SOLUTION BRIEF

FortiCWP 流量分析

管理层摘要

如今的多云环境提供了更好的灵活性，但是也降低了安全可见性：使用云和服务越多，随之而来的攻击平面就越大也越复杂。第一步就是要提升多云安全态势，来获得一个针对跨Region和云的资产和资源的中央化且实时的态势视图。第二步是对流量进行检测，并通过全球化的威胁情报来识别可疑行为，以分析真实流量和可接受流量之间的差距。在执行了这些之后，安全团队可以通过查看威胁数据的全部上下文信息来快速获取对态势的洞察。而上述能力都是可以由FortiCWP来提供的。

FortiCWP管理云安全态势

- 通过云平台API获取全面数据，提供中央化可视化能力
- 跨多云的一致安全管理
- 通过多个全球威胁情报服务分析流量
- 能够获取从Region到独立服务和应用的全部上下文
- 追溯，分析，审计更简单

多云环境更容易藏匿威胁

有太多的原因解释为何公有云服务以17.3%的增速增长，并在2019年达到2060亿美元的全球市场规模[1]。云计算提供了更强的灵活性，更快的价值实现，以及在应用运行过程中能够进行高度的弹性扩缩，并只需为使用的资源而付费，从而节省大量成本。

对于安全团队来说，不好的是，多云中的资源通常被不同的业务组部署在不同的Region中，同时缺乏集中控制。云中的资产持续变化，可见性受限，并且云平台提供的内建安全工具各自为战，关注点不同，产生的安全数据也不同。

这样就带来了一个更大的攻击平面，难以监控网络流量，并提升了网络安全风险。根本性的挑战如下：

- **缺乏可见性**。传统安全监控工具不能应用到云资源、服务以及之上的基础设施。安全团队没有一个有效的工具来维护云中完整的可见性。
- **难以检查流量**。尽管有准确的资产管理配合，由于缺乏合适的工具，监控云内和云间的流量并检测流量中的可疑行为也还是一件难事。
- **复杂性拖慢了安全调查速度**。碎片化的安全解决方案不能让安全团队深入到数据和特定的可疑安全事件中。这将降低攻击事件的响应速度，提升安全风险。

FortiCWP帮助用户快速获得洞察

FortiCWP通过提供如下能力让安全架构师应对上述挑战：

1. **中央化可视化**。FortiCWP使用使用API访问公有云基础设施，从而为用户使用的公有云服务提供一个单独、中央化的安全态势管理窗口。安全团队可以浏览当前云中的资产、服务和资源，以及与之关联的各项风险数据，来快速、集中化的对多云进行统一安全策略管理与执行。
2. **流量分析和威胁检测**。FortiCWP能提供安全管理员所需的可见性来帮助其保护公有云基础设施的内部和外部威胁，来保护其中的资源和服务。通过与FortiGuard Labs提供的失陷信标（IOC）和反僵尸网络数据库集成，FortiCWP可以检测实现云主机和恶意流量，并可以检测出从可疑IP地址连接到敏感工作负载的流量。

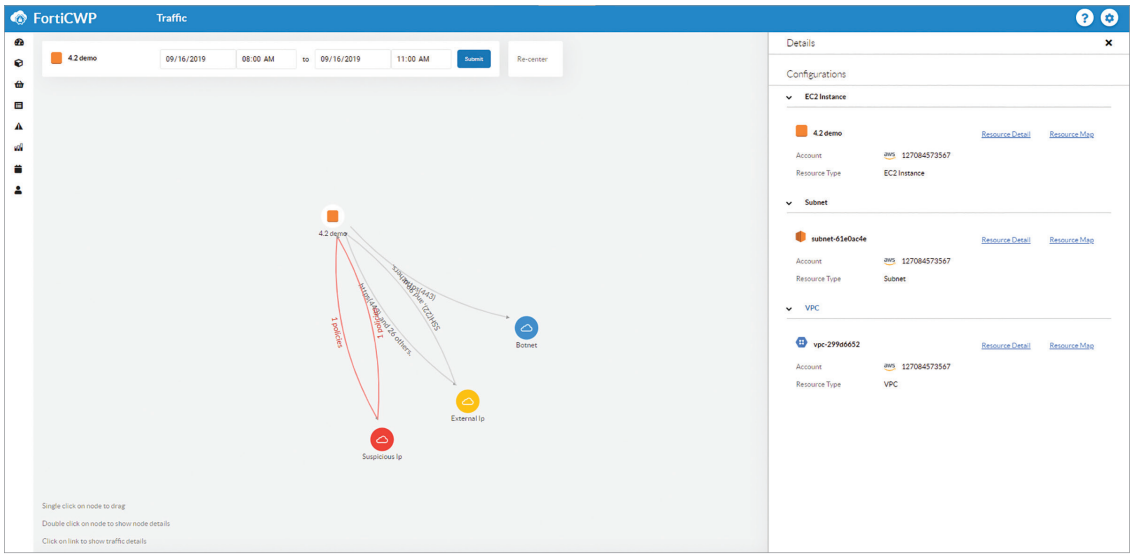

Figure1：可视化云内和云间流量及网络拓扑

来自FortiGuard Labs的威胁情报是由遍布在全球的200余名安全研究员从440余万个传感器产生的数据中分析并生产而来。这个网络还结合了战略性全球安全机构，关键技术合作伙伴以及网络安全联盟。所有这些信息都支撑着FortiCWP，提供最新最及时的保护，防御0-day威胁、僵尸网络、病毒和其他恶意漏洞利用。

3. **为调查提供完整上下文信息**。当一个攻击或不能接受的威胁被检测到，FortiCWP能够让安全团队通过直接查看每个云服务的配置文件，以及查看这些服务关联的流量模型，获得其所需的全面安全信息。这个解决方案让用户能够以很快的速度便能理解安全事件的上下文信息。安全团队可以通过流量可视化来快速查看一个云主机在特定时间范围内的流量进出站情况，并通过直观的图形展示来精准定位可以行为。这让流量追溯、分析和安全事件审计变得很简单，更容易复查安全事件影响，提升安全态势。

多云安全的基础

中央化可视化、洞察与控制能力是一个统一多云安全态势管理解决方案的基石。FortiCWP提供完善的报告工具和高级的控制能力来为组织的多云环境提供极具扩展性的统一安全策略管理与执行。

[1] Louis Columbus, "Roundup Of Cloud Computing Forecasts And Market Estimates, 2018," Forbes, September 23, 2018.

September21,201910:04AM

488526-0-0-EN

D:\Fortinet\Work\2019\September\092119\sb-forticwp-traffic-analysis