第34卷 第22期 计 算 机 工 程 2008年11月
Vol.34 No.22 Computer Engineering November 2008
·网络与通信· 文章编号：1000—3428(2008)22—0148—02 文献标识码：A 中图分类号：TP393.08

增强的 NAT-PT 和 IPSec 兼容解决方案

张志龙，杜学绘，钱雁斌
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：分析 IPv4/IPv6 过渡时期 NAT-PT 和 IPSec 协议的兼容性解决方案，并基于此提出一种增强的 IPSec 分段保护方案，通过对 IKE 协议的适当改进增加了发起方对 NAT-PT 转换网关的发现和自动处理机制，提高了 NAT-PT 转换网关的透明性。性能分析显示该方案具有较好的安全性和适应性，便于过渡网络安全策略的实施。

关键词：协议转换；分段协商；转换网关

Enhanced Compatibility Solution Between NAT-PT and IPSec

ZHANG Zhi-long, DU Xue-hui, QIAN Yan-bin
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 This paper analyzes the solution about the compatibility between IPSec and Network Address Translation-Protocol Translation(NAT-PT) in IPv4/IPv6 interim, and puts forward an enhanced IPSec application solution in segments. It increases the discovery and automatic mechanism through the improvement to IKE protocol, and improves the transparence of the NAT-PT translation gateway. The performance analysis shows that it is more secure and flexible, and is convenient for the implement of security strategy in transition network.

【Key words】 Protocol Translation(PT); negotiation in segments; translation gateway

1 概述

IPv4 向IPv6 过渡时期网络的安全性已经成为下一代互联网发展亟需解决的问题之一。过渡时期IPv4, IPv6 共存网络的安全问题不仅包括IPv4 和IPv6 协议本身的安全问题，而且还包括IPv4 向IPv6 过渡技术所带来的安全影响[1]。

NAT-PT[2]作为边缘网络过渡的主要解决方案，实现了IPv4 网络与IPv6 网络的直接互通。然而NAT-PT的安全性也成为制约其应用的重要因素[3]。IPv6 协议本身内嵌IPSec协议，因此使用IPSec协议保护网络安全相对方便合理。然而在NAT-PT环境下直接应用IPSec将由于NAT-PT和IPSec协议的不兼容而失败。因此必须采用适当的方案解决两者的共存问题，而且该方案在保证网络安全的同时要具有较强的适应性，以便于实施。

2 存在的问题及现有解决方案分析

2.1 兼容性问题

NAT-PT 中地址映射使用的是 NAT，因此两者同 IPSec 的兼容性问题类似。然而 NAT 实现的是相同 IP 协议数据报的翻译，NAT-PT 实现的则是不同 IP 协议数据报的翻译，这种不对称性使得 NAT-PT 同 IPSec 的兼容性问题更加复杂。

IPSec 协议主要由 AH 协议、ESP 协议以及负责密钥管理的 IKE 协议组成。NAT-PT 转换网关对数据报进行 IPv4/IPv6 地址映射和报头翻译，导致应用 IPSec 协议时出现如下问题：

(1)AH 协议提供对整个数据报的完整性保护，通常情况以 IP 地址作为标识，NAT-PT 对报文的更改使得 AH 中 ICV 值认证失效。

(2)ESP 协议实现了对整个 IP 层数据的加密保护，但同时也阻止了传输模式下 NAT-PT 处理之后 TCP/UDP 校验和的重新计算，导致报文在传输层被丢弃。

(3)IKE 用于动态建立和维护 SA。以 IP 地址或 Cookie 作为身份认证标识时，NAT-PT 转换网关需要对 HASH-I, HASH-R 中的 ID 进行更改，而该消息被加密，从而导致 IKE 协商失败。

2.2 现有解决方案分析

在 NAT-PT 网络环境下，转换网关隔开的是 2 个不同协议的网络，这一特性使得常见的 NAT 和 IPSec 兼容解决方案如 UDP 穿越、RSIP 方案不再适用。IP 协议版本的不同使得数据报在通过 UDP 封装穿越 NAT-PT 转换网关之后无法被理解而被丢弃，RSIP 方案花费巨大也不宜采用。

