CHAPTER 10

CSC SSM の設定

ASA 5500 シリーズ 適応型セキュリティ アプライアンスは、Content Security and Control ソフトウェアを実行する CSC SSM をサポートします。CSC SSM は、ウイルス、スパイウェア、スパムなど、望ましくないトラフィックからの保護を提供します。そのために、適応型セキュリティ アプライアンスで FTP、HTTP、POP3、および SMTP トラフィックを CSC SSM に誘導し、スキャンします。

（注） CSC SSM には、ASA ソフトウェア リリース 7.1.1 以降が必要です。CSC SSM は、ASA 5540 ではサポートされません。

次の項目について説明します。

CSC SSM について

CSC SSM は、疑わしいコンテントのシグニチャ プロファイルが含まれるファイルを管理し、Trend Micro のアップデート サーバから定期的にアップデートします。CSC SSM は、適応型セキュリティ アプライアンスから受信したトラフィックをスキャンし、Trend Micro から取得したコンテント プロファイルと比較します。正当なコンテントは適応型セキュリティ アプライアンスに転送してルーティングし、疑わしいコンテントはブロックしてレポートします。

Trend Micro からコンテント プロファイルを取得するほかに、システム管理者は、CSC SSM が追加のトラフィック タイプまたはロケーションをスキャンするように、設定をカスタマイズすることもできます。たとえば、システム管理者は、特定の URL をブロックまたはフィルタリングしたり、FTP や電子メールのパラメータをスキャンするように、CSC SSM を設定できます。

CSC SSM のシステム セットアップおよびモニタリングは、ASDM を使用して実行できます。CSC SSM ソフトウェアのコンテント セキュリティ ポリシーの高度な設定を行うには、ASDM のリンクをクリックして、CSC SSM の Web ベースの GUI にアクセスします。

この章では、配置用に適応型セキュリティ アプライアンスを設定する方法を説明します。CSC SSM GUI の使用方法については、『*Cisco Content Security and Control SSM Administrator Guide*』で説明します。

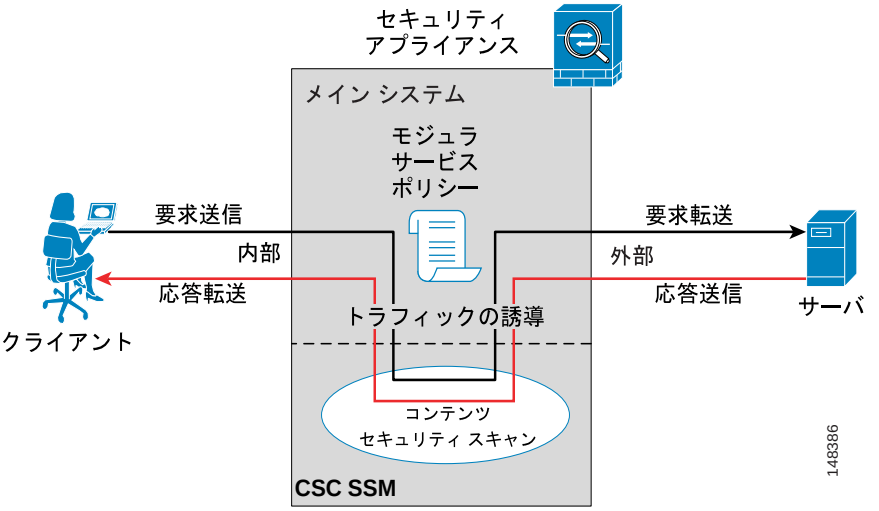
CSC SSM を使用するセキュリティ アプライアンスの配置について

CSC SSM と共に適応型セキュリティ アプライアンスを配置するネットワークでは、スキャンする種類のトラフィックだけを CSC SSM に送信するように、適応型セキュリティ アプライアンスを設定します。

図 10-1 で、企業ネットワーク、適応型セキュリティ アプライアンス、および CSC SSM と、インターネットとの間の基本的なトラフィック フローを示します。図 10-1 で示すネットワークには、次の要素が含まれています。

- CSC SSM が取り付けられ、設定されている適応型セキュリティ アプライアンス
- CSC SSM に誘導してスキャンするトラフィックを指定する、適応型セキュリティ アプライアンスのサービス ポリシー

図 10-1　CSC SSM のトラフィック フロー



この例では、クライアントは Web サイトにアクセスできるネットワーク ユーザ、FTP サーバからファイルをダウンロードできるネットワーク ユーザ、または POP3 サーバからメールを取得できるネットワーク ユーザです。

この設定では、トラフィック フローは次のようになります。

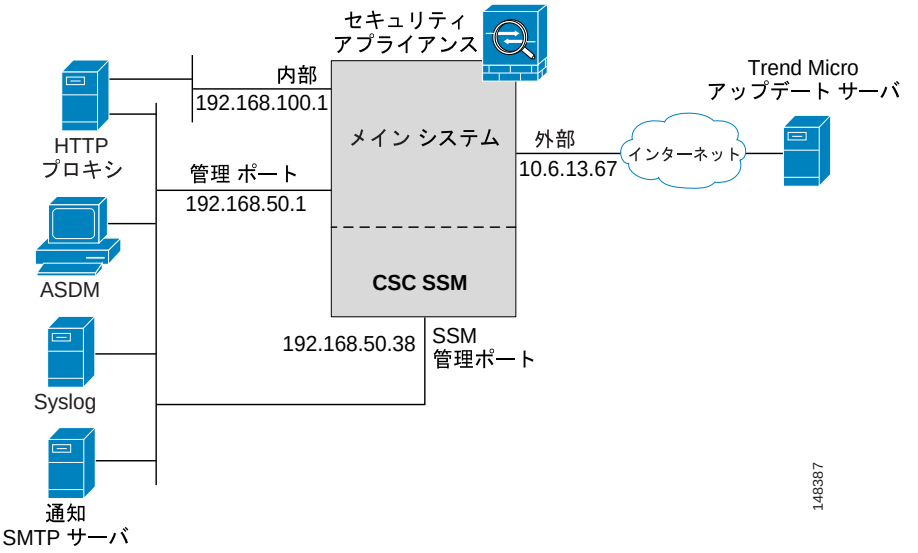
1. クライアントが要求を開始する。
2. 適応型セキュリティ　アプライアンスが要求を受信し、インターネットに転送する。
3. 要求されたコンテントを適応型セキュリティ　アプライアンスが取得し、このコンテント タイプが CSC SSM に誘導し、スキャンする対象としてサービス ポリシーで定義されているかどうかを判別する。定義されている場合は、CSC SSM に誘導する。
4. CSC SSM が適応型セキュリティ アプライアンスからコンテントを受信し、スキャンし、Trend Micro コンテント フィルタの最新アップデートと比較する。
5. コンテントが疑わしい場合、CSC SSM はコンテントをブロックし、イベントをレポートする。コンテントが疑わしくない場合、CSC SSM は要求されたコンテントを適応型セキュリティ アプライアンスに戻し、ルーティングする。

