# Azblink NFV プラットフォーム

概要：本ドキュメントは、Azblink ネットワーク機能仮想化（NFV）プラットフォームを紹介します。Windows または Linux などのオペレーティングシステムをインストールした仮想マシンを提供し、ネットワークインターフェイス上でファイアウォールおよびルーティング関数を提供します。これは、ファイアウォール仮想化および SBC 仮想化に使用でき、仮想マシンをいくつかのゾーンにクリック数回でデプロイできます。

## Table of Contents

# 第 1 章 概要

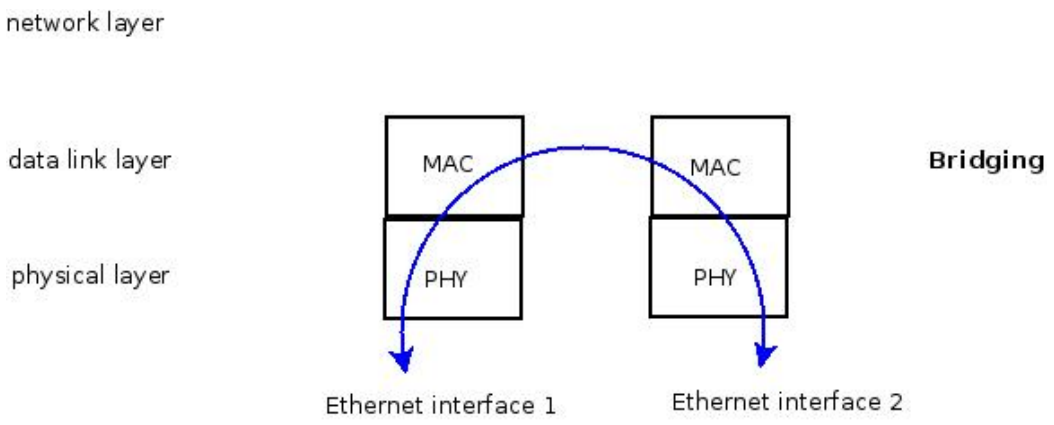
仮想マシンに複数のホストをインストールし、それぞれ異なるネットワークアクセス権限を与えることを考えてみてください。例えば、インターネットへのアクセスのみを許可し、内部ネットワークへのアクセスを禁止するホストと、インターネットへのアクセスを禁止し内部ネットワークへのアクセスのみを許可するホストをインストールします。この目標を達成する方法は、関連するルールを外部ファイアウォールまたはルーターで設定することによって多数の方法があります。当社のソリューションは、外部ネットワーク機器への過度な依存を避けるために、制御されたネットワーク環境における仮想マシンを提供することです。

Azblink Network Functions Virtualization Platform は、あらかじめ定義されたネットワーク環境で仮想ホストを作成するためのプラットフォームです。ネットワークゾーンは、ウェブインターフェースを通して追加または削除できるルールによって管理されます。このプラットフォーム自体がファイアウォールとルーターであるため、仮想ホストは最初から計画された環境で作成することができます。また、各仮想ホストをコンソールからリモートで管理するための VPN も提供されます。

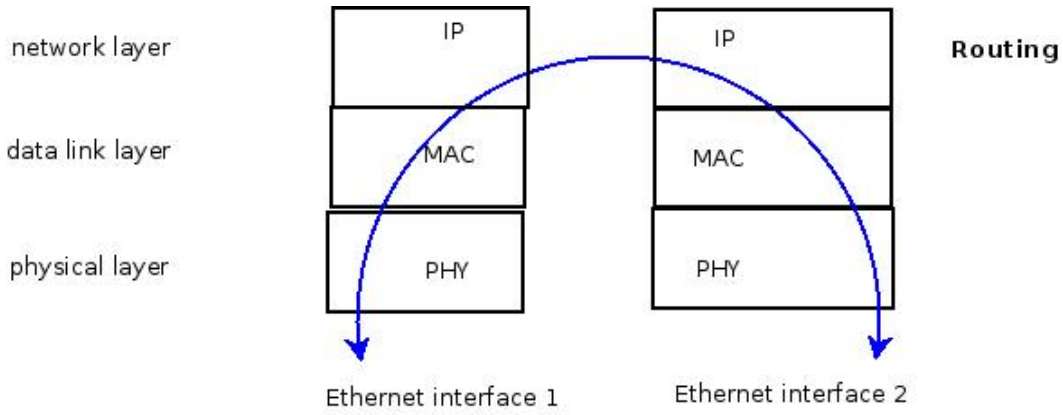
以下のセクションでは、このドキュメントで使用される用語を定義し、それらのネットワーク操作がどのように機能するかを説明します。

## *Bridging and Routing*

まずはブロッキングとルーティングの紹介から始めます。OSI（オープンシステム相互接続）モデルにおいて、データ交換がデータリンク層で行われる場合は「ブロッキング」、ネットワーク層で行われる場合は「ルーティング」と呼びます。TCP/IP/Ethernet においては、データがどこへ行くかを MAC アドレスの Ethernet フレームで判断する場合は「ブロッキング」、IP ヘッダの IP パケットで判断する場合は「ルーティング」と呼びます。データリンク層で送信および受信されるデータについて、人々は通常「フレーム」という用語を使用しますが、ここでは厳密にはそれに従いません。データリンク層またはネットワーク層のどちらにおいても、「ネットワークトラフィック」という用語を使用します。




挿絵 ***1:*** ブリッジ操作




挿絵 ***2:*** ルーティング 操作

「Ethernet」とは、物理層とデータリンク層（通常は PHY と MAC）で構成されています。そして IP（インターネットプロトコル）はネットワーク層に属します。したがって、Ethernet MAC アドレスのみを調べ、どこへ向かうかを判断する場合、それはブリッジングと言います。同様に、IP アドレスを調べ、それがどのカテゴリーに属するかを判断する場合、それはルーティングです。ネットワークアプリケーションが他の端にトラフィックを送信するには、多くの詳細で複雑なプロセスです。

ホストAが既知のIPアドレスを持つホストBにIPパケットを送信する場合でも、ホストBのMACアドレスを見つける必要があります。ARP（Address Resolution Protocol）は、そのIPアドレスに対応するMACアドレスを見つけるために使用されます。ホストAは最初に、そのIPアドレスに関するMACアドレスがlookupテーブルに存在するかどうかを確認します。もしMACアドレスが一致するものがあれば、そのMACアドレスが使用されます。一致するものがない場合、ARPクエリはネットワーク上でブロードキャストされます。ホストB（またはホストBへのゲートウェイ、もし異なるサブネットにいる場合）は、リクエストが自身のIPアドレスと一致する場合、自身のMACアドレスに応答します。このドキュメントでは、これらの詳細を説明することなく、計画と展開の容易さのために、いくつかの原則を概説します。

一般的に、「VLAN」が使用されない場合、ブリッジ（イステーチスイッチ）に接続するネットワーク機器は、同じIPサブネットに属すると考えることができます。異なるサブネットを跨るネットワークトラフィックの場合、つまり、ある足が１つのサブネットに、もう一方の足を異なるサブネットに置くような状況で、ルーターがその間に位置する必要があります。

## バーチャルブリッジとバーチャルホスト

Azblink NFVプラットフォームは、「仮想ブリッジ」と「仮想ホスト」を提供し、WindowsやUbuntuなどの他のオペレーティングシステムを仮想ホストにインストールすることを可能にします。以下のセクションでは、Azblink NFVプラットフォームまたは仮想ホストを作成できるシステムを「ベースプラットフォーム」、「ベースOS」、「ホストOS」と参照し、仮想ホスト内のオペレーティングシステムを「ゲストOS」と参照します。

「base platform」において、ネットワーク運用ポリシーは「仮想ブリッジ」をユニットとして使用します。仮想ホストが作成されると、関連する仮想ネットワークインターフェース（VNI）も同時に作成する必要があります。各仮想ネットワークインターフェースの仮想ホストへの接続に使用する仮想ブリッジを選択するように強制します。

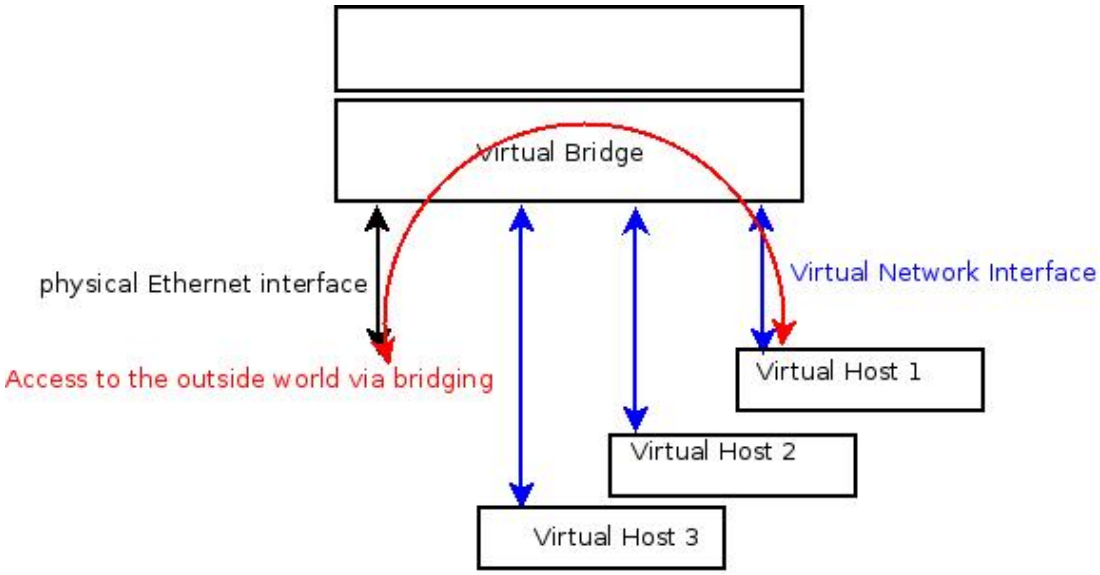


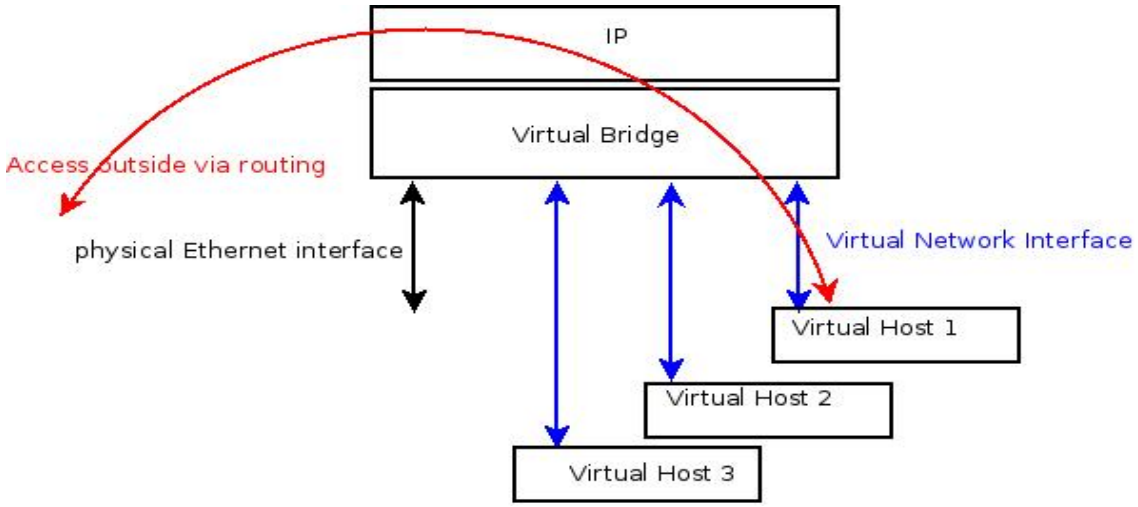

イラスト ***3:*** 橋内交通

各「仮想ネットワークインターフェース」は、仮想ホストの仮想ブリッジに配置されます。物理的なイーサネットインターフェースもブリッジに追加された場合、仮想ホストはブリッジ処理によってベースプラットフォーム外のネットワークにアクセスできます。“仮想ブリッジ”は、ベースプラットフォームのスーパーイーサネットインターフェースとして機能し、自身の IP アドレスとネットマスクで IP サブネットを示すことができます。ブリッジの IP アドレスは、ベースプラットフォーム上のローカルネットワークプロセスに到達するためのインターフェースと見なすことができます。ベースプラットフォーム側では、ブリッジ内のネットワークインターフェース（物理インターフェースまたは仮想インターフェースを問わず）は、ベースプラットフォーム上のネットワークインターフェースには IP アドレスが設定されていません。仮想ホスト側の視点からは、ゲスト OS は仮想ホストで自身の IP アドレスを設定できます。

具体的には、仮想ブリッジが “br0” で、それに IP アドレスが設定されているとします。仮想ブリッジ “br0” の内部には、”eth0” やその他の仮想イーサネットインターフェースが見つかるかもしれません。ベースプラットフォーム側にあるこれらのイーサネットインターフェースは、ブリッジ上で IP アドレスが設定されていません。

実際、「仮想ブリッジ」は、エthern ネットスイッチとして見なすことができます。同じスイッチに接続されたホストは、VLAN が使用されていない限り、同じ IP サブネットに属している必要があります。IP ネットワークをサブネットに分割する理由は、比較的ローカルな環境においてネットワークトラフィックを分離し、グローバルな影響を与えないようにするためです。例えば、ARP リクエストが送信されると、受信したすべてのホストは、自身の IP アドレスがリクエスト内の IP アドレスと一致するかどうかを確認する必要があります。このようなリクエストが頻繁に発生した場合、リソースの消費は効率的でない可能性があります。なぜなら、ARP リクエストの実際のターゲットは 1 つのホストだけだからです。したがって、IP ネットワークにおけるネットワークブロードキャストは、同じサブネットに制限され、他のサブネットに渡りません。ARP リクエストは IP ネットワークブロードキャストで行われ、それ以外にもブロードキャストに依存する他の IP ベースのプロトコルが存在します。それらのホストが互いに通信するためには、同じ IP サブネットに配置する必要があります。

仮想ホストのネットワークパケットがサブネットを通過する可能性があります。以下の図において、ターゲットホストのサブネットへのゲートウェイが、仮想ブリッジ内のその物理イーサネットインターフェースを通じて到達可能である場合、パケットは、その物理イーサネットインターフェースを通して、そのゲートウェイに渡ります。しかし、ベースプラットフォームもブリッジに IP アドレスを持っています。ベースプラットフォームが仮想ホストからの宛先であるサブネットに接続されたネットワークインターフェースに接続されている場合、パケットはベースプラットフォームを通してルーティングプロセスにより、そのサブネットに渡る可能性があります。

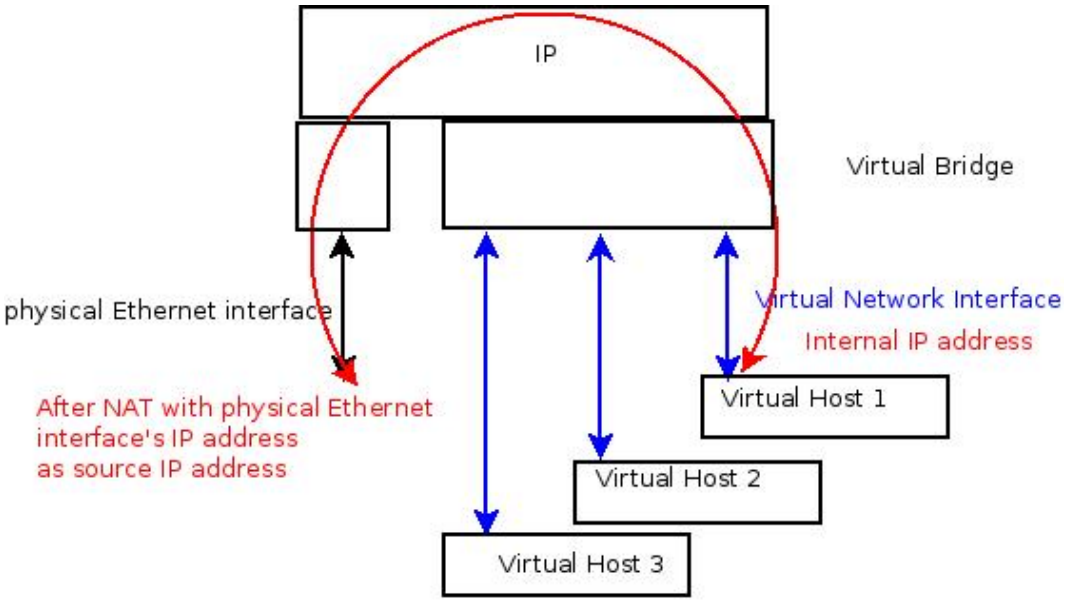



挿絵 ***4:*** 橋を渡って別のサブネットへ向かうトラフィック

要約すると、仮想ブリッジと仮想ホストは、ベースプラットフォームの内側で作成されますが、ベースプラットフォームは、仮想ホストのネットワークレベルにおいて並行するホストとして扱われます。仮想ホスト内のネットワークアプリケーションがベースプラットフォームに連絡を取りたい場合、ベースプラットフォームの IP アドレス（アドレス）を使用してネットワークリクエストを送信します。

## *Other Possible Network Operations( But we do not provide )*

理論上、仮想ホストと基盤プラットフォームに接続されている物理イーサネットインターフェース間での他の操作が存在する可能性があります。ここでは、製品で提供されていないネットワーク操作の一覧を示します。その理由は、Azblink NFV プラットフォームが「サーバー型」アプリケーション向けであるため、これらの操作スキームは「サーバー型」アプリケーションには適切ではない可能性があります。完全性を保つため、これらの操作について以下で説明します。次のセクションでは、Azblink NFV プラットフォームが提供するものを示します。

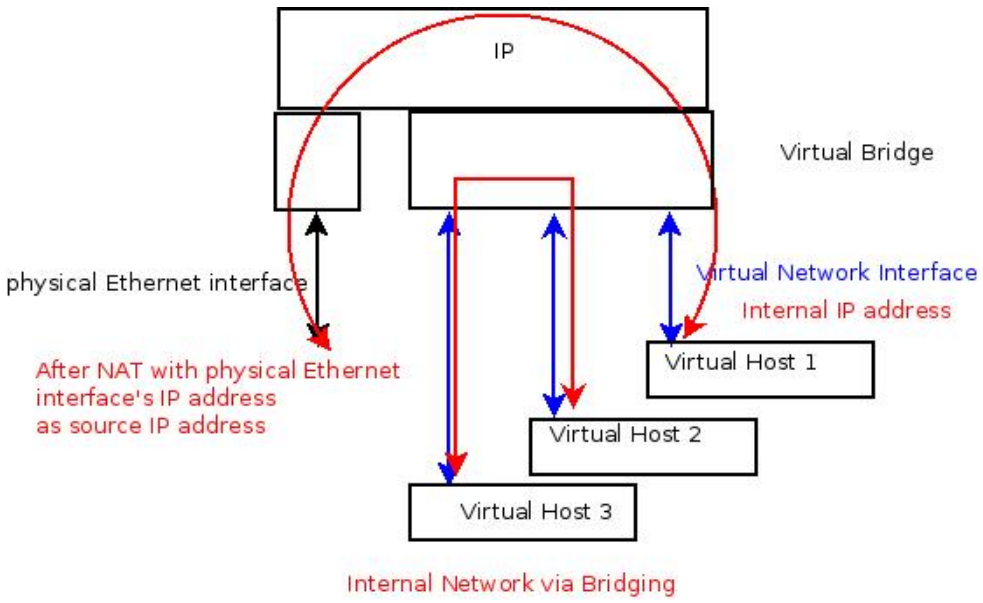



挿絵 ***5:*** 物理ポートごとに ***NAT***

上記の図は、仮想ホストが NAT（Network Address Translation）によって隠されていることを示しています。このシナリオは、通常、「ベース OS」で指定された物理 Ethernet インターフェースの IP アドレスを持つ仮想ホストが作成された場合に発生します。仮想ホストが作成されると、それに対応するブリッジも作成され、物理 Ethernet インターフェースに設定されていた IP アドレスが NULL 化され、その IP アドレスをブリッジデバイスに割り当て、その Ethernet デバイスをブリッジに入れ、仮想ホストにプライベート IP アドレスを与えます。仮想ホストが「ベース OS」の外にあるホストにアクセスしようとするパケットは、ブリッジデバイス（物理 Ethernet インターフェースの元の IP アドレス）の IP アドレスで置き換えられます。

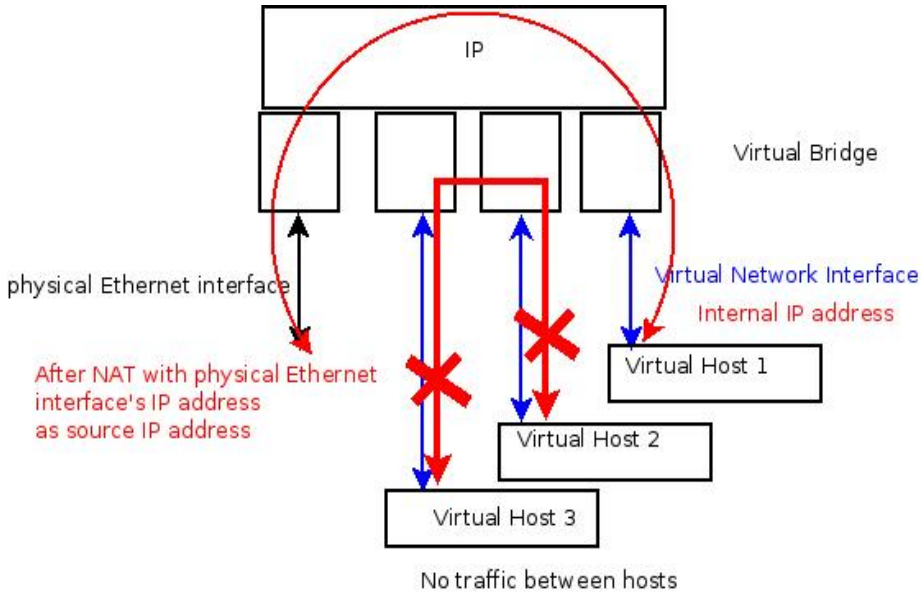
外部の「ベース OS」の外からそのホストにアクセスするには、ポートフォワーディングが必要です。

以下の図は、同じ IP アドレスの背後にある仮想ホストが、NAT を経由せずに独自のプライベート IP アドレスで相互に通信するシナリオを示しています。これは、それらを同じブリッジに接続することで実現されます。



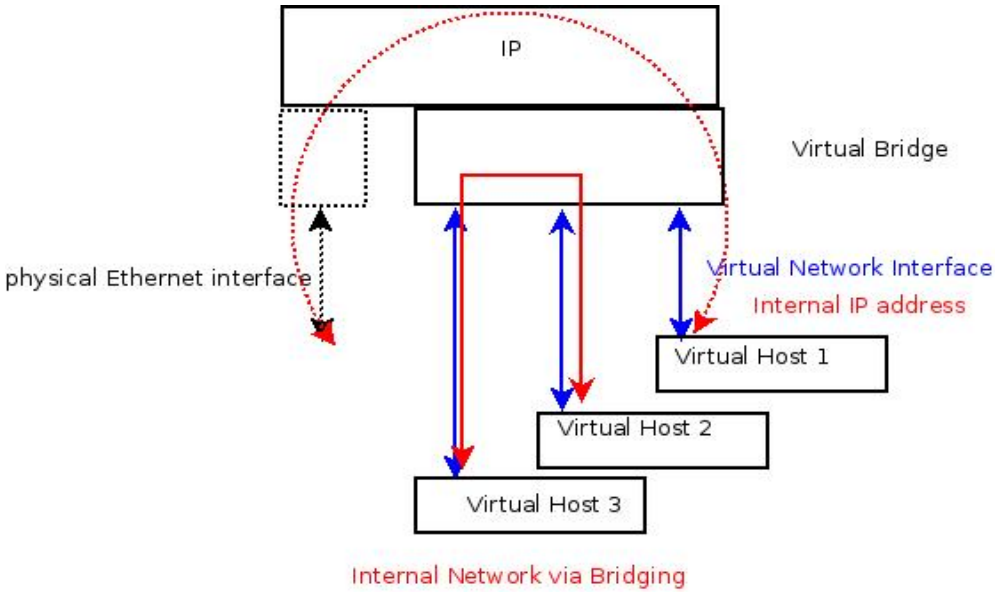

挿絵 ***6:*** 同じブリッジ上の仮想ホスト間でのトラフィックの送信を許可する

仮想ホストが同じ NAT の IP アドレスの下にありながらも互いに通信できない別のシナリオが存在します。それらは外部世界へのアクセスは可能ですが、自身のプライベート IP アドレスを使用して互いに到達することは許可されていません。このシナリオは奇妙に聞こえるかもしれませんが、2 つの仮想ホストが異なる企業に所有されているクラウドベースの環境で発生することがあります。




挿絵 *7:* 仮想ホスト間のブリッジ上でのトラフィックの許可なし

以下の図は、NAT 関数が削除されたことを示しており、仮想ホストは外部の世界にアクセスできず、同じブリッジを通じて、それぞれのローカルのプライベート IP アドレスで互いに通信できることを示しています。




挿絵 ***8***: 橋の中に交通がロックされている

上記の操作は、当社の基盤プラットフォームでは提供されていません。 仮想ネットワークインターフェースの仮想ブリッジが接続されるように、ただ決定するだけをお願いします。

もし、一部の機能（例えば、NAT）がシステム展開中に必要となる場合、私たちはグローバルな仮想ブリッジの配置でシステムを管理します。各ブリッジはそれぞれ事前に定義された機能を持つものです。例えば、サブネットA（ブリッジ経由で接続）からサブネットB（別のブリッジ経由で接続）へのネットワークパケットは、ベースOSで定義されていれば、宛先ネットワークのIPアドレスでソースIPアドレスが置換されます。これは次のセクションで説明します。

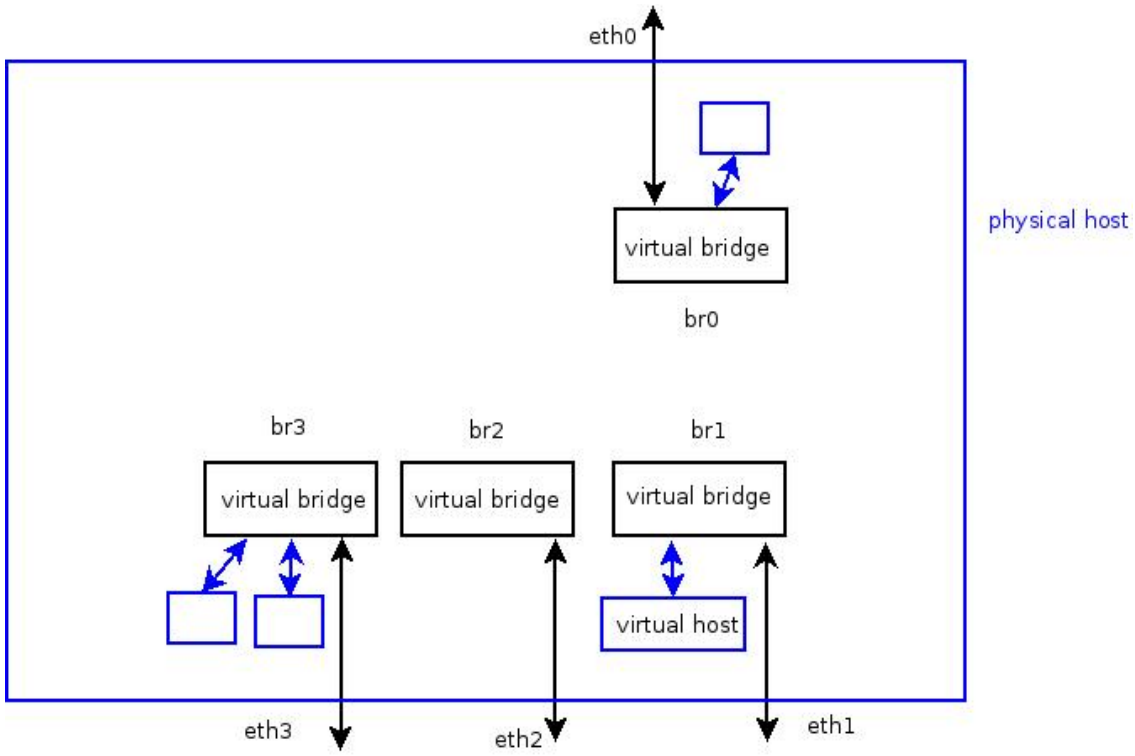
## 橋のファイアウォール運用

Azblink NFV プラットフォームは、複数の仮想ブリッジと、それらの仮想ブリッジ間のあらかじめ定義されたルールを提供する。例えば、ネットワークトラフィックが“br1”、“br2”、“br3”から WAN を介して“br0”に渡る場合、ソース IP アドレスをヘッダー内の“br0”の IP アドレスに置き換えることで NAT（Network Address Translation）が行われる。ネットワークトラフィックは“br3”から“br1”およびその逆方向に行くことができる。しかし，“br1”へのトラフィックは許可されないが、他のサブネットからの“br1”へのトラフィックは許可される。後でこのドキュメントでさらに詳細を検討する。

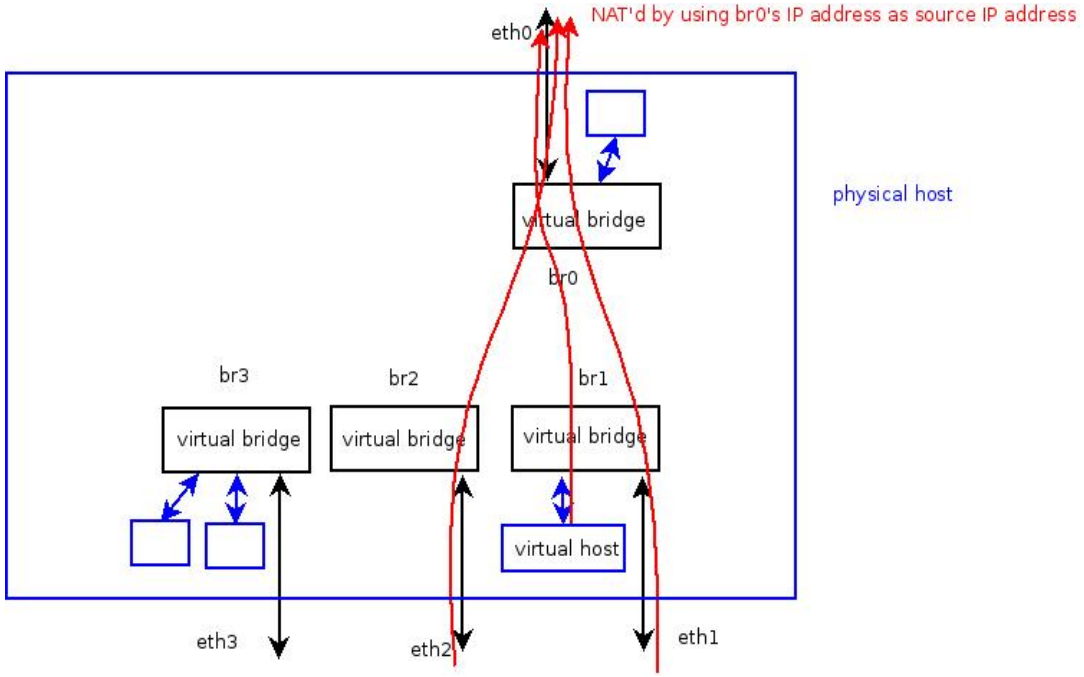
「br0」の下のホストから開始されたネットワーク トラフィックは、他のブリッジに入ることはできません。

この構成のメリットは、異なるゾーンに仮想ホストを、権限レベルに応じて簡単に行うことができる点です。また、防火帯は事前に慎重な計画によって、グローバルなアクセスレベルを制御できます。各仮想ホストの場合、異なるゾーンにデプロイする必要がある場合は、異なるブリッジに複数の仮想ネットワークインターフェースを配置できます。

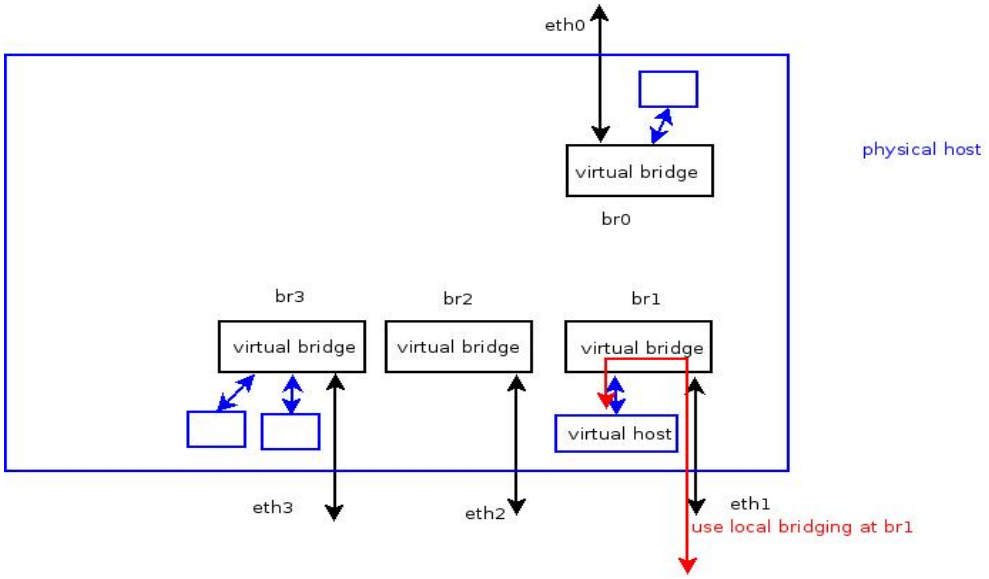
***Illustration 9: Virtual Bridges inside Base Platform***



以下の図は、「br1」または「br2」から「br0」を経由して発生するネットワークトラフィックを NAT（Network Address Translation）で処理し、「br0」の IP アドレスを送信元 IP アドレスとして扱うことを示しています。これは仮想ホストであろうと、ブリッジ“br1”または“br2”の下にある物理ネットワークインターフェースであろうと関係ありません。



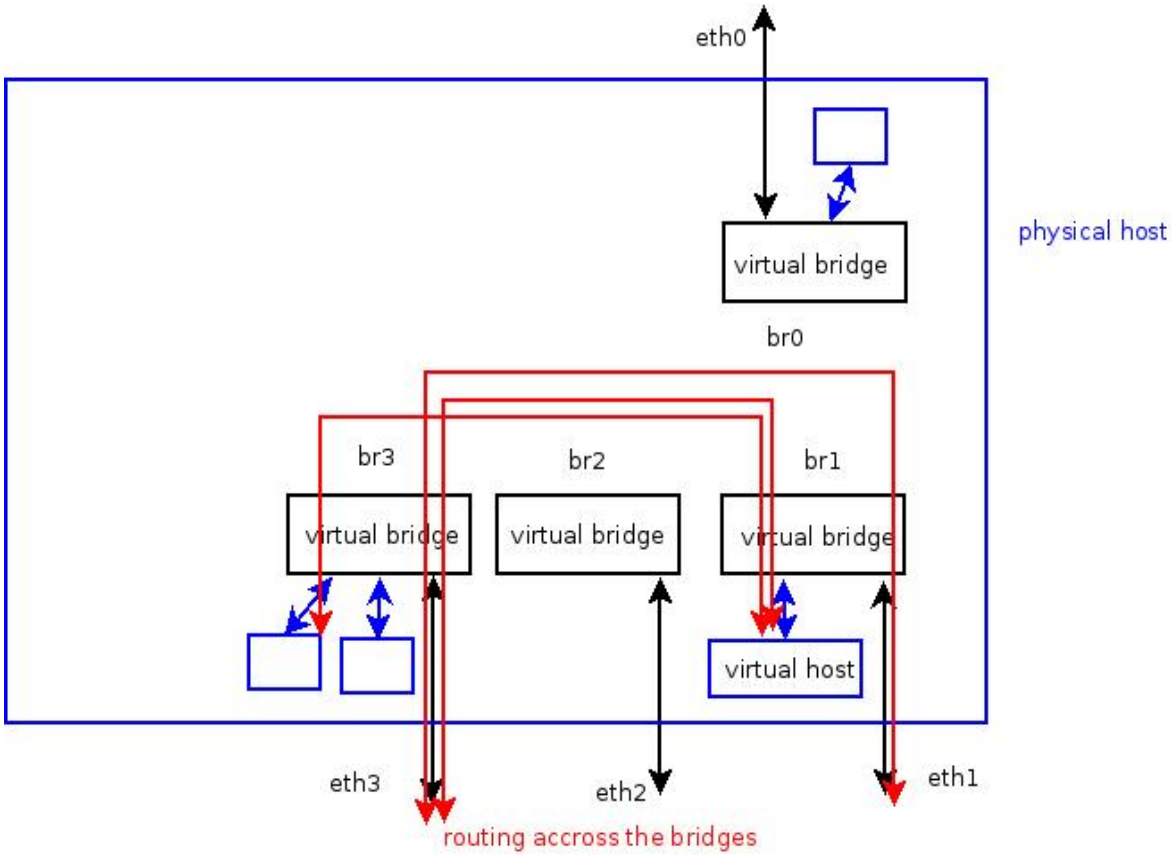

挿絵 ***10: br0*** の境界を越えて ***NAT*** を行う




挿絵 ***11:*** ブリッジ ***br1*** 内での ***NAT*** オペレーション なし

「br1」の下に配置された仮想ホストは、「eth1」経由で制限なしにアクセス可能です。これは仮想ホスト自体が独自のアクセス制御を実装するかどうかによって異なります。仮想ホストが制御スキームを持たない場合、基盤プラットフォームのファイアウォールは、より詳細な制御のために追加のルールを適用できます。

“br1”または“br3”のホストから“br0”のホストへのアクセスは、ポートフォワーディングを使用しない限り禁止されています。




挿絵 ***12:*** ブリッジ境界 ***br1*** と ***br3*** を通過する際に ***NAT*** 動作を行わない

“br1”および“br3”のホストは、ベースプラットフォームが提供するルーティングプロセスによってネットワークトラフィックを交換できます。それらのブリッジ内に存在する仮想ホストは、物理的なエンティティ内にあるにもかかわらず、論理的にはベースプラットフォームから独立しており、それぞれ独自の“ネットワークアイデンティティ”を持ち、他のホストと同様に、コンソールを除く自身の IP アドレスによってのみアクセス可能です。したがって、論理的には、それらは物理ホストの外にあるホストのように見なされるべきです。

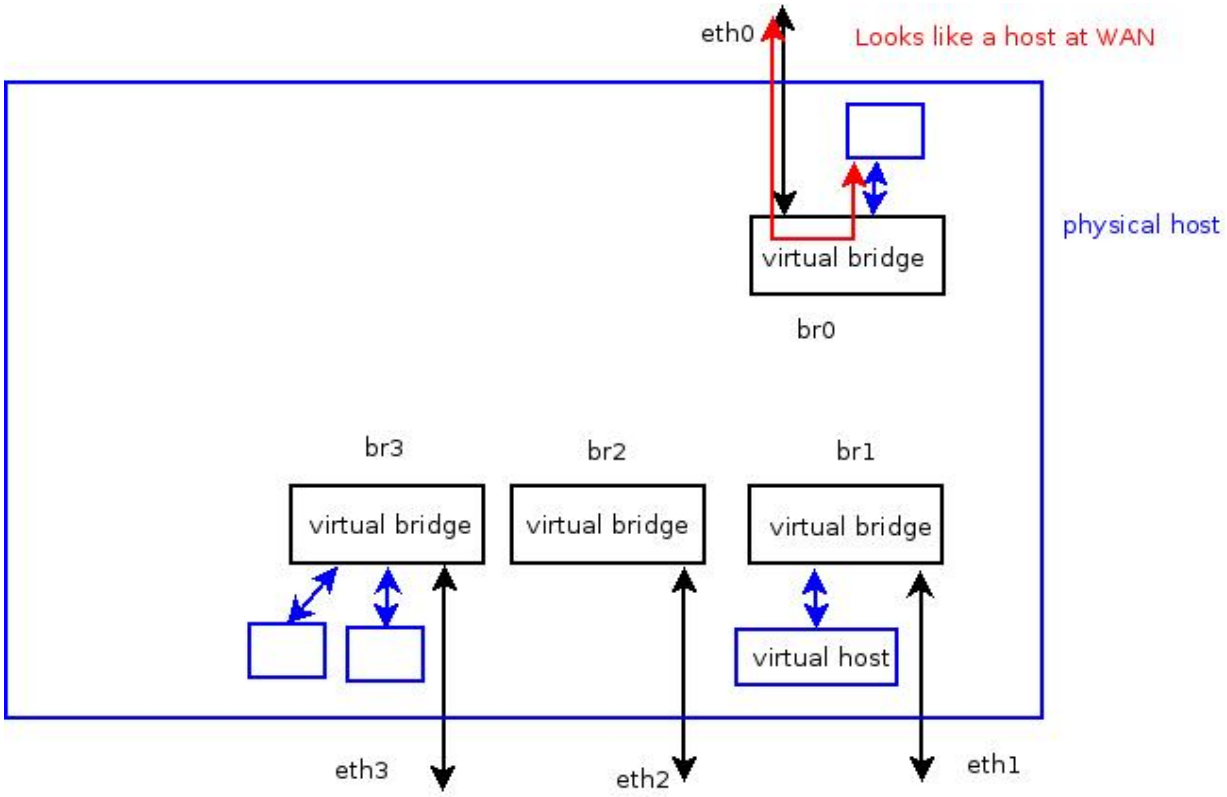
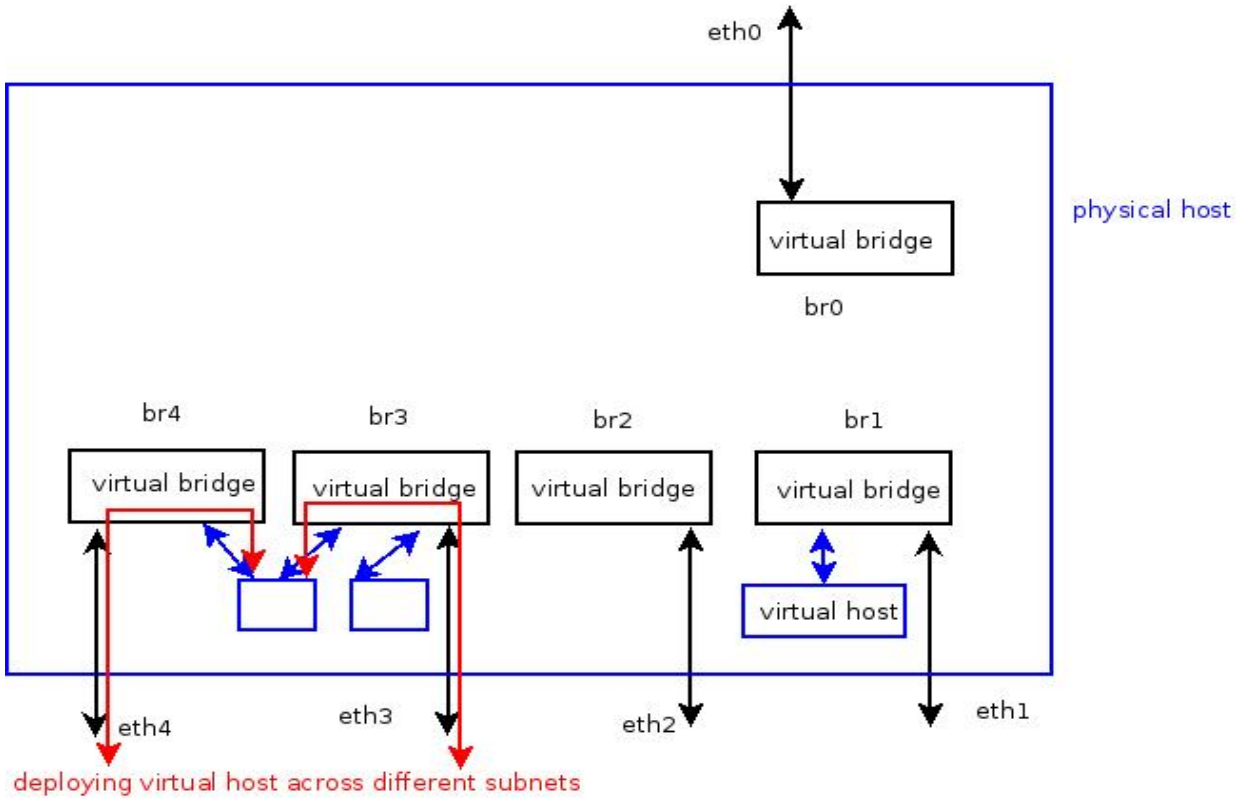



イラスト ***13:*** 仮想ホストがブリッジ ***br0*** に接続

「br0」という仮想ホストを例として使用します。仮想ホストは「br0」の下に作成されます。「br0」というブリッジは IP アドレスを持ち、それがベースプラットフォームのアイデンティティであり、仮想ホストも同じサブネット上の自身の IP アドレスを持ちます。仮想ホストからのインターネットへのアウトバウンドトラフィックは「br0」を経由すべきですが、NAT の操作によって処理されず、自身の IP アドレスをソースアドレスとしてブリッジ経由で出力されます。したがって、この仮想ホストはベースプラットフォームのファイアウォールによって保護されません。また、「br1」または「br2」の下にある他のホストは、「br0」ホストを「ファイアウォール外」のホストとして認識します。

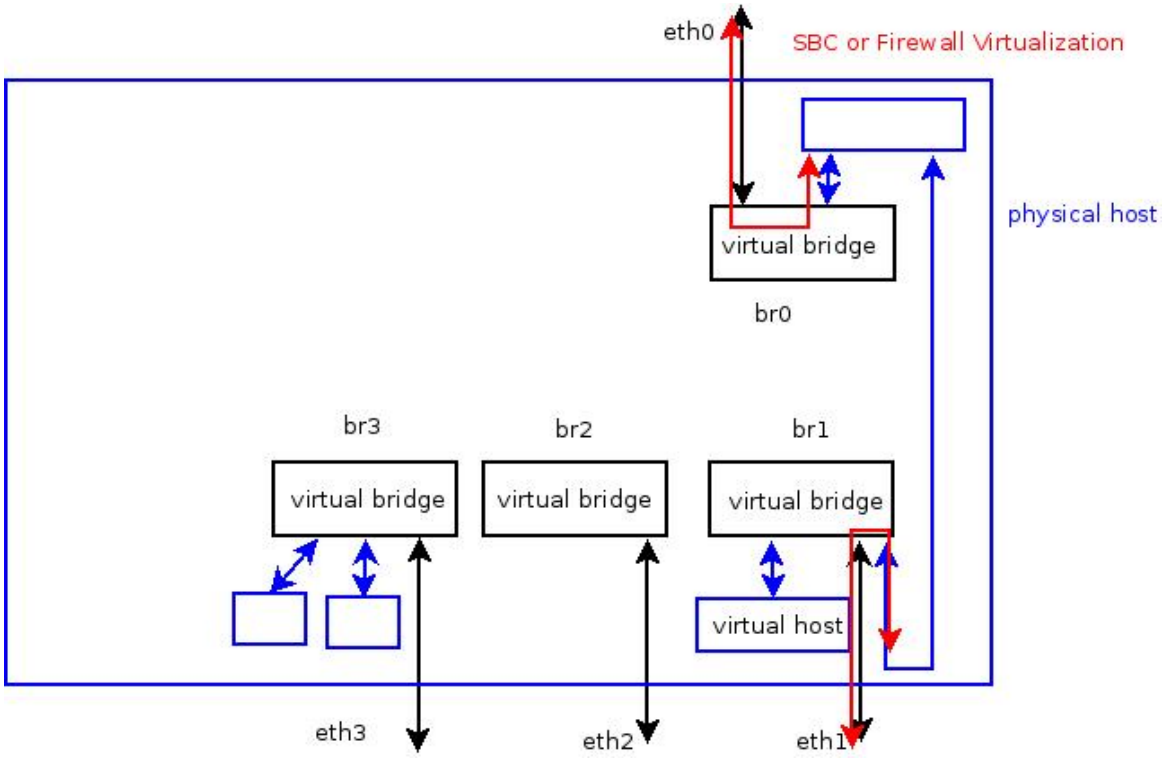
同様に、仮想ホストは複数の「レッグ」を複数の仮想ブリッジに持つことができます。以下の図は、仮想ホストが「br3」と「br4」の仮想ブリッジに複数の「レッグ」を持つ例です。したがって、この仮想ホストからその 2 つのサブネットへの発信されたネットワークトラフィックは、ベースプラットフォームのルーティングプロセスを経ることなく、仮想ホストと 2 つのサブネットの間に直接リンクします。ネットワークプロトコルの中には、サブネットを超えないものもあります。この構成により、この仮想ホストは 2 つのサブネットそれぞれに、それらのネットワークプロトコルを適用できます。




挿絵 ***14:*** 仮想ホストが複数のブリッジに接続

## *Firewall Virtualization or SBC Virtualization*

もし仮想ホストが“br0”と“br1”という 2 つの仮想ネットワークインターフェースを持っている場合、この仮想ホストは“仮想ファイアウォール”または“仮想 SBC”として実装できます。

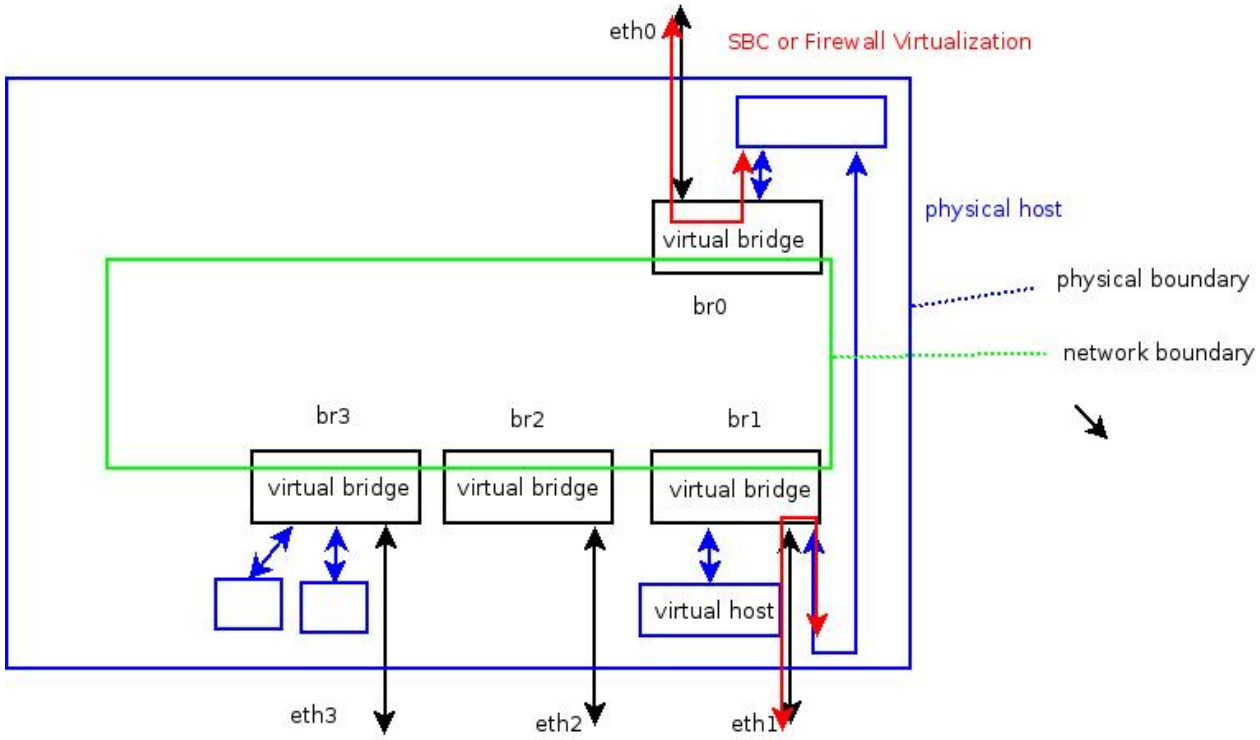



挿絵 ***15:*** 仮想ホストがブリッジ ***br0*** と ***br1*** に接続

この仮想ホストは WAN で 1 つのインターフェース、LAN で別のインターフェースを持っており、「仮想ファイアウォール」または「仮想 SBC」となる可能性を持っています。ベースプラットフォーム自体がファイアウォールでもあるため、「br1」が接続するサブネットのファイアウォールからどのファイアウォールを使用するかはどうすればよいでしょうか。もしそのサブネットの機械がその仮想ファイアウォールの IP アドレスをデフォルトゲートウェイとして使用する場合、トラフィックは仮想ファイアウォールを介してインターネットにルーティングされます。

人を仮想ファイアウォールを使用させるには、DHCP サーバーをオフにし、「br1」から「br0」へのトラフィックをベースプラットフォーム上で禁止するルールをプロビジョニングするだけで十分です。したがって、人々は「br1」からインターネットにアクセスするために、仮想ファイアウォールを使用することしかありません。

同様に、「仮想 SBC」も同じようにデプロイできます。

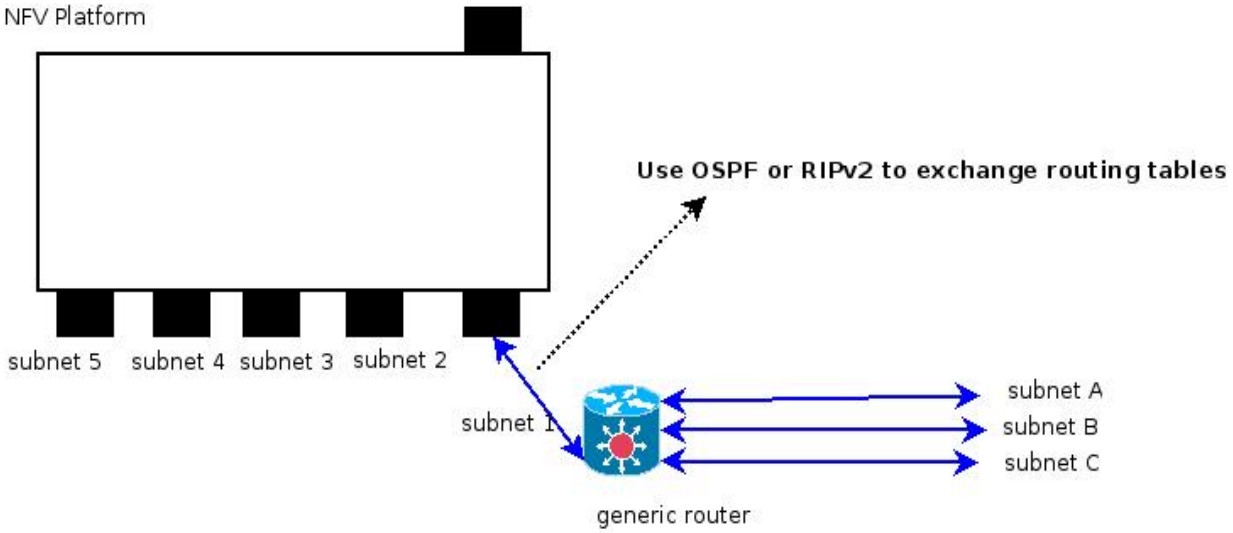



挿絵 ***16:*** ファイアウォール仮想化における仮想ホスト接続

「ベースプラットフォーム」と「仮想ホスト」の関係の混乱を避けるために、これらの仮想ブリッジを複数の「イーサネットスイッチ」と考えることができます。「ベースプラットフォーム」の各足をこれらの「イーサネットスイッチ」に接続し、各足を介して IP アドレスを定義します。「仮想ホスト」も同様に「イーサネットスイッチ」に足を接続します。「イーサネットスイッチ」には同じ IP サブネット内のホストが含まれています。

仮想化の利点は、ネットワークインターフェースを「ブリッジ」にソフトウェア再構成によって追加することができ、実際にネットワークインターフェースカードとケーブルを設置することなく行えることです。また、基となるプラットフォームは仮想ホストのコンソールにネットワーク方法を提供し、仮想ホストのコンソールをリモートでアクセスできます。ゲスト OS は、この機能のために他のソフトウェアパッケージをインストールする必要はありません。

このプラットフォームはまた、OSPF と RIPv2 に対応しており、他のルーターと自動的にルーティングテーブルを交換することができます。




挿絵 ***17:*** ベースプラットフォームとその他のルーター

さらに、ベースプラットフォームは Border Control というファイアウォール機能も提供します。これは後でこのドキュメント内で紹介されます。また、仮想ホスト内で独自のファイアウォールを実装するために、以前このセクションで示された仮想ブリッジに接続することも可能です。次の章では、ベースプラットフォーム上に仮想ホストを作成する方法を紹介します。

# 第 2 章 仮想ホスト

仮想ホストを使用する目的は、物理的なエンティティのような機能を実現することにあると考えられています。多くのアプリケーションは、ハードウェア（例えば、RS232 シリアルポートリンク、または Bluetooth）の物理的なインターフェースに依存して動作します。しかし、当社の製品はネットワークアプリケーションに焦点を当てているため、主なアプリケーショントランザクションはネットワークを介して行われます。アプリケーションがこのカテゴリーに属する場合に注意する必要があります。

概念的に、ここでいう「仮想ホスト」とは、OS（Operation System）ソフトウェアが機能するための容器のようなものです。OS の点では、仮想ホストは CPU、メモリ、ストレージスペース、ネットワークインターフェース（s）、その他の種類の周辺機器を提供し、物理的なマシンと同じように機能します。OS が「仮想ホスト」を提供する OS と、「仮想ホスト」上で実行されている OS との区別のため、「仮想ホスト」を提供する OS は「ホスト OS」、「ホストシステム」、「ベースプラットフォーム」または「ベース OS」と呼び、「仮想ホスト」上で実行されている OS は「ゲスト OS」、「ゲストシステム」と呼びます。「仮想ホスト」という用語は、場合によっては「ゲスト OS」を含むこともありますが、このセクションでは、それはエミュレートされたハードウェアコンポーネントのコレクションを指します。

物理的なマシンで OS をインストールする場合、通常は CD や DVD などのメディアから、または TFTP 経由でネットワークからロードされます。仮想マシンにはこれらの物理的なエンティティが存在しませんが、同様の環境をシミュレートする必要があります。仮想マシンに OS をインストールするには、通常 ISO 形式で OS の CD/DVD イメージを準備し、それを適切な場所に配置することで、ホスト OS がそれを仮想マシンにロードします。

仮想ホストを使用する前に、エミュレートされたハードウェアの仕様を決定する必要があります。例えば、メモリのサイズやストレージスペースのサイズ、ゲスト OS が使用できる CPU の数、または仮想ホストが持つべき Ethernet インターフェースの数などです。いくつかの属性は、最初から正しく決定する必要がありますが、後で変更することも可能です。例えば、ストレージスペースのサイズはいつでも変更できますが、OS がインストールされた後にストレージスペースをリサイズするには、ゲスト OS からハードドライブを再パーティションし、フォーマットする必要があります。これは、ゲスト OS がすぐに利用できるメモリのリサイズとは異なります。これらの問題は最初に考慮する必要があります。

ベースプラットフォームには、複数の仮想ホストインスタンスが実行可能です。実行中の仮想ホストに割り当てられたメモリの合計が、ベースプラットフォームが提供できる実際のメモリ量を超えると、一部の仮想ホストが起動できないか、メモリ不足の問題に遭遇する可能性があります。

ゲスト OS における仮想ホストのハードウェアはすべてベースプラットフォームによってエミュレートされている。したがって、エミュレートされたハードウェアの複雑さが軽減されると、ベースプラットフォームの負荷が軽減される。仮想ホストの選択された周辺機器は、ゲスト OS の要件を満たすだけで、過剰な割り当てをしないようにすれば、より良いパフォーマンスを得られる。

前述のとおり、ベースプラットフォームは仮想ホストのネットワーク構成を支援するものである。各仮想ホストは複数のイーサネットインターフェースを異なるブリッジに配置でき、各ブリッジは異なるサブネットに属する。各ブリッジの役割はベースプラットフォームによって制御される。ゲスト OS はそれぞれイーサネットインターフェースで異なる使用方法を持つ可能性がある。例えば、一方では DHCP クライアントを使用して IP アドレスを取得し、もう一方では DHCP サーバーを使用してクライアントに対して IP アドレスを配布する。この場合、同じサブネットに存在する 2 つの DHCP サーバーを避ける必要がある。ブリッジ A がブリッジ B によって NAT され、ブリッジ A に接続するホストからブリッジ B のホストへのネットワークトラフィックは、ブリッジ B の IP アドレスを IP ヘッダーの送信元 IP アドレスとして NAT される。ソフトウェアパッケージを仮想ホストに導入する前に、これらの制約を検討する必要がある。

ブリッジに接続するだけでなく、ネットワークインターフェースを設定する際には、仮想マシンのエミュレートされたイーサネットカードも指定する必要がある。また、ゲスト OS には、イーサネットを使用するための適切なドライバがインストールされている必要がある。

仮想ホストにおける高精度なクロックソースの提供は、ベースプラットフォームにとってストレスです。クロックタイミングソースは、システムがシステムイベントにどれだけ頻繁に反応するかに関連しています。ゲスト OS からの応答の遅延が見られる場合は、それがシステムクロックタイミングソースによるものである可能性があります。Windows システムは通常、低周波のクロックを使用するため、クロックソースの問題が発生しにくいです。Linux ベースのシステムでクロックソースの問題が発生した場合は、KVM クロックの使用に切り替えてください。

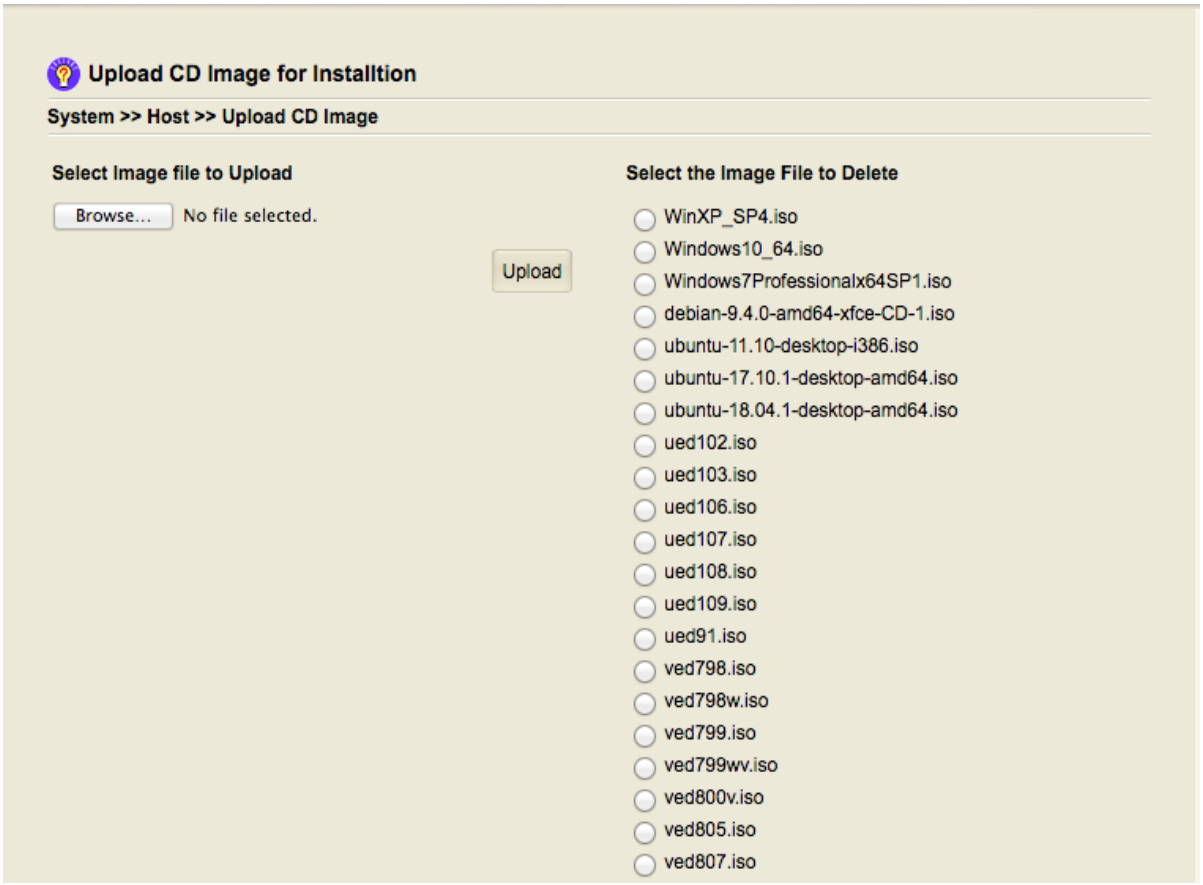
各仮想ホストに対して、VNC Viewer（または SPICE クライアント）を使用して仮想ホストのコンソールに接続できるように TCP ポートが割り当てられます。このネットワーク接続は、ベースプラットフォームのアクセスポリシーによっても管理されます。接続は、アクセスを許可されているネットワークから行う必要があります。

ウェブ管理インターフェースを使用するには、アクセスしてください。

http://ip_address:8082/apps/

「admin」というアカウントはデフォルトのパスワード「admin123」で構成されています。後でウェブ管理インターフェースを通じてパスワードを変更することができます。

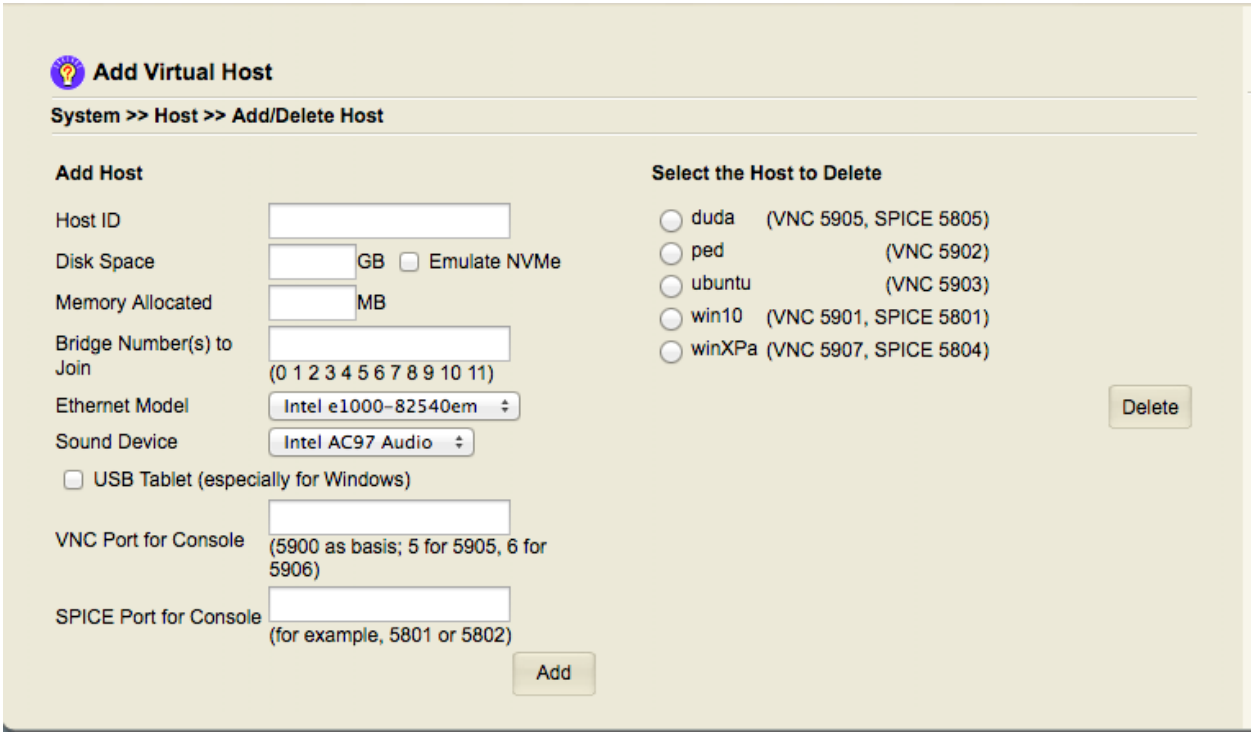
## *Upload CD Image*




挿絵 ***18: CD/DVD*** イメージのゲスト ***OS*** のアップロード

CD/DVD ドライブから OS を仮想ホストにインストールするために、OS のファイル（ISO 形式）を提供し、「System >> Host >> Upload CD Image」でアップロードする必要があります。各イメージのサイズは、ベースプラットフォームの物理メモリの半分を超えてはなりません。そうでない場合、「scp」またはその他の方法でイメージを宛先フォルダ（"/home/qemu/iso"）に配信する必要があります。また、「sshd」が「scp」を使用する場合に動作している必要があります。そして、WAN 側（弊社で「net」とラベル付けしたエリア）からアクセスする場合、TCP ポート 22 が開いている必要があります。

