ICS 33.040.40

YD

中华人民共和国通信行业标准

YD/T 1468-2006

IP 安全协议（IPSec）穿越网络地址翻译（NAT）技术要求

Technical Requirements of IPSec Traverse NAT

2006-06-08 发布　　2006-10-01 实施

中华人民共和国信息产业部　发布

目　次

前　言

本标准是IP安全协议（IPSec）系列标准之一。该系列标准的名称及结构预计如下：

1.《IP安全协议体系结构》（MOD IETF RFC2401）

2.《IP认证头（AH）》（MOD IETF RFC2402）

3.《IP封装安全载荷（ESP）》（MOD IETF RFC2406）

4.《IP安全协议（IPSec）技术要求》

5.《IP安全协议（IPSec）测试方法》

6.《IP安全协议（IPSec）穿越网络地址翻译（NAT）技术要求》

7.《因特网密钥交换协议（IKE v2）第1部分：技术要求》

8.《因特网密钥交换协议（IKE v2）第2部分：测试方法》

本标准的附录A、附录B和附录C是资料性附录。

本标准由中国通信标准化协会提出并归口

本标准起草单位：信息产业部电信研究院
成都迈普产业集团有限公司
中兴通讯股份有限公司

本标准主要起草人：袁　琦　张　炜　王文煜　田　辉　何宝宏

IP 安全协议（IPSec）穿越网络地址翻译（NAT）技术要求

1 范围

本标准规定了IPSec穿越NAT的技术要求，包括IPSec穿越NAT存在的兼容性问题、兼容性要求、解决方法以及穿越NAT对IPSec的影响等。

本标准适用于支持IPSec穿越NAT的数据设备。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

YD/T 1466-2006	IP 安全协议（IPSec）技术要求
IETF RFC 768（1980）	用户数据报协议（UDP）
IETF RFC 1321（1992）	MD5 消息摘要算法
IETF RFC 1828（1995）	使用 MD5 密钥的 IP 认证
IETF RFC 1829（1995）	ESP DES-CBC 转换
IETF RFC 2085（1997）	使用抗重播的 HMAC-MD5 IP 认证
IETF RFC 2104（1997）	HMAC：消息认证的密钥哈希
IETF RFC 2401（1998）	IP 安全架构
IETF RFC 2402（1998）	IP 认证头
IETF RFC 2403（1998）	ESP 和 AH 中 HMAC-MD5-96 的使用
IETF RFC 2404（1998）	ESP 和 AH 中使用 HMAC-SHA-1-96 的使用
IETF RFC 2405（1998）	带有显式 IV 的 ESP DES-CBC 密码算法
IETF RFC 2406（1998）	IP 封装安全载荷
IETF RFC 2407（1998）	对 ISAKMP 的因特网 IP 安全域解释
IETF RFC 2408（1998）	互联网安全联盟和密钥管理协议（ISAKMP）
IETF RFC 2409（1998）	互联网密钥交换协议（IKE）
IETF RFC 2410（1998）	IPSec 的空加密算法和使用
IETF RFC 2663（1999）	IP NAT 的术语和研究
IETF RFC 3022（2001）	传统 IP NAT
IETF RFC 3056（2001）	IPv4 网中连接 IPv6 域
IETF RFC 3103（2001）	域限定 IP：协议说明
IETF RFC 3715（2004）	IPSec-NAT 兼容性要求
IETF RFC 3947（2005）	IKE 中 NAT 地址穿越协商
IETF RFC 3948（2005）	IPSec 数据包的 UDP 封装

3 缩略语

下列缩略语适用于本标准。

AH	Authentication Header	认证头
ALG	Application Layer Gateways	应用层网关
ESP	Encapsulating Security Payload	封装安全载荷
DES	Data Encryption Standard	数据加密标准
DOI	Domian of Interpreter	解释域
DMZ	Demilitarized Zone	非军事区域
FTP	File Transfer Protocol	文件传输协议
GRE	Generic Routing Encapsulation	通用路由封装
HMAC	HASH MAC	散列MAC
IANA	Internet Assigned Numbers Authority	互联网号分配机构
ICMP	Internet Control Message Protocol	互联网控制消息协议
ICV	Integrity Check Value	完整校验值
IKE	Internet Key Exchange	互联网密钥交换
IPSec	IP Security	IP安全
IP	Internet Protocol	互联网协议
IRC	International Relay Chat	互联网中继聊天
ISAKMP	Internet SA Key Management Protocol	互联网SA密钥管理协议
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
MAC	Message Authentication Code	消息验证码
MD5	Message Digest 5	消息摘要5
NA（P）T	Network Address （Port）Translation	网络地址翻译
RSIP	Realm Specific IP	特定领域IP
SA	Security Association	安全联盟
SAD	Security Association Database	安全联盟数据库
SCTP	Stream Control Transmission Protocol	流控制传送协议
SIP	Session Initial Protocol	会话初始协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SPI	Security Parameter Index	安全参数索引
SPD	Security Policy Database	安全策略数据库
TCP	Transmission Control Protocol	传输控制协议
UDP	User Datagram Protocol	用户数据报协议
VPN	Virtual Provider Network	虚拟专用网

4 IPSec 穿越 NAT 存在的兼容性问题

4.1 概述

IPSec作为一种重要的安全技术得到越来越广泛的应用，而客户网络边缘大量使用的NAT地址翻译操作，可能影响到IPSec的正常操作。NAT分为基本NAT（网络地址翻译）和NAPT（网络地址端口翻译）两种类型。基本 NAT只是对IP地址进行翻译；而NAPT除了翻译地址外，还要翻译传输层标识，如TCP/UDP端口号、ICMP的查询标识。本标准中NA（P）T表示为NAT或NAPT。

目前NAT和IPSec之间存在的不兼容性问题可以分为以下三类：

（1）NA（P）T固有的问题。这类不兼容问题直接由NA（P）T与IPSec协议本身不兼容产生，因此存在于所有的NA（P）T设备中；

（2）NA（P）T实现上的问题。这类不兼容问题虽然不是NA（P）T协议所固有的，但却在大量的NA（P）T实现中存在。因为它们不是NA（P）T协议的固有问题，因此原则上在以后的NA（P）T设计实现中可以避免该类问题的产生。但由于这些问题已经广泛存在，因此在NA（P）T穿越方案中也必须考虑这些问题。

（3）辅助功能引入的问题。这类不兼容问题出现在那些试图解决IPSec NA（P）T穿越问题的NA（P）T设备中。在这些NAT设备中，可能由于设计部分穿越辅助功能而产生了新的不兼容性，造成更难于解决的问题。虽然不是所有的NA（P）T设备都提供这种所谓的辅助功能，但考虑到该类问题的普遍性，在NA（P）T穿越方案中也需要考虑这类问题。

4.2 NA（P）T 固有的问题

NA（P）T协议固有的不兼容性包括。

（1）IPSec AH和NAT的不兼容。由于AH所提供的完整性检验中包括了对IP源地址和目的地址的检验，而NAT和反向NAT设备对地址域进行了修改，从而导致AH检验失效。ESP协议中对完整性的检验不包括IP源地址和目的地址，因此在ESP中不存在这类不兼容问题。

（2）NAT与校验和的不兼容。由于TCP和UDP的校验和计算中包含了伪头部，因此校验和的计算结果依赖于IP源地址和目的地址。因此，如果在传输过程中经过了NAT设备，则接收者对校验和的计算也存在问题。因此，IPSec ESP只有在不涉及TCP/UDP协议或者不进行校验和计算时才能够顺利通过NAT（例如，IPSec隧道模式、IPSec/GRE隧道以及IPv4 UDP应用）。

在IPv4中，TCP校验和必须进行计算和确认。在IPv6中，UDP/TCP校验和都必须计算和确认，因此上述问题广泛存在。

SCTP（Stream Control Transmission Protocol）中使用的CRC32C算法只对SCTP包进行校验和计算，而没有包含IP头部。因此，NAT不会使SCTP CRC无效，也就不会产生这类不兼容问题。

因为传输模式的IPSec通信流通过加密方式完成完整性保护和身份验证，在检查UDP/TCP校验和之前对数据包进行修改检测，因此校验和的确认仅用于防止内部处理的错误。

（3）IKE地址标识符和NAT的不兼容。在IKE主模式或快速模式交换中使用IP地址作为标识符，而NAT或反向NAT对IP源/目的地址的修改使得标识符和IP头部中的IP地址不匹配，IKE实现将丢弃存在该类问题的报文。

为避免这种情况的出现，可以使用用户ID和FQDN代替IP地址作为标识符。如果需要用户身份验证，则使用ID类型为ID_USER_FQDN的标识符。而如果使用机器身份验证，则使用ID_FQDN类型。如果证书

在第一阶段交换，以上两种情况中都必须确认所提议的身份与证书中的身份相匹配。然而，某些情况下（如SPD条目描述子网时），不能用USER_FQDN和FQDN作为IKE标识符使用。

