網橋安全

目錄

簡介

在乙太網網段之間設計橋接無線鏈路時，安全是一個至關重要的考慮因素。本檔案將示範如何使用IPSEC通道來保護通過橋接無線連結的流量。

在本示例中，兩個Cisco Aironet 350系列網橋建立WEP;兩台路由器建立了IPSEC隧道。

必要條件

需求

嘗試此組態之前，請確保您偏好使用以下設定：

- Cisco Aironet網橋配置介面
- Cisco IOS命令列介面

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行IOS版本12.1的Cisco 2600系列路由器
- 運行韌體版本11.08T的Cisco Aironet 350系列網橋

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

背景理論

Cisco Aironet 340、350和1400系列網橋提供高達128位WEP加密。由於WEP演算法中的眾所周知問題和易於利用，因此不能依賴此安全連線，如Security of the WEP algorithm （WEP演算法的安全性）和Cisco Aironet Response to Press - Vects in 802.11 Security中所述。

提高通過無線橋接鏈路的流量安全性的一種方法是建立經過鏈路的加密路由器到路由器IPSEC隧道。這是因為網橋在OSI模型的第2層運行。您可以通過網橋之間的連線運行IPSEC路由器到路由器。

如果無線鏈路的安全受到破壞，則它所包含的流量將保持加密和安全狀態。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

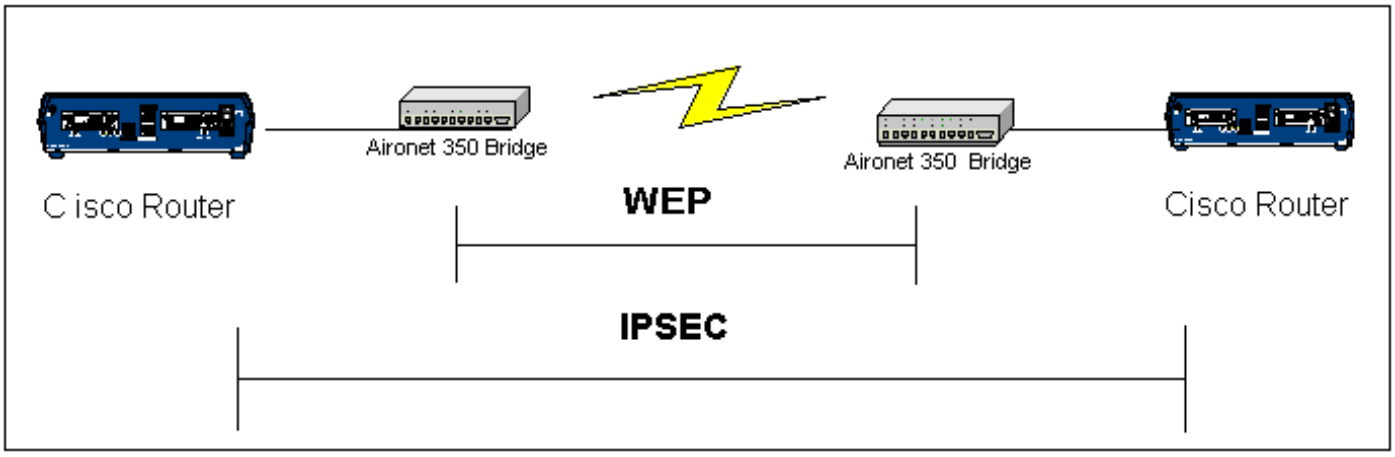
設定

本節提供用於設定本檔案中所述功能的資訊。

注意：要查詢有關本文檔中使用的命令的其他資訊，請使用IOS命令查詢工具。

網路圖表

本檔案會使用下圖所示的網路設定：



組態

本檔案會使用以下設定：

- 路由器 A
- 路由器 B
- Bridge示例

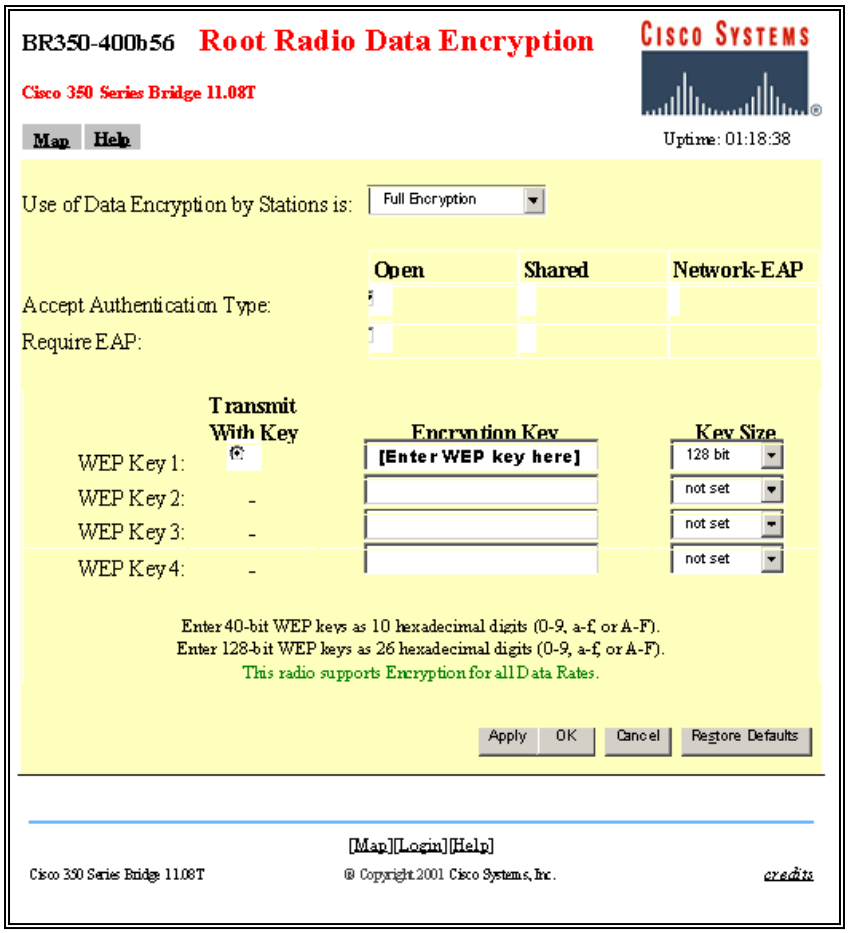
路由器A（思科2600路由器）
RouterA#**show running-config**

```
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
```

路由器B（思科2600路由器）

```
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橋接器



驗證

本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

- **show crypto engine connections active** — 此命令用於檢視當前活動的加密會話連線

```
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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

要排除IPSEC連線故障，請參閱：

- IP安全性故障排除 — 瞭解和使用debug命令
- 思科網路層加密配置和故障排除：IPSec和ISAKMP，第1部分和第2部分

有關對無線連線進行故障排除的資訊，請參閱：

- TAC案件收集工具 — 無線LAN
- 排除無線橋接網路的常見問題
- 排除無線LAN網路中的連線故障

相關資訊

- **技術支援 — 無線LAN**
- **技術支援 — IPSec協商/IKE通訊協定**
- **技術支援 - Cisco Systems**