ファイアウォールと NAT に対する MSRPC ALG サポート

ファイアウォールおよび NAT 対応の MSRPC ALG サポート機能により、ファイアウォールにおける 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、およびネットワーク アドレス変換（NAT）のサポートが提供されます。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）を実行します。MSRPC ALG はプロビジョニング システムと連動して、ネットワーク管理者が MSRPC パケットで検索可能な一致基準を定義するマッチング フィルタを設定できるようにします。

MSRPC ALG はさらに、Virtual Transport Control Protocol（vTCP）機能もサポートします。vTCP 機能は、TCP セグメンテーションを適切に処理し、Cisco IOS Zone-Based ファイアウォール、ネットワーク アドレス変換（NAT）、およびその他のアプリケーションでセグメントを解析するための各種 ALG プロトコルに対応するフレームワークを提供します。

- ファイアウォールと NAT に対する MSRPC ALG サポートに関する前提条件 （1 ページ）
- ファイアウォールと NAT に対する MSRPC ALG サポートに関する制約事項 （2 ページ）
- ファイアウォールと NAT に対する MSRPC ALG サポートに関する情報 （2 ページ）
- ファイアウォールと NAT に対する MSRPC ALG サポートの設定方法 （5 ページ）
- ファイアウォールと NAT に対する MSRPC ALG サポートの設定例 （10 ページ）
- ファイアウォールと NAT に対する MSRPC ALG サポートに関する機能情報 （11 ページ）

ファイアウォールと NAT に対する MSRPC ALG サポートに関する前提条件

- パケットに 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）を適用する前に、Cisco IOS XE ファイアウォールとネットワーク アドレス変換（NAT）を有効にする必要があります。

（注） トラフィックが Cisco IOS XE ファイアウォールと NAT のどちらかまたはその両方によって TCP ポート 135 に送信される場合は、MSRPC ALG が自動的に有効になります。

ファイアウォールと NAT に対する MSRPC ALG サポートに関する制約事項

- TCP ベースの MSRPC のみがサポートされます。
- **allow** コマンドと **reset** コマンドを同時に設定することはできません。
- DPI のために **match protocol msrpc** コマンドを設定する必要があります。
- 宛先ポート 135 に到達したトラフィックのみがサポートされます。この設定はコンフィギュレーションで変更できます。

ファイアウォールと NAT に対する MSRPC ALG サポートに関する情報

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 レイヤ 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 レイヤ 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 の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバ アプリケーションと通信できるようにします。
- アプリケーション固有のコマンドを認識し、これらのコマンドに対するきめ細かいセキュリティ制御を提供します。
- データ交換を行う 2 つのホスト間の複数のデータ ストリームまたはデータ セッションを同期します。
- アプリケーション ペイロードで使用できる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、アプリケーション レイヤ データストリームの送信元 IP アドレスおよび宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換

サービスをNATが実行します。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とは、開発者が一連のアプリケーションとサービスをサーバおよび企業にパブリッシュするために使用するフレームワークのことです。RPCはプロセス間通信技術であり、クライアントとサーバ ソフトウェアがネットワーク経由で通信することを可能にします。MSRPC はアプリケーション層プロトコルで、多岐にわたる Microsoft アプリケーションで使用されています。MSRPCは、多種多様なトランスポートプロトコルでコネクション型（CO）およびコネクションレス型（CL）の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ています。MSRPC のすべてのサービスは、プライマリ接続と呼ばれる初期セッションを確立します。MSRPC の一部のサービスは、1024 ～ 65535 のポート範囲を宛先ポートとするセカンダリ セッションを確立します。

ファイアウォールと NAT が有効にされる時点で MSRPC を機能させるには、MSRPC パケットのインスペクションに加え、ALG がダイナミック 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の 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ことで、ほとんどのMSRPCサービスがサポートされ、レイヤ 7 ポリシー フィルタの必要がなくなります。

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 が MSRPC メッセージの解析を開始します。次の表に、ファイアウォールおよびNAT機能のMSRPC ALGでサポートされるプロトコル データ ユニット（PDU）のタイプを記載します。

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やバージョンの追加プレゼンテーション ネゴシエーションを要求するか、新しいセキュリティ コンテキストのネゴシエーションを要求するか、あるいはその両方を要求します。
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	接続を終了して関連するリソースを解放するようクライアントに要求します。
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、クライアントでキャンセル失敗が発生すると送信されます。
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止するか、進行中の（おそらく長い）応答を中断します。

