ASA/PIX および OSPF の設定例

内容

概要 前提条件 要件 使用するコンポーネント 関連製品 表記法 背景説明 設定 ネットワーク図 設定 ASDM の設定 <u>OSPF 認証の設定</u> <u>Cisco ASA CLI 設定</u> <u>Cisco IOS ルータ(R2) CLI 設定</u> Cisco IOS ルータ(R1) CLI 設定 <u>Cisco IOS ルータ(R3) CLI 設定</u> ASA による OSPF への再配布 確認 トラブルシュート ポイントツーポイント ネットワーク向けのスタティック ネイバー設定 トラブルシューティングのためのコマンド 関連情報

<u>概要</u>

このドキュメントでは、Open Shortest Path First(OSPF)を介してルートを学習し、認証およ び再配布を実行するように、Cisco ASA を設定する方法について説明します。

EIGRP 設定の詳細については、『<u>PIX/ASA 8.x:Cisco Adaptive Security Appliance(ASA)での</u> <u>EIGRP の設定</u>』を参照してください。

注:非対称ルーティングはASA/PIXではサポートされていません。

前提条件

<u>要件</u>

この設定を行う前に、次の要件が満たされていることを確認します。

- Cisco ASA/PIX は、バージョン 7.x 以降を実行する必要があります。
- OSPF は、マルチコンテキスト モードではサポートされていません。これは、シングル モードのみでサポートされます。

<u>使用するコンポーネント</u>

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いています。

ソフトウェア バージョン 8.0 以降が稼働する Cisco 5500 シリーズ適応型セキュリティ アプ
 ライアンス(ASA)

• Cisco Adaptive Security Device Manager(ASDM) ソフトウェア バージョン 6.0 以降 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ました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、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。

関連製品

このドキュメントの情報は、ソフトウェア バージョン 8.0 以降が稼働する Cisco 500 シリーズ PIX ファイアウォールにも適用できます。

<u>表記法</u>

ドキュメント表記の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してくだ さい。

<u>背景説明</u>

OSPF は、すべての既知の宛先までの最短パスを構築および計算するために、リンクステート ア ルゴリズムを使用します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイ スと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれて います。

RIP に比べると OSPF は次の点で有利です。

- OSPF のリンクステート データベースのアップデート送信は RIP ほど頻繁ではありません。
 また、古くなった情報のタイムアウトで徐々にアップデートされるのではなく、リンクステート データベースは瞬時にアップデートされます。
- ルーティング決定はコストに基づいて行われます。これは、特定のインターフェイスを介してパケットを送信するためにオーバーヘッドが必要であることを示しています。セキュリティアプライアンスは、インターフェイスのコストをリンク帯域幅に基づいて計算し、宛先までのホップ数は使用しません。コストは優先パスを指定するために設定できます。

最短パス優先アルゴリズムの欠点は、CPU サイクルとメモリが大量に必要になることです。

セキュリティ アプライアンスは、OSPF プロトコルのプロセス 2 つを異なるインターフェイス セット上で同時に実行できます。同じ IP アドレスを使用する複数のインターフェイス(NAT で はこのようなインターフェイスは共存可能ですが、OSPF ではアドレスの重複は許可されません)があるときに、2 つのプロセスを実行する場合があります。 あるいは、一方のプロセスを内部 で実行しながら別のプロセスを外部で実行し、ルートのサブセットをこの 2 つのプロセス間で再 配布する場合もあります。同様に、プライベート アドレスをパブリック アドレスから分離する必要がある場合もあります。

OSPF ルーティング プロセスには、別の OSPF ルーティング プロセスや RIP ルーティング プロ セスから、または OSPF 対応インターフェイスに設定されているスタティック ルートおよび接続 されているルートから、ルートを再配布できます。

セキュリティ アプライアンスは、次の OSPF 機能をサポートします。

- エリア内ルート、エリア間ルート、および外部ルート(タイプ | とタイプ |)のサポート
- 仮想リンクのサポート
- OSPF の LSA フラッディング
- OSPF パケットの認証(パスワード認証と MD5 認証の両方)
- セキュリティアプライアンスの指定ルータまたは指定バックアップルータとしての設定のサポート。セキュリティアプライアンスは、ABRとして設定することもできます。ただし、セキュリティアプライアンスのASBRとしての設定は、デフォルト情報のみに制限されます(たとえば、デフォルトルートのインジェクトなど)。
- スタブ エリアと not so stubby エリアのサポート
- ABR タイプ 3 LSA フィルタリング

<u>設定</u>

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供して います。

注:このセクションで使用さ<u>れるコマンドの詳細を調べる</u>には、<u>Command Lookup Tool(登録</u>ユ ーザ専用)を使用してください。

<u>ネットワーク図</u>

このドキュメントでは、次のネットワーク セットアップを使用します。



このネットワークトポロジでは、Cisco ASA内部インターフェイスのIPアドレスは10.1.1.1/24で す。目標は、隣接ルータ(R2)を介して内部ネットワーク(172.16.1.0/24、172.16.2.0/24、 172.16.5.0/24、および172.16.10.0/24)へのルートを動的にに学習するために、Cisco ASAに OSPFを設定します。R2 は、他の 2 つのルータ(R1 と R3)を介したリモート内部ネットワーク へのルートを学習します。

