cisco SECURE

要点浅析:

企业选择防火墙的五大考虑事项

改变观念，将防火墙视为全面防护的基础。

cisco SECURE

1 不再将防火墙视为单一控制点。

过去，防火墙一直在网络边缘保护着整个组织。但是时过境迁，如今的网络发生了巨大的变化。网络边界不再有明确的界线。这就要求防火墙必须能通过无处不在的控制点来执行通用策略。换而言之，如今的*防火墙*（无论是实体设备、虚拟设备，还是防火墙云服务）应该不仅能在您需要的位置提供智能控制点和全面可视性，还能实现应用和工作负载控制。

应考虑制定全面的防火墙战略，在需要的位置部署一致的安全控制措施，以便对用户、地点和设备的情景信息进行收集、共享和响应，并确保满足您的组织的安全要求。这种集成化方式有助于区分警报优先级，实现策略统一，共享威胁情报，并加强用户和设备身份验证，让您获得全面的可视性。

- 观看视频，展望防火墙的未来

2 充分利用世界一流的安全情报。

威胁的复杂性日益增加，要保护网络安全，必须依靠业界领先的情报和无处不在的一致保护。而世界一流的威胁情报需要优秀的团队作支持。

思科 Talos 是世界上最大的商业威胁情报团队，成员包括来自研究、分析和工程领域的精英。

该团队凭借切实可行的情报和漏洞研究，帮助思科客户快速检测并有效防御已知和新型威胁。我们还会及时分享研究成果，因此能够阻止正在肆虐的威胁并提供大范围的网络保护。

- 走进 Cisco Talos®

cisco SECURE

3 借助基于云的管理。

无论是分散化管理或策略不一致，还是手动升级防火墙管理器，都会让管理难上加难。基于云的管理模式可以将耗时的管理工作转移给服务提供商。

借助集中化的云端管理服务，安全团队可以轻松而简单地确保整个组织的策略一致性。策略只需创建一次，即可通过上千个执行点快速完成实施。安全团队还可以利用单一管理控制台比较所有设备上的各种对象，从而发现不一致并优化安全状况。不仅如此，随着您的组织不断发展，新部署的设备会自动继承最新的策略。诸如这样的优势还有很多，您可以深入了解基于云的管理解决方案如何让您的组织受益。

- 深入了解 Cisco Defense Orchestrator

4 使防火墙成为开放式安全平台的一部分。

投资防火墙应不仅旨在解决燃眉之急，还应着眼于未来。如能采用保护全面、高度集成的开放式安全平台来自动保护您的环境，您就能放心地开展业务活动。

无论您使用几家供应商的安全产品，开放式平台都能确保整个安全基础设施的所有组成部分一览无遗，帮助您减少安全缺口。以防火墙为基础的平台解决方案可实现全面威胁监测、安全分析和通用策略管理，有助改善决策。一些优秀的平台产品还可以化繁为简：不仅支持开箱集成，而且能自动执行威胁调查、追踪和补救等流程化的安全任务。总而言之，平台解决方案可以有效提高运维效率，减少人为错误并降低运维成本。

- 详细了解 Cisco SecureX™

5 选择值得信赖的供应商。

世界正在飞速变化。或许您的组织也一样。无论怎样，选择能兼顾当前和未来需求的供应商都是有利无弊的。

作为深受所有财富百强企业信赖的领先安全供应商，思科无疑是您的理想选择。我们拥有无与伦比的威胁情报和业界领先的零信任技术，可以为您提供有效的安全解决方案来迎击不断发展的威胁。我们将一流的安全产品整合到一个开放的集成化平台，确保您的基础设施安全无虞。选择思科，您不仅能大幅改善安全状况，还能节省运维成本。

- 观看视频，了解思科的独特之处

深入了解 Cisco Secure 防火墙 >