CHAPTER 6

ファイアウォール負荷分散の設定

この章では、ご使用の ACE でのファイアウォール負荷分散の設定方法を説明します。ファイアウォール負荷分散を設定すると、トラフィックを接続ごとに複数のファイアウォールに分散させることによって、ファイアウォール プロテクションを拡張できます。特定の接続に属するパケットは、すべて同じファイアウォールを通過します。ファイアウォールは、そのインターフェイスすべてにわたり、個々のパケットの伝送を許可または拒否します。

この章の主な内容は、次のとおりです。

- ファイアウォールの概要
- スタンダード ファイアウォール負荷分散の設定
- ステルス ファイアウォール負荷分散の設定
- FWLB 設定の表示
- ファイアウォール負荷分散の設定例
- 次の作業

ファイアウォールの概要

ファイアウォールは、ネットワークの 2 つの部分（たとえば、インターネットとイントラネット）の間で物理的障壁を形成します。ファイアウォールは、一方の側（インターネット）からパケットを受け取ると、そのパケットをもう一方の側（イントラネット）へ転送します。ファイアウォールでは、パケットを修正してから転送したり、そのまま転送したりできます。ファイアウォールは、パケットを拒否すると、通常、そのパケットを廃棄し、廃棄されたパケットをイベントとしてロギングします。

セッションが確立され、パケットのフローが開始されたら、ファイアウォールでは、設定されたポリシーに応じて、フロー内の各パケットを監視したり、フローを監視せずに転送したりできます。

ここでは、次の内容について説明します。

- ファイアウォールのタイプ
- ACE によるファイアウォールへのトラフィック分散方法
- サポート対象のファイアウォール設定

ファイアウォールのタイプ

ファイアウォールには、次のような 2 つの基本タイプがあります。

- スタンダード ファイアウォール
- ステルス ファイアウォール

スタンダード ファイアウォールは、ネットワーク上にプレゼンスを持ちます。IP アドレスが割り当てられるため、ネットワーク上の他のデバイスによって認識され、デバイスとして扱われます。各ファイアウォールは、ファイアウォールの両側に設定された VLAN 上の IP アドレスを持ちます。

ステルス ファイアウォールは、ネットワーク上にプレゼンスを持ちません。IP アドレスが割り当てられないため、ネットワーク上の他のデバイスによって認識されることも対処されることもありません。IP アドレスはファイアウォールの両側で VLAN に設定されます。ネットワークに対して、ステルス ファイアウォールは導線の一部です。

両方のファイアウォール タイプは、次の作業を行います。

- ネットワークの保護されている側と保護されていない側の間を流れる両方向のトラフィックを検査します。
- ユーザ定義のポリシーに基づいてパケットを承認または拒否します。

ACE によるファイアウォールへのトラフィック分散方法

ACE は、サーバ ファーム内の設定されたデバイスにトラフィックをロード バランシングします。これらのデバイスには、ファイアウォール、キャッシュ、サーバ、その他エイリアス IP アドレスなど IP アドレス指定可能なオブジェクトが含まれます。サーバ ファームの詳細については、第 2 章「実サーバおよびサーバ ファームの設定」の「サーバ ファームの設定」の項を参照してください。ACE がトラフィックをファイアウォールにロード バランシングするときに実行する機能は、サーバ ファーム内で実サーバにレイヤ 3 トラフィックをロード バランシングするときに実行する機能と同じです。

ACE は、ロード バランシング アルゴリズムまたはプレディクタを使用して、デバイスのタイプにかかわらず、サーバ ファーム内の設定されたデバイス間でのトラフィック分散方法を決定します。FWLB では、ハッシュ アドレス送信元およびハッシュ アドレス宛先プレディクタのみを使用することを推奨します。FWLB で、特に制御チャネルとデータ チャネルが分離しているアプリケーション（FTP など）に対して他のプレディクタを使用すると、障害が発生してトラフィックがブロックされる場合があります。

ロード バランシングのプレディクタ方式の詳細については、第 2 章「実サーバおよびサーバ ファームの設定」の「サーバ ファーム プレディクタ方式の設定」の項を参照してください。

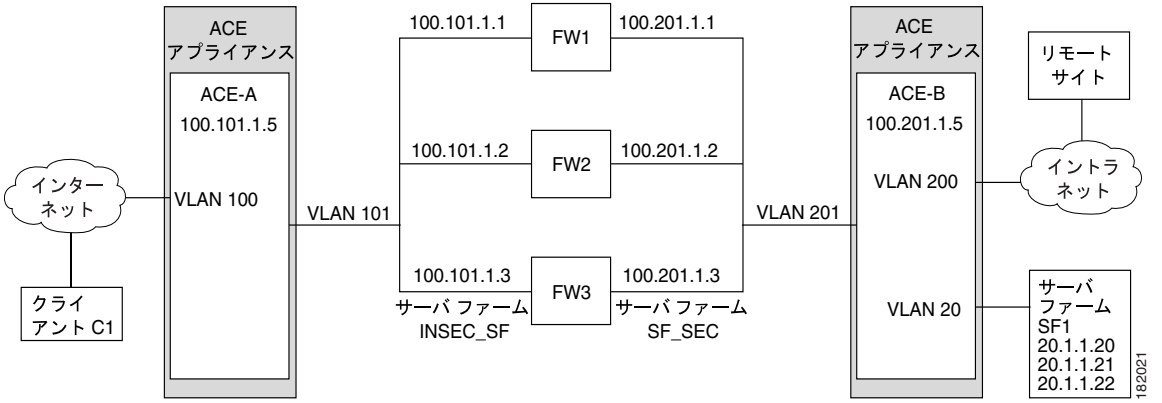
サポート対象のファイアウォール設定

ACE は、スタンダード ファイアウォールとステルス ファイアウォールの両方にトラフィックをロード バランシングできます。

標準的なファイアウォールの場合、ACE がサーバ ファーム内のサーバ間でトラフィックをロード バランシングする方法と同様に、単体の ACE またはペアの ACE が、一意の IP アドレスを備えているファイアウォール間でトラフィックをロード バランシングします（図 6-1）。

図 6-1 では、トラフィックがファイアウォールを通過し、ファイアウォールは両方向でトラフィックをフィルタリングします。インターネットからのトラフィックについては、ACE A がトラフィックをサーバ ファーム SF_INSEC にロード バランシングします。イントラネットからのトラフィックについては、ACE B がトラフィックをサーバ ファーム SF_SEC にロード バランシングします。ファイアウォールは、リターン トラフィックが元のトラフィックと同じファイアウォールを通過するように設定します。

図 6-1　スタンダード ファイアウォールの設定



ステルス ファイアウォールの場合、ACE は、ファイアウォールを経由するパスを提供する異なる ACE 内にある、一意のエイリアス IP アドレスを持つインターフェイス間で、トラフィックをロード バランシングします（図 6-2）。ステルス ファイアウォールは、特定の VLAN 上を流れる両方向のトラフィックがすべて同じファイアウォールを通過するように設定します。

