tufin The Security Policy Company.

企业安全策略合规手册

如何遵守网络安全标准和机构策略

www.tufin.com

存在风险的丛林环境

每家企业都存在经营风险。风险可能是供应链紧张、地缘政治问题、新贵竞争或该企业特有的许多其他问题。网络安全风险如今已成为人们关注的焦点。网络安全已成为许多机构董事会级别关注的问题。

有许多指南和法规可指导公司减少网络风险：ISO/IEC 27002、NIST网络安全框架、PCI DSS等。机构必须采取适当的控制措施保护其数字资产，这一点至关重要。变更管理是重要的控制措施，因为业务需求决定了需要对数字基础架构进行频繁变更。

网络安全合规性从“勾选原则”的传统观念转变为严格的计划，认真持续执行规定以遵守法规要求并定期审核。许多公司的变更管理程序开始考虑“假设情况”，在批准或实施变更之前预防违规情况的发生。

网络安全首先通过清晰的策略降低业务风险。然后通过IT等运营部门的网络安全专业人员创建、维护和持续执行复杂的规则，控制网络基础架构在法规和内部策略约束下运行。确保企业网络与业务保持同步，在可接受的风险水平运行。

考虑到当今典型IT基础架构的极端复杂性，这是一项艰巨的任务。大多数大型企业拥有多家厂商、多种技术的异构环境，通常包括物理数据中心以及虚拟的私有云和公共云平台。此外，企业不时引入新的网络技术（例如VMware NSX），却继续运行其原有系统长达数月甚至数年。这种混合企业电脑环境如同丛林，管理着数百或数千个物理和逻辑设备，具有任何人都难以尽知的规则。

正如亚马逊热带雨林的阳光几乎无法穿透到森林地面，如今的网络基础架构也缺乏可见度。网络专业人员很少能全面了解混合IT环境的安全性和合规性。此外，在传统、虚拟和云平台上评估风险和应用策略也鲜有一致性。这给必须使用大量工具并检查多个控制台来完成工作的网络安全管理员造成巨大压力。

即使技术和平台如此复杂，企业仍必须维持数据和应用的安全性，并制定验证法规要求和内部策略合规性的措施。必须确保在所有设备和平台的安全机制范围内正确设计、应用和维持策略，包括传统防火墙中使用的子网和区域，新一代防火墙（NGFW）中的应用和用户ID，SDN解决方案微分段和公有云和私有云安全组。难怪安全管理员经常在这样的丛林中迷失方向。

合规与审计就绪—通往地狱之路？

很大程度上，政府和行业法规是为了保护应用和数据以及确保服务连续性而制订的。这当然是出于好意。 但是正如俗话所说：“黄泉路上徒有好意多。”

一般情况下，企业必须在多种法规和安全标准的要求下经营。这些要求的变更速度和广度对于必须理解和应用规定的公司来说是一个艰巨的挑战。根据《2015年汤森路透年度合规成本调查》显示，70％的受访公司预计监管机构在明年将发布更多监管信息。[1] 这会导致“监管疲劳”，因为太多的约束性法规会妨碍敏捷性 。

此外，对于许多机构来说，合规性负担正在增加，但是IT机构用于合规性的预算却未能跟上增长的步伐。被迫以更少的资源完成更多的工作，IT负责人认识到自动化是必然趋势，以便从业务应用角度清楚地了解合规性和风险状况。遗憾的是，许多公司仍然使用人工流程。汤森路透的合规性调查显示，39％的公司仍在使用人工电子表格追踪其合规情况，[2]从而增加了公司面临的风险和不合规的可能性。

通过审核验证对法规和内部策略的合规性，对IT部门来说是一个很大的负担。审核准备工作需要花费时间和金钱 – 整理网络状态文档，并通过物理测试和证明来验证控制措施。例如，审核员可能希望检查所有防火墙规则并测试其中的一部分以确保合规性。一家企业每年针对各种法规（例如PCI DSS和SOX等）可能需要进行几次内部审查和外部评估审核。而且，如今业务合作伙伴在签订服务合同之前要求进行控制评估也变得越来越普遍。这导致了审核工作更加繁重。

企业可通过保持“持续合规”状态来减少合规性和审核准备负担。即达到满足所有合规性要求的状态，然后连续保持该状态。通过自动验证平台和厂商的所有网络配置更改并自动生成审核记录来完成维护工作。保持持续的合规性比采用“时间快照”方法保持合规性更容易且耗时更少。在该情况下，每次进行审核，都要使一切达到合规状态，这是一种重复的工作。

