CHAPTER 2

ACE へのリモート アクセスのイネーブル化

この章では、Secure Shell（SSH; セキュア シェル）または Telnet プロトコルを使用してリモート接続を確立し、Cisco 4700 Series Application Control Engine（ACE）アプライアンス へのリモート アクセスを設定する方法について説明します。SSH からユーザ コンテキストに直接アクセスできるように、ACE を設定する方法についても説明します。また、ホストからの ICMP メッセージを受信するように ACE を設定する方法についても説明します。

この章の内容は、次のとおりです。

（注） ACE 前面のコンソール ポートに接続された専用端末を使用して直接接続を行い、端末表示属性を設定し、コンソールまたは仮想端末接続を使用して ACE にアクセスできるように端末回線を設定する方法については、第 1 章 「ACE の設定」を参照してください。

ガイドラインと制約事項

ここでは、リモート アクセス機能に関するガイドラインと制約事項について説明します。内容は次のとおりです。

Telnet 管理セッション

ACE は、管理コンテキストの同時 Telnet 管理セッションを最大で 16、各ユーザ コンテキストの同時 Telnet 管理セッションを最大で 4 つサポートします。ACE は、合計で最大 256 の同時 Telnet セッションをサポートします。

SSH 管理セッション

ACE は、管理コンテキストの同時 SSH 管理セッションを最大で 16、各ユーザ コンテキストの同時 SSH 管理セッションを最大で 4 つサポートします。ACE は、合計で最大 256 の同時 SSH セッションをサポートします。

ACE は、SSH セッションの確立とメッセージの暗号化/復号化に必要な DSA キーと RSA キーを生成できます。これらのキーはペアで生成されます（公開キーと秘密キーが 1 つずつ）。グローバル管理者は、管理コンテキストでキー生成を実行します。ACE に関連付けられたすべてのコンテキストで、共通のキーが共有されます。ホスト/キー ペアは 1 つのみ存在します。

ICMP メッセージ

ACE はデフォルトで、ACE インターフェイスでの ICMP メッセージの受信、または ACE インターフェイスを介した ICMP メッセージの送信を許可していません。ICMP はネットワーク接続をテストするための重要なツールですが、ネットワーク ハッカーが ICMP を使用して ACE またはネットワークを攻撃することもできます。初期テスト中は ICMP を許可し、通常操作中は禁止することを推奨します。

デフォルト設定

表 2-1 に、ACE のリモート アクセス機能のデフォルト設定を示します。

表 2-1　デフォルト リモート アクセス パラメータ

パラメータ	デフォルト
コンテキストごとの同時 Telnet 管理セッション数	• 管理コンテキスト：16 • ユーザ コンテキスト：4（それぞれ）
コンテキストごとの同時 SSH 管理セッション数	• 管理コンテキスト：16 • ユーザ コンテキスト：4（それぞれ）
ACE インターフェイスで ICMP メッセージを受信できるかどうか、または、このインターフェイスを介して ICMP メッセージを送信できるかどうか	無効
http、https、icmp、kalap-udp、snmp、ssh、telnet、および xml-https の **match protocol** コマンド プロトコルのステータス	無効

ACE へのリモート アクセスのイネーブル化

ここでは、ACE へのリモート アクセスのイネーブル化に関連したタスクについて説明します。内容は次のとおりです。

ACE へのリモート アクセスをイネーブルにするためのタスク フロー

ACE へのリモート アクセスをイネーブルにするには、次の手順を実行します。

ステップ 1　複数のコンテキストで動作する場合は、CLI プロンプトを観察して、適切なコンテキストで動作しているかどうかを確認してください。必要に応じて、適切なコンテキストに直接ログインするか、または切り替えてください。

```
host1/Admin# changeto C1
host1/C1#
```

これ以降、この表の例では、特に指定しないかぎり管理コンテキストを使用します。コンテキスト作成の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*』を参照してください。

ステップ 2　設定モードに入ります。

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)#
```

ステップ 3　ネットワーク管理プロトコル（SSH または Telnet）およびクライアント送信元 IP アドレスに基づいて、ACE でネットワーク管理トラフィックを受信できるように許可するクラス マップを作成します。

```
host1/Admin(config)# class-map type management match-all SSH-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol ssh source-address 172.16.10.0
255.255.255.254
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)#
host1/Admin(config)# class-map type management match-all TELNET-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol telnet source-address 172.16.10.0
255.255.255.254
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)#
```

ステップ 4　SSH および Telnet 管理プロトコル分類をアクティブにするポリシー マップを設定します。

```
host1/Admin(config)# policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
host1/Admin(config-pmap-mgmt)# class SSH-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# class TELNET-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
```

```
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# exit
host1/Admin(config)#
```

ステップ 5　単一 VLAN インターフェイスにトラフィック ポリシーを接続するか、または同じコンテキスト内のすべての VLAN インターフェイスにグローバルに接続します。たとえば、特定のインターフェイス VLAN を指定し、リモート管理ポリシー マップを適用するには、次のように入力します。

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 172.16.1.100 255.255.0.0
host1/Admin(config-if)# service-policy input REMOTE_MGMT_ALLOW_POLICY
host1/Admin(config-if)# exit
```

ステップ 6　（オプション）コンテキストごとに許可する Telnet セッションの最大数を設定します。

```
host1/Admin(config)# telnet maxsessions 3
```

ステップ 7　（オプション）コンテキストごとに許可する SSH セッションの最大数を設定します。

```
host1/Admin(config)# ssh maxsessions 3
```

ステップ 8　ユーザにグローバル管理権限がある場合は、**ssh key** コマンドを使用して、SSH サーバで使用される SSH 秘密キーと対応する公開キーを生成します。ホスト/キー ペアは 1 つだけです。たとえば、管理コンテキストで RSA1 キー ペアを生成するには、次のように入力します。

```
host1/Admin(config)# ssh key rsa1 1024
generating rsa1 key
.....
generated rsa1 key
```

ステップ 9　（オプション）フラッシュ メモリに設定変更を保存します。

```
host1/Admin(config)# exit
host1/Admin# copy running-config startup-config
```

ステップ 10　（オプション）EXEC モードで次のいずれかのコマンドを使用して、アクティブ コンテキストのアクティブ SSH または Telnet セッションを終了します。

- **clear ssh** {*session_id* | **hosts**}
- **clear telnet** *session_id*

```
host1/Admin# clear ssh 345
```

リモート ネットワーク管理トラフィック サービスの設定

ここでは、ACE へのリモート ネットワーク アクセス用のクラス マップ、ポリシー マップ、およびサービス ポリシーの作成方法について簡単に説明します。ACE へのリモート ネットワーク管理アクセスを設定するうえで、各機能が果たす役割を簡単に説明します。

