Cisco RV Router VPN 개요 및 모범 사례

목표

이 문서의 목적은 Cisco RV Series 라우터를 처음 사용하는 사용자에게 VPN(Virtual Private Network) 모범 사례를 개략적으로 설명하는 것입니다.

목차

소개

아주 오래전 일이라 일할 수 있는 곳은 사무실뿐이었던 것 같아요. 과거에는 주말에 업무 문제를 해결하기 위해 사무실로 들어가야 했던 것을 기억하실 것입니다. 사무실에서 물리적으로 근무하지 않는 이상 회사 리소스로부터 데이터를 얻을 수 있는 다른 방법이 없었습니다. 그 시절은 끝났어. 오늘날에는 가정, 다른 사무실, 커피숍 또는 다른 국가에서 업무를 수행하는 등 이동 중에도 업무를 수행할 수 있습니다. 단점은 해커들이 항상 민감한 데이터를 확보하려 한다는 것입니다. 공용 인터넷을 사용하는 것만으로는 안전하지 않습니다. 유연성과 보안을 위해 무엇을 할 수 있을까요? VPN을 설정합니다!

VPN 연결을 통해 사용자는 인터넷과 같은 공용 또는 공유 네트워크를 통해 사설 네트워크에서 데이터를 액세스하고 송수신할 수 있지만, 사설 네트워크와 해당 리소스를 보호하기 위해 기본 네트워크 인프라에 안전하게 연결할 수는 있습니다.

VPN 터널은 데이터를 인코딩하기 위해 암호화를 사용하고 클라이언트의 ID를 확인하기 위해 인증을 사용하여 데이터를 안전하게 전송할 수 있는 사설 네트워크를 설정합니다. 회사 사무실에서는

VPN 연결을 사용하는 경우가 많습니다. 사무실 외부에 있는 직원도 개인 네트워크에 액세스할 수 있도록 하는 것이 유용하고 필요하기 때문입니다.

일반적으로 Site-to-Site VPN은 전체 네트워크를 서로 연결합니다. 네트워크를 확장하고 한 위치의 컴퓨터 리소스를 다른 위치에서 사용할 수 있도록 허용합니다. VPN 가능 라우터를 사용하면 인터넷과 같은 공용 네트워크를 통해 여러 개의 고정 사이트를 연결할 수 있습니다.

VPN에 대해 설정된 클라이언트-사이트 모드에서는 원격 호스트 또는 클라이언트가 동일한 로컬 네트워크에 있는 것처럼 작동할 수 있습니다. 인터넷 연결을 위해 라우터를 구성한 후 라우터와 엔드포인트 간에 VPN 연결을 설정할 수 있습니다. VPN 클라이언트는 VPN 라우터의 설정에 따라 다르며, 연결을 설정하기 위해 일치하는 설정이 필요합니다. 또한 일부 VPN 클라이언트 애플리케이션은 플랫폼에 따라 다르며 OS(운영 체제) 버전에도 종속됩니다. 설정이 정확히 일치해야 합니다. 그렇지 않으면 통신할 수 없습니다.

VPN은 다음 중 하나로 설정할 수 있습니다.

- SSL(Secure Socket Layer)
- IPSec(인터넷 프로토콜 보안)
- PPTP(Point-to-Point Tunneling Protocol) - SSL 또는 IPSec만큼 안전하지 않음
- GRE(Generic Routing Encapsulation)
- L2TP(Layer 2 Tunneling Protocol)

이전에 VPN을 설정하지 않은 경우 이 문서 전체에서 많은 새로운 정보를 받게 됩니다. 이는 단계별 가이드가 아니라 참조를 위한 개요에 대한 것입니다. 따라서 다음으로 이동하여 네트워크에서 VPN을 설정하기 전에 이 문서를 전체적으로 읽는 것이 좋습니다. 특정 단계에 대한 링크는 이 문서 전체에서 제공됩니다.

TheGreenBow, OpenVPN, Shrew Soft, EZ VPN을 비롯한 타사 제품은 Cisco에서 지원하지 않습니다. 그것들은 지도 목적상 엄격하게 포함되어 있다. 기사 외에 이에 대한 지원이 필요한 경우 제3자에게 지원을 요청해야 합니다.

VPN 연결 사용의 이점

- VPN 연결을 사용하면 기밀 네트워크 데이터 및 리소스를 보호할 수 있습니다.
- 원격 근무자 또는 기업 직원이 본사의 리소스에 물리적으로 상주하지 않고도 쉽게 액세스할 수 있고, 사설 네트워크 및 리소스의 보안을 유지할 수 있으므로 이에 대한 편의성과 접근성을 제공합니다.
- VPN 연결을 사용하는 통신은 다른 원격 통신 방법에 비해 높은 수준의 보안을 제공합니다. 고급 암호화 알고리즘을 사용하면 이러한 작업을 수행할 수 있어 사설 네트워크가 무단 액세스로부터 보호됩니다.
- 사용자의 실제 지리적 위치는 보호되며 인터넷과 같은 공용 또는 공유 네트워크에 노출되지 않습니다.
- VPN을 사용하면 구성 요소를 추가하거나 복잡한 구성을 수행할 필요 없이 새 사용자 또는 사

용자 그룹을 추가할 수 있습니다.

