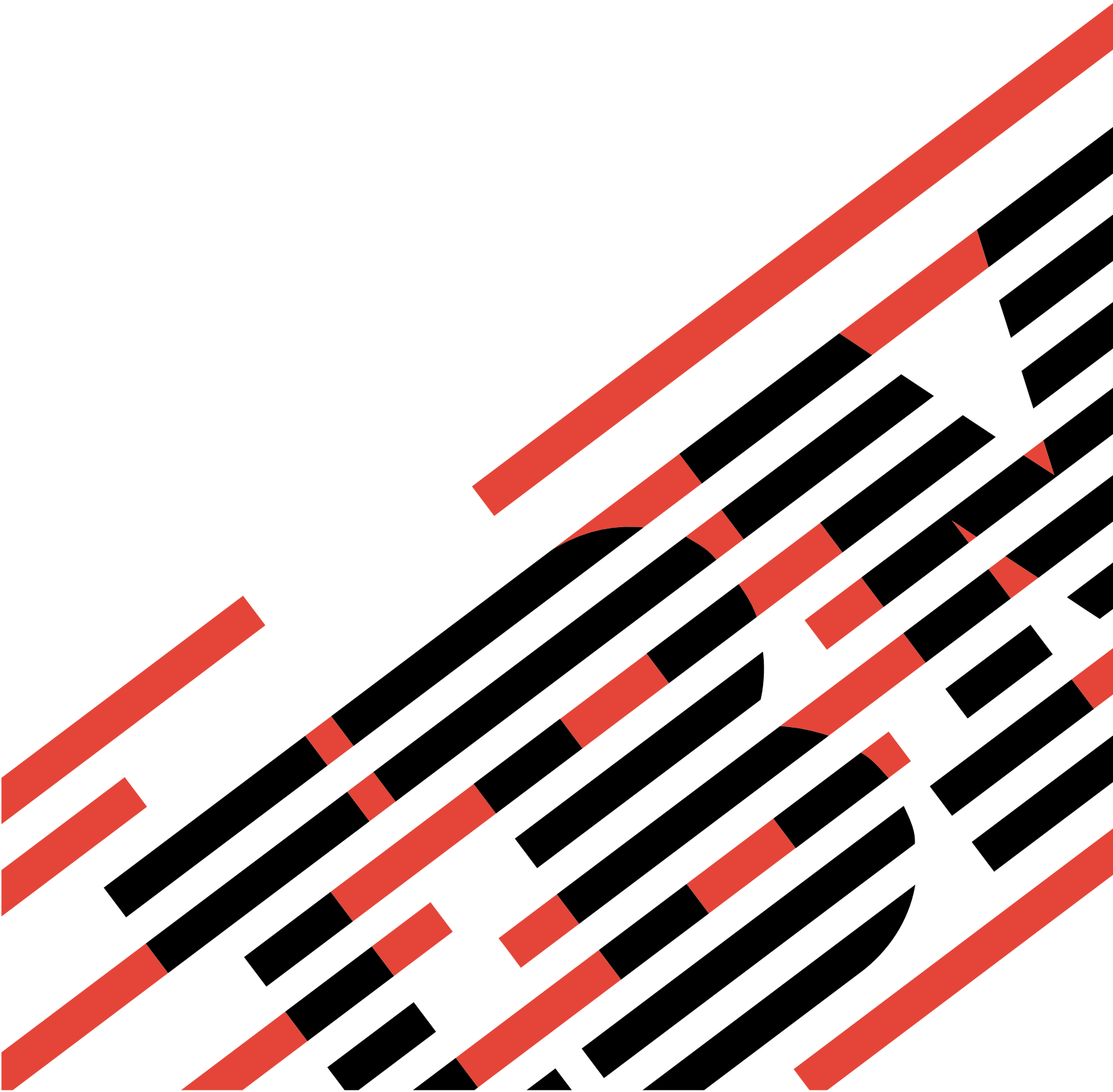
IBM

eserver

iSeries

IP 필터링 및 네트워크 주소 변환(NAT) 네트워크 보안



IBM

@server

iSeries

IP 필터링 및 네트워크 주소 변환(NAT) 네트워크 보안

목차

제 1 부 IP 필터링 및 네트워크 주소 변환(NAT)

IP 필터링과 네트워크 주소 변환(NAT)은 방화벽처럼 침입자로부터 사설망을 보호합니다. IP 필터링을 통해 사설망에 대해 허용할 IP 통신을 제어할 수 있습니다. 기본적으로 IP 필터링은 정의하는 규칙에 따라 패킷을 필터링함으로써 사설망을 보호합니다. 한편 NAT는 등록되지 않은 사설 IP 주소를 등록된 IP 주소 세트 뒤에 숨길 수 있도록 합니다. 이는 외부 네트워크로부터 사설망을 보호하는데 도움이 됩니다. NAT는 또한 다수의 사설 주소를 작은 세트의 등록된 주소로 나타낼 수 있으므로 IP 주소 디플리션 문제점을 줄이는데 도움이 됩니다.

주: **패킷 규칙**은 IP 필터링과 NAT의 조합입니다. 이 주제에서 사용되는 패킷 규칙이라는 용어는 IP 필터링 및 NAT 둘 모두에 적용됩니다.

아래의 주제는 패킷 규칙의 개념, 용도 및 사용 방법을 이해하는데 도움이 됩니다.

V5R2의 새로운 사항
V5R2 패킷 규칙에서의 변경 및 개선점을 설명합니다.

이 주제 인쇄
이 정보의 하드카피 버전을 원하는 경우에는 여기로 가서 PDF를 인쇄하십시오.

패킷 규칙 시나리오
패킷 규칙의 보다 일반적인 사용에 대해 친숙해지려면 이러한 시나리오를 검토하십시오. 각 시나리오에서는 일러스트레이션 및 샘플 구성을 제공합니다.

패킷 규칙 개념
시작하기 전에 적어도 패킷 규칙 기술 및 개념에 대한 기본 지식이 있어야 합니다. 이 주제에서는 IP 필터링 및 NAT에 대한 정보를 제공합니다. 여기에는 주소 맵핑 및 주소 숨기기와 같은 주제가 포함됩니다. 또한, iSeries™ 고유 전문 용어의 목록도 포함됩니다.

패킷 규칙 계획
계획은 보호해야 할 자원과 자원 사용을 제한해야 할 사람들을 결정하는 데 있어서 매우 중요합니다. 이 주제에서는 특별한 보안 요구사항에 가장 적합한 것을 결정하는데 도움이 되는 계획 작업용지 및 기타 정보를 제공합니다.

패킷 규칙 구성
이 주제에서는 패킷 규칙에 대해 수행 가능한 작업 및 수행 방법에 대한 정보를 제공합니다.

패킷 규칙 관리
이 주제에서는 패킷 규칙을 관리하기 위해 수행할 수 있는 다양한 타스크에 대해 설명합니다. 일부 피처에는 규칙 파일의 저널링, 편집 및 보기가 포함됩니다.

패킷 규칙 문제 해결
오류가 발생하거나 잠재적으로 문제가 발생할 수 있는 부분이 있을 때 문제를 해결하려면 이 주제를 참조하십시오.

패킷 규칙 관련 정보
다른 패킷 규칙 정보 소스 및 관련 주제로의 링크를 참조하려면 여기로 가십시오.

이 주제에 들어 있는 정보와 함께 iSeries Navigator의 패킷 규칙 편집기에서 사용할 수 있는 온라인 도움말을 사용하십시오. iSeries Navigator 온라인 도움말에서는 **방법**도움말, **수행** 도움말 및 광범위한 문맥 도움말을 비롯하여 패킷 규칙을 최대한 활용하기 위한 추가 정보 및 기술을 제공합니다.

제 1 장 V5R2의 새로운 사항

향상된 V5R2 패킷 규칙 기능에는 다음이 포함됩니다.

- **패킷 규칙 편집기**
  새롭고 사용하기 쉬운 패킷 규칙 편집기는 마법사 및 등록 정보 페이지를 사용하여 패킷 규칙을 작성 및 수정할 수 있도록 합니다.
- **새 마법사**
  구성하고자 하는 규칙 유형에 따른 세 개의 새로운 마법사가 사용자를 대신하여 필요한 모든 필터 및 NAT 명령문을 작성합니다. 다음과 같습니다.
  - **서비스 허용** 마법사
  - **주소 변환** 마법사
  - **위장 보호** 마법사
- **패킷 규칙 보기의 새로운 방법**
  iSeries Navigator에 있는 새 보기를 통해 인터페이스를 선택하고 그와 연관된 활동 패킷 규칙 및 필터 명령문을 볼 수 있습니다.
- **패킷 규칙 파일 작성 지원**
  다음 파일에 있는 XML 데이터 유형 정의에 따라 패킷 규칙 파일을 작성할 수 있도록 지원합니다.

  `/QIBM/XML/DTD/QtofPacketRules.dtd`
- **패킷 규칙 파일 샘플**
  이 파일을 전형적인 .i3p 형식 또는 .xml 형식으로 볼 수 있습니다. 이 샘플 파일을 사용하여 iSeries에 패킷 규칙을 작성하는데 적합한 구문을 학습하고 다양한 명령문이 하나의 파일에서 함께 작동하는 방법을 볼 수 있습니다.

이 릴리스의 새로운 사항 및 변경된 사항에 대한 추가 정보는 사용자 주의사항 을 참조하십시오.

제 2 장 이 주제 인쇄

PDF 버전을 보거나 다운로드하려면 패킷 규칙(약 245KB 또는 42 페이지)을 선택하십시오.

워크스테이션에 보기용 또는 인쇄용으로 PDF를 저장하려면 다음과 같이 하십시오.

1. 브라우저에서 PDF를 마우스 오른쪽 클릭하십시오(링크 위에 놓고 오른쪽 클릭).
2. **다른 이름으로 목표 저장**을 클릭하십시오.
3. PDF를 저장할 디렉토리로 이동하십시오.
4. **저장**을 클릭하십시오.

Adobe Acrobat Reader 다운로드

이러한 PDF를 보거나 인쇄하기 위해 Adobe Acrobat Reader가 필요한 경우,Adobe 웹 사이트 (http://www.adobe.com/products/acrobat/readstep.html) 에서 사본을 다운로드할 수 있습니다.

제 3 장 패킷 규칙 시나리오

다음 시나리오를 사용하여 네트워크를 보호하기 위해 NAT와 IP 필터링을 사용하는 방법을 설명해 줍니다. 각 시나리오에는 다이어그램과 샘플 구성이 포함됩니다.

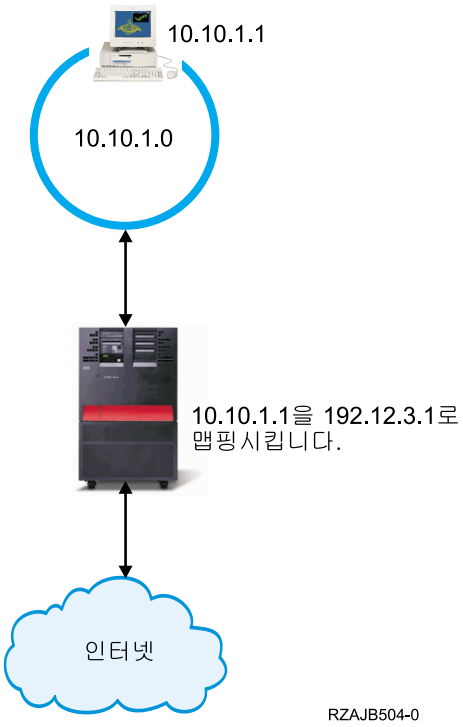
- **패킷 규칙 시나리오: IP 주소 맵핑(정적 NAT)**
  이 시나리오에서 사용자 회사는 정적 NAT를 사용하여 사설 IP 주소를 공용 주소로 맵핑합니다.
- **패킷 규칙 시나리오: HTTP, Telnet 및 FTP를 사용할 수 있도록 필터 규칙 작성**
  이 시나리오에서 사용자 회사는 IP 필터링을 사용하여 해당 웹 서버에 액세스하는 IP 통신을 HTTP, Telnet 및 FTP로 제한합니다.
- **패킷 규칙 시나리오: NAT와 IP 필터링 조합**
  이 시나리오에서 사용자 회사는 NAT와 IP 필터링 둘 다를 사용하여 해당 PC 및 웹 서버를 단일의 공용 IP 주소 뒤에 숨기고 다른 회사에서 해당 웹 서버에 액세스할 수 있게 합니다.
- **패킷 규칙 시나리오: IP 주소 숨기기(가면 NAT)**
  이 시나리오에서 사용자 회사는 가면 NAT를 사용하여 해당 PC의 사설 주소를 숨기고 동시에 회사 직원들이 인터넷에 액세스할 수 있게 합니다.

주: 각 시나리오에서 192.x.x.x IP 주소는 공개 IP 주소를 나타냅니다. 여기에 나오는 모든 주소는 예를 위한 것입니다.

패킷 규칙 시나리오: IP 주소 맵핑(정적 NAT)

상황

사용자에게 자신이 소유하는 회사가 있으며 사설망을 시작하기로 결정합니다. 그러나 공용 IP 주소를 사용하기 위한 허가를 등록하거나 확보한 적은 없습니다. 인터넷에 액세스할 때까지는 모든 것이 제대로 진행되는 듯 했습니다. 그러나 회사의 주소 범위가 다른 누군가에게 등록된 것으로 판명되면, 현재 설정값은 쓸모없다는 것을 알게 됩니다. 그러나 공용 사용자들이 웹 서버에 액세스할 수 있게 만들어야 합니다. 어떻게 해야 할까요?



솔루션

정적 NAT를 사용할 수 있습니다. 정적 NAT는 하나의 원래(사설) 주소를 하나의 등록(공용) 주소로 할당합니다. iSeries는 이 등록 주소를 사설 주소로 맵핑합니다. 등록 주소로 사설 주소가 인터넷과 통신할 수 있습니다. 실질적으로 이 주소가 두 개의 네트워크 사이에 브릿지를 형성합니다. 그리고 나면 둘 중 하나의 네트워크에서 통신을 시작할 수 있습니다.

