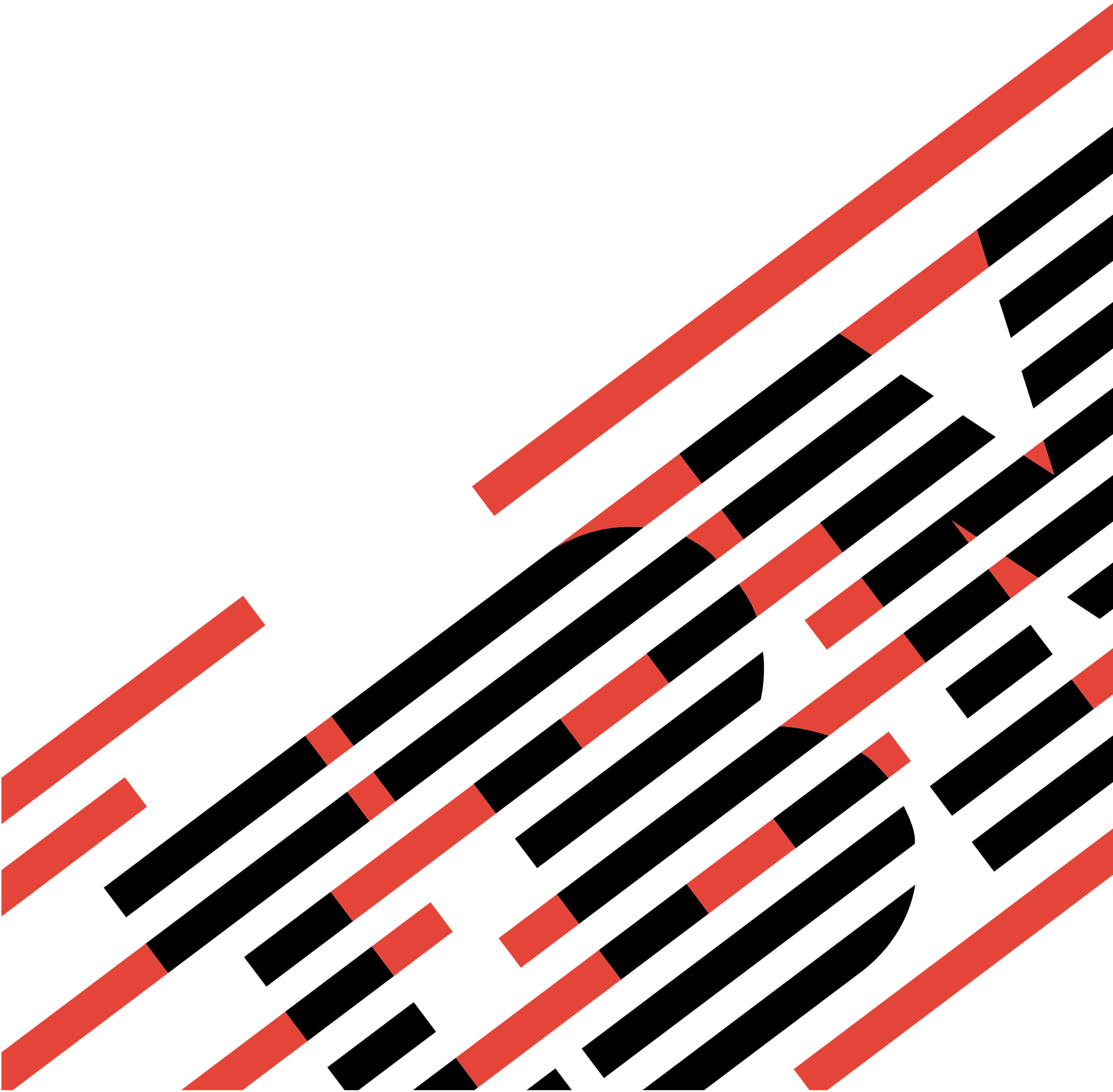
IBM

eserver

iSeries

VPN(가설 사설망)



IBM

@server

iSeries

VPN(가설 사설망)

목차

VPN(가상 사설망)

VPN(가상 사설망)을 사용하면 회사 사설 인트라넷을 인터넷과 같은 기존 공용 네트워크 구조를 통해 안전하게 확장할 수 있습니다. VPN을 사용하면 인증 및 자료 비밀 유지와 같은 중요한 보안 피처를 제공하면서 네트워크 통신을 제어할 수 있습니다.

OS/400 VPN은 선택적으로 설치 가능한 iSeries Navigator 구성요소로, OS/400용 그래픽 사용자 인터페이스(GUI)입니다. AS/400 VPN을 사용하면 호스트와 게이트웨이의 임의 조합 사이에서 보안 단말 경로를 작성할 수 있습니다. OS/400 VPN은 인증 메소드, 암호화 알고리즘 및 기타 예방책을 사용하여 두 연결 종료점간에 송신된 자료가 보안 상태로 있도록 합니다.

VPN은 TCP/IP 계층 통신 스택 모델의 네트워크층이 실행됩니다. 특히, VPN은 IP 보안(IPSec) 개방형 구조를 사용합니다. IPSec은 강력하고 안전한 가상 사설망을 작성할 수 있는 유연한 빌딩 블록을 제공할 뿐만 아니라, 인터넷에 대한 기본 보안 기능을 제공합니다.

VPN은 L2TP(Layer 2 Tunnel Protocol) VPN 솔루션도 지원합니다. 가상 회선이라고도 하는 L2TP 연결은 사내 네트워크 서버가 해당 리모트 사용자에게 할당된 IP 주소를 관리할 수 있게 함으로써 리모트 사용자에게 비용이 효율적인 액세스를 제공합니다. 또한 L2TP 연결은 IPSec와 함께 사용하면 시스템 또는 네트워크에 대한 보안 액세스를 제공합니다.

VPN이 전체 네트워크에 미치는 영향을 이해하는 것이 중요합니다. 적절한 계획 및 구현은 필수적인 성공 요소입니다. VPN 작동 방법 및 그 사용 방법을 확실하게 알려면 다음 주제를 검토하십시오.

V5R2의 새로운 사항
이 주제에서는 이 릴리스의 신규 정보 또는 상당히 변경된 정보가 무엇인지 설명합니다.

이 주제 인쇄
이 정보의 하드 카피 버전을 원하는 경우에는 여기로 찾아 가서 PDF 파일을 인쇄하십시오.

VPN 시나리오
이 시나리오를 검토하여 기본 VPN 유형과 VPN 구성 단계를 알아 두십시오.

VPN 개념
표준 VPN 기술에 대한 최소한의 기본 지식을 지니는 것이 중요합니다. 이 주제에서는 VPN 구현에 사용하는 프로토콜에 대한 개념 정보를 제공합니다.

VPN 계획
VPN을 성공적으로 사용하기 위한 첫 번째 단계는 계획입니다. 이 주제에서는 이전 릴리스로부터의 마이그레이트, 설정 요구사항, 그리고 사용자 스펙에 맞게 사용자 정의된 계획 작업용지를 생성할 계획 어드바이저에 대한 링크 관련 정보를 제공합니다.

VPN 구성
VPN 계획을 완료하면 VPN 통신을 허용하는 IP 필터 규칙을 구성해야 합니다. 이 주제에서는 VPN을 사용하여 수행할 수 있는 작업과 작업 방법을 개략적으로 설명합니다.

VPN 관리
이 주제에서는 연결 변경, 모니터 또는 삭제 방법을 포함하여 활동 VPN 연결을 관리하기 위해 수행할 수 있는 다양한 타스크를 설명합니다.

VPN 문제점
VPN 연결에 문제점이 발생하면 이 주제를 참조하십시오.

VPN에 대한 관련 정보
여기에서는 VPN 정보 소스 및 관련 주제로 링크할 수 있습니다.

V5R2의 새로운 사항

버전 5 릴리스 2(V5R2) VPN(가상 사설망) 기능에 대한 확장 기능은 다음과 같습니다.

- NAT 호환 IPSec. 기술적으로는 UDP 캡슐화로도 알려져 있으며, IPSec 및 네트워크 주소 변환(NAT) 기술 사이의 다양한 비호환성에 대해 제시합니다. UDP 캡슐화는 사용자의 iSeries가 NAT를 사용하는 방화벽 뒤에 놓이도록 합니다. OS/400 VPN의 이전 릴리스와는 달리, 더 이상 iSeries를 네트워크의 주위에 놓거나, 공용 주소를 사용하거나, 가상 IP를 사용하여 VPN 연결을 만들지 않아도 됩니다.
- 동적 정책 필터. 이제 연관되는 정책 필터 규칙이 없는 VPN을 작성할 수 있습니다. 시스템 관리자는 모두 연결에 대해 동적으로 필터됩니다. 즉, VPN 연결을 위해 패킷 규칙을 구성하지 않아도 됩니다.
- 정책 필터 마이그레이트 마법사. 시스템을 V4R4 또는 V4R5에서 업그레이드한 후 업그레이드 이전 시스템에 로드된 규칙을 사용하려면, 정책 규칙 마이그레이트 마법사를 사용하여 사용자가 작성한 패킷 규칙 파일에서 정책 필터를 제거해야 합니다. 마법사는 VPN이 생성하는 정책 필터에 동등한 정책 필터를 삽입합니다. 그러면 이전 정책 필터와 새 정책 필터가 사용자 의도대로 함께 작동될 수 있습니다.
- 암호화 표준(AES) 알고리즘. OS/400 VPN은 이제 자료 보호를 위해 AES를 지원합니다.

V5R2 VPN 주제에 대한 변경사항은 다음과 같습니다.

- VPN이 통합 설정으로 작동하는 방법을 이해할 수 있도록 하기 위한 추가 시나리오:
- 특정 업무 요구를 처리하기 위해 작성해야 할 VPN 유형을 판별하는 데 도움이 되는 VPN 계획 어드바이저에 대한 갱신 또한 어드바이저는 VPN을 구성하기 위해 취할 단계를 제안합니다.

이 릴리스에서 새로운 사항과 변경된 사항에 대한 추가 정보를 보려면 Memo to Users  를 참조하십시오.

VPN 시나리오

다음 시나리오를 검토하여 각각의 기본 연결 유형과 관련된 기술 및 구성 세부사항을 잘 알아두십시오.

- **VPN 시나리오: 기본 지점 연결**
  이 시나리오에서, 회사는 VPN 게이트웨이 역할을 하는 한 쌍의 iSeries 시스템을 통해 멀리 떨어져 있는 두 부서의 서브네트 주소간 VPN을 설정하려고 합니다.
- **VPN 시나리오: 기본 기업간 연결**
  이 시나리오에서, 회사는 제조 부서에 있는 클라이언트 워크스테이션과 업무 상대 회사의 공급 부서에 있는 클라이언트 워크스테이션간 VPN을 설정하려고 합니다.
- **VPN 시나리오: IPSec를 사용하여 L2TP 임의 터널 보호**
  이 시나리오는 지점 호스트와 IPSec로 보호된 L2TP 회사 사무실간 연결을 설명합니다. 회사 사무실이 글로벌로 라우트할 수 있는 정적 IP 주소를 갖는 반면, 지점은 동적으로 지정된 IP 주소를 갖습니다.
- **VPN 시나리오: VPN에 대한 네트워크 주소 변환 사용**
  이 시나리오에서, 회사는 OS/400 VPN을 사용하여 해당되는 업무 파트너 중 하나와 민감한 자료를 교환하려고 합니다. 회사 네트워크 구조의 개인보호정책을 추가로 보호하기 위해, 회사에서는 VPN NAT도 사용하여, 업무 파트너가 액세스를 가지고 있는 어플리케이션을 호스팅하기 위해 사용하는 iSeries의 개인 IP 주소를 감출 것입니다.

기타 VPN 시나리오

자세한 VPN 구성 시나리오를 보려면, 다음 VPN 기타 정보 소스를 참조하십시오.

- **QoS 시나리오: 보안 및 예측 가능 결과(VPN 및 QoS)**
  VPN과 함께 서비스 품질(QoS) 정책을 작성할 수 있습니다. 이 예는 두 가지가 함께 사용되는 것을 보여줍니다.
- **OS/400 V5R1 Virtual Private Networks: Remote Access to the IBM e(logo)server iSeries Server with Windows 2000 VPN Clients, REDP0153**
  이 IBM Redpaper는 V5R1 VPN과 Windows 2000 원시(native) L2TP 및 IPSec 지원을 사용하여 VPN 터널을 구성하는 단계별 프로세스를 제공합니다.
- **AS/400 Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00**
  이 레드북은 VPN 개념을 설명하고, IP 보안(IPSec) 및 L2TP(Layer 2 Tunneling Protocol)를 사용하여 OS/400에서 VPN을 구현하는 방법을 설명합니다.
- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00**
  이 레드북에서는 AS/400 시스템에서 사용할 수 있는 모든 고유 네트워크 보안 피처(예: IP 필터, NAT, VPN, HTTP 프록시 서버, SSL, DNS, 메일 릴레이, 감사 및 기록 등)를 설명합니다. 실제 사용 예를 통해 설명합니다.

VPN 시나리오: 기본 지점 연결

회사가 지점간 통신에서 발생하는 비용을 최소화하려 한다고 가정하십시오. 현재, 회사는 프레임 릴레이 또는 전용 회선을 사용하고 있지만 보다 저렴하고, 안전하며 글로벌로 액세스할 수 있는 내부 기밀 자료 전송에 대해 다른 옵션을 찾으려고 합니다. 인터넷을 탐색해 보면 회사 요구에 맞는 VPN(가상 사설망)을 쉽게 설정할 수 있습니다.

회사와 지점 모두 인터넷을 통한 VPN 보호가 필요하지만, 각각의 인트라넷 내에서는 보호가 필요하지 않습니다. 인트라넷이 신뢰할 수 있다고 간주하기 때문에, 최적의 솔루션은 게이트웨이간 VPN을 작성하는 것입니다. 이 경우, 양쪽 게이트웨이 모두 중재 네트워크에 직접 연결됩니다. 즉, *경계* 또는 *테두리* 시스템으로 방화벽의 보호를 받지 못합니다. 이 예는 기본 VPN 구성 설정과 관련된 단계를 소개하는 유용한 역할을 합니다. 이 시나리오가 *인터넷*이라는 용어를 언급할 때, 이 용어는 두 개의 VPN 게이트웨이의 중재 네트워크를 말하는데 회사 자체 사설망일 수도 있고 공용 인터넷일 수도 있습니다.

중요한 주:
이 시나리오는 인터넷에 직접 접속된 iSeries 보안 게이트웨이를 나타낸 것입니다. 시나리오를 단순화하기 위해 방화벽은 없습니다. 그렇다고 해서 방화벽을 사용하지 않아도 된다는 의미는 아닙니다. 사실, 인터넷에 연결할 때 관련된 보안 문제를 고려해야 합니다. 보안 위험을 줄이는 다양한 방법에 대한 자세한 설명은 레드북 AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00 을 검토하십시오.

장점

이 시나리오의 장점은 다음과 같습니다.

- 인터넷 또는 기존 인트라넷을 사용하므로 리모트 서브네트간 사설 회선 비용을 줄입니다.
- 인터넷 또는 기존 인트라넷을 사용하므로 사설 회선 및 연관된 장비의 설치와 유지보수의 복잡성을 줄입니다.
- 인터넷을 사용하므로 리모트 위치에서 전세계의 거의 모든 장소로 연결할 수 있습니다.
- VPN을 사용하므로 사용자들이 전용 회선 또는 광역 네트워크(WAN) 연결을 사용하여 연결된 것과 같이 한 쪽 연결로 모든 서버 및 자원에 액세스할 수 있습니다.
- 업계 표준 암호화 및 인증 메소드를 사용하므로 한 위치에서 다른 위치로 전달되는 민감한 정보에 대한 보안을 보장합니다.
- 암호화 키를 동적으로 그리고 정기적으로 교환하므로 설정이 간단하고 키가 해독되어 보안이 침해될 위험이 줄어듭니다.
- 각각의 리모트 서브네트 주소에서 사설 IP 주소를 사용하므로 중요한 공용 인터넷 주소를 각각의 클라이언트에 할당할 필요가 없습니다.

목적

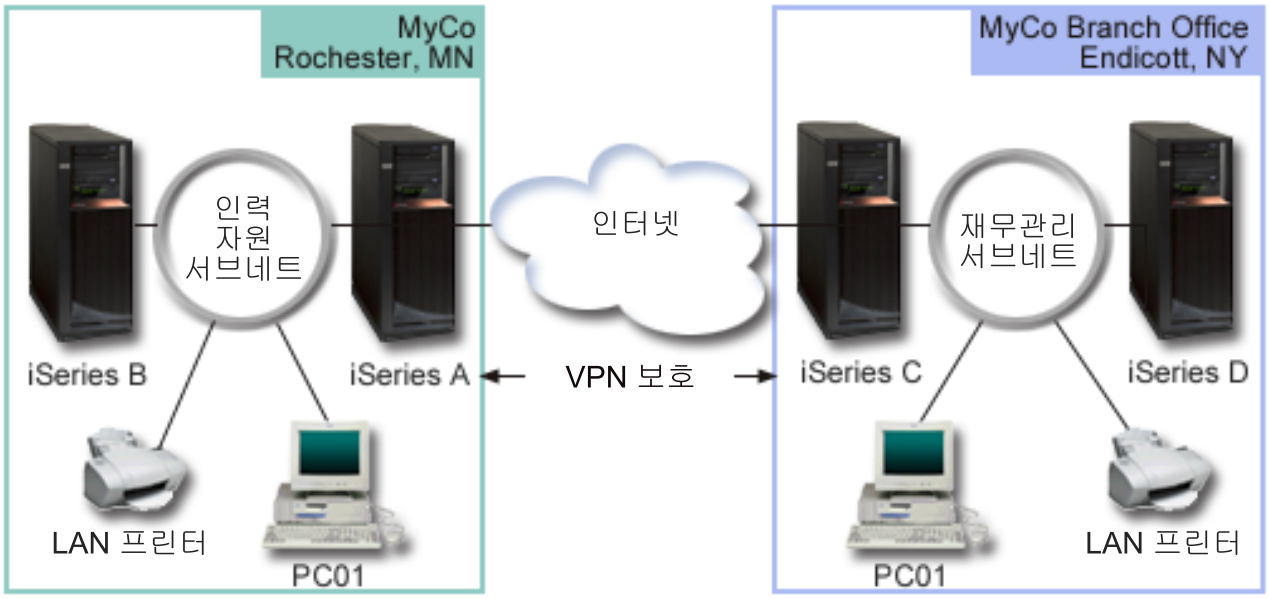
이 시나리오에서, 우리 회사는 한 쌍의 iSeries 서버를 통해 인력 자원 부서와 재무관리 부서의 서브네트 주소간에 VPN을 설정하려고 합니다. 두 서버 모두 VPN 게이트웨이 역할을 합니다. VPN 구성면에서, 게이트웨이 키 관리를 수행하고, 터널을 통해 흐르는 자료에 IPSec를 적용합니다. 게이트웨이 연결의 자료 종료점이 아닙니다.

이 시나리오의 목적은 다음과 같습니다.

- VPN은 인력 자원 부서의 서브네트 주소와 재무관리 부서의 서브네트 주소간 모든 자료 통신량을 보호해야 합니다.
- 자료 통신량은 두 부서 중 한 부서의 서브네트 주소에 도달하면 VPN 보호를 하지 않아도 됩니다.
- 각 네트워크의 모든 클라이언트와 호스트는 모든 어플리케이션을 포함하여 서로의 네트워크에 완전히 액세스할 수 있습니다.
- 게이트웨이 서버는 서로 통신할 수 있으며, 상호간 어플리케이션에 액세스할 수 있습니다.

세부사항

다음 그림은 우리 회사의 네트워크 특성을 설명한 것입니다.



인력 자원 부서

- iSeries-A는 OS/400 버전 5 릴리스 2(V5R2)에서 실행되며, 인력 자원 부서 VPN 게이트웨이 역할을 합니다.
- 서브네트 주소는 10.6.0.0이고 마스크는 255.255.0.0입니다. 이 서브네트 주소는 우리 회사 Rochester 사이트의 VPN 터널 자료 종료점을 표시합니다.
- iSeries-A는 IP 주소 204.146.18.227로 인터넷에 연결합니다. 이것은 연결 종료점입니다. 즉, iSeries-A는 키 관리를 수행하고, IPSec를 수신 및 송신 IP 데이터그램에 적용합니다.
- iSeries-A는 IP 주소 10.6.11.1로 서브네트 주소에 연결합니다.
- iSeries-B는 표준 TCP/IP 어플리케이션을 실행하는 인력 자원 부서 서브네트 주소에 있는 생산 서버입니다.

재무관리 부서

- iSeries-C는 OS/400 버전 5 릴리스 2(V5R2)에서 실행되며, 재무관리 부서 VPN 게이트웨이 역할을 합니다.
- 서브네트 주소는 10.196.8.0이고 마스크는 255.255.255.0입니다. 이 서브네트 주소는 우리 회사 Endicott 사이트의 VPN 터널 자료 종료점을 표시합니다.
- iSeries-C는 IP 주소 208.222.150.250으로 인터넷에 연결합니다. 이것은 연결 종료점입니다. 즉, iSeries-C는 키 관리를 수행하고, IPSec를 수신 및 송신 IP 데이터그램에 적용합니다.
- iSeries-C는 IP 주소 10.196.8.5로 서브네트 주소에 연결합니다.

타스크 구성

이 시나리오에 설명한 지점 연결을 구성하려면 다음 타스크를 완료해야 합니다.

1. TCP/IP 라우팅을 확인하여 두 개의 게이트웨이 서버가 인터넷을 통해 서로 통신할 수 있는지 확인하십시오. 이렇게 하면 각 서브네트 주소의 호스트가 리모트 서브네트 주소에 액세스하기 위해 각 게이트웨이로 올바로 라우팅하는지 확인할 수 있습니다.
   주: 라우팅은 이 주제에서는 다루지 않습니다. 질문이 있으면, Information Center에서 TCP/IP 라우팅 및 작업부하 균형 조절을 참조하십시오.
2. 양쪽 시스템 모두에 대해 계획 작업용지와 체크 리스트를 완료(6 페이지 참조)하십시오.
3. 인력 자원 VPN 게이트웨이(iSeries-A)에 VPN을 구성(7 페이지 참조)하십시오.
4. 재무관리 부서 VPN 게이트웨이(iSeries-C)에 VPN을 구성(8 페이지 참조)하십시오.
5. VPN 서버가 시작(9 페이지 참조)되었는지 확인하십시오.
6. 두 리모트 서브네트 주소간 통신을 테스트(9 페이지 참조)하십시오.

구성 세부사항

첫 번째 단계를 완료한 후, TCP/IP 라우팅이 올바로 작동되고 있고 게이트웨이 서버가 통신할 수 있는지 확인하면 VPN 구성을 시작할 준비가 됩니다.

2단계: 계획 작업용지 완료

다음의 계획 체크 리스트에서는 VPN 구성을 시작하기 전에 필요한 정보 유형을 설명합니다. VPN 설정을 계속하기 전에 요구사항 체크 리스트의 모든 응답이 예가 되어야 합니다.

주: 이 작업용지들은 iSeries-A에 적용됩니다. iSeries-C의 경우 프로세스를 반복하고 필요하면 IP 주소를 반대로 하십시오.

필수 체크 리스트	응답
OS/400 V5R2(5722-SS1) 이상입니까?	예
디지털 인증 관리자 옵션(5722-SS1 옵션 34)이 설치되어 있습니까?	예
Cryptographic Access Provider(5722-AC2 또는 AC3)가 설치되어 있습니까?	예
Windows용 iSeries Access(5722-XE1)가 설치되어 있습니까?	예
iSeries Navigator가 설치되었습니까?	예

iSeries Navigator의 네트워크 부속 구성요소가 설치되어 있습니까?	예
OS/400용 TCP/IP 연결 유틸리티(5722-TC1)가 설치되어 있습니까?	예
서버 보안 자료 보유(QRETSVRSEC *SEC) 시스템 값을 1로 설정했습니까?	예
iSeries에 TCP/IP가 구성되어 있습니까(IP 인터페이스, 라우트, 로컬 호스트명, 로컬 정의역명 포함)?	예
필수 종료점간에 정상 TCP/IP 통신이 설정되어 있습니까?	예
최신 PTF(Program Temporary Fixes)를 적용했습니까?	예
VPN 터널이 방화벽이나 IP 패킷 필터링을 구현하는 라우터를 오가는 경우, 방화벽이나 라우터 필터 규칙이 AH와 ESP 프로토콜을 지원합니까?	예
방화벽이나 라우터가 IKE(UDP 포트 500), AH 및 ESP 프로토콜을 허용하도록 구성되어 있습니까?	예
방화벽이 IP 이송이 가능하도록 구성되어 있습니까?	예

이 정보는 VPN을 구성하는 데 필요합니다	**응답**
작성 중인 연결 유형은 무엇입니까?	게이트웨 대 게이트웨이
동적-키 그룹명을 무엇이라 명명하겠습니까?	HRgw2FINgw
키를 보호하는 데 필요한 보안 유형과 시스템 성능 유형은 무엇입니까?	균형 조절
인증을 사용하여 연결을 인증하고 있습니까? 아니면, 사전공유 키는 무엇입니까?	아니오 topsecretstuff
로컬 키 서버의 ID는 무엇입니까?	IP 주소: 204.146.18.227
로컬 자료 종료점의 ID는 무엇입니까?	서브네트 주소: 10.6.0.0 마스크: 255.255.0.0
리모트 키 서버의 ID는 무엇입니까?	IP 주소: 208.222.150.250
리모트 자료 종료점의 ID는 무엇입니까?	서브네트 주소: 10.196.8.0 마스크: 255.255.255.0
연결을 통해 흐름을 허용할 포트와 프로토콜을 무엇입니까?	임의
자료를 보호하는 데 필요한 보안 유형과 시스템 성능 유형은 무엇입니까?	균형 조절
연결을 적용할 인터페이스는 어느 것입니까?	TRLINE

3단계: iSeries-A에 VPN 구성

작업용지의 정보를 사용하여 다음과 같이 iSeries-A에 VPN을 구성하십시오.

1. iSeries Navigator에서 iSeries-A —> **네트워크** —> **IP 정책**을 확장하십시오.
2. **가상 사설망**을 마우스 오른쪽 버튼으로 클릭하고 **신규 연결**을 선택하여 새로운 연결 마법사를 시작하십시오.
3. 마법사가 작성하는 오브젝트에 대한 정보는 **시작** 페이지를 검토하십시오.
4. **다음**을 클릭하여 **연결명** 페이지로 찾아 가십시오.
5. **이름** 필드에 HRgw2FINgw를 입력하십시오.
6. (선택적) 이 연결 그룹에 대한 설명을 지정하십시오.
7. **다음**을 클릭하여 **연결 시나리오** 페이지로 찾아 가십시오.
8. **게이트웨이에서 다른 게이트웨이로 연결**을 선택하십시오.

9. **다음**을 클릭하여 **인터넷 키 교환 정책** 페이지로 찾아 가십시오.
10. **신규 정책 작성**을 선택한 후, **보안과 성능 균형 조절**을 선택하십시오.
11. **다음**을 클릭하여 **로컬 연결 종료점에 대한 인증** 페이지로 찾아 가십시오.
12. 인증을 사용하여 연결을 인증하지 않음을 나타내려면 **아니오**를 선택하십시오.
13. **다음**을 클릭하여 **로컬 키 서버**로 찾아 가십시오.
14. **ID 유형** 필드에서 **버전 4 IP 주소**를 선택하십시오.
15. **IP 주소** 필드에서 204.146.18.227를 선택하십시오.
16. **다음**을 클릭하여 **리모트 키 서버**로 찾아 가십시오.
17. **ID 유형** 필드에서 **버전 4 IP 주소**를 선택하십시오
18. **ID** 필드에 208.222.150.250을 입력하십시오.
19. **사전공유 키** 필드에 topsecretstuff를 입력하십시오.
20. **다음**을 클릭하여 **로컬 자료 종료점** 페이지로 찾아 가십시오.
21. **ID 유형** 필드에서 **IP 버전 4 서브네트 주소**를 선택하십시오.
22. **ID** 필드에 10.6.0.0을 입력하십시오.
23. **서브네트 마스크** 필드에 255.255.0.0을 입력하십시오.
24. **다음**을 클릭하여 **리모트 자료 종료점** 페이지로 찾아 가십시오.
25. **ID 유형** 필드에서 **IP 버전 4 서브네트 주소**를 선택하십시오.
26. **ID** 필드에 10.196.8.0을 입력하십시오.
27. **서브네트 마스크** 필드에 255.255.255.0을 입력하십시오.
28. **다음**을 클릭하여 **자료 서비스** 페이지로 찾아 가십시오.
29. 디폴트 값을 허용한 후, **다음**을 클릭하여 **자료 정책** 페이지로 찾아 가십시오.
30. **신규 정책 작성**을 선택한 후, **보안과 성능 균형 조절**을 선택하십시오. **RC4 암호화 알고리즘 사용**을 선택하십시오.
31. **다음**을 클릭하여 **적용 가능한 인터페이스** 페이지로 찾아 가십시오.
32. **행** 표에서 **TRLINE**을 선택하십시오.
33. **다음**을 클릭하여 **요약** 페이지로 찾아 가십시오. 마법사가 작성할 오브젝트가 올바른지 검토하십시오.
34. **완료**를 클릭하여 구성을 완료하십시오.
35. **정책 필터 활성화** 대화상자가 나타나면 **예, 생성된 정책 필터 활성화**를 선택한 후 **기타 모든 통신 허가**를 선택하십시오. **확인**을 클릭하여 구성을 완료하십시오. 프롬트되면, 모든 인터페이스에 대해 규칙을 활성화 할 것을 지정하십시오.

이제 iSeries-A에 VPN 구성을 완료하였습니다. 다음 단계는 재무관리 부서 VPN 게이트웨이(iSeries-C)에 VPN을 구성하는 것입니다.

4단계: iSeries-C에 VPN 구성

iSeries-A 구성에 사용한 것과 동일한 단계를 따르고 필요하면 IP 주소를 반대로 하십시오. 지침용 계획 작업 용지를 사용하십시오. 재무관리 부서 VPN 게이트웨이 구성이 완료되면, 연결은 *요청시* 상태가 됩니다. 이는 VPN 연결이 보호해야 IP 프로그램이 송신될 때 연결이 시작됨을 의미합니다. 다음 단계는 VPN 서버가 아직 시작되지 않은 경우 이를 시작하는 것입니다.

6단계: VPN 서버 시작

VPN 서버를 시작하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 **서버 —> 네트워크 —> IP 정책**을 확장하십시오.
2. **가상 사설망**을 마우스 오른쪽 버튼으로 클릭하고 **시작**을 선택하십시오.

7단계: 연결 테스트

양쪽 서버를 모두 구성하여 VPN서버를 시작한 후, 연결을 테스트하여 리모트 서브네트가 서로 통신할 수 있는지 확인해야 합니다. 이를 수행하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 **iSeries-A —> 네트워크**를 확장하십시오.
2. **TCP/IP 구성**을 오른쪽 마우스 버튼으로 클릭하고 **유틸리티**를 선택한 후 **핑(Ping)**을 선택하십시오.
3. **핑(Ping) 위치** 대화상자에서 **핑(Ping)** 필드에 iSeries-C를 입력하십시오.
4. **지금 핑(Ping)**을 클릭하여 iSeries-A에서 iSeries-C로 연결을 확인하십시오.
5. 완료되었으면 **확인**을 클릭하십시오.

