NAT でのアプリケーション レベル ゲートウェイの使用

このモジュールでは、Network Address Translation（NAT; ネットワーク アドレス変換）で使用される Application Level Gateway（ALG; アプリケーション レベル ゲートウェイ）を設定するための基本的な作業について説明します。また、IP ヘッダー変換に ALG を使用するプロトコルについてもこのモジュールで説明します。

NAT は、アプリケーション 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/UDP トラフィックにおいて変換サービスを実行します。このようなプロトコルには、HTTP、TFTP、telnet、archie、finger、Network Time Protocol（NTP; ネットワーク タイム プロトコル）、Network File System（NFS; ネットワーク ファイル システム）、Remote Login（rlogin; リモート ログイン）、Remote Shell（RSH; リモート シェル）プロトコル、および Remote Copy（RCP; リモート コピー）があります。ペイロードに IP アドレス情報を埋め込むプロトコルは、ALG のサポートを必要とします。

ALG を伴う NAT は、H.323 を使用していないアプリケーションがポート 1720 を使用している限り、このアプリケーションからのパケットを変換します。

NAT を通じた IPsec ESP 機能のサポートにより、オーバーロード モード、または Port Address Translation（PAT; ポート アドレス変換）モードで設定された Cisco IOS NAT デバイス経由で、複数の同時 IPsec Encapsulating Security Payload（ESP）トンネルまたは接続をサポートできるようになります。

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、「NAT でアプリケーション レベル ゲートウェイを使用する場合の機能情報」（P.15）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

NAT でアプリケーション レベル ゲートウェイを使用するための要件

- このモジュールの作業を実行する前に、「Configuring NAT for IP Address Conservation」モジュールで説明されている概念をよく理解しておく必要があります。
- このモジュールの作業で使用する必要のあるアクセス リストはすべて、設定作業を開始する前に設定しておく必要があります。アクセス リストの設定方法については、次の URL にある『*IP Access List Sequence Numbering*』マニュアルを参照してください。

  http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_ip_entry_numbrng.html
- このモジュールの作業を実行する前に、Session Initiation Protocol（SIP; セッション開始プロトコル）および H.323 がディセーブルにされていないことを確認する必要があります。SIP および H.323 はデフォルトでイネーブルです。

NAT でのアプリケーション レベル ゲートウェイの使用について

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 ゲートウェイは、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。

NAT でのアプリケーション レベル ゲートウェイの設定方法

ここでは、次の手順について説明します。

NAT を通じた IPsec の設定

NAT とともにアプリケーション レベル ゲートウェイを設定するには、次の概念について理解する必要があります。

ここでは、NAT を通じた IPsec の設定に関連する次の作業について説明します。

NAT ALG 設定の利点

- SIP の NAT サポートによって、SIP ベースの VoIP ソリューション間に Cisco IOS NAT を導入できるようになりました。
- お客様は自分の IP アドレス方式を制御し、H.323 v2 ゲートキーパー設定のサポートをすべて取り込むことができます。
- NAT により、お客様は自分のネットワークにプライベート IP アドレスを導入し、インターネットへの接続、または別の企業ネットワークとの内部接続を行うときに、パブリック IP アドレスに変換することができるようになります。
- 通常、変換テーブルの ESP エントリの送信は、宛先から応答が届くまで、延期されます。予想可能な Security Parameter Index（SPI; セキュリティ パラメータ インデックス）と SPI マッチングにより、SPI エントリが照合されるため、この延期を回避することができます。一部サードパーティのコンセントレータでは、送信元ポートと受信ポートの両方でポート 500 を使用する必要があります。**ip nat service** コマンドで **preserve-port** キーワードを使用することにより、ポートを変更するのではなく、標準 NAT で必要とされるポートを保持することができます。

IP セキュリティ

IPsec は、オープン標準のフレームワークに含まれる IP プロトコル ファミリへの拡張セットで、インターネット上でプライベートな会話をセキュアに行えるようにするためにあります。IETF により開発された標準に基づいて、IPsec はパブリック ネットワーク上でのデータ通信の機密性、整合性、および信頼性を保証し、暗号化によるセキュリティ サービスを提供します。

