SD-WAN 虚拟化多功能安全网关

作

品

说

明

书

学院名称：四川信息职业技术学院

项目名称：SD-WAN 虚拟化多功能安全网关

指导教师：陈亚威

团队名称：open studio

队　　长：谢欧

队　　员：李红剑　陈奇

二零一八年十月十二日

目录

一、摘要

随着物联网 IOT 的兴起，虚拟世界和物理世界连在了一起。对这样一个复杂网络的保护，无疑将会成为一个巨大的挑战。在 16 年 4 月，习近平总书记在网络安全和信息化工作座谈会中指出增强网络安全防御能力和威慑能力。强调网络安全的本质在对抗，对抗的本质在攻防两段的能力较量，要落实网络安全责任制，制定网络安全标准。为满足国家信息安全等级保护要求，保护企业信息系统的安全稳定运行，建立与完善国产 Linux 操作系统的产业链和生态环境亦尤为重要。

普华 iSoft-Linux 国产服务器操作系统软件，以高效、稳定、安全为突破点，提供完善的系统服务和网络平台，以“可信物联，谁主沉浮。隧道飞鸿，开源卫士”为目标，开发创新，轻松构建自主可控、安全可靠的系统平台。龙芯中科在面向信息化建设时，以安全可控为主题，以产业发展为主线，以体系建设为目标，坚持自主创新，为信息产业及工业信息化的创新发展提供了更有力的保障。

二、项目概述

2.1 操作系统简介

Linux 操作系统的诞生、发展的成长过程始终依赖着五个重要支柱：UNIX 操作系统、MINIX 操作系统、GNU 计划、POSIX 标准和 Internet 网络。自 Linux 操作系统诞生以来，经过一步步的更新迭代、发展与完善，已然趋于成熟。作为一个多用户、多任务的操作系统，以其稳定、可靠，且系统内核代码的开源性，获得广大用户的青睐。现如今，不少中小企业或用户已然开始使用搭载 Linux 操作系统的服务器使其广泛用于网络服务中，以 Linux 系统搭建多种 Web 服务器：FTP 服务器、DNS 服务器、DHCP 服务器等，成为当今主流

操作系统之一。

近一两年发生网络安全事件数不胜数，在 2017 年 5 月 12 日，WannaCry 蠕虫席卷全球，只是一起大规模的勒索软件感染事件。WannaCry 勒索蠕虫感染的电脑将被锁定，包括照片、文档、压缩包、音频等可执行程序的多种类型文件被加密，被加密后的文件后缀名改为“。WNCRY”， 勒索软件运用了高强度的加密算法使得目前难以破解，暴力破解需要极高的运算量，基本不可能成功解密。为满足国家信息安全等级保护要求，保护企业信息系统的安全稳定运行，建立与完善国产 Linux 操作系统的产业链和生态环境亦尤为重要。

国家信息安全以及公共隐私安全的问题已经为各国政府关注的重点。而桌面操作系统作为基础软件，更应该加强安全防护。基于这些需求，普华 iSoft-linux 国产操作系统应运而生，普华 iSoft-linux 国产操作系统形成自己的“生态系统”，在关注安全的同时提高系统的易用性。适用于办公、上网、开发以及娱乐等应用场景。提供个性化定制以及系统优化方案，为行业定制需求领域提供了可靠稳定的基础平台。普华基础软件作为国内较早家把基于 Linux 内核的桌面操作系统部署到切实的生产环境当中的厂商，其设计采用云应用无缝投射到本地桌面的方式，在技术上解决了在当前阶段尚不能完全替代 windows 的难题，是“自主可控”国产操作系统推广过程中一个重要的里程碑。

2.2 KVM

- 2.2.1 kvm 简介

Kernel-based Virtual Machine 的简称，是一个开源的系统虚拟化模块，自 Linux 2.6.20 之后集成在 Linux 的各个主要发行版本中。它使用 Linux 自身的调度器进行管理，所以相对于 Xen，其核心源码很少。KVM 目前已成为学术界的主流 VMM 之一。

KVM 的虚拟化需要硬件支持（如 Intel VT 技术或者 AMD V 技术)。是基于硬件的完全虚拟化。而 Xen 早期则是基于软件模拟的

Para-Virtualization，新版本则是基于硬件支持的完全虚拟化。但 Xen 本身有自己的进程调度器，存储管理模块等，所以代码较为庞大。广为流传的商业系统虚拟化软件 VMware ESX 系列是基于软件模拟的 Full-Virtualization。

- 2.2.2 KVM 优势

1. KVM 所使用的方法是通过简单地加载内核模块而将 Linux 内核转换为一个系统管理程序（在安装 KVM 内核模块时）。这个内核模块导出一个名为/dev/kvm 的设备，他可以启用内核的客户模式（除了传统的内核模式和用户模式），但是打开/dev/kvm 的进程看到的是不同的映射。

2. 安装 KVM 之后，可以在用户空间启动客户操作系统。每个客户操作系统都是主机操作系统的一个单一进程（图 1 提供了一个使用 KVM 进行虚拟化的试图）

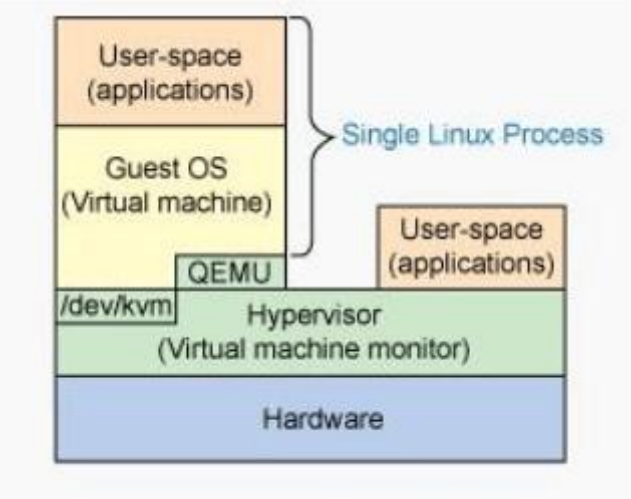


图 1 使用 KVM 的虚拟化组件

3. KVM 是解决虚拟化问题的一个有趣的解决方案，但是它是第一个进入内核的虚拟化解决方案，所以还有其他一些方法一直在为进入内核而竞争，比如 UML 和 Xen，由于 KVM 需要的修改较少，并且可以将标准内核转换成一个系统管理程序，因此它的优势不言而喻。KVM 的另一个优点是它是内核本身的一部分，因此可以利用内核和优化和改进。与其他独立的系统管理员程序集觉方案相比，KVM 是一种不会过时的技术

