H3C IMC NTA/UBA
NTAホストトラフィック分析の設定例

ソフトウェアバージョン:IMC NTA7.3(E0503)

内容

はじめに

このドキュメントでは、指定されたホストからのネットワークトラフィックを監視および分析し、これらのホストの帯域幅使用を分析するためにNTAを構成する例を示します。

一般的な制限およびガイドライン

ホストトラフィックのモニタリングおよび分析用にNTAを設定する場合は、次の制約事項およびガイドラインに従ってください。

- NTAは、次のネットワーク監視プロトコルのいずれかをサポートするスイッチまたはルータと連動する必要があります。
  - NetStream
  - sFlow
  - NetFlow
- NTAの各トラフィック分析タスクに少なくとも1つのホストが含まれていることを確認しします。
- ホストタスクの正しいIP統計情報方法を選択します。
  - **Include**: ホストタスクは、指定された範囲内のIPアドレスを持つホストの統計情報を収集します。
  - **Exclude**: ホストタスクでは、ターゲットホスト範囲内のIPアドレスを持つが除外ホスト範囲内にはないホストの統計が収集されます。除外ホストはターゲットホストのサブセットである必要があります。
- インターフェイスまたはプローブが指定されている場合、トラフィック分析タスクはこれらのインターフェイスまたはプローブからフローレコードを収集します。指定されていない場合、タスクはすべてのインターフェイスおよびプローブからフローレコードを収集します。

例:ホストトラフィック分析タスクのNTAへの追加

設定例は、次のネットワークで使用できます。

- sFlowをサポートするIMC NTAおよびHPE A5820Xスイッチ
- IMC NTA、H3C S7503Eスイッチ、およびNetStreamをサポートするSecBladeカード
- NetFlowをサポートするIMC NTAおよびCisco C2900スイッチ

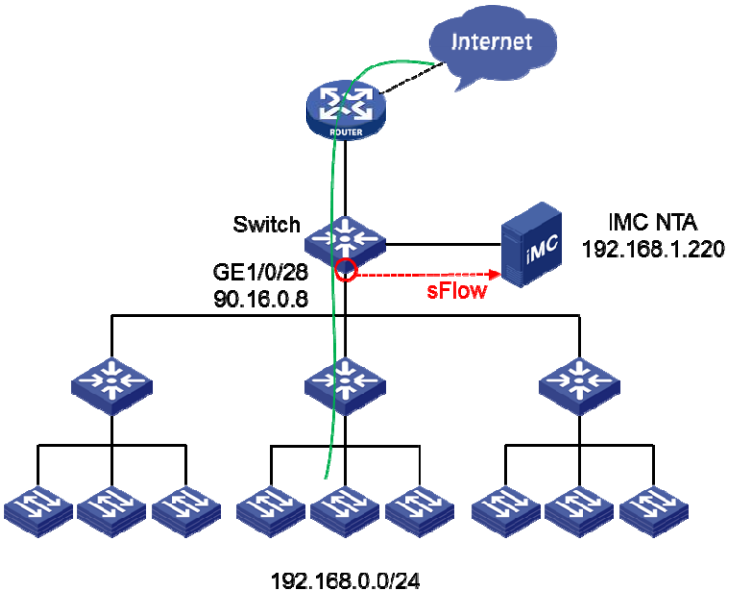
sFlowのネットワーク構成

図1に示すように、192.168.0.0/24のホストはインターネットにアクセスできます。

NTAサーバーがホストトラフィック統計情報を収集できるようにするには、次のタスクを実行します。

- スイッチ上でsFlowを有効にします。
- GigabitEthernet1/0/28でカウンタサンプリングを設定します。
- インターフェイスカウンタ情報を収集し、トラフィック統計情報をNTAサーバーに送信するようにスイッチを設定します。

図1 ネットワーク図



sFlowに使用されるソフトウェアバージョン

この構成例は、HPE A5820Xスイッチ、HPE Comwareソフトウェア、バージョン5.20.105、リリース1808P12で作成および検証されています。

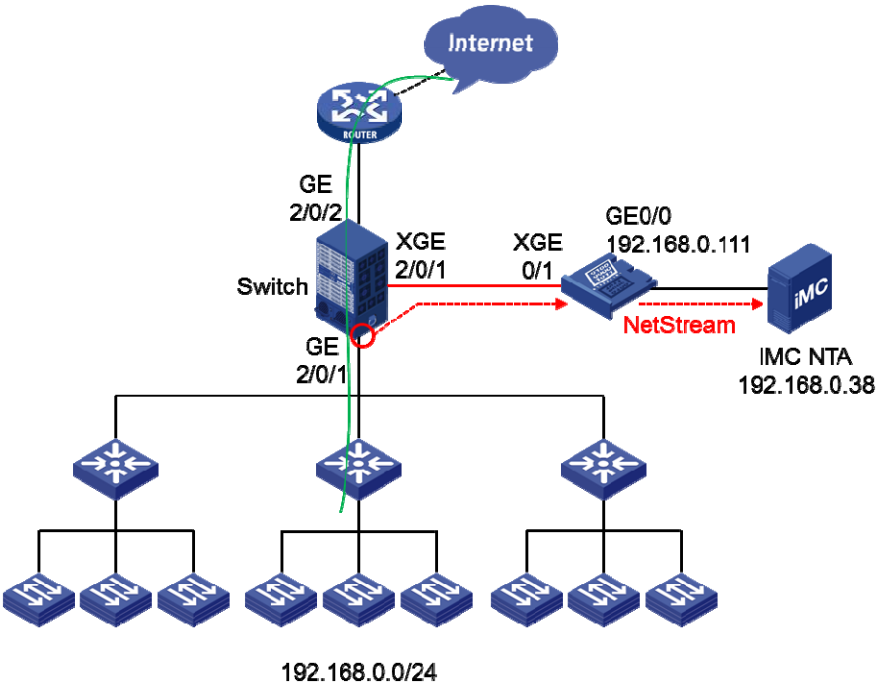
NetStreamのネットワーク構成

図2に示すように、NetStreamカードはスイッチにインストールされています。

NTAサーバーを使用して、ネットワークセグメント192.168.0.0/24内のホストによって生成されたFTPおよびHTTPトラフィックの統計情報を収集するには、次のタスクを実行します。

- スイッチのGigabitEthernet2/0/1上のポートミラーリングを設定して、双方向データをNetStreamカードのTen-GigabitEthernet0/1にミラーリングします。
- NetStreamカードの10ギガビットイーサネット0/1でNetStreamをイネーブルにして、ミラーリングされたデータを分析します。
- 収集されたフローデータをGigabitEthernet0/0経由でNTAサーバーに送信するように、NetStreamカードを設定します。

図2 ネットワーク図



NetStreamに使用されるソフトウェアバージョン

設定例は、次のプラットフォームで作成および確認されています。

- H3C S7503Eスイッチ、H3C Comware Software、バージョン5.20、リリース6708P08
- H3C SecBlade NetStreamカード、H3C Comware Software、バージョン5.20、リリース3109P03

