# 無効なセキュリティ パラメータ インデックスによって発生するトンネル フラップをトラブルシューティングするために使われる EEM スクリプト

## 内容



## 概要

このドキュメントでは、セキュリティ アソシエーション（SA）がピア デバイス間の同期信号の対象外になる可能性があるという最も一般的な IPSec の問題の 1 つを説明します。その結果、暗号化のデバイスは、ピアの暗号化で認識されていない SA を使用してトラフィックを暗号化します。

## 前提条件

### 要件

このドキュメントに特有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、Cisco IOS®リリース15.1(4)M4で完了したテストに基づいています。スクリプトと設定は、Cisco IOSリリース12.4(22)T以降でサポートされているEmbedded Event Manager(EEM)バージョン3.0を使用します。ただし、これはテストされていません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

# 問題

パケットは、syslog に記録されるこのメッセージを使用してピアで廃棄されます。

```
*Mar 12 18:22:10.706: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet
   has invalid spi for destaddr=213.163.222.7, prot=50, spi=0x68842105(1753489669),
   srcaddr=11.1.1.3, input interface=Ethernet0/0
```

無効なセキュリティ パラメータ インデックス（SPI）の詳細については、『IPSec %RECVD_PKT_INV_SPI エラーおよび無効な SPI の回復機能 情報』を参照してください。このドキュメントでは、トラブルシュートするために必要なデータを収集することが困難な、断続的にエラーが発生するシナリオでのトラブルシュート方法を説明します。

この種の問題は、問題が発生したときにデバッグできる通常の VPN トラブルシューティングとは異なります。無効な SPI による断続的なトンネル フラップをトラブルシュートするには、最初に 2 台のヘッドエンドが同期信号からどのように外れたのかを判断する必要があります。次の停止がいつ発生するかを予測することはできないため、EEM スクリプトが解決策になります。

# 解決方法

この Syslog メッセージがトリガーされる前に何が起きたのかを知ることが重要であるため、実稼働トラフィックに影響しないようにルータで条件付きデバッグを実行し続け、その情報を Syslog サーバに送信します。代わりにスクリプトでデバッグを有効にした場合は、Syslog メッセージがトリガーされた後でデバッグが生成されるため役に立たないことがあります。このログの送信側と受信側で実行するデバッグの一覧を次に示します。

```
debug crypto condition peer ipv4 <peer IP address> debug crypto isakmp debug crypto ipsec debug
crypto engine
```

EEM スクリプトは次の 2 つのことをするように設計されています。

1. 最初の Syslog メッセージが生成されてから 18 秒間デバッグが収集された時に、受信側のデバッグをオフにします。生成されたデバッグとログの量をもとに遅延タイマーを修正する必要がある場合があります。
2. 同時にデバッグが無効化され、ピアに SNMP トラップを送信し、これがピア デバイスのデバッグを無効化します。

## SNMP の設定（SNMP Configuration）

Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）の設定を次に示します。

```
Receiver:
========

snmp-server enable traps event-manager
snmp-server host 11.1.1.3 public event-manager
snmp-server manager



Sender:
=======

snmp-server enable traps event-manager
snmp-server host 213.163.222.7 public event-manager
snmp-server manager
```

## 最終的なスクリプト

受信側と送信側のスクリプトを次に示します。

```
Receiver:
========
!--- To test if this output gets logged to the file called "hub" sh ip int bri | tee /append
disk0:hub.txt conf t ! event manager applet command_hub event syslog pattern "CRYPTO-4-
RECVD_PKT_INV_SPI.*srcaddr=11.1.1.3" action 1 cli command "enable" action 2 syslog msg
"command_hub is running ..." priority informational action 3 cli command "show crypto sockets |
append disk0:hub.txt" action 4 cli command "show crypto isa sa | append disk0:hub.txt" action 5
cli command "show crypto ipsec sa detail | append disk0:hub.txt" action 6 cli command "show
dmvpn detail | append disk0:hub.txt" action 7 wait 18 action 8 cli command "undebug all" action
8.1 snmp-trap intdata1 2323232 strdata "" action 9 syslog priority informational msg "DONE ON
HUB" ! end

Sender:
=======

conf t
!
event manager applet spoke_app
 event snmp-notification oid 1.3.6.1.4.1.9.10.91.1.2.3.1.9.
    oid-val "2323232" op eq src-ip-address 213.163.222.7 maxrun 35
 action 1.0 syslog msg "Received trap from Hub..."
 action 2.0 cli command "enable"
 action 3.0 cli command "undebug all"
 action 4.0 syslog msg "DONE ON SPOKE"
!
end
```

## EEM スクリプト ログ

EEM スクリプト ログのメッセージのリストを次に示します。

```
Receiver:
=======

*Mar 12 18:22:10.706: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet
    has invalid spi for destaddr=213.163.222.7, prot=50, spi=0x68842105(1753489669),
    srcaddr=11.1.1.3, input interface=Ethernet0/0
*Mar 12 18:22:10.727: %HA_EM-6-LOG: command_hub: command_hub is running ...
```

```
hub#
*Mar 12 18:22:30.026: %HA_EM-6-LOG: command_hub: DONE ON HUB



Sender:
=======

spoke#
*Mar 12 18:22:30.542: %HA_EM-6-LOG: spoke_app: Received trap from Hub...
*Mar 12 18:22:30.889: %HA_EM-6-LOG: spoke_app: DONE ON SPOKE
```

## 確認

問題が解決されたことを確認するために、show debug コマンドを入力します。

```
Receiver:
=========
hub# show debug


Sender:
=======
spoke# show debug
```

# 関連情報

- テクニカル サポートとドキュメント – Cisco Systems