VPN 연결 사용 시 위험

- 컨피그레이션 오류로 인해 보안 위험이 발생할 수 있습니다. VPN의 설계와 구현은 복잡할 수 있으므로, 사설 네트워크의 보안이 손상되지 않도록 하기 위해 전문적이고 숙련된 전문가에게 연결 구성 작업을 맡겨야 합니다.
- 신뢰도가 떨어질 수 있습니다 VPN 연결에는 인터넷 연결이 필요하므로, 우수한 인터넷 서비스를 제공하고 다운타임을 최소화하려면 검증되고 테스트된 평판을 가진 공급업체를 확보하는 것이 중요합니다.
- 새로운 인프라 또는 새로운 컨피그레이션 집합을 추가해야 하는 상황이 발생할 경우, 특히 이미 사용 중인 제품 또는 공급업체가 아닌 다른 제품이나 공급업체와 관련된 경우 비호환성으로 인해 기술적인 문제가 발생할 수 있습니다.
- 연결 속도가 느려질 수 있습니다. 무료 VPN 서비스를 제공하는 ISP 연결을 사용하는 경우 이러한 공급자가 연결 속도의 우선순위를 지정하지 않기 때문에 연결 속도도 느려질 수 있습니다. VPN 처리량은 라우터의 하드웨어 기능에 따라 달라집니다.

VPN의 작동 방식에 대한 자세한 내용을 보려면 여기를 클릭하십시오.

VPN 구성 시 사용할 팁

1. 서로 다른 사이트 간에 VPN을 구성하는 동안 양쪽 끝에서 서로 다른 LAN IP 서브넷을 사용합니다. 예를 들어 연결하는 사이트에서 192.168.x.x 주소 지정 체계를 사용하는 경우 10.x.x.x 또는 172.16.x.x - 172.31.x.x 서브넷을 사용할 수 있습니다. 다른 옵션은 서로 다른 서브넷 마스크를 사용하는 것입니다. 라우터 IP 주소를 변경하면 DHCP(Dynamic Host Configuration Protocol)의 디바이스가 해당 서브넷의 IP 주소를 자동으로 선택합니다.
2. 안정적인 VPN 연결을 위해 라우터의 WAN 인터페이스에서 고정 공용 IP를 사용합니다.
3. 선택한 암호화 및 인증 수준이 VPN에 대해 VPN 터널을 설정하려는 라우터와 동일한지 확인합니다.
4. 입력한 PSK 및 키 수명이 원격 라우터와 동일한지 확인하십시오. PSK는 원하는 대로 사용할 수 있습니다. PSK는 사이트에서 클라이언트와 일치해야 하며 PSK가 컴퓨터에서 클라이언트로 설정되어야 합니다. 장치에 따라 사용할 수 없는 금지된 기호가 있을 수 있습니다. Key Lifetime은 시스템에서 키를 변경하는 빈도입니다. 인증서는 더 안전한 것으로 간주되므로 선호됩니다.
5. 대부분의 VPN에서 클라이언트는 VPN을 사용하기 위해 인증서가 필요하지 않으며 라우터를 통해 확인하는 용도로만 사용됩니다. 예를 들어 OpenVPN에는 클라이언트 및 사이트 인증서가 모두 필요합니다.
6. I단계의 SA 수명을 II단계의 SA 수명보다 길게 설정합니다. Phase I를 Phase II보다 짧게 만들면 데이터 터널이 아니라 터널을 앞뒤로 자주 재협상해야 합니다. 데이터 터널은 보안을 강화해야 하므로 Phase II의 수명을 Phase I보다 짧게 설정하는 것이 좋습니다.
7. 모든 비밀번호를 좀 더 복잡한 비밀번호로 변경합니다.

VPN 유형

SSL(Secure Sockets Layer)

Cisco RV34x Series 라우터는 AnyConnect를 사용하여 SSL VPN을 지원합니다. RV160 및 RV260에는 또 다른 SSL VPN인 OpenVPN을 사용할 수 있는 옵션이 있습니다. SSL VPN 서버를 통해 원격 사용자는 웹 브라우저를 사용하여 보안 VPN 터널을 설정할 수 있습니다. 이 기능을 사용하면 SSL HTTPS(Hypertext Transfer Protocol Secure) 브라우저 지원을 통해 기본 HTTP(Hypertext Transfer Protocol)를 사용하는 광범위한 웹 리소스 및 웹 지원 애플리케이션에 쉽게 액세스할 수 있습니다.

