基于 EVE-NG 仿真环境下 IPSec VPN 穿越 NAT 的设计与实现

李　超
（广州松田职业学院，广东 广州 511300）

摘要：IPSec VPN 是在企业内网之间的数据通过这些网关建立的隧道实现安全互联，NAT 是网络间地址转换，当 NAT 运行在 IPSec VPN 间时会对隧道产生影响。针对通用的 EVE-NG 虚拟化仿真环境进行个性化开发、配置灵活、紧贴真实案例的实践教学环节中，构建出 IPSec VPN 穿越 NAT（以下称“NAT-T”）的实验方案。通过设计网络环境，给出关键命令，通过 PING 及其他测试方法对实验效果进行验证。本次实验使学生不仅可以学习到 IPSec VPN 和 NAT 的相融合，还可以把该实例迁移到现网环境中，更有效的针对我们实践教学。

关键词：IPSec VPN；EVE-NG；NAT；NAT-T；虚拟化

随着互联网的快速发展和“互联网 +”的战略部署，在当今计算机网络技术在不断发展中，对于我们在平时教学中，基于传统的 C/S 结构的实验环境模拟器已经无法满足，我们需要借助云端实验环境满足我们网络专业的教学。目前我们采用的 EVE-NG 虚拟化仿真环境，虚拟化技术的诞生给我们带来了不同的生活改变。随着网络安全事件的频发，当前各行业的安全态势愈发严峻，面对工作和生活我们也离不开网络，而网络安全正是我们现如今各行各业要解决的重大问题。在国家统一战略的部署下，增强我们自身的认识，我们要基于向 B/S 结构的云平台去学习使用，在面对新一代信息技术的计算机网络设备配置，我们在日常教学过程中要运用前沿的虚拟化仿真实验环境。因此，在这样的虚拟化仿真环境下构建企业网 NAT-T 的实验方案，让学生更充分的理解 IPSec VPN 穿越 NAT 的实现与原理，以及相关知识技能的掌握。

一、IPSec VPN 和 NAT 理论

IPsec 它是一种互联网 VPN 的解决方案，支持 DES、3DES、AES 加密算法。它提供了数据的完整性、源认证、机密性以及不可否认性。其中完整性代表数据在传输的过程中要保证数据的信息内容不发生变化，保证数据的完整性。源认证代表数据是由该发送者发送信息，机密性确保数据在传输的过程中要保证信息不被泄露是密文的，不可否认性代表是信息是你发送的，不可以抵赖。它支持网络层的数据加解密，在明文的 IP 头部和网络层数据之间插入了一个 IPSec 的头部，保证了网络负载的安全。IPSec 广泛的应用在大型企业网内部，实现端到端的数据加密，确保在企业内部的不同部门之间传递的信息是加密的。NAT 简称网络地址转换协议，通常部署在企业网出口位置，目的是将企业网内部的数据流 IP 转换为公网 IP 实现内网的可达和连通性。NAT 一般分为静态 NAT、动态 NAT 和 PAT，企业中常用 PAT 技术实现内部员工上网。然而 NAT-T 是基于对 IPSec VPN 穿越 NAT，对 IPSec 协议的数据包再进行 UDP 的封装，此时当数据包经过 NAT 转换时，其对应的数据包就会发生变化。

二、EVE-NG 平台

EVE-NG 平台是基于虚拟化仿真技术，模拟多个厂家不同型号的产品实现的网络环境，通过虚拟路由器和交换机连接成的逻辑网络拓扑，利用统一界面进行配置。而 EVE-NG 平台理论上，它可以运行虚拟磁盘格式为 qcow2 的虚拟机，充分展现了虚拟化的技术，因此，EVE-NG 可以算得上是虚拟化仿真实验环境。它支持了 dynamips，IOL，KVM 等特性，通过 Ubuntu 操作系统，直接可以安装在 x86 架构的服务器上，而且 EVE-NG 也有 ova 版本，可以直接导入到 VMware 中进行使用。这里注意，EVE-NG 平台还可以进行二次开发，满足市场的需求。EVE-NG 作为新一代的虚拟化仿真实验环境，可以模拟出和企业现网同样的真实环境，满足了在校学生和实际工作中的场景对接，提升了学生的操作能力。