因为第二阶段标识符中的源地址常用来形成五元的入流量SA选择符，为了不减弱入流量的SA处理，在选择符中使用目的地址、协议、源端口和目的端口。

（4）固定IKE目的端口和NAPT之间的不兼容。如果在NAPT设备后面有多个主机对同一个响应方发起IKE安全联盟协商，这时需要提供一种机制使NAPT能够对响应方返回的IKE报文进行解复用。典型的解决方法是由发起方转换IKE UDP源端口，因此响应方必须能接收从一个非500端口发送来的IKE通信流，并必须对该端口进行响应。

在密钥重生成期间应避免在非预期的情况下产生的动作。如果在密钥重生成时，浮动的源端口没有作为目的端口，则NAT就不能将密钥重生成期间的报文发送到正确的目的地。

（5）重叠（overlap）SPD条目和NAT间的不兼容。如果NAT后面的主机在IKE快速模式中使用相同的目的地址协商重叠的SPD条目，则报文可能被发送到错误的IPSec SA中。产生该问题的原因在于发送方，因为发送方是相同的终端并可以用来传送相同的通信流，从而使发送方的IPSec SA看起来是完全相同的。

（6）IPSec SPI选择和NAT的不兼容。因为IPSec ESP通信流是被加密的，其内容对NAT是不可知的，因此NAT必须使用在IP和IPSec头中的信息来解复用输入的IPSec通信流。通常使用IP地址、安全协议和IPSec SPI的组合来达到该目的。然而，因为主机或网关选择输出/输入SPI是独立的，所以NAT无法仅仅通过检查输出流来确定某个输入流到底对应哪个目的主机。因此，如果NAT后面的两个主机同时向一个目的地址发起建立IPSec SA，则NAT可能将输入的IPSec报文发送到错误的目的地址上。

本质上讲这并不是IPSec的不兼容性问题，而是IPSec实现方法的问题。在AH和ESP中，接收方主机指定用于给定SA的SPI。当前，目的IP地址、SPI和安全协议一起可以惟一识别一个安全关联，这意味着接收方主机可以选择这样两个SA：其中一个是SPI=470，目的IP = 10.2.3.4，而另一个是SPI=470，目的IP = 10.3.4.5。

对于接收主机来说，也可能给每一个单播的SA分配惟一的SPI。在这种情况下，目的IP地址只需要用来检查它是否是“该主机的任意有效的单播IP地址”，而不必检查它是否是由发送方主机使用的特定目的IP地址。该方法完全向后兼容，只需要接收主机改变它的SPI分配方式和IPSec_esp_input（）代码。

（7）嵌套IP地址和NAT的不兼容。因为IPSec对载荷进行了完整性保护，不允许NAT对封装在IPSec报文中的IP地址进行转换，从而使得NAT应用层网关（Application Layer Gateways，ALG）失效。

应用层内部包含IP地址的协议包括：FTP、IRC、SNMP、LDAP、H.323、SIP、SCTP（可选包含）以及许多游戏协议。为解决这个问题，在主机或安全网关上安装应用层网关时，必须保证在IPSec封装以前和IPSec解封装以后对应用通信流进行处理。

（8）NA（P）T隐含的方向性问题。通常内部主机发送一个输出报文通过NAT设备时，NAT才为之创建输入的映射状态。这种方向性的存在，妨碍了外部主机向NAT后面的主机主动建立IPSec SA的操作。

（9）入流量的SA选择符验证。假设IKE协商第二阶段的选择符，因为RFC 2401要求报文的源地址和SA选择符值匹配，入流量的SA处理将丢弃解封装的报文，而ESP报文的NA（P）T处理将改变报文的源地址。

4.3 NA（P）T实现上的问题

很多NA（P）T实现上带来的不兼容性有。

（1）不能处理非UDP/TCP通信流。一些NAPT直接丢弃非UDP/TCP报文（如实现NAT功能的防火墙），这些NAPT是无法传递SCTP、ESP或AH通信流的。

（2）NAT映射超时。相同UDP端口映射条目的超时时间在各种NA（P）T实现中互不相同。因此，即使IKE包被正确地转换，其转换状态也可能被过早地删除。

（3）不能处理输出的分片。当输出IP包长大于本地出接口的MTU时，大多NA（P）T能够正确地为数据包分片。然而，如果数据包本身就是分片包，则大多NAPT都不能正确处理这种分片包的转换。两个主机在向同一个目的主机发送分片数据包，其分片标识可能会重叠。而目的主机通过分片标识符和分片偏移进行重组，所以其结果会导致数据重组的失败。极少数NA（P）T通过支持标识符转换来避免这种标识符冲突的情况。

分片由NAT执行则不会发生标识符冲突，因为在一个源/目的地址对中可以保证使用惟一的分片标识符。

因为分片可能只有68字节长，所以无法保证在第一个分片中一定包含完整的TCP头部，这时就需要重计算TCP校验和的NA（P）T就需要修改随后的分片。因为分片可能乱序、IP地址可能嵌套在报文中且可能分布在不同的分片中，因此NA（P）T必须在完成转换之前先完成分片重组。由于处理的复杂性，极少数NA（P）T支持重计算校验和功能。

（4）不能处理输入的分片。因为通常只有第一个分片包含完整的IP/UDP/SCTP/TCP头部，所以NAPT应该能够执行基于源/目的IP地址和分片标识的转换。由于分片可以重新排序，如果后续分片在第一个分片之前到达，则对一个给定的分片标识符的头部可能是未知的，并且该头部还可能被划分到几个分片之中。因此，NA（P）T需要在转换之前先执行重组，极少数NA（P）T支持这个功能。对于NAT来说，源/目的地址就足以确定转换了，因此不存在NAPT中的这种情况。然而，由于IPSec或IKE头可能分在不同的分片中，因此在NAT中仍可能需要进行重组。

4.4 辅助功能引入的问题

在IPSec和NAT的辅助功能之间存在的不兼容问题包括。

（1）ISAKMP头部检查。部分NAT设备试图使用IKE Cookies来实现IKE通信流的解复用。与源端口解复用相似，因为阶段1的密钥重生成将使用不同于以前通信流所使用的Cookie值，使用IKE Cookie解复用在密钥重生成时将产生相同的问题。

（2）对端口500的特殊处理。一些IKE实现中，由于不能处理源端口非500的UDP包，所以一些NAT就对源端口是500的UDP包不进行转换。对于每个目的网关来说，这些NAT只允许使用一个IPSec客户端，除非它们检查ISAKMP头部中造成上述问题的Cookie值。

（3）ISAKMP载荷检查。对于试图解析ISAKMP载荷的NAT实现，它可能不能处理所有的载荷序列组合，或者不支持IKE可选协商的vendor_id载荷。

5 IPSec 穿越 NAT 的兼容性要求

为了评估IPSec穿越NAT解决方案的兼容性，应该考虑以下因素。

（1）可部署性

IPv6将最终解决地址短缺问题，而地址短缺正是IPv4引入NAT的原因，因此IPSec-NAT的穿越问题只是在广泛使用IPv6之前需要解决的过渡性问题。所以，IPSec-NAT兼容性解决方案必须比IPv6易于部署，并且比IPv6先于部署。

IPv6的部署不但需要修改主机而且还要修改路由器，所以需要同时改变路由器和主机的IPSec-NAT兼容性解决方案，从部署难度上来说与IPv6相接近。因此，IPSec-NAT兼容性方案应该只修改主机，而不需要改变路由器。

在IPSec-NAT兼容性方案中主机和NA（P）T网关之间不应该再存在其他的额外通信。如果还要定义主机与NAT的额外通信，则需要改变已有的NA（P）T实现，同时还要进行主机和NA（P）T实现之间的互操作性测试。为了在短时间内实现穿越方案的部署，必须要求兼容性解决方案可以与现存的路由器和NA（P）T产品协同工作。

（2）协议兼容性

IPSec NAT穿越方案不解决某些协议与NAT的兼容性问题，这些协议是指使用IPSec协议不能进行安全保护时无法穿越NA（P）T的协议。因此，即使获得了IPSec NAT穿越方案，ALG还需要支持其他协议的穿越方案。

（3）方向性

因为NA（P）T的方向性也是一种安全功能，所以IPSec穿越方案不应该允许NA（P）T后面的主机接收来自任意IP地址随意发送的IPSec或IKE通信流。一旦双向IKE和IPSec通信已经建立，地址转换的映射已经连接。

（4）远程访问

因为IPSec的一个重要应用是远程访问公司的内部网络，则NA（P）T穿越方案必须支持通过IPSec隧道模式或者L2TP over IPSec的NAT穿越，这就要求穿越方案必须考虑远程客户端与VPN网关之间存在多个NA（P）T的情况。