정적 NAT를 사용함으로써 현재 내부 IP 주소를 모두 보존하면서 인터넷에 액세스할 수 있습니다. 인터넷에 액세스하는 사설 주소마다 하나의 등록 IP 주소가 있어야 합니다. 예를 들어, 12명의 사용자가 있으면 12개의 사설 주소에 맵핑하기 위해 12개의 공용 IP 주소가 필요합니다.

위의 그림에서, NAT 주소 192.12.3.1은 쉘처럼 정보가 리턴되기를 기다리는 사용이 불가능한 상태입니다. 정보가 리턴되면 역으로 NAT가 PC로 다시 주소를 맵핑합니다. 정적 NAT가 활동하면 주소 192.12.3.1에 직접 지정된 인바운드 통신이 내부 주소만 표시하기 때문에 인터페이스에 도달하지 않습니다. iSeries 외부에서는 192.12.3.1이 원하는 IP 주소로 보일지라도 실제 개인 주소 10.10.1.1이 목적지입니다.

구성

이 시나리오에 설명된 패킷 규칙을 구성하려면 iSeries Navigator에 있는 **주소 변환** 마법사를 사용해야 합니다. 마법사는 다음과 같은 정보를 요구합니다.

- 맵핑할 사설 주소: 10.10.1.1
- 사설 주소를 맵핑할 공용 주소: 192.12.3.1
- 주소 맵핑이 발생하는 위치의 회선 이름: TRNLINE

주소 변환 마법사를 사용하려면 다음 단계를 수행하십시오.

1. iSeries Navigator에서 **서버 -> 네트워크 -> IP 정책**을 선택하십시오.
2. **패킷 규칙**을 마우스 오른쪽 클릭하고 **규칙 편집기**를 선택하십시오.
3. **패킷 규칙 구성 환영** 대화 상자에서 **새 패킷 규칙 파일 작성**을 선택한 후 **확인**을 클릭하십시오.
4. **마법사** 메뉴에서, **주소 변환**을 선택한 후 맵 주소 변환 패킷 규칙을 구성하기 위한 마법사의 지시사항을 따르십시오.

패킷 규칙은 다음과 유사하게 나타납니다.

```
-----------------------------------------------------
TRNLINE에서 10.1.1.1을 192.12.3.1로 맵핑하는 명령문
-----------------------------------------------------
ADDRESS MAPPRIVATE1   IP = 10.1.1.1
ADDRESS MAPPUBLIC1   IP = 192.12.3.1
MAP MAPPRIVATE1   TO MAPPUBLIC1   LINE = TRNLINE
-----------------------------------------------------
```

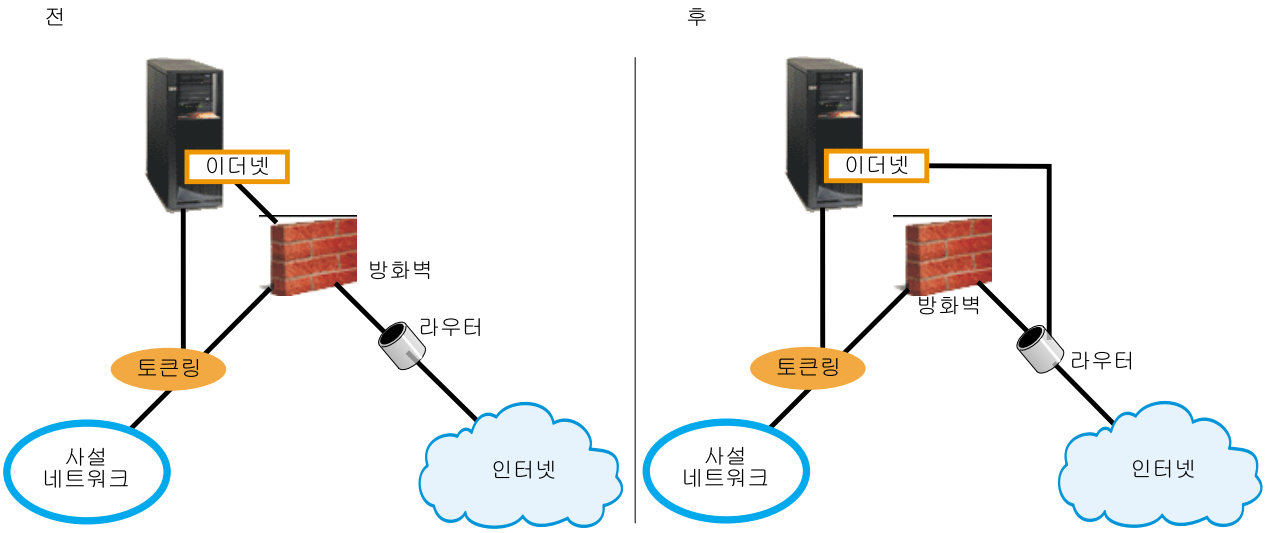
이러한 규칙 및 사용자가 필요로 하는 규칙을 작성한 후에는, 오류 없이 활성화되도록 규칙을 검증해야 합니다. 그런 후 활성화할 수 있습니다.

주: 위에 정의되어 있는 토큰링 회선(LINE=TRNLINE)은 192.12.3.1을 사용하는 회선이어야 합니다. 정적 NAT는 10.10.1.1이 위에 정의된 토큰링 회선을 사용하는 경우 작동하지 않습니다. NAT를 사용할 때마다 IP 이송도 작동하도록 설정해야 합니다. 자세한 내용은 패킷 규칙 문제 해결 섹션을 참조하십시오.

패킷 규칙 시나리오: HTTP, Telnet 및 FTP를 사용할 수 있도록 필터 규칙 작성

상황

고객에게 웹 어플리케이션을 제공하려고 하나 현재 방화벽이 규정 시간을 초과하여 작동하고 있으며, 여기에 추가적인 부담을 원하지 않습니다. 동료들은 방화벽 외부에서 어플리케이션을 실행할 것을 제안합니다. 그러나 인터넷에서 HTTP, FTP 및 Telnet 통신만으로 iSeries 웹 서버에 액세스하려고 합니다. 어떻게 해야 할까요?



솔루션

IP 필터링은 허용하려는 정보를 정의하는 규칙을 설정할 수 있게 해 줍니다. 이 시나리오에서는 웹 서버(이 경우에는 사용자의 iSeries)와의 HTTP, FTP 및 Telnet 통신(인바운드 및 아웃바운드)을 허용하는 필터 규칙을 작성합니다. 서버의 공용 주소는 192.54.5.1이며, 사설 IP 주소는 10.1.2.3입니다.

구성

이 시나리오에 설명된 패킷 규칙을 구성하려면 iSeries Navigator에 있는 **서비스 허용** 마법사를 사용해야 합니다. 마법사는 다음과 같은 정보를 요구합니다.

- 허용할 서비스 유형: HTTP
- iSeries 서버의 공용 주소: 192.54.5.1
- 클라이언트의 주소: 임의의 IP 주소
- 서비스가 실행되는 인터페이스: TRNLINE
- 서비스가 실행되는 방향: INBOUND
- 필터 세트를 식별하는 데 사용할 이름: external_files

서비스 허용 마법사를 사용하려면 다음 단계를 수행하십시오.

1. iSeries Navigator에서 **서버 -> 네트워크 -> IP 정책**을 선택하십시오.
2. **패킷 규칙**을 마우스 오른쪽 클릭하여 **규칙 편집기**를 선택하십시오.
3. **패킷 규칙 구성 환영** 대화 상자에서 **새 패킷 규칙 파일 작성**을 선택한 후 **확인**을 클릭하십시오.
4. **마법사** 메뉴에서, **서비스 허용**을 선택한 후 마법사의 지시사항에 따라 필터 규칙을 작성하십시오.

이러한 패킷 규칙은 시스템으로 들어오고 나가는 HTTP 통신을 허용합니다. 패킷 규칙은 다음과 유사하게 나타납니다.

```
-----------------------------------------------------------------------------------------------------
TRNLINE에서 인바운드 HTTP를 허용하는 명령문
-----------------------------------------------------------------------------------------------------
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
-----------------------------------------------------------------------------------------------------
```

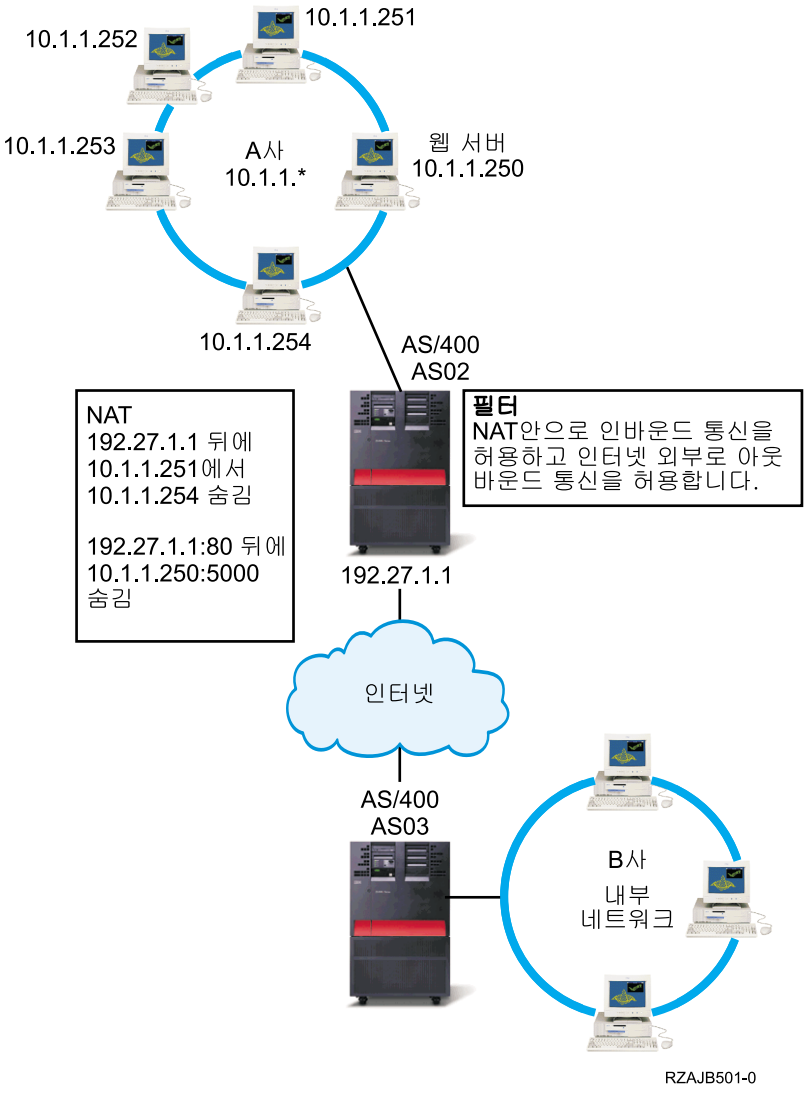
서비스 허용 마법사를 두 번 더 사용하여 시스템으로 들어오고 나가는 FTP 통신 및 Telnet 통신을 허용하는 필터 규칙을 작성하십시오.

이러한 필터 규칙을 작성한 후에는, 오류 없이 활성화되도록 규칙을 검증해야 합니다. 그런 후 활성화할 수 있습니다.

패킷 규칙 시나리오: NAT와 IP 필터링 조합

상황

사용자 회사는 iSeries를 게이트웨이로 사용하는 적절한 크기의 내부 네트워크가 있습니다. 게이트웨이 iSeries로부터의 모든 웹 통신을 게이트웨이 뒤에 있는 전용 웹 서버로 전송하고자 합니다. 웹 서버는 포트 5000에서 실행됩니다. 모든 사설 PC와 웹 서버를 게이트웨이 iSeries 인터페이스의 주소 뒤에 숨기려고 합니다(아래의 다이어그램에서 AS02). 또한 다른 회사들이 웹 서버에 액세스할 수 있게 할 것입니다. 어떻게 해야 할까요?



솔루션

IP 필터링과 NAT를 동시에 사용하여 구성할 수 있습니다.

1. 사용자 PC가 인터넷에 액세스할 수 있도록 공용 주소 192.27.1.1 뒤에 PC를 숨기는 숨김 NAT.
2. 공용 주소 192.27.1.1 및 포트 번호 80 뒤에 사용자 웹 서버 주소 10.1.1.250 및 포트 번호 5000을 숨기는 포트 맵핑된 NAT. 이 두 NAT 규칙이 192.27.1.1 뒤에 숨겨집니다. 숨긴 주소가 겹치지 않는 한 허용됩니다. 포트 맵핑된 NAT 규칙은 포트 80에서 외부적으로 시작된 통신만이 시스템에 액세스할 수 있도록 합니다. 외부적으로 시작된 통신이 정확한 주소 및 포트 번호와 일치하지 않으면, NAT는 통신을 변환하지 않고 해당 패킷은 삭제됩니다.
3. 목적지가 사설망에서 NAT로 지정된 모든 인바운드 통신과 인터넷으로 가는 모든 아웃바운드 통신을 필터링하는 규칙.

구성

이 시나리오에 설명된 숨김 NAT 패킷 규칙을 구성하려면 iSeries Navigator에 있는 **주소 변환** 마법사를 사용해야 합니다. 마법사는 다음과 같은 정보를 요구합니다.

- 숨길 주소 세트: 10.1.1.251 - 10.1.1.254
- 주소 세트를 뒤에 숨길 인터페이스 주소: 192.27.1.1

주소 변환 마법사를 사용하려면 다음 단계를 수행하십시오.

1. iSeries Navigator에서 **서버 -> 네트워크 -> IP 정책**을 선택하십시오.
2. **패킷 규칙**을 마우스 오른쪽 클릭하여 **규칙 편집기**를 선택하십시오.
3. **패킷 규칙 구성 환영** 대화 상자에서 **새 패킷 규칙 파일 작성**을 선택한 후 **확인**을 클릭하십시오.
4. **마법사** 메뉴에서, **주소 변환**을 선택한 후 숨김 주소 변환 패킷 규칙을 구성하기 위한 마법사의 지시사항을 따르십시오.