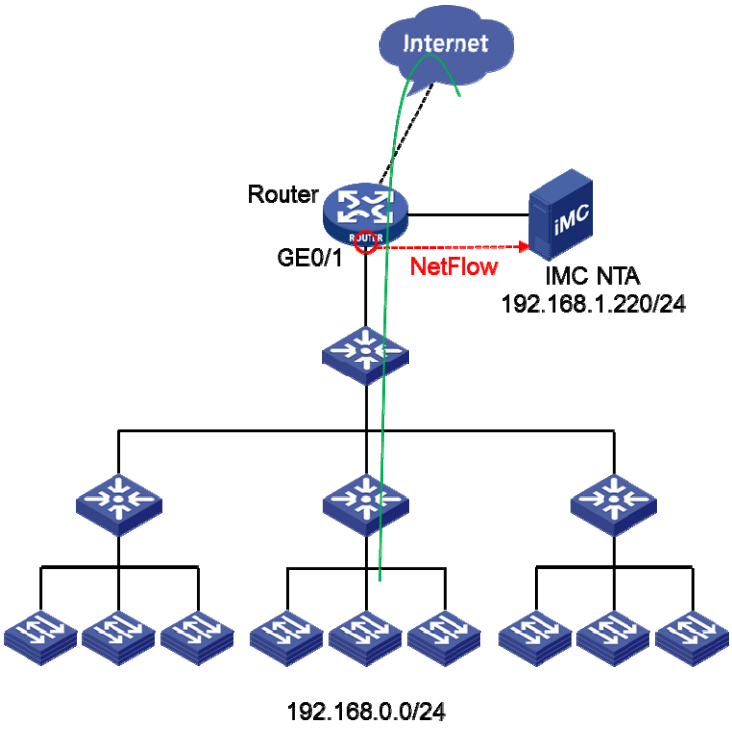
NetFlowのネットワーク設定

図3に示すように、Cisco C2900ルータは出力ルータとして機能します。

NTAサーバーを使用して、ネットワークセグメント192.168.0.0/24内のホストによって生成されたトラフィックの統計情報を収集するには、次のタスクを実行します。

- ルータのGigabitEthernet0/1でNetFlowをイネーブルにします。
- 収集されたトラフィック統計情報をNTAサーバーに送信するようにルータを設定します。

図3 ネットワーク図



NetFlowに使用されるソフトウェアバージョン

この設定例は、Cisco C2900ルータ、Cisco IOSソフトウェア、C2900ソフトウェア(C2900-UNIVERSALK9-M)バージョン15.1(4)M2リリースソフトウェア(fc1)で作成および検証されています。

制限事項およびガイドライン

NTAサーバーを設定する場合は、次の制約事項およびガイドラインに従ってください。

- スイッチを追加するときに設定するSNMPコミュニティおよびSNMPポートが、スイッチ上で設定されているものと同じであることを確認します。
- プローブを追加するときに設定したプローブパスワードが、プローブのインストール時に設定したパスワードと同じであることを確認します。
- FTPメインディレクトリが、FTPサーバーで設定されているディレクトリと同じであることを確認します。
- NTAサーバーのFTPユーザー名とパスワードが、FTPサーバーに設定されているものと同じであることを確認します。

デバイスの設定

sFlowデバイスの設定

1. HPE A5820XでsFlowエージェントのIPアドレスを90.16.0.8に設定します。

   <H3C>system-view

   [H3C] sflow agent ip 90.16.0.8

2. sFlowコレクタ用に次のパラメータを設定します。
   - sFlow collector ID1。
   - IPアドレス192.168.1.220。
   - ポート番号9020、9021、または6343。
   - description ntaserver。

   [H3C] sflow collector 1 ip 192.168.1.220 port 9020 description ntaserver
3. カウンタサンプリングの設定:

   #GigabitEthernet1/0/28でカウンタサンプリングをイネーブルにし、カウンタサンプリング間隔を120秒に設定します。

   [H3C] interface GigabitEthernet 1/0/28

   [H3C-GigabitEthernet1/0/28] sflow counter interval 120

   #カウンタサンプリング用にsFlowコレクタ1を指定します。

   [H3C-GigabitEthernet1/0/28] sflow counter collector 1

   [H3C-GigabitEthernet1/0/28] quit

NetStream 装置の設定

1. S7503Eスイッチを設定します。

   #ローカルポートミラーリンググループ1を作成します。

   [Sysname] system-view

   [Sysname] mirroring-group 1 local

   #GigabitEthernet2/0/1をローカルポートミラーリンググループ1の送信元ポートとして設定します。

   [Sysname] mirroring-group 1 GigabitEthernet2/0/1 both

   #Ten-GigabitEthernet2/0/1をローカルポートミラーリンググループ1のモニタポートとして設定します。

   [Sysname] mirroring-group 1 monitor-port Ten-GigabitEthernet2/0/1

   #ACSEIサーバーを有効にします。

   [Sysname] acsei server enable
2. NetStreamカードを設定します。

   #ブラックホールタイプのインライン転送グループ1を作成します。

   [Sysname] inline-interfaces 1 blackhole

   #Ten-GigabitEthernet0/1をインライン転送グループ1に追加します。

   [Sysname] interface Ten-GigabitEthernet0/1

   [Sysname-Ten-GigabitEthernet0/1] port inline-interfaces 1

   # Enable NetStream for inbound traffic on Ten-GigabitEthernet 0/1.

   [Sysname-Ten-GigabitEthernet0/1] ip netstream inbound

   #Ten-GigabitEthernet0/1上でACSEIクライアントをイネーブルにします。

   [Sysname-Ten-GigabitEthernet0/1]acsei client enable

   [Sysname-Ten-GigabitEthernet0/1]quit

   #NetStreamデータエクスポートの宛先IPアドレスおよび宛先UDPポート番号を設定します(UDPポート番号は9020、9021、または6343に設定できます)。

[Sysname] ip netstream export host 192.168.0.38 9020

#NetStreamデータをバージョン9形式でエクスポートするか、この手順をスキップしてデフォルトのNetStreamデータエクスポート形式バージョン5を使用します。

