



Citrix Secure Web Gateway 12.1

Machine translated content

Disclaimer

本内容的正式版本为英文版。部分 Cloud Software Group 文档内容采用了机器翻译，仅供您参考。Cloud Software Group 无法控制机器翻译的内容，这些内容可能包含错误、不准确或不合适的语言。对于从英文原文翻译成任何其他语言的内容的准确性、可靠性、适用性或正确性，或者您的 Cloud Software Group 产品或服务沿用了任何机器翻译的内容，我们均不作任何明示或暗示的保证，并且适用的最终用户许可协议或服务条款或者与 Cloud Software Group 签订的任何其他协议（产品或服务与已进行机器翻译的任何文档保持一致）下的任何保证均不适用。对于因使用机器翻译的内容而引起的任何损害或问题，Cloud Software Group 不承担任何责任。

Contents

发行说明	3
支持的硬件和软件平台	3
许可要求	4
安装	9
入门使用 Citrix ADC MPX 和 VPX SWG 设备	9
在 Citrix ADC SDX 设备上开始使用 SWG 实例	12
代理模式	12
SSL 拦截	14
SSL 配置文件	15
用于 SSL 截获的 SSL 策略基础结构	23
SSL 截获证书存储	27
SSL 错误自动学习	30
用户身份管理	32
网址筛选	36
URL 列表	37
URL 模式语义	43
映射 URL 类别	44
用例：使用自定义 URL 集进行 URL 过滤	44
URL 分类	46
安全配置	57
URL 信誉分数	57
使用 ICAP 进行远程内容检查	59
与 IPS 或 NGFW 集成作为内联设备	69

分析	116
用例：使企业 Internet 接入合规且安全	117
用例：通过使用 ICAP 远程恶意软件检查，确保企业网络安全	131
操作方法文章	144
如何创建 URL 分类策略	145
如何创建 URL 列表策略	147
如何将特殊 URL 列入白名单	149
如何阻止成人类别的 Web 站点	150
系统	152
网络连接	153
AppExpert	153
SSL	154
常见问题解答	154

发行说明

April 27, 2021

Citrix Secure Web Gateway 产品的发行说明在 Citrix ADC 设备的主要发行说明中捕获。请参阅 [Citrix ADC 发行说明](#)。

支持的硬件和软件平台

April 27, 2021

Citrix Secure Web Gateway (SWG) 设备目前可作为硬件设备和虚拟设备使用。详细规格可在数据手册中找到，该数据表可在 www.citrix.com 上获得。将鼠标指针悬停在产品上，然后在网络列表中选择 **Citrix Secure Web Gateway**。

在安装 SWG 设备之前，请确保拥有正确的许可证。高可用性设置中的每台设备都需要自己的许可证。有关许可证的信息，请参阅 [许可证要求](#)。有关高可用性的信息，请参阅 [高可用性简介](#) 主题。

硬件设备 (MPX)

- Citrix SWG MPX 14020/14030/14040
- Citrix SWG MPX 14020-40G/14040-40G
- Citrix SWG MPX 14060-40S/14080-40S/14100-40S

虚拟设备 (VPX)

- Citrix SWG VPX 200
- Citrix SWG VPX 1000
- Citrix SWG VPX 3000
- Citrix SWG VPX 5000
- Citrix SWG VPX 8000
- Citrix SWG VPX 10G
- Citrix SWG VPX 15G
- Citrix SWG VPX 25G

硬件设备 (SDX)

可以在任何 SDX 平台上预配 SWG 实例,方法是安装“SDX 2-Instance Secure Web Gateway 的加载项包”许可证。在安装一个许可证的情况下,可以在 SDX 设备上预配两个 SWG 实例。您可以通过添加更多许可证在设备上预配更多 SWG 实例。有关预配 Citrix SWG 实例的详细信息,请参阅[预配 Citrix ADC 实例](#)。

许可要求

April 27, 2021

通过许可证,您可以访问 Citrix Secure Web Gateway (SWG) 设备上的一组功能。

Citrix 许可框架允许您专注于从 Citrix 产品中获得最大价值。分配许可证的过程非常简单。在 SWG 配置实用程序 (GUI) 中,您可以使用硬件序列号 (HSN) 或许可证激活码 (LAC) 来分配许可证。如果本地计算机上已存在许可证,则可以将其上传到设备。

对于所有其他功能(例如返回或重新分配许可证),您必须使用许可门户(如果愿意,也可以使用该门户进行初始许可证分配)。有关许可门户的详细信息,请参阅<http://support.citrix.com/article/CTX131110>。

可以根据您的部署的需要部分分配许可证。例如,如果您的许可证文件包含十个许可证,但您当前的要求仅为六个许可证,那么您现在可以分配六个许可证,稍后再分配其他许可证。分配的数量不能超过许可证文件中存在的许可证总数。

在使用 SWG 设备之前,应使用 GUI 或 CLI 安装以下许可证:

- **Citrix Secure Web Gateway** 许可证
 - Citrix SWG 平台许可证是使用 MPX SWG 设备以及在不同虚拟机管理程序(如 XenServer、VMware ESX、Microsoft Hyper-V 和 Linux-KVM)上部署 VPX 实例的最低要求。
 - 对于 SDX 平台,在 Citrix ADC SDX 设备上预配 Citrix SWG 实例时,必须至少有一个 SDX 10K 并发会话 SWG 附加包许可证。
- **URL** 威胁情报功能许可证。使用 URL 过滤、URL 分类和 URL 信誉评分功能需要此许可证。

必备条件

要使用硬件序列号或许可证激活码分配许可证,请执行以下操作:

- 您必须能够通过设备访问公共域。例如,设备应该能够访问 www.citrix.com。许可证分配软件在内部访问您的许可证的 Citrix 许可证门户。要访问公有域,您可以使用代理服务器或设置 DNS 服务器,然后在 Citrix ADC 设备上配置 NSIP 地址或子网 IP (SNIP) 地址。
- 您的许可证必须与硬件关联,或者您必须拥有有效的许可证激活码 (LAC)。购买许可证时,Citrix 会通过电子邮件向您的 LAC 发送。

高可用性设置中设备的许可证

您必须为高可用性 (HA) 对中的每台设备购买单独的许可证。确保两台设备上安装了相同类型的许可证。

在 Citrix ADC SDX 设备上，您可以在同一设备上的两个 SWG 实例之间配置高可用性 (HA) 设置。但是，Citrix 建议您在不同 Citrix ADC SDX 设备上的两个 SWG 实例之间配置 HA 设置。

分配和安装许可证

您可以使用 GUI 分配和安装许可证。使用 CLI 安装许可证需要将许可证复制到 `/nsconfig/license/` 目录。

使用 Citrix SWG GUI 分配您的许可

1. 在 Web 浏览器中，键入 Citrix SWG 设备的 IP 地址。
2. 在 **User Name** (用户名) 和 **Password** (密码) 中，键入管理员凭据。
3. 在 **Configuration** (配置) 选项卡上，导航到 **System** (系统) > **Licenses** (许可证)。
4. 在详细信息窗格中，单击 **Manage Licenses** (管理许可证)，单击 **Add New License** (添加新许可证)，然后选择以下选项之一：
 - **Use Serial Number** (使用序列号)。软件在内部获取设备的序列号，然后使用此号码显示您的许可证。
 - 使用许可证激活码。Citrix 将您购买的许可证的许可证激活码 (LAC) 通过电子邮件发送。在文本框中输入 LAC。

如果不希望在 Citrix ADC 设备上配置 Internet 连接，可以使用代理服务器。选择“通过代理服务器连接”，然后指定代理服务器的 IP 地址和端口。

5. 单击获取许可证。
6. 选择要用于分配许可证的许可证文件。
7. 在 **Allocate** (分配) 列中，输入要分配的许可证数。然后单击获取。
8. 单击 **重启** 使许可证生效。
9. 在 **Reboot** (重新启动) 对话框中，单击 **OK** (确定)。

使用 Citrix SWG GUI 安装许可证

1. 在 Web 浏览器中，键入 Citrix SWG 设备的 IP 地址 (例如 <http://192.168.100.1>)。
2. 在 **User Name** (用户名) 和 **Password** (密码) 中，键入管理员凭据。
3. 在 **Configuration** (配置) 选项卡上，导航到 **System** (系统) > **Licenses** (许可证)。
4. 在详细信息窗格中，单击 **Manage Licenses** (管理许可证)。

5. 单击 添加新许可证，然后选择 上传许可证文件。
6. 单击浏览。导航到许可证文件的位置，选择许可证文件，然后单击 **Open**（打开）。
7. 单击 **Reboot**（重新启动）以应用许可证。
8. 在 **Reboot**（重新启动）对话框中，单击 **OK**（确定）。

使用 Citrix SWG CLI 安装许可证

1. 使用 SSH 客户端（例如 PuTTY）打开与 Citrix SWG 设备之间的 SSH 连接。
2. 使用管理员凭据登录到该设备。
3. 切换到 shell 提示符，然后将新的许可证文件复制到 nsconfig 目录的许可证子目录中。如果子目录不存在，请在复制文件之前创建该子目录。

示例：

```
1 login: nsroot
2
3 Password: nsroot
4
5 Last login: Mon Aug 4 03:37:27 2008 from 10.102.29.9
6
7 Done
8
9 > shell
10
11 Last login: Mon Aug 4 03:51:42 from 10.103.25.64
12
13 root@ns# mkdir /nsconfig/license
14
15 root@ns# cd /nsconfig/license
16 <!--NeedCopy-->
```

将新的许可证文件复制到此目录。

注意

CLI 不会提示您重新启动设备以激活许可证。运行 **reboot -w** 命令以热重启系统，或运行 **reboot** 命令以正常重新启动系统。

验证许可的功能

在使用某项功能之前，请确保您的许可证支持该功能。

使用 **Citrix SWG GUI** 验证许可的功能

1. 在 Web 浏览器中，键入 Citrix SWG 设备的 IP 地址（例如 <http://192.168.100.1>）。
2. 在 **User Name**（用户名）和 **Password**（密码）中，键入管理员凭据。
3. 导航到 系统 > 许可证。
屏幕的每个许可功能旁边都有一个绿色复选标记。

使用 **Citrix SWG CLI** 验证许可的功能

1. 使用 SSH 客户端（例如 PuTTY）打开与 Citrix SWG 设备之间的 SSH 连接。
2. 使用管理员凭据登录到该设备。
3. 在命令提示窗口中，输入 `sh ns license` 命令以显示许可证支持的功能。

示例：

```
1 > sh license
2
3 License status:
4
5 Web Logging: NO
6
7 Surge Protection: NO
8
9 Load Balancing: YES
10
11 ...
12
13 Forward Proxy: YES
14
15 SSL 截获：是
16
17 Model Number ID: 25000
18
19 Licensing mode: Local
20
21 完成
```

启用或禁用功能

首次使用 Citrix Secure Web Gateway 设备时，必须先启用某项功能，然后才能使用该功能。如果在启用某项功能之前对其进行配置，则会显示一条警告消息。将保存配置，但在启用此功能后才会应用。

使用 **Citrix SWG GUI** 启用功能

1. 在 Web 浏览器中，键入 Citrix SWG 设备的 IP 地址（例如 <http://192.168.100.1>）。

2. 在 **User Name** (用户名) 和 **Password** (密码) 中, 键入管理员凭据。
3. 导航到 系统 > 设置 > 配置高级功能。
4. 选择要启用的功能 (例如, 转发代理、SSL 截获和 URL 过滤)。

使用 Citrix SWG CLI 启用功能

在命令提示窗口中, 键入以下命令以启用某项功能并验证配置:

```
enable feature <FeatureName>
```

```
show feature
```

以下示例说明如何启用 SSL 拦截、转发代理和 URL 过滤功能。

```
1 > enable feature forwardProxy sslinterception urlfiltering
2
3 Done
4
5 >show feature
6
7     Feature                               Acronym           Status
8
9     -----                               -
10
11 1)    Web Logging                         WL                OFF
12
13 2)    Surge Protection                   SP                OFF
14
15 ...
16
17 ...
18
19 36)   URL Filtering                       URLFiltering      ON
20
21 37)   Video Optimization                  VideoOptimization OFF
22
23 38)   Forward Proxy                       ForwardProxy       ON
24
25 39)   SSL Interception                    SSLInterception    ON
26
27 Done
28 <!--NeedCopy-->
```

注意

如果许可证密钥不可用于某项功能, 则会显示该功能的以下错误消息:

```
ERROR: feature(s) not licensed (错误: 功能未获许可)
```

安装

April 27, 2021

Citrix Secure Web Gateway (SWG) 设备必须正确安装并可供互联网访问，然后才能开始对其进行配置以保护企业安全。

有关硬件设备的安装和初始配置的信息，请参阅 [设置 SWG 硬件](#)。

不同的虚拟化平台支持 Citrix SWG 虚拟设备 (VPX)。

有关支持的虚拟机管理程序的信息以及部署 VPX 设备的说明，请参阅 [部署 Citrix ADC VPX 实例](#)。

入门使用 Citrix ADC MPX 和 VPX SWG 设备

April 27, 2021

安装硬件 (MPX) 或软件 (VPX) 设备并执行初始配置后，即可将其配置为用于接收流量的 Secure Web Gateway 设备。

重要：

- OSCP 检查需要 Internet 连接以检查证书的有效性。如果您的设备无法通过使用 NSIP 地址从 Internet 访问，则添加访问控制列表 (ACL)，以从 NSIP 地址向子网 IP (截图) 地址执行 NAT。必须可以从 Internet 访问 SNIP。例如，

```
1  add ns acl a1 ALLOW -srcIP = <NSIP> -destIP "!="  
    10.0.0.0-10.255.255.255  
2  
3  set rnat a1 -natIP <SNIP>  
4  
5  apply acls  
6  <!--NeedCopy-->
```

- 指定用于解析域名的 DNS 名称服务器。有关详细信息，请参阅 [初始配置](#)。
- 请确保设备上的日期与 NTP 服务器同步。如果日期未同步，设备将无法有效验证源服务器证书是否已过期。

要使用 Citrix SWG 设备，必须执行以下任务：

- 以显式或透明模式添加代理服务器。
- 启用 SSL 拦截。
 - 配置 SSL 配置文件。
 - 将 SSL 策略添加并绑定到代理服务器。
 - 添加和绑定 CA 证书密钥对以进行 SSL 拦截。

注意：在透明代理模式下配置的 Citrix SWG 设备只能拦截 HTTP 和 HTTPS 协议。若要绕过任何其他协议（如 telnet），必须在代理虚拟服务器上添加以下侦听策略。

虚拟服务器现在仅接受 HTTP 和 HTTPS 传入流量。

```
1 set cs vserver transparent-pxy1 PROXY * * -cltTimeout 180 -Listenpolicy  
   "CLIENT.TCP.DSTPORT.EQ(80) || CLIENT.TCP.DSTPORT.EQ(443)"`  
2 <!--NeedCopy-->
```

您可能需要配置以下功能，具体取决于您的部署：

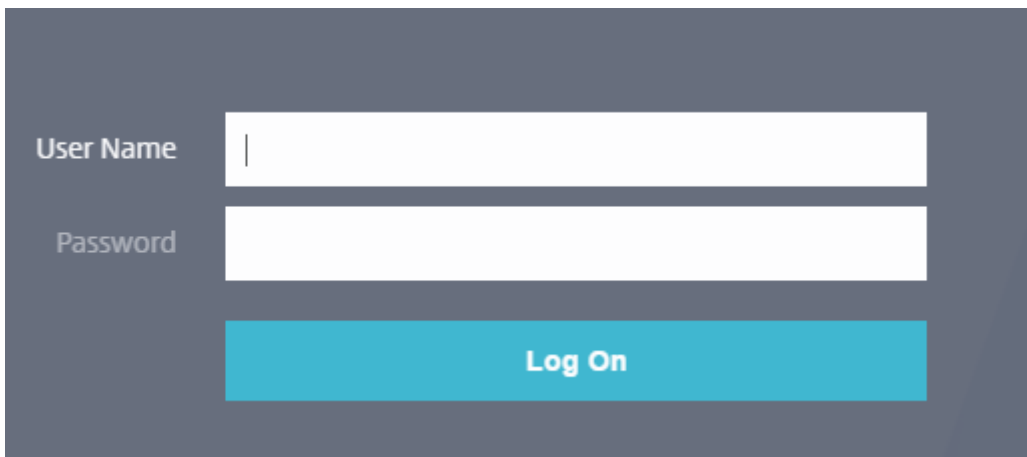
- 身份验证服务（推荐）-对用户进行身份验证。如果没有身份验证服务，则用户活动基于客户端 IP 地址。
- URL 过滤-按类别、信誉分数和 URL 列表过滤 URL。
- 分析—查看 Citrix Application Delivery Management (ADM) 中的用户活动、用户风险指标、带宽消耗和事务细分。

注意：SWG 实施了大多数典型的 HTTP 和 HTTPS 标准，其次是类似产品。这个实现是在没有特定的浏览器的情况下完成的，并且与大多数常见的浏览器兼容。SWG 已使用常见浏览器和最新版本的谷歌 Chrome、Internet Explorer 和 Mozilla Firefox 进行了测试。

Secure Web Gateway 向导

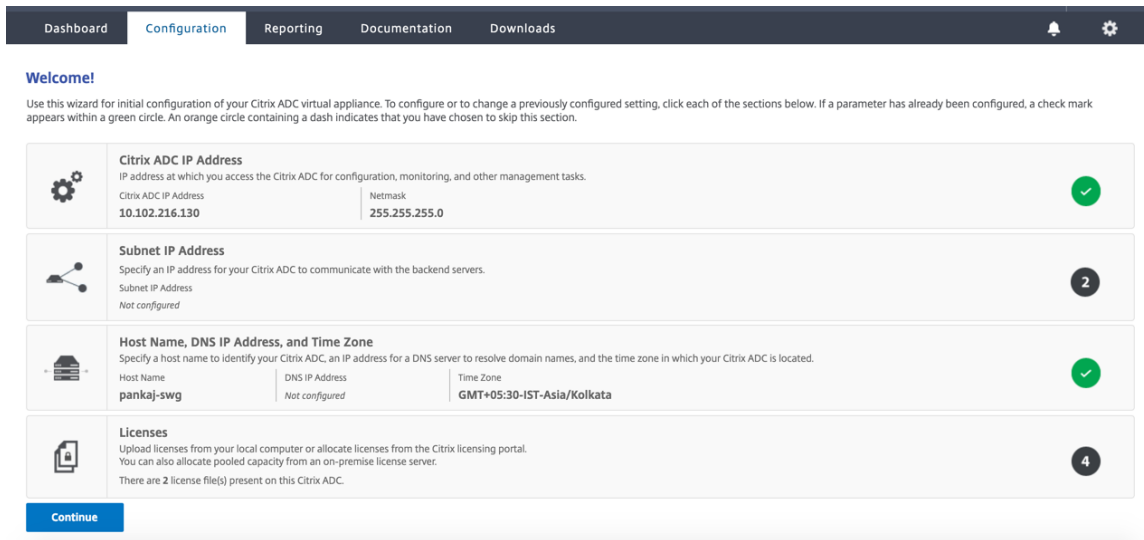
SWG 向导为管理员提供了使用 Web 浏览器管理整个 SWG 部署的工具。它有助于指导客户快速启动 SWG 服务，并通过遵循一系列明确定义的步骤来帮助简化配置。

1. 打开 Web 浏览器并输入在初始配置过程中指定的 NSIP 地址。有关初始配置的详细信息，请参阅 [初始配置](#)。
2. 键入用户名和密码。



The screenshot shows a dark gray background with a white login form. The form has two input fields: 'User Name' and 'Password'. Below the 'Password' field is a blue button with the text 'Log On' in white. The 'User Name' field has a vertical cursor on the left side.

3. 如果未指定子网 IP (SNIP) 地址，则将显示以下屏幕。

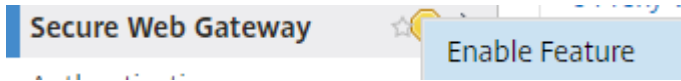


在“子网 IP 地址”中，输入 IP 地址和子网掩码。绿色圆圈中的复选标记表示该值已配置。

4. 在主机名、**DNS IP** 地址和时区中，添加 DNS 服务器的 IP 地址以解析域名，并指定您的时区。
5. 单击继续。
6. (可选) 您可能会看到感叹号，如下所示：



此标记表示该功能未启用。要启用该功能，请右键单击该功能，然后单击 启用功能。



7. 在导航窗格中，单击 **Secure Web Gateway**。在入门中，单击 **Secure Web Gateway** 向导。



8. 按照向导中的步骤配置部署。

向透明代理服务器添加侦听策略

1. 导航到 **Secure Web Gateway > Proxy Servers** (代理服务器)。选择透明代理服务器，然后单击 编辑。
2. 编辑 基本设置，然后单击 更多。
3. 在“聆听优先级”中，输入 1。

4. 在“侦听策略表达式”中，输入以下表达式：

```
1 (CLIENT.TCP.DSTPORT.EQ(80) || CLIENT.TCP.DSTPORT.EQ(443))
2 <!--NeedCopy-->
```

此表达式假定 HTTP 和 HTTPS 流量的标准端口。如果您配置了不同的端口（例如 HTTP 的 8080 或 HTTPS 的 8443），请修改表达式以反映这些端口。

限制

群集设置、管理分区和 Citrix ADC FIPS 设备不支持 SWG。

在 Citrix ADC SDX 设备上开始使用 SWG 实例

April 27, 2021

Citrix ADC SDX 设备是一种多租户平台，您可以在其中预配和管理多个虚拟 Citrix ADC 实例。SDX 设备允许单个管理员配置和管理设备，并将每个托管实例的管理委托给租户，从而满足云计算和多租户需求。SDX 设备使设备管理员能够为每个租户提供以下好处。下面给出了它们：

- 一个完整的实例。每个实例都具有以下权限：
 - 专用 CPU 和内存资源
 - 实体的单独空间
 - 自己选择的发布版本和构建的独立性
 - 生命周期独
- 一个完全隔离的网络。针对特定实例的流量仅发送到该实例。

如果尚未安装 Citrix ADC SDX 设备，请参阅[硬件安装](#)，了解有关安装设备的信息。

必须使用管理服务来执行 Citrix ADC SDX 设备的初始配置。有关详细信息，请参阅[管理服务用户界面入门](#)。

您可以按照预配 Citrix ADC VPX 实例的方式，在 Citrix ADC SDX 设备上预配 Citrix SWG 实例。要在 SDX 设备上预配 SWG 实例，需要安装“SDX-10K 并发会话 SWG 附件包”许可证。此许可证类似于 VPX 的 SDX 实例包，但是仅限于 SWG 实例。有关预配 Citrix ADC 实例的详细信息，请参阅[预配 Citrix ADC 实例](#)。

要将 Citrix SWG 实例配置为接收流量，请按照[入门使用 Citrix SWG 设备](#)中的说明进行操作。

代理模式

April 27, 2021

Citrix Secure Web Gateway (SWG) 设备用作连接到 Internet 和 SaaS 应用程序的客户端代理。作为代理，它接受所有流量并确定流量的协议。除非流量是 HTTP 或 SSL，否则流量按原样转发到目标。当设备收到来自客户端的请求时，它会拦截请求并执行一些操作，例如用户身份验证、站点分类和重定向。它使用策略来确定允许哪些流量以及要阻止哪些流量。

设备维护两个不同的会话，一个在客户端和代理之间，另一个在代理和源服务器之间。代理依赖于客户定义的策略来允许或阻止 HTTP 和 HTTPS 流量。因此，定义策略以绕过敏感数据（如财务信息）非常重要。设备提供了一套丰富的 4 层到 7 层流量属性和用户身份属性以创建流量管理策略。

对于 SSL 流量，代理验证源服务器的证书并与服务器建立合法连接。然后它模拟服务器证书，使用 Citrix SWG 上安装的 CA 证书对其进行签名，然后将创建的服务器证书呈现给客户端。您必须将 CA 证书作为受信任证书添加到客户端的浏览器，以便成功建立 SSL 会话。

设备支持透明和显式的代理模式。在显式代理模式下，客户端必须在浏览器中指定 IP 地址，除非组织将设置推送到客户端的设备上。此地址是在 SWG 设备上配置的代理服务器的 IP 地址。所有客户端请求都发送到此 IP 地址。对于显式代理，必须配置 Proxy 类型的内容交换虚拟服务器，并指定 IP 地址和有效端口号。

顾名思义，透明代理对客户端是透明的。也就是说，客户端可能不知道代理服务器正在调解他们的请求。SWG 设备是在内联部署中配置的，并以透明方式接受所有 HTTP 和 HTTPS 流量。对于透明代理，您必须配置一个内容交换虚拟服务器的 PROOPE 类型，并使用星号 (*) 作为 IP 地址和端口。在 GUI 中使用 Secure Web Gateway 向导时，无需指定 IP 地址和端口。

注意

要在透明代理模式下拦截 HTTP 和 HTTPS 以外的协议，必须添加侦听策略并将其绑定到代理服务器。

使用 Citrix SWG CLI 配置 SSL 转发代理

在命令提示符下，键入：

```
1 add cs vserver <name> PROXY <ipaddress> <port>
2 <!--NeedCopy-->
```

参数：

名称：

代理服务器的名称。必须以 ASCII 字母数字或下划线 (_) 字符开头，并且必须仅包含 ASCII 字母数字、下划线、哈希 (#)、句点 (.)、空格、冒号 (:)、位于 (@)、等于 (=) 和连字符 (-)。创建 CS 虚拟服务器后无法更改。

以下要求仅适用于 CLI：

如果名称包含一个或多个空格，请将名称用双引号或单引号括起来（例如，“我的服务器”或“我的服务器”）。

这是一个强制性的论点。最大长度：127

IP 地址：

代理服务器的 IP 地址。

端口：

代理服务器的端口号。最小值：1

显式代理示例：

```
1 add cs vserver swgVS PROXY 192.0.2.100 80
2 <!--NeedCopy-->
```

透明代理的示例：

```
1 add cs vserver swgVS PROXY * *
2 <!--NeedCopy-->
```

使用 **Citrix SWG GUI** 向透明代理服务器添加侦听策略

1. 导航到 **Secure Web Gateway > Proxy Servers** (代理服务器)。选择透明代理服务器，然后单击 **编辑**。
2. 编辑 **基本设置**，然后单击 **更多**。
3. 在“**聆听优先级**”中，输入 1。
4. 在“**侦听策略表达式**”中，输入以下表达式：

```
1 (CLIENT.TCP.DSTPORT.EQ(80) || CLIENT.TCP.DSTPORT.EQ(443))
2 <!--NeedCopy-->
```

注意

此表达式假定 HTTP 和 HTTPS 流量的标准端口。如果您配置了不同的端口，例如 HTTP 的 8080 或 HTTPS 的 8443，请修改上述表达式以指定这些端口。

SSL 拦截

April 27, 2021

为 SSL 截获配置的 Citrix Secure Web Gateway (SWG) 设备用作代理。它可以拦截和解密 SSL/TLS 流量，检查未加密的请求，并使管理员能够强制执行合规性规则和安全检查。SSL 截获使用用于指定要截获、阻止或允许的流量的策略。例如，不能截获进出财务 Web 站点的流量（例如银行），但可以截获其他流量，并且可以确定和阻止列入黑名单的站点。Citrix 建议您配置一个通用策略以拦截流量，并配置更具体的策略以绕过某些流量。

客户端和 Citrix SWG 代理建立 HTTPS/TLS 握手。SWG 代理与服务器建立另一个 HTTPS/TLS 握手并接收服务器证书。代理代表客户端验证服务器证书，并使用联机证书状态协议 (OCSP) 检查服务器证书的有效性。它会重新生成服务器证书，使用设备上安装的 CA 证书的密钥对其进行签名，然后将其呈现给客户端。因此，在客户端和 Citrix ADC 设备之间使用一个证书，在设备和后端服务器之间使用另一个证书。

重要

必须在所有客户端设备上预安装用于签署服务器证书的 CA 证书，以便客户端信任重新生成的服务器证书。

对于截获的 HTTPS 流量，SWG 代理服务器解密出站流量，访问明文 HTTP 请求，并可以使用任何第 7 层应用程序处理流量，例如通过查看纯文本 URL 以及根据公司策略和 URL 信誉允许或阻止访问。如果策略决策是允许访问源服务器，则代理服务器会将重新加密的请求转发到目标服务（在源服务器上）。代理解密来自源服务器的响应，访问明文 HTTP 响应，并有选择地将任何策略应用于响应。然后，代理会重新加密响应并将其转发给客户端。如果策略决策是阻止对源服务器的请求，则代理可以向客户端发送错误响应，例如 HTTP 403。

要执行 SSL 截获，除了以前配置的代理服务器外，还必须在 SWG 设备上配置以下各项：

- SSL 配置文件
- SSL 策略
- CA 证书存储
- SSL - 错误自动学习和缓存

SSL 配置文件

April 27, 2021

SSL 配置文件是 SSL 设置的集合，如密码和协议。如果您具有针对不同服务器的常用设置，则配置文件非常有用。您可以创建配置文件，在配置文件中指定设置，然后将配置文件绑定到不同的服务器，而不是为每个服务器指定相同的设置。如果未创建自定义前端 SSL 配置文件，则默认前端配置文件绑定到客户端实体。此配置文件允许您配置用于管理客户端连接设置的设置。对于 SSL 截获，必须创建 SSL 配置文件并在配置文件中启用 SSL 截获 (SSLi)。默认密码组绑定到此配置文件，但您可以配置更多密码以适应您的部署。必须将 SSLi CA 证书绑定到此配置文件，然后将配置文件绑定到代理服务器。对于 SSL 截获，配置文件中的基本参数是用于检查原始服务器证书的 OCSP 状态的参数，如果原始服务器请求重新协商，则触发客户端重新协商，然后在重复使用前端 SSL 会话。与源服务器通信时，必须使用默认的后端配置文件。在默认后端配置文件中设置任何服务器端参数，例如密码套件。不支持自定义后端配置文件。

有关最常用 SSL 设置的示例，请参阅本部分末尾的“示例配置文件”。

内部和外部网络的密码/协议支持不同。在下表中，用户与 SWG 设备之间的连接是内部网络。外部网络位于设备和 Internet 之间。



表 1: 内部网络的密码/协议支持列表

(密码/协议) /平台	MPX (N3)*	VPX
TLS 1.1/1.2	12.1	12.1
ECDHE/DHE (示例 TLS1-ECDHE-RSA-AES128-SHA)	12.1	12.1
AES-GCM (示例 TLS1.2-AES128-GCM-SHA256)	12.1	12.1
SHA-2 密码 (示例 TLS1.2-AES-128-SHA256)	12.1	12.1
ECDSA (示例 TLS1-ECDHE- ECDSA-AES256-SHA)	12.1	12.1

表 2: 外部网络的密码/协议支持列表

(密码/协议) /平台	MPX (N3)*	VPX
TLS 1.1/1.2	12.1	12.1
ECDHE/DHE (示例 TLS1-ECDHE-RSA-AES128-SHA)	12.1	12.1
AES-GCM (示例 TLS1.2-AES128-GCM-SHA256)	12.1	12.1
SHA-2 密码 (示例 TLS1.2-AES-128-SHA256)	12.1	12.1
ECDSA (示例 TLS1-ECDHE- ECDSA-AES256-SHA)	12.1	不支持

* 使用 **sh hardware** (show hardware) 命令确定设备是否具有 N3 芯片。

示例:

```

1 sh hardware
2
3 Platform: NSMPX-22000 16\*CPU+24\*IX+12\*E1K+2\*E1K+4*CVM N3 2200100
4
5 Manufactured on: 8/19/2013
6
7 CPU: 2900MHZ
8
9 Host Id: 1006665862
10
11 Serial no: ENUK6298FT
12
13 Encoded serial no: ENUK6298FT
14

```

```
15 Done
16 <!--NeedCopy-->
```

使用 **Citrix SWG CLI** 添加 **SSL** 配置文件并启用 **SSL** 拦截

在命令提示符下，键入：

```
add ssl profile <name> -sslinterception ENABLED -ssliReneg ( ENABLED
| DISABLED )-ssliOCSPCheck ( ENABLED | DISABLED )-ssliMaxSessPerServer
<positive_integer>
```

参数：

sslInterception:

启用或禁用对 SSL 会话的拦截。

可能的值：ENABLED、DISABLED

默认值：禁用

斯利利内斯：

从源服务器收到重新协商请求时启用或禁用触发客户端重新协商。

可能的值：ENABLED、DISABLED

默认值：ENABLED

ssliOCSPCheck:

启用或禁用 OCSP 检查原始服务器证书。

可能的值：ENABLED、DISABLED

默认值：ENABLED

ssliMaxSessPerServer:

每个动态源服务器要缓存的最大 SSL 会话数。将为客户端 Hello 消息中从客户端接收的每个 SNI 扩展创建一个唯一的 SSL 会话。匹配的会话用于服务器会话重用。

默认值：10

最小值：1

最大值：1000

示例：

```
1 add ssl profile swg_ssl_profile -sslinterception ENABLED
2
3 Done
```

```
4
5 sh ssl profile swg_ssl_profile
6
7 1) Name: swg_ssl_profile (Front-End)
8
9         SSLv3: DISABLED                TLSv1.0: ENABLED  TLSv1
          .1: ENABLED  TLSv1.2: ENABLED
10
11         Client Auth: DISABLED
12
13         Use only bound CA certificates: DISABLED
14
15         Strict CA checks:                                NO
16
17         Session Reuse: ENABLED
          Timeout: 120 seconds
18
19         DH: DISABLED
20
21         DH Private-Key Exponent Size Limit: DISABLED
          Ephemeral RSA: ENABLED
          Refresh Count: 0
22
23         Deny SSL Renegotiation
          ALL
24
25         Non FIPS Ciphers: DISABLED
26
27         Cipher Redirect: DISABLED
28
29         SSL Redirect: DISABLED
30
31         Send Close-Notify: YES
32
33         Strict Sig-Digest Check: DISABLED
34
35         Push Encryption Trigger: Always
36
37         PUSH encryption trigger timeout:                1 ms
38
39         SNI: DISABLED
40
41         OCSP Stapling: DISABLED
42
43         Strict Host Header check for SNI enabled SSL sessions:
          NO
44
45         Push flag:                0x0 (Auto)
46
47         SSL quantum size:                8 kB
48
49         Encryption trigger timeout                100 mS
50
```

```

51      Encryption trigger packet count:                45
52
53      Subject/Issuer Name Insertion Format: Unicode
54
55      SSL Interception: ENABLED
56
57      SSL Interception OCSP Check: ENABLED
58
59      SSL Interception End to End Renegotiation: ENABLED
60
61      SSL Interception Server Cert Verification for Client
        Reuse: ENABLED
62
63      SSL Interception Maximum Reuse Sessions per Server: 10
64
65      Session Ticket: DISABLED                        Session Ticket
        Lifetime: 300 (secs)
66
67      HSTS: DISABLED
68
69      HSTS IncludeSubDomains: NO
70
71      HSTS Max-Age: 0
72
73      ECC Curve: P_256, P_384, P_224, P_521
74
75 1)      Cipher Name: DEFAULT Priority :1
76
77          Description: Predefined Cipher Alias
78
79 Done
80 <!--NeedCopy-->

```

使用 **Citrix SWG CLI** 将 **SSL** 拦截 **CA** 证书绑定到 **SSL PROFILE**

在命令提示符下，键入：

```
bind ssl profile <name> -ssliCACertkey <ssli-ca-cert >
```

示例：

```

1 bind ssl profile swg_ssl_profile -ssliCACertkey swg_ca_cert
2
3 Done
4
5 sh ssl profile swg_ssl_profile
6
7 1)      Name: swg_ssl_profile (Front-End)
8
9          SSLv3: DISABLED                        TLSv1.0: ENABLED  TLSv1
        .1: ENABLED  TLSv1.2: ENABLED
10

```

```
11 Client Auth: DISABLED
12
13 Use only bound CA certificates: DISABLED
14
15 Strict CA checks: NO
16
17 Session Reuse: ENABLED
   Timeout: 120 seconds
18
19 DH: DISABLED
20
21 DH Private-Key Exponent Size Limit: DISABLED
   Ephemeral RSA: ENABLED
   Refresh Count: 0
22
23 Deny SSL Renegotiation
   ALL
24
25 Non FIPS Ciphers: DISABLED
26
27 Cipher Redirect: DISABLED
28
29 SSL Redirect: DISABLED
30
31 Send Close-Notify: YES
32
33 Strict Sig-Digest Check: DISABLED
34
35 Push Encryption Trigger: Always
36
37 PUSH encryption trigger timeout: 1 ms
38
39 SNI: DISABLED
40
41 OCSP Stapling: DISABLED
42
43 Strict Host Header check for SNI enabled SSL sessions:
   NO
44
45 Push flag: 0x0 (Auto)
46
47 SSL quantum size: 8 kB
48
49 Encryption trigger timeout 100 mS
50
51 Encryption trigger packet count: 45
52
53 Subject/Issuer Name Insertion Format: Unicode
54
55 SSL Interception: ENABLED
56
57 SSL Interception OCSP Check: ENABLED
58
```

```
59          SSL Interception End to End Renegotiation: ENABLED
60
61          SSL Interception Server Cert Verification for Client
           Reuse: ENABLED
62
63          SSL Interception Maximum Reuse Sessions per Server: 10
64
65          Session Ticket: DISABLED           Session Ticket
           Lifetime: 300 (secs)
66
67          HSTS: DISABLED
68
69          HSTS IncludeSubDomains: NO
70
71          HSTS Max-Age: 0
72
73          ECC Curve: P_256, P_384, P_224, P_521
74
75 1)          Cipher Name: DEFAULT Priority :1
76
77             Description: Predefined Cipher Alias
78
79 1)          SSL Interception CA CertKey Name: swg_ca_cert
80
81 Done
82 <!--NeedCopy-->
```

使用 Citrix SWG GUI 将 SSL 拦截 CA 证书绑定到 SSL

1. 导航到 系统 > 配置文件 > **SSL** 配置文件。
2. 单击添加。
3. 指定配置文件的名称。
4. 启用 **SSL** 会话拦截。
5. 单击确定。
6. 在“高级设置”中，单击“证书密钥”。
7. 指定要绑定到配置文件的 SSLi CA 证书密钥。
8. 单击 选择，然后单击 绑定。
9. 或者，配置密码以适合您的部署。
 - 单击编辑图标，然后单击 添加。
 - 选择一个或多个密码组，然后单击向右箭头。
 - 单击确定。
10. 单击完成。

使用 **Citrix SWG GUI** 将 **SSL** 配置文件绑定到代理服务器

1. 导航到 **Secure Web Gateway** > 代理服务器，然后添加新服务器或选择要修改的服务器。
2. 在 **SSL** 配置文件中，单击编辑图标。
3. 在 **SSL** 配置文件 列表中，选择您之前创建的 SSL 配置文件。
4. 单击确定。
5. 单击完成。

样本配置文件：

```
1 Name: swg_ssl_profile (Front-End)
2
3           SSLv3: DISABLED           TLSv1.0: ENABLED  TLSv1
           .1: ENABLED  TLSv1.2: ENABLED
4
5           Client Auth: DISABLED
6
7           Use only bound CA certificates: DISABLED
8
9           Strict CA checks:                               NO
10
11          Session Reuse: ENABLED
           Timeout: 120 seconds
12
13          DH: DISABLED
14
15          DH Private-Key Exponent Size Limit: DISABLED
           Ephemeral RSA: ENABLED
           Refresh Count: 0
16
17          Deny SSL Renegotiation
           ALL
18
19          Non FIPS Ciphers: DISABLED
20
21          Cipher Redirect: DISABLED
22
23          SSL Redirect: DISABLED
24
25          Send Close-Notify: YES
26
27          Strict Sig-Digest Check: DISABLED
28
29          Push Encryption Trigger: Always
30
31          PUSH encryption trigger timeout:                 1 ms
32
33          SNI: DISABLED
34
35          OCSP Stapling: DISABLED
36
37          Strict Host Header check for SNI enabled SSL sessions:
```

```

38                                     NO
39     Push flag:                        0x0 (Auto)
40
41     SSL quantum size:                 8 kB
42
43     Encryption trigger timeout        100 mS
44
45     Encryption trigger packet count:   45
46
47     Subject/Issuer Name Insertion Format: Unicode
48
49     SSL Interception: ENABLED
50
51     SSL Interception OCSP Check: ENABLED
52
53     SSL Interception End to End Renegotiation: ENABLED
54
55     SSL Interception Maximum Reuse Sessions per Server: 10
56
57     Session Ticket: DISABLED          Session Ticket
58     Lifetime: 300 (secs)
59
60     HSTS: DISABLED
61
62     HSTS IncludeSubDomains: NO
63
64     HSTS Max-Age: 0
65
66     ECC Curve: P_256, P_384, P_224, P_521
67 1)     Cipher Name: DEFAULT Priority :1
68
69     Description: Predefined Cipher Alias
70
71 1)     SSL Interception CA CertKey Name: swg_ca_cert
72 <!--NeedCopy-->

```

用于 SSL 截获的 SSL 策略基础结构

April 27, 2021

策略的作用类似于对传入流量进行筛选。Citrix Secure Web Gateway (SWG) 设备上的策略有助于定义如何管理代理连接和请求。处理基于为该策略配置的操作。也就是说，将连接请求中的数据与策略中指定的规则进行比较，并将操作应用于匹配规则（表达式）的连接。定义策略的操作并创建策略后，将其绑定到代理服务器，以便它应用于流经该代理服务器的流量。

SSL 截获 SSL 策略会评估传入流量，并对与规则（表达式）匹配的请求应用预定义的操作。截取、绕过或重置连接的决

定是根据定义的 SSL 策略做出的。您可以为策略配置三个操作之一-拦截、绕过或重置。在创建策略时指定操作。要使策略生效，您必须将其绑定到设备上的代理服务器。要指定策略专用于 SSL 截获，在将策略绑定到代理服务器时，必须将类型（绑定点）指定为 INTERCEPT_REQ。取消绑定策略时，必须将类型指定为 TACT_REQ。

注意：

只有在指定策略时，代理服务器才能决定拦截。

流量拦截可以基于任何 SSL 握手属性。最常用的是 SSL 域。SSL 域通常由 SSL 握手的属性表示。它可以是从 SSL 客户端 Hello 消息中提取的服务器名称指示器值（如果存在），也可以是从源服务器证书中提取的服务器备用名称 (SAN) 值。Citrix SWG 上的 SSLI 策略提供了名为 DETECTED_DOMAIN 的特殊属性，这使客户可以更轻松地根据源服务器证书中的 SSL 域制作拦截策略。客户可以将域名与字符串、URL 列表（URL 集或 `patset`）或从域派生的 URL 类别进行匹配。

