Bridge Security

Inhoud

Inleiding

Beveiliging is een vitale overweging bij het ontwerpen van een overbrugde draadloze verbinding tussen Ethernet-segmenten. Dit document toont aan hoe de oversteek van een overbrugde draadloze verbinding door het gebruik van een IPSEC-tunnel kan worden beveiligd.

In dit voorbeeld, twee Cisco Aironet 350 Series bruggen vormen de overbrugging van de LG. de twee routers zetten een IPSEC-tunnel op.

Voorwaarden

Vereisten

Zorg er voordat u deze configuratie probeert, voor dat u deze gemakkelijk kunt gebruiken:

- Cisco Aironet 3500 brug-configuratieinterface
- Cisco IOS-opdrachtregelinterface

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 2600 Series routers en IOS-versie 12.1
- Cisco Aironet 350 Series bruggen met firmware versie 11.08T

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde

(standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de potentiële impact van om het even welke opdracht begrijpt alvorens het te gebruiken.

Achtergrondinformatie

Cisco Aironet 340, 350 en 1400 Series bruggen bieden tot 128-bits EFN-encryptie. Dit kan niet worden vertrouwd op veilige connectiviteit door bekende problemen in de algoritmen van EFG en het gemak van exploitatie, zoals die in Beveiliging van het algoritme van EFG en in de Reactie van Cisco Aironet op Pers worden beschreven - Voetgebreken in 802.11 Beveiliging.

Eén methode om de veiligheid van verkeer te verhogen dat over een draadloze overbrugde verbinding wordt doorgegeven is om een gecodeerde router-naar-router IPSEC-tunnel te maken die de link overschrijdt. Dit werkt omdat bruggen functioneren op Layer 2 van het OSI-model. U kunt IPSEC router-to-router via de verbinding tussen de bruggen uitvoeren.

Als de beveiliging van de draadloze link wordt overtreden, blijft het verkeer dat het bevat versleuteld en beveiligd.

Conventies

Zie de Cisco Technical Tips Convention voor meer informatie over documentconventies.

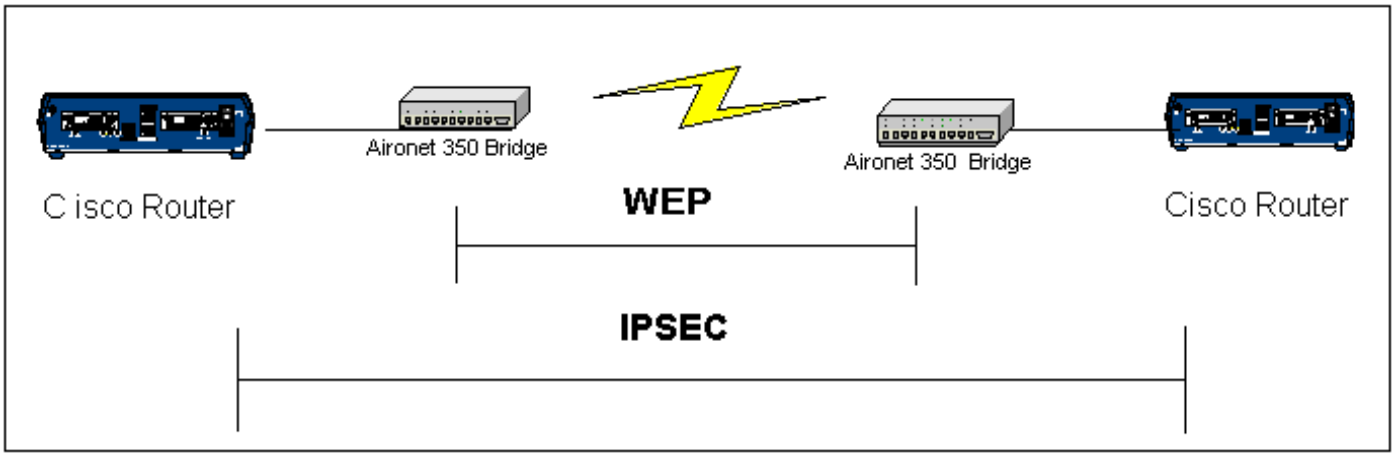
Configureren

Deze sectie verschaft informatie om de functies te configureren die in dit document worden beschreven.