远程通信时必须考虑多种情况：客户端可能有可路由的公网地址，而VPN网关可能在至少一个的NA（P）T后面；也可能是客户端和VPN网关都在一个或多个不同的NA（P）T后面；在远程访问者连接到VPN网关时，在每个不同的NA（P）T后面，不同远程访问者可能使用相同的私有IP地址；或者在同一个NA（P）T后面多个远程访问者可能位于同一个私网，使用不同的私有IP地址。

在网关到网关的方案中，公司网络和Internet之间可能还存在一个私有地址网络。在这种情况下，连接公司部分网络的IPSec安全网关将在外部接口中配置私有地址，并由一个NA（P）T网络连接DMZ网络到因特网。

IPSec-NAT解决方案中必须能像保护主机到网关的通信那样对主机到主机的通信进行安全保护。在私网中的主机必须能够与另一个主机建立使用IPSec的TCP连接或UDP会话，即使在它们中间存在一个或多个NA（P）T，例如，在办公室到公司的边界处可能部署了NA（P）T，而在公司与Internet之间又部署了另外的NA（P）T，这可能需要主机上的TCP和UDP通信流进行一些特殊的处理。

存在NA（P）T的两个主机之间建立SCTP连接可能遇到更多的问题。因为SCTP支持多穴，那么如果某一方主机使用了多个IP地址，这些地址将在关联建立的时候作为SCTP包（INIT和INIT-ACK）的一部分传输给对方主机。如非必要，在SCTP包中不应该包含IP地址。而在SCTP进行NAT穿越时，如果包含了IP地址，则双方主机的关联将无法建立。

（5）防火墙兼容性

因为防火墙已经广泛应用，IPSec-NAT兼容性方案必须能使防火墙管理员创建简单的、静态的访问规则，来决定是否允许IKE以及IPSec-NAT的穿越，应该避免IKE或者IPSec目的端口的动态分配。

（6）可扩展性

IPSec-NAT兼容性方案应该具有良好的扩展性，能够部署在大规模远程访问的环境之中。在大量远程接入的环境下，不可能在同一时间段内只有一个主机使用同一个给定的地址进行通信。因此，在兼容性方案中必须解决SPD条目重叠和接收包解复用的问题。

（7）模式支持

IPSec-NAT方案必须支持IPSec ESP模式的穿越。例如，IPSec安全网关必须支持ESP隧道模式的NA(P)T穿越；IPSec主机必须支持IPSec传输模式的NA（P）T穿越。

AH的目的就是要保护IP头部中不变的区域（包括地址域），而NA（P）T必须转换地址，从而使AH完整性检验失效。因此，NA（P）T和AH从根本上就是不兼容的，在IPSec-NAT兼容性方案中没有必要支持AH传输或隧道模式。

（8）后向兼容和互操作性

IPSec-NAT兼容性方案中必须能够与已有的IKE/IPSec实现互操作，与不经过NA（P）T的IKE/IPSec进行通信，即IPSec-NAT穿越方案必须能向后兼容RFC 2401定义的IPSec和RFC 2409定义的IKE。另外，穿越方案应该能够自动检测是否存在NAT，从而使得通信双方只在必要的时候才使用NA(P)T穿越支持。要求方案必须能够判断通信对方的IKE实现是否支持NA（P）T穿越，以协商双方可以只进行标准的IKE会话。这也表明虽然IKE在发起协商时目的端口只能使用500端口，但并没有对源端口提出特殊要求，因此UDP源端口可以使用500或非500的端口。

（9）安全性

不允许由于IPSec-NAT兼容性解决方案的引入，对IKE或IPSec安全性带来影响，例如，一个可行的方案必须证明它没有引入新的拒绝服务攻击和欺骗攻击。IKE必须允许双向方式的密钥重生成。

6 IPSec 穿越 NAT 实现要求

6.1 概述

因为AH中外部IP地址的保护与NAT是不兼容的，AH不在本实现要求的讨论范围之内。本实现假定使用IKEv1或IKEv2协商SA。为了完成IPSec穿越NAT，本实现要求使用IKE协商和UDP封装两种方法。

IKE协商分为两部分。第一部分是在NAT穿越过程中，IKE阶段1需要检测另一端是否支持NAT穿越，检测两端之间是否存在一个或多个的NAT。第二部分是在IKE快速模式中，如何协商UDP封装IPSec包的使用，如何传送原始的源和目的地址到对端。传输模式中原始地址用来更新TCP/IP校验和，这样在NAT转换后这些地址能相互匹配。

UDP报文封装和解封装ESP包时，UDP端口号与IKE流使用的端口号相同，采用这种方式扩展性好，易于配置和实现。此时IKE实现不能使ESP包中SPI为零字段，以便能区分IKE包和ESP包。

6.2 IKE 协商

6.2.1 阶段 1

在阶段 1 协商中，需要针对 NAT 执行两种探测：其一是探测是否支持 NAT 穿越，其二是探测在通信路径中是否存在 NAT。NAT 会改变 IKE UDP 的源端口，从而接收方必须能处理源端口不是 500 的 IKE 报文。在下列两种情况中 NAT 不会改变源端口：

- NAT 后面只有一个 IPSec 主机；
- 对于第一个发起协商的 IPSec 主机，NAT 可以保持其端口为 500，并只改变指定的 IPSec 主机 IP

地址。

接收方必须将响应发送至包的源地址，那么当响应方进行密钥重生成或者发送通告时，其报文必须以相同的端口和 IP 地址进行发送，该端口和 IP 地址与最近一次 IKE SA 的报文所使用的端口和 IP 地址相同。

例如，当发起方以源和目的端口都为 500 发送一个报文时，NAT 会将其转换为源端口为 12312 而目的端口为 500 的报文，响应方必须能处理这个源端口为 12312 的报文，并能以源端口为 500、目的端口为 12312 进行回应，然后 NAT 再将回应报文转换成源端口和目的端口都为 500 的报文。

6.2.1.1 探测是否支持 NAT 穿越

通过 Vendor ID 载荷交换来确定远程主机是否支持 NAT 穿越。如果协商双方支持 NAT 穿越，则协商双方在阶段 1 的前两条消息中加入一个 Vendor ID 载荷，载荷的内容为对特定字串进行 MD5 运算得出的散列值。在该字串中表明其支持的 NAT 穿越方法所遵循的要求。

6.2.1.2 探测是否存在 NAT

NAT-D（NAT Discovery）载荷有两重目的：它不仅用于探测两个 IKE 实体之间是否存在 NAT，同时也用于探测 NAT 位于何处，这样 keepalive 消息就能从位于 NAT 后面的实体发出。

为了探测出两台主机之间的 NAT，则需要检查 IP 地址和端口沿着传输路径是否发生改变。协商双方各自向对端发送源方和目的方的 IP 地址与端口的散列值，这样就可以检测地址和端口在传输过程中是否发生改变。如果协商双方计算出的散列值与它们收到的散列值相同，则它们之间没有 NAT。反之，则是在传输中对地址或端口进行了转换，这就说明通过的 IPSec 报文经过了 NAT 穿越的处理。

如果发送者不能确定它自己的 IP 地址（比如拥有多个网络接口，并且不能确定将包路由到哪一个接口），它可以在报文中包含多个本地 IP 地址的散列值。在这种情况下，当且仅当所有的散列值均不匹配时表明 NAT 的存在。

通过使用一系列的 NAT-D 载荷来传送这些散列值。每个载荷包含一个散列值，所以对于多个散列值需要传送多个 NAT-D 载荷。一般情况下只需要两个 NAT-D 载荷。

对于主模式，NAT-D 载荷包含在其第三和第四条交换消息中，野蛮模式则包含在第二和第三条消息中。

NAT-D 载荷的类型是 15，其格式如图 1 所示。

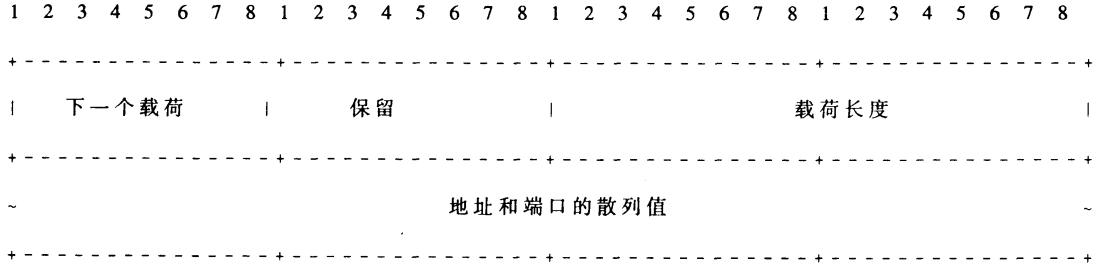


图 1 NAT-D 载荷格式

散列值的计算使用已协商的 HASH 算法，其计算公式如下：

HASH = HASH（CKY-I|CKY-R|IP|Port）

上式中，括号内的所有数据都是网络字节顺序。对于 IPv4，IP 域占 4 个字节，而对于 IPv6 则占 16 个字上节。端口号占两个字节。在消息交换过程中，第一个 NAT-D 载荷包含远程节点（也就是 UDP 包

