



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、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 \(13 ページ\)](#)
- [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、または Visual Networking Index (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してください。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。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」のように機能するレイヤ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。

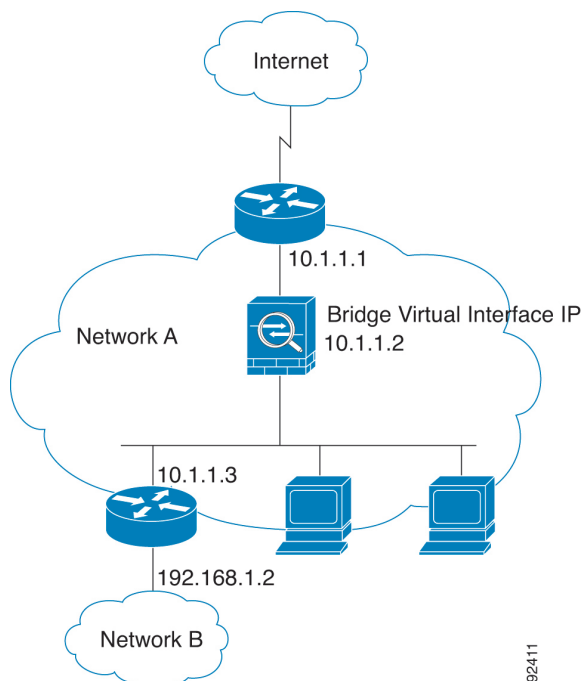
レイヤ2の接続は、ネットワーク上の内部と外部のインターフェイスをまとめた「ブリッジグループ」を使用して確立されます。また、ASA はブリッジング技術を使用してインターフェイス間のトラフィックを通します。各ブリッジグループには、ネットワーク上で IP アドレスが割り当てられるブリッジ仮想インターフェイス (BVI) が含まれます。複数のネットワークに複数のブリッジグループを設定できます。トランスペアレントモードでは、これらのブリッジグループは相互通信できません。

ネットワークでの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。内部ルータと各ホストは、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



Management 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Management 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チェックがすべて実施されます。

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 サーバーと ASA 由来の他のトラフィック：syslog サーバー（または SNMP サーバー、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、または EtherChannel 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

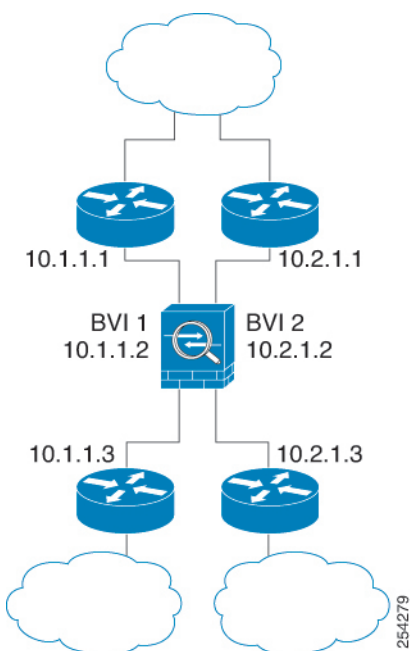
ブリッジグループのトラフィックは他のブリッジグループから隔離され、トラフィックは ASA 内の他のブリッジグループにはルーティングされません。また、トラフィックは外部ルータから ASA 内の他のブリッジグループにルーティングされる前に、ASA から出る必要があります。ブリッジング機能はブリッジグループごとに分かれています。その他の多くの機能はすべてのブリッジグループ間で共有されます。たとえば、syslog サーバーまたは AAA サーバーの設定は、すべてのブリッジグループで共有されます。セキュリティ ポリシーを完全に分離

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 \(13ページ\)](#) 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



