

思享家 | 思科安全上新，“墙”化零售门店安全




作者：思科大中华区安全事业部资深架构师 赵帆

思享家

是一个介绍如何利用思科先进技术解决客户难题的栏目。每期聚焦一个技术热点或应用场景，邀请资深思科技术专家深入浅出地介绍，为读者提供实用性强的建议。

反复的疫情让已是微利运营的零售企业雪上加霜。原本就捉襟见肘的 IT 预算，都用来勉力维持系统运营，老旧安全设备更新和一些新安全项目只能暂时搁置。然而，网络安全威胁并不会因疫情而止步，反而有愈演愈烈之势。零售企业经营信息泄露、门店因中毒被迫停业等安全事件层出不穷。一方面是有限的资金和人力资源，一方面是复杂的网络安全形势，零售企业的 IT 部门陷入两难境界，不知道如何又好又省地解决安全问题。



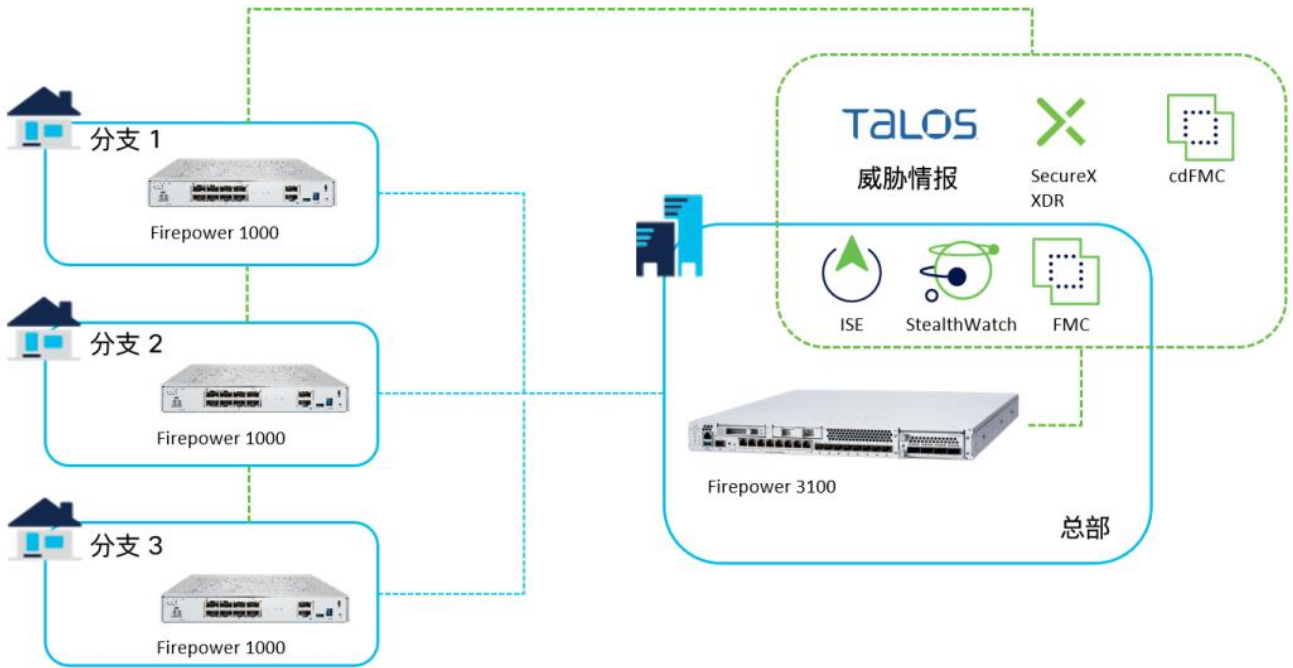
作为全球领先网络安全方案供应商，思科结合服务海内外零售企业的经验，建议零售用户以防火墙为企业网络安全系统的“基本盘”，门店安全围绕防火墙破局。这会带来以下几个确定的优势：

- 防火墙是成熟市场，厂商价格，功能体系相对完整，被“杀猪盘”的几率较低。
- 分支网点面临的网络攻击，特点是杂而不专，多而不深。防火墙，尤其是下一代防火墙中的IPS，反病毒，应用控制等技术，防范基础网络攻击依然十分有效。
- 基础的行业合规、等保等要求，通过防火墙能够快速满足。