使用 Citrix SWG CLI 创建 SSL 策略

在命令提示符下，键入：

```
1 add ssl policy <name> -rule <expression> -action <string>
2 <!--NeedCopy-->
```

示例：

以下示例适用于具有使用 `detected_domain` 属性检查域名的表达式的策略。

不要拦截到金融机构（如 XYZBank）的流量

```
1 add ssl policy pol1 -rule client.ssl.detected_domain.contains("XYZBANK"
) -action BYPASS
2 <!--NeedCopy-->
```

不允许用户从公司网络连接到 YouTube。

```
1 add ssl policy pol2 -rule client.ssl.client.ssl.detected_domain.
url_categorize(0,0).category.eq ("YouTube") -action RESET
2 <!--NeedCopy-->
```

拦截所有用户流量。

```
1 add ssl policy pol3 - rule true - action INTERCEPT
2 <!--NeedCopy-->
```

如果客户不想使用已检测的 `_domain`，他们可以使用任何 SSL 握手属性来提取和推断域。

例如，在客户端 `hello` 消息的 SNI 扩展中找不到域名。域名必须取自源服务器证书。以下示例适用于具有在源服务器证书的使用者名称中检查域名的表达式的策略。

拦截到任何 Yahoo 域的所有用户流量。

```
1 add ssl policy pol4 -rule client.ssl.origin_server_cert.subject.  
  contains("yahoo") - action INTERCEPT  
2 <!--NeedCopy-->
```

截获“购物/零售”类别的所有用户流量。

```
1 add ssl policy pol_url_category -rule client.ssl.origin_server_cert.  
  subject.URL_CATEGORIZE(0,0).CATEGORY.eq("Shopping/Retail") -action  
  INTERCEPT  
2 <!--NeedCopy-->
```

拦截未分类 URL 的所有用户流量。

```
1 add ssl policy pol_url_category -rule client.ssl.origin_server_cert.  
  subject.url_categorize(0,0).category.eq("Uncategorized") -action  
  INTERCEPT  
2 <!--NeedCopy-->
```

以下示例适用于将域与 URL 集中的条目匹配的策略。

如果 SNI 中的域名与 URL 集“top100”中的条目匹配，则拦截所有用户流量。

```
1 add ssl policy pol_url_set -rule client.ssl.client_hello.SNI.  
  URLSET_MATCHES_ANY("top100") -action INTERCEPT  
2 <!--NeedCopy-->
```

如果源服务器证书与 URL 集“top100”中的条目匹配，则拦截域名的所有用户流量。

```
1 add ssl policy pol_url_set -rule client.ssl.origin_server_cert.subject  
  .URLSET_MATCHES_ANY("top100") -action INTERCEPT  
2 <!--NeedCopy-->
```

使用 **SWG GUI** 为代理服务器创建 **SSL** 策略

1. 导航到 **Secure Web Gateway > SSL > 策略**。
2. 在“**SSL 策略**”选项卡上，单击“添加”并指定以下参数：
 - 策略名称
 - 策略操作—从拦截、绕过或重置中选择。
 - 表达式
3. 单击创建。

使用 **SWG CLI** 将 **SSL** 策略绑定到代理服务器

在命令提示符下，键入：

```

1 bind ssl vserver <vServerName> -policyName <string> -priority <
  positive_integer> -type INTERCEPT_REQ
2 <!--NeedCopy-->

```

示例：

```

1 bind ssl vserver <name> -policyName pol1 -priority 10 -type
  INTERCEPT_REQ
2 <!--NeedCopy-->

```

使用 Citrix SWG GUI 将 SSL 策略绑定到代理服务器

1. 导航到 **Secure Web Gateway >** 代理虚拟服务器。
2. 选择虚拟服务器，然后单击 **Edit**（编辑）。
3. 在高级设置中，单击 **SSL** 策略。
4. 在 **SSL** 策略框中单击。
5. 在“选择策略”中，选择要绑定的策略。
6. 在类型中，选择拦截 **_REQ**。
7. 单击 **绑定**，然后单击 **确定**。

使用命令行取消将 SSL 策略绑定到代理服务器

在命令提示符下，键入：

```

1 unbind ssl vserver <vServerName> -policyName <string> -type
  INTERCEPT_REQ
2 <!--NeedCopy-->

```

SWG 的 SSL 策略中使用的 SSL 表达式

表达式	说明
<code>CLIENT.SSL.CLIENT_HELLO.SNI.*</code>	以字符串格式返回 SNI 扩展名。评估字符串以查看它是否包含指定的文本。示例： <code>client.ssl.client_hello.sni.contains("xyz.com")</code>
<code>CLIENT.SSL.ORIGIN_SERVER_CERT.*</code>	返回从后端服务器接收的字符串格式的证书。评估字符串以查看它是否包含指定的文本。示例： <code>client.ssl.origin_server_cert.subject.contains("xyz.com")</code>

表达式	说明
<code>CLIENT.SSL.DETECTED_DOMAIN.*</code>	从 SNI 扩展或源服务器证书返回字符串格式的域。评估字符串以查看它是否包含指定的文本。示例： <code>client.ssl.detected_domain.contains("xyz.com")</code>

SSL 截获证书存储

April 27, 2021

SSL 证书是任何 SSL 交易的一个组成部分，是标识公司（域）或个人的数字数据表格 (X509)。SSL 证书由证书颁发机构 (CA) 颁发。CA 可以是专用的或公共的。公共 CA 颁发的证书（例如 Verisign）由执行 SSL 事务的应用程序信任。这些应用程序维护一个受信任的 CA 列表。

作为转发代理，Citrix Secure Web Gateway (SWG) 设备对客户端和服务器之间的流量执行加密和解密。它充当客户端（用户）的服务器和服务器的客户端。设备在处理 HTTPS 流量之前，必须验证服务器的身份，以防止任何欺诈事务。因此，作为源服务器的客户端，设备必须先验证原始服务器证书，然后才能接受该证书。要验证服务器的证书，设备上必须存在用于签名和颁发服务器证书的所有证书（例如，根证书和中间证书）。在设备上预安装了一组默认 CA 证书。Citrix SWG 可以使用这些证书来验证几乎所有常见的源服务器证书。无法修改此默认集。但是，如果您的部署需要更多 CA 证书，则可以创建此类证书的捆绑包并将该捆绑包导入设备。捆绑包还可以包含单个证书。

将证书捆绑导入设备时，设备会从远程位置下载该捆绑包，并在验证捆绑包是否仅包含证书后，将其安装在设备上。必须先应用证书捆绑，然后才能使用它验证服务器证书。您还可以导出证书捆绑包以进行编辑或将其作为备份存储在脱机位置。

使用 Citrix SWG CLI 在设备上导入和应用 CA 证书包

在命令提示符下，键入：

```
1 import ssl certBundle <name> <src>
2 <!--NeedCopy-->
```

```
1 apply ssl certBundle <name>
2 <!--NeedCopy-->
```

```
1 show ssl certBundle
2 <!--NeedCopy-->
```

参数：

名称:

要分配给导入的证书捆绑的名称。必须以 ASCII 字母数字或下划线 (_) 字符开头，并且必须仅包含 ASCII 字母数字、下划线、哈希 (#)、句点 (.)、空格、冒号 (:)、位于 (@)、等于 (=) 和连字符 (-)。以下要求仅适用于 CLI:

如果名称包含一个或多个空格，请将名称用双引号或单引号括起来（例如，“我的文件”或“我的文件”）。

最大长度: 31

src:

指定要导入或导出的证书捆绑包的协议、主机和路径（包括文件名）的 URL。例如 `http://www.example.com/cert_bundle_file`。

注意: 如果要导入的对象位于需要客户端证书身份验证才能访问的 HTTPS 服务器上，则导入失败。

最大长度: 2047

示例:

```
1 import ssl certbundle swg-certbundle http://www.example.com/cert_bundle
2 <!--NeedCopy-->
```

```
1 apply ssl certBundle swg-certbundle
2 <!--NeedCopy-->
```

```
1 show ssl certbundle
2
3           Name : swg-certbundle(Inuse)
4
5           URL  : http://www.example.com/cert_bundle
6
7           Done
8 <!--NeedCopy-->
```

使用 **Citrix SWG GUI** 在设备上导入和应用 **CA** 证书包

1. 导航到 **Secure Web Gateway** > 入门 > 证书捆绑包。
2. 执行以下操作之一：
 - 从列表中选择证书捆绑包。
 - 要添加新的证书捆绑包，请单击“+”并指定名称和源 URL。单击确定。
3. 单击确定。

使用 **CLI** 从设备中删除 **CA** 证书捆绑包

在命令提示符下，键入:

```
1 remove certBundle <cert bundle name>
2 <!--NeedCopy-->
```

示例:

```
1 remove certBundle mytest-cacert
2 <!--NeedCopy-->
```

使用 **Citrix SWG CLI** 从设备导出 **CA** 证书包

在命令提示符下，键入：

```
1 export certBundle <cert bundle name> <Path to export>
2 <!--NeedCopy-->
```

参数：

名称：

要分配给导入的证书捆绑的名称。必须以 ASCII 字母数字或下划线 (_) 字符开头，并且必须仅包含 ASCII 字母数字、下划线、哈希 (#)、句点 (.)、空格、冒号 (:)、位于 (@)、等于 (=) 和连字符 (-)。以下要求仅适用于 CLI：

如果名称包含一个或多个空格，请将名称用双引号或单引号括起来（例如，“我的文件”或“我的文件”）。

最大长度：31

src:

指定要导入或导出的证书捆绑包的协议、主机和路径（包括文件名）的 URL。例如 http://www.example.com/cert_bundle_file。

注意：如果要导入的对象位于需要客户端证书身份验证才能访问的 HTTPS 服务器上，则导入失败。

最大长度：2047

示例：

```
1 export certBundle mytest-cacert http://192.0.2.20/
2 <!--NeedCopy-->
```

从 **Mozilla CA** 证书存储中导入、应用和验证 **CA** 证书捆绑包

在命令提示符下，键入：

```
1 > import certbundle mozilla_public_ca https://curl.haxx.se/ca/cacert.
   pem
2 Done
3 <!--NeedCopy-->
```

要应用捆绑包，请键入：

```
1 > apply certbundle mozilla_public_ca
2 Done
3 <!--NeedCopy-->
```

要验证正在使用的证书捆绑包，请键入：

```
1 > sh certbundle | grep mozilla
2     Name : mozilla_public_ca (Inuse)
3 <!--NeedCopy-->
```

限制

群集设置中或分区的设备上不支持证书捆绑包。

SSL 错误自动学习

April 27, 2021

如果学习模式处于启用状态，Citrix SWG 设备将域添加到 SSL 绕过列表。学习模式基于从客户端或源服务器收到的 SSL 警报消息。也就是说，学习取决于发送警报消息的客户端或服务器。如果未发送警报消息，则无法学习。设备将了解是否满足以下任一条件：

1. 从服务器接收客户端证书的请求。
2. 作为握手的一部分，将收到以下任何一个警报：
 - BAD_CERTIFICATE
 - UNSUPPORTED_CERTIFICATE
 - CERTIFICATE_REVOKED
 - CERTIFICATE_EXPIRED
 - CERTIFICATE_UNKNOWN
 - UNKNOWN_CA (如果客户端使用固定，它会在收到服务器证书时发送此警报消息。)
 - HANDSHAKE_FAILURE

要启用学习，必须启用错误缓存并指定为此预留的内存。

使用 Citrix SWG GUI 启用学习

1. 导航到 **Secure Web Gateway > SSL**。
2. 在 设置中，单击 更改高级 **SSL** 设置。

3. 在 **SSL 拦截** 中，选择 **SSL 拦截错误缓存**。
4. 在 **SSL 拦截最大错误缓存内存** 中，指定要保留的内存（以字节为单位）。

5. 单击确定。

使用 **Citrix SWG CLI** 启用学习

在命令提示符下，键入：

```
set ssl parameter -ssliErrorCache ( ENABLED | DISABLED )-ssliMaxErrorCacheMem
<positive_integer>
```

参数：

缓存：

- 1 启用或禁用动态学习，并缓存学到的信息，以便后续决策拦截或绕过请求。启用后，设备将执行缓存查找以确定是否跳过请求。
- 2
- 3 可能的值：已启用、已禁用
- 4
- 5 默认值：已禁用

最大限度的误差：

- 1 指定可用于缓存学习数据的最大内存（以字节为单位）。此内存用作 LRU 缓存，以便在设定的内存限制用完之后将旧条目替换为新条目。值 0 会自动决定限制。
- 2
- 3 默认值：0
- 4
- 5 最小值：0
- 6
- 7 最大值：4294967294

用户身份管理

April 27, 2021

如果移动设备的安全漏洞越来越多，并且移动设备的普及日益增加，则需要确保使用外部 Internet 符合企业策略，并且只有获得授权的用户才可以访问由以下各项预配的外部资源企业人员。身份管理可以通过验证个人或设备的身份来实现这一点。它不确定个人可以执行哪些任务或个人可以看到哪些文件。

在允许访问 Internet 之前，Secure Web Gateway (SWG) 部署会对用户进行标识。检查用户的所有请求和响应。将记录用户活动，并将记录导出到 Citrix Application Delivery Management (ADM) 以进行报告。在 Citrix ADM 中，可以查看与用户活动、事务和带宽占用量有关的统计信息。

默认情况下，仅会保存用户的 IP 地址，但您可以将 Citrix SWG 设备配置为记录有关用户的更多详细信息，并使用此身份信息为特定用户创建更加丰富的 Internet 使用策略。

Citrix ADC 设备支持以下身份验证模式进行显式代理配置。

- **轻型目录访问协议 (LDAP)**。通过外部 LDAP 身份验证服务器对用户进行身份验证。有关详细信息，请参阅[LDAP 身份验证策略](#)。
- **RADIUS**。通过外部 RADIUS 服务器对用户进行身份验证。有关详细信息，请参阅[RADIUS 身份验证策略](#)。
- **TACACS+**。通过外部端点访问控制器访问控制系统 (TACACS) 身份验证服务器对用户进行身份验证。有关详细信息，请参阅[身份验证策略](#)。
- **谈判**。通过 Kerberos 身份验证服务器对用户进行身份验证。如果 Kerberos 身份验证中出现错误，设备将使用 NTLM 身份验证。有关详细信息，请参阅[协商身份验证策略](#)。

对于透明代理，当前仅支持基于 IP 的 LDAP 身份验证。收到客户端请求时，代理会通过检查活动目录中客户端 IP 地址的条目对用户进行身份验证，并根据用户 IP 地址创建会话。但是，如果您在 LDAP 操作中配置 SSONAME 属性，则会通过使用用户名而不是 IP 地址创建会话。透明代理设置中的身份验证不支持经典策略。

注意

对于显式代理，必须将 LDAP 登录名设置为 `sAMAccountName`。对于透明代理，必须将 LDAP 登录名称设置为 `networkAddress`，将 `attribute1` 设置为 `sAMAccountName`。

显式代理示例：

```
1 add authentication ldapAction swg-auth-action-explicit -serverIP
   10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
   CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
   frebsd123$ -ldapLoginName sAMAccountName
2 <!--NeedCopy-->
```

透明代理的示例：

```
1 add authentication ldapAction swg-auth-action-explicit -serverIP
   10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
   CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
```

```

freebsd123$ -ldapLoginName networkAddress -authentication disable -
Attribute1 sAMAccountName
2 <!--NeedCopy-->

```

使用 **Citrix SWG CLI** 设置用户身份验证

在命令提示符下，键入：

```

1 add authentication vsServer <vsServer name> SSL
2
3 bind ssl vsServer <vsServer name> -certKeyName <certkey name>
4
5 add authentication ldapAction <action name> -serverIP <ip_addr> -
  ldapBase <string> -ldapBindDn <string> -ldapBindDnPassword -
  ldapLoginName <string>
6
7 add authentication Policy <policy name> -rule <expression> -action <
  string>
8
9 bind authentication vsServer <vsServer name> -policy <string> -priority <
  positive_integer>
10
11 set cs vsServer <name> -authn401 ON -authnVsName <string>
12 <!--NeedCopy-->

```

参数：

虚拟服务器名称：

要绑定策略的身份验证虚拟服务器的名称。

最大长度：127

服务类型：

身份验证虚拟服务器的协议类型。始终是 SSL。

可能的值：SSL

默认值：SSL

操作名称：

新 LDAP 操作的名称。必须以字母、数字或下划线字符 (_) 开头，并且必须仅包含字母、数字和连字符 (-)、句点 (.) (#)、空格 ()、位于 (@)、equals (=)、冒号 (:) 和下划线字符。添加 LDAP 操作后无法更改。以下要求仅适用于 CLI：

如果名称包含一个或多个空格，请将名称括在双引号或单引号中（例如，“我的身份验证操作”或“我的身份验证操作”）。

最大长度：127

服务器 IP：

分配给 LDAP 服务器的 IP 地址。

ldapBase:

从中开始 LDAP 搜索的基数 (节点)。如果 LDAP 服务器在本地运行, 则基础的默认值为 dc = 网络扩展器, DC=com。

最大长度: 127

ldapBindDn:

用于绑定到 LDAP 服务器的完整可分辨名称 (DN)。

默认值: `cn=Manager,dc=netScaler,dc=com`

最大长度: 127

ldapBindDnPassword:

用于绑定到 LDAP 服务器的密码。

最大长度: 127

LDAPLOGO 名称:

LDAP 登录名属性。Citrix ADC 设备使用 LDAP 登录名来查询外部 LDAP 服务器或活动目录。最大长度: 127

策略名称:

高级身份验证策略的名称。必须以字母、数字或下划线字符 (_) 开头, 并且必须仅包含字母、数字和连字符 (-)、句点 (.) (#)、空格 ()、位于 (@)、equals (=)、冒号 (:) 和下划线字符。创建身份验证策略后无法更改。以下要求仅适用于 CLI:

如果名称包含一个或多个空格, 请将名称用双引号或单引号括起来 (例如, “我的身份验证策略” 或 “我的身份验证策略”)。

最大长度: 127

规则:

策略用于确定是否尝试使用身份验证服务器对用户进行身份验证的规则名称或默认语法表达式。

最大长度: 1499

操作:

策略匹配时要执行的身份验证操作的名称。

最大长度: 127

优先权:

指定策略优先级的正整数。较低的数字指定了较高的优先级。策略将按其优先级顺序进行评估, 并应用与请求匹配的最后一个策略。必须在绑定到身份验证虚拟服务器的策略列表中唯一。

最小值: 0

最大值: 4294967295

示例:

```
1 add authentication vserver swg-auth-vs SSL
2
3 Done
4
5 bind ssl vserver explicit-auth-vs -certkeyName ns-swg-ca-certkey
6
7 Done
8
9 add authentication ldapAction swg-auth-action-explicit -serverIP
  192.0.2.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "CN=
  Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword zzzzz
  -ldapLoginName sAMAccountName
10
11 Done
12
13 add authenticationpolicy swg-auth-policy -rule true -action swg-auth-
  action-explicit
14
  Done
15 bind authentication vserver swg-auth-vs -policy swg-auth-policy -
  priority 1
16
17 Done
18
19 set cs vserver testswg -authn401 ON -authnVsName swg-auth-vs
20
21 Done
22 <!--NeedCopy-->
```

使用 **Citrix SWG CLI** 启用用户名记录

在命令提示符下，键入：

```
1 set appflow param -AAAUserName ENABLED
2 <!--NeedCopy-->
```

参数：

AAAUserName

启用 AppFlow AAA 用户名记录。

可能的值：ENABLED, DISABLED

默认值：DISABLED

示例：

```
1 set appflow param -AAAUserName ENABLED
2 <!--NeedCopy-->
```

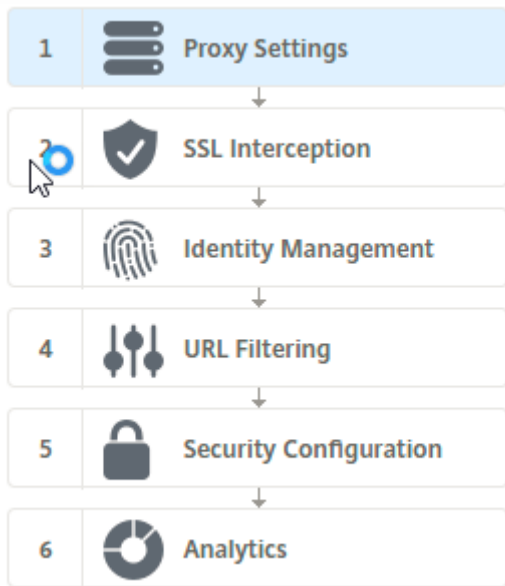
网址筛选

April 27, 2021

URL 过滤功能使用 URL 中包含的信息对 Web 站点提供基于策略的控制。此功能可帮助网络管理员监视和控制用户对网络上的恶意 Web 站点的访问。

快速入门

如果您是新用户并希望配置 URL 过滤，则必须完成初始 SWG 设置。要开始使用 URL 过滤，必须首先登录 Citrix SWG 向导。在应用 URL 筛选策略之前，向导将引导您完成一系列配置步骤。



注意

在开始之前，请确保您的设备上安装了有效的 URL 威胁智能功能许可证。如果您使用的是试用版，请务必购买有效许可证以继续在 SWG 设备上使用此功能。

登录 **SWG** 向导

Citrix SWG 向导将引导您完成一系列简化的配置任务，右窗格将显示相应的流序列。您可以使用此向导将 URL 筛选策略应用于 URL 列表或预定义类别列表。

步骤 **1**：配置代理设置

您必须首先配置代理服务器，客户端通过该服务器访问 SWG 网关。此服务器为 SSL 类型，并且在显式或透明模式下运行。有关代理服务器配置的详细信息，请参阅[代理模式](#)。

步骤 2: 配置 SSL 拦截

配置代理服务器后，必须将 SSL 拦截代理配置为在 Citrix SWG 设备上拦截加密流量。在 URL 过滤的情况下，SSL 代理会拦截流量并阻止列入黑名单的 URL，而所有其他流量都可以绕过。有关配置 SSL 截获的详细信息，请参阅 [SSL 截获](#)。

步骤 3: 配置身份管理

用户在被允许登录到企业网络之前进行身份验证。身份验证提供了根据用户角色为用户或用户组定义特定策略的灵活性。有关用户身份验证的详细信息，请参阅 [用户识别管理](#)。

步骤 4: 配置 URL 筛选

管理员可以使用 URL 分类功能或使用 URL 列表功能应用 URL 筛选策略。

URL 分类。 基于预定义类别列表过滤流量，以控制对 Web 站点和 Web 页面的访问。

URL 列表。 通过拒绝访问导入到设备中的 URL 集中的 URL，控制对列入黑名单的 Web 站点和 Web 页面的访问权限。

步骤 5: 配置安全配置

此步骤允许您配置信誉分数，并允许用户在分数过低时通过拒绝访问来控制对 Web 站点的访问。您的信誉分数可以从 1 到 4 不等，您可以配置该分数变得不可接受的阈值。对于超过阈值的分数，您可以选择允许、阻止或重定向流量的策略操作。有关详细信息，请参阅 [安全配置](#)。

步骤 6: 配置 SWG 分析

此步骤允许您激活 SWG 分析以对 Web 流量进行分类、在用户事务日志中记录 URL 类别以及查看流量分析。有关 SWG Analytics 的详细信息，请参阅 [分析](#)。

步骤 7: 单击完成以完成初始配置并继续管理 URL 过滤配置

URL 列表

April 27, 2021

通过 URL 列表功能，企业客户能够控制对特定 Web 站点和 Web 站点类别的访问权限。此功能通过应用绑定到 URL 匹配算法的响应方策略来过滤 Web 站点。此算法将传入 URL 与包含最多 1000000 个条目的 URL 集匹配。如果传入 URL 请求与集中的条目匹配，设备将使用响应程序策略评估请求 (HTTP/HTTPS) 并控制对其的访问。

网址集类型

URL 集中的每个条目都可以包含 URL 及其元数据（URL 类别、类别组或任何其他相关数据）。对于包含元数据的 URL，设备将使用一个用于评估元数据的策略表达式。有关详细信息，请参阅[网址集](#)。

Citrix SWG 支持自定义 URL 集。还可以使用模式集过滤 URL。

自定义 **URL** 集。您可以创建包含最多 1,000,000 个 URL 条目的自定义 URL 集，并将其作为文本文件导入到您的设备中。

图案集。SWG 设备可以使用模式集来过滤 URL，然后再授予对 Web 站点的访问权限。模式集是一种字符串匹配算法，用于查找传入 URL 和最多 5000 个条目之间的精确字符串匹配。有关详细信息，请参阅[图案集](#)。

导入的 URL 集中的每个 URL 都可以具有 URL 元数据形式的自定义类别。您的组织可以托管该集并将 SWG 设备配置为定期更新该集，而无需手动干预。

更新集后，Citrix ADC 设备会自动检测元数据，该类别可用作策略表达式，用于评估 URL 并应用允许、阻止、重定向或通知用户等操作。

与 URL 集一起使用的高级策略表达式

下表描述了可用于评估传入流量的基本表达式。

1. `.URLSET_MATCHES_ANY` - 如果 URL 与 URL 集中的任何条目完全匹配，则会评估为 `TRUE`。
2. `.GET_URLSET_METADATA()` - 如果 URL 与 URL 集中的任何模式完全匹配，`GET_URLSET_METADATA()` 表达式将返回关联的元数据。如果没有匹配，则返回空字符串。
3. `.GET_URLSET_METADATA().EQ(<METADATA>)` - `.GET_URLSET_METADATA().EQ(<METADATA>)`
4. `.GET_URLSET_METADATA().TYPECAST_LIST_T(',',').GET(0).EQ()` - 如果匹配的元数据位于类别的开头，则评估为 `TRUE`。此模式可用于对元数据中的单独字段进行编码，但仅匹配第一个字段。
5. `HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL)` - 加入主机和 URL 参数，然后可以将其用作匹配。

响应程序操作类型

注意：在下表中，`HTTP.REQ.URL` 通常表示为 `<URL expression>`。

下表介绍了可应用于传入的 Internet 流量的操作。

响应者操作	说明
允许	允许请求访问目标 URL。
重定向	将请求重定向到指定为目标的 URL。

响应者操作	说明
-------	----

阻止	拒绝请求。
----	-------

必备条件

如果从主机名 URL 导入 URL 集，则必须配置 DNS 服务器。如果您使用 IP 地址，则不需要此操作。

在命令提示符下，键入：

```
add dns nameServer ((<IP> [-local]) | <dnsVserverName>)[-state (
ENABLED | DISABLED )] [-type <type>] [-dnsProfileName <string>]
```

示例：

```
1 add dns nameServer 10.140.50.5
```

配置 URL 列表

要配置 URL 列表，可以使用 Citrix SWG 向导或 Citrix ADC 命令行界面 (CLI)。在 Citrix SWG 设备上，您必须首先配置响应程序策略，然后将策略绑定到 URL 集。

Citrix 建议您使用 Citrix SWG 向导作为配置 URL 列表的首选选项。使用向导将响应程序策略绑定到 URL 集。或者，您可以将策略绑定到模式集。

使用 Citrix SWG 向导配置 URL 列表

要使用 Citrix SWG GUI 配置 HTTPS 流量的 URL 列表，请执行以下操作：

1. 登录 Citrix SWG 设备并导航到 **Secure Web Gateway** 页面。
2. 在详细信息窗格中，执行以下操作之一：
 - a) 单击受保护的 **Web Gateway** 向导，以使用 URL 列表功能创建新 SWG 配置。
 - b) 选择现有配置，然后单击 **编辑**。
3. 在“**URL 过滤**”部分中，单击“**编辑**”。
4. 选中“**URL 列表**”复选框以启用该功能。
5. 选择 **URL 列表** 策略，然后单击 **绑定**。
6. 单击 **继续**，然后单击 **完成**。

有关详细信息，请参阅[如何创建 URL 列表策略](#)。

使用 Citrix SWG CLI 配置 URL 列表

要配置 URL 列表，请执行以下操作。

1. 为 HTTP 和 HTTPS 流量配置代理虚拟服务器。
2. 配置 SSL 拦截以拦截 HTTPS 流量。
3. 配置包含 HTTP 流量的 URL 集的 URL 列表。
4. 配置包含 HTTPS 流量设置的 URL 列表。
5. 配置专用 URL 集。

注意

如果您已经配置了 SWG 设备，则可以跳过步骤 1 和 2，然后使用步骤 3 进行配置。

为 **Internet** 流量配置代理虚拟服务器 Citrix SWG 设备支持透明代理虚拟服务器和显式代理虚拟服务器。要在显式模式下为 Internet 通信配置代理虚拟服务器，请执行以下操作：

1. 添加代理 SSL 虚拟服务器。
2. 将响应程序策略绑定到代理虚拟服务器。

要使用 Citrix SWG CLI 添加代理虚拟服务器，请执行以下操作：

在命令提示符下，键入：

```
1 add cs vsrver <name> <serviceType> <IPAddress> <port>
2 <!--NeedCopy-->
```

示例：

```
1 add cs vsrver starcs PROXY 10.102.107.121 80 -cltTimeout 180
2 <!--NeedCopy-->
```

要使用 Citrix SWG CLI 将响应程序策略绑定到代理虚拟服务器，请执行以下操作：

```
1 bind ssl vsrver <vServerName> -policyName <string> [-priority <
  positive_integer>]
2 <!--NeedCopy-->
```

注意

如果您已将 SSL 拦截器配置为 Citrix SWG 配置的一部分，则可以跳过以下过程。

为 **HTTPS** 流量配置 **SSL** 拦截 要为 HTTPS 流量配置 SSL 拦截，请执行以下操作：

1. 将 CA 证书密钥对绑定到代理虚拟服务器。
2. 启用默认 SSL 配置文件。
3. 创建前端 SSL 配置文件，并将其绑定到代理虚拟服务器，并在前端 SSL 配置文件中启用 SSL 拦截。

要使用 Citrix SWG CLI 将 CA 证书密钥对绑定到代理虚拟服务器，请执行以下操作：

在命令提示符下，键入：

```
1 bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>
2 <!--NeedCopy-->
```

要使用 Citrix SWG CLI 配置前端 SSL 配置文件，请执行以下操作：

在命令提示符下，键入：

```
1 set ssl parameter -defaultProfile ENABLED
2
3 add ssl profile <name> -sslInterception ENABLED -ssliMaxSessPerServer <
  positive_integer>
4 <!--NeedCopy-->
```

使用 Citrix SWG CLI 将前端 SSL 配置文件绑定到代理虚拟服务器

在命令提示符下，键入：

```
1 set ssl vserver <vServer name> -sslProfile <name>
2 <!--NeedCopy-->
```

通过导入 HTTP 流量的 URL 集来配置 URL 列表 有关如何为 HTTP 流量配置 URL 集的信息，请参阅[网址集](#)。

执行显式子域匹配 现在，您可以对导入的 URL 集执行显式子域匹配。要执行此操作，请在 **import policy URLset** 命令中添加新参数 **subdomainExactMatch**。

启用参数时，URL 筛选算法将执行显式子域匹配。例如，如果传入的 URL 为 **news.example.com**，并且 URL 集中的条目为 **example.com**，该算法将与这些 URL 不匹配。

在命令提示符下，键入：

```
import policy urlset <name> [-overwrite] [-delimiter <character>][-
rowSeparator <character>] -url [-interval <secs>] [-privateSet][-
subdomainExactMatch] [-canaryUrl <URL>]
```

示例

```
import policy urlset test -url http://10.78.79.80/top-1k.csv -privateSet
-subdomainExactMatch -interval 900
```

为 HTTPS 流量配置 URL 集 使用 Citrix SWG CLI 为 HTTPS 流量配置 URL 集

在命令提示符下，键入：

```
1 add ssl policy <name> -rule <expression> -action <string> [-undefAction
  <string>] [-comment <string>]
2 <!--NeedCopy-->
```

示例：

```
1 add ssl policy pol1 -rule "client.ssl.client_hello.SNI.
   URLSET_MATCHES_ANY("top1m") -action INTERCEPT
2 <!--NeedCopy-->
```

使用 **Citrix SWG** 向导为 **HTTPS** 流量配置 **URL 集** Citrix 建议您使用 Citrix SWG 向导作为配置 URL 列表的首选选项。使用向导导入自定义 URL 集并绑定到响应程序策略。

1. 登录 **Citrix SWG** 设备并导航到受保护的 **Web Gateway > URL 过滤 > URL 列表**。
2. 在详细信息窗格中，单击 **Add** (添加)。
3. 在“**URL 列表策略**”页面上，指定策略名称。
4. 选择一个选项以导入 URL 集。
5. 在“**URL 列表策略**”选项卡页上，选中“导入 **URL 集**”复选框并指定以下 URL 集参数。
 - a) URL 集名称-自定义 URL 集的名称。
 - b) URL—访问 URL 集的位置的 Web 地址。
 - c) 覆盖-覆盖之前导入的 URL 集。
 - d) 分隔符—用于分隔 CSV 文件记录的字符序列。
 - e) 行分隔符-CSV 文件中使用的行分隔符。
 - f) 时间间隔—更新 URL 集的时间间隔（以秒为单位），舍入到最接近的秒数（等于 15 分钟）。
 - g) 私有集—用于防止导出 URL 集的选项。
 - h) Canary URL —如果要保密的 URL 集的内容是否保密，用于测试的内部 URL。URL 的最大长度为 2047 个字符。
6. 从下拉列表中选择响应程序操作。
7. 单击创建和关闭。

配置专用 URL 集 如果您配置了专用 URL 集并保持其内容为机密，网络管理员可能不知道该集中列入黑名单的 URL。在这种情况下，您可以配置一个 Canary URL 并将其添加到 URL 集。通过使用 Canary URL，管理员可以请求将专用 URL 集用于每个查找请求。有关每个参数的说明，可以参阅向导部分。

要使用 Citrix SWG CLI 导入 URL 集，请执行以下操作：

在命令提示符下，键入：

```
1 import policy urlset <name> [-overwrite] [-delimiter <character>] [-
   rowSeparator <character>] -url <URL> [-interval <secs>] [-privateSet
   ] [-canaryUrl <URL>]
2 <!--NeedCopy-->
```

示例：

```
1 import policy urlset test1 -url http://10.78.79.80/alytra/top-1k.csv -
   private -canaryUrl http://www.in.gr
2 <!--NeedCopy-->
```

显示导入的 URL 集

除了添加的 URL 集之外，您现在可以显示导入的 URL 集。要执行此操作，请将新参数 `imported` 添加到 `show urlset` 命令中。如果启用此选项，设备将显示所有导入的 URL 集，并将导入的 URL 集与添加的 URL 集区分开来。

在命令提示符下，键入：

```
show policy urlset [<name>] [-imported]
```

示例

```
show policy urlset -imported
```

配置审核日志消息

审核日志记录使您能够在 URL 列表过程的任何阶段查看条件或情况。当 Citrix ADC 设备接收到传入 URL 时，如果响应程序策略具有 URL 集高级策略表达式，审核日志功能将收集 URL 中的 URL 集信息，并将详细信息存储为审核日志记录允许的任何目标的日志消息。

1. 日志消息包含以下信息：
2. 时间戳。
3. 日志消息类型。
4. 预定义的日志级别（严重、错误、通知、警告、信息、调试、警报和紧急）。
5. 日志消息信息，如 URLSet 名称、策略操作、URL。

要配置 URL 列表功能的审核日志记录，您必须完成以下任务：

1. 启用审核日志。
2. 创建审核日志消息操作。
3. 使用审核日志消息操作设置 URL 列表响应程序策略。

有关详细信息，请参阅 [审核日志记录](#) 主题。

URL 模式语义

April 27, 2021

下表显示了用于指定要筛选的页面列表的 URL 模式。例如，模式 `www.example.com/bar` 只匹配 `www.example.com/bar` 上的一个页面。要匹配网址以 `www.example.com/bar` 开头的所有页面，请在 URL 的末尾添加星号 (*)。

匹配元数据映射的 URL 模式语义

模式匹配语义以表格式提供。有关详细信息，请参阅 [模式语义 pdf](#) 页面。

映射 **URL** 类别

April 27, 2021

第三方类别和类别组的列表。有关详细信息，请参阅 [URL 类别映射](#) 页面。

用例：使用自定义 **URL** 集进行 **URL** 过滤

April 27, 2021

如果您是企业客户，希望能够控制对特定 Web 站点和 Web 站点类别的访问，则可以通过使用绑定到响应方策略的自定义 URL 集来完成。贵组织的网络基础结构可以使用 URL 过滤器来阻止访问恶意或危险的 Web 站点（例如，具有成人、暴力、游戏、毒品、政治或职位门户的 Web 站点）。除过滤 URL 外，您还可以创建自定义的 URL 列表并将其导入到 SWG 设备。例如，贵组织的策略可能会调用阻止访问某些 Web 站点（例如社交网络、购物门户和职位门户）。

列表中的每个 URL 都可以具有元数据形式的自定义类别。组织可以作为在 Citrix SWG 设备上设置的 URL 来托管 URL 列表，并将设备配置为定期更新设置，而无需手动干预。

更新集后，Citrix ADC 设备会自动检测元数据，响应程序策略使用 URL 元数据（类别详细信息）评估传入 URL 并应用允许、阻止、重定向或通知用户等操作。

要在网络中实现此配置，您可以执行以下任务：

1. 导入自定义 URL 集
2. 添加自定义 URL 集
3. 在 Citrix SWG 向导中配置自定义 URL 列表

要使用 **Citrix SWG CLI** 导入自定义 **URL** 集，请执行以下操作：

在命令提示符下，键入：

```
import policy urlset <name> [-overwrite] [-delimiter <character>] [-rowSeparator <character>] -  
url <URL> [-interval <secs>] [-privateSet] [-canaryUrl <URL>]
```

```
1 import policy urlset test1 -url http://10.78.79.80/alytra/top-1k.csv
```

要使用 **Citrix SWG CLI** 添加自定义 **URL** 集，请执行以下操作：

在命令提示符下，键入：

```
add urlset <urlset_name>
```

```
1 Add urlset test1
```

使用 **Citrix SWG** 向导配置 **URL** 列表

Citrix 建议您使用 Citrix SWG 向导作为配置 URL 列表的首选选项。使用向导导入自定义 URL 集并将其绑定到响应程序策略。

1. 登录 **Citrix SWG** 设备并导航到受保护的 **Web Gateway > URL 过滤 > URL** 列表。
2. 在详细信息窗格中，单击 **Add** (添加)。
3. 在“**URL 列表策略**”页面上，指定策略名称。
4. 选择一个选项以导入 URL 集。
 - a) URL 集名称-自定义 URL 集的名称。
 - b) URL—访问 URL 集的位置的 Web 地址。
 - c) 覆盖-覆盖之前导入的 URL 集。
 - d) 分隔符—用于分隔 CSV 文件记录的字符序列。
 - e) 行分隔符-CSV 文件中使用的行分隔符。
 - f) 间隔—间隔 (以秒为单位)，四舍五入到最接近的 15 分钟，在此时更新 URL 集。
 - g) 私有集—用于防止导出 URL 集的选项。
 - h) Canary URL—用于测试 URL 集的内容是否保密的内部 URL。URL 的最大长度为 2047 个字符。
6. 从下拉列表中选择响应程序操作。
7. 单击创建和关闭。

The screenshot shows the 'URL List Policy' configuration page in the Citrix SWG management console. The page has a dark header with 'URL List Policies' and 'URL List Policy' tabs. The main content area is titled 'URL List Policy' and contains several input fields and checkboxes:

- URL***: A text input field containing 'http://10.78.79.80/alytra/top-1k.csv'.
- Overwrite**: A checkbox that is currently unchecked.
- Delimiter**: A text input field containing '4'.
- Row Separator**: A text input field containing '10'.
- Interval**: A text input field containing '15'.
- Private Set**: A checkbox that is currently unchecked.
- Canary URL**: An empty text input field.

Below these fields, there is an **Action*** dropdown menu set to 'Allow'. At the bottom of the form, there are two buttons: 'Create' (in a blue box) and 'Close' (in a white box with a grey border).