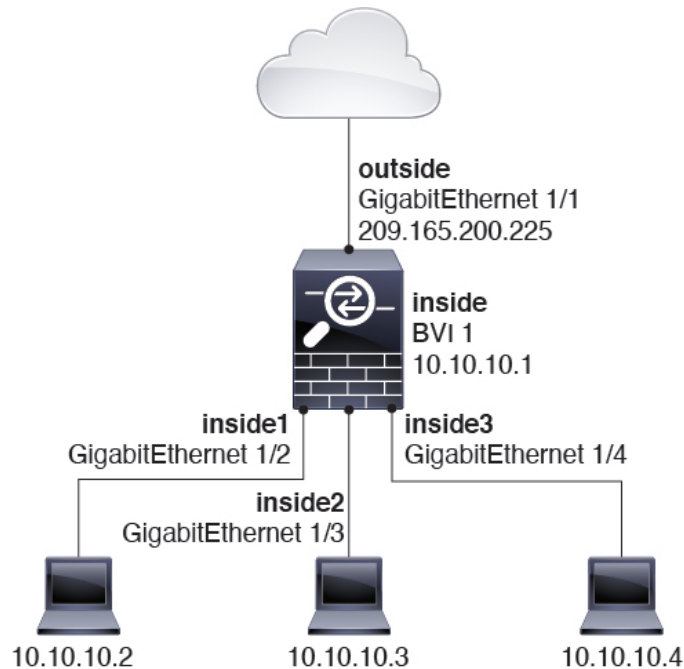
ルーテッドファイアウォールモードのブリッジグループ

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ことで、ブリッジグループのトラフィックを分離することもできます。BVIに名前を付けると、そのBVIはその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、デバイスの中には、通常のインターフェイスとして外部インターフェイスを持ち、その他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るというデフォルト設定のものがあります。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ので、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、デフォルト設定と同様に、すべてのインターフェイスを同じセキュリティレベルに設定し、同じセキュリティレベルのインターフェイス間の通信を有効にします。この通信では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 処理

スパニングツリープロトコルを使用するときのループを防止するために、デフォルトで BPDU が渡されます。BPDU をブロックするには、BPDU を拒否するように EtherType ルールを設定する必要があります。外部スイッチで BPDU をブロックすることもできます。たとえば、同じブリッジグループのメンバーが異なる VLAN のスイッチポートに接続されている場合、スイッチで BPDU をブロックできます。この場合、一方の VLAN からの BPDU がもう一方の VLAN で認識されるため、スパニングツリールートブリッジの選定プロセスで問題が発生する可能性があります。

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 サーバー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。
- トランスペアレント ファイアウォール モードで有効になっている SSL ポリシー—
 - TLS 1.3 トラフィックが ASA デバイスを通過します。
 - ASA TCP プロキシとして機能します。これにより、クライアント側の TCP 接続が終了し、別のサーバー側の接続が開始されます。ASA TCP スタックはセッション状態を保持します。
 - アイドル状態のプロキシセッションの場合、ASA は TCP ACK キープアライブプローブを生成して接続状態を保存します。これらはパススルーパケットではありません。ファイアウォールがこれらのパケットを発信し、TLS トランジット接続の状態に応じてクライアントまたはサーバーに送信します。
 - ASA はこれらのキープアライブを開始するため、トランスペアレントモードであっても隣接関係テーブルルックアップ（ネクストホップまたは出力 MAC 解決）を実行する必要があります。
 - これらのプロキシで生成されたパケットのいずれかで隣接関係ルックアップが失敗した場合、ASA では syslog 110003 がログに記録されます。

これらの syslog メッセージを防止するには、トランジット接続エンドポイント（クライアントおよびサーバーの IP アドレス）の ASA でルートを設定します。適切にルーティングすると、キープアライブパケットの隣接関係検索が成功します。

ASA が TCP キープアライブを正常に送信し、応答を受信すると、トランジット接続はアクティブなままになります。デバイスがキープアライブを送信できない、または応答を受信しない場合、約 240 秒後にトランジット接続が削除されます。