図 6-2　ステルス ファイアウォールの設定（デュアル ACE のみ）

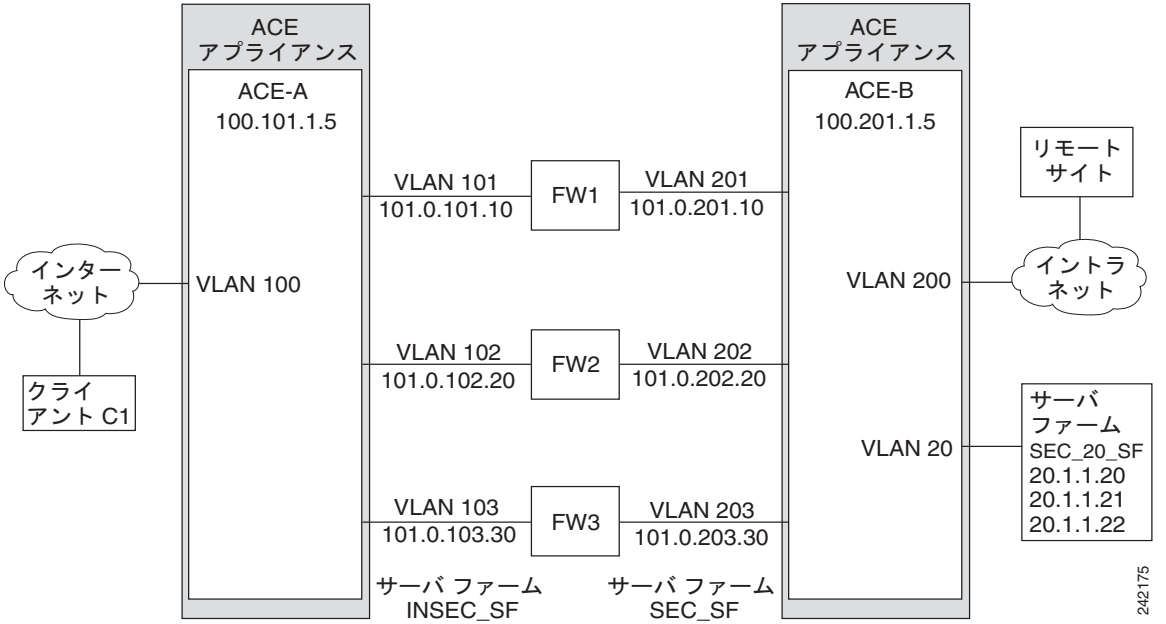


図 6-2 では、トラフィックがファイアウォールを通過し、ファイアウォールは両方向でトラフィックをフィルタリングします。イントラネットへのパスでは、ACE A が VLAN 101、102、および 103 にわたってトラフィックを ACE B へのファイアウォールにバランシングします。インターネットへのパスでは、ACE B が VLAN 201、202、および 203 にわたってトラフィックを ACE A へのファイアウォールにバランシングします。各 ACE は、ロード バランシング プロセスのターゲットとして、もう一方の ACE に設定されたエイリアス IP アドレスを使用します。

スタンダード ファイアウォール負荷分散の設定

この項では、スタンダード ファイアウォールのファイアウォール負荷分散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。

- スタンダード FWLB 設定の概要
- スタンダード FWLB 設定のクイック スタート

（注）　ネットワーク内のファイアウォール デバイスの設定の詳細については、ご使用のファイアウォール製品に付属のマニュアルを参照してください。

スタンダード FWLB 設定の概要

このスタンダード FWLB の設定例では（図 6-1 を参照）、2 台の ACE（ACE A、ACE B）間で 3 つのファイアウォール（FW1、FW2、FW3）を設定します（スタンダード FWLB は、ACE が 1 台だけでも設定できます）。トラフィックは、ファイアウォールの両側の共有 VLAN を経由してファイアウォールに出入りします（低セキュリティ側は VLAN 101、高セキュリティ側は VLAN 201）。各共有 VLAN 上のサーバ ファーム内で実サーバとして設定された各ファイアウォールに一意の IP アドレスを割り当てます。

他の VLAN は、次のロケーションへの接続を提供します。

- インターネット（VLAN 100）
- 内部ネットワーク（VLAN 200）
- 内部サーバ ファーム（VLAN 20）

スタンダード FWLB 設定のクイック スタート

ここでは、2 台の ACE でスタンダード FWLB を設定するためのステップバイステップ手順を含んだクイック スタート表を提供します。スタンダード FWLB は、ACE が 1 台だけでも設定できます。次の内容について説明します。

- ACE A のスタンダード FWLB 設定のクイック スタート
- ACE B のスタンダード FWLB 設定のクイック スタート

ACE A のスタンダード FWLB 設定のクイック スタート

表 6-1 は、ACE A でスタンダード FWLB を設定するために必要な手順の概要を示しています（図 6-1 を参照）。各ステップには、作業の完了に必要な CLI コマンドが示されています。

表 6-1　ACE A のスタンダード FWLB 設定のクイック スタート

作業およびコマンドの例

1. 複数のコンテキストを使用している場合は、CLI プロンプトに注意し、目的のコンテキスト内で作業を実行していることを確認します。必要な場合は、正しいコンテキストに変更するか、または正しいコンテキストに直接ログインしてください。
`host1/Admin# changeto C1`
`host1/C1#`
この表の以降の例では、特に記載がない限り、管理コンテキストが使用されています。コンテキストの作成に関する詳細は、『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照してください。

2. コンフィギュレーション モードを開始します。
`host1/Admin# config`
`Enter configuration commands, one per line. End with CNTL/Z`
`host1/Admin(config)#`

3. Access Control List（ACL; アクセス コントロール リスト）を設定してトラフィックを許可します。ACL は、アプリケーションのニーズに合わせて修正できます。ACL の設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照してください。
`host1/Admin(config)# access-list ACL1 line 10 extended permit ip any any`
`host1/Admin(config-acl)# exit`

表 6-1　ACE A のスタンダード FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

4. 3 台の実サーバで、VLAN 101 に属するファイアウォールの低セキュリティ側を設定します。実サーバの設定の詳細については、第 2 章「実サーバおよびサーバ ファームの設定」を参照してください。
`host1/Admin(config)# rserver FW_INSEC_1`
`host1/Admin(config-rserver-host)# ip address 100.101.1.1`
`host1/Admin(config-rserver-host)# inservice`
`host1/Admin(config-rserver-host)# exit`
 	
`host1/Admin(config)# rserver FW_INSEC_2`
`host1/Admin(config-rserver-host)# ip address 100.101.1.2`
`host1/Admin(config-rserver-host)# inservice`
`host1/Admin(config-rserver-host)# exit`
 	
`host1/Admin(config)# rserver FW_INSEC_3`
`host1/Admin(config-rserver-host)# ip address 100.101.1.3`
`host1/Admin(config-rserver-host)# inservice`
`host1/Admin(config-rserver-host)# exit`

5. ファイアウォールの低セキュリティ側（インターネット）からの接続を処理するようにサーバ ファームを設定します。ACE は、ハッシュ アドレス送信元プレディクタを使用して、送信元 IP アドレスに基づいてファイアウォールを選択します。サーバ ファームの設定の詳細については、第 2 章「実サーバおよびサーバ ファームの設定」を参照してください。
`host1/Admin(config)# serverfarm SF_INSEC`
`host1/Admin(config-sfarm-host)# transparent`
`host1/Admin(config-sfarm-host)# predictor hash address source 255.255.255.255`
`host1/Admin(config-sfarm-host)# rserver FW_INSEC_1`
`host1/Admin(config-sfarm-host-rs)# inservice`
`host1/Admin(config-sfarm-host-rs)# exit`
`host1/Admin(config-sfarm-host)# rserver FW_INSEC_2`
`host1/Admin(config-sfarm-host-rs)# inservice`
`host1/Admin(config-sfarm-host-rs)# exit`
`host1/Admin(config-sfarm-host)# rserver FW_INSEC_3`
`host1/Admin(config-sfarm-host-rs)# inservice`
`host1/Admin(config-sfarm-host-rs)# exit`
`host1/Admin(config-sfarm-host)# exit`

表 6-1　ACE A のスタンダード FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

6. 要求がサーバ ファーム SF-INSEC にバランシングされるように、レイヤ 7 ロード バランシング ポリシー マップを設定します。そのポリシー マップとデフォルト クラス マップおよびサーバ ファーム SF-INSEC を関連付けます。SLB のトラフィック ポリシー設定の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。
`host1/Admin(config)# policy-map type loadbalance first-match LB_FW_INSEC`
`host1/Admin(config-pmap-lb)# class class-default`
`host1/Admin(config-pmap-lb-c)# serverfarm SF_INSEC`
`host1/Admin(config-pmap-lb-c)# exit`
`host1/Admin(config-pmap-lb)# exit`

7. ファイアウォールの低セキュリティ側の VLAN 100 で VIP アドレス 255.1.1.1 にマッチするインターネットからのトラフィックを分類するように、レイヤ 3 クラス マップを設定します。SLB のトラフィック ポリシー設定の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。
`host1/Admin(config)# class-map match-any FW_VIP`
`host1/Admin(config-cmap)# match virtual-address 255.1.1.1 255.255.0.0 any`
`host1/Admin(config-cmap)# exit`

