IPsec NAT 透過性

IPsec NAT透過性機能では、ネットワーク アドレス変換（NAT）とポートアドレス変換（PAT）の間における多くの既知の非互換性に対処することによって、ネットワーク内の NAT ポイントまたは PAT ポイントを経由して送信される IP セキュリティ（IPsec）のサポートが導入されています。

IPsec NAT 透過性の制約事項

この機能では、NAT および IPsec 間における多くの非互換性に対して対処が行われていますが、次の問題が依然として残されています。

インターネット キー交換（IKE）IP アドレスと NAT

この非互換性が問題になるのは、IPアドレスを、事前共有キーを検索するための検索キーとして使用する場合だけです。NAT またはリバース NAT によって IP 発信元アドレスまたは宛先アドレスが変更されると、IP アドレスと事前共有キーの間でミスマッチが生じます。

組み込み IP アドレスと NAT

ペイロードの完全性は保護されているので、NAT によって IPsec パケット内の IP アドレスを変換することが不可能です。組み込みIPアドレスを使用するプロトコルには、FTP、インターネット リレー チャット（IRC）、簡易ネットワーク管理プロトコル（SNMP）、Lightweight Directory Access Protocol（LDAP）、H.323、および Session Initiation Protocol（SIP）などがあります。

IPsec NAT 透過性に関する情報

IPsec NAT 透過性の利点

IPsec パケットの配信パス内に 1 つ以上の NAT または PAT ポイントがない場合、この機能を導入しなければ、標準の IPsec バーチャル プライベート ネットワーク（VPN）トンネルは動作しません。この機能によって NAT が IPsec 認識となり、その結果、リモート アクセス ユーザは、ホーム ゲートウェイへの IPsec トンネルを構築できます。

IPsec NAT Traversal の機能設計

IPsec NAT 透過性機能では、ユーザ データグラム プロトコル（UDP）ラッパ内に IPsec パケットをカプセル化することによって、NAT または PAT ポイントを通過する IPsec トラフィックのサポートが導入されており、その結果、パケットによる各 NAT デバイス間の通過が可能となっています。次の項では、NAT トラバーサルの詳細を定義します。

IKE フェーズ 1 ネゴシエーション：NAT 検出

インターネット キー エクスチェンジ（IKE）のフェーズ 1 ネゴシエーション中、IKE Quick Mode が開始される前に、NAT サポート、およびネットワーク パス上の NAT イグジスタンスという、2 つのタイプの NAT 検出が実行されます。

NAT サポートを検出するには、リモート ピアとベンダー ID ストリングを交換する必要があります。IKE フェーズ 1 のメイン モード（MM）1 および MM 2 の間、リモート ピアによって、ベンダー ID ストリング ペイロードが、そのピアに送信され、このバージョンでは NAT トラバーサルがサポートされていることが示されます。その後、ネットワーク パス上の NAT イグジスタンスを検出できます。

ネットワーク パス上に NAT が存在しているかどうかを検出すると、2 つのピア間のすべての NAT と、NAT の正確な位置がわかります。NAT デバイスによって、プライベート IP アドレスおよびポートがパブリック値に（またはパブリックからプライベートに）変換されます。パケットがデバイスを通過すると、この変換によって IP アドレスとポートが変更されます。ネットワーク パス上に NAT デバイスが存在しているかどうかを検出するには、ピアによって、各終端からの送信元アドレスと宛先アドレスの両方の IP アドレスおよびポートのハッシュを持つペイロードが送信される必要があります。両端でハッシュが計算され、ハッシュが一致した場合、各ピアによって、両ピア間におけるネットワーク パス上に NAT デバイスが存在しないことが認識されます。ハッシュが一致しない（つまり、誰かがアドレスまたはポートを変換した）場合、各終端では、NAT トラバーサルを実行し、ネットワークを介して IPsec パケットを取得する必要があります。

ハッシュは一連の NAT Discovery（NAT-D）ペイロードとして送信されます。各ペイロードには 1 つのハッシュが格納されます。複数のハッシュが存在する場合、複数の NAT-D が送信されます。ほとんどの環境では、NAT-D ペイロードは 2 つだけです。1 つは送信元 アドレスおよびポート用、もう 1 つは宛先アドレスおよびポート用です。最初に宛先 NA-D ペイロードが

