Citrix Secure Web Gateway 12.1

Machine translated content

Disclaimer

Die offizielle Version dieses Inhalts ist auf Englisch. Für den einfachen Einstieg wird Teil des Inhalts der Cloud Software Group Dokumentation maschinell übersetzt. Cloud Software Group hat keine Kontrolle über maschinell übersetzte Inhalte, die Fehler, Ungenauigkeiten oder eine ungeeignete Sprache enthalten können. Es wird keine Garantie, weder ausdrücklich noch stillschweigend, für die Genauigkeit, Zuverlässigkeit, Eignung oder Richtigkeit von Übersetzungen aus dem englischen Original in eine andere Sprache oder für die Konformität Ihres Cloud Software Group Produkts oder Ihres Diensts mit maschinell übersetzten Inhalten gegeben, und jegliche Garantie, die im Rahmen der anwendbaren Endbenutzer-Lizenzvereinbarung oder der Vertragsbedingungen oder einer anderen Vereinbarung mit Cloud Software Group gegeben wird, dass das Produkt oder den Dienst mit der Dokumentation übereinstimmt, gilt nicht in dem Umfang, in dem diese Dokumentation maschinell übersetzt wurde. Cloud Software Group kann nicht für Schäden oder Probleme verantwortlich gemacht werden, die durch die Verwendung maschinell übersetzter Inhalte entstehen können.

Contents

Versionshinweise 3

Unterstützte Hardware- und Softwareplattformen 3

Lizenzierungsanforderung 4

Installation 10

Erste Schritte mit einer Citrix ADC MPX- und VPX-SWG-Appliance 10

Erste Schritte mit einer SWG-Instanz auf einer Citrix ADC SDX-Appliance 14

Proxy-Modi 14

SSL-Interception 17

SSL-Profil 18

SSL-Richtlinieninfrastruktur für SSL-Interception 27

Zertifikatspeicher für SSL-Interception 31

SSL-Fehler beim automatischen Lernen 35

Benutzeridentitätsverwaltung 37

URL-Filterung 42

URL-Liste 44

URL-Muster-Semantik 51

Zuordnungs-URL-Kategorien 52

Anwendungsfall: URL-Filterung mithilfe benutzerdefinierter URL-Sets 52

URL-Kategorisierung 55

Sicherheitskonfiguration 68

URL-Reputationsbewertung 68

Verwenden von ICAP für die Remote-Content-Inspektion 70

Integration mit IPS oder NGFW als Inline-Geräte 82

Analytics **131**

Anwendungsfall: Konformität und Sicherheit des Internetzugangs im Unternehmen **132**

Anwendungsfall: Sicherung des Unternehmensnetzwerks durch Verwendung von ICAP für die Remote-Malware-Inspektion **148**

Anleitungsartikel **161**

Erstellen einer URL-Kategorisierungsrichtlinie **162**

Erstellen einer URL-Listenrichtlinie **164**

Wie man eine außergewöhnliche URL auf die Positivliste setzt **167**

So blockieren Sie die Website der Erwachsenenkategorie **168**

System **171**

Netzwerke **171**

AppExpert **172**

SSL **173**

FAQ **174**

Versionshinweise

July 1, 2019

Die Versionshinweise für Citrix Secure Web Gateway-Produkt werden in den Haupt-Versionshinweisen für eine Citrix ADC-Appliance erfasst. Siehe Citrix ADC —Versionshinweise.

Unterstützte Hardware- und Softwareplattformen

April 26, 2021

Die Citrix Secure Web Gateway (SWG) -Appliance ist derzeit als Hardware-Appliance und als virtuelle Appliance verfügbar. Ausführliche Spezifikationen finden Sie im Datenblatt unter www.citrix.com. Bewegen Sie den Mauszeiger über **Produkte**, und wählen Sie in der Liste **NetzwerkCitrix Secure Web Gateway**aus.

Stellen Sie vor der Installation Ihrer SWG-Appliance sicher, dass Sie über die richtige (n) Lizenz (n) verfügen. Jede Appliance in einem Hochverfügbarkeits-Setup erfordert eine eigene Lizenz. Hinweise zu den Lizenzen finden Sie unterLizenzanforderungen. Informationen zur Hochverfügbarkeit finden Sie unter Einführung in die hohe Verfügbarkeit.

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

Virtuelle Appliance (VPX)

- Citrix SWG VPX 200
- Citrix SWG VPX 1000
- Citrix SWG VPX3000
- Citrix SWG VPX 5000
- Citrix SWG VPX 8000
- Citrix SWG VPX 10G
- Citrix SWG VPX 15G
- Citrix SWG VPX 25G

Hardware-Appliance (SDX)

SWG-Instanzen können auf jeder SDX-Plattform bereitgestellt werden, indem die Lizenz SDX 2-Instance Add-On Pack for Secure Web Gateway installiert wird. Mit einer Lizenzinstallation können Sie zwei SWG-Instanzen auf einer SDX-Appliance bereitstellen. Sie können mehr SWG-Instanzen auf Ihrer Appliance bereitstellen, indem Sie weitere Lizenzen hinzufügen. Weitere Hinweise zum Bereitstellen einer Citrix SWG-Instanz finden Sie unter Provisioning von Citrix ADC-Instanzen.

