# 초기 및 원격 클라이언트 액세스를 위한 Cisco VPN 5000 Concentrator 설정

## 목차



## 소개

이 설명서에서는 Cisco VPN 5000 Concentrator의 초기 컨피그레이션, 특히 IP를 사용하여 네트워크에 연결하고 원격 클라이언트 연결을 제공하도록 구성하는 방법에 대해 설명합니다.

방화벽과 관련하여 네트워크에 연결하는 위치에 따라 두 가지 컨피그레이션 중 하나로 Concentrator를 설치할 수 있습니다.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 보호되는 LAN의 방화벽 뒤에 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.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

### 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 Concentrator의 콘솔 포트에 연결하고 터미널 소프트웨어를 사용하여 Ethernet 0 포트에서 IP 주소를 구성하는 것입니다.이더넷 0 포트에서 IP 주소를 구성한 후 텔넷을 사용하여 Concentrator에 연결하여 컨피그레이션을 완료할 수 있습니다.적절한 텍스트 편집기에서 컨피그레이션 파일을 생성하여 TFTP를 사용하여 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 다음과 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

이더넷 1 포트의 TCP/IP 주소 지정 정보는 Concentrator에 할당한 외부 인터넷 라우팅 가능 TCP/IP 주소입니다.VPN Concentrator에서 TCP/IP를 비활성화하므로 이더넷 0과 동일한 TCP/IP 네트워크에서 주소를 사용하지 마십시오.

시스템 정보로 프롬프트에 **응답하여 configure ip ethernet 1** 명령을 입력합니다.프롬프트 순서는 다음과 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 기본 경로를 구성해야 합니다.

## 기본 경로

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.나중에 IPSec Gateway 매개 변수를 사용하여 인터넷을 오가는 IPSec 트래픽을 전송하도록 인터포트를 구성합니다.기본 경로 컨피그레이션을 시작하려면 시스템 정보로 프롬프트에 응답하여 edit config ip static 명령을 입력합니다.프롬프트 순서는 다음과 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#
```

이제 IPSec 게이트웨이를 구성해야 합니다.

## IPSec 게이트웨이

IPSec 게이트웨이는 집중기가 모든 IPSec 또는 터널링된 트래픽을 전송하는 위치를 제어합니다.이는 방금 구성한 기본 경로와 독립적입니다.먼저 configure **general** 명령을 입력하여 시스템 정보로 프롬프트에 응답합니다.프롬프트 순서는 다음과 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#
```

다음으로, IKE 정책을 구성합니다.

# IKE 정책

집중장치에 대한 ISAKMP/IKE(Internet Security Association Key Management Protocol/Internet