自定义 URL 集的元数据语义

要导入自定义 URL 集，请将 URL 添加到文本文件中，并将其绑定到响应方策略以阻止社交网络 URL。

下面是可能会添加到文本文件中的 URL 示例：

有线电视新闻

BBC.com, 新闻

搜索引擎

搜索引擎

社交媒体

社交媒体

使用 **Citrix ADC CLI** 配置响应程序策略以阻止社交媒体 URL

```
add responder action act_url_unauthorized respondwith “HTTP/1.1 451 Unavailable For Legal Reasons\r\n\r\nURL is NOT authorized\r\n”
```

```
add responder policy pol_url_meta_match ‘HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).GET_URLSET_META(“u1” ).EQ( “Social Media” )’ act_url_meta_match
```

URL 分类

April 27, 2021

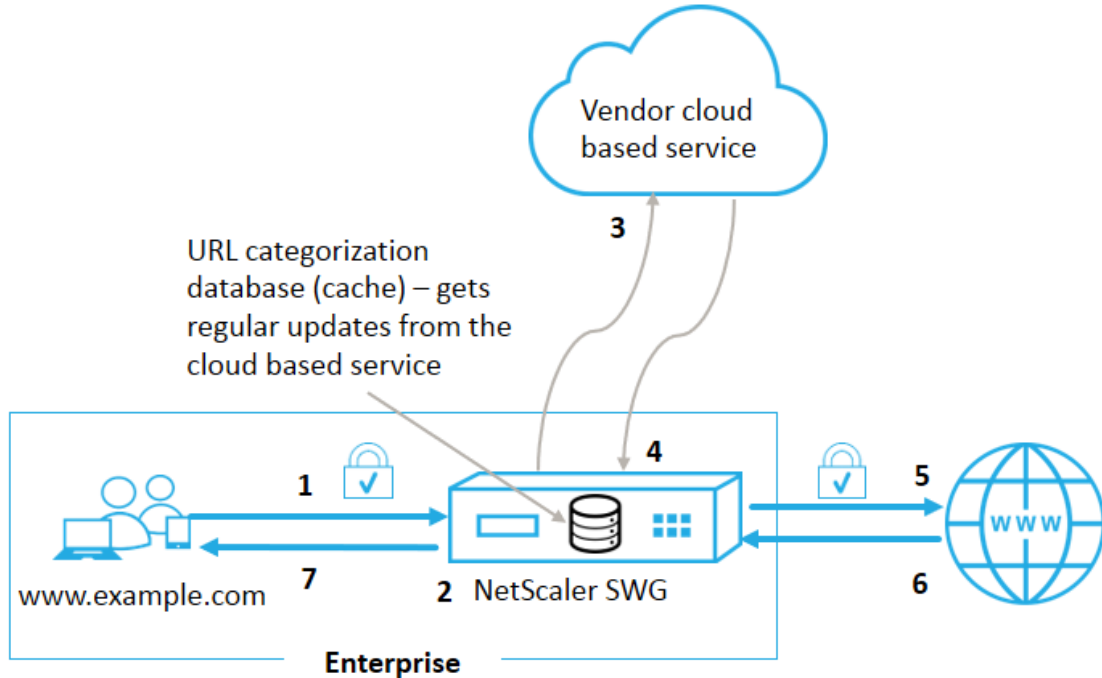
URL 分类会限制用户对特定 Web 站点和 Web 站点类别的访问权限。作为 Citrix Secure Web Gateway (SWG) 提供的订阅服务，该功能使企业客户能够使用商业分类数据库过滤 Web 流量。数据库中包含的大量（数十亿个）URL 分为不同的类别，例如社交网络、赌博、成人内容、新媒体和网上购物。除了分类之外，每个 URL 都有一个基于站点的历史风险概况保持最新的信誉评分。要筛选流量，您可以根据类别、类别组（如恐怖主义、非法药物）或站点信誉评分配置高级策略。

例如，您可能会阻止对危险站点（例如已知受恶意软件感染的站点）的访问，并有选择地限制企业用户对成人内容或娱乐流媒体等内容的访问。还可以捕获用户的事务详细信息以及用于监视 Citrix ADM 服务器上的 Web 流量分析的出站流量详细信息。

Citrix ADC 从预配置的 NetSTAR 设备 `nsv10.netstar-inc.com` 上传或下载数据，默认情况下用作云分类请求的云主机。`incompasshybridpc.netstar-inc.com` 设备使用其 NSIP 地址作为源 IP 地址，443 作为通信的目标端口。

URL 分类的工作原理

下图显示了 Citrix SWG URL 分类服务如何与商业 URL 分类数据库和云服务集成以实现频繁更新。



组件的交互方式如下：

1. 客户端发送 Internet 绑定的 URL 请求。
2. Citrix SWG 代理根据从 URL 分类数据库中检索的类别详细信息（例如类别、类别组和站点信誉评分）对请求应用策略强制执行。如果数据库返回类别详细信息，则该过程将跳转到步骤 5。
3. 如果数据库未找到分类详细信息，则请求将发送到由 URL 分类供应商维护的基于云的查找服务。但是，设备不等待响应，而是将 URL 标记为未分类并执行策略强制执行（跳转到步骤 5）。设备继续监视云查询反馈并更新缓存，以便将来的请求可以从云查找中受益。
4. SWG 设备从基于云的服务接收 URL 类别详细信息（类别、类别组和信誉评分），并将其存储在分类数据库中。
5. 策略允许 URL，请求将发送到源服务器。否则，设备会删除、重定向或使用自定义 HTML 页面进行响应。
6. 源服务器将使用请求的数据响应 SWG 设备。
7. 设备将响应发送到客户端。

用例：企业合规下的 **Internet** 使用情况

您可以使用 URL 筛选功能来检测和实施合规性策略，以阻止违反公司合规性的站点。这些站点可能是成人、流媒体、社交网络等站点，它们可能被视为非生产力或在企业网络中消耗过多的互联网带宽。阻止访问这些网站可以提高员工的生产力，降低带宽使用的运营成本，并降低网络消耗的开销。

必备条件

URL 分类功能仅在 Citrix SWG 平台具有可选订阅服务且具有适用于 Citrix Secure Web Gateway 的 URL 过滤功能和威胁情报的可选订阅服务时才能使用。订阅允许客户下载最新的 Web 站点威胁分类，然后在 Secure Web Gateway 上实施这些类别。该订阅适用于 Secure Web Gateway 的硬件设备和软件 (VPX) 版本。

在启用和配置此功能之前，必须安装以下许可证：

CNS_WEBF_SSERVER_Retail.lic

CNS_XXXXX_SERVER_SWG_Retail.lic.

其中，XXXXX 是平台类型，例如：V25000

响应程序策略表达式

下表列出了可用于验证是否必须允许、重定向或阻止传入 URL 的不同策略表达式。

1. `<text>. URL_CATEGORIZE (<min_reputation>, <max_reputation>)` -返回 URL_CATEGORY 对象。如果大<min_reputation> 于 0，则返回的对象不包含信誉低于的类别<min_reputation>。如果大<max_reputation> 于 0，则返回的对象不包含信誉高于的类别<max_reputation>。如果类别未能及时解析，则返回 undef 值。
2. `<url_category>. CATEGORY ()` -返回此对象的类别字符串。如果 URL 没有类别，或者 URL 格式不正确，则返回值为“Unknown”（未知）。
3. `<url_category>. CATEGORY_GROUP ()` -返回标识对象类别组的字符串。这是一个较高级别的类别分组，在需要较少详细的 URL 类别信息的操作中非常有用。如果 URL 没有类别，或者 URL 格式不正确，则返回值为“Unknown”（未知）。
4. `<url_category>. REPUTATION ()` -以 0 到 5 的数字形式返回信誉评分，其中 5 表示风险最高的信誉。如果分类为“未知”，则信誉值为 1。

策略类型：

1. 为搜索引擎中的 URL 类别选择请求的策略 - `add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY().EQ("Search Engine")`
2. 选择“成人”类别组中 URL 的请求的策略 - `add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY_GROUP().EQ("Adult")'`
3. 选择信誉得分低于 4 的搜索引擎 URL 请求时使用的策略 - `add responder policy p2 'HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL).URL_CATEGORIZE(4,0).HAS_CATEGORY("Search Engine")`
4. 用于选择请求搜索引擎和购物 URL 的策略 - `add responder policy p3 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY().EQ ("good_categories")`

5. 为信誉分数等于或高于 4 的搜索引擎 URL 选择请求数的策略 - `add responder policy p5 'CLIENT.SSL.DETECTED_DOMAIN.URL_CATEGORIZE(4,0).CATEGORY().EQ("Search Engines")`
6. 为搜索引擎类别中的 URL 选择请求并将其与 URL 集进行比较的策略 - `'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY().EQ("Search Engine")&& HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URLSET_MATCHES_ANY("u1")'`

响应程序策略类型

URL 分类功能中使用两种类型的策略，每种策略类型将在下面进行说明：

策略类型	说明
URL 类别	对 Web 流量进行分类，并根据评估结果阻止、允许或重定向流量。
URL 信誉分数	确定 Web 站点的信誉分数，并允许您根据管理员设置的信誉分数阈值级别控制访问。

配置 URL 分类

要在 Citrix SWG 设备上配置 URL 分类，请执行以下操作：

1. 启用 URL 筛选。
2. 为 Web 流量配置代理服务器。
3. 在显式模式下为 Web 流量配置 SSL 拦截。
4. 配置共享内存以限制缓存内存。
5. 配置 URL 分类参数。
6. 使用 Citrix SWG 向导配置 URL 分类。
7. 使用 SWG 向导配置 URL 分类参数。
8. 配置种子数据库路径和云服务器名称

步骤 1：启用 URL 筛选

要启用 URL 分类，请启用 URL 筛选功能并启用 URL 分类模式。

使用 Citrix SWG 启用 URL 分类：CLI

在命令提示符下，键入：

```
enable ns feature URLFiltering
disable ns feature URLFiltering
```

步骤 2: 在显式模式下为 **Web** 流量配置代理服务器

Citrix SWG 设备支持透明代理虚拟服务器和显式代理虚拟服务器。要在显式模式下为 SSL 流量配置代理虚拟服务器，请执行以下操作：

1. 添加代理服务器。
2. 将 SSL 策略绑定到代理服务器。

使用 Citrix SWG CLI 添加代理服务器

在命令提示符下，键入：

```
1 add cs vsver <name> [-td <positive_integer>] <serviceType> [-  
  cltTimeout <secs>]  
2 <!--NeedCopy-->
```

示例：

```
1 add cs vsver starcs PROXY 10.102.107.121 80 -cltTimeout 180  
2 <!--NeedCopy-->
```

使用 **Citrix SWG CLI** 将 **SSL** 策略绑定到代理虚拟服务器

```
1 bind ssl vsver <vServerName> -policyName <string> [-priority <  
  positive_integer>]  
2 <!--NeedCopy-->
```

步骤 3: 为 **HTTPS** 流量配置 **SSL** 拦截

要为 HTTPS 流量配置 SSL 拦截，请执行以下操作：

1. 将 CA 证书密钥对绑定到代理虚拟服务器。
2. 使用 SSL 参数配置默认 SSL 配置文件。
3. 将前端 SSL 配置文件绑定到代理虚拟服务器，并在前端 SSL 配置文件中启用 SSL 拦截。

使用 Citrix SWG CLI 将 CA 证书密钥对绑定到代理虚拟服务器

在命令提示符下，键入：

```
1 bind ssl vsver <vServerName> -certkeyName <certificate-KeyPairName> -  
  CA - skipCAName  
2 <!--NeedCopy-->
```

使用 Citrix SWG CLI 配置默认 SSL 配置文件

在命令提示符下，键入：

```
1 set ssl profile <name> -denySSLReneg <denySSLReneg> -sslInterception (
  ENABLED | DISABLED) -ssliMaxSessPerServer positive_integer>
2 <!--NeedCopy-->
```

使用 **Citrix SWG CLI** 将前端 **SSL** 配置文件绑定到代理虚拟服务器

在命令提示符下，键入：

```
1 set ssl vserver <vServer name> -sslProfile ssl_profile_interception
2 <!--NeedCopy-->
```

步骤 4：配置共享内存以限制缓存内存

使用 Citrix SWG CLI 配置共享内存以限制缓存内存

在命令提示符下，键入：

```
1 set cache parameter [-memLimit <megaBytes>]
2 <!--NeedCopy-->
```

其中，为缓存配置的内存限制设置为 10 MB。

步骤 5：配置 **URL** 分类参数

使用 Citrix SWG CLI 配置 URL 分类参数

在命令提示符下，键入：

```
1 set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer>]
  [-TimeOfDayToUpdateDB <HH:MM>]
2 <!--NeedCopy-->
```

示例：

```
1 Set urlfiltering parameter -urlfilt_hours_betweenDB_updates 20
2 <!--NeedCopy-->
```

步骤 6：使用 **Citrix SWG** 向导配置 **URL** 分类

使用 Citrix SWG GUI 配置 URL 分类

1. 登录 Citrix SWG 设备并导航到 **Secure Web Gateway** 页面。
2. 在详细信息窗格中，执行以下操作之一：
 - a) 单击 **安全 Web** 网关向导 以创建新配置。

- b) 选择现有配置，然后单击 编辑。
3. 在“URL 过滤”部分中，单击“编辑”。
4. 选中“URL 分类”复选框以启用该功能。
5. 选择 URL 分类策略，然后单击 绑定。
6. 单击 继续，然后单击 完成。

有关 URL 分类策略的详细信息，请参阅[如何创建 URL 分类策略](#)。

步骤 7：使用 SWG 向导配置 URL 分类参数

使用 Citrix SWG GUI 配置 URL 分类参数

1. 登录 Citrix SWG 设备并导航到受保护的 Web Gateway > URL 过滤。
2. 在“URL 筛选”页面中，单击“更改 URL 筛选设置”链接。
3. 在“配置 URL 筛选参数”页面中，指定以下参数。
 - a) 数据库更新之间的小时数。URL 过滤数据库更新之间的小时数。最小值：0，最大值：720。
 - b) 更新数据库的一天时间。URL 过滤一天中的时间以更新数据库。
 - c) 云主机。云服务器的 URL 路径。
 - d) 种子数据库路径。种子数据库查找服务器的 URL 路径。
4. 单击确定和关闭。

示例配置：

```
1 enable ns feature LB CS SSL IC RESPONDER AppFlow URLFiltering
2
3 enable ns mode FR L3 Edge USNIP PMTUD
4
5 set ssl profile ns_default_ssl_profile_frontend -denySSLReneg NONSECURE
   -sslInterception ENABLED -ssliMaxSessPerServer 100
6
7 add ssl certKey swg_ca_cert -cert ns_swg_ca.crt -key ns_swg_ca.key
8
9 set cache parameter -memLimit 100
10
11 add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180
12
13 add responder action act1 respondwith ""HTTP/1.1 200 OK\r\n\r\n" + http
   .req.url.url_categorize(0,0).reputation + "\n"
14
15 add responder policy p1 "HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.eq("
   Shopping/Retail") || HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.eq("
   Search Engines & Portals
16
17 ")" act1
18
```

```

19 bind cs vserver starcs_PROXY -policyName p1 -priority 10 -
    gotoPriorityExpression END -type REQUEST
20
21 add dns nameServer 10.140.50.5
22
23 set ssl parameter -denySSLReneg NONSECURE -defaultProfile ENABLED -
    sigDigestType RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-
    SHA512 -ssliErrorCache ENABLED
24
25 -ssliMaxErrorCacheMem 100000000
26
27 add ssl policy pol1 -rule "client.ssl.origin_server_cert.subject.
    URL_CATEGORIZE(0,0).CATEGORY.eq("Search Engines & Portals")" -
    action INTERCEPT
28
29 add ssl policy pol3 -rule "client.ssl.origin_server_cert.subject.ne("
    citrix)" -action INTERCEPT
30
31 add ssl policy swg_pol -rule "client.ssl.client_hello.SNI.
    URL_CATEGORIZE(0,0).CATEGORY.ne("Uncategorized")" -action INTERCEPT
32
33 set urlfiltering parameter -HoursBetweenDBUpdates 3 -
    TimeOfDayToUpdateDB 03:00
34 <!--NeedCopy-->

```

配置种子数据库路径和云服务器名称

现在，您可以配置种子数据库路径和云查找服务器名称，以便手动设置云查找服务器名称和种子数据库路径。要执行此操作，请将两个新参数 CloudHost 和 SeedDBPath 添加到 URL 过滤参数命令中。

在命令提示符下，键入：

```

set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer
>] [-TimeOfDayToUpdateDB <HH:MM>] [-LocalDatabaseThreads <positive_integer
>] [-CloudHost <string>] [-SeedDBPath <string>]

```

示例

```

set urlfiltering parameter -HoursBetweenDBUpdates 3 -TimeOfDayToUpdateDB
03:00 -CloudHost localhost -SeedDBPath /mypath

```

Citrix ADC 设备之间的通信 NetSTAR 可能需要域名服务器。您可以使用设备的简单控制台或 telnet 连接进行测试。

示例：

```

1 root@ns# telnet nsv10.netstar-inc.com 443
2 Trying 1.1.1.1...
3 Connected to nsv10.netstar-inc.com.
4 Escape character is '^]'.
5
6 root@ns# telnet incompasshybridpc.netstar-inc.com 443

```

```
7 Trying 10.10.10.10...
8 Connected to incompasshybridpc.netstar-inc.com.
9 Escape character is '^]'.
10 <!--NeedCopy-->
```

配置审核日志消息

审核日志记录使您能够在 URL 分类过程的任何阶段查看条件或情况。Citrix ADC 设备收到传入 URL 时，如果响应程序策略具有 URL 过滤表达式，则审核日志功能将在 URL 中收集 URL 集信息，并将其存储为审计日志记录允许的任何目标的日志消息。

- 源 IP 地址（发出请求的客户端的 IP 地址）。
- 目标 IP 地址（请求服务器的 IP 地址）。
- 请求的 URL 包含架构、主机和域名 (<http://www.example.com>)。
- URL 过滤框架返回的 URL 类别。
- URL 筛选框架返回的 URL 类别组。
- URL 筛选框架返回的 URL 信誉号。
- 策略执行的审核日志操作。

要配置 URL 列表功能的审核日志记录，您必须完成以下任务：

1. 启用审核日志。
2. 创建审核日志消息操作。
3. 使用审核日志消息操作设置 URL 列表响应程序策略。

有关详细信息，请参阅 [审核日志记录主题](#)。

使用 **SYSLOG** 消息传递存储失败错误

在 URL 筛选过程的任何阶段，如果出现系统级故障，Citrix ADC 设备将使用审核日志机制将日志存储在 ns.log 文件中。错误以 SYSLOG 格式存储为文本消息，以便管理员稍后可以按事件发生的时间顺序查看错误。这些日志也会发送到外部 SYSLOG 服务器进行存档。有关详细信息，请参阅[文章 CTX229399](#)。

例如，如果初始化 URL 筛选 SDK 时发生故障，错误消息将以以下消息格式存储。

```
Oct 3 15:43:40 <local0.err> ns URLFiltering[1349]: Error initializing
NetStar SDK (SDK error=-1). (status=1).
```

Citrix ADC 设备将错误消息存储在四个不同的故障类别中：

- 下载失败。如果您尝试下载分类数据库时发生错误。
- 集成失败。如果将更新集成到现有分类数据库中时发生错误。
- 初始化失败。如果初始化 URL 分类功能、设置分类参数或结束分类服务时发生错误。
- 检索失败。如果设备检索请求的分类详细信息时发生错误。

通过命令界面显示 **URL** 分类结果

通过 URL 分类，您可以输入 URL 并从 NetStar 第三方 URL 分类数据库中检索分类结果（例如类别、组和信誉评分）。

输入 URL 时，URL 过滤功能将检索并在命令界面上显示分类结果。输入更多 URL 时，设备将从列表中排除较旧的 URL，并显示最新的三个 URL 的结果。

要显示最多三个 URL 的 URL 的 URL 类别的 URL，请完成以下步骤：

1. 添加 URL 分类 URL
2. 显示最多三个 URL 的 URL 分类详细信息
3. 清除 URL 分类数据。

添加 **URL** 过滤分类 **URL**

要添加 URL 并检索其分类详细信息，请执行以下操作：

在命令提示符处键入：

```
add urlfiltering categorization -Url <string>
```

示例：

```
add urlfiltering categorization -Url www.facebook.com
```

显示最多三个 **URL** 的 **URL** 分类详细信息

在命令提示符下，键入：

```
> show urlfiltering categorization
```

示例：

```
1 show urlfiltering categorization
2 Url: http://www.facebook.com    Categorization: Facebook,Social
   Networking,1
3 Url: http://www.google.com      Categorization: Search Engines &
   Portals,Search,1
4 Url: http://www.citrix.com      Categorization: Computing & Internet,
   Computing & Internet,1
5 Done
6 <!--NeedCopy-->
```

示例配置：

```
1 add urlfiltering categorization -url www.facebook.com
2 Done
3 show urlfiltering categorization
```



```
4 Url: http://www.facebook.com    Categorization: Facebook,Social
   Networking,1
5 Done
6
7 add urlfiltering categorization -url www.google.com
8 Done
9 show urlfiltering categorization
10 Url: http://www.facebook.com    Categorization: Facebook,Social
   Networking,1
11 Url: http://www.google.com      Categorization: Search Engines &
   Portals,Search,1
12 Done
13
14 add urlfiltering categorization -url www.citrix.com
15 Done
16 show urlfiltering categorization
17 Url: http://www.facebook.com    Categorization: Facebook,Social
   Networking,1
18 Url: http://www.google.com      Categorization: Search Engines &
   Portals,Search,1
19 Url: http://www.citrix.com      Categorization: Computing & Internet,
   Computing & Internet,1
20 Done
21
22 add urlfiltering categorization -url www.in.gr
23 Done
24 show urlfiltering categorization
25 Url: http://www.google.com      Categorization: Search Engines &
   Portals,Search,1
26 Url: http://www.citrix.com      Categorization: Computing & Internet,
   Computing & Internet,1
27 Url: http://www.in.gr          Categorization: Search Engines & Portals,Search
   ,1 Done
28 <!--NeedCopy-->
```

清除 **URL** 分类结果

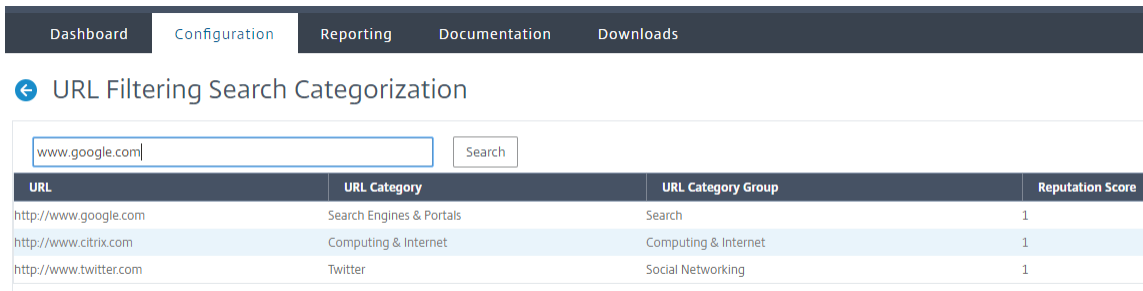
在命令提示符下，键入：

```
1 clear urlfiltering categorization
2 done
3
4 show urlfiltering categorization
5 done
6 <!--NeedCopy-->
```

通过 **GUI** 界面显示 **URL** 分类结果

1. 在“导航”窗格中，展开 **Secure Web Gateway > URL 过滤**。

2. 在详细信息窗格中，单击工具部分中的 **URL** 过滤搜索分类链接。
3. 在 **URL** 过滤搜索分类页面上，输入 URL 请求，然后单击搜索。



4. 设备将显示请求的 URL 和前两个 URL 请求的类别结果。

安全配置

April 27, 2021

通过安全配置功能，您可以配置用于过滤 URL 的安全策略。URL 信誉分数主题提供了基于其信誉分数过滤 URL 的概念性和配置性详细信息。

您可以使用 ICAP 进行远程内容检查。

URL 信誉分数

URL 分类功能使用 URL 信誉分数提供基于策略的控制，以阻止非常危险的 Web 站点。有关详细信息，请参阅[URL 信誉分数](#)。

使用 ICAP 进行远程内容检查

HTTPS 流量被拦截、解密并发送到 ICAP 服务器进行内容检查，以进行反恶意软件检查和防止数据泄漏。

URL 信誉分数

April 27, 2021

“URL 分类”功能提供了基于策略的控制以限制列入黑名单的 URL。您可以根据 URL 类别、信誉分数或 URL 类别和信誉分数来控制对 Web 站点的访问。如果网络管理员监视了访问具有非常危险的 Web 站点的用户，则他或她可以使用绑定到 URL 信誉分数的响应程序策略来阻止此类有风险的 Web 站点。

收到传入 URL 请求后, 设备将从 URL 分类数据库中检索类别和信誉评分。根据数据库返回的信誉得分, 设备会为 Web 站点分配信誉等级。值的范围为 1 到 4, 其中 4 为 riskiest 类型的 Web 站点, 如下表所示。

URL 信誉评级	声誉评论
1	清洁工地
2	未知网站
3	潜在危险或附属于危险场所
4	恶意网站

用例: 按 URL 信誉评分筛选

考虑使用网络管理员监视用户事务和网络带宽消耗的企业组织。如果恶意软件可以进入网络, 管理员必须增强数据安全性并控制对访问网络的恶意 Web 站点的访问。为了保护网络免受此类威胁, 管理员可以将 URL 筛选功能配置为允许或拒绝按 URL 信誉评分进行访问。

有关监视网络上的出站流量和用户活动的详细信息, 请参阅 [SWG 分析](#)。

如果组织的员工尝试访问社交网络 Web 站点, SWG 设备将接收 URL 请求并查询 URL 分类数据库, 以将 URL 类别检索为社交网络和信誉分数 3, 这表示潜在危险的 Web 站点。然后, 设备检查由管理员配置的安全策略, 例如阻止对信誉等级为 3 或更高的站点的访问。然后应用策略操作以控制对 Web 站点的访问。

要实施此功能, 必须使用 Citrix SWG 向导配置 URL 信誉评分和安全阈值级别。

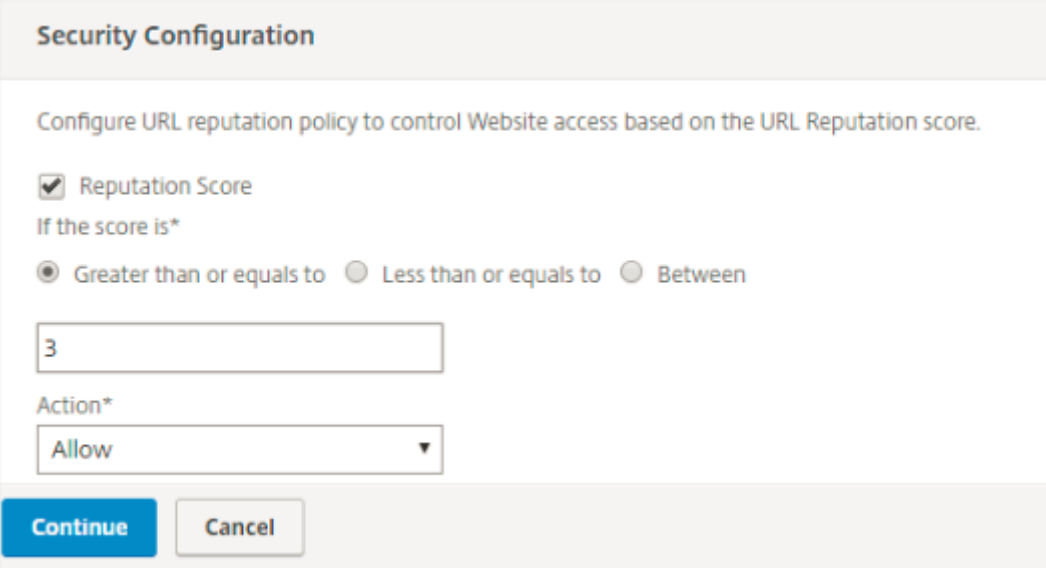
使用 **Citrix SWG GUI** 配置信誉分数:

Citrix 建议您使用 Citrix SWG 向导配置信誉评分和安全级别。根据配置的阈值, 您可以选择允许、阻止或重定向流量的策略操作。

1. 登录 **Citrix SWG** 设备并导航到 **Secure Web Gateway**。
2. 在详细信息窗格中, 单击受保护的 **Web Gateway** 向导。
3. 在 **Secure Web Gateway Configuration** (Secure Web Gateway 配置) 页面中, 指定 SWG 代理服务器设置。
4. 单击 **继续** 指定其他设置, 如 SSL 拦截和标识管理。
5. 单击 **继续** 访问安全配置部分。
6. 在“安全配置”部分中, 选择“信誉评分”复选框以根据 URL 信誉评分控制访问。
7. 选择安全级别并指定信誉评分阈值:
 - a) 大于或等于—在阈值大于或等于 N 的情况下, 允许或阻止 Web 站点, 其中 N 的范围为 1 到 4。
 - b) 小于或等于—在阈值小于或等于 N 的情况下, 允许或阻止 Web 站点, 其中 N 的范围为 1 到 4。
 - c) 介于—如果阈值介于 N1 和 N2 之间, 范围为 1 到 4, 则允许或阻止 Web 站点。
8. 从下拉列表中选择响应程序操作。

9. 单击 **继续** 并关闭。

下图显示了 Citrix SWG 向导上的“安全配置”部分。启用 URL 信誉评分选项以配置策略设置。



Security Configuration

Configure URL reputation policy to control Website access based on the URL Reputation score.

Reputation Score

If the score is*

Greater than or equals to Less than or equals to Between

3

Action*

Allow

Continue Cancel

使用 **ICAP** 进行远程内容检查

April 27, 2021

互联网内容适应协议 (ICAP) 是一种简单、轻量级的开放协议。它通常用于在代理和提供反恶意软件支持和数据泄漏防护服务的设备之间传输 HTTP 消息。会计师协会为内容调整创建了一个标准界面，以便在内容分发和提供增值服务方面具有更大的灵活性。ICAP 客户端将 HTTP 请求和响应转发到 ICAP 服务器进行处理。ICAP 服务器对请求执行一些转换，并将响应发回 ICAP 客户端，并对请求或响应采取适当的操作。

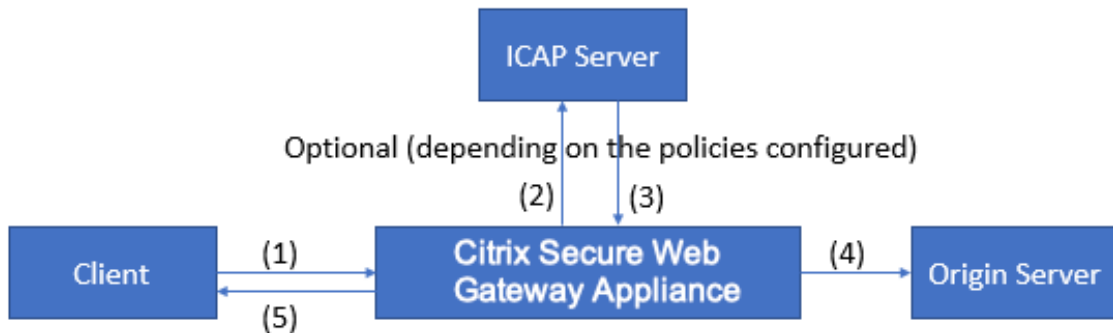
在 **Citrix Secure Web Gateway** 设备上使用 **ICAP**

注意

内容检查功能需要 SWG Edition 许可证。

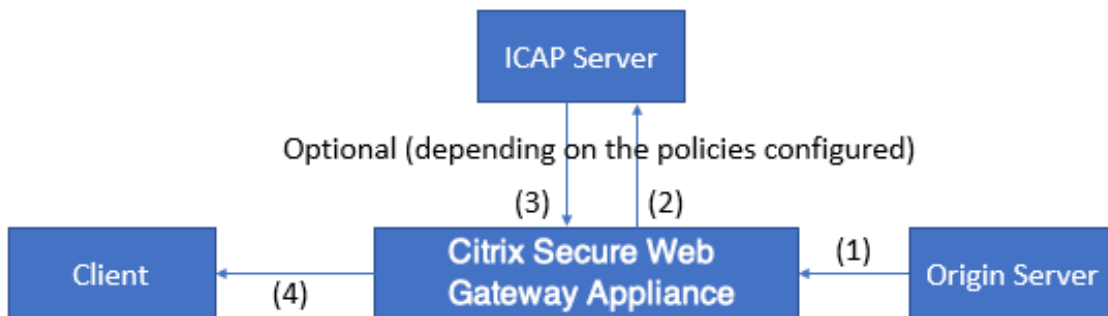
Citrix Secure Web Gateway (SWG) 设备充当 ICAP 客户端，并使用策略与 ICAP 服务器进行交互。该设备与专门从事反恶意软件和数据泄漏防护 (DLP) 等功能的第三方 ICAP 服务器进行通信。在 SWG 设备上使用 ICAP 时，也会扫描加密的文件。安全供应商之前绕过了这些文件。设备会执行 SSL 截获，对客户端流量进行解密，然后将其发送到 ICAP 服务器。ICAP 服务器会检查病毒、恶意软件或间谍软件检测、数据泄漏检查或任何其他内容适应服务。设备充当代理，解密源服务器的响应，然后将其以纯文本形式发送到 ICAP 服务器进行检查。配置策略以选择发送到 ICAP 服务器的流量。

请求模式流程的工作方式如下：



(1) Citrix SWG 设备拦截来自客户端的请求。(2) 设备根据设备上配置的策略将这些请求转发到 ICAP 服务器。(3) ICAP 服务器响应消息，指示“无需适应”、错误或已修改的请求。设备要么 (4) 将内容转发到客户端请求的源服务器，或者 (5) 向客户端返回适当的消息。

响应模式流程的工作原理如下：



(1) 源服务器响应 Citrix SWG 设备。(2) 设备根据设备上配置的策略将响应转发到 ICAP 服务器。(3) ICAP 服务器会以消息响应“无需适应”、“错误”或已修改的请求。(4) 取决于来自 ICAP 服务器的响应，设备要么将请求的内容转发给客户端，或者发送适当的消息。

在 Citrix Secure Web Gateway 设备上配置 ICAP

以下步骤说明如何在 Citrix SWG 设备上配置 ICAP。

1. 启用内容检查功能。
2. 配置代理服务器。
3. 配置代表 ICAP 服务器的 TCP 服务。要在 SWG 设备和 ICAP 服务之间建立安全连接，请将服务类型指定为 SSL_TCP。有关 secure ICAP 的详细信息，请参阅本页面后面的“保护 ICAP 安全”部分。
4. 或者，添加负载均衡虚拟服务器以对 ICAP 服务器进行负载均衡，然后将 ICAP 服务绑定到此虚拟服务器。
5. 配置自定义 ICAP 配置文件。配置文件必须包含 ICAP 服务的 URI 或服务路径以及 ICAP 模式（请求或响应）。没有类似于 HTTP 和 TCP 默认配置文件的 ICAP 默认配置文件。

6. 配置内容检查操作并指定 ICAP 配置文件名称。在服务器名称参数中指定负载平衡虚拟服务器名称或 TCP/SSL_TCP 服务名称。
7. 配置内容检查策略以评估客户端流量并将其绑定到代理服务器。在此策略中指定内容检查操作。

使用 CLI 配置 ICAP

配置以下实体：

1. 启用功能。

```
enable ns feature contentInspection
```

2. 配置代理服务器。

```
add cs vserver <name> PROXY <IPAddress>
```

示例：

```
add cs vserver explicitSWG PROXY 192.0.2.100 80
```

3. 配置 TCP 服务以表示 ICAP 服务器。

```
add service <name> <IP> <serviceType> <port>
```

将服务类型指定为 SSL_TCP，以便与 ICAP 服务器建立安全连接。

示例：

```
add service icap_svc1 203.0.113.100 TCP 1344
```

```
add service icap_svc 203.0.113.200 SSL_TCP 11344
```

4. 配置负载平衡虚拟服务器。

```
add lb vserver <name> <serviceType> <IPAddress> <port>
```

示例：

```
add lbvserver lbicap TCP 0.0.0.0 0
```

将 ICAP 服务绑定到负载平衡虚拟服务器。

```
bind lb vserver <name> <serviceName>
```

示例：

```
bind lb vserver lbicap icap_svc
```

5. 添加自定义 ICAP 配置文件。

```
add ns icapProfile <name> -uri <string> -Mode ( REQMOD | RESPMOD )
```

示例：

```
add icaprofile icaprofile1 -uri /example.com -Mode REQMOD
```

参数

名称

ICAP 配置文件的名称。必须以 ASCII 字母数字或下划线 (_) 字符开头，并且必须仅包含 ASCII 字母数字、下划线、哈希 (#)、句点 (.)、空格、冒号 (:)、at 符号 (@)、等号 (=) 和连字符 (-)。

CLI 用户：如果名称包含一个或多个空格，请将名称用双引号或单引号括起来（例如，“我的 icap 配置文件”或“我的 icap 配置文件”）。

最大长度：127

uri

表示 ICAP 服务路径的 URI。

最大长度：511 个字符

模式

ICAP 模式。可用设置功能如下：

- REQMOD：在请求修改模式下，ICAP 客户端将 HTTP 请求转发给 ICAP 服务器。
- RESPMOD：在响应修改模式下，ICAP 服务器将 HTTP 响应从源服务器转发到 ICAP 服务器。

可能的值：REQMOD、RESPMOD

6. 配置策略返回 true 时要执行的操作。

```
add contentInspection action <name> -type ICAP -serverName <string> -icapProfileName <string>
```

示例：

```
add contentInspection action CiRemoteAction -type ICAP -serverName lbicap -icapProfileName icaprofile1
```

7. 配置策略以评估流量。

```
add contentInspection policy <name> -rule <expression> -action <string>
```

示例：

```
add contentInspection policy CiPolicy -rule true -action CiRemoteAction
```

8. 将策略绑定到代理服务器。

```
bind cs vserver <vServerName> -policyName <string> -priority <positive_integer> -type [REQUEST | RESPONSE]
```

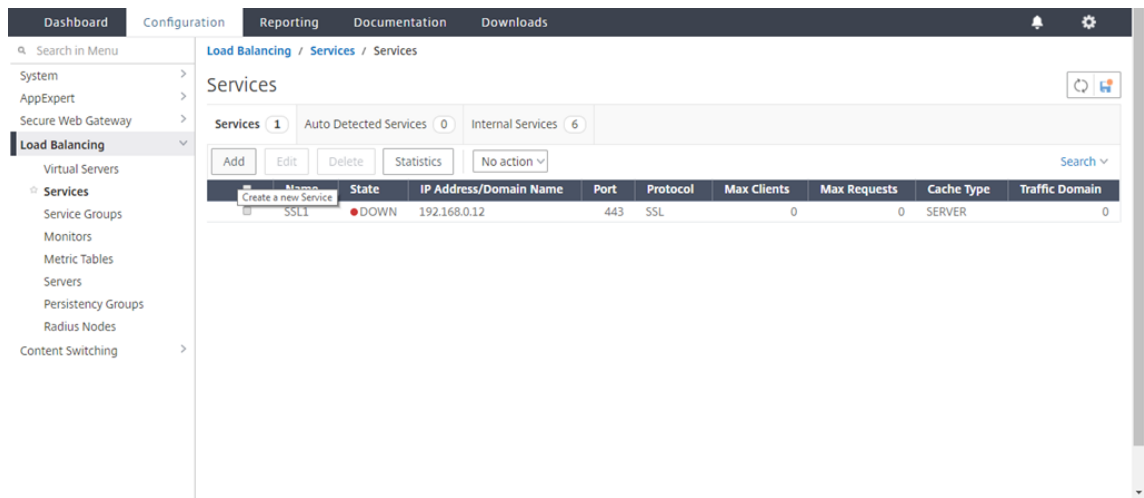
示例：

```
bind cs vserver explicitSWG -policyName CiPolicy -priority 200 -
type REQUEST
```

使用 GUI 配置 ICAP

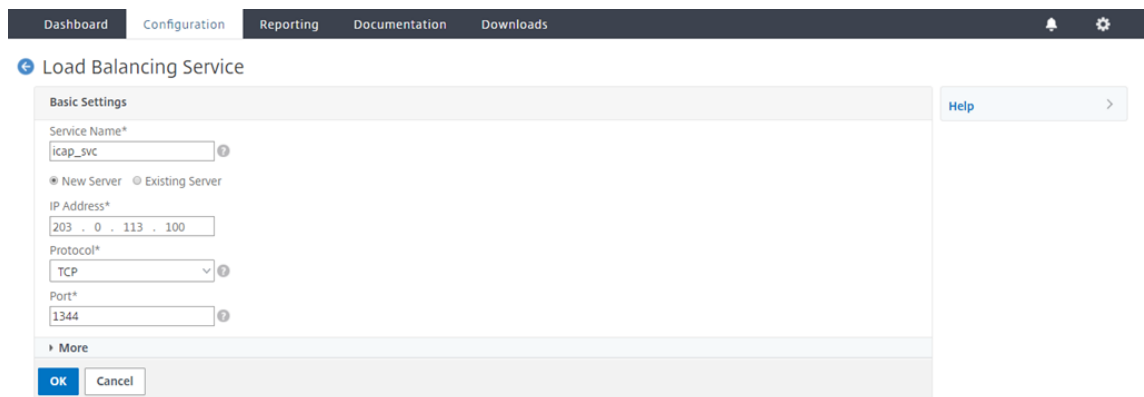
执行以下步骤：

1. 导航至“负载均衡” > “服务”，然后单击“添加”。

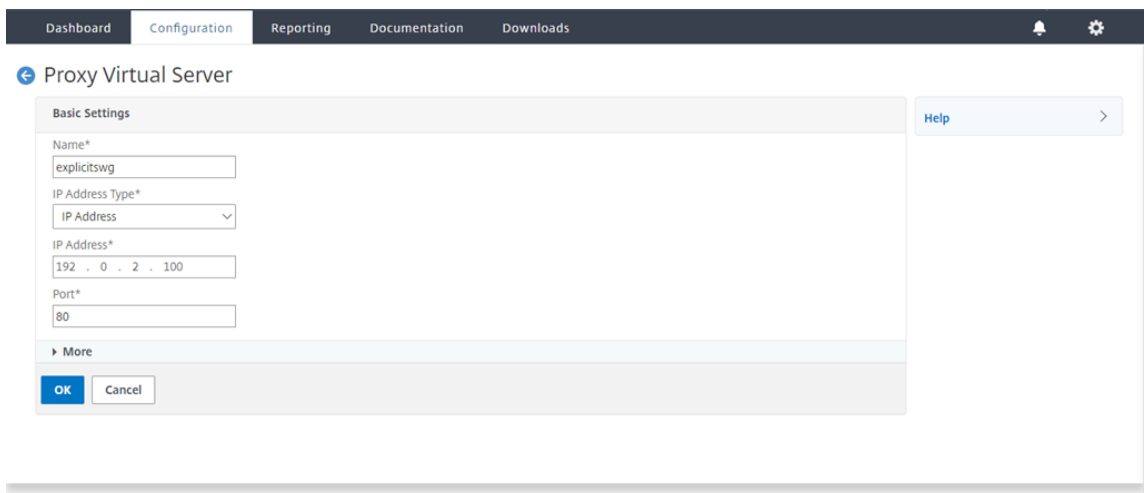


2. 键入名称和 IP 地址。在协议中，选择 **TCP**。在端口，键入 **1344**。单击确定。

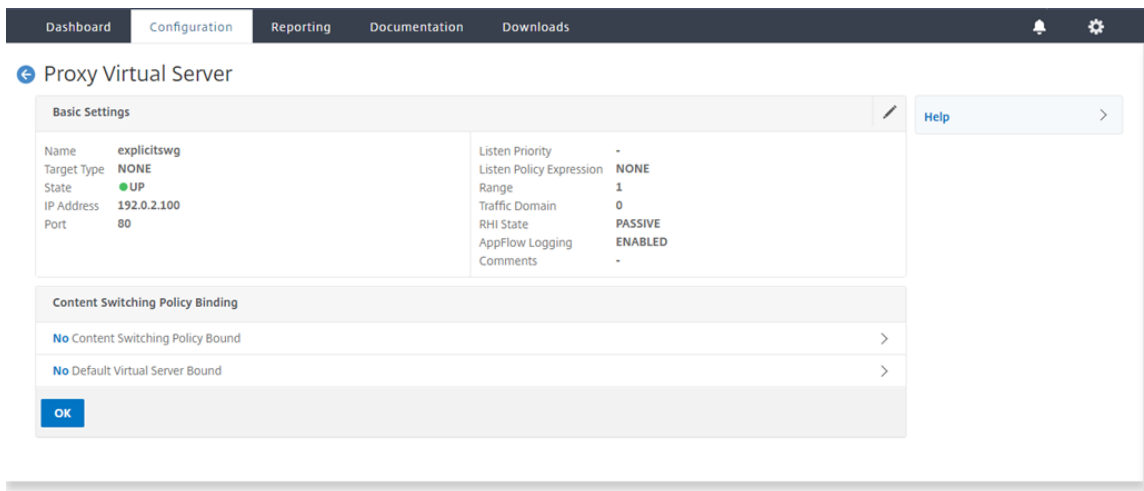
要与 ICAP 服务器的安全连接，请选择 TCP_SSL 协议并将端口指定为 11344。