Lizenzierungsanforderung

April 26, 2021

Mit einer Lizenz erhalten Sie Zugriff auf eine Reihe von Features auf einer Citrix Secure Web Gateway (SWG) -Appliance.

Mit dem Citrix Lizenzierungsframework können Sie sich darauf konzentrieren, den maximalen Nutzen aus Citrix Produkten zu erzielen. Die Zuteilung Ihrer Lizenzen ist sehr einfach. Im SWG-Konfigurationsdienstprogramm (GUI) können Sie Ihre Lizenzen mit der Hardwareseriennummer (HSN) oder des Lizenzaktivierungscodes (LAC) zuweisen. Wenn auf Ihrem lokalen Computer bereits eine Lizenz vorhanden ist, können Sie sie auf die Appliance hochladen.

Für alle anderen Funktionen, z. B. die Rückgabe oder Neuzuweisung Ihrer Lizenz, müssen Sie das Lizenzportal verwenden (das Sie auch für die erste Lizenzzuweisung verwenden können). Weitere Informationen über das Lizenzierungsportal finden Sie unter http://support.citrix.com/article/CTX131110.

Sie können Lizenzen nach Bedarf für Ihre Bereitstellung teilweise zuweisen. Wenn Ihre Lizenzdatei z. B. zehn Lizenzen enthält, Ihre aktuelle Anforderung jedoch nur für sechs Lizenzen gilt, können Sie jetzt sechs Lizenzen zuweisen und später weitere Lizenzen zuweisen. Sie können nicht mehr als die Gesamtzahl der Lizenzen in Ihrer Lizenzdatei zuweisen.

Bevor Sie Ihre SWG-Appliance verwenden, sollten Sie die folgenden Lizenzen entweder über die GUI oder die CLI installieren:

- **Citrix Secure Web Gateway-Lizenz**
  - Die Citrix SWG-Plattformlizenz ist die Mindestvoraussetzung für die Verwendung Ihrer MPX SWG-Appliance und für die Bereitstellung Ihrer VPX-Instanz auf verschiedenen Hypervisoren wie XenServer, VMware ESX, Microsoft Hyper-V und Linux-KVM.
  - Für SDX-Plattformen ist mindestens eine SDX 10K Concurrent Sessions SWG Add-on Pack-Lizenz erforderlich, um eine Citrix SWG-Instanz auf einer Citrix ADC SDX-Appliance bereitzustellen.

- **URL Threat Intelligence-Feature-Lizenz**. Diese Lizenz ist für die Verwendung der URL-Filter, URL-Kategorisierung und URL-Reputationsbewertung erforderlich.

Voraussetzungen

So verwenden Sie die Hardwareseriennummer oder den Lizenzaktivierungscode, um Ihre Lizenzen zuzuweisen:

- Sie müssen über die Appliance auf öffentliche Domänen zugreifen können. Beispielsweise sollte die Appliance Zugriff habenwww.citrix.com. Die Lizenzzuweisungssoftware greift intern auf das Citrix Lizenzportal für Ihre Lizenz zu. Um auf eine öffentliche Domäne zuzugreifen, können Sie entweder einen Proxyserver verwenden oder einen DNS-Server einrichten und auf Ihrer Citrix ADC-Appliance eine NSIP-Adresse oder eine Subnetz-IP-Adresse (SNIP) konfigurieren.
- Ihre Lizenz muss mit Ihrer Hardware verknüpft sein, oder Sie müssen über einen gültigen Lizenzaktivierungscode (LAC) verfügen. Citrix sendet Ihren LAC per E-Mail, wenn Sie eine Lizenz erwerben.

Lizenzen für Appliances in Hochverfügbarkeits-Setup

Sie müssen eine separate Lizenz für jede Appliance in einem Hochverfügbarkeitspaar erwerben. Stellen Sie sicher, dass der gleiche Lizenztyp auf beiden Appliances installiert ist.

Auf einer Citrix ADC SDX-Appliance können Sie ein Hochverfügbarkeits-Setup (HA) zwischen zwei SWG-Instanzen auf derselben Appliance konfigurieren. Citrix empfiehlt jedoch, ein HA-Setup zwischen zwei SWG-Instanzen auf verschiedenen Citrix ADC SDX-Appliances zu konfigurieren.

Zuweisen und Installieren Ihrer Lizenzen

Sie können Ihre Lizenzen mit der GUI zuweisen und installieren. Wenn Sie Ihre Lizenzen mit der CLI installieren, müssen Sie die Lizenzen in das Verzeichnis /nsconfig/license/ kopieren.

