

NetScaler® 安全部署指南

Contents

NetScaler MPX™、VPX 和 SDX 安全性最佳实践	5
其他信息资源	5
部署指南	5
物理安全最佳实践	6
将 NetScaler 设备部署在安全位置	6
保护 NetScaler 前面板和控制台端口的访问安全	6
电源保护	6
加密密钥保护	6
NetScaler 安全最佳实践	6
执行 NetScaler 软件更新	6
保护托管 NetScaler VPX 的服务器操作系统	6
重置 NetScaler 远程管理 (LOM)	7
持久数据的维护和删除	7
配置指南	7
网络安全	8
关键网络安全注意事项	8
其他网络安全注意事项	9
保护 NetScaler® 上的直通流量	16
管理	24
系统和用户帐户	24
日志记录和监控	31
配置网络时间协议	31
配置 SNMP	32
配置日志记录到外部 NetScaler 日志主机	32
通过安全通道配置消息导出	34
LOM 配置	34

应用程序和服务	34
配置 NetScaler® 以删除或传递升级标头	34
配置 NetScaler 以丢弃无效的 HTTP 请求	35
配置针对 HTTP 拒绝服务攻击的保护	36
配置 NetScaler 以防御 TCP 欺骗攻击	36
配置 RFC 5961 合规性	37
配置 NetScaler 以接受特定的 HTTP 标头	37
配置 HTTP 标头的标头大小	38
在 NetScaler 中规范化 URL	38
增强型 TCP ISN 生成	39
配置关闭通知	39
保护管理 GUI、NITRO API 和 RPC 通信	39
DNSSEC 安全建议	40
KSK/ZSK 私钥使用 1024 位或更高位的 RSA	40
启用 DNSSEC 密钥过期 SNMP 警报	40
在 x.509 证书过期之前轮换 KSK/ZSK 私钥	40
保护 DNSSEC ADNS 服务器	40
旧版配置	42
配置 NetScaler® 以禁用密码重定向	42
在 NetScaler 上配置 SSL 重新协商设置	42
配置 NDcPP 合规性证书检查	43
NetScaler® 加密建议	43
管理 TLS 证书和密钥	43
为 FIPS 和 NDcPP 部署配置 TLS 密码套件	43
NetScaler -FIPS 建议	45
在基于 FIPS 的部署中配置 NetScaler SDX	45
将 HSM 密码存储在安全位置	46
其他功能	46

NetScaler® Web App Firewall 安全建议	46
以双臂模式部署 NetScaler	46
使用“默认拒绝”策略	47
NetScaler Web App Firewall – 构建多层安全	47
NetScaler® Gateway 安全建议	49
使用“默认拒绝”策略	49
在服务器之间使用 TLS1.2 通信	49
使用内部网应用程序	49
身份验证、授权和审计安全建议	50
NetScaler® Console 安全最佳实践	53
请勿将 NetScaler Console IP 地址和 NetScaler 代理 IP 地址暴露于互联网	53
系统用户的强密码	53
更改默认证书	54
禁用本地身份验证	54
fix	55

NetScaler MPX™、VPX 和 SDX 安全性最佳实践

NetScaler MPX 是一种应用交付控制器，可加速网站，提供 L4-L7 流量管理，提供集成的 NetScaler Web App Firewall，并分载服务器。NetScaler VPX 实例是一种虚拟设备，它具有 NetScaler MPX 的所有功能，在标准服务器上运行，并为包括 Citrix Virtual Apps and Desktops 在内的 Web 应用程序提供更高的可用性。NetScaler SDX 提供高级虚拟化，兼具 VPX 的所有灵活性和 MPX 的性能。通过使用 MPX、VPX 和 SDX，组织可以部署弹性或真正的多租户解决方案，该解决方案通过将大容量共享网络服务与处理器密集型、特定于应用程序的服务分离，从而优化您的 Web 应用程序交付基础架构。NetScaler 还提供与 Citrix OpenCloud Access 的无缝集成，可利用云的强大功能扩展数据中心。

为了在部署生命周期中保持安全性，我们建议您查看以下方面的注意事项：

- 物理安全
- 设备安全
- 网络安全
- 管理和维护

不同的部署可能需要不同的安全注意事项。本文档提供了一般安全指南，以帮助您根据特定的安全要求决定适当的安全部署。

其他信息资源

有关 NetScaler® 和 NetScaler Gateway 的其他安全信息，请参阅以下资源：

- [安全门户](#)
- [产品文档](#)

如需有关 NetScaler 配置的进一步帮助，您可以在以下位置提交支持请求：<https://www.citrix.com/support.html>

部署指南

部署 NetScaler 时，请考虑以下物理和设备安全最佳实践：

物理安全最佳实践

将 NetScaler 设备部署在安全位置

NetScaler 设备必须部署在安全位置，并具有足够的物理访问控制，以保护 NetScaler 免受未经授权的访问。至少，服务器机房的访问必须通过锁、电子读卡器或其他类似的物理方法进行控制。

其他措施可以包括使用电子监控系统（例如闭路电视）来持续监控房间的活动。如果发生未经授权的入侵，此系统的输出必须通知安全人员。如果安装了闭路电视，则录制的录像可用于审计目的。

保护 NetScaler 前面板和控制台端口的访问安全

NetScaler 或 VPX 托管服务器必须部署在可用合适的钥匙或其他物理方法锁定的机架或机笼中。锁定可防止访问 NetScaler 的物理端口，或者在 VPX 部署中，防止访问虚拟化主机控制台。

电源保护

NetScaler（或托管服务器）必须配备合适的不断电电源保护。如果发生断电，不断电电源可确保 NetScaler 的持续运行，或允许对物理或虚拟 NetScaler 进行受控关机。使用不断电电源还有助于防止电涌。

加密密钥保护

如果您的部署中需要对加密密钥进行额外保护，请考虑使用符合 FIPS 140-2 Level 2 标准的 NetScaler。FIPS 平台使用硬件安全模块来保护 NetScaler 中的关键加密密钥免受未经授权的访问。

NetScaler 安全最佳实践

执行 NetScaler 软件更新

我们建议客户在部署前确保其 NetScaler 已更新到最新的固件版本。如果远程执行，我们建议客户使用安全协议（例如 SFTP 或 HTTPS）来升级 NetScaler。

建议客户查阅与其 NetScaler 产品相关的安全公告。有关新的和更新的安全公告的信息，请参阅 NetScaler 安全公告网页 <https://support.citrix.com/knowledge-center/search#/> 并考虑注册以接收新的和更新的公告警报 <https://support.citrix.com/user/alerts>。

保护托管 NetScaler VPX 的服务器操作系统

NetScaler VPX 既可以在标准虚拟化服务器上作为虚拟设备运行，也可以在 NetScaler SDX 上作为虚拟设备运行。

除了应用正常的物理安全程序外，您还必须通过基于角色的访问控制和强大的密码管理来保护对虚拟化主机的访问。此外，服务器必须在操作系统有最新安全补丁可用时及时更新，并在服务器上部

署最新的防病毒软件（如果适用于虚拟化类型）。使用 NetScaler SDX 平台托管 NetScaler VPX 的客户必须确保他们使用的是其 NetScaler SDX 的最新固件版本。

重置 NetScaler 远程管理 (LOM)

我们建议，在配置 LOM 以用于生产部署之前，您对 LOM 执行出厂重置以恢复默认设置。

1. 在 NetScaler shell 提示符下，运行以下命令：

```
>ipmitool raw 0x30 0x41 0x1
```

注意：

运行此命令会将 LOM 重置为出厂默认设置并删除所有 SSL 证书。有关如何重新配置 LOM 端口的说明，请参阅 [NetScaler MPX 设备远程管理端口](#)。

2. 在 LOM GUI 中，导航到 **Configuration > SSL Certification**，然后添加证书和私钥。

此外，我们建议使用 LOM GUI 执行以下用户配置：

- 导航到 **Configuration > Users > Modify User**，并更改 **nsroot** 超级用户帐户的密码。
- 导航到 **Configuration > Users > Modify User**，并为用户创建策略或将现有策略绑定到用户。
- 导航到 **Configuration > IP Access Control > Add**，并配置 IP 访问控制以允许访问已知 IP 地址范围。
- 导航到 **Configuration > Users > Modify User**，并创建一个备用超级用户帐户并将策略绑定到此帐户。

有关 LOM 配置的更多详细信息，请参阅 [LOM 配置](#)。

持久数据的维护和删除

如果 NetScaler 重新部署到其他环境、退役或根据 RMA 返回，请确保从 NetScaler 中正确删除持久数据。

有关此过程的更多信息，请参阅 [将 ADC 设备发送给 Citrix 之前擦除数据](#)。

配置指南

配置 NetScaler 时，请考虑以下配置指南：

- [网络安全](#)
- [保护 NetScaler 上的直通流量](#)

网络安全

在生产环境中部署 NetScaler 时，我们建议进行以下关键配置更改：

- 请勿将 NetScaler 管理员界面 (NSIP) 暴露到互联网。
- 必须更换 NetScaler 默认 SSL 证书。
- 访问 GUI 时必须使用 HTTPS (HTTP over TLS)，并禁用默认的 HTTP 接口。

以下部分提供了有关这些关键注意事项的更多信息，以及建议进行的其他更改。

关键网络安全注意事项

请勿将 NSIP 和管理服务 IP 地址暴露到互联网：

我们建议 NetScaler 管理 IP (NSIP) 地址和 SDX 的管理服务 IP 地址不应暴露给公共互联网，并部署在适当的有状态数据包检测 (SPI) 防火墙之后。

更换 NetScaler 默认 TLS 证书：

在 NetScaler 的初始配置期间，会创建默认的 TLS 证书。这些证书不适用于生产部署，必须更换。

我们建议客户将 NetScaler 配置为使用来自信誉良好的证书颁发机构 (CA) 的证书，或来自您的企业证书颁发机构的适当证书。

当绑定到面向公众的虚拟服务器时，来自信誉良好的 CA 的有效 TLS 证书可简化面向互联网的 Web 应用程序的用户体验；用户 Web 浏览器在与 Web 服务器启动安全通信时无需用户交互。要将默认 NetScaler 证书替换为受信任的 CA 证书，请参阅知识中心文章 CTX122521：[“如何将 NetScaler 设备默认证书替换为与设备主机名匹配的受信任 CA 证书。”](#)

或者，可以创建和使用自定义 TLS 证书和私钥。虽然此操作可以提供同等水平的传输层安全性，但它要求将 TLS 证书分发给用户，并在启动与 Web 服务器的连接时需要用户交互。有关如何创建自定义证书的更多信息，请参阅知识中心文章 CTX121617：[“如何在 NetScaler 设备上创建和安装自签名证书。”](#)

