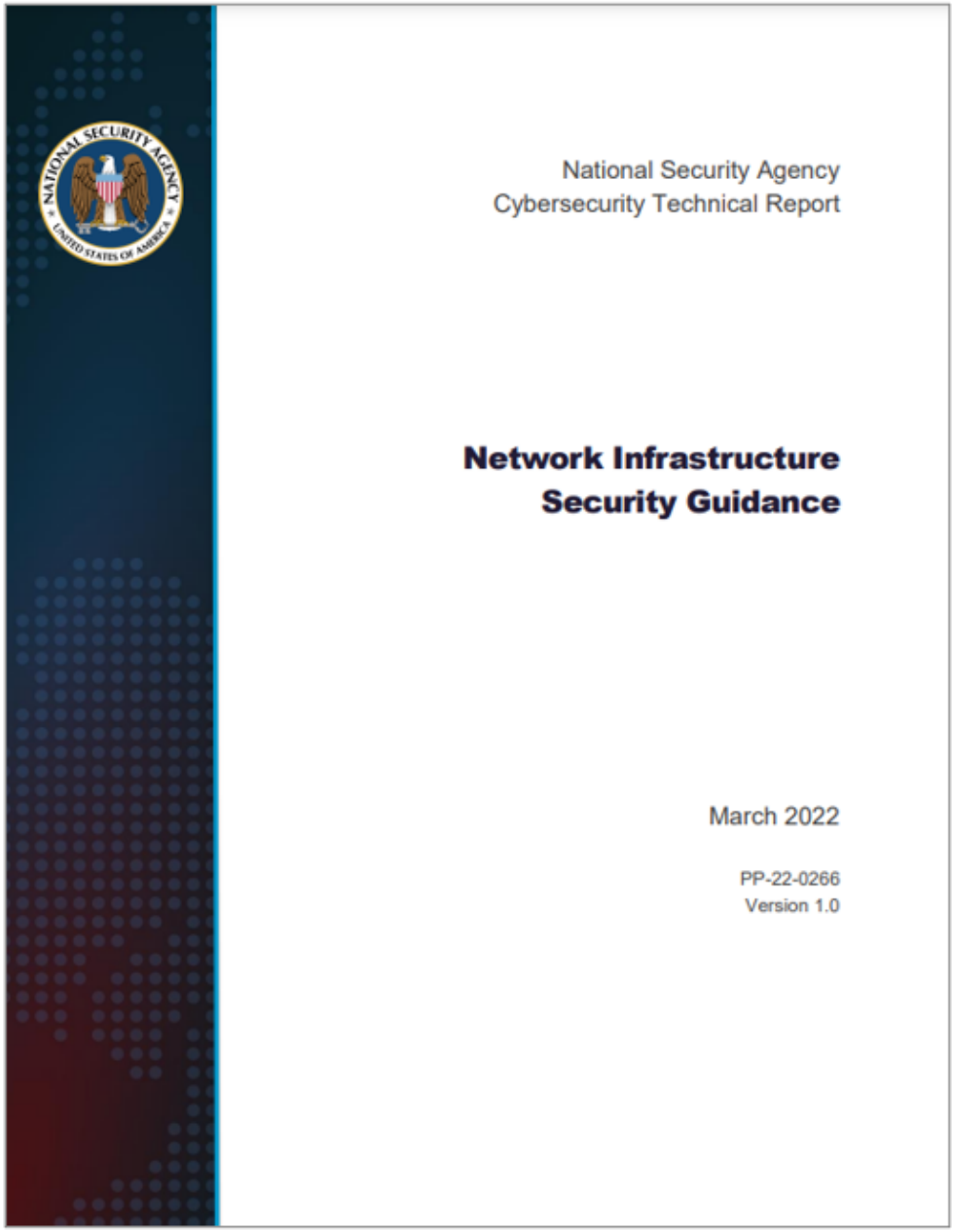
美国家安全局《网络基础设施安全指南》概述

通信邮政 (https://www.secrss.com/articles?tag=通信邮政) · 学术plus (https://www.secrss.com/articles?author=学术plus) · 2022-03-09

