CHAPTER 15

ファイアウォール モードの概要

この章では、各ファイアウォール モードでファイアウォールがどのように機能するかを説明します。ファイアウォール モードを設定するには、「トランスペアレントまたはルーテッド ファイアウォール モードの設定」（P.2-6）を参照してください。

（注） マルチ コンテキスト モードでは、コンテキストごとに個別にファイアウォール モードを設定できません。ファイアウォール モードはセキュリティ アプライアンス全体に対してだけ設定できます。

この章は、次の項で構成されています。

ルーテッド モードの概要

ルーテッド モードでは、セキュリティ アプライアンスはネットワーク内のルータ ホップと見なされます。このモードでは、接続されているネットワークの間で NAT が実行されます。また、OSPF または RIP（のシングル コンテキスト モード）を使用できます。ルーテッド モードは多数のインターフェイスをサポートしています。インターフェイスはそれぞれ異なるサブネット上に置かれます。コンテキスト間でインターフェイスを共有することもできます。

この項では、次のトピックについて取り上げます。

IP ルーティング サポート

セキュリティ アプライアンスは、接続されたネットワーク間のルータとして機能します。インターフェイスごとに、異なるサブネット上の IP アドレスが必要です。シングルコンテキスト モードでは、ルーテッド ファイアウォールは OSPF および RIP をサポートします。マルチ コンテキスト モードでは、スタティック ルートだけがサポートされます。過度なルーティングのニーズをセキュリティ アプライアンスに頼るのではなく、アップストリーム ルータとダウンストリーム ルータの拡張ルーティング機能を使用することをお勧めします。

ネットワーク アドレス変換

NAT は、パケット内のローカル アドレスを、宛先ネットワーク上のルーティング可能なグローバル アドレスと置き換えます。デフォルトでは、NAT は必要ではありません。低いセキュリティ インターフェイス（外部）と通信するときに、NAT を使用するために高いセキュリティ インターフェイス（内部）上のホストを必要とする NAT ポリシーを適用する場合は、NAT 制御をイネーブルにできます（**nat-control** コマンドを参照）。

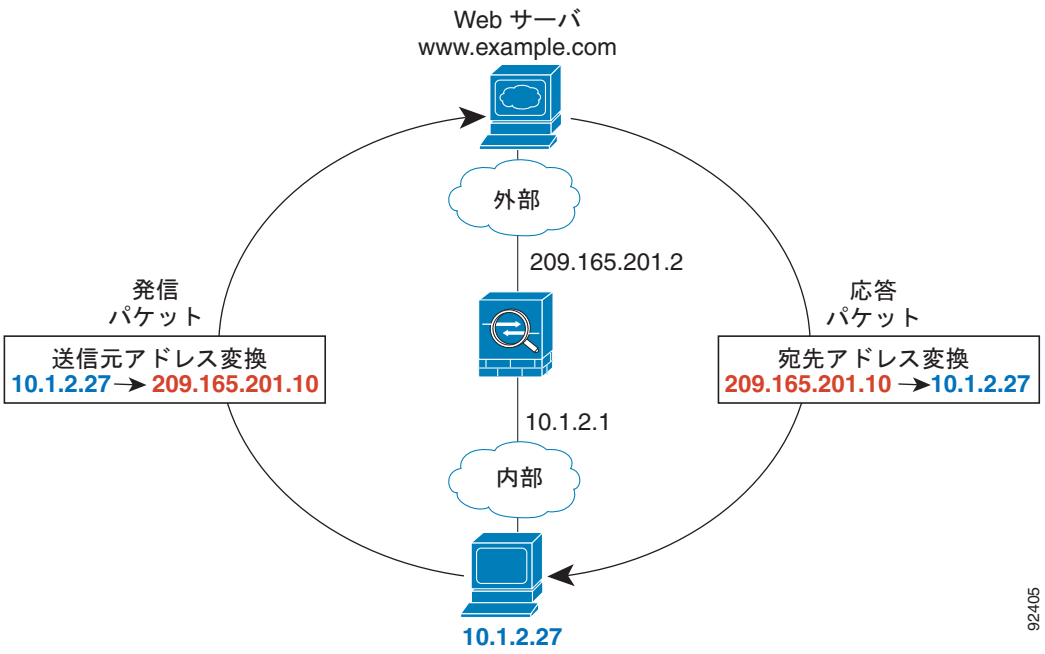
（注）　NAT 制御はバージョン 7.0 よりも前のソフトウェア バージョンのデフォルト動作でした。先行のバージョンからセキュリティ アプライアンスをアップグレードする場合、期待される動作を維持するために **nat-control** コマンドがコンフィギュレーションに自動的に追加されます。

NAT の利点のいくつかを次に示します。

- 内部ネットワークでプライベート アドレスを使用できます。プライベート アドレスは、インターネットにルーティングできません。
- NAT はローカル アドレスを他のネットワークから隠蔽するため、攻撃者はホストの実際のアドレスを取得できません。
- NAT は、重複 IP アドレスをサポートすることで、IP ルーティングの問題を解決できます。