Opmerking: Als u aanvullende informatie wilt vinden over de opdrachten die in dit document worden gebruikt, gebruikt u het IOS-opnamegereedschap.

Netwerkdiagram

Dit document gebruikt de netwerkinstellingen die in dit diagram worden weergegeven:



Configuraties

Dit document gebruikt deze configuraties:

- routerA
- routerB
- Bridge-voorbeeld

routerA (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
```

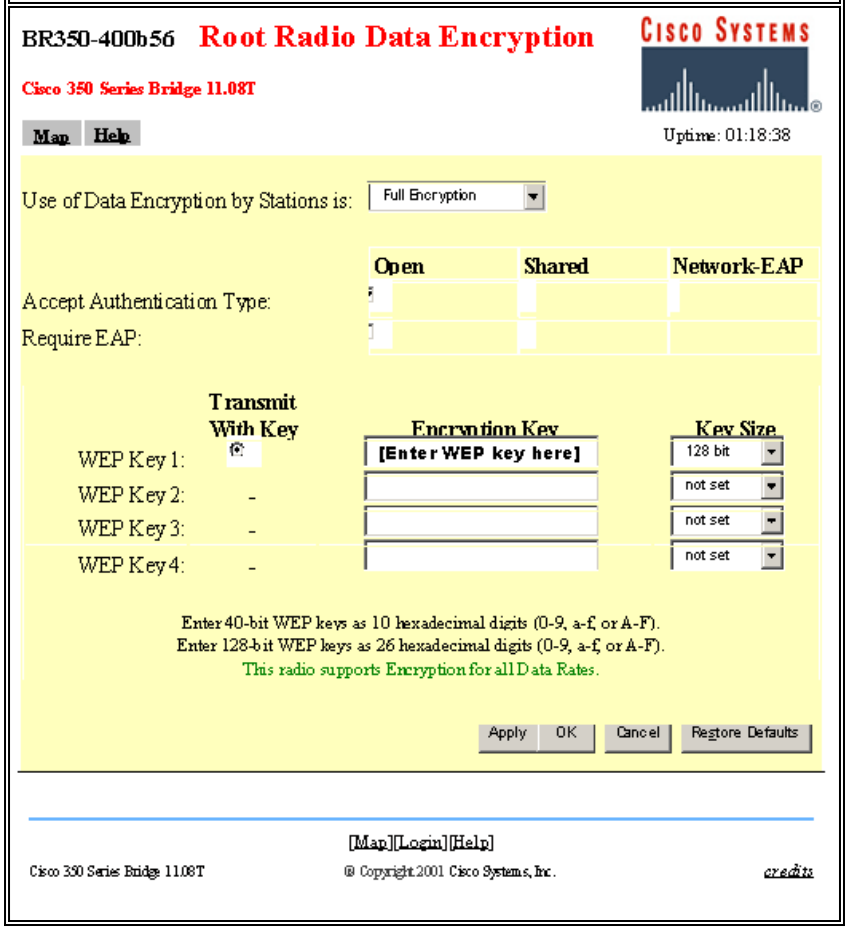
routerB (Cisco 2600 router)

```
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
```

Cisco Aironet-bruggen



Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

- **tonen de crypto motorverbindingen actief** - deze opdracht wordt gebruikt om de huidige actieve gecodeerde sessies te bekijken

```
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
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Raadpleeg voor probleemoplossing de connectiviteit van IPSEC:

- IP-beveiligingsprobleemoplossing door middel van debug-opdrachten
- Configuratie- en probleemoplossing van Cisco Network-Layer Encryption: IPsec en ISAKMP, deel 1 en deel 2

Zie voor meer informatie over het oplossen van draadloze verbindingen:

- TAC Case Collector - draadloos LAN
- Probleemoplossing voor gemeenschappelijke problemen met draadloze overbrugde netwerken
- Connectiviteit met probleemoplossing in een draadloos LAN-netwerk

Gerelateerde informatie

- **Technische ondersteuning - draadloos LAN**
- **Technische ondersteuning - IPsec-onderhandeling/IKE-protocollen**
- **Technische ondersteuning - Cisco-systemen**