- 2.2.3 KVM 相关安装包及其作用

qemu-kvm.....主要的 KVM 程序包

python-virtinst.....创建虚拟机所需要的命令行工具和程序库

virt-manager.....GUI 虚拟机管理工具

virt-top.....虚拟机统计命令

virt-viewer.....GUI 连接程序，连接到已配置好的虚拟机

libvirt.....C 语言工具包，提供 libvirt 服务

libvirt-client.....虚拟客户机提供的 C 语言工具包

virt-install.....基于 libvirt 服务的虚拟机创建命令

2.3 VyOS

- 2.3.1 VyOS 简介

VyOS--开源路由操作系统，也是一款受大众喜欢的一款软路由器。VyOS 是基于 Debian GNU/Linux 的，提供了和其他诸如 Cisco 的 IOS、Juniper 的 JUNOS 类似的操作方式，配置起来感觉特别的舒服，尤其可以使用 compare、rollback 之类的命令，方便对比配置和错误回滚。VyOS 这个项目的第一个版本释放于 2013 年，目前还在持续活跃中。相对其他项目——像 Juniper 管理下的 opencontrail,它有完整的使用与安装文档,更提供了 API 文档供开发者参考（这点也是我们选择这个操作系统的原因之一）。可以用它来实现软件防火墙、路由器、负载均衡等功能。

1. 特性

1) 平台支持

32-bit x86

64-bit x86

KVM (virtio drivers included)

Xen HVM (including XenServer and EC2)

VMWare (open-vm-tools included)

Hyper-V (drivers included)

VirtualBox (guest additions not included)、

(默认情况下支持串口的终端是启用的)

2) 路由

BGP (IPv4 and IPv6)

OSPFv2

OSPFv3 (incomplete)

RIP

RIPng

Policy-based routing

3) 网络接口

Ethernet

802.1q VLAN, QinQ

NIC bonding

Bridges, STP (no RSTP or other extensions)

Port mirroring and redirection

Dummy interfaces (analogous to multiple loopbacks)

Pseudo-ethernet (aka MAC VLAN)

802.11 wireless (client and access point)

Some wireless modems (not very good support)

PPPoE

Note: No support for serial WAN, ISDN, dial-up, DSL cards. Use an external device for that.

4) 防火墙与 NAT

Stateful firewall

Network/address/port groups (IPv4 only for now)

Zone-based firewall

Source and destination NAT

5) 网络服务

DHCP server and relay

Caching DNS server

Web proxy with some URL filtering support (no HTTPS filtering)

Telnet and SSH for remote management

IGMP proxy

QoS support

6) 高可用

VRRP (IPv4 only for now)

Conntrack sync

WAN failover and load balancing

7) IPV6 支持

IPv6 routing (static and dynamic)

Router advertisment

DHCPv6 client and server/relay

IPv6 firewall

8) 系统维护和监控

Task scheduler

SNMP

Configuration versioning and remote archiving

Event handling

Remote syslog

其他特性详见链接：http://vyos.net/wiki/Feature_list

- 2.3.2 VyOS 特点

1. VyOS 与其他路由器发行版本的不同

1) 硬件路由器风格的统一命令行界面

2) 可编写脚本的 CLI

3) 有状态配置系统：立刻准备更改和提交或丢弃，将修订存档到远程服务器，在提交时执行挂钩

4) 基于镜像的升级

5) 支持在 kvm,Xen Hvm 等多种虚拟化平台上运行，可以大大的节约资源。

- 2.3.3 VyOS 安装

1. 简单配置

VyOS CLI 提供两种模式：operational mode 和 configuration mode. 输入 configure 之后即进入 configuration 模式，跟路由器和其他 linux 发行版一样，支持[tab]补齐和？查看帮助信息。配置完之后用 **compare** 命令查看修改的配置，**commit** 提交配置，**save** 保存到/config/config.boot 配置文件中。

2. 步骤说明

eth0 为公网 ip、eth1 为内网 ip 并做了 nat 转发.这样网关就做成了

```
set interfaces ethernet eth0 address 公网 ip/子网掩码
set interfaces ethernet eth0 description 'OUTSIDE'
set interfaces ethernet eth0 duplex 'auto'
set interfaces ethernet eth0 speed 'auto'
set interfaces ethernet eth1 address 192.168.4.1/22
set interfaces ethernet eth1 description 'INSIDE'
set interfaces ethernet eth1 duplex 'auto'
set interfaces ethernet eth1 speed 'auto'
set nat source rule 100 outbound-interface 'eth0'
set nat source rule 100 source address '192.168.4.0/22
'
set nat source rule 100 translation address masquerade
```

```
set system gateway-address //外网网关
set system host-name vyos
delete system ntp server '0.pool.ntp.org'
delete system ntp server '1.pool.ntp.org'
delete system ntp server '2.pool.ntp.org'
set system ntp server IP 地址
set system time-zone Asia/Shanghai
set system name-server 202.106.0.20
set system ipv6 disable
set system options reboot-on-panic true #系统崩溃后重启
commit
save
```

2.4 IPSec

- 2.4.1 IPSec 简介

1.IPSec（IP Security）是一组开放协议的总称，特定的通信方之间在 IP 层通过加密与数据源验证，以保证数据包在 Internet 网上传输时的私有性、完整性和真实性。IPSec 通过 AH （Authentication Header）和 ESP（Encapsulating Security Payload）这两个安全协议来实现。而且此实现不会对用户、主机或其它 Internet 组件造成影响，用户还可以选择不同的硬件和软件加密算法，而不会影响其它部分的实现。

