ASA 및 Native L2TP-IPSec Android 클라이언트 컨피그레이션 예

목차

소개

IPSec을 통한 L2TP(Layer 2 Tunneling Protocol)는 단일 플랫폼에서 IPSec VPN 및 방화벽 서비스와 함께 L2TP VPN 솔루션을 구축하고 관리하는 기능을 제공합니다.원격 액세스 시나리오에서 L2TP over IPSec의 컨피그레이션의 주요 이점은 원격 사용자가 게이트웨이 또는 전용 회선 없이 공용 IP 네트워크를 통해 VPN에 액세스할 수 있다는 것입니다. 이 경우 POTS(Plain Old Telephone Service)를 통해 거의 모든 장소에서 원격 액세스를 수행할 수 있습니다. 또 다른 이점은 VPN 액세스를 위한 유일한 클라이언트 요구 사항은 Windows와 Microsoft DUN(Dial-Up Networking)을 사용하는 것입니다. Cisco VPN 클라이언트 소프트웨어와 같은 추가 클라이언트 소프트웨어는 필요하지 않습니다.

이 문서에서는 네이티브 L2TP/IPSec Android 클라이언트에 대한 샘플 컨피그레이션을 제공합니다.Cisco ASA(Adaptive Security Appliance)에 필요한 모든 명령과 Android 디바이스 자체에서 수행해야 하는 단계를 안내합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Android L2TP/IPSec에는 Cisco ASA 소프트웨어 버전 8.2.5 이상, 버전 8.3.2.12 이상 또는 버전 8.4.1 이상이 필요합니다.
- L2TP/IPSec 프로토콜을 사용할 때 ASA는 Microsoft Windows 7 및 Android 네이티브 VPN 클라이언트에 대해 SHA2(Secure Hash Algorithm 2) 인증서 시그니처 지원을 지원합니다.
- CLI, 8.4 및 8.6을 사용하는 Cisco ASA 5500 Series 컨피그레이션 가이드를 참조하십시오 .L2TP over IPSec 구성:L2TP over IPSec의 라이센싱 요구 사항

이 문서의 정보는 특정 랩 환경의 디바이스에서 생성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하기 위해 필요한 정보에 대해 설명합니다.

Android에서 L2TP/IPSec 연결 구성

다음 절차에서는 Android에서 L2TP/IPSec 연결을 구성하는 방법에 대해 설명합니다.

1. 메뉴를 열고 **설정**을 선택합니다.
2. Wireless **and Network** 또는 **Wireless Controls를 선택합니다**.사용 가능한 옵션은 Android 버전에 따라 다릅니다.
3. **VPN Settings를 선택합니다**.
4. Add **VPN(VPN 추가)을 선택합니다**.
5. Add **L2TP/IPsec PSK VPN을 선택합니다**.
6. **VPN Name(VPN 이름)**을 선택하고 설명 이름을 입력합니다.
7. Set **VPN Server(VPN 서버 설정)**를 선택하고 설명 이름을 입력합니다.
8. Set **IPSec pre-shared key를 선택합니다**.
9. Enable **L2TP secret(L2TP 암호 활성화)를 선택 취소합니다**.
10. [선택 사항] IPSec 식별자를 ASA 터널 그룹 이름으로 설정합니다.No 설정은 ASA의 DefaultRAGroup에 해당함을 의미합니다.
11. 메뉴를 열고 [저장]을 **선택합니다**.

ASA에서 L2TP/IPSec 연결 구성

이는 L2TP over IPSec 프로토콜을 사용할 때 네이티브 VPN 클라이언트가 ASA에 VPN 연결을 만들 수 있도록 엔드포인트의 운영 체제와 통합된 기본 VPN 클라이언트를 허용하는 필수 ASA IKEv1(IKEv1)(Internet Security Association and Key Management Protocol[ISAKMP]) 정책 설정입니다.