- 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。

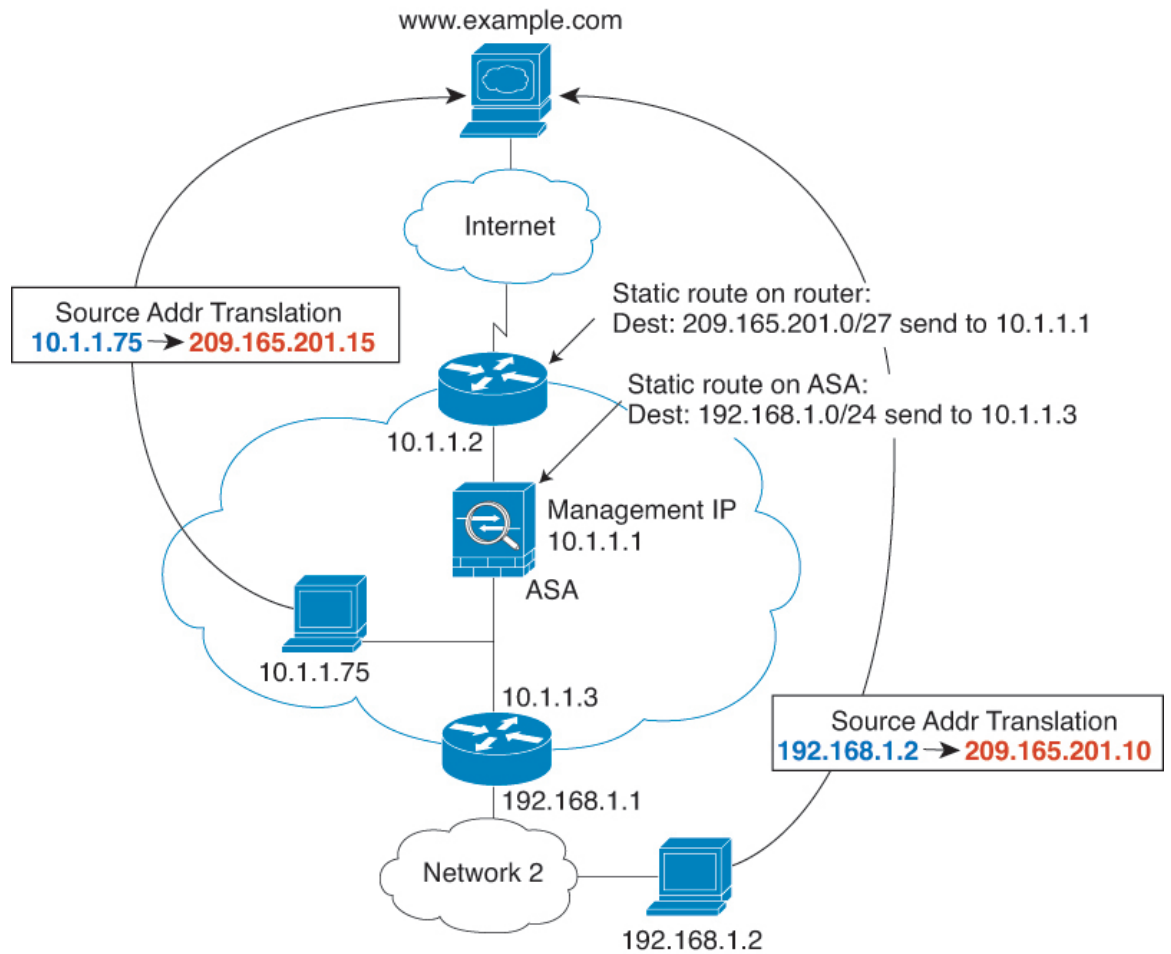
影響を受けるアプリケーションは次のとおりです。

- 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、インスペクションと 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



トランスペアレント 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、トランスペアレント 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: トランスペアレント 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。

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サーバーとして機能することができますが、DHCP リレーはサポートしません。2つのアクセスルール（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つはサーバーからの応答を逆方向に許可します。）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。
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終端	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。
Unified Communications	—

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。 Management インターフェイスもサポートされていません。
クラスタリング	ブリッジグループはクラスタリングで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	DHCPv4 サーバーのみが BVI でサポートされます。

機能	説明
DHCP リレー	ルーテッドファイアウォールはDHCPv4サーバーとして機能することができますが、DHCPリレーをBVIまたはブリッジグループメンバーインターフェイスでサポートしません。
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せん。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せん。
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せん。
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をサポートしません。
通過トラフィック用のVPN終端	VPN接続をBVIで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。 ブリッジグループメンバーインターフェイスは、管理接続専用のサイト間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SSLVPNもサポートされていません。
Unified Communications	非ブリッジグループインターフェイスは、Unified Communicationsをサポートしません。

デフォルト設定

デフォルトモード (Default Mode)

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。

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。
- デバイスとデバイス間の管理トラフィック、および ASA を通過するデータトラフィック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。IPv4 トラフィックの場合は、IPv4 アドレスを指定します。IPv6 トラフィックの場合は、IPv6 アドレスを指定します。
- 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。
- ブリッジされた ixgbev インターフェイスを備えた VMware の ASA v50 の場合、トランスペアレントモードはサポートされておらず、ブリッジグループはルーテッドモードで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。
- 200/1010/ では、同じブリッジグループ内に論理 VLAN インターフェイスと物理ファイアウォールインターフェイスを混在させることはできません。
- 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デフォルトルートは、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。

