H3C iMC NTAの導入

内容

- NTAの特徴
- NTAの設定
- トラブルシューティング

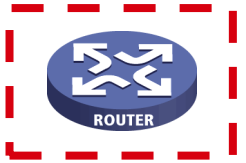
iMCのシステム構造

モニタリング

iMC

点

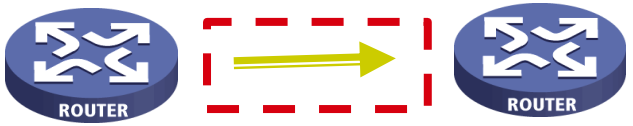
PLAT/APM/SSM



Platform(PLAT)
Application Manager(APM)
Security Service Manager(SSM)

線

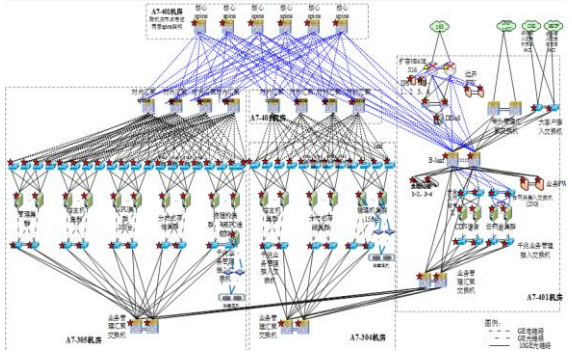
NTA/NPD/MVM



Network Traffic Analyzer(NTA)
Network Performance Diagnosis(NPD)
MPLS VPN Manager(MVM)

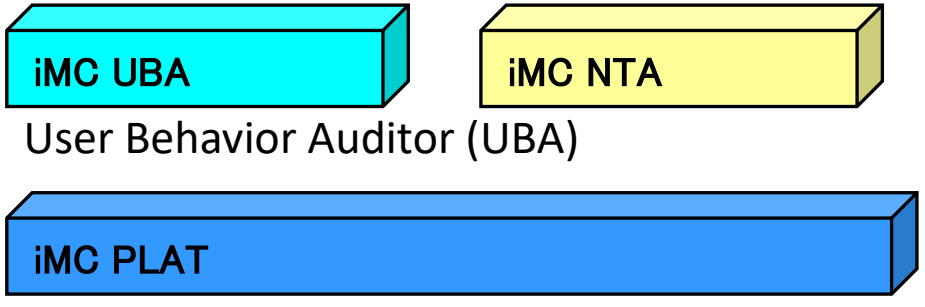
システム

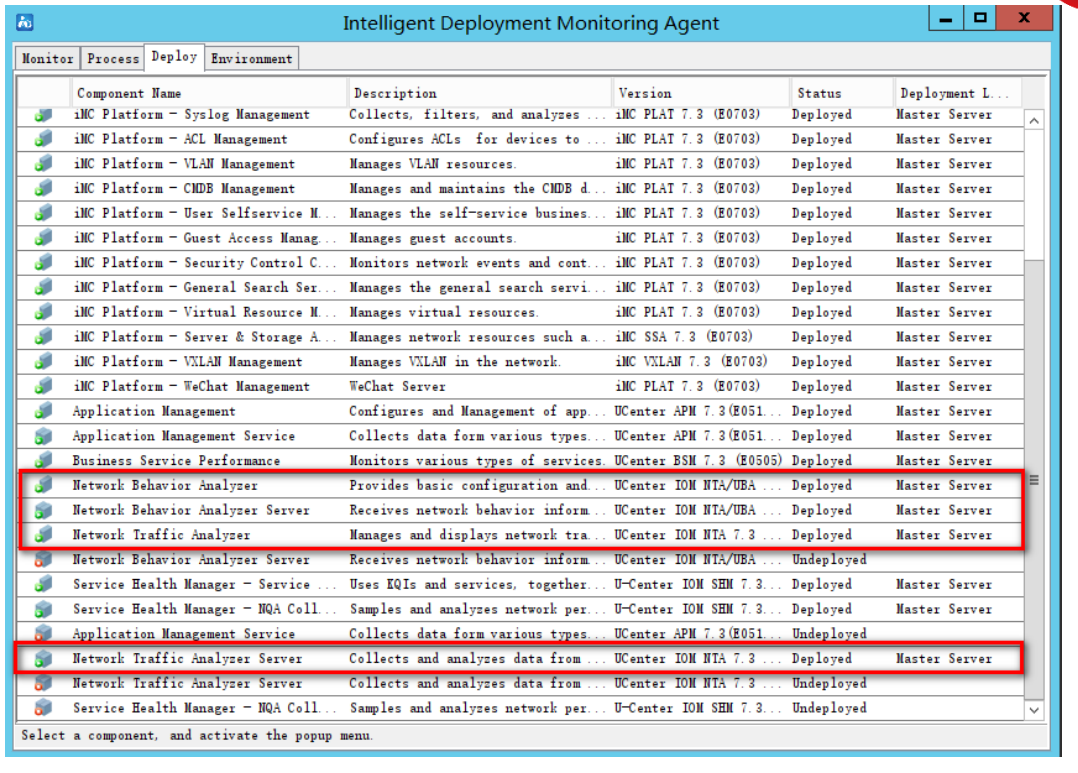
BSM/CMDB



Business Service Manager(BSM)
Configuration Management Database Management(CMDB)

NTAの簡単な紹介





- NTAは、プラットフォームに基づくiMCのコンポーネントです。
- NTAコンポーネントには、ネットワーク動作解析、ネットワーク動作解析サーバ、ネットワークトラフィック解析、ネットワークトラフィック解析サーバが含まれます。

- ネットワークトラフィック分析およびネットワークトラフィック分析は、iMCメインサーバーにインストールされたNTAのインタフェースおよび構成を管理します。ネットワークトラフィック分析サービスおよびネットワークトラフィック分析サーバーは、NTA固有のビジネスロジック、ログデータ分析、集計などを管理します。分散した方法で導入できるため、パフォーマンスのロードバランスを実現

NTA基本環境に関する注意事項

- 環境要求事項
  - ✓ PLATと同じバージョン
  - ✓ 高パフォーマンスのサーバー
  - ✓ 場合によっては複数サーバーの導入
  - ✓ CPU/メモリー/ディスク容量などのハードウェア要因
- 異なるシナリオ
  - ✓ Netstream: 全てのデータを検査するために処理の負荷がかかります。そのため1秒あたりに処理されるログの量に配慮する必要があります
  - ✓ SFlow: データをサンプリングして検査するため、データが大量である場合に有効です。考慮する点としては、どれ位の数のインタフェースにSflowを設定するかです
  - ✓ DIG: DIGコレクタによって処理されるトラフィック量に配慮

NTA基本環境に関する注意事項

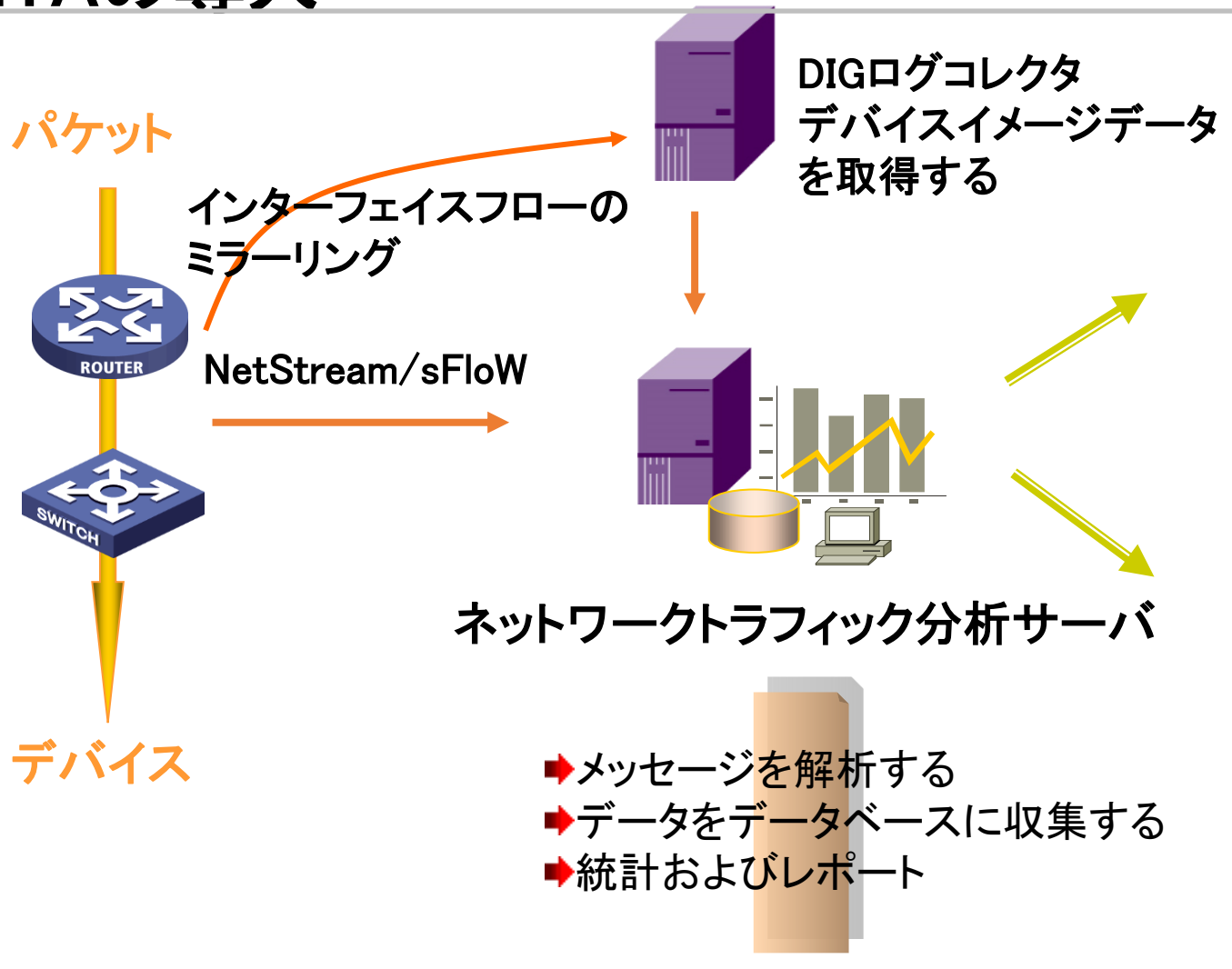
比較項目	NetFlow	SFlow
データ取得方法	全データ	サンプリング
プロトコル	IPパケットのみ。ただし、v9からはMACアドレスも対象可能。	レイヤー2からレイヤー7のパケットが対象
処理の特徴	大量のトラフィックの場合、高パフォーマンスなサーバーを要求される	大量のトラフィックでもサンプリングするため効率よく処理できる
パケットの検証方法	トラフィックパターンのテンプレートを予め用意し、パターンと異なるトラフィックの発見に強い	トラフィックをサンプリングして検証するためより詳細のデータが確認できる