监管挑战

[2] Ibi

由于制订原因和执法机构不同，各种法规的标准并不统一，有时甚至会存在不一致。企业需自行斟酌遵守哪些标准，然后将这些标准转换为规定安全设备如何控制网络通信的规则和策略。这意味着对受监管数据、使用数据的应用、应用的位置和交互的深入了解。合规人员不一定是精通IT的人，而IT人员也不总是对所有法规都了解。实现和保持合规性是一项非常复杂的任务，若没有团队合作和技术自动化就无法完成。

有趣的是，一些针对特定区域制订的法规成为了其他区域的规范。如美国法规NERC CIP。北美以外的许多公用事业公司也遵循此法规的准则。欧洲数据保护改革法规也是世界其他地区数据隐私和保护的规范。

表1仅列出了一部分最常见的政府和行业法规。[3]

政府或行业法规或标准	法规适用机构
DISA STIG – 国防信息系统局安全技术实施指南	美国国防部（DoD）机构
FERPA – 家庭教育权利和隐私法	根据美国教育部适用计划获得资助的所有学校
FISMA - 联邦信息安全管理法	• 美国联邦政府内的所有机构 • 负责失业保险、学生贷款、医疗保险和医疗补助等联邦计划的州立机构 • 与美国政府有合同关系的任何私营公司，无论是提供服务、支持联邦计划还是接收补助资金
GDPR – 通用数据保护条例	• GDPR适用于收集或处理欧盟居民个人数据的所有实体 • 数据保护指令的第二部分适用警察和刑事司法部门
GLBA – 格雷姆-里奇-比利雷法案，又称1999年金融服务现代化法案	“主要从事”向美国消费者提供金融产品或服务的所有公司，无论规模大小

[3] 其他数据隐私法规列于2015年国际数据隐私法汇编 ， BakerHostetler发布

HIPAA – 健康信息携带和责任法案	有权访问、处理、存储或管理受保护的健康信息的所有美国实体及其业务伙伴（BA）
HITECH – 经济与临床健康信息科技法案	有权访问、处理、存储或管理受保护的健康信息的所有美国实体及其业务伙伴（BA）
ITAR – 国际武器交易条例	美国军事用品管控目录上制造、出售和分销与国防及太空有关的商品和服务的所有实体
NERC CIP – 北美电力可靠度公司关键基础设施保护标准	北美电力系统的运营商，也为全球许多其他地区的监管体系提供参考
NIST – 美国国家标准及技术研究所网络安全框架	任何希望遵循自愿性框架（基于现有标准、准则和惯例）以降低关键基础设施的网络风险的实体
PCI DSS – 支付卡行业数据安全标准	接受、传输、处理或存储各种支付卡持卡人的数据的所有机构或商家，无论规模或交易量如何
SOX – 2002年萨班斯-奥克斯利法案	美国公开上市公司及其在美国公开上市或在美国开展业务的全资子公司和外国公司

表1：部分法规列表

企业安全策略挑战

除了外部监管外，大多数机构都制定了网络内部规则。但是，仍然有一些机构尚未制定内部安全策略。在这种情况下，他们可能需要帮助来制定策略，其被认为是提高网络安全性的最佳实践。

一般而言，企业安全策略是阐明公司计划如何保护其物理和信息技术资产的文档。主要挑战是该策略通常非常复杂。由于网络变得高度动态，为当今的高度敏捷的业务提供服务，因此很难追踪所有更改并保持对企业策略的持续合规性。

企业的安全策略通常包括可接受的使用策略。可接受使用策略的规则可包括公司允许（白名单）或不允许（黑名单）通过公司网络或入站流量访问的子网和主机。例如，假设某个机构与梦幻体育没有实际业务需求，则可能选择不允许员工访问梦幻体育网站。另一方面，它会将在业务运营中起重要作用的网络服务（例如已批准的SaaS应用）的IP地址列入白名单。

如今，许多企业都订购了威胁情报服务，该服务会定期汇编存在安全威胁的IP地址。例如，僵尸网络和受病毒感染网站的命令和控制服务器。此类列表会经常更新，并且此任务的快速性可能会阻止验证新规则或更新规则不会引起违规疑虑。

另一个主要挑战是，东西流量的域间访问必须符合合规性要求，确保合理分段。例如，规范能源部门的NERC CIP版本5标准要求将电网网络资产归入大型电网（BES）网络系统，并根据影响因子对关键基础设施的风险类别进行分类。由策略定义，在整个企业范围内集中管理分段，以减少攻击面，同时保持合规性。