- トランスパレント モードでは、PPPoE は Management 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（13 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。このバックアップは、新しいコンフィギュレーション作成時の参照として使用できます。[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と復元](#)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パレントに設定し、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パ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パ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。

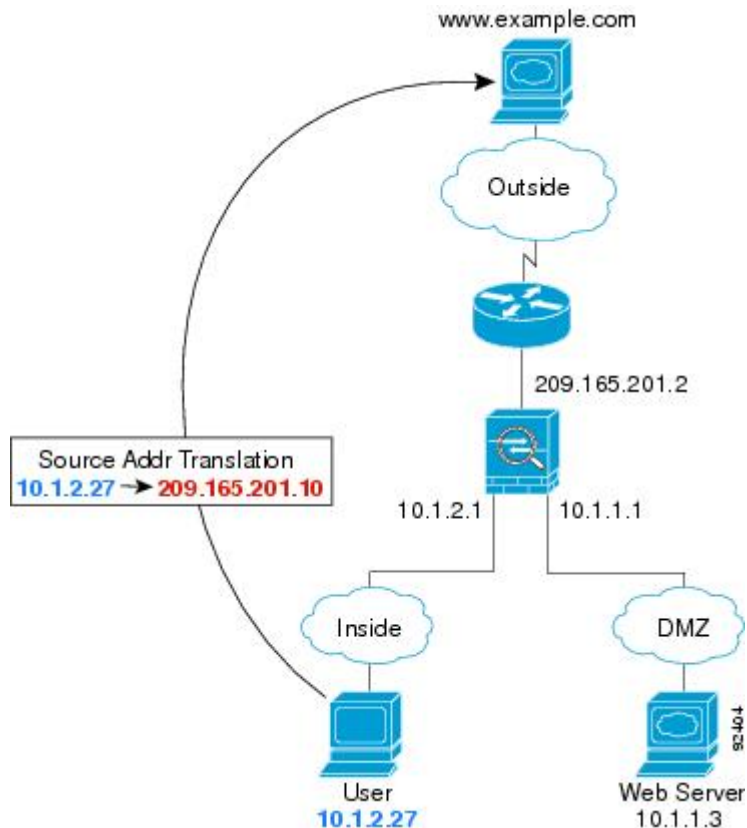
ルーテッド ファイアウォール モードで ASA を通過するデータ

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。

内部ユーザーが Web サーバーにアクセスする

次の図は、内部ユーザーが外部 Web サーバー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ーは、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。

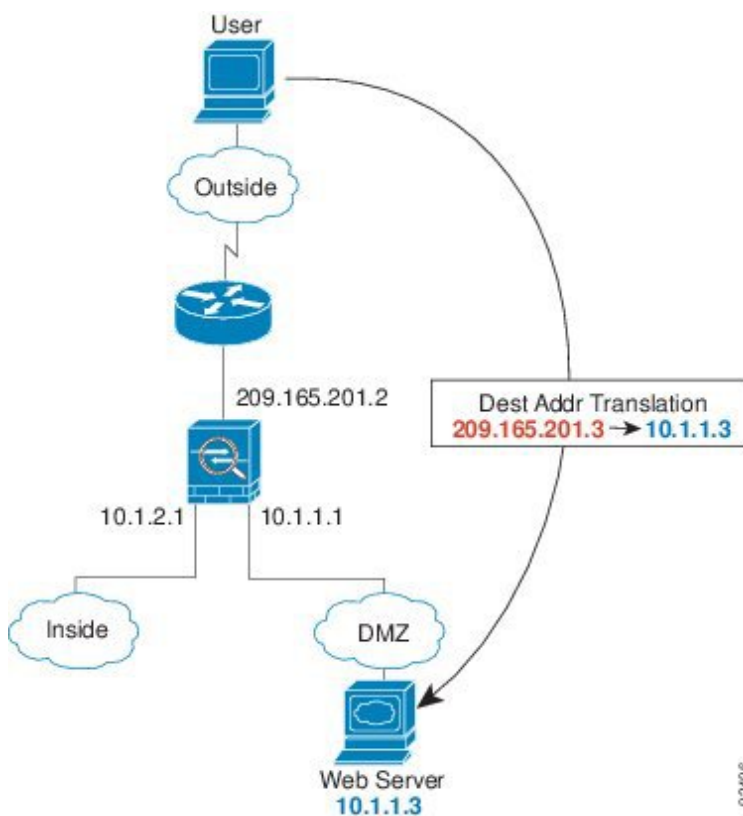
マップ アドレスは任意のサブネット上に設定できますが、外部インターフェイスのサブネット上に設定すると、ルーティングが簡素化されます。

