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 （11 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 （13 ページ）
- ファイアウォール モードの例 （14 ページ）
- ファイアウォール モードの履歴 （25 ページ）

ファイアウォール モードについて

ASA は、でルーテッド 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。

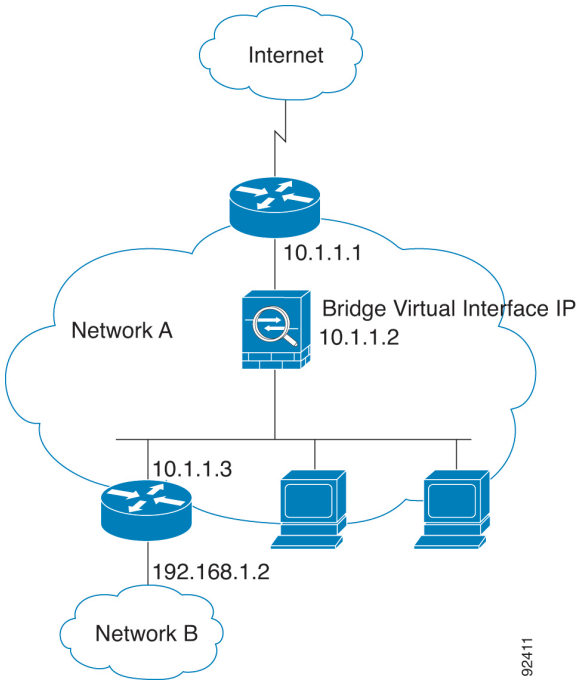
レイヤ2の接続は、ネットワーク上の内部と外部のインターフェイスをまとめた「ブリッジ グループ」を使用して確立されます。また、ASAはブリッジング技術を使用してインターフェイス間のトラフィックを通します。各ブリッジグループには、ネットワーク上で IP アドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。複数のネットワークに複数のブリッジグループを設定できます。トランスペアレントモードでは、これらのブリッジグループは相互通信できません。

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



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

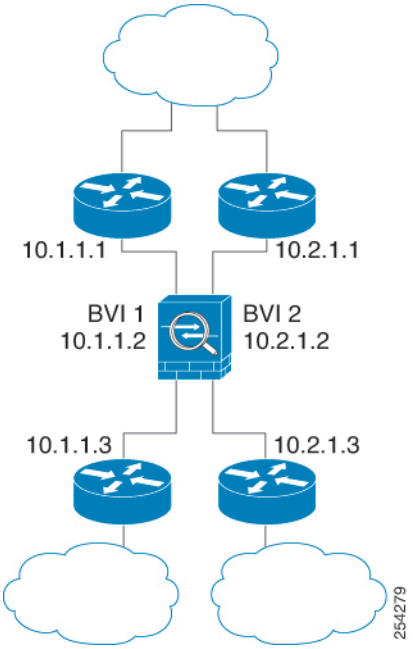
ブリッジグループのトラフィックは他のブリッジグループから隔離され、トラフィックはASA内の他のブリッジグループにはルーティングされません。また、トラフィックは外部ルータからASA内の他のブリッジ グループにルーティングされる前に、ASAから出る必要があります。ブリッジング機能はブリッジグループごとに分かれていますが、その他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、syslogサーバまたはAAAサーバの設定は、すべてのブリッジ グループで共有されます。セキュリティ ポリシーを完全に分離する

