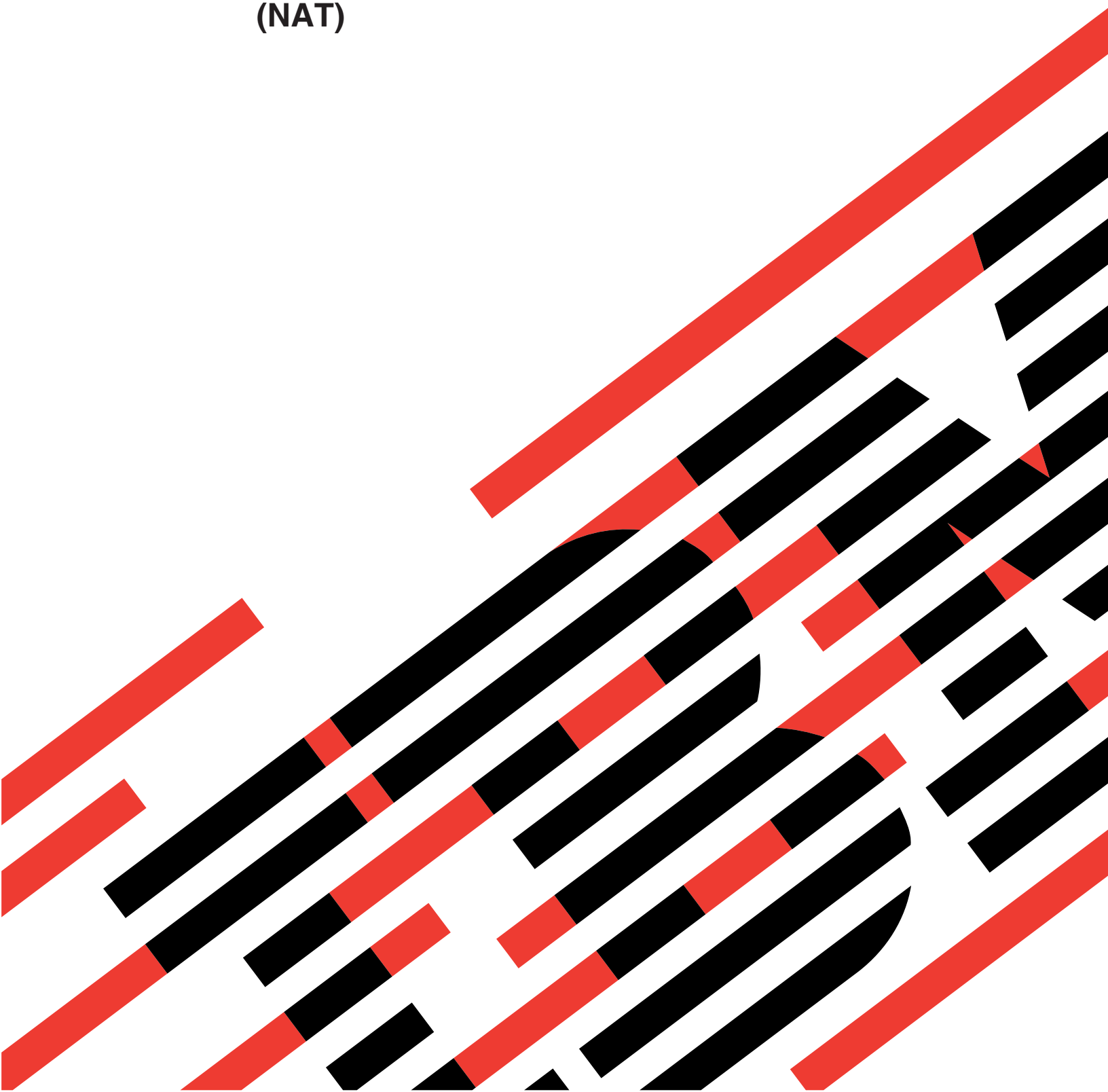
IBM

eserver

iSeries

ネットワーキング・セキュリティー
IP フィルター操作とネットワーク・アドレス変換 (NAT)



IBM

@server

iSeries

ネットワーキング・セキュリティー
IP フィルター操作とネットワーク・アドレス変換 (NAT)

目次

第 1 部 IP フィルター操作とネットワーク・アドレス変換 1

| **第 1 章 V5R2 の新機能** 3

第 2 章 トピックの印刷 5

第 3 章 パケット・ルールの実例 7
パケット・ルールの実例: IP アドレスのマップ (静的 NAT) 7
パケット・ルールの実例: HTTP、Telnet、および FTP を許可するフィルター・ルールの作成 9
パケット・ルールの実例: NAT と IP フィルターの組み合わせ 11
パケット・ルールの実例: 隠蔽 IP アドレス (マスカレード NAT) 16

第 4 章 パケット・ルールの概念 19
パケット・ルールの用語 19
パケット・ルールとその他の iSeries セキュリティー・ソリューション 20
ネットワーク・アドレス変換 (NAT) 21
静的 (マップ) NAT 21
マスカレード (隠蔽) NAT 22
マスカレード (ポート・マップ) NAT 23
IP フィルター 24
サンプル・フィルター・ステートメント 25
IP パケット・ヘッダー 26
IP フィルター・ルールを併用した NAT ルールの編成 26
複数の IP フィルター・ルールの編成 27
| スプーフ保護 27

第 5 章 パケット・ルールの計画 29
パケット・ルール: ユーザー権限要件 29
パケット・ルール: システム要件 30
パケット・ルール: 計画ワークシート 30

第 6 章 パケット・ルールの構成 31
パケット・ルールへのアクセス 32
アドレスおよびサービスの定義 32
NAT ルールの作成 33
IP フィルター・ルールの作成 33
IP フィルター・インターフェースの定義 35
パケット・ルールへのファイルの組み込み 35
パケット・ルールでのコメントの作成 36
パケット・ルールの検証 36
| パケット・ルールのアクティブ化 37

第 7 章 パケット・ルールの管理 39
パケット・ルールの非アクティブ化 39
パケット・ルールの表示 39
パケット・ルールの編集 40
パケット・ルールのバックアップ 40
パケット・ルールのアクションのジャーナルおよび監査 41

第 8 章 パケット・ルールのトラブルシューティング 43

| 第 9 章 パケット・ルールの関連情報 45

第 1 部 IP フィルター操作とネットワーク・アドレス変換

IP フィルターとネットワーク・アドレス変換 (NAT) は、侵入者から内部ネットワークを保護するファイアウォールとして機能します。IP フィルターを使用すると、ネットワークに入ったり、ネットワークから出たりすることを許可する IP トラフィックを制御できます。基本的に、IP フィルターは、定義されたルールに従ってパケットをフィルター操作することによりネットワークを保護します。一方 NAT は、登録済み IP アドレスのセットの背後に未登録の専用 IP アドレスを隠すことができます。これによって、内部ネットワークを外部ネットワークから守ることができます。また、NAT は、少ない登録済みアドレスでたくさんの専用アドレスを表すことができるため、IP アドレスが足りなくなるという問題を減らすこともできます。

注: **パケット・ルール**とは、IP フィルターと NAT の組み合わせたものです。このトピックでパケット・ルールという用語が使用されている場合は、これらの両方のコンポーネントに当てはまることを意味します。

下記のトピックを検討して、パケット・ルールとは何か、なぜ使用するのか、どのように使用するのかを理解してください。

V5R2 の新機能
V5R2 のパケット・ルールに関して行われた変更と改良について説明しています。

トピックの印刷
この情報をハードコピー版で欲しい場合に、この内容を読んで PDF を印刷してください。

パケット・ルールの実例
パケット・ルールの一般的な使用に関して理解していただくために、これらの実例を示します。それぞれの実例で、図とサンプル構成が示されています。

パケット・ルールの概念
まず最初に、パケット・ルールのテクノロジーと概念について最低限の基礎知識を身に付けておいてください。このトピックでは、IP フィルターと NAT に関する情報が提供されています。ここではマッピングやアドレスの隠蔽などのトピックも含まれてます。また、iSeries™ 固有の用語に関するリストも含まれています。

パケット・ルールの計画
計画は、どのリソースを何に対して保護する必要があるかを決定する上で、非常に重要です。このトピックでは計画ワークシートとその他の情報を提供します。それらを使用して、情報を得た上で特定のセキュリティー要件に最適な手段を決定することができます。

パケット・ルールの構成
このトピックでは、パケット・ルールで何ができるか、またそれを行なう手段についての情報を提供します。

パケット・ルールの管理
このトピックでは、パケット・ルールを管理するために実行するさまざまなタスクについて説明します。ルール・ファイルのジャーナル記録、編集、および表示などの機能があります。

パケット・ルールのトラブルシューティング
このトピックは、エラーが発生して、考えられる問題領域を確認する際に参照してください。

パケット・ルールの関連情報
このトピックには、パケット・ルール情報および関連トピックの他の情報源へのリンクを記載しています。

このトピックに含まれる情報の他に、iSeries ナビゲーターのパケット・ルール・エディターから入手できるオンライン・ヘルプも使用してください。 iSeries ナビゲーターのオンライン・ヘルプでは、パケット・ルールを最大限に活用するためのヒントおよび手法を記載しています。これには、「**How do I... (方法)**」ヘルプ、「**Tell me about... (説明)**」ヘルプ、および広範囲なコンテキスト・ヘルプなどがあります。

第 1 章 V5R2 の新機能

V5R2 のパケット・ルール機能は、以下の点で強化されました。

- **パケット・ルール・エディター**
  新しいパケット・ルール・エディターは、ウィザードおよびプロパティー・ページを使用してパケット・ルールの作成および変更ができる、使いやすい機能です。
- **新規ウィザード**
  構成するルールのタイプによって異なる 3 つの新規ウィザードがあり、必要なフィルターおよび NAT ステートメントを作成します。3 つの新規ウィザードとは、以下のとおりです。
  - 「**サービスの許可 (Permit A Service)**」ウィザード
  - 「**アドレス変換 (Address Translation)**」ウィザード
  - 「**スプーフ保護 (Spoof Protection)**」ウィザード
- **パケット・ルールの新しい表示方法**
  iSeries ナビゲーターの新しい表示方法では、インターフェースを選択して、それに関連したアクティブなパケット・ルール (フィルター・ステートメントも含めて) を表示することができます。
- **パケット・ルール・ファイルの作成のサポート**
  ファイル内で検出される XML データ型に基づいて、パケット・ルール・ファイルを作成することをサポートします。

  `/QIBM/XML/DTD/QtofPacketRules.dtd`
- **パケット・ルール・ファイルのサンプル**
  このファイルは、従来の .i3p フォーマットでも、.xml ファイルでも表示することができます。サンプル・ファイルを使用して、iSeries でパケット・ルールを作成するための正しい構文を学んだり、ファイル内でさまざまなステートメントがどのように機能するかを参照することができます。

このリリースでの新機能または変更点についてこの他の情報を知りたい場合は、「プログラム資料説明書」

 を参照してください。

第 2 章 トピックの印刷

PDF 版を表示またはダウンロードするには、「パケット・ルール」(約 683 KB または 54 ページ) を選択します。

表示用または印刷用の PDF をワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF を右マウス・ボタンでクリックする (上記のリンクを右マウス・ボタンでクリックする)。
2. 「**リンクを名前を付けて保存**」(Netscape Navigator) または「**対象をファイルに保存**」(Internet Explorer) をクリックする。
3. PDF を保存したいディレクトリーに進む。
4. 「**保存**」をクリックする。

Adobe Acrobat Reader のダウンロード

これらの PDF を表示または印刷するのに Adobe Acrobat Reader が必要な場合は、Adobe Web サイト (http://www.adobe.com/products/acrobat/readstep.html) からコピーをダウンロードできます。

第 3 章 パケット・ルールの実例

以下の実例を使用して、ネットワークを保護するために NAT と IP フィルターをどのように使用できるかを説明します。各実例には図およびサンプル構成が含まれています。

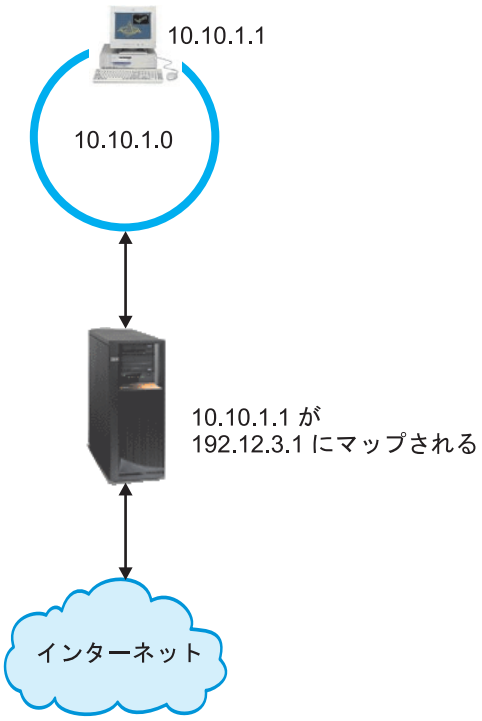
- **パケット・ルールの実例: IP アドレスのマップ (静的 NAT)**
  この実例では、ユーザーの会社が静的 NAT を使用して、専用 IP アドレスを公衆アドレスにマップします。
- **パケット・ルールの実例: HTTP、Telnet、および FTP を許可するフィルター・ルールの作成**
  この実例では、ユーザーの会社が IP フィルターを使用して、社内の Web サーバーにアクセスできる HTTP、Telnet、および FTP の IP トラフィックを制限します。
- **パケット・ルールの実例: NAT と IP フィルターの組み合わせ**
  この実例では、ユーザーの会社が NAT と IP フィルターの両方を使用して、社内の PC および Web サーバーを 1 つの公衆 IP アドレスの背後に隠しておいて、他の会社がユーザーの Web サーバーにアクセスできるようにします。
- **パケット・ルールの実例: IP アドレスの隠蔽 (マスカレード NAT)**
  この実例では、ユーザーの会社がマスカレード NAT を使用して、社内の PC の専用アドレスを隠しておいて、その上で従業員がインターネットにアクセスできるようにします。

注: 各実例の 192.x.x.x IP アドレスは、公衆 IP アドレスを表します。ここで使用されているアドレスは、すべて説明のためのものです。

パケット・ルールの実例: IP アドレスのマップ (静的 NAT)

状況

ユーザーが会社を所有しており、私設ネットワークの利用を決定したとします。しかし、公衆 IP アドレスを使用するための許可の登録も取得もしていません。これでは、インターネットにアクセスするには不十分です。会社のアドレス範囲は他者に登録されていることが判明しました。したがって、現在のセットアップを使用することはできません。まずは、公衆ユーザーが、ユーザーの Web サーバーにアクセスできるようにする必要があります。何をすべきでしょうか?