（注） SMTP トラフィックは、他のコンテント タイプとは異なる方法で処理されます。スキャンしたトラフィックを適応型セキュリティ アプライアンスに戻してルーティングするのではなく、適応型セキュリティ アプライアンスで保護されている SMTP サーバに、CSC SSM が SMTP トラフィックを直接転送します。

シナリオ：コンテント セキュリティ用に配置されている CSC SSM を使用するセキュリティ アプライアンス

図 10-2 で、CSC SSM を使用する適応型セキュリティ アプライアンスの一般的な配置を示します。このシナリオのプロパティは、この章の後半の設定手順で例として使用します。

図 10-2　CSC SSM 配置のシナリオ



このシナリオでは、顧客がコンテント セキュリティ用に CSC SSM を使用する、適応型セキュリティ アプライアンスを配置しています。次の点に注意してください。

- 適応型セキュリティ　アプライアンスが専用管理ネットワークにある。必ずしも専用管理ネットワークを使用する必要はないが、セキュリティの理由により、使用することが推奨される。
- この適応型セキュリティ　アプライアンス設定には、2 つの管理ポートがある。1 つは、適応型セキュリティ アプライアンス自身の管理ポートで、もう 1 つは、CSC SSM の管理ポート。すべての管理ホストが、両方の IP アドレスにアクセスできる必要がある。

- HTTP プロキシ サーバが、内部ネットワークと専用管理ネットワークの両方に接続されている。これによって、CSC SSM は Trend Micro のアップデート サーバから、最新のコンテント セキュリティ フィルタを取得できる。
- 管理ネットワークに SMTP サーバが含まれており、管理者は CSC SSM イベントの通知を受けることができる。管理ネットワークには syslog サーバも含まれており、CSC SSM が生成したログを保管できる。

設定の要件

適応型セキュリティ アプライアンスの配置を計画するときは、ネットワークが次の要件を満たしている必要があります。

- SSM の管理ポートの IP アドレスに、ASDM の実行に使用するホストからアクセスできる。ただし、SSM の管理ポートと適応型セキュリティ アプライアンス管理インターフェイスの IP アドレスは、別のサブネットにできる。
- SSM の管理ポートは、CSC SSM が Trend Micro のアップデート サーバに到達できるように、インターネットに接続できる必要がある。

コンテント セキュリティ用の CSC SSM の設定

適応型セキュリティ アプライアンスと同時にオプションの CSC SSM モジュールを注文した場合、初期設定を完了するために、いくつかの手順を実行する必要があります。設定手順の一部は適応型セキュリティ アプライアンスで実行し、残りの設定手順は CSC SSM で実行するソフトウェアで実行します。

このマニュアルの前の手順を実行していた場合、この時点で、ASA システムはライセンス付きのソフトウェアを実行し、セットアップ ウィザードで基本的なシステム値が入力されています。次に、コンテント セキュリティ配置用に、適応型セキュリティ アプライアンスを設定します。

基本的な手順は、次のとおりです。

1. Cisco.com からソフトウェア アクティベーション キーを取得する。
2. CSC SSM の設定に必要な情報を収集する。
3. Cisco.com からアクティベーション キーを取得する。
4. このセットアップ プロセスのすべての設定作業に使用する ASDM を開く。
5. 時間設定を確認する。

6. CSC セットアップ ウィザードを実行して、CSC SSM を設定する。
7. 適応型セキュリティ アプライアンス を設定して、トラフィックを CSC SSM に誘導してスキャンする。

これらの手順は、次の項で詳しく説明します。

Cisco.com からのソフトウェア アクティベーション キーの取得

CSC SSM を使用して、Product Authorization Key（PAK）を受信します。PAK を使用して、次の URL で CSC SSM を登録します。

http://www.cisco.com/go/license

登録後、電子メールでアクティベーション キーを受信します。このアクティベーション キーは、「CSC セットアップ ウィザードの実行」で説明する手順で必要になります。

情報の収集

適応型セキュリティ アプライアンス、および CSC SSM の設定を開始する前に、次の情報を収集します。

- CSC SSM の管理ポートの IP アドレス ネットマスク、ゲートウェイ IP アドレス、およびネットマスク（適応型セキュリティ アプライアンスの IP アドレスは、第 5 章「適応型セキュリティ アプライアンスの設定」で説明するように、Setup Wizard を実行したときに割り当てられます）

（注）　SSM の管理ポート IP アドレスには、ASDM の実行に使用するホストからアクセスできる必要があります。SSM の管理ポートと、適応型セキュリティ アプライアンス管理インターフェイスの IP アドレスは、別のサブネットにできます。

- CSC SSM で使用するホスト名とドメイン名
- DNS サーバの IP アドレス
- HTTP プロキシ サーバの IP アドレス（ネットワークで、インターネットへの HTTP アクセスにプロキシを使用している場合）

- 電子メール通知に使用する電子メール アドレスと、SMTP サーバの IP アドレスおよびポート番号
- CSC SSM への管理アクセスを許可するホスト、およびネットワークの IP アドレス

ASDM の起動

ASDM を使用して、CSC SSM の設定と管理を行います。CSC SSM ソフトウェアのコンテント セキュリティ ポリシーの高度な設定を行うには、ASDM のリンクをクリックして、CSC SSM の Web ベースの GUI にアクセスします。