- クラス マップ：リモート ネットワーク トラフィックの一致基準を提供します。トラフィックを許可する場合の基準は、次のとおりです。
  - リモート アクセス ネットワーク管理プロトコル（SSH、Telnet、または ICMP）
  - クライアント送信元 IP アドレス
- ポリシー マップ：クラス マップで示された基準と一致するトラフィック分類に関して、リモート ネットワーク管理アクセスをイネーブルにします。
- サービス ポリシー：ポリシー マップをアクティブにして、インターフェイスにトラフィック ポリシーを接続するか、またはすべてのインターフェイス上でグローバルに接続します。

ACE への Telnet および SSH リモート アクセス セッションは、コンテキスト単位で確立されます。ユーザとコンテキストの作成方法については、『*Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*』を参照してください。

ここでは、次の内容について説明します。

- リモート管理クラス マップの作成と設定
- レイヤ 3 およびレイヤ 4 リモート アクセス ポリシー マップの作成
- 同じコンテキスト内のすべての VLAN インターフェイスへのサービス ポリシーのグローバルな適用
- 特定の VLAN インターフェイスへのサービス ポリシーの適用

リモート管理クラス マップの作成と設定

ここでは、ACE で受信されるリモート ネットワーク管理トラフィックを分類するためのレイヤ 3 およびレイヤ 4 クラス マップの作成方法について説明します。このクラス マップを使用すると、ACE で受信可能な着信 IP プロトコルだけでなく、クライアント送信元 IP アドレスとサブネット マスクを一致基準として識別することによって、ACE でネットワーク管理トラフィックを受信できるようになります。許可するネットワーク トラフィックを定義して、SSH、Telnet、ICMP などのプロトコルのセキュリティを管理します。また、クラス マップ内に複数の一致基準が存在する場合の ACE による複数の match 文処理の評価方法を定義します。

クラス マップによって、ACE で受信可能なリモート ネットワーク アクセス管理プロトコルが指定されます。対応するポリシー マップを設定して、指定された管理プロトコルに ACE へのアクセスを許可します。ネットワーク管理アクセス トラフィック分類の一部として、クライアント送信元ホストの IP アドレスおよびサブネット マスクも一致条件として指定するか、またはあらゆるクライアント送信元アドレスを管理トラフィック分類で許可するように ACE に指示します。

詳細手順

	コマンド	目的
ステップ 1	**config** **例：** host1/Admin# config host1/Admin(config)#	グローバル コンフィギュレーション モードに入ります。
ステップ 2	**class-map type management** [**match-all** | **match-any**] *map_name* **例：** host1/Admin(config)# class-map type management match-all SSH-TELNET_ALLOW_CLASS host1/Admin(config-cmap-mgmt)#	ACE で受信されるリモート ネットワーク管理トラフィックを分類するためのレイヤ 3 およびレイヤ 4 クラス マップを作成します。 キーワード、引数、およびオプションは次のとおりです。 • **match-all | match-any**：（オプション）クラス マップ内に一致基準が複数存在する場合に、ACE でのレイヤ 3 およびレイヤ 4 ネットワーク管理トラフィックの評価方法を定義します。クラス マップは、match コマンドが次の条件の 1 つを満たした場合に、一致と見なされます。 – **match-all**：（デフォルト）クラス マップで指定されたすべての一致基準が、クラス マップ内のネットワーク トラフィック クラス、通常は、同じタイプのコマンドと一致するように設定されます。 – **match-any**：クラス マップで指定された一致基準のいずれかが、クラス マップ内のネットワーク トラフィック クラス、通常は、別のタイプのコマンドと一致するように設定されます。 • *map_name*：クラス マップに割り当てる名前を指定します。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。 CLI がクラス マップ管理設定モードに入ります。
	no class-map type management [**match-all** | **match-any**] *map_name* **例：** host1/Admin(config)# no class-map type management match-all SSH-TELNET_ALLOW_CLASS	（オプション）ACE からレイヤ 3 およびレイヤ 4 ネットワーク管理クラス マップを削除します。

	コマンド	目的
ステップ 3	[line_number] **match protocol** {**http** | **https** | **icmp** | **kalap-udp** | **snmp** | **ssh** | **telnet**| **xml-https**} {**any** | **source-address** *ip_address mask*} **例：** ACE_1/Admin(config-cmap-mgmt)# match protocol ssh source-address 172.16.10.0 255.255.255.254 ACE_1/Admin(config-cmap-mgmt)# match protocol telnet source-address 172.16.10.0 255.255.255.254	ACE で受信されるリモート ネットワーク管理トラフィックを分類します。1 つ以上の **match protocol** コマンドを追加して、クラス マップ用の一致基準を設定します。 キーワードと引数は次のとおりです。 • *line_number*：（オプション）個別の **match** コマンドの編集または削除を支援します。行番号として 2 ～ 255 の整数を入力します。**no *line_number*** を入力すると、行全体を入力しなくても、長い **match** コマンドを削除できます。行番号は、**match** 文のプライオリティまたは順番を示すものではありません。 • **http**：Hypertext Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）を指定します。HTTP 管理プロトコルの設定については、第 8 章 「XML インターフェイスの設定」を参照してください。 • **https**：ポート 443 を使用している ACE 上でデバイス マネージャ GUI と接続するためのセキュアな（SSL）HTTP を指定します。 • **icmp**：ACE への Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）メッセージを指定します。ICMP 管理プロトコルの設定については、「ACE への ICMP メッセージのイネーブル化」を参照してください。 • **kalap-udp**：KAL-AP over UDP を使用した管理アクセスを指定します。KAL-AP 管理アクセスの設定については、『*Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*』の Configuring Health Monitoring を参照してください。 • **snmp**：Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を指定します。SNMP 管理プロトコルの設定については、第 7 章 「簡易ネットワーク管理プロトコル（SNMP）の設定」を参照してください。 • **ssh**：ACE への SSH リモート接続を指定します。ACE は、SSH バージョン 1 で提供される SSH リモート シェル機能と DES 暗号および 3DES 暗号をサポートしています。SSH 管理プロトコルの設定については、「SSH 管理セッション パラメータの設定」を参照してください。 **（注）** SSH v1.*x* と v2 は全く別のプロトコルであり、互換性はありません。ACE にアクセスする場合は、必ず SSH v1.*x* クライアントを使用してください。