図 15-1 は、内部にプライベート ネットワークを持つ典型的な NAT シナリオを示しています。内部ユーザがインターネットの Web サーバにパケットを送信すると、パケットのローカル送信元アドレスはルーティング可能なグローバル アドレスに変更されます。Web サーバが応答すると、これはグローバル アドレスに応答を送信し、セキュリティ アプライアンスはパケットを受信します。次にセキュリティ アプライアンスは、ユーザに送信する前にグローバル アドレスをローカル アドレスに変換します。

図 15-1　NAT の例



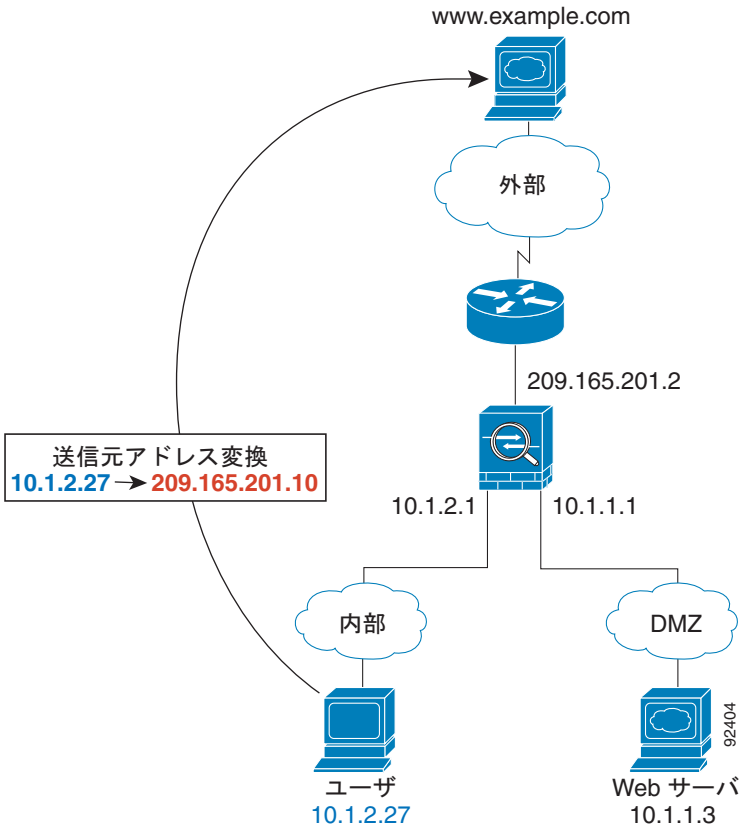
ルーテッド ファイアウォール モードでデータがセキュリティ アプライアンスを通過する方法

ここでは、ルーテッド ファイアウォール モードにおいて、データが セキュリティ アプライアンス をどのように通過するかについて説明します。内容は次のとおりです。

内部ユーザが Web サーバにアクセスする

図 15-2 は、内部ユーザが外部 Web サーバにアクセスしていることを示しています。

図 15-2　　内部から外部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します（図 15-2 を参照）。

1. 内部ネットワークのユーザは、www.example.com から Web ページを要求します。

2. セキュリティ アプライアンスはパケットを受信します。これは新しいセッションであるため、セキュリティ アプライアンスはセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

   マルチ コンテキスト モードの場合、セキュリティ アプライアンスは、コンテキストに関連付けられる固有なインターフェイスまたは固有な宛先アドレスに従ってパケットを分類します。宛先アドレスは、コンテキストでのアドレス変換と照合することによって関連付けられます。この場合、インターフェイスは固有です。www.example.com の IP アドレスは、コンテキスト内に最新のアドレス変換を持っていません。

3. セキュリティ アプライアンスは、ローカル送信元アドレス（10.1.2.27）を、外部インターフェイス サブネット上のグローバル アドレス 209.165.201.10 に変換します。