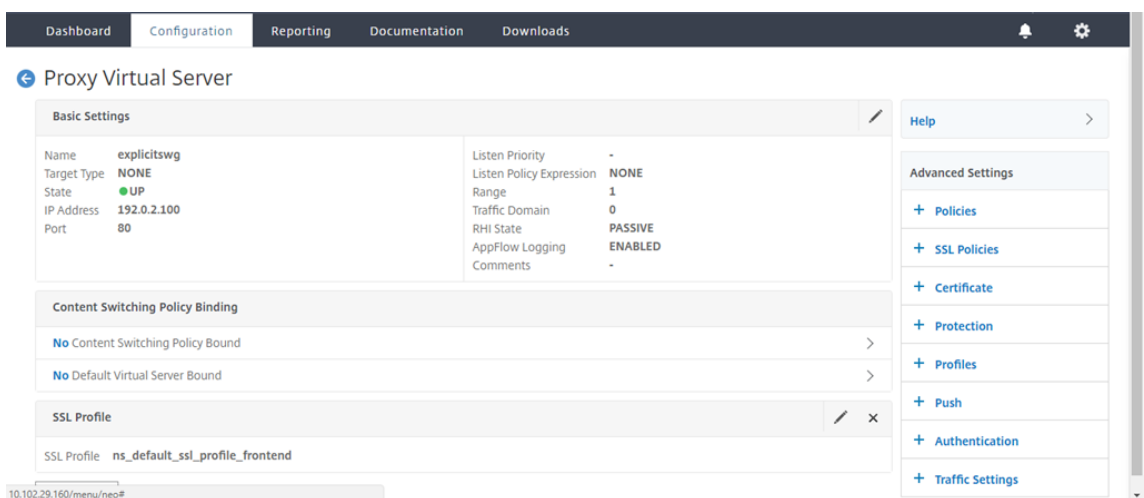
3. 导航到 **Secure Web Gateway > Proxy Virtual Servers**（代理虚拟服务器）。添加代理虚拟服务器或选择虚拟服务器，然后单击“编辑”。输入详细信息后，单击 确定。



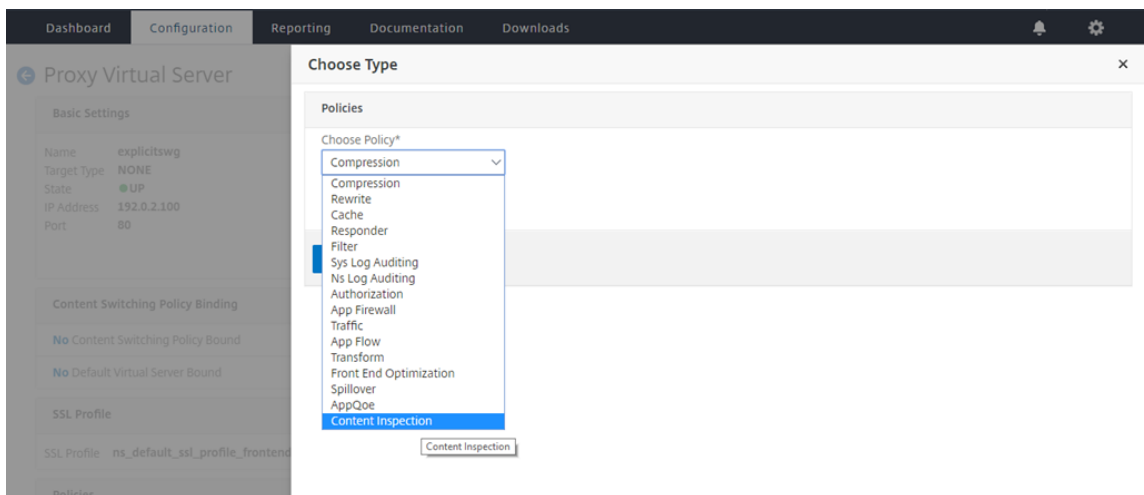
再次点击确定。



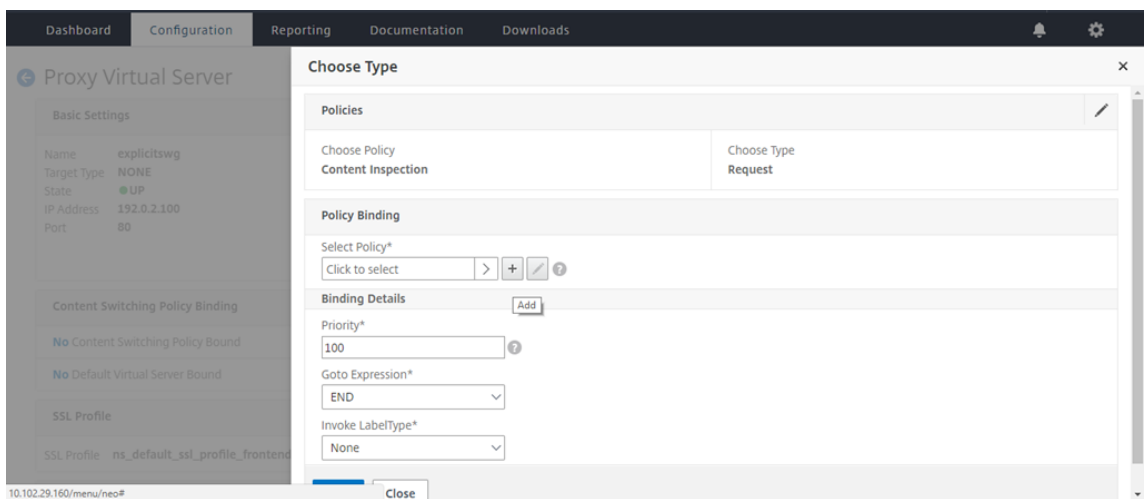
4. 在“高级设置”中，单击“策略”。



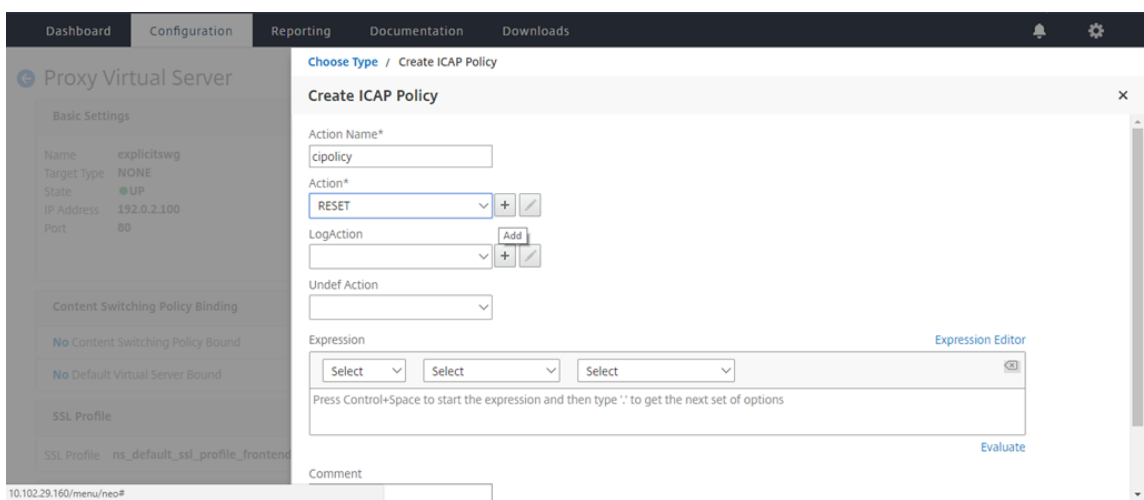
5. 在“选择策略”中，选择“内容检查”。单击继续。



6. 在选择策略中，单击“+”符号以添加策略。

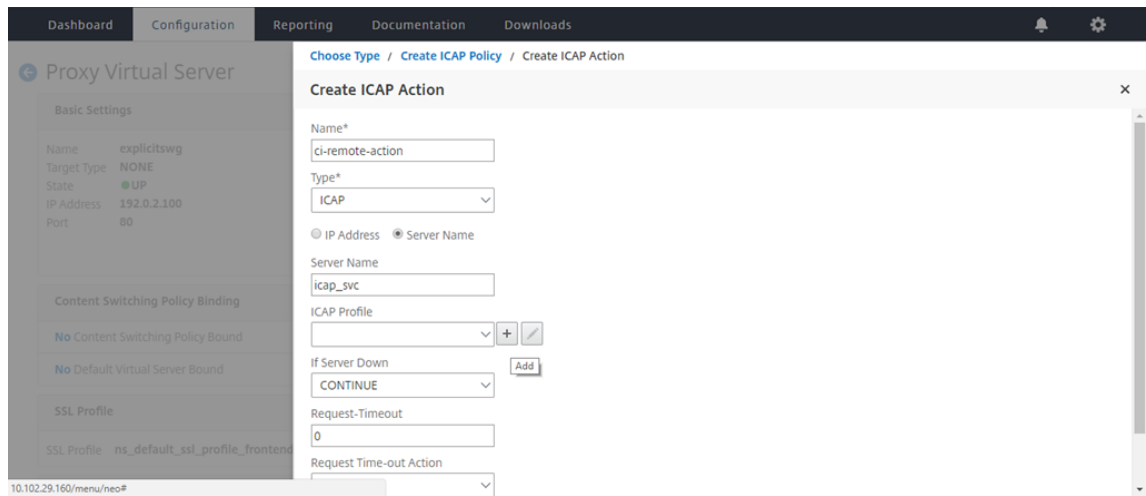


7. 输入策略的名称。在操作中，单击“+”符号以添加操作。

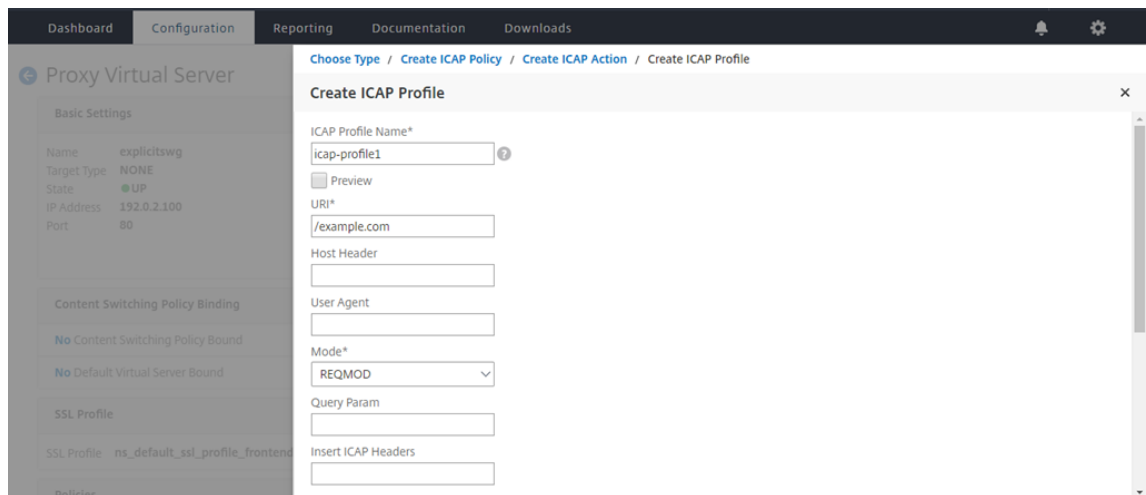


8. 键入操作的名称。在“服务器名称”中，键入之前创建的 TCP 服务的名称。在会计师事务所配置文件中，单击“+”

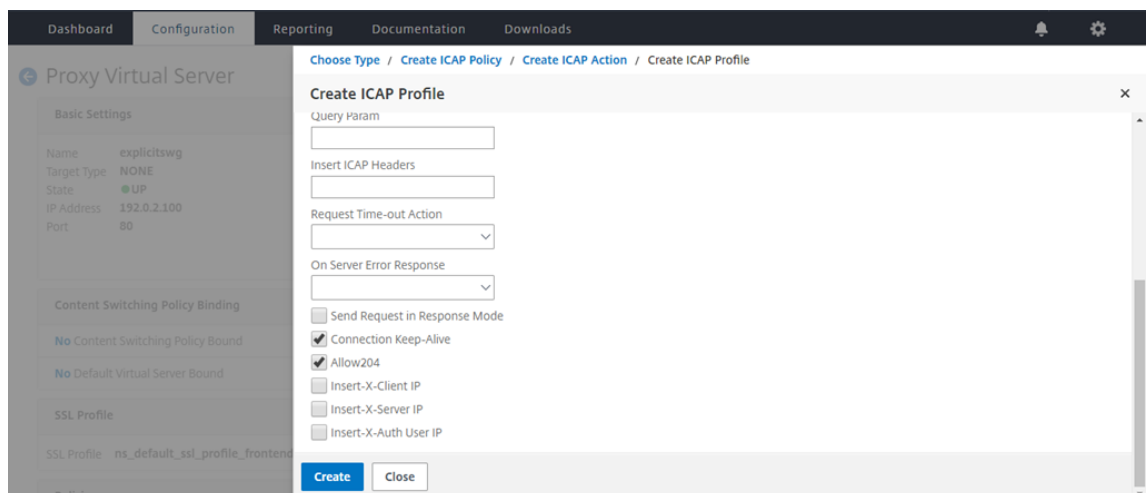
符号以添加会计师事务所配置文件。



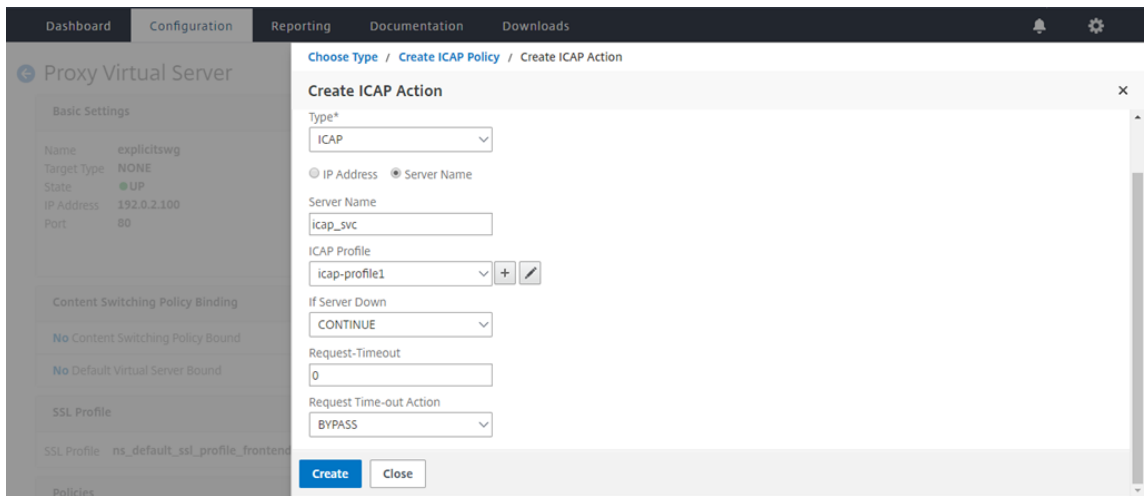
9. 键入配置文件名称 URI。在 模式下，选择 **REQMOD**。



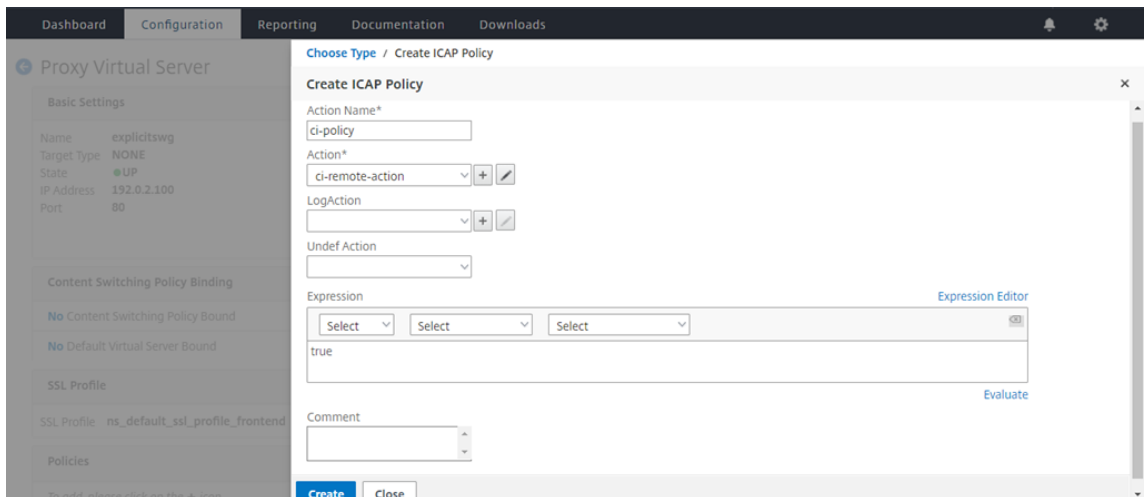
10. 单击创建。



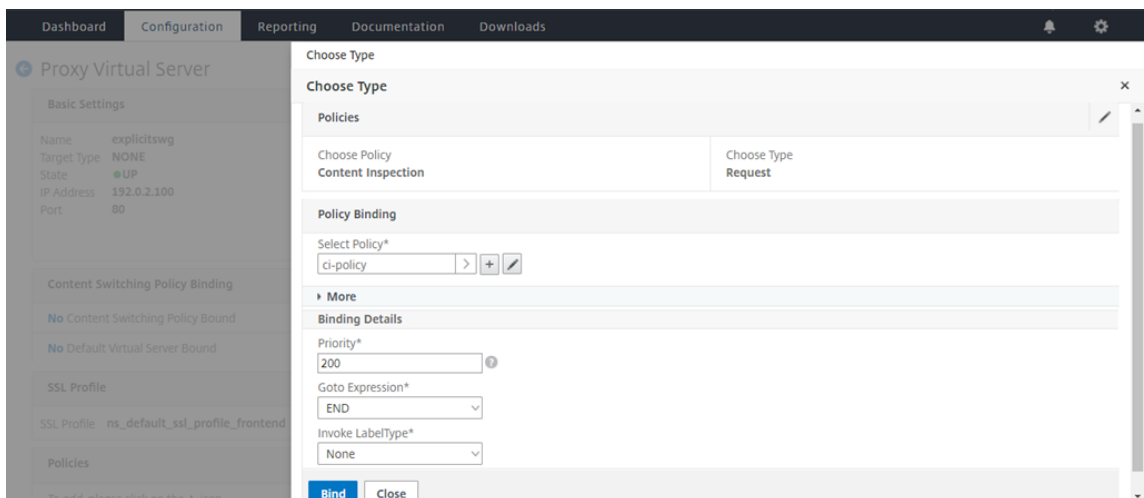
11. 在创建 **ICAP** 操作页面上，单击创建。



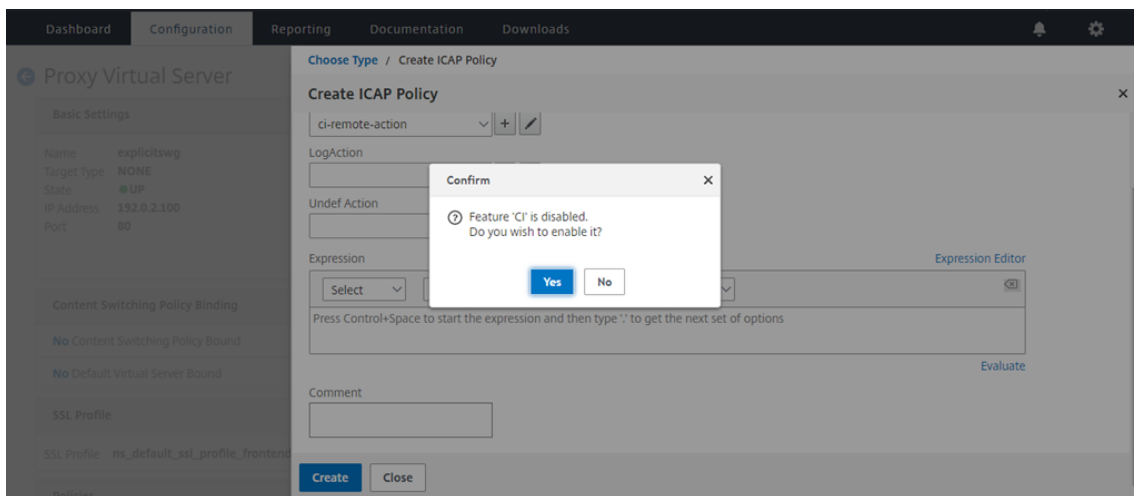
12. 在创建 **ICAP** 策略页面的表达式编辑器中，输入 true。然后，单击创建。



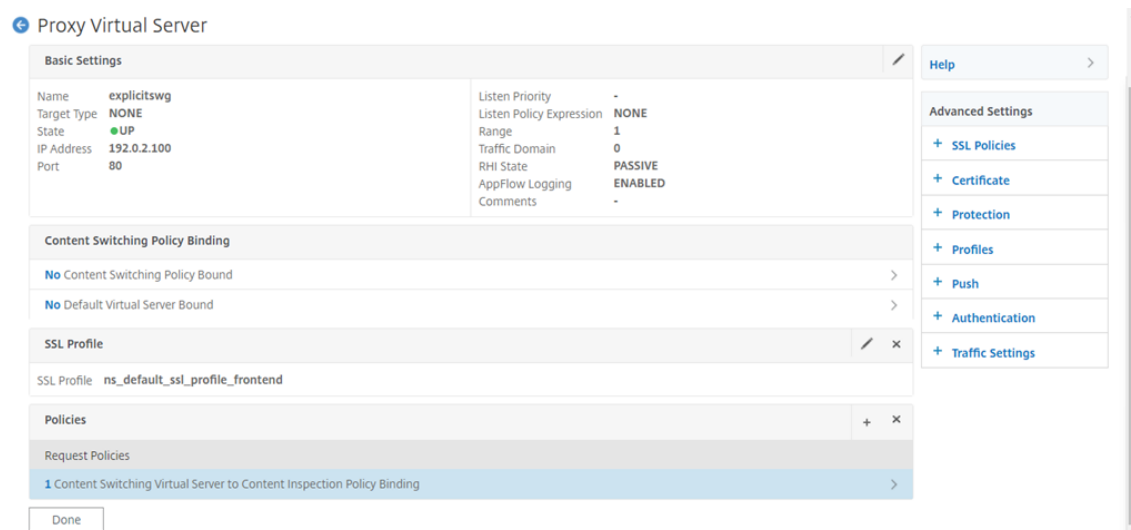
13. 单击 **Bind** (绑定)。



14. 当系统提示启用内容检查功能时，选择 是。



15. 单击完成。



安全的 ICAP

您可以在 SWG 设备和 ICAP 服务器之间建立安全连接。为此，请创建 SSL_TCP 服务而不是 TCP 服务。配置 SSL_TCP 类型的负载均衡虚拟服务器。将 ICAP 服务绑定到负载均衡虚拟服务器。

使用 CLI 配置安全 ICAP

在命令提示符下，键入：

- `add service <name> <IP> SSL_TCP <port>`
- `add lb vserver <name> <serviceType> <IPAddress> <port>`
- `bind lb vserver <name> <serviceName>`

示例:

```
1 add service icap_svc 203.0.113.100 SSL_TCP 1344
2
3 add lbvserver lbicap SSL_TCP 0.0.0.0 0
4
5 bind lb vserver lbicap icap_svc
6 <!--NeedCopy-->
```

使用 GUI 配置安全 ICAP

1. 导航到 负载均衡 > 虚拟服务器，然后单击 添加。
2. 指定虚拟服务器的名称、IP 地址和端口。将协议指定为 SSL_TCP。
3. 单击确定。
4. 在 负载均衡虚拟服务器服务绑定 部分内单击以添加 ICAP 服务。
5. 单击 “+” 以添加服务。
6. 指定服务名称、IP 地址、协议 (SSL_TCP) 和端口 (安全 ICAP 的默认端口为 11344)。
7. 单击确定。
8. 单击完成。
9. 单击 **Bind** (绑定)。
10. 单击 继续 两次。
11. 单击完成。

限制

不支持以下功能:

- ICAP 响应缓存。
- 插入 X-auth-User-URI 标头。
- 在 RESPMOD 的 ICAP 请求中插入 HTTP 请求。

与 IPS 或 NGFW 集成作为内联设备

April 27, 2021

入侵防护系统 (IPS) 和下一代防火墙 (NGFW) 等安全设备可保护服务器免受网络攻击。这些设备可以检查实时流量，并且通常以第 2 层内联模式部署。当访问 Internet 上的资源时，Citrix Secure Web Gateway (SWG) 提供用户和企业网络的安全性。

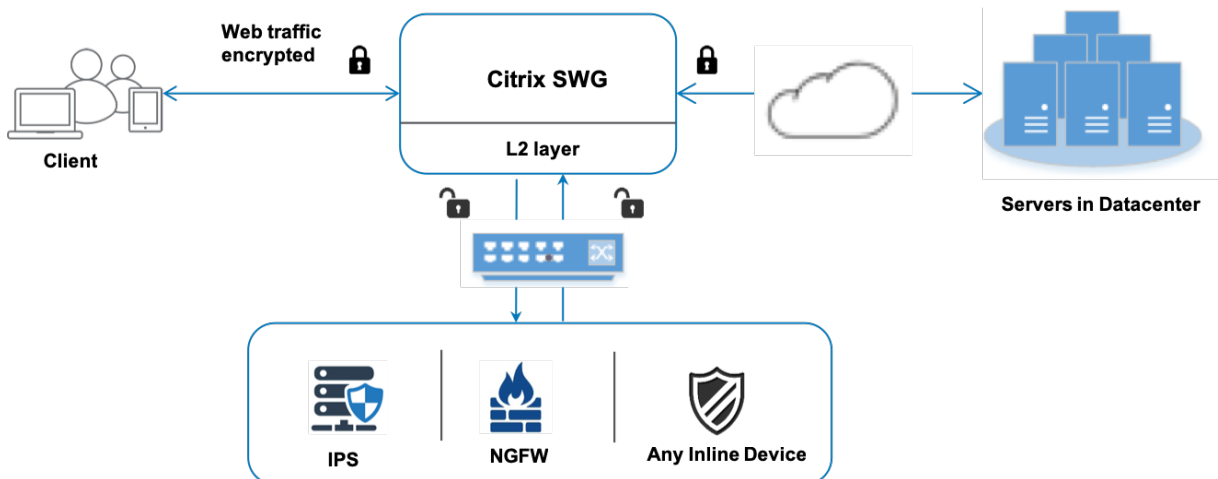
Citrix SWG 设备可与一个或多个内联设备集成，以防止威胁并提供高级安全防护。内联设备可以是任何安全设备，例如 IPS 和 NGFW。

您可以通过使用 Citrix SWG 设备和内联设备集成获益的一些使用案例包括：

- 检查加密流量：大多数 IPS 和 NGFW 设备都会绕过加密流量，这可能会使服务器容易受到攻击。Citrix SWG 设备可以解密流量并将其发送到内联设备进行检查。这种集成增强了客户的网络安全。
- 从 **TLS/SSL** 处理中卸载内联设备：TLS/SSL 处理费用昂贵，如果 IPS 或 NGFW 设备也解密流量，可能会导致 CPU 利用率高。Citrix SWG 设备有助于从内联设备卸载 TLS/SSL 处理。因此，内联设备可以检查更高的流量。
- 负载均衡内联设备：如果您已将多个内联设备配置为管理大流量，Citrix SWG 设备可以对流量进行负载均衡并均匀分配到这些设备。
- 智能流量选择：设备不是将所有流量发送到内联设备进行检查，而是智能选择流量。例如，它跳过向内联设备发送要检查的文本文件。

Citrix SWG 与内联设备集成

下图显示了 Citrix SWG 如何与内联安全设备集成。



将内联设备与 Citrix SWG 设备集成时，组件的交互方式如下：

1. 客户端向 Citrix SWG 设备发送请求。
2. 设备将数据发送到内联设备，以便根据策略评估进行内容检查。对于 HTTPS 流量，设备将解密数据并以纯文本形式将其发送到内联设备以进行内容检查。

注意：

如果有两个或多个内联设备，则设备负载均衡设备并发送流量。

3. 内联设备检查数据是否存在威胁，并决定是删除、重置或将数据发回设备。
4. 如果存在安全威胁，设备将修改数据并将其发送到设备。
5. 对于 HTTPS 流量，设备会重新加密数据并将请求转发到后端服务器。
6. 后端服务器将响应发送到设备。

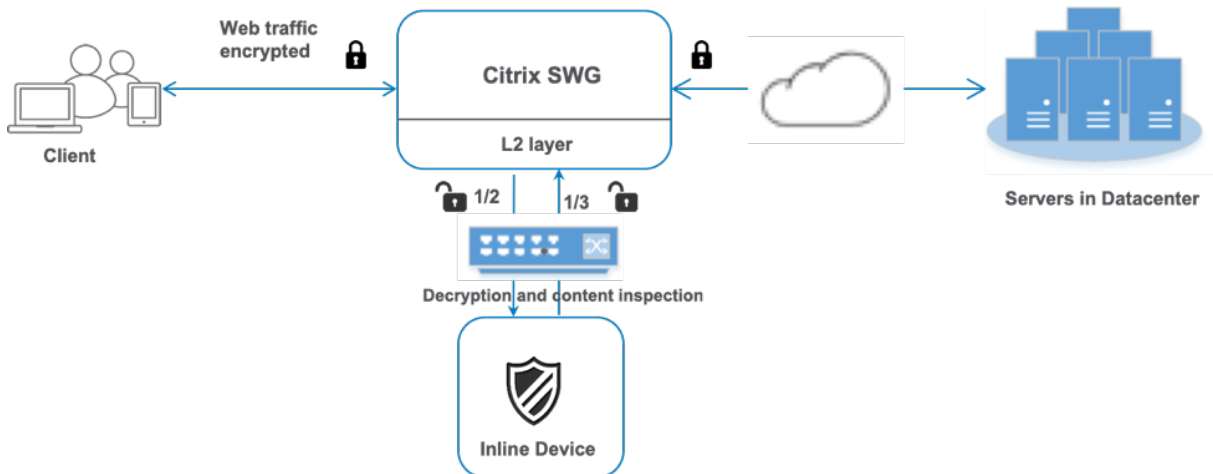
7. 设备再次解密数据并将其发送到内联设备进行检查。
8. 内联设备检查数据。如果存在安全威胁，设备将修改数据并将其发送到设备。
9. 设备会重新加密数据并将响应发送到客户端。

配置内联设备集成

您可以通过以下三种不同的方式配置 Citrix SWG 设备与内联设备：

方案 1：使用单个内联设备

要在内联模式下集成安全设备（IPS 或 NGFW），必须在 SWG 设备上以全局模式启用内容检查和基于 Mac 的转发 (MBF)。然后，添加内容检查配置文件、TCP 服务、内联设备的内容检查操作，以便根据检查重置、阻止或删除流量。此外，还添加内容检查策略，设备用于决定要发送到内联设备的流量子集。最后，配置在服务器上启用了 2 层连接的代理虚拟服务器，并将内容检查策略绑定到此代理虚拟服务器。



执行以下步骤：

1. 启用基于 MAC 的转发 (MPF) 模式。
2. 启用内容检查功能。
3. 为服务添加内容检查配置文件。内容检查配置文件包含将 SWG 装置与内联设备集成的内联设备设置。
4. (可选) 添加 TCP 监视器。

注意：

透明设备没有 IP 地址。因此，要执行运行状况检查，必须显式绑定监视器。

5. 添加服务。服务表示内联设备。
6. (可选) 将服务绑定到 TCP 监视器。

7. 为服务添加内容检查操作。
8. 添加内容检查策略并指定操作。
9. 添加 HTTP 或 HTTPS 代理（内容交换）虚拟服务器。
10. 将内容检查策略绑定到虚拟服务器。

使用 **CLI** 进行配置 在命令提示符处键入以下命令。在大多数命令之后给出了示例。

1. 启用 MBF。

```
1 enable ns mode mbf
2 <!--NeedCopy-->
```

2. 启用功能。

```
1 enable ns feature contentInspection
2 <!--NeedCopy-->
```

3. 添加内容检查配置文件。

```
1 add contentInspection profile <name> -type InlineInspection -
  egressInterface <interface_name> -ingressInterface <
  interface_name>[-egressVlan <positive_integer>] [-ingressVlan <
  positive_integer>]
2 <!--NeedCopy-->
```

示例：

```
1 add contentInspection profile ipsprof -type InlineInspection -
  ingressinterface "1/2" -egressInterface "1/3"
2 <!--NeedCopy-->
```

4. 添加服务。指定不属于任何设备（包括内联设备）所拥有的虚拟 IP 地址。将 `use source IP address (USIP)` 设置为是。设置 `useproxyport` 为否。关闭运行状况监视器。仅当您将此服务绑定到 TCP 监视器时，才打开运行状况监视。如果将显示器绑定到某个服务，请将显示器中的“透明”选项设置为“开”。

```
1 add service <service_name> <IP> TCP <Port> -
  contentInspectionProfileName <Name> -healthMonitor NO -usip
  YES - useproxyport NO
2 <!--NeedCopy-->
```

示例：

```
1 add service ips_service 198.51.100.2 TCP * -healthMonitor YES -
  usip YES -useproxyport NO -contentInspectionProfileName ipsprof
2
3 <!--NeedCopy-->
```

5. 添加内容检查操作。

```

1 add contentInspection action <name> -type INLINEINSPECTION -
  serverName <string>
2 <!--NeedCopy-->

```

示例:

```

1 add contentInspection action ips_action -type INLINEINSPECTION -
  serverName ips_service
2 <!--NeedCopy-->

```

6. 添加内容检查策略。

```

1 add contentInspection policy <name> -rule <expression> -action <
  string>
2 <!--NeedCopy-->

```

示例:

```

1 add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE("
  CONNECT")" -action ips_action
2 <!--NeedCopy-->

```

7. 添加代理虚拟服务器。

```

1 add cs vserver <name> PROXY <IPAddress> <port> -cltTimeout <secs>
  -Listenpolicy <expression> -authn401 ( ON | OFF ) -authnVsName
  <string> -l2Conn ON
2 <!--NeedCopy-->

```

示例:

```

1 add cs vserver transparentcs PROXY * * -cltTimeout 180 -
  Listenpolicy exp1 -authn401 on -authnVsName swg-auth-vs-trans-
  http -l2Conn ON
2 <!--NeedCopy-->

```

8. 将策略绑定到虚拟服务器。

```

1 bind cs vserver <name> -policyName <string> -priority <
  positive_integer> -gotoPriorityExpression <expression> -type
  REQUEST
2 <!--NeedCopy-->

```

示例:

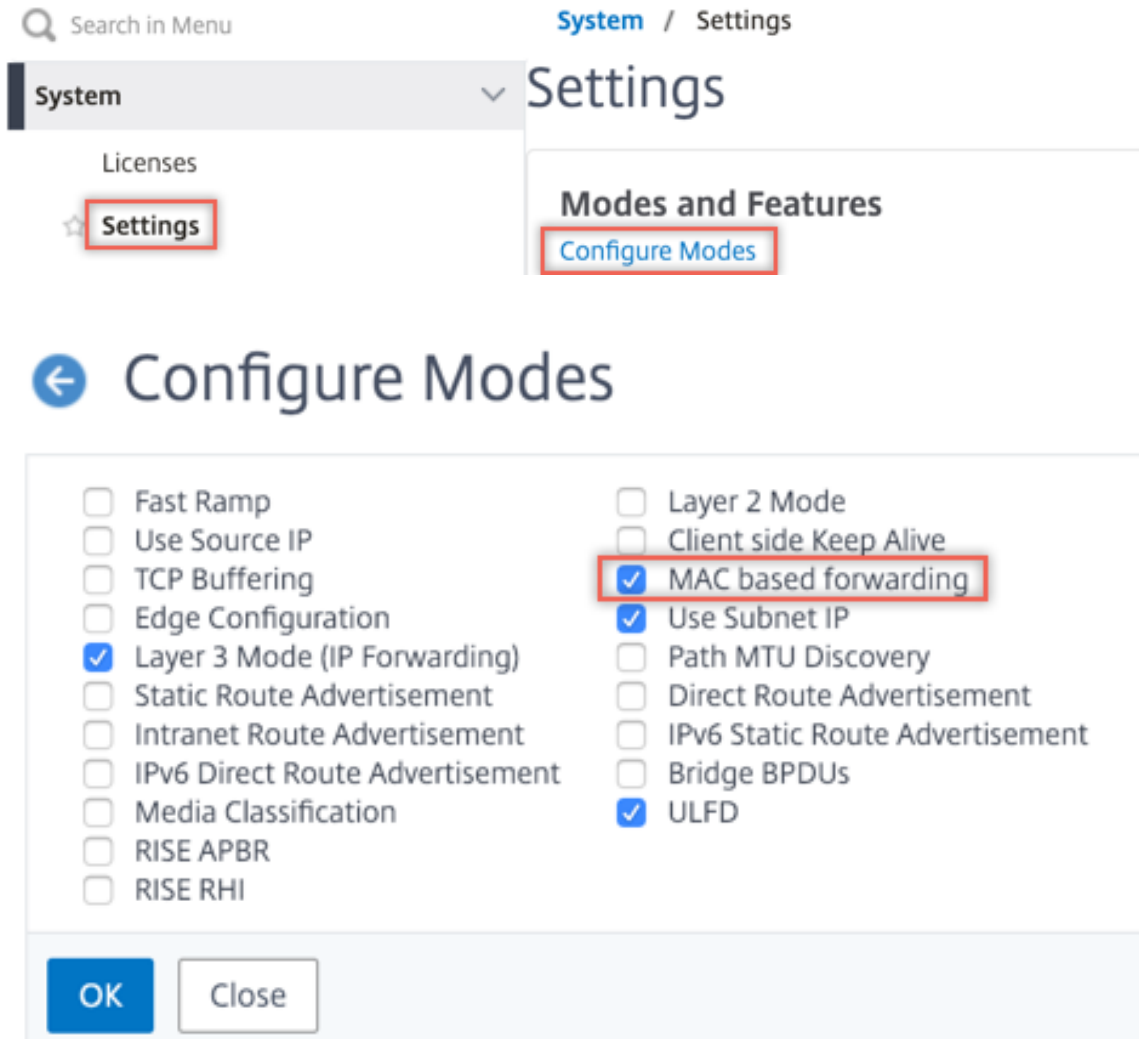
```

1 bind cs vserver explicitcs -policyName ips_pol -priority 1 -
  gotoPriorityExpression END -type REQUEST
2 <!--NeedCopy-->

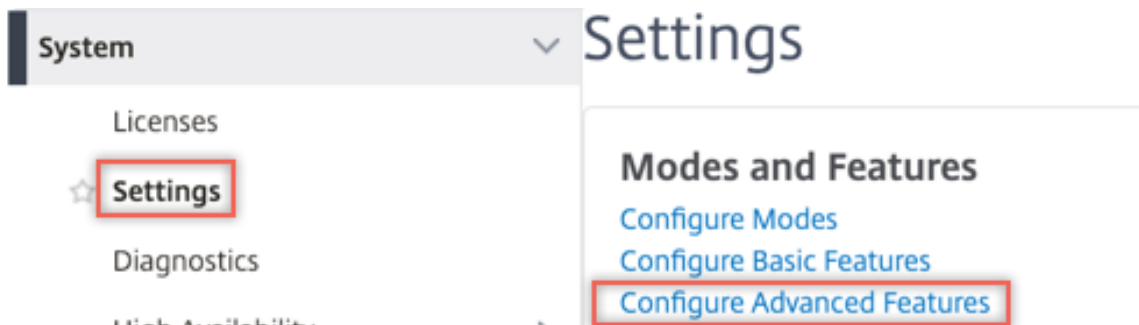
```

使用 **GUI** 进行配置

1. 导航到 **System** (系统) > **Settings** (设置)。在“模式和功能”中，单击“配置模式”。



2. 导航到 **System** (系统) > **Settings** (设置)。在“模式和功能”中，单击“配置高级功能”。



← Configure Advanced Features

<input type="checkbox"/> Surge Protection	<input type="checkbox"/> Sure Connect
<input type="checkbox"/> Priority Queuing	<input type="checkbox"/> Http Dos Protection
<input type="checkbox"/> Cache Redirection	<input type="checkbox"/> Global Server Load Balancing
<input type="checkbox"/> Web Logging	<input type="checkbox"/> OSPF Routing
<input type="checkbox"/> RIP Routing	<input type="checkbox"/> BGP Routing
<input type="checkbox"/> IPv6 Protocol Translation	<input checked="" type="checkbox"/> Responder
<input type="checkbox"/> EdgeSight Monitoring (HTML Injection)	<input type="checkbox"/> Citrix ADC Push
<input checked="" type="checkbox"/> AppFlow	<input type="checkbox"/> Cloud Bridge
<input type="checkbox"/> ISIS Routing	<input type="checkbox"/> Callhome
<input type="checkbox"/> AppQoE	<input type="checkbox"/> Front End Optimization
<input type="checkbox"/> Video Optimization	<input type="checkbox"/> Content Accelerator
<input type="checkbox"/> Large Scale NAT	<input type="checkbox"/> vPath
<input type="checkbox"/> RDP Proxy	<input type="checkbox"/> Reputation
<input checked="" type="checkbox"/> URL Filtering	<input checked="" type="checkbox"/> Forward Proxy
<input checked="" type="checkbox"/> SSL Interception	<input type="checkbox"/> Adaptive TCP
<input type="checkbox"/> Connection Quality Analytics	<input checked="" type="checkbox"/> Content Inspection
<input type="checkbox"/> RISE	

OK Close

3. 导航到 **Secure Web Gateway > 内容检查 > 内容检查配置文件**。单击添加。

4. 导航到 **负载均衡 > 服务 > 添加并添加服务**。在高级设置中，单击 **配置文件**。在 **CI 配置文件名称** 列表中，选择之前创建的内容检查配置文件。在“服务设置”中，将“使用源 IP 地址”设置为“是”，并将“使用代理端口”设置为“否”。在“基本设置”中，将“运行状况监视”设置为“否”。仅当您将此服务绑定到 TCP 监视器时，才打开运行状况监视。如果将监视器绑定到某个服务，请将监视器中的“透明”选项设置为“开”。

Profiles

Net Profile

Add ?