仮想ホストのインスタンスを作成する




挿絵 ***19:*** 仮想ホストのインスタンスを作成するための画面スナップショット

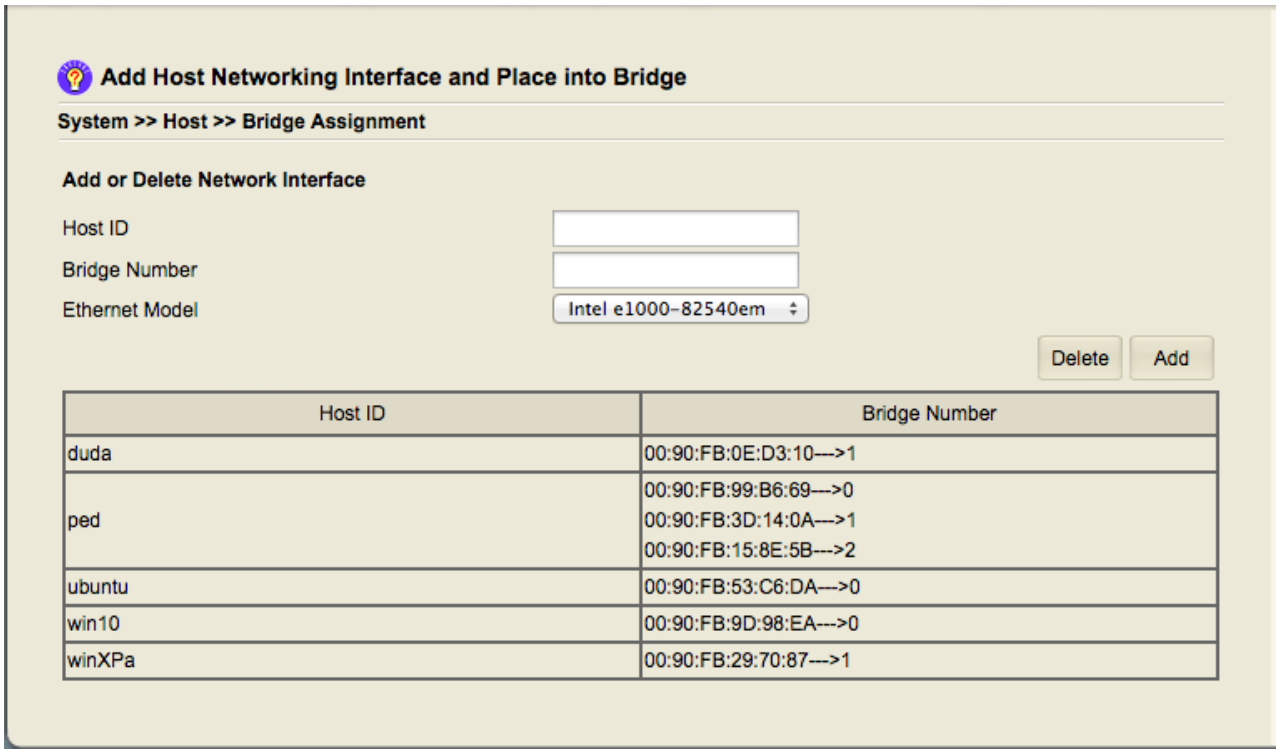
仮想ホストのインスタンスを作成するには、ディスクスペース、メモリ、ブリッジ（ブリッジを参加する）、イーサネットインターフェースモデル、および VNC 接続用のポートとは別に、「Host ID」を指定する必要があります。Host ID は、ベースプラットフォーム上で仮想ホストを識別するために使用され、ホスト名またはゲスト OS で使用される識別子とは関係ありません。

“USB Tablet”のチェックボックスは、VNC と接続先のホスト間でのマウスポインタの同期問題の解決に使用されます。ゲスト OS が Windows システムの場合、このチェックボックスをクリックする必要があります。デフォルトでは、PS2 キーボードとマウスが提供されます。

一部の SPICE クライアントは、「ゲスト OS」からの音声を「クライアント OS」（SPICE クライアントを実行している OS）に提供できます。「ゲスト OS」からの音声を使いいただく場合は、適切にオーディオデバイスを選択する必要があります。古いオペレーティングシステム（Windows XP のようなもの）では、AC97 と RealTek 8139 のみオーディオとして検出できます。しかし、新しいオペレーティングシステム（Windows 7 や Windows 10 のようなもの）では、AC97 は使用できません。Intel HD オーディオと ICH9 チップセットを使用する必要があります。ここではすべての可能性を列挙することはできず、すべての解決策を提供することはできません。インストールする OS の前に、適切なエミュレートされたハードウェアを評価する必要があります。

一度「Add」をクリックして完了したら、「Host ID」が表示されます。修正や調整するものが何もなければ、「System >> Host >> Host Management」に移動して、仮想ホストに CD/DVD イメージをインストールしてください。

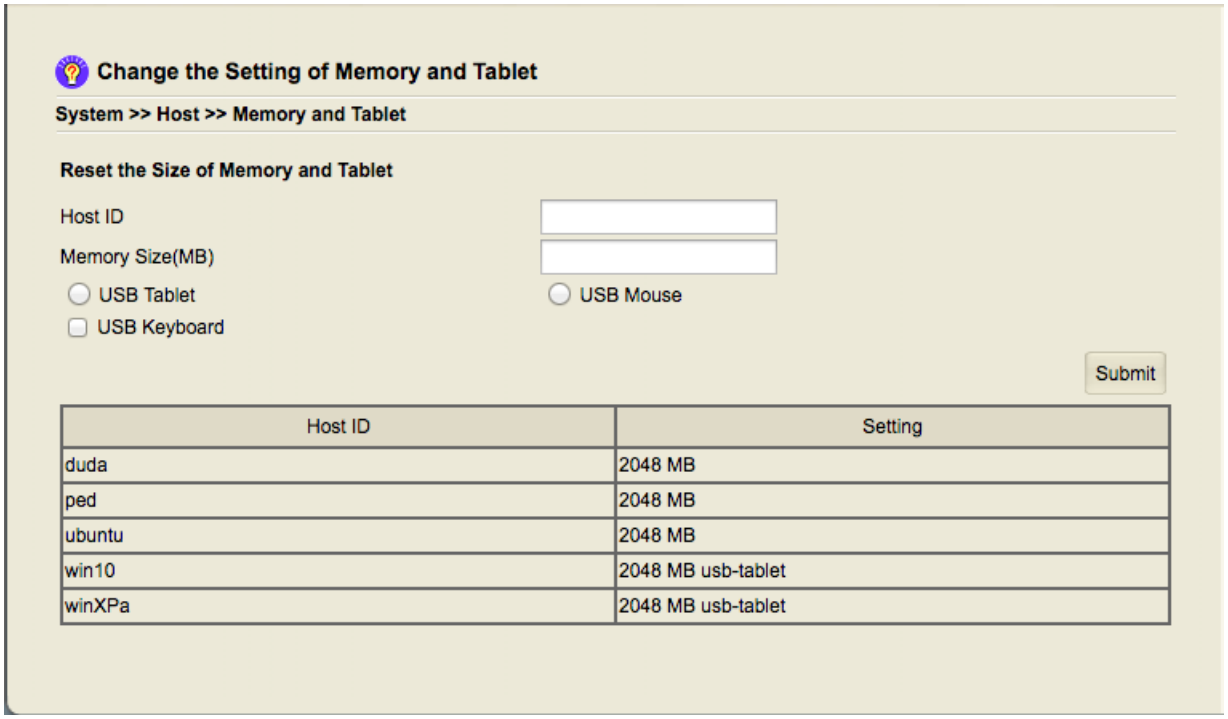
## *Bridge Assignment*




挿絵 ***20***：仮想ホストのブロージェクト割り当てとイーサネットタイプ

この管理ページでは、Ethernet インターフェース（その MAC アドレスで）と、関連付けられたブリッジ番号をリスト表示します。設定を変更する必要がある場合は、「Host ID」と「Bridge Number」を上記にタイプし、「Delete」ボタンを押してください。そして、「Host ID」、「Bridge Number」と Ethernet モデルを入力して「Add」ボタンを押してください。

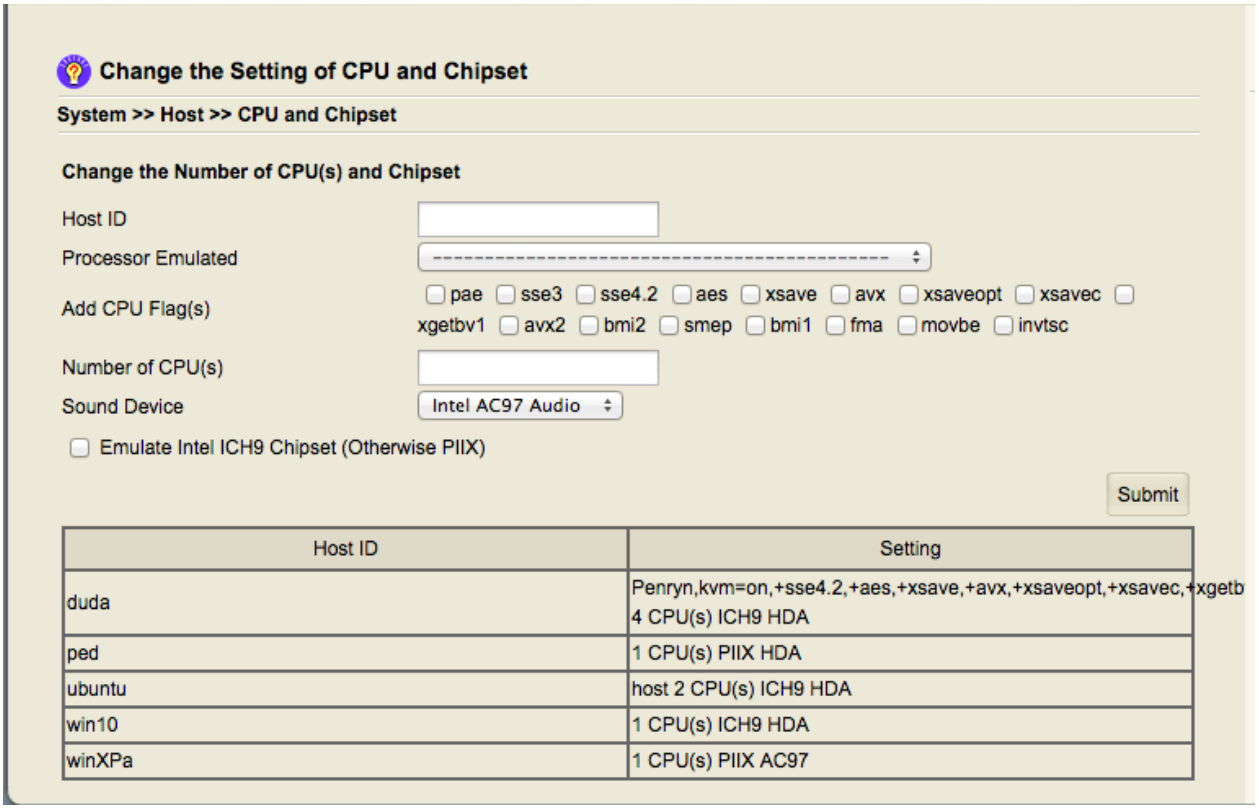
メモリとタブレットの設定を変更する




挿絵 ***21:*** メモリサイズ変更と ***USB*** タブレットの有効化の ***VM***

もしメモリのサイズを変更する必要がある場合は、ここでリセットできます。 Guest OS と Client OS の間で VNC ビューアを使用する際に、「ゲスト OS」と「クライアント OS」の間でマウスポインタの同期の問題が見つかった場合、USB タブレットを使用できます。 弊社では、PS2 マウスとキーボードをデフォルトで提供しています。 「ゲスト OS」がこれらをサポートしている場合は、他のものを選択する必要はありません。 ただし、一部のオペレーティングシステム（たとえば、Mac OS X “Mojave”）は PS マウスとキーボードおよび USB タブレットをサポートしていない場合があります。 その場合は、USB マウスとキーボードを選択し、SPICE クライアント（virt-viewer や remote-viewer のようなもの）を使用することをお勧めします。

## *CPU and Chipset*

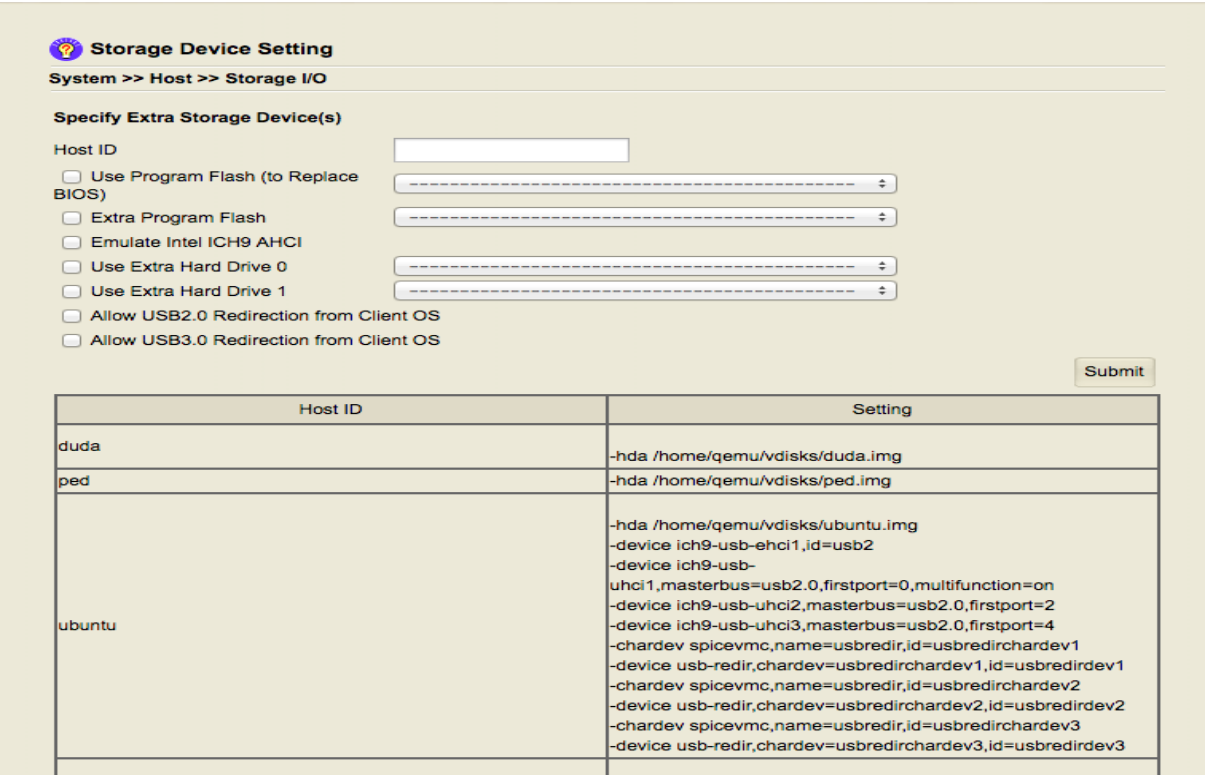



挿絵 ***22: CPU*** と チップセット の 変更

デフォルトで Intel PIIX チップセットが仮想ホストのインスタンスを作成する際に使用されます。 Intel PIIX チップセットは主に PCI-to-ISA、PCI IDE 関数、AC97 のようなオーディオデバイスに使用されます。 Intel ICH9 チップセットは主に SATA (Serial ATA) に使用されます。 IDE ハードドライブをエミュレートする場合は PIIX を使用し、SATA の場合は ICH9 を使用します。 一部の古いシステムでは SATA ドライヴをサポートしていない場合、PIIX を使用する必要があります。

通常、弊社では “Base OS” が使用している CPU モデルと同じ CPU モデルを “Guest OS” のエミュレーションで使用します。もし、一部のオペレーティングシステムが特定の CPU モデルや CPU フラグを使用する必要がある場合は、この画面から選択することができます。

# ストレージデバイス設定




挿絵 23: 追加ストレージデバイス設定

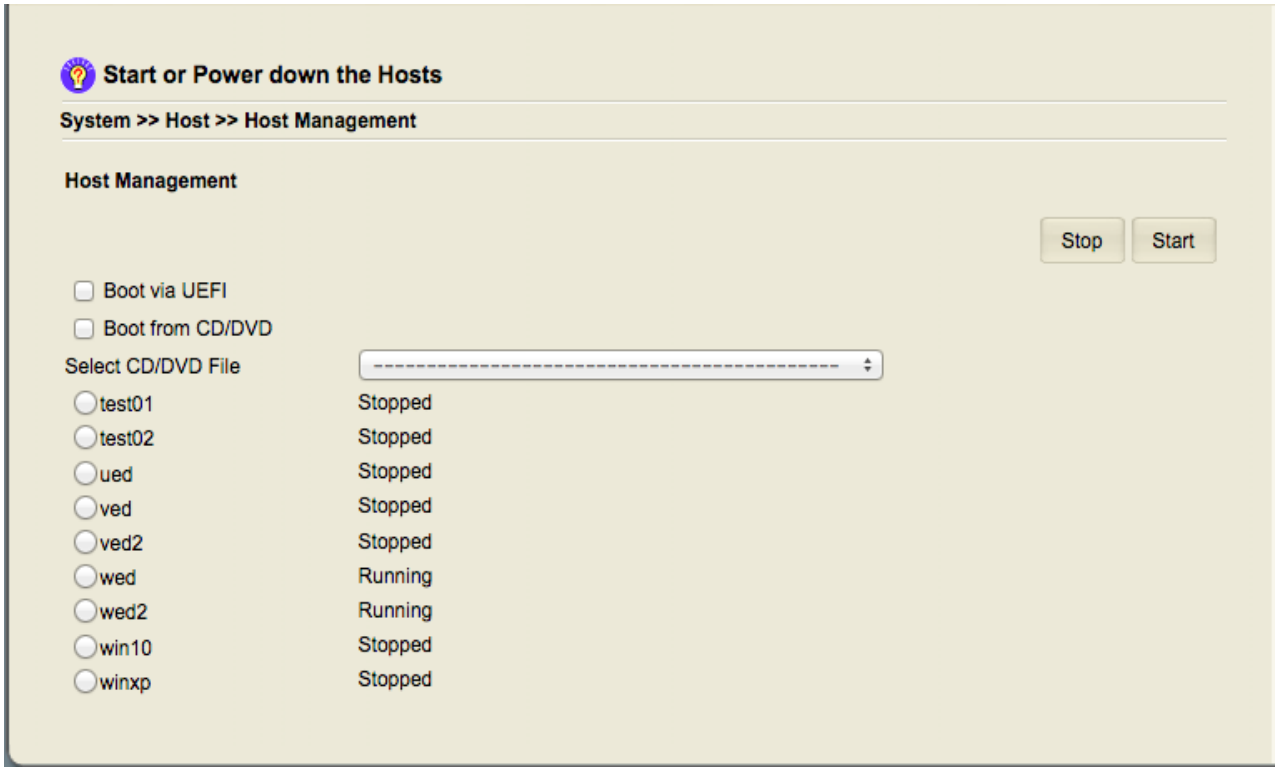
この画面は標準配布には含まれない場合があります。これは、カスタマイズされた BIOS や特定のアプリケーション用の追加ストレージデバイスをロードするための「プログラムフラッシュ」を提供するために使用されます。これらの画像は、「/home/qemu/extra」に配置することで、選択リストに表示されます。

“ベース OS”は通常、ゲスト OS に対して単一のディスクのみをストレージデバイスとして提供します。もし追加のストレージデバイスをプロビジョニングしたい場合は、それらは IDE バスを使用する場合は “hdb” と “hdd” に、ICH9 ACHI ( SATA ) を使用する場合は “仮想ホスト” が最初に持つディスクの前にバス ID が付いたディスクと共に配置されます。ディスクイメージは “qcow2” 形式で提供する必要があります。他の Linux システムで他の形式のディスクイメージを変換するために、 “qemu-img” ツールを使用することができます。

USB リダイレクトは、「ゲスト OS」と「クライアント OS」の間で行われ、SPICE クライアントが「クライアント OS」で実行されている間に発生します。これは「クライアント OS」で USB リダイレクトを自由に利用することを許可するものではありません。「ゲスト OS」側では、ICH9 USB コントローラー（EHCI および UHCI）によって提供される USB2.0 デバイスまたは NEC チップセットによって提供される USB3.0 デバイスを検出する必要があります。「クライアント OS」側の USB デバイスは、USB リダイレクト中に「クライアント OS」によって使用することはできません。 一部の SPICE クライアントでは、USB リダイレクトのために追加のソフトウェアパッケージのインストールを求められます（たとえば、「remote-viewer」は Windows 環境で USB リダイレクトを機能させるために「usbDK」をインストールする必要があります）。

ホスト管理画面からカスタム BIOS（または UEFI）イメージを提供した場合、ブートオプションを指定することなく、そのまま起動できます。

## *Host Management*




挿絵 ***24:*** 仮想マシンのホスト管理

初めて仮想ホストを起動させる場合、OS を仮想ホストにインストールするために CD/DVD イメージから起動する必要があります。 “Boot from CD/DVD” のチェックボックスをクリックし、CD/DVD ファイルを選択し、対応する仮想ホストを選択します。その後、「Start」ボタンを押します。 仮想ホストが正常に起動された場合、「Running」が対応する「Host ID」の隣に表示されます。　場合によっては、CD/DVD イメージが起動機能ではなく、OS インストール後のソフトウェアパッケージがロードされていることがあります。そのような場合、CD/DVD イメージを選択する際に、「Boot from CD/DVD」を選択する必要はありません。

VNC ビューアは、インストールプロセス中にコンソールにアクセスするために使用できます。それはゲスト OS がインストール手順を整えることに依存します。CD/DVD からのブート処理が完了した後、仮想ホストを停止して再度起動しても構いません。VNC ビューア（または SPICE クライアント）のベースプラットフォームの IP アドレス(エ)と TCP ポートを使用して仮想マシンのコンソールにアクセスします。仮想ホストの IP アドレスではなく、です。

以下の情報は、Azblink マニュアルからのスクリーンショットです。“VNC ビューア”を使用して、Windows 仮想ホストのコンソールにアクセスする方法を示しています。

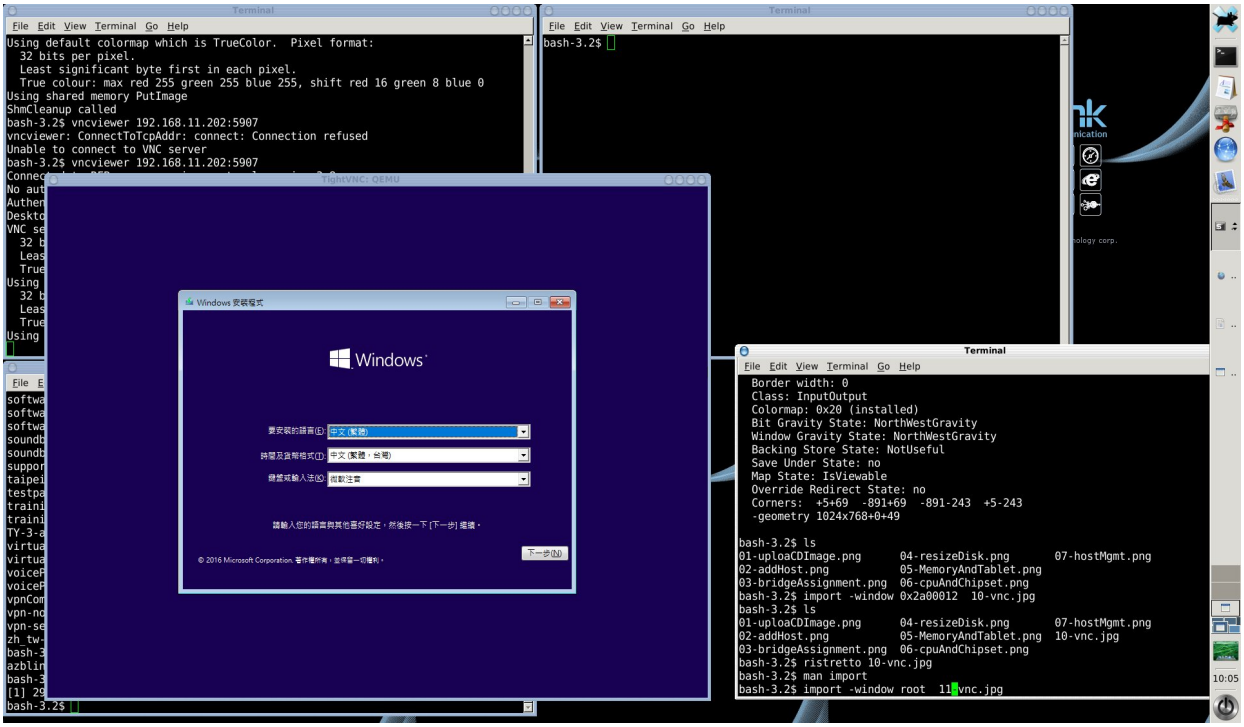



イラスト ***25: VNC*** を使用するための画面スナップショット

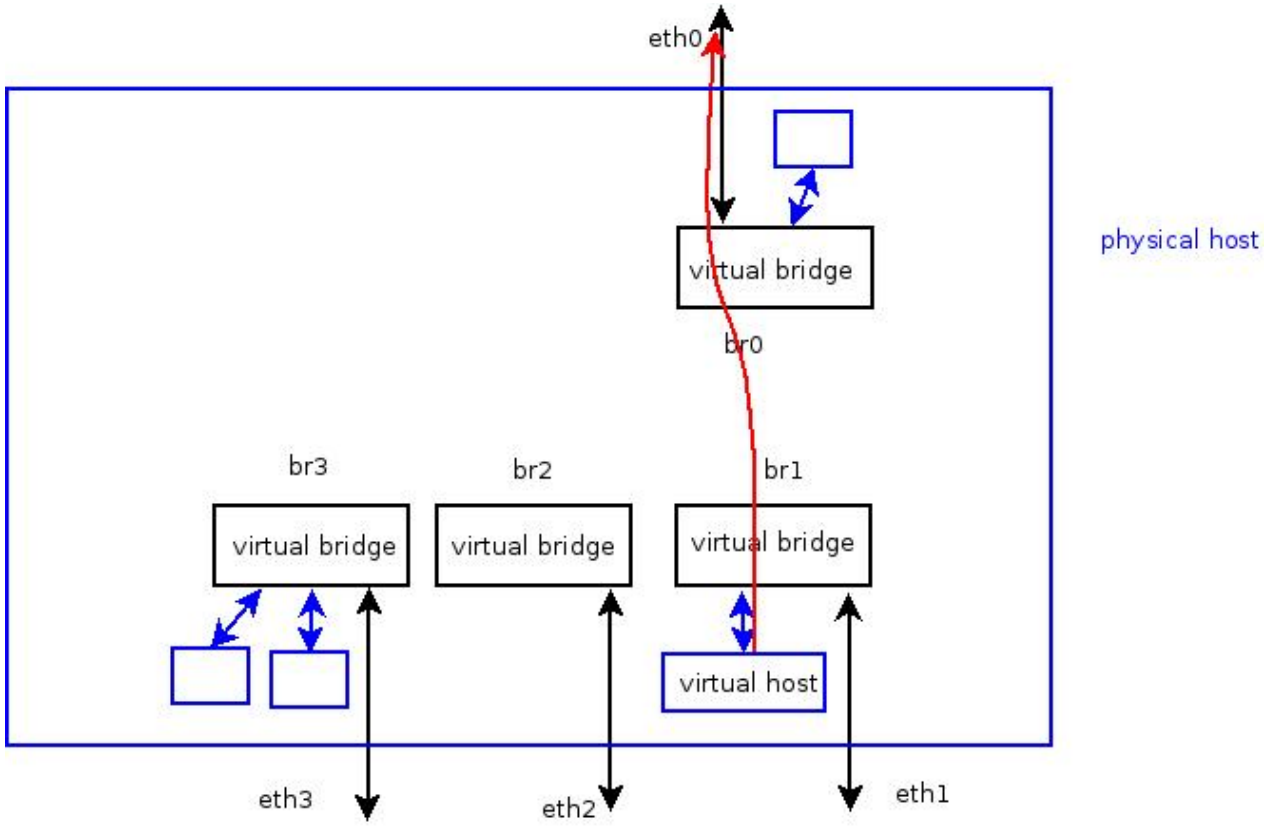
“UEFI”でシステムを起動する必要がある場合、必ず「Boot via UEFI」のチェックボックスもご記入ください。UEFI ファームウェアは 64 ビットシステム向けですので、対応するメディア上の UEFI 実行可能ファイルも 64 ビットバイナリである必要があります。

SPICE クライアントを使用して仮想マシンのコンソールにアクセスすることも可能です。SPICE クライアントは VNC クライアントほどスムーズには動作しませんが、オーディオをクライアントサイドに送信することができます。任意のベースプラットフォームの IP アドレスを SPICE または VNC クライアントから使用して仮想ホストにアクセスできます。仮想ホストが Microsoft Windows でロードされている場合、Microsoft の Remote Desktop Service を使用する必要があります。Microsoft の Remote Desktop を使用するには、仮想ホストの IP アドレスを直接使用する必要があります。

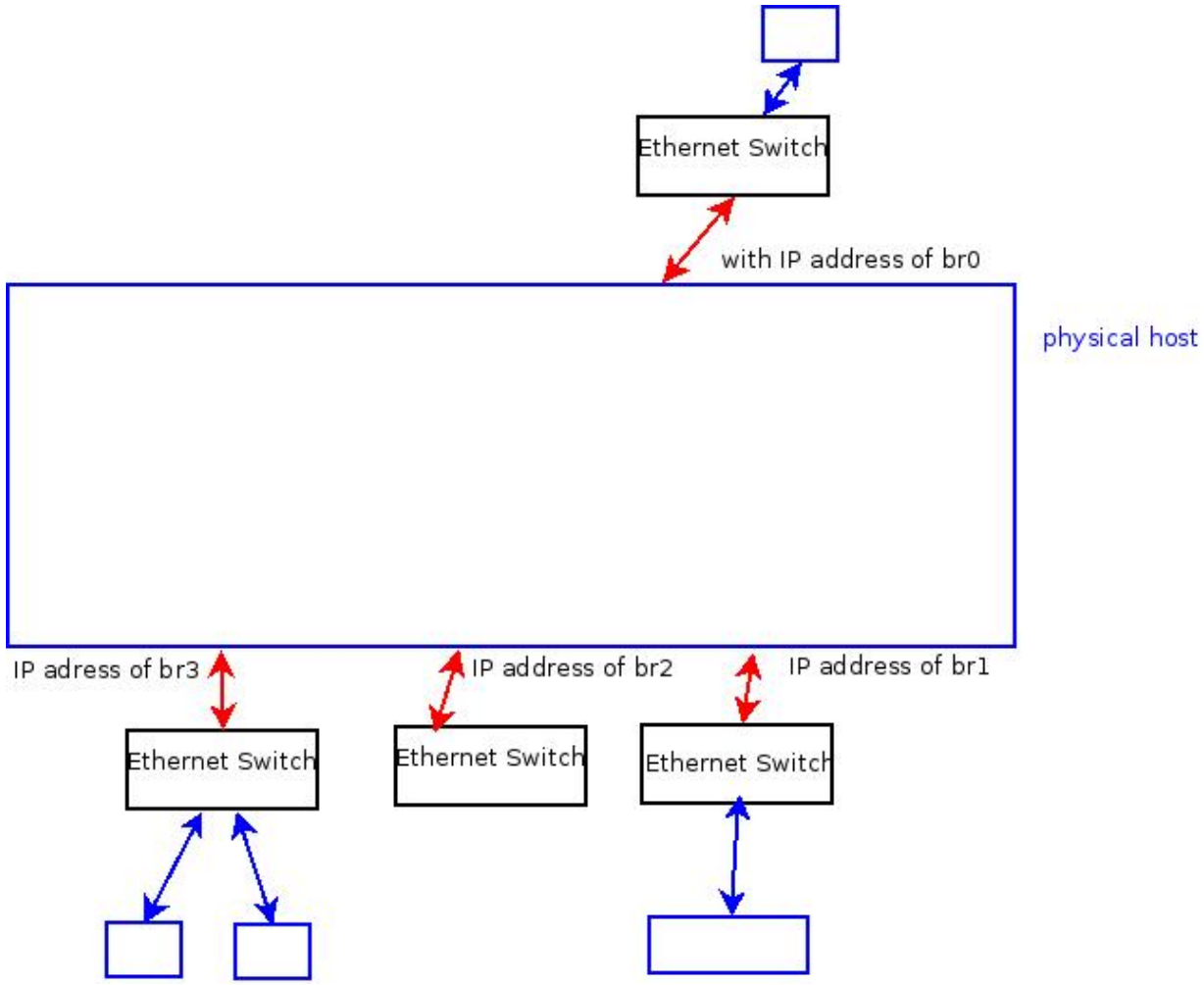
# 第 3 章 境界制御

ベースプラットフォームによる入境管理の運用は「オンブリッジ方式」です。「オンブリッジ方式」という用語は、ベースプラットフォームの物理的なイーサネットインターフェースではなく、ブリッジデバイスの境界線に従ってゾーン分割が行われることを意味します。ベースプラットフォームの物理的なイーサネットインターフェースは、ブリッジがプラットフォーム外のネットワークを接続するためにのみ使用されます。

これまでの章では、仮想ホストの Ethernet インターフェース(s)ができることは、それらの Ethernet インターフェース(s)が接続できる仮想ブリッジを決定することだけでした。



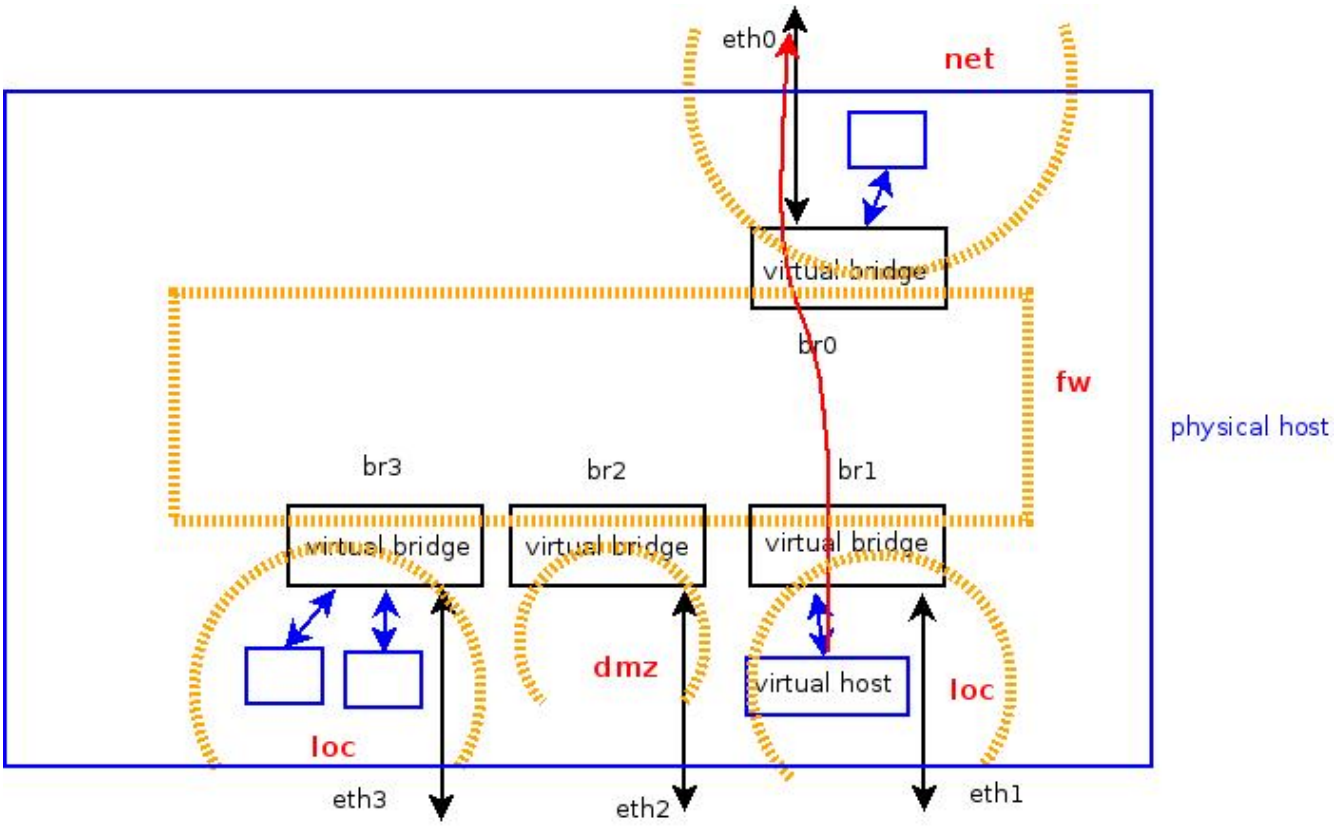

挿絵 ***26:*** 仮想ブリッジを持つベースプラットフォーム




挿絵 ***27:*** 物理的なイーサネットスイッチを使用した等価モデル

上記２つのイラストは、ベースプラットフォームの仮想ブリッジを正しく表示する方法を説明するために使用されています。仮想ブリッジは、ベースプラットフォームの外にある物理的なイーサネットスイッチと見なされ、ベースプラットフォームは、仮想ブリッジに設定された元の IP アドレスを持つ追加のイーサネットインターフェースを物理的なイーサネットスイッチに接続します。

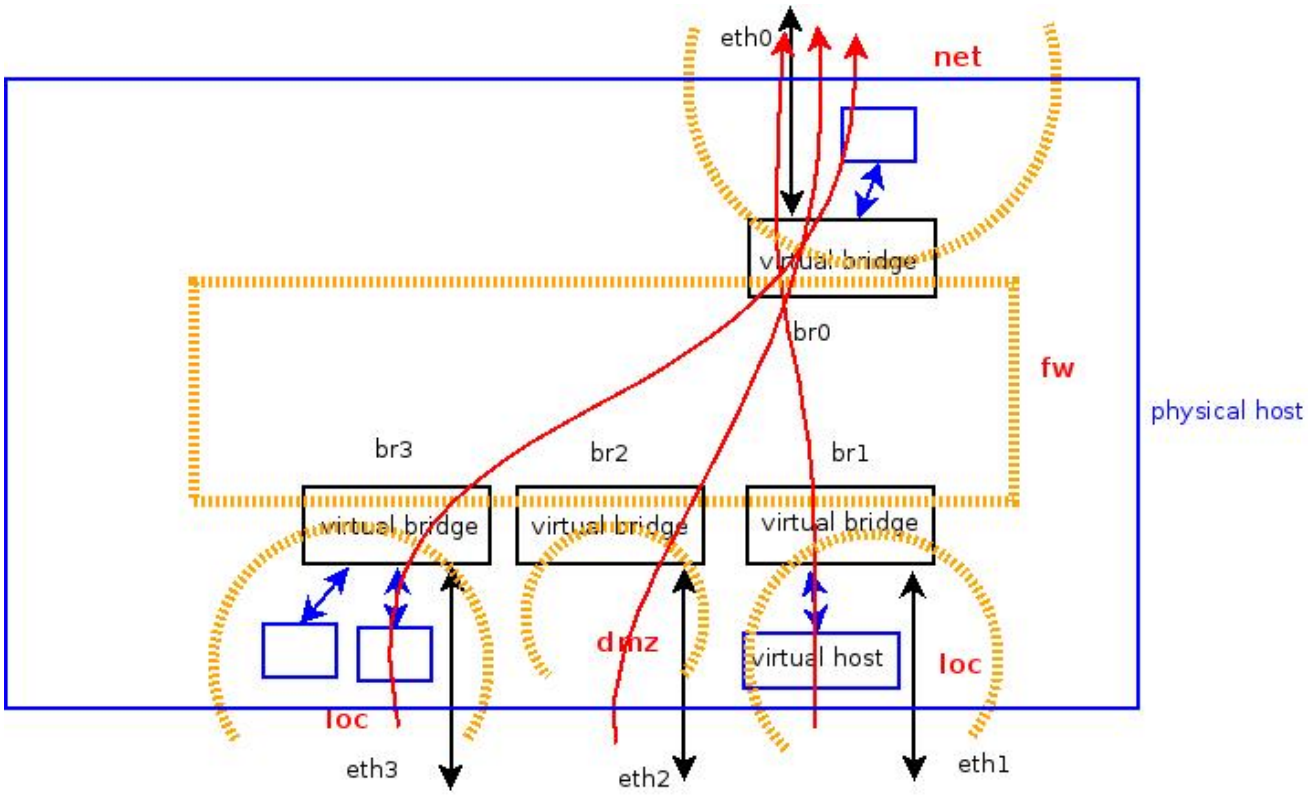
デフォルトで、基盤プラットフォームは以下の構成で設定されています。「br0」の境界に接続するネットワークは「net」、「br2」の境界に接続するネットワークは「dmz」、そして「br1」、「br3」、「br4」～「br10」、「br11」に接続するネットワークは「loc」とラベル付けされています。




挿絵 ***28:*** 基本プラットフォームにおけるゾーン分割

そして、仮想ホストを作成し、そのいずれかのイーサネットインターフェースを仮想ブリッジに配置すると、そのイーサネットインターフェースは、そのインターフェースが属するゾーンに関連付けられたルールによって制御されます。したがって、そのゾーンの定義と操作の機能について理解しておくことが必要です。

“loc”または“dmz”から開始されたネットワークトラフィックは、“net”内のホストへのアクセスを許可されます。




挿絵 ***29:*** 目的地が「***net***」のトラフィック

「loc」または「dmz」から「net」へのネットワークトラフィックは、元の IP ヘッダーの送信元 IP アドレスを「br0」で伝送された IP アドレスに置き換えることで NAT（ネットワークアドレス変換）処理が行われ、他方でネットワークトラフィックは、置き換えられた IP アドレスと送信元ポートに基づいてベースプラットフォームから対応するホスト「loc」または「dmz」へ応答します。

「net」ゾーンからのトラフィックは、デフォルトでは「loc」または「dmz」へのアクセスが禁止されています。

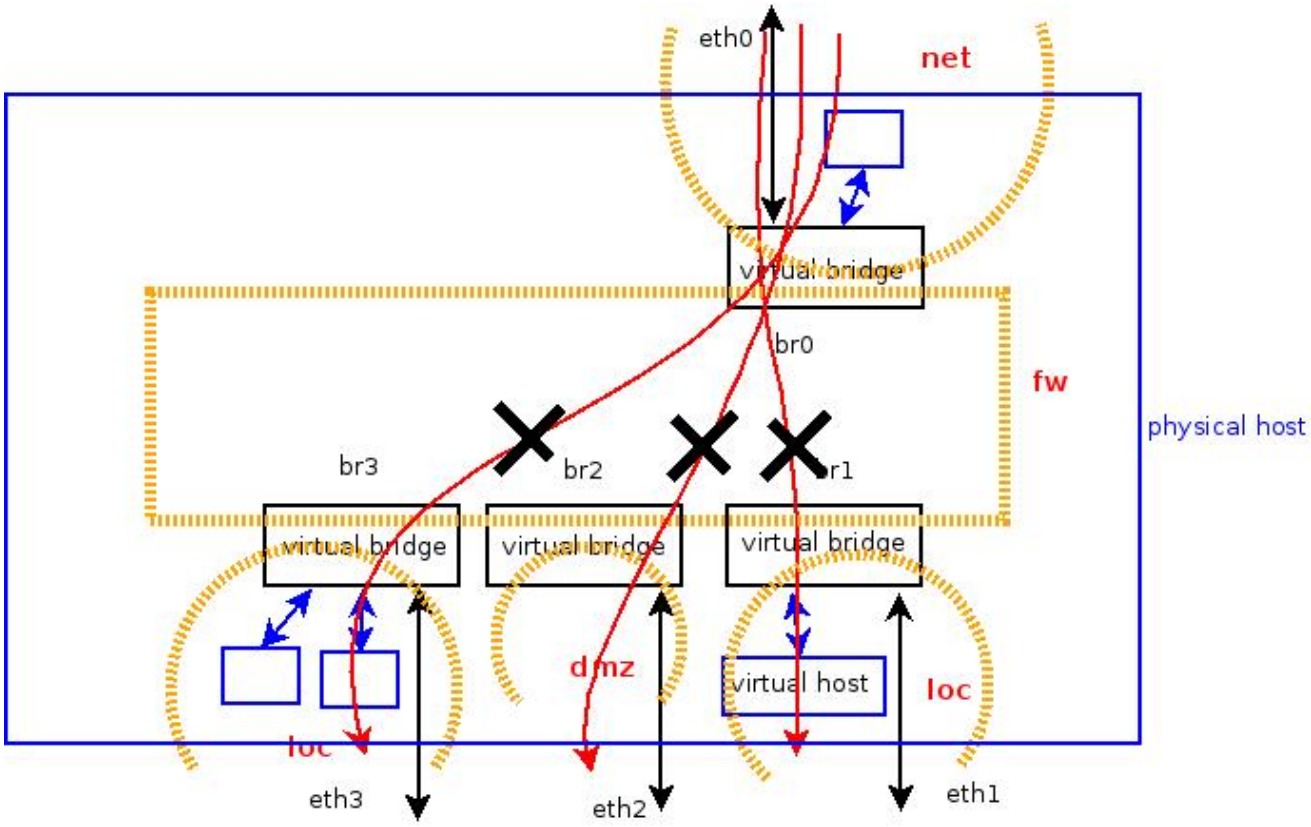
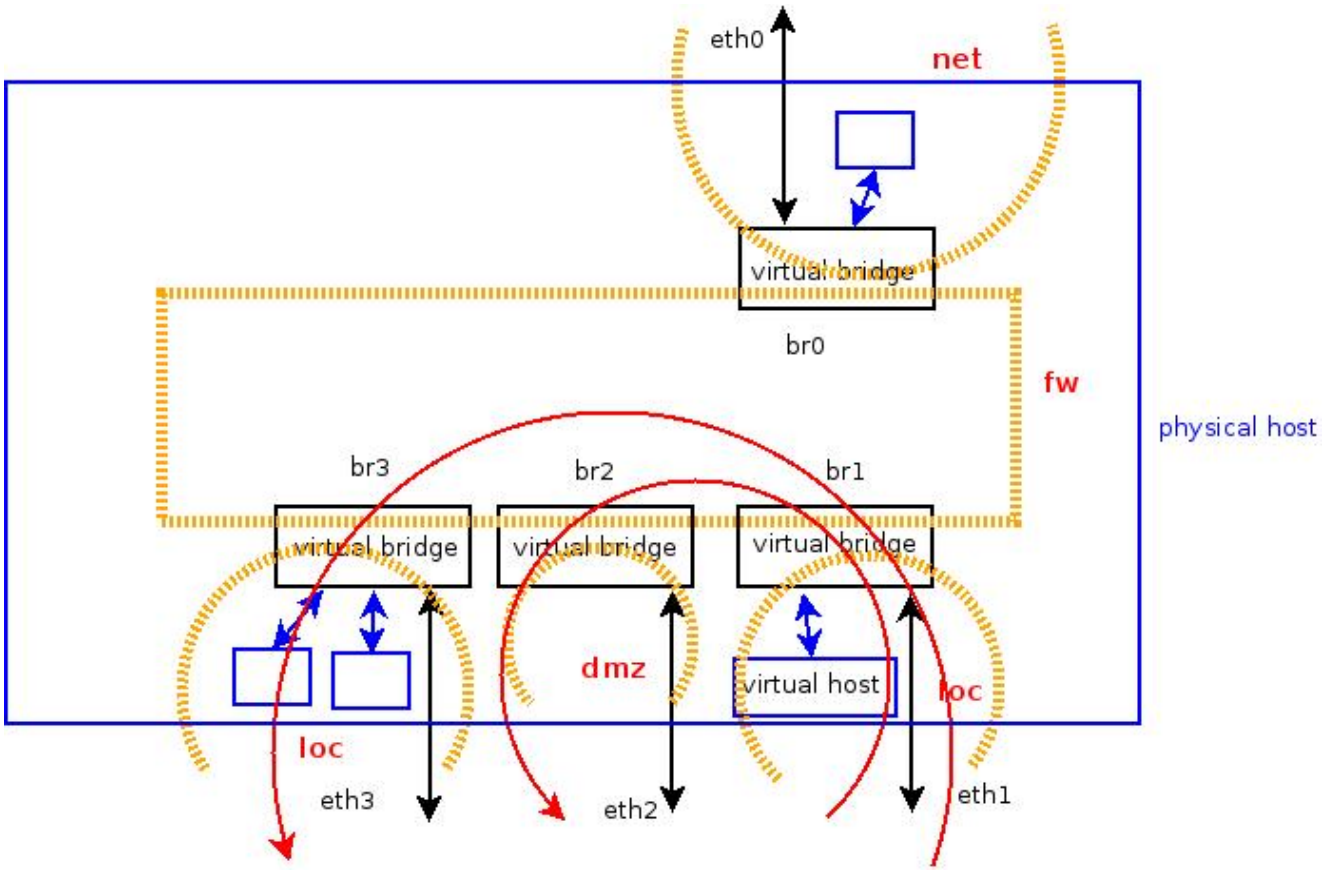



イラスト ***30: "net"*** から発生したトラフィックは ***"loc"*** または ***"dmz"*** へのアクセスが禁止されています。

再度、この設定は例外ルールを追加することで変更できます。"net"ゾーンのホストは"loc"ゾーンまたは"dmz"ゾーンのホストにアクセスできません。 通常、インターネットに接続する"net"ゾーンを"WAN"（wide-area network）とラベル付けします。"net"ゾーンのホストから"dmz"ゾーンまたは"loc"ゾーンのホストに到達するために、ポートフォワーディングという例外ルールが必要です。 ポートフォワーディングは、基地プラットフォームに到着したネットワークトラフィックを選択して、"dmz"または"loc"ゾーンのホストに転送する操作です。 通常，"dmz"は"net"から接続を処理し，"loc"はローカルにアクセスできるホストのために使用されます。

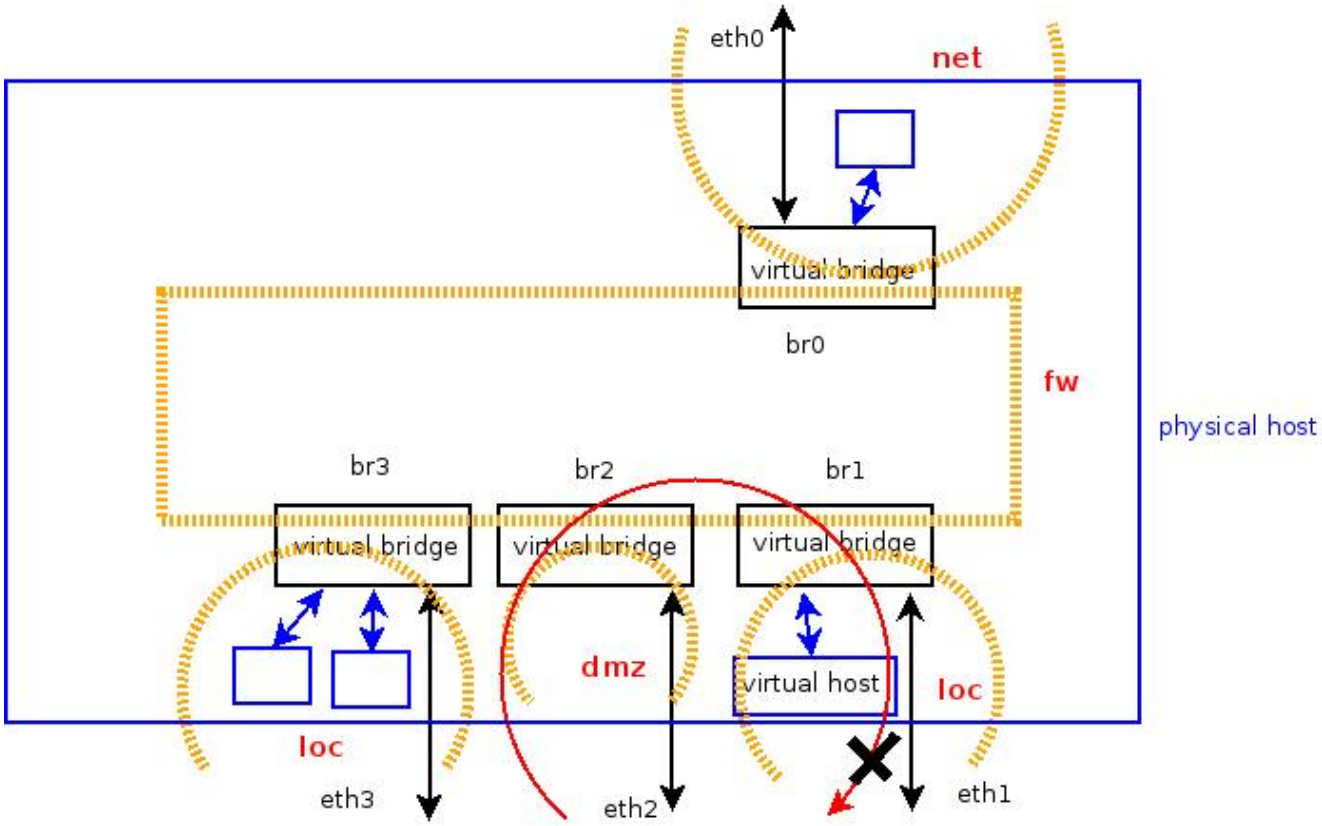
ネットワークトラフィックがゾーン“loc”から発信された場合、ゾーン“loc”と“dmz”のホストへのアクセスが許可されます。




挿絵 ***31:*** 交通は「***loc***」ゾーンから発生した。

「loc」のホストは、任意のゾーンのホストにアクセスできます。“loc” からゾーン “net” へのネットワークトラフィックは NAT の下で動作しますが、“loc” から “dmz” などの “loc” サブネットへのトラフィックでは NAT 動作は行われません。“異なる IP サブネットを跨ぐ” ネットワークトラフィックは、ベースプラットフォーム上で “routing” を行う必要があります。ネットワークパケットがベースプラットフォームのいずれかのブリッジに到達すると、その操作はベースプラットフォームによって自動的に処理されます。しかし、他のサブネット宛のネットワークパケットを送信するホストの場合、そのサブネットへのデフォルトゲートウェイを設定するか、またはローカルサブネット上のベースプラットフォームの IP アドレスをデフォルトゲートウェイとして使用する必要があります。

“dmz”ゾーンからのトラフィックは“loc”のホストへのアクセスが禁止されています。




挿絵 ***32: “dmz”*** ゾーンからのトラフィックは ***“loc”***ゾーンへのアクセスが禁止されています。

“dmz”のホストは“loc”のホストへのアクセスが禁止されていますが、“net”のホストへのアクセスは可能です。この性質上、オフィスを訪れるゲスト用の Wifi AP をこのゾーンに配置するか、インターネットからの接続を処理するためのホストに例外的なポートフォワーディングルールを追加することが一般的です。

以下の定義済みのルールを以下のようにまとめます。

loc → net (OK)
loc → dmz (OK)
loc → loc (OK )
dmz → net (OK)
dmz → loc ( Forbidden )
net → loc (Forbidden)
net → dmz (Forbidden)

ベースプラットフォーム自体、仮想ホストを除くものは、ゾーン“fw”としてラベル付けされます。ゾーン“fw”に関連付けられた定義済みのルールは以下の通りです。

fw → net (OK)
fw → loc (OK)
fw → dmz (OK)
net → fw (Forbidden)
loc → fw (OK)
dmz → fw (Forbidden)

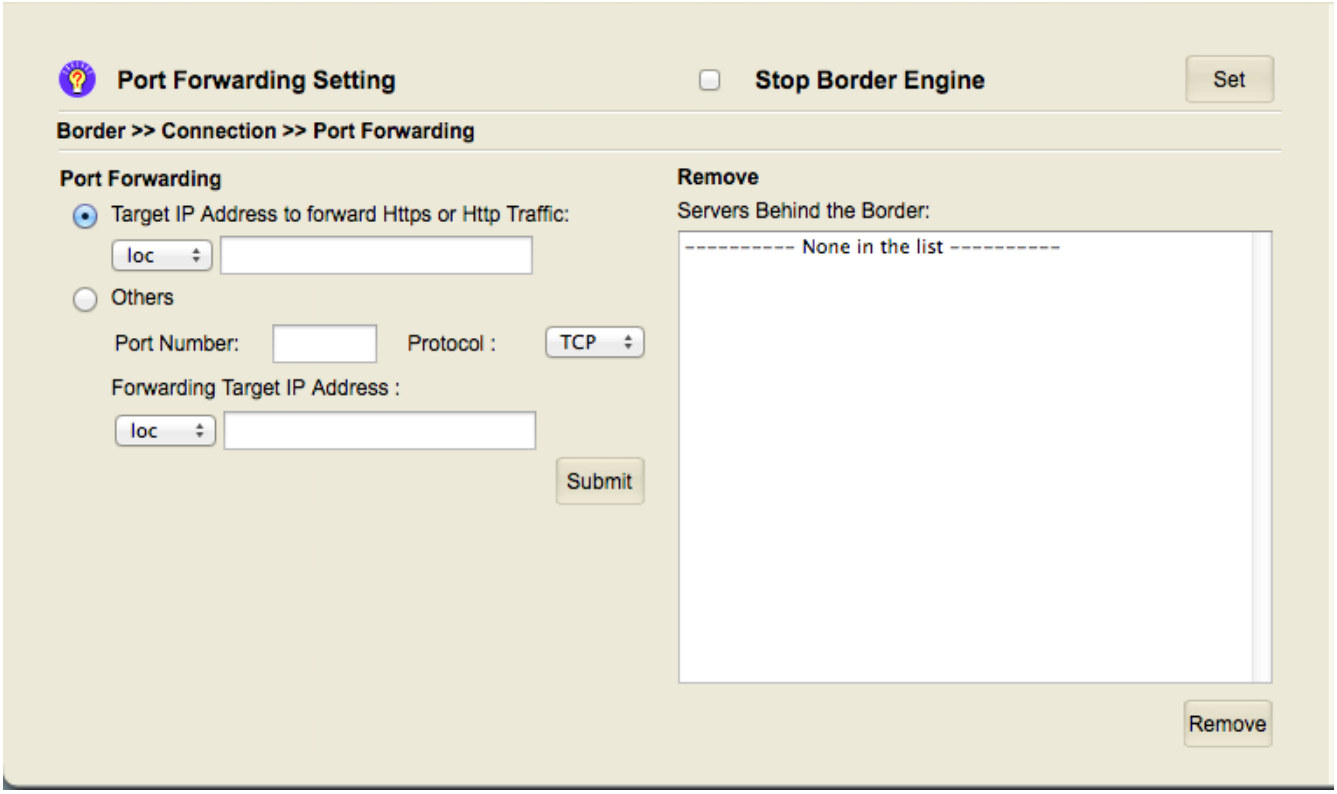
それらの定義済みのルールは、ウェブ管理インターフェースに表示されません。ただし、例外ルールを追加したり、ゾーンのコンポーネントを変更したりすることができます。別のゾーン「road」があり、それは VPN や他のベースプラットフォームで使用される内部インターフェースに関連付けられています。その項目は、次のセクションで機能について言及した後で紹介されます。

## *Port Forwarding*

ポートフォワーディングは NAT（Network Address Translation）に伴ってきます。 私たちが以前に述べたように、ゾーン“dmz”または“loc”からゾーン“net”へのトラフィックは、ゾーン“dmz”または“loc”の元のホストの IP アドレスと新しい TCP または UDP ポートを使用して、ゾーン“dmz”または“loc”からゾーン“net”へのトラフィックは、ゾーン“dmz”または“loc”の元のホストの IP アドレスと新しい TCP または UDP ポートを使用して置き換えられ、応答トラフィックは、このソース IP アドレスとポートを宛先として使用し、基盤プラットフォームは応答を元のホストに“dmz”または“loc”から転送します。

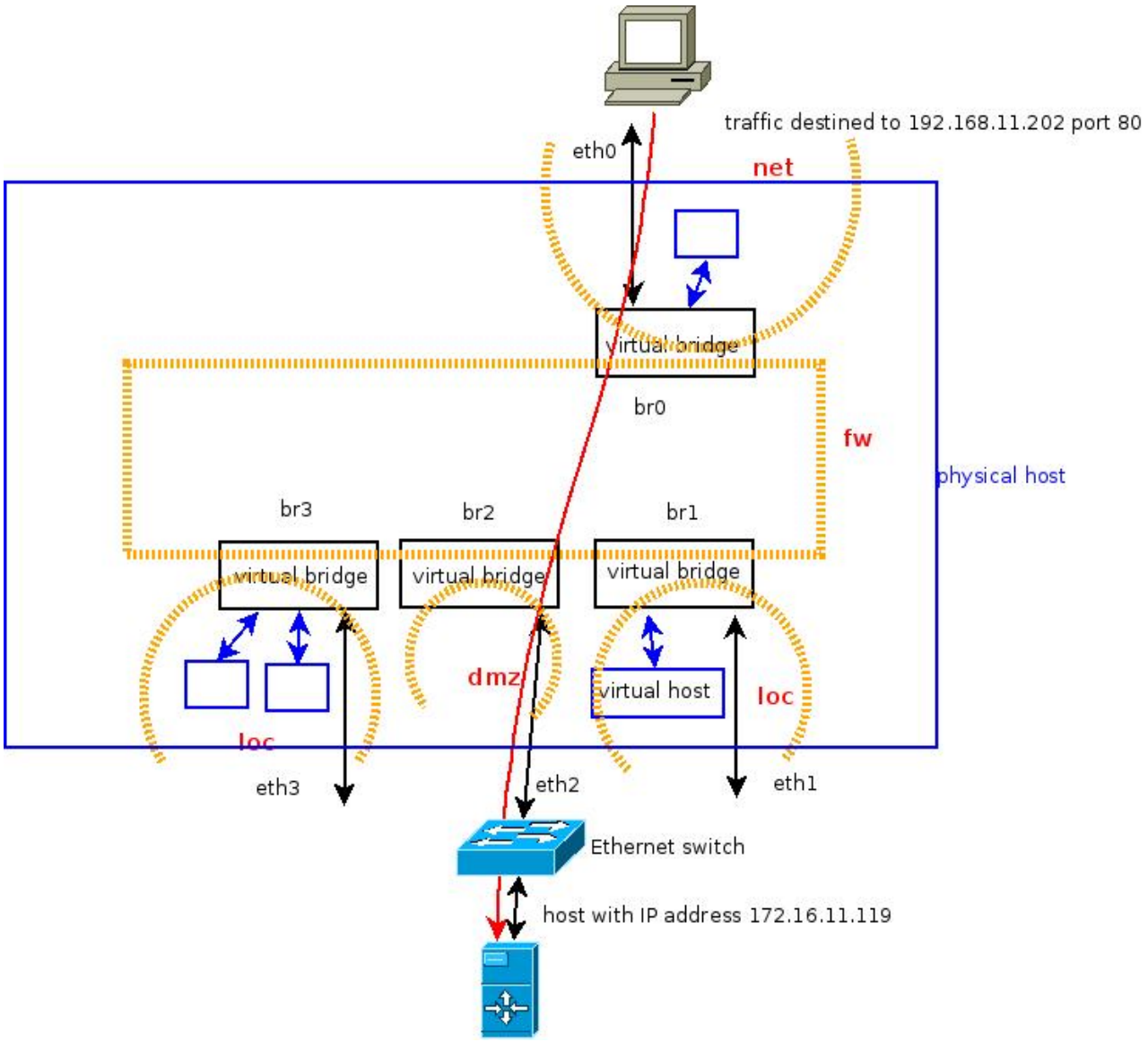
ただし、「net」ゾーンから基となるプラットフォームへ到着したトラフィックは、基となるプラットフォームが特定のデーモンで対応する TCP/UDP ポートを開放しておらず、あるいはこの種のトラフィックと一致するルールを持っており、他のホストに転送しない限り、単純にドロップされます。「ポートフォワーディング」とは、基となるプラットフォーム宛の、関連するポートと一致するトラフィックを、ゾーン“dmz”または“loc”にある他のホストに指定する TCP または UDP ポートを確立するプロセスです。

ポート転送ルールは、「`Border >> Connection >> Port Forwarding`」で指定できます。



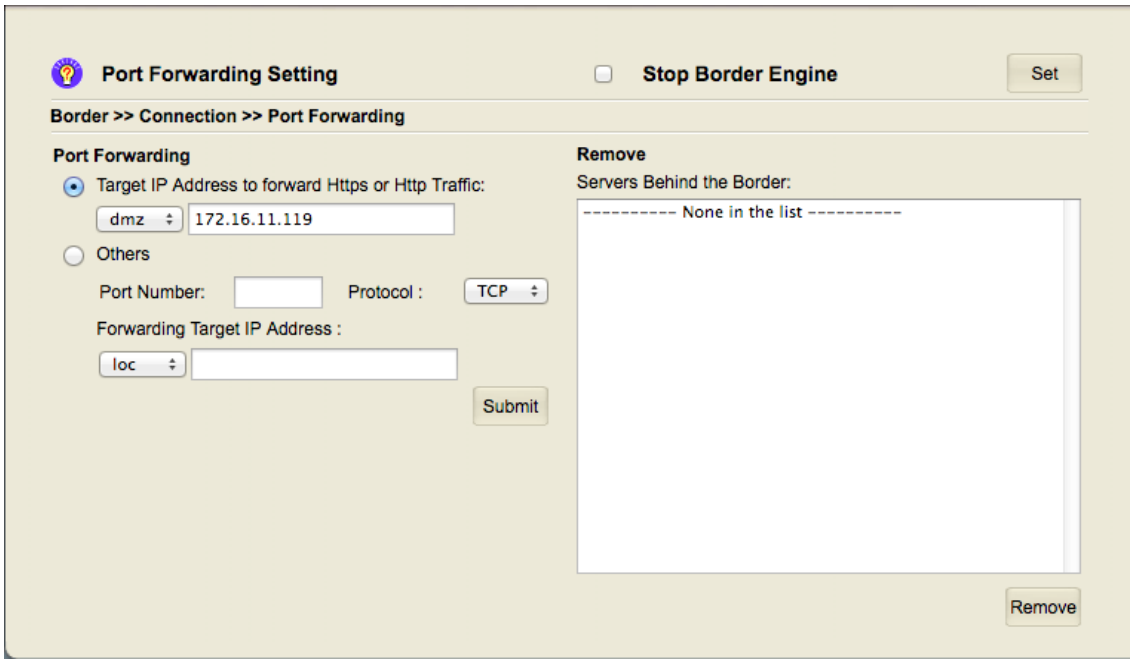
挿絵 ***33:*** ポート転送のスクリーンショット

以下の図は例です。ベースプラットフォームは IP アドレス“192.168.11.202”で“br0”を使用し、ゾーン“dmz”にあるホストが IP アドレス“172.16.11.119”で“br0”を使用し、元の宛先“192.168.11.202”への TCP ポート 80（http トラフィック）のトラフィックを受信します。




挿絵 ***34:*** ポートフォワーディングの例

http および https トラフィック を 転送 する ルール を 入力 する ため、"dmz" を選択し、以下のスクリーンショットに示す IP アドレス "172.16.119" を入力してください。




挿絵 ***35*** : ***HTTP*** ポートフォワーディングの例

そして「Submit」ボタンを押すと、右側に TCP ポート 80 とポート 443 に関連付けられたトラフィックが「dmz」ゾーンの 172.16.11.119 にフォワードされると表示されます。

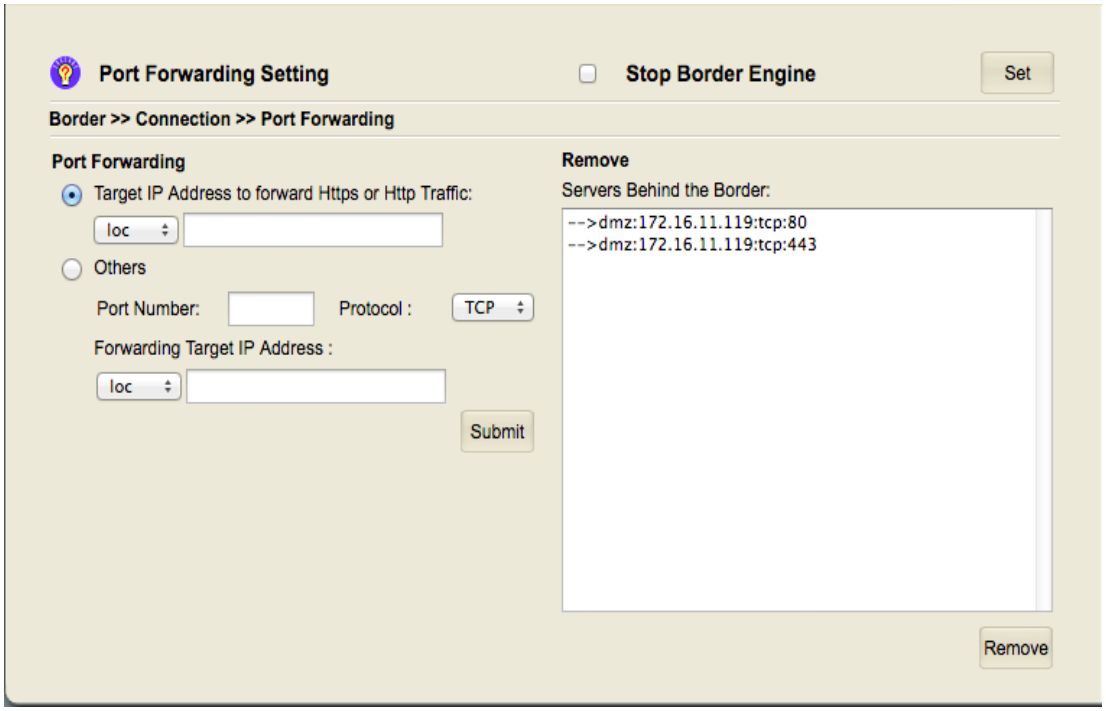
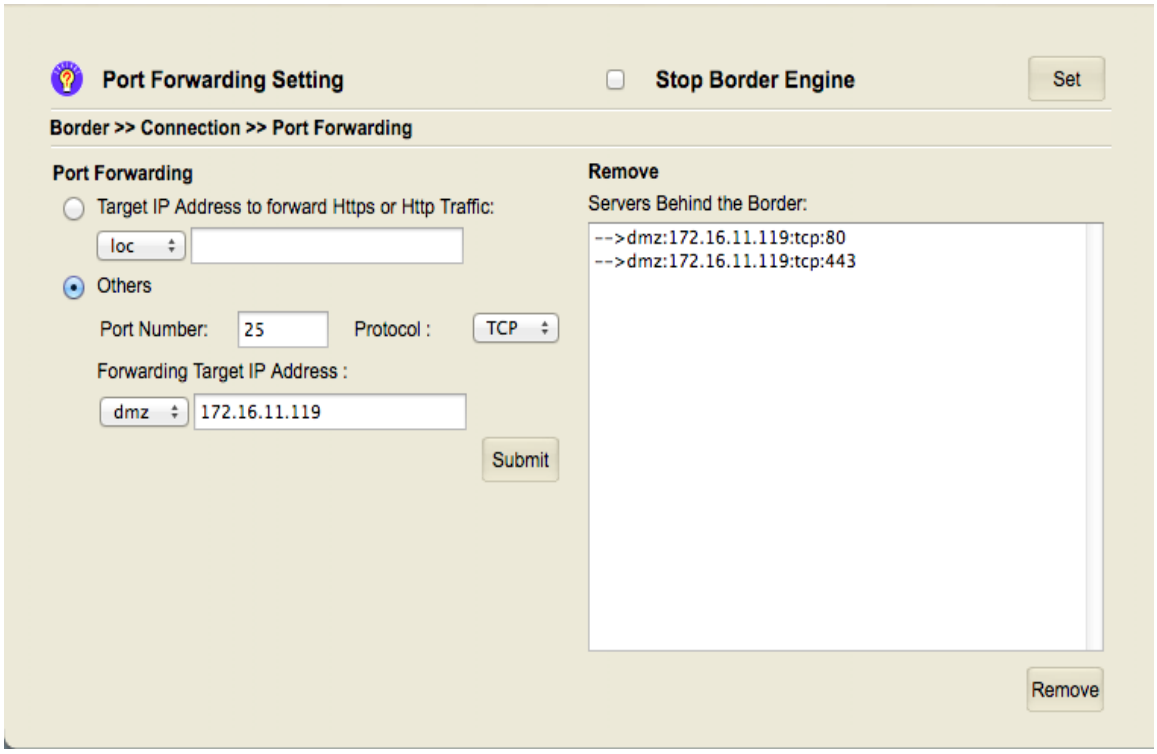



