Configuration du protocole de tunnelisation de couche 2 sur IPSec

Contenu

Introduction

Les protocoles de tunnellisation de couche 2, tels que L2TP, ne fournissent pas les mécanismes de chiffrement pour le trafic dans les tunnels. Au lieu de cela, ils se basent sur d'autres protocoles de sécurité, tels qu'IPSec, pour chiffrer leurs données. Utilisez cet exemple de configuration pour chiffrer le trafic L2TP à l'aide du protocole IPSec pour les utilisateurs qui se connectent par réseau commuté.

Le tunnel L2TP est établi entre le concentrateur L2TP Access (LAC) et le serveur de réseau L2TP (LNS). Un tunnel d'IPSec est également établi entre ces périphériques et tout le trafic de tunnel L2TP est chiffré utilisant IPSec.

Conditions préalables

Conditions requises

Ce document exige une compréhension de base de protocole IPsec. Pour se renseigner plus sur IPSec, référez-vous s'il vous plaît à une introduction au cryptage de sécurité IP (IPSec).

Composants utilisés

Les informations dans ce document sont basées sur les versions de logiciel et matériel suivantes :

- Version de logiciel 12.2(24a) de Cisco IOS®

- Routeurs de la gamme Cisco 2500

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés seulement).

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant. L'appel l'utilisateur initie une session PPP avec le LAC au-dessus du réseau téléphonique de téléphone analogique. Après que l'utilisateur soit authentifié, le LAC initie un tunnel L2TP au LNS. L'extrémité de tunnel se dirige, LAC et le LNS, s'authentifient avant que le tunnel soit créé. Une fois que le tunnel est établi, une session L2TP est créée pour l'utilisateur de connexion téléphonique. Pour chiffrer tout le trafic L2TP entre le LAC et le LNS, le trafic L2TP est défini comme trafic intéressant (le trafic à chiffrer) pour IPSec.

Configurations

Ce document utilise les configurations suivantes.

- Configuration LAC
- Configuration LNS

Configuration LAC

```
Current configuration:
!
version 12.2
service timestamps debug datetime msec localtime show-
timezone
service timestamps log datetime msec localtime show-
timezone
service password-encryption
!
hostname LAC
!
enable password  7 094F471A1A0A
!
!--- Usernames and passwords are used !--- for L2TP
```

```
tunnel authentication. username LAC password 7
0107130A550E0A1F205F5D username LNS password 7
001006080A5E07160E325F !--- Username and password used
for authenticating !--- the dial up user. username
dialupuser password 7 14131B0A00142B3837 ip subnet-zero
! !--- Enable VDPN. vpdn enable vpdn search-order domain
! !--- Configure vpdn group 1 to request dialin to the
LNS, !--- define L2TP as the protocol, and initiate a
tunnel to the LNS 20.1.1.2. !--- If the user belongs to
the domain cisco.com, !--- use the local name LAC as the
tunnel name. vpdn-group 1 request-dialin protocol l2tp
domain cisco.com initiate-to ip 20.1.1.2 local name LAC
! !--- Create Internet Key Exchange (IKE) policy 1, !---
which is given highest priority if there are additional
!--- IKE policies. Specify the policy using pre-shared
key !--- for authentication, Diffie-Hellman group 2,
lifetime !--- and peer address. crypto isakmp policy 1
authentication pre-share group 2 lifetime 3600 crypto
isakmp key cisco address 20.1.1.2 ! !--- Create an IPSec
transform set named "testtrans" !--- with the DES for
ESP with transport mode. !--- Note: AH is not used.
crypto ipsec transform-set testtrans esp-des ! !---
Create crypto map l2tpmap (assigned to Serial 0), using
IKE for !--- Security Associations with map-number 10 !-
-- and using "testrans" transform-set as a template. !--
- Set the peer and specify access list 101, which is
used !--- to determine which traffic (L2TP) is to be
protected by IPSec. crypto map l2tpmap 10 ipsec-isakmp
set peer 20.1.1.2 set transform-set testtrans match
address 101 ! interface Ethernet0 ip address 10.31.1.6
255.255.255.0 no ip directed-broadcast ! interface
Serial0 ip address 20.1.1.1 255.255.255.252 no ip
directed-broadcast no ip route-cache no ip mroute-cache
no fair-queue !--- Assign crypto map l2tpmap to the
interface. crypto map l2tpmap ! interface Async1 ip
unnumbered Ethernet0 no ip directed-broadcast
encapsulation ppp no ip route-cache no ip mroute-cache
async mode dedicated peer default ip address pool
my_pool ppp authentication chap ! !--- Create an IP Pool
named "my_pool" and !--- specify the IP range. ip local
pool my_pool 10.31.1.100 10.31.1.110 ip classless ip
route 0.0.0.0 0.0.0.0 Serial0 !--- Specify L2TP traffic
as interesting to use with IPSec. access-list 101 permit
udp host 20.1.1.1 eq 1701 host 20.1.1.2 eq 1701 ! line
con 0 exec-timeout 0 0 transport input none line 1
autoselect during-login autoselect ppp modem InOut
transport input all speed 38400 flowcontrol hardware
line aux 0 line vty 0 4 password
```

