Router to Router Encrypting DLSw Traffic

Document ID: 14128

Contents

Introduction

In the sample configuration in this document, there are two routers with data−link switching (DLSw) peers set up between their loopback interfaces. All DLSw traffic is encrypted between them. This configuration works for any self−generated traffic the router transmits.

In this configuration, the crypto access−list is generic. The user can be more specific and allow DLSw traffic between the two loopback addresses. In general, only DLSw traffic travels from loopback interface to loopback interface.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This configuration was developed and tested using these software and hardware versions:

- Cisco IOS® Software Release 12.0. This configuration has been tested with 12.28T.
- Cisco 2500−is56i−l.120−7.T
- Cisco 2513

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

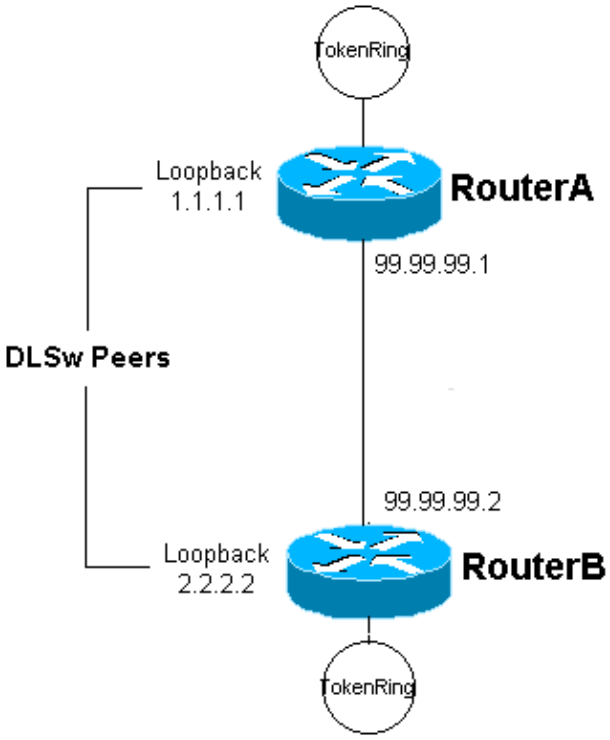
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- Router A
- Router B

Router 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
```

Router 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
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

Use this section to troubleshoot your configuration.

debug and show Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug crypto ipsec** This command displays the IP Security Protocol (IPSec) negotiations of Phase 2.
- **debug crypto isakmp** This command displays the Internet Security Association and Key Management Protocol (ISAKMP) negotiations of Phase 1.
- **debug crypto engine** This command displays the traffic that is encrypted.
- **show crypto ipsec sa** This displays the Phase 2 security associations.
- **show crypto isakmp sa** This command displays the Phase 1 security associations.
- **show dlsw peer** This command displays the DLSw peer status and the connect status.

Related Information

- **IPSec Support Page**
- **DLSW Support Page**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jun 08, 2006 Document ID: 14128