的目的方）的 IP 地址和端口，其余的 NAT-D 载荷包含所有可能的本地节点（也就是 UDP 的源方）的 IP 地址和端口。

如果在协商双方之间没有 NAT，则在接收到的消息中，其第一个 NAT-D 载荷应该能匹配某个本地的 NAT-D 载荷（也就是本地主机所发送的本地 NAT-D 载荷），而在剩下的载荷中必须有一个能够匹配接收方的远程节点的 IP 地址和端口。如果第一次检查失败（也就是第一个载荷不能匹配任何本地的 IP 地址和端口），这就说明在协商双方之间存在 NAT，同时本地主机应该开始发送 keepalive 消息。

CKY-I 和 CKY-R 是发起方和响应方的 Cookie 值，将它们加到 HASH 运算中以防止针对 IP 地址和端口的预先计算攻击。

在主模式中使用 NAT 穿越的阶段 1 交换的例子如图 2 所示。

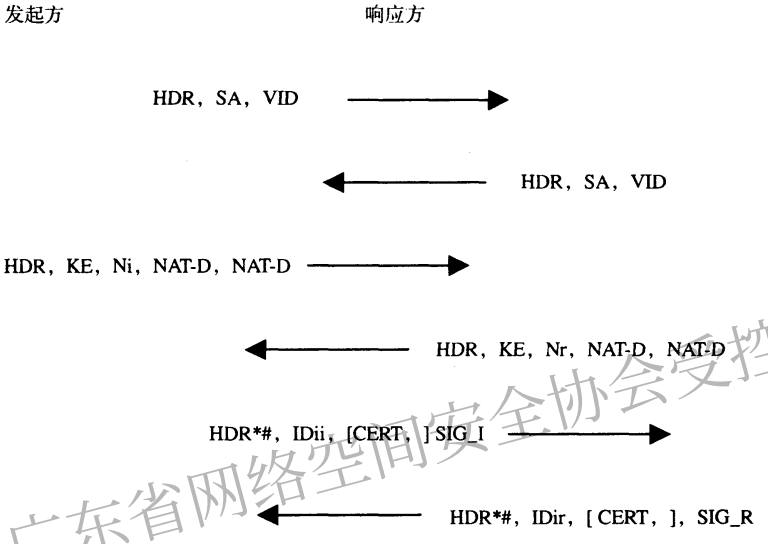


图 2 在主模式中使用 NAT 穿越的阶段 1 交换的例子

在野蛮模式中使用 NAT 穿越的阶段 1 交换的例子如图 3 所示。

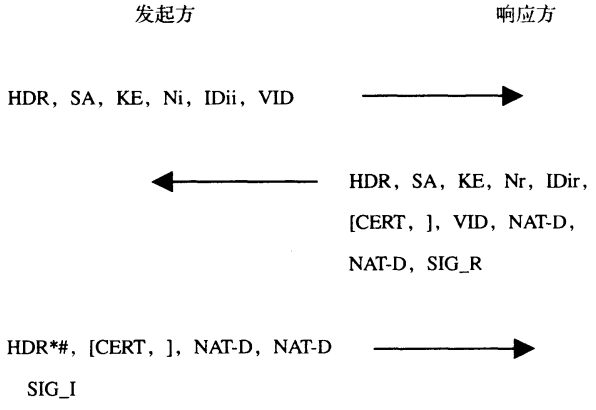


图 3 在野蛮模式中使用 NAT 穿越的阶段 1 交换的例子

注：“#”表示如果探测到存在 NAT，则该消息发送至已浮动的端口。

6.2.2 端口浮动

对 IPSec 存在特殊处理的 NAT 设备会造成问题。即使 NAT 后有多个客户端，某些 NAT 不改变 500 的源端口号，也能将 IKE Cookie 值映射到分解的通信流而不是使用源端口。对于 IKE 来说很难发现 NAT 是否具有上述能力，对于 NAT 的透明性这些方法都是有问题的。最好的办法是使 IKE 通信流简单地离开

500 端口，以避免任何 IPSec-aware NAT 的特殊处理。

以最为常见的发起方在 NAT 后面的这种情形为例，一旦探测到 NAT，发起方必须尽快将发送端口浮动到 4500 以减少发生 IPSec-aware NAT 问题的机会。

在主模式中，如果存在 NAT，发起方必须在发送 ID 载荷的时候浮动端口。发起方必须将 UDP 源和目的端口都设置为 4500，其后所有发送到该实体的报文（包括信息通告）都必须使用 4500 端口。另外，考虑到通信流分解，IKE 数据必须预先考虑一个非 ESP 标记。

因此，假设使用数字签名方式的进行身份验证，则现在的 IKE 报文格式变为：

IP UDP（4500，4500）<non-ESP marker> HDR*，IDii，[CERT，] SIG_I

当响应方接收到这个报文时，它执行正常的解密和载荷处理。如果执行成功，则响应方必须更新本地状态，以使其后所有发送到对端的报文（包括信息通告）都使用新的端口，同时也可能使用新的 IP 地址，该地址从接收的有效报文中获得。因为 NAT 将把 UDP（500，500）映射成 UDP（*X*，500），并将把 UDP（4500，4500）映射成 UDP（*Y*，4500），因此端口一般情况下是不同的，而 IP 地址却极少与 NAT 已转换的 IP 地址不同。响应方必须使用 UDP（4500，*Y*）响应随后所有的 IKE 报文。

如果响应方需要执行阶段 1 的密钥重生成，它必须用 UDP（4500，*Y*）来发起协商。任何支持 NAT 穿越的实现必须支持由端口 4500 发起的协商。如果协商是从端口 4500 发起的，则它不需要在交换中改变。

一旦端口已经发生改变，如果此时在端口 500 上接收到报文，则认为是过时的报文。如果该报文是信息通告，那么可以根据本地策略来决定是否进行处理。如果是主模式或野蛮模式中的报文，则应该丢弃。

