IP 隧道网络安全性策略的研究与实现

Research and Implementation of IP Tunnel Network Security Strategy

甘卫民

Weimin Gan

广州软件学院　中国·广东 广州 510980

Software Engineering Institute of Guangzhou, Guangzhou, Guangdong, 510980, China

摘　要：IP 隧道安全通信是靠互联网安全协议技术支撑。隧道安全协议主要是通过对 IP 协议分组进行加密与认证，在网络层的通信双方通过加密认证、数据源认证、完整性校验认证来保证分组传输的完整性、机密性和防重放性。在企业网络管理中，为了实现总部与分支的安全通信，通常可借用 IP 安全协议的虚拟网络技术建立安全通道。论文使用创建安全策略研究来保证 IP 隧道网络通信的安全可靠。

Abstract: IP tunnel security communication is supported by internet security protocol technology. The tunnel security protocol mainly encrypts and authenticates the IP protocol packets, and the two communicating parties at the network layer ensure the integrity, confidentiality and anti-replay of packet transmission through encryption authentication, data source authentication, and integrity verification authentication. In enterprise network management, in order to realize the secure communication between the headquarters and the branches, the virtual network technology of the IP security protocol can usually be used to establish a secure channel. This paper uses the research of creating security policy to ensure the security and reliability of IP tunnel network communication.

关键词：IP 隧道安全协议；虚拟专用网络；安全策略

Keywords: IP tunnel security protocol; virtual private network; security policy

基金项目：广州软件学院质量工程项目资助（项目编号：JPJC202102）。

DOI: 10.12346/csai.v1i1.6882

1 引言

随着互联网企业网络大规模的发展，网络安全技术问题越来越得到重视，解决网络安全技术的安全策略研究及实现是最棘手的问题，在传统网络中，严重缺乏机制的安全认证与保密认知。在企业网络管理中，为了实现总部与分支安全通信，IP 隧道安全策略的引入，使传统网络数据通信得到安全保障，在发送端可以用加密技术，用密文的形式对数据进行加密保护进行通信，在接收端使用解密技术使数据进行检测认证，这样能确保数据报文在传输过程中得到安全，不会篡改，保证数据完整性。引用网络安全策略不仅能使通信数据得到安全，也可防止不明用户通过重复发送捕获的数据包进行恶意攻击 [1]。

2 IP 隧道安全应用

在企业网络管理中，为了某些私有数据在公网传输时的安全，确保数据的机密性与完整性，网络管理员通常通过 IPSec VPN 技术来实现。技术员通常会在企业网络总部的边缘路由器和分支机构路由器间创建 IP 网络安全隧道，在隧道内通过部署安全策略技术来解决网络通信安全，以及控制网络安全通信的数据流量 [2]。

3 IP 隧道安全架构

IP 隧道安全架构主要通过 IP 安全协议的 VPN 架构，即 IPSec VPN，体系结构如图 1 所示。IPSec 协议主要包含三种协议，分别是 AH（Authentication Header）认证协议、

【作者简介】甘卫民（1979-），男，中国江西吉安人，硕士，高级工程师，从事云计算、雾计算、云服务研究。

ESP（Encapsulating Security Payload）加密协议、IKE（Internet Key Exchange）网络密钥交换协议。AH 协议主要用来进行数据源验证、数据完整性的校验、防报文重放等功能。ESP 协议主要用来对 IP 报文数据进行加密功能。这样 IP 数据报文在传送的过程能够保证在一个安全的网络中通信。IKE 协议主要用于自动协商 AH 和 ESP 所使用的密码算法，建立和维护 SA 等服务。

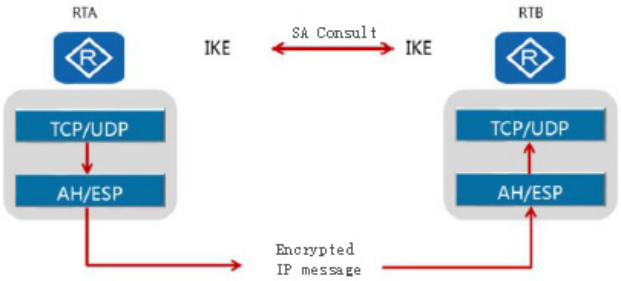


图 1 IPSec VPN 体系结构

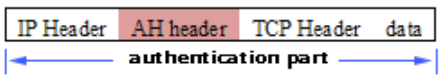
4 IPSec 协议封装模式

IPSec 协议主要提供两种封装模式：传输模式（Transport）和隧道模式（Tunnel）[3]。

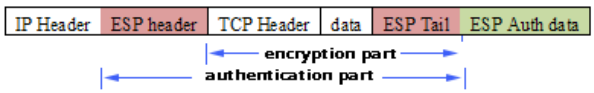
4.1 传输模式

在传输模式下，AH 或 ESP 报头位于 IP 报头和传输层报头之间。在 AH、ESP 处理前后 IP 头部保持不变，主要用于 End-to-End 的应用场景，也就是只能适合 PC 到 PC 场景。