   グローバル アドレスは任意のサブネット上に置くことができますが、外部インターフェイス サブネットに置くとルーティングが簡素化されます。

4. 次に、セキュリティ アプライアンスはセッションが確立されたことを記録し、外部インターフェイスからパケットを転送します。

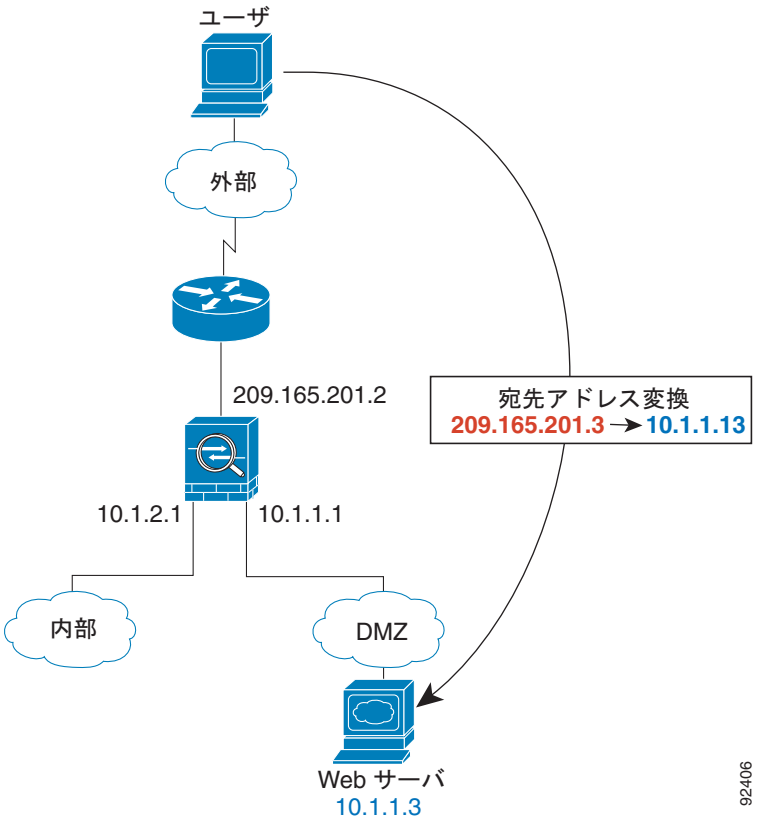
5. www.example.com が要求に応答すると、パケットはセキュリティ アプライアンスを通過します。これはすでに確立されているセッションであるため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。セキュリティ アプライアンスは、グローバル宛先アドレスをローカル ユーザ アドレス 10.1.2.27 に変換することによって、NAT を実行します。

6. セキュリティ アプライアンスは、パケットを内部ユーザに転送します。

外部ユーザが DMZ 上の Web サーバにアクセスする

図 15-3 は、外部ユーザが DMZ Web サーバにアクセスしていることを示しています。

図 15-3　外部から DMZ へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します（図 15-3 を参照）。

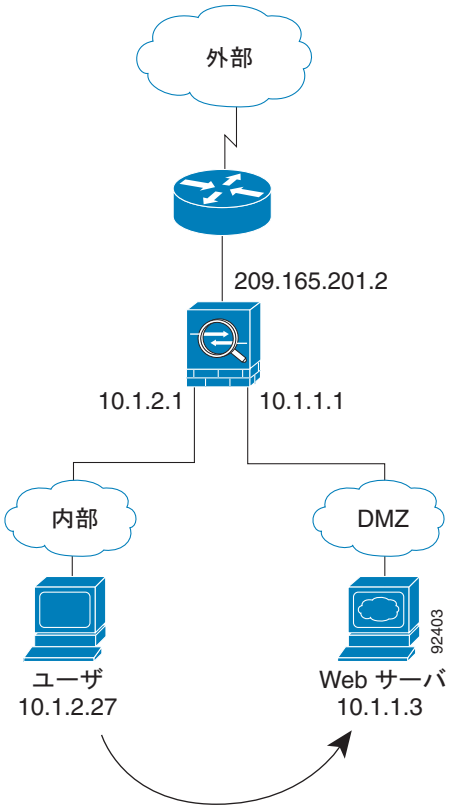
1. 外部ネットワーク上のユーザは、外部インターフェイス サブネット上にあるグローバル宛先アドレス 209.165.201.3 を使用して DMZ Web サーバから Web ページを要求します。
2. セキュリティ アプライアンスはパケットを受信します。これは新しいセッションであるため、セキュリティ アプライアンスはセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

   マルチ コンテキスト モードの場合、セキュリティ アプライアンスは、コンテキストに関連付けられる固有なインターフェイスまたは固有な宛先アドレスに従ってパケットを分類します。宛先アドレスは、コンテキストでのアドレス変換と照合することによって関連付けられます。この場合、分類子は DMZ Web サーバ アドレスがサーバ アドレス変換のため特定のコンテキストに属すことを「認識」しています。
3. セキュリティ アプライアンスは、宛先アドレスをローカル アドレス 10.1.1.3 に変換します。
4. 次に、セキュリティ アプライアンスはセッション エントリを高速パスに追加し、DMZ インターフェイスからパケットを転送します。
5. DMZ Web サーバが要求に応答すると、パケットはセキュリティ アプライアンスを通過します。また、セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。セキュリティ アプライアンスは、ローカル送信元アドレスを 209.165.201.3 に変換することによって、NAT を実行します。
6. セキュリティ アプライアンスは、パケットを外部ユーザに転送します。

内部ユーザが DMZ 上の Web サーバにアクセスする

図 15-4 は、内部ユーザが DMZ Web サーバにアクセスしていることを示しています。

図 15-4　　内部から DMZ へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します（図 15-4 を参照）。