NTAライセンス

プロジェクトコード	モデル	説明	
0231A816	SWP-IMC-NTAW-CN	functional module-H3C iMC-SW7M1NTAW-Network traffic analysis component-pure software (CD)	The NTA must be configured PLAT
3130A212	LIS-IMC-NTAA-CN-1	License-H3C iMC-SW7M1NTAA-Network traffic analysis component license fee-manage 1 device	
3130A213	LIS-IMC-NTAB-CN-2	License-H3C iMC-SW7M1NTAB-iMC-SW7M1NTAA-Network traffic analysis component license fee-manage 2 device	
3130A214	LIS-IMC-NTAC-CN-5	License-H3C iMC-SW7M1NTAC-iMC-SW7M1NTAA-Network traffic analysis component license fee-manage 5 device	

- iMC NTAは収集ポイント(デバイスまたはプローブ)に従ってライセンスを計算します。デフォルトでは、1つの収集ポイントライセンスが使用され、拡張は1/2/5に分割されます。
  デバイス上に複数のNetStreamボードがある場合、各NetStreamボードは収集ポイントとなります。

NTAの導入



主な機能
H3Cのさまざまなルータ、スイッチ、およびポートミラーリングをサポートするすべてのネットワークデバイスと連携
NetStreamやSflowなどの複数のログフォーマットをサポート
ベースラインのインテリジェントな確立、異常なトラフィックに対する自動アラーム
P2Pアプリケーショントラフィックの監視および分析
MACおよびホスト名に基づくトラフィック監視
データベース使用スペースのリアルタイム監視

NTAの導入

- 管理される装置へのNetStreamのコンフィグ

ステップ	コマンド	備考
1.システムビューに入ります。	System-view	該当なし
2.NetStreamの従来のデータエクスポートの宛先アドレスと宛先UDPポート番号を設定します。	**ip netstream export *host*** *ip-address udp-port* [**vpn-instance** *vpn-instance-name*]	デフォルトでは、宛先アドレスまたは宛先UDPポート番号は設定されていません。
3.インタフェースビューに入ります。	**Interface** *interface-type interface-number*	該当なし
4.インタフェースでNetStreamを有効にします。	**ip netstream { inbound | outbound }**	デフォルトでは、NetStreamはインターフェイス上でディセーブルです。

NTAの導入

- 管理される装置へのNetStreamのコンフィグ

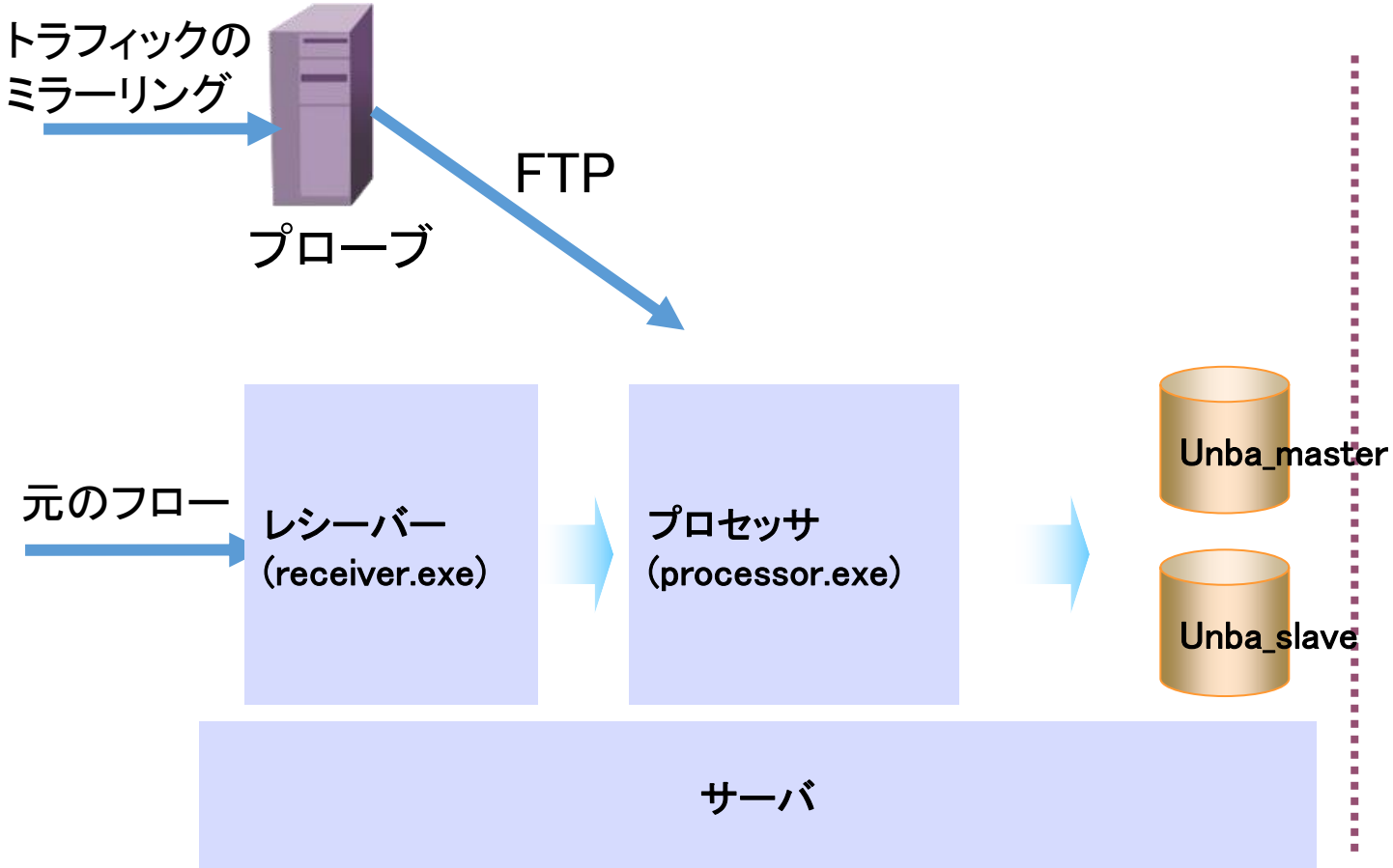
#Ten-GigabitEthernet0/1上の着信トラフィックに対してNetStreamをイネーブルにします。
[NS] system-view
[NS] interface Ten-GigabitEthernet0/1
[NS-Ten-GigabitEthernet0/1] **ip netstream inbound**
[NS-Ten-GigabitEthernet0/1] quit
#NetStreamデータエクスポートのホストとして、iMC NTAのIPアドレスとリスニングポートを指定します。
[NS] **ip netstream export host 192.168.1.220 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。
[NS] **ip netstream export version 9**

NTAの導入

- 管理される装置へのSFlowのコンフィグ

#sFlowエージェントのIPアドレスを90.16.0.9に設定します。
<3600V2> system-view
[3600V2] **sflow agent ip 90.16.0.9**
#sFlowコレクタ用に次のパラメータを設定します。
•sFlowコレクタID1。
•IPアドレス192.168.1.220。
•ポート番号6343(デフォルト)。
•説明NTA Server。
[3600V2**] sflow collector 1 ip 192.168.1.220 port 6343 description NTAServer**
#イーサネット1/0/1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。
[3600V2] interface Ethernet 1/0/1
[3600V2-Ethernet1/0/1] **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。
[3600V2-Ethernet1/0/1] **sflow counter collector 1**
[3600V2-Ethernet1/0/1] quit

NTAのシステム構造



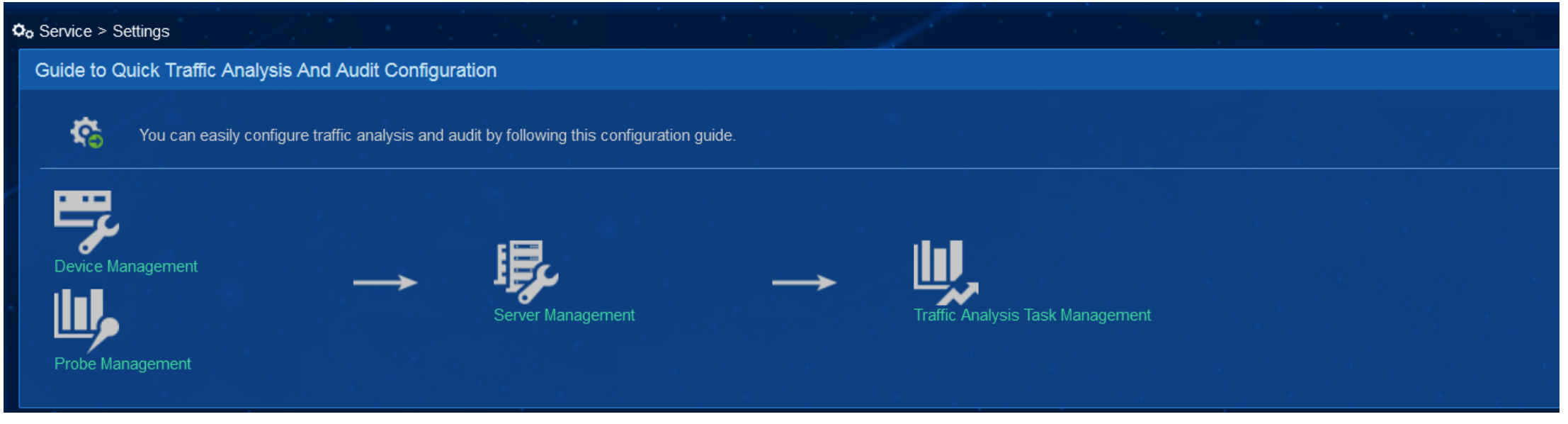
主な機能
トラフィック分析
レポートの表示
ログのダンプ
7層認識
アプリケーション分析
……

