



トランスペアレント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

この章では、ファイアウォールモードをルーテッドまたはトランスペアレントに設定する方法と、ファイアウォールが各ファイアウォールモードでどのように機能するかについて説明します。

マルチコンテキストモードでは、コンテキストごとに別個にファイアウォールモードを設定できます。

- [ファイアウォールモードについて \(1 ページ\)](#)
- [デフォルト設定 \(12 ページ\)](#)
- [ファイアウォールモードのガイドライン \(12 ページ\)](#)
- [ファイアウォールモードの設定 \(14 ページ\)](#)
- [ファイアウォールモードの例 \(15 ページ\)](#)
- [ファイアウォールモードの履歴 \(26 ページ\)](#)

ファイアウォールモードについて

ASA は、ルーテッドファイアウォールモードとトランスペアレントファイアウォールモードの 2 つのファイアウォールモードをサポートします。

ルーテッドファイアウォールモードについて

ルーテッドモードでは、ASA はネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。コンテキスト間でレイヤ 3 インターフェイスを共有することもできます。

統合ルーティングおよびブリッジングにより、ネットワーク上の複数のインターフェイスをまとめた「ブリッジグループ」を使用できます。そして、ASA はブリッジング技術を使用してインターフェイス間のトラフィックを通すことができます。各ブリッジグループには、ネット

ワーク上で IP アドレスが割り当てられるブリッジ仮想インターフェイス (BVI) が含まれます。ASA は BVI と通常のルーテッドインターフェイス間でルーティングを行います。マルチコンテキストモード、クラスタリング、EtherChannel、冗長または VNI メンバーインターフェイスが必要ない場合は、トランスペアレント モードではなくルーテッド モードの使用を検討すべきです。ルーテッド モードでは、トランスペアレント モードと同様に 1 つ以上の分離されたブリッジグループを含めることができます。また、モードが混在する導入に関しては、通常のルーテッドインターフェイスも含めることができます。

トランスペアレント ファイアウォール モードについて

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。これに対し、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しては認識されません。ただし、他のファイアウォールのように、インターフェイス間のアクセス制御は管理され、ファイアウォールによる通常のすべてのチェックが実施されます。

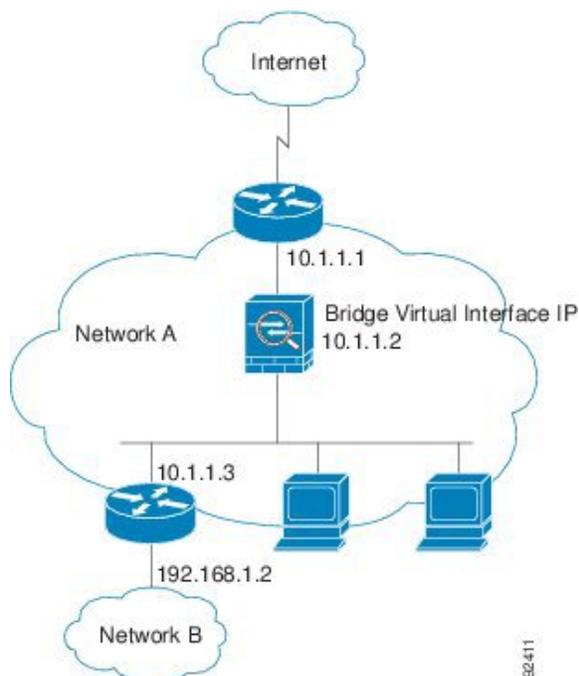
レイヤ2の接続は、ネットワークの内部と外部のインターフェイスをまとめた「ブリッジグループ」を使用して実現されます。また、ASA はブリッジング技術を使用してインターフェイス間のトラフィックを通すことができます。各ブリッジグループには、ネットワーク上で IP アドレスが割り当てられるブリッジ仮想インターフェイス (BVI) が含まれます。複数のネットワークに複数のブリッジグループを設定できます。トランスペアレント モードでは、これらのブリッジグループは相互通信できません。

ネットワーク内でトランスペアレント ファイアウォールの使用

ASA は、自身のインターフェイス間を同じネットワークで接続します。トランスペアレント ファイアウォールはルーティングされたホップではないため、既存のネットワークに簡単に導入できます。

次の図に、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 1: トランスペアレントファイアウォールネットワーク



管理インターフェイス

各ブリッジ仮想インターフェイス（BVI）IPアドレスのほかに、別の管理スロット/ポートインターフェイスを追加できます。このインターフェイスはどのブリッジグループにも属さず、ASAへの管理トラフィックのみを許可します。詳細については、[管理インターフェイス](#)を参照してください。

ルーテッドモード機能のためのトラフィックの通過

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、アクセスルールを使用することによって、（サポートされていないDHCPリレー機能の代わりに）DHCPトラフィックを許可したり、IP/TVで作成されるようなマルチキャストトラフィックを許可したりできます。また、トランスペアレントファイアウォールを通過するルーティングプロトコル隣接関係を確立することもできます。つまり、OSPF、RIP、EIGRP、またはBGPトラフィックをアクセスルールに基づいて許可できます。同様に、HSRPやVRRPなどのプロトコルはASAを通過できます。

ブリッジグループについて

ブリッジグループは、ASAがルーティングではなくブリッジするインターフェイスのグループです。ブリッジグループはトランスペアレントファイアウォールモード、ルーテッドファイアウォールモードの両方でサポートされています。他のファイアウォールインターフェイス

スのように、インターフェイス間のアクセス制御は管理され、ファイアウォールによる通常のすべてのチェックが実施されます。

ブリッジ仮想インターフェイス (BVI)

各ブリッジグループには、ブリッジ仮想インターフェイス (BVI) が含まれます。ASA は、ブリッジグループから発信されるパケットの送信元アドレスとしてこの BVI IP アドレスを使用します。BVI IP アドレスは□ブリッジグループ メンバー インターフェイスと同じサブネット上になければなりません。BVI では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。

トランスペアレントモード：インターフェイスベースの各機能はブリッジグループのメンバーインターフェイスだけを指定でき、これらについてのみ使用できます。

ルーテッドモード：BVI はブリッジグループと他のルーテッドインターフェイス間のゲートウェイとして機能します。ブリッジグループ/ルーテッドインターフェイス間でルーティングするには、BVI を指定する必要があります。一部のインターフェイスベース機能に代わり、BVI 自体が利用できます。

- アクセスルール：ブリッジグループのメンバーインターフェイスと BVI 両方のアクセスルールを設定できます。インバウンドのルールでは、メンバーインターフェイスが先にチェックされます。アウトバウンドのルールでは BVI が最初にチェックされます。
- DHCPv4 サーバ：BVI のみが DHCPv4 サーバの構成をサポートします。
- スタティックルート：BVI のスタティックルートを設定できます。メンバーインターフェイスのスタティックルートは設定できません。
- Syslog サーバと ASA 由来の他のトラフィック：syslog サーバ（または SNMP サーバ、ASA からトラフィックが送信される他のサービス）を指定する際、BVI またはメンバーインターフェイスのいずれかも指定できます。

