CHAPTER 4

初期設定

この章では、基本的な動作設定をデバイスに提供する、インストーラの Out-Of-Box エクスペリエンス（OBE）について説明します。Cisco ISA 3000では工場出荷時にデフォルトのパラメータ セットが設定されています。

この章の内容は、次のとおりです。

- 工場出荷時のデフォルト設定（4-1ページ）
  - ポート情報（4-1ページ）
  - ASA のデフォルト設定（4-2ページ）
  - CLI の工場出荷時のデフォルト設定（4-4ページ）
- MIB 情報（4-7ページ）
- 設定のためにデバイスに接続する（4-7ページ）
  - 配線の手順（4-8ページ）
  - ISA3000 の電源投入（4-9ページ）
  - ASDM の起動（4-9ページ）
  - 他の ASDM ウィザードおよび詳細設定の実行（4-15ページ）
  - ASA Firepowerモジュールの設定（4-15ページ）
  - 次の作業（4-16ページ）
- 初期設定の確認（4-16ページ）

工場出荷時のデフォルト設定

ISA 3000の工場出荷時のデフォルト設定は、他の ASA デバイスとは若干異なります。次のセクションでは、そうした違いの一部について説明します。

ポート情報

ポート番号付け

ポートの番号付け、つまりインターフェイスの番号付けは、他の ASA デバイスとは異なります。ASA の一般的なポート番号付けは 0 から始まりますが、ISA 3000のポートの番号付けは 1 から始まります。ポートのインターフェイス名は次のようになります。

- ギガビット イーサネット 1/1

- ギガビット イーサネット 1/2
- ギガビット イーサネット 1/3
- ギガビット イーサネット 1/4

管理ポートは次のようになります。

- Management 1/1

USB ポート

外部からアクセス可能なタイプ A の USB 2.0（4 ピン）コネクタが 2 つあります。これらのポートは、大容量ストレージ デバイスをサポートします。これらの 2 つの USB ポートは、ASA では disk1、disk2 と表示されます。以下に例を示します。

```
ciscoasa# show file system
File Systems:
     Size(b)     Free(b)      Type      Flags  Prefixes
* 15621070848   15401517056   disk      rw      disk0: flash:
              -             -  disk      rw      disk1:
              -             -  disk      rw      disk2:
              -             -  network   rw      tftp:
```

これらのポートはデフォルトでイネーブルになっており、オフにすることはできません。

ASA のデフォルト設定

次のセクションでは、ASA のデフォルト設定と Out-Of-Box 動作について説明します。

ファイアウォール モード

ISA 3000はデフォルトではトランスペアレント モードで動作します。ファイアウォール ポリシーについては、このセクションで後述します。

管理ポート

管理ポートにはデフォルトのスタティック IP アドレス、192.168.1.1 が割り当てられています。

次に例を示します。

```
interface Management1/1
         management-only
         no shutdown
         nameif management
         security-level 100
         ip address 192.168.1.1 255.255.255.0
```

DHCP サーバ

管理ポートに接続されている DHCP が有効なクライアントは、ISA 3000から直接、IP アドレスを取得できます。デフォルト設定では、ISA 3000の管理ポートで有効になっている DHCP サーバを指定します。DHCP クライアントにリースできる IP アドレスの範囲は、管理ポートに割り当てられた IP アドレスに重複しない範囲です。この IP アドレスのデフォルトの範囲は 192.168.1.5 から 192.168.1.254 の間で選択されます。

HTTP サーバ

デフォルト設定では、管理ポートでクライアントからISA 3000への Cisco ASDM アクセスを提供します。デフォルト設定は、管理ポートの HTTP サーバを自動的にイネーブルにします。初回の Cisco ASDM アクセスではパスワードが施行されません。

データ ポート

デフォルトではすべてのデータ ポートがブリッジ グループにあります。これにより、どのインターフェイスを介してもトラフィック フローが他のインターフェイスに流れることができます（ブリッジ モード）。ただし、必要に応じてハードウェア バイパス機能を利用するには、トラフィックにギガビット イーサネット 1/1 および 1/2 ペア（または、Copper SKU では、ギガビット イーサネット 1/3 および 1/4 ペア）を使用することが推奨されます。

allowAll アクセス リストを作成し、CLI または ASDM を使用してそれをデータ インターフェイスに適用できます。SourceFire トラフィック用には別のアクセス リスト、sfrAccesList が作成されます。

