



NAM の設定

ここでは、Catalyst 6500 シリーズ スイッチ、Catalyst 6000 シリーズ スイッチ、または Cisco 7600 シリーズ ルータ Network Analysis Module (NAM; ネットワーク解析モジュール) の設定方法を説明します。具体的な内容は次のとおりです。

- [NAM の設定 \(p.3-1\)](#)
- [NAM のトラフィックをキャプチャするトラフィック ソースの設定 \(p.3-2\)](#)
- [オペレーティング システムに依存しない設定 \(p.3-13\)](#)

NAM の設定

スイッチ上の NAM の設定手順は、Cisco IOS ソフトウェアと Catalyst オペレーティング システム ソフトウェアのいずれを使用しているかによって異なります。ただし、両方のスイッチ オペレーティング システムに共通する手順もいくつかあります。

NAM の初期設定については、『*Quick Start Guide for the Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module*』を参照してください。

NAM を初期設定すると、ネットワーク トラフィック モニタするように VLAN Access Control List (VACL; VLAN アクセス コントロール リスト)、ローカルまたはリモートの NetFlow Data Export (NDE; NetFlow データ エクスポート)、Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) を設定できます。詳細については、「[NAM のトラフィックをキャプチャするトラフィック ソースの設定](#)」(p.3-2) を参照してください。

ソフトウェア別の NAM 属性の設定が完了すると、両方のソフトウェアに共通した属性を設定できます。詳細については、「[オペレーティング システムに依存しない設定](#)」(p.3-13) を参照してください。

NAM のトラフィックをキャプチャするトラフィック ソースの設定

WS-SVC-NAM-1 プラットフォームには SPAN セッションの宛先ポートが 1 つあります。

WS-SVC-NAM-2 プラットフォームには VACL および SPAN セッションで使用可能な宛先ポートが 2 つあります。デフォルトでは、SPAN の GUI (グラフィカル ユーザ インターフェイス) で使用する宛先ポート名は data-port 1 および data-port 2 です。CLI (コマンドライン インターフェイス) SPAN ポート名は表 1-2 を参照してください。

VACL および SPAN を同じポートに同時に設定することはできません。表 3-1 に、NAM でサポートされる SPAN および VACL ポート設定を示します。

表 3-1 NAM SPAN および VACL ポートの設定

NAM-1	NAM-2
1 つの SPAN セッションのみ	2 つの SPAN セッション
1 つの VACL セッションのみ	1 つの SPAN セッションと 1 つの VACL セッション
	2 つの VACL セッション

SPAN の詳細については、次の URL を参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/span.htm>

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_2/config_gd/span.htm

VACL の詳細については、次の URL を参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/vacl.htm>

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_82/config_gd/acc_list.htm#1053650

NDE の詳細については、次の URL を参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/nde.htm#1035105>

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_2/config_gd/nde.htm

以下の各セクションでは、VACL、ローカルまたはリモート NDE、SPAN を設定して NAM でネットワークトラフィックを監視する方法について説明します。

- Cisco IOS ソフトウェア (p.3-2)
- Catalyst オペレーティングシステム ソフトウェア (p.3-9)

Cisco IOS ソフトウェア

1 つまたは複数の VLAN から、NAM を監視するトラフィックをキャプチャできます。特定の VLAN だけで監視するには、監視に使用しない VLAN をキャプチャ機能から外します。

トラフィック ソースとして SPAN を使用する場合

CLI でも NAM Traffic Analyzer アプリケーションでも、SPAN をトラフィック ソースとして設定できます。

NAM は、イーサネット、ファストイーサネット、ギガビットイーサネット、トランクポート、または Fast EtherChannel SPAN 送信元ポートからのイーサネットトラフィックを解析できます。また、イーサネット VLAN を SPAN 送信元に指定することもできます。

SPAN の詳細については、次の URL で『*Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*』を参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/index.htm>

NAM モジュール上のポートを SPAN 送信元ポートとして使用することはできません。

NAM 上で SPAN をイネーブルにするには、次のいずれかの作業を行います。

コマンド	目的
Router (config)# monitor session { <i>session_number</i> } { source { interface type slot/port } { vlan <i>vlan_ID</i> }} [, - rx tx both]	監視セッションの送信元インターフェイスおよび VLAN を設定します。
Router (config)# monitor session { <i>session_number</i> } { destination analysis module <i>NAM module number</i> data-port <i>port</i> }	NAM のポート 1 を SPAN 宛先ポートとしてイネーブルにします。
Router (config)# no monitor session <i>session_number</i>	監視セッションをディセーブルにします。
Router (config)# monitor session { <i>session_number</i> } { filter { <i>vlan_ID</i> } [, -]}	SPAN セッションをフィルタリングして、特定の VLAN だけがスイッチ ポート トランクから見えるようにします。
Router # show monitor session { <i>session_number</i> }	現在の監視セッションを表示します。