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ペアレント ファイアウォール ネットワーク



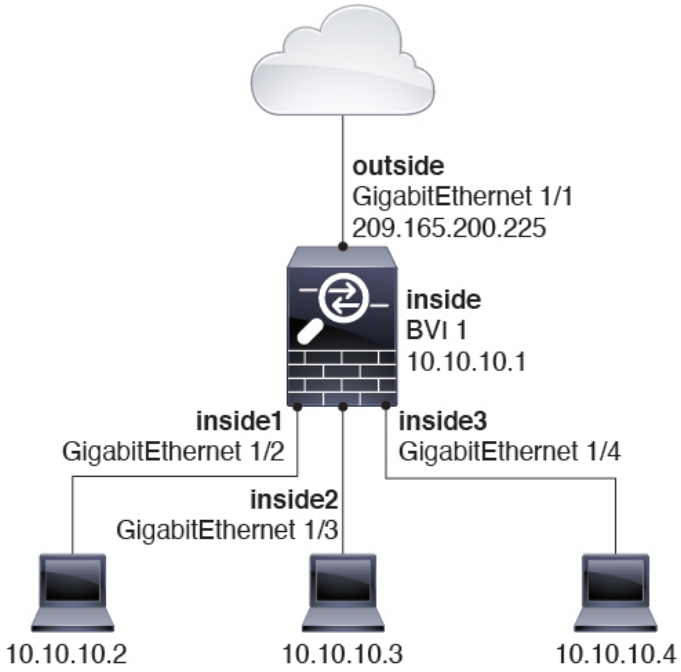
ルーテッド ファイアウォール モードのブリッジグループ

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ル 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 の IPv4 マルチキャスト MAC アドレス
- 3333.0000.0000 ～ 3333.FFFF.FFFF の IPv6 マルチキャスト MAC アドレス
- 0100.0CCC.CCCD に等しい 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 ネットワーク宛て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。
- インスペク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 エンドポイント宛て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。