次に例を示します。

```
interface BVI 1
!
interface GigabitEthernet1/1
  bridge-group 1
 no shutdown
 nameif outside1
 security-level 0
!
interface GigabitEthernet1/2
 bridge-group 1
 no shutdown
 nameif inside1
 security-level 100
!
interface GigabitEthernet1/3
 bridge-group 1
 no shutdown
 nameif outside2
 security-level 0
!
interface GigabitEthernet1/4
 bridge-group 1
 no shutdown
 nameif inside2
 security-level 100
!
access-list allowAll permit ip any any
access-list sfrAccessList extended permit ip any any
```

(注) ISA3000 データポートは、/30 または /31 のマスクを持つことはできません。

ファイアウォール ポリシー

データ ポートはデフォルトで有効になっています。トラフィックは、デフォルトで存在するポリシー マップとクラス マップを使用して、SFR に転送されます。

(注)　BVI インターフェイスがデータの転送を有効にするには、適切な IP アドレスが必要です。同じネットワークに明示的に設定された BVI IP アドレスがなければ、トラフィック フローが停止します。

アクセス リストの sfrAccessList のデフォルト設定では、すべてのトラフィックを突き合わせます。たとえば、以下を使用して HTTP トラフィックのみを識別し、SFR に送ることができます。

```
access-list httpTraffic permit tcp any any eq http
class-map httpClass
 match access-list httpTraffic

policy-map global_policy
 class httpClass
  sfr fail-open
```

FirePOWER 検査のトラフィックを識別するクラス マップのデフォルト設定は次のとおりです。

```
class-map sfrclass
 match access-list sfrAccessList

Default configuration of policy map for the actions to be performed on the traffic
identified:

policy-map global_policy
 class sfrclass
  sfr fail-open monitor-only
```

CLI の工場出荷時のデフォルト設定

CLI の一般的な工場出荷時のデフォルト設定は次のとおりです。

```
ciscoasa# show run

: Saved

:
: Serial Number: FCH1XXXXX
: Hardware:   ISA3000, 8xxx MB RAM, CPU Demo MHz, 1 CPU (4 cores)
:
ASA Version 9.x(x)x
!
firewall transparent
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
名前
!
interface GigabitEthernet1/1
 bridge-group 1
 nameif outside1
 no shutdown
!
interface GigabitEthernet1/2
 bridge-group 1
 nameif inside1
 security-level 100
 no shutdown
!
interface GigabitEthernet1/3
```

```
 bridge-group 1
 nameif outside2
 no shutdown
!
interface GigabitEthernet1/4
 bridge-group 1
 nameif inside2
 security-level 100
 no shutdown
!
```

(注)　ギガビット イーサネット 1/1 ～ 1/4 は、任意のポートから他の任意のポートへのトラフィックが可能なブリッジ グループ 1 にあります。

```
interface Management1/1
 management-only
 no shutdown
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
```

(注)　192.168.1.1 は、デフォルトの管理 IP アドレスです。これは、単一のデバイス マネージャ、ASDM または CLI で ISA 3000を管理するために使用できるアドレスです

```
!
interface BVI 1
no ip address
!
```

(注)　ASA がトランスペアレント モードのときにポート間でデータが流れるためには、BVI インターフェイスに IP アドレスが必要です。

```
ftp mode passive
no hardware-bypass boot-delay module-up sfr
hardware-bypass Gigabit Ethernet 1/1-1/2
hardware-bypass Gigabit Ethernet 1/3-1/4
```

(注)　デフォルトでは、copper SKU の両方のペアでハードウェア バイパスがイネーブルになっています。ASA が復旧すると、ハードウェア バイパスはオフになります。

```
access-list allowAll extended permit ip any any
access-list sfrAccessList extended permit ip any any

access-group allowAll in interface outside1
access-group allowAll in interface outside2

same-security-traffic permit inter-interface

pager lines 24
logging asdm informational
mtu management 1500
mtu inside1 1500
mtu outside1 1500
mtu inside2 1500
mtu outside2 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
```

```
arp timeout 14400
no arp permit-nonconnected
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
user-identity default-domain LOCAL
http server enable
http 192.168.1.0 255.255.255.0 management
```

(注)　管理ポートにより、ASDM アクセスを有効にします。

```
no snmp-server location
no snmp-server contact
service sw-reset-button
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
no ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
dhcpd address 192.168.1.5-192.168.1.254 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
 match default-inspection-traffic
!
class-map sfrclass
 match access-list sfrAccessList
!
policy-map type inspect dns preset_dns_map
 パラメータ
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  class sfrclass
```

```
  sfr fail-open monitor-only
 !
!
```

(注)　FirePOWER モジュールで障害が発生した場合、「fail-open」モードにより、ASA でトラフィックの無視および転送が可能になります。コマンド「monitor-only」を実行すると ASA から SFR へのパケットがコピーされ、パッシブ/オフライン インスペクションが行われます。

```
service-policy global_policy global
prompt hostname context

Cryptochecksum:61c9397c4e5eb7f0ffc14e902ccba3e7

: end

ciscoasa#
```