该指南向所有组织提供了最新的保护IT网络基础设施应对网络攻击的建议。

2022年3月1日，美国国家安全局（National Security Agency，NSA）发布网络安全技术报告：**网络基础设施安全指南（Network Infrastructure Security Guidance）**，该指南向所有组织提供了最新的保护IT网络基础设施应对网络攻击的建议。安全指南建议涵盖**网络设计、设备密码和密码管理、远程登录、安全更新、密钥交换算法、以及NTP、SSH、HTTP、SNMP协议**等重要的协议。



NSA发布未来基础设施安全指南

编译：学术plus高级观察员 张涛

本文主要内容及关键词

1.网络架构和设计：强调边界与控制①安装边界和内部防护设备②对网络系统进行聚类③移除后门连接④使用严格的边界访问控制⑤实现网络访问控制方案⑥限制和加密VPN

2.安全维护：软硬件结合①验证软件和配置完整性②维护适当的文件系统和启动管理③维持最新的软件和操作系统④使用厂商支持的硬件

3.认证、授权和审计：中心化管理①实现中心化的服务器②配置认证③配置授权④配置审计⑤应用最小权限原则⑥限制认证尝试次数

4.管理员账号和密码：①使用唯一的用户名和账号设置②修改默认密码③移除非必要的账号④使用个人账户⑤使用安全算法保存密码⑥创建强密码⑦使用唯一的密码⑧必要的时候修改密码

5.远程日志和监控：中心化+同步①启用日志②建立中心化的远程登录日志服务器③获取必要的日志信息④同步时钟

6.远程管理和网络服务：加强协议，严格禁用①禁用明文管理服务②确保充足的加密强度③使用安全协议④限制对服务的访问⑤设置可接受的超时周期⑥启用TCP Keep-alive⑦禁用外部连接⑧移除SNMP read-write community字符串⑨禁用非必要的网络服务⑩禁用特定接口上的发现协议⑪网络服务配置

7.路由：①禁用IP源路由②启用uRPF③用路由认证

8.接口端口

内容主要整理自外文网站相关资料

仅供学习参考，欢迎交流指正！

文章观点不代表本机构立场

*****

1.网络架构设计

安全的网络设计要实现多层防护以应对威胁和保护网络中的资源。在安全网络设计中，网络边界和内部设备都需要遵循安全最佳实践和零信任原则。

1.1 安装边界和内部防护设备

NSA建议根据安全最佳实践在网络边界配置和安装安全设备：

- 安装边界路由器来建立与外部网络的连接，比如网络服务提供商（ISP）
- 实现多层下一代防火墙来限制入流量、出流量，并检查所有异构网络区域的内部活动。每层应该使用不同厂商的产品来保护内部网络
- 将公开可访问的系统和外部代理放置在一个或多个DMZ（非军事区）子网中的防火墙层，在DMZ子网中，访问可以由外部设备、DMZ设备和内部系统控制
- 实现网络监控解决方案来记录来追踪入和出流量，比如网络入侵检测系统、流量检查器或全包抓取设备
- 部署多个远程日志服务器来记录与设备相关的活动
- 在核心区域内实现冗余设备来确保可用性，可以通过负载均衡来增加网络吞吐量和减少延迟

