

VPN-systeem configureren en oplossen op RFGW-10

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[VPME configureren op RFGW-10](#)

[Probleemoplossing voor VPN op RFGW-10](#)

Inleiding

In dit document wordt het VoD Privacy Mode Encryption (VPME)-systeem beschreven, hoe u het op RFGW-10 configureren en stappen naar probleemoplossing zet.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

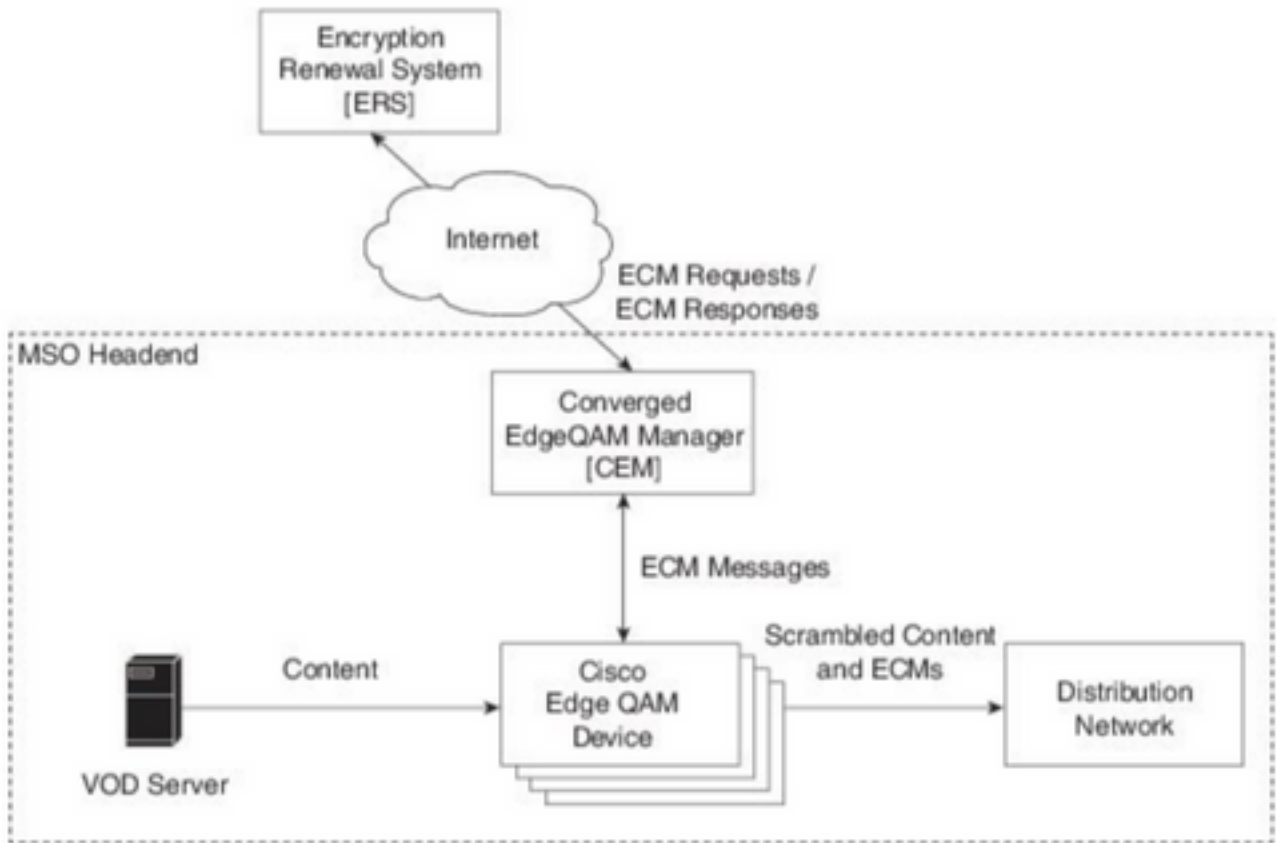
Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Cisco Converged Edge QAM Manager (CEM), ook bekend als Cisco Encryption Manager of Converged Encryption Manager, is een Java-toepassing die op Windows-/Linux-systemen draait. Het communiceert met het Encryption Renewal System (ERS) via het internet en verkrijgt de Entitlement Control Messages (ECM's), dat het Control Word bevat om de video te scammelen, en stuurt de ECM-berichten naar Cisco Edge QAM-apparaten op de website. Met de EQAM-apparaten kan de stroom worden gescammeld met het Control Word (CW) in het ECM en worden de gescande inhoud plus het ECM naar de Settopboxen (STB's) verzonden:



Nieuwe ECM's worden periodiek verzonden (volgorde van dagen), afhankelijk van het veiligheidsniveau dat de SP wil waarborgen. Totdat het ECM wordt verlengd, blijven de EQAMS de laatst ontvangen.

VPME configureren op 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

```

Probleemoplossing voor VPN op RFGW-10

Stap 1. Controleer de videosessies.

```
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 zie je het probleem met een VoD sessie die probeert vast te stellen. Gedurende enkele seconden (voordat het valt) is het actief, met verkeer in invoerbitraat maar niet versleuteld. Dit gedrag suggereert een encryptie probleem.

U kunt dit verder bevestigen door een toegangslijst op de uplinks te zetten, om het verkeer met de IP's van de loopback aan te passen en te controleren of u pakketovereenkomsten op de toegangslijst ziet.

Stap 2. Controleer de CEM-status op de 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

```

Opmerking: de CEM IP is het IP van de VM, aangezien de CEM slechts een java-toepassing is die er bovenop draait.

Hoe moet het eruit zien:

```
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
```

Stap 3. Controleer de connectiviteit door het CEM IP-adres ingedrukt te houden.

Stap 4. Controleer de CEM-configuratie.

U hebt GUI-toegang tot de VM nodig om de GUI van de CEM-toepassing in te voeren. Daarna moet u de configuratie van de interfaces met de RFGW-10-knooppunten en de ERS-server verifiëren, zoals uitgelegd in de CEM-gids: [Cisco geconvergeerde Edge QAM Manager-gebruikershandleiding](#)

Als u alleen CLI-toegang tot de VM hebt, kunt u **ps-ef** uitvoeren om te controleren of de CEM-toepassing draait en de logbestanden ook controleren met **staart-f CEM.log**