



ファイアウォール ロードバランシング の設定

この章では、ファイアウォール ロードバランシングの設定方法について説明します。

- [ファイアウォールの機能 \(p.13-2\)](#)
- [ステルス ファイアウォール ロードバランシングの設定 \(p.13-8\)](#)
- [標準ファイアウォール ロードバランシングの設定 \(p.13-18\)](#)
- [ファイアウォール用リバーススティッキの設定 \(p.13-27\)](#)
- [ステートフル ファイアウォール接続のリマッピングの設定 \(p.13-30\)](#)

ファイアウォール ロードバランシングを使用すると、接続単位で複数のファイアウォールにトラフィックを分散させることによって、ファイアウォールの保護を拡張することができます。特定の接続に属すパケットはすべて、同じファイアウォールに送られなければなりません。ファイアウォールが個々のパケットについて、ファイアウォールのインターフェイスを通過することを許可または拒否します。

ファイアウォールの機能

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など）の間に物理的な境界を形成します。ファイアウォールは一方（インターネット）からパケットを受け付け、そのパケットを他方（イントラネット）に送り出します。ファイアウォールはパケットを変更してから渡すことも、そのまま送り出すこともできます。ファイアウォールがパケットを拒否する場合、通常はパケットを廃棄し、パケット廃棄をイベントとして記録します。

セッションが確立され、パケット フローが開始されると、ファイアウォールはそのファイアウォールに設定されているポリシーに従って、フロー内の各パケットをモニタするか、またはモニタしないでフローを流し続けます。

この章の内容は、次のとおりです。

- [ファイアウォールのタイプ \(p.13-2\)](#)
- [Content Switching Module with SSL \(CSM-S\) によるファイアウォールへのトラフィック分散 \(p.13-2\)](#)
- [サポート対象のファイアウォール \(p.13-3\)](#)
- [ファイアウォールに対するレイヤ 3 ロードバランシング \(p.13-3\)](#)
- [ファイアウォール構成タイプ \(p.13-3\)](#)
- [ファイアウォール用 IP リバーススティッキ \(p.13-4\)](#)
- [CSM-S のファイアウォール設定 \(p.13-4\)](#)
- [フォールトトレラントな CSM-S ファイアウォール設定 \(p.13-7\)](#)

ファイアウォールのタイプ

ファイアウォールの基本的なタイプは、次のとおりです。

- 標準ファイアウォール
- ステルス ファイアウォール

標準ファイアウォールは、ネットワーク上でその存在が認識されます。装置として宛先になれるように、また、ネットワーク上の他の装置によって認識されるように、IP アドレスが割り当てられます。

ステルス ファイアウォールは、ネットワーク上でその存在が認識されません。したがって、IP アドレスは割り当てられず、宛先になることも、ネットワーク上の他の装置に認識されることもありません。ネットワークにとって、ステルス ファイアウォールは配線の一部です。

どちらのファイアウォール タイプも、(ネットワークの保護された側と保護されていない側の間で) 双方向に流れるトラフィックを検証し、ユーザが定義したポリシー セットに基づいて、パケットを受け付けるか、または拒否します。

Content Switching Module with SSL (CSM-S) によるファイアウォールへのトラフィック分散

CSM-S は、サーバ ファーム内に設定されている装置にトラフィックの負荷を分散させます。対象となる装置はサーバ、ファイアウォール、またはエイリアス IP アドレスを含め、IP アドレス指定が可能なあらゆるオブジェクトです。CSM-S は装置タイプに関係なく、ロードバランス アルゴリズムを使用して、サーバ ファーム内で設定されている装置間でトラフィックをどのように分散させるかを決定します。



(注) 上位レイヤのロードバランス アルゴリズムとサーバ アプリケーション間の相互作用を考えると、ファイアウォールが含まれるサーバ ファームにレイヤ 3 ロードバランシングを設定することを推奨します。

サポート対象のファイアウォール

CSM-S は、標準ファイアウォールまたはステルス ファイアウォールにトラフィックの負荷を分散させることができます。

標準ファイアウォールでは、CSM-S がサーバにトラフィックを分散させる場合と同様、単一またはペアの CSM-S が固有の IP アドレスを持つファイアウォール間でトラフィックを分散させます。

ステルス ファイアウォールの場合、CSM-S はステルス ファイアウォール経由のパスを提供する別の CSM-S 上の、固有の VLAN (仮想 LAN) 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分散させます。ステルス ファイアウォールは、その VLAN 上を双方向に流れるあらゆるトラフィックがファイアウォールを通過するように設定します。

ファイアウォールに対するレイヤ 3 ロードバランシング

CSM-S がトラフィックの負荷をファイアウォールに分散させる場合、CSM-S はサーバにトラフィックの負荷を分散させる場合と同じ機能を実行します。ファイアウォールに対するレイヤ 3 ロードバランシングを設定する手順は、次のとおりです。

-
- ステップ 1** ファイアウォールの両側にサーバ ファームを作成します。
- ステップ 2** サーバファーム サブモードで、プレディクタの **hash address** コマンドを入力します。
- ステップ 3** ファイアウォール宛のトラフィックを受け付ける仮想サーバに、サーバ ファームを割り当てます。
-



(注) ファイアウォールに対するレイヤ 3 ロードバランシングを設定するときには、正方向で送信元 Network Address Translation (NAT; ネットワーク アドレス変換) を、逆方向で宛先 NAT を使用します。

ファイアウォール構成タイプ

CSM-S は、2 種類のファイアウォール構成をサポートします。

- デュアル CSM-S 構成 — 2 つの CSM モジュールの間にファイアウォールを配置します。ファイアウォールは一方の CSM-S からトラフィックを受け付け、他方の CSM-S に送ってサーバへの負荷分散を図るか、または要求側装置に戻します。
- シングル CSM-S 構成 — ファイアウォールは CSM-S からトラフィックを受け付け、同じ CSM-S に送り返してサーバへの負荷分散を図るか、または要求側装置にトラフィックを戻します。

ファイアウォール用 IP リバーススティッキ

CSM-S は現在、固定 (sticky) 接続をサポートしています。固定接続によって、同じクライアントから発信された異なる 2 つのデータ フローが、同じ宛先にロードバランスされます。

ロードバランスを図る宛先は、実サーバになることがよくあります。ファイアウォール、キャッシュ、またはその他のネットワーキング装置になることもあります。固定接続は、ロードバランス対象のアプリケーションを正しく動作させるために必要です。これらのアプリケーションは、同一クライアントから特定のサーバへの複数の接続を利用します。ある接続で転送された情報が、別の接続で転送された情報の処理を左右する場合があります。

IP スティッキ インサート (sticky intert) 機能は、同一クライアントから同一サーバへの新しい接続のバランスを図るために設定します。「[ファイアウォール用リバーススティッキの設定](#)」(p.13-27)を参照してください。この機能は、FTP (ファイル転送プロトコル) データ チャネル、ストリーミング UDP データ チャネルなど、バディ (buddy) 接続の場合に特に重要です。

CSM-S のファイアウォール設定

CSM-S がサポートできるファイアウォール設定は、次のとおりです。

- デュアル CSM-S 構成のステルス ファイアウォール (図 13-1)
- デュアル CSM-S 構成の標準ファイアウォール (図 13-2)
- シングル CSM-S 構成の標準ファイアウォール (図 13-3)
- デュアル CSM-S 構成の混在型 (ステルスおよび標準) ファイアウォール (図 13-4)

図 13-1 では、トラフィックはファイアウォールを通過し、双方向でフィルタリングされます。図は、インターネットからイントラネットへの流れを示しています。イントラネットへの経路では、CSM-S A が VLAN 5、6、および 7 にトラフィックを分散させ、ファイアウォール経由で CSM-S B に送ります。インターネットへの経路では、CSM-S B が VLAN 15、16、および 17 にトラフィックを分散させ、ファイアウォール経由で CSM-S A に送ります。CSM-S A はサーバファームで CSM-S B の VLAN エイリアスを使用し、CSM-S B はサーバファームで CSM-S A の VLAN エイリアスを使用します。

図 13-1 ステルス ファイアウォールの設定 (デュアル CSM-S モジュール専用)

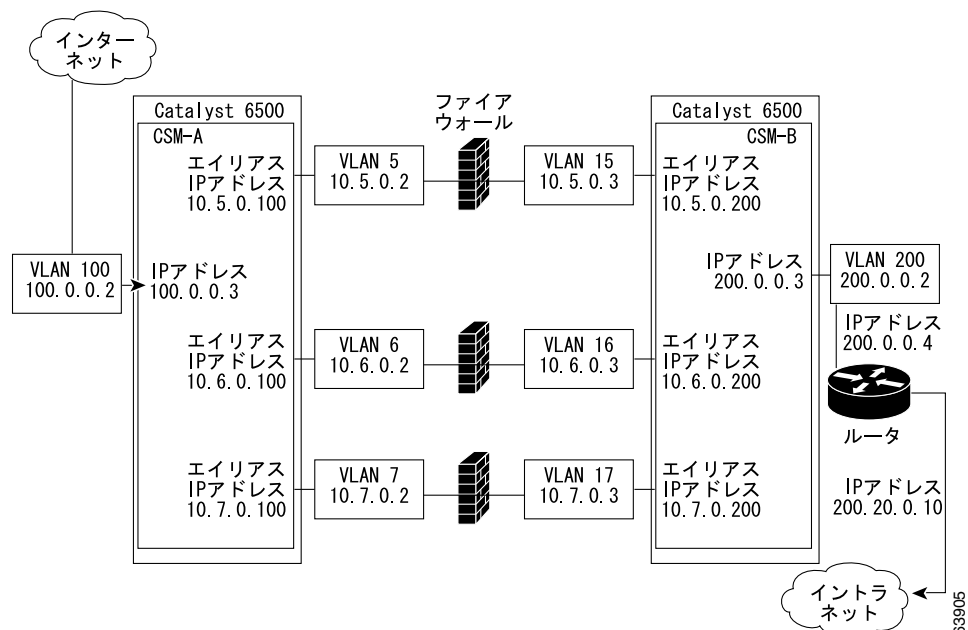


図 13-2 では、トラフィックはファイアウォールを通過し、双方向でフィルタリングされます。図は、インターネットからイントラネットへの流れを示しています。VLAN 11 および 111 が同じサブネットにあり、VLAN 12 および 112 が同じサブネットにあります。