Key Exchange) 매개변수를 설정합니다.이러한 설정은 Concentrator와 클라이언트가 터널 세션을 설정하기 위해 상호 식별 및 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 클라이언트가 개별 터널 세션을 처리하는 방법을 제어합니다.VPN Concentrator 및 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 클라이언트 간의 ISAKMP/IKE 협상을 위한 보호 제품군을 지정합니다.이 키워드는 이 섹션 내에서 여러 번 나타날 수 있으며, 이 경우 Concentrator는 지정된 모든 보호 모음을 제안합니다.클라이언트는 협상에 대한 옵션 중 하나를 수락합니다.각 옵션의 첫 번째 부분인 MD-5(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.

```
* 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 그룹 매개변수를 입력합니다.

# VPN 그룹 컨피그레이션

그룹 매개변수를 입력할 때 명령줄 파서를 통해 VPN 그룹 이름에 공백을 입력할 수 있지만 VPN 그룹 이름에는 공백을 포함할 수 없습니다.VPN 그룹 이름은 문자, 숫자, 대시 및 밑줄을 포함할 수 있습니다.

IP 작업을 위해 각 VPN 그룹에 필요한 4가지 기본 매개변수가 있습니다.

- 최대 연결 수
- StartIPaddress 또는 LocalIPNet
- 변형
- IPNet

Maxconnections 매개변수는 이 특정 VPN 그룹 컨피그레이션에서 허용되는 최대 동시 클라이언트 세션 수입니다.이 번호는 StartIPAddress 또는 LocalIPNet 매개 변수와 함께 작동하므로 주의하십

시오.

VPN Concentrator는 두 가지 다른 구성인 StartIPAddress 및 LocalIPNet에 의해 원격 클라이언트에 IP 주소를 할당합니다.StartIPAddress는 이더넷 0에 연결된 서브넷에서 IP 번호를 할당하고, 연결된 클라이언트에 대해 프록시-arps를 할당합니다.LocalIPNet은 VPN 클라이언트에 고유한 서브넷에서 원격 클라이언트에 IP 번호를 할당하며, 네트워크의 나머지 부분에서는 정적 또는 동적 라우팅을 통해 VPN 서브넷의 존재를 인식해야 합니다.StartIPAddress는 더 쉬운 구성을 제공하지만 주소 공간의 크기를 제한할 수 있습니다.LocalIPNet은 원격 사용자를 위한 주소 지정의 유연성을 높이지만, 필요한 라우팅을 구성하려면 약간 더 많은 작업이 필요합니다.

StartIPAddress의 경우 수신 클라이언트 터널 세션에 할당된 첫 번째 IP 주소를 사용합니다.기본 컨피그레이션 설정에서는 내부 TCP/IP 네트워크의 IP 주소(이더넷 0 포트와 동일한 네트워크)여야 합니다. 아래 예에서는 첫 번째 클라이언트 세션에 192.168.233.50 주소, 다음 동시 클라이언트 세션 192.168.233.51이 할당됩니다.Maxconnections 값 30을 할당했습니다. 즉, 192.168.233.50부터 시작하여 192.168.233.79으로 끝나는 30개의 미사용 IP 주소(있는 경우 DHCP 서버 포함)로 구성된 블록이 있어야 합니다. 다른 VPN 그룹 구성에서 사용되는 IP 주소가 중복되지 않도록 하십시오.

LocalIPNet은 LAN의 다른 위치에서 사용되지 않아야 하는 서브넷에서 원격 클라이언트에 IP 주소를 할당합니다.예를 들어, VPN 그룹 구성에서 "LocalIPNet=182.168.1.0/24" 매개변수를 지정하면 Concentrator는 192.168.1.1으로 시작하는 클라이언트에 IP 주소를 할당합니다. 따라서 LocalIPNet을 사용하여 IP 번호를 할당할 때 Concentrator가 서브넷 경계를 고려하지 않으므로 "Maxconnections=254"를 할당해야 합니다.

Transform 키워드는 Concentrator가 IKE 클라이언트 세션에 사용하는 보호 유형 및 알고리즘을 지정합니다.옵션은 다음과 같습니다.

```
Transform = [ 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) ]
```

각 옵션은 인증 및 암호화 매개변수를 지정하는 보호 부분입니다.이 키워드는 이 섹션 내에서 여러 번 나타날 수 있습니다. 이 경우 Concentrator는 세션 중에 사용할 수 있도록 클라이언트가 허용할 때까지 지정된 보호 요소를 구문 분석된 순서대로 제안합니다.대부분의 경우 Transform 키워드는 하나만 필요합니다.

ESP(SHA,DES), ESP(SHA,3DES), ESP(MD5,DES) 및 ESP(MD5,3DES)는 패킷을 암호화하고 인증하는 ESP(Encapsulating Security Payload) 헤더를 나타냅니다.DES(Data Encryption Standard)는 56비트 키를 사용하여 데이터를 스크램블합니다.3DES는 DES 알고리즘의 세 가지 키 및 세 가지 애플리케이션을 사용하여 데이터를 스크램블합니다.MD5는 메시지 다이제스트 5 해시 알고리즘이며 SHA는 MD5보다 다소 더 안전한 것으로 간주되는 보안 해시 알고리즘입니다.

ESP(MD5,DES)가 기본 설정이며 대부분의 설치에 권장됩니다.ESP(MD5) 및 ESP(SHA)는 ESP 헤더를 사용하여 암호화 없이 패킷을 인증합니다.AH(MD5) 및 AH(SHA)는 AH(Authentication Header)를 사용하여 패킷을 인증합니다.AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES) 및 AH(SHA)+ESP(3DES)는 인증 헤더를 사용하여 패킷을 인증하고 ESP 헤더를 사용하여 패킷을 암호화합니다.

**참고:** Mac OS 클라이언트 소프트웨어는 AH 옵션을 지원하지 않습니다.Mac OS 클라이언트 소프트웨어를 사용하는 경우 하나 이상의 ESP 옵션을 지정해야 합니다.

IPNet 필드는 Concentrator 클라이언트가 이동할 수 있는 위치를 제어하므로 중요합니다.이 필드에 입력하는 값은 터널링되는 TCP/IP 트래픽 또는 일반적으로 이 VPN 그룹에 속한 클라이언트가 네트워크에서 이동할 수 있는 경로를 결정합니다.

내부 네트워크(이 예에서는 192.168.233.0/24)을 구성하는 것이 좋습니다. 따라서 내부 네트워크로 가는 클라이언트의 모든 트래픽이 터널을 통해 전송되므로, 암호화를 활성화한 경우 인증되고 암호화됩니다. 이 시나리오에서는 다른 트래픽이 터널링되지 않습니다.대신 정상적으로 라우팅됩니다 .단일 또는 호스트 주소를 포함하여 여러 항목을 가질 수 있습니다.형식은 주소(예: 네트워크 주소 192.168.233.0)과 해당 주소와 연결된 마스크(비트)(/24(클래스 C 마스크)입니다.

configure VPN group basic-user 명령을 입력하여 컨피그레이션의 이 부분을 시작한 다음 시스템 정보로 프롬프트에 응답합니다.다음은 전체 컨피그레이션 시퀀스의 예입니다.