VPN 시나리오: 기본 기업간 연결

많은 회사가 프레임 릴레이 또는 전용 회선을 사용하여 업무 상대 회사, 자회사 및 공급업체에 보안 통신을 제공합니다. 불행히도, 이 솔루션은 종종 비용이 많이 들고 지리적 한계성을 갖고 있습니다. VPN은 비용면에서 효율적인 사설 통신을 원하는 회사에게 한 가지 대안을 제시합니다.

제조업체에 주요 부품을 공급하는 업체라고 가정하십시오. 제조업체가 요구하는 정확한 시간에 특정 부품 및 수량을 확보하는 것이 매우 중요하기 때문에, 항상 제조업체의 재고 상태 및 생산 스케줄을 알고 있어야 합니다. 현재 이 상호작용을 수동으로 처리하고 있으며, 처리하는 데 시간이 많이 걸리고 비용도 많이 들며 심지어 때로는 부정확하다고 느끼기도 합니다. 사용자는 제조업체와 보다 쉽고 빠르며 효과적으로 통신하는 방법을 찾으려고 합니다. 그러나 제조업체는 정보의 기밀성 및 시간을 다투는 속성 때문에 이 정보를 회사 웹 사이트에 게시하거나 외부 보고서 형태로 매달 분배하려고 하지 않습니다. 공용 인터넷을 탐색해 보면 두 회사의 요구에 맞는 VPN(가상 사설망)을 쉽게 설정할 수 있습니다.

목적

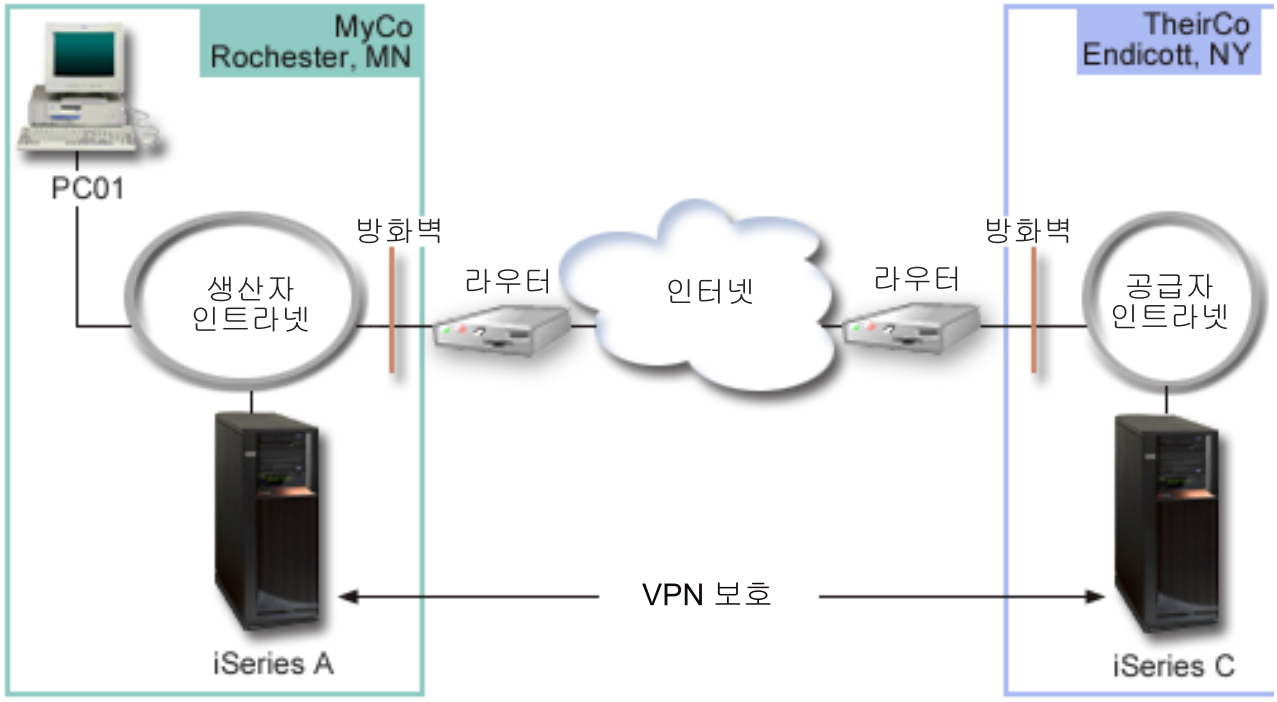
이 시나리오에서, 우리 회사는 부품 자재 부서에 있는 호스트와 비즈니스 상대방인 상대 회사 제조 부서의 호스트간 VPN을 설정하려고 합니다.

이 두 회사가 공유하는 정보는 아주 중요하기 때문에, 인터넷을 통해 정보가 전달될 때 보안되어야 합니다. 또한 각 네트워크가 상대 네트워크를 신뢰할 수 없다고 생각하기 때문에 각 회사의 네트워크 내에서 자료가 흐르게 되어서는 안됩니다. 즉, 두 회사 모두 단말 인증, 무결성 및 암호화가 필요합니다.

중요한 주:
이 시나리오의 목적은 예를 제시하여 호스트간 단순한 VPN 구성을 소개하는 것입니다. 일반적인 네트워크 환경에서, 다른 네트워크간에 방화벽 구성, IP 주소지정 요구사항, 라우팅도 고려해야 합니다.

세부사항

다음 그림은 우리 회사 및 상대 회사의 네트워크 특성을 설명한 것입니다.



우리 회사 공급 네트워크

- iSeries-A는 OS/400 버전 5 릴리스 2(V5R2)에서 실행됩니다.
- iSeries-A의 IP 주소는 10.6.1.1입니다. 이것은 자료 종료점일 뿐만 아니라 연결 종료점이기도 합니다. 즉, iSeries-A는 IKE 협의를 수행하고, IPSec를 수신 및 송신 IP 데이터그램에 적용하며, VPN을 통해 흐르는 자료의 소스이자 목적이기도 합니다.
- iSeries-A의 서브네트 주소는 10.6.0.0이고 마스크는 255.255.0.0입니다.
- iSeries-A만 iSeries-C와의 연결을 시작할 수 있습니다.

상대 회사 제조 네트워크

- iSeries-C는 OS/400 버전 5 릴리스 2(V5R2)에서 실행됩니다.
- iSeries-C의 IP 주소는 10.196.8.6입니다. 이것은 자료 종료점일 뿐만 아니라 연결 종료점이기도 합니다. 즉, iSeries-A는 IKE 협의를 수행하고, IPSec를 수신 및 송신 IP 데이터그램에 적용하며, VPN을 통해 흐르는 자료의 소스이자 목적이기도 합니다.
- iSeries-C 서브네트 주소는 10.196.8.0이고 마스크는 255.255.255.0입니다.

타스크 구성

이 시나리오에 설명한 기업간 연결을 구성하려면 다음 타스크를 완료해야 합니다.

1. TCP/IP 라우팅을 확인하여 iSeries-A와 iSeries-C가 인터넷을 통해 서로 통신할 수 있는지 확인하십시오. 이렇게 하면 각 서브네트 주소의 호스트가 리모트 서브네트 주소에 액세스하기 위해 각 게이트웨이가 올바로 라우팅하는지 확인할 수 있습니다. 이 시나리오의 경우, 전에는 없던 사설 주소 라우팅을 고려해야 한다는 점을 알고 있어야 합니다.

   주: 라우팅은 이 주제에서는 다루지 않습니다. 질문이 있으면, Information Center에서 TCP/IP 라우팅 및 작업부하 균형 조절을 참조하십시오.
2. 양쪽 시스템 모두에 대해 계획 작업용지와 체크 리스트를 완료(11 페이지 참조)하십시오.
3. 우리 회사의 공급 네트워크에서 iSeries-A에 VPN을 구성(12 페이지 참조)하십시오.
4. 상대 회사의 제조 네트워크에서 iSeries-C에 VPN을 구성(14 페이지 참조)하십시오.
5. 양쪽 서버에서 필터 규칙을 활성화(14 페이지 참조)하십시오.
6. iSeries-A에서 연결을 시작(14 페이지 참조)하십시오.
7. 두 리모트 서브네트 주소간 통신을 테스트(15 페이지 참조)하십시오.

구성 세부사항

첫 번째 단계를 완료한 후, TCP/IP 라우팅이 올바로 작동되고 있고 서버가 통신할 수 있는지 확인하면 VPN 구성을 시작할 준비가 됩니다.

2단계: 계획 작업용지 완료

다음의 계획 체크 리스트에서는 VPN 구성을 시작하기 전에 필요한 정보 유형을 설명합니다. VPN 설정을 계속하기 전에 요구사항 체크 리스트의 모든 응답이 예가 되어야 합니다.

주: 이 작업용지들은 iSeries-A에 적용됩니다. iSeries-C의 경우 프로세스를 반복하고 필요하면 IP 주소를 반대로 하십시오.

필수 체크 리스트	**응답**
OS/400 V5R2(5722-SS1) 이상입니까?	예
디지털 인증 관리자 옵션(5722-SS1 옵션 34)이 설치되어 있습니까?	예
Cryptographic Access Provider(5722-AC2 또는 AC3)가 설치되어 있습니까?	예
Windows용 iSeries Access(5722-XE1)가 설치되어 있습니까?	예
iSeries Navigator가 설치되었습니까?	예
iSeries Navigator의 네트워크 부속 구성요소가 설치되어 있습니까?	예
OS/400용 TCP/IP 연결 유틸리티(5722-TC1)가 설치되어 있습니까?	예
서버 보안 자료 보유(QRETSVRSEC *SEC) 시스템 값을 1로 설정했습니까?	예
iSeries에 TCP/IP가 구성되어 있습니까(IP 인터페이스, 라우트, 로컬 호스트명, 로컬 정의역명 포함)?	예
필수 종료점간에 정상 TCP/IP 통신이 설정되어 있습니까?	예
최신 PTF(Program Temporary Fixes)를 적용했습니까?	예
VPN 터널이 방화벽이나 IP 패킷 필터링을 구현하는 라우터를 오가는 경우, 방화벽이나 라우터 필터 규칙이 AH와 ESP 프로토콜을 지원합니까?	예
방화벽이나 라우터가 IKE(UDP 포트 500), AH 및 ESP 프로토콜을 허용하도록 구성되어 있습니까?	예
방화벽이 IP 이송이 가능하도록 구성되어 있습니까?	예

이 정보는 VPN을 구성하는 데 필요합니다.	**응답**
작성 중인 연결 유형은 무엇입니까?	호스트간
동적-키 그룹명을 무엇이라 명명하겠습니까?	MyCo2TheirCo
키를 보호하는 데 필요한 보안 유형과 시스템 성능 유형은 무엇입니까?	최대
인증을 사용하여 연결을 인증하고 있습니까? 아니면, 사전공유 키는 무엇입니까?	예
로컬 키 서버의 ID는 무엇입니까?	IP 주소: 10.6.1.1
로컬 자료 종료점의 ID는 무엇입니까?	IP 주소: 10.6.1.1
리모트 키 서버의 ID는 무엇입니까?	IP 주소: 10.196.8.6
리모트 자료 종료점의 ID는 무엇입니까?	IP 주소: 10.196.8.6
연결을 통해 흐름을 허용할 포트와 프로토콜을 무엇입니까?	임의
자료를 보호하는 데 필요한 보안 유형과 시스템 성능 유형은 무엇입니까?	최대
연결을 적용할 인터페이스는 어느 것입니까?	TRLINE

3단계: iSeries-A에 VPN 구성

작업용지의 정보를 사용하여 다음과 같이 iSeries-A에 VPN을 구성하십시오.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책**을 확장하십시오.

2. **가상 사설망**을 마우스 오른쪽 버튼으로 클릭하고 **신규 연결**을 선택하여 연결 마법사를 시작하십시오.
3. 마법사가 작성하는 오브젝트에 대한 정보는 **시작** 페이지를 검토하십시오.
4. **다음**을 클릭하여 **연결명** 페이지로 이동하십시오.
5. **이름** 필드에 MyCo2TheirCo를 입력하십시오.
6. (선택적) 이 연결 그룹에 대한 설명을 지정하십시오.
7. **다음**을 클릭하여 **연결 시나리오** 페이지로 찾아 가십시오.
8. **호스트를 다른 호스트에 연결**을 선택하십시오.
9. **다음**을 클릭하여 **인터넷 키 교환 정책** 페이지로 찾아 가십시오.
10. **신규 정책 작성**을 선택한 후, **최대 보안, 최소 성능**을 선택하십시오.
11. **다음**을 클릭하여 **로컬 연결 종료점에 대한 인증** 페이지로 찾아 가십시오.
12. 인증을 사용하여 연결을 인증할 것임을 나타내려면 **예**를 선택하십시오. 그런 다음, iSeries-A를 나타내는 인증을 선택하십시오.
    주: 인증을 사용하여 로컬 연결 종료점을 인증하려는 경우, 먼저 디지털 인증 관리자 (DCM)에서 인증을 작성해야 합니다.
13. **다음**을 클릭하여 **로컬 연결 종료점 ID** 페이지로 찾아 가십시오.
14. **버전 4 IP 주소**를 ID 유형으로 선택하십시오. 연관 IP 주소는 10.6.1.1이어야 합니다. 이 정보는 다시 DCM에서 작성하는 인증에 정의됩니다.
15. **다음**을 클릭하여 **리모트 키 서버**로 찾아 가십시오.
16. **ID 유형** 필드에서 **버전 4 IP 주소**를 선택하십시오.
17. **ID** 필드에 10.196.8.6을 입력하십시오.
18. **다음**을 클릭하여 **자료 서비스** 페이지로 찾아 가십시오.
19. 디폴트 값을 허용한 후, **다음**을 클릭하여 **자료 정책** 페이지로 찾아 가십시오.
20. **신규 정책 작성**을 선택한 후, **최대 보안, 최소 성능**을 선택하십시오. **RC4 암호화 알고리즘 사용**을 선택하십시오.
21. **다음**을 클릭하여 **적용 가능한 인터페이스** 페이지로 찾아 가십시오.
22. **TRLINE**을 선택하십시오.
23. **다음**을 클릭하여 **요약** 페이지로 찾아 가십시오. 마법사가 작성할 오브젝트가 올바른지 검토하십시오.
24. **완료**를 클릭하여 구성을 완료하십시오.
25. **정책 필터 활성화** 대화상자가 나타나면 **아니오, 나중에 패킷 규칙을 활성화함**을 선택한 후 **확인**을 클릭하십시오.

다음 단계는 iSeries-A만 이 연결을 시작할 수 있도록 지정하는 것입니다. 마법사가 작성한 동적-키 그룹 (MyCo2TheirCo) 등록 정보를 사용자 정의하여 이를 수행하십시오.

1. VPN 인터페이스 왼쪽 분할 창에서 **그룹별**을 클릭하십시오. 신규 동적-키 그룹(MyCo2TheirCo)이 오른쪽 분할 창에 표시됩니다. 신규 그룹을 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
2. **정책** 페이지로 찾아 가서 **로컬 시스템이 연결 시작** 옵션을 선택하십시오.

3. **확인**을 클릭하여 변경사항을 저장하십시오.

이제 iSeries-A에 VPN 구성을 완료하였습니다. 다음 단계는 상대 회사의 제조 네트워크에서 iSeries-C에 VPN을 구성하는 것입니다.

4단계: iSeries-C에 VPN 구성

iSeries-A 구성에 사용한 것과 동일한 단계를 따르고 필요하면 IP 주소를 반대로 하십시오. 지침용 계획 작업용지를 사용하십시오. iSeries-C 구성을 완료하면, 연결 마법사가 각 서버에 작성한 필터 규칙을 활성화해야 합니다.

5단계: 패킷 규칙 활성화

마법사는 이 연결이 올바로 작동되는 데 필요한 패킷 규칙을 자동으로 작성합니다. 그러나 VPN 연결을 시작하기 전에 먼저 양쪽 시스템에서 패킷 규칙을 활성화해야 합니다. iSeries-A에서 규칙을 활성화하려면, 다음 단계를 따르십시오.

1. iSeries Navigator에서, **iSeries-A —> 네트워크 —> IP 정책**을 확장하십시오.
2. **패킷 규칙**을 마우스 오른쪽 버튼으로 클릭하고 **활성화**를 선택하십시오. 그러면 패킷 규칙 활성화 대화 상자가 열립니다.
3. VPN 생성 규칙만이나, 선택한 파일만 또는 VPN 생성 규칙과 선택된 파일 모두를 활성화할 것인지 선택하십시오. 나중에(예를 들어, VPN 생성 규칙 외에도 인터페이스에 대해 시행하려고 하는 기타 PERMIT 및 DENY 규칙이 있는 경우) 선택할 수도 있습니다.
4. 규칙을 활성화할 인터페이스를 선택하십시오. 이 경우에는 **모든 인터페이스**를 선택하십시오.
5. 대화상자에서 **확인**을 클릭하여 지정한 인터페이스에 대해 규칙을 확인하고 활성화를 확인하십시오. 확인을 클릭하고 나면, 시스템은 구문 및 시멘틱 오류에 대해 규칙을 검사하고 편집기의 맨 아래에 있는 메세지 창에 결과를 보고합니다. 특정 파일 및 행 번호와 연관되는 오류 메세지에 대해, 오류를 마우스 오른쪽 버튼으로 클릭하고 **행 찾아 가기**를 선택하여 파일에서 오류를 강조표시할 수 있습니다.
6. iSeries-C에서 패킷 규칙을 활성화하려면 위의 단계를 반복하십시오.

6단계: 연결 시작

iSeries-A에서 MyCo2TheirCo 연결을 시작하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서, **iSeries-A —> 네트워크 —> IP 정책**을 확장하십시오.
2. VPN 서버가 시작되지 않는 경우, **가상 사설망**을 마우스 오른쪽 버튼으로 클릭하고 **시작**을 선택하십시오. 그러면 VPN 서버가 시작됩니다.
3. **가상 사설망 —> 보안 연결**을 확장하십시오.
4. **모든 연결**을 클릭하여 오른쪽 분할 창에 연결 리스트를 표시하십시오.
5. **MyCo2TheirCo**를 마우스 오른쪽 버튼으로 클릭하고 **시작**을 선택하십시오.

6. **보기** 메뉴에서 **화면정리**를 선택하십시오. 연결이 시작되면, 상태가 *유휴*에서 *작동가능*으로 변경되어야 합니다. 연결이 시작되려면 몇 분 정도 소요되므로 상태가 *작동 가능*으로 변경될 때까지 정기적으로 화면정리를 하십시오.

7단계: 연결 테스트

양쪽 서버를 모두 구성하여 연결을 시작한 후, 연결을 테스트하여 리모트 호스트가 서로 통신할 수 있는지 확인해야 합니다. 이를 수행하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 **iSeries-A —> 네트워크**를 확장하십시오.
2. **TCP/IP 구성**을 마우스 오른쪽 버튼으로 클릭하고 **유틸리티**를 선택한 후 **핑(Ping)**을 선택하십시오.
3. **핑(Ping) 위치** 대화상자에서 **핑(Ping)** 필드에 `iSeries-C`를 입력하십시오.
4. **지금 핑(Ping)**을 클릭하여 iSeries-A에서 iSeries-C로 연결을 확인하십시오.
5. 완료되었으면 **확인**을 클릭하십시오.

VPN 시나리오: IPSec를 사용하여 L2TP 임의 터널 보호

회사가 다른 지역에 작은 지점을 소유하고 있다고 가정하십시오. 지정 근무일내내 지점은 회사 인트라넷 내의 iSeries에 있는 기밀 정보에 액세스해야 할 수 있습니다. 회사는 현재 고비용의 전용 회선을 사용하여 지점에 사내 네트워크 액세스를 제공합니다. 회사가 인트라넷에 대한 보안 액세스를 계속 제공하려고 해도 결국 전용 회선에 연관된 비용을 줄이려고 할 것입니다. 마치 지점이 사내 서브네트 주소의 부분인 것처럼 사내 네트워크를 확장하는 L2TP(Layer 2 Tunnel Protocol) 자발적 터널을 작성하면 이를 수행할 수 있습니다. VPN은 L2TP 터널을 통한 자료 통신량을 보호합니다.

리모트 지점은 L2TP 자발적 터널을 사용하여 사내 네트워크의 LNS(L2TP Network Server)에 대해 직접 터널을 구축합니다. LAC(L2TP Access Concentrator) 기능은 클라이언트에 상주합니다. 터널은 리모트 클라이언트의 인터넷 서비스 제공자(ISP)에게 투명하므로, ISP는 L2TP를 지원할 필요가 없습니다. L2TP 개념에 대한 자세한 내용은 L2TP(Layer 2 Tunnel Protocol)를 참조하십시오.

> **중요한 주:**
> 이 시나리오는 인터넷에 직접 접속된 iSeries 보안 게이트웨이를 나타낸 것입니다. 시나리오를 단순화하기 위해 방화벽은 없습니다. 그렇다고 해서 방화벽을 사용하지 않아도 된다는 의미는 아닙니다. 사실, 인터넷에 연결할 때 관련된 보안 문제를 고려해야 합니다. 보안 위험을 줄이는 다양한 방법에 대한 자세한 설명은 레드북 AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00 을 검토하십시오.

목적

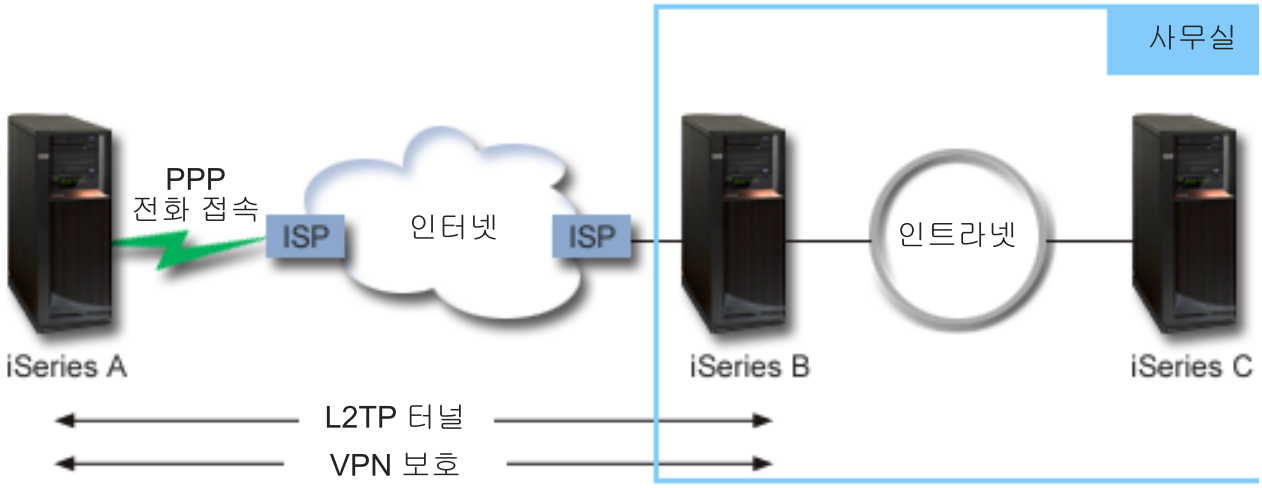
이 시나리오에서 지점 iSeries는 VPN이 보호하는 L2TP 터널을 사용하여 게이트웨이를 통해 회사 네트워크에 연결합니다.

이 시나리오의 주요 목적은 다음과 같습니다.

- 지점 시스템이 항상 회사 사무실로 연결을 시작합니다.
- 지점 시스템은 회사 네트워크에 액세스해야 하는 지점 네트워크에 있는 유일한 시스템입니다. 즉, 지점 네트워크에서 게이트웨이 역할을 하는 것이 아니라 호스트의 역할을 합니다.
- 회사 시스템은 회사 사무실 네트워크에 있는 호스트 컴퓨터입니다.

세부사항

다음 그림은 이 시나리오의 네트워크 특성을 설명한 것입니다.



iSeries-A

- 회사 네트워크에 있는 모든 시스템의 TCP/IP 어플리케이션에 액세스해야 합니다.
- ISP로부터 동적으로 지정된 IP 주소를 수신합니다.
- L2TP를 지원하도록 구성되어야 합니다.

iSeries-B

- iSeries-A의 TCP/IP 어플리케이션에 액세스해야 합니다.
- 서브네트 주소는 10.6.0.0이고 마스크는 255.255.0.0입니다. 이 서브네트 주소는 회사 사이트의 VPN 터널 자료 종료점을 표시합니다.
- IP 주소 205.13.237.6으로 인터넷에 연결합니다. 이것은 연결 종료점입니다. 즉, iSeries-B는 키 관리를 수행하고, IPSec를 수신 및 송신 IP 데이터그램에 적용합니다. iSeries-B는 IP 주소 10.6.11.1로 서브네트 주소에 연결합니다.

L2TP 측면에서 볼 때, *iSeries-A*는 L2TP 개시자의 역할을 하고, *iSeries-B*는 L2TP 종료자의 역할을 합니다.

타스크 구성

TCP/IP가 이미 구성되어 작동한다고 가정하고 다음 타스크를 완료해야 합니다.

1. iSeries-A에 VPN 구성(17 페이지 참조)을 수행하십시오.
2. iSeries-A에 가상 회선 및 PPP 연결 프로파일 구성(19 페이지 참조)을 수행하십시오.
3. PPP 프로파일에 동적-키 그룹을 적용(20 페이지 참조)하십시오.
4. iSeries-B에 VPN 구성(21 페이지 참조)을 수행하십시오.
5. iSeries-B에 가상 회선 및 PPP 연결 프로파일 구성(21 페이지 참조)을 수행하십시오.
6. iSeries-A와 iSeries-B에서 패킷 규칙을 활성화(22 페이지 참조)하십시오.
7. iSeries-A에서 연결을 시작(23 페이지 참조)하십시오.

구성 세부사항

TCP/IP가 적절하게 작동하고 iSeries 서버가 통신할 수 있는지 확인하고 나면, 이 시나리오에 설명된 연결 구성을 시작할 수 있는 준비가 된 것입니다.

1단계: iSeries-A에 VPN 구성

iSeries-A VPN을 구성하려면 다음 단계를 따르십시오.

1. **인터넷 키 교환 정책 구성**
   a. iSeries Navigator에서, iSeries-A —> **네트워크** —> **IP 정책** —> **가상 사설망** —> **IP 보안 정책**을 확장하십시오.
   b. **인터넷 키 교환 정책**을 마우스 오른쪽 버튼으로 클릭하고 **신규 인터넷 키 교환 정책**을 선택하십시오.
   c. **리모트 서버** 페이지에서, ID 유형으로 **버전 4 IP 주소**를 선택한 후 **IP 주소** 필드에 `205.13.237.6`을 입력하십시오.
   d. **연관사항** 페이지에서, **사전공유 키**를 선택하여 이 연결이 사전공유 키를 사용하여 이 정책을 인증함을 나타내십시오.
   e. **키** 필드에 사전공유 키를 입력하십시오. 사전공유 키를 암호처럼 취급하십시오.
   f. 로컬 키 서버 ID 유형에 **키 ID**를 선택한 후 **ID** 필드에 키 ID를 입력하십시오(예: `thisisthekeyid`). 로컬 키 서버에는 사전에 알 수 없는 동적으로 지정된 IP 주소가 있음을 기억하십시오. iSeries-B는 iSeries-A가 연결을 시작할 때 이 ID를 사용하여 iSeries-A를 식별합니다.
   g. **변형** 페이지에서, **추가**를 클릭하여 iSeries-A가 iSeries-B에 키 보호로 제안하는 변환을 추가하고 1단계 협의를 시작할 때 IKE 정책이 ID 보호를 사용할지 여부를 지정하십시오.
   h. **IKE 정책 변형** 페이지에서, 인증 메소드에 **사전공유 키**를, 해시 알고리즘에 **SHA**를, 암호화 알고리즘에 **3DES-CBC**를 선택하십시오. Diffie-Hellman 그룹 및 Expire IKE 키에 디폴트 값을 허용하십시오.
   i. **확인**을 클릭하여 **변형** 페이지로 리턴하십시오.
   j. **IKE 전체 갱신 모드 조정(ID 보호 없음)**를 선택하십시오.
   k. **확인**을 클릭하여 구성내용을 저장하십시오.
2. **자료 정책 구성**

a. VPN 인터페이스에서, **자료 정책**을 마우스 오른쪽 버튼으로 클릭하고 **신규 자료 정책**을 선택하십시오.

b. **일반** 페이지에서 자료 정책명을 지정하십시오. 예를 들면, l2tpremoteuser를 지정하십시오.

c. **제안** 페이지로 찾아 가십시오. 제안은 개시 및 응답 키 서버가 두 종료점간 동적 연결을 구축하는 데 사용하는 프로토콜 콜렉션입니다. 여러 개의 연결 오브젝트에서 하나의 자료 정책을 사용할 수 있습니다. 그러나 모든 리모트 VPN 키 서버가 반드시 동일한 자료 정책 등록 정보를 가져야 하는 것은 아닙니다. 그러므로 여러 개의 제안을 하나의 자료 정책에 추가할 수 있습니다. 리모트 키 서버에 VPN 연결을 설정할 때에는 최소 하나의 일치하는 제안이 개시자 및 응답자의 자료 정책에 있어야 합니다.

d. **추가**를 클릭하여 자료 정책 변환을 추가하십시오.

e. 캡슐화 모드의 경우 **전송**을 선택하십시오.

f. 키 만기 값을 지정하십시오.

g. **확인**을 클릭하여 **변형** 페이지로 리턴하십시오.

h. **확인**을 클릭하여 신규 자료 정책을 저장하십시오.

3. **동적-키 그룹 구성**

4.

a. VPN 인터페이스에서, **보안 연결**을 확장하십시오.

b. **그룹별**을 마우스 오른쪽 버튼으로 클릭하고 **신규 동적-키 그룹**을 선택하십시오.

c. **일반** 페이지에서 그룹명을 지정하십시오. 예를 들면, l2tptocorp를 지정하십시오.

d. **로컬로 시작된 L2TP 터널 보호**를 선택하십시오.

e. 시스템 역할의 경우, **두 시스템 모두 호스트**를 선택하십시오.

f. **정책** 페이지로 찾아 가십시오. **자료 정책** 드롭 다운 리스트에서 2단계에서 작성한 자료 정책 l2tpremoteuser를 선택하십시오.

g. **로컬 시스템이 연결 시작**을 선택하여 iSeries-A만 iSeries-B로 연결을 시작할 수 있음을 나타내십시오.

h. **연결** 페이지로 찾아 가십시오. **이 그룹에 다음 정책 필터 생성**을 선택하십시오. **편집**을 클릭하여 정책 필터 매개변수를 정의하십시오.

i. **정책 필터 - 로컬 주소** 페이지에서 ID 유형에 **키 ID**를 선택하십시오.

j. ID의 경우, IKE 정책에서 정의한 키 ID thisisthekeyid를 선택하십시오.

k. **정책 필터 - 리모트 주소** 페이지로 찾아 가십시오. **ID 유형** 드롭 다운 리스트에서 **IP 버전 4 주소**를 선택하십시오.

l. **ID** 필드에 205.13.237.6을 입력하십시오.

m. **정책 필터 - 서비스** 페이지로 찾아 가십시오. **로컬 포트** 및 **리모트 포트** 필드에 1701을 입력하십시오. 포트 1701은 잘 알려진 L2TP 포트입니다.

n. **프로토콜** 드롭 다운 리스트에서 **UDP**를 선택하십시오.

o. **확인**을 클릭하여 **연결** 페이지로 리턴하십시오.

p. **인터페이스** 페이지로 찾아 가십시오. 이 그룹이 적용할 회선이나 PPP 프로파일을 선택하십시오. 아직 이 그룹에 PPP 프로파일을 작성하지 않았습니다. 프로파일을 작성한 후 다음 단계에서 사용자가 작성한 PPP 프로파일을 그룹에 적용할 수 있도록 이 그룹의 등록 정보를 편집해야 합니다.

q. **확인**을 클릭하여 동적-키 그룹 l2tptocorp를 작성하십시오.