2.IPSec 提供以下几种网络安全服务：

私有性 — IPSec 在传输数据包之前将其加密.以保证数据的私有性；

完整性 — IPSec 在目的地要验证数据包，以保证该数据包在传输过程中没有被修改；

真实性 — IPSec 端要验证所有受 IPSec 保护的数据包；

防重放 — IPSec 防止了数据包被捕捉并重新投放到网上，即目的地会拒绝老的或重复的数据包，它通过报文的序列号实现。

3.IPSec 在两个端点之间通过建立安全联盟（Security Association）

进行数据传输。安全联盟定义了数据保护中使用的协议和算法以及安全联盟的有效时间等属性。IPSec 在转发加密数据时产生新的 AH 和/或 ESP 附加报头，用于保证 IP 数据包的安全性。IPSec 有隧道和传输两种工作方式。在隧道方式中，用户的整个 IP 数据包被用来计算附加报头，且被加密，附加报头和加密用户数据被封装在一个新的 IP 数据包中；在传输方式中，只是传输层（如 TCP、UDP、ICMP）数据被用来计算附加报头，附加报头和被加密的传输层数据被放置在原 IP 报头后面。

- 2.4.2 IPSec 的优势

说起 IPSec 的优势，为什么我们选择 IPSec，那就有必要把 vpn 的几种不同的模式都一一拿出来介绍一下。

Pptp:pptp 使用的传输协议是 tcp 协议，所以一般更适合小流量传输的场景。比如逛网页，收邮件等。

L2tp:L2tp 所使用的传输协议是 udp 协议，udp 协议的特点就是舍弃了更加安全稳定的传输而选择了快，所以 L2tp 更适合大流量传输的场景。比如看直播，看视频。

Open vpn:Open vpn 拥有超强的穿透性，适合多子网的场景，比如校园网，公司局域网等受限网络环境

IPSec:IPSec 是封装的隧道模式，防止网络上窃听通讯的人获取原始数据包数据，更安全.

对于 SD-WAN 虚拟化多功能安全网关来说，本产品跟适合的场景是公司的局域网，我们要实现的就是，能让公司里的运维人员以及各种从事计算机技术的人士能够更加方便的管理公司的服务器，实现在家也能轻松管理服务器。那么应选择的 vpn 模式就只有了 open vpn 与 IPsec 了，open vpn 拥有很强的穿透性，能够轻松的胜任在公司的复杂局域网中与外网对接的功能。那么为什么我们选择 IPsec 呢？原因很简单：因为安全，我们舍弃了强有力的穿透性而选择了更加安全的 vpn 模式。对于企业的服务器来说，安全实为至关重要的一件事，我们要做到的是更安全，更加更加的安全，IPSec 刚好满足企业对安全的需求，更加不容易被坏人盗取公司的信息。

- 2.4.3 IPSec 配置（VyOS 中的配置）

1.设置宽带上网

```
set int eth eth0 pppoe 0
set int eth eth0 pppo 0 user-id youre_username
set int eth eth0 pppo 0 password your_password
```

2.配置 dhcp

```
set service dhcp-server shared-network-name LAN authoritative enable
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 start 192.168.1.100 stop 192.168.1.150
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 default-router 192.168.1.1
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 dns-server 223.5.5.5
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 dns-server 223.6.6.6
set service dhcp-server shared-network-name LAN subnet 192.168.1.0/24 lease 86400
```

3.设置 nat

```
set nat source rule 1 outbound-interface pppoe0
set nat source rule 1 source address 192.168.1.0/24
set nat source rule 1 translation address masquerade
```

4.配置 IP sec

```
set vpn ipsec ipsec-interfaces interface pppoe0
set vpn ipsec nat-traversal enable
set vpn ipsec nat-networks allowed-network 0.0.0.0/0
set vpn l2tp remote-access outside-address <public-address>
set vpn l2tp remote-access client-ip-pool start 192.168.255.1
```

set vpn l2tp remote-access client-ip-pool stop 192.168.255.255

set vpn l2tp remote-access ipsec-settings authentication mode pre-shared-secret

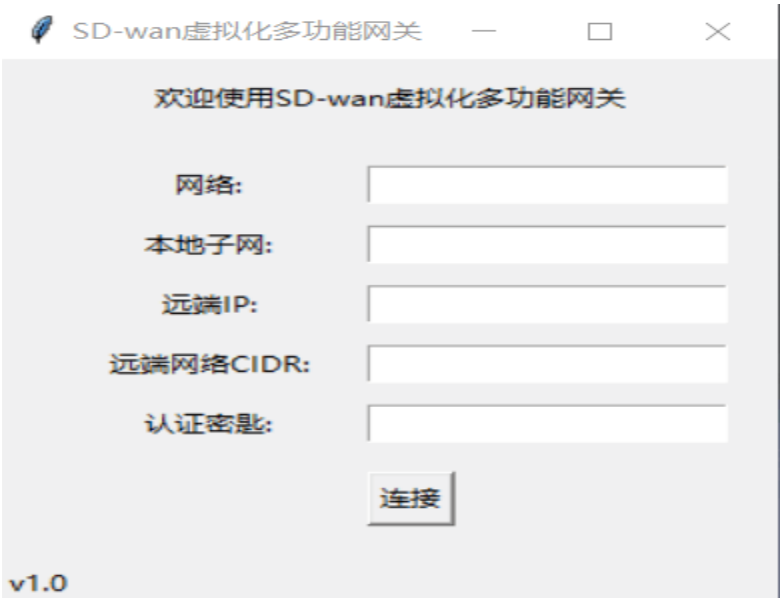
set vpn l2tp remote-access ipsec-settings authentication pre-shared-secret <secret>

set vpn l2tp remote-access authentication mode local

set vpn l2tp remote-access authentication local-users username <username> password <password>