[Sysname] ip netstream export version 9

NetFlowデバイスの設定

#ルータのGigabitEthernet0/1でNetFlowをイネーブルにします。

Router# config

Router(config)# interface GigabitEthernet0/1

Router(config-if)# ip flow ingress

Router(config-if)# ip flow egress

Router(config-if)# exit

#UDPポート9020を使用して、エクスポート宛先アドレスを192.168.1.220に設定します。

Router(config)# ip flow-export destination 192.168.1.220 9020

NTAの構成

NetStreamおよびNetFlowのNTA構成は、sFlowのNTA構成と同じです。次に、sFlowのNTA構成についてのみ説明します。

sFlow、NetFlow、またはNetStreamデバイスの追加

1. Serviceタブをクリックします。
2. ナビゲーションツリーで、Traffic Analysis and Audit>Settingsを選択します。

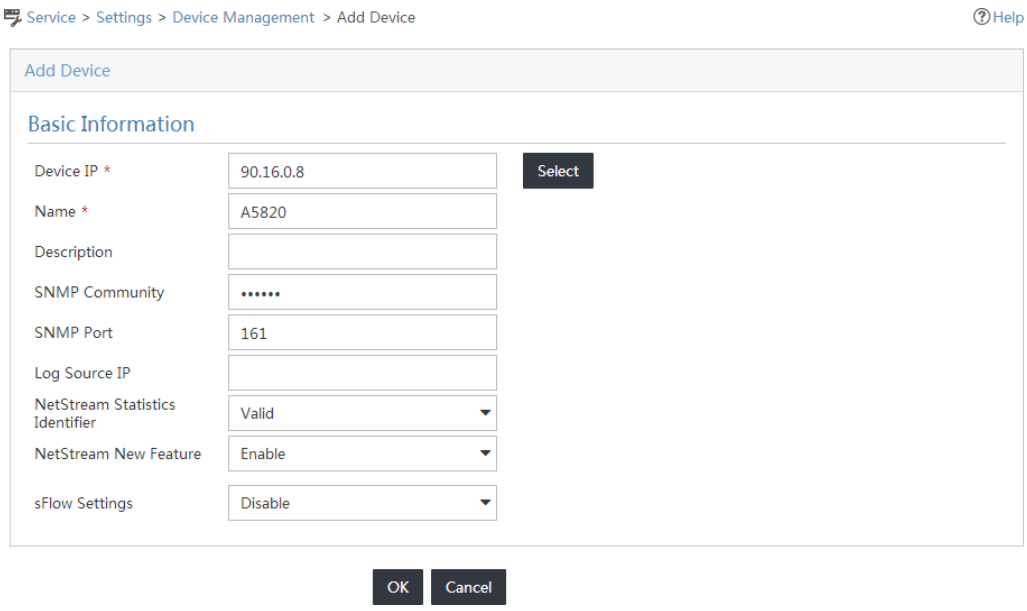
   Settingsページが開きます。
3. Device Managementをクリックします。

   Device Managementページが開きます。
4. Addをクリックします。

   Add Deviceページが開きます。
5. 図4に示すように、次のパラメータを設定します。
   a. Device IPフィールドにデバイスのIPアドレスを入力するか、Selectをクリックしてimcプラットフォームからデバイスを選択します。この例では、selectionメソッドを使用しています。

      デバイス90.16.0.8が選択されると、次のフィールドが自動的に入力されます。
      Name、SNMPコミュニティ、および[SNMPポート]。
   b. NetStream Statistics IdentifierリストからValidを選択します。
   c. NetStream New FeatureリストからEnableを選択します。
   d. sFlow設定リストからDisableを選択します。
   e. 他のパラメータにはデフォルト値を使用します。
6. OKをクリックします。

図4 デバイスの追加

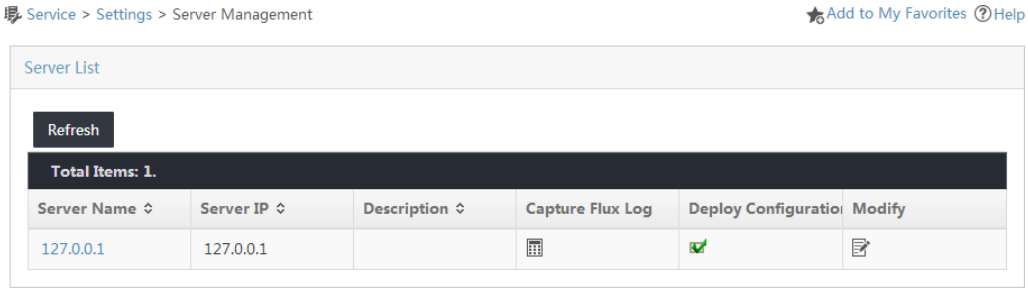


NTAサーバー構成の配布

1. Settingsページにアクセスします。
2. Server Managementをクリックします。

   図5に示すように、Server Managementページが開きます。

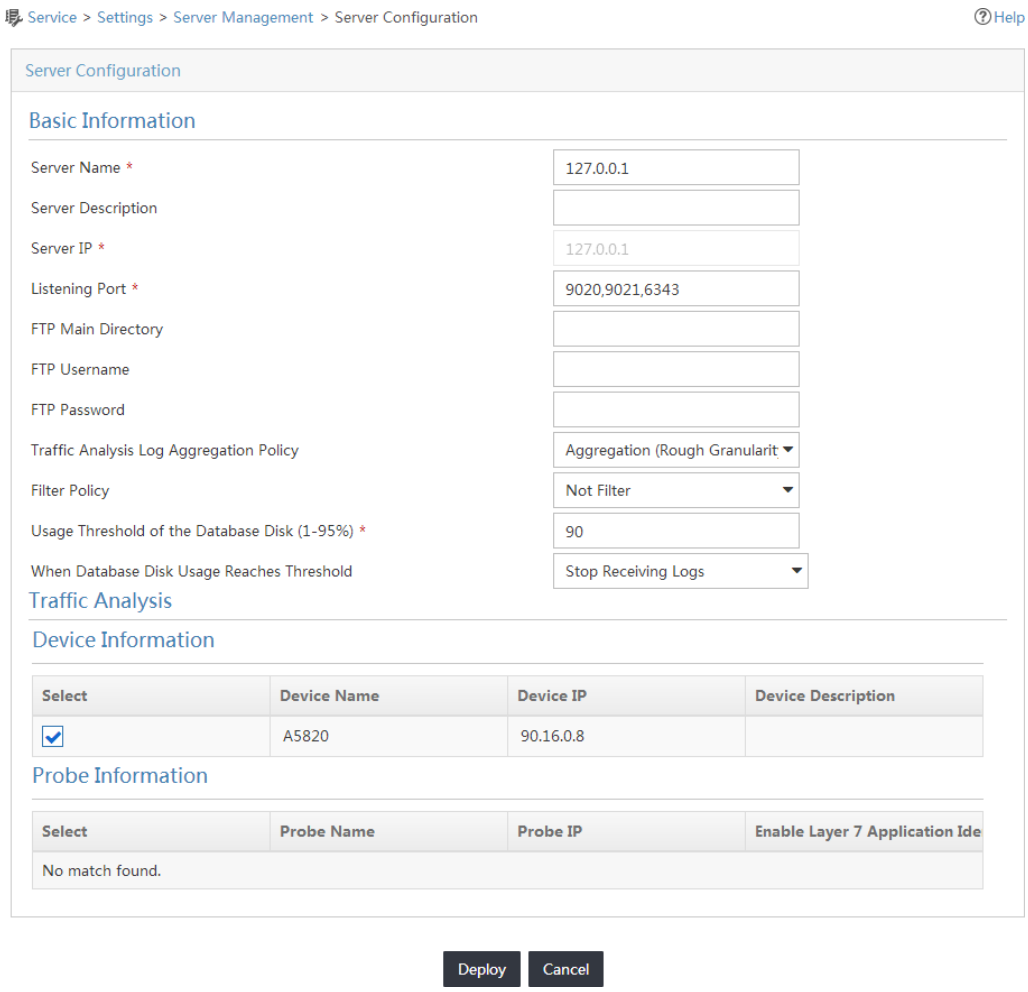
   図5 Server Management ページへのアクセス



3. IPアドレスが127.0.0.1のNTAサーバーのModifyアイコンをクリックします。

   Server Configurationページが開きます。
4. 図6に示すように、以下のパラメータを変更する:
   a. Device Information領域で、ホストトラフィックを分析するデバイスを選択します。この例では、IPアドレスが90.16.0.8のデバイスを選択します。
   b. 他のパラメータにはデフォルト値を使用します。
5. Deployをクリックします。

