



Citrix Secure Web Gateway 12.1

Contents

Release Notes	3
Supported hardware and software platforms	3
Licensing requirement	4
Installation	9
Getting started with a Citrix ADC MPX and VPX SWG appliance	10
Get started with an SWG instance on a Citrix ADC SDX appliance	13
Proxy modes	14
SSL interception	16
SSL profile	17
SSL policy infrastructure for SSL interception	26
SSL interception certificate store	29
SSL error autolearning	33
User identity management	35
URL filtering	39
URL list	41
URL Pattern Semantics	48
Mapping URL Categories	49
Use case: URL filtering by using custom URL set	49
URL Categorization	52
Security configuration	64
URL reputation score	64
Using ICAP for remote content inspection	66
Integration with IPS or NGFW as inline devices	77

Analytics	126
Use case: Making enterprise internet access compliant and secure	127
Use case: Making enterprise network secure by using ICAP for remote malware inspection	142
How-to articles	156
How to create a URL categorization policy	157
How to create a URL list policy	159
How to whitelist an exceptional URL	162
How to block adult category website	163
System	165
Networking	166
AppExpert	166
SSL	168
FAQs	168

Release Notes

February 15, 2019

The release notes for Citrix Secure Web Gateway product are captured in the main release notes for a Citrix ADC appliance. See [Citrix ADC Release Notes](#).

Supported hardware and software platforms

June 25, 2019

The Citrix Secure Web Gateway (SWG) appliance is currently available as a hardware appliance and as a virtual appliance. Detail specifications are available in the data sheet, which is available on www.citrix.com. Hover the mouse pointer over **Products**, and in the **Networking** list, select **Citrix Secure Web Gateway**.

Before you install your SWG appliance, ensure that you have the correct license(s). Each appliance in a high availability setup requires its own license. For information about the licenses, see [License Requirements](#). For information about high availability, see [Introduction to high availability](#) topic.

Hardware appliance (MPX)

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

Virtual appliance (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

Hardware appliance (SDX)

SWG instance(s) can be provisioned on any SDX platform by installing “SDX 2-Instance Add-On Pack for Secure Web Gateway” license. With one license install, you can provision two SWG instances on an SDX appliance. You can provision more SWG instances on your appliance by adding more licenses. For more information about provisioning a Citrix SWG instance, see [Provisioning Citrix ADC Instances](#).

Licensing requirement

July 1, 2019

A license gives you access to a set of features on a Citrix Secure Web Gateway (SWG) appliance.

The Citrix licensing framework allows you to focus on getting maximum value from Citrix products. The process of allocating your licenses is very simple. In the SWG configuration utility (GUI), you can use your hardware serial number (HSN) or your license activation code (LAC) to allocate your licenses. If a license is already present on your local computer, you can upload it to the appliance.

For all other functionality, such as returning or reallocating your license, you must use the licensing portal (which you can also use for initial license allocation if you prefer). For more information about the licensing portal, see <http://support.citrix.com/article/CTX131110>.

You can partially allocate licenses as required for your deployment. For example, if your license file contains ten licenses, but your current requirement is for only six licenses, you can allocate six licenses now, and allocate additional licenses later. You cannot allocate more than the total number of licenses present in your license file.

Before using your SWG appliance, you should install the following licenses by using either the GUI or the CLI:

- **Citrix Secure Web Gateway license**
 - Citrix SWG Platform license is the minimum requirement for using your MPX SWG appliance, and for deploying your VPX instance on different hypervisors, such as XenServer, VMware ESX, Microsoft Hyper-V, and Linux-KVM.
 - For SDX platforms, at least one SDX 10K concurrent sessions SWG add-on pack license is required to provision a Citrix SWG instance on a Citrix ADC SDX appliance.
- **URL Threat Intelligence feature license.** This license is required for use of the URL filtering, URL categorization, and URL reputation score features.

Prerequisites

To use the hardware serial number or license activation code to allocate your licenses:

- You must be able to access public domains through the appliance. For example, the appliance should be able to access www.citrix.com. The license allocation software internally accesses the Citrix licensing portal for your license. To access a public domain, you can either use a proxy server or set up a DNS server and, on your Citrix ADC appliance, configure a NSIP address or a subnet IP (SNIP) address.
- Your license must be linked to your hardware, or you must have a valid license activation code (LAC). Citrix sends your LAC by email when you purchase a license.

Licenses for appliances in a high availability setup

You must purchase a separate license for each appliance in a high availability (HA) pair. Make sure that the same type of license is installed on both appliances.

On a Citrix ADC SDX appliance, you can configure a high availability (HA) setup between two SWG instances on the same appliance. However, Citrix recommends that you configure an HA setup between two SWG instances on different Citrix ADC SDX appliances.

Allocate and install your licenses

You can allocate and install your licenses by using the GUI. Installing your licenses by using the CLI requires copying the licenses to the `/nsconfig/license/` directory.

Allocate your licenses by using the Citrix SWG GUI

1. In a web browser, type the IP address of the Citrix SWG appliance.
2. In **User Name** and **Password**, type the administrator credentials.
3. On the **Configuration** tab, navigate to **System > Licenses**.
4. In the details pane, click **Manage Licenses**, click **Add New License**, and then select one of the following options:
 - **Use Serial Number**. The software internally fetches the serial number of your appliance and uses this number to display your license(s).
 - **Use License Activation Code**. Citrix emails the license activation code (LAC) for the license that you purchased. Enter the LAC in the text box.

If you do not want to configure internet connectivity on the Citrix ADC appliance, you can use a proxy server. Select **Connect through Proxy Server** and specify the IP address and port of your proxy server.

5. Click **Get Licenses**.
6. Select the license file that you want to use to allocate your licenses.
7. In the **Allocate** column, enter the number of licenses to be allocated. Then click **Get**.
8. Click **Reboot** for the license to take effect.
9. In the **Reboot** dialog box, click **OK**.

Install your licenses by using the Citrix SWG GUI

1. In a web browser, type the IP address of the Citrix SWG appliance (for example, <http://192.168.100.1>).
2. In **User Name** and **Password**, type the administrator credentials.
3. On the **Configuration** tab, navigate to **System > Licenses**.
4. In the details pane, click **Manage Licenses**.
5. Click **Add New License**, and then select **Upload license files**.
6. Click **Browse**. Navigate to the location of the license files, select the license file, and then click **Open**.
7. Click **Reboot** to apply the license.
8. In the **Reboot** dialog box, click **OK**.

Install your licenses by using the Citrix SWG CLI

1. Open an SSH connection to the Citrix SWG appliance by using an SSH client, such as PuTTY.
2. Log on to the appliance by using the administrator credentials.
3. Switch to the shell prompt and copy the new license file(s) to the license subdirectory of the `nsconfig` directory. If the subdirectory does not exist, create it before copying the file(s).

Example:

```
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-->
```

Copy the new license file(s) to this directory.

Note

The CLI does not prompt you to reboot the appliance to activate the licenses. Run the **reboot -w** command to warm reboot the system, or run the **reboot** command to reboot the system normally.

Verify the licensed features

Before using a feature, make sure that your license supports the feature.

Verify the licensed features by using the Citrix SWG GUI

1. In a Web browser, type the IP address of the Citrix SWG appliance (for example, <http://192.168.100.1>).
2. In **User Name** and **Password**, type the administrator credentials.
3. Navigate to **System > Licenses**.
The screen has a green check mark next to each licensed feature.

Verify the licensed features by using the Citrix SWG CLI

1. Open an SSH connection to the Citrix SWG appliance by using an SSH client, such as PuTTY.
2. Log on to the appliance by using the administrator credentials.
3. At the command prompt, enter the `sh ns license` command to display the features supported by the license.

Example:

```
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 Interception: YES
16
17          Model Number ID: 25000
18
19          Licensing mode: Local
20
21 Done
```

Enable or disable a feature

When you use the Citrix Secure Web Gateway appliance for the first time, you have to enable a feature before you can use it. If you configure a feature before it is enabled, a warning message appears. The configuration is saved, but it does not apply until the feature is enabled.

Enable a feature by using the Citrix SWG GUI

1. In a Web browser, type the IP address of the Citrix SWG appliance (for example, <http://192.168.100.1>).
2. In **User Name** and **Password**, type the administrator credentials.
3. Navigate to **System > Settings > Configure Advanced Features**.
4. Select the features (for example, Forward Proxy, SSL Interception, and URL Filtering) that you want to enable.

Enable a feature by using the Citrix SWG CLI

At the command prompt, type the following commands to enable a feature and verify the configuration:

```
enable feature <FeatureName>
```

```
show feature
```

The following example shows how to enable the SSL interception, forward proxy, and URL filtering features.

```

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-->

```

Note

If the license key is not available for a feature, the following error message appears for that feature:

```
ERROR: feature(s) not licensed
```

Installation

June 25, 2019

A Citrix Secure Web Gateway (SWG) appliance must be properly installed and accessible to the internet before you can begin configuring it for securing your enterprise.

For information about installation and initial configuration of your hardware appliance, see [Setting Up the SWG Hardware](#).

A Citrix SWG virtual appliance (VPX) is supported on different virtualization platforms.

For information about the supported hypervisors and instructions for deploying a VPX appliance, see [Deploy a Citrix ADC VPX instance](#).

Getting started with a Citrix ADC MPX and VPX SWG appliance

June 25, 2019

After installing your hardware (MPX) or software (VPX) appliance and performing the initial configuration, you are ready to configure it as a secure web gateway appliance to receive traffic.

Important:

- OCSP check requires an internet connection to check the validity of certificates. If your appliance is not accessible from the internet by using the NSIP address, add access control lists (ACLs) to perform NAT from the NSIP address to the subnet IP (SNIP) address. The SNIP must be accessible from the Internet. For example,

```
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-->
```

- Specify a DNS name server to resolve domain names. For more information, see [Initial configuration](#).
- Make sure that the date on the appliance is synchronized with the NTP servers. If the date is not synchronized, the appliance cannot effectively verify whether an origin server certificate is an expired one.

To use the Citrix SWG appliance, you must perform the following tasks:

- Add a proxy server in explicit or transparent mode.
- Enable SSL interception.
 - Configure an SSL profile.
 - Add and bind SSL policies to the proxy server.
 - Add and bind a CA certificate-key pair for SSL interception.

Note: A Citrix SWG appliance configured in transparent proxy mode can intercept only HTTP and HTTPS protocols. To bypass any other protocol, such as telnet, you must add the following listen policy on the proxy virtual server.

The virtual server now accepts only HTTP and HTTPS incoming traffic.

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

You might need to configure the following features, depending on your deployment:

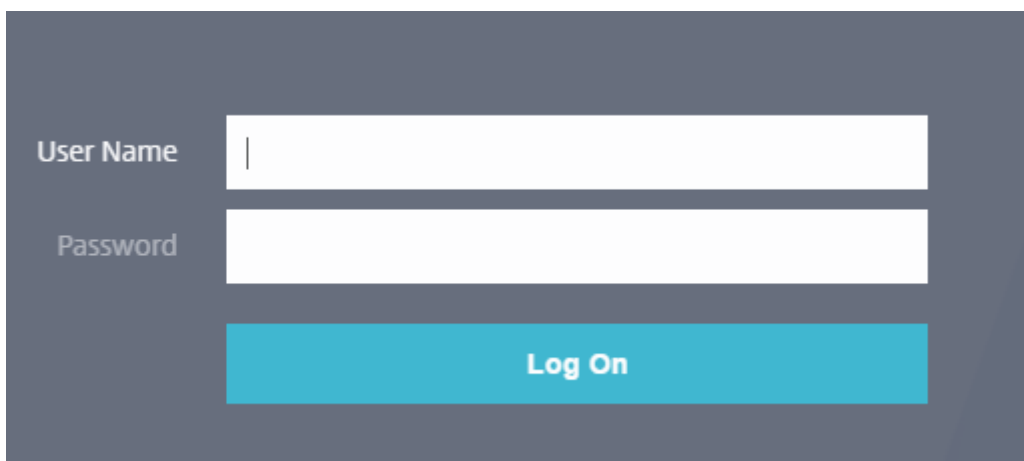
- Authentication Service (recommended) –to authenticate users. Without the Authentication Service, user activity is based on client IP address.
- URL Filtering –to filter URLs by categories, reputation score, and URL lists.
- Analytics –to view user activity, user risk indicators, bandwidth consumption, and transactions break down in Citrix Application Delivery Management (ADM).

Note: SWG implements the majority of typical HTTP and HTTPS standards followed by similar products. This implementation is done with no specific browser in mind and is compatible with most common browsers. SWG has been tested with common browsers and recent versions of Google Chrome, Internet Explorer, and Mozilla Firefox.

Secure web gateway wizard

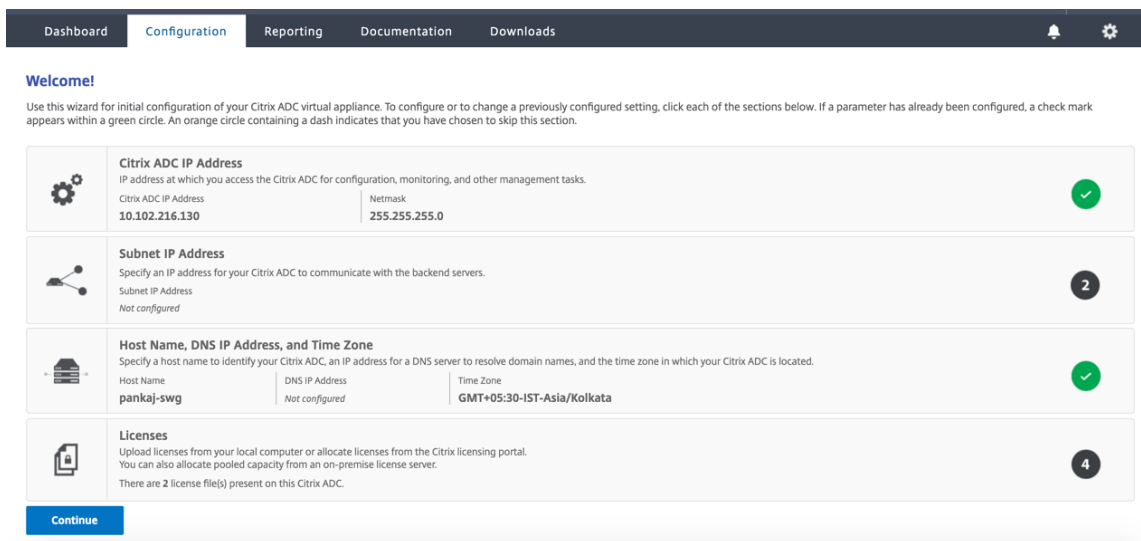
The SWG wizard provides administrators with a tool for managing the entire SWG deployment by using a web browser. It helps guide the customers to bring up an SWG service quickly and helps simplify the configuration by following a sequence of well-defined steps.

1. Open your web browser and enter the NSIP address that you specified during initial configuration. For more information about initial configuration, see [Initial configuration](#).
2. Type your user name and password.



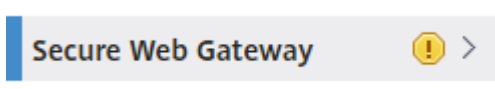
The image shows a login form with a dark blue background. On the left, the labels 'User Name' and 'Password' are displayed in a light gray font. To the right of each label is a white rectangular input field. Below these two fields is a wide, horizontal blue button with the text 'Log On' in white, centered on the button.

3. If you have not specified a subnet IP (SNIP) address, the following screen appears.

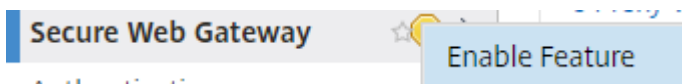


In Subnet IP Address, enter an IP address and subnet mask. The check mark in a green circle indicates that the value is configured.

4. In **Host Name, DNS IP Address, and Time Zone**, add the IP address of a DNS server to resolve domain names, and specify your time zone.
5. Click **Continue**.
6. (Optional) You might see an exclamation mark, as follows:



This mark indicates that the feature is not enabled. To enable the feature, right-click the feature and then click **Enable Feature**.



7. In the navigation pane, click **Secure Web Gateway**. In **Getting Started**, click **Secure Web Gateway Wizard**.



8. Follow the steps in the wizard to configure your deployment.

Add a listen policy to the transparent proxy server

1. Navigate to **Secure Web Gateway > Proxy Servers**. Select the transparent proxy server and click **Edit**.
2. Edit **Basic Settings**, and click **More**.
3. In **Listen priority**, enter 1.
4. In **Listen Policy Expression**, enter the following expression:

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

This expression assumes standard ports for HTTP and HTTPS traffic. If you have configured different ports, for example 8080 for HTTP or 8443 for HTTPS, modify the expression to reflect those ports.

Limitations

SWG is not supported in a cluster setup, in admin partitions, and on a Citrix ADC FIPS appliance.

Get started with an SWG instance on a Citrix ADC SDX appliance

June 25, 2019

The Citrix ADC SDX appliance is a multitenant platform on which you can provision and manage multiple virtual Citrix ADC instances. The SDX appliance addresses cloud computing and multitenancy requirements by allowing a single administrator to configure and manage the appliance and delegate the administration of each hosted instance to tenants. The SDX appliance enables the appliance administrator to provide each tenant the following benefits. They are given below:

- One complete instance. Each instance has the following privileges:
 - Dedicated CPU and memory resources
 - A separate space for entities
 - The independence to run the release and build of their choice
 - Lifecycle independence
- A completely isolated network. Traffic meant for a particular instance is sent only to that instance.

If you have not already installed your Citrix ADC SDX appliance, see [Hardware Installation](#) for information about installing the appliance.

You must use the Management Service to perform initial configuration of the Citrix ADC SDX appliance. For more information, see [Getting Started with the Management Service User Interface](#).

You can provision Citrix SWG instances on the Citrix ADC SDX appliance the same way that you would provision a Citrix ADC VPX instance. To provision an SWG instance on an SDX appliance, you need to install an “SDX - 10K concurrent sessions SWG add-on pack” license. This license is similar to SDX instance packs for VPX but is exclusive to SWG instances. For more information about provisioning Citrix ADC instances, see [Provisioning Citrix ADC instances](#).

To configure the Citrix SWG instance to receive traffic, follow the instructions in [Getting Started with a Citrix SWG Appliance](#).

Proxy modes

April 28, 2020

The Citrix Secure Web Gateway (SWG) appliance acts as a client’s proxy to connect to the internet and SaaS applications. As a proxy, it accepts all the traffic and determines the traffic’s protocol. Unless the traffic is HTTP or SSL, it is forwarded to the destination as is. When the appliance receives a request from a client, it intercepts the request and performs some actions, such as user authentication, site categorization, and redirection. It uses policies to determine which traffic to allow and which traffic to block.

The appliance maintains two different sessions, one between the client and the proxy and the other between the proxy and the origin server. The proxy relies on customer defined policies to allow or block HTTP and HTTPS traffic. Therefore, it is important that you define policies to bypass sensitive data, such as financial information. The appliance offers a rich set of Layer 4 to Layer 7 traffic attributes and user-identity attributes to create traffic management policies.

For SSL traffic, the proxy verifies the origin server’s certificate and establishes a legitimate connection with the server. It then emulates the server certificate, signs it using a CA certificate installed on Citrix SWG, and presents the created server certificate to the client. You must add the CA certificate as a trusted certificate to the client’s browser in order for the SSL session to be successfully established.

The appliance supports transparent and explicit proxy modes. In explicit proxy mode, the client must specify an IP address in their browser, unless the organization pushes the setting onto the client’s device. This address is the IP address of a proxy server that is configured on the SWG appliance. All client requests are sent to this IP address. For explicit proxy, you must configure a content switching virtual server of type PROXY and specify an IP address and a valid port number.

Transparent proxy, as the name implies, is transparent to the client. That is, the clients might not be aware that a proxy server is mediating their requests. The SWG appliance is configured in an inline deployment, and transparently accepts all HTTP and HTTPS traffic. For transparent proxy, you must configure a content switching virtual server of type PROXY, with asterisks (* *) as the IP address and port. When using the Secure Web Gateway wizard in the GUI, you do not have to specify an IP address and port.

Note

To intercept protocols other than HTTP and HTTPS in transparent proxy mode, you must add a listen policy and bind it to the proxy server.

Configure SSL forward proxy by using the Citrix SWG CLI

At the command prompt, type:

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

Arguments:**Name:**

Name for the proxy server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the CS virtual server is created.

The following requirement applies only to the CLI:

If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my server" or 'my server').

This is a mandatory argument. Maximum Length: 127

IPAddress:

IP address of the proxy server.

port:

Port number for proxy server. Minimum value: 1

Example for explicit proxy:

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

Example for transparent proxy:


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

Add a listen policy to the transparent proxy server by using the Citrix SWG GUI

1. Navigate to **Secure Web Gateway > Proxy Servers**. Select the transparent proxy server and click **Edit**.
2. Edit **Basic Settings**, and click **More**.
3. In **Listen priority**, enter 1.
4. In **Listen Policy Expression**, enter the following expression:

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

Note

This expression assumes standard ports for HTTP and HTTPS traffic. If you have configured different ports, for example 8080 for HTTP or 8443 for HTTPS, modify the above expression to specify those ports.

SSL interception

January 30, 2019

A Citrix Secure Web Gateway (SWG) appliance configured for SSL interception acts as a proxy. It can intercept and decrypt SSL/TLS traffic, inspect the unencrypted request, and enable an admin to enforce compliance rules and security checks. SSL Interception uses a policy that specifies which traffic to intercept, block, or allow. For example, traffic to and from financial web sites, such as banks, must not be intercepted, but other traffic can be intercepted, and blacklisted sites can be identified and blocked. Citrix recommends that you configure one generic policy to intercept traffic and more specific policies to bypass some traffic.

The client and the Citrix SWG proxy establish an HTTPS/TLS handshake. The SWG proxy establishes another HTTPS/TLS handshake with the server and receives the server certificate. The proxy verifies the server certificate on behalf of the client, and also checks the validity of the server certificate by using Online Certificate Status Protocol (OCSP). It regenerates the server certificate, signs it by using the key of the CA certificate installed on the appliance, and presents it to the client. Therefore, one certificate is used between the client and the Citrix ADC appliance, and another certificate between the appliance and the back-end server.

Important

The CA certificate that is used to sign the server certificate must be preinstalled on all the client devices, so that the regenerated server certificate is trusted by the client.

For intercepted HTTPS traffic, the SWG proxy server decrypts the outbound traffic, accesses the clear text HTTP request, and can use any Layer 7 application to process the traffic, such as by looking into the plain text URL and allowing or blocking access on the basis of the corporate policy and URL reputation. If the policy decision is to allow access to the origin server, the proxy server forwards the reencrypted request to the destination service (on the origin server). The proxy decrypts the response from the origin server, accesses the clear text HTTP response, and optionally applies any policies to the response. The proxy then reencrypts the response and forwards it to the client. If the policy decision is to block the request to the origin server, the proxy can send an error response, such as HTTP 403, to the client.

To perform SSL interception, in addition to the proxy server configured earlier, you must configure the following on an SWG appliance:

- SSL profile
- SSL policy
- CA certificate store
- SSL-error autolearning and caching

SSL profile

June 25, 2020

An SSL profile is a collection of SSL settings, such as ciphers and protocols. A profile is helpful if you have common settings for different servers. Instead of specifying the same settings for each server, you can create a profile, specify the settings in the profile, and then bind the profile to different servers. If a custom front-end SSL profile is not created, the default front-end profile is bound to client-side entities. This profile enables you to configure settings for managing the client-side connections. For SSL interception, you must create an SSL profile and enable SSL interception (SSLi) in the profile. A default cipher group is bound to this profile, but you can configure more ciphers to suit your deployment. You must bind an SSLi CA certificate to this profile and then bind the profile to a proxy server. For SSL interception, the essential parameters in a profile are the ones used to check the OCSP status of the origin server certificate, trigger client renegotiation if the origin server requests renegotiation, and verify the origin server certificate before reusing the front-end SSL session. You must use the default backend profile when communicating with the origin servers. Set any server-side parameters, such as cipher suites, in the default backend profile. A custom back-end profile is not supported.

For examples of the most commonly used SSL settings, see “Sample Profile” at the end of this section.

Cipher/protocol support differs on the internal and external network. In the following tables, the connection between the users and an SWG appliance is the internal network. The external network is between the appliance and the internet.



Table 1: Cipher/protocol support matrix for the internal network

(Cipher/protocol)/Platform	MPX (N3)*	VPX
TLS 1.1/1.2	12.1	12.1
ECDHE/DHE(Example TLS1-ECDHE-RSA-AES128-SHA)	12.1	12.1
AES-GCM(Example TLS1.2-AES128-GCM-SHA256)	12.1	12.1
SHA-2 Ciphers(Example TLS1.2-AES-128-SHA256)	12.1	12.1
ECDSA(Example TLS1-ECDHE-ECDSA-AES256-SHA)	12.1	12.1

Table 2: Cipher/protocol support matrix for the external network

(Cipher/protocol)/Platform	MPX (N3)*	VPX
TLS 1.1/1.2	12.1	12.1
ECDHE/DHE(Example TLS1-ECDHE-RSA-AES128-SHA)	12.1	12.1
AES-GCM(Example TLS1.2-AES128-GCM-SHA256)	12.1	12.1
SHA-2 Ciphers(Example TLS1.2-AES-128-SHA256)	12.1	12.1
ECDSA(Example TLS1-ECDHE-ECDSA-AES256-SHA)	12.1	Not supported

* Use the **sh hardware** (show hardware) command to identify whether your appliance has N3 chips.

Example:

```
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-->
```

Add an SSL profile and enable SSL interception by using the Citrix SWG CLI

At the command prompt, type:

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

Arguments:

sslInterception:

Enable or disable interception of SSL sessions.

Possible values: ENABLED, DISABLED

Default value: DISABLED

ssliReneg:

Enable or disable triggering client renegotiation when a renegotiation request is received from the origin server.

Possible values: ENABLED, DISABLED

Default value: ENABLED

ssliOCSPCheck:

Enable or disable OCSP check for an origin-server certificate.

Possible values: ENABLED, DISABLED

Default value: ENABLED

sslMaxSessPerServer:

Maximum number of SSL sessions to be cached per dynamic origin server. A unique SSL session is created for each SNI extension received from the client in a client hello message. The matching session is used for server-session reuse.

Default value: 10

Minimum value: 1

Maximum value: 1000

Example:

```
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:
44                                     NO
45
46     Push flag:           0x0 (Auto)
47
48     SSL quantum size:           8 kB
49
50     Encryption trigger timeout           100 mS
51
52     Encryption trigger packet count:           45
53
54     Subject/Issuer Name Insertion Format: Unicode
55
56     SSL Interception: ENABLED
57
58     SSL Interception OCSP Check: ENABLED
59
60     SSL Interception End to End Renegotiation: ENABLED
61
62     SSL Interception Server Cert Verification for Client
63     Reuse: ENABLED
64
65     SSL Interception Maximum Reuse Sessions per Server: 10
66
67     Session Ticket: DISABLED           Session Ticket
68     Lifetime: 300 (secs)
69
70     HSTS: DISABLED
71
72     HSTS IncludeSubDomains: NO
73
74     HSTS Max-Age: 0
75
76     ECC Curve: P_256, P_384, P_224, P_521
77
78     1) Cipher Name: DEFAULT Priority :1
79     Description: Predefined Cipher Alias
80 Done
81 <!--NeedCopy-->
```

Bind an SSL interception CA certificate to an SSL profile by using the Citrix SWG CLI

At the command prompt, type:

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

Example:

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

Bind an SSL interception CA certificate to an SSL profile by using the Citrix SWG GUI

1. Navigate to **System > Profiles > SSL Profile**.
2. Click **Add**.
3. Specify a name for the profile.

4. Enable **SSL Sessions Interception**.
5. Click **OK**.
6. In **Advanced Settings**, click **Certificate Key**.
7. Specify an SSLi CA certificate key to bind to the profile.
8. Click **Select** and then click **Bind**.
9. Optionally, configure ciphers to suit your deployment.
 - Click the edit icon, and then click **Add**.
 - Select one or more cipher groups, and click the right arrow.
 - Click **OK**.
10. Click **Done**.

Bind an SSL profile to a proxy server by using the Citrix SWG GUI

1. Navigate to **Secure Web Gateway > Proxy Servers**, and add a new server or select a server to modify.
2. In **SSL Profile**, click the edit icon.
3. In the **SSL Profile** list, select the SSL profile that you created earlier.
4. Click **OK**.
5. Click **Done**.

Sample Profile:

```
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:
    NO
38
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
    Lifetime: 300 (secs)
58
59 HSTS: DISABLED
60
61 HSTS IncludeSubDomains: NO
62
63 HSTS Max-Age: 0
64
65 ECC Curve: P_256, P_384, P_224, P_521
66
```

```
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-->
```

SSL policy infrastructure for SSL interception

February 24, 2020

A policy acts like a filter on incoming traffic. Policies on the Citrix Secure Web Gateway (SWG) appliance help define how to manage proxied connections and requests. The processing is based on the actions that are configured for that policy. That is, data in connection requests is compared to a rule specified in the policy, and the action is applied to connections that match the rule (expression). After defining an action for the policy and creating the policy, bind it to a proxy server, so that it applies to traffic flowing through that proxy server.

An SSL policy for SSL interception evaluates incoming traffic and applies a predefined action to requests that match a rule (expression). A decision to intercept, bypass, or reset a connection is made based on the defined SSL policy. You can configure one of three actions for a policy—INTERCEPT, BYPASS, or RESET. Specify an action when you create a policy. To put a policy into effect, you must bind it to a proxy server on the appliance. To specify that a policy is intended for SSL interception, you must specify the type (bind point) as INTERCEPT_REQ when you bind the policy to a proxy server. When unbinding a policy, you must specify the type as INTERCEPT_REQ.

Note:

The proxy server can decide to intercept only if you specify a policy.

Traffic interception can be based on any SSL handshake attribute. The most commonly used is the SSL domain. The SSL domain is usually indicated by the attributes of the SSL handshake. It can be the Server Name Indicator value extracted from the SSL Client Hello message, if present, or the Server Alternate Name (SAN) value extracted from the origin server certificate. The SSLi policy on Citrix SWG presents a special attribute named DETECTED_DOMAIN, which makes it easier for the customers to author interception policies based on the SSL domain from the origin server certificate. The customer can match the domain name against a string, URL list (URL set or [patset](#)), or a URL category derived from the domain.

Create an SSL policy by using the Citrix SWG CLI

At the command prompt, type:

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

Examples:

The following examples are for policies with expressions that use the `detected_domain` attribute to check for a domain name.

Do not intercept traffic to a financial institution, such as XYZBANK

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

Do not allow a user to connect to YouTube from the corporate network.

