Chiffrement du trafic DLSw entre deux routeurs

Contenu

Introduction

Dans la configuration d'échantillon dans ce document, il y a deux Routeurs avec des pairs de Data-Link Switching (DLSw) installés entre leurs interfaces de bouclage. Tout le trafic de DLSw est chiffré entre eux. Cette configuration fonctionne pour n'importe quel trafic auto-généré que le routeur transmet.

Dans cette configuration, la crypto liste d'accès est générique. L'utilisateur peut être plus de particularité et permettre le trafic de DLSw entre les deux adresses de bouclage. Généralement seulement le trafic de DLSw voyage de l'interface de bouclage à l'interface de bouclage.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Cette configuration a été développée et testée utilisant des ces le logiciel et les versions de matériel :

- Version de logiciel 12.0 de Cisco IOS®. Cette configuration a été testée avec 12.28T.
- Cisco 2500-is56i-l.120-7.T
- Cisco 2513

Les informations contenues dans ce document ont été créées à partir des périphériques d'un

environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configurations

Ce document utilise les configurations suivantes :

- routeur A
- routeur B

routeur 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
```

routeur 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
```

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Utilisez cette section pour dépanner votre configuration.

Commandes debug et show

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant

d'utiliser les commandes de **débogage**.

- **debug crypto ipsec** — Cette commande affiche les négociations de protocole de sécurité IP (IPSec) du Phase 2.
- **debug crypto isakmp** — Cette commande affiche les négociations de Protocole ISAKMP (Internet Security Association and Key Management Protocol) du Phase 1.
- **debug crypto engine** — Cette commande affiche le trafic qui est chiffré.
- **show crypto ipsec sa** — Ceci affiche les associations de sécurité de Phase 2.
- **show crypto isakmp sa** — Cette commande affiche les associations de sécurité de Phase 1.
- **affichez le pair de dlsw** — Cette commande affiche l'état de pair de DLSw et l'état de connecter.

Informations connexes

- Page d'assistance IPsec
- Page de support DLSW
- Support et documentation techniques - Cisco Systems