Esempio di configurazione di ASA e client Android L2TP-IPSec nativo

Sommario

Introduzione

Il protocollo L2TP (Layer 2 Tunneling Protocol) su IPSec consente di distribuire e amministrare una soluzione VPN L2TP insieme ai servizi VPN e firewall IPSec in un'unica piattaforma. Il vantaggio principale della configurazione di L2TP su IPSec in uno scenario di accesso remoto è che gli utenti remoti possono accedere a una VPN su una rete IP pubblica senza un gateway o una linea dedicata, il che consente l'accesso remoto praticamente da qualsiasi luogo con POTS (Plain Old Telephone Service). Un ulteriore vantaggio è che l'unico requisito del client per l'accesso VPN è l'utilizzo di Windows con Microsoft Dial-Up Networking (DUN). Non è necessario alcun software client aggiuntivo, ad esempio il software client VPN Cisco.

In questo documento viene fornita una configurazione di esempio per il client Android L2TP/IPSec nativo. Permette di eseguire tutti i comandi necessari richiesti su una Cisco Adaptive Security Appliance (ASA), nonché i passaggi da eseguire sullo stesso dispositivo Android.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Android L2TP/IPSec richiede il software Cisco ASA versione 8.2.5 o successive, versione 8.3.2.12 o successive o versione 8.4.1 o successive.
- ASA supporta il supporto della firma del certificato SHA2 (Secure Hash Algorithm 2) per client VPN nativi di Microsoft Windows 7 e Android quando si utilizza il protocollo L2TP/IPSec.
- Vedere la guida alla configurazione di Cisco ASA serie 5500 dall'interfaccia CLI, versione 8.4 e 8.6: Configurazione di L2TP su IPSec: Requisiti di licenza per L2TP su IPSec.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

In questa sezione vengono descritte le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Configurare la connessione L2TP/IPSec su Android

In questa procedura viene descritto come configurare la connessione L2TP/IPSec su Android:

1. Aprire il menu e scegliere **Impostazioni**.
2. Scegliere **Wireless e Rete** o **Controlli wireless**. L'opzione disponibile dipende dalla versione di Android in uso.
3. Scegliere **Impostazioni VPN**.
4. Scegliere **Aggiungi VPN**.
5. Scegliere **Aggiungi VPN PSK L2TP/IPsec**.
6. Scegliere **Nome VPN** e immettere un nome descrittivo.
7. Scegliere **Imposta server VPN** e immettere un nome descrittivo.
8. Scegliere **Imposta chiave già condivisa IPSec**.
9. Deselezionare **Abilita segreto L2TP**.
10. [Facoltativo] Impostare l'identificatore IPSec come nome del gruppo di tunnel ASA. Se non si specifica alcuna impostazione, il gruppo ricadrà in DefaultRAGroup sull'appliance ASA.
11. Aprire il menu e scegliere **Salva**.

Configurazione della connessione L2TP/IPSec sull'appliance ASA

Di seguito sono riportate le impostazioni dei criteri ASA Internet Key Exchange versione 1 (IKEv1) (Internet Security Association and Key Management Protocol [ISAKMP]) che consentono ai client VPN nativi, integrati con il sistema operativo di un endpoint, di stabilire una connessione VPN all'appliance ASA quando viene utilizzato il protocollo L2TP su IPSec:

- Fase 1 di IKEv1 - crittografia 3DES (Triple Data Encryption Standard) con metodo hash SHA1

- Crittografia IPSec fase 2 - 3DES o AES (Advanced Encryption Standard) con MD5 (Message Digest 5) o metodo di hash SHA
- Autenticazione PPP - Protocollo PAP (Password Authentication Protocol), Microsoft Challenge Handshake Authentication Protocol versione 1 (MS-CHAPv1) o MS-CHAPv2 (preferibile)
- Chiave già condivisa

Nota: L'ASA supporta solo le autenticazioni PPP PAP e MS-CHAP (versioni 1 e 2) sul database locale. Il protocollo EAP (Extensible Authentication Protocol) e la protezione CHAP vengono eseguiti dai server di autenticazione proxy. Pertanto, se un utente remoto appartiene a un gruppo di tunnel configurato con i comandi **authentication eap-proxy** o **authentication chap** e l'ASA è configurata per utilizzare il database locale, tale utente non sarà in grado di connettersi.

Inoltre, Android non supporta PAP e, poiché il protocollo LDAP (Lightweight Directory Access Protocol) non supporta MS-CHAP, LDAP non è un meccanismo di autenticazione valido. L'unica soluzione è utilizzare RADIUS. Per ulteriori informazioni sui problemi relativi a MS-CHAP e LDAP, vedere l'ID bug Cisco CSCtw58945, "L2TP over IPSec connections fail with ldap authorization and mschapv2" (Le connessioni L2TP su IPSec hanno esito negativo con l'autorizzazione LDAP e mschapv2).

