Netflow および sFlow によるネットワークトラフィック監視

Netflow および sFlow によるネットワークトラフィック監視

Pandora FMS ドキュメント一覧に戻る

リアルタイムネットワーク分析の概要

Pandora FMS はリアルタイムでネットワークを分析するために Pandora NTA と Netflow の 2つの異なるシステムを使用します。どちらのシステムもイーサネットを連続的に *リスニング*し、トラフィックを分析して統計を生成するという同じ手法を用います。どちらの場合も、何らかの方法でネットワークトラフィックを“傍受”してそれを分析するプローブに送信し、その結果を Pandora FMS に送信することが必要です。

ネットワークトラフィックを傍受して分析できるようにするには、ネットワークのキャプチャポイントを適切に判断する必要があるため、そのネットワークに物理的に確認するか、少なくともそのトポロジを理解する必要があります。たとえば、ルータまたはローカルAPのネットワークトラフィックをキャプチャすることは、ルータに到達する前のサーバのすべてのネットワークトラフィックをキャプチャするのとは同じではありません。

トラフィックをキャプチャするには、ポートミラーリングを使用して、スイッチのあるポートから別のポートにトラフィックを再送信します。すべてのネットワークデバイスが対応しているわけではありません(中価格帯以上のみ)。いくつかの商用ファイアーウォールでもポートミラーはできます。これはトラフィックを傍受する最も簡単な方法であり、追加のハードウェアを必要としません。すべてのトラフィックを特定のポートに送信するので、そのポートはネットワークアナライザ netflow probe を直接接続します。

ハイエンドスイッチやファイアウォールでは監視が容易になります。

それは、これらのデバイスが、個別のプローブを使用せずに、ネットワークフロー統計情報を Pandora FMS の Netflow コレクターに直接送信するためです。

ハードウェアの機能を調べて Netflow を有効にし、フローを独立したNetflow コレクター（この場合は Pandora FMS Netflow コレクター）に送信できるかどうかを確認する必要があります。

NetFlow ネットワーク監視

Pandora FMS は、NetFlow プロトコルを使用して IP トラフィックを監視できます。

NetFlow® は Cisco Systems® によって開発されたネットワーク プロトコルで、現在 Cisco IOS® および NXOS® に加えて Juniper® Enterasys Switches® などのメーカーのデバイスや

Linux®、FreeBSD®、NetBSD®、OpenBSD®などのオペレーティングシステムなど、いくつかのプラットフォームでサポートされています。

NetFlow

Netflowに対応したデバイス(netflowプローブ)は、情報の小さなかたまりで構成されるnetflowレコードを生成します。それは中央デバイスまたは netflow サーバ(netflowコレクタ)へ送信され、情報が保存、処理されます。

データは、UDP または SCTP にて Netflow プロトコルにより送信されます。netflow レコードは小さなパケットで、流れている全通信内容ではなく、接続に関する統計情報のみを含んでいます。

オリジナルの仕様から異なり追加情報を含んだいくつかの Netflow 実装がありますが、ほとんどの場合少なくとも次の情報を含んでいます。 Netflow はさまざまな方法で説明されていますが、Cisco の従来の定義では 7要素キーを使用しています。フローは、次の 7つの値を共有する一方向のパケットシーケンスとして定義されています。

- 発信元 IP アドレス
- 宛先 IP アドレス
- 発信元 UDP または TCP ポート
- 宛先 UDP または TCP ポート
- IP プロトコル
- インタフェース (SNMP ifIndex)
- サービスのタイプ

いくつかのベンダでは、異なる名前で似たようなプロトコルを定義していますが、目的は同じです。

- Juniper Networks の Jflow または cflowd
- 3Com/H3C|HP の NetStream
- Huawei の NetStream
- Alcatel Lucent の Cflowd
- Ericsson の Rflow
- AppFlow
- sFlow

Netflow コレクタ

Netflowコレクタは、ルータやスイッチから送られた全てのNetflow情報を収集するためにネットワーク上に置かれたデバイス(PCやサーバ)です。

Netflow サーバは、データを受け取り保存するために必要です。Pandora FMS は、この目的に nfcapd を利用しています。Pandora FMS が Netflow データを処理できるようにするには、これをインストールする必要があります。Pandora FMS は、必要なときに自動的にこのサーバを起動・停止します。

Netflow プローブ

プローブ (Raspberry など) は通常NetFlow が有効化され、設定され、情報を NetFlow コレクター (この場合は nfcapd デーモンが有効な Pandora FMS サーバです) に送信するルータです。

インストールと必要要件

Pandora FMS は、全ての netflow 通信を処理するためにオープンソースのツールである nfcapd (nfdump パッケージに含まれています) を利用します。このデーモンは、Pandora FMS サーバにより自動的に起動されます。このシステムは、データを特定の場所のバイナリファイルに保存しますNetflow を使うには、nfcapd をインストールする必要があります。

デーモン nfcapd のデフォルトの待ち受けポートは 9995/UDP です。ファイアーウォールがある場合は、このポートを開ける必要があることに注意してください。

nfcapd のインストール

nfcapd は、手動でインストールする必要がありますPandora FMS 自身は nfcapd をインストールしません。インストール方法の詳細は、nfcapd プロジェクトの公式ページを参照してください。

Pandora FMS はデフォルトで、Netflow データを保存するのに “/var/spool/pandora/data_in/netflow” ディレクトリを利用しますPandora FMS サーバによって起動されるときにnfcapd にこのディレクトリが指定されます。何を行っているかがわからない場合は、変更しないでください。

Pandora FMS ではNetflow データを処理するのに nfdump
バージョン 1.6.8p1 が必要です。

nfcapd が正しくインストールできたか確認するには、以下のようにコマンドを実行してプロセスを起動します。

```
nfcapd -l /var/spool/pandora/data_in/netflow
```

すべて正しく動作していれば、以下のような出力が見られます。

```
Add extension: 2 byte input/output interface index
Add extension: 4 byte input/output interface index
Add extension: 2 byte src/dst AS number
Add extension: 4 byte src/dst AS number
Add extension: 4 byte output bytes
Add extension: 8 byte output bytes
Add extension: NSEL Common block
Add extension: NSEL xlate ports
Add extension: NSEL xlate IPv4 addr
Add extension: NSEL xlate IPv6 addr
```

```
Add extension: NSEL ACL ingress/egress acl ID
Add extension: NSEL username
Add extension: NSEL max username
Add extension: NEL Common block
Bound to IPv4 host/IP: any, Port: 9995
Startup.
Init IPFIX: Max number of IPFIX tags: 62
```

Pandora FMS コンソール(具体的には、それを実行する Web サーバ)がデータにアクセスできる必要があることに注意してください。 この例では次の場所です。

```
/var/spool/pandora/data_in/netflow
```

Netflow プローブのインストール

Netflow に対応したルータが無く、Linux サーバをルータとして利用している場合は、netflow 情報を Netflow サーバへ送信するソフトウエアの Netflow プローブをインストールできます。

fprobe のインストール

fprobe がトラフィックを取得し Netflow サーバへ送信します。インターフェイスを通過するすべてのトラフィックから Netflow トラフィックを生成できます。

RPM パッケージをダウンロードおよびインストールするには、以下のコマンドを用います。

```
wget http://repo.iotti.biz/CentOS/7/x86_64/fprobe-1.1-2.el7.lux.x86_64.rpm
yum install fprobe-1.1-2.el7.lux.x86_64.rpm
```

たとえば、このコマンドを実行すると、すべての eth0 インターフェイストラフィックが IP アドレス 192.168.70.185 のポート 9995 で待ち受けている Netflow コレクターに送信されます。

```
/usr/sbin/fprobe -i eth0 192.168.70.185:9995
```

トラフィックが生成されたら、次のコマンドでトラフィックの状態を見る事ができます。

```
nfdump -R /var/spool/pandora/data_in/netflow
```

