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、ネットワーク アドレス変換（NAT）で使用されるアプリケーション レベル ゲートウェイ（ALG）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。 送信元および宛先 IP アドレスを伝送しないプロトコルには、HTTP、TFTP、Telnet、Archie、Finger、ネットワーク タイム プロトコル（NTP）、ネットワーク ファイル システム（NFS）、リモート ログイン（rlogin）、リモート シェル（rsh）プロトコルおよびリモート コピー（rcp）が含まれます。

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。 NAT は、パケット ペイロードでの埋め込み IP アドレスおよびポート番号の変換や、制御チャネルからの新規接続/セッション情報の抽出といった、アプリケーション データ ストリーム（レイヤ 7）プロトコル固有のサービスを処理するためのさまざまな ALG を必要とします。

NAT は、サポートされる ALG を持つプロトコルに対し、仮想ルーティングおよび転送（VRF）をサポートします。

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、またはポート アドレス変換（PAT）モードで設定された 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。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース 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の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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。

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、「IP アドレス節約のための NAT 設定」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 リストの設定方法の詳細については、『IP Access List Sequence Numbering』マニュアルを参照してください。
- このモジュールの作業を実行する前に、Session Initiation Protocol（SIP）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

IPSec

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。

カプセル化セキュリティ ペイロード（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、インターネット キー交換（IKE）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ありません。

NAPT デバイスを経由する IPsec セッションを実行する場合は、TCP および UDP を使用することをお勧めします。 ただし、すべての VPN サーバまたはクライアントで TCP または UDP がサポートされるわけではありません。

SPI マッチング

SPI 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 リストと一致するエンドポイントの変換テーブルに配置されます。

NAT IPsec 設定の利点

- 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、プライベート IP アドレスをパブリック IP アドレスに変換することができるようになります。
- Session Initiation Protocol（SIP）の NAT サポートによって、SIP ベースの VoIP ソリューションに NAT を導入する機能が追加されます。
- お客様は NAT ALG を使用して、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。
- 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。 予想可能なセキュリティ パラメータ インデックス（SPI）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。 これらのポートは、通常の NAT で必要であるように変更するのではなく、**ip nat service preserve-port** コマンドを使用して保持します。

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。

セッション記述プロトコル（SDP）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 よりも前では、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、バージョン 1、バージョン 2、バージョン 3、およびバージョン 4 の 4 つのバージョンの H.323 プロトコルをサポートします。 v2 互換モードでの H.323 v3 および v4 に対する NAT サポート機能を使用すると、H.323 バージョン 3 およびバージョン 4 でコード化されたメッセージに H.323 バージョン 2 と互換性を持つフィールドが含まれている場合に、NAT ルータでこれらのメッセージをサポートできるようになります。 この機能では、アドレス変換を必要とする新しいメッセージ タイプまたは新しいフィールドなどの H.323 バージョン 3 およびバージョン 4 で導入された H.323 機能はサポートされません。

NAT H.245 トンネリングのサポート

NAT H.245 トンネリングのサポート機能では、H.323 ALG で H.245 トンネリングをサポートします。 H.245 トンネリングでは、メディア チャネル設定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しています。

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。 H.323 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 トンネル型メッセージが NAT で理解されない場合、メディア アドレスおよびポート番号は NAT により変換されず、メディア トラフィックが失敗します。 H.245 トンネル型メッセージが NAT によって理解されない場合、H.245 FastConnect プロシージャは役に立ちません。これは、H.245 トンネル型メッセージが送信されるとすぐに、FastConnect が終了するためです。

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、ドメインネームシステム（DNS）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

Skinny Client Control Protocol（SCCP）メッセージ（スキニー制御メッセージとも呼ばれます）は、TCP 経由で交換されます。 IP Phone、または Cisco Unified CallManager のいずれかの TCP 最大セグメント サイズ（MSS）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。 この機能が導入される前は、NAT スキニー ALG でスキニー制御メッセージを再構成できなかったため、TCP セグメンテーション中にスキニー制御メッセージの交換が失敗していました。SCCP フラグメンテーションの NAT サポート機能は、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。これにより、IP 変換やポート変換を必要とする、分割されたペイロードがドロップされなくなります。

