Cisco RV320 Gigabit Dual WAN VPN Router와 Cisco 500 Series Integrated Services Adapter 간에 사이트 대 사이트 VPN 터널 구성

목표

VPN(Virtual Private Network)은 원격 네트워크를 주 사설 네트워크에 연결하는 데 널리 사용되는 기술로 존재하며, 공용 회선을 통해 암호화된 채널의 형태로 사설 링크를 시뮬레이션합니다.원격 네트워크는 보안 문제 없이 사설 기본 네트워크의 일부로 존재하는 것처럼 사설 기본 네트워크에 연결할 수 있습니다. VPN 엔드포인트만 암호 해독 방법을 아는 방식으로 VPN 트래픽을 암호화하는 2단계 협상 때문입니다.
이 짧은 설명서에서는 Cisco 500 Series Integrated Services Adapter와 Cisco RV Series Router 간에 사이트 대 사이트 IPsec VPN 터널을 구축하기 위한 설계의 예를 제공합니다.

적용 가능한 디바이스

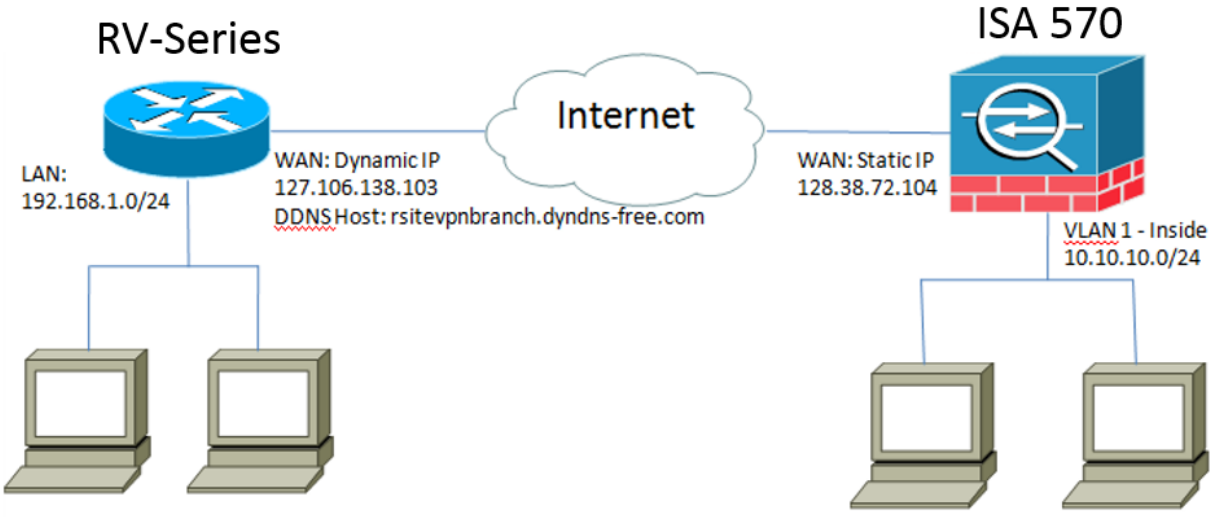
·Cisco RV Series 라우터(RV320)
· Cisco 500 Series Integrated Services Adapter(ISA570)

소프트웨어 버전

·4.2.2.08 [Cisco RV0xx Series VPN Router]

사전 구성

네트워크 다이어그램
다음은 Site-to-Site VPN 토폴로지를 보여줍니다.



Site-to-Site IPsec VPN 터널은 Remote Office의 Cisco RV Series Router와 Main Office의

Cisco 500 Series ISA 간에 구성 및 설정됩니다.
이 컨피그레이션을 사용하면 LAN 192.168.1.0/24의 원격 사무소와 LAN 10.10.10.0/24의 호스트가 VPN을 통해 안전하게 통신할 수 있습니다.

핵심 개념

IKE(Internet Key Exchange)

IKE(Internet Key Exchange)는 IPsec 프로토콜 제품군에서 SA(Security Association)를 설정하는 데 사용되는 프로토콜입니다.IKE는 Oakley 프로토콜, Internet Security Association 및 ISAKMP(Key Management Protocol)를 기반으로 하며, Diffie-Hellman 키 교환을 사용하여 암호화 키가 파생되는 공유 세션 암호를 설정합니다.

