

Catalyst 9500和Nexus 9000之间的MACSec XPN流量发生故障，无效数据包和FCS错误增加

目录

问题

在Catalyst 9500-28C8D和Nexus N9K-C93180YC-FX之间启用MACSec XPN后，MKA会话成功建立，但数据流量不会通过链路。Catalyst 9500报告物理接口上的SA统计信息和FCS输入错误下的“无效数据包”增加。具体来说，可以观察到以下症状：

- 启用MACSec后无连接
- MKA会话显示为已建立，但Catalyst 9500端显示SA统计信息，其中“Notvalid pkts 118”增加，“Valid pkts:0”
- Catalyst 9500物理接口上的FCS输入错误增加
- 删除MACSec配置会立即恢复连接并停止FCS错误

已在两台设备上建立MKA会话并成功协商GCM-AES-XPB-256密码。Nexus端显示加密处于活动状态，但Catalyst 9500接收了加密数据包，由于验证不匹配而将其拒绝，导致接受零个有效数据包。

环境

- 运行Cisco IOS®的Catalyst 9500-28C8D
- Nexus N9K-C-93180-FX
- 使用GCM-AES-XPB-256密码套件的MACSec XPN配置
- 400千兆以太网接口（Catalyst上的400GigE 1/0/15, Nexus上的Ethernet1/52）
- Catalyst 9500配置为密钥服务器优先级1, Nexus配置为密钥服务器优先级100
- 用于预共享密钥的AES-256-CMAC加密算法

分辨率

此问题通过实施更改设备间密钥服务器角色分配的解决方法得以解决。建议的解决方案涉及以下步骤：

步骤 1：确定密钥服务器配置问题

验证两台设备上的当前密钥服务器优先级配置。有问题的配置显示：

Catalyst 9500配置：

```
mka policy MEHEALTH-ORG-XPN
key-server priority 1
macsec-cipher-suite gcm-aes-xpn-256
```

Nexus配置

```
macsec policy MEHEALTH-ORG-XPN
key-server-priority 100
```

步骤 2：实施密钥服务器角色解决方法

将Nexus设备配置为MACSec密钥服务器而不是Catalyst 9500。这包括调整密钥服务器优先级值，以便Nexus承担密钥服务器角色。

修改Nexus配置，使其具有较低的密钥服务器优先级值（较低的值具有更高的优先级）：

```
macsec policy MEHEALTH-ORG-XPN
key-server-priority 1
```

修改Catalyst 9500配置，使其具有更高的密钥服务器优先级值：

```
mka policy MEHEALTH-ORG-XPN
key-server priority 100
macsec-cipher-suite gcm-aes-xpn-256
```

步骤 3：验证MACSec操作

实施密钥服务器角色更改后，请验证：

- MKA会话在两个设备上成功建立
- 数据流量通过启用MACSec的链路
- Catalyst 9500 SA统计信息上没有增加“无效数据包”
- 物理接口上未发生FCS输入错误

此解决方法允许MACSec XPN配置正常工作，直到完成平台调查和软件升级规划。

原因

此问题的根本原因与Cisco Bug ID CSCvs00410有关，该案例描述了MKA会话建立成功但数据无法在链路上通过的场景，当使用AES-256-XPB和Catalyst 9500时，在与Nexus设备的特定互操作性条件下与Nexus设备一起使用密钥服务器角色。该行为表现为验证不匹配，其中Catalyst 9500拒绝来自Nexus的加密数据包，导致无效数据包计数和FCS错误增加。Cisco IOS被列为该缺陷的修复项目，对此存在明显差异，需要Catalyst平台团队进一步调查。

相关内容

- Cisco Bug ID CSCvs00410 — 当使用具有Catalyst 9500密钥服务器角色的AES-256-XPB时，MKA会话已启动，但无法通过链路传递数据

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。