



Flexible NetFlow NBAR アプリケーション認識の概要

NBARによって、key フィールドまたはnonkey フィールドとしてアプリケーション名を収集するフロー レコードがあるフロー モニタを適用し、2 つの IP ホスト間で表示されるアプリケーションごとに異なるフローを作成できます。

- [機能情報の確認, 1 ページ](#)
- [Flexible NetFlow NBAR アプリケーション認識について, 2 ページ](#)
- [Flexible NetFlow NBAR アプリケーション認識の設定方法, 2 ページ](#)
- [Flexible NetFlow NBAR アプリケーション認識の設定例, 9 ページ](#)
- [その他の関連資料, 10 ページ](#)
- [Flexible NetFlow NBAR アプリケーション認識の機能情報, 11 ページ](#)

機能情報の確認

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。最新の警告および機能情報については、『[Bug Search Tool](#)』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Flexible NetFlow NBAR アプリケーション認識について

Flexible NetFlow NBAR アプリケーション認識の概要

DHCPv6 ガード機能は、不正な DHCP サーバやリレー エージェントからのアドバタイズメント メッセージへの応答をブロックします。

パケットは 3 種類の DHCP メッセージのいずれかに分類されます。すべてのクライアント メッセージは、デバイス ロールに関係なく常にスイッチドです。DHCP サーバメッセージは、デバイス ロールがサーバに設定されている場合にだけ、さらに処理が進められます。サーバ メッセージのさらなる処理には、DHCP サーバアドバタイズメント（送信元検証およびサーバプリファレンス）や DHCP サーバ応答（許可されたプレフィックスの場合）が含まれます。

デバイスが DHCP サーバとして設定されている場合、すべてのメッセージがデバイス ロールの設定に関係なくスイッチドである必要があります。

Flexible NetFlow NBAR アプリケーション認識の設定方法

カスタマイズしたフロー レコードの設定

カスタム フロー レコードを設定するには、次の作業を実行します。

カスタマイズしたフロー レコードは、特定の目的でトラフィック データを分析するために使用します。カスタマイズしたフロー レコードには、**key** フィールドとして使用する 1 つ以上の **match** 基準が必須で、通常は **nonkey** フィールドとして使用する 1 つ以上の **collect** 基準があります。

カスタマイズしたフロー レコードの順列は、数百もの可能性があります。この作業では、可能性のある順列の 1 つを作成するための手順について説明します。必要に応じてこの作業の手順を変更し、要件に合わせてカスタム フロー レコードを作成します。

手順の概要

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **description** *description*
5. **match** {**ipv4** | **ipv6**} {**destination** | **source**} **address**
6. 必要に応じてステップ 5 を繰り返し、レコードの追加 key フィールドを設定します。
7. **collect interface** {**input** | **output**}
8. 必要に応じてステップ 7 を繰り返し、レコードの追加 nonkey フィールドを設定します。
9. **end**
10. **show flow record** *record-name*
11. **show running-config flow record** *record-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	flow record <i>record-name</i> 例 : Device(config)# flow record FLOW-RECORD-1	フロー レコードを作成し、Flexible NetFlow フロー レコード コンフィギュレーション モードを開始します。 • このコマンドでは、既存のフロー レコードを変更することもできます。
ステップ 4	description <i>description</i> 例 : Device(config-flow-record)# description Used for basic traffic analysis	(任意) フロー レコードの説明を作成します。
ステップ 5	match { ipv4 ipv6 } { destination source } address	フロー レコードの key フィールドを設定します。