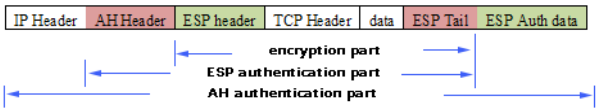
AH：



ESP：



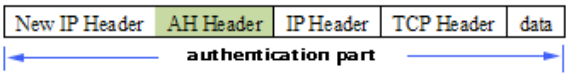
AH-ESP：



4.2 隧道模式

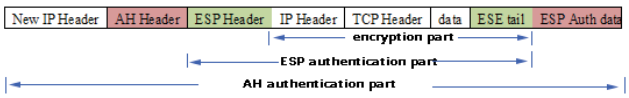
在隧道模式下，IPSec 会另外生成一个新的 IP 报头封闭在 AH 或 ESP 报头之前。则在 AH、ESP 处理之后再封装了一个外网 IP 头，主要用于 Site-to-Site 的应用场景。也可以适用于任何场景，由于隧道模式需要多一层 IP 头开销，所以在 PC 到 PC 的场景，建议还是使用传输模式 [4]。

AH：



ESP：

AH-ESP:



5 安全策略创建于应用

①配置网络可达：检查报文发送方和接收方之间的网络层可达性，确保双方只有建立 IPSec VPN 隧道才能进行 IPSec 通信。

②配置 ACL 识别兴趣流：完整性和机密性要求部分流量是无法满足，对流量进行过滤是有必要的，选择出需要进行 IPSec 处理的兴趣流，不同的数据流可以通过配置 ACL 来定义区分。

③创建安全提议：为了能够正常传输数据流，IPSec 提议定义了保护数据流的传输安全，安全隧道两端必须使用一样的认证算法、安全协议、加密算法和封装模式。如果要在两个安全网关之间建立 IPSec 安全隧道，IPSec 隧道模式可以方便隐藏通信过程中使用的实际源 IP 和目的 IP。

④创建安全策略：每一个 IPSec 安全策略都使用唯一的名称和序号来标识。IPSec 策略中会应用 IPSec 提议中定义的封装模式、安全协议与认证加密算法。IPSec 策略可分成两类：手工建立 SA 的策略和 IKE 协商建立 SA 的策略。在本文中主要介绍手工建立 SA 的策略。

⑤应用安全策略：在某一个接口上应用 IPSec 安全策略。

6 安全策略实现

这里通过 eNSP 模拟搭建实验网络，网络拓扑及主要参数如图 2 所示，根据实现过程完成配置如下：

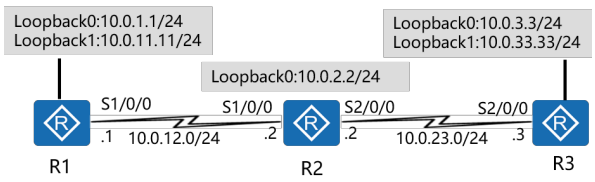


图 2 IPSec VPN 实验拓扑图

6.1 定义 ACL 感兴趣流

[R1-acl-adv-3001] rule 5 permit ip source 10.0.1.0 0.0.0.255 destination 10.0.3.0 0.0.0.255

[R3-acl-adv-3001] rule 5 permit ip source 10.0.3.0 0.0.0.255 destination 10.0.1.0 0.0.0.255

6.2 创建安全提议

[R1-ipsec-proposal-tran1] esp authentication-algorithm sha1 [R1-ipsec-proposal-tran1] esp encryption-algorithm 3des

[R3-ipsec-proposal-tran1] esp authentication-algorithm sha1 [R3-ipsec-proposal-tran1] esp encryption-algorithm 3des

6.3 创建 IP 协议安全策略

[R1] ipsec policy P1 10 manual

[R1-ipsec-policy-manual-P1-10] securityacl 3001 [R1-ipsec-policy-manual-P1-10] proposal tran1