内容

- NTAの特徴
- **NTAの設定**
- トラブルシューティング

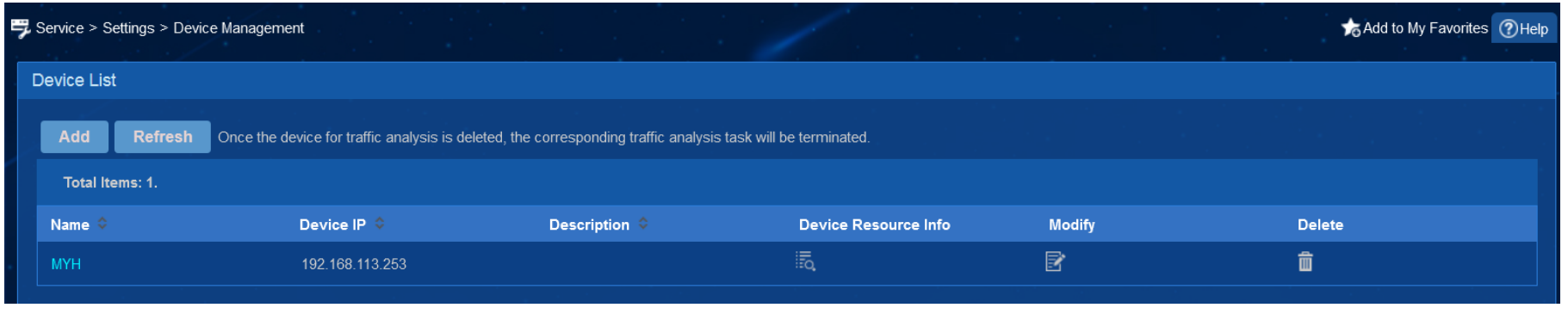
NTAの設定

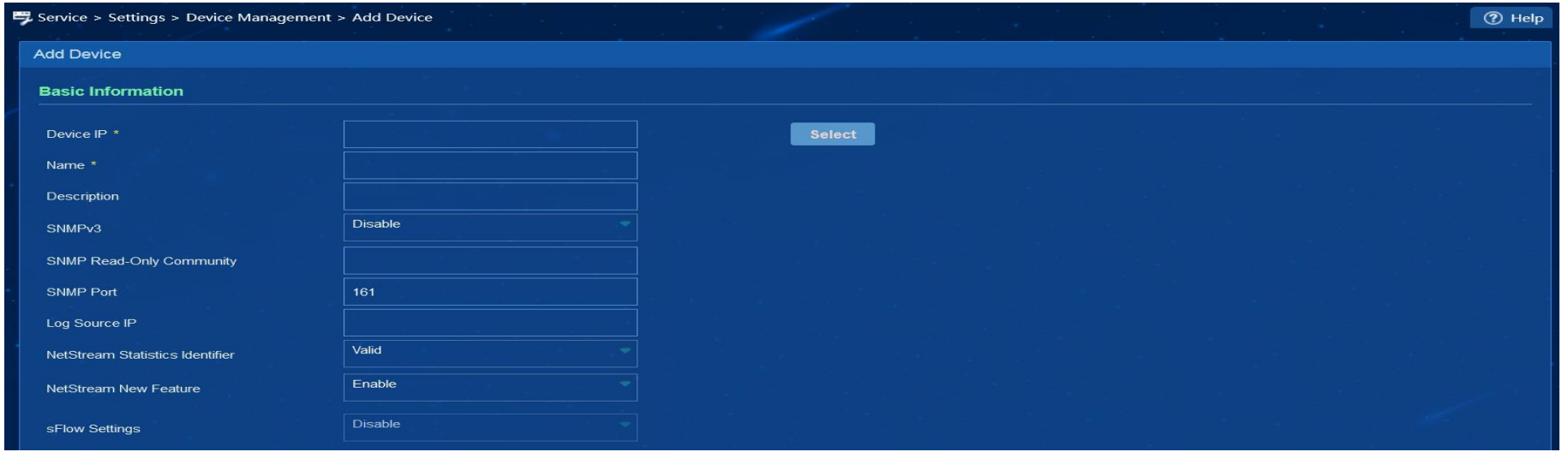
- NTA構成ガイド
  デバイス管理、プローブ管理、サーバ管理、およびトラフィック分析タスク管理を含む