TCP Profile

Add

HTTP Profile

Add

DNS Profile Name

Add

CI Profile Name

ipsprof
▼

Add ?

Service Settings

Sure Connect	
Surge Protection	OFF
Use Proxy Port	NO
Down State Flush	ENABLED
Access Down	NO
Use Source IP Address	YES
Client Keep-Alive	NO
TCP Buffering	NO
Insert Client IP Address Header	DISABLED
	client-ip

Basic Settings

Service Name	ips_service	Traffic Domain	0
Server Name	198.51.100.2	Number of Active Connections	-
IP Address	198.51.100.2	Hash ID	-
Server State	● UP	Server ID	None
Protocol	TCP	Cache Type	SERVER
Port	*	Cacheable	NO
Comments		Health Monitoring	NO
		AppFlow Logging	ENABLED
Monitoring Connection Close Bit	NONE		

5. 导航到 **Secure Web Gateway > 代理虚拟服务器 > 添加**。指定名称、IP 地址和端口。在“高级设置”中，选择“策略”。点击“+”符号。

Proxy Virtual Server

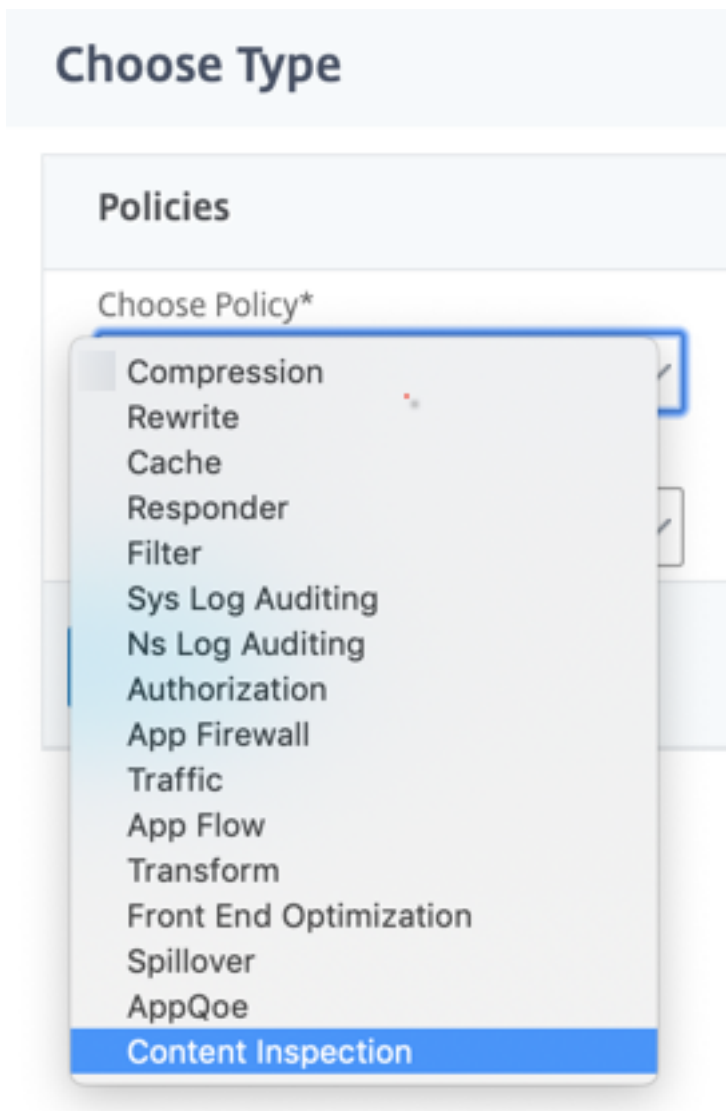
Basic Settings	
Name	proxyvsr
State	● UP
IP Address	198.51.200.2
Port	80
Listen Priority	-
Listen Policy Expression	NONE
Range	1
IPset	-
Traffic Domain	0
RHI State	PASSIVE
AppFlow Logging	ENABLED
Comments	-

Content Switching Policy Binding	
No Content Switching Policy Bound	>
No Default Virtual Server Bound	>

Certificate	
No Server Certificate	>
No CA Certificate	>

Policies	
	+ x

6. 在“选择策略”中，选择“内容检查”。单击继续。



7. 单击添加。指定名称。在“操作”中，单击“添加”。

[Choose Type](#) / Create ContentInspection Policy

Create ContentInspection Policy

Policy Name*

Action*

Add

Edit

Log Action

Add

Edit

UNDEF Action

- 指定名称。在“类型”中，选择“在线检查”。在“服务器名称”中，选择之前创建的 TCP 服务。

← Create ContentInspection Action

Name*

Type*

Server Name*

If Server Down

Request-Timeout

Request timeout action

9. 单击创建。指定规则，然后单击创建。

Configure ContentInspection Policy

Policy Name

Action*

Log Action

UNDEF Action

Expression* Expression Editor

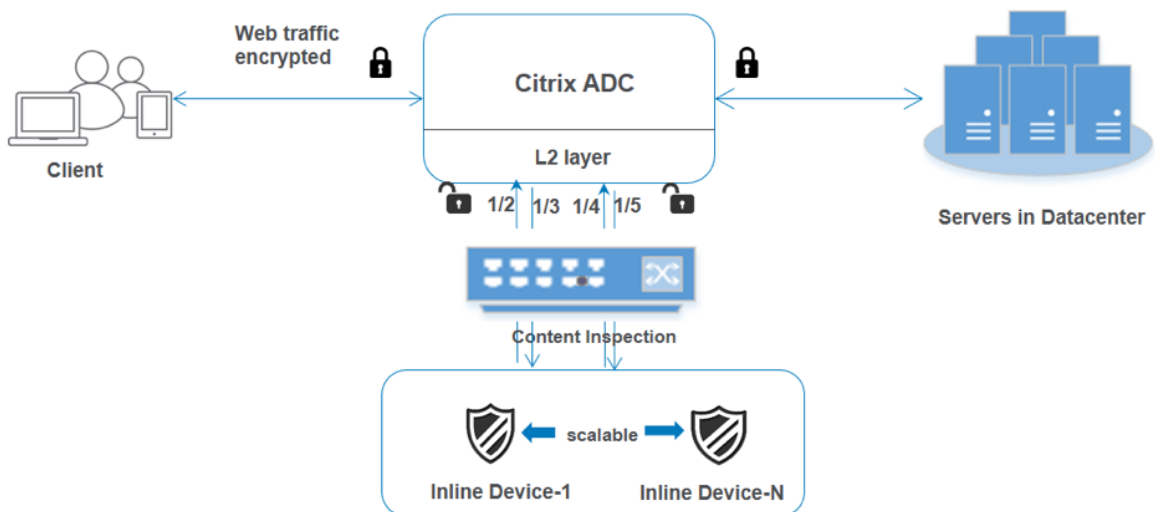
Comment

10. 单击 **Bind** (绑定)。

11. 单击完成。

场景 2：具有专用接口的多个内联设备负载均衡

如果您使用的是两个或多个内联设备，则可以使用具有专用接口的不同内容检测服务对设备进行负载均衡。在这种情况下，Citrix SWG 设备会对通过专用接口发送到每台设备的流量子集进行负载均衡。子集是根据配置的策略决定的。例如，TXT 或图像文件可能不会被发送到内联设备以进行检查。



基本配置与场景 1 保持相同。但是，您必须为每个内联设备创建内容检查配置文件，并在每个配置文件中指定入口和导出界面。为每个内联设备添加服务。添加负载均衡虚拟服务器并在内容检查操作中指定该服务器。执行以下额外步骤：

1. 为每个服务添加内容检查配置文件。
2. 为每个设备添加服务。
3. 添加负载均衡虚拟服务器。
4. 在内容检查操作中指定负载均衡虚拟服务器。

使用 **CLI** 进行配置 在命令提示符处键入以下命令。每个命令之后都会给出示例。

1. 启用 MBF。

```
1 enable ns mode mbf
2 <!--NeedCopy-->
```

2. 启用功能。

```
1 enable ns feature contentInspection
2 <!--NeedCopy-->
```

3. 为服务 1 添加配置文件 1。

```
1 add contentInspection profile <name> -type InlineInspection -
  egressInterface <interface_name> -ingressInterface <
  interface_name>[-egressVlan <positive_integer>] [-ingressVlan <
  positive_integer>]
2 <!--NeedCopy-->
```

示例：

```
1 add contentInspection profile ipsprof1 -type InlineInspection -
  ingressInterface "1/2" -egressInterface "1/3"
2 <!--NeedCopy-->
```

4. 为服务 2 添加配置文件 2。

```
1 add contentInspection profile <name> -type InlineInspection -
  egressInterface <interface_name> -ingressInterface <
  interface_name>[-egressVlan <positive_integer>] [-ingressVlan <
  positive_integer>]
2 <!--NeedCopy-->
```

示例：

```
1 add contentInspection profile ipsprof2 -type InlineInspection -
  ingressInterface "1/4" -egressInterface "1/5"
2 <!--NeedCopy-->
```

5. 添加服务 1。指定不属于任何设备（包括内联设备）所拥有的虚拟 IP 地址。将 `use source IP address` (USIP) 设置为是。设置 `useproxyport` 为否。关闭运行状况监视器。仅当您将此服务绑定到 TCP 监视器时，才打开运行状况监视。如果将显示器绑定到某个服务，请将显示器中的“透明”选项设置为“开”。

```
1 add service <service_name> <IP> TCP <Port> -
  contentinspectionProfileName <Name> -healthMonitor NO -usip
  YES - useproxyport NO
2 <!--NeedCopy-->
```

示例：

```
1 add service ips_service1 192.168.10.2 TCP * -healthMonitor NO -
  usip YES -useproxyport NO -contentInspectionProfileName
  ipsprof1
2 <!--NeedCopy-->
```

6. 添加服务 2。指定不属于任何设备（包括内联设备）所拥有的虚拟 IP 地址。将 `use source IP address` (USIP) 设置为是。设置 `useproxyport` 为否。关闭运行状况监视器。仅当您将此服务绑定到 TCP 监视器时，才打开运行状况监视。如果将显示器绑定到某个服务，请将显示器中的“透明”选项设置为“开”。

```
1 add service <service_name> <IP> TCP <Port> -
  contentinspectionProfileName <Name> -healthMonitor NO -usip
  YES - useproxyport NO
2 <!--NeedCopy-->
```

示例：

```
1 add service ips_service2 192.168.10.3 TCP * -healthMonitor NO -
  usip YES -useproxyport NO -contentInspectionProfileName
  ipsprof2
2 <!--NeedCopy-->
```

7. 添加负载均衡虚拟服务器。

```
1 add lb vserver <LB_VSERVER_NAME> TCP <IP> <port>
2 <!--NeedCopy-->
```

示例：

```
1 add lb vserver lb_inline_vserver TCP 192.0.2.100 *
2 <!--NeedCopy-->
```

8. 将服务绑定到负载均衡虚拟服务器。

```
1 bind lb vserver <LB_VSERVER_NAME> <service_name>
2 bind lb vserver <LB_VSERVER_NAME> <service_name>
3 <!--NeedCopy-->
```

示例：

```
1 bind lb vserver lb_inline_vserver ips_service1
2 bind lb vserver lb_inline_vserver ips_service2
```

```
3 <!--NeedCopy-->
```

9. 在内容检查操作中指定负载均衡虚拟服务器。

```
1 add contentInspection action <name> -type INLINEINSPECTION -
  serverName <string>
2 <!--NeedCopy-->
```

示例:

```
1 add contentInspection action ips_action -type INLINEINSPECTION -
  serverName lb_inline_vserver
2 <!--NeedCopy-->
```

10. 添加内容检查策略。在策略中指定内容检查操作。

```
1 add contentInspection policy <name> -rule <expression> -action <
  string>
2 <!--NeedCopy-->
```

示例:

```
1 add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE("
  CONNECT)" -action ips_action
2 <!--NeedCopy-->
```

11. 添加代理虚拟服务器。

```
1 add cs vserver <name> PROXY <IPAddress> <port> -l2Conn ON
2 <!--NeedCopy-->
```

示例:

```
1 add cs vserver transparentcs PROXY * * -l2Conn ON
2 <!--NeedCopy-->
```

12. 将内容检查策略绑定到虚拟服务器。

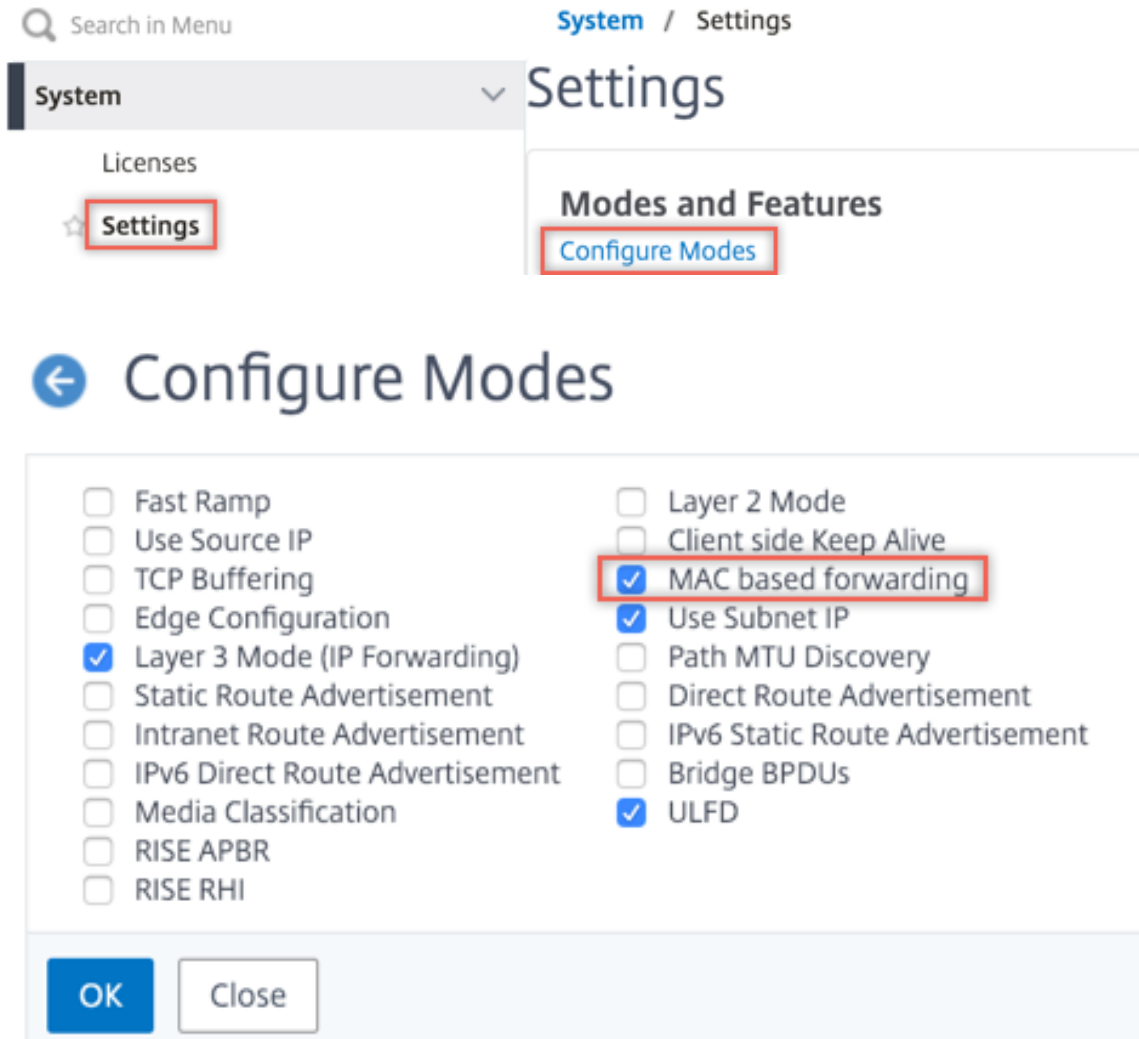
```
1 bind cs vserver <name> -policyName <string> -priority <
  positive_integer> -gotoPriorityExpression <expression> -type
  REQUEST
2 <!--NeedCopy-->
```

示例:

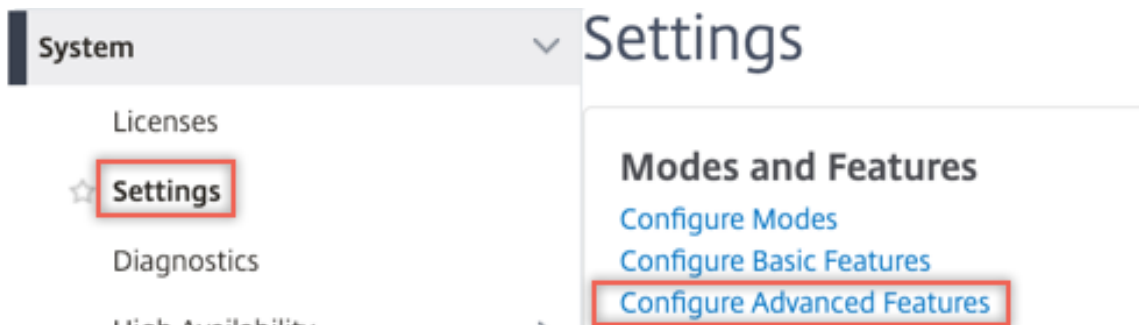
```
1 bind cs vserver explicitcs -policyName ips_pol -priority 1 -
  gotoPriorityExpression END -type REQUEST
2 <!--NeedCopy-->
```

使用 **GUI** 进行配置

1. 导航到 **System** (系统) > **Settings** (设置)。在“模式和功能”中，单击“配置模式”。



2. 导航到 **System** (系统) > **Settings** (设置)。在“模式和功能”中，单击“配置高级功能”。

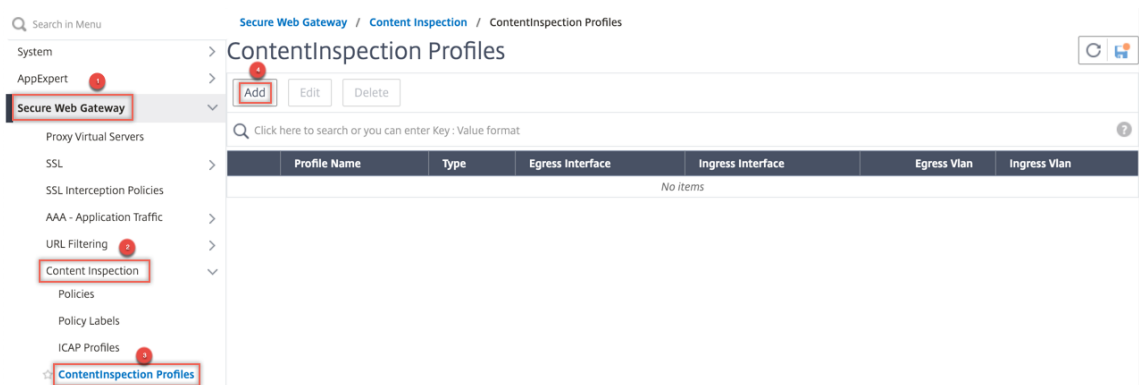


← Configure Advanced Features

<input type="checkbox"/> Surge Protection	<input type="checkbox"/> Sure Connect
<input type="checkbox"/> Priority Queuing	<input type="checkbox"/> Http Dos Protection
<input type="checkbox"/> Cache Redirection	<input type="checkbox"/> Global Server Load Balancing
<input type="checkbox"/> Web Logging	<input type="checkbox"/> OSPF Routing
<input type="checkbox"/> RIP Routing	<input type="checkbox"/> BGP Routing
<input type="checkbox"/> IPv6 Protocol Translation	<input checked="" type="checkbox"/> Responder
<input type="checkbox"/> EdgeSight Monitoring (HTML Injection)	<input type="checkbox"/> Citrix ADC Push
<input checked="" type="checkbox"/> AppFlow	<input type="checkbox"/> Cloud Bridge
<input type="checkbox"/> ISIS Routing	<input type="checkbox"/> Callhome
<input type="checkbox"/> AppQoE	<input type="checkbox"/> Front End Optimization
<input type="checkbox"/> Video Optimization	<input type="checkbox"/> Content Accelerator
<input type="checkbox"/> Large Scale NAT	<input type="checkbox"/> vPath
<input type="checkbox"/> RDP Proxy	<input type="checkbox"/> Reputation
<input checked="" type="checkbox"/> URL Filtering	<input checked="" type="checkbox"/> Forward Proxy
<input checked="" type="checkbox"/> SSL Interception	<input type="checkbox"/> Adaptive TCP
<input type="checkbox"/> Connection Quality Analytics	<input checked="" type="checkbox"/> Content Inspection
<input type="checkbox"/> RISE	

OK Close

3. 导航到 **Secure Web Gateway > 内容检查 > 内容检查配置文件**。单击添加。



指定入口和导出接口。

← Create ContentInspectionProfile

Profile Name*

Type*

Egress Interface*

Ingress Interface*

Egress Vlan

Ingress Vlan

创建两个配置文件。在第二个配置文件中指定不同的入口和导出界面。

4. 导航到负载平衡 > 服务 > 添加并添加服务。在高级设置中，单击 配置文件。在 **CI** 配置文件名称 列表中，选择之前创建的内容检查配置文件。在“服务设置”中，将“使用源 IP 地址”设置为“是”，并将“使用代理端口”设置为“否”。在“基本设置”中，将“运行状况监视”设置为“否”。仅当您将此服务绑定到 TCP 监视器时，才打开运行状况监视。如果将显示器绑定到某个服务，请将显示器中的“透明”选项设置为“开”。

Profiles

Net Profile

Add ?

TCP Profile

Add

HTTP Profile

Add

DNS Profile Name

Add

CI Profile Name

ipsprof

Add ?

Service Settings

Sure Connect	
Surge Protection	OFF
Use Proxy Port	NO
Down State Flush	ENABLED
Access Down	NO
Use Source IP Address	YES
Client Keep-Alive	NO
TCP Buffering	NO
Insert Client IP Address Header	DISABLED
	client-ip

Basic Settings

Service Name	ips_service	Traffic Domain	0
Server Name	198.51.100.2	Number of Active Connections	-
IP Address	198.51.100.2	Hash ID	-
Server State	● UP	Server ID	None
Protocol	TCP	Cache Type	SERVER
Port	*	Cacheable	NO
Comments		Health Monitoring	NO
		AppFlow Logging	ENABLED
Monitoring Connection Close Bit	NONE		

创建两个服务。指定不属于任何设备（包括内联设备）所拥有的虚拟 IP 地址。

5. 导航到负载平衡 > 虚拟服务器 > 添加。创建 TCP 负载平衡虚拟服务器。

Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address.
You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name*

Protocol*

IP Address Type*

IP Address*

Port*

More

单击确定。

6. 在 负载均衡虚拟服务器服务绑定 部分内单击。在“服务绑定”中，单击“选择服务”中的箭头。选择之前创建的两个服务，然后单击“选择”。单击 **Bind**（绑定）。

Service Binding

Select Service*

Binding Details

Weight

Service Binding / Service

Service

Select Add Edit

🔍 Click here to search or you can enter

<input type="checkbox"/>	Name
<input type="checkbox"/>	icap_svc
<input type="checkbox"/>	icap_domain1
<input type="checkbox"/>	ssltcp_svc1
<input type="checkbox"/>	s1
<input type="checkbox"/>	ips_service
<input checked="" type="checkbox"/>	ips_service1
<input checked="" type="checkbox"/>	ips_service2

Service Binding

Service Binding

Select Service*

ips_service1, ips_service2 > Add Edit ?

Binding Details

Weight

1

Bind Close

7. 导航到 **Secure Web Gateway > 代理虚拟服务器 > 添加**。指定名称、IP 地址和端口。在“高级设置”中，选择“策略”。点击“+”符号。

← Proxy Virtual Server

Basic Settings

Name	proxyvsvr	Listen Priority	-
State	● UP	Listen Policy Expression	NONE
IP Address	198.51.200.2	Range	1
Port	80	IPset	-
		Traffic Domain	0
		RHI State	PASSIVE
		AppFlow Logging	ENABLED
		Comments	-

Content Switching Policy Binding

No Content Switching Policy Bound >

No Default Virtual Server Bound >

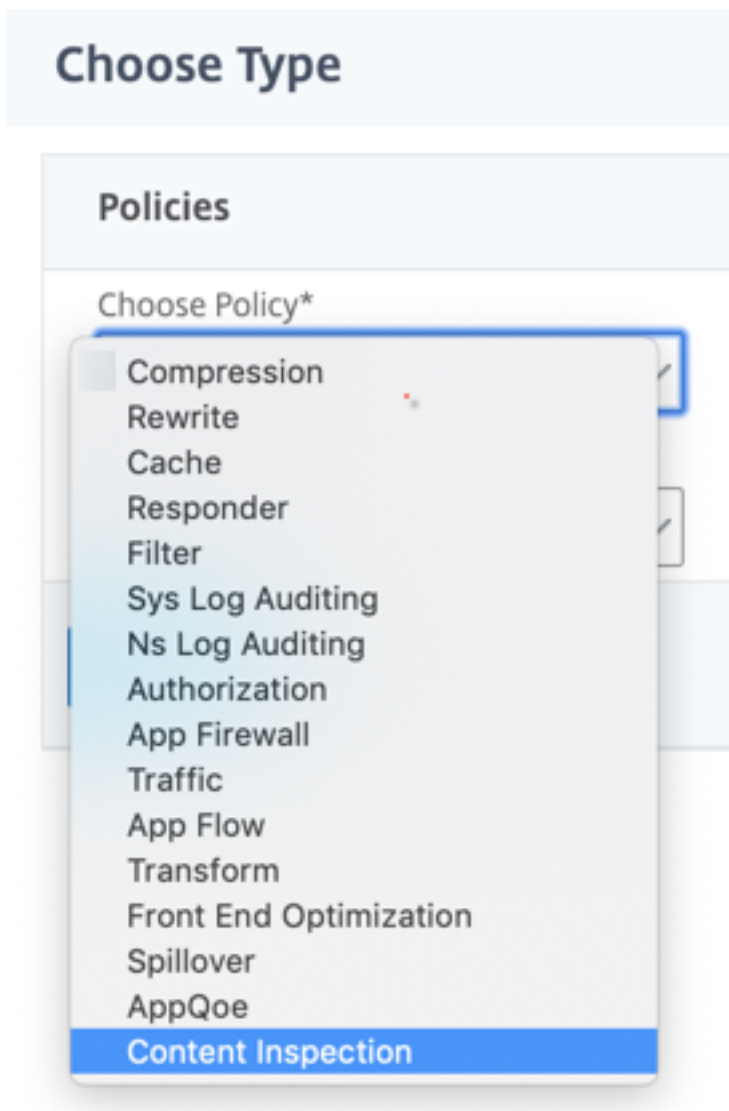
Certificate

No Server Certificate >

No CA Certificate >

Policies + x

8. 在“选择策略”中，选择“内容检查”。单击继续。



9. 单击添加。指定名称。在“操作”中，单击“添加”。

[Choose Type](#) / Create ContentInspection Policy

Create ContentInspection Policy

Policy Name*

Action*

Log Action

UNDEF Action

10. 指定名称。在“类型”中，选择“在线检查”。在“服务器名称”中，选择之前创建的负载均衡虚拟服务器。

← Create ContentInspection Action

Name*

Type*

Server Name*

If Server Down

Request-Timeout

Request timeout action

11. 单击创建。指定规则，然后单击创建。

Configure ContentInspection Policy

Policy Name
ips_pol

Action*
ips_action Add Edit

Log Action
Add Edit

UNDEF Action

Expression* Expression Editor
Select Select Select ✕
HTTP.REQ.METHOD.NE("CONNECT") Evaluate

Comment

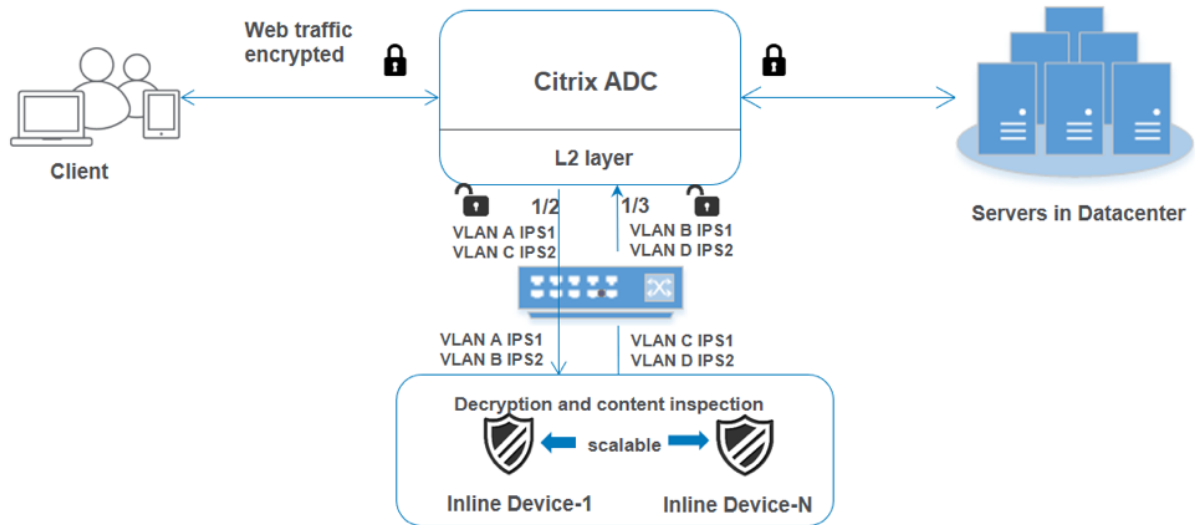
OK Close

12. 单击 **Bind** (绑定)。

13. 单击完成。

场景 3：具有共享接口的多个内联设备负载均衡

如果您使用的是两个或多个内联设备，则可以使用具有共享接口的不同内容检查服务对设备进行负载均衡。在这种情况下，Citrix SWG 设备会对通过共享接口发送到每台设备的流量子集进行负载均衡。子集是根据配置的策略决定的。例如，TXT 或图像文件可能不会被发送到内联设备以进行检查。



基本配置与场景 2 保持相同。在这种情况下，请将接口绑定到不同的 VLAN，以便为每个内嵌设备分离流量。在内容检查配置文件中指定 VLAN。执行以下额外步骤：

1. 将共享接口绑定到不同的 VLAN。
2. 在内容检查配置文件中指定入站和出站 VLAN。

使用 **CLI** 进行配置 在命令提示符处键入以下命令。每个命令之后都会给出示例。

1. 启用 MBF。

```
1 enable ns mode mbf
2 <!--NeedCopy-->
```

2. 启用功能。

```
1 enable ns feature contentInspection
2 <!--NeedCopy-->
```

3. 将共享接口绑定到不同的 VLAN。

```
1 bind vlan <id> -ifnum <interface> -tagged
2 <!--NeedCopy-->
```

示例：

```
1 bind vlan 100 -ifnum 1/2 tagged
2 bind vlan 200 -ifnum 1/3 tagged
3 bind vlan 300 -ifnum 1/2 tagged
4 bind vlan 400 -ifnum 1/3 tagged
5 <!--NeedCopy-->
```

4. 为服务 1 添加配置文件 1。在配置文件中指定入站和出站 VLAN。

```
1 add contentInspection profile <name> -type InlineInspection -
  egressInterface <interface_name> -ingressInterface <
  interface_name>[-egressVlan <positive_integer>] [-ingressVlan <
  positive_integer>]
2 <!--NeedCopy-->
```

示例:

```
1 add contentInspection profile ipsprof1 -type InlineInspection -
  egressInterface "1/3" -ingressinterface "1/2" - egressVlan 100
  -ingressVlan 300
2 <!--NeedCopy-->
```

5. 为服务 2 添加配置文件 2。在配置文件中指定入站和出站 VLAN。

```
1 add contentInspection profile <name> -type InlineInspection -
  egressInterface <interface_name> -ingressInterface <
  interface_name>[-egressVlan <positive_integer>] [-ingressVlan <
  positive_integer>]
2 <!--NeedCopy-->
```

示例:

```
1 add contentInspection profile ipsprof2 -type InlineInspection -
  egressInterface "1/3" -ingressinterface "1/2" - egressVlan 200
  -ingressVlan 400
2 <!--NeedCopy-->
```

6. 添加服务 1。

```
1 add service <service_name> <IP> TCP <Port> -
  contentinspectionProfileName <Name> -healthMonitor NO -usip
  YES - useproxyport NO
2 <!--NeedCopy-->
```

示例:

```
1 add service ips_service1 192.168.10.2 TCP * -healthMonitor NO -
  usip YES -useproxyport NO -contentInspectionProfileName
  ipsprof1
2 <!--NeedCopy-->
```

7. 添加服务 2。

```
1 add service <service_name> <IP> TCP <Port> -
  contentinspectionProfileName <Name> -healthMonitor NO -usip
  YES - useproxyport NO
2 <!--NeedCopy-->
```

示例:

```

1 add service ips_service2 192.168.10.3 TCP * -healthMonitor NO -
  usip YES -useproxyport NO -contentInspectionProfileName
  ipsprof2
2 <!--NeedCopy-->

```

8. 添加负载均衡虚拟服务器。

```

1 add lb vserver <LB_VSERVER_NAME> TCP <IP> <port>
2 <!--NeedCopy-->

```

示例：

```

1 add lb vserver lb_inline_vserver TCP 192.0.2.100 *
2 <!--NeedCopy-->

```

9. 将服务绑定到负载均衡虚拟服务器。

```

1 bind lb vserver <LB_VSERVER_NAME> <service_name>
2 bind lb vserver <LB_VSERVER_NAME> <service_name>
3 <!--NeedCopy-->

```

示例：

```

1 bind lb vserver lb_inline_vserver ips_service1
2 bind lb vserver lb_inline_vserver ips_service2
3 <!--NeedCopy-->

```

10. 在内容检查操作中指定负载均衡虚拟服务器。

```

1 add contentInspection action <name> -type INLINEINSPECTION -
  serverName <string>
2 <!--NeedCopy-->

```

示例：

```

1 add contentInspection action ips_action -type INLINEINSPECTION -
  serverName lb_inline_vserver
2 <!--NeedCopy-->

```

11. 添加内容检查策略。在策略中指定内容检查操作。

```

1 add contentInspection policy <name> -rule <expression> -action <
  string>
2 <!--NeedCopy-->

```

示例：

```

1 add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE("
  CONNECT)" -action ips_action
2 <!--NeedCopy-->

```

12. 添加代理虚拟服务器。

```
1 add cs vserver <name> PROXY <IPAddress> <port> -l2Conn ON
2 <!--NeedCopy-->
```

示例:

```
1 add cs vserver transparentcs PROXY * * -l2Conn ON
2 <!--NeedCopy-->
```

13. 将内容检查策略绑定到虚拟服务器。

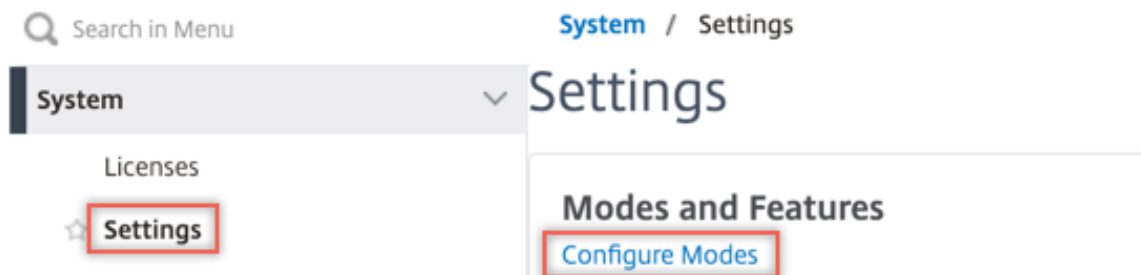
```
1 bind cs vserver <name> -policyName <string> -priority <
  positive_integer> -gotoPriorityExpression <expression> -type
  REQUEST
2 <!--NeedCopy-->
```

示例:

```
1 bind cs vserver explicitcs -policyName ips_pol -priority 1 -
  gotoPriorityExpression END -type REQUEST
2 <!--NeedCopy-->
```

使用 **GUI** 进行配置

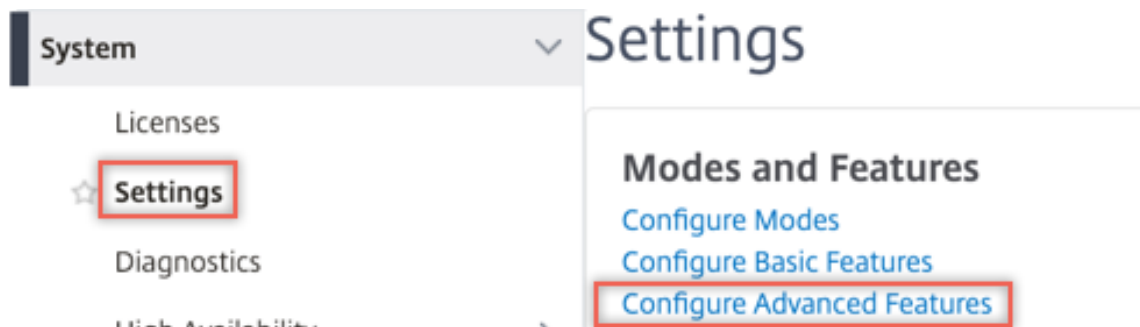
1. 导航到 **System** (系统) > **Settings** (设置)。在“模式和功能”中，单击“配置模式”。



← Configure Modes

<input type="checkbox"/> Fast Ramp	<input type="checkbox"/> Layer 2 Mode
<input type="checkbox"/> Use Source IP	<input type="checkbox"/> Client side Keep Alive
<input type="checkbox"/> TCP Buffering	<input checked="" type="checkbox"/> MAC based forwarding
<input type="checkbox"/> Edge Configuration	<input checked="" type="checkbox"/> Use Subnet IP
<input checked="" type="checkbox"/> Layer 3 Mode (IP Forwarding)	<input type="checkbox"/> Path MTU Discovery
<input type="checkbox"/> Static Route Advertisement	<input type="checkbox"/> Direct Route Advertisement
<input type="checkbox"/> Intranet Route Advertisement	<input type="checkbox"/> IPv6 Static Route Advertisement
<input type="checkbox"/> IPv6 Direct Route Advertisement	<input type="checkbox"/> Bridge BPDUs
<input type="checkbox"/> Media Classification	<input checked="" type="checkbox"/> ULFD
<input type="checkbox"/> RISE APBR	
<input type="checkbox"/> RISE RHI	

2. 导航到 **System** (系统) > **Settings** (设置)。在“模式和功能”中，单击“配置高级功能”。



← Configure Advanced Features

<input type="checkbox"/> Surge Protection	<input type="checkbox"/> Sure Connect
<input type="checkbox"/> Priority Queuing	<input type="checkbox"/> Http Dos Protection
<input type="checkbox"/> Cache Redirection	<input type="checkbox"/> Global Server Load Balancing
<input type="checkbox"/> Web Logging	<input type="checkbox"/> OSPF Routing
<input type="checkbox"/> RIP Routing	<input type="checkbox"/> BGP Routing
<input type="checkbox"/> IPv6 Protocol Translation	<input checked="" type="checkbox"/> Responder
<input type="checkbox"/> EdgeSight Monitoring (HTML Injection)	<input type="checkbox"/> Citrix ADC Push
<input checked="" type="checkbox"/> AppFlow	<input type="checkbox"/> Cloud Bridge
<input type="checkbox"/> ISIS Routing	<input type="checkbox"/> Callhome
<input type="checkbox"/> AppQoS	<input type="checkbox"/> Front End Optimization
<input type="checkbox"/> Video Optimization	<input type="checkbox"/> Content Accelerator
<input type="checkbox"/> Large Scale NAT	<input type="checkbox"/> vPath
<input type="checkbox"/> RDP Proxy	<input type="checkbox"/> Reputation
<input checked="" type="checkbox"/> URL Filtering	<input checked="" type="checkbox"/> Forward Proxy
<input checked="" type="checkbox"/> SSL Interception	<input type="checkbox"/> Adaptive TCP
<input type="checkbox"/> Connection Quality Analytics	<input checked="" type="checkbox"/> Content Inspection
<input type="checkbox"/> RISE	

3. 导航到系统 > 网络 > **VLAN** > 添加。添加四个 VLAN 并将其标记为接口。

← Create VLAN

VLAN ID*

100 ?