Configuration LNS

```
Current configuration:
!
version 12.2
service timestamps debug datetime msec localtime show-
timezone
service timestamps log datetime msec localtime show-
timezone
service password-encryption
!
hostname LNS
!
enable password 7 0822455D0A16
!--- Usernames and passwords are used for !--- L2TP
tunnel authentication. username LAC password 7
```

```
0107130A550E0A1F205F5D username LNS password 7
120D10191C0E00142B3837 !--- Username and password used
to authenticate !--- the dial up user. username
dialupuser@cisco.com password 7 104A0018090713181F ! ip
subnet-zero ! !--- Enable VDPN. vpdn enable ! !---
Configure VPDN group 1 to accept !--- an open tunnel
request from LAC, !--- define L2TP as the protocol, and
identify virtual-template 1 !--- to use for cloning
virtual access interfaces. vpdn-group 1 accept-dialin
protocol l2tp virtual-template 1 terminate-from hostname
LAC local name LNS ! !--- Create IKE policy 1, which is
!--- given the highest priority if there are additional
IKE policies. !--- Specify the policy using the pre-
shared key for authentication, !--- Diffie-Hellman group
2, lifetime and peer address. crypto isakmp policy 1
authentication pre-share group 2 lifetime 3600 crypto
isakmp key cisco address 20.1.1.1 ! ! !--- Create an
IPSec transform set named "testtrans" !--- using DES for
ESP with transport mode. !--- Note: AH is not used.
crypto ipsec transform-set testtrans esp-des ! !---
Create crypto map l2tpmap !--- (assigned to Serial 0),
using IKE for !--- Security Associations with map-number
10 !--- and using "testrans" transform-set as a
template. !--- Set the peer and specify access list 101,
which is used !--- to determine which traffic (L2TP) is
to be protected by IPSec. crypto map l2tpmap 10 ipsec-
isakmp set peer 20.1.1.1 set transform-set testtrans
match address 101 ! interface Ethernet0 ip address
200.1.1.100 255.255.255.0 no ip directed-broadcast no
keepalive ! !--- Create a virtual-template interface !--
- used for "cloning" !--- virtual-access interfaces
using address pool "mypool" !--- with Challenge
Authentication Protocol (CHAP) authentication. interface
Virtual-Template1 ip unnumbered Ethernet0 no ip
directed-broadcast no ip route-cache peer default ip
address pool mypool ppp authentication chap ! interface
Serial0 ip address 20.1.1.2 255.255.255.252 no ip
directed-broadcast no ip route-cache no ip mroute-cache
no fair-queue clockrate 1300000 !--- Assign crypto map
l2tpmap to the interface. crypto map l2tpmap ! !---
Create an IP Pool named "mypool" and !--- specify the IP
range. ip local pool mypool 200.1.1.1 200.1.1.10 ip
classless ! !--- Specify L2TP traffic as interesting to
use with IPSec. access-list 101 permit udp host 20.1.1.2
eq 1701 host 20.1.1.1 eq 1701 ! line con 0 exec-timeout
0 0 transport input none line aux 0 line vty 0 4
password login ! end
```

Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Utilisez ces **commandes show** de vérifier la configuration.