ASDM を起動するには、次の手順を実行します。

ステップ 1　適応型セキュリティ アプライアンス、および CSC SSM の管理ポートにアクセスできる PC で、インターネット ブラウザを起動します。

ステップ 2　ブラウザのアドレス フィールドに、URL「**https://*IP_address/***」を入力します。

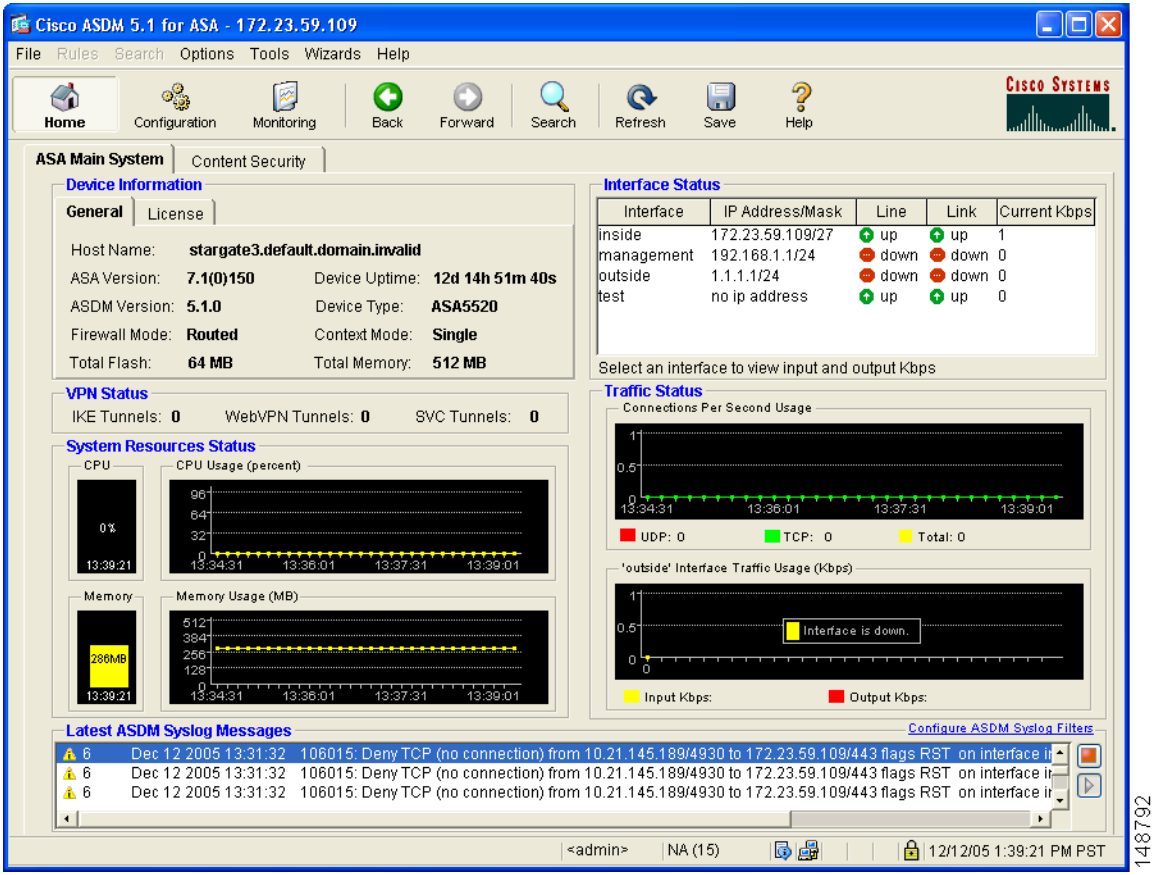
ここで、*IP_address* は、適応型セキュリティ アプライアンスの IP アドレスです。

（注）　適応型セキュリティ アプライアンスの出荷時のデフォルト IP アドレスは 192.168.1.1 です。「**s**」を追加して「**https**」にすることに注意してください。追加しないと、接続が失敗します。HTTPS（HTTP over SSL）は、ブラウザと適応型セキュリティ アプライアンスとの間で、セキュアな接続を提供します。

ステップ 3　ユーザ名とパスワードを要求するダイアログボックスで、両方のフィールドを空のままにします。**Enter** キーを押します。

ステップ 4　**Yes** をクリックして、証明書を受け付けます。すべてのユーザ認証および証明書ダイアログボックスで、**Yes** をクリックします。

ASDM のメイン ウィンドウが表示されます。


Cisco ASDM 5.1 for ASA - 172.23.59.109
File Rules Search Options Tools Wizards Help
Home
Configuration
Monitoring
Back
Forward
Search
Refresh
Save
Help
Cisco Systems
ASA Main System
Content Security
Device Information
General
License
Host Name: stargate3.default.domain.invalid
ASA Version: 7.1(0)150
Device Uptime: 12d 14h 51m 40s
ASDM Version: 5.1.0
Device Type: ASA5520
Firewall Mode: Routed
Context Mode: Single
Total Flash: 64 MB
Total Memory: 512 MB
Interface Status
Interface | IP Address/Mask | Line | Link | Current Kbps
inside | 172.23.59.109/27 | up | up | 1
management | 192.168.1.1/24 | down | down | 0
outside | 1.1.1.1/24 | down | down | 0
test | no ip address | up | up | 0
Select an interface to view input and output Kbps
VPN Status
IKE Tunnels: 0
WebVPN Tunnels: 0
SVC Tunnels: 0
System Resources Status
CPU
CPU Usage (percent)
Memory
Memory Usage (MB)
Traffic Status
Connections Per Second Usage
UDP: 0
TCP: 0
Total: 0
'outside' Interface Traffic Usage (Kbps)
Interface is down.
Input Kbps:
Output Kbps:
Latest ASDM Syslog Messages
Configure ASDM Syslog Filters
6 Dec 12 2005 13:31:32 106015: Deny TCP (no connection) from 10.21.145.189/4930 to 172.23.59.109/443 flags RST on interface
6 Dec 12 2005 13:31:32 106015: Deny TCP (no connection) from 10.21.145.189/4930 to 172.23.59.109/443 flags RST on interface
6 Dec 12 2005 13:31:32 106015: Deny TCP (no connection) from 10.21.145.189/4930 to 172.23.59.109/443 flags RST on interface
<admin>
NA (15)
12/12/05 1:39:21 PM PST
148792