次のような情報が表示されます。

```
Aggregated flows 1286
Top 10 flows ordered by packets:
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP
Addr:Port   Packets    Bytes Flows
```

```
2011-12-22 20:41:35.697   901.035 TCP     192.168.60.181:50935 ->
192.168.50.2:22        2105   167388     4
2011-12-22 20:41:35.702   900.874 TCP       192.168.50.2:22    ->
192.168.60.181:50935     1275   202984     4
2011-12-22 20:48:15.057     1.347 TCP       157.88.36.34:80    ->
192.168.50.15:40044      496   737160     1
2011-12-22 20:48:14.742     1.790 TCP     91.121.124.139:80    ->
192.168.50.15:60101      409   607356     1
2011-12-22 20:46:02.791    76.616 TCP      192.168.50.15:80    ->
192.168.60.181:40500      370   477945     1
2011-12-22 20:48:15.015     1.389 TCP      192.168.50.15:40044 ->
157.88.36.34:80         363    22496     1
2011-12-22 20:46:02.791    76.616 TCP     192.168.60.181:40500 ->
192.168.50.15:80         303    24309     1
2011-12-22 20:48:14.689     1.843 TCP      192.168.50.15:60101 ->
91.121.124.139:80         255    13083     1
2011-12-22 20:48:14.665     1.249 TCP     178.32.239.141:80    ->
192.168.50.15:38476      227   335812     1
2011-12-22 20:48:21.350     0.713 TCP     137.205.124.72:80    ->
192.168.50.15:47551      224   330191     1

Top 10 flows ordered by bytes:
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP
Addr:Port   Packets    Bytes Flows
2011-12-22 20:48:15.057     1.347 TCP       157.88.36.34:80    ->
192.168.50.15:40044      496   737160     1
2011-12-22 20:48:14.742     1.790 TCP     91.121.124.139:80    ->
192.168.50.15:60101      409   607356     1
2011-12-22 20:46:02.791    76.616 TCP      192.168.50.15:80    ->
192.168.60.181:40500      370   477945     1
2011-12-22 20:48:14.665     1.249 TCP     178.32.239.141:80    ->
192.168.50.15:38476      227   335812     1
2011-12-22 20:48:21.350     0.713 TCP     137.205.124.72:80    ->
192.168.50.15:47551      224   330191     1
2011-12-22 20:48:15.313     1.603 TCP       89.102.0.150:80    ->
192.168.50.15:52019      212   313432     1
2011-12-22 20:48:14.996     1.433 TCP     212.219.56.138:80    ->
192.168.50.15:36940      191   281104     1
2011-12-22 20:51:12.325    46.928 TCP      192.168.50.15:80    ->
192.168.60.181:40512      201   245118     1
2011-12-22 20:52:05.935    34.781 TCP      192.168.50.15:80    ->
192.168.60.181:40524      167   211608     1
2011-12-22 20:41:35.702   900.874 TCP       192.168.50.2:22    ->
192.168.60.181:50935     1275   202984     4

Summary: total flows: 1458, total bytes: 5.9 M, total packets: 15421, avg bps:
49574, avg pps: 15, avg bpp: 399
Time window: 2011-12-22 20:40:46 - 2011-12-22 20:57:21
Total flows processed: 1458, Records skipped: 0, Bytes read: 75864
Sys: 0.006s flows/second: 208345.2   Wall: 0.006s flows/second: 221177.2
```

ここまでの動作確認ができたら、次はそれを利用できるようにするための Pandora FMS の設定です。

pmacct のインストール

実験的

pmacct プローブは、IPv4 および IPv6 を介して NetFlow v1/v5/v7/v8/v9□sFlow v2/v4/v5 で動作する機能があります。

ソースコードは以下にあります。

https://github.com/pmacct/pmacct

Rocky Linux 8

依存ファイルの管理者権限でのインストール。

```
<code>

dnf config-manager --set-enabled powertools
dnf groupinstall 'Development Tools'
dnf install libpcap libpcap-devel
```

pmacct のソースをダウンロード(wget の代わりに curl も使えます)してビルドします。

```
cd /tmp
wget -O pmacct-1.7.7.tar.gz
"https://github.com/pmacct/pmacct/releases/download/v1.7.7/pmacct-1.7.7.tar.gz"
tar xvzf pmacct-1.7.7.tar.gz
cd pmacct-1.7.7
./autogen.sh
./configure
make && make install
```

デーモンモードで、pmacct を NetFlow プローブとして起動します。

- pmacct 設定の作成:

例では、すべての eth0 インターフェイストラフィックが、IP アドレス 192.168.70.185 のポート 9995 で待ち受けている NetFlow コレクタに送信されます。

```
cat> pmacctd_probe.conf <<EOF
daemonize: true
pcap_interface: eth0
aggregate: src_host, dst_host, src_port, dst_port, proto, tos
plugins: nfprobe
nfprobe_receiver: 192.168.70.185:9995
```

```
nfprobe_version: 9
EOF
```

- pmacctd の起動:

```
# pmacctd -f pmacctd_probe.conf
```

Pandora FMS における Netflow の動作

Pandora FMS は、補助システムとしての Netflow と連動します。つまり、データベースに NetFlow データを保存しません Pandora FMS は、その情報をオンデマンドでレポートとして表示します。

Pandora FMS は、フィルタを使って Netflow データを処理します。フィルタは、通信パターンにマッチするルールのセットです。ルールは、'all the traffic from 192.168.70.0/24 network'(サブネット 192.168.70.0/24 からの通信すべて) といったように簡単です。また、pcap のフィルタ書式も利用できます。

フィルタを作成したら、フィルタにマッチした情報をどのように表示するか(グラフや表)および時間範囲をレポートで定義する必要があります Netflow レポートは、他の Pandora FMS レポートと同様にオンデマンドでのアクセスです。

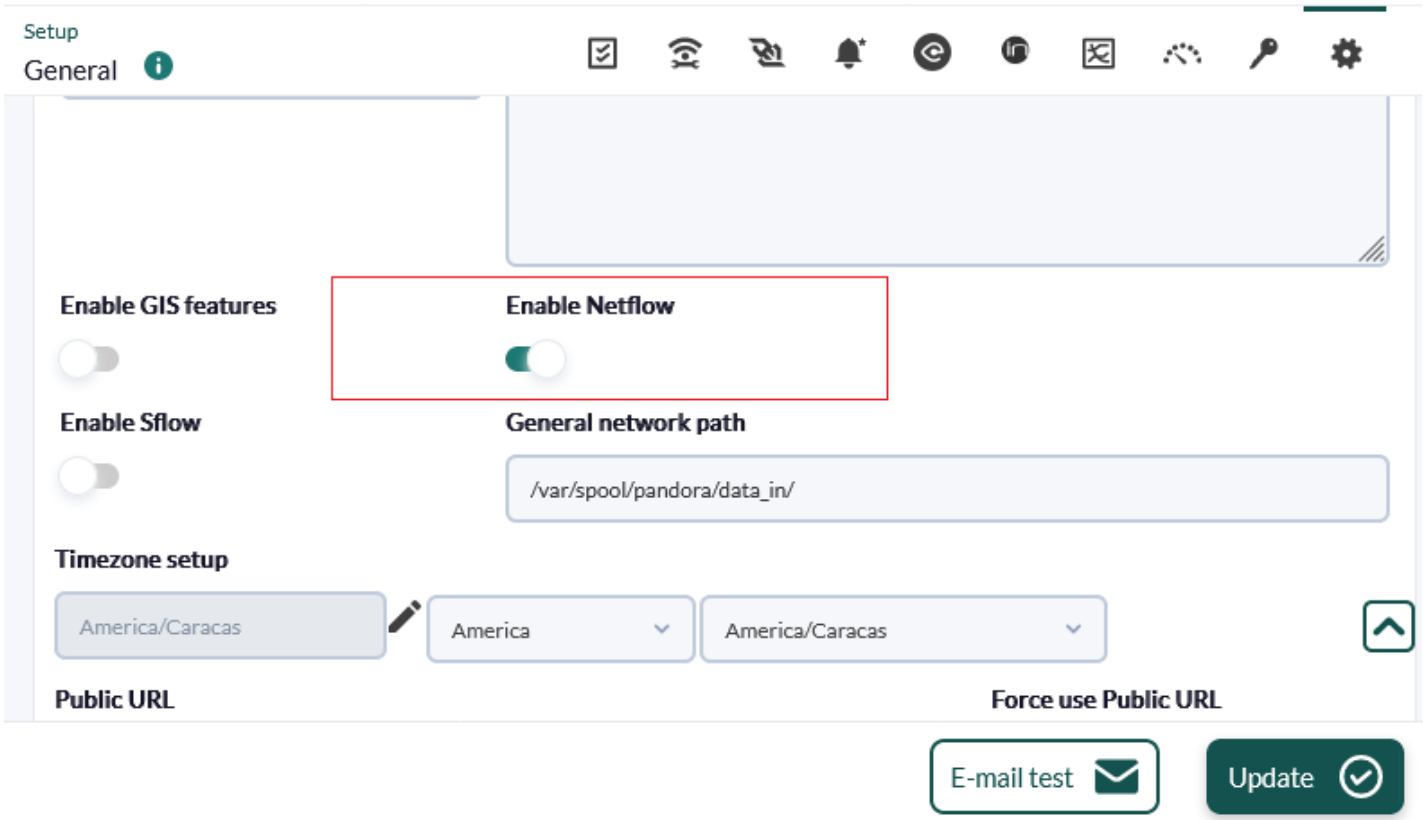
Netflow レポートは、“ レポートタイプ ” として Pandora FMS カスタムレポートに現れます Pandora FMS の “ 通常 ” のレポートへ追加することができます。

