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、P.2-7 の「透過ファイアウォール モードまたはルーテッド ファイアウォール モードの設定」を参照してください。

次の事項について説明します。

- ルーテッド モードの概要（P.15-2）
- 透過モードの概要（P.15-9）

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。接続されたネットワーク間で NAT を実行し、（シングルコンテキスト モードで）OSPF または RIP を使用することができます。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。

ここでは、次の項目について説明します。

- IP ルーティングのサポート（P.15-2）
- ネットワーク アドレス変換（P.15-2）
- 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（P.15-3）

IP ルーティングのサポート

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、パケット上のローカル アドレスを、宛先ネットワークでルーティングできるグローバル アドレスに置換します。デフォルトでは、NAT は必要ありません。高セキュリティ インターフェイス（内部）上のホストに対して、低セキュリティ インターフェイス（外部）と通信する際に NAT を使用することを要求する NAT ポリシーを強制する場合は、NAT 制御をイネーブルにします（**nat-control** コマンドを参照）。

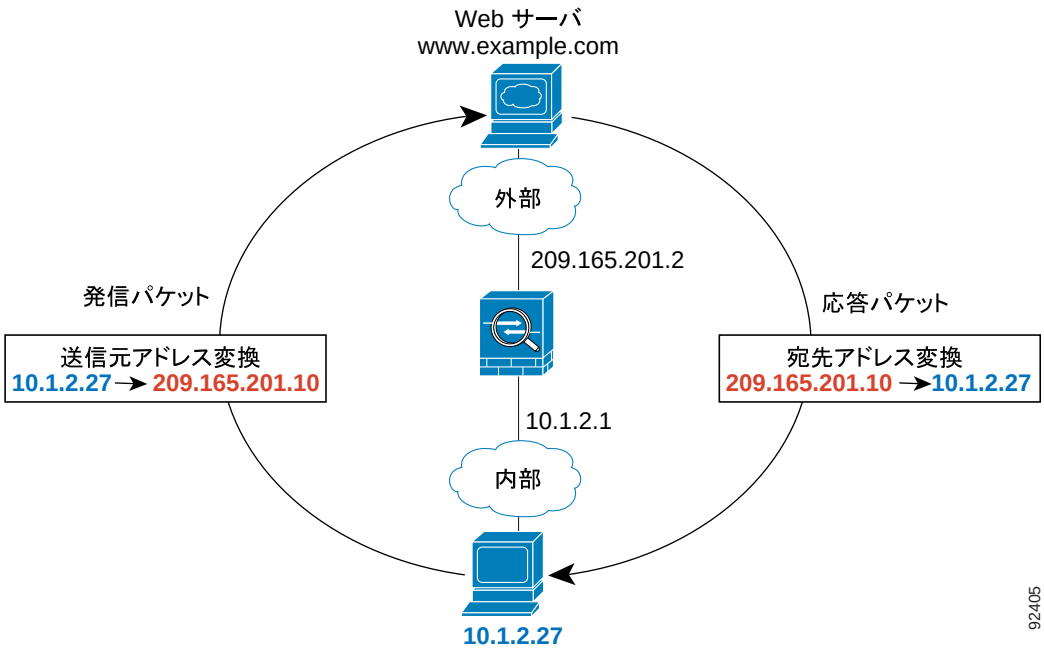
（注）　NAT 制御は、バージョン 7.0 より前のソフトウェア バージョンではデフォルトの処理です。セキュリティ アプライアンスを以前のバージョンからアップグレードする場合は、期待される処理を維持するために、**nat-control** コマンドが自動的にコンフィギュレーションに追加されます。

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一般的な 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上の 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が、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 サーバは応答をグローバル アドレスに送信し、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 アプライアンスはグローバル アドレスをローカル アドレスに変換してから、それをユーザに送信します。