- IKEv1 1단계 - SHA1 해시 방법을 사용한 3DES(Triple Data Encryption Standard) 암호화
- MD5(Message Digest 5) 또는 SHA 해시 방법을 사용하는 IPSec 2단계 - 3DES 또는 AES(Advanced Encryption Standard) 암호화

- PPP 인증 - PAP(Password Authentication Protocol), MS-CHAPv1(Microsoft Challenge Handshake Authentication Protocol version 1) 또는 MS-CHAPv2(기본 설정)
- 사전 공유 키

  참고:ASA는 로컬 데이터베이스에서 PPP 인증 PAP 및 MS-CHAP(버전 1 및 2)만 지원합니다.EAP(Extensible Authentication Protocol) 및 CHAP는 프록시 인증 서버에 의해 수행됩니다.따라서 원격 사용자가 **authentication eap-proxy** 또는 **authentication chap** 명령으로 구성된 터널 그룹에 속하고 ASA가 로컬 데이터베이스를 사용하도록 구성된 경우 해당 사용자는 연결할 수 없습니다.

  또한 Android는 PAP를 지원하지 않으며 LDAP(Lightweight Directory Access Protocol)는 MS-CHAP를 지원하지 않으므로 LDAP는 실행 가능한 인증 메커니즘이 아닙니다.유일한 해결 방법은 RADIUS를 사용하는 것입니다.MS-CHAP 및 LDAP의 문제에 대한 자세한 내용은 Cisco Bug ID CSCtw58945, "L2TP over IPSec 연결이 ldap 권한 부여 및 mschapv2에서 실패"를 참조하십시오.

다음 절차에서는 ASA에서 L2TP/IPSec 연결을 구성하는 방법에 대해 설명합니다.

1. 그룹 정책의 클라이언트에 IP 주소를 할당하려면 로컬 주소 풀을 정의하거나 Adaptive Security Appliance에 dhcp-server를 사용합니다.
2. 내부 그룹 정책을 생성합니다. l2tp-ipsec이 될 터널 프로토콜을 정의합니다.클라이언트에서 사용할 DNS(도메인 이름 서버)를 구성합니다.
3. 새 터널 그룹을 생성하거나 기존 DefaultRAGroup의 특성을 수정합니다.(전화기에서 IPSec 식별자가 group-name으로 설정된 경우 새 터널 그룹을 사용할 수 있습니다.전화 컨피그레이션은 10단계를 참조하십시오.)
4. 사용되는 터널 그룹의 일반 특성을 정의합니다. 정의된 그룹 정책을 이 터널 그룹에 매핑합니다.이 터널 그룹에서 사용할 정의된 주소 풀을 매핑합니다.LOCAL 이외의 다른 것을 사용하려면 authentication-server 그룹을 수정합니다.
5. 사용할 터널 그룹의 IPSec 특성 아래에 사전 공유 키를 정의합니다.
6. chap, ms-chap-v1 및 ms-chap-v2만 사용하도록 사용되는 터널 그룹의 PPP 특성을 수정합니다.
7. ESP(Encapsulating Security Payload) 암호화 유형 및 인증 유형을 사용하여 변형 집합을 생성합니다.
8. IPSec에서 터널 모드가 아닌 전송 모드를 사용하도록 지시합니다.
9. SHA1 해시 방법을 사용하여 3DES 암호화를 사용하여 ISAKMP/IKEv1 정책을 정의합니다.
10. 동적 암호화 맵을 만들고 암호화 맵에 매핑합니다.
11. 인터페이스에 암호화 맵을 적용합니다.
12. 해당 인터페이스에서 ISAKMP를 활성화합니다.

ASA 호환성을 위한 구성 파일 명령

참고:이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

이 예에서는 모든 운영 체제에서 ASA가 네이티브 VPN 클라이언트와의 호환성을 보장하는 구성 파일 명령을 보여줍니다.