	コマンド	目的
	match protocol (continued)	• **telnet**：ACE への Telnet リモート接続を指定します。Telnet 管理プロトコルの設定については、「最大 Telnet 管理セッション数の設定」を参照してください。 • **xml-https**：HTTPS を転送プロトコルとして指定して、ACE と Network Management System（NMS; ネットワーク管理システム）間で XML ドキュメントの送受信を行います。通信は、ポート 10443 を使用して行われます。XML を利用する場合の HTTPS 管理プロトコルの使用については、第 8 章 「XML インターフェイスの設定」を参照してください。 **（注）** レイヤ 3 およびレイヤ 4 ネットワーク管理クラス マップでは、**https** と **xml-https** の両方をイネーブルにできます。 • **any**：管理トラフィック分類用の任意のクライアント送信元アドレスを指定します。 • **source-address**：ネットワーク トラフィック一致条件として、クライアント送信元ホストの IP アドレスとサブネット マスクを指定します。分類の一部として、ACE は暗黙的に、ポリシー マップが適用されるインターフェイスから宛先 IP アドレスを取得します。 • *ip_address*：クライアントの送信元 IP アドレス。 • *mask*：ドット区切りの 10 進表記のクライアントのサブネット マスク。
	no match protocol {**http** | **https** | **icmp** | **kalap-udp** | **snmp** | **ssh** | **telnet**| **xml-https**} {**any** | **source-address** *ip_address mask*} **例**： ACE_1/Admin(config-cmap-mgmt)# no match protocol ssh source-address 192.168.10.1 255.255.255.0	（オプション）クラス マップから指定されたネットワーク管理プロトコル一致条件を選択解除します。
ステップ 4	**description** *text* **例**： host1/Admin(config-cmap-mgmt)# description Allow Telnet access to the ACE	レイヤ 3 およびレイヤ 4 リモート管理クラス マップの概要を提供します。
	no description *text* **例**： host1/Admin(config-cmap-mgmt)# no description	（オプション）クラス マップから説明を削除します。
ステップ 5	**do copy running-config startup-config** **例**： ACE_1/Admin(config-cmap-mgmt))# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

レイヤ 3 およびレイヤ 4 リモート アクセス ポリシー マップの作成

ここでは、ACE で受信されるネットワーク管理トラフィックを定義するためのアクションを使用して、レイヤ 3 およびレイヤ 4 トラフィック分類用のレイヤ 3 およびレイヤ 4 ポリシー マップを作成する方法について説明します。レイヤ 3 およびレイヤ 4 ネットワーク トラフィック ポリシーを設定するための一般的な手順は次のとおりです。

- ACE で受信される IP 管理トラフィックに適用されるさまざまなアクションを定義するレイヤ 3 およびレイヤ 4 ポリシー マップを設定します。ACE では、ポリシー マップと最初に一致した分類に適合するトラフィックに対してのみ、指定されたアクションが実行されます。ACE は、それ以上のアクションは実行しません。
- オプションで、レイヤ 3 およびレイヤ 4 リモート管理ポリシー マップの概要を提供します。
- ネットワーク トラフィックとトラフィック ポリシーを関連付けるために **class-map** コマンドを使用して作成したレイヤ 3 およびレイヤ 4 トラフィック クラスを指定します。
- レイヤ 3 およびレイヤ 4 クラス マップで指定されたネットワーク管理トラフィックを ACE で受信または拒否できるようにします。

詳細手順

	コマンド	目的

ステップ 1	**config**
	
	例：
	`host1/Admin# config`
	`host1/Admin(config)#`
		グローバル コンフィギュレーション モードに入ります。

ステップ 2	`policy-map type management first-match` *map_name*
	
	例：
	`host1/Admin(config)# policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY`
	`host1/Admin(config-pmap-mgmt)#`
		ACE で受信される IP 管理トラフィックに適用されるさまざまなアクションを定義するレイヤ 3 およびレイヤ 4 ポリシー マップを設定します。
		
		map_name 引数は、レイヤ 3 およびレイヤ 4 ネットワーク管理ポリシー マップに割り当てる名前を指定します。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。
		
		このコマンドを使用するときは、ポリシー マップ管理コンフィギュレーション モードにアクセスします。

	`no policy-map type management first-match` *map_name* **例：** `host1/Admin(config)# no policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY`	（オプション）ACE からポリシー マップを削除します。
ステップ 3	**description** *text* **例：** `host1/Admin(config-pmap-mgmt)# description Allow Telnet access to the ACE`	レイヤ 3 およびレイヤ 4 リモート管理ポリシー マップの概要を提供します。 *text* 引数は、提供する説明を指定します。最大 240 文字の英数字からなる、引用符で囲まれていないテキスト文字列を入力します。
	no description **例：** `host1/Admin(config-pmap-mgmt)# no description`	（オプション）ポリシー マップから説明を削除します。

	コマンド	目的
ステップ 4	**class** {*name1* [**insert-before** *name2*] | **class-default**} **例：** host1/Admin(config-pmap-mgmt)# class L4_REMOTE_ACCESS_CLASS host1/Admin(config-pmap-mgmt-c)#	ネットワーク トラフィックとトラフィック ポリシーを関連付けるために **class-map** コマンドを使用して作成したレイヤ 3 およびレイヤ 4 トラフィック クラスを指定します。 引数、キーワード、およびオプションは次のとおりです。 • *name1*：トラフィックとトラフィック ポリシーを関連付けるために **class-map** コマンドを使用して設定された、定義済みのレイヤ 3 およびレイヤ 4 トラフィック クラスの名前。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。 • **insert-before** *name2*：（オプション）ポリシー マップ コンフィギュレーションの *name2* 引数で指定された、既存のクラス マップまたはインライン一致条件の前に、現在のクラス マップを配置します。ACE では、コンフィギュレーションの一部として順序の並べ替えを保存しません。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。 • **class-default**：レイヤ 3 およびレイヤ 4 トラフィック ポリシー用に、class-default クラス マップを指定します。これは、ACE が作成する予約済みのクラス マップです。このクラスの削除または変更はできません。指定されたクラス マップの他の一致条件と一致しなかったすべてのネットワーク トラフィックは、デフォルトのトラフィック クラスに割り当てられます。指定された分類がいずれも一致しなかった場合、ACE は **class class-default** コマンドで指定されたアクションと一致させます。class-default クラス マップには、暗黙の **match any** 文が含まれており、任意のトラフィック分類との一致に使用されます。class-default クラス マップには、すべてのトラフィックと一致する暗黙の **match any** 文が含まれています。 このコマンドを使用すると、ポリシー マップ管理クラス コンフィギュレーション モードが開始します。
	no class {*name1* [**insert-before** *name2*] | **class-default**} **例：** host1/Admin(config-pmap-mgmt)# no class L4_REMOTE_ACCESS_CLASS	（オプション）レイヤ 3 およびレイヤ 4 ポリシー マップからクラス マップを削除します。

	コマンド	目的
ステップ 5	**permit** | **deny** **例：** host1/Admin(config-pmap-mgmt-c)# permit	レイヤ 3 およびレイヤ 4 クラス マップで指定されたネットワーク管理トラフィックを次のように ACE で受信または拒否できるようにします。 • クラス マップで指定されたリモート管理プロトコルを ACE で受信できるようにするには、ポリシー マップ クラス コンフィギュレーション モードで **permit** コマンドを使用します。 • クラス マップで指定されたリモート管理プロトコルを ACE で受信できないようにするには、ポリシー マップ クラス コンフィギュレーション モードで **deny** コマンドを使用します。
ステップ 6	**do copy running-config startup-config** **例：** host1/Admin(config-pmap-mgmt-c)# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

