Cisco NetFlow コンフィギュレーショ

ベスト プラクティス/ハイライト
Cisco IOS NetFlow コンフィギュレーション ガイド
Cisco 6500 & 7600 NetFlow 構成ガイド
Catalyst 4500 NetFlow 構成ガイド
Cisco 3850 NetFlow 構成ガイド
Cisco 3560/3750 NetFlow コンフィギュレーション ガイド
Cisco Nexus 7000 NetFlow の構成
Cisco Nexus 1000v NetFlow の構成
Cisco ASR 9000 NetFlow の構成
付録

ベスト プラクティス/ハイライト

- NetFlow 構成はハードウェア モデルごとに若干異なります。
- アクティブ タイムアウトを 1 分に設定：「ip flow-cache timeout active」は時間間隔です。長時間存在したフロー（大規模な FTP 転送など）で NetFlow レコードがエクスポートされます。1 分が推奨値で、構成は IOS では分単位、MLS と NX-OS では 秒単位です。
- Catalyst 6500/7600 では MSFC および PFC 内で NetFlow のエクスポートを有効にする必要があります。
- 以下のコマンドでは、Catalyst の同じ VLAN 内で NetFlow がキャプチャされます。6500/7600: ip flow ingress layer2-switched vlan {vlanlist}
- NetFlow は 7 つのキー フィールドに基づいています。
  - 発信元の IP アドレス
  - 宛先 IP アドレス
  - 送信元ポート番号
  - 宛先ポート番号
  - レイヤ 3 プロトコル タイプ（例：TCP、UDP）
  - ToS（タイプ オブ サービス）バイト
  - 入力論理インターフェイス

  1 つのフィールドが異なる場合、フロー キャッシュに新しいフローが作成されます。
- 完全な可視性のためすべてのレイヤ 3 インターフェイスで NetFlow が有効になっています。
- ループバック インターフェイスなどをダウンさせることのない NetFlow の「送信元インターフェイス」を使用するのがベスト プラクティスです。
- Flexible NetFlow（NX-OS で使用されている）内の「フロー レコード」は、NetFlow で フロー内のパケットを識別するために使用するキーとともに、NetFlow がフローについて収集する関連フィールドを定義します。

ベスト プラクティス/
ハイライト

Cisco IOS NetFlow
コンフィギュレーション ガイド

Cisco 6500 & 7600 NetFlow
構成ガイド

Catalyst 4500 NetFlow
構成ガイド

Cisco 3850 NetFlow
構成ガイド

Cisco 3560/3750 NetFlow
コンフィギュレーション ガイド

Cisco Nexus 7000 NetFlow
の構成

Cisco Nexus 1000v NetFlow
の構成

Cisco ASR 9000 NetFlow
の構成

付録

『Cisco IOS NetFlow Configuration Guide』

Netflow の構成

コンフィギュレーション モードで、NetFlow エクスポートを有効にするのには次を実行します。

ip flow-export destination <xe_netflow_collector_IP_address> 2055
ip flow-export source <interface> → *(ループバック インターフェイスの使用など)*
ip flow-export version 9 → *(バージョン 9 が機能しない場合は、バージョン 5 を使用)*
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
snmp-server ifindex persist

トラフィックの監視に関心のある各レイヤ 3 インターフェイスで NetFlow を有効にします。

interface <interface>
ip flow ingress

オプション

ip flow-export version 9 origin-as → (BGP 起点 AS を含める)
ip flow-capture mac-addresses → show ip cache verbose flow
ip flow-capture vlan-id

注: ルータがリリース 12.2(14)S、12.0(22)S、または 12.2(15)T より前のバージョンの Cisco IOS を実行している場合は、ip route-cache flow コマンドを使用してインターフェイスで NetFlow を有効にします。ルータで Cisco IOS リリース 12.2(14)S、12.0(22)S、12.2(15)T またはそれ以上を実行している場合は、ip flow ingress コマンドを使用してインターフェイスで NetFlow を interface。

構成の検証

show ip cache flow
show ip flow export
show ip flow interface
show ip flow export template

参考資料:

http://www.cisco.com/en/US/docs/ios/netflow/configuration/guide/12_2sr/nf_12_2sr_book.html

ベスト プラクティス/
ハイライト

Cisco IOS NetFlow
コンフィギュレーション ガイド

Cisco 6500 & 7600 NetFlow
構成ガイド

Catalyst 4500 NetFlow
構成ガイド

Cisco 3850 NetFlow
構成ガイド

Cisco 3560/3750 NetFlow
コンフィギュレーション ガイド

Cisco Nexus 7000 NetFlow
の構成

Cisco Nexus 1000v NetFlow
の構成

Cisco ASR 9000 NetFlow
の構成

付録

Cisco 6500 および 7600 シリーズ IOS NetFlow 構成ガイド

ネイティブ IOS Netflow の構成

コンフィギュレーション モードで、NetFlow エクスポートを有効にするのには次を実行します。

```
mls nde sender version 5
mls aging long 64
mls aging normal 32
mls nde interface
mls flow ip interface-full
ip flow ingress layer2-switched vlan {vlanlist}

ip flow-export destination <xe_netflow_collector_IP_address> 2055
ip flow-export source <interface> → (ループバック インターフェイスの使用など)
ip flow-export version 9 → (バージョン 9 が機能しない場合は、バージョン 5 を使用)
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
snmp-server ifindex persist
```

トラフィックの監視に関心のある各レイヤ 3 インターフェイスで NetFlow を有効にします。

```
interface <interface>
ip flow ingress
```