SSL VPN을 통해 사용자는 네트워크 트래픽을 암호화하여 안전하고 인증된 경로를 사용하여 제한된 네트워크에 원격으로 액세스할 수 있습니다.

SSL에서 액세스를 설정하는 옵션은 두 가지입니다.

1. 자체 서명 인증서: 자체 작성자가 서명한 인증서입니다. 이는 권장되지 않으며 테스트 환경에서만 사용해야 합니다.
2. CA 서명 인증서: 훨씬 더 안전하고 권장됩니다. 유료로 서드파티는 네트워크가 합법적인지 확인하고 CA 인증서를 생성하여 사이트에 연결합니다. CA 인증서에 대한 자세한 내용은 이 문서의 Certificates 섹션을 참조하십시오.

이 문서에는 AnyConnect에 대한 기사 링크가 있습니다. AnyConnect에 대한 개요를 보려면 여기를 클릭하십시오.

IPsec 프로필

Easy VPN(EZVPN), TheGreenBow 및 Shrew Soft는 IPSec(Internet Protocol Security) VPN입니다. IPSec VPN은 두 피어 간 또는 클라이언트-사이트 간 보안 터널을 제공합니다. 민감한 패킷으로 간주되는 패킷은 이러한 보안 터널을 통해 전송해야 합니다. 이러한 민감한 패킷을 보호하기 위해 해시 알고리즘, 암호화 알고리즘, 키 수명, 모드 등의 매개 변수를 사용해야 하며 이러한 터널의 특성을 지정하여 정의해야 합니다. 그런 다음 IPsec 피어가 이러한 민감한 패킷을 발견하면 적절한 보안 터널을 설정하고 이 터널을 통해 패킷을 원격 피어로 전송합니다.

IPsec을 방화벽 또는 라우터에 구현할 경우 경계를 넘는 모든 트래픽에 적용할 수 있는 강력한 보안을 제공합니다. 회사 또는 작업 그룹 내의 트래픽은 보안 관련 처리 오버헤드가 발생하지 않습니다.

VPN 터널의 양단이 성공적으로 암호화 및 설정되려면 암호화, 암호 해독 및 인증 방법에 동의해야 합니다. IPsec 프로필은 IPsec의 중앙 컨피그레이션으로, 자동 모드 및 수동 키 모드에서 Phase I 및 II 협상을 위한 암호화, 인증 및 DH(Diffie-Hellman) 그룹과 같은 알고리즘을 정의합니다.

IPsec의 중요한 구성 요소로는 IKE(Internet Key Exchange) 1단계와 2단계가 있습니다.

IKE 1단계의 기본 목적은 IPSec 피어를 인증하고 피어 간에 보안 채널을 설정하여 IKE 교환을 활성화하는 것입니다. IKE 1단계에서는 다음 기능을 수행합니다.

- IPSec 피어의 ID를 인증하고 보호합니다
- IKE 교환을 보호하기 위해 피어 간에 일치하는 IKE SA(Security Associations) 정책을 협상합니다

- 일치하는 공유 비밀 키를 갖게 된 최종 결과와 함께 인증된 Diffie-Hellman 교환을 수행합니다
- IKE 2단계 매개변수를 협상하도록 보안 터널을 설정합니다
- 주 모드와 적극적인 모드의 두 가지 모드에서 발생합니다.

IKE 2단계의 목적은 IPSec 터널을 설정하기 위해 IPSec SA를 협상하는 것입니다. IKE 2단계에서는 다음 기능을 수행합니다.

- 기존 IKE SA에 의해 보호되는 IPSec SA 매개변수를 협상합니다.
- IPSec 보안 연결 설정
- 보안을 보장하기 위해 정기적으로 IPSec SA 재협상
- 선택적으로 추가 Diffie-Hellman 교환 수행
- 한 가지 모드만 사용됨, 빠른 모드

IPSec 정책에 PFS(Perfect Forward Secrecy)가 지정된 경우 각 빠른 모드에서 새로운 DH 교환이 수행되어 더 큰 엔트로피(키 자료 수명)를 가져 암호화 공격에 대한 저항력이 더 큰 키 자료를 제공합니다. 각 DH 교환에는 대량의 지표가 필요하므로 CPU 사용이 증가하고 성능 비용이 절감됩니다.