Alias Name

Maximum Transmission Unit

- Dynamic Routing
- IPv6 Dynamic Routing
- Partitions Sharing

Interface Bindings

IP Bindings

<input type="checkbox"/>	Name	Tagged
<input type="checkbox"/>	1/1	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1/2	<input checked="" type="checkbox"/>
<input type="checkbox"/>	1/3	<input type="checkbox"/>

← Create VLAN

VLAN ID*

200



Alias Name

Maximum Transmission Unit

- Dynamic Routing
- IPv6 Dynamic Routing
- Partitions Sharing

Interface Bindings

IP Bindings

<input type="checkbox"/>	Name	Tagged
<input type="checkbox"/>	1/1	<input type="checkbox"/>
<input type="checkbox"/>	1/2	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1/3	<input checked="" type="checkbox"/>

← Create VLAN

VLAN ID*

300



Alias Name

Maximum Transmission Unit

- Dynamic Routing
- IPv6 Dynamic Routing
- Partitions Sharing

Interface Bindings

IP Bindings

<input type="checkbox"/>	Name	Tagged
<input type="checkbox"/>	1/1	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1/2	<input checked="" type="checkbox"/>
<input type="checkbox"/>	1/3	<input type="checkbox"/>

← Create VLAN

VLAN ID*

400



Alias Name

Maximum Transmission Unit

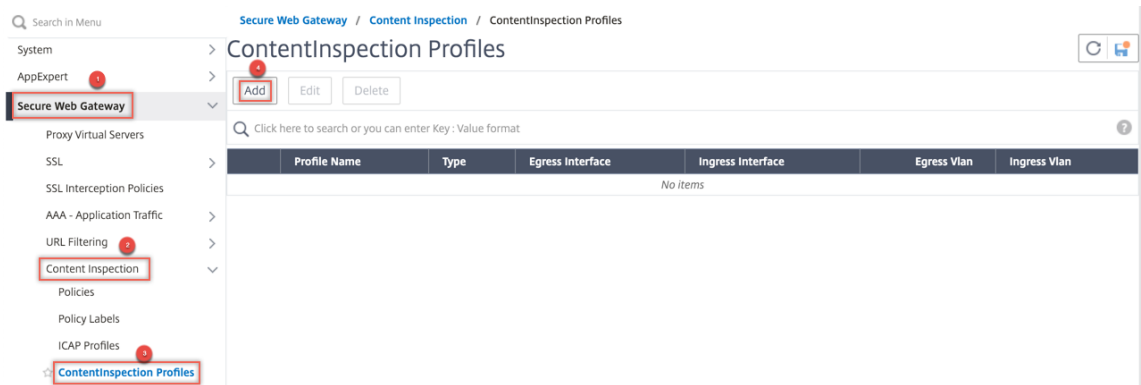
- Dynamic Routing
- IPv6 Dynamic Routing
- Partitions Sharing

Interface Bindings

IP Bindings

<input type="checkbox"/>	Name	Tagged
<input type="checkbox"/>	1/1	<input type="checkbox"/>
<input type="checkbox"/>	1/2	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1/3	<input checked="" type="checkbox"/>

4. 导航到 **Secure Web Gateway** > 内容检查 > 内容检查配置文件。单击添加。



指定入站和出站 VLAN。

← Create ContentInspectionProfile

Profile Name*

Type*

Egress Interface*

Ingress Interface*

Egress Vlan

Ingress Vlan

创建另一个配置文件。在第二个配置文件中指定不同的入口和导出 VLAN。

← Create ContentInspectionProfile

Profile Name*

Type*

Egress Interface*

Ingress Interface*

Egress Vlan

Ingress Vlan

5. 导航到负载平衡 > 服务 > 添加并添加服务。在高级设置中，单击 配置文件。在 **CI** 配置文件名称 列表中，选择之前创建的内容检查配置文件。在“服务设置”中，将“使用源 IP 地址”设置为“是”，并将“使用代理端口”设置为“否”。在“基本设置”中，将“运行状况监视”设置为“否”。

创建两个服务。指定不属于任何设备（包括内联设备）所拥有的虚拟 IP 地址。在服务 1 中指定配置文件 1，在服务 2 中指定配置文件 2。

Profiles

Net Profile

 ?

TCP Profile

HTTP Profile

DNS Profile Name

CI Profile Name

 ?

Profiles

Net Profile

▼ Add ?

TCP Profile

▼ Add

HTTP Profile

▼ Add

DNS Profile Name

▼ Add

CI Profile Name

▼ Add ?

OK

Service Settings

Sure Connect		Use Source IP Address	YES
Surge Protection	OFF	Client Keep-Alive	NO
Use Proxy Port	NO	TCP Buffering	NO
Down State Flush	ENABLED	Insert Client IP Address	DISABLED
Access Down	NO	Header	client-ip

Basic Settings

Service Name	ips_service	Traffic Domain	0
Server Name	198.51.100.2	Number of Active Connections	-
IP Address	198.51.100.2	Hash ID	-
Server State	● UP	Server ID	None
Protocol	TCP	Cache Type	SERVER
Port	*	Cacheable	NO
Comments		Health Monitoring	NO
		AppFlow Logging	ENABLED
Monitoring Connection Close Bit	NONE		

6. 导航到负载平衡 > 虚拟服务器 > 添加。创建 TCP 负载平衡虚拟服务器。

Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address.
You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name*

Protocol*

IP Address Type*

IP Address*

Port*

► More

单击确定。

7. 在 负载均衡虚拟服务器服务绑定 部分内单击。在“服务绑定”中，单击“选择服务”中的箭头。选择之前创建的两个服务，然后单击“选择”。单击 **Bind**（绑定）。

Service Binding

Select Service*

Binding Details

Weight

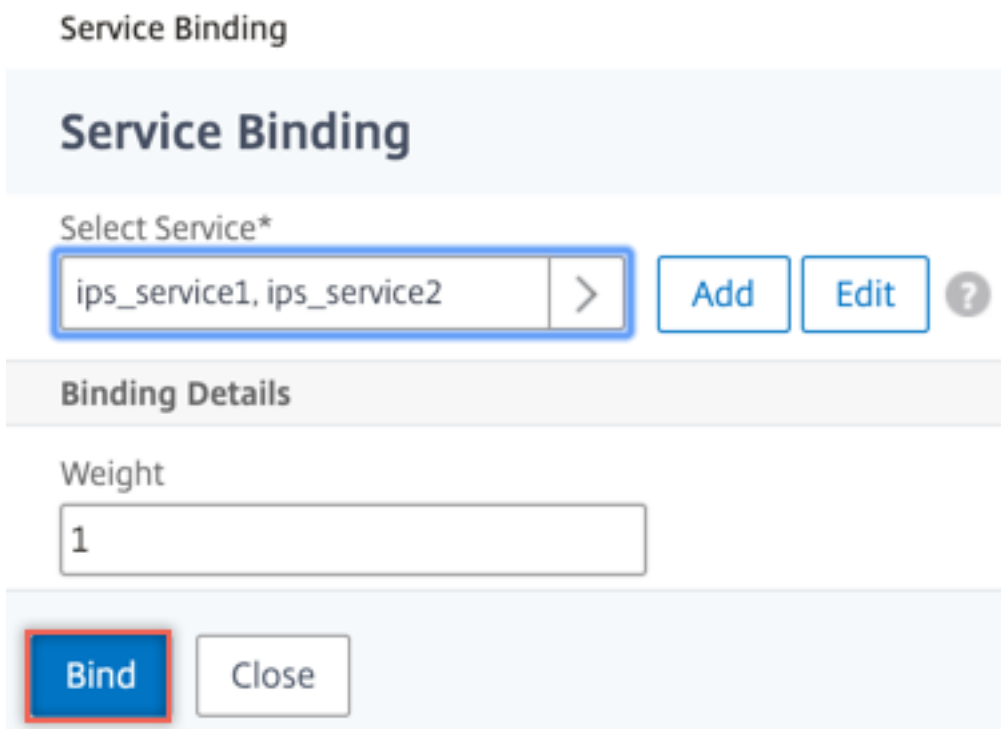
Service Binding / Service

Service

Select Add Edit

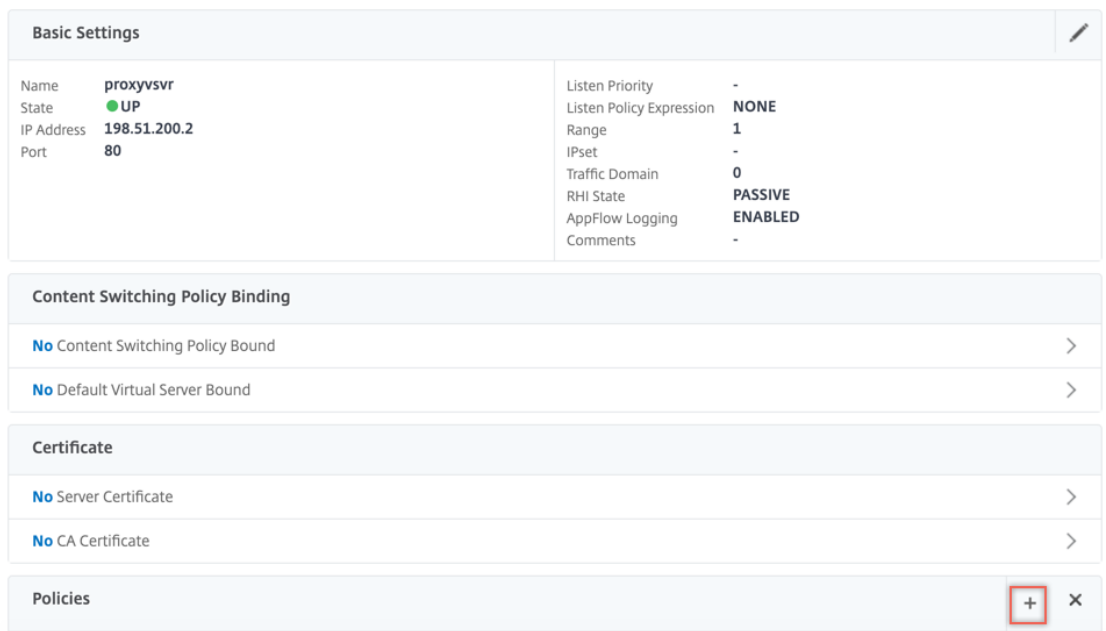
🔍 Click here to search or you can enter

<input type="checkbox"/>	Name
<input type="checkbox"/>	icap_svc
<input type="checkbox"/>	icap_domain1
<input type="checkbox"/>	ssltcp_svc1
<input type="checkbox"/>	s1
<input type="checkbox"/>	ips_service
<input checked="" type="checkbox"/>	ips_service1
<input checked="" type="checkbox"/>	ips_service2

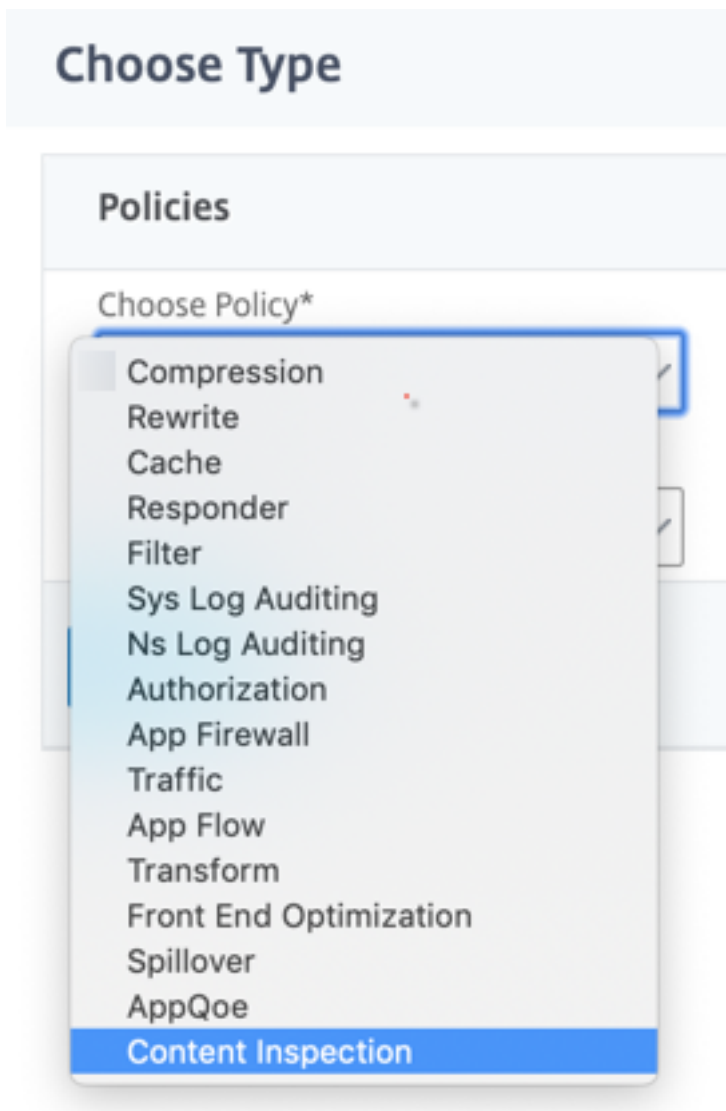


8. 导航到 **Secure Web Gateway > 代理虚拟服务器 > 添加**。指定名称、IP 地址和端口。在“高级设置”中，选择“策略”。点击“+”符号。

← Proxy Virtual Server



9. 在“选择策略”中，选择“内容检查”。单击继续。



10. 单击添加。指定名称。在“操作”中，单击“添加”。

[Choose Type](#) / Create ContentInspection Policy

Create ContentInspection Policy

Policy Name*

Action*

Log Action

UNDEF Action

11. 指定名称。在“类型”中，选择“在线检查”。在“服务器名称”中，选择之前创建的负载均衡虚拟服务器。

← Create ContentInspection Action

Name*

Type*

Server Name*

If Server Down

Request-Timeout

Request timeout action

12. 单击创建。指定规则，然后单击创建。

Configure ContentInspection Policy

Policy Name
ips_pol

Action*
ips_action Add Edit

Log Action
Add Edit

UNDEF Action

Expression* Expression Editor
Select Select Select
HTTP.REQ.METHOD.NE("CONNECT") Evaluate

Comment

OK Close

13. 单击 **Bind** (绑定)。

14. 单击完成。

分析

April 27, 2021

在 Citrix SWG 设备中，所有用户记录和后续记录都将被记录。当您将在 Citrix Application Delivery Management (ADM) 与 Citrix SWG 设备相集成时，将使用日志流将记录的用户活动和该设备中的后续记录导出到 Citrix ADM。

Citrix ADM 会整理和提供有关用户活动的信息，例如，所访问的 Web 站点和所占用的带宽。它还报告带宽使用和检测到的威胁，例如，恶意软件和钓鱼网站。您可以使用这些关键指标监视您的网络，并对 Citrix SWG 设备采取纠正措施。有关详细信息，请参阅 [Citrix Secure Web Gateway Analytics](#)。

要将 Citrix SWG 设备与 Citrix ADM 相集成，请执行以下操作：

1. 在 Citrix SWG 设备上，配置 Secure Web Gateway 时，启用“Analytics”（分析）并提供您要用于分析的 Citrix ADM 实例的详细信息。
2. 在 Citrix ADM 中，将 Citrix SWG 设备作为实例添加到 Citrix ADM。有关详细信息，请参阅 [将新实例添加到 Citrix ADM](#)。

用例：使企业 **Internet** 接入合规且安全

April 27, 2021

财务组织中的网络安全主管希望以恶意软件形式从 Web 抵御来自 Web 的任何外部威胁来保护企业网络。要执行此操作，主管需要在其他情况下能够看到其他跳过加密流量的情况，并控制对恶意 Web 站点的访问。董事必须执行以下操作：

- 拦截并检查进出企业网络的所有流量，包括 SSL/TLS（加密流量）。
- 跳过滤过包含敏感信息的 Web 站点的请求，例如，用户财务信息或电子邮件。
- 阻止访问被识别为有害或成人内容的有害 URL。
- 确定企业中的最终用户（员工），这些用户在访问恶意 Web 站点时阻止这些用户的 Internet 访问权限或阻止使用有害的 URL。

为了实现上述所有目标，主管可以在组织中的所有设备上设置代理，并将其指向 Citrix Secure Web Gateway (SWG)，后者充当网络中的代理服务器。代理服务器拦截通过企业网络传递的所有加密和未加密的流量。它会提示用户进行身份验证，并将流量与用户关联。可以指定 URL 类别以阻止对非法的或有害、成人、恶意软件和垃圾 Web 站点的访问。

要实现上述目标，请配置以下实体：

- DNS 名称服务器来解析主机名。
- 子网 IP (SNIP) 地址，用于与源服务器建立连接。SNIP 地址应具有 Internet 访问权限。
- 代理服务器以显式模式拦截所有出站 HTTP 和 HTTPS 流量。
- SSL 配置文件来定义连接的 SSL 设置，例如密码和参数。
- CA 证书 - 密钥对用于为 SSL 截获签名服务器证书。
- 用于定义要截获并跳过的 Web 站点的 SSL 策略。
- 身份验证虚拟服务器、策略和操作，以确保只授予有效用户的访问权限。
- 将数据发送到 Citrix Application Delivery Management (ADM) 的应用程序流收集器。

此示例配置列出 CLI 和 GUI 过程。使用以下示例值。将它们替换为 IP 地址、SSL 证书和密钥以及 LDAP 参数的有效数据。

名称	示例配置中使用的值
NSIP 地址	192.0.2.5
子网 IP 地址	198.51.100.5
LDAP 虚拟服务器 IP 地址	192.0.2.116
DNS 名称服务器 IP 地址	203.0.113.2
代理服务器 IP 地址	192.0.2.100
MAS IP 地址	192.0.2.41

名称	示例配置中使用的值
SSL 拦截的 CA 证书	ns-swg-ca-certkey (certificate: ns_swg_ca.crt and key: ns_swg_ca.key)
LDAP 基本 DN	CN=Users,DC=CTXNSSFB,DC=COM
LDAP 绑定 DN	CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM
LDAP 绑定 DN 密码	齐兹

使用 **Secure Web Gateway** 向导配置对企业网络流量的侦听与检查

创建拦截和检查加密流量的配置以及进出网络的其他流量需要配置代理设置、SSLi 设置、用户身份验证设置和 URL 筛选设置。以下过程包括所输入值的示例。

配置 **SNIP** 地址和 **DNS** 名称服务器

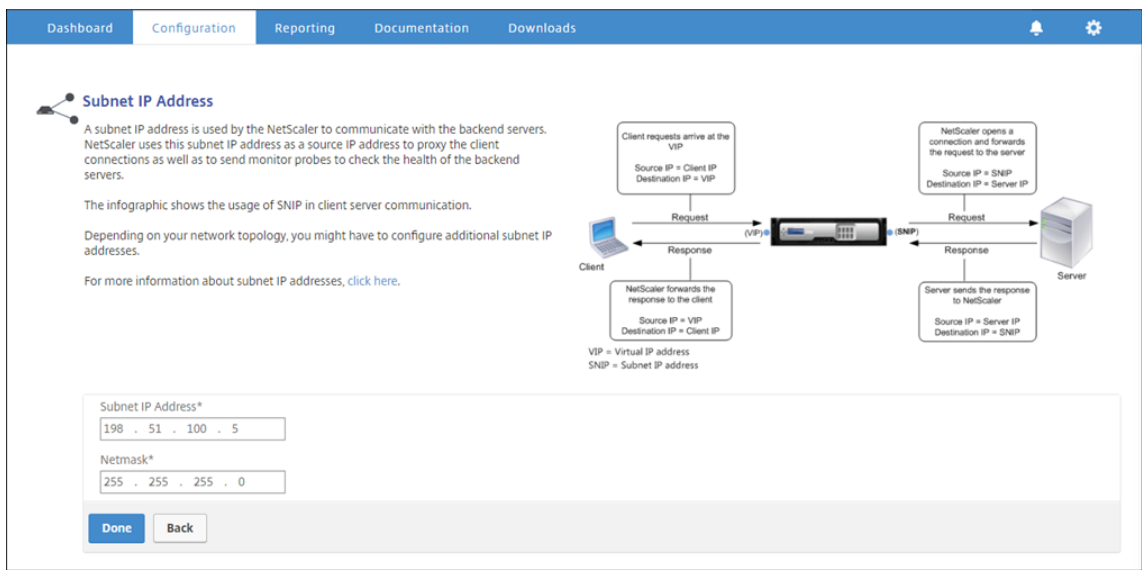
1. 在 Web 浏览器中，键入 NSIP 地址。例如 <http://192.0.2.5>。
2. 在 **User Name**（用户名）和 **Password**（密码）中，键入管理员凭据。此时将显示以下屏幕。

The screenshot shows the NetScaler configuration wizard interface. It has a navigation bar with 'Dashboard', 'Configuration', 'Reporting', 'Documentation', and 'Downloads'. The main content area is divided into several sections:

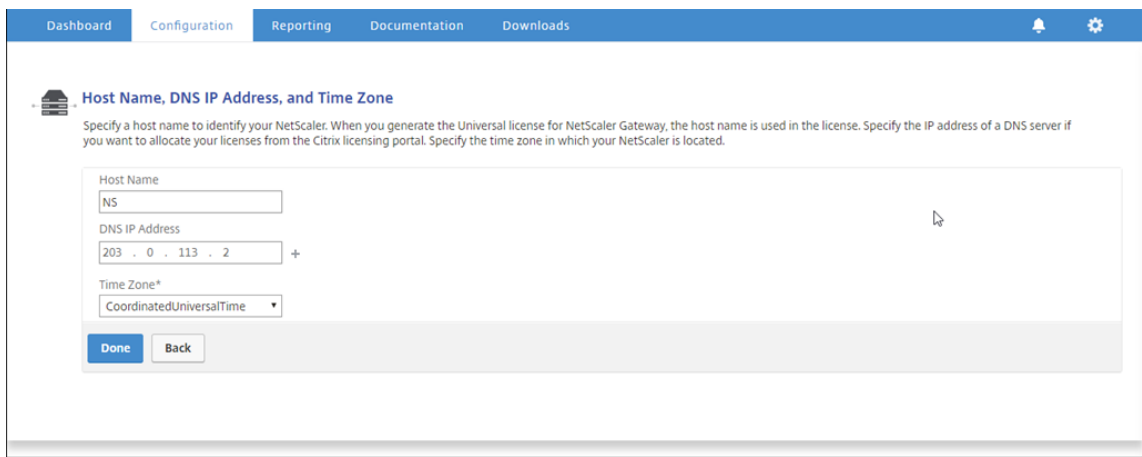
- NetScaler IP Address:** IP address at which you access the NetScaler for configuration, monitoring, and other management tasks. Fields: NetScaler IP Address (192.0.2.5), Netmask (255.255.255.0). Status: Green checkmark.
- Subnet IP Address:** Specify an IP address for your NetScaler to communicate with the backend servers. Field: Subnet IP Address (198.51.100.5). Status: Green checkmark.
- Host Name, DNS IP Address, and Time Zone:** Specify a host name to identify your NetScaler, an IP address for a DNS server to resolve domain names, and the time zone in which your NetScaler is located. Fields: Host Name (NS), DNS IP Address (203.0.113.2), Time Zone (CoordinatedUniversalTime). Status: Green checkmark.
- Licenses:** Upload licenses from your local computer or allocate licenses from the Citrix licensing portal. You can also allocate pooled capacity from an on-premise license server. There are 2 license file(s) present on this NetScaler. Status: 4 (indicating 4 steps or items).

A 'Continue' button is visible at the bottom left of the configuration area.

3. 单击内部子网 **IP** 地址部分，并输入 IP 地址。



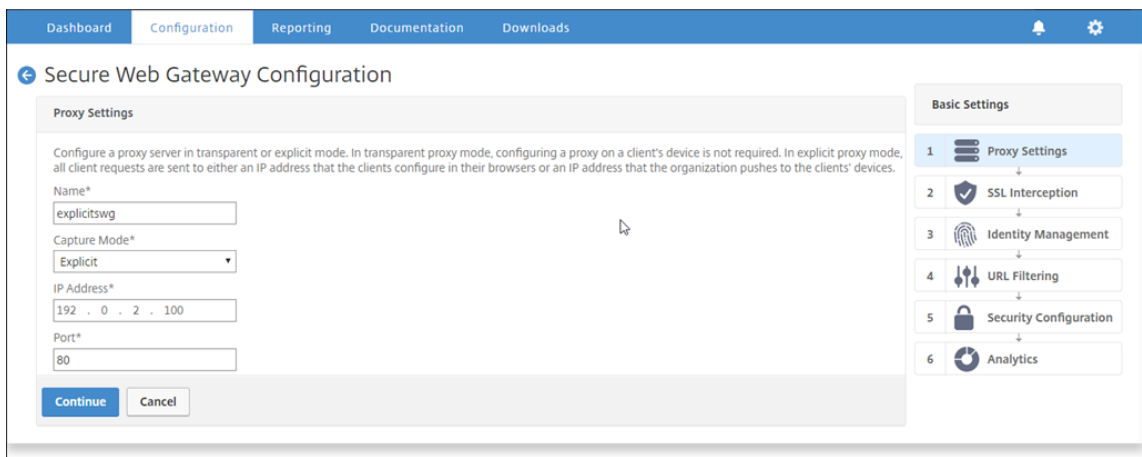
4. 单击完成。
5. 在主机名、**DNS IP** 地址和时区部分中单击，并为这些字段输入值。



6. 单击完成，然后单击继续。

配置代理设置

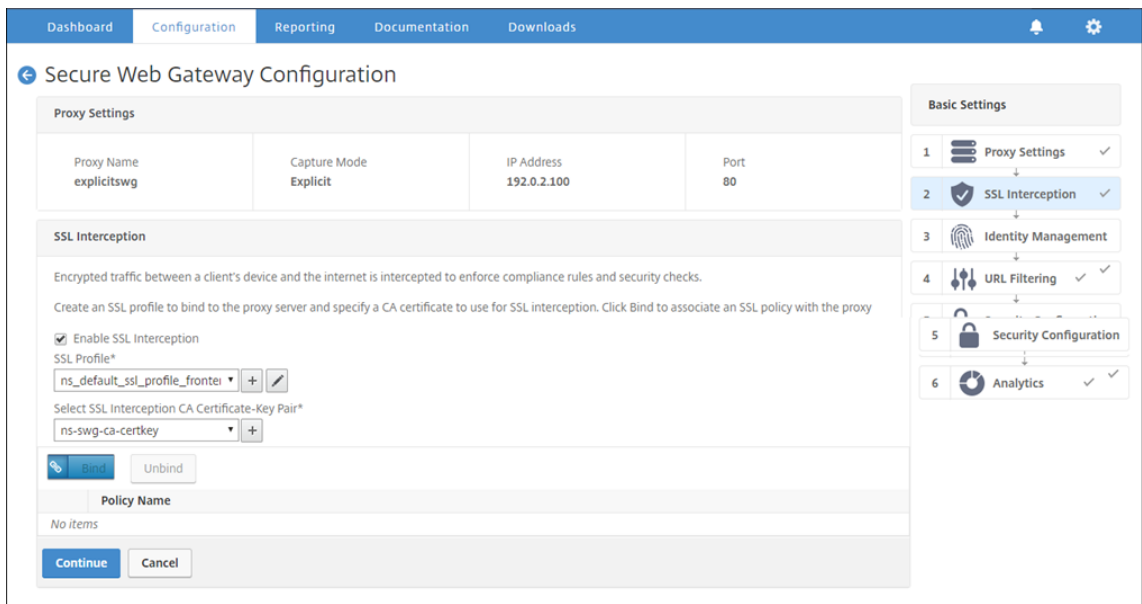
1. 导航到 **Secure Web Gateway > Secure Web Gateway** 向导。
2. 单击开始，然后单击继续。
3. 在“代理设置”对话框中，输入显式代理服务器的名称。
4. 对于 **Capture Mode**（捕获模式），请选择 **Explicit**（显式）。
5. 输入 IP 地址和端口号。



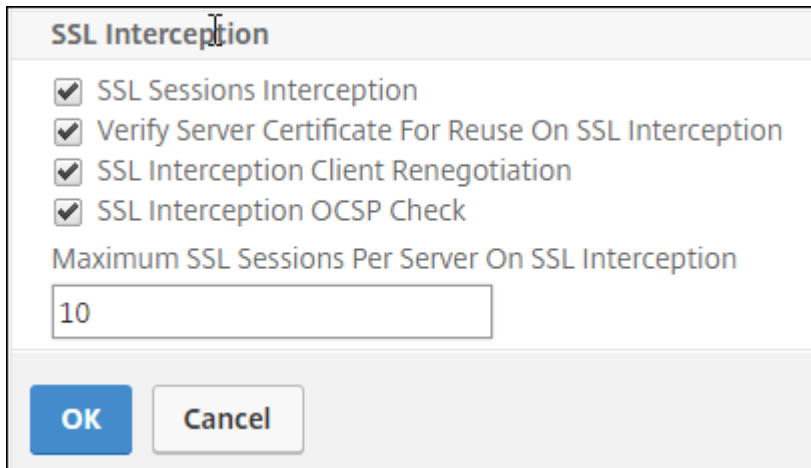
6. 单击继续。

配置 SSL 拦截设置

1. 选择 **Enable SSL Interception** (启用 SSL 拦截)。



2. 在 **SSL** 配置文件中，单击 “+” 以添加新的前端 SSL 配置文件，然后在此配置文件中启用 **SSL** 会话拦截。



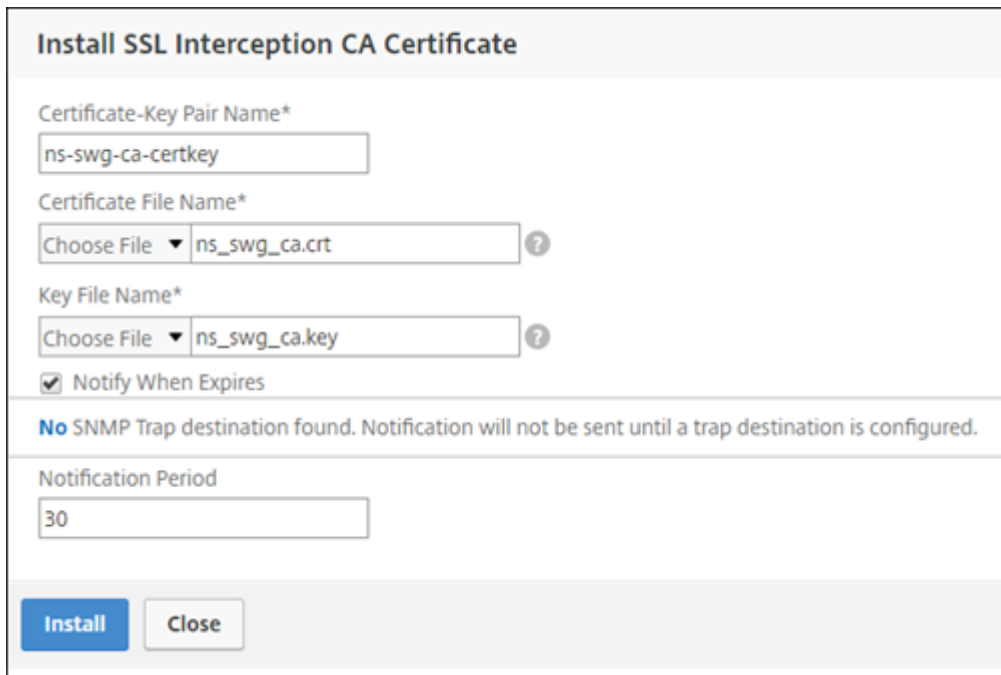
SSL Interception

- SSL Sessions Interception
- Verify Server Certificate For Reuse On SSL Interception
- SSL Interception Client Renegotiation
- SSL Interception OCSP Check

Maximum SSL Sessions Per Server On SSL Interception

OK **Cancel**

3. 单击 确定，然后单击 完成。
4. 在 选择 **SSL** 拦截 **CA** 证书密钥对中，单击 “+” 以安装用于 SSL 拦截的 CA 证书密钥对。



Install SSL Interception CA Certificate

Certificate-Key Pair Name*

Certificate File Name*
Choose File ▾ ns_swg_ca.crt ?

Key File Name*
Choose File ▾ ns_swg_ca.key ?

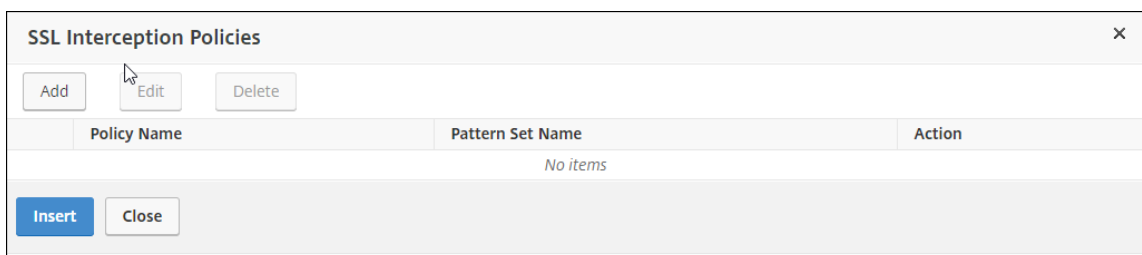
Notify When Expires

No SNMP Trap destination found. Notification will not be sent until a trap destination is configured.

Notification Period

Install **Close**

5. 单击 安装，然后单击 关闭。
6. 添加用于拦截所有流量的策略。单击 绑定，然后单击 添加。



SSL Interception Policies ×

Add Edit Delete

Policy Name	Pattern Set Name	Action
No items		

Insert **Close**

7. 输入策略的名称，然后选择“高级”。在表达式编辑器中，输入 true。

8. 对于操作，请选择 拦截。

The screenshot shows the 'SSL Interception Policy' configuration window. At the top, it says 'SSL Interception Policies / SSL Interception Policy'. Below that, the title is 'SSL Interception Policy'. A subtitle reads: 'Create a policy to intercept or bypass traffic on the basis of the defined URL category, pattern set, or URL reputation score.' The 'Name*' field is filled with 'ssl-pol'. There are four tabs: 'URL Categories', 'Create Patset', 'Security Configuration', and 'Advanced' (which is selected). Below the tabs is the 'Expression*' field, which contains 'true'. Above this field are three buttons: 'Operators', 'Saved Policy Expressions', and 'Frequently Used Expressions'. To the right of the expression field is an 'Expression Editor' icon. Below the expression field is an 'Evaluate' button. At the bottom, the 'Action*' dropdown is set to 'INTERCEPT'. There are 'Create' and 'Close' buttons at the very bottom.

9. 单击创建，然后单击添加以添加其他策略以绕过敏感信息。
10. 输入策略的名称，然后在 **URL** 类别中单击 添加。
11. 选择 财务 和 电子邮件 类别并将其移动到 已配置 列表。
12. 对于“操作”，请选择“绕过”。

SSL Interception Policies / SSL Interception Policy

SSL Interception Policy

Create a policy to intercept or bypass traffic on the basis of the defined URL category, pattern set, or URL reputation score.

Name*

URL Categories
 Create Patset
 Security Configuration
 Advanced

URL Categories*

Available (17) Select All

- Illegal/Harmful
- Adult
- Malware and SPAM
- Remote Proxies
- Search
- Business and Industry
- News/Entertainment/Society
- Gambling
- Messaging/Chat/Telephony

Configured (6) Remove All

- Market Rates
- Online Trading
- Insurance
- Financial Products
- Web based Mail
- E-Mail Subscriptions

Action*

13. 单击创建。

14. 选择之前创建的两个策略，然后单击“插入”。

SSL Interception Policies

SSL Interception Policies

<input checked="" type="checkbox"/>	Policy Name	Pattern Set Name	Action
<input checked="" type="checkbox"/>	ssli-pol_ssli		INTERCEPT
<input checked="" type="checkbox"/>	cat_pol1_ssli	cat_pol1_ssli_cat	BYPASS

15. 单击继续。

SSL Interception

Encrypted traffic between a client's device and the internet is intercepted to enforce compliance rules and security checks.

Create an SSL profile to bind to the proxy server and specify a CA certificate to use for SSL interception. Click Bind to associate an SSL policy with the proxy server.

Enable SSL Interception

SSL Profile*
ns_default_ssl_profile_frontend + ✎

Select SSL Interception CA Certificate-Key Pair*
ns-swg-ca-certkey +

<input type="checkbox"/>	Policy Name
<input type="checkbox"/>	ssl-pol_ssl
<input type="checkbox"/>	cat_pol1_ssl

配置用户身份验证设置

1. 选择启用户身份验证。在身份验证类型字段中，选择 **LDAP**。

Dashboard Configuration Reporting Documentation Downloads

Secure Web Gateway Configuration

Proxy Settings

Proxy Name explicitswg	Capture Mode Explicit	IP Address 192.0.2.100	Port 80
---------------------------	--------------------------	---------------------------	------------

SSL Interception

SSL Profile ns_default_ssl_profile_frontend	SSL Intercept CA CertKey YES
--	---------------------------------

Identity Management

Enable authentication to view user details in the logs and on the MAS dashboard.

Enable user authentication

Authentication Type*
LDAP

LDAP Server*
explicit-auth-server + ✎

Basic Settings

- 1 Proxy Settings ✓
- 2 SSL Interception ✓
- 3 Identity Management
- 4 URL Filtering ✓
- 5 Security Configuration
- 6 Analytics ✓

2. 添加 LDAP 服务器详细信息。

Create Authentication LDAP Server

Name*
explicit-auth-vs

Server Name Server IP

IP Address*
192 . 0 . 2 . 116

Security Type
PLAINTEXT

Port
389

Server Type
AD

Time-out (seconds)
3

Authentication

Connection Settings

Base DN (location of users)*
CN=Users,DC=CTXNSSFB,DC=COI

Administrator Bind DN*
CN=Administrator,CN=Users,DC=C

Administrator Password*
.....

Confirm Administrator Password*
.....

[Retrieve Attributes](#)

Test Connection

Other Settings

Server Logon Name Attribute
sAMAccountName

Search Filter

Group Attribute

Sub Attribute Name

SSO Name Attribute

Default Authentication Group

User Required
 Referrals

Maximum Referral Level
1

Referral DNS Lookup
A-REC

Validate LDAP Server Certificate

LDAP Host Name

OTP Secret

► More

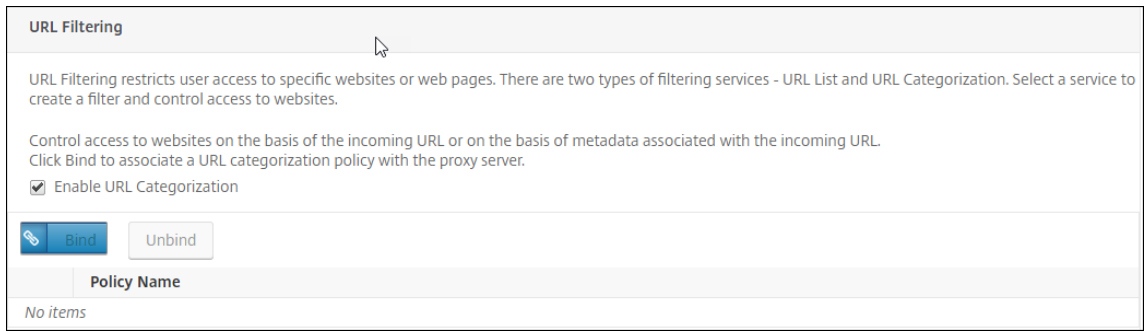
Create **Close**

3. 单击创建。

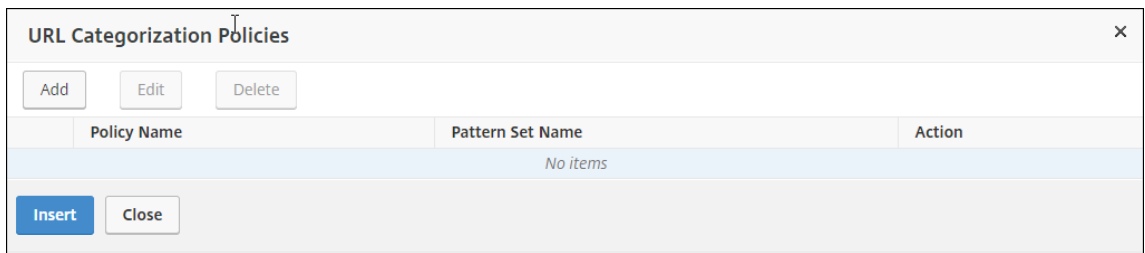
4. 单击继续。

配置 URL 过滤设置

1. 选择“启用 URL 分类”，然后单击“绑定”。



2. 单击添加。



3. 输入策略的名称。对于操作，请选择拒绝。对于 URL 类别，选择“非法/有害”、“成人”和“恶意软件”和“垃圾邮件”，然后将它们移至“已配置”列表。

URL Categorization Policies / URL Categorization Policy

URL Categorization Policy

Select Basic to choose from a predefined list of categories.
 Select Advanced to use the expression editor to create policy rules to suit your deployment.

Name*

Basic Advanced

Action*

URL Categories*

Available (16) Select All

- Remote Proxies
- Search
- Business and Industry
- News/Entertainment/Society
- Finance
- Gambling
- Messaging/Chat/Telephony
- Email
- Social Networking

Configured (29) Remove All

- Illegal Activities
- Illegal Drugs
- Medication
- Terrorism/Extremists
- Weapons
- Hate/Slander
- Violence/Suicide
- Advocacy in general
- Adult/Porn
- Nudity
- Sexual Services
- Adult Search/Links
- Dating
- Grotesque

4. 单击创建。
5. 选择策略，然后单击 插入。

URL Categorization Policies

URL Categorization Policies

✕

Add Edit Delete

<input checked="" type="checkbox"/>	Policy Name	Pattern Set Name	Action
<input checked="" type="checkbox"/>	cat_pol2_url_cat	cat_pol2_patset	DROP

6. 单击继续。

URL Filtering

URL Filtering restricts user access to specific websites or web pages. There are two types of filtering services - URL List and URL Categorization. Select a service to create a filter and control access to websites.

Control access to websites on the basis of the incoming URL or on the basis of metadata associated with the incoming URL.
Click Bind to associate a URL categorization policy with the proxy server.

Enable URL Categorization

Enable URL List

<input checked="" type="checkbox"/>	Policy Name
<input checked="" type="checkbox"/>	cat_pol2_url_cat

Continue **Cancel**

7. 单击继续。
8. 单击 启用分析。
9. 输入 Citrix ADM 的 IP 地址和端口，指定 5557。

Analytics

Enable Analytics to monitor the outbound traffic and user transactions by using NetScaler Management and Analytics System (MAS). To view the metrics, make sure that you add the NetScaler SWG appliance as an instance to NetScaler MAS.