2 台のルータなど、2 つのピアの間にセキュリティ トンネルが提供され、どのパケットの機密性が高く、これらのセキュアなトンネル経由で送信されるべきと見なされるか、また、これらのトンネルの特徴を指定して、このような機密性の高いパケットを保護するにはどのパラメータを使用すべきかが判断されます。IPsec ピアは機密性の高いパケットを受信すると、適切でセキュアなトンネルを設定し、このトンネルを通じてパケットをリモート ピアに送信します。

ESP を使用する IPsec は、Network Address Port Translation（NAPT）、またはアドレス オーバーロードが設定されていない限り、特別なサポートなしに、NAT を実行しているルータを通過することができます。

複数のプライベート内部 IP アドレスを 1 つのパブリック外部 IP アドレスとして表した NAPT デバイスを通過する IPsec VPN 接続を行うときに、考慮しなければならない要因がいくつかあります。このような要因には、VPN サーバおよびクライアントの能力、NAPT デバイスの能力、NAPT デバイス上で同時に複数の接続が行われているかどうかが含まれます。

ルータに NAPT を使用する IPsec を設定する方法には、次の 2 通りがあります。

- TCP や UDP のようなレイヤ 4 プロトコルに IPsec をカプセル化する。この場合、IPsec は NAT を*忍び出る*ことができます。NAT デバイスはカプセル化に気づきません。
- IPsec 固有のサポートを NAPT に追加します。この場合、IPsec は、NAT を*忍び出る*のとは逆の働きをします。IPSec ESP の NAT サポート：フェーズ II 機能は、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）および ESP をサポートします。NAPT で設定された Cisco IOS ルータを通じたトンネル モードでカプセル化する必要は必要ありません。

NAPT デバイスを通過する IPsec セッションを実行するときに使用するプロトコルには、TCP と UDP が推奨されますが、すべての VPN サーバやクライアントが TCP または UDP をサポートしているわけではありません。

SPI マッチング

Security Parameter Index（SPI; セキュリティ パラメータ インデックス）マッチングは、複数の宛先ペアの間に VPN 接続を確立するために使用されます。NAT エントリはただちに設定済みのアクセス リストとマッチするエンドポイントの変換テーブルに配置されます。SPI マッチングは、Cisco IOS Release 12.2(15)T に実装されている予測アルゴリズムに従って SPI を選択するエンドポイントでのみ使用できます。

IP ネットワークを経由する音声およびマルチメディア

SIP は、IETF Multiparty Multimedia Session Control（MMUSIC）Working Group により開発されたプロトコルです。Cisco SIP 機能は Cisco ルータが IP ネットワーク経由した音声通話およびマルチメディア通話のセットアップを通知できるようにします。SIP は、VoIP インターネットワーキング ソフトウェアの H.323 に代わるものです。

Session Description Protocol（SDP; セッション記述プロトコル）は、マルチメディア セッションを記述するためのプロトコルです。SDP は、SIP メッセージの本文で、複数のユーザが参加するマルチメディア セッションの作成および制御のために使用されるマルチメディア セッションを記述するために使用できます。

SIP に対する NAT サポート機能により、NAT を使って設定されたルータを通過する SIP 埋め込みメッセージは、変換後、パケットに暗号化されます。SIP または SDP メッセージの変換には、NAT とともに ALG が使用されます。

（注） デフォルトでは、SIP のサポートはポート 5060 でイネーブルになっています。したがって、NAT 対応デバイスはこのポートのパケットをすべて、SIP コール メッセージと解釈します。同じシステムにある別のアプリケーションがポート 5060 を使用してパケットを送信している場合、NAT サービスはこのパケットを SIP コール メッセージとして解釈しようとするため、このパケットが破損する可能性があります。