下の例は、SSH、Telnet、および ICMP 接続を ACE で受信できるようにするレイヤ 3 およびレイヤ 4 リモート ネットワーク トラフィック管理ポリシー マップの作成方法を示しています。

```
host1/Admin(config)# policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
host1/Admin(config-pmap-mgmt)# class SSH-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# class TELNET-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# class ICMP-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
```

下の例は、ACE で ICMP 接続を制限するポリシー マップの作成方法を示しています。

```
host1/Admin(config)# policy-map type management first-action ICMP_RESTRICT_POLICY
host1/Admin(config-pmap-mgmt)# class ICMP-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# deny
```

同じコンテキスト内のすべての VLAN インターフェイスへのサービス ポリシーのグローバルな適用

ここでは、同じコンテキスト内のすべての VLAN インターフェイスに作成済みのポリシー マップをグローバルに適用する方法について説明します。

サービス ポリシーの適用時は次のガイドラインに注意してください。

- コンテキストでグローバルに適用されるポリシー マップは、コンテキスト内に存在するすべてのインターフェイスに内部的に適用されます。
- インターフェイス上でアクティブになったポリシーは、重複する分類およびアクションに関して、指定されているあらゆるグローバル ポリシーを上書きします。

次のいずれかの方法を使用して、VLAN からトラフィック ポリシー マップを削除できます。

- サービス ポリシーを最後に適用した VLAN インターフェイスから個別に
- 同じコンテキストのすべての VLAN インターフェイスからグローバルに

次にトラフィック ポリシーが特定の VLAN インターフェイスに付加されるか、同じコンテキスト内のすべての VLAN インターフェイスにグローバルに付加されたときに、ACE では、関連するサービス ポリシー統計情報が自動的にリセットされ、サービス ポリシー統計情報の新しい開始点が設定されます。

（注）　特定の VLAN インターフェイスにポリシー マップを適用するには、「特定の VLAN インターフェイスへのサービス ポリシーの適用」を参照してください。

制約事項

ACE では、特定の機能タイプのポリシーのみを特定のインターフェイス上で入力方向にのみアクティブにすることができます。

詳細手順

	コマンド	目的
ステップ 1	**config** **例：** host1/Admin# config host1/Admin(config)#	グローバル コンフィギュレーション モードに入ります。
ステップ 2	service-policy input *policy_name* **例：** host1/Admin(config)# service-policy input REMOTE_MGMT_ALLOW_POLICY	1 つのコンテキストに関連付けられたすべての VLAN にリモート アクセス ポリシー マップをグローバルに適用します。 *policy_name* 引数は、作成済みの **policy-map** コマンドで設定された、定義済みポリシー マップの名前です。名前は 40 文字以内の英数字にすることができます。
	no service-policy input *policy_name* **例：** host1/Admin(config)# no service-policy input REMOTE_MGMT_ALLOW_POLICY	（オプション）1 つのコンテキストに関連付けられたすべての VLAN からリモート アクセス トラフィック ポリシーをグローバルに削除します。
ステップ 3	**do copy running-config startup-config** **例：** host1/Admin(config)# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

	コマンド	目的
ステップ 4	**do show service-policy** [*policy_name* [**detail**]] **例：** host1/Admin(config)# do show service-policy REMOTE_MGMT_ALLOW_POLICY	（オプション）すべてのポリシー マップまたは特定のレイヤ 3 およびレイヤ 4 リモート ネットワーク トラフィック管理ポリシー マップに関するサービス ポリシー統計情報を表示します。 キーワード、オプション、および引数は次のとおりです。 • *policy_name*：（オプション）最大 64 文字の英数字からなる引用符で囲まれていない文字列として現在使用されている（インターフェイスに適用されている）既存のポリシー マップ。既存のポリシー マップの名前を入力しなかった場合は、ACE にすべてのポリシー マップに関する統計情報が表示されます。 • **detail**：（オプション）より詳細なポリシー マップの統計情報とステータス情報を一覧表示します。 **（注）** ACE は、該当する接続の終了後、**show service-policy** コマンドによって表示されるカウンタをアップデートします。
ステップ 5	**do clear service-policy** *policy_name* **例：** host1/Admin(config)# do clear service-policy REMOTE_MGMT_ALLOW_POLICY	（オプション）ポリシー マップに関するサービス ポリシー統計情報をクリアします。 *policy_name* 引数には、現在使用されている（インターフェイスに適用されている）既存のポリシー マップの ID を入力します。

特定の VLAN インターフェイスへのサービス ポリシーの適用

ここでは、特定の VLAN インターフェイスに作成済みのポリシー マップを適用する方法について説明します。インターフェイス上でアクティブになったポリシーは、重複する分類およびアクションに関して、指定されているあらゆるグローバル ポリシーを上書きします。

次のいずれかの方法を使用して、VLAN からトラフィック ポリシー マップを削除できます。

- サービス ポリシーを最後に適用した VLAN インターフェイスから個別に
- 同じコンテキスト内のすべての VLAN インターフェイスからグローバルに（「同じコンテキスト内のすべての VLAN インターフェイスへのサービス ポリシーのグローバルな適用」を参照）

次にトラフィック ポリシーが特定の VLAN インターフェイスに付加されるか、同じコンテキスト内のすべての VLAN インターフェイスにグローバルに付加されたときに、ACE では、関連するサービス ポリシー統計情報が自動的にリセットされ、サービス ポリシー統計情報の新しい開始点が設定されます。

（注） ポリシー マップを同じコンテキスト内のすべての VLAN インターフェイスにグローバルに適用するには、「同じコンテキスト内のすべての VLAN インターフェイスへのサービス ポリシーのグローバルな適用」を参照してください。

制約事項

ACE では、特定の機能タイプのポリシーのみを特定のインターフェイス上で入力方向にのみアクティブにすることができます。

詳細手順

	コマンド	目的
ステップ 1	**config** **例：** host1/Admin# config host1/Admin(config)#	グローバル コンフィギュレーション モードに入ります。
ステップ 2	interface vlan *number* **例：** host1/Admin(config)# interface vlan 50 host1/Admin(config-if)#	（オプション）リモート アクセス ポリシー マップを適用する VLAN を指定します。 *number* 引数は、VLAN を指定します。 このコマンドによって、インターフェイス コンフィギュレーション モードに入ります。
ステップ 3	service-policy input *policy_name* **例：** host1/Admin(config-if)# service-policy input REMOTE_MGMT_ALLOW_POLICY	リモート アクセス ポリシー マップを指定された VLAN にのみアタッチします。 *policy_name* 引数は、ポリシー マップ名を指定します。 1 つのコンテキストに関連付けられたすべての VLAN にグローバルにポリシー マップを適用するには、「同じコンテキスト内のすべての VLAN インターフェイスへのサービス ポリシーのグローバルな適用」を参照してください。
	no service-policy input *policy_name* **例：** host1/Admin(config-if)# no service-policy input REMOTE_MGMT_ALLOW_POLICY	（オプション）VLAN からリモート アクセス トラフィック ポリシーをデタッチします。
ステップ 4	**do copy running-config startup-config** **例：** host1/Admin(config-if)# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