ISAKMP(Internet Security Association and Key Management Protocol)

ISAKMP(Internet Security Association and Key Management Protocol)는 두 VPN 엔드포인트 간의 VPN 터널을 협상하는 데 사용됩니다. 인증, 통신 및 키 생성 절차를 정의하며 IKE 프로토콜에서 암호화 키를 교환하고 보안 연결을 설정하는 데 사용됩니다.

IPsec(인터넷 프로토콜 보안)

IPsec(IP Security Protocol)은 데이터 스트림의 각 IP 패킷을 인증하고 암호화하여 IP 통신을 보호하는 프로토콜 모음입니다.또한 IPsec에는 세션 시작 시 에이전트 간 상호 인증을 설정하는 프로토콜과 세션 중에 사용할 암호화 키의 협상을 위한 프로토콜도 포함되어 있습니다
. IPsec을 사용하여 호스트, 게이트웨이 또는 네트워크 쌍 간의 데이터 흐름을 보호할 수 있습니다.

설계 팁

VPN 토폴로지 — 포인트 투 포인트 VPN 토폴로지는 기본 사이트와 원격 사이트 간에 보안 IPsec 터널이 구성되었음을 의미합니다.
기업은 멀티 사이트 토폴로지에 여러 원격 사이트가 필요하고 허브 앤 스포크(hub and spoke) VPN 토폴로지 또는 전체 메시 VPN 토폴로지를 구현해야 하는 경우가 많습니다.허브 앤 스포크(hub-and-spoke) VPN 토폴로지는 원격 사이트가 다른 원격 사이트와의 통신을 필요로 하지 않으며, 각 원격 사이트는 기본 사이트와의 보안 IPsec 터널만 설정합니다.풀 메시 VPN 토폴로지는 원격 사이트가 다른 원격 사이트와의 통신을 필요로 하고 각 원격 사이트가 주 사이트 및 기타 모든 원격 사이트와의 보안 IPsec 터널을 설정한다는 것을 의미합니다.
VPN 인증 — VPN 터널을 설정할 때 VPN 피어를 인증하는 데 IKE 프로토콜이 사용됩니다.다양한 IKE 인증 방법이 있으며 사전 공유 키가 가장 편리한 방법입니다.강력한 사전 공유 키를 적용할 것을 권장합니다.
VPN 암호화 — VPN을 통해 전송되는 데이터의 기밀성을 보장하기 위해 암호화 알고리즘을 사용하여 IP 패킷의 페이로드를 암호화합니다.DES, 3DES 및 AES는 세 가지 일반적인 암호화 표준입니다.AES는 DES 및 3DES와 비교할 때 가장 안전한 것으로 간주됩니다.Cisco에서는 AES-128비트 이상의 암호화(예: AES-192 및 AES-256)를 적용하는 것이 좋습니다. 그러나 더 강력한 암호화 알고리즘에는 라우터에서 더 많은 처리 리소스가 필요합니다.
동적 WAN IP 주소 지정 및 DDNS(Dynamic Domain Name Service) — 두 공용 IP 주소 간에 VPN 터널을 설정해야 합니다.WAN 라우터가 ISP(Internet Service Provider)로부터 고정 IP 주소를 수신하는 경우 고정 공용 IP 주소를 사용하여 VPN 터널을 직접 구현할 수 있습니다.그러나 대부분의 중소기업에서는 DSL이나 케이블과 같은 비용 효율적인 광대역 인터넷 서비스를 사용하며 ISP로부터 동적 IP 주소를 수신합니다.이 경우 DDNS(Dynamic Domain Name Service)를 사용하여 동적 IP 주소를 FQDN(정규화된 도메인 이름)에 매핑할 수 있습니다.
LAN IP 주소 지정 — 각 사이트의 프라이빗 LAN IP 네트워크 주소는 중복되지 않아야 합니다

.각 원격 사이트의 기본 LAN IP 네트워크 주소는 항상 변경해야 합니다.

