



クイック スタート ガイド



Cisco ASA の APIC との統合

改訂日: 2015 年 10 月 9 日

バージョン 1.2

- 1 [ASA の APIC との統合について](#)
- 2 [ASA の展開](#)
- 3 [ASA への管理アクセスの設定](#)
- 4 [ジャンボ フレーム サポートの設定](#)
- 5 [マルチ コンテキスト モードの設定](#)
- 6 [ASA クラスタの設定](#)
- 7 [ASA デバイス パッケージのインストール](#)
- 8 [APIC 内での ASA の設定](#)

1 ASA の APIC との統合について

Cisco Application Policy Infrastructure Controller (APIC) は、エンドポイントグループ (EPG) と呼ばれるアプリケーション間のノースバウンド サービス (ASA ファイアウォールなど) の挿入を自動化します。APIC は、ネットワークとサービスを設定するためにノースバウンド API を使用します。管理対象オブジェクトを使用して設定を作成、削除、変更するのに、これらの API を使用します。



注 現在の ASA バージョンでサポートされない設定を作成しようとすると、次のようなエラーが APIC で表示されることがあります。

```
" *Major script error: Configuration error: ... ERROR: % Invalid input detected at
'^' marker. "
```

サポートされる機能については、ASA バージョンのマニュアルを参照してください。

サービス機能の挿入

サービス機能がアプリケーション間のサービス グラフに挿入されると、これらのアプリケーションからのトラフィックは APIC で分類され、オーバーレイ ネットワークのタグを使用して識別されます。サービス機能はタグを使用して、トラフィックにポリシーを適用します。APIC との ASA 統合の場合、サービス機能はルーテッドまたはトランスペアレント ファイアウォール動作を使用してトラフィックを転送します。

APIC については、『*ACI Fundamentals*』ガイドの「Cisco Application Centric Infrastructure」の章を参照してください。

サービス グラフについては、『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*』の「*Configuring a Service Graph*」の章を参照してください。

レイヤ 4 からレイヤ 7 サービスの挿入については、『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*』の「*Overview*」の章を参照してください。

サポートされる ASA モデルと機能

次の表に、サポートされる ASA モデルを示します。

ASA モデル	ソフトウェアバージョン
ASA 5500-X(5512 から 5555)	ASA ソフトウェア バージョン 8.4.x 以降
ASA 5585-X(SSP 10 から SSP 60)	
ASA v	

次の表に、ASA v および ASA 5585-X でサポートされる機能を示します。BGP と OSPF をサポートするリリースについては、『Release Notes for the Cisco ASA Device Package Software, Version 1.2(1) for ACI』を参照してください。

機能	ASA v サポート (Yes/No)	ASA 5500-X/5585-X サポート(Yes/No)
アクセス制御ポリシー	Yes	Yes
アクセス リストおよびグループ	Yes	Yes
アプリケーション インспекション	Yes	Yes
BGP	Yes	Yes
クラスタ	No	Yes
接続制限	Yes	Yes
DNS クライアント	Yes	Yes
イーサ チャンネル	No	Yes
ハイ アベイラビリティ(アクティブ/アクティブ、 アクティブ/スタンバイ)	アクティブ/スタン バイのみ	Yes
インターフェイス コンフィギュレーション	Yes	Yes
IP 監査	Yes	Yes
IPv6	Yes	Yes
ロギング	Yes	Yes
マルチ コンテキスト	No	Yes
NAT/ Twice NAT	Yes	Yes
Netflow	Yes	Yes

機能	ASAv サポート (Yes/No)	ASA 5500-X/5585-X サポート (Yes/No)
ネットワーク、サービス オブジェクト、グループ	Yes	Yes
NTP	Yes	Yes
OSPF	Yes	Yes
プロトコルのタイムアウト	Yes	Yes
AnyConnect Premium (共有) ライセンス	No	Yes
Smart Call Home の有効化	Yes	Yes
スタティック ルーティング	Yes	Yes
TCP インターセプト (初期接続制限)	Yes	Yes
脅威の検出	Yes	Yes

2 ASA の展開

- ASAv: インストール手順については、次の URL の『*Cisco Adaptive Security Virtual Appliance (ASAv) Quick Start Guide*』を参照してください。

<http://www.cisco.com/c/en/us/support/security/virtual-adaptive-security-appliance-firewall/products-installation-guides-list.html>



注

ASAv の展開時に、管理インターフェイスの `nameif` プロパティの値を `management` として定義する必要があります。インターフェイス名を `management` 以外の値に定義した場合、デバイス クラスタは `AuditRequested/AuditPending` 状態で停止し、読み取り操作がタイムアウトしたことを示すエラーが表示されます。管理インターフェイスとデフォルトゲートウェイの設定は ASAv から削除され、インターフェイスはシャットダウンされます。

- ASA 5585-X: インストール手順については、次の URL の『*Cisco ASA 5585-X Quick Start Guide*』を参照してください。

<http://www.cisco.com/go/asa5585x-quick>

3 ASA への管理アクセスの設定

APIC が ASA を管理できるように ASA への管理アクセスを設定する必要があります。

ASAv への管理アクセスの設定については、[ASA の展開](#)を参照してください。

ASA 5585-X への管理アクセスの設定については、次の手順を参照してください。

ステップ 1 既存の設定を削除します。

```
ciscoasa(config)# clear configure all
```

ステップ 2 (任意)ファイアウォール モードをトランスペアレント ファイアウォール モードに設定します。

```
ciscoasa(config)# firewall transparent
```