時間設定の確認

適応型セキュリティ アプライアンスの時間設定が、時間帯を含めて正しいことを確認します。時間は、CSC SSM でのセキュリティ イベントのロギング、およびコンテント フィルタ リストの自動アップデートにとって重要です。また、ライセンスは時間の影響を受けるため、ライセンスにとっても重要です。

- 時間設定を手動で制御する場合は、クロック設定を確認します。ASDM で、**Configuration > Properties > Device Administration > Clock** をクリックします。
- NTP を使用して時間設定を制御する場合は、NTP 設定を確認します。ASDM で、**Configuration > Properties > Device Administration > NTP** をクリックします。

CSC セットアップ ウィザードの実行

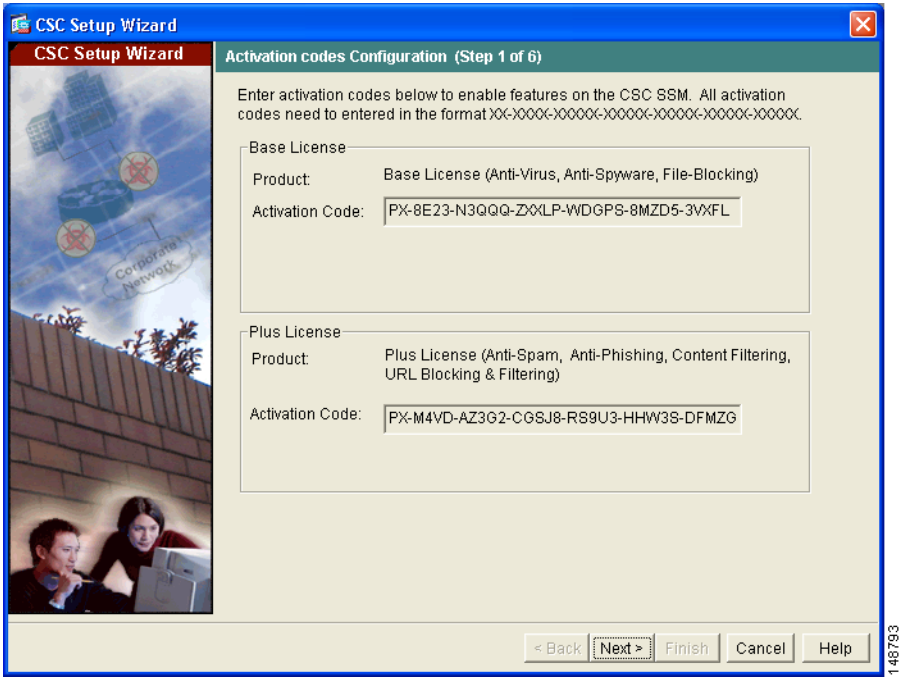
ステップ 1　ASDM のメイン ウィンドウで、**Configuration** タブをクリックします。

ステップ 2　左ペインで、**Trend Micro Content Security** タブをクリックします。

Wizard Setup 画面が表示されます。

ステップ 3　CSC Wizard の Step 1 で、Base License の **Software Activation Codes**（アクティベーション コード）を入力します。オプションで、Plus License のアクティベーション コードを入力します。

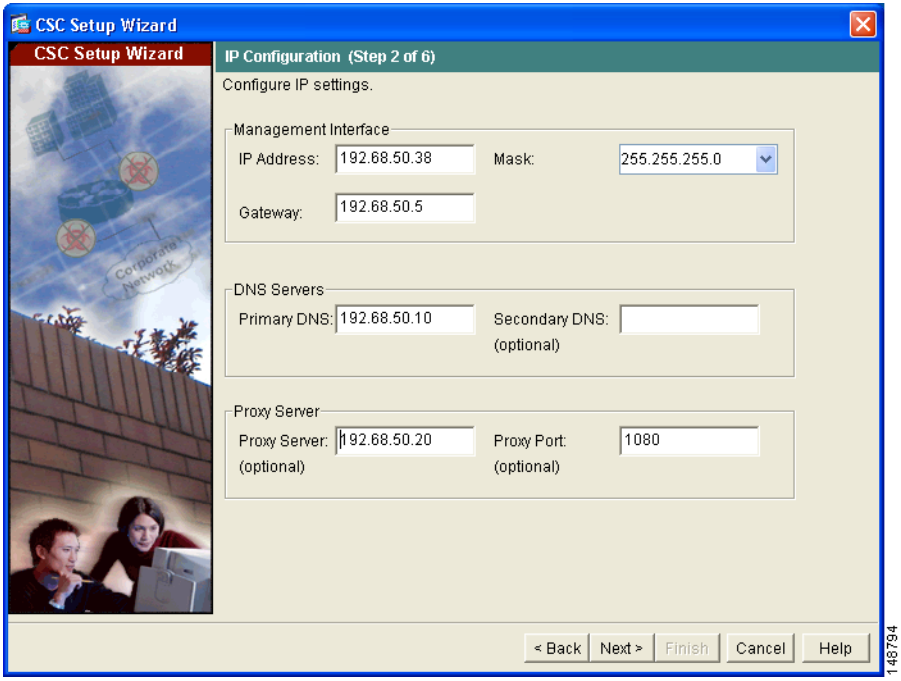
Plus License のアクティベーション コードは、CSC SSM の初期設定の後でも入力できます。



ステップ 4　**Next** をクリックします。

ステップ 5　CSC Wizard の Step 2 で、次の情報を入力します。

- CSC 管理インターフェイスの IP アドレス、ネットマスク、およびゲートウェイ IP アドレス
- プライマリ DNS サーバの IP アドレス
- HTTP プロキシ サーバの IP アドレスおよびプロキシ ポート（ネットワークで HTTP 要求をインターネットに送信するときに、HTTP プロキシを使用している場合のみ）