図 13-2 標準ファイアウォールの設定（デュアル CSM-S モジュール）

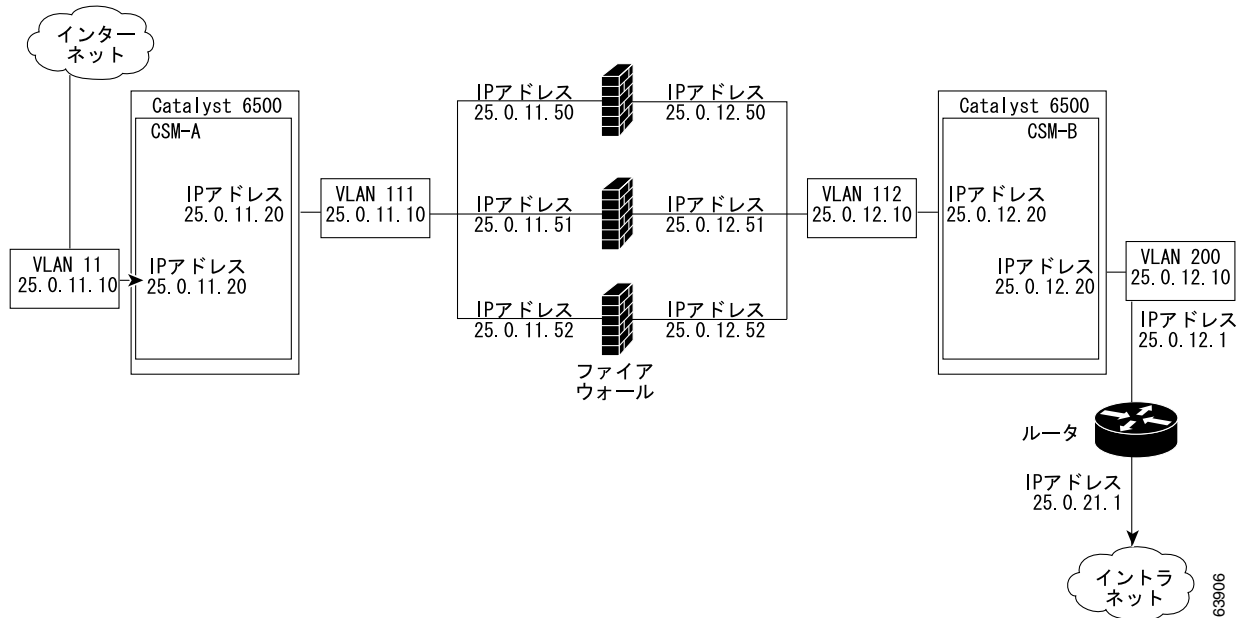


図 13-3 では、トラフィックはファイアウォールを通過し、双方向でフィルタリングされます。図に示されているのは、インターネットからイントラネットへの流れだけです。VLAN 11 および 111 は同じサブネットにあります。VLAN 12 および 112 は同じサブネットにあります。

図 13-3 標準ファイアウォールの設定（シングル CSM-S）

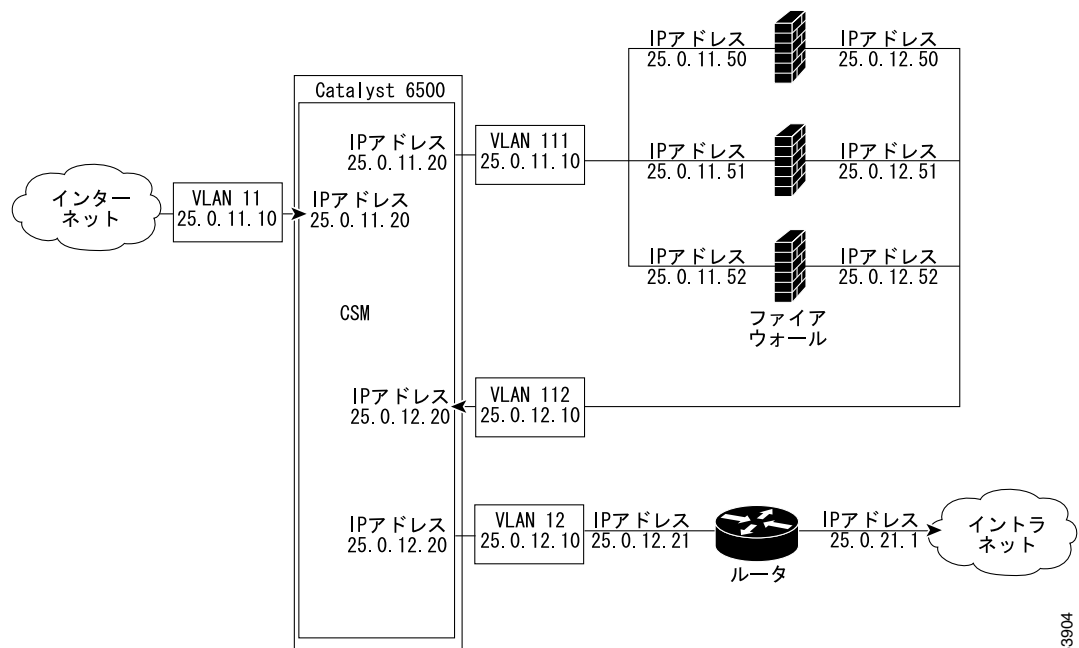
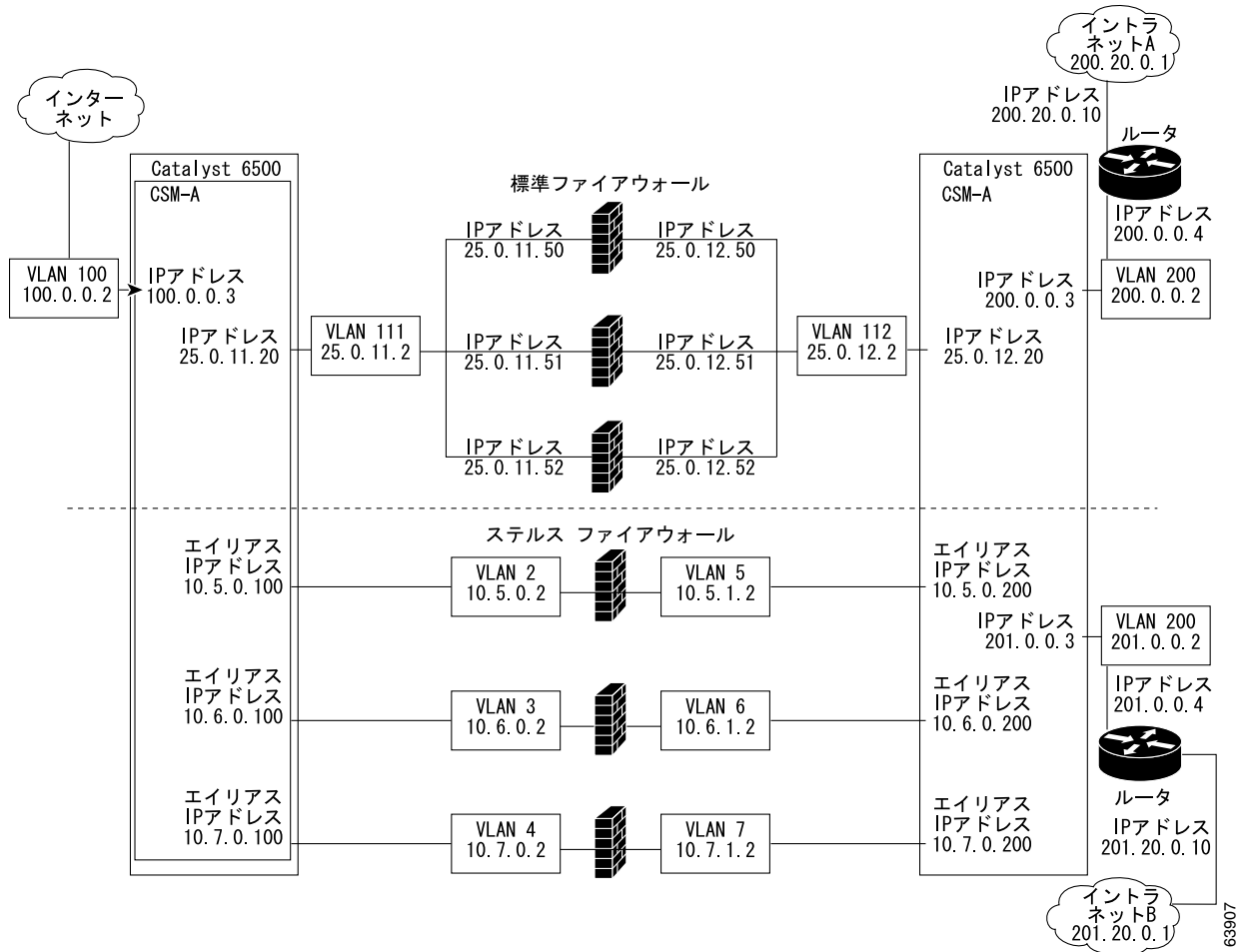


図 13-4 では、トラフィックは標準ファイアウォールとステルス ファイアウォールの両方を通して、双方向でフィルタリングされます。図は、インターネットからイントラネットへの流れを示しています。VLAN 5、6、および 7 は CSM-S A および CSM-S B 間で共有されます。イントラネットへの経路上で、CSM-S A は VLAN 5、6、および 7 間でトラフィックを分散させ、ファイアウォール経由で CSM-S B に送ります。イントラネットへの経路上で、CSM-S B は VLAN 5、6、および 7 間でトラフィックを分散させ、ファイアウォール経由で CSM-S A に送ります。

図 13-4 ステルスおよび標準ファイアウォールの混在型ファイアウォール設定（デュアル CSM-S 専用）



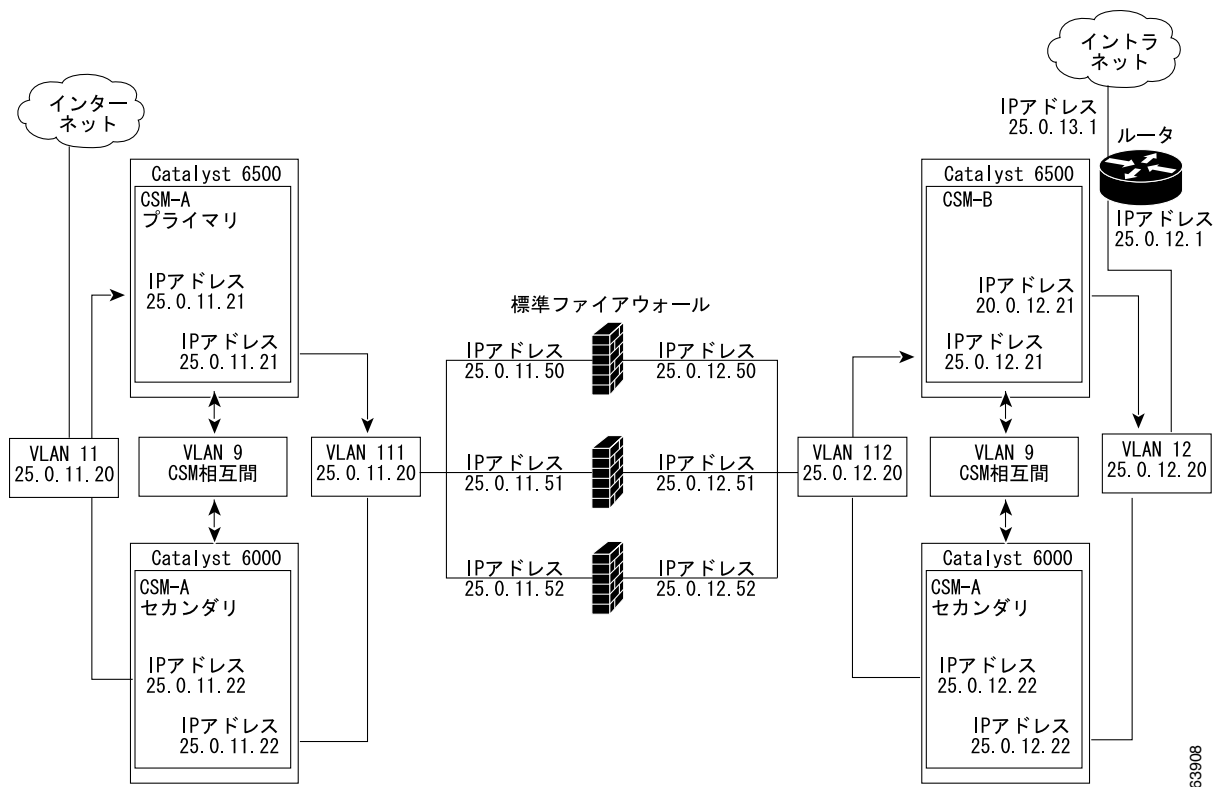
フォールトトレラントな CSM-S ファイアウォール設定

CSM-S は、次の構成でフォールトトレランスをサポートします。

- フォールトトレラントデュアル CSM-S 構成のステルスファイアウォール
- フォールトトレラントデュアル CSM-S 構成の標準ファイアウォール
- フォールトトレラントシングル CSM-S 構成の標準ファイアウォール
- フォールトトレラントデュアル CSM-S 構成の混在型ファイアウォール（ステルスおよび標準）