有关 TLS 证书管理和配置的更多信息，请参阅本指南的“NetScaler TLS 建议”部分。

禁用对管理员界面的 HTTP 访问：

为保护 NetScaler 管理界面和 GUI 的流量，必须将 NetScaler 配置为使用 HTTPS。请执行以下步骤：

- 创建 2048 位或更大的 RSA 私钥和公钥对，并使用这些密钥通过 HTTPS 和 SSH 访问 NetScaler IP 地址，替换出厂提供的 512 位 RSA 私钥和公钥对。
- 将 NetScaler 配置为仅使用强密码套件，并将 NetScaler 上的“DEFAULT”密码套件集更改为强密码套件。我们建议您使用 NIST 特别出版物 800-52（修订版 1）第 3.3 节中批准的 TLS 密码套件列表。该文档可在 NIST 网站上找到，地址为：https://www.nist.gov/publications/guidelines-selection-configuration-and-use-transport-layer-security-tls-implementations?pub_id=915295
- 将 NetScaler 配置为使用 SSH 公钥身份验证来访问管理员界面。请勿使用 NetScaler 默认密钥。创建并使用您自己的 2048 位 RSA 私钥和公钥对。有关详细信息，请参阅知识中心文章 CTX109011：[如何使用公钥身份验证保护对 NetScaler 设备的 SSH 访问](#) 和 NetScaler 产品文档：[本地系统用户的 SSH 密钥身份验证](#)
- 将 NetScaler 配置为使用这些新证书后，可以使用以下命令禁用对 GUI 管理界面的 HTTP 访问：

```
set ns ip <NSIP> -gui SECUREONLY
```

其他网络安全注意事项

限制不信任管理 SDX 的 VPX 管理员的 VPX shell 访问：

在需要由不同于管理服务的人员管理 VPX 的情况下，管理服务管理员必须创建一个在 VPX 上具有有限 shell 访问权限的 VPX 管理员用户，并且只向 VPX 管理员提供受限的管理员用户帐户。

某些操作可能需要 shell 访问（例如管理 SSL 证书）。但是，只有受信任管理 SVM 的个人才能获得 VPX 实例 shell 的访问权限。本节后面列出的 RBAC 级别命令可以分配给这些帐户。这些建议适用于所有 SVM-IP/VPX-NSIP (L2/L3) 管理工作流，并且必须遵循以实现安全访问审计目的。

可以使用以下步骤从 VPX 管理员中删除 shell 访问权限。

保护现有 VPX 实例：

1. 以 `nsroot` 或超级用户身份登录 VPX CLI。

我们建议不要使用 `nsroot` 帐户，而是创建一个超级用户帐户。使用 `nsroot` 帐户时，请确保密码强度高，包含特殊字符。有关强密码的详细信息，请参阅[管理和安全](#)。

- 在 NetScaler SDX 上的 VPX 实例中创建用户和 RBAC 策略。
- 将该用户绑定到策略。

```

> add system user userabc

Enter password:

Confirm password:

Done

> bind system user userabc superuser 2

Done

> add system cmdpolicy shell deny (shell)

Done

> bind system user userabc shell 1

Done

```

注意：

在此示例中，创建系统 `cmdpolicy`（例如：`cmdpolicy` 名称：`shell`）以拒绝 shell 访问。此策略以高优先级绑定到用户 `userabc`。默认超级用户 `cmdpolicy` 也以较低优先级绑定到系统用户。通过此配置，新的系统用户具有超级用户 RBAC 策略，但 shell 访问被拒绝。

2. 以新系统用户身份登录并执行以下操作：

- 验证当前用户已应用 RBAC 策略。
- 运行用户被授权的任何命令。（例如，`show system cmdpolicy`）
- 运行 `shell` 命令以验证 shell 访问是否受限。

登录为：`userabc`

来自服务器的预认证横幅消息：

```

|
#####
#####

```

```
> ##  
  
| #  
  
> #  
  
| #      WARNING: Access to this system is for authorized users only  
  
> #  
  
| #      Disconnect IMMEDIATELY if you are not an authorized user!  
  
> #  
  
| #  
  
> #  
  
|  
#####  
#####  
  
> ##  
  
|  
  
End of banner message from server  
  
Keyboard-interactive authentication prompts from server:  
  
| Password:  
  
End of keyboard-interactive prompts from server  
  
Last login: Thu May 13 04:11:15 2021 from 10.10.1.1  
  
Done
```

```
> whoami  
  
UserName:  userabc      LoggedIn:  "Thu May 13 04:18:50 2021"
```

```
Done
```

3. 在该 VPX 的控制台中，以该用户身份登录并确保该用户不允许 shell 访问：

```
> shell
```

```
ERROR: Not authorized to execute this command [shell]
```

4. 以普通管理员用户 (`nsroot`) 身份登录并确保允许 shell 访问：

```
> shell
```

```
Copyright (c) 1992-2013 The FreeBSD Project.
```

```
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993,  
1994
```

```
The Regents of the University of California. All rights reserved.
```

```
root@Zela-40G-10#
```

保护新的 VPX 实例：

1. 从管理服务 GUI 创建新的 VPX 实例时，创建 INSTANCE ADMIN 用户，并清除 **Shell/SFTP/SCP 访问** 复选框。禁用 shell 访问后，`svm_access_policy`（操作 DENY）将显式绑定到指定的实例管理员用户。
2. 将此用户信息提供给 VPX 管理员。SDX 管理员必须保留此 `nsroot` 管理员密码，并且不得与 VPX 管理员共享。

注意：

- 要更改 `nsroot` 密码，请登录到管理服务，选择实例，然后更改密码。切勿通过 VPX CLI 更改 `nsroot` 密码。
- 有关 RBAC 用户的详细信息，请参阅 [用户、用户组和命令策略](#)。
- 要从 SVM 修改 NetScaler 的密码，请参阅 [修改 NetScaler 实例](#)。
- 要通过实例管理预配 NetScaler，请参阅 [添加 NetScaler 实例](#)。

禁用 SSH 端口转发：

NetScaler 不需要 SSH 端口转发。如果您不想使用此功能，建议您按照以下步骤禁用它：

1. 编辑 `/etc/sshd_config` 文件，添加以下行：

```
AllowTcpForwarding no
```

2. 保存文件并将其复制到 `/nsconfig` 目录，以确保在测试期间重新启动时更改仍然存在。
3. 使用以下命令重新启动 `sshd` 进程：

```
kill -HUP `cat /var/run/sshd.pid`
```

配置 NetScaler 高可用性：

在需要持续运行的部署中，NetScaler 可以部署在高可用性设置中。如果其中一个 NetScaler 停止运行或需要脱机升级，这种设置可提供持续运行。

有关如何配置高可用性设置的信息，请参阅 [配置高可用性](#)。

设置对等设备之间的安全通信：

如果您已将 NetScaler 配置为高可用性、群集或 GSLB 设置，请确保 NetScaler 设备之间的通信安全。

为了保护通信安全，建议您更改内部用户帐户或 RPC 节点密码，并启用 **Secure** 和 **-validateCert** 选项。RPC 节点是内部系统实体，用于系统间的配置和会话信息通信。`-validateCert` 选项允许对节点之间的 RPC 通信（例如配置同步或配置传播）进行服务器证书验证。

```
set ns rpcNode <IP> -secure ON -validateCert YES
```

仅当 `-secure` 参数设置为 `ON` 时，`-validateCert` 选项才有效。

为了验证服务器证书，必须配置 CA `/nsconfig/ssl/certs/ca.pem` 文件。因此，请使用对 `nsrpcs-127.0.0.1-3008` 服务服务器证书进行签名的对等 CA 证书配置 CA 文件 `/nsconfig/ssl/certs/ca.pem`。有关详细信息，请参阅 [更改 RPC 节点密码](#)。

当内部用户帐户被禁用时，NetScaler 功能还可以使用基于 SSH 密钥的身份验证进行内部通信。在这种情况下，密钥名称必须设置为“ns_comm_key”。有关详细信息，请参阅 [使用 SSH 密钥且无需密码访问 NetScaler 设备](#)。

更改默认密码：

为了增强安全性，建议您更改本地和云部署的管理员、内部用户帐户或 RPC 节点密码。建议经常更改密码。

- 管理员密码：请参阅 [更改管理员密码](#)。
- 内部用户帐户或 RPC 节点密码：请参阅 [更改 RPC 节点密码](#)。

注意

我们还建议您禁用内部用户帐户，转而使用基于密钥的身份验证。

配置网络安全域和 VLAN：

建议将流向 NetScaler 管理接口的网络流量与普通网络流量物理或逻辑分离。推荐的最佳实践是拥有三个 VLAN：

- 外部 Internet VLAN
- 管理 VLAN
- 内部服务器 VLAN

我们建议配置网络，使 LOM 端口成为管理 VLAN 的一部分。

在双臂模式下部署 NetScaler 时，请将特定端口专用于特定网络。如果需要 VLAN 标记并将两个网络绑定到一个端口，则必须确保这两个网络具有相同或相似的安全级别。

如果两个网络具有不同的安全级别，则不得使用 VLAN 标记。相反，请考虑为每个特定网络分配一个端口，并使用分布在 NetScaler 端口上的独立 VLAN。

考虑使用 NetScaler Web App Firewall： 获得高级版许可的 NetScaler 提供内置的 NetScaler Web App Firewall，它使用积极的安全模型，并自动学习正确的应用程序行为，以防止命令注入、SQL 注入和跨站点脚本等威胁。

使用 NetScaler Web App Firewall 时，用户无需更改代码，只需对配置进行少量更改，即可为 Web 应用程序添加额外的安全性。有关更多信息，请参阅 [NetScaler Web Application Firewall 简介](#)。

限制非管理应用程序访问： 运行以下命令以限制非管理应用程序访问 NetScaler 的能力。

```
set ns ip <NSIP> -restrictAccess enabled
```

保护群集部署：

为了保护群集部署，我们建议您启用安全心跳功能，该功能可提供针对网络攻击的保护。

注意：

安全心跳功能从 NetScaler 14.1 版本 12.x 及更高版本开始提供。

要启用安全心跳功能，请登录到群集 IP 地址并运行以下命令：

```
set cluster instance <clId> secureHeartbeats ENABLED
```

有关安全心跳功能的更多信息，请参阅 [配置安全心跳](#)。

为了保护通信安全，我们建议您更改内部用户帐户或 RPC 节点密码，并启用 **Secure** 和 **-validateCert** 选项。

```
set rpcnode <ip> -secure on -validateCert YES
```

注意： 可能需要其他配置。有关更多信息，请参阅 [产品文档](#) 中的 **群集** 主题。

在 L3 群集部署中，NetScaler 节点之间的报文通过未加密的 GRE 隧道交换，该隧道使用源节点和目标节点的 NSIP 地址进行路由。当交换通过互联网发生时，在没有 IPsec 隧道的情况下，NSIP 会暴露在互联网上，这是不推荐的，因为它不符合 NetScaler 的安全最佳实践。

我们建议客户建立自己的 IPsec 解决方案，以便通过 L3 功能使用集群。

如果未使用 IP 转发功能，请使用以下命令禁用 L3 模式：

```
disable ns mode L3
```

为全局服务器负载均衡 (GSLB) 使用安全的 MEP：要加密 NetScaler 之间用于 GSLB 的 MEP，请从 NSCLI 运行以下命令：

```
set rpcNode <GSLB Site IP> -secure yes
```