オプション

```
ip flow-capture mac-addresses
ip flow-capture vlan-id
```

ハイブリッド/CatOS Netflow の構成

```
set mls nde <xe_address> 2055
set mls nde version 5
set mls agingtime long 64
set mls agingtime 32
set mls flow full
set mls bridged-flow-statistics enable <vlanlist>
set mls nde enable
```

設定の検証

```
show ip cache flow
show ip flow export
show ip flow export template
show mls nde
```

参考資料:

http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SXF/configuration/guide/nde.html

ベスト プラクティス/ハイライト
Cisco IOS NetFlow コンフィギュレーション ガイド
Cisco 6500 & 7600 NetFlow 構成ガイド
Catalyst 4500 NetFlow 構成ガイド
Cisco 3850 NetFlow 構成ガイド
Cisco 3560/3750 NetFlow コンフィギュレーション ガイド
Cisco Nexus 7000 NetFlow の構成
Cisco Nexus 1000v NetFlow の構成
Cisco ASR 9000 NetFlow の構成
付録

Catalyst 4500 シリーズ スイッチ IOS NetFlow 構成ガイド

NetFlow 機能を使用するには、Supervisor Engine V-10GE (機能はスーパーバイザ エンジンに組み込まれている) 、または NetFlow Services Card (WS-F4531) および Supervisor Engine IV か Supervisor Engine V が必要です。

ドーター カードの確認

Switch# show module all

.

<簡略化のため省略>

Mod	サブモジュール	モデル	Serial No.	Hw	Status (ステータス)
1.	Netflow サービス カード	WS F4531	JAB062209CG	0.2	Ok
2.	Netflow サービス カード	WS F4531	JAB062209CG	0.2	Ok

Netflow の構成

4500 のコンフィギュレーション モードで、NetFlow エクスポートを有効にするには次を実行します。

```
ip flow ingress
ip flow ingress infer-fields
ip flow-export destination <xe_netflow_collector_IP_address> 2055
ip flow-export source <interface> → (ループバック インターフェイスの使用など)
ip flow-export version 5
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
snmp-server ifindex persist
```

設定の検証

```
show ip cache flow
show ip flow export
show ip flow interface
```

参考資料:

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/25ew/configuration/guide/nfswitch.html

ベスト プラクティス/
ハイライト

Cisco IOS NetFlow
コンフィギュレーション ガイド

Cisco 6500 & 7600 NetFlow
構成ガイド

Catalyst 4500 NetFlow
構成ガイド

Cisco 3850 NetFlow
構成ガイド

Cisco 3560/3750 NetFlow
コンフィギュレーション ガイド

Cisco Nexus 7000 NetFlow
の構成

Cisco Nexus 1000v NetFlow
の構成

Cisco ASR 9000 NetFlow
の構成

付録

Cisco 3850 NetFlow の構成

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告と機能情報については、「Cisco Bug Search Tool」と使用するプラットフォームとソフトウェア リリースのリリース ノートを参照してください。

1. フロー レコードの作成（エクスポートするフィールドの指定）

フロー レコードは、フロー内のパケット、フローごとに収集されるカウンタのタイプなどの NetFlow が収集する情報を定義します。一連の「match」および「collect」コマンドを指定して、発信 NetFlow PDU に含めるフィールドをルータに伝える必要があります。

「match」フィールドはキー フィールドです。これらのフィールドは、フローの一意性を判断するために使用されます。「collect」フィールドは単なる追加情報であり、コレクタにレポートと分析のための詳細を提供するものです。

下記で「必須」と記載されているフィールドは、Stealthwatch がフロー レコードを受け入れて作成するために必要なフィールドです。

```
sw3850(config)# flow record LANCOPE1
sw3850(config-flow-record)# description NetFlow record format to send to StealthWatch
sw3850(config-flow-record)# match datalink mac source address input
sw3850(config-flow-record)# match datalink mac destination address input
sw3850(config-flow-record)# match datalink vlan input                  キー フィールド
sw3850(config-flow-record)# match ipv4 ttl                             キー フィールド。パス情報を提供
sw3850(config-flow-record)# match ipv4 tos                             必須。キー フィールド
sw3850(config-flow-record)# match ipv4 protocol                        必須。キー フィールド
sw3850(config-flow-record)# match ipv4 source address                  必須。キー フィールド
sw3850(config-flow-record)# match ipv4 destination address             必須。キー フィールド
sw3850(config-flow-record)# match transport source-port                必須。キー フィールド
sw3850(config-flow-record)# match transport destination-port           必須。キー フィールド
sw3850(config-flow-record)# match interface input                      必須。キー フィールド
sw3850(config-flow-record)# collect interface output                   必須。bps レートの計算に使用
sw3850(config-flow-record)# collect counter bytes long                 必須。bps の計算に使用
sw3850(config-flow-record)# collect counter packets long               必須。pps の計算に使用
sw3850(config-flow-record)# collect timestamp absolute first           必須。時間の計算に使用
sw3850(config-flow-record)# collect timestamp absolute last            必須。時間用
```

ベスト プラクティス/
ハイライト

Cisco IOS NetFlow
コンフィギュレーション ガイド

Cisco 6500 & 7600 NetFlow
構成ガイド

Catalyst 4500 NetFlow
構成ガイド

Cisco 3850 NetFlow
構成ガイド

Cisco 3560/3750 NetFlow
コンフィギュレーション ガイド

Cisco Nexus 7000 NetFlow
の構成

Cisco Nexus 1000v NetFlow
の構成

Cisco ASR 9000 NetFlow
の構成

付録

Cisco 3850 NetFlow の構成

2. フロー エクスポータの作成 (NetFlow の送信場所と方法を指定)

```
sw3850(config)#flow exporter NETFLOW_TO_STEALTHWATCH
sw3850(config-flow-exporter)#description Export NetFlow to StealthWatch
sw3850(config-flow-exporter)#destination <fc_collector_IP_address>
sw3850(config-flow-exporter)#source <interface> → (ループバックの使用など)
sw3850(config-flow-exporter)#transport udp 2055
```