図 13-5 では、トラフィックはファイアウォールを通過し、双方向でフィルタリングされます。図に示されているのは、プライマリ CSM を通過する、インターネットからイントラネットへの流れだけです。VLAN 11 および 111 は同じサブネットにあります。VLAN 12 および 112 は同じサブネットにあります。

図 13-5 フォールトトレラントな標準ファイアウォールの設定（デュアル CSM）



ステルス ファイアウォール ロードバランシングの設定

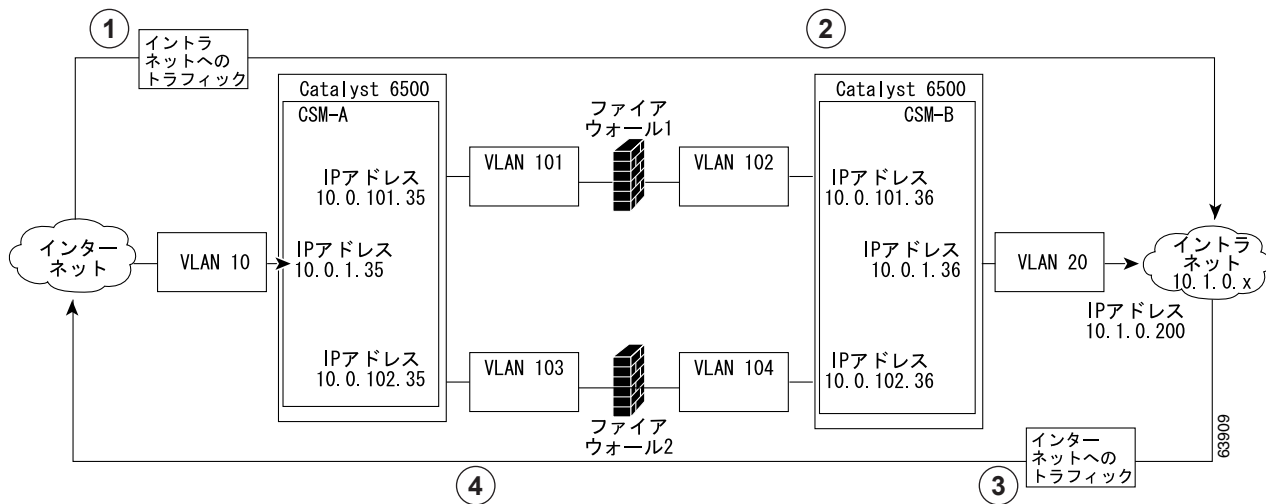
ここでは、ステルス ファイアウォール用にファイアウォール ロードバランシングを設定する方法について説明します。

- ステルス ファイアウォールの設定 (p.13-8)
- ステルス ファイアウォールの設定例 (p.13-9)

ステルス ファイアウォールの設定

ステルス ファイアウォール設定では、ファイアウォールは 2 つの異なる VLAN に接続し、接続先 VLAN の IP アドレスを指定して設定します (図 13-6 を参照)。

図 13-6 ステルス ファイアウォールの設定例



位置	トラフィックの方向	入口	出口
1	イントラネットへ	VLAN 10	VLAN 101 および 103
2	イントラネットへ	VLAN 101 および 103	VLAN 20
3	インターネットへ	VLAN 20	VLAN 102 および 104
4	インターネットへ	VLAN 101 および 103	VLAN 10

図 13-6 では、2 つの標準ファイアウォール（ファイアウォール 1 およびファイアウォール 2）が 2 つの CSM モジュール（CSM-S A および CSM-S B）の間にあります。



(注) ステルス ファイアウォールは VLAN 上にアドレスがありません。

インターネットからイントラネットへの経路上で、トラフィックはファイアウォールの保護されていない側から入り、別個の VLAN (VLAN 101 および VLAN 103) を通過し、ファイアウォールの保護された側から出て別個の VLAN (VLAN 102 および VLAN 104) を通過します。イントラネットからインターネットへの経路では、この流れが逆になります。VLAN はインターネット (VLAN 10) およびイントラネット (VLAN 20) への接続も可能にします。

ステルスの設定では、CSM-S A および CSM-S B がトラフィックの負荷を分散させてファイアウォールに通します。

ステルス ファイアウォールの設定例

ステルス ファイアウォールの設定例では、2 つの CSM-S（CSM-S A および CSM-S B）をそれぞれ別個の Catalyst 6500 シリーズ スイッチに搭載しています。



(注) ステルス ファイアウォールの設定では、各 CSM-S をそれぞれ別個の Catalyst 6500 シリーズ スイッチに搭載する必要があります。

ここでは、CSM-S A および CSM-S B 用に、ステルス ファイアウォール コンフィギュレーションを作成する手順について説明します。

CSM-S A の設定（ステルス ファイアウォールの例）

標準の設定例を作成するには、CSM-S A に対して次の作業が必要です。

- [スイッチ A 上での VLAN の作成 \(p.13-9\)](#)
- [CSM-S A 上での VLAN の設定 \(p.13-10\)](#)
- [CSM-S A 上でのサーバファームの設定 \(p.13-10\)](#)
- [CSM-S A 上での仮想サーバの設定 \(p.13-11\)](#)



(注) 設定作業は CSM-S A でも CSM-S B でも同じですが、手順、入力するコマンド、およびパラメータが異なります。

スイッチ A 上での VLAN の作成

スイッチ A 上で 2 つの VLAN を作成する手順は、次のとおりです。

	コマンド	目的
ステップ 1	Switch-A(config)# vlan	VLAN モードを開始します ¹ 。
ステップ 2	Switch-A(vlan)# vlan 10	VLAN 10 を作成します ² 。
ステップ 3	Switch-A(vlan)# vlan 101	VLAN 101 を作成します ³ 。
ステップ 4	Switch-A(vlan)# vlan 103	VLAN 103 を作成します ⁴ 。

1. この作業は、CSM-S A が搭載されたスイッチのコンソールで行います。
2. VLAN 10 は、CSM-S A をインターネットに接続します。
3. VLAN 101 は、ファイアウォール 1 経由で CSM-S B に接続します。
4. VLAN 103 は、ファイアウォール 2 経由で CSM-S B に接続します。

CSM-S A 上での VLAN の設定

3 つの VLAN を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	Switch-A(config)# module csm 5	マルチモジュール コンフィギュレーション モードを開始し、CSM-S A がスロット 5 に搭載されていることを指定します。
ステップ 2	Switch-A(config-module-csm)# vlan 10 client	設定対象の VLAN として VLAN 10 を指定し、クライアント VLAN であることを指定し、VLAN コンフィギュレーション モードを開始します。
ステップ 3	Switch-A(config-slb-vlan-client)# ip address 10.0.1.35 255.255.255.0	VLAN 10 の IP アドレスおよびネットマスクを指定します。
ステップ 4	Switch-A(config-slb-vlan-client)# alias 10.0.1.30 255.255.255.0	VLAN 10 用のエイリアス IP アドレスおよびネットマスクを指定します ¹ 。
ステップ 5	Switch-A(config-slb-vlan-client)# exit	VLAN コンフィギュレーション モードに戻ります。
ステップ 6	Switch-A(config-module-csm)# vlan 101 server	設定対象の VLAN として VLAN 101 を指定し、サーバ VLAN であることを指定し、VLAN コンフィギュレーション モードを開始します。
ステップ 7	Switch-A(config-slb-vlan-server)# ip address 10.0.101.35 255.255.255.0	VLAN 101 の IP アドレスおよびネットマスクを指定します。
ステップ 8	Switch-A(config-slb-vlan-server)# alias 10.0.101.100 255.255.255.0	VLAN 101 用のエイリアス IP アドレスおよびネットマスクを指定します ¹ 。
ステップ 9	Switch-A(config-slb-vlan-server)# exit	VLAN コンフィギュレーション モードに戻ります。
ステップ 10	Switch-A(config-module-csm)# vlan 103 server	設定対象の VLAN として VLAN 103 を指定し、サーバ VLAN であることを指定し、VLAN コンフィギュレーション モードを開始します。
ステップ 11	Switch-A(config-slb-vlan)# ip address 10.0.102.35 255.255.255.0	VLAN 103 の IP アドレスおよびネットマスクを指定します。
ステップ 12	Switch-A(config-slb-vlan)# alias 10.0.102.100 255.255.255.0	VLAN 103 用のエイリアス IP アドレスおよびネットマスクを指定します ¹ 。

1. このステップで、ロードバランシングの決定に使用する、CSM-S B のターゲットを特定します。

CSM-S A 上でのサーバ ファームの設定



(注) CSM-S B の IP アドレスを INSIDE-SF サーバファームで実サーバとして指定するので、CSM-S A は CSM-S B への経路上にある 2 つのファイアウォール間で負荷を分散させます。

CSM-S A 上で 2 つのサーバ ファームを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	Switch-A(config)# module csm 5	マルチモジュール コンフィギュレーション モードを開始し、CSM-S A がスロット 5 に搭載されていることを指定します。

