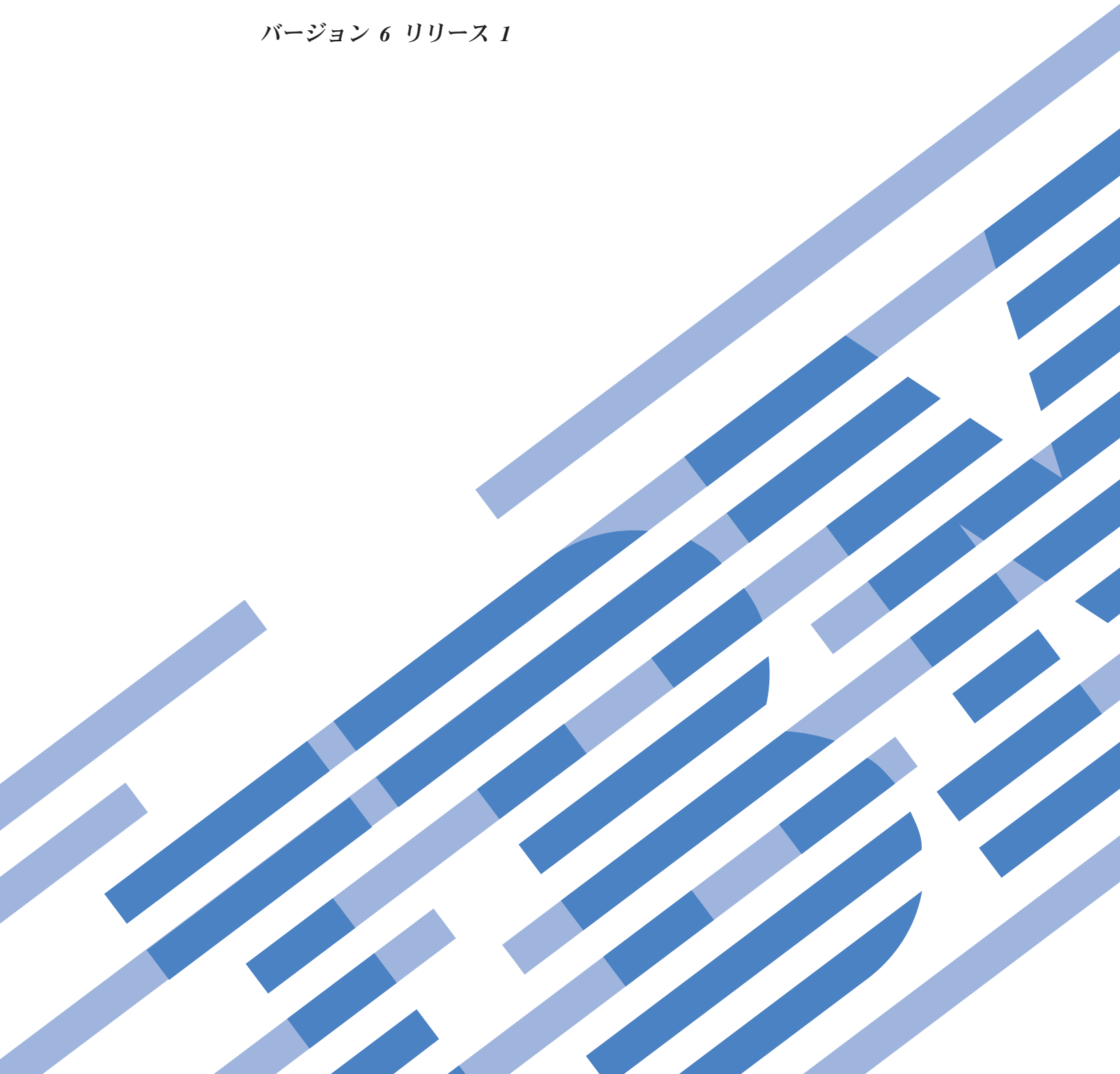
System i

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

バージョン 6 リリース 1



System i

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

バージョン 6 リリース 1

お願い

本書および本書で紹介する製品をご使用になる前に、 39 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM i5/OS (プロダクト番号 5761–SS1) のバージョン 6、リリース 1、モディフィケーション 0 に適用されます。また、改訂版で断りがない限り、それ以降のすべてのリリースおよびモディフィケーションにも適用されます。このバージョンは、すべての RISC モデルで稼働するとは限りません。また、CISC モデルでは稼働しません。

IBM 発行のマニュアルに関する情報のページ

http://www.ibm.com/jp/manuals/

こちらから、日本語版および英語版のオンライン・ライブラリーをご利用いただけます。また、マニュアルに関するご意見やご感想を、上記ページよりお送りください。今後の参考にさせていただきます。

(URL は、変更になる場合があります)

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原　典： System i
Networking
IP filtering and network address translation
Version 6 Release 1

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 2008.2

この文書では、平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財) 日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、平成角ゴシック体™W7

目次

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プライベート 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プライベート・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 を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、主題が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。

このトピックに含まれる情報の他に、System i™ 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。 System i ナビゲーターのオンライン・ヘルプには、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が記載されています。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。

注: コーディング例を使用すると、「コードに関するライセンス情報および特記事項」の条件に同意したものとみなされます。

IP フィルター操作とネットワーク・アドレス変換の PDF ファイル

本書の PDF ファイルを表示およびプリントすることができます。

PDF 版を表示またはダウンロードするには、「IP フィルター操作とネットワーク・アドレス変換 (NAT)」を選択します。

PDF ファイルの保管

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

1. ご使用のブラウザーで PDF リンクを右クリックする。
2. PDF をローカル上に保管するオプションをクリックする。
3. PDF を保管するディレクトリーを指定する。
4. 「**保管**」をクリックする。

Adobe Reader のダウンロード

これらの PDF を表示または印刷するには、Adobe® Reader がシステムにインストールされている必要があります。Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html) から、無償のコピーをダウンロードできます。