ソリューション

静的 NAT を使用することができます。静的 NAT は、1 つのオリジナル (専用) アドレスを 1 つの登録済み (公衆) アドレスに割り当てます。 iSeries は、この登録済みアドレスを専用アドレスにマップします。登録済みアドレスによって、ユーザーの専用アドレスはインターネットと通信できるようになります。本質的には、この公衆アドレスが 2 つのネットワークの橋渡しを行います。通信はどちらのネットワークからも開始できます。

静的 NAT を使用すると、現在の内部 IP アドレスすべてを保持しながらインターネットにもアクセスできます。インターネットにアクセスするには、専用アドレスごとに登録済みの IP アドレスが必要になります。たとえば、12 のユーザーがいる場合は、12 個の専用アドレスにマップする 12 個の公衆 IP アドレスが必要になります。

上記の図では、NAT アドレスの 192.12.3.1 はシェルのように使用不可のまま、戻ってくる情報を待ちます。情報が戻ってくると、NAT はアドレスを PC に戻してマップします。静的 NAT がアクティブな場合、アドレス 192.12.3.1 に直接送られるインバウンド・トラフィックは、内部アドレスを示すだけなので、そのインターフェースまでは達することはありません。 (iSeries の外部からは) 192.12.3.1 が要求された IP アドレスであるように見えますが、実専用アドレス 10.10.1.1 が実際の宛先となります。

構成

この実例で説明されているパケット・ルールを構成するには、 iSeries ナビゲーターの「**アドレス変換 (Address Translation)**」ウィザードを使用します。このウィザードでは、以下の情報が必要になります。

- マップする専用アドレス: 10.10.1.1
- その専用アドレスのマップ先となる公衆アドレス: 192.12.3.1
- アドレス・マッピングを行なう回線名: TRNLINE

「**アドレス変換 (Address Translation)**」ウィザードを使用するには、以下のステップに従います。

1. iSeries ナビゲーターで、「**ユーザーのサーバー (your server)**」-->「**ネットワーク (Network)**」-->「**IP ポリシー (IP policies)**」を選択する。
2. 「**パケット・ルール (Packet Rules)**」を右マウス・ボタンでクリックし、「**ルール・エディター (Rules Editor)**」を選択する。
3. 「**パケット・ルールの構成へようこそ (Welcome Packet Rules Configuration)**」ダイアログから「**新規パケット・ルール・ファイルの作成 (Create a new packet rules file)**」を選択し、「**OK**」をクリックする。
4. 「**ウィザード (Wizards)**」メニューから「**アドレス変換 (Address Translation)**」を選択し、ウィザードの指示に従ってマップ・アドレス変換パケット・ルールを構成する。

パケット・ルールは、以下のようになります。

```
-----------------------------------------------------
Statements to map 10.1.1.1 to 192.12.3.1 over TRNLINE
-----------------------------------------------------
ADDRESS MAPPRIVATE1   IP = 10.1.1.1
ADDRESS MAPPUBLIC1   IP = 192.12.3.1
MAP MAPPRIVATE1   TO MAPPUBLIC1   LINE = TRNLINE
-----------------------------------------------------
```

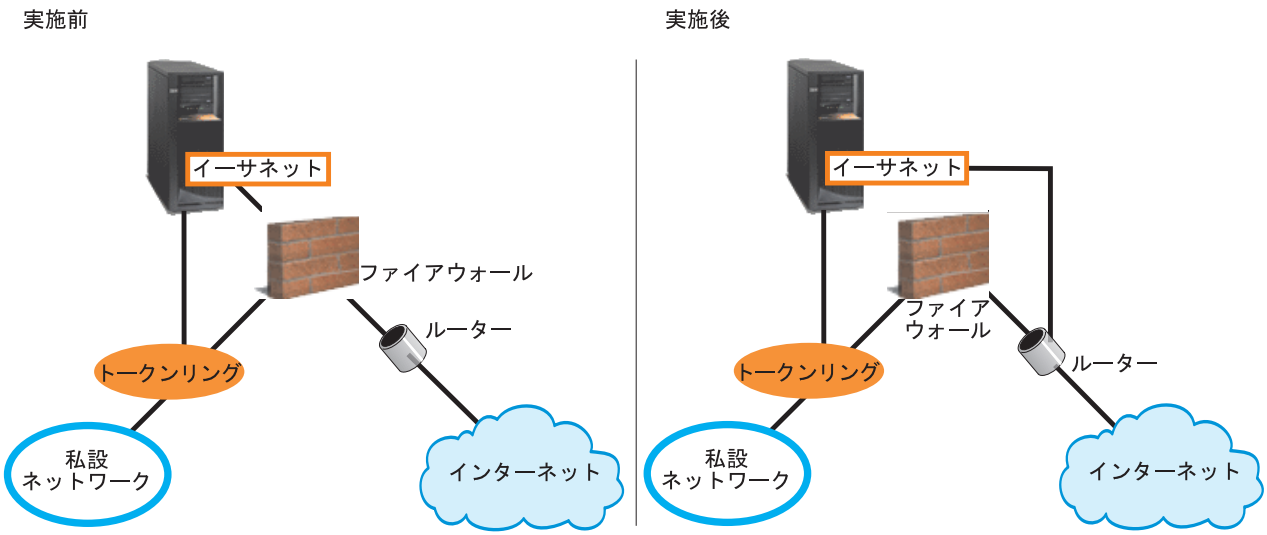
これらのルールおよびその他の必要なルールの作成を終えたら、これらのルールをアクティブにする際にエラーが発生しないことを検証してください。その後で、これらのルールをアクティブにすることができます。

注: 上記に定義されているトークンリング回線 (LINE=TRNLINE) は、192.12.3.1 が使用する回線でなければなりません。上記に定義されたトークンリングが 10.10.1.1 によって使用されている場合、この静的 NAT は機能しません。 NAT を使用する場合、常に IP 転送も使用可能にする必要があります。詳しくは、『パケット・ルールのトラブルシューティング』のセクションを参照してください。

パケット・ルールの実例: HTTP、Telnet、および FTP を許可するフィルター・ルールの作成

状況

ユーザーは、顧客に対して Web アプリケーションを提供したいのですが、現在のファイアウォールは過度に作動しているため、さらに負荷をかけたくないものとします。同僚がファイアウォール外でアプリケーションを実行することを提案しています。しかし、インターネットからは、HTTP、FTP、および Telnet のトラフィックのみが、iSeries Web サーバーにアクセスできるようにしたいとします。何をすべきでしょうか?



ソリューション

IP フィルターを使用すると、許可する情報を定義するためのルールを設定できます。この実例では、Web サーバーへの HTTP、FTP、および Telnet のトラフィック (インバウンドおよびアウトバウンド) を許可するフィルター・ルールを作成します。この場合の Web サーバーは iSeries です。サーバーの公衆アドレスは 192.54.5.1 で、専用 IP アドレスは 10.1.2.3 です。

構成

この実例で説明されているパケット・ルールを構成するには、iSeries ナビゲーターの「**サービスの許可 (Permit A Service)**」ウィザードを使用します。このウィザードでは、以下の情報が必要になります。

- 許可するサービスのタイプ: HTTP
- iSeries サーバーの公衆アドレス: 192.54.5.1
- クライアントのアドレス: 任意の IP アドレス
- サービスが稼働されるインターフェース: TRNLINE
- サービスが稼働される方向: INBOUND
- このフィルター・セットを識別するのに使用する名前: external_files

「**サービスの許可 (Permit A Service)**」ウィザードを使用するには、以下のステップに従います。

1. iSeries ナビゲーターで、「**ユーザーのサーバー (your server)**」-->「**ネットワーク (Network)**」-->「**IP ポリシー (IP policies)**」を選択する。
2. 「**パケット・ルール (Packet Rules)**」を右マウス・ボタンでクリックし、「**ルール・エディター (Rules Editor)**」を選択する。
3. 「**パケット・ルールの構成へようこそ (Welcome Packet Rules Configuration)**」ダイアログから「**新規パケット・ルール・ファイルの作成 (Create a new packet rules file)**」を選択し、「**OK**」をクリックする。
4. 「**ウィザード (Wizards)**」メニューから「**サービスの許可 (Permit A Service)**」を選択し、ウィザードの指示に従ってフィルター・ルールを作成する。

これらのパケット・ルールによって、システムに入って来る、およびシステムから出て行く、HTTP トラフィックが許可されます。パケット・ルールは、以下のようになります。

```
-----------------------------------------------
Statements to permit inbound HTTP over TRNLINE
-----------------------------------------------
INCLUDE   FILE = /QIBM/UserData/OS400/TCPIP/PacketRules/Services.i3p
FILTER SET external_files   ACTION = PERMIT   DIRECTION = OUTBOUND   SRCADDR = 192.54.5.1   DSTADDR = *
  SERVICE = HTTP_80_FS   JRN = OFF
FILTER SET external_files   ACTION = PERMIT   DIRECTION = INBOUND   SRCADDR = *   DSTADDR = 192.54.5.1
   SERVICE = HTTP_80_FC   JRN = OFF
FILTER SET external_files   ACTION = PERMIT   DIRECTION = OUTBOUND   SRCADDR = 192.54.5.1   DSTADDR = *
   SERVICE = HTTP_443_FS   JRN = OFF
FILTER SET external_files   ACTION = PERMIT   DIRECTION = INBOUND   SRCADDR = *   DSTADDR = 192.54.5.1
   SERVICE = HTTP_443_FC   JRN = OFF
FILTER_INTERFACE   LINE = TRNLINE   SET = external_files
-----------------------------------------------
```

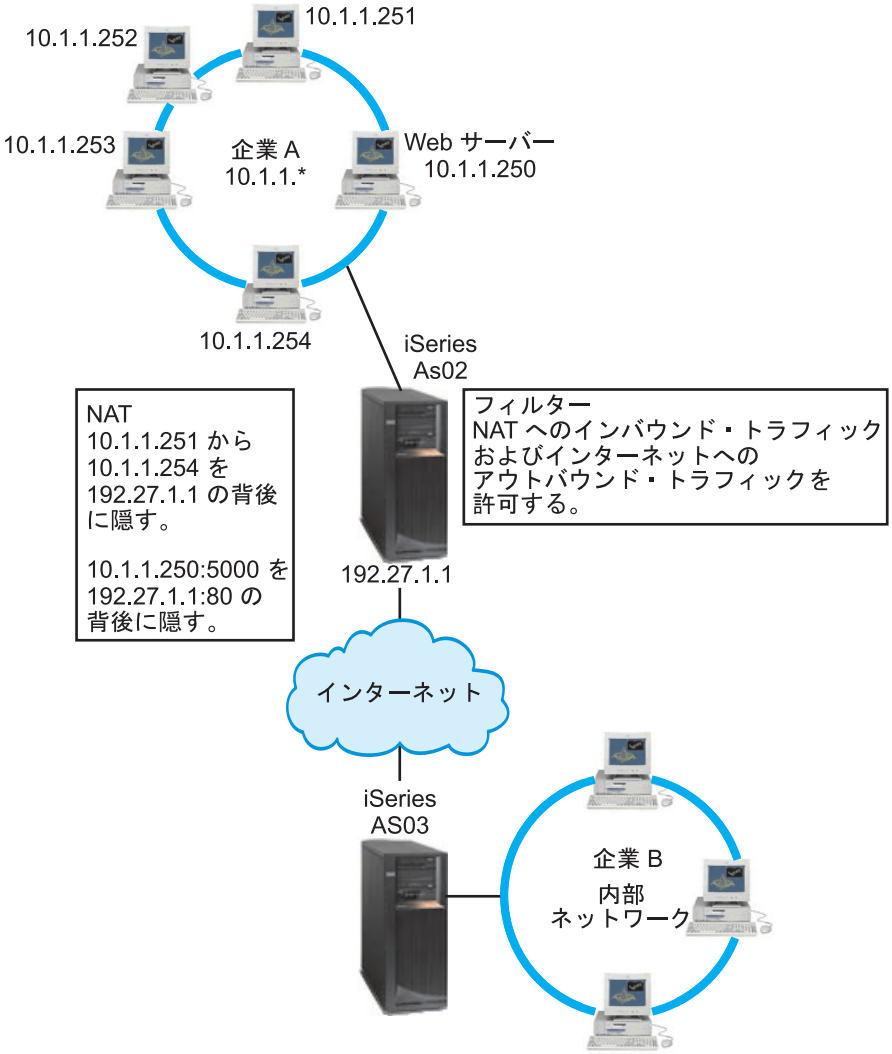
システムに入ってくる、およびシステムから出て行く、FTP トラフィックおよび Telnet トラフィックを許可するフィルター・ルールを作成するには、「**サービスの許可 (Permit a Service)**」ウィザードをさらに 2 回使用します。

これらのフィルター・ルールの作成を終えたら、これらのルールをアクティブにする際にエラーが発生しないことを検証してください。その後で、これらのルールをアクティブにすることができます。

パケット・ルールの実例: NAT と IP フィルターの組み合わせ

状況

社内に iSeries を使用した中規模サイズの内部ネットワークがあるとします。すべての Web トラフィックをゲートウェイ iSeries からそのゲートウェイの背後にある別のサーバーに転送する必要があるとします。Web サーバーはポート 5000 で稼働しています。ゲートウェイ iSeries インターフェース、つまり下記の図の AS02 背後に、すべての専用 PC と Web サーバーを隠したいとします。また、他の会社からこの Web サーバーへのアクセスを許可したいとも考えています。何をすべきでしょうか?