	コマンド	目的
ステップ 2	Switch-A(config-module-csm) # serverfarm FORWARD-SF	FORWARD-SF ¹ サーバ ファーム（実際にはフォワーディング ポリシー）を作成して名前を指定し、サーバ ファーム コンフィギュレーション モードを開始します。
ステップ 3	Switch-A(config-slb-sfarm) # no nat server	サーバの IP アドレスおよびポート番号の NAT をディセーブルにします ² 。
ステップ 4	Switch-A(config-slb-sfarm) # predictor forward	ロードバランス アルゴリズムではなく、内部ルーティング テーブルに従って、トラフィックを転送します。
ステップ 5	Switch-A(config-slb-sfarm) # exit	マルチモジュール コンフィギュレーション モードに戻ります。
ステップ 6	Switch-A(config-module-csm) # serverfarm TO-INSIDE-SF	(実サーバではなくエイリアス IP アドレスを指定する) INSIDE-SF ³ サーバ ファームを作成して名前を指定し、サーバ ファーム コンフィギュレーション モードを開始します。
ステップ 7	Switch-A(config-slb-sfarm) # no nat server	サーバの IP アドレスおよびポート番号の NAT をディセーブルにします ⁴ 。
ステップ 8	Switch-A(config-slb-sfarm) # predictor hash address source 255.255.255.255	送信元 IP アドレスに基づくハッシュ値を使用して、サーバを選択します ⁵ 。
ステップ 9	Switch-A(config-slb-sfarm) # real 10.0.101.200	ファイアウォール 1 への経路上にある、CSM-S B のエイリアス IP アドレスを実サーバとして指定し、実サーバ コンフィギュレーション サブモードを開始します。
ステップ 10	Switch-A(config-slb-real) # inservice	ファイアウォールをイネーブルにします。
ステップ 11	Switch-A(config-slb-real) # exit	サーバ ファーム コンフィギュレーション モードに戻ります。
ステップ 12	Switch-A(config-slb-sfarm) # real 10.0.102.200	ファイアウォール 2 への経路上にある、CSM-S B のエイリアス IP アドレスを実サーバとして指定し、実サーバ コンフィギュレーション サブモードを開始します。
ステップ 13	Switch-A(config-slb-real) # inservice	ファイアウォールをイネーブルにします。

- FORWARD-SF は実際には、実サーバ ファームではなく、トラフィックが (VLAN 10 経由で) インターネットに到達できるようにする、ルート フォワーディング ポリシーです。実サーバは含まれません。
- このステップは、実サーバではなくフォワーディング ポリシーからなるサーバ ファームを設定する場合に必要です。
- INSIDE-SF は、イントラネットから CSM-S B にトラフィックが到達できるようにする実サーバとして指定された、CSM-S B の 2 つのエイリアス IP アドレスからなります。
- このステップは、ファイアウォールが含まれるサーバ ファームを設定する場合に必要です。
- この作業は、サーバ ファームで保護されない側のファイアウォール インターフェイスを設定する場合に行ってください。

CSM-S A 上での仮想サーバの設定

CSM-S A 上で 3 つの仮想サーバを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	Switch-A(config) # module csm 5	マルチモジュール コンフィギュレーション モードを開始し、CSM-S A がスロット 5 に搭載されていることを指定します。
ステップ 2	Switch-A(config-module-csm) # vserver FORWARD-V101	設定対象の仮想サーバとして FORWARD-V101 ¹ を指定し、仮想サーバ コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	Switch-A(config-slb-vserver)# virtual 0.0.0.0 0.0.0.0 any	あらゆる IP アドレスおよびあらゆるプロトコルと一致することを指定します ² 。
ステップ 4	Switch-A(config-slb-vserver))# vlan 101	仮想サーバが VLAN 101 に届いたトラフィック、すなわちファイアウォールの保護されていない側からのトラフィックだけを受け付けることを指定します。
ステップ 5	Switch-A(config-slb-vserver)# serverfarm FORWARD-SF	この仮想サーバに対応するサーバ ファームを指定します ³ 。
ステップ 6	Switch-A(config-slb-vserver)# inservice	仮想サーバをイネーブルにします。
ステップ 7	Switch-A(config-slb-vserver)# exit	マルチモジュール コンフィギュレーション モードに戻ります。
ステップ 8	Switch-A(config-module-csm)# vserver FORWARD-V103	設定対象の仮想サーバとして FORWARD-V103 ⁴ を指定し、仮想サーバ コンフィギュレーション モードを開始します。
ステップ 9	Switch-A(config-slb-vserver)# virtual 0.0.0.0 0.0.0.0 any	あらゆる IP アドレスおよびあらゆるプロトコルと一致することを指定します ⁵ 。
ステップ 10	Switch-A(config-slb-vserver))# vlan 103	仮想サーバが VLAN 103 に届いたトラフィック、すなわちファイアウォールの保護されていない側からのトラフィックだけを受け付けることを指定します。
ステップ 11	Switch-A(config-slb-vserver)# serverfarm FORWARD-SF	この仮想サーバに対応するサーバ ファームを指定します ³ 。
ステップ 12	Switch-A(config-slb-vserver)# inservice	仮想サーバをイネーブルにします。
ステップ 13	Switch-A(config-slb-vserver)# exit	マルチモジュール コンフィギュレーション モードに戻ります。
ステップ 14	Switch-A(config-module-csm)# vserver OUTSIDE-VS	設定対象の仮想サーバとして OUTSIDE-VS ⁶ を指定し、仮想サーバ コンフィギュレーション モードを開始します。
ステップ 15	Switch-A(config-slb-vserver)# virtual 10.1.0.0 255.255.255.0 any	この仮想サーバの IP アドレス、ネットマスク、およびプロトコル（あれば）を指定します。クライアントはこのアドレスによって、この仮想サーバが提供するサーバファームに到達します。
ステップ 16	Switch-A(config-slb-vserver))# vlan 10	仮想サーバが VLAN 10 に届いたトラフィック、すなわちインターネットからのトラフィックだけを受け付けることを指定します。
ステップ 17	Switch-A(config-slb-vserver)# serverfarm TO-INSIDE-SF	この仮想サーバに対応するサーバ ファームを指定します ⁷ 。
ステップ 18	Switch-A(config-slb-vserver)# inservice	仮想サーバをイネーブルにします。

- FORWARD-V101 は、インターネット トラフィックを（VLAN 101 経由で）ファイアウォールの保護されていない側に送ります。
- クライアントの一致を制限するのは、VLAN 制約だけです（ステップ 4 を参照）。
- このサーバファームは、実サーバからなる実サーバファームではなく、実際にはフォワーディングプレディクタです。
- FORWARD-V103 は、インターネット トラフィックを（VLAN 103 経由で）ファイアウォールの保護されていない側に送ります。
- クライアントのつねに一致（ステップ 9 を参照）を制限するのは、VLAN 制約だけです（ステップ 10 を参照）。
- OUTSIDE-VS は、インターネットからのトラフィックを（VLAN 10 経由で）CSM-S A に送ります。
- サーバファームは、ファイアウォール 1 およびファイアウォール 2 の経路上にある、CSM-S B のエイリアス IP アドレスで構成されます。

CSM-S B の設定（ステルス ファイアウォールの例）

標準の設定例を作成するには、CSM-S B に対して次の設定作業が必要です。

- スイッチ B 上での VLAN の作成 (p.13-13)
- CSM-S B 上での VLAN の設定 (p.13-13)
- CSM-S B 上でのサーバファームの設定 (p.13-14)
- CSM-S B 上での仮想サーバの設定 (p.13-16)



(注) 設定作業は CSM-S A でも CSM-S B でも同じですが、手順、入力するコマンド、およびパラメータが異なります。

スイッチ B 上での VLAN の作成

スイッチ B 上で 3 つの VLAN を作成する手順は、次のとおりです。



(注) この例では、CSM-S がそれぞれ別個の Catalyst 6500 シリーズ スイッチに搭載されているものとします。同一シャーシに搭載されている場合は、同じ Catalyst 6500 シリーズ スイッチのコンソールですべての VLAN を作成できます。

	コマンド	目的
ステップ 1	Switch-B(config)# vlan	VLAN モードを開始します ¹ 。
ステップ 2	Switch-B(vlan)# vlan 102	VLAN 102 を作成します ² 。
ステップ 3	Switch-B(vlan)# vlan 104	VLAN 104 を作成します ³ 。
ステップ 4	Switch-B(vlan)# vlan 200	VLAN 200 を作成します ⁴ 。

1. この作業は、CSM-S B が搭載されたスイッチのコンソールで行います。
2. VLAN 102 は、ファイアウォール 1 経由で CSM-S A に接続します。
3. VLAN 104 は、ファイアウォール 2 経由で CSM-S A に接続します。
4. VLAN 200 は、内部ネットワークに接続します。

CSM-S B 上での VLAN の設定

3 つの VLAN を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	Switch-B(config)# module csm 6	マルチモジュール コンフィギュレーション モードを開始し、CSM-S B がスロット 6 に搭載されていることを指定します。
ステップ 2	Switch-B(config-module-csm)# vlan 102 server	設定対象の VLAN として VLAN 102 を指定し、サーバ VLAN であることを指定し、VLAN コンフィギュレーション モードを開始します。
ステップ 3	Switch-B(config-slb-vlan-server)# ip address 10.0.101.36 255.255.255.0	VLAN 102 の IP アドレスおよびネットマスクを指定します。
ステップ 4	Switch-B(config-slb-vlan-server)# alias 10.0.101.200 255.255.255.0	VLAN 102 用のエイリアス IP アドレスおよびネットマスクを指定します ¹ 。

	コマンド	目的
ステップ 5	Switch-B(config-slb-vlan-server)# exit	マルチモジュール コンフィギュレーション モードに戻ります。
ステップ 6	Switch-B(config-module-csm)# vlan 104 server	設定対象の VLAN として VLAN 104 を指定し、サーバ VLAN であることを指定し、VLAN コンフィギュレーション モードを開始します。
ステップ 7	Switch-B(config-slb-vlan-server)# ip address 10.0.102.36 255.255.255.0	VLAN 104 の IP アドレスおよびネットマスクを指定します。
ステップ 8	Switch-B(config-slb-vlan)# alias 10.0.102.200 255.255.255.0	VLAN 104 用のエイリアス IP アドレスおよびネットマスクを指定します ¹ 。
ステップ 9	Switch-B(config-slb-vlan-server)# exit	マルチモジュール コンフィギュレーション モードに戻ります。
ステップ 10	Switch-B(config-module-csm)# vlan 20 server	設定対象の VLAN として VLAN 20 を指定し、サーバ VLAN であることを指定し、VLAN コンフィギュレーション モードを開始します。
ステップ 11	Switch-B(config-slb-vlan-server)# ip address 10.1.0.36 255.255.255.0	VLAN 20 の IP アドレスおよびネットマスクを指定します。

1. このステップで、ロードバランシングの決定に使用する、CSM-S A のターゲットを特定します。

CSM-S B 上でのサーバファームの設定

CSM-S B 上で 3 つのサーバファームを設定する手順は、次のとおりです。



- (注) SERVERS-SF では、この例ですでに **natpool** コマンドで作成した、クライアント NAT アドレスプールを使用して、クライアント NAT を実行することを指定します。コマンドを参照する前に、NAT プールを作成する必要があります。