関連資料

37 ページの『IP フィルター操作とネットワーク・アドレス変換の関連情報』
IBM® Redbooks™ 資料には、IP フィルター操作およびネットワーク・アドレス変換に関するトピック集が記載されています。 PDF ファイルはいずれも表示または印刷することができます。

実例: パケット・ルール

ネットワーク・アドレス変換 (NAT) と IP フィルターを使用してネットワークを保護することができます。

各実例には図およびサンプル構成が含まれています。

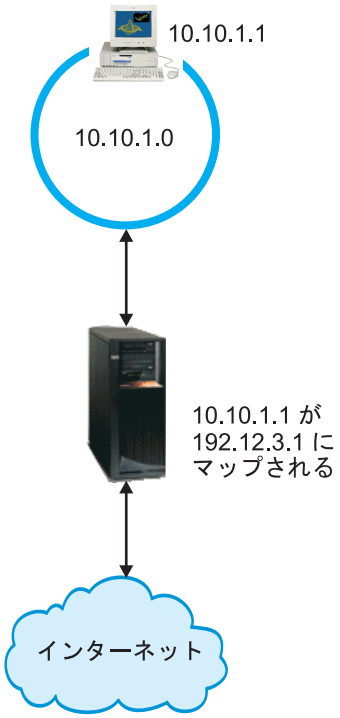
ヒント: 各実例の 192.*x*.*x*.*x* IP IP アドレスは、パブリック IP アドレスを表します。ここで使用されているアドレスは、すべて説明のためのものです。

実例: NAT の使用による IP アドレスのマップ

この実例で、ユーザーの会社は静的 NAT (Network Address Translation) を使用して、プライベート IP アドレスをパブリック・アドレスにマップしています。

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開始を決定したとします。しかし、パブリック 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。インターネットにアクセスしたところ、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。パブリック・ユーザーが、この 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 (プライベート) アドレスを 1 つの登録済み (パブリック) アドレスに割り当てます。システムは、この登録済みアドレスをプライベート・アドレスにマップします。登録済みアドレスによって、このプライベート・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、このパブリック・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、プライベート・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。例えば、12 のユーザーがいる場合は、12 個のプライベート・アドレスにマップする 12 個のパブリック IP アドレスが必要になります。

この例では、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 はアドレスをパーソナル・コンピューター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達することはありません。 (システムの外部からは) 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、実プライベート・アドレス 10.10.1.1 が実際の宛先です。

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、System i ナビゲーター の「**アドレス変換**」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。

- マップするプライベート・アドレス: 10.10.1.1
- そのプライベート・アドレスのマップ先となるパブリック・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. System i ナビゲーター で、「**ユーザーのシステム *(your system)***」 → 「**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、以下の例のようになります。

```
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
```

RZAJB507-0

これらのルールの作成を終了したら、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。

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。

関連概念

16 ページの『静的 (マップ) NAT』
静的 (マップ) ネットワーク・アドレス変換 (NAT) は、プライベート IP アドレスをパブリック 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、パブリック・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。

関連タスク

30 ページの『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。そのようにすれば、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。

31 ページの『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。

関連資料

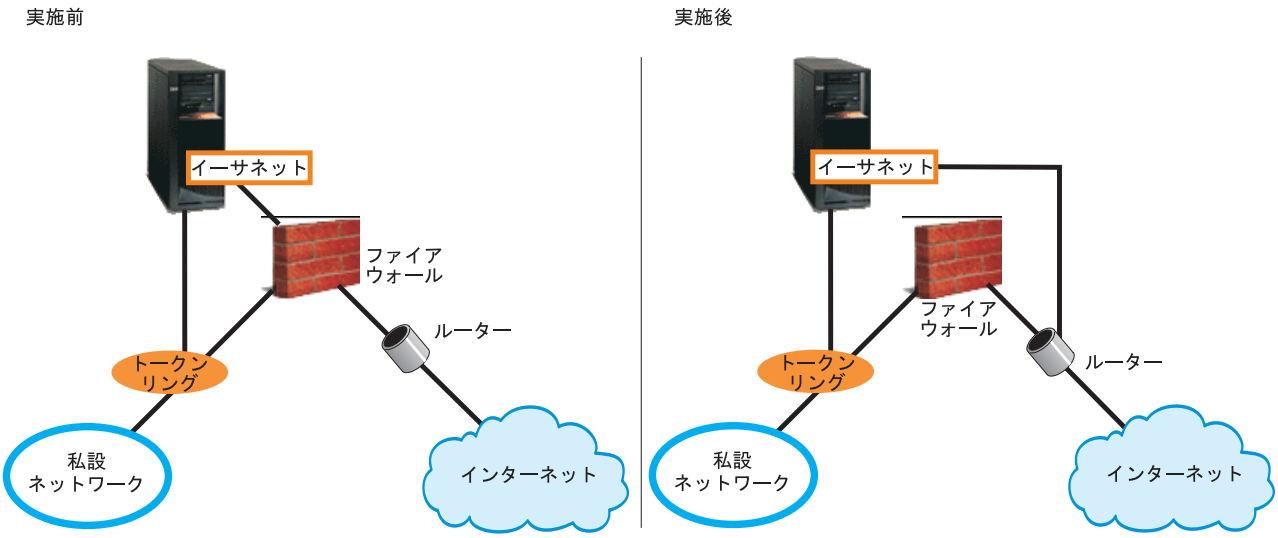
35 ページの『パケット・ルールのトラブルシューティング』
このトピックでは、パケット・ルールの一般的な問題に対するトラブルシューティングに役立つ内容を提供します。

実例: HTTP、Telnet、および FTP トラフィックを許可するフィルター・ルールの作成

この実例で、ユーザーの会社は、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 IP トラフィックを HTTP、Telnet、およびファイル転送プロトコル (FTP) のトラフィックのみに制限しています。

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、ファイアウォールはフルに稼動しているため、さらに負荷をかけたくないものとします。同僚は、ファイアウォール外でアプリケーションを実行するよう提案しています。しかし、ユーザーは、インターネットから該当の System i Web サーバーにアクセスできるのは、HTTP、FTP、および Telnet トラフィックにのみ限定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