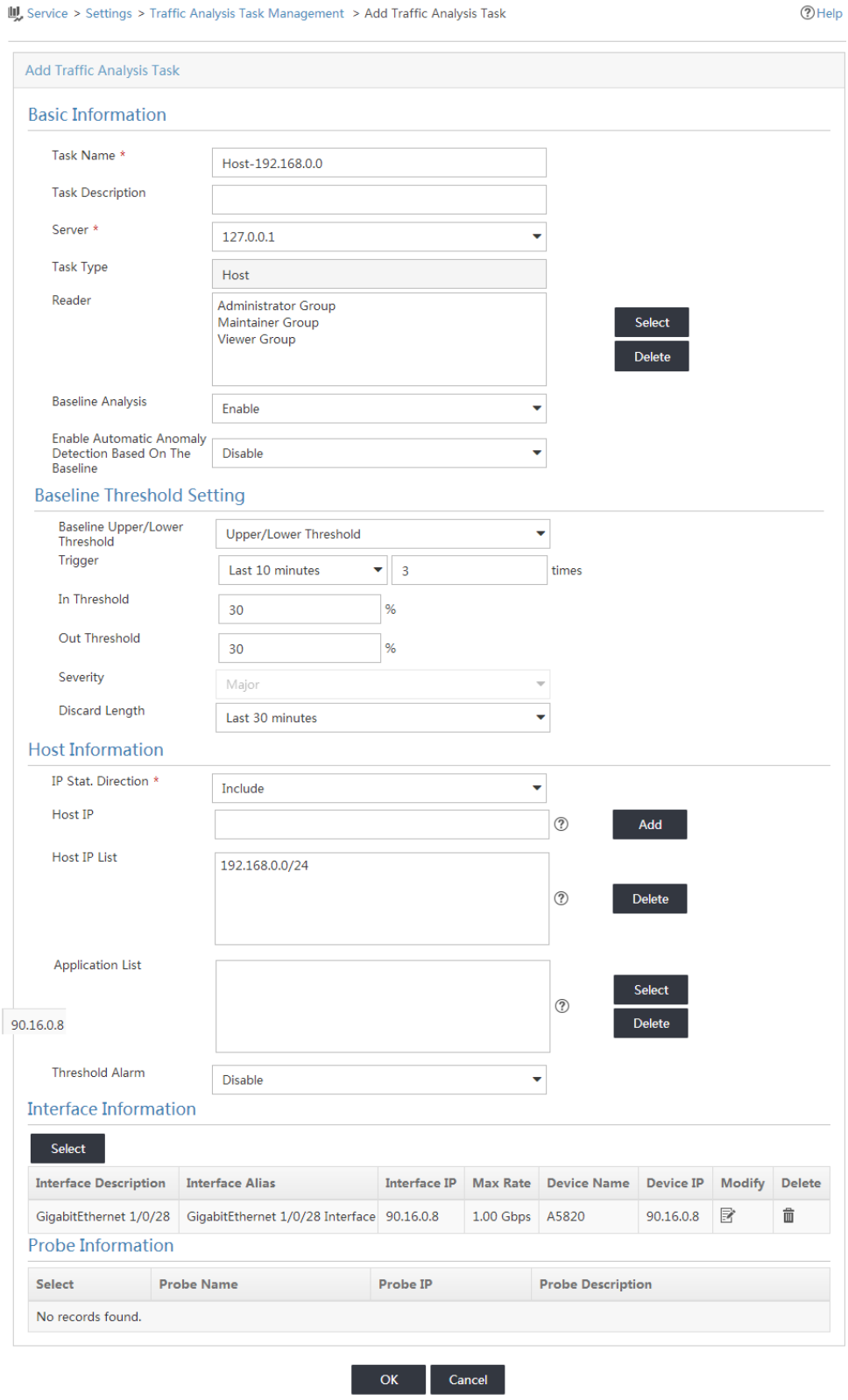
図6 NTAサーバーの設定



ホストトラフィック分析タスクの追加

1. Settingsページにアクセスします。
2. **Traffic Analysis Task Managementをクリックします。**
   Traffic Analysis Task Managementページが開きます。
3. Addをクリックします。
   Select task typeページが開きます。
4. Hostを選択し、Nextをクリックします。
   Add Traffic Analysis Taskページが開きます。
5. 図7に示すように、次のパラメータを設定します。

図7 ホストトラフィック分析タスクの追加



a. Task NameフィールドにHost-192.168.0.0と入力します。

b. Readerフィールドの横にあるSelectをクリックします。

c. 開いたウィンドウで、タスクおよびタスクによって生成されたレポートを表示する権限を持つオペ

レータグループを選択し、OKをクリックします。

この例では、管理者グループ、メンテナグループ、およびビューアグループを使用します。

d. Baseline Analysis listリストからEnableを選択します。

Enable Automatic Anomaly Detection Based Based the Baselineフィールドと Baseline Threshold Setting領域が表示されます。

e. **Enable Automatic Anomaly Detection Based On The BaselineでDisableを選択します。** となります。

f. Baseline Threshold Setting領域で、In ThresholdとOut Thresholdに30と入力します。 フィールドに入力し、他のパラメータのデフォルト値を使用します。

g. IP Stat.DirectionリストからIncludeを選択します。

h. Host IPフィールドに192.168.0.0/24と入力します。Host IPフィールドの横にあるAddをクリックして、IPセグメントをホストIPリストに追加します。

i. Application Listフィールドの横にあるAddをクリックして、監視対象のアプリケーションを追加します。この例では、アプリケーションは選択されません。