- RV34x Series 라우터의 IPSec(Internet Protocol Security) 프로파일 컨피그레이션
- RV160 및 RV260에서 IPSec 프로파일(자동 키 지정 모드) 구성
- RV160 및 RV260 라우터에서 IPsec Profile Manual Keying Mode 구성

PPTP(Point-to-Point 터널링 프로토콜)

PPTP는 공용 네트워크 간에 VPN 터널을 생성하는 데 사용되는 네트워크 프로토콜입니다. PPTP 서버는 VPDN(Virtual Private Dialup Network) 서버라고도 합니다. PPTP는 속도가 더 빠르고 모바일 장치에서 작업할 수 있기 때문에 다른 프로토콜을 통해 사용되기도 합니다. 그러나 다른 유형의 VPN만큼 안전하지 않다는 점에 유의해야 합니다. PPTP 유형 계정에 연결하는 방법은 여러 가지가 있습니다. 자세한 내용을 보려면 링크를 클릭하십시오.

- Rv34x Series Router에서 PPTP(Point-to-Point Tunneling Protocol) 서버 구성
- Windows의 RV320 및 RV325 VPN Router Series에서 PPTP(Point-to-Point Tunneling Protocol) 서버 구성

일반 라우팅 캡슐화

GRE(Generic Routing Encapsulation)는 캡슐화를 통해 한 프로토콜의 패킷을 다른 프로토콜로 전송하기 위한 간단한 일반적인 접근 방식을 제공하는 터널링 프로토콜입니다.

GRE는 외부 IP 패킷 내에서 목적지 네트워크로 전달해야 하는 페이로드, 즉 내부 패킷을 캡슐화합니다. GRE 터널은 터널 소스 및 터널 대상 주소로 식별되는 두 개의 엔드포인트가 있는 가상 포인트-투-포인트 링크로 작동합니다.

터널 엔드포인트는 중간 IP 네트워크를 통해 캡슐화된 패킷을 라우팅하여 GRE 터널을 통해 페이로드를 전송합니다. 도중에 있는 다른 IP 라우터는 페이로드(내부 패킷)를 구문 분석하지 않습니다. 외부 IP 패킷이 GRE 터널 엔드포인트로 전달될 때에만 구문 분석합니다. 터널 엔드포인트에 도달하면 GRE 캡슐화가 제거되고 패킷의 최종 목적지로 페이로드가 전달됩니다.

네트워크에서 데이터그램 캡슐화는 소스 서버가 패킷이 목적지 호스트에 도달하는 데 걸리는 경로에 영향을 미치려는 경우와 같이 여러 가지 이유로 수행됩니다. 소스 서버를 캡슐화 서버라고도 합니다.

IP-in-IP 캡슐화에는 기존 IP 헤더 위에 외부 IP 헤더를 삽입하는 작업이 포함됩니다. 외부 IP 헤더의 소스 및 목적지 주소는 IP-in-IP 터널의 엔드포인트를 가리킵니다. 네트워크 관리자가 패킷을 전송하는 라우터의 루프백 주소를 알고 있는 경우, IP 헤더의 스택은 패킷이 미리 지정된 경로를 통해 목적지로 향하도록 하는 데 사용됩니다.

이 터널링 메커니즘은 대부분의 네트워크 아키텍처의 가용성과 레이턴시를 결정하는 데 사용할 수 있습니다. 소스에서 대상까지의 전체 경로가 헤더에 포함될 필요는 없지만, 패킷 전달을 위해 네트워크의 세그먼트를 선택할 수 있습니다.

레이어 2 터널링 프로토콜

L2TP는 터널링하는 트래픽에 대해 암호화 메커니즘을 제공하지 않습니다. 대신 IPSec과 같은 다른 보안 프로토콜을 사용하여 데이터를 암호화합니다.

L2TP 터널은 L2TP LAC(Access Concentrator)와 L2TP LNS(Network Server) 사이에 설정됩니다. 이러한 디바이스 간에는 IPSec 터널도 설정되며 모든 L2TP 터널 트래픽은 IPSec을 사용하여 암호화됩니다.

L2TP와 관련된 몇 가지 주요 조건:

- CHAP - Challenge Handshake 인증 프로토콜. PPP(Point to Point Authentication Protocol).
- L2TP LAC(Access Concentrator) - LAC는 PSTN(public switched telephone network)에 연결된 Cisco 네트워크 액세스 서버일 수 있습니다. LAC는 L2TP를 통한 작동을 위해 미디어만 구현하면 됩니다. LAC는 LAN 또는 LAN(Wide-Area Network)(예: 퍼블릭 또는 프라이빗 프레임 릴레이)을 사용하여 LNS에 연결할 수 있습니다. LAC는 수신 통화의 개시자 및 발신 통화의 수신자입니다.
- L2TP 네트워크 서버(LNS) - 로컬 영역 네트워크 또는 광역 네트워크에 연결된 거의 모든 Cisco 라우터(예: 퍼블릭 또는 프라이빗 프레임 릴레이)가 LNS 역할을 할 수 있습니다. L2TP 프로토콜의 서버측이며 PPP 세션을 종료하는 모든 플랫폼에서 작동해야 합니다. LNS는 발신 통화의 개시자 및 수신 통화의 수신자입니다. 그림 1은 LAC와 LNS 간의 통화 루틴입니다.
- VPDN(Virtual Private Dial Network) - PPP를 사용하여 서비스를 제공하는 액세스 VPN의 유형입니다.