IP フィルターを使用すると、該当の Web サーバーを通すことができる情報を定義するルールを設定できます。この実例では、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。サーバーのパブリック・アドレスは 192.54.5.1 で、プライベート 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、System i 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
- Web サーバーのパブリック・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. System i ナビゲーターで、「**ユーザーのシステム *(your system)***」 → 「**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、以下の例のようになります。

```
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
```

RZAJB508-0

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・ルールの作成を終了したら、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。

関連タスク

30 ページの『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。そのようにすれば、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。

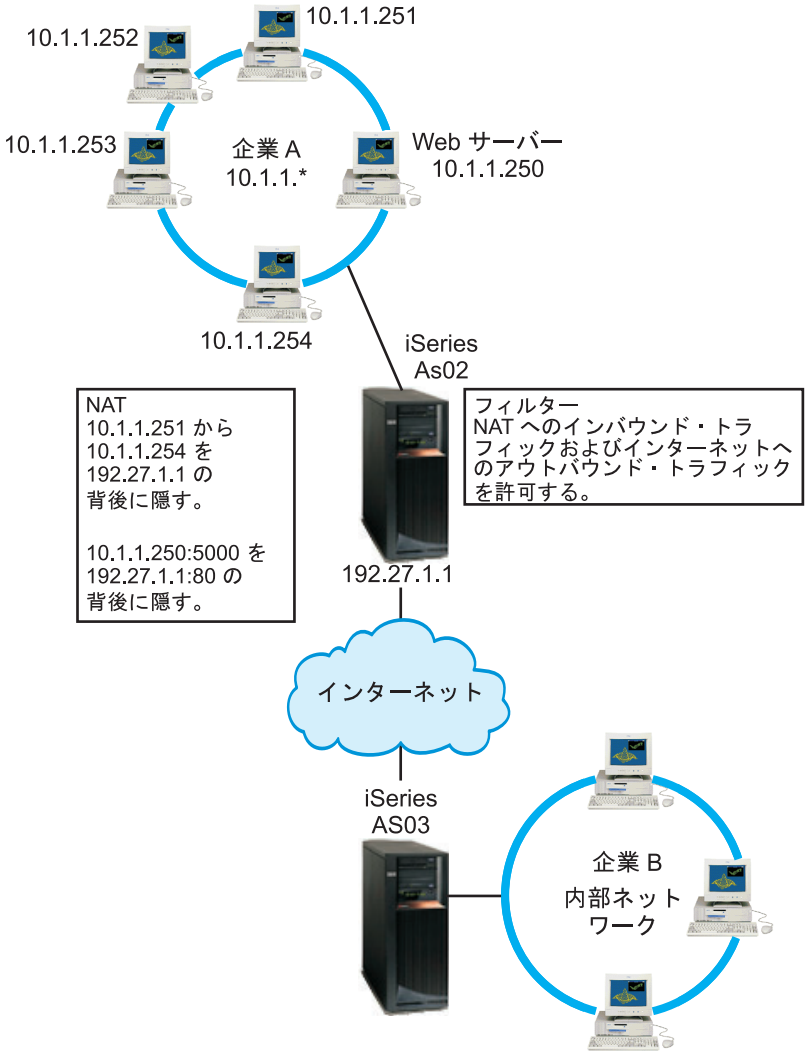
31 ページの『パケット・ルールのアクティブ化』
作成したパケット・ルールのアクティブ化は、パケット・ルールの構成における最後のステップです。

実例: NAT と IP フィルターの組み合わせ

この実例では、ユーザーの会社はネットワーク・アドレス変換 (NAT) と IP フィルターを組み合わせています。ユーザーの会社は、社内のパーソナル・コンピューターおよび Web サーバーを 1 つのパブリック IP アドレスの背後に隠しておいた上で、他の会社がこの Web サーバーにアクセスできるようにしようとしています。

状況

社内にゲートウェイとして System i モデル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・システムからそのゲートウェイの背後にある専用 Web 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。プライベートのパーソナル・コンピューターおよび Web サーバーのすべてを、System i インターフェース上のアドレス、すなわち、次の図の AS02 の後に隠したいとします。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、パーソナル・コンピューターと Web サーバーを次のように構成することができます。

- 隠蔽 NAT。社内のパーソナル・コンピューターをパブリック・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。
- ポート・マップ NAT。この Web サーバー・アドレス 10.1.1.250 およびポート番号 5000 を、パブリック・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 ルールでは、ポート 80 の外部から開始されたトラフィックについては、システムにアクセスすることだけが許可されています。外部から開始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。
- NAT を通じてこ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・ルールを構成するために、System i ナビゲーターの中で、アドレス変換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。

- 隠蔽するアドレスのセット: 10.1.1.251 から 10.1.1.254
- そのアドレス・セットを背後に隠蔽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. System i ナビゲーターで、「**ユーザーのシステム *(your system)*** 」 → 「**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 台のパーソナル・コンピューターをパブリック・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、以下の例のようになります。

```
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
```

RZAJB509-0

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. System i 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)**」フィールドに Web250 を入力する。
   c. 「**定義アドレス (Defined address)**」リストで「**IP アドレス**」を選択する。「**追加**」をクリックして、フィールドに Web サーバー 10.1.1.250 の IP アドレスを入力する。
   d. 「**OK**」をクリックする。
3. パブリック・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パブリック・アドレス 192.27.1.1 を表す定義アドレスを既に作成してあるので、この特定の実例ではこのステップを省略し、ステップ 4 にスキップす

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)**」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「**隠蔽 (Hide)**」を選択する。
   b. 「一般」ページの「**非公開アドレス名 (Hide address name)**」リストから「Web250」を選択する。
   c. 「**背後のアドレス名 (Behind address name)**」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、「**隠蔽ポート**」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)**」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、パブリック・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 ルールでは、ポート 80 の外部から開始されたトラフィックについては、このシステムにアクセスすることだけが許可されています。

