cisco SECURE

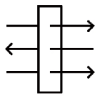
Cisco Secure Firewall
产品手册

思科Secure Firewall 介绍

企业数字化转型的过程中有几个根本性的变化，第一是核心生产业务逐渐向多云多平台过渡，第二是企业办公逐渐实现数字化和移动化，员工可随时随地访问公司内网。由此带来的网络边界的扩展使得传统的防火墙部署不再有效，我们的单一网络边界已经发展为多个微边界。因此，企业正在努力提升防火墙部署的弹性、访问策略的管理能力和统一的威胁可见性，以更好地支撑现代的生产和办公业务。

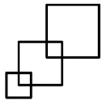
在思科，我们正在构建一个平台式的网络安全愿景。通过构建敏捷、自动化和集成的安全体系，来协调跨架构，跨区域和跨租户的安全防护一致性。Secure Firewall作为思科下一代防火墙产品， 既是现代用户网络和安全的核心，也是面向未来的安全体系的基石，为用户激活SASE、零信任、XDR等高级使用场景提供重要支撑。

作为权威网络安全测试和评估机构，SE Labs在2023年度的安全报告中，因为思科优异的产品特性和客户口碑，评选Secure Firewall为年度下一代防火墙。



- 在多功能叠加下的稳定性能表现

- 高效安全的威胁情报和生态集成

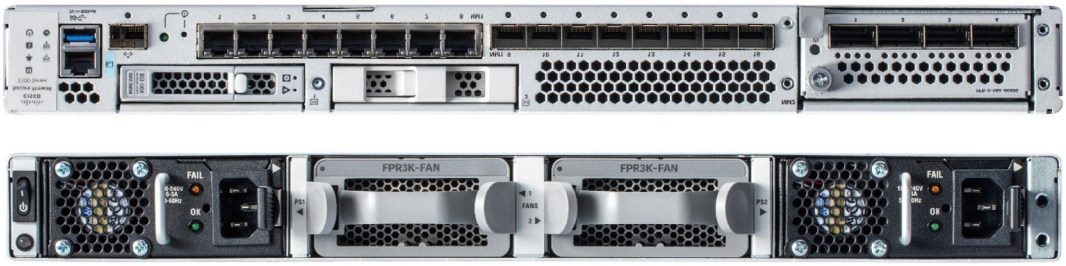


- 优异的扩展与集中管理能力

关键能力

- 全新ZTNA和SD-WAN功能支持，加速网络接入和安全的融合
- 全新3100系列硬件架构、虚拟化和公有云部署，搭配集群特性，构建安全+弹性的下一代网络
- 与思科的网络及数据中心解决方案深度集成
- Snort 3 下一代IPS引擎搭配思科Talos威胁情报中心，提供全天候一站式的威胁防御能力
- 卓越的检测和机器学习能力，应对加密流量带来的可视性挑战
- 每个Secure Firewall 都包含 SecureX™ 授权，以实现思科及第三方的威胁情报共享，并通过XDR事件响应实现威胁关联并加速自动处理
- 集中云端管理平台cdFMC正式上线，扩展了不同场景下的统一管理能力

思科Secure Firewall 3100系列介绍



面向中高端的 Cisco Secure Firewall 3100 系列由五款防火墙型号组成，可提供业务弹性和卓越的威胁防御能力。每个3100型号都搭载了现代的CPU 架构以及专属的硬件芯片，从而大幅地提升了表现性能，确保能够平稳支撑检测加密和威胁防御等重要安全特性。

3100系列还支持集群技术，以及更高的端口密度和 Q-in-Q 支持，从而极大地提升部署的弹性，能够广泛适用于互联网边缘、中大型数据中心及私有云部署。

在2023年初，全新的3105也加入了3100的系列家族，这一模型适合中小型防火墙部署场景，与过去的中端平台相比，性能提升高达 500%。通过全新的硬件框架和软件，全面强化合作伙伴及用户在中小型场所，分支站点等网络部署的安全弹性。