送信され、次に送信元 NAT-D ペイロードが送信されます。これは、受信側では、最初にローカル NAT-D ペイロードを処理し、次にリモート NAT-D ペイロードを処理することを予期する必要があることを意味します。メイン モードでは、NAT-D ペイロードは 3 番目および 4 番目のメッセージに格納され、アグレッシブ モード（AM）では、2 番目および 3 番目のメッセージ内に格納されます。

IKE フェーズ 2 ネゴシエーション：NAT トラバーサル決定

IKE フェーズ 1 による NAT サポート、およびネットワーク パス上の NAT イグジスタンスの検出中に、IKE フェーズ 2 によって両端の各ピアによって NAT トラバーサルが使用されるかどうかが決定されます。QM1 および QM2 におけるクイック モード（QM）セキュリティ アソシエーション（SA）ペイロードは、NAT トラバーサル ネゴシエーション用に使用されます。

NAT デバイスによって IP アドレスおよびポート番号が変更されるので、NAT と IPsec との間に非互換性が発生する可能性があります。そのため、元の送信元アドレスを交換することで、いかなる非互換性も回避できます。

NAT Traversal 用 IPsec パケットの UDP カプセル化

UDP カプセル化によって、IPsec パケットが NAT デバイスを経由できるようにするだけでなく、IPsec、NAT、および PAT 間における多くの非互換性問題に対処できます。解決できる問題は以下のとおりです。

IPsec ESP と PAT との間における非互換性：解決

PAT によって立法 IP アドレスおよびポートが検出されると、その PAT によって Encapsulating Security Payload（ESP）パケットが廃棄されます。このようなシナリオを防ぐために、UDP カプセル化が使用され、UDP ヘッダーの背後に ESP パケットが隠蔽されます。その結果、PAT によって ESP パケットが UDP パケットとして扱われ、ESP パケットが通常の UDP パケットとして処理されます。

チェックサムと NAT との間における非互換性：解決

新しい UDP ヘッダー内では、チェックサムの値は必ずゼロに割り当てられます。この値によって、中間デバイスによるパケットのチェックサムを参照したチェックサムの確認が防止され、それにより、NAT によって IP 送信元アドレスおよび宛先アドレスが変更されるので、TCP UDP チェックサム問題が解決されます。