NAM 上で SPAN をイネーブルにする例を示します。

```
Router# show monitor
Session 1
-----
Source Ports:
  RX Only:      None
  TX Only:      None
  Both:         None
Source VLANs:
  RX Only:      None
  TX Only:      None
  Both:         None
Destination Ports:None
Filter VLANs:   None

Session 2
-----
Source Ports:
  RX Only:      None
  TX Only:      None
  Both:         None
Source VLANs:
  RX Only:      None
  TX Only:      None
  Both:         None
Destination Ports:None
Filter VLANs:   None

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# monitor session 1 source vlan 1 both
```



(注) スイッチの CLI を使用し、NAM-1 のトラフィック送信元として SPAN を設定する場合、NAM-1 の SPAN 宛先ポートは data-port 1 です。NAM-2 の SPAN 宛先ポートは data-port 1 および data-port 2 です。

```
Router#
00:21:10:%SYS-5-CONFIG_I:Configured from console by console
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# monitor session 1 destination analysis-module 8 data-port 1
Router# show monitor
Session 1
-----
Type           :Local Session
Source Ports:
  RX Only:      None
  TX Only:      None
  Both:         None
Source VLANs:
  RX Only:      None
  TX Only:      None
  Both:         1
Source RSPAN VLAN:None
Destination Ports:analysis-module 8 data-port 1

Filter VLANs:   None
Dest RSPAN VLAN: None
Session 2
-----
Type           :Local Session
Source Ports:
  RX Only:      None
  TX Only:      None
  Both:         None
Source VLANs:
  RX Only:      None
  TX Only:      None
  Both:         None
Source RSPAN VLAN:None
Destination Ports:None
Filter VLANs:   None
Dest RSPAN VLAN: None
```

トラフィック ソースとして VACL を使用する場合

ここでは、Cisco IOS Release 12.1(13)E1 以降を実行するスイッチに VACL を設定する方法について説明します。Catalyst オペレーティング システム上で LAN VACL を設定する場合、セキュリティ ACL 機能を使用すると同じように設定できます。詳細については、「[オペレーティング システムに依存しない設定](#)」(p.3-13) を参照してください。

WAN インターフェイス上での VACL の設定

WAN インターフェイスは SPAN をサポートしません。NAM を使用して WAN インターフェイス上でトラフィックを監視する場合は、スイッチの CLI を使用してスイッチ上に VACL を手動で設定する必要があります。この機能は、WAN インターフェイスの IP トラフィックでのみ有効です。フィルタリング規則を追加して、特定のデータ フローを監視することもできます。

トラフィックを NAM に送信する SPAN セッションがない場合にも VACL が使用できます。この場合は、SPAN の代わりに VACL を設定して VLAN トラフィックを監視します。

次の例では、Cisco IOS Release 12.1(13)E1 以降を実行するスイッチの VACL 設定に必要な手順を示します。Catalyst オペレーティング システムを実行するスイッチに LAN VACL を設定する場合、同じ設定になるように ACL 機能を使用します。

この例では、Asynchronous Transfer Mode (ATM; 非同期転送モード) の WAN インターフェイス上で VACL を設定して NAM に入出トラフィックをどちらも転送する手順を示します。

```
Cat6500# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cat6509(config)# access-list 100 permit ip any any
Cat6509(config)# vlan access-map wan 100
Cat6509(config-access-map)# match ip address 100
Cat6509(config-access-map)# action forward capture
Cat6509(config-access-map)# exit
Cat6509(config)# vlan filter wan interface ATM6/0/0.1
Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1-4094
Cat6509(config)# analysis module 3 data-port 1 capture
Cat6509(config)# exit
```

出トラフィックのみを監視する場合は、WAN インターフェイス コマンドに関連付けられる VLAN ID が取得できます。次に例を示します。

```
Cat6509# show cwan vlan
Hidden VLAN  swidb->if_number  Interface
-----
1017          94                ATM6/0/0.1
```

VLAN ID を取得したら、次のように NAM データ ポート キャプチャを設定します。

```
Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1017
```

入トラフィックを監視するには、前回キャプチャ設定した VLAN 1017 を入トラフィックを送信する VLAN ID に置き換えます。たとえば、NAM に次のような設定をすると WAN インターフェイス上の入トラフィックだけが監視できます。

```
Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1
```

LAN VLAN インターフェイス上での VACL 設定

LAN 上で VLAN トラフィックを監視するには、SPAN を使って NAM にトラフィックを転送します。ただし、状況によっては転送されたトラフィックが NAM のモニタリング能力を超えることもあります。このため、あらかじめ LAN トラフィックにフィルタを設定してから NAM に転送することもできます。

