ファイアウォールおよびNAT対応のMSRPC ALGサポート

ファイアウォールおよびNAT対応のMSRPC ALGサポート機能は、ファイアウォールおよびネットワーク アドレス変換（NAT）での、Microsoft（MS）リモート プロシージャ コール（RPC）アプリケーション レベル ゲートウェイ（ALG）のサポートを提供します。MSRPC ALGは、MSRPCプロトコルのディープ パケット インスペクション（DPI）を提供します。MSRPC ALGは、ネットワーク管理者に、MSRPC パケットで検索可能な一致基準を定義するための一致フィルタの設定を許可するプロビジョニング システムと連携します。

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

- パケットにMSRPC ALGを適用する前に、Cisco IOS XE ファイアウォールとNATをイネーブルにする必要があります。

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

- TCP-based MSRPC のみがサポートされます。
- **allow** および **reset** コマンドを同時に設定することはできません。
- DPI に **match protocol msrpc** コマンドを設定する必要があります。

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

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション層ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内のIPアドレス情報を変換するアプリケーションです。 ALG はアプリケーション層プロトコルを解釈し、ファイアウォールおよびネットワーク アドレス変換（NAT）アクションを実行するために使用されます。 これらのアクションは、ファイアウォールおよび NAT の設定に応じた次の 1 つ以上のアクションです。

- ダイナミック TCP または UDP ポートを使用したサーバ アプリケーションとの通信をクライアント アプリケーションに許可します。
- アプリケーション固有のコマンドを認識し、それらのコマンドに対するきめ細かなセキュリティ制御を提供します。
- データ交換を行う 2 台のホスト間のデータの複数のストリームまたはセッションを同期します。
- アプリケーション ペイロードで使用可能なネットワーク層アドレス情報を変換します。

ファイアウォールがピンホールを開き、NATは、アプリケーション層データ ストリームで送信元および宛先 IP アドレスを伝送しない TCP または UDP トラフィックで変換サービスを実行します。 IPアドレス情報を埋め込む特定のプロトコルまたはアプリケーションには、ALGのサポートが必要です。

MSRPC

MSRPCは、サーバおよび企業に対し一連のアプリケーションとサービスを公開するために開発者が使用するフレームワークです。 RPCは、クライアントおよびサーバ ソフトウェアがネットワークを介して通信できるようにするための、プロセス間通信技術です。 MSRPC は、さまざまな

Microsoft アプリケーションが使用するアプリケーション層プロトコルです。 MSRPC は、さまざまなトランスポート プロトコルで、コネクション型（CO）およびコネクレションレス型（CL）両方の分散コンピューティング環境（DCE）RPC モードをサポートします。 MSRPC のすべてのサービスで、プライマリ接続と呼ばれる最初のセッションが確立されます。 MSRPC の一部のサービスにより、1024 ～ 65535 の間のポート範囲を宛先ポートとして、セカンダリ セッションが確立されます。

ファイアウォールおよび NAT がイネーブルになったときに MSRPC が動作するようにするには、MSRPC パケットのインスペクションに加え、ALG で、ダイナミック ファイアウォール セッションの確立や、NAT 後のパケット コンテンツの修正など、MSRPC 固有の問題を処理する必要があります。

MSRPC プロトコル インスペクションを適用すると、ほとんどの MSRPC サービスがサポートされるため、レイヤ 7 ポリシー フィルタが不要になります。

ファイアウォールでの MSRPC ALG

MSRPC プロトコルを検査するようにファイアウォールを設定すると、MSRPC ALG によって MSRPC メッセージの解析が開始されます。 次の表は、ファイアウォールおよび NAT 対応の MSRPC ALG サポート機能でサポートされるプロトコル データ ユニット（PDU）のタイプについて説明しています。

表 *1*：サポートされる *PDU* タイプ

PDU	番号	タイプ	説明
REQUEST	0	コール	コール要求を開始します。
RESPONSE	2	コール	コール要求に応答します。
FAULT	3	コール	RPC ランタイム、RPC スタブ、または RPC 固有の例外を示します。
BIND	11	アソシエーション	本文データのプレゼンテーションのネゴシエーションを開始します。
BIND_ACK	12	アソシエーション	バインド要求を受け入れます。
BIND_NAK	13	アソシエーション	アソシエーション要求を拒否します。

PDU	番号	タイプ	説明
ALTER_CONTEXT	14	アソシエーション	別のインターフェイスまたはバージョンについて追加のプレゼンテーションのネゴシエーションを要求するか、新しいセキュリティ コンテキストをネゴシエートするか、またはその両方を行います。
ALTER_CONTEXT_RESP	15	アソシエーション	ALTER_CONTEXT PDU に応答します。 有効な値は accept または deny です。
SHUTDOWN	17	コール	クライアントに接続の終了を要求し、関連するリソースを解放します。
CO_CANCEL	18	コール	接続をキャンセルするか、孤立させます。 このメッセージは、クライアントがキャンセルのエラーを検出した場合に送信されます。
ORPHANED	19	コール	進行中の要求、およびまだ完全に送信されていない要求を中断するか、進行中の（多くの場合時間のかかる）応答を中断します。