	コマンドまたはアクション	目的
	例 : <pre>Device(config-flow-record)# match ipv4 destination address</pre>	(注) この例では、IPv4 宛先アドレスをレコードの key フィールドとして設定します。 match ipv4 コマンドで使用可能なその他の key フィールド、および key フィールドの設定に使用可能なその他の match コマンドについては、『<i>Cisco IOS Flexible NetFlow Command Reference</i>』を参照してください。
ステップ 6	必要に応じてステップ 5 を繰り返し、レコードの追加 key フィールドを設定します。	—
ステップ 7	collect interface {input output} 例 : <pre>Device(config-flow-record)# collect interface input</pre>	入力インターフェイスをレコードの nonkey フィールドとして設定します。 (注) 次に、入力インターフェイスをレコードの nonkey フィールドとして設定する例を示します。 nonkey フィールドの設定に使用可能なその他の collect コマンドについては、『<i>Cisco IOS Flexible NetFlow Command Reference</i>』を参照してください。
ステップ 8	必要に応じてステップ 7 を繰り返し、レコードの追加 nonkey フィールドを設定します。	—
ステップ 9	end 例 : <pre>Device(config-flow-record)# end</pre>	Flexible NetFlow フロー レコード コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 10	show flow record record-name 例 : <pre>Device# show flow record FLOW_RECORD-1</pre>	(任意) 指定されたフロー レコードの現在のステータスを表示します。
ステップ 11	show running-config flow record record-name 例 : <pre>Device# show running-config flow record FLOW_RECORD-1</pre>	(任意) 指定されたフロー レコードの設定を表示します。

カスタマイズしたフロー モニタの作成

カスタム フロー モニタを作成するには、次の必須作業を実行します。

各フローモニタには、専用のキャッシュが割り当てられています。フローモニタごとに、キャッシュ エントリの内容およびレイアウトを定義するレコードが必要です。

はじめる前に

Flexible NetFlow の事前定義済みレコードの代わりにカスタマイズしたレコードを使用する場合は、このタスクを実行する前に、カスタマイズしたレコードを作成する必要があります。

データをエクスポートするためにフローエクスポートをフローモニタに追加する場合は、このタスクを完了する前にエクスポートを作成する必要があります。



(注) フロー モニタで **record** コマンドのパラメータを変更する前に、**no ip flow monitor** コマンドを使用して、すべてのインターフェイスから適用済みのフロー モニタを削除する必要があります。 **ip flow monitor** コマンドについては、『Cisco IOS Flexible NetFlow Command Reference』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **flow monitor monitor-name**
4. **description description**
5. **record {record-name | netflow-original | netflow {ipv4 | ipv6} record [peer]}**
6. **cache {entries number | timeout {active | inactive | update} seconds | type {immediate | normal | permanent}}**
7. 必要に応じてステップ 6 を繰り返して、このフロー モニタのキャッシュ パラメータの変更を完了します。
8. **statistics packet protocol**
9. **statistics packet size**
10. **exporter exporter-name**
11. **end**
12. **show flow monitor [[name] monitor-name [cache [format {csv | record | table}]] [statistics]]**
13. **show running-config flow monitor monitor-name**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	flow monitor monitor-name 例 : Device(config)# flow monitor FLOW-MONITOR-1	フロー モニタを作成し、Flexible NetFlow フロー モニタ コンフィギュレーションモードを開始します。 • このコマンドでは、既存のフロー モニタを変更することもできます。
ステップ 4	description description 例 : Device(config-flow-monitor)# description Used for basic ipv4 traffic analysis	(任意) フロー モニタの説明を作成します。
ステップ 5	record {record-name netflow-original netflow {ipv4 ipv6} record [peer]} 例 : Device(config-flow-monitor)# record FLOW-RECORD-1	フロー モニタのレコードを指定します。
ステップ 6	cache {entries number timeout {active inactive update} seconds type {immediate normal permanent}} 例 : Device(config-flow-monitor)# cache type normal	(任意) フロー モニタ キャッシュ パラメータ（タイムアウト値、キャッシュエントリ数、キャッシュタイプなど）を変更します。 • timeout キーワードに関連するキーワードの値は、キャッシュタイプが immediate に設定されている場合には反映されません。
ステップ 7	必要に応じてステップ 6 を繰り返して、このフロー モニタのキャッシュ パラメータの変更を完了します。	—

	コマンドまたはアクション	目的
ステップ 8	statistics packet protocol 例 : <pre>Device(config-flow-monitor)# statistics packet protocol</pre>	(任意) Flexible NetFlow モニタのプロトコル分散統計情報の収集をイネーブルにします。
ステップ 9	statistics packet size 例 : <pre>Device(config-flow-monitor)# statistics packet size</pre>	(任意) Flexible NetFlow モニタのサイズ分散統計情報の収集をイネーブルにします。
ステップ 10	exporter exporter-name 例 : <pre>Device(config-flow-monitor)# exporter EXPORTER-1</pre>	(任意) 事前に作成されたエクスポートの名前を指定します。
ステップ 11	end 例 : <pre>Device(config-flow-monitor)# end</pre>	Flexible NetFlow フロー モニタ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 12	show flow monitor [[name] monitor-name [cache [format {csv record table}]] [statistics]] 例 : <pre>Device# show flow monitor FLOW-MONITOR-2 cache</pre>	(任意) Flexible NetFlow フロー モニタのステータスおよび統計情報を表示します。
ステップ 13	show running-config flow monitor monitor-name 例 : <pre>Device# show running-config flow monitor FLOW_MONITOR-1</pre>	(任意) 指定されたフロー モニタの設定を表示します。

