ASA und nativer L2TP-IPSec Android Client - Konfigurationsbeispiel

Inhalt

Einführung

Layer 2 Tunneling Protocol (L2TP) über IPSec ermöglicht die Bereitstellung und Verwaltung einer L2TP-VPN-Lösung zusammen mit IPSec VPN- und Firewall-Services in einer einzigen Plattform. Der Hauptvorteil der Konfiguration von L2TP über IPSec in einem Remote-Zugriffsszenario besteht darin, dass Remote-Benutzer über ein öffentliches IP-Netzwerk ohne Gateway oder dedizierte Leitung auf ein VPN zugreifen können, wodurch der Remote-Zugriff von praktisch jedem Ort aus möglich ist, der über einen herkömmlichen Telefondienst (Plain Old Telefone Service, POTS) verfügt. Ein weiterer Vorteil ist, dass der einzige Client, der einen VPN-Zugriff benötigt, die Verwendung von Windows mit Microsoft Dial-Up Networking (DUN) ist. Es ist keine zusätzliche Client-Software wie die Cisco VPN-Client-Software erforderlich.

Dieses Dokument enthält eine Beispielkonfiguration für den nativen L2TP/IPSec-Android-Client. Sie führt Sie durch alle erforderlichen Befehle für eine Cisco Adaptive Security Appliance (ASA) sowie die Schritte, die auf dem Android-Gerät selbst ausgeführt werden müssen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Für Android L2TP/IPSec ist die Cisco ASA-Software Version 8.2.5 oder höher, Version 8.3.2.12 oder höher oder Version 8.4.1 oder höher erforderlich.
- ASA unterstützt die Unterstützung von SHA2-Zertifikatssignaturen (Secure Hash Algorithm 2) für Microsoft Windows 7- und Android-native VPN-Clients, wenn das L2TP/IPSec-Protokoll verwendet wird.
- Siehe Konfigurationsleitfaden zur Cisco Serie ASA 5500 mit den CLI, 8.4 und 8.6: Konfigurieren von L2TP über IPSec: Lizenzanforderungen für L2TP über IPSec.

Die Informationen in diesem Dokument wurden von Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

In diesem Abschnitt werden die Informationen beschrieben, die zur Konfiguration der in diesem Dokument beschriebenen Funktionen erforderlich sind.

Konfigurieren der L2TP/IPSec-Verbindung auf dem Android-Gerät

Dieses Verfahren beschreibt, wie die L2TP/IPSec-Verbindung auf dem Android-Gerät konfiguriert wird:

1. Öffnen Sie das Menü, und wählen Sie **Einstellungen**.
2. Wählen Sie **Wireless- und Netzwerk-** oder **Wireless-Steuerelemente aus**. Die verfügbare Option hängt von Ihrer Android-Version ab.
3. Wählen Sie **VPN-Einstellungen aus**.
4. Wählen Sie **VPN hinzufügen aus**.
5. Wählen Sie **L2TP/IPsec PSK VPN hinzufügen aus**.
6. Wählen Sie **VPN Name**, und geben Sie einen beschreibenden Namen ein.
7. Wählen Sie **VPN-Server festlegen**, und geben Sie einen beschreibenden Namen ein.
8. Wählen Sie **IPSec Pre-shared Key festlegen aus**.
9. Deaktivieren Sie **L2TP geheim aktivieren**.
10. [Optional] Legen Sie die IPSec-Kennung als ASA-Tunnelgruppennamen fest. Keine Einstellung bedeutet, dass sie in die DefaultRAG-Gruppe der ASA fällt.
11. Öffnen Sie das Menü, und wählen Sie **Speichern aus**.

Konfigurieren der L2TP/IPSec-Verbindung auf der ASA

Dies sind die erforderlichen Richtlinieneinstellungen für die ASA Internet Key Exchange Version 1 (IKEv1) (Internet Security Association and Key Management Protocol [ISAKMP]), die es nativen VPN-Clients, die in das Betriebssystem auf einem Endgerät integriert sind, ermöglichen, eine

VPN-Verbindung zur ASA herzustellen, wenn L2TP über IPSec verwendet wird:

- IKEv1 Phase 1 - 3DES-Verschlüsselung (Triple Data Encryption Standard) mit SHA1-Hash-Methode
- IPSec Phase 2 - 3DES- oder AES-Verschlüsselung (Advanced Encryption Standard) mit Message Digest 5 (MD5)- oder SHA-Hash-Methode
- PPP-Authentifizierung - Password Authentication Protocol (PAP), Microsoft Challenge Handshake Authentication Protocol Version 1 (MS-CHAPv1) oder MS-CHAPv2 (bevorzugt)
- Vorläufiger gemeinsamer Schlüssel

  Hinweis: Die ASA unterstützt nur die PPP-Authentifizierungen PAP und MS-CHAP (Versionen 1 und 2) in der lokalen Datenbank. Das Extensible Authentication Protocol (EAP) und CHAP werden von Proxy-Authentifizierungsservern durchgeführt. Wenn ein Remote-Benutzer zu einer Tunnelgruppe gehört, die mit den **Authentifizierungs-EAP-Proxy-** oder **Authentifizierungsschlüssel-**Befehlen konfiguriert ist und die ASA für die Verwendung der lokalen Datenbank konfiguriert ist, kann dieser Benutzer keine Verbindung herstellen.

  Darüber hinaus unterstützt Android PAP nicht, und da das Lightweight Directory Access Protocol (LDAP) MS-CHAP nicht unterstützt, ist LDAP kein praktikabler Authentifizierungsmechanismus. Die einzige Problemumgehung ist die Verwendung von RADIUS. Weitere Informationen zu Problemen mit MS-CHAP und LDAP finden Sie unter Cisco Bug ID CSCtw58945 "L2TP over IPSec connections fail with ldap autorization and mschapv2".