ソリューション

IP フィルターと NAT を両方一緒に使用して、以下のものを構成できます。

1. 隠蔽 NAT。社内の PC を公衆アドレス 192.27.1.1 の背後に隠し、インターネットにアクセスできるようにするもの。
2. ポート・マップ NAT。ユーザーの Web サーバー・アドレス 10.1.1.250 およびポート番号 5000 を、公衆アドレス 192.27.1.1 およびポート番号 80 の背後に隠すもの。両方の NAT ルールが 192.27.1.1 の背後に隠されることに注意してください。これは、隠しているアドレスが重複していない限り、問題ありません。このポート・マップ NAT ルールは、ポート 80 の外部から発信されたトラフィックに対して、ユーザーのシステムにアクセスすることだけを許可します。外部から発信されたトラフィックがこのアドレスやポート番号と完全に一致しない場合、NAT はこの通信を変換せず、パケットは廃棄されます。
3. NAT を通じてユーザーの私設ネットワークに送られるすべてのインバウンド・トラフィックと、インターネットへのアウトバウンド・トラフィックをフィルターに掛けるルール。

構成

この実例で説明されている隠蔽 NAT パケット・ルールを構成するには、 iSeries ナビゲーターの「**アドレス変換 (Address Translation)**」ウィザードを使用します。このウィザードでは、以下の情報が必要になります。

- 非公開にするアドレスのセット: 10.1.1.251 〜 10.1.1.254
- そのアドレス・セットを背後に非公開にするインターフェース・アドレス: 192.27.1.1

「**アドレス変換 (Address Translation)**」ウィザードを使用するには、以下のステップに従います。

1. iSeries ナビゲーターで、「**ユーザーのサーバー (your server)**」-->「**ネットワーク (Network)**」-->「**IP ポリシー (IP policies)**」を選択する。
2. 「**パケット・ルール (Packet Rules)**」を右マウス・ボタンでクリックし、「**ルール・エディター (Rules Editor)**」を選択する。
3. 「**パケット・ルールの構成へようこそ (Welcome Packet Rules Configuration)**」ダイアログから「**新規パケット・ルール・ファイルの作成 (Create a new packet rules file)**」を選択し、「**OK**」をクリックする。
4. 「**ウィザード (Wizards)**」メニューから「**アドレス変換 (Address Translation)**」を選択し、ウィザードの指示に従って隠蔽アドレス変換パケット・ルールを構成する。

このパケット・ルールは、4 台の PC を公衆アドレスの背後に隠し、インターネットにアクセスできるようにするものです。隠蔽 NAT パケット・ルールは、以下のようになります。

```
------------------------------------------------------------
Statements to hide 10.1.1.251 - 10.1.1.254 behind 192.27.1.1
------------------------------------------------------------
ADDRESS HIDE1   IP = 10.1.1.251 THROUGH 10.1.1.254
ADDRESS BEHIND1   IP = 192.27.1.1
HIDE HIDE1   BEHIND BEHIND1
------------------------------------------------------------
```

ポート・マップ NAT を構成するには、以下のステップに従います。

1. iSeries ナビゲーターからパケット・ルール・エディターにアクセスする。
2. Web サーバー・アドレスおよびポート 5000 の定義アドレスを作成する。
   a. 「**挿入**」メニューから「**アドレス**」を選択する。
   b. 「**一般**」ページの「**アドレス名 (Address name)**」フィールドで **Web250** を入力する。
   c. 「**定義アドレス (Defined address)**」ドロップダウン・リストで「**IP アドレス**」を選択する。「**追加**」をクリックして、編集フィールドに Web サーバー 10.1.1.250 の IP アドレスを入力します。
   d. 「**OK**」をクリックする。
3. 公衆アドレス 192.27.1.1 を表す定義アドレスを作成する。
   注: 隠蔽 NAT パケット・ルールを構成したときに公衆アドレス 192.27.1.1 を表す定義アドレスをすでに作成してあるので、この特定の実例ではこのステップとステップ 4 を省略することができます。しかし、これらの指示に従って自分のネットワーク用のポート・マップ NAT を構成する場合で、かつ隠蔽 NAT パケット・ルールを構成していない場合は、このステップの指示に従ってください。
   a. 「**挿入**」メニューから「**アドレス**」を選択する。
   b. 「**一般**」ページの「**アドレス名 (Address name)**」フィールドで「**BEHIND1**」を入力または選択する。

c. 「**定義アドレス (Defined address)**」ドロップダウン・リストで「**IP アドレス**」を選択する。「**追加**」をクリックして、「**IP アドレス**」編集フィールドに 192.27.1.1 と入力します。

d. 「**OK**」をクリックする。

4. ポート・マップ NAT ルールを作成する。

a. 「**挿入**」メニューから「**非公開**」を選択する。

b. 「**一般**」ページの「**非公開アドレス名 (Hide address name)**」ドロップダウン・リストから「Web250」を選択する。

c. 「**背後のアドレス名 (Behind address name)**」ドロップダウン・リストから「**BEHIND1**」を選択する。

d. 「**インバウンド接続の許可 (Allow inbound connections)**」を選択して、「**非公開ポート**」フィールドに 5000 を入力する。

e. 「**背後のポート**」フィールドに 80 と入力する。

f. 「**タイムアウト**」フィールドに 16 と入力して、「**秒**」を選択する。

g. 「**最大会話 (Maximum conversations)**」フィールドに 64 と入力する。

h. 「**ジャーナル処理 (Journaling)**」ドロップダウン・リストから「**オフ (OFF)**」を選択する。

i. 「**OK**」をクリックする。

このポート・マップ NAT は、Web サーバー・アドレスとポート番号を、公衆アドレスとポート番号の背後に隠します。両方の NAT ルールが 1 つの共通 IP アドレスの背後に隠されることに注意してください。これは、隠しているアドレスが重複していない限り、問題ありません。このポート・マップ NAT ルールは、ポート 80 で外部から発信されたトラフィックに対して、ユーザーのシステムにアクセスすることだけを許可します。

ポート・マップ NAT ルールは、以下のようになります。

```
ADDRESS Web250   IP = 10.1.1.250
ADDRESS BEHIND1   IP = 192.27.1.1
HIDE Web250:5000   BEHIND BEHIND1:80   TIMEOUT = 16   MAXCON = 64   JRN = OFF
```

この実例で説明されているフィルター・ルールを作成するには、以下のステップに従います。

1. iSeries ナビゲーターからパケット・ルール・エディターにアクセスする。
2. ユーザーの私設ネットワークに送られてくるインバウンド・トラフィックを許可するフィルター・ルールを作成する。

a. 「**パケット・ルールの構成へようこそ (Welcome Packet Rules Configuration)**」ダイアログから「**新規パケット・ルール・ファイルの作成 (Create a new packet rules file)**」を選択し、「**OK**」をクリックする。

b. 「**挿入**」メニューから「**フィルター (Filter...)**」を選択する。

c. 「**一般**」ページの「**セット名 (Set name)**」フィールドに「external_rules」を入力する。

d. 「**処置**」ドロップダウン・リストから「**PERMIT**」を選択する。

e. 「**方向 (Direction)**」ドロップダウン・リストから「**INBOUND**」を選択する。

f. 「**ソース・アドレス名 (Source address name)**」ドロップダウン・リストから「=」および「*」を選択する。

g. 「**宛先アドレス名 (Destination address name)**」フィールドで「=」を選択し、192.27.1.1 を入力する。

h. 「**ジャーナル処理 (Journaling)**」ドロップダウン・リストから「**オフ (OFF)**」を選択する。

i. 「**サービス**」ページで「**サービス (Service)**」を選択する。

j. 「**プロトコル**」ドロップダウン・リストから「**TCP**」を選択する。
k. 「**ソース・ポート (Source port)**」ドロップダウン・リストから「=」および「*」を選択する。
l. 「**宛先ポート (Destination port)**」ドロップダウン・リストから「=」および「*」を選択する。
m. 「**OK**」をクリックする。

3. ユーザーの私設ネットワークからインターネットに送るアウトバウンド・トラフィックを許可するフィルター・ルールを作成する。
   a. 「**パケット・ルールの構成へようこそ (Welcome Packet Rules Configuration)**」ダイアログから「**既存のパケット・ルール・ファイルのオープン (Open an existing packet rules file)**」を選択し、「**OK**」をクリックする。
   b. 「**ファイルのオープン (Open file)**」ダイアログから「**external_rules**」ファイルを選択し、「**開く (Open)**」をクリックする。
   c. 「**挿入**」メニューから「**フィルター (Filter...)**」を選択する。
   d. 「**一般**」ページの「**セット名 (Set name)**」ドロップダウン・リストから「external_rules」を選択する。
   e. 「**処置**」ドロップダウン・リストから「**PERMIT**」を選択する。
   f. 「**方向 (Direction)**」ドロップダウン・リストから「**OUTBOUND**」を選択する。
   g. 「**ソース・アドレス名 (Source address name)**」フィールドで「=」を選択し、192.27.1.1 を入力する。
   h. 「**宛先アドレス名 (Destination address name)**」ドロップダウン・リストから「=」および「*」を選択する。
   i. 「**ジャーナル処理 (Journaling)**」ドロップダウン・リストから「**オフ (OFF)**」を選択する。
   j. 「**サービス**」ページで「**サービス (Service)**」を選択する。
   k. 「**プロトコル**」ドロップダウン・リストから「**TCP**」を選択する。
   l. 「**ソース・ポート (Source port)**」ドロップダウン・リストから「=」および「*」を選択する。
   m. 「**宛先ポート (Destination port)**」ドロップダウン・リストから「=」および「*」を選択する。
   n. 「**OK**」をクリックする。
4. 作成したフィルター・セット用のフィルター・インターフェースを定義する。
   a. 「**挿入**」メニューから「**フィルター・インターフェース (Filter interface...)**」を選択する。
   b. 「**回線名 (Line name)**」を選択し、「**回線名 (Line name)**」ドロップダウン・リストから「**TRNLINE**」を選択する。
   c. 「**フィルター・セット (Filter sets)**」ページの「**フィルター・セット (Filter set)**」ドロップダウン・リストから「**external_rules**」を選択する。それから、「**追加 (Add)**」をクリックします。
   d. 「**OK**」をクリックする。

これらのフィルターを HIDE ステートメントと組み合わせて使用することにより、NAT を通じて私設ネットワークに送られるインバウンド・トラフィックと、インターネットへのアウトバウンド・トラフィックが許可されます。しかし、この NAT は、ポート 80 で外部から発信されたトラフィックに対して、サーバーにアクセスすることだけを許可します。NAT は、ポート・マップ NAT ルールに一致しない、外部から発信されたトラフィックは変換しません。フィルター・ルールは、以下のようになります。

```
FILTER SET external_files   ACTION = PERMIT   DIRECTION = INBOUND   SRCADDR = *   DSTADDR = 192.27.1.1
   PROTOCOL = TCP   DSTPORT = *   SRCPORT = *   JRN = OFF
FILTER SET external_files   ACTION = PERMIT   DIRECTION = OUTBOUND   SRCADDR = 192.27.1.1   DSTADDR = *
   PROTOCOL = TCP   DSTPORT = *   SRCPORT = *   JRN = OFF
```

以下のステートメントは、正しい物理インターフェースに設定された「external_rules」フィルターをバインド (関連化) するものです。

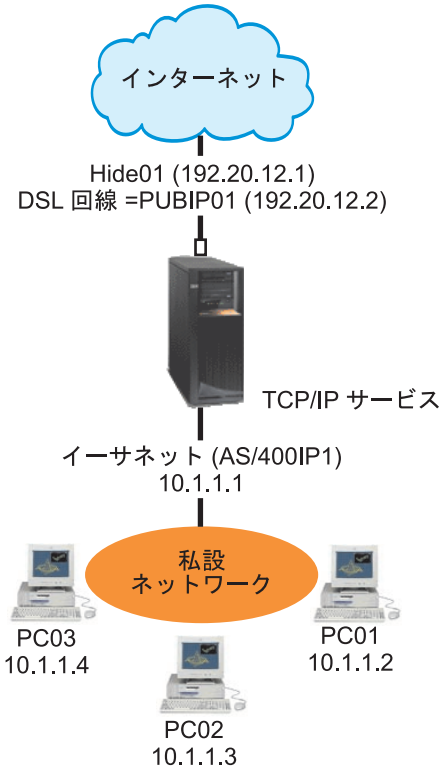
```
FILTER_INTERFACE   LINE = TRNLINE   SET = external_files
```

これらのフィルター・ルールの作成を終えたら、これらのルールをアクティブにする際にエラーが発生しないことを検証してください。その後で、これらのルールをアクティブにすることができます。

パケット・ルールの実例: 隠蔽 IP アドレス (マスカレード NAT)

状況

小規模な会社で、iSeries 上で HTTP サービスを開始したいと考えているとします。 1 枚のイーサネット・カードを装備したモデル 170e と 3 台の PC があるとします。インターネット・サービス・プロバイダー (ISP) からは、DSL 接続 1 つと DSL モデム 1 つが提供されています。また、ISP から公衆 IP アドレスとして 192.20.12.1 と 192.20.2.2 が割り当てられています。社内のすべての PC には、内部ネットワークでアドレス 10.1.1.x が割り当てられています。社内の PC の専用アドレスを隠したままにして、外部ユーザーが内部ネットワークと通信を開始することを防ぎ、その上で従業員がインターネットにアクセスできるようにしたいと考えています。何をすべきでしょうか?