最后，拥有传统技术的企业在安全性和合规性方面面临其他挑战。Gartner[4]最近的一项研究指出，“传统配置管理工具不是基于策略的。它们并不总是能实时报告或将网络问题与设备配置相关联…需要网络自动化来满足企业对数据中心和混合云敏捷性的要求。”

在复杂的IT环境中确保合规性的步骤

尽管当今IT环境的复杂性以及企业策略和法规要求不断增加带来了挑战，但通过妥善规划、周密流程和技术自动化，仍可实现持续合规。首先，我们将说明需要采取的步骤，然后说明自动化在整个过程的必要性。

确保持续合规的六个步骤：

1. 定义机构安全策略
2. 发现现有的网络拓扑
3. 定义系统架构，并根据企业策略重构拓扑
4. 识别安全漏洞，根据策略调整
5. 为变更请求创建定义明确且可审核的流程
6. 审核就绪

以下说明为何每个步骤皆为持续合规的要素。

步骤1: 定义机构安全策略

机构安全策略为业务驱动，定义公司如何保护其信息和技术资产。定义高级别安全策略时应考虑以下方面：机构必须遵守的外部法规要求和行业标准（例如PCI DSS、NIST、SOX、HIPAA、NERC CIP等）；内部管理要求（例如，可接受的使用策略）；以及公司遵守的一般最佳做法。

[4] “Effective Network Orchestration Starts by Automating Provisioning”, Simon Richard, 2015年8月31日

公司的安全策略可包括公司如何培训员工保护公司资产，对安全措施将如何执行和实施，以及评估安全策略有效性的程序，确保进行必要的更正。

为实施统一的安全策略，需要将特定要求转换为技术规则，定义允许/不允许流向/通过各个网段的安全设备的流量。例如，接受信用卡的商户受PCI DSS的监管，建立和控制收集、处理或存储敏感持卡人数据的网段的安全范围。不允许其他类型的应用共享或访问此网段。机构还必须制定规则，控制允许哪些连接和流量进出网络PCI DSS分段。

步骤2: 发现现有的网络拓扑

在过去十年里，大多数企业网络都发生了巨大的变化。随着组织采用虚拟化、云计算、移动计算、软件定义的基础架构等，拓扑结构发生了巨大的技术转变。因此，至关重要的是了解本地、云和混合网络中现有的网络拓扑，包括所有分段和区域。企业必须深入了解其网络拓扑，才能计算需要管理的安全区域的数量。该网络图须包括所有业务应用，其连接性和依赖性，以及厂商和平台的现有安全策略。这是件难以做到的事情！所有此类信息皆有助于了解当前的安全性和合规性，并最终为流程自动化创建可重复的任务。理想的情况是将所有此类信息配置于一个方便的位置—但不是人工电子表格！

步骤3: 定义系统架构，并根据企业策略重构拓扑

下一步是根据安全区域（由保护数据和应用的企业策略规定）定义系统结构。仅保护周边已不再足够，需要内部分段将敏感资产与通常可访问的区域隔离开来。对网络过分细分（例如为每个应用定义安全区域）的公司面临着复杂的安全监管和管理带来的风险和成本。

准确呈现网络拓扑图可帮助分析由传统防火墙和新一代防火墙建立的网络分段，并识别需要进行哪些更多的分段。

步骤4: 识别安全漏洞，并根据策略调整

在此阶段，统一的安全策略是网络的“期望”状态，而不一定是网络的“实际”状态。实际状态是不同平台的安全策略的集合，无论是物理和虚拟防火墙中的安全规则和微分段，还是私有云和公共云平台中的安全组。有必要比较两者，识别存在的任何安全漏洞，并尽可能采取措施修补这些漏洞，并使网络配置完全符合所规定的策略。

继续上面的PCI DSS示例，“期望”状态是其他应用不能访问处理支付应用的网段。但是，与实际状态比较之后，漏洞分析表明，营销应用也驻留在该网段，以便在特殊场合下从支付应用访问客户数据。这不仅严重违反了PCI DSS，而且使企业面临着代价高昂的数据泄露风险。应给这一情况做个标记以进行修正。

步骤5: 为变更请求创建定义明确且可审核的流程

清理网络环境并使“实际”状态达到策略的“期望”状态只是一个开始。接下来，机构需要一个处理网络配置更改请求的流程。由于业务需求会随时间变化，因此经常会发生变更请求。许多公司正在采用如DevOps的方法，对应用执行更快的更改。通常情况下，应用更新需要修改网络配置，并且需要非常迅速地进行这些更改以跟上业务发展的步伐。网络团队必须有一个流程来迅速响应请求。