ルーテッドモードで BVI を指定しない場合、ASA はブリッジグループのトラフィックをルーティングしません。この設定は、ブリッジグループのトランスペアレント ファイアウォールモードを複製します。マルチコンテキストモード、クラスタリング、EtherChannel、冗長または VNI メンバーインターフェイスが不要であれば、ルーテッドモードの使用を検討すべきです。ルーテッドモードでは、トランスペアレントモードと同様に1つ以上の分離されたブリッジグループを含めることができます。また、モードが混在する導入に関しては、通常のルーテッドインターフェイスも含めることができます。

トランスペアレント ファイアウォール モードのブリッジグループ

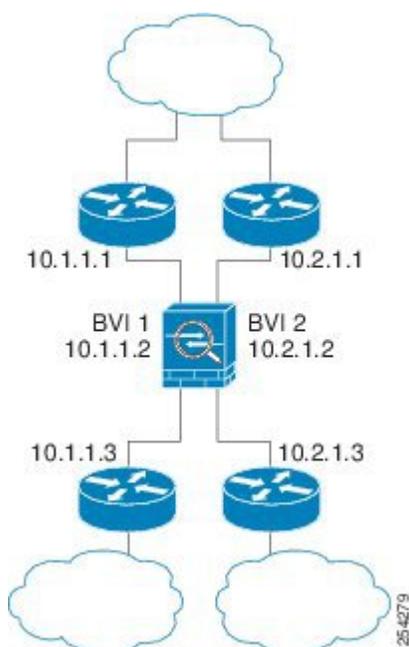
ブリッジグループのトラフィックは他のブリッジグループから隔離され、トラフィックは ASA 内の他のブリッジグループにはルーティングされません。また、トラフィックは外部ルータから ASA 内の他のブリッジグループにルーティングされる前に、ASA から出る必要があります。ブリッジング機能はブリッジグループごとに分かれています。その他の多くの機能はすべてのブリッジグループ間で共有されます。たとえば、syslog サーバまたは AAA サーバの設定は、すべてのブリッジグループで共有されます。セキュリティ ポリシーを完全に分離する

には、各コンテキスト内に1つのブリッジグループにして、セキュリティコンテキストを使用します。

1つのブリッジグループにつき複数のインターフェイスを入れることができます。サポートされるブリッジグループとインターフェイスの正確な数については、[ファイアウォールモードのガイドライン \(12 ページ\)](#) を参照してください。ブリッジグループごとに2つ以上のインターフェイスを使用する場合は、内部、外部への通信だけでなく、同一ネットワーク上の複数のセグメント間の通信を制御できます。たとえば、相互通信を希望しない内部セグメントが3つある場合、インターフェイスを別々のセグメントに置き、外部インターフェイスとのみ通信させることができます。または、インターフェイス間のアクセスルールをカスタマイズし、希望通りのアクセスを設定できます。

次の図に、2つのブリッジグループを持つ、ASAに接続されている2つのネットワークを示します。

図2: 2つのブリッジグループを持つトランスパアレントファイアウォールネットワーク



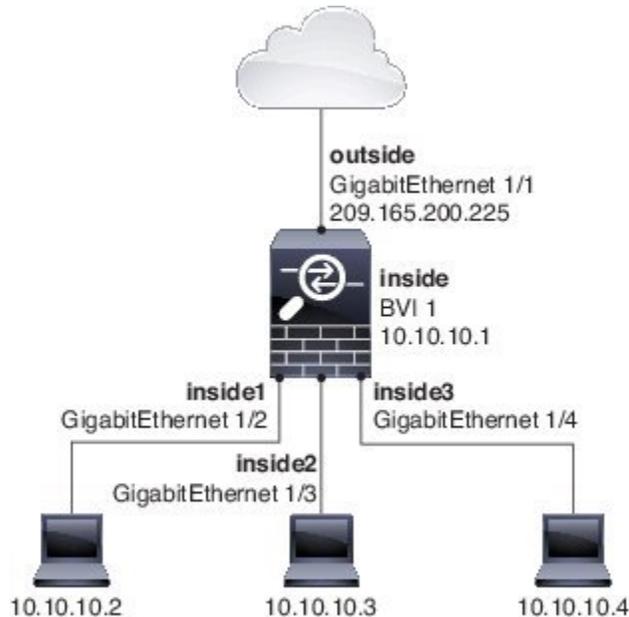
ルーテッドファイアウォールモードのブリッジグループ

ブリッジグループトラフィックは、他のブリッジグループまたはルーテッドインターフェイスにルーティングできます。ブリッジグループのBVIインターフェイスに名前を割り当てないでおくことで、ブリッジグループトラフィックを分離できます。BVIの名前を指定すると、このBVIは他の通常のインターフェイスと同様にルーティングに参加します。

ルーテッドモードでブリッジグループを使用する方法として、外部スイッチの代わりにASA追加のインターフェイスを使用する方法があります。たとえば、一部のデバイスのデフォルト設定では、外部インターフェイスが通常のインターフェイスとして含まれており、その他のすべてのインターフェイスが内部ブリッジグループに割り当てられています。このブリッジグループは、外部スイッチを置き換えることを目的としているため、すべてのブリッジグループ

インターフェイスが自由に通信できるようにアクセス ポリシーを設定する必要があります。たとえば、デフォルト設定ではすべてのインターフェイスを同一のセキュリティレベルに設定し、同じセキュリティ インターフェイス通信を有効にします。アクセス ルールは不要です。

図 3: 内部ブリッジグループと外部ルーテッドインターフェイスからなるルーテッドファイアウォールネットワーク



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 ルールで許可しても、いくつかのタイプのトラフィックは ASA を通過できません。ただし、ブリッジグループは、アクセス ルール (IP トラフィックの場合) または EtherType ルール (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。

- IP トラフィック : ルーテッド ファイアウォール モードでは、ブロードキャストとマルチキャストトラフィックは、アクセスルールで許可されている場合でもブロックされます。これには、サポートされていないダイナミック ルーティング プロトコルおよび DHCP (DHCP リレーを設定している場合を除く) が含まれます。ブリッジグループ内では、このトラフィックをアクセスルール (拡張 ACL を使用) で許可できます。
- 非 IP トラフィック : AppleTalk、IPX、BPDU や MPLS などは、EtherType ルールを使用することで、通過するように設定できます。



(注) ブリッジグループは、CDP 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。サポートされる例外は、BPDU および IS-IS です。

レイヤ3トラフィックの許可

- ユニキャストの IPv4 および IPv6 トラフィックは、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に移動する場合、アクセスルールなしで自動的にブリッジグループを通過できます。
- セキュリティの低いインターフェイスからセキュリティの高い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、セキュリティの低いインターフェイスでアクセスルールが必要です。
- ARP は、アクセスルールなしで両方向にブリッジグループを通過できます。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。
- IPv6 ネイバー探索およびルータ送信要求パケットは、アクセスルールを使用して通過させることができます。
- ブロードキャストおよびマルチキャストトラフィックは、アクセスルールを使用して通過させることができます。