Enable Analytics

NetScaler MAS IP Address*

192 . 0 . 2 . 41

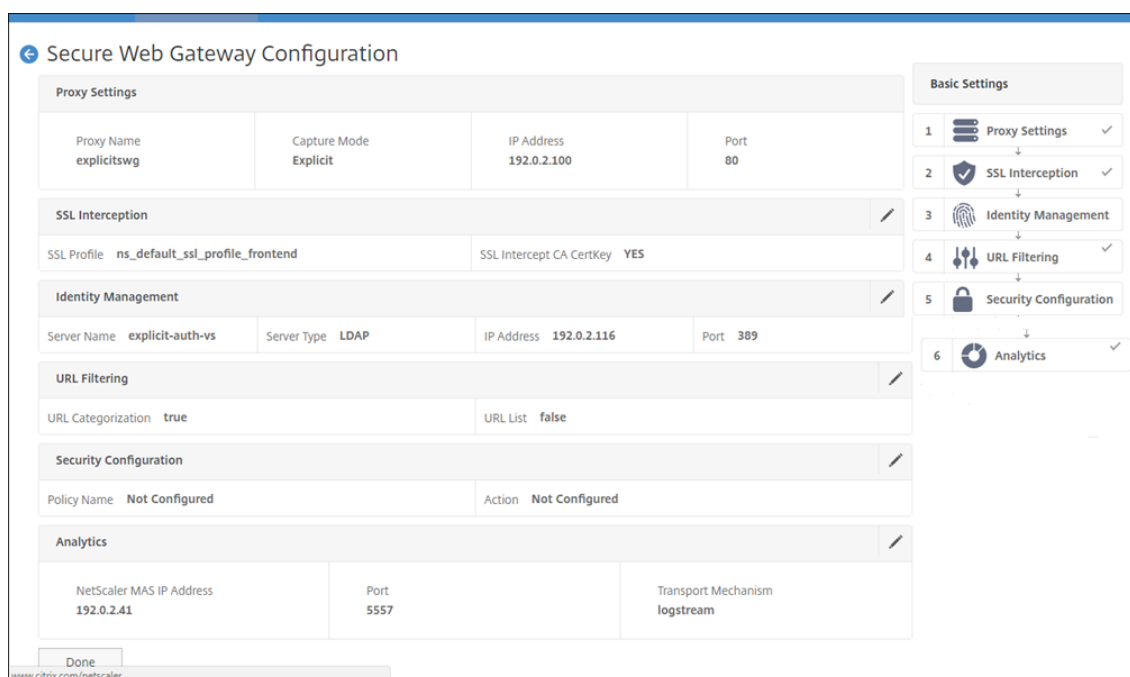
Port*

5557

Transport Mechanism: LogStream

Continue **Cancel**

10. 单击继续。
11. 单击完成。



使用 Citrix ADM 查看用户的主要衡量指标，并确定以下各项：

- 企业中用户的浏览行为。
- 您企业中的用户访问的 URL 类别。
- 用于访问 URL 或域的浏览器。

使用此信息可确定用户的系统是否受到恶意软件的感染，或了解用户的带宽消耗模式。您可以对 Citrix SWG 设备上的策略进行微调，以限制这些用户或阻止某些更多的 Web 站点。有关在 MAS 上查看衡量指标的详细信息，请参阅[MAS 用例](#)中的“检查端点”用例。

注意

使用 CLI 设置以下参数。

```

1 set syslogparams -sslInterception ENABLED
2
3 set cacheparameter -memLimit 100
4
5 set appflow param -AAAUserName ENABLED
6 <!--NeedCopy-->

```

CLI 示例

以下示例包括用于配置拦截和检查进出企业网络的流量的所有命令。

一般配置：

```
1 add ns ip 192.0.2.5 255.255.255.0
2
3 add ns ip 198.51.100.5 255.255.255.0 -type SNIP
4
5 add dns nameServer 203.0.113.2
6
7 add ssl certKey ns-swg-ca-certkey -cert ns_swg_ca.crt -key
  ns_swg_ca.key
8
9 set syslogparams -sslInterception ENABLED
10
11 set cacheparameter -memLimit 100
12
13 set appflow param -AAAUserName ENABLED
14 <!--NeedCopy-->
```

身份验证配置:

```
1 add authentication vserver explicit-auth-vs SSL
2
3 bind ssl vserver explicit-auth-vs -certkeyName ns-swg-ca-certkey
4
5 add authentication ldapAction swg-auth-action-explicit -serverIP
  192.0.2.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "CN=
  Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
  zzzzzz -ldapLoginName sAMAccountName
6
7 add authenticationpolicy swg-auth-policy -rule true -action swg-auth-
  action-explicit
8
9 bind authentication vserver explicit-auth-vs -policy swg-auth-policy -
  priority 1
10 <!--NeedCopy-->
```

代理服务器和 SSL 截获配置:

```
1 add cs vserver explicitswg PROXY 192.0.2.100 80 - Authn401 ENABLED -
  authnVsName explicit-auth-vs
2
3 set ssl parameter -defaultProfile ENABLED
4
5 add ssl profile swg_profile -sslInterception ENABLED
6
7 bind ssl profile swg_profile -ssliCACertkey ns-swg-ca-certkey
8
9 set ssl vserver explicitswg -sslProfile swg_profile
10
11 add ssl policy ssli-pol_ssli -rule true -action INTERCEPT
12
13 bind ssl vserver explicitswg -policyName ssli-pol_ssli -priority 100 -
  type INTERCEPT_REQ
14 <!--NeedCopy-->
```

URL 类别配置:

```

1 add ssl policy cat_pol1_ssli -rule "client.ssl.client_hello.SNI.
    URL_CATEGORIZE(0,0).GROUP.EQ("Finance") || client.ssl.client_hello.
    SNI.URL_CATEGORIZE(0,0).GROUP.EQ("Email")" -action BYPASS
2
3 bind ssl vserver explicitSWG -policyName cat_pol1_ssli -priority 10 -
    type INTERCEPT_REQ
4
5 add ssl policy cat_pol2_ssli -rule "client.ssl.client_hello.sni.
    url_categorize(0,0).GROUP.EQ("Adult") || client.ssl.client_hello.sni.
    url_categorize(0,0).GROUP.EQ("Malware and SPAM") || client.ssl.
    client_hello.SNI.URL_CATEGORIZE(0,0).GROUP.EQ("Illegal/Harmful")" -
    action RESET
6
7 bind ssl vserver explicitSWG -policyName cat_pol2_ssli -priority 20 -
    type INTERCEPT_REQ
8 <!--NeedCopy-->

```

AppFlow 配置, 用于将数据提取到 **Citrix ADM** 中:

```

1 add appflow collector _swg_testSWG_apfw_cl -IPAddress 192.0.2.41 -port
    5557 -Transport logstream
2
3 set appflow param -templateRefresh 60 -httpUrl ENABLED -AAAUserName
    ENABLED -httpCookie ENABLED -httpReferer ENABLED -httpMethod ENABLED
    -httpHost ENABLED -httpUserAgent ENABLED -httpContentType ENABLED -
    httpVia ENABLED -httpLocation ENABLED -httpDomain ENABLED -
    cacheInsight ENABLED -urlCategory ENABLED
4
5 add appflow action _swg_testSWG_apfw_act -collectors
    _swg_testSWG_apfw_cl -distributionAlgorithm ENABLED
6
7 add appflow policy _swg_testSWG_apfw_pol true _swg_testSWG_apfw_act
8
9 bind cs vserver explicitSWG -policyName _swg_testSWG_apfw_pol -priority
    1
10 <!--NeedCopy-->

```

用例: 通过使用 ICAP 远程恶意软件检查, 确保企业网络安全

April 27, 2021

Citrix Secure Web Gateway (SWG) 设备充当代理并拦截所有客户端流量。设备使用策略评估流量并将客户端请求转发到资源所在的源服务器。设备解密来自源服务器的响应, 并将纯文本内容转发到 ICAP 服务器进行反恶意软件检查。ICAP 服务器会回应一条消息, 指示“无需适应”、错误或已修改的请求。根据来自 ICAP 服务器的响应, 请求的内容将转发到客户端, 或发送适当的消息。

对于此使用案例, 您必须在 Citrix SWG 设备上执行一些常规配置、代理和 SSL 拦截相关的配置以及 ICAP 配置。

一般配置

配置以下实体：

- NSIP 地址
- 子网 IP (SNIP) 地址
- 域名服务器
- CA 证书-密钥对用于为 SSL 截获签名服务器证书

代理服务器和 **SSL** 截获配置

配置以下实体：

- 代理服务器以显式模式拦截所有出站 HTTP 和 HTTPS 流量。
- SSL 配置文件来定义连接的 SSL 设置，例如密码和参数。
- 用于定义截获流量的规则的 SSL 策略。设置为 true 以拦截所有客户端请求。

有关更多详细信息，请参阅以下主题：

- [代理模式](#)
- [SSL 拦截](#)

在以下示例配置中，反恶意软件检测服务位于 www.example.com。

常规配置示例：

```
1 add ns ip 192.0.2.5 255.255.255.0
2
3 add ns ip 198.51.100.5 255.255.255.0 -type SNIP
4
5 add dns nameServer 203.0.113.2
6
7 add ssl certKey ns-swg-ca-certkey -cert ns_swg_ca.crt -key ns_swg_ca.
  key
8 <!--NeedCopy-->
```

代理服务器和 **SSL** 截获配置示例：

```
1 add cs vserver explicitSWG PROXY 192.0.2.100 80 - Authn401 ENABLED -
  authnVsName explicit-auth-vs
2
3 set ssl parameter -defaultProfile ENABLED
4
5 add ssl profile swg_profile -sslInterception ENABLED
6
7 bind ssl profile swg_profile -ssliCACertkey ns-swg-ca-certkey
8
9 set ssl vserver explicitSWG -sslProfile swg_profile
10
```

```

11 add ssl policy ssl-pol_ssl_i -rule true -action INTERCEPT
12
13 bind ssl vserver explicitSWG -policyName ssl-pol_ssl_i -priority 100 -
    type INTERCEPT_REQ
14 <!--NeedCopy-->

```

会计师协会配置示例：

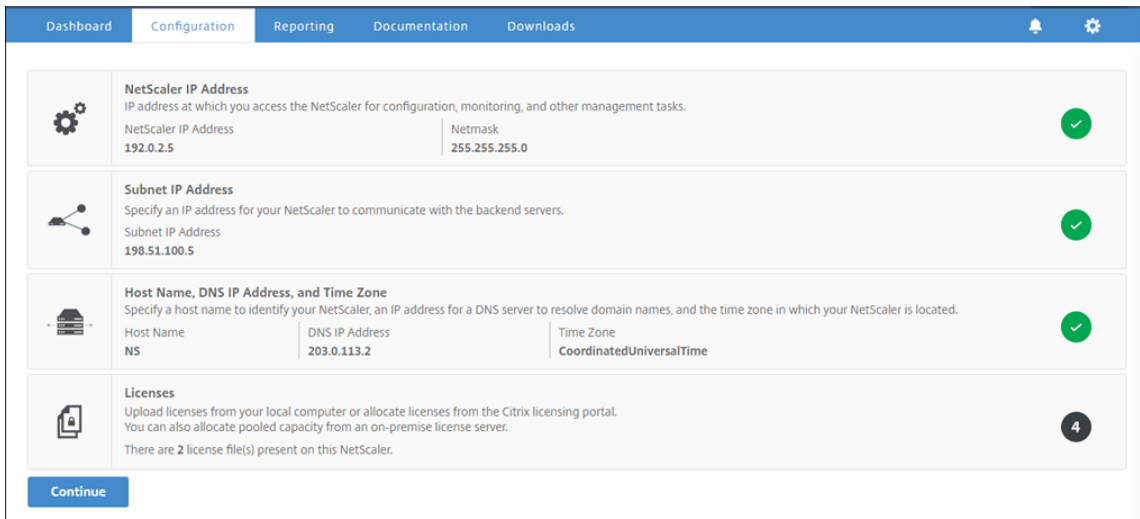
```

1 add service icap_svc 203.0.113.225 TCP 1344
2
3 enable ns feature contentinspection
4
5 add icaprofile icaprofile1 -uri /example.com -Mode RESMOD
6
7 add contentInspection action CiRemoteAction -type ICAP -serverName
    icap_svc -icapProfileName icaprofile1
8
9 add contentInspection policy CiPolicy -rule "HTTP.REQ.METHOD.NE("
    CONNECT")" -action CiRemoteAction
10
11 bind cs vserver explicitSWG -policyName CiPolicy -priority 200 -type
    response
12 <!--NeedCopy-->

```

配置 SNIP 地址和 DNS 名称服务器

1. 在 Web 浏览器中，键入 NSIP 地址。例如 <http://192.0.2.5>。
2. 在 **User Name** (用户名) 和 **Password** (密码) 中，键入管理员凭据。此时将显示以下屏幕。如果未出现以下屏幕，请跳至代理设置部分。

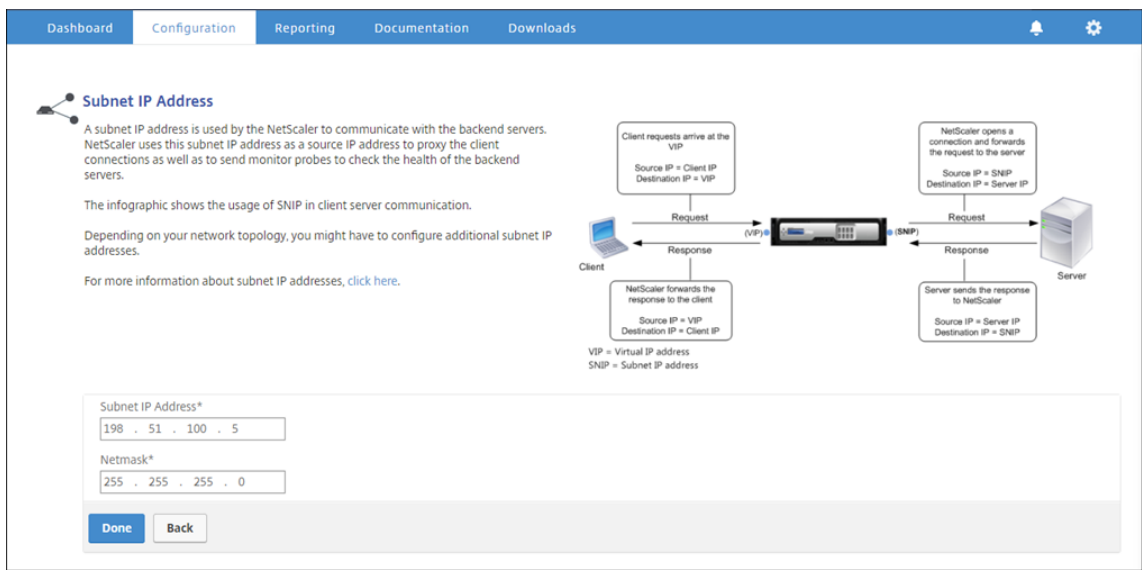


The screenshot shows the 'Configuration' tab in the NetScaler management interface. It displays several configuration sections:

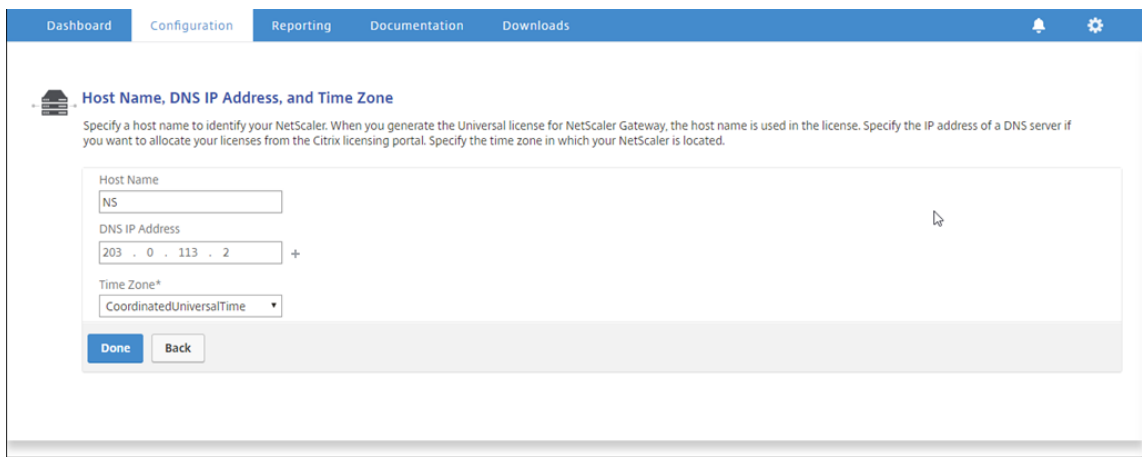
- NetScaler IP Address:** IP address at which you access the NetScaler for configuration, monitoring, and other management tasks. Fields: NetScaler IP Address (192.0.2.5), Netmask (255.255.255.0). Status: Green checkmark.
- Subnet IP Address:** Specify an IP address for your NetScaler to communicate with the backend servers. Field: Subnet IP Address (198.51.100.5). Status: Green checkmark.
- Host Name, DNS IP Address, and Time Zone:** Specify a host name to identify your NetScaler, an IP address for a DNS server to resolve domain names, and the time zone in which your NetScaler is located. Fields: Host Name (NS), DNS IP Address (203.0.113.2), Time Zone (CoordinatedUniversalTime). Status: Green checkmark.
- Licenses:** Upload licenses from your local computer or allocate licenses from the Citrix licensing portal. You can also allocate pooled capacity from an on-premise license server. There are 2 license file(s) present on this NetScaler. Status: 4 (indicating 4 licenses).

A 'Continue' button is visible at the bottom left of the configuration area.

3. 单击内部子网 **IP** 地址部分，并输入 IP 地址。



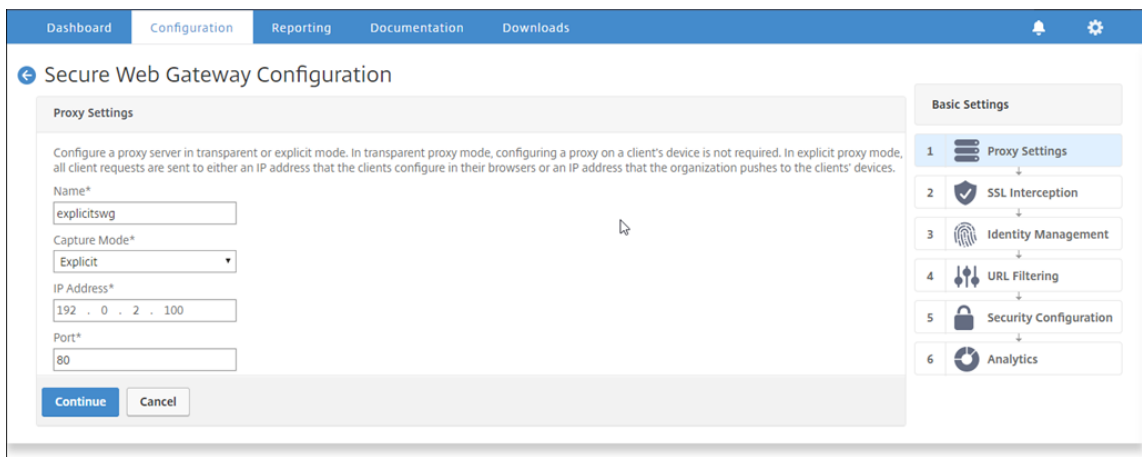
4. 单击完成。
5. 在主机名、**DNS IP** 地址和时区部分中单击，并为这些字段输入值。



6. 单击完成，然后单击继续。

配置代理设置

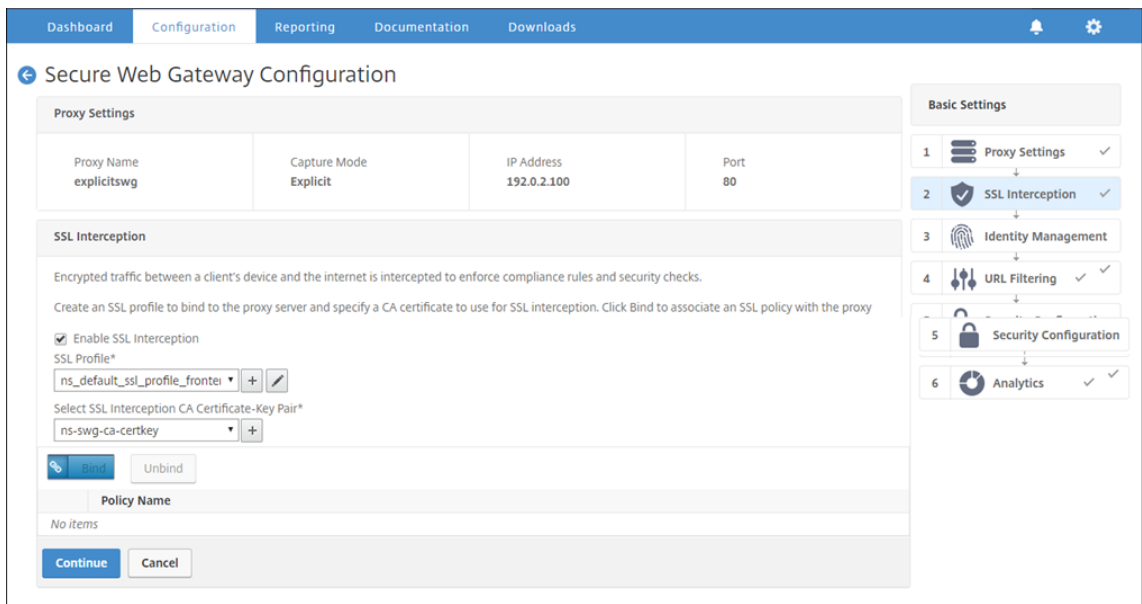
1. 导航到 **Secure Web Gateway > Secure Web Gateway** 向导。
2. 单击开始，然后单击继续。
3. 在“代理设置”对话框中，输入显式代理服务器的名称。
4. 对于 **Capture Mode**（捕获模式），请选择 **Explicit**（显式）。
5. 输入 IP 地址和端口号。



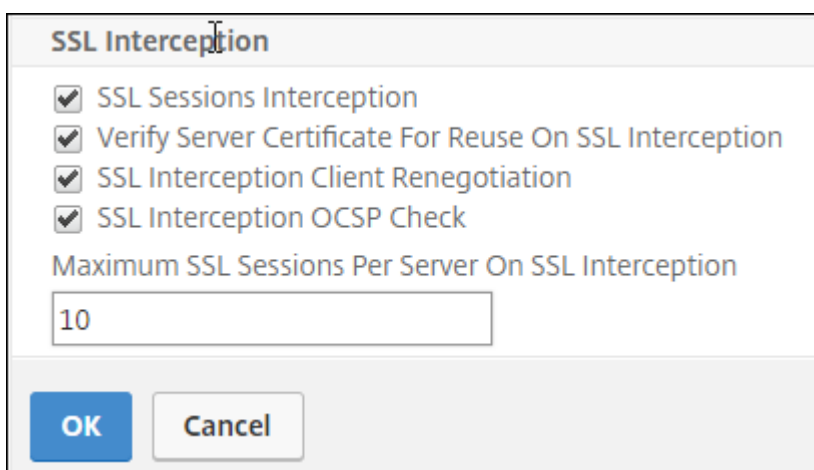
6. 单击继续。

配置 SSL 拦截设置

1. 选择 **Enable SSL Interception** (启用 SSL 拦截)。

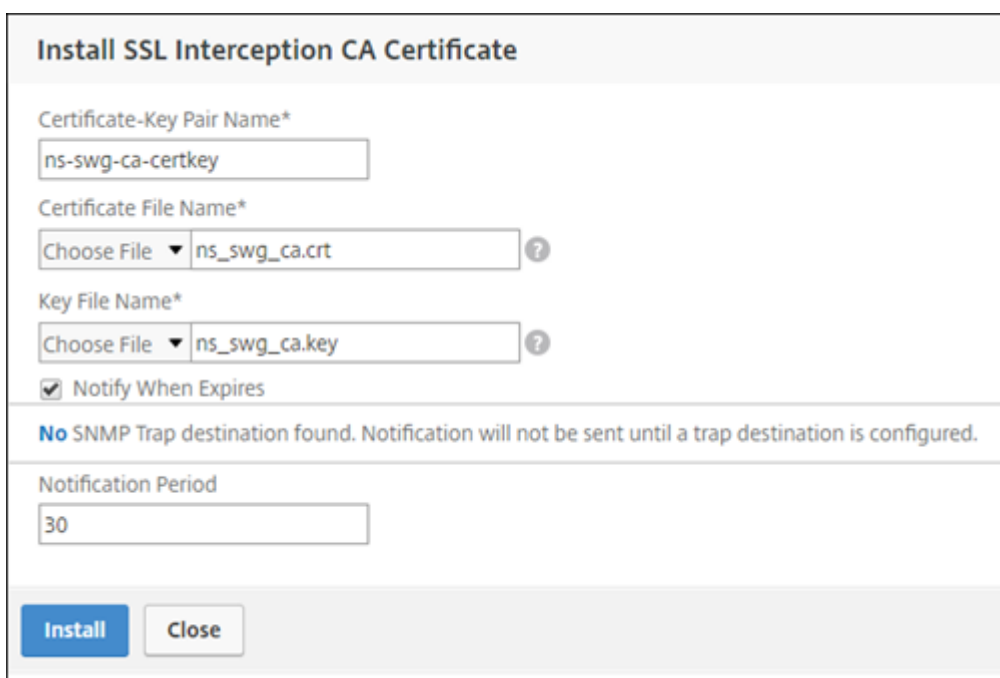


2. 在 **SSL** 配置文件中，选择现有配置文件或单击“+”以添加新的前端 SSL 配置文件。在此配置文件中启用 **SSL** 会话拦截。如果您选择现有配置文件，请跳过下一步。



The screenshot shows a dialog box titled "SSL Interception". It contains four checked checkboxes: "SSL Sessions Interception", "Verify Server Certificate For Reuse On SSL Interception", "SSL Interception Client Renegotiation", and "SSL Interception OCSP Check". Below these is a text input field labeled "Maximum SSL Sessions Per Server On SSL Interception" with the value "10". At the bottom are "OK" and "Cancel" buttons.

3. 单击 确定，然后单击 完成。
4. 在 选择 **SSL** 拦截 **CA** 证书密钥对中，选择现有证书或单击 “+” 以安装用于 SSL 拦截的 CA 证书密钥对。如果选择现有证书，请跳过下一步。



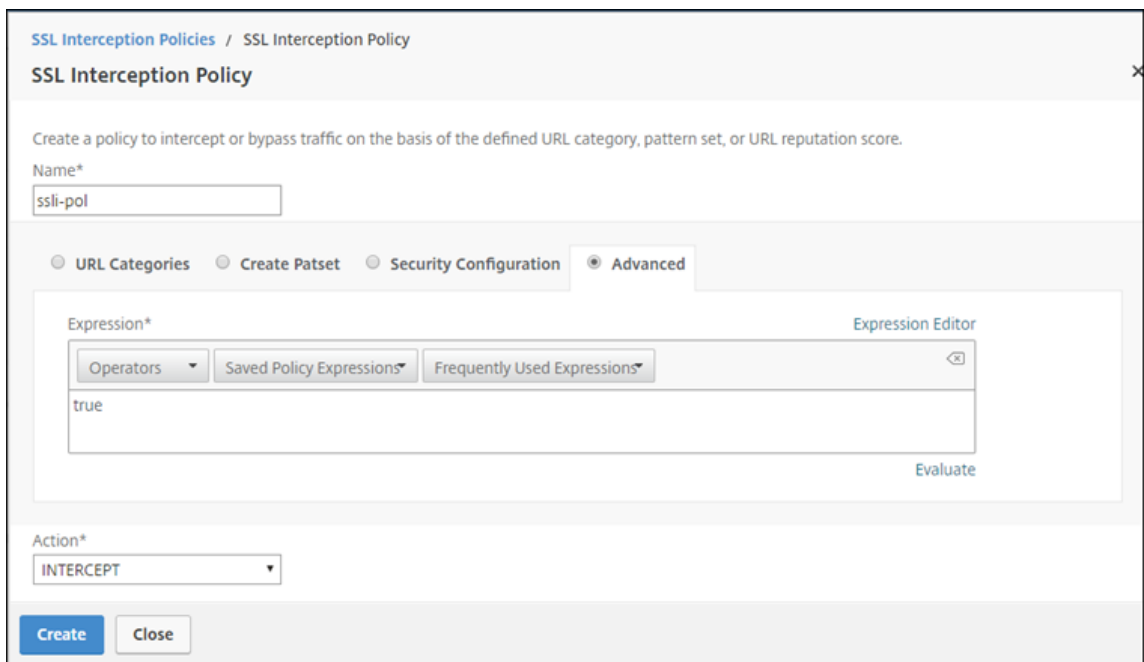
The screenshot shows a dialog box titled "Install SSL Interception CA Certificate". It has several fields: "Certificate-Key Pair Name*" with the value "ns-swg-ca-certkey"; "Certificate File Name*" with a "Choose File" dropdown and the value "ns_swg_ca.crt"; "Key File Name*" with a "Choose File" dropdown and the value "ns_swg_ca.key"; and a checked checkbox "Notify When Expires". A message states: "No SNMP Trap destination found. Notification will not be sent until a trap destination is configured." Below this is a "Notification Period" field with the value "30". At the bottom are "Install" and "Close" buttons.

5. 单击 安装，然后单击 关闭。
6. 添加用于拦截所有流量的策略。单击 **Bind** (绑定)。单击 “添加” 以添加新策略或选择现有策略。如果选择现有策略，请单击 “插入”，然后跳过后续三个步骤。



7. 输入策略的名称，然后选择“高级”。在表达式编辑器中，输入 true。

8. 对于操作，请选择 拦截。

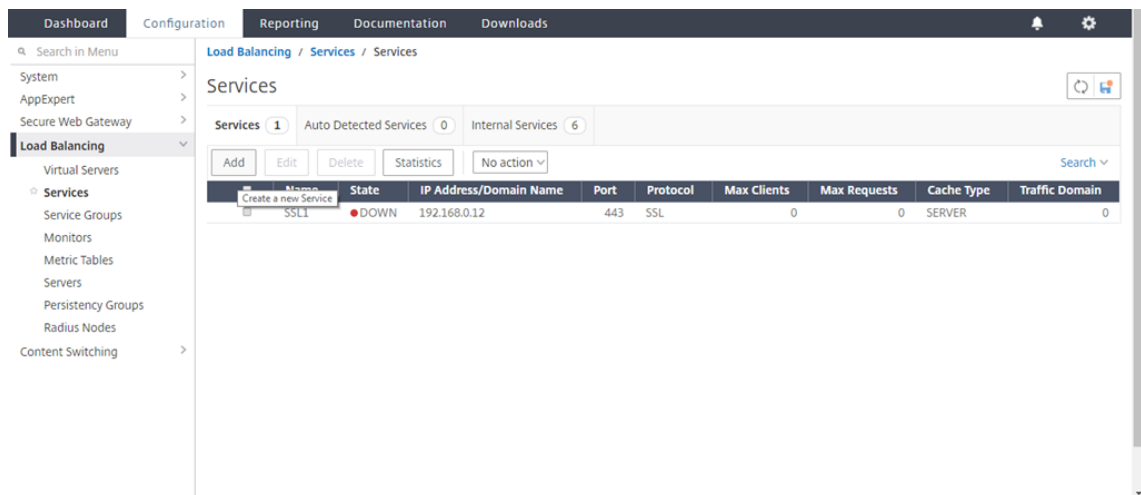


9. 单击创建。

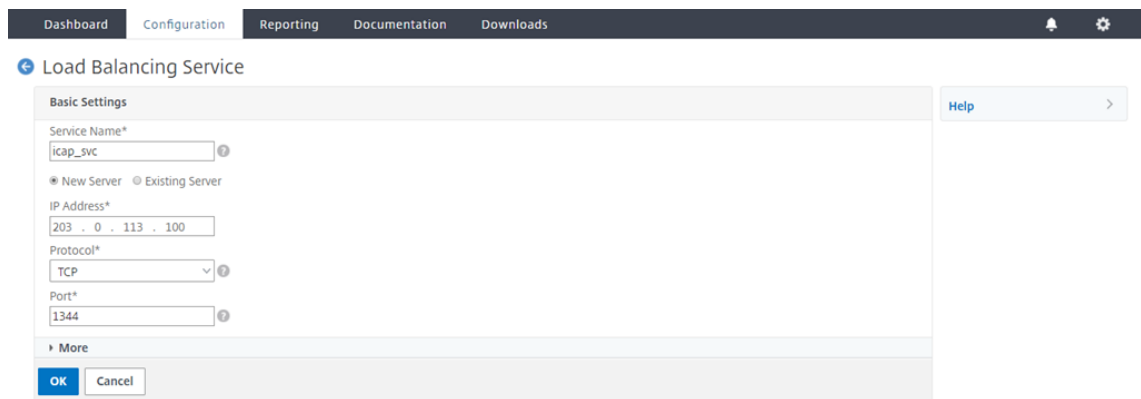
10. 单击 继续 四次，然后单击 完成。

配置会计师事务所设置

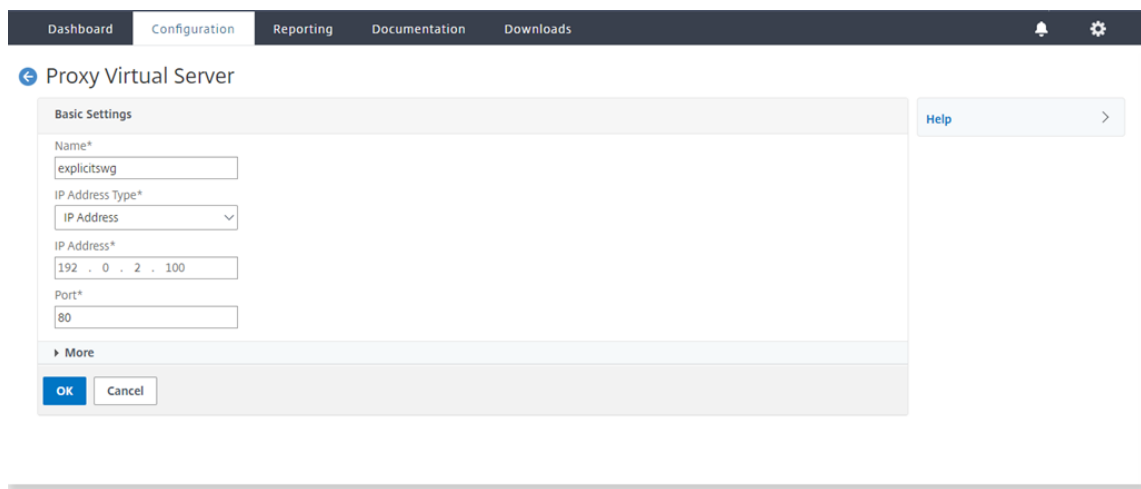
1. 导航至“负载均衡” > “服务”，然后单击“添加”。



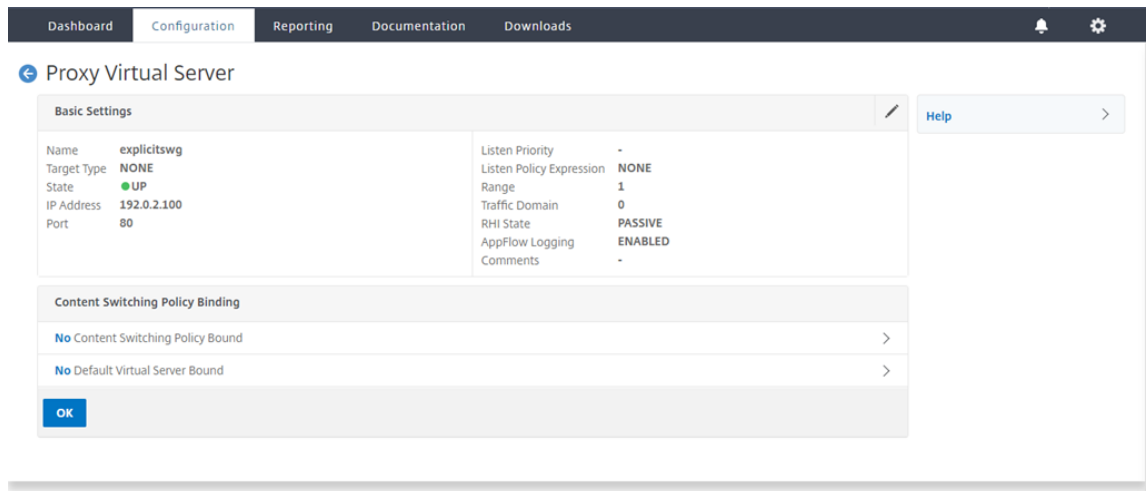
2. 键入名称和 IP 地址。在协议中，选择 **TCP**。在港口，键入 **1344**。单击确定。



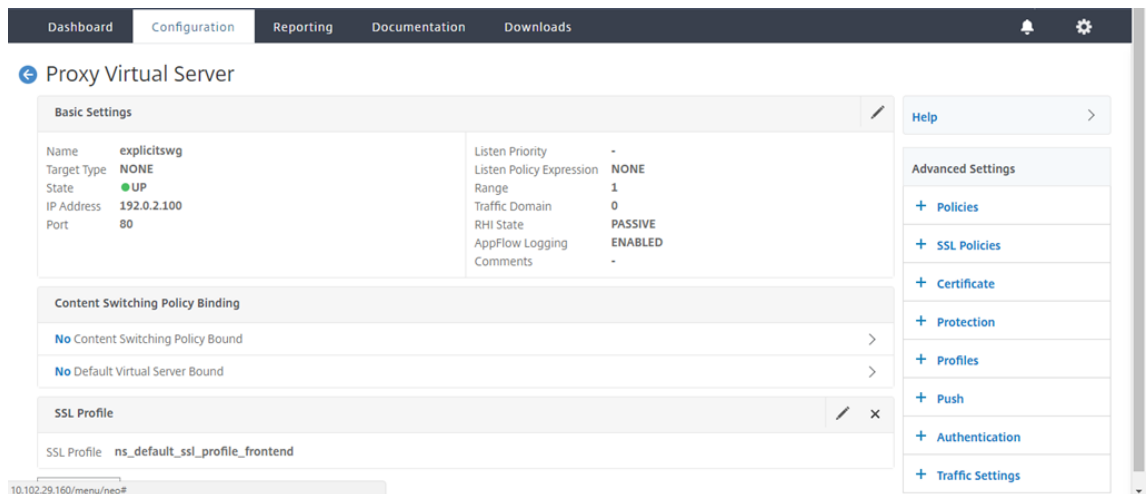
3. 导航到 **Secure Web Gateway > Proxy Virtual Servers**（代理虚拟服务器）。添加代理虚拟服务器或选择虚拟服务器，然后单击“编辑”。输入详细信息后，点击 确定。



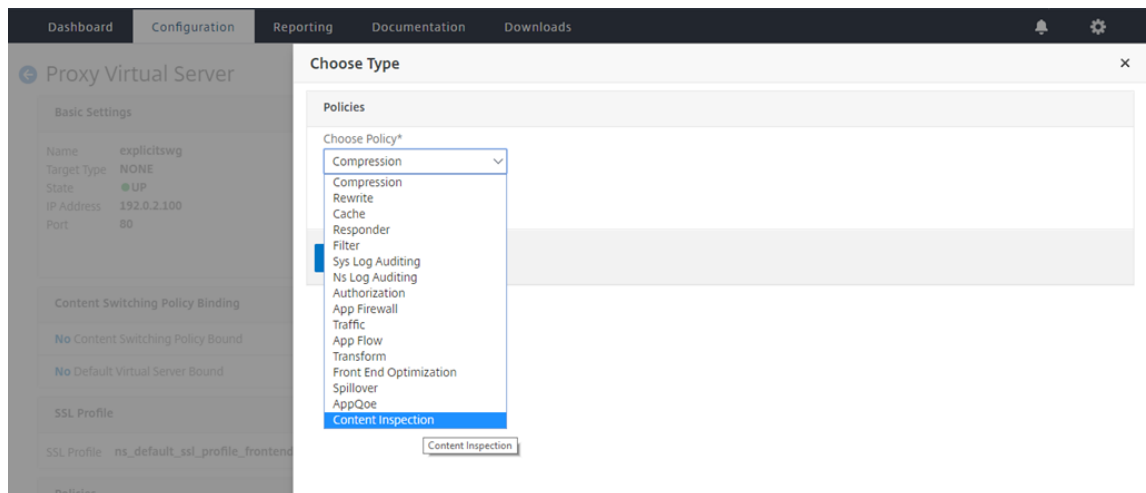
再次点击确定。



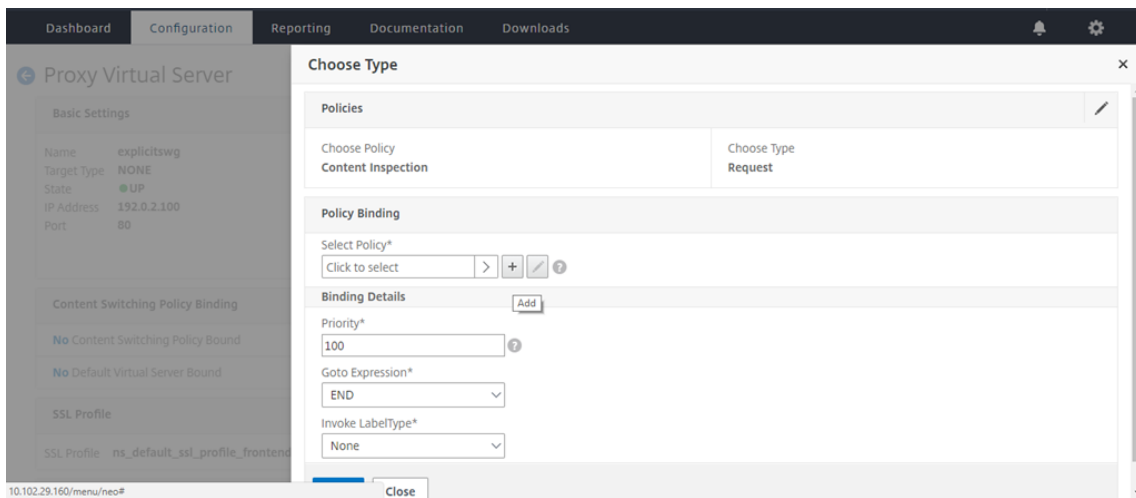
4. 在“高级设置”中，单击“策略”。



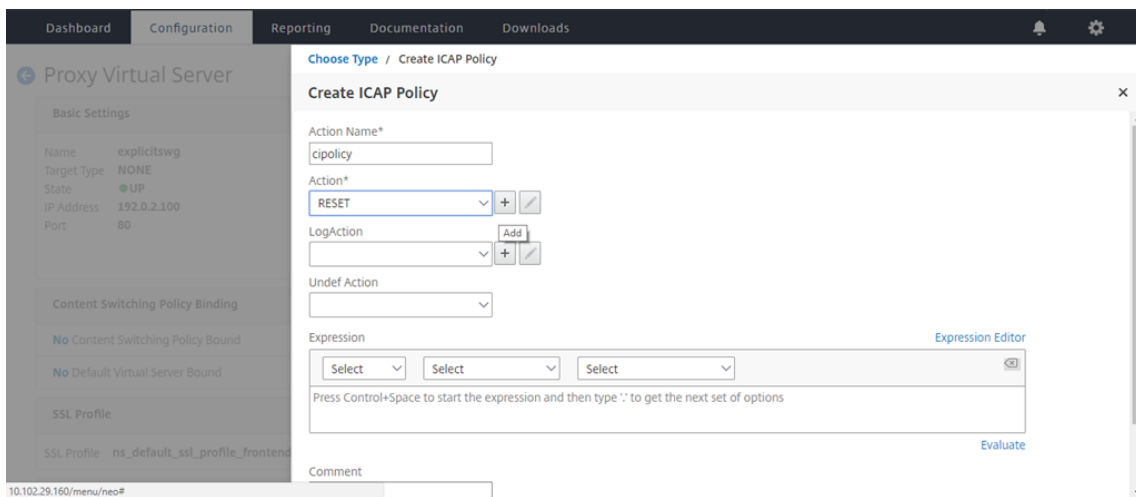
5. 在“选择策略”中，选择“内容检查”。单击继续。



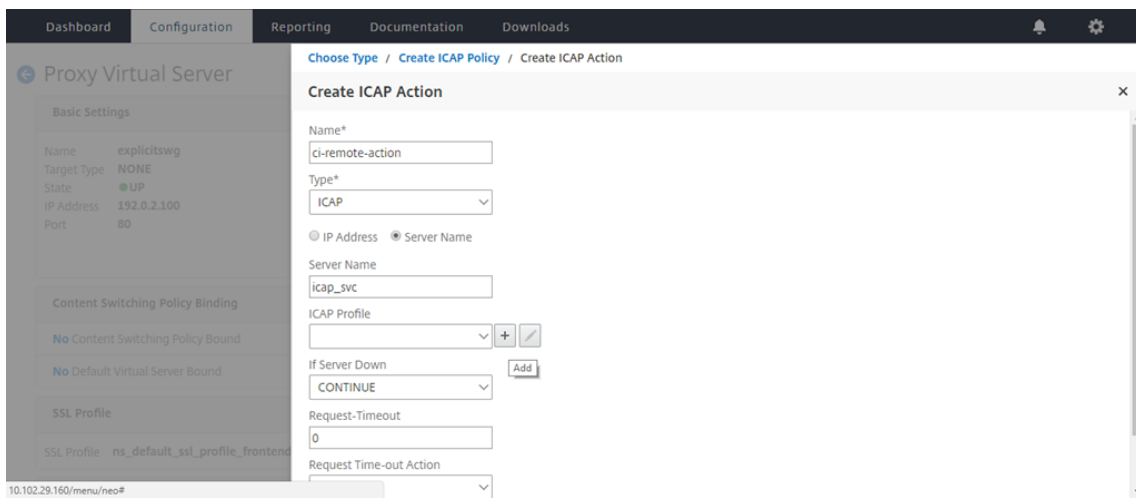
6. 在选择策略中，单击“+”符号以添加策略。



7. 输入策略的名称。在操作中，单击“+”符号以添加操作。



8. 键入操作的名称。在“服务器名称”中，键入之前创建的 TCP 服务的名称。在会计师事务所配置文件中，单击“+”符号以添加会计师事务所配置文件。



9. 键入配置文件名称 URI。在 模式下，选择 **REQMOD**。

The screenshot shows the 'Create ICAP Profile' dialog box. The 'Mode*' dropdown menu is set to 'REQMOD'. The 'ICAP Profile Name*' field is filled with 'icap-profile1'. The 'URI*' field is filled with '/example.com'. Other fields like 'Host Header', 'User Agent', 'Query Param', and 'Insert ICAP Headers' are empty. The 'Preview' checkbox is unchecked.