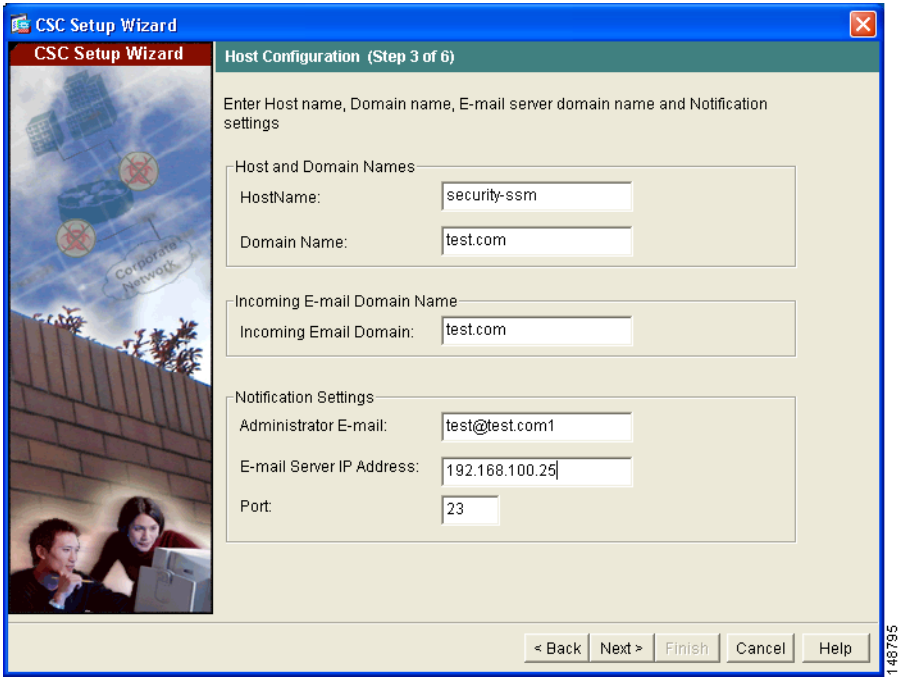
ステップ 6　**Next** をクリックします。

ステップ 7　CSC Setup Wizard の Step 3 で、次の情報を入力します。

- CSC SSM の **Hostname**（ホスト名）および **Domain**（ドメイン名）
- **Domain**（ドメイン名）は、着信ドメインとしてローカル メール サーバで使用します。

（注）　アンチスパム ポリシーは、このドメインに着信した電子メール トラフィックにのみ適用されます。

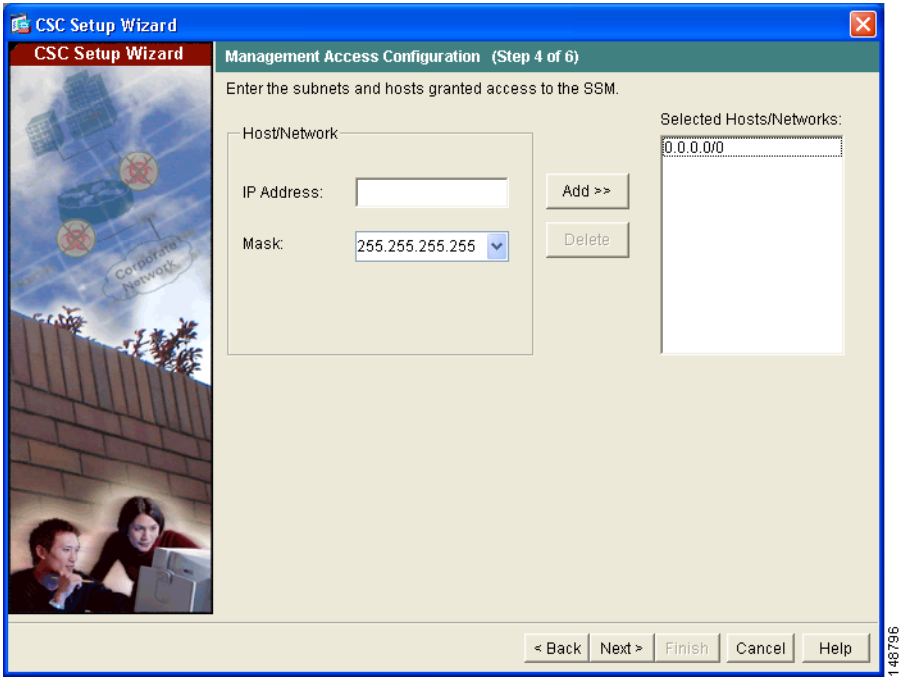
- 通知に使用する管理者の電子メール アドレスと、電子メール サーバの IP アドレスおよびポート



ステップ 8　**Next** をクリックします。

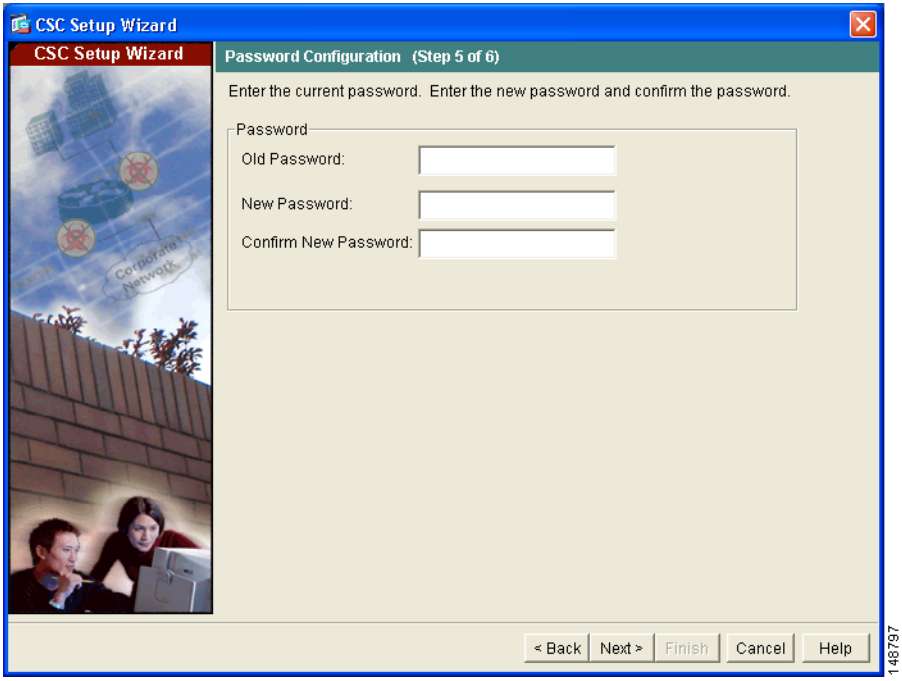
ステップ 9　CSC Setup Wizard の Step 4 で、CSC SSM への管理アクセスが必要な各サブネットおよびホストの、IP アドレスとマスクを入力します。

