IS-IS 認証の設定

目次

概要

ルーティング テーブルに悪意のある情報が混入しないようにするために、ルーティング プロトコルの認証を設定することを推奨します。 このドキュメントでは、IP 用の Intermediate System-to-Intermediate System (IS-IS) を実行しているルータ間のクリア テキスト認証について説明します。

この資料は IS-IS クリアテキスト 認証だけを取り扱っています。 IS-IS 認証の他の型に関する詳細については IS-IS HMAC-MD5 認証および拡張 な クリアテキスト 認証を参照して下さい。

前提条件

要件

この ドキュメント を 読む人は IS-IS オペレーションおよび設定について詳しく知っているはずです。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。 この資料の設定は Cisco IOSバージョン 12.2(24a) を実行するテストされた on Cisco 2500 シリーズ ルータでした

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。

背景説明

規定 された リンク、エリア、またはドメインのためのパスワードの設定を IS-IS 可能に。 ルータ同士が隣接関係を結びたい場合、それぞれのルータで設定されている認証のレベルに対して同じパスワードを交換する必要があります。 適切なパスワードが設定されていないルータは、対応する機能（回線の初期化、エリアのメンバになること、レベル 2 のドメインのメンバになることなど）に関与することが禁止されます。

Cisco IOS ® ソフトウェアは IS-IS 認証の 3 つの型が設定されるようにします。

- **IS-IS 認証**—長い間、これは IS-IS のための認証を設定する唯一の方法でした。
- **IS-IS HMAC-MD5 認証**—この機能は各 IS-ISプロトコル データユニット（PDU）に HMAC-MD5 ダイジェストを追加します。 それは Cisco IOS ソフトウェア バージョン 12.2(13)T で導入され、限られた数 プラットフォームだけでサポートされます。
- **拡張 な クリアテキスト 認証**—この新しい 機能を使うと、クリアテキスト 認証はパスワードが暗号化されるようにする新しいコマンドを使用してソフトウェアコンフィギュレーションが表示するとき設定することができます。 それはまたパスワードを管理し、変更することももっと簡単にします。

注: ISIS MD-5 および拡張 な クリアテキスト 認証の情報に関しては IS-IS HMAC-MD5 認証および拡張 な クリアテキスト 認証を参照して下さい。

IS-ISプロトコルは、RFC 1142 で指定どおりに Hellos およびリンク状態パケット（LSP）の認証を LSP の一部として認証情報の包含を通って、提供します。 この認証情報は、Type Length Value（TLV）の 3 つの組み合わせとして符号化されています。 認証 TLV の種類は 10 です; TLV の長さは可変です; そして TLV の値は使用される認証種別によって決まります。 デフォルトでは、認証は無効にされています。

設定

このセクションはリンクの、エリアのためのおよびドメインのための IS-IS クリアテキスト 認証を設定する方法を論議します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

インターフェイス認証

インターフェイスの IS-IS 認証を設定するとき、または両方 Level 1/Level 2 ルーティング レベル 1 のためのパスワードを、レベル 2 の有効に する、ことができます。 レベルを規定 しない場合、デフォルトはレベル 1 であり、認証が設定されるレベルによるレベル 2.は、パスワード 対応した HELLO メッセージ送られます。 IS-IS インターフェイス認証のレベルは、そのインターフェイスでの隣接関係のタイプと一致している必要があります。 隣接関係の種類がある **show clns neighbor コマンドを**使用して下さい。 エリアやドメイン認証には、レベルを指定することはできません。

ネットワーク図、およびルータ A の Ethernet 0 とルータ B の Ethernet 0 でのインターフェイス認証の設定は次のとおりです。 ルータ A およびルータ B はレベル 1 およびレベル両方 2.のための IS-IS パスワード SECr3t で設定されます両方。 これらのパスワードは大文字/小文字が区別されます。

Connectionless Network Service (CLNS; コネクションレス型ネットワーク サービス) の IS-IS を使用して設定されたシスコ ルータ間では、CLNS 隣接関係はデフォルトで レベル 1 またはレベル 2 となります。 したがって、ルータ A およびルータ B では、レベル 1 またはレベル 2 のいずれか一方だけが特別に設定されない限り、両方のタイプの隣接関係を持つことになります。

ルータ A	ルータ B
interface ethernet 0 ip address 10.3.3.1 255.255.255.0 ip router isis isis password SECr3t interface ethernet1 ip address 10.1.1.1 255.255.255.0 ip router isis router isis net 49.1234.1111.1111.1111.00	interface ethernet 0 ip address 10.3.3.2 255.255.255.0 ip router isis isis password SECr3t interface ethernet1 ip address 172.16.1.1 255.255.255.0 ip router isis router isis net 49.1234.2222.2222.2222.00

