Software Engineering and Applications 软件工程与应用, 2021, 10(3), 321-328
Published Online June 2021 in Hans. http://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2021.103036

Hans汉斯

基于VPN的公司总部与分部的互连网络

曹　瑞，黄金城，张雅恒

盐城工学院，江苏　盐城
Email: 16792417@qq.com

收稿日期：2021年5月19日；录用日期：2021年6月14日；发布日期：2021年6月21日

摘　要

随着规模的扩大，很多公司都设置了分支机构，如何实现公司总部与分支机构的网络资源共享，同时又保证内部数据安全传输，是一个非常重要的课题。VPN技术在网络安全领域发挥着重要的作用，本文提出了一种基于VPN的公司总部与分部的互连网络，运用虚拟机与模拟器对网络的拓扑机构进行了设计，对网络的运行进行了模拟。

关键词

网络安全，虚拟机，VPN网络，IPSec协议，虚拟机

A Corporate Headquarters and Corporate Branches Network Based on VPN Technology

Rui Cao, Jincheng Huang, Yaheng Zhang

Yancheng Institute of Technology, Yancheng Jiangsu
Email: 16792417@qq.com

Received: May 19th, 2021; accepted: Jun. 14th, 2021; published: Jun. 21st, 2021

Abstract

With the expansion of development, many companies have headquarters and branches. The network between the headquarters and branches should be built and the network transmission security should be ensured. VPN technology plays an important role in network security. This paper proposes a corporate headquarters and corporate branches network based on VPN technology, the virtual machine and simulator are used to realize the topology design and operation of the

文章引用: 曹瑞, 黄金城, 张雅恒. 基于 VPN 的公司总部与分部的互连网络[J]. 软件工程与应用, 2021, 10(3): 321-328.
DOI: 10.12677/sea.2021.103036

network.

Keywords

Network Security, Simulator, VPN network, IPSec Protocol, Virtual Machine

1. 引言

随着公司业务的拓展，企业需要在公司总部以外设置各种分支机构，网络成为了多数公司总部与分部之间数据传输的必备桥梁。为了提升公司自身的数据的传输效率及数据的安全性，加强公司网络的安全建设必不可少，一个性能高效、安全稳定的网络能使得企业公司能够平稳运行，提高企业的工作效率[1]。

VPN 是一种能在公共网络中建立的一种专用数据通道，目前该技术在大型公司和企事业单位得到了广泛的使用，但由于网络安全设备的成本较高，一些技术诸如 ACG 及防火墙等较为复杂，使得该技术很难在中小公司应用[2]。

本文提出一种基于 VPN [3]的公司总部与分部的互连网络，该网络设备少，通过简单的配置可以很方便的更改 VPN 连接，在公网上建立起如同专线一样的效果，产生了与 NAT 不同的效果，能够保证数据的安全。该网络使用 SSL [4]作为安全协议，可以为基于 TCP 技术的数据进行安全的传输。SSL VPN 是以 SSL 的安全技术如认证加密等手段为基础开发出的 VPN 技术。SSL VPN 主要是通过先连接到公司总部的网关然后再通过网关对内部资源访问[5]，安全主要依靠它自身的加密等技术。具体为先在 SSL VPN 网关上创建接口，并配置能够发给客户端的路由表。用户使用客户端登录后，对网关进行连接，在经历了认证和授权后，网关会给虚拟网卡分配一个 IP 地址，再将可接入 IP 资源发给客户端。在客户端对资源进行访问时，报文会被 SSL 封装，在通过虚拟网卡发送到网关上，网关在解析后转发给服务器，服务器会产生报文再通过网关的帮助下发给客户端。该网络具有实现简单、成本低的特点，能够满足大部分中小公司的要求，对中小公司的 VPN 网络的普及具有重要的理论意义和实际价值。

