Sécurité des ponts

Contenu

Introduction

La Sécurité est une considération essentielle en concevant une liaison sans fil traversière entre les segments d'Ethernets. Ce document explique comment sécuriser le trafic croisant une liaison sans fil traversière en employant un tunnel IPSEC.

Dans cet exemple, deux Ponts de la gamme Cisco Aironet 350 établissent WEP ; les deux Routeurs ont installé un tunnel IPSEC.

Conditions préalables

Conditions requises

Avant de tenter cette configuration, assurez-vous que vous êtes confortable avec l'utilisation de ces derniers :

- Interface de configuration de pont de Cisco Aironet
- Interface de ligne de commande Cisco IOS

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeurs de gamme Cisco 2600 exécutant la version IOS 12.1
- Ponts de la gamme Cisco Aironet 350 exécutant la version 11.08T de micrologiciels

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Théorie générale

Cisco Aironet 340, 350, et les passerelles de gamme 1400 fournissent jusqu'au chiffrement 128-bit WEP. Ceci ne peut pas être compté au moment pour la connectivité sécurisée due aux problèmes réputés dans des algorithmes WEP et la facilité de l'exploitation, comme décrit dans la Sécurité de l'algorithme WEP et en réponse de Cisco Aironet pour appuyer sur - des imperfections dans la Sécurité de 802.11.

Une méthode d'augmenter la Sécurité du trafic passée à travers un lien pont par radio est de créer un tunnel chiffré du routeur à routeur IPSEC qui croise le lien. Ceci fonctionne parce que les passerelles fonctionnent à la couche 2 du modèle OSI. Vous pouvez exécuter le routeur à routeur IPSEC au-dessus de la connexion entre les passerelles.

Si la Sécurité de la liaison sans fil est ouverte une brèche, le trafic elle contient des restes chiffrés et les sécurise.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

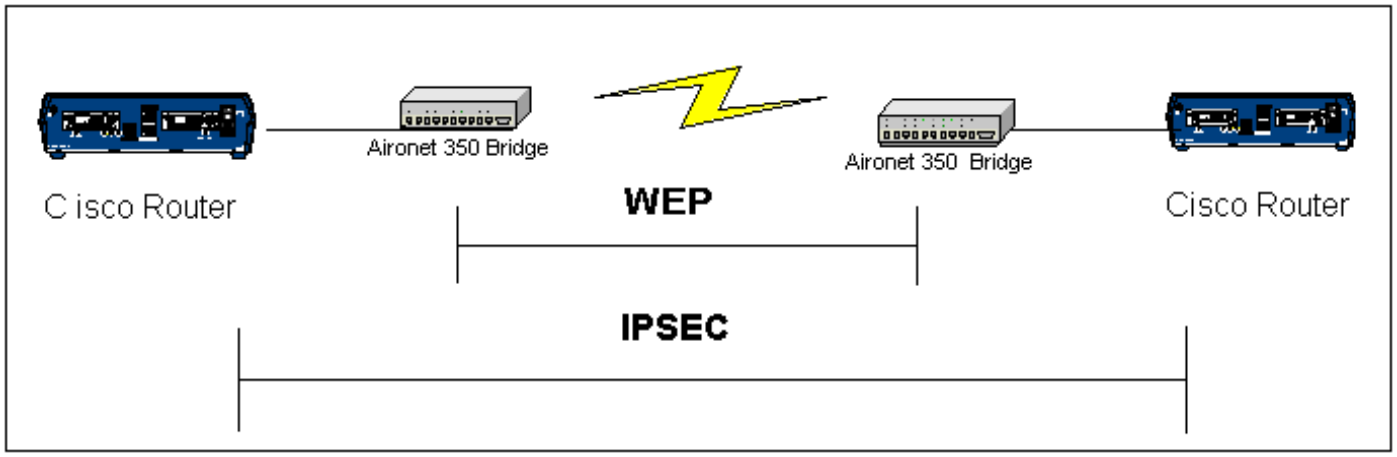
Configurez

Cette section présente les informations pour configurer les caractéristiques décrites dans ce document.

Remarque: Pour trouver les informations complémentaires sur les commandes utilisées dans ce document, utilisez l'utilitaire de recherche de commande IOS.

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :



Configurations

Ce document utilise les configurations suivantes :