이제 방금 작성한 그룹에 연결을 추가해야 합니다.

5. **동적-키 연결 구성**

a. VPN 인터페이스에서, **그룹별**을 확장하십시오. iSeries-A에 구성한 모든 동적-키 그룹 리스트가 표시됩니다.

b. **l2tptocorp**를 마우스 오른쪽 버튼으로 클릭하고 **신규 동적-키 연결**을 선택하십시오.

c. **일반** 페이지에서 연결에 대한 선택적 설명을 지정하십시오.

d. 리모트 키 서버의 경우, ID 유형에 **버전 4 IP 주소**를 선택하십시오.

e. **IP 주소** 드롭 다운 리스트에서 `205.13.237.6`을 선택하십시오.

f. **요청시 시작**을 선택 취소하십시오.

g. **로컬 주소** 페이지로 찾아 가십시오. ID 유형에 **키 ID**를 선택한 후 **ID** 드롭 다운 리스트에서 `thisisthekeyid`를 선택하십시오.

h. **리모트 주소** 페이지로 찾아 가십시오. ID 유형에 **IP 버전 4 주소**를 선택하십시오.

i. **ID** 필드에 `205.13.237.6`을 입력하십시오.

j. **서비스** 페이지로 찾아 가십시오. **로컬 포트** 및 **리모트 포트** 필드에 `1701`을 입력하십시오. 포트 1701은 잘 알려진 L2TP 포트입니다.

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

l. **확인**을 클릭하여 동적-키 연결을 작성하십시오.

이제 iSeries-A에 VPN 구성을 완료하였습니다. 다음 단계는 iSeries-A에 PPP 프로파일을 구성하는 것입니다.

2단계: iSeries-A에 PPP 연결 프로파일 및 가상 회선 구성

이 섹션에서는 iSeries-A에 PPP 프로파일을 작성하는 데 수행해야 할 단계를 설명합니다. PPP 프로파일은 그와 연관된 실제 회선이 없는 대신에 가상 회선을 사용합니다. 그 이유는 VPN이 L2TP 터널을 보호하는 동안 PPP 통신량이 L2TP 터널을 통과하기 때문입니다.

iSeries-A에 PPP 연결 프로파일을 작성하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서, iSeries-A **—> 네트워크 —> 리모트 액세스 서비스**를 확장하십시오.
2. **발신자 연결 프로파일**을 마우스 오른쪽 버튼으로 클릭하고 **신규 프로파일**을 선택하십시오.
3. **설정** 페이지에서 프로토콜 유형에 **PPP**를 선택하십시오.
4. 모드 선택의 경우, **L2TP(가상 회선)**를 선택하십시오.
5. **조작 모드** 드롭 다운 리스트에서 **개시자 요청시(자발적 터널)**를 선택하십시오.

6. **확인**을 클릭하여 PPP 프로파일 등록 정보 페이지로 찾아 가십시오.
7. **일반** 페이지에서 연결 유형 및 목적지를 식별하는 이름을 입력하십시오. 이 경우에는 toCORP를 입력하십시오. 지정하는 이름은 10자 이하여야 합니다.
8. (선택적) 프로파일에 대한 설명을 지정하십시오.
9. **연결** 페이지로 찾아 가십시오.
10. **가상 회선명** 필드의 드롭 다운 리스트에서 **tocorp**를 선택하십시오. 이 회선에 연관된 실제 인터페이스가 없다는 점을 기억하십시오. 가상 회선은 이 PPP 프로파일의 다양한 특성을 설명합니다(예: 최대 프레임 크기, 인증 정보, 로컬 호스트 이름 등). **L2TP 회선 등록 정보** 대화상자가 열립니다.
11. **일반** 페이지에서 가상 회선에 대한 설명을 입력하십시오.
12. **인증** 페이지로 찾아 가십시오.
13. **로컬 호스트명** 필드에서 로컬 키 서버의 호스트명 iSeriesA를 입력하십시오.
14. **확인**을 클릭하여 신규 가상 회선 설명을 저장하고 **연결** 페이지로 리턴하십시오.
15. **리모트 터널 종료점 주소** 필드에 리모트 터널 종료점 주소 205.13.237.6을 입력하십시오.
16. **IPSec 보호 필요**를 선택하고, **연결 그룹명** 드롭 다운 리스트에서 1단계에서 작성한 동적-키 그룹 l2tptocorp를 선택하십시오.
17. **TCP/IP 설정** 페이지로 찾아 가십시오.
18. **로컬 IP 주소** 섹션에서 **리모트 시스템에 의해 지정**을 선택하십시오.
19. **리모트 IP 주소** 섹션에서 **고정 IP 주소 사용**을 선택하십시오. 서브네트 주소에 있는 리모트 시스템의 IP 주소인 10.6.11.1을 입력하십시오.
20. 라우팅 섹션에서 **추가 정적 라우트 정의**를 선택하고 **라우트**를 클릭하십시오. PPP 프로파일에 제공된 라우팅 정보가 없는 경우, iSeries-A는 리모트 터널 종료점에만 도달할 수 있을 뿐 10.6.0.0 서브네트 주소의 다른 시스템에는 도달할 수 없습니다.
21. **추가**를 클릭하여 정적 라우트 항목을 추가하십시오.
22. 서브네트 주소 10.6.0.0 및 서브네트 마스크 255.255.0.0을 입력하여 L2TP 터널을 통해 모든 10.6.*.* 통신량을 라우트하십시오.
23. **확인**을 클릭하여 정적 라우트를 추가하십시오.
24. **확인**을 클릭하여 라우팅 대화상자를 닫으십시오.
25. **인증** 페이지로 찾아 가서 이 PPP 프로파일에 대한 사용자명과 암호를 설정하십시오.
26. 로컬 시스템 식별 섹션에서 **리모트 시스템이 이 시스템의 ID를 확인하도록 허용**을 선택하십시오.
27. **사용할 인증 프로토콜** 밑에서 **암호화된 암호(CHAP-MD5) 필요**를 선택하십시오.
28. 사용자명 iSeriesA와 암호를 입력하십시오.
29. **확인**을 클릭하여 PPP 프로파일을 저장하십시오.

3단계: l2tptocorp 동적-키 그룹을 toCorp PPP 프로파일에 적용

PPP 연결 프로파일을 구성한 후에는 작성한 동적-키 그룹 l2tptocorp로 다시 돌아가서 이 그룹을 PPP 프로파일과 연관시켜야 합니다. 이를 수행하려면 다음 단계를 따르십시오.

1. VPN 인터페이스로 이동한 후 **보안 연결 —> 그룹별**을 확장하십시오.
2. 동적-키 그룹 l2tptocorp를 마우스 오른쪽 버튼으로 클릭한 후 **등록 정보**를 선택하십시오.
3. **인터페이스** 페이지로 찾아 가서 2단계에서 작성한 PPP 프로파일 toCorp에 **이 그룹 적용**을 선택하십시오.
4. **확인**을 클릭하여 l2tptocorp를 PPP 프로파일 toCorp에 적용하십시오.

4단계: iSeries-B에 VPN 구성

iSeries-A 구성에 사용한 것과 동일한 단계를 따르고 필요하면 IP 주소와 ID를 반대로 하십시오. 시작하기 전에 다음 사항을 고려하십시오.

- iSeries-A에서 로컬 키 서버에 대해 지정한 키 ID로 리모트 키 서버를 식별하십시오. 예를 들면, thisisthekeyid입니다.
- *정확히* 동일한 사전공유 키를 사용하십시오.
- 변환내용이 iSeries-A에서 구성한 내용과 일치하는지 확인하십시오. 일치하지 않으면, 연결은 실패합니다.
- 동적-키 그룹의 **일반** 페이지에서 **로컬로 시작된 L2TP 터널 보호**를 지정하지 마십시오.
- 리모트 시스템이 연결을 시작합니다.
- 연결이 요청시를 시작하도록 지정하십시오.

5단계: iSeries-B에 PPP 연결 프로파일 및 가상 회선 구성

iSeries-B에 PPP 연결 프로파일을 작성하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서, iSeries-B —> **네트워크 —> 리모트 액세스 서비스**를 확장하십시오.
2. **Receiver 연결 프로파일**을 마우스 오른쪽 버튼으로 클릭하고 **신규 프로파일**을 선택하십시오.
3. **설정** 페이지에서 프로토콜 유형에 **PPP**를 선택하십시오.
4. 모드 선택의 경우, **L2TP(가상 회선)**를 선택하십시오.
5. **조작 모드** 드롭 다운 리스트에서 **종료자(네트워크 서버)**를 선택하십시오.
6. **확인**을 클릭하여 PPP 프로파일 등록 정보 페이지로 찾아 가십시오.
7. **일반** 페이지에서 연결 유형 및 목적지를 식별하는 이름을 입력하십시오. 이 경우에는 tobranch를 입력하십시오. 지정하는 이름은 10자 이하여야 합니다.
8. (선택적) 프로파일에 대한 설명을 지정하십시오.
9. **연결** 페이지로 찾아 가십시오.
10. 로컬 터널 종료점의 IP 주소 205.13.237.6을 선택하십시오.
11. **가상 회선명** 필드의 드롭 다운 리스트에서 **tobranch**를 선택하십시오. 이 회선에 연관된 실제 인터페이스가 없다는 점을 기억하십시오. 가상 회선은 이 PPP 프로파일의 다양한 특성을 설명합니다(예: 최대 프레임 크기, 인증 정보, 로컬 호스트 이름 등). **L2TP 회선 등록 정보** 대화상자가 열립니다.
12. **일반** 페이지에서 가상 회선에 대한 설명을 입력하십시오.

13. **인증** 페이지로 찾아 가십시오.
14. **로컬 호스트명** 필드에서 로컬 키 서버의 호스트명 iSeriesB를 입력하십시오.
15. **확인**을 클릭하여 신규 가상 회선 설명을 저장하고 **연결** 페이지로 리턴하십시오.
16. **TCP/IP 설정** 페이지로 찾아 가십시오.
17. **로컬 IP 주소** 섹션에서 로컬 시스템의 고정 IP 주소 10.6.11.1을 선택하십시오.
18. **리모트 IP 주소** 섹션에서 주소 지정 메소드로 **주소 풀(pool)**을 선택하십시오. 시작 주소를 입력한 후 리모트 시스템에 지정할 수 있는 주소 수를 지정하십시오.
19. **리모트 시스템이 다른 네트워크에 액세스하도록 허용(IP 이송)**을 선택하십시오.
20. **인증** 페이지로 찾아 가서 이 PPP 프로파일에 대한 사용자명과 암호를 설정하십시오.
21. 로컬 시스템 식별 섹션에서 **리모트 시스템이 이 시스템의 ID를 확인하도록 허용**을 선택하십시오. **로컬 시스템 식별** 대화상자가 열립니다.
22. **사용할 인증 프로토콜** 밑에서 **암호화 암호(CHAP-MD5) 필요**를 선택하십시오.
23. 사용자명 iSeriesB와 암호를 입력하십시오.
24. **확인**을 클릭하여 PPP 프로파일을 저장하십시오.

6단계: 패킷 규칙 활성화

VPN은 이 연결이 올바로 작동되는 데 필요한 패킷 규칙을 자동으로 작성합니다. 그러나 VPN 연결을 시작하기 전에 먼저 양쪽 시스템에서 패킷 규칙을 활성화해야 합니다. iSeries-A에서 규칙을 활성화하려면, 다음 단계를 따르십시오.

1. iSeries Navigator에서, **iSeries-A —> 네트워크 —> IP 정책**을 확장하십시오.
2. **패킷 규칙**을 마우스 오른쪽 버튼으로 클릭하고 **활성화**를선택하십시오. 그러면 패킷 규칙 활성화 대화 상자가 열립니다.
3. VPN 생성 규칙만이나 선택한 파일만, 또는 VPN 생성 규칙과 선택된 파일 모두를 활성화할 것인지 선택하십시오. 나중에(예를 들어, VPN 생성 규칙 외에도 인터페이스에 대해 시행하려고 하는 기타 PERMIT 및 DENY 규칙이 있는 경우) 선택할 수도 있습니다.
4. 규칙을 활성화할 인터페이스를 선택하십시오. 이 경우에는 **모든 인터페이스**를 선택하십시오.
5. 대화상자에서 **확인**을 클릭하여 지정한 인터페이스에 대해 규칙을 확인하고 활성화를 확인하십시오. 확인을 클릭하고 나면, 시스템은 구문 및 시멘틱 오류에 대해 규칙을 검사하고 편집기의 맨 아래에 있는 메세지 창에 결과를 보고합니다. 특정 파일 및 행 번호와 연관되는 오류 메세지에 대해, 오류를 마우스 오른쪽 버튼으로 클릭하고 **행 찾아 가기**를 선택하여 파일에서 오류를 강조표시할 수 있습니다.
6. iSeries-B에서 패킷 규칙을 활성화하려면 위 단계를 반복하십시오.

7단계: 연결 시작

마지막 단계는 연결을 시작하는 단계입니다. L2TP 연결을 개시하기 전에 먼저 L2TP 종료자가 개시자 요구에 응답할 수 있어야 합니다. 요구된 모든 서비스가 시작되는지 확인한 후, 종료자 측에서 PPP 연결을 시작하십시오. 다음 단계에서는 iSeries-B에서 PPP 연결을 시작하는 방법을 설명합니다.

1. iSeries Navigator에서, iSeries-B —> **네트워크** —> **리모트 액세스 서비스**를 확장하십시오.
2. **응답자 연결 프로파일**을 클릭하여 오른쪽 분할 창에 응답자 프로파일 리스트를 표시하십시오.
3. tobranch를 마우스 오른쪽 버튼으로 클릭하고 **시작**을 선택하십시오. 연결 프로파일이 시작된 후, 창이 화면정리되어 연결이 연결 요구 대기 중으로 표시됩니다. 이제, iSeries-A가 iSeries-B의 L2TP 연결 요구에 응답할 수 있습니다.

iSeries-A에서 L2TP 연결을 시작하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서, iSeries-A —> **네트워크** —> **리모트 액세스 서비스**를 확장하십시오.
2. **발신자 연결 프로파일**을 클릭하여 오른쪽 분할 창에 응답자 프로파일 리스트를 표시하십시오.
3. **toCORP**를 마우스 오른쪽 버튼으로 클릭한 후 **시작**을 선택하십시오. 연결 프로파일이 시작된 후, 창이 화면정리되어 연결이 L2TP 터널 설정으로 표시됩니다.
4. F5 키를 눌러 화면정리하십시오. L2TP 터널이 시작된 경우, 연결 상태는 이제 활동 연결로 표시됩니다.

VPN 시나리오: VPN에 대한 네트워크 주소 변환 사용

미네아폴리스에 있는 작은 제조업체의 네트워크 관리자라고 가정합니다. 업부 상대 중 하나인 시카고의 부품 공급업체는 인터넷을 통해 회사와의 더 많은 업무 수행을 시작하려고 합니다. 제조업체가 요구하는 정확한 시간에 특정 부품 및 수량을 확보하는 것이 매우 중요하기 때문에, 항상 제조업체의 재고 상태 및 생산 스케줄을 알고 있어야 합니다. 현재 이 상호작용을 수동으로 처리하고 있지만, 처리하는 데 시간이 많이 걸리고 비용도 많이 들며 심지어 때로는 부정확하다고 느껴져서, 옵션을 더 많이 조사하려고 합니다.

교환하는 정보가 기밀성과 시간에 민감한 성질을 가지고 있어서, 공급업체의 네트워크와 회사의 네트워크 사이에 VPN을 작성할 것을 결정합니다. 회사 네트워크 구조의 개인보호정책을 추가로 보호하기 위해, 공급업체가 액세스를 가지고 있는 어플리케이션을 호스팅하는 iSeries의 개인 IP 주소를 감출 것을 결정합니다. 여기서 질문은 이 작업을 수행하는 방법은 무엇입니까?

답은 OS/400 VPN입니다. 회사 네트워크의 VPN 게이트웨이에서 연결 정의를 작성 뿐만 아니라 로컬 개인 주소를 숨겨야 하는 주소 변환을 제공하려면 이를 사용하십시오. VPN이 기능해야 하는 보안 협약(SA)에서 IP 주소를 변경하는 전통적인 네트워크 주소 변환(NAT)과는 달리, VPN NAT는 연결이 시작될 때 연결에 주소를 지정하여 SA가 유효화되기 전에 주소 변환을 수행합니다.

목적

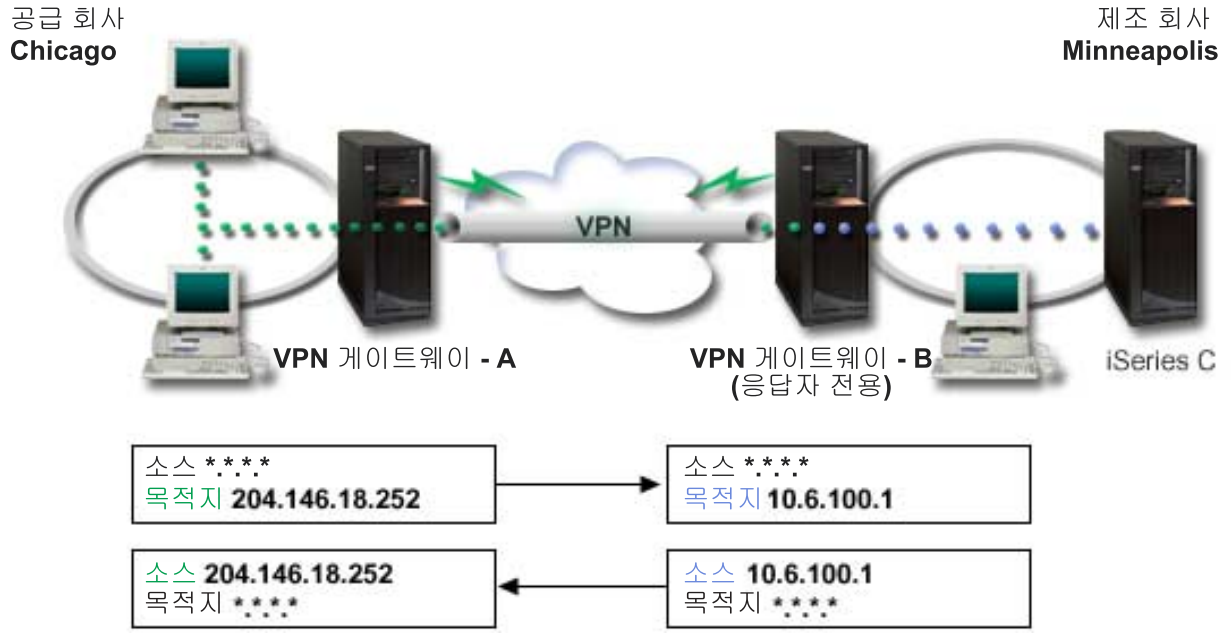
이 시나리오의 목적은 다음과 같습니다.

- 공급업체 네트워크에 있는 모든 클라이언트가 게이트웨이간 VPN 연결을 통해 제조업체의 네트워크에서 단일 호스트 iSeries에 액세스할 수 있게 합니다.

- VPN에 대한 네트워크 주소 변환(VPN NAT)을 사용하여 개인 IP 주소를 공용 IP 주소로 변환하여, 제조 업체의 네트워크에서 호스트 iSeries의 개인 IP 주소를 숨깁니다.

세부사항

다음 다이어그램은 공급업체 네트워크와 제조 네트워크 둘 다의 네트워크 특성을 보여줍니다.



- VPN 게이트웨이 A는 항상 VPN 게이트웨이 B에 대한 연결을 초기화하도록 구성됩니다.
- VPN 게이트웨이 A는 연결에 대한 목적지 종료점을 204.146.18.252(iSeries-C에 지정된 공용 주소)로 정의합니다.
- iSeries-C에는 제조업체 네트워크 10.6.100.1에 IP 주소를 가지고 있습니다.
- iSeries-C의 개인 주소 10.6.100.1에 대해 VPN 게이트웨이 B에서 로컬 서비스 풀에 공용 주소 204.146.18.252가 정의되었습니다.
- VPN 게이트웨이 B는 인바운드 데이터그램에 대해 iSeries-C의 공용 주소를 해당되는 개인 주소 10.6.100.1로 변환합니다. VPN 게이트웨이 B는 리턴되는 아웃바운드 데이터그램을 10.6.100.1에서 다시 iSeries-C의 공용 주소 204.146.18.252로 변환합니다. 공급업체 네트워크의 클라이언트가 관련되어 있는 한, iSeries-C는 IP 주소 204.146.18.252를 갖습니다. 클라이언트는 주소 변환이 발생했다는 것을 인식하지 못해야 합니다.

타스크 구성

이 시나리오에 설명된 연결을 구성하려면 다음 타스크 각각을 완료해야 합니다.

1. **VPN 게이트웨이 A** 및 **VPN 게이트웨이 B** 사이의 게이트웨이간 VPN을 구성하십시오.
2. **VPN 게이트웨이 B**에서 로컬 서비스 풀을 정의하여 **iSeries-C**의 개인 주소를 공용 ID 204.146.18.252 뒤에 숨기십시오.
3. 로컬 서비스 풀 주소를 사용하여 로컬 주소를 변환하도록 **VPN 게이트웨이 B**를 구성하십시오.

VPN 개념

VPN(가상 사설망)은 몇 개의 중요한 TCP/IP 프로토콜을 사용하여 자료 통신을 보호합니다. VPN 연결 작동 방법을 보다 잘 이해하려면 이 프로토콜과 개념, OS/400 VPN이 이 프로토콜을 사용하는 방법을 잘 알고 있어야 합니다.

- **IP 보안(IPSec) 프로토콜**
  IPSec는 네트워크 레이어 보안을 제공하기 위한 안정적이고 지속적인 기반을 제공합니다.
- **키 관리**
  동적 VPN은 키 관리를 위해 인터넷 키 교환(IKE)을 사용하여 통신에 추가 보안을 제공합니다. IKE는 연결 각 끝에 있는 VPN 서버가 지정된 간격으로 신규 키를 협상할 수 있게 합니다.
- **L2TP(Layer 2 Tunneling Protocol)**
  VPN 연결을 사용하여 네트워크와 리모트 클라이언트간 통신 보안을 수행하려면 L2TP(Layer 2 Tunneling Protocol)도 잘 알아야 합니다.
- **VPN에 대한 네트워크 주소 변환(VPN NAT)**
  OS/400 VPN은 네트워크 주소 변환(VPN NAT)을 수행하기 위한 수단을 제공합니다. VPN NAT는 IKE 및 IPSec 프로토콜을 적용하기 전에 주소를 변환한다는 점에서 일반적인 NAT와 다릅니다. 자세히 배우려면 다음 주제를 참조하십시오.
- **UDP 캡슐화**
  UDP 캡슐화는 IPSec 통신이 전통적인 NAT 장치를 통해 전달되도록 합니다. 캡슐화가 무엇이고 VPN 연결에 대해 이를 사용해야 하는 이유에 대한 자세한 정보는 다음 주제를 검토하십시오.
- **IP 압축(IPComp)**
  IPComp는 두 VPN 상대방간 통신 성능을 향상시키기 위해 데이터그램을 압축하여 IP 데이터그램 크기를 줄입니다.
- **VPN 및 IP 필터링**
  IP 필터링 및 VPN은 거의 관련되어 있습니다. 사실, 대부분의 VPN 연결에서 필터 규칙이 적절하게 작동되어야 합니다. 이 주제는 VPN에서 요고하는 필터와 VPN에 관련되는 기타 필터링 개념에 대한 정보를 제공합니다.

IP 보안(IPSec) 프로토콜

IPSec는 네트워크 보안을 제공하기 위한 안정적이고 오래 지속되는 기반을 제공합니다. IPSec는 현재 사용되는 모든 암호 알고리즘을 지원하고, 향후 사용될 더욱 새롭고 강력한 알고리즘도 지원할 수 있습니다. IPSec 프로토콜은 다음과 같은 주요 보안 논점을 처리합니다.

자료 원점 인증
각 데이터그램이 요구받은 송신자로부터 기원하였음을 확인합니다.
자료 무결성
데이터그램의 내용이 고의적으로 또는 임의적 오류로 인해 전송 과정에서 변경되지 않았음을 확인합니다.
자료 비밀성
일반적으로 암호화를 사용하여 메세지 내용을 감춥니다.
재생 방지
공격자가 데이터그램을 가로채거나 나중에 다시 재생할 수 없게 합니다.

암호화 키 및 보안 연관(SA)의 자동 관리
약간의 수동 조작 또는 아무런 수동 조작도 하지 않은 구성의 확장 네트워크를 통해 VPN 정책을 구현할 수 있게 합니다.

VPN은 인증 헤더(AH) 및 보안 ESP(보안 페이로드 캡슐화)라는 두 개의 IPSec 프로토콜을 사용하여 VPN을 통해 흐르는 자료를 보호합니다. IPSec 구현의 다른 부분은 인터넷 키 교환(IKE) 프로토콜 또는 키 관리입니다. IPSec이 자료를 암호화하는 동안, IKE는 보안 연관(SA)의 자동 대화 및 암호화 키의 자동 생성과 화면정리를 지원합니다.

주요 IPSec 프로토콜은 다음과 같습니다.

- **AH 프로토콜**
- **ESP 프로토콜**
- **AH 및 ESP 결합 프로토콜**
- **IKE 프로토콜**

IETF(Internet Engineering Task Force)는 IPSec를 RFC(Request for Comment) 2401, *인터넷 프로토콜용 보안 구조*에서 공식적으로 정의하고 있습니다. 인터넷 웹 사이트 http://www.rfc-editor.org 에서 이 RFC를 볼 수 있습니다.

인증 헤더

인증 헤더(AH) 프로토콜은 자료 원점 인증, 자료 무결성 및 재생 방지를 제공합니다. 그러나 AH는 자료 비밀성을 제공하지 않기 때문에 모든 자료가 암호가 아닌 명시적 문장으로 전송됩니다.

AH는 MD5와 같은 메세지 인증 코드가 생성하는 체크섬을 사용하여 자료 무결성을 보장합니다. AH에는 인증용으로 사용하는 알고리즘에 비밀 공유 키를 포함시켜 자료 원점 인증을 보장합니다. AH는 AH 헤더 내부에서 순번 필드를 사용하여 재생 방지를 보장합니다. 이 세 개의 고유한 기능을 통틀어 **인증**이라고 부르기도 하는데, 여기에 주목할 필요가 있습니다. 가장 간단하게 말해서, AH는 자료가 최종 목적지까지 가는 도중에 변경되지 않음을 보장합니다.

AH가 IP 데이터그램을 최대한 인증하더라도, 리시버는 IP 헤더에 있는 특정 필드의 값을 예상할 수 없습니다. AH는 **변하기 쉬운** 필드로 알려진 이 필드를 보호하지 않습니다. 그러나 AH는 항상 IP 패킷의 페이로드를 보호합니다.

IETF(Internet Engineering Task Force)는 AH를 RFC(Request for Comment) 2402, *IP 인증 헤더*에서 공식적으로 정의하고 있습니다. 인터넷 웹 사이트 http://www.rfc-editor.org 에서 이 RFC를 볼 수 있습니다.

AH 사용 방법

AH를 전송 모드 또는 터널 모드의 두 가지 방법으로 적용할 수 있습니다. 전송 모드에서, 데이터그램의 IP 헤더는 가장 외부의 IP 헤더인데, 그 다음에는 AH 헤더가 뒤따르고 그리고 데이터그램 페이로드가 위치합니다. AH는 변하기 쉬운 필드를 제외한 전체 데이터그램을 인증합니다. 그러나 데이터그램에 담긴 정보는 암호문이 아닌 명시적 문장으로 전송되므로 그 보안이 보장되지 않습니다. 전송 모드는 터널 모드보다 적은 오버헤드 처리가 필요하지만, 충분한 보안을 제공하지 않습니다.

터널 모드는 신규 IP 헤더를 작성한 후 이를 데이터그램의 가장 외부에 있는 IP 헤더로서 사용합니다. AH 헤더는 신규 IP 헤더 다음에 위치합니다. 원래의 데이터그램(IP 헤더 및 원래의 페이로드 모두)은 가장 마지막으로 위치합니다. AH는 전체 데이터그램을 인증하는데, 이는 데이터그램이 전송 과정에서 변경되었는지의 여부를 응답 시스템에서 감지할 수 있음을 의미합니다.

보안 연관의 한쪽 끝이 게이트웨이일 경우, 터널 모드를 사용하십시오. 터널 모드에서, 가장 외부의 IP 헤더에 있는 소스 및 목적지 주소가 원래의 IP 헤더에 있는 주소와 동일할 필요는 없습니다. 예를 들어, 두 개의 보안 게이트웨이 터널을 작동하여 그들이 함께 연결한 네트워크 사이에서 발생하는 모든 통신을 인증할 수 있습니다. 실제로, 이 구성 형태가 가장 일반적입니다.

터널 모드 사용의 기본 장점은 터널 모드가 캡슐화된 IP 데이터그램을 완전히 보호한다는 점입니다. 또한 터널 모드는 사설 주소를 사용할 수 있게 합니다.

AH를 선택해야 하는 이유는?
대부분의 경우, 자료는 인증만 요구합니다. ESP(보안 페이로드 캡슐화 프로토콜이 인증을 수행할 수 있는 반면에, AH는 ESP처럼 시스템 성능에 영향을 미치지 않습니다. AH 사용의 또다른 장점은 AH가 전체 데이터그램을 인증한다는 점입니다. 반면, ESP는 ESP 헤더 앞에 있는 IP 헤더 또는 기타 정보를 인증하지 않습니다.

또한 ESP를 구현하려면 강력한 암호 알고리즘이 필요합니다. AH가 규제를 받지 않고 전세계적으로 자유롭게 사용될 수 있는 반면, 강력한 암호는 일부 국가에서 제한됩니다.