[R1-ipsec-policy-manual-P1-10] tunnel remote 10.0.23.3

[R1-ipsec-policy-manual-P1-10] tunnel local 10.0.12.1

[R1-ipsec-policy-manual-P1-10] saspi outbound esp 54321 [R1-ipsec-policy-manual-P1-10] saspi inbound esp 12345

[R1-ipsec-policy-manual-P1-10] sa string-key outbound esp simple huawei [R1-ipsec-policy-manual-P1-10] sa string-key inbound esp simple huawei

[R3] ipsec policy P1 10 manual

[R3-ipsec-policy-manual-P1-10] securityacl 3001 [R3-ipsec-policy-manual-P1-10] proposal tran1

[R3-ipsec-policy-manual-P1-10] tunnel remote 10.0.12.1

[R3-ipsec-policy-manual-P1-10] tunnel local 10.0.23.3

[R3-ipsec-policy-manual-P1-10] saspi outbound esp 12345 [R3-ipsec-policy-manual-P1-10] saspi inbound esp 54321

[R3-ipsec-policy-manual-P1-10] sa string-key outbound esp simple huawei [R3-ipsec-policy-manual-P1-10] sa string-key inbound esp simple huawei

6.4 安全策略应用

[R1] interface Serial 1/0/0

[R1-Serial1/0/0] ipsec policy P1

[R3] interface Serial 2/0/0

[R3-Serial2/0/0] ipsec policy P1

7 安全策略检测

通过以上策略创建于应用，这里主要检测网络的连通性状况。

7.1 不感兴趣流量

在这里我们对不感兴趣流量不进行 IPSec 加密处理，display ipsec statistics esp 查看情况如下。

<R1>ping -a 10.0.11.11 10.0.33.33

PING 10.0.33.33: 56 data bytes, press CTRL_C to break

Reply from 10.0.33.33: bytes=56 Sequence=1 ttl=254 time=60 ms

Reply from 10.0.33.33: bytes=56 Sequence=2 ttl=254 time=50 ms

Reply from 10.0.33.33: bytes=56 Sequence=3 ttl=254 time=50 ms

Reply from 10.0.33.33: bytes=56 Sequence=4 ttl=254 time=60 ms

Reply from 10.0.33.33: bytes=56 Sequence=5 ttl=254 time=50 ms

---

<R1>display ipsec statistics esp

Inpacket count **0**

Inpacketauth count 0

Inpacketdecap count 0

Outpacket count **0**

PktDuplicateDrop count 0

PktSeqNoTooSmallDrop count 0

PktInSAMissDrop count 0

7.2 感兴趣流量

在这里我们对感兴趣流量进行 IPSec 加密处理，display ipsec statistics esp 查看情况如下。

<R1>ping -a 10.0.1.1 10.0.3.3

PING 10.0.3.3: 56 data bytes, press CTRL_C to break

Reply from 10.0.3.3: bytes=56 Sequence=1 ttl=255 time=80 ms

Reply from 10.0.3.3: bytes=56 Sequence=2 ttl=255 time=77 ms

Reply from 10.0.3.3: bytes=56 Sequence=3 ttl=255 time=77 ms

Reply from 10.0.3.3: bytes=56 Sequence=4 ttl=255 time=80 ms

Reply from 10.0.3.3: bytes=56 Sequence=5 ttl=255 time=77 ms

<R1>display ipsec statistics esp

Inpacket count : 5

Inpacketauth count : 0

Inpacketdecap count : 0

Outpacket count : 5

PktDuplicateDrop count 0

PktSeqNoTooSmallDrop count 0

PktInSAMissDrop count 0

8 结语

论文简单介绍了 IP 隧道安全应用与架构。重点描述了 IPsec 协议的封装报文类型，安全策略的引入创建及应用原理，通过实验了解安全策略的设计与实现过程。掌握 IPSec 提议、策略、绑定方法等，通过 ACL 定义感兴趣流，经过 IPSec 过滤后的感兴趣数据流将会对协商的各种参数进行处理并封装，之后通过 IPSec 隧道进行转发。

参考文献

[1] 王笛,陈福玉.基于IPsec VPN技术的应用与研究[J].电脑知识与技术,2020,16(11):4.

[2] 肖蔚琪.IPSEC VPN技术在私有虚拟专网中的应用探讨[J].信息通信,2014(12):2.

[3] 王霞俊.基于H3C HCL的IPSec VPN实验设计与仿真[J].实验室研究与探索,2018(3):4.

[4] 李超凡,马凯.IPSec VPN应用场景分析与实验仿真[J].新疆师范大学学报(自然科学版),2022,41(1):6.