구성 팁

사전 구성 체크리스트

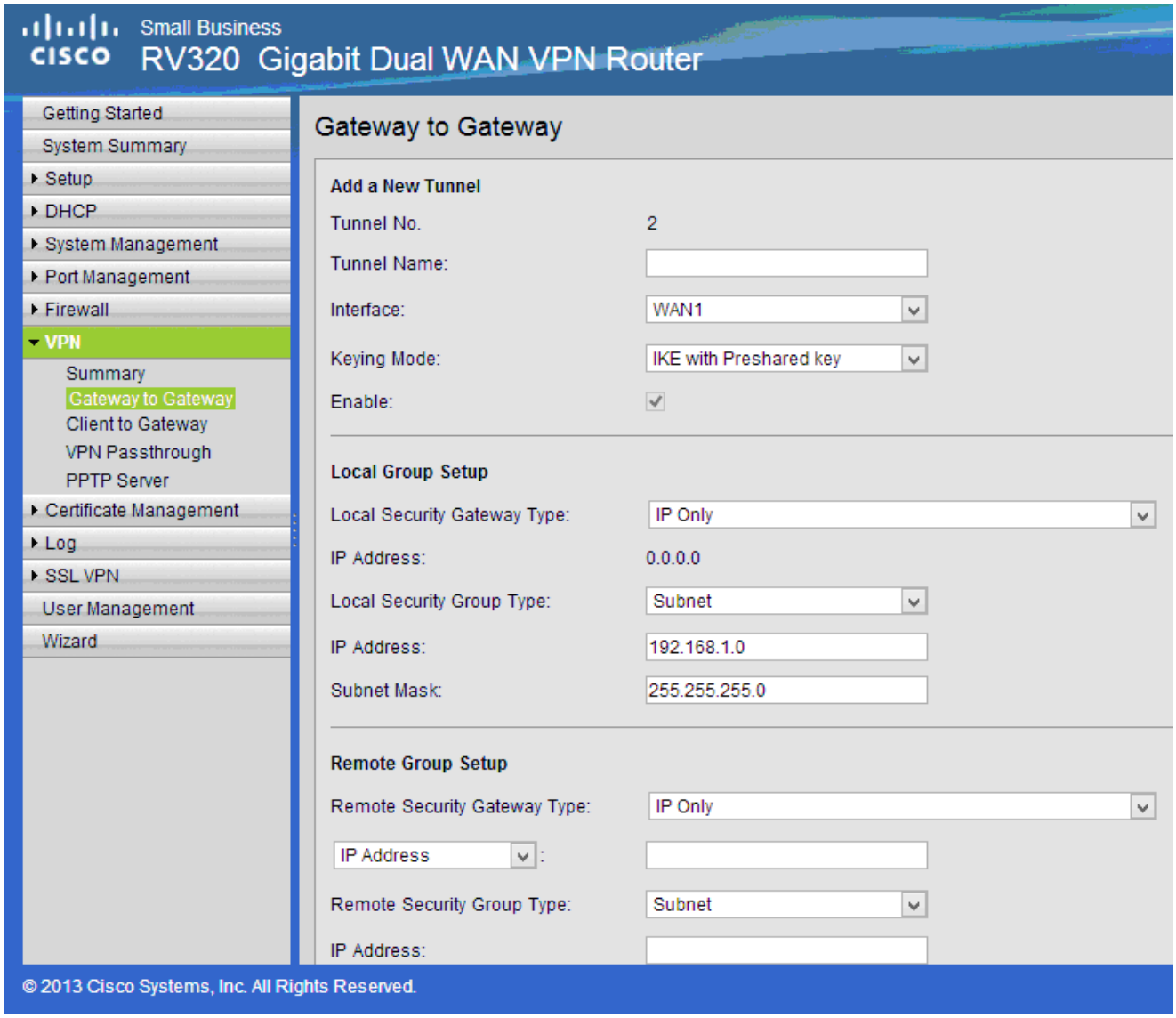
1단계. RV320과 DSL 또는 케이블 모뎀 사이에 이더넷 케이블을 연결하고 ISA570과 DSL 또는 케이블 모뎀 사이에 이더넷 케이블을 연결합니다.
2단계. RV320을 켜고 내부 PC, 서버 및 기타 IP 장치를 RV320의 LAN 포트에 연결합니다.
3단계. ISA570을 켜고 내부 PC, 서버 및 기타 IP 장치를 ISA570의 LAN 포트에 연결합니다.
4단계. 서로 다른 서브넷의 각 사이트에 네트워크 IP 주소를 구성해야 합니다.이 예에서는 원격 사무실 LAN이 192.168.1.0을 사용하고 주 사무실 LAN에서 10.10.10.0을 사용하고 있습니다.
5단계. 로컬 PC가 해당 라우터와 동일한 LAN의 다른 PC에 연결할 수 있는지 확인합니다.