性能与功能

Cisco Secure Firewall 3100 系列性能和规格摘要

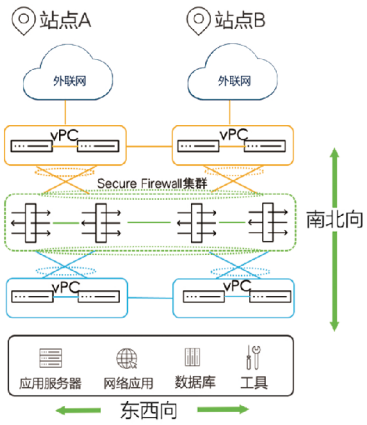
防火墙型号	Firewall	FW+AVC+IPS	IPS	接口	可选接口模块
3105	10G	10G	10G	8 x RJ45, 8 x 1/10G SFP+	10G SFP+
3110	18G	17G	17G	8 x RJ45, 8 x 1/10G SFP+	10G SFP+
3120	22G	21G	21G	8 x RJ45, 8 x 1/10G SFP+	10G SFP+
3130	42G	38G	38G	8 x RJ45, 8 x 1/10/25G SFP+	10G/25G/40G SFP+, 4X40G NM
3140	49G	45G	45G	8 x RJ45, 8 x 1/10/25G SFP+	10G/25G/40G SFP+, 4x40G NM

Cisco Secure Firewall 3100 系列功能特性

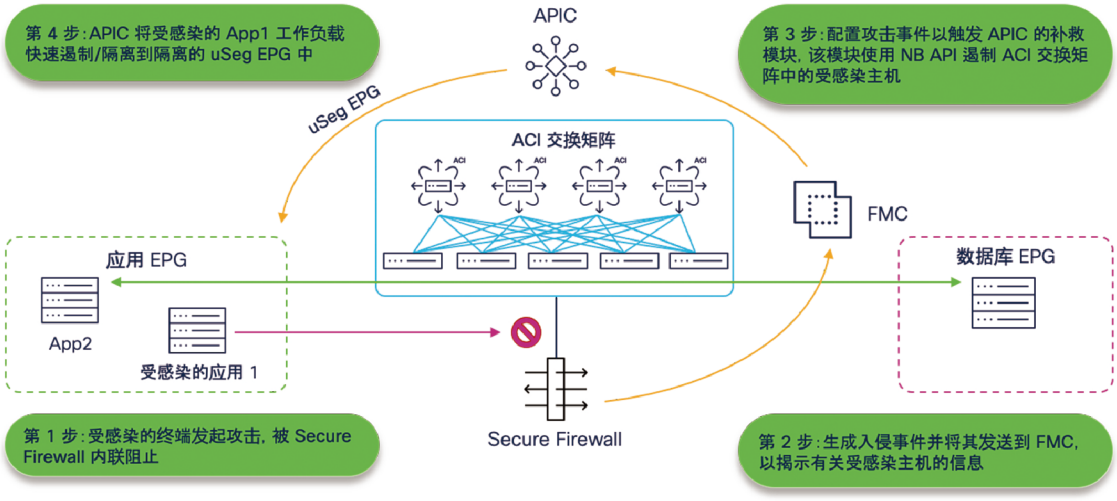
功能特性	3110	3120	3130	3140
本地管理	开箱支持本地简易管理 - FDM			
集中管理平台	支持本地和SaaS化集中管理 - FMC，cdFMC			
应用可视与控制（AVC）	支持超过 5000 个应用程序，支持OpenAppID、地理位置、用户、网站和自 定义应用程序，包含在基础授权许可里			
思科威胁情报（SI）	根据源/目标 IP 地址或目标 URL(例如僵尸网络、CnC、漏洞利用、垃圾邮 件、网络钓鱼等)，由 Talos 定义和更新 ，包含在威胁授权许可里			
思科安全IPS	Snort 3 IPS 可以被动检测端点和设施，构建威胁关联和侵害指标 (IoC)，包含在威胁授权许可里			
网络恶意软件防御（AMP）	检测、阻止、跟踪、分析和补救，保护企业免受针对性的持续恶意软件攻击，包含在文件授权许可里			
加密可见性引擎（EVE）	无需解密即可检测加密数据包中的操作系统、应用程序和威胁			
URL内容过滤	对可疑网络流量发出警报和控制。对 80 多个类别的数亿个 URL 实施策略			
第三方支持和开源生态	与第三方集成的开放 API；针对新威胁和特定威胁的 Snort® 和 OpenAppID 社区资源			
高可用性和集群	主/主、主/备。3100 系列允许最多 8 个设备的多活集群			