H.323 v2 RAS に対する NAT サポート

Cisco IOS NAT は、Registration, Admission, and Status（RAS）プロトコルで送信されたものを含め、H.225 および H.245 メッセージ タイプをすべてサポートしています。RAS は、ソフトウェア クライアントや VoIP デバイスにより、場所の登録、通話のセットアップ サポートの要求、および帯域幅の制御に使用される多数のメッセージを提供します。RAS メッセージは、H.323 ゲートキーパーに向けて送信されます。

一部の RAS メッセージには、ペイロードに IP アドレス情報が含まれていますが、これは通常、ゲートキーパーへのユーザの登録、または別の登録済みユーザに関する情報の取得を意図したものです。このようなメッセージが NAT に認識されない場合、誰にでも確認できる IP アドレスには変換されません。

Cisco IOS Release 12.2(2)T 以降のリリースでは、埋め込み IP アドレスがアドレス変換される可能性があるかどうかを検査できるようになりました。Cisco IOS Release 12.2(2)T 以前では、NAT で H.323 v2 RAS メッセージはサポートされていませんでした。

v2 互換モードでの H.323 v3 および v4 に対する NAT サポート

H.323 は、パケット ネットワーク経由でのオーディオ、ビデオ、およびデータ送信に関する ITU-T 仕様です。NAT は、4 バージョンの H.323 プロトコル、v1、v2、v3、および v4 をサポートします。v2 互換モードでの H.323 v3 および v4 に対する NAT サポート機能により、Cisco NAT ルータは H.323 v3 および v4 でコーディングされたメッセージに H.323 v2 互換のフィールドが含まれている場合に、これらのメッセージをサポートできるようになります。この機能により、アドレス変換を必要とする新しいメッセージ タイプや新しいフィールドなど、v3 および v4 で導入された H.323 機能のサポートが追加されるわけではありません。

NAT H.245 トンネリングのサポート

NAT H.245 トンネリングにより、H.323 ALG で H.245 トンネリングができるようになります。NAT H.245 トンネリングは、メディア チャネル セットアップを作成するために必要な H.245 トンネル メッセージをサポートするためのメカニズムを提供します。

H.323 コールを行うには、TCP ポート 1720 で H.225 接続を開く必要があります。H.225 接続が開かれると、H.245 セッションが開始され、確立されます。この接続は H.225 とは異なるチャネルで行うことができます。また、H.245 メッセージを H.225 メッセージに埋め込み、以前に確立された H.225 チャネルに送信することにより、同じ H.225 チャンネル上で H.245 トンネリングを使用して行うこともできます。

H.245 トンネリングされたメッセージが認識されない場合、メディア アドレスまたはポートは Cisco IOS NAT によって変換されずに残され、この結果、メディア トラフィックでエラーが発生します。H.245 FastConnect プロシージャは、H.245 トンネリングされたメッセージが送信されると同時に終了するので役に立ちません。

制約事項

NAT により変換されるのは、埋め込み IP バージョン 4 アドレスのみです。

NAT を通じた IPsec ESP の設定

NAT を通じた IPsec ESP により、オーバーロード モード、または PAT モードで設定された Cisco IOS NAT デバイス経由で、複数の同時 ESP トンネルまたは接続をサポートできるようになります。

NAT を通じた IPsec ESP を設定するには、次の作業を実行します。

（注） IPsec はスタティック NAT 設定のみならず、どのような NAT 設定についても設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat** [**inside** | **outside**] **source static** *local-ip global-ip* [**vrf** *vrf-name*]
4. **exit**
5. **show ip nat translations**

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	**ip nat** [**inside** | **outside**] **source static** *local-ip global-ip* [**vrf** *vrf-name*] **例：** `Router(config)# ip nat inside source static 10.10.10.10 192.168.30.30`	スタティック NAT をイネーブルにします。
ステップ 4	**exit** **例：** `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**show ip nat translations** **例：** `Router# show ip nat translations`	（任意）アクティブな NAT を表示します。

保持ポートのイネーブル化

この作業は、送信元ポートにポート 500 を使用している IPsec トラフィックに対して使用します。送信元ポートとしてポート 500 を保持できるようにするには、このタスクを実行します。

制約事項

これは、ある特定の VPN コンセントレータで必要とされる作業です。Cisco VPN デバイスでは、通常、この機能は使用されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat service list** *access-list-number* **IKE preserve-port**

