ファイアウォールおよび NAT 対応の Sun RPC ALG サポート

ファイアウォールおよび NAT 対応の Sun RPC ALG サポート機能により、ファイアウォールにおける Sun Microsystems（Sun）Remote Procedure Call（RPC; リモート プロシージャ コール）Application Layer Gateway（ALG; アプリケーション レイヤ ゲートウェイ）のサポート、および Network Address Translation（NAT; ネットワーク アドレス変換）のサポートが追加されます。Sun RPC は、リモート サーバ プログラム内の関数をクライアント プログラムが呼び出すことができるようにするアプリケーション レイヤ プロトコルです。

機能情報の検索

ご使用のソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、ご使用のプラットフォームおよびソフトウェア リリースのリリースノートを参照してください。このモジュールに記載されている機能に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの機能情報」（P.13）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、およびシスコのソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

ファイアウォールおよび NAT 対応の Sun RPC ALG サポートに関する制約事項

- ポートマッパー バージョン 2 のみサポートされます。
- RPC バージョン 2 のみサポートされます。

ファイアウォールおよび NAT 対応の Sun RPC ALG サポートについて

Sun RPC

Sun RPC ALG は、Sun RPC プロトコルのディープ パケット インスペクションを提供します。Sun RPC ALG は、管理者が一致フィルタを設定できるプロビジョニング システムと連動します。一致フィルタは、Sun RPC パケット内の検索で使用される一致基準を定義し、それにより、基準に一致するパケットのみ許可されます。

RPC では、クライアント プログラムは、サーバ プログラム内の関数を呼び出します。RPC ライブラリは、プロシージャ引数をネットワーク メッセージ内にパッケージ化し、それをサーバに送信します。次にサーバは、RPC ライブラリを使用して、ネットワーク メッセージから引数を取り出し、指定されたサーバ プロシージャを呼び出します。サーバ関数が戻り値を返すと、その戻り値がネットワーク メッセージ内にパッケージ化され、クライアントに送り返されます。

Sun RPC プロトコルの詳細については、RFC 1057、『*RPC: Remote Procedure Call Protocol Specification Version 2*』を参照してください。

ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの設定方法

ファイアウォールおよび NAT がイネーブルの場合に Sun RPC を動作させるには、ALG で Sun RPC パケットを検査する必要があります。また ALG で、ダイナミック ファイアウォール セッションの確立、NAT 変換後のパケット コンテンツの修正など、Sun RPC 固有の問題を処理する必要もあります。

ここでは、次の作業について説明します。

Sun RPC ALG 対応のファイアウォールの設定

Sun RPC は、ポリシーおよびクラス マップを使用して作成するゾーンベースのファイアウォールを使用して設定します。レイヤ 7 クラス マップを使用することで、管理者は、一致フィルタを設定できます。このフィルタでは、Sun RPC パケット内で検索するプログラム番号を指定します。Sun RPC レイヤ 7 ポリシー マップは、**service-policy** コマンドを使用するレイヤ 4 ポリシー マップの子ポリシーとして設定します。

Sun RPC レイヤ 4 クラス マップが設定され、一方でレイヤ 7 ファイアウォール ポリシーが設定されていない場合、Sun RPC により戻されるトラフィックはファイアウォールを通過できますが、レイヤ 7 レベルではセッションは検査されません。この結果、後続の RPC 呼び出しはファイアウォールによりブロックされます。Sun RPC レイヤ 4 クラス マップおよびレイヤ 7 ポリシーを設定すると、レイヤ 7 インスペクションが使用できるようになります。空のレイヤ 7 ファイアウォール ポリシー、つまり、一致フィルタが設定されていないレイヤ 7 ファイアウォール ポリシーを設定できます。

ファイアウォールの設定には、次の作業が含まれます。

制約事項

- シスコは、同じインターフェイスに対してセキュリティ ゾーンと検査ルールの両方を設定することを推奨していません。
- Sun RPC プロトコルを検査する場合（つまり、レイヤ 4 クラス マップで **match protocol sunrpc** コマンドを指定した場合）、レイヤ 7 Sun RPC ポリシー マップが必要になります。

ゾーンベースのファイアウォール ポリシーの詳細については、『*Cisco* IOS Security Configuration Guide: Securing the Data Plane』の「Zone-Based Firewall Policy」モジュールを参照してください。

レイヤ 7 ファイアウォール ポリシー対応のクラス マップの設定

ネットワーク トラフィックを分類するためのクラス マップを設定するには、この作業を実行します。この設定により、Sun RPC を使用する mount（100005）、Network File System（NFS; ネットワーク ファイル システム）（100003）などのプログラムが使用できるようになります。100005 および 100003 は Sun RPC プログラムの番号です。デフォルトでは、Sun RPC ALG はすべてのプログラムをブロックします。