<u>設定</u>

このドキュメントでは、次の構成を使用します。

- <u>ASDM の設定</u>
- OSPF 認証の設定
- Cisco ASA CLI 設定
- <u>Cisco IOS ルータ(R2)CLI 設定</u>
- <u>Cisco IOS ルータ (R1) CLI 設定</u>
- <u>Cisco IOS ルータ(R3)CLI 設定</u>
- <u>ASA による OSPF への再配布</u>

<u>ASDM の設定</u>

Adaptive Security Device Manager (ASDM)は、セキュリティ アプライアンスのソフトウェアの 設定およびモニタに使用されるブラウザベースのアプリケーションです。ASDM は、セキュリテ ィ アプライアンスからロードされ、デバイスの設定、モニタ、管理に使用されます。また、 ASDM Launcher (Windows のみ)を使用して、Java アプレットより高速に ASDM アプリケーシ ョンを起動することもできます。ここでは、この ASDM のマニュアルで説明する機能を設定する 際に必要な情報を説明します。

Cisco ASA で OSPF を設定するには、次の手順を実行してください。

- 1. Cisco ASA の ASDM にログインします。
- 2. この図に示すように、ASDM インターフェイスの [Configuration] > [Device Setup] > [Routing] > [OSPF] エリアに移動します。



3. この図に示すように、[Setup] > [Process Instances] タブで OSPF ルーティング プロセスを イネーブルにします。この例では、OSPF ID プロセスは 1 です。

D	evice Setup 라무×	Configuration > Device Setup > Routing > OSPF > Setup
Device List	Startup Wizard Interfaces Startup Wizard Interfaces Static Routes Static Routes Static Routes Filtering Filtering Static Neighbor Summary Address Virtual Link EIGRP	Configuration > Device Setup > Routing > OSPF > Setup Enable at least one OSPF Processs Instance and define areas and area network Process Instances Area / Networks Route Summarization Maximum of two OSPF processes can be configured on this device. To rem the checkbox. OSPF Process 1 Image: Comparison of two OSPF Process 1 Advance Image: OSPF Process 2 Image: Enable this OSPF Process OSPF Process 1D: Image: Enable this OSPF Process OSPF Process 1D: Advance OSPF Process 1D: Advance
	Remote Access VPN Site-to-Site VPN Device Management	Apply Reset

4. [Setup > Process Instances] タブで [Advanced] をクリックして、オプションの高度な OSPF ルーティング プロセス パラメータを設定できます。[Router ID]、[Adjacency Changes]、[Administrative Route Distances]、[Timers] および [Default Information Originate] 設定など、プロセス固有の設定を編集できます。

it OSPF Process Advanced Properties	
OSPE Process:	Router ID: 10.1.1.1
Ignore LSA MOSPF (suppress the sending of syslog messages when router receives a LSA MOSPF packets)	RFC1583 Compatible (calculate ✓ summary route costs per RFC 1583)
Adjacency Changes	
Enable this for the firewall to send a syslog message when an OSPF neighbor goes up/down.	Enable this for the firewall to send a syslog for each state change.
🔽 Log Adjacency Changes	🔲 Log Adjacency Change Details
Administrative Route Distances	
Inter Area (distance for all Intra Area (di routes from one area to within an area another area)	a) External (distance for all routes from other routing domains, learned by redistribution)
110 110	110
Timers (in seconds)	
SPF Delay Time (between when OSPF receives a topology change and when it starts a SPF calculation)	e (between two LSA Group Pacing (interval at which iPF calculations) OSPF LSAs are collected into a group and refreshed)
5 10	240
Default Information Originate	
Configure this to generate default external route into	o an OSPF routing domain.
Enable Default Information Originate	Always advertise the default route
Metric Value: 1 Metric Type:	2 💌 Route Map:
OK Car	ncel Help

このリストは各フィールドについて説明します。[OSPF Process]:設定している OSPF プロセスを表示します。この値は変更できません。[Router ID]:固定のルータ ID を使用する には、[Router ID] フィールドにルータ ID を IP アドレス形式で入力します。この値をブラン クのままにした場合、セキュリティ アプライアンスで最上位の IP アドレスがルータ ID と して使用されます。この例では、[Router ID] は、内部インターフェイス(10.1.1.1)の IP ア ドレスで静的に設定されます。[Ignore LSA MOSPF]:セキュリティ アプライアンスがタイ プ 6 (MOSPF) LSA パケットを受信するときにシステム ログ メッセージの設定を抑制する には、このチェックボックスをオンにします。デフォルトでは、この設定はオフになってい ます。[RFC 1583 Compatible]: RFC 1583 あたりのサマリー ルート コストを計算するには 、このチェックボックスをオンにします。RFC 2328 あたりのサマリー ルート コストを計 算するには、このチェックボックスをオフにします。ルーティング ループの可能性を最小 限に抑えるには、OSPF ルーティング ドメイン内のすべての OSPF デバイスに同じように RFC 互換性が設定されている必要があります。この設定は、デフォルトでオンになってい ます。[Adjacency Changes]:隣接関係の変更を定義する設定が含まれます。隣接関係が変 更されると、システム ログ メッセージが送信されます。[Log Adjacency Changes]: OSPF