In diesem Verfahren wird beschrieben, wie die L2TP/IPSec-Verbindung auf der ASA konfiguriert wird:

1. Definieren Sie einen lokalen Adresspool, oder verwenden Sie einen DHCP-Server für die Adaptive Security Appliance, um den Clients für die Gruppenrichtlinie IP-Adressen zuzuweisen.
2. Erstellen Sie eine interne Gruppenrichtlinie. Legen Sie als Tunnelprotokoll l2tp-ipsec fest.Konfigurieren Sie einen DNS (Domain Name Server), der von den Clients verwendet werden soll.
3. Erstellen Sie eine neue Tunnelgruppe, oder ändern Sie die Attribute der vorhandenen DefaultRAGroup. (Eine neue Tunnelgruppe kann verwendet werden, wenn die IPSec-ID auf dem Telefon als Gruppenname festgelegt ist. Siehe Schritt 10 für die Telefonkonfiguration.)
4. Definieren Sie die allgemeinen Attribute der verwendeten Tunnelgruppe. Ordnen Sie die definierte Gruppenrichtlinie dieser Tunnelgruppe zu.Ordnen Sie den von dieser Tunnelgruppe zu verwendenden definierten Adresspool zu.Ändern Sie die Authentifizierungsserver-Gruppe, wenn Sie etwas Anderes als LOCAL verwenden möchten.
5. Definieren Sie den vorinstallierten Schlüssel unter den IPSec-Attributen der zu verwendenden Tunnelgruppe.
6. Ändern Sie die PPP-Attribute der Tunnelgruppe, die verwendet werden, sodass nur chap, ms-chap-v1 und ms-chap-v2 verwendet werden.
7. Erstellen Sie einen Transformationssatz mit einem bestimmten Verschlüsselungstyp und Authentifizierungstyp für die Kapselung der ESP-Verschlüsselung.
8. Weisen Sie IPSec an, den Transportmodus anstelle des Tunnelmodus zu verwenden.
9. Definieren Sie eine ISAKMP/IKEv1-Richtlinie mithilfe der 3DES-Verschlüsselung mit der SHA1-Hash-Methode.

10. Erstellen Sie eine dynamische Crypto Map, und ordnen Sie sie einer Crypto Map zu.
11. Wenden Sie die Crypto Map auf eine Schnittstelle an.
12. Aktivieren Sie ISAKMP auf dieser Schnittstelle.

Konfigurationsdateibefehle für die ASA-Kompatibilität

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

In diesem Beispiel werden die Befehle in der Konfigurationsdatei veranschaulicht, die die ASA-Kompatibilität mit einem nativen VPN-Client auf jedem Betriebssystem sicherstellen.

ASA 8.2.5 oder höher Konfigurationsbeispiel

```
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
```

Konfigurationsbeispiel für ASA 8.3.2.12 oder höher

```
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
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

In diesem Verfahren wird beschrieben, wie Sie die Verbindung einrichten:

1. Öffnen Sie das Menü, und wählen Sie **Einstellungen**.
2. Wählen Sie **Wireless- und Netzwerk-** oder **Wireless-Steuerelemente aus**. (Die verfügbare Option hängt von Ihrer Android-Version ab.)
3. Wählen Sie die VPN-Konfiguration aus der Liste aus.
4. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.
5. Wählen Sie **Benutzernamen speichern aus**.
6. Wählen Sie **Verbinden aus**.

In diesem Verfahren wird beschrieben, wie Sie die Verbindung trennen:

1. Öffnen Sie das Menü, und wählen Sie **Einstellungen**.
2. Wählen Sie **Wireless- und Netzwerk-** oder **Wireless-Steuerelemente aus**. (Die verfügbare Option hängt von Ihrer Android-Version ab.)
3. Wählen Sie die VPN-Konfiguration aus der Liste aus.
4. Wählen Sie **Trennen aus**.

Verwenden Sie diese Befehle, um zu überprüfen, ob Ihre Verbindung ordnungsgemäß funktioniert.

- **show run crypto isakmp** - Für ASA Version 8.2.5
- **show run crypto ikev1** - Für ASA Version 8.3.2.12 oder höher
- **show vpn-sessiondb ra-ikev1-ipsec -** Für ASA Version 8.3.2.12 oder höher
- **show vpn-sessiondb remote -** Für ASA Version 8.2.5

  Hinweis: Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Bekannte Einwände

- Cisco Bug-ID CSCtq21535, "ASA traceback when connected with Android L2TP/IPsec client"
- Cisco Bug-ID CSCtj57256, "L2TP/IPSec-Verbindung von Android wird nicht zur ASA55xx hergestellt"
- Cisco Bug-ID CSCtw58945: "L2TP over IPSec-Verbindungen schlagen mit LDAP-Autorisierung und mschapv2 fehl"

Zugehörige Informationen

- Konfigurationsanleitung für die Cisco Serie ASA 5500 unter Verwendung der CLI, 8.4 und 8.6: Konfigurieren von L2TP über IPsec
- Versionshinweise für die Cisco Serie ASA 5500, Version 8.4(x)
- Konfigurationsanleitung für die Cisco Serie ASA 5500 unter Verwendung der CLI 8.3: Informationen zur NAT
- ASA-NAT-Konfigurationsbeispiele vor 8.3 bis 8.3
- Technischer Support und Dokumentation - Cisco Systems