tufin The Security Policy Company.

在新常态下保护网络安全
通过自动化加速决策和响应时间

化转型几乎是一夜之间发生的，这就是新的现实。疫情过后，组织都在想办法，弥合曾经有效（且运行良好）的流程和工作流与需要调整以适应，新常态的流程和工作流之间的鸿沟。

为适应复杂的新常态，企业需要安全策略自动化。网络和安全团队现在要面对在外围运行的应用程序，用户在边界之外的移动，以及网络异构性的增加。这导致网络更加分散，组织需要管理的防火墙或类似防火墙的解决方案数量大幅增加。网络和安全专业人员现在必须利用更多的工具、操作和知识来完成工作。任何一个人都不可能同时精通所有这些技术和平台。组织需要自动化、统一化和集中化的管理，以控制谁可以和谁对话，什么可以和什么对话，以跟上这些变化的规模。

最近，我们与网络安全领导者进行了数十次对话，以了解他们应对远程办公的方式、变化对其网络安全的影响、所部署的解决方案以及下一步计划。在本指南中，您将了解我们反复提到的行动和建议，以适应不断变化的环境，更好地为未来的突发事件做好准备。

企业如何应对“一夜之间”的转变？

疫情使企业的运作方式发生了巨大变化。根据对大型组织的调查，在3月初，许多公司不得不在短短几天内将其远程工作队伍的规模增加5至7倍。一家大型银行的远程员工从5000人增加到4万人。现在，很多组织的员工中90%以上都在远程办公。

网络团队原本就面临很多挑战，现在又增加了一系列障碍 – 他们不得不处理大量的访问更改请求，以适应夜班工作。对速度的要求使他们无法遵循所有的安全规范，甚至无法利用最近获得的一些技术。

快速转变：重要发现

远程用户增加

5-7倍

在家办公的员工比例

>90%

网络变更请求

急剧增加

大多数IT部门依靠现有的、成熟的技术来实现远程访问。一些公司部署现有的本地远程VPN解决方案，其他公司则使用防火墙供应商提供的远程访问VPN解决方案。此外，许多公司针对一小部分员工使用了远程虚拟桌面基础设施（VDI）技术。

为满足流量需求，管理员必须用员工的新IP池快速更新网络安全设备和防火墙。此外，一些组织还设置了额外的VPN网关，以满足所需的流量容量。

密歇根州的CIO办公室：橙色条代表了每月的访问变更请求数量，我们可以看到，3月份增加了30-50%。

快速转变：重要发现

使用的技术：

依靠传统技术和现有技术（虚拟专用网络、虚拟数据交换）

实施：

- 增加IP池的规模/建更多的池
- 同一个池中的用户获得相同的访问权限

结果：

扁平的网络，尽可能少的分段，过度宽松的访问，增加攻击面

VPN：使访问成为可能的首要技术

基础设施的变更发生得非常快，往往没有进行标准的安全和风险审查。大多数组织更改了他们的VPN配置，增加IP池或创建额外的池，以满足所有用户的访问需求。通过部署少量的远程访问IP池，所有连线的远程员工都可以获得相同的内部网络资源访问权限。

令人意外的是，即使是已经升级到新一代防火墙（NGFW）的组织也未能使用它们，更好地保护和控制通过VPN连接的远程用户。据推测，这是由于他们无法简单、快速地将NGFW策略转换到其他传统网络安全设备，以实现端到端策略执行。

绕过控制以快速实现访问

由于变化的速度很快，实现快速访问的最简单方法是授予访问权，而不管员工的角色和正常权限级别如何。此外，大多数变更并没有遵循标准的变更和评估程序，也没有完整的记录。而且，很多都是手动进行的，这会导致更多的人为错误和错误配置。

因此，访问控制只能依靠特定应用的用户权限和认证。从本质上讲，忽视分段意味着入侵者能够轻松访问网络和横向移动。更重要的是，这与良好的安全实践背道而驰。为了适应远程员工的变化，安全态势被削弱；额外的不必要的访问导致攻击面增加。

您当前可以采取的三个基本步骤

根据与几位CISO和高级网络安全领导的讨论，最有效的方法是：首先制定一个坚实的、可操作的、基于三种不同实践的框架，然后认真贯彻。Securing Your Network for the Remote 为

