ZStack 技术白皮书精选

基于 ZStack 云平台部署 FortiGate

扫一扫二维码，获取更多技术干货吧

版权声明

摘要

大道至简·极速部署，ZStack 致力于产品化私有云和混合云。

ZStack 是新一代创新开源的云计算 IaaS 软件，由英特尔、微软、CloudStack 等世界上最早一批虚拟化工程师创建，拥有 KVM、Xen、Hyper-V 等成熟的技术背景。

ZStack 创新提出了云计算 4S 理念，即 Simple（简单）、Strong（健壮）、Smart（智能）、Scalable（弹性），通过全异步架构，无状态服务架构，无锁架构等核心技术，完美解决云计算执行效率低，系统不稳定，不能支撑高并发等问题，实现 HA 和轻量化管理。

ZStack 发起并维护着国内最大的自主开源 IaaS 社区——zstack.io，吸引了 6000 多名社区用户，对外公开的 API 超过 1000 个。基于这 1000 多个 API，用户可以自由组装出自己的私有云、混合云，甚至利用 ZStack 搭建公有云对外提供服务。

ZStack 拥有充足的知识产权储备，积极申报多项软著和专利，参与业内标准、白皮书的撰写，入选云计算行业方案目录，还通过了工信部云服务能力认证和信通院可信云认证。

ZStack 面向企业用户提供基于 IaaS 的私有云和混合云，是业内唯一一家实现产品化，并领先业内首家推出同时打通数据面和控制面无缝混合云的云服务商。选择 ZStack，用户可以官网直接下载、1 台 PC 也可上云、30 分钟完成从裸机的安装部署。

目前已有 1000 多家企业用户选择了 ZStack 云平台。

基于 ZStack 云平台部署 FortiGate

作者：邵悠锋

前言

随着云计算技术的不断完善和发展，云计算已经得到了广泛的认可和接受，许多组织已经或即将进行云计算系统建设。同时，以信息服务为中心的模式深入人心， 大量的应用正如雨后春笋般出现， 组织也开始将传统的应用向云中迁移。

云计算技术给传统的 IT 基础设施、应用、数据以及 IT 运营管理都带来了革命性改变，同时也给安全措施改进和升级、安全应用设计和实现、安全运维和管理等带来了问题和挑战，也推进了安全服务内容、实现机制和交付方式的创新和发展。

云计算模式通过将数据统一存储在云计算服务器中，在传统 IT 技术的基础上，增加了一个虚拟化层，并且具有了资源池化、按需分配，弹性调配，高可靠等特点，但是这样也导致虚拟网络中无法更好的进行防护，比如同网段的流量可能内部进行交互，无法进行流量监控；同租户的不同网络的流量可能不经过物理防火墙，无法进行审计。

在云计算环境中，为了适应虚拟化环境，以及对虚拟机之间的流量、跨安全域边界的流量进行监测和访问控制的需要，安全设备在保持架构和功能的基础上，在产品形态和部署方式上发生了一定的变化。

在产品形态方面，主要体现是由硬件到软件。在部署方式方面，主要通过合理设计虚拟化网络逻辑结构，将虚拟化安全设备部署在合理的逻辑位置，同时保证随着虚拟主机的动态迁移，能够做到安全防护措施和策略的跟随。

在 ZStack 云平台上，我们可以非常快速的以虚拟机的形式部署安全设备，本文以 FortiGate 为例。

1 ZStack 简介

ZStack是下一代开源的云计算IaaS（基础架构即服务）软件。它主要面向未来的智能数据中心，通过灵活完善的APIs来管理包括计算、存储和网络在内的数据中心资源。用户可以利用ZStack快速构建自己的智能云数据中心，也可以在稳定的ZStack之上搭建灵活的云应用场景。

ZStack功能架构

ZStack产品优势：

ZStack是基于专有云平台4S（Simple简单，Strong健壮，Scalable弹性，Smart智能）标准设计的下一代云平台IaaS软件。

1） 简单（Simple）

简单安装部署，单机即可POC，30分钟完成安装，全UI操作界面

2） 健壮（Strong）

稳定且高效的系统架构设计，支撑高并发的API请求，支持HA的严格要求

3） 弹性（Scalable）

物理机规模可达上万台，虚拟机支持横向纵向扩展

4） 智能（Smart）

自动化运维管理，5分钟一键升级，实时全局监控

2 FortiGate 简介

FortiGate是Fortinet公司的UTM解决方案，可以有效地防御网络层和内容层的攻击。FortiGate解决方案能够发现和消除多层的攻击，比如病毒、蠕虫、入侵、以及Web恶意内容等等实时的应用，而不会导致网络性能下降。它所涉及到的全面的安全体系是涵盖防病毒、反垃圾邮件、防火墙、VPN、入侵检测和防御、和流量优化。