ポート・マップ NAT ルールは、以下の例のようになります。

```
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. System i 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**」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**」リストから「**PERMIT**」を選択する。
   e. 「**方向 (Direction)**」リストから「**INBOUND**」を選択する。
   f. 「**ソース・アドレス名 (Source address name)**」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)**」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**」リストから「**TCP**」を選択する。
k. 「**ソース・ポート (Source port)**」リストから「**=**」および「*****」を選択する。
l. 「**宛先ポート (Destination port)**」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**」を選択する。
   d. 「一般」ページの「**セット名 (Set name)**」リストから「**external_rules**」を選択する。
   e. 「**処置**」リストから「**PERMIT**」を選択する。
   f. 「**方向 (Direction)**」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)**」リストから「**=**」および「*****」を選択する。
   i. 「**ジャーナル処理 (Journaling)**」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**」リストから「**TCP**」を選択する。
   l. 「**ソース・ポート (Source port)**」リストから「**=**」および「*****」を選択する。
   m. 「**宛先ポート (Destination port)**」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)**」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)**」リストから「**external_rules**」を選択して、「**追加 (Add)**」をクリックする。
   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した場合は、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 で外部から開始されたトラフィックについては、システム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、外部から開始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、以下の例のようになります。

```
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。

関連タスク

30 ページの『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。そのようにすれば、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。

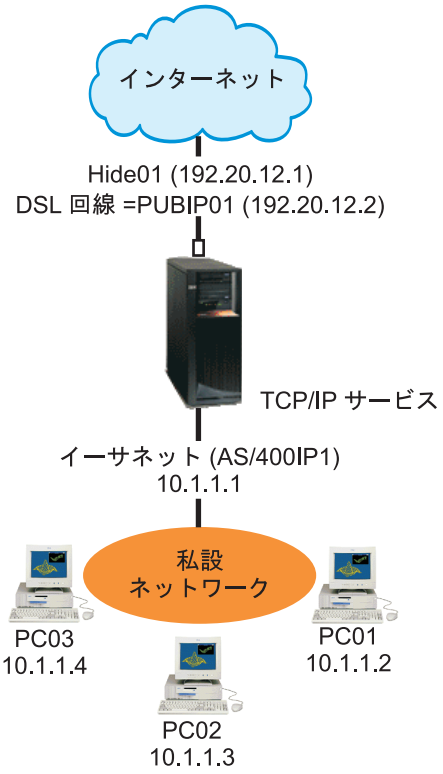
31 ページの『パケット・ルールのアクティブ化』
作成したパケット・ルールのアクティブ化は、パケット・ルールの構成における最後のステップです。

実例: マスカレード NAT の使用による IP アドレスの隠蔽

この実例では、ユーザーの会社がマスカレード・ネットワーク・アドレス変換 (NAT) を使用して、パーソナル・コンピューターのプライベート・アドレスを隠しています。同時に、ユーザーの会社は従業員がインターネットにアクセスできるようにしています。

状況

小規模な会社で、System i プラットフォーム上で 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・カードと 3 台のパーソナル・コンピューターを持つシステムがあるとします。インターネット・サービス・プロバイダー (ISP) からは、デジタル・サブスクライバー・ライン (DSL) 接続と DSL モデム 1 つが提供されています。また、ISP からパブリック 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。社内のパーソナル・コンピューターにはすべて、内部ネットワーク上でアドレス 10.1.1.x *x* が割り当てられています。社内のパーソナル・コンピューターのプライベート・アドレスを隠すようにして、外部ユーザーが内部ネットワークと通信を開始するのを防ぐ一方で、自社の従業員は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

社内のパーソナル・コンピューター・アドレス 10.1.1.1 から 10.1.1.4 を、パブリック・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) によって、ご使用のパーソナル・コンピューターは、ネットワーク外部から発信された通信から保護されます。しかし、範囲 NAT は System i インターフェースの保護はしません。ユーザーのシステムが希望しない情報を受信しないようにするために、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、System i ナビゲーターの「アドレス変換」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。

- 隠蔽するアドレスのセット: 10.1.1.1 から 10.1.1.4
- そのセットを背後に隠蔽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. System i ナビゲーターで、「**ユーザーのシステム *(your system)*** 」 → 「**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、以下の例のようになります。

```
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
```

RZAJB510-0

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。

関連概念

16 ページの『マスカレード (隠蔽) NAT』
マスカレード (隠蔽) NAT (Network Address Translation) を使用すると、プライベートのパーソナル・コンピューター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 NAT によってパーソナル・コンピューターからシステムに経路指定され、その結果、システムが基本的にパーソナル・コンピューターのゲートウェイになります。

関連タスク

30 ページの『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。そのようにすれば、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。

31 ページの『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。

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・ルールの両方からなります。これら 2 つのルールは、TCP/IP スタックの IP 層で実行され、通常の TCP/IP トラフィックで共通して関連付けられる潜在的な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・ルールの働きをよく理解するには、これらの概念を知り、それらがユーザーのシステムにどのように適用されるかを知る必要があります。

- パケット・ルールとその他の i5/OS® セキュリティー・ソリューション
- NAT

注: コーディング例を使用すると、「コードに関するライセンス情報および特記事項」の条件に同意したものとみなされます。

パケット・ルールの用語

ここでは、パケット・ルールに関連する、役に立つ用語を説明します。

ボーダー・アドレス

ボーダー・アドレスとは、トラステッド・ネットワークと非トラステッド・ネットワークとの境界

としての働きをするパブリック・アドレスのことです。これは、システム上で実際のインターフェースとして IP アドレスを記述するものです。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。例えば、パーソナル・コンピューターの IP アドレスはトラステッドですが、システムのパブリック IP アドレスはボーダー・アドレスです。

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、マスカレード・ネットワーク・アドレス変換 (NAT) フィルター・ルールの一部である、パラメーターです。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、この数を定義する必要があります。デフォルト値は 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)。
- パブリック (NAT) ソースの IP アドレスとパブリック (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。

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。デフォルト値は 16 です。

関連情報

シナリオ: グループ・ポリシーおよび IP フィルター処理を使用した、リソースへのリモート・ユーザーのアクセス管理

パケット・ルールとその他の i5/OS セキュリティー・ソリューション

実動システムを保護したり、ご使用の System i プラットフォーム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。