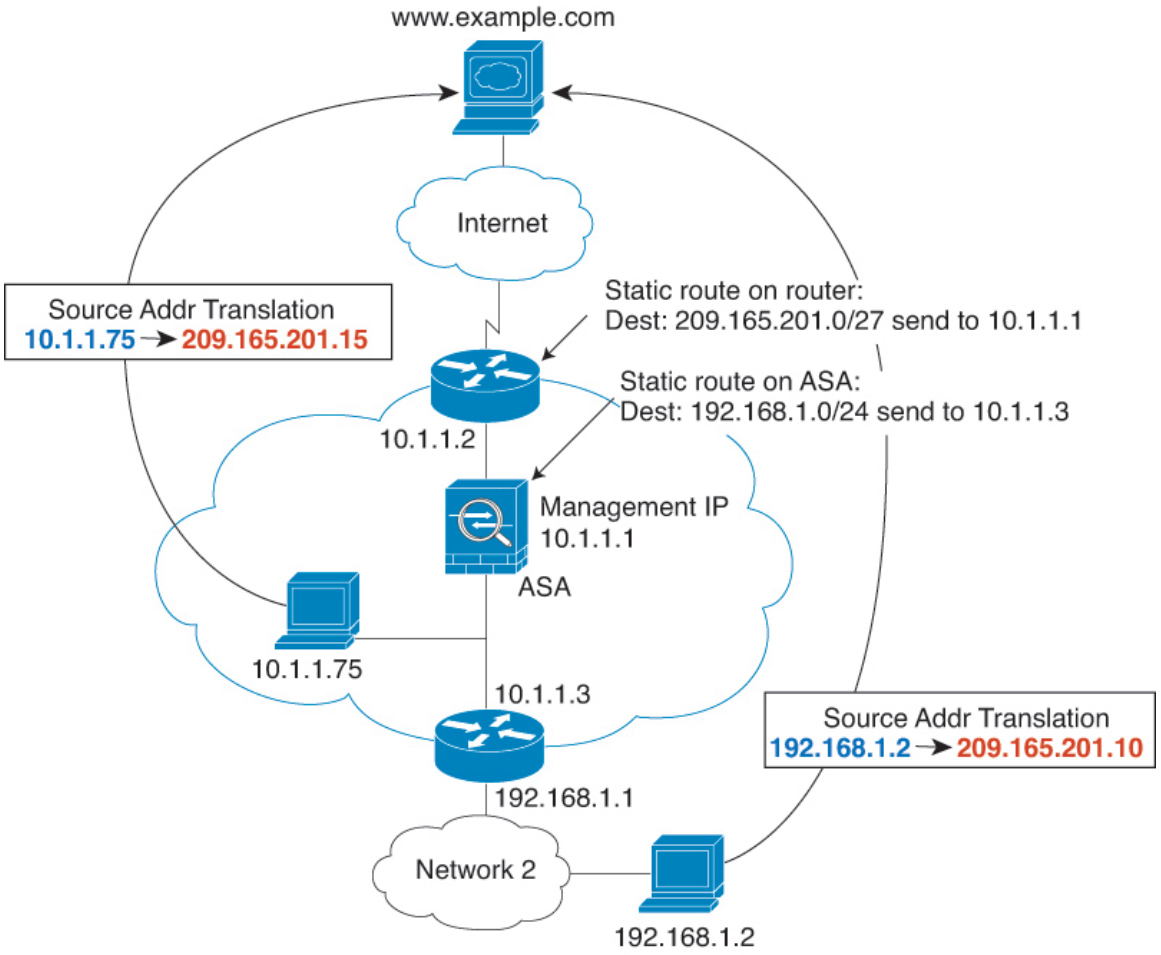
  影響を受けるアプリケーションは次のとおりです。

  - 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 ネットワーク宛て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 アドレス宛て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

特長	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。

特長	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。クライアントレス SSL VPN もサポートされていません。
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

特長	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。 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。

特長	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。
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 SSL VPN 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 をサポートします。

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 ixgbevf インターフェイスを備えた VMware の ASAv50 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 1010 および Secure Firewall 1210/20 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 *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 （13 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。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。