WAN 연결 식별

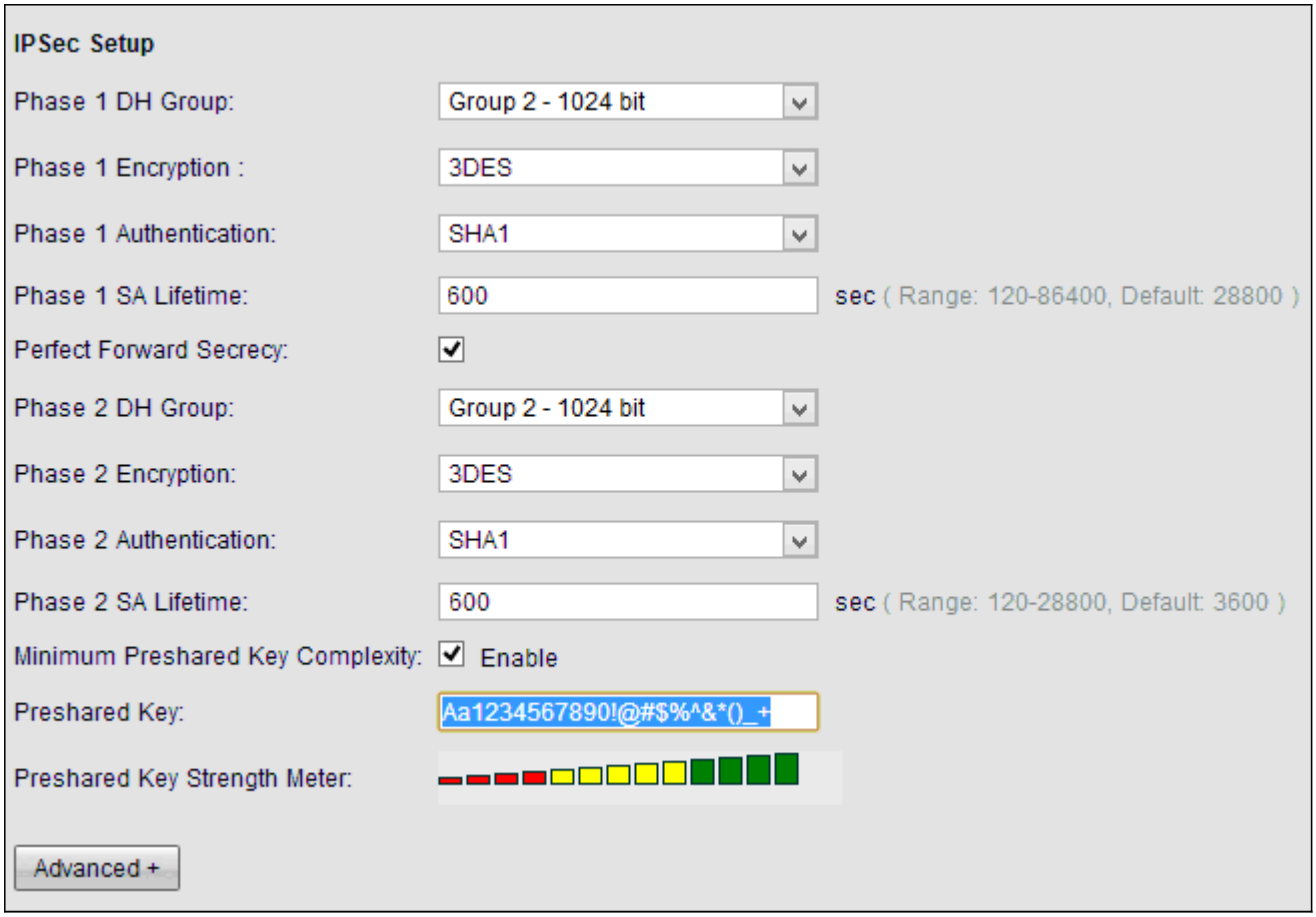
ISP에서 동적 IP 주소 또는 고정 IP 주소를 제공하는지 확인해야 합니다.ISP는 일반적으로 동적 IP 주소를 제공하지만 사이트 간 VPN 터널 컨피그레이션을 완료하기 전에 이를 확인해야 합니다.