MIB 情報

ISA 3000は、現在 ASA ソフトウェアでサポートされるすべての MIB をサポートします。

ASA でサポートされる MIB は、SNMP 構成ガイドの URL で確認できます。

http://www.cisco.com/c/en/us/td/docs/security/asa/asa94/configuration/general/asa-general-cli/monitor-snmp.html

そこで、ネットワーク管理 MIB の URL を見つけることができます。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

設定のためにデバイスに接続する

Cisco ISA 3000には、初期設定を行うために使用できる 3 つのオプションがあります。

1. USB ポートを使用する CLI

   このオプションでは、USB ケーブルを使ってデバイスのミニ USB ポートに PC を接続します。

   正しいドライバがインストールされていれば、ターミナル プログラムを起動できます。ルータと通信する適切なドライバがないという警告が PC やラップトップに表示された場合は、ドライバをパソコン メーカーから入手するか、または次の URL を参照してください。https://www.silabs.com/products/mcu/Pages/USBtoUARTBridgeVCPDrivers.aspx

2. RJ-45 コンソール ポートを使用する CLI

   このオプションでは、DB9 コネクタおよびケーブルに標準の RJ45 を使用して、Cisco ISA 3000の RJ-45 コンソール ポートに PC を接続します。

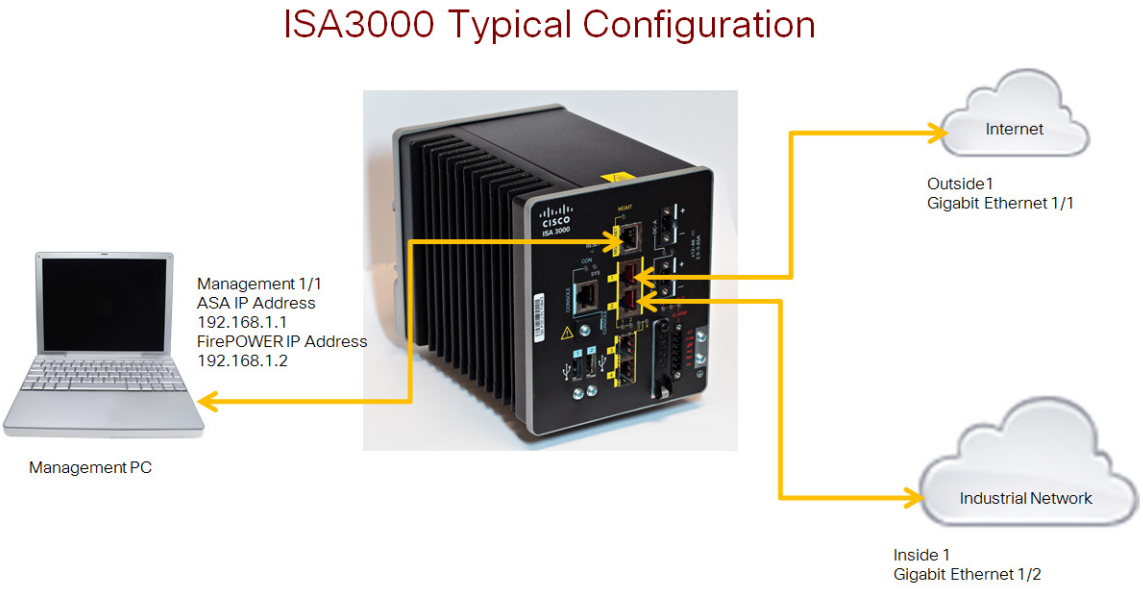
3. 管理 1/1 インターフェイスから ASDM

   設定する PC がCisco ISA 3000の管理インターフェイスと同じサブネットワークにある場合は、ASDM を使用してデバイスを設定できます。IP アドレスの範囲は、192.168.1.5 から 192.168.1.254 です。ASDM GUI を起動して、デバイスの設定を開始できます。

配線の手順

次の図は、基本的なネットワークの接続です。

図 4-1　　基本的なネットワーク



手順 1　以下をケーブルで直接、デバイスまたはレイヤ 2 イーサネット スイッチに接続します。

- ギガビット イーサネット 1/2 インターフェイス（内部）
- 管理 1/1 インターフェイス（ASA FirePOWER モジュール用）

（注）　管理インターフェイスは ASA FirePOWER モジュールだけに属する別のデバイスとして動作するため、内部インターフェイスと管理インターフェイスは同じネットワークで接続できます。