现有解决 NAT-PT 和 IPSec 兼容问题的方案主要有：

(1)分段IPSec协议保护[4]，即在转换网关和IPv6 节点、IPv4 节点之间分别建立IPSec隧道进行保护。IPSec保护的路径不包括转换网关，不需考虑AH和ESP同NAT-PT的兼容性，只适用于IPSec的隧道模式。

(2)通过对IKE协议进行改进，在IKE协商过程中将翻译信息发送到发起方，发起方在发送数据包之前提前生成接收方验证正确的ICV值及TCP/UDP检验和，消除了转换网关对数据报的转换而导致的ICV值及TCP/UDP校验和的计算问题[5]。该方法适用于IPSec的AH或ESP传输模式。

方案(1)需要在 NAT-PT 转换网关和 IPv6、IPv4 节点之间手工配置 IPSec 隧道，不适合于较大规模网络之间的安全通信。方案(2)的前提是 IPSec 发起方负责产生响应方验证正确的 IPSec 数据包。协商过程中对 IKE 协议进行了改进，发起方需要作较大改动。

本文提出的方案在(1)的基础上增加了 NAT-PT 转换网关发现和处理机制，实现了分段 IPSec 保护的自动实施，提高

作者简介：张志龙(1982－)，男，硕士研究生，主研方向：网络安全，IPv4/IPv6 过渡技术；杜学绘，副教授、博士；钱雁斌，博士研究生
收稿日期：2008-01-27 **E-mail：**zzl321_long@126.com

了其适应性。

3 增强的分段协商方案

3.1 应用场景

该方案适用于所有类型的 NAT-PT。本文重点研究基本的双向 NAT-PT，由此可以扩展到所有类型的 NAT-PT。研究的过渡场景如图 1 所示，IPv6 网络中的纯 IPv6 主机和 IPv4 网络中的纯 IPv4 主机借助 NAT-PT 转换网关中的 DNS-ALG 进行双向访问。

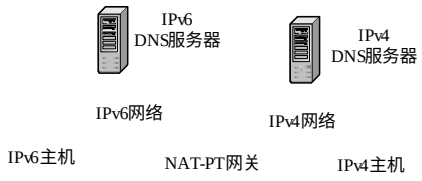

图 1 NAT-PT 过渡场景

3.2 NAT-PT 转换网关发现和处理机制

在 NAT-PT 网络环境下，通信对端手工配置 IPSec 隧道之前，首先要检测通信路径中是否存在 NAT-PT 转换网关。若通信路径中存在此类设备，则双方进行 IKE SA 协商时会因为转换网关对地址等报文信息的改变而失败。通过对 IKE 协议进行适当改进，使得通信对端在首次 IKE 协商过程中将转换网关的信息发送给协商发起方，然后在协商失败后由发起方和转换网关重新发起 IKE 协商，从而建立了分段 IKE SA。

在预共享密钥认证的主模式下，通信对端要建立 IPSec 隧道，首先进行 IKE SA 协商。NAT-PT 转换网关若检测到有穿越转换网关的端口号为 500 的 UDP 数据包，首先在地址映射表项中添加相应的标识，表示通信对端欲建立安全连接。然后产生包含 NAT-PT 转换网关信息的 IP GWI 载荷消息，等待响应方的 IKE 响应报文，将该消息附加在报文之后发送给发起方。

这里定义了包含转换网关地址信息的 IP GWI 载荷消息，使用 IANA 中未使用的 150 标识。图 2 显示了定义的 IP GWI 消息格式，主要包括网关的 IPv4 地址和 IPv6 地址 2 个字段。

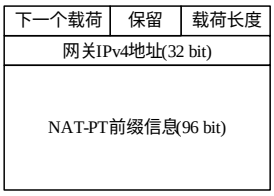

图 2 IP GWI 消息格式

3.3 分段协商

首次 IKE 协商失败后，由通信发起方和转换网关分别向转换网关和响应方再次发起 IKE 协商请求，协商过程同正常的 IKE 协商一样，协商结束即在转换网关和发起方、响应方之间分别建立了 IKE SA。之后，在转换网关同发起方、响应方之间分别建立了 IPSec 安全隧道，通信对端的数据包在 2 段安全隧道中传输。

