目次

概要

イーサネット セグメント間のブリッジド ワイヤレス リンクを設計する際には、セキュリティを考慮することが重要です。 この文書では、IPSec トンネルを使用してブリッジド ワイヤレス リンクを通過するトラフィックのセキュリティを確保する方法を例示します。

この例では、2 つの Cisco Aironet 350 シリーズ ブリッジは WEP を確立します; 2 人のルータは IPSecトンネルを設定しました。

前提条件

要件

設定を開始する前にこれらの使用と快適であることを確認して下さい:

- Cisco Aironet ブリッジ設定 インターフェイス
- Cisco IOS コマンド ライン インターフェース

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- IOSバージョン 12.1 を実行する Cisco 2600 シリーズ ルータ
- ファームウェアのバージョン 11.08T を実行する Cisco Aironet 350 シリーズ ブリッジ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

背景理論

Cisco Aironet 340、350、および 1400 シリーズ ブリッジは 128-bit WEP暗号化まで提供します。これは WEP アルゴリズムのよく知られている な問題によるセキュア接続および不正利用の、WEP アルゴリズムのセキュリティに記述されているようにおよび Cisco Aironet 応答の容易さのために - 802.11 セキュリティの欠陥を押すために頼ることができません。

ワイヤレス ブリッジド リンクを通過するトラフィックのセキュリティを向上させる 1 つの方法は、リンクを使用するルータ間で暗号化された IPSec トンネルを作成する方法です。 この方法を使用できるのは、ブリッジが OSI モデルのレイヤ 2 で動作しているためです。 ブリッジ間の接続を利用するルータ間に IPSec を適用できます。

ワイヤレスリンクのセキュリティが破られる場合、残り、暗号化されて保護する含まれているトラフィック。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

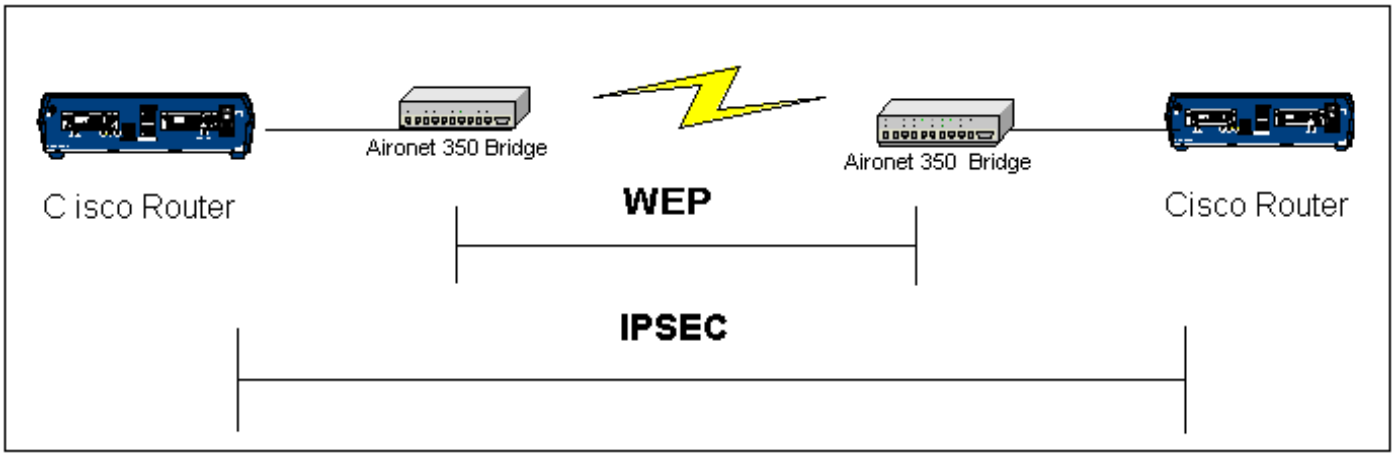
設定

このセクションでは、この文書で説明する機能を設定するために必要な情報を提供します。

注このドキュメントで使用されているコマンドに関する詳細情報について調べるには、IOS Command Lookup ツールを使用してください。

ネットワーク図

この文書では、次のダイヤグラムに示すネットワーク設定を使用します。



設定

このドキュメントでは、次の設定を使用します。

- RouterA
- RouterB
- ブリッジ例

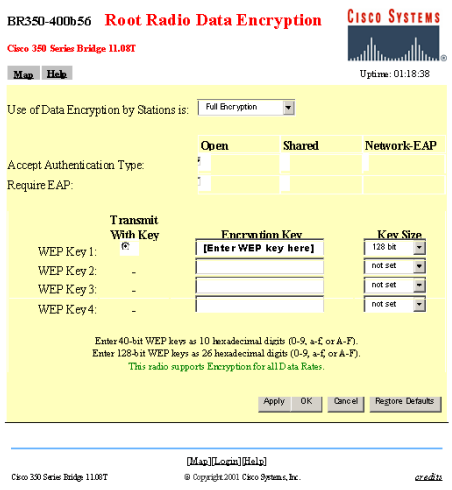
RouterA（Cisco 2600 ルータ）

```
RouterA#show running-config Building
configuration...Current configuration : 1258
bytes!version 12.1no service single-slot-reload-enableno
service padservice timestamps debug uptimeservice
timestamps log uptimeno service password-
encryption!hostname RouterA!logging rate-limit console
10 except errors!ip subnet-zerono ip fingerip dhcp
excluded-address 10.1.1.20ip dhcp excluded-address
10.1.1.30!ip dhcp pool wireless network 10.1.1.0
255.255.255.0!ip audit notify logip audit po max-events
100call rsvp-sync!crypto isakmp policy 10hash
md5authentication pre-sharecrypto isakmp key cisco
address 10.1.1.30!!crypto ipsec transform-set set esp-
3des esp-md5-hmac!crypto map vpn 10 ipsec-isakmpset peer
10.1.1.30set transform-set setmatch address
120!interface Loopback0ip address 20.1.1.1
255.255.255.0!interface Ethernet0ip address 10.1.1.20
255.255.255.0crypto map vpn!!ip classlessip route
0.0.0.0 0.0.0.0 10.1.1.30no ip http serverno 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 0transport input
noneline vty 0 4!end
```

RouterB（Cisco 2600 ルータ）

```
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-synccrypto
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 120interface 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 ブリッジ



確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- **show crypto engine connections active** 現在のアクティブな暗号化されたセッション接続を表示するのに-このコマンドが使用されています

```
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
```

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

IPSec 接続のトラブルシューティングについては、次の文書を参照してください。

- IP セキュリティ トラブルシューティングか。debug コマンドの説明と使用
- Cisco ネットワークレイヤの暗号化の設定とトラブルシューティング： IPSec および ISAKMP、Part 1 および Part 2

無線接続のトラブルシューティングために、以下を参照して下さい:

- TAC Case Collection ツール - ワイヤレス LAN
- ワイヤレス ブリッジド ネットワークに関する一般的な障害のトラブルシューティング
- ワイヤレス LAN ネットワークの接続に関するトラブルシューティング

関連情報

- テクニカル サポート：ワイヤレス LAN
- テクニカル サポート- IPSec ネゴシエーション/IKE プロトコル
- テクニカルサポート - Cisco Systems