Zuweisen von Lizenzen mit der Citrix SWG-GUI

1. Geben Sie in einem Webbrowser die IP-Adresse der Citrix SWG-Appliance ein.
2. Geben Sie im Feld **User Name** und **Password** die Administratoranmeldeinformationen ein.
3. Navigieren Sie auf der Registerkarte **Konfiguration** zu **System** > **Lizenzen**.
4. Klicken Sie im Detailbereich auf **Lizenzen verwalten**, klicken Sie auf **Neue Lizenz hinzufügen**, und wählen Sie dann eine der folgenden Optionen aus:

- **Seriennummer verwenden**. Die Software ruft intern die Seriennummer Ihrer Appliance ab und verwendet diese Nummer, um Ihre Lizenz (en) anzuzeigen.
- **Verwenden Sie den Lizenzaktivierungscode**. Citrix sendet eine E-Mail an den Lizenzaktivierungscode (LAC) für die erworbene Lizenz. Geben Sie die LAC in das Textfeld ein.

Wenn Sie keine Internetverbindung auf der Citrix ADC-Appliance konfigurieren möchten, können Sie einen Proxyserver verwenden. Wählen Sie Über Proxy-Server verbinden aus, und geben Sie die IP-Adresse und den Port Ihres Proxy-Servers an.

5. Klicken Sie auf **Get Licenses**.
6. Wählen Sie die Lizenzdatei aus, die Sie zum Zuweisen Ihrer Lizenzen verwenden möchten.
7. Geben Sie in der Spalte **Zuweisen** die Anzahl der zu zuweisenden Lizenzen ein. Klicken Sie dann auf **Abrufen**.
8. Klicken Sie auf **Neu starten**, damit die Lizenz wirksam wird.
9. Klicken Sie im Dialogfeld **Neustart** auf **OK**.

Installieren Sie Ihre Lizenzen mit der Citrix SWG-GUI

1. Geben Sie in einem Webbrowser die IP-Adresse der Citrix SWG-Appliance ein (z. B. `http://192.168.100.1`).
2. Geben Sie im Feld **User Name** und **Password** die Administratoranmeldeinformationen ein.
3. Navigieren Sie auf der Registerkarte **Konfiguration** zu **System** > **Lizenzen**.
4. Klicken Sie im Detailbereich auf **Lizenzen verwalten**.
5. Klicken Sie auf **Neue Lizenz hinzufügen**, und wählen Sie **Lizenzdateien hochladen**aus.
6. Klicken Sie auf **Durchsuchen**. Navigieren Sie zum Speicherort der Lizenzdateien, wählen Sie die Lizenzdatei aus, und klicken Sie dann auf **Öffnen**.
7. Klicken Sie auf **Neu starten**, um die Lizenz anzuwenden.
8. Klicken Sie im Dialogfeld **Neustart** auf **OK**.

Installieren Sie Ihre Lizenzen mit der Citrix SWG CLI

1. Öffnen Sie eine SSH-Verbindung mit der Citrix SWG-Appliance mithilfe eines SSH-Clients, z. B. PuTTY.
2. Melden Sie sich mit den Administratoranmeldeinformationen bei der Appliance an.

3. Wechseln Sie zur Shell-Eingabeaufforderung, und kopieren Sie die neue Lizenzdatei (en) in das Lizenzunterverzeichnis des Verzeichnisses nsconfig. Wenn das Unterverzeichnis nicht vorhanden ist, erstellen Sie es, bevor Sie die Datei (en) kopieren.

Beispiel:

```
    login: nsroot

    Password: nsroot

    Last login: Mon Aug  4 03:37:27 2008 from 10.102.29.9

    Done

    > shell

    Last login: Mon Aug  4 03:51:42 from 10.103.25.64

    root@ns# mkdir /nsconfig/license

    root@ns# cd /nsconfig/license
<!--NeedCopy-->
```

Kopieren Sie die neue Lizenzdatei (en) in dieses Verzeichnis.

> **Hinweis**
>
> Die Befehlszeilenschnittstelle fordert Sie nicht auf, die Appliance neu zu starten, um die Lizenzen zu aktivieren. Führen Sie den Befehl **reboot -w** aus, um das System neu zu starten, oder führen Sie den Befehl **reboot** aus, um das System normal neu zu starten.

Überprüfen Sie die lizenzierten Funktionen

Stellen Sie vor der Verwendung einer Funktion sicher, dass Ihre Lizenz die Funktion unterstützt.

Überprüfen der lizenzierten Funktionen mit der Citrix SWG-GUI

1. Geben Sie in einem Webbrowser die IP-Adresse der Citrix SWG-Appliance ein (z. B.`http://192.168.100.1`).
2. Geben Sie im Feld **User Name** und **Password** die Administratoranmeldeinformationen ein.
3. Navigieren Sie zu **System** > **Lizenzen** .
   Der Bildschirm hat ein grünes Häkchen neben jedem lizenzierten Feature.

Überprüfen der lizenzierten Funktionen mit der Citrix SWG CLI

1. Öffnen Sie eine SSH-Verbindung mit der Citrix SWG-Appliance mithilfe eines SSH-Clients, z. B. PuTTY.
2. Melden Sie sich mit den Administratoranmeldeinformationen bei der Appliance an.
3. Geben Sie an der Eingabeaufforderung den Befehl sh ns license ein, um die von der Lizenz unterstützten Funktionen anzuzeigen.