イラスト ***36: HTTP*** ポート転送の設定画面のスクリーンショット

ルールを有効にするには、ボーダーエンジンを停止し、再度起動する必要があります。それは、トップのチェックボックスをチェックし、「Set」ボタンを押した後、チェックボックスを解除し、「Set」ボタンを再度押すことで行えます。 どのルール変更を行う場合でも、ボーダーエンジンの再起動が必要です。




挿絵 ***37: SMTP*** のポート転送の例

同様に、TCP ポート 25 は SMTP で使用されます。SMTP のトラフィックを「172.16.11.119」宛に転送するには、上記のように入力し、「Submit」ボタンを押してください。右側の表示ボックスには、TCP ポート 25 に関連付けられたトラフィックが「dmz」ゾーンのホスト「172.16.11.119」宛に転送されることが表示されます。ポート転送を使用する場合、転送されたトラフィックを受信するホストのデフォルトゲートウェイは、ベースプラットフォームのインターフェース（この場合は「br1」の IP アドレス）に設定する必要があります。そうしないと、返信パケットが送信者に戻りません。

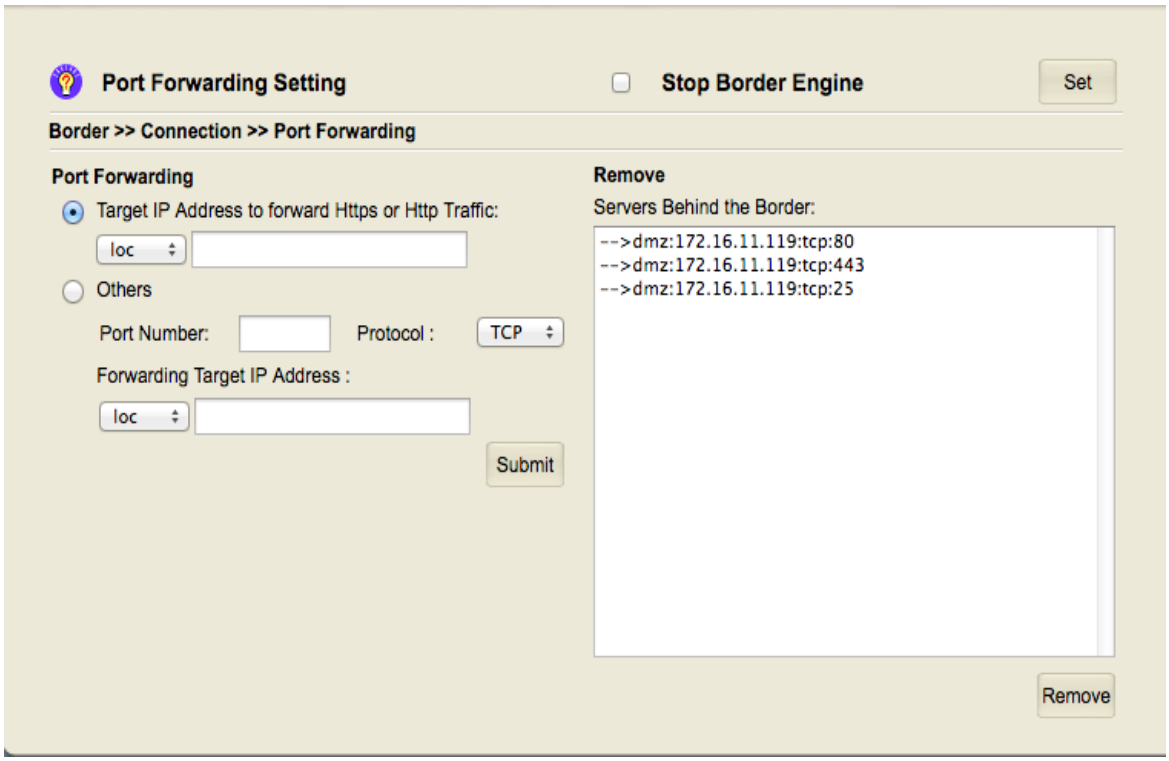



イラスト ***38: SMTP*** ポートフォワーディングを追加した後の画面スナップショット

実際、「ポートフォワーディング」は、基盤プラットフォーム上で「DNAT」というアクションを用いて実装されています。「DNAT」とは、到着したパケットの宛先 IP アドレスを変更し、新しい宛先 IP アドレスに基づいてパケットを配信するアクションです。したがって、ここでルールを追加すると、「**Border >> Rule >> List / Remove Rule**」に該当するルールが見つかります。

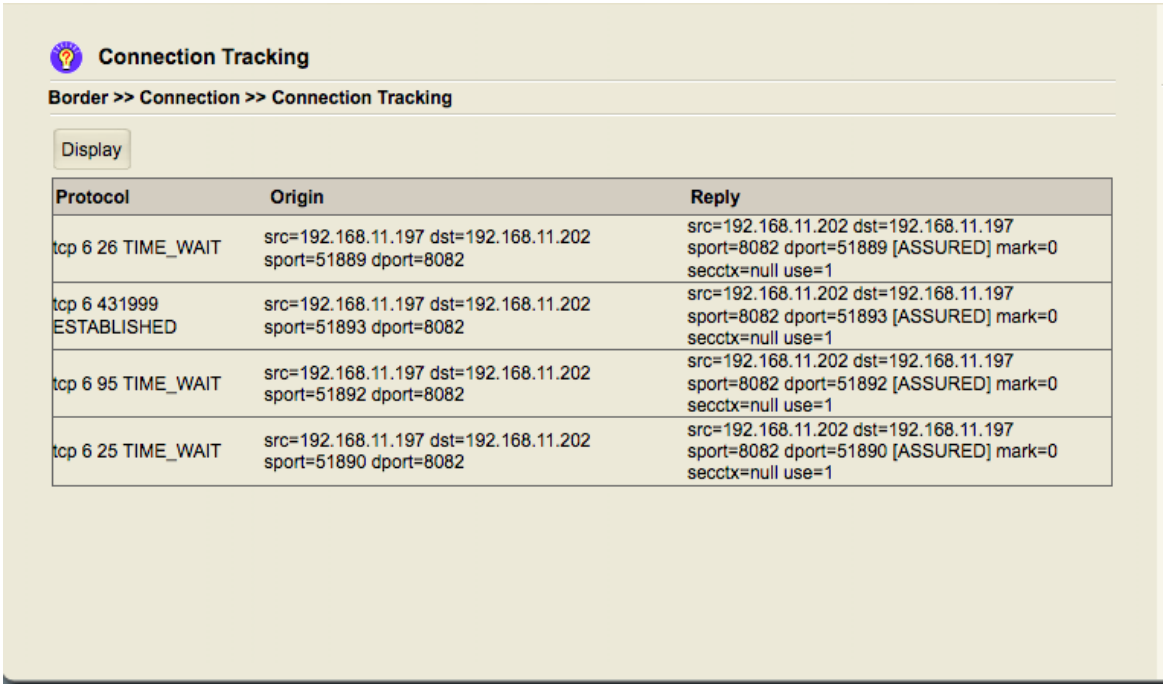
一般的に、ゾーン “dmz” のホストに “Port forwarding” を使用することを推奨します。ゾーン “loc” のホストへの “Port forwarding” は、インターネットからのスパムがローカルエリアネットワークに流れる原因となる可能性があります。それに加えて、Port Forwarding からターゲットホストのゾーンからのトラフィックループバックを依頼されることもあります。

例えば、ゾーン「loc」内のホストにポートフォワーディングを行うと、ゾーン「net」のパブリック IP アドレス（ベースプラットフォームの「br0」の IP アドレス）を使用しているユーザーは、そのホストにアクセスできます。しかし、ゾーン「loc」内のユーザーも、そのパブリック IP アドレスを使用してそのホストにアクセスしたい場合があります。この場合、「ループバック」が必要です。ベースプラットフォームでは「ループバック」は提供されていません。この機能にご興味がある場合は、「ved」ビルドをご覧ください。

## 接続追跡

ネットワークの問題の診断には、接続アクティビティの確認が役立ちます。これは、「Border >> Connection >> Connection Tracking」で「Display」ボタンをクリックすることで行えます。


挿絵 ***39:*** 接続追跡の画面スナップショット



Connection Tracking

Border >> Connection >> Connection Tracking

Display

| Protocol | Origin | Reply |
|---|---|---|
| tcp 6 26 TIME_WAIT | src=192.168.11.197 dst=192.168.11.202 sport=51889 dport=8082 | src=192.168.11.202 dst=192.168.11.197 sport=8082 dport=51889 [ASSURED] mark=0 secctx=null use=1 |
| tcp 6 431999 ESTABLISHED | src=192.168.11.197 dst=192.168.11.202 sport=51893 dport=8082 | src=192.168.11.202 dst=192.168.11.197 sport=8082 dport=51893 [ASSURED] mark=0 secctx=null use=1 |
| tcp 6 95 TIME_WAIT | src=192.168.11.197 dst=192.168.11.202 sport=51892 dport=8082 | src=192.168.11.202 dst=192.168.11.197 sport=8082 dport=51892 [ASSURED] mark=0 secctx=null use=1 |
| tcp 6 25 TIME_WAIT | src=192.168.11.197 dst=192.168.11.202 sport=51890 dport=8082 | src=192.168.11.202 dst=192.168.11.197 sport=8082 dport=51890 [ASSURED] mark=0 secctx=null use=1 |

図 ***40:*** 接続ステータスの表示

もし、ある特定のパーソナルコンピュータが、非常に多くの接続を伴う場合、それはウイルスに感染しているか、またはピアツーピアソフトウェアを使用している可能性がある。その根本的な原因を特定するために、以下の手がかりを参照してください。

## *Actions after Receiving Network Packets*

ネットワークパケットを受信した後、ベースプラットフォームは、このパケットに対して以下のいずれかの対応を行うことができます。ACCEPT、DROP、REJECT、DNAT、および REDIRECT。IP トラフィックを操作する各ルールの属性は、パケットがどこから来たか（Source）、パケットがどこへ向かうべきか（Destination）、プロトコルが TCP か UDP であるか、目的ポート、ソースポート、および元の宛先 IP アドレスを含みます。これらの属性に基づいて、ベースプラットフォームは対応を実行します。ここではこれらの対応を大まかに紹介し、その使用法は次のセクションで示されます。

「ACCEPT」アクションは、ネットワークトラフィックがすべての属性とルールに一致した場合にトラフィックを受け入れることです。たとえば、TCP ポート 23 のすべての「telnet 接続」（ゾーン「net」からベースプラットフォーム「fw」への）を受け入れるために、「ACCEPT」アクションを使用して指定することができます。

ソース: net
Destination: fw
プロトコル: TCP
Destination Port: 23

“DROP”というアクションは、指定された属性の到着パケットを単に無視することです。“DROP”と“REJECT”の違いは、“REJECT”が、接続が利用できない場合に送信者にメッセージを返送することです。 また、ゾーン間のプリ定義されたルールがデフォルトで存在します。 したがって、“DROP”と“REJECT”を必要としない限り指定する必要はありません。例えば、ゾーン “loc” からゾーン ‘net’ へのトラフィックは、デフォルトで許可されています。 もし、ゾーン “loc” からゾーン ‘net’ への http アクセスをすべてブロックしたい場合、“DROP” を指定することができます。

ソース: loc
Destination: net
プロトコル: TCP
Destination Port: 80

“REDIRECT”というアクションは、ベースプラットフォームへの到着するトラフィックを、ベースプラットフォームの別のポートにリダイレクトします。 通常はアプリケーションデーモンを再構成せずにこれを実行しますが、デーモンがより多くのポートを聞き取るようにしたい場合に便利です。 例えば、「telnet 交通」は通常「TCP ポート 23」を使用します。ただし、「TCP ポート 28」も「telnet デーモン」が処理できるようにしたい場合です。このような場合、「REDIRECT」を使用できます。

そして、以前に述べたように、アクション「DNAT」は「ポートフォワーディング」を行い、到着パケットの宛先 IP アドレスを「net」ゾーンから「dmz」ゾーンまたは「loc」ゾーンのホストに変更することです。このホストは物理エンティティである必要はなく、トラフィックを処理できる仮想ホストでも構いません。

ルールを追加

「Border >> Rule >> Add Rule」を通じて例外ルールを追加できます。

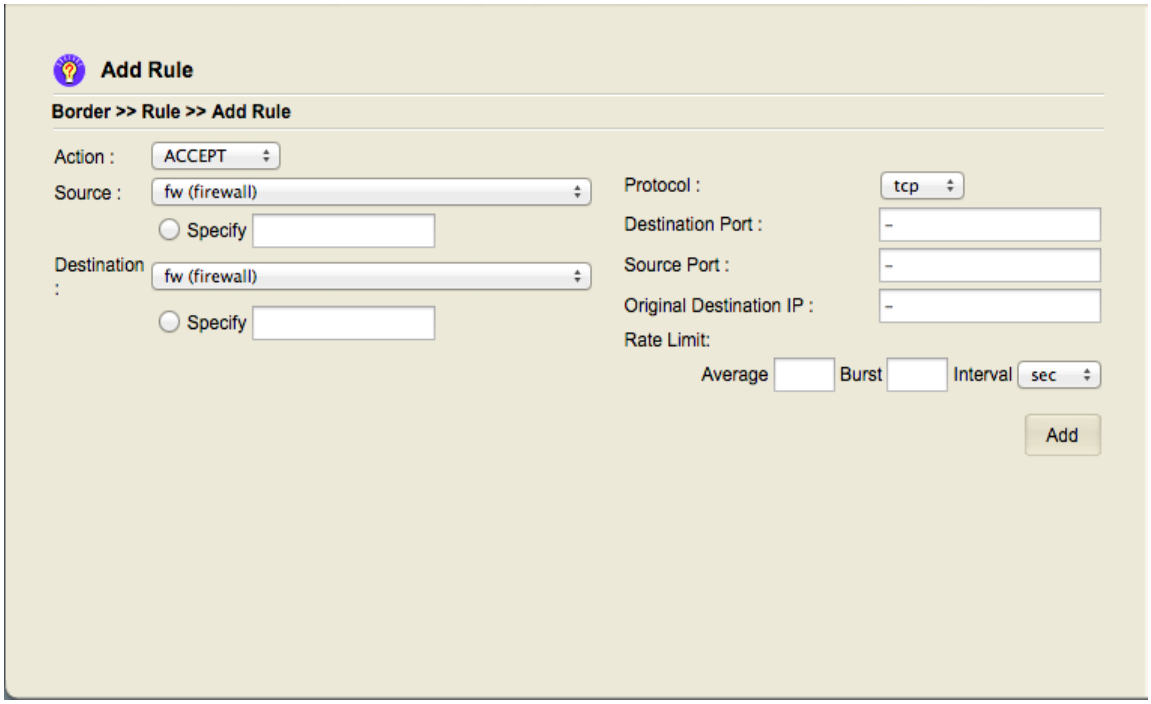
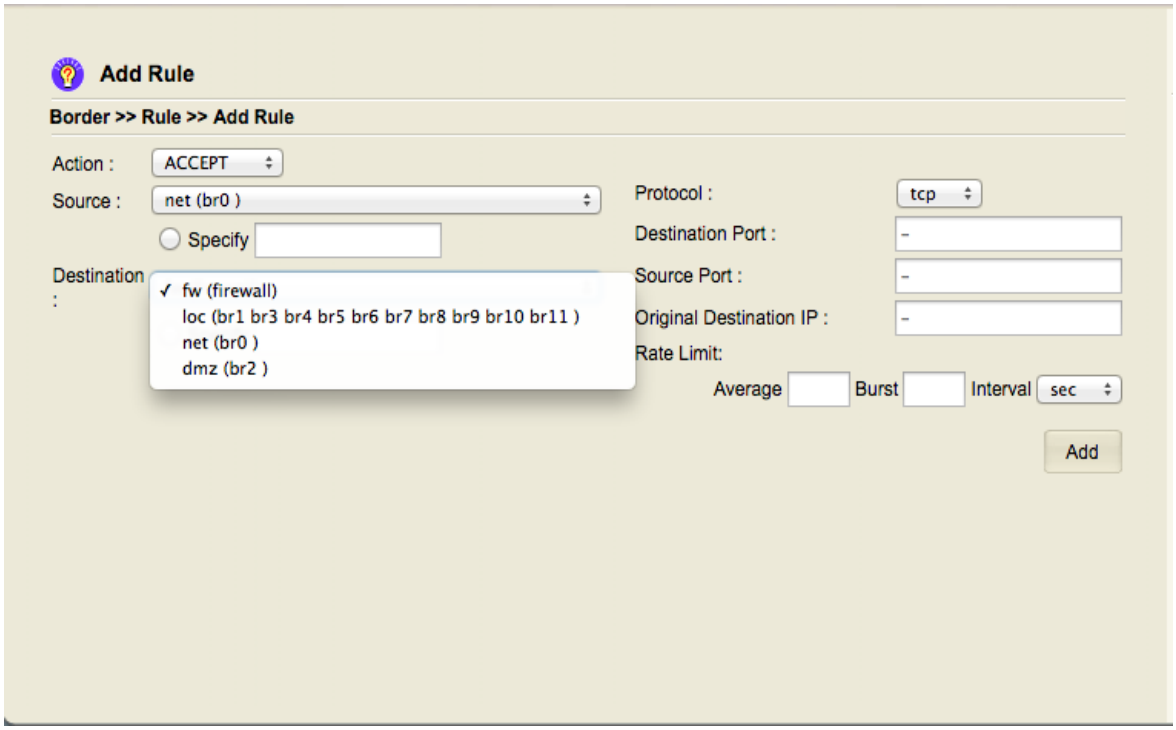



イラスト ***41:*** 画面スナップショット ***for Adding Rule***

ルールを追加する前に、ホスト（仮想ホストであっても、物理エンティティを持つホストでも）がどこに配置されているかを確認してください。仮想ホストの場合は、そのブリッジに接続するネットワークインターフェースを持っていることを確認する必要があります。物理エンティティを持つホストの場合は、適切に接続されているかを確認してください。ゾーン“dmz”に配置されているホストの場合、ベースプラットフォームから DHCP で IP アドレスを取得することはできません。これは、ゾーン“fw”へのアクセスをブロックするプリ定義ルールがあるためです。ゾーン“DMZ”に配置されているホストには、手動で IP アドレスを設定する必要があります。




挿絵 ***42***：ルールに関連するソースと宛先

あらかじめ定義されたルールは表示されませんが、例外ルールを追加する際には、それらに精通しておく必要があります。“loc”から“dmz”への接続を許可するルールを追加することは無意味です。なぜなら、ベースプラットフォームはすでにそのルールをデフォルトで許可しているからです。しかし、"dmz"から“loc”への接続を許可する例外ルールを追加することは合理的です。なぜなら、接続はデフォルトでブロックされているからです。

同様に、接続がデフォルトでブロックされているため、ゾーン“net”からのゾーン“fw”への例外を追加することも適切です。例えば、

ソース: net
Destination: fw
プロトコル: tcp
Destination Port: 23

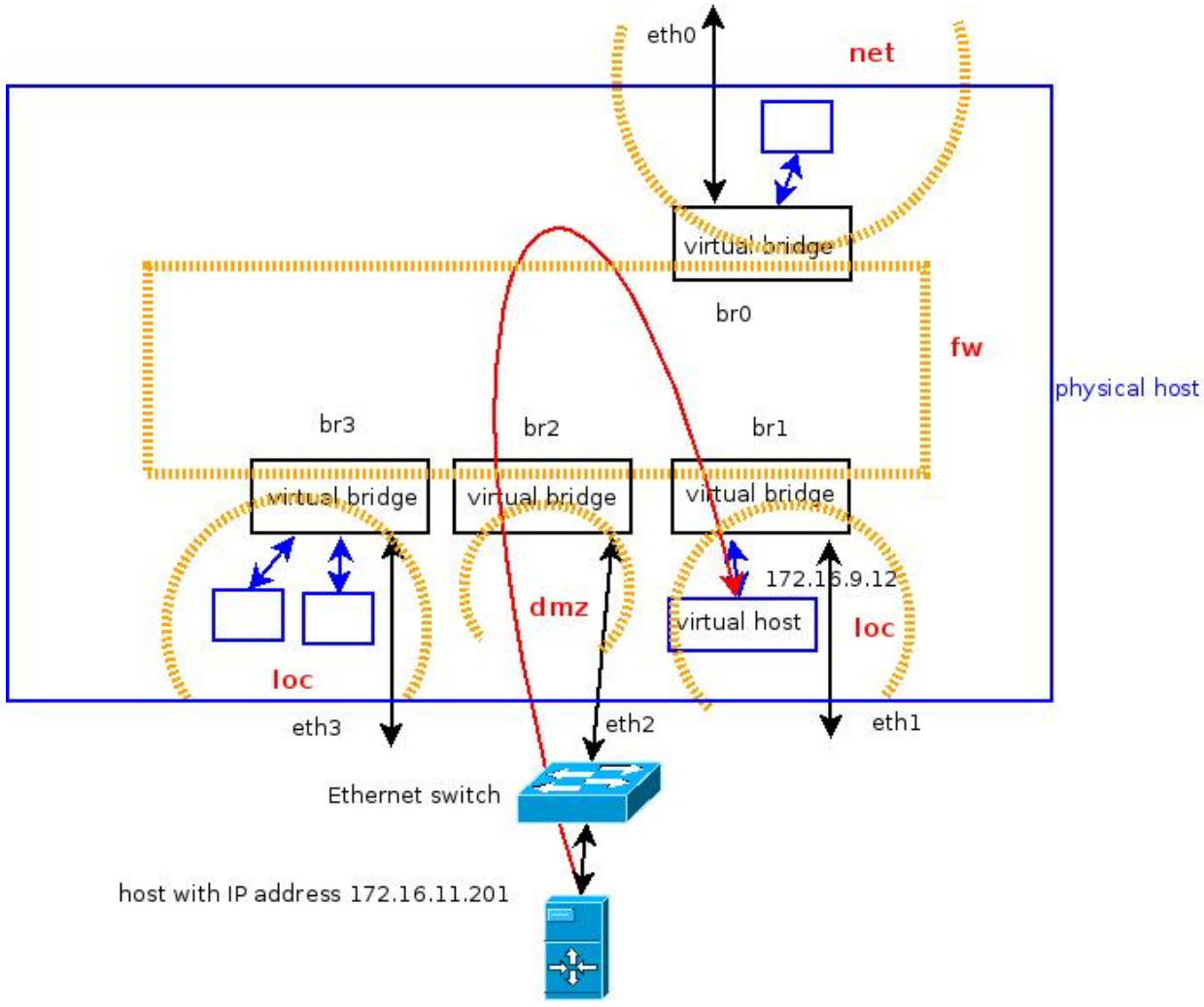
“Add”ボタンを押してください。ルールは境界制御エンジンの再起動後に有効になります。

「telnet 接続」（TCP ポート 23）を「net」ゾーンから「fw」ゾーンに許可します。

以下のセクションでは、参照のための例を提供します。

## *Allowing Exceptions for TCP Connections from dmz to loc*

“dmz”から“loc”への接続はデフォルトでブロックされています。しかし、“dmz”から IP アドレス“172.16.9.12”を持つホストへの TCP 接続を許可するルールを追加したいと思います。“loc”。




挿絵 ***43:*** 「***dmz***」ゾーンから「***loc***」ゾーンへの例外ルールを追加

以下のスクリーンショットで、ゾーン “loc” においてホストの特定の IP アドレス “172.16.9.12” を指定してください。

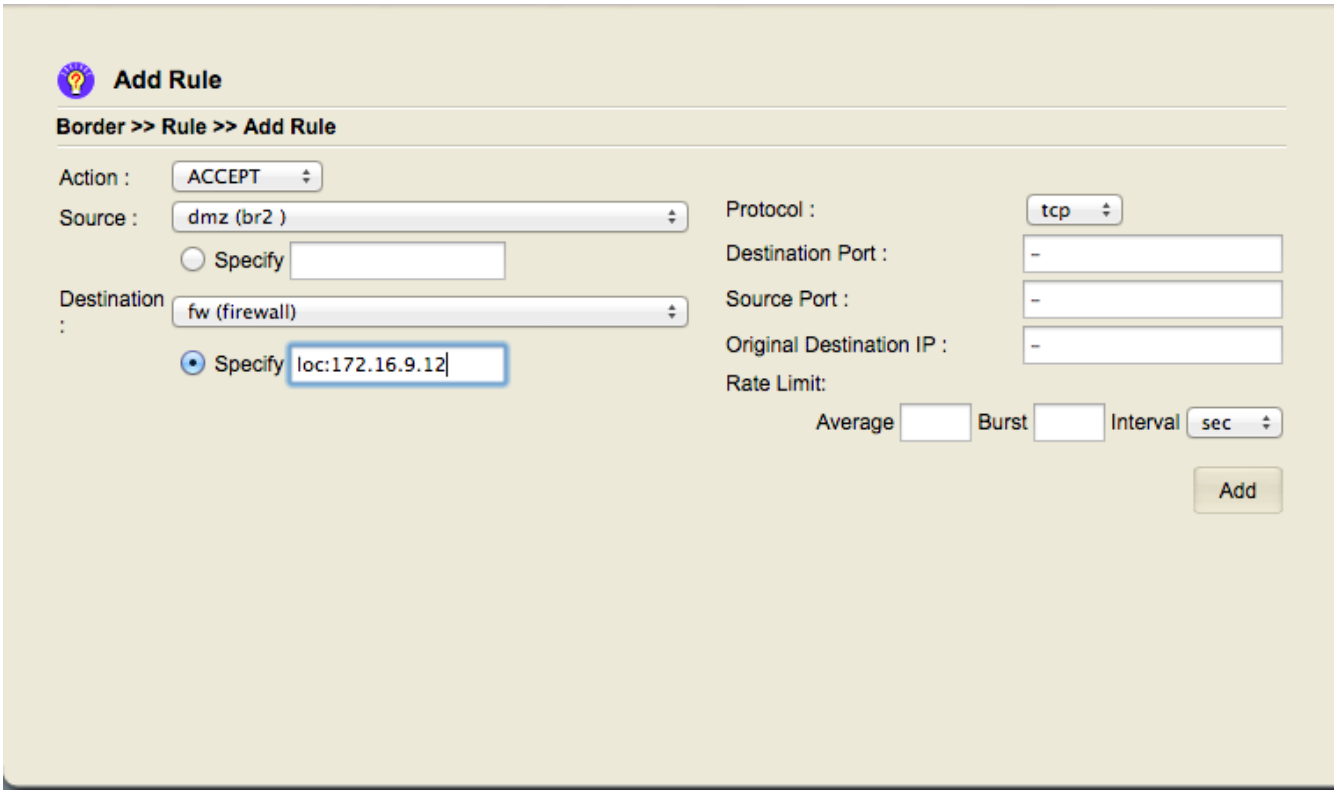



イラスト ***44: “dmz”から“loc”***のホストへのスクリーンショット

「Specify」の欄に特定のホストを指定するには、以下の形式を使用する必要があります。

“zone:IP_ADDRESS”
or
“zone:SUBNET”

For example, 例示として

“loc:172.16.9.12”
or
“loc: 172.16.12.0/24”

「Add」ボタンを押すと、関連するルールは「Border >> Rule >> List / Remove Rule」で表示できます。

**Border >> Rule >> List / Remove Rule**

**Current Rules**

| Action | Source | Destination | Protocol | Destination Port | Source Port | Original Destination IP | Rate Limit | Remove |
|---|---|---|---|---|---|---|---|---|
| ?SECTION | NEW | | | | | | | |
| ACCEPT | fw | net | udp | 53 | | | | |
| ACCEPT | loc | fw | tcp | 22 | | | | |
| ACCEPT | fw | loc | udp | 137:139 | | | | |
| ACCEPT | fw | loc | tcp | 137,139 | | | | |
| ACCEPT | fw | loc | udp | 1024: | 137 | | | |
| ACCEPT | loc | fw | udp | 137:139 | | | | |
| ACCEPT | loc | fw | tcp | 137,139 | | | | |
| ACCEPT | loc | fw | udp | 1024: | 137 | | | |
| ACCEPT | loc | fw | tcp | ssh | | | | |
| ACCEPT | net | fw | tcp | http | | | | |
| ACCEPT | net | fw | tcp | 443 | | | | |
| ACCEPT | net | fw | tcp | 8080 | | | | |
| ACCEPT | net | fw | tcp | 8081 | | | | |
| ACCEPT | net | fw | tcp | 8082 | | | | |
| ACCEPT | net | fw | udp | 1194 | | | | |
| ACCEPT | net | fw | udp | 1195 | | | | |
| ACCEPT | net | fw | udp | 7777 | | | | |
| ACCEPT | net | fw | udp | 4569 | | | | |
| ACCEPT | net | fw | tcp | 25 | | | | |
| ACCEPT | net | fw | tcp | 23 | - | - | | |
| ACCEPT | net | fw | tcp | 22 | - | - | | |
| ACCEPT | net | fw | tcp | 5901-5909 | - | - | | |
| ACCEPT | dmz | loc:172.16.9.12 | tcp | - | - | - | | |

挿絵 ***45:*** 「***dmz***」から「***loc***」のホストへのルールを表示

## 接続の拒否または切断

“net”から“loc”への接続はデフォルトで禁止されています。そのため、“net”から“loc”への拒否またはドロップルールを追加する必要はありません。同様に、“dmz”から“loc”への接続も禁止されています。 “loc”から“net”への接続はデフォルトで許可されています。 “loc”から“net”への HTTP トラフィックをブロックするための例外ルールを追加したい場合は、それを実行できます。

ソース: loc
Destination: net
プロトコル: TCP
Destination Port: 80

ソース: loc
Destination: net
プロトコル : TCP
Destination Port: 443

HTTP および HTTPS は、TCP ポート 80 と TCP ポート 443 を使用しています。これらのポートを入力するには、「Add」ボタンを押してください。ルールは「Border Engine」を再起動することで有効になります。

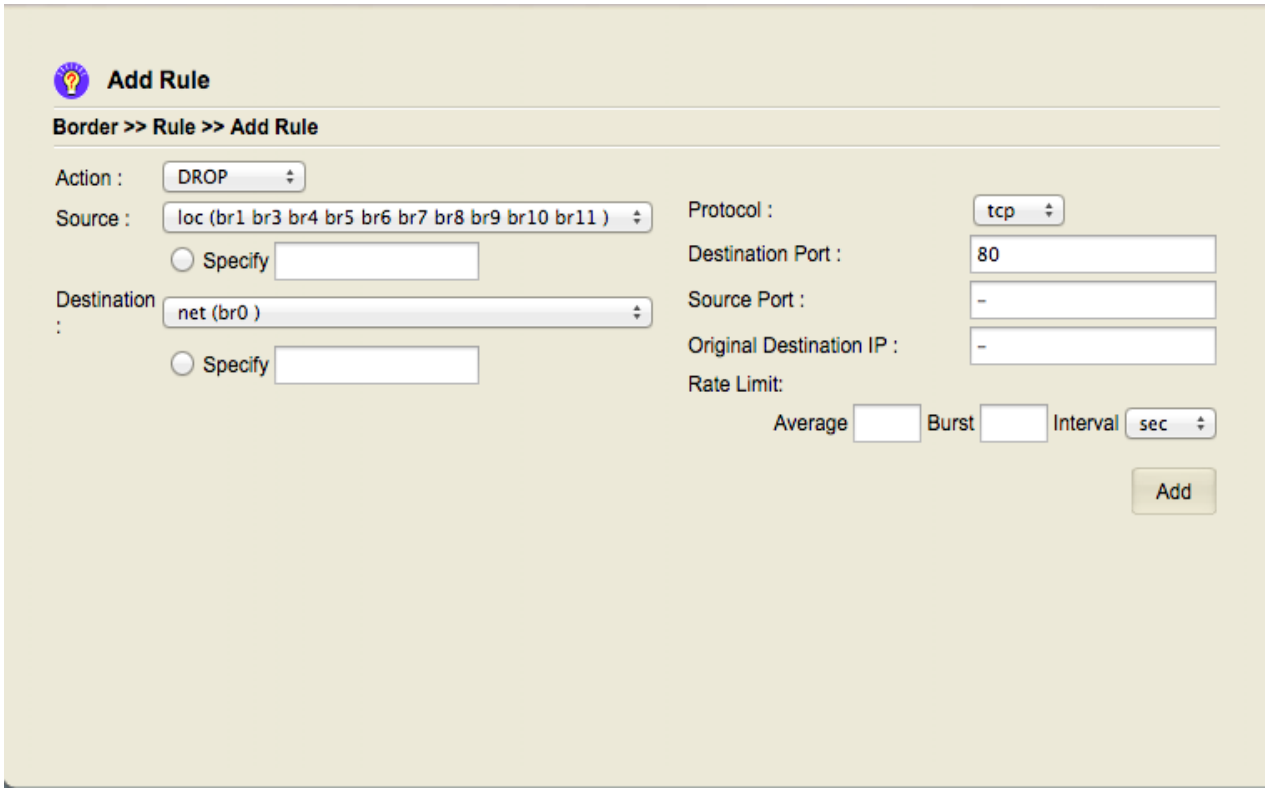



イラスト ***46:*** 「***loc***」から「***net***」への ***Http*** トラフィックのドロップの画面スナップショット

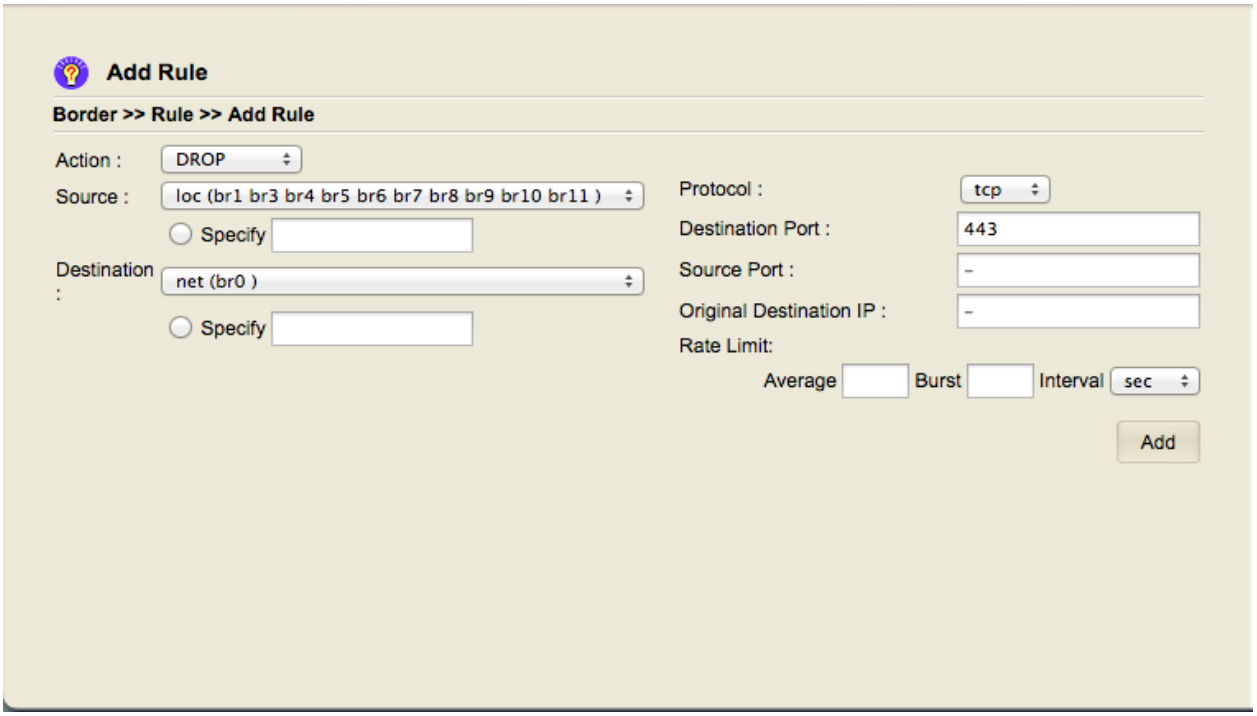



イラスト ***47:*** スクリーンショット フォーム から ***HTTPS*** トラフィックを ***"loc"*** から ***"net"*** へドロップする

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ACCEPT | net | fw | udp | 7777 | | | | |
| ACCEPT | net | fw | udp | 4569 | | | | |
| ACCEPT | net | fw | tcp | 25 | | | | |
| ACCEPT | net | fw | tcp | 23 | - | - | | |
| ACCEPT | net | fw | tcp | 22 | - | - | | |
| ACCEPT | net | fw | tcp | 5901-5909 | - | - | | |
| ACCEPT | dmz | loc:172.16.9.12 | tcp | - | - | - | | |
| DROP | loc | net | tcp | 80 | - | - | | |
| DROP | loc | net | tcp | 443 | - | - | | |

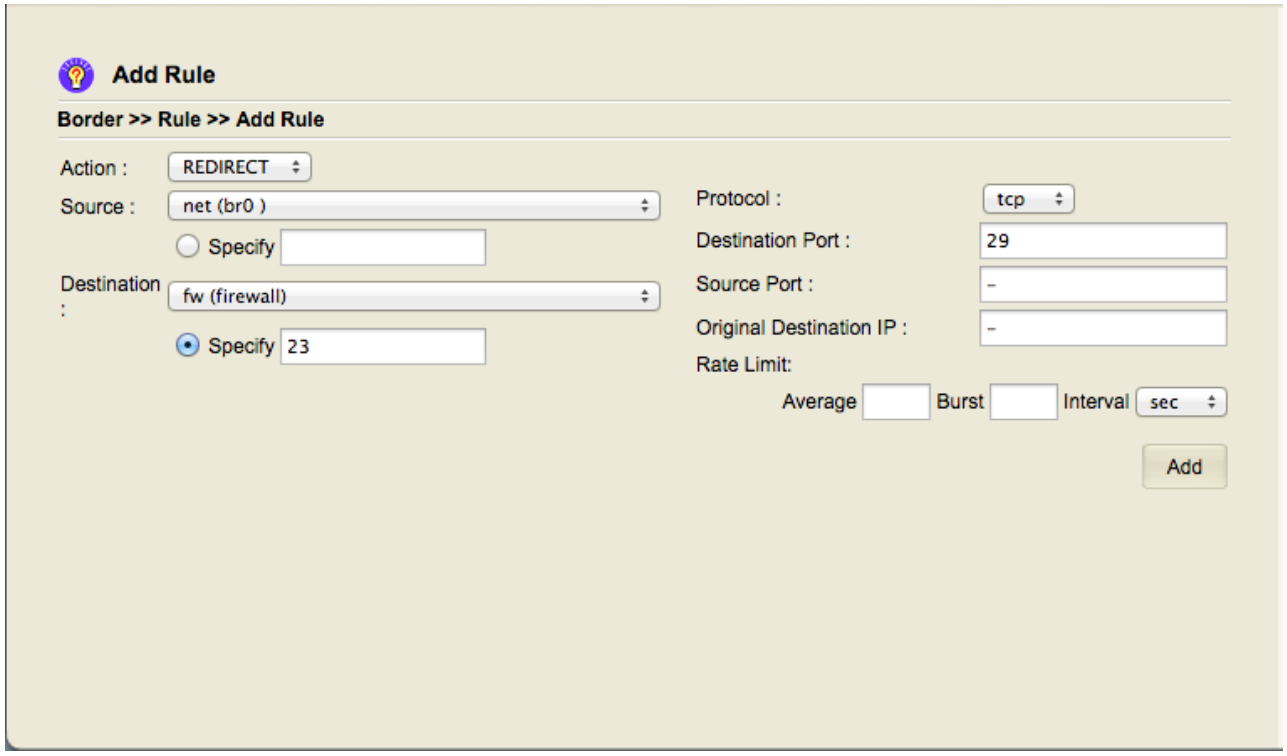
挿絵 ***48: HTTP*** および ***HTTPS (***ポート ***80*** と ***443)*** の落とし方の例

## *Redirect Traffic to Another Port of the Base Platform*

ネットワークトラフィックを 1 つの TCP/UDP ポートから別のポートにリダイレクトするには、通常、いくつかのネットワーク環境の問題やレガシーシステムが関与します。 例えば、TELNET 接続（TCP ポート 23 でリッスンする）をブロックしている環境にありながら、他の接続を許可している場合です。 そのような場合、TELNET 用の別のポートを設定することになります。

Action: REDIRECT
Source: net
Destination: 23
Protocol: TCP
宛先ポート：29

この設定は、TCP ポート 29 のトラフィックを TCP ポート 23 にリダイレクトします。



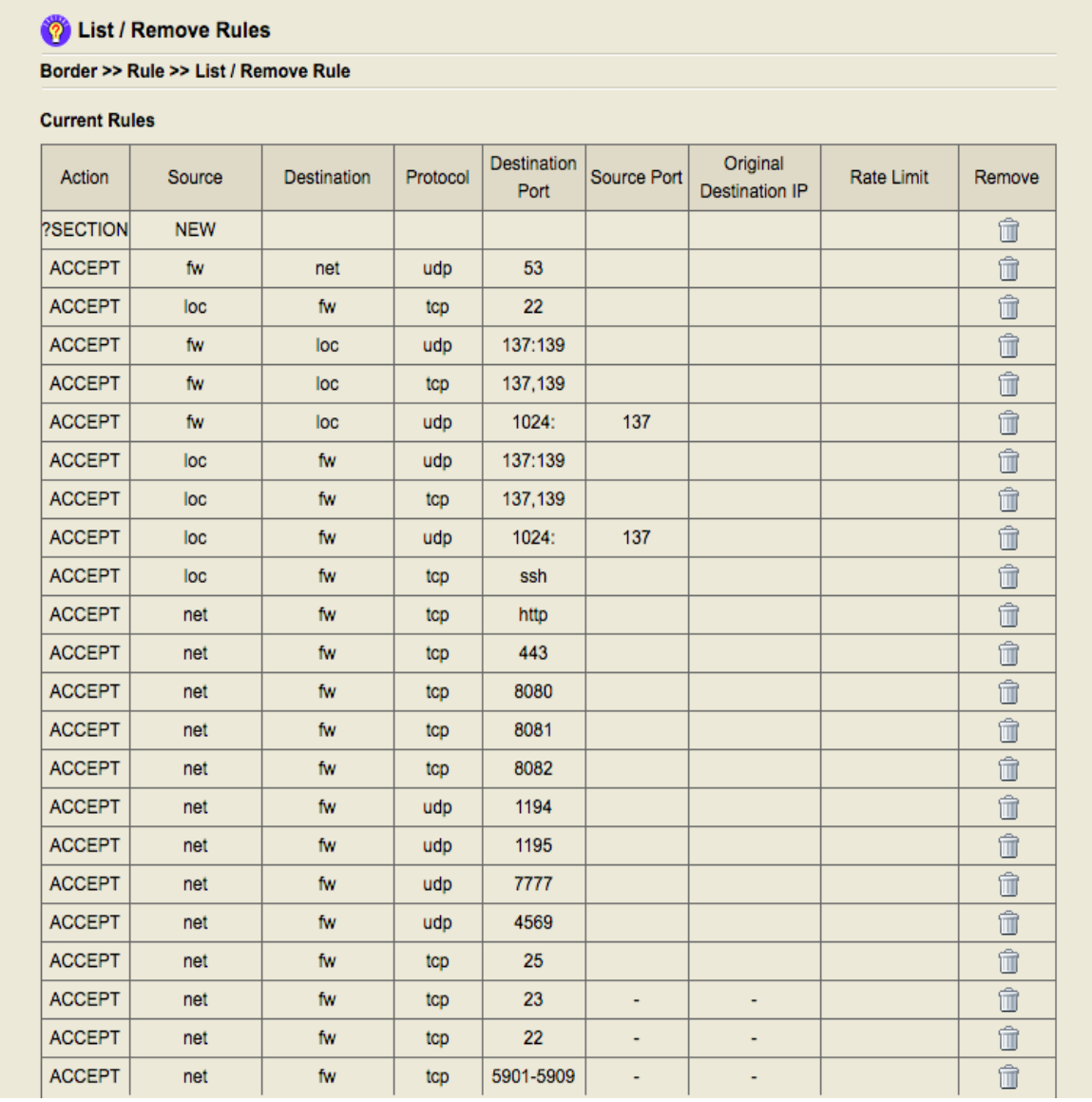

挿絵 49: リダイレクトのトラフィックを別のポートに

| Action | Source | Destination | Protocol | Destination Port | Source Port | Original Destination IP | Rate Limit | Remove |
|---|---|---|---|---|---|---|---|---|
| ?SECTION | NEW | | | | | | | |
| ACCEPT | fw | net | udp | 53 | | | | |
| ACCEPT | loc | fw | tcp | 22 | | | | |
| ACCEPT | fw | loc | udp | 137:139 | | | | |
| ACCEPT | fw | loc | tcp | 137,139 | | | | |
| ACCEPT | fw | loc | udp | 1024: | 137 | | | |
| ACCEPT | loc | fw | udp | 137:139 | | | | |
| ACCEPT | loc | fw | tcp | 137,139 | | | | |
| ACCEPT | loc | fw | udp | 1024: | 137 | | | |
| ACCEPT | loc | fw | tcp | ssh | | | | |
| ACCEPT | net | fw | tcp | http | | | | |
| ACCEPT | net | fw | tcp | 443 | | | | |
| ACCEPT | net | fw | tcp | 8080 | | | | |
| ACCEPT | net | fw | tcp | 8081 | | | | |
| ACCEPT | net | fw | tcp | 8082 | | | | |
| ACCEPT | net | fw | udp | 1194 | | | | |
| ACCEPT | net | fw | udp | 1195 | | | | |
| ACCEPT | net | fw | udp | 7777 | | | | |
| ACCEPT | net | fw | udp | 4569 | | | | |
| ACCEPT | net | fw | tcp | 25 | | | | |
| ACCEPT | net | fw | tcp | 5901-5909 | - | - | | |
| REDIRECT | net | 23 | tcp | 29 | - | - | | |

挿絵 ***50:*** ディスプレイリストにおける ***REDIRECT*** ルール

そして、効果が発動するのは Border Engine の再起動後に始まります。ネットワークパケットが 1 つの TCP ポートから別の TCP ポートにリダイレクトされても、上位のネットワークプロトコルが中断される可能性があります。たとえば、非標準ポートから HTML ページに HTTP でアクセスする場合、HTML がハードコードされたローカル URL を含んでいるため、別のポートを使用してもブラウザで完全に表示されない可能性があります。

ルールをリスト表示または削除する



**List / Remove Rules**

**Border >> Rule >> List / Remove Rule**

**Current Rules**

| Action | Source | Destination | Protocol | Destination Port | Source Port | Original Destination IP | Rate Limit | Remove |
|---|---|---|---|---|---|---|---|---|
| ?SECTION | NEW | | | | | | | |
| ACCEPT | fw | net | udp | 53 | | | | |
| ACCEPT | loc | fw | tcp | 22 | | | | |
| ACCEPT | fw | loc | udp | 137:139 | | | | |
| ACCEPT | fw | loc | tcp | 137,139 | | | | |
| ACCEPT | fw | loc | udp | 1024: | 137 | | | |
| ACCEPT | loc | fw | udp | 137:139 | | | | |
| ACCEPT | loc | fw | tcp | 137,139 | | | | |
| ACCEPT | loc | fw | udp | 1024: | 137 | | | |
| ACCEPT | loc | fw | tcp | ssh | | | | |
| ACCEPT | net | fw | tcp | http | | | | |
| ACCEPT | net | fw | tcp | 443 | | | | |
| ACCEPT | net | fw | tcp | 8080 | | | | |
| ACCEPT | net | fw | tcp | 8081 | | | | |
| ACCEPT | net | fw | tcp | 8082 | | | | |
| ACCEPT | net | fw | udp | 1194 | | | | |
| ACCEPT | net | fw | udp | 1195 | | | | |
| ACCEPT | net | fw | udp | 7777 | | | | |
| ACCEPT | net | fw | udp | 4569 | | | | |
| ACCEPT | net | fw | tcp | 25 | | | | |
| ACCEPT | net | fw | tcp | 23 | - | - | | |
| ACCEPT | net | fw | tcp | 22 | - | - | | |
| ACCEPT | net | fw | tcp | 5901-5909 | - | - | | |

挿絵 ***51:*** リストからルールを削除する

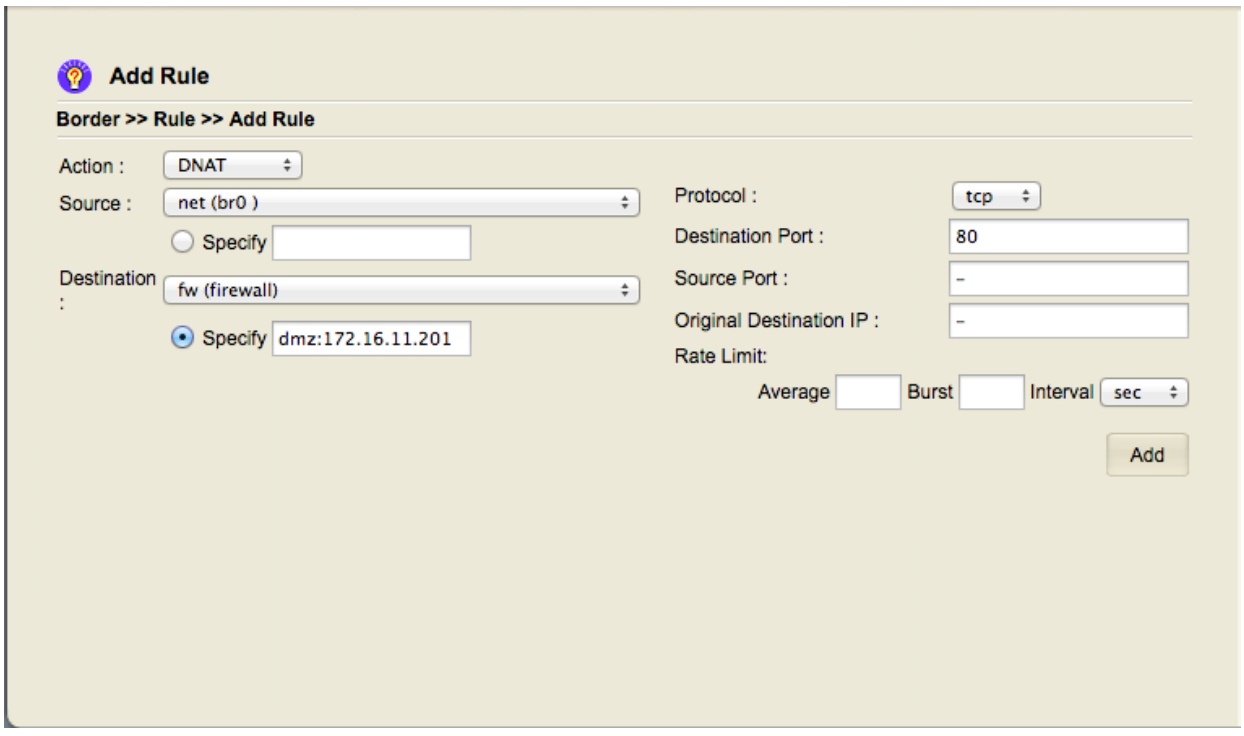
これ以前のセクションで見てきた通り、ルールを削除するには、ルール名の右にあるゴミ箱アイコンを押してください。システムは削除を確認するように尋ねます。効果があるように、ボーダーエンジンを再起動してください。

## *Using DNAT for Port Forwarding*

ポートフォワーディングは、「DNAT」という機能を使用して行われます。「DNAT」という機能は、ベースプラットフォーム上で受信したパケットの宛先 IP アドレスを変更し、変更された宛先 IP アドレスに基づいてパケットを転送することです。

例えば、ゾーン“dmz”におけるホストの IP アドレス“172.16.11.201”への HTTP トラフィック（TCP ポート 80）を転送するには、次のようにします。

アクション: DNAT
Source: net
宛先：dmz:172.16.11.201
Protocol: tcp
目的地ポート：80

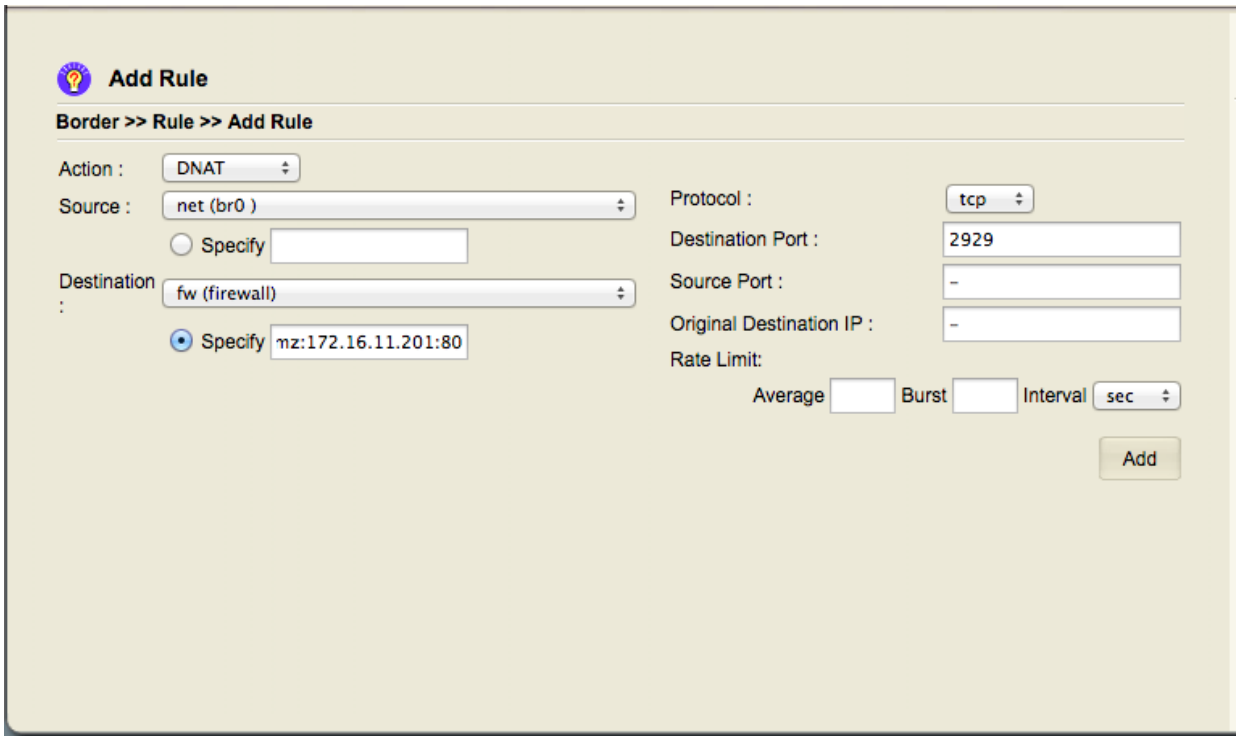



挿絵 ***52: DNAT*** を使用したポートフォワーディングの利用

これは、ベースプラットフォームの“TCP ポート 80”からの到着トラフィックを、ホストの受信トラフィックの“TCP ポート 80”に転送します。しかし、ホストの別のポートに転送したい場合があります。

例えば、「TCP Port 2929」のトラフィックは、ゾーン“dmz”のホスト“172.16.11.201”の“TCP port 80”にフォワードされます。これは、“TCP Port 2929”を設定することで実行できます。

アクション: DNAT
Source: net
宛先 : dmz:172.16.11.201:80
Protocol: tcp
宛先ポート: 2929




挿絵 ***53:*** ホストへの異なるポートの転送

「Add」ボタンを押すと、ルールは以下のようになります。

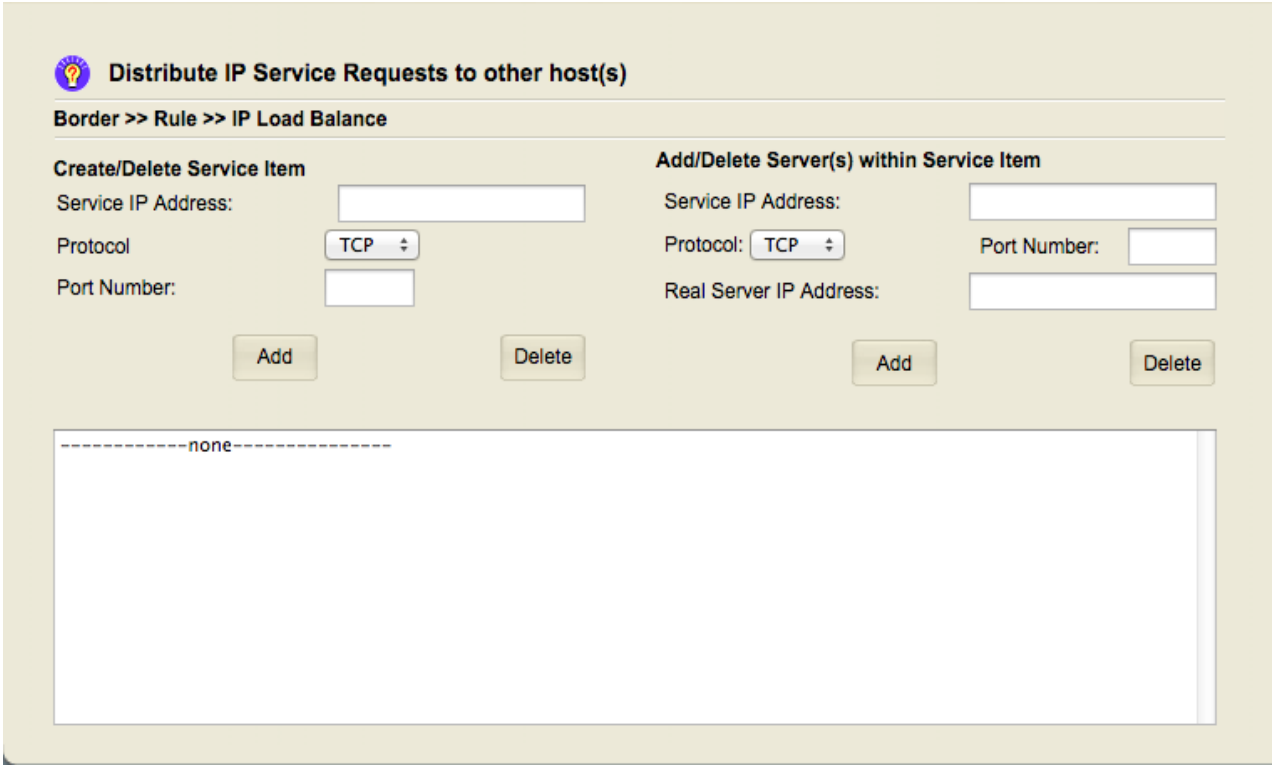
| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ACCEPT | net | fw | udp | 1195 | | | | |
| ACCEPT | net | fw | udp | 7777 | | | | |
| ACCEPT | net | fw | udp | 4569 | | | | |
| ACCEPT | net | fw | tcp | 25 | | | | |
| ACCEPT | net | fw | tcp | 5901-5909 | - | - | | |
| ACCEPT | net | fw | tcp | 22 | - | - | | |
| ACCEPT | net | fw | tcp | 23 | - | - | | |
| DNAT | net | dmz:172.16.11.201 | tcp | 80 | - | - | | |
| DNAT | net | dmz:172.16.11.201:80 | tcp | 2929 | - | - | | |

挿絵 ***54:*** ポートフォワーディングのルールリスト

“br0” のベースプラットフォームの IP アドレスが “192.168.11.202” であるとします。したがって、“TCP port 80” をホスト “172.16.11.202” に zone “dmz” から到達するには、“http://192.168.11.202:2929/” を使用します。

## *IP* バランス調整

各タプル (IP_ADDRESS, TCP_OR_UDP, PORT_NUMBER) について、"ポートフォワーディング" を行うことは、トラフィックを 1 つのホストにのみ送信できます。 ある IP アドレスの場合、特定のポートのトラフィックを複数のホストに送信したい場合は、"Load Balance" と呼ばれます。 これは、"Border >> Rule >> IP Load Balance" の設定で行うことができます。

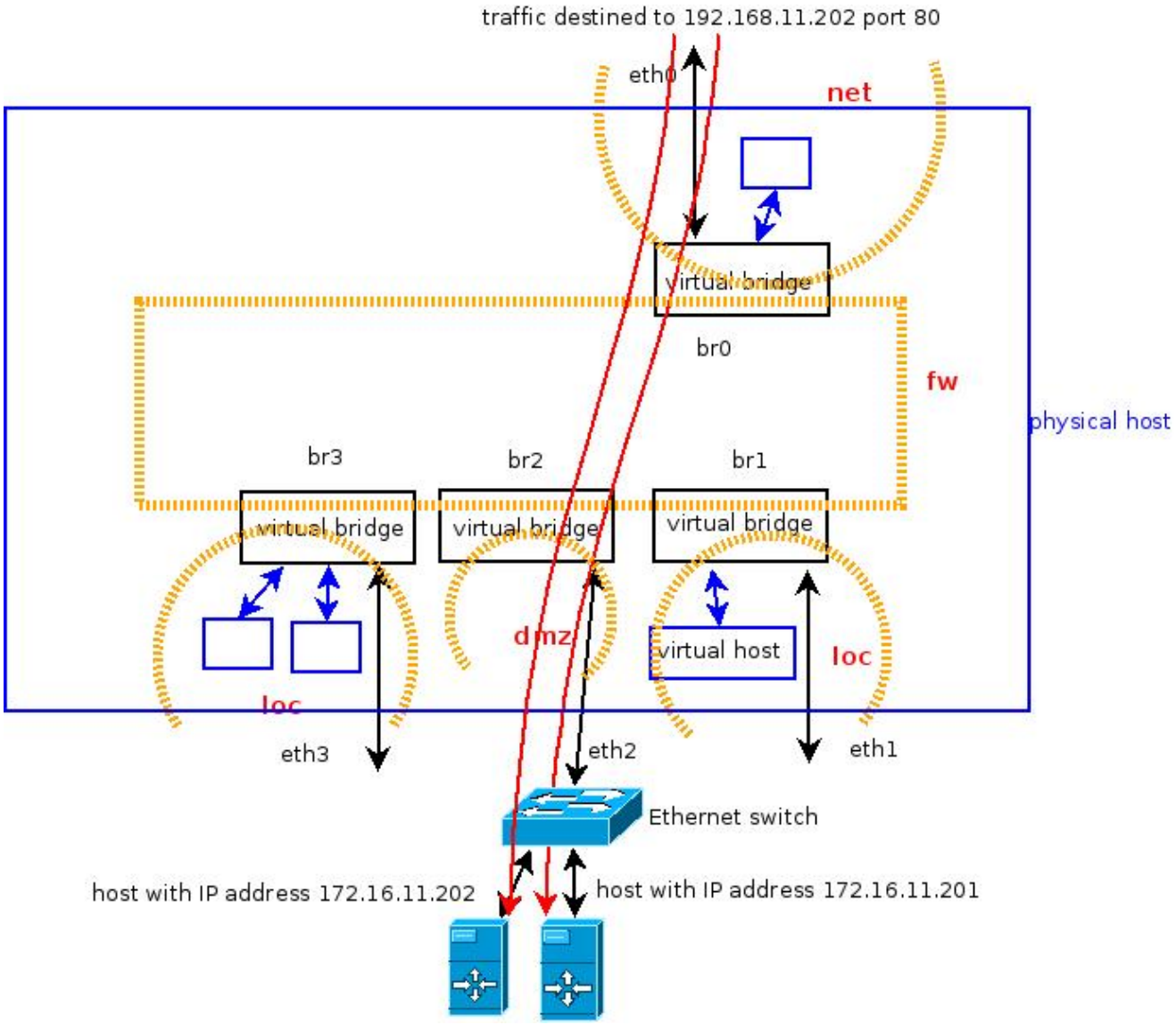



挿絵 ***55*** : ***IP*** 負荷分散画面スナップショット

各タプル（IP_ADDRESS、TCP_OR_UDP、PORT_NUMBER）を「サービスアイテム」と呼びます。各サービスアイテムには、複数のホストに関連付けられ、ネットワークリクエストがそれらのホストにラウンドロビン方式で分散されます。ネットワークリクエストが 1 つのホストに送信されると、同じクライアントからのリクエストは、300 秒以内には同じホストに送信されます。

このプラットフォームで提供されている関数は、負荷を複数のサーバーに分散させるためのものです。アプリケーション固有のデータに関しては、デザイナーがホスト間でデータを同期させる必要があります。このプラットフォームは、ホスト内のデータを扱ることができません。

以下の情報は、ベースプラットフォームにおける HTTP トラフィックのロードバランシングの例です。ベースプラットフォームの "br0" の IP アドレスは "192.168.11.202" です。"dmz" ゾーンのホスト "172.16.11.201" と "172.16.11.202" に、HTTP トラフィックを配信したいと考えています。最初に、HTTP トラフィック (TCP ポート 80) がベースプラットフォームで受け入れられるように、"net" ゾーンから "fw" ゾーンへの TCP ポート 80 の例外ルールを追加する必要があります。その後、ロードバランシングをここで処理できます。