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

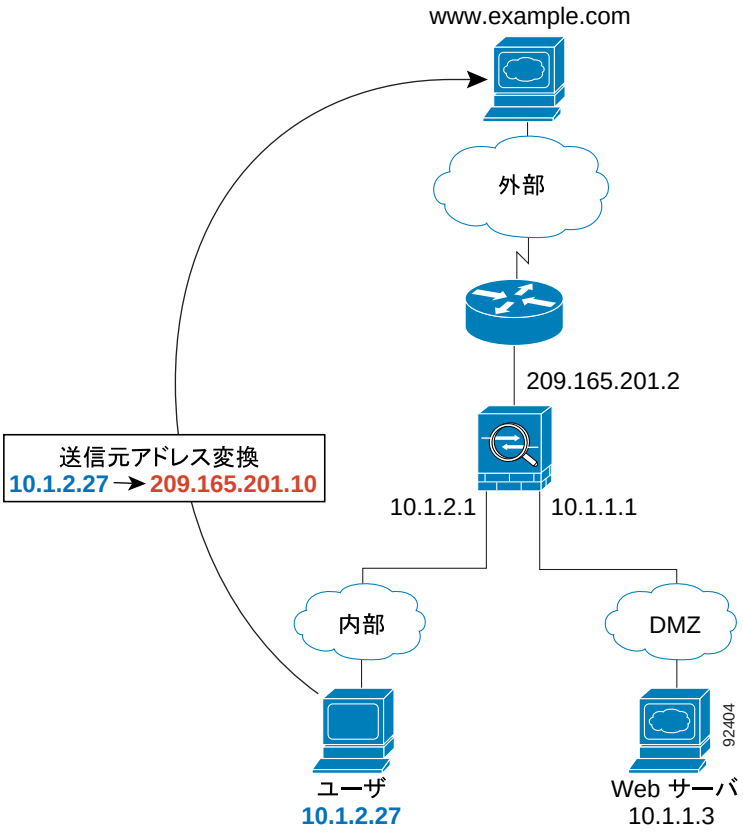
この項では、ルーテッド ファイアウォール モードでデータがセキュリティ アプライアンスをどのように通過するかを説明します。次の項目について説明します。

- 内部ユーザが Web サーバにアクセスする（P.15-3）
- 外部ユーザが DMZ 上の Web サーバにアクセスする（P.15-5）
- 内部ユーザが DMZ 上の Web サーバにアクセスする（P.15-6）
- 外部ユーザが内部ホストにアクセスしようとする（P.15-7）
- DMZ ユーザが内部ホストにアクセスしようとする（P.15-8）

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。

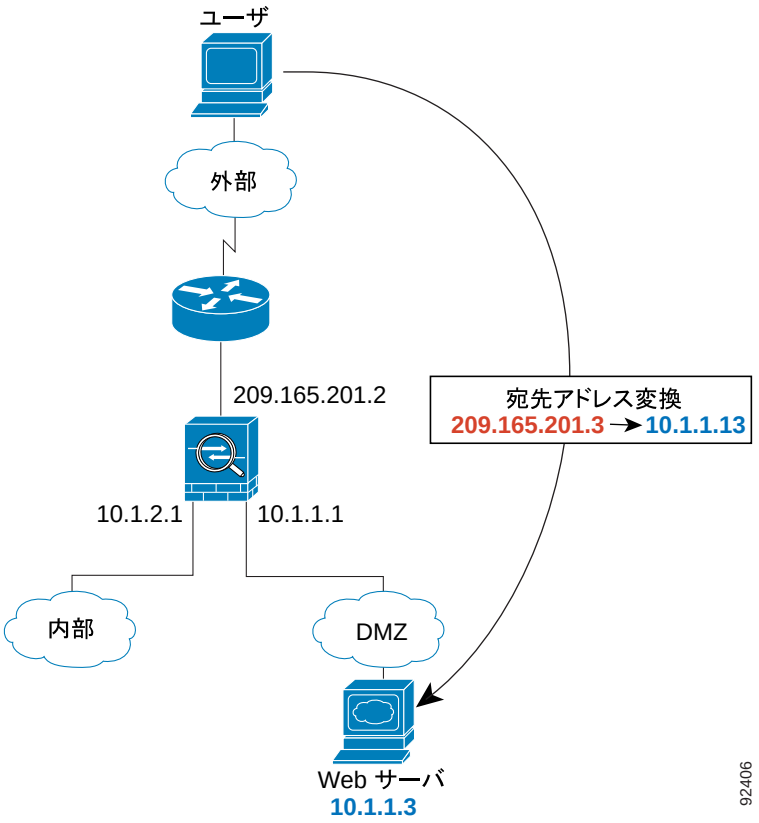
   マルチコンテキスト モードの場合、セキュリティ アプライアンスは、コンテキストに関連付けられる一意なインターフェイスまたは一意な宛先アドレスに従ってパケットを分類します。宛先アドレスは、コンテキストでのアドレス変換と照合することによって関連付けられます。この場合、インターフェイスは固有です。www.example.com の IP アドレスは、コンテキスト内に最新のアドレス変換を持っていません。
3. セキュリティ アプライアンスは、ローカル送信元アドレス（10.1.2.27）を、外部インターフェイス サブネット上のグローバル アドレス 209.165.201.10 に変換します。

