Configure and Troubleshoot VPME System on RFGW-10

Contents

Introduction

This document describes the VoD Privacy Mode Encryption (VPME) system, how to configure it on RFGW-10, and steps to troubleshoot.

Prerequisites

Requirements

There are no specific requirements for this document.

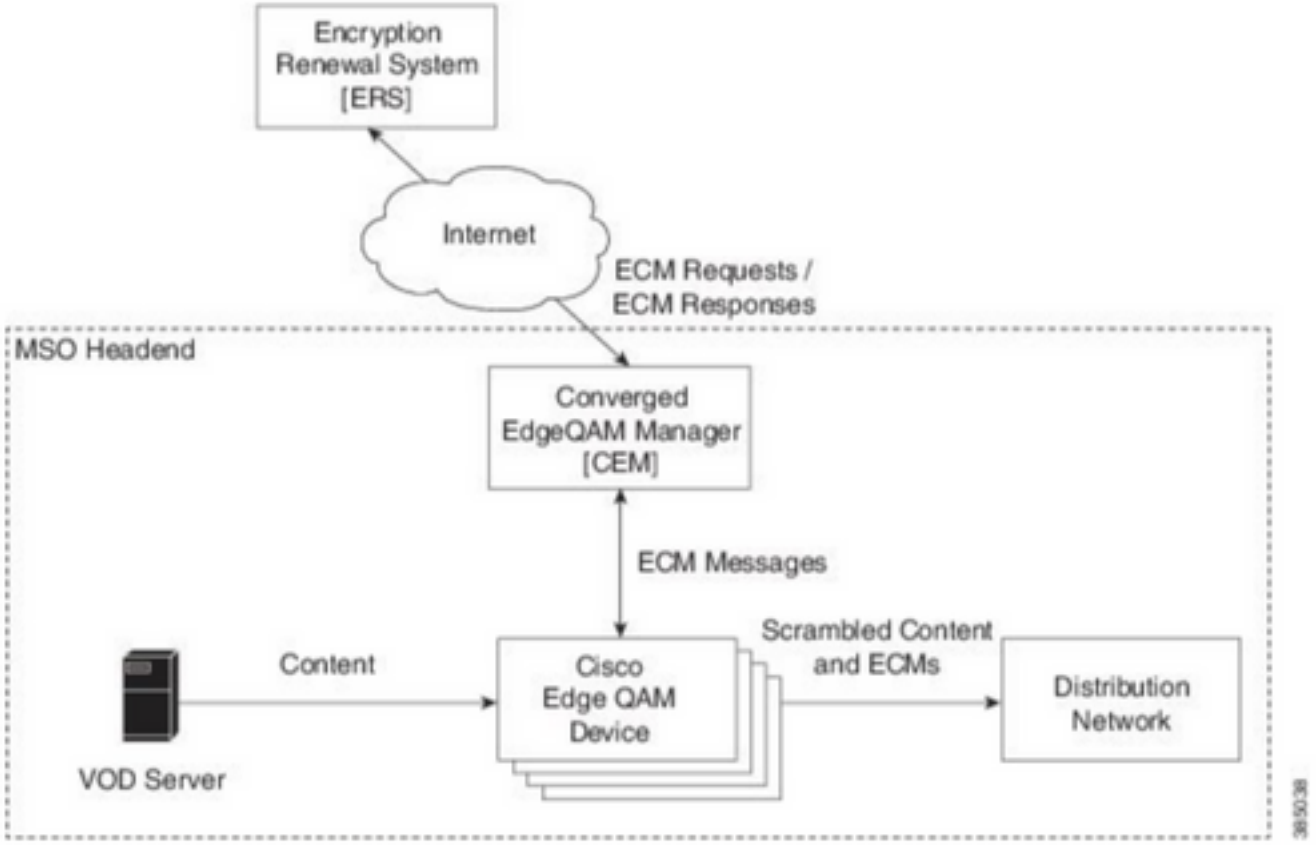
Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The Cisco Converged EdgeQAM Manager (CEM), a.k.a. Cisco Encryption Manager or Converged Encryption Manager is a Java application that runs on Windows/Linux Systems. It communicates with the Encryption Renewal System (ERS) over the Internet and obtains the Entitlement Control Messages (ECMs), containing the Control Word to scramble the video, then forwards the ECM messages to Cisco Edge QAM devices in the site. The EQAM devices scramble the stream with the Control Word (CW) contained in the ECM, and send the scrambled content plus the ECM to the Set-Top Boxes (STBs):



New ECMs are sent periodically (order of days), depending on the level of security the SP wants to ensure. Until the ECM is renewed, the EQAMS keeps using the last one received.

Configure VPME on 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
```

Troubleshoot VPME on RFGW-10

Step 1. Check the video sessions.

```
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
```

Here you can see the problem with a VoD session that is trying to establish. For few seconds (before it drops) it is in ACTIVE state, with traffic in input bitrate but not encrypted. This behavior suggests an encryption problem.

You can further confirm this by putting an access list on the uplinks, in order to match the traffic with the loopback IPs, and verify that you see packets matches on the access list.

Step 2. Check the CEM status on the 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
```

> **Note**: the CEM IP is the IP of the VM, as the CEM is just a java application running on top of it.

How it must look like:

```
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
```

Step 3. Check connectivity by pinging the CEM IP address.

Step 4. Check the CEM configuration.

You need GUI access to the VM in order to enter the CEM application's GUI. Once there, you need to verify the configuration of the interfaces to the RFGW-10 nodes and the ERS server, as explained in the CEM guide: Cisco Converged EdgeQAM Manager User Guide

If you have only CLI access to the VM, you can issue **ps -ef** to check whether the CEM application runs, and also check the logs with **tail -f CEM.log**