但是在这之外，我们还需讨论防火墙在零售业的几个实践要点：

- 部署和管理简易。目前零售瘦IT是主流趋势，需要确保防火墙能够多设备集中部署和管理，在偏远或海外场景中，甚至需要云上线，云管理。
- 网络和安全融合。边界设备能够具备安全防护能力，并在安全防护栈和网络加解密，转发等能力叠加后保持稳定的吞吐，同时应该具备基础的网络选路和流量调度功能，在一些没有完整SD-WAN需求的门店可充当基础的出口网关。
- 全面的合规能力。对于门店或分支员工或用户私接设备，浏览非法内容，占用带宽等违规行为，可通过技术手段进行监控和干预。

思科 **Firepower 3100** 系列的发布，和新系统的功能更新，为零售行业门店提供了很好的产品支持。



▲图一：安全分支整体架构

首先，针对零售企业 IT 人力有限的特点，思科强化了集中管理功能。Firepower 全系列支持统一管理平台 Firepower Management Center(FMC)，或 FMC 集中管理。零售门店可在管理界面统一配置安全策略并集中推送。FMC 策略配置界面支持 IPS，AMP 和行为制策略的集中模板配置。

Base_Policy

Analyze Hit Counts Save Cancel

Inheritance Settings | Policy Assignments (1)

Rules Security Intelligence HTTP Responses Logging Advanced Prefilter Policy: Demo Prefilter Policy SSL Policy: None Identity Policy: NGFWIdentityPolicy

Filter by Device Search Rules Show Rule Conflicts Add Category Add Rule

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SET	Dest SET	Action	Icons
Mandatory - Base_Policy (1-6)														
1	Splunk Access	OutZone	InZone	198.18.13	SplunkSic	Any	Any	Any	LDP (17):8	Any	Any	Any	Trust	Icons
2	Block SSH for HI	Any	Any	Any	Any	Any	dCloudRes	OpenSSH SSH	Any	Any	Any	Any	Block with	Icons
3	Block Extranet11	InZone	OutZone	Any	Extranet12	Any	Any	Any	Any	Any	Any	Any	Block with	Icons
4	Block ICMP Over	ORE	Any	Any	Any	Any	Any	ICMP ICMP for ID	Any	Any	Any	Any	Block	Icons
5	Block Unacceptz	Any	Any	Any	Any	Any	Any	Any	Any	Pornograp Adult (Any) Gambling (L) Lotteries (J) Hats (Spa)	Any	Any	Block with	Icons
6	Block Extra to Int	OutZone	InZone	Extranet	Infrastruct	Any	Any	Any	Any	Any	Any	Any	Block with	Icons

Displaying 1 - 11 of 11 rules | Page 1 of 1 | Rules per page: 100

▲图二： FMC 集中策略管理页面

海外的分支站点，对应站点管理和数据存储本地化要求，思科在最新版本中提供 SaaS 版本的防火墙集中管理 cdFMC，对海外的零售站点提供云管理服务，用户无需承担一次性购买成本，只需要订阅云管理服务，即可在 Day 1 上线即纳管。