In questa procedura viene descritto come configurare la connessione L2TP/IPSec sull'appliance ASA:

1. Definire un pool di indirizzi locali o utilizzare un server dhcp per l'appliance Adaptive Security per allocare gli indirizzi IP ai client per i Criteri di gruppo.
2. Creare un criterio di gruppo interno. Definire il protocollo del tunnel come l2tp-ipsec.Configurare un server dei nomi di dominio (DNS) che verrà utilizzato dai client.
3. Creare un nuovo gruppo di tunnel o modificare gli attributi dell'oggetto DefaultRAGroup esistente. (È possibile utilizzare un nuovo gruppo di tunnel se l'identificatore IPSec è impostato come nome di gruppo sul telefono; vedere il punto 10 per la configurazione del telefono.)
4. Definire gli attributi generali del gruppo di tunnel utilizzato. Eseguire il mapping dei Criteri di gruppo definiti a questo gruppo di tunnel.Eseguire il mapping del pool di indirizzi definito da utilizzare per questo gruppo di tunnel.Modificare il gruppo di server di autenticazione se si desidera utilizzare un valore diverso da LOCAL.
5. Definire la chiave già condivisa negli attributi IPSec del gruppo di tunnel da utilizzare.
6. Modificare gli attributi PPP del gruppo di tunnel utilizzati in modo che vengano utilizzati solo i protocolli chap, ms-chap-v1 e ms-chap-v2.
7. Creare un set di trasformazioni con un tipo di crittografia ESP (Encapsulating Security Payload) e un tipo di autenticazione specifici.
8. Indicare a IPSec di utilizzare la modalità di trasporto anziché la modalità tunnel.
9. Definire un criterio ISAKMP/IKEv1 utilizzando la crittografia 3DES con il metodo hash SHA1.
10. Creare una mappa crittografica dinamica e mapparla a una mappa crittografica.
11. Applicare la mappa crittografica a un'interfaccia.
12. Abilitare ISAKMP su tale interfaccia.

Comandi del file di configurazione per la compatibilità ASA

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

In questo esempio vengono mostrati i comandi del file di configurazione che garantiscono la compatibilità dell'ASA con un client VPN nativo su qualsiasi sistema operativo.

Esempio di configurazione di ASA 8.2.5 o versioni successive

```
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
```

Esempio di configurazione di ASA 8.3.2.12 o versioni successive

```
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
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

In questa procedura viene descritto come impostare la connessione:

1. Aprire il menu e scegliere **Impostazioni**.
2. Selezionare **Wireless e Rete** o **Controlli wireless**. L'opzione disponibile dipende dalla versione di Android in uso.
3. Selezionare la configurazione VPN dall'elenco.
4. Immettere il nome utente e la password.
5. Selezionare **Memorizza nome utente**.
6. Selezionare **Connetti**.

In questa procedura viene descritto come disconnettersi:

1. Aprire il menu e scegliere **Impostazioni**.
2. Selezionare **Wireless e Rete** o **Controlli wireless**. L'opzione disponibile dipende dalla versione di Android in uso.
3. Selezionare la configurazione VPN dall'elenco.
4. Selezionare **Disconnetti**.

Utilizzare questi comandi per verificare che la connessione funzioni correttamente.

- **show run crypto isakmp** - Per ASA versione 8.2.5
- **show run crypto ikev1** - Per ASA versione 8.3.2.12 o successive
- **show vpn-sessiondb ra-ikev1-ipsec -** Per ASA versione 8.3.2.12 o successive
- **show vpn-sessiondb remote -** Per ASA versione 8.2.5

  Nota: Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi show. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

Avvertenze note

- ID bug Cisco CSCtq21535, "ASA traceback when connecting with Android L2TP/IPsec client"
- ID bug Cisco CSCtj57256, "La connessione L2TP/IPSec da Android non viene stabilita con ASA55xx"
- ID bug Cisco CSCtw58945, "L2TP over IPSec connections fail with ldap authorization and

mschapv2" (Le connessioni L2TP su IPSec hanno esito negativo con l'autorizzazione LDAP e mschapv2)

Informazioni correlate

- Guida alla configurazione di Cisco ASA serie 5500 dall'interfaccia CLI, 8.4 e 8.6: Configurazione di L2TP su IPsec
- Note sulla versione per Cisco ASA serie 5500, versione 8.4(x)
- Guida alla configurazione di Cisco ASA serie 5500 dall'interfaccia CLI, 8.3: Informazioni su NAT
- Esempi di configurazione ASA precedenti alla versione 8.3 o 8.3 NAT
- Documentazione e supporto tecnico – Cisco Systems