   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）。

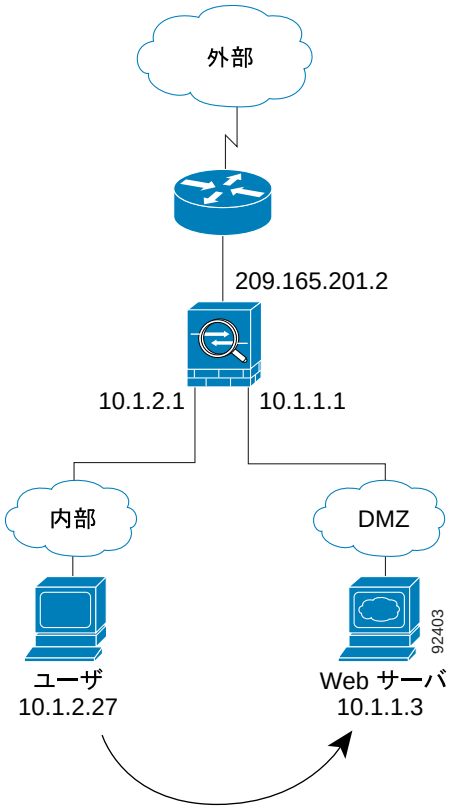
1. 外部ネットワーク上のユーザは、外部インターフェイス サブネット上にあるグローバル宛先アドレス 209.165.201.3 を使用して DMZ Web サーバから Web ページを要求します。
2. セキュリティ アプライアンスはパケットを受信します。これは新しいセッションであるため、セキュリティ アプライアンスはセキュリティ ポリシー（アクセスリスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

   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一意なインターフェイスまたは一意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）。

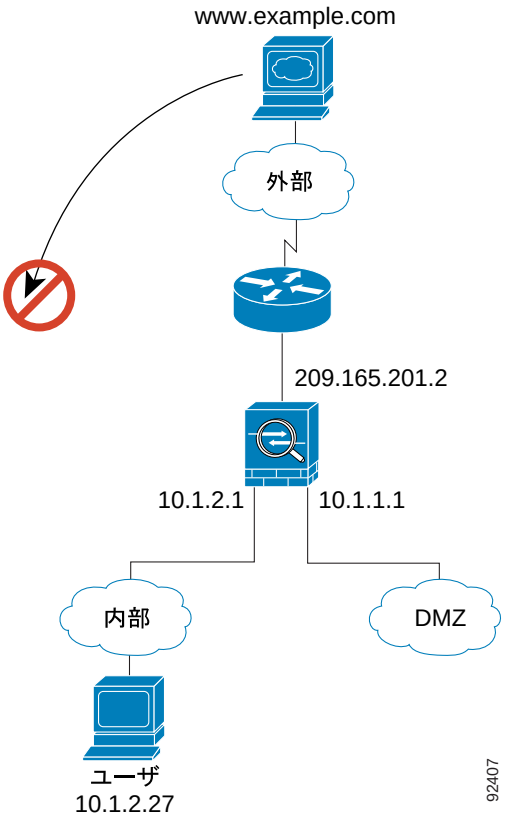
1. 内部ネットワーク上のユーザは、宛先アドレス 10.1.1.3 を使用して DMZ Web サーバから Web ページを要求します。
2. セキュリティ アプライアンスはパケットを受信します。これは新しいセッションであるため、セキュリティ アプライアンスはセキュリティ ポリシー（アクセスリスト、フィルタ、AAA）の条件に従って、パケットが許可されていることを確認します。

   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一意なインターフェイスまたは一意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。