AH가 정보를 보호하는 데 사용하는 알고리즘은 무엇입니까?
AH는 **헤시 메세지 인증 코드(HMAC)**라는 알고리즘을 사용합니다. 특히, VPN은 HMAC-MD5 또는 HMAC-SHA 중 하나를 사용합니다. MD5 및 SHA는 모두 가변 길이 입력 자료 및 비밀 키를 사용하여 고정 길이 출력 자료(해시 값이라 함)를 생성합니다. 두 메세지의 해시가 일치하는 경우에는 메세지가 동일할 가능성이 매우 높습니다. MD5 및 SHA 모두 메세지 길이를 출력할 때 코드화하지만, SHA가 더욱 큰 해시를 생성하기 때문에 보다 안전하다고 간주됩니다.

IETF(Internet Engineering Task Force)는 HMAC-MD5를 RFC(Request for Comments) 2085, *재생 방지를 사용한 HMAC-MD5 IP 인증*에서 공식적으로 정의하고 있습니다. IETF(Internet Engineering Task Force)는 HMAC-SHA를 RFC(Request for Comments) 2404, *ESP 및 AH 내에서의 HMAC-SHA-1-96 사용*에서 공식적으로 정의하고 있습니다. 인터넷 웹 사이트 http://www.rfc-editor.org 에서 이 RFC를 볼 수 있습니다.

보안 페이로드 캡슐화

ESP(Encapsulatong Security Payload) 프로토콜은 자료 비밀성을 제공하고 자료 원점 인증, 자료 무결성 점검 및 재생 방지도 선택적으로 제공합니다. ESP와 인증 헤더(AH) 프로토콜의 차이점은 ESP가 암호화를 제공한다는 점이며, 두 가지 프로토콜 모두 인증, 무결성 검사 및 재생 방지를 제공합니다. ESP와 함께, 두 통신 시스템은 모두 공유 키를 사용하여 교환 자료를 암호화하고 암호를 해독합니다.

두 암호화 및 인증을 모두 사용하려는 경우, 응답 시스템은 먼저 패킷을 인증하고 첫 번째 단계가 완료되면 암호를 해독합니다. 이 구성 유형은 오버헤드 처리를 줄일 뿐만 아니라, 서비스 거부 공격에 대한 취약성을 줄입니다.

ESP를 사용하는 두 가지 방법

ESP를 전송 모드 또는 터널 모드의 두 가지 방법으로 적용할 수 있습니다. 전송 모드에서, ESP 헤더는 원래 IP 데이터그램의 IP 헤더 다음에 위치합니다. IPSec 헤더가 이미 데이터그램에 있는 경우에는 그 앞에 ESP 헤더가 위치합니다. ESP 트레일러 및 선택적 인증 자료는 페이로드 다음에 위치합니다.

전송 모드는 IP 헤더를 인증하거나 암호화하지 않는데, 이는 데이터그램이 전송되는 과정에서 잠재적 공격자에게 주소지정 정보를 노출시킬 수 있습니다. 전송 모드는 터널 모드보다 적은 오버헤드 처리가 필요하지만, 충분한 보안을 제공하지 않습니다. 대부분의 경우, 호스트는 ESP를 전송 모드로 사용합니다.

터널 모드는 신규 IP 헤더를 작성한 후 이를 데이터그램의 가장 외부에 있는 IP 헤더로서 사용하는데, 그 다음에는 ESP 헤더가 뒤따르고 그 다음에는 원래 데이터그램(IP 헤더 및 원래 페이로드 모두)이 위치합니다. ESP 트레일러 및 선택적 인증 자료는 페이로드에 첨부됩니다. 암호화 및 인증을 모두 사용할 때, 원래 데이터그램이 이제는 신규 ESP 패킷에 대한 페이로드 자료가 되었기 때문에 ESP는 원래 데이터그램을 완전히 보호합니다. 그러나 ESP는 신규 IP 헤더를 보호하지 않습니다. 게이트웨이는 ESP를 터널 모드로 사용해야 합니다.

ESP가 정보를 보호하는 데 사용하는 알고리즘은 무엇입니까?

ESP는 두 통신 당사자가 모두 교환 자료를 암호화하고 암호를 해독하는 데 사용하는 대칭 키를 사용합니다. 송신자 및 리시버는 그들 사이에서 보안 통신이 발생하기 전에 먼저 키를 동의해야 합니다. OS/400 VPN은 자료 암호화 표준(DES), 3중 DES(3DES), RC5, RC4 및 확장 암호화 표준(AES)를 사용하여 암호화합니다.

IETF(Internet Engineering Task Force)는 DES를 RFC(Request for Comment) 1829, *ESP DES-CBC 변환*에서 공식적으로 정의하고 있습니다. IETF(Internet Engineering Task Force)는 3DES를 RFC 1851, *ESP 3DES 변환*에서 공식적으로 정의하고 있습니다. IETF(Internet Engineering Task Force)는 3DES를 RFC 1851, *ESP Triple DES 변환*에서 공식적으로 정의하고 있습니다. 인터넷 웹 주소 http://www.rfc-editor.org 에서 이 RFC를 볼 수 있습니다.

ESP는 HMAC-MD5 및 HMAC-SHA 알고리즘을 사용하여 인증 기능을 제공합니다. MD5 및 SHA는 모두 가변 길이 입력 자료 및 비밀 키를 사용하여 고정 길이 출력 자료(해시 값이라 함)를 생성합니다. 두 메세지의 해시가 일치하는 경우에는 메세지가 동일할 가능성이 매우 높습니다. MD5 및 SHA 모두 메세지 길이를 출력할 때 코드화하지만, SHA가 더욱 큰 해시를 생성하기 때문에 보다 안전하다고 간주됩니다.

IETF(Internet Engineering Task Force)는 HMAC-MD5를 RFC(Request for Comments) 2085, *재생 방지를 사용한 HMAC-MD5 IP 인증*에서 공식적으로 정의하고 있습니다. IETF(Internet Engineering Task Force)는 HMAC-SHA를 RFC(Request for Comments) 2404, *ESP 및 AH 내에서의 HMAC-SHA-1-96 사용*에서 공식적으로 정의하고 있습니다. 인터넷 웹 주소 http://www.rfc-editor.org 에서 이 RFC를 볼 수 있습니다 .

AH 및 ESP 결합

VPN은 호스트간 연결에 AH 및 ESP를 전송 모드로 결합할 수 있게 합니다. 두 프로토콜을 결합하면 전체 IP 데이터그램이 보호됩니다. 두 프로토콜을 결합하면 보안을 더욱 강하게 유지할 수 있지만, 관련 오버헤드 처리가 이 장점보다 더욱 중요할 수 있습니다.

키 관리

각각의 협의가 끝나면, VPN 서버는 연결을 보호하는 키를 재생성하므로 공격자가 연결로부터 정보를 캡처하기가 더욱 어렵게 됩니다. 또한 완벽한 전송 비밀을 사용하는 경우에는 공격자가 기존의 키 지정 정보를 근거로 그 이후의 키를 도출해낼 수 없습니다.

VPN 키 관리자는 인터넷 키 교환(IKE) 프로토콜을 IBM이 구현한 것입니다. 키 관리자는 보안 협약(SA)의 자동 협의 및 암호화 키 자동 생성과 화면정리를 지원합니다.

보안 협약(SA)에는 IPSec 프로토콜을 사용하는 데 필요한 정보가 들어 있습니다. 예를 들면, SA는 알고리즘 유형, 키 길이와 수명, 참여 당사자 및 캡슐화 모드를 식별합니다.

이름에서 알 수 있듯이, 암호 키는 최종 목적지에 안전하게 도달할 때까지 정보를 잠그거나 보호합니다.

주: 안전하게 키를 생성하는 것이 안전한 비밀 연결을 설정하는 데 가장 중요한 요소입니다. 키가 손상되면 인증 및 암호화 노력이 아무리 강력하더라도 소용이 없습니다.

키 관리 단계

VPN 키 관리자는 구현시 두 개의 고유한 단계를 사용합니다.

1단계

1단계는 사용자 자료 통신량을 보호하기 위한 후속 암호 키가 도출되는 마스터 비밀을 설정합니다. 이는 두 종료점 간에 아무런 안전 보호가 없더라도 적용됩니다. VPN은 RSA 모드나 사전공유 키를 사용하여 1단계 협의를 인증할 뿐만 아니라, 후속 2단계 협의 과정에서 흐르는 IKE 메세지를 보호하는 키도 설정합니다.

*사전공유 키*는 최대 128자나 되는 스트링입니다. 양쪽 연결 끝이 모두 사전공유 키에 동의해야 합니다. 사전공유 키를 사용할 때 장점은 간단하다는 점이고, 단점은 IKE 협의에 앞서 공유 비밀이 대역 밖에서(예를 들면, 전화나 등록된 메일을 통해) 분배되어야 한다는 점입니다. 사전공유 키를 암호처럼 취급해야 합니다.

RSA 서명 인증은 디지털 인증을 사용하여 인증을 제공하기 때문에 사전공유 키에 비해 보안이 잘 됩니다. 디지털 인증 관리자(5722-SS1 옵션 34)를 사용하여 디지털 인증을 구성해야 합니다. 또한 일부 VPN 솔루션에는 상호운영성을 위해 RSA 서명이 필요합니다. 예를 들면, Windows 2000 VPN은 RSA 서명을 디폴트 인증 메소드로 사용합니다. 마지막으로, RSA 서명은 사전공유 키에 비해 스케일러빌리티가 높습니다. 양쪽 키 서버가 모두 신뢰하는 인증 기관의 인증을 사용해야 합니다.

2단계

반면에, 2단계는 실제 어플리케이션 자료 교환을 보호하는 키와 보안 협약을 협상합니다. 현재까지 어떤 어플리케이션 자료도 실제로 송신되지 않았음을 기억하십시오. 1단계는 2단계 IKE 메세지를 보호합니다.

2단계 협의가 완료되면, VPN은 정의된 연결 종료점간에 네트워크를 통한 안전한 동적 연결을 설정합니다. VPN을 통해 흐르는 모든 자료는 1단계 및 2단계 협의 프로세스 동안에 키 서버가 동의했던 보안 및 효율성 수준으로 전달됩니다.

일반적으로, 1단계 협의는 매일 한 번씩 협상되는 반면, 2단계 협의는 60분마다 또는 5분마다 화면정리됩니다. 화면정리 비율을 높일수록 자료 보안이 증가하지만, 시스템 성능은 감소합니다. 가장 민감한 자료를 보호하려면 키 수명을 짧게 사용하십시오.

iSeries Navigator를 사용하여 동적 VPN을 작성할 때, IKE 정책 정의를 수행하여 1단계 협의가 작동할 수 있도록 하고 자료 정책을 정의하여 2단계 협의를 제어해야 합니다. 선택적으로, 신규 연결 마법사를 사용할 수 있습니다. 마법사는 IKE 정책, 자료 정책을 포함하여, VPN이 적절하게 작동하는 데 필요한 각각의 구성 오브젝트를 자동으로 작성합니다.

제안된 읽기 자료

인터넷 키 교환(IKE) 프로토콜 및 키 관리에 대한 자세한 내용은 다음 IETF(Internet Engineering Task Force) 및 RFC(Request for Comments)를 검토하십시오.

- RFC 2407, *ISAKMP 해석에 대한 인터넷 IP 보안 정의역*
- RFC 2408, *인터넷 보안 협약 및 키 관리 프로토콜(ISAKMP)*
- RFC 2409, *인터넷 키 교환(IKE)*

인터넷 웹 사이트 http://www.rfc-editor.org 에서 이 RFC를 볼 수 있습니다.

L2TP(Layer 2 Tunnel Protocol)

가상 회선이라고도 하는 L2TP 연결은 사내 네트워크 서버가 리모트 사용자에게 할당된 IP 주소를 관리하게 하여 리모트 사용자를 위한 비용 효율적 액세스를 제공합니다. 또한 L2TP 연결을 IP 보안(IPSec)과 함께 사용하면 시스템 또는 네트워크에 대한 보안 액세스가 제공됩니다.

L2TP는 자발적 터널 및 강제적 터널의 두 가지 터널 모드를 지원합니다. 두 터널 모드간 주요 차이점은 종료점입니다. 자발적 터널에서는 터널이 리모트 클라이언트에서 종료되지만, 강제적 터널에서는 터널이 ISP에서 종료됩니다.

L2TP **강제적 터널**이 사용되는 경우, 리모트 호스트는 인터넷 서비스 제공자(ISP)로 연결을 시작합니다. 그러면, ISP는 리모트 사용자와 사내 네트워크 사이에서 L2TP 연결을 구축합니다. ISP가 연결을 설정하더라도, VPN을 사용하여 통신 보호 방법을 결정하십시오. 강제적 터널이 사용되는 경우, ISP는 LT2P를 지원해야 합니다.

L2TP **자발적 터널**이 사용되는 경우, 리모트 사용자는 일반적으로 L2TP 터널링 클라이언트를 사용하여 연결을 작성합니다. 결과적으로, 리모트 사용자는 L2TP 패킷을 ISP에게 송신하고 ISP는 이를 사내 네트워크로 전송합니다. 자발적 터널이 사용되는 경우, ISP는 L2TP를 지원할 필요가 없습니다. 시나리오 *IPSec을 사용하여 L2TP 임의 터널 보호*는 지점 iSeries가 VPN이 보호하는 L2TP 터널을 사용하여 게이트웨이를 통해 회사 네트워크에 연결하도록 구성하는 방법에 대한 예를 제공합니다.

L2TP는 실제로 IP 캡슐화 프로토콜을 변화시킨 것입니다. L2TP 터널은 L2TP 프레임을 사용자 데이터그램 프로토콜(UDP) 패킷 내부로 캡슐화하여 작성됩니다. 여기서, UDP는 반대로 IP 패킷 내부로 캡슐화됩니다. 이 IP 패킷의 소스 및 목적지 주소는 연결 종료점을 정의합니다. 외부의 캡슐화 프로토콜이 IP이기 때문에, IPSec

프로토콜은 복합 IP 패킷에 적용될 수 있습니다. 이렇게 하면, L2TP 터널 내에서 흐르는 자료가 보호됩니다. 그러면, 인증 헤더(AH), ESP(보안 페이로드 캡슐화) 및 인터넷 키 교환(IKE) 프로토콜을 간단하게 적용할 수 있습니다.

VPN에 대한 네트워크 주소 변환

네트워크 주소 변환(NAT)은 사설 IP 주소를 가져와 공용 IP 주소로 변환합니다. 이것은 네트워크의 호스트가 인터넷을 통해(또는 다른 공용 네트워크를 통해) 리모트 호스트와 서비스에 액세스할 수 있도록 하는 동시에 귀한 공용 주소도 보존하는 데 도움이 됩니다.

또한 사설 IP 주소를 사용하는 경우에는 IP 주소가 유사한 수신 IP 주소와 충돌할 수 있습니다. 예를 들어, 다른 네트워크와 통신하려는 경우, 두 네트워크가 모두 주소 10.*.*.*를 사용하면 주소가 충돌하여 모든 패킷이 드롭(drop)됩니다. 아웃바운드 주소에 NAT를 적용하면 이 문제를 해결할 수 있습니다. 그러나 VPN이 자료 통신을 보호하는 경우, VPN이 기능하는 데 필요한 보안 협약(SA)에 있는 IP 주소를 변경하기 때문에 일반적인 NAT가 작동하지 않습니다. 이런 문제점이 발생하지 않도록 VPN은 VPN NAT라는 고유한 네트워크 주소 변환 버전을 제공합니다. VPN NAT는 연결이 시작될 때 연결에 주소를 지정하여 SA가 유효화되기 전에 주소 변환을 수행합니다. 이 주소는 연결이 삭제될 때까지 해당 연결과 연관된 상태를 유지합니다.

주: FTP는 현재 VPN NAT를 지원하지 않습니다.

VPN NAT를 어떻게 사용해야 합니까?

시작하기 전에 고려해야 할 두 가지 서로 다른 VPN NAT 유형이 있습니다. 다음과 같습니다.

IP 주소 충돌을 방지하기 위한 VPN NAT

이 VPN NAT 유형을 사용하면 유사한 주소지정 체계를 사용하는 네트워크 또는 시스템간에 VPN 연결을 구성할 때 가능한 IP 주소 충돌을 피할 수 있습니다. 일반적인 시나리오는 두 회사가 지정된 사설 IP 주소 범위 중 하나를 사용하여 VPN 연결을 작성하려는 시나리오입니다(예: 10.*.*.*). 이 VPN NAT 유형 구성 방법은 서버가 VPN 연결에 대한 개시자인지 아니면 응답자인지에 따라 다릅니다. 서버가 연결 개시자인 경우에는 로컬 주소를 VPN 연결 상대의 주소와 호환되는 주소로 변환할 수 있습니다. 서버가 연결 응답자인 경우에는 VPN 상대의 리모트 주소를 로컬 주소지정 체계와 호환되는 주소로 변환할 수 있습니다. 동적 연결에 대해서만 이 주소 변환 유형을 구성하십시오.

로컬 주소를 숨기기 위한 VPN NAT

이 VPN NAT 유형은 주소를 공개적으로 사용할 수 있는 다른 주소로 변환하여 로컬 시스템의 실제 IP 주소를 숨기는 데 주로 사용됩니다. VPN NAT를 구성할 때, 공용으로 알려진 각 IP 주소를 숨겨진 주소 풀(pool) 중 하나로 변환하도록 지정할 수 있습니다. 또한 복수 주소를 사용하여 개별 주소에 대한 통신량 로드의 밸런스를 유지할 수도 있습니다. 로컬 주소용 VPN NAT를 사용하려면 서버가 연결에 대한 응답자의 역할을 해야 합니다.

다음 질문에 대한 응답이 예인 경우에는 로컬 주소를 숨기기 위해 VPN NAT를 사용하십시오.

1. VPN을 사용하여 다른 사용자가 액세스하게 하려는 서버가 하나 이상 있습니까?
2. 시스템의 실제 IP 주소에 대해 유연성을 부여해야 합니까?
3. 글로벌로 라우트할 수 있는 IP 주소가 하나 이상 있습니까?

시나리오 *VPN에 대한 네트워크 주소 변환 사용*은 iSeries에서 로컬 주소를 숨기기 위해 VPN NAT를 구성하는 방법에 대한 예를 제공합니다.

iSeries에서 VPN NAT를 설정하는 방법에 대한 단계별 지시사항에 대해서는 iSeries Navigator에서 VPN 인터페이스를 통해 사용 가능한 온라인 도움말을 참조하십시오.

NAT 호환 IPSec

문제점: 전통적인 NAT가 VPN을 일시 중단함
네트워크 주소 변환(NAT)은 등록된 IP 주소 세트 뒤에 등록되지 않은 개인 IP 주소를 숨기는 것을 허용합니다. 이렇게 하면 외부 네트워크로부터 내부 네트워크를 보호할 수 있습니다. NAT는 또한 많은 개인 주소가 작은 등록 주소 세트로 표시될 수 있으므로 IP 주소 소모 문제점을 완화시키는 데 도움을 줍니다.

불행히도, 전통적인 NAT는 패킷이 NAT 장치를 통해 이동할 때 패킷의 소스 주소가 변경되어 패킷이 유효하지 않게 되므로 IPSec 패킷에 대해 작동되지 않습니다. 이러한 상황이 발생하면, VPN 연결의 수신측에서 패킷을 버리므로 VPN 연결 협의가 실패합니다.

솔루션: UDP 캡슐화
nutshell에서, UDP 캡슐화는 새 것이지만 중복되는 IP/UDP 헤더 내에서 IPSec 패킷을 랩핑합니다. 새 IP 헤더의 주소는 NAT 장치를 통과할 때 변환됩니다. 그러면, 패킷이 목적지에 도달할 때 수신측이 추가 헤더를 분해하여 원래 IPSec 패킷(지금은 다른 모든 유효성 검증을 통과해야 하는)을 버립니다.

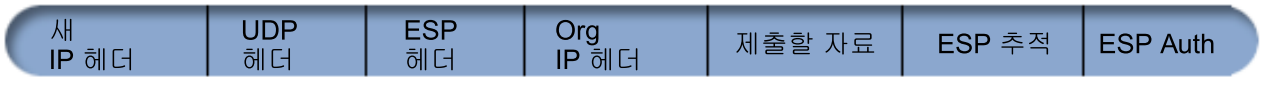
터널 모드나 전송 모드에서 IPSec ESP를 사용할 UDP 캡슐화만 VPN에 적용할 수 있습니다. 또한 V5R2에서는, iSeries가 UDP 캡슐화에 대한 클라이언트로만 작동할 수 있습니다. 즉, UDP 캡슐화 통신을 *초기화*할 수만 있습니다.

아래 그래픽은 터널 모드에서의 UDP 캡슐화 ESP 패킷 형식을 보여줍니다.

원래 IPv4 데이터그램

터널 모드에서 IPSec ESP 적용 후:

UDP 캡슐화 적용 후:



아래 그래픽은 전송 모드에서의 UDP 캡슐화 ESP 패킷 형식을 보여줍니다.

원래 IPv4 데이터그램

전송 모드에서 IPSec ESP 적용 후:

UDP 캡슐화 적용 후:

패킷이 캡슐화되면, iSeries는 UDP 포트 500을 통해 패킷의 VPN 상대에 패킷을 송신합니다. VPN 상대는 이미 UDP 포트 500을 통해 KIE 협의를 수행한 것을 기억하도록 하십시오. 같은 포트를 통해 UDP 캡슐화 통신을 송신하면, 두 VPN 상대가 방화벽을 통해 추가 포트를 열거나 연결을 통한 통신을 허용하기 위한 새 패킷 규칙을 작성하지 않아도 됩니다. 연결의 수신측은 UDP 페이로드의 처음 8바이트가 UDP 캡슐화 패킷에서 0으로 설정되므로, 패킷이 IKE 패킷인지 아니면 UDP 캡슐화 패킷인지 판별할 수 있습니다. 연결의 양측은 UDP 캡슐화가 적절하게 작동하도록 이를 지원해야 합니다.

IP 압축(IPComp)

IP 페이로드 압축 프로토콜(IPComp)은 상대방간의 통신 성능을 향상시키기 위해 데이터그램을 압축하여 IP 데이터그램 *크기*를 줄입니다. 압축을 하는 목적은 통신 속도가 너무 느리거나 정체된 *링크*가 있는 경우 전반적인 통신 성능을 향상시키기 위해서입니다. IPComp는 보안을 제공하지 않으며, VPN 연결을 통해 통신이 발생할 때 AH 또는 ESP 변환과 함께 사용해야 합니다.

IETF(Internet Engineering Task Force)는 IPComp를 RFC(Request for Comments) 2393, *IP 페이로드 압축 프로토콜(IPComp)*에서 공식적으로 정의하고 있습니다. 인터넷 웹 사이트 http://www.rfc-editor.org 에서 이 RFC를 볼 수 있습니다.

VPN 및 IP 필터링

대부분의 VPN 연결에서는 필터 규칙이 적절하게 작동되어야 합니다. 필요한 필터 규칙은 구성 중인 VPN 연결 유형과 제어할 통신 유형에 따라 다릅니다. 일반적으로, 각 연결에는 정책 필터가 수반됩니다. 정책 필터는

VPN을 사용할 수 있는 주소, 프로토콜, 포트를 정의합니다. 또한 인터넷 키 협약(IKE) 프로토콜을 지원하는 연결에는 보통 연결을 통한 IKE 처리를 허용하기 위해 명시적으로 작성된 규칙이 있습니다.

오퍼레이팅 시스템 V5R1을 사용하여 시작할 경우, VPN은 이러한 규칙을 자동으로 작성할 수 있습니다. 가능할 때마다, VPN이 정책 필터를 생성하도록 허용해야 합니다. 그러면 오류를 없앨 수 있으며 iSeries Navigator에서 패킷 규칙 편집기를 사용하여 별도의 단계로 규칙을 구성하지 않아도 됩니다.

물론 예외는 있습니다. 일반적이진 않지만 특정 상황에 적용할 수 있는 다른 VPN 및 필터링 개념 및 기술에 대해 배우려면 다음 주제를 검토하십시오.

- **현재 릴리스로 정책 필터 마이그레이트**
  오퍼레이팅 시스템의 V4R4 및 V4R5에서는 VPN 패킷 규칙을 별도의 단계로 구성해야 했습니다. VPN 구성의 일부로 자동으로 생성되지 않았습니다. 이 주제에서는 V4R4 및 V4R5 정책 필터를 현재 릴리스로 마이그레이트하는 작업에 대한 특수 고려사항에 대해 자세히 설명하고 이를 수행하는 방법을 알려줍니다.
- **정책 필터가 없는 VPN 연결**
  VPN의 연결 종료점이 단일의 특정 IP 주소이고 시스템에서 필터 규칙을 작성하거나 활성화하지 않고 VPN을 시작하려면, 동적 정책 필터를 구성하면 됩니다. 이 주제에서는 이를 고려할 수도 있는 이유에 대해 설명하고 이를 수행하는 방법에 대해 요약합니다.
- **내재적 IKE**
  VPN에 대해 IKE 협의가 발생하도록 하려면, 이 유형의 IP 통신에 대해 포트 500을 통한 UDP 데이터그램을 허용해야 합니다. 그러나 IKE 통신을 허용하기 위해 특별히 작성된 필터 규칙이 시스템에 없으면, 시스템은 내재적으로 IKE 통신 흐름을 허용합니다. iSeries에서 이를 작동하는 방법에 대한 자세한 정보는 이 주제를 읽으십시오.

현재 릴리스로 정책 필터 마이그레이트

오퍼레이팅 시스템의 V4R4 및 V4R5에서는 iSeries Navigator의 패킷 규칙 인터페이스에서 별도의 단계로 VPN 패킷 규칙을 구성해야 했습니다. VPN 구성의 일부로 자동으로 생성되지 않았습니다. 오퍼레이팅 시스템 V5R1을 사용하여 시작할 경우, VPN GUI는 이러한 패킷 규칙을 자동으로 작성할 수 있습니다.

V4R4 또는 V4R5에서 정책 필터 규칙(조치=IPSEC인 규칙)을 작성했고 동일한 해당 규칙을 현재 릴리스에서 사용하려는 경우, 고려해야 할 몇 가지 항목이 있습니다. 또는, VPN이 정책 필터 규칙을 생성할 것이지만 연결을 통해 다른 IP 통신(예: 텔넷)을 허용하는 규칙을 추가해야 합니다. 구성 오류가 발생하지 않도록 하려면 다음 권장사항을 따르십시오.

확인: 이 주제에서 *고객* 규칙 파일로 간주될 경우, 이는 사용자가 iSeries Navigator에서 패킷 규칙 편집기를 사용하여 작성한 규칙 파일을 말하는 것입니다. 이 파일을 VPN이 VPN 구성의 일부로 자동 생성하는 규칙 파일인 *VPNPOLICYFILTERS.I3P* 규칙 파일과 대조하십시오.

- V4R4 또는 V4R5에서 VPN 연결을 작성하고 현재 릴리스에서 다른 VPN 연결을 구성하지 않을 경우, 필터 규칙을 활성화하여 평소처럼 연결을 시작할 수 있습니다.

- 

  V4R4 또는 V4R5에서 VPN 연결을 작성하고 현재 릴리스에서 새 VPN 연결을 구성할 경우, **정책 필터 마이그레이트** 마법사를 사용해야 합니다. 이 마법사는 작성한 패킷 규칙 파일에서 정책 필터를 제거하고 동등한 정책 필터를 VPN이 생성한 VPNPOLICYFILTERS.I3P에 삽입합니다. 마법사를 액세스하려면 다음 단계를 따르십시오.

  1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책**을 확장하십시오.
  2. **VPN(가상 사설망)**을 마우스 오른쪽 버튼으로 클릭하고 **마이그레이트 정책 필터**를 선택하십시오.
  3. 마법사를 완료하면, **완료**를 클릭하십시오.
  4. 페이지나 필드 완료 방법에 대한 질문이 있으면 **도움말**을 클릭하십시오.

- VPN이 정책 필터 규칙을 생성했지만 VPN이 아닌 일부 필터 규칙을 추가해야 하는 경우, iSeries Navigator에서 패킷 규칙 편집기를 사용하여 규칙을 구성해야 합니다. VPN이 아닌 이러한 필터 규칙이 VPN 필터 앞에 와야 하는 경우, 세트명은 PREIPSEC로 시작해야 합니다(예: PREIPSECMYRULES). 그러면 시스템이 사용자의 필터 규칙을 처리해야 하는 순서를 쉽게 판별할 수 있습니다. 다른 모든 VPN이 아닌 규칙의 세트명에는 PREIPSEC 접두부가 없어야 합니다(예: MORERULES).
- 항상 VPN이 정책 필터 규칙을 작성할 수 있도록 허용해야 합니다. 그러나 VPN이 아닌 필터 규칙은 사용자 정의 파일에 남아 있어야 합니다. VPN이 아닌 필터가 VPNPOLICYFILTERS.I3P 규칙 파일에서 정책 필터 앞에 와야 하는 경우, 세트명 앞에 PREIPSEC를 추가해야 한다는 점을 기억하십시오. 이렇게 하면 사용자 규칙과 VPN이 의도한 대로 함께 작동하게 됩니다. 예를 들어, VPN이 정책 필터 규칙(VPN 세트)을 생성했으나 연결에서 다른 IP 통신을 허용하기 위해 추가 규칙(사용자 세트)을 추가했습니다. 시스템에서 규칙을 로드할 때, 규칙 순서는 다음과 같이 지정됩니다.

  1. 세트명이 PREIPSEC로 시작하는 사용자 세트
  2. 세트명이 PREIPSEC로 시작하는 VPN 세트
  3. ACTION=IPSEC(정책 필터)인 VPN 세트
  4. ACTION=IPSEC(정책 필터)인 사용자 세트
  5. 그 밖의 사용자 세트
  6. 그 밖의 VPN 세트

  병합된 출력 파일 순서를 보려면 EXPANDED.OUT 파일을 검사하십시오. EXPANDED.OUT는 사용자 규칙 파일이 위치한 디렉토리에 기록됩니다.

- 

  iSeries Navigator를 사용하여, 다음을 활성화할 것을 선택할 수 있습니다.

  – VPN에서만 생성한 규칙 파일인 VPNPOLICYFILTERS.I3P
  – 고객 규칙 파일만
  – VPN 생성 규칙과 고객 규칙 파일 모두

- 개별 인터페이스가 아닌 모든 인터페이스에 대해 이 필터 규칙을 활성화하십시오. 이렇게 하면 필터가 활성화되고 정책 필터 순서도 올바로 설정됩니다.
- 필터 규칙을 활성화하기 전에 항상 먼저 필터 규칙을 확인해야 합니다. 확인 작업이 오류 없이 실행되면, EXPANDED.OUT를 검사하여 규칙이 의도한 대로 순서화되어 있는지 검사해야 합니다. 이 단계를 완료한 후에 규칙을 활성화할 수 있습니다.

정책 필터가 없는 VPN 연결

정책 필터 규칙은 VPN을 사용할 수 있는 주소, 프로토콜, 포트를 정의하고 연결을 통해 해당되는 통신의 경로를 지정합니다. 어떤 경우에는 정책 필터 규칙이 필요하지 않은 연결을 구성할 수도 있습니다. 예를 들어, VPN 연결이 사용할 인터페이스에 로드된 비VPN 패킷 규칙을 가지고 있어서, 해당되는 인터페이스에서 활동 규칙을 비활성화하기 보다는 시스템이 연결에 대해 모든 필터를 동적으로 관리하도록 VPN을 구성할 수 있습니다. 이 유형의 연결에 대한 정책 필터를 **동적 정책 필터**라고 합니다. VPN 연결에 대해 동적 정책 필터를 사용하기 전에, 다음의 모든 사항이 만족되어야 합니다.