三、IPSec VPN 穿越 NAT 实验设计与实现

（一）实验目的

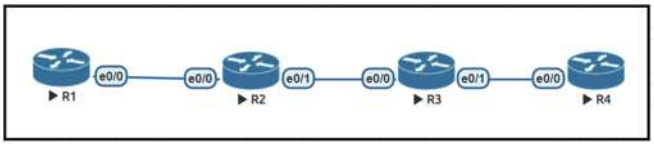
目前网络在高速的发展，各行各业都在全方位的应用互联网，比如短视频、语音、自媒体等多种方式，需要网络的传输要实现高质量和高效。在我们使用互联网的时候，提到用户体验的思路，IT 的运维不在是简单的保证内网的网络系统正常通信，也要考虑到企业的架构、产品的应用，最终实现高评价的用户体验。在企业网内部，当我们要搭建 IPSec VPN 时，面对有 NAT 需求的情况，要掌握 NAT-T 的关键配置方法，即包括在 EVE-NG 仿真环境中配置 IPSec VPN、NAT 网络地址转换、静态路由、在各个网络设备的基础命令，理解 IPSec VPN 隧道建立的过程、以及在企业网络中配置了 NAT 的需求，当 NAT-T 时需要注意的内容以及解决方案，实现 NAT-T 时隧道上如何安全的通信，以及测试各个结果。

（二）实验背景

在当今互联网快速发展的背景下，IPSec VPN 解决方案要时刻关注企业的发展，当在复杂的网络系统环境中，网络中出现了 NAT 技术，我们要考虑到 NAT 对 IPSec VPN 的影响，这就需要使用 NAT-T 的解决方案，实现网络架构的综合部署和可扩展的技术手段，使企业网络可以更好的服务内部和客户。

（三）实验设计

NAT -T 实验设计如图 1 所示。虚拟化仿真环境拓扑分为路由器 R1，路由器 R2，路由器 R3 以及路由器 R4，R2 是互联网 Internet，R1、R3 分别是企业边界网络设备，R4 是内网设备，网络设备分别都包括 2 台核心路由器、2 台汇聚路由器。内网采用当今主流的“扁平化”结构，R1 和 R4 设备建立 IPSec VPN，R3 设备开启 NAT 功能将内网 R4 数据源 IP 转换到公网。两个设备 R1 和 R4 配置 IPSec VPN 是重点，R3 设备启动 NAT 功能，配置 NAT-T 是难点，确保 R1 和 R4 的内网数据流可以正常安全通信。



1. 实验环境规划

根据 NAT -T 实验设计，设备 R1 和设备 R3 的 E0/0 口连接公

网，R1 和 R4 设备都设置有环回口 loopback 口，R3 启动 NAT 功能，最终保证 R1 和 R4 的内网流量可以实现安全通信。

实验中用到 2 个公网接口分别是 R1 的 E0/0，R3 的 E0/0，所对应的 IP 分别是 202.100.1.1 和 61.128.1.1，设备 R1 设置环回口地址是 Loopback0 环回口 10.1.1.1，设备 R2 设置环回口地址是 Loopback0 环回口 20.1.1.1，其中主要网络设备 IP 规划表如表 1 所示。

表 1　网络设备 IP 规划表

设备	端口	IP 地址	业务描述
R1	E0/0	202.100.1.1	R1
	Loopback0	10.1.1.1	R1
R2	E0/0	202.100.1.10	R2
	E0/1	61.128.1.10	R2
R3	E0/0	61.128.1.1	R3
	E0/1	172.16.1.30	R3
R4	E0/0	172.16.1.40	R4
	Loopback0	20.1.1.1	R4

2. 虚拟化仿真环境拓扑设备接口配置

接口配置非常重要，在 NAT-T 建立中，设置正确的接口可以确保网络间的正常访问，为搭建 IPSec VPN 的建立提供保障，这个步骤在实验环境中非常重要，主要代码如下见表 2：

表 2　网络设备 IP 配置

R1： interface Loopback0 ip address 10.1.1.1 255.255.255.0 interface E0/0 ip address 202.100.1.1 255.255.255.0 ip route 0.0.0.0 0.0.0.0 202.100.1.10	R2： interface E0/0 ip address 202.100.1.10 255.255.255.0 interface Ethernet0/1 ip address 61.128.1.10 255.255.255.0
R3： interface E0/0 ip address 61.128.1.1 255.255.255.0 interface Ethernet0/1 ip address 172.16.1.30 255.255.255.0 ip route 0.0.0.0 0.0.0.0 61.128.1.10	R4： interface Loopback0 ip address 20.1.1.1 255.255.255.0 interface Ethernet0/0 ip address 172.16.1.40 255.255.255.0 ip route 0.0.0.0 0.0.0.0 172.16.1.3

3. 网络设备 R3 配置 NAT

网络设备 R3 需要进行 NAT 配置是本实验实现中至关重要的环节，它转换了 IPSec VPN 中的感兴趣流，内网加解密的 IP 被 NAT 所改动，此时感兴趣流发生了变化，造成感兴趣流在加解密的过程中就会造成通信失败，该报文会被认为是非法数据流而被丢弃，从而导致了在使用了 NAT 设备的通信路径中无法实现 IPSec 流量正常加解密访问。

```
access-list 10 permit any
ip nat inside source list 10 interface Ethernet0/0 overload
interface E0/1
 ip nat Inside
!
interface E0/0
 ip nat Outside
```