許可される MAC アドレス

アクセスポリシーで許可されている場合、以下の宛先 MAC アドレスをブリッジグループで使用できます ([レイヤ3トラフィックの許可 \(7 ページ\)](#) を参照)。このリストにない MAC アドレスはドロップされます。

- 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 MAC アドレス

BPDU の処理

スパニングツリープロトコルの使用によるループを回避するために、デフォルトで BPDU が渡されます。BPDU をブロックするには、これらを拒否する EtherType ルールを設定する必要があります。フェールオーバーを使用している場合、BPDU をブロックして、トポロジが変更されたときにスイッチポートがブロッキングステートに移行することを回避できます。詳細については、「[フェールオーバーのブリッジグループ要件](#)」を参照してください。

MAC アドレスとルートルックアップ

ブリッジグループ内のトラフィックでは、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宛先 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。

ただし、次の場合にはルートルックアップが必要です。

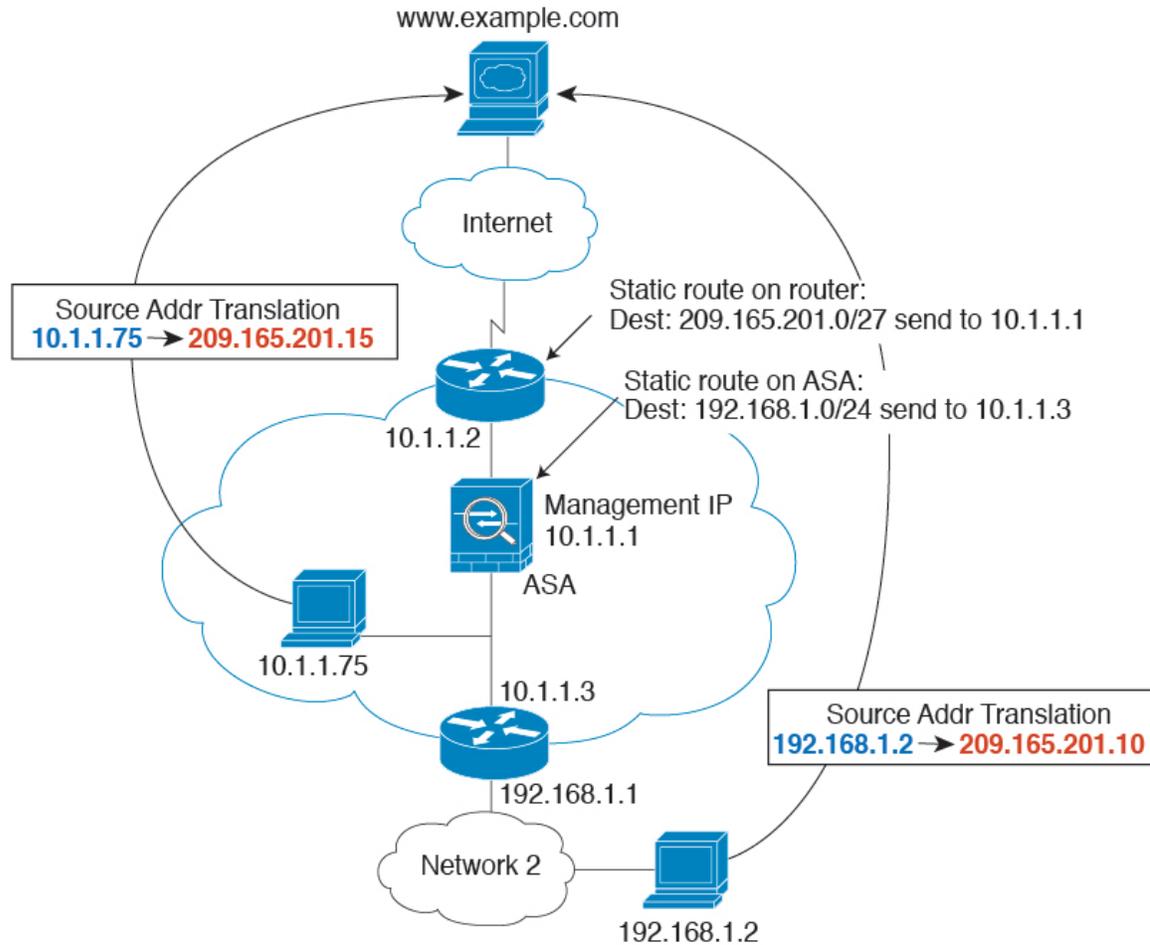
- トラフィックの発信元が ASA : syslog サーバなどがあるリモート ネットワーク宛でのトラフィック用に、ASA にデフォルト/スタティック ルートを追加します。
- インспекションが有効になっている Voice over IP (VoIP) および TFTP トラフィック、エンドポイントが1ホップ以上離れている：セカンダリ接続が成功するように、リモートエンドポイント宛でのトラフィック用に、ASA にスタティックルートを追加します。ASA は、セカンダリ接続を許可するためにアクセス コントロール ポリシーに一時的な「ピンホール」を作成します。セカンダリ接続ではプライマリ接続とは異なる IP アドレスのセットが使用される可能性があるため、ASA は正しいインターフェイスにピンホールをインストールするために、ルート ルックアップを実行する必要があります。

影響を受けるアプリケーションは次のとおりです。

- CTIQBE
 - GTP
 - H.323
 - MGCP
 - RTSP
 - SIP
 - Skinny (SCCP)
 - SQL*Net
 - SunRPC
 - TFTP
- ASA が NAT を実行する 1 ホップ以上離れたトラフィック：リモート ネットワーク宛でのトラフィック用に、ASA にスタティック ルートを設定します。また、ASA に送信されるマッピングアドレス宛でのトラフィック用に、上流に位置するルータにもスタティック ルートが必要です。

このルーティング要件は、インспекションと NAT が有効になっている VoIP と DNS の、1 ホップ以上離れている組み込み IP アドレスにも適用されます。ASA は、変換を実行できるように正しい出力インターフェイスを識別する必要があります。

図 4: NAT の例 : ブリッジグループ内の NAT



トランスパレントモードのブリッジグループのサポートされていない機能

次の表に、トランスパレントモードのブリッジグループでサポートされない機能を示します。

表 1: トランスパレントモードでサポートされない機能

機能	説明
ダイナミック DNS	-
DHCPv6 ステートレス サーバ	ブリッジグループメンバーインターフェイスでは、DHCPv4 サーバのみがサポートされます。