- RouterA
- RouterB
- Exemple de passerelle

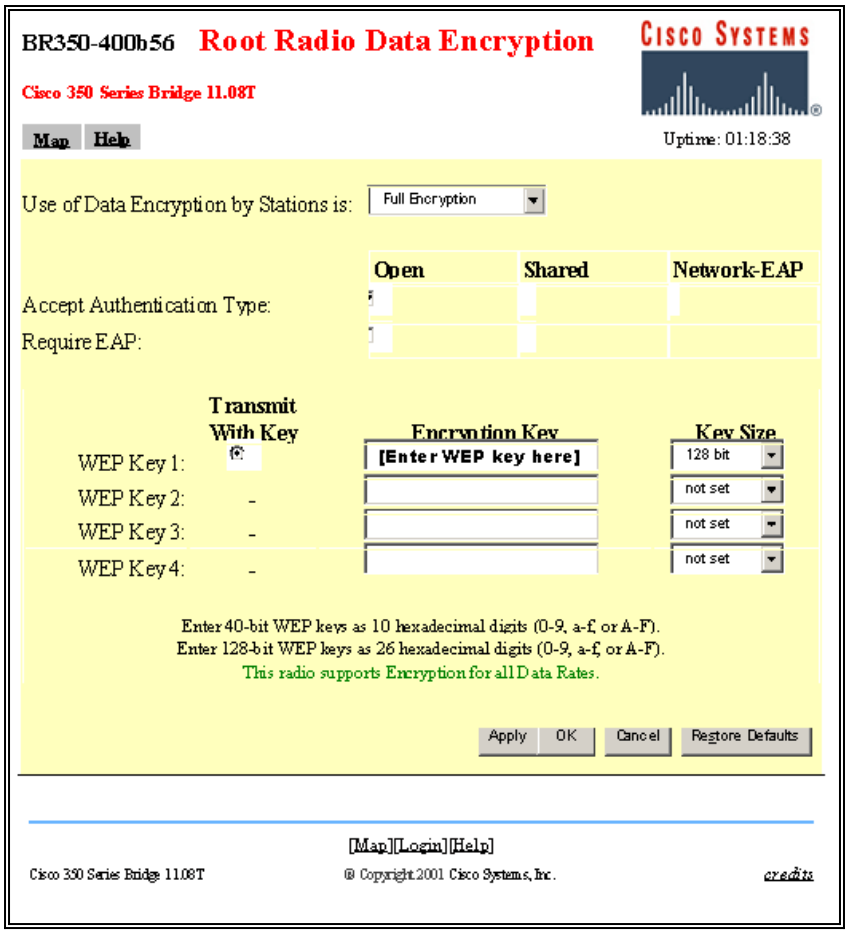
RouterA (routeur de Cisco 2600)

```
RouterA#show running-config Building configuration...
Current configuration : 1258 bytes ! version 12.1 no
service single-slot-reload-enable no service pad service
timestamps debug uptime service timestamps log uptime no
service password-encryption ! hostname RouterA ! logging
rate-limit console 10 except errors ! ip subnet-zero no
ip finger ip dhcp excluded-address 10.1.1.20 ip dhcp
excluded-address 10.1.1.30 ! ip dhcp pool wireless
network 10.1.1.0 255.255.255.0 ! ip audit notify log ip
audit po max-events 100 call rsvp-sync ! crypto isakmp
policy 10 hash md5 authentication pre-share crypto
isakmp key cisco address 10.1.1.30 ! ! crypto ipsec
transform-set set esp-3des esp-md5-hmac ! crypto map vpn
10 ipsec-isakmp set peer 10.1.1.30 set transform-set set
match address 120 ! interface Loopback0 ip address
20.1.1.1 255.255.255.0 ! interface Ethernet0 ip address
10.1.1.20 255.255.255.0 crypto map vpn ! ! ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.30 no ip http server no
ip http cable-monitor ! access-list 120 permit ip
20.1.1.0 0.0.0.255 30.1.1.0 0.0.0.255 ! ! line con 0
transport input none line vty 0 4 ! end
```

RouterB (routeur de Cisco 2600)

```
RouterB#show running-config Building configuration...
Current configuration : 1177 bytes ! version 12.1 no
service single-slot-reload-enable no service pad service
timestamps debug uptime service timestamps log uptime no
service password-encryption ! hostname RouterB ! logging
rate-limit console 10 except errors ! ip subnet-zero no
ip finger ! ip audit notify log ip audit po max-events
100 call rsvp-sync crypto isakmp policy 10 hash md5
authentication pre-share crypto isakmp key cisco address
10.1.1.20 ! ! crypto ipsec transform-set set esp-3des
esp-md5-hmac ! crypto map vpn 10 ipsec-isakmp set peer
10.1.1.20 set transform-set set match address 120
interface Loopback0 ip address 30.1.1.1 255.255.255.0 !
interface Ethernet0 ip address 10.1.1.30 255.255.255.0
no ip mroute-cache crypto map vpn ! ip classless ip
route 0.0.0.0 0.0.0.0 10.1.1.20 no ip http server no ip
http cable-monitor ! access-list 120 permit ip 30.1.1.0
0.0.0.255 20.1.1.0 0.0.0.255 ! ! line con 0 transport
input none line vty 0 4 login ! end
```

Passerelles de Cisco Aironet



Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **active de connexions de show crypto engine** - cette commande est utilisée de visualiser les connexions de session chiffrées par active en cours

```
RouterA#show crypto engine connection active ID Interface IP-Address State Algorithm Encrypt
Decrypt 1 Ethernet0 10.1.1.20 set HMAC_MD5+DES_56_CB 0 0 2002 Ethernet0 10.1.1.20 set
HMAC_MD5+3DES_56_C 0 3 2003 Ethernet0 10.1.1.20 set HMAC_MD5+3DES_56_C 3 0 RouterB#show
crypto engine connection active ID Interface IP-Address State Algorithm Encrypt Decrypt 1
<none> <none> set HMAC_MD5+DES_56_CB 0 0 2000 Ethernet0 10.1.1.30 set HMAC_MD5+3DES_56_C 0 3
2001 Ethernet0 10.1.1.30 set HMAC_MD5+3DES_56_C 3 0
```

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Pour dépanner la Connectivité IPSEC, référez-vous :

- Dépannage de sécurité IP - Comprendre et utiliser les commandes de dépannage
- Configuration et dépannage du chiffrement de couche réseau Cisco IPSec et ISAKMP, partie et partie

Pour dépanner la connexion Sans fil, référez-vous :

- Outil TAC Case Collection - RÉSEAU LOCAL Sans fil
- Résolution des problèmes fréquents avec les réseaux pontés sans fil
- Résolution des problèmes de connectivité dans un réseau LAN sans fil

Informations connexes

- Soutien technique - RÉSEAU LOCAL Sans fil
- Soutien technique - Négociation IPSec/protocoles IKE
- Support technique - Cisco Systems