원격 사무실에서 RV320에 대한 Site-to-Site IPsec VPN 터널 구성

1단계. VPN > **Gateway-to-Gateway로** 이동합니다(그림 참조).
a.) RemoteOffice와 같은 터널 이름을 입력합니다.
나.) Interface를 WAN1로 설정합니다.
다.) Keying Mode(키잉 모드)를 Preshared Key(사전 공유 키)가 있는 IKE로 설정합니다.
d.) 로컬 IP 주소 및 원격 IP 주소를 입력합니다.
다음 이미지는 RV320 Gigabit Dual WAN VPN Router Gateway to Gateway 페이지를 보여줍니다.



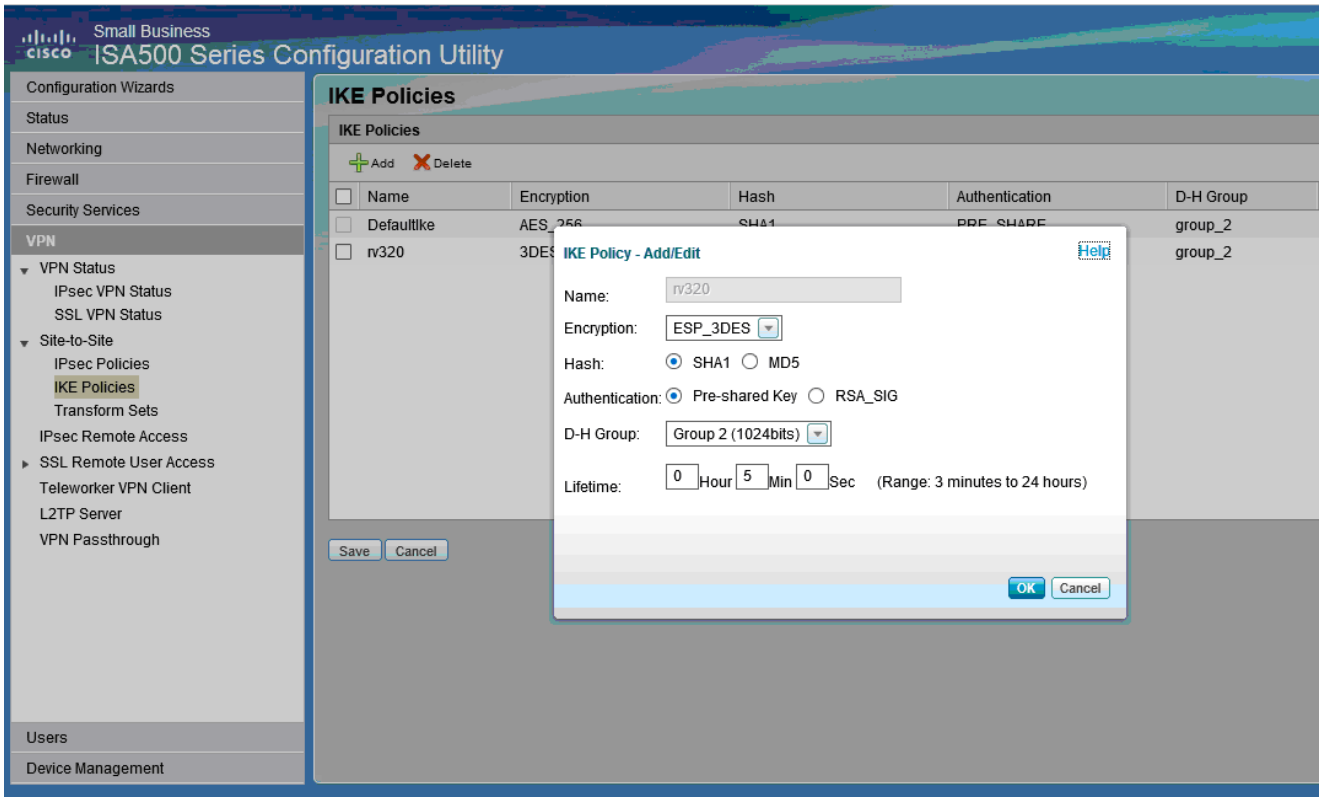
2단계. IPSec 터널 설정(그림 참조)
a.) 암호화를 3DES로 설정합니다.
나.) Authentication(*인증)*을 SHA1로 설정합니다.
다.) Perfect *Forward Secrecy를 확인합니다*.
d.) 사전 공유 *키*를 설정합니다(두 라우터에서 동일해야 함).
다음은 IPSec 설정(1단계 및 2단계)을 보여줍니다.