また、Virtual Fragmentation Reassembly（VFR）を使用して、スキニー制御メッセージを IP 分割することもできます。

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機能は、H.323、Skinny Client Control Protocol（SCCP）、および TCP ドメイン ネーム システム（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、最大セグメント サイズ（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、ドロップされません。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、NAT ALG から受信した変換後パケットを、出力パケット パスに送信します。

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ファイアウォールが設定されている。（コンテキストベース アクセス コントロール（CBAC）のファイアウォールはサポートされません。ゾーンベースのファイアウォールは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。

- マルチプロトコル ラベル スイッチング（MPLS）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 のコロケーション ソリューションが使用されます。
- NAT 仮想インターフェイス（NVI）が設定されている。
- ステートフル ネットワーク アドレス変換（SNAT）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。

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

NAT を通じた IPsec の設定

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。 • 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	**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。

（注） 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。 • 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	**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。

セキュリティ パラメータ インデックス（SPI）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。

はじめる前に

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。

（注） 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。 • 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	**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。 • この例では、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

はじめる前に

送信元デバイスと、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 ソフトウェアを実行する必要があります。

（注） セキュリティ パラメータ インデックス（SPI）マッチングは、ネットワーク アドレス変換（NAT）デバイスおよび両方のエンドポイント デバイスに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**
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： `Device> 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： `Device# 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： `Device(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。
ステップ 4	**end** 例： `Device(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 モードを開始します。

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 サポート機能により、SIP ALG での MultiPart セッション記述プロトコル（SDP）のサポートが提供されます。 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。

（注） NAT では、埋め込み IPv4 アドレスのみを変換します。

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： `Device> 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： `Device# 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： `Device(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： `Device(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 モードを開始します。
ステップ 5	**show ip nat translations** 例： `Device# 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。

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。 • 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	**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