Beispiel:

```
> sh Lizenz

        License status:

                            Web Logging: NO

                       Surge Protection: NO

                         Load Balancing: YES

              ...

            Forward Proxy: YES

                       SSL Interception: YES

                        Model Number ID: 25000

                         Licensing mode: Local

 Fertig
```

Aktivieren oder Deaktivieren einer Funktion

Wenn Sie die Citrix Secure Web Gateway-Appliance zum ersten Mal verwenden, müssen Sie ein Feature aktivieren, bevor Sie es verwenden können. Wenn Sie ein Feature vor der Aktivierung konfigurieren, wird eine Warnmeldung angezeigt. Die Konfiguration wird gespeichert, sie wird jedoch erst angewendet, wenn das Feature aktiviert ist.

Aktivieren einer Funktion mit der Citrix SWG-GUI

1. Geben Sie in einem Webbrowser die IP-Adresse der Citrix SWG-Appliance ein (z. B.`http://192.168.100.1`).
2. Geben Sie im Feld **User Name** und **Password** die Administratoranmeldeinformationen ein.
3. Navigieren Sie zu **System** > **Einstellungen** > **Erweiterte Funktionen konfigurieren**.

4. Wählen Sie die Features aus (z. B. Forward-Proxy, SSL-Interception und URL-Filterung), die Sie aktivieren möchten.

Aktivieren einer Funktion mit der Citrix SWG CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um ein Feature zu aktivieren und die Konfiguration zu überprüfen:

```
enable feature <FeatureName>
```

```
show feature
```

Das folgende Beispiel zeigt, wie die SSL-Interception-, Forward-Proxy- und URL-Filterfunktionen aktiviert werden.

```
> enable feature forwardProxy sslinterception urlfiltering

 Done

 >show feature

    Feature                        Acronym              Status

        -------                        -------              ------

 1)     Web Logging                    WL                   OFF

 2)     Surge Protection               SP                   OFF

...

...

36)    URL Filtering                  URLFiltering         ON

37)    Video Optimization             VideoOptimization    OFF

38)    Forward Proxy                  ForwardProxy         ON

39)    SSL Interception               SSLInterception      ON

Done
<!--NeedCopy-->
```

> **Hinweis**
>
> Wenn der Lizenzschlüssel für ein Feature nicht verfügbar ist, wird für dieses Feature die folgende Fehlermeldung angezeigt:
>
> ERROR: feature(s) not licensed

Installation

April 26, 2021

Eine Citrix Secure Web Gateway (SWG) -Appliance muss ordnungsgemäß installiert und für das Internet zugänglich sein, bevor Sie mit der Konfiguration für die Sicherung Ihres Unternehmens beginnen können.

Informationen zur Installation und Erstkonfiguration der Hardware-Appliance finden Sie unterEinrichten der SWG-Hardware.

Eine virtuelle Citrix SWG-Appliance (VPX) wird auf verschiedenen Virtualisierungsplattformen unterstützt.

Informationen zu den unterstützten Hypervisoren und Anweisungen zum Bereitstellen einer VPX-Appliance finden Sie unterBereitstellen einer Citrix ADC VPX- Instanz.

Erste Schritte mit einer Citrix ADC MPX- und VPX-SWG-Appliance

April 26, 2021

Nachdem Sie Ihre Hardware (MPX) oder Software (VPX) -Appliance installiert und die Erstkonfiguration durchgeführt haben, können Sie sie als sichere Web-Gateway-Appliance konfigurieren, um Datenverkehr zu empfangen.

WICHTIG:

- OCSP-Prüfung erfordert eine Internetverbindung, um die Gültigkeit von Zertifikaten zu überprüfen. Wenn die Appliance über die NSIP-Adresse nicht über das Internet zugegriffen werden kann, fügen Sie Zugriffssteuerungslisten (ACLs) hinzu, um NAT von der NSIP-Adresse zur Subnetz-IP-Adresse (SNIP) auszuführen. Das SNIP muss über das Internet zugänglich sein. Zum Beispiel:

```
add ns acl a1 ALLOW -srcIP = <NSIP> -destIP "!="
   10.0.0.0-10.255.255.255

set rnat a1 -natIP <SNIP>

apply acls
<!--NeedCopy-->
```

- Geben Sie einen DNS-Namensserver an, um Domänennamen aufzulösen. Weitere Informationen finden Sie unter Erstmalige Konfiguration.

- Stellen Sie sicher, dass das Datum auf der Appliance mit den NTP-Servern synchronisiert ist. Wenn das Datum nicht synchronisiert wird, kann die Appliance nicht effektiv überprüfen, ob es sich bei einem Ursprungsserverzertifikat um ein abgelaufenes Zertifikat handelt.

Um die Citrix SWG-Appliance zu verwenden, müssen Sie die folgenden Aufgaben ausführen:

- Fügen Sie einen Proxyserver im expliziten oder transparenten Modus hinzu.
- Aktivieren Sie SSL-Interception.
  - Konfigurieren Sie ein SSL-Profil.
  - Fügen Sie SSL-Richtlinien hinzu und binden Sie sie an den Proxyserver.
  - Fügen Sie ein Zertifizierungsstellen-Zertifikatschlüsselpaar für SSL-Interception hinzu und binden Sie sie.