- show crypto isakmp sa - Affiche toutes les associations de sécurité actuelles d'IKE (SA) sur

un pair.

```
LAC#show crypto isakmp sa dst src state conn-id slot 20.1.1.2 20.1.1.1 QM_IDLE 1 0 LAC#
```

- show crypto ipsec sa — Affiche les paramètres utilisés par les SA.

```
LAC#show crypto ipsec sa interface: Serial0 Crypto map tag: l2tpmap, local addr. 20.1.1.1 local
ident (addr/mask/prot/port): (20.1.1.1/255.255.255.255/0/0) remote ident (addr/mask/prot/port):
(20.1.1.2/255.255.255.255/0/0) current_peer: 20.1.1.2 PERMIT, flags={transport_parent,} #pkts
encaps: 0, #pkts encrypt: 0, #pkts digest 0 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0,
#pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 20.1.1.1, remote
crypto endpt.: 20.1.1.2 path mtu 1500, ip mtu 1500, ip mtu interface Serial0 current outbound
spi: 0 inbound esp sas: inbound ah sas: inbound pcp sas: outbound esp sas: outbound ah sas:
outbound pcp sas: local ident (addr/mask/prot/port): (20.1.1.1/255.255.255.255/17/1701) remote
ident (addr/mask/prot/port): (20.1.1.2/255.255.255.255/17/1701) current_peer: 20.1.1.2 PERMIT,
flags={origin_is_acl,reassembly_needed,parent_is_transport,} #pkts encaps: 1803, #pkts encrypt:
1803, #pkts digest 0 #pkts decaps: 1762, #pkts decrypt: 1762, #pkts verify 0 #pkts compressed:
0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress
failed: 0 #send errors 5, #recv errors 0 local crypto endpt.: 20.1.1.1, remote crypto endpt.:
20.1.1.2 path mtu 1500, ip mtu 1500, ip mtu interface Serial0 current outbound spi: 43BE425B
inbound esp sas: spi: 0xCB5483AD(3411313581) transform: esp-des , in use settings ={Tunnel, }
slot: 0, conn id: 2000, flow_id: 1, crypto map: l2tpmap sa timing: remaining key lifetime
(k/sec): (4607760/1557) IV size: 8 bytes replay detection support: N inbound ah sas: inbound pcp
sas: outbound esp sas: spi: 0x43BE425B(1136542299) transform: esp-des , in use settings
={Tunnel, } slot: 0, conn id: 2001, flow_id: 2, crypto map: l2tpmap sa timing: remaining key
lifetime (k/sec): (4607751/1557) IV size: 8 bytes replay detection support: N outbound ah sas:
outbound pcp sas: LAC#
```

- show vpdn — Affiche les informations sur le tunnel L2TP actif.

```
LAC#show vpdn L2TP Tunnel and Session Information Total tunnels 1 sessions 1 LocID RemID Remote
Name State Remote Address Port Sessions 26489 64014 LNS est 20.1.1.2 1701 1 LocID RemID TunID
Intf Username State Last Chg Fastswitch 41 9 26489 As1 dialupuser@cisco.com est 00:12:21 enabled
%No active L2F tunnels %No active PPTP tunnels %No active PPPoE tunnels LAC#
```

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Remarque: Avant d'exécuter les commandes **debug**, référez-vous à la section **Informations importantes sur les commandes Debug**.

- **debug crypto engine** — Affiche des événements du moteur.
- **debug crypto ipsec** — Affiche des événements IPsec.
- **debug crypto isakmp**—Affichage de messages d'événements IKE.
- **debug ppp authentication** — Affiche des messages du protocole d'authentification, y compris des échanges de paquet de CHAP et des échanges de Password Authentication Protocol (PAP).
- **événement de debug vpdn** — Affiche des messages au sujet des événements qui sont partie de l'établissement normal d'un tunnel ou arrêt.
- **erreur de debug vpdn** — Affiche les erreurs qui empêchent un tunnel d'être établi ou les

erreurs qui causent un tunnel établi d'être fermé.
- **debug ppp negotiation** — Paquets PPP d'affichages transmis pendant le startup de PPP, où des options PPP sont négociées.

Informations connexes

- RFC 1825 d'IPSec
- Pages de support d'IPSec
- Sécurité des réseaux de configuration d'IPSec
- Configurer le protocole de sécurité IKE
- Support technique - Cisco Systems