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。

外部ユーザーが DMZ 上の Web サーバーにアクセスする

次の図は、外部ユーザーが DMZ の Web サーバー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。

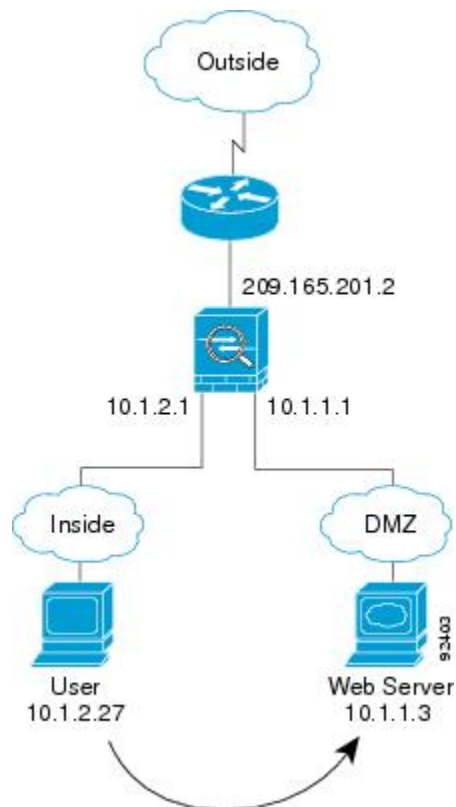
1. 外部ネットワーク上のユーザーがマップアドレス `209.165.201.3` を使用して、DMZ 上の Web サーバーに Web ページを要求します。これは、外部インターフェイスのサブネットワーク上のアドレスです。
2. ASA はパケットを受信し、マッピングアドレスは実アドレス `10.1.1.3` に変換しません。

- 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。
- 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。
- 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。
- ASA は、パケットを外部ユーザに転送します。

内部ユーザーが DMZ 上の Web サーバーにアクセスする

次の図は、内部ユーザーが DMZ の Web サーバー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。

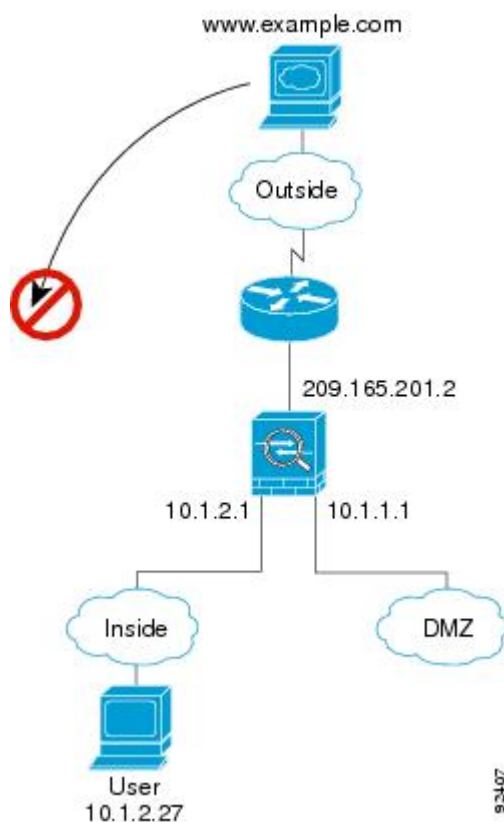
- 内部ネットワーク上のユーザーは、宛先アドレス 10.1.1.3 を使用して DMZ Web サーバーから Web ページを要求します。

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サーバー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。

外部ユーザーが内部ホストにアクセスしようとする

次の図は、外部ユーザー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ーが、内部ホストに到達しようとし（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）。

DMZ ユーザーによる内部ホストへのアクセスの試み

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、外部ユーザーが 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。外部ユーザーは既存の NAT セッションを使用して内部ユーザーに到達しようとするのが考えられます。

