CHAPTER 5

統合侵入検知セキュリティ

Cisco NX-OS ソフトウェアは、IPv4 と IPv6 の侵入検知パケット チェックによって特定の条件に一致し、ほとんどの実稼動ネットワークでは通常必要のないパケットをドロップして、ネットワークのセキュリティを強化します。デフォルトでは、ほとんどの Intrusion Detection System（IDS; 侵入検知システム）パケット チェックが有効になっています。このチェックを無効にする明確な理由がない限り、有効にしておく必要があります。

この章で説明する内容は、次のとおりです。

IDS チェックのステータスとカウンタの確認

導入：Cisco NX-OS Release 4.0(1)

show hardware forwarding ip verify コマンドを使用して、IDS パケット チェックのステータスとカウンタを確認する必要があります。「Packets Failed」カウンタでは、パケットが IDS チェックに当てはまったかどうかを確認できます。この出力は、ネットワーク トラフィックを確認するとき、アプリケーションの問題をトラブルシューティングするときに役立ちます。場合によっては、IDS パケット チェックを無効にする必要があります。Cisco NX-OS Release 5.0(3) では、パケットがドロップされたときの Syslog メッセージと Embedded Event Manager（EEM）イベント トリガーのサポートが導入されました。

```
n7000# show hardware forwarding ip verify

IPv4 and v6 IDS Checks          Status     Packets Failed
-----------------------------+---------+------------------
address source broadcast        Enabled    0
address source multicast        Enabled    0
address destination zero        Enabled    0
address identical               Enabled    0
address reserved                Enabled    0
address class-e                 Disabled   --
checksum                        Enabled    0
protocol                        Enabled    0
fragment                        Disabled   --
length minimum                  Enabled    0
length consistent               Enabled    0
length maximum max-frag         Enabled    0
length maximum udp              Disabled   --
length maximum max-tcp          Enabled    0
tcp flags                       Disabled   --
tcp tiny-frag                   Enabled    0
```

```
version                          Enabled    0
------------------------------+---------+------------------
IPv6 IDS Checks                  Status     Packets Failed
------------------------------+---------+------------------
length consistent                Enabled    0
length maximum max-frag          Enabled    0
length maximum udp               Disabled   --
length maximum max-tcp           Enabled    0
```

IDS パケット チェックの無効化と有効化

導入：Cisco NX-OS Release 4.0(1)

この項は、参考のために記載しており、必要のない場合があります。

アプリケーションが適切に機能するように、IDS パケット チェックを無効にする必要がある場合があります。次のグローバル コマンドを使用して、パケット チェックを無効および有効にすることができます。この例では、「length maximum max-tcp」IDS チェックを無効および有効にします。他のパケット チェックも同じ手順で設定できます。

```
n7000(config)# no hardware ip verify length maximum max-tcp

n7000(config)# hardware ip verify length maximum max-tcp
```