이 패킷 규칙은 사용자의 PC가 인터넷에 액세스할 수 있도록 공용 주소 뒤에 네 PC를 숨깁니다. 숨김 NAT 패킷 규칙은 다음과 유사하게 나타납니다.

```
------------------------------------------------------------
192.27.1.1 뒤에 10.1.1.251 - 10.1.1.254를 숨기는 명령문
------------------------------------------------------------
ADDRESS HIDE1   IP = 10.1.1.251 THROUGH 10.1.1.254
ADDRESS BEHIND1   IP = 192.27.1.1
HIDE HIDE1   BEHIND BEHIND1
------------------------------------------------------------
```

포트 맵핑된 NAT를 구성하려면 다음 단계를 수행하십시오.

1. iSeries Navigator에서 패킷 규칙 편집기에 액세스하십시오.
2. 웹 서버 주소 및 포트 5000에 대해 정의된 주소를 작성하십시오.
   a. **삽입** 메뉴에서 **주소...**를 선택하십시오.
   b. **일반** 페이지에서 **주소 이름** 필드에 **Web250**을 입력하십시오.
   c. **정의된 주소** 드롭 다운 리스트에서 **IP 주소**를 선택하십시오. 그런 다음, **추가**를 클릭하고 편집 필드에 웹 서버에 대한 IP 주소 10.1.1.250을 입력하십시오.
   d. **확인**을 클릭하십시오.
3. 공용 주소 192.27.1.1을 표시하려면 정의된 주소를 작성하십시오.
   주: 숨김 NAT 패킷 규칙을 구성할 때 공용 주소 192.27.1.1을 표시하는 정의된 주소를 이미 작성했으므로, 이 시나리오에서는 이 단계를 생략하고 4단계로 건너뛸 수 있습니다. 그러나 숨김 NAT 패킷 규칙을 구성하지 않은 상태에서 이 지침에 따라 사용자 고유의 네트워크에 대해 포트 맵핑된 NAT를 구성할 경우에는 이 단계의 지침대로 계속하십시오.
   a. **삽입** 메뉴에서 **주소...**를 선택하십시오.
   b. **일반** 페이지에서 **주소 이름** 필드에 **BEHIND1**을 입력하거나 선택하십시오.

c. **정의된 주소** 드롭 다운 리스트에서 **IP 주소**를 선택하십시오. 그런 다음, **추가**를 클릭하고 **IP 주소** 편집 필드에 192.27.1.1을 입력하십시오.

d. **확인**을 클릭하십시오.

4. 포트 맵핑된 NAT 규칙을 작성하려면 다음을 수행하십시오.

a. **삽입** 메뉴에서 **숨기기...**를 선택하십시오.

b. **일반** 페이지에서 **주소 이름 숨기기** 드롭 다운 리스트의 Web250을 선택하십시오.

c. **주소 이름 뒤** 드롭 다운 리스트에서 **BEHIND1**을 선택하십시오.

d. **인바운드 연결 허용**을 선택한 후 **포트 숨기기** 필드에 5000을 입력하십시오.

e. **포트 뒤** 필드에 80을 입력하십시오.

f. 16을 입력한 후 **시간종료** 필드에서 **초**를 선택하십시오.

g. **최대 대화 수** 필드에 64를 입력하십시오.

h. **저널링** 드롭 다운 리스트에서 **OFF**를 선택하십시오.

i. **확인**을 클릭하십시오.

이 포트 맵핑된 NAT는 공용 주소와 포트 번호 뒤에 웹 서버 주소와 포트 번호를 숨깁니다. 두 NAT 규칙이 하나의 일반 IP 주소 뒤에 숨는다는 점에 주의하십시오. 숨긴 주소가 겹치지 않는 한 허용됩니다. 이 포트 맵팽된 NAT 규칙은 포트 80에서 외부적으로 시작된 통신만이 사용자의 시스템에 액세스할 수 있게 해 줍니다.

포트 맵핑된 NAT 규칙은 다음과 유사하게 나타납니다.

```
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
```

이 시나리오에 설명된 필터 규칙을 작성하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 패킷 규칙 편집기에 액세스하십시오.
2. 목적지가 사설망으로 지정된 인바운드 통신을 허용하는 필터 규칙을 작성하십시오.

a. **패킷 규칙 구성 환영** 대화 상자에서 **새 패킷 규칙 파일 작성**을 선택한 후 **확인**을 클릭하십시오.

b. **삽입** 메뉴에서 **필터...**를 선택하십시오.

c. **일반** 페이지에서 **이름 설정** 필드에 external_rules을 입력하십시오.

d. **조치** 드롭 다운 리스트에서 **PERMIT**를 선택하십시오.

e. **방향** 드롭 다운 리스트에서 **INBOUND**를 선택하십시오.

f. **소스 주소 이름** 드롭 다운 리스트에서 = 및 *를 선택하십시오.

g. =를 선택한 후 **목적지 주소 이름** 필드에 192.27.1.1을 입력하십시오.

h. **저널링** 드롭 다운 리스트에서 **OFF**를 선택하십시오.

i. **서비스** 페이지에서 **서비스**를 선택하십시오.

j. **프로토콜** 드롭 다운 리스트에서 **TCP**를 선택하십시오.

k. **소스 포트** 드롭 다운 리스트에서 = 및 *를 선택하십시오.

l. **목적지 포트** 드롭 다운 리스트에서 = 및 *를 선택하십시오.

m. **확인**을 클릭하십시오.

3. 사설망에서 인터넷으로의 아웃바운드 통신을 허용하는 필터 규칙을 작성하십시오.

   a. **패킷 규칙 구성 환영** 대화 상자에서 **기존 패킷 규칙 파일 열기**를 선택한 후 **확인**을 클릭하십시오.

   b. **파일 열기** 대화 상자에서, **external_rules** 파일을 선택한 후 **열기**를 클릭하십시오.

   c. **삽입** 메뉴에서 **필터...**를 선택하십시오.

   d. **일반** 페이지에서 **이름 설정** 드롭 다운 리스트에서 external_rules를 선택하십시오.

   e. **조치** 드롭 다운 리스트에서 **PERMIT**를 선택하십시오.

   f. **방향** 드롭 다운 리스트에서 **OUTBOUND**를 선택하십시오.

   g. =를 선택한 후 **소스 주소 이름** 필드에 192.27.1.1을 입력하십시오.

   h. **목적지 주소 이름** 드롭 다운 리스트에서 = 및 *를 선택하십시오.

   i. **저널링** 드롭 다운 리스트에서 **OFF**를 선택하십시오.

   j. **서비스** 페이지에서 **서비스**를 선택하십시오.

   k. **프로토콜** 드롭 다운 리스트에서 **TCP**를 선택하십시오.

   l. **소스 포트** 드롭 다운 리스트에서 = 및 *를 선택하십시오.

   m. **목적지 포트** 드롭 다운 리스트에서 = 및 *를 선택하십시오.

   n. **확인**을 클릭하십시오.

4. 작성한 필터 세트에 대한 필터 인터페이스를 정의하십시오.

   a. **삽입** 메뉴에서 **필터 인터페이스...**를 선택하십시오.

   b. **회선 이름**을 선택한 후 **회선 이름** 드롭 다운 리스트에서 **TRNLINE**을 선택하십시오.

   c. **필터 세트** 페이지에서, **필터 세트** 드롭 다운 리스트에서 external_rules를 선택하십시오. 그런 다음, **추가**를 클릭하십시오.

   d. **확인**을 클릭하십시오.

이들 필터는 HIDE문과 함께 사용시 목적지가 사용자의 사설망에서 NAT로 지정된 모든 인바운드 통신과 인터넷으로 가는 모든 아웃바운드 통신을 허용합니다. 그러나 NAT는 포트 80에서 외부적으로 시작한 통신만 서버에 입력될 수 있게 해 줍니다. NAT는 포트 맵핑된 NAT 규칙에 일치하지 않는 외부적으로 시작된 통신은 변환시키지 않습니다. 필터 규칙은 다음과 유사하게 나타납니다.

```
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
```

다음 명령문으로 ‘external_rules’ 필터 세트를 올바른 실제 인터페이스와 바인드(연관)시킵니다.

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

이러한 규칙을 작성한 후에는, 오류 없이 활성화되도록 규칙을 검증해야 합니다. 그런 후 활성화할 수 있습니다.

패킷 규칙 시나리오: IP 주소 숨기기(가면 NAT)

상황

귀사는 iSeries에서 HTTP 서비스를 허용하려고 하는 작은 회사입니다. 이더넷 카드가 하나인 모델 170e과 세 대의 PC가 있습니다. 인터넷 서비스 제공자(ISP)로부터 DSL 연결 및 DSL 모뎀을 제공받습니다. 또한 ISP로부터 192.20.12.1 및 192.20.12.2.의 공용 IP 주소를 할당받습니다. 모든 PC는 내부 네트워크에 10.1.1.x 주소를 사용합니다. 외부 사용자가 내부 네트워크와 통신을 시작하지 못하도록 하면서 동시에 회사 직원들이 인터넷에 액세스할 수 있게 하기 위해, PC의 사설 주소를 숨겨진 상태로 유지하고자 합니다. 어떻게 해야 할까요?

솔루션

PC 주소 10.1.1.1 - 10.1.1.4를 공용 주소 192.20.12.1 뒤에 숨기십시오. 이렇게 하면 10.1.1.1 주소에서 TCP/IP 서비스를 실행할 수 있습니다. 범위 NAT(내부 주소 범위를 숨기는)는 사설망 외부에서 시작되는 통신으로부터 사용자 PC를 보호합니다. 그 이유는 범위 NAT를 시작하기 위해서는 내부적으로 통신을 시작해야 하기 때문입니다. 그러나 NAT 범위는 iSeries 인터페이스를 보호하지 않습니다. iSeries가 변환되지 않은 정보를 수신하지 못하게 보호하려면 통신을 필터링하십시오.

구성

이 시나리오에 설명된 패킷 규칙을 구성하려면 iSeries Navigator에 있는 **주소 변환** 마법사를 사용해야 합니다. 마법사는 다음과 같은 정보를 요구합니다.

- 숨길 주소 세트: 10.1.1.1 - 10.1.1.4
- 세트를 뒤에 숨길 인터페이스 주소: 192.20.12.1

주소 변환 마법사를 사용하려면 다음 단계를 수행하십시오.

1. iSeries Navigator에서 **서버 -> 네트워크 -> IP 정책**을 선택하십시오.
2. **패킷 규칙**을 마우스 오른쪽 클릭하고 **규칙 편집기**를 선택하십시오.
3. **패킷 규칙 구성 환영** 대화 상자에서 **새 패킷 규칙 파일 작성**을 선택한 후 **확인**을 클릭하십시오.
4. **마법사** 메뉴에서, **주소 변환**을 선택한 후 주소 숨김 변환 패킷 규칙을 구성하기 위한 마법사의 지시사항을 따르십시오.

패킷 규칙은 다음과 유사하게 나타납니다.

```
------------------------------------------------------------
192.20.12.1 뒤에 10.1.1.1 - 10.1.1.4를 숨기는 명령문
------------------------------------------------------------
ADDRESS HIDE1   IP = 10.1.1.1 THROUGH 10.1.1.4
ADDRESS BEHIND1   IP = 192.20.12.1
HIDE HIDE1   BEHIND BEHIND1
------------------------------------------------------------
```

이러한 규칙을 작성한 후에는, 오류 없이 활성화되도록 규칙을 검증해야 합니다. 그런 후 활성화할 수 있습니다.

제 4 장 패킷 규칙 개념

패킷 규칙은 네트워크 주소 변환(NAT) 및 IP 필터링 규칙으로 구성됩니다. 이 두 구성요소는 TCP/IP 스택의 IP 계층에서 실행되며 주로 TCP/IP 통신과 연관된 잠재적 위험으로부터 시스템을 보호하는데 도움이 됩니다.

패킷 규칙이 작동하는 방법에 대한 이해를 높이려면 패킷 규칙의 개념 및 사용자의 iSeries에 패킷 규칙이 적용되는 방법을 잘 알고 있어야 합니다.

- **패킷 규칙 전문 용어**
  사용자가 알아야 하는 iSeries 고유의 전문 용어 리스트를 제공합니다.
- **패킷 규칙 대 기타 iSeries 보안 솔루션**
  패킷 규칙이 다른 iSeries 보안 솔루션과 어떻게 비교되는가? 이에 대한 정보를 보려면 여기로 가십시오.
- **네트워크 주소 변환(NAT)**
  서로 다른 몇 개의 주소 변환 유형이 있습니다. 이 주제에서는 사용자 네트워크에 적합한 유형을 결정하는 데 필요한 정보를 제공합니다.
- **IP 필터링**
  패킷 규칙의 IP 필터링 구성요소가 작동하는 방법에 대한 자세한 내용은 이 주제를 참조하십시오.
- **IP 필터 규칙으로 NAT 규칙 구성**
  NAT 규칙 및 IP 필터 규칙을 개별적으로 또는 함께 사용할 수 있습니다. 이 주제에서는 두 구성요소가 함께 작동하는 방법에 대해 설명합니다.
- **복수 IP 필터 규칙 구성**
  필터 규칙을 작성하면, 시스템이 특정 순서로 이들을 처리합니다. 이 주제에서는 복수 필터 규칙이 처리되는 방법을 설명하고 예를 제공합니다.
- **위장 보호**
  이 페이지에서는 위장 보호를 정의하고 이것을 사용해야 하는 이유를 설명합니다.

패킷 규칙 전문 용어

다음 리스트에는 Information Center 주제 전반에 걸쳐 사용된 iSeries 특정 용어가 들어 있습니다.

경계 경계는 신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 사이의 경계를 형성하는 공용 주소입니다. 경계는 IP 주소를 iSeries상의 실제 인터페이스로서 설명합니다. 시스템은 사용자가 정의하는 주소의 ″유형″을 알아야 합니다. 예를 들어, PC의 IP 주소는 신뢰할 수 있지만 서버의 공용 IP 주소가 경계입니다.

방화벽 네트워크에 있어서 시스템 주위의 논리적 벽을 말합니다. 방화벽은 하드웨어, 소프트웨어, 보안(신뢰할 수 있는) 시스템과 비보안(신뢰할 수 없는) 시스템간의 정보 액세스 및 흐름을 제어하는 보안 정책으로 구성됩니다.

maxcon

Maxcon은 한 번에 활성화시킬 수 있는 대화의 수입니다. 시스템은 사용자가 NAT 가면 규칙을 설정할 때 이 수를 정의하도록 요구합니다. 디폴트 값은 128입니다. Maxcon은 가면 NAT 규칙에만 관련이 있습니다.