2.5 Python GUI

```
from tkinter import *
def connection():
    pass

root = Tk()
root.title('SD-wan虚拟化多功能网关')

frame1 = Frame(root)
frame1.pack(padx = 20,pady = 10)

frame2 = Frame(root)
frame2.pack(padx = 20,pady = 10)

frame3 = Frame(root)
frame3.pack(anchor = W)

v1 = StringVar()
v2 = StringVar()
v3 = StringVar()
v4 = StringVar()
v5 = StringVar()

Label(frame1,text="欢迎使用SD-wan虚拟化多功能网关").pack()

theLabel1 = Label(frame2,text="网络:").grid(row = 0,column = 0,\
                                        padx = 20,pady = 5)

theLabel2 = Label(frame2,text="本地子网:").grid(row = 1,column = 0,\
                                        padx = 20,pady = 5)

theLabel3 = Label(frame2,text="远端IP:").grid(row = 2,column = 0,\
                                        padx = 20,pady = 5)

theLabel4 = Label(frame2,text="远端网络CIDR:").grid(row = 3,column = 0,\
                                        padx = 20,pady = 5)

theLabel5 = Label(frame2,text="认证密匙:").grid(row = 4,column = 0,\
                                        padx = 20,pady = 5)

#e1 = Entry(root,textvariable = v1, validate="key", \
           #validatecommand=(test1CMD,"%p")).grid(row = 0,column = 1)

e1 = Entry(frame2,textvariable = v1).grid(row = 0,column = 1)

e2 = Entry(frame2,textvariable = v2).grid(row = 1,column = 1)

e3 = Entry(frame2,textvariable = v3).grid(row = 2,column = 1)

e4 = Entry(frame2,textvariable = v4).grid(row = 3,column = 1)

e5 = Entry(frame2,textvariable = v5).grid(row = 4,column = 1)

Button(frame2, text="连接", command=connection).grid(row = 5, column = 1,\
                                                stick = W, pady = 10)
Label(frame3,text="v1.0").pack()

mainloop()
```



//Python 图形化界面测试中

运用 python 编写界面，原因在于 python 能更好的与后台交互，写出简易可观的界面能让用户更轻松的使用本产品。基于现今的计算机行业现状来考虑，并不是每一个人都能做到对网络有非常深层次的了解，本产品在 UI 界面方面做到更友好更简易，我们想要做到的是用户仅仅需要输入远端的子网与服务端的 ip 地址，就能轻松连接到该子网，把复杂的参数传递，计算机配置交给代码来完成，对于后太的配置，python 语言就能胜任此工作，简易的代码，完美的兼容性与可移植性，支持各种平台运行，还有能和后台的完美交互，虽然相比上 c，java 来说 python 语言的效率低，但是对于本产品来说，并不需要太高的计算需求，python 完全可以胜任此工作。

2.6 Ansible

- 2.6.1 Ansible 简介

Ansible 是新出现的自动化运维工具，基于 Python 开发，集合了众多运维工具（puppet、cfengine、chef、func、fabric）的优点，实现了批量系统配置、批量程序部署、批量运行命令等功能。

Ansible 是基于模块工作的，本身没有批量部署的能力。真正具有批量部署的是 Ansible 所运行的模块，Ansible 只是提供一种框架。主要包括：

(1)连接插件 connection plugins：负责和被监控端实现通信；

(2)host inventory：指定操作的主机，是一个配置文件里面定义监控的主机；

(3)各种模块核心模块、command 模块、自定义模块；

(4)借助于插件完成记录日志邮件等功能；

(5)playbook：剧本执行多个任务时，非必需可以让节点一次性运行多个任务。

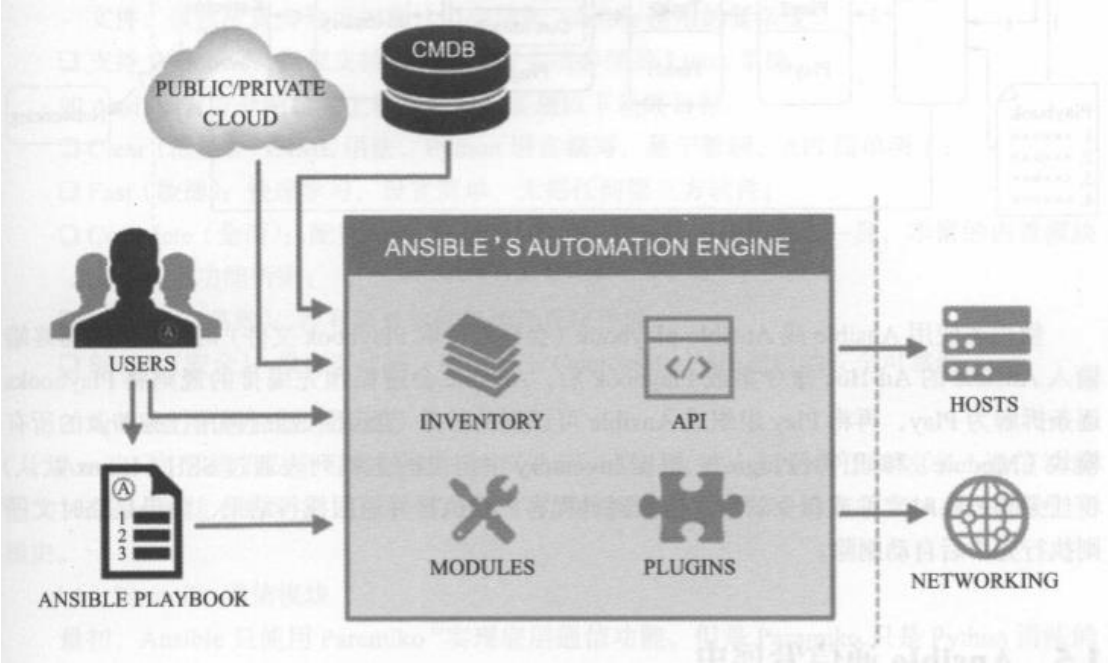


图 2 Ansible 工作机制

- 2.6.2 Ansible 优势

1. 为何选择 Ansible

1) Ansible 完全基于 Python 开发，而 DevOps 在国内已然是一种趋势，Python 被逐步普及，运维人员自己开发工具的门槛逐步降低，得益于此，方便对 Ansible 二次开发。