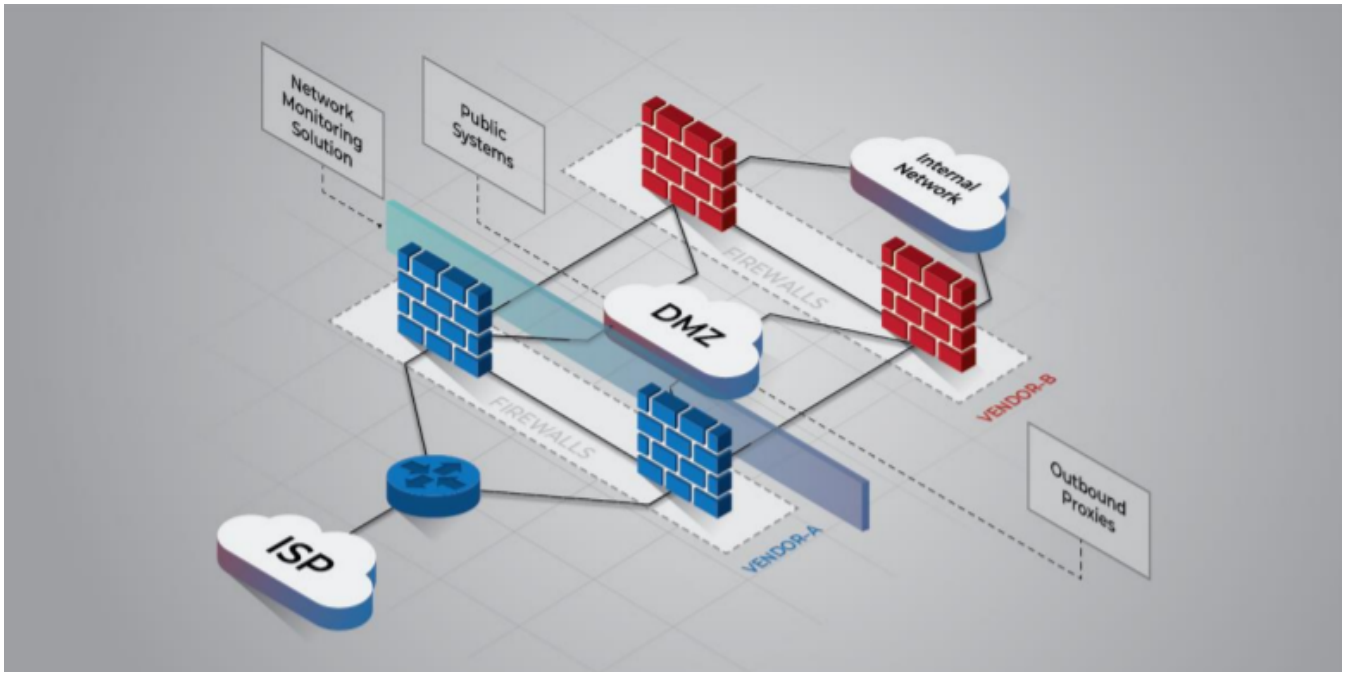


图 部署了防火墙和DMZ的网络边界

1.2 对网络系统进行聚类

网络中类似的系统应该进行逻辑聚类以更好地保护系统。

NSA建议将网络中相似的系统隔离为不同的子网或VLAN（虚拟本地区域网络）或通过防火墙或路由器物理隔离为不同的子网。工作站、服务器、打印机、通信系统等应该彼此隔离。

1.3 移除后门连接

后门网络连接是位于不同网络区域的2个或多个设备的连接，一般拥有不同类型的数据和安全要求。

NSA建议移除所有后门网络连接，尤其是在用多个网络接口连接设备时间要非常注意。对设备的所有网络接口进行验证，确保具有相同的安全等级，中继设备要能够提供不同网络区域的逻辑和物理隔离。

1.4 使用严格的边界访问控制

NSA建议认真考虑允许哪些连接，并创建带有**白名单的规则集。**使用该方法只需要一条规则就可以拒绝多种类型的连接，而不需要对每个拦截的连接创建一条规则。如果需要动态应用额外的边界规则来预防漏洞利用，NSA建议使用入侵防御系统（IPS）。

NSA还建议对这些规则集进行记录日志，至少应该包含所有拒绝或丢弃的网络流量，以及对关键设备成功或失败的管理员访问。

1.5 实现网络访问控制方案

NSA建议实现网络访问控制解决方案来识别和认证连接到网络中的唯一的设备。可以在交换机上实现端口安全机制来检测非授权的设备对网络的连接。

1.6 限制和加密VPN

NSA建议限制VPN网关对UDP 500、4500端口、EP和其他端口的访问。如果可以的话，限制接收到已知的VPN节点IP地址的流量。

2.安全维护

升级硬件和软件来确保效率和安全

2.1 验证软件和配置完整性

NSA建议验证安装和设备上运行的操作系统文件的完整性，并将文件的哈希结果与厂商发布的哈希结果进行比较。在升级操作系统文件时，也需要进行完整性验证，以确保文件没有被修改。