8. レイヤ 3 ポリシー マップを設定し、それとレイヤ 3 クラス マップおよびレイヤ 7 ポリシー マップを関連付けて、トラフィック ポリシー設定を完了します。SLB のトラフィック ポリシー設定の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。
`host1/Admin(config)# policy-map multi-match POL_INSEC`
`host1/Admin(config-pmap)# class FW_VIP`
`host1/Admin(config-pmap-c)# loadbalance vip inservice`
`host1/Admin(config-pmap-c)# loadbalance policy LB_FW_INSEC`
`host1/Admin(config-pmap-c)# exit`
`host1/Admin(config-pmap)# exit`

表 6-1　ACE A のスタンダード FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

9. インターネットからのトラフィックを受信し、イントラネットからのトラフィックをインターネットに送信するために ACE で使用するインターフェイスを設定します。ACL（ACL1）とレイヤ 3 ポリシー（POL_INSEC）を、そのインターフェイスに適用します。インターフェイスの設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*』を参照してください。
`host1/Admin(config)# interface vlan 100`
`host1/Admin(config-if)# ip address 100.100.1.100 255.255.0.0`
`host1/Admin(config-if)# access-group input ACL1`
`host1/Admin(config-if)# service-policy input POL_INSEC`
`host1/Admin(config-if)# no shutdown`
`host1/Admin(config-if)# exit`

10. ファイアウォールの低セキュリティ側のインターフェイスを設定します。ACE は、このインターフェイスを使用してトラフィックをファイアウォールにロード バランシングし、イントラネットからのトラフィックを受信します。インターフェイスの設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*』を参照してください。
`host1/Admin(config)# interface vlan 101`
`host1/Admin(config-if)# ip address 100.101.1.101 255.255.0.0`
`host1/Admin(config-if)# access-group input ACL1`
`host1/Admin(config-if)# mac-sticky enable`
`host1/Admin(config-if)# service-policy input POL_INSEC`
`host1/Admin(config-if)# no shutdown`
`host1/Admin(config-if)# Ctrl-z`

11. 次の **show** コマンドを使用して、FWLB の設定を確認します。
`host1/Admin# show running-config access-list`
`host1/Admin# show running-config class-map`
`host1/Admin# show running-config interface`
`host1/Admin# show running-config policy-map`
`host1/Admin# show running-config rserver`
`host1/Admin# show running-config serverfarm`

12.（任意）設定変更をフラッシュ メモリに保存します。 `host1/Admin# copy running-config startup-config`

ACE B のスタンダード FWLB 設定のクイック スタート

表 6-2 は、ACE B でスタンダード FWLB を設定するために必要な手順の概要を示しています（図 6-1 を参照）。ステップごとに、CLI コマンドおよび作業に必要な手順の参照を示します。

表 6-2　ACE B のスタンダード FWLB 設定のクイック スタート

作業およびコマンドの例

1. 複数のコンテキストを使用している場合は、CLI プロンプトに注意し、目的のコンテキスト内で作業を実行していることを確認します。必要な場合は、正しいコンテキストに変更するか、または正しいコンテキストに直接ログインしてください。
`host1/Admin# changeto C1`
`host1/C1#`
この表の以降の例では、特に記載がない限り、管理コンテキストが使用されています。コンテキストの作成に関する詳細は、『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照してください。

2. コンフィギュレーション モードを開始します。
`host1/Admin# config`
`Enter configuration commands, one per line. End with CNTL/Z`
`host1/Admin(config)#`

3. ACL を設定してトラフィックを許可します。ACL は、アプリケーションのニーズに合わせて修正できます。ACL の設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照してください。
`host1/Admin(config)# access-list ACL1 line 10 extended permit ip any any`
`host1/Admin(config-acl)# exit`

表 6-2　ACE B のスタンダード FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

4. 3 台の実サーバで、VLAN 201 に属するファイアウォールの高セキュリティ側を設定します。実サーバの設定の詳細については、第 2 章「実サーバおよびサーバ ファームの設定」を参照してください。
 	
`host1/Admin(config)# rserver FW_SEC_1`
`host1/Admin(config-rserver-host)# ip address 100.201.1.1`
`host1/Admin(config-rserver-host)# inservice`
`host1/Admin(config-rserver-host)# exit`
 	
`host1/Admin(config)# rserver FW_SEC_2`
`host1/Admin(config-rserver-host)# ip address 100.201.1.2`
`host1/Admin(config-rserver-host)# inservice`
`host1/Admin(config-rserver-host)# exit`
 	
`host1/Admin(config)# rserver FW_SEC_3`
`host1/Admin(config-rserver-host)# ip address 100.201.1.3`
`host1/Admin(config-rserver-host)# inservice`
`host1/Admin(config-rserver-host)# exit`

5. ファイアウォールの高セキュリティ側（イントラネット）からの接続を処理するようにサーバ ファームを設定します。この場合、ACE は、ハッシュ アドレス宛先プレディクタを使用して、宛先 IP アドレスに基づいてファイアウォールを選択します。このプレディクタによって、ACE は、リターン フローおよび関連する接続に対して同じファイアウォールを選択できます。たとえば、FTP の場合、制御チャネルとデータ チャネルがいずれも同じファイアウォールを通過できます。サーバ ファームの設定の詳細については、第 2 章「実サーバおよびサーバ ファームの設定」を参照してください。
 	
`host1/Admin(config)# serverfarm SF_SEC`
`host1/Admin(config-sfarm-host)# transparent`
`host1/Admin(config-sfarm-host)# predictor hash address destination 255.255.255.255`
`host1/Admin(config-sfarm-host)# rserver FW_SEC_1`
`host1/Admin(config-sfarm-host-rs)# inservice`
`host1/Admin(config-sfarm-host-rs)# exit`
`host1/Admin(config-sfarm-host)# rserver FW_SEC_2`
`host1/Admin(config-sfarm-host-rs)# inservice`
`host1/Admin(config-sfarm-host-rs)# exit`
`host1/Admin(config-sfarm-host)# rserver FW_SEC_3`
`host1/Admin(config-sfarm-host-rs)# inservice`
`host1/Admin(config-sfarm-host)# exit`

表 6-2　ACE B のスタンダード FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

6. ファイアウォールの高セキュリティ側の VLAN 20 でコンテンツをロードバランシングするように 2 台の実サーバを設定します。サーバ ファームの設定の詳細については、第 2 章「実サーバおよびサーバ ファームの設定」を参照してください。
`host1/Admin(config)# rserver REAL1`
`host1/Admin(config-rserver-host)# ip address 20.1.1.1`
`host1/Admin(config-rserver-host)# inservice`
`host1/Admin(config-rserver-host)# exit`
 	
`host1/Admin(config)# rserver REAL2`
`host1/Admin(config-rserver-host)# ip address 20.1.1.2`
`host1/Admin(config-rserver-host)# inservice`
`host1/Admin(config-rserver-host)# exit`
 	
`host1/Admin(config)# rserver REAL3`
`host1/Admin(config-rserver-host)# ip address 20.1.1.3`
`host1/Admin(config-rserver-host)# inservice`
`host1/Admin(config-rserver-host)# exit`

7. HTTP サーバの標準的なサーバ ファームを設定します。サーバ ファームの設定の詳細については、第 2 章「実サーバおよびサーバ ファームの設定」を参照してください。
`host1/Admin(config)# serverfarm SEC_20_SF`
`host1/Admin(config-sfarm-host)# rserver REAL1`
`host1/Admin(config-sfarm-host-rs)# inservice`
`host1/Admin(config-sfarm-host-rs)# exit`
`host1/Admin(config-sfarm-host)# rserver REAL2`
`host1/Admin(config-sfarm-host-rs)# inservice`
`host1/Admin(config-sfarm-host-rs)# exit`
`host1/Admin(config-sfarm-host)# rserver REAL3`
`host1/Admin(config-sfarm-host-rs)# inservice`
`host1/Admin(config-sfarm-host-rs)# exit`
`host1/Admin(config-sfarm-host)# exit`

表 6-2　ACE B のスタンダード FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

8. デフォルト クラス マップを使用して、トラフィックを VLAN 20 の HTTP サーバ ファームにロード バランシングするレイヤ 7 ポリシー マップを設定します。SLB のトラフィック ポリシー設定の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。
`host1/Admin(config)# policy-map type loadbalance first-match SEC_20_LB`
`host1/Admin(config-pmap-lb)# class class-default`
`host1/Admin(config-pmap-lb-c)# serverfarm SEC_20_SF`
`host1/Admin(config-pmap-lb-c)# exit`
`host1/Admin(config-pmap-lb)# exit`