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	**ip nat service list** *access-list-number* **IKE preserve-port** **例：** `Router(config)# ip nat service list 10 IKE preserve-port`	ポートを保持するために、アクセス リストと一致する IPsec トラフィックを指定します。

NAT デバイスでの SPI マッチングのイネーブル化

（注） SPI マッチングはデフォルトでディセーブルにされています。

Security Parameter Index（SPI; セキュリティ パラメータ インデックス）マッチングは、複数の宛先ペアの間に VPN 接続を確立するために使用されます。NAT エントリはただちに設定済みのアクセス リストとマッチするエンドポイントの変換テーブルに配置されます。SPI マッチングは、Cisco IOS Release 12.2(15)T に実装されている予測アルゴリズムに従って SPI を選択するエンドポイントでのみ使用できます。

予測可能で対称的な SPI の生成がイネーブル化されます。NAT デバイス全体で複数の ESP 接続が望ましい場合は、NAT デバイスとともに SPI マッチングを使用する必要があります。

前提条件

送信元ルータと、並列処理をイネーブル化するリモート ゲートウェイの両方で、Cisco IOS ソフトウェアを実行する必要があります。

制約事項

SPI マッチングは、NAT デバイス、および両方のエンドポイント デバイスで設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat service list** *access-list-number* **ESP spi-match**

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	**ip nat service list** *access-list-number* **ESP spi-match** **例：** `Router(config)# ip nat service list 10 ESP spi-match`	SPI マッチングをイネーブル化するアクセス リストを指定します。 • 次の例では、デバイスが両方ともシスコ デバイスで、マッチング可能な SPI を提供するように設定されていると仮定して、ESP トラフィック マッチング リスト 10 を NAT テーブルに入力します。

エンドポイントでの SPI マッチングのイネーブル化

この作業は、両方のエンドポイントで SPI マッチングをイネーブルにするために実行します。

前提条件

送信元ルータと、並列処理をイネーブル化するリモート ゲートウェイの両方で、Cisco IOS ソフトウェアを実行する必要があります。

制約事項

SPI マッチングは、NAT デバイス、および両方のエンドポイント デバイスで設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec nat-transparency spi-matching**

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	**crypto ipsec nat-transparency spi-matching** **例：** `Router(config)# crypto ipsec nat-transparency spi-matching`	両方のエンドポイントで SPI マッチングをイネーブル化します。

NAT に対する MultiPart SDP サポートのイネーブル化

NAT に対する MultiPart SDP サポート機能は、NAT の拡張ポートフォリオに対する SIP ALG で MultiPart SDP のサポートを提供します。NAT に対する MultiPart SDP サポートはデフォルトでディセーブルです。

NAT に対する MultiPart SDP サポートをイネーブルにするには、次のタスクを実行します。

制約事項

NAT により変換されるのは、埋め込み IP バージョン 4 アドレスのみです。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat service allow-multipart**
4. **exit**
5. **show ip nat translations**

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	**ip nat service allow-multipart** **例：** `Router(config)# ip nat service allow-multipart`	Multipart SDP をイネーブルにします。
ステップ 4	**exit** **例：** `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**show ip nat translations** **例：** `Router# show ip nat translations`	（任意）アクティブな NAT を表示します。

IP Phone と Cisco CallManager の間での NAT の設定

ここでは、Cisco IP Phone における Cisco CallManager 通信のための Cisco Skinny Client Control Protocol（SCCP）の設定について説明します。このセクションで説明する作業では、IP Phone と Cisco CallManager の間に NAT を設定します。

Skinny Client Control Protocol に対する NAT サポート

Cisco IP Phone は、Cisco CallManager との接続、および登録に SCCP を使用します。

スケーラブルな環境で、IP Phone と Cisco CallManager の間に Cisco IOS NAT を設定できるようにするには、NAT は SCCP を検出し、メッセージで渡される情報を理解できなければなりません。電話での通話が可能な他の IP Phone ユーザの識別に使用される IP アドレスやポート情報を含むメッセージは両方向に行き来します。