Sun RPC プログラムおよびプログラム番号の詳細については、RFC 1057、『*RPC: Remote Procedure Call Protocol Specification Version 2*』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect** *protocol-name* {**match-any** | **match-all**} *class-map-name*
4. **match program-number** *program-number*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect** *protocol-name* {**match-any** | **match-all**} *class-map-name* **例：** `Router(config)# class-map type inspect sunrpc match-any sunrpc-l7-cmap`	レイヤ 7（アプリケーション固有）検査タイプ クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。
ステップ 4	**match program-number** *program-number* **例：** `Router(config-cmap)# match program-number 100005`	許可する RPC プロトコル プログラム番号を一致基準として指定します。
ステップ 5	**exit** **例：** `Router(config-cmap)# exit`	クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

レイヤ 3 およびレイヤ 4 ファイアウォール ポリシー対応のクラス マップの設定

ネットワーク トラフィックを分類するためのクラス マップを設定するには、この作業を実行します。完全一致基準を指定すると、Sun RPC トラフィックは、クラスのすべての Sun RPC レイヤ 7 フィルタ（プログラム番号として指定）に従います。部分一致基準を指定すると、Sun RPC トラフィックは、クラスの Sun RPC レイヤ 7 フィルタ（プログラム番号として指定）の少なくとも 1 つに従います。

手順の概要

1. **class-map type inspect** {**match-any** | **match-all**} *class-map-name*
2. **match protocol** *protocol-name*
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**class-map type inspect** {**match-any** | **match-all**} *class-map-name* **例：** `Router(config)# class-map type inspect match-any sunrpc-l4-cmap`	レイヤ 3 およびレイヤ 4 検査タイプ クラス マップを作成し、クラス マップ タイプ コンフィギュレーション モードを開始します。
ステップ 2	**match protocol** *protocol-name* **例：** `Router(config-cmap)# match protocol sunrpc`	指定したプロトコルに基づいてクラス マップの一致基準を設定します。
ステップ 3	**exit** **例：** `Router(config-cmap)# exit`	クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

Sun RPC ファイアウォール ポリシー マップの設定

Sun RPC ファイアウォール ポリシー マップを設定するには、この作業を実行します。ポリシー マップを使用して、レイヤ 7 ファイアウォール ポリシーのクラス マップで定義する Sun RPC レイヤ 7 クラスごとにパケット転送を許可します。

手順の概要

1. **policy-map type inspect** *protocol-name policy-map-name*
2. **class type inspect** *protocol-name class-map-name*
3. **allow**
4. **exit**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**policy-map type inspect** *protocol-name policy-map-name* **例：** `Router(config)# policy-map type inspect sunrpc sunrpc-l7-pmap`	レイヤ 7（プロトコル固有）検査タイプ ポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 2	**class type inspect** *protocol-name class-map-name* **例：** `Router(config-pmap)# class type inspect sunrpc sunrpc-l7-cmap`	アクションを実行する対象のトラフィック（クラス）を指定し、ポリシー マップ クラス コンフィギュレーションを開始します。
ステップ 3	**allow** **例：** `Router(config-pmap-c)# allow`	パケット転送を許可します。
ステップ 4	**exit** **例：** `Router(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 5	**exit** **例：** `Router(config-pmap)# exit`	ポリシー マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