デフォルトでは、すべてのネットワークが CSC SSM に管理アクセスできます。セキュリティ上の理由により、特定のサブネットまたは管理ホストにアクセスを制限することが推奨されます。



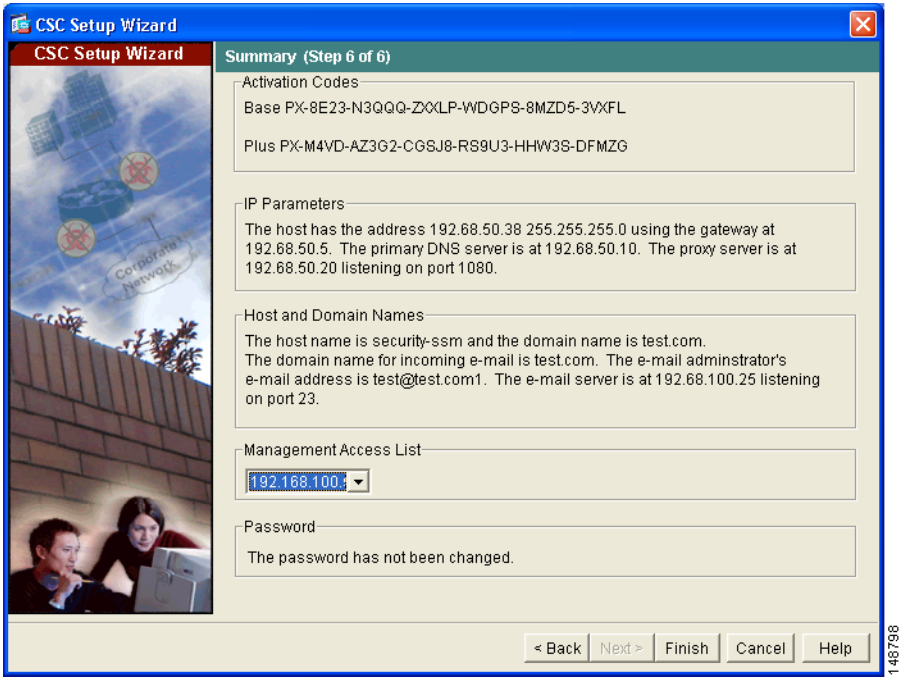
ステップ 10　**Next** をクリックします。

ステップ 11　CSC Setup Wizard の Step 5 で、管理アクセス用の新しいパスワードを入力します。Old Password フィールドに、工場出荷時のデフォルト パスワード「cisco」を入力します。



ステップ 12　**Next** をクリックします。

ステップ 13　CSC Setup Wizard の Step 6 で、CSC SSM に入力したコンフィギュレーション設定値を確認します。



これらの設定が正しいことを確認したら、Finish をクリックします。

ASDM に、CSC デバイスがアクティブになったことを示すメッセージが表示されます。

コンテント スキャン用の CSC SSM へのトラフィック誘導

適応型セキュリティ アプライアンスは、ファイアウォール ポリシーを適用した後、出力インターフェイスから出る前に、パケットを CSC SSM に誘導します。たとえば、アクセスリストによってブロックされたパケットは、CSC SSM に転送されません。

適応型セキュリティ アプライアンスで、CSC SSM に誘導するトラフィックを指定するサービス ポリシーを設定します。CSC SSM は、HTTP、POP3、FTP、および SMTP プロトコルの既知のポートに送信された、これらのトラフィックをスキャンできます。

初期設定プロセスを簡素化するために、この手順では、サポートされるプロトコルのすべてのトラフィック（着信および発信）を CSC SSM に誘導する、グローバル サービス ポリシーを作成します。適応型セキュリティ アプライアンスを通過するすべてのトラフィックをスキャンすると、適応型セキュリティ アプライアンス、および CSC SSM のパフォーマンスが低下する可能性があるため、このセキュリティ ポリシーは後で変更できます。たとえば、通常、内部ネットワークからの着信トラフィックは、信頼される発信元から着信しているため、すべてをスキャンする必要はありません。CSC SSM が信頼されない発信元からのトラフィックだけをスキャンするようにサービス ポリシーを調整することによって、セキュリティの目的を達成しながら、適応型セキュリティ アプライアンス、および CSC SSM の最大のパフォーマンスが得られます。

スキャンするトラフィックを特定するグローバル サービス ポリシーを作成するには、次の手順を実行します。

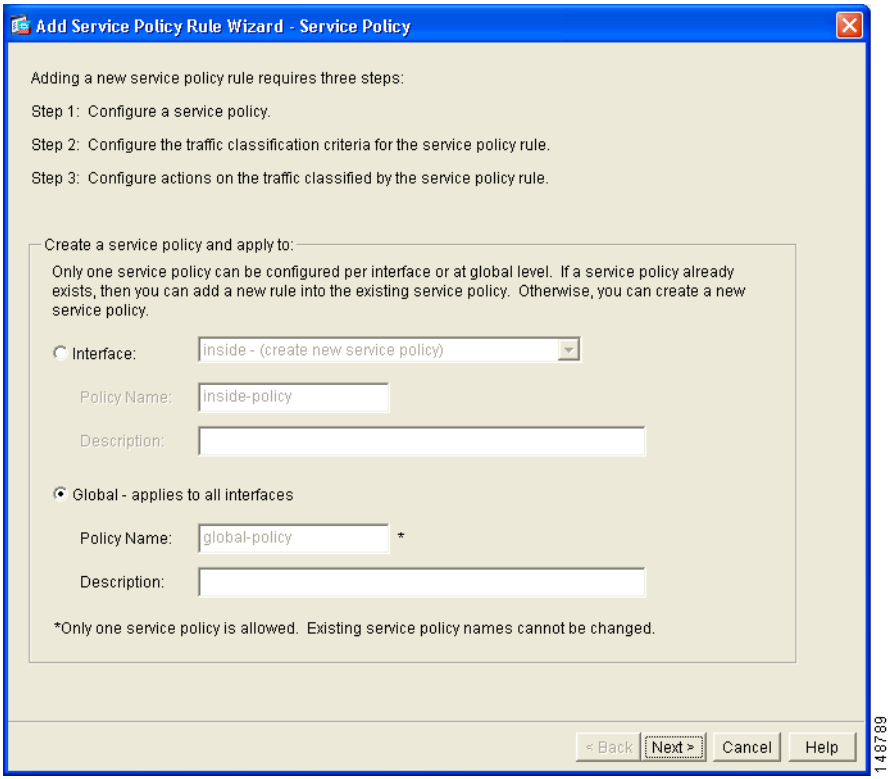
ステップ 1　ASDM のメイン ウィンドウで、**Configuration** タブをクリックします。

