

ルータからルータへの暗号化 DLSw トラフィック

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[debug コマンドと show コマンド](#)

[関連情報](#)

概要

このドキュメントの設定例では、ループバック インターフェイス間で設定されたデータリンク スイッチング (DLSw) ピアを使用する 2 台のルータがあります。これらの間では、すべての DLSw トラフィックが暗号化されます。この設定は、ルータが送信するすべての自己生成トラフィックに動作します。

この設定では、暗号化アクセスリストは汎用です。ユーザはより具体的になり、2つのループバックアドレス間でDLSwトラフィックを許可できます。一般に、DLSwトラフィックだけがループバックインターフェイスからループバックインターフェイスに送信されます。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

この設定は、次のバージョンのソフトウェアとハードウェアを使用して開発、テストされています。

- Cisco IOS®ソフトウェアリリース12.0。この設定は12.28Tでテストされています。
- Cisco 2500-is56i-l.120-7.T

- Cisco 2513

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

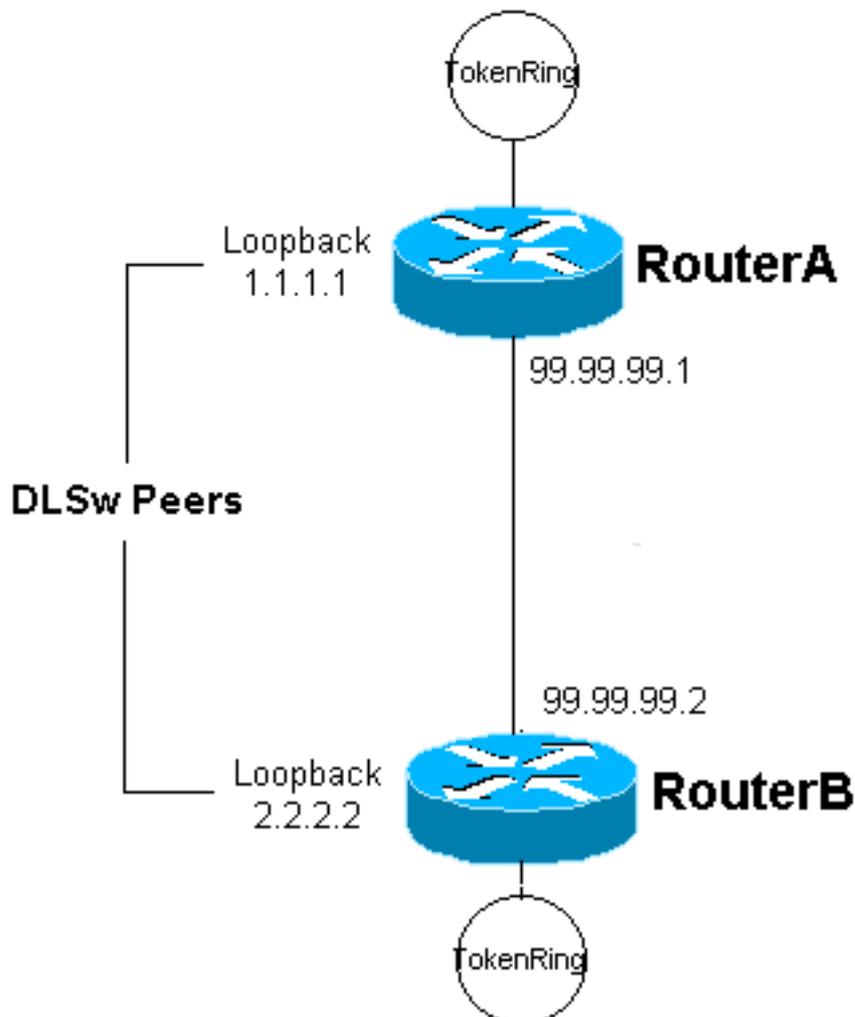
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このドキュメントで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#)（[登録ユーザ専用](#)）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



設定

このドキュメントでは、次の構成を使用します。

- ルータ A
- ルータ B

ルータ 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
```

ルータ B

Current configuration:

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname RouterB  
!  
enable secret 5 $1$7WP3$aEqtNjvRJ9Vy6i41x0RJf0  
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
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

このセクションは、設定のトラブルシューティングを行う際に参照してください。

debug コマンドと show コマンド

[アウトプット インタープリタ ツール \(登録ユーザ専用\) \(OIT\)](#) は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

注：[debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

- **debug crypto ipsec**：このコマンドは、フェーズ2のIPセキュリティプロトコル(IPSec)ネゴシエーションを表示します。
- **debug crypto isakmp**：このコマンドは、フェーズ1のInternet Security Association and Key Management Protocol(ISAKMP)ネゴシエーションを表示します。
- **debug crypto engine**：このコマンドは、暗号化されたトラフィックを表示します。
- **show crypto ipsec sa**：フェーズ2のセキュリティアソシエーションを表示します。
- **show crypto isakmp sa**：このコマンドは、フェーズ1のセキュリティアソシエーションを表示します。
- **show dlsw peer**：このコマンドは、DLSwピアステータスと接続ステータスを表示します。

関連情報

- [IPSec に関するサポート ページ](#)
- [DLSw に関するサポート ページ](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)