3. フロー モニタの作成 (フロー レコードをフロー エクスポートに結びつける)

```
sw3850(config)#flow monitor IPv4_NETFLOW
sw3850(config-flow-monitor)#record LANCOPE1
sw3850(config-flow-monitor)#exporter NETFLOW_TO_STEALTHWATCH
sw3850(config-flow-monitor)#cache timeout active 60
```

4. 選択したインターフェイスへのフロー モニタの割り当て

トラフィックの監視に関心のあるすべてのインターフェイスでこの手順を繰り返します。

```
sw3850(config)#interface <interface> → (VLAN1 または g2/1 など)
sw3850(config-if)#ip flow monitor IPv4_NETFLOW input
```

構成の検証

```
show flow record LANCOPE1
show flow monitor IPv4_NETFLOW statistics
show flow monitor IPv4_NETFLOW cache
```

参考資料:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/flexible_netflow/command_reference/b_fnf_32se_3850_cr_chapter_010.html

ベスト プラクティス/
ハイライト

Cisco IOS NetFlow
コンフィギュレーション ガイド

Cisco 6500 & 7600 NetFlow
構成ガイド

Catalyst 4500 NetFlow
構成ガイド

Cisco 3850 NetFlow
構成ガイド

Cisco 3560/3750 NetFlow
コンフィギュレーション ガイド

Cisco Nexus 7000 NetFlow
の構成

Cisco Nexus 1000v NetFlow
の構成

Cisco ASR 9000 NetFlow
の構成

付録

Cisco 3560X および 3750X NetFlow の構成

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告と機能情報については、「Cisco Bug Search Tool」とプラットフォームおよびソフトウェアリリースのリリース ノートを参照してください。

Flexible NetFlow は 10GE サービス モジュールの Catalyst 3560-X および 3750-X (Cat3k-X) シリーズスイッチでサポートされています。以前プラットフォームでサポートされていなかったサービス モジュールは、モジュールを通過するすべてのトラフィックでハードウェアでサポートされるラインレート NetFlow を有効にできます。

1. フロー レコードの作成 (エクスポートするフィールドの指定)

フロー レコードは、フロー内のパケット、フローごとに収集されるカウンタのタイプなどの NetFlow が収集する情報を定義します。一連の「match」および「collect」コマンドを指定して、発信 NetFlow PDU に含めるフィールドをデバイスに伝える必要があります。「match」フィールドは「key」フィールドです。これらのフィールドは、フローの一意性を判断するために使用されます。「collect」フィールド単なる追加情報であり、コレクタにレポートと分析のための詳細を提供するものです。

下記で「必須」と記載されているフィールドは、Stealthwatch がフロー レコードを受け入れて作成するために必要なフィールドです。

```
sw3X50(config)# flow record LANCOPE1
sw3X50(config-flow-record)# description NetFlow record format to send to StealthWatch
sw3X50(config-flow-record)# match datalink mac source address input
sw3X50(config-flow-record)# match datalink mac destination address input
sw3X50(config-flow-record)# match ipv4 ttl                          キー フィールド。パス情報を提供
sw3X50(config-flow-record)# match ipv4 tos                          必須。キー フィールド
sw3X50(config-flow-record)# match ipv4 protocol                     必須。キー フィールド
sw3X50(config-flow-record)# match ipv4 source address               必須。キー フィールド
sw3X50(config-flow-record)# match ipv4 destination address          必須。キー フィールド
sw3X50(config-flow-record)# match transport source-port             必須。キー フィールド
sw3X50(config-flow-record)# match transport destination-port        必須。キー フィールド
sw3X50(config-flow-record)# collect interface input snmp            必須。キー フィールド
sw3X50(config-flow-record)# collect interface output snmp           必須。
sw3X50(config-flow-record)# collect counter bytes                   必須。bps の計算に使用
sw3X50(config-flow-record)# collect counter packets                 必須。pps の計算に使用
sw3X50(config-flow-record)# collect timestamp sys-uptime first      必須。時間用
sw3X50(config-flow-record)# collect timestamp sys-uptime last       必須。時間用
```

ベスト プラクティス/
ハイライト

Cisco IOS NetFlow
コンフィギュレーション ガイド

Cisco 6500 & 7600 NetFlow
構成ガイド

Catalyst 4500 NetFlow
構成ガイド

Cisco 3850 NetFlow
構成ガイド

Cisco 3560/3750 NetFlow
コンフィギュレーション ガイド

Cisco Nexus 7000 NetFlow
の構成

Cisco Nexus 1000v NetFlow
の構成

Cisco ASR 9000 NetFlow
の構成

付録

Cisco 3560X および 3750X NetFlow の構成

2. フロー エクスポータの作成 (NetFlow の送信場所と方法を指定)

```
sw3x50(config)#flow exporter NETFLOW_TO_STEALTHWATCH
sw3x50(config-flow-exporter)#description Export NetFlow to StealthWatch
sw3x50(config-flow-exporter)#destination <fc_collector_IP_address>
sw3x50(config-flow-exporter)#source <interface> → (ループバックの使用など)
sw3x50(config-flow-exporter)#transport udp 2055
```

3. フロー モニタの作成 (フロー レコードをフロー エクスポートに結びつける)

```
sw3x50(config)#flow monitor IPv4_NETFLOW
sw3x50(config-flow-monitor)#レコード LANCOPE1
sw3x50(config-flow-monitor)#exporter NETFLOW_TO_STEALTHWATCH
sw3x50(config-flow-monitor)#cache timeout active 60
```