ステップ 2　**Security Policies** をクリックし、**Service Policy Rules** オプション ボタンをクリックします。

ステップ 3　**Add** をクリックします。

Add Service Policy Rule が表示されます。

ステップ 4　Service Policy ページで、**Global - applies to all interfaces** オプション ボタンをクリックします。

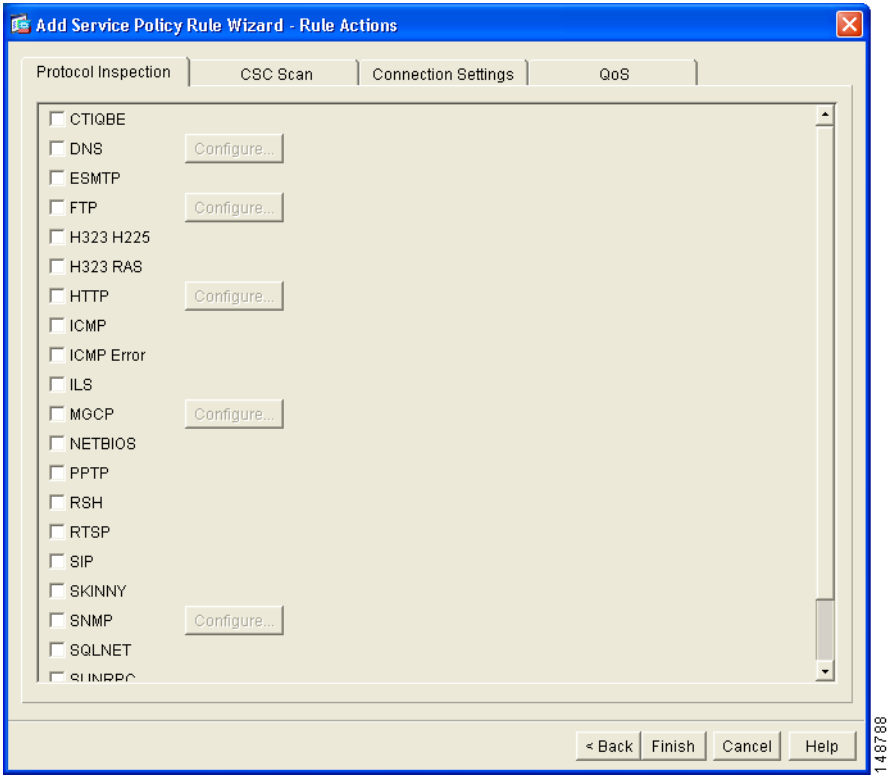


ステップ 5　**Next** をクリックします。Traffic Classification Criteria ページが表示されます。

ステップ 6　Traffic Classification Criteria ページで、**User class-default as the traffic class** オプション ボタンをクリックします。

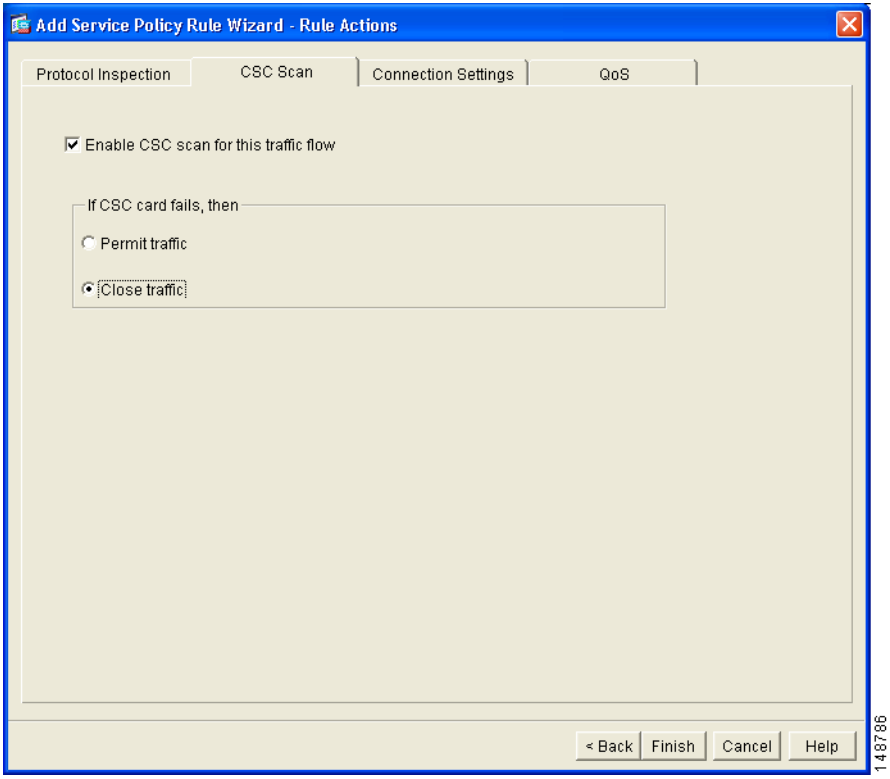
ステップ 7　**Next** をクリックします。Add Service Policy Rule Wizard - Rule Actions ページが表示されます。