また、通信の分析や素ぽーっとでルールを作成したり修正するためのライブ Netflow ビューワがあります。これは、問題を調査したり、保存しない一時的なグラフを表示するのにするのにとても便利です。

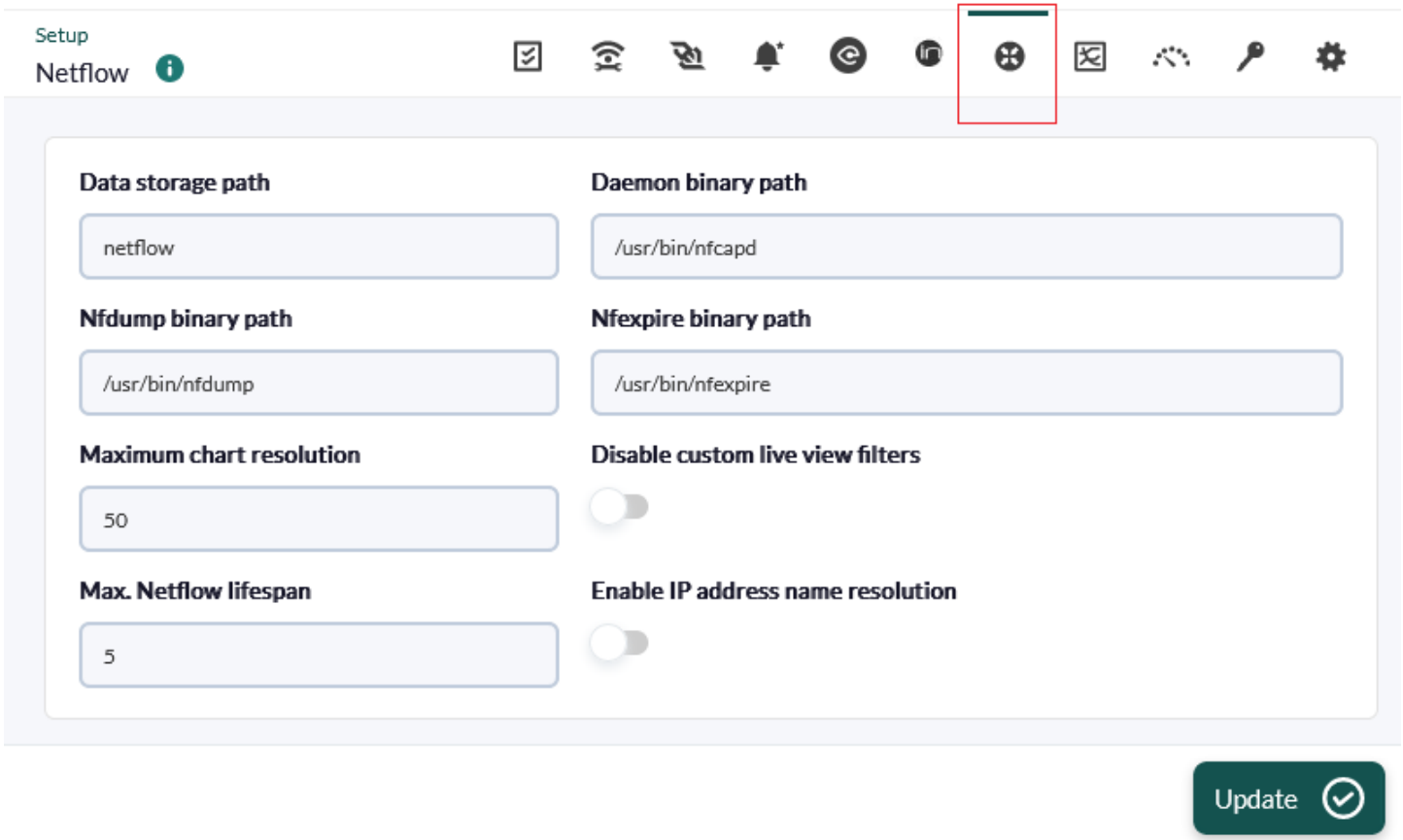
設定

Netflowデータが保存されるハードディスクアクセス速度は、
通常、パフォーマンスに関わる重要な要素です。

まず最初に、Netflow を 操作(Operation) および システム管理(Administration) メニューからアクセスできるようにする必要があります。設定画面(管理メニュー)に、Netflow を有効化・無効化するオプションがあります。



有効化すると、新たに Netflow 設定オプションが表示されます。



ここでは、nfcapd デーモンが Pandora FMS サーバと同時に起動するように正しく設定する必要があります。

- データ保存パス(Data storage path): Netflow データが保存されるディレクトリです。ディレクトリ名のみを入力します。デフォルトは netflow です(一般設定を参照)
- デーモンバイナリパス(Daemon binary path): nfcapd バイナリのパスです。
- Nfdump バイナリパス(Nfdump binary path): nfdump バイナリのパスです。
- Nfexpire バイナリパス(Nfexpire binary path): nfexpire バイナリのパスです。
- 最大グラフ解像度(Maximum chart resolution): Netflow グラフを表示するエリアの最大サイズです。解像度を高くするとパフォーマンスが下がります。50 と 100 の間の値をお勧めします。
- ライブビューカスタムフィルタの無効化(Disable custom live view filters): 有効にすると、管理者によってあらかじめ作成された Netflow フィルタのみが Netflow ライブビューで利用できます。
- Netflow 最大保存期間(Netflow max lifespan): 指定した日数よりも古い Netflow データが削除されます。
- IP アドレス名前解決の有効化(Enable IP address name resolution): Netflow デバイスから IP アドレスの名前解決をするようにします。
- デーモン間隔(Daemon interval): (*バージョン NG 769 およびそれ以前*) データファイルをローテートする時間間隔(秒)です。3600を推奨します。間隔を大きくすると大きなファイルとなり I/O のオーバーヘッドは小さくなりますが、特定の時間間隔におけるデータの検索は遅くなります。

コンソールで NetFlow を設定したら Pandora FMS サーバを再起動して、nfcapd サーバを起動します。 このサーバは、実行する前に適切にインストールする必要があります。 疑わしい場合はサーバのログを確認してください。

NetFlow データを PFMS サーバ以外のデバイス (nfcapd のインストール手順 および 分散設定 を参照) に保存する場合は、バイナリファイル `/usr/bin/nfexpire` をそのデバイスに追加し、次のエントリを `/etc/crontab` に追加します。

```
0 * * * * root yes 2>/dev/null | /usr/bin/nfexpire -e
"/var/spool/pandora/data_in/netflow" -t X_days d
```

ここで、x_dias は、デバイスに残す NetFlow データの最大日数です(*Pandora FMS コンソールの設定とは関係ありません*)

フィルタ

リソース(Resources) > NetFlow フィルタ(NetFlow Filters) をクリックすることにより、作成および編集ができます。このセクションには、変更または削除できる作成済みのフィルタのリストが含まれています。

NetFlow ライブビューからすぐにフィルタを作成し、アクティブなフィルタを新しいフィルタとして保存することもできます NetFlow フィルタには “ 基本(basic)” または “ 高度(advanced)” があります。 違いは、前者には固定のフィルタリングフィールド (ソース IP ターゲット IP ソースポート、ターゲットポート) があるのに対し、高度なフィルタリングフィールドは *pcap* 式 (ネットワークトラフィックのフィルタリング式の標準) によって定義され、あらゆる種類を使用することができます。

NetFlow 監視の有効化

バージョン 770 以降

フィルターを作成するときに、Enable NetFlow monitoring トークンを有効にすることでフィルタ監視を有効にできます。

- これにより、このフィルタのトラフィック量を監視するエージェントを作成できるようになります。
- このフィルタ内のいずれかの IP アドレスからのトラフィックが特定のしきい値を超えているかどうかを測定するモジュールを作成します。
- このフィルター内の各 IP アドレスのトラフィックレートを含むテキストモジュールが 5 分ごとに作成されます (最もトラフィックが多い 10 個の IP アドレス)。