9. VLAN 201 で設定された仮想 IP アドレス 200.1.1.1 に向かうトラフィックを分類するように、レイヤ 3 クラス マップを設定します。SLB のトラフィック ポリシー設定の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。
`host1/Admin(config)# class-map match-any SEC_20_VS`
`host1/Admin(config-cmap)# match virtual-address 200.1.1.1 255.255.0.0 any`
`host1/Admin(config-cmap)# exit`

10. レイヤ 3 ポリシー マップを設定し、それとレイヤ 3 クラス マップ（SEC_20_VS）およびレイヤ 7 ポリシー マップ（SEC_20_LB）を関連付けます。このステップによって、トラフィックを VLAN 20 の HTTP サーバにロード バランシングするポリシーが完成します。SLB のトラフィック ポリシー設定の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。
`host1/Admin(config)# policy-map multi-match POL_SEC_20`
`host1/Admin(config-pmap)# class SEC_20_VS`
`host1/Admin(config-pmap-c)# loadbalance vip inservice`
`host1/Admin(config-pmap-c)# loadbalance policy SEC_20_LB`

表 6-2　ACE B のスタンダード FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

11. VLAN 200 または VLAN 20 からインターネットに向かうトラフィックを VLAN 201 でファイアウォールの高セキュリティ側にロード バランシングするように、レイヤ 7 ポリシー マップを設定します。SLB のトラフィック ポリシー設定の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。
`host1/Admin(config)# policy-map type loadbalance first-match LB_FW_SEC`
`host1/Admin(config-pmap-lb)# class class-default`
`host1/Admin(config-pmap-lb-c)# serverfarm SF_SEC`
`host1/Admin(config-pmap-lb-c)# exit`
`host1/Admin(config-pmap-lb)# exit`

12. ファイアウォールの高セキュリティ側からインターネットに向かうすべてのトラフィックを分類するように、レイヤ 3 クラス マップを設定します。SLB のトラフィック ポリシー設定の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。
`host1/Admin(config)# class-map match-any FW_SEC_VIP`
`host1/Admin(config-cmap)# match virtual-address 0.0.0.0 0.0.0.0 any`
`host1/Admin(config-cmap)# exit`

13. レイヤ 3 ポリシー マップを設定し、それとレイヤ 7 ポリシー マップ（LB_FW_SEC）およびレイヤ 3 クラス マップ（FW_SEC_VIP）を関連付けます。VIP でロード バランシングを有効にします。このステップによって、ファイアウォールの高セキュリティ側からインターネットに向かうすべての要求をロード バランシングするポリシーが完成します。SLB のトラフィック ポリシー設定の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。
`host1/Admin(config)# policy-map multi-match POL_SEC`
`host1/Admin(config-pmap)# class FW_SEC_VIP`
`host1/Admin(config-pmap-c)# loadbalance vip inservice`
`host1/Admin(config-pmap-c)# loadbalance LB_FW_SEC`
`host1/Admin(config-pmap-c)# exit`
`host1/Admin(config-pmap)# exit`

表 6-2　ACE B のスタンダード FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

14. ファイアウォールの高セキュリティ側のインターフェイスを、インターネットから発信されてそのファイアウォールを通過するトラフィック用に設定します。ACE は、このインターフェイスを使用してファイアウォールからのトラフィックを捕捉し、それを HTTP サーバ ファームにロード バランシングして、リモート ホストにルーティングします。インターフェイスの設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*』を参照してください。
`host1/Admin(config)# interface vlan 201`
`host1/Admin(config-if)# ip address 100.201.1.201 255.255.0.0`
`host1/Admin(config-if)# access-group input ACL1`
`host1/Admin(config-if)# mac-sticky enable`
`host1/Admin(config-if)# service-policy input POL_SEC_20`
`host1/Admin(config-if)# no shutdown`
`host1/Admin(config-if)# exit`

15. ファイアウォールの高セキュリティ側のインターフェイスを、VLAN 20 の HTTP サーバ ファームからのトラフィック用に設定します。インターフェイスの設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*』を参照してください。
`host1/Admin(config)# interface vlan 20`
`host1/Admin(config-if)# ip address 20.1.1.20 255.255.255.0`
`host1/Admin(config-if)# access-group input ACL1`
`host1/Admin(config-if)# service-policy input POL_SEC`
`host1/Admin(config-if)# no shutdown`
`host1/Admin(config-if)# exit`

16. ファイアウォールの高セキュリティ側のインターフェイスを、VLAN 200 のリモート ホストからのトラフィック用に設定します。インターフェイスの設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*』を参照してください。
`host1/Admin(config)# interface vlan 200`
`host1/Admin(config-if)# ip address 200.1.1.200 255.255.255.0`
`host1/Admin(config-if)# access-group input ACL1`
`host1/Admin(config-if)# service-policy input POL_SEC`
`host1/Admin(config-if)# no shutdown`
`host1/Admin(config-if)# Ctrl-z`

表 6-2　ACE B のスタンダード FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

17. 次の **show** コマンドを使用して、FWLB の設定を確認します。
`host1/Admin# show running-config access-list`
`host1/Admin# show running-config class-map`
`host1/Admin# show running-config interface`
`host1/Admin# show running-config policy-map`
`host1/Admin# show running-config rserver`
`host1/Admin# show running-config serverfarm`

18.（任意）設定変更をフラッシュ メモリに保存します。 `host1/Admin# copy running-config startup-config`

ステルス ファイアウォール負荷分散の設定

この項では、ステルス FWLB 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。

- ステルス ファイアウォール負荷分散設定の概要
- ステルス ファイアウォール負荷分散設定のクイック スタート

（注）　ネットワーク内のファイアウォール デバイスの設定の詳細については、ご使用のファイアウォール製品に付属のマニュアルを参照してください。

ステルス ファイアウォール負荷分散設定の概要

（注）　ステルス FWLB の設定では、2 台の ACE を設定する必要があります。

このステルス FWLB の設定例では（図 6-2 を参照）、ACE A と ACE B が、3 つのファイアウォールを通じてトラフィックをロード バランシングします。サーバファーム内で実サーバとして設定された各ファイアウォールは、2 つの異なる VLAN に接続します。その 1 つはファイアウォールの低セキュリティ側、もう 1 つは高セキュリティ側にあります。ステルス ファイアウォールは、VLAN 上で IP アドレスを持ちません。エイリアス IP アドレスは、ファイアウォールが接続する各 ACE インターフェイスに設定します。ACE は、エイリアス IP アドレスを使用して、トラフィックを正しいファイアウォールへ送信します。

インターネットからイントラネットへのパスでは、トラフィックは、異なる VLAN（VLAN 101、VLAN 102、VLAN 103）からファイアウォールの低セキュリティ側に入り、それらの高セキュリティ側から別々の VLAN（VLAN 201、VLAN 202、VLAN 203）へ出て行きます。イントラネットからインターネットへのパスでは、フローは逆になります。他の VLAN は、次のロケーションへの接続を提供します。

- インターネット（VLAN 100）
- リモート ホスト（VLAN 200）
- イントラネット サーバ ファーム（VLAN 20）

ステルス ファイアウォール負荷分散設定のクイック スタート

ここでは、2 台の ACE アプライアンスでステルス FWLB を設定するためのステップバイステップ手順を含んだクイック スタート表を提供します。次の内容について説明します。

- ACE A のステルス FWLB 設定のクイック スタート
- ACE B のステルス FWLB 設定のクイック スタート

ACE A のステルス FWLB 設定のクイック スタート

表 6-3 は、ACE A（低セキュリティ側）でステルス FWLB を設定するために必要な手順の概要を示しています。各ステップには、作業の完了に必要な CLI コマンドが示されています。

表 6-3　ACE A のステルス FWLB 設定のクイック スタート

作業およびコマンドの例

1. 複数のコンテキストを使用している場合は、CLI プロンプトに注意し、目的のコンテキスト内で作業を実行していることを確認します。必要な場合は、正しいコンテキストに変更するか、または正しいコンテキストに直接ログインしてください。
`host1/Admin# changeto C1`
`host1/C1#`
この表の以降の例では、特に記載がない限り、管理コンテキストが使用されています。コンテキストの作成に関する詳細は、『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照してください。

