ブリッジのセキュリティ

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 ブリッジが WEP を確立し、 2 つのルータが IPSEC トンネルをセットアップします。

前提条件

要件

この設定を試す前に、次の項目の使用に関して問題ないか確認してください。

- Cisco Aironet Bridge 設定インターフェイス
- Cisco IOS IOC コマンド ライン インターフェイス

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 を実行している Cisco2600 シリーズ ルータ
- ファームウェア バージョン 11.08T を実行している 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 ブリッジは最大 128 ビットの WEP 暗号化を提供します。 「WEP アルゴリズムのセキュリティ」および 「Cisco Aironet Response to Press - 802.11 セキュリティの欠陥」で説明したように、既知の WEP アルゴリズムの問題点とセキュリティ侵害の容易さのために、この暗号化機能はセキュアな接続に関しては信頼できません。

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侵害されても、それに含まれるトラフィックは引き続き暗号化されたままで安全です。

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
- ブリッジの例

RouterA (Cisco 2600 ルータ)

```
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 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-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 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** ：このコマンドは、現在アクティブな暗号化セッションの接続を表示するのに使用されます。

```
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 Security のトラブルシューティング：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、パート 1 および パート 2

ワイヤレス接続のトラブルシューティングについては、次を参照してください。

- 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