NTAの設定

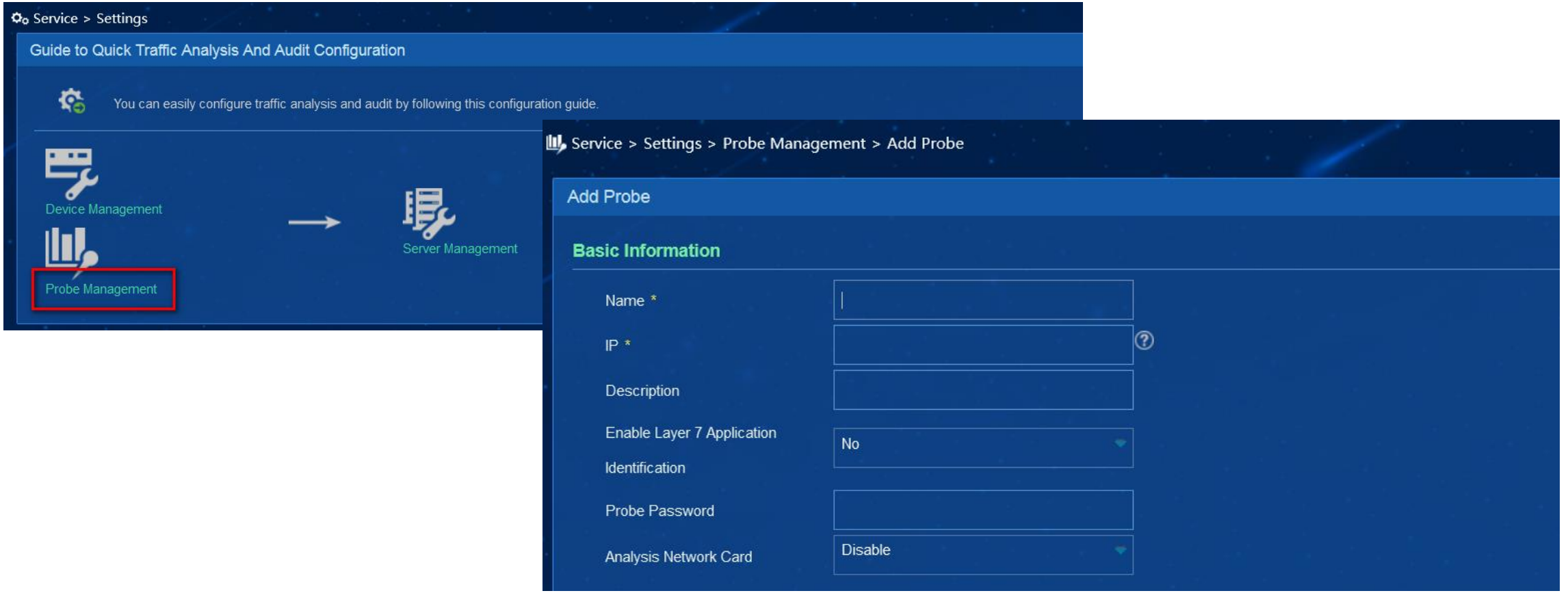
- デバイス管理
  トラフィック分析装置操作の追加、変更、および削除を含む





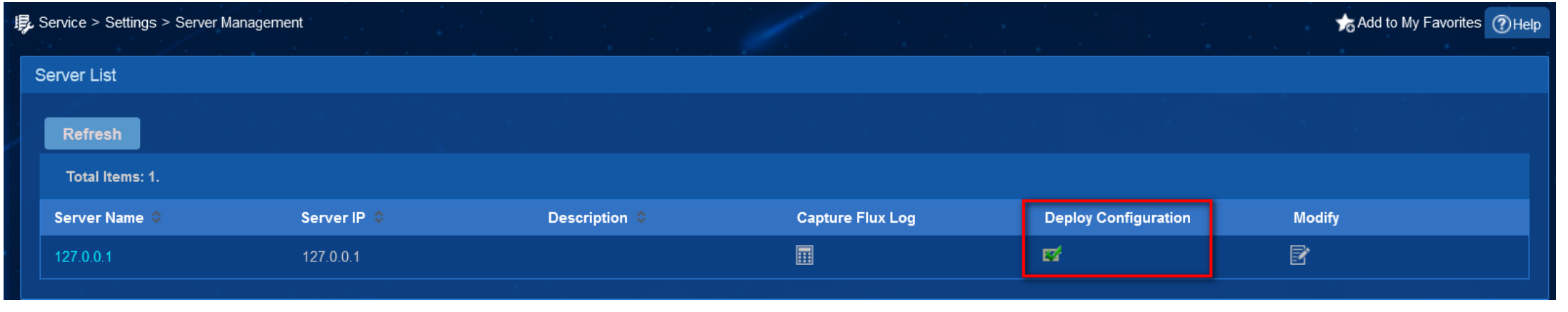
NTAの設定

- プローブ管理
  プローブ操作の追加、変更、および削除を含む

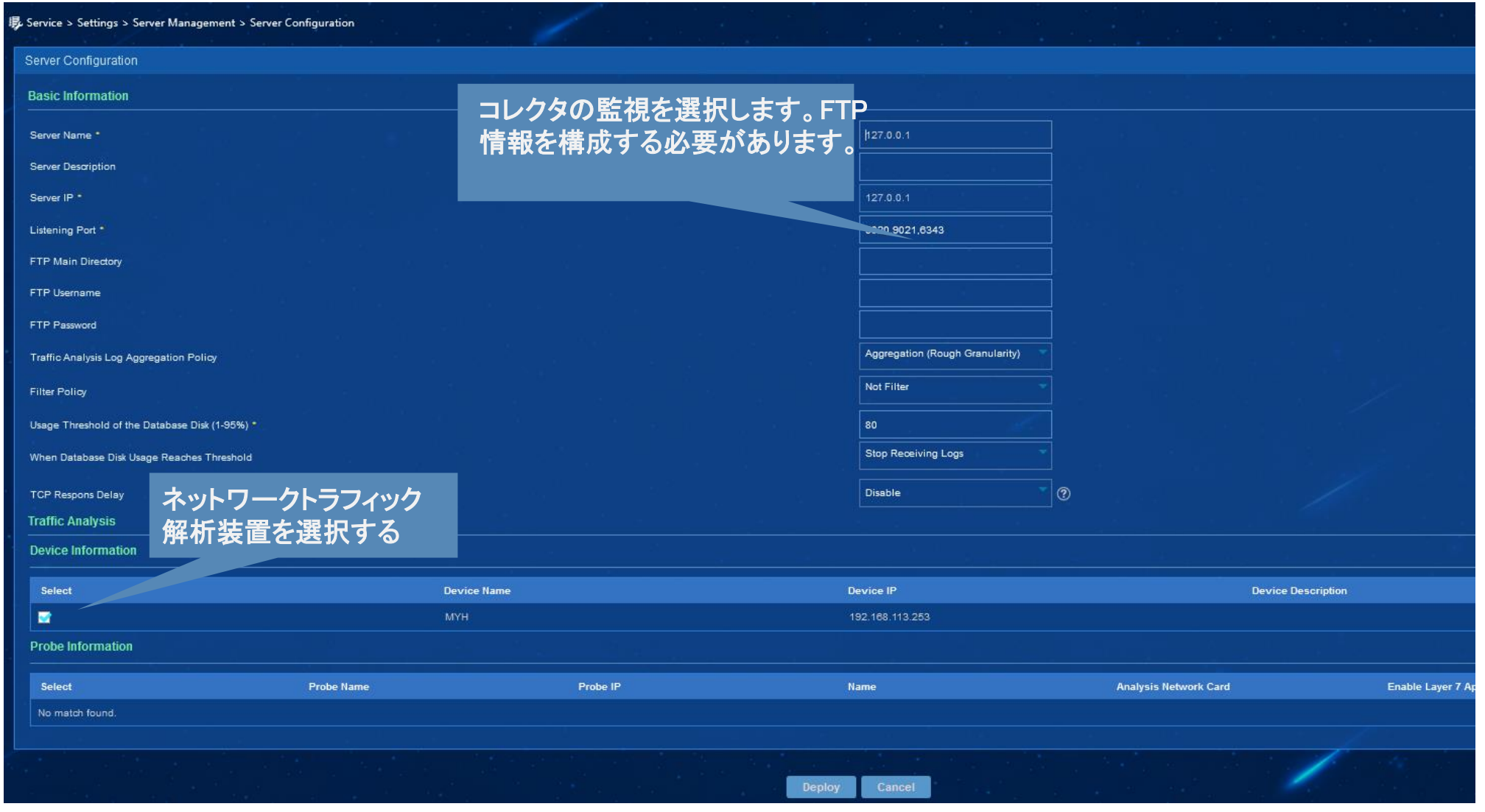


NTAの設定

- サーバ管理
  サーバ設定とは、配置されたネットワークトラフィック分析サーバコンポーネントに関連する情報の設定を指します。
  サーバの設定が完了したら、新しい設定を受信側、プロセッサ側、およびプローブ側で有効にする前に、設定を配信する必要があります。



NTAの構成(サーバー管理)

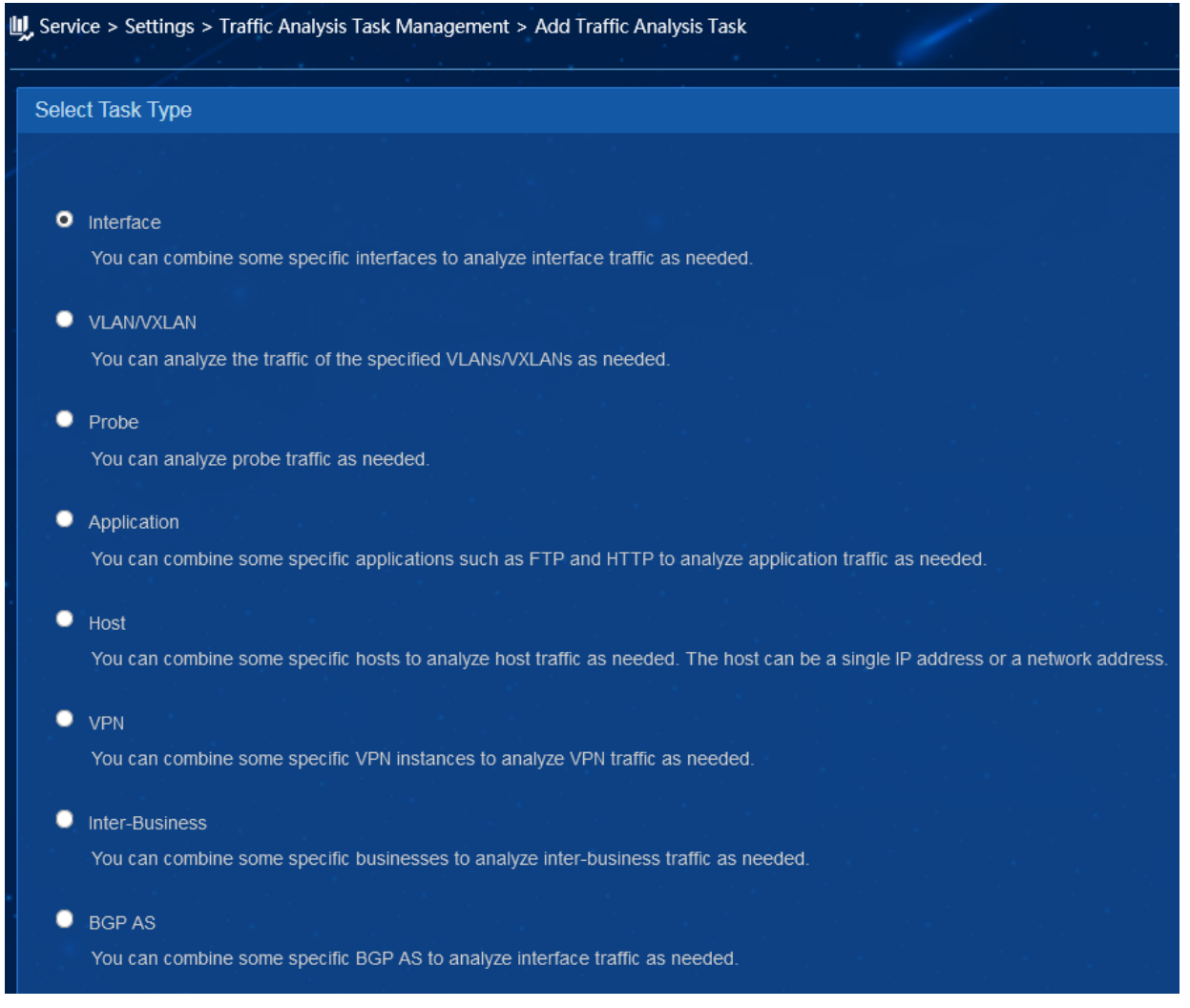


NTAの構成(サーバー管理)

