Konfiguration und Fehlerbehebung für VPME-System auf RFGW-10

Inhalt

Einführung

Dieses Dokument beschreibt das VPME-System (VoD Privacy Mode Encryption), die Konfiguration auf RFGW-10 und die Schritte zur Fehlerbehebung.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

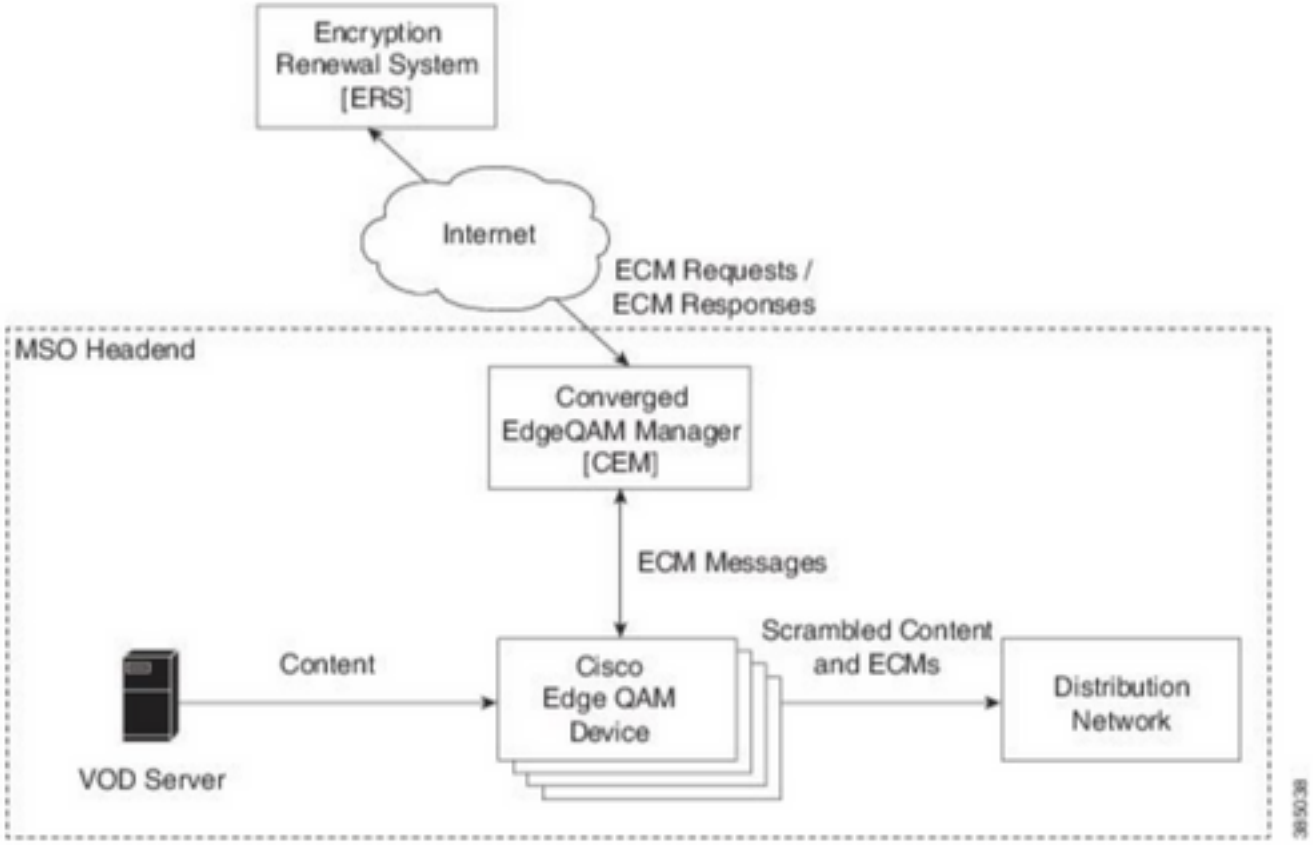
Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Cisco Converged EdgeQAM Manager (CEM), auch bekannt als Cisco Encryption Manager oder Converged Encryption Manager ist eine Java-Anwendung, die auf Windows/Linux-Systemen ausgeführt wird. Sie kommuniziert über das Internet mit dem Encryption Renewal System (ERS) und ruft ECMs (Berechtigungskontrollnachrichten) ab, die das Kontrollwort enthalten, um das Video zu verschlüsseln, und leitet die ECM-Nachrichten dann an Cisco Edge QAM-Geräte am Standort weiter. Die EQAM-Geräte verwirbeln den Stream mit dem im ECM enthaltenen Kontrollwort (Control Word, CW) und senden den verschlüsselten Inhalt sowie das ECM an die Set-Top-Boxen (STBs):



Neue ECMs werden in regelmäßigen Abständen (in der Reihenfolge von Tagen) gesendet, je nach Sicherheitsstufe, die der Service Provider gewährleisten möchte. Bis zur Verlängerung des ECM nutzt der EQAMS weiterhin den zuletzt erhaltenen.