挿絵 *56: 2* ホストへの *HTTP* トラフィックの分散

設定手順は以下の通りです。「192.168.11.202」と TCP ポート 80 を使用してサービス項目を作成します。

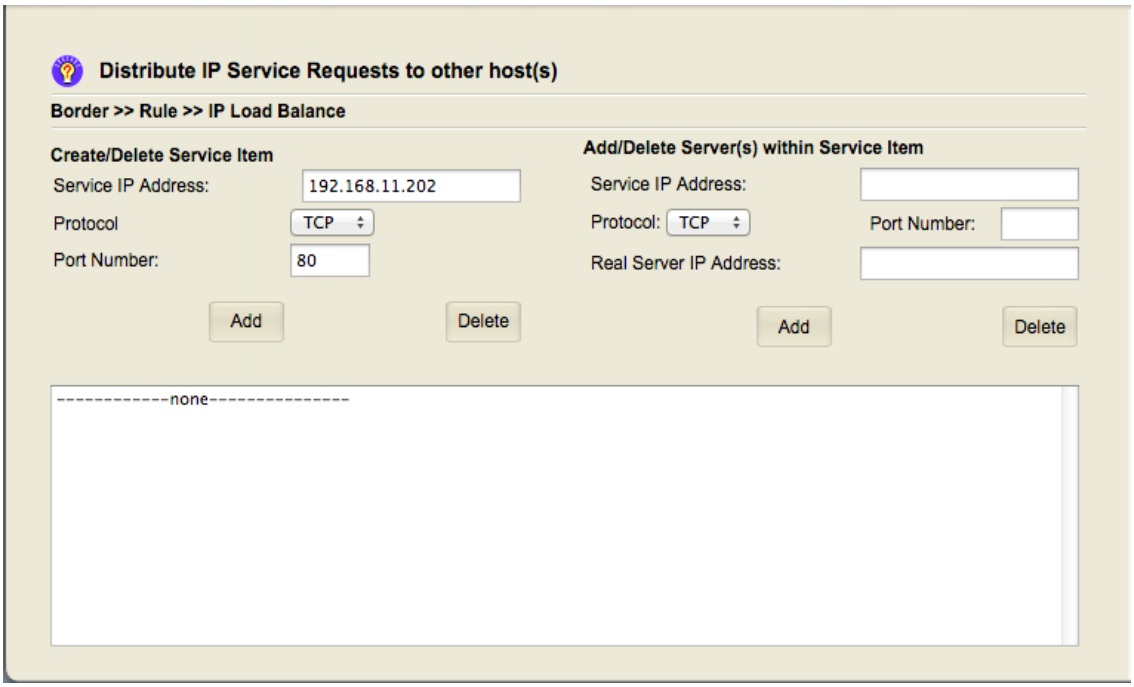
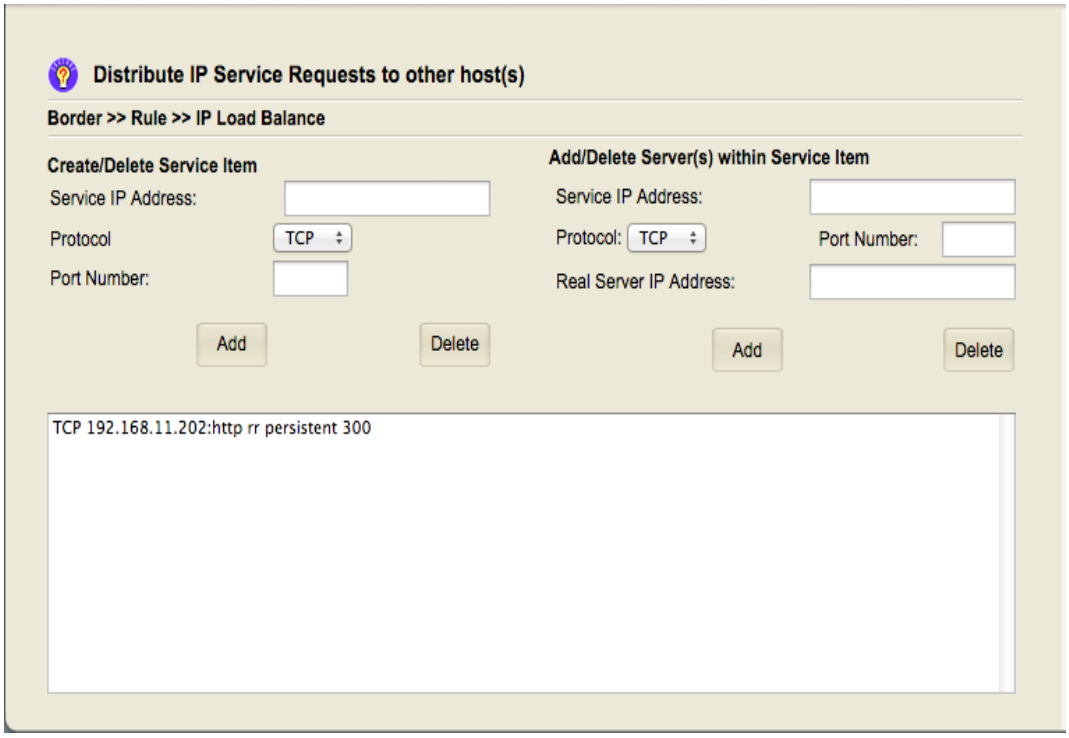



イラスト *57: Load Balance* のためのサービスアイテムを作成する

そして、「ADD」を押してこのサービス項目を追加します。




挿絵 *58:* ロードバランシングの項目リスト

そして、このサービス項目にホスト“172.16.11.201”を追加してください。

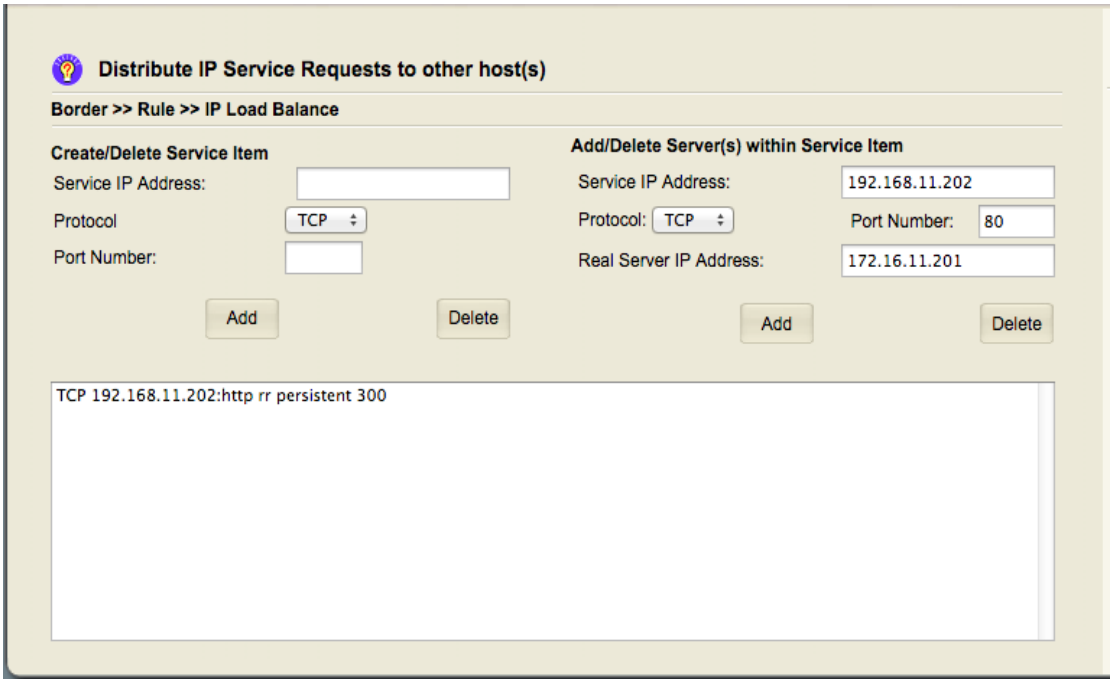
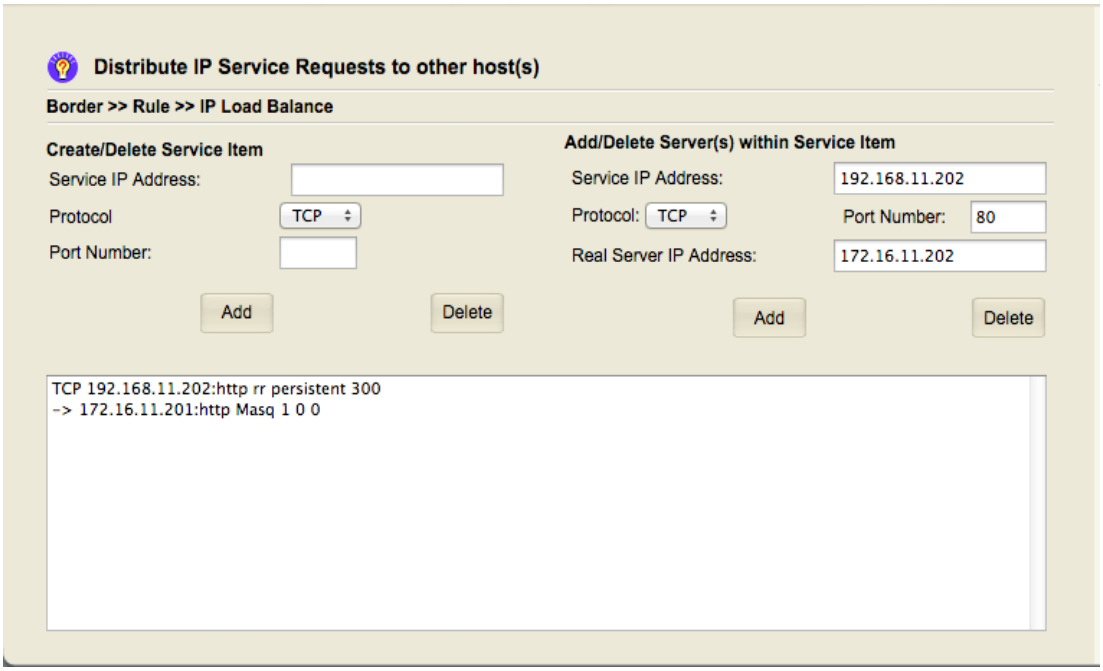
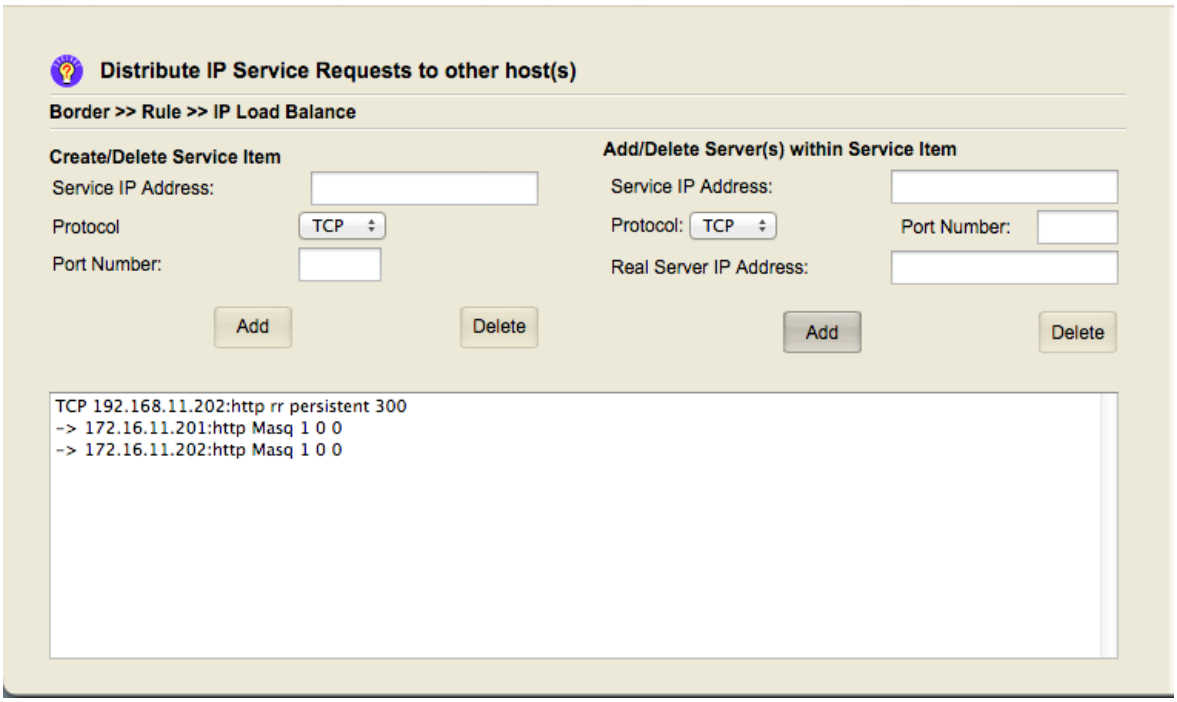



イラスト *59:* サービス アイテムにホストを *1* つ追加してロード バランスを設定する

172.16.11.202”というホストをこのサービスアイテムに追加してください。




挿絵 *60*：サービスアイテムに別のホストを追加してロードバランシング




挿絵 *61*：ロードバランシングのリストにおけるサービス項目のホストの表示

したがって、ホスト“172.16.11.201”および“172.16.11.202”が、“192.168.11.202”に到着する HTTP リクエストを処理しています。

## *Use Web Proxy*

“DNAT”、“ACCEPT”、“DROP”、“REJECT”および“REDIRECT”のといったアクションは、IP アドレス、または TCP/UDP ポート番号に基づいてネットワークトラフィックを操作します。ウェブプロキシの場合、制御は HTTP 自体に固有です。

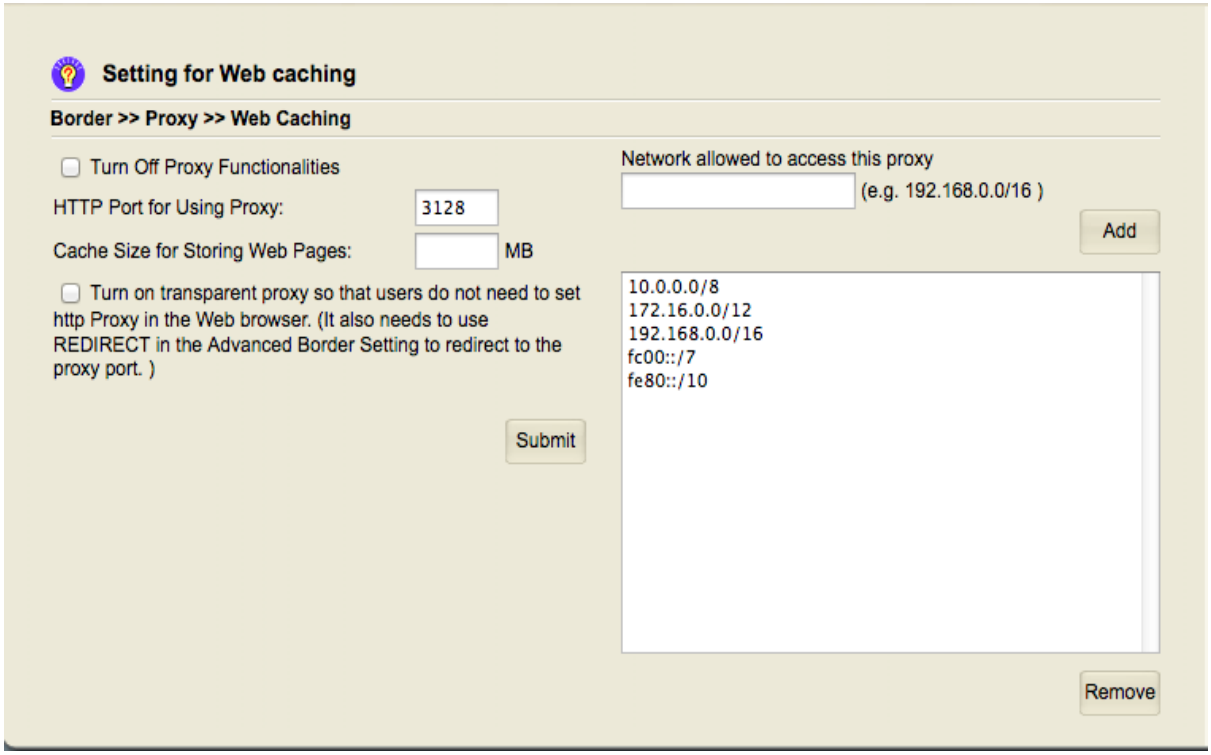
プロキシはクライアントプログラムからリクエストを受け取り、実際のサーバーにそれらを転送し、サーバーから応答を取得して元のクライアントプログラムに送信します。 ウェブプロキシは、以前にロードされたデータをキャッシュしたり、ウェブリンクをフィルタリングしたり、ウェブアクセスの時間帯を制御したりするために使用できます。 「loc」ゾーンから「net」ゾーン（インターネット）へのウェブプロキシを使用する場合の考慮事項はこれらです。

「loc」ゾーン内に複数の内部ホストが存在する場合を想定してください。 「net」ゾーンのユーザーがそれらのホストにアクセスする方法は、デフォルトではブロックされています。しかし、「fw」ゾーンのプロキシへのアクセス手段があれば、「loc」ゾーンのウェブホストへのアクセスが可能になります。なぜなら、「fw」ゾーンから「loc」ゾーンへの接続が許可されているからです。そして、「fw」ゾーンへのアクセスという問題は、「fw」ゾーンのプロキシへのアクセスという問題に帰着します。通常、VPN のみを用いると、一部のウェブホストが VPN のサブネットへのゲートウェイの設定がない場合に解決しないことがあります。ウェブプラットフォーム上で提供されているウェブプロキシは、すべてのネットワークインターフェースでリクエストを受信するように構成されており、ウェブホストへのアクセスは、ウェブプラットフォームからウェブホストにアクセスする場合と同様になります。これにより、ルーティングテーブルの設定の問題を回避できます。

ウェブプロキシを使用する理由としては、例えば、一部の古い Web アプリケーションが特定の IP アドレスからの接続のみを受け入れる場合がある。大規模なユーザーへのアクセスを、アプリケーションを変更せずに実現するために、ウェブプロキシを使用して古い Web アプリケーションにアクセスすることは、良いアプローチとなる可能性がある。次のセクションでは、ベースプラットフォームで提供されているウェブプロキシの設定を変更する方法を紹介する。

## *Web Caching*

ウェブプロキシは、デフォルトではベースプラットフォーム上で TCP ポート 3128 で動作しています。また、「Border >> Proxy >> Web Caching」で変更できます。



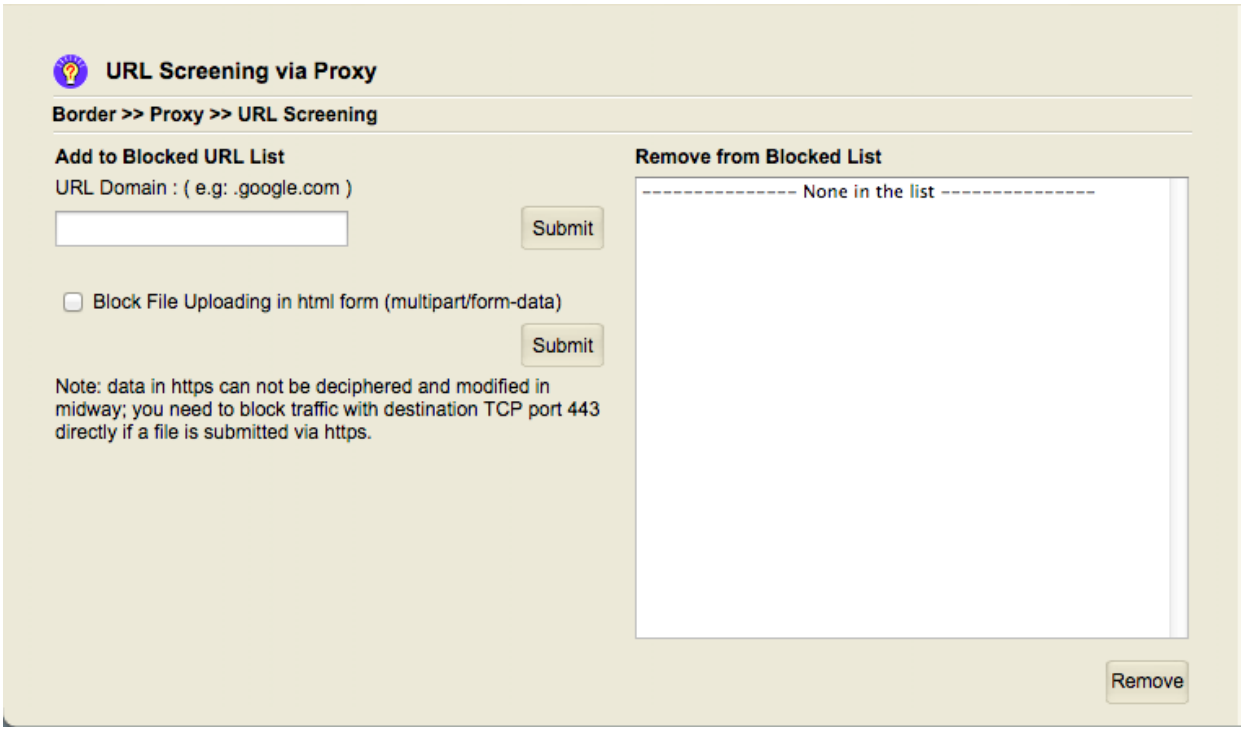

挿絵 ***62:*** ウェブプロキシキャッシュおよびアクセス画面スナップショット

ウェブプロキシを使用するには、ブラウザの設定を変更する必要があります。
“REDIRECT”アクションからポート 80 をこのプロキシポートにリダイレクトする場合、これは“Transparent Proxy”と呼ばれ、ユーザーにウェブブラウザのプロキシ設定を変更してもらう必要はありません。

そして、このプロキシにアクセスできるネットワークは、右側のボックスに設定されています。必要に応じて制限を変更することができます。

## *URL Screening*

もしウェブプロキシが使用されている場合、「Border >> Proxy >> URL Screening」にてブロックするURLのリストを追加できます。

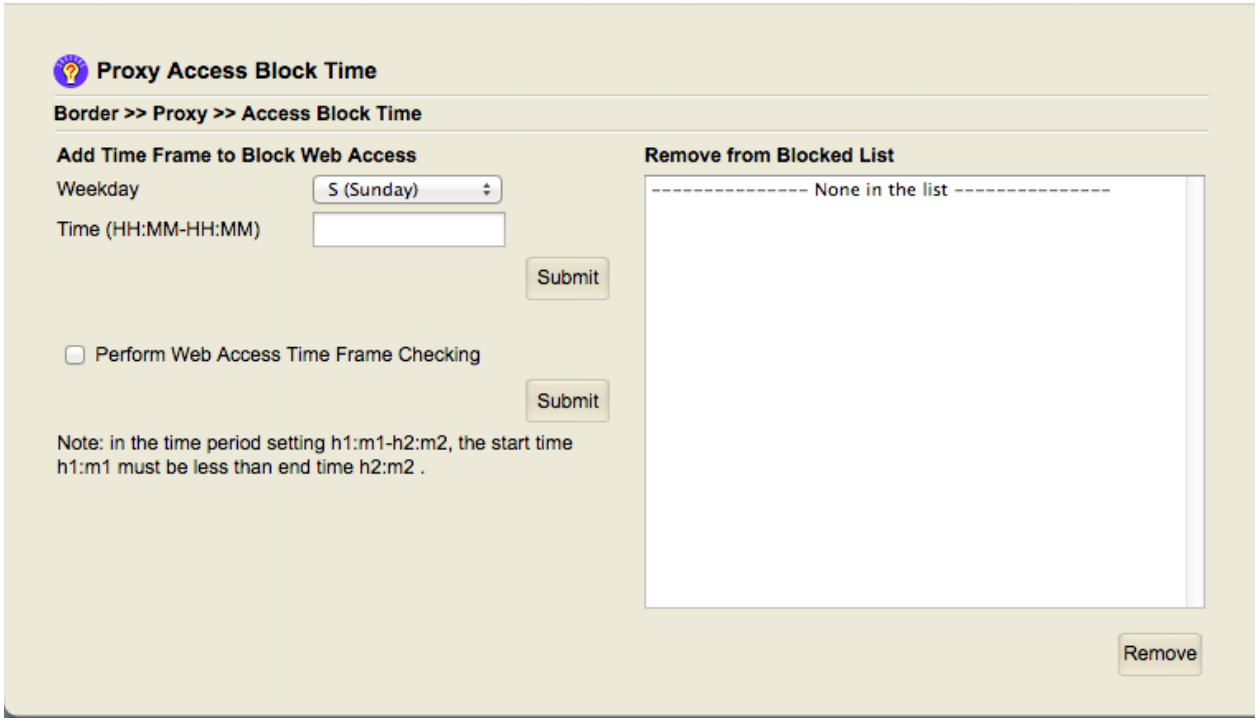



挿絵 ***63:*** ウェブプロキシにおける ***URL*** フィルタリング

HTMLフォームによるファイルアップロードもブロックできます。ただし、HTTPSのデータは証明書に関連付けられた鍵なしには解読できないため、HTTPSのトラフィック全体をブロックする必要があります。

アクセスブロックタイム

ウェブアクセスをプロキシ経由で特定の時間枠でブロックすることができます。




挿絵 ***64:*** ウェブプロキシでの ***HTTP*** アクセスをブロックするためのタイムスロット設定

たとえば、毎週月曜日の 08:00 から 12:00 の時間帯では、HTTP の使用が禁止されます。「Time」の欄には“08:00-12:00”と入力し、「Weekday」の欄で“M(Monday)”を選択してください。

## *Traffic Bandwidth Control*

ネットワークトラフィックの帯域幅を調整するために、以下の手順に従って設定を行います。物理ネットワークインターフェースでの制限を設定し、そのインターフェースのトラフィックをいくつかのグループに分類し、各グループに対して制限と優先度を設定し、その後、ソース、宛先、TCP/UDP ポート番号に基づいてパケットをグループ化します。

例えば、インターフェース “eth0” のインバウンドおよびアウトバウンド帯域幅を 100 Mbits/秒に制限し、トラフィックを 4 つのクラスに分類します。

クラス 1：最高優先度（優先度 1）
the minimum rate is 100 kbits/sec,
そして、最大許容量は 180 kbits/sec です。

クラス 2：2 番目の優先度で
the minimum rate is ¼ of the total bandwidth of the interface,
そして、最大許可される帯域幅は、帯域幅のフルバンド幅です。

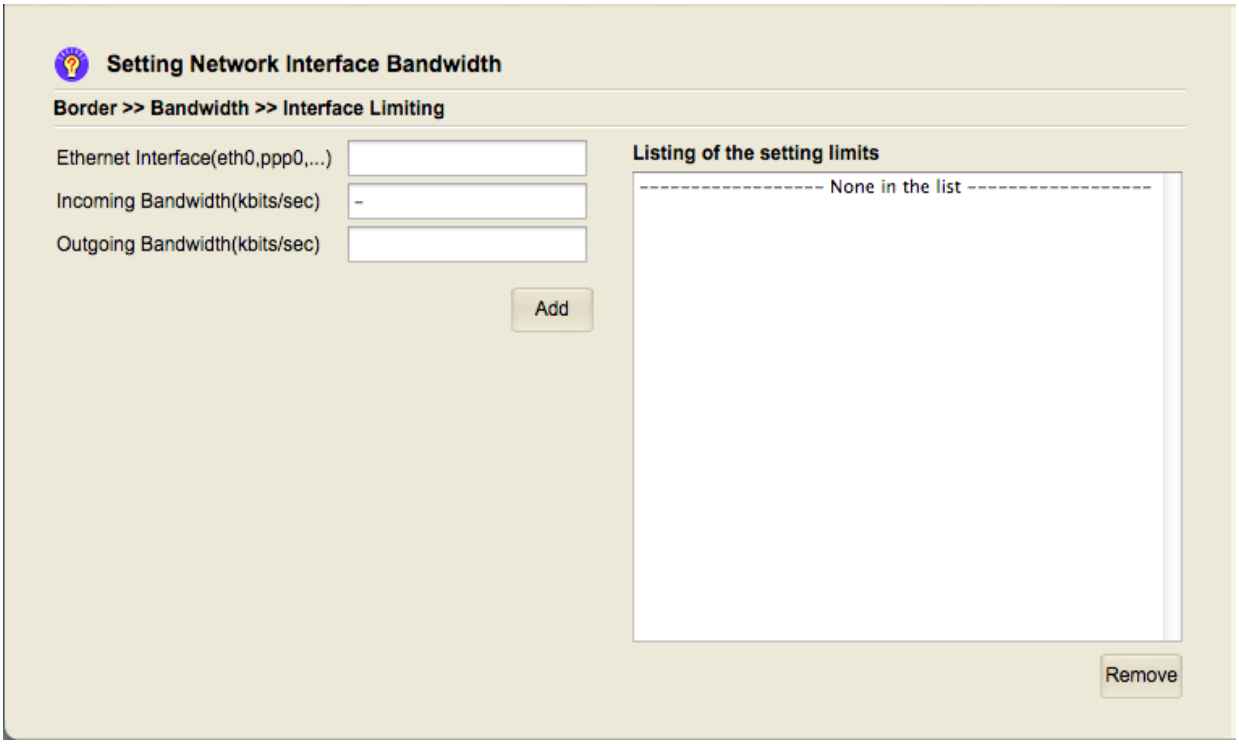
クラス 3：第 3 の優先順位で、
the minimum rate is ¼ of the total bandwidth,
そして、最大許可される帯域幅は、フル帯域幅です。

クラス 4：4 番目の優先度
the minimum rate is 1/8 of the total bandwidth,
そして、最大許可される帯域幅は全体の 80%である。

しかし、どのようなトラフィックを「クラス 1」、「クラス 2」、「クラス 3」、「クラス 4」としてマークすべきでしょうか？マークは、ネットワークパケットのいくつかの属性、例えばソース、宛先、TCP/UDP ポート番号に基づいて行われます。ネットワークパケットが指定したものでない場合、"クラス 3"としてマークされます。これは、ネットワークトラフィックの帯域幅設定の粗い調整に相当します。

以下のセクションでは、詳細な手順が “Border >> Bandwidth >> Interface Limiting”、 “Border >> Bandwidth >> Priority Classes”、および “Border >> Bandwidth >> Traffic Prioritizing” で紹介されます。

ネットワークインターフェースの帯域を設定する

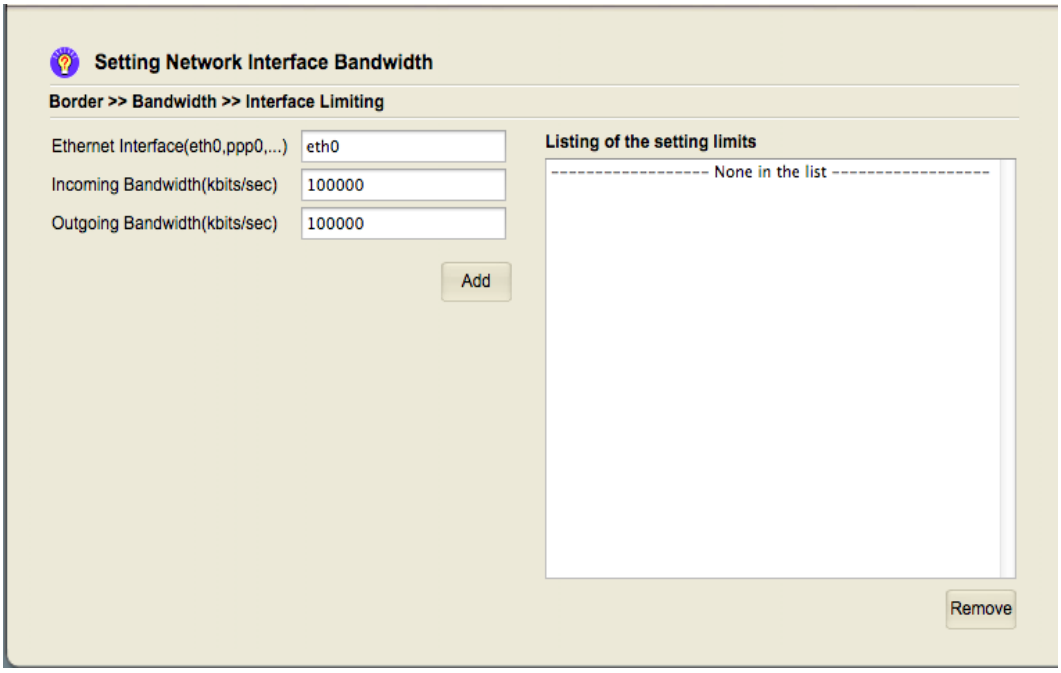



挿絵 ***65:*** ネットワークインターフェース帯域幅の設定 ***(Shasai 65: Netwokku inteppa-su biyou-fuku no settei)***

「Border >> Bandwidth >> Interface Limiting」の設定により、Ethernet インタフェースのインバウンド帯域とアウトバウンド帯域を規制できます。Ethernet インタフェースのハードウェア仕様において、インタフェースの帯域は通常、「1000Mb/s」、「100Mb/s」、または「10Mb/s」という値で提供されます。これは、自動交渉から選択された値です。ここで設定する内容は、その値を変更するのではなく、Ethernet インタフェースから送信または受信するフレームの数を決定するための制御プロセスです。

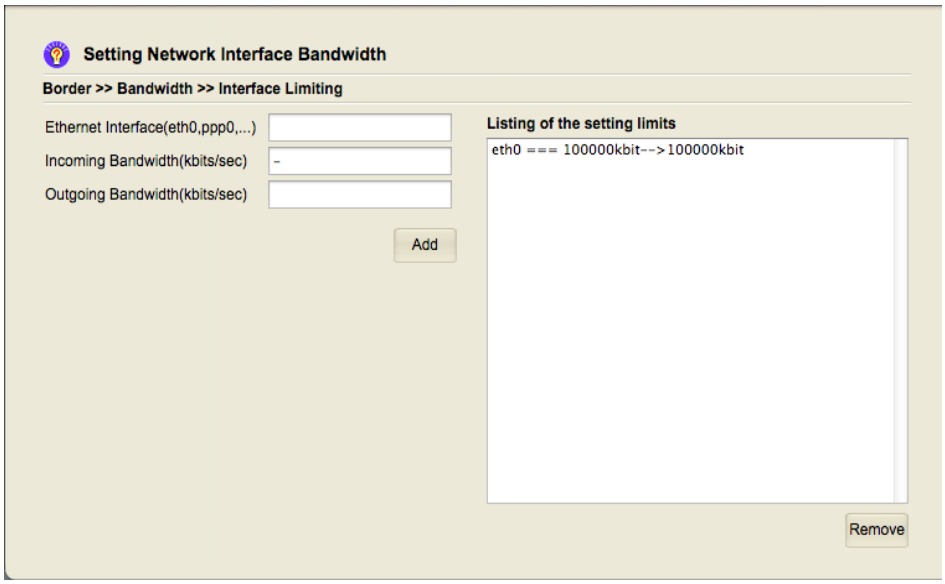
インバウンド帯域幅の設定において、ネットワークフレームは既にイーサネットインターフェースによって受信されています。したがって、ベースプラットフォームがそれらを処理する前に、受信したパケットを一部削除することでのみ、インバウンド帯域幅を規制することができます。受信したトラフィックを廃棄することは、他の端でそれらを再度送信する必要があることを意味します。上層アプリケーションの有効な帯域幅は、はるかに低くなる可能性があります。

以下の例は、入出バッファードを 100 Mbits/sec に設定するものです。注意して、この数値は kbits/sec の単位に変換する必要があります。



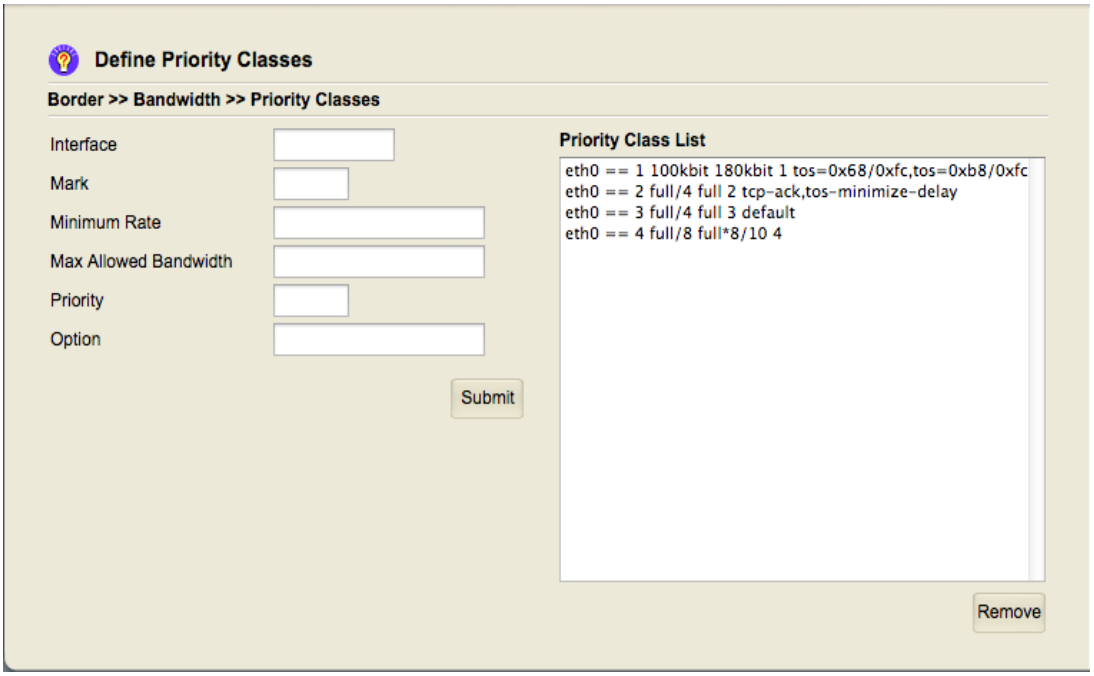

挿絵 ***66:*** インバウンドおよびアウトバウンド帯域幅の設定

「Add」ボタンを押すと、右側のボックスには以下が表示されます。




挿絵 ***67:*** インターフェース帯域幅を設定後の画面スナップショット

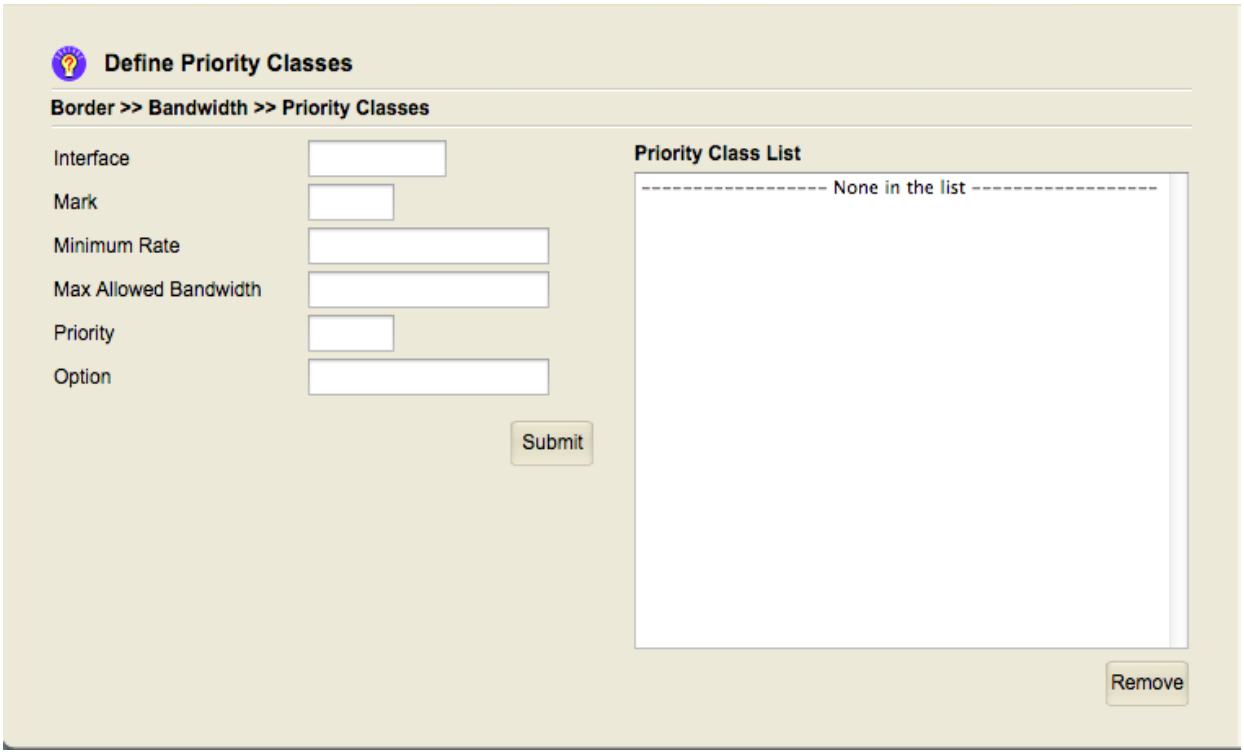
同時並行して、4 つの優先度クラスが自動的に作成されます。それらは「Border >> Bandwidth >> Priority Classes」で確認できます。




挿絵 ***68:*** インターフェース帯域制限を設定後の優先度クラス

設定は、アプリケーションに合わせて変更される場合があります。 画面のキャプチャにある「3」がデフォルトクラスです。 どのような変更をしても、ネットワークトラフィックに対してデフォルトクラスが存在する必要があります。 そうしないと、ボーダーエンジンが正常に起動しません。

## *Define Priority Classes*




挿絵 ***69:*** 優先クラスを定義するためのスクリーンショット

前述したように、帯域幅が設定された後、4 つの優先度クラスが作成されます。設定はその後変更可能です。フィールド“Mark”は整数で 1～255 の範囲、フィールド“Priority”は整数で 1～65535 の範囲です。

“Option”のフィールドは、次のいずれかになります。

default:
明示的にマークされていないトラフィックのクラスを示す

tos=0xvalue/0xmask: tos=0xvalue/0xmask:
this is to define a class by selecting IP packet's TOS/Precedence/DiffSev Octet.

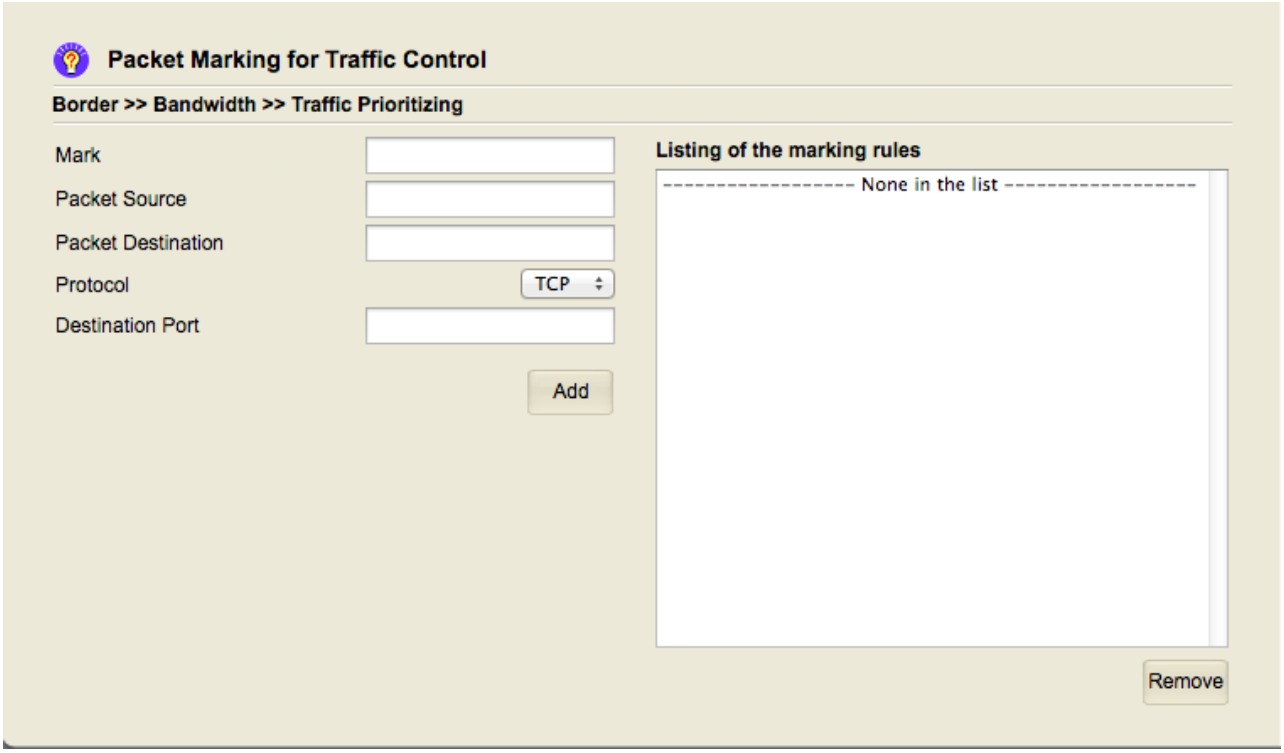
tos-tosname:
The following “tosnames” are used to represent some 関連マスクの TOS 値のリスト

tos-minimize-delay 0x10/0x10
tos-maximize-throughput 0x08/0x08
tos-maximize-reliability 0x04/0x04
tos-minimize-cost 0x02/0x02
tos-normal-service 0x00/0x1e

tcp-ack:
This is for all the TCP-ack packets.

パケットマーキングによるトラフィック制御

優先クラスが事前に定義されたので、それぞれの優先クラスの詳細なコンテンツを指定できます。

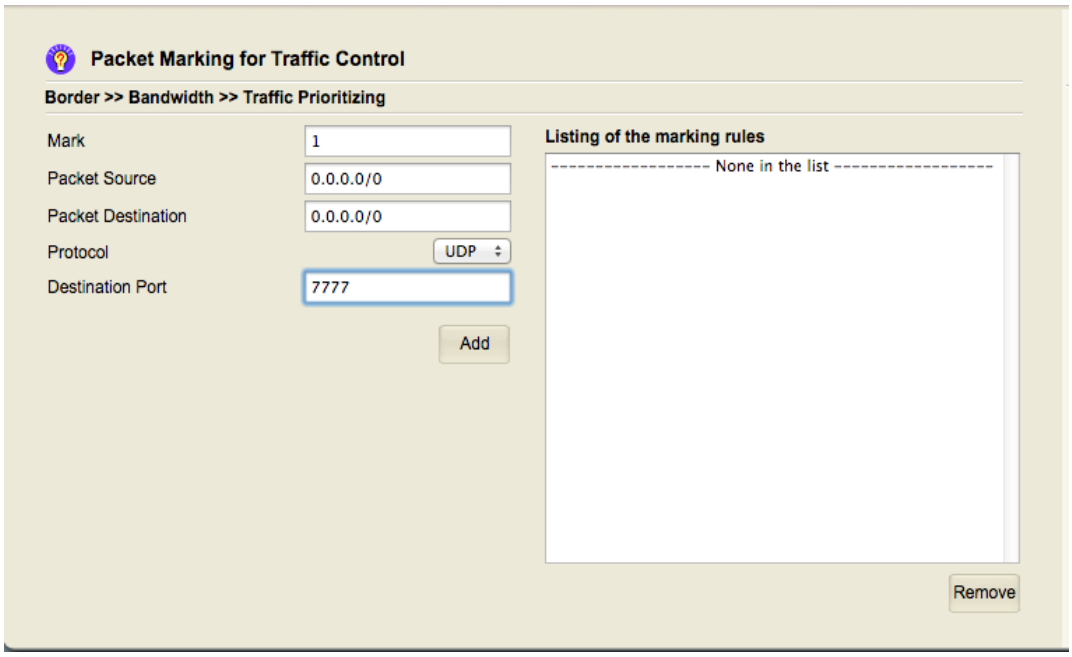



挿絵 ***70:*** 交通優先制御のスクリーンショット

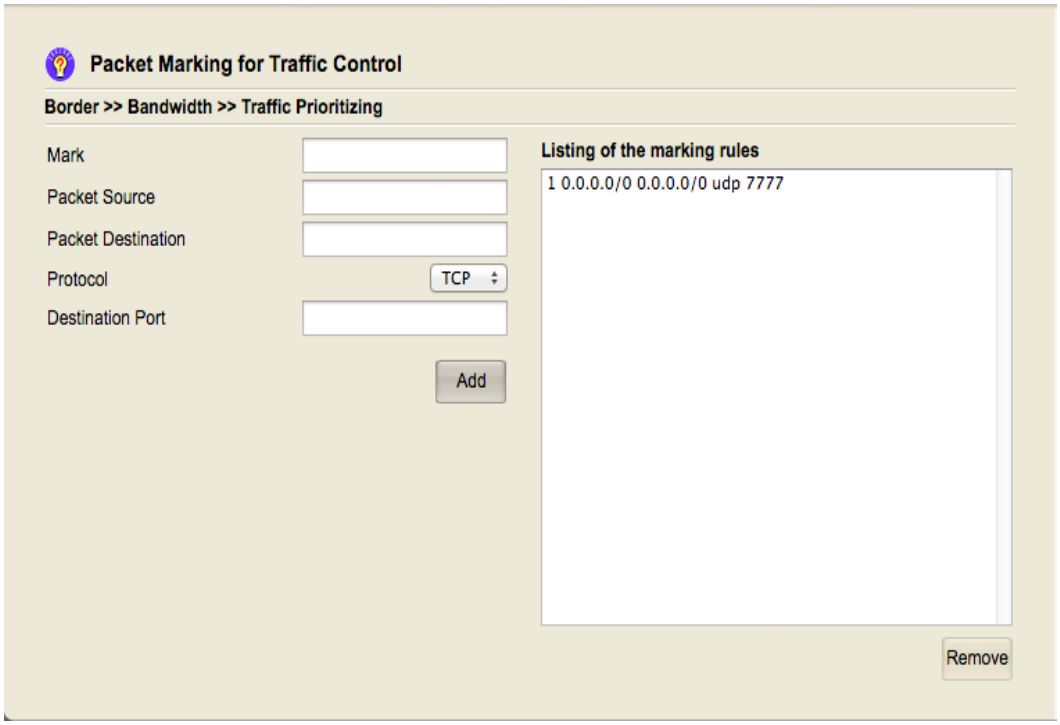
例えば、サイト間VPNトラフィック（UDPポート7777を想定）を優先させたい場合、以下の手順で設定します。

Mark: 1
**Packet Source**: 0.0.0.0/0
パケット宛先: 0.0.0.0/0
**Protocol**: UDP
宛先ポート：7777

この意味は：どこからでも（0.0.0.0/0）どこへでも（0.0.0.0/0）UDP ポート 7777 のトラフィックは“1”でマークされます。そして、以前のセクションで、Ethernet インターフェースを設定した後で 4 つの優先度クラスが作成されています。マーク“1”のネットワークパケットは、最も高い優先度（優先度番号は“1”）で、最大許容帯域幅 180 kbits/sec です。




挿絵 ***71:*** 交通優先のためのマークの設定



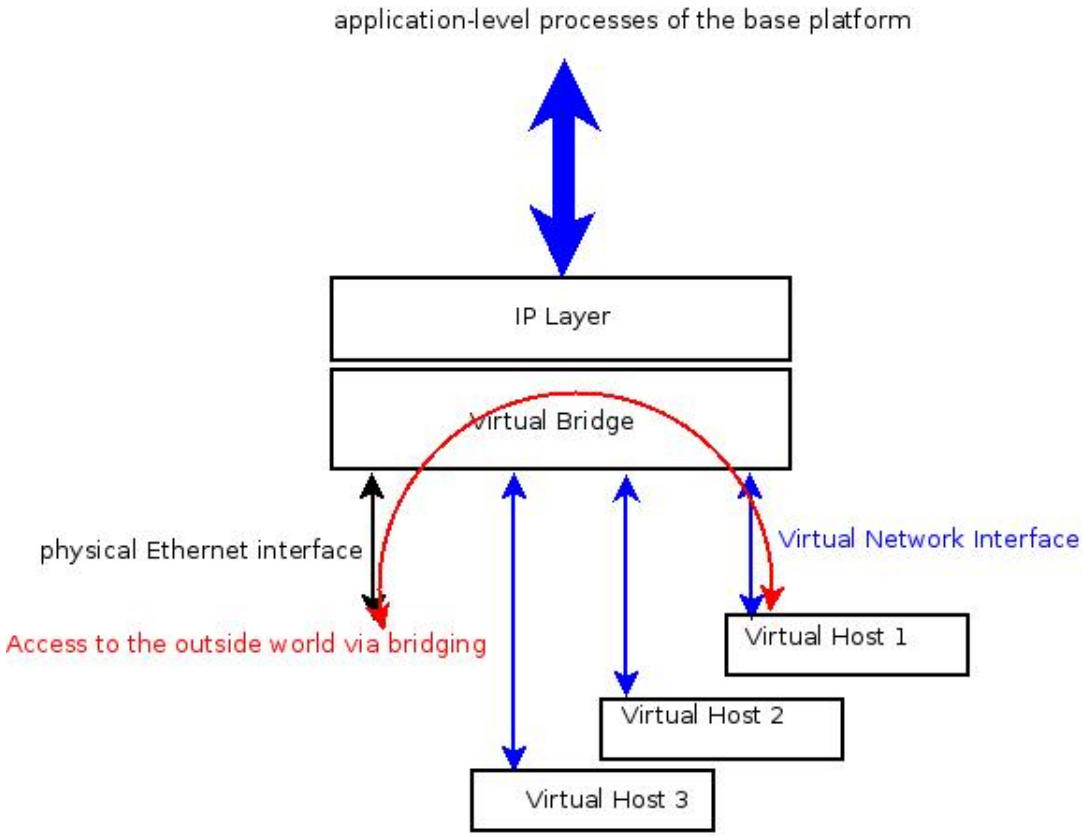

挿絵 ***72:*** マーク ルーティングリスト

ネットワークトラフィックを優先することは、帯域幅が非常に限られている場合に、非常に混雑したチャネルでネットワークトラフィックを優先するために使用されます。しかし、それらをうまく定義することは容易ではありません。上記の例では、上位優先度のトラフィックの最小レートは 100 kbits/sec で、最小接続を維持するために設定されています。最大帯域幅は 180 kbits/sec で、このサイト間 VPN で実行されているアプリケーションには十分ではありません。ただし、最大帯域幅が大きすぎると、他のアプリケーションが圧迫される可能性があります。したがって、設定は、環境における利用パターンに大きく依存します。

帯域の使用制限は通常、システムが乱用されている場合に発生し、特定のエリアからの使用を制限する必要がある場合に起こります。

## *The Components of a Bridge*

冒頭のセクションでは、「ブリッジ」という基本的なユニットのネットワークオペレーションについて言及しています。仮想ホストのネットワークインターフェースが他のホストにアクセスする際に、ブリッジに接続します。また、「net」「loc」「fw」「dmz」のゾーン定義においては、ブリッジの境界線を用いて、全体をこれらの領域に分割します。そして、ベースプラットフォームの IP アドレスはブリッジデバイスの上位に設定され、他のホストがこれらの IP アドレスを使用してベースプラットフォームにアクセスできるようにします。

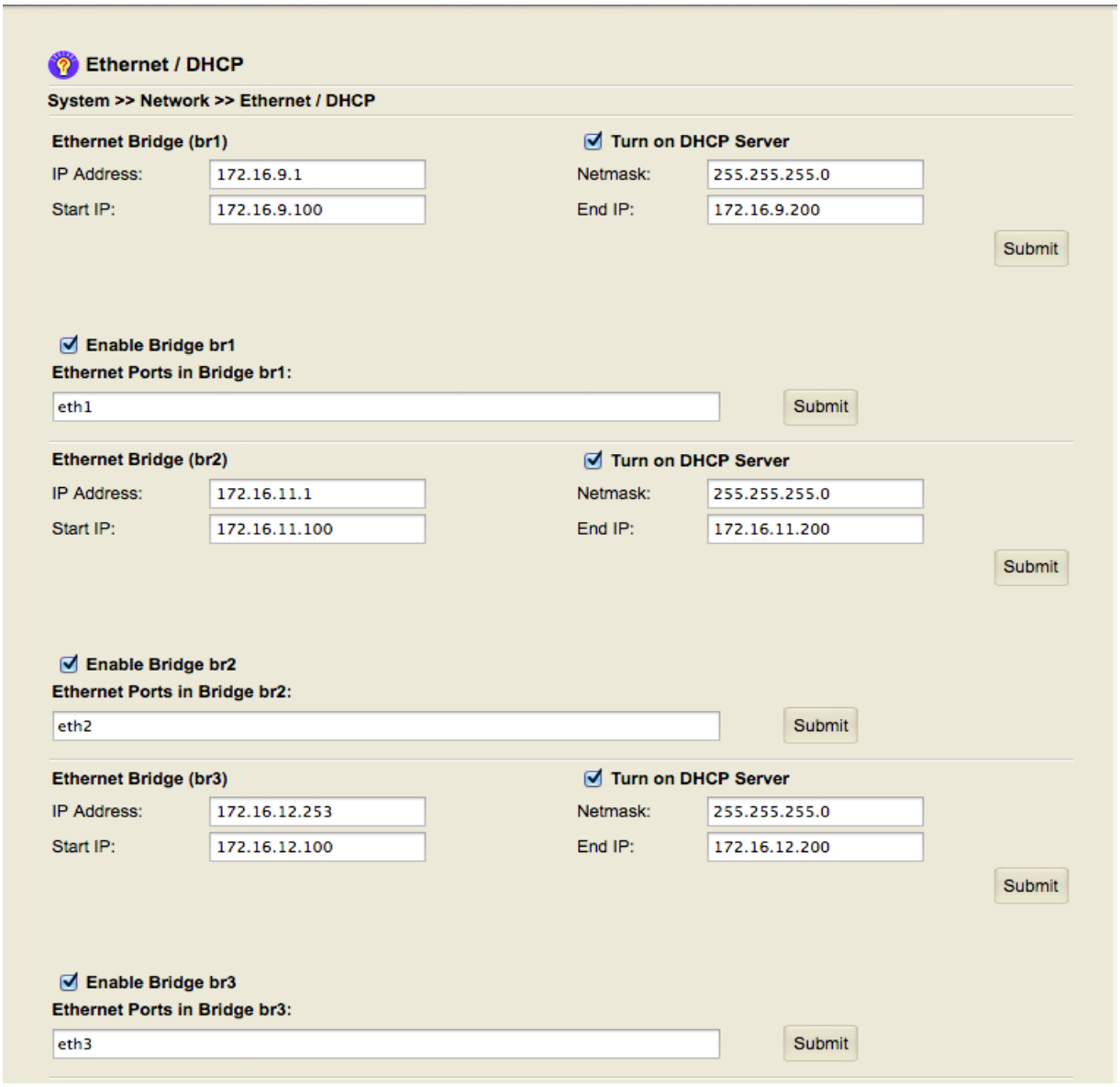



挿絵 ***73:*** ブリッジ、ベースプラットフォーム、物理的なイーサネットインターフェース、および仮想ホスト間の関係

ベースプラットフォームには“br0”、“br1”、“br2”、“...”といった 12 個のブリッジがあります。“eth0”、“eth1”、“...”といったイーサネットインターフェースは、物理エンティティとの接続に使用され、ネットワークデバイス“tap0”、“tap1”、“...”は、VPN でブリッジモードおよび仮想ホストで使用されます。

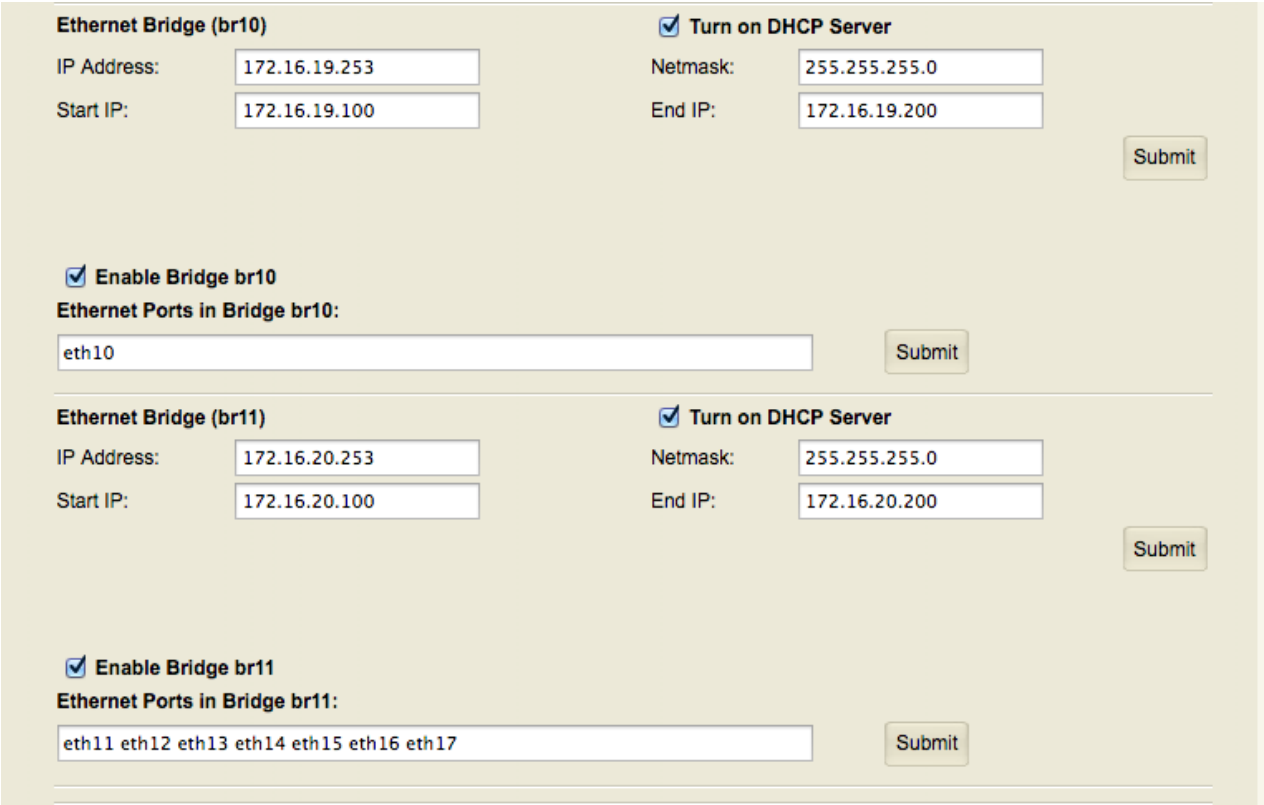
ブロードネットワークの物理エンティティが 1 つのブリッジに存在することは可能ですが、それは非効率的です。現代のハードウェアでは、スイッチのブリッジ使用分のみの費用が、ルーターの分よりも安価であるため、その他の具体的な使用目的がない限り、物理インターフェイスをルーターとして機能させる方が良いでしょう。

設定は「**System >> Network >> Ethernet / DHCP**」から変更できます。「eth0」は“br0”になっている必要があります – これは変更しないでください。そして“br0”は WAN デバイス（“net”ゾーン）で使用され、パブリック IP アドレスを持っています。それ以外のものは、以下のスクリーンショットに示すように調整できます。




DHCP サーバーは、そのアドレス プールとともにお啟用/停止できます。

執筆時点では、ベースプラットフォーム上のブリッジの数は 12 であり、どのような数の物理イーサネットインターフェースが新たに存在しても変わりません。物理イーサネットインターフェースの数が 12 を超えるハードウェアがある場合は、それらを 1 つのブリッジにまとめることを推奨します。

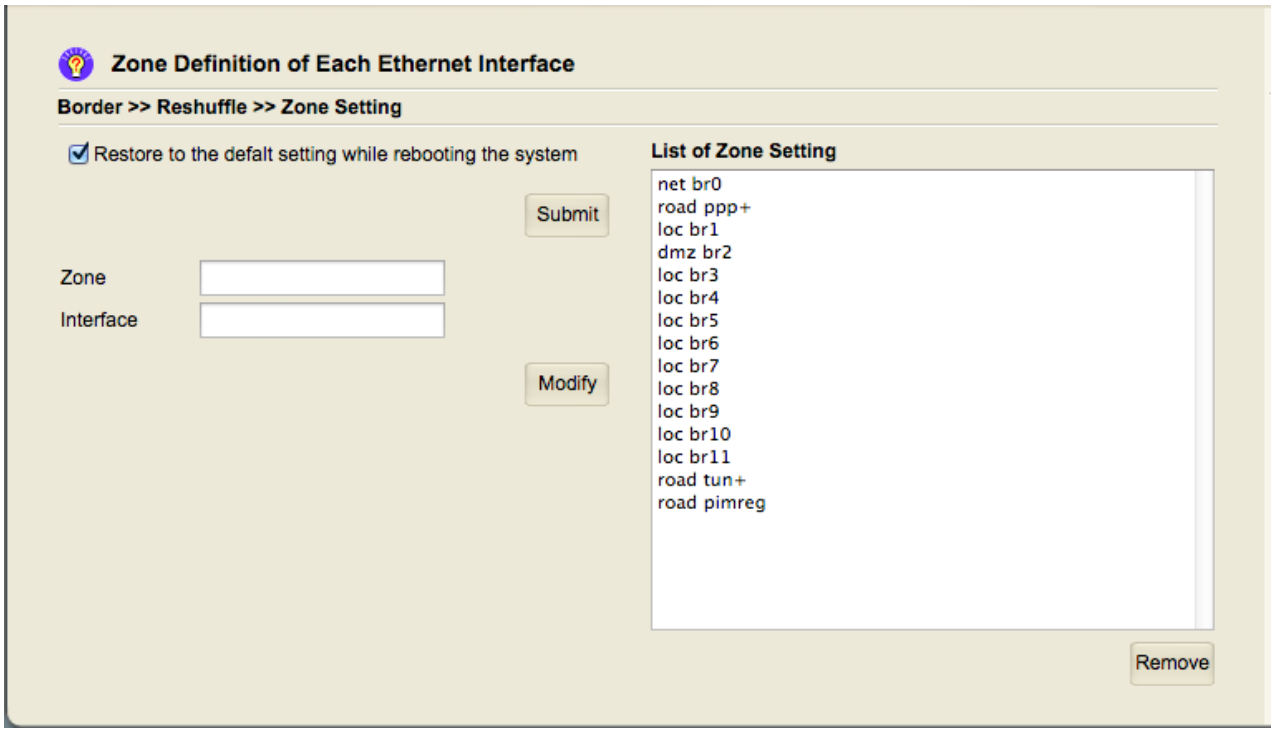



挿絵 ***74:*** 複数のイーサネットインターフェースを物理エンティティと ***1*** つのブリッジに配置する

“net”、“loc”、“dmz”に関連付けられたゾーンの定義は、次のセクションに記載されています。

## ゾーン定義

以下のスクリーンショットは、ネットワーク運用で使用するゾーンを示しています。「net」「loc」「dmz」「road」というゾーンがあります。「fw」というゾーンは、「fw」が基盤プラットフォーム自体のネットワーク的なものを示すため、リストには含まれていません。

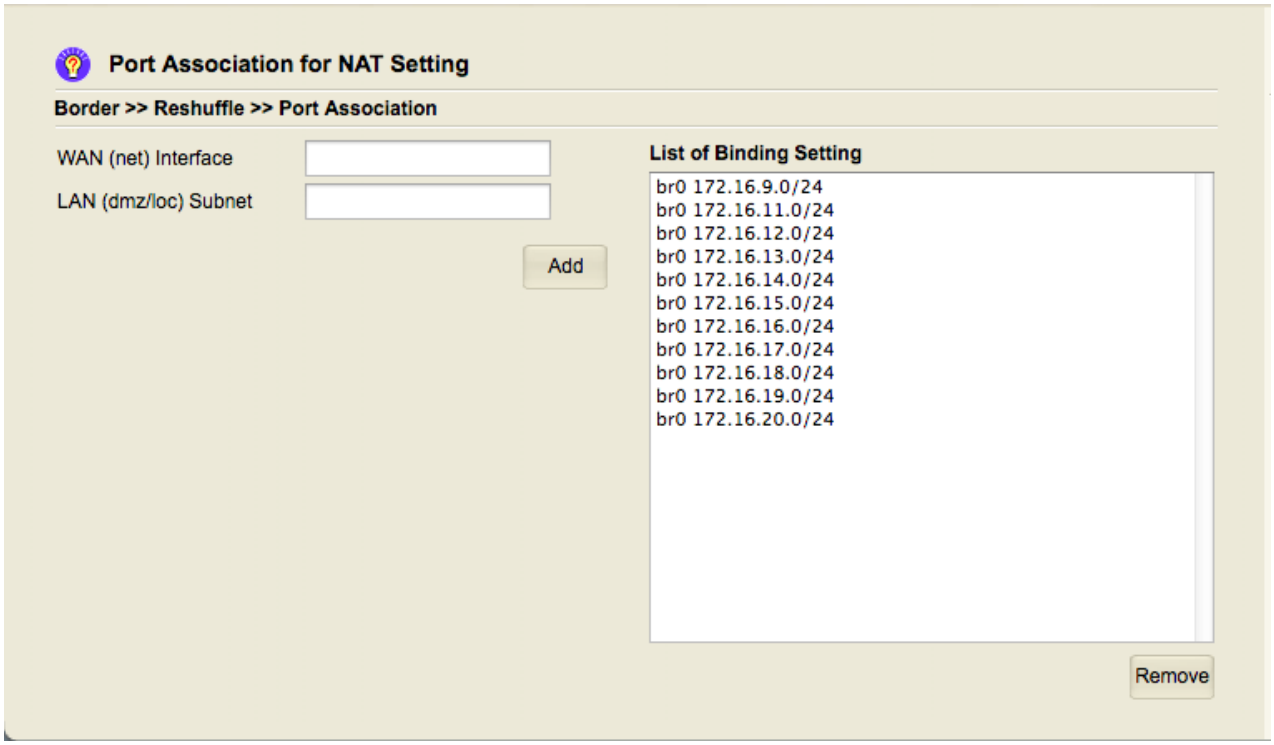



挿絵 ***75:*** ゾーン設定のキャプチャ

しかし、もし上部のボックスがまだ「チェック」されている場合、再起動後にデフォルト設定に復元されます。もしご自身でよくご検討した上で、そのボックスを「アンチェック」してください。