ソリューション

社内の PC アドレス 10.1.1.1 ～ 10.1.1.4 を、公衆アドレス 192.20.12.1 の背後に隠します。これによって、10.1.1.1 アドレスから TCP/IP サービスを実行できるようになります。範囲 NAT を開始するにはトラフィックが内部から発信されなければならないので、この範囲 NAT (一連の内部アドレスを隠している)

が、ネットワーク外部から発信された通信から PC を保護します。しかし、範囲 NAT は iSeries インターフェースを保護しません。変換されていない情報を iSeries が受信しないようにするため、トラフィックをフィルター操作する必要があります。

構成

この実例で説明されているパケット・ルールを構成するには、 iSeries ナビゲーターの「**アドレス変換 (Address Translation)**」ウィザードを使用します。このウィザードでは、以下の情報が必要になります。

- 非公開にするアドレスのセット: 10.1.1.1 〜 10.1.1.4
- そのセットを背後に非公開にするインターフェース・アドレス: 192.20.12.1

「**アドレス変換 (Address Translation)**」ウィザードを使用するには、以下のステップに従います。

1. iSeries ナビゲーターで、「**ユーザーのサーバー (your server)**」-->「**ネットワーク (Network)**」-->「**IP ポリシー (IP policies)**」を選択する。
2. 「**パケット・ルール (Packet Rules)**」を右マウス・ボタンでクリックし、「**ルール・エディター (Rules Editor)**」を選択する。
3. 「**パケット・ルールの構成へようこそ (Welcome Packet Rules Configuration)**」ダイアログから「**新規パケット・ルール・ファイルの作成 (Create a new packet rules file)**」を選択し、「**OK**」をクリックする。
4. 「**ウィザード (Wizards)**」メニューから「**アドレス変換 (Address Translation)**」を選択し、ウィザードの指示に従って隠蔽アドレス変換パケット・ルールを構成する。

パケット・ルールは、以下のようになります。

```
-------------------------------------------------------
Statements to hide 10.1.1.1 - 10.1.1.4 behind 192.20.12.1
-------------------------------------------------------
ADDRESS HIDE1   IP = 10.1.1.1 THROUGH 10.1.1.4
ADDRESS BEHIND1   IP = 192.20.12.1
HIDE HIDE1   BEHIND BEHIND1
-------------------------------------------------------
```

これらのフィルター・ルールの作成を終えたら、これらのルールをアクティブにする際にエラーが発生しないことを検証してください。その後で、これらのルールをアクティブにすることができます。

第 4 章 パケット・ルールの概念

パケット・ルールは、ネットワーク・アドレス変換 (NAT) ルールと IP フィルター・ルールの両方から成ります。これら 2 つのコンポーネントは、TCP/IP スタックの IP 層で実行され、通常の TCP/IP トラフィックで発生しうるリスクからシステムを保護するのに役立ちます。

パケット・ルールの働きを理解するには、これらの概念を知り、それらが iSeries にどのように適用されているを知る必要があります。

- **『パケット・ルールの用語』**
  知っておくべき iSeries 固有の用語のリストを提供します。
- **『パケット・ルールとその他の iSeries セキュリティー・ソリューション』**
  パケット・ルールとその他の iSeries セキュリティー・ソリューションとはどのように比較できるか? ここではそれについて説明します。
- **『ネットワーク・アドレス変換 (NAT)』**
  アドレス変換にはいくつかの異なるタイプがあります。このトピックでは、ご使用のネットワークに適しているタイプを判断するのに必要な情報を提供します。
- **『IP フィルター』**
  パケット・ルールの IP フィルター・コンポーネントの働きについての詳細は、このトピックを参照してください。
- **『IP フィルター・ルールを併用した NAT ルールの編成』**
  NAT ルールと IP フィルター・ルールは、別々に使用することも、一緒に使用することもできます。このトピックでは、この 2 つのコンポーネントを一緒に使用した際の働きについて説明します。
- **『複数の IP フィルター・ルールの編成』**
  フィルター・ルールを作成するとき、システムはそれらのルールを特定の順序で処理します。このトピックでは、複数のフィルター・ルールがどのように処理されるかを説明し、例を示します。
- **『スプーフ保護』**
  このページではスプーフ保護について定義し、なぜそれを使用する必要があるのかについて説明しています。

パケット・ルールの用語

以下のリストには、この Information Center のトピックで使用されている iSeries 固有の用語が含まれています。

ボーダー

ボーダーとは、トラステッド・ネットワークとアントラステッド・ネットワークとの境界を形成する公衆アドレスのことです。iSeries では実際のインターフェースとして IP アドレスを記述します。システムは、ユーザーが定義したアドレスの「タイプ」を知っている必要があります。たとえば、PC の IP アドレスはトラステッドですが、サーバーの公衆 IP アドレスはボーダーになります。

ファイアウォール

ネットワーク内のシステム周辺における論理バリアのことです。ファイアウォールは、セキュア (トラステッド) システムと非セキュア (アントラステッド) システム間の情報のアクセスやフローを制御するハードウェア、ソフトウェア、およびセキュリティー・ポリシーによって構成されます。

maxcon

Maxcon とは、一度にアクティブにできる会話の数です。 NAT のマスカレード・ルールを設定するとき、この数を定義するようにシステムに要求されます。デフォルトは 128 です。 Maxcon は NAT のマスカレード・ルールの場合にのみ関係します。

NAT 会話

NAT 会話は次の IP アドレスとポート番号間のいずれかの関係を示します。

- 私用ソースの IP アドレスとソースのポート番号 (NAT なし)
- 公衆 (NAT) ソースの IP アドレスと公衆 (NAT) ソースのポート番号
- 宛先 IP アドレスとポート番号 (外部ネットワーク)

PPP フィルター ID

PPP フィルター ID によって、Point-to-Point プロファイルで定義されているインターフェースに、フィルター・ルールを適用することができます。PPP フィルター ID は、Point-to-Point プロファイル内のユーザー・グループにも、フィルター・ルールにもリンクします。 Point-to-Point プロファイルは特定の IP アドレスに関連しているので、フィルター ID は、ルールを適用するインターフェースを暗黙的に定義しています。さらに詳しく知りたい場合は、『リモート・アクセス・サービス: *PPP*』トピックの『グループ・ポリシーおよび IP フィルターを使用したリソースへのリモート・ユーザー・アクセスの管理』の実例を参照してください。

タイムアウト

タイムアウトは会話の許可される継続時間を制御します。タイムアウトの設定が短すぎると、会話がすぐに停止します。デフォルトは 16 です。

パケット・ルールとその他の iSeries セキュリティー・ソリューション

iSeries には、さまざまなリスクからシステムを保護することができる統合セキュリティー・コンポーネントが備わっています。そのうちの 1 つであるパケット・ルールは、システムを保護するための経済的な方法を提供します。場合によっては、必要なものはすべてパケット・ルールで提供され、その他のものを購入しなくて済みます。ただし、システムのセキュリティーはコストに優先させるべきです。

実動システムを保護したり、iSeries とその他のシステムとの間の通信を保護したりするようなリスクの高い状態では、他の iSeries セキュリティー・ソリューションを検討して、保護を強化する必要があります。

セキュリティー戦略に複数回線の防御を確実に含めるための情報については、Information Center の以下のトピックを参照してください。

- **『IBM® SecureWay®: iSeries およびインターネット』**
  このトピックでは、インターネットを使用する前に考慮すべきリスクとその解決策についての多くの情報を提供します。
- **『Secure Sockets Layer (SSL)』**
  SSL は、サーバー・アプリケーションとそのクライアントの間にセキュアな接続を提供します。このトピックでは、iSeries アプリケーションで SSL を使用可能にする方法を述べています。
- **『仮想私設ネットワーク (VPN)』**
  VPN を使用すると、自社の専用イントラネットを、公衆ネットワークの既存のフレームワーク (インターネットなど) に安全に拡張することができます。このトピックでは、VPN について説明し、VPN を iSeries で使用する方法について述べています。

- 「**iSeries セキュリティーの手引き**」
  この PDF ブックでは、iSeries を使用してどのようにセキュリティーを強化できるかについての高レベルな情報について記載しています。

ネットワーク・アドレス変換 (NAT)

インターネットの急速な成長により、IP アドレスが不足しています。組織などは使用したい IP アドレスを選択できるようにするため、私設ネットワークを使用しています。しかし、2 つの会社が重複する IP アドレスを持っていて、相互に通信を行なおうとした場合に、問題が生じます。インターネット上で通信を行うためには、固有の登録アドレスが必要になります。ネットワーク・アドレス変換 (NAT) を使用することで、私設ネットワークの IP アドレスを変更せずに、安全にインターネットにアクセスすることができます。用語の示すとおり、NAT は 1 つのインターネット・プロトコル (IP) アドレスを別のアドレスに変換するメカニズムです。

パケット・ルールには、NAT の方式が 3 つ用意されています。NAT は、通常、アドレスのマップ (静的 NAT) またはアドレスの隠蔽 (マスカレード NAT) に使用されます。各種類の NAT の詳細については、次のリンクを参照してください。

- 『静的 (マップ) NAT』
- 『マスカレード (隠蔽) NAT』
- 『マスカレードまたは隠蔽 (ポート・マップ) NAT』

アドレスを隠す、またはマッピングすることにより、NAT はさまざまなアドレスの問題を解決します。次の例では、NAT が解決できるいくつかの問題を示してあります。

例 1: 公衆から内部 IP アドレスを隠す

iSeries を公衆 Web サーバーとして構成するとします。しかし、サーバーの実際の内部 IP アドレスは外部ネットワークに知られないようにしたいと考えています。 NAT ルールを作成して、専用アドレスをインターネットにアクセスできる公衆アドレスに変換することができます。この場合、サーバーの「真の」アドレスは隠されたままなので、サーバーがアタックされにくくなります。

例 2: 内部ホストの IP アドレスを別の IP アドレスに変換する

内部ネットワークの専用 IP アドレスを使用して、インターネット・ホストとの通信を行いたいとします。これを行うには、内部ホストの IP アドレスを別の IP アドレスに変換します。インターネット・ホストと通信するには、公衆 IP アドレスを使用する必要があります。そこで NAT を使い、専用 IP アドレスを公衆 IP アドレスに変換します。これにより、内部ホストからの IP トラフィックがインターネットに確実に経路指定されます。

例 3: 2 つの異なるネットワークの IP アドレスが共存できるようにする

内部ネットワークの特定のホストと、別のネットワーク (ベンダーなど) のホスト・システムとを通信させたいものとします。しかし両方のネットワークが専用アドレス (10.x.x.x) を使用しており、 2 つのホスト間のトラフィックを経路指定するとアドレス競合が生じる可能性があります。 NAT を使用して、内部ホストのアドレスを別の IP アドレスに変換すると、競合を避けることができます。

静的 (マップ) NAT

静的 (マップ) NAT は、専用 IP アドレスを公衆 IP アドレスに 1 対 1 でマップします。内部ネットワーク上の IP アドレスを、公衆アドレスとして使用する IP アドレスにマップすることができます。

静的 NAT では、インターネットのように内部ネットワークまたは外部ネットワークから発信された通信を許可します。内部ネットワーク内にサーバーがあり、これに対して公衆ユーザーにアクセス許可を与える場合は、特に便利です。この場合、実際のサーバーのアドレスを公衆アドレスにマップする NAT ルールを作成する必要があります。公衆アドレスは外部の情報になります。これにより、システムへのアタックから、私用の情報を確実に守ることができます。

次のリストでは、静的 NAT の機能について説明しています。

- 1 対 1 のマッピング
- 外部および内部ネットワークの開始
- マップまたは関連付けるアドレスは任意のアドレスにできる
- マップまたは関連付けるアドレスは IP アドレスとして使用できない
- ポート・マップ NAT を使用できない

重要

PC を iSeries の「予約済み」アドレスにマップする場合は注意してください。予約済みアドレスは、大半のインターネットおよびイントラネットのトラフィックのために予約されている IP アドレスです。この IP アドレスへのマップが行われると、NAT はすべてのトラフィックを変換して内部の専用アドレスに送信します。このインターフェースは NAT 用に予約されるので、iSeries およびインターフェースは使用できなくなります。

静的 NAT の実例と図については、『パケット・ルールの実例: IP アドレスのマップ』を参照してください。

マスカレード (隠蔽) NAT

マスカレード (隠蔽) NAT を使用すると、外部 (iSeries の外部) から PC の実アドレスを知られないようにすることができます。トラフィックは PC から iSeries に経路指定され、これにより iSeries が基本的に PC のゲートウェイとなります。ここにその仕組みを示します。

マスカレード NAT は、複数の IP アドレスを別の 1 つの IP アドレスに変換します。マスカレード NAT は、公衆にする IP アドレスの背後に 1 つ以上の内部ネットワーク IP アドレスを隠す ために使用します。この公衆アドレスは、専用アドレスを変換したアドレスと一致し、iSeries サーバー上の定義済みインターフェースである必要があります。インターフェースを定義するには、対象の公衆アドレスを BORDER アドレスとして定義しなければなりません。

複数のアドレスを隠す

複数のアドレスを隠すには、NAT が iSeries サーバーを通じて変換するアドレスの範囲を指定します。次に一般的なプロセスを示します。

1. ソース IP アドレスを変換した IP アドレスに置き換えます。これは IP パケットの IP ヘッダーで行われます。
2. 転送制御プロトコル (TCP) にある IP ソースのポート番号 (存在する場合) またはユーザー・データグラム・プロトコルのヘッダーは、一時的なポート番号に置き換えられます。
3. 既存の会話は、新しい IP ソース・アドレスとポート番号の関係になります。
4. この既存の会話を使用すると、NAT サーバーは外部マシンからの IP データグラムを変換しません。