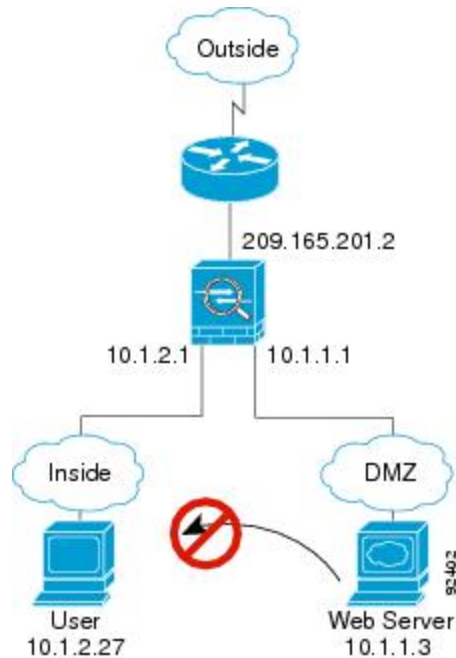
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティポリシーに従って、パケットが許可されているか確認します。
3. パケットが拒否され、ASA はパケットをドロップし、接続試行をログに記録します。

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 ユーザーによる内部ホストへのアクセスの試み

次の図は、DMZ 内のユーザー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。

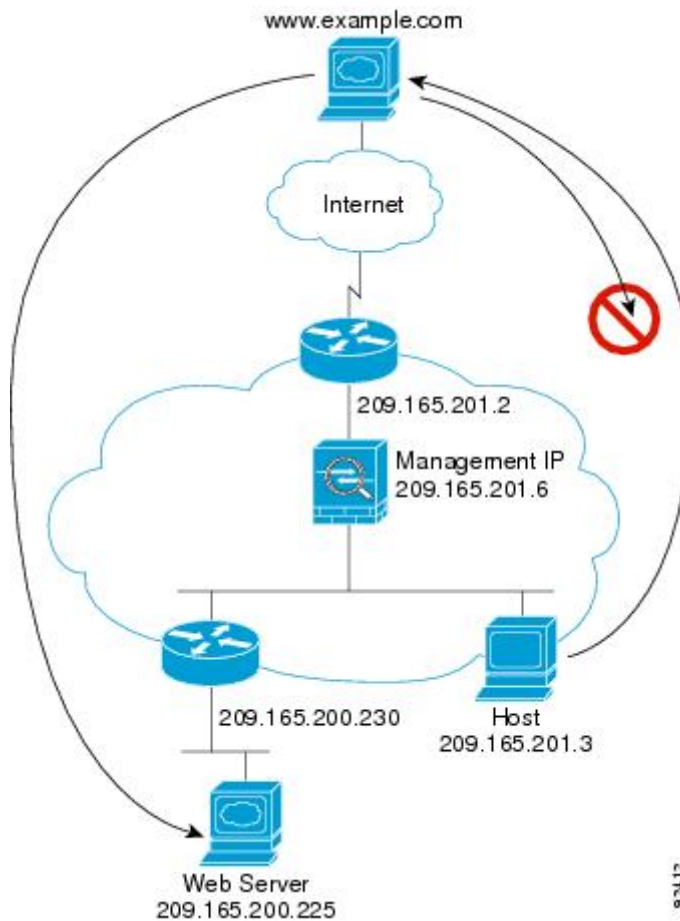
1. DMZ ネットワーク上のユーザーが、内部ホストに到達しようとします。DMZ はインターネット上のトラフィックをルーティングする必要がないので、プライベートアドレッシング方式はルーティングを回避しません。
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティポリシーに従って、パケットが許可されているか確認します。

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。

トランスパ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パレントファイアウォールの実装を示します。内部ユーザー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、外部ユーザー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