NAT 대화

NAT 대화는 다음 IP 주소와 포트 번호 사이의 관계를 말합니다.

- 사설 소스 IP 주소와 소스 포트 번호(NAT 없는)
- 공용(NAT) 소스 IP 주소와 공용(NAT) 소스 포트 번호
- 목적지 IP 주소와 포트 번호(외부 네트워크)

PPP 필터 ID

PPP 필터 ID를 사용하여 지점 간 프로파일에 정의된 인터페이스에 필터 규칙을 적용할 수 있습니다. PPP 필터 ID는 또한 지점 간 프로파일에 있는 사용자 그룹으로 필터 규칙을 링크합니다. 지점 간 프로파일은 특정 IP 주소와 연관되어 있으므로, 필터 ID는 규칙이 적용되는 인터페이스를 내재적으로 정의합니다. 자세한 내용은 *리모트 액세스 서비스: PPP 연결* 주제에 있는 그룹 정책 및 IP 필터링을 사용하여 자원에 대한 리모트 사용자 액세스 관리 시나리오를 참조하십시오.

시간종료

시간종료는 허용되는 대화 시간을 제어합니다. 시간종료 값을 너무 짧게 설정하면 대화가 너무 빨리 중단됩니다. 디폴트 값은 16입니다.

패킷 규칙 대 기타 iSeries 보안 솔루션

iSeries에는 여러 가지 유형의 위험으로부터 시스템을 보호할 수 있는 통합 보안 구성요소가 있습니다. 그 중 하나로 패킷 규칙은 시스템 보안을 위한 경제적인 방법을 제공합니다. 어떤 경우에는 추가로 제품을 구입할 필요 없이 패킷 규칙이 사용자가 필요로 하는 모든 것을 제공할 수 있습니다. 그러나 시스템 보안이 비용보다 우선되어야 합니다.

생산 시스템을 보안하거나 사용자의 iSeries와 네트워크의 다른 시스템 간의 통신을 보안하는 것과 같은 위험률이 높은 상황에서는, 다른 iSeries 보안 솔루션을 조사하여 보호 범위를 확장시켜야 합니다.

보안 전략에 여러 방어선을 포함시키는데 도움이 되는 정보를 보려면 다음과 같은 Information Center 주제를 참조하십시오.

- **IBM® SecureWay®®: iSeries 및 인터넷**
  이 주제에서는 인터넷을 사용하기 전에 사용자가 고려해야 할 위험과 솔루션에 대한 풍부한 정보를 제공합니다.
- **보안 소켓 계층(SSL)**
  SSL은 서버 응용프로그램과 해당 클라이언트간의 보안 연결을 제공합니다. 이 주제에는 iSeries 응용프로그램에서 SSL을 작동하도록 하는 방법에 대한 정보를 포함합니다.

- **VPN(가상 사설망)**
  VPN은 사용자 회사가 인터넷과 같은 공용 네트워크의 기존 구조로 사설 인트라넷를 안전하게 확장할 수 있게 합니다. 이 주제에서는 VPN에 대해 설명하며 iSeries에서 VPN을 사용하는 방법을 알려줍니다.
- **iSeries용 보안 추가 정보 및 툴**
  이 PDF 서적에서는 iSeries에서 보안을 향상시키는 방법에 대한 고급 정보를 제공합니다.

네트워크 주소 변환(NAT)

IP 주소는 폭발적으로 늘어나는 인터넷 인구로 인해 빠르게 고갈되고 있습니다. 조직은 사설망을 사용함으로써 원하는 IP 주소를 마음대로 선택할 수 있습니다. 그러나 두 개의 회사가 중복된 IP 주소를 가진 상태에서 서로 통신하려고 하면 문제가 발생합니다. 인터넷에서 통신하기 위해서는 고유한 등록 주소가 있어야 합니다. 네트워크 주소 변환(NAT)은 사용자의 사설망 IP 주소를 변경하지 않고 안전하게 인터넷에 액세스할 수 있게 해 줍니다. 이름에서 의미하는 것처럼 NAT는 하나의 인터넷 프로토콜(IP) 주소를 다른 주소로 변환하는 메카니즘입니다.

패킷 규칙에는 세 가지 NAT 방법이 있습니다. 일반적으로 주소를 맵핑하거나(정적 NAT) 주소를 숨기기 위해(가면 NAT) NAT를 사용합니다. 여러 가지 NAT 양식에 관한 자세한 정보는 아래의 링크를 검토하십시오.

- 정적(맵핑) NAT
- 가면(숨기기) NAT
- 가면 또는 숨기기(포트 맵핑) NAT

주소를 숨기거나 맵핑하는 방식으로 NAT는 여러 가지 주소지정 문제를 해결합니다. 아래 나오는 예는 NAT로 해결할 수 있는 몇 가지 문제에 관해 설명합니다.

예 1: 외부로부터 내부 IP 주소 숨기기

iSeries를 공용 웹 서버로 구성하는 중입니다. 그러나 외부 네트워크에서 서버의 실제 내부 IP 주소를 아는 것을 원치 않습니다. 이제 사설 주소를 인터넷에 액세스할 수 있는 공용 주소로 변환하는 NAT 규칙을 작성하십시오. 이 경우에 서버의 ″실제″ 주소는 숨겨진 상태로 있기 때문에 외부 침입으로부터 서버를 일정 수준까지는 보호합니다.

예 2: 내부 호스트의 IP 주소를 다른 IP 주소로 변환

내부 네트워크의 사설 IP 주소로 인터넷 호스트와 통신하려고 합니다. 이 경우 내부 호스트의 IP 주소를 다른 IP 주소로 변환할 수 있습니다. 인터넷 호스트와 통신할 때에는 반드시 공용 IP 주소를 사용해야 합니다. 이제 NAT를 사용하여 사설 IP 주소를 공용 주소로 변환하십시오. 이렇게 하면 내부 호스트에서 나온 IP 통신을 인터넷을 통해 라우트시킬 수 있습니다.

예 3: 두 개의 다른 네트워크간 IP 주소 호환

다른 네트워크의 호스트 시스템(예: 공급업체)이 사용자의 내부 네트워크에 있는 특정 호스트와 통신하도록 하려 합니다. 그러나 두 네트워크 모두 사설 주소(10.x.x.x)를 사용하므로 양쪽 호스트 사이에서의 통신 라우팅 시 주소 충돌 가능성이 있습니다. 이 경우 충돌을 피하기 위해 NAT를 사용하여 내부 호스트의 주소를 다른 IP 주소로 변환할 수 있습니다.

정적(맵핑) NAT

정적(맵핑) NAT는 사설 IP 주소와 공용 IP 주소의 일대일 맵핑을 제공합니다. 정적 NAT를 사용하여 내부 네트워크상의 IP 주소를 공용화시킬 IP 주소로 맵핑할 수 있습니다.

정적 NAT는 내부 네트워크나 인터넷과 같은 외부 네트워크로부터 통신을 초기화할 수 있게 해 줍니다. 내부 네트워크에 공용 사용자가 액세스할 수 있는 서버가 있으면 매우 유용합니다. 이와 같은 경우에는 실제 서버 주소를 공용 주소로 맵핑하는 NAT 규칙을 작성해야 합니다. 이때 공용 주소는 외부 정보가 됩니다. 이것은 시스템 침입자로부터 사용자의 개인 자료를 안전하게 지켜줍니다.

다음 리스트는 정적 NAT의 피처를 요약한 것입니다.

- 일대일 맵핑
- 외부 및 내부 네트워크 초기화
- 연관 또는 맵핑시킨 주소를 어느 주소로나 사용할 수 있음
- 연관 또는 맵핑시킨 주소를 IP 인터페이스로 사용할 수 없음
- 포트 맵핑된 NAT를 사용하지 않음

주의

PC를 iSeries의 ″잘 알려진″ 주소로 맵핑할 경우 주의해야 합니다. 잘 알려진 주소란 대부분의 인터넷 및 인트라넷 통신을 위해 예약된 IP 주소를 말합니다. 이러한 IP 주소로 맵핑하는 경우 NAT가 모든 통신을 변환하여 내부 사설 주소로 송신합니다. 이 인터페이스는 NAT에 예약되는 것이므로 iSeries와 인터페이스를 사용할 수 없습니다.

정적 NAT의 시나리오와 일러스트레이션에 대한 패킷 규칙 시나리오: IP 주소 맵을 검토하십시오.

가면(숨기기) NAT

가면(숨기기) NAT를 사용하여 외부(iSeries의 외부)에서 PC의 실제 주소를 알 수 없도록 할 수 있습니다. NAT는 통신을 PC에서 iSeries로 라우트하므로, 실질적으로 iSeries가 PC의 게이트웨이가 됩니다. 다음은 그 작동 방식을 설명한 것입니다.

가면 NAT로 여러 개의 IP 주소를 또 다른 하나의 IP 주소로 변환할 수 있습니다. 내부 네트워크에 있는 여러 개의 IP 주소를 공용화시킬 IP 주소 뒤에 *숨길* 때 가면 NAT를 사용하십시오. 이 공용 주소는 사설 주소가 변환되는 주소이며 사용자의 iSeries 서버에서 정의된 인터페이스이어야 합니다. 인터페이스를 정의하려면 공용 주소를 BORDER 주소로 정의하십시오.

복수 주소 숨기기

복수 주소를 숨기려면 NAT가 iSeries 서버를 통해 변환시켜야 하는 주소의 범위를 지정하십시오. 일반적인 프로세스는 다음과 같습니다.

1. 변환된 IP 주소가 소스 IP 주소를 대체합니다. 이것은 IP 패킷의 IP 헤더에서 발생합니다.
2. 전송 제어 프로토콜(TCP) 또는 사용자 데이터그램 프로토콜(UDP) 헤더의 IP 소스 포트 번호(하나가 있을 경우)가 임시 포트 번호로 대체됩니다.
3. 기존 대화는 새로운 IP 소스 주소와 포트 번호간의 관계입니다.
4. 기존의 대화는 NAT 서버가 외부 기계로부터 IP 데이터그램을 변환하지 않게 해 줍니다.

IP 데이터그램 헤더를 보려면 IP 패킷 헤더로 가십시오.

가면 NAT를 사용할 때 내부 시스템이 통신을 초기화합니다. 초기화가 발생하면, NAT가 iSeries NAT 서버를 통해 IP 패킷을 전달할 때 이를 변환시킵니다. 외부 호스트가 사용자의 네트워크로 통신을 시작할 수 없기 때문에 가면 NAT를 선택하는 것이 좋습니다. 그 결과, 사용자의 네트워크를 외부 침입으로부터 보호할 수 있습니다. 또한 다수의 내부 사용자를 위해 하나의 공용 IP 주소만 사용하면 됩니다.

다음 리스트는 가면 NAT의 피처를 요약한 것입니다.

- 사설 IP 주소나 IP 주소 범위를 NAT 기계의 공용 IP 주소 뒤에 바인드합니다.
- 내부 네트워크만 초기화합니다.
- 포트 번호를 어느 포트 번호와도 연관시킵니다. 이것은 주소와 포트 번호가 모두 인터넷에서 숨겨짐을 의미합니다.
- NAT 기계에 등록된 주소는 NAT 외부에서 사용할 수 있는 인터페이스입니다.

주의

- 사용하려는 대화 수를 수용할 수 있을 만큼 충분한 MAXCON을 설정해야 합니다. 예를 들어, FTP를 사용 중인 경우 PC에서는 두 개의 대화가 활동하게 됩니다. 이 경우 각 PC에 복수 대화를 수용할 수 있도록 충분한 MAXCON을 설정해야 합니다. 네트워크에서 허용할 동시 대화 수도 결정하십시오. 디폴트 값은 128입니다.
- PC간의 대화를 종료할 수 있을 만큼 충분한 TIMEOUT(HIDE 규칙 명령문)을 설정하십시오. 숨기기 NAT를 적절하게 발생시키기 위해서는 진행 중인 내부 대화가 있어야 합니다. 시간종료 값이 내부 대화에 대한 응답 대기 시간을 코드로 통지합니다. 디폴트 값은 16입니다.
- 가면 NAT는 TCP, UDP, ICMP 프로토콜만 지원합니다.
- NAT를 사용할 때마다 IP 이송도 작동하도록 설정해야 합니다. CHGTCPA(TCP/IP 속성 변경) 명령을 사용하여 IP 데이터그램 이송을 예로 설정하였는지 확인하십시오.

가면 NAT나 숨기기 NAT의 예에 관해서는 IP 주소 숨기기(가면 NAT)에서 시나리오와 일러스트레이션을 보십시오.

가면(포트 맵핑) NAT

포트 맵핑 NAT는 가면 NAT의 변경입니다. 어떻게 다를까요? 포트 맵핑된 NAT에는 변환할 IP 주소와 포트 번호를 모두 지정할 수 있습니다. 이것은 내부 PC와 외부 기계 모두가 IP 통신을 초기화할 수 있게 해 줍니다. 외부 기계(또는 클라이언트)가 네트워크 내부의 기계나 서버에 액세스하는 경우 이를 사용할 수 있습니다. IP 주소와 포트 번호 둘다 일치하는 IP 통신에만 액세스를 허용합니다. 다음은 작동 방식을 설명한 것입니다.

내부 초기화

*주소 1: 포트 1*인 내부 PC가 외부의 기계로 통신을 시작할 때 변환 코드가 *주소 1: 포트 1*에 대해 NAT 규칙 파일을 검사합니다. 소스 IP 주소(주소 1)와 소스 포트 번호(포트 1) 둘 다 NAT 규칙과 일치하면 NAT가 대화를 시작하고 변환을 수행합니다. NAT 규칙에서 나온 지정 값이 IP 소스 주소와 소스 포트 번호를 대체합니다. *주소 1: 포트 1*을 *주소 2: 포트 2*로 대체합니다.

외부 초기화

외부 기계가 *주소 2*의 목적지 IP 주소로 IP 통신을 시작합니다. 목적지 포트 번호는 *포트 2*입니다. NAT 서버가 "기존 대화"의 유무에 관계 없이 데이터그램을 변환하지 않습니다. 즉, NAT가 아직 없을 경우 자동으로 대화를 작성합니다. *주소 2: 포트 2*를 *주소 1: 포트 1*로 변환하지 않습니다.