2. 网络设计

2.1. 拓扑图

图 1 为运用虚拟机与模拟器实现的网络拓扑图，该网络将防火墙作为网关边缘设备，用到了核心交换机、接入交换机、POE 交换机、AC 控制器、无线 AP 等设备，模拟了公司本部和公司分部的 VPN 连接。公司总部网络采用由防火墙连接到核心交换机，再由核心交换机连接到接入交换机，最后由接入交换机连接到用户主机或无线 AP 的网络架构。公司分部网络采用由防火墙到接入交换机，接入交换机再连接到用户主机或无线 AP 的网络架构。虽然图中只有一个分部，但很容易据此推广到多分部的情形，下面不再累述。

2.2. 防火墙

防火墙采用 H3C SecPath F1000-AK115，该设备吞吐量达到 2 G，每秒新建连接数可以达到 2 万，并发连接也能达到 50 万，适用于中小公司的环境下使用。该防火墙支持 IPSec、L2TP、SSL VPN 满足了公司对于访问数据的需求，它能够基于地址等属性，配置入侵防御、防病毒、文件过滤、数据过滤、URL 过滤、

会话老化时间、日志记录等高级访问控制功能用来保护数据安全。同时防火墙还能实现对安全区域进行划分，对控制列表进行访问，配置策略保证数据的流向，动态的对无用的数据包进行过滤，创立黑名单禁止某些用户的访问，使 MAC 地址和 IP 地址绑定，基于 MAC 地址的对访问的 IP 地址进行限制创建列表等功能。

防火墙支持对 DDoS 攻击进行的防护，可以抵御多种多样的攻击，如 SYN flood 等攻击手段。它还拥有一些上网行为管理的功能，可以对一些常见的应用进行控制。也拥有一些行为审计的功能，可以对所作的事情进行记录。它支持的 web 页面管理也是一大亮点，因为这个我们可以不用特别对命令行深入了解，通过网页方式无疑大大降低了维护人员上手的难度。

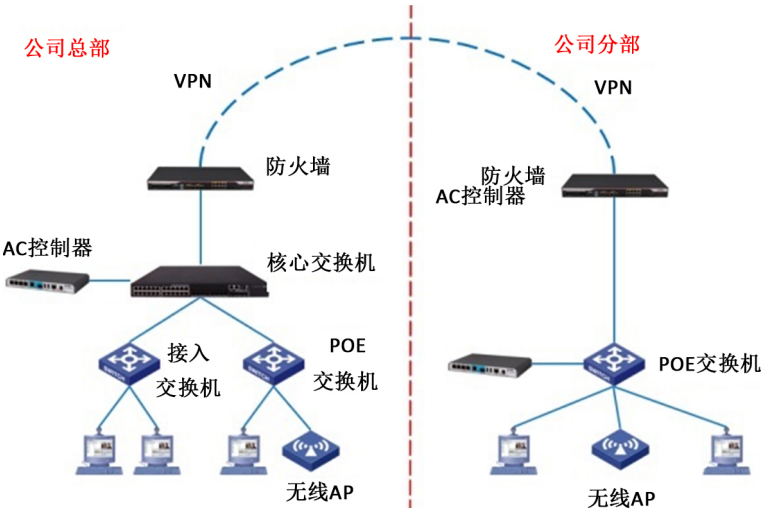

Figure 1. The topology of the network
图 1. 网络拓扑图

2.3. 接入交换机

5130S-52P-EI 这个型号作为接入交换机，他属于弱三层的交换机，支持 OSPF 等多数的三层协议，拥有 48 个千兆电口，减少了对核心交换机的端口数要求，与所选的核心交换机类似该设备也能使用智能管理平台利用图像化的界面方便管理。同时该设备支持对 ARP 攻击防御等安全技术来保护通信安全。

2.4. POE 交换机

网络选择 5130S-28P-PWR-EI 作为 POE 交换机，它的供电要求只有 185 W，供电功耗相对较低同时又能满足一般用户无线覆盖所需 AP 的供电要求。

