Roteador ao roteador que cifra o tráfego de DLSw

Índice

Introdução

Na configuração de exemplo neste documento, há dois Roteadores com os pares do switching de link de dados (DLSw) estabelecidos entre suas interfaces de loopback. Todo o tráfego de DLSw é cifrado entre elas. Esta configuração trabalha para todo o tráfego que auto-gerado o roteador transmitir.

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

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Software Release 12.0 de Cisco IOS®. Esta configuração foi testada com 12.28T.
- Cisco 2500-is56i-l.120-7.T
- Cisco 2513

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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 ferramenta Command Lookup Tool (apenas para 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:

- Roteador A
- roteador B

Roteador 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
```

roteador 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.

Troubleshooting

Use esta seção para resolver problemas de configuração.

comandos debug e show

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta 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**.

- **IPsec do debug crypto** — Este comando indica as negociações do protocolo de segurança IP (IPsec) da fase 2.
- **isakmp do debug crypto** — Este comando indica as negociações do Internet Security Association and Key Management Protocol (ISAKMP) da fase 1.
- **motor do debug crypto** — Este comando indica o tráfego que é cifrado.
- **mostre IPsec cripto sa** — Isto indica as associações de segurança da fase 2.
- **mostre isakmp cripto sa** — Este comando indica as associações de segurança da fase 1.
- **par do show dlsw** — Este comando indica o status de peer de DLSw e o estado da conexão.

Informações Relacionadas

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