IP データグラムのヘッダーを表示するには、IP パケットのヘッダーに移動します。

マスカレード NAT を使用すると、内部システムがトラフィックを開始します。この場合、NAT は iSeries NAT サーバーを通過した時点で IP パケットを変換します。外部ホストから内部ネットワークへのトラフィックを開始できないため、マスカレード NAT を選択することは非常に有効です。その結果、外部からのアタックに対するネットワーク保護がさらに強化されます。また、複数の内部ユーザーに 1 つの公衆 IP アドレスを購入するだけで済みます。

次のリストでは、マスカレード NAT の機能について説明しています。

- 専用 IP アドレスまたは一連の専用 IP アドレスは NAT マシン上の公衆 IP アドレスの背後にバインドされます。
- 内部ネットワークからしか開始できません。
- ポート番号がランダム・ポート番号に関連付けられます。これは、アドレスとポート番号の両方をインターネットから隠すことを意味します。
- NAT マシン上の登録アドレスは、NAT 外部のインターフェースで使用できます。

重要

- 必要数の会話が使用可能となるように、MAXCON の設定値を上げる必要があります。たとえば、FTP を使用している場合、PC では 2 つの会話がアクティブになります。この場合、PC ごとに複数の会話が使用可能となるように、MAXCON の設定値を上げる必要があります。ネットワークで同時に行われる会話の許可数を設定する必要があります。デフォルトは 128 です。
- PC 間での会話が終了するまでに必要な時間を十分に確保するため、TIMEOUT (HIDE ルール・ステートメントの 1 つ) の設定値を上げる必要があります。隠蔽 NAT が正常に動作するには、内部の会話が進行中である必要があります。タイムアウト値は、この内部の会話に対する応答を待つ時間をコードに伝えます。デフォルトは 16 です。
- マスカレード NAT は TCP、UDP、および ICMP のプロトコルのみをサポートします。
- NAT を使用する場合は、常に IP 転送を使用可能にしなければなりません。TCP/IP 属性の変更 (CHGTCPA) コマンドを使用して、IP データグラムの転送が YES に設定されていることを確認します。

マスカレードまたは隠蔽 NAT の例については、『IP アドレスの隠蔽 (マスカレード NAT)』の実例と図を参照してください。

マスカレード (ポート・マップ) NAT

ポート・マップ NAT はマスカレード NAT の一種です。違いは何でしょうか。ポート・マップ NAT では、変換に IP アドレスとポート番号の両方を指定できます。これにより、内部 PC と外部マシンの両方から IP トラフィックを開始できます。外部マシン (またはクライアント) がネットワーク内部のマシンまたはサーバーにアクセスする場合に、この機能を使用します。 IP アドレスとポート番号の両方に一致する IP トラフィックのみがアクセスを許可されます。ここにその仕組みを示します。

内部からの開始

アドレス 1: ポート 1 の内部 PC として、外部マシンへのトラフィックを開始します。変換コードは、*アドレス 1: ポート 1* があるかどうかを NAT ルールのファイルで検査します。アドレス (アドレス 1) とソース・ポート番号 (ポート 1) の両方が NAT ルールと一致している場合、NAT は会話を開始し、変換を実行します。 NAT ルールから指定された値が、IP ソース・アドレスとソースのポート番号に置き換えられます。*アドレス 1: ポート 1* はアドレス *2: ポート 2* に置き換えられます。

外部からの開始

外部マシンはアドレス *2* の宛先 IP アドレスを使用して IP トラフィックを開始します。宛先ポート番号はポート *2* です。 NAT サーバーは「既存の会話」の有無にかかわらず、データグラムを変換しません。つまり、NAT は会話がすでに存在していない場合は自動的に会話を作成します。*アドレス 2: ポート 2* は *アドレス 1: ポート 1* に変換されていません。

次のリストでは、マスカレード・ポート・マップ NAT の機能について説明しています。

- 1 対 1 関係。
- 外部および内部ネットワークでの開始。
- 専用アドレスを背後に隠す登録済みアドレスを、NAT 操作を実行している iSeries において定義する必要があります。
- NAT 操作外の IP トラフィックは、登録済みアドレスを使用できません。しかし、このアドレスが NAT ルールで隠蔽されたポートと一致するポート番号を使用しようとした場合、トラフィックが変換されるようになります。インターフェースは使用できなくなります。
- 通常、ポート番号は予約済みポート番号にマップされるので、特別な情報は不要です。たとえば、ポート 5123 にバインドした HTTP サーバーを稼働させることができますが、その場合は、このポートを公衆 IP およびポート 80 にマップします。内部ポート番号を別の (一般的ではない) ポート番号の背後に隠したい場合は、クライアントに宛先ポート番号の値を物理的に通知する必要があります。これを行わない場合、通信の開始が困難になります。

重要

- 必要数の会話が使用可能となるように、MAXCON の設定値を上げる必要があります。たとえば、FTP を使用している場合、PC では 2 つの会話がアクティブになります。 PC ごとに複数の会話が使用可能となるように、MAXCON の設定値を上げる必要があります。デフォルトは 128 です。
- マスカレード NAT は TCP、UDP、および ICMP のプロトコルのみをサポートします。
- NAT を使用する場合は、常に IP 転送を使用可能にしなければなりません。TCP/IP 属性の変更 (CHGTCPA) コマンドを使用して、IP データグラムの転送が YES に設定されていることを確認します。

IP フィルター

パケット・ルールは、それ自体で完全に機能するファイアウォールではありませんが、iSeries のパケットをフィルター操作できる堅固なコンポーネントを備えています。特に、パケット・ルールの IP フィルター・コンポーネントを使用することで、自社のネットワークに入ってきたり、自社のネットワークから出て行ったりすることを許可する IP トラフィックを制御することができます。 IP フィルターを使用して、指定されたルールに従ってパケットをフィルター操作することによりシステムを保護します。これらのルールは、『IP パケット・ヘッダー』に記載されている情報に基づいています。

フィルター・ルールを複数の回線に適用したり、回線ごとに異なるルールを適用したりすることができます。フィルター・ルールはトークンリング (trnline) などの回線に関連付けられており、論理インターフェースや IP アドレスには関連付けられていません。システムは回線に関連付けられた各ルールに対して、各パケットを検査します。ルールは順番に検査されます。パケットがルールに適合すると、システムは処理を停止し、適合したルールを適用します。

適合したルールがシステムに適用されると、そのルールによって指定されたアクションを実際にシステムが実行します。 iSeries は次の 3 つのアクションをサポートしています (V4R4 以降)。

1. PERMIT − パケットの通常どおりの処理を許可する

2. DENY － 即座にパケットを廃棄する
3. IPSEC － VPN 接続を介してパケットを送信する (フィルター・ルールで指定したもの)

注: この場合、IPSEC はユーザーがフィルター・ルールで定義したアクションとなります。このトピックでは IPSec について特に説明しませんが、フィルターと仮想私設ネットワーク (VPN) が密接に関係している点に注意してください。 VPN の詳細については、『仮想私設ネットワーク (VPN)』のトピックを参照してください。

ルールを適用した後、システムは引き続きルールとパケットの比較を順番に行い、すべての対応するルールにアクションを割り当てます。特定のパケットに対して適合ルールが検出できない場合、システムは自動的にそのパケットを廃棄します。システムのデフォルト拒否ルールによって、システムは確実に、フィルター・ルールに適合しないパケットを自動的に廃棄します。フィルター・ルールでインバウンドまたはアウトバウンドのうち一方向のトラフィックのみが許可されている場合は、システムは両方向についてデフォルト拒否ルールをインプリメントすることに注意してください。つまり、インバウンドとアウトバウンドの両方のパケットが廃棄されます。

サンプル・フィルター・ステートメント

このサンプル・フィルター・ステートメントは、iSeries でフィルター・ルールを作成するための正しい構文を示し、ファイル内でさまざまなステートメントがどのように機能するかを示すことを目的としています。これは、例としてのみ使用してください。

一般的なフィルター・ステートメントは、以下のようなものです。

```
FILTER SET TestFilter   ACTION = PERMIT   DIRECTION = INBOUND   SRCADDR = 162.56.39.100
DSTADDR = *   PROTOCOL = *   DSTPORT >= 1024   SRCPORT = 80
```

このフィルターは、インターフェースに入って来る (INBOUND)、ソース・アドレスが 162.56.39.100、ソース・ポートが 80、宛先ポートが 1024 以上のすべてのトラフィックを許可します。

IP トラフィックは、一般的には接続上 INBOUND と OUTBOUND の両方向に流れるので、両方向のトラフィックを許可するための 2 つの関連ステートメントがあるのが普通です。これら 2 つのステートメントは相互のミラーと呼ばれます。以下に例を示します。

```
FILTER SET TestFilter   ACTION = PERMIT   DIRECTION = INBOUND   SRCADDR = 162.56.39.100
DSTADDR = *   PROTOCOL = *   DSTPORT >= 1024   SRCPORT = 80
FILTER SET TestFilter   ACTION = PERMIT   DIRECTION = OUTBOUND   SRCADDR = *   DSTADDR =
162.56.39.100   PROTOCOL = *   DSTPORT = 80   SRCPORT >= 1024
```

これらのフィルター・ステートメントでは、両方とも同じセット名 TestFilter になっています。同じセット名のフィルターはすべて、同じセット内にあると見なされます。 1 つのセットに、フィルターがいくつあっても構いません。指定されたセット内でフィルターをアクティブにすると、それらのフィルターはファイル中に現れる順序で処理されます。

ルールをアクティブにしたとき、フィルター・ステートメント単体では何も機能しません。フィルター・セットをフィルター・インターフェースに適用する必要があります。セット TestFilter をイーサネット回線インターフェースに適用する例を、以下に示します。

```
FILTER_INTERFACE   LINE = ETH237   SET = TestFilter
```

これらのルールをアクティブにした後は、ETH237 上で許可される IP トラフィックは、TestFilter セットによって許可されているもののみになります。

注: インターフェースでアクティブにされるすべてのフィルターの最後に、システムによって、デフォルトで DENY ALL TRAFFIC ルールが追加されます。したがって、iSeries を構成しているインターフェースにルールを適用する際は、自分自身のワークステーションを許可するか、または iSeries を構成する可能性のある別の人のワークステーションを許可することが大変重要です。これを行なわないと、iSeries との通信が失われてしまいます。

以下のように、複数のセットを 1 つのフィルター・インターフェース・ステートメントに適用することができます。

```
FILTER_INTERFACE   LINE = ETH237   SET = set1, set2, set3
```

これらのセットは、フィルター・インターフェース・ステートメントでリストしたのと同じ順番 (セット 1、セット 2、最後にセット 3) で処理されます。それぞれのセットごとに、そのセット内のフィルターは、ファイル中に現れる順序で処理されます。つまり、異なるセット間のフィルターの順序は無意味であることになります。フィルターの順序は、フィルターが同じセット内にあるときに問題になります。

IP パケット・ヘッダー

フィルター・ルールを作成して、IP ヘッダー、TCP ヘッダー、UDP ヘッダー、および ICMP ヘッダーなどのさまざまな部分を参照することができます。以下のリストは、IP パケット・ヘッダーを構成するフィルター・ルール内で参照するフィールドを示します。

- ソース IP アドレス
- プロトコル (TCP、UDP など)
- 宛先 IP アドレス
- ソース・ポート
- 宛先ポート
- IP データグラムの方向 (インバウンド、アウトバウンド、または両方)
- TCP SYN ビット

たとえば、宛先 IP アドレス、ソース IP アドレス、および方向 (インバウンド) に基づいてパケットをフィルターに掛けるルールを作成し、適用することができます。この場合、システムは、(起点や宛先アドレスに応じて) すべての着信パケットを対応するルールにマッチングします。そして、ルールに指定されているアクションが実行されます。システムはフィルター・ルールで許可されていない パケットを破棄します。これは、デフォルト拒否ルールと呼ばれています。

注: システムは、物理インターフェースにアクティブなルールが少なくとも 1 つある場合に限り、デフォルト拒否ルールをパケットに適用します。このルールは、ユーザー定義にすることも、iSeries ナビゲーターを使用して生成することもできます。フィルター・ルールがインバウンド・トラフィックを許可するのかアウトバウンド・トラフィックを許可するのかにかかわらず、システムは両方向でデフォルト拒否ルールをインプリメントします。物理インターフェースにアクティブなフィルター・ルールがない場合は、デフォルト拒否ルールは機能しません。

IP フィルター・ルールを併用した NAT ルールの編成

NAT と IP フィルターは、お互いに独立して作動します。しかし、IP フィルター操作と NAT を関連付けて使用することができます。 NAT ルールのみを適用するようにした場合、システムはアドレス変換だけを行います。同様に、IP フィルター・ルールのみを適用するようにした場合、システムは IP トラフィックだけをフィルター操作します。しかし、両方のタイプのルールを適用すると、システムはアドレスを変換し、フィルター操作を行います。 NAT とフィルターを一緒に使用すると、特定の順序でルールが実行されます。インバウンド・トラフィックの場合は、NAT ルールが先に処理されます。アウトバウンド・トラフィックの場合は、フィルターが先に処理されます。

NAT ルールとフィルター・ルールを別々のファイルに作成することができます。これは必須ではありませんが、フィルター・ルールを読みやすくしたり、トラブルシューティングが容易になります。いずれの方法 (別々または一緒のファイル) にしても、発生するエラーは同じです。 NAT ルールとフィルター・ルールに別々のファイルを使用する場合、両方のルールをアクティブにすることができます。ただし、ルールがお互いに競合しないようにしてください。