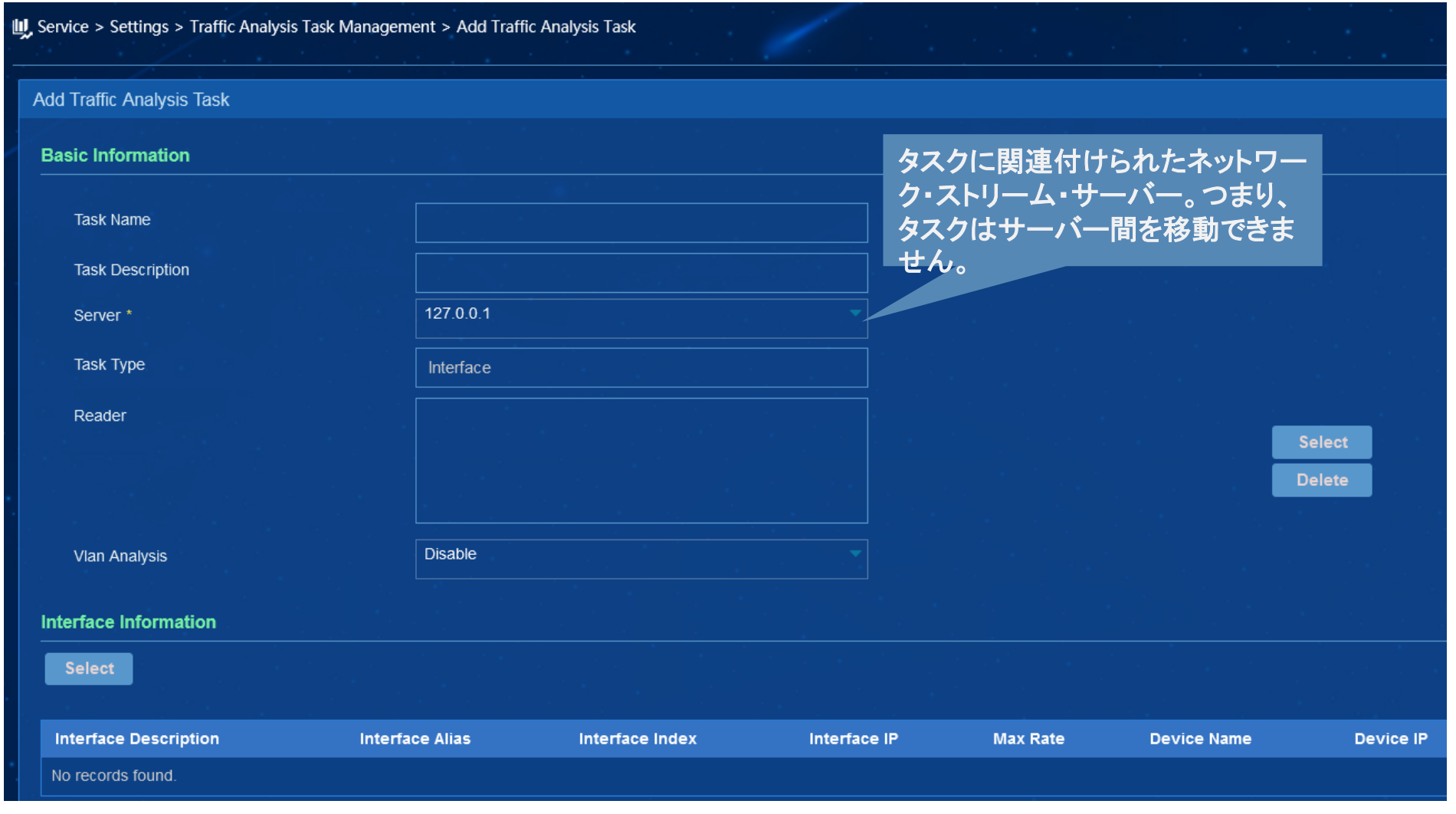
- トラフィック分析タスク

NTAコンポーネントは、複数の次元からネットワークトラフィックを分析できます。

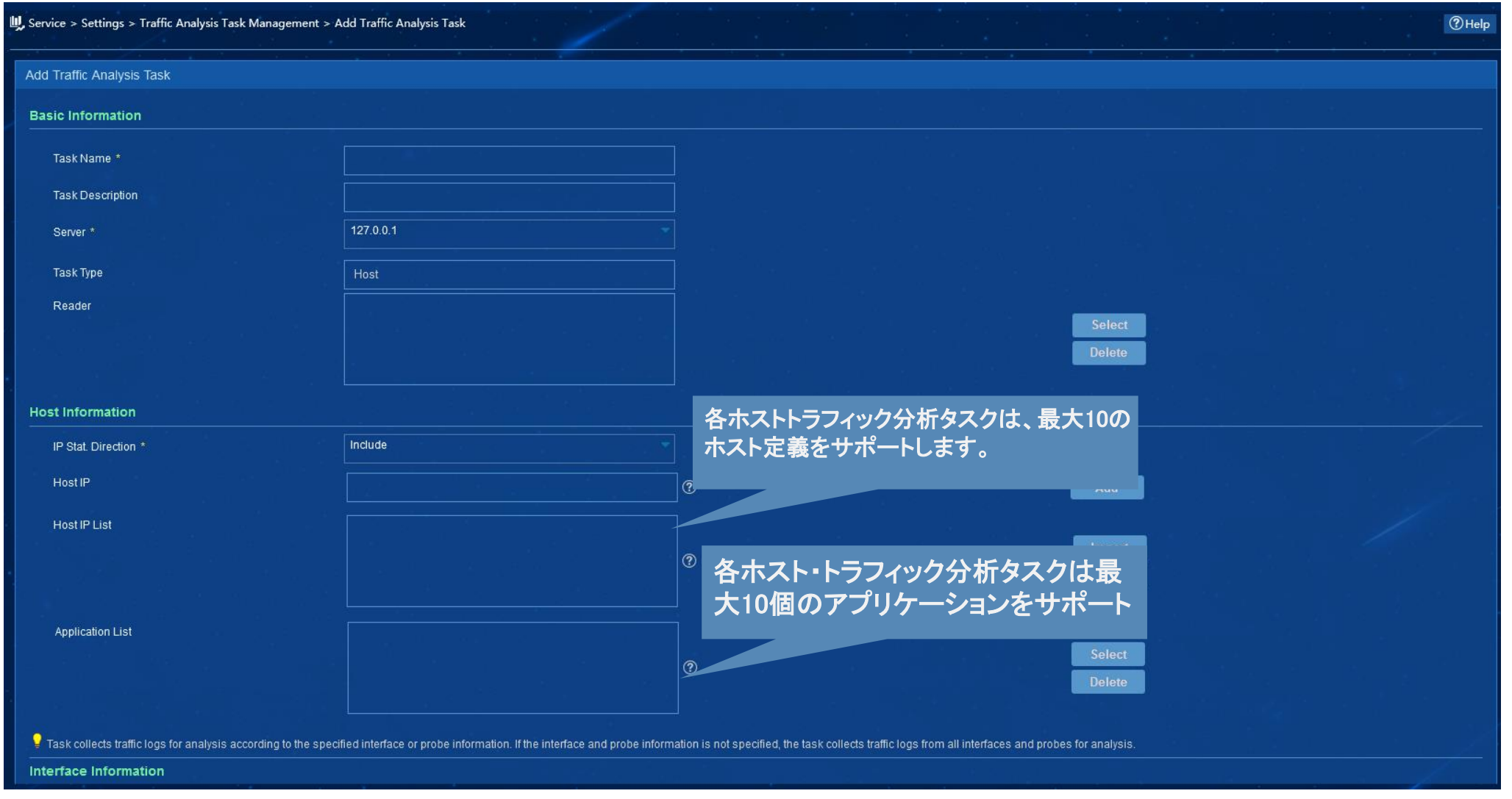
✓ インターフェイスベースのトラフィック分析
✓ VLANベースのトラフィック分析
✓ プローブベースのトラフィック分析
✓ アプリケーションベースのトラフィック分析
✓ ホストベースのトラフィック分析
✓ VPNベースのトラフィック分析
✓ BGP-ASベースのトラフィック分析
……



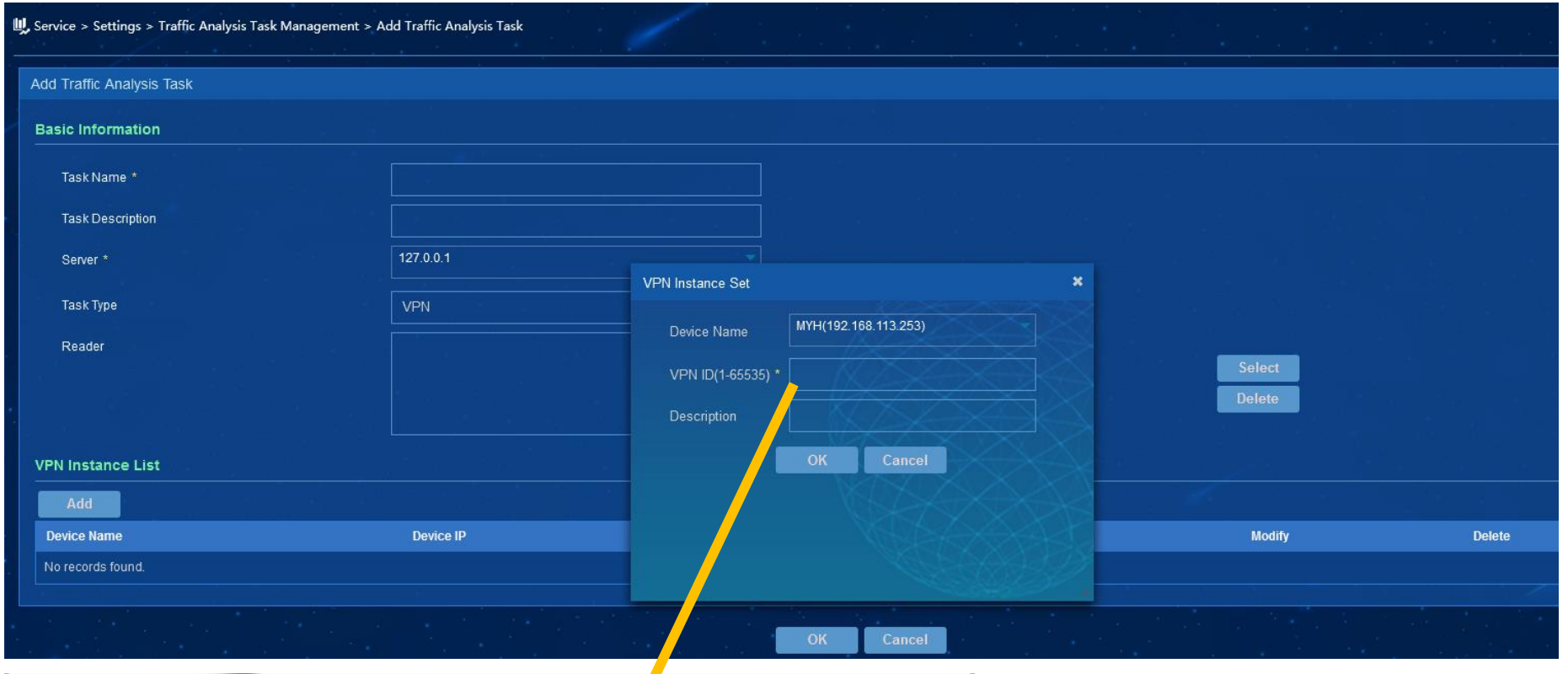
トラフィック分析タスクインターフェイス



トラフィック分析タスク:ホスト



トラフィック分析タスク:VPN




```
<Sysname> display ip vpn-instance instance-name vpn1
  VPN-Instance Name and ID : vpn1, 2
  Create time : 2006/04/08 13:01:30
  Up time : 0 days, 00 hours, 11 minutes and 42 seconds
```