固定 IKE 宛先ポートおよび PAT 間における非互換性：解決

PAT によって、新しい変換用 UDP ヘッダー内のポート アドレスが変更され、元のペイロードは変更されないままとなります。

UDP カプセル化によってどのように IPSec パケットの送信が可能になるのかを確認するには、次の図を参照してください。

図 *1 : NAT/PAT* ポイントを介した標準的な *IPsec* トンネル（*UDP* カプセル化なし）

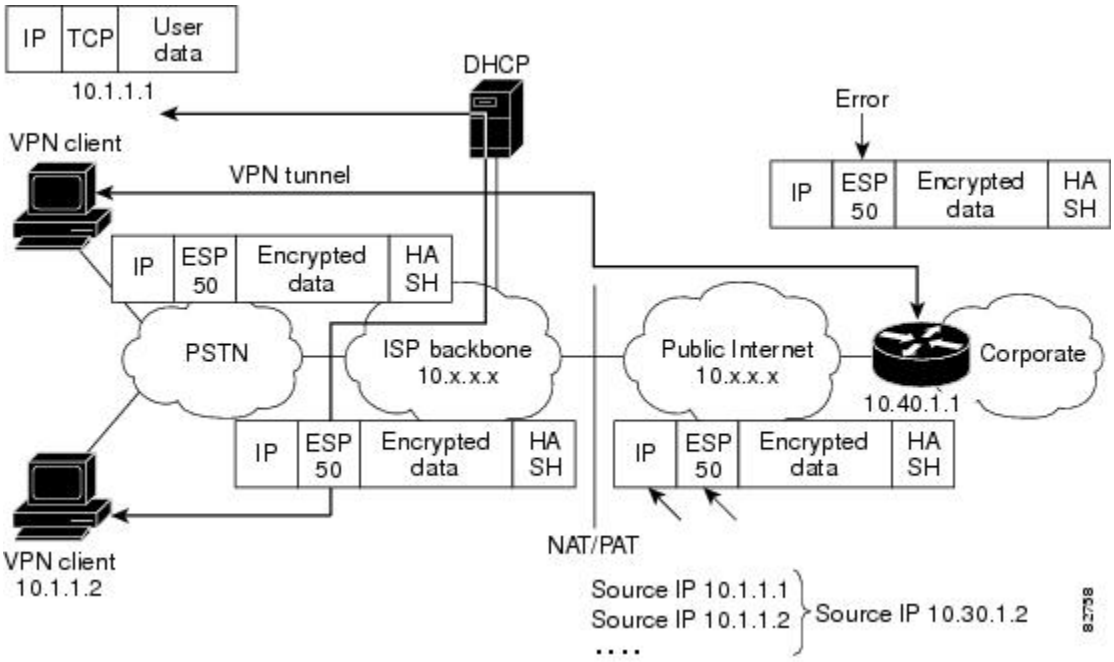
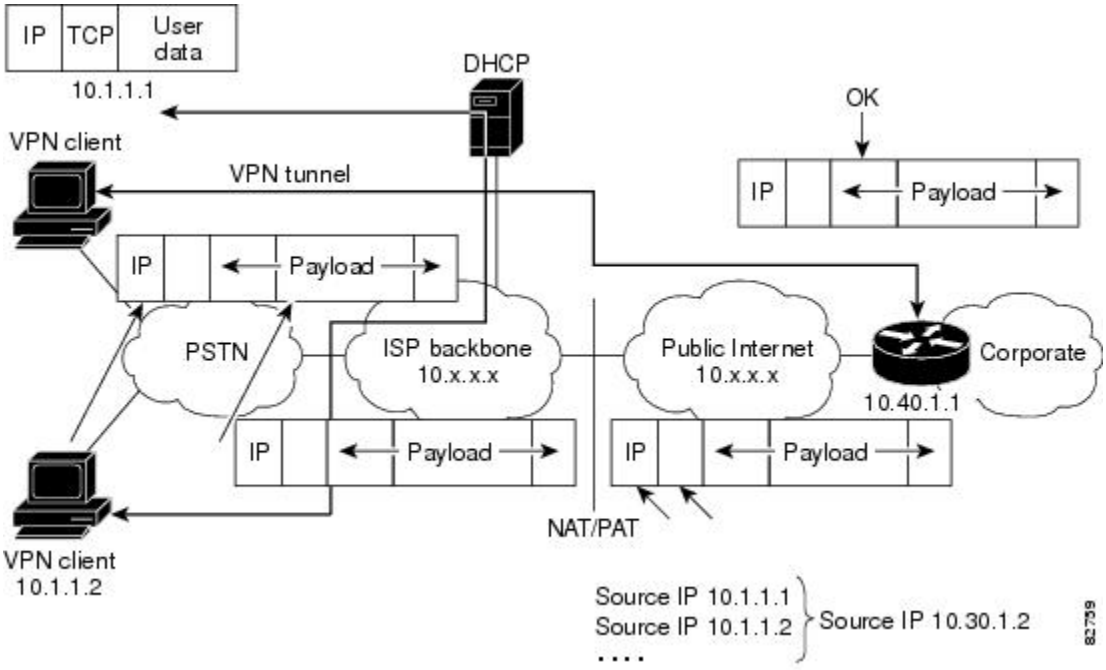


図 *2 : UDP* カプセル化を使用した *IPsec* パケット



ソフトウェア エンジン用 UDP カプセル化処理：トランスポート モードおよびトンネル モード EDP カプセル化

IPsec パケットがハードウェア アクセラレータまたはソフトウェア暗号化エンジンによって暗号化されると、UDP ヘッダーおよび非 IKE マーカ（長さは 8 バイト）が、元の IP ヘッダーと ESP ヘッダーの間に挿入されます。合計長フィールド、プロトコルフィールド、およびチェックサム フィールドはこの変更に合せて変更されます。次の 1 番目の図に、トランスポート モードが適用される前後の IPsec パケットを示します。2 番目の図には、トンネル モードが適用される前後の IPsec パケットを示します。