다음 리스트는 가면 포트 맵핑된 NAT의 피처를 요약한 것입니다.

- 일대일 관계
- 외부 및 내부 네트워크 초기화
- 사설 주소가 뒤에 숨는 등록된 주소는 NAT 조작을 수행하는 iSeries에 정의되어야 합니다.
- NAT 조작 외부의 IP 통신은 등록된 주소를 사용할 수 없습니다. 그러나 이 주소가 NAT 규칙의 숨겨진 포트에 일치하는 포트 번호를 사용하려고 시도하면 그 통신을 변환시킵니다. 인터페이스는 사용할 수 없게 됩니다.
- 보통은 포트 번호를 잘 알려진 포트 번호에 맵핑시키므로 다른 정보가 필요 없습니다. 예를 들어, 5123 포트에 바인드시킨 HTTP 서버를 실행시킨 후 이 서버를 공용 IP와 포트 80에 맵핑시킬 수 있습니다. 내부 포트 번호를 다른(비공용) 포트 번호 뒤에 숨기려는 경우, 클라이언트가 목적지 포트 번호 값을 실제로 알아야 합니다. 그렇지 않으면 통신이 어렵습니다.

주의

- 사용하려는 대화 수를 수용할 수 있을 만큼 충분한 MAXCON을 설정해야 합니다. 예를 들어, FTP를 사용 중인 경우 PC에서는 두 개의 대화가 활동하게 됩니다. 각 PC의 복수 대화에 충분한 MAXCON을 설정해야 합니다. 디폴트 값은 128입니다.
- 가면 NAT는 TCP, UDP, ICMP 프로토콜만 지원합니다.
- NAT를 사용할 때마다 IP 이송도 작동하도록 설정해야 합니다. CHGTCPA(TCP/IP 속성 변경) 명령을 사용하여 IP 데이터그램 이송을 예로 설정하였는지 확인하십시오.

IP 필터링

그 자체로는 완벽한 방화벽이 아니더라도, 패킷 규칙은 사용자의 iSeries의 패킷을 필터링할 수 있는 확실한 구성요소입니다. 구체적으로, 패킷 규칙의 IP 필터링 구성요소는 사용자 회사의 네트워크로 들어오고 나갈 수 있는 IP 통신을 제어할 수 있도록 합니다. IP 필터링은 사용자가 지정하는 규칙에 따라 패킷을 필터링하여 시스템을 보호합니다. 이러한 규칙은 IP 패킷 헤더에 있는 정보를 토대로 합니다.

이 필터 규칙을 여러 회선에 적용하거나 각 회선에 다른 규칙을 적용할 수 있습니다. 필터 규칙은 논리 인터페이스나 IP 주소가 아닌 토큰링(trnline)과 같은 회선과 연관됩니다. 시스템이 회선과 연관된 각 규칙에 대해 각 패킷을 검사합니다. 순차적인 처리로 각 규칙을 검사합니다. 일단 시스템이 패킷을 규칙에 일치시키면 그 프로세스를 중단하고 일치하는 규칙을 적용합니다.

시스템이 일치하는 규칙을 적용할 때 실제로 그 규칙이 지정하는 조치가 수행됩니다. iSeries는 세 가지 조치를 지원합니다(V4R4 이상).

1. PERMIT -- 평상시와 같이 패킷 처리
2. DENY -- 즉각적으로 패킷 삭제
3. IPSEC -- 필터 규칙에 지정하는 VPN 연결을 통해 패킷 송신

주: 이 경우, IPSEC은 사용자의 필터 규칙에 정의할 수 있는 조치입니다. 이 주제에서는 IPSec에 관해 구체적으로 다루지 않으나, 필터링과 가상 사설망(VPN)은 밀접한 관련이 있음에 유의하십시오. VPN에 대한 자세한 정보는 VPN(가상 사설망) 주제를 참조하십시오.

사용자가 규칙을 적용하면 시스템이 규칙과 패킷에 대해 이 순차 비교를 계속하여 모든 해당 규칙으로 조치를 할당합니다. 시스템이 특정 패킷에 맞는 규칙을 찾지 못하면 자동으로 해당 패킷을 삭제합니다. 시스템의 디폴트 거부 규칙은 시스템이 필터 규칙에 일치하지 않는 패킷을 자동으로 삭제하는 것을 보장합니다. 필터 규칙이 단방향(인바운드 또는 아웃바운드)으로의 통신만 허용하도록 설계된 경우, 시스템은 양쪽 방향에서 디폴트 거부 규칙을 구현합니다. 즉, 인바운드 및 아웃바운드 패킷은 삭제됩니다.

샘플 필터 명령문

이 샘플 필터 명령문의 목적은 iSeries에 필터 규칙을 작성하는데 적합한 구문을 설명하고 다양한 명령문이 파일에서 함께 작동되는 방법을 보여주기 위한 것입니다. 단지 예로서만 사용하십시오.

일반적인 필터 명령문은 다음과 유사하게 나타납니다.

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

이 필터는 인터페이스로 들어가는(INBOUND) 소스 주소 162.56.39.100, 소스 포트 80, 목적지 포트가 1024 이상인 모든 통신을 허용합니다.

IP 통신은 일반적으로 하나의 연결에서 INBOUND 및 OUTBOUND 두 방향으로 흐르므로, 두 방향의 통신을 허용하는 두 개의 관련된 명령문을 가지는 것이 일반적입니다. 이러한 두 명령문을 서로의 미러(mirror)라고 하며 다음 예에서 볼 수 있습니다.

```
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
```

이 두 필터 명령문 모두 TestFilter라는 동일한 세트명을 가집니다. 동일한 세트명을 가지는 모든 필터는 동일한 세트에 있는 것으로 간주됩니다. 하나의 세트에 포함되는 필터 수에는 제한이 없습니다. 주어진 세트 내의 필터를 활성화하면 파일에 있는 순서대로 필터가 처리됩니다.

규칙을 활성화할 때, 필터 명령문 그 자체만으로는 아무런 영향을 미치지 않습니다. 필터 인터페이스에 필터 세트를 적용해야 합니다. 이더넷 회선 인터페이스에 TestFilter 세트를 적용하는 예는 다음과 같습니다.

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

이러한 규칙을 활성화한 후에는, TestFilter 세트가 허용하는 IP 통신만이 ETH237에서 허용됩니다.

주: 시스템이 인터페이스의 활성화된 필터 끝에 디폴트 DENY ALL TRAFFIC 규칙을 추가합니다. 따라서 iSeries를 구성하는 인터페이스에 규칙을 적용할 때는 사용자 고유의 워크스테이션이나 iSeries를 구성할 수도 있는 다른 누군가의 워크스테이션을 허용하는 것이 매우 중요합니다. 그러지 않을 경우, iSeries와의 통신이 유실됩니다.

다음과 같이 필터 인터페이스 명령문에 복수 세트를 적용할 수도 있습니다.

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

이들 세트는 필터 인터페이스 명령문에 나열된 순서대로 처리됩니다(set1, set2, 그리고 마지막에 set3). 각 세트에 있는 필터는 파일에 있는 순서대로 처리됩니다. 이는 서로 다른 세트 간의 필터 순서 지정은 아무런 관련이 없음을 의미합니다. 필터 순서는 필터가 동일한 세트에 있을 때에만 문제가 됩니다.

IP 패킷 헤더

IP, TCP, UDP, ICMP 헤더의 여러 부분을 참조할 때 필터 규칙을 작성할 수 있습니다. 다음은 IP 패킷 헤더를 구성하며 필터 규칙에서 참조되는 필드 리스트입니다.

- 소스 IP 주소
- 프로토콜(예: TCP, UDP)
- 목적지 IP 주소
- 소스 포트
- 목적지 포트
- IP 데이터그램 방향(인바운드, 아웃바운드 또는 두 방향 모두)
- TCP SYN 비트

예를 들어, 목적지 IP 주소, 소스 IP 주소, 방향(인바운드)을 기초로 패킷을 필터링하는 규칙을 작성하여 활성화할 수 있습니다. 이 경우에 시스템은(기점 및 목적지 주소에 따라) 모든 수신 패킷을 해당 규칙과 일치시킵니다. 그리고 나서 시스템이 사용자가 규칙에 지정한 조치를 취합니다. 필터 규칙에 허용되지 않는 패킷은 삭제합니다. 이것을 디폴트 거부 규칙이라고 합니다.

주: 시스템은 실제 인터페이스에서 적어도 하나의 규칙이 활동할 경우에만 디폴트 거부 규칙을 패킷에 적용합니다. 이 규칙은 사용자가 정의하거나 iSeries Navigator가 생성합니다. 필터 규칙이 인바운드 통신을 허용하는지 혹은 아웃바운드 통신을 허용하는지와 무관하게, 시스템은 두 방향에서 디폴트 거부 규칙을 구현합니다. 실제 인터페이스에서 활동하는 필터 규칙이 없으면 디폴트 거부 규칙이 작동하지 않습니다.

IP 필터 규칙으로 NAT 규칙 구성

NAT와 IP 필터링은 서로 독립적으로 작동합니다. 이 경우에도 IP 필터링과 함께 NAT를 사용할 수 있습니다. NAT 규칙만 적용하도록 선택하면 시스템이 단지 주소 변환을 수행합니다. 마찬가지로, IP 필터 규칙만 적용하기로 하면 시스템은 IP 통신만을 필터링합니다. 그러나 두 가지 유형의 규칙을 모두 적용하면, 시스템이 주소를 변환하고 필터링 작업을 수행합니다. NAT와 필터링을 함께 사용하면 규칙은 특정 순서로 발생합니다. 인바운드 통신에서는 NAT 규칙을 먼저 처리합니다. 아웃바운드 통신에서는 필터 규칙을 먼저 처리합니다.

NAT와 필터 규칙을 작성하기 위해 별도의 파일을 사용하는 것을 고려할 수 있습니다. 이와 같이 하는 것이 반드시 필요한 것은 아니더라도 쉽게 사용자 필터 규칙을 읽거나 문제를 해결할 수 있게 도와줍니다. 어느 방법(별도로 또는 함께)에서나 같은 오류가 발생합니다. NAT와 필터 규칙에 대해 별도의 파일을 사용하는 경우 두 가지 규칙 세트를 모두 활성화할 수 있습니다. 그러나, 사용자의 규칙이 서로간에 방해가 되지 않는지 확인하십시오.

NAT와 필터링 규칙을 동시에 활성화하려면 *포함* 피처를 사용해야 합니다. 예를 들어 파일 A를 필터 규칙으로 파일 B를 NAT 규칙으로 작성할 경우가 있습니다. 이때 모든 사용자 규칙을 다시 작성하지 않고 파일 B의 내용을 파일 A에 포함시킬 수 있습니다. 이렇게 하는 방법에 대한 자세한 정보는 패킷 규칙에 있는 포함 파일을 참조하십시오.

복수 IP 필터 규칙 구성

필터 규칙을 작성할 때 하나의 필터가 하나의 규칙 명령문을 참조합니다. 그리고 하나의 세트가 하나의 필터 그룹을 참조합니다. 세트 안의 필터들은 물리적인 순서에 따라 맨 위에서 아래로 처리됩니다. 마찬가지로 여러 개의 세트 역시 FILTER_INTERFACE 명령문에서의 물리적인 순서에 따라 처리됩니다.

다음은 하나의 세트에 세 개의 필터 명령문이 들어 있는 예입니다. 이 세트를 참조할 때마다 세 개의 규칙을 모두 포함시키십시오. 세트 하나에 필터 규칙을 모두 포함시키는 것이 가장 쉽습니다.

```
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
```

위장 보호

누군가가 사용자 고유 네트워크에서 일반적으로 신뢰되는 시스템인 것처럼 가장하여 사용자 시스템에 액세스하려고 할 때 Spoofing이 발생합니다. 이러한 유형의 침입으로부터 공용 네트워크에 링크된 인터페이스를 보호하는 것이 좋습니다. iSeries Navigator의 패킷 규칙 편집기에 있는 위장 보호 마법사를 완료함으로써 spoofing으로부터 보호할 수 있습니다. 이 마법사는 침입당하기 쉬운 인터페이스에 규칙을 할당하는데 도움이 됩니다. 규칙이 활성화되면, 공용(신뢰할 수 없는) 네트워크의 시스템은 사설망(신뢰할 수 있는)의 신뢰할 수 있는 머신으로 가장할 수 없습니다.

제 5 장 패킷 규칙 계획

네트워크 자원을 인터넷에 연결하기 전에, 보안 계획을 세우고 관련이 있는 잠재적 보안 위험에 대해 잘 알고 있어야 합니다. 일반적으로 내부 네트워크 구성을 설명하는 문서 및 인터넷의 사용 계획에 필요한 자세한 정보를 수집해야 합니다. 이러한 정보의 수집 결과를 토대로 보안 요구사항을 정확하게 평가할 수 있습니다. 주제 IBM SecureWay: iSeries 및 인터넷에서는 전체 네트워크 보안 계획을 작성하는데 필요한 세부사항을 제공합니다. 계획의 일부에 패킷 규칙 사용이 포함될 경우, 패킷 규칙을 구성하는데 필요한 모든 정보를 수집하려면 다음 주제를 참조해야 합니다.

- **패킷 규칙: 사용자 권한 요구사항**
  패킷 규칙을 관리하는 적절한 권한이 있는지 확인하십시오.
- **패킷 규칙: 시스템 요구사항**
  사용자의 iSeries가 패킷 규칙을 사용하기 위한 최소 시스템 요구사항을 충족시키는지 확인하십시오.
- **패킷 규칙: 작업용지 계획**
  이 작업용지를 사용하면 패킷 규칙을 구성하는데 필요한 정보를 수집하는데 도움이 됩니다.

계획을 세웠으면 패킷 규칙 구성을 시작할 수 있습니다.