■ NAM のトラフィックをキャプチャするトラフィック ソースの設定

次に、LAN VLAN インターフェイスに VACL を設定する例を示します。この例では、VLAN 1 上のサーバ 172.20.122.226 に送信するトラフィックをすべてキャプチャし、スロット 3 に搭載された NAM に転送しています。

```
Cat6500# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cat6500(config)# access-list 100 permit ip any any
Cat6500(config)# access-list 110 permit ip any host 172.20.122.226
Cat6500(config)# vlan access-map lan 100
Cat6500(config-access-map)# match ip address 110
Cat6500(config-access-map)# action forward capture
Cat6500(config-access-map)# exit
Cat6500(config)# vlan access-map lan 200
Cat6500(config-access-map)# match ip address 100
Cat6500(config-access-map)# action forward
Cat6500(config-access-map)# exit
Cat6500(config)# vlan filter lan vlan-list 1
Cat6500(config)# analysis module 3 data-port 1 capture allowed-vlan 1
Cat6500(config)# analysis module 3 data-port 1 capture
Cat6500(config)# exit
```

トラフィック ソースとして NDE を使用する場合

NDE は、外部データ コレクタが収集したトラフィック統計情報を解析に使用できるようにします。NDE を使用すると、レイヤ 3 スイッチングおよびルーティングが行われたすべての IP ユニキャストトラフィックを監視できます。NAM のトラフィック ソースとして NDE を使用する場合は、NetFlow モニタ オプションをイネーブルにして、NAM が NDE ストリームを受信できるようにします。統計情報は、予約された ifIndex.3000 で提供されます。

NetFlow デバイスに NDE を設定して NDE パケットを NAM にエクスポートする手順は、送信デバイスのプラットフォームやバージョンによって異なります。詳細については、デバイスの NDE 設定ガイドラインを参照してください。

NDE の設定

ローカルおよびリモートの NDE デバイスに Cisco IOS ソフトウェアの NDE を設定する手順は次のとおりです。

ステップ 1 次の手順で、NDE を設定します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface type slot/port
```

ステップ 2 インターフェイスの NetFlow をイネーブルにします。

```
Router(config)# ip route-cache flow
```

ステップ 3 ルーティングされたフロー キャッシュのエントリを NAM UDP ポート 3000 にエクスポートします。

```
Router(config)# ip flow-export destination NAM-address 3000
```



(注) UDP ポート番号は、3000 に設定する必要があります。

NAM モジュールを NDE コレクタとして設定する場合、(NAM モジュールとのセッションによって設定した) NAM の IP アドレスを使用する必要があります。

次に、基本的な NDE を設定する手順を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface vlan 2
Router(config)# ip route-cache flow
Router(config)# ip flow-export destination 172.20.104.74 3000
Router(config)# exit
```

MLS キャッシュからの NDE の設定

Policy Feature Card (PFC; ポリシー フィーチャ カード) (Multilayer Switching [MLS; マルチレイヤ スイッチング] キャッシュ) から NDE を設定する手順は、次のとおりです。

ステップ 1 設定モードを入力します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

ステップ 2 NDE のバージョンを選択します。

```
Router(config)# mls nde sender version version-number
```



(注) NAM は NDE バージョン 1、5、6、7、8 およびバージョン 8 の集計キャッシュをサポートします。NAM で使用できる NDE バージョンについては、スイッチ ソフトウェアがサポートする NDE のバージョンを Cisco IOS のマニュアルで参照してください。

ステップ 3 NDE フロー マスクを選択します。

```
Router(config)# mls flow ip [interface-full | full]
```



(注) full キーワードを使用して、フロー マスクに収集データの詳細が含まれるようにします。

ステップ 4 NetFlow のエクスポートをイネーブルにします。

```
Router(config)# mls nde sender
```

ステップ 5 NetFlow パケットを NAM UDP ポート 3000 にエクスポートします。

```
Router(config)# ip flow-export destination NAM-Address 3000
```

次に、Multilayer Switch Feature Card (MSFC; マルチレイヤ スイッチ フィーチャ カード) から NDE を設定する方法を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# mls nde sender version 5
Router(config)# mls flow ip full
Router(config)# mls nde sender
Router(config)# ip route-cache flow
Router(config)# ip flow-export destination 172.20.104.74 3000
Router# show ip cache flow
Router# show ip flow export
```



(注)

PFC に NDE を設定する方法の詳細については、次の URL を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/nde.htm - xtocid14

バージョン 8 集計の NDE の設定



(注)

NAM は NDE 集計をサポートしますが、指定した集計タイプについて受信する内容は集計に限られます。他の内容については受信できません。NDE 設定についての詳細を受け取るには、フルフローモードを指定します。

NetFlow デバイスが NDE バージョン 8 集計をサポートしている場合、1 つまたは複数のバージョン 8 集計キャッシュからのフローを NAM にエクスポートできます。具体的な手順は次のとおりです。

ステップ 1 NDE バージョン 8 集計を選択します。