3.4 分段 IPSec 隧道建立全过程

假设 IPv6 主机的地址为 A，IPv4 主机的地址为 B，NAT-PT 转换网关的 IPv4 地址为 G，网关为 IPv6 主机 A 分配的 IPv4 临时地址为 C，IPv6 地址前缀为 P。由于 DNS-ALG 的存在，IPv4 主机向 IPv6 主机发起连接的情况同 IPv6 主机向 IPv4 主机发起连接的情况类似，因此本文仅分析 IPv6 主机向 IPv4 主机发起连接的情况。

(1)IPv6 主机要向 IPv4 主机发起连接，通过 DNS 查询之后，网关采用地址欺骗的方式返回 IPv4 主机的地址 P::B。

(2)分段 IKE 协商过程

IPv6 主机取得 IPv4 主机的 IP 地址之后，向 IPv4 主机发起 IKE 协商。图 3 显示了 IPv6 主机、NAT-PT 网关和 IPv4 主机之间包括发送 IP GWI 消息的整个 IKE 协商过程。

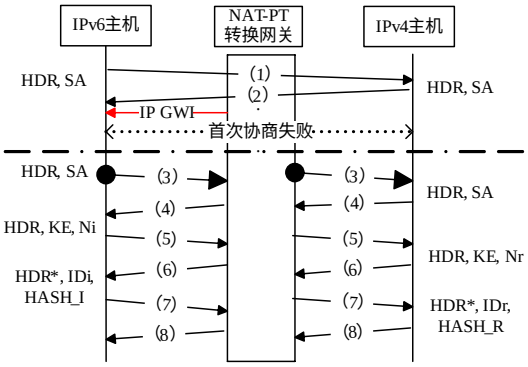

图 3 分段 IKE 协商全过程

协商分为 2 个阶段：1)网关发现和分段协商准备阶段。NAT-PT 网关从 IPv6 主机收到端口号为 500 的 UDP 数据包，记录响应方 IP 地址，并将消息转发 IPv4 主机，然后等待接收端的响应。IPv4 主机响应该请求，返回的消息经过 NAT-PT 转换网关时网关将包含网关 IP 地址的 IP GWI 消息附加其后，然后发送给 IPv6 主机。2)分段协商阶段，由 IPv6 主机和 NAT-PT 网关分别发起 IKE 协商请求，在 NAT-PT 网关和 IPv6 主机、IPv4 主机之间分别建立了 IKE SA。该阶段 IKE 协商过程(3)~(8)同原来一样。

(3)IKE SA 协商成功之后，在 NAT-PT 网关和 IPv6 主机、IPv4 主机之间分别建立了安全隧道保护。图 4 显示了 IPv6 主机和 IPv4 主机在建立的 AH 隧道中传输数据包的过程。

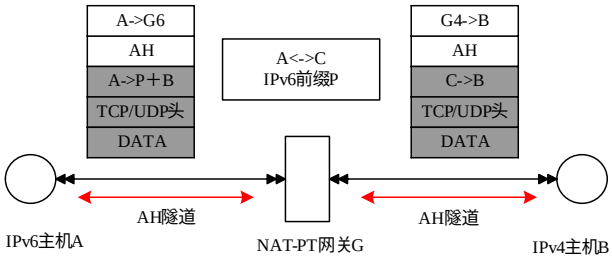

图 4 AH 隧道模式下 IPv4 和 IPv6 主机之间安全通信图

4 性能分析

本文提出的增强 IPSec 和 NAT-PT 兼容性解决方案，在分段 IPSec 协商的基础上增加了转换网关的发现和处理机制，提高方案实施的透明性，方便用户的使用。

在安全性方面，该方案侧重 IKE 协议的改进，增加了 IP GWI 载荷消息，在转换网关的地址映射表中增加指示通信对端有无使用安全隧道保护的安全标识。IP GWI 载荷消息附加在 IKE 协商报文之后传送，协议的安全性没有受到影响。在 IPv6 主机和 NAT-PT 转换网关、IPv4 主机和 NAT-PT 转换网关之间分别建立安全隧道，避免了数据包在通信中被恶意篡改及受到重放攻击，但是在转换网关节点处的安全性不能受

(下转第 152 页)