

路由器到路由器的加密DLSw数据流

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[debug 和 show 命令](#)

[相关信息](#)

简介

在本文的配置示例中，两台路由器的loopback接口之间设置有数据链路交换(DLSW)对等体。在他们之间的所有DLSw流量都是加密的。配置为路由器传输的所有自生的流量工作。

在此配置中，crypto访问列表是通用的。用户可以更具体，并允许两个环回地址之间的DLSw流量。一般来说，仅DLSw流量从回环接口流入到回环接口。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

此配置使用这些软件和硬件版本开发并测试：

- Cisco IOS软件版本12.0。此配置用12.28T测试。
- 思科2500-is56i-l.120-7.T
- Cisco 2513

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

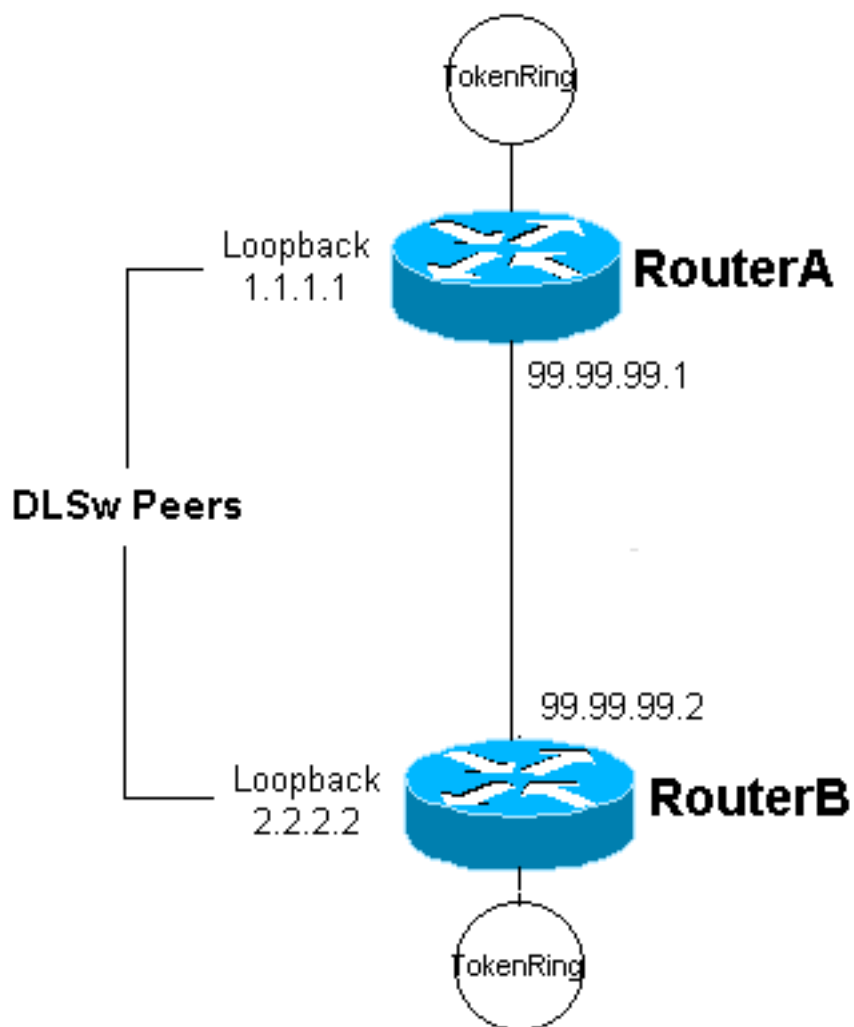
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 有关本文档所用命令的详细信息，请使用 [命令查找工具](#) ([仅限注册用户](#))。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

- 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$7WP3$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
```

[验证](#)

当前没有可用于此配置的验证过程。

[故障排除](#)

使用本部分可排除配置故障。

[debug 和 show 命令](#)

[命令输出解释程序 \(仅限注册用户 \)](#) (OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

注意： 使用 debug 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

- **debug crypto ipsec** —此命令显示第2阶段的IP安全协议(IPSec)协商。
- **debug crypto isakmp** —此命令显示阶段1的互联网安全协会和密钥管理协议(ISAKMP)协商。
- **debug crypto engine** —此命令显示加密的流量。
- **show crypto ipsec sa** —这显示第2阶段安全关联。
- **show crypto isakmp sa** —此命令显示阶段1安全关联。
- **show dls w peer** —此命令显示DLSw对等体状态和连接状态。

[相关信息](#)

- [IPSec 支持页面](#)
- [DLSw支持页面](#)
- [技术支持和文档 - Cisco Systems](#)