L2TP에 대한 자세한 내용을 보려면 다음 링크를 클릭하십시오.

- RV34x 라우터에서 L2TP WAN 설정 구성
- 광역 네트워킹 컨피그레이션 가이드: 레이어 2 서비스, Cisco IOS XE 릴리스 3S

Cisco RV Series VPN Router와 호환되는 VPN

	RV34X	RV32X	RV160X/RV260X

IPSec(IKEv1)			
슈레프소프트	예	예	예
그린보우	예	예	예
Mac 내장 클라이언트	예	예	아니요
iPhone/iPad	예	예	아니요
안드로이드	예	예	예
L2TP/IPSec	예(PAP)	아니요	아니요
PPTP	예(PAP)	예*	예(PAP)
기타			
AnyConnect	예	아니요	아니요
Openvpn	아니요	예	예
IKEv2			
창	예*	아니요	예*
맥	예	아니요	예
아이폰	예	아니요	예
안드로이드	예	아니요	예

VPN 기술	지원되는 디바이스	지원되는 클라이언트*	세부사항 및 주의 사항
IPSec(IKEv1)	RV34X, RV32X, RV160X/RV260X	기본: Mac, iPhone, iPad, Android 기타: EasyVPN(Cisco VPN Client), ShrewSoft, Greenbow	설치, 문제 해결 및 지원이 가장 쉽습니다. 모든 라우터에서 사용 가능하고 설정이 간단하며 (대부분의 경우) 문제 해결을 위한 최적의 로깅을 제공합니다. 대부분의 디바이스가 포함됩니다. 이것이 우리가 일반적으로 ShrewSoft (무료 및 일) 및 Greenbow (무료, 하지만 일) 권장 이유입니다. Windows의 경우 ShrewSoft 및 Greenbow 클라이언트를 옵션으로 제공합니다. Windows에는 순수 IPSec 네이티브 VPN 클라이언트가 없기 때문입니다. ShrewSoft와 Greenbow는 조금 더 관여하지만 어렵지 않습니다. 처음 설정하면 클라이언트 프로파일을 내보낸 다음 다른 클라이언트로 가져올 수 있습니다. RV160X/RV260X 라우터의 경우 Easy VPN 옵션이 없으므로 Mac, iPhone 또는 iPad에서 작동하지 않는 타사 클라이언트 옵션을 사용해야 합니다. ShrewSoft, Greenbow, Android 클라이언트를 설정하여 연결할 수 있습니다. Mac, iPhone 및 iPad 클라이언트의 경우 IKEv2를

			권장합니다(아래 참조).
AnyConnect	RV34X	윈도우, 맥, 아이폰, 아이패드, 안드로이드	일부 고객은 완전한 Cisco 솔루션을 요청하며, 이것이 바로 그 해결책입니다. 설정이 간단하고 로깅이 있지만 로그를 이해하는 데 어려움이 있을 수 있습니다. 클라이언트 라이센싱 요구 사항으로 인해 비용이 발생합니다. 전체 Cisco 솔루션이며 업데이트됩니다. 트러블슈팅은 IPSec만큼 쉽지는 않지만 다른 VPN 옵션보다 우수합니다.
L2TP/IPSec	RV34X	네이티브: Windows	Windows에서 내장형 VPN 클라이언트를 사용해야 하는 고객에게 권장할 사항입니다. 두 가지 주의 사항은 다음과 같습니다. 1. 로컬 인증을 사용할 때만 PAP 인증을 지원합니다. 각 클라이언트로 이동하여 암호화 옵션 또는 없음을 선택하고 MS-CHAP 옵션을 비활성화하며 PAP를 활성화해야 합니다. 이는 사용자 이름/비밀번호가 암호화되지 않은 상태로 전송됨을 의미합니다. 모든 것이 IPSec으로 암호화되어 있고 각 클라이언트에서 설정해야 하기 때문에 큰 거래는 아닙니다. Windows에서는 이 기능을 구성할 수 있지만 Mac, iPhone, iPad 또는 Android 디바이스에서는 구성할 수 없습니다. 따라서 Windows 클라이언트에 Radius 또는 LDAP와 같은 외부 인증 서버가 없는 한 Windows 클라이언트에서만 사용할 수 있습니다. 2. 라우터가 NAT 장치 뒤에 있으면 Windows 컴퓨터에서 연결이 실패합니다. 해결 방법은 클라이언트와 라우터 모두에서 NAT를 허용하기 위해 각 클라이언트에 레지스트리 키를 만드는 것입니다.
IPSec(IKEv2)	RV34X, RV160X/RV260X	기본: Windows, Mac, iPhone, iPad, Android	IKEv2용 Windows 네이티브 클라이언트에는 인증서 인증이 필요합니다. 이 경우 라우터와 모든 클라이언트가 동일한 CA(또는 다른 신뢰할 수 있는 CA)의 인증서를 가져야 하므로 PKI 인프라가 필요합니다. IKEv2를 사용하려는 사용자의 경우 Mac, iPhone, iPad 및 Android 장치에 대해 IKEv2를