FortiGate产品优势:

随着网络环境、使用模式和威胁的不断变化，现在的企业正面临着各种挑战。而FortiGate下一代防火墙模块可以帮助企业解决这些挑战，它提供了丰富的功能，经过验证的安全性，并且简单易用。管理员还能够获得关于网络和威胁状况的至关重要的实时可视性，使他们能够迅速采取有效的行动。

面向未来的安全网关

FortiGate可扩展架构让企业能够轻松地激活安全模块，而不需要复杂的授权和硬件模块。

经过行业验证的安全性

与其它竞争产品相比， FortiGate拥有更多的行业证书，这能够保证该产品的功能质量，并为客户提供一流的保护。

简单易用

直观的单窗格管理能够确保一致的政策创建和执行，帮助管理员最大限度地减小部署和配置挑战。

全面的可视性

FortiGate提供更好的流量可视性，并提供对用户、设备、应用程序和敏感数据的更一致、更细粒度的控制。

广泛的网络支持

FortiGate支持多种网络设计要求，并可与其他网络设备互操作。

基于身份执行政策

FortiGate同时支持本地和远程身份验证服务（例如LDAP、Radius和TACACS+）来识别用户，以及部署相应的访问政策和安全配置文件。

高级入侵防护

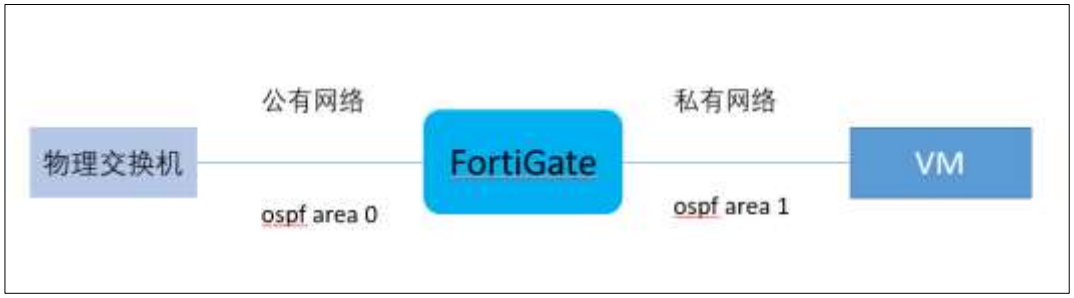
Fortinet下一代IPS技术可以在应用程序层保护网络，帮助抵御可规避安全技术的高级攻击。

3 部署 FortiGate

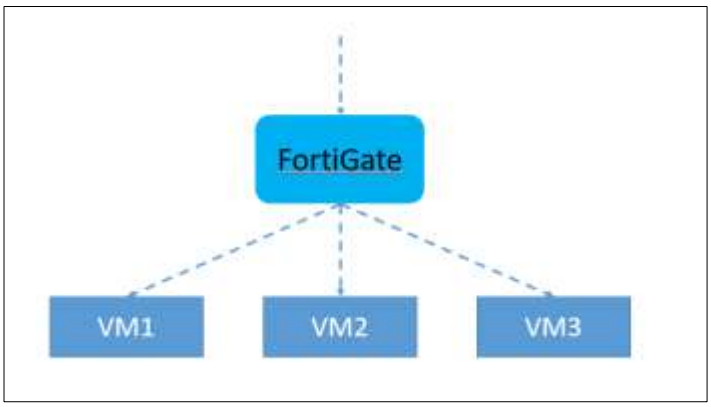
3.1 架构介绍

安全防护在网络环境中必不可少，传统的安全防护手段是在网络出口部署物理防火墙、IPS、防毒墙等一系列物理安全设备，在云网络中也有虚拟防火墙，但是云平台的虚拟防火墙功能偏少，只能支持4层包过滤，缺少入侵检测、入侵防护、病毒防护等功能。能否将专业安全厂家的设备和云平台结合使用呢？答案是使用安全厂家的虚拟设备。Fortinet公司的各类产品都提供虚拟机形式部署，本文介绍防火墙FortiGate的部署方式。