j. Interface Information領域でSelectをクリックします。

k. 開いたページでGigabitEthernet1/0/28を選択し、OKをクリックします。

6. OKをクリックします。

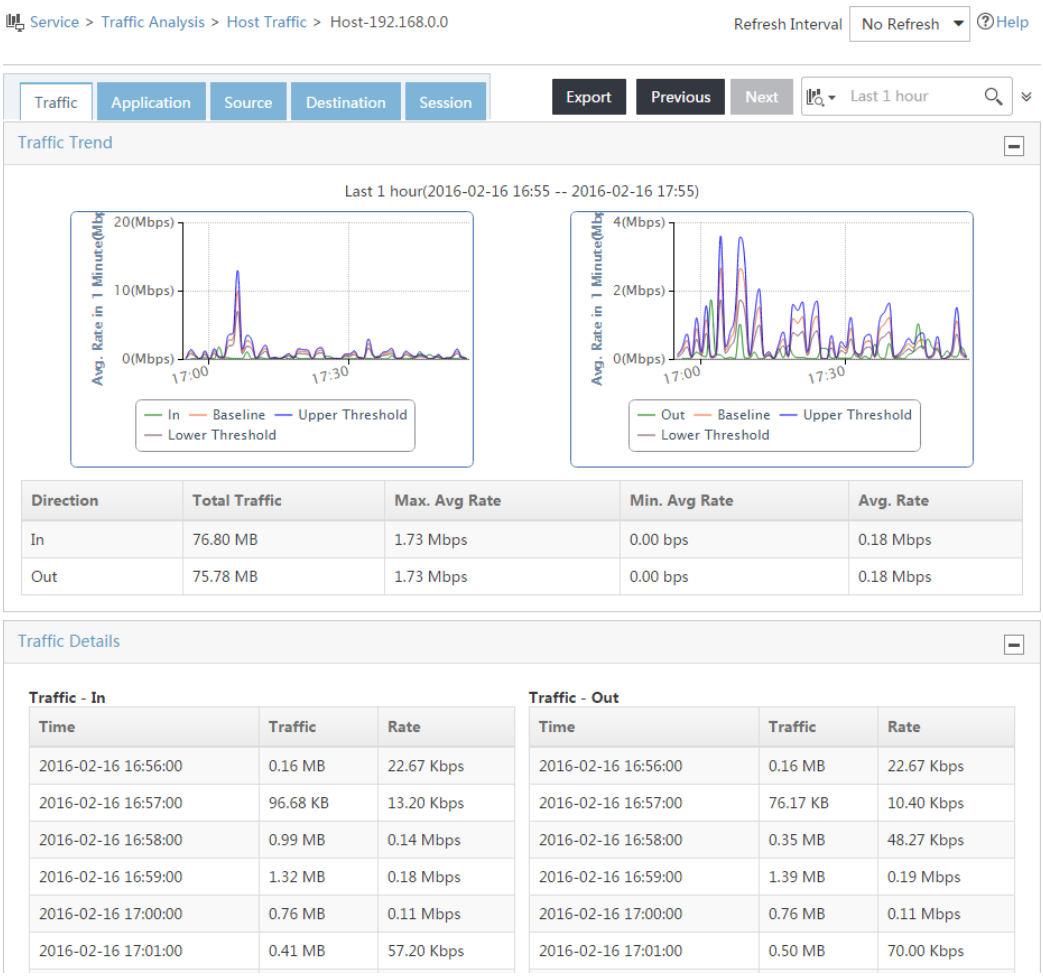
設定の確認

1. Serviceタブをクリックします。

2. ナビゲーションツリーで、Traffic Analysis and Audit>Host Traffic Analysis Task> Host-192.168.0.0を選択します。

Host-192.168.0.0ページには、図8に示すように、ネットワークセグメント192.168.0.0内のすべてのアプリケーションのトラフィック傾向とトラフィックの詳細が表示されます。

図8 トラフィック分析結果の表示



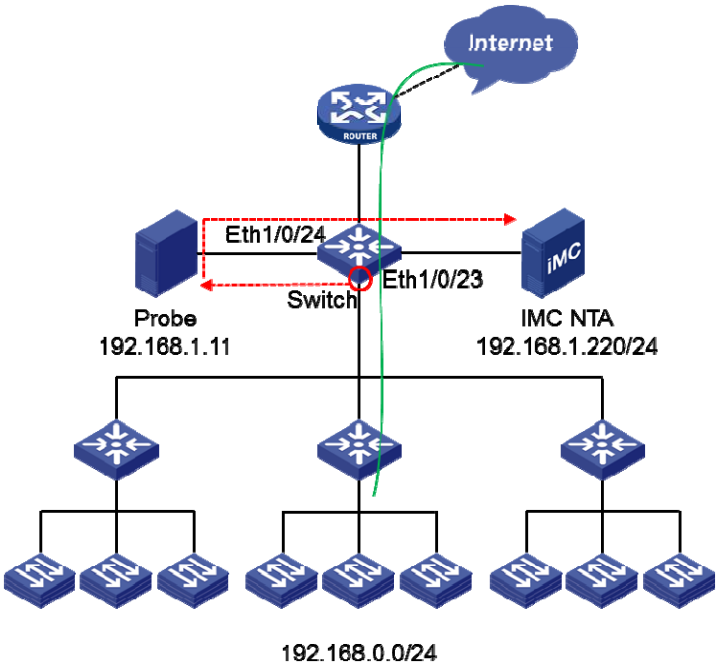
例:プローブを使用したトラフィック統計情報の収集

ネットワーク構成

NTAを使用してネットワークセグメント192.168.0.0/24内のホストによって生成されたネットワークトラフィックを監視するには、図9に示すように、次のタスクを実行します。

- Ethernet 1/0/23上のトラフィックに関する情報を収集するようにプローブを設定します。
- トラフィック情報をNTAサーバーに送信するようにプローブを設定します。

図9 ネットワーク図



要件の分析

プローブを使用してトラフィック情報を収集および送信するには、次の作業を実行します。

- スイッチ上でローカルポートミラーリングを設定します。
- Ethernet1/0/23を送信元ポートとして設定し、Ethernet1/0/24を監視ポートとして設定します。
- プローブをEthernet1/0/24に直接接続します。
- トラフィック情報をFTP経由でNTAサーバーに送信するようにプローブを設定します。

使用されるソフトウェアバージョン

この設定例は、H3C S3600V2-28TP-EIスイッチ、H3C Comware Software、バージョン5.20、リリース2103で作成および検証されています。