思科Secure Firewall 数据中心部署

现代企业广泛采用多活数据中心和应用部署架构，Secure Firewall是思科整体数据中心解决方案中的重要一环，通过防火墙集群，我们可以增加防火墙成员的方式扩展性能，其次防火墙集群的跨数据中心部署保证了服务在多数据中心间的多活和迁移，避免了服务切换过程中因来回路径不一致导致的服务中断问题。在防火墙策略层面，整个集群也保持了一致性的策略。



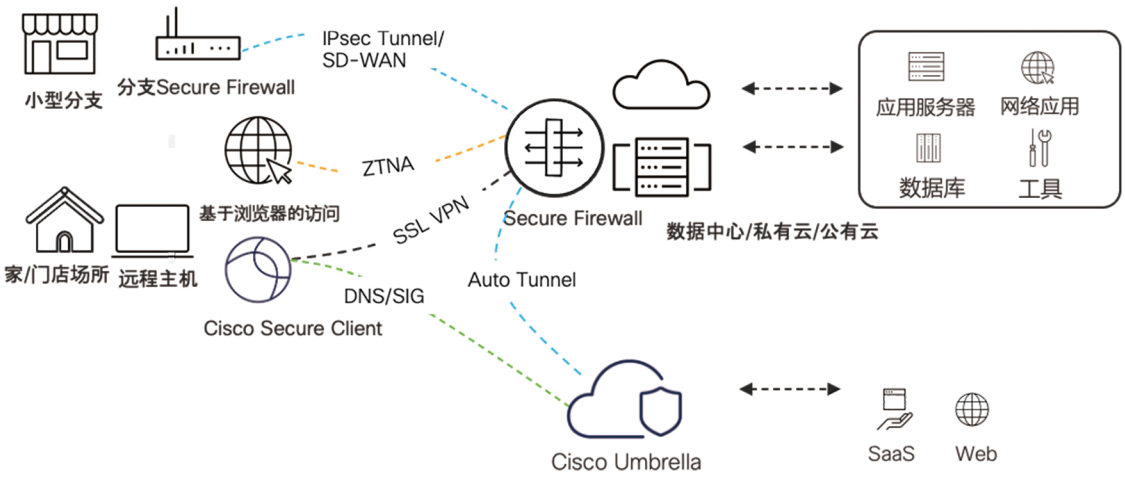
Secure Firewall支持与思科ACI集成，通过防火墙威胁防御联动APIC实现企业数据中心中的威胁处理与自动遏制。



