Cisco VPN 3000 Concentrator 및 Network Associates PGP 클라이언트 구성

목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>표기 규칙</u> <u>Cisco VPN 3000 Concentrator에 연결하도록 Network Associates PGP 클라이언트 구성</u> <u>Network Associates PGP 클라이언트의 연결을 허용하도록 Cisco VPN 3000 Concentrator 구성</u> <u>관련 정보</u>

<u>소개</u>

이 문서에서는 버전 6.5.1을 실행하는 Cisco VPN 3000 Concentrator 및 PGP(Network Associates Pretty Good Privacy) Client를 모두 구성하여 서로 연결하는 방법을 설명합니다.

<u>사전 요구 사항</u>

<u>요구 사항</u>

이 문서에 대한 특정 요건이 없습니다.

<u>사용되는 구성 요소</u>

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

• Cisco VPN 3000 Concentrator 버전 4.7

• Networks Associates PGP Client 버전 6.5.1

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

<u>표기 규칙</u>

문서 규칙에 대한 자세한 내용은 <u>Cisco 기술 팁 표기 규칙</u>을 참조하십시오.

<u>Cisco VPN 3000 Concentrator에 연결하도록 Network Associates</u> <u>PGP 클라이언트 구성</u>

이 절차를 사용하여 Network Associates PGP Client가 VPN 3000 Concentrator에 연결하도록 구성 합니다.

- 1. PGPNet > Hosts를 시작합니다.
- 2. Add(**추가**)를 클릭한 다음 **Next(다음)**를 클릭합니다.
- 3. Gateway(게이트웨이) 옵션을 선택하고 Next(다음)를 클릭합니다

PGP	Select the type of communication you want to configure : Host communication with a specific individual computer. Subnet communication with a group of computers which occupy a contiguous range of internet addresses. Gateway communication with computers which are located on the other side of a secure gateway (thewal).

4. 연결을 설명하는 이름을 입력하고 Next(**다음**)를 클릭합니다

Add Host Wizard		×
PGP	Enter a descriptive name for the gateway with which you want to communicate. As examples, you could use the host domain name of the gateway (e.g. "gateway" company.com") or something more descriptive (e.g. "Departmental finewall").	
	<back next=""> Cancel</back>	_

5. VPN 3000 Concentrator의 공용 인터페이스의 호스트 도메인 이름 또는 IP 주소를 입력하고

Host Domain Name :	P) 2
	_
JP Address : 90 . 90 . 90 . 74	

6. Use public-key cryptographic security only를 선택하고 Next를 클릭합니다



7. 예를 선택하고 다음을 클릭합니다. 새 호스트 또는 서브넷을 추가하면 연결이 보안된 후 사설



- 네트워크에 연결할 수 있습니다.
- 8. 서브넷을 선택하고 **다음**을 클릭합니다



9. Allow insecure **communications(비보안 통신 허용)**를 선택하고 Next(다음)를 **클릭합니다**.VPN 3000 Concentrator는 PGP 클라이언트 소프트웨어가 아닌 연결의 보안을 처리합니다

	×
An entry in the host list can indicate that you want to enforce secure communication for the specified compute(s) or that you want to allow insecure communications with them. For the new entry that you are creating now, select the desired type of communication: C Enforce secure communications C Allow insecure communications	
< <u>B</u> ack <u>N</u> est> Cancel	-
	An entry in the host list can indicate that you want to enforce secure communication for the specified computer(s) or that you want to allow insecure communications with them. For the new entry that you are creating now, select the desired type of communication: C Enforce geoure communications C Allow insecure communications

10. <u>연결할 네트워크를 고유하게 식별하기 위한 설명 이름을 입</u>력하고 **Next(다음**)를 클릭합니다

Add Host Wizard		×
	Enter a descriptive name for the subnet with which you want to communicate.	
	Corporate Internal Network	
PGP		
	< <u>B</u> ack Newt> Cancel	

11. VPN 3000 Concentrator 뒤에 있는 네트워크의 네트워크 번호와 서브넷 마스크를 입력하고

	Enter the Intern the subnet with	et Protocol (IP) address and the subnet which you want to communicate.	mask of
No.	[P Address :	10.10.0.0	
100 M	Subnet Mask :	255.255.0.0	
PGP			
		< Back Next >	Cancel

12. 내부 네트워크가 더 많은 경우 예를 선택합니다. 그렇지 않으면 No를 선택하고 Next를 클릭



<u>Network Associates PGP 클라이언트의 연결을 허용하도록 Cisco</u> <u>VPN 3000 Concentrator 구성</u>

Network Associates PGP Client의 연결을 허용하도록 Cisco VPN 3000 Concentrator를 구성하려면 다음 절차를 따르십시오.

- 1. Configuration > Tunneling and Security > IPSec > IKE Proposals를 선택합니다.
- 2. Inactive **Proposals(비활성 제안)** 열에서 선택하여 IKE-3DES-SHA-DSA 제안을 활성화합니다. 그런 다음 **활성화** 버튼을 클릭한 다음 필요 저장 버튼을 클릭합니다.
- 3. Configuration > Policy Management > Traffic Management > SAs를 선택합니다.
- 4. Add(추가)를 클릭합니다.
- 5. 다음 필드를 제외한 모든 필드를 기본 설정으로 둡니다.**SA 이름:** 이를 식별하기 위해 고유한 이름을 만듭니다.**디지털 인증서:** 설치된 서버 ID 인증서를 선택합니다.**IKE 제안: IKE-3DES-SHA-DSA를 선택합니다**.
- 6. Add(추가)를 클릭합니다.
- 7. Configuration(구성) > User Management(사용자 관리) > Groups(그룹)를 선택하고 Add Group(그룹 추가)을 클릭하고 다음 필드를 구성합니다.참고: 모든 사용자가 PGP 클라이언트 인 경우 새 그룹을 생성하는 대신 기본 그룹(Configuration > User Management > Base Group)을 사용할 수 있습니다. 이 경우 ID 탭의 단계를 건너뛰고 IPSec 탭의 1단계와 2단계만 완료합니다.ID 탭에서 다음 정보를 입력합니다.그룹 이름: 고유한 이름을 입력합니다. (이 그룹 이름은 PGP 클라이언트의 디지털 인증서에 있는 OU 필드와 같아야 합니다.)암호: 그룹의 비 밀번호를 입력합니다.IPSec 탭에서 다음 정보를 입력합니다.인증: 이 값을 없음으로 설정합니 다.모드 구성: 선택을 취소합니다.
- 8. Add(추**가)를 클릭합니다**.
- 9. 필요한 만큼 전체 시간 동안 저장합니다.

<u>관련 정보</u>

- <u>Cisco VPN 3000 Series Concentrator 지원 페이지</u>
- <u>IPSec 지원 페이지</u>
- <u>VPN 소프트웨어 다운로드(등록된</u> 고객만 해당)

<u>Technical Support - Cisco Systems</u>