选择防火墙的五大考虑事项

目录

重新审视防火墙，为应对新型分布式混合环境奠定灵活可靠的安全基础。

1. 突破常规，锐意创新

现代防火墙具有哪些特征？能够与网络基础设施全面集成，但最重要的也许是能够随时随地通过单一管理平台实施策略。新一代防火墙可提供跨平台的统一策略、移动设备情报、情景信息和威胁情报，满足您的可视性需求，助您妥善管理通过易受攻击的移动应用和无处不在的终端与网络建立的连接。

2. 深入洞察加密流量

一直以来，要真正了解加密流量的内部状况，主要困难在于如何充分解密。解密过程费用高昂，从法律和运营层面而言都不切实际，而任由加密流量进出网络，会导致网络和基础设施极易遭受各种攻击，包括从数据泄露（漏洞）到勒索软件攻击。

真正的挑战在于，如何找到一种合适的方式来检测加密流量中的恶意活动。新型防火墙应优先考虑此功能，确保能够以极少的解密操作和极低成本提供最大限度的高可视性。

3. 即时获取威胁情报

企业受攻击面不断扩大，加上网络、分支机构以及通常易受攻击的过时基础设施随时面临着日益复杂的威胁，不论何种情报框架，都需要未雨绸缪，提前防范网络犯罪分子。此类框架还应能准确识别传入的威胁，确定是垃圾邮件、恶意软件还是其他类型的攻击。

这些信息有助于您初步了解防火墙应具备的功能，即，针对整个网络中的设备、位置和用户，为您提供动态情景信息。

4. 构筑安全弹性

在混合环境中，用户经常会使用易受攻击的设备和应用访问网络，这为黑客渗透网络提供了可乘之机，尤其是那些过时的基础设施，非常容易成为攻击目标。要解决这一问题，势必需要构筑安全弹性。

安全弹性是指保护作为高可用性安全基础设施的核心的防火墙，根据风险确定警报和任务的优先级，预测未来趋势，每小时自动执行安全更新并应对意外攻击，最终达到省时、省钱、省心的目的。

5. 选择着眼于全局的方法

既然可以利用多种工具获得更高的可视性、更多的情景信息，通过统一的方式管理流量和情报，为什么还要局限于使用防火墙呢？凭借一套可提高防火墙性能的工具，您可以获得更全面的可视性，更深入地了解情景信息，而无需支付额外费用。

各种服务、多个控制面板和架构彼此孤立，让威胁管理变得异常复杂。寻找合适的防火墙和增强功能，有助于您更快做出决策，减少威胁驻留时间，同时提供有意义且切实可行的指标。

了解 Cisco Secure Firewall 如何助您改善安全态势，保护您的组织免受日益复杂的威胁侵害：

深入了解 Cisco Secure Firewall

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

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。

美国印刷 C95-3416352-00 01/23