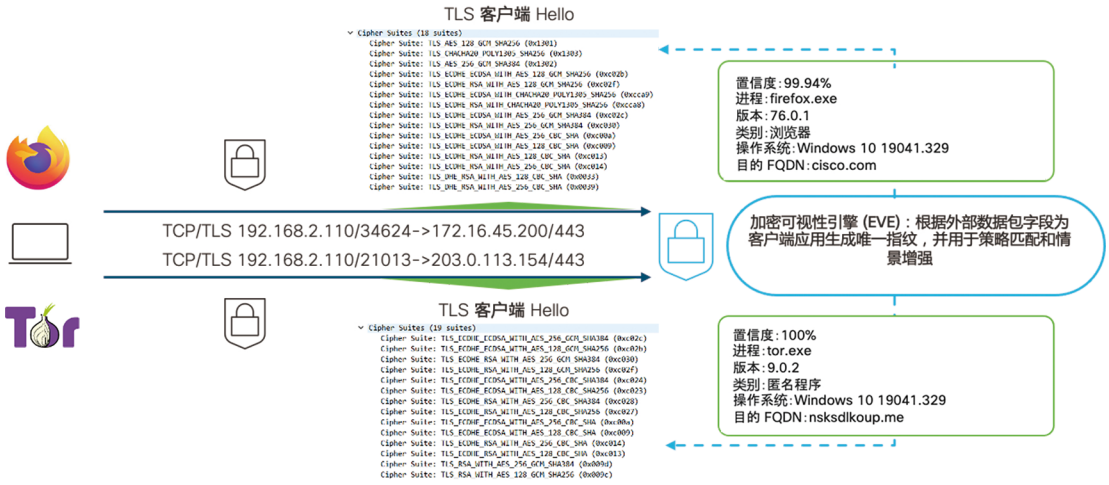
思科Secure Firewall 混合办公部署

近年来，企业网络弹性增强成为了建设的方向，以应对复杂的发展形势。在一个跨区域多分支的大型企业网络中，通过思科Secure Firewall部署以及思科全球出海解决方案，用户可按照目标应用的部署地点和访问等级，获取细粒度的一体安全接入。包括 -

- 远程用户通过隧道专网或ZTNA远程接入访问内网应用
- 远程和分支用户通过Cisco Umbrella控制和防护对外部Web服务的访问
- 分支门店通过SD-WAN网络连接至中心Secure Firewall

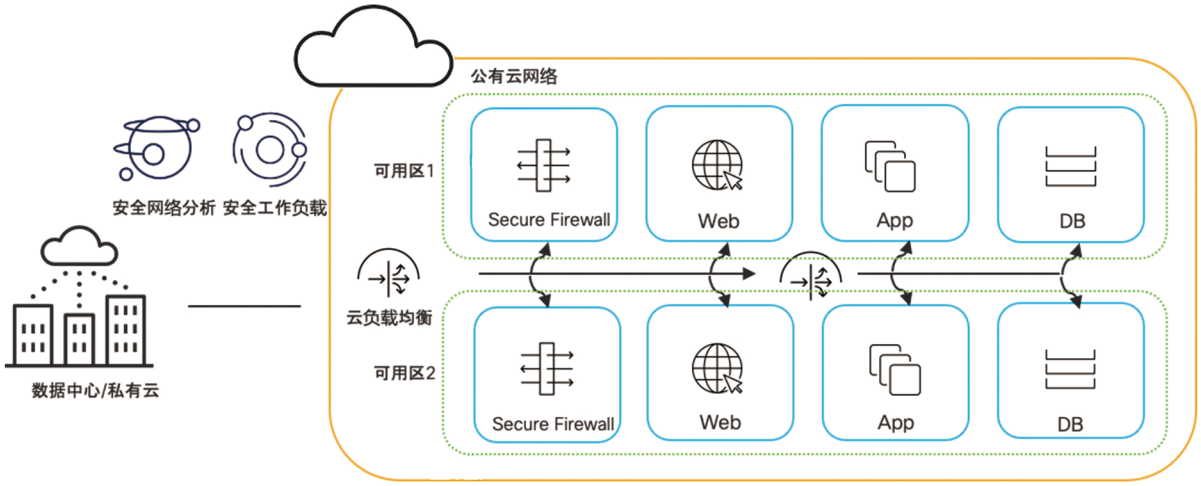


针对办公网络里加密的应用和Web流量，Secure Firewall推出全新的加密可视性引擎（EVE），能够在不拆解TLS加密的情况下通过机器学习的方式分析流量，识别应用，提升安全控制能力。