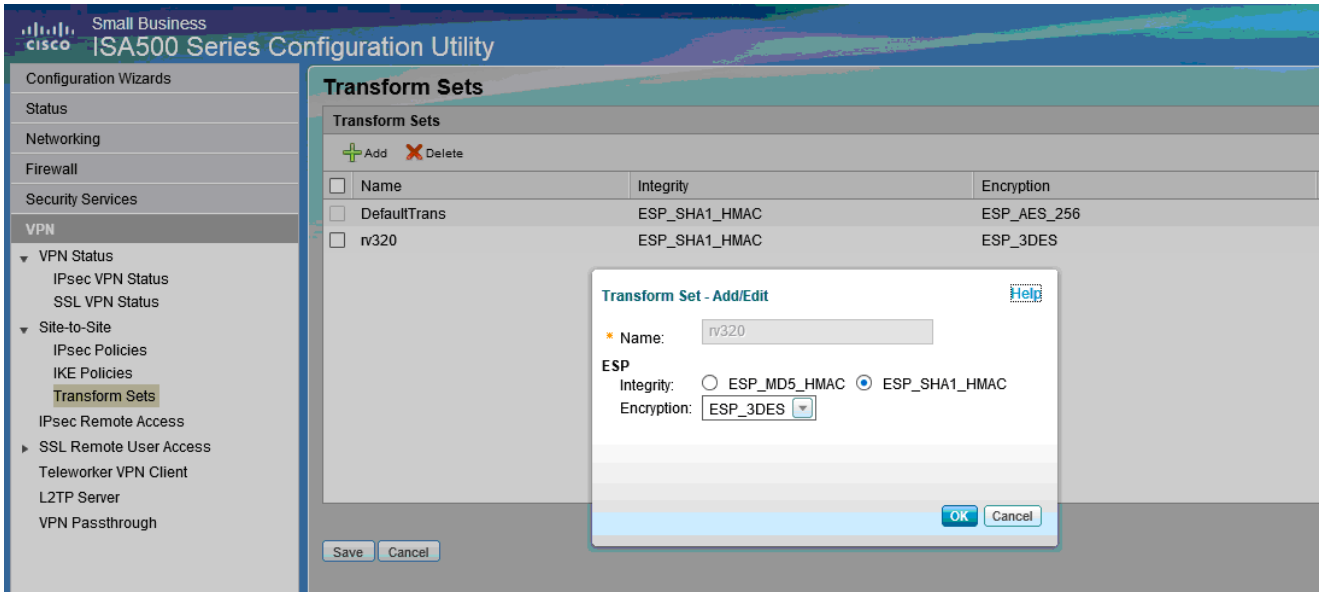
참고:사이트 간 IPsec VPN 터널의 양쪽에 있는 IPsec 터널 설정이 일치해야 합니다.RV320의 IPsec Tunnel Settings(IPsec 터널 설정)와 ISA570 간에 불일치가 발생할 경우 두 디바이스 모두 암호화 키를 협상하지 못하고 연결하지 못합니다.
3단계. **Save(저장)**를 클릭하여 구성을 완료합니다.

주 사무실에서 ISA570에 대한 Site-to-Site IPsec VPN 터널 구성

1단계. **VPN > IKE** Policies(그림 참조)로 이동합니다.
a.) Encryption*(암호화)*을 ESP_3DES로 설정합니다.
나.) Hash*를* SHA1로 설정합니다.
다.) Authentication(*인증*)을 Pre-shared Key(사전 공유 키)로 설정합니다.
d.) *D-H Group*을 Group 2(1024비트)로 설정합니다.
다음 이미지는 IKE 정책을 보여줍니다.