Hinweis: Eine Citrix SWG-Appliance, die im transparenten Proxymodus konfiguriert ist, kann nur HTTP- und HTTPS-Protokolle abfangen. Um andere Protokolle wie Telnet zu umgehen, müssen Sie die folgende Abhörrichtlinie auf dem virtuellen Proxyserver hinzufügen.

Der virtuelle Server akzeptiert jetzt nur den eingehenden HTTP- und HTTPS-Datenverkehr.

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

Je nach Bereitstellung müssen Sie möglicherweise die folgenden Funktionen konfigurieren:

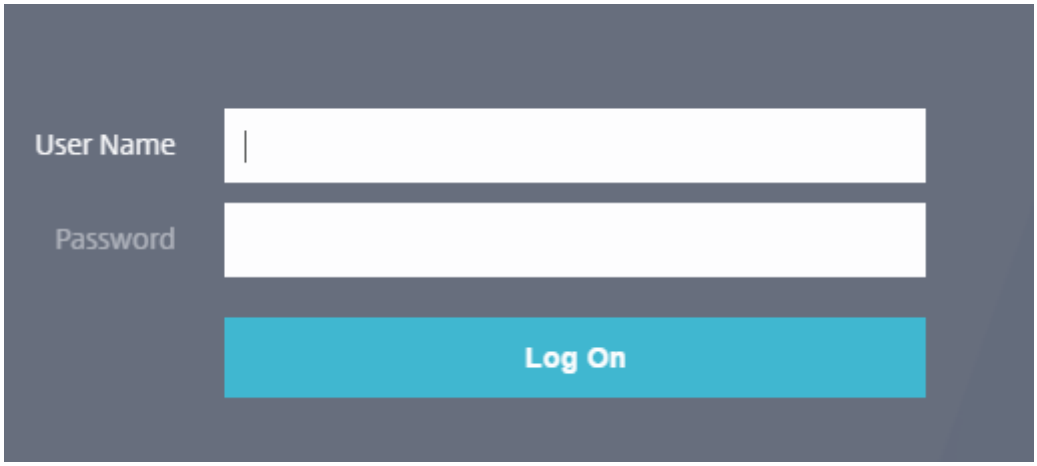
- Authentifizierungsdienst (empfohlen) —zur Authentifizierung von Benutzern. Ohne den Authentifizierungsdienst basiert die Benutzeraktivität auf der Client-IP-Adresse.
- URL-Filter —zum Filtern von URLs nach Kategorien, Reputationsbewertung und URL-Listen.
- Analytics: Zum Anzeigen von Benutzeraktivitäten, Benutzerrisikoindikatoren, Bandbreitenverbrauch und Transaktionen in Citrix Application Delivery Management (ADM).

Hinweis: SWG implementiert die meisten typischen HTTP- und HTTPS-Standards, gefolgt von ähnlichen Produkten. Diese Implementierung wird ohne einen bestimmten Browser durchgeführt und ist mit den meisten gängigen Browsern kompatibel. SWG wurde mit gängigen Browsern und aktuellen Versionen von Google Chrome, Internet Explorer und Mozilla Firefox getestet.