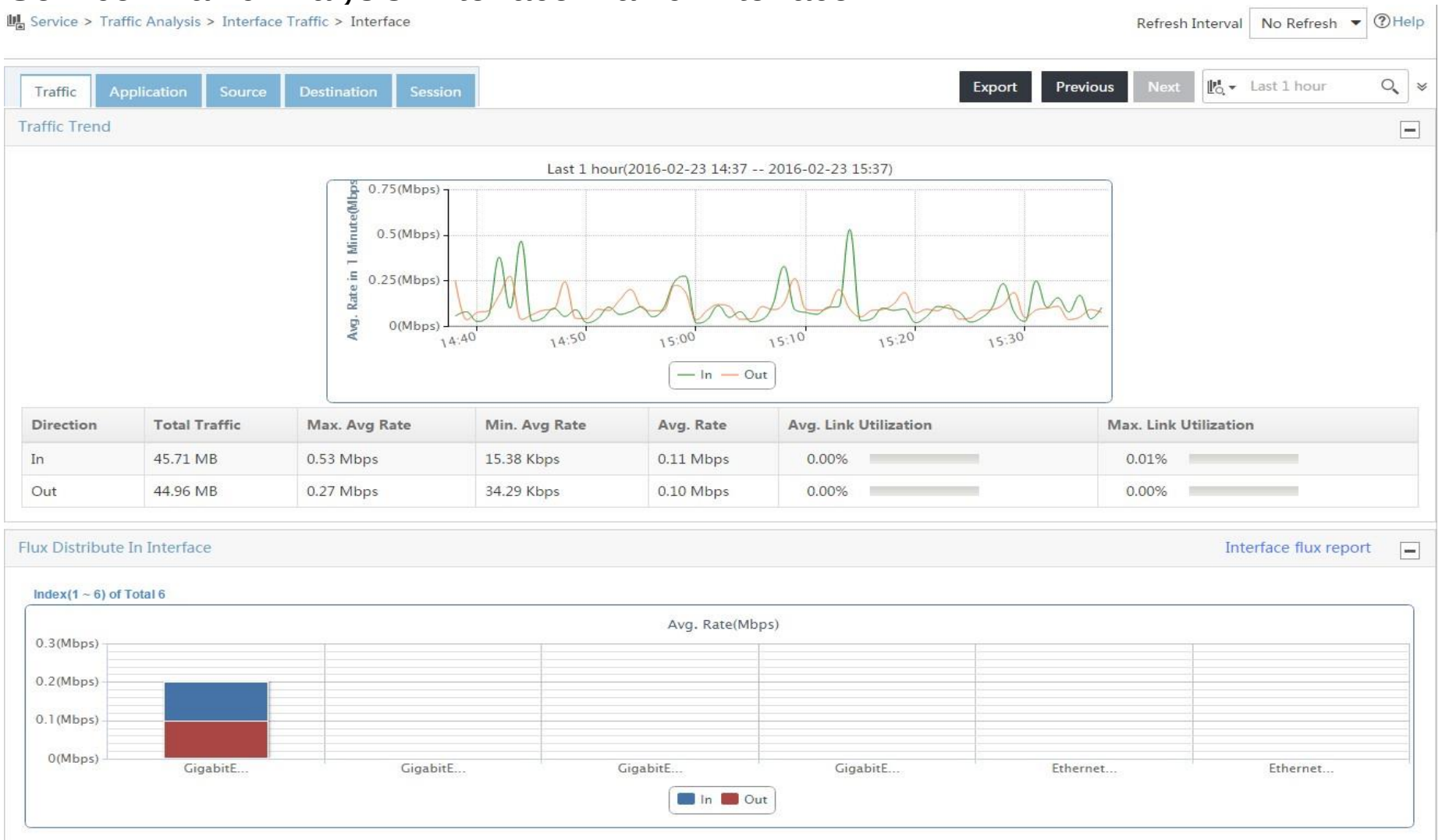
トラフィック分析タスクの情報

NetStream:インターフェイストラフィック分析タスクの概要情報

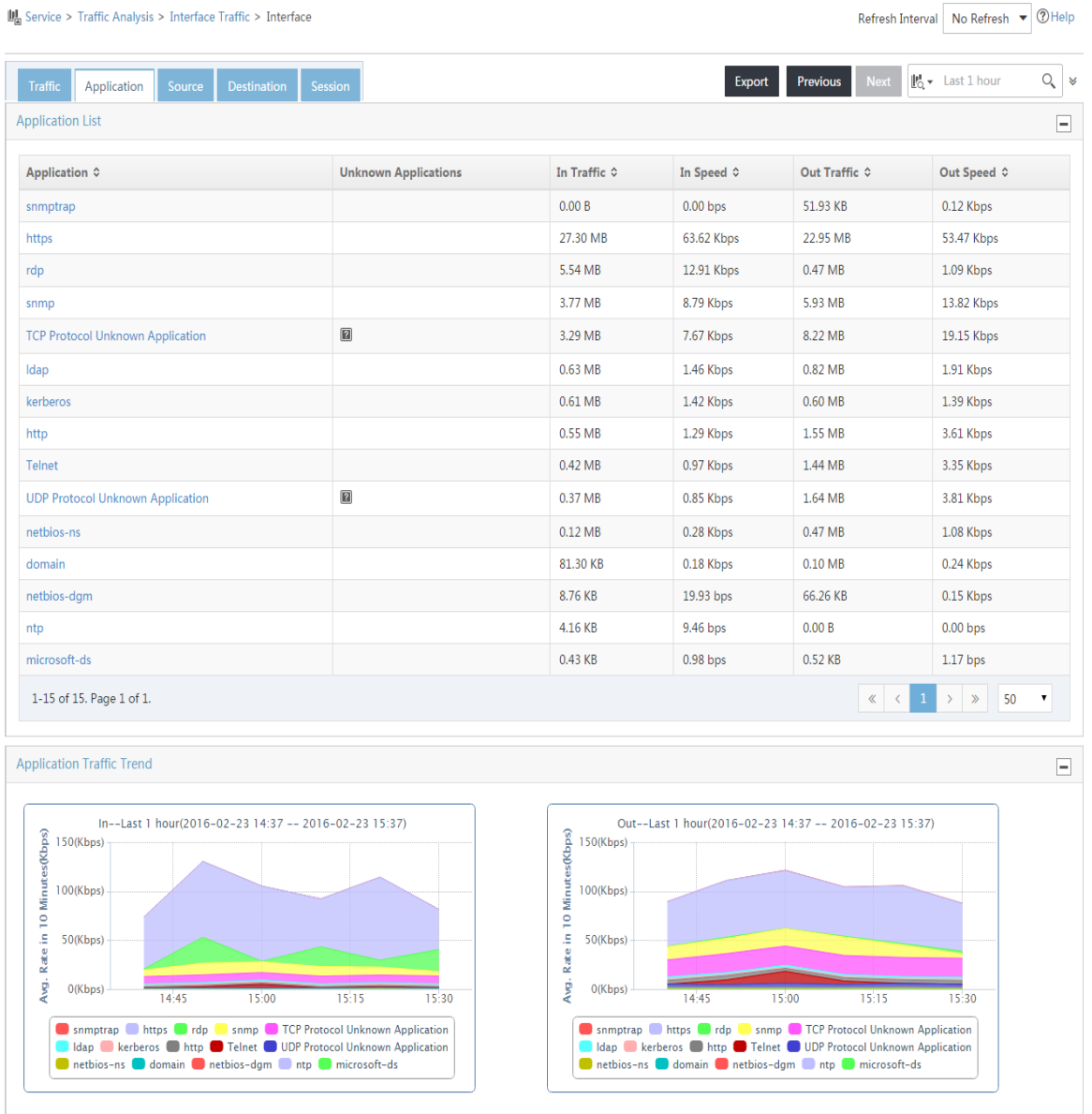
Service>Traffic Analysis>Interface Traffic

トラフィック分析タスクの情報表示

NetStream:インターフェイストラフィック分析タスクのトラフィック情報
Service>Traffic Analysis>Interface Traffic>Interface



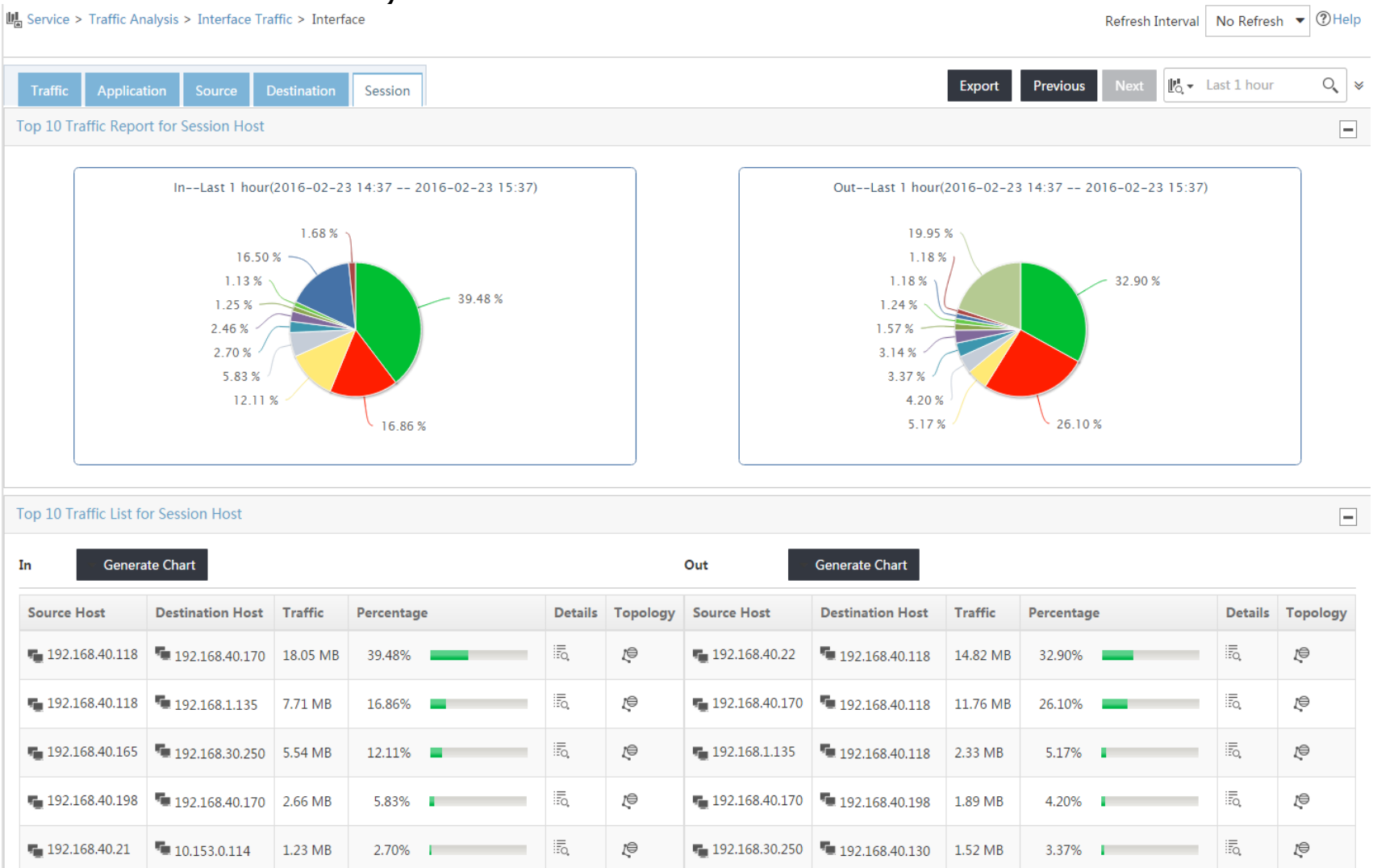
トラフィック分析タスクの情報表示



NetStream:インターフェイストラフィック分析タスクのアプリケーション情報
Service>Traffic Analysis>Interface Traffic>Interface