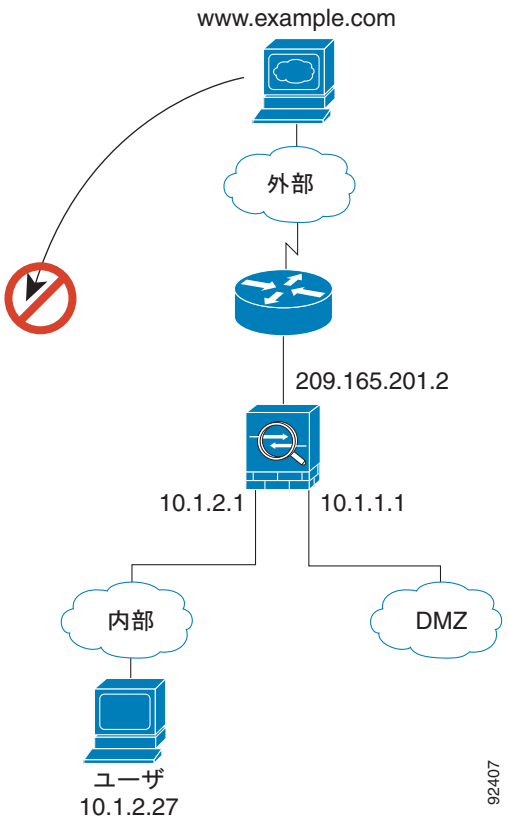
1. 内部ネットワーク上のユーザは、宛先アドレス 10.1.1.3 を使用して DMZ Web サーバから Web ページを要求します。
2. セキュリティ アプライアンスはパケットを受信します。これは新しいセッションであるため、セキュリティ アプライアンスはセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

   マルチ コンテキスト モードの場合、セキュリティ アプライアンスは、コンテキストに関連付けられる固有なインターフェイスまたは固有な宛先アドレスに従ってパケットを分類します。宛先アドレスは、コンテキストでのアドレス変換と照合することによって関連付けられます。この場合、インターフェイスは固有です。Web サーバ IP アドレスは、最新のアドレス変換を持っていません。
3. 次に、セキュリティ アプライアンスはセッションが確立されたことを記録し、DMZ インターフェイスからパケットを転送します。
4. DMZ Web サーバが要求に応答すると、パケットは高速パスを通過します。これのため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
5. セキュリティ アプライアンスは、パケットを内部ユーザに転送します。

外部ユーザが内部ホストにアクセスしようとする

図 15-5 は、外部ユーザが内部ネットワークにアクセスしようとしていることを示しています。

図 15-5　外部から内部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します（図 15-5 を参照）。

1. 外部ネットワーク上のユーザが、内部ホストに到達しようとします（ホストにルーティング可能な IP アドレスがあると想定します）。

   内部ネットワークがプライベート アドレスを使用している場合、外部ユーザが NAT なしで内部ネットワークに到達することはできません。外部ユーザは既存の NAT セッションを使用して内部ユーザに到達しようとすることが考えられます。

2. セキュリティ アプライアンスはパケットを受信します。これは新しいセッションであるため、セキュリティ アプライアンスはセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）に従って、パケットが許可されているかどうかを確認します。

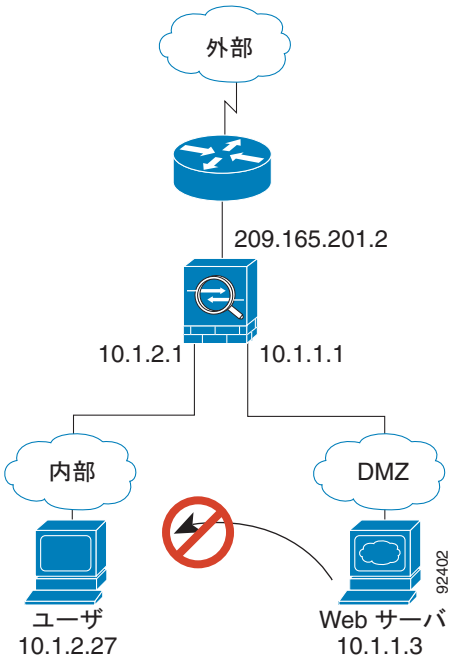
3. パケットが拒否され、セキュリティ アプライアンスはパケットをドロップし、接続試行をログに記録します。

   外部ユーザが内部ネットワークを攻撃しようとした場合、セキュリティ アプライアンスは多数のテクノロジーを使用して、すでに確立されたセッションに対してパケットが有効かどうかを判別します。

DMZ ユーザが内部ホストにアクセスしようとする

図 15-6 は、DMZ 内のユーザが内部ネットワークにアクセスしようとしていることを示しています。

図 15-6　DMZ から内部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します（図 15-6 を参照）。

1. DMZ ネットワーク上のユーザが、内部ホストに到達しようとします。DMZ はインターネット上のトラフィックをルーティングする必要がないので、プライベート アドレッシング方式はルーティングを回避しません。
2. セキュリティ アプライアンスはパケットを受信します。これは新しいセッションであるため、セキュリティ アプライアンスはセキュリティ ポリシー（アクセス リスト、フィルタ、AAA）に従って、パケットが許可されているかどうかを確認します。
3. パケットが拒否され、セキュリティ アプライアンスはパケットをドロップし、接続試行をログに記録します。

トランスペアレント モードの概要

従来、ファイアウォールはルーテッド ホップであり、保護されたサブネットのいずれかに接続するホストのデフォルト ゲートウェイとして機能します。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとは見なされません。

ここでは、トランスペアレント ファイアウォール モードについて次の項目で説明します。

- 「トランスペアレント ファイアウォール ネットワーク」（P.15-9）
- 「レイヤ 3 トラフィックの許可」（P.15-9）

トランスペアレント ファイアウォール ネットワーク

セキュリティ アプライアンスでは、内部インターフェイスと外部インターフェイスに同じネットワークが接続されます。トランスペアレント ファイアウォールはルーティング対象のホップではないので、既存のネットワークに容易に導入できます。IP 再アドレッシングは不要です。