	コマンド	目的
ステップ 5	**do show service-policy** [*policy_name* [**detail**]] **例：** host1/Admin(config-if)# do show service-policy REMOTE_MGMT_ALLOW_POLICY	（オプション）すべてのポリシー マップまたは特定のレイヤ 3 およびレイヤ 4 リモート ネットワーク トラフィック管理ポリシー マップに関するサービス ポリシー統計情報を表示します。 キーワード、オプション、および引数は次のとおりです。 • *policy_name*：（オプション）最大 64 文字の英数字からなる引用符で囲まれていない文字列として現在使用されている（インターフェイスに適用されている）既存のポリシー マップ。既存のポリシー マップの名前を入力しなかった場合は、ACE にすべてのポリシー マップに関する統計情報が表示されます。 • **detail**：（オプション）より詳細なポリシー マップの統計情報とステータス情報を一覧表示します。 **（注）** ACE は、該当する接続の終了後、**show service-policy** コマンドによって表示されるカウンタをアップデートします。
ステップ 6	**do clear service-policy** *policy_name* **例：** host1/Admin(config-if)# do clear service-policy REMOTE_MGMT_ALLOW_POLICY	（オプション）ポリシー マップに関するサービス ポリシー統計情報をクリアします。 *policy_name* 引数には、現在使用されている（インターフェイスに適用されている）既存のポリシー マップの ID を入力します。

例

下の例は、インターフェイス VLAN を指定して、リモート アクセス ポリシー マップを VLAN に適用する方法を示しています。

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 172.16.1.100 255.255.0.0
host1/Admin(config-if)# service-policy input REMOTE_MGMT_ALLOW_POLICY
```

下の例は、REMOTE_MGMT_ALLOW_POLICY ポリシー マップに関するサービス ポリシー統計情報を表示する方法を示しています。