スイッチの設定

#ローカルミラーリンググループ1を作成します。

<Switch> system-view

[Switch] mirroring-group 1 local

#ローカルミラーリンググループ1を設定して、イーサネット1/0/23上の双方向トラフィックを監視します。

[Switch] mirroring-group 1 mirroring-port Ethernet1/0/23 both

#Ethernet1/0/24をローカルミラーリンググループ1の監視ポートとして構成します。

[Switch] mirroring-group 1 monitor-port Ethernet1/0/24

NTAサーバーの設定

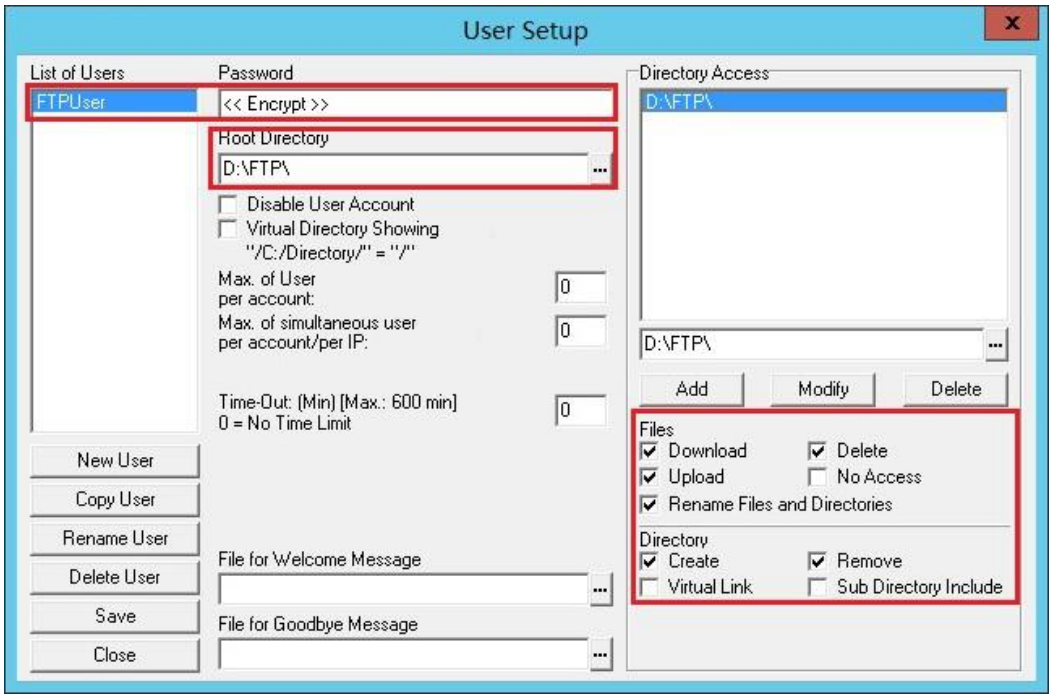
FTPの設定

1. NTAサーバーが配置されているホストにFTPサーバーを作成します。

   この例では、FTPサーバーソフトウェアTYPSoftを使用します。別のタイプのソフトウェアを使用する場合は、ソフトウェアの操作ガイドを参照して構成手順を入手してください。

2. 図10に示すように、user name、password、root directoryおよびユーザー権限を構成します。

   図10 FTPの設定



プローブの追加

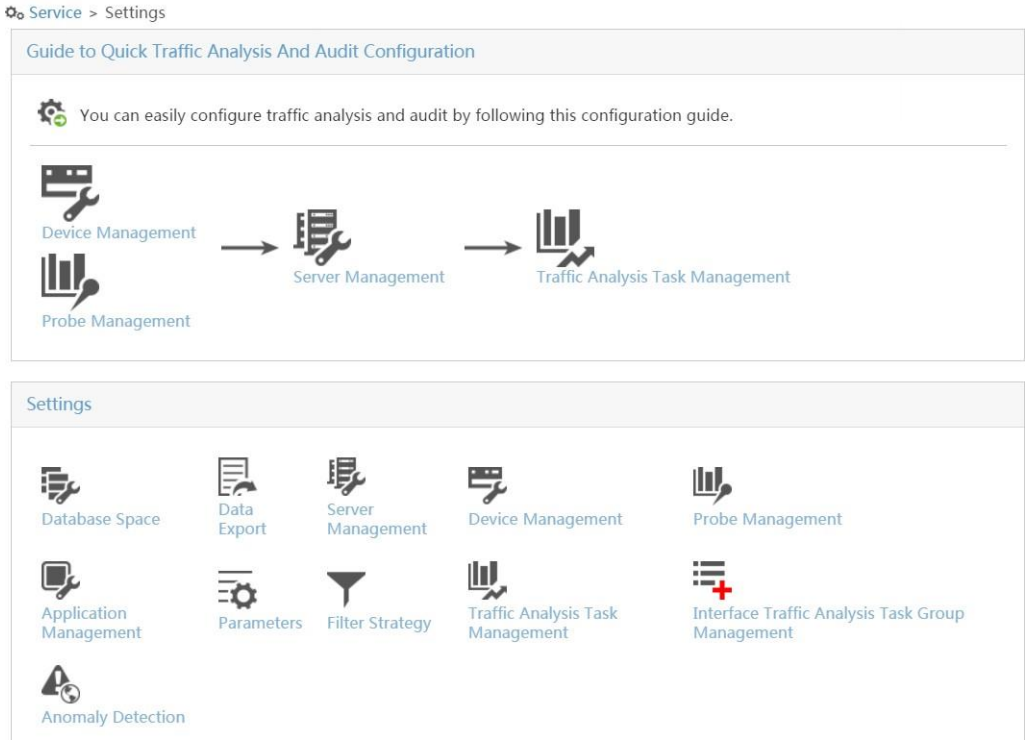
1. Serviceタブをクリックします。
2. ナビゲーションツリーで、Traffic Analysis and Audit>Settingsを選択します。