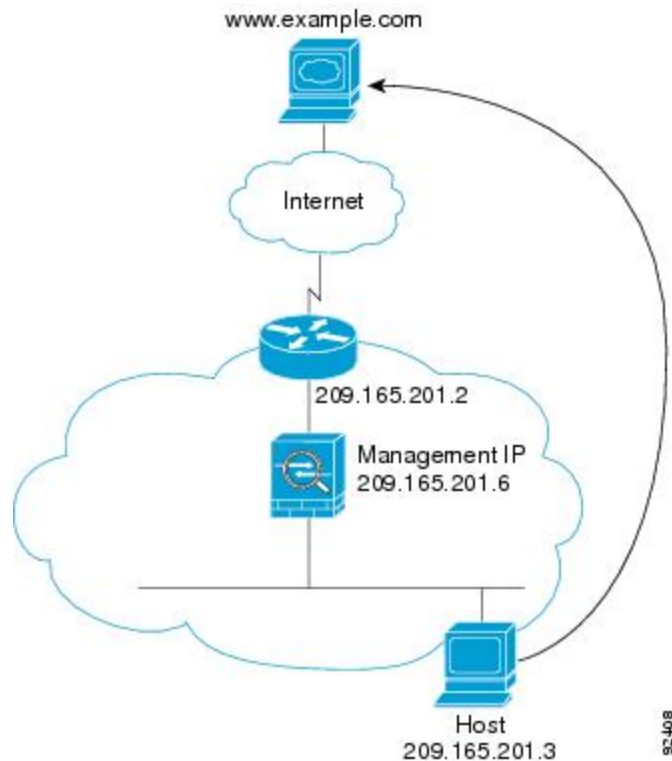


次のセクションでは、データが ASA をどのように通過するかを示します。

内部ユーザーが Web サーバにアクセスする

この図は、内部ユーザーが外部 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ーは、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。

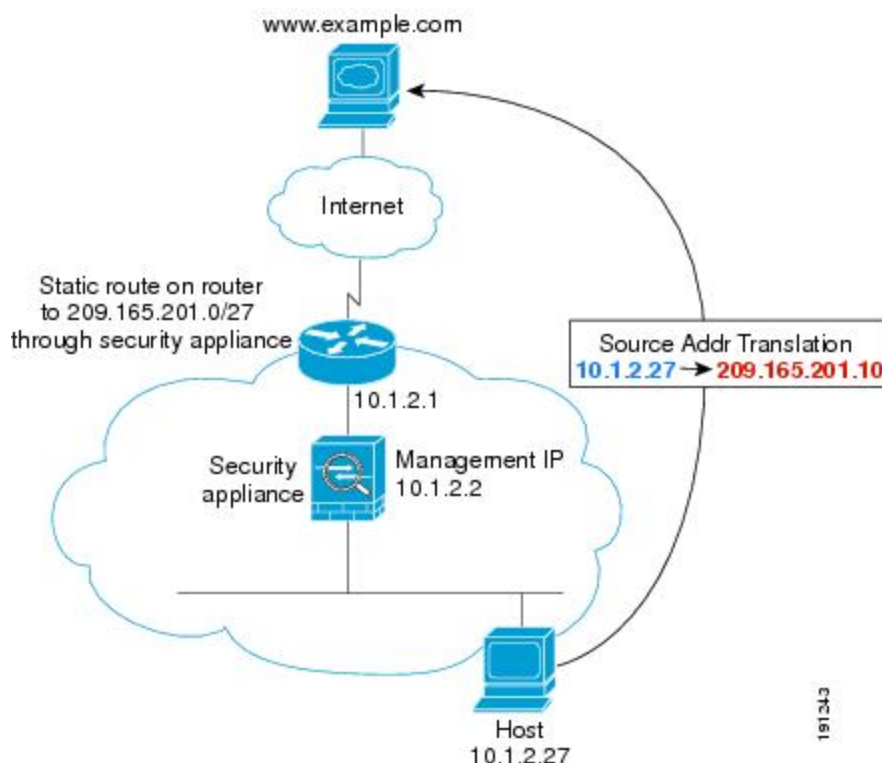
宛先 MAC アドレスが ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求または ping を送信します。最初のパケットはドロップされます。

5. Web サーバー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、パケットを内部ユーザに転送します。

NATを使用して内部ユーザーがWebサーバーにアクセスする

次の図は、内部ユーザーが外部 Web サーバー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ーは、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。