패킷 규칙: 사용자 권한 요구사항

iSeries에서 패킷 규칙을 관리하려면 적절한 권한이 있어야 합니다. 사용자 프로파일에 *IOSYSCFG 특수 권한이 있어야 합니다. QSECOFR 사용자 ID 또는 *SECOFR 유형의 사용자 ID로 패킷 규칙을 관리하고자 하거나 또는 *ALLOBJ 권한이 있는 경우에는 이것으로 충분합니다. 그렇지 않은 경우에는 다음 디렉토리, 파일 및 QSYS 사용자 ID에 대한 권한이 필요합니다.

1. 오브젝트 권한 *RXW와 자료 권한 OBJMGT를 다음 세 파일에 추가하십시오.
   /QIBM/ProdData/OS400/TCPIP/PacketRules/Template4PacketRules.i3p
   /QIBM/ProdData/OS400/TCPIP/PacketRules/Template4PacketRules.txt
   /QIBM/ProdData/OS400/TCPIP/PacketRules/Template4PacketRules.tcpipml
2. 오브젝트 권한 *RWX를 다음 디렉토리에 추가하십시오.
   /QIBM/UserData/OS400/TCPIP/PacketRules
   /QIBM/UserData/OS400/TCPIP/OpNavRules
3. 오브젝트 권한 *RWX를 다음 파일에 추가하십시오.
   /QIBM/UserData/OS400/TCPIP/OpNavRules/VPNPolicyFilters.i3p
   /QIBM/UserData/OS400/TCPIP/OpNavRulesPPPFilters.i3p
4. QSYS는 새로 작성된 규칙 파일을 소유하므로 QSYS 프로파일에 대한 ADD 권한도 필요합니다.

이들은 패킷 규칙 편집기가 사용하는 디폴트 디렉토리 및 파일입니다. 위에 나열된 디렉토리 이외의 디렉토리에 파일을 저장하고자 할 경우에는 해당 디렉토리에 대한 권한이 필요합니다.

패킷 규칙: 시스템 요구사항

패킷 규칙이 사용자의 iSeries에서 제대로 기능하려면 다음이 필요합니다.

1. OS/400® 버전 5 릴리스 2(5722-SS1) 이상
2. Windows®용 iSeries Access(5722-XE1) 및 iSeries Navigator
   - iSeries Navigator의 네트워크 구성요소
3. TCP/IP(5722-TC1)는 IP 인터페이스, 라우트, 로컬 호스트명, 로컬 도메인명을 포함하여 구성해야 합니다.

주: TCP/IP, 네트워킹 또는 IP 주소에 대해 이해하지 못한 경우, TCP/IP Tutorial and Technical Overview ®: V4 TCP/IP: More Cool Things Than Ever를 참조하십시오. 그리고 AS/400

패킷 규칙: 작업용지 계획

패킷 규칙 계획 작업용지를 사용하여 패킷 규칙 사용 계획에 대한 자세한 정보를 수집하십시오. 보안 요구를 정확하게 찾아내기 위해 이 정보가 필요합니다. 이 정보는 패킷 규칙을 구성하는 데에도 사용할 수 있습니다. 시스템에서 패킷 규칙을 구성하기 전에 각 질문에 응답해야 합니다.

패킷 규칙 사용에 대한 계획을 작성하는데 이 정보가 필요합니다	**응답**
네트워크와 연결의 배치는 어떻게 됩니까? 그림으로 그려 보여주십시오.	
사용할 라우터와 IP 주소는 무엇입니까?	
시스템을 통해 전달되는 TCP/IP 통신을 제어하기 위해 사용할 규칙은 무엇입니까? 나열하는 각 규칙에 대해 TCP/IP 통신 흐름의 다음과 같은 측면을 지정하십시오. • 허용 또는 거부할 서비스 유형(예: HTTP, FTP 등) • 서비스에 잘 알려진 포트 번호 • 통신 방향 • 통신의 특성(응답 통신인지 아니면 시작 통신인지) • 통신의 IP 주소(소스 및 목적지)	
다른 주소로 맵핑하거나 다른 주소 뒤에 숨길 IP 주소는 어떤 것입니까? (네트워크 주소 변환을 사용할 경우에만 이 리스트가 필요합니다.)	

제 6 장 패킷 규칙 구성

시스템에 패킷 규칙을 구성하기 위한 계획을 세운 후에는 실제로 패킷 규칙을 작성하고 적용할 수 있습니다. 패킷 규칙 편집기 온라인 도움말에서 구체적인 단계별 정보를 찾을 수 있습니다. 그러나 다음 체크 리스트에서 패킷 규칙을 활성화할 때 패킷 규칙이 제대로 기능하도록 하기 위해 완료해야 하는 타스크의 개요를 제공합니다.

__ 1. 패킷 규칙 편집기 액세스
iSeries Navigator에 있는 패킷 규칙 편집기를 액세스하려면 다음 지침을 따르십시오.

__ 2. 패킷 규칙 편집기(V5R2 이상)의 일부로서 제공되는 마법사를 사용하여 규칙 파일을 작성하십시오.

- **서비스 허용 마법사**
  이 마법사는 주어진 TCP 또는 UDP 서비스에 필요한 통신을 허용하는 패킷 규칙 명령문 세트를 생성하고 삽입합니다.
- **위장 보호 마법사**
  이 마법사는 이 서버로 들어오기 위해 사용해야 하는 인터페이스가 아닌 다른 인터페이스 상의 모든 통신을 거부하는 패킷 규칙 명령문 세트를 생성하고 삽입합니다.
- **주소 변환 마법사**
  이 마법사는 맵 또는 숨김 패킷 규칙 명령문 세트를 생성하고 삽입합니다.

구성하고자 하는 규칙 유형에 따라, 이 세 개의 마법사가 사용자를 대신하여 필요한 모든 필터 및 NAT 명령문을 작성합니다. 패킷 규칙 편집기에 있는 **마법사** 메뉴에서 마법사에 액세스할 수 있습니다. 규칙을 직접 작성하고자 할 경우에는 체크 리스트의 다음 항목으로 가십시오.

__ 3. 주소 및 서비스 정의
복수 규칙을 작성할 주소 및 서비스의 별명을 작성하십시오.

주: NAT 규칙을 작성할 경우 *반드시* 주소를 정의해야 합니다.

__ 4. NAT 규칙 작성
NAT를 사용할 *경우에만* 이 타스크를 수행하십시오.

__ 5. 필터 규칙 작성
이 시스템이 관리하는 네트워크에 적용할 필터를 정의하십시오.

__ 6. 포함 파일
"마스터" 규칙 파일에 포함시킬 임의의 추가 파일을 지정하십시오. 새 규칙 파일에 다시 사용할 기존 규칙 파일이 있을 *경우에만* 이 타스크를 완료하십시오.

__ 7. 인터페이스 정의
규칙을 인터페이스에 적용시키십시오.

__ 8. 주석 작성
각 규칙 파일이 수행하는 작업을 설명하십시오.

__ 9. 규칙 파일 확인
오류 및 문제점 없이 규칙이 활성화되는지 확인하십시오.

__ 10. 규칙 파일 활성화
패킷 규칙이 기능하도록 하려면 이들을 활성화해야 합니다.
__ 11. 패킷 규칙 관리
패킷 규칙을 활성화한 후에는 이들을 정기적으로 관리하여 시스템 보안을 유지보수해야 합니다. 이 주제에는 규칙 파일 편집, 패킷 규칙 조치 저널링 및 감사, 그리고 백업 및 복구 추가 정보 및 기술에 대한 정보가 들어 있습니다.

패킷 규칙 액세스

iSeries 자원에 대한 작업을 가능하게 하는 그래픽 인터페이스인 iSeries Navigator를 통해 패킷 규칙 편집기에 액세스해야 합니다. 패킷 규칙 편집기를 사용하여 시스템에 패킷 규칙을 작성하십시오. 새 파일을 작성하거나, 기존 파일을 편집하거나 또는 시스템에서 제공하는 샘플 파일로 작업할 수 있습니다.

패킷 규칙 편집기에 액세스하려면 다음 단계를 수행하십시오.
1. iSeries Navigator에서, **서버 -> 네트워크 -> IP 정책**을 펼치십시오.
2. **패킷 규칙**을 마우스 오른쪽 클릭하여 **규칙 편집기**를 선택하십시오.

이 주제의 패킷 규칙 구성 섹션에 기술된 각 타스크를 완료하는 방법에 대한 단계별 지침은 온라인 도움말을 참조하십시오.

주소 및 서비스 정의

패킷 규칙을 작성할 때 규칙을 적용시킬 IP 주소와 서비스를 지정해야 합니다. **정의된 주소**는 기호명이 주어진 인터페이스 스펙입니다. 표시하고자 하는 주소가 주소 범위, 서브네트, 지점 간 ID 리스트 또는 비연속 주소일 때는 주소를 정의해야 합니다. 맵 주소 변환 규칙을 작성하고자 할 때 정의된 주소 명령문이 필요합니다. 표시하고자 하는 주소가 필터 명령문에 있는 단일 IP 주소이면 정의된 주소 명령문이 필요하지 않습니다. **서비스 별명**은 서비스를 정의하여 원하는 수의 필터에 이들을 재사용할 수 있도록 합니다. 서비스 별명은 또한 서로 다른 서비스 정의의 목적을 추적합니다.

주소와 서비스 별명을 정의하는 것은 패킷 규칙 작성을 쉽게 해 줍니다. 규칙을 작성할 때에는 특정 주소나 서비스 세부사항보다는 주소 별명이나 서비스 별명을 참조하십시오. 필터 규칙에 별명을 사용하면 다음과 같은 장점이 있습니다.

1. 인쇄 오류의 위험을 최소화합니다.
2. 작성해야 할 필터 규칙 수를 최소화합니다.

예를 들어, 인터넷 액세스를 필요로 하는 31명의 사용자가 네트워크에 있습니다. 하지만 이 사용자들을 웹 액세스로만 제한시키려고 합니다. 이 경우 필요한 필터 규칙을 작성하는 방법에 대해 두 가지의 선택이 있습니다.

1. 각 사용자의 IP 주소에 대해 하나의 필터 규칙을 정의합니다.
2. 주소를 정의하여 사용자를 대표하는 전체 주소 세트에 대해 하나의 별명을 작성합니다.

첫번째 선택은 사용자가 규칙 파일을 위해 수행해야 하는 유지보수의 작업량을 증가시킬 뿐만 아니라 인쇄 오류의 가능성도 증가시킵니다. 두 번째 선택을 사용하면 두 개의 필터 규칙을 작성해야 합니다. 규칙이 적용되는 전체 주소 세트를 참조하려면 각 규칙의 별명을 사용하십시오.

또한 서비스별로 별명도 작성할 수 있으며 주소 별명과 같은 방법으로 그 별명을 사용할 수도 있습니다. 서비스 별명이 사용자가 선택하려는 TCP, UDP, ICMP 범주를 정의합니다. 사용하려는 소스 및 목적지 포트를 선택하십시오.

주: NAT를 사용하려면 *반드시* 주소를 정의해야 합니다. NAT 규칙은 정의된 주소만 가리킬 수 있습니다.

주소, 서비스 별명 및 ICMP 서비스를 정의하는 방법에 대한 단계별 지침은 패킷 규칙 편집기 온라인 도움말을 참조하십시오.

다음 단계

네트워크 주소 변환을 사용할 계획이면 NAT 규칙 작성으로 가십시오. 그렇지 않은 경우에는 사설망으로 들어오고 나가는 IP 통신을 필터링하는 IP 필터 규칙 작성으로 가십시오.

NAT 규칙 작성

NAT를 사용하기로 결정한 경우, 사용하려는 IP 주소에 대한 별명을 *정의해야 합니다*. 표준 32비트 주소 표기법으로는 NAT 규칙을 작성할 수 없습니다. 193.112.14.90과 같은 실제 주소를 지정하기 보다는 *이름*별 193.112.14.90을 참조해야 합니다. 시스템은 정의된 이름을 해당 주소와 연관시킨 후 변환시킵니다. 따라서 시스템이 NAT 규칙을 주소에 적용하기 전에 주소를 정의해야 합니다.

패킷 규칙 편집기는 두 가지 유형의 NAT 규칙을 작성하도록 허용합니다. 하나의 유형으로 주소를 숨길 수 있으며 다른 유형으로 주소를 맵핑할 수 있습니다.

주소 숨기기

개인 주소를 공개적으로 보지 못하게 숨기기를 원하면 주소를 가려야 합니다. 숨긴 주소 규칙을 사용하면 여러 개의 내부 주소를 하나의 공개 IP 주소 뒤에 감출 수 있습니다. 이 NAT 유형을 *가면* NAT라고도 합니다.

주소 맵핑

하나의 공용 IP 주소에서 하나의 내부 주소로 통신을 라우트하려면 주소를 맵핑해야 합니다. 이 NAT 유형을 *정적* NAT라고도 합니다.

주소를 숨기거나 맵핑하는 방법에 대한 단계별 지침은 패킷 규칙 편집기 온라인 도움말을 참조하십시오.

다음 단계

네트워크로 들어오고 나가는 통신을 필터링하려면 IP 필터 규칙 작성으로 가십시오. 그러지 않을 경우에는 패킷 규칙에 주석 작성으로 가십시오.

IP 필터 규칙 작성

필터를 작성할 때 시스템으로 송수신되는 IP 통신 흐름을 제어할 규칙을 지정하십시오. 사용자가 정의하는 규칙이 시스템에 액세스를 시도하는 패킷의 허용 여부를 지정합니다. 시스템이 IP 패킷 헤더의 정보 유형을 기초로 IP 패킷을 지정합니다. 또한 시스템이 적용하도록 지정한 조치에 IP 패킷을 지정합니다. 특정 규칙에 부합하지 않는 패킷은 삭제됩니다. 이러한 자동 삭제 규칙을 *디폴트 거부 규칙*이라고 합니다. 파일 끝에 위치한 디폴트 거부 규칙은 패킷이 앞에 오는 규칙의 기준과 일치하지 않을 때마다 자동으로 활성화됩니다. 활성화를 위해서는 디폴트 거부 규칙에 대해 최소한 하나의 필터 규칙이 활동하고 있어야 합니다.

주: iSeries를 구성하는 인터페이스에 규칙을 적용할 때는 사용자 고유의 워크스테이션이나 iSeries를 구성할 수도 있는 다른 누군가의 워크스테이션을 허용하는 것이 매우 중요합니다. 그러지 않을 경우, iSeries와의 통신이 유실됩니다. 이러한 상황이 발생하면 오퍼레이터 콘솔과 같은 여전히 연결성을 가지는 인터페이스를 사용하여 iSeries에 로그온해야 합니다. RMVTCPTBL 명령을 사용하여 시스템에서 모든 필터를 제거하십시오.