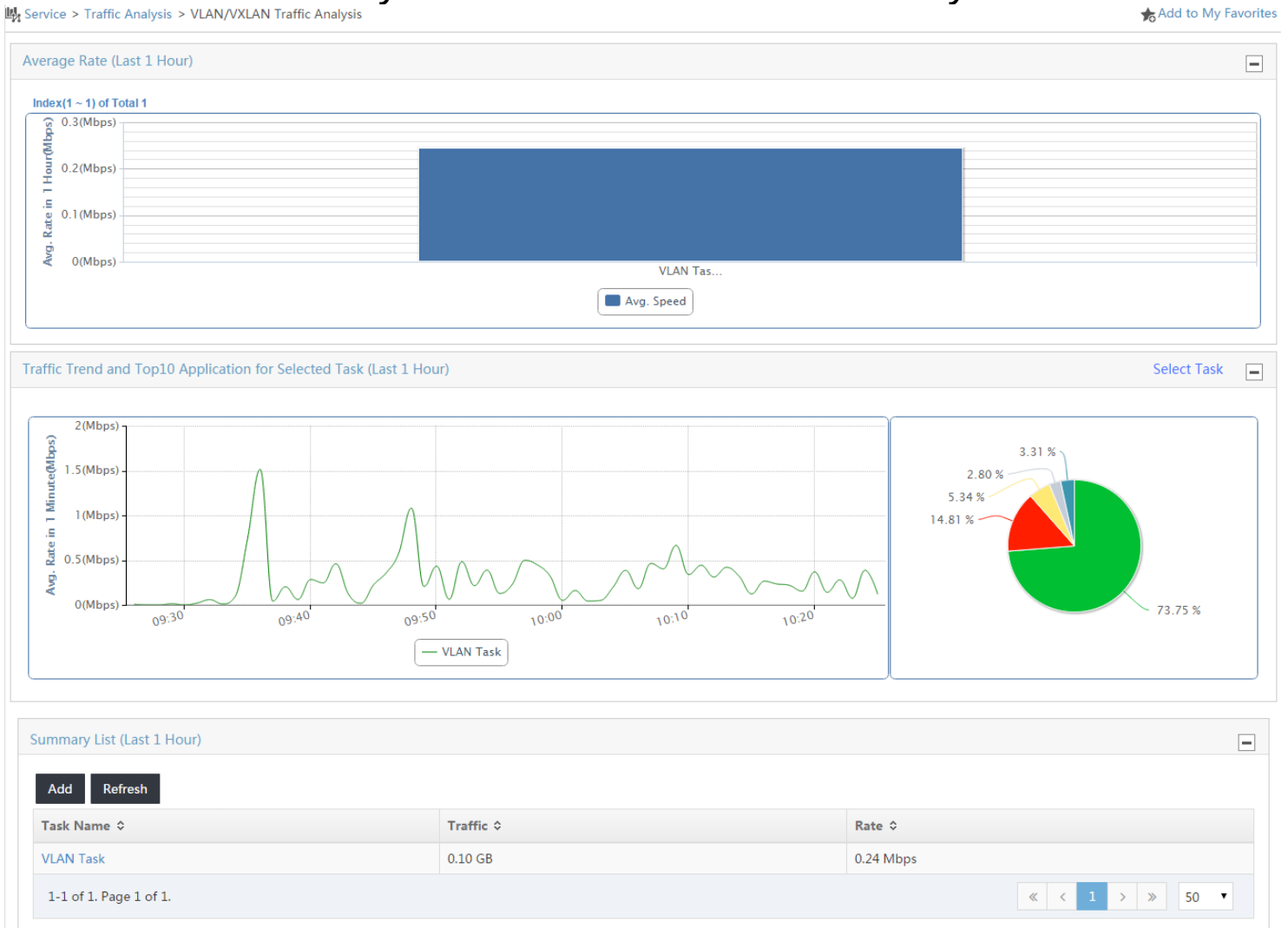
トラフィック分析タスクの情報表示

NetStream:インターフェイストラフィック分析タスクのセッション情報
Service>Traffice Analysis>Interface Traffic>Interface



トラフィック分析タスクの情報表示

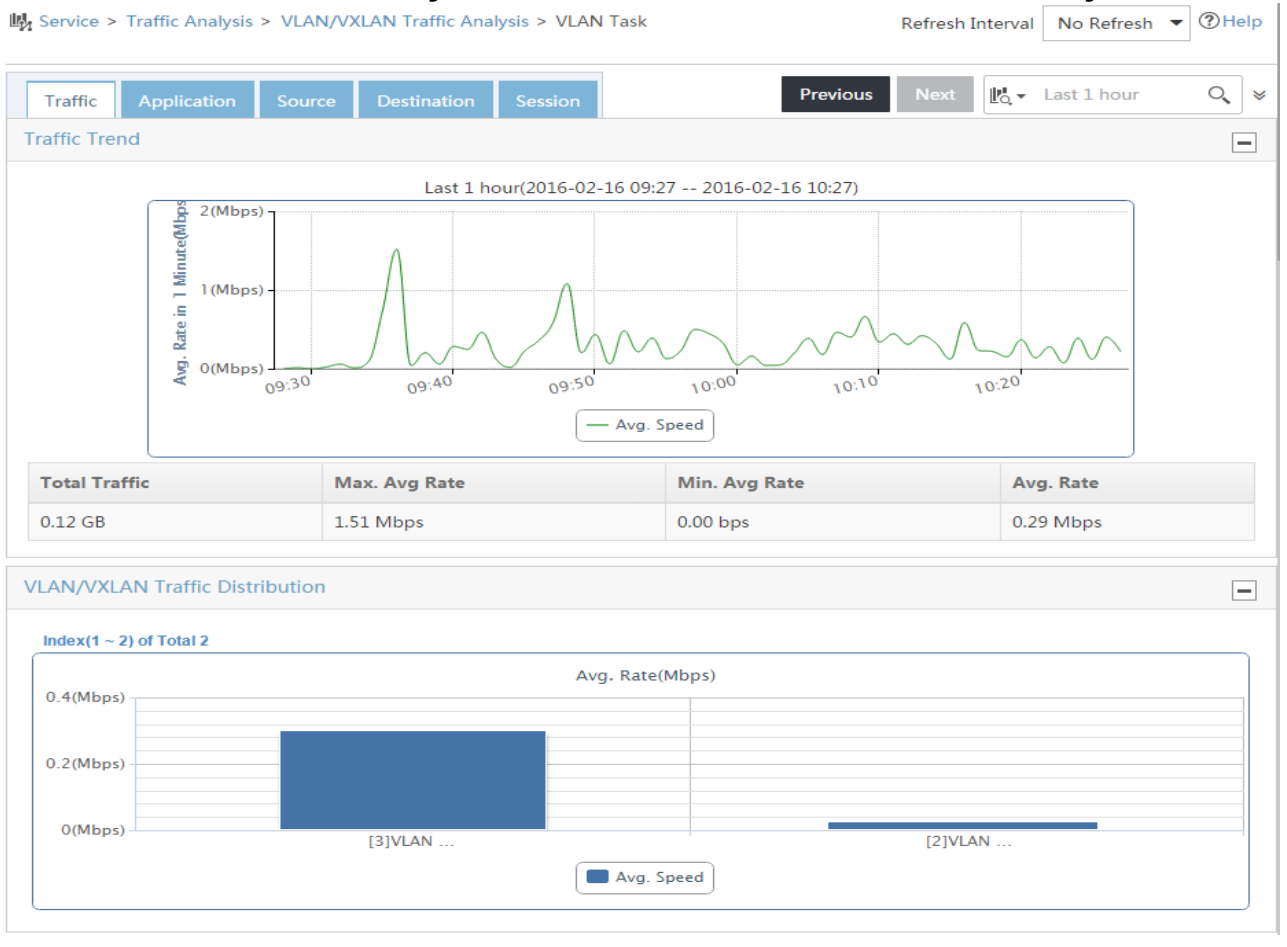
Sflow:VLANトラフィックタスクに関するサマリー情報の表示
Service>Traffic Analysis>VLAN/VXLAN Traffic Analysis