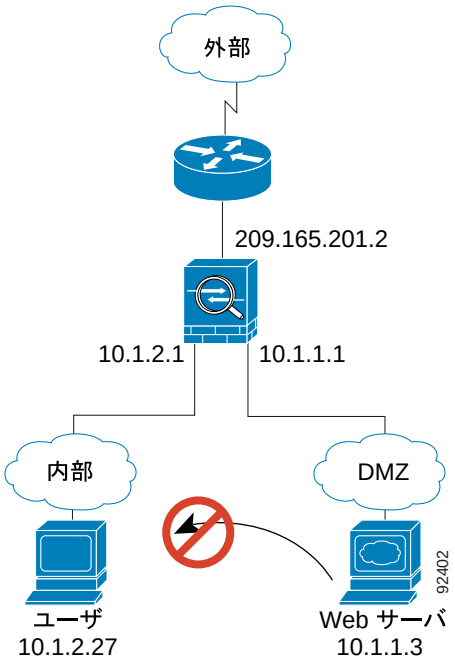
3. パケットが拒否され、セキュリティ アプライアンスはパケットをドロップし、接続試行をログに記録します。

   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。

透過モードの概要

通常、ファイアウォールはルーティングされたホップであり、スクリーニング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、透過ファイアウォールは、「bump-in-the-wire（BITW）」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、透過ファイアウォール モードについて次の項目で説明します。

- 透過ファイアウォール 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）
- ルーテッド モードで許可されないトラフィックの通過（P.15-10）
- MAC アドレス ルックアップ（P.15-10）
- ネットワークでの透過ファイアウォールの使用（P.15-11）
- 透過ファイアウォール ガイドライン（P.15-11）
- 透過モードでサポートされない機能（P.15-12）
- 透過ファイアウォールを通過するデータの動き（P.15-13）

透過ファイアウォール 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。透過ファイアウォールはルーティングされたホップではないので、既存のネットワークに簡単に導入できます。IP 再アドレッシングは必要ありません。

レイヤ 3 トラフィックの許可

IPv4 トラフィックは、自動的に高位のセキュリティ インターフェイスから低位のセキュリティ インターフェイスにアクセスリストなしで透過ファイアウォールを通過できます。ARP は、アクセスリストなしで両方向に透過ファイアウォールを通過できます。ARP トラフィックは ARP 検査によって制御されます。低位から高位のセキュリティ インターフェイスに移動するレイヤ 3 トラフィックでは、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、透過ファイアウォールから許可されます。このリストにない MAC アドレスはすべてドロップされます。

- 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。一方、透過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（IP 以外のトラフィックの場合）を使用して、ほとんどのトラフィックを許可することができます。

（注）　透過モードのセキュリティ アプライアンスは CDP パケットの通過も IPv6 パケットの通過も拒否し、0x600 以上の有効な EtherType を持たないパケットの通過も拒否します。たとえば、IS-IS パケットを通過させることはできません。例外は BPDU で、これはサポートされます。

たとえば、透過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することができます。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。

透過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トラフィックなどのマルチキャスト トラフィックを許可できます。

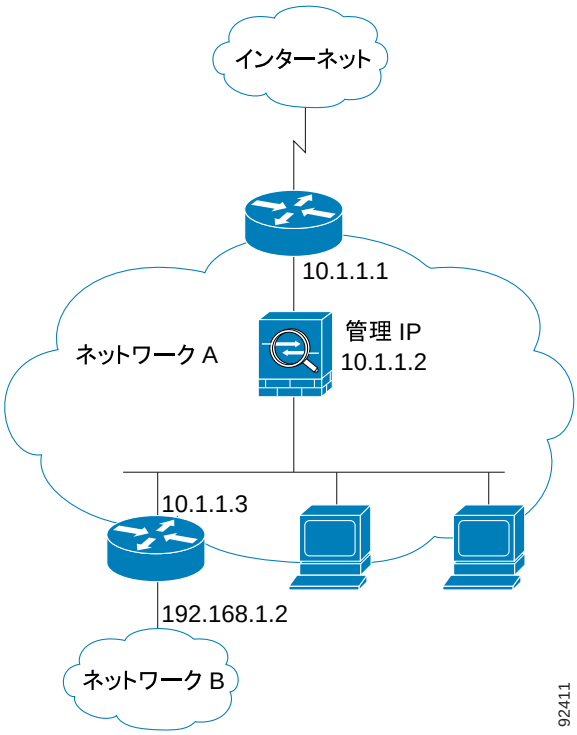
MAC アドレス ルックアップ

セキュリティ アプライアンスが透過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。この場合もルート文を設定することはできますが、セキュリティ アプライアンスから発信されたトラフィックだけに適用されます。たとえば、syslog サーバがリモート ネットワークにある場合は、セキュリティ アプライアンスがそのサブネットに到達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。

