Cisco VPN 5000 Concentrator 구성 및 IPSec 기본 모드 LAN-to-LAN VPN 연결 구현

목차

소개

이 문서에서는 Cisco VPN 5000 Concentrator의 초기 컨피그레이션에 대해 설명하고 IP를 사용하여 네트워크에 연결하는 방법과 IPSec 기본 모드 LAN-to-LAN VPN 연결을 제공하는 방법을 설명합니다.

방화벽과 관련하여 네트워크에 연결하는 위치에 따라 두 가지 컨피그레이션 중 하나로 VPN Concentrator를 설치할 수 있습니다. VPN Concentrator에는 2개의 이더넷 포트가 있으며, 그중 하나는(이더넷 1)에서만 IPSec 트래픽을 전달합니다. 다른 포트(이더넷 0)는 모든 IP 트래픽을 라우팅합니다. 방화벽과 함께 VPN Concentrator를 설치하려는 경우 이더넷 0이 보호된 LAN을 향하고 이더넷 1이 네트워크의 인터넷 게이트웨이 라우터를 통해 인터넷에 연결되도록 두 포트를 모두 사용해야 합니다. 또한 보호된 LAN의 방화벽 뒤에 VPN Concentrator를 설치하고 이더넷 0 포트를 통해 연결할 수 있으므로 인터넷과 Concentrator 간에 전달되는 IPSec 트래픽이 방화벽을 통과하도록 할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco VPN 5000 Concentrator를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 라이브 네트워크에서 작업하는 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

기본 연결 구성

기본 네트워크 연결을 설정하는 가장 쉬운 방법은 직렬 케이블을 VPN Concentrator의 콘솔 포트에 연결하고 터미널 소프트웨어를 사용하여 이더넷 0 포트에서 IP 주소를 구성하는 것입니다. 이더넷 0 포트에서 IP 주소를 구성한 후 텔넷을 사용하여 VPN Concentrator에 연결하여 컨피그레이션을 완료할 수 있습니다. 적절한 텍스트 편집기에서 컨피그레이션 파일을 생성하고 TFTP를 사용하여 VPN Concentrator로 전송할 수도 있습니다.

콘솔 포트를 통해 터미널 소프트웨어를 사용하면 처음에 비밀번호를 입력하라는 프롬프트가 표시됩니다. "letmein" 비밀번호를 사용합니다. 비밀번호로 응답한 후 **configure ip ethernet 0** 명령을 실행하여 시스템 정보로 프롬프트에 응답합니다. 프롬프트 순서는 다음 예와 같아야 합니다.

```
*[ IP Ethernet 0 ]# configure ip ethernet 0
      Section 'ip ethernet 0' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IP Ethernet 0 ]# ipaddress=192.168.233.1
      *[ IP Ethernet 0 ]# subnetmask=255.255.255.0
      *[ IP Ethernet 0 ]# ipbroadcast=192.168.233.255
      *[ IP Ethernet 0 ]# mode=routed
      *[ IP Ethernet 0 ]#
```

이제 이더넷 1 포트를 구성할 준비가 되었습니다.

이더넷 1 포트 구성

이더넷 1 포트의 TCP/IP 주소 지정 정보는 VPN Concentrator에 대해 할당한 외부 인터넷 라우팅 가능 TCP/IP 주소입니다. 이더넷 0과 동일한 TCP/IP 네트워크에서 주소를 사용하지 마십시오. 이렇게 하면 집중기에서 TCP/IP가 비활성화됩니다.

시스템 정보로 프롬프트에 **응답하여 configure ip ethernet 1** 명령을 입력합니다. 프롬프트 순서는 다음 예와 같아야 합니다.

```
*[ IP Ethernet 0 ]# configure ip ethernet 1
      Section 'ip ethernet 1' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IP Ethernet 1 ]# ipaddress=206.45.55.1
      *[ IP Ethernet 1 ]# subnetmask=255.255.255.0
      *[ IP Ethernet 1 ]# ipbroadcast=206.45.55.255
      *[ IP Ethernet 1 ]# mode=routed
```

```
      *[ IP Ethernet 1 ]#
```
이제 IPSec 게이트웨이를 구성해야 합니다.