필터 규칙을 작성하기 전에 네트워크 주소 변환(NAT)을 사용할 것인지를 결정해야 합니다. NAT 규칙을 사용할 경우 *반드시* 주소와 서비스를 정의해야 합니다. NAT는 정의된 주소가 필요한 유일한 기능입니다. 그러나 다른 기능에 대해서도 이 프로세스를 사용할 수 있습니다. 주소와 서비스를 정의하면 인쇄 오류의 가능성을 최소화하는 것은 물론 작성해야 할 규칙의 수를 줄일 수 있습니다.

다음은 필터 규칙을 작성할 때 오류를 최소화하고 효율을 최대화할 수 있는 몇 가지 방법입니다.

- **한 번에 하나의 필터 규칙을 정의하십시오.** 예를 들어 텔넷에 대한 모든 허가를 동시에 작성하십시오. 이 방법으로 규칙을 참조할 때마다 연관 규칙들을 그룹화할 수 있습니다.
- **필터 규칙은 파일에 나오는 순서대로 처리됩니다.** 규칙을 작성할 때 적용하려는 방식에 따라 규칙을 정렬하십시오. 순서가 맞지 않으면 패킷이 의도한대로 처리되지 않으므로 시스템이 공격을 받기 쉽습니다. 보다 쉽게 처리하려면 다음 조치를 고려하십시오.
  1. 물리적으로 파일에 세트를 정의한 것과 같은 순서로 FILTER_INTERFACE문에 필터 세트명을 입력하십시오.
  2. 세트 순서와 관련된 문제를 방지할 수 있도록 하나의 세트에 모든 필터 규칙을 포함시키십시오.
- **처리를 진행하면서 각 규칙의 구문을 확인하십시오.** 이것이 모든 규칙을 한 번에 디버깅하는 것보다 쉽고 빠릅니다.
- **논리적으로 상호 연관된 파일 그룹 세트명을 작성하십시오.** 한 번에 하나의 규칙 파일만 사용되므로 이것은 매우 중요합니다. 아래 예를 참조하십시오.
- **허용할 데이터그램에 대해서만 필터 규칙을 작성하십시오.** 그 이외의 것은 자동 거부 규칙에 따라 무시됩니다.
- **통신량이 많은 볼륨에 대한 규칙을 먼저 작성하십시오.**

예: 위에 나오는 *세트명 작성* 추가 정보를 참조하십시오. 전체 사용자가 아닌 일정한 수의 내부 사용자들에게 텔넷 액세스를 허용할 수 있습니다. 이 규칙을 더 쉽게 관리하기 위해 각 규칙에 `TelnetOK` 세트명을 할당할 수 있습니다. 두 번째 기준은 특정 인터페이스를 통해 텔넷을 허용하고 다른 모든 인터페이스로부터 텔넷 통신

을 차단할 수 있게 해 줍니다. 이 경우 텔넷 액세스를 완전히 차단하는 두 번째 규칙 세트를 작성해야 합니다. 이 규칙에는 TelnetNever 세트명을 할당할 수 있습니다. 세트명을 작성함으로써 규칙의 목적을 더 쉽게 구별할 수 있습니다. 또한 특정 세트에 적용시킬 인터페이스를 쉽게 판별할 수 있습니다. 위에 나오는 모든 추가 정보를 사용하여 간편한 필터 작성 프로세스를 만들 수 있습니다.

IP 필터 규칙을 작성하는 방법에 대한 단계별 지침은 패킷 규칙 편집기 온라인 도움말을 참조하십시오.

다음 단계

필터를 작성한 후에는 필터 명령문에 하나 또는 여러 개의 파일을 포함시키고자 할 수도 있습니다. 그렇지 않은 경우에는, 규칙이 적용되는 인터페이스를 정의하십시오.

IP 필터 인터페이스 정의

시스템이 어떤 인터페이스에 어떤 필터 규칙을 적용하는지를 설정하기 위해서는 *반드시* 필터 인터페이스를 정의해야 합니다. 필터 인터페이스를 정의하기 전에 시스템이 여러 가지 인터페이스에 적용할 필터를 작성하십시오. 주소를 정의하도록 선택하면(인터페이스를 정의할 때) 이름별로 주소를 참조하십시오. 주소를 정의하지 않도록 선택하면(인터페이스를 정의할 때) IP 주소별로 참조하십시오.

필터를 작성할 때 여러 필터를 하나의 세트에 포함시킬 수 있습니다. 그런 다음에 이 세트를 FILTER_INTERFACE 명령문에 추가합니다. 명령문에서 사용되는 세트명은 필터 명령문에서 정의한 세트명이어야 합니다. 예를 들어, ALL이라는 세트명이 있고 모든 필터가 이 세트에 들어 있는 경우, 필터가 제대로 기능하도록 하려면 세트명 ALL을 필터 인터페이스 명령문에 포함시켜야 합니다. 하나의 세트에 여러 필터를 포함시킬 수 있을 뿐만 아니라, 하나의 FILTER_INTERFACE문에 복수 세트를 포함시킬 수도 있습니다.

인터페이스를 정의하기 위해서는 먼저 사용하려는 모든 추가 파일을 포함시켜야 합니다. 그런 다음, 인터페이스를 정의할 수 있습니다. 필터 세트는 필터 인터페이스 명령문에 지정된 순서로 적용된다는 것을 기억하십시오. 따라서 파일에 물리적으로 세트를 정의한 것과 같은 순서로 FILTER_INTERFACE문에 필터 규칙이 나와야 합니다.

필터 인터페이스를 정의하는 방법에 대한 단계별 지침은 패킷 규칙 편집기 온라인 도움말을 참조하십시오.

다음 단계

필터 인터페이스를 정의한 후 다음 단계는 패킷 규칙에 주석 작성입니다.

패킷 규칙에 파일 포함

패킷 규칙 편집기에 있는 *포함* 피처를 사용하여 시스템에 있는 둘 이상의 패킷 규칙 파일을 활성화할 수 있습니다. 복수 파일을 사용하면 규칙에 대한 작업이 훨씬 더 쉽습니다. 특히 여러 개의 인터페이스에 대한 통신을 제어하기 위해 많은 규칙을 사용해야 할 경우에 유용합니다. 예를 들어 여러 개의 인터페이스에 하나의 규칙 그룹을 사용할 수 있습니다.

이와 같은 경우 이 그룹을 개별 파일에 작성할 수 있습니다. 다른 파일에 규칙을 사용하려고 할 때 매번 다시 작성하지 않고 마스터 파일에 규칙을 포함시킬 수 있습니다. 마스터 파일은 언제든지 활성화시킬 수 있는 단 하나의 파일입니다. 규칙을 마스터 파일에 추가하려는 경우 포함 피처만 사용해야 합니다.

포함 파일을 작성할 때 인터페이스에 대한 NAT 규칙을 그 인터페이스에 대한 필터 규칙과 분리시킬 수 있습니다. 그러나 일정 시점에서는 하나의 파일만 사용할 수 있습니다.

새로운 규칙 파일을 작성할 때 모든 기존 파일을 신규 파일의 일부로 포함시킬 수 있습니다. 이를 위해서는 먼저 사용하려는 신규 필터 규칙을 작성해야 합니다. 규칙을 작성할 때마다 유형별로 규칙을 파일(그룹화)해야 합니다. 이 방법에는 전에 사용했던 규칙을 다시 작성할 필요가 없습니다. 필요에 따라 규칙을 포함시키거나 제거할 수 있습니다.

규칙에 파일을 포함시키는 방법에 대한 단계별 지침은 패킷 규칙 편집기 온라인 도움말을 참조하십시오.

다음 단계

사용하려는 모든 추가 규칙 파일을 포함시킨 후 다음 단계는 IP 필터 인터페이스 정의입니다.

패킷 규칙에 주석 작성

규칙 파일에 관해 주석을 작성하는 것은 매우 중요합니다. 규칙이 작업하는 방식을 기록하려고 합니다. 예를 들어 특정 규칙을 허용하거나 거부하는 항목을 기록할 수 있습니다. 이와 같은 정보로 인해 나중에 많은 시간을 절약할 수 있습니다. 보안 누출 문제를 신속하게 정정해야 할 경우 주석을 사용하여 기억을 되살릴 수 있습니다. 충분한 시간을 갖고 규칙의 의미를 이해하지 못할 수 있으므로 광범위하게 주석을 사용하십시오.

패킷 규칙 작성 및 활성화와 관련된 각 대화에는 **설명** 필드가 있습니다. 이것은 주석을 작성하기 위해 예약되어 있는 필드입니다. 시스템은 사용자가 이 필드에 기록하는 모든 것을 무시합니다. 규칙 작성 프로세스의 각 단계에서 주석 필드를 사용할 수도 있습니다. 이와 같이 하면 중요한 주석을 작성해야 하는 것을 쉽게 잊지 않을 것입니다. 주석 작성 프로세스를 기억하고 있을 때 주석을 작성하는 것이 가장 좋습니다. 그러나 모든 규칙을 작성할 때까지 기다릴 수도 있습니다.

규칙 파일에 주석을 작성하는 방법에 대한 단계별 지침은 패킷 규칙 편집기 온라인 도움말을 참조하십시오.

다음 단계

이 단계 이전의 각 패킷 규칙 구성 단계를 완료했으면 다음은 패킷 규칙을 저장하고 검증하는 단계입니다.

패킷 규칙 확인

규칙을 활성화하기 전에 항상 규칙을 검증해야 합니다. 이러한 작업은 규칙이 문제점 없이 활성화되도록 합니다. 패킷 규칙을 검증할 때, 시스템은 패킷 규칙에 구문 및 의미상의 오류가 있는지 점검하고 패킷 규칙 편집기의 맨 아래에 있는 메시지 창에 결과를 보고합니다. 특정 파일 및 행 번호와 연관된 오류 메시지가 있으면, 해당 오류를 마우스 오른쪽 단추로 클릭하고 **행 찾아 가기**를 선택하여 편집 중인 파일에서 해당 오류를 강조표시할 수 있습니다.

확인 기능을 사용하기 전에 눈에 보이는 오류를 검사하기 위해 패킷 규칙 보기를 고려할 수 있습니다. 구문상의 오류가 있는 규칙은 활성화시킬 수 없습니다. 확인 기능은 구문상의 특성에 관한 오류를 검사합니다. 사용자가 규칙을 올바로 정렬했는지를 시스템이 확인하는 것은 불가능합니다. 따라서 규칙 순서를 수동으로 확인해야 합니다. 패킷 규칙은 순서 종속적이며, 이는 적용되는 순서대로 규칙을 정렬해야 함을 의미합니다. 규칙을 틀리게 정렬하면 의도한 결과가 나오지 않습니다. 규칙을 활성화하기 전에 규칙이 올바른지 그리고 적용할 방식대로 정렬시켰는지 확인하십시오.

패킷 규칙 검증 방법에 대한 단계별 지침은 패킷 규칙 편집기 온라인 도움말을 참조하십시오.

경고 메세지: 사용자가 필터 규칙을 활성화할 때마다 시스템이 자동으로 이 규칙을 확인합니다. 여러 가지 경고 및 오류 메세지가 나올 수 있습니다. 경고 메세지는 단지 정보를 위한 것으로서 확인 프로세스를 중단시키지 않습니다. 모든 메세지를 주의 깊게 읽어보십시오. 확인이나 활성화가 완료되었음을 표시하는 하나의 메세지가 나옵니다. 심각한 오류가 있으면 마지막 문장에 규칙 로드에 실패했다는 내용이 나올 수 있습니다.

다음 단계

규칙이 성공적으로 검증되면 그 다음 단계는 규칙을 활성화하는 것입니다.

패킷 규칙 활성화

작성한 패킷 규칙을 활성화하는 것이 패킷 규칙을 구성하는 마지막 단계입니다. 규칙이 기능하도록 하려면 작성한 규칙을 활성화(로드)해야 합니다. 그러나 규칙을 활성화하기 전에 규칙이 올바른지 확인해야 합니다. 패킷 규칙을 활성화하기 전에 항상 모든 문제를 해결하십시오. 오류가 있거나 틀리게 정렬된 규칙을 활성화하면 시스템은 위험한 상황에 처할 수 있습니다. 시스템에는 사용자가 규칙을 활성화할 때 언제든지 자동으로 호출하는 확인 기능이 있습니다. 이 자동 피처는 중요한 구문 오류만 확인하므로 이 기능에만 의존해서는 안됩니다. 규칙 파일에 오류가 있는지도 항상 수동으로 확인해야 합니다.

필터 규칙을 인터페이스에 적용시키지 않으면(예: 필터링 규칙이 아닌 NAT 규칙만 사용할 때) 경고(TCP5AFC)가 표시됩니다. 이것은 오류가 아닙니다. 하나의 인터페이스를 사용하는 것인지만 확인합니다. 항상 마지막 메세지를 보십시오. 활성화가 완료되었음을 나타내는 메세지의 경우 위의 내용은 모두 경고 메세지입니다.

주: 모든 인터페이스에서 새로운 규칙을 활성화시킬 때 모든 물리적 인터페이스에서 이전의 모든 규칙이 대체됩니다. 물리적 인터페이스를 새로운 규칙에 언급하지 않은 경우에도 대체됩니다. 그러나 특정 인터페이스에 있어서 새로운 규칙을 활성화하면 그 인터페이스의 규칙들만 대체됩니다. 다른 인터페이스의 기존 규칙들은 그대로 남아 있습니다.

마지막 단계

패킷 규칙이 구성되고 활성화되면, 시스템 보안이 유지되도록 이들을 정기적으로 관리해야 합니다. 패킷 규칙을 적절히 유지보수하고 모니터하기 위해 수행할 수 있는 타스크 리스트는 이 주제의 패킷 규칙 관리 섹션을 참조하십시오.

제 7 장 패킷 규칙 관리

시스템 보안 및 패킷 규칙의 무결성을 유지보수하려면 정기적으로 다음과 같은 관리 타스크를 수행해야 합니다.