保护负载均衡持久性 Cookie：

除了 SSL/TLS 通道之外，我们还建议加密负载均衡持久性 Cookie。有关更多信息，请参阅 [HTTP cookie persistence](#)。

Helloverifyrequest 参数可缓解 DTLS DDoS 放大攻击：

从 NetScaler 12.1 版本 62.x 和 13.0 版本 79.x 开始，`helloverifyrequest` 参数默认启用。在 DTLS 配置文件上启用 `helloverifyrequest` 参数有助于降低攻击者或机器人使网络吞吐量过载的风险，这可能导致出站带宽耗尽。也就是说，它有助于缓解 DTLS DDoS 放大攻击。

要查看 `helloverifyrequest` 参数状态，请在 CLI 提示符下键入：

```
show dtlsProfile
```

保护 NetScaler® 上的直通流量

基础设施模式设置可用于保护 NetScaler 上的直通流量。这些基础设施模式设置提供了基本的安全级别，而不会中断任何应用程序。以下列表总结了可用的基础设施模式设置。

- 会话状态保护
- 会话固定保护（启用仅限 HTTP）
- HSTS（启用 HTTP 严格传输安全 (HSTS)）
- 强身份验证
- 首选端到端 SSL
- 代理 HTTPS / 拒绝所有其他流量

会话状态保护：

建议：已启用 NetScaler：默认情况下为大多数实体启用

会话状态保护设置默认启用，无需特定配置。当 NetScaler 配置为代理连接时。例如，当流量选择配置的虚拟服务器或 TCP 或更高类型的服务时，NetScaler 会创建一个有状态会话。NetScaler 会继续维护这些连接的状态，并且只处理落入此状态机的报文。其他报文将被丢弃或重置。

以下服务类型实体在 NetScaler 上实现此有状态行为。

- ADNS_TCP
- DIAMETER, DNS_TCP
- FTP-c
- GRE-c
- HTTP
- MYSQL, MSSQL
- NNTP
- ORACLE
- PUSH, PPTP
- RTSP, RDP
- SIP_SSL, SIP_TCP
- SMPP
- SSL, SSL_BRIDGE, SSL_DIAMETER, SSL_PUSH
- SSL_TCP, SYSLOG_TCP
- TCP
- ADNS_TCP
- RNAT (rnat_tcpproxy 已启用)

会话固定保护（通过启用 HttpOnly 标志或添加重写策略）：

建议：为 NetScaler 或后端服务器设置的 Cookie 启用 HttpOnly

NetScaler：对于 NetScaler 插入的 Cookie 默认启用，对于后端服务器设置的 Cookie 可通过重写实现。

HttpOnly：当您为 Cookie 标记 HttpOnly 标志时，它会告知浏览器此 Cookie 只能由服务器访问。任何尝试从客户端脚本访问 Cookie 的行为都将严格禁止。如果正确实施，HttpOnly Cookie 将使大量常见的跨站脚本攻击更难实现。

以下是设置了 HttpOnly 标志的 Cookie 示例：

```
Set-Cookie: ASP.NET_SessionId=ig2fac55; path=/; HttpOnly
```

NetScaler 为 Cookie 插入持久性而插入的 Cookie 默认设置 HttpOnly 标志，以指示该 Cookie 不可脚本化，并且不得向客户端应用程序公开。因此，客户端脚本无法访问该 Cookie，并且客户端不易受到跨站脚本攻击。

使用命令行界面启用 HttpOnly 标志设置：

在命令提示符下，键入：

```
set lb parameter -HttpOnlyCookieFlag (ENABLED)
```

使用重写策略为 Cookie 插入 Secure 和 HttpOnly：

重写策略为后端服务器发送的 Cookie 插入 Secure 和 HttpOnly。

注意： Secure 和 HttpOnly Cookie 可以一起用于 SSL VIP。对于非 SSL VIP，可以插入 HttpOnly 标志。

使用 NetScaler，可以为服务器设置的 Cookie 包含 HttpOnly 和 Secure 标志。

- HttpOnly - Cookie 上的此选项使 Web 浏览器仅使用 HTTP（或 HTTPS）协议返回 Cookie；非 HTTP 方法（例如 JavaScript document.cookie 引用）无法访问 Cookie。此选项有助于防止因跨站脚本攻击导致的 Cookie 窃取。
- Secure - Cookie 上的此选项使 Web 浏览器仅在传输通过 SSL 加密时返回 Cookie 值。此选项可用于防止通过连接窃听导致的 Cookie 窃取。

使用 CLI 创建重写策略

1. 如果尚未启用，请启用重写功能。

```
enable feature REWRITE
```

2. 创建重写操作（此示例配置为同时设置 Secure 和 HttpOnly 标志。如果缺少其中任何一个，请根据其他组合的需要进行修改）。

```
add rewrite action <action name> replace_all http.RES.full_Header  
"\"path=/; Secure; HttpOnly\"" -search "regex(re!(path=/\; Secure;
```

```
HttpOnly)|(path=/\;; Secure)|(path=/\;; HttpOnly)|(path=/)!)"
-bypassSafetyCheck YES
```

示例：

```
add rewrite action act_cookie_Secure replace_all http.RES.full_Header
 "\"path=/; Secure; HttpOnly\"" -search "regex(re!(path=/\;; Secure;
 HttpOnly)|(path=/\;; Secure)|(path=/\;; HttpOnly)|(path=/)!)"
```

or

```
add rewrite action act_cookie_Secure replace_all http.RES.full_Header
 "\"path=/; Secure; HttpOnly\"" -search "regex(re!(path=/\;; Secure;
 HttpOnly)|(path=/\;; Secure)|(path=/\;; HttpOnly)|(path=/)!)"
-bypassSafetyCheck YES
```

注意：

从 NetScaler 13.1 版本开始，`bypassSafetyCheck` 参数不再适用。但是，对于 13.1 之前的版本，此参数受支持。

3. 创建重写策略以触发操作。

```
add rewrite policy <policy name> "http.RES.HEADER(\"Set-
 Cookie\").EXISTS" <action name>
```

示例：

```
add rewrite policy rw_force_secure_cookie "http.RES.HEADER(\"Set-
 Cookie\").EXISTS" act_cookie_Secure
```

4. 将重写策略绑定到要保护的虚拟服务器（如果使用“安全”选项，则必须使用 SSL 虚拟服务器）。

```
bind lb vserver <vserver name> - <policy name> -priority <priority
 number> -gotoPriorityExpression NEXT -type RESPONSE
```

示例：

```
bind lb vserver mySSLVServer -policyName rw_force_secure_cookie  
-priority 100 -gotoPriorityExpression NEXT -type RESPONSE
```

有关更多信息，请参阅 <https://support.citrix.com/article/CTX138055>。

HSTS（启用 HTTP 严格传输安全 (HSTS)）：

要使用 NetScaler 命令行启用 HSTS：

在命令提示符下，键入：

```
set ssl vserver <vServerName> -HSTS ( ENABLED ) maxage <positive_integer>  
-IncludeSubdomains ( YES | NO )
```

或

```
set ssl profile <name> -HSTS ( ENABLED ) -maxage <positive_integer>  
-IncludeSubdomains ( YES | NO )
```

有关更多信息，请参阅以下主题。

- [配置对 HTTP 严格传输安全 \(HSTS\) 的支持。](#)
- <https://support.citrix.com/article/CTX205221>

强身份验证：

必须为所有对敏感数据、应用程序和管理的访问启用强身份验证（或多因素身份验证 – MFA）。

有关如何为多因素身份验证设置敏感应用程序的详细信息，请参阅 [多因素 \(nFactor\) 身份验证](#)。

首选端到端 SSL：

建议在前端和后端都使用 SSL。可以在 SSL 实体上禁用较旧的不安全协议版本，例如 SSLv3、TLS 1.0 和 TLS 1.1。您只能启用 TLS 1.2 和 TLS 1.3。这可以在 SSL 实体级别或配置文件级别完成，并且所有 SSL 实体都从配置文件继承 SSL 设置。

使用 CLI 在 SSL 实体上禁用不安全协议版本并启用安全协议版本

在命令提示符下，键入：

```
set ssl vserver <vServerName> -ssl2 DISABLED -ssl3 DISABLED -tls1  
DISABLED -tls11 DISABLED -tls12 ENABLED -tls13 ENABLED  
  
set ssl service <vServiceName> -ssl2 DISABLED -ssl3 DISABLED -tls1  
DISABLED -tls11 DISABLED -tls12 ENABLED -tls13 ENABLED
```

如果启用了 SSL 配置文件，请使用以下命令：

```
set ssl profile <frontend profile> -ssl3 DISABLED -tls1 DISABLED -  
tls11 DISABLED -tls12 ENABLED -tls13 ENABLED  
  
set ssl profile <backend profile> -ssl3 DISABLED -tls1 DISABLED -  
tls11 DISABLED -tls12 ENABLED -tls13 ENABLED
```

****注意：**

我们建议使用配置文件启用 TLS 1.3，而不是在虚拟服务器实体上启用它。有关更多信息，请参阅 [支持 TLS 1.3 协议](#)。

NetScaler 推荐的密码套件：

NetScaler 支持的以下密码不包含“强制丢弃”列表中的任何组件。这些密码按密钥交换（RSA、DHE 和 ECDHE）进行组织，性能较高的位于顶部，安全性较高的位于底部：

推荐的 RSA 密钥交换密码套件：

- TLS1-AES-128-CBC-SHA
- TLS1-AES-256-CBC-SHA
- TLS1.2-AES-128-SHA256
- TLS1.2-AES-256-SHA256
- TLS1.2-AES128-GCM-SHA256
- TLS1.2-AES256-GCM-SHA384

推荐的 DHE 密钥交换密码套件：

- TLS1-DHE-RSA-AES-128-CBC-SHA
- TLS1-DHE-RSA-AES-256-CBC-SHA
- TLS1.2-DHE-RSA-AES-128-SHA256
- TLS1.2-DHE-RSA-AES-256-SHA256
- TLS1.2-DHE-RSA-AES128-GCM-SHA256
- TLS1.2-DHE-RSA-AES256-GCM-SHA384

推荐的 ECDHE 密钥交换密码套件：

- TLS1-ECDHE-RSA-AES128-SHA
- TLS1-ECDHE-RSA-AES256-SHA
- TLS1.2-ECDHE-RSA-AES-128-SHA256
- TLS1.2-ECDHE-RSA-AES-256-SHA384
- TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
- TLS1.2-ECDHE-RSA-AES256-GCM-SHA384

推荐的密码套件（按优先顺序）：

以下密码列表包括 RSA、DHE 和 ECDHE 密钥交换。它在安全性、性能和兼容性之间提供了最佳折衷方案。

1. TLS1.2-AES128-GCM-SHA256
2. TLS1.2-AES-128-SHA256
3. TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
4. TLS1.2-ECDHE-RSA-AES-128-SHA256
5. TLS1-ECDHE-RSA-AES128-SHA
6. TLS1.2-DHE-RSA-AES128-GCM-SHA256
7. TLS1.2-DHE-RSA-AES-128-SHA256
8. TLS1-DHE-RSA-AES-128-CBC-SHA
9. TLS1-AES-128-CBC-SHA