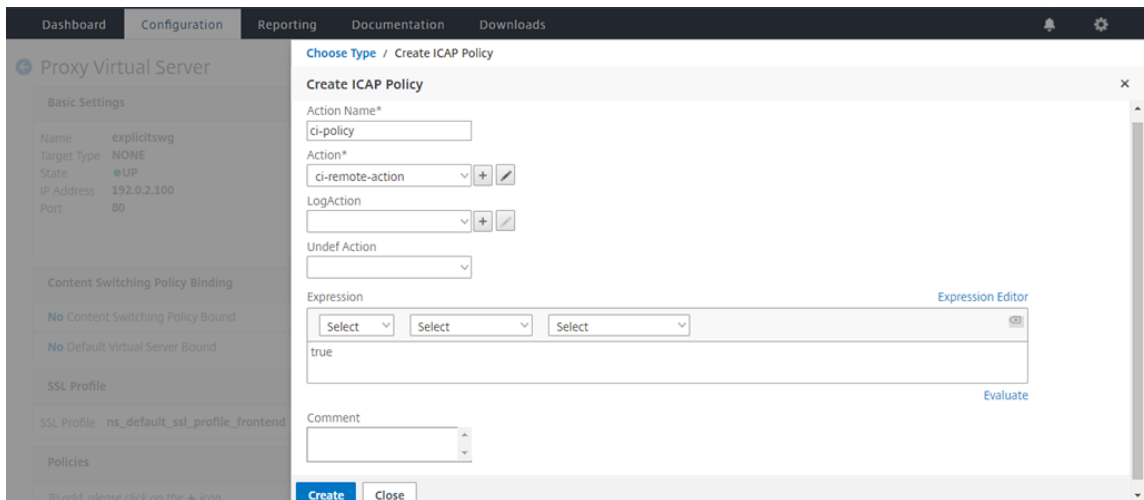
10. 单击创建。

This screenshot shows the bottom portion of the 'Create ICAP Profile' dialog. The 'Query Param' field is empty. The 'Request Time-out Action' dropdown is set to 'Request Time-out Action'. The 'On Server Error Response' dropdown is set to 'On Server Error Response'. There are several checkboxes: 'Send Request in Response Mode' is unchecked, 'Connection Keep-Alive' is checked, 'Allow204' is checked, and 'Insert-X-Client IP', 'Insert-X-Server IP', and 'Insert-X-Auth User IP' are all unchecked. At the bottom, there are 'Create' and 'Close' buttons.

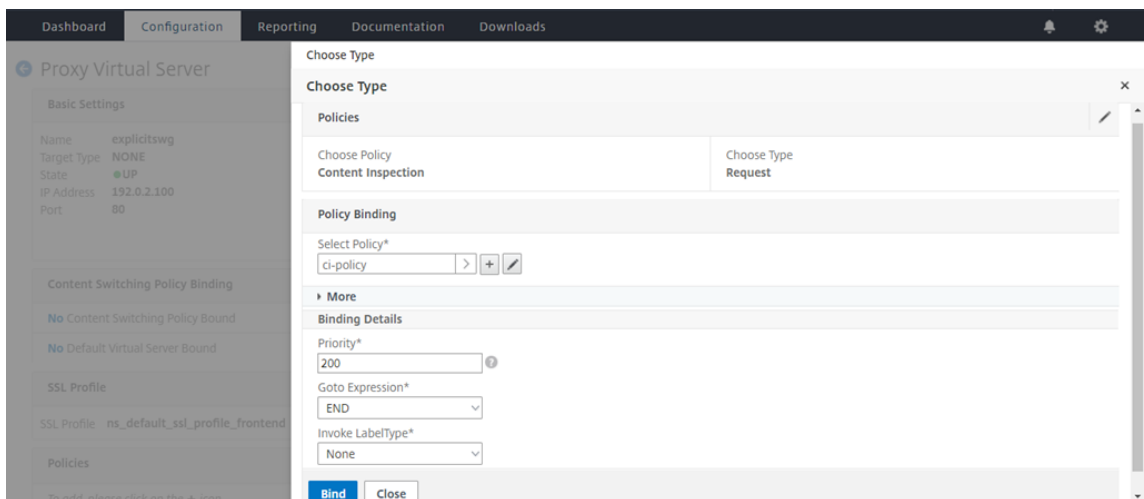
11. 在创建 ICAP 操作页面上，单击创建。

The screenshot shows the 'Create ICAP Action' dialog box. The 'Type*' dropdown is set to 'ICAP'. The 'Server Name' field is filled with 'icap_svc'. The 'ICAP Profile' dropdown is set to 'icap-profile1'. The 'If Server Down' dropdown is set to 'CONTINUE'. The 'Request-Timeout' field is filled with '0'. The 'Request Time-out Action' dropdown is set to 'BYPASS'. At the bottom, there are 'Create' and 'Close' buttons.

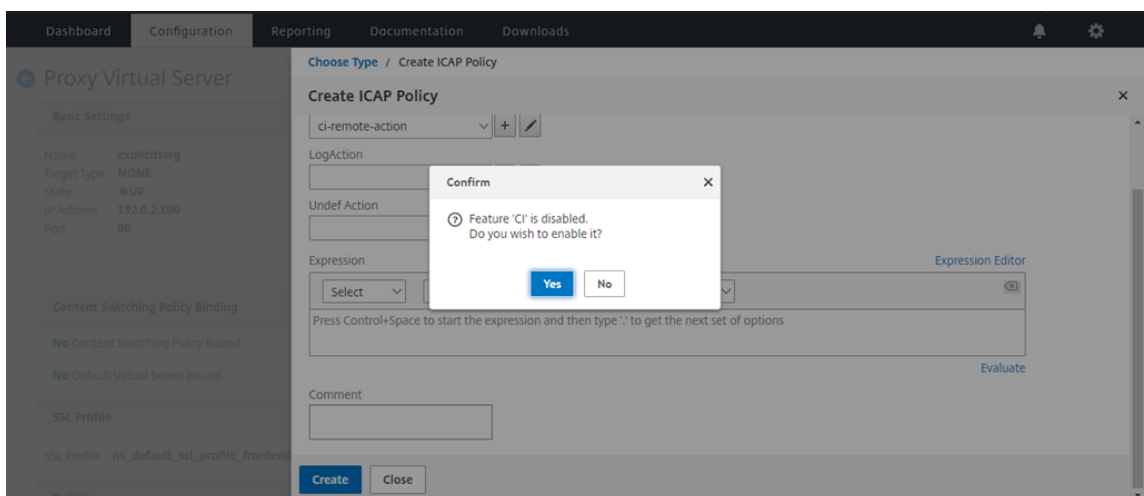
12. 在创建 **ICAP** 策略页面的表达式编辑器中，输入 true。然后，单击创建。



13. 单击 **Bind** (绑定)。



14. 如果提示启用内容检查功能，请选择是。



15. 单击完成。

Proxy Virtual Server

Basic Settings	
Name	explicitSWG
Target Type	NONE
State	UP
IP Address	192.0.2.100
Port	80
Listen Priority	-
Listen Policy Expression	NONE
Range	1
Traffic Domain	0
RHI State	PASSIVE
AppFlow Logging	ENABLED
Comments	-

Content Switching Policy Binding

- No Content Switching Policy Bound
- No Default Virtual Server Bound

SSL Profile

SSL Profile ns_default_ssl_profile_frontend

Policies

Request Policies

- 1 Content Switching Virtual Server to Content Inspection Policy Binding

Done

Help

Advanced Settings

- + SSL Policies
- + Certificate
- + Protection
- + Profiles
- + Push
- + Authentication
- + Traffic Settings

在 **RESPMOD** 中 **Citrix SWG** 设备和 **ICAP** 服务器之间的 **ICAP** 事务示例

从 **Citrix SWG** 设备向 **ICAP** 服务器发出请求：

```

1 RESPMOD icap://10.106.137.15:1344/resp ICAP/1.0
2
3 Host: 10.106.137.15
4
5 Connection: Keep-Alive
6
7 Encapsulated: res-hdr=0, res-body=282
8
9 HTTP/1.1 200 OK
10
11 Date: Fri, 01 Dec 2017 11:55:18 GMT
12
13 Server: Apache/2.2.21 (Fedora)
14
15 Last-Modified: Fri, 01 Dec 2017 11:16:16 GMT
16
17 ETag: "20169-45-55f457f42aee4"
18
19 Accept-Ranges: bytes
20
21 Content-Length: 69
22
23 Keep-Alive: timeout=15, max=100
24
25 Content-Type: text/plain; charset=UTF-8
26
27 X50!P%@AP[4\PZX54(P^)7CC)7 }
28 $EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
29 <!--NeedCopy-->

```


从 **ICAP** 服务器向 **Citrix SWG** 设备发出响应:

```
1 ICAP/1.0 200 OK
2
3 Connection: keep-alive
4
5 Date: Fri, 01 Dec, 2017 11:40:42 GMT
6
7 Encapsulated: res-hdr=0, res-body=224
8
9 Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$
10
11 IStag: "9.8-13.815.00-3.100.1027-1.0"
12
13 X-Virus-ID: Eicar_test_file
14
15 X-Infection-Found: Type=0; Resolution=2; Threat=Eicar_test_file;
16
17 HTTP/1.1 403 Forbidden
18
19 Date: Fri, 01 Dec, 2017 11:40:42 GMT
20
21 Cache-Control: no-cache
22
23 Content-Type: text/html; charset=UTF-8
24
25 Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$
26
27 Content-Length: 5688
28
29 <html><head><META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset
    =UTF-8"/>
30
31 ...
32
33 ...
34
35 </body></html>
36 <!--NeedCopy-->
```

操作方法文章

April 27, 2021

以下是一些配置说明或功能用例，可作为“如何”文章提供，以帮助您管理 SWG 部署。

网址筛选

[如何创建 URL 分类策略](#)

[如何创建 URL 列表策略](#)

[如何将特殊 URL 列入白名单](#)

[如何阻止成人类别的 Web 站点](#)

如何创建 **URL** 分类策略

April 27, 2021

作为网络管理员，您可能希望阻止特定类别的 Web 站点进行用户访问。您可以通过创建 URL 分类策略并将策略绑定到要限制访问的预定义类别列表来执行此操作。

例如，您可能希望根据组织策略限制对所有社交网络 Web 站点的访问。在这种情况下，您必须创建一个分类策略，并将该策略绑定到社交网络类别 Web 站点的预定义列表。

要使用基本方法创建 URL 分类策略，请执行以下操作：

1. 登录 **Citrix SWG** 设备并导航到受保护的 **Web Gateway > URL 过滤 > URL 分类**。
2. 在详细信息窗格中，单击 **添加** 以访问 **URL 分类策略** 页面并指定以下参数。
 - a) **URL 分类策略**。响应程序策略的名称。
 - b) **基本**。选择使用预定义的类别列表配置。
 - c) **操作**。控制 URL 访问的操作。
 - d) **URL 类别**。要选择并将其添加到配置列表的预定义类别列表。
3. 单击 **创建** 和 **关闭**。

URL Categorization Policies / URL Categorization Policy

URL Categorization Policy

Select Basic to choose from a predefined list of categories.
Select Advanced to use the expression editor to create policy rules to suit your deployment.

Name*

Basic Advanced

Action*

URL Categories*

Available (16) Select All

Search Categories

- + Remote Proxies
- + Search
- + Business and Industry
- + News/Entertainment/Society
- + Finance
- + Gambling
- + Messaging/Chat/Telephony
- + Email
- + Social Networking

Configured (29) Remove All

- Illegal Activities
- Illegal Drugs
- Medication
- Terrorism/Extremists
- Weapons
- Hate/Slander
- Violence/Suicide
- Advocacy in general
- Adult/Porn
- Nudity
- Sexual Services
- Adult Search/Links
- Dating
- Grotesque

使用高级方法创建 URL 分类策略：

1. 使用高级分类配置新的 URL 分类策略。
2. 单击添加。
3. 在“**URL 分类策略**”页面中，指定以下参数。
 - a) **URL 分类策略**。响应程序策略的名称。
 - b) 先进。使用自定义表达式配置策略。
4. 单击创建和关闭。

← URL Categorization Policy

Select Basic to choose from a predefined list of categories.
Select Advanced to use the expression editor to create policy rules to suit your deployment.

Name*

Basic Advanced

Expression*

Operators Saved Policy Expressions Frequently Used Expressions

HTTPREQ.URL.SUFFIX.EQ(“)HTTPREQ.HEADER(“)CONTAINS(“)

如何创建 **URL** 列表策略

April 27, 2021

作为网络管理员，您可能希望阻止特定类别的 Web 站点进行用户访问。您可以通过创建 URL 列表策略来执行此操作，并将策略与作为文本文件导入到设备中的 URL 集绑定。URL 集是您想要过滤的 Web 站点的集合。

例如，您可能希望按组织策略限制对所有恶意软件 Web 站点的访问。在这种情况下，您必须创建 URL 列表策略并将策略绑定到导入到设备中的 URL 集。

要配置 URL 列表策略，请执行以下操作：

1. 登录 **Citrix SWG** 设备，然后导航到 **安全 Web 网关 > URL 过滤 > URL 列表**。
2. 在详细信息窗格中，单击 **Add**（添加）。
3. 在“**URL 列表策略**”页面上，指定策略名称。
4. 选择一个选项以导入 URL 集或创建模式集，然后执行此过程最后一步的过程之一。
5. 从下拉列表中选择响应程序操作。
6. 单击创建和关闭。

要导入自定义 URL 集或第三方 URL 集：

1. 在“**URL 列表策略**”选项卡页中，选中“导入 **URL 集**”复选框并指定以下 URL 集参数。
 - a) **URL 集名称**—URL 集的名称。
 - b) **URL**—访问 URL 集的位置的 Web 地址。

- c) 覆盖—覆盖之前导入的 URL 集。
- d) 分隔符—用于分隔 CSV 文件记录的字符序列。
- e) 行分隔符—CSV 文件中使用的行分隔符。
- f) 间隔—间隔（以秒为单位），四舍五入到最接近的 15 分钟，在此时更新 URL 集。
- g) 私有集—用于防止导出 URL 集的选项。
- h) **Canary URL**—用于测试 URL 集的内容是否保密的内部 URL。URL 的最大长度为 2047 个字符。有关 Canary URL 的详细信息，请参阅“配置专用 URL 集合”部分。

← URL List Policy

Configure a URL List policy to filter or blacklist URLs by importing a URL set or by creating a pattern set.

Name*

Import URL Set Create Patset

URL Set Name*

URL*

Overwrite

Delimiter

Row Separator

Interval

Private Set

Canary URL

Action*

Responder Action*
 + ?

要创建一个模式集：

1. 在创建模式选项卡页面中，输入阵列集的名称。
2. 单击“插入”以创建模式。

3. 在“将策略修补集配置为模式绑定”页面上，设置以下参数。
 - a) 模式—构成模式的字符串
 - b) 字符集—字符集类型：ASCII 或 UTF_8 格式
 - c) 索引 - 用户分配的索引值（从 1 到 4294967290）
4. 单击“插入”以添加模式集，然后单击“关闭”。

← URL List Policy

Configure a URL List policy to filter or blacklist URLs by importing a URL set or by creating a pattern set.

Name*
URL List

Import URL Set Create Patset

Patset Name*
Patset

Patset	Pattern
<input checked="" type="checkbox"/>	Pattern
<input checked="" type="checkbox"/>	Pattern

Configure Policy Patset to Pattern Binding

Pattern*
Patset

Charset
ASCII

Index
5

Action*
Respond with html page

Responder Action*
 + ?

如何将特殊 URL 列入白名单

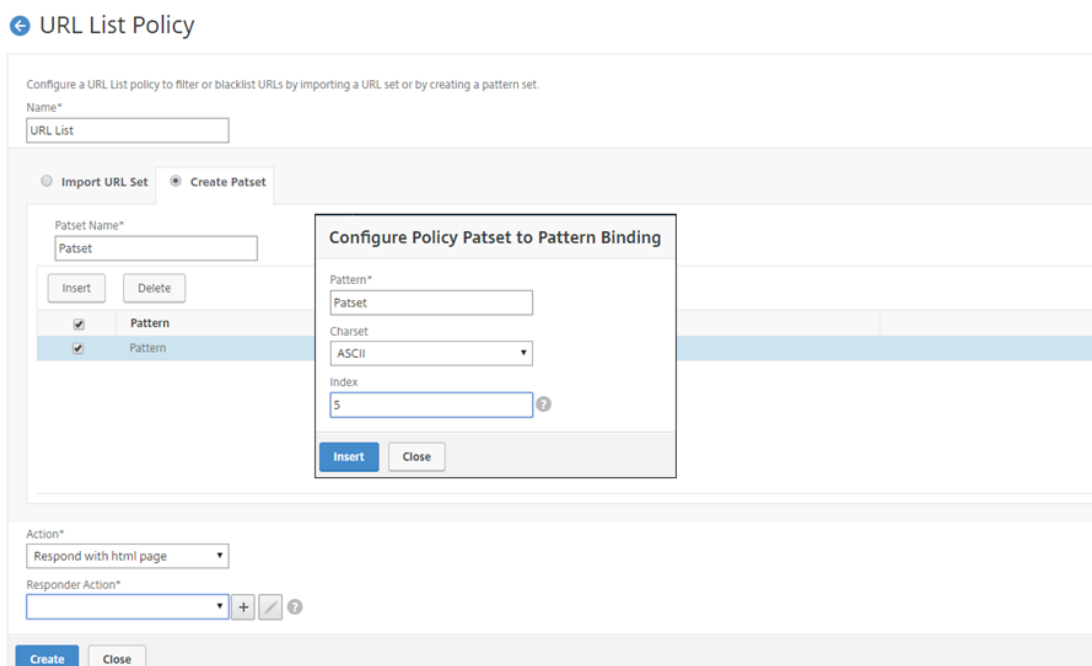
April 27, 2021

使用 URL 过滤器向一类 Web 站点添加黑名单时，可能需要列入白名单或允许特定 Web 站点例外。例如，如果您更倾向于将游戏 Web 站点添加到黑名单中，但仅首选将 www.supersports.com 列入白名单，则必须创建一个带有 URL 列表策略的 patset，然后将该策略绑定到优先级高于其他绑定策略的代理服务器。

使用 Citrix SWG 向导创建模式集

1. 登录 **Citrix SWG** 设备并导航到受保护的 **Web Gateway > URL 过滤 > URL 列表**。
2. 在详细信息窗格中，单击 **Add**（添加）。
3. 在 **URL 列表策略** 页面中，指定策略名称。
4. 选择一个选项以导入 URL 集或创建模式集。
5. 在创建模式选项卡页面中，输入阵列集的名称。

6. 单击“插入”以创建模式。
7. 在“将策略修补集配置为模式绑定”页面中，设置以下参数。
 - a) 模式-构成模式的字符串。
 - b) 字符集—字符集类型定义为 ASCII 或 UTF_8 格式。
 - c) 索引 - 用户分配的索引值（从 1 到 4294967290）
8. 单击“插入”以添加模式集，然后单击“关闭”。



要使用 Citrix SWG GUI 设置策略表达式的优先级，请执行以下操作：

1. 登录 **Citrix SWG** 设备并导航到 **Secure Web Gateway >** 代理虚拟服务器。
2. 在详细信息页面中，选择一个服务器，然后单击 编辑。
3. 在“代理虚拟服务器”页面中，转到“策略”部分，然后单击铅笔图标以编辑详细信息。
4. 选择您创建的修补集策略，并在“策略绑定”页面中指定优先级值低于其他绑定策略。
5. 单击 绑定 并完成。

如何阻止成人类别的 **Web** 站点

April 27, 2021

作为企业客户，您可能希望阻止属于成人类别组的 Web 站点。执行此操作的方法是：配置用于选择属于成人类别的请求并阻止访问此类黑名单 URL 的响应程序策略。

配置 **URL** 分类以阻止属于成人类别的 **Web** 站点

要使用 CLI 配置策略并阻止成人 Web 站点，请执行以下操作：

在命令提示符下，键入以下命令：

```
1  \*\*add responder policy\*\* <name> <rule> <respondwithhtml> [<
    undefAction>] [-comment <string>] [-logAction <string>] [-
    appflowAction <string>]
2  <!--NeedCopy-->
```

示例：

```
1      add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).
      URL_CATEGORIZE(0,0). GROUP.EQ("Adult")'
2  <!--NeedCopy-->
```

使用 **Citrix SWG** 向导配置 **URL** 分类以阻止成人网站

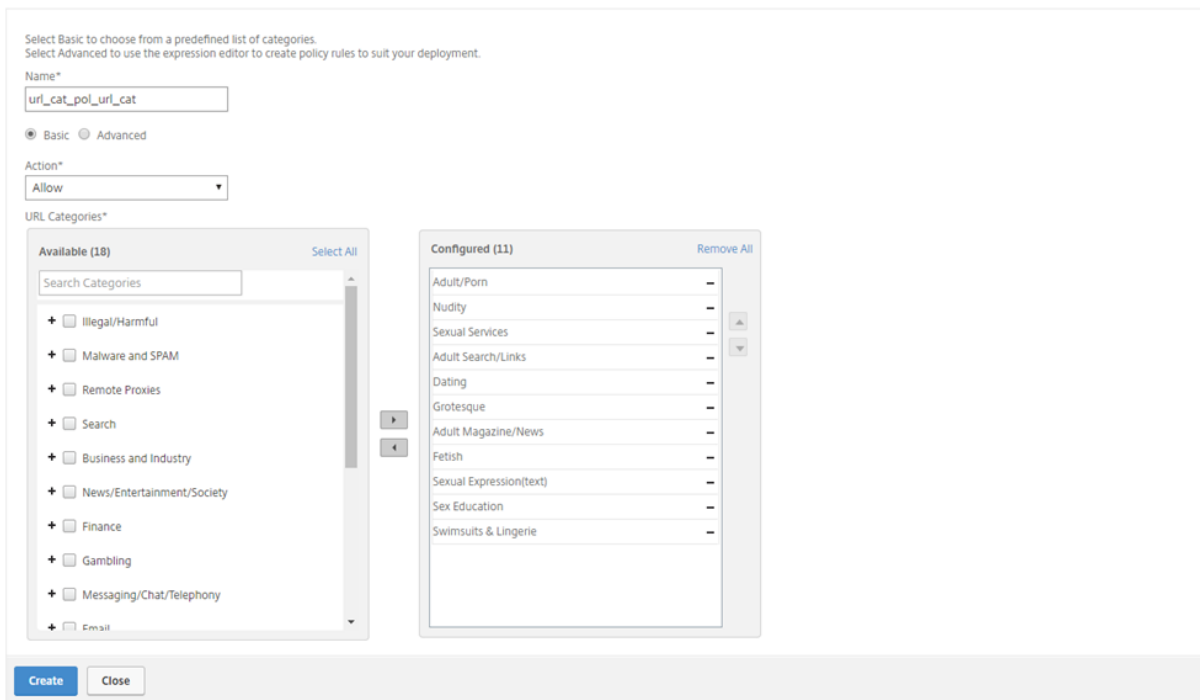
使用 Citrix SWG 向导阻止成人类别

1. 登录 **Citrix SWG** 设备并导航到 **Secure Web Gateway**。
2. 在详细信息窗格中，单击受保护的 **Web Gateway** 向导。
3. 在 **Secure Web Gateway Configuration** (Secure Web Gateway 配置) 页面中，指定 SWG 代理服务器设置。
4. 单击 **继续** 指定其他设置，如 SSL 拦截和标识管理。
5. 单击 **继续** 以访问 **URL** 筛选部分。
6. 选择“启用 **URL** 分类”复选框以启用该功能。
7. 单击绑定以访问 **URL** 分类策略 滑块。
8. 选择一个策略，然后单击“插入”以绑定该策略。
9. 选择阻止成人 Web 站点的响应程序策略。
10. 要添加新策略，请单击“添加”以访问“**URL** 分类策略”页面并执行以下操作之一。
 - a) 要使用基本分类配置策略，请单击“添加”。
 - i. 在“**URL** 分类策略”页面中，指定以下参数。
 - A. URL 分类策略。响应程序策略的名称。
 - B. Basic)。使用基本配置方法配置策略。
 - C. 操作。控制 URL 访问的操作。
 - D. URL 类别。从预定义列表中选择成人类别。
11. 单击创建和关闭。
 - a) 要使用高级分类配置新的 URL 分类策略，请单击“添加”。
 - i. 在“**URL** 分类策略”页面中，指定以下参数。

- A. **URL** 分类策略。响应程序策略的名称。
- B. 先进。配置策略以阻止成人类别组的请求。

12. 单击创建和关闭。

← URL Categorization Policy



系统

April 27, 2021

系统功能提供了配置 Citrix SWG 设备时可能需要参考的概念信息和配置说明。

下表介绍了 Citrix SWG 设备中的功能。

[基本操作](#) -Citrix ADC 设备的系统级操作和配置详细信息。

[身份验证和授权](#) -创建用户、用户组和命令策略以及为用户帐户分配策略的配置详细信息

[TCP 配置](#) -Citrix ADC 设备上的 TCP 配置文件和 TCP 功能的配置详细信息。

[HTTP 配置](#) -Citrix ADC 设备上的 HTTP 配置文件和 HTTP 功能的配置详细信息。

[SNMP](#) -一种网络管理协议，监控 Citrix ADC 设备并及时响应设备上的问题。

[审核日志记录](#) -用于记录内核和用户级守护程序中各个模块收集的 Citrix ADC 设备状态和状态信息的标准协议。对于审计日志记录，您可以使用 SYSLOG 或 NSLOG 协议或两者。

[Call Home](#) -用于监控和解决 Citrix SWG 设备上的关键错误条件的通知系统。

[报告工具](#) - 从 Citrix SWG 设备访问的基于 Web 的界面，用于以图表形式查看系统性能报告。

网络连接

April 27, 2021

以下主题提供了您可能希望在 Citrix SWG 设备上配置的网络功能的概念参考信息和配置说明。

- [IP 寻址](#) Citrix ADC 拥有 IP 地址及其配置详细信息。
- [接口](#) 访问和配置 Citrix SWG 设备。
- [访问控制列表 \(ACL\)](#) Citrix ADC 设备上使用的不同类型的访问控制列表以及配置详细信息。
- [IP 路由](#) Citrix ADC 设备上使用的不同 IP 路由协议。
- [互联网协议版本 6 \(IPv6\)](#) Citrix ADC 设备上的互联网协议支持，以及该设备如何作为 IPv6 节点运行。
- [VXLAN](#) Citrix ADC 网络基础架构中的虚拟可扩展局域网 (VXLAN) 支持，以及 VXLAN 如何通过将第 2 层帧封装在 UDP 数据包中，将第 2 层网络叠加到第 3 层基础架构上。

AppExpert

April 27, 2021

以下主题提供了您可能希望在 Citrix SWG 设备上配置的 AppExpert 功能的概念信息和配置说明。

[模式集和数据集](#) -用于对大量字符串模式执行字符串匹配操作的策略表达式。

根据要匹配的模式类型，可以使用以下功能之一来实现模式匹配：

- 模式集是在默认语法策略评估期间用于字符串匹配的索引模式数组。模式集的示例：图像类型 {svg、bmp、png、gif、TIFF、jpg}。
- 数据集是模式集的一种特殊形式。它是类型数（整数）、IPv4 地址或 IPv6 地址的模式数组。

[变体](#) -以令牌形式存储信息并供响应者策略操作使用的对象。

变量有两种类型，如下所示：

- 单例变量。可以有以下类型之一的单个值：`ulong` 和文本（最大尺寸）。`ulong` 类型是无符号的 64 位整数，文本类型是字节序列，最大大小是序列中的最大字节数。
- 映射变量。映射保存与键关联的值：每个键值对称为映射条目。每个条目的键在映射中都是唯一的。

策略和表达式 - 策略控制进入 Citrix SWG 设备的 Web 流量。策略使用逻辑表达式（也称为规则）来评估请求、响应或其他数据，并应用由评估结果确定的一个或多个操作。或者，策略可以应用定义复杂操作的配置文件。

响应方 - 根据发送请求的人、发送请求的位置以及其他具有安全性和系统管理影响的标准发送响应的策略。该功能是简单和快速的使用。通过避免调用更复杂的功能，它可以减少处理不需要复杂处理的请求的 CPU 周期和时间。要处理敏感数据（例如财务信息），如果要确保客户端使用安全连接来浏览 Web 站点，可以使用 HTTPS 协议将请求重定向到安全连接。

重写 - 重写 Citrix SWG 设备处理的请求和响应中信息的策略。重写可以帮助您提供对请求内容的访问，而不会显示有关 Web 站点实际配置的不必要的详细信息。

URL 集 - 用于将 1000000 个 URL 条目加入黑名单的高级策略表达式。要阻止访问受限制的 Web 站点，Citrix SWG 设备使用专用 URL 匹配算法。此算法使用的 URL 集可以包含最多 1000000 个黑名单条目的 URL 列表。每个条目都可以包含将 URL 类别和类别组定义为索引模式的元数据。该设备还可以定期下载由互联网执法机构（通过政府网站）或独立互联网组织管理的高度敏感的 URL 集的 URL 集。

SSL

April 27, 2021

以下主题提供了您可能想要在 Citrix SWG 设备上配置的 SSL 功能的概念参考信息和配置说明。

- [证书](#)
- [证书吊销列表 \(CRL\)](#)
- [SSL 策略](#)
- [OCSP 响应者](#)

常见问题解答

April 27, 2021

问：Citrix Secure Web Gateway (SWG) 支持哪些硬件平台？

答：Citrix SWG 可在以下硬件平台上使用：

- Citrix SWG MPX 14020/14030/14040
- Citrix SWG MPX 14020-40G/14040-40G
- Citrix SWG MPX 14060-40S/14080-40S/14100-40S
- Citrix SWG MPX 5901/5905/5910
- Citrix SWG MPX/SDX 8905/8910/8920/8930

- 所有基于 Cavium N2 和 N3 的 SDX 平台

问：在 SWG 设备上创建代理时，我可以设置哪两种捕获模式？

答：SWG 解决方案支持显式和透明的代理模式。在显式代理模式下，客户端必须在浏览器中指定 IP 地址和端口，除非组织将设置推送到客户端的设备上。此地址是在 SWG 设备上配置的代理服务器的 IP 地址。顾名思义，透明代理对客户端是透明的。SWG 设备是在内联部署中配置的，设备以透明方式接受所有 HTTP 和 HTTPS 流量。

问：Citrix SWG 是否有配置向导？

答：是。该向导位于配置实用程序中的 SWG 节点上。

问：配置 Citrix SWG 时使用哪些 Citrix ADC 功能？

答：响应程序、AAA-TM、内容切换、SSL、转发代理、SSL 拦截和 URL 过滤。

问：Citrix SWG 支持哪些身份验证方法？

答：在显式代理模式下，支持 LDAP、RADIUS、TACACS+ 和 NEGOTIATE 身份验证方法。在透明模式下，仅支持 LDAP 身份验证。

问：是否有必要在客户端设备上安装 CA 证书？

答：是。Citrix SWG 设备模拟源服务器证书。此服务器证书必须由受信任的 CA 证书签名，该证书必须安装在客户端的设备上，以便客户端能够信任重新生成的服务器证书。

问：我可以在 Citrix SWG 平台上使用 Citrix ADC 平台许可证吗？

答：不。Citrix SWG 平台需要自己的平台许可证。

问：Citrix Secure Web Gateway 部署是否支持 HA？

答：是。

问：哪个文件包含 Citrix SWG 的日志？

答：ns.log 文件记录 Citrix SWG 信息。必须使用 CLI 或 GUI 启用日志记录。在命令提示窗口中，键入 **set syslog-params -ssli Enabled**。

在 GUI 中，导航到系统 > 审核。在设置中，单击更改审核系统日志设置。选择 **SSL 截获**。

问：我可以使用的哪些 nsconmsg 命令来解决问题？

答：您可以使用以下一个或两个命令：

```
1 nsconmsg -d current -g ssli
2 <!--NeedCopy-->
```

```
1 nsconmsg -d current -g err
2 <!--NeedCopy-->
```

问：如果证书捆绑包是内置的，我该如何获取更新？

答：版本中包含最新的捆绑包。有关更新，请联系 Citrix 支持。

问：可以在 Citrix ADM from Citrix SWG 上捕获数据吗？

答：是。必须在 Secure Web Gateway 向导中启用 **Analytics**。

重要：请务必使用同一个 12.0 内部版本的 MAS 和 SWG。

问：什么是 URL 过滤服务？

答：URL 过滤是一种 Web 内容过滤器，用于控制对受限制的 Web 页面列表的访问权限。此过滤器基于 URL 类别、类别组和信誉分数限制用户访问 Internet 上不适宜的内容。网络管理员可以监视 Web 流量，并阻止用户访问非常危险的 Web 站点。您可以通过使用 URL 分类或基于策略实施的 URL 列表功能来实现此功能。有关详细信息，请参阅 [URL 过滤](#) 主题。

问：URL 过滤如何适合 Citrix SWG？

答。URL 过滤利用 Citrix SWG 设备来控制对特定 Web 站点的访问。位于网络边缘的 SWG 设备用作代理，用来截获 Web 流量以及执行身份验证、检查、缓存和重定向等操作。此过滤器随后将控制使用 URL 分类或 URL 列表功能对 Web 站点的访问，并采用策略实施。

问：URL 分类数据库多久更新一次？

答：如果您使用 URL 分类功能控制对受限 Web 站点的访问，您必须定期使用基于云的供应商服务的最新数据更新分类数据库。要更新数据库，Citrix SWG GUI 允许您配置 URL 过滤参数，例如数据库更新之间的小时数”或“更新数据库的每日时间。

问：今天哪些用例最适合 URL 过滤服务？

答。以下是面向企业客户的一些目标使用案例：

- [按 URL 信誉评分过滤 URL](#)
- [企业合规下的互联网使用控制](#)
- [使用自定义 URL 列表过滤 URL](#)

问：URL 分类服务中的缓存是否有内存限制？

答：是。缓存的内存限制设置为 10 GB，您只能通过 CLI 界面进行配置。

问：如果没有类别与传入请求匹配，URL 分类数据库将返回什么？

答：如果传入的请求与类别不匹配或 URL 格式错误，设备将该 URL 标记为“未分类”，然后将请求发送到分类供应商维护的基于云的服务。设备继续监视云查询反馈并更新缓存，以便将来的请求可以从云查找中受益。

问：URL 信誉分数是什么，您如何基于信誉分数控制对恶意 Web 站点的访问？

答：URL 信誉分数是 Citrix SWG 分配给 Web 站点的等级。此值的范围为 1 到 4，其中 4 为恶意 Web 站点，1 为干净的 Web 站点。如果网络管理员监视了访问高风险 Web 站点的用户，则将根据您在 Citrix SWG 设备上配置的 URL 信誉分数和安全级别来控制对这些站点的访问权限。有关详细信息，请参阅[URL 信誉分数](#)。

问：如果您使用 URL 集（但不正确过滤特定 Web 站点）过滤 Web 站点，启用卓越 Web 站点的过程是什么？

答。URL 过滤使用响应程序策略控制对 Web 站点的访问。要将特定 URL 列入白名单作为例外情况，请在 SWG 向导中创建一个 patset 策略，然后使用“允许”操作添加特殊 URL。创建策略后，退出向导并执行以下步骤：

要使用 Citrix SWG GUI 更改策略表达式的优先级，请执行以下操作：

1. 登录 **Citrix SWG** 设备并导航到 **Secure Web Gateway >** 代理虚拟服务器。
2. 在详细信息页面中，选择一个服务器，然后单击 **编辑**。
3. 在“代理虚拟服务器”页面中，转到“策略”部分，然后单击铅笔图标以编辑详细信息。
4. 选择 **Patset** 策略，然后在策略绑定页面中，指定低于其他绑定策略的优先级值。
5. 单击 **绑定** 并完成。

问：使用 Citrix SWG URL 过滤功能的主要好处是什么？

答：URL 过滤功能易于部署、配置和使用。它提供了以下好处，并允许企业客户：

- 监视 Web 流量和用户事务
- 过滤恶意软件和互联网传播的安全威胁。
- 控制恶意 Web 站点的未经授权访问。
- 强制执行企业安全策略以控制对受限数据的访问。

问：如果您使用 URL 列表功能过滤 Web 站点，如何编辑 URL 列表策略？

答：您可以通过 Citrix SWG 向导修改 URL 列表策略，方法是覆盖或删除绑定到响应程序策略的导入列表。

问：与 URL 关联的元数据包含什么？

答：分类数据库中的每个 URL 都有一个与之关联的元数据。元数据包含 URL 类别、类别组和信誉评分信息。例如，如果 URL 是购物门户网站，则元数据将分别为“购物”、“购物/零售”和 1。

使用以下表达式获取传入 URL 的这些值。这些表达式如下：

```
1 URL_CATEGORIZE(0,0).CATEGORY
2 <!--NeedCopy-->
```

```
1 URL_CATEGORIZE(0,0).GROUP
2 <!--NeedCopy-->
```

```
1 URL_CATEGORIZE(0,0).REPUTATION
2 <!--NeedCopy-->
```

问：URL 分类功能需要什么类型的许可证和订阅？

答：URL 分类功能需要使用 Citrix SWG 版的 URL 威胁智能订阅服务（可用一年或三年）。

问：我可以配置 URL 过滤的方法是什么？

答：配置 URL 过滤的方法有两种。您可以通过 Citrix SWG 命令界面或 Citrix SWG 向导执行此操作。Citrix 建议您使用向导配置筛选策略。

问：您可以阻止哪些类型的 URL 类别？

答：URL 分类数据库包含数百万个包含元数据的 URL。管理员可以配置响应程序策略来决定可以阻止哪些 URL 类别以及允许用户访问哪些 URL 类别。有关 URL 类别映射的信息，请参阅 [映射类别](#) 页面。

问：如果我们无法访问使用 WebSocket 的源服务器，我们该怎么办，例如 [whatsapp](#)

您必须在默认 HTTP 配置文件中启用 WebSocket。

在 CLI 中，键入：

```
1 > set httpprofile nshttp_default_profile -webSocket ENABLED
2 <!--NeedCopy-->
```

什么是会计师协会？

ICAP 代表互联网内容适应协议。

Citrix SWG 的哪个版本支持 ICAP？

Citrix SWG 版本 12.0 版本 57.x 及更高版本支持 ICAP。

Citrix SWG 支持哪两种 ICAP 模式？

支持请求修改 (REQMOD) 模式和响应修改 (RESPMOD) 模式。

ICAP 的默认端口是什么？

1344.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).