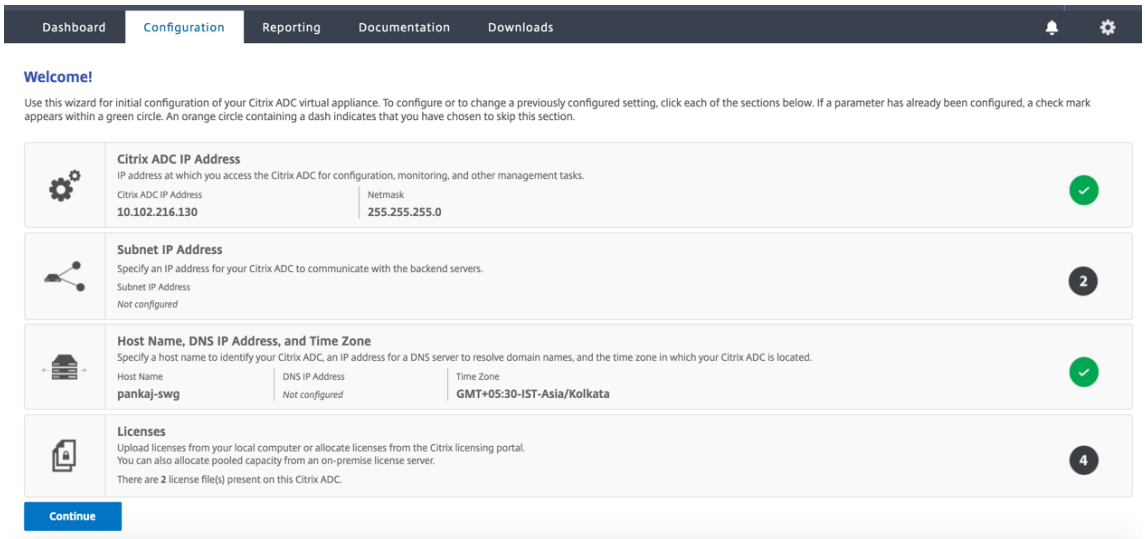
Secure Web Gateway-Assistent

Der SWG-Assistent stellt Administratoren ein Tool zur Verfügung, mit dem Sie die gesamte SWG-Bereitstellung mithilfe eines Webbrowsers verwalten können. Es hilft den Kunden dabei, einen SWG-Service schnell einzurichten und vereinfacht die Konfiguration durch eine Reihe von klar definierten Schritten.

1. Öffnen Sie Ihren Webbrowser und geben Sie die NSIP-Adresse ein, die Sie bei der Erstkonfiguration angegeben haben. Weitere Hinweise zur Erstkonfiguration finden Sie unterErstmalige Konfiguration.
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.

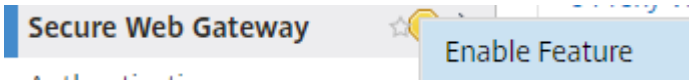


3. Wenn Sie keine Subnetz-IP-Adresse (SNIP) angegeben haben, wird der folgende Bildschirm angezeigt.



   Geben Sie unter Subnetz-IP-Adresse eine IP-Adresse und eine Subnetzmaske ein. Das Häkchen in einem grünen Kreis zeigt an, dass der Wert konfiguriert ist.
4. Fügen Sie **unter Hostname**, **DNS-IP-Adresse und Zeitzone**die IP-Adresse eines DNS-Servers hinzu, um Domänennamen aufzulösen, und geben Sie Ihre Zeitzone an.
5. Klicken Sie auf **Weiter**.
6. (Optional) Möglicherweise wird ein Ausrufezeichen wie folgt angezeigt:

Diese Markierung zeigt an, dass das Feature nicht aktiviert ist. Um das Feature zu aktivieren, klicken Sie mit der rechten Maustaste auf das Feature, und klicken Sie dann auf **Feature aktivieren**.



7. Klicken Sie im Navigationsbereich auf **Secure Web Gateway**. Klicken Sie unter **Erste Schritte**auf **Secure Web Gateway-Assistent**.

8. Führen Sie die Schritte im Assistenten aus, um Ihre Bereitstellung zu konfigurieren.

Hinzufügen einer Listenrichtlinie zum transparenten Proxyserver

1. Navigieren Sie zu **Secure Web Gateway** > **Proxyserver**. Wählen Sie den transparenten Proxyserver aus, und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie die **Grundeinstellungen**, und klicken Sie auf **Mehr**.
3. Geben Sie unter **Listenpriorität** 1 ein.
4. Geben Sie unter **Listen-Richtlinienausdruck** den folgenden Ausdruck ein:

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

Dieser Ausdruck setzt Standardports für HTTP- und HTTPS-Datenverkehr voraus. Wenn Sie verschiedene Ports konfiguriert haben, z. B. 8080 für HTTP oder 8443 für HTTPS, ändern Sie den Ausdruck so, dass er diese Ports widerspiegelt.

Einschränkungen

SWG wird in einem Cluster-Setup, in Administratorpartitionen und auf einer Citrix ADC FIPS-Appliance nicht unterstützt.

Erste Schritte mit einer SWG-Instanz auf einer Citrix ADC SDX-Appliance

July 16, 2019

Die Citrix ADC SDX-Appliance ist eine Multimandantenplattform, auf der Sie mehrere virtuelle Citrix ADC-Instanzen bereitstellen und verwalten können. Die SDX-Appliance erfüllt Cloudcomputing- und Mehrmandantenanforderungen, indem sie einem einzelnen Administrator ermöglicht, die Appliance zu konfigurieren und zu verwalten und die Verwaltung jeder gehosteten Instanz an Mandanten zu delegieren. Die SDX-Appliance ermöglicht es dem Appliance-Administrator, jedem Mandanten die folgenden Vorteile zu bieten. Sie sind unten angegeben:

- Eine vollständige Instanz. Jede Instanz verfügt über die folgenden Berechtigungen:
  - Dedizierte CPU- und Speicherressourcen
  - Ein separater Raum für Entitäten
  - Die Unabhängigkeit, die Veröffentlichung und den Aufbau ihrer Wahl auszuführen
  - Lebenszyklusunabhängigkeit
- Ein vollständig isoliertes Netzwerk. Datenverkehr, der für eine bestimmte Instanz bestimmt ist, wird nur an diese Instanz gesendet.

Wenn Sie Ihre Citrix ADC SDX-Appliance noch nicht installiert haben, finden Sie weitere InformationenHardwareinstallationzur Installation der Appliance.

Sie müssen den Verwaltungsdienst verwenden, um die Erstkonfiguration der Citrix ADC SDX-Appliance durchzuführen. Weitere Informationen finden Sie unter Erste Schritte mit der Benutzeroberfläche des Management Service.