NAT での MSRPC ALG

NAT では、MSRPC パケットを受信すると、パケット ペイロードを解析し、埋め込み IP アドレスを変換するためのトークンを作成する MSRPC ALG を呼び出します。 このトークンは NAT に渡され、ユーザの NAT 設定に従ってアドレスまたはポートを変換します。 変換後のアドレスは、MSRPC ALG によってパケット ペイロードに再び書き込まれます。

ファイアウォールと NAT の両方を設定している場合、NAT は ALG を最初に呼び出します。

MSRPC ステートフル パーサー

MSRPC ステート マシンまたはパーサーは、MSRPC ALG の中枢です。 MSRPC ステートフル パーサーは、すべてのステートフル情報を、いずれの機能が最初にパーサーを起動したかに応じて、ファイアウォールまたは NAT 内に保持します。 パーサーは、MSRPC プロトコル パケットの DPI を提供します。 これは、プロトコルへの準拠を確認し、シーケンス外コマンドや不正パケットを

検出します。 ステート マシンでは、パケットの解析時に、さまざまなデータを記録し、NAT およびファイアウォール インスペクション用に正しいトークン情報を入力します。

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

（注） デフォルトでは、NAT をイネーブルにすると、MSRPC ALG は自動的にイネーブルになります。 NAT のみの設定では MSRPC 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 MSRPC 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。

レイヤ 4 MSRPC クラス マップおよびポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **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	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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。

	コマンドまたはアクション	目的
ステップ 3	**class-map type inspect match-any** *class-map-name* 例： `Router(config)# class-map type inspect match-any msrpc-cmap`	トラフィック クラスの検査タイプ クラス マップを作成し、QoS 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 protocol** *protocol-name* 例： `Router(config-cmap)# match protocol msrpc`	指定されたプロトコルを基づくクラス マップの一致基準を設定します。 • 検査タイプ クラス マップでは Cisco IOS XE ステートフル パケット インスペクションがサポートするプロトコルのみを一致基準として使用できます。
ステップ 5	**exit** 例： `Router(config-cmap)# exit`	QoS 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。
ステップ 6	**policy-map type inspect** *policy-map-name* 例： `Router(config)# policy-map type inspect msrpc-pmap`	レイヤ 3 またはレイヤ 4 の検査タイプ ポリシー マップを作成し、QoS 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 7	**class type inspect** *class-map-name* 例： `Router(config-pmap)# class type inspect msrpc-class-map`	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、QoS 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 8	**inspect** 例： `Router(config-pmap-c)# inspect`	Cisco IOS XE 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 9	**end** 例： `Router(config-pmap-c)# end`	QoS 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、特権 EXEC モードを開始します。

ゾーン ペアの設定および MSRPC ポリシー マップの付加

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *security-zone-name*
4. **exit**
5. **zone security** *security-zone-name*
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** [*destination-zone*]]
8. **service-policy type inspect** *policy-map-name*
9. **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	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Rotuer# 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	**zone security** *security-zone-name* 例： `Router(config)# zone security in-zone`	インターフェイスを割り当てることができるセキュリティ 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 モードを開始します。
ステップ 5	**zone security** *security-zone-name* 例： `Router(config)# zone security out-zone`	インターフェイスを割り当てることができるセキュリティ 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。

	コマンドまたはアクション	目的
ステップ 6	**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 モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** [*destination-zone*]] 例： `Router(config)# zone-pair security in-out source in-zone destination out-zone`	ゾーン ペアを作成し、セキュリティ 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。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Router(config-sec-zone-pair)# service-policy type inspect msrpc-pmap`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**end** 例： `Router(config-sec-zone-pair)# end`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

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

例：レイヤ 4 MSRPC クラス マップおよびポリシー マップの設定

```
Router# configure terminal
Router(config)# class-map type inspect match-any msrpc-cmap
Router(config-cmap)# match protocol msrpc
Router(config-cmap)# exit
Router(config)# policy-map type inspect msrpc-pmap
Router(config-pmap)# class type inspect msrpc-cmap
Router(config-pmap-c)# inspect
Router(config-pmap-c)# end
```

例：ゾーン ペアの設定および MSRPC ポリシー マップの付加

```
Router# configure terminal
Router(config)# zone security in-zone
Router(config-sec-zone)# exit
Router(config)# zone security out-zone
Router(config-sec-zone)# exit
Router(config)# zone-pair security in-out source in-zone destination out-zone
Router(config-sec-zone-pair)# service-policy type inspect msrpc-pmap
Router(config-sec-zone-pair)# end
```

ファイアウォールおよび NAT 対応の MSRPC ALG サポートに関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
NAT コマンド	『Cisco IOS IP Addressing Services Command Reference』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
NAT ALG	「Using Application-Level Gateways with NAT」モジュール
ALG サポート	『*NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするため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 MSRPC ALG サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 2：ファイアウォールおよび *NAT* 対応の *MSRPC 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 MSRPC ALG サポート	Cisco IOS XE Release 3.5S	ファイアウォールおよび NAT 対応の MSRPC ALG サポート機能は、ファイアウォールおよび NAT における MSRPC ALG のサポートを提供します。MSRPC ALG は、MSRPC 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。MSRPC ALG は、ネットワーク管理者に、MSRPC パケットで検索可能な一致基準を定義するための一致フィルタの設定を許可するプロビジョニング システムと連携します。 コマンド **ip nat service msrpc**、**match protocol msrpc** が導入または変更されました。