ネイバーが起動またはダウンしたときだけでなく、セキュリティ アプライアンスがシステ ム ログ メッセージを送信するようにするには、このチェックボックスをオンにします。こ の設定は、デフォルトでオンになっています。[Log Adjacency Changes Detail]:ネイバーが 起動またはダウンしたときだけでなく、状態の変更が発生するたびにセキュリティ アプラ イアンスがシステム ログ メッセージを送信するようにするには、このチェックボックスを オンにします。デフォルトでは、この設定はオフになっています。[Administrative Route Distances]: ルート タイプに基づくルートのアドミニストレーティブ ディスタンスの設定を 含みます。[Inter Area]:1つのエリアから別のエリアへのすべてのルートのアドミニストレ ーティブ ディスタンスを設定します。有効な値の範囲は1~255です。既定値は100です。 [Intra Area]:エリア内のすべてのルートのアドミニストレーティブ ディスタンスを設定しま す。有効な値の範囲は1~255です。既定値は100です。[External]:再配布を通じて取得さ れる他のルーティング ドメインからのすべてのルートのアドミニストレーティブ ディスタ ンスを設定します。有効な値の範囲は1 ~ 255です。既定値は100です。[Timers] : LSA ペー シングおよび SPF 計算タイマーの設定に使用する設定が含まれます。[SPF Delay Time]:OSPFがトポロジの変更を受信してからSPFの計算を開始するまでの時間を指定しま す。有効な値の範囲は0~ 65535です。既定値は5です。[SPFホールドタイム(SPF Hold Time)]:連続するSPF計算の間のホールドタイムを指定します。有効な値の範囲は1~ 65534です。デフォルト値は10です。[LSAグループペーシング(LSA Group Pacing)]:LSAが グループに収集され、更新、チェックサム、またはエージングされる間隔を指定します。有 効な値の範囲は 10 ~ 1800 です。デフォルト値は 240 です。[Default Information Originate]: ASBR がデフォルトの外部ルートを OSPF ルーティング ドメインに生成すると きに使用する設定を含みます。[Enable Default Information Originate]: OSPF ルーティング ドメインへのデフォルト ルートの生成をイネーブルにするには、このチェックボックスを オンにします。[Always advertise the default route]: デフォルト ルートを常にアドバタイズ するには、このチェックボックスをオンにします。このオプションは、デフォルトではオフ になっています。[Metric Value]: OSPF デフォルト メトリックを指定します。有効な値の 範囲は0 ~ 16777214です。既定値は1です。[Metric Type]:OSPF ルーティング ドメインに アドバタイズされたデフォルト ルートに関連付けられた外部リンク タイプを指定します。 有効値は1または2です。それぞれタイプ1またはタイプ2外部ルートを示します。デフ オルト値は 2 です。[Route Map]: (任意)適用するルート マップの名前です。ルート マッ プが一致すると、ルーティング プロセスによってデフォルト ルートが生成されます。

5. これまでの手順を完了したら、[Setup] > [Area/Networks] タブで OSPF ルーティングに参加 するネットワークおよびインターフェイスを定義し、この図に示すように、[Add] をクリッ クします。

	Networks	Authentication	Options	Cost [
--	----------	----------------	---------	--------

[Add OSPF Area] ダイアログ ボックスが表示されます。

d OSPF Area				
OSPF Process:	1		Area ID: 0	
Area Type				
💿 Normal				
C Stub	🔽 Summary (allo	ws sending LSAs	into the stub area)	
O NSSA	🔽 Redistribute (imports routes to	normal and NSSA are	eas)
	🔽 Summary (allo	ws sending LSAs	into the NSSA area)	
	🔲 Default Infor	nation Originate (generate a Type 7 d	efault)
	Metric Valu	e: 1	Metric Type: 2	
		I		
- Area Network	s			
Enter IP Ad	dress and Mask	1	IP Address	Netmask
		(10.1.1.0	255.255.255.0
IP Address:		Add >>		
Netmask:	255.255.255.0			
	·	Delete		
Authenticatio	n	_		
None	C Password	C MD5	Default Cost:	1
	(ок)	Cancel	Help	

この例では、OSPF が内部インターフェイスのみでイネーフルにされているため、追加され るネットワークだけが内部ネットワーク(10.1.1.0/24)です。**注:定義された**ネットワーク 内にあるIPアドレスを持つインターフェイスだけが、OSPFルーティングプロセスに参加し ます。

6. [OK] をクリックします。このリストは各フィールドについて説明します。[OSPF

Process]:新しいエリアを追加する場合、OSPF プロセスの ID を選択します。セキュリテ ィ アプライアンスでイネーブルにされている OSPF プロセスが 1 つだけの場合、そのプロ セスがデフォルトで選択されます。既存のエリアを編集する場合、OSPF プロセス ID は変 更できません。[Area ID]:新しいエリアを追加する場合、エリア ID を入力します。このエ リア ID には、10 進数か IP アドレスを指定できます。有効な10進数値の範囲は0 ~ 4294967295です。既存のエリアを編集する場合は、エリアIDを変更できません。この例で は、[Area ID] は 0 です。[Area Type]:設定しているエリアのタイプに対する設定を含みま す。[Normal]:このエリアを標準の OSPF エリアにする場合、このオプションを選択します 。エリアを最初に作成するときは、このオプションがデフォルトで選択されています。 [Stub]:このエリアをスタブ エリアにする場合、このオプションを選択します。スタブ エリ アには、その向こう側にルータまたはエリアはありません。スタブ エリアでは、AS External LSA(タイプ 5 LSA)がスタブ エリアにフラッディングされないようになっていま す。スタブ エリアを作成する場合、[Summary] チェックボックスをオフにして、サマリー LSA(タイプ 3 および 4)がエリアにフラッディングされないようにします。