```
*IntraPort2+_A56CB700# configure VPN group basic-user
      Section 'VPN Group basic-user' 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 "?"
      *[ VPN Group "basic-user" ]# startipaddress=192.168.233.50
                                   or
      *[ VPN Group "basic-user" ]# localipnet=192.168.234.0/24
      *[ VPN Group "basic-user" ]# maxconnections=30
      *[ VPN Group "basic-user" ]# Transform=ESP(SHA,DES)
      *[ VPN Group "basic-user" ]# ipnet=192.168.233.0/24
      *[ VPN Group "basic-user" ]# exit
      Leaving section editor.
      *IntraPort2_A51EB700#
```

다음 단계는 사용자의 데이터베이스를 정의하는 것입니다.

# VPN 사용자 구성

컨피그레이션의 이 섹션에서는 VPN 사용자 데이터베이스를 정의합니다.각 행은 해당 사용자의 VPN 그룹 컨피그레이션 및 비밀번호와 함께 VPN 사용자를 정의합니다.다중 행 항목에는 백슬래시로 끝나는 줄 바꿈이 있어야 합니다.그러나 큰따옴표로 묶은 줄 바꿈을 유지합니다.

VPN 클라이언트가 터널 세션을 시작하면 클라이언트의 사용자 이름이 디바이스에 전송됩니다.디바이스가 이 섹션에서 사용자를 찾으면 항목의 정보를 사용하여 터널을 설정합니다.(VPN 사용자 인증에 RADIUS 서버를 사용할 수도 있습니다.) 디바이스에서 사용자 이름을 찾지 못하고 인증을 수행하도록 RADIUS 서버를 구성하지 않은 경우 터널 세션이 열리지 않고 오류가 클라이언트에 반환됩니다.

edit config VPN users 명령을 입력하여 컨피그레이션을 시작합니다."User1"이라는 사용자를 VPN 그룹 "basic-user"에 추가하는 예를 살펴보겠습니다.

```
*IntraPort2+_A56CB700# edit config VPN users
      Section 'VPN users' not found in the config.
      Do you want to add it to the config? y
      <Name> <Config> <SharedKey>
      Editing "[ VPN Users ]"...
      1: [ VPN Users ]
      End of buffer
      Edit [ VPN Users ]> append 1
      Enter lines at the prompt. To terminate input, enter
      a . on a line all by itself.
      Append> User1 Config="basic-user" SharedKey="Burnt"
      Append> .
      Edit [ VPN Users ]> exit
      Saving section...
```

```
      Checking syntax...
      Section checked successfully.
      *IntraPort2+_A56CB700#
```

이 사용자의 SharedKey는 "Burned"입니다. 이러한 모든 컨피그레이션 값은 대/소문자를 구분합니다."User1"을 구성하는 경우 사용자는 클라이언트 소프트웨어에 "User1"을 입력해야 합니다."user1"을 입력하면 유효하지 않거나 권한이 없는 사용자 오류 메시지가 표시됩니다.편집기를 종료하는 대신 사용자를 계속 입력할 수 있지만 편집기를 종료하려면 기간을 입력해야 합니다.이렇게 하지 않으면 컨피그레이션에 잘못된 항목이 발생할 수 있습니다.

# 마무리

마지막 단계는 컨피그레이션을 저장하는 것입니다.컨피그레이션을 다운로드하고 디바이스를 다시 시작할지 묻는 메시지가 나타나면 y를 입력하고 Enter 키를 누릅니다.부팅 과정에서 집중 장치를 끄지 마십시오.Concentrator가 재부팅되면 사용자는 Concentrator 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 Concentrator에 연결된 경우 위의 출력만 볼 수 있습니다.콘솔을 통해 연결된 경우 다음과 유사한 출력이 더 오래 표시됩니다.이 출력이 끝나면 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