トラフィック分析の構成

この章では、Cisco NX-OS デバイス上でトラフィック分析機能を構成する方法について説明します。

トラフィック分析について

トラフィック分析（Traffic Analytics、TA）機能には、次の機能があります。

- 集約された分析データを提供するために、スイッチの背後にあるサーバによって提供されるサービスを識別する機能を提供します。サーバとクライアントを区別するために、 3 ウェイハンドシェイクの TCP フラグ（SYN および SYN ACK）が使用されます。
- クライアントからサーバまたはサーバからクライアントへの複数の TCP セッションデータトラフィックを show flow cache データベース内の 1 つのレコードに集約し、それをコレクタにエクスポートします。トラフィック分析集約中、 TCP の送信元ポートは値 0 に設定されます。
- トラブルシュートフローのエクスポート頻度の高速化をサポートします。
- TA インターフェイスフィルタおよび VRF フィルタをサポートします。

フローは、送信元インターフェイス、プロトコル、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート値によって定義されます。トラフィック分析が有効になっている場合、TCP セッションのフローは、サーバからクライアントへのトラフィックの送信元 IP アドレス（SIP）、宛先 IP アドレス（DIP）、送信元ポート（SP）、およびクライアントからサーバへのトラフィック。

トラフィック データベース エントリのエージング

トラフィック データベース エントリは、タイマーを使用して 24 時間ごとにモニターされます。データベース エントリにトラフィックが到達しない場合、24 ～ 48 時間以内にそのトラフィック データベース エントリが削除されます。デフォルトでは、データベースのサイズは 5000 です。

トラブルシューティング ルール

トラブルシューティング ルールは、分析 ACL フィルタをプログラミングしてフローをデバッグするために使用されます。これらのルールはトラフィック分析ルールよりも優先され、特定のフローをキャプチャするために使用できます。ルールのトラブルシューティングによって、フロー キャッシュに 2 つのエントリが生成される場合があります。

トラブルシューティング ルールは、特定のフローに対してのみ使用する必要があります。

トラブルシューティングフローのエクスポート頻度の高速化

現在、フローレコードとトラブルシュートレコードは、1 分の固定間隔でエクスポートされます。トラブルシューティング分析の効率を高めるために、新しい **filter export-interval** コマンドが導入されました。このコマンドを使用すると、専用のハッシュデータベースを使用して、より短い間隔でトラブルシュートレコードをエクスポートできます。

この構成は、トラフィック分析が有効になっており、フローシステム設定内でフィルタ処理が設定されている場合にのみ適用できます。**filter export-interval** コマンドの詳細については、トラフィック分析の例 （7 ページ） を参照してください。

UDP ポートのサポートについて

Cisco NX-OSリリース 10.5（2）F 以降、トラフィック分析は、エクスポートされたフローをマスクする UDP ポート構成をサポートします。

マスキングについては、次の手順に従います：

- UDP ポートが構成されている場合、フローは TA DB および NFM フロー キャッシュでマスクされます。
- 宛て先ポートが一致すると、送信元ポートがマスクされ、その逆も同様です。
- NetFlow エントリが最初に挿入され、その後に TA エントリが挿入されます。
- UDP ポートが構成されていない場合、現在の機能は影響を受けません。

UDPポートを構成するために、次の **[no] udp-port** *port-range* コマンドがフロー traffic-analytics サブモード（分析の下）に導入されました。

UDP ポートは 1 ー 65565 の範囲である必要があります。ポートは、カンマ区切りまたは範囲ベースのフォーマット（例： `2000-3000, 400, 500`）で入力できます。

入力のポート数が 1回線コマンドで表示できるポートの最大数を超えると、次の例に示すように、新しい設定回線に表示されます：

```
analytics
  flow traffic-analytics
    udp-port
540,550,1024,1040,1060,1080,1100,1102,1104,1106,1300,1302,1304,1306,1308,1310,1312,1314,1316,1318,1320,1322,1324,1326,1328,1330,1332,1334,1336,1338,1340,1342,1344,1346,1348,1350,1352,1354,1356,1358,1360,1362,1364,1366,1368,1370,1372,1374,1376,1378,1380,1382,1384,1386,1388,1390,1392,1394,1396,1398,1400,1402,1404,1406,1408,1410,1412,1414,1416,1418,1420,1422

    udp-port
1124,1126,1128,1130,1132,1134,1136,1138,1140,1142,1144,1146,1148,1150,1152,1154,1156,1158,1160,1162,1164,1166,1168,1170,1172,1174,1176,1178,1180,1182,1184,1186,1188,1190,1192,1194,1196,1198,1200,2000-3000,3002,3004,3006
```