レイヤ 3 トラフィックの許可

セキュリティの高いインターフェイスからセキュリティの低いインターフェイスへの IPv4 トラフィックは、アクセス リストとは無関係に、トランスペアレント ファイアウォールを自動的に通過できます。ARP は、アクセス リストに関係なく、両方向ともトランスペアレント ファイアウォールを通過できます。ARP トラフィックは、ARP インスペクションによって制御できます。低いセキュリティ インターフェイスから高いセキュリティ インターフェイスに移動するレイヤ 3 トラフィックの場合は、拡張アクセス リストが必要です。

許可される MAC アドレス

次の宛先 MAC アドレスは、トランスペアレント ファイアウォールを通過できます。このリストに存在しない MAC アドレスはドロップされません。

- FFFF.FFFF.FFFF の TRUE ブロードキャスト宛先 MAC アドレス
- 0100.5E00.0000 ～ 0100.5EFE.FFFF までの IPv4 マルチキャスト MAC アドレス
- 3333.0000.0000 ～ 3333.FFFF.FFFF までの IPv6 マルチキャスト MAC アドレス
- 0100.0CCC.CCCD の BPDU マルチキャスト アドレス
- 0900.0700.0000 ～ 0900.07FF.FFFF までの AppleTalk マルチキャスト MAC アドレス

ルーテッド モードで許可されないトラフィックの通過

ルーテッド モードでは、アクセス リストで許可しても、いくつかのタイプのトラフィックはセキュリティ アプライアンスを通過できません。ただし、トランスペアレント ファイアウォールは、拡張アクセス リスト（IP トラフィックの場合）または EtherType アクセス リスト（非 IP トラフィックの場合）を使用してほとんどすべてのトラフィックを許可できます。

（注）　トランスペアレント モードのセキュリティ アプライアンスは、CDP パケット、IPv6 パケット、および 0x600 以上の有効な EtherType を持たないパケットの通過を拒否します。たとえば、IS-IS パケットは通過できません。例外として、BPDU はサポートされています。

たとえば、トランスペアレント ファイアウォールでルーティング プロトコルの隣接関係を確立できます。つまり、拡張アクセス リストに基づいて、OSPF、RIP、EIGRP、または BGP トラフィックを許可できます。同様に、HSRP や VRRP などのプロトコルは セキュリティ アプライアンス を通過できます。

IP 以外のトラフィック（AppleTalk、IPX、BPDU、および MPLS など）は、EtherType アクセス リストを使用して通過するように構成できます。

トランスペアレント ファイアウォールで直接サポートされていない機能の場合は、アップストリーム ルータとダウンストリーム ルータが機能をサポートできるようにトラフィックの通過を許可することができます。たとえば、拡張アクセス リストを使用して、DHCP トラフィック（サポートされない DHCP リレー機能の代わりに）または IP/TV によって作成されたマルチキャスト トラフィックを許可できます。

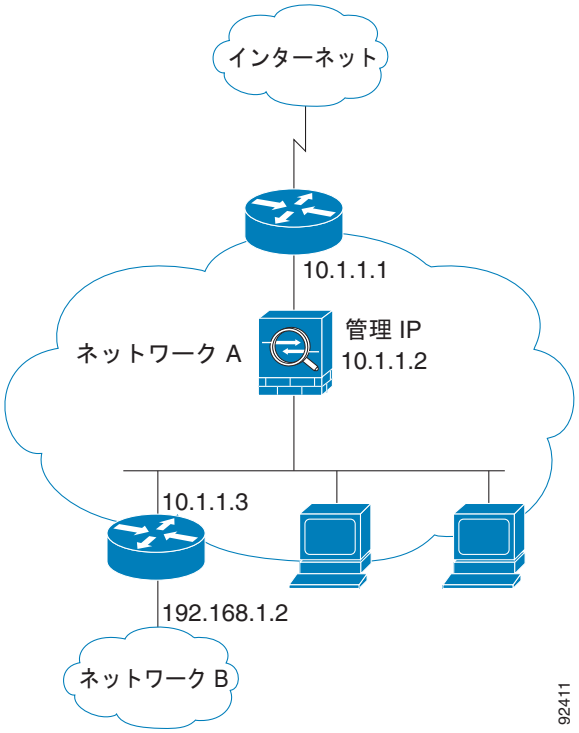
MAC アドレス ルックアップ

セキュリティ アプライアンスがトランスペアレント モードで動作している場合、パケットの発信インターフェイスは、ルート ルックアップではなく MAC アドレス ルックアップを実行することによって決定されます。ルート ステートメントも設定できますが、適用されるのは セキュリティ アプライアンス を起点とするトラフィックだけです。たとえば、Syslog サーバがリモート ネットワークに配置されている場合、セキュリティ アプライアンス がそのサブネットにアクセスできるように、スタティック ルートを使用する必要があります。