ルーテッド モードのブリッジ グループのサポートされていない機能

機能	説明
DHCP リレー	トランスペアレント ファイアウォールは DHCPv4 サーバとして機能することができませんが、DHCP リレー コマンドはサポートしません。2つのアクセスルールを使用して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、ブリッジグループ メンバー インターフェイスの場合、ASA で発信されたトラフィックにスタティック ルートを追加できます。アクセスルールを使用して、ダイナミック ルーティング プロトコルが ASA を通過できるようにすることもできます。
マルチキャスト IP ルーティング	アクセス ルール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ASAを通過できるようにすることができます。
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、ブリッジグループ メンバー インターフェイスでのみ、管理接続用のサイト間VPNトンネルをサポートします。これは、ASA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。アクセスルールを使用してVPNトラフィックにASA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。クライアントレスSSLVPNもサポートされていません。
ユニファイド コミュニケーション	—

ルーテッド モードのブリッジ グループのサポートされていない機能

次の表に、ルーテッド モードのブリッジ グループでサポートされていない機能を示します。

表 2: ルーテッドモードでサポートされていない機能

機能	説明
EtherChannel または VNI メンバー インターフェイス	物理インターフェイス、冗長インターフェイス、およびサブインターフェイスのみがブリッジグループメンバーインターフェイスとしてサポートされます。 管理 インターフェイスもサポートされていません。
クラスタ	クラスタリングではブリッジグループはサポートされません。
ダイナミック DNS	-
DHCPv6 ステートレス サーバ	BVI では DHCPv4 サーバのみがサポートされます。
DHCP リレー	ルーテッドファイアウォールは DHCPv4 サーバとして機能しますが、BVI またはブリッジグループメンバーインターフェイス上での DHCP リレーはサポートしません。
ダイナミック ルーティング プロトコル	ただし、BVI のスタティック ルートを追加することはできます。アクセス ルールを使用して、ダイナミック ルーティング プロトコルが ASA を通過できるようにすることもできます。非ブリッジグループインターフェイスはダイナミック ルーティングをサポートします。
マルチキャスト IP ルーティング	アクセス ルール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 ASA を通過できるようにすることができます。非ブリッジグループインターフェイスはマルチキャスト ルーティングをサポートします。
マルチ コンテキスト モード	ブリッジグループは、マルチ コンテキスト モードではサポートされていません。
QoS	非ブリッジグループインターフェイスは QoS をサポートします。

機能	説明
通過トラフィック用のVPNターミネーション	<p>BVI で VPN 接続を終端することはできません。非ブリッジグループインターフェイスは VPN をサポートします。</p> <p>ブリッジグループメンバーインターフェイスは、管理接続についてのみ、サイト間 VPN トンネルをサポートします。これは、ASA 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。アクセスルールを使用して VPN トラフィックにブリッジグループ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。クライアントレス SSL VPN もサポートされていません。</p>
ユニファイド コミュニケーション	非ブリッジグループインターフェイスはユニファイド コミュニケーションをサポートします。

デフォルト設定

デフォルト モード

デフォルト モードはルーテッド モードです。

ブリッジグループのデフォルト

デフォルトでは、すべての ARP パケットはブリッジグループ内で渡されます。

ファイアウォール モードのガイドライン

コンテキストモードのガイドライン

コンテキストごとにファイアウォール モードを設定します。

モデルのガイドライン

-
- ASAv50 では、ブリッジグループはサポートされていません。
- Firepower 2100 シリーズでは、ルーテッドモードのブリッジグループはサポートされません。

ブリッジグループのガイドライン（トランスペアレントおよびルーテッドモード）

- 64 のインターフェイスをもつブリッジグループを 250 まで作成できます。
- 直接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。
- ASA では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。
- IPv4 の場合は、管理トラフィックと、ASA を通過するトラフィックの両方の各ブリッジグループに対し、BVI の IP アドレスが必要です。IPv6 アドレスは BVI でサポートされませんが必須ではありません。
- IPv6 アドレスは手動でのみ設定できます。
- BVI IP アドレスは、接続された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。
- 管理インターフェイスはブリッジグループのメンバーとしてサポートされません。
- トランスペアレントモードでは、少なくとも 1 つのブリッジグループを使用し、データインターフェイスがブリッジグループに属している必要があります。
- トランスペアレントモードでは、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 BVI IP アドレスを指定しないでください。デバイスは ASA の他方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。
- トランスペアレントモードでは、管理トラフィックの戻りパスを指定するために必要な *default* ルートは、1 つのブリッジグループネットワークからの管理トラフィックにだけ適用されます。これは、デフォルトルートはブリッジグループのインターフェイスとブリッジグループネットワークのルータ IP アドレスを指定しますが、ユーザは 1 つのデフォルトルートしか定義できないためです。複数のブリッジグループネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティックルートを指定する必要があります。
- トランスペアレントモードでは、PPPoE は管理インターフェイスでサポートされません。
- ルーテッドモードでは、ブリッジグループと他のルーテッドインターフェイスの間をルーティングするために、BVI を指定する必要があります。
- ルーテッドモードでは、ASA 定義の EtherChannel および VNI インターフェイスがブリッジグループのメンバーとしてサポートされません。Firepower 4100/9300 上の Etherchannel は、ブリッジグループメンバーにすることができます。
- Bidirectional Forwarding Detection (BFD) エコーパケットは、ブリッジグループメンバーを使用するときに、ASA を介して許可されません。BFD を実行している ASA の両側に 2 つのネイバーがある場合、ASA は BFD エコーパケットをドロップします。両方が同じ送信元および宛先 IP アドレスを持ち、LAND 攻撃の一部であるように見えるからです。

その他のガイドラインと制限事項

- ファイアウォールモードを変更すると、多くのコマンドが両方のモードでサポートされていないため、ASA は実行コンフィギュレーションをクリアします。スタートアップ コンフィギュレーションは変更されません。保存しないでリロードすると、スタートアップ コンフィギュレーションがロードされて、モードは元の設定に戻ります。コンフィギュレーション ファイルのバックアップについては、[ファイアウォールモードの設定 \(14 ページ\)](#) を参照してください。
- **firewall transparent** コマンドでモードを使用して変更するテキスト コンフィギュレーションを ASA にダウンロードする場合、コマンドをコンフィギュレーションの先頭に配置してください。このコマンドが読み込まれるとすぐに ASA がモードを変更し、その後ダウンロードされたコンフィギュレーションを引き続き読み込みます。コマンドがコンフィギュレーションの後ろの方にあると、ASA はそのコマンドよりも前の位置に記述されているすべての行をクリアします。テキストファイルのダウンロードの詳細については、[ASA イメージ、ASDM、およびスタートアップコンフィギュレーションの設定](#)を参照してください。

ファイアウォール モードの設定

この項では、ファイアウォールモードを変更する方法を説明します。



- (注) ファイアウォールモードを変更すると実行コンフィギュレーションがクリアされるので、他のコンフィギュレーションを行う前にファイアウォールモードを設定することをお勧めします。

始める前に

モードを変更すると、ASA は実行コンフィギュレーションをクリアします (詳細については、[ファイアウォールモードのガイドライン \(12 ページ\)](#) を参照してください)。