- 연결이 로컬 서버에 의해서만 초기화될 수 있습니다.
- 연결의 자료 종료점은 단일 시스템이어야 합니다. 즉, 서브네트나 주소 범위가 될 수 없습니다.
- 연결에 대해 로드할 수 있는 정책 필터 규칙이 없습니다.

연결이 이 기준에 만족될 경우, 정책 필터가 필요하지 않도록 연결을 구성할 수 있습니다. 연결이 시작되면, 시스템에 로드되는 다른 패킷 규칙에 관계없이 자료 종료점들 사이의 통신이 흐릅니다.

정책 필터가 필요하지 않은 연결을 구성하는 방법에 대한 단계별 지시사항에 대해서는 VPN에 대한 온라인 도움말을 참조하십시오.

내재적 IKE

연결을 설정하려면, 대부분의 VPN은 IPSec 처리가 이루어지기 전에 IKE(Internet Key Exchange) 협의를 요구합니다. IKE는 잘 알려진 포트 500을 사용하므로, IKE가 적절하게 작동하려면 이 유형의 IP 통신에 대해 포트 500을 통한 UDP 데이터그램을 허용해야 합니다. IKE 통신을 허용하기 위해 특별히 작성된 필터 규칙이 시스템에 없으면, 내재적으로 IKE 통신이 허용됩니다. 그러나 UDP 포트 500 통신량에 대해 특별히 작성된 규칙은 활동 필터 규칙에 정의된 것을 기초로 처리됩니다.

VPN 계획

계획은 전체 VPN 솔루션 중 필수적인 부분입니다. 연결이 적절히 작동하려면 많은 복잡한 결정을 내려야 합니다. VPN을 성공적으로 수행하는 데 필요한 모든 정보를 수집하려면 다음 자원을 사용하십시오.

- **VPN 설정 요구사항**
  시작하기 전에 먼저 VPN 작성을 위한 최소 요구사항을 충족하는지 확인하십시오.
- **작성할 VPN 유형 판별**
  VPN 사용 방법 판별은 성공적인 계획의 첫 번째 단계 중 하나입니다. 이 주제에서는 구성할 수 있는 다양한 연결 유형에 대해 설명합니다.
- **VPN 계획 어드바이저 사용**
  계획 어드바이저는 네트워크에 대한 질문을 제시하고 응답을 기초로 하여 VPN 작성에 대한 제안사항을 제공합니다.
  주: 인터넷 키 교환(IKE) 프로토콜을 지원하는 연결에 대해서만 VPN 계획 어드바이저를 사용하십시오. 수동 연결 유형에 대해서는 수동 연결용 계획 작업용지를 사용하십시오.
- **VPN 계획 작업용지 완료**
  계획 작업용지를 인쇄하고 완료하여 VPN 사용 계획에 대한 자세한 정보를 수집할 수 있습니다.

VPN 구현 계획을 완료한 후에는 VPN 구성을 시작할 수 있습니다.

VPN 설정 요구사항

iSeries와 네트워크 클라이언트에서 올바로 기능하려면 iSeries와 클라이언트 PC가 다음 요구사항을 만족하는지 확인하십시오.

V5R2 iSeries 요구사항

- OS/400, 버전 5 릴리스 2(5722-SS1) 이상
- 디지털 인증 관리자(5722-SS1 옵션 34)
- Cryptograhpic Access Provider(5722-AC2 또는 AC3)
- Windows용 iSeries Access(5722-XE1) 및 iSeries Navigator
  - iSeries Navigator의 네트워크 구성요소
- 서버 보안 자료 보유(QRETSVRSEC *SEC) 시스템 값을 1로 설정
- TCP/IP 구성(IP 인터페이스, 라우트, 로컬 호스트명 및 로컬 정의역명 포함)

클라이언트 요구사항

- iSeries에 올바로 연결되고 TCP/IP 구성이 된 Windows 32비트 오퍼레이팅 시스템이 있는 워크스테이션
- 233Mhz 처리 장치
- Windows 95/98 클라이언트용 32MB RAM
- Windows NT 및 2000 클라이언트용 64MB RAM
- 클라이언트 PC에 설치된 Windows용 iSeries Access 및 iSeries Navigator
- IP 보안(IPSec) 프로토콜을 지원하는 소프트웨어
- L2TP를 지원하는 소프트웨어(리모트 사용자가 L2TP를 사용하여 시스템과 연결을 설정할 경우)

작성할 VPN 유형 판별

VPN 사용 방법 판별은 성공적인 계획의 첫 번째 단계 중 하나입니다. VPN 사용 방법을 판별하려면 로컬 키 서버 및 리모트 키 서버 모두가 연결 시 수행하는 역할을 이해해야 합니다. 예를 들어, *연결* 종료점은 *자료* 종료점과 다릅니다. 두 가지가 서로 동일합니까 아니면, 두 가지의 조합입니까? 연결 종료점은 연결에 대한 자료 통신을 인증하고 암호화(또는 암호해독)하고, 키 관리에 인터넷 키 교환(IKE) 프로토콜을 선택적으로 제공합니다. 반면에, 자료 종료점은 VPN을 통해 흐르는 IP 통신에 대한 두 가지 시스템간 연결을 정의합니다(예: 123.4.5.6과 123.7.8.9간의 모든 TCP/IP 통신량). 보통, 연결 및 자료 종료점이 서로 다른 경우, VPN 서버는 일반적으로 게이트웨이입니다. 연결 및 자료 종료점이 동일한 경우, VPN 서버는 호스트입니다.

대부분의 회사 요구에 잘 맞는 다양한 VPN 구현 유형은 다음과 같습니다.

게이트웨이 대 게이트웨이
두 시스템간의 연결 종료점은 자료 종료점과 다릅니다. IP 보안(IPSec) 프로토콜은 게이트웨이 사이를 흐르는 통신량을 보호합니다. 그러나 IPSec는 내부 네트워크 내에 있는 게이트웨이 중 어느 한 쪽에서도 자료 통신량을 보호하지 않습니다. 이 유형은 지점 게이트웨이를 통해 내부 네트워크로 라우트되는 통신량이 종종 신뢰할 수 있다고 간주되기 때문에 지점간 연결에 대한 일반적인 설정입니다.

게이트웨이 대 호스트
IPSec는 게이트웨이와 리모트 네트워크의 호스트간에 흐르는 자료 통신량을 보호합니다. VPN은 신뢰할 수 있다고 간주하기 때문에 로컬 네트워크의 자료 통신량을 보호하지 않습니다.

호스트 대 게이트웨이
VPN은 로컬 네트워크의 호스트와 리모트 게이트웨이 사이로 흐르는 자료 통신량을 보호합니다. VPN은 리모트 네트워크의 자료 통신량을 보호하지 않습니다.

호스트 대 호스트
연결 종료점은 로컬 및 리모트 시스템 모두에 있는 자료 종료점과 동일합니다. VPN은 로컬 네트워크의 호스트와 리모트 네트워크의 호스트간에 흐르는 자료 통신량을 보호합니다. 이 VPN 유형은 단말 IPSec 보호를 제공합니다.

VPN 계획 작업용지 완료

VPN 계획 작업용지를 사용하여 VPN 사용 계획에 대한 자세한 정보를 수집하십시오. 이 정보는 VPN 전략을 적절히 계획하는 데 필요합니다. 또한 이 정보는 VPN을 구성하는 데 사용될 수 있습니다. 작성할 연결 유형에 대한 작업용지를 선택하십시오.

- **동적 연결용 계획 작업용지**
  동적 연결을 구성하기 전에 먼저 이 작업용지를 완료하십시오.

- **수동 연결용 계획 작업용지**
  수동 연결을 구성하기 전에 먼저 이 작업용지를 완료하십시오.
- **VPN 계획 어드바이저**
  또는 대화식 계획 및 구성 지침을 위해 필요한 경우에는 어드바이저를 사용하십시오. 계획 어드바이저는 네트워크에 대한 질문을 제시하고 응답을 기초로 하여 VPN 작성에 대한 제안사항을 제공합니다.
  주: 동적 연결에 대해서만 VPN 계획 어드바이저를 사용하십시오. 수동 연결 유형에 대해서는 수동 연결용 계획 작업용지를 사용하십시오.

유사한 등록 정보를 사용하여 복수 연결을 작성하는 경우, VPN 디폴트를 설정할 경우가 있습니다. 구성하는 디폴트 값은 VPN 등록 정보 용지에 제시되어 있습니다. 즉, 동일한 등록 정보를 여러 번 구성할 필요가 없습니다. VPN 디폴트 값을 설정하려면 VPN 기본 메뉴에서 **편집**을 선택한 후 **디폴트**를 선택하십시오.

동적 연결용 계획 작업용지

동적 VPN 연결을 작성하기 전에 먼저 이 작업용지를 완료하십시오. 이 작업용지에서는 신규 연결 마법사를 사용할 것이라고 가정합니다. 마법사를 사용하면 기본 보안 요구사항을 근거로 VPN을 설정할 수 있습니다. 일부 경우에는 마법사가 연결에 대해 구성하는 등록 정보를 세밀하게 해야 할 수도 있습니다. 예를 들어, 저널링이 필요하거나 TCP/IP를 시작할 때마다 VPN 서버를 시작하려 할 경우가 있습니다. 이 경우에는 마법사가 작성한 동적-키 그룹 또는 연결을 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.

VPN 설정을 계속하기 전에 다음 질문에 모두 응답해야 합니다.

필수 체크 리스트	응답
OS/400 V5R2(5722-SS1) 이상입니까?	
디지털 인증 관리자 옵션(5722-SS1 옵션 34)이 설치되어 있습니까?	
Cryptograhic Access Provider(5722-AC2 또는 AC3)가 설치되어 있습니까?	
iSeries Access(5722-XE1)가 설치되어 있습니까?	
iSeries Navigator가 설치되었습니까?	
iSeries Navigator의 네트워크 부속 구성요소가 설치되어 있습니까?	
OS/400용 TCP/IP Connectivity Utilities(5722-TC1)가 설치되어 있습니까?	
서버 보안 자료 보유(QRETSVRSEC *SEC) 시스템 값을 1로 설정했습니까?	
iSeries에 TCP/IP가 구성되어 있습니까(IP 인터페이스, 라우트, 로컬 호스트명, 로컬 정의역명 포함)?	
필수 종료점간에 정상 TCP/IP 통신이 설정되어 있습니까?	
최신 프로그램 임시 수정(PTF)을 적용했습니까?	
VPN 터널이 방화벽이나 IP 패킷 필터링을 구현하는 라우터를 오가는 경우, 방화벽이나 라우터 필터 규칙이 AH와 ESP 프로토콜을 지원합니까?	
방화벽이나 라우터가 IKE(UDP 포트 500), AH 및 ESP 프로토콜을 허용하도록 구성되어 있습니까?	
방화벽이 IP 이송이 가능하도록 구성되어 있습니까?	

이 정보는 동적 VPN 연결을 구성하는 데 필요합니다	응답

작성 중인 연결 유형은 무엇입니까? • 게이트웨이 대 게이트웨이 • 호스트 대 게이트웨이 • 게이트웨이 대 호스트 • 호스트 대 호스트	
동적-키 그룹명을 무엇이라 명명하겠습니까?	
키를 보호하는 데 필요한 보안 유형 및 시스템 성능 유형은 무엇입니까? • 최고 보안, 최저 성능 • 보안과 성능간 밸런스 유지 • 최저 보안, 최고 성능	
인증을 사용하여 연결을 인증하고 있습니까? 아니면, 사전공유 키는 무엇입니까?	
로컬 키 서버의 ID는 무엇입니까?	
로컬 자료 종료점의 ID는 무엇입니까?	
리모트 키 서버의 ID는 무엇입니까?	
리모트 자료 종료점의 ID는 무엇입니까?	
자료를 보호하는 데 필요한 보안 유형 및 시스템 성능 유형은 무엇입니까? • 최고 보안, 최저 성능 • 보안과 성능간 밸런스 유지 • 최저 보안, 최고 성능	

수동 연결용 계획 작업용지

키 관리를 위해 IKE를 사용하지 않는 VPN(가상 사설망)을 작성할 때 도움을 받으려면 이 작업용지를 완성하십시오.

VPN 설정을 계속하기 전에 다음 질문에 모두 응답해야 합니다.

필수 체크 리스트	응답
OS/400 V5R2(5722-SS1) 이상입니까?	
디지털 인증 관리자 옵션(5722-SS1 옵션 34)이 설치되어 있습니까?	
Cryptographic Access Provider(5722-AC2 또는 AC3)가 설치되어 있습니까?	
iSeries Access(5722-XE1)가 설치되어 있습니까?	
iSeries Navigator가 설치되었습니까?	
iSeries Navigator의 네트워크 부속 구성요소가 설치되어 있습니까?	
OS/400용 TCP/IP Connecitivity Utilities(5722-TC1)가 설치되어 있습니까?	
서버 보안 자료 보유(QRETSVRSEC *SEC) 시스템 값을 1로 설정했습니까?	
iSeries에 TCP/IP가 구성되어 있습니까(IP 인터페이스, 라우트, 로컬 호스트명, 로컬 정의역명 포함)?	
필수 종료점간에 TCP/IP 통신이 설정되어 있습니까?	
최신 프로그램 임시 수정(PTF)를 적용했습니까?	
VPN 터널이 방화벽이나 IP 패킷 필터링을 구현하는 라우터를 오가는 경우, 방화벽이나 라우터 필터 규칙이 AH와 ESP 프로토콜을 지원합니까?	

방화벽이나 라우터가 AH와 ESP 프로토콜을 허용하도록 구성되어 있습니까?	
방화벽이 IP 이송이 가능하도록 구성되어 있습니까?	

이 정보는 수동 VPN을 구성하는 데 필요합니다.	**응답**
작성 중인 연결 유형은 무엇입니까? • 호스트 대 호스트 • 호스트 대 게이트웨이 • 게이트웨이 대 호스트 • 게이트웨이 대 게이트웨이	
연결명을 무엇이라 명명하겠습니까?	
로컬 연결 종료점의 ID는 무엇입니까?	
리모트 연결 종료점의 ID는 무엇입니까?	
로컬 자료 종료점의 ID는 무엇입니까?	
리모트 자료 종료점의 ID는 무엇입니까?	
이 연결에 대해 허용하는 통신 유형은 무엇입니까(로컬 포트, 리모트 포트 및 프로토콜)?	
이 연결에 대한 주소 변환이 필요합니까? 자세한 내용은 VPN에 대한 네트워크 주소 변환을 참조하십시오.	
터널 모드를 사용합니까 아니면 전송 모드를 사용합니까?	
연결은 어떤 IPSec 프로토콜을 사용합니까(AH, ESP 또는 AH와 ESP를 함께 사용)? 자세한 내용은 IP 보안(IPSec)을 참조하십시오.	
연결은 어떤 인증 알고리즘을 사용합니까(HMAC-MD5 또는 HMAC-SHA)?	
연결은 어떤 암호화 알고리즘을 사용합니까(DES-CBC 또는 3DES-CBC)? **주:** ESP를 IPSec 프로토콜로 선택한 경우에만 암호화 알고리즘을 지정하십시오.	
AH 인바운드 키는 무엇입니까? MD5를 사용하는 경우, 키는 16바이트의 16진 스트링입니다. SHA를 사용하는 경우, 키는 20바이트의 16진 스트링입니다. 인바운드 키는 리모트 서버의 아웃바운드 키와 정확히 일치해야 합니다.	
AH 아웃바운드 키는 무엇입니까? MD5를 사용하는 경우, 키는 16바이트의 16진 스트링입니다. SHA를 사용하는 경우, 키는 20바이트의 16진 스트링입니다. 아웃바운드 키는 리모트 서버의 인바운드 키와 정확히 일치해야 합니다.	
ESP 인바운드 키는 무엇입니까? DES를 사용하는 경우, 키는 8바이트의 16진 스트링입니다. 3DES를 사용하는 경우, 키는 24바이트의 16진 스트링입니다. 인바운드 키는 리모트 서버의 아웃바운드 키와 정확히 일치해야 합니다.	
ESP 아웃바운드 키는 무엇입니까? DES를 사용하는 경우, 키는 8바이트의 16진 스트링입니다. 3DES를 사용하는 경우, 키는 24바이트의 16진 스트링입니다. 아웃바운드 키는 리모트 서버의 인바운드 키와 정확히 일치해야 합니다.	
인바운드 보안 정책 색인(SPI)는 무엇입니까? 인바운드 SPI는 4바이트의 16진 스트링인데, 여기서 첫 번째 바이트는 00으로 설정됩니다. 인바운드 SPI는 리모트 서버의 아웃바운드 SPI와 정확히 일치해야 합니다.	
아웃바운드 SPI는 무엇입니까? 아웃바운드 SPI는 4바이트의 16진 스트링입니다. 아웃바운드 SPI는 리모트 서버의 인바운드 SPI와 정확히 일치해야 합니다.	

VPN 구성

VPN 인터페이스는 VPN 연결을 구성하는 몇 가지 서로 다른 방법을 제공합니다. 구성할 연결 유형과 구성 방법을 결정하는 데 도움을 받으려면 다음 내용을 계속 읽으십시오.

구성해야 하는 연결 유형은 무엇입니까?

동적 연결은 연결이 활동 중인 동안 인터넷 키 교환(IKE) 프로토콜을 사용하여 연결을 보안하는 키를 동적으로 생성하고 협상하는 연결입니다. 동적 연결은 키가 정기적으로 자동 변경되기 때문에 흐르는 자료에 대한 보안 레벨을 추가로 제공합니다. 결과적으로, 공격자는 키를 캡쳐하여 키를 구분한 후 키를 사용하여 키가 보호하는 통신을 전환하거나 캡쳐할 가능성이 적습니다.

반면에, **수동(43 페이지 참조)** 연결은 IKE 협의에 대한 지원을 제공하지 않으므로 결국 자동 키 관리에 대한 지원을 제공하지 않습니다. 또한 양쪽 연결 끝에서 몇 가지 속성이 정확히 일치하도록 구성해야 합니다. 수동 연결은 연결이 활동 중인 동안 화면정리되거나 변경되지 않는 정적 키를 사용합니다. 연관된 키를 변경하려면 수동 연결을 중단해야 합니다. 이 중단이 보안상 위험을 초래할 것으로 간주되는 경우에는 동적 연결 작성을 대신 고려할 수 있습니다.

어떻게 동적 VPN 연결을 구성해야 합니까?

VPN은 실제로 연결 특성을 정의하는 구성 오브젝트 그룹입니다. 동적 VPN 연결이 올바르게 작동하려면 이러한 오브젝트가 있어야 합니다. VPN 구성 오브젝트 각각을 구성하는 방법에 대한 특정 정보를 보려면 아래 링크를 따라가십시오.

> **추가 정보:**
>
> **새로운 연결 마법사를 사용하여 연결 구성**
>
> 일반적으로, 모든 동적 연결을 작성하려면 연결 마법사를 사용해야 합니다. 마법사는 패킷 규칙을 포함하여 VPN이 올바로 작동하는 데 필요한 각각의 구성 오브젝트를 자동으로 작성합니다. 마법사가 VPN 패킷 규칙을 활성화하도록 지정한 경우, 아래 6단계 *연결 시작*을 건너뛸 수 있습니다. 그렇지 않은 경우에는 마법사가 VPN 구성을 완료한 후, 패킷 규칙을 활성화한 다음에 연결을 시작할 수 있습니다.

마법사를 사용하여 동적 VPN 연결을 구성하도록 선택하지 않은 경우, 다음 단계를 따라 구성을 완료하십시오.

1. **VPN 보안 정책 구성**

   모든 동적 연결에 대한 VPN 보안 정책을 정의해야 합니다. 인터넷 키 교환 정책 및 자료 정책은 IKE가 1단계 및 2단계 협의를 보호하는 방법을 규정합니다.

2. **보안 연결 구성**

   연결에 대한 보안 정책을 정의했으면, 보안 연결을 구성해야 합니다. 동적 연결의 경우, 보안 연결 오브젝트에는 동적-키 그룹과 동적-키 연결이 포함됩니다. **동적-키 그룹**이 하나 이상의 VPN 연결의 일반적인 특성을 정의하는 반면에, **동적-키 연결**은 종료점 쌍간의 개별 자료 연결 특성을 정의합니다. 동적-키 연결은 동적-키 그룹 내에 존재합니다.

주: VPN 인터페이스에서 **동적-키 그룹-연결** 페이지의 **정책 필터 규칙이 패킷 규칙에 정의됨** 옵션을 선택하면 다음 두 단계(*패킷 규칙 구성* 및 *규칙에 대한 인터페이스 정의*)만 완료하면 됩니다. 그렇지 않으면, VPN 구성의 일부로 이 규칙이 작성되어 지정하는 인터페이스에 적용됩니다.

VPN 인터페이스를 통해 항상 정책 필터 규칙이 작성되도록 하는 것이 좋습니다. **동적-키 그룹-연결** 페이지에서 **이 그룹에 다음 정책 필터 생성**을 선택하면 됩니다.

3. **패킷 규칙 구성**
   VPN 구성을 완료한 후에는 자료 통신이 연결을 통해 흐르도록 하는 필터 규칙을 작성하여 적용해야 합니다. VPN **사전 IPSec** 규칙은 IKE가 연결을 협상할 수있도록 지정된 인터페이스에 대한 모든 IKE 통신을 허용합니다. **정책 필터** 규칙은 연관된 신규 동적-키 그룹을 사용할 수 있는 주소, 프로토콜, 포트를 정의합니다.

   V4R4 또는 V4R5에서 마이그레이트 중이고 현재 릴리스에서 계속 사용할 VPN 연결 및 정책 필터를 가지고 있으면, 주제 *현재 릴리스로 정책 필터 마이그레이트*를 검토하여 이전 정책 필터와 새 정책 필터가 의도한 대로 작동되도록 해야 합니다.

4. **규칙에 대한 인터페이스 정의**
   패킷 규칙을 구성하고 기타 VPN 연결을 작동할 수 있게 하는 데 필요한 기타 규칙을 구성한 후에는 이를 적용할 인터페이스를 정의해야 합니다.

5. **패킷 규칙 활성화**
   패킷 규칙에 대한 인터페이스를 정의한 후에는 연결을 시작하기 전에 먼저 이 규칙을 활성화해야 합니다

6. **연결 시작**
   연결을 시작하려면 이 단계를 완료하십시오.

어떻게 수동 VPN 연결을 구성해야 합니까?

제목에서 알 수 있듯이, 수동 연결은 인바운드/인바운드 키를 포함하여 모든 VPN 등록 정보를 수동으로 구성해야 하는 연결입니다. 수동 연결 구성 방법에 대한 특정 정보를 보려면 아래 링크를 따라가십시오.

1. **수동 연결 구성**
   수동 연결은 보안 프로토콜과 연결 및 자료 종료점을 포함하여 연결 특성을 정의합니다.

   주: VPN 인터페이스에서 **수동 연결-연결** 페이지의 **정책 필터 규칙이 패킷 규칙에 정의됨** 옵션을 선택하면 다음 두 단계(*정책 필터 규칙 구성* 및 *규칙에 대한 인터페이스 정의*)만 완료하면 됩니다. 그렇지 않으면, VPN 구성의 일부로 이 규칙이 작성됩니다.

   VPN 인터페이스를 통해 항상 정책 필터 규칙이 작성되도록 하는 것이 좋습니다. **수동 연결 - 연결** 페이지에서 **자료 종료점과 일치하는 정책 필터 생성** 옵션을 선택하면 됩니다.

2. **정책 필터 규칙 구성**
   수동 연결 속성 구성을 완료한 후에는 자료 통신이 연결을 통해 흐르도록 하는 정책 필터 규칙을 작성하여 적용해야 합니다. **정책 필터** 규칙은 연관된 연결을 사용할 수 있는 주소, 프로토콜, 포트를 정의합니다.

3. **규칙에 대한 인터페이스 정의**
   패킷 규칙을 구성하고 기타 VPN 연결을 작동할 수 있게 하는 데 필요한 기타 규칙을 구성한 후에는 이를 적용할 인터페이스를 정의해야 합니다.

4. **패킷 규칙 활성화**
   패킷 규칙에 대한 인터페이스를 정의한 후에는 연결을 시작하기 전에 먼저 이 규칙을 활성화해야 합니다
5. **연결 시작**
   로컬로 시작된 연결을 시작하려면 이 타스크를 완료하십시오.

새 연결 마법사를 사용하여 VPN 연결 구성

새로운 연결 마법사를 사용하면 모든 호스트와 게이트웨이 조합 형태간에 VPN(가상 사설망)을 작성할 수 있습니다. 예를 들면, 호스트 대 호스트, 게이트웨이 대 호스트, 호스트 대 게이트웨이 또는 게이트웨이 대 게이트웨이

마법사는 패킷 규칙을 포함하여 VPN이 올바로 작동하는 데 필요한 각각의 구성 오브젝트를 자동으로 작성합니다. 그러나 VPN에 기능(예: 저널링 또는 VPN에 대한 네트워크 주소 변환(VPN NAT))을 추가해야 할 경우, 해당되는 동적-키 그룹 또는 연결의 등록 정보 용지를 통해 VPN을 세밀하게 구성하려 할 수 있습니다. 이를 수행하려면 먼저 활동 중인 연결을 중단해야 합니다. 그런 다음, 동적-키 그룹 또는 연결을 마우스 오른쪽 버튼으로 클릭한 후 **등록 정보**를 선택하십시오.

시작하기 전에 VPN 계획 어드바이저를 완료하십시오. 어드바이저는 VPN을 작성하는 데 필요한 중요한 정보를 모을 수 있는 수단을 제공합니다.

연결 마법사를 사용하여 VPN을 작성하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책**을 확장하십시오.
2. **가상 사설망**을 마우스 오른쪽 버튼으로 클릭하고 **신규연결**을 선택하여 마법사를 시작하십시오.
3. 마법사를 완료하여 기본 VPN 연결을 작성하십시오. 도움이 필요하면 **도움말**을 클릭하십시오.

VPN 보안 정책 구성

VPN 사용 방법을 판별한 후에는 VPN 보안 정책을 정의해야 합니다. 특히, 다음을 수행해야 합니다.

- **인터넷 키 교환(IKE) 정책 구성**
  IKE 정책은 1단계 협의 중에 IKE가 사용하는 인증 및 암호화 보호 레벨을 정의합니다. IKE 1단계는 후속 2단계 협의에서 흐르는 메세지를 보호하는 키를 설정합니다. 수동 연결을 작성할 경우, IKE 정책을 정의하지 않아도 됩니다. 또한 새로운 연결 마법사를 사용하여 VPN을 작성하는 경우에는 마법사가 IKE 정책을 작성할 수 있습니다.
- **자료 정책 구성**
  자료 정책은 VPN을 통해 흐르는 자료를 보호하는 인증 또는 암호화 레벨을 정의합니다. 통신 시스템은 인터넷 키 교환(IKE) 프로토콜 2단계 협의를 하는 동안 이 속성에 동의합니다. 수동 연결을 작성하는 경우에는 자료 정책을 정의하지 않아도 됩니다. 또한 신규 연결 마법사를 사용하여 VPN을 작성하는 경우에는 마법사가 자료 정책을 작성할 수 있습니다.

VPN 보안 정책을 구성한 후에는 보안 연결을 구성해야 합니다.

인터넷 키 교환(IKE) 정책 구성

IKE 정책은 IKE가 1단계 협의 중에 사용하는 인증 또는 암호화 보호 레벨을 정의합니다. IKE 1단계는 후속 2단계 협의에서 흐르는 메세지를 보호하는 키를 설정합니다. VPN은 RSA 서명 모드나 사전공유 키를 사용하여 1단계 협의를 인증합니다. 디지털 인증을 사용하여 키 서버를 인증하려는 경우, 디지털 인증 관리자(5722-SS1 옵션 34)를 사용하여 먼저 인증을 구성해야 합니다. IKE 정책은 이 정책을 사용할 리모트 키 서버도 식별합니다.

IKE 정책을 정의하거나 기존 정책을 변경하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책** —> **가상 사설망** —> **IP 보안 정책**을 확장하십시오.
2. 신규 정책을 작성하려면, **인터넷 키 교환 정책**을 마우스 오른쪽 버튼으로 클릭하고 **신규 인터넷 키 교환 정책**을 선택하십시오. 기존 정책을 변경하려면, 왼쪽 분할 창에서 **인터넷 키 교환 정책**을 클릭한 후 오른쪽 분할 창에서 변경할 정책을 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
3. 등록 정보 용지를 모두 완료하십시오. 페이지나 필드 완료 방법에 대한 질문이 있으면 **도움말**을 클릭하십시오.
4. **확인**을 클릭하여 변경사항을 저장하십시오.

자료 정책 구성

자료 정책은 VPN을 통해 흐르는 자료를 보호하는 인증 또는 암호화 레벨을 정의합니다. 통신 시스템은 IKE(Internet Key Exchange) 프로토콜 2단계 협의를 하는 동안 이 속성에 동의합니다.

자료 정책을 정의하거나 기존 자료 정책을 변경하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책** —> **가상 사설망** —> **IP 보안 정책**을 확장하십시오.
2. 신규 자료 정책을 작성하려면, **자료 정책**을 마우스 오른쪽 버튼으로 클릭하고 **신규 자료 정책**을 선택하십시오. 기존 자료 정책을 변경하려면, 왼쪽 분할 창에서 **자료 정책**을 클릭한 후 오른쪽 분할 창에서 변경할 자료 정책을 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
3. 등록 정보 용지를 모두 완료하십시오. 페이지나 필드 완료 방법에 대한 질문이 있으면 **도움말**을 클릭하십시오.
4. **확인**을 클릭하여 변경사항을 저장하십시오.

VPN 보안 연결 구성

연결에 대한 보안 정책을 구성했으면, 보안 연결을 구성해야 합니다. 동적 연결의 경우, 보안 연결 오브젝트에는 동적-키 그룹과 동적-키 연결이 포함됩니다.

동적-키 그룹은 하나 이상의 VPN 연결의 일반적인 특성을 정의합니다. 동적-키 그룹을 구성하면 그룹 내의 각 연결에 대해 동일한 정책과 서로 다른 자료 종료점을 사용할 수 있습니다. 또한 동적-키 그룹은 리모트 시스템이 제안한 자료 종료점이 미리 명확하게 알려지지 않을 때 리모트 개시자와 협상할 수 있게 합니다. 이는 동

적-키 그룹에 있는 정책 정보를 IPSEC 조치 유형의 정책 필터 규칙과 연관시켜 수행됩니다. 리모트 개시자가 제공한 특정 자료 종료점이 IPSEC 필터 규칙에 지정된 범위 내에 있는 경우에는 동적-키 그룹에 정의된 정책에 종속될 수 있습니다.

동적-키 연결은 종료점 쌍간의 개별 자료 연결 특성을 정의합니다. 동적-키 연결은 동적-키 그룹 내에 존재합니다. 그룹에 있는 연결이 어떤 정책을 사용할 것인지를 설명하기 위해 동적-키 그룹을 구성한 후에는 로컬로 시작하는 연결에 대한 개별 동적-키 연결을 작성해야 합니다.