FortiGate使用一台云主机来部署，云主机有两个网卡，分别连接公有网络和私有网络，通过公有网络连接物理网络设备，私有网络连接业务虚拟机，作为业务虚拟机的网关。



FortiGate上启动ospf，将虚拟机的网段宣告给物理交换机邻居，从而通告给全网，使得全网可以访问业务虚拟机。访问业务虚拟机的流量先经过FortiGate进行安全审计，然后发送给业务虚拟机。



3.2 云平台环境准备

ZStack云平台部署步骤详情参考官方文档：

https://www.zstack.io/help/product_manuals/user_guide/3.html#c3

创建云主机

选择“云资源池”→点击“云主机”→点击“创建云主机按钮”打开云主机创建页面；

创建云主机的步骤：

1）选择添加方式，创建单台虚拟机

2）设置云主机名称为 FortiGate

3）选择计算规格

4）选择 FortiGate 镜像模板

5）选择三层网络；配置网络的时候需要注意，私有网络需要预留一个 IP 给 FortiGate 使用，因为云平台虚拟机无法直接配置网关 IP，比如网关为 10.20.0.1，预留 10.20.0.254 给 FortiGate，创建 FortiGate 虚拟机时直接指定 10.20.0.254，后续再登录 FortiGate 虚拟机将 IP 修改为 10.20.0.1

6）确认配置无误后点击“确定”开始创建。

4 配置 FortiGate

4.1 基础配置

打开 FortiGate 虚拟机控制台，默认用户名 admin，默认密码为空，登录 FortiGate CLI 终端

配置端口 IP

```
config system interface
  edit port1
  set mode dhcp
  set allowaccess ping https ssh snmp http
  next
  edit port2
  set ip 10.20.0.1 255.255.255.0
  set allowaccess ping https ssh snmp http
  next
  end
```