ネットワークでのトランスペアレント ファイアウォールの使用

図 15-7 に、外部デバイスが内部デバイスと同じサブネット上にある一般的なトランスペアレント ファイアウォール ネットワークを示します。内部ルータとホストは、外部ルータに直接接続されているように見えます。

図 15-7　トランスペアレント ファイアウォール ネットワーク



トランスペアレント ファイアウォール ガイドライン

トランスペアレント ファイアウォール ネットワークを計画する場合は、次のガイドラインに従ってください。

- 管理 IP アドレスが必要です。マルチ コンテキスト モードの場合は、各コンテキストごとに IP アドレスが必要です。

  インターフェイスごとに IP アドレスが必要なルーテッド モードと異なり、トランスペアレント ファイアウォールではデバイス全体に IP アドレスが割り当てられます。セキュリティ アプライアンスは、この IP アドレスを、システム メッセージや AAA 通信など、セキュリティ アプライアンスで発信されるパケットの送信元アドレスとして使用します。

  管理 IP アドレスは、接続されているネットワークと同じサブネット内にある必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。

  管理専用インターフェイス（Management 0/0）の IP アドレスを設定できます。この IP アドレスは、メインの管理 IP アドレスとは別のサブネットに設定できます。

（注）　管理 IP アドレスが設定されていない場合、一時的トラフィックはトランスペアレント ファイアウォールを通過しません。マルチ コンテキスト モードの場合、一時的トラフィックは仮想コンテキストを通過しません。

- 透過セキュリティ アプライアンスは、内部インターフェイスと外部インターフェイスだけを使用します。プラットフォームに専用の管理インターフェイスが含まれている場合は、管理トラフィック専用の管理インターフェイスまたはサブインターフェイスを設定することもできます。

  シングルモードでは、セキュリティ アプライアンスに 3 つ以上のインターフェイスが含まれている場合でも、2 つのデータ インターフェイス（および使用可能な場合は専用の管理インターフェイス）だけを使用できます。
- 直接に接続された各ネットワークは同一のサブネット上にある必要があります。
- 接続されたデバイス用のデフォルト ゲートウェイとしてセキュリティ アプライアンス管理 IP アドレスを指定しないでください。デバイスはセキュリティ アプライアンスの他方の側のルータをデフォルト ゲートウェイとして指定する必要があります。
- マルチ コンテキスト モードでは、各コンテキストが別個のインターフェイスを使用する必要があります。コンテキスト間でインターフェイスを共有することはできません。
- マルチ コンテキスト モードでは、通常、各コンテキストが別個のサブネットを使用します。重複するサブネットを使用することもできますが、ルーティング スタンドポイントから可能にするため、ネットワーク トポロジにルータと NAT コンフィギュレーションが必要です。

トランスペアレント モードでサポートされていない機能

表 15-1 にトランスペアレント モードでサポートされていない機能を示します。

表 15-1　トランスペアレント モードでサポートされていない機能

機能	説明
ダイナミック DNS	—
DHCP リレー	トランスペアレント ファイアウォールは DHCP サーバとして機能することができますが、DHCP リレー コマンドはサポートしません。2 つの拡張アクセス リストを使用して DHCP トラフィックを通過させることができるので、DHCP リレーは必要ありません。1 つは内部インターフェイスから外部インターフェイスへの DHCP 要求を許可し、もう 1 つはサーバからの応答を逆方向に許可します。
ダイナミック ルーティング プロトコル	ただし、セキュリティ アプライアンスで発信されたトラフィックのスタティック ルートを追加できます。拡張アクセス リストを使用して、ダイナミック ルーティング プロトコルがセキュリティ アプライアンスを通過できるようにすることもできます。
IPv6	EtherType アクセス リストを使用した IPv6 は許可できません。
マルチキャスト	拡張アクセス リストで許可することによって、マルチキャスト トラフィックがセキュリティ アプライアンスを通過できるようにすることができます。
NAT	NAT はアップストリーム ルータで実行されます。