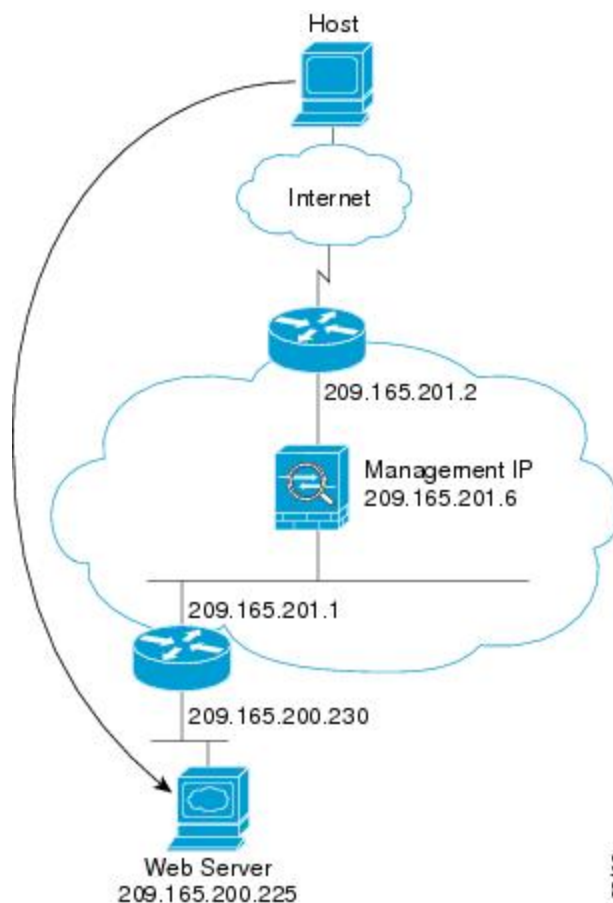
宛先 MAC アドレスが ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求と ping を送信します。最初のパケットはドロップされます。

6. Web サーバー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。

外部ユーザーが内部ネットワーク上の Web サーバーにアクセスする

次の図は、外部ユーザーが内部の Web サーバー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ーは、内部 Web サーバーから 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。

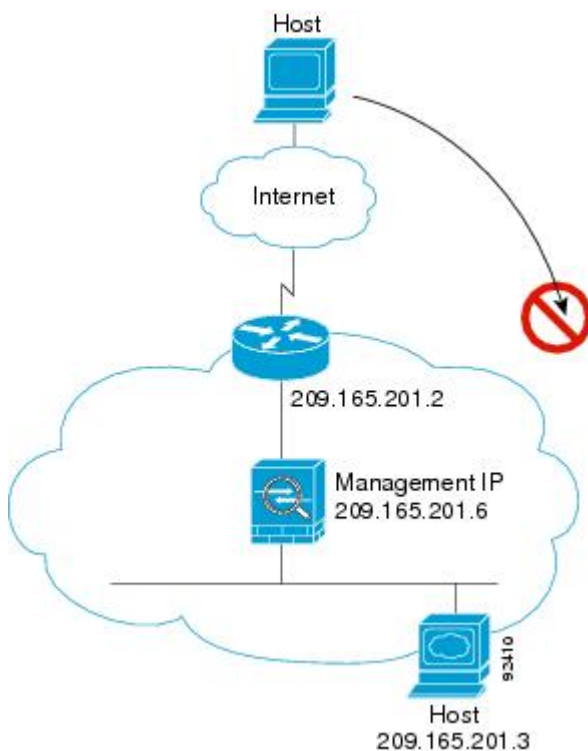
マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。

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 サーバー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。

外部ユーザーが内部ホストにアクセスしようとする

次の図は、外部ユーザー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ーが、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	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。
トランスペアレントファイアウォールブリッジグループ	8.4(1)	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。 (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 のトランスペア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。 interface bvi 、 bridge-group 、 show bridge-group の各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
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ペア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>
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)	<p>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。</p> <p>interface bvi コマンド、bridge-group コマンドが変更されました。</p>
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)	<p>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。</p> <p>変更されたコマンドはありません。</p>

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)	<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、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って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 サーバー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、BVI ではサポートされません。</p> <p>次のコマンドが変更されました。access-group、access-list ethertype、arp-inspection、dhcpcd、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</p>

機能名	プラットフォームリリース	機能情報
Firepower 4100/9300 ASA 論理デバイスのトランスパレントモード展開のサポート	9.10(1)	Firepower 4100/9300 で ASA を展開するときに、トランスパレントまたはルーテッドモードを指定できるようになりました。 新規/変更された FXOS コマンド : enter bootstrap-key FIREWALL_MODE 、 set value routed 、 set value transparent

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。