NAT ルールとフィルター操作ルールを同時にアクティブにするには、*組み込み* 機能を使用する必要があります。たとえば、フィルター・ルールにファイル A を NAT ルールにファイル B を作成したとします。ファイル B の内容を、ルールを一切書き直さずにファイル A に組み込むことができます。この方法の詳細については、『パケット・ルールにファイルを組み込む』を参照してください。

複数の IP フィルター・ルールの編成

フィルター・ルールを作成する場合、1 つのフィルターにつき 1 つのルール・ステートメントが参照されます。1 つのセットにつき 1 つのフィルター・グループが参照されます。1 つのセット内のフィルターは、物理的な順序に従い、上位から下位へと処理されます。同様に、複数のセットも、FILTER_INTERFACE ステートメント内の物理的な順序に従って処理されます。

下の例では、1 つのセットに 3 つのフィルター・ステートメントが含まれています。このセットを参照する場合、常にこれらの 3 つのルールがすべて組み込まれます。通常、フィルター・ルールをすべて 1 つのセットに組み込むのが最も簡単です。

```
FILTER SET all ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR  %
        = * PROTOCOL = TCP/STARTING DSTPORT = * SRCPORT = * FRAGMENTS  %
        = HEADERS JRN = FULL
FILTER SET all ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR  %
        = * PROTOCOL = TCP DSTPORT = * SRCPORT = * FRAGMENTS = NONE  %
        JRN = OFF
FILTER SET all ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR  %
        = * PROTOCOL = ICMP TYPE = * CODE = * FRAGMENTS = NONE JRN  %
        = OFF
FILTER_INTERFACE LINE = ETHLINE SET = all
###Ethernet line ETHLINE
```

スプーフ保護

誰かが、自社ネットワーク内で通常のトラステッド・システムであることをよそおって、そのシステムにアクセスしようとしたときに、スプーフィングが発生します。公衆ネットワークにリンクしているインターフェースを、この種の攻撃から守る必要があります。 iSeries ナビゲーターのパケット・ルール・エディターで提供されている「スプーフ保護 (Spoof Protection)」ウィザードを完成させることで、スプーフィングから保護することができます。このウィザードは、侵入されやすいインターフェースにルールを割り当てるのに役立ちます。ルールがアクティブになると、公衆 (非トラステッド) ネットワークからのシステムが、専用 (トラステッド) ネットワークからのトラステッド・マシンとして振る舞うことはできなくなります。

第 5 章 パケット・ルールの計画

自社のネットワーク・リソースをインターネットに接続する前に、セキュリティー計画を立てて、発生しうるセキュリティー上のリスクを理解しておく必要があります。一般的には、インターネットを使用するための計画の立て方について詳細な情報を集め、また内部ネットワークの構成を記述した文書を集める必要があります。これらの情報を集めた結果に基づいて、セキュリティー要件を正確に評価することができます。トピック『IBM SecureWay: iSeries とインターネット』に、全体のネットワーク・セキュリティー計画を作成するのに必要な詳細事項が記載されています。パケット・ルールを使用する計画がある場合、以下のトピックを参照して、パケット・ルールの構成を開始するのに必要な情報をすべて集めてください。

- **『パケット・ルール: ユーザー権限要件』**
  パケット・ルールを管理するための正しい権限を持っているかどうかを確認します。
- **『パケット・ルール: システム要件』**
  ご使用の iSeries が、パケット・ルールを使用して作動するための最低限のシステム要件に合っているかどうかを確認します。
- **『パケット・ルール: 計画ワークシート』**
  このワークシートを使用すると、パケット・ルールの構成を開始するのに必要な情報を集めるのに役立ちます。

計画の作成が完了したら、パケット・ルールの構成を開始することができます。

パケット・ルール: ユーザー権限要件

iSeries でパケット・ルールを管理するためには、その前に、正しい権限を持っているかどうかを確認してください。ユーザー・プロファイルに *IOSYSCFG 特殊権限を持っている必要があります。 QSECOFR ユーザー ID または *SECOFR タイプのユーザー ID からパケット・ルールを管理する計画を立てている場合、あるいは *ALLOBJ 権限を持っている場合は、それで管理することができます。そうでない場合は、以下のディレクトリー、ファイル、および QSYS ユーザー ID に対する権限が必要です。

1. 以下の 3 つのファイルに対するオブジェクト権限 `*RXW` およびデータ権限 `OBJMGT` を追加します。
   `/QIBM/ProdData/OS400/TCPIP/PacketRules/Template4PacketRules.i3p`
   `/QIBM/ProdData/OS400/TCPIP/PacketRules/Template4PacketRules.txt`
   `/QIBM/ProdData/OS400/TCPIP/PacketRules/Template4PacketRules.tcpipml`
2. 以下のディレクトリーに対するオブジェクト権限 `*RWX` を追加します。
   `/QIBM/UserData/OS400/TCPIP/PacketRules`
   `/QIBM/UserData/OS400/TCPIP/OpNavRules`
3. 以下のファイルに対するオブジェクト権限 `*RWX` を追加します。
   `/QIBM/UserData/OS400/TCPIP/OpNavRules/VPNPolicyFilters.i3p`
   `/QIBM/UserData/OS400/TCPIP/OpNavRulesPPPFilters.i3p`
4. QSYS プロファイルに対する `ADD` 権限も必要です。これは、新しく作成されるルール・ファイルを QSYS が所有しているからです。

これらは、パケット・ルール・エディターが使用するディレクトリーのディレクトリーおよびファイルです。上記のリスト以外のディレクトリーにファイルを保管することにした場合は、それらのディレクトリーに対する権限が必要です。

パケット・ルール: システム要件

iSeries で正しく機能させるには、パケット・ルールのために以下のものが必要です。

1. OS/400® バージョン 5 リリース 2 (5722-SS1)、またはそれ以上
2. iSeries Access for Windows® (5722-XE1) および iSeries ナビゲーター
   - iSeries ナビゲーターのネットワーク・コンポーネント
3. TCP/IP (5722-TC1) を、IP インターフェース、経路、ローカル・ホスト名、およびローカル・ドメイン・ネームを組み込んで構成しなければなりません。

注: TCP/IP、ネットワーキング、または IP アドレスについて理解していない場合は、「TCP/IP Tutorial and Technical Overview」  および「V4 TCP/IP for AS/400®: More Cool Things Than Ever」  を参照してください。

パケット・ルール: 計画ワークシート

パケット・ルールの計画ワークシートを使用して、パケット・ルールの使用計画に関する詳細情報を集めてください。セキュリティーの要件を特定するために、この情報が必要です。また、この情報を使用して、パケット・ルールを構成することもできます。システムでパケット・ルールの構成を進める前に、各質問に答えてください。

パケット・ルールを使用する計画を作成するために必要な情報	回答
ネットワークおよび接続のレイアウトはどのようになっていますか? それを示す図を作成してください。	
使用するルーターと IP アドレスは何ですか?	
システムを通る TCP/IP トラフィックの制御に使用するルールは何ですか? リストした各ルールごとに、以下の、TCP/IP トラフィック・フローの特性を指定してください。 • 許可または拒否するサービスのタイプ (たとえば、HTTP、FTP など) • そのサービスに対して事前に割り当てられているポート番号 • 通信の方向 • 応答側通信か開始側通信か • 通信の IP アドレス (ソースおよび宛先)	
他のアドレスにマップするかまたは他のアドレスの背後に隠す IP アドレスは何ですか? (このリストは、ネットワーク・アドレス変換を使用する場合にのみ必要です。)	

第 6 章 パケット・ルールの構成

ご使用のシステムに関してパケット・ルールを構成するための計画の作成が完了したら、それらを実際に作成し、適用する準備をする必要があります。パケット・ルール・エディターのオンライン・ヘルプで、特定的なステップバイステップの情報を見ることができます。以下のチェックリストでは、ルールをアクティブにしたときに確実に正しく作動させるために実行する必要のあるタスクの概要を示します。

__ 1. パケット・ルール・エディターにアクセスする。
iSeries ナビゲーターのパケット・ルール・エディターにアクセスするには、ここでの指示に従います。

__ 2. パケット・ルール・エディター (V5R2 以降) の一部として提供されているウィザードを使用して、ルール・ファイルを作成する。

- **「サービスの許可 (Permit a Service)」ウィザード**
このウィザードでは、指定された TCP または UDP サービスのために必要なトラフィックを許可する、パケット・ルール・ステートメントのセットを生成し、挿入します。
- **「スプーフ保護 (Spoof Protection)」ウィザード**
このウィザードでは、あるインターフェース上で、別のインターフェースを通ってこのサーバーに入ってくるはずのトラフィックをすべて拒否する、パケット・ルール・ステートメントのセットを生成し、挿入します。
- **「アドレス変換 (Address Translation)」ウィザード**
このウィザードでは、マップまたは隠蔽パケット・ルール・ステートメントのセットを生成し、挿入します。

構成するルールのタイプに従って、これらのウィザードが、必要なフィルターおよび NAT ステートメントをすべて作成します。ウィザードには、パケット・ルール・エディターの「**ウィザード (Wizards)**」メニューからアクセスできます。自分でルールを作成したい場合は、チェックリスト内の次の項目に進んでください。

__ 3. アドレスおよびサービスを定義する。
複数のルールを作成する計画を立てているアドレスおよびサービスの別名を作成します。

注: NAT の使用を計画している場合は、*必ず* アドレスを定義してください。

__ 4. NAT ルールを作成する。
NAT の使用を計画している場合のみ、このタスクを実行します。

__ 5. フィルター・ルールを作成する。
このシステムが管理する、ネットワークに適用するフィルターを定義します。

__ 6. ファイルを組み込む。
「マスター」ルール・ファイルに組み込む追加ファイルを指定します。新しいルール・ファイルで再利用したい既存のルール・ファイルがある場合にのみ、このタスクを実行します。

__ 7. インターフェースを定義する。
ルールをインターフェースに適用します。

__ 8. コメントを作成する。
それぞれのルール・ファイルが何をするのか説明します。

__ 9. ルール・ファイルを検証する。
エラーおよび問題がなく、ルールをアクティブにできることを確認します。

__ 10. ルール・ファイルをアクティブにする。
パケット・ルールは、作動させるためにはアクティブにする必要があります。

__ 11. パケット・ルールを管理する。
パケット・ルールをアクティブにした後は、定期的に管理して、システムのセキュリティーを保守

する必要があります。このトピックでは、ルール・ファイルの編集、パケット・ルール・アクションのジャーナル記録と監査、およびバックアップと回復のヒントと手法について説明しています。

パケット・ルールへのアクセス

パケット・ルール・エディターにアクセスするには、iSeries リソースでの作業を可能にするグラフィカル・インターフェースである、iSeries ナビゲーターを通して行なう必要があります。システムでパケット・ルールの作成を開始するには、パケット・ルール・エディターを使用してください。新しいファイルの作成、既存のファイルの編集、あるいは、システムで提供されているサンプル・ファイルでの作業が可能です。

パケット・ルール・エディターにアクセスするには、以下のステップに従います。

1. iSeries ナビゲーターで、「ユーザーのサーバー (your server)」-->「**ネットワーク (Network)**」-->「**IP ポリシー (IP Policies)**」を拡張する。
2. 「**パケット・ルール (Packet Rules)**」を右マウス・ボタンでクリックし、「**ルール・エディター (Rules Editor)**」を選択する。

このトピックの『パケット・ルールの構成』セクションで説明されている各タスクを実行する方法については、オンライン・ヘルプにステップバイステップの指示が記載されています。

アドレスおよびサービスの定義

パケット・ルールを作成する際は、そのルールを適用する IP アドレスおよびサービスを指定する必要があります。**定義アドレス**は、シンボル名を与えられたインターフェース指定です。表したいアドレスがアドレス範囲、サブセット、Point-to-Point ID のリスト、または不連続アドレスのリストである場合に、アドレスを定義しなければなりません。マップ・アドレス変換ルールを作成する予定がある場合、定義アドレス・ステートメントが必要になります。表したいアドレスが、フィルター・ステートメント内の 1 つの IP アドレスである場合、定義アドレス・ステートメントは必要ありません。**サービスの別名**を使用すると、サービスを定義して、それらを複数のフィルターで再利用することができます。また、サービスの別名は、別のサービス定義の目的をトラッキングします。

アドレスおよびサービスの別名を定義することで、パケット・ルールの作成が容易になります。ルールを作成すると、特定のアドレスやサービスの詳細ではなく、アドレスのニックネームまたはサービスの別名を参照するようになります。フィルター・ルールにニックネームや別名を使用すると、次の 2 つの利点があります。

1. タイプミスのリスクを最小限にできる。
2. 作成する必要のあるフィルター・ルールの数を最小限にできる。

たとえば、インターネット・アクセスを必要とするユーザーがネットワーク内に 31 人いるとします。ただし、これらのユーザーのアクセスを Web アクセスのみに制限するものとします。この場合、必要なフィルター・ルールを作成する方法を 2 つの中から選択できます。

1. 各ユーザーの IP アドレスにフィルター・ルールを定義します。
2. アドレスを定義して、アドレス・セット全体にユーザーを表すニックネームを作成します。

1 つ目を選択した場合、ルール・ファイルに対して実行しなければならない保守の回数が増えるだけでなく、タイプミスをする可能性も高くなります。2 つ目を選択した場合、2 つのフィルター・ルールを作成するだけです。各ルールにニックネームを使用して、そのルールが適用される全体のアドレス・セットを参照するようにします。

またサービスに対するニックネームを作成して、アドレスのニックネームと同じように使用することもできます。サービスの別名では、選択する TCP、UDP、および ICMP の基準を定義します。また、使用するソースと宛先ポートを選択します。