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

Intercept all user traffic.

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

If the customer doesn't want to use the `detected_domain`, they can use any of the SSL handshake attributes to extract and infer the domain.

For example, a domain name is not found in the SNI extension of the client hello message. The domain name must be taken from the origin server certificate. The following examples are for policies with expressions that check for a domain name in the subject name of the origin server certificate.

Intercept all user traffic to any Yahoo domain.

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

Intercept all user traffic for the category "Shopping/Retail".

```
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-->
```

Intercept all user traffic to an uncategorized URL.

```
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-->
```

The following examples are for policies that match the domain against an entry in a URL set.

Intercept all user traffic if the domain name in SNI matches an entry in the URL set “top100”.

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

Intercept all user traffic of the domain name if the origin server certificate matches an entry in the URL set “top100”.

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

Create an SSL policy to a proxy server by using the SWG GUI

1. Navigate to **Secure Web Gateway > SSL > Policies**.
2. On the **SSL Policies** tab, click **Add** and specify the following parameters:
 - Policy name
 - Policy action –Select from intercept, bypass, or reset.
 - Expression
3. Click **Create**.

Bind an SSL policy to a proxy server by using the SWG CLI

At the command prompt, type:

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

Example:

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

Bind an SSL policy to a proxy server by using the Citrix SWG GUI

1. Navigate to **Secure Web Gateway > Proxy Virtual Servers**.
2. Select a virtual server and click **Edit**.
3. In **Advanced Settings**, click **SSL Policies**.

4. Click inside the **SSL Policy** box.
5. In **Select Policy**, select a policy to bind.
6. In **Type**, select **INTERCEPT_REQ**.
7. Click **Bind** and then click **OK**.

Unbind an SSL policy to a proxy server by using the command line

At the command prompt, type:

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

SSL expressions used in SSL policies for SWG

Expression	Description
<code>CLIENT.SSL.CLIENT_HELLO.SNI.*</code>	Returns the SNI extension in a string format. Evaluate the string to see if it contains the specified text. Example: <code>client.ssl.client_hello.sni.contains("xyz.com")</code>
<code>CLIENT.SSL.ORIGIN_SERVER_CERT.*</code>	Returns a certificate, received from a back-end server, in a string format. Evaluate the string to see if it contains the specified text. Example: <code>client.ssl.origin_server_cert.subject.contains("xyz.com")</code>
<code>CLIENT.SSL.DETECTED_DOMAIN.*</code>	Returns a domain, either from the SNI extension or from the origin server certificate, in a string format. Evaluate the string to see if it contains the specified text. Example: <code>client.ssl.detected_domain.contains("xyz.com")</code>

SSL interception certificate store

August 26, 2019

An SSL certificate, which is an integral part of any SSL transaction, is a digital data form (X509) that identifies a company (domain) or an individual. An SSL certificate is issued by a certificate authority (CA). A CA can be private or public. Certificates issued by public CAs, such as Verisign, are trusted by applications that conduct SSL transactions. These applications maintain a list of CAs that they trust.

As a forward proxy, a Citrix Secure Web Gateway (SWG) appliance performs encryption and decryption of traffic between a client and a server. It acts as a server to the client (user) and as a client to the server. Before an appliance can process HTTPS traffic, it must validate the identity of a server to prevent any fraudulent transactions. Therefore, as a client to the origin server, the appliance must verify the origin server certificate before accepting it. To verify a server's certificate, all the certificates (for example, root and intermediate certificates) that are used to sign and issue the server certificate must be present on the appliance. A default set of CA certificates is preinstalled on an appliance. The Citrix SWG can use these certificates to verify almost all of the common origin-server certificates. This default set cannot be modified. However, if your deployment requires more CA certificates, you can create a bundle of such certificates and import the bundle to the appliance. A bundle can also contain a single certificate.

When you import a certificate bundle to the appliance, the appliance downloads the bundle from the remote location and, after verifying that the bundle contains only certificates, installs it on the appliance. You must apply a certificate bundle before you can use it to validate a server certificate. You can also export a certificate bundle for editing or to store it in an offline location as a backup.

Import and apply a CA certificate bundle on the appliance by using the Citrix SWG CLI

At the command prompt, type:

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

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

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

ARGUMENTS:

Name:

Name to assign to the imported certificate bundle. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the CLI:

If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, “my file” or ‘my file’).

Maximum Length: 31

src:

URL specifying the protocol, host, and path, including file name, to the certificate bundle to be imported or exported. For example, `http://www.example.com/cert_bundle_file`.

NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

Maximum Length: 2047

Example:

```
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-->
```

Import and apply a CA certificate bundle on the appliance by using the Citrix SWG GUI

1. Navigate to **Secure Web Gateway > Getting Started > Certificate Bundles**.
2. Do one of the following:
 - Select a certificate bundle from the list.
 - To add a new certificate bundle, click “+” and specify a name and source URL. Click **OK**.
3. Click **OK**.

Remove a CA certificate bundle from the appliance by using the CLI

At the command prompt, type:

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


Example:

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

Export a CA certificate bundle from the appliance by using the Citrix SWG CLI

At the command prompt, type:

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

ARGUMENTS:**Name:**

Name to assign to the imported certificate bundle. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the CLI:

If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

Maximum Length: 31

src:

URL specifying the protocol, host, and path, including file name, to the certificate bundle to be imported or exported. For example, http://www.example.com/cert_bundle_file.

NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

Maximum Length: 2047

Example:

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

Import, apply, and verify a CA certificate bundle from the Mozilla CA certificate store

At the command prompt, type:

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

To apply the bundle, type:

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

To verify the certificate bundle in use, type:

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

Limitation

Certificate bundles are not supported in a cluster setup, or on a partitioned appliance.

SSL error autolearning

June 25, 2019

The Citrix SWG appliance adds a domain to the SSL bypass list if learning mode is on. The learning mode is based on the SSL alert message received from either a client or an origin server. That is, learning is dependent on the client or server sending an alert message. There is no learning if an alert message is not sent. The appliance learns if any of the following conditions are met:

1. A request for a client certificate is received from the server.
2. Any one of following alerts is received as part of the handshake:
 - BAD_CERTIFICATE
 - UNSUPPORTED_CERTIFICATE
 - CERTIFICATE_REVOKED
 - CERTIFICATE_EXPIRED
 - CERTIFICATE_UNKNOWN
 - UNKNOWN_CA (If a client uses pinning, it sends this alert message if it receives a server certificate.)
 - HANDSHAKE_FAILURE

To enable learning, you must enable the error cache and specify the memory reserved for this.

Enable learning by using the Citrix SWG GUI

1. Navigate to **Secure Web Gateway > SSL**.

2. In **Settings**, click **Change advanced SSL settings**.
3. In **SSL Interception**, select **SSL Interception Error Cache**.
4. In **SSL Interception Max Error Cache Memory**, specify the memory (in bytes) to reserve.

The screenshot shows a dialog box titled "SSL Interception". It has a checked checkbox for "SSL Interception Error Cache". Below it is a text input field for "SSL Interception Max Error Cache Memory" with the value "1048576". At the bottom, there are two buttons: "OK" and "Close".

5. Click **OK**.

Enable learning by using the Citrix SWG CLI

At the command prompt type:

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

Arguments:

ssliErrorCache:

```
1      Enable or disable dynamic learning, and cache the learned
      information to make subsequent decisions to intercept or
      bypass requests. When enabled, the appliance performs a
      cache lookup to decide whether to bypass the request.
2
3      Possible values: `ENABLED, DISABLED`
4
5      Default value: `DISABLED`
```

ssliMaxErrorCacheMem:

```
1      Specify the maximum memory, in bytes, that can be used to
      cache the learned data. This memory is used as a LRU cache
      so that the old entries are replaced with new entries
      after the set memory limit is exhausted. A value of 0
      decides the limit automatically.
2
3      Default value: 0
4
5      Minimum value: 0
6
7      Maximum value: 4294967294
```

User identity management

April 28, 2020

An increasing number of security breaches and the growing popularity of mobile devices has emphasized the need to ensure that use of the external internet is compliant with the corporate policies and only authorized users access external resources provisioned by the corporate personnel. Identity Management makes this possible by verifying the identity of a person or a device. It does not determine what tasks the individual can take or what files the individual can see.

A Secure Web Gateway (SWG) deployment identifies the user before allowing access to the internet. All requests and responses from the user are inspected. User activity is logged, and records are exported to the Citrix Application Delivery Management (ADM) for reporting. In Citrix ADM, you can view the statistics about the user activities, transactions, and bandwidth consumption.

By default, only the user's IP address is saved, but you can configure the Citrix SWG appliance to record more details about the user, and use this identity information to create richer internet usage policies for specific users.

The Citrix ADC appliance supports the following authentication modes for an explicit-proxy configuration.

- **Lightweight Directory Access Protocol (LDAP).** Authenticates the user through an external LDAP authentication server. For more information, see [LDAP Authentication Policies](#).
- **RADIUS.** Authenticates the user through an external RADIUS server. For more information, see [RADIUS Authentication Policies](#).
- **TACACS+.** Authenticates the user through an external Terminal Access Controller Access-Control System (TACACS) authentication server. For more information, see [Authentication Policies](#).
- **Negotiate.** Authenticates the user through a Kerberos authentication server. If there is an error in Kerberos authentication, appliance uses NTLM authentication. For more information, see [Negotiate Authentication Policies](#).

For transparent proxy, only IP-based LDAP authentication is currently supported. When a client request is received, the proxy authenticates the user by checking an entry for the client IP address in the active directory, and creates a session based on the user IP address. However, if you configure the `ssoNameAttribute` in an LDAP action, a session is created by using the username instead of the IP address. Classic policies are not supported for authentication in a transparent proxy setup.

Note

For explicit proxy, you must set the LDAP login name to `sMAccountName`. For transparent proxy, you must set the LDAP login name to `networkAddress` and `attribute1` to

sAMAccountName.

Example for explicit proxy:

```
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
  freesd123$ -ldapLoginName sAMAccountName
2 <!--NeedCopy-->
```

Example for transparent proxy:

```
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
  freesd123$ -ldapLoginName networkAddress -authentication disable -
  Attribute1 sAMAccountName
2 <!--NeedCopy-->
```

Set up user authentication by using the Citrix SWG CLI

At the command prompt type:

```
1 add authentication vservice <vservice name> SSL
2
3 bind ssl vservice <vservice 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 vservice <vservice name> -policy <string> -priority <
  positive_integer>
10
11 set cs vservice <name> -authn401 ON -authnVsName <string>
12 <!--NeedCopy-->
```

Arguments:

Vservice name:

Name of the authentication virtual service to which to bind the policy.

Maximum Length: 127

serviceType:

Protocol type of the authentication virtual service. Always SSL.

Possible values: SSL

Default value: SSL

Action name:

Name for the new LDAP action. Must begin with a letter, number, or the underscore character (`_`), and must contain only letters, numbers, and the hyphen (`-`), period (`.`) pound (`#`), space (), at (`@`), equals (`=`), colon (`:`), and underscore characters. Cannot be changed after the LDAP action is added. The following requirement applies only to the CLI:

If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, “my authentication action” or ‘my authentication action’).

Maximum Length: 127

serverIP:

IP address assigned to the LDAP server.

ldapBase:

Base (node) from which to start LDAP searches. If the LDAP server is running locally, the default value of base is `dc=netcaler,dc=com`. Maximum Length: 127

ldapBindDn:

Full distinguished name (DN) that is used to bind to the LDAP server.

Default: `cn=Manager,dc=netcaler,dc=com`

Maximum Length: 127

ldapBindDnPassword:

Password used to bind to the LDAP server.

Maximum Length: 127

ldapLoginName:

LDAP login name attribute. The Citrix ADC appliance uses the LDAP login name to query external LDAP servers or Active Directories. Maximum Length: 127

Policy name:

Name for the advance AUTHENTICATION policy. Must begin with a letter, number, or the underscore character (`_`), and must contain only letters, numbers, and the hyphen (`-`), period (`.`) pound (`#`), space (), at (`@`), equals (`=`), colon (`:`), and underscore characters. Cannot be changed after AUTHENTICATION policy is created. The following requirement applies only to the CLI:

If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, “my authentication policy” or ‘my authentication policy’).

Maximum Length: 127

rule:

Name of the rule, or a default syntax expression, that the policy uses to determine whether to attempt to authenticate the user with the AUTHENTICATION server.

Maximum Length: 1499

action:

Name of the authentication action to be performed if the policy matches.

Maximum Length: 127

priority:

Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Policies are evaluated in the order of their priorities, and the first policy that matches the request is applied. Must be unique within the list of policies bound to the authentication virtual server.

Minimum value: 0

Maximum Value: 4294967295

Example:

```
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
  Done
14
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-->
```

Enable user name logging by using the Citrix SWG CLI

At the command prompt, type:

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

Arguments:

AAAUserName

Enable AppFlow AAA user name logging.

Possible values: `ENABLED`, `DISABLED`

Default value: `DISABLED`

Example:

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

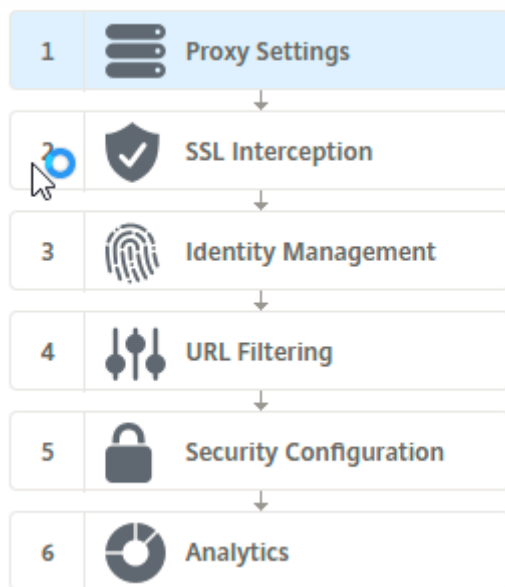
URL filtering

June 25, 2019

URL Filtering provides policy based control of websites by using the information contained in URLs. This feature helps network administrators monitor and control user access to malicious websites on the network.

Get started

If you are a new user and want to configure URL filtering, you must complete the initial SWG setup. To get started with URL Filtering, you must first log on to the Citrix SWG Wizard. The wizard takes you through a series of configuration steps before you apply the URL Filtering policies.

**Note**

Before you begin, be sure you have a valid URL Threat Intelligence feature license installed on your appliance. If you are using a trial version, be sure to purchase a valid license to continue using this feature on the SWG appliance.

Log on to SWG wizard

The Citrix SWG Wizard guides you through a series of simplified configuration tasks and the right pane displays the corresponding flow sequence. You can use this wizard to apply URL Filtering policies to a URL list or a predefined list of categories.

Step 1: Configure proxy settings

You must first configure a proxy server through which the client accesses the SWG gateway. This server is of type SSL, and it operates in explicit or transparent mode. For more information about proxy server configuration, see [Proxy Modes](#).

Step 2: Configure SSL interception

After configuring the proxy server, you must configure the SSL interception proxy to intercept encrypted traffic at the Citrix SWG appliance. In the case of URL filtering, the SSL proxy intercepts the traffic and blocks blacklisted URL while all other traffic can be bypassed. For more information about configuring SSL interception, see [SSL Interception](#).

Step 3: Configure identity management

A user is authenticated before being allowed to log on to the enterprise network. Authentication provides the flexibility to define specific policies for a user or a group of users, based on their roles. For more information about user authentication, see [User Identify Management](#)

Step 4: Configure URL filtering

The administrator can apply a URL filtering policy either by using the URL Categorization feature or by using the URL List feature.

URL Categorization. Controls access to websites and web pages by filtering traffic on the basis of a predefined list of categories.

URL List. Controls access to blacklisted websites and web pages by denying access to URLs that are in a URL set imported into the appliance.

Step 5: Configure security configuration

This step enables you to configure a reputation score and allow users to control access to the websites by denying access if the score is too low. Your reputation score can range from one to four, and you can configure the threshold at which the score becomes unacceptable. For scores that exceed the threshold, you can select a policy action to allow, block, or redirect traffic. For more information, see [Security Configuration](#).

Step 6: Configure SWG analytics

This step enables you to activate SWG analytics for categorizing web traffic, logging URL category in the user transaction logs and viewing traffic analytics. For more information about SWG Analytics, see [Analytics](#).

Step 7: Click Done to complete the initial configuration and continue managing URL filtering configuration

URL list

August 10, 2020

The URL List feature enables enterprise customers to control access to specific websites and website categories. The feature filters websites by applying a responder policy bound to a URL matching algorithm. The algorithm matches the incoming URL against a URL set consisting of up to one million (1,000,000) entries. If the incoming URL request matches an entry in the set, the appliance uses the responder policy to evaluate the request (HTTP/HTTPS) and control access to it.

URL set types

Each entry in a URL set can include a URL and, optionally, its metadata (URL category, category groups, or any other related data). For URLs with metadata, the appliance uses a policy expression that evaluates the metadata. For more information, see [URL Set](#).

Citrix SWG supports custom URL sets. You can also use pattern sets to filter URLs.

Custom URL set. You can create a customized URL set with up to 1,000,000 URL entries and import it as a text file into your appliance.

Pattern set. An SWG appliance can use pattern sets to filter URLs before granting access to websites. A pattern set is a string-matching algorithm that looks for an exact string match between an incoming URL and up to 5000 entries. For more information, see [Pattern Set](#).

Each URL in an imported URL set can have a custom category in the form of URL metadata. Your organization can host the set and configure the SWG appliance to periodically update the set without requiring manual intervention.

After the set is updated, the Citrix ADC appliance automatically detects the metadata, and the category is available as a policy expression for evaluating the URL and applying an action such as allow, block, redirect, or notify the user.

Advanced policy expressions used with URL sets

The following table describes the basic expressions you can use to evaluate incoming traffic.

1. `.URLSET_MATCHES_ANY` - Evaluates to `TRUE` if the URL exactly matches any entry in the URL set.
2. `.GET_URLSET_METADATA()` - The `GET_URLSET_METADATA()` expression returns the associated metadata if the URL exactly matches any pattern within the URL set. An empty string is returned if there is no match.
3. `.GET_URLSET_METADATA().EQ(<METADATA)` - `.GET_URLSET_METADATA().EQ(<METADATA)`
4. `.GET_URLSET_METADATA().TYPECAST_LIST_T(' , ').GET(0).EQ()` - Evaluates to `TRUE` if the matched metadata is at the beginning of the category. This pattern can be used to encode separate fields within metadata but match only the first field.

5. `HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL)` - Joins the host and URL parameters, which can then be used as a for matching.

Responder action types

Note: In the table, `HTTP.REQ.URL` is generalized as `<URL expression>`.

The following table describes the actions that can be applied to incoming internet traffic.

Responder Action	Description
Allow	Allow the request to access the target URL.
Redirect	Redirect the request to the URL specified as the target.
Block	Deny the request.

Prerequisites

You must configure a DNS server if you import a URL Set from a hostname URL. This is not required if you use an IP address.

At the command prompt, type:

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

Example:

```
1 add dns nameServer 10.140.50.5
```

Configure a URL list

To configure a URL list, you can use the Citrix SWG wizard or the Citrix ADC command-line interface (CLI). On the Citrix SWG appliance, you must first configure the responder policy and then bind the policy to a URL set.

Citrix recommends that you use the Citrix SWG Wizard as the preferred option to configure a URL list. Use the wizard to bind a responder policy to a URL set. Alternatively, you can bind the policy to a pattern set.

Configure a URL list by using the Citrix SWG wizard

To configure URL List for HTTPS traffic by using the Citrix SWG GUI:

1. Log on to the Citrix SWG appliance and navigate to **Secured Web Gateway** page.
2. In the details pane, do one of the following:
 - a) Click **Secured Web Gateway Wizard** to create a new SWG configuration with URL List feature.
 - b) Select an existing configuration and click **Edit**.
3. In the **URL Filtering** section, click **Edit**.
4. Select the **URL List** check box to enable the feature.
5. Select a **URL List** policy and Click **Bind**.
6. Click **Continue** and then **Done**.

For more information, see [How to Create a URL List Policy](#).

Configure a URL list by using the Citrix SWG CLI

To configure a URL list, do the following.

1. Configure a proxy virtual server for HTTP and HTTPS traffic.
2. Configure SSL interception for intercepting HTTPS traffic.
3. Configure a URL list containing a URL set for HTTP traffic.
4. Configure URL list containing URL set for HTTPS traffic.
5. Configure a private URL set.

Note

If you have already configured an SWG appliance, you can skip steps 1 and 2, and configure with step 3.

Configuring a proxy virtual server for Internet traffic The Citrix SWG appliance supports transparent and explicit proxy virtual servers. To configure a proxy virtual server for internet traffic in explicit mode, do the following:

1. Add a proxy SSL virtual server.
2. Bind a responder policy to the proxy virtual server.

To add a proxy virtual server by using the Citrix SWG CLI:

At the command prompt, type:

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

Example:

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

To bind a responder policy to a proxy virtual server by using the Citrix SWG CLI:

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

Note

If you have already configured the SSL interceptor as part of Citrix SWG configuration, you can skip the following procedure.

Configure SSL interception for HTTPS traffic To configure SSL interception for HTTPS traffic, do the following:

1. Bind a CA certificate-key pair to the proxy virtual server.
2. Enable the default SSL profile.
3. Create a front-end SSL profile, and bind it to the proxy virtual server and enable SSL interception in the front-end SSL profile.

To bind a CA certificate-key pair to the proxy virtual server by using the Citrix SWG CLI:

At the command prompt, type:

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

To configure a front-end SSL profile by using the Citrix SWG CLI:

At the command prompt, type:

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

To bind a front-end SSL profile to a proxy virtual server by using the Citrix SWG CLI

At the command prompt, type:

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

Configure a URL list by importing a URL set for HTTP traffic For information about how to configure a URL Set for HTTP traffic, see [URL Set](#).

Perform explicit subdomain match You can now perform an explicit subdomain match for an imported URL set. To do this, a new parameter, “subdomainExactMatch” is added to the **import policy URLset** command.

When you enable the parameter, the URL Filtering algorithm performs an explicit subdomain match. For example, if the incoming URL is `news.example.com` and if the entry in the URL set is `example.com`, the algorithm does not match the URLs.

At the command prompt, type:

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

Example

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

Configure a URL set for HTTPS traffic To configure a URL Set for HTTPS traffic by using the Citrix SWG CLI

At the command prompt type:

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

Example:

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

To configure a URL set for HTTPS traffic by using the Citrix SWG wizard Citrix recommends that you use the Citrix SWG wizard as the preferred option to configure a URL list. Use the wizard to import a custom URL set and bind to a responder policy.

1. Log on to the **Citrix SWG** appliance and navigate to **Secured Web Gateway > URL Filtering > URL Lists**.
2. In the details pane, click **Add**.
3. On the **URL List Policy** page, specify the policy name.
4. Select an option to import a URL set.

5. On the **URL List Policy** tab page, select the **Import URL Set** check box and specify the following URL Set parameters.
 - a) URL Set Name—Name of the custom URL set.
 - b) URL—Web address of the location at which to access the URL Set.
 - c) Overwrite—Overwrite a previously imported URL set.
 - d) Delimiter—Character sequence that delimits a CSV file record.
 - e) Row Separator—Row separator used in the CSV file.
 - f) Interval—Interval in seconds, rounded off to the nearest number of seconds equal to 15 minutes, at which the URL set is updated.
 - g) Private Set—Option to prevent exporting the URL set.
 - h) Canary URL—Internal URL for testing whether the content of the URL set is to be kept confidential. The maximum length of the URL is 2047 characters.
6. Select a responder action from the drop-down list.
7. Click **Create** and **Close**.

Configure a private URL set If you configure a private URL set and keep its contents confidential, the network administrator might not know the blacklisted URLs in the set. For such cases, you can configure a Canary URL and add it to the URL set. Using the Canary URL, the administrator can request the private URL Set to be used for every lookup request. You can refer to the wizard section for descriptions of each parameter.

To import a URL set by using the Citrix SWG CLI:

At the command prompt, type:

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

Example:

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

Display imported URL set

You can now display imported URL sets in addition to added URL sets. To do this, a new parameter “imported” is added to the “show urlset” command. If you enable this option, the appliance displays all imported URL sets and distinguishes the imported URL sets from the added URL sets.

At the command prompt, type:

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

Example

```
show policy urlset -imported
```

Configure audit log messaging

Audit logging enables you to review a condition or a situation in any phase of URL List process. When a Citrix ADC appliance receives an incoming URL, if the responder policy has an URL Set advanced policy expression, the audit log feature collects URL Set information in the URL and stores the details as a log message for any target allowed by audit logging.

1. The log message contains the following information:
2. Timestamp.
3. Log message type.
4. The predefined log levels (Critical, Error, Notice, Warning, Informational, Debug, Alert, and Emergency).
5. Log message information, such as URLset name, policy action, URL.

To configure audit logging for URL List feature, you must complete the following tasks:

1. Enable Audit Log.
2. Create Audit Log message action.
3. Set URL List responder policy with Audit Log message action.

For more information, see [Audit Logging](#) topic.

URL Pattern Semantics

July 8, 2020

The following table shows the URL patterns used for specifying the list of pages you to want to filter. For example, the pattern, `www.example.com/bar` matches only one page at `www.example.com/bar`. To match all the pages whose URL starts with ‘`www.example.com/bar`’, you add an asterisk (*) at the end of the URL.

Semantics for URL pattern to match metadata mapping

The pattern matching semantics is available in a table format. For more information, see [Pattern Semantics](#) pdf page.

Mapping URL Categories

July 8, 2020

A list of third party categories and category groups. For more information, see [URL Category Mapping](#) page.

Use case: URL filtering by using custom URL set

June 25, 2020

If you are an enterprise customer looking for a way to control access to specific websites and website categories, you can do by using a custom URL set bound to a responder policy. Your organization's network infrastructure can use a URL filter to block access to malicious or dangerous websites such as websites featuring adult, violence, gaming, drugs, politics, or job portals. In addition to filtering the URLs, you can create a customized list of URLs and import it to the SWG appliance. For example, your organization's policies might call for blocking access to certain websites such as social networking, shopping portals, and job portals.

Each URL in the list can have a custom category in the form of metadata. The organization can host the list of URLs as a URL set on the Citrix SWG appliance and configure the appliance to periodically update the set without requiring manual intervention.

After the set is updated, the Citrix ADC appliance automatically detects the metadata, and the responder policy uses the URL metadata (category details) to evaluate the incoming URL and apply an action such as allow, block, redirect or notify the user.

To implement this configure in your network, you can perform the following tasks:

1. Import a custom URL set
2. Add a custom URL set
3. Configure a custom URL list in the Citrix SWG Wizard

To import a custom URL Set by using the Citrix SWG CLI:

At the command prompt, type:

```
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
```

To add a custom URL set by using the Citrix SWG CLI:

At the command prompt, type:

```
add urlset <urlset_name>
```

```
1 Add urlset test1
```

Configure a URL list by using the Citrix SWG wizard

Citrix recommends that you use the Citrix SWG Wizard as the preferred option to configure a URL list. Use the wizard to import a custom URL set and bind it to a responder policy.

1. Log on to the **Citrix SWG** appliance and navigate to **Secured Web Gateway > URL Filtering > URL Lists**.
2. In the details pane, click **Add**.
3. On the **URL List Policy** page, specify the policy name.
4. Select an option to either import a URL set.
5. In the **URL List Policy** tab page, select the **Import URL Set** check box and specify the following URL Set parameters.
 - a) URL Set Name—Name of the custom URL set.
 - b) URL—Web address of the location at which to access the URL Set.
 - c) Overwrite—Overwrite a previously imported URL set.
 - d) Delimiter—Character sequence that delimits a CSV file record.
 - e) Row Separator—Row separator used in the CSV file.
 - f) Interval—Interval in seconds, rounded off to the nearest 15 minutes, at which the URL set is updated.
 - g) Private Set—Option to prevent exporting the URL set.
 - h) Canary URL—Internal URL for testing if the content of the URL set is to be kept confidential. The maximum length of the URL is 2047 characters.
6. Select a responder action from the drop-down list.
7. Click **Create** and **Close**.

The screenshot shows the 'URL List Policy' configuration page. At the top, there are two tabs: 'URL List Policies' and 'URL List Policy'. The main heading is 'URL List Policy'. Below this, there are 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 blue) and 'Close' (in white).

Metadata semantics for custom URL sets

To import a custom URL set, add the URLs to a text file and bind it to a responder policy to block Social networking URLs.

Following are examples of URLs that you might add to the text file:

cnn.com,News

bbc.com,News

google.com,Search Engine

yahoo.com,Search Engine

facebook.com,Social Media

twitter.com,Social Media

Configure a responder policy to block social media URLs by using the Citrix ADC CLI

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 Categorization

September 23, 2020

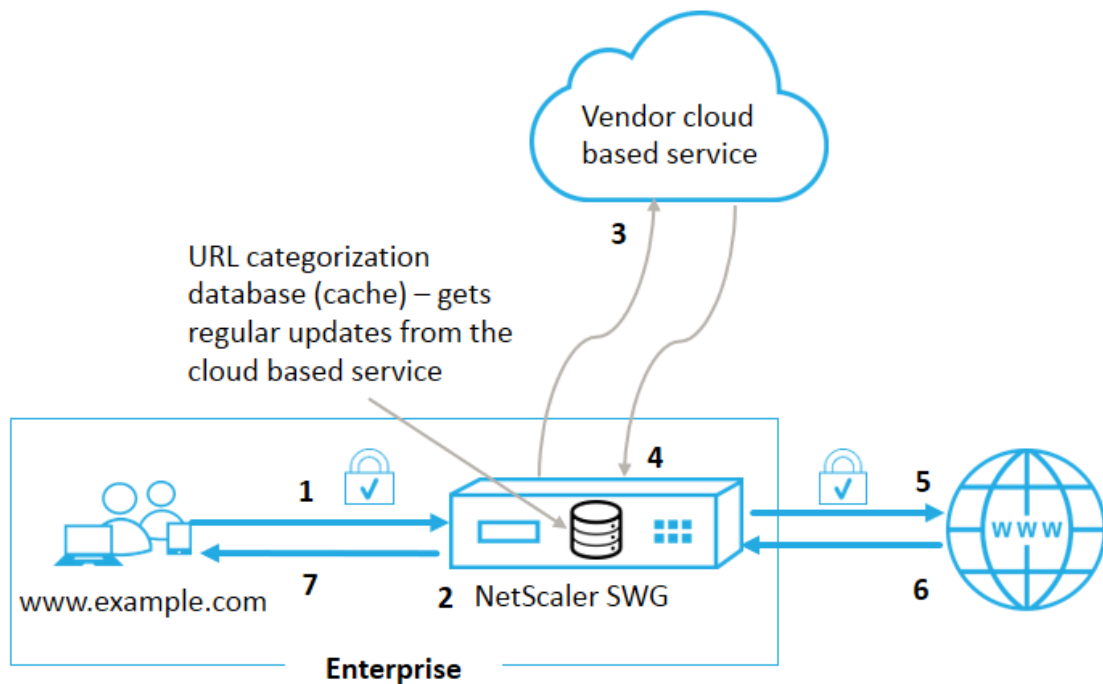
URL Categorization restricts user access to specific websites and website categories. As a subscribed service offered by Citrix Secure Web Gateway (SWG), the feature enables enterprise customers to filter web traffic by using a commercial categorization database. The database has a vast number (billions) of URLs classified into different categories, such as social networking, gambling, adult content, new media, and shopping. In addition to categorization, each URL has a reputation score kept up to date based on the site's historical risk profile. To filter your traffic, you can configure advanced policies based on categories, category groups (such as Terrorism, Illegal drugs), or site-reputation scores.