主模式中进行端口改变的例子如图 4 所示。

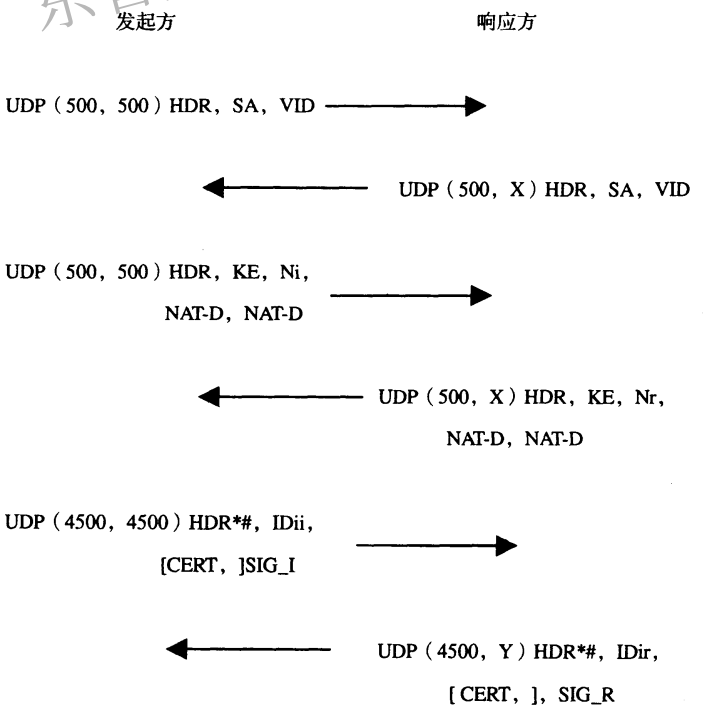


图 4 主模式中端口改变的例子

野蛮模式的算法与主模式非常相似。在探测到 NAT 之后，发起方发送：

IP UDP（4500，4500）〈4byte non-ESP〉HDR*，[CERT，]NAT-D，NAT-D，SIG_I

响应方进行与主模式相似的处理，如果成功则必须更新它的内部 IKE 端口。响应方必须使用 UDP（4500，*Y*）响应随后所有的 IKE 报文。

野蛮模式的例子如图 5 所示。

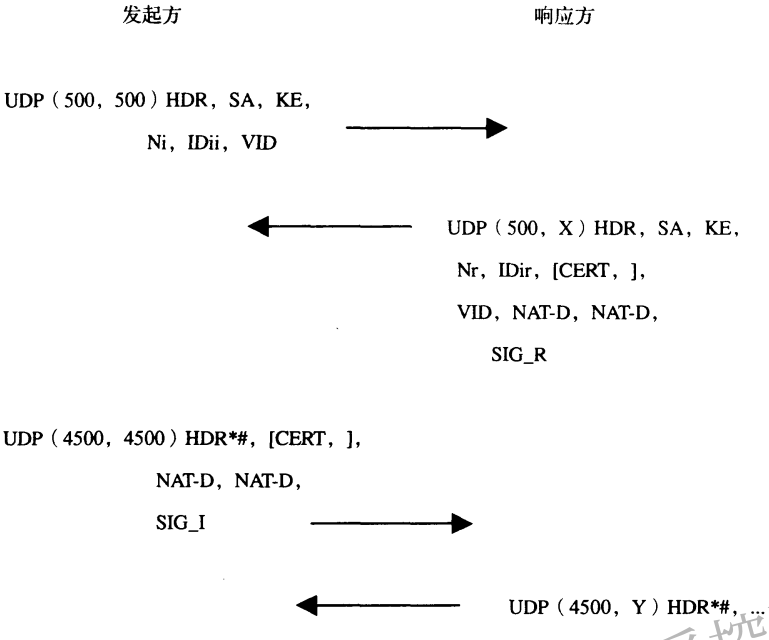


图 5 野蛮模式的例子

当浮动端口时，在主模式和野蛮模式的 ID 载荷中其端口值必须是 0。

对于响应方在 NAT 后面的情况，最普遍的情形是 NAT 只做简单的一对一地址转换。在这种情况下，发起方仍然要将源和目的端口都变为 4500，响应方也使用与上述相同的算法，但 *Y* 将等于 4500，这是因为在 NAT 中不发生端口转换。

另一种不同的情形是 NAT 需要对端口进行改变，此时涉及到对其所使用端口的外部发现机制。例如，如果响应方位于一个进行端口转换的 NAT 后面，即响应方使用的端口被 NAT 进行了转换，此时如果发起方要发起协商，就需要确定 NAT 使用了哪个端口来对应响应方，这通常是通过联系其他服务器来达到的。一旦发起方知道使用哪个端口（一般类似于 UDP（*Z*，4500）的形式）来穿越 NAT，它就使用该端口发起协商。这种情况类似于响应方进行密钥更新，不需要额外的改变。

在改变到新端口后启动第一个 keepalive 计时器，keepalive 消息不发送到端口 500 中。

6.2.3 快速模式

在阶段 1 完成后，协商双方都已明确在它们之间是否存在 NAT，而是否使用 NAT 穿越则由快速模式协商决定。在快速模式的 SA 载荷中协商 NAT 穿越的使用，协商双方能向对端传送 IPSec 报文的原始地址（传输模式情况下），从而使对端有可能在 NAT 转换之后对 TCP/IP 校验和修正。

6.2.3.1 NAT 穿越封装

通过增加两个新的封装模式来完成 NAT 穿越的协商。这些封装模式如下：

UDP-Encapsulated-Tunnel　　3

UDP-Encapsulated-Transport　　4

一般情况下，将 IPSec 普通的传输模式或隧道模式与 UDP 封装模式同时使用是没有意义的。

如果在协商双方之间存在 NAT，则普通的传输模式或隧道模式可能无法工作，而在该情况下应该采

用 UDP 封装模式。如果在协商双方之间不存在 NAT，则采用 UDP 封装模式只会浪费网络带宽，因此在该情况下不应该采用 UDP 封装模式。因此，发起方不应同时包括普通的传输模式或隧道模式与 UDP 封装模式。

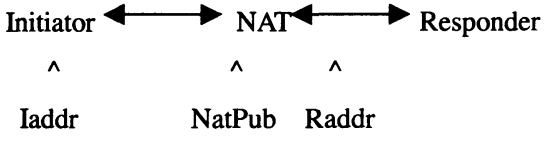
6.2.3.2 发送原始的源和目的地址

为了执行增量的 TCP 校验和修正，协商双方可能需要知道对端在构造报文时所使用的原始 IP 地址。对于发起方，其原始发起方地址定义为发起方的 IP 地址，而原始响应方地址定义为当前所知道的对端的 IP 地址。对于响应方，原始发起方地址定义为当前所知道的对端 IP 地址，原始响应方地址定义为响应方的 IP 地址。

使用 NAT-OA（NAT Original Address）载荷传送原始地址。

发起方 NAT-OA 载荷在前，响应方 NAT-OA 载荷在后。

例 1：



例 1 中，位于 NAT 后面的发起方与具有公共地址的响应方建立会话。发起方和响应方具有 IP 地址：Iaddr、Raddr。NAT 具有公共 IP 地址 NatPub。则发起方和响应方对应的 NAT-OA 载荷所包含的地址内容如下。

发起方：

NAT-OAi = Iaddr

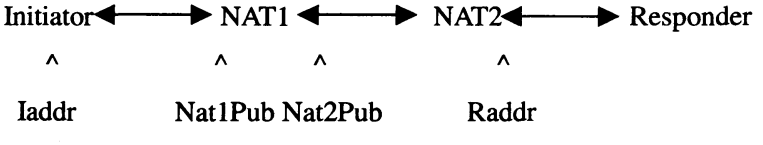
NAT-OAr = Raddr

响应方：

NAT-OAi = NATPub

NAT-OAr = Raddr

例 2：



例 2 中，响应方也位于 NAT 之后，由 NAT2 为响应方提供 Nat2Pub 的公共地址并转发所有到该地址的通信流至响应方。则发起方和响应方对应的 NAT-OA 载荷所包含的地址内容如下。

发起方：

NAT-OAi = Iaddr

NAT-OAr = Nat2Pub

响应方：

NAT-OAi = Nat1Pub

NAT-OAr = Raddr

在传输模式中协商双方必须传送原始发起方和响应方地址到对端。在隧道模式中则不应该传送原始地址到对端。

在快速模式的第一和第二条协商消息中发送 NAT-OA 载荷。如果发起方提议 UDP 封装传输模式，则必须发送 NAT-OA 载荷，而响应方只有在选定 UDP 封装传输模式后才必须发送 NAT-OA 载荷。也就是说，发起方可能发送了 NAT-OA 载荷，但向响应方提议了 UDP 封装传输和 UDP 封装隧道两种模式，这时响应方选择 UDP 封装隧道模式，不必向发起方发送 NAT-OA 载荷。

NAT-OA 载荷的类型为 16，其格式如图 6 所示。

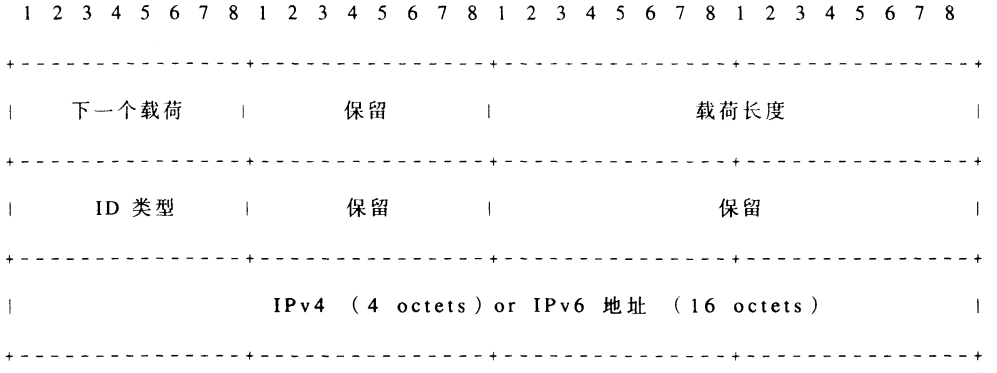


图 6　NAT-OA 载荷的格式

图 6 中，ID 类型字段定义于 RFC 2407，只允许 ID_IPV4_ADDR 和 ID_IPV6_ADDR 类型。ID 类型之后的保留字段必须为 0。

应用 NAT-OA 载荷的快速模式例子如图 7 所示。

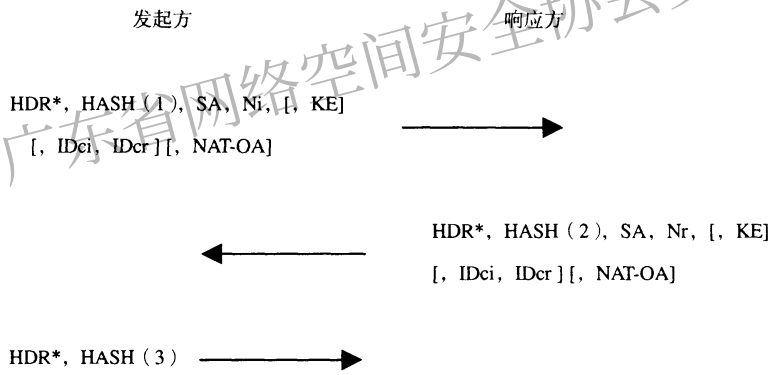


图 7　应用 NAT-OA 载荷的快速模式例子

6.2.4　初始化连接通告

初始化连接通告的源 IP 地址和端口对于在 NAT 后面的主机是没有意义的，所以其 IP 地址和端口不能用于确定删除某个 IKE/IPSec SA，此时应该使用对端传送的 ID 载荷来确定具体的 SA。当从对端收到初始化连接通告时，接收方应该删除所有具有相同 ID 载荷的 SA。

