Verschlüsselungsfunktionalität mit SecurityK9-Technologiepaket-Lizenz erreicht.`

Lösung

Dies ist ein bekanntes Problem, das aufgrund der strengen Richtlinien der Regierung der Vereinigten Staaten auftritt.

Dementsprechend kann die **securityk9**-Lizenz nur eine Payload-Verschlüsselung bis zu Raten von nahezu 90 Mbit/s zulassen und die Anzahl der verschlüsselten Tunnel/TLS-Sitzungen für das Gerät begrenzen.

Weitere Informationen zu den Exportbeschränkungen für Kryptographien finden Sie unter Cisco ISR G2 SEC and HSEC Licensing.

Im Falle von Cisco Geräten wird ein unidirektionaler Datenverkehr von weniger als 85 Mbit/s innerhalb oder außerhalb des ISR G2-Routers abgeleitet (insgesamt 170 Mbit/s bidirektional).

Diese Anforderung gilt für die Cisco ISR G2-Plattformen der 1900-, 2900- und 3900-Serie. Mit diesem Befehl können Sie die folgenden Einschränkungen anzeigen:

<#root>

```
Router#

show platform cerm-information

Crypto Export Restrictions Manager(CERM) Information:
CERM functionality: ENABLED
 ---------------------------------------------------------------
 Resource                      Maximum Limit          Available
 ---------------------------------------------------------------
 Tx Bandwidth(in kbps)         85000                  85000
 Rx Bandwidth(in kbps)         85000                  85000
 Number of tunnels               225                    225
 Number of TLS sessions         1000                   1000
---Output truncated----
```

Um dieses Problem zu vermeiden, erwerben Sie eine HSECK9-Lizenz. Eine â€žhseck9â€œ - Funktionslizenz bietet erweiterte Payload-Verschlüsselungsfunktionen mit einer höheren Anzahl an VPN-Tunneln und sicheren Sprachsitzungen.

Weitere Informationen zur Lizenzierung von Cisco ISR Routern finden Sie unter Software Activation (Softwareaktivierung).

Problem: Ausgehender Verschlüsselungsverkehr in einem IPsec-Tunnel schlägt fehl, selbst wenn eingehender Entschlüsselungsverkehr funktioniert.

Lösung

Dieses Problem wurde bei einer IPsec-Verbindung nach mehreren Schlüssel-Neuerstellungen beobachtet, aber die Triggerbedingung ist nicht eindeutig.

Dieses Problem kann behoben werden, wenn Sie die Ausgabe des Befehls **how asp** drop überprüfen und überprüfen, ob der Kontextzähler für abgelaufene VPN für jedes gesendete ausgehende Paket zunimmt.

Verschiedenes

In der Ausgabe der Befehle â€žshow crypto isakmp saâ€œ und â€ždebugâ€œ wird die Meldung â€žAG_INIT_EXCHâ€œ angezeigt

Wenn der Tunnel nicht initiiert wird, erscheint **die AG_INIT**_EXCHmessage auch in der Ausgabe des Befehls **show crypto isakmp** sacommand und indebugoutput.

Der Grund dafür kann sein, dass isakmp-Richtlinien nicht übereinstimmen oder Port udp 500 unterwegs blockiert wird.

Debug-Meldung â€žReceived an IPC message during invalid stateâ€œ (Eine IPC-Meldung wurde während eines ungültigen Status empfangen) wird angezeigt

Diese Meldung dient nur der Information und hat nichts mit der Trennung des VPN-Tunnels zu tun.

Zugehörige Informationen

- **ASA und Cisco IOS®: VPN-Fragmentierung**
- **Cisco Adaptive Security Appliances der ASA 5500-Serie**
- **IPSec-Aushandlung/IKE-Protokolle**
- **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.