4. 選択したインターフェイスへのフロー モニタの割り当て

トラフィックの監視に関心のあるすべてのインターフェイスでこの手順を繰り返します。

```
sw3x50(config)#interface <interface> → (VLAN1 または g2/1 など)
sw3x50(config-if)#ip flow monitor IPv4_NETFLOW input
```

構成の検証

```
show flow record LANCOPE1
show flow monitor IPv4_NETFLOW statistics
show flow monitor IPv4_NETFLOW cache
```

参考資料:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps10745/white_paper_c11-691508_ps10744_Products_White_Paper.html

ベスト プラクティス/
ハイライト

Cisco IOS NetFlow
コンフィギュレーション ガイド

Cisco 6500 & 7600 NetFlow
構成ガイド

Catalyst 4500 NetFlow
構成ガイド

Cisco 3850 NetFlow
構成ガイド

Cisco 3560/3750 NetFlow
コンフィギュレーション ガイド

Cisco Nexus 7000 NetFlow
の構成

Cisco Nexus 1000v NetFlow
の構成

Cisco ASR 9000 NetFlow
の構成

付録

Cisco Nexus 7000 NetFlow の構成：netflow-original の使用

Cisco Nexus 7000 スイッチでは、Cisco NX-OS オペレーティング システムが実行されます。Netflow の構成は、従来の IOS デバイスと若干異なります。次の 5 つの手順に従って Netflow の監視を有効にします。

1. Netflow 機能を有効にして、タイムアウトを設定

```
switch(config)#feature netflow
switch(config)#flow timeout active 60
switch(config)#flow timeout inactive 15
```

2. フロー レコードの作成（エクスポートするフィールドの指定）

この構成では Nexus で事前定義されている「netflow-original」のレコードを設定を表示します。カスタム フロー レコードの作成については、付録の「*フロー レコード*」セクションを参照してください。

3. フロー エクスポータの作成（NetFlow の送信場所と方法を指定）

```
switch(config)#flow exporter netflow_to_stealthwatch
switch(config-flow-exporter)#description Export NetFlow to StealthWatch
switch(config-flow-exporter)#destination <xe_collector_IP_address>
switch(config-flow-exporter)#source <interface> → (ループバックの使用など)
switch(config-flow-exporter)#transport udp 2055
switch(config-flow-exporter)#version 9
```

4. フロー モニタの作成（フロー レコードをフロー エクスポートに結びつける）

```
switch(config)#flow monitor standard_v9netflow
switch(config-flow-monitor)#record netflow-original
switch(config-flow-monitor)#exporter netflow_to_stealthwatch
```

5. 選択したインターフェイスへのフロー モニタの割り当て

トラフィックの監視に関心のあるすべてのインターフェイスでこの手順を繰り返します。

```
switch(config)#interface <interface> → (VLAN1 または g2/1 など)
switch(config-if)#ip flow monitor standard_v9netflow input
```

構成の検証

```
show flow record netflow-original
show flow monitor standard_v9netflow statistics
show flow monitor standard_v9netflow cache
```

参考資料:

http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/system_management/configuration/guide/sm_netflow.html

ベスト プラクティス/
ハイライト

Cisco IOS NetFlow
コンフィギュレーション ガイド

Cisco 6500 & 7600 NetFlow
構成ガイド

Catalyst 4500 NetFlow
構成ガイド

Cisco 3850 NetFlow
構成ガイド

Cisco 3560/3750 NetFlow
コンフィギュレーション ガイド

Cisco Nexus 7000 NetFlow
の構成

Cisco Nexus 1000v NetFlow
の構成

Cisco ASR 9000 NetFlow
の構成

付録

Cisco Nexus 1000v NetFlow の構成：netflow-original の使用

Cisco Nexus 1000v スイッチは、Cisco NX-OS を実行する仮想スイッチです。Netflow の構成は、従来の IOS デバイスでより少し異なります。次の 4 つの手順に従って Netflow の監視を有効にします。

1. フロー レコードの作成（エクスポートするフィールドの指定）

   この構成では Nexus で事前定義されている「netflow-original」のレコードを設定を表示します。カスタム フロー レコードの作成については、付録のフロー レコードに関するセクションを参照してください。

2. フロー エクスポータの作成（NetFlow の送信場所と方法を指定）

```
n1000v(config)#flow exporter netflow_to_stealthwatch
n1000v(config-flow-exporter)#description Export NetFlow to StealthWatch
n1000v(config-flow-exporter)#destination <xe_collector_IP_address>
n1000v(config-flow-exporter)#source mgmt 0
n1000v(config-flow-exporter)#transport udp 2055
n1000v(config-flow-exporter)#version 9
```

3. フロー モニタの作成（フロー レコードをフロー エクスポートに結びつける）

```
n1000v(config)#flow monitor standard_v9netflow
n1000v(config-flow-monitor)#record netflow-original
n1000v(config-flow-monitor)#exporter netflow_to_stealthwatch
n1000v(config-flow-monitor)#timeout active 60
n1000v(config-flow-monitor)#timeout inactive 15
```

4. 選択したインターフェイスへのフロー モニタの割り当て

トラフィックの監視に関心のあるすべてのインターフェイスでこの手順を繰り返します。

```
n1000v(config)#interface <interface> → (VLAN1 または g2/1 など)
n1000v(config-if)#ip flow monitor standard_v9netflow input
```

構成の検証

```
show flow record netflow-original
show flow monitor standard_v9netflow statistics
show flow monitor standard_v9netflow cache
```

参考資料:

http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0/system_management/configuration/guide/system_9flow.html