## *Port Association for NAT Setting*

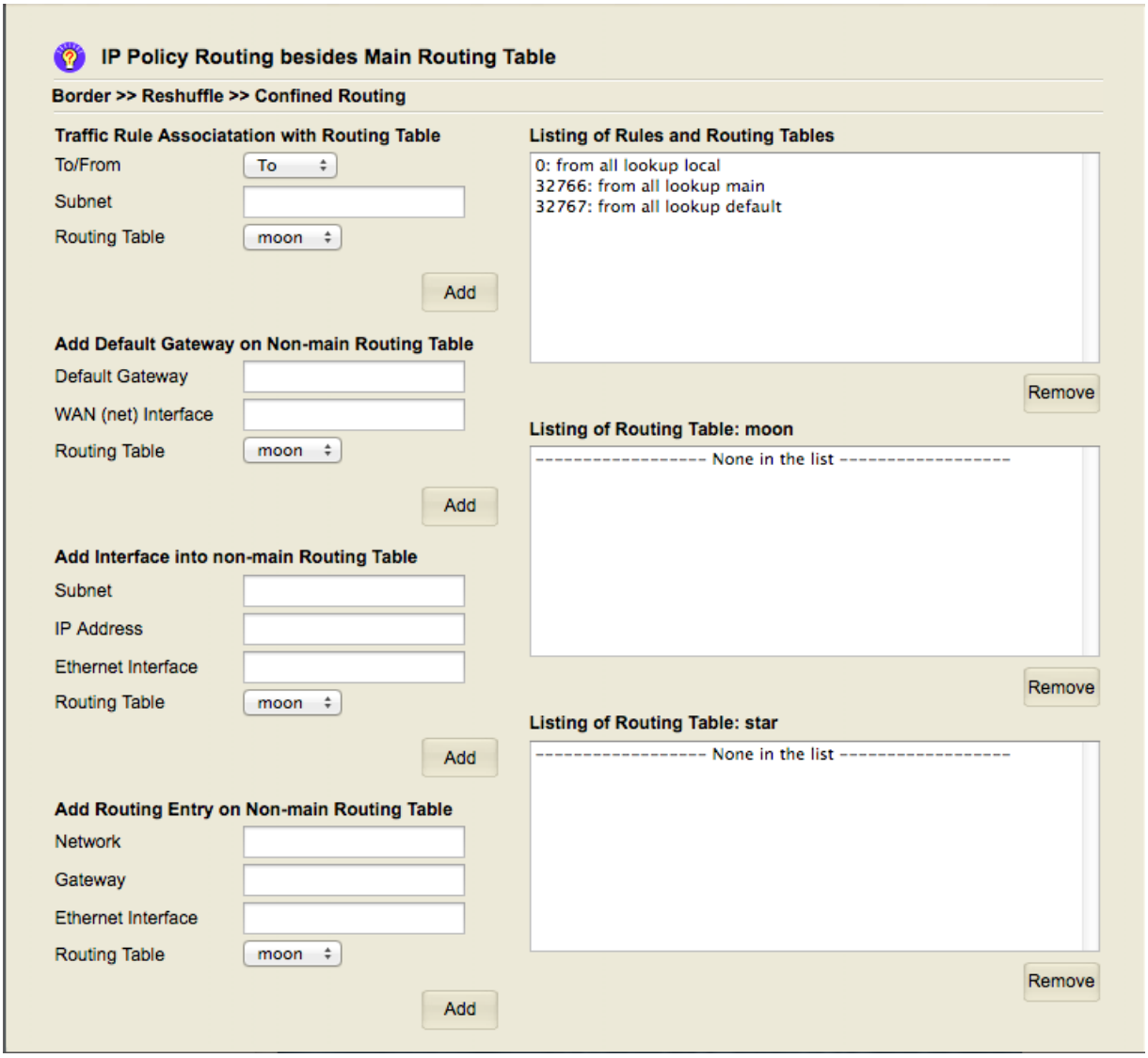
ネットワークパケットがベースプラットフォームの外部世界に境界を越えて通過するかどうかは、「Border >> Reshuffle >> Port Association」の設定によって決定されます。




挿絵 ***76: NAT*** 設定

“br1”が接続しているサブネットは“172.16.9.0/24”です。したがって、そのサブネットからゾーン“net”へのトラフィックは、IP アドレスを“br0”の IP アドレスに置き換えます。同様に，“172.16.11.0/24”が“br2”が接続しているサブネットであり，“br3”は“172.16.12.0/24”に接続します。“br11”はサブネット“172.16.20.0/24”に接続します。それらのサブネットからのトラフィックは“NAT'd”されます。

## *IP Policy Routing*

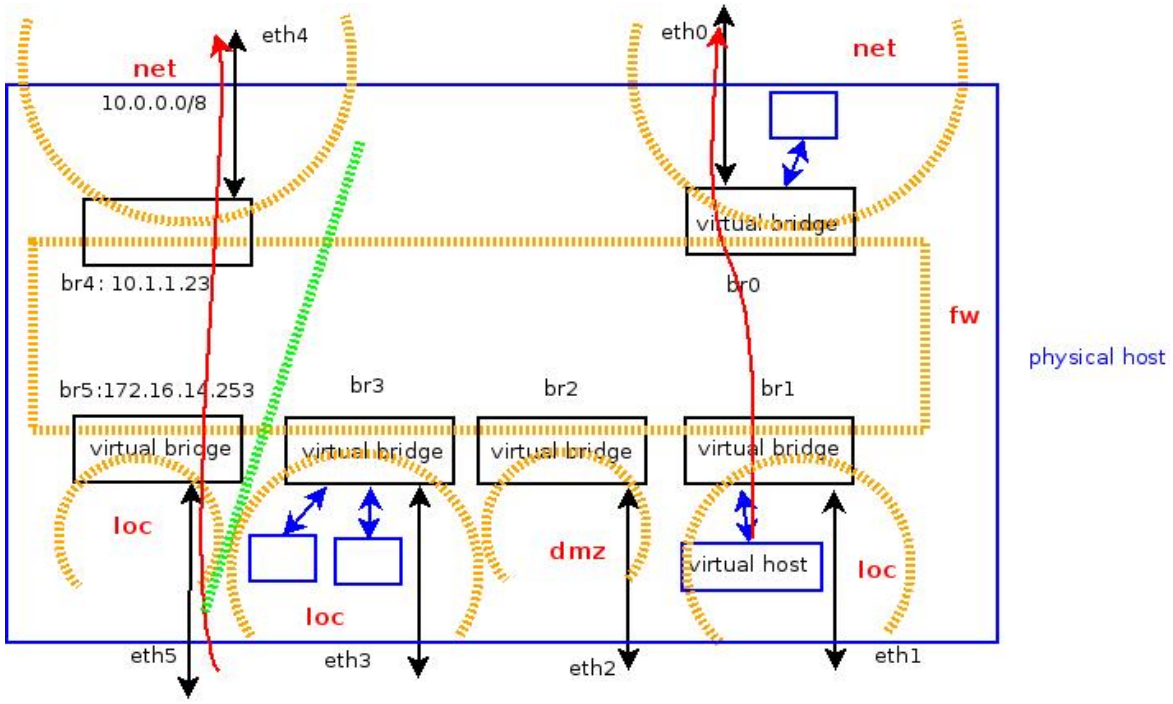



挿絵 ***77: IP*** ポリシー ルーティング に関する情報

ルーティングとは、簡単に言えば、IP ヘッダーの内容を確認し、ルーティングテーブルをチェックしてパケットの行き先を決定することです。IP トラフィックは通常、メインのルーティングテーブルに従って転送されます。ベースプラットフォームには、「moon」と「star」という 2 つの追加ルーティングテーブルがあります。IP ポリシールーティングとは、特定の種類のネットワークトラフィックを選択し、それらの追加ルーティングテーブルに従って転送する動作を指します。

それらのプロセスは、「Border >> Reshuffle >> Confined Routing」の設定で行うことができます。 右側の 3 つのテーブルが表示されます。 上にある最初のテーブルは、特定のサブネットへのトラフィックを/から処理するために、「main」、「moon」、または「star」というルーティングテーブルに従う必要があることを示しています。 右下の 2 番目と 3 番目のテーブルは、「moon」と「star」ルーティングテーブルの内容です。 「main」ルーティングテーブルの内容は、「System >> Network >> Static Routing」で確認できます。 以下の例が、これらの機能の使用方法を示しています。

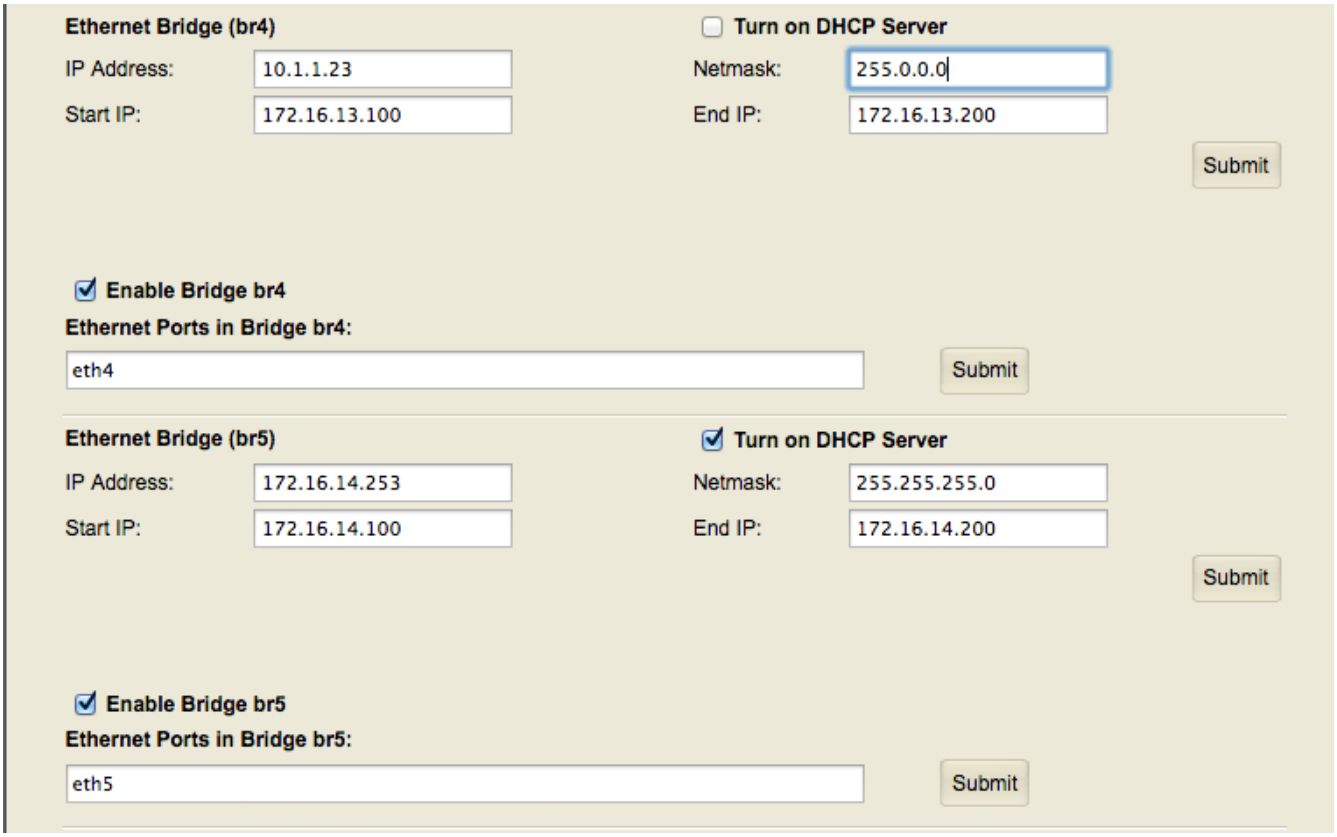
以下の情報は Azblink マニュアルから抽出されたものです。 私たちは IP ポリシールーティングを使用して、プラットフォームを以下のように構成します。ゾーン“net”には“br0”と“br4”という 2 つのブリッジがあり、“br0”はインターネットに接続され、“br4”は“10.0.0.0/8”というサブネットに接続されます。“br4”は“172.16.14.0/24”というサブネットに“172.16.14.253”という IP アドレスで接続されます。 “10.0.0.0/8”というサブネットを使用するために、ISP は“10.1.1.23”という IP アドレスとデフォルトゲートウェイ“10.1.1.1”、ネットマスク“255.0.0.0”を要求します。私たちは“172.16.14.0/24”というサブネットに機器を配置し、それらの機器は ISP のプライベートネットワーク“10.0.0.0/8”にあるサーバーに接続するようにしたいと考えています。しかし，“172.16.14.0/24”は私たちのサブネットであるため、ISP は“172.16.14.0/24”からのソース IP アドレスを持つトラフィックをルーティングしません。したがって，“172.16.14.0/24”から“10.0.0.0/8”へのトラフィックは、“br4”の IP アドレスを使用して NAT によって行われます。




挿絵 ***78: WAN*** ポートの二つの例

ここでは 1 つの質問をします：なぜ“br4”をゾーン“net”に置きたいのでしょうか。理由は、たとえ ISP のプライベートサブネットであっても、他の顧客もそこにいるからです。そのため、他の部分のシステムは通常通りに機能し、“br4”と“br5”のサブネットをシステム全体から隔離したいと考えています。

それでは、以下の設定に進みます。

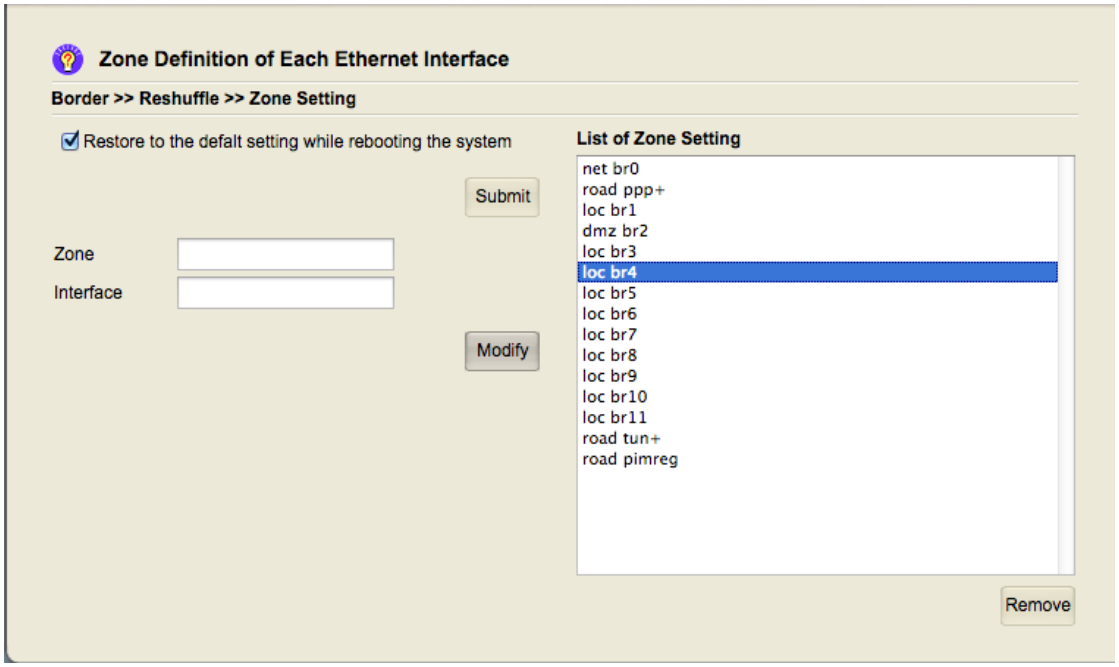



挿絵 ***79:*** 橋の ***IP***アドレスを変更する

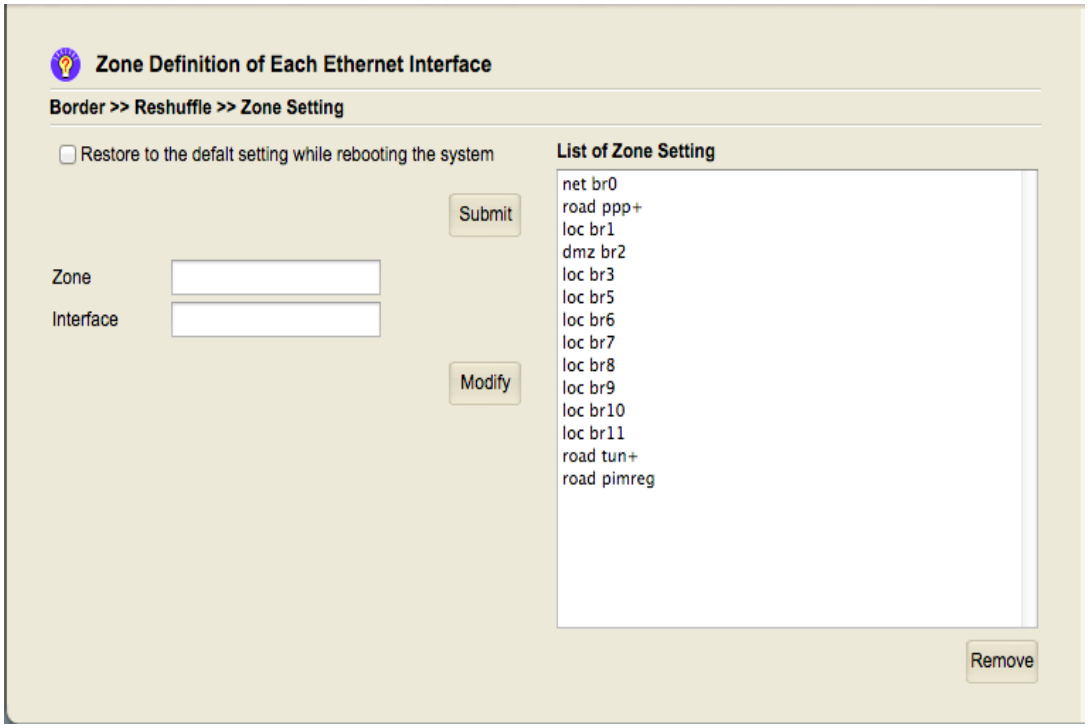
まず、”br4”の IP アドレスは、ISP からの割り当てに従って変更する必要があります。“System >> Network >> Ethernet / DHCP”から行うことができます。システムを再起動することで有効になります。

“br4”は「net」ゾーンに属するように変更する必要があります。“Border >> Reshuffle >> Zone Setting”で、それを「loc」ゾーンから削除し、「net」ゾーンに追加します。リブート後にデフォルト設定に戻らないように、一番上のチェックボックスを解除してください。

以下のスクリーンショットは、”loc” から “br4” の削除を示すものです。

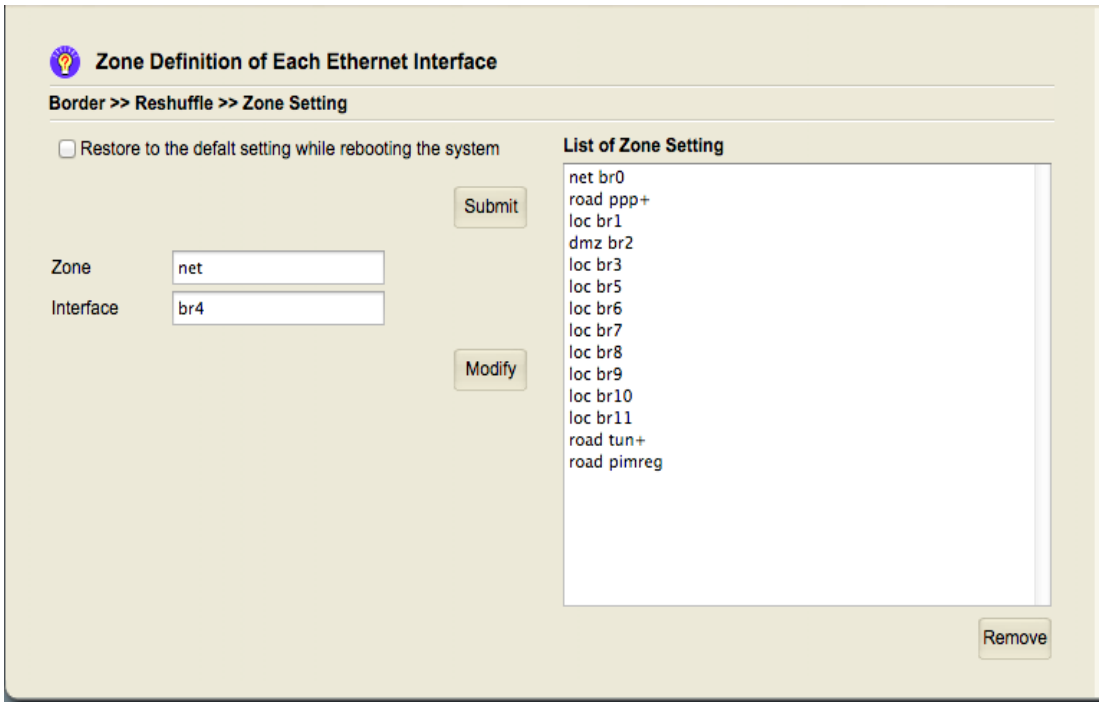



挿絵 ***80:*** 「***br4***」をゾーン「***loc***」から削除する




挿絵 ***81:*** 「***br4***」をゾーン「***loc***」から削除した後のリスト

以下の画面のキャプチャは、「br4」をゾーン「net」に追加する際に使用されます。




挿絵 ***82:*** 「***br4***」をゾーン「***net***」に追加

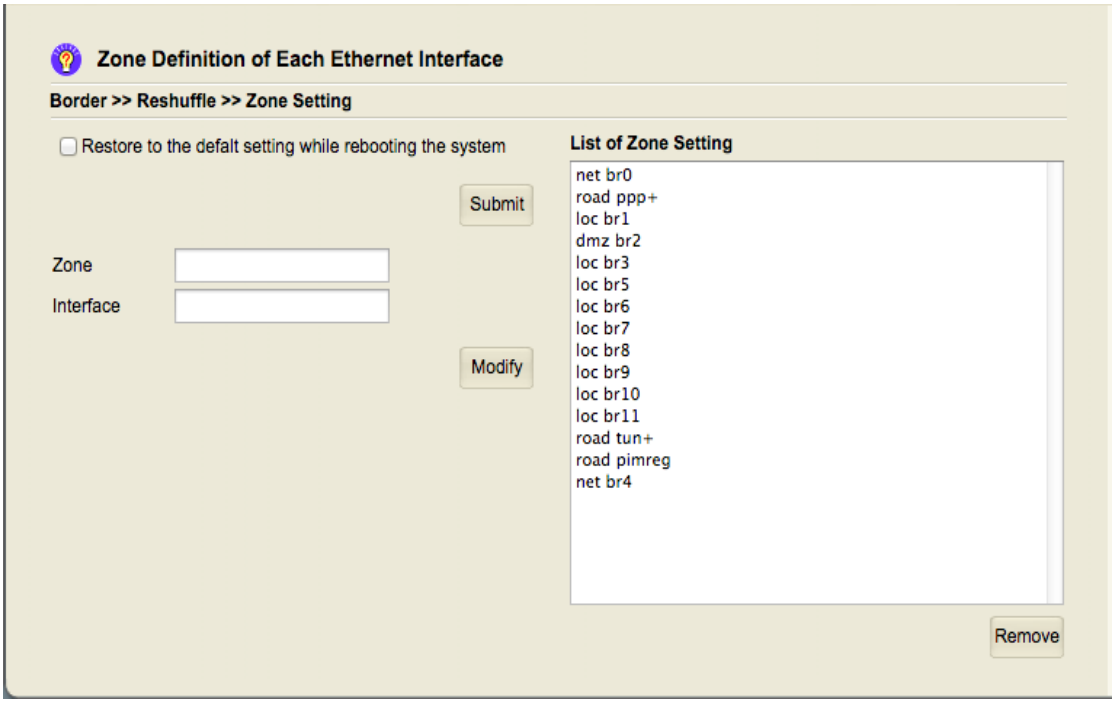
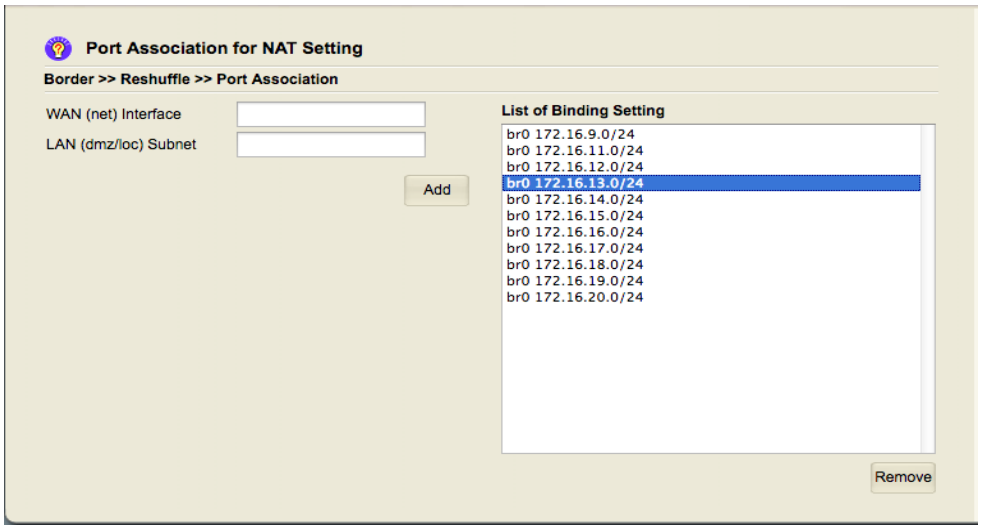
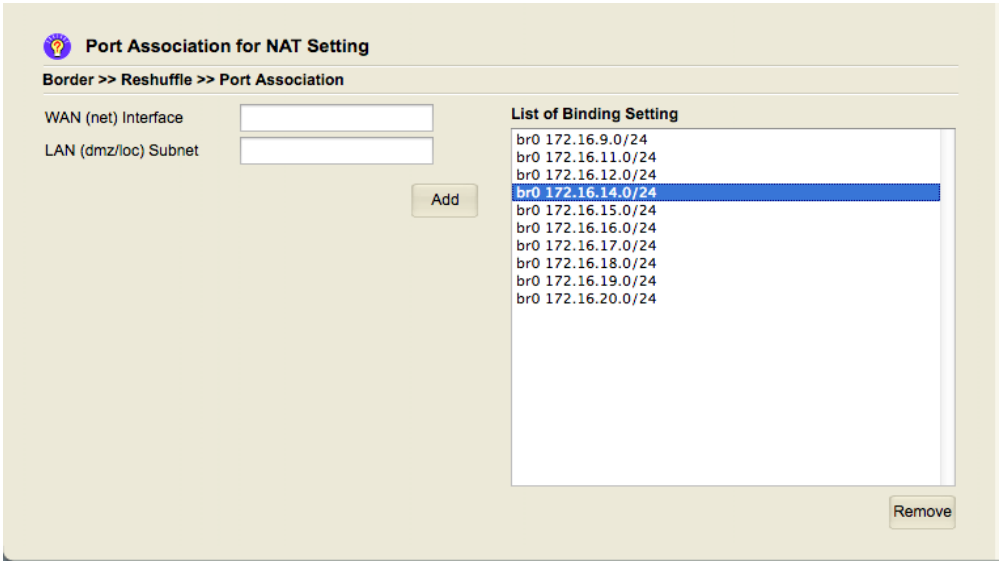



イラスト ***83:*** リスト ***"br4" in*** ゾーン ***"net"***

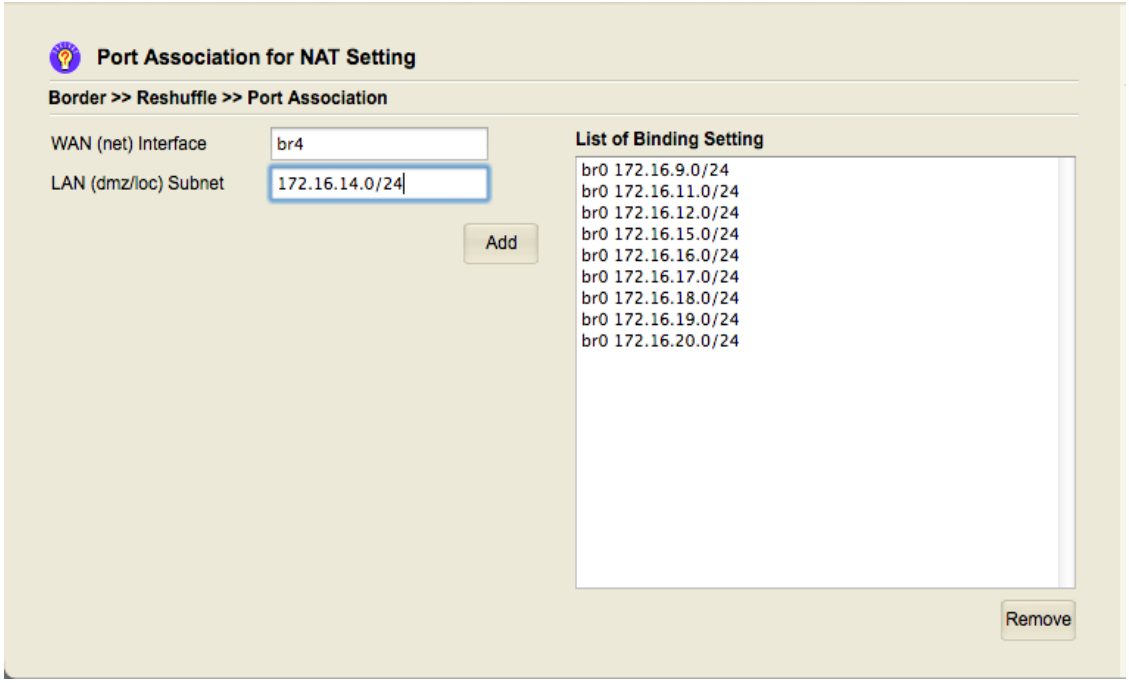
次に、br4 のサブネットからのトラフィックを br4 のサブネットに NAT にかける設定に変更します。つまり、ソース IP アドレスが br4 の IP アドレスで置き換えられます。これは、「Border >> Reshuffle >> Port Association」で実行できます。まず、「br4」と「br5」の元の設定を削除してください。



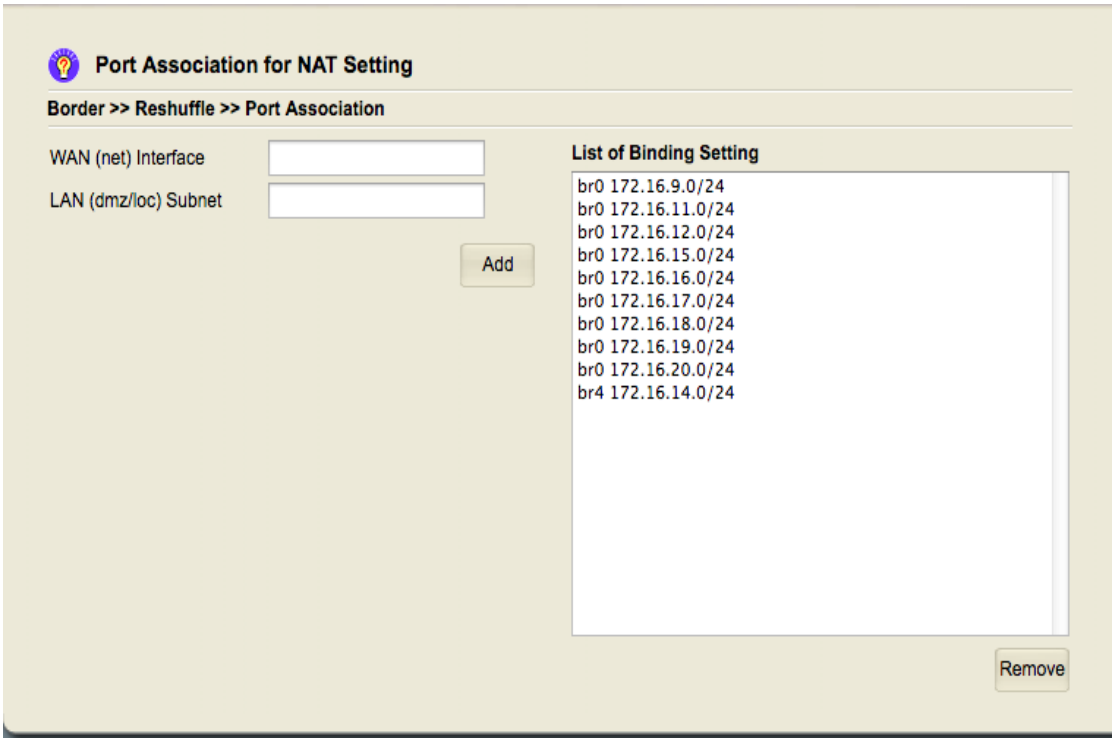

挿絵 ***84:*** 「***br4***」の元のサブネットを削除して、「***br0***」の下で ***NAT***を使用する




挿絵 ***85: "br4"*** のサブネットを ***"br0"*** の ***NAT*** 下で削除




挿絵 ***86: "br5"*** サブネットを ***"br4"*** の下で ***NAT*** を使用して追加




挿絵 ***87:*** サブネット ***"br5"*** のリストを使用する ***NAT*** 以下の ***"br5"***

“br4”の IP アドレス、および “br4” と “br5”、 “br5” と “br4” 間の関係（NAT 用）を調整した後、ルーティングポリシーの設定を行います。以前に述べたように、右側の 1 番目のボックスには対応するルーティングテーブルを表示し、基盤プラットフォームを通過するすべてのネットワークパケットに対して、上位から順にルールを確認します。1 つのルールに一致しない場合、次のルールを確認します。下部の 2 行は“main”ルーティングテーブルと“default”を使用しています。

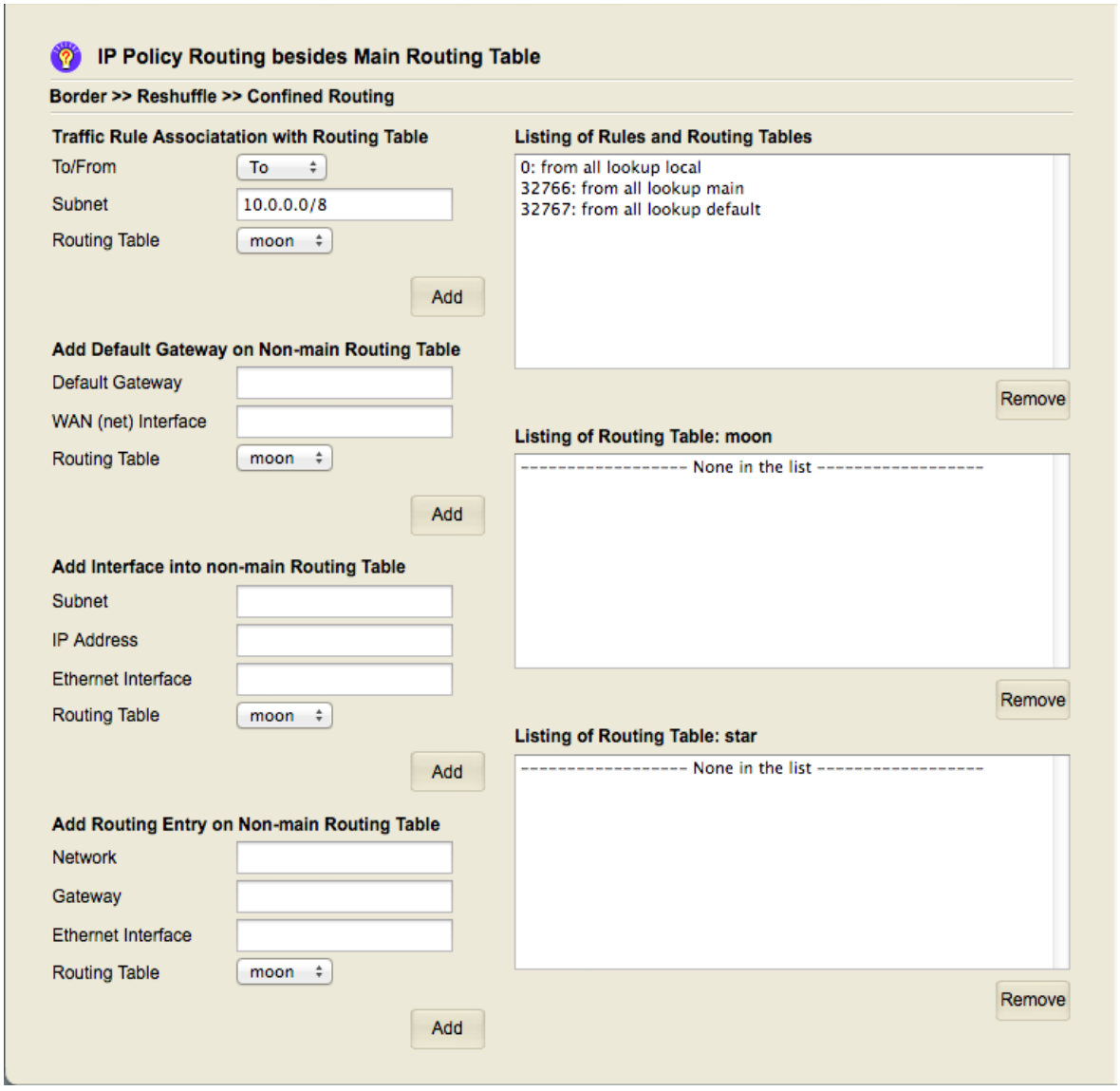
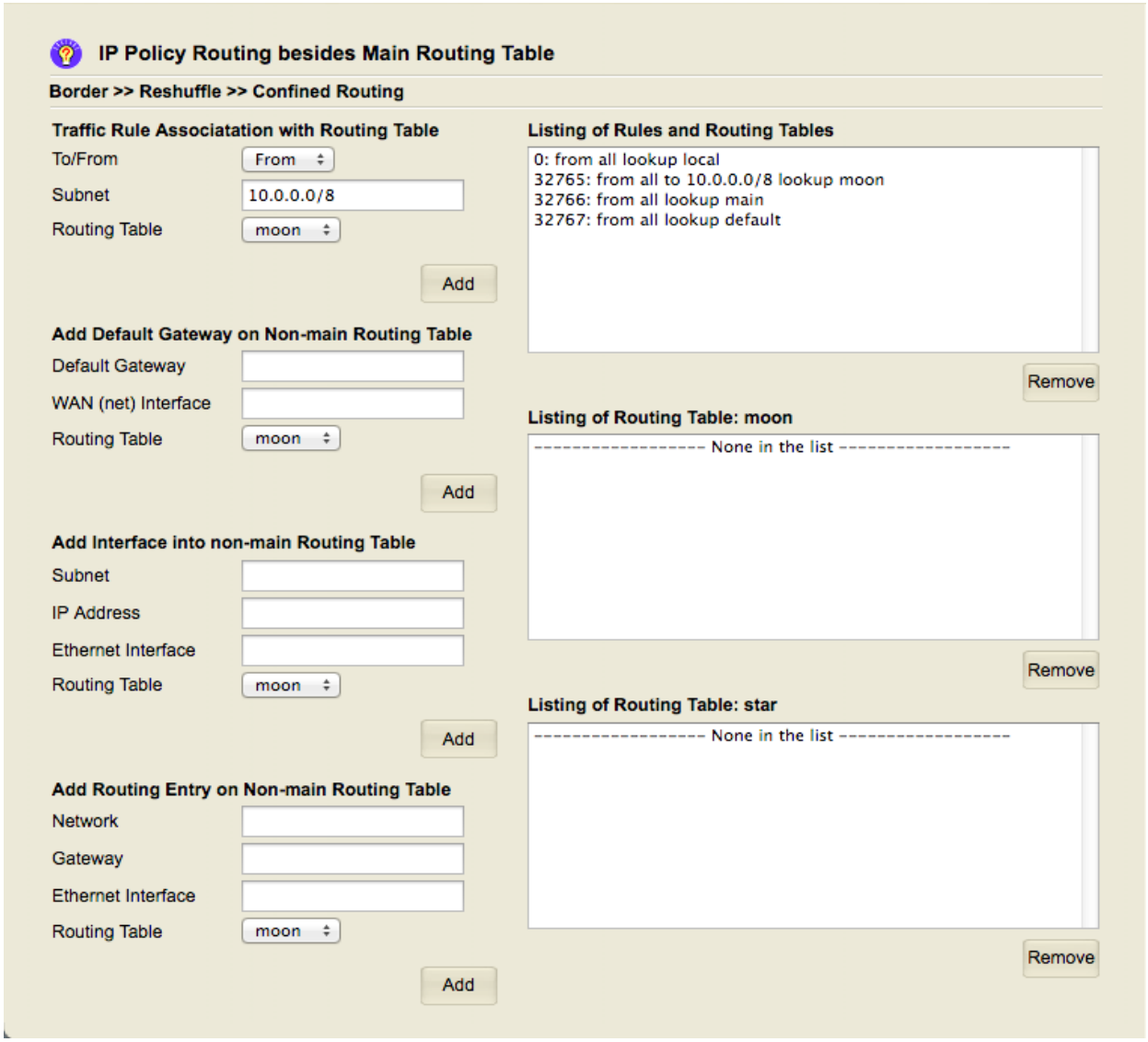



イラスト ***88: 10.0.0.0/8*** サブネットへ向かうトラフィックをキャッチする

考え方はシンプルです。サブネット「br4」と「br5」との間のトラフィックをキャッチし、「moon」ルーティングテーブルを使用して、それらのネットワークパケットの送信先を決定します。次のスクリーンショットは、サブネット「10.0.0.0/8」からのトラフィックをキャッチし、ルーティングテーブル「moon」を参照するように強制することを示しています。




挿絵 ***89:*** サブネット「***10.0.0.0/8***」からのトラフィックを捕獲する

“10.0.0.0/8”は“br4”が接続しているサブネットです。
このサブネットの背後に他のサブネットが存在する可能性があり、ISP が提供するゲートウェイ経由でそれらのサブネットにアクセスできる可能性があります。これらのサブネットへのパケットも捕捉すべきでしょうか？より良いアプローチは、すべての宛先サブネットをリストするのではなく、「送信元」サブネットの捕捉に重点を置くことです。すべてのパケットの宛先となるサブネットは多数あるかもしれませんが、送信元サブネットの数はごく限られています。

したがって、構成画面の「To」フィールドのサブネットに関しては、隣接するサブネットのみを指定します。そして、「リモートサブネット」については、ルーティングテーブルのデフォルトゲートウェイがそれらを処理するようにします。

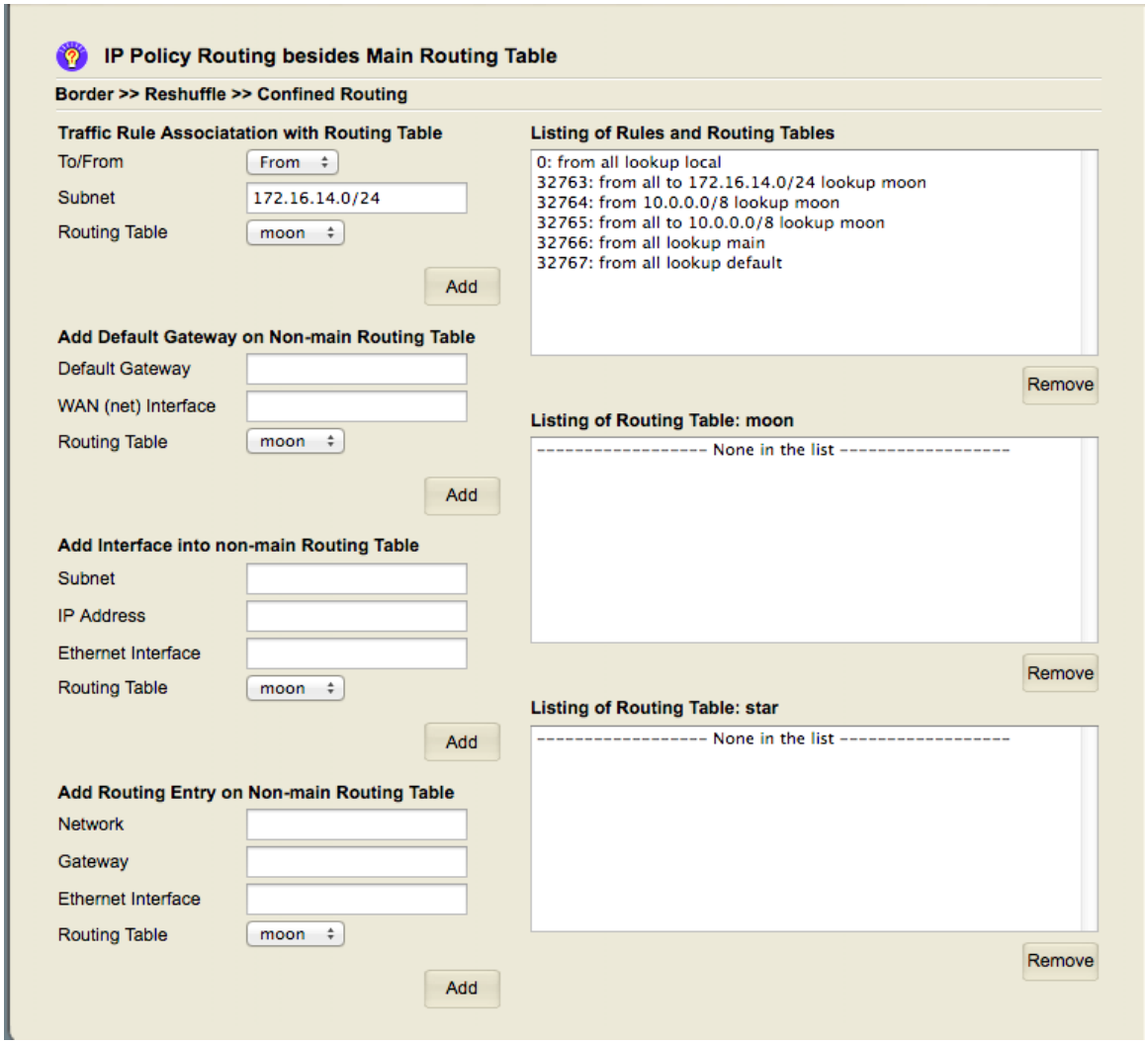



イラスト ***90: "172.16.14.0/24"*** からのトラフィックをキャッチ

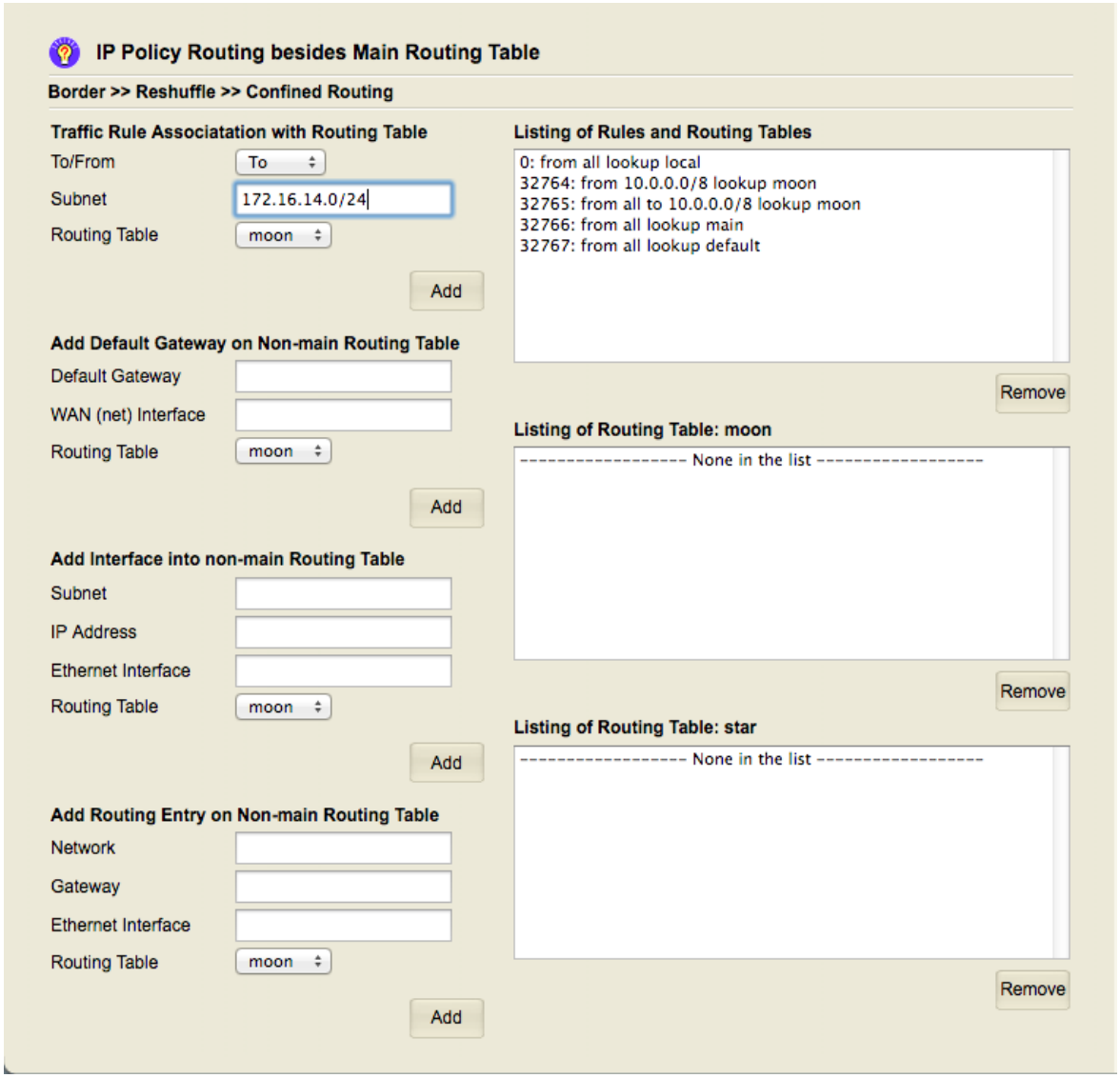



イラスト ***91: 172.16.14.0/24*** に向かう交通をキャッチする

そして、「172.16.14.0/24」が「br5」に接続されていることを忘れないでください。

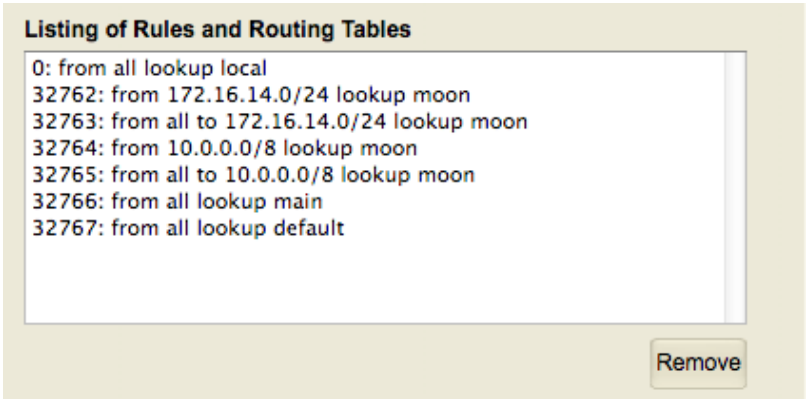


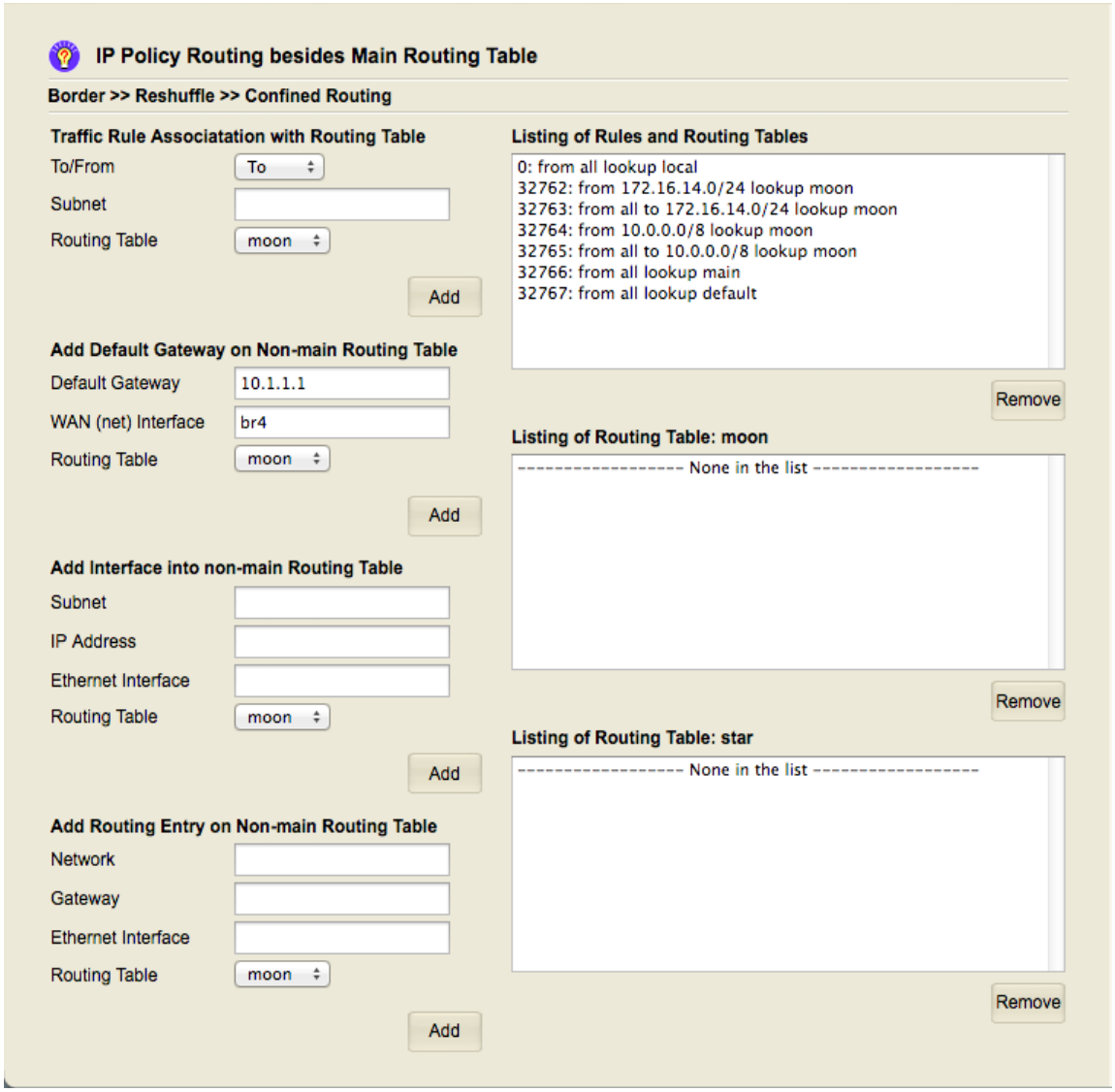

イラスト ***92:*** 参照ルーティングテーブルのリストルール

上記のボックスは、サブネット “172.16.14.0/24” と “10.0.0.0/8” へのトラフィックは、ルーティングテーブル “moon” を参照する必要があります。それ以外のものは、ルーティングテーブル “main” を参照してください。

“moon”ルーティングテーブルの作成残りの作業です。br4 と br5 のみのインターフェースを持つホストの場合、同様の内容のルーティングテーブルを作成したいと考えています。通常、ルーティングテーブルのエントリーは、Ethernet インターフェースが直接接続されているサブネットに対して、Ethernet インターフェースの IP アドレスを設定する際に作成されます。しかし、これらの手順は他のルーティングテーブルでは自動的には行われません。したがって、手動でエントリーを追加する必要があります。

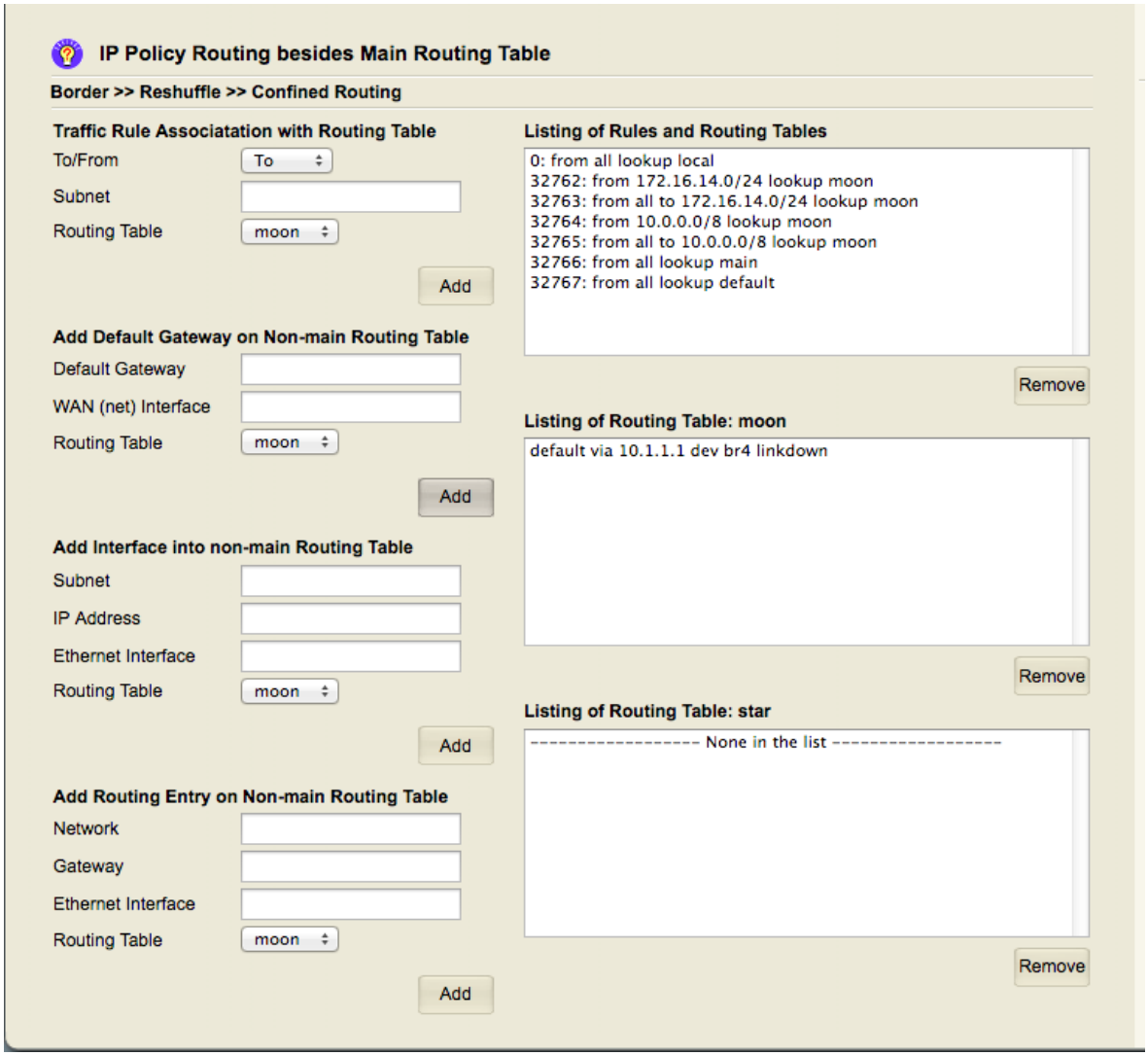
イーサネットインタフェースに関連付けられたサブネットとは別に、デフォルトゲートウェイが必要です。もし、ネットワークパケットの宛先と一致するルーティングエントリがない場合、そのパケットはデフォルトゲートウェイに送信されます。他のローカルサブネットにゲートウェイを追加する可能性もあります。これらはルーティングテーブルのエントリのほぼすべてのシナリオです。

“moon”ルーティングテーブルにデフォルトゲートウェイを追加する方法は次のとおりです。




挿絵 ***93: “moon”*** ルーティングテーブルにデフォルトゲートウェイを追加する

「Add」ボタンを押すと、対応するルーティングエントリが右側にある「moon」ルーティングテーブルに表示されます。 デフォルトゲートウェイを追加しても何も表示されない場合、意図した設定が正しくない可能性があります。その理由は、「br4」の IP アドレスが有効になっていないため、戻って IP アドレスが正しく設定されているかを確認し、システムを再起動して有効にする必要があるからです。ゲートウェイとインターフェースの IP アドレスが同じサブネットにないことは明らかです。




挿絵 ***94:*** 「***moon***」ルーティングテーブルのデフォルトゲートウェイ

デフォルトゲートは上記の図のように表示されます。直接接続されたサブネットのルーティングエントリを追加するプロセスは、イーサネットインターフェースの IP アドレスとネットマスクを設定するのと同じくらい類似しています。

以下のスクリーンショットは、サブネット“br4”が直接接続されているためのルーティングエントリを追加するためのものです。

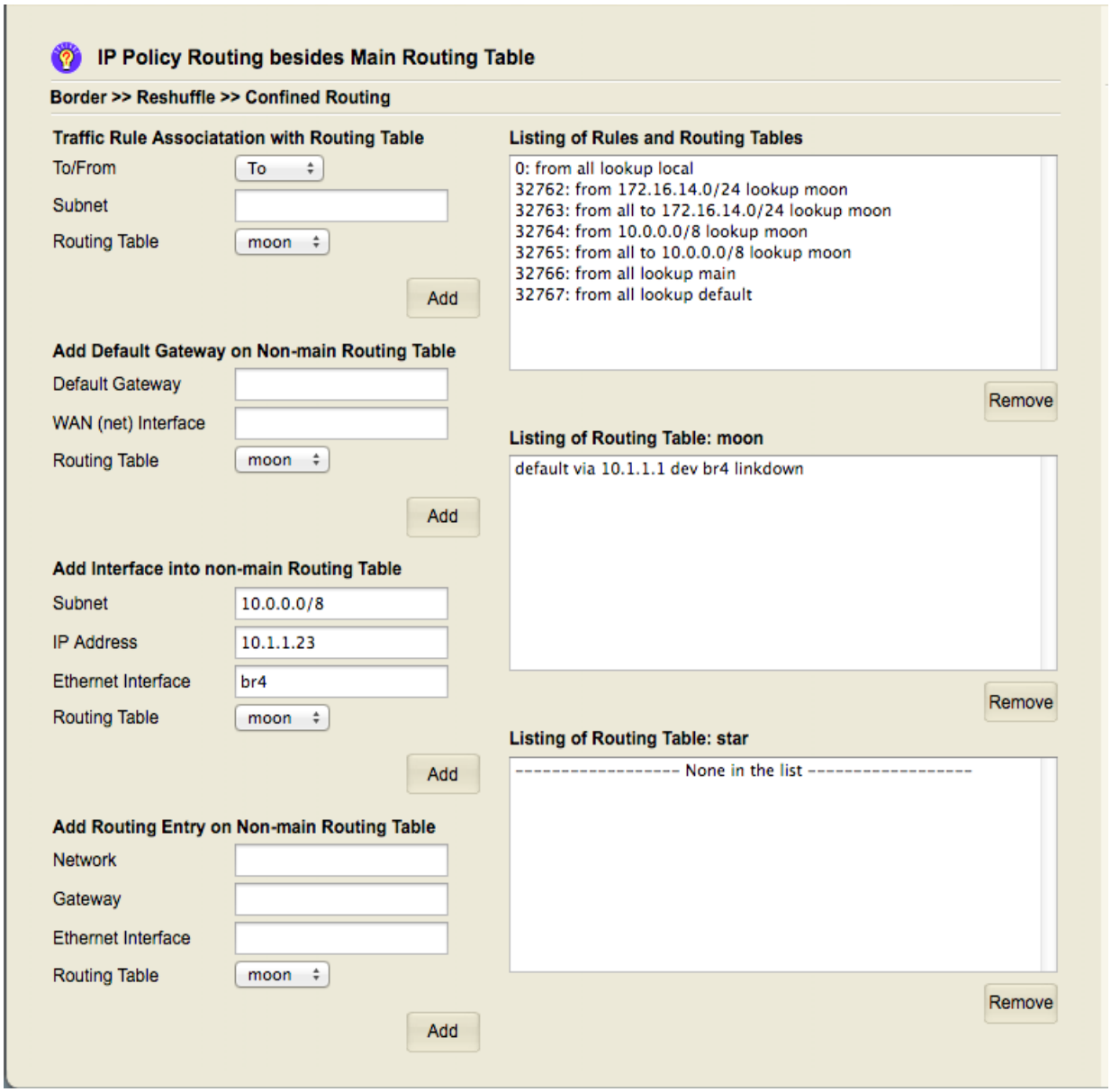
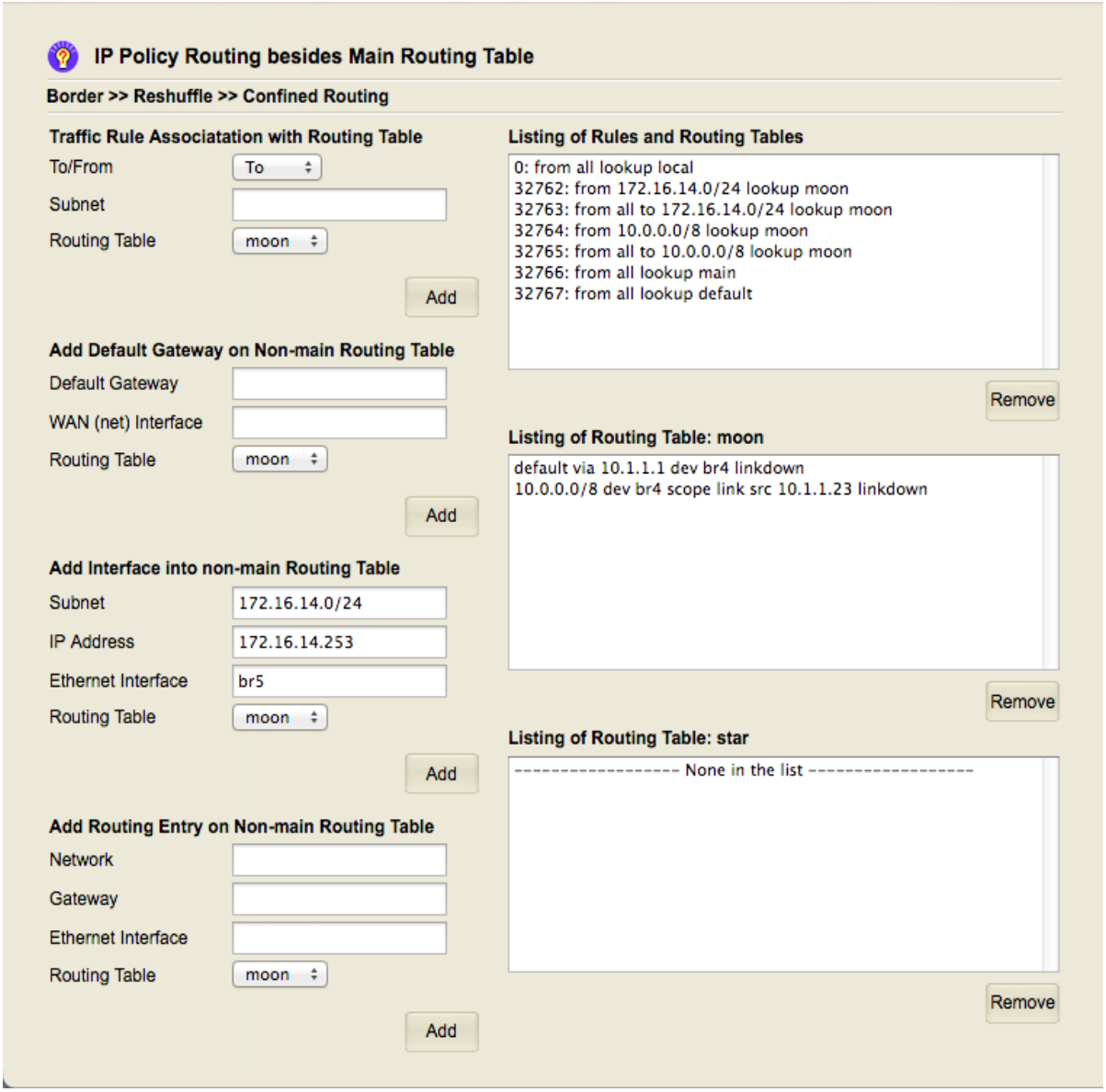



イラスト ***95: “br4”***に接続する***“moon”***のサブネット用のルーティングエントリを追加する




挿絵 ***96: "br5"***に接続する***"moon"***のサブネット用のルーティングエントリを追加する

上記のスクリーンショットは、「br5」が接続しているサブネットのルーティングエントリを追加するためのものです。

“moon” ルーティングテーブルの内容の最終的な結果は次のとおりです。

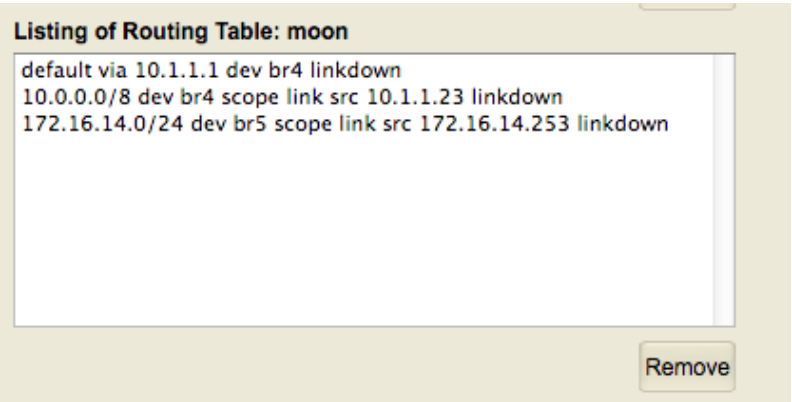


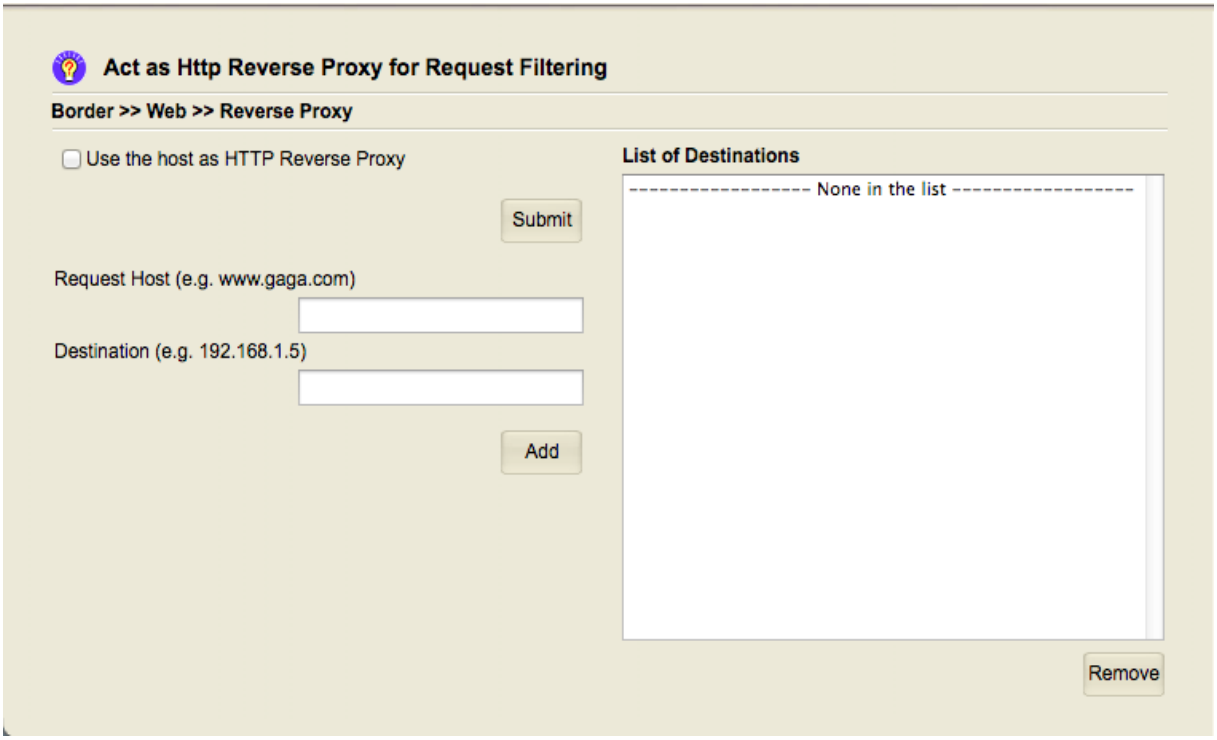

イラスト ***97: “moon”*** ルーティング テーブル の内容

「スター」という別のルーティングテーブルが存在します。もし、同様の用途で別のペアのブリッジをお持ちの場合、その特定のトラフィック用のルーティングエントリは、そのルーティングテーブルに配置することができます。