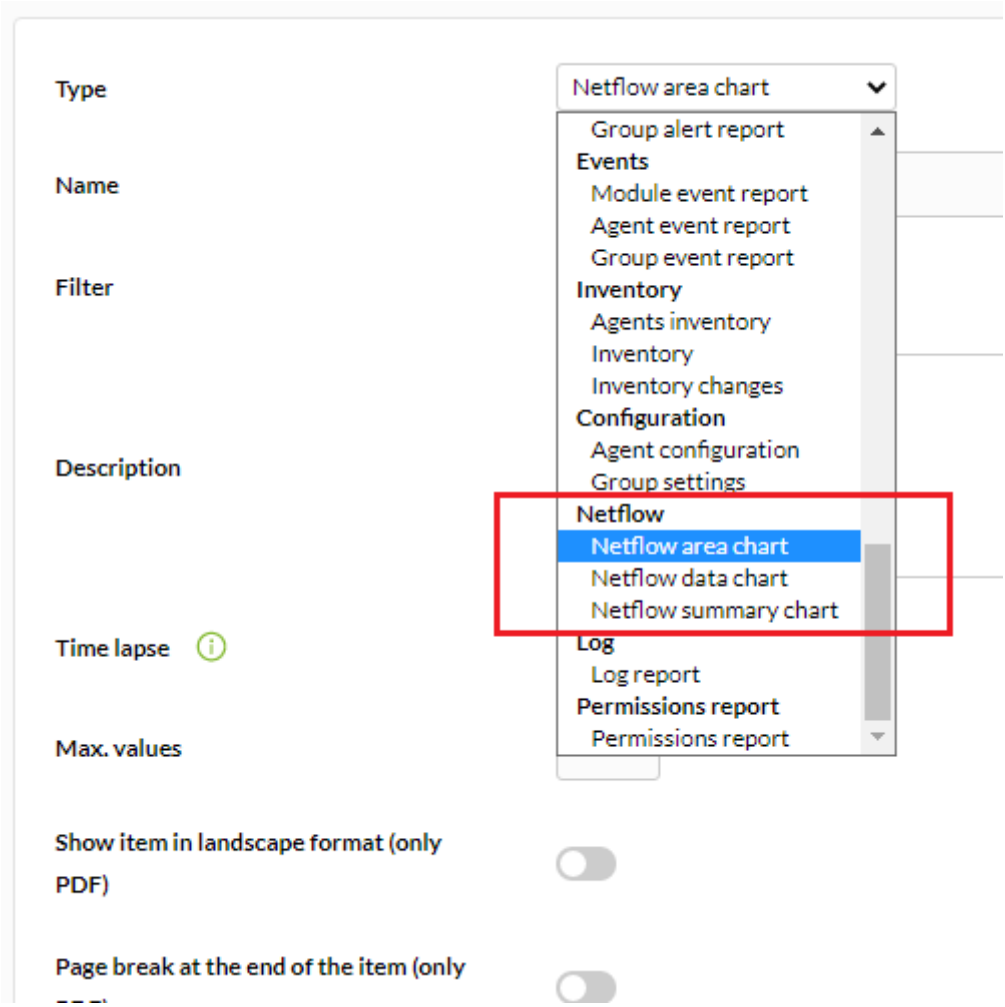
パラメータは次の通りです。

- フィルタの最大トラフィック値(Maximum traffic value of the filter): フィルタトラフィックの最大レート (バイト/秒) を指定します。 次に、これを使用して IP アドレスごとの最大トラフィックの割合が計算されます。
- IP のトラフィックの最大 % の警告しきい値(WARNING threshold for the maximum % of traffic for an IP): フィルタ内のいずれかの IP アドレスが設定された割合を超えると、警告状態が生成されます。
- IP のトラフィックの最大 % の障害しきい値(CRITICAL threshold for the maximum % of traffic for an IP): フィルタ内のいずれかの IP アドレスが設定された割合を超えると、障害状態が生成されます。