ステップ 8　Service Policy Rule Wizard で、**CSC Scan** タブをクリックします。



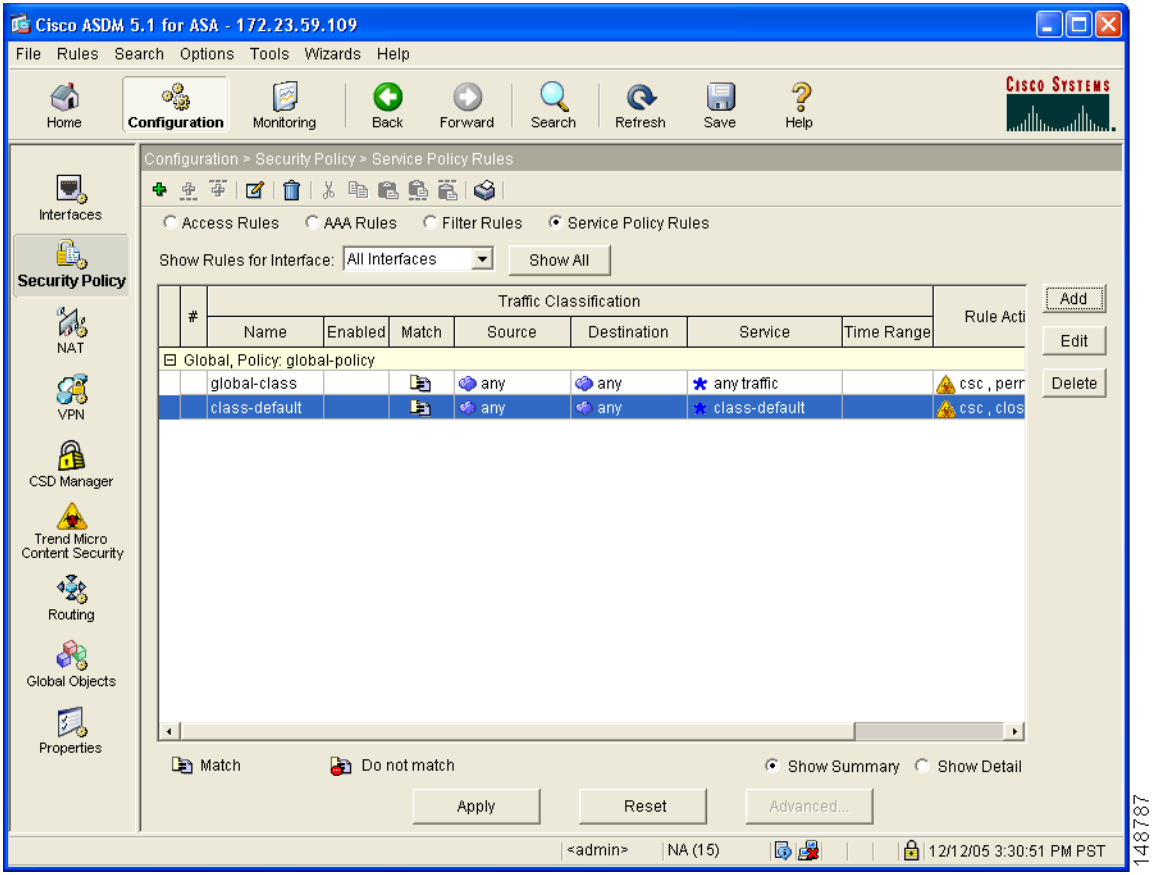
ステップ 9　CSC Scan タブ ページで、**Enable CSC scan for this traffic flow** チェックボックスをオンにします。

If CSC card fails, then 領域で、CSC SSM を使用できないときに選択されたトラフィックを、適応型セキュリティ アプライアンスが許可するか拒否するかを選択します。



ステップ 10　**Finish** をクリックします。

新しいサービス ポリシーが Service Policy Rules ペインに表示されます。



ステップ 11　**Apply** をクリックします。

デフォルトでは、CSC SSM は、購入したライセンスでイネーブルになっているコンテント セキュリティ スキャン（アンチウイルス、アンチスパム、アンチフィッシング、コンテント フィルタリングなど）を実行するように設定されています。また、Trend Micro のアップデート サーバから、定期的にアップデートを取得するように設定されています。

購入したライセンスに含まれている場合、URL ブロッキングおよび URL フィルタリング用のカスタム設定や、電子メールおよび FTP のパラメータを作成できます。詳細については、『*Cisco Content Security and Control SSM Administrator Guide*』を参照してください。

次の手順

これで、Trend Micro Interscan for Cisco CSC SSM ソフトウェアを設定する準備ができました。次のマニュアルを参照して、実装に合わせて適応型セキュリティ アプライアンスを設定します。

作業内容	参照先
CSC SSM ソフトウェアの設定（高度なセキュリティ ポリシーなど）	*Cisco Content Security and Control SSM Administrator Guide*
ASDM による追加の CSC SSM 機能の設定（コンテント フィルタリングなど）	ASDM のオンライン ヘルプ（**Configuration** または **Monitoring** タブをクリックし、**Trend Micro Content Security** タブをクリック）
より効率的なサービス ポリシーの作成によるパフォーマンスの最適化	『*Cisco Security Appliance Command Line Configuration Guide*』の「Managing AIP SSM and CSC SSM」

CSC SSM ソフトウェアを設定した後、次の追加の手順について、実行する必要があるかどうかを検討してください。

作業内容	参照先
設定の調整およびオプション機能と高度な機能の設定	*Cisco Security Appliance Command Line Configuration Guide*
日常のオペレーションの学習	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*
ハードウェア メンテナンスおよびトラブルシューティング情報の確認	*Cisco ASA 5500 Series Hardware Installation Guide*

適応型セキュリティ アプライアンスは、複数のアプリケーション用に設定できます。次の項で、その他の一般的なアプリケーション用に適応型セキュリティ アプライアンスを設定する手順を説明します。

作業内容	参照先
リモートアクセス VPN の設定	第 7 章「シナリオ : リモートアクセス VPN の設定」
サイトツーサイト VPN の設定	第 8 章「シナリオ : サイトツーサイト VPN の設定」
DMZ Web サーバの保護の設定	第 6 章「シナリオ : DMZ の設定」