Sie können Citrix SWG-Instanzen auf der Citrix ADC SDX-Appliance genauso bereitstellen wie eine Citrix ADC VPX-Instanz. Um eine SWG-Instanz auf einer SDX-Appliance bereitzustellen, müssen Sie eine SDX - 10K Concurrent Sessions SWG add-on Pack -Lizenz installieren. Diese Lizenz ähnelt den SDX-Instance-Packs für VPX, ist jedoch exklusiv für SWG-Instanzen. Weitere Hinweise zum Bereitstellen von Citrix ADC-Instanzen finden Sie unterProvisioning von Citrix ADC-Instanzen.

Folgen Sie den Anweisungen unter, um die Citrix SWG-Instanz für den Datenverkehr zu konfigurierenErste Schritte mit einer Citrix SWG-Appliance.

Proxy-Modi

April 26, 2021

Die Citrix Secure Web Gateway (SWG) -Appliance fungiert als Client-Proxy, um eine Verbindung mit dem Internet und SaaS-Anwendungen herzustellen. Als Proxy akzeptiert es den gesamten Datenverkehr und bestimmt das Protokoll des Datenverkehrs. Sofern der Datenverkehr nicht HTTP oder SSL ist, wird er so wie er ist an das Ziel weitergeleitet. Wenn die Appliance eine Anforderung von einem Client empfängt, fängt sie die Anforderung ab und führt einige Aktionen aus, z. B. Benutzerauthentifizierung, Sitekategorisierung und Umleitung. Es verwendet Richtlinien, um zu bestimmen, welcher Datenverkehr zugelassen und welcher Datenverkehr gesperrt werden soll.

Die Appliance verwaltet zwei verschiedene Sitzungen, eine zwischen dem Client und dem Proxy und die andere zwischen dem Proxy und dem Ursprungsserver. Der Proxy stützt sich auf kundendefinierte Richtlinien, um HTTP- und HTTPS-Datenverkehr zuzulassen oder zu blockieren. Daher ist es wichtig, dass Sie Richtlinien definieren, um vertrauliche Daten, z. B. Finanzinformationen, zu umgehen. Die Appliance bietet eine Reihe von Layer-4-zu-Layer-7-Datenverkehrsattributen und Benutzeridentitätsattributen zum Erstellen von Datenverkehrsmanagementrichtlinien.

Bei SSL-Datenverkehr überprüft der Proxy das Zertifikat des Ursprungsservers und stellt eine legitime Verbindung mit dem Server her. Anschließend emuliert er das Serverzertifikat, signiert es mit einem auf Citrix SWG installierten Zertifizierungsstellenzertifikat und präsentiert das erstellte Serverzertifikat dem Client. Sie müssen das Zertifizierungsstellenzertifikat als vertrauenswürdiges Zertifikat zum Browser des Clients hinzufügen, damit die SSL-Sitzung erfolgreich eingerichtet wird.

Die Appliance unterstützt transparente und explizite Proxy-Modi. Im expliziten Proxymodus muss der Client eine IP-Adresse in seinem Browser angeben, es sei denn, die Organisation verschiebt die Einstellung auf das Gerät des Clients. Diese Adresse ist die IP-Adresse eines Proxy-Servers, der auf der SWG-Appliance konfiguriert ist. Alle Client-Anfragen werden an diese IP-Adresse gesendet. Für einen expliziten Proxy müssen Sie einen virtuellen Content Switching-Server vom Typ PROXY konfigurieren und eine IP-Adresse und eine gültige Portnummer angeben.

Transparenter Proxy ist, wie der Name schon sagt, für den Client transparent. Das heißt, die Clients wissen möglicherweise nicht, dass ein Proxyserver ihre Anforderungen vermittelt. Die SWG-Appliance ist in einer Inline-Bereitstellung konfiguriert und akzeptiert transparent den gesamten HTTP- und HTTPS-Datenverkehr. Für transparenten Proxy müssen Sie einen virtuellen Content Switching-Server vom Typ PROXY mit Sternchen (* *) als IP-Adresse und Port konfigurieren. Wenn Sie den Secure Web Gateway-Assistenten in der GUI verwenden, müssen Sie keine IP-Adresse und keinen Port angeben.

> **Hinweis**
>
> Wenn Sie andere Protokolle als HTTP und HTTPS im transparenten Proxymodus abfangen möchten, müssen Sie eine Abhörrichtlinie hinzufügen und an den Proxyserver binden.

Konfigurieren von SSL-Forward-Proxy mit der Citrix SWG-CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


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

Argumente:

Nome:

Name für den Proxyserver. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem der virtuelle CS Server erstellt wurde.

Die folgende Anforderung gilt nur für die CLI:

Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “mein Server”oder “mein Server”).