	コマンド	目的
ステップ 1	Switch-B(config)# module csm 6	マルチモジュール コンフィギュレーション モードを開始し、CSM-S B がスロット 6 に搭載されていることを指定します。
ステップ 2	Switch-B(config-module-csm)# serverfarm FORWARD-SF	FORWARD-SF ¹ サーバファーム（実際にはフォワーディングポリシー）を作成して名前を指定し、サーバファーム コンフィギュレーション モードを開始します。
ステップ 3	Switch-B(config-slb-sfarm)# no nat server	サーバの IP アドレスおよびポート番号の NAT をディセーブルにします ² 。
ステップ 4	Switch-B(config-slb-sfarm)# predictor forward	ロードバランス アルゴリズムではなく、内部ルーティング テーブルに従って、トラフィックを転送します。
ステップ 5	Switch-B(config-slb-sfarm)# exit	マルチモジュール コンフィギュレーション モードに戻ります。
ステップ 6	Switch-B(config-module-csm)# serverfarm TO-OUTSIDE-SF	GENERIC-SF サーバファームを作成して名前を指定し、サーバファーム コンフィギュレーション モードを開始します ³ 。
ステップ 7	Switch-B(config-slb-sfarm)# no nat server	サーバの IP アドレスおよびポート番号の NAT をディセーブルにします ⁴ 。


	コマンド	目的
ステップ 8	Switch-B(config-slb-sfarm)# real 10.0.101.100	ファイアウォール 1 への経路上にある、CSM-S A のエイリアス IP アドレスを実サーバとして指定し、実サーバ コンフィギュレーション サブモードを開始します。
ステップ 9	Switch-B(config-slb-real)# inservice	実サーバ (実際にはエイリアス IP アドレス) をイネーブルにします。
ステップ 10	Switch-B(config-slb-real)# exit	サーバファーム コンフィギュレーション モードに戻ります。
ステップ 11	Switch-B(config-slb-sfarm)# real 10.0.102.100	ファイアウォール 2 への経路上にある、CSM-S B のエイリアス IP アドレスを実サーバとして指定し、実サーバ コンフィギュレーション サブモードを開始します。
ステップ 12	Switch-B(config-slb-real)# inservice	実サーバ (実際にはエイリアス IP アドレス) をイネーブルにします。
ステップ 13	Switch-B(config-slb-real)# exit	サーバファーム コンフィギュレーション モードに戻ります。
ステップ 14	Switch-B(config-module-csm)# serverfarm SERVERS-SF	SERVERS-SF ⁵ サーバファームを作成して名前を指定し、サーバファーム コンフィギュレーション モードを開始します。
ステップ 15	Switch-B(config-slb-sfarm)# real 10.1.0.101	イントラネット内のサーバを実サーバとして指定し、IP アドレスを割り当てて、実サーバ コンフィギュレーション サブモードを開始します。
ステップ 16	Switch-B(config-slb-real)# inservice	実サーバをイネーブルにします。
ステップ 17	Switch-B(config-slb-real)# exit	サーバファーム コンフィギュレーション モードに戻ります。
ステップ 18	Switch-B(config-slb-sfarm)# real 10.1.0.102	イントラネット内のサーバを実サーバとして指定し、IP アドレスを割り当てて、実サーバ コンフィギュレーション サブモードを開始します。
ステップ 19	Switch-B(config-slb-real)# inservice	実サーバをイネーブルにします。
ステップ 20	Switch-B(config-slb-sfarm)# real 10.1.0.103	イントラネット内のサーバを実サーバとして指定し、IP アドレスを割り当てて、実サーバ コンフィギュレーション サブモードを開始します。
ステップ 21	Switch-B(config-slb-real)# inservice	実サーバをイネーブルにします。

1. FORWARD-SF は実際には、実サーバファームではなく、トラフィックが (VLAN 20 経由で) イントラネットに到達できるようにする、ルート フォワーディング ポリシーです。実サーバは含まれません。
2. このステップは、実サーバではなくフォワーディング ポリシーからなるサーバファームを設定する場合に必要です。
3. OUTSIDE-SF は、イントラネットから CSM-S A にトラフィックが到達できるようにする実サーバとして指定された、CSM-S A の 2 つのエイリアス IP アドレスからなります。
4. このステップは、実サーバではなくフォワーディング ポリシーからなるサーバファームを設定する場合に必要です。
5. SERVERS-SF は、イントラネット内に配置された実サーバの IP アドレスからなります。

CSM-S B 上での仮想サーバの設定

CSM-S 上で 3 つの仮想サーバを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	Switch-B(config)# module csm 6	マルチモジュール コンフィギュレーション モードを開始し、CSM-S B がスロット 6 に搭載されていることを指定します。
ステップ 2	Switch-B(config-module-csm)# vserver FORWARD-VS-102	設定対象の仮想サーバとして FORWARD-VS を指定し、仮想サーバ コンフィギュレーション モードを開始します。
ステップ 3	Switch-B(config-slb-vserver)# virtual 0.0.0.0 0.0.0.0 any	あらゆる IP アドレスおよびあらゆるプロトコルと一致することを指定します ¹ 。
ステップ 4	Switch-B(config-slb-vserver)# vlan 102	仮想サーバが VLAN 102 に届いたトラフィック、すなわちファイアウォール1の保護されている側からのトラフィックだけを受け付けることを指定します。
ステップ 5	Switch-B(config-slb-vserver)# serverfarm FORWARD-SF	この仮想サーバに対応するサーバ ファームを指定します ² 。
ステップ 6	Switch-B(config-slb-vserver)# inservice	仮想サーバをイネーブルにします。
ステップ 7	Switch-B(config-slb-vserver)# exit	マルチモジュール コンフィギュレーション モードに戻ります。
ステップ 8	Switch-B(config-module-csm)# vserver FORWARD-VS-104	設定対象の仮想サーバとして FORWARD-VS ³ を指定し、仮想サーバ コンフィギュレーション モードを開始します。
ステップ 9	Switch-B(config-slb-vserver)# virtual 0.0.0.0 0.0.0.0 any	あらゆる IP アドレスおよびあらゆるプロトコルと一致することを指定します ¹ 。
ステップ 10	Switch-B(config-slb-vserver)# vlan 104	仮想サーバが VLAN 104 に届いたトラフィック、すなわちファイアウォール2の保護されている側からのトラフィックだけを受け付けることを指定します。
ステップ 11	Switch-B(config-slb-vserver)# serverfarm FORWARD-SF	この仮想サーバに対応するサーバ ファームを指定します ² 。
ステップ 12	Switch-B(config-slb-vserver)# inservice	仮想サーバをイネーブルにします。
ステップ 13	Switch-B(config-slb-vserver)# exit	マルチモジュール コンフィギュレーション モードに戻ります。
ステップ 14	Switch-B(config-module-csm)# vserver INSIDE-VS	設定対象の仮想サーバとして INSIDE-VS ⁴ を指定し、仮想サーバ コンフィギュレーション モードを開始します。
ステップ 15	Switch-B(config-slb-vserver)# virtual 0.0.0.0 0.0.0.0 any	あらゆる IP アドレスおよびあらゆるプロトコルと一致することを指定します ¹ 。
ステップ 16	Switch-B(config-slb-vserver)# vlan 20	仮想サーバが VLAN 20 に届いたトラフィック、すなわちイントラネットからのトラフィックだけを受け付けることを指定します。
ステップ 17	Switch-B(config-slb-vserver)# serverfarm TO-OUTSIDE-SF	この仮想サーバに対応するサーバ ファーム（実サーバとしての CSM-S A のエイリアス IP アドレスからなり、トラフィックをファイアウォール 1 および 2 に流す）を指定し、実サーバ コンフィギュレーション サブモードを開始します。

	コマンド	目的
ステップ 18	Switch-B(config-slb-vserver)# inservice	仮想サーバをイネーブルにします。
ステップ 19	Switch-B(config-slb-vserver)# exit	マルチモジュール コンフィギュレーション モードに戻ります。
ステップ 20	Switch-B(config-module-csm)# vserver TELNET-VS	設定対象の仮想サーバとして TELNET-VS ⁵ を指定し、仮想サーバ コンフィギュレーション モードを開始します。
		 <p>(注) TELNET-VS は VLAN 制限を使用しません。したがって、(ファイアウォールまたは内部ネットワークからの) あらゆる送信元のトラフィックがこのアドレス経由で負荷分散されます。</p>
ステップ 21	Switch-B(config-slb-vserver)# virtual 10.1.0.200 255.255.255.0 tcp telnet	この仮想サーバの IP アドレス、ネットマスク、プロトコル (TCP)、およびポート (Telnet) を指定します ⁶ 。
ステップ 22	Switch-B(config-slb-vserver)# serverfarm SERVERS-SF	この仮想サーバに対応する、実サーバからなるサーバファームを指定します。
ステップ 23	Switch-B(config-slb-vserver)# inservice	仮想サーバをイネーブルにします。

1. クライアントの一致を制限するのは、VLAN 制約だけです。
2. このサーバファームは、実サーバからなる実サーバファームではなく、実際にはフォワーディングプレディクタです。
3. FORWARD-VS は、インターネットからのトラフィックを (VLAN 20 経由で) イントラネットに送ります。
4. INSIDE-VS は、イントラネットからのトラフィックをファイアウォール 1 経由 (VLAN 102 および 101 経由) またはファイアウォール 2 経由 (VLAN 104 および 103 経由) で CSM-S A に送ります。
5. TELNET-VS は、インターネットからのトラフィックを内部ネットワーク内の Telnet サーバに送ります。
6. クライアントはこのアドレスによって、この仮想サーバが提供するサーバファームに到達します。

標準ファイアウォール ロードバランシングの設定

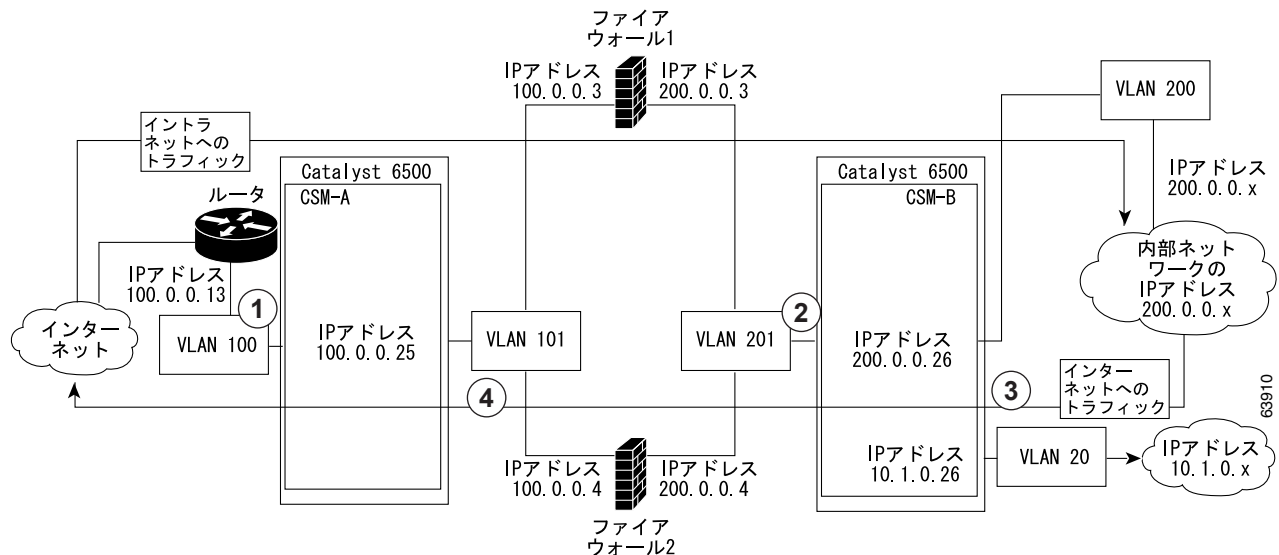
ここでは、標準ファイアウォール用にファイアウォール ロードバランシングを設定する方法について説明します。