			설정하며, 일반적으로 Windows 머신 (ShrewSoft, Greenbow 또는 L2TP/IPSec)에 대해 IKEv1을 설정합니다.
개방형 VPN	RV32X, RV160X/RV260X	Open VPN이 클라이언트임	설정이 어렵고 문제 해결 및 지원이 어렵습니다. RV160X/RV260X 및 RV320에서 지원됩니다. IPSec이나 AnyConnect보다 설정이 더 복잡하며, 특히 인증서를 사용하는 경우 대부분 그렇습니다. 라우터에 유용한 로그가 없고 클라이언트 로그에 의존하기 때문에 문제 해결이 더 어렵습니다. 또한 OpenVPN 클라이언트 버전 업데이트는 경고 없이 어떤 인증서를 수락했는지 변경했습니다. 또한 Chromebook에서는 이 기능이 작동하지 않으므로 IPSec 솔루션으로 이동해야 했습니다.

* 가능한 한 많은 조합을 테스트합니다. 특정 하드웨어/소프트웨어 조합이 있는 경우 여기로 문의하십시오. 그렇지 않은 경우 테스트한 최신 버전에 대한 디바이스별 관련 컨피그레이션 가이드를 참조하십시오.

인증서

웹 사이트를 방문하여 안전하지 않다는 경고를 받은 적이 있습니까? 개인 정보가 안전하다고 확신할 수 없습니다. 그렇지 않습니다! 사이트가 안전한 경우 사이트 이름 앞에 닫힌 잠금 아이콘이 표시됩니다. 이 사이트는 안전한 것으로 검증되었다는 상징입니다. 잠금 아이콘이 닫혀 있는지 확인해야 합니다. VPN도 마찬가지입니다.

VPN을 설정할 때 CA(Certificate Authority)에서 인증서를 가져와야 합니다. 인증서는 타사 사이트에서 구매하여 인증에 사용됩니다. 그것은 당신의 사이트가 안전하다는 것을 증명하는 공식적인 방법입니다. 기본적으로 CA는 합법적인 비즈니스이며 신뢰할 수 있음을 확인하는 신뢰할 수 있는 소스입니다. VPN의 경우 최소 비용으로 더 낮은 수준의 인증서만 있으면 됩니다. CA에서 체크 아웃한 후, CA가 정보를 확인하면 인증서를 발급합니다. 이 인증서는 컴퓨터에 파일로 다운로드할 수 있습니다. 그런 다음 라우터(또는 VPN 서버)로 이동하여 업로드할 수 있습니다.

CA는 디지털 인증서를 발급할 때 PKI(Public Key Infrastructure)를 사용하는데, 이는 보안을 위해 공개 키 또는 개인 키 암호화를 사용합니다. CA는 인증서 요청을 관리하고 디지털 인증서를 발급합니다. 서드파티 CA로는 IdenTrust, Comodo, GoDaddy, GlobalSign, GeoTrust, Verisign 등이 있습니다.

VPN의 모든 게이트웨이가 동일한 알고리즘을 사용하는 것이 중요합니다. 그렇지 않으면 게이트웨이가 통신할 수 없습니다. 모든 인증서를 신뢰할 수 있는 동일한 서드파티에서 구매하는 것이 좋습니다. 이렇게 하면 여러 인증서를 수동으로 갱신해야 하므로 쉽게 관리할 수 있습니다.

참고: 클라이언트는 일반적으로 VPN을 사용하는 데 인증서가 필요하지 않습니다. 라우터를 통해

확인하는 용도로만 사용됩니다. 단, 클라이언트 인증서가 필요한 OpenVPN은 예외입니다.

일부 중소기업에서는 간소화를 위해 인증서 대신 비밀번호 또는 사전 공유 키를 사용하도록 선택합니다. 이는 보안성이 떨어지지만 무료로 설정할 수 있습니다.

인증서에 대한 자세한 내용은 아래 링크를 참조하십시오.