2.5. 无线选型

网络选择 AC 控制器中性价比较高的 WX2540H，该设备拥有 1.6 G 转发性能的同时还能够最大管理 48 个 AP，此 AC 控制器还能对一些常见的如 Dos 攻击进行防御。这种 AC 支持专门对于 CPU 的保护机制，能够对发往 CPU 处理的报文进行控制，保证流量的正常，从而保证 AC 控制器能够在各种情况下能够正常工作。

3 设备的配置

3.1. 接口参数配置

将数据的接口打开然后输入对应的 IP 地址，如图 1 左侧的防火墙上面的 g1/0/2 接口 Int g0/2

进入接口

Ip add 192.168.1.1　255.255.255.0

将地址设为 192.168.1.1，后面是掩码地址。

作为一个 24 网络位地址，当公司网络规模较大时，还可以通过借用主机位的方式增加我们可以使用的网段数量。

3.2. 路由配置

在输入各个接口后，将各个接口的地址宣告进 OSPF 协议[6]之中，具体如下：

OSPF 1

创建 OSPF

Area 0

创建骨干区域 0

Net 192.168.1.1 0.0.0.0

将地址信息录入 OSPF 路由表中

OSPF 是常见的一种动态协议，通过有关于区域的定义对路由进行管理，必须使用 area0 才能够将不同区域连接起来，从而相互传输数据。

在防火墙处配置一个用来访问外网的静态路由

IP route-static 0.0.0.0 0.0.0.0 1.1.1.2

完成上述操作，公司的总部的网络之间和公司分部的网络之间可以分别连通了。

3.3. 进入 WEB 页面

使用自带的 web 界面对防火墙进行配置，这里需要先把地址改成与管理口同一网段的地址，因为只有当主机的地址与要接入的端口地址在一个网段时才能通信，本网络中这个的地址是 192.168.0.1。

将防火墙管理口 g1/0/1 连接到主机的网口，然后再输入

security-zone name Trust

import interface g1/0/1

创建一个名为 Trust 的安全域并且将 g1/0/1 加入此安全域，防火墙拥有安全域的概念，只有不同的安全域才能进行访问，通过将各种接口划分进去，可以更加方便的对网络进行管理，增强安全性能

[H3C]object-policy ip ma

[H3C-object-policy-ip-ma]rule pass

创建策略并且使得流量可以得到顺利的通行

[H3C]zone-pair security source trust destination local

[H3C-zone-pair-security-Trust-Local]object-policy apply ip　ma

在 trust 安全域和 local 安全域之间使用刚刚写好的名为 ma 有利于流量的策略

[H3C]ip http en

[H3C]ip https en

local-user admin class ma

password simple admin

service-type http https

authorization-attribute user-role network-admin

创建一个管理员账号作为我们登录的依据，同样的要使用 http 协议，最下面那句是为了说明创建的是管理员用户。

接下来的图形化界面是为了建立 IPSEC，是一种加密，但并没有建立起隧道。如图 2 所示，在出现的登录防火墙的界面上，用上面设置的用户账户登进去。

Figure 2. Login screen
图 2. 登录界面

将接口手动输入 IP 地址，并划分到 untrust 安全域中，如果操作出了问题也可以在防火墙命令行输入下面内容：

Int g1/0/2

Ip add x.x.x.x

Int 后面的内容要根据对应的链路接口修改，IPadd 后面加上实际的地址和掩码。

最后再根据之前进入 web 界面的配置加入安全域，配置安全策略，使安全域间互通，因为默认安全域之间是不会互通的。

3.4. IPSEC 的配置

为了协商算法和密钥的存在时间，首先需要配置一个 IKE 提议[7]，配置 IPSEC 主要用来建立总部和分部的连接隧道。

Figure 3. VPN tunnel
图 3. VPN 隧道

使用 OSPF 将所有网络全部连接起来，在 VPN-IPSEC 监视视图中会出现如图 3 的效果。

3.5. GEE 隧道

使用 GRE 的隧道技术使得网络能够互相通信[8]。配置如下

interface tunnel 0 mode gre	配置一个隧道端口并将隧道模式设为 GRE
ip address 10.5.1.2 255.255.255.0	对隧道地址进行配置
source 1.1.1.1	设置本端端口为源端口
destination 2.2.2.2	设置对端端口为目的地址
security-zone name Untrust	
import interface Tunnel 0	将隧道配置到安全域中