4. 网络设备 R1 和 R4 配置 IPSec VPN

R1 和 R4 建立 IPSec VPN，它们之间建立一条隧道，第一阶段是彼此相互认证，包括加密算法、认证方式，哈希函数和组要保持两端一致，确保认证相互成功，开始进入第二阶段，最终实现内网的数据流可以安全通信，主要代码详见表 3：

表 3　IPSec VPN 配置

```
R1：
CRYPTO ISAKMP POLICY 200
ENCR AES
AUTHENTICATION PRE-SHARE
GROUP 2
HASH MD5
CRYPTO ISAKMP KEY SONTAN ADDRESS 61.128.1.1
CRYPTO IPSEC TRANSFORM-SET SONTAN ESP-3DES ESP-MD5-HMAC
ACCESS-LIST 200 PERMIT ICMP 10.0.0.0 0.0.0.255 20.0.0.0 0.0.0.255
CRYPTO MAP SONTAN 20 IPSEC-ISAKMP
 SET PEER 61.128.1.1
SET TRANSFORM-SET SONTAN
 MATCH ADDRESS 200
!
INTERFACE E0/0
CRYPTO MAP SONTAN
R4 配置参考 R1 配置，要注意加密点、感兴趣流，加密图的应用
```

四、实验验证

（一）网络连通性

网络环境测试一般采用“由近及远，由易到难”的测试步骤，逐步推进。因此，在配置完成的基础上，首先先测试基础网络联通性，测试 R1 和 R3 公网是连通的，R3 和 R4 是内网连通的，分别见见图 2 和图 3。

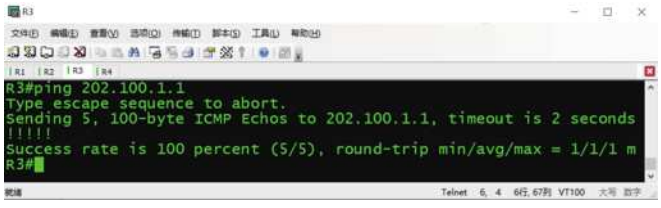


图 2　R1 和 R3 公网连通性

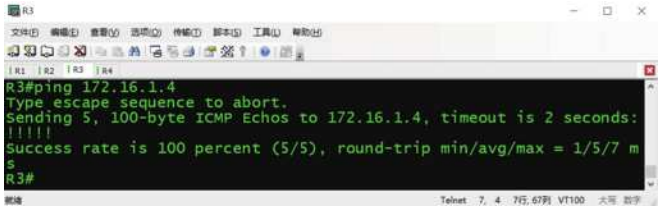


图 3　R3 和 R4 内网连通性

（二）R3 配置 NAT 验证效果

R3 有去往 R2 的默认路由，R2 有直连路由 202.100.1.0 和 61.128.1.0，此时只能确保 R1 与 R3 的公网通信，因此 R3 目前无法访问 10.1.1.0/24 网络，如图 4 所示：

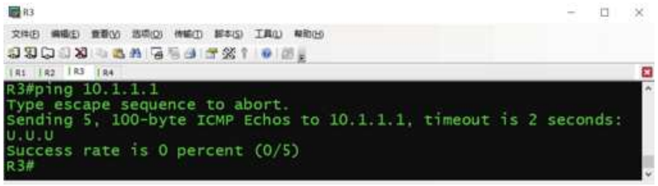


图 4　R3 访问 R1 内网连通性

（三）验证 R4 连接 R1 建立 IPSecVPN

当前 R4 的内网流量发起向 R1 的内网连接时，数据从 R4 出发，经过 NAT 设备，由于数据流是从 NAT 本端设备发起，因此 IPSec VPN 可以成功建立。如果数据从 R1 端发起，需要在路由器 R3 上添加命令，确保 IPSec VPN 可以正常建立，如下图 5、图 6、图 7、图 8 所示：