IPSec 게이트웨이 구성

IPSec 게이트웨이는 VPN Concentrator가 모든 IPSec 또는 터널링된 트래픽을 전송하는 위치를 제어합니다. 이는 나중에 구성하는 기본 경로와 독립적입니다. 먼저 configure **general** 명령을 입력하여 시스템 정보로 프롬프트에 응답합니다. 프롬프트 순서는 아래 예와 같아야 합니다.

```
* IntraPort2+_A56CB700# configure general
      Section 'general' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
       =
      To find a list of valid keywords and additional help enter "?"
      *[ General ]# ipsecgateway=206.45.55.2
      *[ General ]# exit
      Leaving section editor.
      * IntraPort2+_A56CB700#
```
참고: 릴리스 6.x 이상에서 **ipsecgateway** 명령이 vpngateway 명령으로 **변경되었습니다**.

이제 IKE(Internet Key Exchange) 정책을 구성합니다.

IKE 정책 구성

ISAKMP(Internet Security Association Key Management Protocol)/IKE 매개변수는 VPN Concentrator와 클라이언트가 터널 세션을 설정하기 위해 서로를 식별하고 인증하는 방법을 제어합니다. 이 초기 협상을 1단계라고 합니다. 1단계 매개변수는 디바이스에 대해 전역적이며 특정 인터페이스와 연결되지 않습니다. 이 섹션에서 인식되는 키워드는 아래에 설명되어 있습니다. LAN-to-LAN 터널에 대한 1단계 협상 매개변수는 [Tunnel Partner <Section ID>] 섹션에서 설정할 수 있습니다. 2단계 IKE 협상은 VPN Concentrator 및 VPN 클라이언트가 개별 터널 세션을 처리하는 방법을 제어합니다. VPN Concentrator 및 VPN 클라이언트에 대한 2단계 IKE 협상 매개변수는 [VPN Group <Name>] 디바이스에서 설정됩니다.

IKE 정책의 구문은 다음과 같습니다.

```
Protection = [ MD5_DES_G1 | MD5_DES_G2 | SHA_DES_G1 | SHA_DES_G2 ]
```
protection 키워드는 VPN Concentrator와 VPN 클라이언트 간의 ISAKMP/IKE 협상을 위한 보호 제품군을 지정합니다. 이 키워드는 이 섹션 내에서 여러 번 나타날 수 있습니다. 이 경우 VPN Concentrator는 지정된 모든 보호 모음을 제안합니다. VPN 클라이언트는 협상 옵션 중 하나를 수락합니다. 각 옵션의 첫 번째 부분인 MD5(Message Digest 5)는 협상에 사용되는 인증 알고리즘입니다. SHA는 MD5보다 더 안전한 것으로 간주되는 Secure Hash Algorithm을 의미합니다. 각 옵션의 두 번째 부분은 암호화 알고리즘입니다. DES(Data Encryption Standard)는 56비트 키를 사용하여 데이터를 스크램블합니다. 각 옵션의 세 번째 부분은 키 교환에 사용되는 Diffie-Hellman 그룹입니다. 그룹 2(G2) 알고리즘에서 더 큰 숫자를 사용하므로 그룹 1(G1)보다 안전합니다.

컨피그레이션을 시작하려면 **configure IKE policy** 명령을 입력하여 시스템 정보와 함께 프롬프트에 응답합니다. 다음은 예입니다.

```
* IntraPort2+_A56CB700# configure IKE Policy
      Section 'IKE Policy' was not found in the config.
```

```
Do you want to add it to the config? y
Configure parameters in this section by entering:
<Keyword> = <Value>
To find a list of valid keywords and additional help enter "?"
*[ IKE Policy ] Protection = MD5_DES_G1
*[ IKE Policy ] exit
Leaving section editor.
* IntraPort2+_A56CB700#
```

기본 사항을 구성했으므로 이제 터널 및 IP 통신 매개변수를 정의할 때입니다.

