

NetRock® 防火墙

NetRock 防火墙是华城技术有限公司基于多年对网络安全各方面深刻的理解，并积极跟进业界最新技术发展而开发出的一款集网络接入、防火墙、VPN、流量整形、认证授权、内容安全控制、ADSL 接入安全等技术于一身的网络安全智能防御系统。NetRock 防火墙基于专门设计的硬件平台，以华城技术自行定制的安全操作系统为核心，提供高度安全、可信和健壮的安全解决方案，真正实现了单一设备对您的网络的全方位防护。

NetRock -500 系列是当今可应用最广的防火墙，它集成 4 或者 6 个 10/100M 自感应端口，在传统防火墙内、外、DMZ 的基础上增加了一到三个物理端口供灵活配置，用户可根据需要将其设定成 IDS 镜像口、带外管理口或 HA 心跳口，或不做任何配置默认作为流量通讯过滤口使用，是专为大中型企业设计的提供灵活解决方案的产品。

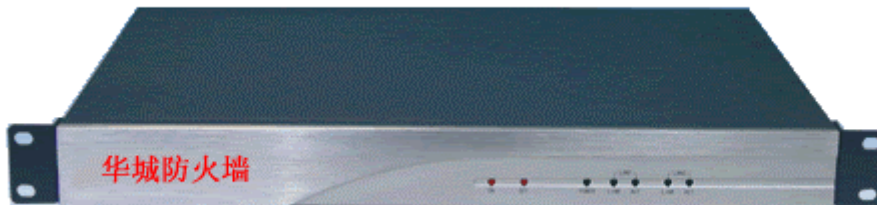


图 1 NetRock-500 防火墙外观图

功能特性

IPSec VPN 支持

基于 IPSEC 协议的 VPN 完全兼容并符合 IPSEC 标准定义，从而保证了与其它支持 IPSEC 的系统和设备的互联互通。支持手工密钥和自动密钥两种协商方式并支持 DES、3DES、AES、Blowfish、Twofish、Serpent 等多种加密算法和 MD5、SHA1、SHA2_256、SHA2_512 多种认证算法。支持完美的前向加密，增强了数据的私密性。

PPTP VPN 支持

基于 PPTP 的 VPN 则严格遵循行业标准，以保证与其它系统或设备的互联互通。NetRock 防火墙的 PPTP 支持 MS-CHAP 和 MS-CHAP V2 身份认证协议。

基于 SSL 的 VPN 同样遵循行业标准，确保与其它系统或设备的互联互通。

状态检测包过滤

NetRock 防火墙采用了基于状态检测的包过滤技术，实现了快速的基于源/目的 IP 地址、服务、用户和时间的细粒度访问控制。通过记录新建应用连接，状态检测检查预先设置的安全规则，允许符合规则的连接通过，并在系统中记录下该连接的相关信息，生成状态表。对该连接的后续数据包，只要符合状态检查表，就可以快速通过。这种方式的好处在于：由于不

需要对每个数据包进行规则检查，而是通过专门设计的算法实现同一连接的后续数据包（通常是大量的数据包）直接进入状态检查，从而整体提升系统性能。

流量整形

带宽管理模块提供了针对带宽资源的分配控制能力，对所有网络流量划分优先级以保证关键任务的服务质量，从而确保有限的带宽资源不会因为非关键应用的过度占用而影响关键任务的服务质量。带宽管理策略可以按照接口、方向、优先级等来对流量进行分级以满足企业不同层面的需求。NetRock 防火墙同时通过专有的 P2P 流量控制技术可以轻松实现对 P2P 流量的限制和带宽控制。

路由模式、透明模式及混合模式

在大型网络中，网络建设是先于网络安全的建设。当用户打算进行网络安全建设时，往往会存在一些关键应用是依赖于网络拓扑的，所以这些关键应用间是必须采用透明模式的，而其他的则应该采用更灵活的路由模式，这样将会导致在同一个网络设备上会存在透明模式和路由模式共存的情况，如果这两个部分不能互通，这将会导致因为引入安全而导致人工割裂了用户的整个网络。NetRock 防火墙提供混合模式，以保证不会因为引入安全需求而导致割裂用户网络的整体性。