手順 2　ギガビット イーサネット 1/1（外部）インターフェイスを WAN デバイス（たとえばケーブル モデムなど）に接続します。

（注）　ケーブル モデムで 192.168.1.0/24 または 192.168.10.0/24 の外部 IP アドレスが指定された場合、別の IP アドレスを使用するように ISA 3000の設定を変更する必要があります。

ISA3000 の電源投入

手順 1　電源プラグの適切な配線手順については、章 3「DC 電源への接続」の説明を参照してください。

手順 2　電源プラグは DC 電源に配線した後に ISA3000 に接続します。

手順 3　LED のステータスを調べて、デバイスが正常に動作していることを確認します。章 3「接続の確認」を参照してください。

ASDM の起動

ASDM を実行するための要件については、Cisco.com の『ASDM release notes』を参照してください。

ここでは、ASA FirePOWER モジュールを管理するために、ASDM を使用することを前提としています。FireSIGHT システムを使用する場合は、モジュール CLI に接続し、セットアップ スクリプトを実行する必要があります。『ASA Firepower quick start guide』を参照してください。

手順

手順 1　ISA 3000に接続されているコンピュータで、Web ブラウザを起動します。

手順 2　[Address] フィールドに **https://192.168.1.1/admin** という URL を入力します。

手順 3　ブラウザで、信頼できないアプリケーションの実行を許可してよいかどうか、確認を求められます。ブラウザによっては、ユーザは別の方法で応答します。適切な応答については、セキュリティの質問に対するブラウザでの応答を参照してください。

手順 4　[Cisco ASDM]Web ページが表示されます。

(注)　管理コンピュータをワイヤレス クライアントとして ASA に接続した場合は、**https://192.168.10.1/admin** で ASDM にアクセスできます。

手順 5　使用可能なオプション（[InstallASDM Launcher]、[Run ASDM]、[Run Startup Wizard]）のいずれかをクリックします。

手順 6　画面の指示に従ってオプションを選択し、ASDM を起動します。[Cisco ASDM-IDM Launcher] が表示されます。

[Install ASDM Launcher]をクリックした場合、場合によっては、「Install an Identity Certificate for ASDM」に従って ISA3000 の ID 証明書と ASA FirePOWER モジュールの証明書をそれぞれインストールすることが必要になります。

手順 7　ユーザ名とパスワードのフィールドを空のまま残し、[OK]をクリックします。メイン ASDM ウィンドウが表示されます。

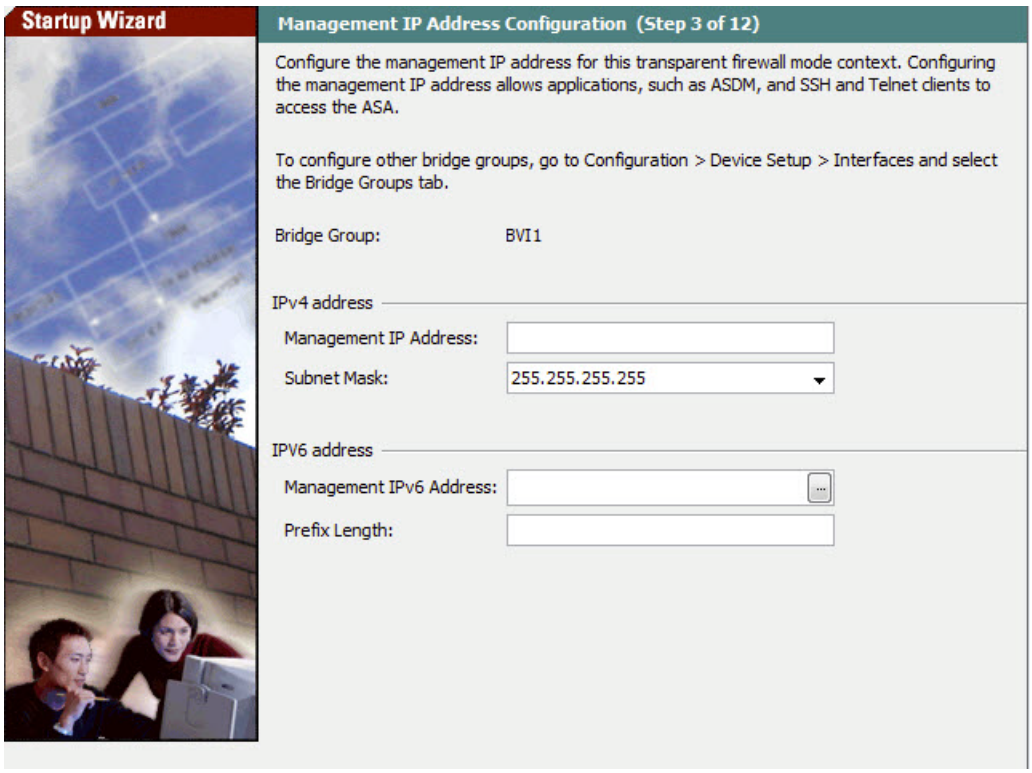
手順 8　インストールする ASA FirePOWER モジュールの IP アドレスを指定するよう求められた場合は、ダイアログボックスをキャンセルします。[Startup Wizard] を使用して、まず、モジュールの IP アドレスを正しい IP アドレスに設定する必要があります。