図 *3:* トランスポート モード：*ESP* カプセル化前後の *IPsec* パケット

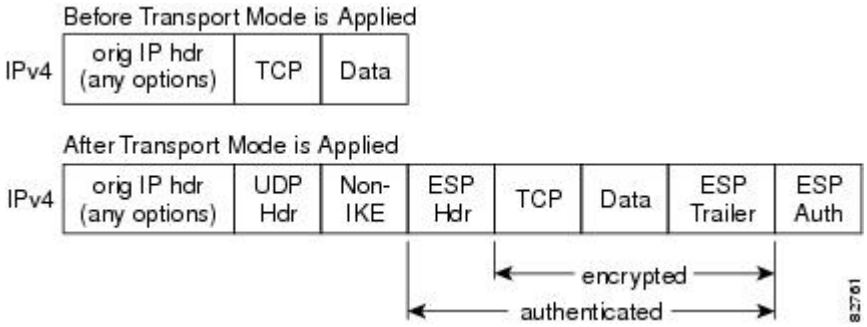
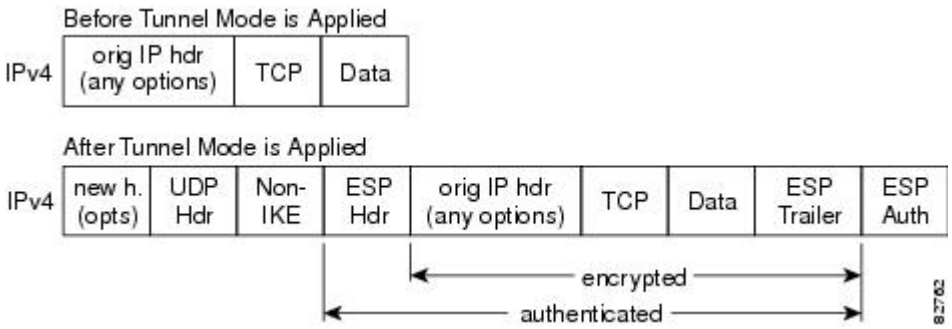


図 *4:* トンネル モード：*ESP* カプセル化前後の *IPsec* パケット



NAT キープアライブ

NAT キープアライブは、2 つのピア間の接続中におけるダイナミック NAT マッピングをアライブに保つためにイネーブルにされます。NAT キープアライブは、1 バイトの非暗号化ペイロードを持つ UDP パケットです。現在の Dead Peer Detection（DPD）実装は NAT キープアライブとほぼ同じですが、若干の違いがあります。DPD は、ピアのステータスを検出するために使用されます。一方、NAT キープアライブは、指定された期間（有効範囲は 5 ～ 3600 秒）にパケットが IPsec エンティティによって送信も受信されなかった場合に送信されます。

NAT キープアライブを（**crypto isakmp nat keepalive** コマンドを使用して）有効化する場合、アイドル値は NAT マッピングの有効期間（20 秒）より小さくなるようにする必要があります。

NAT および IPsec の設定方法

NAT Traversal の設定

NAT Traversal は、VPN デバイスによって自動検出される機能です。Cisco IOS XE Release 2.1 を実行するルータに設定するものはありません。両端の VPN デバイスが NAT-T 対応の場合、NAT Traversal が自動検出され、自動ネゴシエーションが行われます。

NAT Traversal の無効化

ご使用のネットワークですでに IPsec 認識 NAT が使用されている（spi マッチング スキーム）ことがわかっている場合、NAT トラバーサルをディセーブルにする必要が生じることがあります。NAT トラバーサルをディセーブルにするには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no crypto ipsec nat-transparency udp-encapsulation**

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 モードなど、高位の権限レベルを有効にします。 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 crypto ipsec nat-transparency udp-encapsulation**
	例：
	`Router(config)#`
	`no crypto ipsec nat-transparency udp-encapsulation`
		NAT トラバーサルをディセーブルにします。

NAT キープアライブの設定

ルータを、NAT キープアライブを送信するように設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp nat keepalive** *seconds*

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 モードなど、高位の権限レベルを有効にします。 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	**crypto isakmp nat keepalive** *seconds*
	例：
	`Router(config)#`
	`crypto isakmp nat keepalive 20`
		IPsec ノードによる NAT キープアライブ パケットの送信を可能にします。
		• *seconds*：キープアライブパケット間の秒数。範囲は 5 ～ 3,600 秒。
		（注） タイマーが変更されると、インターネット セキュリティ アソシエーションおよびキー管理プロトコル（ISAKMP）SA のキープアライブが既存のタイマーに基づく場合、この秒数は SA ごとに変更されます。
		（注） セキュリティ アソシエーションでキーの再生成の衝突が発生するのを防止するため、5% のジッタ メカニズム値がタイマーに適用されます。ピア ルータが多数あるときに、タイマーが低く設定されすぎている場合、ルータの CPU 使用率が高くなることがあります。

IPsec 設定の確認

設定を確認するには、次の任意の手順を実行します。

手順の概要

1. **enable**
2. **show crypto ipsec sa** [**map** *map-name* | **address** | **identity**] [**detail**