レイヤ 4 クラスとレイヤ 7 ポリシー マップの関連付け

レイヤ 4 クラスおよびレイヤ 7 ポリシー マップを割り当てるには、この作業を実行します。

手順の概要

1. **policy-map type inspect** *policy-map-name*
2. **class type inspect** *class-map-name*
3. **inspect** [*parameter-map-name*]
4. **service-policy** *protocol-name policy-map-name*
5. **exit**
6. **class class-default**
7. **drop**
8. **exit**
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**policy-map type inspect** *policy-map-name* **例：** `Router(config)# policy-map type inspect sunrpc-l4-pmap`	レイヤ 3 およびレイヤ 4 検査タイプ ポリシー マップを作成し、ポリシー マップ コンフィギュレーションを開始します。
ステップ 2	**class type inspect** *class-map-name* **例：** `Router(config-pmap)# class type inspect sunrpc-l4-cmap`	アクションを実行する対象のトラフィック（クラス）を指定し、ポリシー マップ クラス コンフィギュレーションを開始します。
ステップ 3	**inspect** [*parameter-map-name*] **例：** `Router(config-pmap-c)# inspect`	Cisco IOS ステートフル パケット インスペクションをイネーブルにします。
ステップ 4	**service-policy** *protocol-name policy-map-name* **例：** `Router(config-pmap-c)# service-policy sunrpc sunrpc-l7-pmap`	レイヤ 7 ポリシー マップをトップレベルのレイヤ 3 またはレイヤ 4 ポリシー マップにアタッチします。
ステップ 5	**exit** **例：** `Router(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 6	**class class-default** **例：** `Router(config-pmap)# class class-default`	ポリシーを設定する前にデフォルト クラス（一般的にクラス デフォルト クラスと呼ばれます）を指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 7	**drop** **例：** `Router(config-pmap-c)# drop`	特定のクラスに属するパケットを廃棄するトラフィック クラスを設定します。
ステップ 8	**exit** **例：** `Router(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 9	**exit** **例：** `Router(config-pmap)# exit`	ポリシー マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

セキュリティ ゾーンとゾーン ペアの作成、およびポリシー マップのゾーン ペアへのアタッチ

ゾーン ペアを作成するには、2 つのセキュリティ ゾーンが必要です。ただし、1 つのセキュリティ ゾーンのみ作成でき、もう 1 つのセキュリティ ゾーンはシステム定義のセキュリティ ゾーンにすることができます。システム定義のセキュリティ ゾーンを作成するには、**self** キーワードを指定した **zone-pair security** コマンドを設定します。

（注） セルフ ゾーンを選択する場合、検査ポリシングは設定できません。

次の作業を順番どおりに完了します。

- 少なくとも 1 つのセキュリティ ゾーンを作成します。
- ゾーン ペアを定義します。
- インターフェイスをセキュリティ ゾーンに割り当てます。
- ポリシー マップをゾーン ペアにアタッチします。

セキュリティ ゾーンの制約事項

- インターフェイスをゾーンとレガシー検査ポリシーの両方に同時に所属させることはできません。
- インターフェイスは、1 つのセキュリティ ゾーンのみにメンバとして所属させることができます。
- インターフェイスがセキュリティ ゾーンのメンバである場合、そのインターフェイスへのトラフィックおよびそのインターフェイスからのトラフィックはすべてブロックされます。ただし、そのゾーンを含むゾーン ペアに対して明示的なゾーン間ポリシーを設定した場合は、この限りではありません。
- セキュリティ ゾーンのメンバであるインターフェイスと、セキュリティ ゾーンのメンバでないインターフェイスの間でトラフィックを流すことはできません。これは、2 つのゾーン間でしかポリシーを適用できないためです。
- ルータのすべてのインターフェイス間でトラフィックが流れるようにするには、インターフェイスを少なくとも 1 つのセキュリティ ゾーンのメンバにする必要があります。インターフェイスをセキュリティ ゾーンのメンバにした後、ポリシー アクション（検査、通過など）でパケット転送を明示的に許可する必要があるため、これは特に重要です。これを行わないと、パケットはドロップされます。
- ルータのインターフェイスをセキュリティ ゾーンまたはファイアウォール ポリシーに所属させることができない場合、そのインターフェイスをセキュリティ ゾーンに追加し、そのゾーンとトラフィック フローの対象となる他のゾーンとの間に、すべて通過ポリシー（つまり、ダミー ポリシー）を設定する必要があります。
- セキュリティ ゾーンとゾーン ペアの間で Access Control List（ACL; アクセス コントロール リスト）は適用できません。トラフィックをドロップするには、ACL 設定をクラス マップに含め、ポリシー マップを使用します。
- セキュリティ ゾーン内のすべてのインターフェイスは、同じ Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンスに属している必要があります。
- メンバ インターフェイスが個別の VRF にあるセキュリティ ゾーン間でポリシーを設定できます。ただし、設定で許可されていない場合、これらの VRF 間をトラフィックは流れません。トラフィックが VRF 間を流れない場合（VRF 間のルートリークが設定されていないため）、VRF 間のポリシーは実行されません。これは、ポリシー側ではなく、ルーティング側の設定の問題です。
- 同じセキュリティ ゾーン内のインターフェイス間のトラフィックはポリシーには従わず、自由に通過します。

- ゾーン ペアの送信元ゾーンおよび宛先ゾーンは、タイプ セキュリティのゾーンである必要があります。
- 同じゾーンを送信元ゾーンと宛先ゾーンの両方として定義することはできません。

