(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115529206 A
(43)申请公布日 2022.12.27

(21)申请号 202211209601.4

(22)申请日 2022.09.30

(71)申请人 上海地面通信息网络股份有限公司
地址 200072 上海市静安区永和路318弄10号

(72)发明人 胡益明

(74)专利代理机构 上海科盛知识产权代理有限公司 31225
专利代理师 赵志远

(51)Int.Cl.
H04L 12/46(2006.01)
H04L 9/40(2022.01)
H04L 67/10(2022.01)

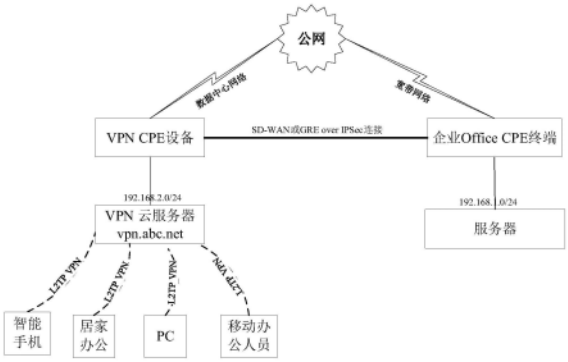
权利要求书1页 说明书4页 附图1页

(54)发明名称

基于拨号云VPN的远程及移动办公协同控制系统及接入方法

(57)摘要

本发明涉及一种基于拨号云VPN的远程及移动办公协同控制系统及接入方法，所述系统包括部署在数据中心的VPN云服务器，其上虚拟出安装有开源VPN软件且与用户一对一对应的VPN虚拟机；所述VPN云服务器前端布置有VPN CPE终端设备，用户办公场所布置有CPE终端设备；所述VPN CPE终端设备和CPE终端设备之间建立有SD-WAN连接或GRE over IPSEC连接；所述CPE终端设备与办公内网服务器连接；其中，数据访问链路环路为：远程拨号IP地址至云VPN服务器的IP分配池，返回路由定义与用户IP VPN实例绑定，并路由到用户端的CPE终端的IPSEC或SDWAN接口上，到达用户内网，形成一条数据访问闭环链路。与现有技术相比，本发明具有成本低、网络安全性高、交付流程简便，无需对客户现有网络架构作出变更的优点。



CN 115529206 A

1.一种基于拨号云VPN的远程及移动办公协同控制系统,其特征在于,所述控制系统包括部署在数据中心的VPN云服务器,其上虚拟出安装有开源VPN软件且与用户一对一对应的VPN虚拟机;

所述VPN云服务器前端布置有VPN CPE终端设备,用户办公场所布置有CPE终端设备;所述VPN CPE终端设备和CPE终端设备之间建立有SD-WAN连接或GRE over IPSEC连接;所述CPE终端设备与办公内网服务器连接。

2.根据权利要求1所述的一种基于拨号云VPN的远程及移动办公协同控制系统,其特征在于,所述CPE终端设备包括防火墙和Router。

3.根据权利要求1所述的一种基于拨号云VPN的远程及移动办公协同控制系统,其特征在于,所述VPN CPE终端设备上设有通过VRF实例绑定的用户接入端口。

4.根据权利要求1所述的一种基于拨号云VPN的远程及移动办公协同控制系统,其特征在于,所述VPN CPE终端设备和CPE终端设备之间的SD-WAN连接或GRE over IPSEC连接均为采用IPSec协议加密认证技术的通信连接。

5.根据权利要求1所述的一种基于拨号云VPN的远程及移动办公协同控制系统,其特征在于,所述VPN CPE终端设备、CPE终端设备分别通过数据中心网络、宽带网络接入公网。

6.根据权利要求1所述的一种基于拨号云VPN的远程及移动办公协同控制系统,其特征在于,所述办公内网服务器包括CRM、OA、NAS文件服务器以及网盘服务器。

7.根据权利要求1所述的一种基于拨号云VPN的远程及移动办公协同控制系统,其特征在于,所述控制系统对应的数据访问链路具体为:

将远程拨号IP地址路由定义到VPN云服务器的IP分配池,在VPN云服务器上绑定到动态分配给远程用户的拨号地址池中,返回路由定义与用户IP VPN实例绑定,并路由到用户办公场所布置的CPE终端设备的IPSEC或SDWAN接口上,到达办公内网服务器,形成一条数据访问闭环链路。

8.一种基于拨号云VPN的远程及移动办公协同控制接入方法,其特征在于,应用权利要求1～7任一项所述的控制系统,所述方法具体为:

移动办公或居家办公用户,PC端上建立PPTP协议或L2TP/IPSec协议到VPN云服务器的拨号连接,PC端上输入VPN连接账号,拨号建立成功后,PC端获取IP地址,网关到VPN云服务器,随后通过缺省路由,数据包经过VPN CPE终端设备,再通过SDWAN或GRE隧道到达用户办公网络的CPE终端设备上,所述CPE终端设备与用户内网交换机互联,查找到网络路由,建立PC端的IP地址和用户办公内网服务器的连接通信关系;访问外网时,再通过用户办公网络防火墙或代理服务器到外网。

9.根据权利要求8所述的方法,其特征在于,所述PPTP协议对应的连接为采用MPPE128位加密的连接。

10.根据权利要求8所述的方法,其特征在于,所述L2TP协议对应的连接为采用IPSec AES256加密算法、SHA2-256哈希认证算法和Pre-Share-Key预共享秘钥的连接。

基于拨号云VPN的远程及移动办公协同控制系统及接入方法

技术领域

[0001] 本发明涉及网络通信技术领域，尤其是涉及一种基于拨号云VPN的远程及移动办公协同控制系统及接入方法。

背景技术

[0002] 现有的企业自建拨号VPN远程或移动协同办公存在以下问题：

[0003] 1)成本高：企业自建VPN需要采购昂贵的SSL VPN防火墙或IPSEC VPN硬件设备，且上述硬件设备还需购买vpn license，成本高，每年的硬件续保及维护费高；同时企业还要向运营商租用互联网专线，但是很多出差或疫情期间居家办公人员的宽带来自各个不同运营商，这就要求企业具备多条专线，同时要分配多个ip来建立VPN连接，带来诸多不便；

[0004] 2)管理不便：客户需要维护VPN硬件设备，认证服务器，企业专线等多个子系统，对客户的技能也提出了更高的要求。

[0005] 针对上述问题，亟需要设计一种更加便捷且成本低廉的远程及移动办公协同控制系统及方法。

发明内容

[0006] 本发明的目的就是为了克服上述现有技术存在的缺陷而提供了一种成本低、网络安全性高、交付流程简便的基于拨号云VPN的远程办公协同控制系统及接入方法。

[0007] 本发明的目的可以通过以下技术方案来实现：

[0008] 根据本发明的第一方面，提供了一种基于拨号云VPN的远程及移动办公协同控制系统，所述控制系统包括部署在数据中心的VPN云服务器，其上虚拟出安装有开源VPN软件且与用户一对一对应的VPN虚拟机；

[0009] 所述VPN云服务器前端布置有VPN CPE终端设备，用户办公场所布置有CPE终端设备；所述VPN CPE终端设备和CPE终端设备之间建立有SD-WAN连接或GRE over IPSEC连接；所述CPE终端设备与办公内网服务器连接。

[0010] 优选地，所述CPE终端设备包括防火墙和Router。

[0011] 优选地，所述VPN CPE终端设备上设有通过IP VPN实例绑定的用户接入端口。

[0012] 优选地，所述VPN CPE终端设备和CPE终端设备之间的SD-WAN连接或GRE over IPSEC连接均为采用IPSec协议加密认证技术的通信连接。

[0013] 优选地，所述VPN CPE终端设备、CPE终端设备分别通过数据中心网络、宽带网络接入公网。

[0014] 优选地，所述办公内网服务器包括CRM、OA、NAS文件服务器以及网盘服务器。

[0015] 优选地，所述控制系统对应的数据访问链路具体为：

[0016] 将远程拨号IP地址路由定义到VPN云服务器的IP分配池，在VPN云服务器上绑定到动态分配给远程用户的拨号地址池中，返回路由定义与用户IP VPN实例绑定，并路由到用户办公场所布置的CPE终端设备的IPSEC或SDWAN接口上，到达办公内网服务器，形成一条数

据访问链路环路。

[0017] 根据本发明的第二方面,提供了一种基于拨号云VPN的远程办公协同控制接入方法,应用任一项所述的控制系统,所述方法具体为:

[0018] 移动办公或居家办公用户,PC端上建立PPTP协议或L2TP协议到VPN云服务器的拨号连接,PC端上输入VPN连接账号,拨号建立成功后,PC端获取IP地址,网关到VPN云服务器,随后通过缺省路由,数据包经过VPN CPE终端设备,再通过SDWAN或GRE隧道到达用户办公网络的CPE终端设备上,所述CPE终端设备与用户内网交换机互联,查找到网络路由,建立PC端的IP地址和用户办公内网服务器的连接通信关系;访问外网时,再通过用户办公网络防火墙或代理服务器到外网。