ベスト プラクティス/
ハイライト

Cisco IOS NetFlow
コンフィギュレーション ガイド

Cisco 6500 & 7600 NetFlow
構成ガイド

Catalyst 4500 NetFlow
構成ガイド

Cisco 3850 NetFlow
構成ガイド

Cisco 3560/3750 NetFlow
コンフィギュレーション ガイド

Cisco Nexus 7000 NetFlow
の構成

Cisco Nexus 1000v NetFlow
の構成

Cisco ASR 9000 NetFlow
の構成

付録

Cisco ASR 1000 NetFlow の構成

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告と機能情報については、「Cisco Bug Search Tool」とプラットフォームおよびソフトウェアリリースのリリース ノートを参照してください。

Flexible NetFlow は 10GE サービス モジュールの Catalyst 3560-X および 3750-X (Cat3k-X) シリーズスイッチでサポートされています。以前プラットフォームでサポートされていなかったサービス モジュールは、モジュールを通過するすべてのトラフィックでハードウェアでサポートされるラインレート NetFlow をイネーブルにできます。

1. フロー レコードの作成 (エクスポートするフィールドの指定)

フロー レコードは、フロー内のパケット、フローごとに収集されるカウンタのタイプなどの NetFlow が収集する情報を定義します。一連の「match」および「collect」コマンドを指定して、発信 NetFlow PDU に含めるフィールドをデバイスに伝える必要があります。「match」フィールドは「key」フィールドです。これらのフィールドは、フローの一意性を判断するために使用されます。「collect」フィールド単なる追加情報であり、コレクタにレポートと分析のための詳細を提供するものです。

下記で「必須」と記載されているフィールドは、Stealthwatch がフロー レコードを受け入れて作成するために必要なフィールドです。

asr1k(config)# **flow record LANCOPE1**	
asr1k(config-flow-record)#**match ipv4 protocol**	*必須。キー フィールド*
asr1k(config-flow-record)#**match ipv4 source address**	*必須。キー フィールド*
asr1k(config-flow-record)#**match ipv4 destination address**	*必須。キー フィールド*
asr1k(config-flow-record)#**match transport source-port**	*必須。キー フィールド*
asr1k(config-flow-record)#**match transport destination-port**	*必須。キー フィールド*
asr1k(config-flow-record)#**match interface input**	*必須。キー フィールド*
asr1k(config-flow-record)#**match ipv4 tos**	*必須。キー フィールド*
asr1k(config-flow-record)#**collect interface output**	*必須。bps レートの計算に使用*
asr1k(config-flow-record)#**collect counter bytes**	*必須。bps の計算に使用*
asr1k(config-flow-record)#**collect counter packets**	*必須。pps の計算に使用*
asr1k(config-flow-record)#**collect timestamp sys-uptime first**	*必須。時間の計算に使用*
asr1k(config-flow-record)#**collect timestamp sys-uptime last**	*必須。時間の計算に使用*
asr1k(config-flow-record)#**collect flow sampler**	*オプション。サンプリング レートの取得に使用*
asr1k(config-flow-record)#**collect routing next-hop address ipv4**	*オプション。最も近いインターフェイスの判別に使用*
asr1k(config-flow-record)#**collect ipv4 dscp**	*オプション。QoS レポートを生成するために使用*
asr1k(config-flow-record)#**collect ipv4 ttl minimum**	*オプション。パス情報を提供*
asr1k(config-flow-record)#**collect ipv4 ttl maximum**	*オプション。パス情報を提供*
asr1k(config-flow-record)#**collect transport tcp flags**	*オプション。セキュリティ分析*
asr1k(config-flow-record)#**collect routing destination as**	*オプション。BGP を使用する場合に有効化*

ベスト プラクティス/
ハイライト

Cisco IOS NetFlow
コンフィギュレーション ガイド

Cisco 6500 & 7600 NetFlow
構成ガイド

Catalyst 4500 NetFlow
構成ガイド

Cisco 3850 NetFlow
構成ガイド

Cisco 3560/3750 NetFlow
コンフィギュレーション ガイド

Cisco Nexus 7000 NetFlow
の構成

Cisco Nexus 1000v NetFlow
の構成

Cisco ASR 9000 NetFlow
の構成

付録

Cisco ASR 1000 NetFlow の構成

6. フロー エクスポータの作成 (NetFlow の送信場所と方法を指定)

```
asr1k(config)#flow exporter NETFLOW_TO_STEALTHWATCH
asr1k(config-flow-exporter)#description Export NetFlow to StealthWatch
asr1k(config-flow-exporter)#destination <fc_collector_IP_address>
asr1k(config-flow-exporter)#source <interface> → (ループバックの使用など)
asr1k(config-flow-exporter)#transport udp 2055
asr1k(config-flow-exporter)#version 9
```

7. フロー モニタの作成 (フロー レコードをフロー エクスポートに結びつける)

```
asr1k(config)#flow monitor IPv4_NETFLOW
asr1k(config-flow-monitor)#record LANCOPE1
asr1k(config-flow-monitor)#exporter NETFLOW_TO_STEALTHWATCH
asr1k(config-flow-monitor)#cache timeout active 60
asr1k(config-flow-monitor)#cache timeout inactive 15
```

8. 選択したインターフェイスへのフロー モニタの割り当て

トラフィックの監視に関心のあるすべてのインターフェイスでこの手順を繰り返します。

```
asr1k(config)#interface <interface> → (VLAN1 または g2/1 など)
asr1k(config-if)#ip flow monitor IPv4_NETFLOW input
```

