Seguridad del Bridge

Contenido

Introducción

La seguridad es una consideración vital cuando se diseña un link inalámbrico con puente entre segmentos Ethernet. Este documento demuestra cómo asegurar el tráfico que cruza un link de red inalámbrica interligado por el uso de un túnel IPsec.

En este ejemplo, dos Puentes Cisco Aironet de la serie 350 establece el WEP; el dos Routers configura un túnel IPsec.

prerrequisitos

Requisitos

Antes de intentar esta configuración, asegúrese de que usted es cómodo con el uso de éstos:

- Interfaz de la configuración de Bridge del Cisco Aironet
- Interfaz de línea del comando cisco ios

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 2600 Series Router que funcionan con la versión de IOS 12.1
- Puentes Cisco Aironet de la serie 350 que funciona con la versión de firmware 11.08T

La información que se presenta en este documento se originó a partir de dispositivos dentro de un

ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Teoría Precedente

El Cisco Aironet 340, 350, y los Bridges de las 1400 Series proporcionan hasta el 128-bit la encripción WEP. Esto no se puede confiar sobre para la conectividad segura debido a los problemas bien conocidos en los algoritmos WEP y la facilidad de la explotación, según lo descrito en la Seguridad del algoritmo WEP y en la respuesta del Cisco Aironet para presionar - los defectos en la Seguridad del 802.11.

Un método de aumentar la Seguridad del tráfico pasajera a través de un Bridged Link inalámbrico es crear un túnel cifrado del IPSEC de router a router que cruce el link. Esto funciona porque los puentes funcionan en la capa 2 del modelo de OSI. Puede ejecutar IPSEC de router a router a lo largo de la conexión entre los puentes.

Si la Seguridad del link de red inalámbrica se viola, el tráfico contiene los restos cifrados y los asegura.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

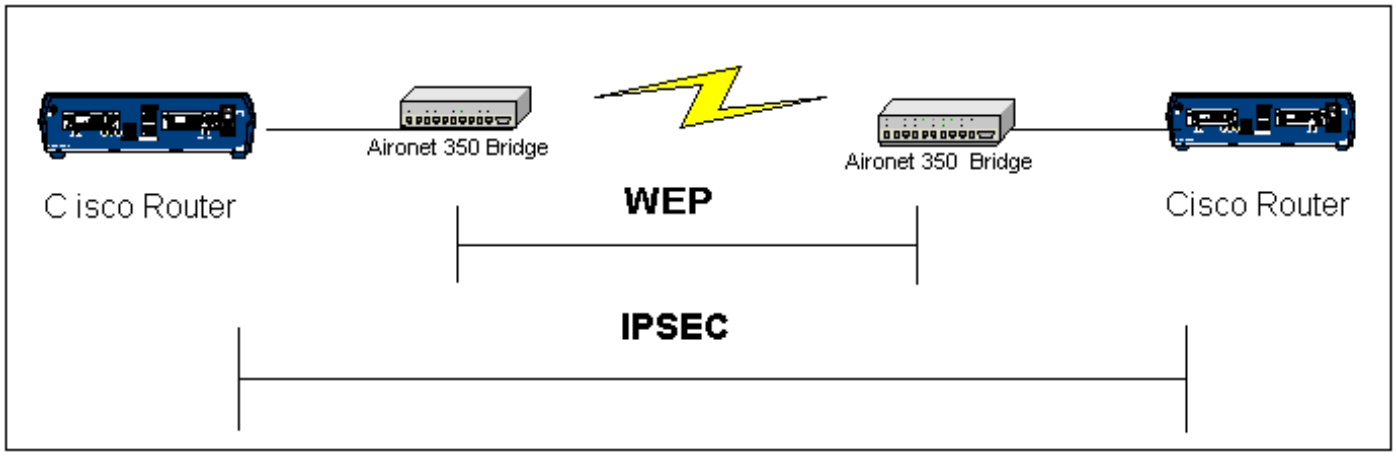
Configurar

Esta sección contiene información para configurar las funciones descritas en este documento.