このシステムには、さまざまなリスクからシステムを保護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。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ています。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。

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。

- **System i およびインターネット・セキュリティー**

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。

- **『SSL (Secure Sockets Layer)』**

  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。このトピックには、i5/OS アプリケーションで SSL を使用可能にする方法が記載されています。

- **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、パブリック・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、さらにこのシステムでの使用法について述べます。

ネットワーク・アドレス変換

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。

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。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。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。

例 : 公の場から内部 IP アドレスを隠す

System i プラットフォームをパブリック Web サーバーとして構成するとします。しかし、システムの実際の内部 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、プライベート・アドレスをインターネットにアクセスできるパブリック・アドレスに変換することができます。この場合、システムの真のアドレスは隠されたままなので、システムは、アタックされにくくなっています。

例 : 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プライベート 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、パブリック IP アドレスを使用する必要があります。そこで NAT を使い、プライベート IP アドレスをパブリック 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 : 2 つの異なるネットワークの IP アドレスが互換性を持つようにする

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・システムとの通信を可能にしたいとします。しかし、両方のネットワークがプライベート・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。

関連資料

27 ページの『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、このシステムに入って来る、あるいはこの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。

静的 (マップ) NAT

静的 (マップ) ネットワーク・アドレス変換 (NAT) は、プライベート IP アドレスをパブリック 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、パブリック・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システムがあり、これに対してパブリック・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、実際のシステムのアドレスをパブリック・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。パブリック・アドレスは外部情報になります。これにより、システムへのアタックから、個人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。

- これは、1 対 1 のマッピングです。
- 外部および内部ネットワークによって開始することができます。
- マップまたは関連付けするアドレスは任意のアドレスにすることができます。
- マップまたは関連付けするアドレスは IP インターフェースとして使用できなくなります。
- ポート・マップ NAT は使用しないでください。

重要: パーソナル・コンピューターを System i プラットフォームの予約済みアドレスにマップするときは、よく注意して静的 NAT を使用してください。*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プライベート・アドレスに送信します。このインターフェースは NAT 用に予約されているので、このシステムおよびインターフェースは使用できなくなります。

関連概念

2 ページの『実例: NAT の使用による IP アドレスのマップ』
この実例で、ユーザーの会社は静的 NAT (Network Address Translation) を使用して、プライベート IP アドレスをパブリック・アドレスにマップしています。

マスカレード (隠蔽) NAT

マスカレード (隠蔽) NAT (Network Address Translation) を使用すると、プライベートのパーソナル・コンピューター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 NAT によってパーソナル・コンピューターからシステムに経路指定され、その結果、システムが基本的にパーソナル・コンピューターのゲートウェイになります。

マスカレード NAT を用いて、ユーザーは複数の IP アドレスを別の 1 つの IP アドレスに変換することができます。ユーザーは、マスカレード NAT を使用して、公開する IP アドレスの背後に 1 つ以上の内部ネットワーク IP アドレスを隠します。このパブリック・アドレスは、プライベート・アドレスを変換したアドレスと一致しており、しかも、システム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、対象のパブリック・アドレスを BORDER アドレスとして定義する必要があります。

複数のアドレスの隠蔽

複数のアドレスを隠すときは、NAT がシステムを介し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 サーバーは外部システムからの IP データグラムを変換なしで実行できます。

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 IP パケットが 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 つのパブリック 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。

- プライベート IP アドレスまたは一連のプライベート IP アドレスは、NAT ワークステーション上のパブリック IP アドレスの背後にバインドされます。
- マスカレード NAT は、内部ネットワークによってのみ開始することができます。
- 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 ワークステーショ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。

注:

この環境に合うパラメーターが設定されていないと、アドレス変換が予期通り機能しない場合があります。例えば、パケット内の IP アドレスが変換されなかったり、パケットが廃棄されたりする場合などです。ただし、これによりハードウェアあるいはシステムに損傷が生じることはありません。ユーザーがパラメーターの値を調整したい場合は、以下の項目を検討してください。

- 必要とされる会話の数が使用可能になるように、MAXCON の設定値を上げる必要があります。例えば、ファイル転送プロトコル (FTP) を使用している場合は、パーソナル・コンピューターでは 2 つの会話がアクティブになります。この場合、パーソナル・コンピューターごとに複数の会話が使用可能になるように、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。デフォルト値は、128 です。
- パーソナル・コンピューターとサーバーの間の会話が終了するまでに必要な時間を十分確保するために、 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。デフォルト値は、16 です。
- マスカレード NAT は、TCP、ユーザー・データグラム・プロトコル (UDP)、および Internet Control Message Protocol (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。

関連概念

20 ページの『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。

11 ページの『実例: マスカレード NAT の使用による IP アドレスの隠蔽』
この実例では、ユーザーの会社がマスカレード・ネットワーク・アドレス変換 (NAT) を使用して、パーソナル・コンピューターのプライベート・アドレスを隠しています。同時に、ユーザーの会社は従業員がインターネットにアクセスできるようにしています。

マスカレード (ポート・マップ) NAT

ポート・マップ NAT (Network Address Translation) はマスカレード NAT の一種です。

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、内部パーソナル・コンピューターと外部ワークステーションの両方から IP トラフィックを開始できます。外部ワークステーション (またはクライアント) がネットワーク内部のワークステーションまたはシステムにアクセスする場合に、ポート・マップ NAT を使用することができます。 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。

内部からの開始

アドレス 1: ポート 1 の内部パーソナル・コンピューターが、外部ワークステーションへのトラフィックを開始すると、変換コードは、*アドレス 1: ポート 1* について NAT ルール・ファイルを検査します。ソース IP 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 ルールに一致している場合は、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

外部ワークステーションは*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関係なく、データグラムを変換しません。つまり、NAT は会話が既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。

- マスカレード・ポート・マップ NAT は、1 対 1 の関係です。
- マスカレード・ポート・マップ NAT は、外部と内部の両方のネットワークから開始することができます。
- プライベート・アドレスを背後に隠している登録済みアドレスを、NAT 操作を実行している System i プラットフォーム上で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。
- 一般に、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。例えば、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、このポートをパブリック 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。