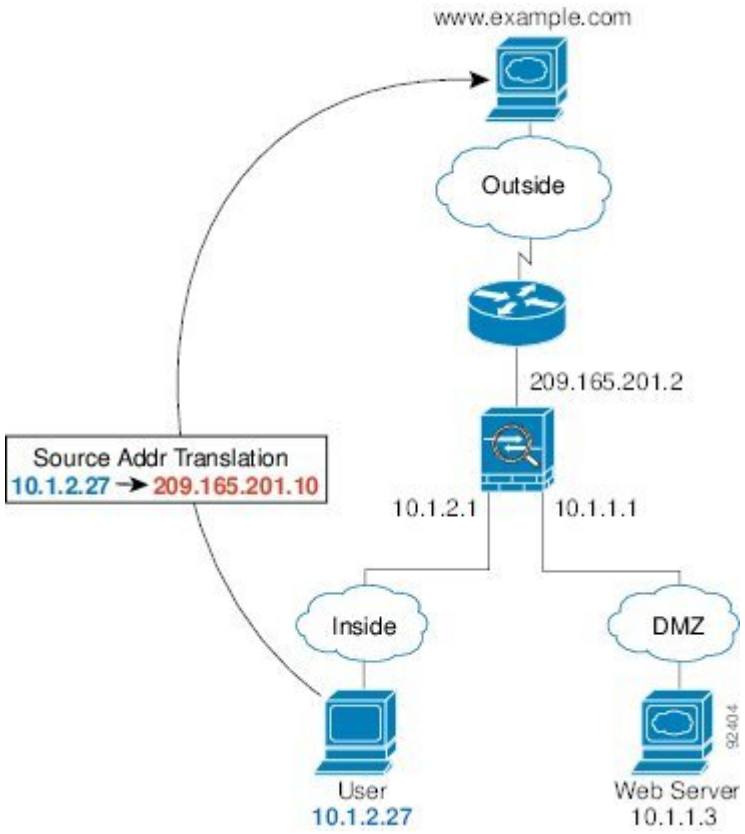
ルーテッド ファイアウォール モードで ASA を通過するデータ

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

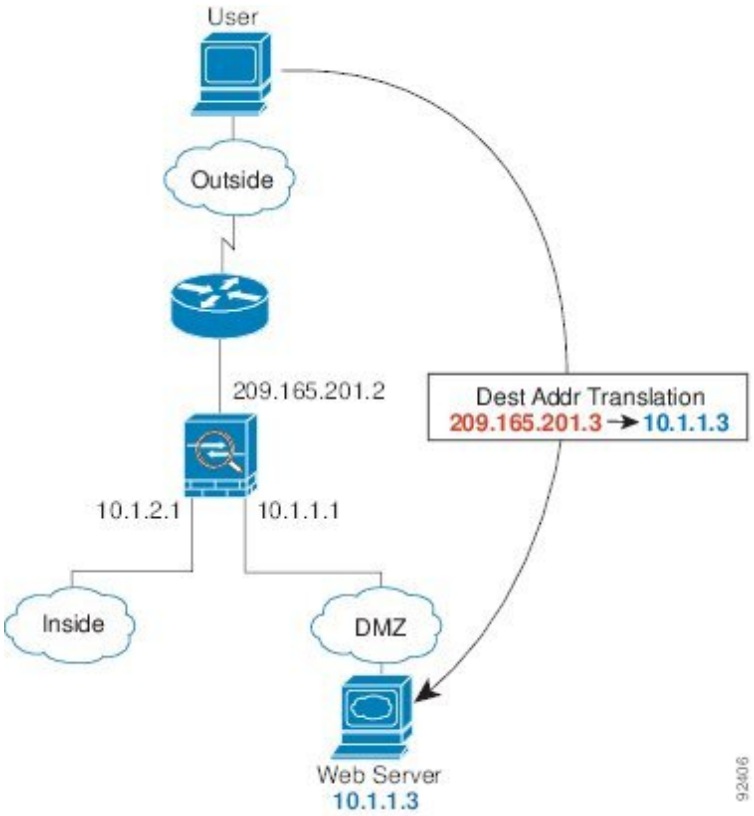
プをバイパスします。ASAは、グローバル宛先アドレスをローカルユーザアドレス10.1.2.27に変換せずに、NAT を実行します。

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。

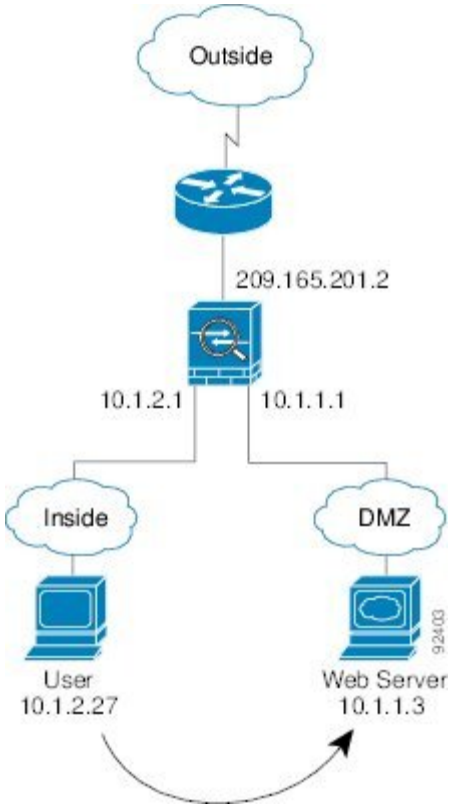
   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
4. 次に、ASAはセッションエントリを高速パスに追加し、DMZインターフェイスからパケットを転送します。

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。

1. 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。

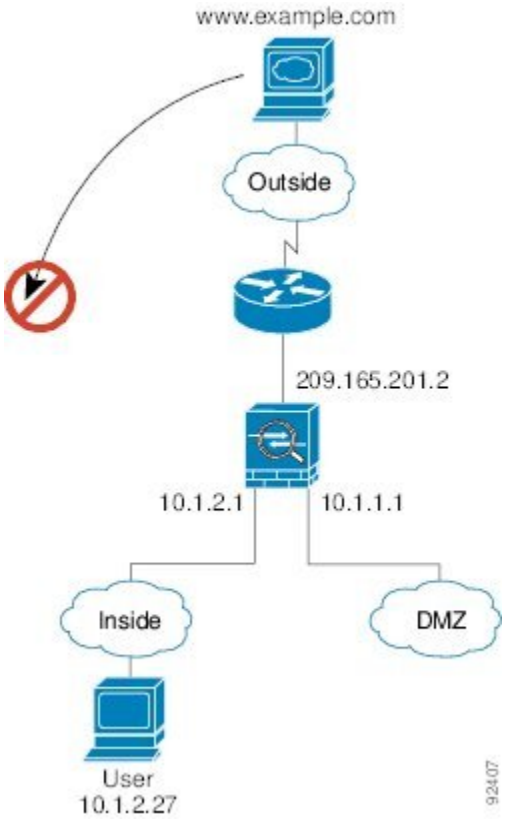
   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. 次に、ASAはセッションが確立されたことを記録し、DMZ インターフェイスからパケットを転送します。