4.2 登录web管理端

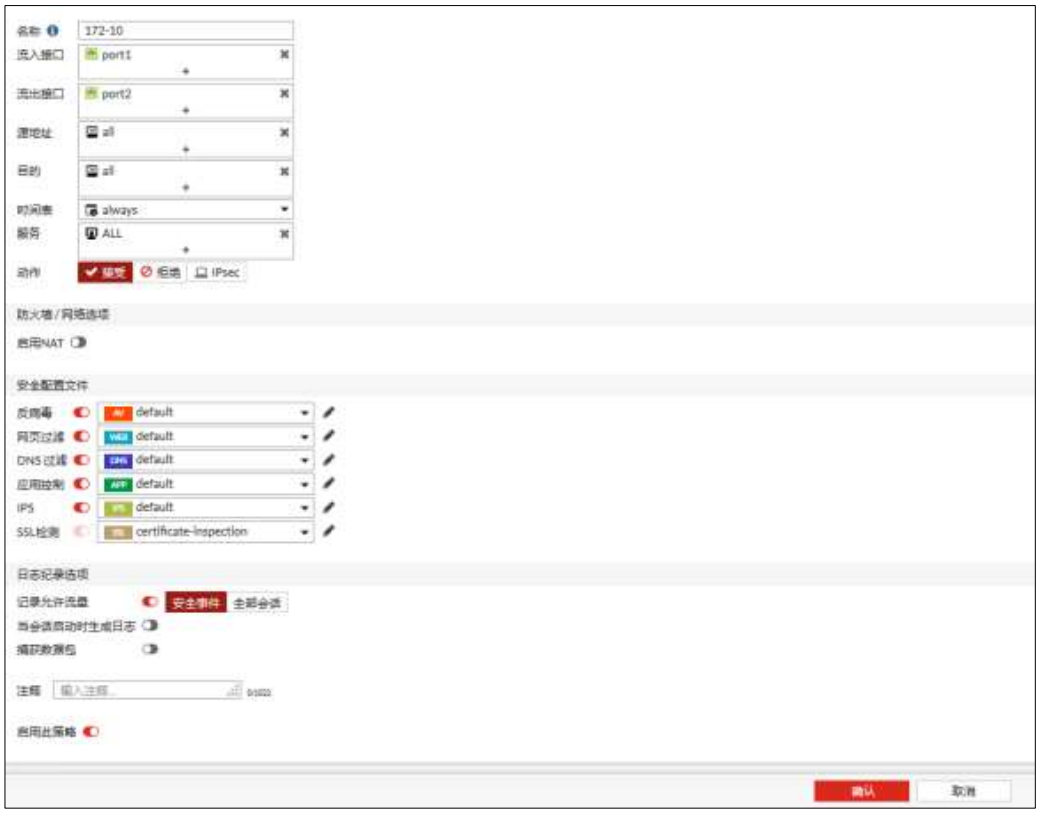
在浏览器中输入port1的ip，172.32.1.240，进入登录页面

输入默认用户名admin，密码为空，点击登录

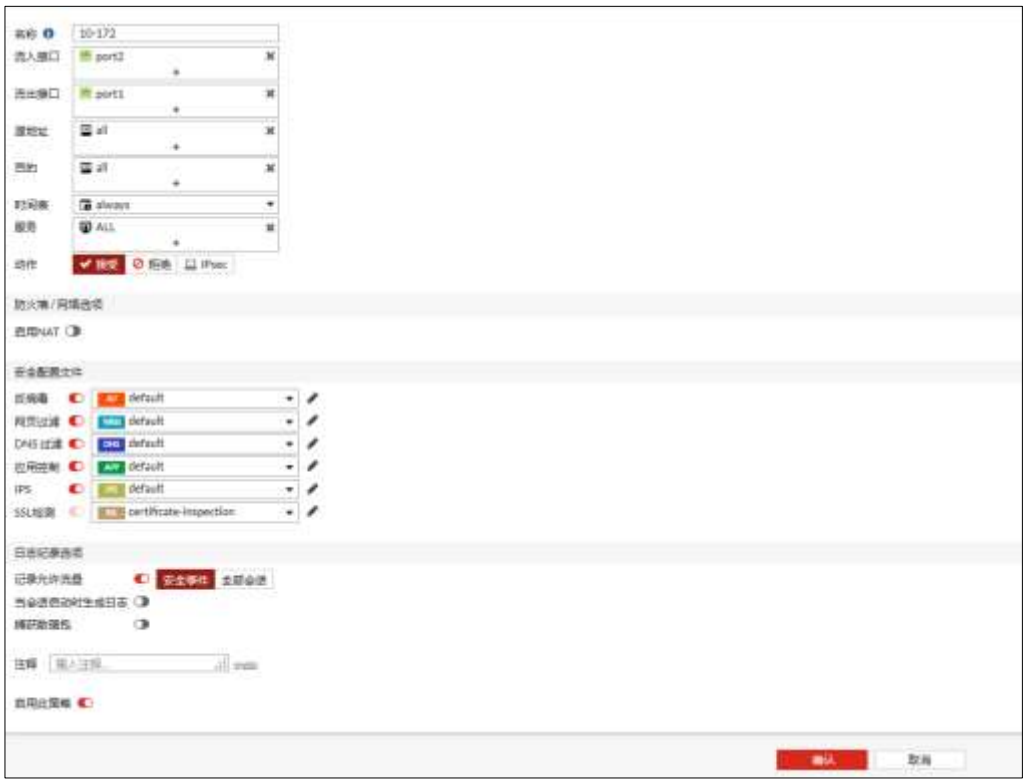
4.3 配置端口策略

在左边导航栏选择策略&对象->IPv4策略

点击“新建”按钮，配置从外部到内部的流量策略，完成后点击确认



再次点击“新建”按钮，配置从内部到外部的流量策略，完成后点击确认



4.4 配置动态路由协议

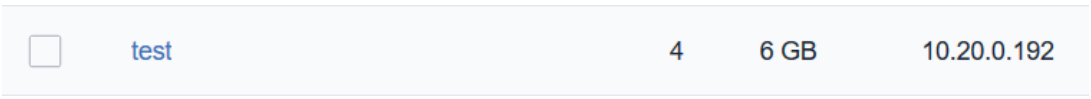
在左边导航栏选择网络->OSPF

配置相应的area和network发布

在物理交换机侧也做相应的配置，和FortiGate建立OSPF邻居并交互路由信息

4.5 连通性测试

使用私有网络创建一台虚拟机，网关设置为FortiGate的port2 ip



在外部使用其他机器来ping这台虚拟机可以ping通

```
[root@pc1 ~]# ping 10.20.0.192
PING 10.20.0.192 (10.20.0.192) 56(84) bytes of data.
64 bytes from 10.20.0.192: icmp_seq=1 ttl=62 time=2.14 ms
64 bytes from 10.20.0.192: icmp_seq=2 ttl=62 time=1.39 ms
64 bytes from 10.20.0.192: icmp_seq=3 ttl=62 time=1.37 ms