3.6. L2tp 配置

l2tp enable	允许 l2tp 协议
l2tp-group 1 mode lac	创建组 1 是 lac 模式
tunnel name LAC	配置隧道名称为 tun
lns-ip 2.2.2.2	对端地址为 2.2.2.2
tunnel authentication	打开隧道检验
tunnel password simple 123	设置隧道密码为 123
interface virtual-ppp 1	建立虚拟接口
ip address ppp-negotiate	地址由对端发送
ppp pap local-user vpn password simple qwe	验证用户名为 vpn，密码是 qwe，使用 pap 验证
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2	配置默认路由使得两个网关出口地址可以通信
interface virtual-ppp 1	进入虚拟口
l2tp-auto-client l2tp-group 1	使用组 1 建立连接，然后是右侧防火墙配置
local-user vpn class network	创建本地用户 vpn
password simple qwe	密码是 qwe
service-type ppp	使用 ppp 协议，创建接口 Virtual-Template1，配置 VT

口 IP 地址，PPP 认证方式为 PAP，并指定为 Client 端分配 IP 地址为 192.168.0.10。

interface virtual-template 1	创建虚拟口
ip address 10.10.10.10 24	地址为 10.10.10.10
ppp authentication-mode pap	使用 pap 验证
remote address 10.10.10.1	对端地址发送 10.10.10.1
security-zone name Untrust	
import interface Virtual-Template 1	将虚拟口划分进安全域
acl basic 2100	
rule permit source any	允许所有流量通过
zone-pair security source untrust destination local	
packet-filter 2100	在从 untrust 到 local 中使用 acl2000
domain system	配置 system 域
authentication ppp local	采用 ppp 本地认证

l2tp enable	打开 l2tp 功能
l2tp-group 1 mode lns	创建 lns 模式的组 1
tunnel name tunnel	隧道名为 tunnel
allow l2tp virtual-template 1 remote LAC tunnel authentication	设置使用的虚拟口配置对端隧道名
tunnel password simple 123	将密码设为 123
router id 1.1.1.1	