IP ポリシールーティングも、別のマシンにトラフィックを送信するためのルールを設定するために使用できます。手順はここではあまり複雑ではありません。ただし、このネットワークルーティングは「静的ルーティング」に限定されます。動的ルーティングは「メイン」ルーティングテーブルでのみ発生します。動的ルーティングのトピックは後で紹介します。

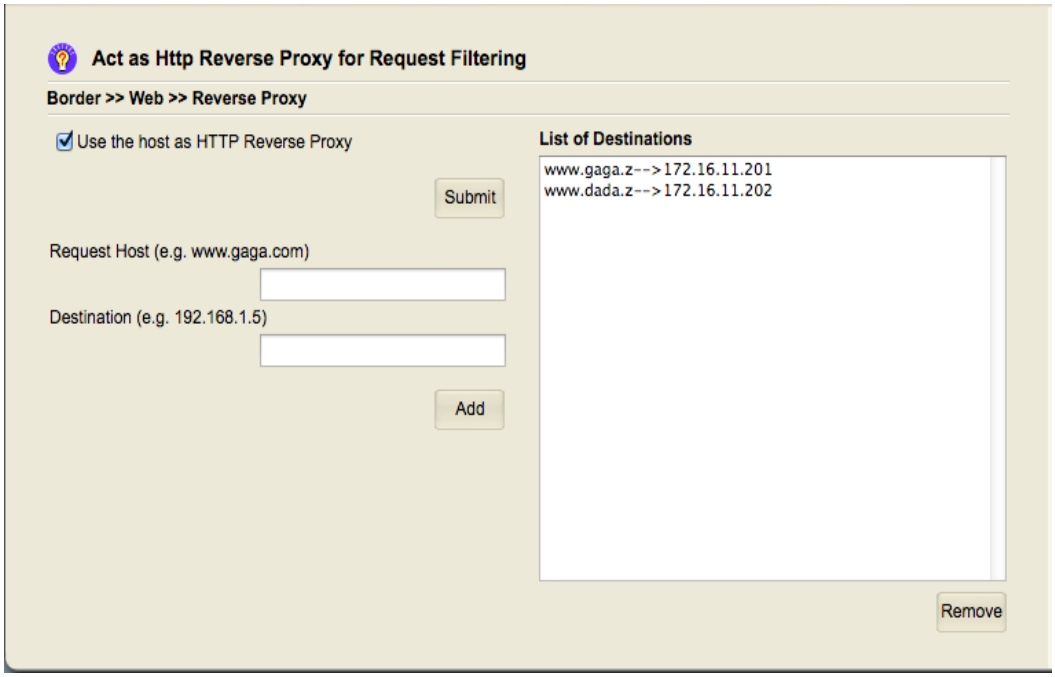
## *Http Reverse Proxy for Request Filtering*

これまでのセクションでは、「ポートフォワーディング」および「IP ロードバランシング」のトピックを扱いました。これらのアプローチは、HTTP リクエスト（TCP ポート 80）をプライベートネットワークのサーバーに転送することができます。



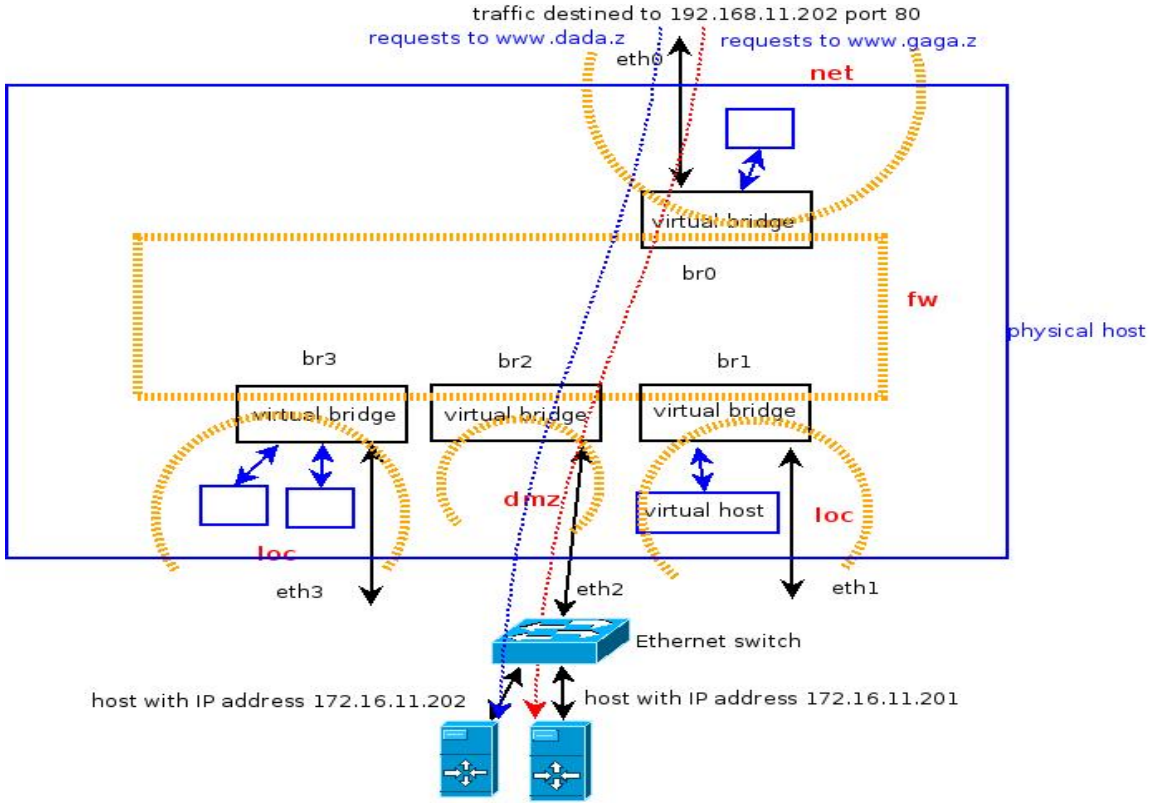

挿絵 ***98: HTTP*** リバースプロキシの画面スナップショット

しかし，“ポートフォワーディング”および“IP ロードバランス”は，“IP ヘッダー”の内容に基づいてリクエストを処理します。 “www.gaga.z”と“www.dada.z”という二つのホスト名が同じ IP アドレスを指している場合、HTTP リクエストの二つを“IP ヘッダー”から区別することができません。 リバースプロキシのアプローチは、URL 内のホスト名に基づいて異なる内部サーバーにリクエストを送信することを可能にします。




挿絵 ***99: HTTP*** リバースプロキシ ***2*** つの異なるホスト名について

***Illustration 100: Http Reverse Proxy for Two Hosts***



# 第 4 章 VPN

VPN (Virtual Private Network) における VPN とは：私有ネットワークインターフェースを VPN サーバーと VPN クライアントの両方に作成し、これらの仮想ネットワークインターフェースが送信されるネットワークトラフィックを物理ネットワークインターフェースのペイロードとして包装し、他の端に到達させるためにペイロードをラップします。 他の端では、VPN サーバー/クライアントはペイロードをアンラップし、アプリケーションレベルのソフトウェアコンポーネントからネットワークトラフィックを取得します。 アプリケーションの視点から見て、VPN は送信または受信するためのネットワークトラフィックを使用できる別のネットワークインターフェースです。

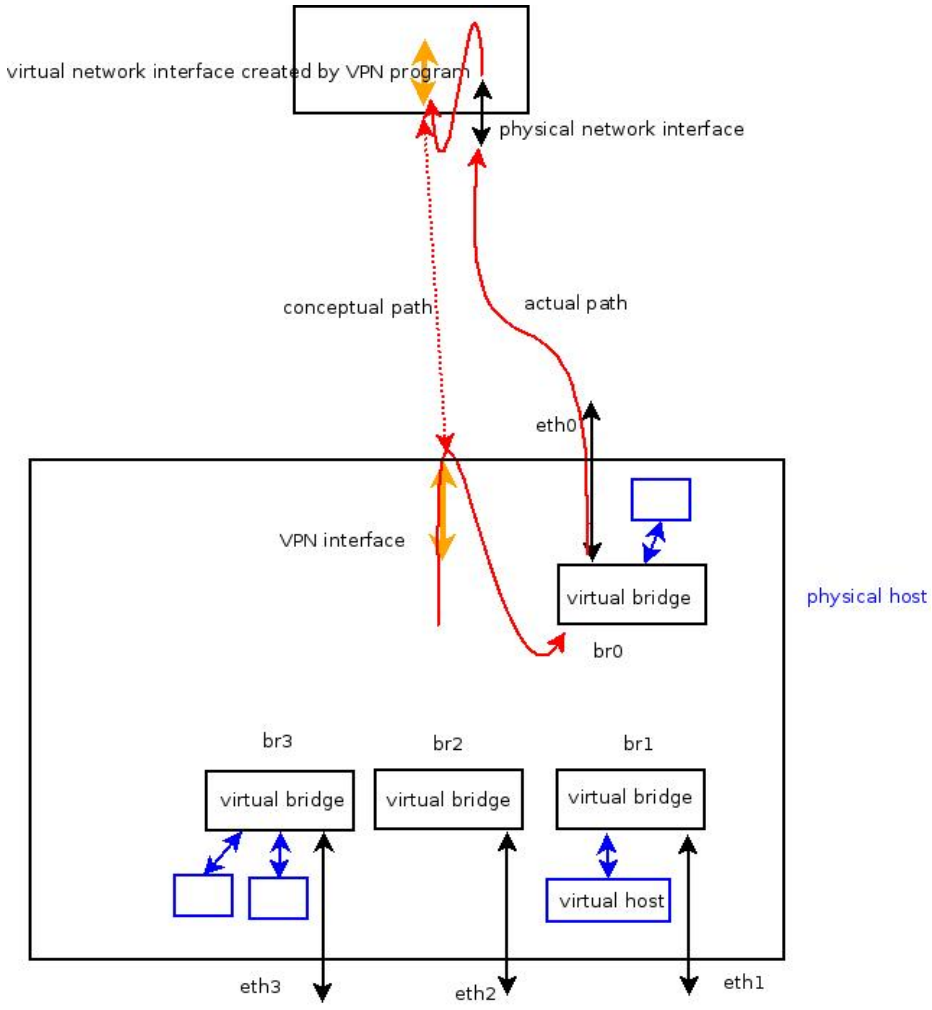


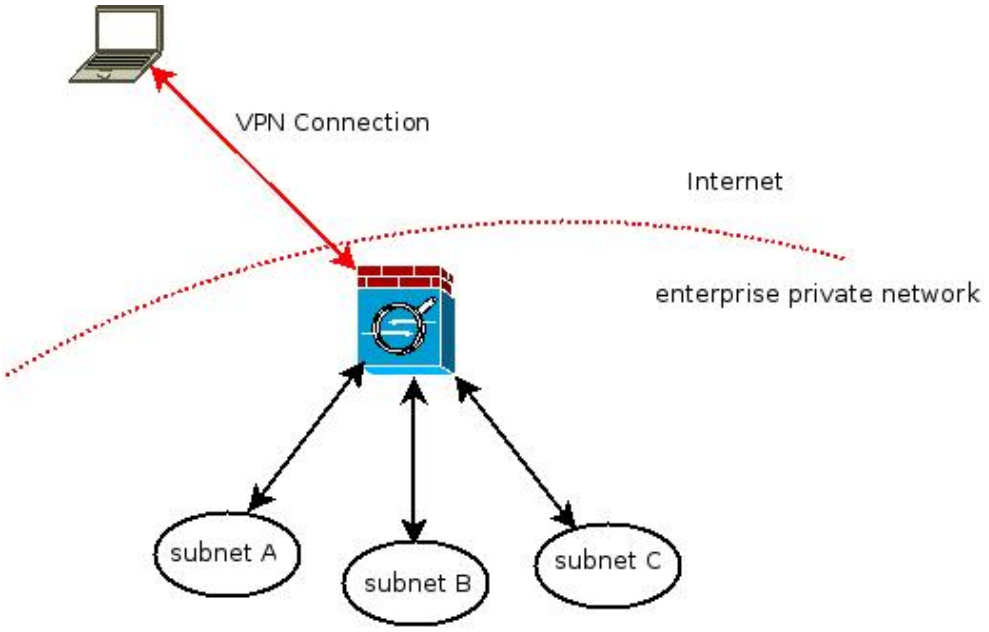

イラスト ***101: VPN*** 動作原理

他の種類の VPN が存在する可能性がある。しかし、このドキュメントで参照する VPN は、他のシステムコンポーネントと相互作用するために仮想ネットワークインターフェースを使用するもの。

ネットワークトポロジーに関しては、クライアント-サイト VPN とサイト-サイト VPN が存在します。ネットワークトラフィックのレベルに関しては、ブリッジングモードとルーティングモードで動作します。VPN がルーティングモードで動作している場合、その VPN は独自の IP サブネットを持ち、VPN プロセスによって作成された仮想ネットワークインターフェースは、そのサブネット内の IP アドレスを持ちます。このモードで VPN を使用するには、そのサブネットにトラフィックをルーティングしてください。

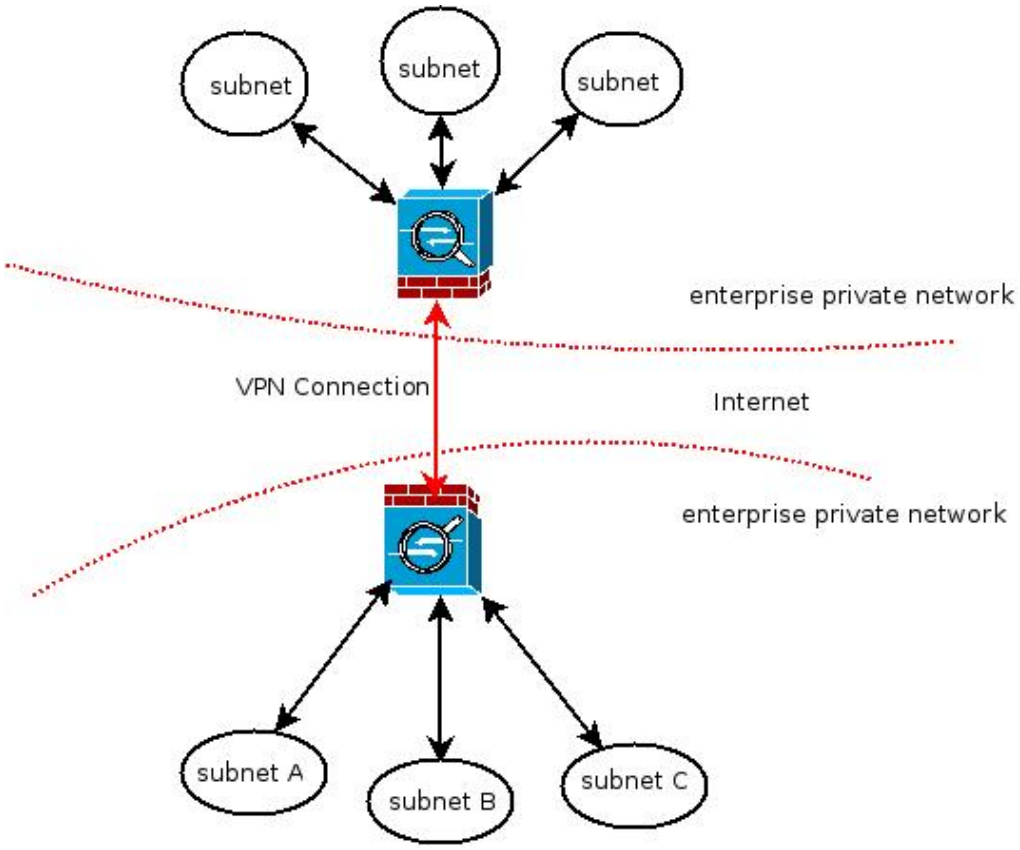
VPN をブリッジモードで実行する場合、イーサネットフレームがエンカプシュレートされ、一端から他端まで運ばれます。ネットワーク計画における一般的な慣行として、IP サブネット内で“ブリッジング”を使用します。したがって、VPN をブリッジモードで実行する場合、規模は比較的小さく、IP サブネットが大きくなり、ネットワーク上の特定のトラフィックを小さな部分に簡単に分離できない可能性があります。

クライアントからサイトへの VPN は、サーバーが IP サブネットの背後にあり、そのネットワークアプリケーションが VPN クライアントによって作成された仮想ネットワークデバイスを使用して、VPN サーバーの背後にあるホストにアクセスできるようにする VPN クライアントです。



挿絵 ***102***：クライアントからサイトへの ***VPN***

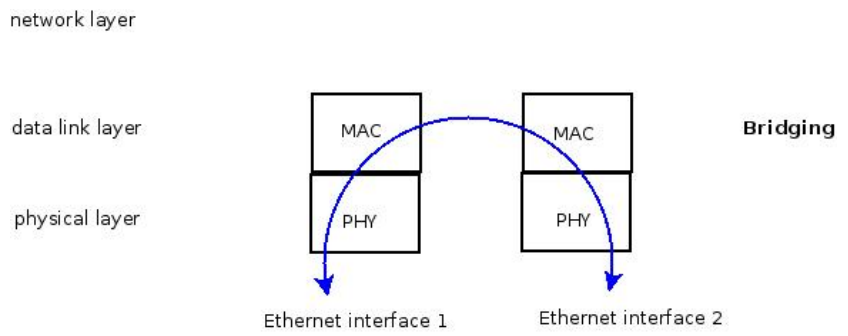
サイト間 VPN は、2 つのマシンが VPN 接続を確立することで、それぞれのマシンが背後にあるサブネットがリモート側のネットワークにアクセスするシナリオです。



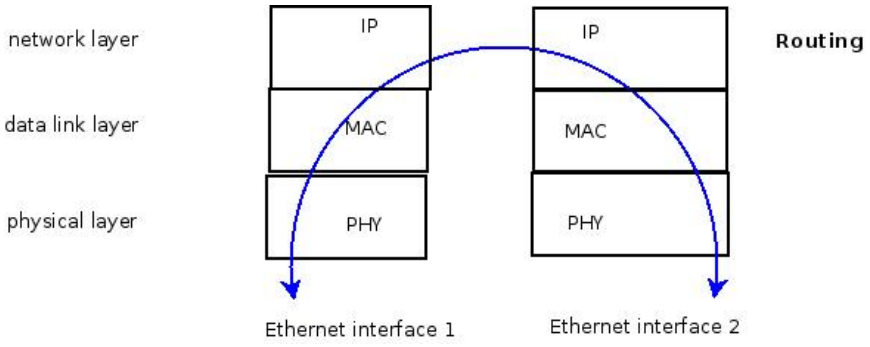

挿絵 ***103:*** サイトからサイト ***VPN***

クライアントからサイトへの接続が「ブリッジングモード」で実行される場合、クライアントの IP アドレスは、エンタープライズプライベートネットワーク内のサブネットのいずれかにある必要があります。サイトからサイトの VPN が「ブリッジングモード」で実行される場合、1 つの IP サブネットが 2 つのサイトにまたがっています。クライアントからサイトへの VPN のブリッジングモードはサポートしていません。ルートモードでのみサポートしています。

ブロッキングはデータリンク層でのみ行われ、システムはイーサネットフレームの MAC アドレスを調べてどのインターフェースに送信するかを決定します。ルーティングについては、システムは IP ヘッダー内の IP アドレスを確認します。



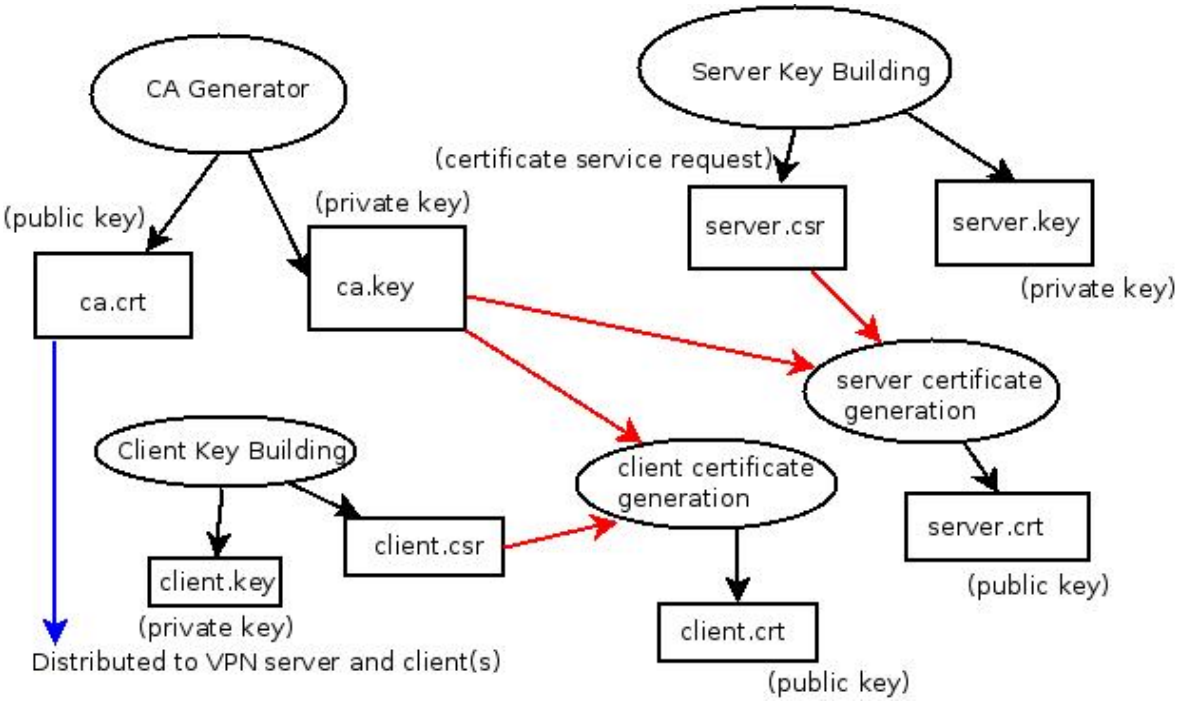

挿絵 ***104:*** ブリッジ




挿絵 ***105:*** ルーティング

VPN がブリッジモードで動作する場合、VPN プロセスによって作成された仮想ネットワークインターフェースには IP アドレスが割り当てられず、他のネットワークインターフェースとトラフィックを交換するためにブリッジに参加する必要があります。また、VPN プロセスによって作成された仮想ネットワークインターフェースには IP アドレスが割り当てられ、システム上のルーティングテーブルがネットワークパケットの宛先を決定します。

ベースプラットフォーム上の VPN は独自の CA（証明書認証局）を持っており、デジタル証明書を自身で発行することができます。これらの証明書は、VPN のベースプラットフォームにおける制御チャネル上の情報を認証するために使用され、暗号化するために使用されます。この“キー生成プロセス”はすべてのシナリオで利用されます。したがって、詳細な説明は省略します。




挿絵 ***106: VPN*** キー生成プロセス

まず、CA の生成から始まります。これによって、「プライベートキー」と「パブリックキー」のペアが生成されます。「プライベートキー」で暗号化されたメッセージは、「パブリックキー」でしか解読できません。「この CA のパブリックキー」は、VPN サーバーとクライアントに提供され、証明書がこの CA から発行されたかどうかを検証するために使用されます。VPN サーバースイートの場合、「パブリックキー」と「証明書サービスリクエスト」が生成され、この「証明書サービスリクエスト」は CA に提出され、CA は「プライベートキー」を使用して「サーバー証明書」を生成します。「サーバー証明書」にはサーバーの「パブリックキー」に加えて、CA が「プライベートキー」を使用して署名した署名が含まれています。VPN クライアントスイートも同様のプロセスを経て「プライベートキー」と「クライアント証明書」を生成します。

VPN クライアントが VPN サーバーに接続されると、両者は証明書ファイルを互いに送信し、各当事者は CA の公開鍵を使用して証明書がこの CA によって発行されたかどうかを検証します。 データ暗号化のための暗号化アルゴリズムと暗号化に使用される鍵の交渉プロセスには、他にいくつかのアルゴリズムが関与しています。

## *Client-to-Site VPN Connection*

以前に申し上げたように、ベースプラットフォームは「ブリッジモード」ではクライアントからサイトへの VPN を提供しません。ルーティングモードでのみ動作します。VPN を使用するには、IP サブネットを割り当てる必要があります。VPN にはコントロールチャネルとデータチャネルがあり、TLS/SSL ではありませんが、TLS/SSL によって提供されるアルゴリズムと暗号を使用します。そして、UDP ポート 1194 を使用します。

VPN のコントロールチャネルは、データチャネルの暗号化キーを交渉するために使用されます。通常は、AES を CBC モードまたは GCM モードで利用します。

もし VPN がサブネット“172.16.38.0/24”を使用している場合、そのサブネット上の VPN サーバーの IP アドレスは“172.16.38.1”です。この IP アドレスを使用して VPN サーバーにアクセスできます。例えば、ベースプラットフォームに仮想ホストをインストールし、VNC でコンソールにアクセスするために TCP ポート 5904 を設定した場合、VNC ビューアで次の設定を使用して仮想ホストのコンソールに VPN でアクセスできます。

172.16.38.1 TCP port 5904

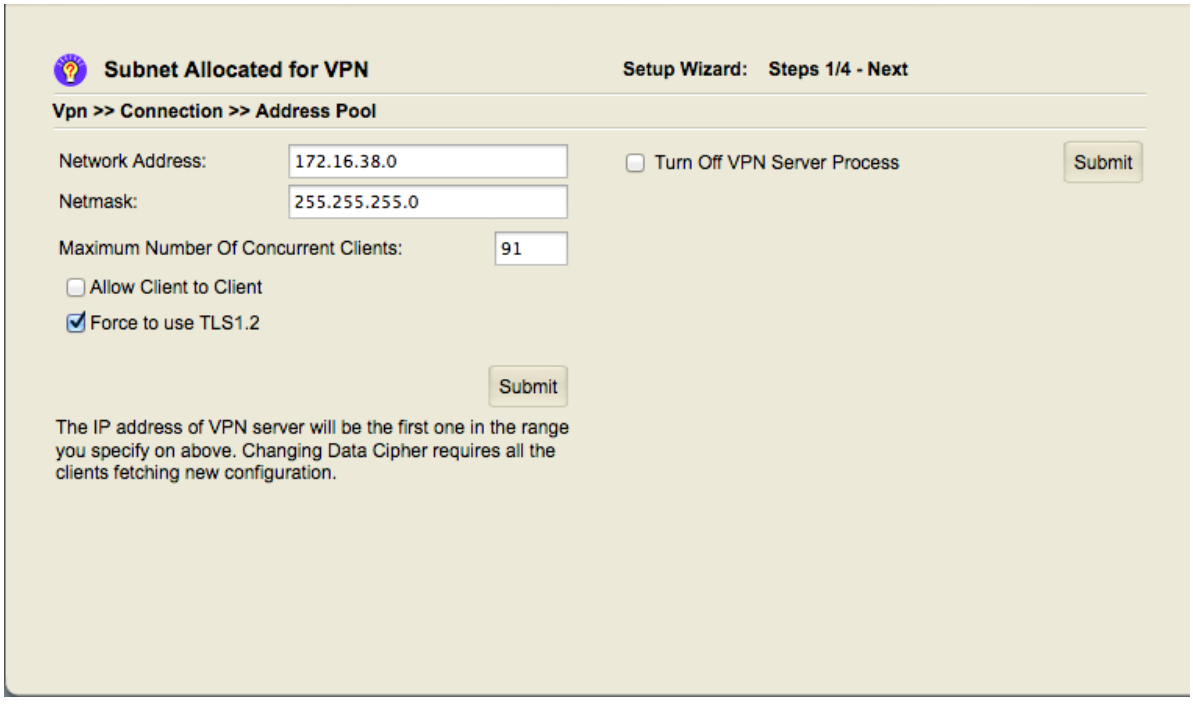
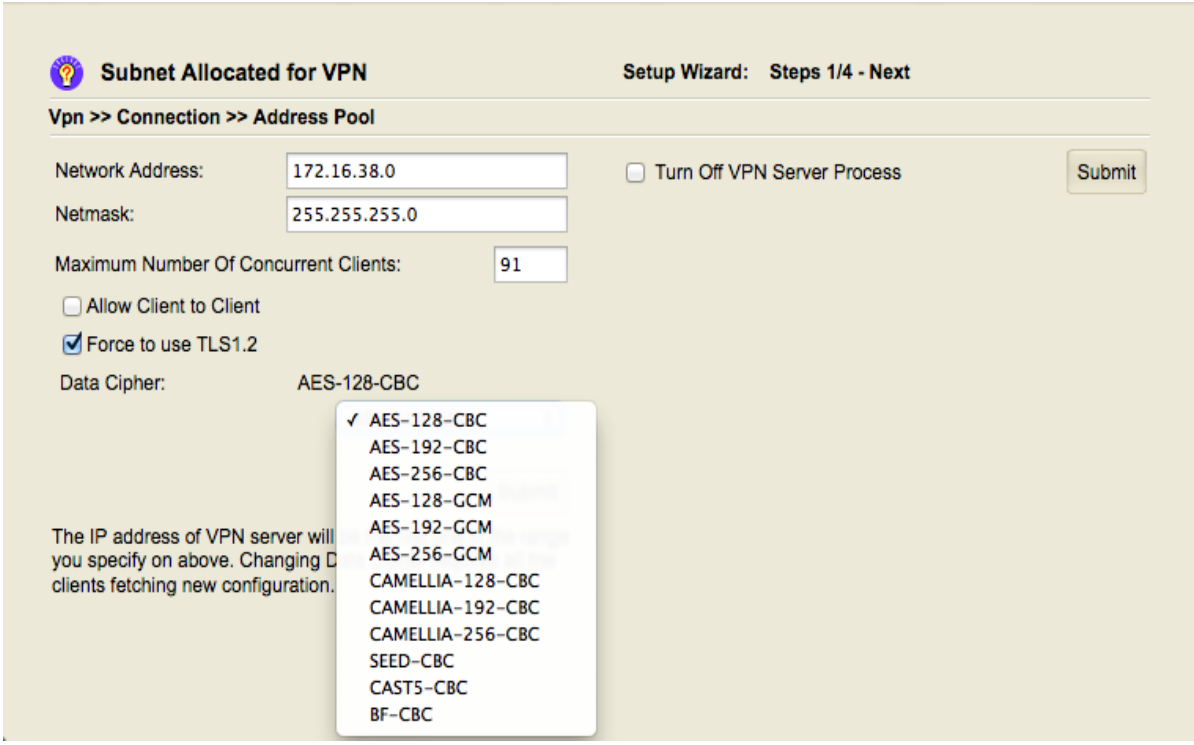


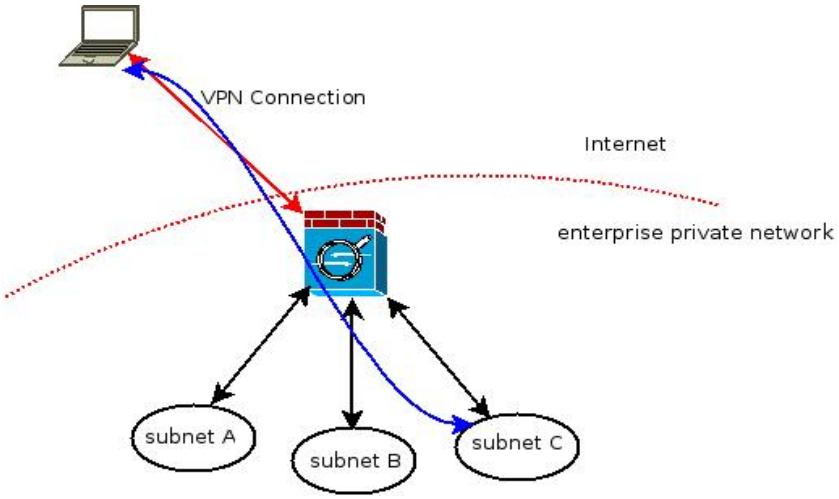

イラスト ***107:*** クライアントからサイトへの ***VPN*** アドレスプール




挿絵 ***108:*** データ暗号の選択

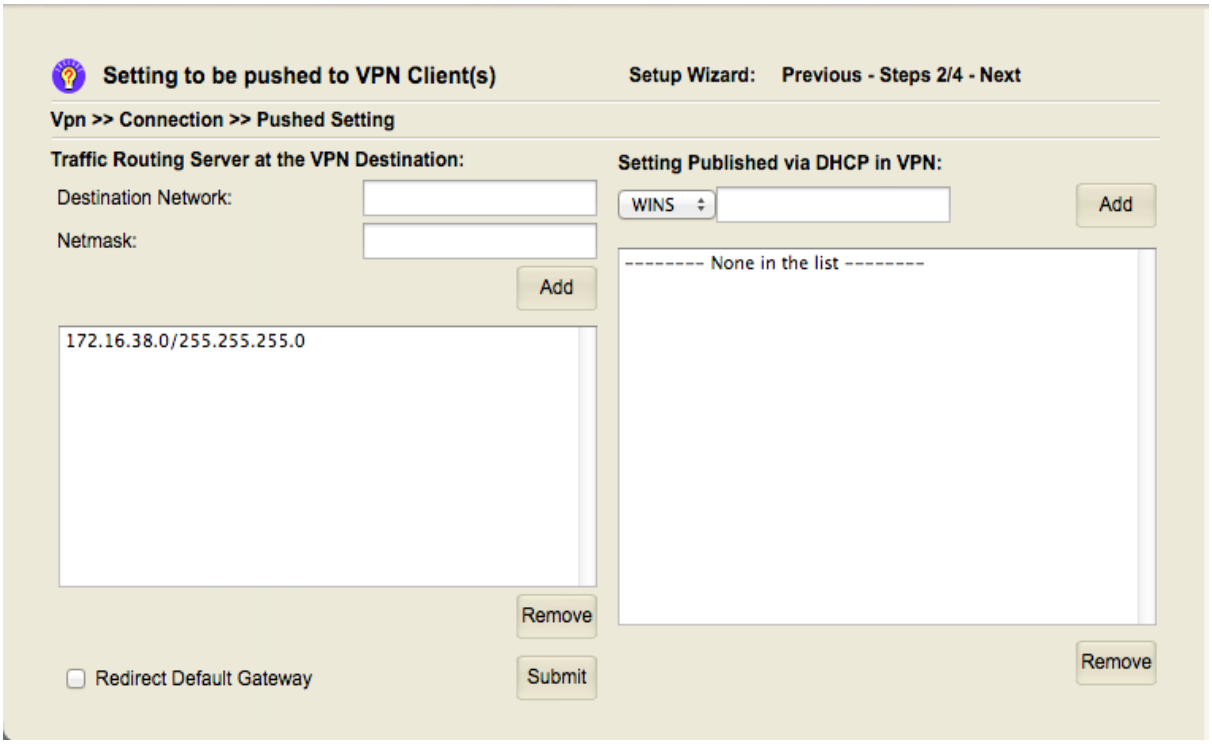
もし、シファーを選択できるバージョンが提供された場合、ハードウェアの計算能力に応じて選択することができます。SEED、CASTS、BF（Blowfish）シファーについては、64ビットシファーであると報告されており、ユーザーが約 700GB のデータを収集した後、これらのシファーがクラックされる可能性があるとされています。この状況を回避するために、シファーのキーの再交渉は、64MB のデータを送信した後に行われます。したがって、ハードウェアが弱い場合は、これらのシファーを使用しても安全です。

VPN サーバーは、指定されたサブネットから VPN クライアントに IP アドレスを割り当てます。VPN クライアント側のルーティングテーブルを変更することで、VPN クライアントが VPN サーバーの背後にあるサブネットへのアクセスを制御できます。




挿絵 ***109: VPN*** クライアントによるサブネットへのアクセス

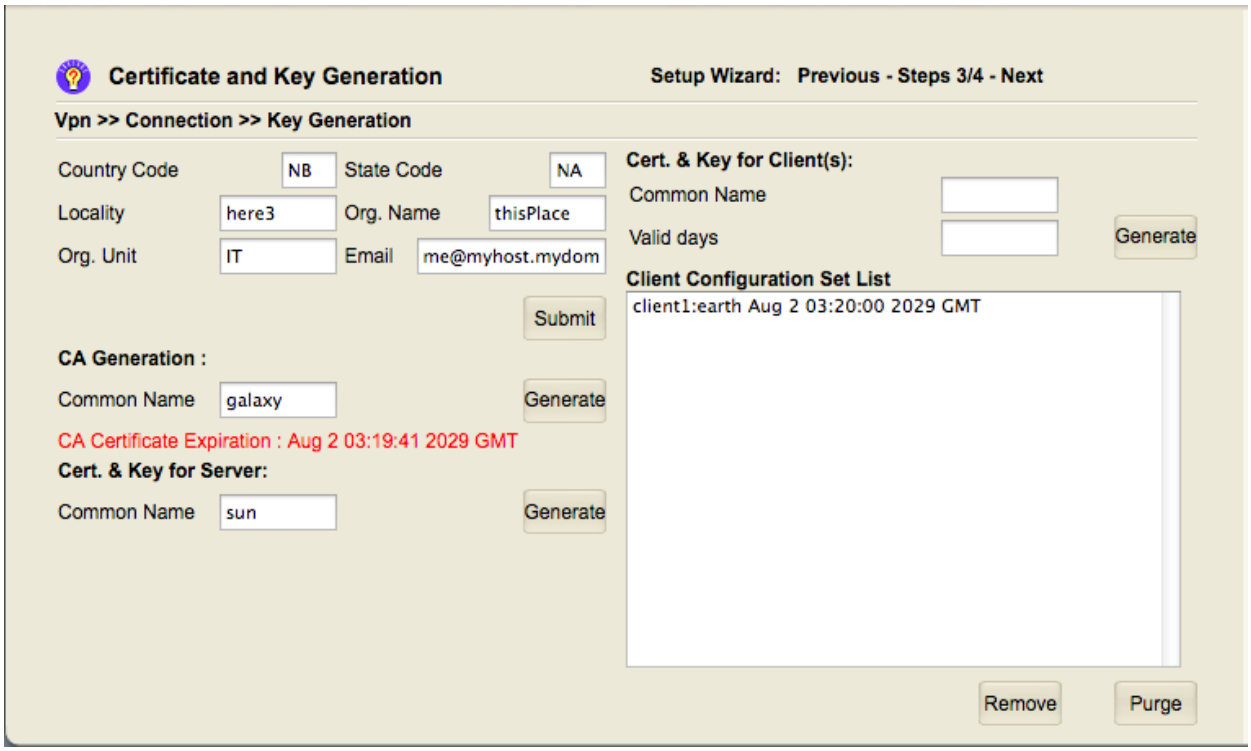
上記の図から、VPN クライアントがサブネット C にあるホストにアクセスするためには、VPN サーバーが“Vpn >> Connection >> Pushed Setting”にサブネット C の設定をプッシュする必要があります。




挿絵 ***110:*** クライアントからサイトへの ***VPN*** におけるプッシュ設定

そうすることで、VPN クライアントは VPN サーバーの IP をそのサブネットのゲートウェイとして使用し、右側の画面に示されている指定された WINS サーバーまたは DNS サーバーを使用して、VPN クライアントに指示することもできます。

CA、サーバーキーと証明書、およびクライアントキーと証明書は、「Vpn >> Connection >> Key Generation」を通じて確立できます。




挿絵 ***111:*** クライアントからサイトへの ***VPN*** 証明書とキーの生成

VPN サーバーに独自の CA（証明書認証局）を持つためには、「Purge」を押して、すべてのプリインストールされたキーと証明書を削除し、新しいものを生成することがあります。

CA は、「Common Name」のフィールドに入力し、「Generate」ボタンを押すことで生成できます。CA を生成した後、「Common Name」と「Valid days」のフィールドに入力して、サーバーの証明書とキーを生成します。サーバーキーの生成には少し時間がかかります。キーと証明書を入手したら、各クライアントに対して「Common Name」と「Valid days」の証明書を入力することで、クライアントのキーと証明書を生成できます。
「Common Name」は、すべてのクライアント、サーバー、CA の間で一意である必要があります。

CA とキーと証明書が生成されたら、VPN サーバーを再起動して、新しい CA、キー、および証明書を使用してください。クライアントキーと証明書は、CA とサーバーキーが生成された後にいつでも作成できます。上記のスクリーンショットに示すように、Common Name “earth”のクライアント証明書が作成されます。そのクライアントのキーと証明書は、「Vpn >> Connection >> Client File Download」でダウンロードできます。


挿絵 ***112:*** クライアント証明書 ダウンロード　クライアントからサイト ***VPN*** 用
***Illustration 112: Client Certificate Download for Client-to-Site VPN***

ファイルセットをボックス内の選択し、ボタンを押すことで、クライアントキーと証明書をダウンロードすることができます。管理者側は、ユーザー（またはユーザー数）にファイルを送信し、VPN クライアントプログラムにインストールするように依頼することができます。

# サイト間 *VPN* 接続（ルーティングモード）

サイト間 VPN は、一部のホストをリモートサイトにまたいでインターネット経由で公開する場合に使用できます。リモートサイトのすべてのユーザーが、VPN クライアントプログラムをコンピューターまたはモバイルデバイスにインストールする必要はなく、サイト間 VPN が展開されている場合です。このセクションでは、ルーティングモードで動作するサイト間 VPN を紹介します。

サイト間 VPN は独自の CA を持ち、クライアント間 VPN で使用される CA とは異なります。独立して作成する必要があります。ベースプラットフォームが提供するサイト間 VPN は、UDP ポート 7777 を使用し、2 つの VPN ゲートウェイは相手のパブリック IP アドレスを厳密にロックします。

何度も述べてきたように、ここで提供される VPN は仮想ネットワークインターフェース（「ローカルトンネルデバイス」とも呼ばれます）を作成するためのものです。VPN がルーティングモードで実行されている場合、この仮想ネットワークインターフェースには IP アドレスが割り当てられます。クライアント対サイト VPN では、VPN クライアントとサーバーが使用する IP アドレスはすべてアドレスプールから取得されます。サイト対サイト VPN では、両側の「ローカルトンネルデバイス」に必要な IP アドレスは 2 つだけです。この 2 つの IP アドレスは、エンタープライズサブネット内の IP アドレスと競合しないように注意してください。

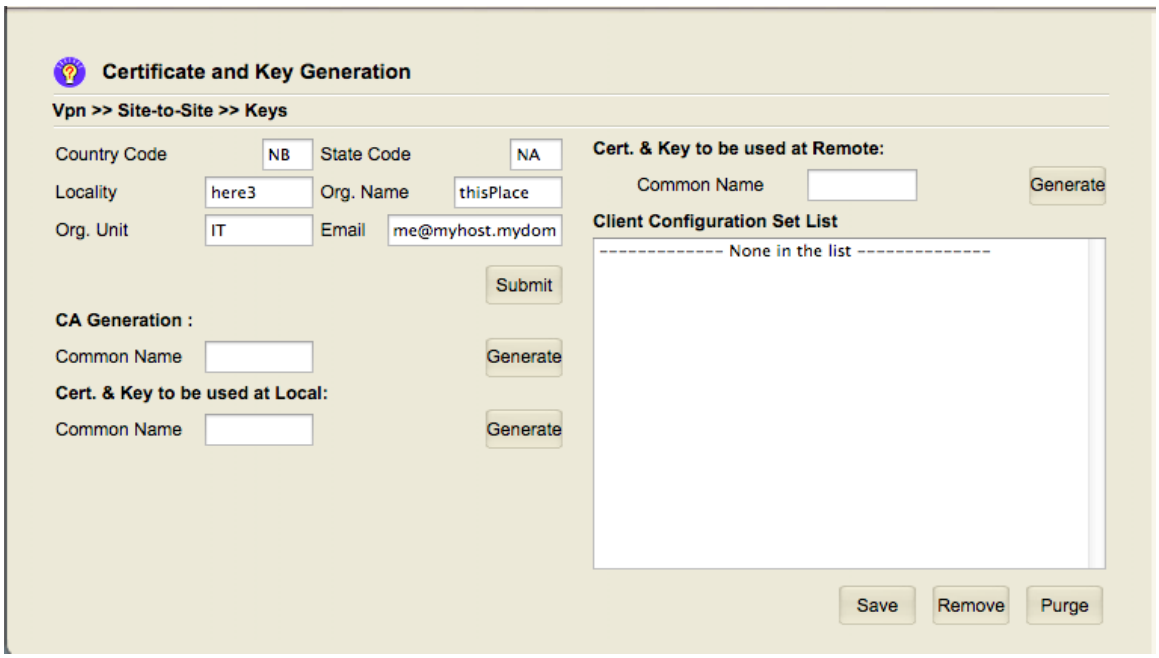
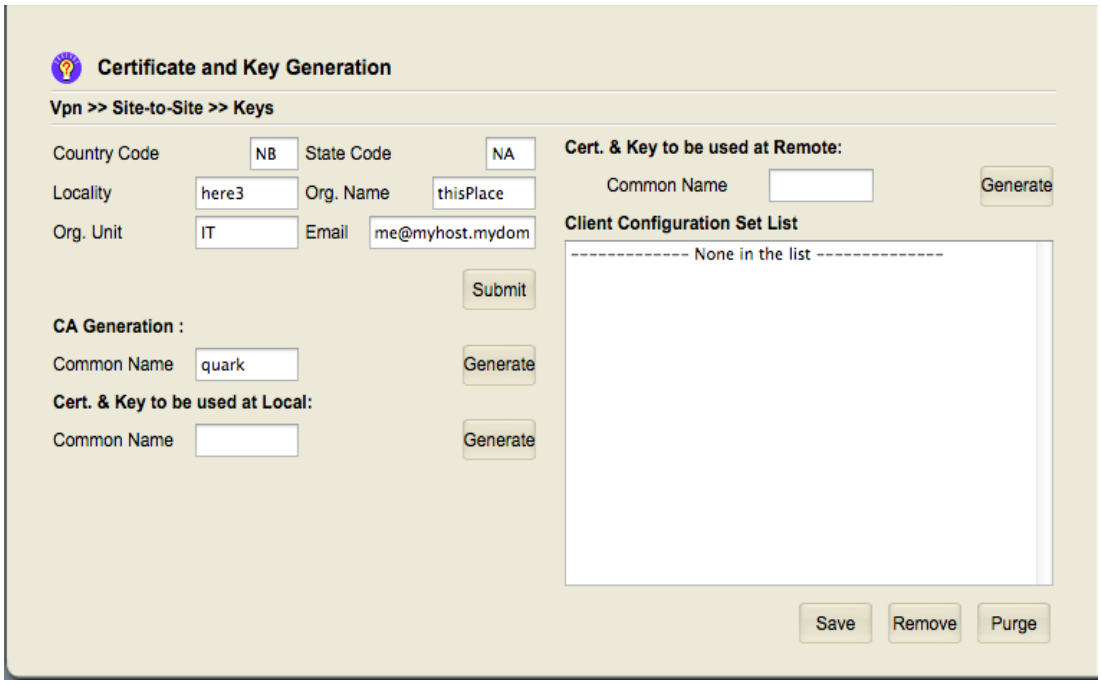
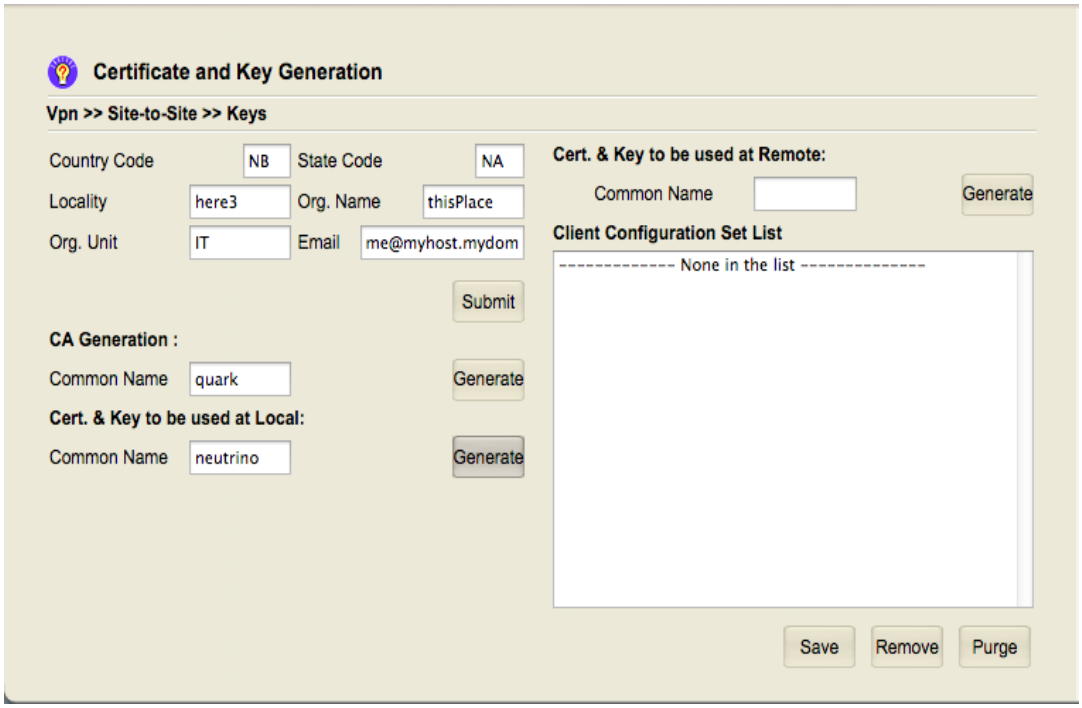


図 ***113:*** サイト間 ***VPN*** キー生成

以下のキー生成プロセスのスクリーンショットです。
Site-to-site VPN's CA is generated as follows:



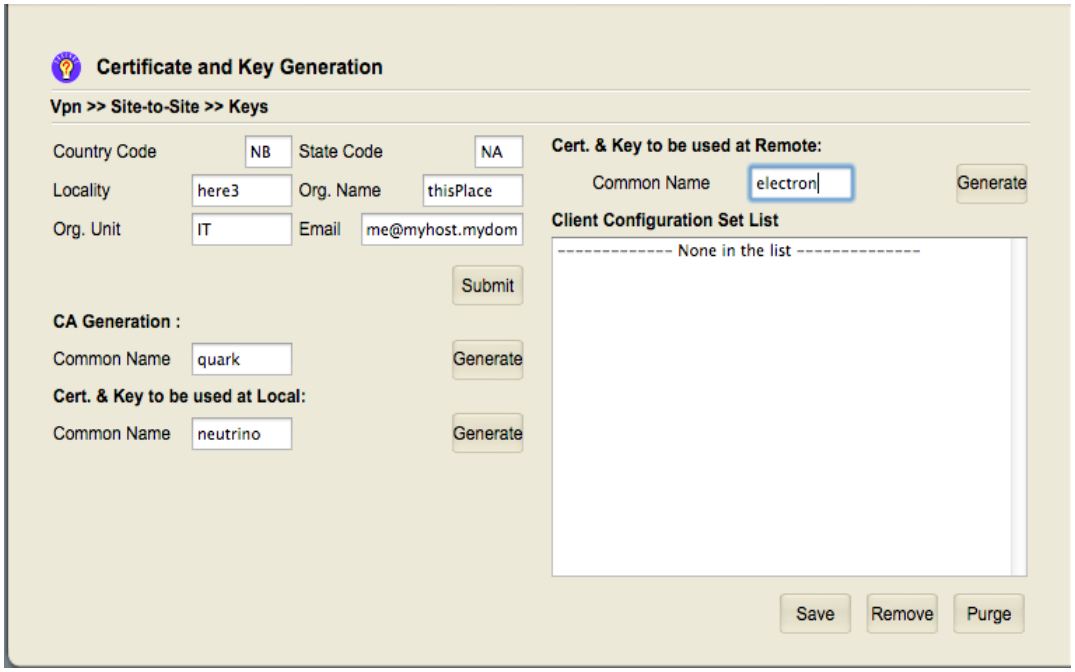

挿絵 ***114:*** サイトからサイト ***VPN CA*** 生成




挿絵 115: サイト間 VPN: サーバーキーと証明書生成

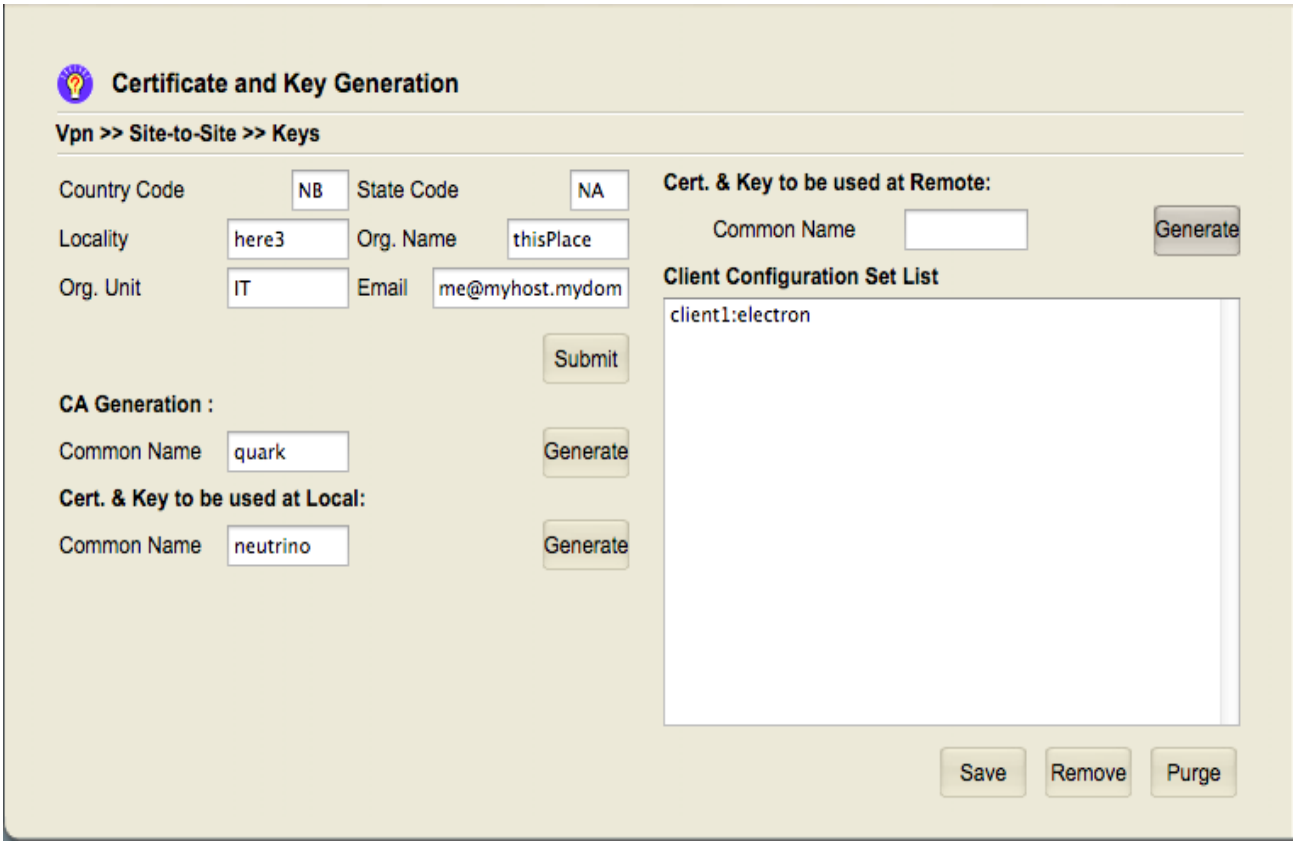
サーバーキーと証明書は、「Common Name」を入力し、「Generate」ボタンを押すことで生成されます。

クライアントキーと証明書を生成するには、「共通名」フィールドに入力し、「生成」ボタンを押します。



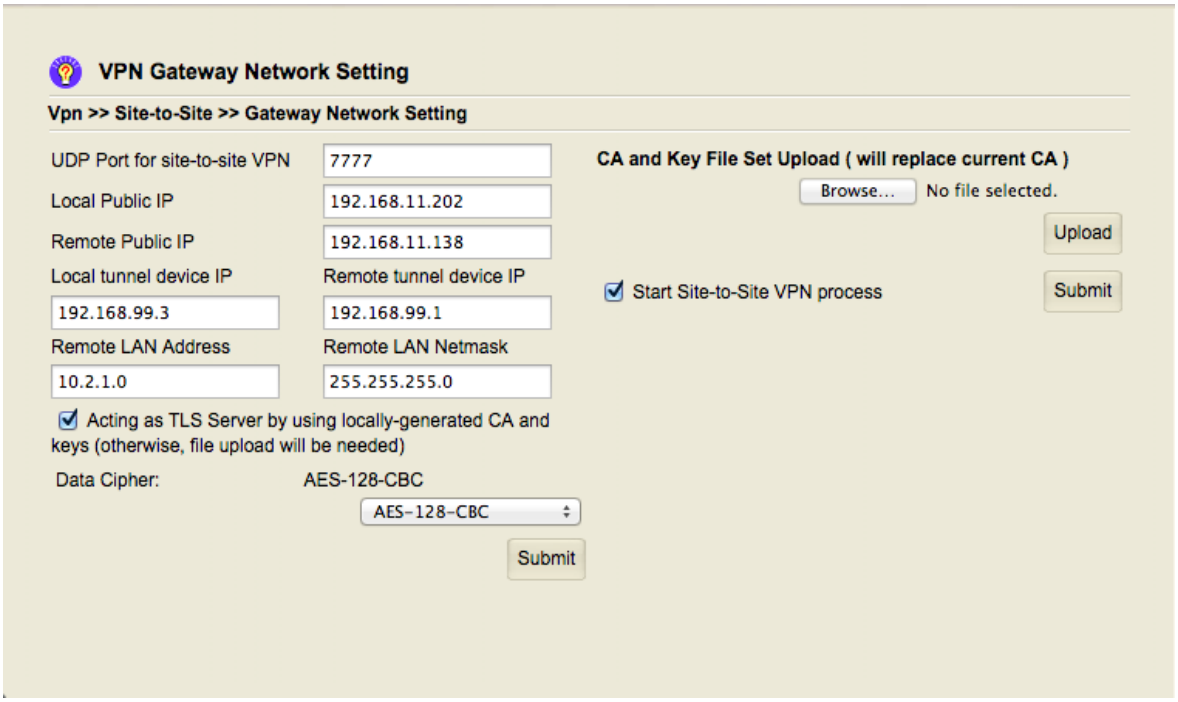

挿絵 ***116:*** サイトからサイト ***VPN:*** クライアントキーと証明書生成

挿絵 ***117:*** サイトからサイト ***VPN:*** キー生成のサンプル



この側のクライアントキーと証明書は、もう一方の側に送信する必要があります。ファイルを選択して「保存」ボタンを押してダウンロードし、その対応する右側の「**Vpn >> Site-to-Site >> Gateway Network Setting**」メニューで遠隔マシンにアップロードしてください。

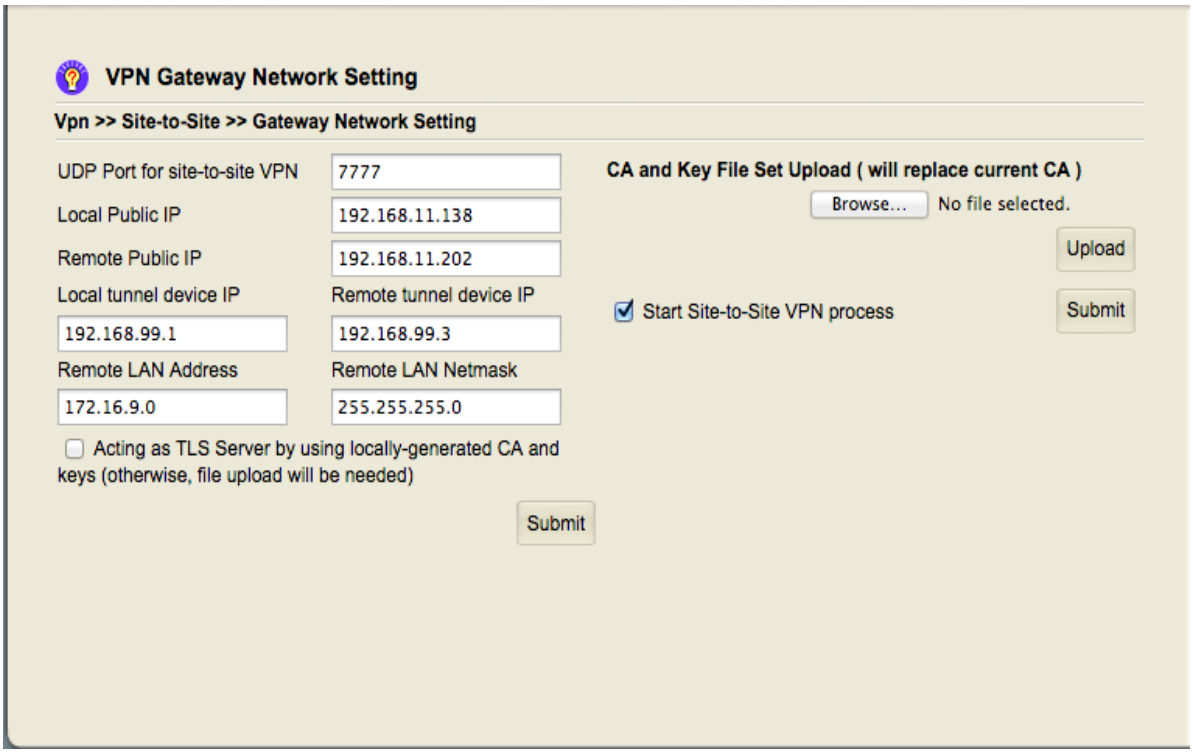
以下の二つのスクリーンショットは、二つの VPN ゲートウェイの設定例です。




挿絵 ***118: VPN*** ゲートウェイとして ***TLS*** サーバー

ホストは IP アドレス“192.168.11.202”で、対向先は IP アドレス“192.168.11.138”です。ローカルトンは IP アドレス“192.168.99.3”で、リモートトンは IP アドレス“192.168.99.1”です。リモート側では、サブネット“10.2.1.0/255.255.255.0”があります。ネットワークパケットがサブネット“10.2.1.0/24”に送信される場合、この VPN ゲートウェイを通してルーティングする必要があります。

以下のリモートホストの設定です。

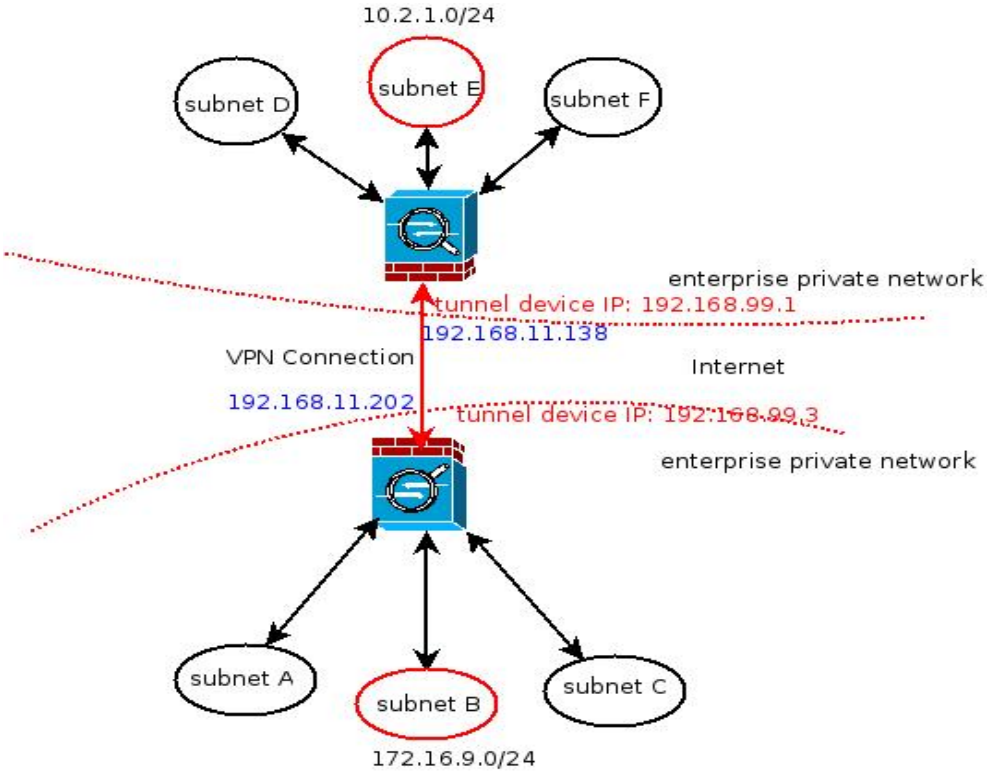



挿絵 119: リモートサイトの VPN ゲートウェイ

同様に、このホストは IP アドレス“192.168.11.138”で、サイトツーサイト VPN 接続は“192.168.11.202”です。ローカルトンデバイスは IP アドレス“192.168.99.1”を使用しており、リモートトンデバイスは IP アドレス“192.168.99.3”です。もう一方の端では、サブネット“172.16.9.0/24”を使用しており、そのトラフィックは、このゲートウェイ経由でルーティングする必要があります。

もちろん、これはラボで使用する設定です。それらをインターネット上で使用する場合は、”192.168.11.202”と“192.168.11.138”という IP アドレスをパブリック IP アドレスに置き換えてください。

この設定が期待どおりに機能するためには、2 つのサブネット“172.16.9.0/24”と'10.2.1.0/24”の間にあるホストが互いに到達できる必要があります。それらのホストのデフォルトゲートウェイまたは対応するサブネットの VPN ゲートウェイの IP アドレスに、それぞれのサブネットの VPN ゲートウェイの IP アドレスが設定されている必要があります。

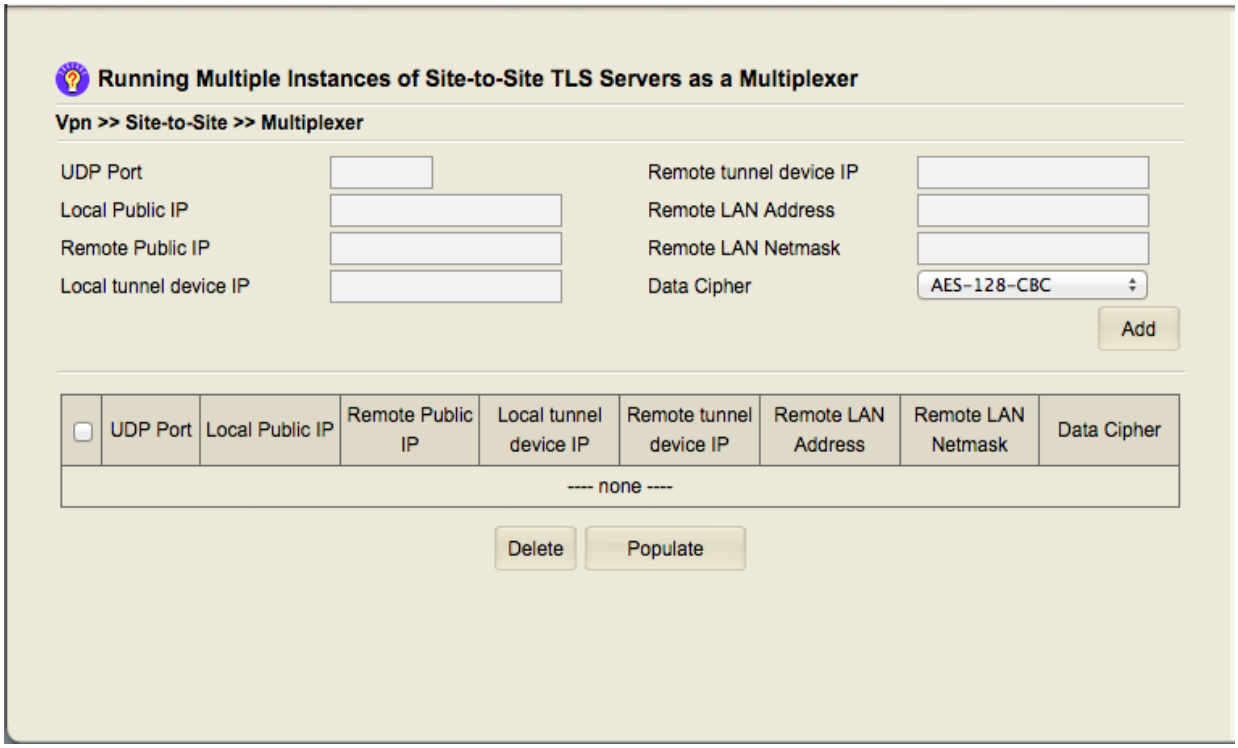



挿絵 ***120:*** サイトからサイト ***VPN*** サンプル設定

例えば、図の底にある VPN ゲートウェイは IP アドレス“172.16.9.1”で、サブネット“172.16.9.0/24”に接続します。そのサブネット内のホストは、“172.16.9.1”をゲートウェイとして使用し、“10.2.1.0/24”に到達する必要があります。