NAT での MSRPC ALG

NAT は MSRPC パケットを受信すると MSRPC ALG を呼び出し、MSRPC ALG によってパケットのペイロードが解析されて、組み込み IP アドレスを変換するためのトークンが形成されます。このトークンが NAT に渡されて、NAT 設定に応じてアドレスまたはポートに変換されます。変換後のアドレスは、MSRPC ALG によってパケットのペイロードに書き込まれます。

ファイアウォールと NAT の両方が設定されている場合、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 の中枢部です。MSRPC ステートフル パーサーにより、ファイアウォールまたは NAT（どちらの機能がパーサーを最初に呼び出したかによります）内のすべてのステートフル情報が保持されます。パーサーは、MSRPC プロトコル パケットの DPI を実行します。つまり、プロトコルへの準拠性をチェックし、順序が正しくないコマンドや形式の誤ったパケットを検出します。パケットが解析されると、ステート マシンが各種のデータを記録して、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取り込みます。

ファイアウォールと NAT に対する MSRPC ALG サポートの設定方法

（注） NAT が有効になっている場合は、デフォルトで、MSRPC ALG が自動的に有効になります。NAT のみの設定では MSRPC ALG を明示的に有効にする必要はありません。NAT 上で MSRPC ALG を無効にするには、**no ip nat service msrpc** コマンドを使用できます。

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 モードを有効にします。 • 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。
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。

	コマンドまたはアクション	目的
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だけ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`	アクションの実行対象となるトラフィック（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 マップのアタッチ

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 モードを有効にします。 • 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。
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。

	コマンドまたはアクション	目的
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 モードを終了して、特権 EXEC モードを開始します。

MSRPC ALG の vTCP サポートの有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **alg vtcp service msrpc**
4. **exit**
5. **set platform hardware qfp active feature alg msrpc tolerance on**

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 モードを有効にします。 • 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。
ステップ 3	**alg vtcp service msrpc** 例： `Rotuer(config)# alg vtcp service msrpc`	MSRPC ALG の vTCP 機能を有効にします。 （注） デフォルトで、MSRPC ALG は vTCP をサポートします。
ステップ 4	**exit** 例： `Rotuer(config)# exit`	グローバル 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。

	コマンドまたはアクション	目的
ステップ 5	**set platform hardware qfp active feature alg msrpc tolerance on** 例： `Rotuer# set platform hardware qfp active feature alg msrpc tolerance on`	MSRPC 不明メッセージの許容を有効にします。 （注） デフォルトでは、許容はオフになっています。

MSRPC ALG の vTCP サポートの無効化

手順の概要

1. **enable**
2. **configure terminal**
3. **no alg vtcp service msrpc**
4. **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 モードを有効にします。 • 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。
ステップ 3	**no alg vtcp service msrpc** 例： `Rotuer(config)# no alg vtcp service msrpc`	MSRPC ALG の vTCP 機能を無効にします。
ステップ 4	**end** 例： `Rotuer(config)# end`	グローバル 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。

ファイアウォールと NAT に対する MSRPC ALG サポートの設定例

例：レイヤ 4 MSRPC クラス マップとポリシー 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 ペアの設定と MSRPC ポリシー マップのアタッチ

```
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
```

例：MSRPC ALG に対する vTCP サポートの有効化

```
Router# configure terminal
Router(config)# alg vtcp service msrpc
Router(config)# end
```

例：MSRPC ALG に対する vTCP サポートの無効化

```
Router# configure terminal
Router(config)# no alg vtcp service msrpc
Router(config)# end
```

ファイアウォールと NAT に対する MSRPC ALG サポートに関する機能情報

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 :* ファイアウォールと *NAT* に対する *MSRPC ALG* サポートに関する機能情報

機能名	リリース	機能情報
ファイアウォールと NAT に対する MSRPC ALG サポート	Cisco IOS XE リリース 3.5S	ファイアウォールと NAT に対する MSRPC ALG サポート機能は、ファイアウォールと 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、プロビジョニング システムと連動して、ネットワーク管理者が MSRPC パケットで検索可能な一致基準を定義する一致フィルタを設定できるようにします。 次のコマンドが導入または変更されました。**ip nat service msrpc**、**match protocol msrpc**。

機能名	リリース	機能情報
ゾーンベース ファイアウォールと NAT に対する MSRPC ALG インスペクション強化	Cisco IOS XE リリース 3.14S	ゾーンベース ファイアウォールと NAT に対する MSRPC ALG インスペクション強化機能は、Cisco ファイアウォール、ネットワーク アドレス変換（NAT）、およびその他のアプリケーションで、さまざまなALGプロトコルが適切にTCP セグメンテーションを処理しセグメントを解析するためのフレームワークを提供する Virtual Transport Control Protocol（vTCP）機能をサポートします。 次のコマンドが導入されました：**alg vtcp service msrpc**

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。