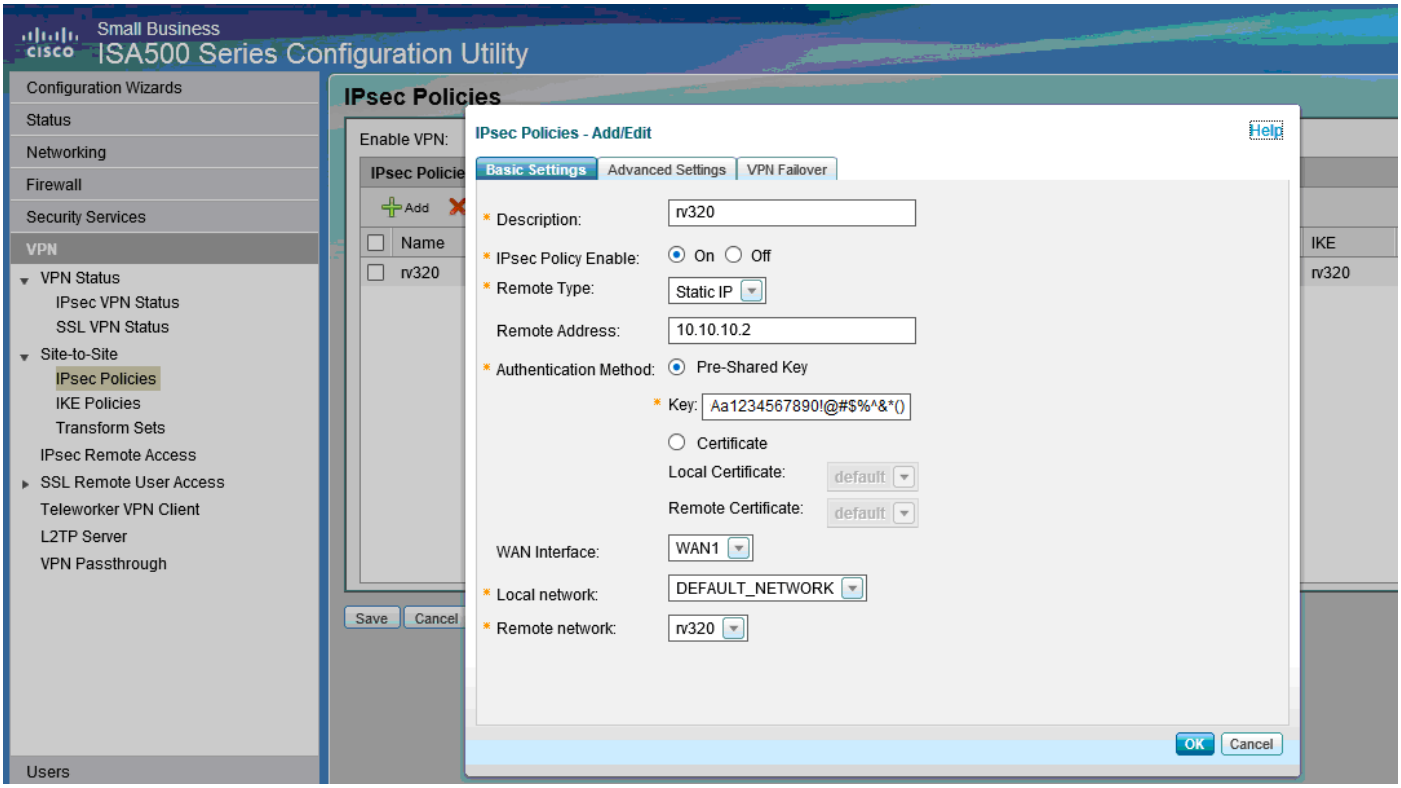
2단계. **VPN > IKE Transform Sets(IKE 변형 집합)**로 이동합니다(그림 참조).
a.) Integrity*를* ESP_SHA1_HMAC로 설정합니다.
나.) Encryption*(암호화)*을 ESP_DES로 설정합니다.
다음은 IKE 변형 집합을 보여줍니다.