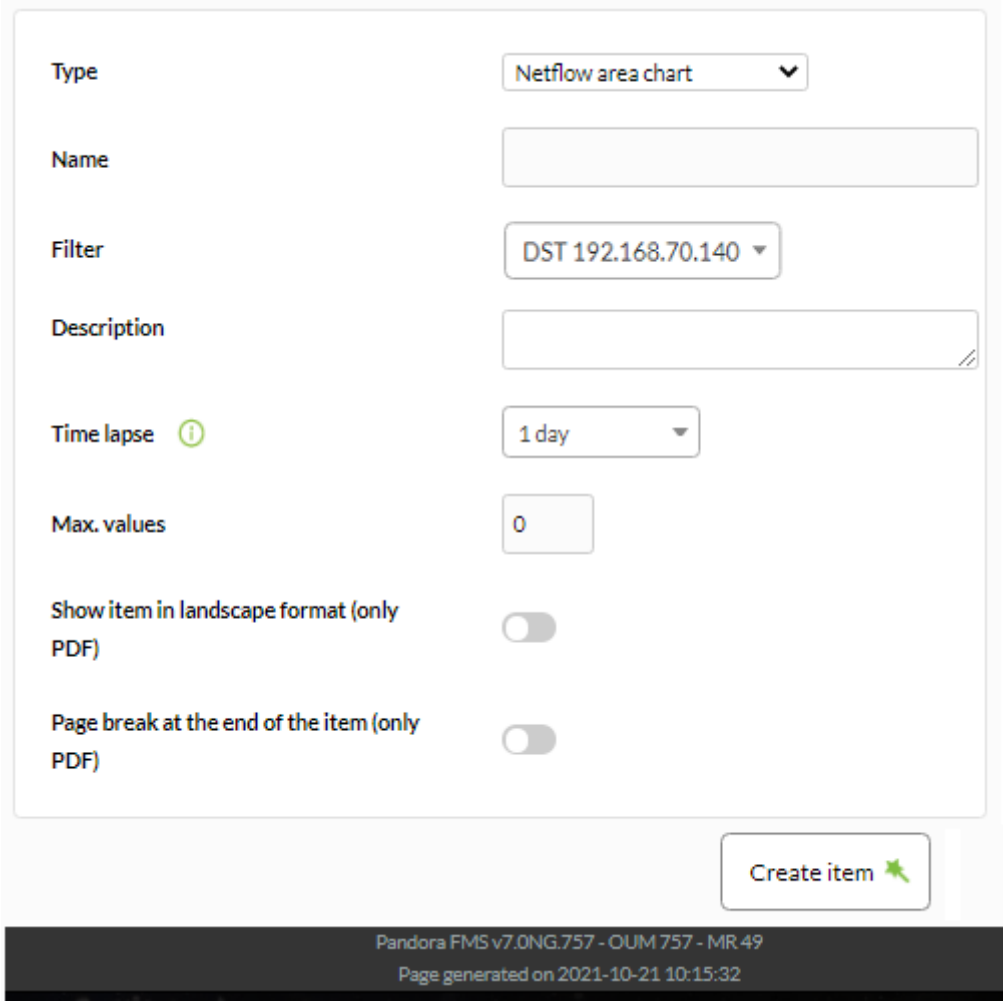
レポート

Netflow レポートは、Pandora FMS のレポート機能に統合されています。

新たにレポートアイテムを作成するには netflow レポートアイテムの一つを選択します。



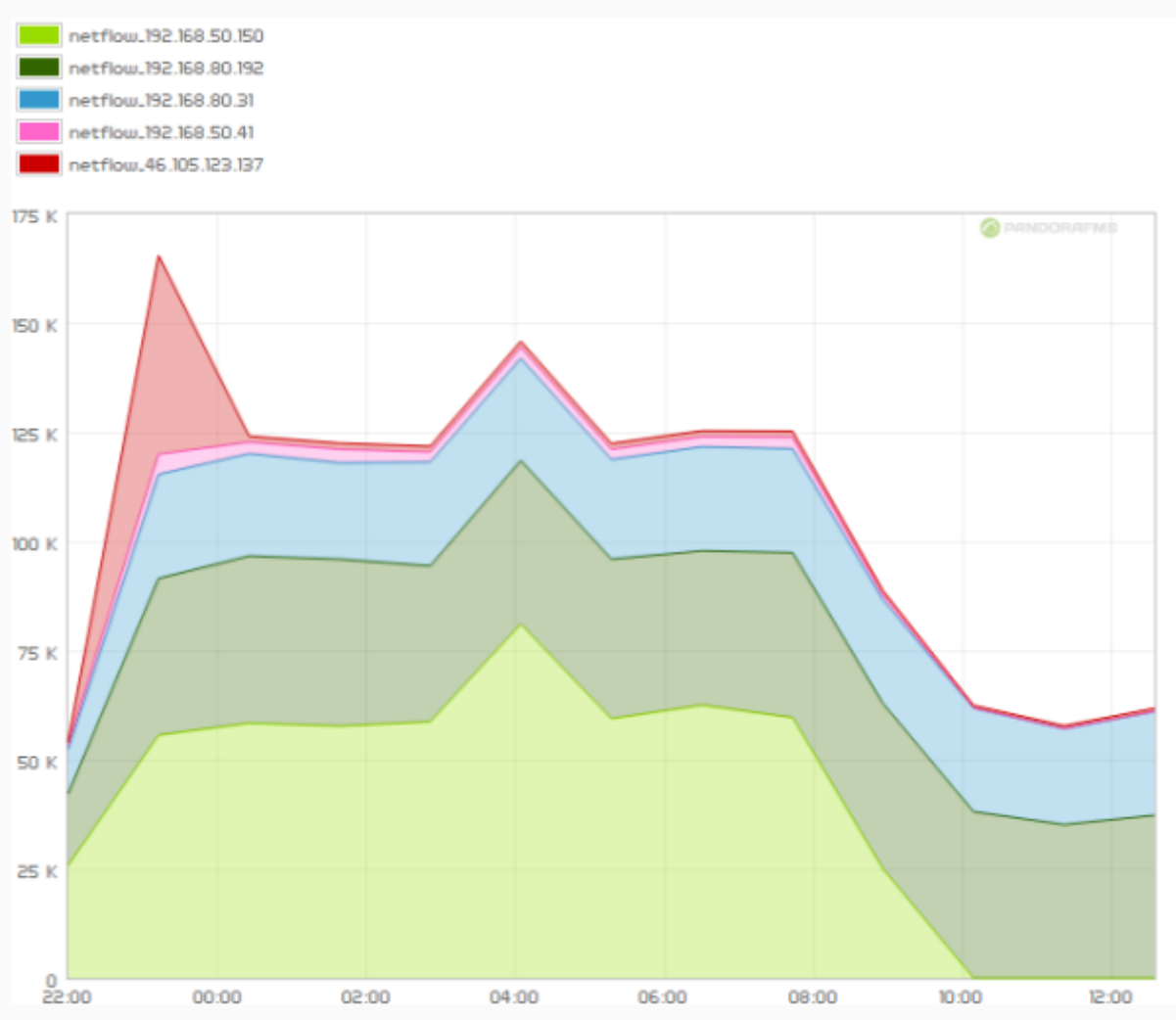
そして、設定します。次のオプションがあります。



- タイプ(Type): 以下に説明するアイテムのタイプです。
- フィルタ(Filter): 利用する Netflow フィルタです。
- 説明(Description): アイテムの説明です。
- 間隔(Period): データを表示する期間です。
- 解像度(Resolution): データは、解像度に指定したサイズで取得されます。もし、間隔/解像度を最大グラフ解像度より大きく設定すると、動的に再調整されます。例えば、間隔が 1日で、解像度が 1時間の場合、24ポイントがグラフに表示されます。
- 最大値(Max. values): 集約する要素の最大値です。例えばHTTP トラフィックのグラフを書く場合、ソースIPアドレスで集約し、最大値が 5 であれば、5つの IP アドレスのみが表示されます。

netflow レポートのアイテムは、3種類あります。

- 塗りつぶしグラフ(Area chart): 集約または未集約の塗りつぶしグラフです。

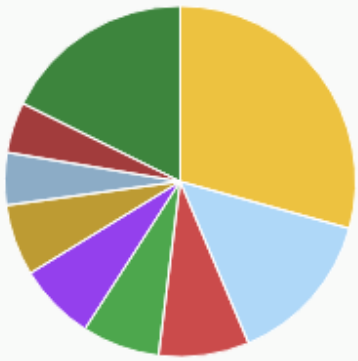


- **データ一覧**(Data table): **塗りつぶしグラフをテキストで表したものです。**

Timestamp	192.168.50.150	192.168.80.192	192.168.80.31	192.168.50.41	46.105.123.137	192.168.80.207
22:00	107.48MB	68.4MB	42.4MB	4.18MB	2.63MB	16.42KB
23:12	231.93MB	149.59MB	99.37MB	19.2MB	189.5MB	51.13KB
00:25	243.36MB	159.52MB	97.77MB	10.92MB	5.64MB	295.38MB
01:38	240.64MB	159.17MB	92.06MB	12.88MB	5.75MB	47.24KB
02:51	244.72MB	148.73MB	99.16MB	9.51MB	5.48MB	56.48KB
04:04	337.9MB	156.11MB	97.5MB	10.62MB	5.71MB	49.42KB
05:17	247.55MB	152.34MB	95.19MB	9.57MB	5.55MB	53.33KB
06:29	260.56MB	147.26MB	99.37MB	9.63MB	5.5MB	3.19MB
07:42	248.66MB	157.46MB	99.18MB	10.95MB	5.77MB	47.74KB
08:55	104.08MB	157.98MB	98.99MB	4.65MB	4.01MB	39.14KB
10:08	53.57KB	158.83MB	98.69MB	284.7KB	2.4MB	47.97KB
11:21	59.4KB	146.61MB	91.24MB	275.65KB	2.65MB	132.61KB
12:34	65.48KB	155.42MB	98.85MB	283.54KB	2.89MB	68.19KB

- Netflow **サマリグラフ**(Netflow summary chart): **指定した間隔のトラフィックサマリです。グローバル情報を含む表、最も関連性のある IP またはポートを含む円グラフ、分割された円グラフと同じ情報を含む表の 3つの要素があります。**

Total flows	1.11M
Total bytes	10.09GB
Total packages	14.65M
Average bits per second	11.77KB
Average packages per second	2
Average bytes per packet	739



Dst IP	Value
192.168.70.133	2.57GB
52.22.201.61	1.26GB
34.228.211.243	748.9MB
34.201.236.93	643.53MB
52.22.67.152	640.85MB
46.105.123.137	589.89MB
192.168.70.178	433.45MB
5.135.121.169	420.85MB
192.168.80.54	306.51MB
192.168.80.207	295.4MB
192.168.80.52	264.87MB
151.80.15.183	264.79MB
192.168.70.102	244.26MB
34.197.189.129	108.22MB
140.82.118.3	104.13MB

Netflow リアルタイム表示

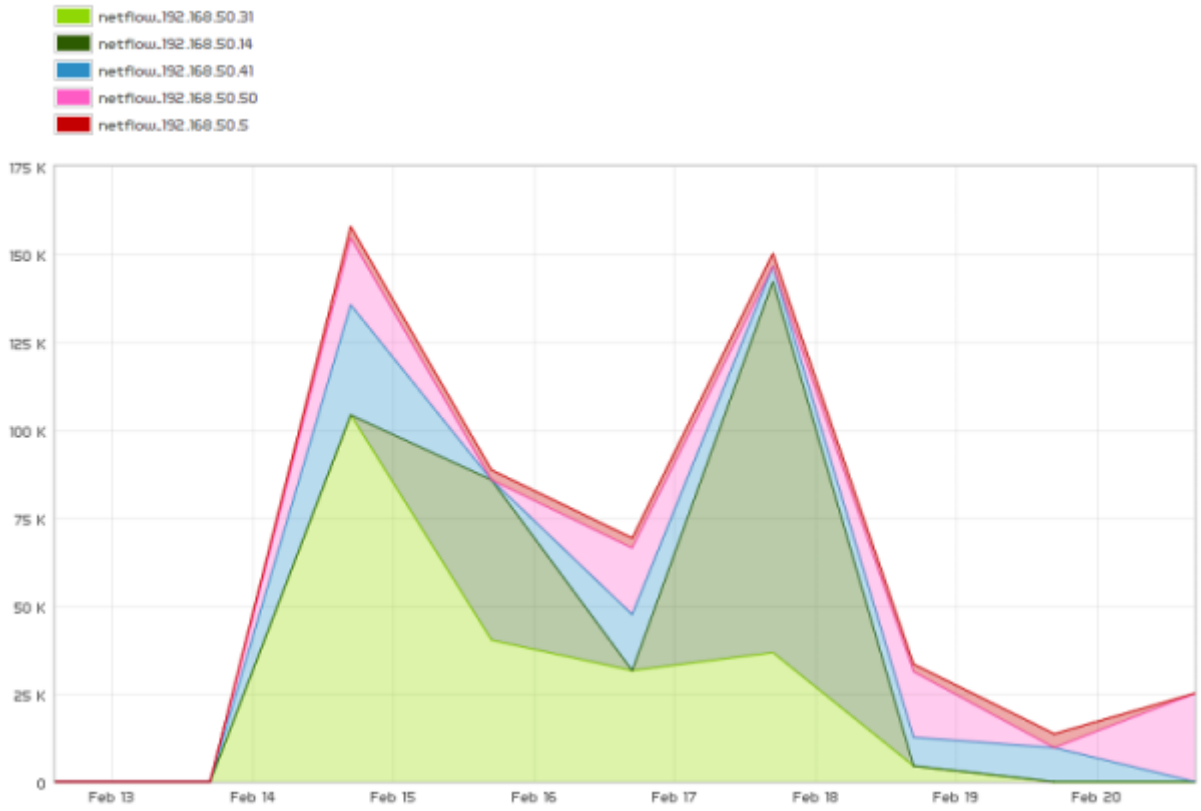
この表示は、さまざまな検索フィルタに基づいて取得されたデータの履歴を調べるために使用します。フィルタを使用して、さまざまな異なる情報を表示することができます。データの視覚化をするには、表示された情報をグループ化する方法と、この情報を取得する方法があります。

