

Crittografia del traffico DLSw da router a router

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi debug e show](#)

[Informazioni correlate](#)

[Introduzione](#)

Nella configurazione di esempio di questo documento, sono presenti due router con peer DLSw (Data-Link Switching) impostati tra le loro interfacce di loopback. Tutto il traffico DLSw tra di essi è crittografato. Questa configurazione funziona su tutto il traffico generato automaticamente dal router.

In questa configurazione, l'elenco degli accessi crittografici è generico. L'utente può essere più specifico e consentire il traffico DLSw tra i due indirizzi di loopback. In generale, solo il traffico DLSw passa dall'interfaccia di loopback all'interfaccia di loopback.

[Prerequisiti](#)

[Requisiti](#)

Nessun requisito specifico previsto per questo documento.

[Componenti usati](#)

Questa configurazione è stata sviluppata e testata utilizzando le seguenti versioni software e hardware:

- Software Cisco IOS® versione 12.0. Questa configurazione è stata testata con la versione 12.28T.
- Cisco 2500-is56i-l.120-7.T
- Cisco 2513

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

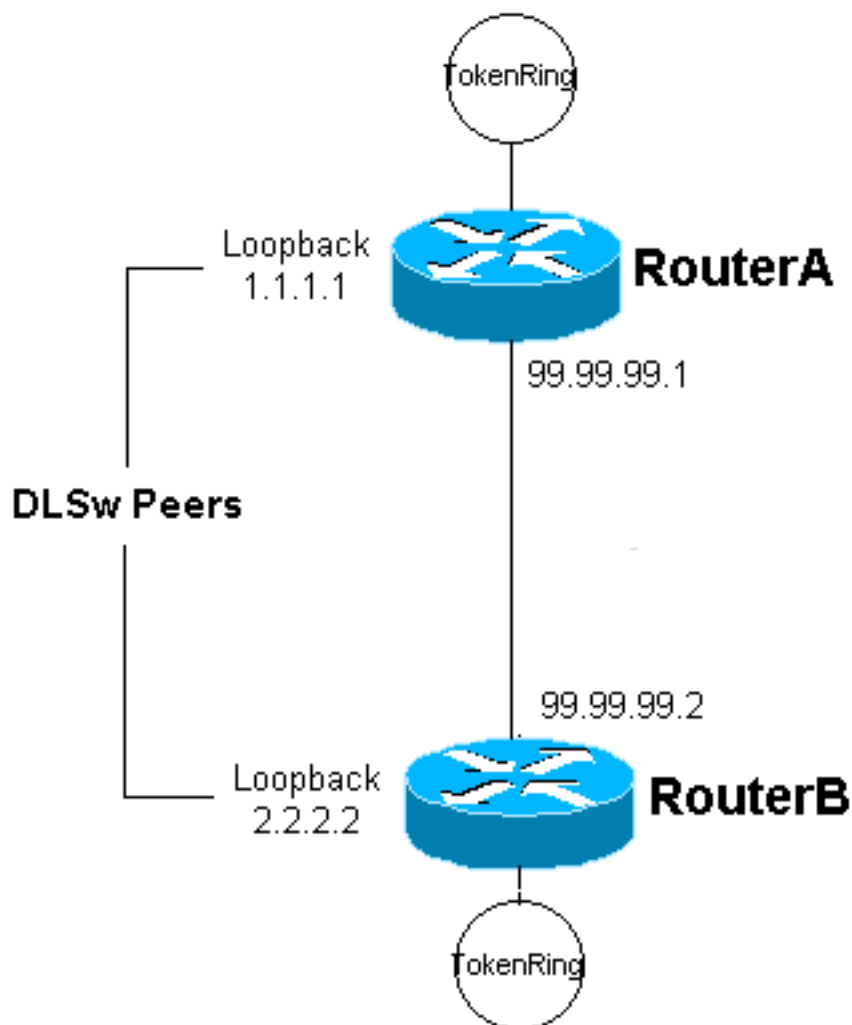
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento vengono usate queste configurazioni:

- 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
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Utilizzare questa sezione per risolvere i problemi relativi alla configurazione.

Comandi debug e show

Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di **debug**.

- **debug crypto ipsec:** questo comando visualizza le negoziazioni IPsec (IP Security Protocol) della fase 2.
- **debug crypto isakmp:** questo comando visualizza le negoziazioni ISAKMP (Internet Security Association and Key Management Protocol) della fase 1.
- **debug crypto engine:** questo comando visualizza il traffico crittografato.
- **show crypto ipsec sa:** visualizza le associazioni di sicurezza della fase 2.
- **show crypto isakmp sa:** questo comando visualizza le associazioni di sicurezza della fase 1.
- **show dlsw peer:** questo comando visualizza lo stato del peer DLSw e lo stato della connessione.

Informazioni correlate

- [Pagina di supporto per IPsec](#)
- [Pagina di supporto DLSW](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)