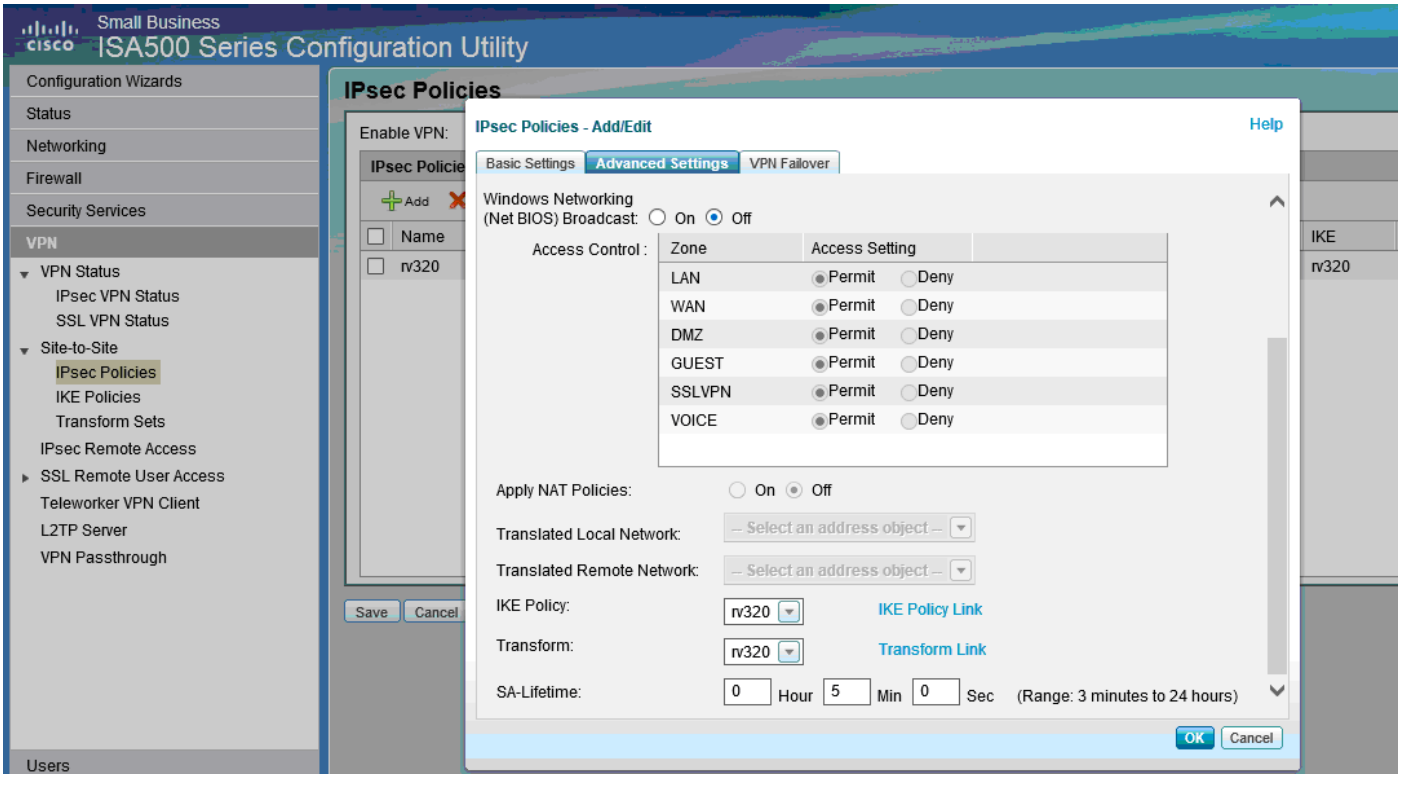
3단계. **VPN > IPsec Policies > Add > Basic Settings로** 이동합니다(그림 참조).

a.) RV320과 같은 *설명*을 입력합니다.
나.) IPsec *Policy Enable(IPsec 정책 활성화)*을 On(켜기)으로 설정합니다.
다.) Remote *Type(원격 유형)을 Static IP로 설정합니다*.
d.) *원격 주소를 입력합니다*.
e) Authentication *Method(인증 방법)*를 Pre-Shared Key(사전 공유 키)로 설정합니다.
바.) WAN *인터페이스*를 WAN1로 설정합니다.
g) 로컬 *네트워크*를 DEFAULT_NETWORK로 설정합니다.

h) Remote *Network(원격 네트워크)*를 RV320으로 설정합니다.
다음 그림에서는 IPsec 정책 기본 설정을 보여줍니다.



4단계. **VPN > IPsec Policies > Add > Advanced Settings로** 이동합니다(그림 참조).
a.) IKE *Policy(IKE 정책)* 및 *IKE Transform Sets(IKE 변형 집합)*를 각각 1단계와 2단계에서 생성한 집합으로 설정합니다.
나.) *SA-Lifetime*을 0시간 5분 0초로 설정합니다.
다.) **확인을 클릭합니다**.
다음은 IPsec 정책 고급 설정을 보여줍니다.



5단계. Site-to-Site IPsec VPN 터널 연결(그림 참조)
a.) Enable *VPN(VPN 활성화)*을 On(켜기)으로 설정합니다.
나.) Connect(**연결**) 버튼을 클릭합니다.
다음 그림에서는 [연결] 단추를 보여 줍니다.