```
host1/Admin# show service-policy REMOTE_MGMT_ALLOW_POLICY
Status     : ACTIVE
Description: Allow mgmt protocols
----------------------------------------
Context Global Policy:
  service-policy: REMOTE_MGMT_ALLOW_POLICY
```

最大 Telnet 管理セッション数の設定

ここでは、コンテキストごとに許可する最大 Telnet セッション数の制御方法について説明します。ACE の Telnet リモート アクセス セッションは、コンテキストごとに確立されます。コンテキストを作成し、インターフェイスおよび IP アドレスを割り当てて、ACE にログインするには、Telnet を使用して、この IP アドレスに接続します。この機能を使用すると、ACE にアクセスする場合に、特定のコンテキストを指定できます。ユーザとコンテキストの作成方法については、『*Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*』を参照してください。

制約事項

ACE は、合計で最大 256 の同時 Telnet セッションをサポートします。ACE は、管理コンテキストの同時 Telnet 管理セッションを最大で 16、各ユーザ コンテキストの同時 Telnet 管理セッションを最大で 4 つサポートします。

詳細手順

	コマンド	目的
ステップ 1	**config** 例： host1/Admin# config host1/Admin(config)#	グローバル コンフィギュレーション モードに入ります。
ステップ 2	**telnet maxsessions** *max_sessions* 例： host1/Admin(config)# telnet maxsessions 3	（オプション）関連コンテキストに許可する最大同時 Telnet セッション数を指定します。 *max_sessions* 引数は、許可する最大同時 Telnet セッション数を設定します。有効範囲は、管理コンテキストの場合は 1 ～ 16、各ユーザ コンテキストの場合は 1 ～ 4 です。デフォルトは 16（管理コンテキスト）および 4（ユーザ コンテキスト）です。
	no telnet maxsessions 例： host1/Admin(config)# no telnet maxsessions	（オプション）コンテキストのデフォルトの最大 Telnet セッション数に戻します。
ステップ 3	**do show telnet maxsessions** [*context_name*] 例： host1/Admin(config)# do show telnet maxsessions Maximum Sessions Allowed is 4	（オプション）イネーブルにする Telnet セッションの最大数を表示します。特定のコンテキストに関連付けられた Telnet セッション情報を表示できるのは、コンテキスト管理者のみです。 オプションの *context_name* 引数は、最大 Telnet セッション数を表示するコンテキスト名を指定します。*context_name* 引数では、大文字と小文字が区別されます。
ステップ 4	**do copy running-config startup-config** 例： host1/Admin(config)# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

SSH 管理セッション パラメータの設定

ここでは、SSH 管理セッション パラメータの設定方法について説明します。ACE の SSH リモート アクセス セッションは、コンテキストごとに確立されます。コンテキストを作成し、インターフェイスおよび IP アドレスを割り当てて、ACE にログインするには、SSH を使用して、この IP アドレスに接続します。この機能を使用すると、ACE にアクセスする場合に、特定のコンテキストを指定できます。ユーザとコンテキストの作成方法については、『*Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*』を参照してください。

ここでは、次の内容について説明します。

- 最大 SSH 管理セッション数の設定
- SSH ホスト キー ペアの生成

最大 SSH 管理セッション数の設定

ここでは、コンテキストごとに許可する最大 SSH セッション数の制御方法について説明します。

制約事項

ACE は、合計で最大 256 の同時 SSH セッションをサポートします。ACE は、管理コンテキストの同時 SSH 管理セッションを最大で 16、各ユーザ コンテキストの同時 SSH 管理セッションを最大で 4 つサポートします。

詳細手順

	コマンド	目的
ステップ 1	**config** **例：** host1/Admin# config host1/Admin(config)#	グローバル コンフィギュレーション モードに入ります。
ステップ 2	**ssh maxsessions** *max_sessions* **例：** host1/Admin(config)# ssh maxsessions 3	（オプション）関連コンテキストに許可する最大同時 SSH セッション数を指定します。 *max_sessions* 引数は、許可する最大同時 SSH セッション数を設定します。有効範囲は、管理コンテキストの場合は 1 ～ 16、各ユーザ コンテキストの場合は 1 ～ 4 です。デフォルトは 16（管理コンテキスト）および 4（ユーザ コンテキスト）です。
	no ssh maxsessions **例：** host1/Admin(config)# no ssh maxsessions	（オプション）コンテキストのデフォルトの最大 SSH セッション数に戻します。
ステップ 3	**do show ssh maxsessions** [*context_name*] **例：** host1/Admin(config)# do show ssh maxsessions Maximum Sessions Allowed is 4	（オプション）イネーブルにする SSH セッションの最大数を表示します。特定のコンテキストに関連付けられた SSH セッション情報を表示できるのは、コンテキスト管理者のみです。 オプションの *context_name* 引数は、コンテキスト管理者が最大 SSH セッション数を表示するコンテキスト名を指定します。*context_name* 引数では、大文字と小文字が区別されます。
ステップ 4	**do copy running-config startup-config** **例：** host1/Admin(config)# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

SSH ホスト キー ペアの生成

ここでは、SSH ホスト キー ペアの生成方法について説明します。ACE は、秘密キーと公開キーのペアを使用してコンテキストの認証を実行する、SSH セッションを介したリモート ログインをサポートしています。DSA キーと RSA キーはペアで生成されます（公開キーと秘密キーが 1 つずつ）。この方式のリモート接続を使用する場合は、生成された秘密キーと公開キーのペアを使用して、メッセージを暗号化および復号化することによって、セキュアな通信に参加します。

グローバル管理者は、管理コンテキストでキー生成を実行します。ACE に関連付けられたすべてのコンテキストで、共通のキーが共有されます。ホスト/キー ペアは 1 つのみ存在します。

SSH サービスをイネーブルにする前に、SSH ホスト/キー ペアと適切なバージョンが存在することを確認します（「リモート ネットワーク管理トラフィック サービスの設定」を参照）。SSH サービスでは、SSH バージョン 1 と 2 で使用される 3 種類のキー ペアが受け入れられます。使用する SSH クライアント バージョンに従って、SSH ホスト キー ペアを生成します。キー ペアごとに指定されるビット数は、768 ～ 4096 です。

詳細手順

	コマンド	目的

ステップ 1	**changeto Admin**
	
	例：
	`host1/context3# changeto Admin`
	`host1/Admin#`
		（オプション）管理コンテキストに変更します。
		
		管理者または管理コンテキストで許可された別のユーザの場合は、このコマンドを EXEC モードで使用して、管理コンテキストに移動します。管理者は、管理コンテキストで許可されたすべての機能を実行できます。

ステップ 2	**config**
	
	例：
	`host1/Admin# config`
	`host1/Admin(config)#`
		グローバル コンフィギュレーション モードに入ります。

ステップ 3	**hostname** *name*
	
	例：
	`host1/Admin(config)# hostname host1`
	`host1/Admin(config)#`
		ホスト名を設定します。この設定が、キーの生成に使用されます。
		
		name 引数は、ACE の新しいホスト名を指定します。大文字と小文字の区別がある、1 ～ 32 文字の英数字からなるテキスト ストリングを入力します。
		
		ホスト名の設定方法については、「ACE へのホスト名の割り当て」（P.1-12）を参照してください。

ステップ 4	**ssh key** {**dsa** | **rsa** | **rsa1**} [*bits* [**force**]] **例：** `host1/Admin(config)# ssh key rsa1 1024`	SSH 秘密キーと対応する公開キーを生成します。 引数、キーワード、およびオプションは次のとおりです。 • **dsa**：SSH バージョン 2 プロトコルに対応する DSA キー ペアを生成します。 • **rsa**：SSH バージョン 2 プロトコルに対応する RSA キー ペアを生成します。 • **rsa1**：SSH バージョン 1 プロトコルに対応する RSA1 キー ペアを生成します。 • *bits*：（オプション）キー ペアのビット数を指定します。DSA の場合の範囲は、768 ～ 2048 です。RSA と RSA1 の場合の範囲は、768 ～ 4096 です。指定したビット数が多いほど、キーの生成に時間がかかります。デフォルトは 768 です。 • **force**：（オプション）すでにキーが存在する場合でも、DSA キーまたは RSA キーの生成を強制します。必要なバージョンに対応した SSH キー ペア オプションがすでに生成されている場合に、以前生成されたキー ペアを上書きするために **force** オプションを使用します。
	no ssh key {**dsa** | **rsa** | **rsa1**} **例：** `host1/Admin(config)# no ssh key rsa1`	（オプション）SSH ホスト キー ペアを削除します。

	コマンド	目的
ステップ 5	**do show ssh key** [**dsa** | **rsa** | **rsa1**] **例：** host1/Admin(config)# do show ssh key rsa	（オプション）指定したキーまたはキーを指定しなかった場合のすべてのキーに関するホスト キー ペアの詳細を表示します。
ステップ 6	**do copy running-config startup-config** **例：** host1/Admin(config)# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。
ステップ 7	**exit** **例：** host1/Admin(config)# exit host1/Admin#	（オプション）EXEC モード プロンプトに戻ります。
ステップ 8	**clear ssh hosts** **例：** host1/Admin# clear ssh hosts	（オプション）信頼されたすべてのホストの公開キーをクリアします。これらのキーは SSH サーバから SSH クライアントに送信される場合と手動で入力される場合があります。ACE からの SSH 接続が確立されると、SSH クライアントは公開キーを受け取り、ローカルに保存します。

例

下の例は、**show ssh key** コマンドの出力を示しています。

```
host1/Admin # show ssh key
**************************************
could not retrieve rsa1 key information
**************************************
rsa Keys generated:Tue Mar 7 19:37:17 2006

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEA4v4DQ8aNl482qDTRju9G07hEIxCgTWanPm+WOCU1kihZ
QNd5ZwA50CBAJSfIIIB4iED6iQbhOkbXSneCvTb5mVoish2wvJrETpIDIeGxxh/jWVsU/MeBbA/7o5tv
gCeT6p7pGF5oUNYFP0OeZ9BiIWDc4jBmYEQLEqJHPrMhSFE=

bitcount:1024
fingerprint:
f5:55:00:18:bc:af:41:74:b6:bc:aa:8e:46:31:74:4f
**************************************
dsa Keys generated:Tue Dec 20 19:37:17 2005

ssh-dss AAAAB3NzaC1kc3MAAACBAPqDdEqU+0gNtKRXM+DQAXnvcB+H89nq8jA4WgJ7uQcuDCLaG7Lq
jtKTltJjA6aZVywsQWQ6n4kTlkavZy3cj6PUbSyqvmCTsaYyYo4UQ6CKrK9V+NsfgzTSLWTH8iDUvYjL
c3nU51QEKjy7mPsQeX31y1M1rhp8qhkbMKxkc49XAAAAFQCPM0QJrq6+kkaghJpeNxeXhUH9HwAAAIEA
keZ1ZJM6sfKqJDYPLHkTro+lpbV9uR4VyYoZmSoehi/LmSaZDq+Mc8UN1LM+i5vkOgnKcearD9lM4/hK
zZGYx5hJOiYCKj/ny2a5p/8HK152cnsOAg6ebkiTTWAprcWrcHDS/1mcaI5GzLrZCdlXW5gBFZtMTJGs
tICmVWjibewAAACBAJQ66zdZQqYiCWtZfmakridEGDTLV6ixIDjBNgb84qlj+Y1XMzqLL0D4oMSb7idE
L3BmhQYQW7hkTK0oS4kVawI1VmW2kvrqoGQnLNQRMvisAXuJWKk1Ln6vWPGZZe8KoALv0GXxsOv2gk/z
TDk01oCaTVw//bXJtoVRgIlWXLIP

