

Segurança da ponte

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Material de Suporte](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

A segurança é uma consideração vital durante o projeto de um link sem fio com ponte entre os segmentos Ethernet. Este original demonstra como fixar o tráfego que cruza um enlace Wireless construído uma ponte sobre pelo uso de um túnel de IPsec.

Neste exemplo, dois Bridges Cisco Aironet série 350 estabelecem o WEP; os dois Roteadores estabelecem um túnel de IPsec.

[Pré-requisitos](#)

[Requisitos](#)

Antes de tentar esta configuração, assegure-se de que você esteja confortável com o uso destes:

- Relação da configuração de bridges do Cisco Aironet
- Interface de linha do comando cisco ios

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 2600 Series Router que executam a Versão do IOS 12.1
- Bridges Cisco Aironet série 350 que executa a versão de firmware 11.08T

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 você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

[Material de Suporte](#)

O Cisco Aironet 340, 350, e as pontes do 1400 Series fornecem até a criptografia de WEP do 128-bit. Isto não pode ser confiado para na conectividade segura devido aos problemas conhecidos nos algoritmos de WEP e na facilidade da exploração, como descrito na [Segurança do algoritmo de WEP](#) e na [resposta do Cisco Aironet para pressionar - falhas na Segurança do 802.11](#).

Um método de aumentar a Segurança do tráfego passada através de um link interligado wireless é criar um túnel cifrado do IPSec de roteador a roteador que cruze o link. Isto funciona porque as pontes operam na camada 2 do modelo de OSI. Você pode executar roteador-para-roteador IPSEC na conexão entre as pontes.

Se a Segurança do enlace Wireless é rompida, o tráfego contém as sobras cifradas e fixa-se.

[Convenções](#)

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

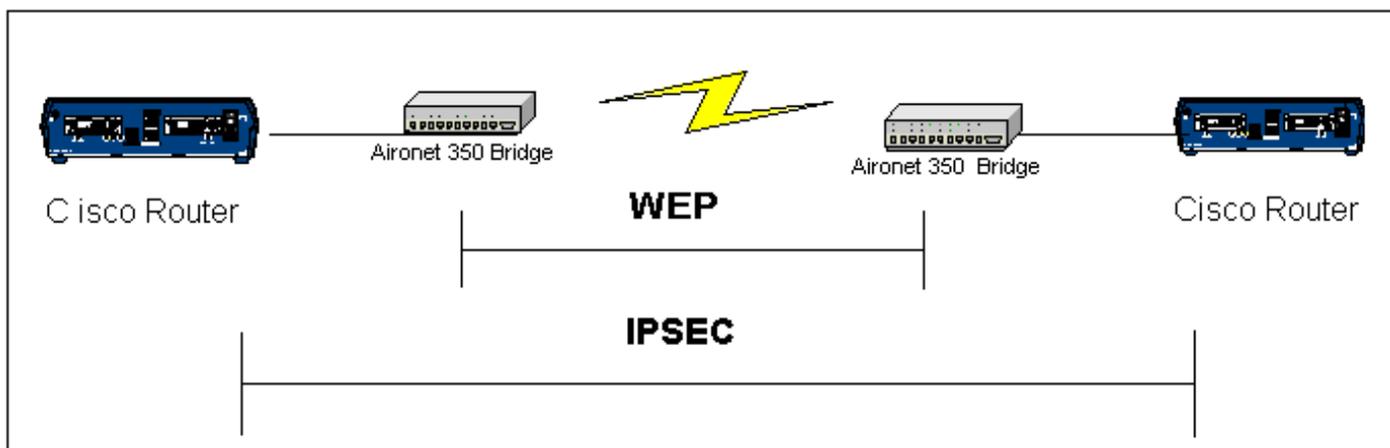
[Configurar](#)

Esta seção apresenta informações para configurar os recursos descritos neste documento.

Nota: Para encontrar informações adicionais sobre comandos usados neste documento, utilize a ferramenta IOS Command Lookup

[Diagrama de Rede](#)

Este documento utiliza a configuração de rede mostrada neste diagrama:



[Configurações](#)

Este documento utiliza as seguintes configurações:

- [RoteadorA](#)
- [RoteadorB](#)
- [Exemplo da ponte](#)

Roteador A (Cisco 2600 Router)

```

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
```

RoteadorB (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

```

Pontes do Cisco Aironet

BR350-400b56 **Root Radio Data Encryption** 

Cisco 350 Series Bridge 11.08T Uptime: 01:18:38

[Map](#) [Help](#)

Use of Data Encryption by Stations is:

Accept Authentication Type:	Open	Shared	Network-EAP
Require EAP:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Transmit With Key	Encryption Key	Key Size
WEP Key 1: <input type="checkbox"/>	<input type="text" value="[Enter WEP key here]"/>	<input type="text" value="128 bit"/>
WEP Key 2: -	<input type="text"/>	<input type="text" value="not set"/>
WEP Key 3: -	<input type="text"/>	<input type="text" value="not set"/>
WEP Key 4: -	<input type="text"/>	<input type="text" value="not set"/>

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
 Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).
 This radio supports Encryption for all Data Rates.

[\[Map\]](#)[\[Login\]](#)[\[Help\]](#)

Cisco 350 Series Bridge 11.08T © Copyright 2001 Cisco Systems, Inc. [credits](#)

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A [Output Interpreter Tool](#) ([somente clientes registrados](#)) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **active do show crypto engine connections** - este comando é usado ver as conexões de sessão de criptografia ativas atuais

```

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

```

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Para fazer Troubleshooting de conectividade de IPSEC, consulte:

- [Troubleshooting de Segurança de IP - Entendendo e Utilizando Comandos debug](#)
- Configurando e pesquisando defeitos a criptografia de camada de rede Cisco: IPsec e ISAKMP, [parte 1](#) e [parte 2](#)

Para pesquisar defeitos a conexão Wireless, refira:

- [Ferramenta TAC Case Collection - LAN sem fio](#)
- [Problemas comuns de Troubleshoot com redes Wireless interligadas](#)
- [Conectividade de Troubleshooting em uma Rede Wireless LAN](#)

Informações Relacionadas

- [Suporte Técnico - Wireless LAN](#)
- [Suporte técnico - Negociação IPsec/Protocolos IKE](#)
- [Suporte Técnico - Cisco Systems](#)