SSL 安全配置文件和安全密码：

我们建议您将安全前端配置文件 (ns_default_ssl_profile_secure_frontend) 绑定到您的 SSL 虚拟服务器。已添加安全密码别名并将其绑定到安全前端配置文件。要列出属于此别名的密码，请在命令提示符下键入：

```
show cipher SECURE
```

```
1) Cipher Name: TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 Priority : 1
```

```
      Description: TLS 1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(256)  
Mac=AEAD  HexCode=0xc030
```

```
2) Cipher Name: TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 Priority : 2
```

```
      Description: TLS 1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(128)  
Mac=AEAD  HexCode=0xc02f
```

```
3) Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384  
Priority : 3
```

```
      Description: TLS 1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(256)  
Mac=AEAD  HexCode=0xc02c
```

```
4) Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256  
Priority : 4
```

```
      Description: TLS 1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(128)  
Mac=AEAD  HexCode=0xc02b
```

```
Done
```

有关安全前端配置文件的更多信息，请参阅 [安全前端配置文件](#)。

低于 TLS 1.2 的协议在 SSL 内部服务上被禁用。如果启用了默认（增强）配置文件，则 `ns_default_ssl_profile_internal_frontend_service` 配置文件将绑定到 SSL 内部服务，并且配置文件中禁用了 SSLv3、TLS 1.0、TLS 1.1 和 TLS 1.3 协议。

代理 HTTPS / 拒绝所有其他流量：

在可行的情况下，使用安全的 SSL 版本（TLS 1.2 或 TLS 1.3）和安全的密码，为 SSL VIP 提供更好的数据加密。在为 VIP 和后端 SSL 服务启用 SSL 时，必须考虑 SSL TPS 和 SSL 吞吐量。

管理

本节提供了一些特定配置更改的示例，这些更改可用于提高 NetScaler 和 NetScaler SDX 的安全性。有关 NetScaler 配置最佳实践的更多指导，请参阅文章 [NetScaler 设备通用实施的推荐设置和最佳实践](#)。

有关更多信息，请参阅以下主题。

- [系统和用户帐户](#)
- [日志记录和监视](#)
- [LOM 配置](#)
- [应用程序和服务](#)
- [DNSSEC 安全建议](#)
- [旧版配置](#)
- [配置 NDCPP 合规性证书检查](#)

系统和用户帐户

更改超级用户帐户的密码： 您无法删除内置的管理员超级用户 (`nsroot`)。因此，请将该帐户的默认密码更改为安全密码。要更改管理员用户的默认密码，请执行以下步骤：

1. 以超级用户身份登录并打开配置实用程序。
2. 在导航窗格中，展开“系统”节点。
3. 选择“用户”节点。
4. 在“系统用户”页面上，选择 `nsroot` 用户。
5. 选择“更改密码”。
6. 在“密码”和“确认密码”字段中输入所需密码。
7. 单击“确定”。

创建备用超级用户帐户： 要创建超级用户帐户，请运行以下命令：

```
add system user <newuser> <password>

bind system user <newuser> superuser 0
```

使用此超级用户帐户，而不是默认的 `nsroot` 超级用户帐户。

对于 NetScaler SDX 部署，管理员必须在初始设置后更改 NetScaler SDX 及其 GUI 管理控制台的默认凭据。要更改默认用户的密码，请执行以下步骤：

1. 以超级用户身份登录并打开配置实用程序。
2. 在导航窗格中，展开“系统”节点。
3. 选择“用户”节点。
4. 在“系统用户”页面上，选择默认用户。
5. 选择“修改”。
6. 在“密码”和“确认密码”字段中输入所需密码。
7. 单击“确定”。

系统用户的强密码：

我们建议为在 NetScaler 中创建的系统用户帐户使用强密码。密码复杂性要求示例如下：

- 密码长度必须至少为八个字符。
- 密码不得包含字典词或字典词的组合。
- 密码必须至少包含一个大写字母、一个小写字母、一个数字和一个特殊字符。

可以通过设置两个参数来强制使用强密码，一个用于密码的最小长度，另一个用于强制密码复杂性：

```
set system parameter -minpasswordlen <positive_integer> -  
-strongpassword ( ENABLED | DISABLED )
```

在需要多个管理员的部署中，请考虑使用外部身份验证方法来验证用户，例如 RADIUS、TACACS+ 或 LDAP(S)。有关更多信息，请参阅[外部用户身份验证](#)。

锁定系统用户帐户以进行管理访问： NetScaler 允许您锁定系统用户 24 小时并拒绝用户访问。NetScaler 支持系统用户和外部用户的配置。在命令提示符下键入：

```
set aaa parameter -persistentLoginAttempts DISABLED
```

现在，要锁定用户帐户，请在命令提示符下键入：

```
lock aaa user test
```

有关如何使用 GUI 配置此功能的信息，请参阅 [用户帐户和密码管理](#)。

解锁锁定的系统用户帐户以进行管理访问：系统用户和外部用户可以使用锁定身份验证、授权和审计用户命令锁定 24 小时。NetScaler 允许您解锁锁定的系统用户。在命令提示符下，键入：

```
unlock aaa user test
```

 有关如何使用 GUI 配置此功能的信息，请参阅 [用户帐户和密码管理](#)。

禁用系统用户帐户的管理访问：当 NetScaler 上配置了外部身份验证，并且作为管理员，您希望拒绝系统用户登录管理访问时，必须禁用系统参数中的 localAuth 选项。

注意：

必须配置外部服务器。

在命令提示符下，键入以下内容：

```
set system parameter localAuth <ENABLED|DISABLED>
```

示例：

```
set system parameter localAuth DISABLED
```

 有关如何使用 GUI 配置此功能的信息，请参阅 [用户帐户和密码管理](#)。

强制管理员用户更改密码：对于 `nsroot` 安全身份验证，如果系统参数中启用了 `forcePasswordChange` 选项，NetScaler 会提示用户将默认密码更改为新密码。您可以在首次使用默认凭据登录时，通过 CLI 或 GUI 更改您的 `nsroot` 密码。在命令提示符下，键入：

```
set system parameter -forcePasswordChange ( ENABLED | DISABLED )
```

有关如何配置此功能的示例，请参阅 [用户帐户和密码管理](#)。

使用 SSH 密钥和无密码访问 NetScaler：在需要管理多个 NetScaler 设备的环境中，请考虑使用 SSH 密钥和无密码。有关如何配置此功能的信息，请参阅 [使用 SSH 密钥和无密码访问 NetScaler 设备](#)。

创建用于数据保护的系统主密钥：从 Citrix ADC 12.1 到 Citrix 13.0–71.44，需要创建一个系统主密钥来保护某些安全参数，例如 LDAP 身份验证所需的服务帐户密码以及本地存储的身份验证、授权和审计用户帐户。

注意：

从 Citrix 13.0 build 76.31 及更高版本开始，升级过程默认会自动创建一个随机系统主密钥。请务必根据组织的密码策略频繁更新 KEK。

要创建系统主密钥：

1. 使用 CLI，以系统管理员身份登录。
2. 输入以下命令：

```
create kek <passphrase>
```

注意：

- 运行 `create kek` 命令后，KEK 用于大多数密码加密（本地用户密码不使用 KEK 加密）。
- 您不得删除 KEK 文件。如果您有 shell 访问权限并错误地删除了密钥片段文件，这可能会导致配置丢失、同步失败、登录失败。请注意以下事项。
 - 降级时，请始终使用与所安装版本匹配的旧配置文件；否则，登录、源配置、同步、故障转移可能会失败。
 - 如果任何密钥片段文件丢失或损坏，敏感数据的加密/解密将失败，这反过来可能导致配置丢失、同步失败、登录失败。
- 密码短语必须至少为 8 个字符。

在已部署的 NetScaler 上更新密钥加密密钥：

NetScaler 支持在已部署的 ADC 上更新 KEK。使用以下命令更新 KEK。

```
update kek -level <basic | extended>
```

更新 KEK 命令仅在 NSIP 接口上受支持。该命令支持以下两个选项。

- **基本**：备份旧密钥，创建密钥，并响应。如果任何文件更新失败，系统将报告错误并恢复到原始状态。
- **扩展**：备份旧密钥并创建新密钥。更新默认和非默认分区下的配置文件，例如 `ns.conf` 和 `ns.conf.0`。在更新期间，阻止所有配置更改。更新完成后，NetScaler 会响应。如果任何文件更新失败，系统将报告错误并恢复到原始状态。

以前，NetScaler 仅支持每个节点的默认 KEK。没有更新 KEK 的选项。

作为一项安全最佳实践，KEK 必须根据组织的密码策略频繁更改。

使用访问控制列表：

默认情况下，NetScaler 上可访问所有协议和端口，包括 GUI 和 SSH。访问控制列表 (ACL) 可以通过仅允许明确指定的用户访问端口和协议来帮助您安全地管理 NetScaler。

控制对 NetScaler 访问的建议：

- 考虑使用 NetScaler Gateway 将对 NetScaler 的访问限制为仅限 GUI。对于需要除 GUI 之外的其他访问方法的管理员，NetScaler Gateway 必须配置一个默认的“DENY”ACL，用于端口 80、443 和 3010，但对于受信任的 IP 地址，则明确“ALLOW”访问这些端口。

此策略可以通过以下 NSCLI 命令扩展，用于受信任的 IP 地址范围：

```
add acl local_access allow -srcip 192.168.0.1-192.168.0.3 -destip  
192.168.0.1-192.168.0.3
```

```
apply acIs
```

- 如果您使用 SNMP，请使用 ACL 明确允许 SNMP 流量。以下是一组示例命令：

```
add acl snmp1-ssh ALLOW -srcip 10.0.0.1-10.0.0.20 -destip  
192.168.0.2-192.168.0.3 -destport 161 -protocol udp
```

```
add acl snmp2-ssh ALLOW -srcip 172.16.0.1-172.16.0.20 -destip  
192.168.0.2-192.168.0.3 -destport 161 -protocol udp
```

```
apply acIs
```

在前面的示例中，该命令为所有 SNMP 查询提供了对两个已定义子网的访问权限，即使这些查询是针对适当定义的社区。

您可以在 NSIP 和 SNIP 地址上启用管理功能。如果启用，请使用 ACL 为 NSIP、SNIP 地址提供访问权限，以保护对管理功能的访问。管理员还可以配置 NetScaler，使其无法通过 ping 命令访问。

- 开放最短路径优先 (OSPF) 和 IPSEC 不是基于 TCP 或 UDP 的协议。因此，如果您需要 NetScaler 支持这些协议，请使用 ACL 明确允许使用这些协议的流量。运行以下命令定义 ACL，以通过协议号指定 OSPF 和 IPSEC：

```
add acl allow_ospf allow -protocolnumber 89
```

```
add acl allow_ipsec allow -protocolnumber 50
```

- 如果使用 XML-API Web 服务，请完成以下任务以保护 API 接口：
- 使用 ACL 为主机提供访问接口的权限。例如，运行以下命令以使 IP 地址范围为 10.0.0.1-20 和 172.16.0.1-20 的主机能够访问 XML-API 接口：

```
add acl xml-api1 ALLOW -srcip 10.0.0.1-10.0.0.20 -destip  
192.168.0.2-192.168.0.3 -destport 80 -protocol tcp
```

```
add acl xml-api2 ALLOW -srcip 172.16.0.1-172.16.0.20 -destip  
192.168.0.2-192.168.0.3 -destport 80 -protocol tcp
```

```
apply acls
```