フィルタした情報は、操作(Operation) → モニタリング(Monitoring) → ネットワーク(Network) → Netflow ライブビュ(Netflow Live View) から表示できます。このツールで、フィルタの変更のプレビューおよび、好みの出力結果を保存できます。設定したフィルタをロードし編集することもできます。

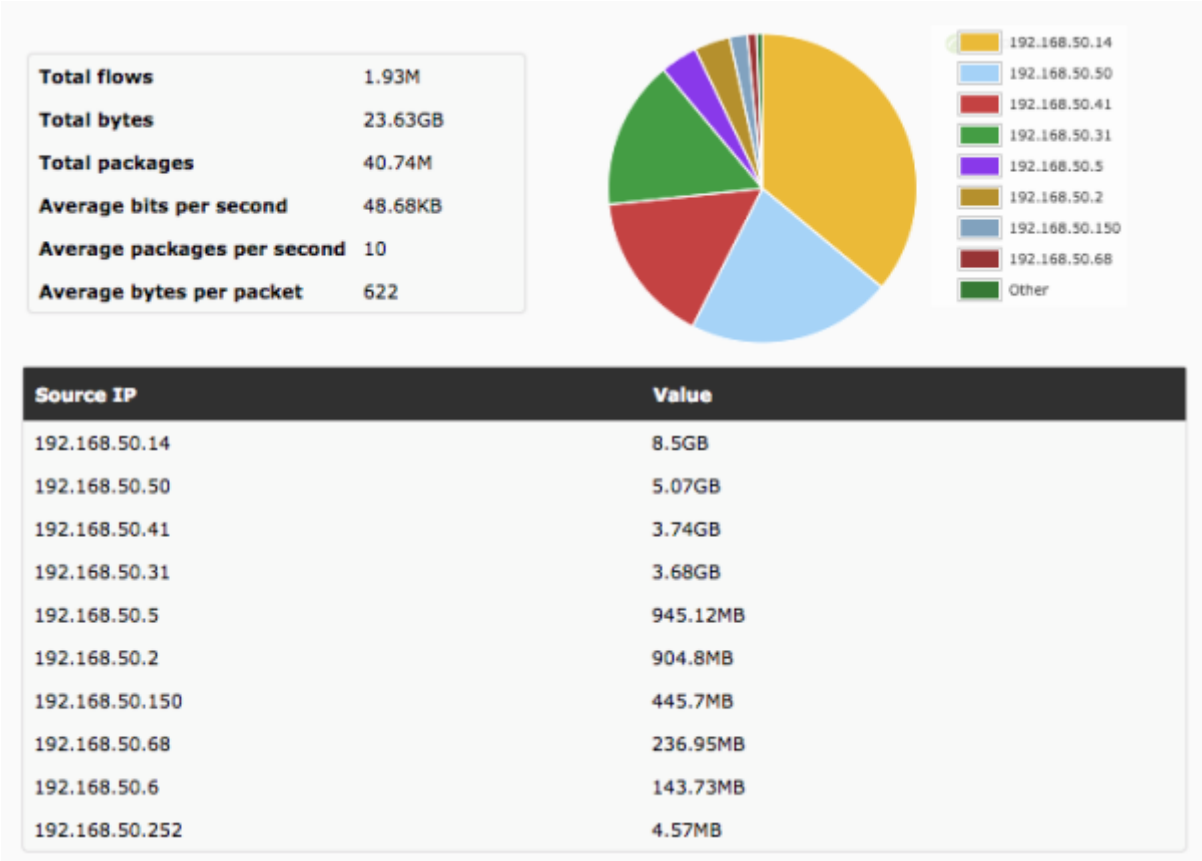
情報を取得する方法は、送信元 IP アドレス、宛先 IP アドレス、送信元ポート、または宛先ポートです。 たとえば、宛先 IP アドレス情報を表示することを選択した場合、情報は、宛先へのトラフィックが最も多い IP アドレスによって、最高から最低の順に並べ替えられて表示されます。 宛先ポートを選択して、プロトコルごとのネットワークの消費量を見る場合も同じことが行われます。

可能な表示方法は以下の通りです。

- 塗りつぶしグラフ(Area Graph) (*積み重ね*): 時間の経過とともに(開始日から終了日まで)、データの変化を表示します。 “ 解像度(Resolution)” で、グラフの精度を選択する必要があります。



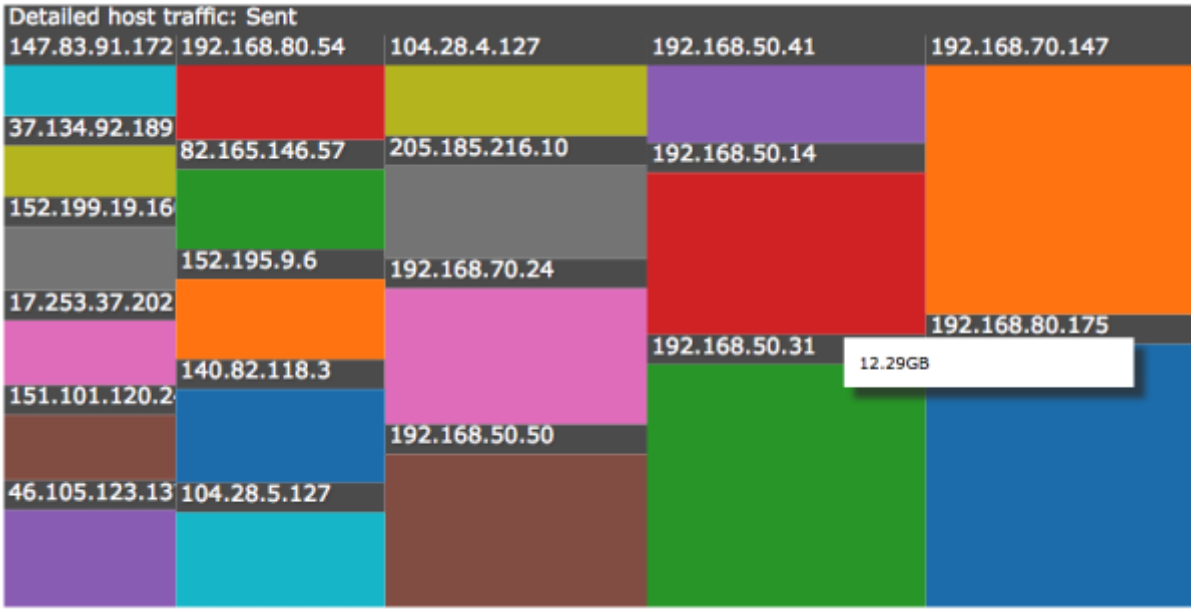
- 概要(Summary): サマリ表、円グラフ、および期間全体のデータを含む表を表示します。



Total flows	1.93M
Total bytes	23.63GB
Total packages	40.74M
Average bits per second	48.68KB
Average packages per second	10
Average bytes per packet	622

Source IP	Value
192.168.50.14	8.5GB
192.168.50.50	5.07GB
192.168.50.41	3.74GB
192.168.50.31	3.68GB
192.168.50.5	945.12MB
192.168.50.2	904.8MB
192.168.50.150	445.7MB
192.168.50.68	236.95MB
192.168.50.6	143.73MB
192.168.50.252	4.57MB