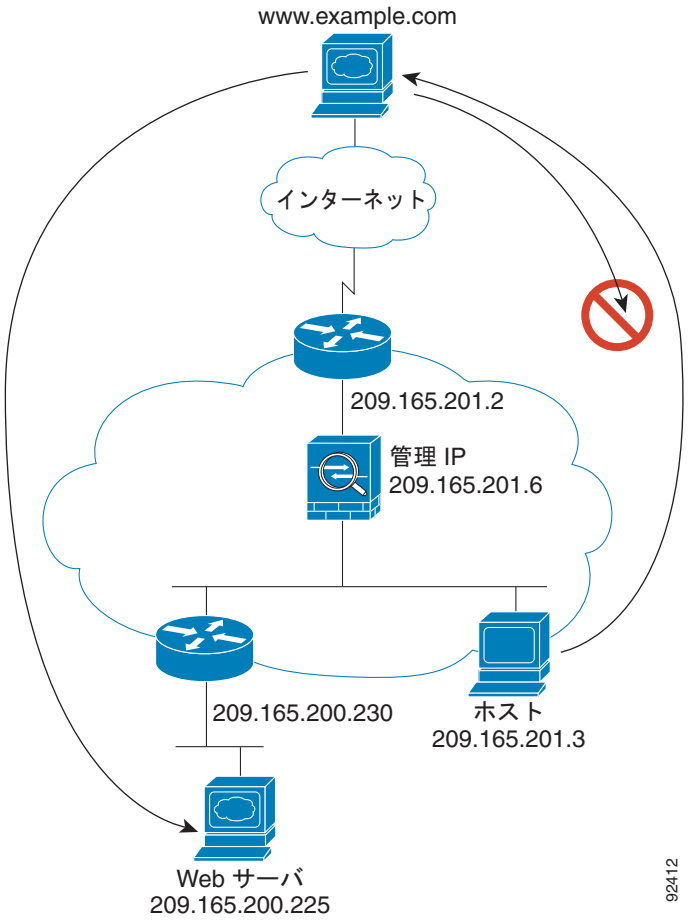
表 15-1　トランスペアレント モードでサポートされていない機能 （続き）

機能	説明
QoS	—
通過トラフィック用の VPN ターミネーション	トランスペアレント ファイアウォールは、管理接続に対してのみサイトツーサイト VPN トンネルをサポートします。これは、セキュリティ アプライアンスを通過するトラフィックに対して VPN 接続を終端しません。拡張アクセス リストを使用して VPN トラフィックにセキュリティ アプライアンスを通過させることはできますが、非管理接続は終端されません。WebVPN もサポートされていません。

トランスペアレント ファイアウォールを通過するデータの動き

図 15-8 に、パブリック Web サーバを含む内部ネットワークを持つ一般的なトランスペアレント ファイアウォールの実装を示します。内部ユーザがインターネット リソースにアクセスできるよう、セキュリティ アプライアンスにはアクセス リストがあります。別のアクセス リストによって、外部ユーザは内部ネットワーク上の Web サーバだけにアクセスできます。

図 15-8　一般的なトランスペアレント ファイアウォールのデータ パス



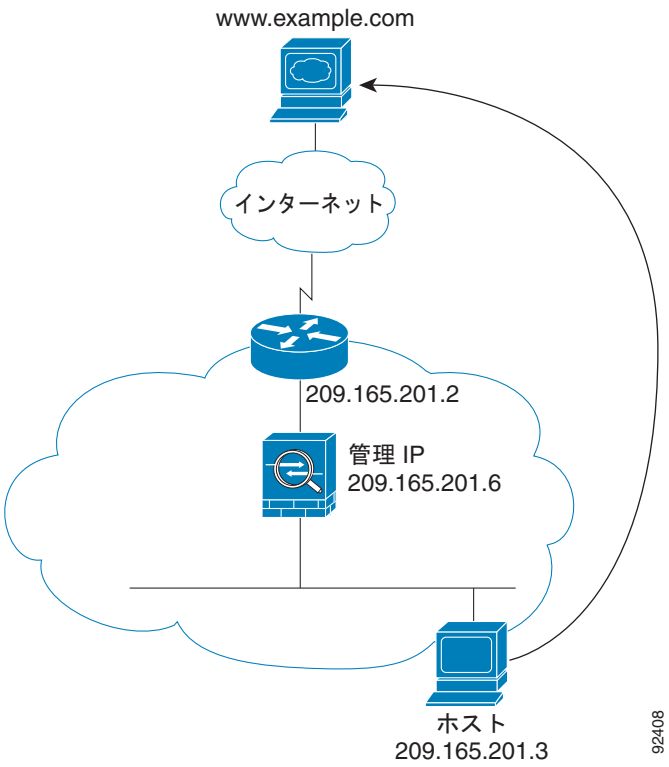
ここでは、データが セキュリティ アプライアンス をどのように通過するかについて説明します。内容は次のとおりです。

- 「内部ユーザが Web サーバにアクセスする」（P.15-15）
- 「外部ユーザが内部ネットワーク上の Web サーバにアクセスする」（P.15-16）
- 「外部ユーザが内部ホストにアクセスしようとする」（P.15-17）

内部ユーザが Web サーバにアクセスする

図 15-9 は、内部ユーザが外部 Web サーバにアクセスしていることを示しています。

図 15-9　内部から外部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します（図 15-9 を参照）。

1. 内部ネットワークのユーザは、www.example.com から Web ページを要求します。
2. セキュリティ アプライアンスはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