每次配置更改都有可能违反安全策略，导致“不合规”状态，这种状态可在审核中检测到，并可能导致安全漏洞或其他影响。当网络是“干净的”（即完全符合策略）时，重要的是评估变更请求及其将产生的影响，并再认证网络将维持持续合规状态。

随着网络安全变更快速发生，对策略、防火墙规则和变更请求的再认证对于在合规丛林中生存至关重要。某些法规，例如PCI DSS和规范能源行业的最新NERC CIP版本5网络安全标准，要求对现有策略进行定期审查和再认证流程/工作流，以证明合规性。通常，再认证使规则优化变得更加容易，包括清理、删除被覆盖的、未使用的和过度许可的规则库。此外，再认证使网络安全变更承担责任。再认证流程包括根据策略评估请求，确认请求的配置更改是否可允许；换句话说，它不会导致策略违反事件。若确实造成违规，应将请求发送给有权拒绝请求的人士，建议对其进行修改，或在指定时间段内允许。若允许请求，应为其指定一个失效日期，以确保不合规操作不会永久保留在原地。

此外，该变更控制流程需要创建文档，准确记录更改内容，更改的业务目的，以及谁请求的更改。该文档需要包含足够的信息，以便审核员了解更改内容和原因。若出现问题并且需要追踪变更的原因，此文档即可派上用场。

再认证流程的重复性使其非常适合自动化工作流程。

步骤6: 审核就绪

机构调整策略以通过特定的审核，然后在审核之后恢复其通常的工作方式十分普遍。这不仅是一种资源密集型方法，而且对提高安全性和验证合规性几乎没有积极作用。更好的方法是保持对安全策略的持续遵守，机构可随时进行审核，无论是内部审核还是外部审核。需要创建记录上述所有步骤的文档。证明合规性的其他方法包括报告、变更审核和历史以及每次变更的再认证。

您的生存工具包:The Tufin Orchestration Suite™

上面列出的步骤涉及到许多错综复杂的情况，而复杂性会增加风险。生存下来的唯一方法是使用网络安全策略编排。它帮助机构发现何时处于风险中，并提供如何减轻风险的指导。

Tufin Orchestration Suite™可在物理、虚拟和混合环境中提供必要的自动化。Tufin的Unified Security Policy™ (USP)可通过单一虚拟管理系统在一个位置集中管理所有机构安全策略。Orchestration Suite提供了对网络上所有应用以及它们之间和与安全设备之间关系的可见性。Tufin解决方案建立并维护网络拓扑的动态模型，包括所有网段和应用连接依赖性，无论它们是在企业数据中心、云还是混合IT环境中。分析引擎分析风险的可能性，确保网络所有未来的更改都符合集中策略，并警示网络中可能引起违规的新情况。Tufin解决方案可识别安全漏洞并对违反策略的情况发出警报，从而减轻风险。Tufin Orchestration Suite还可通过自动审核追踪、按需报告和合规记录，使企业随时审计就绪。

该套件由相互交互以及与网络基础架构和业务应用交互的几个组件组成，分析变更风险，变更批准后将其发送到整个基础架构中。该套件还支持应用编程接口（API），与计算环境的其他要素进行通信，例如IT服务管理系统。架构如图1所示。

图1: Tufin Orchestration Suite的架构

对各组件的简要介绍如下。

- ***Application Connectivity***组件使机构对业务应用和服务进行建模，定义其工作所需的网络资源。识别和保存网络资源，并记录须与安全设备通信的应用。

- ***Security & Compliance***组件包含整个IP网络的企业统一安全策略。USP（下面将更详细地介绍）定义了机构必须执行的期望/要求的安全策略。包括分段策略、最佳做法策略、合规性策略以及机构内部希望遵守的任何其他安全策略。

- ***Network & Security Automation***组件可实现网络变更自动化。该组件执行安全自动化，同时与“Security & Compliance”组件核对，确保这些自动化更改不会违反需要遵守的安全性和合规性策略。

- ***Abstraction Layer***组件隐藏了其他组件的网络复杂性。它映射并保存网络拓扑，并与网络中运行的不同网络和安全技术进行交互。

- ***RESTful APIs***组件可对套件的任何组件进行完全编程，从而可与企业系统和技术轻松集成。

值得注意的是，所有这些组件都可在各种物理和虚拟网络，基于云和内部的应用和系统运行。

Tufin解决方案的要素之一是统一安全策略（USP）。USP提供了在一个位置集中管理所有机构安全策略的能力。USP自动执行复杂的策略管理流程，复杂的规则库以及不断提交的多厂商/多技术网络的变更请求。从传统配置开始，USP根据期望的网络分段控制实际的网络分段，显示存在的违规情况，以便企业纠正。当网络变得“干净”，在进行安全更改之前对违规情况发出警报，帮助防止违规或风险。USP确保网络中所有未来的更改都符合集中策略，并对网络的任何新违规情况发出警报。