- 標準ファイアウォール構成の場合のパケット フロー (p.13-18)
- 標準ファイアウォールの設定例 (p.13-19)

標準ファイアウォール構成の場合のパケット フロー

標準ファイアウォール設定では、ファイアウォールは 2 つの異なる VLAN に接続し、接続先 VLAN の IP アドレスを指定して設定します (図 13-7 を参照)。

図 13-7 標準ファイアウォールの設定例



アイテム	トラフィックの方向	入口	出口
1	イントラネットへ	VLAN 100	VLAN 101
2	イントラネットへ	VLAN 201	VLAN 200 および 20
3	インターネットへ	VLAN 200 および 20	VLAN 201
4	インターネットへ	VLAN 101	VLAN 100

図 13-7 では、2 つの標準ファイアウォール (ファイアウォール 1 およびファイアウォール 2) が 2 つの CSM (CSM-S A および CSM-S B) の間にあります。トラフィックは共有 VLAN (VLAN 101 および VLAN 201) を介してファイアウォールを出入りします。どちらの標準ファイアウォールも、各共有 VLAN 上に固有のアドレスを持っています。

VLAN はインターネット (VLAN 100)、内部ネットワーク (VLAN 200)、および内部サーバファーム (VLAN 20) に接続できるようにします。

CSM-S は、実サーバの場合と同様、標準ファイアウォール間でトラフィックを分散させます。標準ファイアウォールは、実サーバと同様、IP アドレスを指定してサーバファーム内で設定します。標準ファイアウォールが所属するサーバファームは、ロードバランス プレディクタが割り当てられ、仮想サーバと関連付けられます。

標準ファイアウォールの設定例

標準ファイアウォールの設定例では、2 つの CSM-S モジュール（CSM-S A および CSM-S B）をそれぞれ別個の Catalyst 6500 シリーズ スイッチに搭載しています。



(注) この例を使用できるのは、同じ Catalyst 6500 シリーズ スイッチ シャーシに搭載された 2 つの CSM-S モジュールを設定する場合です。また、CSM-S A および CSM-S B の両方を設定するときに、その CSM-S のスロット番号を指定することによって、単一スイッチ シャーシに 1 つだけ搭載された CSM-S を設定する場合にも、この例を使用できます。

CSM-S A の設定（標準ファイアウォールの例）

標準の設定例を作成するには、CSM-S A に対して次の設定作業が必要です。

- [スイッチ A 上での VLAN の作成 \(p.13-19\)](#)
- [CSM-S A 上での VLAN の設定 \(p.13-20\)](#)
- [CSM-S A 上でのサーバファームの設定 \(p.13-20\)](#)
- [CSM-S A 上での仮想サーバの設定 \(p.13-21\)](#)



(注) 設定作業は CSM-S A でも CSM-S B でも同じですが、手順、入力するコマンド、およびパラメータが異なります。

スイッチ A 上での VLAN の作成

[図 13-7](#) に示した例では、スイッチ A 上で VLAN を 2 つ作成する必要があります。



(注) この例では、CSM-S がそれぞれ別個の Catalyst 6500 シリーズ スイッチ シャーシに搭載されているものとします。同一シャーシに搭載されている場合は、同じ Catalyst 6500 シリーズ スイッチのコンソールですべての VLAN を作成できます。

スイッチ A 上で VLAN を作成する手順は、次のとおりです。

	コマンド	目的
ステップ 1	Switch-A(config)# vlan	VLAN モードを開始します ¹ 。
ステップ 2	Switch-A(vlan)# vlan 100	VLAN 100 を作成します ² 。
ステップ 3	Switch-A(vlan)# vlan 101	VLAN 101 を作成します ³ 。

1. この作業は、CSM-S A が搭載されたスイッチのコンソールで行います。
2. VLAN 100 は CSM-S A をインターネットに接続します。
3. VLAN 101 は CSM-S A をファイアウォールの保護されていない側に接続します。

CSM-S A 上での VLAN の設定

2 つの VLAN を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	Switch-A(config)# module csm 5	マルチモジュール コンフィギュレーション モードを開始し、CSM-S A がスロット 5 に搭載されていることを指定します。
ステップ 2	Switch-A(config-module-csm)# vlan 100 client	設定対象の VLAN として VLAN 100 を指定し、クライアント VLAN であることを指定し、VLAN コンフィギュレーション モードを開始します。
ステップ 3	Switch-A(config-slb-vlan-client)# ip address 100.0.0.25 255.255.255.0	VLAN 100 の IP アドレスおよびネットマスクを指定します。
ステップ 4	Switch-A(config-slb-vlan-client)# gateway 100.0.0.13	CSM-S A のインターネット側ルータのゲートウェイ IP アドレスを設定します。
ステップ 5	Switch-A(config-slb-vlan-client)# exit	マルチモジュール コンフィギュレーション モードに戻ります。
ステップ 6	Switch-A(config-module-csm)# vlan 101 server	設定対象の VLAN として VLAN 101 を指定し、サーバ VLAN であることを指定し、VLAN コンフィギュレーション モードを開始します。
ステップ 7	Switch-A(config-slb-vlan-server)# ip address 100.0.0.25 255.255.255.0	VLAN 101 の IP アドレスおよびネットマスクを指定します。
ステップ 8	Switch-A(config-slb-vlan-server)# alias 100.0.0.20 255.255.255.0	VLAN 101 用のエイリアス IP アドレスおよびネットマスクを指定します ¹ 。

1. このステップで、ロードバランシングの決定に使用する、CSM-S B のターゲットを特定します。

CSM-S A 上でのサーバ ファームの設定



(注) ファイアウォール 1 およびファイアウォール 2 の保護された側の IP アドレスは、CSM-S B と関連付けられた SEC-SF サーバ ファーム内の実サーバとして設定します。

CSM-S A 上で 2 つのサーバ ファームを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	Switch-A(config)# module csm 5	マルチモジュール コンフィギュレーション モードを開始し、CSM-S A がスロット 5 に搭載されていることを指定します。
ステップ 2	Switch-A(config-module-csm)# serverfarm FORWARD-SF	FORWARD-SF ¹ サーバ ファーム（実際にはフォワーディング ポリシー）を作成して名前を指定し、サーバ ファーム コンフィギュレーション モードを開始します。
ステップ 3	Switch-A(config-slb-sfarm)# no nat server	サーバの IP アドレスおよびポート番号の NAT をディセーブルにします ² 。
ステップ 4	Switch-A(config-slb-sfarm)# predictor forward	ロードバランス アルゴリズムではなく、内部ルーティング テーブルに従って、トラフィックを転送します。

	コマンド	目的
ステップ 5	Switch-A(config-slb-sfarm)# exit	マルチモジュール コンフィギュレーション モードに戻ります。
ステップ 6	Switch-A(config-module-csm)# serverfarm INSEC-SF	(実サーバとしてのファイアウォールが含まれる) INSEC-SF ³ サーバ ファームを作成して名前を指定し、サーバ ファーム コンフィギュレーション モードを開始します。
ステップ 7	Switch-A(config-slb-sfarm)# no nat server	サーバの IP アドレスおよびポート番号の NAT をディセーブルにします ⁴ 。
ステップ 8	Switch-A(config-slb-sfarm)# predictor hash address source 255.255.255.255	送信元 IP アドレスに基づくハッシュ値を使用して、サーバを選択します ⁵ 。
ステップ 9	Switch-A(config-slb-sfarm)# real 100.0.0.3	ファイアウォール 1 を実サーバとして設定し、ファイアウォールの保護されない側に IP アドレスを割り当て、実サーバ コンフィギュレーション サブモードを開始します。
ステップ 10	Switch-A(config-slb-real)# inservice	ファイアウォールをイネーブルにします。
ステップ 11	Switch-A(config-slb-real)# exit	サーバ ファーム コンフィギュレーション モードに戻ります。
ステップ 12	Switch-A(config-slb-sfarm)# real 100.0.0.4	ファイアウォール 2 を実サーバとして設定し、ファイアウォールの保護されない側に IP アドレスを割り当て、実サーバ コンフィギュレーション サブモードを開始します。
ステップ 13	Switch-A(config-slb-real)# inservice	ファイアウォールをイネーブルにします。

1. FORWARD-SF は実際には、実サーバ ファームではなく、トラフィックが (VLAN 100 経由で) インターネットに到達できるようにする、ルート フォワーディング ポリシーです。実サーバは含まれません。
2. このステップは、実サーバではなくフォワーディング ポリシーからなるサーバ ファームを設定する場合に必要です。
3. INSEC-SF にはファイアウォール 1 およびファイアウォール 2 が含まれます。それぞれの保護されていない側の IP アドレスをこのサーバ ファーム内の実サーバとして設定します。
4. このステップは、ファイアウォールが含まれるサーバ ファームを設定する場合に必要です。
5. このステップは、サーバ ファームで保護されない側のファイアウォール インターフェイスを設定する場合に行ってください。

CSM-S A 上での仮想サーバの設定

CSM-S A 上で 2 つの仮想サーバを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	Switch-A(config)# module csm 5	マルチモジュール コンフィギュレーション モードを開始し、CSM-S A がスロット 5 に搭載されていることを指定します。
ステップ 2	Switch-A(config-module-csm)# vserver FORWARD-VS	設定対象の仮想サーバとして FORWARD-VS ¹ を指定し、仮想サーバ コンフィギュレーション モードを開始します。
ステップ 3	Switch-A(config-slb-vserver)# virtual 0.0.0.0 0.0.0.0 any	あらゆる IP アドレスおよびあらゆるプロトコルと一致することを指定します ² 。
ステップ 4	Switch-A(config-slb-vserver)# vlan 101	仮想サーバが VLAN 101 に届いたトラフィック、すなわちファイアウォールの保護されていない側からのトラフィックだけを受け付けることを指定します。