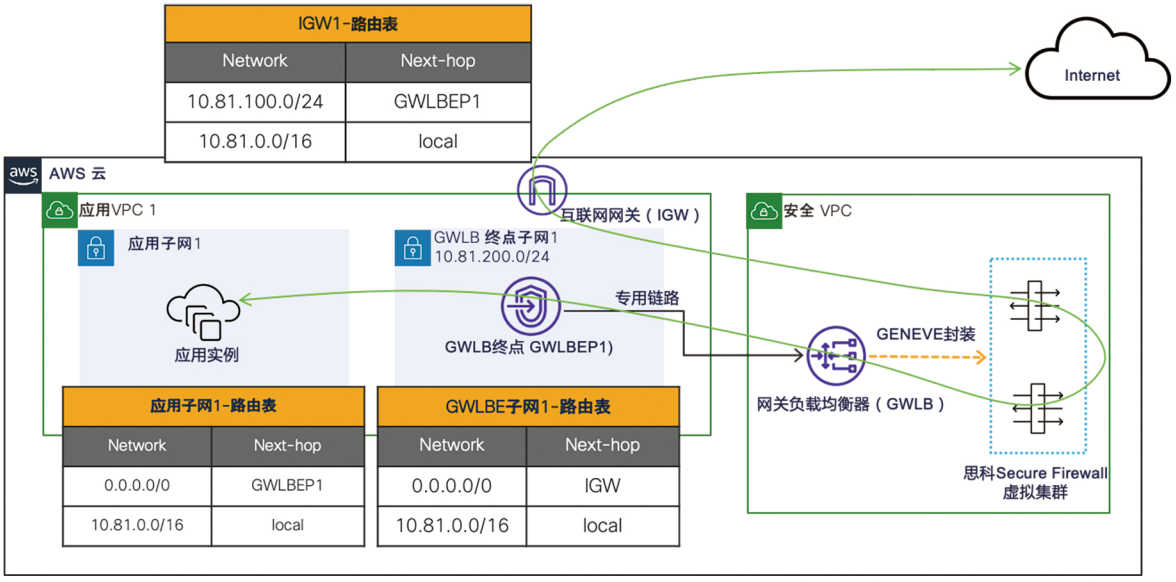


思科Secure Firewall 混合云部署

思科Secure Firewall可无缝地将行业领先的安全性扩展到云端，无论是AWS、Azure、AliCloud还是GCP，企业均可实现跨物理和云环境的一致部署。在广泛上云和混合云部署的时代，通过思科混合云整体方案实现统一安全管理、自动化运维、高级威胁防护以及深入可见性。



思科与公有云平台有紧密的合作和部署集成，以AWS云为例，Secure Firewall支持云上的虚拟集群，以及与AWS 网关负载均衡器集成的能力。这种架构下，用户不同VPC的南北向流量，及VPC间的东西向流量均可以通过统一的安全VPC进行流量的控制和深度检查。在多VPC复杂网络里安全防护的弹性得以大大加强。



思科Secure Firewall 系列数据表

功能特性	1010	1120	1140	1150
L4状态防火墙检测吞吐	2 Gbps	4.5 Gbps	6 Gbps	7.5 Gbps
防火墙 (FW) + 应用可视与控制(AVC) 吞吐(1024B)	890 Mbps	2.3 Gbps	3.3 Gbps	5.3 Gbps
下一代防火墙吞吐（FW+AV+IPS）	880 Mbps	2.3 Gbps	3.3 Gbps	4.9 Gbps
AVC下最大并发	100K	200K	400K	600K
AVC下最大新建	6K	15K	22K	28K
TLS检测吞吐	195 Mbps	850 Mbps	1.2 Gbps	1.4 Gbps
IPS检测吞吐	900 Mbps	2.6 Gbps	3.5 Gbps	6.1 Gbps
IPSec VPN吞吐（1024B TCP Fastpath）	400 Mbps	1.2 Gbps	1.4 Gbps	2.4 Gbps
最大VPN对等体数	75	150	400	800