IEEE 802.1Q 的 VLAN

提供对 IEEE 802.1Q 的支持，极大的扩展了 NetRock 防火墙的适应能力，使其与三层交换机配合得天衣无缝，增强了 NetRock 防火墙在网络中的布置灵活性。同时 NetRock 防火墙还提供对透明模式下的 IEEE 802.1Q 数据报得透明处理，极大地方便了用户。

静态路由

在中小型网络中，路由和防火墙如果整合成一台设备，那么可以最大的降低网络设施的投入成本。更重要的，通过把两台设备的功能整合在一台智能设备上，可以降低网络的延时，保证语音、视频等应用的最优配置。

管理方式

NetRock 防火墙提供了多种配置方式，包括基于 Telnet 和 Console 的命令行管理方式、普通的 WEB 管理方式、基于 SSL 的 WEB 管理方式和基于 SNMP V2 的网管平台。

功能强大的 NAT

在 IP 地址短缺的今天，NAT 成了网络设备必不可少的一项功能。NetRock 防火墙提供丰富的 NAT 支持，支持 1:1 的地址映射、N:M 方式的地址转换和 PAT 方式的地址转换。

认证和授权

NetRock 防火墙本身提供一个内建认证数据库，以满足基本的认证需求，同时支持 Radius 等多种方式外部认证数据库，使其能更好地适应用户的不同规格的需求。

接入控制和计费

NetRock 防火墙提供了网络接入控制和计费功能，可以实现对企业内部用户上网权限的分配和管理。其中可选的计费功能可以使 NetRock 防火墙具备宽带接入设备的能力。

系统监控

NetRock 防火墙提供实时监控系统的 CPU 利用率、各个物理接口的使用情况和链路情况，能够监控系统中的所有并发连接和某条策略授权的所有连接的创建时间、持续时间、上行/下行流量、网络层信息等。

地址对象

为了改善 NetRock 防火墙的可管理性，引入了地址对象的概念。地址对象涵盖的范围包括一台主机、一个子网或者是一个地址范围，还是以上几种地址对象集合。通过对地址对象的使用，可以在网络地址更改时最小的改动设备上的地址相关配置。

多协议支持

基于状态的 NetRock 防火墙在跟踪连接状态时，为了能够正常的处理单会话多连接的应用，NetRock 防火墙能够对多种应用层协议提供支持。目前 NetRock 防火墙支持 FTP、TFTP、IRC、MMS、H.323、ORACLE 等特殊协议。

多种接入能力

NetRock 防火墙提供对 DHCP Relay、DHCP Server、PPPoE 的全面支持，使防火墙具有良好的适应能力，以满足不同网络布置的需求，降低系统管理开销。

日志和审计

提供配置日志、事件日志和流量日志等多种日志，有利于用户进行日志分析，支持根据用户的需求将日志保存在 NetRock 防火墙内部的日志内存，或者发送到远程的标准 syslog 日志主机的功能。

系统配置

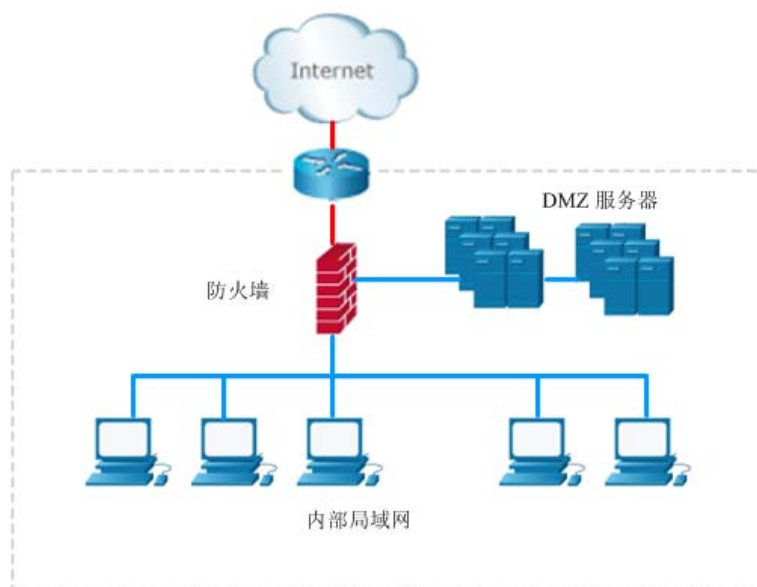
项 目	AppRock-500 描述
外型尺寸 (mm) 宽×深×高	482×370×45 (mm)
重量	5kg
插槽	PCI 扩展