2. コンフィギュレーション モードを開始します。
`host1/Admin# config`
`Enter configuration commands, one per line. End with CNTL/Z`
`host1/Admin(config)#`

表 6-3　ACE A のステルス FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

3. ACL を設定して ACE へのトラフィックを許可します。ACL は、アプリケーションのニーズに合わせて修正できます。ACL の設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照してください。
`host1/Admin(config)# access-list ACL1 line 10 extended permit ip any any`
`host1/Admin(config-acl)# exit`

4. 3 台の実サーバで、VLAN 101、102、および 103 に属するファイアウォールの低セキュリティ側を設定します。実サーバの設定の詳細については、第 2 章「実サーバおよびサーバ ファームの設定」を参照してください。
`host1/Admin(config)# rserver FW_INSEC_1`
`host1/Admin(config-rserver-host)# ip address 101.0.201.100`
`host1/Admin(config-rserver-host)# inservice`
`host1/Admin(config-rserver-host)# exit`
 	
`host1/Admin(config)# rserver FW_INSEC_2`
`host1/Admin(config-rserver-host)# ip address 101.0.202.100`
`host1/Admin(config-rserver-host)# inservice`
`host1/Admin(config-rserver-host)# exit`
 	
`host1/Admin(config)# rserver FW_INSEC_3`
`host1/Admin(config-rserver-host)# ip address 101.0.203.100`
`host1/Admin(config-rserver-host)# inservice`
`host1/Admin(config-rserver-host)# exit`

表 6-3　ACE A のステルス FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

5. ファイアウォールの低セキュリティ側（インターネット）からの接続を処理するようにサーバ ファームを設定します。ACE は、ハッシュ アドレス送信元プレディクタを使用して、送信元 IP アドレスに基づいてファイアウォールを選択します。サーバ ファームの設定の詳細については、第 2 章「実サーバおよびサーバ ファームの設定」を参照してください。
`host1/Admin(config)# serverfarm SF_INSEC`
`host1/Admin(config-sfarm-host)# transparent`
`host1/Admin(config-sfarm-host)# predictor hash address source 255.255.255.255`
`host1/Admin(config-sfarm-host)# rserver FW_INSEC_1`
`host1/Admin(config-sfarm-host-rs)# inservice`
`host1/Admin(config-sfarm-host-rs)# exit`
`host1/Admin(config-sfarm-host)# rserver FW_INSEC_2`
`host1/Admin(config-sfarm-host-rs)# inservice`
`host1/Admin(config-sfarm-host-rs)# exit`
`host1/Admin(config-sfarm-host)# rserver FW_INSEC_3`
`host1/Admin(config-sfarm-host-rs)# inservice`
`host1/Admin(config-sfarm-host-rs)# exit`
`host1/Admin(config-sfarm-host)# exit`

6. ファイアウォールから受信したパケットをインターネットに転送するように、レイヤ 7 ロード バランシング ポリシー マップを設定します。そのポリシー マップとデフォルト クラス マップを関連付けます。SLB のトラフィック ポリシー設定の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。
`host1/Admin(config)# policy-map type loadbalance first-match FORWARD_FW_INSEC`
`host1/Admin(config-pmap-lb)# class class-default`
`host1/Admin(config-pmap-lb-c)# forward`
`host1/Admin(config-pmap-lb-c)# exit`
`host1/Admin(config-pmap-lb)# exit`

7. ファイアウォールの低セキュリティ側の VLAN 101、102、および 103 ですべての VIP アドレス、ネットマスク、およびプロトコルにマッチするファイアウォールからのトラフィックを分類するように、レイヤ 3 クラス マップを設定します。
`host1/Admin(config)# class-map match-any FORWARD_VIP`
`host1/Admin(config-cmap)# match virtual-address 0.0.0.0 0.0.0.0 any`
`host1/Admin(config-cmap)# exit`

表 6-3　ACE A のステルス FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

8. レイヤ 3 ポリシー マップを設定し、それとレイヤ 3 フォワーディング クラス マップ（FORWARD_VIP）およびレイヤ 7 フォワーディング ポリシー マップ（FORWARD_FW_INSEC）を関連付けて、フォワーディング ポリシー設定を完了します。
 	
`host1/Admin(config)# policy-map multi-match FORWARD_INSEC`
`host1/Admin(config-pmap)# class FORWARD_VIP`
`host1/Admin(config-pmap-c)# loadbalance vip inservice`
`host1/Admin(config-pmap-c)# loadbalance policy FORWARD_FW_INSEC`
`host1/Admin(config-pmap-c)# exit`
`host1/Admin(config-pmap)# exit`

9. インターネットからの要求がサーバ ファーム SF-INSEC にバランシングされるように、レイヤ 7 ロード バランシング ポリシー マップを設定します。そのポリシー マップとデフォルト クラス マップおよびサーバ ファーム SF-INSEC を関連付けます。
 	
`host1/Admin(config)# policy-map type loadbalance first-match LB-FW-INSEC`
`host1/Admin(config-pmap-lb)# class class-default`
`host1/Admin(config-pmap-lb-c)# serverfarm SF_INSEC`
`host1/Admin(config-pmap-lb-c)# exit`
`host1/Admin(config-pmap-lb)# exit`

10. ファイアウォールの低セキュリティ側の VLAN 100 で VIP アドレス 200.1.1.1、ネットマスク 255.255.0.0、およびすべてのプロトコルにマッチするインターネットからのトラフィックを分類するように、レイヤ 3 クラス マップを設定します。
 	
`host1/Admin(config)# class-map match-any FW_VIP`
`host1/Admin(config-cmap)# match virtual-address 200.1.1.1 255.255.0.0 any`
`host1/Admin(config-cmap)# exit`

11. レイヤ 3 ポリシー マップを設定し、それとレイヤ 3 クラス マップ（FW-VIP）およびレイヤ 7 ポリシー マップ（LB_FW_INSEC）を関連付けて、ロード バランシング ポリシー設定を完了します。
 	
`host1/Admin(config)# policy-map multi-match POL_INSEC`
`host1/Admin(config-pmap)# class FW_VIP`
`host1/Admin(config-pmap-c)# loadbalance vip inservice`
`host1/Admin(config-pmap-c)# loadbalance policy LB_FW_INSEC`
`host1/Admin(config-pmap-c)# exit`
`host1/Admin(config-pmap)# exit`

表 6-3　ACE A のステルス FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

12. インターネットからのトラフィックを受信し、そのトラフィックをファイアウォールの低セキュリティ側にロード バランシングするために ACE で使用するインターフェイスを設定します。ACL（ACL1）とレイヤ 3 ポリシー（POL_INSEC）を、そのインターフェイスに適用します。インターフェイスの設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*』を参照してください。
`host1/Admin(config)# interface vlan 100`
`host1/Admin(config-if)# ip address 100.100.1.100 255.255.0.0`
`host1/Admin(config-if)# access-group input ACL1`
`host1/Admin(config-if)# service-policy input POL_INSEC`
`host1/Admin(config-if)# no shutdown`
`host1/Admin(config-if)# exit`

13. トラフィックを FW1 にロード バランシングし、イントラネットからのトラフィックを受信するために ACE A で使用するファイアウォールの低セキュリティ側のインターフェイスを設定します。インターフェイスの設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*』を参照してください。
`host1/Admin(config)# interface vlan 101`
`host1/Admin(config-if)# ip address 101.0.101.10 255.255.255.0`
`host1/Admin(config-if)# alias 101.0.101.100 255.255.255.0`
`host1/Admin(config-if)# access-group input ACL1`
`host1/Admin(config-if)# mac-sticky enable`
`host1/Admin(config-if)# service-policy input FORWARD_INSEC`
`host1/Admin(config-if)# no shutdown`
`host1/Admin(config-if)# exit`