ASR が NAT に使用されていて、StealthWatch 内での NAT 変換をログに記録する場合は、次のコマンドを実行します。

ip nat log translations flow-export v9 udp destination *X.X.X.X YYYY*

X.X.X.X は FlowCollector IP で、YYYY は設定されている NetFlow エクスポート ポートです。

構成の検証

```
show flow record LANCOPE1
show flow monitor IPv4_NETFLOW statistics
show flow monitor IPv4_NETFLOW cache
```

参考資料:

http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/xe-3s/asr1000/cfg-de-fnflow-exprts-xe.html
http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/xe-3s/cfg-avc-xe.html

ベスト プラクティス/
ハイライト

Cisco IOS NetFlow
コンフィギュレーション ガイド

Cisco 6500 & 7600 NetFlow
構成ガイド

Catalyst 4500 NetFlow
構成ガイド

Cisco 3850 NetFlow
構成ガイド

Cisco 3560/3750 NetFlow
コンフィギュレーション ガイド

Cisco Nexus 7000 NetFlow
の構成

Cisco Nexus 1000v NetFlow
の構成

Cisco ASR 9000 NetFlow
の構成

付録

Cisco ASR 9000 NetFlow の構成

Cisco IOS XR で NetFlow を構成する場合は、次の制限を考慮します。ソフトウェア：送信元インターフェイスを構成する必要があります。送信元インターフェイスを構成しなかった場合、エクスポータはディセーブル ステートのままです。Cisco IOS XR ソフトウェアエクスポート フォーマット バージョン 9 だけをサポートします。すべてのフロー モニタ マップに対して有効なレコード マップを構成する必要があります。詳細な手順については、以下の参照リンクを参照してください。ASR9000 はフローエクスポートをサンプリングでき、Lancope では、100 % の可視性とアカウンティングのためにできる限り export 1:1 を推奨しています。これは展開されている環境に固有です。

1. エクスポータ マップの設定

```
router(config)# flow exporter-map FLOW_TO_SW
router(config- FLOW_TO_SW)# destination <xe_collector_IP_address>
router(config- FLOW_TO_SW)# source <interface> → (ループバックの使用など)
router(config- FLOW_TO_SW)# transport udp 2055
router(config- FLOW_TO_SW)# version v9
```

2. モニタ マップの設定

```
router(config)# flow monitor-map IPv4_NETFLOW
router(config- IPv4_NETFLOW)# record ipv4
router(config- IPv4_NETFLOW)# cache timeout active 60
router(config- IPv4_NETFLOW)# cache timeout inactive 15
router(config- IPv4_NETFLOW)# exporter FLOW_TO_SW
```

3. モニタ マップのインターフェイスへの適用

```
router(config)# interface <interface> → (gigabitEthernet 0/0/0/0 など)
router(config-if)# flow ipv4 monitor IPv4_NETFLOW ingress
```

構成の検証

```
show flow exporter-map FLOW_TO_SW
show flow monitor-map IPv4_NETFLOW
```

参考資料:

http://www.cisco.com/en/US/docs/routers/asr9000/software/asr9k_r3.9.1/netflow/configuration/guide/nfc391flow.html

ベスト プラクティス/
ハイライト

Cisco IOS NetFlow
コンフィギュレーション ガイド

Cisco 6500 & 7600 NetFlow
構成ガイド

Catalyst 4500 NetFlow
構成ガイド

Cisco 3850 NetFlow
構成ガイド

Cisco 3560/3750 NetFlow
コンフィギュレーション ガイド

Cisco Nexus 7000 NetFlow
の構成

Cisco Nexus 1000v NetFlow
の構成

Cisco ASR 9000 NetFlow
の構成

付録

IPv6 NetFlow エクスポート

IPv6 NetFlow エクスポートの詳細については、以下の参照リンクを参照してください。

コンフィギュレーション モードで、NetFlow エクスポートを有効にするのには次を実行します。

```
ipv6 flow-export destination <xe_netflow_collector_IP_address> 2055
ip flow-export source <interface> → (ループバック インターフェイスの使用など)
ipv6 flow-export version 9
ipv6 flow-cache timeout active 1
ipv6 flow-cache timeout inactive 15
snmp-server ifindex persist
```

トラフィックの監視に関心のある各レイヤ 3 インターフェイスで NetFlow を有効にします。

```
interface <interface>
ipv6 flow ingress
```

オプション

ipv6 flow-export version 9 origin-as → *(BGP 起点 AS を含める)*

構成の検証

```
show ip cache flow
```

参考資料:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-netflow.html
http://www.cisco.com/en/US/docs/ios/netflow/configuration/guide/nfv9_ipv6.html

ベスト プラクティス/
ハイライト

Cisco IOS NetFlow
コンフィギュレーション ガイド

Cisco 6500 & 7600 NetFlow
構成ガイド

Catalyst 4500 NetFlow
構成ガイド

Cisco 3850 NetFlow
構成ガイド

Cisco 3560/3750 NetFlow
コンフィギュレーション ガイド

Cisco Nexus 7000 NetFlow
の構成

Cisco Nexus 1000v NetFlow
の構成

Cisco ASR 9000 NetFlow
の構成

付録

付録:フロー レコードの作成と各種 show コマンド

フロー レコードの作成

フロー レコードは、フロー内のパケット、フローごとに収集されるカウンタのタイプなどの NetFlow が収集する情報を定義します。あらかじめ定義された「netflow-original」以外のカスタム フロー レコードを作成する場合は、一連の「match」コマンドと「collect」コマンドを指定して、送信 NetFlow PDU に含めるフィールドをルータに指示します。

「match」フィールドは「key」フィールドです。これらのフィールドは、フローの一意性を判断するために使用されます。「collect」フィールドは単なる追加情報であり、コレクタにレポートと分析のための詳細を提供するものです。