   Settingsページが開きます。

3. 図11に示すように、Probe Managementをクリックします。

   Probe Managementページが開きます。

図11 Settingsページへのアクセス



4. Addをクリックします。

   Add probeページが開きます。

5. 図12に示すように、プローブを追加します。

   a. Nameフィールドに192.168.1.11と入力します。

   b. IPフィールドにプローブのIPアドレスを入力します。

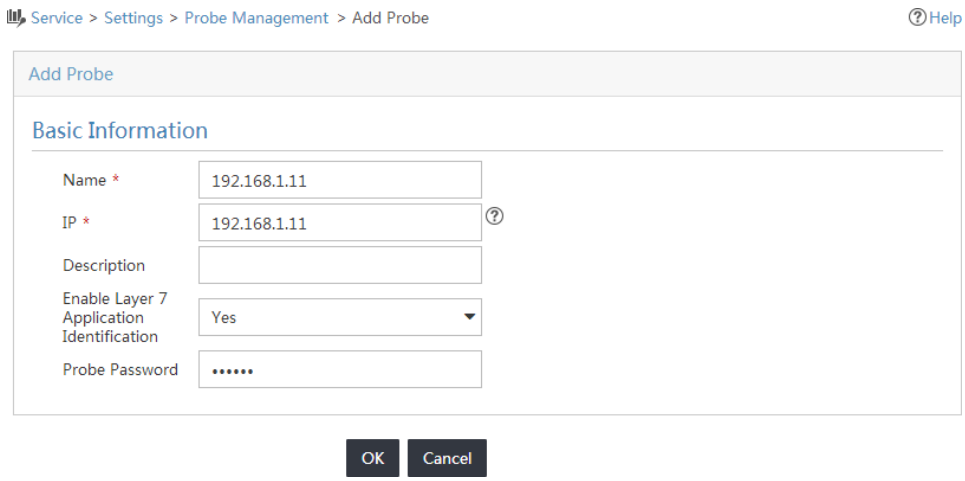
      この例では192.168.1.11を使用しています。

   c. Enable Layer7Application IdentificationでYesを選択します。

   d. Probe Passwordフィールドに、プローブのインストール時に設定したパスワードを入力します。

   e. OKをクリックします。

図12 プローブの追加



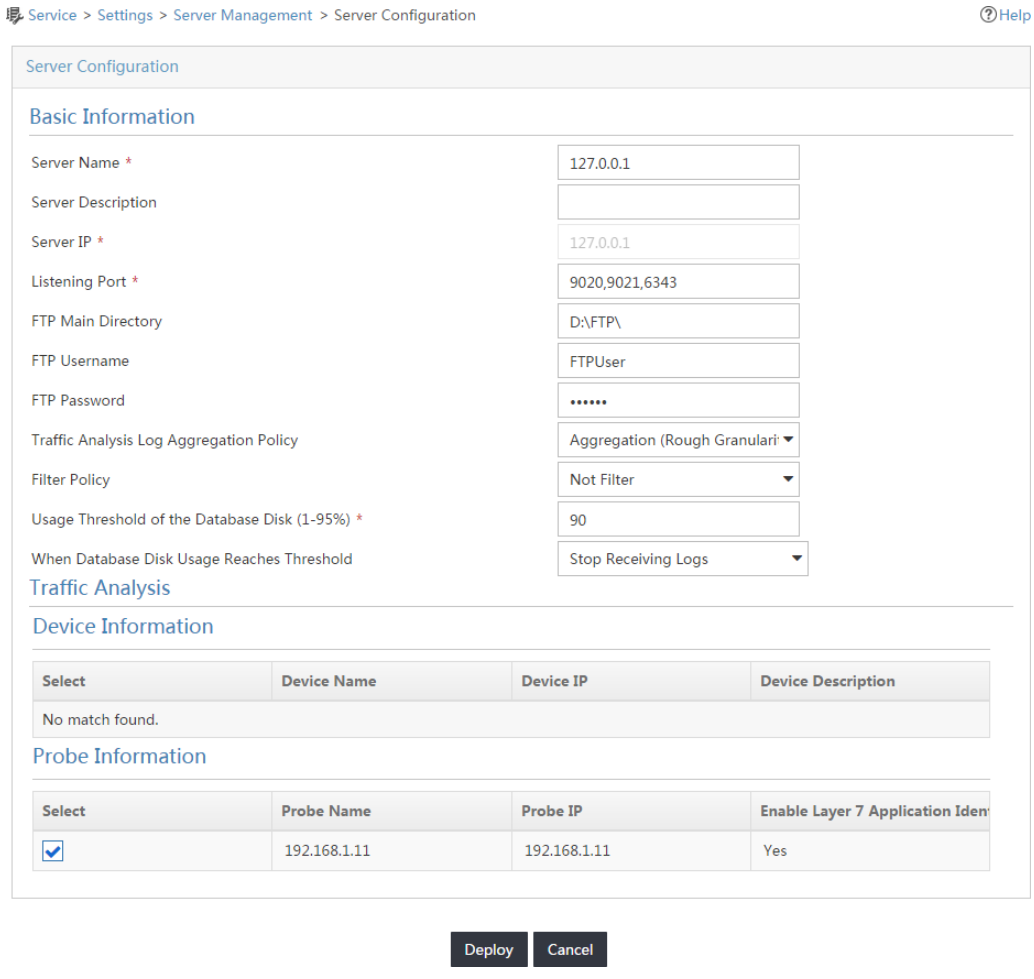
NTAサーバー構成の配布

1. Settingsページにアクセスします。
2. Server Managementをクリックします。

   Server Managementページが開きます。
3. IPアドレスが127.0.0.1のサーバーのModifyアイコンをクリックします。

   Server Configurationページが開きます。
4. 図13に示すように、次のパラメータを変更します。
   a. FTP Main Directoryフィールドに、FTPサーバーに構成されているディレクトリを入力します。この例では、D:\FTP\と入力します。
   b. FTP UsernameフィールドとFTP Passwordフィールドに、FTPサーバーで設定されているユーザー名とパスワードを入力します。
   c. Probe Information領域で、IPアドレスが192.168.1.11のプローブを選択します。
   d. 他のパラメータにはデフォルト値を使用します。
5. Deployをクリックします。

図13 NTAサーバーの設定



ホストトラフィック分析タスクの追加

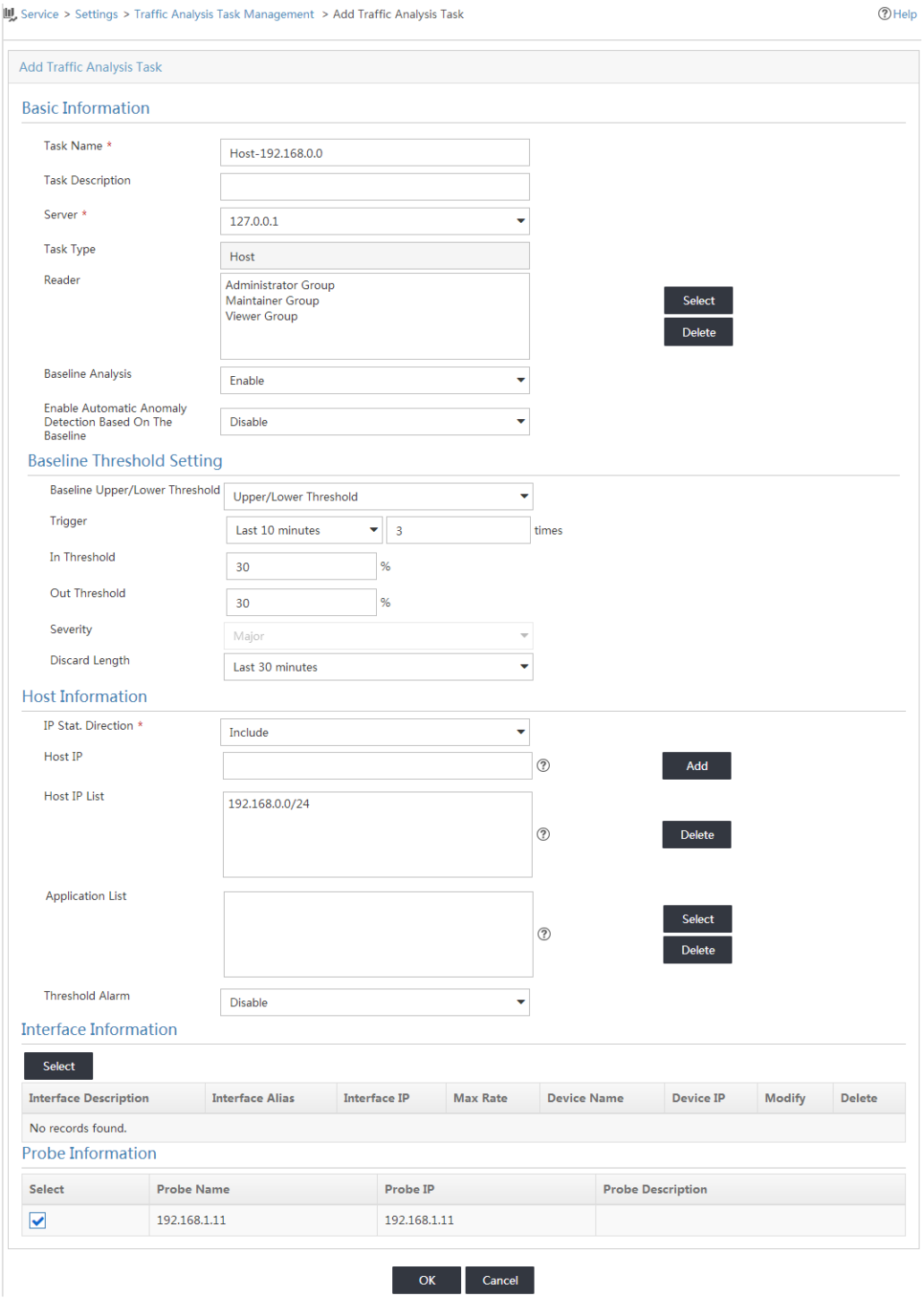
1. Settingsページにアクセスします。
2. Traffice Analysis Task Managementをクリックします。