보안 연결 오브젝트를 구성하려면, 다음 타스크를 완료하십시오.

파트 1: 동적-키 그룹 구성:

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책** —> **가상 사설망** —> **보안 연결**을 확장하십시오.
2. **그룹별**을 마우스 오른쪽 버튼으로 클릭하고 **신규 동적-키 그룹**을 선택하십시오.
3. 페이지나 필드 완료 방법에 대한 질문이 있으면 **도움말**을 클릭하십시오.
4. **확인**을 클릭하여 변경사항을 저장하십시오.

파트 2: 동적-키 연결 구성:

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책** —> **가상 사설망** —> **보안 연결** —> **그룹별**을 확장하십시오.
2. iSeries Navigator 창 왼쪽 분할 창에서 파트 1에서 작성한 동적-키 그룹을 마우스 오른쪽 버튼으로 클릭하고 **신규 동적-키 연결**을 선택하십시오.
3. 페이지나 필드 완료 방법에 대한 질문이 있으면 **도움말**을 클릭하십시오.
4. **확인**을 클릭하여 변경사항을 저장하십시오.

위 단계를 완료한 후에는 연결이 올바로 작동되는 데 필요한 패킷 규칙을 활성화해야 합니다.

주: 대부분의 경우, **동적-키 그룹-연결** 페이지에서 **이 그룹에 다음 정책 필터 생성** 옵션을 선택하여 VPN 인터페이스를 통해 VPN 패킷 규칙이 자동으로 생성되도록 해야 합니다. 그러나 **정책필터 규칙이 패킷 규칙에 정의됨** 옵션을 선택하면, 수동으로 VPN 패킷 규칙 구성을 수행한 후에 규칙을 활성화해야 합니다.

수동 연결 구성

제목에서 알 수 있듯이, 수동 연결은 모든 VPN 등록 정보를 직접 구성해야 하는 연결입니다. 또한 양쪽 연결 끝에서 여러 요소가 *정확히* 일치되도록 구성해야 합니다. 예를 들어, 인바운드 키는 리모트 시스템의 아웃바운드 키를 일치시켜야 합니다. 그렇지 않으면 연결에 실패합니다.

수동 연결은 연결이 사용 중인 동안 화면정리되거나 변경되지 않는 정적 키를 사용합니다. 연관된 키를 변경하려면 수동 연결을 중단해야 합니다. 이 중단이 보안상 위험을 초래할 것으로 간주되고, 연결 양 끝이 인터넷 키 교환(IKE) 프로토콜을 지원하는 경우에는 동적 연결 설정을 대신 고려할 수 있습니다.

등록 정보를 수동 연결에 대해 정의하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책** —> **가상사설망** —> **보안 연결**을 확장하십시오.
2. **모든 연결**을 마우스 오른쪽 버튼으로 클릭하고 **신규 수동 연결**을 선택하십시오.
3. 등록 정보 용지를 모두 완료하십시오. 페이지나 필드 완료 방법에 대한 질문이 있으면 **도움말**을 클릭하십시오.
4. **확인**을 클릭하여 변경사항을 저장하십시오.

주: 대부분의 경우, **수동 연결-연결** 페이지에서 **자료 종료점과 일치하는 정책 필터 생성** 옵션을 선택하여 VPN 인터페이스를 통해 VPN 패킷 규칙이 자동으로 생성되도록 해야 합니다. 그러나 **정책 필터 규칙이 패킷 규칙에 정의됨** 옵션을 선택하면, 수동으로 VPN 패킷 규칙 구성을 수행한 후에 규칙을 활성화해야 합니다.

VPN 패킷 규칙 구성

처음 연결을 작성하고 있는 경우, VPN이 자동으로 VPN 패킷 규칙을 생성하도록 해야 합니다. 새로운 연결 마법사를 사용하거나 VPN 등록 정보 페이지를 사용하여 연결을 구성하면 규칙이 자동 생성됩니다.

iSeries Navigator에서 패킷 규칙 편집기를 사용하여 VPN 패킷 규칙을 작성하려는 경우, 추가 규칙도 이와 같은 방법으로 작성해야 합니다. 반대로, VPN이 정책 필터 규칙을 생성하도록 한 경우, 모든 추가 정책 필터 규칙도 이런 방법으로 작성해야 합니다.

일반적으로, VPN은 두 가지 유형의 필터 규칙인 사전 IPSec 필터 규칙과 정책 필터 규칙을 요구합니다. iSeries Navigator에서 패킷 규칙 편집기를 사용하여 이러한 규칙을 구성하는 방법에 대해 배우려면 아래에 있는 주제를 검토하십시오. 다른 VPN 및 필터링 옵션에 대해 보려면, VPN 개념 주제에서 *VPN 및 IP 필터링* 섹션을 참조하십시오.

- **사전 IPSec 규칙**
  사전 IPSec 규칙은 IPSec 조치 유형을 사용하는 규칙 앞에 오는 시스템에 대한 규칙입니다. 이 주제에서는 VPN이 올바로 작동하는 데 필요한 사전 IPSec 규칙에 대해서만 설명합니다. 이 경우, 사전 IPSec 규칙은 연결을 통해 IKE 처리를 허용하는 규칙 쌍입니다. IKE는 연결이 발생하도록 동적 키 생성 및 협의를 허용합니다. 특정 네트워크 환경 및 보안 정책에 따라 다른 사전 IPSec 규칙을 추가해야 할 수도 있습니다.

  주: 특정 시스템에 대해 IKE를 허용하는 다른 규칙을 이미 가지고 있으면 이 유형의 사전 IPSec 규칙만 구성하면 됩니다. IKE 통신을 허용하기 위해 특별히 작성된 필터 규칙이 시스템에 없으면, 내재적으로 IKE 통신이 허용됩니다.
- **정책 필터 규칙**
  정책 필터 규칙은 VPN이 사용할 수 있는 통신을 정의하고 해당 통신에 적용할 자료 보호 정책을 정의합니다.

시작하기 전에 고려할 사항

인터페이스에 필터 규칙를 추가할 때, 시스템이 자동으로 해당 인터페이스에 대한 디폴트 DENY 규칙을 추가합니다. 이는 명시적으로 허용되지 않는 통신이 모두 거부됨을 의미합니다. 이 규칙을 보거나 변경할 수 없습니다. 따라서, 이전에는 신기하게 작동했던 통신이 VPN 필터 규칙을 활성화한 후에는 실패합니다. VPN이 아닌 다른 통신을 인터페이스에 허용하려면 명시적인 PERMIT 규칙을 추가해야 합니다.

해당 필터 규칙을 구성한 후에는 적용할 인터페이스 정의를 수행한 후 이를 활성화해야 합니다.

필터 규칙을 적절히 구성해야 합니다. 그렇지 않으면, 필터 규칙이 iSeries을 출입하는 모든 IP 통신을 차단할 수 있습니다. 여기에는 필터 규칙을 구성하는 데 사용하는 iSeries Navigator로의 연결이 포함됩니다.

필터 규칙이 iSeries Navigator 통신을 허용하지 않으면 iSeries Navigator는 iSeries와 통신할 수 없습니다. 이런 상황에 직면하면, 아직 연결이 되어 있는 인터페이스(예: Operations Console)를 사용하여 iSeries에 로그온해야 합니다. 이 시스템에서 모든 필터를 제거하려면 RMVTCPTBL 명령을 사용하십시오. 또한 이 명령은 *VPN 서버를 종료한 후 이를 재시작합니다. 그런 다음, 필터를 구성하고 이를 재활성화하십시오.

사전 IPSec 필터 규칙 구성

주의: VPN이 자동으로 정책 필터 규칙을 생성하지 않도록 지정한 경우에만 이 타스크를 완료해야 합니다.

인터넷 키 교환(IKE) 서버 한 쌍은 키를 동적으로 대화하고 화면정리합니다. IKE는 잘 알려진 포트 500을 사용합니다. IKE가 올바로 작동하도록 포트 500을 통해 이 IP 통신에 대한 UDP 데이터그램을 허용해야 합니다. 이를 위해 한 쌍의 필터 규칙을 작성하게 되는데, 하나는 인바운드 통신량용이고, 다른 하나는 아웃바운드 통신량용입니다. 따라서, 연결은 동적으로 키를 협상하여 연결을 보호할 수 있습니다.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책**을 확장하십시오.
2. **패킷 규칙**을 마우스 오른쪽 버튼으로 클릭하고 **편집기 규칙**을 선택하십시오. 그러면 iSeries에 대한 필터 및 NAT 규칙을 작성하거나 편집할 수 있는 패킷 규칙 편집기가 열립니다.
3. 환영 대화 상자에서, **새 패킷 규칙 파일 작성**을 선택하고 **확인**을 클릭하십시오.
4. 패킷 규칙 편집기에서 **삽입** —> **필터**를 선택하십시오.
5. **일반** 페이지에서 VPN 필터 규칙에 대한 세트명을 지정하십시오. 서로 다른 세트를 최소한 세 개 작성하는 것이 좋습니다. 하나는 사전 IPSec 필터 규칙용, 또 하나는 사용자 정책 필터 규칙용, 나머지 하나는 기타 PERMIT 및 DENYfilter 규칙용입니다. 사전 IPSec 필터 규칙이 들어 있는 세트에는 *preipsec* 접두부가 있습니다(예: preipsecfilters).
6. **조치** 필드의 드롭 다운 리스트에서 **PERMIT**를 선택하십시오.
7. **방향** 필드의 드롭 다운 리스트에서 **OUTBOUND**를 선택하십시오.
8. **소스 주소명** 필드의 첫 번째 드롭 다운 리스트에서 =를 선택한 후, 두 번째 필드에 로컬 키 서버의 IP 주소를 입력하십시오. IKE 정책에서 로컬 키 서버의 IP 주소를 지정했습니다.
9. **목적지 주소명** 필드의 첫 번째 드롭 다운 리스트에서 =를 선택한 후, 두 번째 필드에 리모트 키 서버의 IP 주소를 입력하십시오. IKE 정책에서 리모트 키 서버의 IP 주소도 지정했습니다.
10. **서비스** 페이지에서 **서비스**를 선택하십시오. 그러면 **프로토콜**, **소스 포트** 및 **목적지 포트** 필드를 작동할 수 있습니다.
11. **프로토콜** 필드의 드롭 다운 리스트에서 **UDP**를 선택하십시오.
12. **소스 포트**의 경우, 첫 번째 필드에서 =를 선택한 후, 두 번째 필드에 500을 입력하십시오.
13. **목적지 포트**에 대해서도 이전 단계를 반복하십시오.
14. **확인**을 클릭하십시오

15. 위 단계를 반복하여 INBOUND 필터를 구성하십시오. 동일한 세트명을 사용하고 필요하면 주소를 반대로 사용하십시오.

주: 보안면에서는 못하지만 연결을 통해 IKE 통신을 허용하는 편리한 옵션은 사전 IPSec 필터를 하나만 구성하고 **방향**, **소스 주소명** 및 **목적지 주소명** 필드에 와일드카드 값(*)을 사용하는 것입니다.

다음 단계는 정책 필터 규칙 구성을 수행하여 VPN 연결이 보호하는 IP 통신량을 정의하는 것입니다.

정책 필터 규칙 구성

주의: VPN이 자동으로 정책 필터 규칙을 생성하지 않도록 지정한 경우에만 이 타스크를 완료해야 합니다.

정책 필터 규칙(조치가 IPSEC인 규칙)은 VPN을 사용할 수 있는 주소, 프로토콜, 포트를 정의합니다. VPN 연결시 통신에 적용될 정책도 정의합니다. 정책 필터 규칙을 구성하려면 다음 단계를 따르십시오.

주: 사전 IPSec 규칙(동적 연결의 경우에만)을 방금 구성한 경우, 패킷 규칙 편집기가 아직 열려 있어야 합니다. 4단계로 찾아 가십시오.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책**을 확장하십시오.
2. **패킷 규칙**을 마우스 오른쪽 버튼으로 클릭하고 **편집기 규칙**을 선택하십시오. 그러면 iSeries에 대한 필터 및 NAT 규칙을 작성하거나 편집할 수 있는 패킷 규칙 편집기가 열립니다.
3. 환영 대화 상자에서, **새 패킷 규칙 파일 작성**을 선택하고 **확인**을 클릭하십시오.
4. 패킷 규칙 편집기에서 **삽입** —> **필터**를 선택하십시오.
5. **일반** 페이지에서 VPN 필터 규칙에 대한 세트명을 지정하십시오. 서로 다른 세트를 최소한 세 개 작성하는 것이 좋습니다. 하나는 사전 IPSec 필터 규칙용, 또 하나는 사용자 정책 필터 규칙용, 나머지 하나는 기타 PERMIT 및 DENYfilter 규칙용입니다. 예를 들면, `policyfilters`입니다.
6. **조치** 필드의 드롭 다운 리스트에서 **IPSEC**를 선택하십시오. **방향** 필드의 디폴트 값은 OUTBOUND이며, 이를 변경할 수는 없습니다. 이 필드의 디폴트 값이 OUTBOUND이지만 실제로는 양방향입니다. OUTBOUND가 입력 값의 의미를 명확히 하기 위해 표시됩니다. 예를 들면, 소스 값은 로컬 값이고 목적지 값은 리모트 값입니다.
7. **소스 주소명**의 경우, 첫 번째 필드에서 =를 선택한 후, 두 번째 필드에 로컬 자료 종료점의 IP 주소를 입력하십시오. **주소 정의** 기능을 사용하여 주소를 정의한 후 IP 주소 범위 또는 서브네트 마스크가 있는 IP 주소 범위를 지정할 수도 있습니다.
8. **목적지 주소명**의 경우, 첫 번째 필드에서 =를 선택한 후, 두 번째 필드에 리모트 자료 종료점의 IP 주소를 입력하십시오. **주소 정의** 기능을 사용하여 주소를 정의한 후 IP 주소 범위 또는 서브네트 마스크가 있는 IP 주소 범위를 지정할 수도 있습니다.
9. **저널링** 필드에서 필요한 저널링 레벨을 지정하십시오.
10. **연결명** 필드에서 이 필터 규칙을 적용할 연결 정의를 선택하십시오.
11. (선택적) 설명을 입력하십시오
12. **서비스** 페이지에서 **서비스**를 선택하십시오. 그러면 **프로토콜**, **소스 포트** 및 **목적지 포트** 필드를 작동할 수 있습니다.

13. **프로토콜** 필드, **소스 포트** 및 **목적지 포트** 필드에서 적절한 통신량 값을 선택하십시오. 그렇지 않으면, 드롭 다운 리스트에서 별표(*)를 선택할 수 있습니다. 그러면 모든 포트를 사용하는 모든 프로토콜에서 VPN을 사용할 수 있습니다.
14. **확인**을 클릭하십시오.

다음 단계는 이 필터 규칙을 적용할 인터페이스 정의를 하는 단계입니다.

주: 인터페이스에 필터 규칙를 추가할 때, 시스템이 자동으로 해당 인터페이스에 대한 DENY 규칙을 추가합니다. 이는 명시적으로 허용되지 않은 통신이 모두 거부됨을 의미합니다. 이 규칙을 보거나 변경할 수 없습니다. 따라서, 이전에는 신기하게 작동했던 연결이 VPN 패킷 규칙을 활성화한 후에는 실패합니다. VPN이 아닌 다른 통신을 인터페이스에 허용하려면 명시적인 PERMIT 규칙을 추가해야 합니다.

VPN 필터 규칙에 대한 인터페이스 정의

VPN 패킷 규칙을 구성하고 기타 VPN 연결을 작동할 수 있게 하는 데 필요한 기타 규칙을 구성한 후에는 이를 적용할 인터페이스를 정의해야 합니다.

VPN 필터 규칙을 적용할 인터페이스를 정의하려면 다음 단계를 따르십시오.

주: VPN 패킷 규칙을 방금 구성한 경우, 패킷 규칙 인터페이스가 아직 열려 있어야 합니다. 4단계로 가십시오.

1. iSeries Navigator에서, 서버 **—> 네트워크 —> IP 정책**을 확장하십시오.
2. **패킷 규칙**을 마우스 오른쪽 버튼으로 클릭하고 **편집기 규칙**을 선택하십시오. 그러면 iSeries에 대한 필터 및 NAT 규칙을 작성하거나 편집할 수 있는 패킷 규칙 편집기가 열립니다.
3. 환영 대화 상자에서, **새 패킷 규칙 파일 작성**을 선택하고 **확인**을 클릭하십시오.
4. 패킷 규칙 편집기에서 **삽입 —> 인터페이스 필터**를 선택하십시오.
5. **일반** 페이지에서 **회선명**을 선택한 후, 드롭 다운 리스트에서 VPN 패킷 규칙을 적용할 회선 설명을 선택하십시오.
6. (선택적) 설명을 입력하십시오
7. **필터 세트** 페이지에서 **추가**를 클릭하여 방금 구성한 각 필터에 세트명을 추가하십시오.
8. **확인**을 클릭하십시오.
9. 규칙 파일을 저장하십시오. 파일은 .i3p 확장자를 사용하여 iSeries의 통합 파일 시스템에 저장됩니다.
   주: 파일을 다음 디렉토리에 저장하지 마십시오.

   ```
   /QIBM/UserData/OS400/TCPIP/RULEGEN
   ```

   이 디렉토리는 시스템 전용입니다. RMVTCPTBL *ALL 명령으로 패킷 규칙을 비활성화해야 하는 경우, 이 명령은 이 디렉토리에 있는 모든 파일을 삭제합니다.

필터 규칙에 대한 인터페이스를 정의한 후에는 VPN을 시작하기 전에 먼저 이 규칙을 활성화해야 합니다

VPN 패킷 규칙 활성화

VPN 연결을 사용하기 전에 먼저 VPN 패킷 규칙을 활성화해야 합니다. VPN 연결이 시스템에서 실행되고 있을 때는 패킷 규칙을 활성화(또는 비활성화)할 수 없습니다. 그러므로, VPN 필터 규칙을 활성화하기 전에 먼저 규칙과 연관된 활동 연결이 없음을 확인해야 합니다.

새 연결 마법사와의 VPN 연결을 작성한 경우, 연관된 규칙이 자동으로 활성화되도록 할 것을 선택할 수 있습니다. 사용자가 지정하는 인터페이스 중 어느 하나에 활동 중인 패킷 규칙이 있는 경우, VPN 정책 필터 규칙이 이를 대체합니다.

패킷 규칙 편집기를 사용하여 VPN이 생성한 규칙을 활성화할 것을 선택할 경우, 다음 단계를 수행하십시오.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책**을 확장하십시오.
2. **패킷 규칙**을 마우스 오른쪽 버튼으로 클릭하고 **활성화**를 선택하십시오. 그러면 패킷 규칙 활성화 대화 상자가 열립니다.
3. VPN 생성 규칙만, 선택한 파일만, 또는 VPN 생성 규칙과 선택된 파일 모두를 활성화할 것인지 선택하십시오. 나중에(예를 들어, VPN 생성 규칙 외에도 인터페이스에 대해 시행하려고 하는 기타 PERMIT 및 DENY 규칙이 있는 경우) 선택할 수도 있습니다.
4. 규칙을 활성화할 인터페이스를 선택하십시오. 특정 인터페이스, 지점 간 ID, 또는 모든 인터페이스와 모든 지점 간 ID에 대해 활성화할 것을 선택할 수 있습니다.
5. 대화상자에서 **확인**을 클릭하여 지정한 인터페이스에 대해 규칙을 확인하고 활성화를 확인하십시오. 확인을 클릭하고 나면, 시스템은 구문 및 시멘틱 오류에 대해 규칙을 검사하고 편집기의 맨 아래에 있는 메세지 창에 결과를 보고합니다. 특정 파일 및 행 번호와 연관되는 오류 메세지에 대해, 오류를 마우스 오른쪽 버튼으로 클릭하고 **행 찾아 가기**를 선택하여 파일에서 오류를 강조표시할 수 있습니다.

필터 규칙을 활성화한 후에 VPN 연결 시작을 할 수 있습니다.

VPN 연결 시작

다음 지침에서는 VPN 연결이 올바로 구성되었다고 가정합니다. VPN 연결을 시작하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책**을 확장하십시오.
2. VPN 서버가 시작되지 않는 경우, **가상 사설망**을 마우스 오른쪽 버튼으로 클릭하고 **시작**을 선택하십시오. 그러면 VPN 서버가 시작됩니다.
3. 패킷 규칙이 활성화되었는지 확인하십시오.
4. **가상 사설망** —> **보안 연결**을 확장하십시오.
5. **모든 연결**을 클릭하여 오른쪽 분할 창에 연결 리스트를 표시하십시오.

6. 시작할 연결을 마우스 오른쪽 버튼으로 클릭하고 **시작**을 선택하십시오. 복수 연결을 시작하려면, 시작할 각 연결을 선택하고 마우스 오른쪽 버튼으로 클릭한 후 **시작**을 선택하십시오.

VPN 관리

iSeries Navigator의 VPN 인터페이스를 사용하여 다음과 같은 모든 관리 타스크를 처리하십시오.

- **VPN 연결 시작**
  로컬로 개시할 연결을 시작하려면 이 타스크를 완료하십시오.
- **연결에 대한 디폴트 속성 설정**
  디폴트 값은 신규 정책과 연결을 작성하는 데 사용하는 패널을 제공합니다. 보안 레벨, 키 세션 관리, 키 수명 및 연결 수명에 대한 디폴트 값을 설정할 수 있습니다.
- **오류 상태의 연결 재설정**
  오류 상태의 연결을 재설정을 하면 유휴 상태로 리턴됩니다.
- **오류 정보 보기**
  연결이 오류 상태인 이유를 판별하려면 이 타스크를 완료하십시오.
- **활동 연결 속성 보기**
  활동 연결 상태 및 기타 속성을 검사하려면 이 타스크를 완료하십시오.
- **VPN 서버 추적 사용**
  VPN 추적을 사용하여 VPN 연결 관리자와 VPN 키 관리자 서버 추적을 구성, 시작, 중단 및 볼 수 있습니다. 이것은 연결이 활동 중인 동안 추적을 볼 수 있다는 점을 제외하고 녹색 화면에서 TRCTCPAPP *VPN 명령을 사용하는 것과 유사합니다.
- **VPN 서버 작업 기록부 보기**
  VPN 키 관리자와 VPN 연결 관리자에 대한 작업 기록부를 보려면 다음 지침을 따르십시오.
- **연결 중단**
  활동 연결을 중단하려면 이 타스크를 완료하십시오.
- **보안 협약(SA) 속성 보기**
  작동할 수 있는 연결과 연관된 보안 협약(SA) 속성을 표시하려면 이 타스크를 완료하십시오.
- **VPN 구성 오브젝트 삭제**
  VPN 정책 데이터베이스에서 VPN 구성 오브젝트를 삭제하기 전에 먼저 연결이 다른 VPN 연결 및 연결 그룹에 어떠한 영향을 미치는지를 확실히 이해하십시오.

연결에 대한 디폴트 속성 설정

디폴트 보안 값은 신규 VPN 오브젝트를 처음에 작성할 때 여러 필드를 제공합니다.

VPN 연결에 디폴트 보안 값을 설정하려면, 다음 단계를 따르십시오.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책**을 확장하십시오.
2. **가상 사설망**을 마우스 오른쪽 버튼으로 클릭하고 **디폴트**를 선택하십시오.
3. 페이지나 필드 완료 방법에 대한 질문이 있으면 **도움말**을 클릭하십시오.

4. 등록 정보 용지를 모두 완료한 후 **확인**을 클릭하십시오.

오류 상태의 연결 재설정

오류 상태의 연결을 화면정리하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책** —> **가상 사설망** —> **보안 연결**을 확장하십시오.
2. **모든 연결**을 클릭하여 오른쪽 분할 창에 연결 리스트를 표시하십시오.
3. 재설정할 연결을 마우스 오른쪽 버튼으로 클릭하고 **재설정**를 선택하십시오. 연결이 유휴 상태로 재설정됩니다. 오류 상태의 복수 연결을 재설정하려면 재설정할 각 연결을 선택하고 마우스 오른쪽 버튼으로 클릭한 후 **재설정**을 선택하십시오.

오류 정보 보기

연결 오류 정보를 보려면, 다음 단계를 따르십시오.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책** —> **가상 사설망** —> **보안 연결**을 확장하십시오.
2. **모든 연결**을 클릭하여 오른쪽 분할 창에 연결 리스트를 표시하십시오.
3. 보려는 오류 연결을 마우스 오른쪽 버튼으로 클릭하고 **오류 정보**를 선택하십시오.

활동 연결 속성 보기

활동 또는 요청시 연결의 현재 속성을 보려면 다음 단계를 따르십시오.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책** —> **가상 사설망** —> **보안 연결**을 확장하십시오.
2. **모든 연결**을 클릭하여 오른쪽 분할 창에 연결 리스트를 표시하십시오.
3. 보려는 활동 또는 요청시 연결을 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
4. **현재 속성** 페이지로 찾아 가서 연결 속성을 보십시오.

iSeries Navigator 창에서 모든 연결 속성을 볼 수도 있습니다. 디폴트 값으로 상태, 설명 및 연결 유형 속성만 표시됩니다. 다음 단계를 따라 자료 표시 화면을 변경할 수 있습니다.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책** —> **가상 사설망** —> **보안 연결**을 확장하십시오.
2. **모든 연결**을 클릭하여 오른쪽 분할 창에 연결 리스트를 표시하십시오.
3. **오브젝트** 메뉴에서 **열**을 선택하십시오. iSeries Navigator 창에 표시할 속성을 선택할 수 있는 대화상자가 열립니다.

보려는 열을 변경할 때 변경사항이 특정 사용자나 PC에 국한되지 않고 시스템 전반에 적용된다는 점을 알아두십시오.

VPN 서버 추적 사용

VPN 서버 추적을 보려면 다음 단계를 따르십시오.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책**을 확장하십시오.
2. **가상사설망**을 마우스 오른쪽 버튼으로 클릭하고, **진단 툴**을 선택한 후 **서버 추적**을 선택하십시오.

VPN 키 관리자와 VPN 연결 관리자가 생성할 추적 유형을 지정하려면 다음 단계를 따르십시오.

1. **가상 사설망 추적** 창에서,  (옵션)을 클릭하십시오.
2. **연결 관리자** 페이지에서 연결 관리자 서버가 실행할 추적 유형을 지정하십시오.
3. **키 관리자 페이지**에서 키 관리자 서버가 실행할 추적 유형을 지정하십시오.
4. 페이지나 필드 완료 방법에 대한 질문이 있으면 **도움말**을 클릭하십시오.
5. **확인**을 클릭하여 변경사항을 저장하십시오.
6. 추적을 시작하려면  (시작)을 클릭하십시오. 정기적으로 최신 추적 정보를 보려면  (화면정리)를 클릭하십시오.

VPN 서버 작업 기록부 보기

VPN 키 관리자나 VPN 연결 관리자의 현재 작업 기록부를 보려면 다음 단계를 따르십시오.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책**을 확장하십시오.
2. **가상 사설망**을 마우스 오른쪽 버튼으로 클릭하고 **진단 툴**을 선택한 후 보려는 서버 작업 기록부를 선택하십시오.

보안 협약(SA) 속성 보기

작동할 수 있는 연결과 연관된 보안 협약(SA) 속성을 보십시오. 속성을 보려면 다음 단계를 따르십시오.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책** —> **가상 사설망** —> **보안 연결**을 확장하십시오.
2. **모든 연결**을 클릭하여 오른쪽 분할 창에 연결 리스트를 표시하십시오.
3. 해당 활동 연결을 마우스 오른쪽 버튼으로 클릭하고 **보안 협약**을 선택하십시오. 결과 창에서 특정 연결과 연관된 각 SA 등록 정보를 볼 수 있습니다.

VPN 연결 중단

활동 또는 요청시 연결을 중단하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책** —> **가상 사설망** —> **보안 연결**을 확장하십시오.
2. **모든 연결**을 클릭하여 오른쪽 분할 창에 연결 리스트를 표시하십시오.
3. 중단할 연결을 마우스 오른쪽 버튼으로 클릭하고 **중단**을 선택하십시오. 복수 연결을 중단하려면, 중단할 각 연결을 선택하고 마우스 오른쪽 버튼으로 클릭한 후 **중단**을 선택하십시오.

VPN 구성 오브젝트 삭제

VPN 정책 데이터베이스에서 VPN 연결을 삭제해야 하는 경우에는 다음 단계를 수행하십시오.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책** —> **가상 사설망** —> **보안 연결**을 확장하십시오.
2. **모든 연결**을 클릭하여 오른쪽 분할 창에 연결 리스트를 표시하십시오.
3. 삭제할 연결을 마우스 오른쪽 버튼으로 클릭하고 **삭제**를 선택하십시오.

VPN 문제점

VPN은 최소한 표준 IPSec 기술에 대한 기본 지식을 필요로 하는 복잡하면서도 급속히 변경되는 기술입니다. VPN이 올바로 작동하려면 몇 가지 필터 규칙이 필요하기 때문에 IP 패킷 규칙도 잘 알고 있어야 합니다. 이 복잡성 때문에, VPN 연결 문제점을 수시로 겪을 수 있습니다. VPN 문제해결이 항상 쉬운 타스크는 아닙니다. 시스템 및 네트워크 환경 뿐만 아니라, 이를 관리하는 데 사용하는 구성요소도 이해해야 합니다. 다음 주제에서는 VPN을 사용하는 동안 발생할 수 있는 다양한 문제점을 해결하는 방법에 대한 힌트를 제공합니다.

- **VPN 문제 해결 시작하기**
  VPN 연결 문제점을 찾아 정정하려면 여기로 가십시오.
- **일반적인 VPN 구성 오류 및 오류 수정 방법**
  이 주제에서는 가장 일반적인 사용자 오류를 식별하고 가능한 해결책을 제시합니다.
- **QIPFILTER 저널을 사용하여 VPN 문제 해결**
  이 주제에서는 VPN 필터 규칙에 대한 정보를 제공합니다.
- **QVPN을 사용하여 VPN 문제 해결**
  이 주제에서는 IP 통신 및 연결 정보를 제공합니다.
- **VPN 작업 기록부를 사용하여 VPN 문제 해결**
  이 주제에서는 VPN이 사용하는 다양한 작업 기록부를 설명합니다.
- **OS/400 통신 추적을 사용하여 VPN 문제 해결**
  이 주제에서는 통신 회선에 관한 자료를 추적하는 방법을 설명합니다.

VPN 문제 해결 시작하기

VPN 문제점 분석을 시작하는 방법에는 몇 가지가 있습니다.

1. 항상 최신 프로그램 임시 수정(PTF)을 적용했는지 확인하십시오.
2. 최소 VPN 설정 요구사항을 충족하는지 확인하십시오.
3. 로컬 및 리모트 시스템 모두에 대해 오류 정보 창이나 VPN 서버 작업 기록부에 있는 오류 메세지를 검토하십시오. 실제로, VPN 연결 문제점을 해결할 때 연결 양 끝 모두를 살펴봐야 합니다. 또한 검사해야 할 네 개의 주소가 있다는 점도 고려해야 합니다. IPSec가 IP 패킷에 적용된 주소인 로컬 및 리모트 연결 종료점, IP 패킷의 소스이면서 목적지인 로컬 및 리모트 자료 종료점을 검사해야 합니다.
4. 오류 메세지에서 문제점 해결을 위한 충분한 정보를 찾을 수 없는 경우에는 IP 필터 저널을 검사하십시오.