2.2 维护适当的文件系统和启动管理

许多网络设备都有至少2种不同的配置，一个保存在硬盘上，一个运行在内存中。NSA鉴于检查设备上未使用的或非必要的文件并移除，比如老版的操作系统文件或过时的备份配置文件。

2.3 维持最新的软件和操作系统

维持最新版本的操作系统和稳定的软件版本可以应对已经识别和修复的关键漏洞。NSA建议在所有的设备上升级操作系统和软件到最新的稳定版本。许多网络基础设施设备并不支持自动更新，因此需要手动从厂商处获得最新的软件并安装。

2.4 使用厂商支持的硬件

NSA建议在厂商发布不再更新或提供技术支持的产品清单后，建立使用新设备来替换或升级受影响设备的计划。过期的或不再支持的设备应该立刻进行升级或替换来确保网络服务和安全支持的可用性。

3.认证授权审计

中心化的认证、授权和审计（AAA）服务器可以提供一种对设备的管理权限访问的管理。对这些服务器进行适当的配置可以提供一种管理和监控访问的授权源，改善访问控制的一致性，减少配置维护和管理成本。

3.1 实现中心化的服务器

NSA建议在网络中至少部署2个AAA服务器来确保可用性，以及帮助检测和预防恶意活动。如果一个服务器由于定期维护或其他原因不可用，其余服务器可以继续提供中心化的AAA服务。

3.2 配置认证

认证是对个人或实体身份的验证。所有的设备都应该配置为使用中心化的服务器来进行AAA服务，本地管理员账户作为一种备份方法只有所有的中心化服务器不可用时才使用。NSA建议对登录和启用访问配置中心化的认证。

3.3 配置授权

授权会验证个人或身体是否有权限访问特定的资源或执行特定的操作。NSA建议限制合法管理员被授权执行的操作，以预防恶意用户使用被入侵的账户来执行非授权的操作。

3.4 配置审计

审计记录着访问的所有相关的资源和执行的操作，以供管理员进行审计。NSA建议系统配置变化进行中心化记录，定期检查这些记录以检测可能的恶意活动。

3.5 应用最小权限原则

NSA建议所有的账户采用最小权限原则，并要求管理员在提升到更高权限来执行一些操作时需要额外输入凭证信息。并且对权限等级进行定期检查。

3.6 限制认证尝试次数

NSA建议将错误远程管理（认证）尝试的次数限制为3次及以下。此外，NSA还建议延长登陆尝试的间隔为至少1秒，以减缓暴力破解的次数。

4.管理员信息

管理员账号和密码

4.1 使用唯一的用户名和账号设置

大多数设备的默认管理员账户和凭证都是公开的，而管理员账户具有设备的管理权限。NSA建议移除设备的默认配置，并对每个设备重新配置一个唯一的、安全的管理员账户。

4.2 修改默认密码

大多数设备在管理员进行初始化配置前都有默认密码，甚至没有密码。而这些默认密码一般都是公开的。NSA建议移除所有的默认密码，并分配一个唯一的、复杂的、安全的密码。此外，在新设备加入网络时，修改默认用户和特权等级密码。

4.3 移除非必要的账号

NSA建议将授权登录设备的账户限制为必要的范围，其他账户建议移除。管理员离开组织或角色发生变化后，相关的账户应当被禁用或移除。

4.4 使用个人账户

NSA建议禁用所有共享和组管理员账户，对每个管理员使用唯一的账户来提供对配置变化的访问，以确保对每个设备的可审计性。如果组账户是必要的，NSA建议监控这些账号来检测可能的可疑活动。

4.5 使用安全算法保存密码

NSA建议设备上保存的所有密码都使用最安全的算法进行加密，不要明文保存。建议使用单向哈希算法，如果单向哈希算法不可用，应当使用强唯一密钥来加密密码。

4.6 创建强密码

NSA建议对不同级别的访问分配唯一的、复杂的密码，包括用户和特权级别访问。在路由认证、时间同步、VPN通道、SNMP和其他配置中需要保存密码的场景中也应该使用唯一的、复杂的密码。