	コマンド	目的
ステップ 5	Switch-A(config-slb-vserver)# serverfarm FORWARD-SF	この仮想サーバに対応するサーバ ファームを指定します ³ 。
ステップ 6	Switch-A(config-slb-vserver)# inservice	仮想サーバをイネーブルにします。
ステップ 7	Switch-A(config-slb-vserver)# exit	マルチモジュール コンフィギュレーション モードに戻ります。
ステップ 8	Switch-A(config-module-csm)# vserver INSEC-VS	設定対象の仮想サーバとして INSEC-VS ⁴ を指定し、仮想サーバ コンフィギュレーション モードを開始します。
ステップ 9	Switch-A(config-slb-vserver)# virtual 200.0.0.0 255.255.255.0 any	この仮想サーバの IP アドレス、ネットマスク、およびプロトコル（あれば）を指定します ⁵ 。
ステップ 10	Switch-A(config-slb-vserver)# vlan 100	仮想サーバが VLAN 100 に届いたトラフィック、すなわちインターネットからのトラフィックだけを受け付けることを指定します。
ステップ 11	Switch-A(config-slb-vserver)# serverfarm INSEC-SF	この仮想サーバに対応するサーバ ファームを指定します ⁶ 。
ステップ 12	Switch-A(config-slb-vserver)# inservice	仮想サーバをイネーブルにします。

1. FORWARD-VS は、インターネット トラフィックを（VLAN 101 経由で）ファイアウォールの保護されていない側に送ります。
2. クライアントの一致を制限するのは、VLAN 制約だけです（ステップ 4 を参照）。
3. このサーバファームは、実サーバからなる実サーバファームではなく、実際にはフォワーディングプレディクタです。
4. INSEC-VS は、インターネットからのトラフィックを（VLAN 101 経由で）CSM-S A に送ります。
5. クライアントはこのアドレスによって、この仮想サーバが提供するサーバファームに到達します。
6. サーバファームは実サーバではなくファイアウォールからなります。

CSM-S B の設定（標準ファイアウォールの例）

標準の設定例を作成するには、CSM-S B に対して次の設定作業が必要です。

- [スイッチ B 上での VLAN の作成（p.13-23）](#)
- [CSM-S B 上での VLAN の設定（p.13-23）](#)
- [CSM-S B 上でのサーバファームの設定（p.13-24）](#)
- [CSM-S B 上での仮想サーバの設定（p.13-25）](#)



(注) 設定作業は CSM-S A でも CSM-S B でも同じですが、手順、入力するコマンド、およびパラメータが異なります。

スイッチ B 上での VLAN の作成



(注) この例では、CSM-S がそれぞれ別個の Catalyst 6500 シリーズ スイッチ シャーシに搭載されているものとします。同一シャーシに搭載されている場合は、同じ Catalyst 6500 シリーズ スイッチのコンソールですべての VLAN を作成できます。

スイッチ B 上で 3 つの VLAN を作成する手順は、次のとおりです。

	コマンド	目的
ステップ 1	Switch-B(config)# vlan	VLAN モードを開始します ¹ 。
ステップ 2	Switch-B(vlan)# vlan 201	VLAN 201 を作成します ² 。
ステップ 3	Switch-B(vlan)# vlan 200	VLAN 200 を作成します ³ 。
ステップ 4	Switch-B(vlan)# vlan 20	VLAN 20 を作成します ⁴ 。

1. この作業は、CSM-S B が搭載されたスイッチのコンソールで行います。
2. VLAN 201 はファイアウォールの保護されている側に接続します。
3. VLAN 20 は、内部サーバファームに接続します。
4. VLAN 200 は、内部ネットワークに接続します。

CSM-S B 上での VLAN の設定

CSM-S B 上で 3 つの VLAN を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	Switch-B(config)# module csm 6	マルチモジュール コンフィギュレーション モードを開始し、CSM-S B がスロット 6 に搭載されていることを指定します。
ステップ 2	Switch-B(config-module-csm)# vlan 201 server	設定対象の VLAN として VLAN 201 を指定し、サーバ VLAN であることを指定し、VLAN コンフィギュレーション モードを開始します。
ステップ 3	Switch-B(config-slb-vlan-server)# ip address 200.0.0.26 255.255.255.0	VLAN 201 の IP アドレスおよびネットマスクを指定します。
ステップ 4	Switch-B(config-slb-vlan-server)# alias 200.0.0.20 255.255.255.0	VLAN 201 用のエイリアス IP アドレスおよびネットマスクを指定します ¹ 。
ステップ 5	Switch-B(config-slb-vlan-server)# exit	VLAN コンフィギュレーション モードに戻ります。
ステップ 6	Switch-B(config-module-csm)# vlan 20 server	設定対象の VLAN として VLAN 20 を指定し、サーバ VLAN であることを指定し、VLAN コンフィギュレーション モードを開始します。
ステップ 7	Switch-B(config-slb-vlan-server)# ip address 10.1.0.26 255.255.255.0	VLAN 20 の IP アドレスおよびネットマスクを指定します。
ステップ 8	Switch-B(config-slb-vlan-server)# exit	VLAN コンフィギュレーション モードに戻ります。
ステップ 9	Switch-B(config-module-csm)# vlan 200 client	設定対象の VLAN として VLAN 200 を指定し、クライアント VLAN であることを指定し、VLAN コンフィギュレーション モードを開始します。
ステップ 10	Switch-B(config-slb-vlan)# ip address 200.0.0.26 255.255.255.0	VLAN 200 の IP アドレスおよびネットマスクを指定します。

1. このステップで、ロードバランシングの決定に使用する、CSM-S A のターゲットを特定します。

CSM-S B 上でのサーバファームの設定



(注) ファイアウォール 1 およびファイアウォール 2 の保護された側の IP アドレスは、CSM-S A と関連付けられた INSEC-SF サーバファーム内の実サーバとして設定します。

CSM-S B 上で 2 つのサーバファームを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	Switch-B(config)# module csm 6	マルチモジュール コンフィギュレーション モードを開始し、CSM-S B がスロット 6 に搭載されていることを指定します。
ステップ 2	Switch-B(config-module-csm)# serverfarm GENERIC-SF	GENERIC-SF ¹ サーバファームを作成して名前を指定し、サーバファーム コンフィギュレーション モードを開始します。
ステップ 3	Switch-B(config-slb-sfarm)# real 10.1.0.101	内部サーバファームのサーバを実サーバとして指定し、IP アドレスを割り当てて、実サーバコンフィギュレーション サブモードを開始します。
ステップ 4	Switch-B(config-slb-real)# inservice	実サーバをイネーブルにします。
ステップ 5	Switch-B(config-slb-real)# exit	サーバファーム コンフィギュレーション モードに戻ります。
ステップ 6	Switch-B(config-slb-sfarm)# real 10.1.0.102	内部サーバファームのサーバを実サーバとして指定し、IP アドレスを割り当てて、実サーバコンフィギュレーション サブモードを開始します。
ステップ 7	Switch-B(config-slb-real)# inservice	実サーバをイネーブルにします。
ステップ 8	Switch-B(config-slb-real)# exit	サーバファーム コンフィギュレーション モードに戻ります。
ステップ 9	Switch-B(config-slb-sfarm)# exit	マルチモジュール コンフィギュレーション モードに戻ります。
ステップ 10	Switch-B(config-module-csm)# serverfarm SEC-SF	SEC-SF ² サーバファームを作成して名前を指定し、サーバファーム コンフィギュレーション モードを開始します。
ステップ 11	Switch-B(config-slb-sfarm)# no nat server	サーバの IP アドレスおよびポート番号の NAT をディセーブルにします ³ 。
ステップ 12	Switch-B(config-slb-sfarm)# predictor hash address destination 255.255.255.255	宛先 IP アドレスに基づくハッシュ値を使用して、サーバを選択します ⁴ 。
ステップ 13	Switch-B(config-slb-sfarm)# real 200.0.0.3	ファイアウォール 1 を実サーバとして設定し、ファイアウォールの保護されない側に IP アドレスを割り当て、実サーバコンフィギュレーション サブモードを開始します。
ステップ 14	Switch-B(config-slb-real)# inservice	ファイアウォールをイネーブルにします。
ステップ 15	Switch-B(config-slb-real)# exit	サーバファーム コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 16	Switch-B(config-slb-sfarm)# real 200.0.0.4	ファイアウォール 2 を実サーバとして設定し、ファイアウォールの保護されない側に IP アドレスを割り当て、実サーバ コンフィギュレーション サブモードを開始します。
ステップ 17	Switch-B(config-slb-real)# inservice	ファイアウォールをイネーブルにします。

1. GENERIC-SF は、内部サーバ ファーム内の実サーバからなります。
2. SEC-SF にはファイアウォール 1 およびファイアウォール 2 が含まれます。それぞれの保護される側の IP アドレスをこのサーバ ファーム内の実サーバとして設定します。
3. このステップは、ファイアウォールが含まれるサーバ ファームを設定する場合に必要です。
4. このステップは、サーバ ファームで保護される側のファイアウォールインターフェイスを設定する場合に行ってください。

CSM-S B 上での仮想サーバの設定

CSM-S B 上で 3 つの仮想サーバを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	Switch-B(config)# module csm 6	マルチモジュール コンフィギュレーション モードを開始し、CSM-S B がスロット 6 に搭載されていることを指定します。
ステップ 2	Switch-B(config-module-csm)# vserver GENERIC-VS	設定対象の仮想サーバとして GENERIC-VS ¹ を指定し、仮想サーバ コンフィギュレーション モードを開始します。
ステップ 3	Switch-B(config-slb-vserver)# virtual 200.0.0.127 tcp 0	この仮想サーバの IP アドレス、プロトコル (TCP)、およびポート (0=any) を指定します ² 。
ステップ 4	Switch-B(config-slb-vserver)# vlan 201	仮想サーバが VLAN 201 に届いたトラフィック、すなわちファイアウォールの保護されている側からのトラフィックだけを受け付けることを指定します。
ステップ 5	Switch-B(config-slb-vserver)# serverfarm GENERIC-SF	この仮想サーバに対応するサーバ ファームを指定します ³ 。
ステップ 6	Switch-B(config-slb-vserver)# inservice	仮想サーバをイネーブルにします。
ステップ 7	Switch-B(config-slb-vserver)# exit	マルチモジュール コンフィギュレーション モードに戻ります。
ステップ 8	Switch-B(config-module-csm)# vserver SEC-20-VS	設定対象の仮想サーバとして SEC-20-VS ⁴ を指定し、仮想サーバ コンフィギュレーション モードを開始します。
ステップ 9	Switch-B(config-slb-vserver)# virtual 200.0.0.0 255.255.255.0 any	この仮想サーバの IP アドレス、ネットマスク、およびプロトコル (あれば) を指定します ² 。
ステップ 10	Switch-B(config-slb-vserver)# vlan 20	仮想サーバが VLAN 20 に届いたトラフィック、すなわち内部サーバ ファームからのトラフィックだけを受け付けることを指定します。
ステップ 11	Switch-B(config-slb-vserver)# serverfarm SEC-SF	この仮想サーバに対応するサーバ ファームを指定します ⁵ 。
ステップ 12	Switch-B(config-slb-vserver)# inservice	仮想サーバをイネーブルにします。
ステップ 13	Switch-B(config-slb-vserver)# exit	マルチモジュール コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 14	Switch-B(config-module-csm)# vserver SEC-200-VS	設定対象の仮想サーバとして SEC-20-VS ⁶ を指定し、仮想サーバ コンフィギュレーション モードを開始します。
ステップ 15	Switch-B(config-slb-vserver)# virtual 200.0.0.0 255.255.255.0 any	この仮想サーバの IP アドレス、ネットマスク、およびプロトコル（あれば）を指定します ² 。
ステップ 16	Switch-B(config-slb-vserver)# vlan 200	仮想サーバが VLAN 200 に届いたトラフィック、すなわち内部ネットワークからのトラフィックだけを受け付けることを指定します。
ステップ 17	Switch-B(config-slb-vserver)# serverfarm SEC-SF	この仮想サーバに対応するサーバ ファームを指定します ⁵ 。
ステップ 18	Switch-B(config-slb-vserver)# inservice	仮想サーバをイネーブルにします。