[Summary]:エリアがスタブエリアとして定義される場合、LSA がスタブエリアに送信さ れないようにこのチェックボックスをオフにします。スタブ エリアの場合、このチェック ボックスはデフォルトでオンになっています。[NSSA]:エリアをnot-so-stubbyエリアにす るには、このオプションを選択します。NSSA はタイプ 7 LSA を受け入れます。NSSA を 作成する場合、[Summary] チェックボックスをオフにして、サマリー LSA がエリアにフラ ッディングされないようにします。また、[Redistribute] チェックボックスをオフにし、 [Default Information Originate] をイネーブルにして、ルート再配布をディセーブルにするこ ともできます。[Redistribute]: ルートが NSSA にインポートされないようにするには、この チェックボックスをオフにします。このチェックボックスは、デフォルトでオンになってい ます。[Summary]:エリアが NSSA として定義される場合、LSA がスタブ エリアに送信さ れないようにこのチェックボックスをオフにします。NSSA の場合、このチェックボックス はデフォルトでオンになっています。[Default Information Originate]: タイプ 7 デフォルト を NSSA に生成するには、このチェックボックスをオンにします。このチェックボックス は、デフォルトでオフになっています。[Metric Value]: デフォルト ルートの OSPF メトリ ック値を指定するには、値を入力します。有効な値の範囲は0~16777214です。既定値は 1です。[Metric Type]: デフォルト ルートの OSPF メトリック タイプを指定するには、値を 入力します。選択肢は1(タイプ1)または2(タイプ2)です。 デフォルト値は2です。 [Area Networks]: OSPF エリアを定義する設定を含めます。[Enter IP Address and Mask]:そのエリア内のネットワークを定義するのに使用する設定を含みます。[IP Address]:そのエリアに追加するネットワークまたはホストの IP アドレスを入力します。 デフォルト エリアを作成するには、0.0.0.0 およびネットマスク 0.0.0.0 を使用します。 0.0.0.0 は 1 つのエリア内だけで使用できます。[Netmask]:エリアに追加する IP アドレス またはホストのネットワーク マスクを選択します。ホストを追加する場合、 255.255.255.255 マスクを選択します。この例では、10.1.1.0/24 は、設定されるネットワー クです。[Add]: [Enter IP Address and Mask] エリアで定義したネットワークをエリアに追 加します。追加されたネットワークは、[Area Networks] テーブルに表示されます。 [Delete]:選択したネットワークを [Area Networks] テーブルから削除します。[Area Networks]:そのエリアに対して定義されたネットワークを表示します。[IP Address]:ネッ トワークの IP アドレスを表示します。[Netmask]:ネットワークのネットワーク マスクを 表示します。[Authentication]: OSPF エリア認証の設定が含まれます。[None]: OSPF エリ ア認証をディセーブルにするには、このオプションを選択します。これがデフォルト設定で す。[Password]:エリア認証用のクリア テキスト パスワードを使用する場合、このオプシ ョンを選択します。セキュリティ面が懸念される場合、このオプションは推奨しません。 [MD5]:MD5認証を使用するには、このオプションを選択します。[Default Cost]:エリアのデ フォルトコストを指定します。有効な値の範囲は0~65535です。既定値は1です。 7. [Apply] をクリックします。

Configure the are	ea properties and a	area networks for	OSPF Process	
OSPF Process	Area ID	Area Type	Networks	Authe
1	0	Normal	10.1.1.0 / 255.255.255.0	None
				_
•				•

- 8. オプションで、[Filter Rules] ペインでルート フィルタを定義できます。ルート フィルタに より、OSPF 更新で送受信することを許可されているルートをより細かく制御できます。
- オプションで、ルート再配布を設定できます。Cisco ASA は、RIP および EIGRP により検 出されるルートを OSPF ルーティング プロセスに再配布できます。スタティック ルートお よび接続されているルートも、OSPF ルーティング プロセスに再配布できます。
 [Redistribution] ペインでルート再配布を定義します。
- 10. OSPF hello パケットはマルチキャスト パケットとして送信されます。OSPF ネイバーが、 トンネルなど、非ブロードキャスト ネットワークを越えた場所にある場合、そのネイバー を手動で定義する必要があります。手動で OSPF ネイバーを定義すると、hello パケットは ユニキャスト メッセージとしてそのネイバーに送信されます。スタティック OSPF ネイバ ーを定義するには、[Static Neighbor] ペインに移動します。
- 11. 他のルーティング プロトコルから学習したルートをサマライズできます。サマリーのアド バタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです 。サマリー ルートは、ルーティング テーブルのサイズを削減するのに役立ちます。OSPF のサマリー ルートを使用すると、OSPF ASBR は、そのアドレスでカバーされるすべての 再配布ルートの集約として、1 つの外部ルートをアドバタイズします。OSPF に再配布さ れている、他のルーティング プロトコルからのルートだけをサマライズできます。
- IVirtual link] ペインで、エリアを OSPF ネットワークに追加できます。ただし、エリアを バックボーン エリアに直接接続することはできません。この場合、仮想リンクを作成する 必要があります。仮想リンクは、通過エリアと呼ばれる共通エリアを持つ 2 つの OSPF デ バイスを接続します。OSPF デバイスのいずれかは、バックボーン エリアに接続されてい る必要があります。