手順の概要

1. **zone security** {*zone-name* | **default**}
2. **exit**
3. **zone security** {*zone-name* | **default**}
4. **exit**
5. **zone-pair security** *zone-pair-name* **source** {*source-zone-name* | **self** | **default**} **destination** {*destination-zone-name* | **self** | **default**}
6. **service-policy type inspect** *policy-map-name*
7. **exit**
8. **interface** *type number*
9. **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
10. **zone-member security** *zone-name*
11. **exit**
12. **interface** *type number*
13. **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
14. **zone-member security** *zone-name*
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**zone security** {*zone-name* | **default**} **例：** `Router(config)# zone security z-client`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 2	**exit** **例：** `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 3	**zone security** {*zone-name* | **default**} **例：** `Router(config)# zone security z-server`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** **例：** `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

ステップ 5	**zone-pair security** *zone-pair-name* **source** {*source-zone-name* | **self** | **default**} **destination** {*destination-zone-name* | **self** | **default**} **例：** `Router(config)# zone-pair security clt2srv source z-client destination z-server`	ゾーン ペアを作成し、ゾーンペア コンフィギュレーション モードを開始します。
ステップ 6	**service-policy type inspect** *policy-map-name* **例：** `Router(config-sec-zone-pair)# service-policy type inspect sunrpc-l4-pmap`	ファイアウォール ポリシー マップをゾーン ペアにアタッチします。
ステップ 7	**exit** **例：** `Router(config-sec-zone-pair)# exit`	ゾーンペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *type number* **例：** `Router(config)# interface Serial2/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]] **例：** `Router(config-if)# ip address 192.168.6.5 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 10	**zone-member security** *zone-name* **例：** `Router(config-if)# zone-member security z-client`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 11	**exit** **例：** `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**interface** *type number* **例：** `Router(config)# interface Serial2/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 13	**ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]] **例：** `Router(config-if)# ip address 192.168.6.5 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。

ステップ 14	**zone-member security** *zone-name* **例：** `Router(config-if)# zone-member security z-server`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 15	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

Sun RPC ALG 対応の NAT の設定

デフォルトでは、NAT をイネーブルにすると、Sun RPC ALG は自動的にイネーブルになります。NAT のみの設定では Sun RPC ALG を明示的にイネーブルにする必要はありません。NAT において Sun RPC ALG をディセーブルにするには、**no ip nat service alg** コマンドを使用します。

ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの設定例

ここでは、次の設定例について説明します。

- 「例：Sun RPC ALG 対応のファイアウォールの設定」（P.11）

例：Sun RPC ALG 対応のファイアウォールの設定

以下は、Sun RPC ALG サポート対応のファイアウォールの設定例です。

```
class-map type inspect sunrpc match-any sunrpc-l7-cmap
 match program-number 100005
class-map type inspect match-any sunrpc-l4-cmap
 match protocol sunrpc
!
!
policy-map type inspect sunrpc sunrpc-l7-pmap
 class type inspect sunrpc sunrpc-l7-cmap
  allow
policy-map type inspect sunrpc-l4-pmap
 class type inspect sunrpc-l4-cmap
  inspect
  service-policy sunrpc sunrpc-l7-pmap
 class class-default
  drop
!
zone security z-client
zone security z-server
zone-pair security clt2srv source z-client destination z-server
 service-policy type inspect sunrpc-l4-pmap
!
interface GigabitEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 zone-member security z-client
!
```

```
interface GigabitEthernet0/2
 ip address 192.168.23.1 255.255.255.0
 zone-member security z-server
```

参考資料

関連資料

関連項目	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
IP アドレッシング コマンド	『*Cisco IOS IP Addressing Command Reference*』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
ファイアウォール	『*Cisco IOS Security Configuration Guide: Securing the Data Plane*』の「Zone-Based Firewall Policy」モジュール
NAT	『*Cisco IOS IP Addressing Configuration Guide*』の「Configuring NAT」モジュール

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能で変更された既存規格のサポートはありません。	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、シスコのソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1057	『*RPC: Remote Procedure Call Protocol Specification Version 2*』

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポートおよびドキュメンテーション Web サイトでは、オンライン リソースを提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。これらのリソースは、ソフトウェアのインストールと設定や、シスコ製品とテクノロジーに関する技術上の問題のトラブルシューティングおよび解決に使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの機能情報

表 1 に、この機能のリリース履歴を示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの機能情報

機能名	リリース	機能情報
ファイアウォールおよび NAT 対応の Sun RPC ALG サポート	15.1(1)S	ファイアウォールおよび NAT 対応の Sun RPC ALG サポート機能は、ファイアウォールおよび NAT における Sun RPC ALG のサポートを追加します。