ASDM は ASA バックプレーンを介して ASA FirePOWER モジュールの IP アドレス設定を変更できます。ただし、モジュールを管理するには、ネットワークを介して管理 1/1 インターフェイス上のモジュール（および新しい IP アドレス）にアクセスする必要があります。推奨される

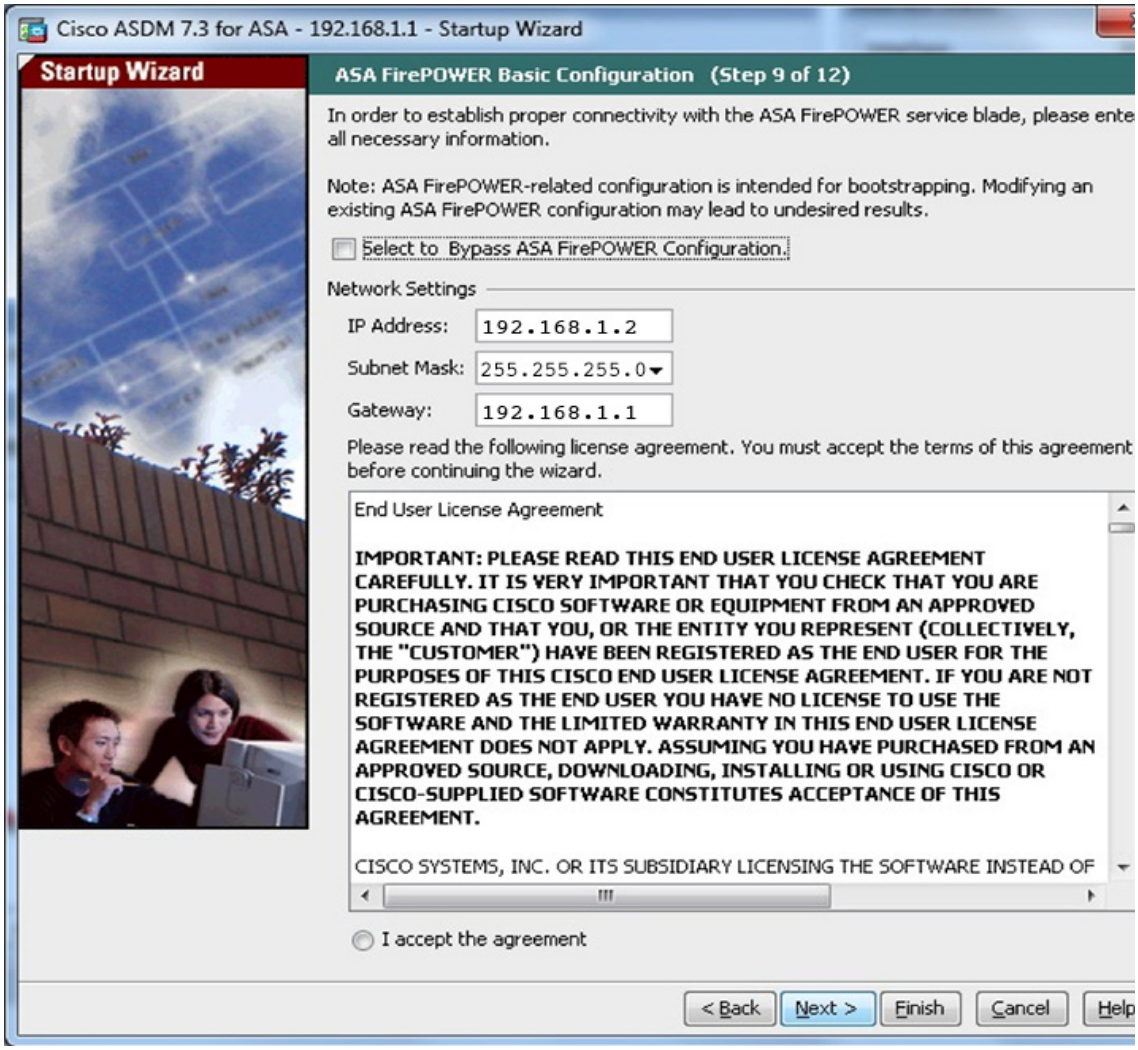
展開ではモジュールの IP アドレスが内部ネットワークに存在するため、このアクセスが可能です。IP アドレスを設定した後に ASDM がネットワーク上のモジュールに到達できない場合は、エラーが表示されます。