<u>OSPF 認証の設定</u>

Cisco ASA は、OSPF ルーティング プロトコルからのルーティング アップデートの MD5 認証を サポートします。MD5 キーを使用したダイジェストが各 OSPF パケットに含まれており、承認 されていない送信元からの不正なルーティング メッセージや虚偽のルーティング メッセージが取 り込まれないように阻止します。認証を OSPF メッセージに追加すると、ルータおよび Cisco ASA のみが、同じ事前共有キーで設定される他のルーティング デバイスからルーティング メッ セージを受信します。この認証を設定しない場合、ネットワークへの異なるまたは逆方向のルー ト情報を持つ別のルーティング デバイスが別のユーザにより導入されると、ルータまたは Cisco ASA のルーティング テーブルが破損し、Denial of Service 攻撃が発生します。ルーティング デ バイス(ASA を含む)間で送信される EIGRP メッセージに認証を追加すると、意図する場合で もしない場合でも別のルータがネットワークに追加されたり、問題が発生したりすることを回避 できます。

OSPF ルート認証は、インターフェイスごとに設定します。OSPF メッセージ認証対象として設定されたインターフェイス上にあるすべての OSPF ネイバーには、隣接関係を確立できるように同じ認証モードとキーを設定する必要があります。

Cisco ASA で OSPF MD5 認証をイネーブルにするには、次の手順を実行します。

1. ASDM で、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Interface] に移動して、 この図に示すように、[Authentication] タブをクリックします。

Interf	ace	Authentication Type	
inside	dee	Area	_
dmz		Area	
outside		Area	

- この場合、OSPF は、内部インターフェイスでイネーブルにされます。
- 2. [inside] インターフェイスを選択して、[Edit] をクリックします。
- 3. [Authentication] で、[MD5 authentication] を選択して、認証パラメータに関する情報を追加 します。この場合は、事前共有キーは cisco123 であり、キー ID は 1 です。

Interface: Inside Authentication Area authentication, if defined Password authentication MD5 authentication Authentication Password Password authentication MD5 authentication Authentication Password enerry Password: enerry Password: Enter Password: enerry Password: mostery Password: MD5 IDs and Keys mostery Password: mostery Password: MD5 Key ID: Actor mostery Password: MD5 Key ID: Actor mostery Password: MD5 Key: Delete mostery Password: MD5 Key: Delete mostery Password: Vectory 7 UC T, [Apply] & 20 U Y 7 U E t at the password: mostery Password: Specify the authentication properties for each interface: Muthentication Type Interface: Authentication Type mostery Password: Interface: Mostery Password: Area	Interface: inside	
Interface: Inside Authentication C Area authentication, if defined C Password authentication C MD5 authentication Authentication Password Enter Password: Enter Password: Re-enter Password: MDS IDs and Keys MD5 Key ID MD5 MDS Key ID: Add D MD5 I ciscol23 MDS Key: Delete Help Enter Password Cancel Help MD5 Key: Delete Help MD5 Key: Delete Help Enterface Sectip X Equivo 2 U v 2 U v 2 U z 3. Granteel Help Iterface Help Help Specify the authentication properties for each interface. Interface Interface Authentication Type Inside MD5 Interface Authentication Type Inside MD5	Authentication	
Authentication C Area authentication, if defined C Password authentication C MDS authentication Authentication Password Enter Password: Enter Password: Re-enter Password: MD5 IDs and Keys MDS Key ID MD5 Key ID: Add MD5 Key: Delete Specify the pathentication > Device Setup > Routing > OSPF > Interface Configure Interface specific OSPF routing parameters. Authentication Properties Specify the authentication properties for each interface. Interface Authentication Type Inside MD5 MD5 Area	Authentication	
No authentication Area authentication Password authentication Authentication Password Enter Password: Re-enter Password: MD5 IDs and Keys MD5 Key ID: Add MD5 Key ID: Add Delete MD5 Key: Delete Delete Delete Delete Delete Specify the authentication properties for each interface. Interface Authentication Type dnz dutside Authentication Type		
Password authentication Authentication Password Enter Password: MD5 IDs and Keys MD5 Key ID: MD5 Key ID: MD5 Key: Delete Delete Delete Delete Delete Delete </td <td>C No authentication</td> <td>O Area authentication, if defined</td>	C No authentication	O Area authentication, if defined
Authentication Password Enter Password: MD5 IDs and Keys MD5 Key ID: MD5 Key: Delete Help Acd Help Acd MD5 Key: Delete Help Acd Help Acd Help Acd Help Acd Help Acca Acca Acca	C Password authentication	MD5 authentication
Enter Password: Re-enter Password: MD5 IDs and Keys MD5 Key ID: MD5 Key: OK Cancel Help Enterface Specific OSPF routing parameters. MD5 Rey: Interface Specific OSPF routing parameters. Interface Authentication Type Inside MD5 MD5 MD5 MD5 MD5 MD5 MD5 MD5	Authentication Password	
MD5 IDs and Keys MD5 Key ID MD5 MD5 Key ID: Add I cisco123 MD5 Key: Delete Delete MD5 Key: Delete Help E OK Cancel Help E ØV OV Cancel Help E ØV ØV Delete Help E ØV ØV ØV ØV Delete NO Outside ØV ØV ØV ØV ØV ØV ØV ØV ØV ØV ØV ØV Ø	Enter Password:	Re-enter Password:
MD5 Key ID: Add MD5 Key: Delete MD5 Key: Delete OK Cancel Help E E E Figuration > Device Setup > Routing > OSPF > Interface) onfigure Interface specific OSPF routing parameters. uthentication Properties Specify the authentication properties for each interface. Interface Authentication Type Inside MD5 dm2 Area outside Area	MD5 IDs and Keys	
MD5 Key: Delete OK Cancel Help をクリックして、[Apply] をクリックします。 figuration > Device Setup > Routing > OSPF > Interface) onfigure Interface specific OSPF routing parameters. withentication Properties Specify the authentication properties for each interface. Interface Authentication Type Inside MD5 dmz Area outside Area	MD5 Key ID:	MD5 Key ID MD5 Ke Add
OK Cancel Help ● をクリックして、[Apply] をクリックします。	MD5 Key:	Delete
をクリックして、[Apply] をクリックします。 figuration > Device Setup > Routing > OSPF > Interface onfigure Interface specific OSPF routing parameters. Authentication Properties Specify the authentication properties for each interface. Interface Authentication Type inside MD5 dmz Area outside Area	OK	Cancel Help
Interface specific OSPF routing parameters. withentication Properties Specify the authentication properties for each interface. Interface Authentication Type inside MD5 dmz Area outside Area	をクリックして、[Apply] をクリックし	,ます。 Ex Interface
Interface Authentication Type Interface MD5 dmz Area outside Area	nguration > bevice setup > Routing > OSP	r > Interface)
Specify the authentication properties for each interface. Interface Authentication Type inside MD5 dmz Area outside Area	uthentication properties	eters.
Interface Authentication Type Inside MD5 dmz Area outside Area	Specify the authentication properties for each	interface
Interface Authentication Type inside MD5 dmz outside Area	pectry the addicitication properties for each	ricertace.
dmz Area outside Area	Interface	Authentication Type
outside Area		MD5
	outside	Area