エリア認証

エリア認証に関するネットワーク図と設定を次に示します。 エリア認証が設定されるとき、パスワードは L1 LSP、CSNPs および PSNPS 送られます。 すべてのルータが同一の IS-IS エリアである 49.1234 に属し、またすべてのルータに対してエリア パスワードとして「tiGHter」が設定されています。

ルータ A	ルータ B
interface ethernet 0 ip address 10.3.3.1 255.255.255.0 ip router isis interface ethernet1 ip address 10.1.1.1 255.255.255.0 ip router isis router isis net 49.1234.1111.1111.1111.00 **area-password tiGHter**	interface ethernet 0 ip address 10.3.3.2 255.255.255.0 ip router isis interface ethernet1 ip address 172.16.1.1 255.255.255.0 ip router isis router isis net 49.1234.2222.2222.2222.00 **area-password tiGHter**
ルータ C	**ルータ D**
interface ethernet1 ip address 172.16.1.2 255.255.255.0 ip router isis interface ethernet0 ip address 192.168.50.1 255.255.255.0 ip router isis	interface ethernet1 ip address 10.1.1.2 255.255.255.0 ip router isis interface ethernet0 ip address 192.168.50.2 255.255.255.0 ip router isis

router isis net 49.1234.3333.3333.3333.00 **area-password tiGHter**	router isis net 49.1234.4444.4444.4444.00 **area-password tiGHter**

ドメイン認証

ドメイン認証に関するネットワーク図と設定を次に示します。 ルータ A およびルータ B は IS-IS 領域 49.1234 にあります; ルータ C は IS-IS 領域 49.5678 にあります; そしてルータ D はエリア 49.9999 にあります。 これらのルータはすべて同一の IS-IS ドメインである 49 に属し、またすべてのルータに対してドメイン パスワードとして「seCurity」が設定されています。

ルータ A	ルータ B
interface ethernet 0 ip address 10.3.3.1 255.255.255.0 ip router isis interface ethernet1 ip address 10.1.1.1 255.255.255.0 ip router isis router isis net 49.1234.1111.1111.1111.00 **domain-password seCurity**	interface ethernet 0 ip address 10.3.3.2 255.255.255.0 ip router isis interface ethernet1 ip address 172.16.1.1 255.255.255.0 ip router isis router isis net 49.1234.2222.2222.2222.00 **domain-password seCurity**
ルータ C	**ルータ D**
interface ethernet1 ip address 172.16.1.2 255.255.255.0 ip router isis interface ethernet0 ip address 192.168.50.1 255.255.255.0 ip router isis router isis net 49.5678.3333.3333.3333.00 **domain-password seCurity**	interface ethernet1 ip address 10.1.1.2 255.255.255.0 ip router isis interface ethernet0 ip address 192.168.50.2 255.255.255.0 ip router isis router isis net 49.9999.4444.4444.4444.00 **domain-password seCurity**

ドメイン、エリア、インターフェイス認証の組み合わせ

このセクションのトポロジーおよびコンフィギュレーションの一部はドメイン、エリアおよびインターフェイス 認証の組み合せを説明します。 ルータ A とルータ B は同じエリアにあり、エリア パスワード「tiGHter」が設定されています。 ルータ C およびルータ D はルータ A およびルータ B.より 2 つの個別の領域に属します。 すべてのルータが同じドメインにあり、ドメインレベルのパスワードとして「seCurity」を共有しています。 ルータ B とルータ C には、これらの間でイーサネット回線が設定が行されています。 ルータ C およびルータ D は相手との L2 隣接関係だけ形成し、設定エリア パスワードが必要となりません。

ルータ A	ルータ B
interface ethernet 0 ip address 10.3.3.1	interface ethernet 0 ip address 10.3.3.2

255.255.255.0 ip router isis interface ethernet1 ip address 10.1.1.1 255.255.255.0 ip router isis router isis net 49.1234.1111.1111.1111.00 **domain-password seCurity** **area-password tiGHter**	255.255.255.0 ip router isis interface ethernet1 ip address 172.16.1.1 255.255.255.0 ip router isis clns router isis **isis password Fri3nd level-2** router isis net 49.1234.2222.2222.2222.00 **domain-passwordseCurity area-password tiGHter**

