IPsec-NAT Traversal（トラサーバルではなくトラバーサル）

●トンネルモード及びトランスポートモードにかかわらず、ESP では TCP ヘッダ部分は暗号化されるため、ポート番号がわからなくなり、NAPT を使用することができない。

●もちろん IP アドレスの変換のみでポートへの対処はなし（パススルー）もありだが、変換後のグローバル IP アドレス等が 1 つしか使えない場合には、通信は 1 つだけになることは当然のこと。

●そこで ESP では、ESP ヘッダの前に UDP ヘッダを付けて UDP でカプセル化することで、UDP ヘッダにポート番号が復活するので NAT 越えができるようになる。この際、UDP500 にしておけば、Fire Wall を通過できるはずである。

●UDP によるカプセル化は IKE が ISAKMP SA 構築時にネットワーク上に NAT（NAPT）デバイスの存在を探知すると IKE が自動的にカプセル化してくれる。

●上記とは別に、トンネルモード及びトランスポートモードにかかわらず、AH では IP アドレスは認証範囲なので、NAT で IP アドレスを変更すると認証エラーとなる。これについての NAT 越えは言及しない。

PFS 又は FS（Perfect Forward Security：前方秘匿性）

●鍵交換アルゴリズム（ECDHE や DHE：ECDHE 等）による使い捨ての鍵ペアとサーバ証明書に使用する鍵ペアとは無関係。

●鍵交換の際のパラメータが漏洩しても、そのパラメータを使用して鍵ペアを作らないため、過去の暗号文の安全性が保たれることを PFS という。

●TLS1.2 の RSA 鍵交換（TLS1.3 で廃止）は、以下のとおり共通鍵を生成するため、PFS は確保できず

①最初の Client Hello でクライアントはサーバに乱数を送る。その逆も実施

②クライアントがサーバの公開鍵で暗号化したプレマスターシークレットをサーバに送信。サーバは自身の秘密鍵で復号。この暗号化と復号に RSA（素因数分解問題の困難性を利用）を使用。

③サーバとクライアントは、①の乱数及び②のプレマスターシークレットからマスターシークレットを生成し、そこから共通鍵を生成する。

●TLS1.2 及び 1.3 における ECDHE 等は PFS を確保している。共通鍵を生成は以下のとおり

①サーバ側ではサーバで生成した秘密鍵とクライアントで生成してクライアントから送られてきた公開鍵から共通鍵を生成。クライアント側ではクライアントで生成した秘密鍵とサーバで生成してサーバから送られてきた公開鍵から共通鍵を生成。

②上記①における各々の秘密鍵（乱数）とセッション確立時に交換した乱数等（A）を基に各々の公開鍵を生成している。

③上記②において、DHE では離散対数問題の困難性を利用して、ECDHE では楕円曲線問題の困難性を利用しているため、相手の秘密鍵を知ることは極めて困難ではあるが、A があることにより、上記①で秘密鍵と公開鍵から生成される各々の共通鍵は同じものとなる。

●TLS1.2 は主体認証、鍵交換の順であるが、TLS1.3 は逆なので主体認証は暗号化されている。

DH 鍵交換アルゴリズム

●DH は離散対数、ECDH は楕円曲線問題の困難性を利用している。RSA は素因数分解の困難性を利用。

①最初の Client Hello と Server Hello で交換される乱数が次の 2 つの数であるかは定かではないが、とりあえず、交換した乱数は、g（整数）と n（素数）であり、g＜n とする。

②A の秘密鍵（乱数）を x とすると、公開鍵は　p=(g∧x) mod n であり、B に送る。

　B の秘密鍵（乱数）を y とすると、公開鍵は　q=(g∧y) mod n であり、A に送る。

③A の秘密鍵 x と B の公開鍵 q から、共通鍵は z1=(q∧x) mod n

　B の秘密鍵 y と A の公開鍵 p から、共通鍵は z2=(p∧y) mod n

④z1=z2 と z2 に p=(g∧x) mod n を代入して、**(q∧x) mod n = (p∧y) mod n = (g^xy) mod n**

⑤g, n, p, q は既知であり、x, y が秘密であるが、離散対数の困難性から、x, y を探し出すことは極めて困難。n を大きくすればするほど、不可能になる。