1. GENERIC-VS によって、インターネットを宛先とする、内部サーバファームおよび内部ネットワークからのトラフィックが、ファイアウォールの保護されている側に（VLAN 101 経由で）送られます。
2. クライアントはこのアドレスによって、この仮想サーバが提供するサーバ ファームに到達します。
3. サーバ ファームは、内部サーバファーム ネットワーク内にあります。
4. SEC-20-VS は、インターネットからのトラフィックを（VLAN 20 経由で）内部サーバファームに送ります。
5. サーバファームは実サーバではなくファイアウォールからなります。
6. SEC-200-VS は、インターネットからのトラフィックを（VLAN 20 経由で）内部ネットワークに送ります。

ファイアウォール用リバーススティッキの設定

リバーススティッキ機能では、クライアント IP アドレスに基づいたロードバランスの決定に関するデータベースを作成します。この機能によって、データベースにリバーススティッキ エントリがあった場合に、ロードバランスの決定が変更されます。データベースにリバーススティッキ エントリがなかった場合は、ロードバランスの決定が実行され、今後のマッチングのために結果が保存されます。

ファイアウォール用リバーススティッキの概要

リバーススティッキは、接続を反対方向からのものとみなして、スティッキ データベースにエントリを追加する 1 つの方法を提供します。リバーススティッキが行われた仮想サーバは、着信実サーバが含まれている指定のデータベースにエントリを追加します。



(注)

着信実サーバは、サーバファーム内の実サーバでなければなりません。

このエントリは、別の仮想サーバ上の `sticky` コマンドによってマッチングされます。他方の仮想サーバは、前もって作成されたこのエントリに基づいて、クライアントにトラフィックを送ります。

CSM-S は、送信元 IP キーから実サーバへのリンクとして、リバーススティッキ情報を保存します。ロードバランサがスティッキ データベースの割り当てられた仮想サーバと新しくセッションを開始するときには、最初にデータベースにエントリがすでにあるかどうかを確認します。一致するエントリがあった場合、セッションは指定された実サーバに接続されます。それ以外の場合は、スティッキ キーと適切な実サーバを結びつける、新しいエントリが作成されます。図 13-8 に、ファイアウォールでリバーススティッキ機能をどのように使用するかを示します。

図 13-8 ファイアウォール用リバーススティッキ

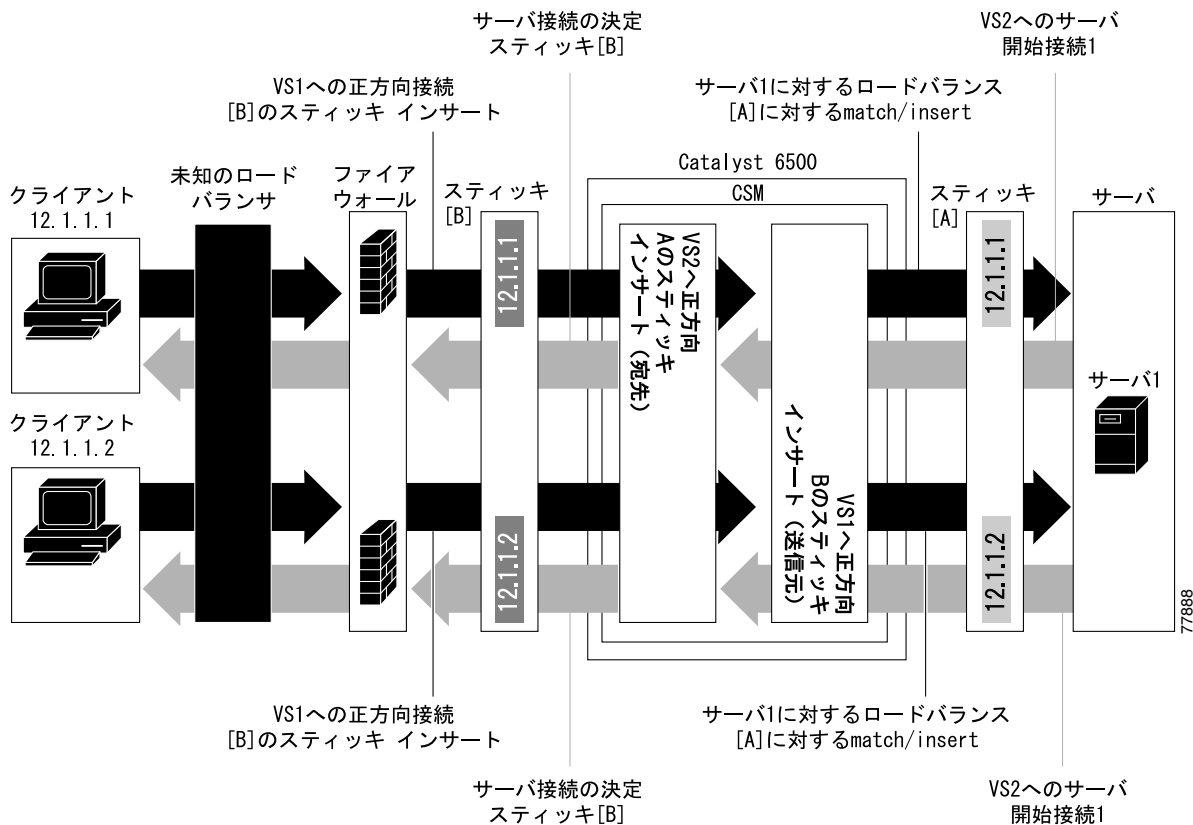


図 13-8 のリバーススティッキ プロセスは、次のとおりです。

- クライアントは、ロードバランス対象のファイアウォールを通過して、CSM-S 仮想サーバである VS1 に接続します。このロードバランスの決定は、CSM-S と対話しないで行われます。
- サーバ 1 は最初のクライアントに戻る接続を作成します。この接続は仮想サーバ VS2 と対応します。VS2 は、最初の VS1 リバーススティッキによって追加されたスティッキ情報を使用します。したがって、同じファイアウォール 1 に強制的に接続されます。
- 別のファイアウォールを通過する第 2 のクライアントは、同じ VS1 が接続します。リバーススティッキによって、第 2 のクライアント用にファイアウォール 2 を示す新しいエントリがデータベース B に作成されます。VS1 もサーバ 1 に対して通常のスティッキを実行します。
- サーバ 1 はクライアント 2 に戻る接続を作成します。この接続は VS2 の接続と一致します。VS2 は、最初の VS1 リバーススティッキによって追加されたスティッキ情報を使用します。この接続は、ファイアウォール 2 への接続に使用されます。
- サーバが最初の接続を開始すると、サーバに戻るリンクが VS2 によって作成され、通常のロードバランス決定によって一方のファイアウォールへの接続が作成されます。



(注)

この設定では、任意のバランシング メトリックを使用する正方向の接続（クライアントからサーバ）がサポートされます。ただし、サーバが開始したトラフィックへのクライアント応答が適切なファイアウォールに送られるようにするには、VS2 からファイアウォールへのバランシング メトリックが未知のロードバランサのメトリックと一致しなければなりません。または、未知のロードバランサが同様に新しい buddy 接続を固定（stick）しなければなりません。

ファイアウォール用リバーススティッキの設定

ファイアウォール ロードバランスのために IP リバーススティッキを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	SLB-Switch(config)# module csm slot	特定の CSM-S モジュールにロードバランス コマンドを関連付け、指定したスロットに対して CSM-S モジュール コンフィギュレーション サブモードを開始します。
ステップ 2	SLB-Switch(config-module-csm)# vserver virtserver-name	仮想サーバを特定し、仮想サーバ コンフィギュレーション サブモードを開始します。
ステップ 3	SLB-Switch(config-slb-vserver)# sticky duration [group group-id] [netmask ip-netmask] [source destination both]	スティッキ エントリ キーに使用する IP 情報の部分 (送信元、宛先、または両方) を定義します。
ステップ 4	SLB-Switch(config-slb-vserver)# reverse-sticky group-id	最初の送信元に戻る反対方向で、CSM-S が接続を維持するようにします。
ステップ 5	SLB-Switch# show module csm slot sticky	スティッキ データベースを表示します。

ステートフル ファイアウォール接続のリマッピングの設定

ファイアウォールの再割り当て機能を設定するには、Cisco IOS ソフトウェアの Release 12.1(19)E の MSFC イメージが必要です。

ファイアウォールの再割り当てを設定する手順は、次のとおりです。

- ステップ 1** ファイアウォール用のサーバファーム サブモードで、次の動作を設定します。

```
Cat6k-2(config)# serverfarm FW-FARM
failaction reassign
```

- ステップ 2** 実サーバが失敗した場合（プローブまたは Address Resolution Protocol [ARP; アドレス解決プロトコル]）は、各ファイアウォール用のバックアップ実サーバを割り当てます。

```
Cat6k-2(config-slb-sfarm)# serverfarm FW-FARM
Cat6k-2(config-slb-sfarm)# real 1.1.1.1
Cat6k(config-slb-module-real)# backup real 2.2.2.2
Cat6k(config-slb-module-real)# inservice
Cat6k-2(config-slb-sfarm)# real 2.2.2.2
Cat6k(config-slb-module-real)# backup real 3.3.3.3
Cat6k(config-slb-module-real)# inservice
Cat6k-2(config-slb-sfarm)# real 3.3.3.3
Cat6k(config-slb-module-real)# backup real 1.1.1.1
Cat6k(config-slb-module-real)# inservice
```

- ステップ 3** このサーバファーム用の Internet Control Message Protocol (ICMP) プローブ（ファイアウォールを経由）を設定します。

- ステップ 4** ファイアウォールの外側および内側に CSM-S モジュール用 ICMP プローブを設定します。

バックアップ実サーバが、同じ順序で CSM-S の両側に設定されていることを確認します。

接続の宛先または負荷分散先が失敗したプライマリ サーバの場合、実サーバに割り当てられた稼働中のスタンバイ オプションにより、このサーバが接続のみを受信するよう指定されます。**real 2.2.2.2** として指定された実サーバを稼働中のスタンバイで設定する場合、すべての接続は **real 1.1.1.1** または **real 3.3.3.3** として指定された実サーバのいずれかに達します。実サーバ **real 1.1.1.1** が失敗した場合は、実サーバ **real 1.1.1.1** の代わりに **real 2.2.2.2** として指定された実サーバがアクティブになります。