Cisco CallManager 通信を行う SCCP クライアントは通常、内部から外部へ向かって進みます。Cisco CallManager が内部（NAT デバイスの背後）にある場合、Cisco CallManager IP アドレス接続を解決するには、Domain Name System（DNS; ドメイン ネーム システム）を使用する必要があります。それ以外の場合は、内部にある Cisco CallManager にアクセスするようにスタティック NAT を設定する必要があります。

Cisco CallManager への接続を試みた IP Phone が設定済み NAT 規則と一致する場合、NAT はもともとの送信元 IP アドレスを変換して、設定済みプールにある IP アドレスで置き換えます。この新しいアドレスは Cisco CallManager に反映され、他の IP Phone ユーザから確認できるようになります。

SCCP フラグメンテーションの NAT サポート

スキニー制御メッセージは TCP 上でやりとりされます。IP Phone、または Cisco CallManager のいずれかの TCP Maximum Segment Size（MSS; 最大セグメント サイズ）がスキニー制御メッセージのペイロードを下回るように設定されている場合、スキニー制御メッセージは、複数の TCP セグメントに分割されます。この機能以前、スキニー制御メッセージのやりとりは、NAT スキニー ALG はスキニー制御メッセージを組み立てなおすことができなかったため、TCP セグメンテーション シナリオでエラーとなっていました。NAT SCCP フラグメンテーション サポートは、NAT スキニー ALG の TCP セグメントに対するサポートを追加する機能です。IP やポートの変換を必要とする、分割されたペイロードはドロップされなくなります。

また、スキニー制御メッセージを IP 分割することもできますが、このようなメッセージのサポートには、Virtual Fragmentation Reassembly（VFR）が使用されます。

Cisco IOS Release 15.1(3)T またはそれ以降のリリースでは、NAT はバージョン 17 以降の SCCP 電話で機能します。

レイヤ 4 フォワーディングを使った NAT セグメンテーション

レイヤ 4 フォワーディングを使った NAT セグメンテーションは、H.323、SCCP、および TCP DNS プロトコル用に実装された機能です。NAT は、複数のパケットに分割された H.323、SCCP、または TCP DNS メッセージの処理をサポートします。

レイヤ 4 フォワーディング、または TCP プロキシは、シーケンス番号の並べ替え、パケット内の番号の確認、MSS を超える変換後パケットの再分割、パケット損失の場合の再送信などのセッションを処理します。また、レイヤ 4 フォワーディングは順番に並んでいないパケットの処理も行います。このようなパケットはバッファされます。ドロップされることはありません。

レイヤ 4 フォワーディングは受信したパケットをバッファし、順番に並んだパケットが使用できるようになったときに、NAT ALG に知らせます。また、受信したパケットについて、エンド ホストに確認応答を送信します。レイヤ 4 フォワーディングは NAT ALG から受信した変換後パケットを、出力パケット パスへ送信する作業も行います。

制約事項

レイヤ 4 フォワーディングを使った NAT セグメンテーションは、次の場合には機能しません。

- **ip inspect name** コマンドを使用するように Cisco IOS ファイアウォールが設定されている （ゾーンベースのファイアウォールがサポートされています）。
- H.323、SCCP、または TCP DNS メッセージのサイズが 18 KB を超える。
- Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）が設定されている。
- NAT と Cisco CallManager が同一のデバイス上に設定されている。この場合、Call Manager Express（CME）のコロケーション ソリューションが使用されます。
- NAT Virtual Interface（NVI; NAT 仮想インターフェイス）が設定されている。
- Stateful Network Address Translation（SNAT; ステートフル ネットワーク アドレス変換）がイネーブル化されている。
- パケット変換のため、**match-in-vrf** キーワードが **ip nat inside source** コマンドとともに設定されている。
- パケットが IPv6 パケットである。

手順の概要

1. **enable**

2. **configure terminal**
3. **ip nat service skinny tcp port** *number*

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	**ip nat service skinny tcp port** *number* **例：** `Router(config)# ip nat service skinny tcp port 20002`	指定された TCP ポートにスキニー プロトコルを設定します。