「match」フィールドについては、それほど変更する必要はありません。次の例に示されている 7 つの match エントリは、常に FnF 設定に含まれている必要があります。ただし、「collect」フィールドは、コレクタに送信する情報によって大きく異なる場合があります。以下の構成はすべての StealthWatch インストールで推奨されます。

下記で「必須」と記載されているフィールドは、Stealthwatch がフロー レコードを受け入れて作成するために必要なフィールドです。

switch(config)#**flow record LANCOPE1**	
switch(config-flow-record)#**match ipv4 protocol**	*必須。キー フィールド*
switch(config-flow-record)#**match ipv4 source address**	*必須。キー フィールド*
switch(config-flow-record)#**match ipv4 destination address**	*必須。キー フィールド*
switch(config-flow-record)#**match transport source-port**	*必須。キー フィールド*
switch(config-flow-record)#**match transport destination-port**	*必須。キー フィールド*
switch(config-flow-record)#**match interface input**	*必須。キー フィールド*
switch(config-flow-record)#**match ipv4 tos**	*必須。キー フィールド*
switch(config-flow-record)#**collect interface output**	*必須。bps レートの計算に使用*
switch(config-flow-record)#**collect counter bytes**	*必須。bps の計算に使用*
switch(config-flow-record)#**collect counter packets**	*必須。pps の計算に使用*
switch(config-flow-record)#**collect timestamp sys-uptime first**	*必須。時間の計算に使用*
switch(config-flow-record)#**collect timestamp sys-uptime last**	*必須。時間の計算に使用*
switch(config-flow-record)#**collect routing next-hop address ipv4**	*オプション。最も近いインターフェイスの判別に使用*
switch(config-flow-record)#**collect ipv4 dscp**	*オプション。QoS レポートを生成するためにレポート*
switch(config-flow-record)#**collect ipv4 ttl minimum**	*オプション。パス情報を提供*
switch(config-flow-record)#**collect ipv4 ttl maximum**	*オプション。パス情報を提供*
switch(config-flow-record)#**collect transport tcp flags**	*省略可能。セキュリティ文政*
switch(config-flow-record)#**collect routing destination as**	*オプション。BGP を使用する場合に有効化*

「フロー レコード」が作成されたら、「フロー モニタ」と関連付けます。

参考資料:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/ps6965/prod_white_paper0900aecd804be1cc.html

ベスト プラクティス/
ハイライト

Cisco IOS NetFlow
コンフィギュレーション ガイド

Cisco 6500 & 7600 NetFlow
構成ガイド

Catalyst 4500 NetFlow
構成ガイド

Cisco 3850 NetFlow
構成ガイド

Cisco 3560/3750 NetFlow
コンフィギュレーション ガイド

Cisco Nexus 7000 NetFlow
の構成

Cisco Nexus 1000v NetFlow
の構成

Cisco ASR 9000 NetFlow
の構成

付録

show ip cache flow

```
LCHQSW01#show ip cache flow

------------------------------------------------------------------------------

Displaying software-switched flow entries on the MSFC in Module 5:

IP packet size distribution (116635425 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .074 .016 .005 .004 .010 .004 .007 .000 .001 .000 .002 .002 .001 .005

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .003 .007 .063 .787 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  136 active, 3960 inactive, 2812503 added
  93810001 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 33992 bytes
  272 active, 752 inactive, 5624981 added, 2812503 added to flow
  0 alloc failures, 15446 force free
  1 chunk, 840 chunks added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet        3008      0.0         2    43      0.0       6.9      15.4
TCP-FTP             10      0.0         1    52      0.0       1.8      15.4
TCP-WWW          13984      0.0       938  1491     23.1       0.3       1.7
TCP-SMTP            27      0.0         1    45      0.0       0.7      15.4
TCP-other        46023      0.0       180    48     14.6      14.4      15.3
UDP-DNS          75959      0.1         1    68      0.1       0.4      14.2
UDP-NTP           8009      0.0         1    76      0.0       0.0      15.4
UDP-other      2622929      4.6        35  1231    165.9      19.2      11.2
ICMP             24379      0.0        32   558      1.3      38.6       7.7
IGMP                18      0.0         1    39      0.0       1.0      15.5
IP-other         17907      0.0        13    60      0.4      58.6       1.8
Total:         2812253      4.9        41  1168    205.7      18.9      11.2

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Vl240         209.182.184.1   Null          10.202.4.91     11 C39D 0807    17
Vl240         209.182.184.1   Null          10.202.4.90     11 C39D 0807    17
Vl240         209.182.184.1   Null          10.202.2.164    11 C39D 0807    17
Vl240         209.182.184.1   Null          10.202.2.163    11 C39D 0807    17
Vl240         209.182.184.1   Null          10.202.2.216    11 C39D 0807    17
Vl240         209.182.184.1   Null          10.202.2.215    11 C39D 0807    17
Vl240         209.182.184.1   Null          10.202.2.213    11 C39D 0807    17
Vl240         10.201.1.162    Null          10.203.7.4      11 8006 0807    66
 --More--
```

show ip flow export

```
LCHQSW01#show ip flow export
Flow export v9 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Source(1)       10.201.0.1 (Vlan1)
    Destination(1)  10.203.1.108 (2055)
  Version 9 flow records
  2837811 flows exported in 129115 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  11 export packets were dropped due to no fib
  16 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
  0 export packets were dropped enqueuing for the RP
  0 export packets were dropped due to IPC rate limiting
```