For example, you might block access to dangerous sites, such as sites known to be infected with malware, and selectively restrict access to content such as adult content or entertainment streaming media for enterprise users. You can also capture the user's transactional details and outbound traffic details for monitoring web traffic analytics on the Citrix ADM server.

Citrix ADC uploads or downloads data from the pre-configured NetSTAR device `nsv10.netstar-inc.com` and `incompasshybridpc.netstar-inc.com` is used as a cloud host by default for cloud-categorization requests. The appliance uses its NSIP address as source IP address and 443 as the destination port for communication.

How URL categorization works

The following figure shows how Citrix SWG URL categorization service is integrated with a commercial URL Categorization database and cloud services for frequent updates.



The components interact as follows:

1. A client sends internet bound URL request.
2. The Citrix SWG proxy applies a policy enforcement to the request based on the category details (such as, category, category group, and site-reputation score) retrieved from the URL categorization database. If the database returns the category details, the process jumps to step 5.
3. If the database misses the categorization details, the request is sent to a cloud-based lookup service maintained by a URL categorization vendor. However, the appliance does not wait for a response, instead, the URL is marked as uncategorized and a policy enforcement is performed (jump to step 5). The appliance continues to monitor the cloud query feedback and updates the cache so that future requests can benefit from the cloud lookup.
4. The SWG appliance receives the URL category details (category, category group, and reputation score) from the cloud-based service and stores it in the categorization database.
5. The policy allows the URL and the request is sent to the origin server. Otherwise, the appliance drops, redirects, or responds with a custom HTML page.
6. The origin server responds with the requested data to the SWG appliance.
7. The appliance sends the response to the client.

Use Case: Internet usage under corporate compliance for enterprises

You can use the URL Filtering feature to detect and implement compliance policies to block sites that violate corporate compliance. These can be sites such as adult, streaming media, social networking which might be deemed nonproductive or consume excess internet bandwidth in an enterprise network. Blocking access to these websites can improve employee productivity, reduce operating costs for bandwidth usage, and reduce the overhead of network consumption.

Prerequisites

The URL Categorization feature works on a Citrix SWG platform only if it has an optional subscription service with URL filtering capabilities and threat intelligence for Citrix Secure Web Gateway. The subscription allows customers to download the latest threat categorizations for websites and then enforce those categories on the Secure Web Gateway. The subscription is available for both hardware appliances and software (VPX) versions of Secure Web Gateway.

Before enabling and configuring the feature, you must install the following licenses:

CNS_WEBF_SSERVER_Retail.lic

CNS_XXXXX_SERVER_SWG_Retail.lic.

Where, XXXXX is the platform type, for example: V25000

Responder policy expressions

The following table lists the different policy expressions that you can use to verify if an incoming URL must be allowed, redirected, or blocked.

1. `<text>. URL_CATEGORIZE (<min_reputation>, <max_reputation>)` - Returns a `URL_CATEGORY` object. If `<min_reputation>` is greater than 0, the returned object does not contain a category with a reputation lower than `<min_reputation>`. If `<max_reputation>` is greater than 0, the returned object does not contain a category with a reputation higher than `<max_reputation>`. If the category fails to resolve in a timely manner, the `undef` value is returned.
2. `<url_category>. CATEGORY()` - Returns the category string for this object. If the URL does not have a category, or if the URL is malformed, the returned value is "Unknown."
3. `<url_category>. CATEGORY_GROUP()` - Returns a string identifying the object's category group. This is a higher level grouping of categories, which is useful in operations that require less detailed information about the URL category. If the URL does not have a category, or if the URL is malformed, the returned value is "Unknown."

4. `<url_category>. REPUTATION()` - Returns the reputation score as a number from 0 to 5, where 5 indicates the riskiest reputation. If there is the category is "Unknown", the reputation value is 1.

Policy types:

1. Policy to select requests for URLs that are in the Search Engine category - `add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY().EQ("Search Engine")`
2. Policy to select requests for URLs that are in the Adult category group - `add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY_GROUP().EQ("Adult")'`
3. Policy to select requests for Search Engine URLs with a reputation score lower than 4 - `add responder policy p2 'HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL).URL_CATEGORIZE(4,0).HAS_CATEGORY("Search Engine")`
4. Policy to select requests for Search Engine and Shopping URLs - `add responder policy p3 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY().EQ ("good_categories")`
5. Policy to select requests for Search Engine URLs with a reputation score equal to or greater than 4 - `add responder policy p5 'CLIENT.SSL.DETECTED_DOMAIN .URL_CATEGORIZE(4,0).CATEGORY().EQ("Search Engines")`
6. Policy to select requests for URLs that are in the Search Engine category and compare them with a URL Set - `' 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")'`

Responder policy types

There are two types of policies used in the URL Categorization feature and each of these policy types is explained below:

Policy Type	Description
URL Category	Categorize web traffic and based on evaluation result blocks, allows, or redirects traffic.
URL Reputation Score	Determines the reputation score of the website and allows you to control access based on the reputation score threshold level set by the administrator.

Configure URL categorization

To configure URL categorization on a Citrix SWG appliance, do the following:

1. Enable URL filtering.
2. Configure a proxy server for Web traffic.
3. Configure SSL interception for Web traffic in explicit mode.
4. Configure shared memory to limit cache memory.
5. Configure URL categorization parameters.
6. Configure URL categorization by using the Citrix SWG wizard.
7. Configure URL categorization parameters by using the SWG wizard.
8. Configure seed database path and cloud server name

Step 1: Enabling URL Filtering

To enable URL categorization, enable the URL filtering feature and enable modes for URL categorization.

To enable URL Categorization by using the Citrix SWG: CLI

At the command prompt, type:

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

Step 2: Configure a proxy server for web traffic in explicit mode

The Citrix SWG appliance supports transparent and explicit proxy virtual servers. To configure a proxy virtual server for SSL traffic in explicit mode, do the following:

1. Add a proxy server.
2. Bind an SSL policy to the proxy server.

To add a proxy server by using the Citrix SWG CLI

At the command prompt, type:

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

Example:

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

Bind an SSL policy to a proxy virtual server by using the Citrix SWG CLI

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

Step 3: Configure SSL interception for HTTPS traffic

To configure SSL interception for HTTPS traffic, do the following:

1. Bind a CA certificate-key pair to the proxy virtual server.
2. Configure the default SSL profile with SSL parameters.
3. Bind a front-end SSL profile to the proxy virtual server and enable SSL interception in the front-end SSL profile.

To bind a CA certificate-key pair to the proxy virtual server by using the Citrix SWG CLI

At the command prompt, type:

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

To configure the default SSL profile by using the Citrix SWG CLI

At the command prompt, type:

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

Bind a front-end SSL profile to a proxy virtual server by using the Citrix SWG CLI

At the command prompt, type:

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

Step 4: Configure shared memory to limit cache memory

To configure shared memory to limit cache memory by using the Citrix SWG CLI

At the command prompt, type:

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

Where, the memory limit configured for caching is set as 10 MB.

Step 5: Configure URL categorization parameters

To configure the URL categorization parameters by using the Citrix SWG CLI

At the command prompt, type:

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

Example:

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

Step 6: Configure URL Categorization by using the Citrix SWG Wizard

To configure URL Categorization by using the Citrix SWG GUI

1. Log on to the Citrix SWG appliance and navigate to **Secured Web Gateway** page.
2. In the details pane, do one of the following:
 - a) Click **Secured Web Gateway Wizard** to create a new configuration.
 - b) Select an existing configuration and click **Edit**.
3. In the **URL Filtering** section, click **Edit**.
4. Select the **URL Categorization** check box to enable the feature.
5. Select a **URL Categorization** policy and Click **Bind**.
6. Click **Continue** and then **Done**.

For more information about URL Categorization policy, see [How to Create a URL Categorization Policy](#).

Step 7: Configuring URL Categorization parameters by using SWG Wizard

To configure URL Categorization parameters by using the Citrix SWG GUI

1. Log on to **Citrix SWG** appliance and navigate to **Secured Web Gateway > URL Filtering**.
2. In the **URL Filtering** page, click **Change URL filtering settings** link.
3. In the **Configuring URL Filtering Params** page, specify the following parameters.
 - a) Hours Between DB Updates. URL Filtering hours between database updates. Minimum value: 0 and Maximum value: 720.

- b) Time of Day to Update DB. URL Filtering time of day to update database.
- c) Cloud Host. The URL path of the cloud server.
- d) Seed DB Path. The URL path of the seed database lookup server.

4. Click **OK** and **Close**.

Sample Configuration:

```
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-->

```

Configure seed database path and cloud server name

You can now configure the seed database path and cloud lookup server name for manual setting of the cloud lookup server name and the seed database path. To do this, two new parameters, “CloudHost” and “SeedDBPath”, are added to the URL filtering parameter command.

At the command prompt, type:

```

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

```

Example

```

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

```

The Communication between a Citrix ADC appliance and NetSTAR might require a domain name server. You can test using a simple console or telnet connection from the appliance.

Example:

```

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-->

```

Configure audit log messaging

Audit logging enables you to review a condition or a situation in any phase of URL Categorization process. When a Citrix ADC appliance receives an incoming URL, if the responder policy has a URL Filtering expression, the audit log feature collects URL Set information in the URL and stores it as log messages for any target allowed by audit logging.

- Source IP address (the IP address of the client that made the request).
- Destination IP address (the IP address of the requested server).
- Requested URL containing the schema, the host, and the domain name (<http://www.example.com>).
- URL category that the URL filtering framework returns.

- URL category group that the URL filtering framework returned.
- URL reputation number that the URL filtering framework returned.
- Audit log action taken by the policy.

To configure audit logging for the URL List feature, you must complete the following tasks:

1. Enable Audit Log.
2. Create Audit Log message action.
3. Set URL List responder policy with Audit Log message action.

For more information, see [Audit Logging](#) topic.

Storing failure errors using SYSLOG messaging

At any stage of the URL Filtering process, if there is a system-level failure, the Citrix ADC appliance uses the audit log mechanism to store logs in the ns.log file. The errors are stored as text messages in SYSLOG format so that, an administrator can view it later in a chronological order of event occurrence. These logs are also sent to an external SYSLOG server for archival. For more information, see [article CTX229399](#).

For example, if a failure occurs when you initialize the URL Filtering SDK, the error message is stored in the following messaging format.

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

The Citrix ADC appliance stores the error messages under four different failure categories:

- **Download failure.** If an error occurs when you try to download the categorization database.
- **Integration failure.** If an error occurs when you integrate an update into the existing categorization database.
- **Initialization failure.** If an error occurs when you initialize the URL Categorization feature, set categorization parameters, or end a categorization service.
- **Retrieval failure.** If an error occurs when the appliance retrieves the categorization details of the request.

Display URL Categorization result through Command Interface

URL categorization enables you to enter a URL and retrieve categorization results (such as category, group, and reputation score) from the NetSTAR third-party URL categorization database.

When you enter a URL, the URL filtering feature retrieves and displays the categorization result on the command interface. When you enter further URLs, the appliance excludes older URLs from the list and displays the result for the latest three URLs.

To display URL category result up to three URLs, complete the following steps:

1. Add URL categorization URL
2. Display URL categorization details up to three URLs
3. Clear URL categorization data.

To add URL filtering categorization URL

To add a URL and retrieve its categorization details, do the following:

At the command prompt, type:

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

Example:

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

To display URL categorization details up to three URLs

At the command prompt, type:

```
> show urlfiltering categorization
```

Example:

```
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-->
```

Sample Configuration:

```
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-->
```

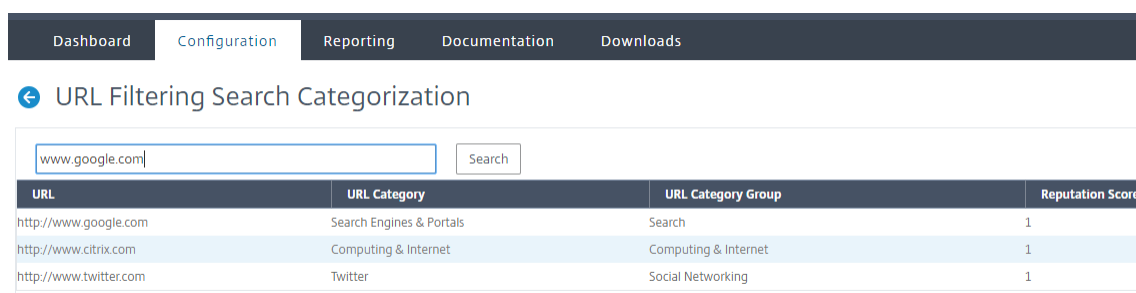
To clear URL categorization result

At the command prompt, type:

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

Display URL Categorization result through GUI Interface

1. In the navigation pane, expand **Secure Web Gateway > URL Filtering**.
2. In the details pane, click **URL Filtering Search Categorization** link from the **Tools** section.
3. In the **URL Filtering Search Categorization** page, enter a URL request and click **Search**.



URL	URL Category	URL Category Group	Reputation Score
http://www.google.com	Search Engines & Portals	Search	1
http://www.citrix.com	Computing & Internet	Computing & Internet	1
http://www.twitter.com	Twitter	Social Networking	1

4. The appliance displays the category result for the requested URL and for the previous two URL requests.

Security configuration

June 25, 2019

The Security Configuration feature enables you to configure the security policy for filtering URLs. The URL Reputation Score topic provides conceptual and configurational details for filtering URLs based on its reputation score.

You can use ICAP for remote content inspection.

URL reputation score

The URL Categorization feature uses the URL reputation score to provide policy-based control to block highly risky websites. For more information, see [URL reputation score](#).

Using ICAP for remote content inspection

HTTPS traffic is intercepted, decrypted, and sent to the ICAP servers for content inspection for anti-malware checks and data leak prevention.

URL reputation score

June 25, 2019

The URL Categorization feature provides policy-based control to restrict blacklisted URLs. You can control access to websites based on URL category, reputation score, or URL category and reputation

score. If a network administrator monitors a user accessing highly risky websites, he or she can use a responder policy bound to the URL reputation score to block such risky websites.

Upon receiving an incoming URL request, the appliance retrieves the category and reputation score from the URL categorization database. Based on the reputation score returned by the database, the appliance assigns a reputation rating for websites. The value can range from 1 to 4, where 4 is the riskiest type of websites, as shown in the following table.

URL Reputation Rating	Reputation Comment
1	Clean site
2	Unknown site
3	Potentially dangerous or affiliated to a dangerous site
4	Malicious site

Use Case: Filtering by URL reputation score

Consider an enterprise organization with a network administrator monitoring user transactions and network bandwidth consumption. If malware can enter the network, the administrator must enhance the data security and control access to malicious and dangerous websites accessing the network. To protect the network against such threats, the administrator can configure the URL filtering feature to allow or deny access by URL reputation score.

For more information about monitoring outbound traffic and user activities on the network, see [SWG Analytics](#).

If an employee of the organization tries to access a social networking website, the SWG appliance receives a URL request and queries the URL Categorization database to retrieve the URL category as social networking and a reputation score 3, which indicates a potentially dangerous website. The appliance then checks the security policy configured by the administrator, such as block access to sites with reputation rating of 3 or more. It then applies the policy action to control access to the website.

To implement this feature, you must configure the URL reputation score and security threshold levels by using the Citrix SWG Wizard.

Configuring reputation score by using the Citrix SWG GUI:

Citrix recommends that you use the Citrix SWG Wizard to configure the reputation score and security levels. Based on the configured threshold, you can select a policy action to allow, block or redirect traffic.

1. Log on to the **Citrix SWG** appliance and navigate to **Secure Web Gateway**.
2. In the details pane, click **Secured Web Gateway Wizard**.
3. In the **Secure Web Gateway Configuration** page, specify the SWG proxy server settings.
4. Click **Continue** to specify other settings such as SSL interception and identify management.
5. Click **Continue** to access the **Security Configuration** section.
6. In the **Security Configuration** section, select the **Reputation Score** checkbox to control access based on URL reputation score.
7. Select the security level and specify the reputation score threshold value:
 - a) Greater than or equals to—Allow or block a website if the threshold value is greater than or equal to N, where N ranges from one to four.
 - b) Less than or equals to—Allow or block a website if the threshold value is less than or equal to N, where N ranges from one to four.
 - c) In between—Allow or block a website if the threshold value is between N1 and N2 and the range is from one to four.
8. Select a responder action from the drop-down list.
9. Click **Continue** and Close.

The following image shows the Security Configuration section on the Citrix SWG Wizard. Enable the URL Reputation Score option to configure the policy settings.

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

Action*

Continue

Using ICAP for remote content inspection

June 25, 2020

Internet Content Adaptation Protocol (ICAP) is a simple, lightweight open protocol. It is typically used to transport HTTP messages between the proxy and the devices that provide antimalware support and data leak prevention services. ICAP has created a standard interface for content adaptation to allow greater flexibility in content distribution and for providing a value-added service. An ICAP client forwards HTTP requests and responses to an ICAP server for processing. The ICAP server performs some transformation on requests and sends back responses to the ICAP client, with appropriate action on the request or response.

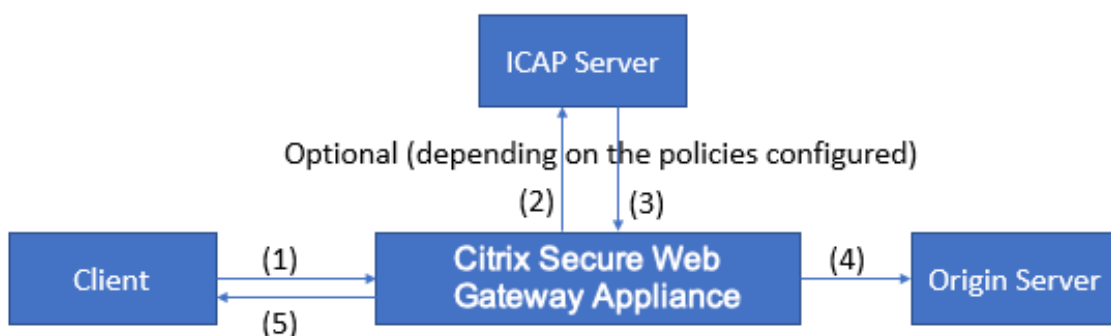
Using ICAP on the Citrix Secure Web Gateway appliance

Note

The content inspection feature requires an SWG Edition license.

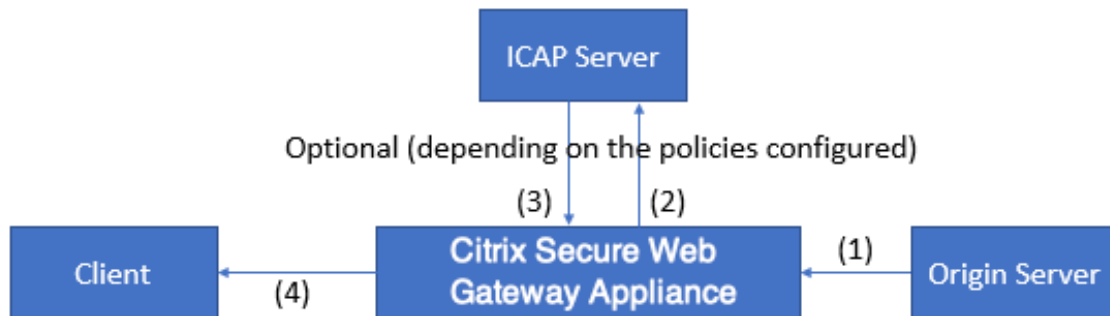
The Citrix Secure Web Gateway (SWG) appliance acts as an ICAP client and uses policies to interact with ICAP servers. The appliance communicates with third-party ICAP servers that specialize in functions such as antimalware and data leak prevention (DLP). When you use ICAP on an SWG appliance, encrypted files are also scanned. Security vendors earlier bypassed these files. The appliance performs SSL interception, decrypts the client traffic, and sends it to the ICAP server. The ICAP server checks for virus, malware or spyware detection, data leak inspection, or any other content adaptation services. The appliance acts as a proxy, decrypts the response from the origin server, and sends it in plain text to the ICAP server for inspection. Configure policies to select the traffic that is sent to the ICAP servers.

Request mode flow works as follows:



(1) The Citrix SWG appliance intercepts requests from the client. (2) The appliance forwards these requests to the ICAP server, based on the policies configured on the appliance. (3) The ICAP server responds with a message indicating “No adaptation required,” error, or modified request. The appliance either (4) forwards the content to the origin server that the client requested, or (5) returns an appropriate message to the client.

Response mode flow works as follows:



(1) The origin server responds to the Citrix SWG appliance. (2) The appliance forwards the response to the ICAP server, based on the policies configured on the appliance. (3) The ICAP server responds with a message indicating “No adaptation required,” or error, or modified request. (4) Depending on the response from the ICAP server, the appliance either forwards the content requested to the client, or sends an appropriate message.

Configuring ICAP on the Citrix Secure Web Gateway appliance

The following steps explain how to configure ICAP on the Citrix SWG appliance.

1. Enable the content inspection feature.
2. Configure a proxy server.
3. Configure a TCP service that represents the ICAP server. To establish a secure connection between the SWG appliance and ICAP service, specify the service type as `SSL_TCP`. For more information about secure ICAP, see the “Secure ICAP” section later in this page.
4. Optionally, add a load balancing virtual server to load balance the ICAP servers and bind the ICAP service to this virtual server.
5. Configure a custom ICAP profile. The profile must include the URI or the service path for the ICAP service, and the ICAP mode (request or response.) There are no ICAP default profiles similar to the HTTP and TCP default profiles.
6. Configure a content inspection action and specify the ICAP profile name. Specify the load balancing virtual server name or the TCP/SSL_TCP service name in the server name parameter.
7. Configure a content inspection policy to evaluate client traffic and bind it to the proxy server. Specify the content inspection action in this policy.

Configure ICAP by using the CLI

Configure the following entities:

1. Enable the feature.

```
enable ns feature contentInspection
```

2. Configure a proxy server.

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

Example:

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

3. Configure a TCP service to represent the ICAP servers.

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

Specify the service type as SSL_TCP for a secure connection with the ICAP server.

Example:

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

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

4. Configure a load balancing virtual server.

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

Example:

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

Bind the ICAP service to the load balancing virtual server.

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

Example:

```
bind lb vserver lbicap icap_svc
```

5. Add a custom ICAP profile.

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

Example:

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

Parameters**name**

Name for an ICAP profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters.

CLI users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my icap profile" or 'my icap profile'.)

Maximum Length: 127

uri

URI representing the ICAP service path.

Maximum Length: 511 characters

Mode

ICAP mode. Available settings function as follows:

- REQMOD: In request modification mode, the ICAP client forwards an HTTP request to the ICAP server.
- RESPMOD: In response modification mode, the ICAP server forwards an HTTP response from the origin server to the ICAP server.

Possible values: REQMOD, RESPMOD

6. Configure an action to perform if the policy returns true.

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

Example:

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

7. Configure a policy to evaluate traffic.

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

Example:

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

8. Bind the policy to the proxy server.

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

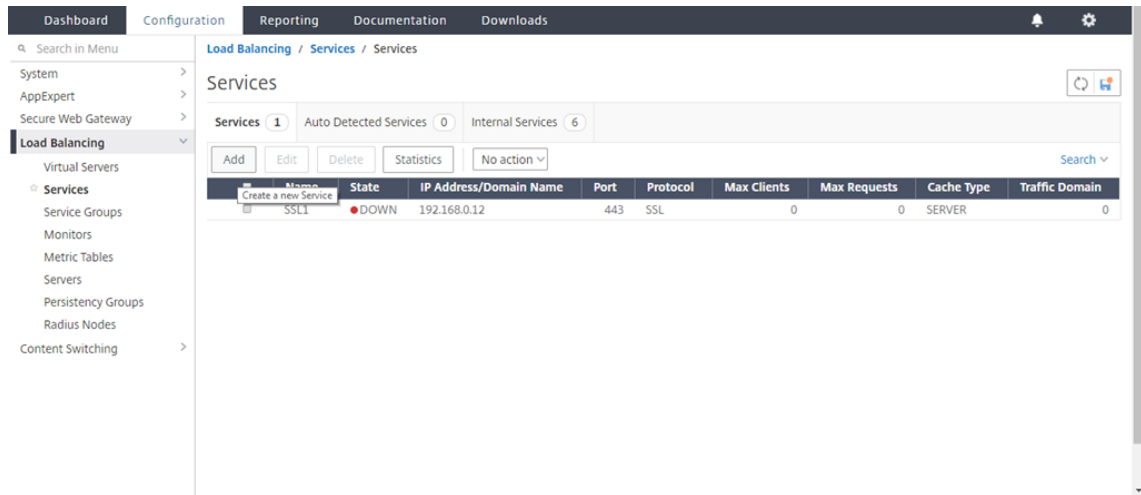
Example:

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

Configure ICAP by using the GUI

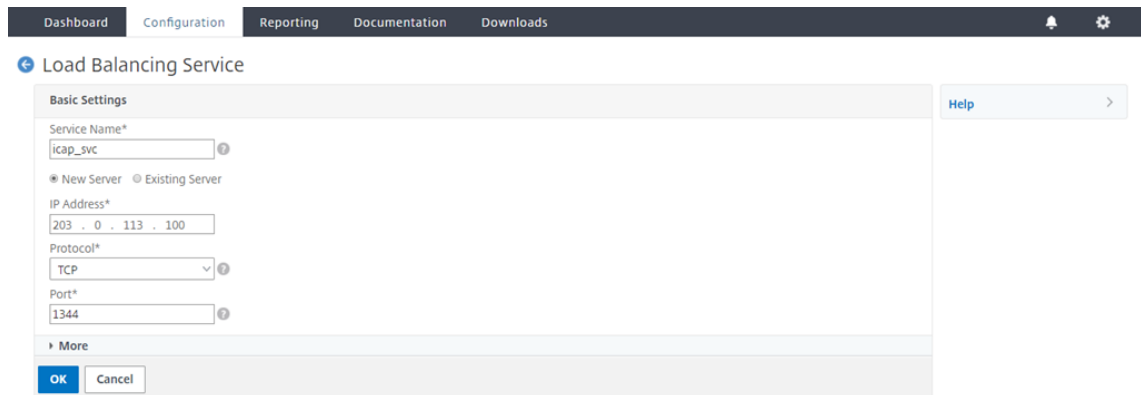
Perform the following steps:

1. Navigate to **Load Balancing > Services** and click **Add**.

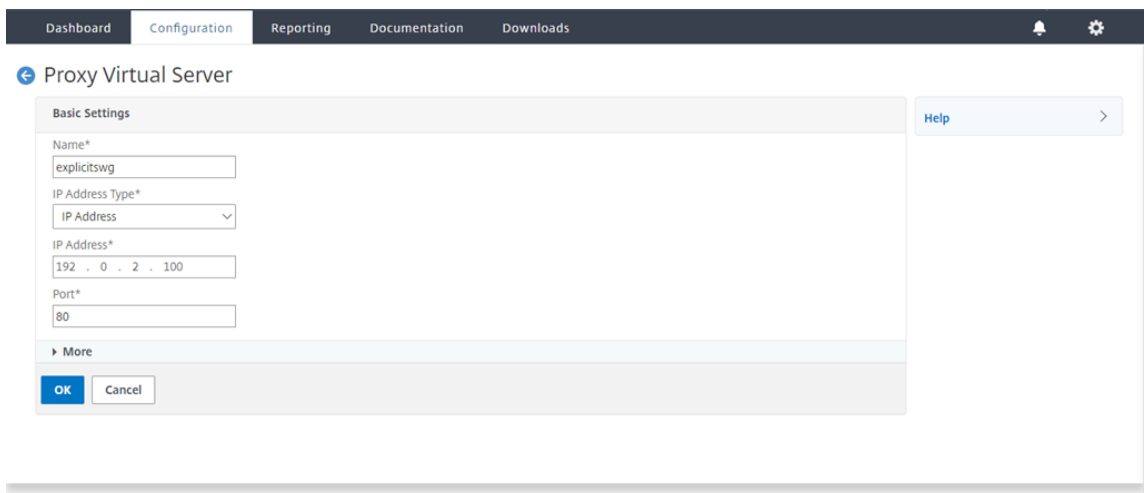


2. Type a name and IP address. In **Protocol**, select **TCP**. In **Port**, type **1344**. Click **OK**.

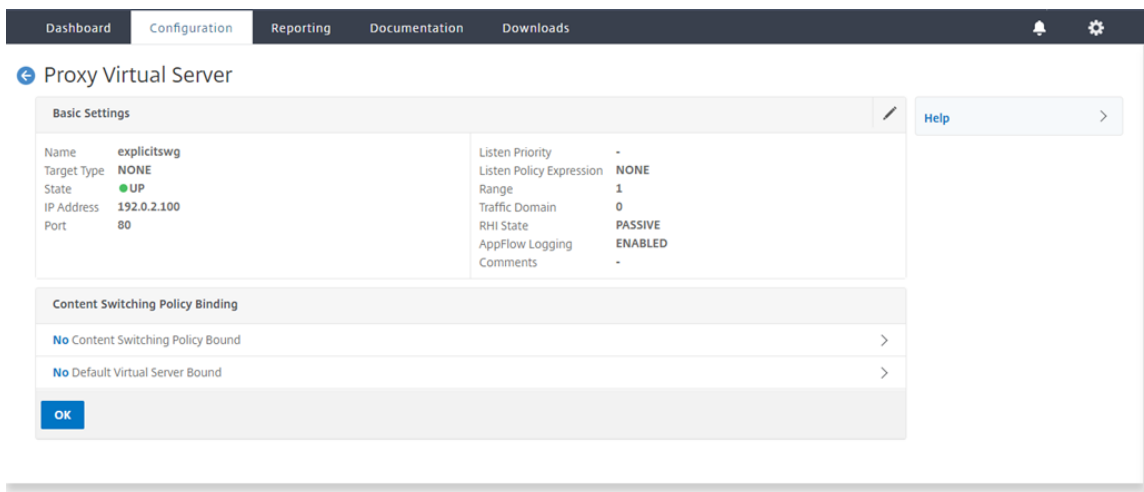
For a secure connection to the ICAP servers, select TCP_SSL protocol and specify the port as 11344.



