Bridge-Sicherheit

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundtheorie](#)
[Konventionen](#)
[Konfigurieren](#)
[Netzwerkdiagramm](#)
[Konfigurationen](#)
[Überprüfen](#)
[Fehlerbehebung](#)
[Zugehörige Informationen](#)

Einführung

Sicherheit ist ein wichtiger Aspekt beim Design einer überbrückten Wireless-Verbindung zwischen Ethernet-Segmenten. In diesem Dokument wird veranschaulicht, wie der Datenverkehr über eine überbrückte Wireless-Verbindung mithilfe eines IPSEC-Tunnels gesichert wird.

In diesem Beispiel stellen zwei Cisco Aironet Bridges der Serie 350 WEP her. Die beiden Router richten einen IPSEC-Tunnel ein.

Voraussetzungen

Anforderungen

Stellen Sie vor dem Versuch dieser Konfiguration sicher, dass Sie mit den folgenden Vorteilen vertraut sind:

- Cisco Aironet Bridge-Konfigurationsoberfläche
- Cisco IOS Befehlszeilenschnittstelle

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Router der Serie 2600 mit IOS-Version 12.1
- Cisco Aironet Bridges der Serie 350 mit Firmware-Version 11.08T

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Hintergrundtheorie

Cisco Aironet Bridges der Serien 340, 350 und 1400 bieten eine WEP-Verschlüsselung mit bis zu 128 Bit. Aufgrund bekannter Probleme in WEP-Algorithmen und der Benutzerfreundlichkeit bei der Nutzung können Sie sich nicht auf die sichere Anbindung verlassen, wie in Sicherheit des WEP-Algorithmus und in Cisco Aironet Response to Press - Faults in 802.11 Security beschrieben.

Eine Möglichkeit zur Erhöhung der Sicherheit des Datenverkehrs, der über eine Wireless Bridge-Verbindung übertragen wird, besteht darin, einen verschlüsselten Router-zu-Router-IPSEC-Tunnel zu erstellen, der die Verbindung passiert. Dies funktioniert, weil Bridges auf Layer 2 des OSI-Modells arbeiten. Sie können IPSEC-Router-zu-Router über die Verbindung zwischen den Bridges ausführen.

Wenn die Sicherheit der Wireless-Verbindung verletzt wird, bleibt der darin enthaltene Datenverkehr verschlüsselt und sicher.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

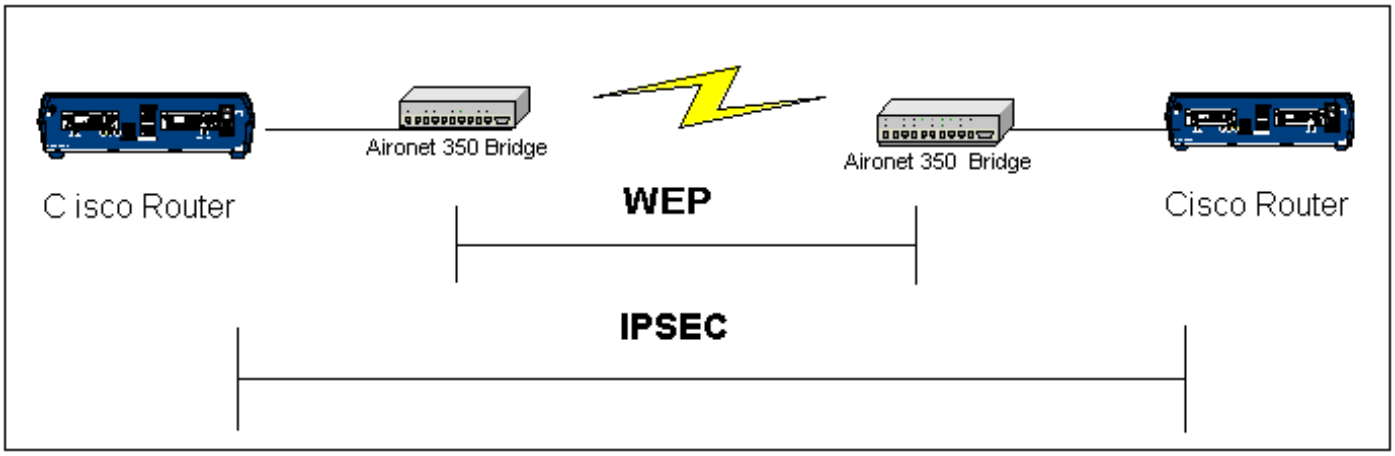
Konfigurieren

In diesem Abschnitt werden Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen beschrieben.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das IOS-Befehlssuche-Tool.