项 目	AppRock-500 描述
固定接口	1 个 RS-232 配置口 4 个以太网口
处理器	3.0GHz
网络吞吐量 (Mbps)	500
安全过滤带宽 (Mbps)	500
并发连接数	500000
用户数	不限制
固态存储	128MB
SDRAM	1GB
输入电压	DC
	额定电压: +5V
工作环境温度	0 ~ 60°C
环境湿度	5~ 90% 不结露
抗冲击	10G 峰-峰加速度 (11ms)
抗震动	5-17Hz, 0.1" 双峰位移; 17-640Hz, 1.5G 峰-峰加速度
电磁干扰	符合 FCC/VDE A 级标准

组网应用

普通企业环境

这是最为普通的企业环境防火墙部署案例。利用防火墙将网络分为三个安全区域，企业内部网络，外部网络和服务器专网(DMZ 区)。

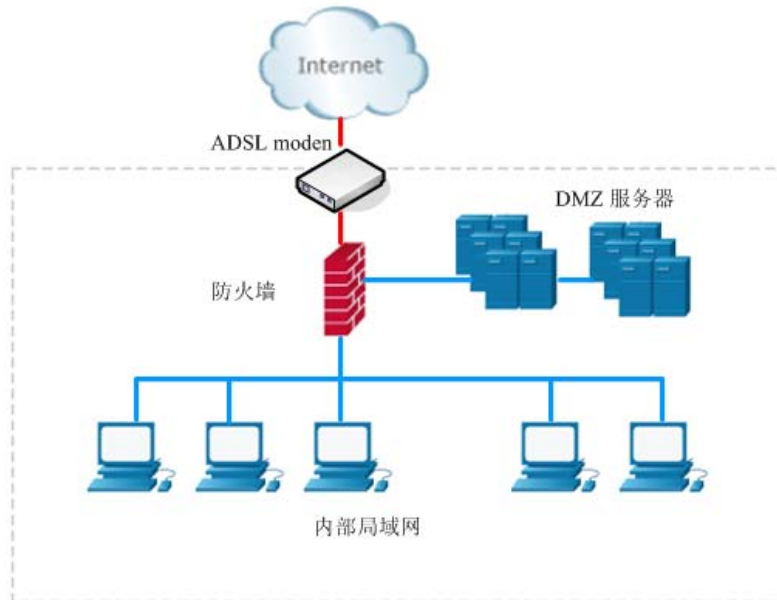


内部网络一般采用私有的 IP 地址，DMZ 的服务器可以采用公网地址，也可以采用私有地址，但是需要在防火墙上做相应的地址转换来保证外部用户对服务器的正常访问。一般常用的安全策略是：外部网络不允许访问内部网络，内部网络用户可以根据不同的权限访问

Internet 资源；内部用户和外部用户只允许访问 DMZ 区指定服务器的指定服务。

ADSL 接入部署

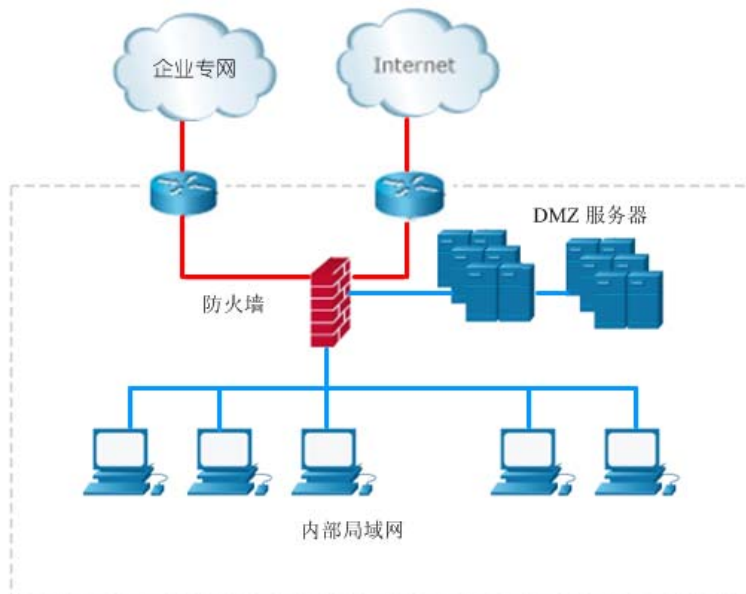
ADSL 接入是一种经济实惠的 Internet 接入方式，NetRock 防火墙提供了对 ADSL 接入，也就是 PPPOE 拨号的支持。