ASA 8.2.5 이상 컨피그레이션 예

```
Username <name> password <passwd> mschap
ip local pool l2tp-ipsec_address 192.168.1.1-192.168.1.10
group-policy l2tp-ipsec_policy internal
group-policy l2tp-ipsec_policy attributes
           dns-server value <dns_server>
           vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
           default-group-policy l2tp-ipsec_policy
           address-pool l2tp-ipsec_address
tunnel-group DefaultRAGroup ipsec-attributes
           pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
           no authentication pap
           authentication chap
           authentication ms-chap-v1
           authentication ms-chap-v2
crypto ipsec transform-set trans esp-3des esp-sha-hmac
crypto ipsec transform-set trans mode transport
crypto dynamic-map dyno 10 set transform-set set trans
crypto map vpn 65535 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto isakmp enable outside
crypto isakmp policy 10
           authentication pre-share
           encryption 3des
           hash sha
           group 2
           lifetime 86400
```

ASA 8.3.2.12 이상 컨피그레이션 예

```
Username <name> password <passwd> mschap
ip local pool l2tp-ipsec_address 192.168.1.1-192.168.1.10
group-policy l2tp-ipsec_policy internal
group-policy l2tp-ipsec_policy attributes
           dns-server value <dns_server>
           vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
           default-group-policy l2tp-ipsec_policy
           address-pool l2tp-ipsec_addresses
tunnel-group DefaultRAGroup ipsec-attributes
           pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
           no authentication pap
           authentication chap
           authentication ms-chap-v1
           authentication ms-chap-v2
crypto ipsec ikev1 transform-set my-transform-set-ikev1 esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport
crypto dynamic-map dyno 10 set ikev1 transform-set my-transform-set-ikev1
crypto map vpn 20 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto ikev1 enable outside
crypto ikev1 policy 10
           authentication pre-share
           encryption 3des
           hash sha
           group 2
           lifetime 86400
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

다음 절차에서는 연결을 설정하는 방법에 대해 설명합니다.

1. 메뉴를 열고 **설정**을 선택합니다.
2. Wireless **and Network** 또는 **Wireless Controls를 선택합니다**.사용 가능한 옵션은 Android 버전에 따라 다릅니다.
3. 목록에서 VPN 컨피그레이션을 선택합니다.
4. 사용자 이름과 비밀번호를 입력합니다.
5. Remember username(**사용자 이름 기억)을 선택합니다**.
6. Connect를 **선택합니다**.

이 절차에서는 연결을 끊는 방법에 대해 설명합니다.

1. 메뉴를 열고 **설정**을 선택합니다.
2. Wireless **and Network** 또는 **Wireless Controls를 선택합니다**.사용 가능한 옵션은 Android 버전에 따라 다릅니다.
3. 목록에서 VPN 컨피그레이션을 선택합니다.
4. 연결 **끊기를 선택합니다**.

이 명령을 사용하여 연결이 제대로 작동하는지 확인합니다.

- **show run crypto isakmp** - ASA 버전 8.2.5용
- **show run crypto ikev1** - ASA 버전 8.3.2.12 이상의 경우
- **show vpn-sessiondb ra-ikev1-ipsec -** ASA 버전 8.3.2.12 이상
- **show vpn-sessiondb remote -** ASA 버전 8.2.5용

  참고: Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령**을** 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

알려진 주의 사항

- Cisco 버그 ID CSCtq21535, "Android L2TP/IPsec 클라이언트에 연결할 때 ASA 추적"
- Cisco 버그 ID CSCtj57256, "Android에서 L2TP/IPSec 연결이 ASA55xx로 설정되지 않음"
- Cisco 버그 ID CSCtw58945, "L2TP over IPSec 연결은 ldap 권한 부여 및 mschapv2로 실패"

관련 정보

- CLI를 사용하는 Cisco ASA 5500 Series 컨피그레이션 가이드, 8.4 및 8.6:L2TP over IPsec 구성
- Cisco ASA 5500 Series 버전 8.4(x)의 릴리스 정보
- CLI를 사용하는 Cisco ASA 5500 Series 컨피그레이션 가이드, 8.3:NAT 정보
- ASA Pre-8.3~8.3 NAT 컨피그레이션 예
- 기술 지원 및 문서 – Cisco Systems