

路由器到路由器加密DLSw流量

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[設定](#)

[網路圖表](#)

[組態](#)

[驗證](#)

[疑難排解](#)

[debug和show命令](#)

[相關資訊](#)

簡介

在本文檔的示例配置中，兩台路由器的環回介面之間設定了資料鏈路交換(DLSw)對等體。所有DLSw流量都會在它們之間加密。此組態適用於路由器傳輸的任何自產生流量。

在此配置中，加密訪問清單是通用的。使用者可以更加具體，並允許兩個環回地址之間的DLSw流量。通常，只有DLSw流量從環回介面傳輸到環回介面。

必要條件

需求

本文件沒有特定需求。

採用元件

使用以下軟體和硬體版本開發並測試此組態：

- Cisco IOS®軟體版本12.0。此組態已使用12.28T進行測試。
- Cisco 2500-is56i-l.120-7.T
- Cisco 2513

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

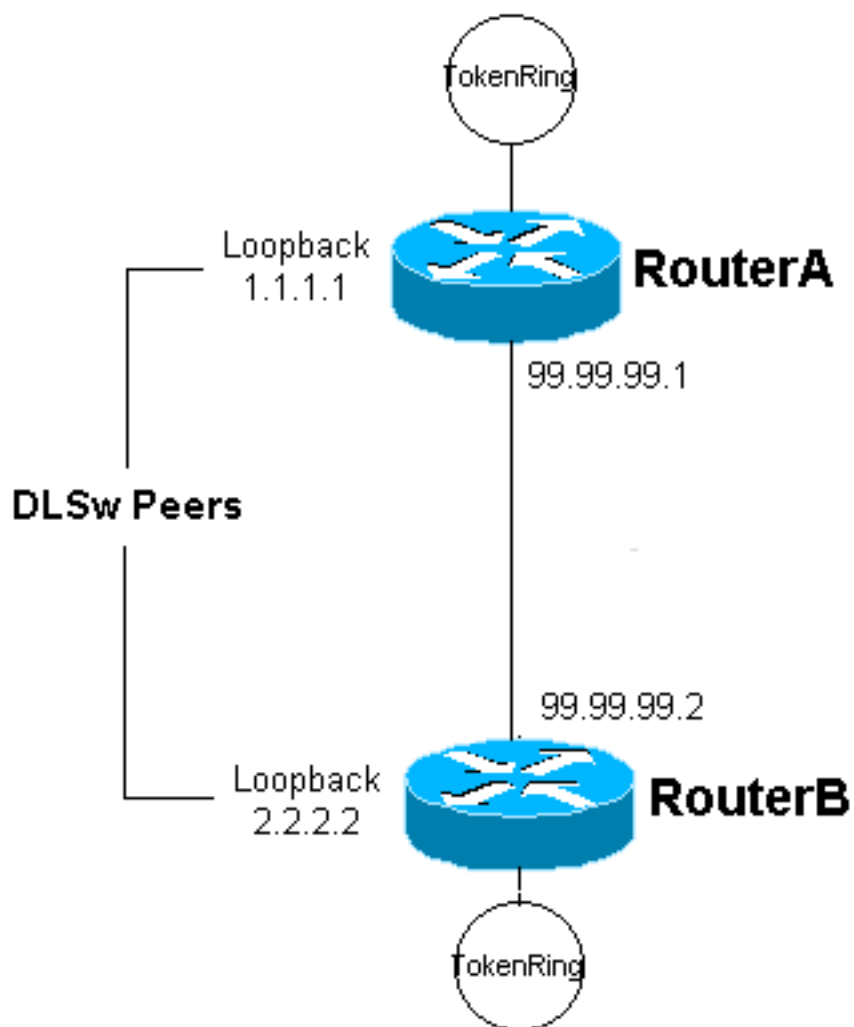
設定

本節提供用於設定本文中所述功能的資訊。

註：使用[Command Lookup Tool](#)(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