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. 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）。

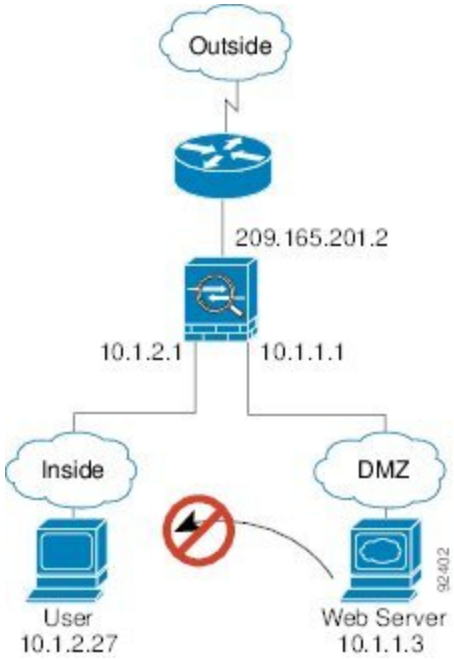
   内部ネットワークがプライベート アドレスを使用している場合、外部ユーザーが NAT なしで内部ネットワークに到達することはできません。外部ユーザーは既存のNATセッションを使用して内部ユーザーに到達しようとすることが考えられます。
2. ASAはパケットを受信します。これは新しいセッションであるため、ASAはセキュリティポリシーに従って、パケットが許可されているか確認します。
3. パケットが拒否され、ASAはパケットをドロップし、接続試行をログに記録します。

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。

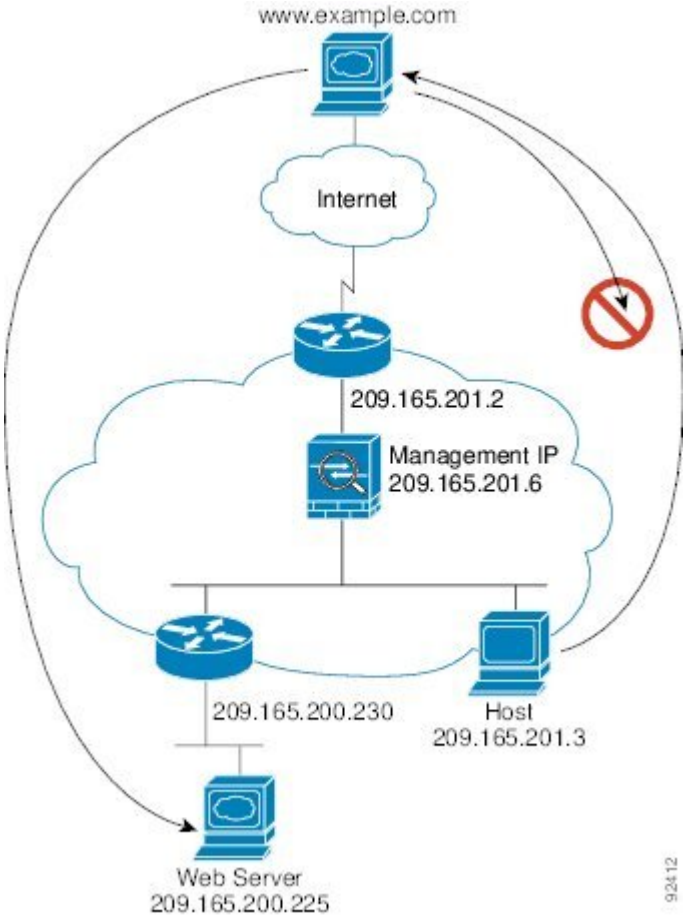
1. DMZ ネットワーク上のユーザーが、内部ホストに到達しようとします。DMZ はインターネット上のトラフィックをルーティングする必要がないので、プライベートアドレッシング方式はルーティングを回避しません。
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティポリシーに従って、パケットが許可されているか確認します。