用防火墙代替原有的拨号客户端来连接 ADSL Modem，实现自动拨号的功能，可以配置防火墙自动做一条动态的地址转换，实现内部的多个用户通过一条 ADSL 实现对互联网的访问。这样防火墙配置的一般策略为只允许内部网络访问外部网络的指定服务。

多出口部署

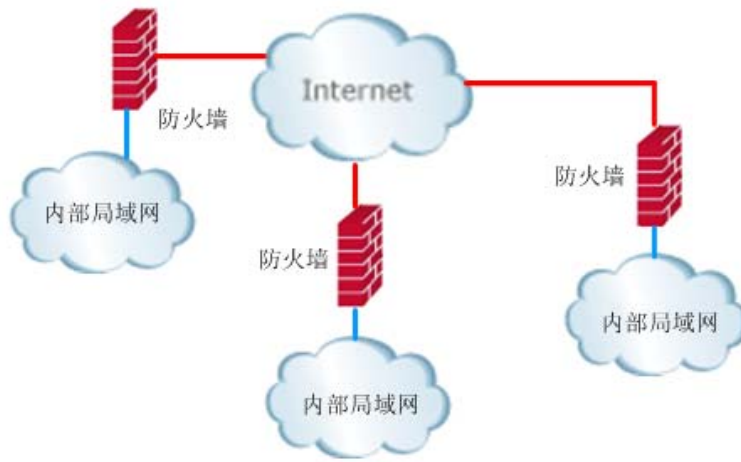
在企业局域网有多个出口的情况下，比如 Internet 出口，总部出口等。NetRock 防火墙支持将 DMZ 接口做为一个外网接口，支持多出口的接入。



我们可以将防火墙的外网口接 Internet 接入服务器,将 DMZ 口接入总部接入的服务器,利用路由的选择来分流去往两个区域的流量,可以将缺省的网关指向 Internet 处的路由器,添加相应的去往总部网络方向的路由策略。然后针对不同的网络之间的数据通讯,采用相应的安全策略。另外的一种多出口的接入方式也可以两个防火墙的方式,分别对于与相应的链路,这种方式也可以利用路由的选择来实现。

分布式部署

分布式的环境一般分为一个中心节点和多个分支节点, NetRock 防火墙支持对这种结构的整体的配置。



中心节点采用性能高的 NetRock-200/500/1000 防火墙,可以采用双机热备份的模式,保证网络的可靠性;对于分支节点,可以采用 NetRock-200 防火墙,一方面保证该分支网络的边界安全,另外也可以通过 VPN 功能实现与总部的信息通讯的安全;对于没有专线的分支节点,可以采用 NetRock-200 防火墙自带的对子网拨号的 VPN 功能,实现与总部之间的安全通讯。

华城技术支持与服务

华城技术为您提供专业完善的技术支持与服务，确保用户可以放心地购买华城安全产品。更多信息请登录 <http://www.secnumen.com>

技术支持部: support@secnumen.com

市场销售部: marketing@secnumen.com

商业合作部: business@secnumen.com

信息反馈部: webmaster@secnumen.com

北京华城技术有限公司

北京总部 北京市海淀区知本时代 邮编: 100096

免责声明: 虽然北京华城技术有限公司试图在本资料中提供准确的信息, 但华城技术并不保证这些内容的准确、完整、充分和可靠性, 并且明确声明不对内容的错误或遗漏承担责任。华城技术可以在没有任何通知或提示的情况下随时对本资料的内容进行修改, 为了得到最新版本的信息, 请定时访问公司网站。