[0019] 优选地,所述PPTP协议对应的连接为采用MPPE128位加密的连接。

[0020] 优选地,所述L2TP协议对应的连接为采用IPSec AES256加密算法、SHA2-256哈希认证算法和Pre-Share-Key预共享秘钥的连接。

[0021] 与现有技术相比,本发明具有以下优点:

[0022] 相较于传统部署方式,用户需要申请固定ip地址的专线,购买昂贵的VPN设备,自己部署,还需要聘请专业的IT来维护,提高了一般中小企业的运营维护成本;而本发明用户基于拨号云VPN连接企业办公网络,以账号的方式进行交付给客户使用,客户通过远程拨号IP地址至VPN云服务器的IP分配池,返回路由定义与用户VRF实例绑定,并路由到用户办公场所布置的CPE终端设备的IPSEC或SDWAN接口上,到达办公内网服务器,形成一条数据访问链路环路,即客户仅需一个账号即可建立拨号连接实现远程办公,简化了交付流程,对客户现有网络架构不需要做任何变更。

附图说明

[0023] 图1为本发明的系统架构图。

具体实施方式

[0024] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例是本发明的一部分实施例,而不是全部实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例,都应属于本发明保护的范围。

[0025] 实施例

[0026] 首先对本发明的相关术语进行解释说明:

[0027] CPE:指用户前端设备,主要是各类协议转换,实现数据加密,路由交换等一系列复杂的功能;

[0028] VPN云服务器:指通用的x86服务器,经过虚拟化后,分成多个虚机,然后虚机上安装通用Linux操作系统,部署通用的开源L2TP+IPSEC软件,提供客户终端拨号访问,并对拨号通道进行加密、算法和认证等;

[0029] VPN CPE终端设备:指VPN前端CPE设备,通过VRF隔离技术,将不同用户通过RD进行隔离,使每个用户的通道都是相互隔离的,类似于二层电路的虚通道VPI/VCI,以太网的VLAN ID等功能。

[0030] SDWAN:软件定义广域网,通过SDWAN技术实现两台CPE设备之间的数据安全通道连接;

[0031] GRE over IPSec:加密隧道协议,通过加密隧道技术实现两台CPE设备之间的数据安全通道连接;

[0032] 服务器:指用户内网运行财务软件、CRM软件、文件服务器或网盘服务器,供用户移动或居家办公远程连接用的,一般企业内部服务器都是放在内网的,不允许部署公网之上,避免被攻击,窃取数据。

[0033] 如图1所示,本实施例给出了一种基于拨号云VPN的远程及移动办公协同控制系统,所述控制系统包括部署在数据中心的VPN云服务器,其上虚拟出安装有开源VPN软件(部署PPTP和L2TP VPN软件)且与用户一对一对应的VPN虚拟机,即每个客户对应一台逻辑上独立的VPN虚拟机,通过IP VPN技术对不同用户进行隔离,做到每个客户相互隔离;所述VPN CPE终端设备上设有通过VRF实例绑定的用户接入端口。

[0034] 所述VPN云服务器前端布置有VPN CPE终端设备,用户办公场所布置有CPE终端设备(如防火墙、Router等网关设备互联);所述VPN CPE终端设备和CPE终端设备之间建立有SD-WAN连接或GRE over IPSEC连接,且VPN CPE终端设备、CPE终端设备分别通过数据中心网络、宽带网络接入公网。

[0035] 所述CPE终端设备与办公内网服务器连接。其中,办公内网服务器包括CRM、OA、NAS文件服务器以及网盘服务器。所述VPN CPE终端设备和CPE终端设备之间的SD-WAN连接或GRE over IPSEC连接均为采用IPSec协议加密认证技术的通信连接。

[0036] 所述控制系统对应的数据访问链路具体为:将远程拨号IP地址路由定义到云vpn服务器的IP Pool分配池,在VPN云服务器上绑定到动态分配给远程用户的拨号地址池中,其中PPTP连接拨号池IP范围为192.168.2.2-192.168.2.127,L2TP连接拨号池IP范围定义为192.168.2.128-192.168.2.255,返回路由定义与用户VRF实例绑定,并路由到用户办公场所的CPE终端设备的IPSec或SDWAN接口上,到达用户内网,形成一条数据访问链路环路。

[0037] 接下来,给出一种基于拨号云VPN的远程办公接入方法,应用所述的控制系统,所述方法具体为:

[0038] 移动办公或居家办公用户,PC端上建立PPTP协议或L2TP协议到VPN云服务器的拨号连接,PC端上输入VPN连接账号,拨号建立成功后,PC端获取IP地址,网关到VPN云服务器,随后通过缺省路由,数据包经过VPN CPE终端设备,再通过SDWAN或GRE隧道到达用户办公网络的CPE终端设备上,所述CPE终端设备与用户内网交换机互联,查找到网络路由,建立PC端的IP地址和用户办公内网服务器的连接通信关系;访问外网时,再通过用户办公网络防火墙或代理服务器到外网。

[0039] 所述PPTP协议对应的连接为采用MPPE128位加密的连接。所述L2TP协议对应的连接为采用IPSec AES256加密算法、SHA2-256哈希认证算法和Pre-Share-Key预共享秘钥的连接。

[0040] 对于附图1中VPN云服务器中的vpn.abc.net,其中abc为泛指。

[0041] 以上所述,仅为本发明的具体实施方式,但本发明的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本发明揭露的技术范围内,可轻易想到各种等效的修改或替换,这些修改或替换都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应以权利

要求的保护范围为准。

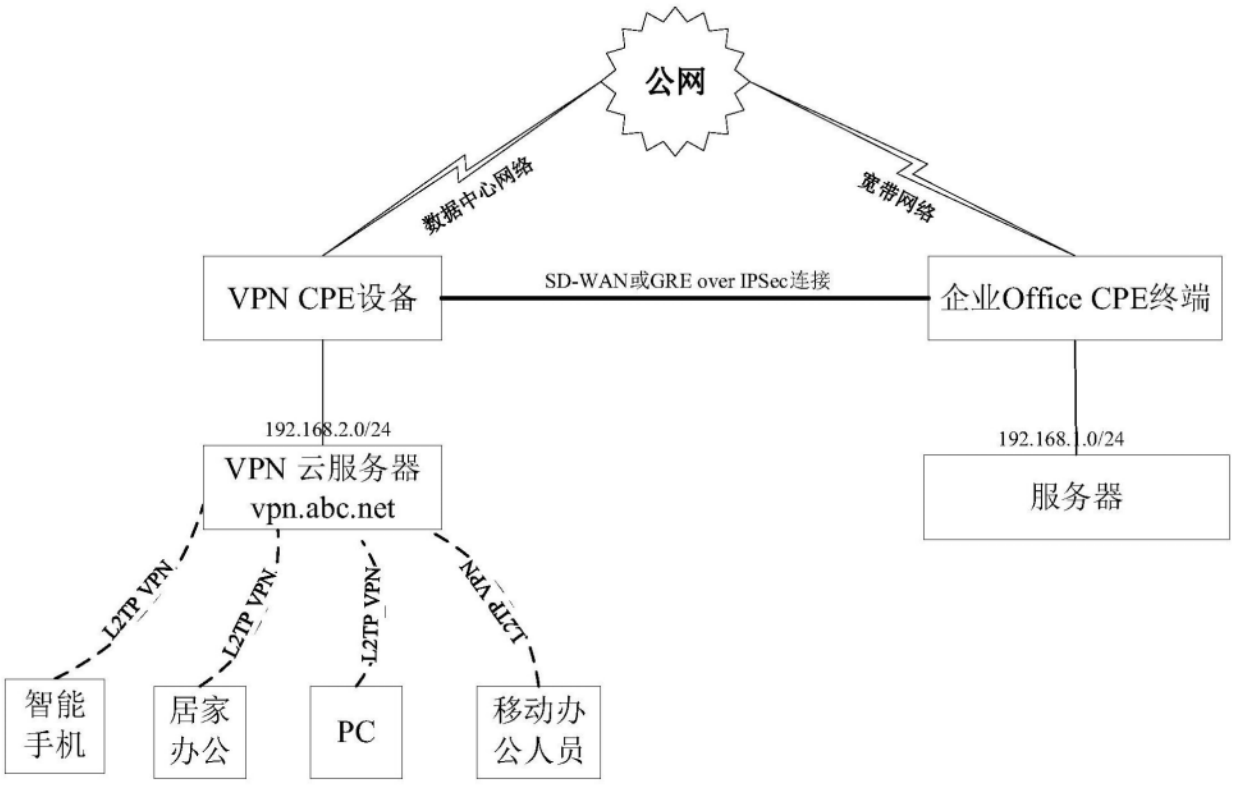

公网
数据中心网络
宽带网络
VPN CPE设备
SD-WAN或GRE over IPSec连接
企业Office CPE终端
192.168.2.0/24
VPN 云服务器
vpn.abc.net
192.168.1.0/24
服务器
L2TP VPN
L2TP VPN
L2TP VPN
L2TP VPN
智能手机
居家办公
PC
移动办公人员

图1