ベスト プラクティス/
ハイライト

Cisco IOS NetFlow
コンフィギュレーション ガイド

Cisco 6500 & 7600 NetFlow
構成ガイド

Catalyst 4500 NetFlow
構成ガイド

Cisco 3850 NetFlow
構成ガイド

Cisco 3560/3750 NetFlow
コンフィギュレーション ガイド

Cisco Nexus 7000 NetFlow
の構成

Cisco Nexus 1000v NetFlow
の構成

Cisco ASR 9000 NetFlow
の構成

付録

show ip flow interface

```
lchome1#show ip flow interface
Dot11Radio0
  ip flow ingress
FastEthernet4
  ip flow ingress
Vlan1
  ip flow ingress
BVI1
  ip flow ingress
```

show ip flow export template

```
LCHQSW01#show ip flow export template
   Template Options Flag = 1
   Total number of Templates added = 3
   Total active Templates = 3
   Flow Templates active = 2
   Flow Templates added = 2
   Option Templates active = 1
   Option  Templates added = 1
   Template ager polls = 1132420
   Option Template ager polls = 566291
Main cache version 9 export is enabled
 Template export information
   Template timeout = 30
   Template refresh rate = 20
 Option export information
   Option timeout = 30
   Option refresh rate = 20
```

show mls nde

```
LCHQSW01#show mls nde
 Netflow Data Export enabled
 Exporting flows to  10.203.1.108 (2055)
 Exporting flows from 10.201.0.1 (53191)
 Version: 9
 Layer2 flow creation is enabled on vlan 1,168,192,201-204,208-209,240
 Layer2 flow export is enabled on vlan 1,168,192,201-204,208-209,240
 Include Filter not configured
 Exclude Filter not configured
 Total Netflow Data Export Packets are:
    1177779 packets, 0 no packets, 37561689 records
 Total Netflow Data Export Send Errors:
        IPWRITE_NO_FIB = 0
        IPWRITE_ADJ_FAILED = 0
        IPWRITE_PROCESS = 0
        IPWRITE_ENQUEUE_FAILED = 0
        IPWRITE_IPC_FAILED = 0
        IPWRITE_OUTPUT_FAILED = 0
        IPWRITE_MTU_FAILED = 0
        IPWRITE_ENCAPFIX_FAILED = 0
 Netflow Aggregation Disabled
```

show run | inc mls

```
LCHQSW01#show run | inc mls
mls aging long 64
mls aging normal 32
mls netflow interface
mls flow ip interface-full
mls nde sender
mls cef error action reset
```

ベスト プラクティス/
ハイライト

Cisco IOS NetFlow
コンフィギュレーション ガイド

Cisco 6500 & 7600 NetFlow
構成ガイド

Catalyst 4500 NetFlow
構成ガイド

Cisco 3850 NetFlow
構成ガイド

Cisco 3560/3750 NetFlow
コンフィギュレーション ガイド

Cisco Nexus 7000 NetFlow
の構成

Cisco Nexus 1000v NetFlow
の構成

Cisco ASR 9000 NetFlow
の構成

付録

show l3-mgr flowmask

```
LCHQSW01#show l3-mgr flowmask
 current flowmask registries for protocol:
 |-----------------------------------------|
 | fmask\idx|    00    |    01    |    10    |
 |----------+----------+----------+----------|
 |    ip    |   null   |  if-full |   null   |
 |----------+----------+----------+----------|
 |   ipv6   |   null   |   null   |   null   |
 |----------+----------+----------+----------|
 |   mpls   |   null   |   null   |   null   |
 |----------+----------+----------+----------|
 |   mac    |   null   |   null   |   null   |
 |----------+----------+----------+----------|
 NDE for IPv4 is NOT globally enabled!

 l3_mgr_fmask_pending[proto/val]: [ipv6/ no]
 l3_mgr_fie_was_busy[proto/val]:   [ipv6/ no]
 l3_mgr_flowmask[proto:context/fmaskpak_count]: [ipv6: 0 / 1]
 l3_mgr_current_cli_fmask[prot/val]:  [ip  /  if-full ]
 current ip   flowmask for unicast:   if-full
 current ipv6 flowmask for unicast:    null
```

show mls netflow table-contention summary

```
LCHQSW01#show mls netflow table-contention summary
Earl in Module 5
Summary of Netflow CAM Utilization (as a percentage)
=====================================================
TCAM Utilization              :    2%
ICAM Utilization              :    0%
Netflow Creation Failures     :    0
Netflow CAM aliases           :    0
```

show mls netflow ip

```
LCHQSW01#show mls netflow ip
Displaying Netflow entries in Active Supervisor EARL in module 5
DstIP            SrcIP            Prot:SrcPort:DstPort  Src i/f          :AdjPtr
------------------------------------------------------------------------------
Pkts          Bytes          Age   LastSeen  Attributes
-----------------------------------------------------
10.203.0.10      10.201.3.53      tcp :3544   :5222      Vl1              :0x0
0             0              30     03:32:30   L2 - Dynamic
10.201.0.16      10.201.0.21      tcp :15683  :3268      Vl1              :0x0
5             809            23     03:32:54   L2 - Dynamic
10.242.0.194     10.201.0.25      tcp :1121   :1178      Vl1              :0x0
2             280            31     03:32:30   L3 - Dynamic
10.201.0.10      10.201.3.122     tcp :1115   :139       Vl1              :0x0
0             0              6      03:32:54   L2 - Dynamic
10.201.0.12      192.168.1.111    udp :41838  :dns       Vl168            :0x0
1             56             30     03:32:30   L3 - Dynamic
10.201.1.162     10.201.1.164     tcp :48159  :443       Vl1              :0x0
0             0              9      03:32:52   L2 - Dynamic
10.201.0.21      10.201.0.12      tcp :3268   :15710     Vl1              :0x0
 --More--
```