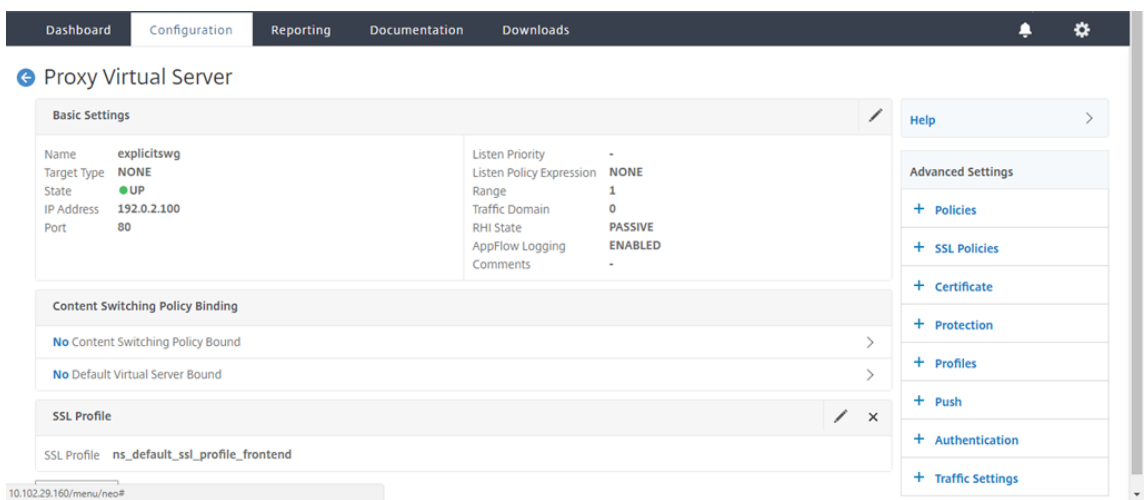
3. Navigate to **Secure Web Gateway > Proxy Virtual Servers**. Add a proxy virtual server or select a virtual server and click **Edit**. After entering details, click **OK**.



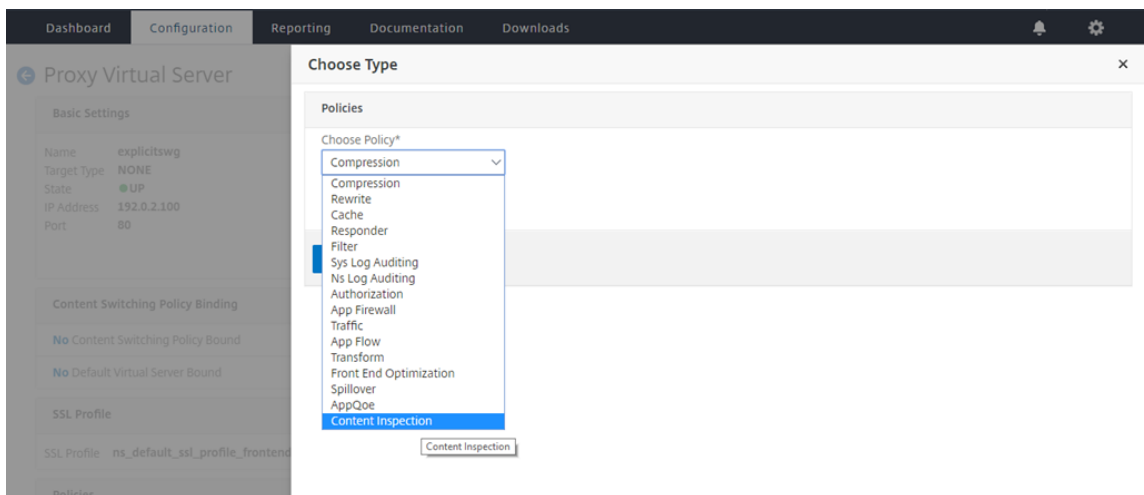
Click **OK** again.



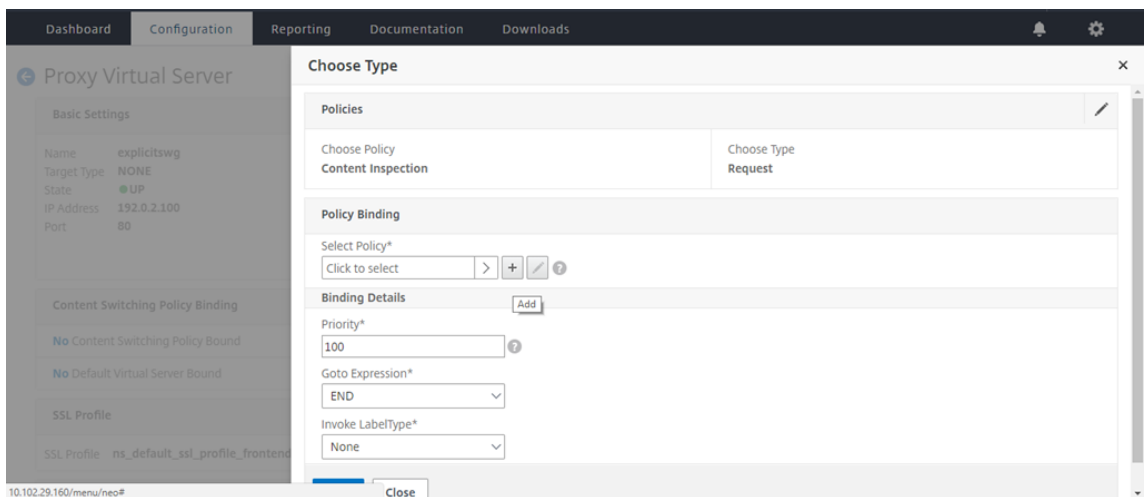
4. In **Advanced Settings**, click **Policies**.



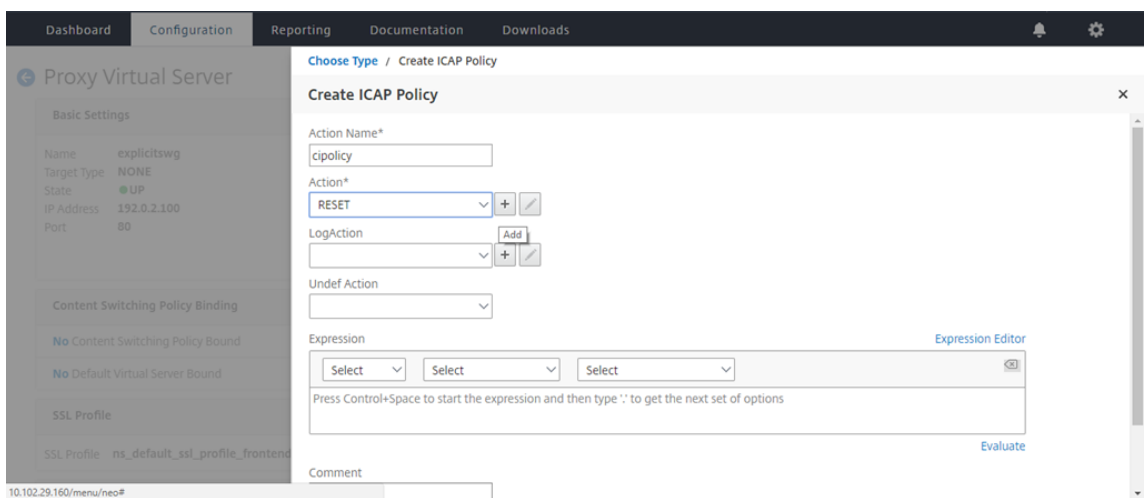
5. In **Choose Policy**, select **Content Inspection**. Click **Continue**.



6. In **Select Policy**, click the “+” sign to add a policy.

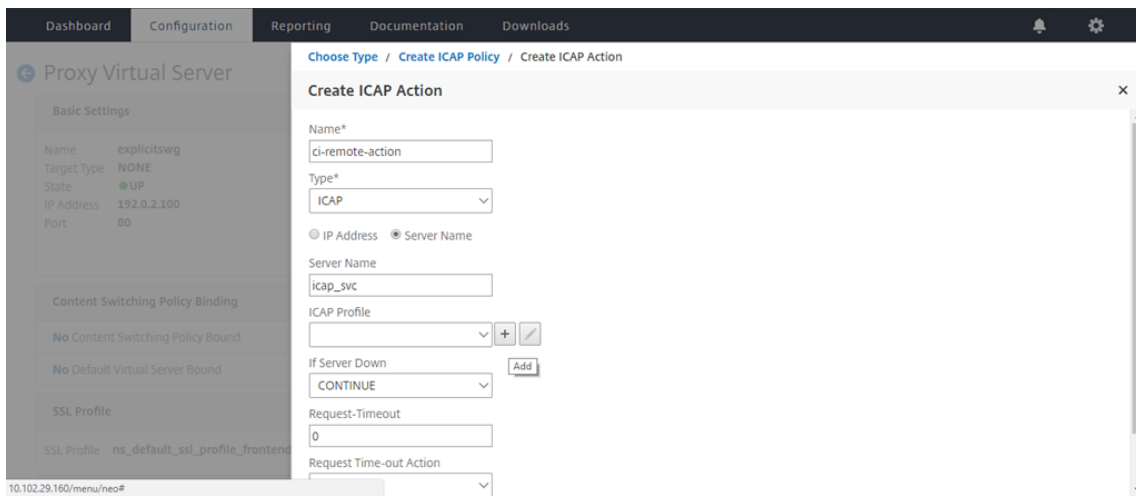


7. Enter a name for the policy. In **Action**, click the “+” sign to add an action.

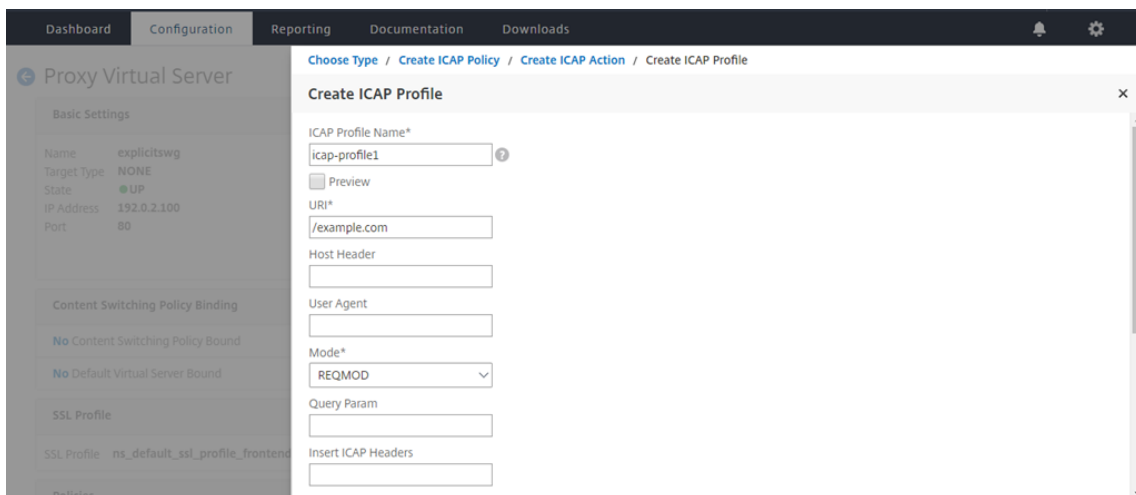


8. Type a name for the action. In **Server Name**, type the name of the TCP service created earlier.

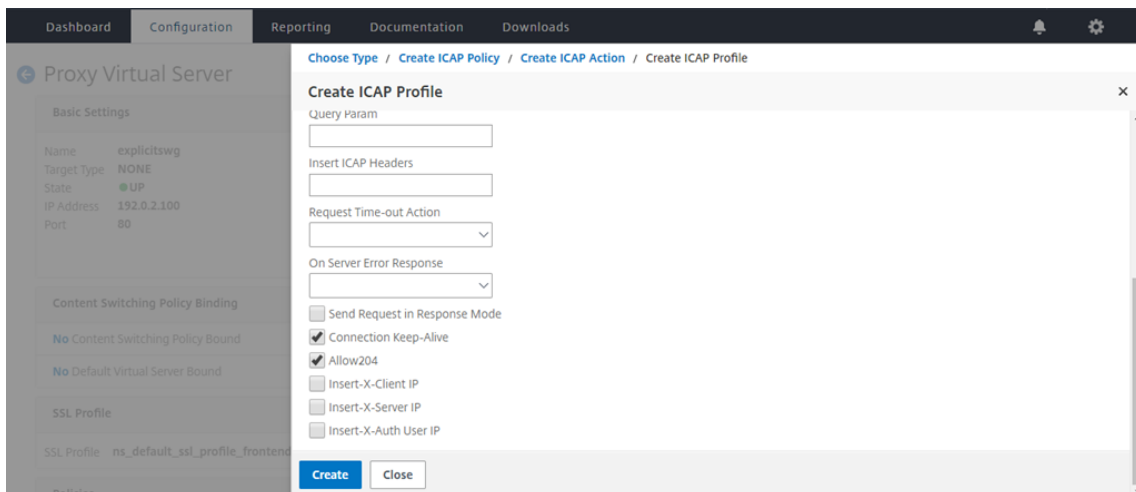
In **ICAP Profile**, click the “+” sign to add an ICAP profile.



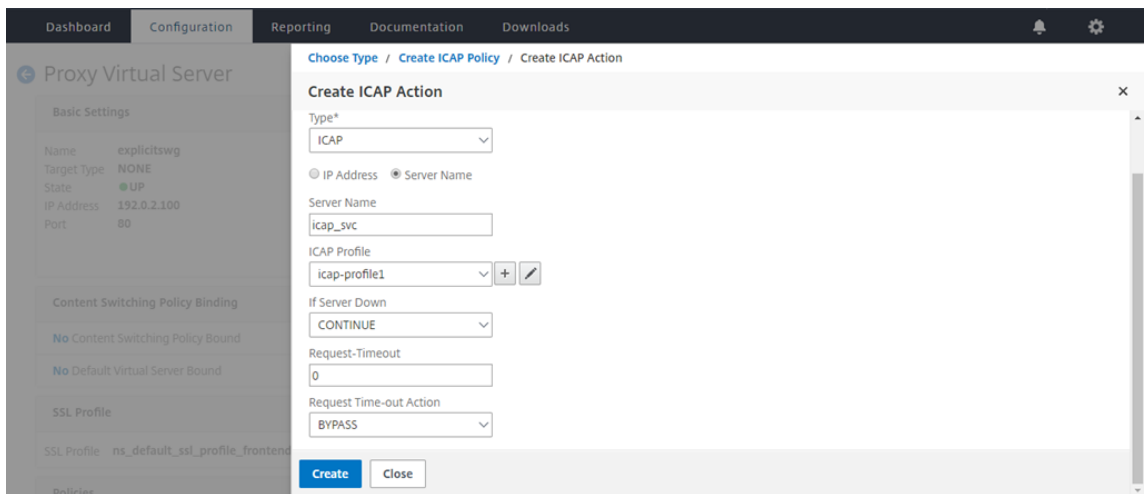
9. Type a profile name, URI. In **Mode**, select **REQMOD**.



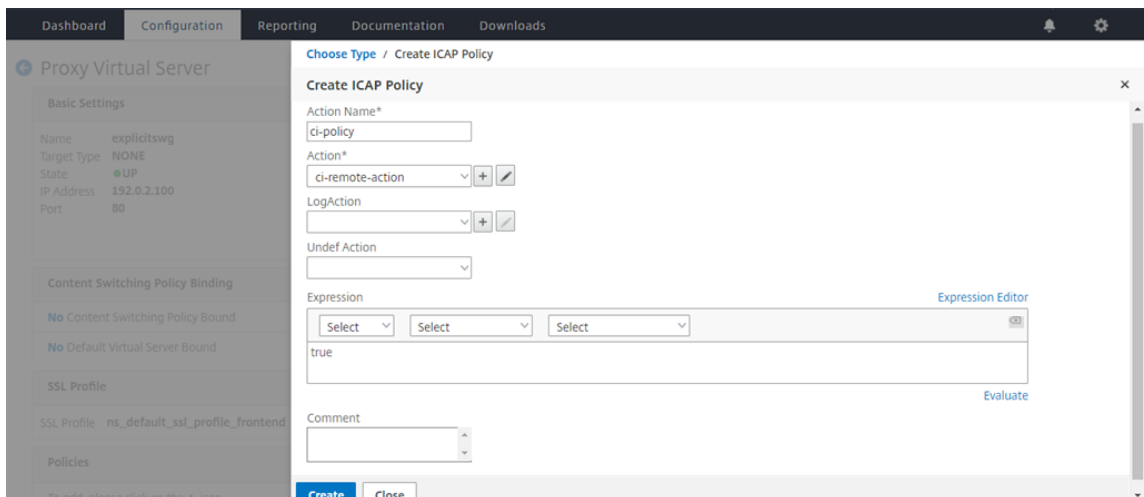
10. Click **Create**.



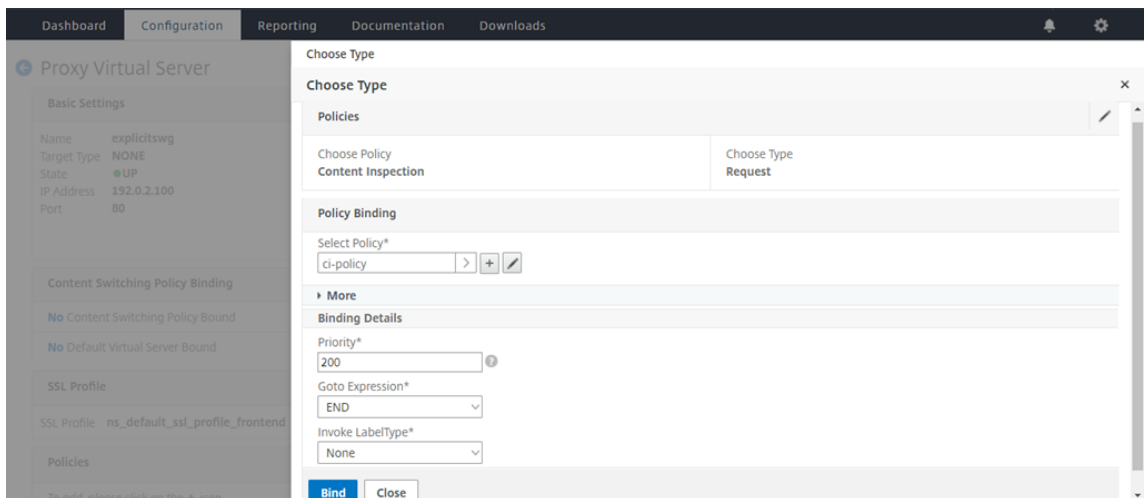
11. In the **Create ICAP Action** page, click **Create**.



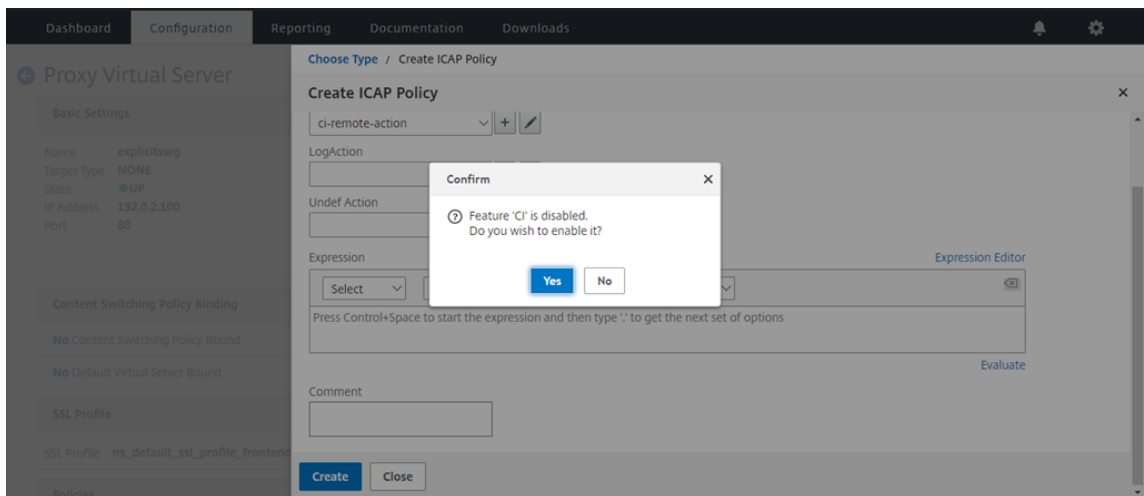
12. In the **Create ICAP Policy** page, enter true in the **Expression Editor**. Then, click **Create**.



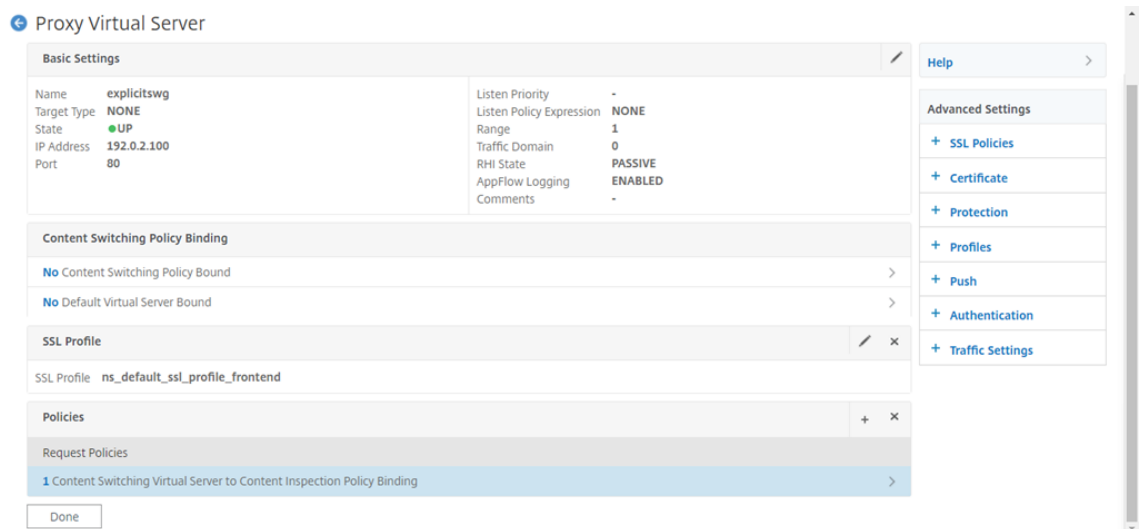
13. Click **Bind**.



14. When prompted to enable the content inspection feature, select **Yes**.



15. Click **Done**.



Secure ICAP

You can establish a secure connection between the SWG appliance and the ICAP servers. To do this, create an SSL_TCP service instead of a TCP service. Configure a load balancing virtual server of type SSL_TCP. Bind the ICAP service to the load balancing virtual server.

Configure secure ICAP by using the CLI

At the command prompt, type:

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

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

Example:

```
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-->
```

Configure secure ICAP by using the GUI

1. Navigate to **Load Balancing > Virtual Servers**, and click **Add**.
2. Specify a name for the virtual server, IP address and port. Specify protocol as SSL_TCP.
3. Click **OK**.
4. Click inside the **Load Balancing virtual Server Service Binding** section to add an ICAP service.
5. Click “+” to add a service.
6. Specify a service name, IP address, protocol (SSL_TCP), and port (default port for secure ICAP is 11344).
7. Click **OK**.
8. Click **Done**.
9. Click **Bind**.
10. Click **Continue** twice.
11. Click **Done**.

Limitations

The following features are not supported:

- ICAP response caching.
- Inserting X-Auth-User-URI header.
- Inserting the HTTP request in the ICAP request in RESPMOD.

Integration with IPS or NGFW as inline devices

June 25, 2020

Security devices such as Intrusion Prevention System (IPS) and Next Generation Firewall (NGFW) protect servers from network attacks. These devices can inspect live traffic and are typically deployed in

layer 2 inline mode. Citrix Secure Web Gateway (SWG) provides security of users and the enterprise network when accessing resources on the internet.

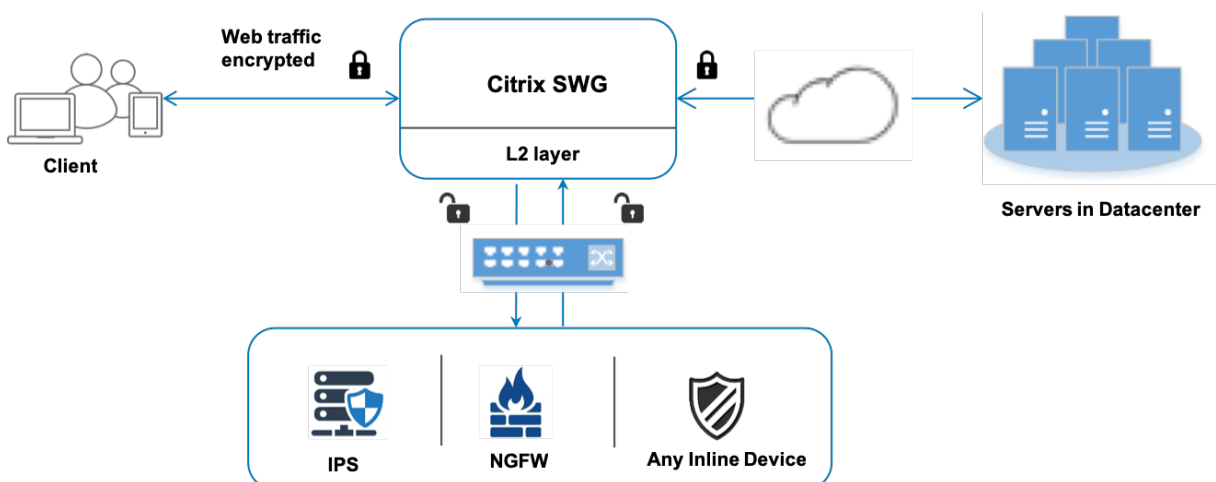
A Citrix SWG appliance can be integrated with one or more inline devices to prevent threats and provide advanced security protection. The inline devices can be any security device, such as IPS and NGFW.

Some use cases where you can benefit by using the Citrix SWG appliance and inline device integration are:

- **Inspecting encrypted traffic:** Most IPS and NGFW appliances bypass encrypted traffic, which can leave servers vulnerable to attacks. A Citrix SWG appliance can decrypt traffic and send it to the inline devices for inspection. This integration enhances the customer's network security.
- **Offloading inline devices from TLS/SSL processing:** TLS/SSL processing is expensive, which can result in high CPU utilization in IPS or NGFW appliances if they also decrypt the traffic. A Citrix SWG appliance helps in offloading TLS/SSL processing from inline devices. As a result, inline devices can inspect a higher volume of traffic.
- **Loading balancing inline devices:** If you have configured multiple inline devices to manage heavy traffic, a Citrix SWG appliance can load balance and distribute traffic evenly to these devices.
- **Smart selection of traffic:** Instead of sending all the traffic to the inline device for inspection, the appliance does a smart selection of traffic. For example, it skips sending text files for inspection to the inline devices.

Citrix SWG integration with inline devices

The following diagram shows how a Citrix SWG is integrated with inline security devices.



When you integrate inline devices with Citrix SWG appliance, the components interact as follows:

1. A client sends a request to a Citrix SWG appliance.
2. The appliance sends the data to the inline device for content inspection based on the policy evaluation. For HTTPS traffic, the appliance decrypts the data and sends it in plain text to the inline device for content inspection.

Note:

If there are two or more inline devices, the appliance load balances the devices and sends the traffic.

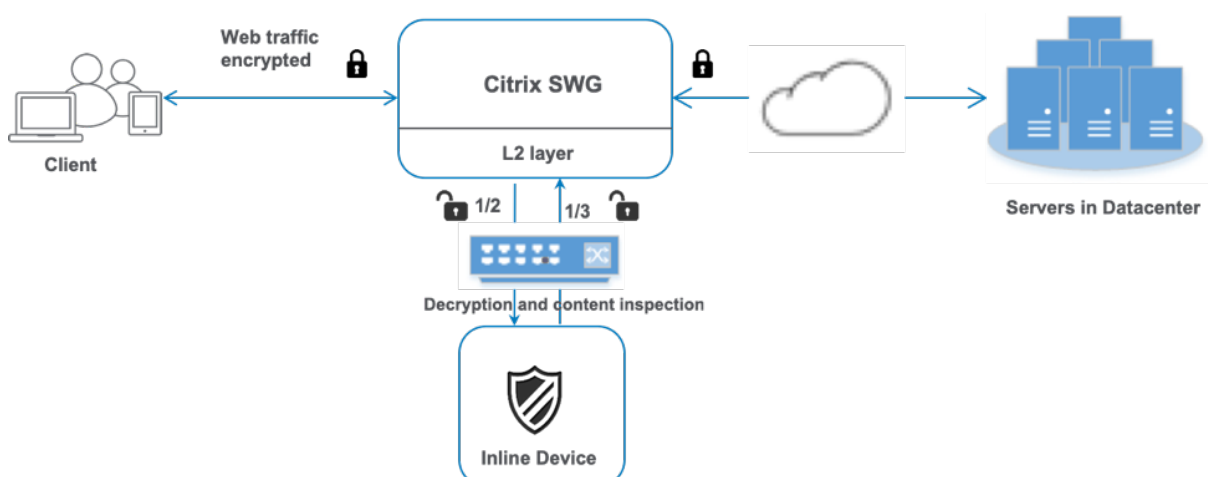
3. The inline device inspects the data for threats and decides whether to drop, reset, or send the data back to the appliance.
4. If there are security threats, the device modifies the data and sends it to the appliance.
5. For HTTPS traffic, the appliance re-encrypts the data and forwards the request to the backend server.
6. The backend server sends the response to the appliance.
7. The appliance again decrypts the data and sends it to the inline device for inspection.
8. The inline device inspects the data. If there are security threats, the device modifies the data and sends it to the appliance.
9. The appliance re-encrypts the data and sends the response to the client.