2) Ansible 丰富的内置模块，甚至还有专门为商业平台开发的功能模块，近 600 个模块完全可以满足日常功能所需。

3) 在 Ansible 去中心化概念下，一个简单的复制操作即可完成管理配置中心的迁移。

4) Agentless（无客户端），客户端无需任何配置，由管理端配置好后

即可使用，这点非常诱人。

2. Ansible 的优势

1) 无客户端，只需要安装 SSH、Python 即可，其中 Python 建议版本为 2.6.6 以上。

2) 基于 OpenSSH 通信，底层基于 SSH 协议（Windows 基于 PowerShell）。支持密码和 SSH 认证，因可通过系统账户密码认证或公私钥认证，所以整个过程简单、方便、安全。

3) 建议使用公私钥方式认证，因为密码认证方式的密码需明文写配置文件，虽然配置文件可加密，但会增加 Ansible 使用的复杂度。

4) 支持 Windows，但仅支持客户端，服务端必须是 Linux 系统。

3. 正如 Ansible 官方介绍，如上特性是希望实现以下最终目标：

1) Clear（简易）：YAML 语法，Python 语言编写，易于管理，API 简单明了；

2) Fast（敏捷）：快速学习，设置简单，无需任何第三方软件；

3) Complete（全面）：配置管理、应用部署、任务编排等功能集于一身，富的内置模块满足日常功能所需；

4) Efficient（高效）：没有额外软件包消耗系统性能；

5) Secure（安全）：没有客户端，底层基于 OpenSSH，保证通信的安全可靠性。

- 2.6.3 Ansible 安装部署和配置

PS：为了安全，尽量不要配置外网，首先保证可以免密钥登录被管理

环境：

测试机 test1:10.17.160.105 ——管理端

测试机 test2:10.17.107.225 ——被管理端

1. 管理端安装：yum install ansible -y
2. 被管理端安装：yum install libselinux-python -y //被管理端安装软件（被管理端需要关闭 selinux）
3. 创建密钥对：ssh-keygen -t rsa

4. 分发密钥对： ssh-copy-id -i /root/.ssh/id_rsa.pub 10.17.107.225
5. 登录验证：ssh 10.17.107.225
6. 配置文件：Ansible 主配置文件/etc/ansible/ansible.cfg
   hosts 主机文件 /etc/ansible/hosts
7. Ansible 系统命令帮助文档查看方法：
   ansible-doc -l --- 列出所有可用的模块信息
   ansible-doc -s cron --- 查看指定模块的参数信息

2.7 项目总述

相比传统的 VPN，本软件做到了简便，并无太多复杂的操作，能使并不太了解本技术的人也能轻易的使用本软件，界面设计简洁明了，用户仅需要输入几个字段就能轻松连接到专有的子网。

本软件利用 Ansible 自动化运维工具实现了传统 VPN 繁杂参数的一键传输，服务搭建也只需使用专有的一键部署脚本，轻松部署。这能让更多的人能接触到 VPN，能让更多人能搭建出 VPN 服务，而不仅仅是网络工程师才能实现。

在网络安全方面，SD-WAN 虚拟化多功能安全网关就非常出色了。接下来将用几个网络安全漏洞来举例子说明 SD-WAN 虚拟化多功能安全网关在安全方面的防护。

传统 VPN 都存在的一个漏洞，路由伪造，不同网段网络的传输都要经过路由器的转发，VPN 更是如此。然而一些黑客就利用这一点，将自己的主机伪造成消息转发必经的一台路由器的地址，将信息截取下来之后再将信息由本机转发到消息的目的地址。这样引起的问题是用户自己并不能发现有什么异样，但发送的消息缺被黑客截取得一干二净。不知不觉中自己的信息就全被暴露出去了。SD-WAN 对于此问题的解决办法是：记录了必经之路每一条路由的 MAC 地址，每一个路由在转发消息的时候会先确认对端 MAC 地址与对应的 IP 地址是否一致，确认一致再进行转发，如果出现异常会立即断开 VPN

网络的连接。

服务端伪造：此漏洞与上一个漏洞大体一致，黑客伪造成服务器，接收用户消息，将消息转发给真实的服务端，服务端给出回应，也会直接传输到伪造服务端这边。这样会出现极大的安全隐患，因为消息都是由伪造的服务器中转发，如果将要传输的消息中添加一点别的东西，比如木马，病毒之类的东西，或者直接篡改信息内容，就会导致客户端出现极大的安全隐患。对于此漏洞。各个不同的 VPN 都有自己的防护方式，而对于 SD-WAN 虚拟化多功能安全网关来说，解决方法是：进行多项认证。SD-WAN 虚拟化多功能安全网关有明匙，暗匙，与主机专有指纹来进行验证，消息采用 md5 加密技术加密，对于认证不通过的主机不给予解密秘钥。

传统 VPN 都要在服务端和服务端网关的路由同时部署，并且是将服务端个服务网关分开的。如果服务端所在网络段有黑客伪造的主机或者已经被黑客侵入的主机，那么网络的安全就会岌岌可危。而 SD-WAN 虚拟化多功能安全网关的路由采用的是 VyOS 软路由，并使用 KVM 技术将其实例化出来，实现了服务端与服务端路由合二为一，使得 VPN 专有网络的安全大大的提升了。可以说 SD-WAN 虚拟化多功能安全网关的诞生就是解决了目前各大 VPN 技术存在的网络安全漏洞。

2.7 网络安全的重要性

随着移动互联网技术的不断发展，经济和生活中越来越多的同行网络参与，人们的生活享受到了这种便利，但是近几年信息泄露事件的发生频率也越来越高，各种网络安全事件层出不穷。

2017 年 2 月，俄罗斯黑猫黑客“Rasputin”利用 SQL 注入漏洞获得了系统访问权限，黑掉了 60 多所大学和美国政府机构的系统；同年 4 月，BBC 新闻报道洲际酒店超过 1000 家旗下酒店遭遇支付卡信息泄露问题，这是当年 2 月洲际酒店选不遭遇黑客影响后再次受到相同的攻击。同年 5 月，WannaCry 勒索病毒全球爆发，以类似于蠕虫病毒的方式传播，攻击主机并加密主机上存储的文件，这一病毒爆发后，至少 150 个国家、30 万名用户中招，