주 모드 사이트 대 사이트 구성

LAN-to-LAN 연결을 지원하도록 VPN Concentrator를 구성하려면 터널에서 사용할 IP 통신 매개변수와 터널 컨피그레이션을 정의해야 합니다. 이 작업은 [Tunnel Partner VPN x] 섹션과 [IP VPN x] 섹션이라는 두 섹션으로 구성됩니다. 지정된 Site-to-Site 컨피그레이션의 경우 이 두 섹션에 정의된 *x*가 일치해야 터널 컨피그레이션이 프로토콜 컨피그레이션과 올바르게 연결됩니다.

각 섹션을 자세히 살펴보겠습니다.

터널 파트너 섹션 구성

터널 파트너 섹션에서 다음 8개 이상의 매개변수를 정의해야 합니다.

- 변형
- 파트너
- 키 관리
- 공유 키
- 모드로 들어갑니다
- 로컬 액세스
- 피어
- 바인딩 대상

변형

Transform 키워드는 IKE 클라이언트 세션에 사용되는 보호 유형 및 알고리즘을 지정합니다. 이 매개변수와 연결된 각 옵션은 인증 및 암호화 매개변수를 지정하는 보호 부분입니다. Transform 매개변수는 이 섹션 내에 여러 번 나타날 수 있습니다. 이 경우 VPN Concentrator는 세션 중에 사용할 수 있도록 클라이언트가 허용할 때까지 지정된 보호 요소를 구문 분석된 순서대로 제안합니다. 대부분의 경우 Transform 키워드는 하나만 필요합니다.

Transform 키워드에 대한 옵션은 다음과 같습니다.

```
[ ESP(SHA,DES) | ESP(SHA,3DES) | ESP(MD5,DES) | ESP(MD5,3DES) | ESP(MD5) |
ESP(SHA) | AH(MD5) | AH(SHA) |AH(MD5)+ESP(DES) | AH(MD5)+ESP(3DES) |
AH(SHA)+ESP(DES) | AH(SHA)+ESP(3DES) ]
```

ESP는 Encapsulating Security Payload를 의미하며 AH는 Authentication Header를 의미합니다. 이 두 헤더 모두 패킷을 암호화하고 인증하는 데 사용됩니다. DES(Data Encryption Standard)는 56비트 키를 사용하여 데이터를 스크램블합니다. 3DES는 DES 알고리즘의 세 가지 키 및 세 가지 애플리케이션을 사용하여 데이터를 스크램블합니다. MD5는 message-digest 5 해시 알고리즘입니다. SHA는 MD5보다 다소 더 안전한 것으로 간주되는 보안 해시 알고리즘입니다.

ESP(MD5,DES)가 기본 설정이며 대부분의 설정에 권장됩니다. ESP(MD5) 및 ESP(SHA)는 ESP를 사용하여 패킷(암호화 없음)을 인증합니다. AH(MD5) 및 AH(SHA)는 AH를 사용하여 패킷을 인증합니다. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES) 및 AH(SHA)+ESP(3DES)는 AH를 사용하여 패킷을 인증하고 ESP를 사용하여 패킷을 암호화합니다.

파트너

Partner 키워드는 터널 파트너십에서 다른 터널 종료자의 IP 주소를 정의합니다. 이 번호는 로컬 VPN Concentrator가 IPSec 연결을 생성할 수 있는 라우팅 가능한 공용 IP 주소여야 합니다.