<u>Cisco ASA CLI 設定</u>

Cisco ASA

```
ciscoasa#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!--- Inside interface configuration interface
Ethernet0/1 nameif inside security-level 100 ip address
10.1.1.1 255.255.255.0 ospf cost 10 !--- OSPF
authentication is configured on the inside interface
ospf message-digest-key 1 md5 <removed> ospf
authentication message-digest ! !--- Outside interface
configuration interface Ethernet0/2 nameif outside
security-level 0 ip address 192.168.1.2 255.255.255.0
ospf cost 10 ! !--- Output Suppressed icmp unreachable
rate-limit 1 burst-size 1 asdm image disk0:/asdm-602.bin
no asdm history enable arp timeout 14400 ! !--- OSPF
Configuration router ospf 1
network 10.1.1.0 255.255.255.0 area 0
log-adj-changes
!
!--- This is the static default gateway configuration in
order to reach Internet route outside 0.0.0.0 0.0.0.0
192.168.1.1 1 ciscoasa#
```

<u>Cisco IOS ルータ(R2)CLI 設定</u>

Cisco IOS ルータ(R2) !--- Interface that connects to the Cisco ASA. !---Notice the OSPF authentication parameters interface Ethernet0 ip address 10.1.1.2 255.255.255.0 ip ospf authentication message-digest ip ospf message-digest-key 1 md5 cisco123 !--- Output Suppressed !--- OSPF Configuration router ospf 1 log-adjacency-changes network 10.1.1.0 0.0.0.255 area 0 network 172.16.1.0 0.0.0.255 area 0 network 172.16.2.0 0.0.0.255 area 0

<u>Cisco IOS ルータ(R1)CLI 設定</u>

Cisco IOS ルータ(R1)

```
!--- Output Suppressed !--- OSPF Configuration router
ospf 1
log-adjacency-changes
network 172.16.5.0 0.0.0.255 area 0
```

<u>Cisco IOS ルータ(R3)CLI 設定</u>

Cisco IOS ルータ (R3)

<pre>! Output Suppressed ! OSPF Configuration router</pre>	
ospf 1	
log-adjacency-changes	
network 172.16.1.0 0.0.0.255 area 0	
network 172.16.10.0 0.0.0.255 area 0	

<u>ASA による OSPF への再配布</u>

上記のとおり、OSPF ルーティング プロセスには、別の OSPF ルーティング プロセスや RIP ル ーティング プロセスから、または OSPF 対応インターフェイスに設定されているスタティック ルートおよび接続されているルートから、ルートを再配布できます。

この例では、次のようなネットワーク図で、RIP ルートを OSPF に再配布します。



ASDM の設定

1. [Configuration] > [Device Setup] > [Routing] > [RIP] > [Setup] を選択し、RIP をイネーブルに して、次の図に示すように、ネットワーク 192.168.1.0 を追加します。