64 bytes from 10.20.0.192: icmp_seq=4 ttl=62 time=1.31 ms
64 bytes from 10.20.0.192: icmp_seq=5 ttl=62 time=1.22 ms
64 bytes from 10.20.0.192: icmp_seq=6 ttl=62 time=1.49 ms
64 bytes from 10.20.0.192: icmp_seq=7 ttl=62 time=1.43 ms
64 bytes from 10.20.0.192: icmp_seq=8 ttl=62 time=1.55 ms
64 bytes from 10.20.0.192: icmp_seq=9 ttl=62 time=1.61 ms
64 bytes from 10.20.0.192: icmp_seq=10 ttl=62 time=1.44 ms
64 bytes from 10.20.0.192: icmp_seq=11 ttl=62 time=1.12 ms
```

4.6 修改策略

将入口策略修改为只有TCP包可以通过

在测试ping，发现已经无法ping通

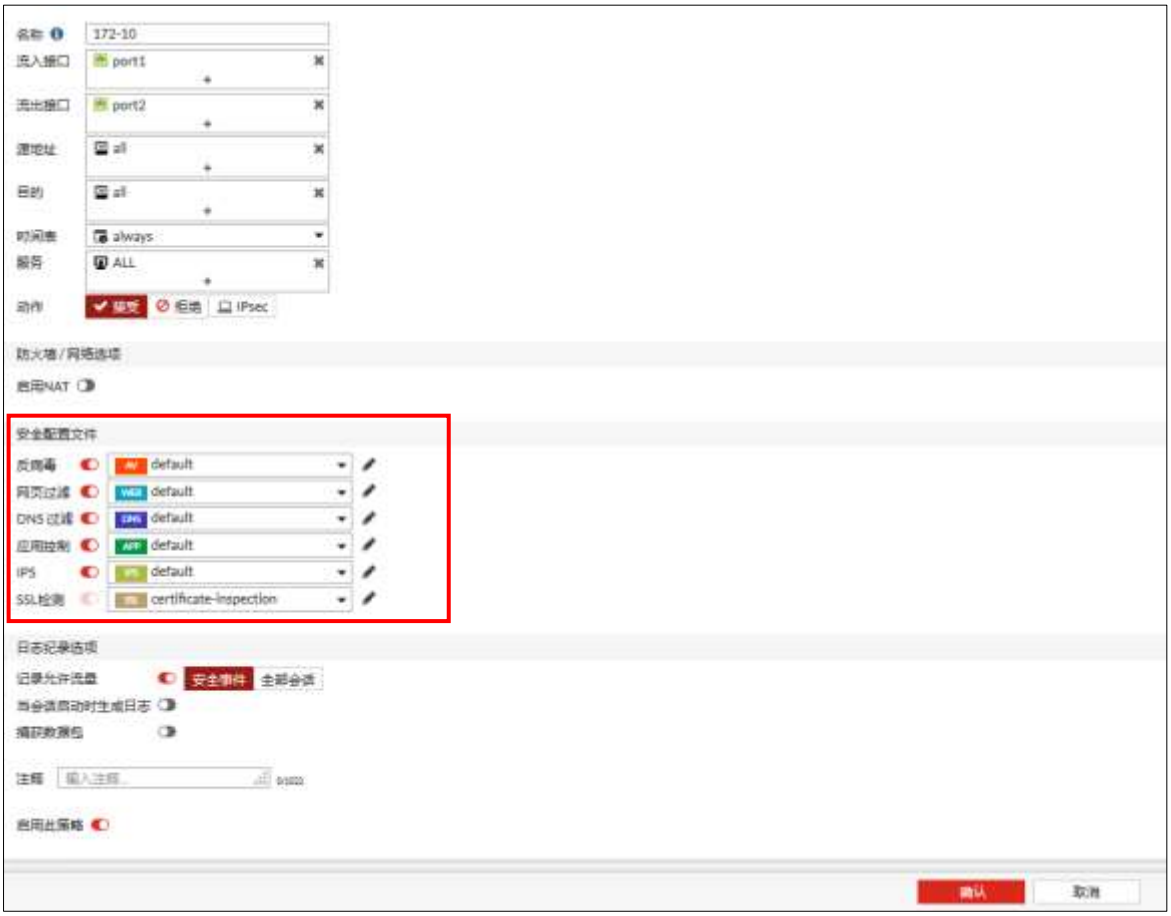
```
[root@pc1 ~]# ping 10.20.0.192 -i 0.01
PING 10.20.0.192 (10.20.0.192) 56(84) bytes of data.
^C
--- 10.20.0.192 ping statistics ---
121 packets transmitted, 0 received, 100% packet loss, time 2399ms

[root@pc1 ~]# _
```