功能特性	2110	2120	2130	2140
L4状态防火墙检测吞吐	3 Gbps	6 Gbps	10 Gbps	20 Gbps
防火墙 (FW) + 应用可视与控制(AVC) 吞吐(1024B)	2.6 Gbps	3.4 Gbps	5.4 Gbps	10.4 Gbps
下一代防火墙吞吐（FW+AV+IPS）	2.6 Gbps	3.4 Gbps	5.4 Gbps	10.4 Gbps
AVC下最大并发	1 million	1.5 million	2 million	3 million
AVC下最大新建	14K	18K	30K	57K
TLS检测吞吐	365 Mbps	475 Mbps	760 Mbps	1.4 Gbps
IPS检测吞吐	2.6 Gbps	3.5 Gbps	5.4 Gbps	10.5 Gbps
IPSec VPN吞吐（1024B TCP Fastpath）	950 Mbps	1.2 Gbps	1.9 Gbps	3.6 Gbps
最大VPN对等体数	1,500	3,500	7,500	10,000

功能特性	3105	3110	3120	3130	3140
L4状态防火墙检测吞吐	10 Gbps	18.0 Gbps	22.0 Gbps	42.0 Gbps	49.0 Gbps
防火墙 (FW) + 应用可视与控制(AVC) 吞吐(1024B)	10 Gbps	17.0 Gbps	21.0 Gbps	38.0 Gbps	45.0 Gbps
下一代防火墙吞吐（FW+AV+IPS）	10 Gbps	17.0 Gbps	21.0 Gbps	38.0 Gbps	45.0 Gbps
AVC下最大并发	1.5 million	2 million	4 million	6 million	10 million
AVC下最大新建	110,000	130,000	170,000	240,000	300,000
TLS检测吞吐	3.2 Gbps	4.8 Gbps	6.7 Gbps	9.1 Gbps	11.5 Gbps
IPS检测吞吐	10 Gbps	17.0 Gbps	21.0 Gbps	38.0 Gbps	45.0 Gbps
IPSec VPN吞吐（1024B TCP Fastpath）	5.5 Gbps	11.0 Gbps	13.5 Gbps	33.0 Gbps	39.4 Gbps
最大VPN对等体数	2,000	3,000	6,000	15,000	20,000

功能特性	4112	4115	4125	4145
L4状态防火墙检测吞吐	40 Gbps	80 Gbps	80 Gbps	80 Gbps
防火墙 (FW) + 应用可视与控制(AVC) 吞吐(1024B)	19 Gbps	33 Gbps	45 Gbps	53 Gbps
下一代防火墙吞吐（FW+AV+IPS）	19 Gbps	33 Gbps	45 Gbps	53 Gbps
AVC下最大并发	10 million	15 million	25 million	30 million
AVC下最大新建	98K	210K	269K	365K
TLS检测吞吐	4.5 Gbps	6.5 Gbps	8.5 Gbps	10 Gbps
IPS检测吞吐	19 Gbps	33 Gbps	45 Gbps	55 Gbps
IPSec VPN吞吐（1024B TCP Fastpath）	8.5 Gbps	12.5 Gbps	19 Gbps	24 Gbps
最大VPN对等体数	10,000	15,000	20,000	20,000

北京
北京市朝阳区建国门外大街2号
银泰中心银泰写字楼C座7-9层
邮编:100022
电话:(8610)85155000
传真:(8610)85155960

上海
上海市长宁区红宝石路500号
东银中心A栋21层
邮编:2001103
电话:(8621)22014000
传真:(8621)22014999

广东
广州市天河区林和西路161号
中泰国际广场A塔34层
邮编:510620
电话:(8620)85193000
传真:(8620)85193008

思科在全球设有200多个办事处、地址、电话号码和传真号码均列在思科网站 www.cisco.com/go/offices 中。