远程员工保护网络安全：基础知识检查表

1 查明、评估风险并确定其优先次序

为改善安全态势，组织普遍认为，首要任务是识别和评估安全漏洞，并确定风险的优先级。需要对快速做出的变更进行重新评估，以降低风险，防止审计问题，并恢复合规。这将使您能够在复工过程中抢占先机。

✓ **确定做了哪些变更，由谁做，变更的原因，并了解远程员工现在拥有的网络访问权限。**

小贴士

Tufin Object Change Report（对象变更报告）https://tinyurl.com/y2ola474可按设备、安全组或时间段提供即时可见性。在这里，您可以查看对象（服务、用户和网络对象）的更改列表。该报告标记了对象被变更的确切时刻和变更者，并对关键对象的敏感变更发出警报。

✓ **确定所有访问变更是否必要。对于风险较高的区域或资产，确定访问是否有正当的业务理由，以及是否使用了访问规则。**

小贴士

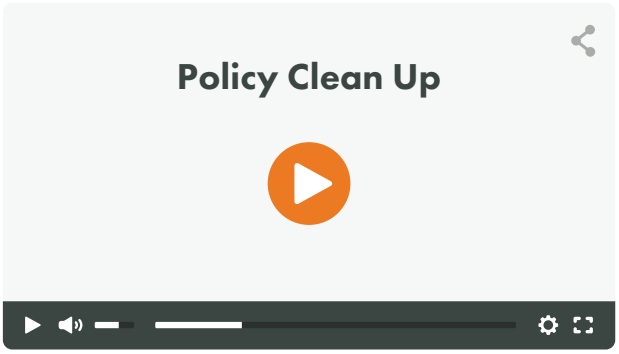
Tufin Rule and Object Usage Report（规则和对象使用情况报告）https://tinyurl.com/y2yhrvvr提供了有关使用最多/最少和未使用的规则及对象的统计数据。在这里，对于每个规则或对象，您可以查看通过或被阻止的、有记录的网络（“规则命中”）流量的数量。您可以使用此报告来优化您的规则库，确定哪些规则未被使用，因此考虑删除，哪些规则被大量使用，因此应在规则库中向上移动。未使用的对象也应该成为删除的候选对象。

此外，您可能希望查找带有失效日期的规则，或者在某个特定日期之后注释部分留空的规则。这有助于识别和评估那些可能过于宽松的规则。

评估变更的风险。根据组织的安全政策来衡量访问规则，以确定对合规性的影响。

小贴士

Tufin SecureTrack (https://tinyurl.com/yxttzkw8) 提供风险评估、许可级别检查以及针对您的分段策略的规则变更验证。在这里，您可以设置您的策略，了解多供应商、混合网络的所有防火墙变更。您可以查看基于规则命中、区域变更或异常端口网络行为等检测到的策略违规行为。一旦检测到违规行为，您可以使用Tufin SecureChange对规则进行修改和变更，以降低风险。



观看这段简短的视频（7分钟）(https://tinyurl.com/yxs7ymex)，了解如何从完全映射的规则中快速、准确地清理网络策略。

2. 执行快速修复，以实现快速有效的缓解，同时保持业务连续性。

一旦评估了风险，就会推荐安全政策最佳实践。以下是可以轻松实施的快速改进列表，以帮助您在不妨碍业务连续性的情况下改善网络安全态势。

重新评估有风险的访问权限变更，以判断每一个变更是否必要，评估访问是否有正当的业务理由，以及所有访问规则是否真的被使用。这可以确保涉及敏感资产/区域的变更经过既定的风险分析、验证和批准流程。

小贴士

使用Tufin SecureChange来模拟变更，并进行影响和风险分析，确保与组织的安全策略相一致。这可以作为一个独立的步骤，也可以作为访问变更请求工作流程的一部分。

观看这段简短的视频（4分钟）(https://tinyurl.com/y3nxpvmx)，了解如何使用Tufin SecureChange访问请求工作流来快速、准确地实施网络变更。

通过执行规则优化或清理，收紧远程访问策略。

用更细化的规则取代过度允许的规则。“过度允许”被定义为允许未使用的访问。这有助于建立最低权限访问，确保远程用户只被授予必要的访问权限。

小贴士

Tufin Automated Policy Generation（APG，自动策略生成）(https://tinyurl.com/y2n9or3g)检查实际流量，并推荐一套规则/对象，以降低或减少现有规则的许可级别或范围。APG可以处理来自任何领先防火墙供应商的数周或数月的日志数据。