키 관리

KeyManage 키워드는 터널 파트너십의 두 VPN Concentrator가 터널을 시작하는 디바이스와 따라야 할 터널 설정 절차의 유형을 결정하는 방법을 정의합니다. 옵션은 Auto, Initiate, Respond, Manual입니다. 처음 세 가지 옵션을 사용하여 IKE 터널을 구성하고 Manual 키워드를 사용하여 고정 암호화 터널을 구성할 수 있습니다. 이 문서에서는 고정 암호화 터널을 구성하는 방법을 다루지 않습니다. Auto는 터널 파트너가 터널 설정 요청을 시작하고 응답할 수 있도록 지정합니다. Initiate는 터널 파트너가 터널 설정 요청만 전송하고 응답하지 않도록 지정합니다. Respond(응답)는 터널 파트너가 터널 설정 요청에 응답하도록 지정하지만, 이를 시작하지 않도록 지정합니다.

공유 키

SharedKey 키워드는 IKE 공유 암호로 사용됩니다. 두 터널 파트너에서 동일한 SharedKey 값을 설정해야 합니다.

모드로 들어갑니다

Mode 키워드는 IKE 협상 프로토콜을 정의합니다. 기본 설정은 Aggressive이므로 상호 운용성 모드에 대해 VPN Concentrator를 설정하려면 Mode 키워드를 Main으로 설정해야 합니다.

로컬 액세스

LocalAccess는 호스트 마스크부터 기본 경로까지 터널을 통해 액세스할 수 있는 IP 번호를 정의합니다. LocalProto 키워드는 터널을 통해 액세스할 수 있는 IP 프로토콜 번호(예: ICMP(1), TCP(6), UDP(17) 등)를 정의합니다. 모든 IP 번호를 전달하려면 LocalProto=0을 설정해야 합니다. LocalPort는 터널을 통해 연결할 수 있는 포트 번호를 결정합니다. LocalProto와 LocalPort는 모두 기본적으로 0 또는 all-access입니다.

피어

Peer 키워드는 터널을 통해 찾을 서브넷을 지정합니다. PeerProto는 원격 터널 엔드포인트를 통해 허용되는 프로토콜을 지정하며, PeerPort는 터널의 다른 끝에서 액세스할 수 있는 포트 번호를 설정합니다.

바인딩 대상

BindTo는 사이트 간 연결을 종료하는 이더넷 포트를 지정합니다. VPN Concentrator가 단일 포트 모드에서 실행되는 경우를 제외하고 항상 이 매개변수를 이더넷 1로 설정해야 합니다.

매개변수 구성

이러한 매개변수를 구성하려면 **configure Tunnel Partner VPN 1** 명령을 입력하여 시스템 정보로 프롬프트에 응답합니다.

프롬프트 순서는 아래 예와 같아야 합니다.

```
*IntraPort2+_A56CB700# configure Tunnel Partner VPN 1
      Section ?config Tunnel Partner VPN 1? not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
       =
      To find a list of valid keywords and additional help enter "?"
      *[ Tunnel Partner VPN 1 ]# transform=ESP(MD5,DES)
      *[ Tunnel Partner VPN 1 ]# sharedkey=letmein
      *[ Tunnel Partner VPN 1 ]# partner=208.203.136.10
      *[ Tunnel Partner VPN 1 ]# mode=main
      *[ Tunnel Partner VPN 1 ]# peer=10.0.0.0/8
      *[ Tunnel Partner VPN 1 ]# localaccess=192.168.233.0/24
      *[ Tunnel Partner VPN 1 ]# bindto=Ethernet 1
      *[ Tunnel Partner VPN 1 ]# exit
      Leaving section editor.
```

이제 IP 섹션을 구성해야 합니다.

IP 섹션 구성

각 터널 파트너십의 IP 컨피그레이션 섹션에서 번호 또는 번호가 지정되지 않은 연결(WAN 연결의 IP 컨피그레이션)을 사용할 수 있습니다. 여기서는 번호가 없는 것을 사용했습니다.