bitcount:1024
fingerprint:
8e:13:5c:3e:1a:9c:7a:ed:d0:84:eb:96:12:db:82:be
**************************************
```

アクティブ ユーザ セッションの終了

ここでは、アクティブ コンテキストのアクティブ SSH セッションまたは Telnet セッションの終了方法について説明します。

詳細手順

	コマンド	目的
ステップ 1	**show** {**ssh session-info** | **telnet**} **例：** host1/Admin# show ssh session-info	（オプション）現在のすべての SSH セッションまたは Telnet セッションの、セッション ID を含む、セッション情報を表示します。 キーワードは次のとおりです。 • **ssh session-info**：SSH セッション情報を表示します。 • **telnet**：Telnet セッション情報を表示します。
ステップ 2	**clear** {**ssh** | **telnet**} *session_id* **例：** host1/Admin# clear ssh 345	入力されたコマンドに応じて、現在の SSH セッションまたは Telnet セッションを終了します。 引数とキーワードは次のとおりです。 • **ssh**：SSH セッション タイプを選択します。 • **telnet**：Telnet セッション タイプを選択します。 • *session_id*：切断する SSH セッションまたは Telnet セッションの ID を指定します。

ACE への ICMP メッセージのイネーブル化

ここでは、ACE 上で ICMP メッセージをイネーブルにする方法について説明します。ACE はデフォルトで、ACE インターフェイスでの ICMP メッセージの受信、または ACE インターフェイスを介した ICMP メッセージの送信を許可していません。ICMP はネットワーク接続をテストするための重要なツールですが、ネットワーク ハッカーが ICMP を使用して ACE またはネットワークを攻撃することもできます。初期テスト中は ICMP を許可し、通常操作中は禁止することを推奨します。

ホストから ACE に、または ACE から ICMP 応答の返送許可を要求するホストに送信される ICMP メッセージを使用して ACE インターフェイスに到達するためのアドレスを許可または拒否するには、次のいずれかを設定します。

- ACE の ICMP ネットワーク トラフィック一致基準を指定するクラス マップ
- ACE に対する ICMP ネットワーク管理アクセスをイネーブルにするポリシー マップ
- ポリシー マップをアクティブにして、トラフィック ポリシーを特定のインターフェイスまたはすべてのインターフェイスにグローバルにアタッチし、ポリシーの適用方向を指定するサービス ポリシー

「リモート ネットワーク管理トラフィック サービスの設定」のネットワーク管理クラス マップ、ポリシー マップ、サービス ポリシーの設定方法については、ACE を参照してください。

ACE を介した ICMP メッセージの送信を許可するには、ICMP タイプ（echo、echo-reply、unreachable など）に基づいてネットワーク接続を許可または拒否するように ICMP ACL（アクセス コントロール リスト）を設定します。詳細については、『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照してください。

（注）　ACE からホストへの ping のみを許可し（インターフェイスへのエコー返信を許可し）、ホストから ACE への ping を許可しない場合は、クラス マップおよびポリシー マップを定義しないで、ICMP アプリケーション プロトコル インスペクションをイネーブルにします。詳細については、『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照してください。

例

下の例は、ACE に ICMP ping の受信を許可する方法を示しています。

```
host1/Admin(config)# class-map type management match-all ICMP-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# description Allow ICMP packets
host1/Admin(config-cmap-mgmt)# match protocol icmp source-address 172.16.10.0
255.255.255.254
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)# policy-map type management first-action ICMP_ALLOW_POLICY
host1/Admin(config-pmap-mgmt)# class ICMP-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# exit
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 172.16.1.100 255.255.0.0
host1/Admin(config-if)# service-policy input ICMP_ALLOW_POLICY
```

SSH を介したユーザ コンテキストへの直接アクセス

ここでは、ユーザ コンテキストを設定して、リモート SSH セッションからそのユーザ コンテキストへの直接ログイン アクセスを可能にする方法について説明します。この手順を実行するには、グローバル管理者になって、管理コンテキストに入る必要があります。

タスク フロー

SSH からユーザ コンテキストへの直接アクセスを提供するように ACE を設定してから、ユーザ コンテキストにアクセスするには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、ユーザ コンテキストを作成します。

```
host1/Admin(config)# context C1
host1/Admin(config-context)#
```

『*Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*』を参照してください。

ステップ 2　既存の VLAN にユーザ コンテキストを関連付けて、コンテキストが自身に分類されたトラフィックを受信できるようにするには、次のコマンドを入力します。

```
host1/Admin(config-context)# allocate-interface vlan 100
```

『*Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*』を参照してください。

ステップ 3　次のコマンドを入力して、SSH ホスト キー ペアを生成します。

```
host1/Admin(config-context)# ssh key rsa1 1024
generating rsa1 key
.....
generated rsa1 key
```

「SSH ホスト キー ペアの生成」を参照してください。

ステップ 4　次のコマンドを入力して、ステップ 1 で作成した C1 コンテキストに変更し、このコンテキストでコンフィギュレーション モードに入ります。

```
host1/Admin(config-context)# do changeto C1
host1/C1(config-context)# exit
host1/C1(config)#
```

changeto コマンドを使用できるのは、管理コンテキストで認証されたユーザのみです。

ステップ 5　次のコマンドを入力して、ステップ 2 のユーザ コンテキストに割り当てられた VLAN インターフェイスを設定します。

```
host1/C1(config)# interface vlan 50
host1/C1(config-if)# ip address 192.168.1.1 255.255.255.0
host1/C1(config-if)# no shutdown
host1/C1(config-if)# exit
host1/C1(config)#
```

たとえば、インターフェイスに IP アドレスを割り当て、**no shutdown** コマンドを使用して、コンテキスト内でインターフェイスを再イネーブルにします。『*Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*』を参照してください。

ステップ 6　次のコマンドを入力して、SSH リモート管理ポリシーを作成し、関連するサービス ポリシーをすべての VLAN インターフェイスに適用するか、ユーザ コンテキストに割り当てられた VLAN インターフェイスにのみ適用します。