   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。内部ユーザーがインターネット リソースにアクセスできるよう、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 サーバーだけにアクセスできます。

図 *10*：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

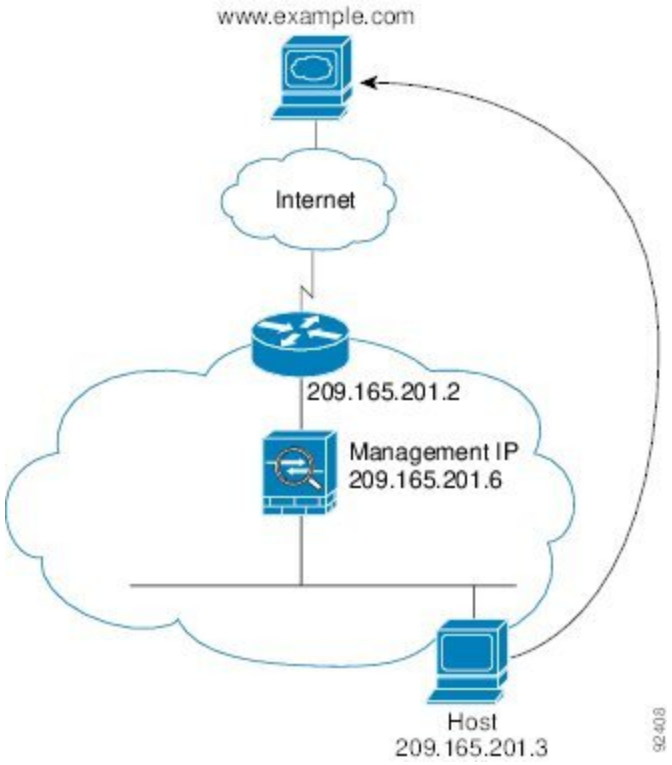


次のセクションでは、データが ASA をどのように通過するかを示します。

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 *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。

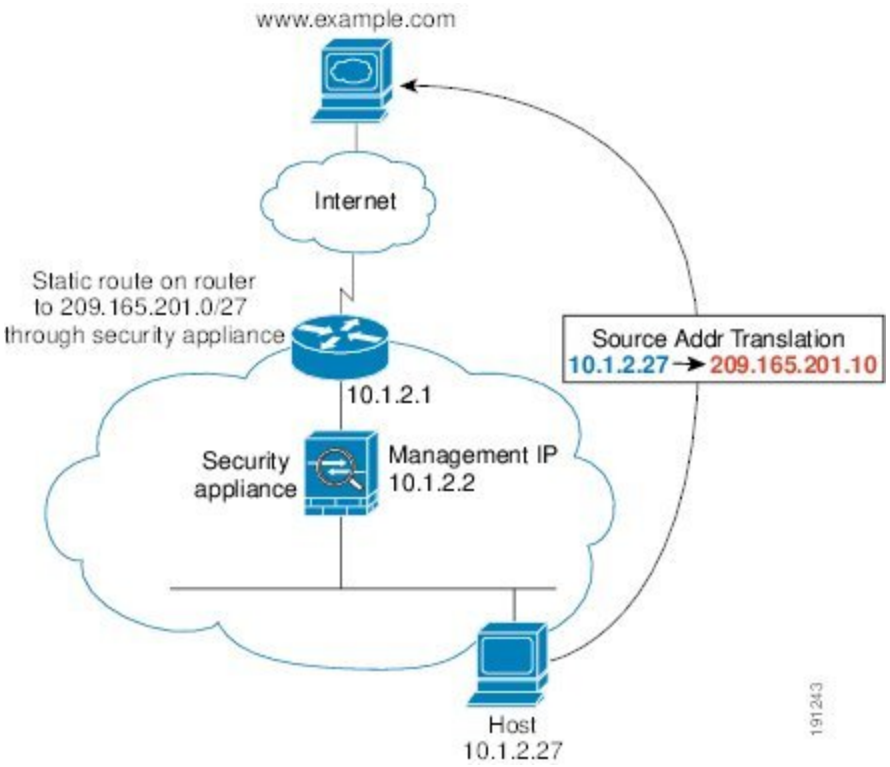
   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. ASAは、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、ASAは外部インターフェイスからパケットを転送します。宛先 MAC アドレスは、アップストリーム ルータのアドレス 209.165.201.2 です。