5 FortiGate 其他功能简介

5.1 单一页面全部策略配置

FortiGate 支持将策略相关的所有配置都放在一个配置页面中，方便用户进行配置，减少不断跳转页面的复杂性，且配置顺序也非常符合逻辑



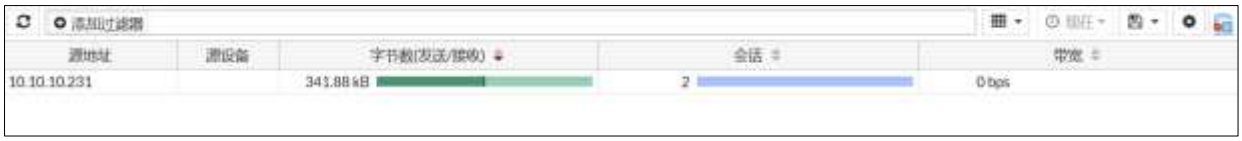
首先是连通性配置，因此要配置流入和流出接口，下面自然就是要配置策略的启用时间以及涉及的服务和需要执行动作。比如：9-18 点，FTP 服务，允许。

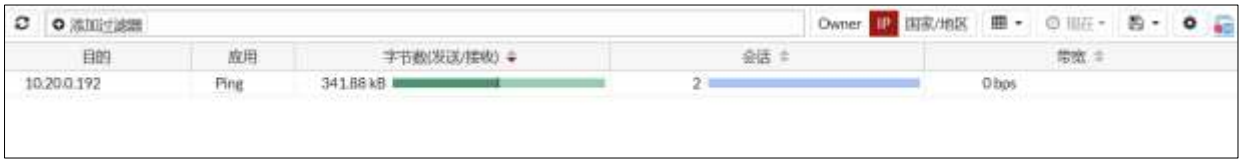
在解决了连通性问题后，下一步自然就是安全防护，比如入侵防护、防病毒、web 防护等。FortiGate 的配置非常简单，只需要在需要启用的功能处点击按钮，然后选择相应的配置文件即可，比如我想启用应用控制和 IPS，只需要将灰色的 OFF 点亮为红色的 ON，即可在后面的下拉列表框中选取对应的安全配置文件，如果没有，也可以在此页面中直接新建。之后就是额外的功能了，比如限速和带宽保证以及日志记录等等。至此，一条完整的策略就配置完成了。

5.2 策略统计命中

随着网络设备使用时间的增长，在各种网络设备中充斥着大量的策略规则，网管员面临的很大的一个挑战就是维护这些策略和规则，使得业务持续受保护。但是很多时候随着规则的变化，管理员会在防火墙上来回增加和修改策略，久而久之会出现很多无用的策略，既影响防火墙性能，又不利于管理员管理。

对于下一代防火墙来说，要能够实时追踪这些策略的使用情况，才能给予管理员指导意见，帮助删减无用和冗余策略。在 FortiGate 的图形化管理界面中，可以清晰地展示每条策略的命中使用情况，方便管理员来判断规则是否还需要使用，是否可以删除。