インターフェイスへのフロー モニタの適用

フロー モニタをアクティブ化する前に、1つ以上のインターフェイスに適用する必要があります。フロー モニタをアクティブ化するには、次の必須作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **{ip | ipv6} flow monitor** *monitor-name* **{input | output}**
5. ステップ 3 および 4 を繰り返して、トラフィックをモニタするデバイスの他のインターフェイスでフロー モニタをアクティブ化します。
6. **end**
7. **show flow interface** *type number*
8. **show flow monitor name** *monitor-name* **cache format record**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface <i>type number</i> 例 : Device(config)# interface GigabitEthernet 0/0/0	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	{ip ipv6} flow monitor <i>monitor-name</i> {input output} 例 : Device(config-if)# ip flow monitor FLOW-MONITOR-1 input	作成済みのフローモニタを、トラフィックの分析対象となるインターフェイスに割り当てることで、そのフロー モニタをアクティブにします。
ステップ 5	ステップ 3 および 4 を繰り返して、トラフィックをモニタするデバイスの他のインターフェイスでフロー モニタをアクティブ化します。	—

	コマンドまたはアクション	目的
ステップ 6	end 例 : Device(config-if)# end	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	show flow interface <i>type number</i> 例 : Device# show flow interface GigabitEthernet 0/0/0	指定されたインターフェイスの Flexible NetFlow のステータス（イネーブルまたはディセーブル）を表示します。
ステップ 8	show flow monitor name <i>monitor-name</i> cache format record 例 : Device# show flow monitor name FLOW_MONITOR-1 cache format record	指定されたフローモニタのステータス、統計情報、およびキャッシュ内のフローデータを表示します。

Flexible NetFlow NBAR アプリケーション認識の設定例

例：ネットワークベースアプリケーション認識のためのFlexibleNetFlowの設定

次に、key フィールドとしてアプリケーション名を収集するフロー レコードがあるフロー モニタを適用し、ネットワークベース アプリケーション認識（NBAR）を使用して、2つの IP ホスト間で表示されるアプリケーションごとに異なるフローを作成する例を示します。

この例は、グローバル コンフィギュレーション モードで開始します。

```

!
flow record rm_1
match application name
match ipv4 source address
match ipv4 destination address
collect interface input
collect interface output
collect counter packets
!
flow monitor mm_1
record rm_1
!
interface FastEthernet0/0
ip address 172.16.2.2 255.255.255.0
ip flow monitor mm_1 input

```

!
end

その他の関連資料

関連資料

関連項目	参照先
Cisco IOS コマンド	『 Cisco IOS Master Command List, All Releases 』
Flexible NetFlow の概念情報および設定作業	『 <i>Flexible NetFlow</i> コンフィギュレーション ガイド』
Flexible NetFlow コマンド	『 <i>Cisco IOS Flexible NetFlow Command Reference</i> 』

標準/RFC

標準	タイトル
この機能によりサポートされる新規または変更された標準/RFC はありません。	—

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、シスコソフトウェア リリース、およびフィーチャセットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンラインリソースを提供しています。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Flexible NetFlow NBAR アプリケーション認識の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 1 : Flexible NetFlow NBAR アプリケーション認識の機能情報

機能名	リリース	機能情報
Flexible NetFlow : NBAR アプリケーション認識	15.0(1)M Cisco IOS XE Release 3.1S	ネットワークベースアプリケーション認識 (NBAR) によって、key フィールドまたは nonkey フィールドとしてアプリケーション名を収集するフローレコードがあるフローモニタを適用し、2つの IP ホスト間に表示されるアプリケーションごとに異なるフローを作成できます。 次のコマンドが導入または変更されました。 collect application name、match application name、option (Flexible NetFlow)、show flow monitor