6.2.5　从到期的 NAT 映射中恢复

当 NAT 决定删除仍然存活的映射时（例如，keepalive 间隔过长，或者 NAT 设备重启），对于不在 NAT 后面的终端来说，为了能从这种情况中恢复映射，需使用从对端收到的最近一个有效报文来确定应该使用哪个 IP 地址和端口。而位于动态 NAT 后面的主机不能这样做，否则就会引入 DoS 攻击。由于对端（也就是不在 NAT 后面的终端）的 IP 地址和端口没有发生改变，对于该主机来说不需要这样做。

因为 keepalive 没有经过验证，不能使用 keepalive 达到恢复的目的，但任何已验证的 IKE 报文或 ESP 报文都能用于探测已变化的 IP 地址或端口。

6.3 UDP 封装

6.3.1 报文格式

6.3.1.1 UDP 封装 ESP 头部格式

UDP封装ESP头部的格式如图8所示。

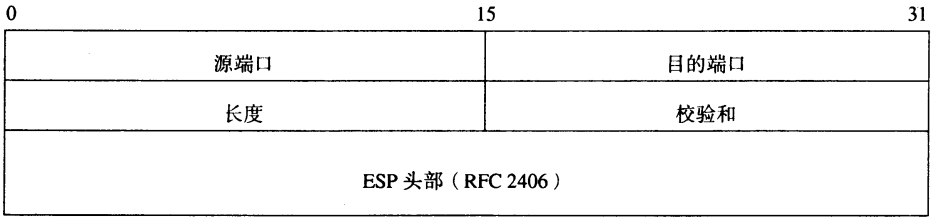


图 8 UDP 封装 ESP 头部的格式

UDP 头部是 RFC 768 中定义的标准头部，其中：

- 源端口和目的端口必须与浮动后的 IKE 通信流所使用的相同；
- 校验和字段应该为 0；
- 接收方的处理不能依赖于 UDP 校验和的值是否为 0，因为如果 UDP 校验和不为 0，接收方也应能正确处理。

在 ESP 头部中的 SPI 字段不能为 0。

6.3.1.2 端口为 4500 的 IKE 头部格式

端口为4500的IKE头部格式如图9所示。

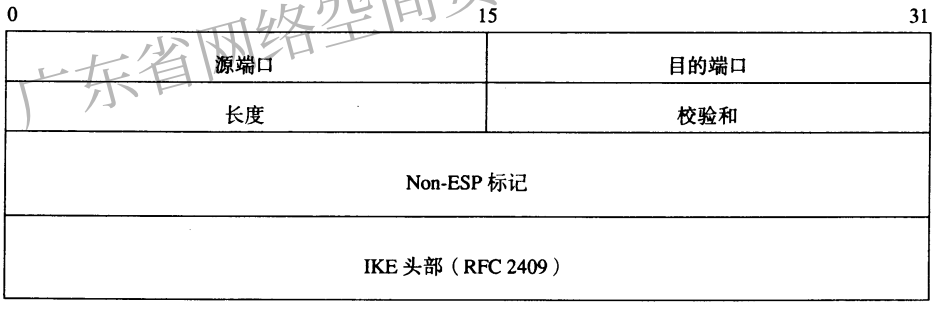


图 9 端口为 4500 的 IKE 头部格式

UDP 头是 RFC 768 中定义的标准头部。本标准对 IKE 报文的校验和处理不做新的要求。

Non-ESP 标记是置 0 的 4 字节字串，其位置对应于 ESP 报文中的 SPI 字段。

6.3.1.3 NAT-keepalive 报文格式

NAT-keepalive报文格式如图10所示。

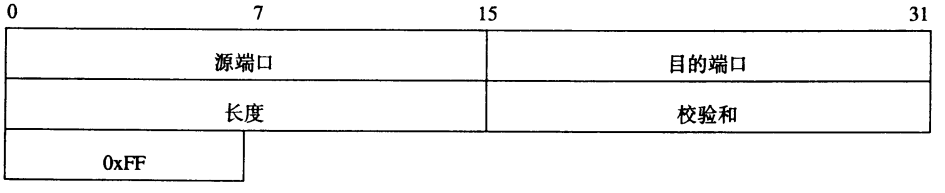


图 10 NAT-keepalive 报文格式

UDP 头部是 RFC 768 中定义的标准头部，其中：

- 源端口和目的端口必须与 UDP-ESP 封装中的一样；
- 校验和应该为 0；

● 接收方的处理不能依赖于 UDP 校验和的值是否为 0，因为如果 UDP 校验和不为 0，接收方也应能正确处理。

发送方应该使用一个字节长的载荷，内容为 0xFF。

接收方应该忽略接收到的 NAT-keepalive 报文。

6.3.2 封装与解封处理

6.3.2.1 辅助处理

（1）隧道模式解封装 NAT 处理

当使用隧道模式传送报文时，内部 IP 头中会包含不适合当前网络的地址。下面定义将其转换成适合当前网络地址的处理方法。

根据本地策略必须完成下列任务之一。

● 如果在策略中已为对端的封装报文定义了一个有效的源 IP 地址空间，则根据策略检查在内部报文中的 IP 源地址是否属于有效范围。

● 如果已经为远程对端分配了一个地址，检查内部报文中的 IP 源地址是否与该地址一致。

● 对报文执行 NAT 转换，使其适合在本地网络中传输。

（2）传输模式解封装 NAT 处理

当使用传输模式传送报文时，如果在传输中 IP 头部发生变化，TCP 或 UDP 头部中将包含错误的校验和。下面定义修正这些校验和的处理方法。

根据本地策略必须完成以下任务之一。

● 如果在 ESP 头部之后的协议头部是一个 TCP/UDP 头，并且已经获得对端的真实源/目的 IP 地址，则增量计算 TCP/UDP 校验和：

— 从校验和中减去接收包的 IP 源地址；

— 在校验和中增加通过 IKE 获得的真实 IP 源地址（从 NAT-OA 中获得）；

— 从校验和中减去接收包的 IP 目的地址；

— 在校验和中增加通过 IKE 获得的真实 IP 目的地址（从 NAT-OA 中获得）。

注：如果接收到的地址和真实地址是相同的，则取消相关操作。

● 如果在 ESP 头后面的协议头是 TCP/UDP 头，重新计算在 TCP/UDP 头中的校验和字段。

● 如果在 ESP 头后面的协议头部是 UDP 头，将 UDP 头中的校验和字段置 0。如果在 ESP 头后面的协议头是 TCP 头，并且存在一个选项，该选项用于指示协议栈不用检查 TCP 效验和，则可以使用该选项，仅在传输模式中且对报文进行了完整性保护时应使用这种情况。隧道模式的 TCP 校验和必须进行验证。因为校验和由发送方产生并由接收方验证，该校验和是对整个 IPSec 处理的报文的完整性检验。