注: NAT の使用を計画している場合は、必ず アドレスを定義してください。 NAT ルールは定義アドレスのみを指すことができます。

アドレス、サービスの別名、および ICMP サービスを定義する方法については、パケット・ルール・エディターのオンライン・ヘルプにステップバイステップの指示が記載されています。

次のステップ
ネットワーク・アドレス変換を使用する予定がある場合は、『NAT ルールの作成』に進んでください。それ以外の場合は、『IP フィルター・ルールの作成』に進み、自社ネットワークに入って来る、あるいは自社ネットワークから出て行く、IP トラフィックをフィルター操作します。

NAT ルールの作成

NAT の使用を決定する場合、使用する IP アドレスにニックネームを定義しなければなりません。標準の 32 ビット・アドレス表記を使用している場合、NAT ルールを作成できません。 193.112.14.90 などの実アドレスを指定するのではなく、*名前* によって 193.112.14.90 を参照しなければなりません。システムでは、定義した名前を対応するアドレスに関連付けて、それらを適宜変換します。したがって、システムが NAT ルールをアドレスに適用する前に、アドレスの定義を行う必要があります。

パケット・ルール・エディターでは、2 つのタイプの NAT ルールを作成できます。一方のタイプではアドレスを隠し、もう一方ではアドレスをマップします。

アドレスを隠す
専用アドレスを公衆で表示しないようにするには、アドレスを隠す必要があります。隠しアドレス・ルールを使用すると、複数の内部アドレスを 1 つの公衆 IP アドレスの陰に隠すことができます。このタイプの NAT は、*マスカレード* NAT とも呼ばれます。

アドレスをマップする

1 つの公衆 IP アドレスから 1 つの内部アドレスにトラフィックを経路指定する場合は、アドレスのマッピングを行う必要があります。このタイプの NAT は、*静的* NAT とも呼ばれます。

アドレスを隠蔽またはマップする方法については、パケット・ルール・エディターのオンライン・ヘルプにステップバイステップの指示が記載されています。

次のステップ
自社ネットワークに入って来る、あるいは自社ネットワークから出て行くトラフィックをフィルター操作する予定がある場合は、『IP フィルター・ルールの作成』に進みます。それ以外の場合は、『パケット・ルールでのコメントの作成』に進みます。

IP フィルター・ルールの作成

フィルターを作成するときに、自社システムに入って来る、あるいは自社システムから出て行く、IP トラフィックの流れを管理するルールを指定します。ユーザー定義のルールによって、システムにアクセスしようとしているパケットの許可または拒否が決まります。システムは、IP パケット・ヘッダー内の情報のタイプに応じて、IP パケットを送信します。システムはまた、システムに適用するよう指定したアクションを IP パケットに指示します。特定のルールに適合しないパケットは廃棄されます。この自動廃棄ルール

は、*デフォルト拒否ルール* と呼ばれます。デフォルト拒否ルールはファイルの最後にあり、パケットが、その前にあったルールの基準にすべて合わなかった場合に、このデフォルト拒否ルールが自動的にアクティブになります。デフォルト拒否ルールをアクティブにするには、少なくとも 1 つのフィルター・ルールをアクティブにする必要があります。

注: iSeries を構成しているインターフェースにルールを適用する際は、自分自身のワークステーションを許可するか、または iSeries を構成する可能性のある別の人のワークステーションを許可することが大変重要です。これを行わないと、iSeries との通信が失われてしまいます。このようなことが起こったら、まだ接続を保っているインターフェース (オペレーター・コンソールなど) を使用して、iSeries にログオンしなければなりません。 RMVTCPTBL コマンドを使用して、システム上のすべてのフィルターを除去します。

フィルター・ルールを作成する前に、ネットワーク・アドレス変換 (NAT) を使用する必要があるかどうかを決めます。NAT ルールを使用する場合は、アドレスおよびサービスの定義を行う必要があります。NAT は、定義アドレスを必要とする唯一の機能ですが、他の機能にも同様に使用することができます。アドレスおよびサービスを定義すると、タイプミスの可能性を最小限にするだけでなく、作成しなければいけないルールの数を減らすことができます。

フィルター・ルールを作成するときに、最小限のエラーと最大限の効率を実現するいくつかの方法を次に示します。

- **一度に 1 つのフィルター・ルールを定義します。**たとえば、Telnet に対する許可を同時にすべて作成します。こうすると、ルールを参照するとき常にルールに関連してグループ化することができます。
- **フィルター・ルールはファイルに並べられている順序で処理されます。**作成時に、ルールを適用する順序に並べるようにしてください。順序に誤りがある場合、パケットが予定通りに処理されなくなるため、システムがアタックされやすくなります。より簡単にするには、次のアクションを検討します。
  1. フィルター・セット名を、ファイルで物理的に定義されているのと全く同じ順序で FILTER_INTERFACE ステートメントに設定します。
  2. 1 つのセットにすべてのフィルター・ルールを設定して、セット順序の問題を回避します。
- **処理しながら各ルールの構文を検証します。**この方が一度にすべてをデバッグするよりも簡単で早く検証できます。
- **論理的に相互関連のあるファイル・グループのセット名を作成します。**一度にアクティブにできるルール・ファイルは 1 つしかないため、これは重要です。次の例を参照してください。
- **許可するデータグラムのフィルター・ルールを書き込むだけです。**他のフィルター・ルールは自動拒否ルールによって破棄されます。
- **大量のトラフィックを扱うルールから先に書き込みます。**

例: 上記の*セット名の作成* ヒントを参照してください。多くの内部ユーザーに Telnet のアクセスを許可しますが、全員に許可するわけではないとします。これらのルールの管理を簡単にするため、各ルールにセット名 `TelnetOK` を割り当てます。特定のインターフェースを経由する Telnet を許可し、他からの Telnet のトラフィックをすべてブロックすることを第 2 の基準にするとします。この場合、Telnet のアクセス全体をブロックする第 2 のルール・セットを作成する必要があります。これらのルールに、セット名 `TelnetNever` を割り当てます。セット名を作成することにより、ルールの目的を区別しやすくなります。また、ある特定のセットに適用することを決めていたインターフェースを判別するのも容易になります。上記のヒントすべてを使用すると、フィルターの作成プロセスが容易になります。

IP フィルター・ルールを作成する方法については、パケット・ルール・エディターのオンライン・ヘルプにステップバイステップの指示が記載されています。

次のステップ

フィルターの作成が完了したら、フィルター・ステートメントに 1 つのファイルを組み込むか、あるいは複数のファイルを組み込むかを検討すべき場合があります。検討の必要がない場合、次のステップでは、ルールを適用するインターフェースを定義します。

IP フィルター・インターフェースの定義

システムがどのインターフェースにどのルールを適用するかを設定するには、フィルター・インターフェースを必ず 定義します。フィルター・インターフェースを定義する前に、システムがさまざまなインターフェースに対して適用するフィルターを作成する必要があります。アドレスの定義を選択した場合 (インターフェースの定義時)、インターフェースは名前で参照されます。アドレスの定義を選択しなかった 場合 (インターフェースの定義時)、インターフェースは IP アドレスで参照されます。

フィルターを作成する際に、1 つのセットに複数のフィルターを組み込むことができます。その後、そのセットを FILTER_INTERFACE ステートメントに追加します。このステートメントで使用するセット名は、フィルター・ステートメントで定義したセット名にする必要があります。たとえば、セット名 ALL があり、すべてのフィルターがこのセットに含まれる場合、フィルターを正しく作動させるためにはセット名 ALL をフィルター・インターフェース・ステートメントに組み込む必要があります。 1 つのセットに複数のフィルターを組み込むだけでなく、1 つの FILTER_INTERFACE ステートメントに複数のセットを組み込むこともできます。

インターフェースを定義する前に、使用する追加ファイルを組み込む必要があります。その後、インターフェースを定義することができます。フィルター・セットは、フィルター・インターフェース・ステートメントで指定された順序で適用されます。したがって、フィルター・ルールは、ファイル内にあるセットの物理的な定義と同じ順序で FILTER_INTERFACE ステートメントに表示されます。

フィルター・インターフェースを定義する方法については、パケット・ルール・エディターのオンライン・ヘルプにステップバイステップの指示が記載されています。

次のステップ

フィルター・インターフェースを定義したら、次のステップでは、パケット・ルールでコメントを作成します。

パケット・ルールへのファイルの組み込み

パケット・ルール・エディターの *Include* 機能を使用して、複数のパケット・ルール・ファイルをシステム上でアクティブにすることができます。複数のファイルを使用すると、ルールの作業が非常に簡単になります。特に、複数インターフェースでトラフィックを制御するのに非常に多くのルールが必要になる場合においては便利です。たとえば、あるルール・グループを複数のインターフェースで使用することができます。

このようなグループを、1 つのファイルの中に作成することができます。マスター・ファイルにルールを組み込めば、別のファイルでルールを使用するたびにルールを再作成しなくて済みます。マスター・ファイルは、任意の時間にアクティブにすることができる唯一のファイルです。マスター・ファイルにルールを追加するのに、この組み込み機能を使用するだけで済みます。

組み込みファイルを作成するときに、インターフェースのフィルター・ルールとは別に、インターフェースの NAT ルールを保持することができます。ただし、指定したときアクティブにできるファイルは 1 つだけです。

新規ルール・ファイルを作成すると、新規ファイルの一部として任意の既存ファイルを組み込むことができます。ただし、その前に、使用する新規フィルター・ルールを作成する必要があります。ルールを作成するときは、必ずタイプ別にルールをファイル (グループ化) します。こうすると、前に使用したルールを再作成する必要がなくなります。必要に応じて組み込んだり削除したりするだけです。

ルールにファイルを組み込む方法については、パケット・ルール・エディターのオンライン・ヘルプにステップバイステップの指示が記載されています。

次のステップ
使用する追加ルール・ファイルをすべて組み込んだら、次のステップでは、IP フィルター・インターフェースを定義します。

パケット・ルールでのコメントの作成

ルール・ファイルのコメントは非常に重要です。ルールをどのように使うかなどを記述します。たとえば、特定のルールによって許可または拒否する事項などを記録します。このようなタイプの情報は将来的には時間の節約につながります。セキュリティーの漏れをす早く解決する必要がある場合は、記憶を呼び起こすためのこれらのコメントが必要になります。ルールの意味を理解する時間がない場合は、コメントを十分に活用してください。

パケット・ルールの作成およびアクティブ化に関連するダイアログのそれぞれに、「**説明 (Description)**」フィールドが用意されています。これは、コメント用に予約されているフィールドです。システムでは、このフィールドに入力したものをすべて無視します。ルール作成プロセスの各ステップにある、コメント・フィールドを使用することもできます。これを使用すれば、重要なコメントを作成し忘れることが少なくなります。コメントを記述する処理が記憶に新しい内にコメントを作成することをお勧めします。ただし、すべてのルールを作成した後でコメントを作成することもできます。

ルール・ファイル内にコメントを作成する方法については、パケット・ルール・エディターのオンライン・ヘルプにステップバイステップの指示が記載されています。

次のステップ
このステップの前の『パケット・ルールの構成』の各ステップを終了したら、次のステップでは、パケット・ルールの保管および『パケット・ルールの検証』を行います。

パケット・ルールの検証

ルールは、必ず検証してからアクティブにしてください。それによって、何も問題を起こさずにルールをアクティブにすることができます。パケット・ルールを検証する際は、システムがそれらの構文エラーおよび意味エラーをチェックし、その結果をパケット・ルール・エディターの下部のメッセージ・ウィンドウで報告します。特定のファイルおよび行番号に関連するエラー・メッセージがあった場合、そのエラーを右マウス・ボタンでクリックして、「**行番号 (Go To Line)**」を選択すると、編集中のファイル内でそのエラーを強調表示にすることができます。

検証機能を使用する前に、パケット・ルールを表示してエラーを目視することができます。構文エラーのあるルールをアクティブにすることはできません。システムの検証機能によって、構文上のエラーがチェックされます。システムはルールの順序が正しいかどうかを検証できません。ルールの順序は手動で検査しなければなりません。パケット・ルールは順序が重要です。つまり、適用したい順序でルールを並べなければなりません。間違った順序で指定すると、期待した結果が得られません。ルールをアクティブにする前に、ルールが適用される順序で正しく指定されていることを確認してください。

パケット・ルールを検証する方法については、パケット・ルール・エディターのオンライン・ヘルプにステップバイステップの指示が記載されています。

警告メッセージ: フィルター・ルールをアクティブにするときは、常にシステムによって自動的にこれらのルールが検証されます。さまざまな警告メッセージおよびエラー・メッセージが表示されることがあります。警告メッセージは単に通知目的用であり、検証プロセスが停止されることはありません。すべてのメッセージを注意深く読んでください。検証またはアクティブ化が正常に行われたことを示すメッセージが表示されます。重大なエラーがあった場合、この最後に表示されるメッセージに、ルールのロードが失敗した旨が示されることもあります。

次のステップ
ルールを正常に検証し終えたら、次のステップでは、ルールをアクティブにします。

パケット・ルールのアクティブ化

作成したパケット・ルールのアクティブ化は、パケット・ルールの構成における最後のステップです。作成したルールを機能させるためには、それらのルールをアクティブにするか、あるいはロードしなければなりません。しかし、ルールをアクティブにする前に、ルールが正しいかどうかを検証する必要があります。常に、パケット・ルールをアクティブにする前に問題を解決するようにしてください。エラーのあるルールや順序の間違っているルールをアクティブにすると、システムの動作にリスクが発生します。システムには、ルールをアクティブにしたときに自動的に呼び出される検証機能があります。この自動検証機能では主要な構文エラーがチェックされるだけなので、これだけに依存することはできません。常に、手動でもルール・ファイルのエラーをチェックしてください。