Configuration > Device Setup > Routing > RIP > Setup
Configure the global Routing Information Protocol (RIP) parameters. You can configure the setting or the RIP routing process.
Enable auto-summarization
🔽 Enable RIP version 🛛 🔿 Version 1 💿 Version 2
(If global version in not configured then device sends Version 1 and receives Versions 1 $\&$ 2.)
Enable default information originate Route Map:
Networks
IP Network to Add: Add >> 192.168.1.0
Delete
Passive Interfaces
Global passive: Configure all the Interface Passive interfaces as passive globally. This inside setting will override the individual dmz
(Apply) Reset
[Apply] をクリックします。

3. [Configuration] > [Device Setup] > [Routing] > [OSPF] > [Redistribution] > [Add] を選択して 、RIP ルートを OSPF に再配布します。

OSPF Process	Protocol	Match	Subnets	Metric Value	Metric Type

4. [OK] をクリックして、[Apply] をクリックします。

OSPF Process:	1	•	C Static	C Connected	I C OSPF	Γ
Optional		5	-			- 89
1. 2						
Match						
Match	External 1	F Exte	rnal 2 🗖	NSSA External 1	MS54 E	kte
Match	F External 1	Exte	rnal 2 🗖	NSSA External 1	🗖 NSSA E	kter
Match	External 1	Exte	rnal 2 🗖 2 🔽 Ta	N55A External 1		kter
Match Internal Metric Value:	External 1	Exte	rnal 2 🔽 2 💽 Ta	N55A External 1 ag Value:	r NSSA E	kte se :

同等の CLI 設定

RIP を OSPF AS に再配布するための ASA の CLI 設定
router ospf 1
network 10.1.1.0 255.255.255.0 area 0
log-adj-changes
redistribute rip subnets
router rip
network 192.168.1.0

RIP ルートを OSPF AS に再配布したら、ネイバー IOS ルータ(R2)のルーティング テーブル を参照できます。

R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
0 172.16.10.1/32 [110/11] via 172.16.1.2, 01:17:29, Ethernet1
0 172.16.5.1/32 [110/65] via 172.16.2.2, 01:17:29, Serial1
C 172.16.1.0/24 is directly connected, Ethernet1
C 172.16.2.0/24 is directly connected, Serial1
10.0.0/24 is subnetted, 1 subnets
C 10.1.1.0 is directly connected, Ethernet0

確認

設定を確認するには、次の手順を実行します。

1. ASDM で、[Monitoring] > [Routing] > [OSPF Neighbors] に移動し、各 OSPF ネイバーを確 認できます。この図は、アクティブ ネイバーとしての内部ルータ(R2)を示しています。 このネイバーが常駐するインターフェイス、ネイバー ルータ ID、状態、デッド タイムも確 認できます。

Each row represen	ts one OSPF Neigl	hbor. Please clicl	< the help button for	a description of	the states.
Neighbor	Priority	State	Dead Time	Address	Inter
172.16.2.1	1 F	ULL/BDR	0:00:34 1	10.1.1.2	inside)

2. また、[Monitoring] > [Routing] > [Routes] に移動して、ルーティング テーブルを確認できます。この図では、the 172.16.1.0/24、172.16.2.0/24、172.16.5.0/24 および 172.16.10.0/24 ネットワークが、R2(10.1.1.2)を介して学習されます。
 Monitoring > Routing > Routes

tes					
Each row represer	nts one route. AD is	the administrative dista	ince.		
Protocol	Туре	Destination IP	Netmask	Gateway	Т
OSPF	-	172.16.10.1	255.255.255.255	10.1.1.2	ins
OSPF	-	172.16.5.1	255.255.255.255	10.1.1.2	ins
OSPF	-	172.16.1.0	255.255.255.0	10.1.1.2	ins
OSPF	-	172.16.2.0	255.255.255.0	10.1.1.2	ins
CONNECTED	-	10.1.1.0	255.255.255.0	-	ins
CONNECTED	-	10.77.241.128	255.255.255.192	-	dn
STATIC	-	10.77.0.0	255.255.0.0	10.77.241.129	dn
CONNECTED	-	192.168.1.0	255.255.255.0	-	ou
STATIC	DEFAULT	0.0.0.0	0.0.0.0	192.168.1.1	OL

3. CLIから、show route command コマンドを使用して、同じ出力を取得できます。 ciscoasa#show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

- 0 172.16.10.1 255.255.255 [110/21] via 10.1.1.2, 0:00:06, inside
- 0 172.16.5.1 255.255.255.255 [110/75] via 10.1.1.2, 0:00:06, inside
- 0 172.16.1.0 255.255.255.0 [110/20] via 10.1.1.2, 0:00:06, inside
- 0 172.16.2.0 255.255.255.0 [110/74] via 10.1.1.2, 0:00:06, inside
- C 10.1.1.0 255.255.255.0 is directly connected, inside
- C 10.77.241.128 255.255.192 is directly connected, dmz
- S 10.77.0.0 255.255.0.0 [1/0] via 10.77.241.129, dmz
- C 192.168.1.0 255.255.255.0 is directly connected, outside
- S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.1.1, outside

4. また、show ospf database コマンドを使用して、学習したネットワークおよび ospf トポロ ジに関する情報を取得することもできます。

ciscoasa#**show ospf database**

OSPF Router with ID (192.168.1.2) (Process ID 1)