手順 9　[Wizards] > [Startup Wizard]を選択します。

手順 10　トラフィック インターフェイス（ギガビット イーサネット1/1 ～ 1/4）に接続するローカル ネットワークと同じサブネットで明示的に設定された IP アドレスをブリッジ グループ管理が持つことを確認してください。



手順 11　必要に応じて追加の ASA 設定を行うか、または、ASA FirePOWER の [Basic Configuration] 画面が表示されるまで、画面を進んでください。



デフォルト設定を使用するには、次の値を設定します。

- [IPAddress]：192.168.1.2
- [SubnetMask]：255.255.255.0
- [Gateway]：192.168.1.1

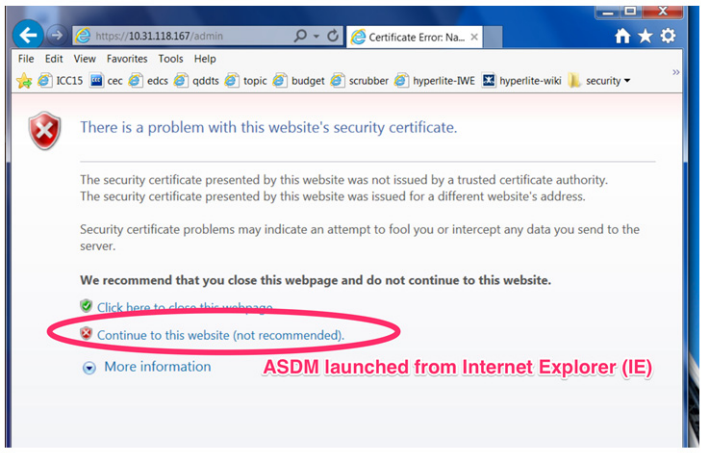
手順 12　[I accept the agreement]をクリックして、[Next] または [Finish] をクリックすると、ウィザードが終了します。

手順 13　ASDM を終了し、再起動します。ホームページに ASA FirePOWER のタブが表示されます。

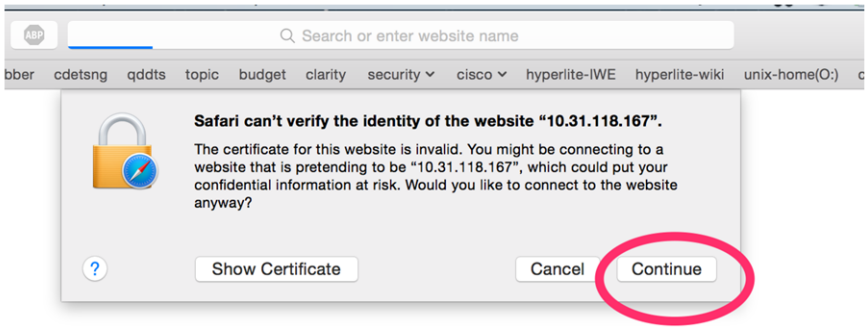
セキュリティの質問に対するブラウザでの応答

ここでは、ASDM の起動中に上記のステップ 3 のセキュリティの質問に応答する方法を示します。

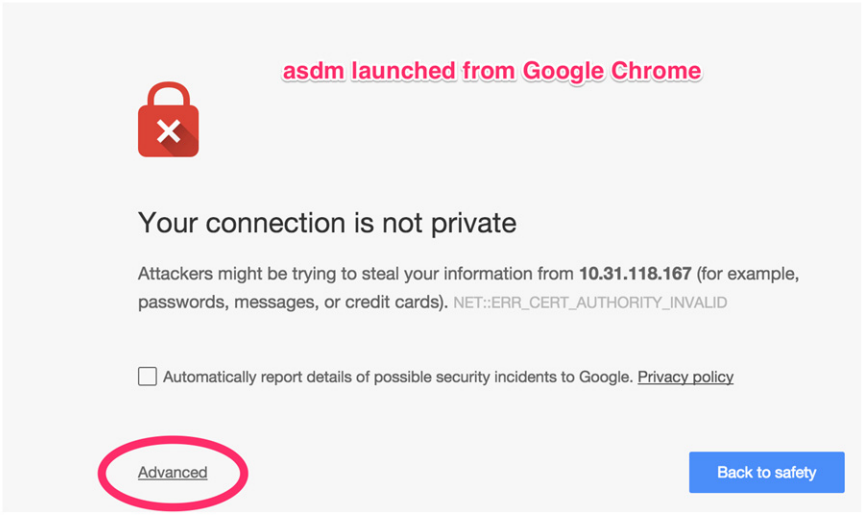
Internet Explorer[InternetExplorer]