- 要为内部端口应用 ACL，请使用以下命令：

```
set l3param -implicitACLAllow DISABLED
```

注意：

implicitACLAllow 命令的默认值为 **已启用**。

- 要从内部端口删除 ACL，请使用以下命令：

```
set l3param -implicitACLAllow ENABLED
```

- 您可以通过使用客户端证书来获得额外的安全性。有关客户端证书和客户端身份验证的更多信息，请参阅[客户端身份验证](#)或知识中心文章 CTX214874：[如何在固件版本 10.1 及更高版本的 NetScaler 设备上创建和使用客户端证书](#)。

对管理用户使用基于角色的访问控制：

NetScaler 包含四种命令策略或角色，例如操作员、只读、网络和超级用户。您还可以定义命令策略，为不同的角色创建不同的管理帐户，并将该角色所需的命令策略分配给这些帐户。以下是一组示例命令，用于将只读访问权限限制为只读用户：

```
add system user readonlyuser

bind system user readonlyuser read-only 0
```

有关配置用户、用户组或命令策略的更多信息，请参阅[用户](#)、[用户组](#)和[命令策略](#)。

配置系统会话超时：

提供会话超时时间间隔是为了限制会话（GUI、CLI 或 API）在不使用时保持活动状态的时间长度。对于 NetScaler，系统会话超时可以在以下级别配置：

- 用户级别超时。适用于特定用户。

GUI：导航到 **System > User Administration > Users**，选择一个用户，然后编辑该用户的超时设置。CLI：在命令提示符下，输入以下命令：

```
set system user <name> -timeout <secs>
```

- 用户组级别超时。适用于组中的所有用户。

GUI：导航到 **System > User Administration > Groups**，选择一个组，然后编辑该组的超时设置。CLI：在命令提示符下，输入以下命令：

```
set system group <groupName> -timeout <secs>
```

- 全局系统超时。适用于所有用户以及未配置超时的组中的用户。

GUI：导航到 **System > Settings**，单击 **Set global system parameters**，然后设置 ANY Client Idle Time-out (secs) 参数。CLI：在命令提示符下，输入以下命令：

```
set system parameter -timeout <secs>
```

为用户指定的超时值具有最高优先级。如果未为用户配置超时，则考虑为成员组配置的超时。如果未为组指定超时（或用户不属于任何组），则考虑全局配置的超时值。如果在任何级别都未配置超时，则将默认值 900 秒设置为系统会话超时。

您还可以限制超时值，以便会话超时值不能超过管理员配置的超时值。您可以将超时值限制在 5 分钟到 1 天之间。要限制超时值：

- GUI：导航到 **System > Settings**，单击 **Set global system parameters**，然后选择 Restricted Timeout 字段。
- CLI：在命令提示符下，输入以下命令：

```
set system parameter -restrictedtimeout <ENABLED/DISABLED>
```

用户启用 restrictedTimeout 参数后，如果超时值已配置为大于 1 天或小于 5 分钟的值，则会通知用户更改超时值。如果用户未更改超时值，则在下次重新启动时，超时值将默认重新配置为 900 秒（15 分钟）。

您还可以为所访问的每个接口指定超时持续时间。但是，为特定接口指定的超时值受限于为访问该接口的用户配置的超时值。例如，假设用户 **publicadmin** 的超时值为 20 分钟。现在，当访问接口时，用户必须指定在 20 分钟内的超时值。

要在每个接口上配置超时持续时间：

- CLI：使用以下命令在命令提示符下指定超时值：

```
set cli mode -timeout <secs>
```

- API：在登录有效负载中指定超时值。

日志记录和监控

配置网络时间协议

我们建议在 NetScaler 上启用网络时间协议 (NTP)，并将其配置为使用受信任的网络时间服务器。启用 NTP 可确保日志条目和系统事件记录的时间准确无误，并与其他网络资源同步。

配置 NTP 时，必须修改 ntp.conf 文件，以限制 NTP 服务器泄露敏感数据包中的信息。

您可以运行以下命令在 NetScaler 上配置 NTP：

```
add ntp server <IP_address> 10

enable ntp sync
```

为您添加的每个受信任的 NTP 服务器修改 ntp.conf 文件。每个服务器条目都必须有一个相应的 restrict 条目。您可以通过从 NetScaler shell 提示符运行 `find . -name ntp.conf` 命令来找到 ntp.conf 文件。

配置 SNMP

NetScaler 支持 SNMP 协议的第 3 版。SNMPv3 包含管理和安全功能，例如身份验证、访问控制和数据完整性检查。有关更多信息，请参阅 [为 SNMPv3 查询配置 NetScaler](#)。

注意：

我们建议您使用 SNMPv3 而不是 SNMPv1 和 SNMPv2。

如果您未配置至少一个 SNMP 管理器，NetScaler 将接受并响应来自网络中所有 IP 地址的 SNMP 查询。运行以下命令添加 SNMP 管理器并限制此行为：

```
add snmp manager <IP_address>
```

在不需要 SNMP 的部署中，必须使用以下命令禁用该功能：

```
set ns ip <IP_Address> -snmp disabled
```

配置日志记录到外部 NetScaler 日志主机

NetScaler 审计服务器记录内核和用户级守护程序中不同模块收集的所有状态和状态信息。审计服务器使管理员能够按时间顺序查看事件历史记录。审计服务器类似于从 NetScaler 收集日志的 SYSLOG 服务器。审计服务器使用管理员凭据从一个或多个设备中获取日志。

- 本地审计服务器配置

运行以下命令以在 NetScaler 中配置到本地审计服务器的日志记录：

```
> set audit nslogparams -serverip <hostname> -serverport <port>
```

- 远程审计服务器配置

要在远程计算机中配置到审计服务器的日志记录，请在该计算机上安装审计服务器。以下是示例审计服务器选项：

```
./audserver -help

usage : audserver -[cmds] [cmd arguments]

cmds cmd arguments: -f <filename> -d debug

-help - detail help

-start - cmd arguments, [starts audit server]

-stop - stop audit server

-verify - cmd arguments [verifies config file]

-addns - cmd arguments [add a netscaler to conf file]

-version - prints the version info
```

这些选项仅提供记录由 NetScaler ns.log 文件生成的审计消息的功能。要记录所有 syslog 消息，请执行以下步骤：

1. 从 /nsconfig/syslog.conf 文件中删除本地设施的日志文件规范。
2. 将日志文件规范替换为远程 syslog 主机的日志主机名或 IP 地址，类似于以下条目：

配置 local0.* 日志到 10.100.3.53

配置 local1.* 日志到 10.100.3.53

3. 配置 syslog 服务器以接受来自上述日志记录设施的日志条目。有关更多信息，请参阅 syslog 服务器文档。
4. 对于大多数使用标准 syslog 软件的基于 UNIX 的服务器，您必须为消息和 nsvpn.log 文件向 syslog.conf 配置文件添加本地设施配置条目。设施值必须与 NetScaler 上配置的值相对应。
5. 任何基于 UNIX 的计算机中的远程 syslog 服务器默认不侦听远程日志。因此，运行以下命令以启动远程 syslog 服务器：

```
syslogd -m 0 -r
```

注意：

请参阅部署在审计服务器中的 syslog 变体的等效选项。

通过安全通道配置消息导出

您可以通过 SSL（安全套接字层）安全地导出 syslog，确保敏感日志数据以加密和经过身份验证的方式遍历网络。通过利用 SSL，您可以保护 syslog 传输免受窃听、篡改和未经授权的访问。有关更多信息，请参阅[通过 SSL 安全导出 syslog](#)。

LOM 配置

我们建议采取以下措施来保护 LOM 接口的安全：

- 请勿将 LOM 端口暴露给互联网。
- 将 LOM 部署在 SPI 防火墙后面。
- 将 LOM 部署到与不受信任的网络流量逻辑上（单独的 VLAN）或物理上（单独的 LAN）隔离的网络段上。
- 为 LOM 和 NetScaler 管理端口设置不同的用户名、密码、SSL 证书和 SSL 密钥值。
- 确保用于访问 LOM 管理接口的设备专门用于网络管理目的，并放置在与同一物理 LAN 或 VLAN 中的其他管理设备端口相同的管理网络段上。
- 为了便于识别和隔离 LOM IP 地址，请为 LOM 管理接口和管理服务器保留特殊的 IP 地址（私有子网）。请勿将保留的 IP 子网与受管 NetScaler 的 LAN 接口一起使用。不建议使用 DHCP 分配的动态 IP 地址，因为它们会使在 LAN 段外部基于 MAC 地址实施防火墙访问控制列表变得困难。
- 将密码设置为至少 8 个字符，包含字母数字和特殊字符的组合。经常更改密码。

应用程序和服务

配置 NetScaler® 以删除或传递升级标头

HTTP 配置文件中新增了一个参数 `passProtocolUpgrade`，用于防止对后端服务器的攻击。根据此参数的状态，升级标头会在发送到后端请求中传递，或者在发送请求之前被删除。

- 如果 `passProtocolUpgrade` 参数已启用，则升级标头将传递到后端。服务器接受升级请求并在其响应中通知。
- 如果此参数已禁用，则升级标头将被删除，剩余的请求将发送到后端。

`passProtocolUpgrade` 参数已添加到以下配置文件中。

- nshttp_default_profile - 默认启用
- nshttp_default_strict_validation - 默认禁用
- nshttp_default_internal_apps - 默认禁用
- nshttp_default_http_quic_profile - 默认启用

我们建议您将 `passProtocolUpgrade` 参数设置为禁用。

使用 CLI 设置 `passProtocolUpgrade` 参数：

在命令提示符下，键入以下内容：

```
set ns httpProfile <name> [-passProtocolUpgrade ( ENABLED | DISABLED )]
```

使用 GUI 设置 `passProtocolUpgrade` 参数：

1. 导航到 **系统 -> 配置文件 -> HTTP 配置文件**。
2. 创建或编辑 HTTP 配置文件。
3. 选中 **通过协议升级** 复选框。

配置 NetScaler 以丢弃无效的 HTTP 请求

建议将 NetScaler 配置为严格检查和强制执行 HTTP 请求，以防止无效的 HTTP 请求通过虚拟服务器。为此，请使用 CLI 上的以下命令将内置 HTTP 配置文件 `nshttp_default_strict_validation` 绑定到一个或多个虚拟服务器：

```
show ns httpProfile (Shows the available http profile (default+user configured profiles))
```

```
set lb vserver <vserver name> -httpProfileName  
nshttp_default_strict_validation
```

建议使用此选项的客户在发布到生产环境之前，在预生产环境中测试这些更改。

默认情况下，严格 HTTP 验证配置文件 (`nshttp_default_strict_validation`) 上启用了针对 HTTP 解同步攻击的保护。将严格配置文件用于所有面向客户端的实体。

有关 HTTP 请求走私攻击及其缓解措施的更多信息，请参阅支持文章 [NetScaler - HTTP 请求走私参考指南](#)。

配置针对 HTTP 拒绝服务攻击的保护

NetScaler 固件支持针对 HTTP 拒绝服务攻击（包括“慢速读取”类型攻击）的有限对策。您可以通过 NetScaler shell 提示符使用 `nsapimgr` 实用程序配置这些功能：