   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。

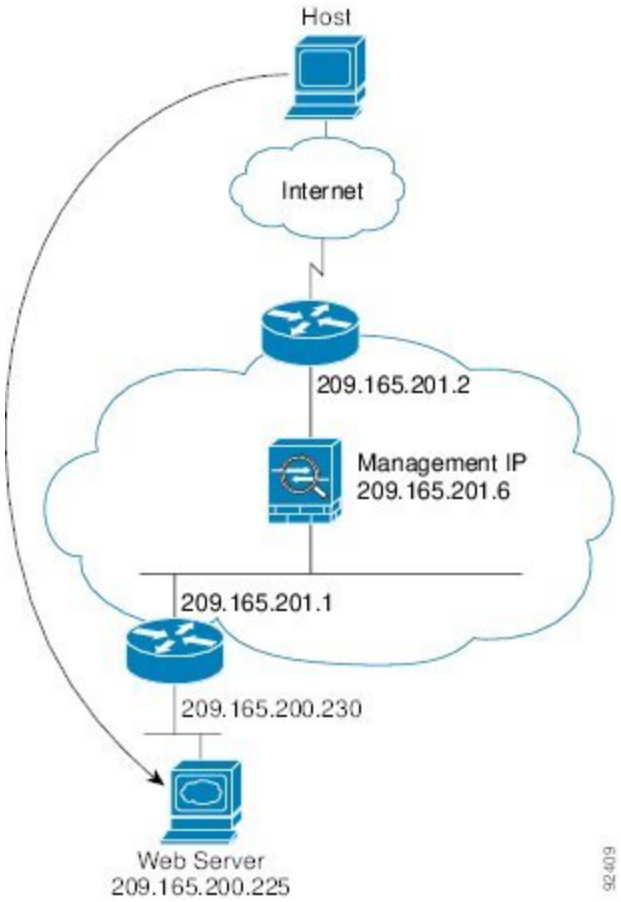
宛先 MAC アドレスが ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求と ping を送信します。最初のパケットはドロップされます。

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 アドレスを実際のアドレス 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。

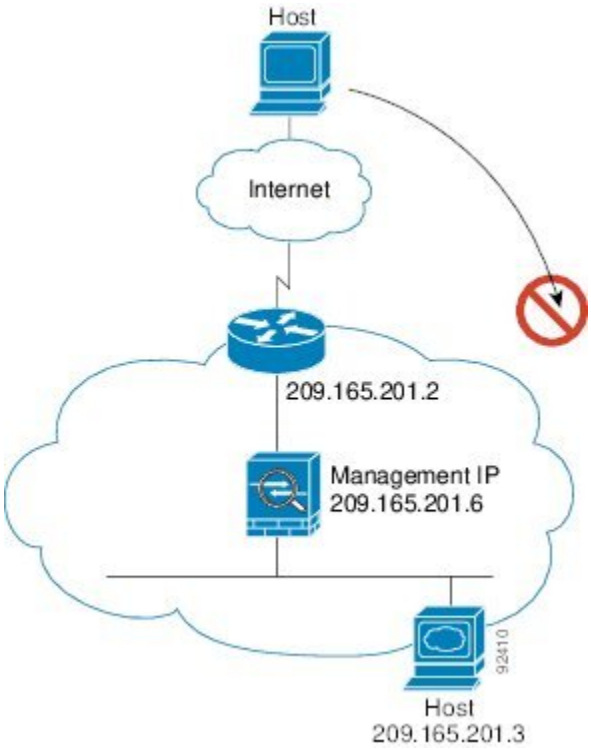
3. ASAは、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、ASAは内部インターフェイスからパケットを転送します。宛先 MAC アドレスは、ダウンストリーム ルータ 209.165.201.1 のアドレスです。

   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。
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)	セキュリティ コンテキス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。 **firewall transparent** コマンドが変更されました。
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)	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。 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。 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**

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ペア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、トランスペア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。