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 モードなど、高位の権限レベルを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**show crypto ipsec sa** [**map** *map-name*	**address**	**identity**] [**detail** 例： `Router# show crypto ipsec sa`	現在の SA によって使用されている設定を表示します。

IPsec および NAT の設定例

NAT キープアライブの設定例

次に、NAT キープアライブを、20 秒毎に送信されるようにイネーブルにする方法の例を示します。

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key 1234 address 10.0.0.1
crypto isakmp nat keepalive 20
!
!
crypto ipsec transform-set t2 esp-des esp-sha-hmac
!
crypto map test2 10 ipsec-isakmp
 set peer 10.0.0.1
 set transform-set t2
 match address 101
```

その他の参考資料

次の項では、IPsec NAT 透過性機能に関連した関連資料を示します。

関連資料

関連項目	マニュアル タイトル
その他の NAT 設定タスク	• 『*Cisco IOS XE IP Addressing Services Configuration Guide*』の「Configuring NAT for IP Address Conservation」モジュール • 『*Cisco IOS XE IP Addressing Services Configuration Guide*』の「Using Application Level Gateways with NAT」モジュール • 『*Cisco IOS XE IP Addressing Services Configuration Guide*』の「Configuring NAT for High Availability」モジュール • 『*Cisco IOS XE IP Addressing Services Configuration Guide*』の「Integrating NAT with MPLS VPNs」モジュール
その他の NAT コマンド	『Cisco IOS IP Addressing Services Command Reference』
その他の IPsec 設定タスク	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Configuring Security for VPNs with IPsec」モジュール
その他の IPsec コマンド	『Cisco IOS Security Command Reference』
IKE に関する情報	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Configuring Internet Key Exchange for IPsec VPNs」モジュール
IKE デッド ピア検出の追加情報	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Easy VPN Server」モジュール

標準

標準	タイトル
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ 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://tools.cisco.com/ITDIT/MIBS/servlet/index

RFC

RFC[1]	Title
RFC 2402	『IP Authentication Header』
RFC 2406	『IP Encapsulating Security Payload (ESP)』

[1] サポートされている RFC がすべて記載されているわけではありません。

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 Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/techsupport

IPsec NAT 透過性の機能情報

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 : IPsec NAT* 透過性の機能情報

機能名	リリース	機能情報
IPsec NAT 透過性	Cisco IOS XE Release 2.1	IPsec NAT 透過性機能では、ネットワーク アドレス変換（NAT）とポート アドレス変換（PAT）の間における多くの既知の非互換性に対処することによって、ネットワーク内の NAT ポイントまたは PAT ポイントを経由して送信される IP セキュリティ（IPsec）のサポートが導入されています。 次のコマンドが導入または変更されました。**crypto isamkp nat keepalive**、 **access-list (IP extended)**、 **show crypto ipsec sa**

用語集

IKE：Internet Key Exchange（インターネット キー エクスチェンジ）。Oakley キー交換や Skeme キー交換をインターネット セキュリティ アソシエーションおよびキー管理プロトコル（ISAKMP）フレームワーク内部に実装したハイブリッド プロトコルです。IKE は、他のプロトコルでも使用できますが、初期実装されるのは IPsec です。IKE は、IPsec ピアを認証し、IPsec キーをネゴシエーションし、IPsec セキュリティ アソシエーション（SA）を実行します。

IPsec：IP Security（IP セキュリティ）。インターネット技術特別調査委員会（IETF）によって開発されたオープン規格のフレームワークです。IPSec は、インターネットなどの保護されていないネットワークを使用して機密情報を送信する場合に、セキュリティを提供します。IPsec はネットワーク層で機能し、Cisco ルータなどの参加している IPsec 装置（ピア）間の IP パケットを保護および認証します。

NAT：Network Address Translation（ネットワークアドレス変換）。企業内で使用されているプライベート IP アドレスを、インターネットなど企業外で使用される、ルーティング可能なパブリック アドレスに変換します。NAT は、アドレスのプライベートからパブリックへの 1 対 1 のマッピングと見なされます。

PAT：Port Address Translation（ポートアドレス変換）。NAT と同様、PAT でもプライベート IP アドレスからルーティング可能なパブリック アドレスへの変換が行われます。NAT とは異なり、PAT では、プライベート アドレスのパブリック アドレスへの多対 1 のマッピングが提供されます。パブリック アドレスの各インスタンスは、一意性を確保するために特定のポート番号と関連付けられます。PAT は、一連のパブリック アドレスを取得するコストが組織にとって高すぎるような環境で使用可能です。

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。