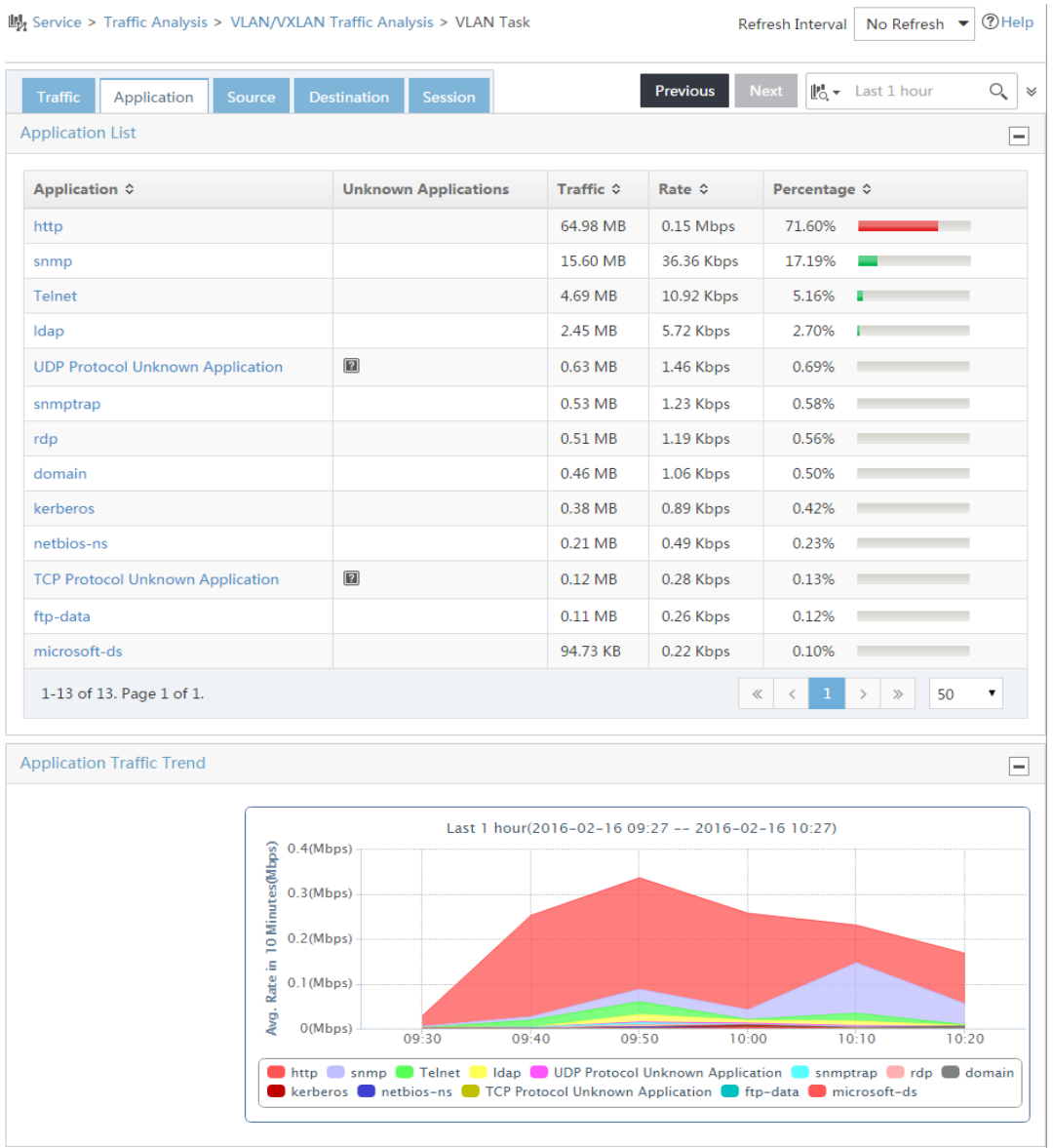
トラフィック分析タスクの情報表示

Sflow: VLANトラフィック分析タスクのトラフィック情報の表示

Service>Traffic Analysis>VLAN/VXLAN Traffic Analysis>VLAN Task

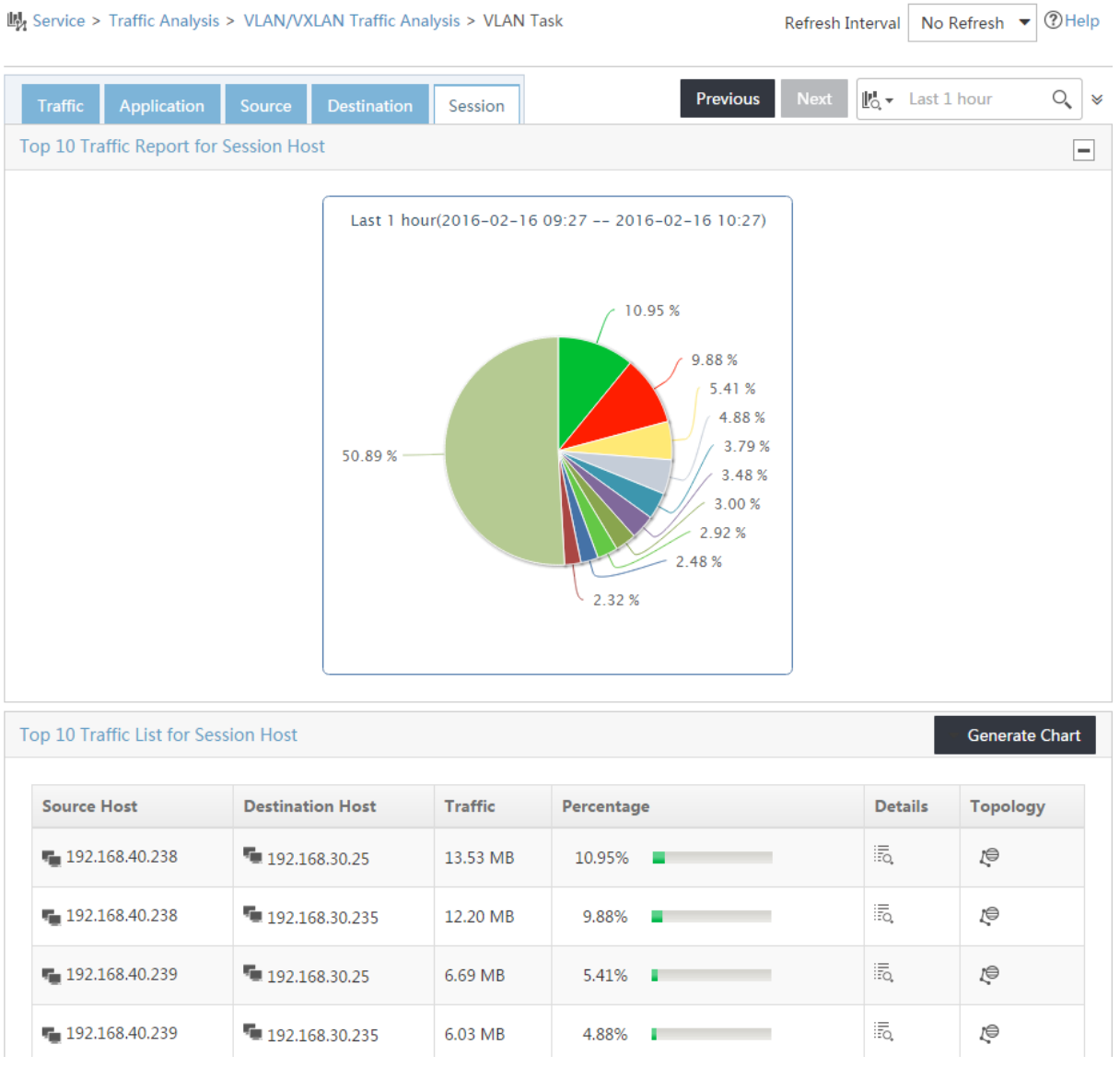


トラフィック分析タスクの情報表示



Sflow: VLANトラフィック分析タスクのアプリケーショントラフィック情報の表示
Service>Traffic Analysis>VLAN/VXLAN Traffice Analysis>VLAN Task

トラフィック分析タスクの情報表示



Sflow: VLANトラフィック分析タスクのセッショントラフィック情報の表示
Service>Traffic Analysis>VLAN/VXLAN Traffic Analysis>VLAN Task

トラフィック分析タスクの情報表示

NetStream: UBA監査結果のログ
Service>User Behavior Audit

Service > User Behavior Audit　　Help

Audit Condition (Note: If plenty of logs exist, it may take several minutes or longer time to query logs.)

Audit Result:2016-02-23 15:30:26-2016-02-23 15:42:50

Custom　Continue

Group　Not Group

Start Time	Source	Destination	Source Port	Destination Port	Protocol	Application	Packets Count	Flux	Device
2016-02-23 15:4...	192.168.40.118	192.168.1.135	443	51486	TCP	https	1	40.00 B	90.16.0.240
2016-02-23 15:4...	192.168.40.118	192.168.1.135	443	51486	TCP	https	1	40.00 B	90.16.0.240
2016-02-23 15:4...	192.168.40.118	192.168.1.135	443	51486	TCP	https	7	3.43 KB	90.16.0.240
2016-02-23 15:4...	192.168.40.118	192.168.1.135	443	51482	TCP	https	7	4.84 KB	90.16.0.240
2016-02-23 15:4...	192.168.40.118	192.168.1.135	443	51482	TCP	https	1	40.00 B	90.16.0.240
2016-02-23 15:4...	192.168.40.118	192.168.1.135	443	51482	TCP	https	1	40.00 B	90.16.0.240
2016-02-23 15:4...	192.168.40.118	192.168.1.135	443	51482	TCP	https	1	40.00 B	90.16.0.240
2016-02-23 15:4...	192.168.40.118	192.168.1.135	443	51483	TCP	https	7	2.29 KB	90.16.0.240

1-8 of 10000. Page 1 of 1250.　« ‹ 1 2 3 4 5 6 7 8 9 10 › »　8

Save

内容

- NTAの特徴
- NTAの設定
- トラブルシューティング

トラブルシューティング

▪トラフィックなしの場合、以下を確認する

✓ インテリジェント管理センター(iMC)とSQL Serverが正常に動作しているかどうか

✓ tbl_nets_yymmddhhにテーブルがある場合は、SQL Serverのunba_slaveデータベース このようなテーブルが存在しない場合、データは保存されていません。

✓ デバイスがログを送信するかどうか、および送信先がNTAスレーブサーバーかどうか

✓ プローブネットワークモードで、プローブがミラーログメッセージを受信するかどうか

✓ サービス構成内のFTPディレクトリが正しく構成されているかどうか、およびFTPサーバーが起動しているかどうか

✓ デバイスの時間帯設定に一貫性があるかどうか、デバイスのIPが正しく設定されているかどうか、およびインターフェイスインデックスに一貫性があるかどうか

✓ スレーブサーバーに複数のネットワークカードがある場合は、NTA内のスレーブサーバーのIPアドレスが、監視トラフィックが通過するIPアドレスであるかどうかを確認します。


ありがとう
www.h3c.com