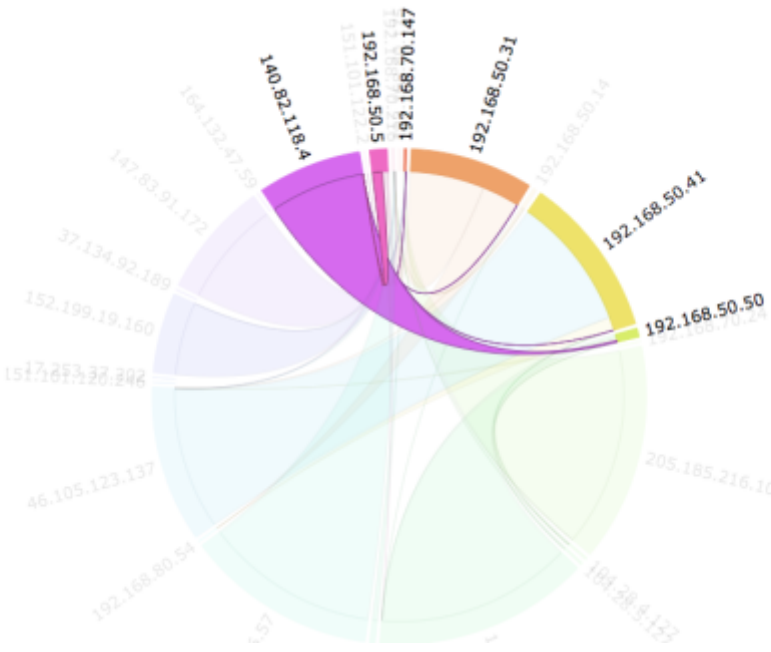
- 詳細(Detailed): IP トラフィックを表すマップを表示します。



- **データ表(Data table)**: 選択に応じて、各 IP と行数を含むデータテーブルを表示します。

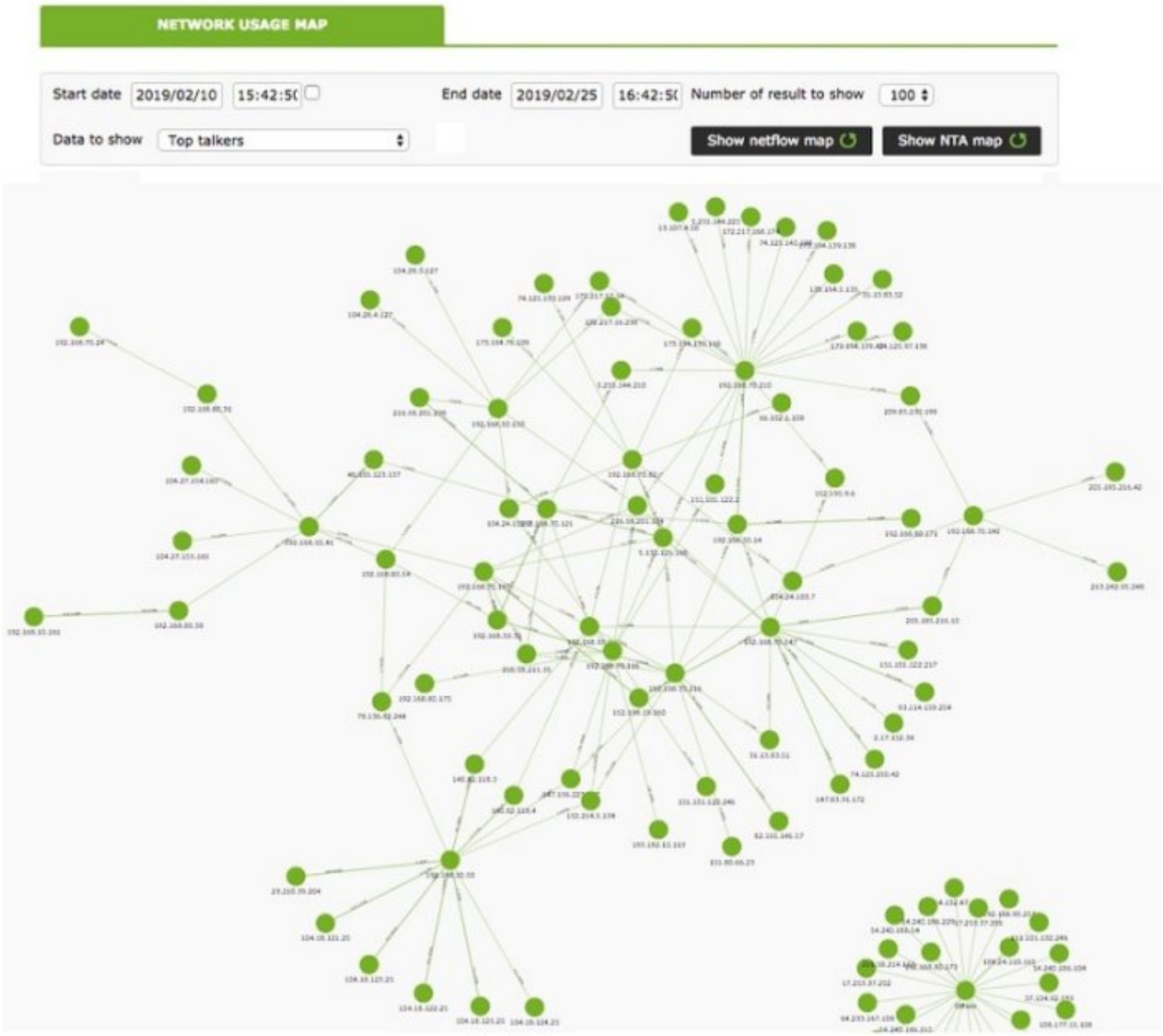
Timestamp	192.168.50.14	192.168.50.50	192.168.50.41	192.168.50.31	192.168.50.5	192.168.50.2	192.168.50.150	192.168.50.68	192.168.50.6	192.168.50.252
Jan 25 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Jan 30 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Feb 04 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Feb 09 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Feb 14 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Feb 19 17h	8.5GB	5.07GB	3.74GB	3.68GB	945.09MB	904.52MB	443.13MB	236.24MB	137.35MB	4.57MB
Feb 24 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Mar 01 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Mar 06 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Mar 11 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Mar 16 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Mar 21 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
Mar 26 17h	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B

- **円グラフ(Circle graph)**: IP とトラフィック量の間の関係を表すインタラクティブな円グラフを表示します。



ネットワークトラフィックマップ

これにより、ノード間のトラフィックに基づいて動的なネットワーク マップを作成できます。 異なるアドレス間の関係 (接続) が表示され、最も重要な N 個の接続が (接続間で転送されるデータのサイズごとに) 表示されます。



分散設定

コンソールから独立したホスト上に Netflow データを収集する pandora ノードを配置することも可能です。大量の Netflow データがある環境では、高速ディスクと 2コア以上の高速 CPU を備えたサーバに配置することをお勧めします Pandora コンソールがNetflow データを抽出するためには、以下の手順に従ってシステムのデフォルト設定を変更する必要があります。

- Web デーモンを実行するユーザと、コレクターノードで nfdump を実行するユーザとの間の自動 SSH 認証を構成します。

その設定には、次の手順を実行する必要があります。

apache ユーザを有効化します。それには/etc/passwd ファイル内の apache ユーザを次のように編集します。

```
apache:x:48:48:Apache:/var/www:/bin/bash
```

/var/www ディレクトリ内に .ssh ディレクトリを作成し、正しいパーミッションを設定します。

```
#mkdir /var/www/.ssh
#chown apache:apache /var/www/.ssh
```

ssh 鍵を作成し、それを Netflow トラフィックを収集するホストにコピーします。

```
#su apache
bash-4.2$ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/var/www/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /var/www/.ssh/id_rsa.
Your public key has been saved in /var/www/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:vYvl5V00E4faa14zN08ARzGUQ9IfAQJnMzkaqLAGRHI apache@<server>
The key's randomart image is:
+---[RSA 2048]----+
|+oE     ...*o=B+.|
|.o .   . .oo+o++ |
|  . o .   o o o+o|
|   o .   o   =  +|
|  .     S . . oo.|
|           .   +o|
|          o . o+=|
|         + + + +*|
|        . o . o .|
+----[SHA256]-----+
bash-4.2$ ssh-copy-id root@<netflow_server>
```

コピーしたら、パスワード無しで apache ユーザがサーバにアクセスできるかどうかを確認します。

```
bash-4.2$ ssh usuario@<netflow_server>
```

- 以下のように Pandora FMS コンソールで /usr/bin/nfdump を置き換えるスクリプトを作成します。

```
#!/bin/bash
NFDUMP_PARAMS=$(sed 's/(\(.*\))/\"\(\1\)\"/' <<< "$@");

ssh usuario@<netflow_server> "/usr/bin/nfdump $NFDUMP_PARAMS"
```