- 設定済みのコンフィギュレーションがある場合は、モードを変更する前にコンフィギュレーションをバックアップしてください。新しいコンフィギュレーション作成時の参照としてこのバックアップを使用できます。[コンフィギュレーションまたはその他のファイルのバックアップおよび復元](#)を参照してください。
- モードを変更するには、コンソールポートで CLI を使用します。ASDM コマンドライン インターフェイス ツールや SSH などの他のタイプのセッションを使用する場合、コンフィギュレーションがクリアされるときにそれが切断されるので、いずれの場合もコンソールポートを使用して ASA に再接続する必要があります。
- コンテキスト内でモードを設定します。



- (注) 設定が削除された後にファイアウォールモードをトランスペアレントに設定し、ASDM への管理アクセスを設定するには、[ASDM アクセスの設定](#)を参照してください。

手順

ファイアウォールモードをトランスペアレントに設定します。

firewall transparent

例：

```
ciscoasa(config)# firewall transparent
```

モードをルーテッドに変更するには、**no firewall transparent** コマンドを入力します。

- (注) ファイアウォールモードの変更では確認は求められず、ただちに変更が行われます。

ファイアウォールモードの例

このセクションには、ルーテッドファイアウォールモードとトランスペアレントファイアウォールモードで、ASA を介してどのようにトラフィックが転送されるかを説明する例が含まれます。

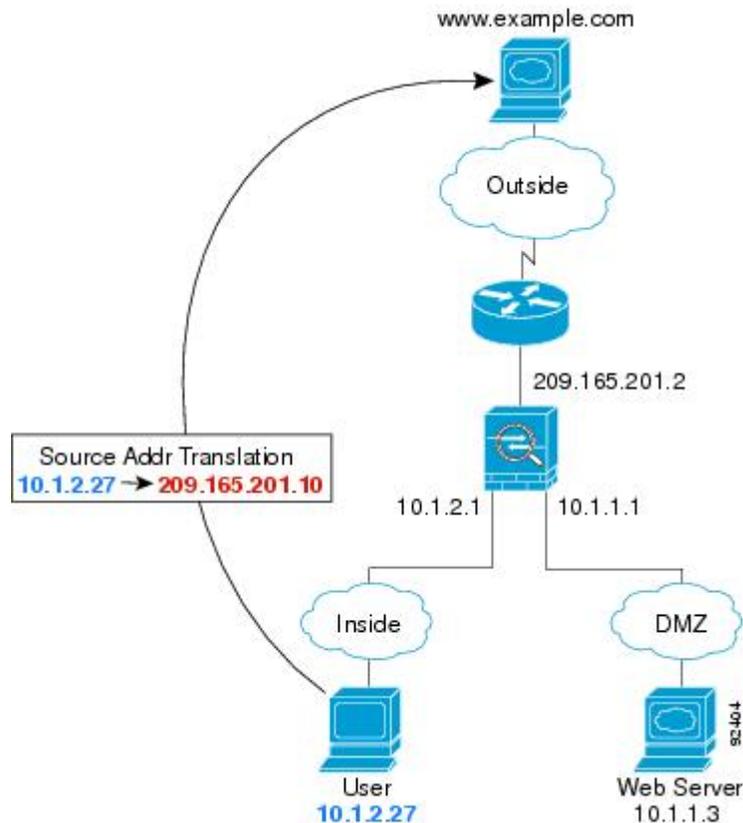
ルーテッドファイアウォールモードで **ASA** を通過するデータ

次のセクションでは、複数のシナリオのルーテッドファイアウォールモードで、データが ASA をどのように通過するかを示します。

内部ユーザが **Web** サーバにアクセスする

次の図は、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 5: 内部から外部へ



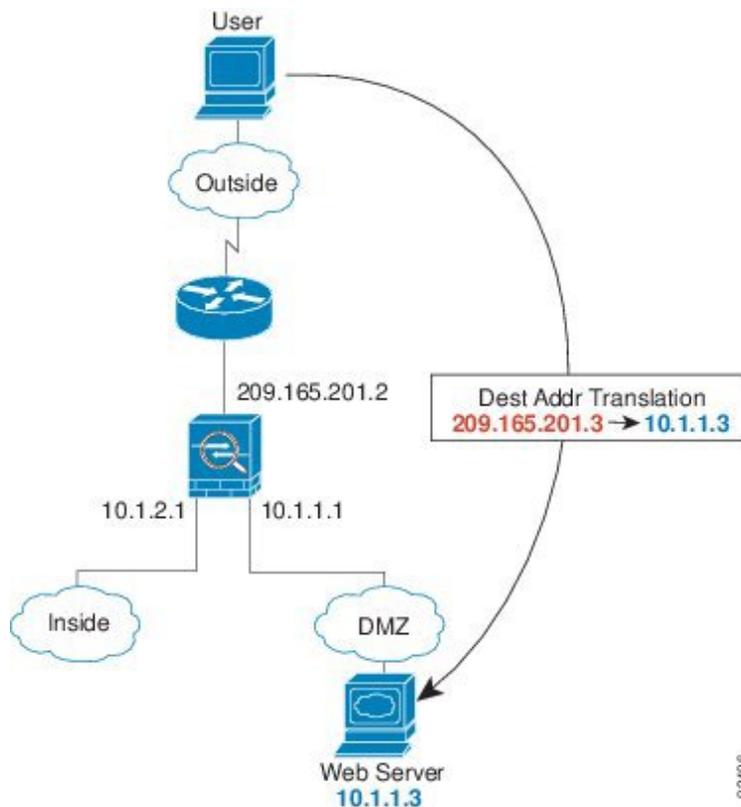
次の手順では、データが ASA をどのように通過するかを示します。

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. ASA 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、ASA はセキュリティポリシーの条件に従って、パケットが許可されているか確認します。
マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. ASA は、実アドレス (10.1.2.27) をマップアドレス 209.165.201.10 に変換します。このマップアドレスは外部インターフェイスのサブネット上にあります。
マップアドレスは任意のサブネット上に設定できますが、外部インターフェイスのサブネット上に設定すると、ルーティングが簡素化されます。
4. 次に、ASA 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 ASA 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。ASA 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 に変換せずに、NAT を実行します。
6. ASA 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