```
host1/C1(config)# class-map type management match-all SSH-ALLOW_CLASS
host1/C1(config-cmap-mgmt)# match protocol ssh source-address 172.16.10.0 255.255.255.254
host1/C1(config-cmap-mgmt)# exit
host1/C1(config)#
host1/C1(config)# policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
host1/C1(config-pmap-mgmt)# class SSH-ALLOW_CLASS
host1/C1(config-pmap-mgmt-c)# permit
host1/C1(config-pmap-mgmt-c)# exit
host1/C1(config-pmap-mgmt)# exit
host1/C1(config)# interface vlan 50
host1/C1(config-if)# ip address 192.168.1.1 255.255.255.0
host1/C1(config-if)# service-policy input REMOTE_MGMT_ALLOW_POLICY
host1/C1(config-if)# exit
host1/C1(config)#
```

「リモート ネットワーク管理トラフィック サービスの設定」を参照してください。

ステップ 7　次のコマンドを入力して、IP ルートを作成します。

```
host1/C1(config)# ip route 0.0.0.0 255.255.255.0 192.168.4.8
```

『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照してください。

ステップ 8　SSH クライアントからユーザ コンテキストに直接アクセスするには、次の手順を実行します。

a. SSH クライアントから、ユーザ コンテキスト VLAN インターフェイスの IP アドレスへのリモート SSH セッションを確立します。

b. ユーザ コンテキスト VLAN インターフェイスのパスワードを入力します。ユーザ コンテキストの EXEC モードで、ACE CLI プロンプトが表示されます。

```
host1/C1#
```

リモート アクセス セッション情報の表示

ここでは、リモート アクセス セッション情報の表示方法について説明します。内容は次のとおりです。

Telnet セッション情報の表示

Telnet セッションを表示するには、次のタスクを実行します。

コマンド	目的
show telnet [*context_name*]	Telnet セッションに関する情報を表示します。特定のコンテキストに関連付けられた Telnet 情報を表示できるのは、コンテキスト管理者のみです。 オプションの *context_name* 引数は、特定の Telnet セッション情報を表示するコンテキスト名を指定します。*context_name* 引数では、大文字と小文字が区別されます。

表 2-2 に、**show telnet** コマンド出力に含まれるフィールドの説明を示します。

表 2-2　show telnet コマンド出力のフィールドの説明

フィールド	説明
SessionID	Telnet セッションの一意なセッション ID。
Remote Host	リモート Telnet クライアントの IP アドレスとポート。
Active Time	ACE が Telnet 接続要求を受信してからの経過時間。

SSH セッション情報の表示

SSH セッションを表示するには、次のタスクを実行します。

コマンド	目的
show ssh session-info [*context_name*]	SSH セッションに関する情報を表示します。特定のコンテキストに関連付けられた SSH セッション情報を表示できるのは、コンテキスト管理者のみです。 オプションの *context_name* 引数は、特定の SSH セッション情報を表示するコンテキスト名を指定します。*context_name* 引数では、大文字と小文字が区別されます。

表 2-3 に、**show ssh session-info** コマンド出力に含まれるフィールドの説明を示します。

表 2-3　show ssh session-info コマンド出力のフィールドの説明

フィールド	説明
SessionID	SSH セッションの一意なセッション ID。

表 2-3　show ssh session-info コマンド出力のフィールドの説明 （続き）

フィールド	説明
Remote Host	リモート SSH クライアントの IP アドレスとポート。
Active Time	ACE が SSH 接続要求を受信してからの経過時間。

その他のリモート アクセス セッション情報の表示

その他のリモート アクセス設定情報を表示するには、次のいずれかのタスクを実行します。

コマンド	目的
show running-config	実行コンフィギュレーションを表示します。
show ssh key [**dsa** | **rsa** | **rsa1**]	指定したキーまたはキーを指定しなかった場合のすべてのキーに関するホスト キー ペアの詳細を表示します。 「SSH ホスト キー ペアの生成」を参照してください。
show ssh maxsessions [*context_name*]	イネーブルにする SSH セッションの最大数を表示します。特定のコンテキストに関連付けられた SSH セッション情報を表示できるのは、コンテキスト管理者のみです。 「最大 SSH 管理セッション数の設定」を参照してください。
show telnet maxsessions [*context_name*]	イネーブルにする Telnet セッションの最大数を表示します。特定のコンテキストに関連付けられた Telnet セッション情報を表示できるのは、コンテキスト管理者のみです。 「最大 Telnet 管理セッション数の設定」を参照してください。

ACE へのリモート アクセスをイネーブルにするための設定例

下の CLI 例は、クラス マップ、ポリシー マップ、およびサービス ポリシーの使用を通して、ACE へのリモート アクセスを設定する方法を示しています。

ステップ 1　コンフィギュレーション モードに入って、最大 Telnet セッション数と最大 SSH セッション数を設定します。

```
host1/Admin# config
host1/Admin(config)# telnet maxsessions 3
host1/Admin(config)# ssh maxsessions 3
```

ステップ 2　アクセス コントロール リストを作成して設定します。この手順で示すサンプル アクセス コントロール リストでは、任意の送信元からのネットワーク トラフィックが許可されます。アクセス コントロール リストの設定方法については、『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照してください。

```
host1/Admin(config)# access-list ACL1 line 10 extended permit ip any any
```

ステップ 3　ネットワーク管理トラフィック用のクラス マップを作成して設定します。

```
host1/Admin(config)# class-map type management match-any L4_REMOTE-MGT_CLASS
host1/Admin(config-cmap-mgmt)# description Allows Telnet, SSH, and ICMP protocols
host1/Admin(config-cmap-mgmt)# 2 match protocol telnet any
host1/Admin(config-cmap-mgmt)# 3 match protocol ssh any
host1/Admin(config-cmap-mgmt)# 4 match protocol icmp any
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)#
```

ステップ 4　SSH および Telnet 管理プロトコル分類をアクティブにするポリシー マップを作成して設定します。

```
host1/Admin(config)# policy-map type management first-match L4_REMOTE-MGT_POLICY
host1/Admin(config-pmap-mgmt)# class L4_REMOTE-MGT_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# exit
host1/Admin(config)#
```

ステップ 5　トラフィック ポリシーを、特定の VLAN インターフェイスに適用するか、すべての VLAN インターフェイスにグローバルに適用して、インターフェイスをイネーブルにします。

特定の VLAN インターフェイスに適用する場合：

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 192.168.1.1 255.255.255.0
host1/Admin(config-if)# access-group input ACL1
host1/Admin(config-if)# service-policy input L4_REMOTE-MGT_POLICY
host1/Admin(config-if)# no shutdown
host1/Admin(config-if)# exit
host1/Admin(config)#
```

すべての VLAN インターフェイスにグローバルに適用する場合：

```
host1/Admin(config)# service-policy input REMOTE_MGMT_ALLOW_POLICY
```

ステップ 6　SSH サーバで使用される SSH 秘密キーと対応する公開キーを生成します。

```
host1/Admin(config)# ssh key rsa1 1024 force
```

ステップ 7　フラッシュ メモリに設定を保存します。

```
host1/Admin(config)# do copy running-config startup-config
```