- `small_window_threshold` (默认值=1)
- `small_window_idle_timeout` (默认值=7 秒)
- `small_window_cleanthresh` (默认值=100)
- `small_window_protection` (默认值=已启用)

默认设置足以防止 HTTP 拒绝服务攻击，包括慢速读取攻击，但对于其他攻击可能需要对参数进行一些调整。

为了防止此类攻击，请在 NetScaler shell 提示符下使用以下 `nsapimgr` 命令向上调整

`small_window_threshold` 属性：

```
$ nsapimgr -ys small_window_threshold=<desired value>
```

注意：

可以根据部署中的传入流量模式设置 `small_window_threshold` 期望值。可接受的范围是 0 到 2^{32} 。

您可以通过在 NetScaler shell 提示符下使用 `nsconmsg -d stats` 命令监控以下计数器来验证针对 HTTP 拒绝服务攻击的保护：

- `nstcp_cur_zero_win_pcb`s：此计数器跟踪当前窗口值较低的 PCB 数量。
- `nstcp_err_conndrop_at_pass`：当 NetScaler 检测到在将数据包从一侧传递到另一侧时，它已超过 `nscfg_small_window_idletimeout` 值时，此计数器会递增。
- `nstcp_err_conndrop_at_retx`：当重传期间经过的时间超过 `nscfg_small_window_idletimeout` 值时，此计数器会递增。
- `nstcp_cur_pcb`s_probed_withKA：此计数器跟踪激增队列中通过 KA 探测器探测的 PCB 数量。

我们建议使用此选项的客户在将其发布到生产环境之前，在预生产环境中测试这些更改。

配置 NetScaler 以防御 TCP 欺骗攻击

以下命令可用于帮助保护后端服务器免受 TCP 欺骗攻击：

```
set ns tcpProfile profile1 -rstWindowAttenuate ENABLED -spoofSynDrop  
ENABLED
```

Done

```
set lb vserver lbvserver1 -tcpProfileName profile1
```

Done

我们建议使用此选项的客户在将其发布到生产环境之前，在预生产环境中测试这些更改。

配置 RFC 5961 合规性

从 NetScaler 14.1-4.x 版本开始，TCP 配置文件中提供了 `-rfc5961Compliance` 选项。此选项包括欺骗保护，并涵盖 `-rstWindowAttenuate` 和 `-spoofSynDrop`。启用 `-rfc5961Compliance` 可获得所有这些保护，而无需单独设置每个选项。

有关更多信息，请参阅 [示例 TCP 配置](#)。

配置 NetScaler 以接受特定的 HTTP 标头

可以将 NetScaler 配置为仅接受特定的 HTTP 标头。这可以通过添加重写操作来实现，以限制具有特定定义的 HTTP 标头的网络流量传递到后端服务器。

以下全局重写操作仅将带有 Host、Accept 和 test 等标头的网络流量发送到服务器：

```
add rewrite action act1 replace_all q/  
HTTP.REQ.FULL_HEADER.after_str("\r\n")/      q{TARGET.REGEX_SELECT(re/  
(iu)^(Host|Accept|test):.*\r\n/) ALT ""} -pattern q{re/(U).+:\r\n/}
```

```
add rewrite policy pol1 HTTP.REQ.IS_VALID act1
```

```
bind rewrite global pol1 100
```

配置 HTTP 标头的标头大小

我们建议您为 `maxHeaderLen` 和 `maxHeaderFieldLen` HTTP 标头大小参数维护一个适合您业务需求的值。默认值设置为 24820，这确保了与需要大型 HTTP 标头的应用程序的兼容性。

```
set httpprofile http-prof -maxHeaderLen <header-length> -maxHeaderFieldLen  
<header-field-length>
```

`maxHeaderLen` 参数控制总标头大小，`maxHeaderFieldLen` 控制单个标头字段的大小。这些参数可用于通过限制基于标头的攻击（例如缓冲区溢出或标头注入攻击）的攻击面来增强安全性。在虚拟服务器上配置的 HTTP 配置文件以及绑定到虚拟服务器的服务组或服务上设置标头大小。

虽然可以将这些参数配置为较低的值，但如果应用程序使用的标头超出配置的限制，这样做可能会导致合法请求被丢弃。因此，管理员在降低这些值之前必须仔细评估其应用程序要求。

在 NetScaler 中规范化 URL

URL 规范化将不一致的 URL 格式标准化为单一、可预测的结构，确保安全规则、搜索引擎和网络爬虫将同一网络资源的不同表示形式视为相同。NetScaler 通过本机 HTTP 配置文件参数解决此问题，有助于防止攻击者利用非规范化 URL 绕过安全过滤器。

URL 规范化在以下 NetScaler 版本中可用：

- 14.1-73.37 及更高版本
- 14.1-73.37 FIPS 及更高版本
- 13.1-64.23 及更高版本
- 13.1 37.279 FIPS 及更高版本

使用以下命令启用 URL 规范化参数：

```
set ns httpProfile <profilename> -normalizeURL ENABLED
```

使用以下命令为发送到源服务器的请求启用 RFC 3986 URL 规范化：

```
set ns httpProfile <profilename> -normalizeURLtoOrigin ENABLED
```

有关更多信息，请参阅 [在 NetScaler 中规范化 URL](#)。

增强型 TCP ISN 生成

增强型 ISN 生成增加了 NetScaler 上 TCP 连接建立期间初始序列号的随机性（仅限服务器端），从而降低了攻击者可能利用的可预测性。此参数默认禁用，但可以通过使用 CLI 启用。

增强型 TCP ISN 生成在以下 NetScaler 版本中可用：

- 14.1-73.37 及更高版本
- 14.1-73.37 FIPS 及更高版本
- 13.1-64.23 及更高版本
- 13.1 37.279 FIPS 及更高版本

使用以下命令启用增强型 ISN 生成参数：

```
set ns tcpparam -enhancedISNgeneration ENABLED
```

有关更多信息，请参阅 [增强型 ISN 生成](#)。

配置关闭通知

关闭通知是一种安全消息，指示 SSL 数据传输的结束。根据 RFC 5246：客户端和服务器必须共享连接正在结束的知识，以避免截断攻击。任何一方都可以通过发送 close_notify 警报来发起关闭消息的交换。在收到关闭警报后收到的任何数据都将被忽略，除非已传输其他致命警报，否则在关闭连接的写入端之前，各方都必须发送 close_notify 警报。为确保捕获 TLS 终止事件的审计事件，请以超级用户或系统管理员身份登录 CLI 并运行以下命令：

```
set ssl parameter -sendCloseNotify y

save ns config
```

保护管理 GUI、NITRO API 和 RPC 通信

为了保护 NetScaler 和 NetScaler Gateway 上的管理 GUI、NITRO API 和 RPC 通信，您必须在 NetScaler 中为内部 HTTP/HTTPS 服务设置 `-maxclient`。

```
set service nshttpd-gui-127.0.0.1-80 -maxclient $max_client{}

set service nshttpd-vpn-127.0.0.1-81 -maxclient $max_client{}
```

```
set service nshttps-127.0.0.1-443 -maxclient $max_client{}
```

有关设置 `-maxclient` 值以及支持此设置的 NetScaler 版本的更多信息，请参阅 [使用 NetScaler GUI、NetScaler CLI 或 NetScaler NITRO API 配置内部 HTTP GUI 服务](#)。

DNSSEC 安全建议

我们建议使用 DNSSEC 的客户应用以下建议：

KSK/ZSK 私钥使用 1024 位或更高位的 RSA

NIST 建议 DNS 管理员维护 1024 位 RSA/SHA-1 或 RSA/SHA-256 ZSK，直到 01 October 2015。

启用 DNSSEC 密钥过期 SNMP 警报

默认情况下，NetScaler 上已启用 DNSSEC 密钥过期 SNMP 警报。密钥过期通知通过名为 `dnskeyExpiry` 的 SNMP trap 发送。三个 MIB 变量 `dnskeyName` 和 `dnskeyUnitsOfExpiry` 随 `dnskeyExpiry` SNMP trap 一起发送。有关更多信息，请参阅 NetScaler SNMP OID 参考。

在 x.509 证书过期之前轮换 KSK/ZSK 私钥

在 NetScaler 上，您可以使用预发布和双签名方法来执行区域签名密钥和密钥签名密钥的轮换。有关更多信息，请参阅 NetScaler 文档中的“[域名系统 > 配置 DNSSEC](#)”主题。

保护 DNSSEC ADNS 服务器

如果 NetScaler 配置为 DNSSEC 代理模式，它会缓存来自后端 ADNS 服务器的响应，并将缓存的响应转发给 DNS 客户端。

当 NetScaler 对给定区域具有权威性时，该区域中的所有资源记录都在 NetScaler 上配置。要签署权威区域，您必须为该区域创建密钥（区域签名密钥和密钥签名密钥），将密钥添加到 NetScaler，然后签署该区域。

要将 NetScaler 配置为权威服务器，请执行以下步骤：

1. 添加 ADNS 服务。

例如：

```
add service s1 <ip address> adns 53`
```

2. 创建 DNS 密钥。

例如，要作为 **com** 域的权威服务器：

```
create dns key -zoneName com -keytype ksk -algorithm rsASHA512 -keysize 3000 -fileNamePrefix com.ksk.rsasha1.3000
```

```
create dns key -zoneName com -keytype zsk -algorithm rsASHA512 -keysize 3000 -fileNamePrefix com.zsk.rsasha1.3000
```

注意：

您必须创建一次 DNS 密钥，它们将保存在 `/nsconfig/dns` 中。

3. 添加 DNS 密钥。

例如，

```
add dns key com.zsk.3000 /nsconfig/dns/com.zsk.rsasha1.3000.key /  
nsconfig/dns/com.zsk.rsasha1.3000.private
```

```
add dns key com.ksk.3000 /nsconfig/dns/com.ksk.rsasha1.3000.key /  
nsconfig/dns/com.ksk.rsasha1.3000.private
```

4. 为 **com** 区域添加 NS 和 SOA 记录，然后对该区域进行签名。

```
add dns soaRec com -originServer n1.com -contact citrix
```

```
add dns nsrec com n1.com
```

```
add dns zone com -proxyMode no
```

```
add dns addRec n1.com 1.1.1.1
```

```
sign dns zone com
```

注意：此外，您还必须在 DNS 全局参数中启用 DNSEC 扩展参数。

有关将 NetScaler 配置为权威域名服务器的更多信息，请参阅 [产品文档](#) 上的“[域名系统 > 将 NetScaler 配置为 ADNS 服务器](#)”主题。

旧版配置

配置 NetScaler® 以禁用密码重定向

通过密码重定向，您可以配置 SSL 虚拟服务器，以便在 SSL 握手失败时提供准确、有意义的错误消息。当 SSL 握手失败时，NetScaler 会将用户重定向到预先配置的 URL。如果未配置 URL，NetScaler 将显示内部生成的错误页面。

在命令提示符下，运行以下命令以配置密码重定向并验证配置：

```
set ssl vservice <vServerName> -cipherRedirect DISABLED

show ssl vservice <vServerName>
```