Configuring inline device integration

You can configure a Citrix SWG appliance with an inline device in three different ways as follows:

Scenario 1: Using a single inline device

To integrate a security device (IPS or NGFW) in inline mode, you must enable content inspection and MAC-based forwarding (MBF) in global mode on the SWG appliance. Then, add a content inspection profile, a TCP service, a content inspection action for inline devices to reset, block, or drop the traffic based on inspection. Also add a content inspection policy that the appliance uses to decide the subset of traffic to send to the inline devices. Finally, configure the proxy virtual server with layer 2 connection enabled on the server and bind the content inspection policy to this proxy virtual server.



Perform the following steps:

1. Enable MAC-based forwarding (MPF) mode.
2. Enable the content inspection feature.
3. Add a content inspection profile for the service. The content inspection profile contains the inline device settings that integrate the SWG appliance with an inline device.
4. (Optional) Add a TCP monitor.

Note:

Transparent devices do not have an IP address. Therefore, to perform health checks, you must explicitly bind a monitor.

5. Add a service. A service represents an inline device.
6. (Optional) Bind the service to the TCP monitor.
7. Add a content inspection action for the service.
8. Add a content inspection policy and specify the action.
9. Add an HTTP or HTTPS proxy (content switching) virtual server.
10. Bind the content inspection policy to the virtual server.

Configuration using the CLI Type the following commands at the command prompt. Examples are given after most commands.

1. Enable MBF.

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

2. Enable the feature.

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

3. Add a content inspection profile.

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

Example:

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

4. Add a service. Specify a dummy IP address that is not owned by any of the devices, including the inline devices. Set `use source IP address` (USIP) to YES. Set `useproxyport` to NO. Turn off the health monitor. Turn on health monitoring only if you bind this service to a TCP monitor. If you bind a monitor to a service, then set the TRANSPARENT option in the monitor to ON.

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

Example:

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

5. Add a content inspection action.

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

Example:

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

6. Add a content inspection policy.
-

```

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

```

Example:

```

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

```

7. Add a proxy virtual server.

```

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

```

Example:

```

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

```

8. Bind the policy to the virtual server.

```

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

```

Example:

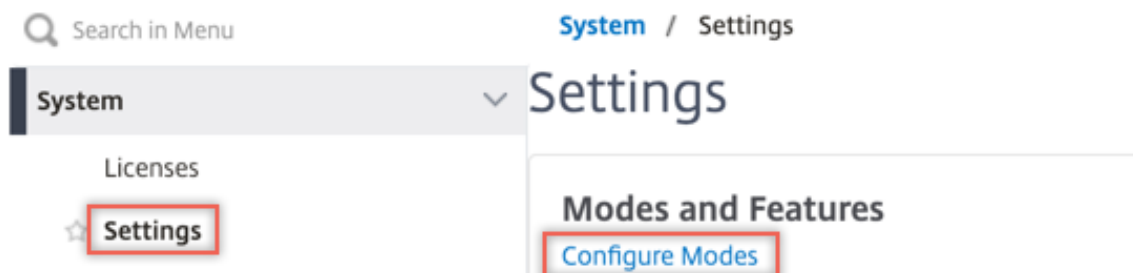
```

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

```

Configuration using the GUI

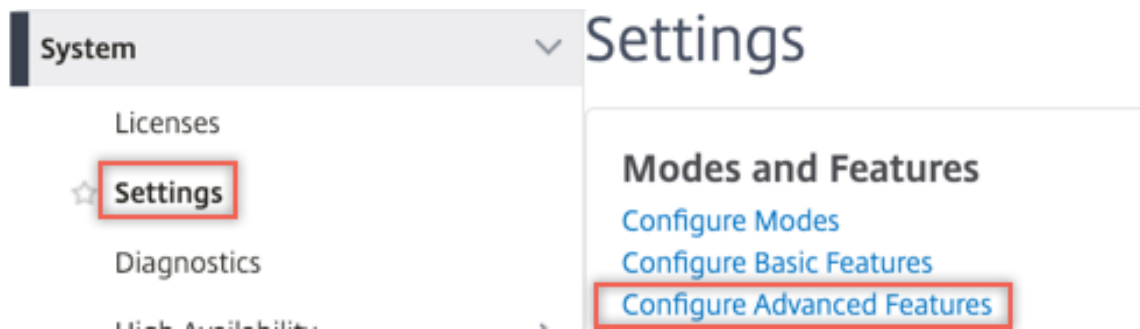
1. Navigate to **System > Settings**. In **Modes and Features**, click **Configure Modes**.



← 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. Navigate to **System > Settings**. In **Modes and Features**, click **Configure Advanced Features**.

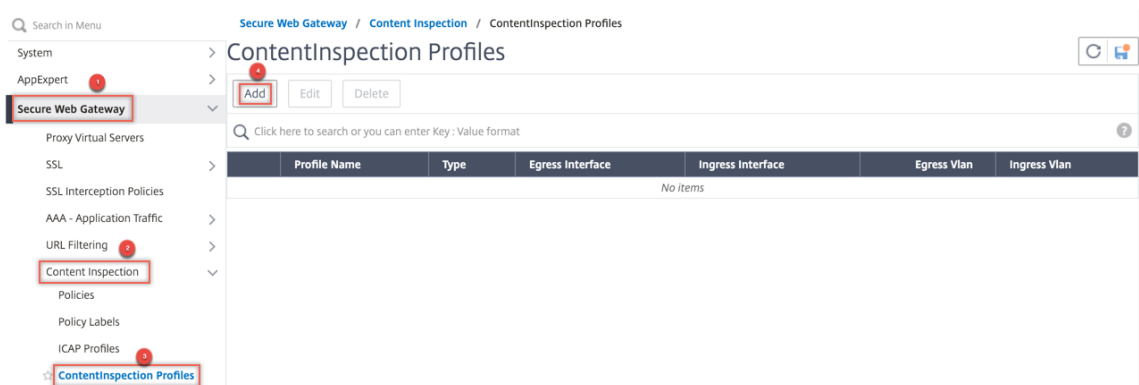


← Configure Advanced Features

<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. Navigate to **Secure Web Gateway > Content Inspection > Content Inspection Profiles**. Click **Add**.



4. Navigate to **Load Balancing > Services > Add** and add a service. In **Advanced Settings**, click **Profiles**. In the **CI Profile Name** list, select the content inspection profile created earlier. In **Service Settings**, set **Use Source IP Address** to YES and **Use Proxy Port** to No. In **Basic Settings**, set **Health Monitoring** to NO. Turn on health monitoring only if you bind this service to a TCP monitor. If you bind a monitor to a service, then set the TRANSPARENT option in monitor

to ON.

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	DISABLED
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		

- Navigate to **Secure Web Gateway > Proxy Virtual Servers > Add**. Specify a name, IP address, and port. In **Advanced Settings**, select **Policies**. Click the “+” sign.

← Proxy Virtual Server

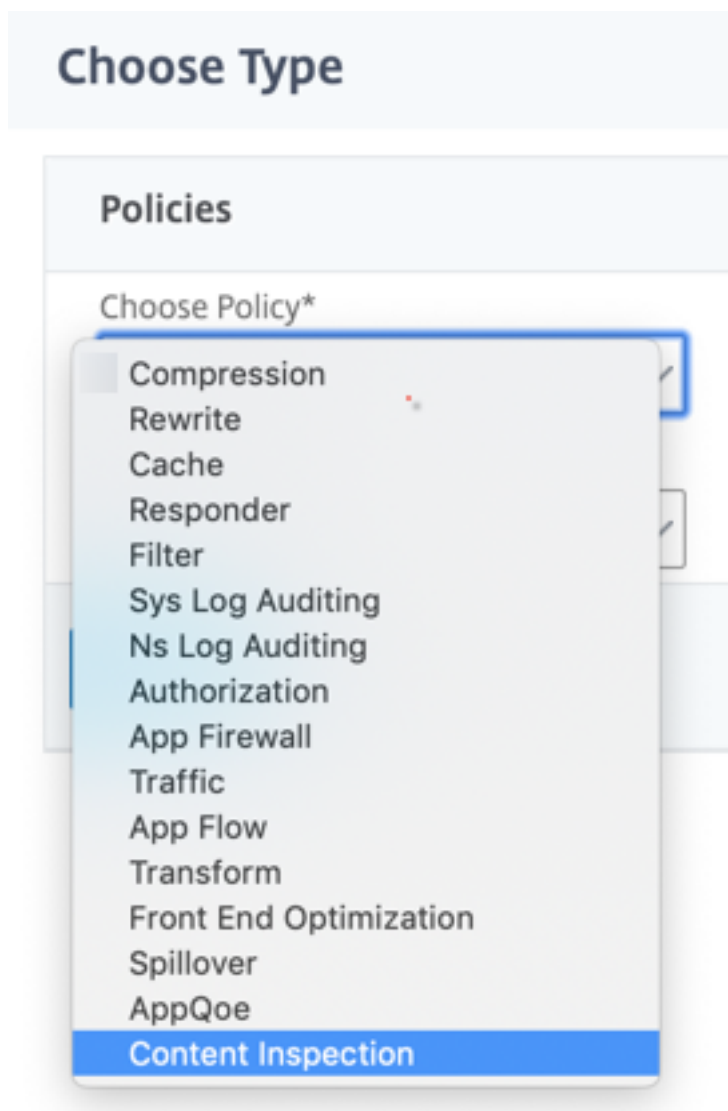
Basic Settings	
Name	proxyvsr
State	● UP
IP Address	198.51.200.2
Port	80
Listen Priority	-
Listen Policy Expression	NONE
Range	1
IPset	-
Traffic Domain	0
RHI State	PASSIVE
AppFlow Logging	ENABLED
Comments	-

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

Certificate	
No Server Certificate	>
No CA Certificate	>

Policies	
	+ x

6. In **Choose Policy** select **Content Inspection**. Click **Continue**.



7. Click **Add**. Specify a name. In **Action**, click **Add**.

[Choose Type](#) / Create ContentInspection Policy

Create ContentInspection Policy

Policy Name*

Action*

Log Action

UNDEF Action

- Specify a name. In **Type**, select **INLINEINSPECTION**. In **Server Name**, select the TCP service created earlier.

← Create ContentInspection Action

Name*

Type*

Server Name*

If Server Down

Request-Timeout

Request timeout action

9. Click **Create**. Specify the rule and click **Create**.

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](#)

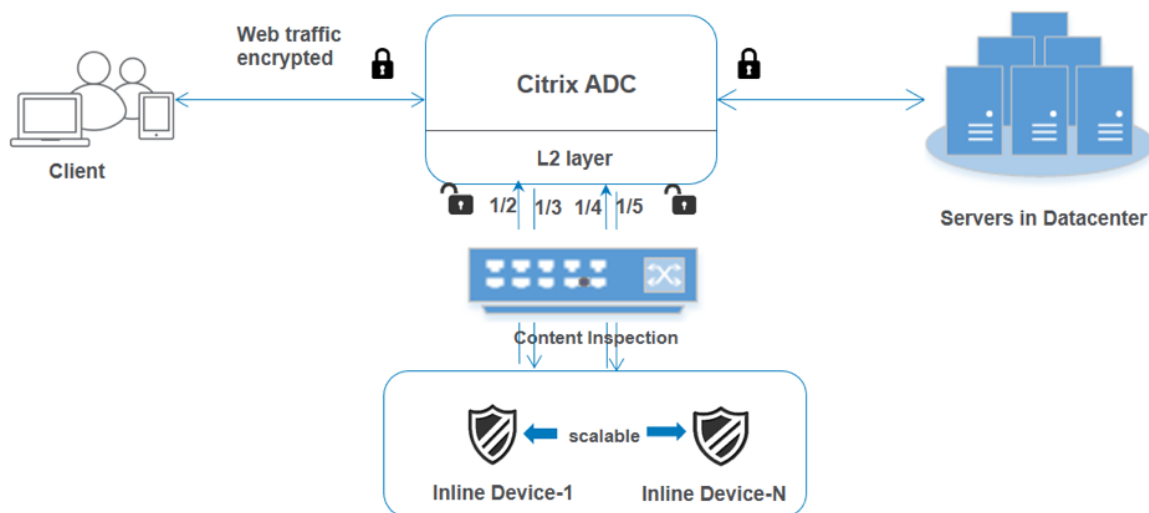
Comment

OK Close

10. Click **Bind**.
11. Click **Done**.

Scenario 2: Load balance multiple inline devices with dedicated interfaces

If you are using two or more inline devices, you can load balance the devices using different content inspection services with dedicated interfaces. In this case, the Citrix SWG appliance load balances the subset of traffic sent to each device through a dedicated interface. The subset is decided based on the policies configured. For example, TXT or image files might not be sent for inspection to the inline devices.



The basic configuration remains the same as in scenario 1. However, you must create a content inspection profile for each inline device and specify the ingress and egress interface in each profile. Add a service for each inline device. Add a load balancing virtual server and specify it in the content inspection action. Perform the following extra steps:

1. Add content inspection profiles for each service.
2. Add a service for each device.
3. Add a load balancing virtual server.
4. Specify the load balancing virtual server in the content inspection action.

Configuration using the CLI Type the following commands at the command prompt. Examples are given after each command.

1. Enable MBF.

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

2. Enable the feature.

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

3. Add profile 1 for service 1.

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

Example:

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

4. Add profile 2 for service 2.

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

Example:

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

5. Add service 1. Specify a dummy IP address that is not owned by any of the devices, including the inline devices. Set `use source IP address (USIP)` to YES. Set `useproxyport` to NO. Turn off the health monitor. Turn on health monitoring only if you bind this service to a TCP monitor. If you bind a monitor to a service, then set the TRANSPARENT option in the monitor to ON.

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

Example:

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

6. Add service 2. Specify a dummy IP address that is not owned by any of the devices, including the inline devices. Set `use source IP address (USIP)` to YES. Set `useproxyport` to NO. Turn off the health monitor. Turn on health monitoring only if you bind this service to a TCP monitor. If you bind a monitor to a service, then set the TRANSPARENT option in the monitor to ON.

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

Example:

```

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

```

7. Add a load balancing virtual server.

```

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

```

Example:

```

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

```

8. Bind the services to the load balancing virtual server.

```

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

```

Example:

```

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

```

9. Specify the load balancing virtual server in the content inspection action.

```

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

```

Example:

```

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

```

10. Add a content inspection policy. Specify the content inspection action in the policy.

```

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

```

Example:

```

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

```

11. Add a proxy virtual server.

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

Example:

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

12. Bind the content inspection policy to the virtual server.

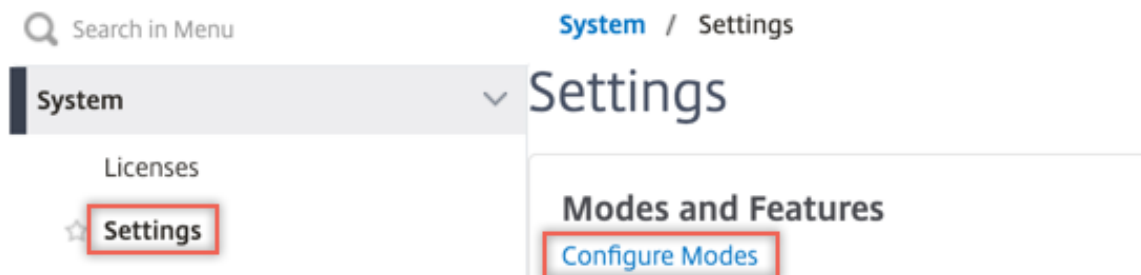
```
1 bind cs vserver <name> -policyName <string> -priority <
  positive_integer> -gotoPriorityExpression <expression> -type
  REQUEST
2 <!--NeedCopy-->
```

Example:

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

Configuration using the GUI

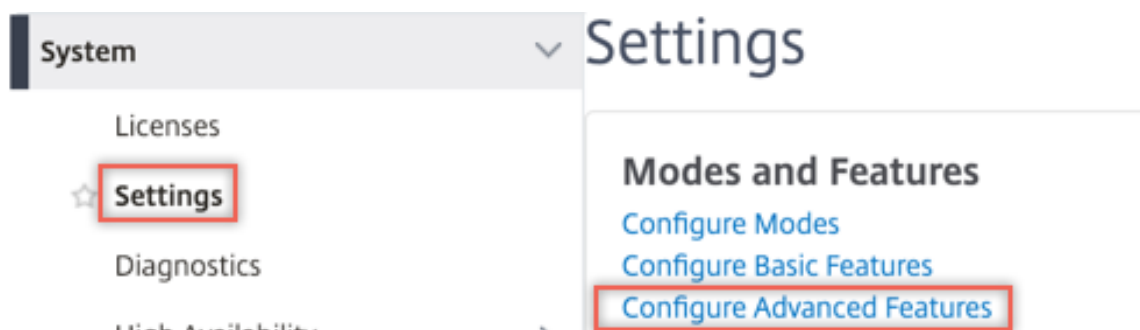
1. Navigate to **System > Settings**. In **Modes and Features**, click **Configure Modes**.



← 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	

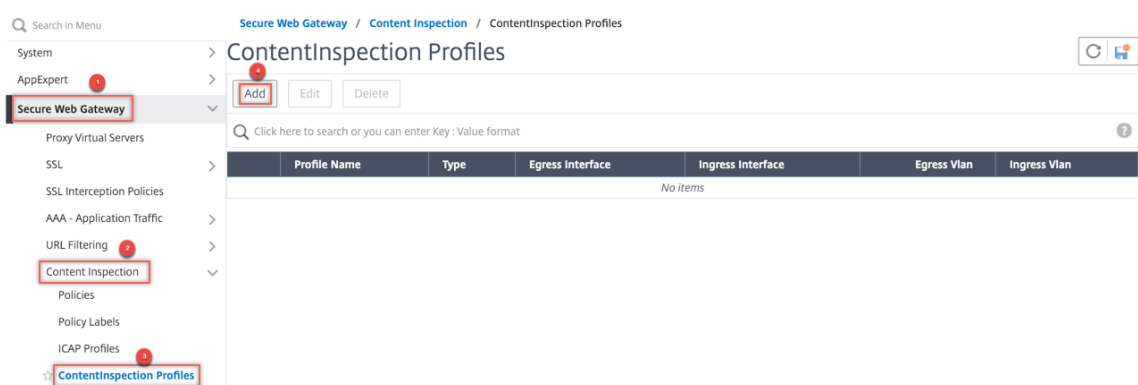
2. Navigate to **System > Settings**. In **Modes and Features**, click **Configure Advanced Features**.



← 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	

3. Navigate to **Secure Web Gateway > Content Inspection > Content Inspection Profiles**. Click **Add**.



Specify the ingress and egress interfaces.

Create ContentInspectionProfile

Profile Name*

Type*

Egress Interface*

Ingress Interface*

Egress Vlan

Ingress Vlan

Create two profiles. Specify a different ingress and egress interface in the second profile.

4. Navigate to **Load Balancing > Services > Add** and add a service. In **Advanced Settings**, click **Profiles**. In the **CI Profile Name** list, select the content inspection profile created earlier. In **Service Settings**, set **Use Source IP Address** to YES and **Use Proxy Port** to No. In **Basic Settings**, set **Health Monitoring** to NO. Turn on health monitoring only if you bind this service to a TCP monitor. If you bind a monitor to a service, then set the TRANSPARENT option in monitor to ON.

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		

Create two services. Specify dummy IP addresses that are not owned by any of the devices, including the inline devices.

- Navigate to **Load Balancing > Virtual Servers > Add**. Create a TCP load balancing virtual server.

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

Click **OK**.

6. Click inside the **Load Balancing Virtual Server Service Binding** section. In **Service Binding**, click the arrow in **Select Service**. Select the two services created earlier, and click **Select**. Click **Bind**.

Service Binding

Select Service*

Binding Details

Weight

Service Binding / Service

Service

Select Add Edi

🔍 Click here to search or you can en

<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*

>

Add
Edit
?

Binding Details

Weight

1

Bind
Close

- Navigate to **Secure Web Gateway > Proxy Virtual Servers > Add**. Specify a name, IP address, and port. In **Advanced Settings**, select **Policies**. Click the “+” sign.

← Proxy Virtual Server

Basic Settings

Name proxyvsrv 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

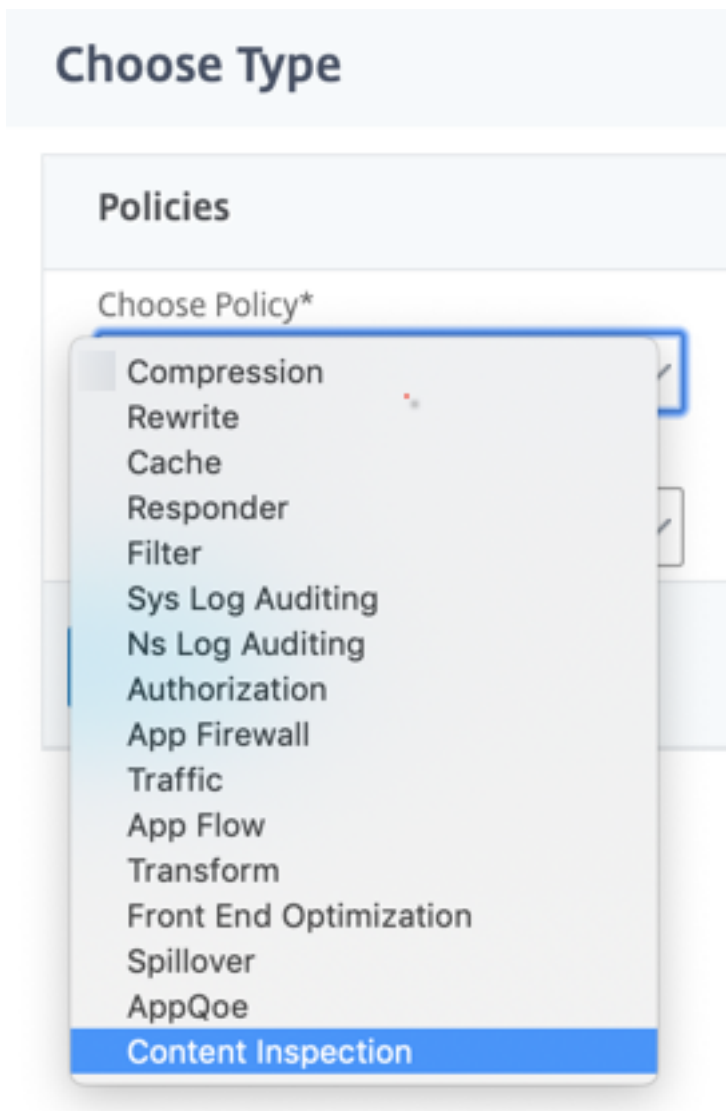
No Server Certificate >

No CA Certificate >

Policies

+
×

- In **Choose Policy** select **Content Inspection**. Click **Continue**.



9. Click **Add**. Specify a name. In **Action**, click **Add**.

[Choose Type](#) / Create ContentInspection Policy

Create ContentInspection Policy

Policy Name*

Action*

Log Action

UNDEF Action

10. Specify a name. In **Type**, select **INLINEINSPECTION**. In **Server Name**, select the load balancing virtual server created earlier.

← Create ContentInspection Action

Name*

Type*

Server Name*

If Server Down

Request-Timeout

Request timeout action

11. Click **Create**. Specify the rule and click **Create**.

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

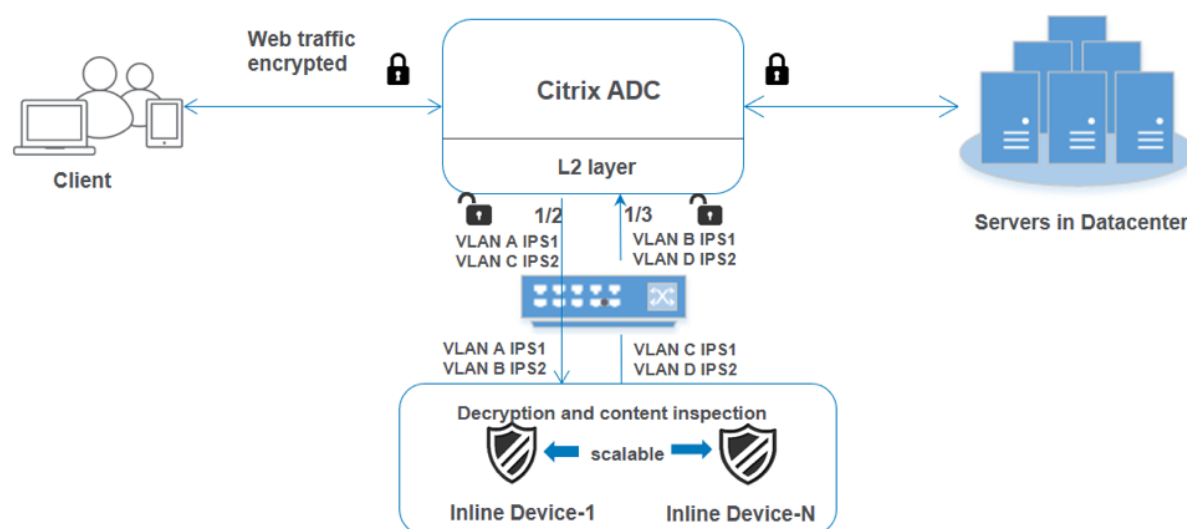
OK Close

12. Click **Bind**.

13. Click **Done**.

Scenario 3: Load balance multiple inline devices with shared interfaces

If you are using two or more inline devices, you can load balance the devices using different content inspection services with shared interfaces. In this case, the Citrix SWG appliance load balances the subset of traffic sent to each device through a shared interface. The subset is decided based on the policies configured. For example, TXT or image files might not be sent for inspection to the inline devices.



The basic configuration remains the same as in scenario 2. For this scenario, bind the interfaces to different VLANs to segregate the traffic for each inline device. Specify the VLANs in the content inspection profiles. Perform the following extra steps:

1. Bind the shared interfaces to different VLANs.
2. Specify the ingress and egress VLANs in the content inspection profiles.

Configuration using the CLI Type the following commands at the command prompt. Examples are given after each command.

1. Enable MBF.

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

2. Enable the feature.

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

3. Bind the shared interfaces to different VLANs.

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

Example:

```
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. Add profile 1 for service 1. Specify the ingress and egress VLANs in the profile.

```

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

```

Example:

```

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

```

5. Add profile 2 for service 2. Specify the ingress and egress VLANs in the profile.

```

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

```

Example:

```

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

```

6. Add service 1.

```

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

```

Example:

```

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

```

7. Add service 2.