造成损失高达 80 亿美元，已经影响到金融、能源、医疗等从多企业的管理问题。

在 16 年，习近平总书记指出“加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑力”和“没有网络安全，就没有国家安全”的重要网络安全观。并在同年 12 月 15 日，国务院发布《“十三五”国家信息化规划》中提出，要全天候全方位感知网络安全态势。加强网络网络台是感知、监测预警和应急处置能力建设。

网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进。从世界范围看，网络安全威胁和风险日益突出，并日益向政治、经济、文化、社会、生态、国防等领域传导渗透。特别是国家关键信息基础设施面临较大风险隐患，网络安全防控能力薄弱，难以有效应对国家级、有组织的高强度网络攻击，这对世界各国都是一个难题。

网络安全工作对于国家经济、国家安全以及企业发展的重要性无须赘述。所以网络安全是最大的“命门”，我们要维护网络安全，必须打好核心技术攻坚战，强化关键信息基础设施安全保护、提升态势感知和应急处理能力、加强数据安全和个人信息保护，确保技术先进、治网权尽在掌握、网络安全坚不可摧。

三、项目计划

3.1 团队介绍

团队名称：Open Studio

队长：谢欧

队员：李红剑　陈奇

3.2 项目计划

首先实现对普华 iSoft-Linux 的优化，以便于 SD-WAN 系统安全应用软件与 iSoft-Linux 内核的兼容，使此能完美与物理设备相结合，并运行在服务器上；在对系统进行优化过后，将 Linux　bridge 部署在系统中，来提供

统一管理物理接口上的网络网卡；再将 VNC 搭建完成之后，开始部署 KVM，创造一个系统虚拟化环境；然后利用 KVM 创造 VyOS 虚拟机，在 VyOS 虚拟机里配置网络，部署 IPSec，来保证网络在 Internet 网络数据传输中的安全性；最在系统中部署 Ansible，来自动化运维所传出的参数，最终能将其进行一键部署，简便快捷。

将软件将实现编程与商业化硬件结合，通过集中管理和软件可编程方式自动部署和管理广域网，加速服务交付，并通过路径优化提升网络性能和可靠性，同时保证数据的安全性。使用户能够零基础自主实施，自主可控地应用本软件。

3.3 项目特点

- 传统 VPN 技术特点

VPN 的英文全称是“Virtual Private Network”，翻译过来就是“虚拟专用网络”。顾名思义，虚拟专用网络我们可以把它理解成是虚拟出来的企业内部专线。它可以通过特殊的加密的通讯协议在连接在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条专有的通讯线路，就好比是架设了一条专线一样，但是它并不需要真正的去铺设光缆之类的物理线路。这就好比去电信局申请专线，但是不用给铺设线路的费用，也不用购买路由器等硬件设备。

而我们针对传统 VPN 技术在企业实施过程中做了以下分析：

1. 费用低廉。

与任何传统的广域网相比，VPN 的运营成本和连接远程用户的成本更低。此外，VPN 的固定通讯成本有助于企业了解其经营开支。一个 VPN 线路还能够提供低成本的全球网络机会。

分析：企业不能直接控制基于互联网的 VPN 的可靠性和性能。机构必须依靠提供 VPN 的互联网服务提供商保证服务的运行。这个因素使企业与互联网服务提供商讨价还价签署一个服务级协议非常重要，要签署一个保证各种性能指标的协议。

2. 安全性。

VPN 能提供高水平的安全，使用高级的加密和身份识别协议保护数据避免受到窥探，阻止数据窃贼和其他非授权用户接触这种数据。

分析：企业创建和部署 VPN 线路并不容易。这种技术需要高水平地理解网络和安全问题，需要认真的规划和配置。因此，选择互联网服务提供商负责运行 VPN 的大多数事情是一个好主意。

3. 兼容性。

设计良好的宽带 VPN 是模块化的和可升级的。这种技术能够让应用者使用一种很容易设置的互联网基础设施，让新的用户迅速和轻松地添加到这个网络。这种能力意味着企业不用增加额外的基础设施就可以提供大量的容量和应用。

分析：不同厂商的 VPN 产品和解决方案总是不兼容的，因为许多厂商不愿意或者不能遵守 VPN 技术标准。因此，混合使用不同厂商的产品可能会出现技术问题。另一方面，使用一家供应商的设备可能会提高成本。

4. 可用性和用户操作便捷和可控性

VPN 能够让移动员工、远程员工、商务合作伙伴和其他人利用本地可用的高速宽带网连接(如 DSL、有线电视或者 WiFi 网络)连接到企业网络。此外，高速宽带网连接提供一种成本效率高的连接远程办公室的方法。

分析：当使用无线设备时，VPN 有安全风险。在接入点之间漫游特别容易出问题。当用户在接入点之间漫游的时候，任何使用高级加密技术的解决方案都可能被攻破。幸运的是有一些能够解决这个缺陷的第三方解决方案

- 虚拟化多功能安全网关的特点

1. 简易、便捷性。

相比传统的 VPN，本软件做到了简便，并无太多复杂的操作，能使并不太了解本技术的人也能轻易的使用本软件，界面设计简洁明了，用户仅需要输入几个字段就能轻松连接到专有的子网。

2. 服务端部署简便

本软件利用 Ansible 自动化运维工具实现了传统 VPN 繁杂参数的一键传输，服务搭建也只需使用专有的一键部署脚本，轻松部署。这能让更多的人能接触到 VPN，能让更多人能搭建出 VPN 服务，而不仅仅是网络工程师才能实现。

3. 本软件最着重的点在于网络的安全上面。

在网络安全方面，SD-WAN 虚拟化多功能安全网关就非常出色了。接下来将用几个网络安全漏洞来举例子说明 SD-WAN 虚拟化多功能安全网关在安全方面的防护。

1）记录了必经之路每一条路由的 MAC 地址，每一个路由在转发消息的时候会先确认对端 MAC 地址与对应的 IP 地址是否一致，确认一致再进行转发，如果出现异常会立即断开 VPN 网络的连接。