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum Link count
172.16.1.2	172.16.1.2	123	0x80000039	0xfd1d 2
172.16.2.1	172.16.2.1	775	0x8000003c	0x9b42 4
172.16.5.1	172.16.5.1	308	0x80000038	0xb91b 3
192.168.1.2	192.168.1.2	1038	0x80000037	0x29d7 1

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
10.1.1.1	192.168.1.2	1038	0x8000034	0x72ee
172.16.1.1	172.16.2.1	282	0x80000036	0x9e68

5. show ospf neighbors コマンドは、アクティブ ネイバーおよび対応情報の確認にも役に立ち ます。この例では、手順1で ASDM から取得した情報と同じ情報を示します。 ciscoasa#show ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.16.2.1	1	FULL/BDR	0:00:36	10.1.1.2	inside

<u>トラブルシュート</u>

このセクションでは、OSPF 問題のトラブルシューティングに役に立つ情報を提供します。

ポイントツーポイント ネットワーク向けのスタティック ネイバー設定

ASA で OSPF ネットワークをポイントツーポイント 非ブロードキャストとして設定している場合、スタティック OSPF ネイバーを定義して、ポイントツーポイント非ブロードキャスト ネット ワーク上で OSPF ルートをアドバタイズする必要があります。詳細については、『<u>スタティック</u> OSPF ネイバーの定義』を参照してください。

<u>トラブルシューティングのためのコマンド</u>

<u>アウトプット インタープリタ ツール(登録ユーザ専用)(OIT)は、特定の show コマンドをサ</u> <u>ポートします。</u>OIT を使用して、show コマンドの出力の分析を表示します。

注:<u>debug</u> コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

```
• debug ospf events : OSPF イベントのデバッグをイネーブルにします。
 ciscoasa(config)#debug ospf events
 OSPF events debugging is on
 ciscoasa(config)# int e0/1
 ciscoasa(config-if)# no shu
 ciscoasa(config-if)#
 OSPF: Interface inside going Up
 OSPF: Send with youngest Key 1
 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
 OSPF: 2 Way Communication to 172.16.2.1 on inside, state 2WAY
 OSPF: Backup seen Event before WAIT timer on inside
 OSPF: DR/BDR election on inside
 OSPF: Elect BDR 172.16.2.1
 OSPF: Elect DR 172.16.2.1
       DR: 172.16.2.1 (Id) BDR: 172.16.2.1 (Id)
 OSPF: Send DBD to 172.16.2.1 on inside seq 0xlabd opt 0x2 flag 0x7 len 32
 OSPF: Send with youngest Key 1
 OSPF: End of hello processing
 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
 OSPF: End of hello processing
 OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x12f3 opt 0x42 flag 0x7 len 32 mtu
  1500 state EXSTART
 OSPF: First DBD and we are not SLAVE
 OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abd opt 0x42 flag 0x2 len 152 mt
 u 1500 state EXSTART
 OSPF: NBR Negotiation Done. We are the MASTER
 OSPF: Send DBD to 172.16.2.1 on inside seq 0xlabe opt 0x2 flag 0x3 len 132
 OSPF: Send with youngest Key 1
 OSPF: Send with youngest Key 1
 OSPF: Database request to 172.16.2.1
 OSPF: sent LS REQ packet to 10.1.1.2, length 12
 OSPF: Rcv DBD from 172.16.2.1 on inside seq 0xlabe opt 0x42 flag 0x0 len 32 mtu
  1500 state EXCHANGE
 OSPF: Send DBD to 172.16.2.1 on inside seq 0xlabf opt 0x2 flag 0x1 len 32
 OSPF: Send with youngest Key 1
 OSPF: Send with youngest Key 1
 OSPF: Rcv DBD from 172.16.2.1 on inside seq 0xlabf opt 0x42 flag 0x0 len 32 mtu
  1500 state EXCHANGE
 OSPF: Exchange Done with 172.16.2.1 on inside
 OSPF: Synchronized with 172.16.2.1 on inside, state FULL
 OSPF: Send with youngest Key 1
 OSPF: Send with youngest Key 1
 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
 OSPF: Neighbor change Event on interface inside
 OSPF: DR/BDR election on inside
 OSPF: Elect BDR 192.168.1.2
 OSPF: Elect DR 172.16.2.1
 OSPF: Elect BDR 192.168.1.2
 OSPF: Elect DR 172.16.2.1
       DR: 172.16.2.1 (Id)
                            BDR: 192.168.1.2 (Id)
 OSPF: End of hello processing
 OSPF: Send with youngest Key 1
 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
 OSPF: End of hello processing
 OSPF: Send with youngest Key 1
 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
 OSPF: End of hello processing
 OSPF: Send with youngest Key 1
 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
 OSPF: End of hello processing
```

OSPF: Send with youngest Key 1 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: End of hello processing

注:問題のトラブルシューティングに役立つさまざまなコマンドの詳細については、『 Ciscoセキュリティアプライアンスコマンドリファレンス、バージョン8.0』の「<u>debug</u> <u>ospf</u>」セクションを参照してください。

<u>関連情報</u>

- Cisco 5500 シリーズ適応型セキュリティ アプライアンスに関するサポート ページ
- <u>Cisco 500 シリーズ PIX に関するサポート ページ</u>
- ・ PIX/ASA 8.X: Cisco Adaptive Security Appliance (ASA)の EIGRP の設定
- <u>テクニカル サポートとドキュメント Cisco Systems</u>