另外，在实现中可以对被 NAT 破坏的所包含的协议进行修正。

6.3.2.2 传输模式 ESP 封装

传输模式ESP封装如图11所示。

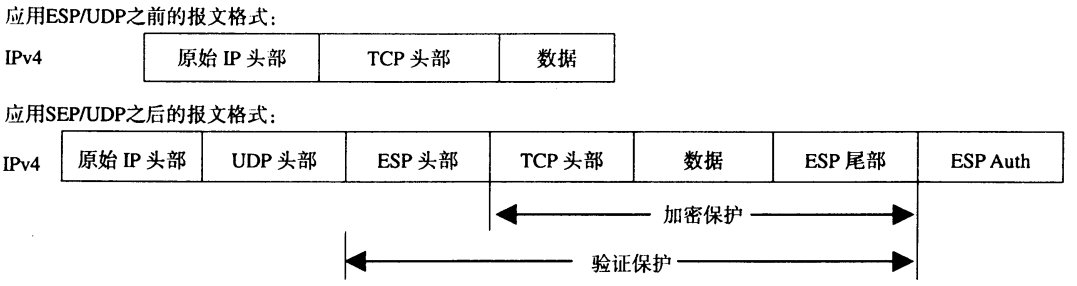


图 11　传输模式 ESP 封装

（1）普通的 ESP 封装处理；

（2）插入一个适当格式的 UDP 头部；

（3）编辑 IP 头中的总长域、协议域以及校验和字段，使之与所得报文相匹配。

6.3.2.3　传输模式 ESP 解封装

（1）从报文中删除 UDP 头；

（2）编辑 IP 头中的总长域、协议域以及校验和域，使之与所得的报文相匹配；

（3）应用普通的 ESP 解封装处理过程；

（4）应用传输模式解封装 NAT 处理过程。

6.3.2.4　隧道模式 ESP 封装

隧道模式ESP封装如图12所示。

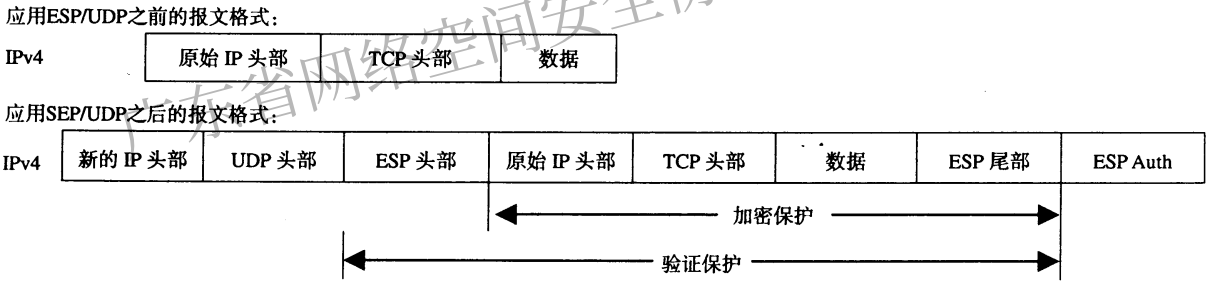


图 12　隧道模式 ESP 封装

（1）普通的 ESP 封装处理；

（2）插入一个适当格式的 UDP 头部；

（3）编辑 IP 头中的总长字段、协议字段以及校验和字段，使之与所得的报文相匹配。

6.3.2.5　隧道模式 ESP 解封装

（1）从报文中删除 UDP 头；

（2）编辑 IP 头中的总长字段、协议字段以及校验和字段，使之与所得的报文相匹配；

（3）应用普通的 ESP 解封装处理过程；

（4）应用隧道模式解封装 NAT 处理过程。

6.3.3　NAT keepalive 处理

发送 NAT-keepalive 报文的惟一目的是保持 NAT 映射处于激活状态。NAT-keepalive 报文不能用于探测连接是否存活。

如果在双方之间存在一个或多个阶段 1 或阶段 2 的 SA，或者这样的 SA 在 *N* 分钟之前曾经存在过（*N* 是本地可配置参数，缺省为 5），则其中一端可以发送 NAT-keepalive 报文。

如果探测到需要发送 keepalive 报文，且在 *M* 秒内没有其他的报文发送到对端（*M* 是本地可配置参数，缺省为 20），此时应该发送一个 NAT-keepalive 报文。

7 穿越 NAT 对 IPSec 的影响

7.1 安全考虑

7.1.1 IPSec－NAT 兼容性的安全考虑

因为 IPSec AH 不能穿越 NAT，只能使用空加密的 ESP 来替代 AH，但空加密的 ESP 不能提供和 AH 完全一样的安全属性。例如，在 AH 中可以排除对于 IP 源路由的安全风险，而在使用空加密的 ESP 中却无法杜绝。

另外，因为使用任何加密变换的 ESP 都不提供防止源地址欺骗的保护，因此必须执行一些源 IP 地址的检验。在 IPSec_{esp，ah}_input 中完成对源 IP 地址的一般性防欺骗检查，这能保证报文是从与最初的 IKE 主模式和快速模式 SA 中所声称的相同地址发送的。当接收方主机在 NAT 后面时，源地址的检测对于单播会话意义不大，然而对于在隧道模式的单播会话中这种检测可以防止欺骗攻击。

让我们考虑两个主机 A 和 C，都在 NAT 设备后面，并都用 IPSec 隧道模式与 B 协商安全联盟。主机 A 和 C 可能有不同的权限，假设主机 A 是以职员身份访问公司内网，而 C 只是以承包方身份访问某个特定的 Web 站点。如果主机 C 作为源方发送一个伪造 A 的 IP 地址的隧道模式包，而作为发起方 C 并不具有与 A 相同的权限。如果接收方只执行身份验证与完整性检验，而不进行防欺骗检验（确定发起方 IP 地址与 SPI 相对应），则 C 可能就被允许访问那些它本没有权限访问的网络资源。因此，IPSec－NAT 兼容性解决方案必须提供一定程度的防欺骗保护。

7.1.2 IKE 协商的安全考虑

IKE 协商应考虑以下安全问题。

（1）IKE 探测对外暴露了协商双方是否支持 NAT 穿越，这不会引入安全问题。

（2）一旦存在 NAT，则失去基于 IP 地址的验证机制。对位于 NAT 后面的所有主机，如果没有组共享密钥，它们就不能在主模式中使用预共享密钥验证方式。而使用组共享密钥是具有巨大安全风险的，不推荐使用组共享密钥。

（3）因为内部地址空间只有 32 位，且通常很少，所以有可能使攻击者通过尝试所有可能的 IP 地址和尝试找出匹配的散列值而发现在 NAT 后面的内部地址。端口号通常固定为 500，并且 Cookie 值可以从报文中分解得出，从而使散列运算的空间降至 2^{32}。如果对私有地址空间进行改进推测，这时需要找出内部 IP 地址的散列运算空间降至 $2^{24} + 2\times2^{16}$。

（4）在主模式和野蛮模式中，NAT-D 载荷和 Verdor ID 载荷都没有经过验证。攻击者能够删除、修改和增加这些载荷。通过删除或增加 NAT-D 载荷，攻击者能够发起 DoS 攻击。通过修改 NAT-D 载荷，攻击者能造成协商双方都使用 UDP 封装模式而不使用隧道或传输模式，从而造成带宽的浪费。

（5）因为在快速模式中发送原始源地址，从而向对端暴露了在 NAT 之后的内部 IP 地址。由于需要对对端的身份验证，且只在传输模式中传送原始源地址，因此不存在安全问题。

（6）当攻击者能监听网络中所有通信流、能修改报文顺序且能在已发现的报文之前注入新的报文时，对每个有效的验证报文更新IKE SA报文和ESP UDP封装报文的IP地址和端口，则会造成DoS攻击。攻击者能够从位于NAT后面的主机截取已验证的报文，修改报文的UDP源方和目的方的IP地址与端口，并在真正的报文到达之前发送给对端。不在NAT后面的主机接收到伪造报文后将根据伪造报文更新它的IP地址

和端口映射，并将随后的通信流发送至错误的主机或端口。这种情况在攻击者停止攻击并接收到第一个正确报文后才能得以修正。实现中应该每次审计映射的改变，一般情况下它不应经常发生。

7.1.3 UDP 封装的安全考虑

（1）DoS

在一些系统中 ESP UDP 可能引发 DoS 攻击，特别是使用普通操作系统的 UDP 功能。因此推荐不打开普通的 UDP 端口。

（2）隧道模式冲突

隧道模式冲突如图 13 所示。实现者需要注意影响到隧道模式使用的一个问题：远程对端会协商在网关中重叠的条目。

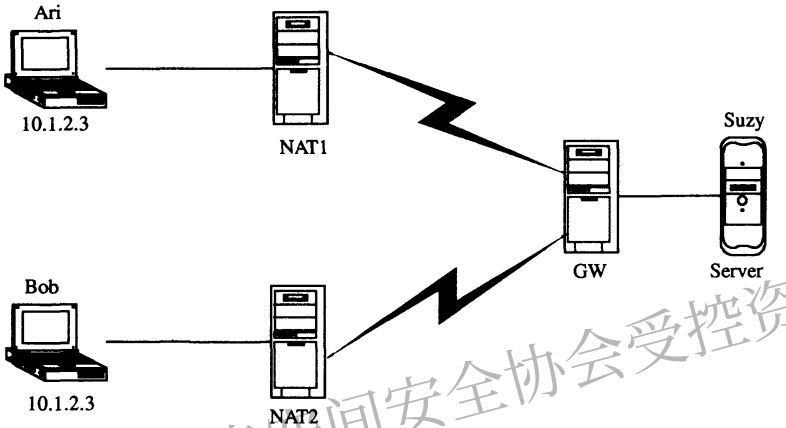


图 13 隧道模式冲突

如图 13 所示，GW 将看到两个目的地址都是 10.1.2.3 的 SA，从而不知道从 suzy 来的报文该通过哪一个 SA 发送。实现必须设计出防止该现象发生的方法。

推荐的方法是，在转发报文至 S 之前，GW 使用 DHCP over IPSec 协议为 Ari 和 Bob 分配本地惟一的 IP 地址，或者使用 NAT 将 Ari 和 Bob 的源 IP 地址改变为本地惟一的 IP 地址。

