

虚拟私人网络安全防护的多措施应用

孙玉峰, 郭志新, 张大志

(中工国际工程股份有限公司, 北京 100080)

摘要 本文探讨了VPN在现代IT中应用的重要性, 说明了VPN在企业实际应用中遭遇多样化的网络攻击, 并提出了一系列预防、监测和阻断策略, 首先通过VPN登录机制、VPN白名单机制、VPN加密算法升级、漏洞管理和补丁更新和VPN访问控制等策略进行VPN网络安全预防; 其次通过相关流量的监测、登录日志审计和入侵检测系统等策略进行VPN网络流量监测; 最后通过其他安全设备和应急响应机制等策略进行网络攻击阻断, 通过以上策略加强VPN的安全性。通过实施这些策略, 可以有效提升VPN的防护能力, 确保数据传输的安全性和网络环境的稳定性。

关键词 VPN防护; 网络安全; 监测技术; 阻断机制

中图分类号: TP393.08

文献标志码: A

文章编号: 2097-3365(2024)12-0016-03

随着信息技术的高速发展, 虚拟私人网络(VPN)已成为企业远程办公、数据传输和资源共享的重要工具。然而, VPN在提供便利性的同时, 也面临着日益严峻的安全威胁。网络攻击者利用VPN的漏洞和弱点, 进行非法入侵、数据窃取和破坏活动, 给企业和个人带来了巨大的损失。因此, 构建一套完善的VPN防护体系, 实现预防、监测和阻断的多重防护, 已成为VPN网络防守的重要课题。

1 VPN技术在IT中应用的重要性

VPN虚拟私人网络(Virtual Private Network, 简称VPN)是一种常用于连接中大型企业或团体内部网络的技术, 以便远程用户和分支机构访问公司数据中心的内部网络资源。

VPN技术经过数十年的发展, 已在全世界范围内得到广泛应用。VPN通过加密和隧道技术, 实现数据的安全传输, 保障用户在互联网上的隐私和信息安全。VPN技术在IT中应用的重要性主要体现在以下几个方面^[1]:

1. 远程访问: 企业员工在外地或家中通过VPN接入企业内网, 实现远程办公。
2. 数据传输: 企业间通过VPN专线进行数据交换, 确保数据安全。
3. 网络安全: 用户通过VPN加密上网, 防止数据被窃取和篡改。
4. 隐私保护: 使用VPN可以隐藏用户的真实IP地址, 保护用户的上网行为不被追踪, 从而保护个人隐私。
5. 跨地域连接: 对于国际化公司, VPN可以实现不同地区分支机构之间的安全互联, 保证数据传输的

一致性和安全性。

6. 网络资源扩展: 通过VPN, 企业可以将分布在不同地点的网络连接起来, 形成一个扩展的、安全的内部网络。

7. 成本效益: 相比于租用专线, VPN的部署和维护成本相对较低, 尤其适用于中小型企业。

8. 访问控制: VPN可以帮助企业实现精细化的访问控制, 确保只有授权用户可以访问特定的网络资源。

9. 业务连续性: 在自然灾害或其他紧急情况下, VPN可以确保关键业务系统的连续运作。

2 VPN遭遇多样化的网络攻击

在实际的网络攻击中, 通过VPN的攻击通常难以发现, 潜在风险非常大。针对VPN的攻击, 一部分是通过钓鱼等手段获取VPN的账号或相关终端权限来攻击, 另一部分是通过VPN的漏洞来进行攻击, 结合目前大部分VPN相关流量的加密特点, 这类型的攻击往往比较难发现。对于很多远程业务访问来说, VPN是必须使用的技术, 因此我们在攻防演练中采用了白名单、账号二次认证、针对VPN流量单独解密检测和自动阻断等多重手段进行防护, 尽最大可能避免遭受通过VPN的攻击。

尽管VPN具有诸多优点, 但其安全性并非无懈可击, 网络攻击者针对VPN的攻击表现出多样化, 主要包括以下几种^[2]:

1. 中间人攻击: 攻击者通过拦截和篡改VPN通信数据, 窃取敏感信息或进行恶意操作。
2. 非法访问: 攻击者通过VPN隧道, 非法访问企

业内网资源。

3. 密码破解：利用暴力破解或字典攻击等手段，尝试破解 VPN 用户的登录密码。

4. 漏洞挖掘：利用 VPN 软件或协议中的已知漏洞，进行非法入侵和数据窃取。

5. 恶意软件感染：通过 VPN 传播恶意软件，如病毒、木马等，对用户设备进行破坏或窃取数据。

6. 数据窃取：攻击者通过入侵 VPN，窃取企业或个人用户的敏感数据。

7. DDOS 攻击：对 VPN 服务器进行分布式拒绝服务攻击，导致服务中断或瘫痪。

8. DNS 泄露：由于配置不当或客户端软件漏洞，导致用户的 DNS 请求不通过 VPN 隧道发送，泄露查询信息。

9. 端口转发攻击：攻击者利用 VPN 客户端或服务器的端口转发功能，将未加密的数据通过 VPN 隧道转发。

10. IP 泄露：由于 VPN 连接不稳定或客户端配置问题，导致用户的真实 IP 地址泄露。

11. 会话劫持：攻击者尝试劫持已经建立的 VPN 会话，接管会话或获取会话数据。

12. 证书伪造或盗用：攻击者伪造或盗用数字证书，以欺骗 VPN 客户端建立不安全的连接。

13. 端口扫描和指纹识别：攻击者通过扫描开放的 VPN 端口和识别服务指纹，寻找潜在的攻击入口。

3 VPN 防护策略

为了有效应对 VPN 面临的安全威胁，需要构建一套包括预防、监测和阻断在内的多举措防护体系。

3.1 预防措施

1. VPN 登录机制：（1）采用多因素认证机制，结合密码、生物识别、动态令牌等多种认证方式，提高 VPN 用户的身份认证强度。（2）VPN 登录的账号密码限制，要求必须使用复杂密码，并必须定期更新密码，以确保账号密码的安全性和复杂性，防止被冒用^[3]。（3）VPN 登录的二次认证，要求登录 VPN 的时候必须通过二次认证，比如通过短信进行二次认证，否则无法登录和操作。

2. VPN 使用的白名单机制：（1）使用 VPN 必须通过网络管理员的许可和认证，否则无法使用 VPN 资源。

（2）根据业务实际需求，给业务相关的人员分配 VPN 账号资源，建立了白名单机制，并根据业务实际情况动态调整该名单。（3）对于因业务需求临时使用 VPN 的情况，通过申请机制，报备给安全管理员，通过开通临时权限来使用 VPN，使用结束后，由管理员收回相关权限。

3. VPN 加密算法升级：（1）采用先进的加密算法

和协议，如 IPsec 等协议，确保 VPN 通信数据在传输过程中的安全性和完整性。（2）对 VPN 协议进行定期更新和升级，以应对新出现的网络安全威胁。

4. VPN 漏洞管理和补丁更新：（1）建立完善的漏洞管理机制，定期对 VPN 软件和协议进行漏洞扫描和评估，如果发现存在漏洞，立即进行修复和更新，防止攻击者利用漏洞进行非法入侵。（2）加强 VPN 软件的安全性：提高 VPN 软件的编码质量，遵守 SDL 编码机制，减少软件自身漏洞。

5. VPN 访问控制策略：制定严格的访问控制策略，限制 VPN 用户的访问权限和范围。根据用户的角色和职责，分配不同的访问权限，防止敏感数据泄露和非法操作。

6. VPN 客户端安全：确保客户端所有软件都是最新版本，并且在客户端上实施安全策略，具体措施例如自动锁屏、防病毒保护。

7. VPN 网络配置和渗透测试：（1）根据攻防演练实战的要求，定期针对 VPN 进行渗透测试，评估 VPN 系统的安全性。（2）根据网络安全专家的评估意见，确保网络设备配置正确，例如关闭不必要的端口和服务。（3）使用 VPN 分割隧道来限制对内部网络的访问。

3.2 VPN 监测措施

1. 针对 VPN 相关流量的监测：（1）通过流量检测设备保留 VPN 相关日志，并在每日监测过程中排查是否有异常，重点关注 VPN 虚拟池流量和访问日志，及时发现异常的 VPN 相关流量或其他相关情况。此外，遇到相关攻击，可以快速通过日志进行回溯和分析。（2）由于 VPN 流量加密，使用了可以解密的流量检测手段，通过证书解密的方式在流量检测设备上对 VPN 相关流量进行解密和实时检测。（3）边界阻断措施，我们在监测的同时使用了边界阻断设备，可以自动化地将流量监测设备上发现的攻击 IP 同步到边界阻断设备上进行阻断，以便在发现攻击的第一时间进行阻断，减少相关损失。

2. VPN 登录日志审计：（1）开启 VPN 的登录日志记录，记录所有用户登录 VPN 的相关日志，包括登录源地址 IP、登录后用户设备的虚拟 IP、使用时间、在线时长等信息。（2）在检测中发现利用 VPN 的相关攻击事件之后，通过登录日志来分析和溯源，进一步确认具体的攻击时间、时长等，辅助判断受威胁的资产等。

3. 入侵检测系统：部署入侵检测系统，对 VPN 网络进行实时监控和检测。入侵检测系统能够识别并响应网络中的恶意行为，如未授权访问、数据篡改等，及时发出警报并采取相应的防护措施。

4. 端点检测与响应: 使用终端杀毒系统来监控端点设备, 及时监测非法流量, 并进行响应恶意活动, 避免造成病毒侵入。

5. 网络安全监控: (1) 实时监测网络流量, 寻找流量模式的异常变化, 这表明 VPN 可能正在受到攻击。

(2) 实时监测 VPN 服务器的性能, 以便及时发现由攻击引起的性能下降。

6. 证书管理和用户行为分析: (1) 定期检查和更新 VPN 使用的数字证书, 确保它们的有效性和安全性。定期监测证书颁发机构 CA 的安全性。(2) 分析用户行为, 及时识别可能出现的内部威胁或账户被接管的情况。