Netzwerkdiagramm

In diesem Dokument wird die in diesem Diagramm dargestellte Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- RouterA
- RouterB
- Bridge-Beispiel

Router 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
```

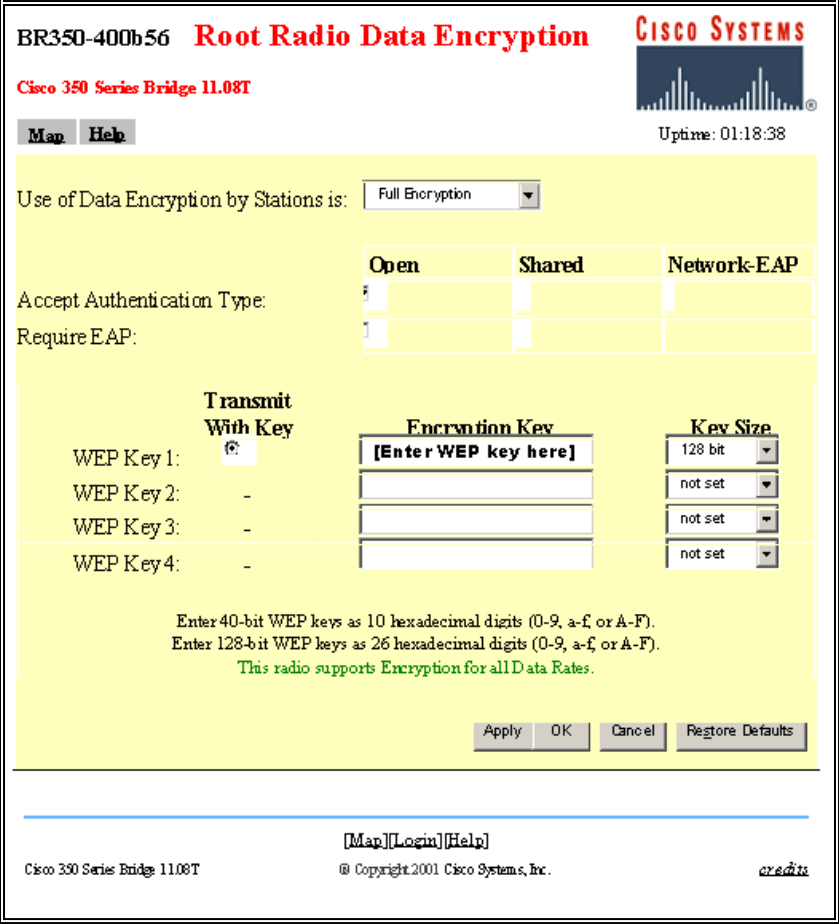
Router B (Cisco 2600 Router)

```
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-Bridges



Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show crypto engine connections active** - dieser Befehl wird verwendet, um die aktuell aktiven verschlüsselten session connections anzuzeigen

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Informationen zur Fehlerbehebung bei IPSEC-Konnektivität finden Sie unter:

- IP Security Troubleshooting - Understanding and Using debug Commands
- Konfiguration und Fehlerbehebung bei Cisco Network Layer Encryption: IPSec und ISAKMP, Teil 1 und Teil 2

Informationen zur Fehlerbehebung bei der Wireless-Verbindung finden Sie unter:

- TAC Case Collection Tool - Wireless LAN
- Fehlerbehebung für häufige Probleme mit Wireless Bridge-Netzwerken
- Fehlerbehebung bei Verbindungen in einem Wireless-LAN-Netzwerk

Zugehörige Informationen

- Technischer Support - Wireless LAN
- Technischer Support - IPSec-Aushandlung/IKE-Protokolle
- Technischer Support - Cisco Systems