TA インターフェイスフィルタおよび VRF フィルタ

トラフィック分析機能は強化されて、既存のFTインターフェイス構成と同様に、インターフェイスと VRF の両方のレベルでフィルタ構成を使用して TCP フローをキャプチャするためのきめ細かいサポートを提供するようになりました。

この TA フィルタ構成では、次のことができます。

- モニタリングに必要な IPアドレスを構成します。
- **deny** キーワードを使用して、フロー収集を必要としない IPアドレスを構成します。
- 特定の VRF 内のすべてのインターフェイスに VRFフィルタを構成します。
- TCPパケットの許可サブネットルール（TCP SYN、SYN ACK、および TCP フラグなし）を指定します。
- プロファイル 31 と見なされる一般的な TCP パケット（SYN または SYN ACK なし）の場合、 **show flow cache** コマンドを使用して、コレクタに転送される TCS フローを停止できます。

TA インターフェイスフィルタおよび VRF フィルタの詳細については、TA インターフェイスフィルタと VRF フィルタの例 （6 ページ） を参照してください。

トラフィック分析の注意事項および制限事項

次の注意事項と制限事項がトラフィック分析に適用されます。

- トラフィック分析機能が有効になっている場合、TCP 以外の他のすべての IP プロトコルは 3 タプル情報を取得します。
- トラフィック分析機能は、スタンドアロン デバイスの混合モードでのみサポートされます。
- トラフィック分析機能を有効にする前に、フローフィルタを削除してください。削除しないと、エラー メッセージが表示されます。
- システム フロー フィルタが構成されている場合、トラフィック フローの動作は次のようになります。

- トラフィック分析データベースに情報がある場合、2 つのフローがキャッシュに表示されます。
- トラフィック分析データベースに情報がない場合、キャッシュには 1 つのフローのみが表示されます。

- トラフィック分析データベースのサイズが縮小された場合、新しいエントリは古いエントリを削除した後にのみ発生します。
- NetFlowとトラフィック分析が有効になっていて、プロファイル 29 ー 31 を使用しているスケールされた NetFlow 構成がある場合、これらのプロファイルは両方の機能に使用されます。ネイバー探索または特殊パケットがこれらのプロファイルにヒットした場合、作成されたレコードがトラフィック分析なのか NetFlow なのかを区別することはできません。その結果、パケットは 2 回処理され、AN プロファイルを持つ 2 つのパケットがあるように見えます。
- NetFlow およびフローテレメトリは、N9K-C9364C-H1 プラットフォームの SFP+ ポート、Ethernet1/65、および Ethernet1/66 ではサポートされていません。
- Cisco NX-OS リリース 10.5（2）F 以降、入力トラフィック分析は次でサポートされています。

プラットフォーム サポート

次の表に、TA 機能でサポートされているプラットフォームのリリースを示します。

機能	プラットフォーム	リリース
TA のサポート	9300-FX、-FX2、-FX3、-GX、および -GX2	10.4（2）F
TA のサポート	9300-H2R および -H1	10.4(4)M
入力 TA	9300-FX、-FX2、-FX3、-GX、-GX2、-H2R、および -H1	10.5（2）F

（注） リリースまでの機能でサポートされるプラットフォームの詳細については、『Nexus スイッチ プラットフォーム サポート マトリックス』を参照してください。

TA トラブルシューティングルールのガイドラインと制限事項

- 中断のないアップグレードを使用してCisco NX-OSリリース 10.5(1)F にアップグレードする場合、 **filter export-interval** のデフォルト値は、NetFlow **flow timeout** 値から導出されます。

トラフィック分析の構成

TA インターフェイスフィルタおよび VRF フィルタのガイドラインと制限事項

- TA インターフェイスフィルタは、ループバック、トンネルインターフェイス（NVE など）、および管理インターフェイスではサポートされません。
- TA インターフェイスフィルタは、L3 サブインターフェイスおよび L3 ポートチャネル（PO）サブインターフェイスではサポートされません。
- VRF フィルタは、デフォルトVRF および管理 VRF ではサポートされません。
- TA インターフェイスフィルタと VRF フィルタが構成されている場合は、TA インターフェイスフィルタが優先されます。

トラフィック分析の構成

トラフィック分析機能は、混合モードでのみ設定できます。

Cisco NX-OSリリース 10.5(1)F 以降では、デバッグ目的でトラフィック分析（TA）フローをトラブルシュートフローとしてマークできます。TA フローはより高速な間隔で Nexus ダッシュボードにエクスポートされます。