```
Router(config)# ip flow-aggregation cache aggregation-type
```

サポートされている集計タイプは次のとおりです。

- 宛先プレフィクス
- 送信元プレフィクス
- プロトコルポート
- プレフィクス

ステップ 2 集計キャッシュをイネーブルにします。

```
Router(config-flow-cache)# enable
```


ステップ 3 集計キャッシュのフロー エントリを NAM UDP ポート 3000 にエクスポートします。

```
Router(config-flow-cache)# export destination NAM-Address 3000
```

ステップ 4 NDE を検証します。

```
Router# show ip cache flow-aggregation aggregation-type
```

次に、NDE バージョン 8 集計の設定方法を示します。

```
Router(config)# ip flow-aggregation cache prefix
Router(config-flow-cache)# enable
Router(config-flow-cache)# export destination 172.20.104.74 3000
Router(config-flow-cache)# exit
Router(config)# show ip cache flow-aggregation prefix
```

Catalyst オペレーティング システム ソフトウェア

1 つまたは複数の VLAN から、NAM を監視するトラフィックをキャプチャできます。特定の VLAN だけで監視するには、監視に使用しない VLAN をキャプチャ機能から外します。

トラフィック ソースとして SPAN を使用する場合

Remote SPAN (RSPAN) をトラフィック ソースとして設定する場合、スイッチの CLI と NAM Traffic Analyzer アプリケーションのどちらでも使用できますが、NAM Traffic Analyzer の使用を推奨します。

SPAN および RSPAN の詳細については、『*Catalyst 6500 Series Switch Software Configuration Guide*』の「Configuring SPAN and RSPAN」を参照してください。

RSPAN トラフィックは、NAM の SPAN 送信元として使用できます。SPAN 送信元が RSPAN に使用されているのと同じ VLAN ID に設定されていることを確認してください。SPAN 宛先は、`nam_module/port` に設定する必要があります。



(注)

スイッチの CLI を使用し、NAM-1 へのトラフィック送信元として SPAN を設定する場合、宛先ポートは 3 に設定してください。NAM-2 へのトラフィック送信元として SPAN を設定する場合は、SPAN ポートを宛先ポート 7 に設定してください。宛先ポート 8 はこのリリースの NAM では使用できません (スイッチおよびハードウェア サポートは利用可能です)。



(注)

NAM ポートを SPAN 送信元ポートとして使用することはできません。

NAM は、イーサネット、ファストイーサネット、ギガビットイーサネット、トランク ポート、または Fast EtherChannel SPAN 送信元ポートからのイーサネットトラフィックを解析できます。また、イーサネット VLAN を SPAN 送信元に指定することもできます。

SPAN および RSPAN の詳しい設定手順については、スイッチ ソフトウェア コンフィギュレーションガイドを参照してください。

NAMをSPAN宛先ポートとして設定するには、イネーブルモードで次の作業を行います。

作業	コマンド
NAMをSPAN宛先ポートとして設定します。	<code>set span {src_mod/src_ports src_vlans sc0} {dest_mod dest_port} [rx tx both] [inpkts {enable disable}] [learning {enable disable}] [multicast {enable disable}] [filter vlans...][create]</code>

スロット5に搭載されているNAM-2にSPAN VLAN 1を設定する場合は、次のように入力します。

```
Console> (enable) set span 1 5/7
```

トラフィックソースとしてLAN VACLを使用する場合

WAN VACLを使用するとインバウンドまたはアウトバウンドVLANパケットをキャプチャしますが、CatalystオペレーティングシステムVACLはVLANパケットが最初にスイッチのVLANにルーティングされたときまたはブリッジされたときにVLANパケットをキャプチャする場合にだけ使用します。

次に、VACLを作成してスイッチのVLAN 1からNAM-1データポート6/3にブリッジまたはルーティングされるすべてのIPパケットをキャプチャする方法を示します。

```
Console> (enable) set security acl ip LANCAPTURE permit ip any any capture
Console> (enable) commit
Console> (enable) set security acl map LANCAPTURE 1
Console> (enable) set security acl capture 6/3
```

次に、VACLを作成して特定のVLAN 1カンパセーションをキャプチャする方法を示します。