その他のサブネットに到達するため、VPN ゲートウェイのメインルーティングテーブルには、各リモートサブネットへの経路を追加する必要があります。

一台の機械で複数のインスタンスのサイト・ツー・サイト VPN を使用する可能性があります。UDP ポートの設定以外は、上記で紹介した設定とほぼ同じです。各インスタンスについては、この機械を“TLS サーバー”として設定し、異なる UDP ポートでリクエストをリッスンする必要があります。




挿絵 ***121:*** サイトツーサイトミキサーの画面スナップショット

フィールドは、サイト間 VPN を確立する際のそれと同じものです。注意が必要です。複数のインスタンスが同じサーバーキーと証明書を「Vpn >> Site-to-Site >> Keys」の下で共有しているため、それらはすべて TLS サーバーである必要があります。複数のサイト間 VPN インスタンスを使用する場合、同じマシン上で TLS サーバーとクライアントの両方を設定することはできません。そうすると、CA が破損します。

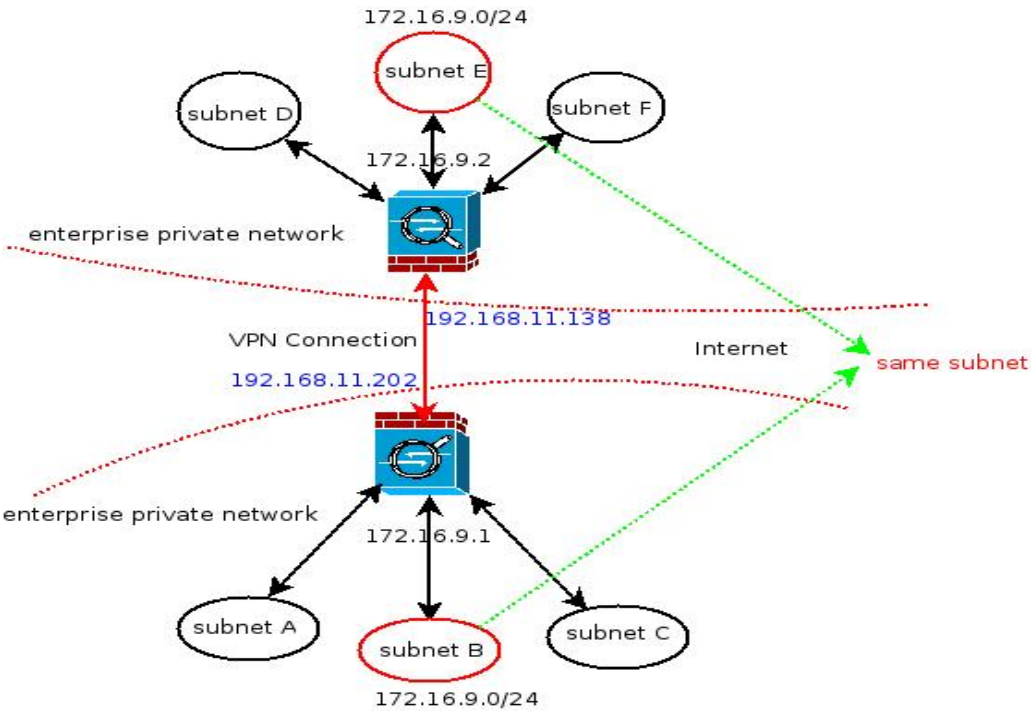
## *Site-to-site VPN in Bridging Mode*

サイトツーサイト VPN をブリッジモードで使用すると、本来ローカル使用を目的としたネットワークトラフィックがインターネットを経由して相手側へ到達するという問題点があります。例えば、DHCP クライアントが DHCP サーバーを探したり、uPnP デバイスを探したりするメッセージは、本来 IP サブネット内に限定されるべきですが、サイトツーサイト VPN をブリッジモードで使用すると、そのトラフィックは相手側へ到達します。これはネットワークプロトコルの問題ではなく、サイトツーサイト VPN をブリッジモードで使用すると、二つのネットワークが一つ目の IP サブネットのように機能するためです。そのため、使用を決定した場合、ネットワーク機器の再構成が必要になる場合があります。例えば、IP サブネット内に DHCP サーバーを一つだけ持つようにし、二つのネットワーク部分が結合される際に IP 競合がないか調査する必要があります。

ただし、サイトからサイト VPN をブリッジモードで利用する場合、そのメリットとして、IP マルチキャストパケットが VPN 接続を介して対向サイトに渡ることが可能である。IP マルチキャストパケットは、ほとんどの ISP（インターネットサービスプロバイダ）がそれらのパケットをルーティングしないため、インターネットを介しては渡ることができない。また、ルーティングプロトコル OSPF も、その Hello または Discovery メッセージに IP マルチキャストを使用する。したがって、サイトからサイト VPN をブリッジモードで利用することで、これらのデプロイメントの問題を簡素化できる場合がある。

以下の図を用いて、ブリッジモードにおけるサイト間 VPN の設定を説明します。192.168.11.202 と 192.168.11.138 という IP アドレスを持つ 2 台の機器を使用します。 インターネットを使用する際には、これらの IP アドレスはパブリック IP アドレスである必要があります。 目的は、ブリッジモードでサイト間 VPN 接続を確立し、サブネット “172.16.9.0/24” が 192.168.11.202 と 192.168.11.138 の背後に見えるようにすることです。

VPN プロセスによって作成された仮想ネットワークデバイスは、IP アドレスを持っていません。それは単にイーサネットフレームを扱います。他のネットワークインターフェースとの間でイーサネットフレームを交換するため、この VPN プロセスによって作成されたネットワークデバイスは、他のネットワークインターフェースとブリッジに結合する必要があります。




挿絵 122: ブリッジモードにおけるサイト間 VPN の例

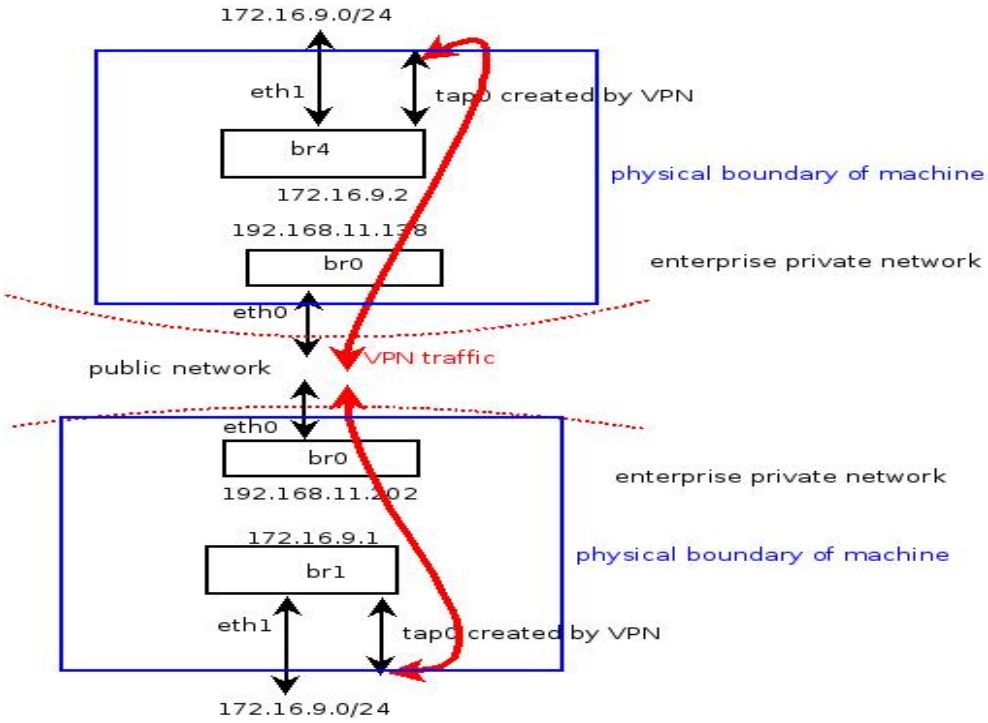
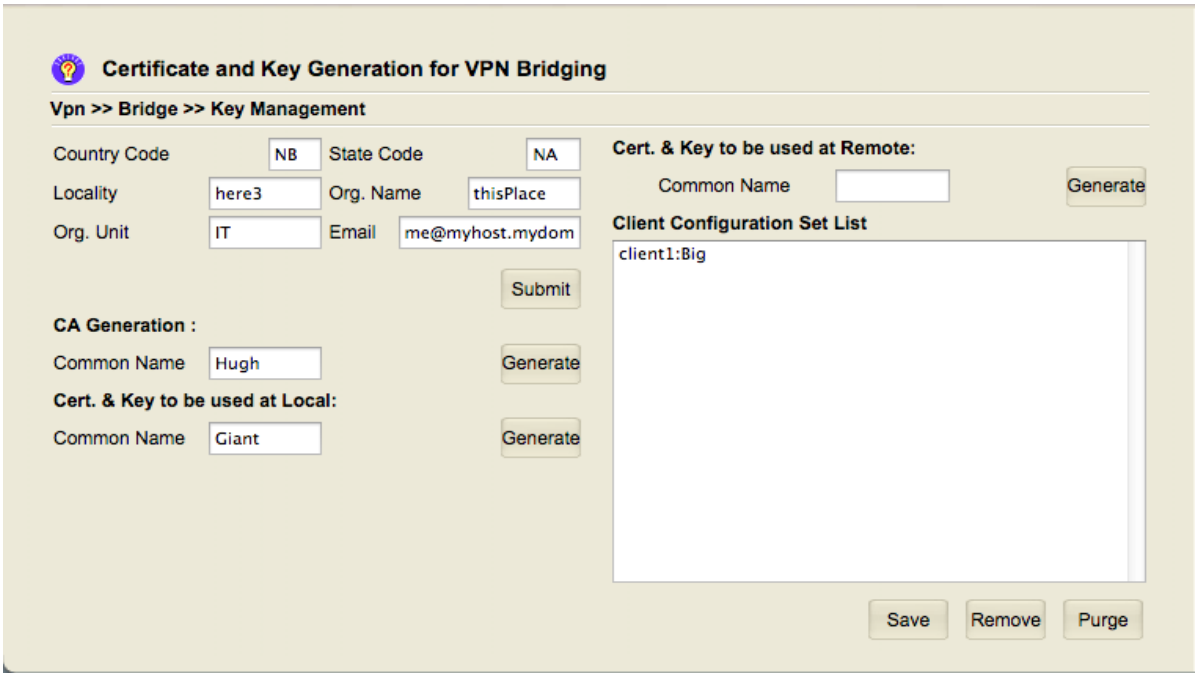



イラスト ***123:*** ブリッジモードにおけるサイト間 ***VPN*** の詳細な操作手順

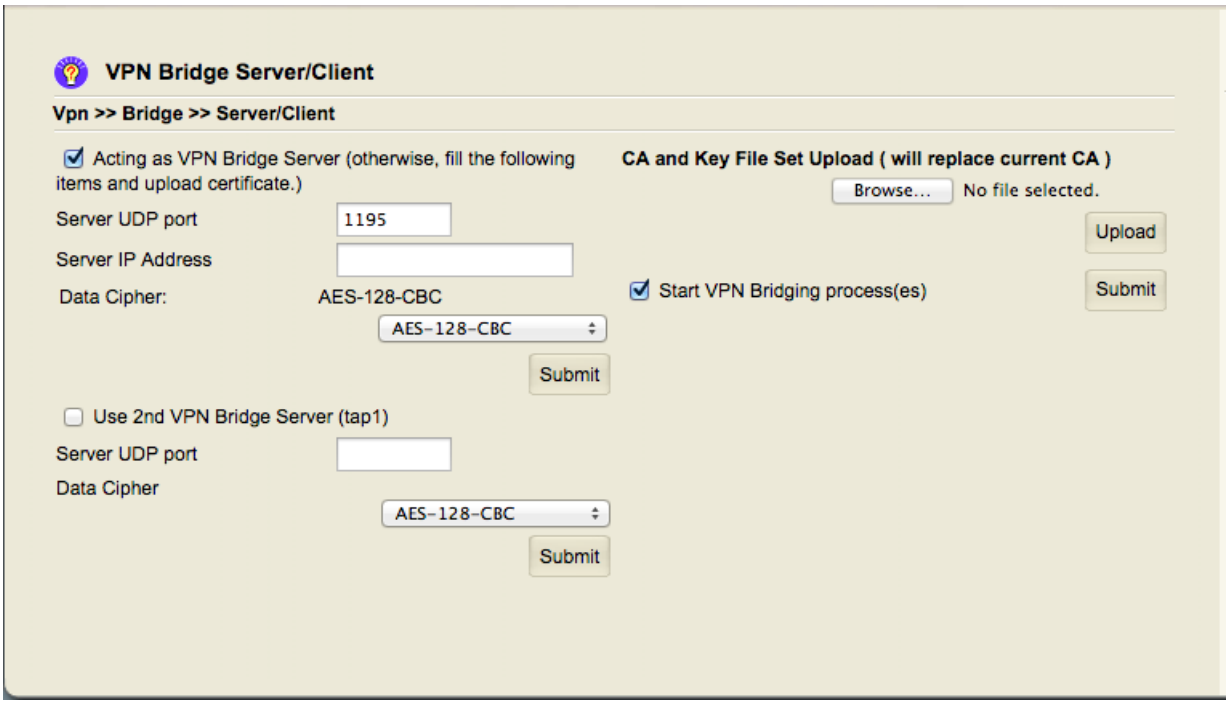
ベースプラットフォームでは、事前に仮想ブリッジが作成されており、物理ネットワークインターフェイスも用意されています。この操作で追加のブリッジを作成する必要はありません。「tap0」は VPN プロセスでブリッジングモードで作成されたネットワークデバイスを使用します。したがって、「tap0」が各サイトでブリッジに参加させ、2 つのサイトにある VPN プロセスが同じ IP サブネットの下で 2 つのブリッジを統合します。各ブリッジに IP アドレスを割り当て、同じサブネットにある 2 つのブリッジは異なる IP アドレスを設定する必要があります。

それがおおよそサイトツーサイト VPN のブリッジモードにおける設定のアイデアです。
CA、サーバーキーと証明書、クライアントキーと証明書を作成します。同様に、これらはクライアントツーサイト VPN とサイトツーサイト VPN（ルーティングモード）で独立して設定されます。“Vpn >> Bridge >> Server/Client”で作成できます。

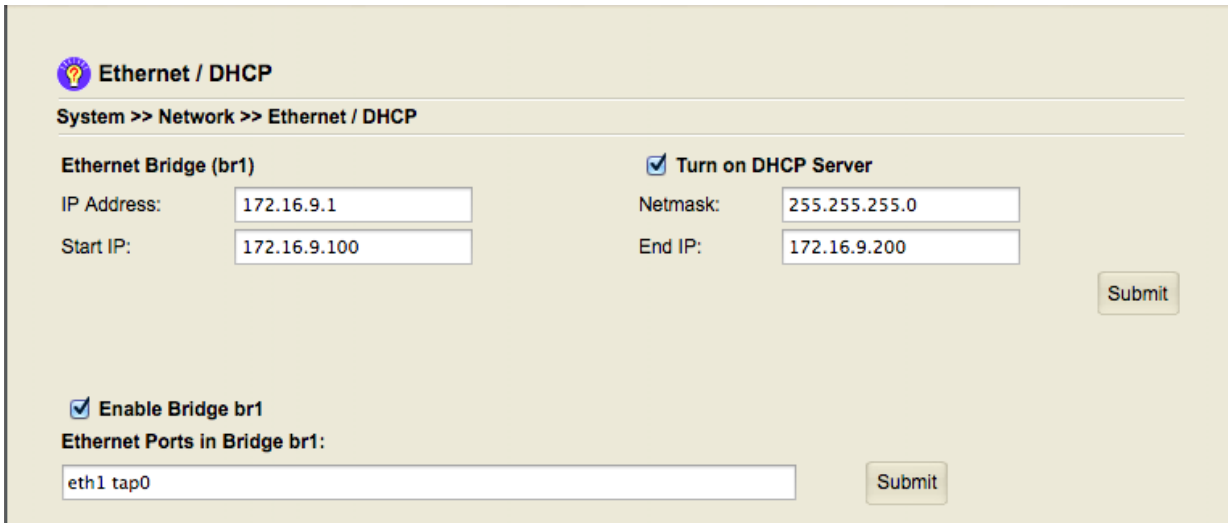



挿絵 ***124: CA***、鍵、およびブリッジモードにおけるサイト間 ***VPN***のための認証局、鍵、および証明書

「192.168.11.202」というマシンで行っています。したがって、クライアントキーと証明書は他のマシンにダウンロードして提出する必要があります。CA およびサーバーキーとサーバー証明書はこのマシンにありますので、これを「VPN ブリッジサーバー」として使用します。



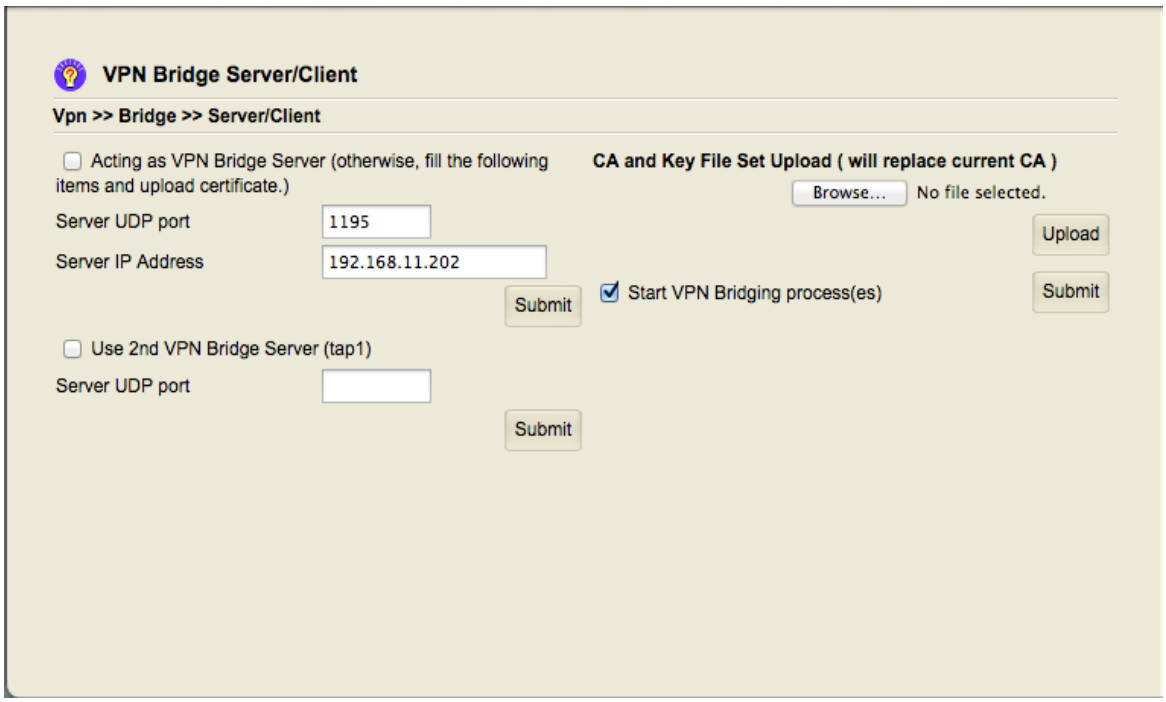

挿絵 ***125: VPN*** ブリッジサーバーのサンプル設定




挿絵 ***126: VPN*** ネットワークデバイスがブリッジ（サーバー側）に参加する例

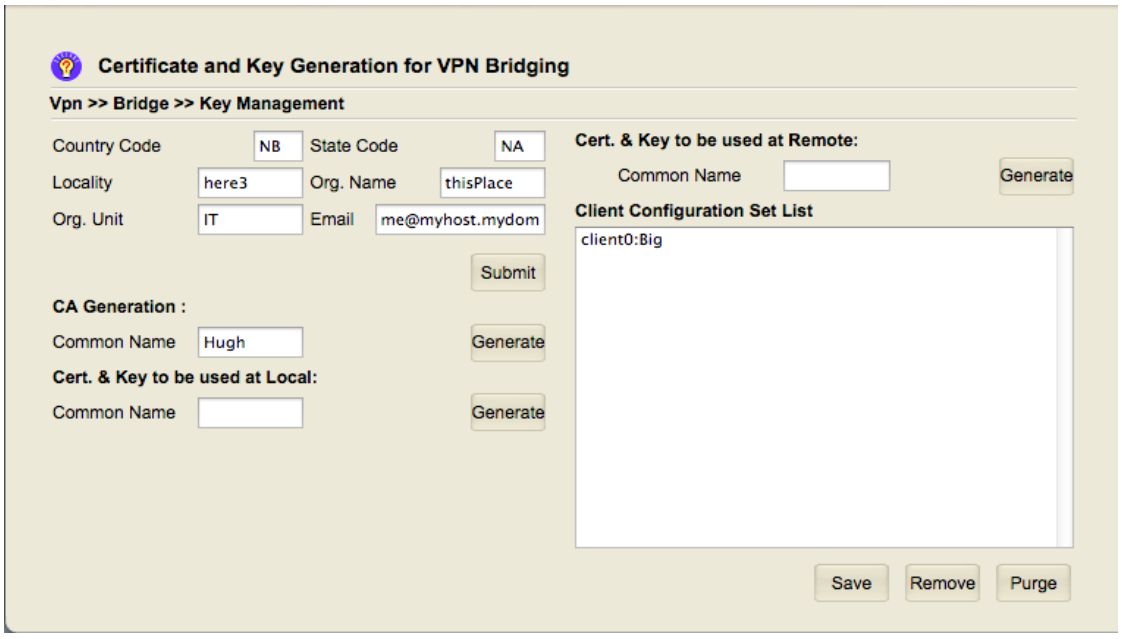
そして、「tap0」を仮想ブリッジ“br1”に“eth1”で接続することを忘れないでください。

もう一方の機械 (“192.168.11.132”) には、「Vpn >> Bridge >> Server/Client」メニューからクライアントキーと証明書をアップロードします。



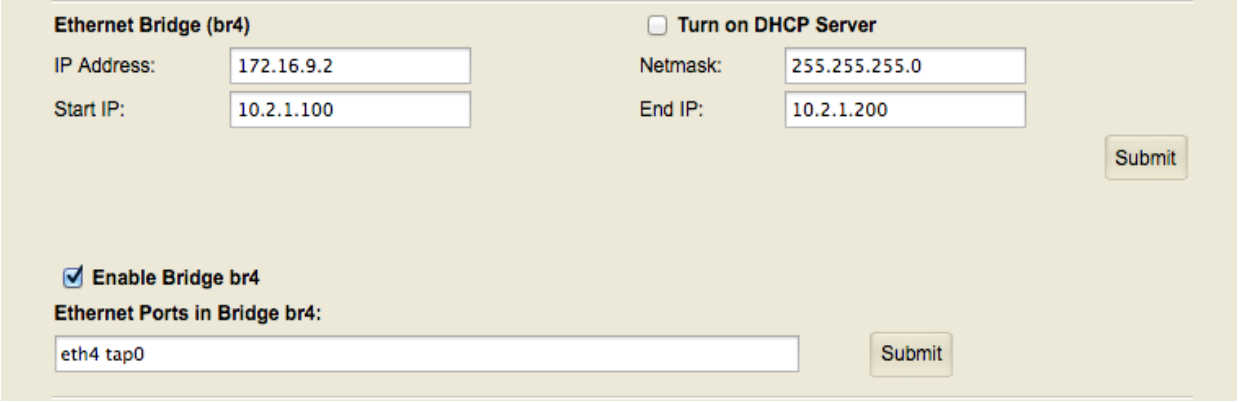

挿絵 ***127:*** ブリッジモードにおけるサイト間 ***VPN*** クライアントの設定サンプル

クライアントキーと証明書を送信した後、「VPN >> ブリッジ >> キー管理」画面が表示されます。




挿絵 ***128:*** クライアント側の証明書表示

そして、「tap0」をブリッジに参加させることを忘れないでください。




挿絵 ***129*** : ***VPN*** ネットワークデバイスがブリッジに参加するサンプル（クライアント部分）

上記の VPN 接続は UDP ポート 1195 を使用しています。したがって、境界制御へのアクセスを開けないとなりません。VPN 接続は両方のマシンを再起動した後で効果を発揮します。

ネットワークデバイスが仮想ホストのために作成された場合、それらはすべて「tapN」としてラベル付けされます。これらのデバイスは動的に作成されるため、site-to-site VPN in bridging mode が使用されていない場合、sometimes “tap0” が仮想ホストによって所有されることがあります。site-to-site VPN in bridging mode を使用する場合は、必ずシステムを再起動して VPN を有効にし、その後、仮想ホストを 1 つずつ有効にしてください。

# 第 5 章 動的ルーティング

このドキュメントにおける「ルーティング」とは「IP ルーティング」を指します。理論的には、ネットワークレベルでパスを選択することを指しますが（例えば、電話網や IP 網）、ここでは「IP 網」に焦点を当てます。まず、ベースプラットフォームにおける「静的ルーティング」と「動的ルーティング」の紹介を開始します。

“Static Routing”とは、ルーティングテーブルにエントリをマニュアルで追加する事を意味します。ネットワークインターフェースで直接接続されているサブネットに対しては、IP アドレスを設定する際に、対応するルーティングエントリをルーティングテーブルに加える必要があります。通常、「ルーティングエントリを追加する」というのは、特定の IP サブネットへのゲートウェイを指定する作業を指します。もしネットワークパケットの宛先に一致するサブネットがない場合、デフォルトゲートウェイに渡されます。

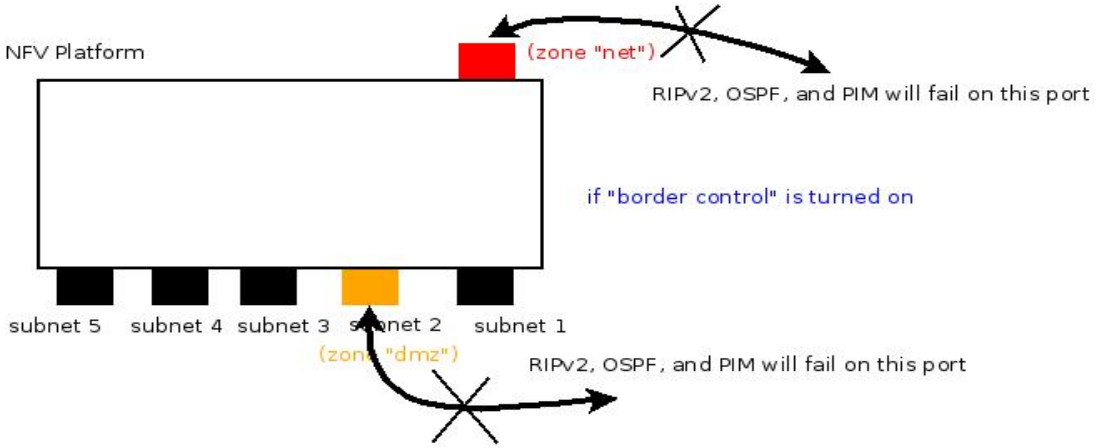
“静的ルーティング”は小規模なネットワークで有用であり、デバッグが容易です。しかし、大規模なネットワークでは、デフォルトでルーティングエントリを一つずつ手動で追加します。“動的ルーティング”は、この問題を解決するために、ルーティングテーブルを自動的に構築しようとします。これは、他のルーターと情報交換を行い、それに応じてルーティングテーブルを構築することによって行われます。

ベースプラットフォームの場合、通常は 12 の IP サブネットを持っています。もしこれらの 12 サブネットで十分であれば、”静的ルーティング”を使用するのに十分です。しかし、他のルーターが存在する場合、各ルーターにルーティングエントリを追加するのは困難になる可能性があります。

存在する他のシナリオは、単純な「静的ルーティング」では解決できないものがあります。例えば、IP マルチキャストを使用する環境では、各ホストは独自の「ユニキャスト」の IP アドレスを持っています。ある程度の機械が IP マルチキャストパケットを受信するためには、その機械は IP マルチキャストのグループアドレスに加入する必要があります。つまり、それらの機械は、それぞれの「ユニキャスト」の IP アドレス宛のパケットと、マルチキャストのグループアドレスのパケットを期待することになります。IP マルチキャストのグループアドレス（224.0.0.0～239.255.255.255）は、任意のサブネットに現れる可能性があります。もしそれらのホストを単一のサブネット内に制限して IP マルチキャストを使用したいのであれば、「静的ルーティング」では実現できません。

ベースプラットフォームでは、RIPv2（Routing Information Protocol , version 2）および OSPF を IP ユニキャスト（IPv4）向けに提供します。PIM（Protocol Independent

Multicast）は、サブネットを跨ぐマルチキャストルーティングに使用されます。




挿絵 ***130:*** 境界制御と動的ルーティング

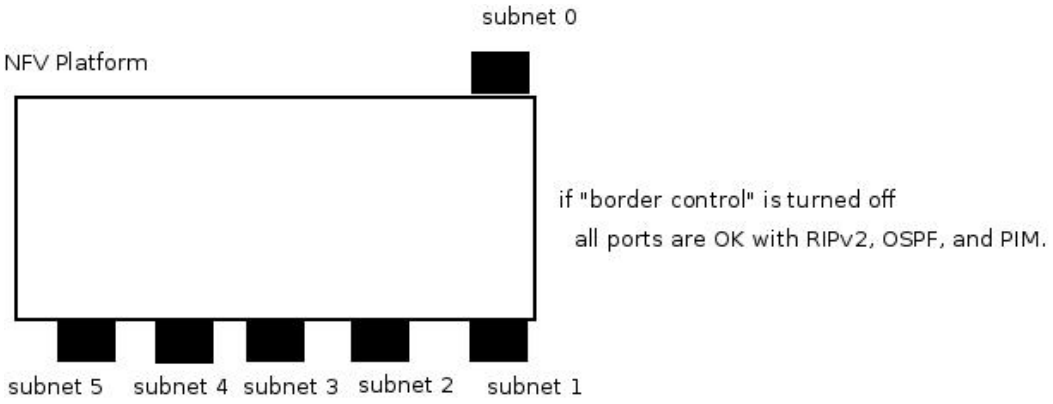
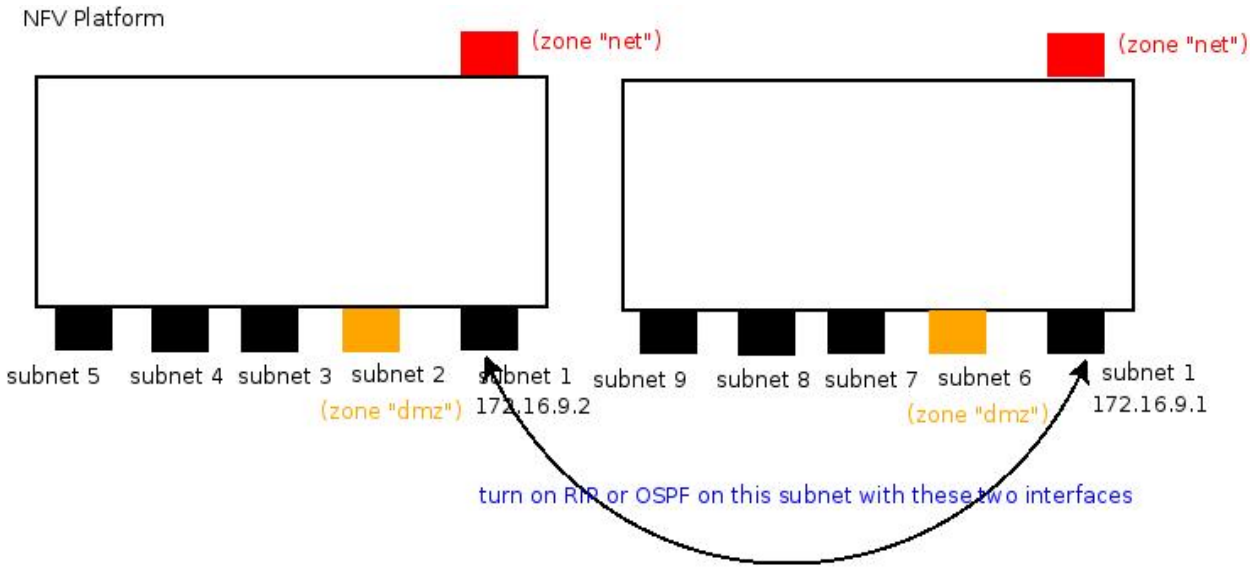



イラスト ***131: Border Control*** をオフにする

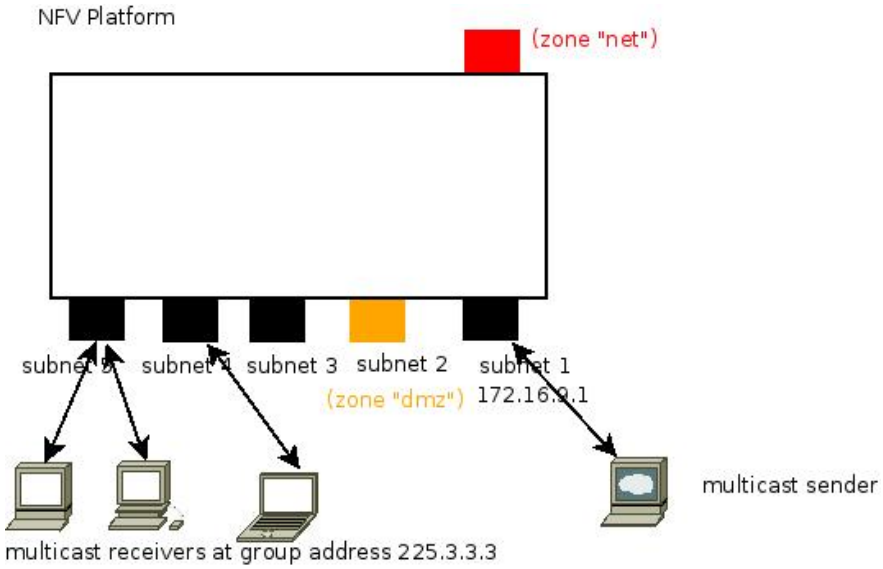
上記の図は、境界制御に関連するベースプラットフォームにおける一般的なネットワーク操作を示しています。それは、「境界 >> 接続 >> ポート転送」の設定でオンまたはオフに切り替えることができます。通常、“net” から “fw” へのトラフィックはドロップされ、“dmz” から “fw” へのトラフィックもドロップされます。したがって、RIPv2 および OSPF は 2 つのゾーンで失敗し、境界制御がオンになっている間は PIM も失敗します。これは念頭に置いて、動的ルーティングを適切に使用してください。

RIPv2 および OSPF（OSPF v2 は IPv4 用、OSPF v3 は IPv6 用）が正しく機能するためには、両者とも IP マルチキャストを使用して他のルーターを見つけます。一方、RIP バージョン 1 はブロードキャストを使用します。IP マルチキャストがサブネット内で機能するためには、そのサブネット上のネットワーク機器は IGMP をサポートする必要があります。

OSPF と RIP はルーティング間で利用され、PIM はマルチキャスト パケット が IP サブネット を横断 するために使用されます。

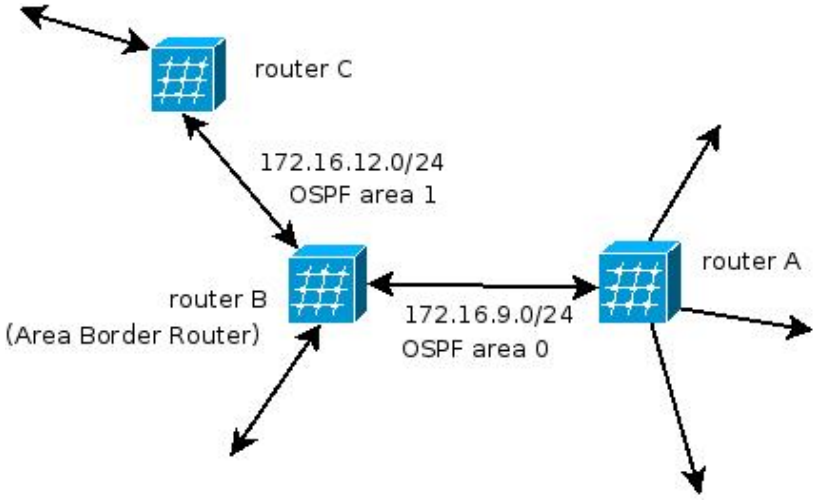



挿図 ***132: 2***台のマシンの連鎖



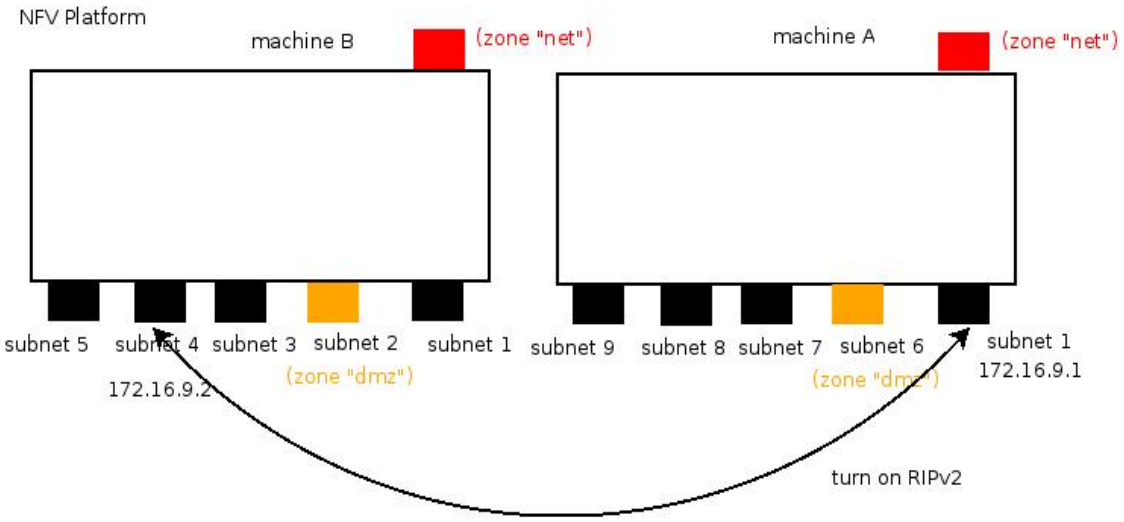

挿絵 ***133: PIM*** の使用に関するシナリオ

OSPF は“Area ID”という概念を使用します。“Area 0”はコアネットワークに使用され、値は 0 から 2^32-1 まで範囲、または a.b.c.d（例えば、1.1.1.1）の形式で設定できます。OSPF において、2 つのエリア間で 1 つのインターフェースを持つルーターは ABR（Area Border Router）と呼ばれます。




挿絵 ***134: OSPF ABR (***エリア境界ルーター***)***

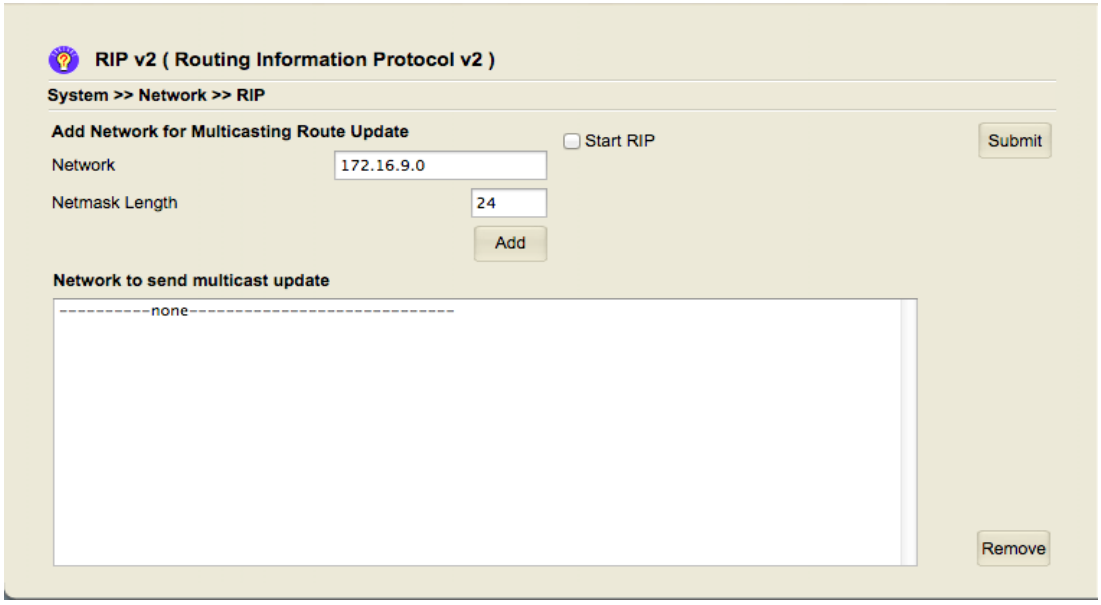
## *RIPv2 (Router Information Protocol, version 2)*



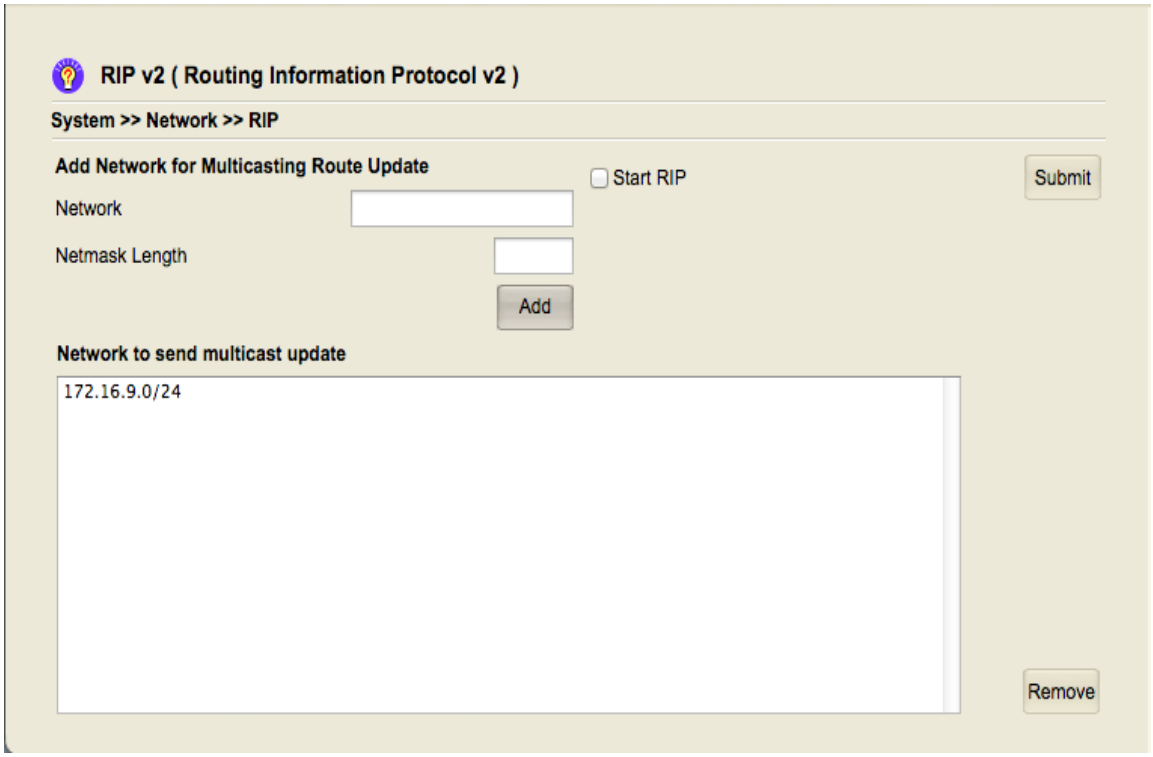

挿絵 ***135: RIPv2*** の例

私たちが RIPv2 を使用して 2 台の機械を接続し、ルーティングテーブルを交換し、個別にルートエントリを追加する必要がないようにしたいと考えています。機械 A の 1 つの物理ポートが機械 B のポートに接続され、機械 A ではその物理ポートが“br0”の下に配置され、機械 B では“br4”の下に配置されます。2 つのポートはそれぞれ IP アドレス“172.16.9.1”および“172.16.9.2”で同じサブネットに接続されます。

両ポートが接続されたら、以下の手順で設定します。マシン A で、「System >> Network >> RIP」をブラウズし、送信するサブネットを指定します。

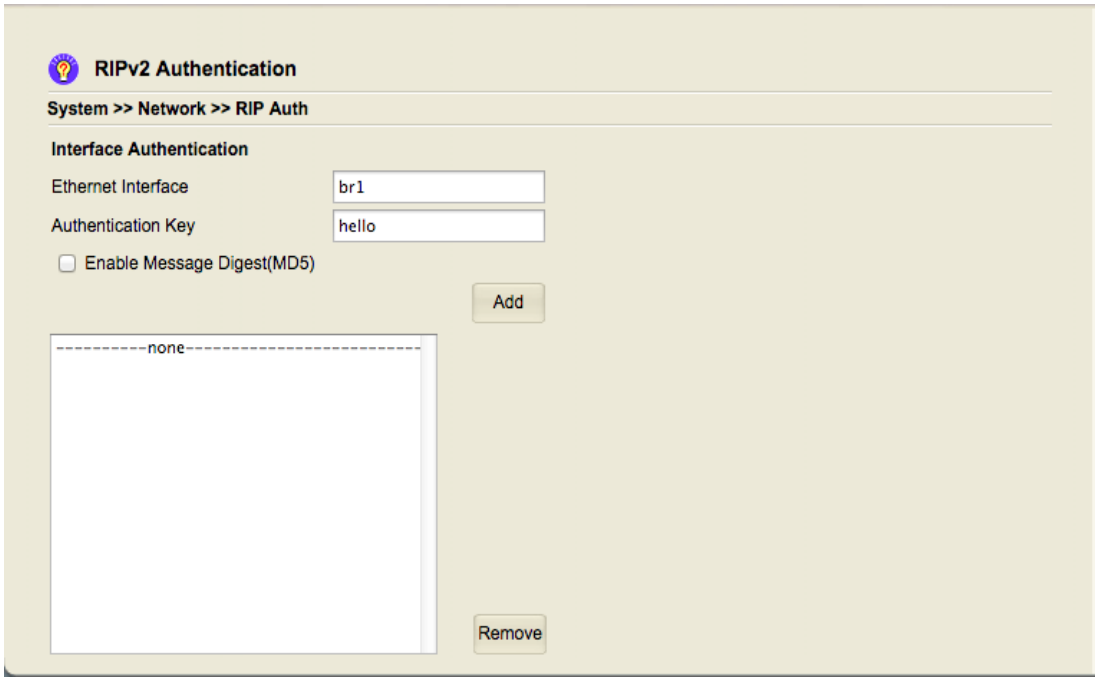



挿絵 ***136: RIPv2*** の送信用マルチキャスト・サブネット

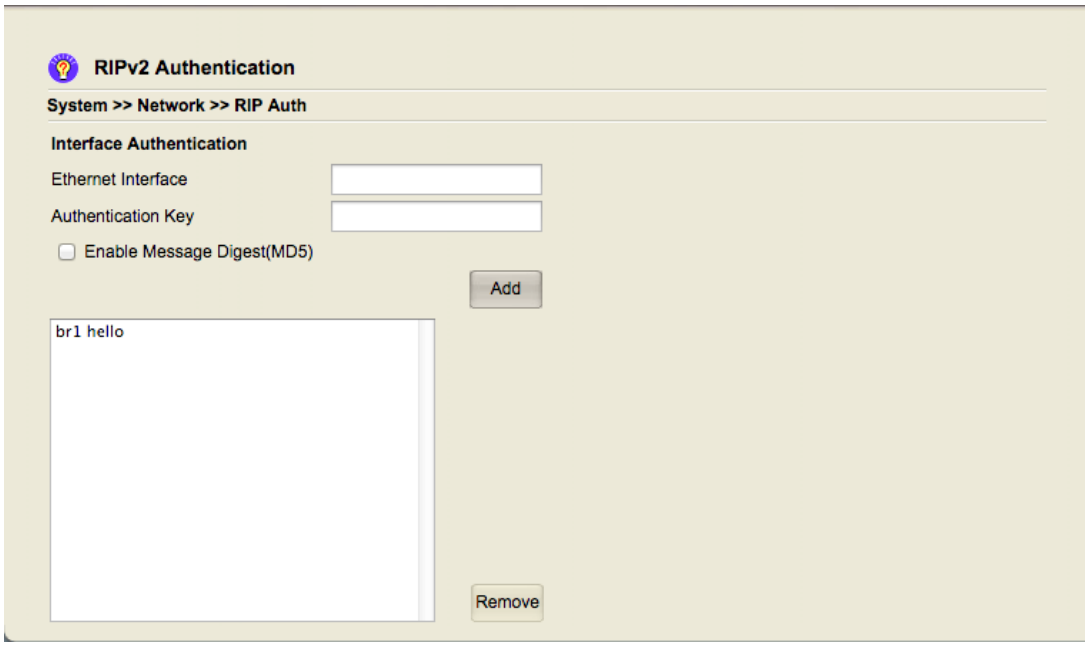



挿絵 ***137:*** 送信するサブネットのリスト（マルチキャストアップデート）

インターフェースへの情報を交換するために、送信先の更新には認証キーを設定する必要があります。これは、「System >> Network >> RIP Auth」で行うことができます。

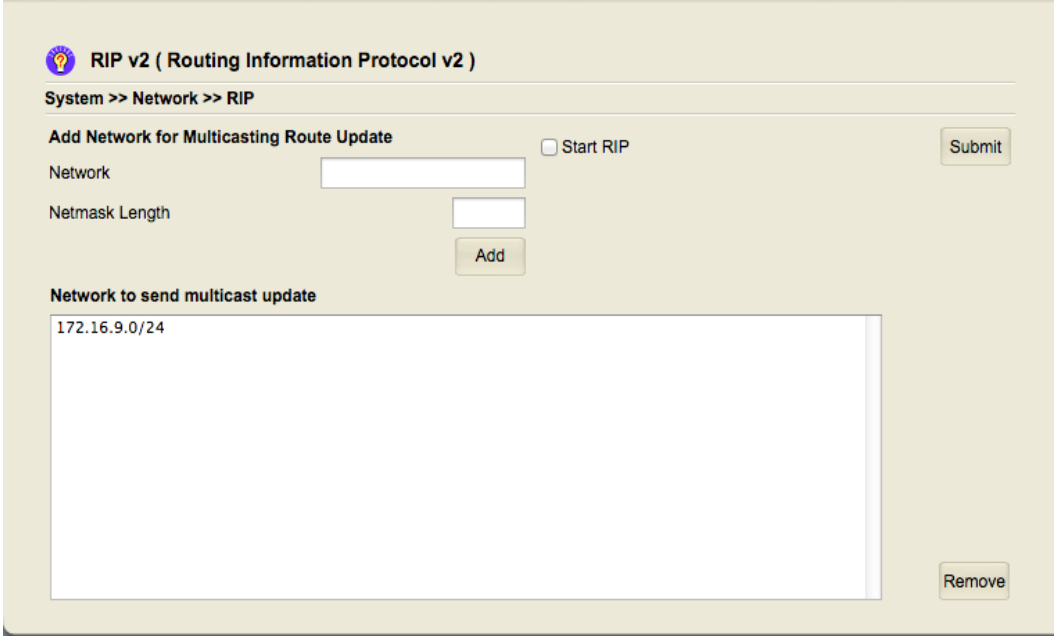



挿絵 ***138: RIPv2*** の認証キーを設定する

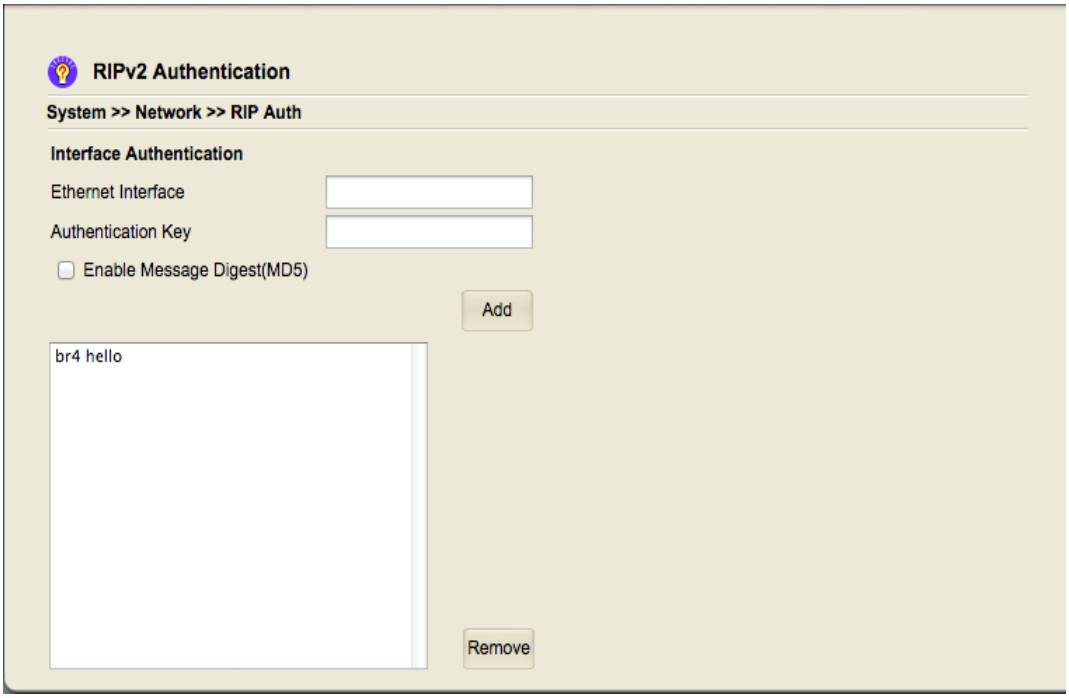



挿絵 ***139:*** 認証キーのリスト

機械 B の側にも同様の構成があります。
サブネットと認証キーを次のように設定します。

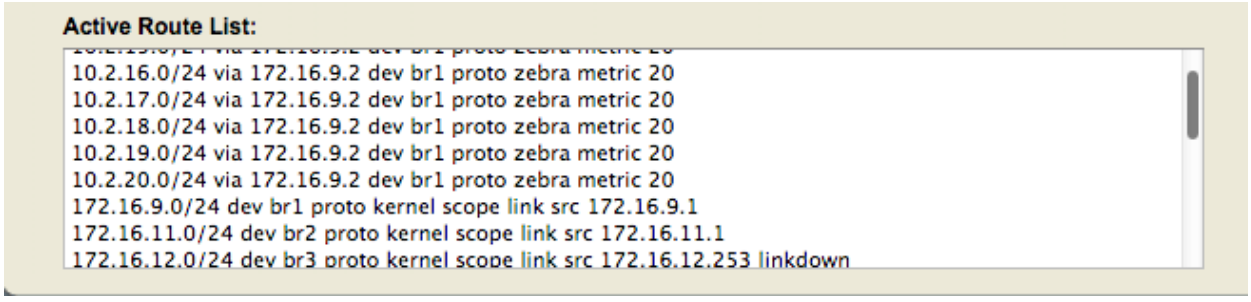



挿絵 ***140:*** マルチキャスト更新のための別のマシン上のサブネット



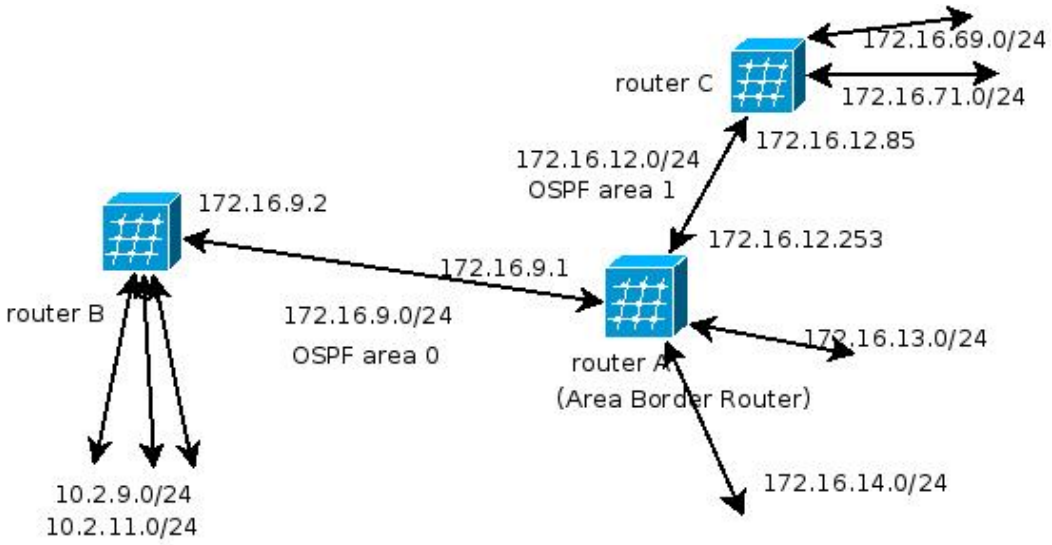

挿絵 ***141:***認証キーのリスト

認証キーは“br4”で設定されます。次に、RIP ルーティングプロセスを開始するために“System >> Network >> RIP”のチェックボックスを選択します。“System >> Network >> Static Routing”でルーティングテーブルを確認すると、相手側のサブネットがルーティングテーブルにリストされているのを確認できます。以下が“machine A”として知られています。




挿絵 ***142*** : ***RIPv2*** を開始した後のルーティングテーブルの内容

## *OSPF(Open Shortest Path First)*




挿絵 ***143: OSPF*** 構築例

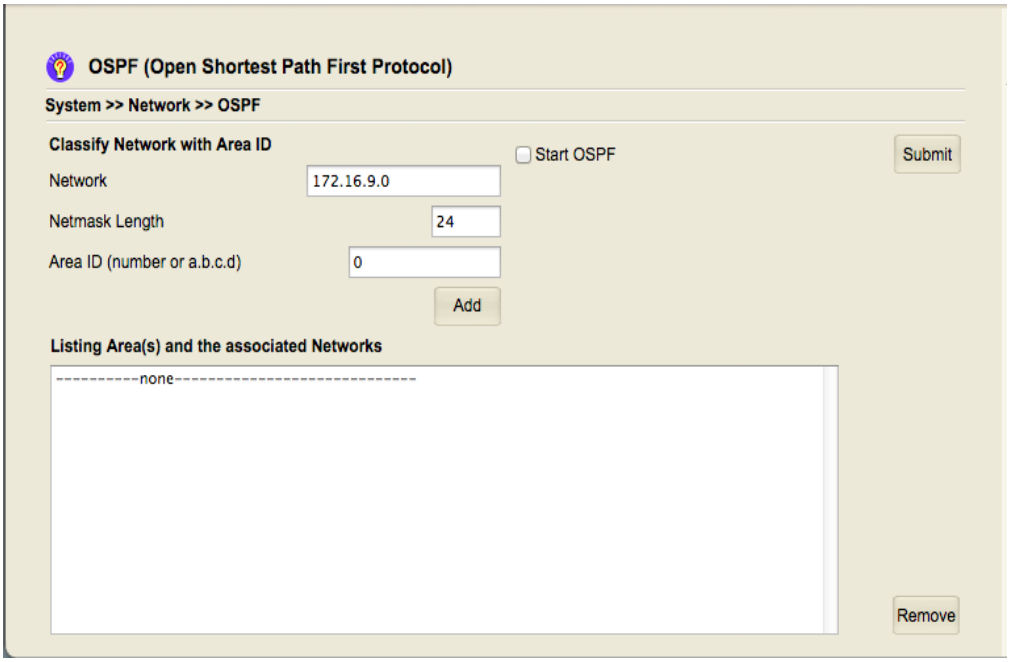
上記の図を例として OSPF ルーティングを設定します。OSPF ルーターとして使用するベースプラットフォームのインスタンスが 3 つあり、それぞれ“router A”、“router B”、“router C”と指定されています。各ルーターの下にある IP サブネットは以下の通りです。

ルーター A: 172.16.9.0/24, 172.16.11.0/24, 172.16.12.0/24, 172.16.13.0/24
172.16.14.0/24, 172. 16.15.0/24, 172.16.16.0/24, 172.16.17.0/24, 172.16.18.0/24, 172.16.19.0/24, 172.16.20.0/24

ルーター B : 10.2.9.0/24、10.2.11.0/24、10.2.12.0/24、172.16.9.0/24
10.2.14.0/24, 10.2.15.0/24, 10.2.16.0/24, 10.2.17.0/24, 10.2.18.0/24, 10.2.19.0/24, 10.2.20.0/24

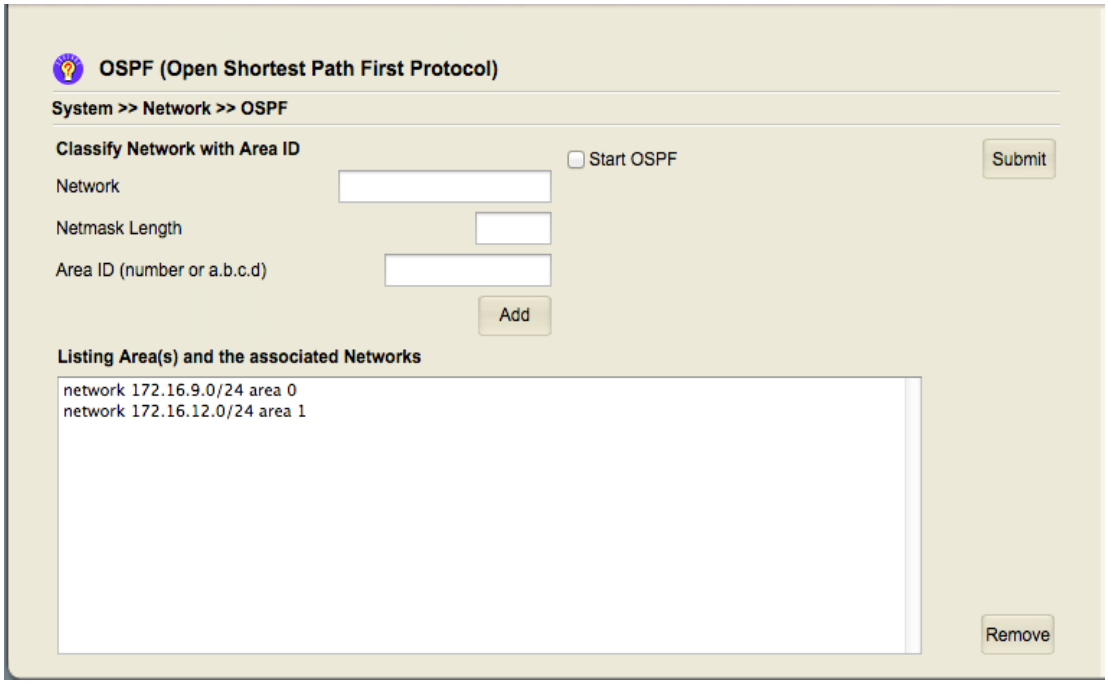
ルーター C: 172.16.12.0/24, 172.16.69.0/24, 172.16.17.0/24, 172.16.72.0/24
172.16.73.0/24, 172.16.74.0/24, 172.16.75.0/24, 172.16.76.0/24, 172.16.77.0/24, 172.16.78.0/24, 172.16.79.0/24, 172.16.80.0/24

ルーターAとルーターBが“172.16.9.0/24”に隣接している場合、それは“エリア0”として指定されます。ルーターAとルーターCが“172.16.12.0/24”に隣接している場合、それは“エリア1”として指定されます。エリアIDはOSPFにおいて0～2^32-1の間で設定可能です。数字“0”はコアネットワークを表します。それに加えて、これまで述べたように、ゾーン“net”および“dmz”のサブネットを用いたOSPF更新は使用しないでください。OSPF更新はこれらの2つのゾーンでは機能しません。



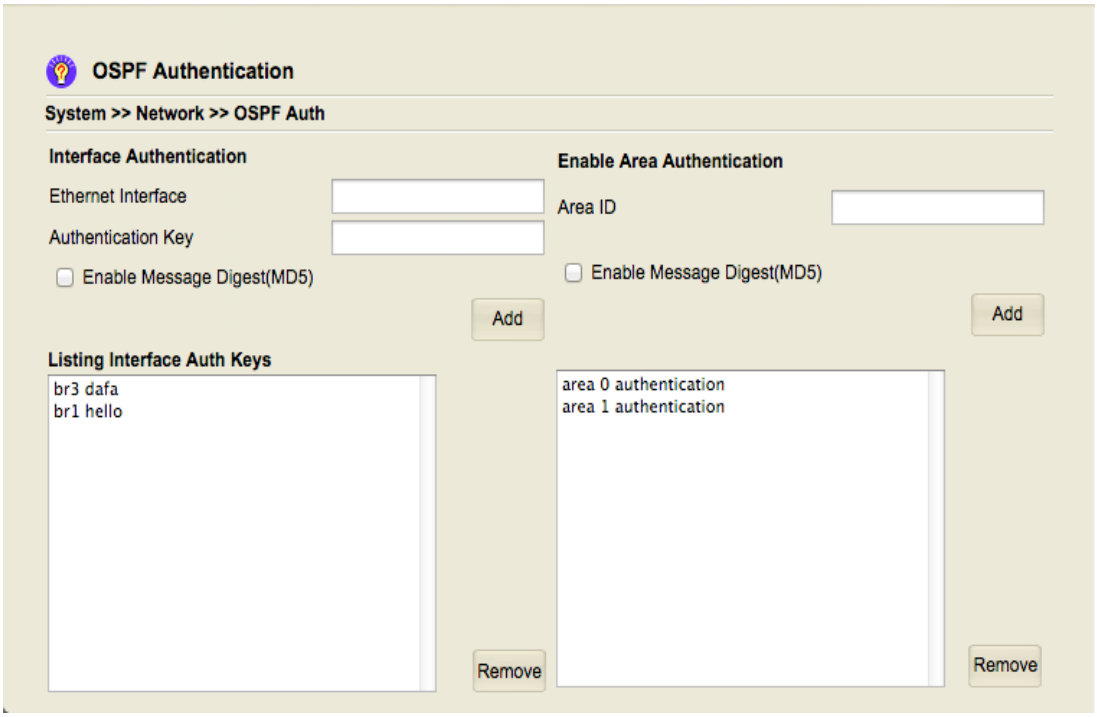

挿絵 144: サブネットおよびエリアIDの設定 (ルーター A)

「router A」では、「172.16.9.0/24」および「172.16.12.0/24」という2つのサブネットに対してOSPFアップデートを実行する必要があります。そのため、「System >> Network >> OSPF」でそれらを開示し、それぞれの「Area ID」を指定します。




挿絵 ***145:*** サブネットのリスト ***(***ルーター ***A)***

OSPF ルーターは互いに認証を行い、ルーティング情報がリモート機器から設定または受け入れられることを確認します。各インターフェースには「認証キー」が必要であり、対側の設定と一致させる必要があります。“エリア認証”が必要な場合は、「エリア ID」を入力して「Add」を押してください。