14. トラフィックを FW2 にロード バランシングし、イントラネットからのトラフィックを受信するために ACE A で使用するファイアウォールの低セキュリティ側のインターフェイスを設定します。インターフェイスの設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*』を参照してください。
`host1/Admin(config)# interface vlan 102`
`host1/Admin(config-if)# ip address 101.0.102.20 255.255.255.0`
`host1/Admin(config-if)# alias 101.0.102.100 255.255.255.0`
`host1/Admin(config-if)# access-group input ACL1`
`host1/Admin(config-if)# mac-sticky enable`
`host1/Admin(config-if)# service-policy input FORWARD_INSEC`
`host1/Admin(config-if)# no shutdown`
`host1/Admin(config-if)# exit`

表 6-3　ACE A のステルス FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

15. トラフィックを FW3 にロード バランシングし、イントラネットからのトラフィックを受信するために ACE A で使用するファイアウォールの低セキュリティ側のインターフェイスを設定します。インターフェイスの設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*』を参照してください。
`host1/Admin(config)# interface vlan 103`
`host1/Admin(config-if)# ip address 101.0.103.30 255.255.255.0`
`host1/Admin(config-if)# alias 101.0.103.100 255.255.255.0`
`host1/Admin(config-if)# access-group input ACL1`
`host1/Admin(config-if)# mac-sticky enable`
`host1/Admin(config-if)# service-policy input FORWARD_INSEC`
`host1/Admin(config-if)# no shutdown`
`host1/Admin(config-if)# Ctrl-z`

16. 次の **show** コマンドを使用して、FWLB の設定を確認します。
`host1/Admin# show running-config access-list`
`host1/Admin# show running-config class-map`
`host1/Admin# show running-config interface`
`host1/Admin# show running-config policy-map`
`host1/Admin# show running-config rserver`
`host1/Admin# show running-config serverfarm`

17.（任意）設定変更をフラッシュ メモリに保存します。 `host1/Admin# copy running-config startup-config`

ACE B のステルス FWLB 設定のクイック スタート

表 6-4 は、ACE B（高セキュリティ側）でステルス FWLB を設定するために必要な手順の概要を示しています。各ステップには、作業の完了に必要な CLI コマンドが示されています。

表 6-4　ACE B のステルス FWLB 設定のクイック スタート

作業およびコマンドの例

1. 複数のコンテキストを使用している場合は、CLI プロンプトに注意し、目的のコンテキスト内で作業を実行していることを確認します。必要な場合は、正しいコンテキストに変更するか、または正しいコンテキストに直接ログインしてください。
`host1/Admin# changeto C1`
`host1/C1#`
この表の以降の例では、特に記載がない限り、管理コンテキストが使用されています。コンテキストの作成に関する詳細は、『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照してください。

2. コンフィギュレーション モードを開始します。
`host1/Admin# config`
`Enter configuration commands, one per line. End with CNTL/Z`
`host1/Admin(config)#`

3. ACL を設定して ACE へのトラフィックを許可します。ACL は、アプリケーションのニーズに合わせて修正できます。ACL の設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照してください。
`host1/Admin(config)# access-list ACL1 line 10 extended permit ip any any`
`host1/Admin(config-acl)# exit`

表 6-4　ACE B のステルス FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

4. 3 台の実サーバで、VLAN 201、202、および 203 に属するファイアウォールの高セキュリティ側を設定します。実サーバの設定の詳細については、第 2 章「実サーバおよびサーバ ファームの設定」を参照してください。
`host1/Admin(config)# rserver FW_SEC_1`
`host1/Admin(config-rserver-host)# ip address 101.0.101.100`
`host1/Admin(config-rserver-host)# inservice`
`host1/Admin(config-rserver-host)# exit`
 	
`host1/Admin(config)# rserver FW_SEC_2`
`host1/Admin(config-rserver-host)# ip address 101.0.102.100`
`host1/Admin(config-rserver-host)# inservice`
`host1/Admin(config-rserver-host)# exit`
 	
`host1/Admin(config)# rserver FW_SEC_3`
`host1/Admin(config-rserver-host)# ip address 101.0.103.100`
`host1/Admin(config-rserver-host)# inservice`
`host1/Admin(config-rserver-host)# exit`

5. ファイアウォールの高セキュリティ側（イントラネット）からの接続を処理するようにサーバ ファームを設定します。この場合、ACE は、ハッシュ アドレス宛先プレディクタを使用して、宛先 IP アドレスに基づいてファイアウォールを選択します。このプレディクタによって、ACE は、リターン フローおよび関連する接続に対して同じファイアウォールを選択できます。たとえば、FTP の場合、制御チャネルとデータ チャネルがいずれも同じファイアウォールを通過できます。サーバ ファームの設定の詳細については、第 2 章「実サーバおよびサーバ ファームの設定」を参照してください。
`host1/Admin(config)# serverfarm SF_SEC`
`host1/Admin(config-sfarm-host)# transparent`
`host1/Admin(config-sfarm-host)# predictor hash address destination 255.255.255.255`
`host1/Admin(config-sfarm-host)# rserver FW_SEC_1`
`host1/Admin(config-sfarm-host)# inservice`
`host1/Admin(config-sfarm-host)# rserver FW_SEC_2`
`host1/Admin(config-sfarm-host)# inservice`
`host1/Admin(config-sfarm-host)# rserver FW_SEC_3`
`host1/Admin(config-sfarm-host)# inservice`
`host1/Admin(config-sfarm-host)# exit`

表 6-4　ACE B のステルス FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

6. ファイアウォールの高セキュリティ側の VLAN 20 でコンテンツをロードバランシングするように 3 台の実サーバを設定します。実サーバの設定の詳細については、第 2 章「実サーバおよびサーバ ファームの設定」を参照してください。
`host1/Admin(config)# rserver REAL1`
`host1/Admin(config-rserver-host)# ip address 20.1.1.1`
`host1/Admin(config-rserver-host)# inservice`
`host1/Admin(config-rserver-host)# exit`
 	
`host1/Admin(config)# rserver REAL2`
`host1/Admin(config-rserver-host)# ip address 20.1.1.2`
`host1/Admin(config-rserver-host)# inservice`
`host1/Admin(config-rserver-host)# exit`
 	
`host1/Admin(config)# rserver REAL3`
`host1/Admin(config-rserver-host)# ip address 20.1.1.3`
`host1/Admin(config-rserver-host)# inservice`
`host1/Admin(config-rserver-host)# exit`

7. 要求が VLAN 20 の HTTP サーバにロード バランシングされるように、HTTP サーバの標準的なサーバ ファームを設定します。サーバ ファームの設定の詳細については、第 2 章「実サーバおよびサーバ ファームの設定」を参照してください。
`host1/Admin(config)# serverfarm SEC_20_SF`
`host1/Admin(config-sfarm-host)# rserver REAL1`
`host1/Admin(config-sfarm-host-rs)# inservice`
`host1/Admin(config-sfarm-host-rs)# exit`
`host1/Admin(config-sfarm-host)# rserver REAL2`
`host1/Admin(config-sfarm-host-rs)# inservice`
`host1/Admin(config-sfarm-host-rs)# exit`
`host1/Admin(config-sfarm-host)# rserver REAL3`
`host1/Admin(config-sfarm-host-rs)# inservice`
`host1/Admin(config-sfarm-host-rs)# exit`
`host1/Admin(config-sfarm-host)# exit`

表 6-4　ACE B のステルス FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

8. デフォルト クラス マップを使用して、トラフィックを VLAN 20 の HTTP サーバ ファームにロード バランシングするレイヤ 7 ポリシー マップを設定します。SLB のトラフィック ポリシー設定の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。
`host1/Admin(config)# policy-map type loadbalance first-match SEC_20_LB`
`host1/Admin(config-pmap-lb)# class class-default`
`host1/Admin(config-pmap-lb-c)# serverfarm SEC_20_SF`
`host1/Admin(config-pmap-lb-c)# exit`
`host1/Admin(config-pmap-lb)# exit`

9. VLAN 201、202、および 203 で仮想 IP アドレス 200.1.1.1 に向かうトラフィックを分類するように、レイヤ 3 クラス マップを設定します。SLB のトラフィック ポリシー設定の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。
`host1/Admin(config)# class-map match-any SEC_20_VS`
`host1/Admin(config-cmap)# match virtual-address 200.1.1.1 255.255.0.0 any`
`host1/Admin(config-cmap)# exit`