次の図は、外部ユーザが DMZ の Web サーバにアクセスしていることを示しています。

図 6: 外部から DMZ へ



次の手順では、データが ASA をどのように通過するかを示します。

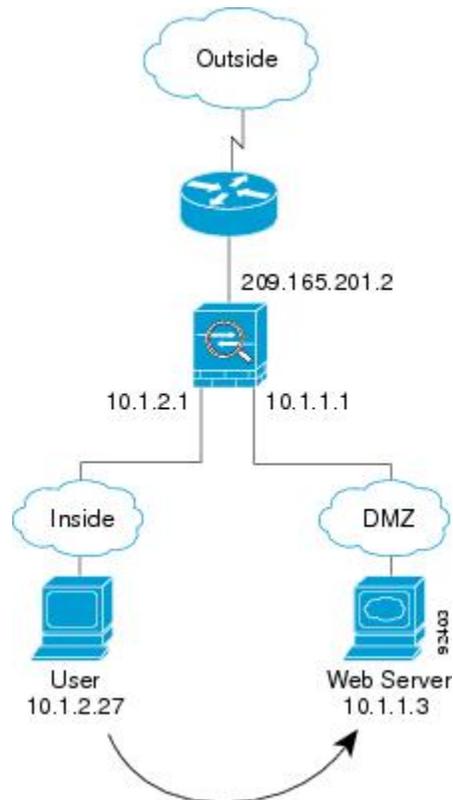
1. 外部ネットワーク上のユーザがマップアドレス 209.165.201.3 を使用して、DMZ 上の Web サーバに Web ページを要求します。これは、外部インターフェイスのサブネット上のアドレスです。
2. ASA はパケットを受信し、マッピングアドレスは実アドレス 10.1.1.3 に変換しません。
3. ASA は新しいセッションであるため、セキュリティポリシーの条件に従って、パケットが許可されていることを確認します。
マルチコンテキストモードの場合、ASA はパケットをまずコンテキストに分類します。
4. 次に、ASA はセッションエントリを高速パスに追加し、DMZ インターフェ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 ASA 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。ASA は、実アドレスを 209.165.201.3 に変換することで NAT を実行します。

6. ASA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

次の図は、内部ユーザが DMZ の Web サーバにアクセスしていることを示しています。

図 7: 内部から DMZ へ



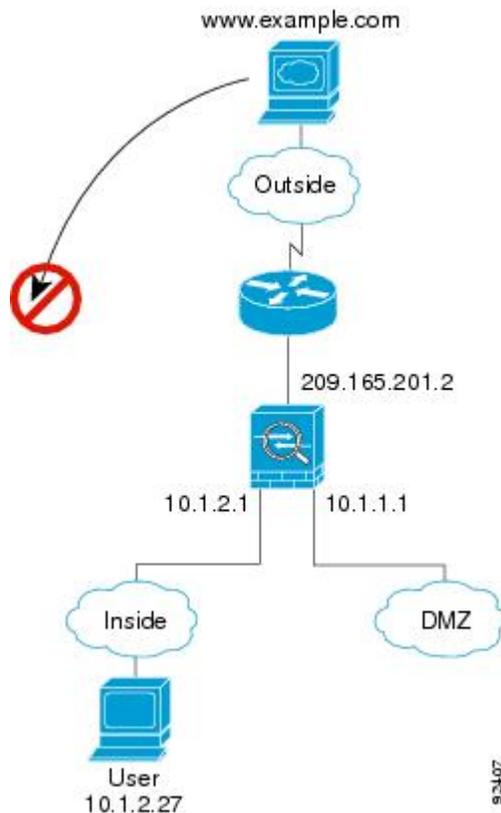
次の手順では、データが ASA をどのように通過するかを示します。

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. ASA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、ASAはセキュリティポリシーの条件に従ってパケットが許可されているか確認します。
マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. 次に、ASA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. ASA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

次の図は、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 8: 外部から内部へ



次の手順では、データが ASA をどのように通過するかを示します。

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のが考えられます。

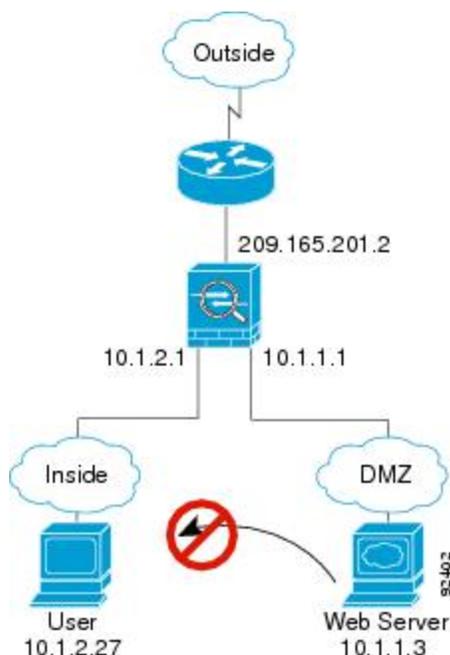
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティポリシーに従って、パケットが許可されているか確認します。
3. パケットが拒否され、ASA はパケットをドロップし、接続試行をログに記録します。

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、ASA 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 ユーザによる内部ホストへのアクセスの試み

次の図は、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 9: DMZ から内部へ



次の手順では、データが ASA をどのように通過するかを示します。

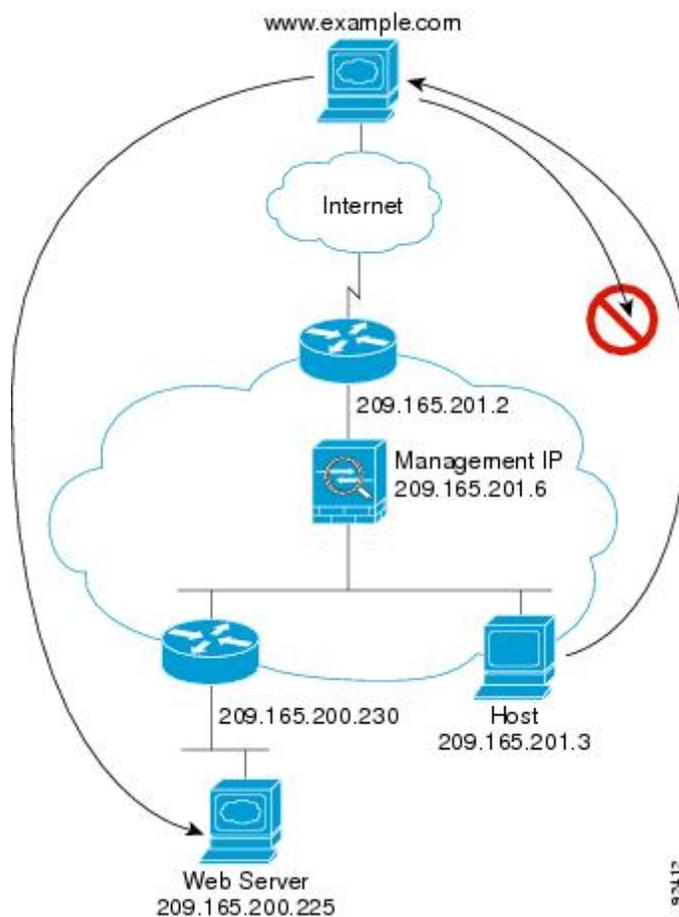
1. DMZ ネットワーク上のユーザが、内部ホストに到達しようとします。DMZ はインターネット上のトラフィックをルーティングする必要がないので、プライベートアドレッシング方式はルーティングを回避しません。
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティポリシーに従って、パケットが許可されているか確認します。