例：NAT 変換用のポートの指定

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

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：エンドポイントでの SPI マッチングのイネーブル化

```
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

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

例：NAT 変換用のポートの指定

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

次の作業

- NAT の概要、および IP アドレス節約のための NAT 設定については、「IP アドレス節約のための NAT 設定」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、「NAT のモニタリングおよびメンテナンス」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、「MPLS VPN と NAT の統合」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、「ハイ アベイラビリティ用 NAT の設定」モジュールを参照してください。

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：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*』
NAT の IP アドレス節約	『*Configuring NAT for IP Address Conservation*』

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

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

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 *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
ALG - H.323 v6 サポート	Cisco IOS XE Release 3.6S	ALG - H.323 v6 は、H.323 v6 パケットの解析および H.323 メッセージにおける IPv4 アドレス情報のインスペクションおよび変換をサポートします。

機能名	リリース	機能の設定情報
ALG - SCCP バージョン 17 サポート	Cisco IOS XE Release 3.5S	ALG - SCCP バージョン 17 サポート機能により、SCCP ALG で SCCP バージョン 17 パケットを解析できるようになります。 Cisco Unified Communications Manager 7.0 および Cisco Unified Communications Manager 7.0 を使用する IP Phone では、SCCP バージョン 17 メッセージのみをサポートします。 SCCP バージョン 17 パケットは IPv6 パケットをサポートします。 SCCP ALG は SCCP メッセージの IPv4 アドレス情報のインスペクションおよび変換をサポートします。
NAT ALG - SIP REFER 方式	Cisco IOS XE Release 3.2S	NAT ALG - SIP REFER 方式機能は、無人（ブラインド）転送と有人（コンサルタティブ）転送の 2 つのタイプのコール転送をサポートします。
NAT ALG - SIP トランキング サポート	Cisco IOS XE Release 3.2S	NAT ALG - SIP トランキング サポート機能では、ローカル データベースを使用して、SIP トランク内のメディア関連情報をすべて格納します。 各コールのコール ID が、このローカル データベースをインデックス化するために使用されます。
NAT 基本 H.323 ALG サポート	Cisco IOS XE Release 2.1	NAT では、パケット ペイロード内の埋め込み IP アドレスおよびポート番号の変換や、制御チャネルからの新規接続/セッション情報の取得といった、レイヤ 7 プロトコル固有のサービスを処理するために、さまざまな ALG を必要とします。 NAT 基本 H.323 ALG サポート機能は、H.323 メッセージにこれらの固有サービスを提供します。
NAT DNS ALG サポート	Cisco IOS XE Release 2.1	NAT DNS ALG サポート機能では、DNS パケットの変換をサポートします。
NAT FTP ALG サポート	Cisco IOS XE Release 2.1	NAT FTP ALG サポート機能では、FTP パケットの変換をサポートします。

機能名	リリース	機能の設定情報
NAT H.323 RAS	Cisco IOS XE Release 2.4	NAT はすべての H.225 および H. 245 メッセージ タイプ（登録、アドミッション、およびステータス（RAS）プロトコルで送信されるものを含む）をサポートします。 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。
ICMP NAT ALG サポート	Cisco IOS XE Release 2.1	NAT ICMP ALG サポート機能では、ICMP パケットの変換をサポートします。
NAT NetBIOS ALG サポート	Cisco IOS XE Release 3.1S	NAT は、Network Basic Input Output System（NetBIOS）メッセージ変換サポートを提供します。 NAT NetBIOS ALG サポート機能には、デバイスの NetBIOS 固有情報を表示するために、**show platform hardware qfp [active | standby] feature alg statistics netbios** コマンドが導入されました。
NAT NetMeeting Directory（LDAP）	Cisco IOS XE Release 2.4	NAT NetMeeting Directory（LDAP）機能は、NetMeeting Directory LDAP メッセージに ALG サポートを提供します。
NAT RCMD ALG サポート	Cisco IOS XE Release 3.1S	NAT はリモート コマンド実行サービス（RCMD）メッセージの変換サポートを提供します。NAT RCMD ALG サポート機能には、デバイスの RCMD 固有情報を表示するために、**show platform software trace message process qfp active** コマンドが導入されました。
NAT RTSP ALG サポート	Cisco IOS XE Release 3.1S	NAT RTSP ALG サポート機能は、RTSP メッセージ変換サポートを提供します。
ビデオ用 NAT - SCCP	Cisco IOS XE Release 2.4	ビデオ用 NAT - SCCP 機能は、SCCP ビデオ メッセージ変換サポートを提供します。
T.38 Fax Relay のための NAT - SIP ALG Enhancement	Cisco IOS XE Release 2.4.1	T.38 Fax Relay のための NAT - SIP ALG Enhancement 機能では、IP 経由の T.38 Fax Relay の SIP ALG サポートに対する変換サポートを提供します。

機能名	リリース	機能の設定情報
NAT - SIP 拡張方式	Cisco IOS XE Release 2.4	NAT - SIP 拡張方式機能では、SIP の拡張方式をサポートします。
IP Phone から Cisco CallManager への NAT サポート	Cisco IOS XE Release 2.1	IP Phone から Cisco CallManager への NAT サポート機能では、Cisco IP Phone から Cisco CallManager への通信に Cisco SCCP を設定するための NAT サポートを追加します。
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	Cisco IOS XE Release 2.1	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 機能は、インターネット キー交換（IKE）および ESP のサポートを提供します。NAPT で設定されたデバイスを通じたトンネル モードでカプセル化する必要はありません。
SIP に対する NAT サポート	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.2S	SIP に対する NAT サポート機能によって、SIP ベースの VoIP ソリューション間に NAT を導入できるようになりました。
NAT TFTP ALG サポート	Cisco IOS XE Release 2.1	NAT TFTP ALG サポート機能では、TFTP パケットの変換をサポートします。
NAT VRF-Aware ALG サポート	Cisco IOS XE Release 2.5	NAT VRF-Aware ALG サポート機能では、サポート対象の ALG を持つプロトコルに対し、VPN ルーティングおよび転送（VRF）をサポートします。
NAT vTCP ALG サポート	Cisco IOS XE Release 3.1S Cisco IOS XE Release 3.2S	NAT vTCP ALG サポート機能では、ALG に対する TCP セグメンテーションおよび再構成を処理するための vTCP サポートを提供します。
NAT を介した IPsec ESP のサポート	Cisco IOS XE Release 2.1	NAT を介した IPsec ESP のサポート機能により、オーバーロード モードまたは PAT モードで設定された NAT デバイス経由で、複数の同時 IPsec 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。