- RV160 및 RV260 Series Router의 인증서(CSR 가져오기/내보내기/생성)
- RV34x Series Router에서 기본 셀프 서명 인증서를 서드파티 SSL 인증서로 교체

라우터의 사이트 대 사이트 VPN

로컬 및 원격 라우터의 경우 VPN 연결에 사용된 사전 공유 키(PSK)/비밀번호/인증서 및 보안 설정이 모두 일치하는지 확인해야 합니다. 하나 이상의 라우터가 대부분의 Cisco RV Series 라우터가 사용하는 NAT(Network Address Translation)를 사용하는 경우 로컬 및 원격 라우터에서 VPN 연결에 대해 방화벽 예외를 적용해야 합니다.

자세한 내용은 다음 사이트 대 사이트 문서를 참조하십시오.

- RV34x에서 Site-to-Site VPN 구성
- RV340 또는 RV345 라우터에서 Site-to-Site VPN 구성
- Cisco Tech Talk: RV340 Series 라우터에서 Site-to-Site VPN 구성(비디오)
- RV160 및 RV260 라우터에서 Site-to-Site VPN 구성(기본 설정)
- RV160 및 RV260 라우터의 Site-to-Site VPN(고급 설정 및 페일오버)

라우터의 클라이언트-사이트 VPN

클라이언트 측에서 VPN을 설정하려면 관리자가 라우터에서 구성해야 합니다.

다음 라우터 컨피그레이션 문서를 보려면 클릭하십시오.

- RV160 및 RV260 라우터에서 VPN 설정 마법사 구성
- RV160 및 RV260으로 Shrew Soft VPN Client 구성
- Cisco Tech Talk: RV160 및 RV260에서 Shrew Soft VPN 구성(비디오)
- GreenBow IPsec VPN Client를 설정하고 사용하여 RV160 및 RV260 라우터와 연결

클라이언트-사이트 프로필 만들기

클라이언트-사이트 VPN 연결에서 인터넷의 클라이언트는 서버에 연결하여 서버 뒤의 회사 네트워크 또는 LAN에 액세스할 수 있지만 네트워크 및 리소스의 보안은 그대로 유지됩니다. 이 기능은 재택 근무자 및 출장 사용자가 개인 정보 및 보안을 손상시키지 않고 VPN 클라이언트 소프트웨어를 사용하여 네트워크에 액세스할 수 있는 새로운 VPN 터널을 만들기 때문에 매우 유용합니다. 다음 문서는 RV34x Series 라우터에 대한 내용입니다.

- RV34x Series Router에서 클라이언트-사이트 VPN(Virtual Private Network) 연결 구성

- RV34x Series 라우터에서 AnyConnect VPN(Virtual Private Network) 연결 설정

Port Forwarding(포트 전달)이 Source All Traffic(소스 모든 트래픽) 및 Destination All Traffic(대상 모든 트래픽)에 대해 설정된 경우 클라이언트-투-사이트 VPN 이 작동하지 않습니다.

사용자 그룹

사용자 그룹은 라우터에서 동일한 서비스 집합을 공유하는 사용자 모음에 대해 생성됩니다. 이러한 사용자 그룹에는 VPN에 액세스하는 방법에 대한 권한 목록과 같은 그룹에 대한 옵션이 포함됩니다. 디바이스에 따라 PPTP, 사이트 간 IPSec VPN 및 클라이언트-사이트 간 IPSec VPN을 허용할 수 있습니다. 예를 들어 RV260에는 OpenVPN을 포함하는 옵션이 있지만 L2TP는 지원되지 않습니다. RV340 시리즈에는 SSL VPN용 AnyConnect는 물론 Captive Portal 또는 EZ VPN도 탑재되어 있습니다.

이러한 설정을 통해 관리자는 권한이 있는 사용자만 네트워크에 액세스할 수 있도록 제어하고 필터링할 수 있습니다. Shrew 소프트 및 TheGreenBow는 다운로드 가능한 가장 일반적인 VPN 클라이언트 중 하나입니다. 라우터의 VPN 설정에 따라 VPN 터널을 성공적으로 설정하도록 구성해야 합니다. 다음 문서에서는 사용자 그룹 생성에 대해 구체적으로 설명합니다.

- RV34x 라우터에서 VPN 설정을 위한 사용자 그룹 생성

VPN에 대한 사용자 그룹을 설정할 때 기본 관리자 계정을 관리자 그룹에 유지하고 VPN에 대한 새 사용자 계정 및 사용자 그룹을 만들어야 합니다. 관리자 계정을 다른 그룹으로 이동하면 라우터에 로그인할 수 없게 됩니다. 따라서 공장 초기화를 수행하고 관리 그룹의 기본 관리자 계정을 그대로 두고 해당 라우터에 대해 다시 구성해야 합니다.