ネットワークでの透過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透過ファイアウォール 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　透過ファイアウォール ネットワーク



透過ファイアウォール ガイドライン

透過ファイアウォール 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、透過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 アドレスとは別々のサブネットに設定することができます。

- 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。

透過モードでサポートされない機能

表 15-1 に透過モードでサポートされていない機能を示します。

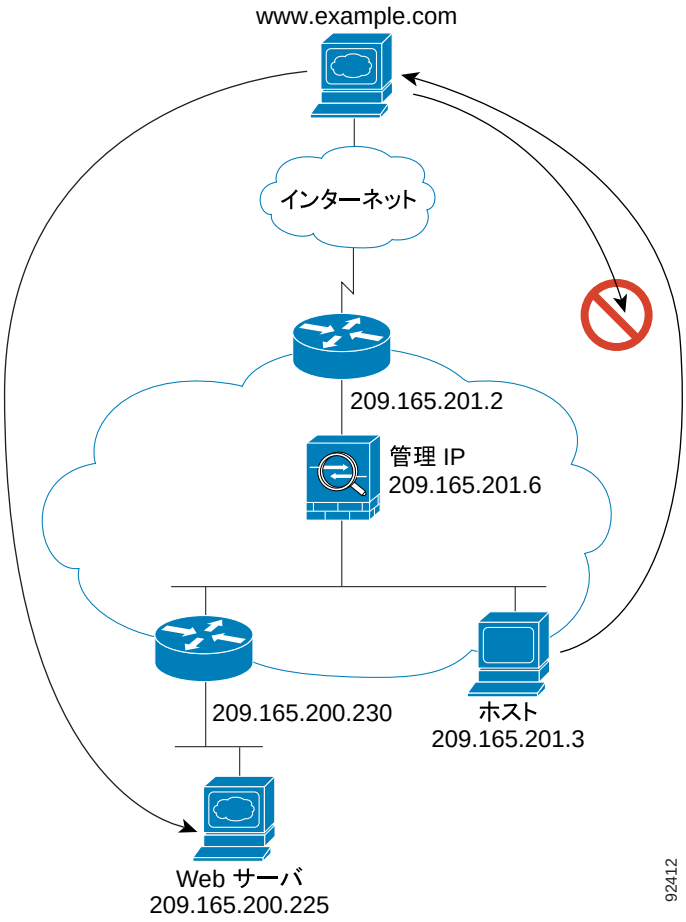
表 15-1　透過モードでサポートされていない機能

機能	説明
ダイナミック DNS	—
DHCP リレー	透過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 DCHP 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。
QoS	—
通過トラフィック用の VPN ターミネーション	透過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。

透過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透過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　一般的な透過ファイアウォールのデータ パス



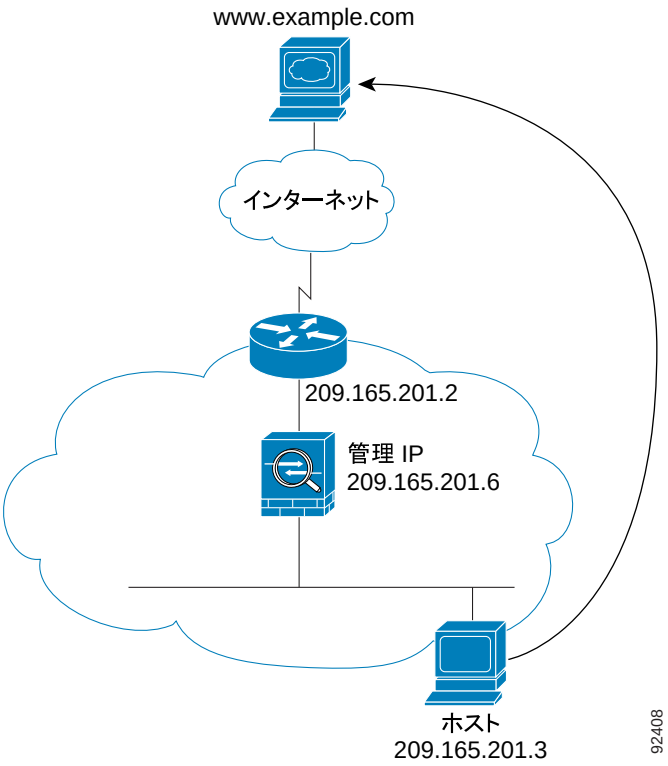
この項では、データがセキュリティ アプライアンスをどのように通過するかを説明します。次の項目について説明します。