注記:

- 必要とされる会話の数が使用可能になるように、MAXCON の設定値を上げる必要があります。例えば、ファイル転送プロトコル (FTP) を使用している場合は、パーソナル・コンピューターでは 2 つの会話がアクティブになります。パーソナル・コンピューターごとに複数の会話が使用可能になるように、MAXCON の設定値を上げる必要があります。デフォルト値は 128 です。
- マスカレード NAT は、TCP、ユーザー・データグラム・プロトコル (UDP)、および Internet Control Message Protocol (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たり、そこから出て行ったりするための 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って、システムを保護します。

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るものであり、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。

- PERMIT - パケットの通常どおりの処理を許可する
- DENY - 即時にパケットを廃棄する
- IPSEC - 仮想プライベート・ネットワーク (VPN) 接続を介して、フィルター・ルールで指定したパケットを送信する

注: この場合、IP セキュリティー・プロトコル (IPSec) は、ユーザーがフィルター・ルールで定義できるアクションです。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。

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。

関連情報

仮想私設ネットワーク (VPN)

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、自社のシステムで、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する際に、1 つのフィルター・ステートメントだけでは効果はありません。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。 System i プラットフォームを構成する場合に使用するインターフェースにルールを適用する際には、自分自身のワークステーションを許可するか、またはSystem i プラットフォームに接続するシステム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、システムとの通信が失われてしまいます。

また、以下の例のように、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、セット 3 の順) で処理されます。各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。フィルターの順序が問題になるのは、フィルターが同じセット内にあるときだけです。

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

例えば、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。このルールは、*デフォルト拒否ルール* と呼ばれます。

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、System i 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、またはアウトバウンド・トラフィックのどちらを許可するかには関係なく、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。

関連概念

16 ページの『マスカレード (隠蔽) NAT』
マスカレード (隠蔽) NAT (Network Address Translation) を使用すると、プライベートのパーソナル・コンピューター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 NAT によってパーソナル・コンピューターからシステムに経路指定され、その結果、システムが基本的にパーソナル・コンピューターのゲートウェイになります。

IP フィルター・ルールを併用した NAT ルールの編成

ネットワーク・アドレス変換 (NAT) と IP フィルターは、お互いに独立して作動しますが、IP フィルター操作と NAT を同時に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・ルール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。例えば、フィルター・ルール用にファイル A を、NAT ルール用にファイル 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。

関連タスク

29 ページの『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**組み込み**機能を使用すると、ご使用のシステムで複数のパケット・ルール・ファイルをアクティブにすることができます。

複数の IP フィルター・ルールの編成

フィルター・ルールを作成する場合、1 つのルール・ステートメントが参照されます。フィルター・ルールのグループのことをセットと呼びます。1 つのセット内のフィルターは、物理的な順序に従って上位から下位へと処理されます。複数のセットは、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。

以下の例では、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。一般に、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。