5. iSeries에서 통신 추적은 로컬 시스템이 연결 요구를 수신하는지 송신하는지 여부에 대한 일반 정보를 찾을 수 있는 또 다른 위치를 제공합니다.
6. TRCTCPAPP(TCP 어플리케이션 추적) 명령은 문제점을 해결할 수 있는 또 다른 방법을 제공합니다. 일반적으로, IBM 서비스는 TRCTCPAPP를 사용하여 연결 문제점을 분석하기 위한 추적 출력을 확보합니다.

기타 검사할 사항

연결을 설정한 후 오류가 발생할 경우, 네트워크에서 오류가 발생한 위치를 확실히 알 수 없으면 환경의 복잡성을 줄여 보십시오. 예를 들어, 한 번에 모든 VPN 연결 부분을 조사하는 대신에 IP 연결 자체부터 조사를 시작하십시오. 다음 리스트에서는 가장 간단한 IP 연결부터 보다 복잡한 VPN 연결에 이르기까지 VPN 문제점 분석을 시작하는 방법에 대한 기본 지침을 제공합니다.

1. 로컬 및 리모트 호스트간 IP 구성으로 시작하십시오. 로컬 및 리모트 시스템 모두가 통신에 사용하는 인터페이스의 IP 필터를 제거하십시오. 로컬에서 리모트 호스트로 PING을 수행할 수 있습니까?

   주: PING 명령에서 프롬트하십시오. 리모트 시스템 주소를 입력하고 추가 매개변수로 PF10을 사용한 후, 로컬 인터넷 주소를 입력하십시오. 실제 또는 논리 인터페이스가 여러 개인 경우, 이것은 특히 중요합니다. 이렇게 하면 올바른 주소가 PING 패킷에 위치됩니다.

   응답이 **예**인 경우에는 2단계로 진행하십시오. 응답이 **아니오**인 경우에는 IP 구성, 인터페이스 상태 및 라우팅 항목을 검사하십시오. 구성이 올바른 경우, 통신 추적 기능을 사용하여 PING 요구가 송신되는지 등을 검사하십시오. PING 요구를 송신하지만 아무런 응답도 수신되지 않는 경우, 네트워크 또는 리모트 시스템에 문제가 있을 가능성이 높습니다.

   주: IP 패킷 필터링을 수행하는 중간 라우터나 방화벽이 있어 PING 패킷을 필터링할 수 있습니다. PING은 일반적으로 ICMP 프로토콜을 기반으로 합니다. PING이 성공하면, 연결되었다는 것을 알 수 있습니다. PING이 실패하면, PING이 실패했다는 사실만 알게 됩니다. 두 시스템간에 Telnet이나 FTP같은 다른 IP 프로토콜을 사용하여 연결성을 확인할 수 있습니다.
2. VPN 필터 규칙을 검사하여 활성화되었는지 확인하십시오. 필터링이 시작됩니까? 응답이 **예**인 경우, 3단계로 진행하십시오. 응답이 **아니오**인 경우에는 iSeries Navigator의 IP 패킷 규칙 창에서 오류 메세지를 검사하십시오. 필터 규칙이 임의의 VPN 통신에 대한 네트워크 주소 변환(NAT)을 지정하지 않는지 확인하십시오.
3. VPN 연결 시작을 하십시오. 연결이 시작됩니까? 응답이 **예**인 경우에는 4단계로 진행하십시오. 응답이 **아니오**이면 QTOVMAN 작업 기록부, QTOKVPNIKE 작업 기록부를 검사하여 오류가 있는지 확인하십시오.

   VPN을 사용할 때, 네트워크에 있는 ISP(인터넷 서비스 제공자) 및 모든 보안 게이트웨이 인증 헤더(AH) 및 ESP(보안 페이로드 캡슐화) 프로토콜을 지원해야 합니다. AH를 선택할 것인지 아니면 ESP를 선택할 것이지는 VPN 연결에 대해 정의한 제안에 따라 다릅니다.
4. VPN 연결을 통해 사용자 세션을 활성화할 수 있습니까? 응답이 **예**인 경우에는 VPN 연결이 제대로 작동합니다. 응답이 **아니오** 경우에는 패킷 규칙을 검사하고 원하는 사용자 통신을 허용하지 않는 필터 정의에 대한 VPN 동적-키 그룹 및 VPN 연결을 검사하십시오.

일반적인 VPN 구성 오류 및 오류 수정 방법

이 섹션에서는 VPN에서 발생하는 보다 일반적인 문제점 몇 가지를 설명하고, 이 문제점을 해결하는 방법에 대한 추가 정보로 링크를 제공합니다.

주: VPN을 구성하는 경우, 실제로는 VPN 연결에 필요한 몇 가지 서로 다른 구성 오브젝트를 작성하게 됩니다. VPN GUI 측면에서 볼 때, 이 오브젝트에는 IP 보안 정책 및 보안 연결이 있습니다. 그러므로, 이 정보가 오브젝트를 참조하는 경우 하나 이상의 이 VPN 부분을 참조하고 있는 것입니다.

나타나는 일반적인 오류 메세지

메세지	증상
TCP5B28	인터페이스에 대해 필터 규칙을 활성화하려고 하면, 다음 메세지를 수신하게 됩니다: TCP5B28 순서 위반
항목을 찾을 수 없음	VPN 오브젝트를 마우스 오른쪽 버튼으로 클릭하고 **등록 정보** 또는 **삭제**를 선택하면, **항목을 찾을 수 없음**이라는 메세지가 나타납니다.
PARAMETER PINBUF IS NOT VALID	연결을 시작하려고 시도하면, **PARAMETER PINBUF IS NOT VALID...**라는 메세지가 나타납니다.
항목을 찾을 수 없음, 리모트키 서버...	동적-키 연결 **등록 정보**를 선택하면, 서버가 사용자가 지정한 리모트 키 서버를 찾을 수 없다는 오류 메세지가 나타납니다.
오브젝트를 갱신할 수 없음	동적-키 그룹이나 수동 연결의 등록 정보 용지에서 **확인**을 선택하면, 시스템이 오브젝트를 갱신할 수 없다는 메세지가 나타납니다.
키를 암호화할 수 없음...	QRETSVRSEC 값이 1로 설정되어 있기 때문에 시스템이 키를 암호화할 수 없다는 메세지가 나타납니다.
CPF9821	iSeries Navigator에서 IP 정책 컨테이너를 확장하거나 열려고 시도하면, CPF9821- QSYS 라이브러리의 QTFRPRS 프로그램에 대한 권한이 없음 메세지가 나타납니다.

발생할 수 있는 기타 문제점

오류	증상
모든 키가 공백임	수동 연결 등록 정보를 볼 때, 연결에 대해 사전공유된 모든 키와 알고리즘 키가 공백입니다.
다른 시스템에 대한 사인온이 나타남	iSeries Navigator에서 패킷 규칙 인터페이스를 처음 사용할 때, 현재 시스템이 아닌 다른 시스템에 대한 사인 온 표시 화면이 나타납니다.
연결 상태 없음	연결이 iSeries Navigator의 **상태** 열에 값을 갖고 있지 않습니다.
중단된 연결을 계속 작동할 수 있음	연결을 중단한 후에도 iSeries Navigator 창에 연결이 계속 작동가능하다고 표시됩니다.
3DES는 암호화 선택사항이 아님	IKE 정책 변환, 자료 정책 변환 또는 수동 연결에 대해 작업할 때, 3DES 암호화 알고리즘을 선택할 수 없습니다.
예기치 않은 열 표시 화면	iSeries Navigator 창에 VPN 연결에 표시할 열을 설정한 후 나중에 이 창을 볼 때 다른 열이 표시됩니다.

활동 필터 규칙 비활성화 실패	현재의 필터 규칙 세트를 비활성화하려고 할 때, 활동 규칙 비활성화 실패 메세지가 결과 창에 나타납니다.
연결에 대한 동적-키 그룹 변경	동적-키 연결을 작성할 때, 리모트 키 서버에 대한 동적-키 그룹 및 ID를 지정하십시오. 나중에 관련된 연결 오브젝트 등록 정보를 볼 때, 등록 정보 용지의 일반 페이지는 동일한 리모트 키 서버 ID를 표시하지만 다른 동적-키 그룹을 표시합니다.

VPN 오류 메세지: TCP5B28

증상

특정 인터페이스에 대해 필터 규칙을 활성화하려고 하면, 다음 오류 메세지를 수신하게 됩니다.

```
TCP5B28: CONNECTION_DEFINITION 순서 위반
```

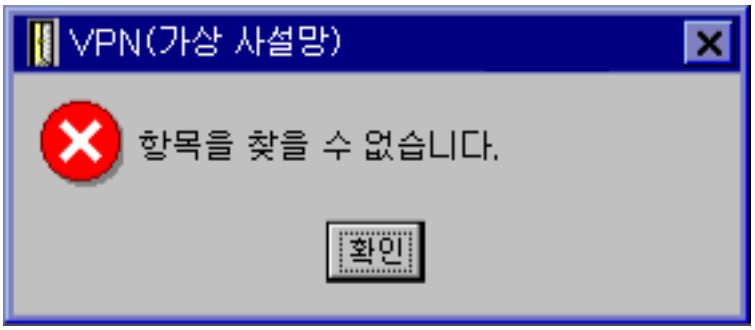
가능한 해결책

활성화를 시도하는 필터 규칙에 이전에 활성화된 규칙 세트와 다른 순서로 정렬된 연결 정의가 포함되어 있습니다. 이 오류를 해결하는 가장 쉬운 방법은 특정 인터페이스가 아니라 **모든 인터페이스**에 대해 규칙을 활성화하는 것입니다.

VPN 오류 메세지: 항목을 찾을 수 없음

증상

가상 사설망 창에서 오브젝트를 마우스 오른쪽 버튼으로 클릭하고 **등록 정보** 또는 **삭제**를 선택하면, 다음과 같은 메세지가 나타납니다.



가능한 해결책

- 오브젝트가 삭제되거나 이름이 변경된 후 창이 아직 화면정리되지 않았습니다. 따라서, 오브젝트가 VPN(가상 사설망) 창에 계속 나타납니다. 이를 확인하려면 **보기** 메뉴에서 **화면정리**를 선택하십시오. 오브젝트가 VPN(가상 사설망) 창에 아직도 나타나는 경우에는 이 리스트의 다음 항목으로 가십시오.
- 오브젝트에 대한 등록 정보를 구성했을 때, VPN 서버와 iSeries간 통신 오류가 발생했을 수 있습니다. VPN(가상 사설망) 창에 나타나는 대부분의 오브젝트는 VPN 정책 데이터베이스에 있는 하나 이상의 오브젝트와 관련됩니다. 즉, 통신 오류는 데이터베이스에 있는 일부 오브젝트가 VPN에 있는 오브젝트와 계속적으로 관련되도록 할 수 있습니다. 오브젝트를 작성하거나 갱신할 때마다 동기화 손실이 실제로 발생하면 오류가 발생합니다. 문제점을 수정하는 유일한 방법은 오류 창에서 **확인**을 선택하는 것입니다. 확인을 선택하면 오류

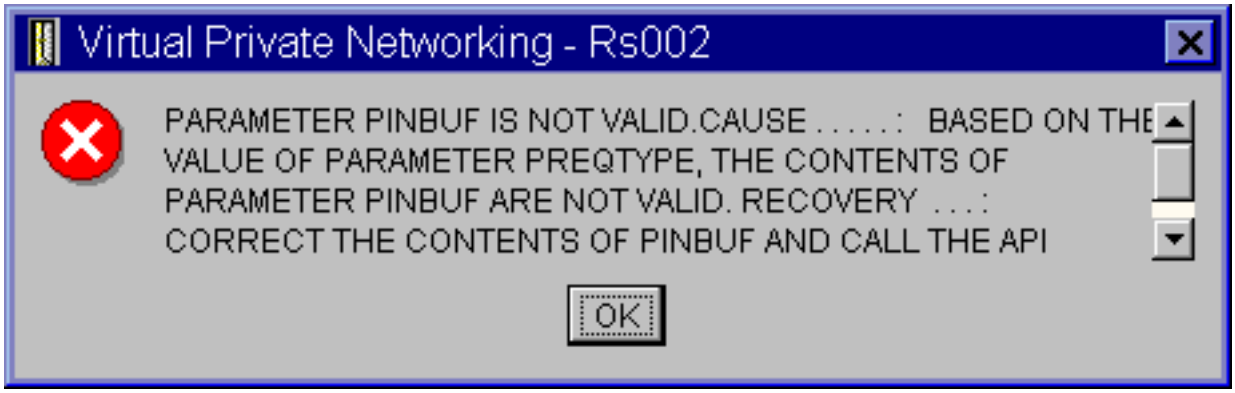
오브젝트에 대한 등록 정보 용지가 시작됩니다. 등록 정보 용지의 이름 필드만 필드 내부에서 값을 가집니다. 다른 모든 필드는 공백(또는 디폴트 값)입니다. 올바른 오브젝트 속성을 입력한 후 **확인**을 선택하여 변경사항을 저장하십시오.

- 오브젝트를 삭제하려는 경우에도 이와 유사한 오류가 발생합니다. 이 문제점을 수정하려면 오류 메세지에서 **확인**을 클릭할 때 열리는 공백 등록 정보 용지를 완료하십시오. 그러면 손실한 VPN 정책 데이터베이스에 대한 모든 링크가 갱신됩니다. 이제 오브젝트를 삭제할 수 있습니다.

VPN 오류 메세지: PARAMETER PINBUF IS NOT VALID

증상

연결을 시작하려고 시도할 때 다음과 유사한 메세지가 나타납니다.



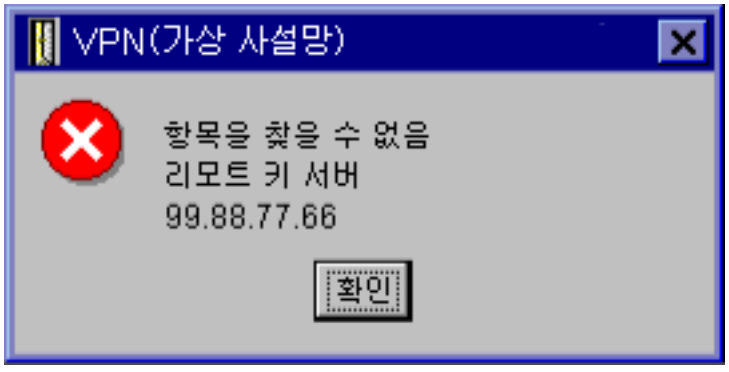
가능한 해결책

이 메세지는 소문자가 정확하게 맵핑되지 않는 특정 로케일을 사용하도록 시스템이 설정되어 있을 때 나타납니다. 이 오류를 수정하려면 모든 오브젝트가 대문자만 사용하도록 하거나 시스템 로케일을 변경해야 합니다.

VPN 오류 메세지: 항목을 찾을 수 없음, 리모트 키 서버...

증상

동적-키 연결 **등록 정보**를 선택하면, 다음과 유사한 메세지가 나타납니다.



가능한 해결책

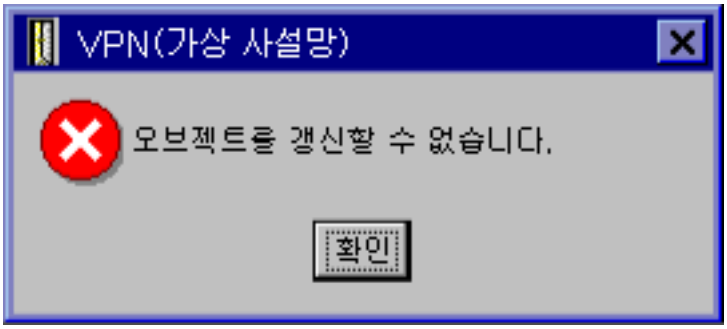
이 메세지는 특정 리모트 키 서버 ID로 연결을 작성한 후 해당 리모트 키 서버가 동적-키 그룹에서 제거될 때

나타납니다. 이 오류를 수정하려면 오류 메세지에서 **확인**을 클릭하십시오. 그러면 오류 상태의 동적-키 연결에 대한 등록 정보 용지가 열립니다. 여기서, 리모트 키 서버를 동적-키 그룹에 다시 추가하거나 다른 리모트 키 서버 ID를 선택할 수 있습니다. 등록 정보 용지에서 **확인**을 클릭하여 변경사항을 저장하십시오.

VPN 오류 메세지: 오브젝트를 갱신할 수 없음

증상

동적-키 그룹, 수동 연결에 대해 등록 정보 용지에서 **확인**을 선택하면 다음과 같은 메세지가 나타납니다.



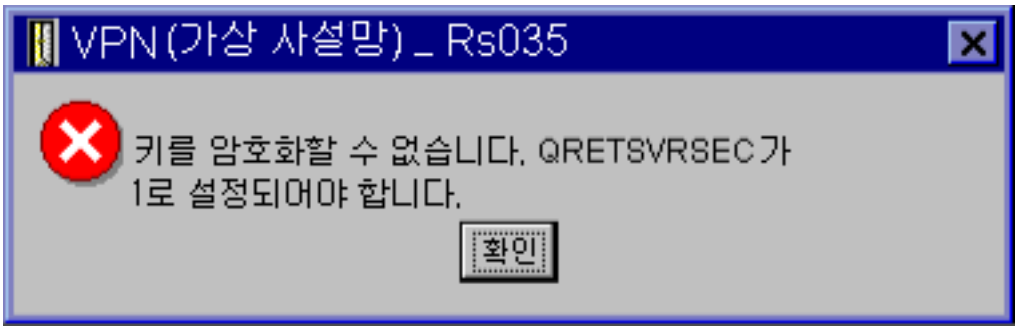
가능한 해결책

이 오류는 변경하려는 오브젝트가 활동 연결에서 사용되고 있을 때 발생합니다. 활동 연결 내부에서 오브젝트를 변경할 수 없습니다. 오브젝트를 변경하려면, 해당 활동 연결을 식별한 후 마우스 오른쪽 버튼으로 클릭하고 결과 상황 메뉴에서 **중단**을 선택하십시오.

VPN 오류 메세지: 키를 암호화할 수 없음...

증상

다음과 같은 오류 메세지가 나타납니다.



가능한 해결책

QRETSVRSEC는 암호화된 키를 시스템에 저장할 수 있는지 여부를 표시하는 시스템 값입니다. 이 값이 0으로 설정되어 있으면, 사전공유 키 및 수동 연결 알고리즘 키가 VPN 정책 데이터베이스에 저장될 수 없습니다. 이 문제점을 수정하려면 5250 에뮬레이션 세션을 시스템에 사용하십시오. 명령행에 `wrksysval`을 입력하고 **Enter**를 누르십시오. 리스트에서 QRETSVRSEC를 찾아 그 옆에 2(변경)를 입력하십시오. 다음 패널에서 1을 입력하고 **Enter**를 누르십시오.

VPN 오류 메세지: CPF9821

증상

iSeries Navigator에서 IP 정책 컨테이너를 확장할 때 CPF9821- QSYS 라이브러리의 QTFRPRS 프로그램에 대한 권한이 없음 메세지가 나타납니다.

가능한 해결책

패킷 규칙 또는 VPN 연결 관리자의 현재 상태를 검색하는 데 필요한 권한이 없습니다. *IOSYSCFG 권한이 있어야 합니다. 이제 iSeries Navigator에서 패킷 규칙 기능에 액세스할 수 있어야 합니다.

VPN 오류: 모든 키가 공백임

증상

수동 연결에 대해 모든 사전공유 키 및 알고리즘 키가 공백입니다.

가능한 해결책

이 오류는 시스템 값 QRETSVRSEC가 다시 0으로 설정될 때마다 발생합니다. 이 시스템 값이 0으로 설정되면 VPN 정책 데이터베이스의 모든 키가 지워집니다. 이 문제점을 해결하려면 시스템 값을 1로 설정한 후 모든 키를 재입력해야 합니다. 이를 수행하는 방법에 대한 자세한 정보는 오류 메세지: 키를 암호화할 수 없음을 참조하십시오.

VPN 오류: 패킷 규칙을 사용할 때 다른 시스템에 대한 사인 온이 나타남

증상

패킷 규칙을 처음 사용할 때, 현재 시스템이 아닌 다른 시스템에 대한 사인 온 표시 화면이 나타납니다.

가능한 해결책

패킷 규칙은 유니코드를 사용하여 패킷 보안 규칙을 통합 파일 시스템에 저장합니다. 추가 사인 온을 수행하면 Client Access Express가 유니코드에 대한 적절한 변환 표를 확보할 수 있습니다. 이 오류는 두 번 이상 발생되어서는 안됩니다.

VPN 오류: iSeries Navigator 창에서 공백 연결 상태

증상

연결이 iSeries Navigator의 **상태** 열에 값을 갖고 있지 않습니다.

가능한 해결책

공백 상태 값은 연결이 시작되고 있음을 표시합니다. 즉, 아직 실행되고 있지 않을 뿐이지 오류가 발생한 것이 아닙니다. 창을 화면정리할 때, 연결 상태는 오류, 작동 가능, On-demand 또는 유휴 상태 중 하나로 표시되어야 합니다.

VPN 오류: 연결을 중단한 후에도 연결이 작동 가능 상태임

증상

연결을 중단한 후에도 iSeries Navigator 창에 연결이 계속 작동 가능하다고 표시됩니다.

가능한 해결책

이 오류는 iSeries Navigator 창을 아직 화면정리하지 않았기 때문에 발생합니다. 그런 경우, 창에는 오래된 정보가 들어 있습니다. 이 오류를 수정하려면 **보기** 메뉴에서 **화면정리**를 선택하십시오.

VPN 오류: 3DES는 암호화 선택사항이 아님

증상

IKE 정책 변환, 자료 정책 변환 또는 수동 연결에 대해 작업할 때, 3DES 암호화 알고리즘을 선택할 수 없습니다.

가능한 해결책

Cryptographic Access Provider AC3(5769-AC3)은 설치되어 있지 않고 Cryptographic Access Provider AC2(5769-AC2) 제품만 시스템에 설치되어 있을 가능성이 높습니다. AC2는 키 길이의 제한으로 인해 자료 암호화 표준(DES) 암호화 알고리즘에 대해서만 허용됩니다.

VPN 오류: iSeries Navigator에서 예상치 못한 열 표시 화면

증상

iSeries Navigator 창에 VPN 연결에 표시할 열을 설정한 후 나중에 이 창을 볼 때 다른 열이 표시됩니다.

가능한 해결책

보려는 열을 변경하면, 변경사항이 특정 사용자나 PC에 국한되지 않고 시스템 전반에 적용됩니다. 따라서, 어떤 사용자가 창에서 열을 변경하면 해당 시스템에서 연결을 보는 모든 사용자에게 변경사항이 적용됩니다.

VPN 오류: 활동 필터 규칙 비활성화 실패

증상

현재의 필터 규칙 세트를 비활성화하려고 할 때, 활동 규칙 비활성화 실패 메세지가 결과 창에 나타납니다.

가능한 해결책

일반적으로, 이 오류 메세지는 최소 하나의 활동 VPN 연결이 있음을 의미합니다. 작동가능 상태인 모든 연결을 중단해야 합니다. 이를 수행하려면, 활동 연결을 각각 마우스 오른쪽 버튼으로 클릭하고 **중단**을 선택하십시오. 이제는 필터 규칙을 비활성화할 수 있습니다.

VPN 오류: 연결에 대한 키 연결 그룹 변경

증상

동적-키 연결을 작성할 때, 리모트 키 서버에 대한 동적-키 그룹 및 ID를 지정하십시오. 나중에 관련된 연결 오브젝트에서 **등록 정보**를 선택하면, 등록 정보 용지의 **일반** 페이지는 동일한 리모트 키 서버 ID를 표시하지만 다른 동적-키 그룹을 표시합니다.

가능한 해결책

ID는 동적-키 연결의 리모트 키 서버를 참조하는 VPN 정책 데이터베이스에 저장된 유일한 정보입니다. 리모트 키 서버 정책을 찾을 때, VPN은 해당 리모트 키 서버 ID를 가진 첫 번째 동적-키 그룹을 찾습니다. 따라서, 이 연결 중 하나에 대한 등록 정보를 볼 때 VPN이 찾은 동일한 동적-키 그룹이 사용됩니다. 동적-키 그룹을 해당 리모트 키 서버와 연관시키지 않으려면, 다음 중 하나를 수행하십시오.

1. 동적-키 그룹에서 리모트 키 서버를 제거하십시오.
2. VPN 인터페이스의 왼쪽 분할 창에서 **그룹별**을 확장한 후, 원하는 동적-키 그룹을 선택하여 오른쪽 분할 창에 있는 표 맨 위로 끄십시오. 이렇게 하면 VPN이 리모트 키 서버에 대해 이 동적-키 그룹을 맨 먼저 검사합니다.

QIPFILTER 저널을 사용하여 VPN 문제 해결

QUSRSYS 라이브러리에 있는 QIPFILTER 저널에는 필터 규칙 세트에 대한 정보 뿐만 아니라, IP 데이터그램이 허용되었는지 아니면 거부되었는지에 대한 정보도 들어 있습니다. 필터 규칙에 지정한 저널링 옵션을 근거로 기록이 수행됩니다.

IP 패킷 필터 저널을 작동할 수 있게 하는 방법

QIPFILTER 저널을 활성화하려면 iSeries Navigator에서 패킷 규칙 편집기를 사용하십시오. 각각의 개별 필터 규칙에 대한 기록 기능을 작동할 수 있게 해야 합니다. 모든 IP 데이터그램을 시스템 내부로 가져오거나 외부로 내보내는 기록을 허용하는 기능은 없습니다.

주: TQIPFILTER 저널을 작동할 수 있게 하려면 필터를 비활성화해야 합니다.

다음 단계에서는 특정 필터 규칙에 대한 저널링을 작동할 수 있게 하는 방법을 설명합니다.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책**을 확장하십시오.
2. **패킷 규칙**을 마우스 오른쪽 버튼으로 클릭하고 **구성**을 선택하십시오. 패킷 규칙 인터페이스가 표시됩니다.
3. 기존의 필터 규칙 파일을 여십시오.
4. 저널링할 필터 규칙을 두 번 클릭하십시오.
5. 위의 대화상자에서와 같이, **일반** 페이지의 **저널링** 필드에서 **FULL**을 선택하십시오. 그러면 이 특정 필터 규칙에 대한 기록을 작동시킬 수 있습니다.
6. **확인**을 클릭하십시오.
7. 변경된 필터 규칙 파일을 저장한 후 활성화하십시오.

IP 데이터그램이 필터 규칙 정의와 일치하는 경우에는 QIPFILTER 저널에 하나의 항목이 작성됩니다.

QIPFILTER 저널 사용 방법

OS/400은 IP 패킷 필터링을 처음 활성화할 때 저널을 자동으로 작성합니다. 화면에 저널 항목을 표시하거나 출력 파일을 사용하면 저널에 있는 입력 항목별 세부사항을 볼 수 있습니다.

저널 항목을 출력 파일에 복사하면 Query/400 또는 SQL과 같은 조회 유틸리티를 사용하여 항목을 쉽게 볼 수 있습니다. 고유 HLL 프로그램을 기록하여 출력 파일의 항목을 처리할 수도 있습니다.

다음은 DSPJRN(저널 표시) 명령의 예입니다.

```
DSPJRN JRN(QIPFILTER) JRNCDE((M)) ENTTYP((TF)) OUTPUT(*OUTFILE)
    OUTFILFMT(*TYPE4) OUTFILE(mylib/myfile) ENTDTALEN(*VARLEN *CALC)
```

QIPFILTER 저널 항목을 출력 파일에 복사하려면 다음 단계를 사용하십시오.

1. CRTDUPOBJ(복제 오브젝트 작성) 명령을 사용하여 시스템 제공 출력 파일 QSYS/QATOFIPF 사본을 사용자 라이브러리에 작성하십시오. 다음은 CRTDUPOBJ 명령의 예입니다.

   ```
   CRTDUPOBJ OBJ(QATOFIPF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(mylib)
        NEWOBJ(myfile)
   ```

2. QUSRSYS/QIPFILTER 저널의 항목을 이전 단계에서 작성한 출력 파일에 복사하려면 DSPJRN(저널 표시) 명령을 사용하십시오.

DSPJRN을 존재하지 않는 출력 파일에 복사하는 경우, 시스템은 파일을 작성하지만 이 파일에는 적절한 필드 설명이 들어 있지 않습니다.

주: QIPFILTER 저널에는 저널링 옵션이 FULL로 설정된 필터 규칙에 대한 허용 또는 거부 항목만 들어 있습니다. 예를 들어, PERMIT 필터 규칙만 설정할 경우에는 명시적으로 허용되지 않는 IP 데이터그램은 거부됩니다. 이렇게 거부된 데이터그램의 경우, 저널에 어떤 항목도 추가되지 않습니다. 문제점 분석을 위해 기타 모든 통신량을 명시적으로 거부하고 FULL 저널링을 수행하는 필터 규칙을 추가할 수 있습니다. 이 경우, 거부된 모든 IP 데이터그램에 대한 저널에는 DENY 항목이 주어집니다. 성능상, 모든 필터 규칙에 대한 저널링을 작동할 수 있게 하지 않는 것이 좋습니다. 필터 세트를 테스트한 후에는 저널링을 유용한 항목 서브세트로 줄이십시오.

QIPFILTER 출력 파일을 설명하는 표에 대해서는 QIPFILTER 저널 필드를 참조하십시오.

QIPFILTER 저널 필드

다음 표에서는 QIPFILTER 출력 파일의 필드를 설명합니다.

필드명	필드 길이	숫자	설명	주석
TFENTL	5	Y	항목 길이	
TFSEQN	10	Y	순번	
TFCODE	1	N	저널 코드	항상 M
TFENTT	2	N	항목 유형	항상 TF
TFTIME	26	N	SAA 시간소인	
TFJOB	10	N	작업 이름	
TFUSER	10	N	사용자 프로파일	
TFNBR	6	Y	작업 수	
TFPGM	10	N	프로그램 이름	
TFRES1	51	N	예약	
TFUSPF	10	N	사용자	
TFSYMN	8	N	시스템 이름	
TFRES2	20	N	예약	
TFRESA	50	N	예약	
TFLINE	10	N	회선 설명	TFREVT가 U*일 때: *ALL, TFREVT가 L*일 때: 공백, TFREVT가 L일 때: 회선 이름

TFREVT	2	N	규칙 이벤트	규칙이 로드될 때: L* 또는 L, 규칙이 언로드될 때: U*, 필터가 작동될 때: A
TFPDIR	1	N	IP 패킷 방향	O: 아웃바운드, I: 인바운드
TFRNUM	5	N	규칙 수	활동 규칙 파일에 있는 규칙 수에 적용
TFACT	6	N	취해진 필터 조치	PERMIT, DENY 또는 IPSEC
TFPROT	4	N	전송 프로토콜	1: ICMP 6: TCP 17: UDP 50: ESP 51: AH
TFSRCA	15	N	소스 IP 주소	
TFSRCP	5	N	소스 포트	TFPROT=1(ICMP)이면 가비지
TFDSTA	15	N	목적지 IP 주소	
TFDSTP	5	N	목적지 포트	TFPROT=1(ICMP)이면 가비지
TFTEXT	76	N	추가 텍스트	TFREVT=L* 또는 U*이면 설명 포함

QVPN을 사용하여 VPN 문제 해결

VPN은 QVPN 저널이라는 별도의 저널을 사용하여 IP 통신량 및 연결 정보를 기록합니다. QVPN은 QUSRSYS 라이브러리에 저장됩니다. 저널 코드는 M이고 저널 유형은 TS입니다. 저널 항목을 매일 사용하지는 않을 것입니다. 그 대신, 저널 항목은 시스템, 키 및 연결이 지정된 방식대로 기능을 하는지를 확인하고 문제점을 해결하는 데 유용합니다. 예를 들어, 저널 항목은 자료 패킷에서 무엇이 발생되는지를 이해하는 데 도움을 줍니다. 또한 현재 VPN 상태도 계속 알려 줍니다.