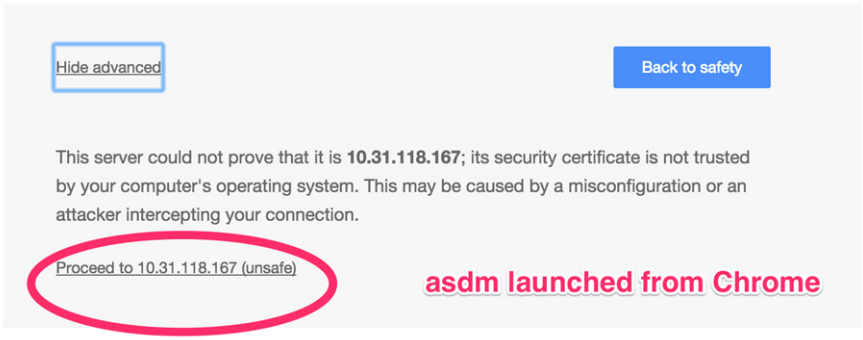
Safari



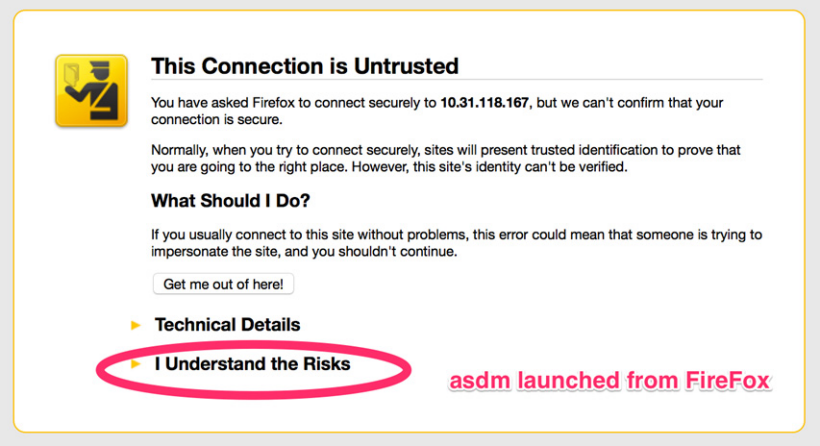
Chrome ステップ 1



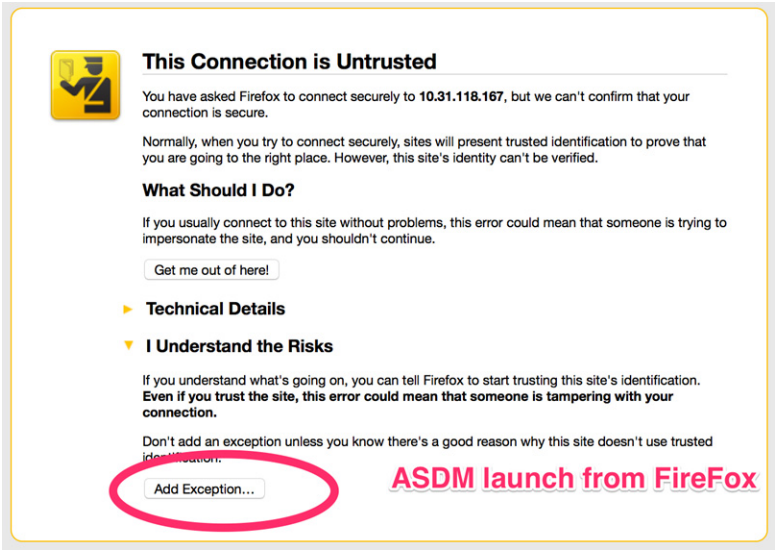
Chrome ステップ 2



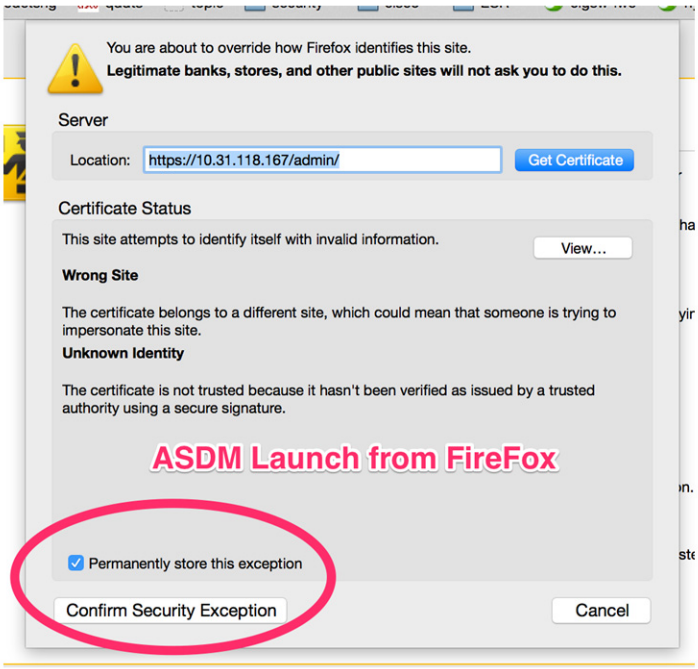
Firefox ステップ 1



Firefox ステップ 2



Firefox ステップ 3



他の ASDM ウィザードおよび詳細設定の実行

ASDM には、セキュリティ ポリシーを設定するためのウィザードが多数含まれています。使用可能なすべてのウィザードを見るには、[Wizards]メニューを参照してください。

ISA 3000の設定を続行するには、『Navigating the Cisco ASA Series Documentation』でソフトウェア バージョンに応じたマニュアルを参照してください。

ASA Firepowerモジュールの設定

ASDM を使用して、モジュールのセキュリティ ポリシーを設定し、モジュールにトラフィックを送信します。

(注)　注：別の方法として、FireSIGHT 管理センターを使用してASA Firepower モジュールを管理することもできます。詳細については、『ASA Firepower Module Quick Start Guide』を参照してください。

手順

手順 1　ASDM のASA Firepowerのページを使用して、モジュールのセキュリティ ポリシーを設定します。ポリシーの設定方法について詳しく知るには、任意のページで [Help]をクリックするか、または [Help] > [ASA FirepowerHelp Topics] を選択します。

手順 2　トラフィックをモジュールに送信するには、[Configuration]> [Firewall] > [Service Policy Rules] を選択します。

手順 3　[Add] > [Add Service PolicyRule] を選択します。

手順 4　ポリシーを特定のインターフェイスに適用するか、または全体的に適用するかを選択し、[Next]をクリックします。

手順 5　トラフィックの一致を設定します。たとえば、インバウンドのアクセス ルールを通過したすべてのトラフィックがモジュールへリダイレクトされるように、一致を [Any Traffic]に設定できます。また、ポート、ACL（送信元と宛先の基準）、または既存のトラフィック クラスに基づいて、より厳密な基準を定義することもできます。このポリシーでは、その他のオプションはあまり有用ではありません。トラフィック クラスの定義が完了したら、[Next]をクリックします。