사용자 계정

PPTP, VPN 클라이언트, 웹 GUI(Graphical User Interface) 로그인, SSLVPN(Secure Sockets Layer Virtual Private Network) 등의 다양한 서비스에 대해 로컬 데이터베이스를 사용하여 로컬 사용자를 인증할 수 있도록 라우터에 사용자 계정이 생성됩니다. 이를 통해 관리자는 네트워크에 액세스하기 위한 권한 있는 사용자만 제어하고 필터링할 수 있습니다. 다음 문서에서는 사용자 계정 생성에 대해 구체적으로 설명합니다.

- RV34x 라우터에서 VPN 클라이언트 설정을 위한 사용자 계정 생성

클라이언트 위치에서 클라이언트-사이트

클라이언트-사이트 VPN 연결에서 인터넷의 클라이언트는 서버에 연결하여 서버 뒤에 있는 회사 네트워크 또는 LAN에 액세스할 수 있지만 네트워크 및 리소스의 보안은 그대로 유지됩니다. 이 기능은 재택 근무자 및 비즈니스 여행자가 개인 정보 보호 및 보안에 영향을 주지 않고 VPN 클라이언트 소프트웨어를 사용하여 네트워크에 액세스할 수 있는 새로운 VPN 터널을 만들기 때문에 매우 유용합니다. VPN은 데이터를 보내고 받을 때 데이터를 암호화하고 해독하도록 설정됩니다.

AnyConnect 애플리케이션은 SSL VPN에서 작동하며 RV34x 라우터와 함께 사용됩니다. 다른 RV 시리즈 라우터에서는 사용할 수 없습니다. 버전 1.0.3.15부터는 라우터 라이센스가 더 이상 필요하지 않지만 VPN의 클라이언트 측에 대한 라이센스를 구매해야 합니다. Cisco AnyConnect Secure

Mobility Client에 대한 자세한 내용을 보려면 여기를 클릭하십시오. 설치에 대한 지침을 보려면 다음 문서 중에서 선택하십시오.

- Mac 컴퓨터에 Cisco AnyConnect Secure Mobility Client 다운로드 및 설치
- Windows 컴퓨터에 Cisco AnyConnect Secure Mobility Client를 다운로드 및 설치

모든 RV Series 라우터를 사용하는 클라이언트-사이트 VPN에 사용할 수 있는 일부 서드파티 애플리케이션이 있습니다. 앞에서 설명한 것처럼 Cisco는 이러한 애플리케이션을 지원하지 않습니다. 이 정보는 지침을 위해 제공되고 있습니다.

GreenBow VPN Client는 호스트 디바이스에서 클라이언트-사이트 IPsec 터널 또는 SSL에 대한 보안 연결을 구성할 수 있도록 해주는 서드파티 VPN 클라이언트 애플리케이션입니다. 이는 지원이 포함된 유료 애플리케이션입니다.

- GreenBow IPsec VPN Client를 설정하고 사용하여 RV160 및 RV260 라우터와 연결

OpenVPN은 SSL VPN에 대해 설정 및 사용할 수 있는 무료 오픈 소스 애플리케이션입니다. 클라이언트-서버 연결을 사용하여 인터넷을 통해 서버와 원격 클라이언트 위치 간의 보안 통신을 제공합니다.

- RV160 및 RV260 라우터의 OpenVPN

Shrew Soft는 IPsec VPN에도 설정하고 사용할 수 있는 무료 오픈 소스 애플리케이션입니다. 클라이언트-서버 연결을 사용하여 인터넷을 통해 서버와 원격 클라이언트 위치 간의 보안 통신을 제공합니다.

- RV160 및 RV260으로 Shrew Soft VPN Client 구성

Easy VPN은 일반적으로 RV32x 라우터에서 사용되었습니다. 다음은 참조할 수 있는 정보입니다.

- RV320 및 RV325 VPN Router Series에서 Easy Client to Gateway Virtual Private Network(VPN) 구성
- Cisco Easy VPN Q&A
- Cisco IOS 소프트웨어 기반 라우터의 Easy VPN

설치 마법사

최신 Cisco RV Series 라우터에는 설치 단계를 안내하는 VPN Setup Wizard가 있습니다. VPN Setup Wizard(VPN 설정 마법사)를 사용하면 기본 LAN-to-LAN 및 원격 액세스 VPN 연결을 구성하고 인증을 위해 사전 공유 키 또는 디지털 인증서를 할당할 수 있습니다. 자세한 내용은 다음 문서를 참조하십시오.

- RV160 및 RV260에서 VPN 설정 마법사 구성
- RV34x Series Router에서 설정 마법사를 사용하여 VPN(Virtual Private Network) 연결 구성

결론

이 문서에서는 VPN에 대한 더 나은 이해와 함께 길을 안내해 주는 팁을 제공합니다. 이제 직접 구성할 준비를 해야 합니다! 잠시 시간을 내어 링크를 보고 Cisco RV Series 라우터에 VPN을 설정하는 가장 좋은 방법을 결정하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.