パケットが拒否され、ASA 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 ファイアウォールを通過するデータの動き

次の図に、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に、ASA にはアクセスルールがあります。別のアクセスルールによって、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 10:一般的なトランスパレントファイアウォールのデータパス

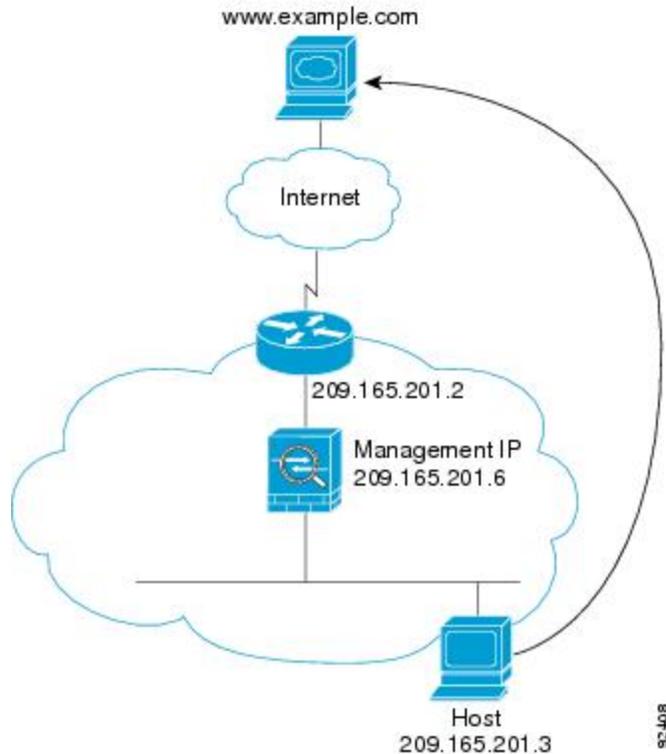


次のセクションでは、データが ASA をどのように通過するかを示します。

内部ユーザが Web サーバにアクセスする

次の図は、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 11: 内部から外部へ



次の手順では、データが ASA をどのように通過するかを示します。

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. ASA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、ASA はパケットをまずコンテキストに分類します。

3. ASA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、ASA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 209.165.201.2 です。

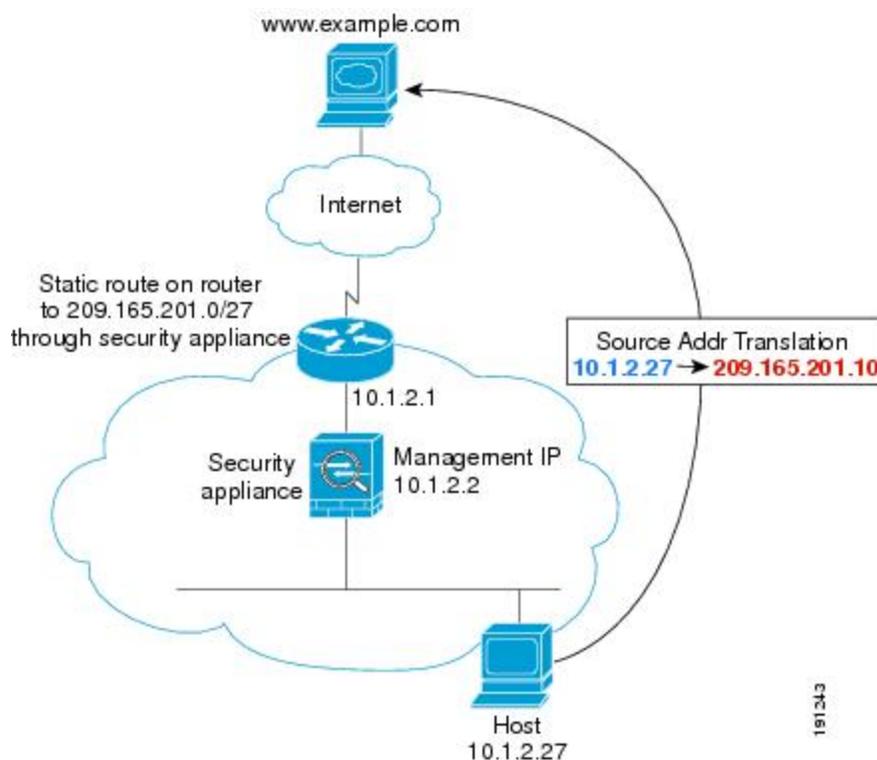
宛先 MAC アドレスが ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求または ping を送信します。最初のパケットはドロップされます。

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ロックアップをバイパスします。
6. ASAは、パケットを内部ユーザに転送します。

NATを使用して内部ユーザがWebサーバにアクセスする

次の図は、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 12: NATを使用して内部から外部へ



次の手順では、データが ASA をどのように通過するかを示します。

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. ASA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、ASA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. ASAは実際のアドレス (10.1.2.27) をマッピング アドレス 209.165.201.10 に変換します。
マッピングアドレスは外部インターフェイスと同じネットワーク上にないため、アップストリーム ルータにASAをポイントするマッピング ネットワークへのスタティック ルートがあることを確認します。
4. 次に、ASA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. 宛先 MAC アドレスがテーブル内にある場合、ASA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 10.1.2.1 です。

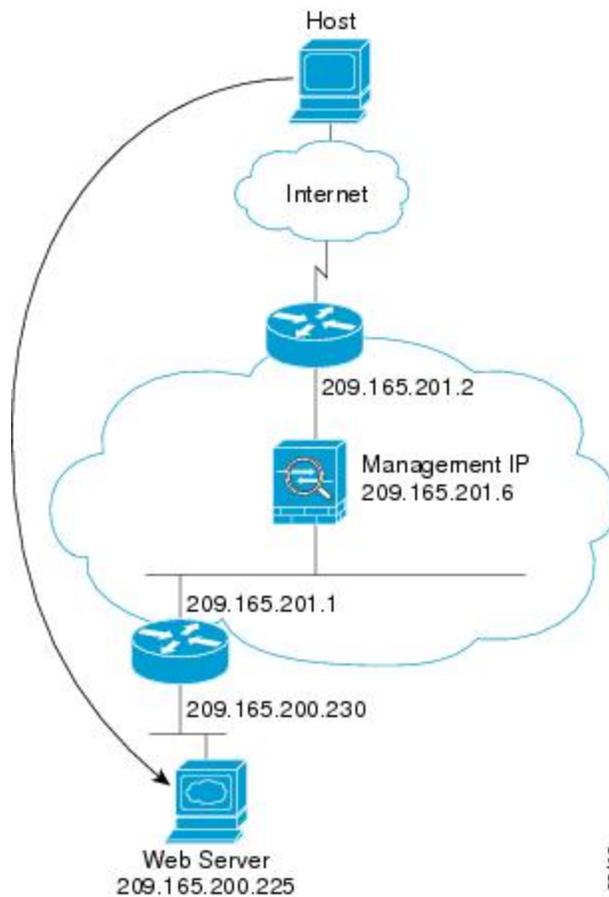
宛先 MAC アドレスが ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求と ping を送信します。最初のパケットはドロップされます。