注: コーディング例を使用すると、「コードに関するライセンス情報および特記事項」の条件に同意したものとみなされます。

```
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・システムの中にい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。パブリック・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。

System i 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、パブリック (非トラステッド) ネットワークにあるシステムは、プライベート (トラステッド) ネットワークにあるトラステッド・ワークステーションとして働くことはできなくなります。

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、発生しうるセキュリティー上のリスクを理解しておいてください。

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

一要件を正確に評価することができます。『 System i および インターネット・セキュリティー』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。

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。

関連タスク

24 ページの『パケット・ルールの構成』
このチェックリストには、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が記載されています。

パケット・ルール: ユーザー権限要件

ご使用のSystem i プラットフォームで、パケット・ルールを管理できるようにするときは、必要なアクセス権限を持っていることを前もって確認してください。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る場合、あるいは *ALLOBJ 権限を持っている場合は、正しい権限を持っています。正しいユーザー ID または *ALLOBJ 権限を持っていない場合は、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フォルト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

システムが、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を満たしているかどうかを確認します。

このシステム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製品が必要です。

- OS/400® V5R2, i5/OS V5R3、またはそれ以降のもの。
- IBM System i Access for Windows® (5761-XE1) および System i ナビゲーター。
  - System i ナビゲーターのネットワーク・コンポーネント。
- IBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1) には、IP インターフェース、ルート、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する必要があります。

関連情報

TCP/IP チュートリアルおよびテクニカルな概説

V4 TCP/IP for AS/400: More Cool Things Than Ever

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ることができます。

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 (例えば、HTTP、ファイル転送プロトコル (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。)	

パケット・ルールの構成

このチェックリストには、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が記載されています。

パケット・ルール・エディターのオンライン・ヘルプで、特定の情報を見ることができます。

ご使用のシステムに関してパケット・ルールの計画を作成したあとで、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・エディターにアクセスする。System i ナビゲーター内でパケット・ルール・エディターにアクセスには、以下の指示にしたがってください。

__ 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 またはユーザー・データグラム・プロトコル (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のみこのサーバーに入ってくるはずのトラフィックはすべて拒否するような、パケット・ルール・ステートメントのセットを生成して挿入します。

- **「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、必要とされるフィルターおよびネットワーク・アドレス変換 (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。

__ 複数のルールを作成する計画を立てる対象のアドレスおよびサービスの別名を作成することにより、アドレスとサービスを定義します。

注: NAT ルールを作成する場合は、必ずアドレスを定義してください。

__ NAT ルールの作成。このタスクは、NAT の使用を計画している場合にのみ実行します。

__ 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するためのフィルター・ルールを作成します。

__ 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。

__ ユーザーのルールを適用することにより、インターフェースを定義します。

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

__ ルール・ファイルを検査して、エラーや問題を起こさずに、ルールをアクティブにできることを確認します。

__ ルール・ファイルをアクティブにします。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。

__ パケット・ルールの管理。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。

関連タスク

22 ページの『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、発生しうるセキュリティー上のリスクを理解しておいてください。

32 ページの『パケット・ルールの管理』
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、ルールが正確で、現行のものであるかどうかに依存しています。

パケット・ルール・エディターへのアクセス

システムでパケット・ルールの作成を開始するために、パケット・ルール・エディターを使用することができます。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。

System i 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必要があります。

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. System i ナビゲーター で、「**ユーザーのシステム *(your system)***」 → 「**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。

これらの各タスクを完了する方法の説明については、オンライン・ヘルプを使用してください。

関連資料

35 ページの『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。

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、サブネット、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、次の利点があります。

- タイプミスのリスクを最小限にできる。
- 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。

例えば、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。

- 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。
- 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、ユーザー・データグラム・プロトコル (UDP)、および Internet Control Message Protocol (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。

要確認: ネットワーク・アドレス変換 (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・ヘルプに指示が記載されています。

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。

関連タスク

30 ページの『パケット・ルールへのコメントの追加』
ルール・ファイルに関するコメントを追加することによって、ルールをどのように使うかを記録することができます。

NAT ルールの作成

ネットワーク・アドレス変換 (NAT) を使用する場合に、使用する IP アドレスにニックネームを定義しておく必要があります。

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、名前を用いて 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 ルールを作成することができます。一方のタイプはアドレスを隠すことができるのに対して、もう一方のタイプはアドレスをマップすることができます。

アドレスの隠蔽

プライベート・アドレスをパブリックに表示しないようにするために、アドレスを隠します。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 つのパブリック IP アドレスの蔭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。

アドレスのマッピング

1 つのパブリック 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には、アドレスをマップします。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・ヘルプに指示が記載されています。

次のトピック

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、 30 ページの『パケット・ルールへのコメントの追加』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、このシステムに入って来る、あるいはこの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。

ユーザーが定義するルールによって、システムにアクセスを試みるパケットを許可するか拒否するかが指定されます。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。

重要: System i プラットフォーム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には、自分自身のワークステーションを許可するか、またはシステム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になります。これを行なわないと、システム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ときは、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) を使用してシステム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判断する必要があります。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ために使用できる、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。例えば、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、パケットがユーザーの意図する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、以下のようなオプションのアクションを検討します。
  - 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まったく同じ順序で FILTER_INTERFACE ステートメントに設定します。
  - 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。以下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・ルールだけを書き込みます。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:

上記のセット名作成の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意図している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・ヘルプに指示が記載されています。

フィルターの作成が完了したら、フィルター・ステートメントへのパケット・ルールによるファイルの組み込みを検討します。検討の必要がない場合、次のステップとして、ルールが適用される 『IP フィルター・インターフェースの定義』に進みます。

関連概念

15 ページの『ネットワーク・アドレス変換』
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。

関連資料

35 ページの『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。

IP フィルター・インターフェースの定義

フィルター・インターフェースを定義して、システムが各インターフェースに適用するフィルター・ルールを設定することができます。

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。例えば、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・ヘルプに指示が記載されています。

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**組み込み**機能を使用すると、ご使用のシステムで複数のパケット・ルール・ファイルを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。例えば、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。このようにすると、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・ヘルプに指示が記載されています。

関連概念

21 ページの『IP フィルター・ルールを併用した NAT ルールの編成』
ネットワーク・アドレス変換 (NAT) と IP フィルターは、お互いに独立して作動しますが、IP フィルター操作と NAT を同時に使用することができます。

パケット・ルールへのコメントの追加

ルール・ファイルに関するコメントを追加することによって、ルールをどのように使うかを記録することができます。

例えば、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。セキュリティーの問題を解決する必要がある場合は、ルールの適用方法を説明するコメントが必要です。ルールの意味をあとでじっくり解釈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・ヘルプに指示が記載されています。

関連タスク

26 ページの『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。

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。そのようにすれば、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検証はできません。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。

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・ヘルプに指示が記載されています。