フィルター・ルールがインターフェースに適用されていない場合 (たとえば、フィルター・ルールを使用せず NAT ルールのみを使用している場合)、警告 (TCP5AFC) が表示されます。これはエラーではありません。単に目的どおり 1 つのインターフェースを使用していることを検証するだけです。必ず最後のメッセージを参照してください。ここでアクティブ化が正常に行われたことを示していれば、上記のメッセージはすべて警告です。

注: すべてのインターフェースに対して新しいルールをアクティブにした場合、すべての物理インターフェースで以前のルールが新しいルールによって置き換えられます。新しいルールに物理インターフェースが記述されていない場合でも、置き換えられます。しかし、新しいルールを 1 つの特定のインターフェースに対してアクティブにするようにした場合は、その特定のインターフェースでのみ以前のルールが新しいルールに置き換えられます。その他のインターフェースの既存のルールは変更されません。

最終ステップ
パケット・ルールを構成し、正常にアクティブ化した後は、それらのルールを定期的に管理して、システムのセキュリティーを確実に維持する必要があります。パケット・ルールを正しく保守およびモニターするためのタスクのリストについては、このトピックの『パケット・ルールの管理』セクションを参照してください。

第 7 章 パケット・ルールの管理

システムのセキュリティーおよびパケット・ルールの保全性を保守するには、以下の管理タスクを定期的に実行する必要があります。

注: パケット・ルール・エディターのオンライン・ヘルプで、これらのタスクに関する特定的なステップバイステップの情報を見ることができます。

- ファイルの消失を保護するには、『パケット・ルールのバックアップ』を行う。
- 何らかの理由で NAT およびフィルター・ルールを停止する必要があるときは、『パケット・ルールの非アクティブ化』を行う。ただし、ルールを非アクティブにすると、ネットワークは保護されない状態になることに注意してください。
- 自社のシステムに入って来る、あるいは自社のシステムから出て行く、IP トラフィックの流れを変更する必要があるときは、『パケット・ルールの編集』を行う。
- パケット・ルールをログに記録するには、『パケット・ルールのアクションのジャーナルおよび監査』を行う。これは、ルールのデバッグが必要な場合に役立ちます。
- エラーのトラブルシューティングが必要なときは、『パケット・ルールの表示』を行う。

パケット・ルールを効率的かつ効果的に管理するために、可能な手段をすべて使用する必要があります。システムのセキュリティーは、現在のルールが正確かどうかに依存しています。トラブルシューティングで援助が必要な場合は、『パケット・ルールのトラブルシューティング』を参照してください。

パケット・ルールの非アクティブ化

アクティブにされたパケット・ルールを変更する必要がある場合、または新しいルールをアクティブにしたい場合は、まず最初に現在アクティブになっているルールを非アクティブにしなければなりません。特定のインターフェース、特定の Point-to-Point ID、またはすべてのインターフェースとすべての Point-to-Point ID のうち、いずれのルールを非アクティブにするか選ぶことができます。

パケット・ルールを非アクティブにする方法については、パケット・ルール・エディターのオンライン・ヘルプにステップバイステップの指示が記載されています。

パケット・ルールの表示

フィルター・ルールを表示してそれらが正しいことを検証してから、フィルター・ルールをアクティブにしてください。作成したフィルター・ルールを表示すると、目で見てわかるエラーをチェックすることができます。フィルター・ルールは、アクティブ化やテストの前だけでなく、印刷やバックアップの前に表示することもあります。エラー・チェックの方法は、ルールの表示だけではありません。しかし、テスト前にエラーを最小限に減らしたり、削除することは効果的な方法です。

作成したフィルター・ルールを出力して、確認できるようにします。こうすると、目で見てわかる誤りを検出し、前に作成したフィルター・ルール・ファイルをすべて組み込んだことを確認します。

またシステムには検証機能がありますが、この機能だけに依存しないでください。すべてのエラーを手作業で確実に訂正するための手段を実行する必要があります。こうすると、貴重な時間とリソースを節約できます。

非アクティブなルールを表示するには、パケット・ルール・エディターでルール・ファイルを開く必要があります。

アクティブなフィルター・ルールを編集したい場合は、まず最初にそれらのルールを表示して、どのように変更するのかを決定してください。

現在アクティブなルールを表示するには、次のステップに従ってください。

1. iSeries ナビゲーターで、「**ユーザーのサーバー (your server)**」-->「**ネットワーク (Network)**」-->「**IP ポリシー (IP policies)**」-->「**パケット・ルール (Packet rules)**」を選択する。
2. アクティブなパケット・ルールを表示したいインターフェースを選択する。
3. 右ペインで、アクティブなパケット・ルールのリストを表示する。

注: このダイアログではルールの編集はできません。ルール・ファイルを非アクティブにしてから、パケット・ルール・エディターを使用してルールを編集しなければなりません。

NAT と IP フィルターの管理に戻ります。

パケット・ルールの編集

ご使用のネットワークのセキュリティー要件が変更になったときは、ルールを編集して、新しいセキュリティー戦略に合わせなければなりません。しかし、アクティブなパケット・ルールを編集するには、最初にそのルールを非アクティブにしなければなりません。その後で、iSeries ナビゲーターのパケット・ルール・エディターを使用して、ルールに必要な変更を行います。ルールを編集し終えたら、必ずそれらのルールを検証してから、再びアクティブにしてください。

パケット・ルールを編集する方法については、パケット・ルール・エディターのオンライン・ヘルプにステップバイステップの指示が記載されています。

パケット・ルールのバックアップ

パケット・ルールのバックアップは、最初は必要ないように思えますが、常に必要なことです。失われた場合は、バックアップがあると、最初からファイルを再作成するための時間と作業を節約できます。

以下に、失ったファイルとの置き換えを容易にするための一般的なヒントを示します。

フィルター・ルールの印刷
最も安全で、必要に応じて情報を追加できる場所に出力を保管します。印刷出力は、フィルター・ルールのエラーを検索する必要がある場合にも便利です。

パケット・ルールを印刷する方法については、パケット・ルール・エディターのオンライン・ヘルプにステップバイステップの指示が記載されています。

ディスクへの情報のコピー
コピーは印刷出力よりも優れています。手動で追加しなくても情報が電子的に存在しているためです。これにより、1 つのオンライン・ソースから別のソースへ情報を直接移動することができます。

注: iSeries では、フロッピー・ディスクにではなく、システム・ディスクに情報がコピーされます。ルール・ファイルは、PC 上ではなく iSeries 上の IFS ファイル・システムに保管されます。システム・ディスクに保管されるデータの保護手段として、バックアップによるディスク保護を利用できます。

iSeries を使用する場合、バックアップおよび回復の戦略について計画を立てる必要があります。ファイルの回復およびバックアップの詳細については、「バックアップおよび回復の手引き」を参照してください。

パケット・ルールのアクションのジャーナルおよび監査

パケット・ルールには、ジャーナル処理機能が含まれます。ジャーナル処理により、NAT やフィルター操作の問題をトラブルシューティングできます。ジャーナルを使用して、ルールのアクションのログを作成できます。これにより、簡単にルールのデバッグやスポット・チェックを行うことができます。また、システム・ログまたはジャーナルを参照して、システムに出入りするトラフィックのフローを監査することができます。

ジャーナル処理機能は、1 ルールごとに使用されます。 NAT または フィルター・ルールを作成する場合、FULL または OFF のジャーナル・オプションを使用できます。詳細については、次の表を参照してください。

オプション	定義
FULL	転送された各パケットがログに記録されます。
OFF	ジャーナル処理は行われません。

ジャーナル処理がオンの場合、データグラムに適用されるルール (NAT またはフィルター) ごとに、ジャーナル・エントリーが生成されます。ジャーナル・エントリーが作成されない唯一のルールは、デフォルト拒否ルールです。このルールは、システムによって作成されるため、ジャーナルには記録されません。

これらのジャーナルを使用して、iSeries 上に汎用ファイルを作成します。そこで、システムのジャーナルに記録された情報を使用して、システムがどのように使用されているかを判別します。これは、セキュリティー計画上のさまざまな要素の変更を決定する助けとなります。

ジャーナル処理機能を「OFF」に設定すると、そのルールのジャーナル・エントリーは作成されません。このような選択をすることはできますが、最良の選択ではない場合もあります。フィルターおよび NAT ルールの作成について熟知していない場合は、必要に応じて FULL (ログ記録) を使用してください。これによって、ログをトラブルシューティング・ツールとして使用することができます。しかし、ジャーナル処理する内容を選択する必要があります。ジャーナル処理はシステムのリソースでかなり負荷がかかります。大量のトラフィックを制御するルールに焦点を合わせるようにしてください。

これらのジャーナルを表示するには、次のようにします。

1. iSeries 上のコマンド・プロンプトで、NAT ジャーナルの場合は DSPJRN JRN(QIPNAT)、IP フィルター・ジャーナルの場合は DSPJRN JRN(QIPFILTER) と入力します。

第 8 章 パケット・ルールのトラブルシューティング

このセクションでは、パケット・ルールの一般的な問題に対するトラブルシューティングに役立つ内容を提供します。

- **iSeries 通信トレース**機能を使用すると、特定のインターフェースのすべてのデータグラム・トラフィックを表示できるようになります。通信トレースの開始 (STRCMNTRC) および通信トレースの印刷 (PRTCMNTRC) コマンドを使用して、情報を収集し、印刷します。
- **NAT および IP フィルター・ルールの順序**では、ルールの処理方法が決定されます。ルールはファイルに現れる順序で処理されます。順序が正しくない場合、パケットは期待通りの処理を実行しないことがあります。こうすると、システムはハッキングに対して無防備になります。フィルター・セット名を、ファイルで物理的に定義されているのと全く同じ順序で FILTER_INTERFACE ステートメントに設定します。

  構文的に正しいフィルター・ルールを書き込むための詳細については、このトピックの『IP フィルター・ルールの作成』セクションを参照してください。次の表に示す処理に注意してください。

インバウンド・トラフィック処理	アウトバウンド・トラフィック処理
1. NAT ルール	1. IP フィルター・ルール
2. IP フィルター・ルール	2. NAT ルール

- **すべてのルールの削除**は、システムをリセットしてエラーを消去する最良の方法です。 iSeries 上で TCP/IP テーブルの削除 (RMVTCPTBL) コマンドを実行します。 iSeries ナビゲーター・アプリケーションからロックアウトしている場合も、このコマンドを使用して、ルールに戻って修正できます。

  注: VPN サーバーの開始もこの「TCP/IP テーブルの削除」コマンドによって行われます。ただし、VPN サーバー (IKE および ConMgr) が以前に稼働していた場合に限られます。
- NAT を使用している場合、iSeries 上の TCP/IP 構成で **IP データグラムの転送の許可**を行うことが不可欠です。TCP/IP 属性の変更 (CHGTCPA) コマンドを使用して、IP データグラムの転送が YES に設定されていることを確認します。
- **デフォルトの戻り経路の確認**では、マップしたか、背後に隠したアドレスが正しいことを確認します。このアドレスについては、iSeries への戻り経路を指定して、NAT によって変換されないように適切な回線を通過できるようになっていなければなりません。

  注: iSeries に複数のネットワークまたは回線が接続されている場合、インバウンド・トラフィックの経路指定には特に注意する必要があります。インバウンド・トラフィックはトラフィックが入る任意の回線で処理されますが、トラフィックを変換しない正しい回線でない場合があります。
- 期待どおりの順序でルールが並べられているか確認するために、EXPANDED.OUT ファイルを開いて**エラー・メッセージと警告メッセージを検証**します。フィルターのセットを検証してアクティブにすると、これらのフィルターは iSeries ナビゲーターによって生成されたルールとマージされます。この組み合わせによって、EXPANDED.OUT という新しいファイルに、マージされたルールが作成されます。このファイルは、ユーザーのルールの置かれているディレクトリーと同じディレクトリーに置かれます (通常は /QIBM)。警告メッセージとエラー・メッセージは、このファイルを参照します。このファイルを表示するには、パケット・ルール・エディターのから開く必要があります。
  1. iSeries ナビゲーターでパケット・ルール・エディターにアクセスする。
  2. 「**ファイル**」メニューから「**開く**」を選択する。
  3. ディレクトリー QIBM/UserData/OS400/TCPIP/PacketRules/、または、デフォルトと異なる場合はパケット・ルールを保管したディレクトリーに移動する。

4. 「**ファイルのオープン (Open file)**」ウィンドウから **EXPANDED.OUT ファイル**を選択する。EXPANDED.OUT ファイルが表示されます。
5. このファイルを選択し、「**開く (Open)**」をクリックします。

EXPANDED.OUT ファイルは、情報を提供する目的のものです。これを編集することはできません。

第 9 章 パケット・ルールの関連情報

下記に、IP フィルターと NAT に関する追加情報を提供する IBM マニュアルおよび Redbooks™ (PDF フォーマット) をリストします。

マニュアル

- 「**iSeries セキュリティーの手引き**」 (約 254 ページ)
  この PDF ブックは、iSeries を使用してどのようにセキュリティーを強化できるかについての高レベルな情報を提供します。

Redbooks

- 「**TCP/IP Tutorial and Technical Overview**」
  TCP/IP ネットワークに関連したセキュリティーの問題についての情報を提供します。

- 「**TCP/IP for AS/400: More Cool Things Than Ever**」
  NAT と IP パケット・フィルターの例を示すいくつかの実例が提供されています。

表示用または印刷用の PDF ファイルをワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF を右マウス・ボタンでクリックする (上記のリンクを右マウス・ボタンでクリックする)。
2. 「**リンクを名前を付けて保存**」(Netscape Navigator) または「**対象をファイルに保存**」(Internet Explorer) を選択する。
3. PDF を保存したいディレクトリーに進む。
4. 「**保存**」をクリックする。

これらの PDF を表示したり印刷したりするには、Adobe Acrobat Reader が必要です。これは、Adobe Web サイト (www.adobe.com/prodindex/acrobat/readstep.html) から、ダウンロードできます。

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12