網路圖表

本檔案會使用以下網路設定：



組態

本檔案會使用以下設定：

- 路由器A
- 路由器B

路由器A

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
enable secret 5 $1$7WP3$aEqtNjvRJ9Vy6i41x0RJf0
enable password ww
!
ip subnet-zero
!
cns event-service server

source-bridge ring-group 20
dlsw local-peer peer-id 1.1.1.1
dlsw remote-peer 0 tcp 2.2.2.2
!
crypto isakmp policy 1
  hash md5
  authentication pre-share
crypto isakmp key cisco123 address 99.99.99.2
!
crypto ipsec transform-set dlswset esp-des esp-md5-hmac
!
crypto map dlswstuff 10 ipsec-isakmp
  set peer 99.99.99.2
  set transform-set dlswset
  match address 101
!
!
interface Loopback0
  ip address 1.1.1.1 255.255.255.0
  no ip directed-broadcast
!
interface TokenRing0
  ip address 10.2.2.3 255.255.255.0
  ring-speed 16
  source-bridge 2 3 20
  source-bridge spanning
  no ip directed-broadcast
  no mop enabled
!
interface Serial0
  ip address 99.99.99.1 255.255.255.0
  no ip directed-broadcast
  crypto map dlswstuff
!
ip classless
ip route 0.0.0.0 0.0.0.0 99.99.99.2
no ip http server
!
access-list 101 permit ip host 1.1.1.1 host 2.2.2.2
!
line con 0
  transport input none
line aux 0
line vty 0 4
  password ww
  login
!
end
```

路由器B

Current configuration:

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname RouterB  
!  
enable secret 5 $1$7WP3$SaEqtNjvRJ9Vy6i41x0RJf0  
enable password ww  
!  
ip subnet-zero  
!  
cns event-service server  
  
source-bridge ring-group 10  
dlsw local-peer peer-id 2.2.2.2  
dlsw remote-peer 0 tcp 1.1.1.1  
!  
crypto isakmp policy 1  
  hash md5  
  authentication pre-share  
crypto isakmp key cisco123 address 99.99.99.1  
!  
crypto ipsec transform-set dlswset esp-des esp-md5-hmac  
!  
crypto map dlswstuff 10 ipsec-isakmp  
  set peer 99.99.99.1  
  set transform-set dlswset  
  match address 101  
!  
!  
interface Loopback0  
  ip address 2.2.2.2 255.255.255.0  
  no ip directed-broadcast  
!  
interface TokenRing0  
  ip address 10.1.1.3 255.255.255.0  
  ring-speed 16  
  source-bridge 2 3 10  
  source-bridge spanning  
  no ip directed-broadcast  
  no mop enabled  
!  
interface Serial0  
  ip address 99.99.99.2 255.255.255.0  
  no ip directed-broadcast  
  crypto map dlswstuff  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 99.99.99.1  
no ip http server  
!  
access-list 101 permit ip host 2.2.2.2 host 1.1.1.1  
!  
line con 0  
  transport input none  
line aux 0  
line vty 0 4
```

```
password ww
login
!
end
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

使用本節內容，對組態進行疑難排解。

debug和show命令

[輸出直譯器工具](#)(僅供[已註冊](#)客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

附註：使用 debug 指令之前，請先參閱[有關 Debug 指令的重要資訊](#)。

- debug crypto ipsec — 此命令顯示第2階段的IP安全協定(IPSec)協商。
- debug crypto isakmp — 此命令顯示第1階段的網際網路安全關聯和金鑰管理協定(ISAKMP)協商。
- debug crypto engine — 此命令顯示加密的流量。
- show crypto ipsec sa — 顯示第2階段安全關聯。
- show crypto isakmp sa — 此命令顯示第1階段安全關聯。
- show dls w peer — 此命令顯示DLSw對等體狀態和連線狀態。

相關資訊

- [IPSec支援頁面](#)
- [DLSW支援頁面](#)
- [技術支援與文件 - Cisco Systems](#)