Roteador para Roteador Criptografando Tráfego DLSw

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Conventions](#)
[Configurar](#)
[Diagrama de Rede](#)
[Configurações](#)
[Verificar](#)
[Troubleshoot](#)
[comandos debug e show](#)
[Informações Relacionadas](#)

Introduction

Na configuração de exemplo neste documento, há dois roteadores com comutação de enlace de dados (DLSw) configurados entre suas interfaces de loopback. Todo o tráfego DLSw é criptografado entre eles. Essa configuração funciona para qualquer tráfego gerado automaticamente que o roteador transmite.

Nesta configuração, a lista de acesso de criptografia é genérica. O usuário pode ser mais específico e permitir o tráfego DLSw entre os dois endereços de loopback. Em geral, somente o tráfego DLSw viaja da interface de loopback para a interface de loopback.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Essa configuração foi desenvolvida e testada usando estas versões de software e de hardware:

- Versão do software Cisco IOS 12.0. Esta configuração foi testada com 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

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

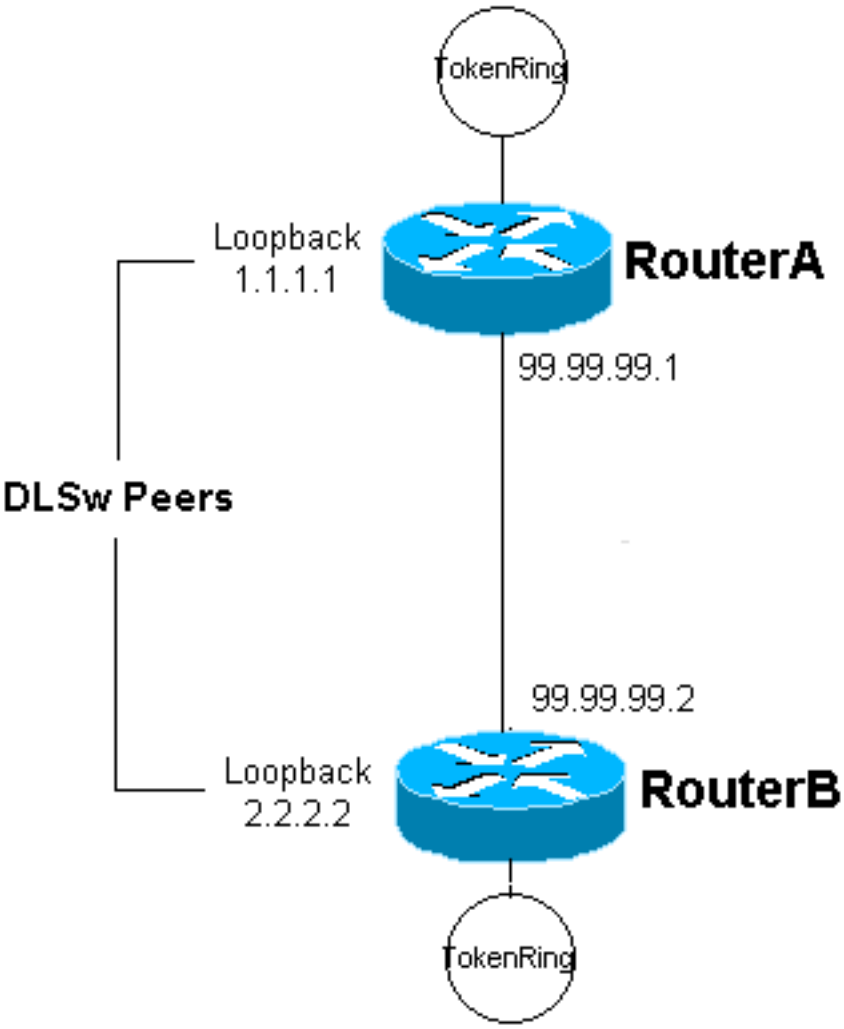
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota:Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- 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
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Use esta seção para resolver problemas de configuração.

comandos debug e show

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

- **debug crypto ipsec** — Este comando exibe as negociações do IP Security Protocol (IPSec) da Fase 2.
- **debug crypto isakmp** — Este comando exibe as negociações de Internet Security Association and Key Management Protocol (ISAKMP) da Fase 1.
- **debug crypto engine** — Este comando exibe o tráfego que está criptografado.
- **show crypto ipsec sa** — Exibe as associações de segurança da Fase 2.
- **show crypto isakmp sa** — Este comando exibe as associações de segurança da Fase 1.
- **show dlsw peer** — Este comando exibe o status do peer DLSw e o status da conexão.

Informações Relacionadas

- Página de suporte do IPSec
- Página de suporte do DLSW
- Suporte Técnico e Documentação - Cisco Systems