ルータ C	ルータ D
interface ethernet1 ip address 172.16.1.2 255.255.255.0 ip router isis **isis password Fri3nd level-2** interfaceethernet0 ip address 192.168.50.1 255.255.255.0 ip router isis router isis net 49.5678.3333.3333.3333.00 **domain-password seCurity**	interface ethernet1 ip address 10.1.1.2 255.255.255.0 ip router isis interface ethernet0 ip address 192.168.50.2 255.255.255.0 ip router isis router isis net 49.9999.4444.4444.4444.00 **domain-password seCurity**

確認

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。

インターフェイス 認証がきちんとはたらいているかどうか確認するために、ユーザか特権 EXECモードで EXEC **show clns neighbors コマンドを**使用して下さい。 コマンドの出力は接続の隣接タイプおよび状態を表示するものです。 **show clns neighbors コマンド**からのこの出力例は正しくインターフェイス 認証のために設定されるルータを示し、として状態を表示する:

```
RouterA# show clns neighbors System Id Interface SNPA State Holdtime Type Protocol RouterB Et0
0000.0c76.2882 Up 27 L1L2 IS-IS
```

エリアおよびドメイン 認証の場合、認証の確認は次の セクションで説明されているように debug コマンドを使用してすることができます。

トラブルシューティング

直接接続されたルータにリンクの一方で、およびない設定される認証が他方ではあればルータは CLNS IS-IS 隣接関係を形成しません。 次の図では、ルータ B では Ethernet 0 インターフェイスに対するインターフェイス認証が設定され、ルータ A では隣接するインターフェイスに認証が設定されていません。

```
Router_A# show clns neighbors System Id Interface SNPA State Holdtime Type Protocol Router_B Et0
00e0.b064.46ec Init 265 IS ES-IS Router_B# show clns neighbors
```

直接接続されたルータにリンクの一方で設定されるエリア認証がある場合 CLNS IS-IS 隣接関係は 2 つのルーティングの間で形成されます。 ただし、エリア認証が設定されるルータは設定され

るエリア認証無しで、CLNS ネイバーからの L1 LSP を受け入れません。 ただし、エリア認証無しのネイバーは L1 および L2 両方 LSP を受け入れ続けます。

これはエリア認証がルータ A のデバッグ メッセージで設定され、L1 LSP をのないルータ ネイバー（B）エリア認証から受け取ります:

```
Router_A# deb isis update-packets IS-IS Update related packet debugging is on Router_A# *Mar 1 00:47:14.755: ISIS-Upd: Rec L1 LSP 2222.2222.2222.00-00, seq 3, ht 1128, *Mar 1 00:47:14.759: ISIS-Upd: from SNPA 0000.0c76.2882 (Ethernet0) *Mar 1 00:47:14.763: ISIS-Upd: LSP authentication failed Router_A# *Mar 1 00:47:24.455: ISIS-Upd: Rec L1 LSP 2222.2222.2222.00-00, seq 3, ht 1118, *Mar 1 00:47:24.459: ISIS-Upd: from SNPA 0000.0c76.2882 (Ethernet0) *Mar 1 00:47:24.463: ISIS-Upd: LSP authentication failed RouterA#
```

1 つのルータのドメイン 認証を設定する場合、ドメイン 認証を設定してもらわないルータからの L2 LSP を拒否します。 認証を設定される認証があるルータからの LSP を受け入れるために設定してもらわないルータ。

次のデバッグ出力では、LSP 認証の失敗を示しています。 ルータ CA はエリアかドメイン 認証のために設定され、ドメインかパスワード認証のために設定されないルータ（ルータ DB）からの受信 レベル 2 LSP です。

```
Router_A# debug isis update-packets IS-IS Update related packet debugging is on Router_A# *Mar 1 02:32:48.315: ISIS-Upd: Rec L2 LSP 2222.2222.2222.00-00, seq 8, ht 374, *Mar 1 02:32:48.319: ISIS-Upd: from SNPA 0000.0c76.2882 (Ethernet0) *Mar 1 02:32:48.319: ISIS-Upd: LSP authentication failed Router_A# *Mar 1 02:32:57.723: ISIS-Upd: Rec L2 LSP 2222.2222.2222.00-00, seq 8, ht 365, *Mar 1 02:32:57.727: ISIS-Upd: from SNPA 0000.0c76.2882 (Ethernet0) *Mar 1 02:32:57.727: ISIS-Upd: LSP authentication failed
```

関連情報

- IS-IS に関するサポートページ
- IP ルーティング プロトコルに関するサポート ページ
- IP ルーティングに関するサポート ページ
- テクニカルサポート - Cisco Systems