（3）传输模式冲突

在传输模式中，当同一个 NAT 后面有两个客户端 Ari 和 Bob 与同一服务器建立安全会话时，也会发生类似的问题。传输模式冲突如图 14 所示。

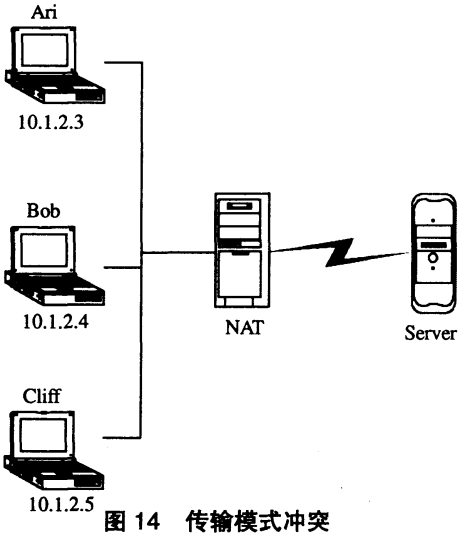


图 14 传输模式冲突

Cliff 想与相同服务器建立普通会话。

现在，在服务器上的 SA 是：

至 Ari：S to NAT，<traffic desc1>，UDP encap <4500，y>

至 Bob：S to NAT，<traffic desc2>，UDP encap <4500，z>

Cliff 是明文传输，因此没有针对它的 SA。

<traffic desc1>是协议与端口信息。UDP 封装端口是在 UDP 封装 ESP 格式中使用的端口。*Y*、*Z* 是由 NAT 在 IKE 协商时动态分配的端口。从 Ari 发出的 IKE 通信流使用端口 UDP<4500，4500>，它到达服务器时是 UDP<Y，4500>，其中 *Y* 是动态分配的端口。

如果<traffic desc1>与<traffic desc2>重叠，那么只使用简单的过滤查找不足以确定通过哪个 SA 来发送报文。实现必须通过禁止有冲突的连接或使用其他方法来防止这种情况的发生。

假设现在 Cliff 想与服务器以明文方式建立连接，因为服务器为了得到<traffic desc>已经存在从 S 到 NAT 外部地址的策略，这会导致很难进行配置。对不重叠的通信流描述，这是可能做到的，如以下的服务器策略：

至 Ari：S to NAT，All UDP，secure

至 Bob：S to NAT，All TCP，secure

至 Cliff：S to NAT，ALL ICMP，clear text

该策略也允许 Ari 和 Bob 发送明文 ICMP 报文至服务器。

由于服务器看到的所有在同一 NAT 后面的客户端具有相同的 IP 地址，因此从原则上就不能对相同的通信流描述应用不同的策略。如下的服务器策略配置就存在问题：

S to NAT，TCP，secure （for Ari and Bob）

S to NAT，TCP，clear （for Cliff）

如果误操作的 Bob 发送了明文数据，服务器将无法实施策略，这时无法将 Bob 发送的明文数据与 Cliff 发送的明文数据区分开来。因此不能为 NAT 后面的某些客户端保证通信安全，也不允许同一 NAT 后面的另一些客户端使用明文传输。如果服务器的安全策略允许采用尽最大努力的安全，当从 NAT 后面的客户端发起安全连接时，客户端能建立起连接；如果客户端发送的是明文，服务器也同样接受。

所以，如果要保证安全，服务器必须不允许出现上述问题，而如果只要求尽最大努力的安全保护，则可以使用上述方案。

7.2 IANA 考虑

本标准包含两个新的 IANA 注册值，并将注册端口修改为 4500，同时还定义了两个新的 IKE 载荷类型，这两种类型在 IANA 中没有注册。

新的封装模式为：

Name	Value	Reference
----	-----	---------
UDP-Encapsulated-Tunnel	3	[RFC XXXX]
UDP-Encapsulated-Transport	4	[RFC XXXX]

注册的端口号为：

Keyword	Decimal	Description	Reference
---	---	---	---
IPSec-nat-t	4500/tcp	IPSec NAT-Traversal	[RFC XXXX]
IPSec-nat-t	4500/udp	IPSec NAT-Traversal	[RFC XXXX]

新的 IKE 载荷号为（没有相关的 IANA 注册）：

NAT-D	15	NAT Discovery Payload
NAT-OA	16	NAT Original Address Payload

附 录 A
（资料性附录）
IPSec 隧道模式

在某些很有限的情况下，IPSec 隧道模式可能成功穿越 NA（P）T，而不需要采用上述地解决方法。但是为使隧道模式得以成功穿越 NA（P）T 会受到很多限制，这些限制包括。

（1）IPSec ESP。IPSec ESP 隧道模式在消息完整性检测中不包含外部 IP 头，这样才能避免由于 NA（P）T 转换所造成的验证数据失效情况。IPSec 隧道模式不需要关心校验和的有效性。

（2）无地址确认。当前几乎所有的 IPSec 隧道模式实现中都不执行源地址确认，这样可以避免对 IKE 身份标识与源地址进行检测时出现的不兼容性，但这又同时引入了安全隐患。

（3）“任意到任意”的 SPD 条目。IPSec 隧道模式客户端能够协商“任意到任意”的 SPD，这样也可以避免地址转换的影响，但却明显地阻碍了 SPD 可对隧道通信流进行过滤的作用。

（4）单客户端操作。如果在 NAT 后面是单个客户端，则不存在重叠 SPD 的风险。因为 NAT 不必在多个客户端之间进行判断，因此不存在密钥重生成时的错误转换风险，对接收的数据流也不存在错误的 SPI 或 Cookie 分用情况。

（5）无分片。当使用证书进行认证时 IKE 可能会出现分片。例如，可能出现在使用证书链时，或者甚至可能出现在只使用单个证书时，只要密钥大小或其他认证字段的大小足够大。但当认证使用预共享密钥时很少出现分片。

（6）主动会话。几乎所有的 VPN 会话在其生命期中通常都要维护正在进行的通信流，因此很少出现因会话停止而造成删除 UDP 端口映射的现象。

附 录 B
（资料性附录）
RSIP

RSIP是位于内网的主机与外界发生联系时发布特定IP 地址所采用的一种协议。当采用RSIP协议时，IPSec很容易解决穿越问题。RSIP包含了IPSec穿越的机制。通过使用主机对网关的通信，RSIP既解决了SPD重叠问题，也解决了SPI分用问题，因此它既适用于家庭网络方案也适用于企业网络方案。RSIP使在NAT后面的主机可以共享网关中的外部IP地址，从而使RSIP可以兼容在协议报文中嵌套了IP地址的协议。

通过对IKE和IPSec报文进行隧道封装，RSIP可以避免对IKE和IPSec协议的更改，而将其主要的改变集中到主机的IKE和IPSec实现中。因此，RSIP可以兼容IPSec中所有已存在的协议（AH/ESP）和模式（传输模式/隧道模式）。

为了处理在IKE密钥重生成期间的分用问题，RSIP要求浮动IKE源端口，因此不能保证与现存IPSec实现的互操作。

一个启用RSIP的主机为了与另一个主机建立IPSec SA，必须有相对应的启用RSIP的网关，因此RSIP并不满足IPSec－NAT兼容性解决方案的部署需求。因为RSIP只需要改变客户端和路由器而不必改变服务器，因此在部署上其难度低于IPv6。但对于开发商实现RSIP需要很大一部分实现IPv6所需的资源。因此RSIP只是在一个长期的时间上解决了“过渡性”的问题，因此并不是适用的解决方案。

附 录 C
（资料性附录）
6to4

使用6to4也可以较好地实现IPSec－NAT穿越，它可以形成一种IPSec－NAT穿越方案的基础。在该方案中NAT为IPv6主机提供了一个由NAT外部IPv4地址产生的IPv6前缀，并封装IPv6报文传输给其他的6to4主机或6to4中继设备，因此采用IPSec的IPv6主机就可以自由地在IPv6或6to4的网络域中与其他主机进行通信。

在只有单个NA（P）T分隔客户端和VPN网关的情况下，6to4确实是一种优秀而健壮的解决方案，但它并不是在任何情况下都能使用。这是因为6to4必须为NA（P）T分配一个可路由的IPv4地址，那么在客户端和VPN网关之间如果存在多个NA（P）T设备，6to4就显得无能为力了。例如，在一个NA（P）T设备的外部接口中分配了私有地址，这样在该NA（P）T后面的主机就不能通过6to4来获得一个IPv6前缀。

虽然6to4对于已支持IPv6的主机来说只需要很少的额外支持，但却需要改变NAT以支持6to4协议。因此，6to4并不适合在短期内部署。

中华人民共和国
通信行业标准
IP 安全协议（IPSec）穿越网络地址翻译
（NAT）技术要求
YD/T 1468-2006
*
人民邮电出版社出版发行
北京市崇文区夕照寺街 14 号 A 座
邮政编码：100061
北京地质印刷厂印刷

*
开本：880 x 1230　1/16　　2006 年 9 月第 1 版
印张：2.0　　2006 年 9 月北京第 1 次印刷
字数：52 千字
ISBN 7 - 115 - 1280/06 - 101
定价：15.00 元
本书如有印装质量问题，请与本社联系　电话：(010)67114922