NAT でアプリケーション レベル ゲートウェイを使用する場合の設定例

ここでは、次の設定例について説明します。

- 「例：NAT を通じた IPsec ESP の設定」（P.12）
- 「例：保持ポートのイネーブル化」（P.13）
- 「例：SPI マッチングのイネーブル化」（P.13）
- 「例：エンドポイント ルータにおける SPI マッチングの設定」（P.13）
- 「例：NAT に対する MultiPart SDP サポートのイネーブル化」（P.13）
- 「例：IP Phone と Cisco CallManager の間での NAT の設定」（P.13）

例：NAT を通じた IPsec ESP の設定

次に、vrf1 および vrf2 VPN について、共有サービスへのスタティック ルートを持つ Provider Edge（PE; プロバイダー エッジ）ルータで設定された NAT の例を示します。NAT は、内部送信元スタティック 1 対 1 変換として設定されます。

```
ip nat pool outside 192.0.2.1 192.0.2.14 netmask 255.255.255.0
ip nat outside source list 1 pool mypool
access-list 1 permit 192.0.2.3 0.0.0.255
ip nat inside source static 192.0.2.23 192.0.2.22 vrf vrf1
ip nat inside source static 192.0.2.21 192.0.2.2 vrf vrf2
```

例：保持ポートのイネーブル化

次の例では、サードパーティ コンセントレータの TCP ポート 500 の設定方法を示します。アクセス リスト 10 が設定されています。

```
ip nat service list 10 IKE preserve-port
access-list 10 permit 10.1.1.1
```

例：SPI マッチングのイネーブル化

次の例に、SPI マッチングをイネーブルにする方法を示します。アクセス リスト 10 が設定されています。

```
ip nat service list 10 ESP spi-match
access-list 10 permit 10.1.1.1
```

例：エンドポイント ルータにおける SPI マッチングの設定

次の例に、エンドポイント ルータで SPI マッチングをイネーブルにする方法を示します。

```
crypto ipsec nat-transparency spi-matching
```

例：NAT に対する MultiPart SDP サポートのイネーブル化

ここでは、NAT に対する Multipart SDP サポートをイネーブルにする例を示します。

```
ip nat service allow-multipart
```

例：IP Phone と Cisco CallManager の間での NAT の設定

ここでは、Cisco CallManager を 20002 ポートに設定する例を示します。

```
ip nat service skinny tcp port 20002
```

次の作業

- NAT の概要、および IP アドレス通信向けに NAT を設定する方法については、「Configuring NAT for IP Address Conservation」モジュールを参照してください。
- NAT の検証、モニタリング、およびメンテナンスについては、「Monitoring and Maintaining NAT」モジュールを参照してください。
- NAT と MPLS VPN の統合については、「Integrating NAT with MPLS VPNs」モジュールを参照してください。
- ハイ アベイラビリティを得るための NAT の設定については、「Configuring NAT for High Availability」モジュールを参照してください。

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*』
NAT コマンド：コマンド構文の詳細、コマンド モード、デフォルト、使用上の注意事項、および例	『*Cisco IOS IP Addressing Services Command Reference*』
IP アクセス リストへのシーケンス番号づけ	『*IP Access List Sequence Numbering*』マニュアル

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS 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

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

NAT でアプリケーション レベル ゲートウェイを使用する場合の機能情報

表 1 に、この機能のリリース履歴を示します。

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

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　NAT でアプリケーション レベル ゲートウェイを使用する場合の機能情報

機能名	リリース	機能の設定情報
NAT に対する MultiPart SDP サポート	15.0(1)M	NAT に対する MultiPart SDP サポート機能は、NAT の拡張ポートフォリオに対する SIP ALG に MultiPart SDP のサポートを追加します。この機能は、デフォルトではディセーブルに設定されています。 次のセクションで、この機能に関する情報を参照できます。 • 「NAT に対する MultiPart SDP サポートのイネーブル化」（P.9） この機能により、コマンド **debug ip nat**、**ip nat service** が変更されました。
NAT H.245 トンネリングのサポート	12.3(11)T	NAT H.245 トンネリングのサポート機能により、H.323 Application Level Gateway（ALG; アプリケーション レベル ゲートウェイ）で H.245 トンネリングが可能になります。 次のセクションで、この機能に関する情報を参照できます。 • 「NAT H.245 トンネリングのサポート」（P.5）