次の例では、トラブルシュートフローが IPv4 と IPv6 の両方の ACL リストで定義され、フローフィルタに接続されています。フローフィルタは、フローシステム構成でシステム全体で有効になっています。

始める前に

トラフィック分析機能を有効にする前に、混合モードになっていることを確認します。混合モードを有効にするには、次のコマンドを使用します。混合モードの詳細については、混合モードで構成する を参照してください。

```
(Config)#feature netflow
(Config)#feature analytics
```

手順

次の方法で、より高い頻度をサポートするように、トラフィック分析機能を構成します。

例：

```
ip access-list ipv4-global_filter
  statistics per-entry
  1 permit ip 10.1.1.2/32 11.1.1.2/32
  2 permit ip 11.1.1.2/32 10.1.1.2/32
  3 permit ip 101.1.1.2/32 111.1.1.2/32
  4 permit ip 111.1.1.2/32 101.1.1.2/32

ipv6 access-list ipv6-global_filter
  statistics per-entry
  1 permit ipv6 10::2/128 11::2/128
  2 permit ipv6 11::2/128 10::2/128
  3 permit ipv6 101::2/128 111::2/128
```

```
  4 permit ipv6 111::2/128 101::2/128

flow filter global_filter
  ipv4 ipv4-global_filter
  ipv6 ipv6-global_filter


switch(config)# feature netflow
switch(config)# feature analytics
switch(config)# analytics
switch(config-analytics)#

switch(config-analytics)#  flow traffic-analytics
switch(config-analytics-traffic-analytics)#  db-size 200
switch(config-analytics-traffic-analytics)#  filter export-interval 30
switch(config-analytics-traffic-analytics)#  flow system config
switch(config-analytics-system)#  traffic-analytics
switch(config-analytics-system)#  monitor monitor input
switch(config-analytics-system)#  profile profile
switch(config-analytics-system)#  event event
switch(config-analytics-system)#  filter global_filter
```

TA インターフェイスフィルタと VRF フィルタの例

インターフェイスフィルタの構成

次の例は、インターフェイスフィルタの構成方法を示しています。

```
ip access-list ipv4-l3_intf_filter
  statistics per-entry
  1 permit tcp 10.1.1.7/32 11.1.1.7/32 syn
  2 permit ip 10.1.1.7/32 11.1.1.7/32

ipv6 access-list ipv6-l3_intf_filter
  statistics per-entry
  1 permit tcp 10::7/128 11::7/128 syn
  2 permit ipv6 10::7/128 11::7/128

flow filter l3_filter
  ipv4 ipv4-l3_intf_filter
  ipv6 ipv6-l3_intf_filter

analytics

  flow traffic-analytics
    db-size 200
    filter export-interval 30
  flow system config
    traffic-analytics
    monitor monitor input
    profile profile
    event event

interface Ethernet1/63/1
  flow filter l3_filter

switch(config-analytics)# show running-config inter e 1/63/1
```

```
interface Ethernet1/63/1
  vrf member vrf1
  flow filter l3_filter
  ip address 10.1.1.1/24
  ipv6 address 10::1/64
  no shutdown
```

VRF フィルタの構成

次の例は、VRF フィルタの構成方法を示しています。

```
ip access-list ipv4-vrf1_filter
  statistics per-entry
  1 permit tcp 10.1.1.9/32 11.1.1.9/32 syn
  2 permit tcp 11.1.1.9/32 10.1.1.9/32 ack syn

ipv6 access-list ipv6-vrf1_filter
  statistics per-entry
  1 permit tcp 10::9/128 11::9/128 syn
  2 permit tcp 11::9/128 10::9/128 ack syn

flow filter vrf1_filter
  ipv4 ipv4-vrf1_filter
  ipv6 ipv6-vrf1_filter

analytics

  flow traffic-analytics
    db-size 200
    filter export-interval 30
  flow system config
    traffic-analytics
    monitor monitor input
    profile profile
    event event

vrf context vrf1

  flow filter vrf1_filter
```

トラフィック分析の例

次に、トラブルシュートフローのエクスポート間隔の出力例を示します。

```
switch(config-analytics-traffic-analytics)# show flow traffic-analytics
Traffic Analytics:
    Service DB Size: 200
    Troubleshoot Export Interval: 30
```

filter export-interval コマンドを使用すると、トラブルシュートタイマーを 10 ～ 60 秒の範囲で設定できます。このタイマーのデフォルト値は 10 秒に設定されます。

no filter export-interval を使用すると、トラブルシュートタイマーの範囲がデフォルト値の 60 秒にリセットされます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。