tufin The Security Policy Company.

swisscom

Swisscom利用SecureTrack实现防火墙操作的完全可视性

案例研究

环境

为了为其托管服务提供全面的安全保障，瑞士电信运营着150多道防火墙，每道防火墙都包含一千多条规则。我们制定了明确的流程以有效地管理这一庞大的防火墙资产。防火墙运营由四个团队管理，每个团队负责管理生命周期的不同阶段。技术连接小组组长从各项目负责人收到变更请求，并设计所需的策略。安全委员会对这些变更请求进行审查和批准，并将变更请求交给实施团队来部署配置。然后，运营团队监控防火墙并处理所有相关事故。

挑战

2007年，一次外部年度审计发现了一些高风险问题，这使瑞士电信的安全管理部门意识到，他们并未完全控制好防火墙的运行。因此，他们开始立即寻找能够应对以下问题的解决方案：

- 减少计划和实施策略变更所需的时间
- 允许管理员查明导致网络事故的确切变化
- 保证在瑞士电信的150多道防火墙中正确执行所有防火墙政策变更

技术连接和实施团队 – 有效设计和实施防火墙策略变更

过去，技术连接团队只能手动检查和分析防火墙策略，以决定在哪里放置新规则或对象，他们也没有简便的方法来检查拟议的规则是否已经存在。因此，每次设计策略变更都非常耗时而费力。此外，实施团队实施所需的变更后，没有自动流程来确保变更的准确性。再加上在整个瑞士电信庞大的安全运营中执行的大量变更，很明显，当时瑞士电信的技术连接团队正面临着严峻的挑战。

运营团队 – 简化事故处理

运营团队没有任何工具可以用来提取匹配特定流量模式（源、目的地和服务）的规则。他们只能在给定的时间按照源、目的地和服务的其中一个标准来过滤防火墙政策，然后手动关联信息。此外，在发生问题或事故时，他们也无法精确地找出是哪项变更导致的。一旦更改防火墙政策，就无法回头，也无法预测未来的更改可能对网络产生的影响。这使得维护和事故处理过程非常繁琐。

安全委员会 – 确保整体网络安全

作为公共和私营部门的主要服务供应商，瑞士电信每年都要接受严格的审计。为确保整体网络完整性，瑞士电信设立了一个安全委员会，负责审查和监测所有变更，并作为第二级核查和授权。该委员会的职责之一是监控新员工在入职前三个月内进行的所有变更。同样，如果没有自动化工具，这几乎是不可能完成的任务。

最后，瑞士电信目前的安全规划、设计、维护和监督工作大多依靠人工记录。这是一个欠缺准确性而低效的过程，会导致高风险状况，且有可能出现安全漏洞，这是瑞士电信无法容忍的。

优点

- 自动化的防火墙审计和管理操作
- 允许实时监控所有变更
- 减少计划和实施安全变更所需的时间
- 确保遵守监管要求
- 提升整体网络安全

Tufin概览

办事处：北美洲、欧洲和亚太
客户：50多个国家的1,600多家客户
在垂直领域遥遥领先：金融、电信、能源和公用事业、医疗保健、零售、教育、政府、制造业、运输和审计机构
渠道合作伙伴：全球240多个
技术合作伙伴与支持平台：亚马逊网络服务、BMC、Blue Coat、Check Point、思科、F5 Networks、Fortinet、Intel Security、瞻博网络、Microsoft Azure、Openstack、Palo Alto Networks、VMware等。

Tufin SecureTrack解决方案

在对各款竞争产品进行严格分析后，Tufin SecureTrack被认为是瑞士电信的最佳解决方案，它不仅能确保未来所有年度审计的顺利实施，而且完全满足他们对综合策略分析和变更跟踪的需求。

策略分析

首先，Tufin SecureTrack使瑞士电信对防火墙操作的所有规则库完全可视。手动检查防火墙日志的日子一去不复返了。通过完整地显示每个规则和对象，设计团队能够轻松检查提议的规则是否已经存在，或者它的某些需求是否已经被其他规则覆盖。这消除了规则重叠的发生，并全面提升了防火墙性能。Tufin SecureTrack的部署使计划和实施变更所需的时间减少了一半，并确保新规则和规则变更的完美配置。

变更管理和风险分析

Tufin SecureTrack的策略比较功能对于瑞士电信的运营团队来说是一大进步，它为他们提供了规则库在执行更改之前和之后的并行视图。如出现任何问题，运营团队可以立即查明其来源，并收集有关已进行更改、何时进行更改以及由谁进行更改的完整信息。除了事后进行故障排除外，他们还可以在实施策略之前使用策略分析功能识别风险。通过查询搜索规则库中有风险的流量模式，他们能够查看可能将新风险引入策略的特定规则。

安全操作监控

Tufin SecureTrack完全满足全面监控安全操作的需要。它让瑞士电信的安全委员会可以按员工身份过滤数据，并更密切地关注那些较为缺乏经验的管理员所作的变更。Tufin SecureTrack为其提供了充分的可见性，并全面保障网络的完整性。

> “Tufin SecureTrack为我们提供了前所未有的可视性和对防火墙操作的控制，我无法想象没有它该怎么办。我们已经有了严密的流程，自动化SecureTrack的部署使我们能够快速了解防火墙状态，以更敏捷、更主动和更有战略意义的方式进行操作，在更短的时间内完成更多的任务，进而确保安全、合规的操作。”
>
> Michel Müller
> 瑞士电信
> 高级网络安全工程师

Tufin Orchestration Suite™介绍

Tufin Orchestration Suite™是一个覆盖从应用层到网络层自动设计、配置、分析和审计网络安全变化的完整解决方案。它将错误和重做最小化，从而实现快速服务交付、持续遵从性和业务连续性。Tufin提供世界级的安全策略编排解决方案，使世界各地的组织能够准确有效地管理网络配置更改。通过协调涉及多个团队、应用程序、服务器和网络设备的复杂流程，Tufin解决了整个组织中各种涉众的挑战，同时使他们能够更有效地协作。

瑞士电信简介

瑞士电信(Swisscom IT Services)是瑞士领先的信息技术服务提供商之一。其核心业务包括系统集成和IT服务外包，如咨询、网络安全、工作场所服务、SAP管理和电子解决方案。瑞士电信向所有主要行业提供服务，包括电信、医疗保健、公共管理、金融和医疗。更多信息参见www.cisco.com。