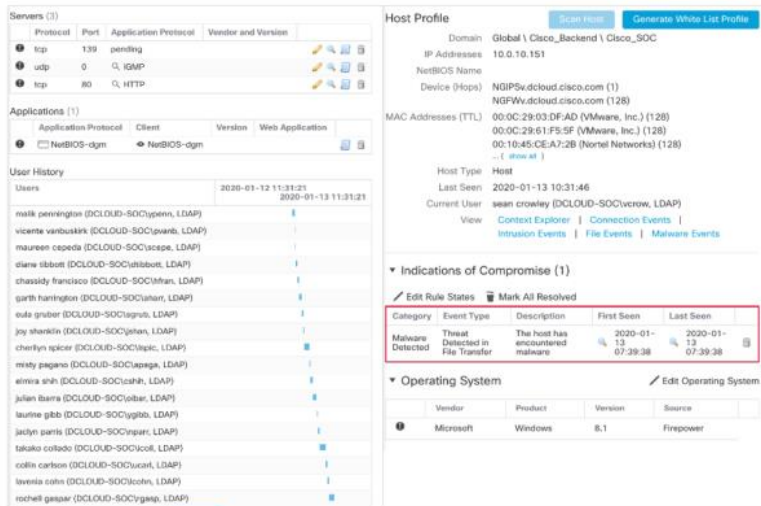
- 基于注册密钥上线设备
- 基于设备序列号零接触上线设备



▲图三： cdFMC 轻接触或零接触上线选项

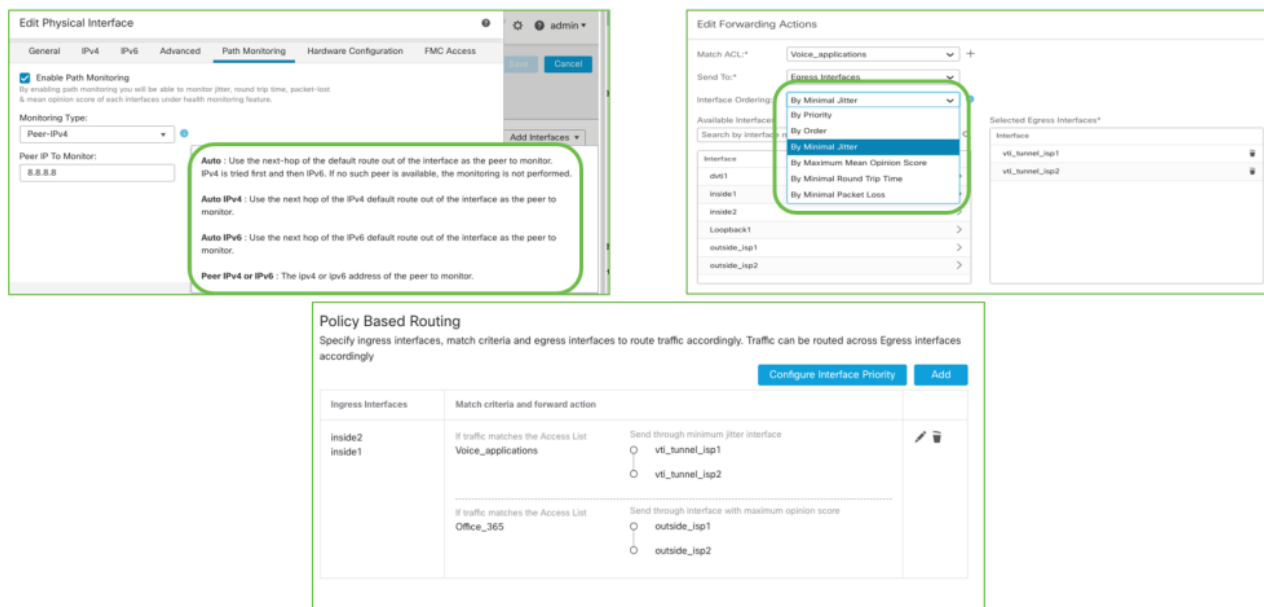
其次，思科强化了自动化功能，让零售企业用较少的人力维护庞大的系统。零售站点由于人流复杂，疏于管理，时常出现私接设备，影子 IT 等现象。Firepower 可基于网络流量的元数据信息，发现网络内设备类型，并自动基于设备类型调整安全等级。

- 通过对网络流量的被动分析发现应用程序、用户和主机
- 提供上下文并帮助确定攻击的影响
- 将 IPS 签名集调整到网络上发现的设备
- 使用第 3 方漏洞管理集成更新主机配置文件



▲图四：Firepower 设备发现功能

Firepower 最新版本添加了路径监测功能，配合策略路由，能够在出口多路径环境下智能地基于应用牵引流量。在精简 IT 场景下，随着功能更新，Firepower 也可作为出口网关，通过 IPsec 安全专用通道连接总部网络，或者公有云上业务。Firepower 也支持在主流公有云平台部署网关，实现混合云整体部署。



▲图五：Firepower 边界多线路和公有云部署

最后，也是对零售企业最重要的，3100 系列防火墙无与伦比的“性价比”。通过硬件架构的升级，专用芯片的实装，3100 系列防火墙在安全和安全专用通道性能上实现了大幅度提升。通过全新的功能和硬件架构，在总部头端的部署可同时支持大数量分支通道的聚合，以及高吞吐安全扫描的稳定。这样的提升能够简化部署架构，节省采购成本，通过技术升级完成降本增效。



*.性能估计值以Gbps为单位，取决于具体数据包大小，协议类型和其他网络变量，IPSec VPN以FTD 7.2版本为准

▲图六：Firepower 3100 系列性能图表

对于用户来说，做安全很大的困扰在于行业的声音不一，厂商百出，时不时出现一个新兴的技术、架构、解决方案。而在新技术方案背后，很大可能是用户被割了技术的韭菜，需求跟不上功能变化，为新的技术付出了溢价。所以企业一定要抓住安全“基本盘”——防火墙不放。

思科防火墙 Firepower 在硬件和软件功能上的更新，让零售企业能够轻松地解决目前突出的安全和部署成本之间的矛盾，为企业克服时艰，继续“新零售”转型保驾护航。

欲了解 Firepower3100 的更多能力，请点击[“思科弹性安全方案”](#)。