```

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

```

Example:

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

8. Add a load balancing virtual server.

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

Example:

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

9. Bind the services to the load balancing virtual server.

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

Example:

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

10. Specify the load balancing virtual server in the content inspection action.

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

Example:

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

11. Add a content inspection policy. Specify the content inspection action in the policy.

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

Example:

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

12. Add a proxy virtual server.

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

Example:

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

13. Bind the content inspection policy to the virtual server.

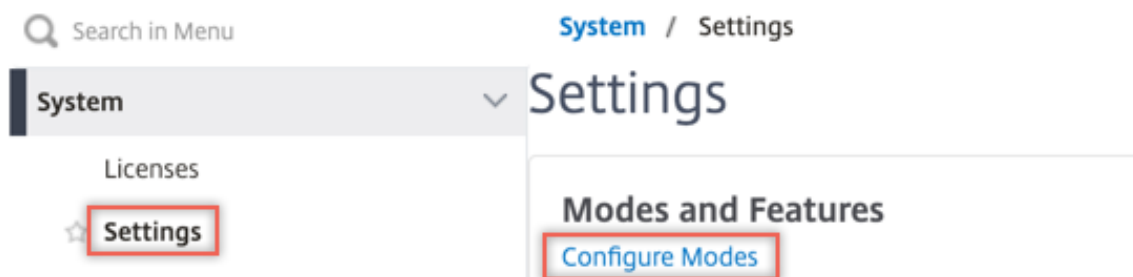
```
1 bind cs vserver <name> -policyName <string> -priority <
  positive_integer> -gotoPriorityExpression <expression> -type
  REQUEST
2 <!--NeedCopy-->
```

Example:

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

Configuration using the GUI

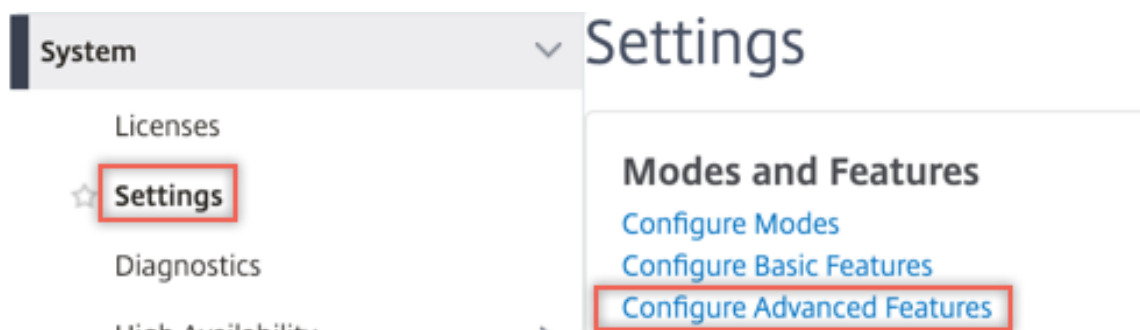
1. Navigate to **System > Settings**. In **Modes and Features**, click **Configure Modes**.



← 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. Navigate to **System > Settings**. In **Modes and Features**, click **Configure Advanced Features**.



← 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. Navigate to **System > Network > VLANs > Add**. Add four VLANs and tag them to the interfaces.

← 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*



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*

 ?

Alias Name

Maximum Transmission Unit

Dynamic Routing

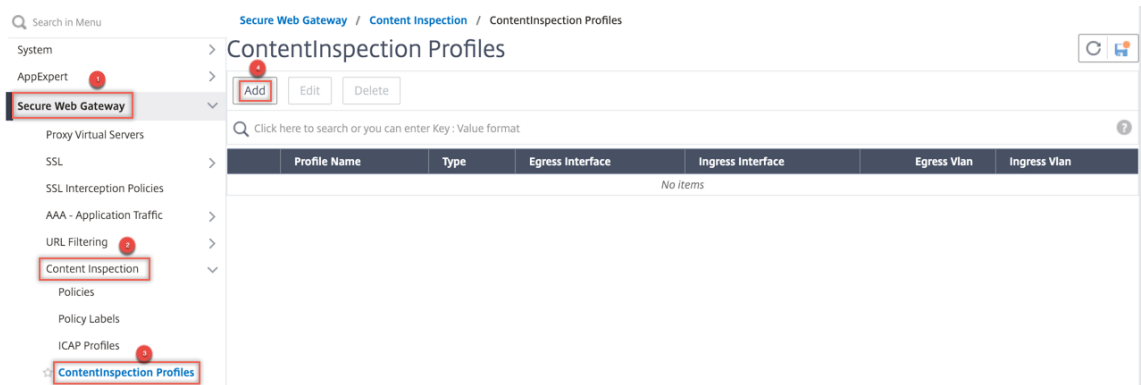
IPv6 Dynamic Routing

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. Navigate to **Secure Web Gateway > Content Inspection > Content Inspection Profiles**. Click **Add**.



Specify the ingress and egress VLANs.

← Create ContentInspectionProfile

Profile Name*

Type*

Egress Interface*

Ingress Interface*

Egress Vlan

Ingress Vlan

Create Close

Create another profiles. Specify a different ingress and egress VLAN in the second profile.

← Create ContentInspectionProfile

Profile Name*

Type*

Egress Interface*

Ingress Interface*

Egress Vlan

Ingress Vlan

5. Navigate to **Load Balancing > Services > Add** and add a service. In **Advanced Settings**, click **Profiles**. In the **CI Profile Name** list, select the content inspection profile created earlier. In **Service Settings**, set **Use Source IP Address** to YES and **Use Proxy Port** to No. In **Basic Settings**, set **Health Monitoring** to NO.

Create two services. Specify dummy IP addresses that are not owned by any of the devices, including the inline devices. Specify profile 1 in service 1, and profile 2 in service 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
Monitoring Connection Close Bit	NONE	AppFlow Logging	ENABLED

6. Navigate to **Load Balancing > Virtual Servers > Add**. Create a TCP load balancing virtual server.

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

Click **OK**.

7. Click inside the **Load Balancing Virtual Server Service Binding** section. In **Service Binding**, click the arrow in **Select Service**. Select the two services created earlier, and click **Select**. Click **Bind**.

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

- Navigate to **Secure Web Gateway > Proxy Virtual Servers > Add**. Specify a name, IP address, and port. In **Advanced Settings**, select **Policies**. Click the “+” sign.

← 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 >

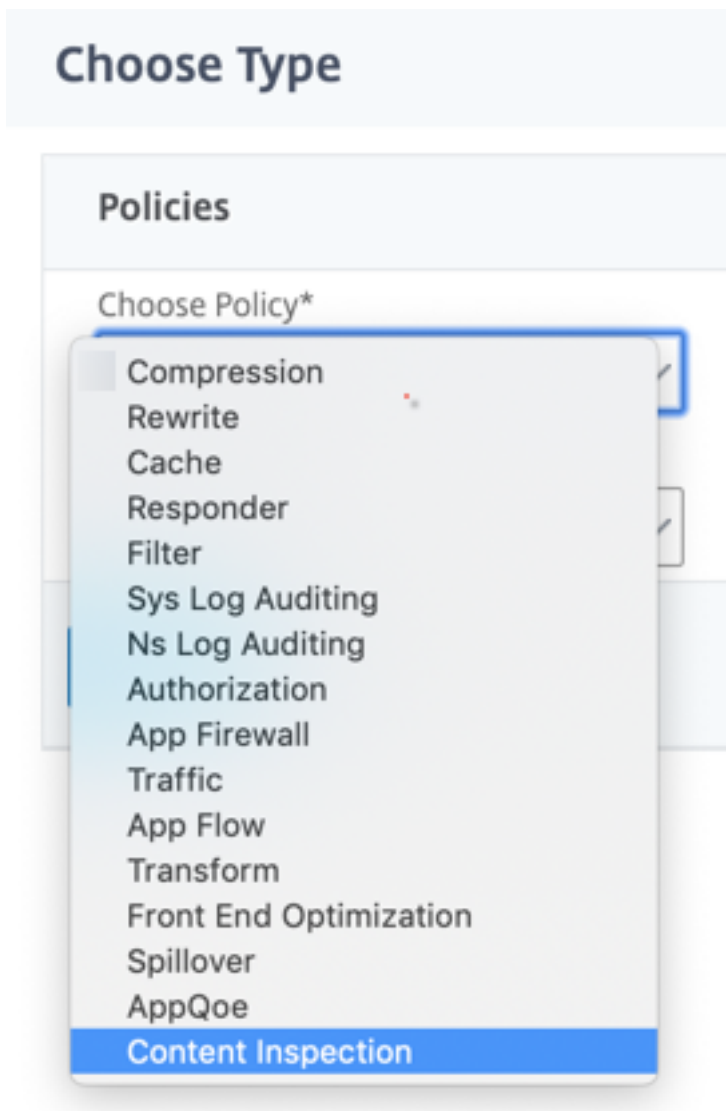
Certificate

No Server Certificate >

No CA Certificate >

Policies + x

- In **Choose Policy** select **Content Inspection**. Click **Continue**.



10. Click **Add**. Specify a name. In **Action**, click **Add**.

[Choose Type](#) / Create ContentInspection Policy

Create ContentInspection Policy

Policy Name*

Action*

Log Action

UNDEF Action

11. Specify a name. In **Type**, select **INLINEINSPECTION**. In **Server Name**, select the load balancing virtual server created earlier.

← Create ContentInspection Action

Name*

Type*

Server Name*

If Server Down

Request-Timeout

Request timeout action

12. Click **Create**. Specify the rule and click **Create**.

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. Click **Bind**.

14. Click **Done**.

Analytics

June 25, 2020

In Citrix SWG appliance, all the user records and subsequent records are logged. When you integrate Citrix Application Delivery Management (ADM) with Citrix SWG appliance, the logged user activity and the subsequent records in the appliance are exported to Citrix ADM using logstream.

Citrix ADM collates and presents information on the activities of users, such as, websites visited and the bandwidth spent. It also reports bandwidth use and detected threats, such as malware and phishing sites. You can use these key metrics to monitor your network and take corrective actions with the Citrix SWG appliance. For more information, see [Citrix Secure Web Gateway Analytics](#).

To integrate Citrix SWG appliance with Citrix ADM:

1. In the Citrix SWG appliance, while configuring the Secure Web Gateway, enable Analytics and provide the details of the Citrix ADM instance that you want to use for analytics.

2. In Citrix ADM, add the Citrix SWG appliance as an instance to Citrix ADM. For more information see [Add new Instances to Citrix ADM](#).

Use case: Making enterprise internet access compliant and secure

June 25, 2020

The director of network security in a financial organization wants to protect the enterprise network from any external threats coming from the web in the form of malware. To do this, the director needs to gain visibility in to otherwise bypassed encrypted traffic and control access to malicious websites. The director is required to do the following:

- Intercept and examine all the traffic, including SSL/TLS (encrypted traffic), coming into and going out of the enterprise network.
- Bypass interception of requests to websites containing sensitive information, such as user financial information or emails.
- Block access to harmful URLs identified as serving harmful or adult content.
- Identify end users (employees) in the enterprise who are accessing malicious websites and block internet access for these users or block the harmful URLs.

To achieve all of the above, the director can set up a proxy on all the devices in the organization and point it to the Citrix Secure Web Gateway (SWG), which acts as a proxy server in the network. The proxy server intercepts all the encrypted and unencrypted traffic passing through the enterprise network. It prompts for user authentication, and associates the traffic with a user. URL categories can be specified to block access to Illegal/Harmful, Adult, and Malware and SPAM websites.

To achieve the above, configure the following entities:

- DNS name server to resolve host names.
- Subnet IP (SNIP) address to establish a connection with the origin servers. The SNIP address should have internet access.
- Proxy server in explicit mode to intercept all outbound HTTP and HTTPS traffic.
- SSL profile to define SSL settings, such as ciphers and parameters, for connections.
- CA certificate-key pair to sign the server certificate for SSL interception.
- SSL policy to define the websites to intercept and to bypass.
- Authentication virtual server, policy, and action to ensure that only valid users are granted access.
- Appflow collector to send data to the Citrix Application Delivery Management (ADM).

Both CLI and GUI procedures are listed for this sample configuration. The following sample values are used. Replace them with valid data for IP addresses, SSL certificate and key, and LDAP parameters.

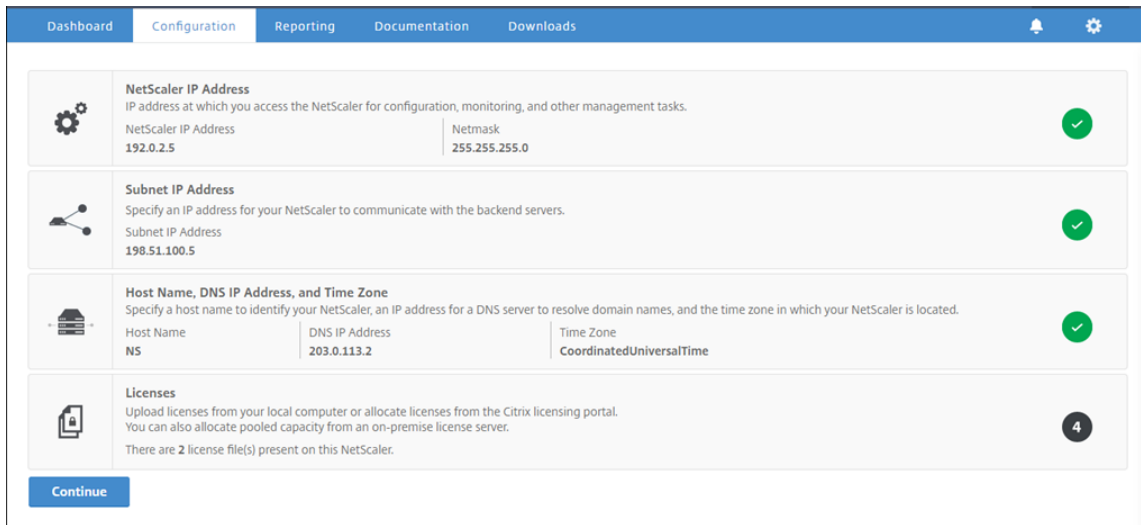
Name	Values used in the sample configuration
NSIP address	192.0.2.5
Subnet IP address	198.51.100.5
LDAP virtual server IP address	192.0.2.116
DNS name server IP address	203.0.113.2
Proxy server IP address	192.0.2.100
MAS IP address	192.0.2.41
CA certificate for SSL interception	ns-swg-ca-certkey (certificate: ns_swg_ca.crt and key: ns_swg_ca.key)
LDAP base DN	CN=Users,DC=CTXNSSFB,DC=COM
LDAP bind DN	CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM
LDAP bind DN password	zzzzz

Using the secure web gateway wizard to configure interception and examination of the traffic to and from the enterprise network

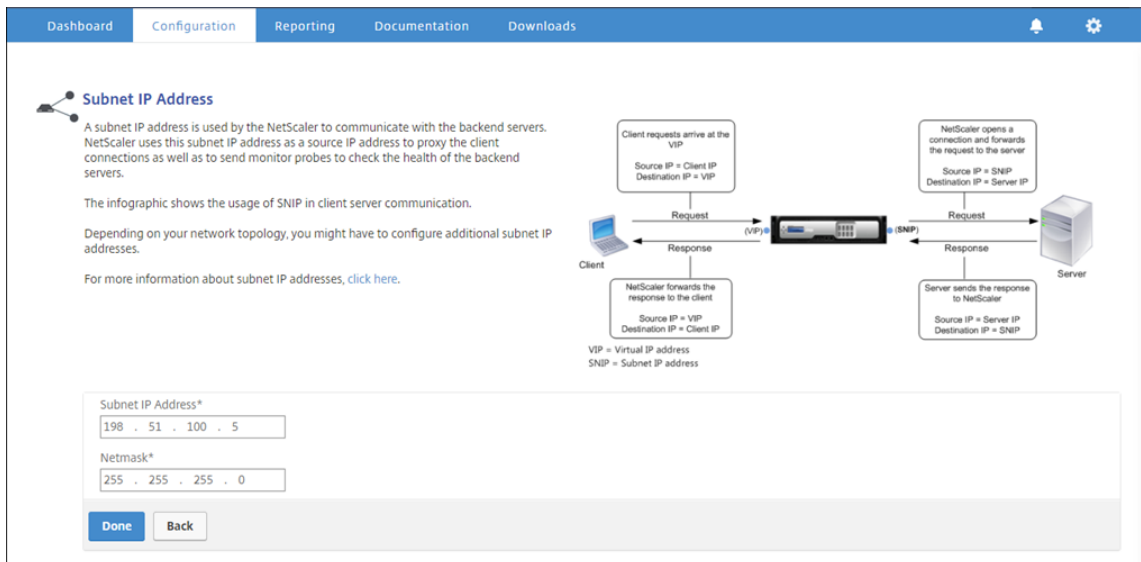
Creating a configuration for intercepting and examining encrypted traffic in addition to the other traffic to and from a network requires configuring proxy settings, SSLi settings, user authentication settings, and URL Filtering settings. The following procedures include examples of the values entered.

Configure SNIP address and DNS name server

1. In a web browser, type the NSIP address. For example, <http://192.0.2.5>.
2. In **User Name** and **Password**, type the administrator credentials. The following screen appears.

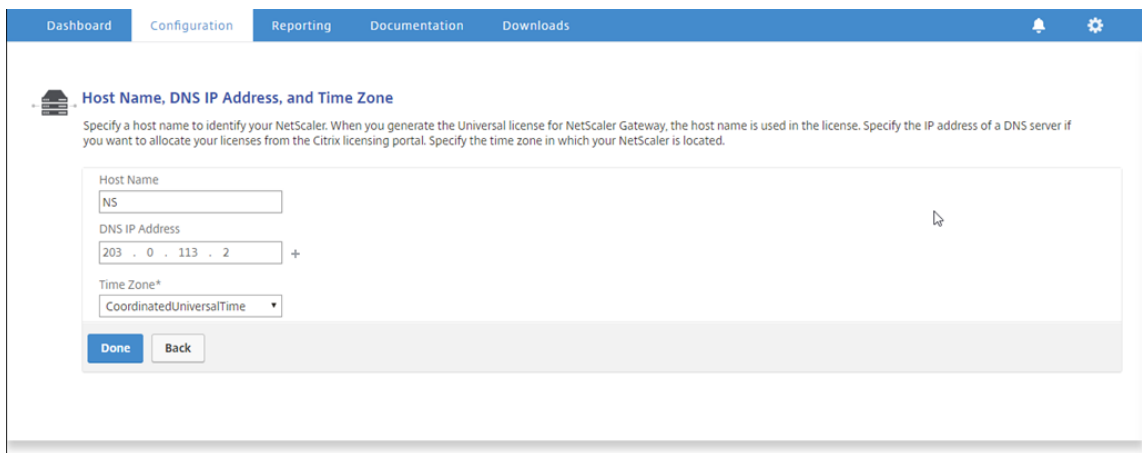


3. Click inside **Subnet IP Address** section, and enter an IP address.



4. Click **Done**.

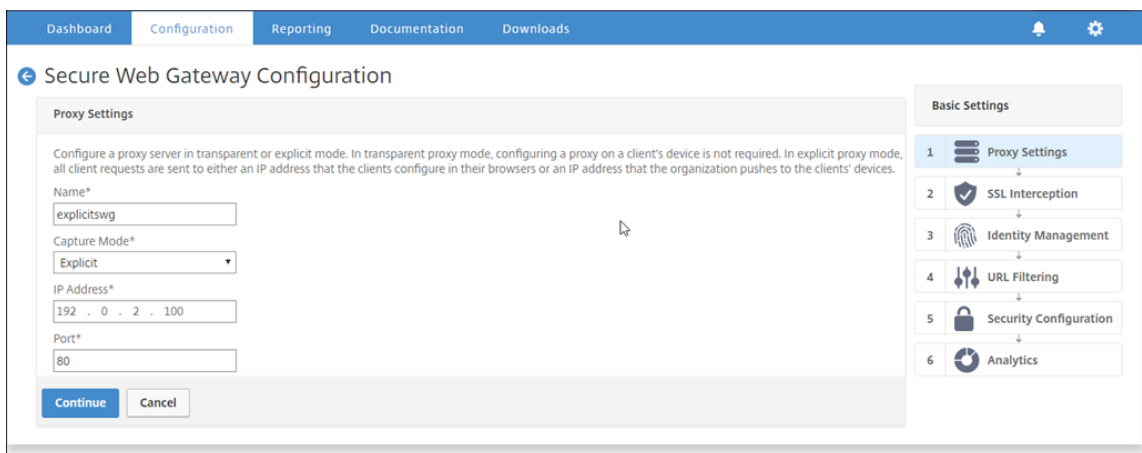
5. Click inside **Host Name, DNS IP Address, and Time Zone** section, and enter values for these fields.



6. Click **Done** and then click **Continue**.

Configure the proxy settings

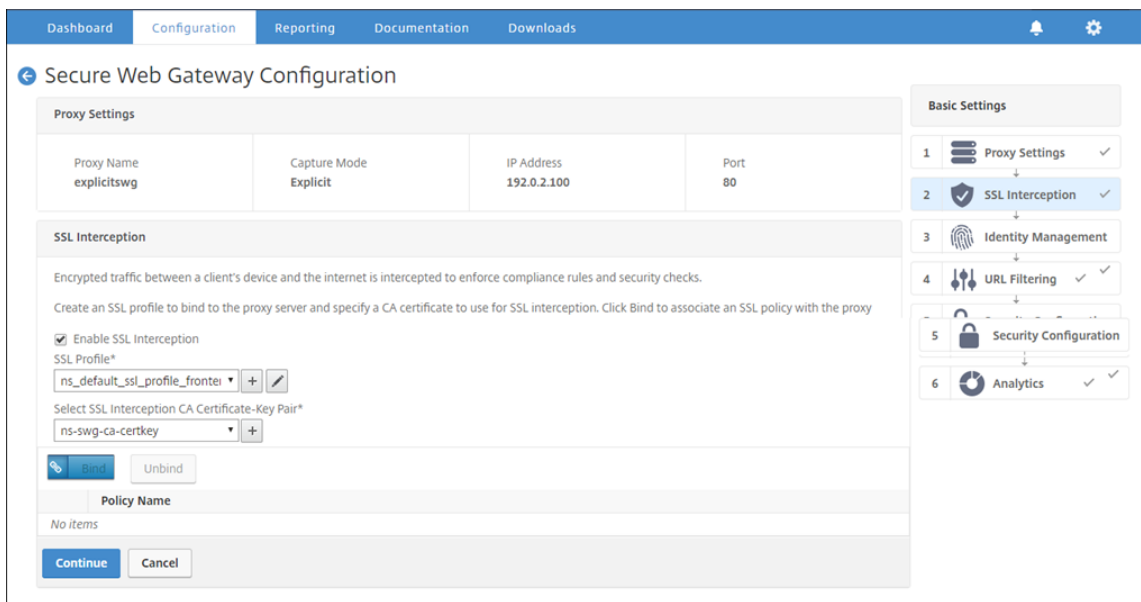
1. Navigate to **Secure Web Gateway > Secure Web Gateway Wizard**.
2. Click **Get Started** and then click **Continue**.
3. In the **Proxy Settings** dialog box, enter a name for the explicit proxy server.
4. For **Capture Mode**, select **Explicit**.
5. Enter an IP address and port number.



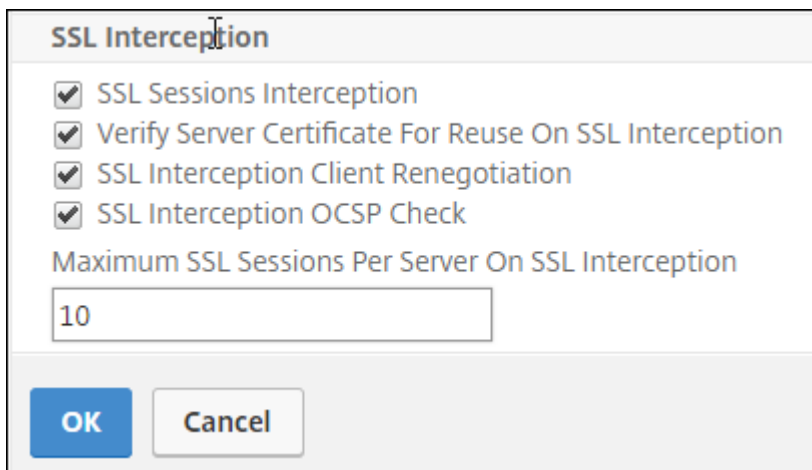
6. Click **Continue**.

Configure the SSL interception settings

1. Select **Enable SSL Interception**.



2. In **SSL Profile**, click “+” to add a new front-end SSL profile and enable **SSL Sessions Interception** in this profile.



3. Click **OK** and then click **Done**.
4. In **Select SSL interception CA Certificate-Key Pair**, click “+” to install a CA certificate-key pair for SSL interception.

Install SSL Interception CA Certificate

Certificate-Key Pair Name*
ns-swg-ca-certkey

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
30

Install **Close**

5. Click **Install** and then click **Close**.
6. Add a policy to intercept all the traffic. Click **Bind** and then click **Add**.

SSL Interception Policies ×

Add Edit Delete

Policy Name	Pattern Set Name	Action
No items		

Insert **Close**

7. Enter a name for the policy and select **Advanced**. In the Expression editor, enter true.
8. For **Action**, select **INTERCEPT**.

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*

ssl-pol

URL Categories Create Patset Security Configuration Advanced

Expression*

Expression Editor

Operators Saved Policy Expressions Frequently Used Expressions

true

Evaluate

Action*

INTERCEPT

Create Close

9. Click **Create** and then click **Add** to add another policy to bypass sensitive information.
10. Enter a name for the policy and in **URL Categories**, click **Add**.
11. Select the **Finance** and **Email** categories and move them to the **Configured** list.
12. For **Action**, select **BYPASS**.

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

Search Categories

- 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. Click **Create**.

14. Select the two policies created earlier, and click **Insert**.

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. Click **Continue**.

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

Configure the user authentication settings

1. Select **Enable user authentication**. In the **Authentication Type** field, select **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. Add LDAP server details.

Create Authentication LDAP Server ✕

Name*

Server Name
 Server IP

IP Address*

Security Type

Port

Server Type

Time-out (seconds)

Authentication

Connection Settings

Base DN (location of users)*

Administrator Bind DN*

Administrator Password*

Confirm Administrator Password*

[Retrieve Attributes](#)

Other Settings

Server Logon Name Attribute

Search Filter

Group Attribute

Sub Attribute Name

SSO Name Attribute

Default Authentication Group

User Required
 Referrals

Maximum Referral Level

Referral DNS Lookup

Validate LDAP Server Certificate

LDAP Host Name

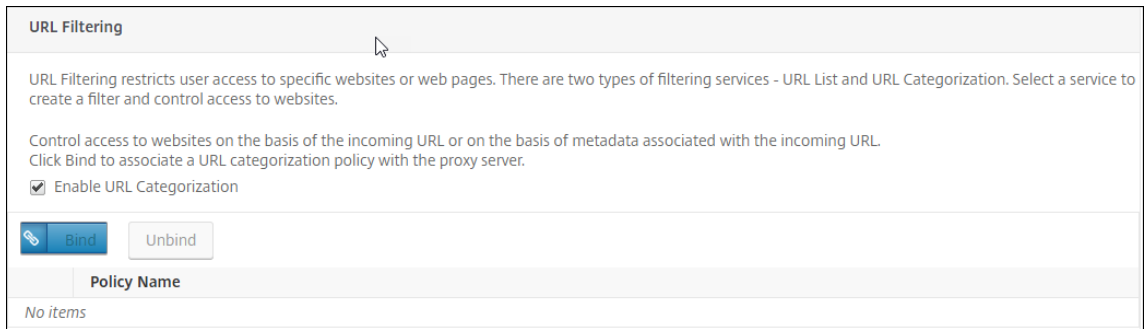
OTP Secret

▶ More

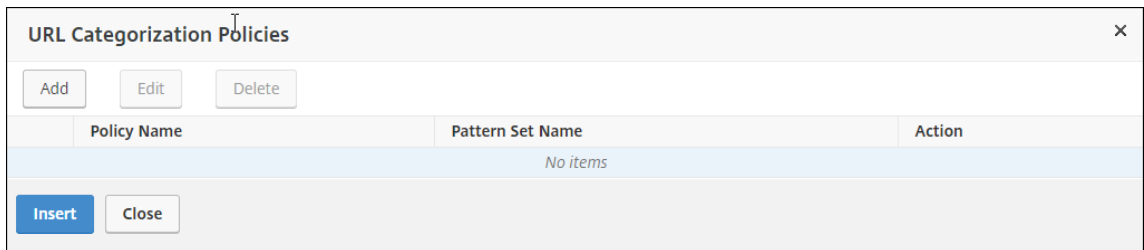
3. Click **Create**.
4. Click **Continue**.

Configure URL Filtering settings

1. Select **Enable URL Categorization**, and then click **Bind**.



2. Click **Add**.



3. Enter a name for the policy. For **Action**, select **Deny**. For **URL Categories**, select **Illegal/Harmful, Adult, and Malware and SPAM**, and move them to the **Configured** list.

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. Click **Create**.
5. Select the policy and then click **Insert**.

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. Click **Continue**.

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

Bind Unbind

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

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 list policy with the proxy server.

Enable URL List

7. Click **Continue**.
8. Click **Enable Analytics**.
9. Enter the IP address of Citrix ADM and for **Port**, specify 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*

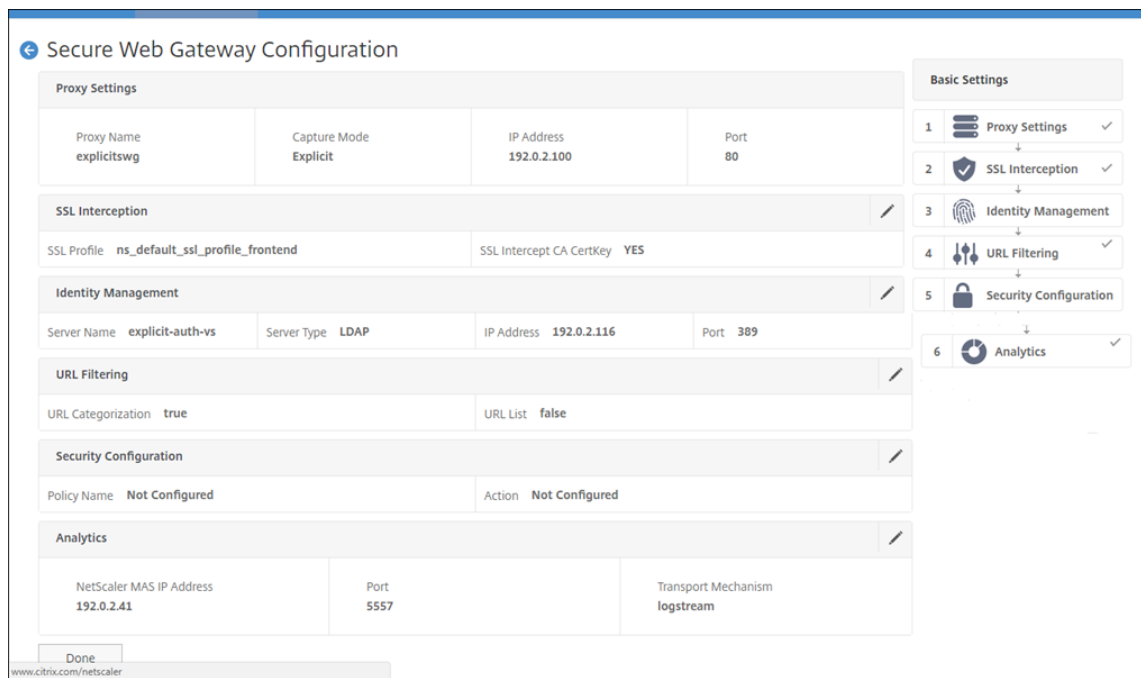
192 . 0 . 2 . 41

Port*

5557

Transport Mechanism: LogStream

10. Click **Continue**.
11. Click **Done**.



Use Citrix ADM to view key metrics for users and determine the following:

- Browsing behavior of the users in your enterprise.
- URL categories accessed by the users in your enterprise.
- Browsers used to access the URLs or domains.

Use this information to determine whether the user's system is infected by malware, or understand the bandwidth consumption pattern of the user. You can fine tune the policies on your Citrix SWG appliance to restrict these users, or block some more websites. For more information about viewing the metrics on MAS, see the "Inspecting Endpoints" use case in [MAS use cases](#).

Note

Set the following parameters by using the CLI.

```

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

```

CLI example

The following example includes all the commands used to configure interception and examination of the traffic to and from the enterprise network.

General configuration:

```
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-->
```

Authentication configuration:

```
1   add authentication vsServer explicit-auth-vs SSL
2
3   bind ssl vsServer 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 vsServer explicit-auth-vs -policy swg-auth-policy -
   priority 1
10  <!--NeedCopy-->
```

Proxy server and SSL interception configuration:

```
1   add cs vsServer 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 vsServer explicitswg -sslProfile swg_profile
10
11  add ssl policy ssli-pol_ssli -rule true -action INTERCEPT
12
13  bind ssl vsServer explicitswg -policyName ssli-pol_ssli -priority 100 -
   type INTERCEPT_REQ
```

```
14 <!--NeedCopy-->
```

URL categories configuration:

```
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 configuration to pull data into Citrix ADM:

```
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-->
```

Use case: Making enterprise network secure by using ICAP for remote malware inspection

June 25, 2020

The Citrix Secure Web Gateway (SWG) appliance acts as a proxy and intercepts all the client traffic. The appliance uses policies to evaluate the traffic and forwards client requests to the origin server

on which the resource resides. The appliance decrypts the response from the origin server and forwards the plain text content to the ICAP server for an antimalware check. The ICAP server responds with a message indicating “No adaptation required,” or error, or modified request. Depending on the response from the ICAP server, the content requested is either forwarded to the client, or an appropriate message is sent.

For this use case, you must perform some general configuration, proxy and SSL interception related configuration, and ICAP configuration on the Citrix SWG appliance.

General configuration

Configure the following entities:

- NSIP address
- Subnet IP (SNIP) address
- DNS name server
- CA certificate-key pair to sign the server certificate for SSL interception

Proxy server and SSL interception configuration

Configure the following entities:

- Proxy server in explicit mode to intercept all outbound HTTP and HTTPS traffic.
- SSL profile to define SSL settings, such as ciphers and parameters, for connections.
- SSL policy to define rules for intercepting traffic. Set to true to intercept all client requests.

For more details, see the following topics:

- [Proxy modes](#)
- [SSL interception](#)

In the following sample configuration, the antimalware detection service resides at www.example.com.