2）进行多项认证。SD-WAN 虚拟化多功能安全网关有明匙，暗匙，与主机专有指纹来进行验证，消息采用 md5 加密技术加密，对于认证不通过的主机不给予解密秘钥。

3）SD-WAN 虚拟化多功能安全网关的路由采用的是 VyOS 软路由，并使用 KVM 技术将其实例化出来，实现了服务端与服务端路由合二为一，使得 VPN 专有网络的安全大大的提升了。可以说 SD-WAN 虚拟化多功能安全网关的诞生就是解决了目前各大 VPN 技术存在的网络安全漏洞。

3.4 具体分工

序号	标 题 名 称	负责人
1	iSoft-Linux 操作系统部署	谢欧
2	Linux Bridge 的部署	谢欧、陈奇
3	VNC+KVM 的部署	谢欧、李红剑
4	VyOS 虚拟机+IPSec 的部署	陈奇、李红剑
5	Ansible 的运维部署	李红剑
6	Python GUI 界面编写	陈奇
7	后期优化测试	陈奇、李红剑

表一：具体分工表

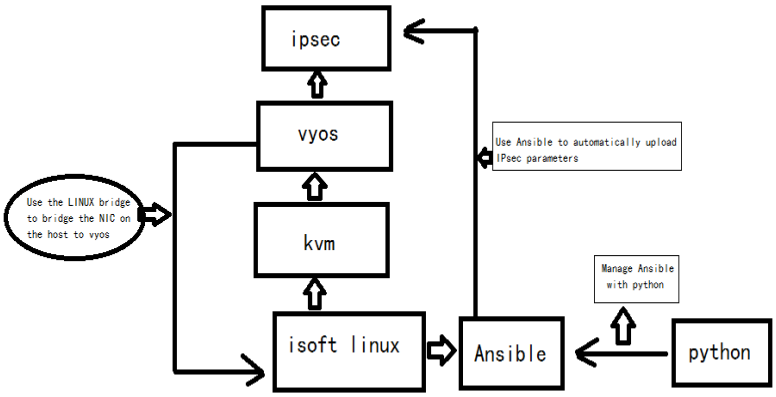
四、项目实施

4.1 软件构成

Python GUI 界面	软件实施层
KVM+VyOS+IPSec+Ansible	应用环境层
ISoft-Linux 操作系统	操作资源层
PC+交换机+千兆路由器	硬件资源层

表二：项目构成表

4.2 项目构架



图三:整体构架图

此项目将在 iSoft-Linux 上实施完成，在 iSoft-Linux 上部署 KVM，将 VyOS 网络操作系统实例化为一台虚拟机，这样就能使服务端与服务路由一体化，解决了一些网络安全上的问题，利用 linux bridge 将 iSoft-Linux 上的真实网关桥接到软路由 VyOS 上，实现了虚拟软路由 VyOS 可以进行路由转发，在 VyOS 上部署 IPSec(VPN 隧道)，实现了软件最终的功能。再在 iSoft-Linux 上部署 Ansible 自动化运维工具，实现 IPSec 冗杂参数的自动传输，在使用 python 脚本语言编写脚本控制管理 Ansible,使用户能轻松，便捷的使用本软件。

4.3 应用领域

本软件适用于各大企业运维人员，安全便捷的运维服务器。利用端到端的 VPN 技术实现了 2 个不同子网的相互连接。取代了以往运维要在公司使用专有网络的麻烦行为，让运维工程师在家也能轻松的管理企业中的各种服务器。本软件也适合学习，由于本软件是完全开源的，适合网络工程师学习参考。本软件同样也是科学上网技术的一种选择，能更加安全的科学上网，而不用担心墙外黑客的入侵。

4.4 项目实施

- 4.4.1 Kvm 的搭建和 VyOS 虚拟机的安装

1. KVM

1) 检查 CPU 是否支持虚拟化：grep vmx /proc/cpuinfo

2) 确保 BIOS 里开启虚拟功能，即查看是否加载 KVM 模块：lsmod | grep kvm

3) 安装 libvirt 及 KVM:

（需以下几个安装包）

libcanberra-gtk2	qemu-kvm.x86_64
qemu-kvm-tools.x86_64	libvirt.x86_64
libvirt-cim.x86_64	libvirt-client.x86_64
libvirt-java.noarch	libvirt-python.x86_64
libiscsi-1.7.0-5.el6.x86_64	dbus-devel
virt-clone	tunctl
virt-manager	libvirt
libvirt-python	python-virtinst

