

技术合作伙伴解决方案简介

网络安全策略自动化 用于Palo Alto Networks新一代防火墙

为贵企业提供的益处：

- 通过Panorama设备组策略变更的零接触自动化提高生产力。
- 利用Tufin对Palo Alto Networks App-ID™、User-ID™和Content-ID™的先进分析和自动化
- 了解和控制混合网络的安全性与连接性
- 通过有效管理分段和优化防火墙和设备组策略, 减少攻击面
- 利用内置的安全功能, 在数分钟而不是数天内实现网络安全变更
- 确保持续合规并为审计做好持续准备



Palo Alto Networks®和Tufin®提供安全、合规、可管理的环境

由于需要应对复杂的网络变化并跟上不断增长的业务需求, 企业IT和安全专家面临的压力越来越大。缺乏网络可视性使企业无法以所需的安全性、速度和准确性提供服务和应用。Tufin Orchestration Suite™和Palo Alto Networks®新一代防火墙共同提供了先进的网络保护和可视性, 可实现灵活和无风险的策略修改。Palo Alto Networks的新一代防火墙功能使用先进的分析和自动化技术, 帮助企业在异构网络、设备、服务器和应用程序之间协调变更流程。

Tufin Orchestration Suite是用于自动设计、配置、分析和审计从应用层到网络层的网络安全变更的完整解决方案。Tufin的解决方案为Palo Alto Networks新一代防火墙或通过Palo Alto Networks Panorama提供管理和变更自动化。

基于应用身份的自动网络安全变更设计与实施

Palo Alto Networks-Tufin 解决方案通过零接触自动化, 大大缩短了网络安全变更所需的时间。自动化基于尖端的网络拓扑模拟分析, 该分析可识别Panorama 设备组的策略, 同时考虑到层次结构以及AppID、UserID 和ContentID, 与 Palo Alto Networks 最佳实践完全一致。然后建议详细的变更计划, 一旦批准, 就部署到相关的Panorama设备组策略中。这可以确保快速、准确地授予所需的应用连接, 同时遵守组织的合规政策。

获得对复杂网络的洞察力和控制力

理解和执行网络分段是IT专家面临的一项重大挑战。Tufin的Security Zone Matrix通过直观地映射所需的网络区域与区域之间的流量, 并即时提供有关网络分段的详细见解, 包括允许在不同网络区域之间提供哪些服务, 以及不同物理、虚拟和混合Palo Alto网络的区域敏感性, 从而简化这项任务。Tufin Orchestration Suite还可实时监控跨异构环境的策略变更, 增强Palo Alto安全策略的可视性, 并允许控制标签、安全配置文件和日志配置文件。

主动的风险分析和影响模拟

Panorama设备组或防火墙策略的每一次更改都是对数据安全和应用程序可用性的潜在威胁。如果没有适当的工具,模拟变更的影响几乎不可能实现。作为自动化变更流程的一部分,Tufin Orchestration Suite会根据所需的企业安全策略和内部合规政策,主动检查每个访问请求,以识别和标记潜在的违规行为。同样的主动分析也应用于应用程序连接更改,以确保应用程序符合内部和行业法规。

From	To	Internet	LAN	DMZ-web	PCI Services	Customer Internal	Development	Production	Restricted App	Engineering	Authentication
Internet			C	H	C	M	H	L	C	C	L
LAN	H			H	C	H	H	L	C	H	L
DMZ-web	L		H		H	L	C	M			M
PCI Services	M		C	L		M	L	C			C
Customer Internal	M		M	L	M		L	H			H
Development	M		H	C				H			H
Production			M				M		C	C	C
Restricted App			L				L	L		C	L
Engineering			H		H	H	H	L	H		L
Authentication	L		M	M	L	L	M	C	M	L	
Management	H		H	H	H	H	H	C	H	H	C
HQ Restricted	H		M		M		H	L	M	H	L
Remote Office	M		C	H	C	M	L	C	C	M	C
Internet	L		M		M	L	H	M	H	L	M

Tufin的Security Zone Matrix — 简化、集中的基线,掌控贵司网络安全策略管理

优化您的防火墙,以减少攻击面

Tufin Orchestration Suite 具有以下功能,助力企业在异构环境中优化新一代防火墙:

- 通过识别配置错误、有风险或未使用的规则和对象(包括未使用的用户和应用程序),优化新一代Panorama设备组和防火墙策略
- 自动流程,用于删除未使用或过时的防火墙策略
- 提出建议,以匹配新一代防火墙策略与行业最佳做法
- 防火墙分析和报告工具,帮助安全团队提高效率
- 内置的、可定制的网络和防火墙变更流程

符合行业标准的持续监管

Tufin Orchestration Suite 提供了一个闭环流程,用于执行、验证和记录对PCI DSS、GDPR、NERC CIP和SOX等行业标准的合规性。每项防火墙策略变更都会在设计前进行评估,以确保提前进行安全部署。此外,它还能自动检测可能导致违规的手动更改,并就修复计划提供建议。

Tufin(纽约证券交易所代码:TUFN)简化了对世界上一些最大、最复杂的网络的管理,这些网络由数千个防火墙和网络设备以及新兴的混合云基础设施组成。Tufin Orchestration Suite™帮助企业更灵活地应对不断变化的业务需求,同时保证充分的安全性。Tufin Orchestration Suite可减少攻击面,满足企业对安全可靠的应用连接的更大可视性的需求。自成立以来,Tufin的网络安全自动化已赢得超过2000家客户,使企业能够在数分钟而非数天内实施变更,同时提升其安全性和业务敏捷性。如需了解更多信息,请访问www.tufin.com。



Palo Alto Networks是新一代安全公司,通过为全球数万家企业安全地实施应用和防止网络漏洞,引领网络安全的新时代。凭借创新的方法和高度差异化的网络威胁预防能力,我们开创性的安全平台所能提供的安全性远远优于传统产品或点产品,使企业能够安全地实现日常业务运营,并保护组织最宝贵的资产。如需了解更多信息,请访问www.paloaltonetworks.com。