Konfigurieren von VPME auf RFGW-10

```
cable video scrambler pme cem 10.11.12.13 5000 cable video scrambler pme vodsid 500
!
cable linecard 3 encryption pme scrambler des
  dvb-conform true
cable video multicast uplink TenGigabitEthernet 12/9 backup TenGigabitEthernet 1/1 bandwidth
9000000
cable video multicast uplink TenGigabitEthernet 12/10 backup TenGigabitEthernet 1/2 bandwidth
9000000
cable video timeout off-session 300
cable route linecard 3 load-balance-group 1 qam-partition default ip 10.20.30.40 udp 1 2000
bitrate 1500000 qam-partition 3 ip 10.20.30.40 udp 2001 65535 gqi-ingress-port 1 bitrate 4000000
cable route linecard 3 load-balance-group 2 qam-partition 3 ip 10.20.30.50 udp 2001 65535 gqi-
ingress-port 2 bitrate 4000000
interface Loopback2
ip address 10.20.30.50 255.255.255.255 secondary [...] ip address 10.20.30.40 255.255.255.255
```

Fehlerbehebung bei VPME auf RFGW-10

Schritt 1: Überprüfen Sie die Videositzungen.

```
RFGW-10#sh cable video sess all

Session    QAM      Stream Sess IP              UDP   Out   Input    Input  Output PSI Ctrl
```

```
Encryption Current
ID         Port     Type   Type Address          Port  Pgm   Bitrate  State  State  Rdy State
Type       State
---------- -------- ------ ---- ---------------- ----- ----- -------- ------ ------ --- ----- --
-------- -----
--> CLEAR SESSIONS / MULTICAST:
203096374  3/1.27   Pass   SSM  -                -     -     22440    ACTIVE ON     YES -     -
-
203096376  3/1.27   Remap  SSM  -                -     1510  12500000 ACTIVE ON     YES -     -
-
203161914  3/1.28   Remap  SSM  -                -     1109  3750000  ACTIVE ON     YES -     -
-
--> PME ENCRYPTED SESSIONS / UNICAST:
GQI ESTABLISHED, EXPECTED WHEN NO VoD REQUEST
204341248  3/1.46   Remap  UDP  10.20.30.40      100   1     0        OFF    ON     NO  -
PME        -
204341249  3/1.46   Remap  UDP  10.20.30.40      101   2     0        OFF    ON     NO  -
PME        -
204341250  3/1.46   Remap  UDP  10.20.30.40      102   3     0        OFF    ON     NO  -
PME        -
VoD SESSION TRYING TO ESTBLISH, BUT NOT ENCRYPTED -> NOT GOOD
293404952  4/8.45   Remap  UDP  10.20.30.40      1450  1     5623706  ACTIVE ON     YES -
PME        -
HOW IT MUST LOOK LIKE
216924331  3/5.46   Remap  UDP  10.20.30.40      901   2     14751242 ACTIVE ON     YES -
PME        Encrypted
220004558  3/6.45   Remap  UDP  10.20.30.40      1056  7     14754740 ACTIVE ON     YES -
PME        Encrypted
274530352  4/2.45   Remap  UDP  10.20.30.40      258   9     30001748 ACTIVE ON     YES -
PME        Encrypted
```

Hier sehen Sie das Problem mit einer VoD-Sitzung, die versucht, zu erstellen. Für einige Sekunden (bevor sie verfällt) befindet sie sich im AKTIVEN Zustand, mit Datenverkehr in der Eingabe-Bitrate, aber nicht verschlüsselt. Dieses Verhalten deutet auf ein Verschlüsselungsproblem hin.

Sie können dies auch bestätigen, indem Sie eine Zugriffsliste auf den Uplinks platzieren, um den Datenverkehr mit den Loopback-IPs abzustimmen, und überprüfen, ob Pakete auf der Zugriffsliste übereinstimmen.

Schritt 2: Überprüfen Sie den CEM-Status auf dem RFGW-10.

```
RFGW-10#show cable video scramble pme stat

Vodsid     : 500
CEM IP     : 10.11.12.13
CEM Port   : 5000
Local Port : 0
Count of ECMs recd   : 0
CEM Connection State : Not Connected
CEM Connection will be attempted after 50 seconds
```

> **Hinweis**: Die CEM-IP ist die IP-Adresse des virtuellen Systems, da das CEM nur eine Java-Anwendung ist, die darauf ausgeführt wird.

Wie muss es aussehen?

```
RFGW-10#show cable video scramble pme stat

Vodsid      : 500
CEM IP      : 10.11.12.13
CEM Port    : 5000
Local Port : 22268
Count of ECMs recd   : 1
CEM Connection State : Connected
```

Schritt 3: Überprüfen Sie die Verbindung, indem Sie die CEM-IP-Adresse pingen.

Schritt 4: Überprüfen Sie die CEM-Konfiguration.

Sie benötigen GUI-Zugriff auf das virtuelle System, um die grafische Benutzeroberfläche der CEM-Anwendung aufzurufen. Danach müssen Sie die Konfiguration der Schnittstellen zu den RFGW-10-Knoten und dem ERS-Server überprüfen, wie im CEM-Leitfaden erläutert: Cisco Converged EdgeQAM Manager - Benutzerhandbuch

Wenn Sie nur über CLI-Zugriff auf das virtuelle System verfügen, können Sie **ps -ef** ausgeben, um zu überprüfen, ob die CEM-Anwendung ausgeführt wird, und die Protokolle mit **tail -f CEM.log** überprüfen.