USP简单直观地显示机构网络中存在的多厂商防火墙、路由器和其他设备的网络分段。所显示的区域可在物理、虚拟或混合网络上。图2显示了USP的用户界面，展示了PCI DSS矩阵。彩色块表示企业网络的不同网段或区域之间的通信权限。可以清楚识别分段允许使用哪些服务。

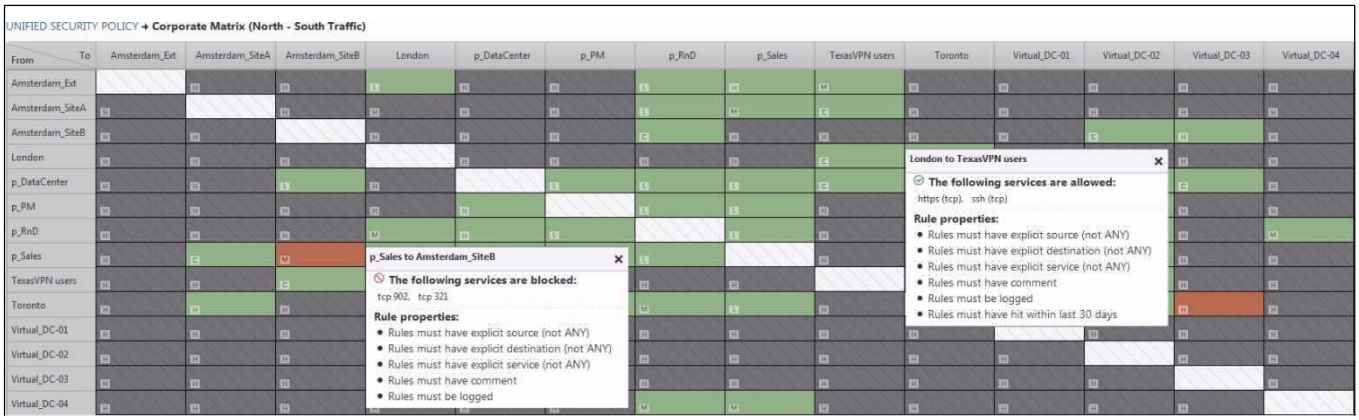

图2 – 企业范围的统一安全策略区域矩阵

Tufin“生存工具包”的另一个重要方面是自动化网络安全更改流程。大多数行业法规要求安全更改必须遵循标准的、可审核的更改流程，并详细记录。一些法规还要求遵守自动化流程。Tufin Orchestration Suite支持为安全更改定义和执行更改流程，或扩展由企业更改管理系统执行的更改流程。可以通过安全性和合规性分析，变更设计和实施来完成端到端地自动化变更流程，最大程度地提高敏捷性并确保策略控制。Tufin解决方案还可以识别并警示变更管理流程之外进行的变更，以及与批准的变更请求不符的变更。

结论

Tufin通过网络安全策略编排，实施统一安全策略，网络配置自动化和变更管理来帮助企业应对法规和机构合规性要求的挑战。Tufin解决方案帮助识别应用及其连接依赖性和设备配置。这有助于对资产进行分组，以便一致评估和应用策略，并持续监控企业所有平台（物理、虚拟和云）的合规性。

Tufin帮助机构完成对内部和外部法规要求的持续合规性和审计就绪。每次网络更改都会自动记录在审核追踪中。进行每次更改之前，都会自动进行风险评估。工作流流程需要获得业务批准才能进行更改。批准后，更改将自动传播到适用的安全设备中。对流程的完成进行验证，为审核合规提供了依据。此外，自动化的工作流流程可帮助机构减少对培训、人工操作以及追踪正在发生的情况的繁琐工作的需求。

总而言之，对于需要保护其复杂网络并保持持续合规性和审计就绪状态的机构，Tufin Orchestration Suite是必不可少的工具。

Tufin简介

Tufin (纽约证交所交易代码: TUFN) 简化了全球一些最大型复杂的网络的管理，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架构组成。企业选择Tufin Orchestration Suite™在不断变化的业务需求下提高敏捷性，同时保持稳定的安全状态。Tufin Orchestration Suite减少攻击面，满足对安全和可靠的应用连接的更大可见性的需求。自成立以来，Tufin的网络安全自动化服务已拥有2000多家客户，使企业能够在数分钟而不是数天的时间内实施更改，同时改善其安全状况和业务敏捷性。