tufin The Security Policy Company.

5大网络运营痛点及应对方法

满足动态业务需求的各种网络变更，如添加新服务器、更新防火墙规则和停用对象等，都是十分艰巨的任务。这是因为它们的请求比较频繁，手动完成时，它们会成为每个网络和服务器管理员的主要痛点。而且很难平衡。当实施一项变更需要很长时间时，很可能会延迟新服务的推出。而如果你过快地实施一个变更，而不首先检查其对网络的影响，则会导致配置错误，使你的网络暴露于潜在的风险之中。

以下是处理网络相关变更时最常见的五个挑战。您认同其中的几个？

1 服务器克隆

服务器管理员不断要求网络和防火墙管理员为新服务器添加防火墙规则。这些请求通常是这样的："能否请你授予Y服务器（这是一台新服务器）和X服务器一样的网络访问权限？"

对于大多数服务器管理员来说，他们的参与通常到此为止。从他们的角度来看，他们已经完成了自己的份内工作 - 服务器已经上线并准备就绪。但其实，网络/防火墙团队的战斗才刚刚开始。

常见的情况是，没有人知道X服务器可以访问什么，特别是网络的哪些区域，以及它可以穿越哪些安全区域。这正是Tufin发挥作用的时候。使用Tufin SecureChange的服务器克隆将定位整个环境中所有相关的访问规则，并自动将新服务器Y添加到这些规则中。在将新服务器添加到组合中前，不再需要花很长的时间甚至数天来追踪细节（每一个防火墙、每一个规则、每一个对象）。

观看这段简短的视频（2分钟）(https://tinyurl.com/y6xas8kx，了解如何自动替换旧的/添加新的服务器，以节省时间并消除Tufin SecureChange的错误配置风险。

2 服务器停用

鉴于上述情况，当服务器管理员在将新服务器Y添加到网络中时，是否是为了替换另一台已经过时、即将关闭的服务器（服务器X）？
如果是，您如何确保您删除了服务器X的网络访问权限？您必须逐个抓取防火墙，还是（希望）在某个地方有一个可搜索的规则索引？

Tufin的做法是，使用服务器停用工作流删除网络上不再需要的服务器访问。通过这样做，您可以降低该服务器的旧IP地址被重新分配和使用的风险，例如，被恶意用户用来访问其他资产。

Tufin还可以与您的ITSM集成。因此，当服务器人员更新服务器记录时，假设它已经停用，它将自动触发对Tufin SecureChange的API调用，并创建一个服务器停用工单。这样一来，Tufin就可以管理移除旧服务器访问的任务，同时您还能保留对这个过程的控制。

观看这段简短的视频（2.5分钟）(https://tinyurl.com/y6dv8275)，了解您如何通过Tufin SecureChange自动停用服务器 – 从影响评估到无风险移除。

3 应用程序连接请求

防火墙管理员一直在处理工单，一些组织每月要处理超过1000个常规防火墙请求的变更。工程师有许多其他任务，如升级防火墙、升级/更换老化的网络基础设施，以及排除常见的网络故障，他们经常手动处理这些更改，导致了大量的运营开销和更改实施的延迟。Tufin SecureChange提供了一个工作流程，可以帮助您加快这个过程，甚至代替您处理。

Tufin可以与您现有的工单系统集成，甚至可以作为您的工单处理管理控制台。Tufin可实现完全自动化的工作流，该工作流将确定应该在哪里实施规则，确保在实施前根据您定义的安全策略对它们进行检查，甚至按计划推送更改。

观看这段简短的视频（4分钟）(https://tinyurl.com/y3nxpvmx)，了解如何使用Tufin SecureChange快速准确地实施网络访问变更。

4 规则重新认证

有多少次, 防火墙/安全团队被问到这样的问题:”在我们测试一个新的小部件时, 能不能开放X、Y和Z端口到服务器A、B和C, 为期90天?”

这种情况屡屡发生, 涉及多个团队, 他们不断尝试新技术, 需要访问网络的其他区域, 甚至互联网。但是, 由于网络/安全团队人手不足, 工作量高, 谁还记得91天后要删除该规则呢?

通过Tufin, 您可以轻松地看到即将到期的规则, 通过简单的点击, 指定的管理员可以延长所需的时间或确认规则可以被禁用或删除。

观看这段简短的视频(3分钟) (https://tinyurl.com/y6dv8275), 了解如何使用Tufin SecureChange内置工作流程来自动管理规则认证流程。

5 无漏洞服务器部署

当服务器管理员部署一台新的服务器, 并请求授予它访问权限时, 通常情况下, 新服务器会被手动添加到环境中的所有防火墙中。

但是, 服务器的操作系统是否已经打过补丁? 它是否已经更新到最新的操作系统版本?

它是否有什么重大漏洞, 应该防止它暴露在网络中? 您要怎么知道这些问题的答案? 您能发现吗?如果能, 什么时候发现?

Tufin可以通过将API集成到您现有的漏洞扫描器中来回答这些问题。通过将Tufin SecureChange与您的扫描器集成, 您可以自动检查服务器是否已被扫描, 如果没有, Tufin可以请求扫描。建议您将此任务添加到流程中, 在您的网络团队批准之前, 可以添加一个检查来验证服务器的网络准备情况。

除了这五个例子, Tufin Orchestration Suite还有许多其他功能来帮助您加速和简化安全管理及操作。最终提高所做更改的准确性, 并大大减轻网络和安全团队的负担。