Bridge Security

Sommario

Introduzione

La sicurezza è un fattore fondamentale nella progettazione di un collegamento wireless tra segmenti Ethernet. In questo documento viene spiegato come proteggere il traffico che attraversa un collegamento wireless con bridging tramite un tunnel IPSEC.

Nell'esempio, due Cisco Aironet serie 350 Bridge stabiliscono un protocollo WEP; i due router hanno configurato un tunnel IPSEC.

Prerequisiti

Requisiti

Prima di provare la configurazione, accertarsi di avere familiarità con l'uso dei seguenti elementi:

- Interfaccia di configurazione Cisco Aironet Bridge
- Interfaccia della riga di comando di Cisco IOS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 2600 router con IOS versione 12.1
- Cisco Aironet serie 350 Bridge con firmware versione 11.08T

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Nozioni di base

Cisco Aironet serie 340, 350 e 1400 Bridge fornisce una crittografia WEP fino a 128 bit. Non ci si può affidare a questo per una connettività sicura a causa di problemi noti negli algoritmi WEP e della facilità di utilizzo, come descritto in Sicurezza dell'algoritmo WEP e in Cisco Aironet Response to Press - Flaws in 802.11 Security.

Un metodo per aumentare la sicurezza del traffico trasmesso attraverso un collegamento con bridging wireless è creare un tunnel IPSEC crittografato da router a router che attraversa il collegamento. Ciò funziona perché i bridge operano al livello 2 del modello OSI. È possibile eseguire il routing IPSEC da router a router sulla connessione tra i bridge.

Se la sicurezza del collegamento wireless viene violata, il traffico in esso contenuto rimane crittografato e sicuro.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

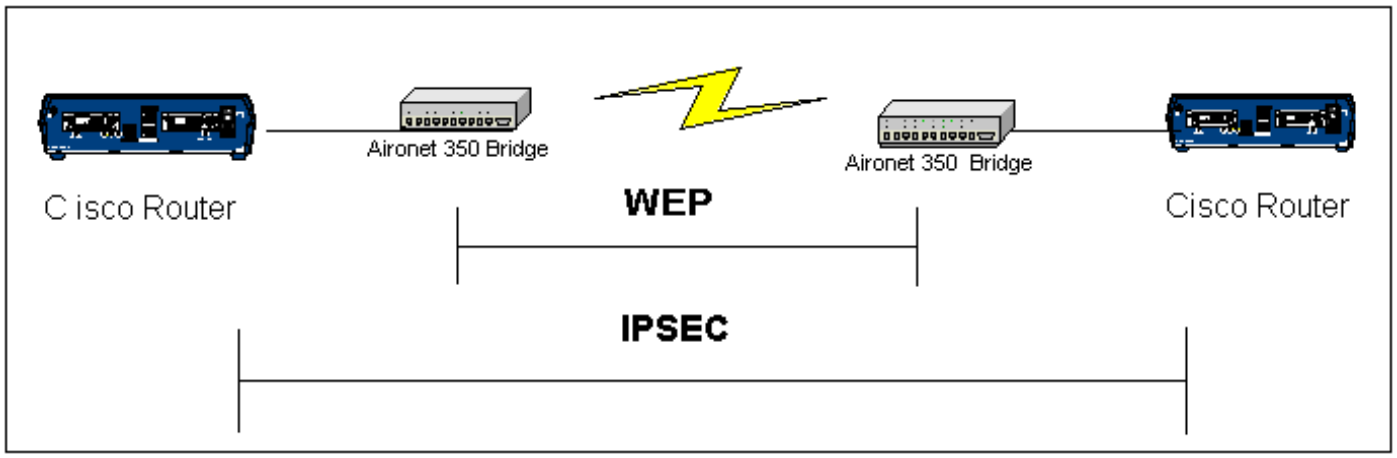
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi di IOS.

Esempio di rete

Nel documento viene usata l'impostazione di rete mostrata nel diagramma:



Configurazioni

Nel documento vengono usate queste configurazioni:

- RouterA
- RouterB
- Esempio di bridge

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
```

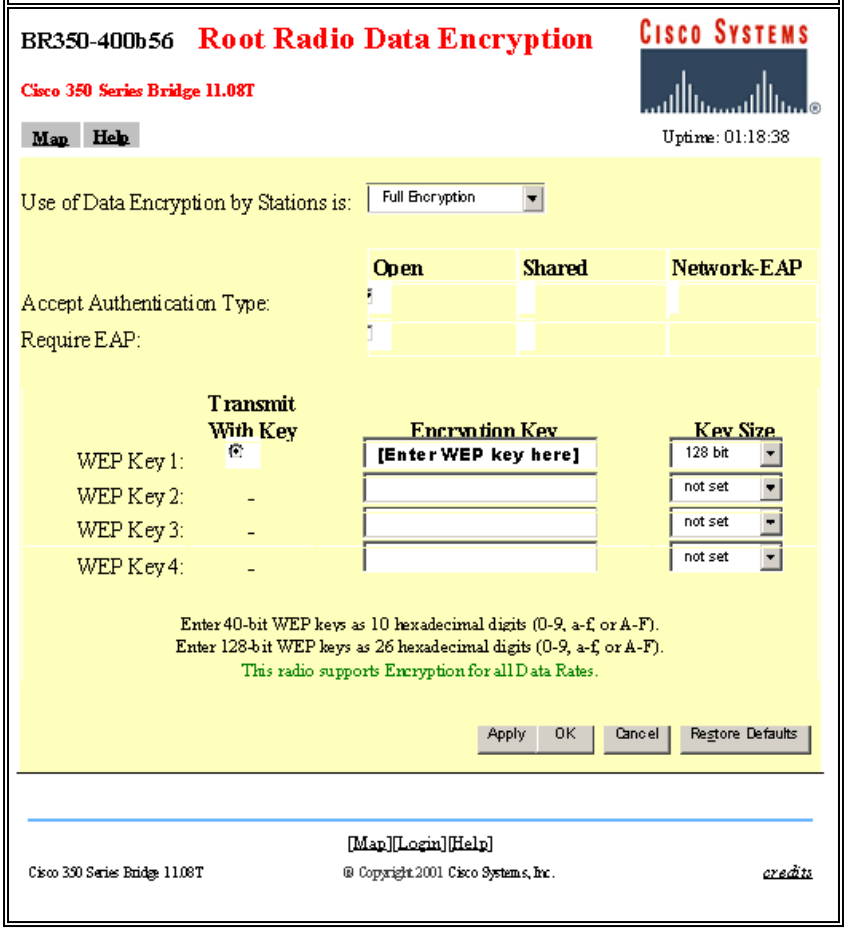
RouterB (Cisco 2600 Router)

```
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 Bridge



Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

- **show crypto engine connections active** - questo comando viene utilizzato per visualizzare le connessioni correnti attive alle sessioni crittografate

```
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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Per risolvere i problemi relativi alla connettività IPSEC, consultare:

- Risoluzione dei problemi di sicurezza IP - Informazioni e uso dei comandi di debug
- Configurazione e risoluzione dei problemi di Cisco Network-Layer Encryption: IPSec e ISAKMP, parte 1 e parte 2

Per la risoluzione dei problemi relativi alla connessione wireless, consultare:

- Strumento TAC Case Collection - LAN wireless
- Risoluzione dei problemi comuni delle reti con bridging wireless
- Risoluzione dei problemi di connettività in una rete LAN wireless

Informazioni correlate

- Supporto tecnico - LAN wireless
- Supporto tecnico - Negoziazione IPSec/protocolli IKE
- Supporto tecnico – Cisco Systems