当您默认 SSL 配置文件绑定到 NetScaler 中的虚拟服务器时，该虚拟服务器的 SSL 参数将从绑定的配置文件继承。因此，您无法直接修改虚拟服务器上的 SSL 参数，因为 SSL 配置文件控制这些设置。

```
set ssl profile <ssl Profile name> -cipherRedirect DISABLED
```

有关详细信息，请参阅 [密码重定向](#)。

在 NetScaler 上配置 SSL 重新协商设置

我们建议您禁用 SSL 重新协商：

```
set ssl parameter -denySSLReneg ALL
```

如果配置文件已启用，我们还建议您在前端和后端配置文件上设置此参数。

```
set ssl profile <frontend ssl profile name> -denySSLReneg ALL

set ssl profile <backend ssl profile name> -denySSLReneg ALL
```

有关详细信息，请参阅 [如何配置和使用 -denySSLReneg 参数](#)。

配置 NDcPP 合规性证书检查

NDcPP 合规性证书检查适用于 NetScaler 作为客户端（后端连接）时。在证书验证期间，如果 SSL 证书中存在 SAN，则忽略通用名称。

在命令提示符下，键入以下命令以配置 SSL 参数中的 "ndcppComplianceCertCheck" 属性：

```
set ssl parameter [-quantumSize <quantumSize>] [-crlMemorySizeMB  
<positive_integer>] [-strictCAChecks (YES | NO)] [-sslTriggerTimeout  
<positive_integer>] [-sendCloseNotify (YES | NO)] [-encryptTriggerPktCount  
<positive_integer>] [-denySSLReneg <denySSLReneg>] [-insertionEncoding  
(Unicode|UTF-8)] [-ocspCacheSize <positive_integer>] [- pushFlag  
<positive_integer>] [- dropReqWithNoHostHeader (YES | NO)] [-  
pushEncTriggerTimeout <positive_integer>] [-ndcppComplianceCertCheck ( YES  
| NO)] [-heterogeneousSSLHW (ENABLED | DISABLED )]
```

示例：

```
set ssl parameter -quantumSize 8 -crlMemorySizeMB 256 -strictCAChecks no  
-ssltriggerTimeout 100 -sendClosenotify no -encryptTriggerPktCount 45  
-denySSLReneg NONSECURE -insertionEncoding unicode -ocspCacheSize 10  
-pushFlag 3 -dropReqWithNoHostHeader YES -pushEncTriggerTimeout 100 ms  
-ndcppComplianceCertCheck YES
```

NetScaler® 加密建议

本节详细介绍了为确保在 NetScaler 上正确保护加密材料而必须遵循的一些关键步骤。它还提供了有关如何配置 NetScaler 以使用此材料来保护 NetScaler、后端服务器和最终用户的信息。

管理 TLS 证书和密钥

为 FIPS 和 NDcPP 部署配置 TLS 密码套件

FIPS 和 NDcPP 部署支持以下 TLS 密码套件。

- TLS1-AES-256-CBC-SHA
- TLS1-AES-128-CBC-SHA
- TLS1-ECDHE-RSA-AES256-SHA

- TLS1-ECDHE-RSA-AES128-SHA
- TLS1.2-ECDHE-RSA-AES-256-SHA384
- TLS1.2-ECDHE-RSA-AES-128-SHA256
- TLS1.2-AES256-GCM-SHA384
- TLS1.2-AES128-GCM-SHA256
- TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
- TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
- TLS1.2-AES-256-SHA256
- TLS1.2-AES-128-SHA256
- TLS1-ECDHE-ECDSA-AES256-SHA
- TLS1-ECDHE-ECDSA-AES128-SHA
- TLS1.2-ECDHE-ECDSA-AES256-SHA384
- TLS1.2-ECDHE-ECDSA-AES128-SHA256
- TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
- TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256
- TLS1.3-AES256-GCM-SHA384
- TLS1.3-AES128-GCM-SHA256

有关 MPX 14000 FIPS 支持的密码列表，请参阅 <https://docs.netscaler.com/zh-cn/citrix-adc/downloads/cipher-support-on-netscaler-mpx-sdx-14000-fips.pdf>。

为确保仅在 NetScaler 上配置经批准的密码套件，请从 CLI 完成以下配置步骤：

1. 从虚拟服务器解除绑定所有密码

```
unbind ssl vs v1 -cipherName FIPS
```

2. 仅绑定 TLS1-AES-256-CBC-SHA，然后绑定 TLS1-AES-128-CBC-SHA，使用以下命令：

```
bind ssl vs v1 -cipherName <cipher>
```

```
bind ssl vs v1 -cipherName TLS1-AES-256-CBC-SHA
```

使用受信任的 CA 安装证书和密钥对：

要从公共或企业证书颁发机构 (CA) 获取证书，您必须首先生成私钥和证书签名请求 (CSR)。请执行以下步骤：

1. 以系统管理员或超级用户身份登录 NetScaler CLI。
2. 创建 RSA 私钥。

```
create fipsKey m1 -keytype RSA -modulus 2048 -exponent F4
```

3. 创建证书签名请求 (CSR)：

```
create certreq csr_1 -fipsKeyName m1 -countryName IN -stateName BA  
-organizationName citrix
```

4. 将 CSR 提交给证书颁发机构。

对于大多数商业和企业 CA，CSR 通过电子邮件请求发送。但是，提交方法可能因企业 CA 环境而异。CA 通过电子邮件返回有效证书，但此操作也可能因企业 CA 而异。从 CA 收到证书后，请将其安全地复制到 /nsconfig/ssl 目录。

以超级用户或系统管理员身份登录，并从 CLI 运行以下命令：

```
> add ssl certKey ck_1 -cert  
cert1_1 -fipsKey m1
```

NetScaler -FIPS 建议

在基于 FIPS 的部署中配置 NetScaler SDX

如果您是现有的 FIPS 客户并使用 NetScaler SDX 实现真正的多租户，请使用 FIPS 认证的 NetScaler MPX 终止 TLS 并将流量转发到 NetScaler SDX。或者，也可以使用 Thales 外部 HSM。更改 FIPS 加密卡密码 当使用 FIPS 认证版本的 NetScaler 和硬件安全模块 (HSM) 时，请更改默认的安全官 (SO) 并按如下方式设置新的用户密码。如果您不知道启用 FIPS 的 NetScaler 的默认 SO 密码，请联系 [NetScaler 支持](#)。注意：只有超级用户或系统管理员才能执行此任务。

```
set ssl fips -initHSM Level-2 <soPassword> <oldSoPassword> <user-Password>  
[-hsmLabel <string>]
```

```
save configuration
```

```
initHSM
```

FIPS 初始化级别。NetScaler 目前支持 Level-2 (FIPS 140-2)。此参数是强制性的。可能的值：
Level-2

hsmLabel

用于标识硬件安全模块 (HSM) 的标签。

最大长度：31

注意： FIPS 卡上的所有数据都将通过上述命令擦除。

将 HSM 密码存储在安全位置

HSM 密码必须按照您公司的操作规程存储在安全位置。

注意： HSM 在三次登录尝试失败后会被锁定。锁定后，它将无法运行，并且您无法更改其配置。

其他功能

本节提供了可应用于 NetScaler Web App Firewall 和 NetScaler Gateway 的配置更改示例，以提高已部署设备的安全性，并提供了有关构建多层或安全性的信息。本节还包含在使用 NetScaler 或 NetScaler Gateway 作为 SAML SP 或 SAML IdP 或两者时的配置详细信息。

有关详细信息，请参阅以下主题。

- [NetScaler Web App Firewall 安全建议](#)
- [NetScaler Gateway 安全建议](#)

NetScaler® Web App Firewall 安全建议

- 对于 RFC 合规性检查，建议将 'APPFW_RFC_BLOCK' 作为 WAF 配置文件的默认 `rfcprofile`。
- WAF 支持插入 `Samesite` cookie 属性值，并且可以通过选择 'Strict' 或 'Lax' 值将 cookie 限制为同站点或跨站点上下文。

以双臂模式部署 NetScaler

在双臂模式安装中，NetScaler 物理上位于用户和 NetScaler 保护的 Web 服务器之间。连接必须通过 NetScaler。这种安排最大限度地减少了绕过 NetScaler 的可能性。

使用“默认拒绝”策略

我们建议管理员在全局级别配置 NetScaler Web App Firewall 的“全部拒绝”策略，以阻止所有不匹配 NetScaler Web App Firewall 策略的请求。以下是用于在全局级别配置“全部拒绝”策略的示例命令集：

```
add appfw profile default_deny_profile -defaults advanced

add appfw policy default_deny_policy true default_deny_profile

bind appfw global default_deny_policy <PRIORITY>
```

注意：

优先级设置必须确保默认策略最后被评估（仅当请求不匹配任何其他已配置策略时）。

NetScaler 软件包含默认配置文件，例如 appfw_block，当配置后，它们会阻止不匹配 NetScaler Web App Firewall 策略的请求。运行以下命令以设置默认配置文件：

```
set appfw settings -defaultProfile appfw_block
```

NetScaler Web App Firewall – 构建多层安全

以下指南可帮助您根据环境和支持的应用程序构建多层安全。

在每个层中为 **sessionCookieName** 参数配置不同的值。

```
set appfw settings -sessionCookieName "citrix_ns_id_1"
```

第一层安全

要构建第一层安全，请执行以下操作：

- 启用缓冲区溢出、SQL 注入和跨站点脚本。
- 当应用程序对必须访问的 URL 有特定要求并需要防止强制浏览时，需要一个起始 URL。
- 如果您的应用程序期望在表单字段中输入，请启用字段格式检查。

跨站点脚本检查可能会产生误报，因为许多公司拥有大量违反同源规则的 JavaScript 增强型 Web 内容。如果您在此类站点上启用 HTML 跨站点脚本检查，则必须生成适当的例外，以使检查不会阻止合法活动。

推出第一层，查找误报，部署例外，然后进入下一层。分阶段实施有助于管理 AppFw 部署。

第二层安全

要构建第二层安全，请执行以下操作：

除了缓冲区溢出、SQL 注入和跨站点脚本之外，还在配置文件上启用签名。有 1300 多个签名。尝试仅启用适用于保护您的应用程序的签名，而不是启用所有签名规则。

推出第二层，查找误报，部署例外，然后进入下一层。分阶段实施有助于管理 NetScaler Web App Firewall 部署。

第三层安全

要构建第三层安全，请执行以下操作：

- 根据应用程序需求，在需要的高级应用程序部分启用高级配置文件安全检查，例如 CSRF 标记、Cookie 一致性和表单字段一致性。
- 高级安全检查需要更多的处理，并可能影响性能。除非您的应用程序需要高级安全性，否则您可能希望从基本配置文件开始，并根据应用程序的要求收紧安全性。

基本 NetScaler Web App Firewall 配置文件中禁用的所有安全检查都对 HTTP 响应中的对象进行操作。因此，这些安全检查对资源的要求更高。当 NetScaler Web App Firewall 执行响应端保护时，它需要记住发送给每个独立客户端的信息。例如，如果表单受 NetScaler Web App Firewall 保护，则响应中发送的表单字段信息会保留在内存中。当客户端在下一个后续请求中提交表单时，会在信息发送到 Web 服务器之前检查其不一致性。此概念称为会话化 (Sessionization)。诸如起始 URL 中的 URL 封装、Cookie 一致性、表单字段一致性和 CSRF 表单标记等安全检查都意味着会话化。这些安全检查使用的 CPU 和内存资源量与通过 NetScaler Web App Firewall 发送的请求数量呈线性增长。例如：