10. レイヤ 3 ポリシー マップを設定し、それとレイヤ 3 クラス マップ（SEC_20_VS）およびレイヤ 7 ポリシー マップ（SEC_20_LB）を関連付けます。このステップによって、トラフィックを VLAN 20 の HTTP サーバにロード バランシングするポリシーが完成します。SLB のトラフィック ポリシー設定の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。
`host1/Admin(config)# policy-map multi-match POL_SEC_20`
`host1/Admin(config-pmap)# class SEC_20_VS`
`host1/Admin(config-pmap-c)# loadbalance vip inservice`
`host1/Admin(config-pmap-c)# loadbalance policy SEC_20_LB`
`host1/Admin(config-pmap-c)# exit`
`host1/Admin(config-pmap)# exit`

表 6-4　ACE B のステルス FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

11. VLAN 200 または VLAN 20 からインターネットに向かう要求を VLAN 201 でファイアウォールの高セキュリティ側にロード バランシングするように、レイヤ 7 ポリシー マップを設定します。SLB のトラフィック ポリシー設定の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。
`host1/Admin(config)# policy-map type loadbalance first-match LB_FW_SEC`
`host1/Admin(config-pmap-lb)# class class-default`
`host1/Admin(config-pmap-lb-c)# serverfarm SF_SEC`
`host1/Admin(config-pmap-lb-c)# exit`
`host1/Admin(config-pmap-lb)# exit`

12. ファイアウォールの高セキュリティ側からのすべてのトラフィック（あらゆる IP アドレス、ネットマスク、およびプロトコル）を分類するように、レイヤ 3 クラス マップを設定します。SLB のトラフィック ポリシー設定の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。
`host1/Admin(config)# class-map match-any FW_SEC_VIP`
`host1/Admin(config-cmap)# match virtual-address 0.0.0.0 0.0.0.0 any`
`host1/Admin(config-cmap)# exit`

13. レイヤ 3 ポリシー マップを設定し、それとレイヤ 7 ポリシー マップ（LB_FW_SEC）およびレイヤ 3 クラス マップ（FW_SEC_VIP）を関連付けます。VIP でロード バランシングを有効にします。このステップによって、ファイアウォールの高セキュリティ側からインターネットに向かうすべての要求をロード バランシングするポリシーが完成します。SLB のトラフィック ポリシー設定の詳細については、第 3 章「サーバ ロード バランシングに関するトラフィック ポリシーの設定」を参照してください。
`host1/Admin(config)# policy-map multi-match POL_SEC`
`host1/Admin(config-pmap)# class FW_SEC_VIP`
`host1/Admin(config-pmap-c)# loadbalance vip inservice`
`host1/Admin(config-pmap-c)# loadbalance policy LB_FW_SEC`
`host1/Admin(config-pmap-c)# exit`
`host1/Admin(config-pmap)# exit`

表 6-4　ACE B のステルス FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

14. トラフィックをイントラネットから FW1 に送信するため、そしてインターネットから発信されてファイアウォールを通過するトラフィックを受信するために ACE で使用するファイアウォールの高セキュリティ側のインターフェイスを設定します。インターフェイスの設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*』を参照してください。
`host1/Admin(config)# interface vlan 201`
`host1/Admin(config-if)# ip address 101.0.201.10 255.255.255.0`
`host1/Admin(config-if)# alias 101.0.201.100 255.255.255.0`
`host1/Admin(config-if)# access-group input ACL1`
`host1/Admin(config-if)# mac-sticky enable`
`host1/Admin(config-if)# service-policy input POL_SEC_20`
`host1/Admin(config-if)# no shutdown`
`host1/Admin(config-if)# exit`

15. トラフィックをイントラネットから FW2 に送信するため、およびインターネットから発信されてファイアウォールを通過するトラフィックを受信するために ACE で使用するファイアウォールの高セキュリティ側のインターフェイスを設定します。インターフェイスの設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*』を参照してください。
`host1/Admin(config)# interface vlan 202`
`host1/Admin(config-if)# ip address 101.0.202.20 255.255.255.0`
`host1/Admin(config-if)# alias 101.0.202.100 255.255.255.0`
`host1/Admin(config-if)# access-group input ACL1`
`host1/Admin(config-if)# mac-sticky enable`
`host1/Admin(config-if)# service-policy input POL_SEC_20`
`host1/Admin(config-if)# no shutdown`
`host1/Admin(config-if)# exit`

表 6-4　ACE B のステルス FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

16. トラフィックをイントラネットから FW3 に送信するため、およびインターネットから発信されてファイアウォールを通過するトラフィックを受信するために ACE で使用するファイアウォールの低セキュリティ側のインターフェイスを設定します。インターフェイスの設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*』を参照してください。
`host1/Admin(config)# interface vlan 203`
`host1/Admin(config-if)# ip address 101.0.203.30 255.255.255.0`
`host1/Admin(config-if)# alias 101.0.203.100 255.255.255.0`
`host1/Admin(config-if)# access-group input ACL1`
`host1/Admin(config-if)# mac-sticky enable`
`host1/Admin(config-if)# service-policy input POL_SEC_20`
`host1/Admin(config-if)# no shutdown`
`host1/Admin(config-if)# exit`

17. VLAN 200 のリモート ホストからインターネットに向かうトラフィックを受信するために ACE で使用するインターフェイスを設定します。ACL（ACL1）とレイヤ 3 ポリシー マップ（POL_SEC）を、そのインターフェイスに適用します。インターフェイスの設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*』を参照してください。
`host1/Admin(config)# interface vlan 200`
`host1/Admin(config-if)# ip address 200.1.1.200 255.255.255.0`
`host1/Admin(config-if)# access-group input ACL1`
`host1/Admin(config-if)# service-policy input POL_SEC`
`host1/Admin(config-if)# no shutdown`
`host1/Admin(config-if)# exit`

18. VLAN 20 の HTTP サーバ ファームからインターネットに向かうトラフィックを受信するために ACE で使用するインターフェイスを設定します。ACL（ACL1）とレイヤ 3 ポリシー マップ（POL_SEC）を、そのインターフェイスに適用します。インターフェイスの設定の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*』を参照してください。
`host1/Admin(config)# interface vlan 20`
`host1/Admin(config-if)# ip address 20.100.1.100 255.255.0.0`
`host1/Admin(config-if)# access-group input ACL1`
`host1/Admin(config-if)# service-policy input POL_SEC`
`host1/Admin(config-if)# no shutdown`
`host1/Admin(config-if)# Ctrl-z`

表 6-4　ACE B のステルス FWLB 設定のクイック スタート（続き）

作業およびコマンドの例

19. 次の **show** コマンドを使用して、FWLB の設定を確認します。
`host1/Admin# show running-config access-list`
`host1/Admin# show running-config class-map`
`host1/Admin# show running-config interface`
`host1/Admin# show running-config policy-map`
`host1/Admin# show running-config rserver`
`host1/Admin# show running-config serverfarm`

20.（任意）設定変更をフラッシュ メモリに保存します。 `host1/Admin# copy running-config startup-config`

FWLB 設定の表示

EXEC モードで **show running-config** コマンドを使用することによって、実行コンフィギュレーション全体を表示できます。このコマンドの構文は次のとおりです。

show running-config

実行コンフィギュレーションの FWLB に関連したセクションを表示するには、EXEC モードで次のコマンドを使用します。

- **show running-config access-list**
- **show running-config class-map**
- **show running-config interface**
- **show running-config policy-map**
- **show running-config rserver**
- **show running-config serverfarm**

ファイアウォール負荷分散の設定例

この項では、スタンダードおよびステルス FWLB の設定例を示します。具体的な内容は次のとおりです。

- スタンダード ファイアウォール負荷分散の設定例
- ステルス ファイアウォールの設定例

スタンダード ファイアウォール負荷分散の設定例

次の例は、実行コンフィギュレーションのスタンダード FWLB に関連した部分を示しています。この設定は、2 台の ACE アプライアンスと、その間に配置されたファイアウォールに基づきます（図 6-1）。スタンダード FWLB は、ACE が 1 台だけでも設定できます。