ステップ 3 管理インターフェイスの IP アドレスとサブネット マスクを設定します。ASA は、APIC と同じサブネット上にある必要があります。

```
ciscoasa(config)# interface management {0/0 | 0/1}  
ciscoasa(config-subif)# ip address ip_address subnet_mask
```

ステップ 4 インターフェイスの名前を "management" と指定します。

```
ciscoasa(config-subif)# nameif management
```

ステップ 5 インターフェイスをイネーブルにします。

```
ciscoasa(config-if)# no shutdown
```

ステップ 6 ASA HTTPS サーバをイネーブルにします。

```
ciscoasa(config)# http server enable
```

ステップ 7 APIC で ASA へのアクセスをイネーブルにします。APIC クラスタの各 APIC に対してこの手順を繰り返します。

```
ciscoasa(config)# http apic_address 255.255.255.255 management
```

ステップ 8 ASA にアクセスする際に APIC が使用するユーザを作成します。

```
ciscoasa(config)# username username password password privilege 15
```



注

このユーザは "management-user" である必要はありません。任意のユーザを指定できます。

4 ジャンボフレームサポートの設定

1500 バイトより大きいイーサネット パケットを使用するには、ジャンボ フレーム サポートを設定する必要があります。

-
- ステップ 1** ジャンボ フレームをイネーブルにします。
- ```
ciscoasa(config)# jumbo-frame reservation
```
- ステップ 2** 実行コンフィギュレーションを保存します。
- ```
ciscoasa(config)# write memory
```
- ステップ 3** ASA をリブートします。
- ```
ciscoasa(config)# reload
```
- 

## 5 マルチ コンテキスト モードの設定

- ステップ 1** マルチ コンテキスト モードを設定する場合、手順については、次の URL の『*Cisco ASA Series General Operations CLI Configuration Guide*』の「High Availability and Scalability」の章を参照してください。

<http://www.cisco.com/c/en/us/td/docs/security/asa/asa94/configuration/general/asa-general-cli/ha-contexts.html>

このリンクでは、システム モードでインターフェイスを設定し、それらをコンテキストに割り当て、各コンテキストでインターフェイスを設定する方法について説明しています。それらの手順はすべて、デバイス パッケージで実行します。

デバイス パッケージは、マルチ コンテキスト モードの各サービス グラフで使用されるインターフェイスの割り当ておよび設定を実行します。ただし、システム管理者は、マルチ コンテキスト ASA を APIC に登録する前に、それらを以下のようにプロビジョニングする必要があります。

- ステップ 2** 必要なユーザ コンテキストを作成します。(デバイス パッケージはコンテキストの作成または削除を行いません)。
- ステップ 3** コンテキストごとに、プロビジョニングをシングル コンテキスト ASA のプロビジョニングと同様にします。
- 管理コンテキストから管理インターフェイスをそのコンテキストに割り当てます。

設定例

```
context tenant1
 allocate-interface Management0/1
 config-url disk0:/tenant1.cfg
```

- b. ユーザ コンテキストで、**nameif** を使用して管理インターフェイスを "management" に設定し、静的 IP アドレスを指定します。

設定例

```
interface management 0/1
 nameif management
 ip address 10.1.1.1 255.255.255.0
 security-level 100
```

- c. ユーザ コンテキストで、管理インターフェイスへの HTTPS のアクセスをイネーブルにします。

設定例

```
http server enable
http 0.0.0.0 0.0.0.0 management
```

- d. ユーザの資格情報を設定します。  
e. 管理ルートを設定します。
- 

## 6 ASA クラスタの設定

ASA クラスタを設定する場合、手順については、次の URL の『*Cisco ASA Series General Operations CLI Configuration Guide*』の「ASA Cluster」の章を参照してください。

<http://www.cisco.com/c/en/us/td/docs/security/asa/asa94/configuration/general/asa-general-cli/ha-cluster.html>

## 7 ASA デバイス パッケージのインストール

各サービス ノードタイプで、デバイス仕様とデバイス スクリプトの 2 つの部分を含むデバイス パッケージを指定する必要があります。同じタイプのサービス ノードは、単一のデバイス パッケージにバインドされます。

ASA デバイス パッケージを使用して、次に示すタスクを実行できます。

- ASA の設定。
- APIC への ASA の登録。

---

**ステップ 1** デバイス パッケージをインストールするための前提条件を確認します。

『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*』の「Overview」および「Prerequisites」の章を参照してください。

**ステップ 2** 次の URL から ASA デバイス パッケージ (Cisco.com から入手できる .zip ファイル) をダウンロードします。

<http://www.cisco.com/go/asa-software>

**ステップ 3** ASA デバイス パッケージをインストールします。

『Cisco APIC Layer 4 to Layer 7 Services Deployment Guide』の「Importing a Device Package」の章を参照してください。

**ステップ 4** APIC に ASA を登録します。

『Cisco APIC Layer 4 to Layer 7 Services Deployment Guide』の「Fabric Connectivity」の章を参照してください。

---

## 8 APIC 内での ASA の設定

ノースバウンド API を使用して、セキュリティ ポリシー (特にサービス グラフについて) を設定します。

ノースバウンド API の使用方法については、『Cisco APIC Management Information Model Reference』を参照してください。

ASA 固有のノースバウンド API の XML サンプルについては、『Cisco ASA API Reference for APIC Integration』を参照してください。

APIC のマニュアルについては、

<http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html> を参照してください。

©2016 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1602R)

この資料の記載内容は2016年2月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先