5.3 应用层安全

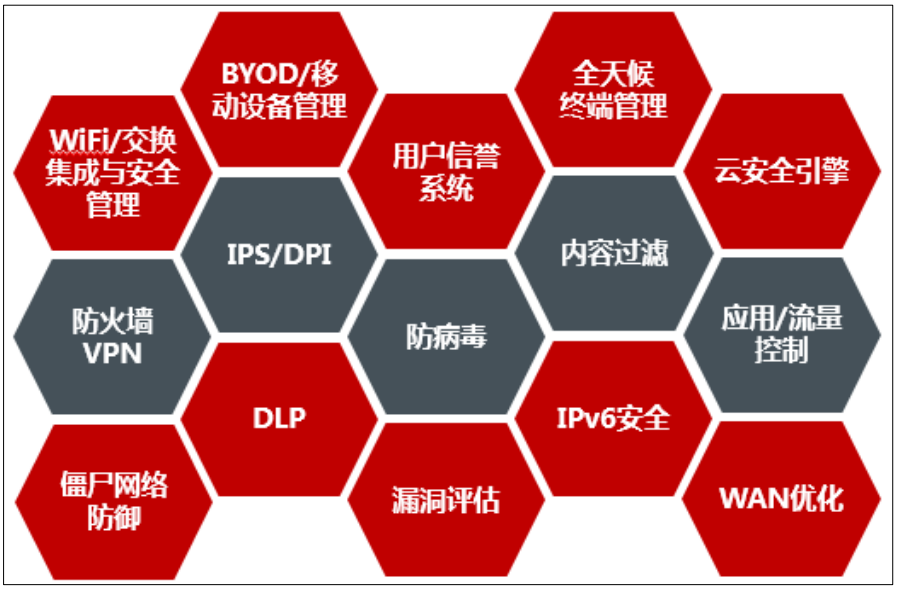
传统的状态检测防火墙通过检查数据包头，状态检测防火墙分析和监视网络层（L3）和协议层（L4），通过 IP 五元组定义的防火墙策略来允许、拒绝或转发网络流量。但是随着网络和应用的发展，它的功能弱点越来越明显，已无法保证网络的安全性。传统状态检测防火墙的弱点主要表现在以下几方面：

只了解 IP 和端口，但不能识别应用。例如 TCP 80 端口既可能是 HTTP 协议，也可能是 QQ 等 IM 或者迅雷等 P2P 下载工具，现在的技术手段可以将任何应用封装在 TCP 80 端口中传输，防火墙完全无法判断；

只检查数据包头部，但不能扫描数据包的载荷（payload），从而不能判断网络访问究竟是安全的，还是存在安全威胁的（如网络入侵、病毒、不良内容、垃圾邮件、数据泄漏……）。

FortiGate 除具备传统防火墙功能外，还可对网络层至应用层的各种安全威胁和滥用进行检测和过滤，这类产品目前被称之为 NGFW（下一代防火墙）或 UTM（统一威胁管理）。

FortiGate 的更多高级功能如下：



5.4 应用层网关

对于 H.323、SIP、RTSP、MMS、MGCP 等多媒体协议，FTP、Oracle 等特殊应用，需要根据会话进程随机开放数据端口。FortiGate 支持超过二十种网络应用的 ALG，可以识别这些协议并在会话控制过程中动态开放和关闭端口，在 NAT 模式下还需要对数据包的 payload 进行修改，最大程度地保证应用的可用性。

5.5 VPN – IPSec && SSL

随着网络威胁种类不断增多，保护企业网络，企业与合作伙伴，公司与移动员工的通讯安全如今已变得比往常更重要了。数据遭到破坏，信息泄露，网络和系统受感染每年会花费企业和政府大笔资金。

Fortinet VPN 技术允许企业运用 IPSec 和 SSL VPN 协议在多种网络和主机之间建立安全通讯和数据隐私。一旦流量被解密，多重威胁监测-包括防病毒，入侵防御，应用控制，邮件过滤和网页过滤可以为所有通过 VPN 隧道的内容所用。

IPSec VPN 隧道通常在 OSI 网络模式的第三层或更低层运行。要启用远程访问，FortiGate 在远程节点和内部网络之间建立了加密网络连接。SSL VPN 配置更易于安装和配置，因为它们在 OSI 模式，独立底层网络架构中进行最高水平的通讯。由于 SSL 协议已经内置到大多数网页浏览器为 HTTPS,无需额外的端点配置。

Fortinet 在 FortiGate 平台的 IPSec 和 SSL VPN 技术与其他的安全功能紧密结合，如防火墙，防病毒，网页过滤和入侵防御，相对单独的 VPN 安全设备能提供更多综合的保护。

6 总结

基于 ZStack 云平台可以快速部署 FortiGate，来进行云主机安全防护。FortiGate 的配置和物理环境没有任何差别，并且部署更加快捷。对于云主机来说，通过部署 FortiGate，获得的不仅仅包括提供防火墙的防护，更具备 IPS、防病毒、WEB 防护等完善的防护功能；相比较云平台仅提供 4 层包过滤的防护，使用 FortiGate 防护更加全面牢固，可以使得业务系统更加安全可靠。