関連概念

2 ページの『実例: NAT の使用による IP アドレスのマップ』
この実例で、ユーザーの会社は静的 NAT (Network Address Translation) を使用して、プライベート IP アドレスをパブリック・アドレスにマップしています。

4 ページの『実例: HTTP、Telnet、および FTP トラフィックを許可するフィルター・ルールの作成』
この実例で、ユーザーの会社は、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 IP トラフィックを HTTP、Telnet、およびファイル転送プロトコル (FTP) のトラフィックのみに制限しています。

6 ページの『実例: NAT と IP フィルターの組み合わせ』
この実例では、ユーザーの会社はネットワーク・アドレス変換 (NAT) と IP フィルターを組み合わせています。ユーザーの会社は、社内のパーソナル・コンピューターおよび Web サーバーを 1 つのパブリック IP アドレスの背後に隠しておいた上で、他の会社がこの Web サーバーにアクセスできるようにしようとしています。

11 ページの『実例: マスカレード NAT の使用による IP アドレスの隠蔽』
この実例では、ユーザーの会社がマスカレード・ネットワーク・アドレス変換 (NAT) を使用して、パーソナル・コンピューターのプライベート・アドレスを隠しています。同時に、ユーザーの会社は従業員がインターネットにアクセスできるようにしています。

関連タスク

33 ページの『パケット・ルールの表示』
フィルター・ルールをアクティブにする前に、そのルールが正しいかどうか検証する必要があります。

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、あるいはロードする必要があります。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検証する必要があります。パケット・ルールをアクティブにする前に、必ず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、ルール・ファイルのエラーを手動でも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 (例えば、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。

1 つのインターフェースを使用するだけでよいのかを確認しているだけです。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が示されていれば、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すると、すべての物理インターフェースについて、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。

パケット・ルールを構成し、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。

関連概念

2 ページの『実例: NAT の使用による IP アドレスのマップ』
この実例で、ユーザーの会社は静的 NAT (Network Address Translation) を使用して、プライベート IP アドレスをパブリック・アドレスにマップしています。

4 ページの『実例: HTTP、Telnet、および FTP トラフィックを許可するフィルター・ルールの作成』
この実例で、ユーザーの会社は、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 IP トラフィックを HTTP、Telnet、およびファイル転送プロトコル (FTP) のトラフィックのみに制限しています。

6 ページの『実例: NAT と IP フィルターの組み合わせ』
この実例では、ユーザーの会社はネットワーク・アドレス変換 (NAT) と IP フィルターを組み合わせています。ユーザーの会社は、社内のパーソナル・コンピューターおよび Web サーバーを 1 つのパブリック IP アドレスの背後に隠しておいた上で、他の会社がこの Web サーバーにアクセスできるようにしようとしています。

11 ページの『実例: マスカレード NAT の使用による IP アドレスの隠蔽』
この実例では、ユーザーの会社がマスカレード・ネットワーク・アドレス変換 (NAT) を使用して、パーソナル・コンピューターのプライベート・アドレスを隠しています。同時に、ユーザーの会社は従業員がインターネットにアクセスできるようにしています。

関連タスク

『パケット・ルールの管理』
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、ルールが正確で、現行のものであるかどうかに依存しています。

パケット・ルールの管理

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、ルールが正確で、現行のものであるかどうかに依存しています。

注: パケット・ルール・エディターのオンライン・ヘルプで (別の注記がない限り)、これらのタスクに固有の情報を見ることができます。

関連タスク

24 ページの『パケット・ルールの構成』
このチェックリストには、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が記載されています。

31 ページの『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。

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・ルールをアクティブにする前に、そのルールが正しいかどうか検証する必要があります。

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・ルールを印刷出力して、確認することができます。このようにすると、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できます。

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。その結果、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. System i ナビゲーターで、「**ユーザーのシステム *(your system)***」 → 「**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: このダイアログ中からルールを編集することはできません。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。

関連タスク

30 ページの『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。そのようにすれば、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。

34 ページの『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。

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。そのあとで、System i 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・ヘルプに指示が記載されています。

関連タスク

33 ページの『パケット・ルールの表示』
フィルター・ルールをアクティブにする前に、そのルールが正しいかどうか検証する必要があります。

パケット・ルールのバックアップ

作成したパケット・ルール・ファイルをバックアップしておくことによって、損失の事態に至った場合に作成し直す時間と手間を省くことができます。

失われ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以下に示します。

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印刷出力を保管します。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: システムでは、ディスケットにではなく、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、パーソナル・コンピューター上ではなく、System i プラットフォーム上の統合ファイル・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の手法を利用できます。

System i プラットフォームを使用する場合は、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。

関連情報


システムのバックアップ

パケット・ルールによるパケット・ルールのアクションのジャーナル処理および監査

このパケット・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、それぞれのパケット・ルールで起こるルール・アクションのログを作成することができます。これにより、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	変換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、システム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. コマンド行に、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。

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。

- **i5/OS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) コマンドおよび 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。このような場合、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まったく同じ順序で FILTER_INTERFACE ステートメントに設定します。

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。 i5/OS の場合は、「TCP/IP テーブルの削除 (Remove TCP/IP Table - RMVTCPTBL)」コマンドを実行します。System i ナビゲーターの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: 仮想プライベート・ネットワーク (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は、そのシステムの 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、システムへの戻り経路を指定して、ネットワーク・アドレス変換 (NAT) によって変換されないよう、適切な回線を通るようになっていなければなりません。

  注: System i プラットフォーム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ってくる任意の回線で処理されますが、それ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。
- 意図したと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**する必要があります。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、System i ナビゲーターで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 (一般に /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、次のステップを完了してパケット・ルール・エディターからこのファイルを開く必要があります。
  1. System i 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. EXPANDED.OUT ファイルを選択し、「**開く (Open)**」をクリックする。

  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。

関連概念

2 ページの『実例: NAT の使用による IP アドレスのマップ』
この実例で、ユーザーの会社は静的 NAT (Network Address Translation) を使用して、プライベート IP アドレスをパブリック・アドレスにマップしています。

関連タスク

25 ページの『パケット・ルール・エディターへのアクセス』
システムでパケット・ルールの作成を開始するために、パケット・ルール・エディターを使用することができます。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。

関連資料

27 ページの『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、このシステムに入って来る、あるいはこの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。

IP フィルター操作とネットワーク・アドレス変換の関連情報

IBM Redbooks 資料には、IP フィルター操作およびネットワーク・アドレス変換に関するトピック集が記載されています。 PDF ファイルはいずれも表示または印刷することができます。

IBM 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。

- **V4 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。

  関連資料

  1 ページの『IP フィルター操作とネットワーク・アドレス変換の PDF ファイル』
  本書の PDF ファイルを表示およびプリントすることができます。

コードに関するライセンス情報および特記事項

IBM は、お客様に、すべてのプログラム・コードのサンプルを使用することができる非独占的な著作使用権を許諾します。お客様は、このサンプル・コードから、お客様独自の特別のニーズに合わせた類似のプログラムを作成することができます。

強行法規で除外を禁止されている場合を除き、IBM、そのプログラム開発者、および供給者は「プログラム」および「プログラム」に対する技術的サポートがある場合にはその技術的サポートについて、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。

いかなる場合においても、IBM および IBM のサプライヤーならびに IBM ビジネス・パートナーは、その予見の有無を問わず発生した以下のものについて賠償責任を負いません。

1. データの喪失、または損傷。
2. 直接損害、特別損害、付随的損害、間接損害、または経済上の結果的損害
3. 逸失した利益、ビジネス上の収益、あるいは節約すべかりし費用

国または地域によっては、法律の強行規定により、上記の責任の制限が適用されない場合があります。

付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-8711
東京都港区六本木 3-2-12
IBM World Trade Asia Corporation
Intellectual Property Law & Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、IBM 機械コードのご使用条件、またはそれと同等の条項に基づいて、 IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年). このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. _年を入れる_. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

プログラミング・インターフェース情報

本書「IP フィルター操作とネットワーク・アドレス変換 (NAT)」には、プログラムを作成するユーザーが IBM i5/OS のサービスを使用するためのプログラミング・インターフェースが記述されています。

商標

以下は、IBM Corporation の商標です。

AS/400
i5/OS
IBM
IBM (ロゴ)

OS/400
Redbooks
System i

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

Microsoft、Windows、および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

個人使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。 ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

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