```
Console> (enable) set sec acl ip LANCAPTURE permit ip host 172.20.122.70 host
172.20.122.226 capture
Console> (enable) set security acl ip LANCAPTURE permit ip any any
Console> (enable) commit
Console> (enable) set security acl map LANCAPTURE 1
Console> (enable) set security acl capture 6/3
```

トラフィックソースとしてNDEを使用する場合

NAMのトラフィックソースとしてNDEを使用する場合は、NetFlow モニタ オプションをイネーブルにして、NAMがNDEストリームを受信できるようにする必要があります。ローカルスイッチの統計情報は、NAMの前のリリースと同様、予約されたifIndex.3000で提供されます。リモートスイッチはifIndex.50000以上を使用します。






(注) NetFlowを使用するには、MSFCの設定が必要です。詳細については、『Catalyst 6500 Series Switch Software Configuration Guide』を参照してください。



(注) NetFlowのカスタムデータソースを作成するCLIコマンドはありません。NetFlowのカスタムデータソースを作成する場合は、NAM Traffic AnalyzerのGUIを使用します。

NDE の設定

次の手順で、Catalyst オペレーティング システムの NetFlow モニタをイネーブルにします。

	作業	コマンド
ステップ 1	NDE のバージョンを選択します。  (注) NAM は NDE バージョン 1、5、6、7、8 およびバージョン 8 の集計キャッシュをサポートします。NAM で使用できる NDE バージョンについては、スイッチ ソフトウェアがサポートする NDE のバージョンを Cisco IOS のマニュアルで参照してください。	<code>set mls nde version nde-version-number</code>
ステップ 2	NDE フロー マスクを full に指定します。  (注) NAM は NDE 集計をサポートしますが、指定した集計タイプについて受信する情報はそのときの集計に限られ、他の内容については受信できません。NDE 設定についての詳細を受け取るには、フルフロー モードを指定します。	<code>set mls flow full</code>
ステップ 3	NAM に NDE パケットを送信します。	<code>set snmp extendedrmon netflow [enable disable] mod</code> <code>set mls nde NAM-address 3000</code>
ステップ 4	NDE エクスポートをイネーブルにします。	<code>set mls nde enable</code>
ステップ 5	(任意) デバイスが if-index をエクスポートすることを確認します。  (注) インターフェイス別の NetFlow データおよび NAM の指示を中止したい場合はこの手順を実行します。	<code>set mls nde destination-ifindex enable</code> <code>set mls nde source-ifindex enable</code>
ステップ 6	NDE エクスポートを検証します。 ローカル デバイス : リモート デバイス :	<code>show snmp and show mls nde</code> <code>show mls nde</code>

■ NAM のトラフィックをキャプチャするトラフィック ソースの設定

NetFlow モニタ オプションをイネーブルにし、イネーブルに設定されたことを確認する例を示します。

```

Console> (enable) set snmp extendedrmon netflow enable 2
Snmp extended RMON netflow enabled
Console> (enable) show snmp
RMON: Enabled
Extended RMON NetFlow Enabled : Module 2
Traps Enabled:
None
Port Traps Enabled: None

Community-Access      Community-String
-----
read-only              public
read-write             private
read-write-all        secret

Trap-Rec-Address      Trap-Rec-Community
-----
(テキスト出力は省略)

```



(注) NAM が搭載されている場合、『*Catalyst 6500 Series Software Configuration Guide*』で説明されているように、`set mls nde collector_ip [udp_port_number]` コマンドで外部データ コレクタを指定する必要はありません。ホストおよびポートが設定されていないというメッセージは無視してください。

ブリッジされたフロー統計情報から NDE をエクスポートする

スイッチがブリッジされたフロー統計情報からの NDE のエクスポートをサポートする場合、ブリッジされたフロー統計情報を使って NDE を NAM にエクスポートできます。

次の手順で、ブリッジされたフロー統計情報を NDE にエクスポートします。

	作業	コマンド
ステップ 1	ブリッジされた VLAN 上のフロー統計情報をイネーブルにします。	<code>set mls bridged-flow-statistics enable <i>vlan-list</i></code>
ステップ 2	NDE パケットを NAM の UDP ポート 3000 にエクスポートします。	<code>set mls nde <i>NAM-address</i> 3000</code>

オペレーティング システムに依存しない設定

ここでは、スイッチのオペレーティング システムに依存しない NAM の設定について説明します。

- HTTP サーバまたは HTTP セキュア サーバの設定 (p.3-13)
- HTTP サーバの設定 (p.3-13)
- HTTP セキュア サーバの設定 (p.3-14)
- 証明書の生成 (p.3-16)
- 証明書のインストール (p.3-17)
- TACACS+ サーバの使用 (p.3-18)

HTTP サーバまたは HTTP セキュア サーバの設定

Web ブラウザ (HTTP または HTTPS) を使用して NAM にアクセスするには、事前に NAM CLI から NAM Traffic Analyzer アプリケーションをイネーブルにする必要があります。HTTP の場合、**ip http server enable** コマンドを使用します。HTTPS の場合、**ip http secure server enable** コマンドを使用します。任意で、HTTP (または HTTPS) サーバがデフォルトとは異なる TCP ポート上で稼働するように設定することもできます。



(注) HTTP サーバまたは HTTP セキュア サーバのどちらでも使用できますが、両方を使用することはできません。



(注) デフォルトでは、**ip http secure** コマンドはすべてディセーブルに設定されています。これらのコマンドをイネーブルにするには、<http://www.cisco.com> から NAM strong crypto パッチをダウンロードしてインストールする必要があります。

HTTP サーバの設定

NAM に HTTP サーバのパラメータを設定する手順は、次のとおりです。

ステップ 1 (任意) 次のコマンドを入力して、HTTP ポートを設定します。