번호가 지정되지 않은 Site-to-Site 연결에 대한 최소 컨피그레이션에는 두 개의 문이 필요합니다. number=false 및 mode=routed. configure **ip vpn 1** 명령을 입력하고 다음과 같이 시스템 프롬프트에 응답합니다.

```
*[ IP Ethernet 0 ]# configure ip vpn 1
      Section ?IP VPN 1? not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IP VPN 1 ]# mode=routed
      *[ IP VPN 1 ]# numbered=false
```

이제 기본 경로를 설정할 때입니다.

기본 경로 구성(TCP/IP 경로 테이블)

VPN Concentrator가 직접 연결된 네트워크 또는 동적 경로가 있는 네트워크 이외의 네트워크로 향하는 모든 TCP/IP 트래픽을 전송하는 데 사용할 수 있는 기본 경로를 구성해야 합니다. 기본 경로는 내부 포트에 있는 모든 네트워크로 다시 연결됩니다. 이미 IPSec Gateway 매개 변수를 사용하여 인터넷을 오가는 IPSec 트래픽을 전송하도록 Introport를 구성했습니다. 기본 경로 컨피그레이션을 시작하려면 시스템 정보로 프롬프트에 응답하여 edit config ip static 명령을 입력합니다. 프롬프트 순서는 아래 예와 같아야 합니다.

```
*IntraPort2+_A56CB700# edit config ip static
      Section 'ip static' not found in the config.
      Do you want to add it to the config? y
      Configuration lines in this section have the following format:
      <Destination> <Mask> <Gateway> <Metric> [<Redist=(RIP|none)>]
      Editing "[ IP Static ]"...
      1: [ IP Static ]
      End of buffer
      Edit [ IP Static ]> append 1
      Enter lines at the prompt. To terminate input, enter
      a . on a line all by itself.
      Append> 0.0.0.0 0.0.0.0 192.168.233.2 1
      Append> .
      Edit [ IP Static ]> exit
      Saving section...
      Checking syntax...
      Section checked successfully.
      *IntraPort2+_A56CB700#
```

마무리

마지막 단계는 컨피그레이션을 저장하는 것입니다. 컨피그레이션을 다운로드하고 디바이스를 다시 시작할지 묻는 메시지가 나타나면 **y**를 입력하고 Enter를 **누릅니다**. 부팅 과정에서 VPN Concentrator를 끄지 마십시오. Concentrator가 재부팅되면 사용자는 Concentrator의 VPN Client 소프트웨어를 사용하여 연결할 수 있습니다.

컨피그레이션을 저장하려면 **save** 명령을 다음과 같이 입력합니다.

```
*IntraPort2+_A56CB700# save
      Save configuration to flash and restart device? y
```

텔넷을 사용하여 VPN Concentrator에 연결된 경우 위의 출력만 볼 수 있습니다. 콘솔을 통해 연결된 경우 다음과 유사한 출력이 더 오래 표시됩니다. 이 출력이 끝나면 VPN Concentrator는 "Hello Console.."을 반환합니다. 암호를 요청합니다. 이게 네가 끝난거야

```
Codesize => 0 pfree => 462
      Updating Config variables...
      Adding section '[ General ]' to config
      Adding -- ConfiguredFrom = Command Line, from Console
      Adding -- ConfiguredOn = Timeserver not configured
      Adding -- DeviceType = IntraPort2
      Adding -- SoftwareVersion = IntraPort2 V4.5
      Adding -- EthernetAddress = 00:00:a5:6c:b7:00
      Not starting command loop: restart in progress.
      Rewriting Flash....
```

관련 정보

- Cisco VPN 5000 Series Concentrator 판매 중단 발표
- Cisco VPN 5000 Concentrator 지원 페이지
- Cisco VPN 5000 클라이언트 지원 페이지
- IPsec 지원 페이지
- 기술 지원 및 문서 – Cisco Systems