주: 특별한 언급이 없는 한, 패킷 규칙 편집기 온라인 도움말에서 이러한 타스크에 대한 구체적인 단계별 지침을 찾을수 있습니다.

- 파일 유실로부터 보호를 받으려면 패킷 규칙을 백업하십시오.
- 특정한 이유로 NAT 및 필터 규칙을 중단해야 할 경우에는 패킷 규칙을 비활성화하십시오. 그러나 규칙을 비활성화하면 네트워크가 보호받지 못하게 된다는 점을 기억하십시오.
- IP 통신이 시스템으로 들어오고 외부로 나가는 방법을 변경해야 할 때에는 패킷 규칙을 편집하십시오.
- 패킷 규칙 조치를 저널링하고 감사하여 패킷 규칙을 기록하십시오. 필요한 경우 이것은 규칙을 디버그하는 데 도움을 줍니다.
- 오류를 해결할 때 패킷 규칙을 참조하십시오.

가능한 모든 수단을 사용하여 효과적이면서 효율적인 방식으로 패킷 규칙을 관리하십시오. 시스템 보안은 정확한 현재 규칙에 따라 이루어집니다. 문제 해결을 위해 도움이 필요한 경우에는 패킷 규칙 문제 해결을 참조하십시오.

패킷 규칙 비활성화

활동 중인 패킷 규칙을 변경해야 하거나 새 규칙을 활성화하려면 먼저 현재 활동 중인 규칙을 비활성화해야 합니다. 특정 인터페이스, 지점 간 ID 또는 모든 인터페이스 및 모든 지점 간 ID의 규칙을 비활성화할 수 있습니다.

패킷 규칙을 비활성화하는 방법에 대한 단계별 지침은 패킷 규칙 편집기 온라인 도움말을 참조하십시오.

패킷 규칙 보기

필터 규칙을 활성화하기 전에 필터 규칙이 올바른지 확인해야 합니다. 작성하는 필터 규칙을 검토하여 눈에 보이는 오류가 있는지 확인할 수 있습니다. 활성화 및 테스트 이전 뿐만 아니라 인쇄 및 백업 전에도 필터 규칙을 보려는 경우가 있습니다. 규칙을 검토하는 것이 오류를 확인하는 유일한 방법은 아닙니다. 그러나 이 방법은 테스트 전에 오류를 최소화하거나 제거할 수 있는 유용한 방법입니다.

작성하는 필터 규칙을 검토하려면 인쇄를 하여 사용하십시오. 이렇게 하면 눈에 보이는 실수를 찾아낼 수 있고 추가하려고 했던(앞서 작성했던) 필터 규칙 파일들을 포함시켰는지 확인할 수 있습니다.

또한 시스템에 확인 기능이 있지만 이 기능에만 의존해서는 안됩니다. 수동으로 모든 오류를 정정하기 위해 필요한 조치를 취하십시오. 이렇게 하면 사용자의 귀중한 시간과 자원을 절약할 수 있습니다.

활동하지 않는 규칙을 보기 위해서는 패킷 규칙 편집기에서 규칙 파일을 열어야 합니다.

활동 중인 필터 규칙을 편집하려면 먼저 이들을 검토하여 어떻게 변경할 것인지 결정해야 합니다.

현재 활동 규칙을 보려면 다음 단계를 수행하십시오.

1. iSeries Navigator에서, **서버 -> 네트워크 -> IP 정책 -> 패킷 규칙**을 선택하십시오.
2. 보고자 하는 활동 중인 패킷 규칙의 인터페이스를 선택하십시오.
3. 오른쪽 분할 창에서 활성 패킷 규칙의 리스트를 보십시오.

주: 이 대화 상자에서는 규칙을 편집할 수 없습니다. 규칙 파일을 비활성화한 다음 패킷 규칙 편집기를 사용하여 규칙을 편집해야 합니다.

NAT 및 IP 필터 관리로 돌아가십시오.

패킷 규칙 편집

네트워크 보안 요구사항이 변함에 따라 새 보안 전략을 신뢰하는지 확인하려면 규칙을 편집*해야 합니다*. 그러나 활동 중인 패킷 규칙을 편집하려면 먼저 이들을 비활성화해야 합니다. 그런 다음, iSeries Navigator의 패킷 규칙 편집기를 사용하여 규칙을 필요에 따라 변경하십시오. 편집을 마친 후에는 규칙을 검증한 다음 다시 활성화하십시오.

패킷 규칙을 편집하는 방법에 대한 단계별 지침은 패킷 규칙 편집기 온라인 도움말을 참조하십시오.

패킷 규칙 백업

처음에는 필요한 것으로 생각되지 않을 수도 있으나 항상 패킷 규칙을 백업하는 것이 좋습니다. 파일을 유실할 경우 백업 복사본을 사용하면 처음부터 파일을 다시 작성하기 위해 소요되는 시간과 작업을 줄여줍니다.

다음은 유실한 파일을 대체하기 위해 사용할 수 있는 일반적인 추가 정보입니다.

필터 규칙 인쇄 출력
인쇄 출력을 가장 안전한 곳에 저장하거나 필요에 따라 정보를 다시 입력할 수 있습니다. 인쇄 출력은 또한 필터 규칙에서 오류를 탐색할 경우에도 유용합니다.

패킷 규칙을 인쇄하는 방법에 대한 단계별 지침은 패킷 규칙 편집기 온라인 도움말을 참조하십시오.

정보를 디스크에 복사
복사는 인쇄 출력에 비해 많은 장점이 있습니다. 한 예로 정보를 수동으로 다시 입력하기 보다 전자적인 방식으로 보존할 수 있습니다. 또한 하나의 온라인 소스에서 다른 소스로 정보를 전송할 수 있는 간단한 방법을 제공합니다.

주: iSeries는 정보를 플로피 디스크가 아닌 시스템 디스크에 복사합니다. 규칙 파일은 PC가 아닌 iSeries의 IFS 파일 시스템에 저장됩니다. 시스템 디스크에 저장된 자료를 보호하기 위한 백업 수단으로 디스크 보호 방법을 사용할 수도 있습니다.

iSeries를 사용할 경우에는 백업 및 회복 전략을 계획해야 합니다. 파일의 회복과 백업에 대한 자세한 정보는 백업 및 회복을 검토하십시오.

패킷 규칙 조치 저널 및 감사

패킷 규칙에는 저널링 피처가 포함됩니다. 저널링으로 NAT 및 필터링 문제를 해결할 수 있습니다. 규칙 조치 기록부를 작성할 때 저널을 사용할 수 있습니다. 이것은 규칙을 디버그하고 부분적으로 무작위로 검사할 수 있게 해 줍니다. 시스템 기록부나 저널을 검토하여 시스템으로 들어오거나 외부로 나가는 통신을 감사할 수 있습니다.

저널링 피처는 규칙별로 사용됩니다. NAT나 필터 규칙을 작성할 경우 Full 또는 Off의 저널링 옵션을 사용할 수 있습니다. 자세한 정보는 아래의 표를 참조하십시오.

옵션	정의
FULL	변환되는 모든 패킷을 기록합니다.
OFF	저널링이 발생하지 않습니다.

저널링이 켜진 경우 저널 항목이 데이터그램(NAT 또는 필터)에 적용된 각 규칙에 대해 생성됩니다. 저널 항목이 작성되지 않는 유일한 규칙은 디폴트 거부 규칙입니다. 이미 시스템에서 작성되었기 때문입니다.

이들 저널을 사용하여 iSeries에서 일반 파일을 작성하십시오. 시스템의 저널에 기록되어 있는 정보를 사용하여 시스템이 사용되는 방법을 판별할 수 있습니다. 이것은 사용자가 다양한 보안 계획 요소를 변경할 때 도움이 될 수 있습니다.

저널링 피처를 OFF로 설정하면 시스템이 해당 규칙에 대한 저널 항목을 작성하지 않습니다. 이것을 수행하도록 선택할 수 있으나 최상의 옵션이 아닐 수 있습니다. 필터 및 NAT 규칙을 작성해 본 적이 없다면 필요에 따라 FULL(기록)을 사용할 수 있습니다. 이 경우 기록부를 문제 해결 툴로 사용할 수 있습니다. 그러나 저널(기록)을 선택할 때는 신중하십시오. 저널링은 시스템의 자원에 큰 부담을 줍니다. 많은 통신량을 제어하는 규칙을 중심으로 작업하십시오.

이 저널을 보려면 다음과 같이 하십시오.

1. iSeries의 명령 프롬트에 NAT 저널의 경우 DSPJRN JRN(QIPNAT), IP 필터 저널의 경우 DSPJRN JRN(QIPFILTER)을 입력하십시오.

제 8 장 패킷 규칙 문제 해결

이 섹션에서는 일부 공통 패킷 규칙 문제를 해결할 때 도움이 될 만한 설명을 제공합니다.

- **iSeries 통신 추적** 기능을 사용하여 지정 인터페이스에 대한 모든 데이터그램 통신을 볼 수 있습니다. STRCMNTRC(통신 추적 시작)과 PRTCMNTRC(통신 추적 인쇄) 명령을 사용하여 정보를 수집한 후 인쇄하십시오.
- **NAT 및 IP 필터링 규칙 순서**가 규칙이 처리되는 방법을 판별합니다. 파일에 나오는 순서로 처리가 이루어집니다. 순서가 올바르지 않으면 의도한 대로 패킷이 처리되지 않습니다. 이렇게 하면 시스템이 침입자에 대해 무방비 상태에 놓입니다. 물리적으로 파일에 세트를 정의한 것과 같은 순서로 FILTER_INTERFACE문에 필터 세트명을 입력하십시오.

  구문상으로 올바른 필터 규칙을 작성하는 데 관한 자세한 도움말은 이 주제의 IP 필터 규칙 작성 섹션을 검토하십시오. 아래의 표에 나오는 프로세스를 기억하십시오.

인바운드 통신 프로세스	아웃바운드 통신 프로세스
1. NAT 규칙	1. IP 필터 규칙
2. IP 필터 규칙	2. NAT 규칙

- **모든 규칙 제거**는 시스템을 재설정하고 오류를 제거하는 최상의 방법입니다. iSeries에서 RMVTCPTBL(TCP/IP 표 제거) 명령을 발행하십시오. iSeries Navigator 어플리케이션을 사용할 수 없으면 이 명령으로 되돌아가 규칙을 수정할 수도 있습니다.

  주: ″TCP/IP 표 제거″ 명령을 사용하면 전에 VPN 서버(IKE 및 ConMgr)를 실행하던 경우에만 VPN 서버를 시작합니다.
- NAT를 사용 중이면 iSeries에서 TCP/IP를 구성할 때 **IP 데이터그램 이송 허용**은 필수적입니다. CHGTCPA(TCP/IP 속성 변경) 명령을 사용하여 IP 데이터그램 이송이 예로 설정되어 있는지 확인하십시오.
- **디폴트 리턴 라우트 확인**은 맵핑하거나 숨겨진 주소가 올바른지를 확인합니다. 이 주소는 iSeries로 다시 리턴 라우트시 라우트시킬 수 있어야 하며 NAT로 변환되지 않은 올바른 회선을 통해 전달합니다.

  주: iSeries가 둘 이상의 네트워크나 이 네트워크에 연결된 회선을 가지고 있으면 인바운드 통신 라우팅에 특히 주의해야 합니다. 인바운드 통신은 입력된 어느 회선에서나 처리되는 것으로서 이 회선이 인바운드 통신을 변환시키지 않는 올바른 회선이 아닐 수도 있습니다.
- EXPANDED.OUT 파일에 있는 **오류 및 경고 메시지 보기**는 규칙이 의도한 순서대로 정렬되어 있는지 확인합니다. 필터 세트를 검증하고 활성화할 때 이 필터들이 iSeries Navigator에서 생성된 규칙과 병합됩니다. 그리고 나서 EXPANDED.OUT이라는 새로운 파일에 병합 규칙이 만들어지고, 이 파일은 사용자의 규칙이 들어있는 디렉토리(보통 /QIBM)에 저장됩니다. 경고 및 오류 메세지가 이 파일을 참조합니다. 이 파일을 보려면 패킷 규칙 편집기에서 파일을 열어야 합니다.
  1. iSeries Navigator에서 패킷 규칙 편집기에 액세스하십시오.
  2. **파일** 메뉴에서 **열기**를 선택하십시오.

3. QIBM/UserData/OS400/TCPIP/PacketRules/ 디렉토리 또는 패킷 규칙을 저장한 디렉토리(디폴트가 아닌 경우)로 가십시오.
4. **파일 열기** 메뉴에서 **EXPANDED.OUT 파일**을 선택하십시오. EXPANDED.OUT 파일이 표시됩니다.
5. 이 파일을 선택하고 **열기**를 클릭하십시오.

EXPANDED.OUT 파일은 정보용입니다. 편집할 수 없습니다.

제 9 장 패킷 규칙 관련 정보

아래 리스트는 IP 필터링 및 NAT에 대한 추가 정보를 제공하는 IBM 매뉴얼 및 레드북™(PDF 형식)입니다.

매뉴얼

- iSeries **보안-팁 및 추가 정보** (약 254 페이지)
  이 PDF 서적에서는 iSeries에서 보안을 향상시키는 방법에 대한 고급 정보를 제공합니다.

레드북

- **TCP/IP Tutorial and Technical Overview**
  TCP/IP 네트워크와 관련된 보안 문제에 대한 정보를 찾으십시오.

- **AS/400: TCP/IP: More Cool Things Than Ever**
  NAT 및 IP 패캣 필터링을 설명하는 몇몇 시나리오를 찾으십시오.

워크스테이션에 보기 또는 인쇄용으로 PDF를 저장하려면 다음과 같이 하십시오.

1. 브라우저에서 PDF를 마우스 오른쪽 클릭하십시오(링크 위에 놓고 오른쪽 클릭).
2. **다른 이름으로 목표 저장**을 클릭하십시오.
3. PDF를 저장할 디렉토리로 이동하십시오.
4. **저장**을 클릭하십시오.

이러한 PDF를 보거나 인쇄하기 위해 Adobe Acrobat Reader가 필요한 경우,Adobe 웹 사이트 (www.adobe.com/prodindex/acrobat/readstep.html) 에서 사본을 다운로드할 수 있습니다.

Printed in U.S.A