```
root@localhost# ip http port 8080
The HTTP server is enabled now. You must restart the
server to change HTTP port. Continue [y/n]? y
```

ポート番号は、1 ~ 65535 の範囲です。



(注) Web ユーザは CLI ユーザとは異なります。ユーザ名とパスワードは、Web ユーザと CLI ユーザでは区別して管理されています。NAM CLI のユーザ名とパスワードを変更する場合は、「Cisco IOS ソフトウェア」(p.4-1) および「Catalyst オペレーティング システム ソフトウェア」(p.4-13) を参照してください。Web インターフェイスでユーザ名とパスワードを変更する場合は、NAM Traffic Analyzer アプリケーションのオンライン ヘルプと『*User Guide for the Network Analysis Module Traffic Analyzer*』 Release 3.3 を参照してください。

ステップ2 次のコマンドを入力して、HTTP サーバをイネーブルにします。

```
root@localhost# ip http server enable
Enabling HTTP server...
No web users configured!
Please enter a web administrator username [admin]:admin
New password:
Confirm password
User admin added.
Successfully enabled HTTP server.
```

HTTP セキュア サーバの設定

デフォルトでは、**ip http secure** コマンドはすべてディセーブルに設定されています。strong crypto パッチをインストールして、HTTP セキュア サーバをイネーブルにする必要があります。Telnet の代わりに SSH を使用する場合は、strong crypto パッチもインストールする必要があります。

strong crypto パッチをインストールする手順は、次のとおりです。

ステップ1 <http://www.cisco.com> からパッチをダウンロードして、FTP サーバに送信します。

ステップ2 次のコマンドを入力して、パッチをインストールします。

```
root@localhost# patch ftp-url
```

ftp-url は、strong crypto パッチの FTP ロケーションおよび名前です。

パッチをインストールする例を示します。

```
root@localhost# patch ftp://host/path/c6nam- 3.3-strong-cryptoK9-patch-1-0.bin

Proceeding with installation. Please do not interrupt.
If installation is interrupted, please try again.

Downloading c6nam- 3.3-strong-cryptoK9-patch-1-0.bin. Please wait...
ftp://host/path/c6nam- 3.3-strong-cryptoK9-patch-1-0.bin (1K)
- [#####] 1K | 228.92K/s
1891 bytes transferred in 0.01 sec (225.40k/sec)

Verifying c6nam- 3.3-strong-cryptoK9-patch-1-0.bin. Please wait...
Patch c6nam- 3.3-strong-cryptoK9-patch-1-0.bin verified.

Applying /usr/local/nam/patch/workdir/c6nam- 3.3-strong-cryptoK9-patch-1-0.bin.
Please wait...
##### [100%]
##### [100%]

Patch applied successfully.
```

ステップ 3 (任意) 次のコマンドを入力して、HTTPS サーバを設定します。



(注) デフォルト (443) 以外のポートを指定する場合は、*port_number* を追加します。

```
root@localhost# ip http secure port 8080
The HTTP server is enabled now. You must restart the
server to change HTTP port. Continue [y/n]? y
```

ポート番号は、1 ~ 65535 の範囲です。



(注) Web ユーザは CLI ユーザとは異なります。

ステップ 4 次のコマンドを入力して、HTTPS サーバをイネーブルにします。

```
root@localhost# ip http secure server enable
Enabling HTTP server...
No web users configured!
Please enter a web administrator username [admin]: admin
New password:
Confirm password
User admin added.
Successfully enabled HTTP server.
```

証明書生成

証明書は、セキュアサーバ接続の正当性を確認する目的で使用します。自己署名の証明書を生成することや認証局から証明書を取得してインストールすることができます。

次に、自己署名証明書を生成する方法を示します。