3.7. 模拟器实现

通过虚拟机与模拟器，本文中所述的基于 VPN 的公司总部与分部的互连网络的模拟拓扑如图 4 所示，同时模拟结果较好的验证了该网络的有效性和安全性。

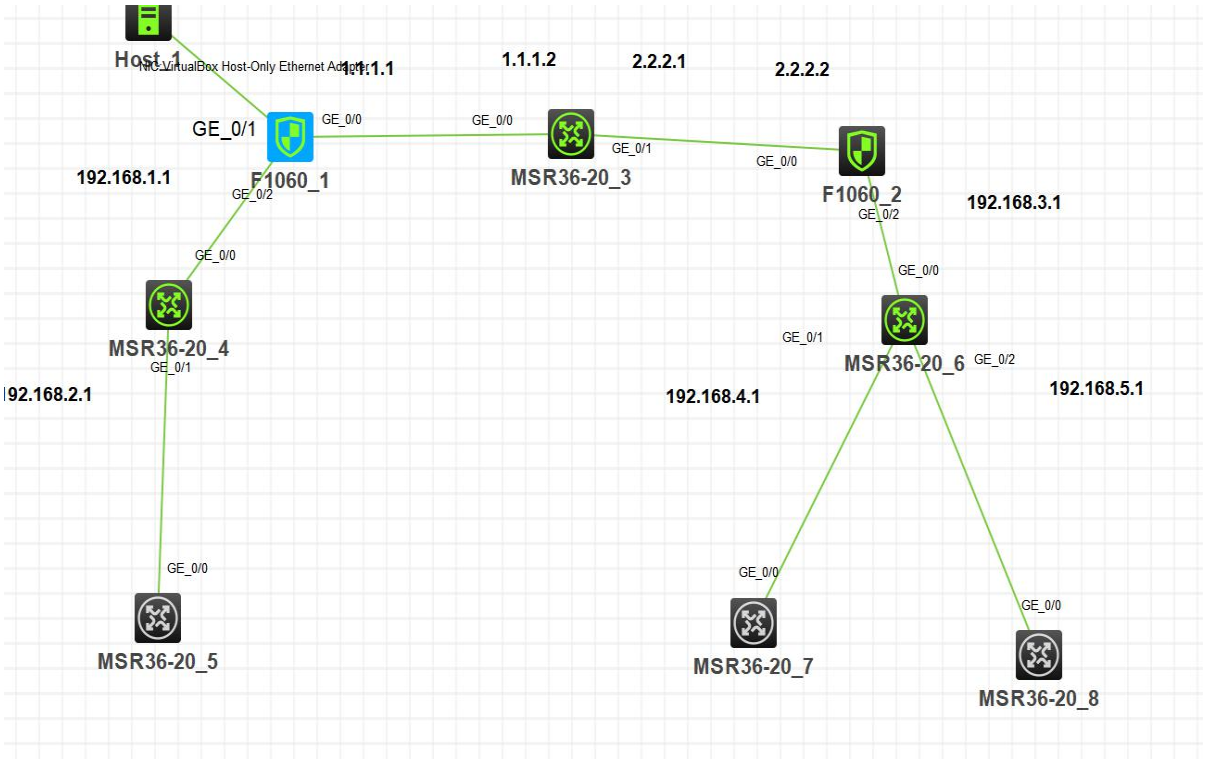

Figure 4. Simulation of topology
图 4. 模拟拓扑图

4. 结语

本文提出了一种于 VPN 的公司总部与分部的互连网络，并用虚拟机与模拟器实现了网络的拓扑设计。文中对网络的各种配置进行了详细说明。该网络可以在少设备、低成本的情况下，为中小公司的总部与分支机构的网络传输提供高效和安全的支持。

参考文献

[1] 龚颖春. 虚拟网络技术在计算机网络安全中的应用[J]. 无线互联科技, 2021, 18(6): 30-31.

[2] 黄金城, 张雅恒, 项慧慧, 田明. 基于 IPSec 协议的点对点 VPN 网络[J]. 软件工程与应用, 2020, 9(4): 278-287.

[3] 秦燊, 劳翠金. 基于虚拟化技术的 IPSec 虚拟专用网络的研究[J]. 江苏通信, 2021, 37(2): 52-54.

[4] 谷小青, 吴金杰, 董安辉, 郑宝周. 基于 TNC 的 SSL VPN 系统的设计[J]. 数字技术与应用, 2019, 37(10): 173-175 + 177.

[5] 李献军, 张少芳, 李岩. 基于 L2TP 的远程访问 VPN 的实现[J]. 电脑知识与技术, 2019, 15(22): 50-52.

[6] 赵占领, 胡威, 韩雨. VPN 安全网关的设计与实现探究[J]. 信息系统工程, 2019(1): 71.

[7] 邹洁, 伍飞. IPSec-IKE 的实现与应用场景分析[J]. 石家庄职业技术学院学报, 2021, 33(2): 9-12.

[8] 薛江波, 胡曦明, 马苗, 李鹏. IPSec VPN 的 NAT 穿越技术与仿真实验[J]. 网络空间安全, 2018, 9(2): 51-55.