- 启用表单字段一致性检查：此检查用于验证客户端是否未不当地修改 Web 表单。提供和托管表单中关键信息的应用程序需要此检查。
- CSRF 表单标记检查：此检查用于表单。跨站请求伪造 (CSRF) 表单标记检查会使用唯一且不可预测的 FormID 标记受保护网站发送给用户的每个 Web 表单，然后检查用户返回的 Web 表单，以确保提供的 FormID 正确。此检查可防止跨站请求伪造攻击。如果应用程序具有基于 Web 的表单，则必须启用此检查。与某些深入分析 Web 表单的其他安全检查相比，此检查所需的 CPU 处理能力相对较少。因此，它能够处理大容量攻击，而不会严重降低受保护网站或 NetScaler Web App Firewall 本身的性能。

NetScaler Web App Firewall workflow 步骤

在 NetScaler Web App Firewall workflow 中执行以下步骤：

1. 配置安全配置文件。
2. 应用所有已知威胁的签名 - 负面模型。
3. 配置流量策略，以检测必须激活此安全配置文件的正确流量流。

您已准备好让生产流量通过系统。第一级流已完成。此外，配置学习基础结构。很多时候，客户希望在生产流量中进行学习，因此应用签名可以避免任何风险。执行以下步骤：

1. 配置学习基础结构。
2. 部署学习到的规则以进行保护。
3. 在上线之前，验证学习数据以及应用的签名。

NetScaler® Gateway 安全建议

使用“默认拒绝”策略

我们建议管理员在全局级别为 NetScaler Gateway 配置“全部拒绝”策略，并结合使用授权策略，以基于组的方式选择性地启用对资源的访问。

默认情况下，defaultAuthorizationAction 参数设置为 DENY。请验证此设置并授予每个用户明确的访问权限。您可以使用 CLI 上的 `show vpn parameter` 命令来验证此设置。要在全局级别将参数设置为拒绝所有资源，请从 CLI 运行以下命令：

```
set vpn parameter -defaultAuthorizationAction DENY
```

在服务器之间使用 TLS1.2 通信

我们建议 NetScaler Gateway 与其他服务（例如 LDAP 和 Web Interface 服务器）之间的链接使用 TLS1.2 或 TLS 1.3。不建议使用此协议的旧版本，即 TLS 1.1、TLS 1.0 以及 SSLv3 和更早版本。

使用内部网应用程序

使用 `Intranet Applications` 功能定义哪些网络由 NetScaler Gateway 插件拦截并发送到网关。以下是定义拦截的示例命令集：

```
add vpn intranetApplication intra1 ANY 10.217.0.0 -netmask 255.255.0.0  
-destPort 1-65535 -interception TRANSPARENT
```

```
bind vpn vserver v1 -intranetapp intra1
```

身份验证、授权和审计安全建议

如果 NetScaler 或 NetScaler Gateway 设备配置为 SAML SP 或 SAML IdP 或两者，请参阅文章

[<https://support.citrix.com/article/CTX316577>](https://support.citrix.com/article/CTX316577) 以获取推荐的配置详细信息。

有关 SAML 身份验证的详细信息，请参阅 [SAML 身份验证](#)。

SAML 拒绝未签名断言

将 NetScaler 配置为 SAML 服务提供商 (SP) 时，请确保 SAML 操作中的 **Reject Unsigned Assertions** 参数设置为 **ON** 或 **Strict**。

- **ON**（默认）：拒绝没有签名的断言。
- **STRICT**：确保 SAML 响应和断言都已签名。

建议：使用 **STRICT**。

注意：

- 如果您的 SAML IdP 支持同时签署 SAML 断言和 SAML 响应，则选择 **STRICT**。
- 使用 **ON** 作为最低可接受设置。

使用以下命令检查 SAML 操作中的“**拒绝未签名断言**”值：

```
show samlaction <SAML Action Name> | grep 'Reject unsigned assertion'
```

拒绝未签名断言：开启

示例配置：

```
set samlAction <SAML Action Name> -samlRejectUnsignedAssertion <STRICT | ON>
```

为 nFactor 身份验证启用 NetScaler Gateway 登录信息加密

具有 nFactor 身份验证功能的 NetScaler Gateway 设备可以在身份验证过程中加密客户端（浏览器或 SSO 应用程序）提交的登录请求字段。加密的登录请求字段提供额外的安全层，以保护用户的敏感数据不被泄露。

要使用 CLI 启用登录加密，请运行以下命令。

```
set aaa parameter [-loginEncryption (ENABLED | DISABLED)]
```

要使用 GUI 启用登录加密

1. 导航到 **安全 > AAA – 应用程序流量**。
2. 在“身份验证设置”部分下，单击“**更改身份验证 AAA 设置**”。
3. 在“**配置 AAA 参数**”页面中，在“**登录加密**”中单击“**已启用**”。

有关登录加密的更多详细信息，请参阅 [nFactor 身份验证的 NetScaler Gateway 登录信息加密](#)。

保护身份验证、授权和审计 VPN 虚拟服务器以及 NetScaler Gateway

我们建议采取以下缓解措施来保护身份验证、授权和审计 VPN 虚拟服务器以及 NetScaler Gateway：

1. 确保为 NetScaler Gateway 启用了多重身份验证，并且多重身份验证验证因子在 LDAP 因子之前。有关更多信息，请参阅 [配置多重身份验证](#)。
2. 创建一个响应器策略，仅允许针对所需 FQDN 的请求，因为某些攻击似乎是针对 NetScaler Gateway IP 地址而不是 FQDN 触发的。

```
add responder policy IP_Block "HTTP.REQ.HOSTNAME.EQ(\"<enter gateway  
FQDN here>\").NOT" DROP
```

```
bind vpn vserver <vserver name> -policy IP_Block -priority 100 -type  
REQUEST
```

3. 启用 IP 信誉。启用 IP 信誉有助于阻止来自已知恶意 IP 地址的请求，并减少攻击的影响。运行以下命令以启用 IP 信誉：

```
enable feature reputation
```

```
add responder policy policy_brute_block_ip  
"CLIENT.IP.SRC.IPREP_IS_MALICIOUS" DROP
```

```
bind vpn vserver <Gateway_vserver_name> -policy policy_brute_block_ip  
-priority 50 -gotoPriorityExpression END -type AAA_REQUEST
```

有关如何配置 IP 信誉的更多信息，请参阅 [IP 信誉](#)。

4. 在 NetScaler 上启用 reCAPTCHA。有关如何配置 reCAPTCHA 的信息，请参阅 [nFactor 身份验证的 reCAPTCHA 配置](#)。

将拆分 DNS 值配置为 REMOTE

我们建议您将 DNS 解析配置为 `REMOTE`。

您可以使用以下任一方法配置 DNS 解析：

1. `set vpn parameter splitDns REMOTE`
2. `set vpn sessionAction <action-name> splitDns REMOTE`

在 `sessionAction` 配置 `splitDns` 是可选的。如果未在 `sessionAction` 提供 `splitDns`，则网关将从 `vpn parameter` 配置中获取 `splitDns` 值。

如果 `splitDns` 在 `sessionAction` 处配置，则 `sessionAction` 配置优先于 `vpn parameter` 配置。

默认情况下，CLI 将 `vpn parameter splitDns` 设置为 `BOTH`。我们建议您将此值配置为 `REMOTE`。

NetScaler® Console 安全最佳实践

NetScaler Console 是一种集中式管理解决方案，通过为管理员提供企业范围的可见性并自动化需要在多个实例上运行的管理任务来简化操作。您可以管理和监控 NetScaler 产品，包括 NetScaler MPX、NetScaler VPX、NetScaler SDX、NetScaler CPX 和 NetScaler Gateway。您可以使用 NetScaler Console 从一个统一的控制台管理、监控和排查整个全球应用程序交付基础架构。

NetScaler Console 是一种虚拟设备，运行在 Citrix XenServer、VMware ESXi 和 Linux KVM 上。NetScaler Console 通过收集有关 Web 应用程序和虚拟桌面流量的以下详细信息来解决应用程序可见性挑战：

- 用户会话级别信息
- 网页性能数据
- 流经您站点的 NetScaler 实例的数据库信息，并提供可操作的报告。

NetScaler Console 使 IT 管理员能够在几分钟内排除故障并主动监控客户问题。

为了在部署生命周期中维护安全性，我们建议考虑以下事项：

请勿将 NetScaler Console IP 地址和 NetScaler 代理 IP 地址暴露于互联网

我们建议 NetScaler Console IP 地址和 NetScaler 代理 IP 地址不暴露给公共互联网，并部署在适当的有状态数据包检测 (SPI) 防火墙之后。

系统用户的强密码

我们建议为在 NetScaler Console 中创建的系统用户帐户使用强密码。密码复杂性要求示例如下：

- 密码长度必须至少为八个字符。
- 密码不得包含字典词或字典词的组合。
- 密码必须包含至少一个大写字母、一个大写字母、一个数字和一个特殊字符。

要使用 NetScaler Console 设置最小密码长度，请执行以下操作：

1. 导航到 **设置 > 用户和角色**。
2. 在 **用户管理** 页面中，单击右侧的 **设置**。

3. 选择 **启用密码复杂性**。
4. 在 **密码策略** 页面中，将最小密码长度指定为 8。
5. 单击 **确定**。

更改默认证书

在 NetScaler Console 的初始配置期间，会创建默认的 TLS 证书。这些证书不适用于生产部署，必须予以替换。

我们建议您将 NetScaler Console 配置为使用来自信誉良好的证书颁发机构 (CA) 的证书，或使用来自您的企业证书颁发机构的相应证书。有关更多信息，请参阅 [安装 SSL 证书](#)。

要在 NetScaler Console 上安装 SSL 证书，请执行以下操作：

1. 导航到 **设置 > 管理**。
2. 在 **SSL 设置** 下，单击 **安装 SSL 证书**。
3. 在 **在控制台上安装 SSL 证书** 页面中，选择证书和密钥文件，如果私钥已加密，则可选择指定密码。
4. 单击 **确定**。

禁用本地身份验证

当在 NetScaler Console 上配置了外部身份验证，并且作为管理员，您希望拒绝本地系统用户登录管理访问时，您必须禁用本地身份验证。有关更多信息，请参阅[启用外部身份验证](#)。

注意：

必须配置外部服务器。

要禁用本地身份验证：

1. 导航到 **设置 > 身份验证**。
2. 在 **身份验证** 页面上，单击 **设置**。
3. 在 **身份验证设置** 页面上，在 **服务器类型** 中选择 EXTERNAL。
4. 单击 **插入**，然后在 **外部服务器** 页面上，选择一个或多个身份验证服务器以进行级联。
5. 清除 **启用回退本地身份验证** 以禁用本地身份验证。
6. 单击 **确定**。

fix

This is the content for the sample heading topic. It is hidden from the main table of contents but remains accessible via links.