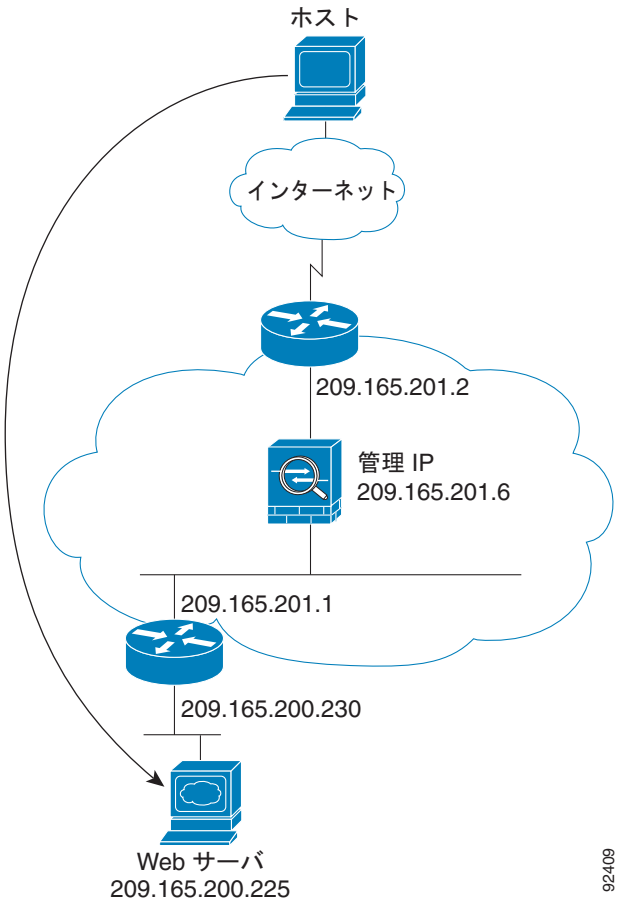
   マルチ コンテキスト モードの場合、セキュリティ アプライアンスは、固有なインターフェイスに従ってパケットを分類します。
3. セキュリティ アプライアンスは、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、セキュリティ アプライアンスは外部インターフェイスからパケットを転送します。宛先 MAC アドレスは、アップストリーム ルータのアドレス 209.165.20 1.2 です。

   宛先 MAC アドレスが セキュリティ アプライアンス のテーブルにない場合、セキュリティ アプライアンス は MAC アドレスを検出するために ARP 要求または ping を送信します。最初のパケットはドロップされます。
5. Web サーバが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
6. セキュリティ アプライアンスは、パケットを内部ユーザに転送します。

外部ユーザが内部ネットワーク上の Web サーバにアクセスする

図 15-10 は、外部ユーザが内部 Web サーバにアクセスしていることを示しています。

図 15-10　外部から内部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します（図 15-10 を参照）。

1. 外部ネットワーク上のユーザは、内部 Web サーバから Web ページを要求します。
2. セキュリティ アプライアンスはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

   マルチ コンテキスト モードの場合、セキュリティ アプライアンスは、固有なインターフェイスに従ってパケットを分類します。
3. セキュリティ アプライアンスは、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、セキュリティ アプライアンスは内部インターフェイスからパケットを転送します。宛先 MAC アドレスは、ダウンストリーム ルータ 209.165.201.1 のアドレスです。

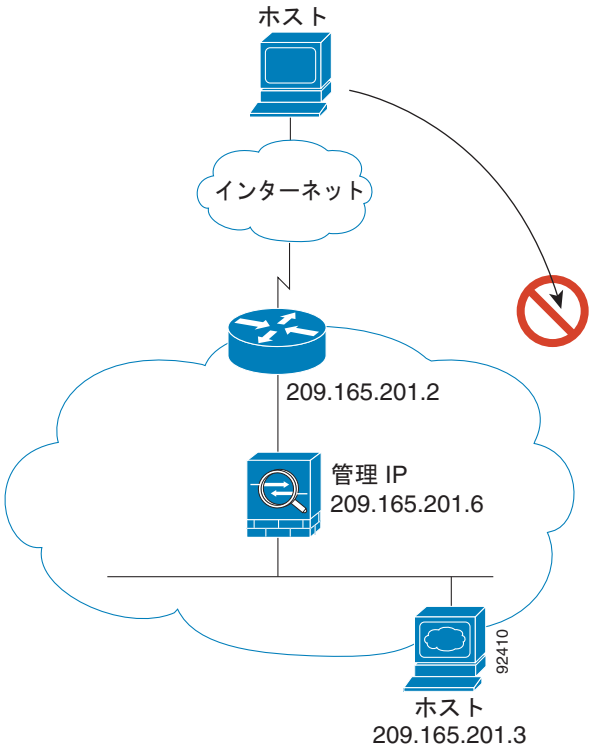
   宛先 MAC アドレスがセキュリティ アプライアンスのテーブルにない場合、セキュリティ アプライアンスは、ARP 要求と ping を送信して、MAC アドレスを検出しようとします。最初のパケットはドロップされます。

5. Web サーバが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
6. セキュリティ アプライアンスは、パケットを外部ユーザに転送します。

外部ユーザが内部ホストにアクセスしようとする

図 15-11 は、外部ユーザが内部ネットワーク上のホストにアクセスしようとしていることを示しています。

図 15-11　外部から内部へ



次の手順では、データがセキュリティ アプライアンスをどのように通過するかを示します（図 15-11 を参照）。

1. 外部ネットワーク上のユーザが、内部ホストに到達しようとします。
2. セキュリティ アプライアンスはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシー（アクセス リスト、フィルタ、AAA）の条件に従って、パケットが許可されているかどうかを確認します。

   マルチ コンテキスト モードの場合、セキュリティ アプライアンスは、固有なインターフェイスに従ってパケットを分類します。
3. パケットが拒否され、セキュリティ アプライアンス がパケットを廃棄します。
4. 外部ユーザが内部ネットワークを攻撃しようとした場合、セキュリティ アプライアンスは多数のテクノロジーを使用して、すでに確立されたセッションに対してパケットが有効かどうかを判別します。