手順 6　[Rule Actions] ページで[ASA Firepower Inspection] タブをクリックします。

手順 7　[Enable ASA Firepower for this traffic flow]チェックボックスをオンにします。

手順 8　[If ASA FirePOWER Card Fails] 領域で、次のいずれかをクリックします。

- [Permittraffic]：モジュールが使用できない場合、すべてのトラフィックの通過を検査なしで許可するように ISA 3000 を設定します。
- [Closetraffic]：モジュールが使用できない場合、すべてのトラフィックをブロックするように ISA 3000 を設定します。

手順 9　（オプション）トラフィックの読み取り専用のコピーをモジュールに送信する（つまりパッシブ モードにする）には、[Monitor-only]をオンにします。

手順 10　[Finish]、[Apply]の順にクリックします。

手順 11　この手順を繰り返して、追加のトラフィック フローを必要に応じて設定します。

次の作業

ASA Firepowerモジュールと ASA 操作の詳細については、ASA/ASDM のファイアウォール設定ガイドの「ASA Firepower Module」の章、または ASDM のオンライン ヘルプを参照してください。ASA/ASDM のすべてのドキュメントのリンクについては、Navigating the Cisco ASA Series Documentation を参照してください。

ASA FirePOWER の設定の詳細については、オンライン ヘルプまたは『ASA Firepower Module User Guide』または『FireSIGHT System User Guide』を参照してください。

初期設定の確認

新しいインターフェイスが正しく動作していることを確認するには、次のテストを実行します。

- インターフェイスおよび回線プロトコルが正常な状態（アップまたはダウン）にあるかどうかを確認するには、**show interfaces** コマンドを入力します。
- IP に設定されたインターフェイスのサマリー ステータスを表示するには、**show ip interface brief** コマンドを使用します。
- 正しいホスト名とパスワードが設定されていることを確認するには、**show configuration** コマンドを入力します。

初期設定を完了し、確認した後は、Cisco ISA 3000で特定の機能を設定できます。