   Task Managementページが表示されます。
3. Addをクリックします。

   Select task typeページが開きます。
4. Hostを選択し、Nextをクリックします。

   Add Traffic Analysis Taskページが開きます。
5. 図14に示すように、トラフィック分析タスクのパラメータを設定します。

   図14 ホストトラフィック分析タスクの追加



a. Task NameフィールドにHost-192.168.0.0と入力します。

b. Readerフィールドの横にあるSelectをクリックします。

c. 開いたページでタスクを表示できるオペレータグループを選択し、OKをクリックします。

d. Host Information領域で、IP Stat.DirectionリストからIncludeを選択します。

e. Host IPフィールドに192.168.0.0/24と入力します。Addをクリックして、ホストIPをホストIPリストに追加します。

f. Baseline AnalysisリストからEnableを選択します。

Enable Automatic Anomaly Detection Based Based the BaselineフィールドとBaseline Threshold Settings領域が表示されます。

g. Enable Automatic Anomaly Detection Based On The BaselineリストでDisableを選択します。

h. Baseline Threshold Setting領域で、In ThresholdとOut Thresholdに30と入力します。他のパラメータのデフォルト値を使用します。

i. Application Information領域で、Addをクリックします。

j. 監視するアプリケーションを選択します。

アプリケーションを選択しない場合、タスクはすべてのアプリケーションに対してトラフィックアカウンティングを実行します。

k. Probe Information領域で、IPアドレスが192.168.1.11のプローブを選択します。

6. OKをクリックします。

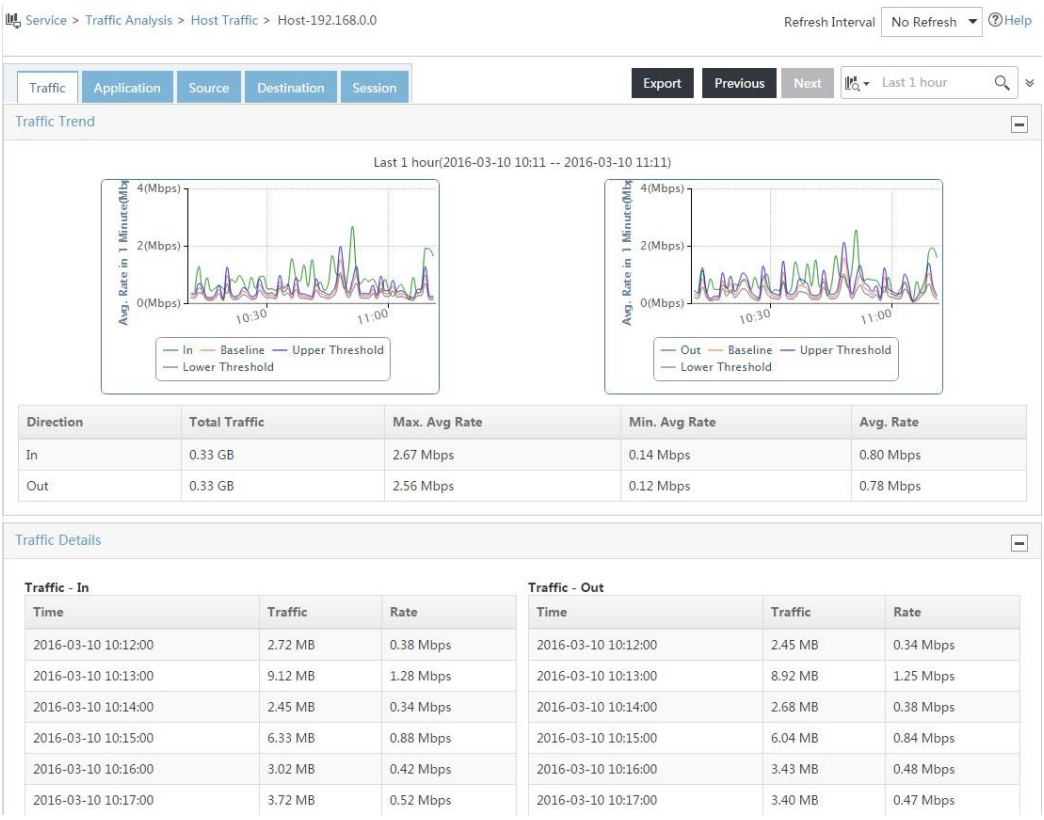
設定の確認

1. Serviceタブをクリックします。

2. ナビゲーションツリーで、Traffic Analysis and Audit>Application Traffic Analysis Task>Host-192.168.0.0を選択します。

Host-192.168.0.0ページには、図15に示すように、ネットワークセグメント192.168.0.0内のすべてのアプリケーションのトラフィック傾向とトラフィックの詳細が表示されます。

図15 トラフィック分析結果の表示



Direction	Total Traffic	Max. Avg Rate	Min. Avg Rate	Avg. Rate
In	0.33 GB	2.67 Mbps	0.14 Mbps	0.80 Mbps
Out	0.33 GB	2.56 Mbps	0.12 Mbps	0.78 Mbps

Time	Traffic	Rate
2016-03-10 10:12:00	2.72 MB	0.38 Mbps
2016-03-10 10:13:00	9.12 MB	1.28 Mbps
2016-03-10 10:14:00	2.45 MB	0.34 Mbps
2016-03-10 10:15:00	6.33 MB	0.88 Mbps
2016-03-10 10:16:00	3.02 MB	0.42 Mbps
2016-03-10 10:17:00	3.72 MB	0.52 Mbps

Time	Traffic	Rate
2016-03-10 10:12:00	2.45 MB	0.34 Mbps
2016-03-10 10:13:00	8.92 MB	1.25 Mbps
2016-03-10 10:14:00	2.68 MB	0.38 Mbps
2016-03-10 10:15:00	6.04 MB	0.84 Mbps
2016-03-10 10:16:00	3.43 MB	0.48 Mbps
2016-03-10 10:17:00	3.40 MB	0.47 Mbps