VPN 저널을 작동할 수 있게 하는 방법

VPN 저널을 활성화하려면 iSeries Navigator에서 VPN(가상 사설망) 인터페이스를 사용하십시오. 모든 VPN 연결에 대해 기록을 허용하는 기능은 없습니다. 따라서, 각각의 개별 동적-키 그룹 또는 수동 연결에 대해 기록 기능을 작동할 수 있게 해야 합니다.

다음 단계에서는 특정 동적-키 그룹 또는 수동 연결에 대해 저널링 기능을 작동할 수 있게 하는 방법을 설명합니다.

1. iSeries Navigator에서, 서버 —> **네트워크** —> **IP 정책** —> **가상 사설망** —> **보안 연결**을 확장하십시오

2. 동적-키 그룹의 경우, **그룹별**을 확장한 후 저널링을 작동할 수 있게 할 동적 키 그룹을 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
3. 수동 연결의 경우, **모든 연결**을 확장한 후 저널링을 작동할 수 있게 할 수동 연결을 마우스 오른쪽 버튼으로 클릭하십시오.
4. **일반** 페이지에서, 필요한 저널링 레벨을 선택하십시오. 네 가지 옵션 중 하나를 선택할 수 있습니다. 옵션은 다음과 같습니다.

   None

   이 연결 그룹에 대한 저널링이 발생하지 않습니다.

   All

   모든 연결 활동(예: 연결 시작 또는 중단, 키 화면정리) 및 IP 통신량 정보에 대한 저널링이 발생합니다.

   Connection Activity

   연결 시작 또는 중단 등의 연결 활동에 대한 저널링이 발생합니다.

   IP traffic

   이 연결과 연관된 모든 VPN 통신량에 대한 저널링이 발생합니다. 필터 규칙이 호출될 때마다 기록부 항목이 작성됩니다. 시스템은 IP 통신량 정보를 QUSRSYS 라이브러리에 있는 QIPFILTER 저널에 기록합니다.
5. **확인**을 클릭하십시오.
6. 연결을 시작하여 저널링을 활성화하십시오.

주: 저널링을 중단하기 전에 먼저 연결이 비활성화 되었는지 확인하십시오. 연결 그룹의 저널링 상태를 변경하려면 해당 특정 그룹과 연관된 활동 연결이 없어야 합니다.

VPN 저널 사용 방법

화면에 항목을 표시하거나 출력 파일을 사용하면 VPN 저널에 있는 입력 항목별 세부사항을 볼 수 있습니다.

저널 항목을 출력 파일에 복사하면 Query/400 또는 SQL과 같은 조회 유틸리티를 사용하여 항목을 쉽게 볼 수 있습니다. 고유 HLL 프로그램을 기록하여 출력 파일의 항목을 처리할 수도 있습니다. 다음은 DSPJRN(저널 표시) 명령의 예입니다.

```
DSPJRN JRN(QVPN) JRNCDE((M)) ENTTYP((TS)) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4)
    OUTFILE(mylib/myfile) ENTDTALEN(*VARLEN *CALC)
```

VPN 저널 항목을 출력 파일에 복사하려면 다음 단계를 사용하십시오.

1. 시스템 제공 출력 파일 QSYS/QATOVSOF를 사용자 라이브러리에 복사하십시오. CRTDUPOBJ(복제 오브젝트 작성) 명령을 사용하여 이를 복사할 수 있습니다. 다음은 CRTDUPOBJ 명령의 예입니다.

   ```
   CRTDUPOBJ OBJ(QATOVSOF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(mylib)
        NEWOBJ(myfile)
   ```
2. QUSRSYS/QVPN 저널의 항목을 이전 단계에서 작성한 출력 파일에 복사하려면 DSPJRN(저널 표시) 명령을 사용하십시오. DSPJRN을 존재하지 않는 출력 파일에 복사하려는 경우, 시스템은 파일을 작성하지만 이 파일에는 적절한 필드 설명이 들어 있지 않습니다.

QVPN 출력 파일의 필드를 설명하는 표에 대해서는 QVPN 저널 필드를 참조하십시오.

QVPN 저널 필드

다음 표에서는 QVPN 출력 파일의 필드를 설명합니다.

필드명	필드 길이	숫자	설명	주석
TSENTL	5	Y	항목 길이	
TSSEQN	10	Y	순번	
TSCODE	1	N	저널 코드	항상 M
TSENTT	2	N	항목 유형	항상 TS
TSTIME	26	N	SAA 항목 시간소인	
TSJOB	10	N	작업명	
TSUSER	10	N	작업 사용자	
TSNBR	6	Y	작업 번호	
TSPGM	10	N	프로그램명	
TSRES1	51	N	사용되지 않음	
TSUSPF	10	N	사용자 프로파일명	
TSSYNM	8	N	시스템 이름	
TSRES2	20	N	사용되지 않음	
TSRESA	50	N	사용되지 않음	
TSESDL	4	Y	특정 자료의 길이	
TSCMPN	10	N	VPN 구성요소	
TSCONM	40	N	연결명	
TSCOTY	10	N	연결 유형	
TSCOS	10	N	연결 상태	
TSCOSD	8	N	시작 날짜	
TSCOST	6	N	시작 시간	
TSCOED	8	N	종료 날짜	
TSCOET	6	N	종료 시간	
TSTRPR	10	N	전송 프로토콜	
TSLCAD	43	N	로컬 클라이언트 주소	
TSLCPR	11	N	로컬 포트	
TSRCAD	43	N	리모트 클라이언트 주소	
TSCPR	11	N	리모트 포트	
TSLEP	43	N	로컬 종료점	
TSREP	43	N	리모트 종료점	
TSCORF	6	N	화면정리된 시간	
TSRFDA	8	N	다음 화면정리 날짜	
TSRFTI	6	N	다음 화면정리 시간	
TSRFLS	8	N	화면정리 시간의 길이	
TSSAPH	1	N	SA 단계	
TSAUTH	10	N	인증 유형	
TSENCR	10	N	암호화 유형	
TSDHGR	2	N	Diffie-Hellman 그룹	

TSERRC	8	N	오류 코드	

VPN 작업 기록부를 사용하여 VPN 문제 해결

VPN 연결 문제점이 발생할 때 작업 기록부를 분석하는 것이 항상 도움이 됩니다. 실제로, 오류 메세지 및 기타 VPN 환경 관련 정보가 포함되어 있는 여러 개의 작업 기록부가 있습니다.

양쪽 모두 iSeries 서버인 경우에는 연결 양쪽에서 작업 기록부를 분석하는 것이 중요합니다. 동적 연결이 시작하는 데 실패할 때 리모트 시스템에 무슨 일이 발생하고 있는지를 이해하면 도움이 됩니다.

VPN 작업 QTOVMAN 및 QTOKVPNIKE는 서브시스템 QSYSWRK에서 실행됩니다. OS/400 Operations Navigator에서 각 작업 기록부 보기를 수행할 수 있습니다.

이 섹션에서는 VPN 환경에 대한 가장 중요한 작업을 소개합니다. 다음 리스트에서는 작업 이름과 작업 사용 목적에 대한 간략한 설명을 보여줍니다.

QTCPIP
이 작업은 모든 TCP/IP 인터페이스를 시작하는 기본 작업입니다. 일반적으로 근본적인 TCP/IP 문제점이 발생한 경우에는 QTCPIP 작업 기록부를 분석하십시오.

QTOKVPNIKE
QTOKVPNIKE 작업은 VPN 키 관리자 작업입니다. VPN 키 관리자는 UDP 포트 500을 청취하여 인터넷 키 교환(IKE) 프로토콜 처리를 수행합니다.

QTOVMAN
이 작업은 VPN 연결용 연결 관리자입니다. 관련 작업 기록부에는 실패한 모든 연결 시도에 대한 메세지가 들어 있습니다.

QTPPANSxxx
이 작업은 PPP 전화접속 연결용으로 사용됩니다. *ANS가 PPP 프로파일에 정의되어 있는 경우, 연결 시도에 응답합니다.

QTPPPCTL
이 작업은 다이얼 아웃 연결용 PPP 작업입니다.

QTPPPL2TP
이 작업은 L2TP 관리자 작업입니다. L2TP 터널 설정 문제점이 발생한 경우에는 이 작업 기록부에서 메세지를 찾아 보십시오.

일반적인 VPN 연결 관리자 오류 메세지

이 섹션에서는 보다 일반적인 VPN 연결 관리자 오류 메세지 중 일부를 설명합니다.

일반적으로, VPN 연결 관리자는 VPN 연결시 오류가 발생하면 QTOVMAN 작업 기록부에 두 개의 오류 메세지를 기록합니다. 첫 번째 메세지는 오류와 관련한 세부사항을 제공합니다. 오류 연결을 마우스 오른쪽 버튼으로 클릭하고 **오류정보**를 선택하면 iSeries Navigator에서 오류 정보를 볼 수 있습니다.

두 번째 메세지는 오류가 발생했을 때 연결에 대해 수행하려고 시도하던 조치를 설명합니다. 연결 시작 또는 중단을 예로 들 수 있습니다. 아래 설명한 메세지 TCP8601, TCP8602 및 TCP860A가 두 번째 메세지의 일반적인 예입니다.

VPN 연결 관리자 오류 메세지

메세지	원인	회복
TCP8601 VPN 연결[*연결명*]을 시작할 수 없음	다음 오류 코드 중 하나로 인해 이 VPN 연결을 시작할 수 없습니다. *0* - VPN 연결명이 동일한 작업 기록부의 이전 메세지에 자세한 정보가 있습니다. *1* - VPN 정책 구성. *2* - 통신 네트워크 실패. *3* - VPN 키 관리자가 신규 보안 협약 협상에 실패했습니다. *4* - 이 연결의 리모트 종료점이 올바로 구성되지 않았습니다. *5* - VPN 키 관리자가 VPN 연결 관리자에 응답하는 데 실패했습니다. *6* - IP 보안 구성요소 VPN 연결 로드 실패. *7* - PPP 구성요소 실패.	1. 메세지를 추가로 보려면 작업 기록부를 검사하십시오. 2. 오류를 정정하고 요구를 다시 시도하십시오. 3. iSeries Navigator를 사용하여 연결 상태 보기를 수행하십시오. 시작할 수 없었던 연결은 오류 상태에 있게 됩니다.
TCP8602 VPN 연결[*연결명*]을 중단하는 중 오류 발생	지정된 VPN 연결 중단 요구가 있었지만 다음 이유 코드로 인해 중단되지 못하고 오류가 발생했습니다. *0* - VPN 연결명이 동일한 작업 기록부의 이전 메세지에 자세한 정보가 있습니다. *1* - VPN 연결이 없습니다. *2* - VPN 키 관리자와의 내부 통신 실패. *3* - IPSec 구성요소와의 내부 통신 실패. *4* - VPN 연결 리모트 종료점과의 통신 실패.	1. 메세지를 추가로 보려면 작업 기록부를 검사하십시오. 2. 오류를 정정하고 요구를 다시 시도하십시오. 3. iSeries Navigator를 사용하여 연결 상태 보기를 수행하십시오. 시작할 수 없었던 연결은 오류 상태에 있게 됩니다.
TCP8604 VPN 연결[*연결명*] 시작 실패	다음 오류 코드 중 하나로 인해 VPN 연결 시작이 실패했습니다. *1* - 리모트 호스트명을 IP 주소로 변환할 수 없습니다. *2* - 로컬 호스트명을 IP 주소로 변환할 수 없습니다. *3* - 이 VPN 연결과 연관된 VPN 정책 필터가 로드되지 않습니다. *4* - 사용자 지정 키 값이 연관된 알고리즘에 유효하지 않습니다. *5* - VPN 연결 시작 값이 지정된 조치를 허용하지 않습니다. *6* - VPN 연결을 위한 시스템 역할이 연결 그룹 정보와 일치하지 않습니다. *7* - 예약. *8* - 이 VPN 연결의 자료 종료점(로컬 및 리모트 주소, 서비스)이 연결 그룹 정보와 일치하지 않습니다. *9* - ID 유형이 유효하지 않습니다.	1. 메세지를 추가로 보려면 작업 기록부를 검사하십시오. 2. 오류를 정정하고 요구를 다시 시도하십시오. 3. iSeries Navigator를 사용하여 VPN 정책 구성을 검사하거나 정정하십시오. 이 연결과 연관된 동적-키 그룹이 허용된 값으로 구성되었는지 확인하십시오.

TCP8605 VPN 연결 관리자가 VPN 키 관리자와 통신할 수 없음	동적 VPN 연결을 위한 보안 협약을 설정하려면 VPN 연결 관리자에 VPN 키 관리자 서비스가 필요합니다. VPN 연결 관리자가 VPN 키 관리자와 통신할 수 없습니다.	1. 메세지를 추가로 보려면 작업 기록부를 검사하십시오. 2. *LOOPBACK 인터페이스가 NETSTAT OPTION(*IFC) 명령을 사용하여 활동 중인지 확인하십시오. 3. ENDTCPSVR SERVER(*VPN) 명령을 사용하여 VPN 서버를 종료하십시오. 그런 다음, STRTCPSRV SERVER(*VPN) 명령을 사용하여 VPN 서버를 재시작하십시오. **주:** 이렇게 하면 현재 VPN 연결이 종료됩니다.
TCP8606 VPN 키 관리자가 연결[*연결명*]에 대해 요구한 보안 협약을 설정할 수 없음	VPN 키 관리자가 다음 이유 코드 중 하나로 인해 요구한 보안 협약을 설정할 수 없습니다. *24* - VPN 키 관리자 키 연결 인증 실패. *8300* - VPN 키 관리자 키 연결 협의 중 실패 발생. *8306* - 로컬 사전공유 키를 찾을 수 없음. *8307* - 리모트 IKE 1단계 정책을 찾을 수 없음. *8308* - 리모트 사전공유 키를 찾을 수 없음. *8327* - VPN 키 관리자 연결 협의 시간종료. *8400* - VPN 키 관리자 VPN 연결 협의 중 실패 발생. *8407* - 리모트 IKE 2단계 정책을 찾을 수 없음. *8408* - VPN 키 관리자 연결 협의 시간종료. *8500 or 8509* - VPN 키 관리자 네트워크 오류가 발생했습니다.	1. 메세지를 추가로 보려면 작업 기록부를 검사하십시오. 2. 오류를 정정하고 요구를 다시 시도하십시오. 3. iSeries Navigator를 사용하여 VPN 정책 구성을 검사하거나 정정하십시오. 이 연결과 연관된 동적-키 그룹이 허용된 값으로 구성되었는지 확인하십시오.
TCP8608 VPN 연결[*연결명*]이 NAT 주소를 획득할 수 없음	이 동적-키 그룹 또는 지정된 자료 연결이 하나 이상의 주소에 대해 네트워크 주소 변환(NAT)이 수행되도록 지정했지만 다음 이유 코드 중 하나로 인해 실패했습니다. *1* - NAT를 적용할 주소가 단일 IP 주소가 아닙니다. *2* - 사용할 수 있는 모든 주소가 사용되었습니다.	1. 메세지를 추가로 보려면 작업 기록부를 검사하십시오. 2. 오류를 정정하고 요구를 다시 시도하십시오. 3. iSeries Navigator를 사용하여 VPN 정책을 검사하거나 정정하십시오. 이 연결과 연관된 동적-키 그룹이 허용된 주소 값으로 구성되었는지 확인하십시오.
TCP8620 로컬 연결 종료점을 사용할 수 없음	로컬 연결 종료점을 사용할 수 없기 때문에 이 VPN 연결을 작동할 수 없습니다.	1. 이 연결에 관한 메세지를 추가로 보려면 작업 기록부를 검사하십시오. 2. 로컬 연결 종료점이 NETSTAT OPTION(*IFC) 명령을 사용하여 정의되고 시작되는지 확인하십시오. 3. 오류를 정정하고 요구를 다시 시도하십시오.

TCP8621 로컬 자료 종료점을 사용할 수 없음	로컬 자료 종료점을 사용할 수 없기 때문에 이 VPN 연결을 작동할 수 없습니다.	1. 이 연결에 관한 메세지를 추가로 보려면 작업 기록부를 검사하십시오. 2. 로컬 연결 종료점이 NETSTAT OPTION (*IFC) 명령을 사용하여 정의되고 시작되는지 확인하십시오. 3. 오류를 정정하고 요구를 다시 시도하십시오.
TCP8622 전송 캡슐화가 게이트웨이와 허용되지 않음	협상 정책이 전송 캡슐화 모드를 지정했고 이 연결이 보안 게이트웨이와 정의되었기 때문에 이 VPN 연결을 작동할 수 없습니다.	1. 이 연결에 관한 메세지를 추가로 보려면 작업 기록부를 검사하십시오. 2. iSeries Navigator를 사용하여 이 VPN 연결과 연관된 VPN 정책을 변경하십시오. 3. 오류를 정정하고 요구를 다시 시도하십시오.
TCP8623 VPN 연결이 기존 연결과 겹침	기존 VPN 연결이 이미 작동되기 때문에 이 VPN 연결을 작동할 수 없습니다. 이 연결에 로컬 자료 종료점[*로컬 자료 종료점 값*] 및 리모트 자료 종료점[*리모트 자료 종료점 값*]이 있습니다.	1. 이 연결에 관한 메세지를 추가로 보려면 작업 기록부를 검사하십시오. 2. iSeries Navigator를 사용하여 로컬 자료 종료점과 리모트 자료 종료점이 연결과 겹치는 모든 작동할 수 있는 연결을 보십시오. 두 연결이 모두 필요한 경우, 기존 연결 정책을 변경하십시오. 3. 오류를 정정하고 요구를 다시 시도하십시오.
TCP8624 VPN 연결이 연관된 정책 필터 규칙 범위 내에 있지 않음	자료 종료점이 정의된 정책 필터 규칙 내에 없기 때문에 이 VPN 연결을 작동할 수 없습니다.	1. 이 연결에 관한 메세지를 추가로 보려면 작업 기록부를 검사하십시오. 2. iSeries Navigator를 사용하여 이 연결 또는 동적-키 그룹에 대한 자료 종료점 제한사항을 표시하십시오. **정책 필터 서브세트** 또는 **정책 필터와 일치하도록 사용자 정의**를 선택한 경우, 연결 자료 종료점을 검사하십시오. 연결 자료 종료점은 이 연결과 연관된 VPN 연결명과 IPSEC 조치가 있는 활동 필터 규칙 내에 있어야 합니다. 기존 연결 정책을 변경하거나 필터 규칙을 변경하여 이 연결이 가능하도록 하십시오. 3. 오류를 정정하고 요구를 다시 시도하십시오.
TCP8625 VPN 연결이 ESP 알고리즘 검사에 실패	연결과 연관된 비밀 키가 부족하기 때문에 이 VPN 연결을 작동할 수 없습니다.	1. 이 연결에 관한 메세지를 추가로 보려면 작업 기록부를 검사하십시오. 2. iSeries Navigator를 사용하여 이 연결과 연관된 정책을 표시하고 다른 비밀 키를 입력하십시오. 3. 오류를 정정하고 요구를 다시 시도하십시오.

TCP8626 VPN 연결 종료점이 자료 종료점과 동일하지 않음	정책이 VPN 연결이 호스트가 되도록 지정했지만 VPN 연결 종료점이 자료 종료점과 동일하지 않기 때문에 이 VPN 연결을 작동할 수 없습니다.	1. 이 연결에 관한 메세지를 추가로 보려면 작업 기록부를 검사하십시오. 2. iSeries Navigator를 사용하여 이 연결 또는 동적-키 그룹에 대한 자료 종료점제한사항을 표시하십시오. **정책 필터 서브세트** 또는 **정책 필터와 일치하도록 사용자 정의**를 선택한 경우, 연결 자료 종료점을 검사하십시오. 연결 자료 종료점은 이 연결과 연관된 VPN 연결명과 IPSEC 조치가 있는 활동 필터 규칙 내에 있어야 합니다. 기존 연결 정책을 변경하거나 필터 규칙을 변경하여 이 연결이 가능하도록 하십시오. 3. 오류를 정정하고 요구를 다시 시도하십시오.
TCP8628 정책 필터 규칙이 로드되지 않음	이 연결에 대한 정책 필터 규칙이 활동 중이 아닙니다.	1. 이 연결에 관한 메세지를 추가로 보려면 작업 기록부를 검사하십시오. 2. iSeries Navigator를 사용하여 활동 정책 필터를 표시하십시오. 이 연결에 대한 사전공유 키를 검사하십시오. 3. 오류를 정정하고 요구를 다시 시도하십시오.
TCP8629 IP 패킷이 VPN 연결에 대해 드롭(drop)됨	이 VPN 연결이 VPN NAT를 구성하였고 필수 NAT 주소 세트가 사용할 수 있는 NAT 주소를 초과하였습니다.	1. 이 연결에 관한 메세지를 추가로 보려면 작업 기록부를 검사하십시오. 2. iSeries Navigator를 사용하여 이 VPN 연결에 지정된 NAT 주소 수를 늘리십시오. 3. 오류를 정정하고 요구를 다시 시도하십시오.
TCP862A PPP 연결 시작 실패	이 VPN 연결이 PPP 프로파일과 연관되었습니다. 연결이 시작될 때 PPP 프로파일을 시작하려고 시도했지만 실패했습니다.	1. 이 연결에 관한 메세지를 추가로 보려면 작업 기록부를 검사하십시오. 2. PPP 연결과 연관된 작업 기록부를 검사하십시오. 3. 오류를 정정하고 요구를 다시 시도하십시오.

OS/400 통신 추적을 사용하여 VPN 문제 해결

iSeries는 근거리 통신망(LAN) 또는 광역 네트워크(WAN) 인터페이스와 같은 통신 회선에 대한 자료를 추적할 수 있는 기능을 제공합니다. 일반 사용자는 추적 자료의 전체 내용을 이해할 수 없습니다. 그러나 추적 항목을 사용하여 로컬 시스템과 리모트 시스템간 자료 교환이 발생했는지 여부를 판별할 수 있습니다.

통신 추적 시작

시스템에서 통신 추적을 시작하려면 STRCMNTRC(통신 추적 시작) 명령을 사용하십시오. 다음은 STRCMNTRC 명령의 예입니다.

```
STRCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN) MAXSTG(2048) TEXT('VPN Problems')
```

명령 매개변수는 다음 리스트에서 설명합니다.

CFGOBJ(구성 오브젝트)
추적할 구성 오브젝트의 이름. 오브젝트는 회선 설명, 네트워크 인터페이스 설명 또는 네트워크 서버 설명 중 하나입니다.

CFGTYPE(구성 유형)
회선(*LIN), 네트워크 인터페이스(*NWI) 또는 네트워크 서버(*NWS)가 추적되고 있는지 여부.

MAXSTG(버퍼 *크기*)
추적용 버퍼 *크기*. 디폴트 값은 128KB입니다. 범위는 128KB - 64MB입니다. 전체 시스템의 실제 최대 버퍼 *크기*는 시스템 서비스 툴(SST) 내에 정의됩니다. 그러므로, SST에 정의된 것보다 더 큰 버퍼 *크기*를 STRCMNTRC 명령에서 사용할 경우에는 오류 메세지가 수신될 수 있습니다. 시작된 모든 통신 추적에 대해 지정된 버퍼 *크기*의 합계가 SST에 정의된 최대 버퍼 *크기*를 초과해서는 안된다는 점에 유의하십시오.

DTADIR(자료 방향)
추적될 자료 통신량의 방향. 방향은 아웃바운드 통신량 전용(*SND), 인바운드 통신량 전용(*RCV) 또는 양방향(*BOTH) 중 하나일 수 있습니다.

TRCFULL(전체 추적)
추적 버퍼가 가득 찰 때 발생하는 사항. 이 매개변수에는 가능한 값이 두 개 있습니다. 디폴트 값은 추적 버퍼가 가득 찰 때 추적이 시작 부분을 랩하는 *WRAP입니다. 가장 오래된 추적 레코드는 수집된 신규 레코드로 대체됩니다.

두 번째 값 *STOPTRC는 MAXSTG 매개변수에 지정된 추적 버퍼가 추적 레코드로 가득 차면 추적을 중단시킵니다. 일반적으로, 항상 모든 추적 레코드를 충분히 저장할 수 있을 만큼 *크게* 버퍼 *크기*를 정의하십시오. 추적이 랩되면 중요한 추적 정보를 손실할 수 있습니다. 매우 간헐적으로 문제점이 발생하는 경우에는 버퍼 랩이 중요한 정보를 삭제하지 못하도록 추적 버퍼를 *크게* 정의하십시오.

USRDTA(추적할 사용자 바이트 수)
자료 프레임의 사용자 자료 부분에 추적될 자료 수를 정의하십시오. 디폴트 값으로, 사용자 자료의 최초 100바이트만 LAN 인터페이스에 대해 캡처됩니다. 기타 모든 인터페이스의 경우에는 모든 사용자 자료가 캡처됩니다. 프레임의 사용자 자료에서 문제점이 예상되는 경우에는 *MAX를 지정해야 합니다.

TEXT(추적 설명)
추적에 대한 의미있는 설명을 제공합니다.

통신 추적 중단

별도로 지정된 경우를 제외하고, 추적은 대개 추적 중인 조건이 발생하자 마자 중단됩니다. 추적을 중단하려면 ENDCMNTRC(통신 추적 끝) 명령을 사용하십시오. 다음 명령은 ENDCMNTRC 명령의 예입니다.

```
ENDCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN)
```

명령에는 다음과 같이 두 개의 매개변수가 있습니다.

CFGOBJ(구성 오브젝트)
추적이 실행될 구성 오브젝트의 이름. 오브젝트는 회선 설명, 네트워크 인터페이스 설명 또는 네트워크 서버 설명 중 하나입니다.

CFGTYPE(구성 유형)
회선(*LIN), 네트워크 인터페이스(*NWI) 또는 네트워크 서버(*NWS)가 추적되고 있는지 여부.

추적 자료 인쇄

통신 추적을 중단한 후에는 추적 자료를 인쇄해야 합니다. 이 타스크를 수행하려면 PRTCMNTRC(통신 추적 인쇄) 명령을 사용하십시오. 추적 기간 동안에는 모든 회선 통신량이 캡쳐되기 때문에, 출력 생성을 위해 복수 필터 옵션이 제공됩니다. 스풀 파일을 기능한 한 작게 보유하십시오. 그러면 분석이 더욱 빨라지고 효율적으로 수행됩니다. VPN 문제점의 경우, IP 통신에서만 필터링하고 가능하면 특정 IP 주소에서 필터링해야 합니다. 특정 IP 포트 수에서 필터링하는 옵션도 제공됩니다. 다음은 PRTCMNTRC 명령의 예입니다.

```
PRTCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN) FMTTCP(*YES) TCPIPADR('10.50.21.1)
    SLTPORT(500) FMTBCD(*NO)
```

이 예에서, 추적은 IP 통신량에 대해 형식화되고 IP 주소에 대한 자료만 포함합니다. 여기서, 소스 또는 목적지 주소는 10.50.21.1이며 소스 또는 목적지 IP 포트 번호는 500입니다.

VPN 문제점 분석을 위한 가장 중요한 명령 매개변수에 대해서는 아래에 설명합니다.

CFGOBJ(구성 오브젝트)
추적이 실행될 구성 오브젝트의 이름. 오브젝트는 회선 설명, 네트워크 인터페이스 설명 또는 네트워크 서버 설명 중 하나입니다.

CFGTYPE(구성 유형)
회선(*LIN), 네트워크 인터페이스(*NWI) 또는 네트워크 서버(*NWS)가 추적되고 있는지 여부.

FMTTCP(TCP/IP 자료 형식화)
TCP/IP 및 UDP/IP 자료에 대해 추적을 형식화할 것인지의 여부. 추적을 IP 자료에 대해 형식화하려면 *YES를 지정하십시오.

TCPIPADR(주소별로 TCP/IP 자료 형식화)
이 매개변수는 두 가지 요소로 구성됩니다. 두 가지 요소 모두에 IP 주소를 지정하면 해당 주소 사이의 IP 통신량만 인쇄됩니다.

SLTPORT(IP 포트 번호)
필터링할 IP 포트 번호.

FMTBCD(브로드캐스트 자료 형식화)
모든 브로드캐스트 프레임을 인쇄할 것인지의 여부. 디폴트 값은 예입니다. 예를 들어, ARP(Address Resolution Protocol) 요구를 인쇄하지 않을 경우에는 *NO를 지정하십시오. 그렇지 않으면, 브로드캐스트 메세지가 불필요하게 인쇄될 수 있습니다.

VPN에 대한 관련 정보

자세한 VPN 구성 시나리오 및 설명을 보려면, 다음 기타 정보 소스를 참조하십시오.

- **OS/400 V5R1 Virtual Private Networks: Remote Access to the IBM e(logo)server iSeries Server with Windows 2000 VPN Clients, REDP0153**
  이 IBM Redpaper는 V5R1 VPN과 Windows 2000 원시(native) L2TP 및 IPSec 지원을 사용하여 VPN 터널을 구성하는 단계별 프로세스를 제공합니다.

- **AS/400 Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00**
  이 레드북은 VPN 개념을 설명하고, IP 보안(IPSec) 및 L2TP(Layer 2 Tunneling Protocol)를 사용하여 OS/400에서 VPN을 구현하는 방법을 설명합니다.

- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00**
  이 레드북에서는 AS/400 시스템에서 사용할 수 있는 모든 고유 네트워크 보안 피처(예: IP 필터, NAT, VPN, HTTP 프록시 서버, SSL, DNS, 메일 릴레이, 감사 및 기록 등)를 설명합니다. 실제 사용 예를 통해 설명합니다.

- **Virtual Private Networking: Securing Connections**
  이 웹 페이지에서는 최신 VPN 소식을 중점적으로 소개하고, 최신 PTF를 나열하며, 다른 관심 사이트로 링크를 제공합니다.

- **기타 보안 관련 매뉴얼 및 레드북**
  여기서는 온라인으로 사용할 수 있는 보안 관련 정보 리스트를 볼 수 있습니다.

워크스테이션에 PDF를 저장하려면 다음을 수행하십시오.

1. 브라우저에서 PDF를 마우스 오른쪽 버튼으로 클릭하십시오(위의 링크를 마우스 오른쪽 버튼으로 클릭).
2. **다른 이름으로 목표 저장...**을 클릭하십시오.
3. PDF를 저장할 디렉토리를 찾아 이동하십시오.
4. **저장**을 클릭하십시오.

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