Sample general configuration:

```
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-->
```


Sample proxy server and SSL interception configuration:

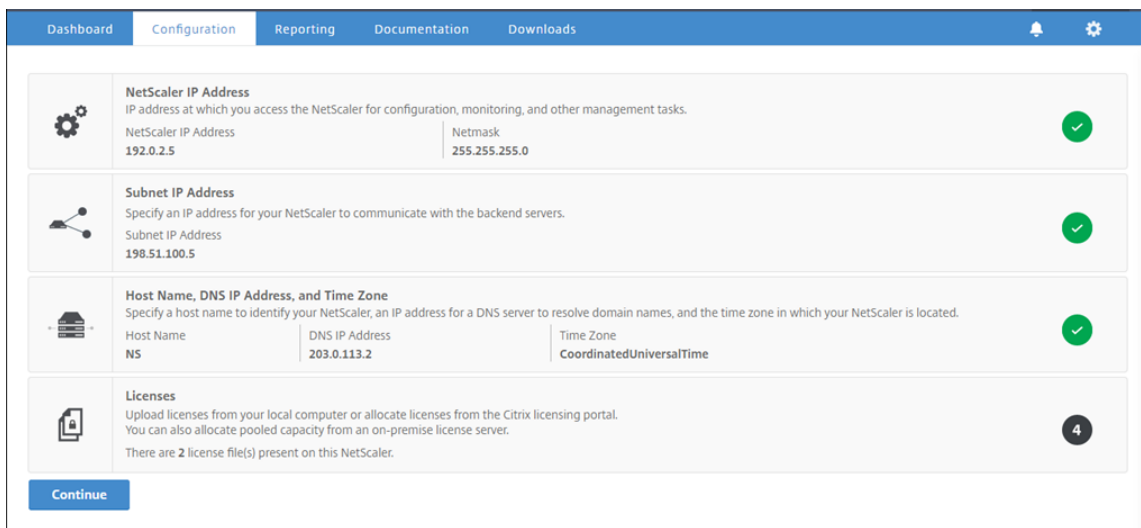
```
1 add cs vserver explicitSWG PROXY 192.0.2.100 80 - Authn401 ENABLED -  
  authnVsName explicit-auth-vs  
2  
3 set ssl parameter -defaultProfile ENABLED  
4  
5 add ssl profile swg_profile -sslInterception ENABLED  
6  
7 bind ssl profile swg_profile -ssliCACertkey ns-swg-ca-certkey  
8  
9 set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

Sample ICAP Configuration:

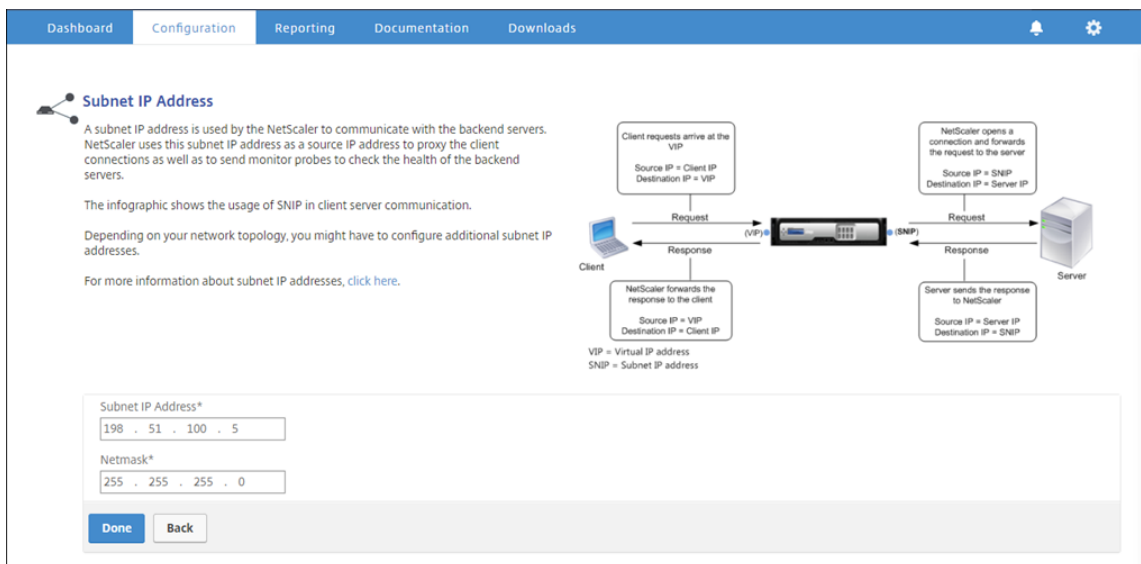
```
1 add service icap_svc 203.0.113.225 TCP 1344  
2  
3 enable ns feature contentinspection  
4  
5 add icaprofile icaprofile1 -uri /example.com -Mode RESMOD  
6  
7 add contentInspection action CiRemoteAction -type ICAP -serverName  
  icap_svc -icapProfileName icaprofile1  
8  
9 add contentInspection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

Configure SNIP address and DNS name server

1. In a web browser, type the NSIP address. For example, <http://192.0.2.5>.
2. In **User Name** and **Password**, type the administrator credentials. The following screen appears. If the following screen does not appear, skip to the proxy settings section.

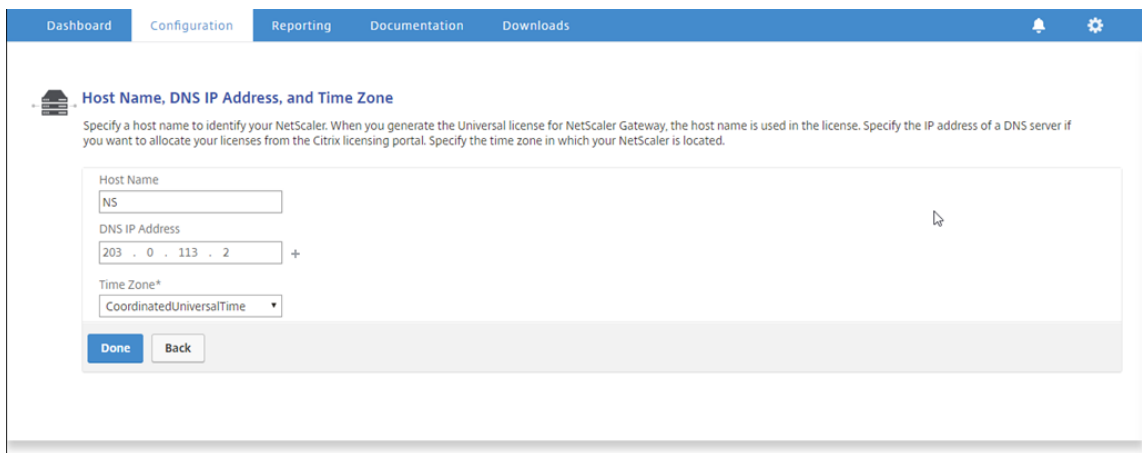


3. Click inside **Subnet IP Address** section, and enter an IP address.



4. Click **Done**.

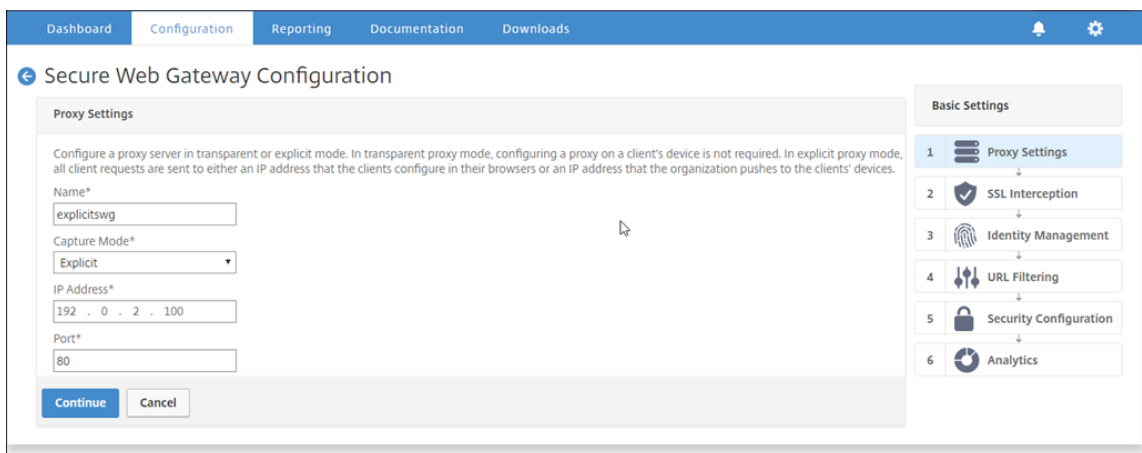
5. Click inside **Host Name, DNS IP Address, and Time Zone** section, and enter values for these fields.



6. Click **Done** and then click **Continue**.

Configure the proxy settings

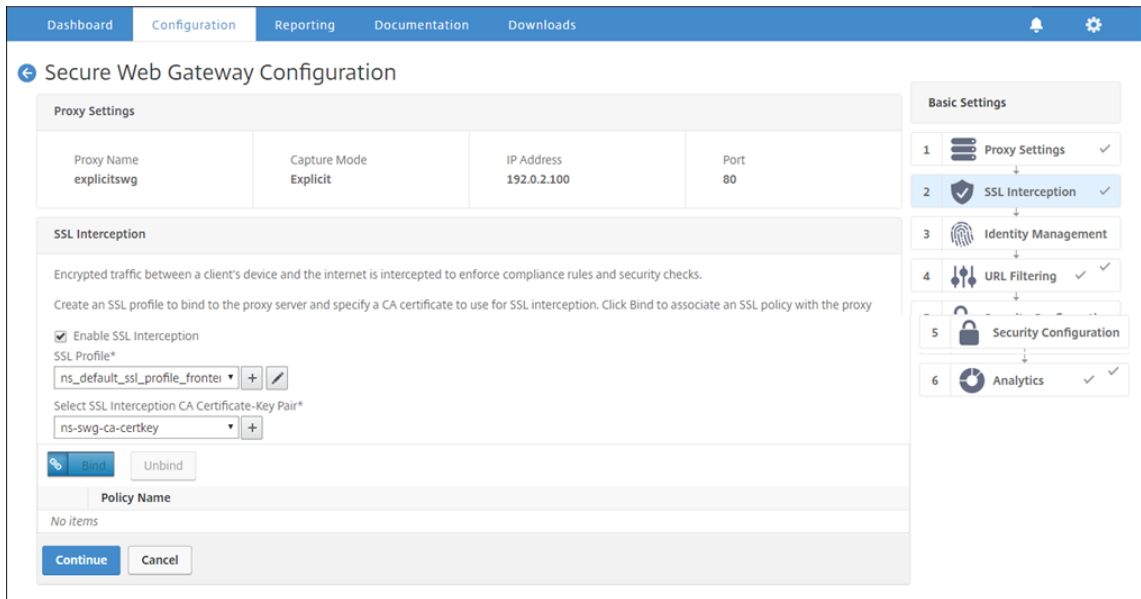
1. Navigate to **Secure Web Gateway > Secure Web Gateway Wizard**.
2. Click **Get Started** and then click **Continue**.
3. In the **Proxy Settings** dialog box, enter a name for the explicit proxy server.
4. For **Capture Mode**, select **Explicit**.
5. Enter an IP address and port number.



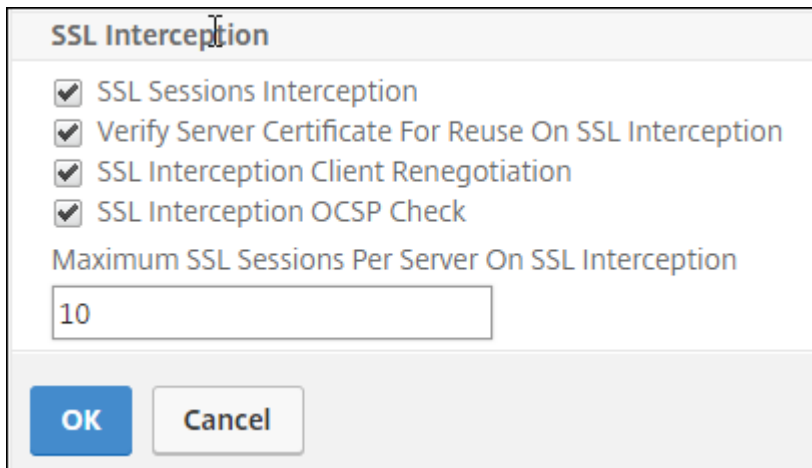
6. Click **Continue**.

Configure the SSL interception settings

1. Select **Enable SSL Interception**.



2. In **SSL Profile**, select an existing profile or click “+” to add a new front-end SSL profile. Enable **SSL Sessions Interception** in this profile. If you select an existing profile, skip the next step.



3. Click **OK** and then click **Done**.
4. In **Select SSL interception CA Certificate-Key Pair**, select an existing certificate or click “+” to install a CA certificate-key pair for SSL interception. If you select an existing certificate, skip the next step.

Install SSL Interception CA Certificate

Certificate-Key Pair Name*

Certificate File Name*
 ?

Key File Name*
 ?

Notify When Expires

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

Notification Period

Install

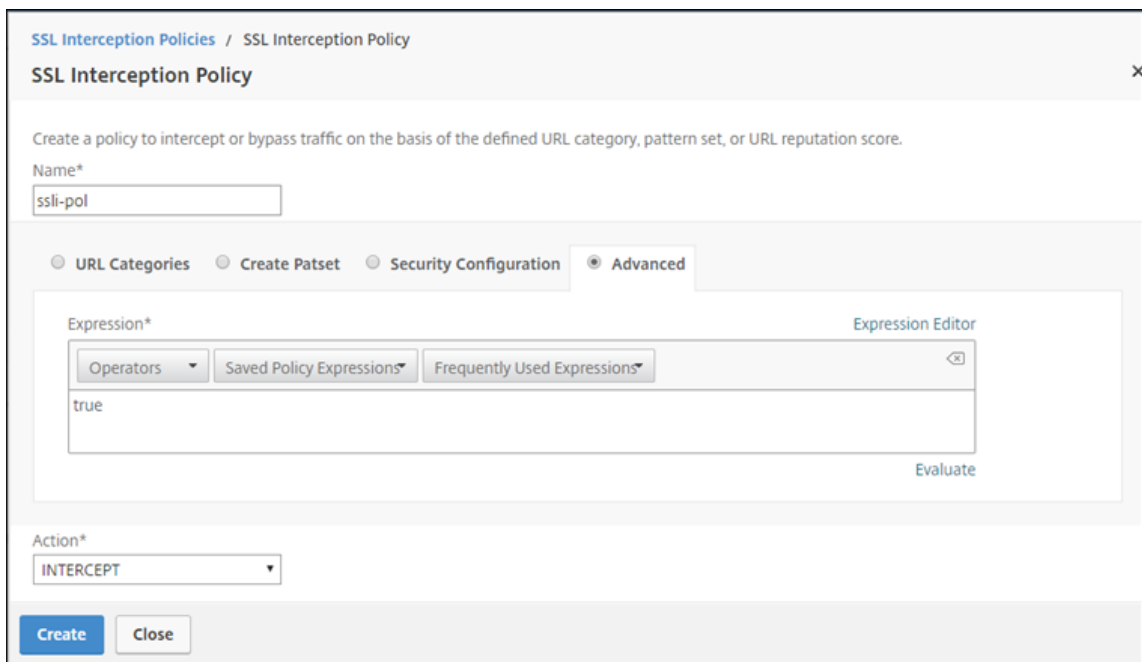
5. Click **Install** and then click **Close**.
6. Add a policy to intercept all the traffic. Click **Bind**. Click **Add** to add a new policy or select an existing policy. If you select an existing policy, click **Insert**, and skip the next three steps.

SSL Interception Policies ×

Policy Name	Pattern Set Name	Action
No items		

Insert

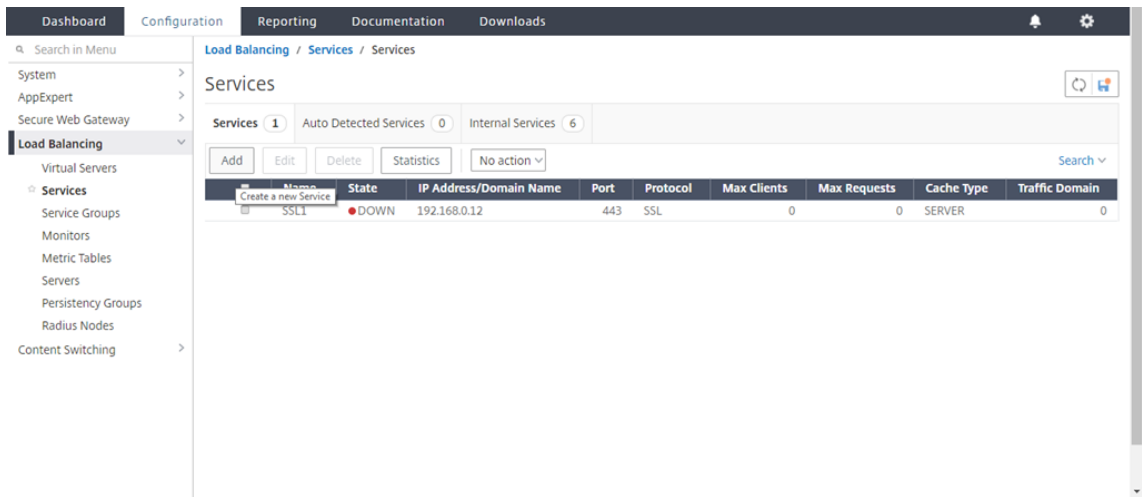
7. Enter a name for the policy and select **Advanced**. In the Expression editor, enter true.
8. For **Action**, select **INTERCEPT**.



9. Click **Create**.
10. Click **Continue** four times, and then click **Done**.

Configure the ICAP settings

1. Navigate to **Load Balancing > Services** and click **Add**.



2. Type a name and IP address. In **Protocol**, select **TCP**. In **Port**, type **1344**. Click **OK**.

Dashboard Configuration Reporting Documentation Downloads

Load Balancing Service

Basic Settings Help >

Service Name*
icap_svc

New Server Existing Server

IP Address*
203 . 0 . 113 . 100

Protocol*
TCP

Port*
1344

More

OK Cancel

3. Navigate to **Secure Web Gateway > Proxy Virtual Servers**. Add a proxy virtual server or select a virtual server and click **Edit**. After entering details, click **OK**.

Dashboard Configuration Reporting Documentation Downloads

Proxy Virtual Server

Basic Settings Help >

Name*
explicitswg

IP Address Type*
IP Address

IP Address*
192 . 0 . 2 . 100

Port*
80

More

OK Cancel

Click **OK** again.

Dashboard Configuration Reporting Documentation Downloads

Proxy Virtual Server

Basic Settings Help >

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

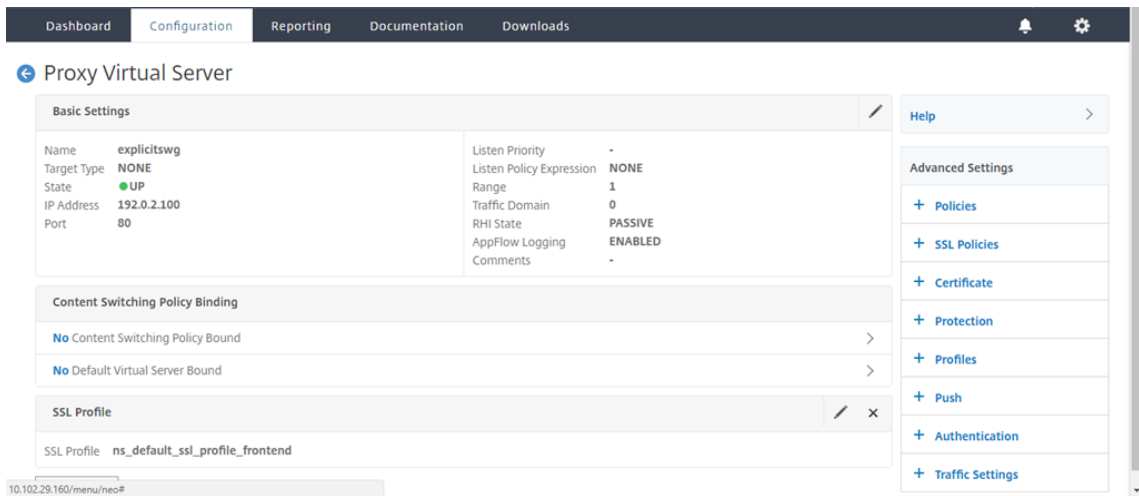
Content Switching Policy Binding

No Content Switching Policy Bound >

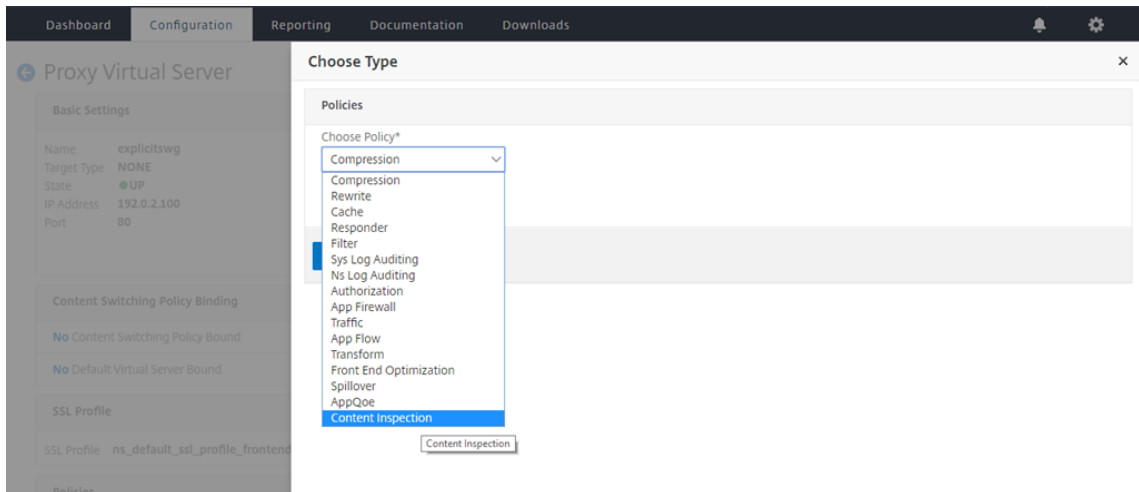
No Default Virtual Server Bound >

OK

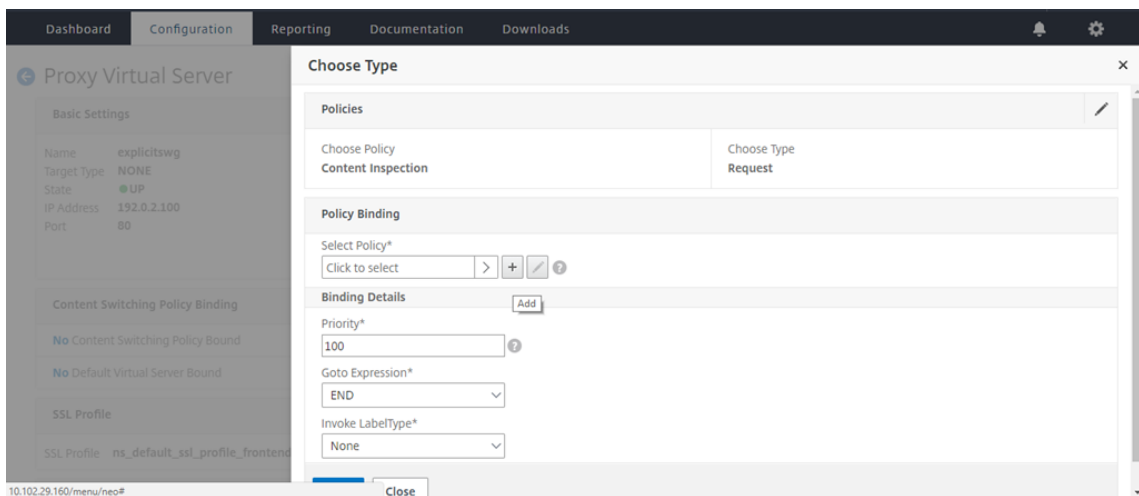
4. In **Advanced Settings**, click **Policies**.



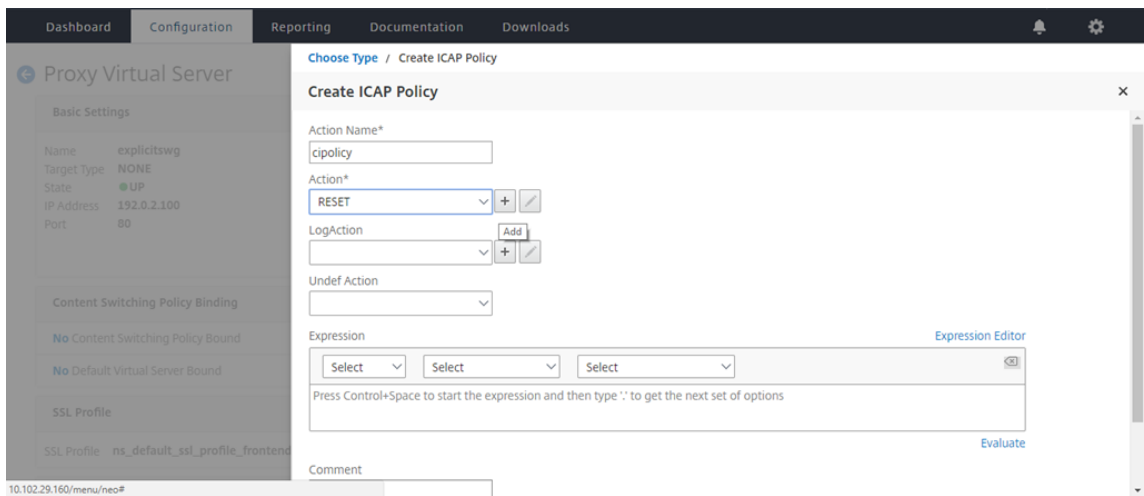
5. In **Choose Policy**, select **Content Inspection**. Click **Continue**.



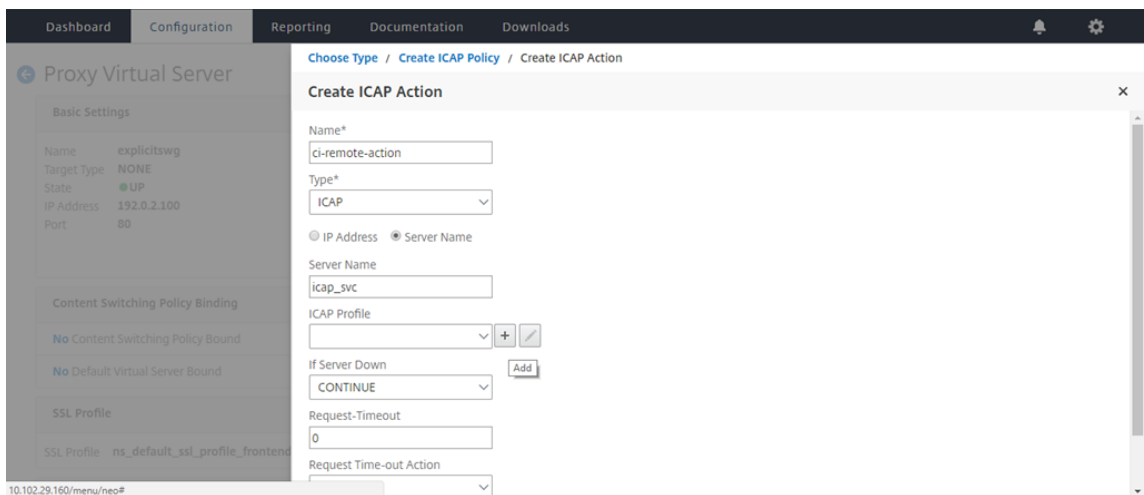
6. In **Select Policy**, click the “+” sign to add a policy.



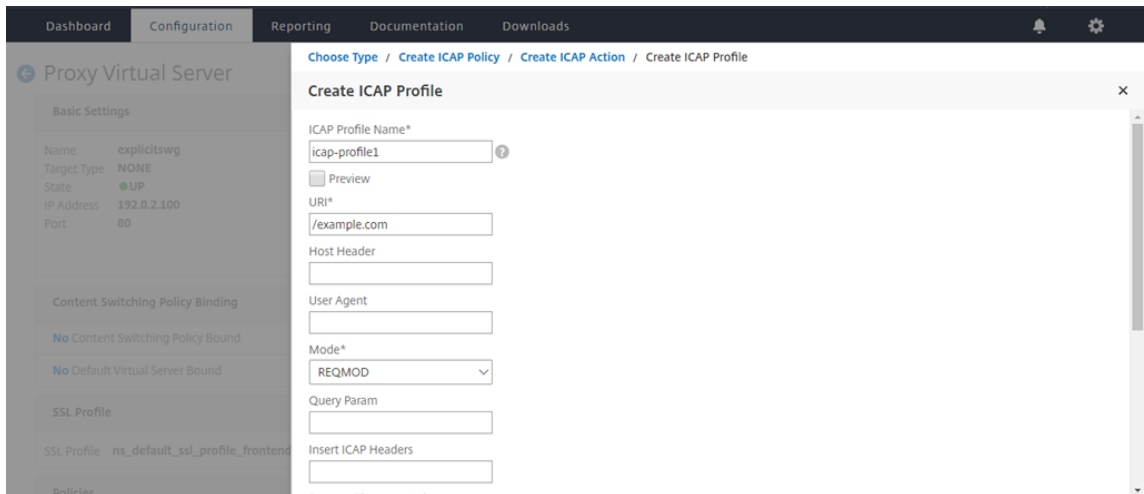
7. Enter a name for the policy. In **Action**, click the “+” sign to add an action.



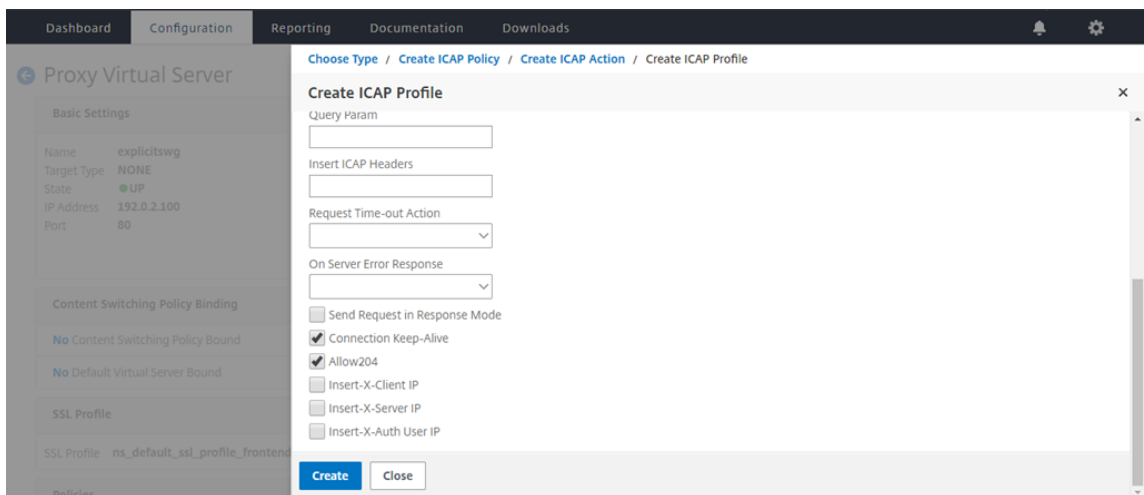
8. Type a name for the action. In **Server Name**, type the name of the TCP service created earlier. In **ICAP Profile**, click the “+” sign to add an ICAP profile.