ACE A のコンフィギュレーション — スタンダード ファイアウォール負荷分散

```
access-list ACL1 line 10 extended permit ip any any

rserver host FW_INSEC_1
  ip address 100.101.1.1
  inservice
rserver host FW_INSEC_2
  ip address 100.101.1.2
  inservice
rserver host FW_INSEC_3
  ip address 100.101.1.3
  inservice

serverfarm INSEC_SF
  transparent
  predictor hash address source 255.255.255.255
  rserver FW_INSEC_1
    inservice
  rserver FW_INSEC_2
    inservice
  rserver FW_INSEC_3
    inservice

class-map match-any FW_VIP
  10 match virtual-address 200.1.1.1 255.255.0.0 any
policy-map type loadbalance first-match LB_FW_INSEC
```

```
  class class-default
    serverfarm INSEC_SF
policy-map multi-match POL_INSEC
  class FW_VIP
    loadbalance vip inservice
    loadbalance policy LB_FW_INSEC

interface vlan 100
  ip addr 100.100.1.100 255.255.0.0
  access-group input ACL1
  service-policy input POL_INSEC
  no shutdown
interface vlan 101
  ip addr 100.101.1.101 255.255.0.0
  access-group input ACL1
  mac-sticky enable
  service-policy input POL_INSEC
  no shutdown
```

ACE B のコンフィギュレーション — スタンダード ファイアウォール負荷分散

```
access-list ACL1 line 10 extended permit ip any any

rserver FW_SEC_1
  ip address 100.201.1.1
  inservice
rserver FW_SEC_2
  ip address 100.201.1.2
  inservice
rserver FW_SEC_3
  ip address  100.201.1.3
  inservice

rserver REAL1
  ip address 20.1.1.1
  inservice
rserver REAL2
  ip address 20.1.1.2
  inservice
rserver REAL3
  ip address 20.1.1.3
  inservice

serverfarm SEC_SF
  predictor hash address destination 255.255.255.255
  transparent
  rserver FW_SEC_1
```

```
    inservice
  rserver FW_SEC_2
    inservice
  rserver FW_SEC_3
    inservice

serverfarm SEC_20_SF
  rserver REAL1
    inservice
  rserver REAL2
    inservice
  rserver REAL3
    inservice

class-map match-any SEC_20_VS
  10 match virtual-address 200.1.1.1 255.255.0.0 any
class-map match any FW_SEC_VIP
  10 match virtual-address 0.0.0.0 0.0.0.0 any

policy-map type loadbalance first-match SEC_20_LB
  class class-default
    serverfarm SEC_20_SF
policy-map multi-match POL_SEC_20
  class SEC_20_VS
    loadbalance vip inservice
    loadbalance policy SEC_20_LB

policy-map type loadbalance first-match LB_FW_SEC
  class class-default
    serverfarm SEC_SF
policy-map multi-match POL_SEC
  class FW_SEC_VIP
    loadbalance vip inservice
    loadbalance policy LB_FW_SEC

interface vlan 201
  ip address 100.201.1.201 255.255.0.0
  access-group input ACL1
  mac-sticky enable
  service-policy input POL_SEC_20
  no shutdown
interface vlan 20
  ip address 20.1.1.20 255.255.255.0
  access-group input ACL1
  service-policy input POL_SEC
  no shutdown
interface vlan 200
  ip address 200.1.1.200 255.255.255.0
```

```
  access-group input ACL1
  service-policy input POL_SEC
  no shutdown
```

ステルス ファイアウォールの設定例

次の例は、実行コンフィギュレーションのステルス FWLB に関連した部分を示しています。この設定は、2 台の ACE アプライアンスを必要とします。

ACE A のコンフィギュレーション ― ステルス ファイアウォール負荷分散

```
access-list ACL1 line 10 extended permit ip any any

rserver FW_INSEC_1
  ip address 101.0.201.100
  inservice
rserver FW_INSEC_2
  ip address 101.0.202.100
  inservice
rserver FW_INSEC_3
  ip address 101.0.203.100
  inservice

serverfarm INSEC_SF
  transparent
  predictor hash address source 255.255.255.255
  rserver FW_INSEC_1
    inservice
  rserver FW_INSEC_2
    inservice
  rserver FW_INSEC_3
    inservice

class-map match-any FORWARD-VIP
  10 match virtual-address 0.0.0.0 0.0.0.0 any
class-map match-any FW_VIP
  10 match virtual-address 200.1.1.1 255.255.0.0 any
policy-map type loadbalance first-match FORWARD_FW_INSEC
  class class-default
    forward
policy-map type loadbalance first-match LB_FW_INSEC
  class class-default
    serverfarm INSEC_SF
policy-map multi-match FORWARD_INSEC
  class FORWARD_VIP
```

```
    loadbalance vip inservice
    loadbalance policy FORWARD_FW_INSEC
policy-map multi-match POL_INSEC
  class FW_VIP
    loadbalance vip inservice
    loadbalance policy LB_FW_INSEC

interface vlan 100
  ip address 100.100.1.10 255.255.0.0
  access-group input ACL1
  service-policy input POL_INSEC
  no shutdown
interface vlan 101
  ip address 101.0.101.10 255.255.255.0
  alias 101.0.101.100 255.255.255.0
  access-group input ACL1
  service-policy input FORWARD_INSEC
  no shutdown
interface vlan 102
  ip address 101.0.102.20 255.255.255.0
  alias 101.0.102.100 255.255.255.0
  access-group input ACL1
  service-policy input FORWARD_INSEC
  no shutdown
interface vlan 103
  ip address 101.0.103.30 255.255.0.0
  alias 101.0.103.100 255.255.255.0
  access-group input ACL1
  service-policy input FORWARD_INSEC
  no shutdown
```

ACE B のコンフィギュレーション ― ステルス ファイアウォール負荷分散

```
access-list ACL1 line 10 extended permit ip any any

rserver host REAL1
  ip address 20.1.1.1
  inservice
rserver host REAL2
  ip address 20.1.1.2
  inservice
rserver host REAL3
  ip address 20.1.1.3
  inservice

rserver host FW_SEC_1
  ip address 101.0.101.100
  inservice
rserver host FW_SEC_2
  ip address 101.0.102.100
  inservice
rserver host FW_SEC_3
  ip address 101.0.103.100
  inservice

serverfarm SEC_20_SF
  rserver REAL1
    inservice
  rserver REAL2
    inservice
  rserver REAL3
    inservice
serverfarm SEC_SF
  transparent
  predictor hash address destination 255.255.255.255
  rserver FW_SEC_1
    inservice
  rserver FW_SEC_2
    inservice
  rserver FW_SEC_3
    inservice

class-map match-any SEC_20_VS
  10 match virtual-address 200.1.1.1 255.255.0.0 any
class-map match-any FW_SEC_VIP
  10 match virtual-address 0.0.0.0 0.0.0.0 any

policy-map type loadbalance first-match SEC_20_LB
  class class-default
```

```
    serverfarm SEC_20_SF
policy-map type loadbalance first-match LB_FW_SEC
  class class-default
    serverfarm SEC_SF
policy-map multi-match POL_SEC_20
  class SEC_20_VS
    loadbalance vip inservice
    loadbalance policy SEC_20_LB
policy-map multi-match POL_SEC
  class FW_SEC_VIP
    loadbalance vip inservice
    loadbalance policy LB_FW_SEC

interface vlan 201
  ip address 101.0.201.10 255.255.255.0
  alias 101.0.201.100 255.255.255.0
  access-group input ACL1
  mac-sticky enable
  service-policy input POL_SEC_20
  no shutdown
interface vlan 202
  ip address 101.0.202.20 255.255.255.0
  alias 101.0.202.100 255.255.255.0
  access-group input ACL1
  mac-sticky enable
  service-policy input POL_SEC_20
  no shutdown
interface vlan 203
  ip address 101.0.203.30 255.255.0.0
  alias 101.0.203.100 255.255.255.0
  access-group input ACL1
  mac-sticky enable
  service-policy input POL_SEC_20
  no shutdown
interface vlan 20
  ip address 20.100.1.100 255.255.0.0
  access-group input ACL1
  service-policy input POL_SEC
  no shutdown
interface vlan 200
  ip address 200.1.1.200 255.255.255.0
  access-group input ACL1
  service-policy input POL_SEC
  no shutdown
```

次の作業

Toolkit Command Language（TCL）スクリプトを ACE で使用する場合は、付録 A「ACE での TCL スクリプトの使用」を参照してください。

次の作業