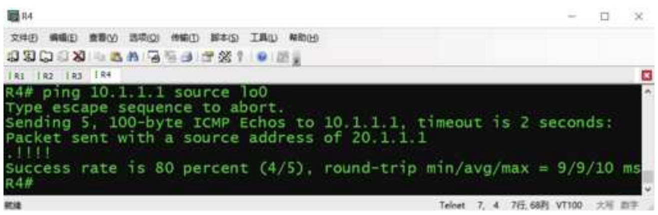


图 5　R4 访问 R1 建立 IPSecVPN

图 6　R4 与 R1 建立的安全关联 SA

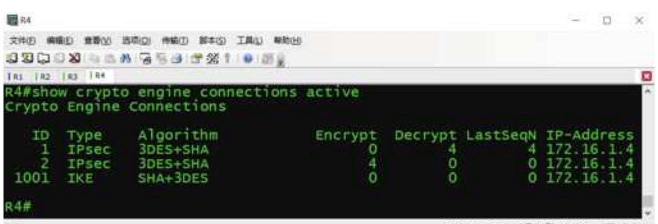


图 7　R1 与 R4 加解密流量

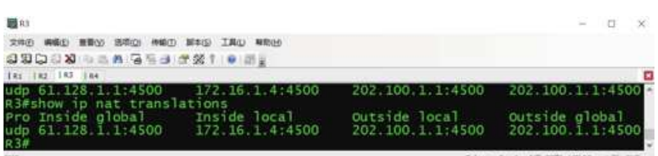


图 8　NAT–T 中所使用的端口情况

（四）验证 R 1 连接 R 4 建立 IPSecVPN

此时通过 R4 连接的 IPSec VPN 已成功建立，现在中断连接，从 NAT 的远端 R1 设备发起连接，查看通信效果，发现如下：

R4：

clear crypto isakmp

clear crypto sa

R1：

clear crypto isakmp

clear crypto sa

R3：

clear ip NAT translation *

此时发现从 NAT 远端的设备发起时无法建立 IPSec VPN，必须在 R3 路由器上添加命令，配置命令如下，否则 IPSec VPN 无法建立正常通信，效果见图 9：

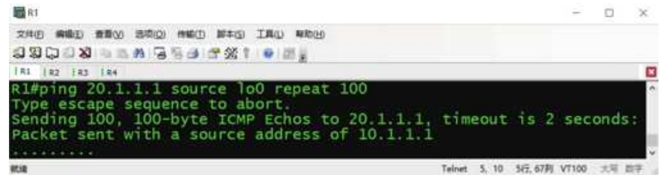


图 9　R1 与访问 R 4 失败建立 IPSecVPN

R3：

IP NAT INSIDE SOURC STATIC UDP 172.16.1.40 4500 INT E0/0 4500

IP NAT INSIDE SOURC STATIC UDP 172.16.1.40 500 INT E0/0 500

此时看到在 NAT 路由器 R3 上配置端口转换命令时，发现从 NAT 远端 R1 发起的 IPSec VPN 连接建立成功，此时可以看到 NAT–T 与远端设备建立 IPSec VPN 使用的端口情况为 UDP 4500、ISAKMP 端口 UDP 500，当再次清掉安全关联 SA 和加解密流量时，重新测试还是可以正常加解密，实现正常通信，我们可以看到 NAT–T 所实现的效果，通过不同端的设备发起时会有不一样的结果，网络通信是要分析整个环境，其中包括路由信息、部署策略、应用等，最终结合实际需求，满足企业的需求条件。效果见图 10：

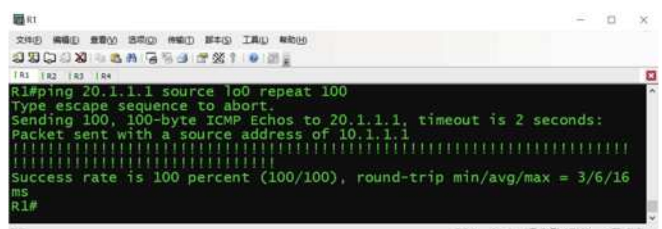


图 10　R1 与访问 R 4 成功建立 IPSecVPN

五、结语

基于 EVE–NG 虚拟化仿真实验环境下，通过搭建 NAT — T 实验运用了路由协议、IPSec　VPN 配置、NAT 配置、NAT — T 等技术，可以帮助学生实践体验 IPSec　VPN 环境下穿越 NAT 的实际效果，对今后的工作有良好的帮助。同时，对于提高学生在做项目的过程中，自己通过搭建环境测试实际效果起到作用。未来，我们要更加借助虚拟化环境才可以培养出更出色的学生。

参考文献：

[1] 温贺平 . 基于 eNSP 的安全园区网实验设计与构建 [J]. 实验室研究与探索，2018（4）：5.

[2] 黄建忠，张沪寅，裴嘉欣 . 网络安全虚拟仿真实验教学体系设计 [J]. 实验室研究与探索，2016，35（10）：170–174.

[3] 孟祥成 . 一种仿真企业网的综合组网实验设计 [J]. 实验室研究与探索，2018，37（06）：135–139.

[4] 周益旻，刘方正，杜镇宇，张凯 .IPSec VPN 安全性漏洞分析及验证 [J]. 计算机工程：2020（12）：1–11.

[5] 刘延锋，王月春，张少芳 . 一种典型的 NAT 实验环境设计 [J]. 电脑编程技巧与维护，2021（03）：11–12+39.

作者简介：李超（1989–），男，汉族，陕西宝鸡人，本科，高级工程师，研究方向为网络安全、云网络。