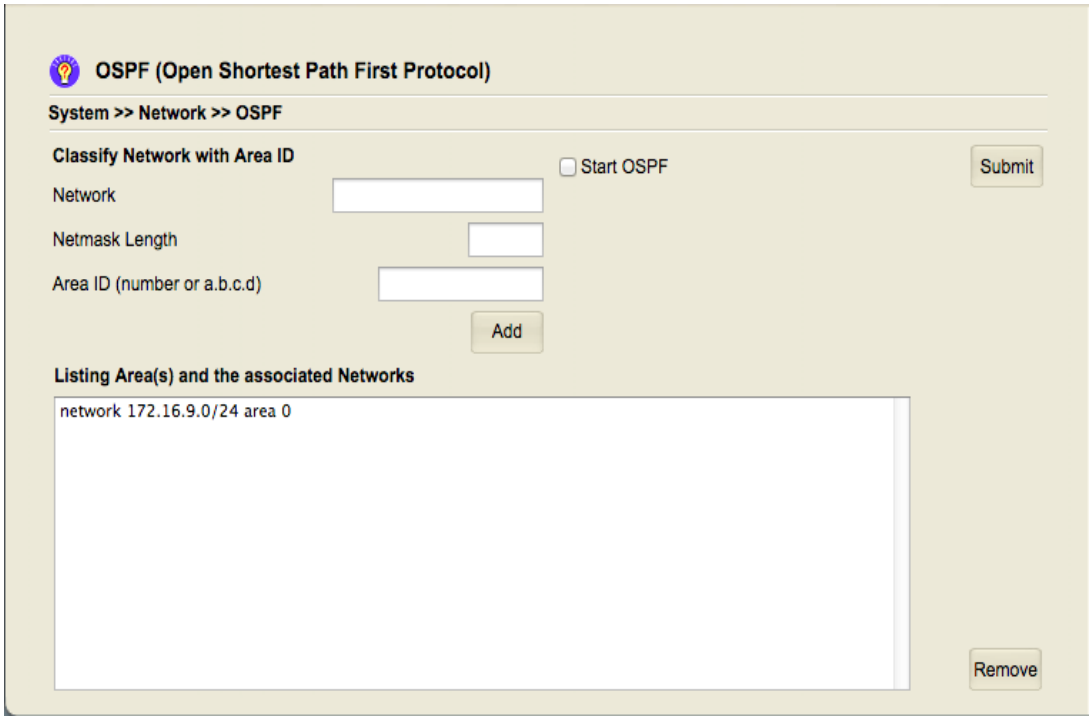



挿絵 ***146: OSPF*** の認証設定 ***(***ルータ ***A)***

「ブリッジデバイス」（“br0”、“br1”、“br11”など）上のインターフェースに IP アドレスが設定されています。これらのインターフェースはここで“Ethernet インターフェース”として使用されるべきです。これらのインターフェースの IP アドレスは、各ルーター間で“unique”である必要があります。これらのうちのいくつかは、各ルーターの“router ID”として使用されます。“router ID”はルーティングパスを計算するために使用されます。たとえ一部のサブネットが使用されていないと思われる場合でも、各ネットワークインターフェースにはユニークな IP アドレスを保持する必要があります。

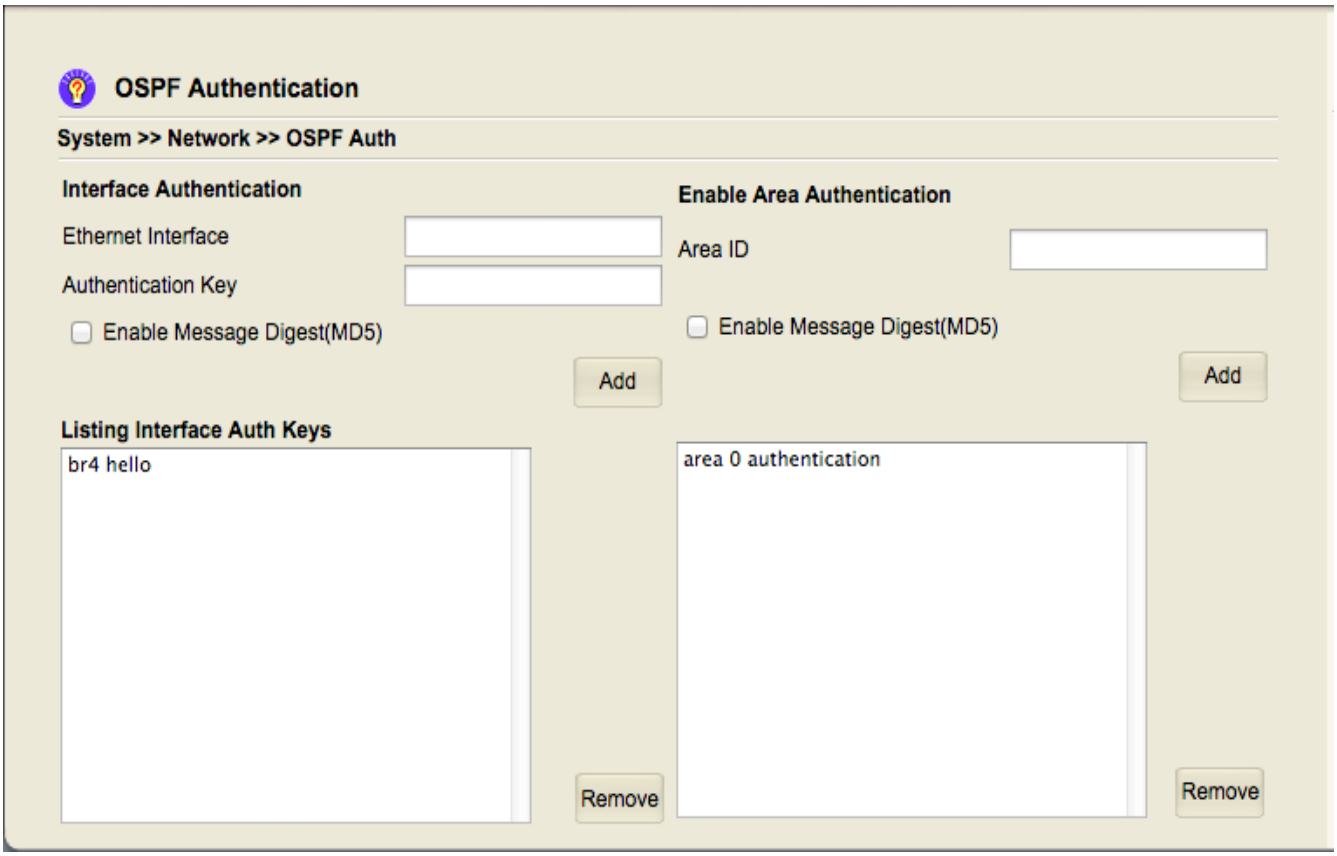
設定が完了したら、再度「System >> Network >> OSPF」にアクセスして、OSPF プロセスを開始できます。

以下の図は「ルーター B」の設定を示しています。




挿絵 ***147:*** サブネット設定（ルーター ***B***）

Authentication key は、“router A”で設定したものを一致させる必要があります。




挿絵 ***148:*** 認証設定 ***(***ルーター ***B)***

OSPF と“router A”と“router B”を起動した後、“router A”のルーティングテーブルを確認し、“router B”のサブネットが“router A”に転送されることを確認します。

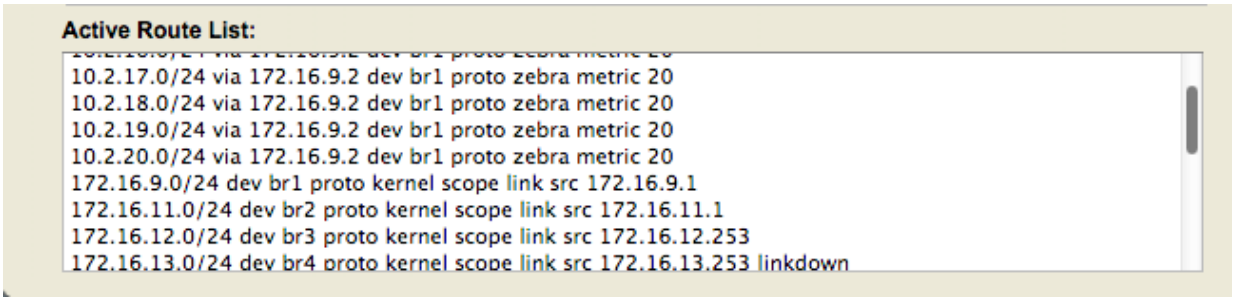



イラスト ***149:*** ルーター ***A*** の現在までのルーティングテーブル ***(OSPF*** を起動した後***)***

それでは「ルーター C」の設定に進みます。

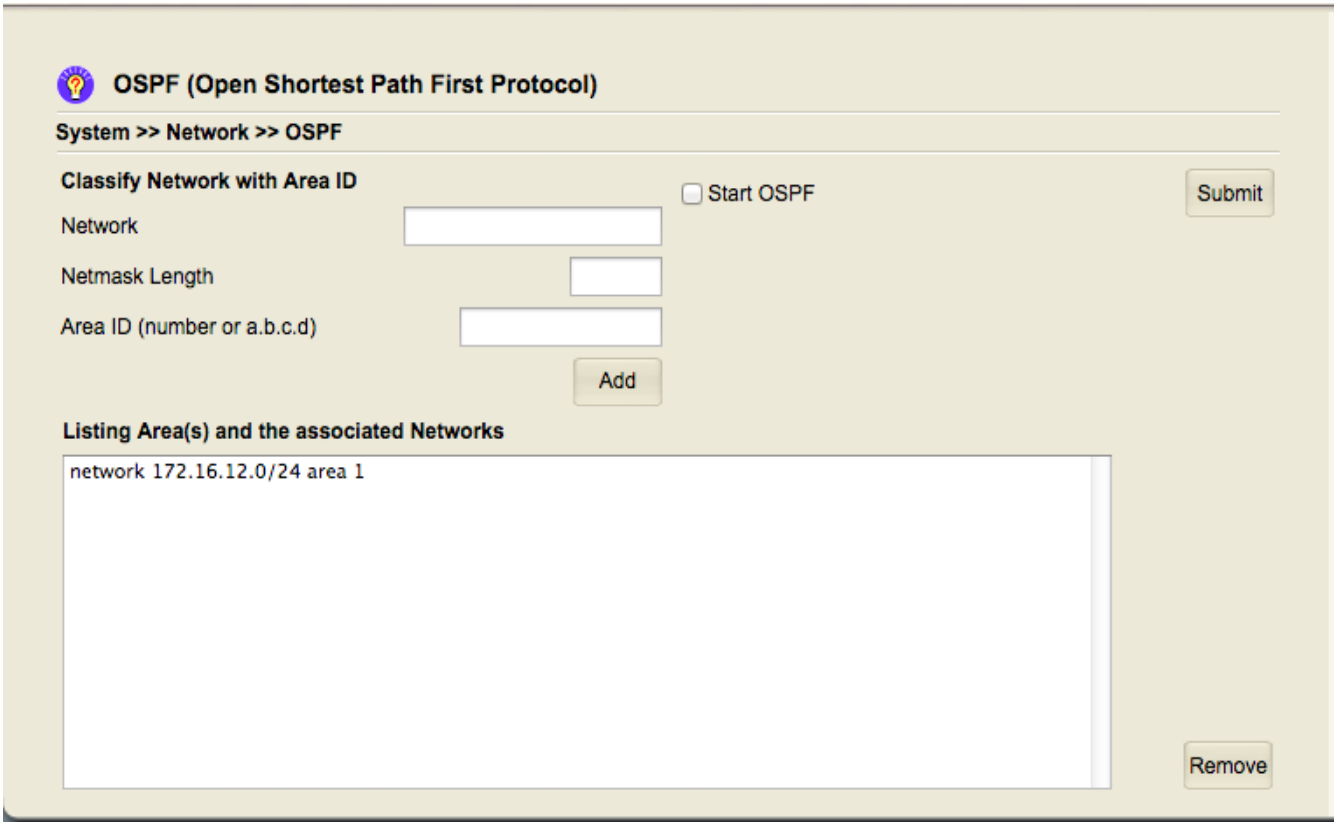
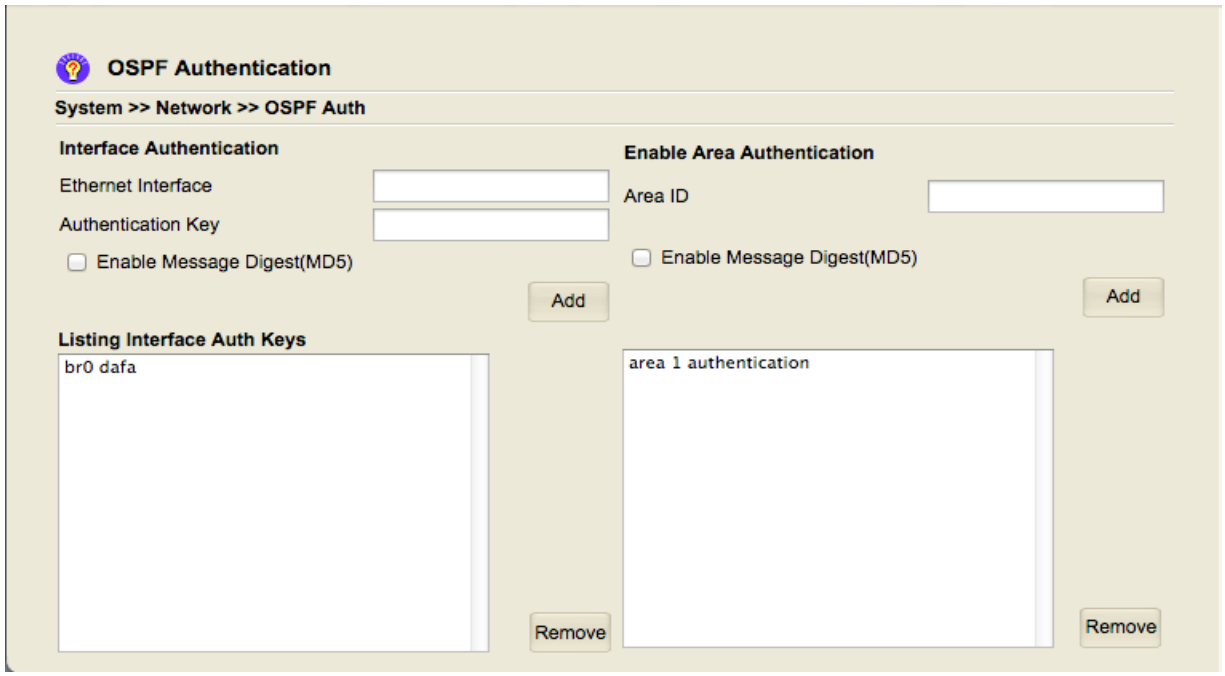
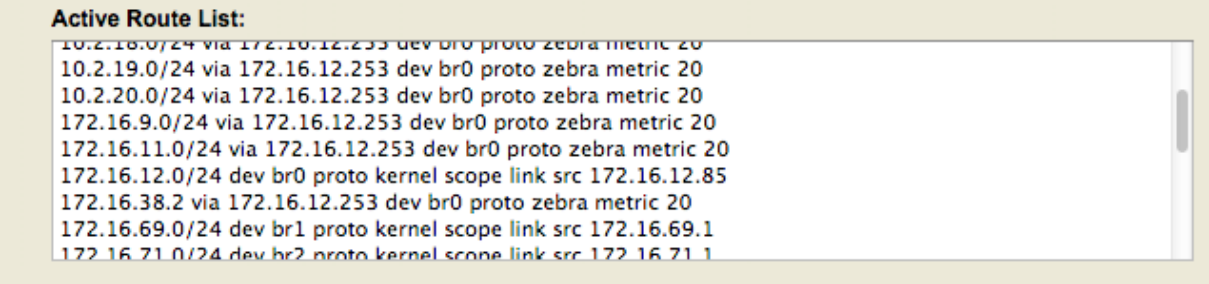



イラスト ***150:*** サブネット設定 ***(***ルーター ***C)***




挿絵 ***151:*** 認証設定 ***(***ルーター ***C)***

同様に、認証キーは「ルータA」で設定されたものと一致させる必要があります。OSPFを「ルータC」で開始した後、「ルータC」のルーティングテーブルは以下の通りです。




挿絵 ***152:*** ルーター表 ***(***ルーター ***C)***

もしサブネットへのリンクがダウンしている場合、対応するルーティングテーブルのエントリは他のルータにポップレートされません。 場合によっては、関連するリンクがダウンしている理由を確認することがあります。

## *PIM(Protocol Independent Multicast)*

IP マルチキャストパケットを送信し、同じサブネットで受信するためには、そのサブネット内のすべてのネットワーク機器が IGMP (Internet Group Management Protocol) をサポートしていればよい。マルチキャストパケットが他のサブネットに到達するためには、ルーターが DVMRP (Distance Vector Multicast Routing Protocol)、MOSPF (Multicast Open Shortest Path First)、または PIM をサポートする必要がある。弊社プラットフォームでマルチキャストルーティングをサポートするために、PIM を使用する。詳細については、IETF RFC 1112 を参照のこと。

PIM は、一つの送信者が IP マルチキャストパケットを送信し、他のサブネットにある受信者がそれを受信できるようにするシナリオを実現するために使用されます。受信者が同じサブネットにある場合、PIM は必要ではなく、IGMP のみで十分です。

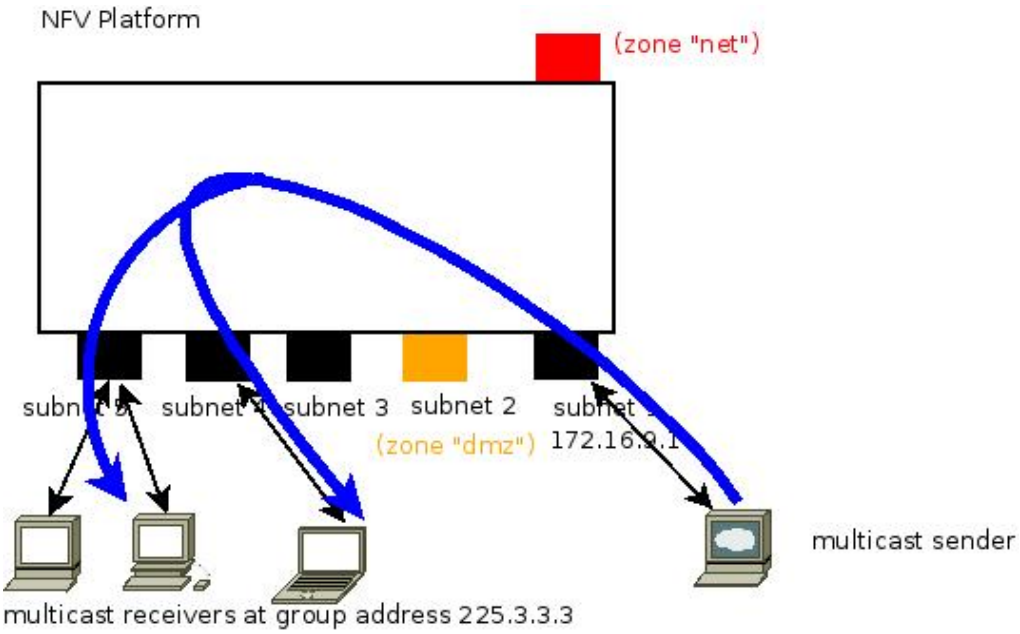



イラスト ***153: IGMP*** と ***PIM*** を使用するシナリオ

また、当社の基盤プラットフォームでは、ゾーン間のポリシーの影響も考慮する必要があります。　「net」ゾーンと「dmz」ゾーンからのパケットは、デフォルトで破棄されます。

上記のシナリオが起こるには、単に「**System >> Network >> Multicast Routing**」で PIM をオンにするだけです。

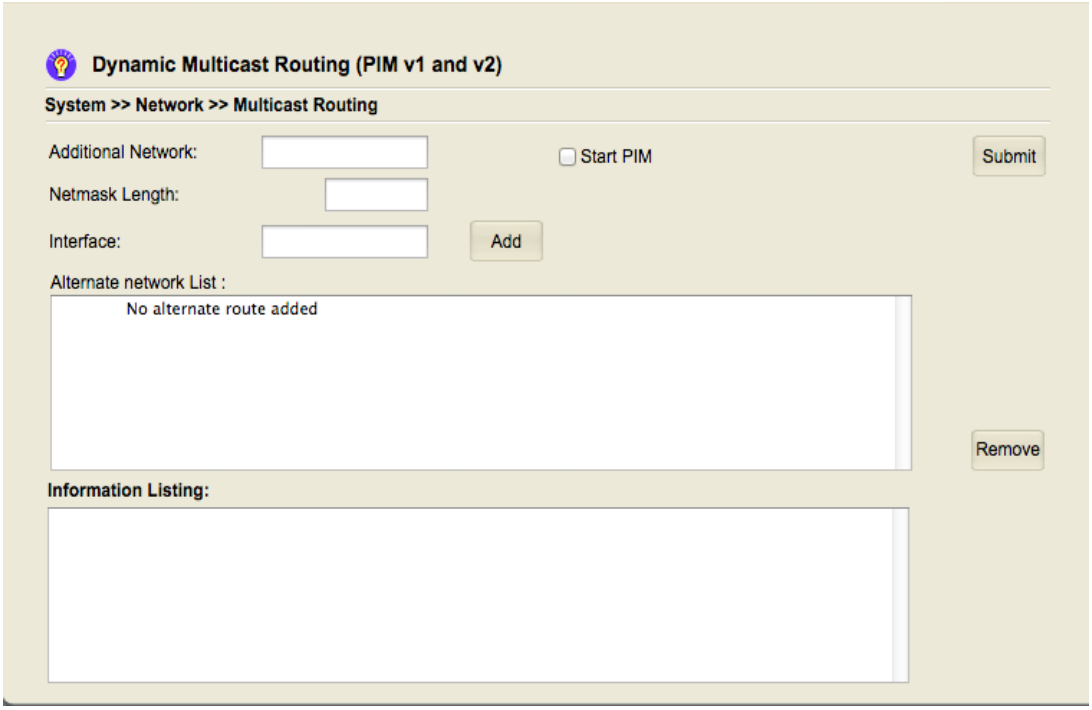



イラスト ***154:*** マルチキャストルーティングの設定

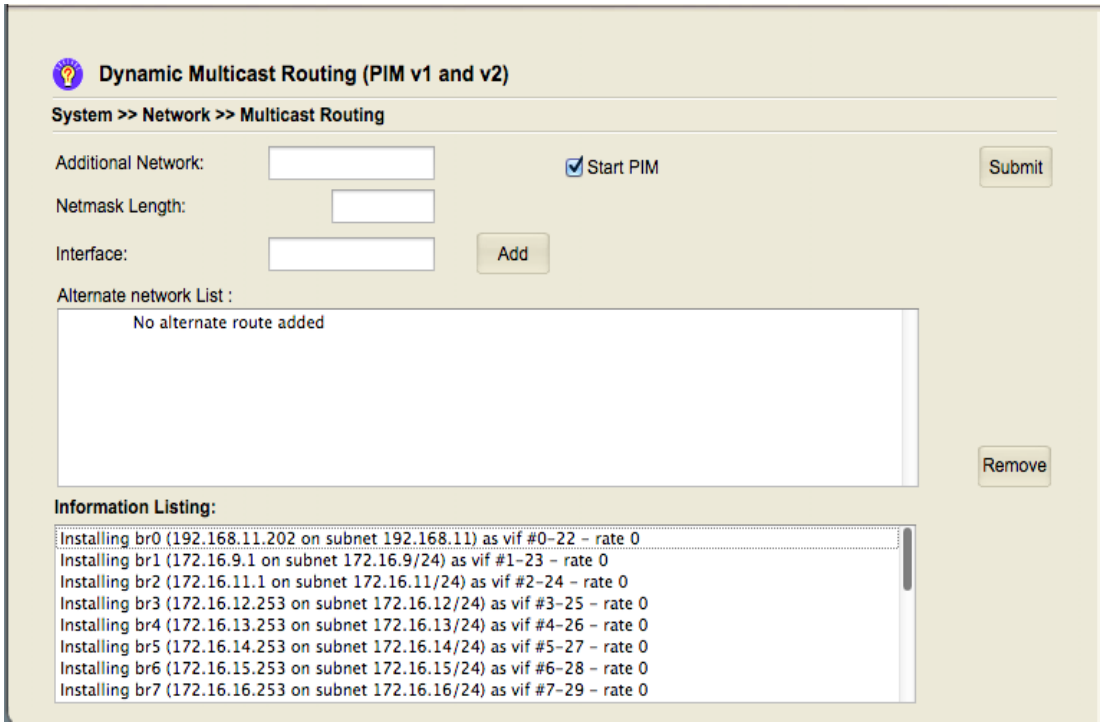
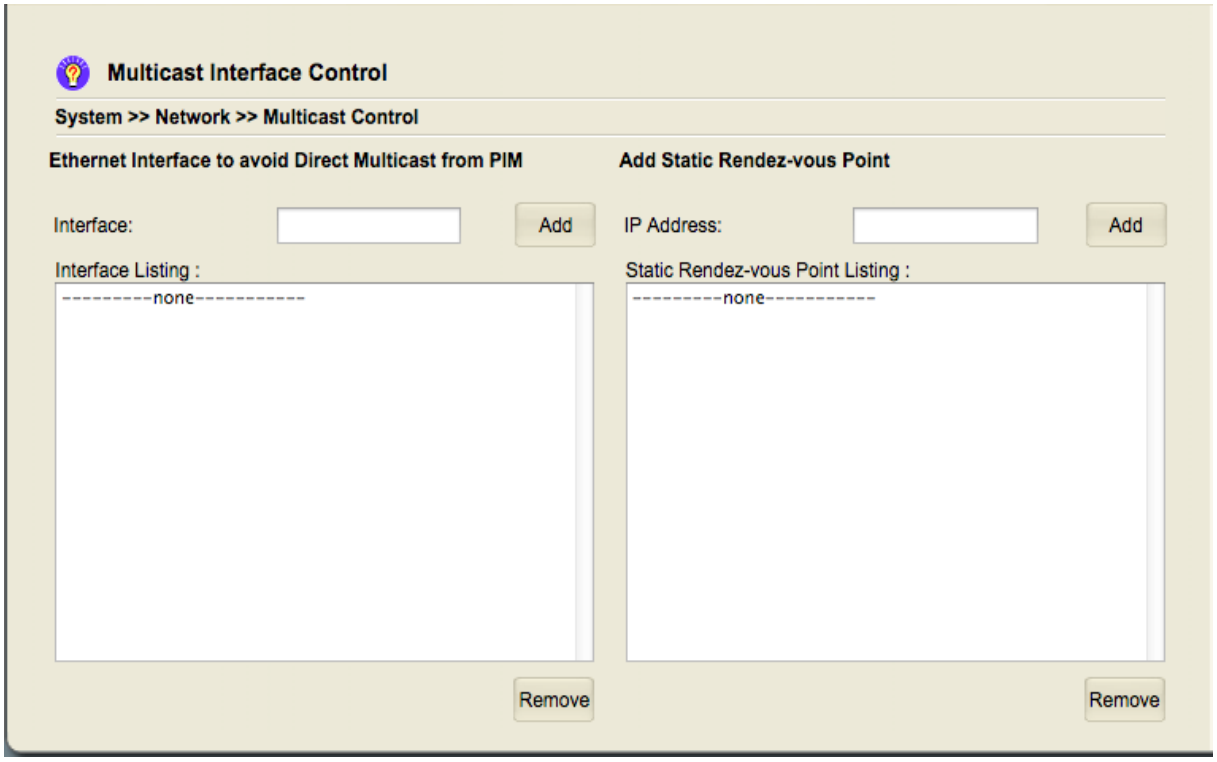



イラスト ***155: PIM*** がオンになった後

送信者がルーターに直接リンクされているサブネットに位置している場合にのみ、サブネットと関連するインターフェイスを指定する必要があります。 それ以外の場合は、他の設定は必要ありません。単に PIM をオンにするだけです。それは自動的にグループ固有の Rendez-vous ポイント (RP) を設定します。

IP マルチキャストは UDP に基づいているため、TCP のように到着確認を行う信頼性のある伝送ではありません。したがって、PIM が機能しているか確認するためには、マルチキャストパケットが予想されるサブネットに到達しない場合、UDP パケットがネットワークの混雑により失われるか確認する必要があります。

IP マルチキャストは、送信者がメッセージを一度だけ送信し、複数の受信者がメッセージを受信できるというメリットがあります。ただし、IP マルチキャストが遠くまで行き過ぎないようにするために、送信者によっては PIM が特定のネットワークインターフェースへのマルチキャストパケットの送信を停止するように依頼することができます。「System >> Network >> Multicast Control」で設定できます。

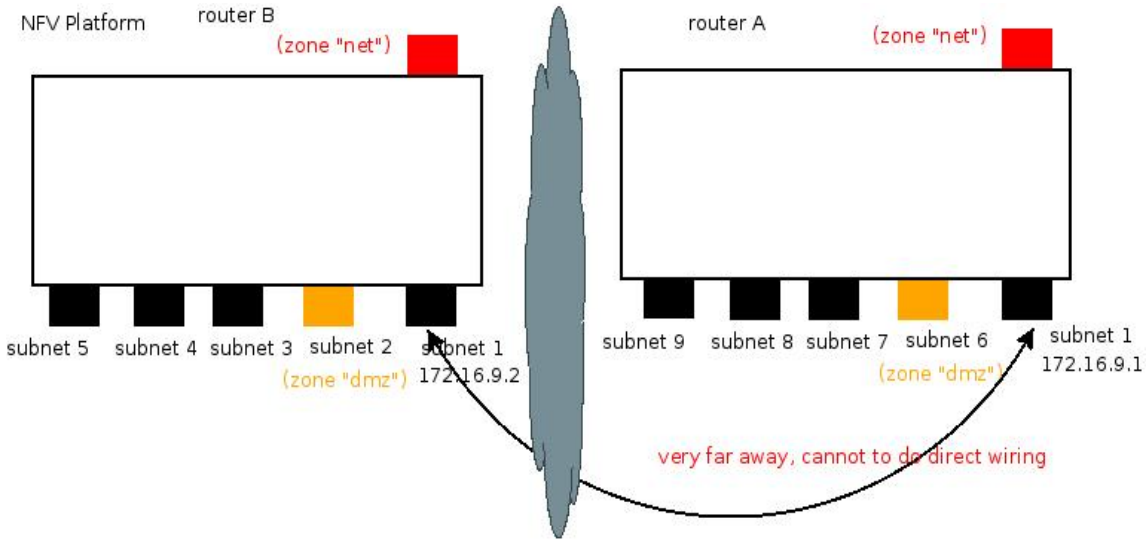



挿絵 ***156:*** マルチキャスト制御

特定のグループアドレスの Rendez-vous Point は、静的に設定することもできます。しかし、これはベースプラットフォームのみの場合には必要ありません。

## ***VPN*** 経由のルーティング

このセクションでは、VPN にわたるルーティングエントリの配置について検討します。可能な限り、RIPv2 または OSPF を使用して動的ルーティングを実行することを検討してください。 2 台のルーターがルーティングエントリを交換できるかどうか（動的にまたは静的に）、少なくとも両方のルーターが同じ IP サブネットにアクセスできる必要があります。この考えに基づいて、図を少し修正します。

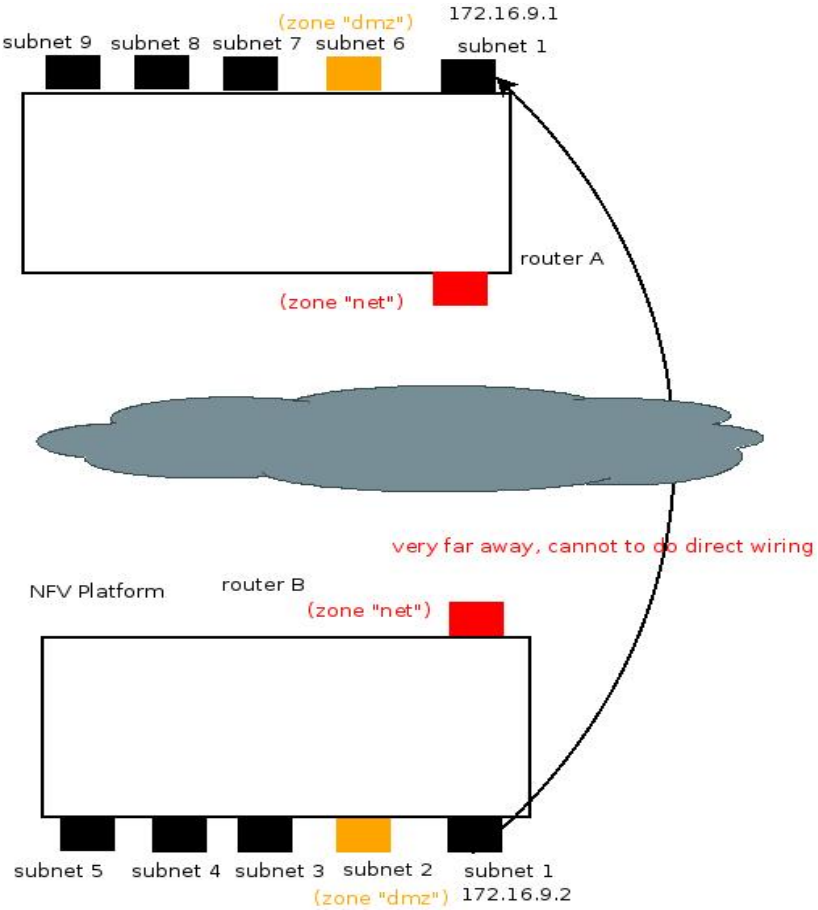



挿絵 ***157:*** インターネットを横断する ***2*** つのルーター

前の例では、両方のルーターの物理ポート間に直接配線（イーサネットケーブルまたはスイッチを使用）を確立できます。しかし、両方のルーターはインターネット上の異なるサイトに存在するため、両方のポート間で直接リンクを確立することはできません。したがって、OSPF または RIPv2 も不可能となります。

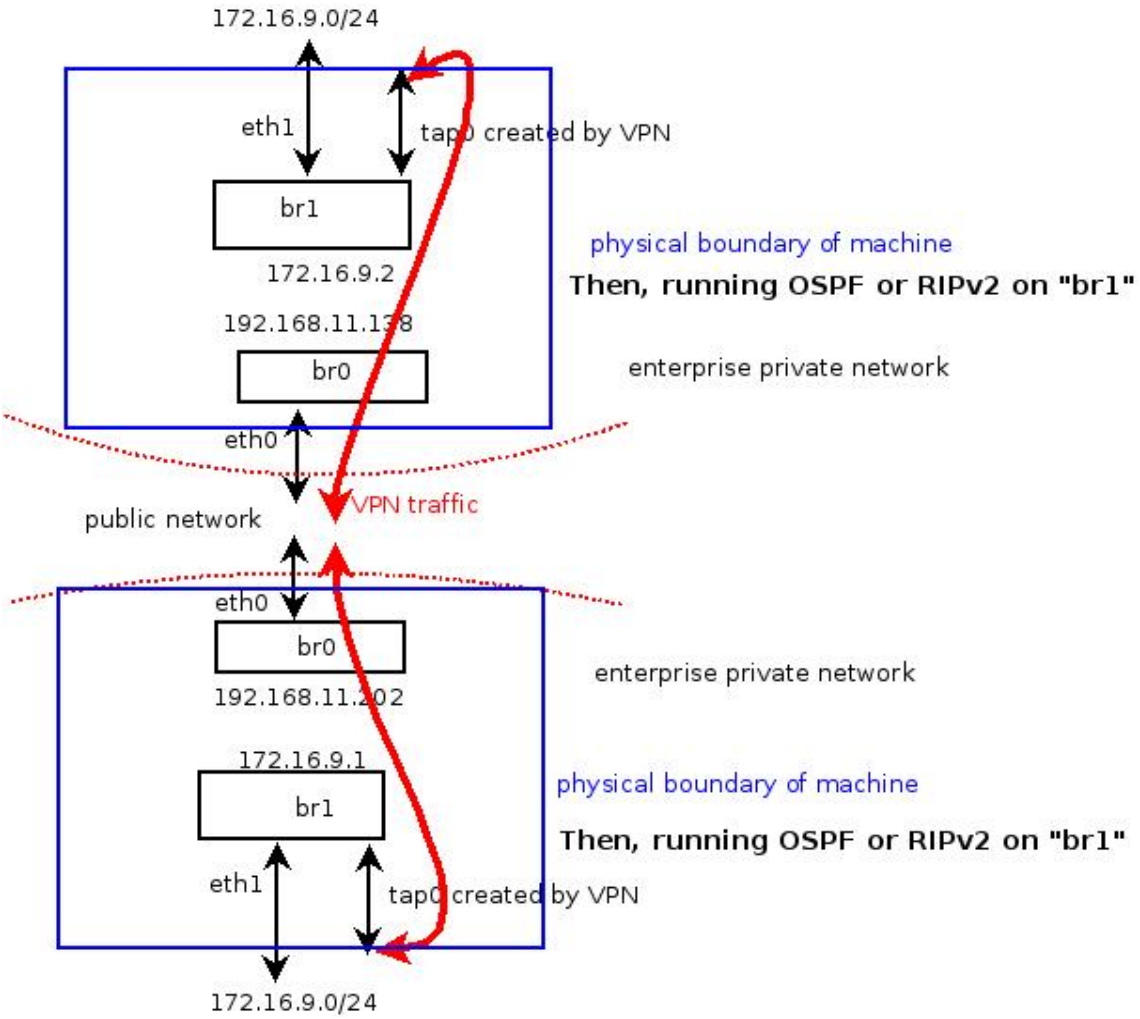
もし物理リンクが不可能であれば、ポートをブリッジして 2 つのポートを橋渡しすることで、仮想リンクを確立できますか。図を再度見直します。OSPF または RIPv2 を同じサブネット上で実行できます。

したがって、問題はサイト間 VPN をブリッジモードで確立することに帰着する。もちろん、VPN 接続は「net」ゾーンを通過して反対側へ到達しなければならない。



挿絵 ***158*** : 二つのプライベートルーターがインターネットを介して接続を試みる

サイト間 VPN をブリッジモードで設定する場合、上記と同様の図を使用します。ただし、この場合は OSPF または RIPv2 を使用して VPN 間でルーティング情報を交換します。




挿絵 ***159: VPN (***ブリッジングモード***)*** における ***OSPF*** または ***RIPv2***

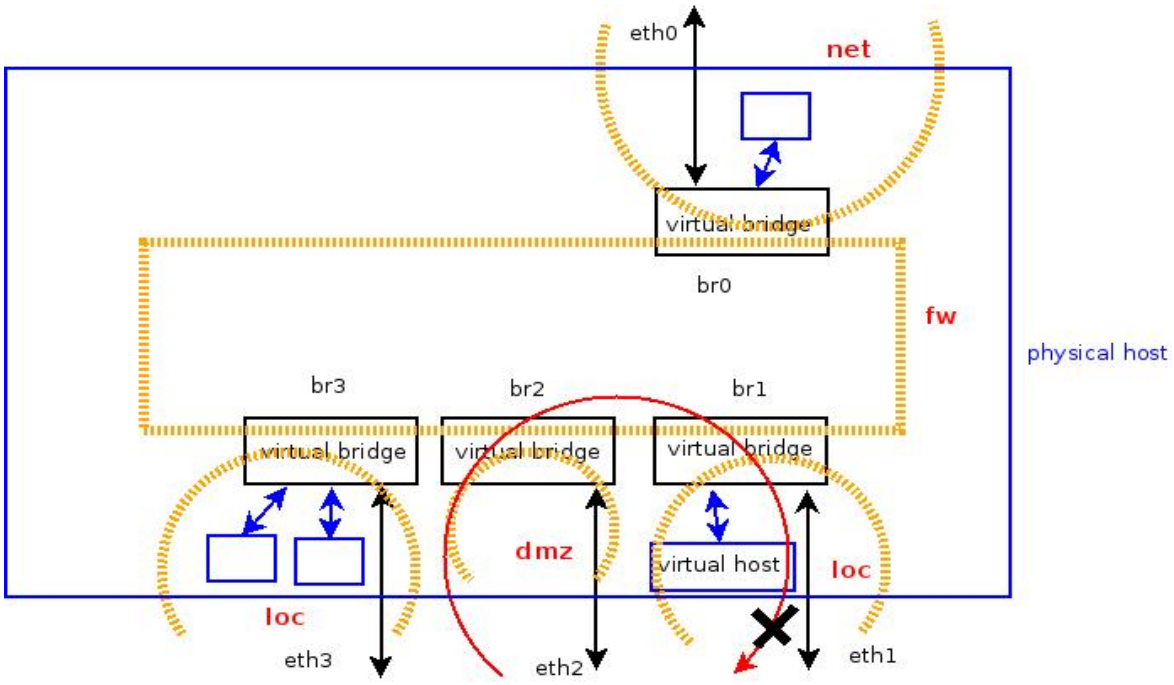
# 第 6 章 Deployment Scenarios

この章では、いくつかの例とその対応する要件を示し、これまでの章で紹介した関数をそれらを満たすために使用する方法を簡単に紹介します。

## 例 *1*：インターネットアクセスのある/ない機械を分離する

この例では、インターネットアクセスを持つ機械と持たない機械を異なるゾーンに配置したいと考えています。セキュリティ上の理由から、内部のビジネス運営のための機械はインターネット接続を許可されておらず、インターネットアクセスを持つ機械は、ビジネス運営のための機械へのネットワーク接続の開始を許可されていません。

「dmz」ゾーンのセクションを、境界制御の章で思い出してください。デフォルトでは、「dmz」ゾーンのホストが「loc」ゾーンの機械に接続を開始することは許可されていません。



挿絵 ***160: “dmz”*** ルール

したがって、インターネットアクセスを持つマシンを「dmz」ゾーンに配置できます。また、内部のビジネス運用を行うマシンを「loc」ゾーンに配置します。「loc」ゾーンはデフォルトで「net」ゾーンへのアクセスが許可されています。そのため、「Border >> Rule >> Add Rule」を通じて、「loc」ゾーンから「net」ゾーンへのアクセスをブロックするルールを追加する必要があります。

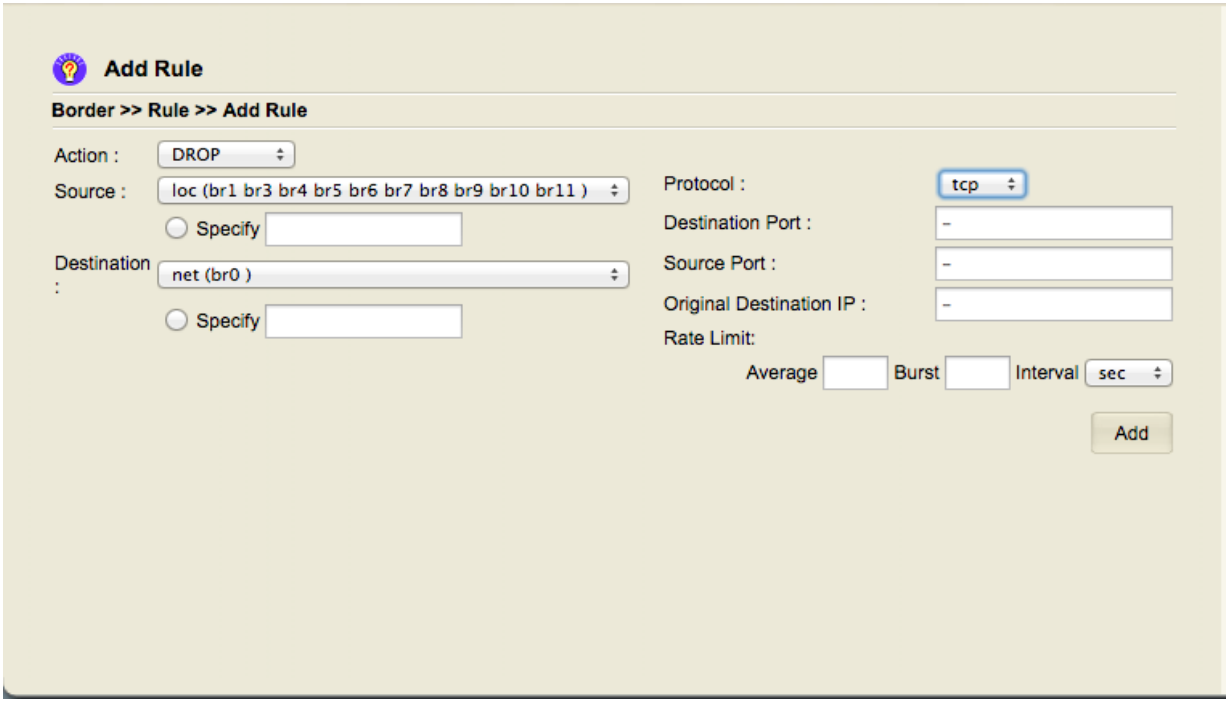
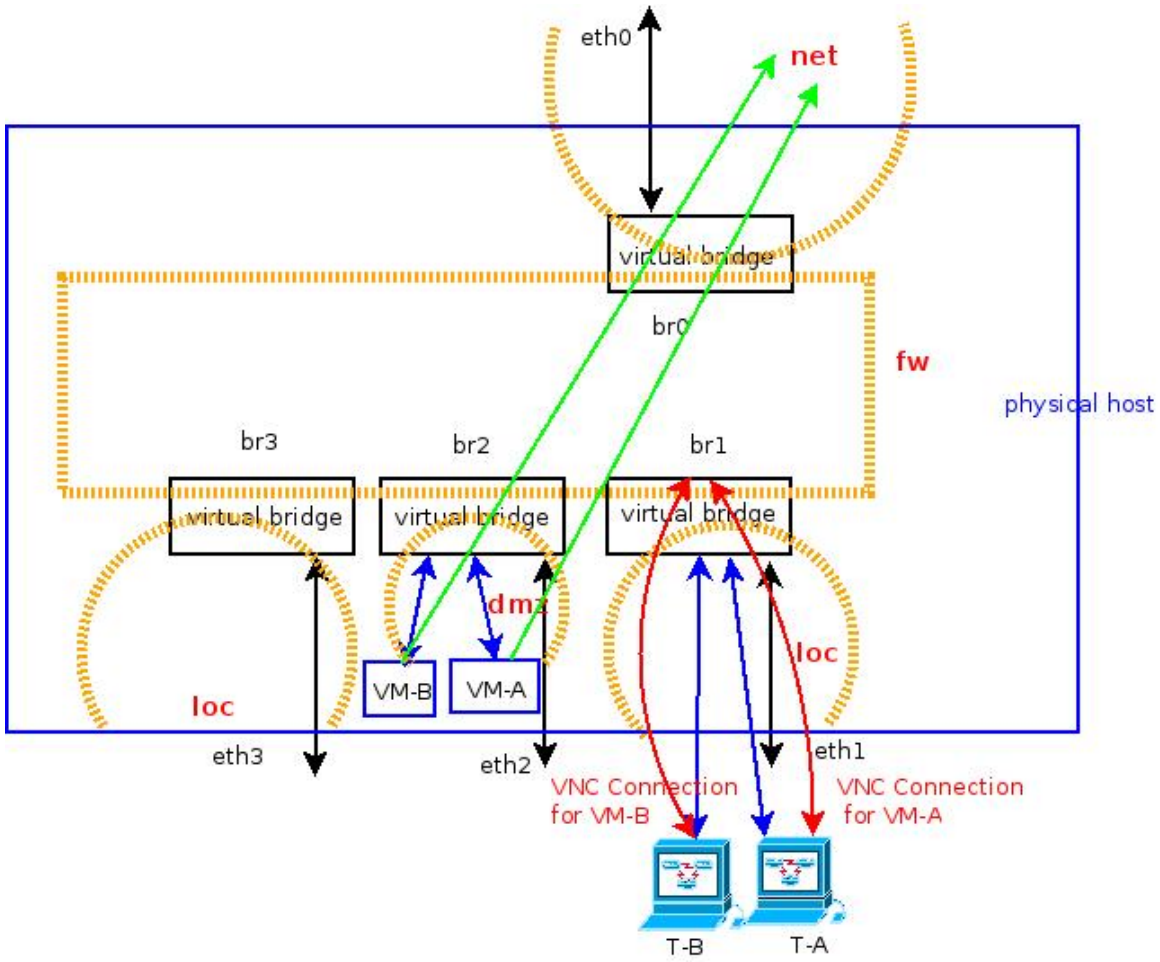



イラスト ***161: Zone "loc"*** からインターネットへのアクセスをブロックする

多くのオフィス環境では、インターネットサーバーを“dmz”ゾーンに配置し、適切なポートフォワーディング設定を行い、他のホストを“loc”ゾーンに配置し、インターネットアクセスを制限する構成に基づいて構築されます。

しかし、この設定はより多くのアプリケーションで利用されます。オフィスで各人が 2 台のデスクトップコンピューターを使用する場合を想定してください。1 台は社内業務用のもの

で、もう 1 台はインターネットアクセス用のものです。インターネットを直接アクセスできる社内業務用コンピューターは禁止されます。この要件を満たすために、DMZ ゾーン内の仮想マシンとしてインターネットアクセス用のコンピューターが存在するようにします。個人は、仮想マシン内のブラウザを使用して、VNC クライアント、SPICE クライアント、または（仮想マシンの OS が Microsoft Windows の場合）Microsoft Remote Terminal を使用して、社内業務用のコンピューターからこれらの仮想マシンにアクセスし、仮想マシン内のブラウザを使用してインターネットにアクセスします。これにより、社内業務用のコンピューターが侵害されるリスクを軽減できます。

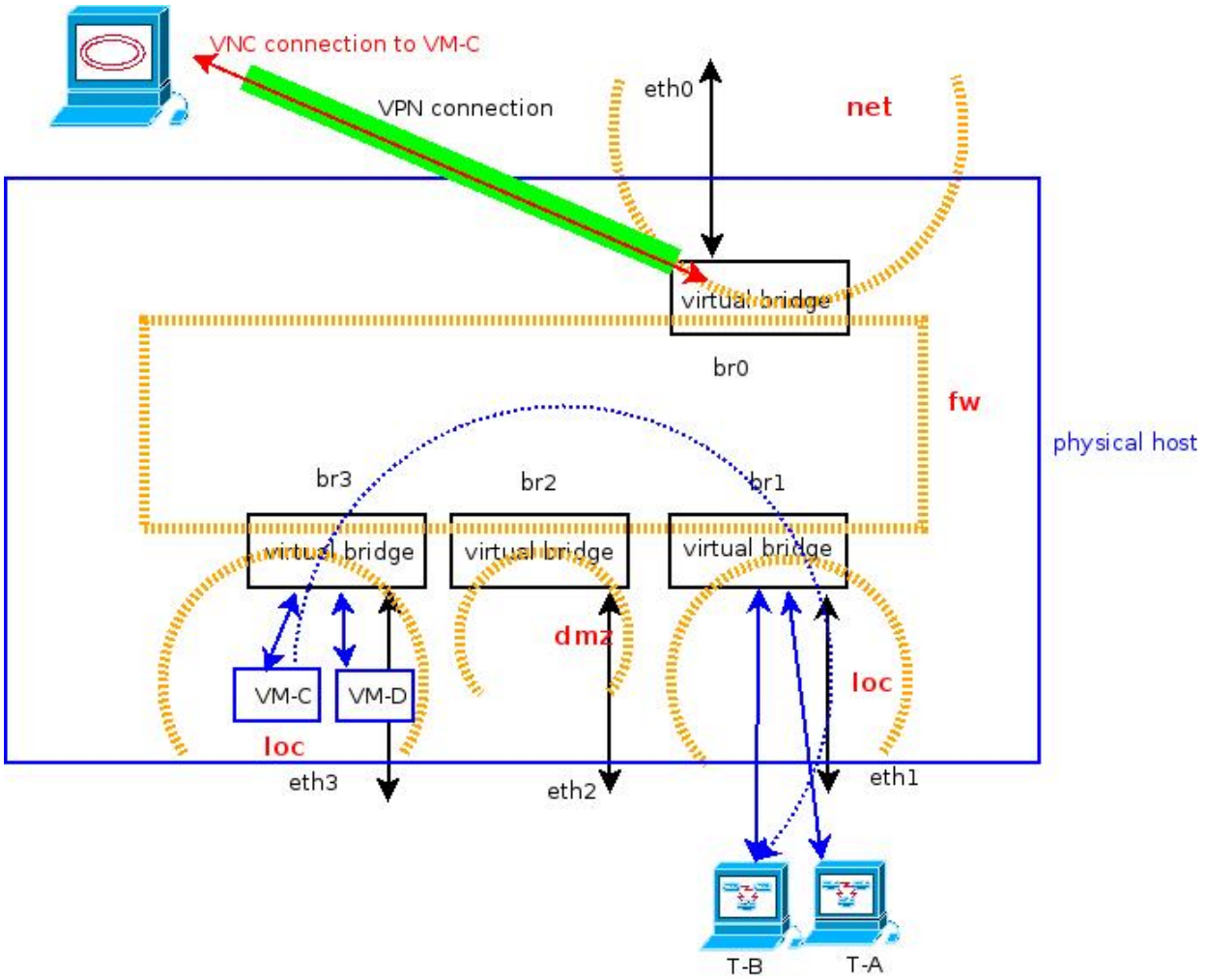



挿絵 ***162:*** 仮想マシンを使用したインターネットアクセスについて

注意していただきたいのは、VNC クライアントから、ベースプラットフォームの IP アドレス（例えば、「br0」の IP アドレス）と TCP ポートに接続することです。上記の図で示すように、マシン T-A には VM-A のコンソールが画面に表示され、その VM-A のコンソールから、VM-A にインストールされたプログラムからインターネットにアクセスできます。

## *Example 2: Use VPN to Access Virtual Desktop*

ベースプラットフォーム内の仮想マシンへの VNC クライアント（または SPICE クライアント）の使用にあたり、VNC クライアントはベースプラットフォームの IP アドレス（IP アドレス）に接続する必要があります。仮想ホストの IP アドレスではなく、ベースプラットフォームの IP アドレスに接続してください。VPN を介して VNC を使用する場合は、VPN の使用に指定されたベースプラットフォームの最初の IP アドレス（デフォルトで 172.16.38.1）を使用してください。VNC で仮想マシンのコンソールが戻ってきたら、その仮想マシンを使用して、オフィス内の他の機械にネットワークポリシーに従ってアクセスできます。

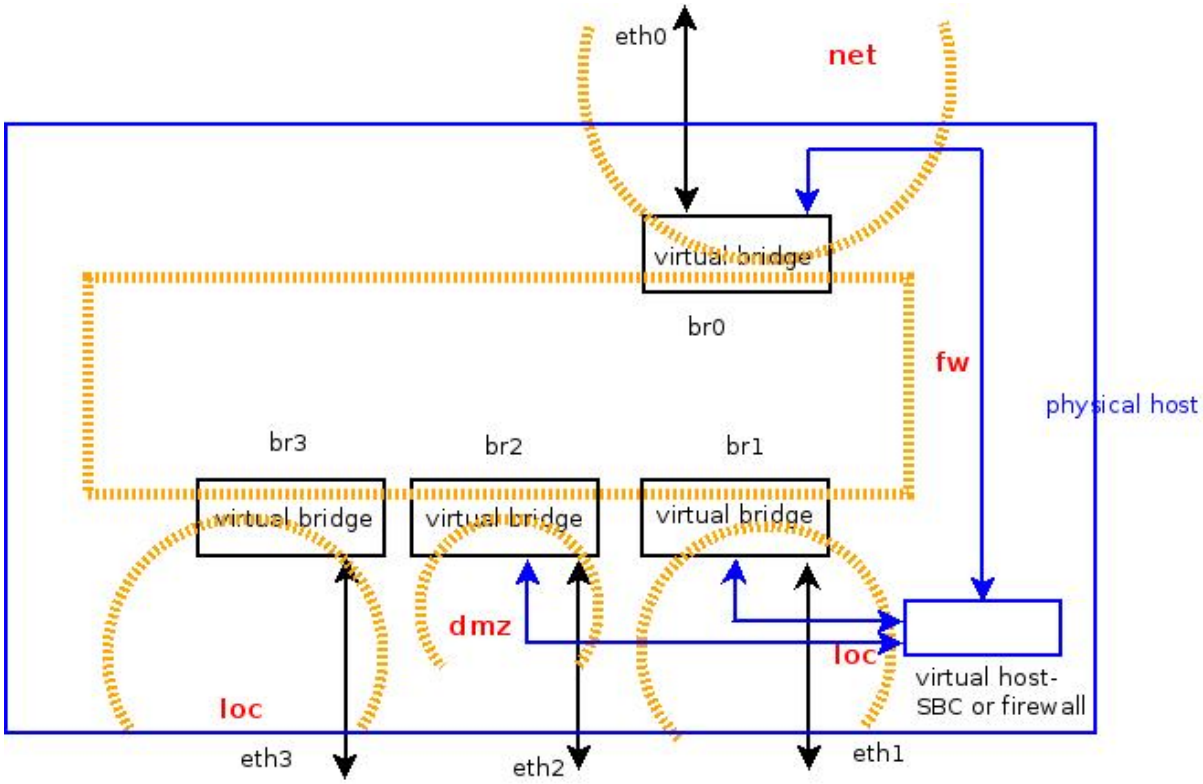



挿絵 ***163: VPN*** を介した仮想マシンのアクセス

上記図の VM-C のコンソールは、オフィス外から VPN 経由で VNC でアクセス可能です。VM-C のコンソールを手に入れたことで、オフィス内の他のマシンへのアクセスが容易になります。この方法では、他のサブネットへの VPN クライアントの直接アクセスを許可する必要はなく、仮想ホスト VM-C 上で別の認証方式を適用できます。

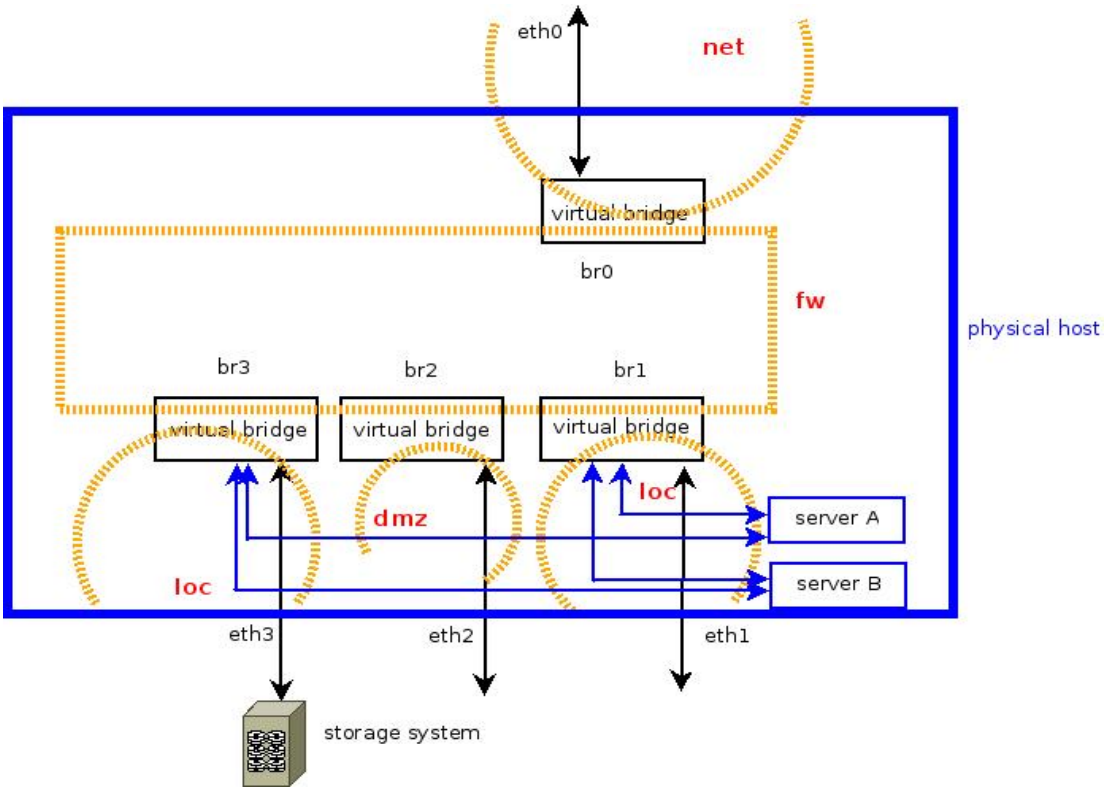
## 例 ***3: SBC*** またはファイアウォール仮想化

SBC およびファイアウォールは少なくとも 2 つのネットワークインターフェースで認識されています。 1 つはインターネットに接続し、もう 1 つはプライベートネットワークに接続します。 そのため、SBC またはファイアウォール用の仮想を作成するには、この仮想マシンのネットワークインターフェースを “br0”（WAN 接続用）と “br1”（LAN 接続用）に提供してください。 SBC またはファイアウォールを使用する場合は、この仮想ホストの LAN IP アドレスをゲートウェイとして使用してトラフィックをリダイレクトします。




挿絵 ***164: SBC*** または ファイアウォール の仮想化

## *Example 4: Place Storage System in Another Subnet*

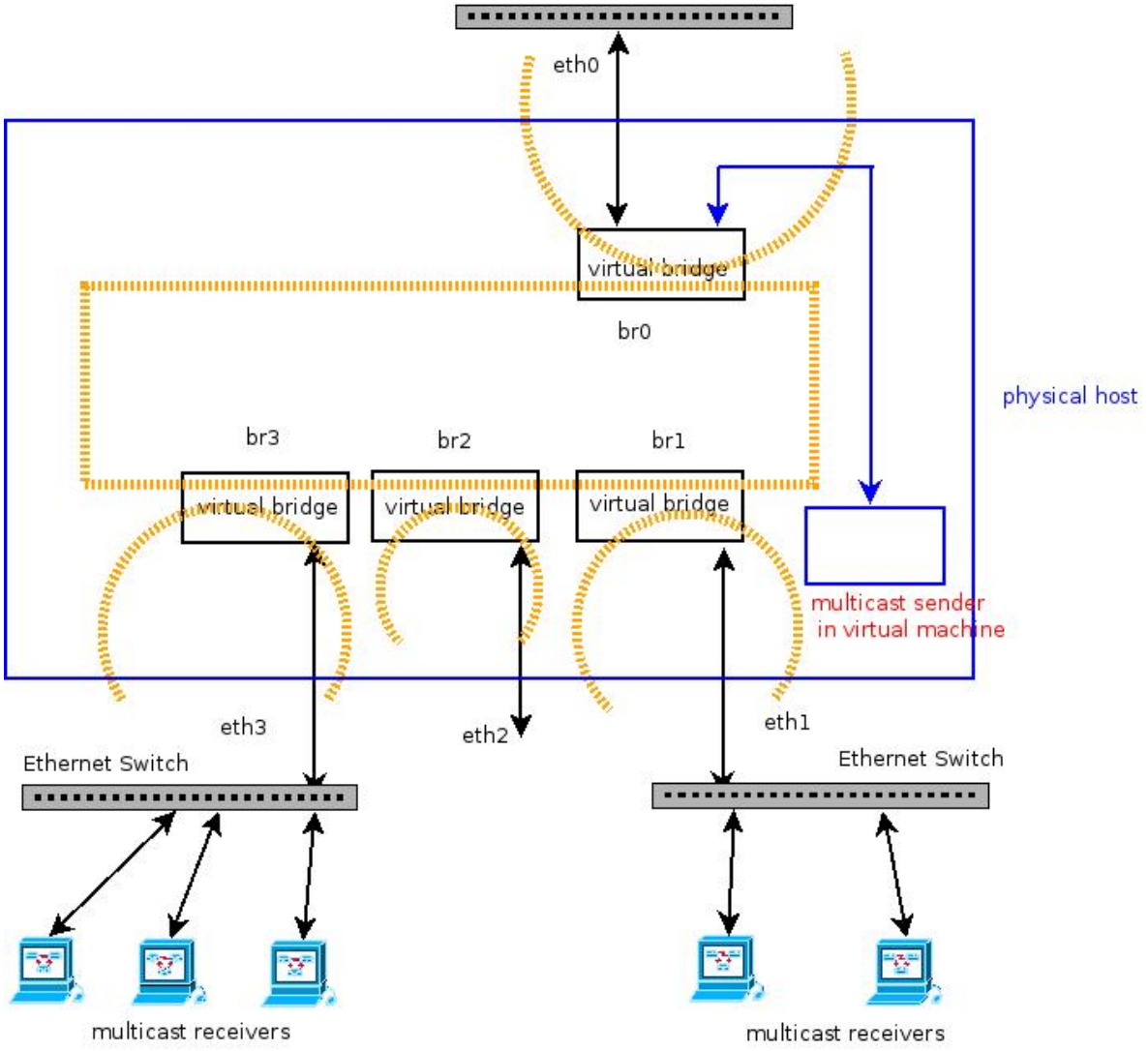



挿絵 ***165:*** 専用ス　ネットをストレージエリアネットワークとして使用する

ベースシステムが仮想マシンに必要な十分なストレージスペースを提供できない可能性があります。上記の図は、この種のアプリケーションの参照として使用できます。「server A」および「server B」は、「br1」に接続するサブネット上のサーバーとして使用されますが、「br3」を使用して外部ストレージシステムに iSCSI で接続するために、追加のネットワークインターフェースを持ちます。つまり、「br3」が存在するサブネットは、ストレージエリアネットワークとして使用されます。

## 例 ***5:*** マルチキャストルータにおけるマルチキャスト送信元

以下の図は、ベースシステムをマルチキャストルーターとして使用する例であり、マルチキャスト送信元は仮想マシン内に存在します。「Border Control」（ファイアウォール機能）がオフになっているのは、ラベル「net」、「dmz」、および「loc」が存在しないようにするためです。「Border Control」をオンにすると、以前に言及したルールに従って「net」と「dmz」が管理されるため、これらのゾーンではマルチキャストルーティングは機能しません。ベースプラットフォームでマルチキャストルーティングを機能させるには、PIM をオンにするだけです。




挿絵 ***166:*** マルチキャスト ルーターとマルチキャスト 送信装置

上記図において、マルチキャスト送信元が “br0” に接続されている仮想マシンにインストールされています。

ベースプラットフォームに関しては、PIM のみをオンにするだけで済みます。残りの作業は、マルチキャスト送信者と受信者に依存します。「TTL」（時間制限）設定は、マルチキャストパケット内で少なくとも 1 より大きくする必要があります。マルチキャストパケットがルーターを通過するたびに、TTL の値は 1 ずつ減少します。TTL の値が 0 以下になると、ルーターはパケットを転送しなくなります。

一部の人は、オープンソースパッケージ“VLC”を使用してマルチキャスト送信と受信をテストするかもしれません。執筆時点では、VLC のデフォルト設定の TTL は“-1”であり、その結果、そのマルチキャストパケットはデフォルトでは自分のサブネットを通過しません。VLC をマルチキャスト送信者として使用する場合は、この設定を変更する必要があります。そうしないと、送信者と受信者は同じサブネットにのみ存在できます。

このドキュメントは VLC のチュートリアルではありません。VLC が私たちが期待する形で機能するためのヒントを提供します。次のスクリーンショットは、VLC で TTL 値を変更する場所についてです。

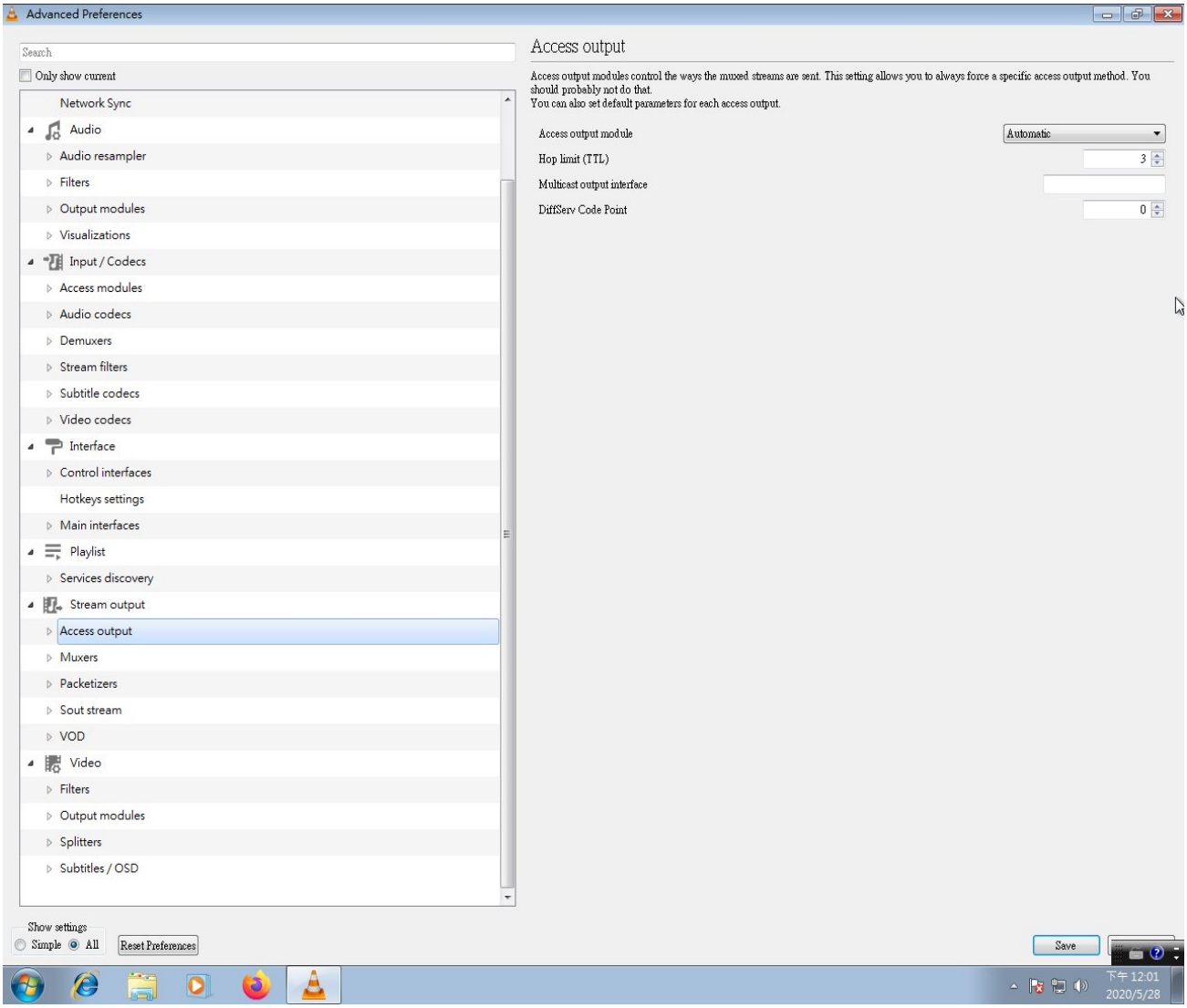



イラスト ***167: VLC*** のマルチキャスト送信者における ***TTL*** 設定の例