表 1　NAT でアプリケーション レベル ゲートウェイを使用する場合の機能情報 （続き）

機能名	リリース	機能の設定情報
NAT SCCP フラグメンテーションのサポート	12.4(6)T 15.1(3)T	NAT SCCP フラグメンテーション サポートは、NAT スキニー ALG の TCP セグメントに対するサポートを追加する機能です。IP やポートの変換を必要とする、分割されたペイロードはドロップされなくなります。 Cisco IOS Release 15.1(3)T では、レイヤ 4 フォワーディングを使った NAT セグメンテーション機能が導入されました。 次のセクションで、この機能に関する情報を参照できます。 • 「SCCP フラグメンテーションの NAT サポート」（P.11） • 「レイヤ 4 フォワーディングを使った NAT セグメンテーション」（P.11） この機能により、コマンド **debug ip nat** が変更されました。
H.323 v2 RAS に対する NAT サポート機能	12.2(2)T 15.0(1)S	Cisco IOS NAT は、RAS プロトコルで送信されたものを含め、H.225 および H.245 メッセージ タイプをすべてサポートしています。 次のセクションで、この機能に関する情報を参照できます。 • 「H.323 v2 RAS に対する NAT サポート」（P.5）
v2 互換モードでの H.323 v3 および v4 に対する NAT サポート	12.3(2)T	v2 互換モードでの H.323 v3 および v4 に対する NAT サポート機能により、Cisco NAT ルータは H.323 v3 および v4 でコーディングされたメッセージに H.323 v2 互換のフィールドが含まれている場合に、これらのメッセージをサポートできるようになります。この機能により、アドレス変換を必要とする新しいメッセージ タイプや新しいフィールドなど、v3 および v4 で導入された H.323 機能のサポートが追加されるわけではありません。 次のセクションで、この機能に関する情報を参照できます。 • 「v2 互換モードでの H.323 v3 および v4 に対する NAT サポート」（P.5）
IPsec セキュリティ チェックに対する NAT サポート：フェーズ II	12.2(15)T	IPSec ESP の NAT サポート：フェーズ II 機能は、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）および ESP をサポートします。NAPT で設定された Cisco IOS ルータを通じたトンネル モードでカプセル化する必要は必要ありません。 次のセクションで、この機能に関する情報を参照できます。 • 「NAT を通じた IPsec の設定」（P.3） • 「例：NAT を通じた IPsec ESP の設定」（P.12）
SIP に対する NAT サポート	12.2(8)T	SIP への NAT サポートにより、SIP に基づく VoIP ソリューションの間に Cisco IOS NAT を設定する機能が追加されます。 次のセクションで、この機能に関する情報を参照できます。 • 「NAT を通じた IPsec の設定」（P.3）

表 1　NAT でアプリケーション レベル ゲートウェイを使用する場合の機能情報 （続き）

機能名	リリース	機能の設定情報
H.323 を使用していないアプリケーションに対するサポート	12.2(33)XNC	ALG を伴う NAT は、H.323 を使用していないアプリケーションがポート 1720 を使用している限り、このアプリケーションからのパケットを変換します。
NAT を介した IPsec ESP のサポート	12.2(13)T	NAT を通じた IPsec ESP は、オーバーロード モード、または Port Address Translation（PAT; ポート アドレス変換）モードで設定された Cisco IOS Network Address Translation（NAT; ネットワーク アドレス変換）デバイス経由で、複数の同時 IPsec Encapsulating Security Payload（ESP）トンネルまたは接続をサポートするための機能を提供します。 次のセクションで、この機能に関する情報を参照できます。 • 「NAT を通じた IPsec ESP の設定」（P.5）