4) 启用 libvirt：systemctl enable libvirtd systemctl start libvirtd

5) 使用 virt-manager 管理 kvm（通过 VNC 连接服务器）

//virt-manager

步骤一：这里我们选择本地安装介质 ISO

步骤二：选择我们在/home/iso 文件下的镜像文件

步骤三：选择 CPU 和内存大小

步骤四：为虚拟机添加磁盘大小

步骤五：点击完成，完成虚拟机的创建

6) 用 virt-install 命令创建虚拟机（新建两个目录分别存放 ISO 文件和虚拟磁盘，我这里在/opt 下新建了 iso 和 kvmimg 目录

mkdir /opt/iso

mkdir /opt/kvmimg

wget

http://packages.vyos.net/iso/release/1.1.8/vyos-1.1.8-amd64.iso

7) 安装完毕（补充）

virsh list –all //可以发现 VyOS 状态是 running

如果发现虚拟机的状态为 shut off，需要手动启动。

virsh start VyOS

systemctl restart network//用 vnc 登录到 VyOS，重启网络获取 IP 地址，至此 VyOS 就可以正常使用了

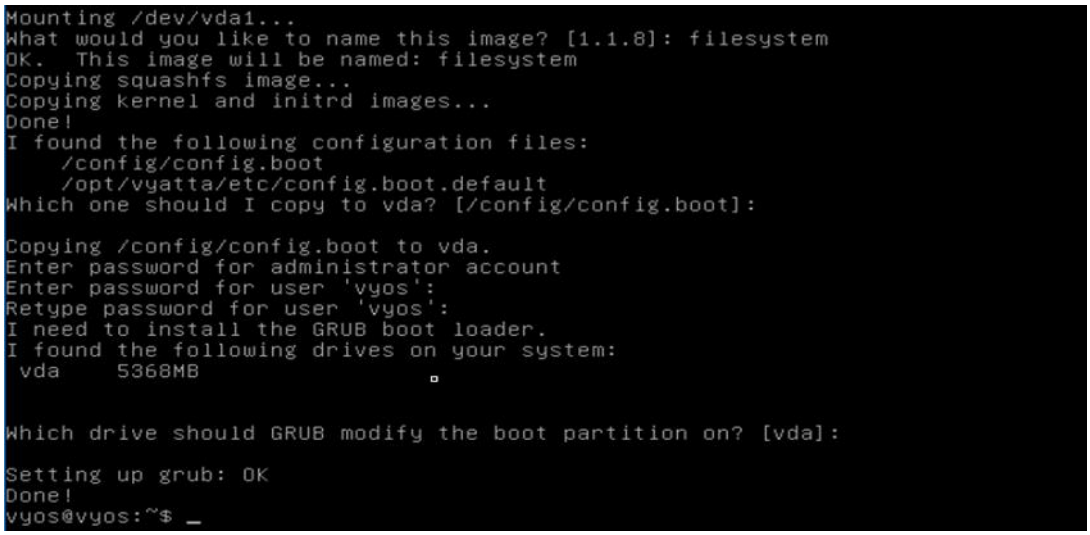
2. Vyos

下载地址：http://packages.vyos.net/iso/release/选择你需要的版本，当前最新版本号 1.1.7，另外其也提供了 OVA 的格式，可以直接部署到 vmware 等平台上。这里说下 iso 镜像安装方式，wiki 上也有详细的安装手册：http://vyos.net/wiki/User_Guide

1) 运行 install image 安装：

install image

安装过程很简单，基本一路回车用默认配置即可，中间需要配置 vyos 用户的密码，安装成功后用的就是 VyOS 这个用户进行系统配置，提示 Setting up grub:OK，即安装成功，之后卸载 CDROM，reboot 重启之后就可以进行系统配置：



- 4.4.2 IPSec、Python 以及 Ansible 的配置

1. IPSec、python

在前面已有了 IPSec 和 Python 的相关配资，在这里就不做介绍

2. Ansible

ansible 是一个基于 python 开发的自动化运维工具！（saltstack）

其功能的实现是基础 SSH 远程连接服务的

ansible 可以实现批量系统配置、批量软件部署、批量文件拷贝、批量运行命令等功能

1） 安装：

i. 管理端：

yum install ansible -y

ii. 被管理端：

yum install libselinux-python -y //被管理端安装软件（被管理端需要关闭 selinux）

PS：如果关闭 selinux，那么被管理端可以不安装（建议安装）

2） 创建密钥对：ssh-keygen -t rsa

```
[root@test1 ~]# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:8SLSr3jzyKujfCNEz6yrJwbgKLjzrCSODeYPmGp+mFc root@test1
The key's randomart image is:
+---[RSA 2048]----+
|                 |
|                 |
|         .       |
|. .   .   o      |
|=. +. o S .      |
|*o. +E o .       |
|B*o..    .       |
|%X=o+ooo         |
|O@@*o==+.        |
+----[SHA256]-----+
```

3) 分发密钥对：ssh-copy-id -i /root/.ssh/id_rsa.pub 10.17.107.225

```
[root@test1 ~]# ssh-copy-id -i /root/.ssh/id_rsa.pub 10.17.107.225
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa
.pub"
The authenticity of host '10.17.107.225 (10.17.107.225)' can't be established.
ECDSA key fingerprint is SHA256:xBYNOe8P4sLkPB+K3AyfcAXIdhxRlLS4F+PncA9hOPs.
ECDSA key fingerprint is MD5:43:0d:d9:08:78:2c:aa:fe:0d:50:8f:7b:0e:86:42:f1.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that
 are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to instal
l the new keys
root@10.17.107.225's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh '10.17.107.225'"
and check to make sure that only the key(s) you wanted were added.
```

4) 登陆验证：ssh 10.17.107.225

```
[root@test1 ~]# ssh 10.17.107.225
Last login: Mon Oct 22 22:02:24 2018 from 10.17.164.79
[root@test2 ~]#
```

登陆测试成功

5) 进行 Ansible 批量管理：ansible host -m command -a 'uptime'

```
[root@test1 ~]# ansible host -m command -a 'uptime'
```

PS： 查看的是 host 主机组，模块为 command，的主机负载信息

host #主机组

-m #指定模块参数（command 为默认模块，不写也可以）

command #模块名称

```
-a    #指定利用模块执行的动作参数，-a 后面的是要执行的命令
uptime #批量执行的命令
```

五、总结

面对今天的信息技术革命，网络的信息中心的安全已成为主要的技术关注点。如今信息安全问题被上升到国家战略层面，在 2017 年，举行“网络技术高峰论坛”，业内大腕聚焦网络安全。中央网信办副主任杨小伟在会上表示，网络信息技术革命和产业变革正在孕育兴起，科技创新呈现出新的发展态势和特征，对整个经济社会发展的融合、渗透、驱动作用日趋明显，深刻改变着人们的生产生活方式，带来的网络安全风险和挑战也不断增大。网络攻击、网络窃密、网络欺诈、侵害公民个人信息等现象频发，网络安全已成为事关经济社会发展、国家长治久安和人民群众福祉的重大战略问题。要立足开放环境维护网络安全，维护网络安全要正确处理开放和自主的关系，树立全球视野和开放心态，坚持自主创新，最大程度利用网络空间发展潜力。

为了迎合当今信息产业安全技术应用作为导向，以“网络空间，坚如磐石”为主题构想，借助企业级安全操作系统实现既定安全等级保护业务的系统安全加固。我们设计出了基于普华操作系统的 SD-WAN 云应用系统，实现企业应对信息时代对数据的处理和对网络的统一化管理，既满足创新性、适用性、设计合理性、稳定性、安全性和自主可控性等多种特点，以及数据安全的保护要求。