```
root@localhost# ip http secure generate self-signed-certificate

The HTTP secure server is enabled now. You must restart
to generate the certificate. Continue [y/n]? y
5243 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
Using configuration from /usr/local/nam/defaults/openssl.cnf
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco Systems, Inc.
Organizational Unit Name (eg, section) []:NAM
Common Name (eg, your name or your server's hostname) [r2d2-186.cisco.com]:
Email Address []:kjchen@cisco.com
Using configuration from /usr/local/nam/defaults/openssl.cnf
-----BEGIN CERTIFICATE-----
MIIDlTCCAV6gAwIBAgIBADANBgkqhkiG9w0BAQQFADCB1DELMAkGA1UEBhMCVVMx
CzAJBgNVBAGTAkNBMREwDwYDVQQHEWhTYW4gSm9zZTEcMBoGA1UEChMTQ2l2Y28g
U3lzdGVtcywgSW5jLjEMMAoGA1UECXMdTkFNMRswGQYDVQQDExJyMmQyLTE4Ni5j
aXNjby5jb20xHDAaBgkqhkiG9w0BCQEWDW5hbUBjaXNjby5jb20wHhcNMDQwMjI0
MDAwNDAxWhcNMDUwMjIzMDAwNDAxWjCB1DELMAkGA1UEBhMCVVMxGzAJBgNVBAGT
AkNBMREwDwYDVQQHEWhTYW4gSm9zZTEcMBoGA1UEChMTQ2l2Y28gU3lzdGVtcywg
SW5jLjEMMAoGA1UECXMdTkFNMRswGQYDVQQDExJyMmQyLTE4Ni5jaXNjby5jb20x
HDAaBgkqhkiG9w0BCQEWDW5hbUBjaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAMDrGqhw2Kt8fimI+b1l6k6+z9nTEQagolQfo08DehBLZl0eoJ/0
YAWlCqx3fnW3csSmGiHj6aEjJhm0W05GvJRbzxbxeSPadDv7IdbIhXTLtPk1W11g
byhUzvi5R8UFGSmerbbnc7qkTDXQdrQ2vETAfxK4oysq+HF55qVjY2KpAgMBAAGj
gfQwgfEWHQYDVR00BYYEFjczj4+vFJmLAo1Njn09MYE/Hn9eoYGapIGXMIGUMQsw
CQYDVQQGEwJVUzEL
MAkGA1UEBMCQ0ExETAkNBMREwDwYDVQQLEwNOQU0xGzAZBgNVBAMTEhIyZDI0MTg2
LmNp
c2NvLmNvbVtEcMBoGCSqGSIb3DQEJARYNbmFtZG9uLnVlbnVlYlBhZAMBgNVHRME
BTADAQH/MA0GCSqGSIb3DQEBAUAA4GBAHwBnz9OALHWkyK4qYTTbBno2MFbmI49
gU4IIPfSgWjyqdiXXGJs7c1q0dMPzdmDIG1TjmkLx2HCl+dVuq/2X4RrOFaoog/s
K9GmULi80tgrkDhXJHT/gDfv+L7gPQCcpq1TUFMVlzxzAHSsBGNlQ8oTysXScEJ
nSr0tR/OKB0t
-----END CERTIFICATE-----
Disabling HTTP secure server...
Successfully disabled HTTP secure server.
Enabling HTTP secure server...
Successfully enabled HTTP secure server.
root@localhost#
```

認証局から証明書を取得するには、まず証明書署名要求を生成し、その要求を認証局に手動で提出する必要があります。認証局から証明書を取得してから、その証明書をインストールします。

証明書のインストール

認証局から取得した証明書をインストールする手順は、次のとおりです。

ステップ1 次のコマンドを入力して、証明書署名要求を生成します。

```

root@localhost# ip http secure generate certificate-request
A certificate-signing request already exists. Generating a
new one will invalidate the existing one and any certificates
already generated from the existing request. Do you still
want to generate a new one? [y/n] y
5244 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
.....+++++
.+++++
e is 65537 (0x10001)
Using configuration from /usr/local/nam/defaults/openssl.cnf
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:Tamil Nadu
Locality Name (eg, city) []:Chennai
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco Systems
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [hostname.Cisco.com]:
Email Address []:xxx@Cisco.com
-----BEGIN CERTIFICATE REQUEST-----
MIIBzzCCATgCAQAwY4xCzAJBgNVBAYTAklOMRMwEQYDVOQIEwpUYW1pbCBOYW11
MRAwDgYDVOQHEwdDaGVubmFpMRyYwFAYDVOQKEw1DaXNjbyBTeXN0ZW1zMRA4wHAYD
VQQDExVuYw1sYWItcGlrMy5jaXNjby5jb20xIDAeBgkqhkiG9w0BCQEWEXNla2Fy
YmNAY2l2Y28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8+SR503gS
ygkf6pnHuh0Le1Nf6LqJjzwFfjqjS8vpkFq/QVbwqTNDIggUfbvRAIRWEKVWhpRf
rr+II2o/Xzb0RLpV2J2p3HGgoRrKC3nArIFFiSqXniEU+g2mPqsFncOyxHNXIxEj
iBQf80DxbmvWFOpunmOQ/pGuEysNfU/46wIDAQABoAAwDQYJKoZIhvcNAQEBBQAD
gYEAVAX89pCAcRDOqPgABEMQCmWD+wqZPnALovr7C81OLBYTgLLqdwPqoSjSYosE
w/pFnIxWN1sJ7MC8+hjnJLJjoCwbyrEyvoiAvzpsGsnAZgWUVaUpR7j1Nbf8x2A1
hAOH9KchS0TpSNy13OyhuAkV0pUcM2AJqB/93u4YvuHfNOA=
-----END CERTIFICATE REQUEST-----

```

ステップ 2 次のコマンドを入力して、認証局から取得した証明書をインストールします。