4.7 使用唯一的密码

NSA建议对每个设备上的每个账户和特权级别分配唯一的、复杂的、安全的密码。NSA还建议对不同账户、不同级别份额、不同设备之间的密码重用进行检查。

4.8 必要的时候修改密码

NSA建议在密码或密码哈希被入侵后立刻修改密码，并安全保存。

5.远程日志

远程日志和监控

5.1 启用日志

启用日志后，网络设备上就会生成日志消息。可以将设备配置为立刻发送日志消息到本地日志缓存或中心化的日志服务器。NSA建议启用系统日志、设置本地日志缓存为16MB，并定期对收到的日志消息进行验证。

5.2 建立中心化的远程登录日志服务器

NSA建议使用至少2个远程、中心化的日志服务器来确保设备日志消息的监控、冗余和可用性。尽可能地确保传输的日志消息是加密的，以预防敏感信息的非授权泄露。

5.3 获取必要的日志信息

NSA建议设置将每个设备的缓存日志级别设置为informational级别以收集所有必要的信息。如果网络跨域多个时区，NSA建议使用UTC时间，所有的日志消息都应含有精确到毫秒的时间戳，以及时区和日期信息。

5.4 同步时钟

NSA建议每个设备和远程日志服务器使用至少2个可信的、可靠的时间服务器来确保信息的准确性和可用性。内部时间服务器应当作为所有设备的主要源，随后与授权的外部源进行同步。NSA建议在所有设备上启用NTP认证来预防时钟篡改，在设备和特定时间源之间配置强、唯一的NTP认证密钥。

6.远程管理

远程管理和网络服务

6.1 禁用明文管理服务

NSA建议使用加密的服务来保护网络通信，禁用所有明文管理服务，如Telnet、HTTP、FTP、SNMP。确保所有的敏感信息无法被恶意敌手通过网络流量抓包来获取。

6.2 确保充足的加密强度

NSA建议非对称密钥生成使用3072位及以上密钥，椭圆曲线加密密钥使用384位，对称加密密钥使用256位。部分系统可能不支持3072位，可以使用4096位来替换。

6.3 使用安全协议

NSA建议确保管理服务使用最新的协议版本，并启用了适当的安全设置。SSH v2是远程访问设备的优选方法。加密的HTTP服务器应当配置为只接受TLS v1.2及更高版本。

6.4 限制对服务的访问

NSA建议配置访问控制列表（ACL）使得只有管理员系统才能连接到设备来进行远程管理。

6.5 设置可接受的超时周期

NSA建议对所有远程设备的管理员连接设置会话超时时间为5分钟或更少。不要将超时周期设置为0，因为大多数设备在将超时周期设置为0后会禁用超时功能。

6.6 启用TCP Keep-alive

NSA建议对所有TCP连接的入和出流量启用TCPKeep-alive设置。

6.7 禁用外部连接

NSA建议禁用出流量来限制攻击者在网络中的移动。

6.8 移除SNMP read-write community字符串

NSA建议移除所有的SNMP read-write community字符串，将加密和认证升级到SNMP v3。

6.9 禁用非必要的网络服务

NSA建议禁用每个设备上非必要的服务。如果该服务是必须的，并且支持密码和ACL，则创建一个强密码，并应用ACL规则来只允许必要的系统连接到该服务。

6.10 禁用特定接口上的发现协议

NSA建议禁用能够使用这些服务的所有设备上CDP和LLDP。

6.11 网络服务配置

NSA建议对远程网络管理服务进行适当的配置，包括SSH、HTTP、SNMP。

7.路由

7.1 禁用IP源路由

NSA建议在所有设备上禁用IP源路由，因为该功能对正常的网络操作来说是非必要的。

7.2 启用uRPF

NSA建议在边界路由器的外部接口启用uRPF。

7.3 启用路由认证

NSA建议在所有接收来自网络中其他设备的路由更新的动态路由协议上启用路由认证。

8.接口端口

适当配置的接口端口可以预防敌手执行针对网络的漏洞利用。NSA建议：

- 禁用动态trunking
- 启用端口安全
- 禁用默认VLAN
- 禁用未使用的端口
- 禁用端口监控
- 禁用代理ARP

参考链接：

https://media.defense.gov/2022/Mar/01/2002947139/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDANCE_20220301.PDF