- 内部ユーザが Web サーバにアクセスする（P.15-14）
- 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.15-15）
- 外部ユーザが内部ホストにアクセスしようとする（P.15-16）

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。

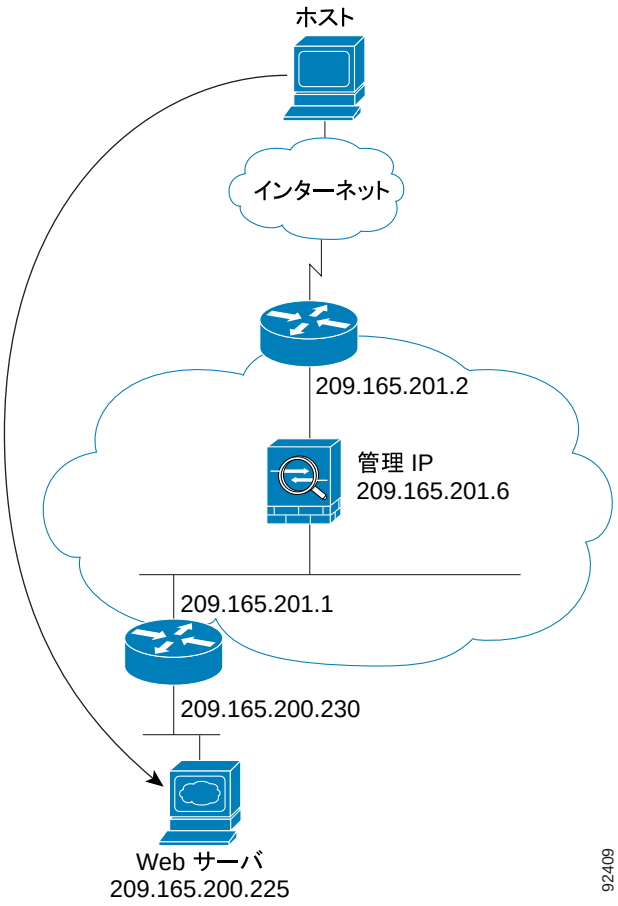
   マルチコンテキスト モードの場合、セキュリティ アプライアンスは、一意なインターフェイスに従ってパケットを分類します。
3. セキュリティ アプライアンスは、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、セキュリティ アプライアンスは外部インターフェイスからパケットを転送します。宛先 MAC アドレスは、アップストリーム ルータ 209.186.201.2 のアドレスです。

   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、一意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 209.186.201.1 のアドレスです。

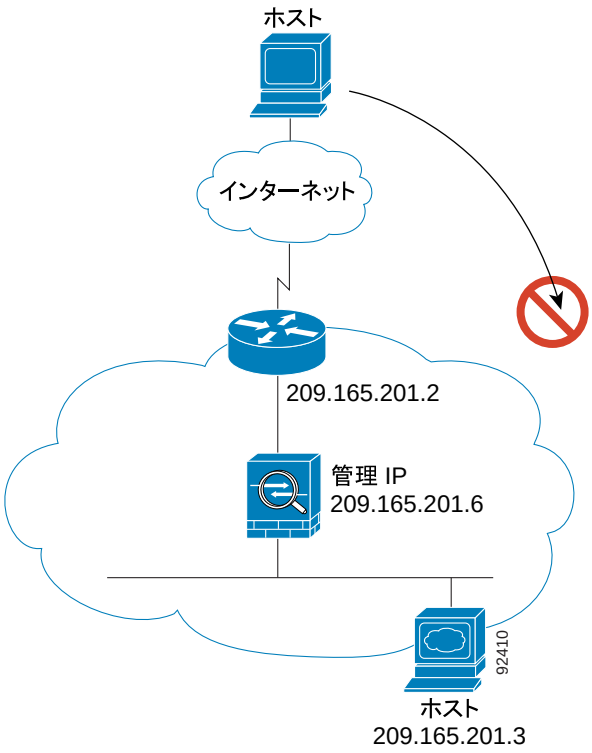
   宛先 MAC アドレスがセキュリティ アプライアンスのテーブルにない場合、セキュリティ アプライアンスは、ARP 要求と ping を送信して、MAC アドレスを検出しようとします。最初のパケットはドロップされます。

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、一意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 アプライアンスはパケットをドロップします。
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。