```
root@localhost# ip http secure install certificate
The HTTP server is enabled now. You must restart the
server to install certificate. Continue [y/n]? y

Cut and paste the certificate you received from
Certificate Authority. Enter a period (.), then
press enter to indicate the end of the certificate.
-----BEGIN CERTIFICATE-----
MIIDAzCCAmygAwIBAgIBADANBgkqhkiG9w0BAQQFADBlMQswCQYDVQQGEwJBVTET
MBEGA1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50ZXJ1ZXQgV2lkZ210cyBQ
dHkgTHRkMR4wHAYDVQQDExVuYW1sYWItcGlrMy5jaXNjby5jb20wHhcNMDEwMDMw
MTAxMDI4WHcnMDIxMDMwMTAxMDI4WjBlMQswCQYDVQQGEwJBVTETMBEGA1UECBMK
U29tZS1TdGF0ZTEhMB8GA1UEChMYSW50ZXJ1ZXQgV2lkZ210cyBQdHkgTHRkMR4w
HAYDVQQDExVuYW1sYWItcGlrMy5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBANs01T5ayA6pvkJad413V+N/ibvND0XRyXfFycTQRzeA8F4A+etV
s0Iq0muFfiL9mDr/es9TkyfIM+T2F6+NE13DxJ53ZBbh7ndb6W0nzeHLKh9EDfSI
cy2s7751CPCjfLcMsWQLWSU7XUbi/ExDpb9e2wQQgi6QBED/YRkr73KNAgMBAAGj
gcIwgb8wHQYDVR0OBBYEFIHsyecd8AW4cvt7voCFeZMarXIqMIGPBgNVHSMegYcw
gYSAFIHsyecd8AW4cvt7voCFeZMarXIqoWmkZzBlMQswCQYDVQQGEwJBVTETMBEG
A1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50ZXJ1ZXQgV2lkZ210cyBQdHkg
THRkMR4wHAYDVQQDExVuYW1sYWItcGlrMy5jaXNjby5jb22CAQAwDAYDVR0TBAUw
AwEB/zANBgkqhkiG9w0BAQQFAAOBgQACDyWhULAUeSIXyt9tuUrdPff97hrpFkKy
njlyEU4piuc9qQtXG9yCGsofAm+CiGFg6P4qJZtBF47mq81qF+48JTYwi68CGCye
suZgw0iCPQVv4KDirHBKFc0Vr/2SMrXcJImczoV2WGcxWxsVaXwpkBF8pcMFFYd
iOULMcvFxf==
-----END CERTIFICATE-----
.
Disabling HTTP server...
Successfully disabled HTTP server.
Enabling HTTP server...
Successfully enabled HTTP server.
```

TACACS+ サーバの使用

TACACS+ は、リモート アクセス認証および関連サービスを提供するシスコシステムズの認証プロトコルです。TACACS+ を使用する場合、ユーザ パスワードは個々のルータではなくセントラルデータベースで管理されます。

ユーザが NAM Traffic Analyzer にログインすると、TACACS+ はそのユーザの名前とパスワードが有効かどうかを確認し、ユーザに割り当てられたアクセス権限を判別します。

NAM で TACACS+ を使用するには、事前に NAM と TACACS+ サーバの両方を設定する必要があります。

NAM に TACACS+ を設定する手順は、次のとおりです。

-
- ステップ 1** NAM Traffic Analyzer アプリケーションを起動します。
 - ステップ 2** **Admin** タブをクリックします。
 - ステップ 3** **Users** を選択します。
 - ステップ 4** **TACACS+** を選択します。
 - ステップ 5** **Enable TACACS+ Administration and Authentication** ボックスをクリックします。

ステップ 6 オンライン ヘルプの説明に従ってください。

■ オペレーティング システムに依存しない設定