スクリプトに実行パーミッションを与えます。

```
chmod 755 /usr/bin/nfdump
```

以下のようにスクリプトを実行してみます。

```
/usr/bin/nfdump -V
```

つぎのような応答があります。

```
nfdump: Version: 1.6.13
```

sFlow でのネットワーク監視

バージョン NG 770 以降

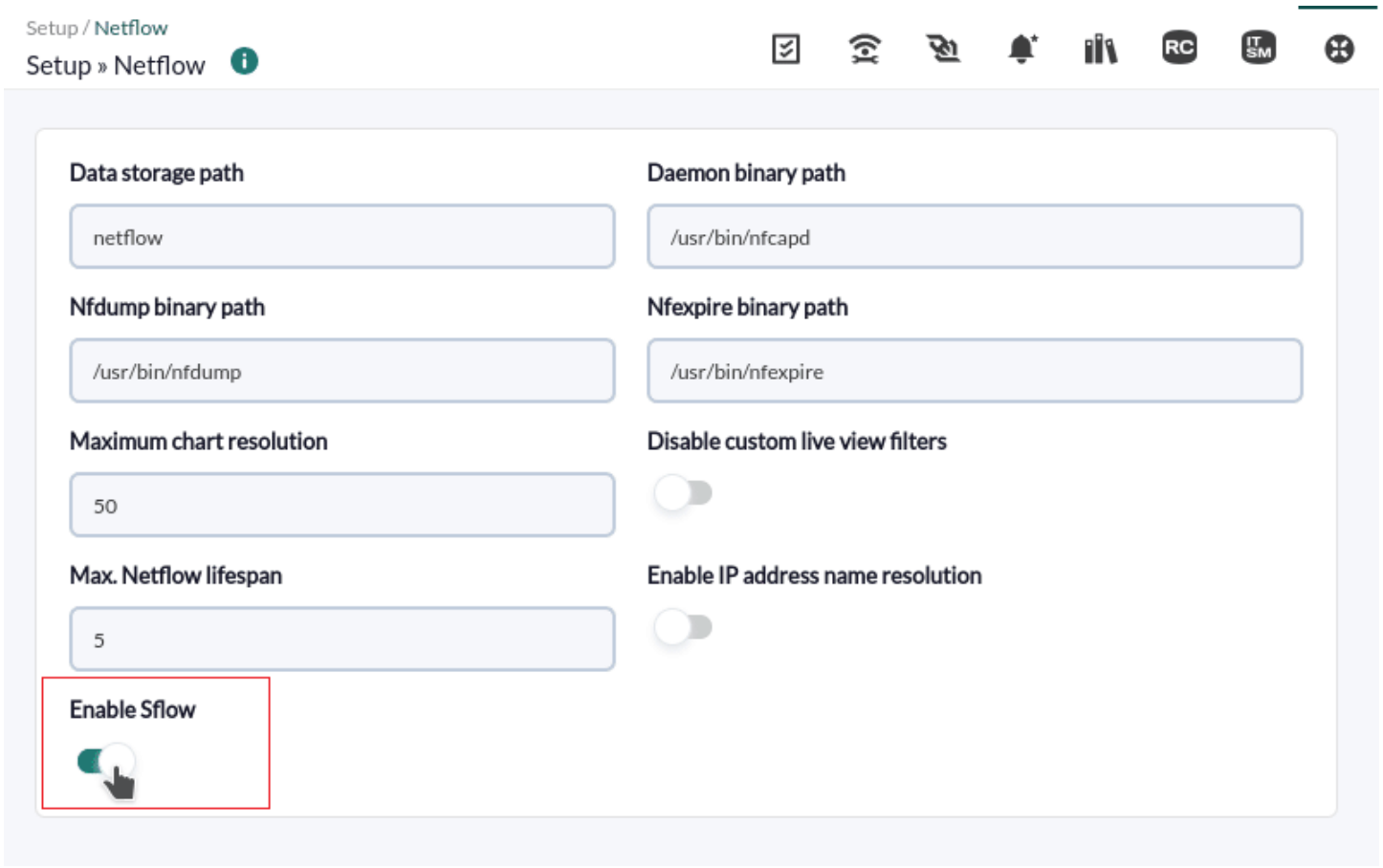
Pandora FMS バージョン 770 以降では、sFlow のサポートが含まれています。sFlow は、データネットワークトラフィック用のハードウェアにおける業界標準のネットワークプロトコルです。

Pandora FMS での sFlow の動作は NetFlow で確立しているものと同様 です。 両方のプロトコルが有効な場合、データはグループ化されます。いずれの場合も、左側のサイドバーの 操作(Operation) メニューにアクセスし、ネットワーク(Network) をクリックすると、常に表示されます。

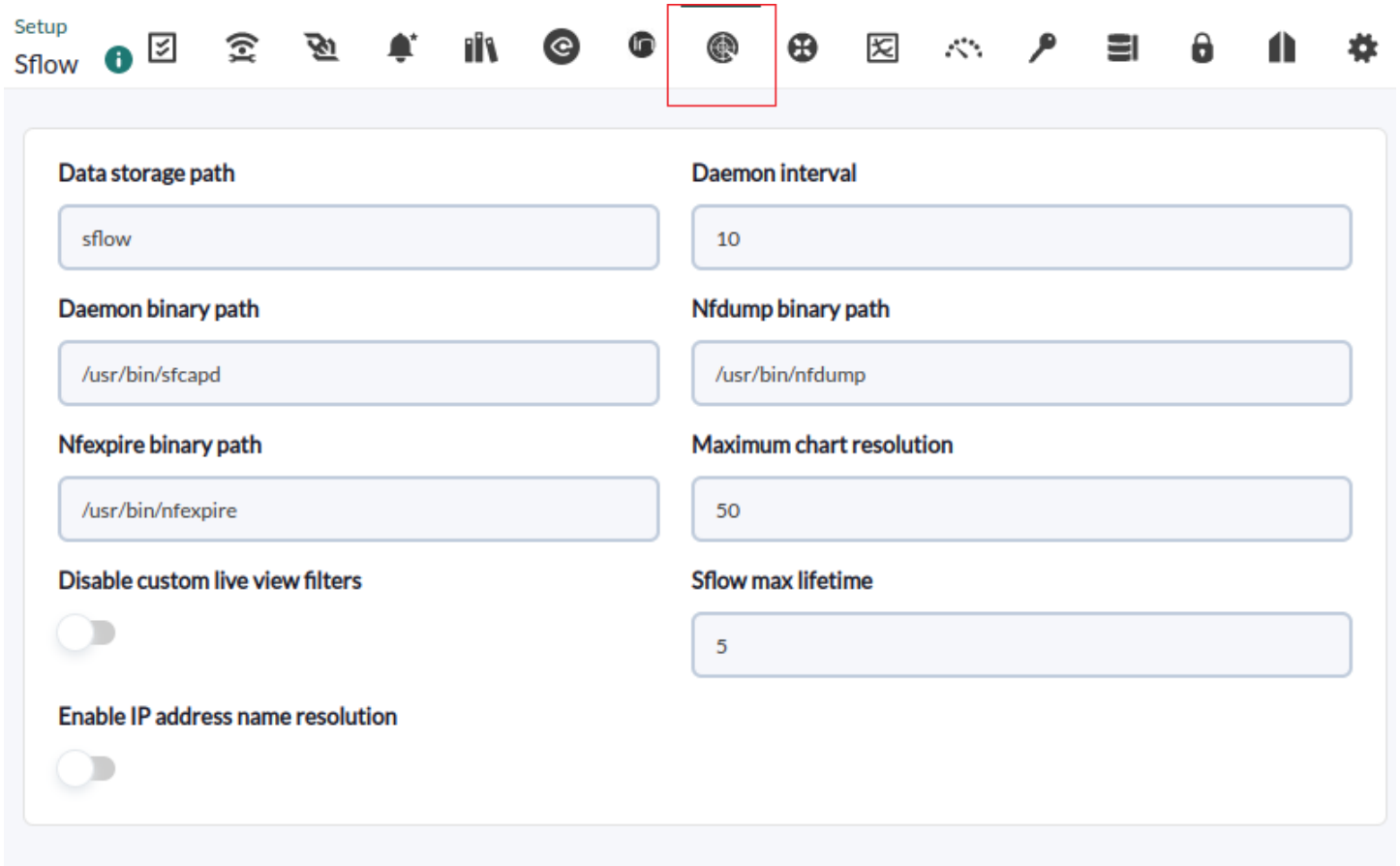
sFlow 設定

バージョン NG 775 以降

操作 と 管理 メニューからアクセスできるようにsFlow を有効化する必要があります。 NetFlow 設定セクションに、sFlow をグローバルに有効または無効にするオプションがあります。



sFlow 専用の新しいタブが有効になります。



- データ保存パス(Data storage path): sFlow データファイルが保存されるディレクトリ。(一般設定を参

照)

- デーモンバイナリパス(Daemon binary path): nfcapd のバイナリのパス。
- nfdump バイナリパス(Nfdump binary path): nfdump のバイナリのパス。
- nfexpire バイナリパス(Nfexpire binary path): nfexpire のバイナリのパス。
- 最大グラフ解像度(Maximum chart resolution): sFlow グラフが表示するポイントの最大数。解像度が高くなるほどパフォーマンスが低下します。 50 から 100 の間の値をお勧めします。
- カスタムライブビューフィルタ無効化(Disable custom live view filters): sFlow 表示のカスタムフィルターの定義を無効にします (既に作成されているフィルターは引き続き使用できます)。
- sFlow 最大保存期間(sFlow max lifetime): sFlow データを保存する最大日数を示します。
- IP アドレス名前解決の有効化(Enable IP address name resolution): sFlow デバイスのホスト名を取得するための IP アドレス名前解決を有効にします。

Pandora FMS ドキュメント一覧に戻る