停用未使用的或多余的规则，这些规则可能是在匆忙启用远程员工访问时实施的，或由于在进行变更时不知道真正需要哪些访问。

Tufin SecureChange提供了无限的、可定制的工作流，帮助您自动设计、审核和实施网络访问变更。

小贴士

您可以使用Rule Decommission（规则停用）工作流(https://tinyurl.com/y6ze78a9)来停用未使用的、过度宽松的规则，或使用Rule Modification（规则修改）工作流(https://tinyurl.com/y4fygnve)来执行现有规则的变更，同时保持业务连续性。

观看这些简短的视频（每个约2分钟），了解如何使用Tufin SecureChange来修改或停用规则。

(https://tinyurl.com/y6ze78a9)

(https://tinyurl.com/y4fygnve)

创建基本的远程访问分段策略，以根据角色/组/位置区分远程用户。这将帮助您对远程用户应用与内部网段相同的分段原则。

小贴士

Tufin提供了基于预定义区域的即用型细分模板，帮助您针对特定区域和AppID设置允许/阻止流量。

From \ To	DMZ	Internal Network	Internet	Third Party Network	Unassociated Networks	VDI Access - Citrix	VDI Access - VM Horiz...	VPN Users
DMZ	✓	⊘	⊘	⊘	⊘	⊘	⊘	⊘
Internal Network	⇄	✓	⊘	⊘	⊘	⇄	⇄	⇄
Internet	⊘	⊘	✓	⊘	⊘	⊘	⊘	⊘
Third Party Network	⊘	⇄	⊘	✓	⇄	⊘	⊘	⊘
Unassociated Networks	⊘	⊘	⊘	⊘	✓	⊘	⊘	⊘
VDI Access - Citrix	✓	⇄	⊘	⊘	⊘	✓	⊘	⇄
VDI Access - VM Horiz...	✓	⊘	⊘	⊘	⊘	⊘	✓	⇄
VPN Users	✓	⇄	⊘	⊘	⊘	⇄	⇄	✓

3. 规划未来 – 长远考虑

通过应用更细化的分段策略（如基于用户ID）改善安全态势。

通过利用NGFW的用户身份技术，创建更精细的分段策略。这使您能够基于身份和上下文而不是IP地址应用网络安全策略，从而允许用户从任何地方访问。

应用规则再认证流程

对所有修改后的防火墙规则应用适当的重新认证流程，以确保定期重新认证防火墙规则，并且组织仍然需要这些规则。

小贴士

Tufin SecureChange Rule Recertification Workflow（规则重新认证工作流程）(https://tinyurl.com/y2enn57u)，可以帮助您通过完全自动化跟踪、监控和管理防火墙规则失效的过程，简化规则重新认证流程。Tufin可以自动识别即将失效的规则，提供规则元数据的可见性，并实现跨供应商和平台的自动重新认证，帮助您保持持续合规，并简化审计准备工作。

自动化原有的手动流程，以实现快速、准确的变更

几乎每一次网络访问变更都涉及到多个多厂商防火墙、交换机和路由器以及安全组的复杂实施。手动执行这些任务不仅无法及时处理工单，而且会将网络暴露于潜在的风险之中。即使只有60%的变更是自动化的，也能节省大量的时间和成本。

> 2020年，**99%的防火墙漏洞**由防火墙错误配置、而不是防火墙缺陷引起。
>
> 高德纳称，对于大多数企业来说，一个品牌的防火墙是一种最佳实践

小贴士

使用Tufin SecureChange工作流配置(https://tinyurl.com/yyeehsl9)来设置工作流，自动简化变更流程中的每一步，确保快速、准确、有记录的访问变更流程。这将帮助您消除日常操作中的瓶颈，并消除配置错误的风险。SecureChange确保每一个策略变更的安全影响都经过评估，然后在您的混合、多供应商网络中自动实施。工作流程是完全可定制的。

观看这段简短的视频(4分钟)(https://tinyurl.com/yyeehsl9)，了解如何使用Tufin SecureChange创建工作流程，以简化网络变更实施流程，并帮助您满足组织流程的特定需求。

在今天这样特殊的情况下，组织比以往任何时候都更需要用更少的资源做更多的事情，比如管理资源短缺，快速响应，并在瞬息万变的环境中应对变化和解决问题。因此，拥有清晰的、有据可查的、可重复的流程，并将人工干预降到最低，变得至关重要。通过实施经过验证的、高度安全的实践来加速变革流程，您的组织将能够自如地应对下一次危机。