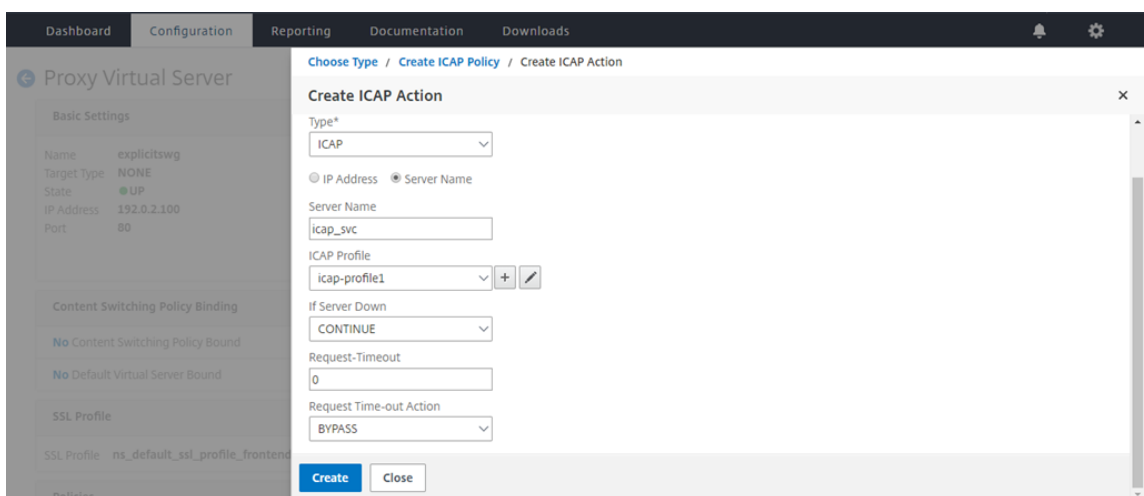
9. Type a profile name, URI. In **Mode**, select **REQMOD**.



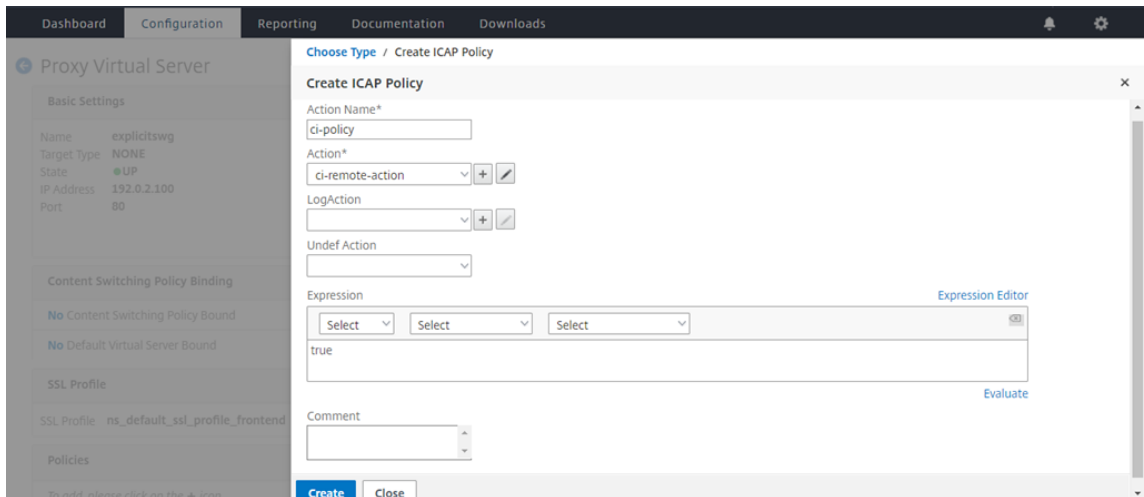
10. Click **Create**.



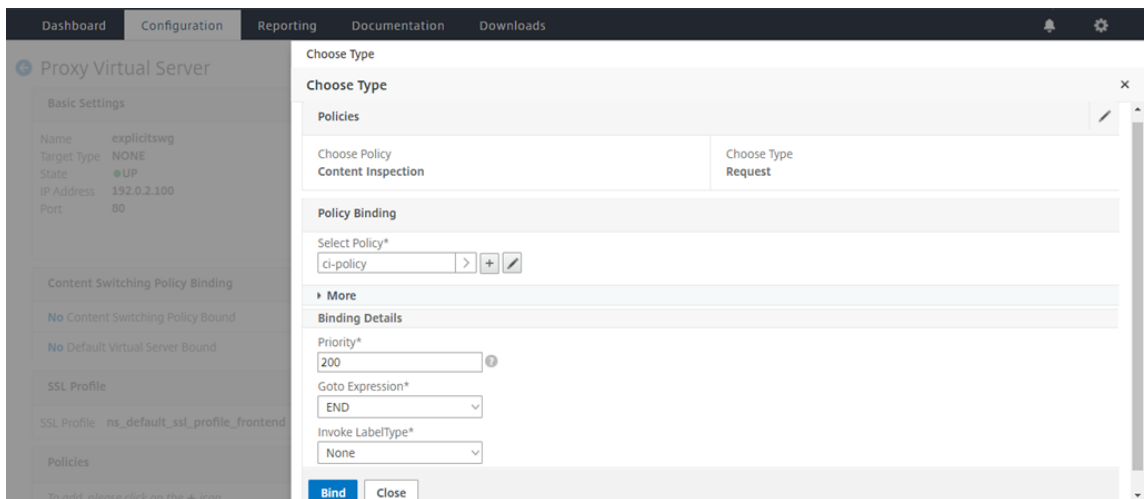
11. In the **Create ICAP Action** page, click **Create**.



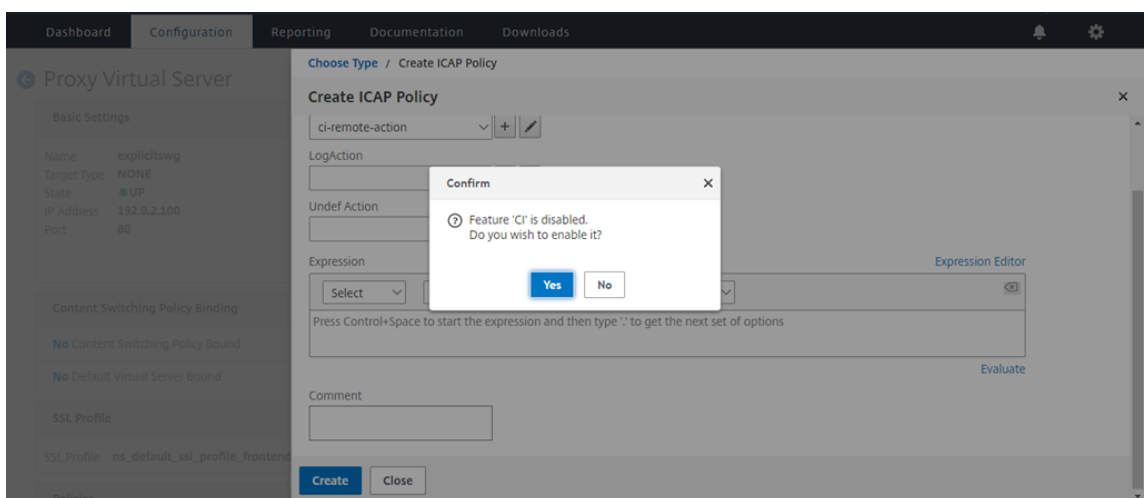
12. In the **Create ICAP Policy** page, enter true in the **Expression Editor**. Then, click **Create**.



13. Click **Bind**.



14. If prompted to enable the content inspection feature, select **Yes**.



15. Click **Done**.

The screenshot shows the configuration page for a Proxy Virtual Server named 'explicitSWG'. The interface is divided into several sections:

- 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

On the right side, there is a 'Help' button and an 'Advanced Settings' sidebar with expandable sections: SSL Policies, Certificate, Protection, Profiles, Push, Authentication, and Traffic Settings. A 'Done' button is located at the bottom left of the configuration area.

Sample ICAP transactions between the Citrix SWG appliance and the ICAP server in RESPMOD

Request from the Citrix SWG appliance to the ICAP server:

```

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-->

```

Response from the ICAP server to the Citrix SWG appliance:

```
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-->
```

How-to articles

June 25, 2019

Following are some configuration instructions or functional use cases available as “How to” articles

to help you manage your SWG deployment.

URL filtering

[How to create a URL categorization policy](#)

[How to create a URL list policy](#)

[How to whitelist an exceptional URL](#)

[How to block adult category web sites](#)

How to create a URL categorization policy

June 25, 2020

As a network administrator, you might want to block specific categories of websites for user access. You can perform this by creating a URL Categorization policy and binding the policy with a pre-defined list of categories that you want to restrict access.

For example, you might want to restrict access to all social networking websites as per organizational policies. In such a scenario, you must create a categorization policy and bind the policy to the pre-defined list of social networking category websites.

To create URL categorization policy by using basic method:

1. Log on to the **Citrix SWG** appliance and navigate to **Secured Web Gateway > URL Filtering > URL Categorization**.
2. In the details pane, click **Add** to access the **URL Categorization Policy** page and specify the following parameters.
 - a) **URL Categorization Policy**. Name of the responder policy.
 - b) **Basic**. Select Configure using a predefined list of categories.
 - c) **Action**. An action to control access to the URL.
 - d) **URL Categories**. A predefined list of categories to select and add it to a configured list.
3. Click **Create** and **Close**.

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

To create URL categorization policy by using advanced method:

1. To configure a new URL Categorization policy using advanced categorization.
2. Click **Add**.
3. In the **URL Categorization Policy** page, specify the following parameters.
 - a) **URL Categorization Policy**. Name of the responder policy.
 - b) **Advanced**. Configure policy using custom expressions.
4. Click **Create** and **Close**.

← 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

How to create a URL list policy

June 25, 2020

As a network administrator, you might want to block specific categories of websites for user access. You can perform this by creating URL List policy and bind the policy with an URL set imported into the appliance as a text file. The URL set is a collection of websites that you prefer to filter.

For example, you might want to restrict access to all malware websites as per organizational policies. In such a scenario, you must create a URL List policy and bind the policy to a URL set imported into the appliance.

To configure a URL list policy:

1. Log on to the **Citrix SWG** appliance and navigate to **Secured Web Gateway > URL Filtering > URL Lists**.
2. In the details pane, click **Add**.
3. On the **URL List Policy** page, specify the policy name.
4. Select an option to either import a URL set or create a pattern set and then perform one of the procedures that follow the last step of this procedure.
5. Select a responder action from the drop-down list.
6. Click **Create** and **Close**.

To import a custom URL set or third party URL set:

1. In the **URL List Policy** tab page, select the **Import URL Set** check box and specify the following URL Set parameters.
 - a) **URL Set Name**—Name of the URL set.
 - b) **URL**—Web address of the location at which to access the URL Set.
 - c) **Overwrite**—Overwrites the previously imported URL set.
 - d) **Delimiter**—Character sequence that delimits a CSV file record.
 - e) **Row Separator**—Row separator used in the CSV file.
 - f) **Interval**—Interval in seconds, rounded off to the nearest 15 minutes, at which the URL set is updated.
 - g) **Private Set**—Option to prevent exporting the URL set.
 - h) **Canary URL**—Internal URL for testing if the content of the URL set is to be kept confidential. The maximum length of the URL is 2047 characters. For more information about Canary URL, see Configuring a Private URL Set section.

← 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*
 + ?

To create a pattern set:

1. In the **Create Pattern** tab page, enter a name for the pattern set.
2. Click **Insert** to create a pattern.
3. On the **Configure Policy Patset to Pattern Binding** page, set the following parameters.
 - a) **Pattern**—String of characters that constitutes a pattern
 - b) **Charset**—Character set type: ASCII or UTF_8 format
 - c) **Index**—User-assigned index value, from 1 through 4294967290
4. Click **Insert** to add the pattern set, and then click **Close**.

How to whitelist an exceptional URL

June 25, 2020

When you use a URL Filter to blacklist a category of websites, you might have to whitelist or allow a specific website as an exception. For example, if you prefer to blacklist gaming websites but prefer to whitelist only www.supersports.com, you must create a patset with a URL list policy and then, bind the policy to the proxy server with a greater priority than other bound policies.

To create a Pattern Set using the Citrix SWG Wizard

1. Log on to the **Citrix SWG** appliance and navigate to **Secured Web Gateway > URL Filtering > URL Lists**.
2. In the details pane, click **Add**.
3. In the **URL List Policy** page, specify the policy name.
4. Select an option to either import a URL Set or create a Pattern Set.
5. In the **Create Pattern** tab page, enter a name for the pattern set.
6. Click **Insert** to create a pattern.
7. In the **Configure Policy Patset to Pattern Binding** page, set the following parameters.
 - a) **Pattern**—A string of characters that constitutes a pattern.
 - b) **Charset**—Character set type defines as ASCII or UTF_8 format.

- c) **Index**—A user assigned index value, from 1 through 4294967290
8. Click **Insert** to add the pattern set and click **Close**.

← 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*

To set priority of the policy expression by using the Citrix SWG GUI:

1. Log on to the **Citrix SWG** appliance and navigate to **Secure Web Gateway > Proxy Virtual Servers**.
2. In the details page, select a server and click **Edit**.
3. In the **Proxy Virtual Servers** page, go to **Policies** section and click the pencil icon to edit the details.
4. Select the patset policy that you created and in **Policy Binding** page, specify the priority value lower than other bound policies.
5. Click **Bind** and **Done**.

How to block adult category website

June 25, 2020

As an enterprise customer, you might want to block websites belonging to Adult category group. This is done by configuring a responder policy that selects requests belonging to an adult category and block access to such blacklisted URLs.

Configure URL categorization to block websites belonging to adult category

To configure a policy and block adult websites by using the CLI:

At the command prompt, type the following command:

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

Example:

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

Configure URL categorization for blocking adult web sites by using the Citrix SWG wizard

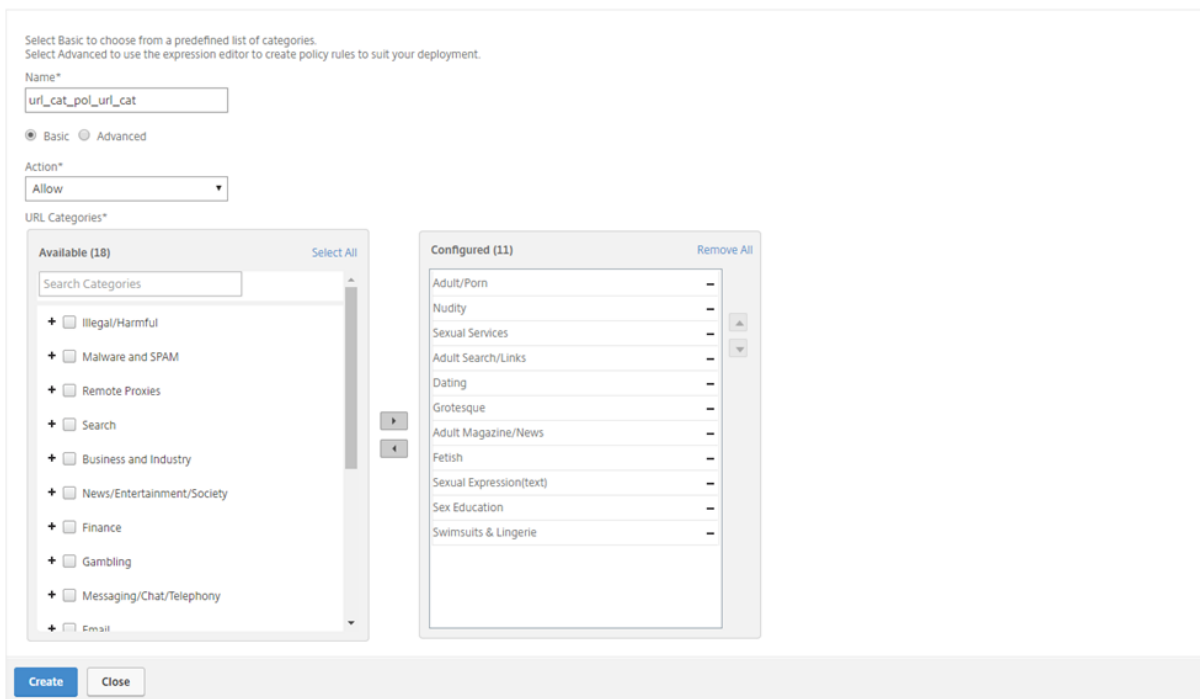
To block adult categories by using the Citrix SWG wizard

1. Log on to **Citrix SWG** appliance and navigate to **Secure Web Gateway**.
2. In the details pane, click **Secured Web Gateway Wizard**.
3. In the **Secure Web Gateway Configuration** page, specify the SWG proxy server settings.
4. Click **Continue** to specify other settings such as SSL interception and identify management.
5. Click **Continue** to access the **URL Filtering** section.
6. Select **Enable URL Categorization** checkbox to enable the feature.
7. Click Bind to access **URL Categorization Policies** slider.
8. Select a policy and click **Insert** to bind the policy.
9. Select the responder policy to block adult websites.
10. To add a new policy, click **Add** to access the **URL Categorization Policy** page and do one of the following.
 - a) To configure a policy using basic categorization, click **Add**.
 - i. In the **URL Categorization Policy** page, specify the following parameters.
 - A. URL Categorization Policy. Name of the responder policy.
 - B. Basic. Configure policy using the basic configuration method.
 - C. Action. An action to control access to the URL.
 - D. URL Categories. Select Adult category from the predefined list.
11. Click **Create** and **Close**.
 - a) To configure a new URL Categorization policy using advanced categorization, click **Add**.
 - i. In the **URL Categorization Policy** page, specify the following parameters.

- A. **URL Categorization Policy**. Name of the responder policy.
- B. **Advanced**. Configure policy to block requests of Adult category group.

12. Click **Create** and **Close**.

← URL Categorization Policy



System

April 2, 2020

System features provide conceptual information and configuration instructions that you might want to refer when configuring a Citrix SWG appliance.

The following table describes the features in a Citrix SWG appliance.

[Basic Operations](#) - System level operation and configuration details of a Citrix ADC appliance.

[Authentication and Authorization](#) - Configuration details in creating users, user groups, and command policies, and assigning policies to user accounts

[TCP Configuration](#) - Configuration details of TCP profile and TCP capabilities on a Citrix ADC appliance.

[HTTP Configuration](#) - Configuration details of HTTP profile and HTTP capabilities on a Citrix ADC appliance.

[SNMP](#) - A network management protocol monitoring the Citrix ADC appliance and promptly responding to issues on the appliance.

[Audit Logging](#) - A standard protocol for logging Citrix ADC appliance states and status information collected by various modules in the kernel and in the user-level daemons. For audit logging, you can use SYSLOG or NSLOG protocol or both.

[Call Home](#) - A notification system for monitoring and solving critical error conditions on a Citrix SWG appliance.

[Reporting Tool](#) - A web based interface accessed from a Citrix SWG appliance for viewing system performance reports as charts.

Networking

January 30, 2019

The following topics provide conceptual reference information and configuration instructions for networking features that you might want to configure on a Citrix SWG appliance.

- [IP addressing](#) Citrix ADC owned IP addresses and their configuration details.
- [Interfaces](#) Accessing and configuring the Citrix SWG appliance.
- [Access control lists \(ACL\)](#) Different types of access control lists used on Citrix ADC appliances, with configuration details.
- [IP routing](#) The different IP routing protocols used on a Citrix ADC appliance.
- [Internet protocol version 6 \(IPv6\)](#) Internet Protocol support on a Citrix ADC appliance, and how the appliance functions as an IPv6 node.
- [VXLAN](#) Virtual eXtensible Local Area Network (VXLAN) support in the Citrix ADC network infrastructure, and how VXLAN overlays Layer 2 networks onto a Layer 3 infrastructure by encapsulating Layer-2 frames in UDP packets.

AppExpert

August 10, 2020

The following topics provide conceptual information and configuration instructions for AppExpert features that you might want to configure on a Citrix SWG appliance.

Pattern Sets and Data Sets - Policy expressions for performing string matching operations on a large set of string patterns.

Depending on the pattern type you want to match, you can use one of the following features to implement pattern matching:

- A pattern set is an array of indexed patterns used for string matching during default syntax policy evaluation. Example of a pattern set: `imagetypes {svg, bmp, png, gif, tiff, jpg}`.
- A data set is a specialized form of pattern set. It is an array of patterns of types number (integer), IPv4 address, or IPv6 address.

Variables - Objects that store information in the form of tokens and are used by responder policy actions.

Variables are of two types as given below:

- Singleton variables. Can have a single value of one of the following types: `ulong` and `text` (max-size). The `ulong` type is an unsigned 64-bit integer, the `text` type is a sequence of bytes, and `max-size` is the maximum number of bytes in the sequence.
- Map variables. Maps hold values associated with keys: each key-value pair is called a map entry. The key for each entry is unique within the map.

Policies and Expressions - Policies control web traffic that enters into a Citrix SWG appliance. A policy uses a logical expression, also called a rule, to evaluate requests, responses, or other data, and applies one or more actions determined by the outcome of the evaluation. Alternatively, a policy can apply a profile, which defines a complex action.

Responder - Policy that sends responses based on who sends the request, where it is sent from, and other criteria with security and system management implications. The feature is simple and quick to use. By avoiding the invocation of more complex features, it reduces CPU cycles and time spent in handling requests that do not require complex processing. For handling sensitive data such as financial information, if you want to ensure that the client uses a secure connection to browse a website, you can redirect the request to secure connection by using HTTPS protocol.

Rewrite - Policy that rewrites information in the requests and responses handled by the Citrix SWG appliance. Rewriting can help in providing access to the requested content without exposing unnecessary details about the website's actual configuration.

URL Sets - Advanced Policy expressions to blacklist one million URL entries. To prevent access to restricted websites, a Citrix SWG appliance uses a specialized URL matching algorithm. The algorithm uses a URL set that can contain a list of URLs up to one million (1,000,000) blacklisted entries. Each entry can include metadata that defines URL categories and category groups as indexed patterns. The appliance can also periodically download URLs of highly sensitive URL sets managed by internet enforcement agencies (with government websites) or independent Internet organizations.

SSL

January 30, 2019

The following topics provide conceptual reference information and configuration instructions for SSL features that you might want to configure on a Citrix SWG appliance.

- [Certificates](#)
- [Certificate revocation lists \(CRL\)](#)
- [SSL policies](#)
- [OCSP responder](#)

FAQs

June 25, 2019

Q. Which hardware platforms are supported for Citrix Secure Web Gateway (SWG)?

A. Citrix SWG is available is on the following hardware platforms:

- 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
- All Cavium N2 and N3 based SDX platforms

Q. What are the two capture modes that I can set when creating a proxy on the SWG appliance?

A. The SWG solution supports explicit and transparent proxy modes. In explicit proxy mode, the clients must specify an IP address and a port in their browsers, unless the organization pushes the setting onto the client's device. This address is the IP address of a proxy server that is configured on the SWG appliance. Transparent proxy, as the name implies, is transparent to the client. The SWG appliance is configured in an inline deployment, and the appliance transparently accepts all HTTP and HTTPS traffic.

Q. Does Citrix SWG have a configuration wizard?

A. Yes. The wizard is located on the SWG node in the configuration utility.

Q. Which Citrix ADC features are used when configuring Citrix SWG?

A. Responder, AAA-TM, content switching, SSL, forward proxy, SSL interception, and URL filtering.

Q. What authentication methods are supported on Citrix SWG?

A. In the explicit proxy mode, LDAP, RADIUS, TACACS+, and NEGOTIATE authentication methods are supported. In transparent mode, only LDAP authentication is supported.

Q. Is it necessary to install the CA Certificate on the client device?

A. Yes. The Citrix SWG appliance emulates the origin server certificate. This server certificate must be signed by a trusted CA certificate, which must be installed on the clients' devices so that the client can trust the regenerated server certificate.

Q. Can I use a Citrix ADC Platform license on the Citrix SWG platform?

A. No. The Citrix SWG platform requires its own platform license.

Q. Is HA supported for a Citrix Secure Web Gateway deployment?

A. Yes.

Q. Which file contains the logs for Citrix SWG?

A. The ns.log file records Citrix SWG information. You must enable logging by using the CLI or GUI. At the command prompt, type: **set syslogparams -ssli Enabled**.

In the GUI, navigate to **System > Auditing**. In **Settings**, click **Change Auditing Syslog Settings**. Select **SSL Interception**.

Q. Which nsconmsg commands can I use to troubleshoot issues?

A. You can use one or both of the following commands:

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

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

Q. If the certificate bundle is built-in, how do I get updates?

A. The latest bundle is included in the build. For updates, contact Citrix Support.

Q. Can data be captured on Citrix ADM from Citrix SWG?

A. Yes. You must enable **Analytics** in the Secure Web Gateway wizard.

Important: Ensure that you are using the same 12.0 build for MAS and SWG.

Q. What is URL Filtering Service?

A. URL Filtering is a web content filter that controls access to a list of restricted websites and web pages. The filter restricts user access to inappropriate content on the internet based on URL category, category groups, and reputation score. A network administrator can monitor the web traffic and block

user access to highly risky websites. You can implement the feature by either using URL Categorization or URL List feature based on policy enforcement. For more information, see [URL Filtering](#) topic.

Q. How does URL Filtering fit into Citrix SWG?

A. URL Filtering leverages with Citrix SWG appliance to control access to specific websites. The SWG appliance at the edge of the network acts as a proxy to intercept the web traffic and perform actions such as authentication, inspection, caching, and redirection. The filter then controls access to websites using URL Categorization or URL List feature with policy enforcement.

Q. How often is the URL Categorization database updated?

A. If you are using URL Categorization feature to control access to restricted websites, you must periodically update the categorization database with the latest data from cloud-based vendor service. To update the database, the Citrix SWG GUI enables you to configure the URL filtering parameters such as Hours Between DB Updates” or “Time of Day to Update DB.

Q. What use-cases are a best fit for URL Filtering service today?

A. Following are some of the targeted use cases for enterprise customers:

- [URL Filtering by URL Reputation Score](#)
- [Internet Usage Control under Corporate Compliance for Enterprises](#)
- [URL Filtering by Using Custom URL List](#)

Q. Is there a memory limit for caching in URL Categorization service?

A. Yes. The memory limit for caching is set as 10 GB and you can configure it through the CLI interface only.

Q. What does the URL Categorization database return if no category matches the incoming request?

A. If the incoming request does not match a category or if the URL is malformed, the appliance marks the URL as “Uncategorized” and sends the request to the cloud-based service maintained by the categorization vendor. The appliance continues to monitor the cloud query feedback and updates the cache so that future requests can benefit from the cloud lookup.

Q. What is a URL reputation score and how do you control access to malicious websites based on the reputation score?

A. A URL reputation score is a rating that Citrix SWG assigns to a website. The value can range from 1 to 4, where 4 is a malicious web site and 1 is a clean website. If a network administrator monitors a user accessing highly risky web sites, then access to such sites is controlled based on the URL reputation score and security level you have configured on the Citrix SWG appliance. For more information, see [URL Reputation Score](#).

Q. If you filter websites using a URL Set but incorrectly filter a specific website, what is the process to enable exceptional websites?

A. URL Filtering uses a responder policy to control access to web sites. To whitelist a specific URL as an exception, in the SWG wizard, create a patset policy and add the exceptional URL with “allow” action. Once you create the policy, exit the wizard and do the following steps:

To change the priority of a policy expression by using the Citrix SWG GUI:

1. Log on to the **Citrix SWG** appliance and navigate to **Secure Web Gateway > Proxy Virtual Servers**.
2. In the details page, select a server and click **Edit**.
3. In the **Proxy Virtual Servers** page, go to **Policies** section and click the pencil icon to edit the details.
4. Select the patset policy and in **Policy Binding** page, specify the priority value lower than other bound policies.
5. Click **Bind** and **Done**.

Q. What are the key benefits of using Citrix SWG URL Filtering feature?

A. URL Filtering feature is easy to deploy, configure, and use. It provides the following benefits and allows enterprise customers to:

- Monitor web traffic and user transaction
- Filter malware and Internet-borne security threats.
- Control unauthorized access to malicious websites.
- Enforce corporate security policies to control access to restricted data.

Q. If you are using a URL List feature to filter websites, how to edit a URL list policy?

A. You can modify a URL List policy through the Citrix SWG Wizard by overwriting or deleting the imported list bound to the responder policy.

Q. What does the metadata associated to a URL contain?

A. Each URL in the categorization database has a metadata associated to it. The metadata contains an URL category, category group, and reputation score information. For example, if the URL is a shopping portal, the metadata will be Shopping, Shopping/Retail, and 1 respectively.

Use the following expressions to get these values for the incoming URL. The expressions are given below:

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

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

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

Q. What type of license and subscription you need for URL Categorization feature?

A. URL Categorization feature requires an URL Threat Intelligence subscription service (available for one year or three years) with Citrix SWG edition.

Q. What are the ways I can configure URL Filtering?

A. There are two ways of configuring URL Filtering. You can either do it through the Citrix SWG command interface or through the Citrix SWG Wizard. Citrix recommends that you use the wizard to configure filtering policies.

Q. What are the types of URL categories that you can block?

A. The URL Categorization database contains millions of URLs with metadata. The administrator can configure a responder policy to decide which URL categories can be blocked and which URL categories can be allowed for user access. For information about the URL category mapping, see [Mapping categories](#) page.

Q. What must we do if we are unable to access Origin servers that use WebSocket, such as [whatsapp](#)

You must enable webSocket in the default HTTP profile.

At the CLI, type:

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

What is ICAP?

ICAP stands for Internet Content Adaption Protocol.

Which version of Citrix SWG supports ICAP?

ICAP is supported in Citrix SWG release 12.0 build 57.x and later.

What are the two ICAP modes supported on Citrix SWG?

Request modification (**REQMOD**) mode and response modification (**RESPMOD**) mode are supported.

What is the default port for ICAP?

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).