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la herramienta Command Lookup del IOS.

Diagrama de la red

Este documento utiliza la configuración de red que se muestra en este diagrama:



Configuraciones

En este documento, se utilizan estas configuraciones:

- RouterA
- RouterB
- Ejemplo del Bridge

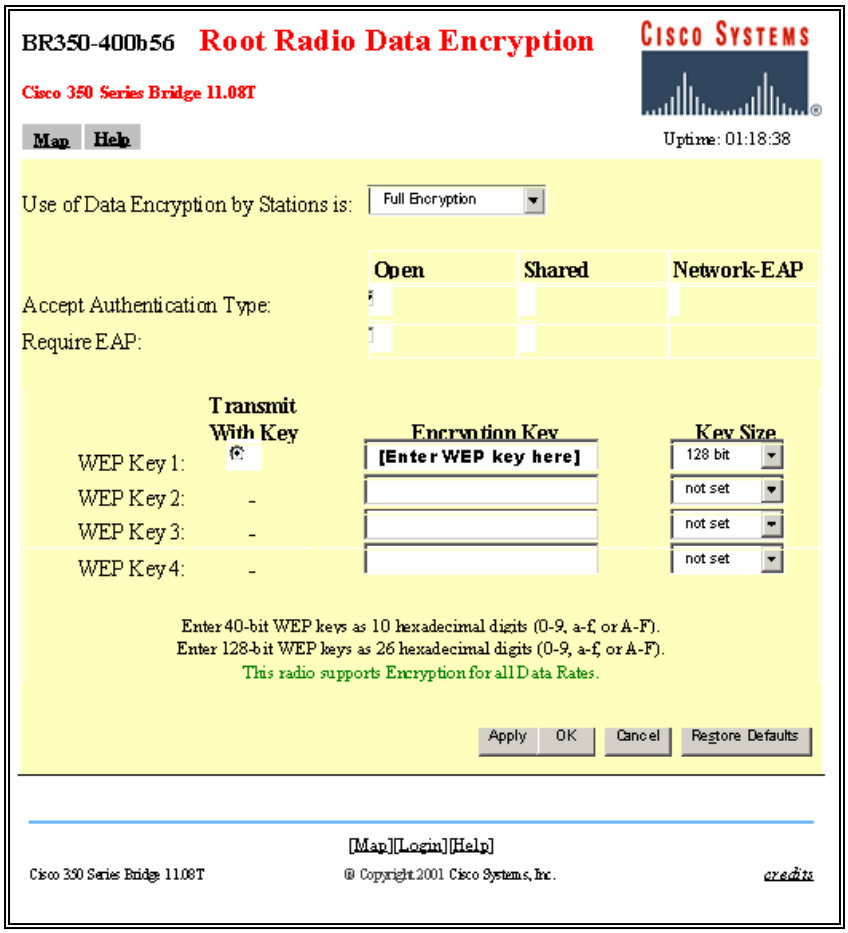
RouterA (Router 2600 de Cisco)

```
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 (Cisco 2600 Router)

```
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
```

Bridges del Cisco Aironet



Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **active del show crypto engine connections** - se utiliza este comando de ver las conexiones de sesión encriptada activas actuales

```
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
```

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Para solucionar los problemas de conectividad de IPSEC, consulte:

- Resolución de problemas de seguridad de IP – Información y uso de los comandos de depuración
- Configurando y resolviendo problemas la encripción de capa de red de Cisco: IPSec y

ISAKMP, parte 1 y parte 2

Para resolver problemas la conexión de red inalámbrica, refiérase:

- Herramienta de recopilación de casos TAC - LAN inalámbrica
- Solución de problemas comunes con redes inalámbricas conectadas con puente
- Resolución de problemas de conectividad en una red inalámbrica de LAN

Información Relacionada

- Soporte técnico: LAN inalámbrica
- Soporte técnico - Negociación IPSec/Protocolos IKE
- Soporte Técnico - Cisco Systems