3.3 VPN 阻断措施

1. 防火墙和入侵防护系统: (1) 在 VPN 网络边界部署防火墙^[4], 对进出 VPN 网络的数据包进行过滤和检测, 防火墙能够阻止未经授权的访问和恶意流量进入 VPN 网络。(2) 在 VPN 网络边界部署入侵防护系统则能够实时检测和防护网络攻击行为, 保护 VPN 网络免受攻击。

2. 访问控制列表和速率及阈值设置: (1) 在网络设备上实施访问控制规则, 限制对 VPN 服务器的访问, 只允许来自自己 IP 地址的连接。(2) 对 VPN 连接尝试实施速率限制, 防止暴力破解攻击。(3) 设置连接阈值, 超过阈值则自动阻断来源 IP。

3. VPN 服务降级和 IP 地址封锁: (1) 在检测到攻击时, 临时降级 VPN 服务, 例如限制连接数或带宽。(2) 封锁来自自己已知恶意 IP 地址或 IP 地址范围的连接。

4. 物理和逻辑隔离: 将 VPN 服务器与内部网络进行物理和逻辑隔离, 以减少潜在的攻击面。

5. 应急响应机制: (1) 建立完善的应急响应机制, 制定详细的应急预案和处置流程。一旦发生安全事件, 立即启动应急响应机制, 迅速定位问题、评估影响并采取相应的处置措施, 最大限度地减少损失。(2) 隔离受影响的系统, 将受攻击的 VPN 服务器或客户端从网络中隔离, 以防止攻击扩散到其他系统。(3) 通知相关方人员, 并告知高层管理人员、法务部门、IT 部门和其他相关方关于安全事件的详细信息^[5]。(4) 用户培训和教育, 对用户进行安全意识培训, 强调 VPN 安全使用的重要性, 以及如何识别潜在的安全威胁。

4 防守实现的效果及亮点

4.1 防守实现的效果

通过实施上述多举措的 VPN 防护体系, 可以显著提升 VPN 网络的安全性和稳定性, 具体效果如下:

1. 降低安全风险: 通过强化身份认证、加密技术

升级、漏洞管理和补丁更新等措施, 降低 VPN 网络面临的安全风险。

2. 提高响应速度: 通过流量监测、日志审计和入侵检测等措施, 及时发现并阻断潜在的攻击行为, 提高响应速度和处置效率。

3. 保障业务连续性: 通过应急响应机制和防火墙、入侵防护系统等设备的部署, 确保 VPN 网络在遭受攻击时能够迅速恢复业务运行, 保障业务连续性。

4.2 防守实现的亮点

1. 多层次防护: 构建了一套包括预防、监测和阻断在内的多层次防护体系, 实现了对 VPN 网络全方位、立体化的安全防护。通过不同层次的防护措施相互配合、相互补充, 形成了强大的安全防护网。

2. 智能化监测: 采用先进的流量监测和日志审计技术, 实现了对 VPN 通信流量的智能化监测和分析。通过人工智能、大数据分析等技术手段, 能够自动识别异常流量和可疑行为, 提高监测的准确性和效率。

3. 灵活可扩展: 构建的 VPN 防护体系具有灵活可扩展的特点。随着网络环境和安全威胁的不断变化, 可以根据实际需求对防护体系进行调整和优化, 以适应新的安全挑战。

5 结束语

面对日益严峻的网络安全形势, 构建多举措的 VPN 防护体系具有重要意义。通过构建一套包括预防、监测和阻断在内的多举措防护体系, 可以显著提升 VPN 网络的安全性和稳定性, 保障企业和个人用户的网络安全。VPN 作为远程办公和数据传输的重要工具, 其安全性直接关系到企业及个人的本身利益, 随着 IT 技术的不断发展和安全威胁的不断变化, 我们需要持续关注 VPN 安全领域的新动态和新挑战, 不断完善和优化防护体系, 为网络安全保驾护航。

参考文献:

[1] 邓诗钊. 计算机网络信息安全中虚拟专用网络技术的应用[J]. 信息系统工程, 2023(08):84-87.

[2] 房建利. 虚拟专用网络技术在安全领域的应用[J]. 数字技术与应用, 2023(08):231-233.

[3] 邹佳彬. 虚拟专用网络技术在计算机网络信息安全中的应用[J]. 中国高新科技, 2022(18):11-12.

[4] 李威. 计算机网络信息安全中虚拟专用网络技术的应用[J]. 科技经济市场, 2023(07):19-21.

[5] 孔勇, 范佳雪. 信息时代下美国关键基础设施加强信息系统保护:《信息时代的关键基础设施保护》解读[J]. 中国信息化, 2022(07):48-52.