6. 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。
7. ASA は、マッピングアドレスを実際アドレス 10.1.2.27 にせずに、NAT を実行します。

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

次の図は、外部ユーザが内部の Web サーバにアクセスしていることを示しています。

図 13: 外部から内部へ



次の手順では、データが ASA をどのように通過するかを示します。

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. ASA 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、ASA はパケットをまずコンテキストに分類します。

3. ASA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、ASA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。

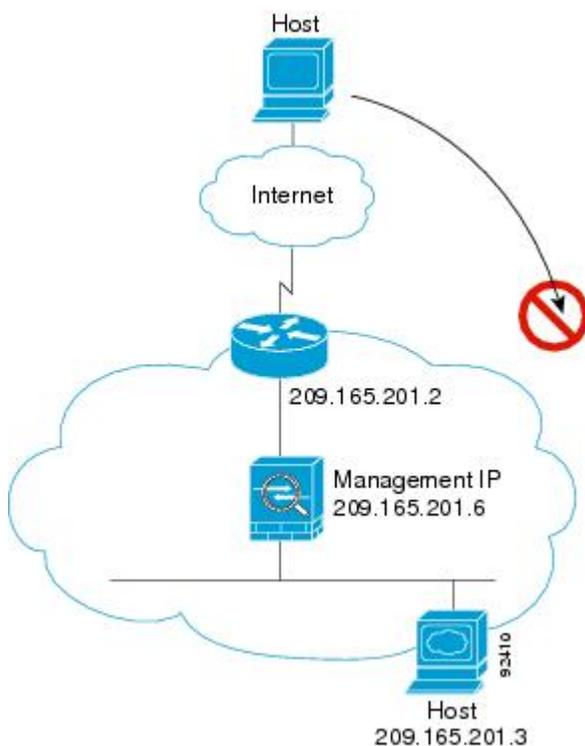
宛先 MAC アドレスが ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求と ping を送信します。最初のパケットはドロップされます。

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. ASA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

次の図は、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 14: 外部から内部へ



次の手順では、データが ASA をどのように通過するかを示します。

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ています。
2. ASA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の条件に従って、パケットが許可されているか確認します。

マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。

3. 外部ホストを許可するアクセス ルールは存在しないため、パケットは拒否され、ASA によってドロップされます。
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、ASA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。

ファイアウォールモードの履歴

表 3: ファイアウォールモードの各機能履歴

機能名	プラットフォーム リリース	機能情報
トランスペアレントファイアウォールモード	7.0(1)	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しては認識されません。 firewall transparent 、および show firewall コマンドが導入されました。

機能名	プラットフォーム リリース	機能情報
トランスパレントファイアウォールブリッジグループ	8.4(1)	<p>セキュリティコンテキストのオーバーヘッドを避けたい場合、またはセキュリティコンテキストを最大限に使用したい場合、インターフェイスをブリッジグループにグループ化し、各ネットワークに1つずつ複数のブリッジグループを設定できます。ブリッジグループのトラフィックは他のブリッジグループから隔離されます。シングルモードでは最大8個、マルチモードではコンテキストあたり最大8個のブリッジグループを設定でき、各ブリッジグループには最大4個のインターフェイスを追加できます。</p> <p>(注) ASA 5505 に複数のブリッジグループを設定できますが、ASA 5505 のトランスパレントモードのデータインターフェイスは2つという制限は、実質的にブリッジグループを1つだけ使用できることを意味します。</p> <p>interface bvi、bridge-group、show bridge-group の各コマンドが導入されました。</p>
マルチコンテキストモードのファイアウォールモードの混合がサポートされます。	8.5(1)/9.0(1)	<p>セキュリティコンテキストごとに個別のファイアウォールモードを設定できます。したがってその一部をトランスパレントモードで実行し、その他をルーテッドモードで実行することができます。</p> <p>firewall transparent コマンドが変更されました。</p>

機能名	プラットフォーム リリース	機能情報
トランスペアレントモードのブリッジグループの最大数が 250 に増加	9.3(1)	ブリッジグループの最大数が8個から250個に増えました。シングルモードでは最大250個、マルチモードではコンテキストあたり最大8個のブリッジグループを設定でき、各ブリッジグループには最大4個のインターフェイスを追加できます。 interface bvi コマンド、 bridge-group コマンドが変更されました。
トランスペアレントモードで、ブリッジグループごとのインターフェイス数が最大で 64 に増加	9.6(2)	ブリッジグループあたりのインターフェイスの最大数が4から64に拡張されました。 変更されたコマンドはありません。

機能名	プラットフォーム リリース	機能情報
Integrated Routing and Bridging (IRB)	9.7(1)	

機能名	プラットフォーム リリース	機能情報
		<p>Integrated Routing and Bridging (統合ルーティングおよびブリッジング) は、ブリッジグループとルーテッドインターフェイス間をルーティングする機能を提供します。ブリッジグループとは、ASAがルートの代わりにブリッジするインターフェイスのグループのことです。ASAは、ASAがファイアウォールとして機能し続ける点で本来のブリッジとは異なります。つまり、インターフェイス間のアクセス制御が実行され、通常のファイアウォール検査もすべて実行されます。以前は、トランスペアレント ファイアウォールモードでのみブリッジグループの設定が可能だったため、ブリッジグループ間でのルーティングはできませんでした。この機能を使用すると、ルーテッドファイアウォールモードのブリッジグループの設定と、ブリッジグループ間およびブリッジグループとルーテッドインターフェイス間のルーティングを実行できます。ブリッジグループは、ブリッジ仮想インターフェイス (BVI) を使用してそのブリッジグループのゲートウェイとして機能することにより、ルーティングに参加します。そのブリッジグループに指定するASA上に別のインターフェイスが存在する場合、Integrated Routing and Bridging (IRB) は外部レイヤ2スイッチの使用に代わる手段を提供します。ルーテッドモードでは、BVIは名前付きインターフェイスとなり、アクセスルールやDHCPサーバなどの一部の機能に、メンバーインターフェイスとは個別に参加できます。</p> <p>トランスペアレントモードでサポートされるマルチ コンテキスト モードやASA クラスタリングの各機能は、ルーテッドモードではサポートされません。マルチキャストルーティングとダイナミック ルーティングの機能も、</p>

機能名	プラットフォーム リリース	機能情報
		BVI ではサポートされません。 次のコマンドが変更されました。 access-group 、 access-list ethertype 、 arp-inspection 、 dhcpd 、 mac-address-table static 、 mac-address-table aging-time 、 mac-learn 、 route 、 show arp-inspection 、 show bridge-group 、 show mac-address-table 、 show mac-learn