Dies ist ein obligatorisches Argument. Maximale Länge: 127

IPAddress:

IP-Adresse des Proxyservers.

port:

Portnummer für Proxy-Server. Mindestwert: 1

Beispiel für expliziten Proxy:

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

Beispiel für transparenten Proxy:

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

Hinzufügen einer Abhörrichtlinie zum transparenten Proxyserver mit der Citrix SWG-GUI

1. Navigieren Sie zu **Secure Web Gateway** > **Proxyserver**. Wählen Sie den transparenten Proxyserver aus, und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie die **Grundeinstellungen**, und klicken Sie auf **Mehr**.
3. Geben Sie unter **Listenpriorität** 1 ein.
4. Geben Sie unter **Listen-Richtlinienausdruck** den folgenden Ausdruck ein:

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


> **Hinweis**
>
> Dieser Ausdruck setzt Standardports für HTTP- und HTTPS-Datenverkehr voraus. Wenn Sie verschiedene Ports konfiguriert haben, z. B. 8080 für HTTP oder 8443 für HTTPS, ändern Sie den obigen Ausdruck, um diese Ports anzugeben.

SSL-Interception

April 26, 2021

Eine Citrix Secure Web Gateway (SWG) -Appliance, die für das SSL-Interception konfiguriert ist, fungiert als Proxy. Es kann SSL/TLS -Datenverkehr abfangen und entschlüsseln, die unverschlüsselte Anforderung überprüfen und einen Administrator ermöglichen, Compliance-Regeln und Sicherheitsprüfungen durchzusetzen. SSL-Interception verwendet eine Richtlinie, die angibt, welchen Datenverkehr abgefangen, blockiert oder zugelassen werden soll. Beispielsweise darf der Datenverkehr von und zu Finanzwebsites wie Banken nicht abgefangen werden, aber anderer Datenverkehr kann abgefangen werden, und Websites auf der Sperrliste können identifiziert und blockiert werden. Citrix empfiehlt, dass Sie eine allgemeine Richtlinie zum Abfangen des Datenverkehrs und spezifischere Richtlinien konfigurieren, um einen bestimmten Datenverkehr zu umgehen.

Der Client und der Citrix SWG-Proxy richten einen HTTPS/TLS -Handshake ein. Der SWG-Proxy richtet einen weiteren HTTPS/TLS -Handshake mit dem Server ein und empfängt das Serverzertifikat. Der Proxy überprüft das Serverzertifikat im Auftrag des Clients und überprüft auch die Gültigkeit des Serverzertifikats mit dem OCSP (Online Certificate Status Protocol). Es generiert das Serverzertifikat neu, signiert es mit dem Schlüssel des auf der Appliance installierten Zertifizierungsstellenzertifikats und stellt es dem Client zur Verfügung. Daher wird ein Zertifikat zwischen dem Client und der Citrix ADC-Appliance und ein anderes Zertifikat zwischen der Appliance und dem Back-End-Server verwendet.

> **Wichtig**
>
> Das Zertifizierungsstellenzertifikat, das zum Signieren des Serverzertifikats verwendet wird, muss auf allen Clientgeräten vorinstalliert sein, damit das regenerierte Serverzertifikat vom Client als vertrauenswürdig eingestuft wird.

Bei abgefangenem HTTPS-Datenverkehr entschlüsselt der SWG-Proxyserver den ausgehenden Datenverkehr, greift auf die Klartext-HTTP-Anforderung zu und kann jede Layer 7-Anwendung verwenden, um den Datenverkehr zu verarbeiten, z. B. indem Sie die Nur-Text-URL betrachten und den Zugriff aufgrund der Unternehmensrichtlinie und der URL-Reputation zulassen oder blockieren. Wenn die Richtlinienentscheidung besteht, den Zugriff auf den Ursprungsserver zu ermöglichen, leitet der

Proxy-Server die neu verschlüsselte Anforderung an den Zieldienst (auf dem Ursprungsserver) weiter. Der Proxy entschlüsselt die Antwort vom Ursprungsserver, greift auf die HTTP-Antwort im Klartext zu und wendet optional alle Richtlinien auf die Antwort an. Der Proxy verschlüsselt dann die Antwort erneut und leitet sie an den Client weiter. Wenn die Richtlinienentscheidung darin besteht, die Anforderung an den Ursprungsserver zu blockieren, kann der Proxy eine Fehlerantwort, z. B. HTTP 403, an den Client senden.

Um SSL-Interception durchzuführen, müssen Sie zusätzlich zu dem zuvor konfigurierten Proxyserver Folgendes auf einer SWG-Appliance konfigurieren:

- SSL-Profil
- SSL-Richtlinie
- Zertifizierungsstellenzertifikatspeicher
- SSL-Fehler Autolearning und Caching

SSL-Profil

April 26, 2021

Ein SSL-Profil ist eine Sammlung von SSL-Einstellungen, wie Verschlüsselungen und Protokolle. Ein Profil ist hilfreich, wenn Sie gemeinsame Einstellungen für verschiedene Server haben. Anstatt für jeden Server dieselben Einstellungen anzugeben, können Sie ein Profil erstellen, die Einstellungen im Profil angeben und das Profil dann an verschiedene Server binden. Wenn kein benutzerdefiniertes Front-End-SSL-Profil erstellt wird, ist das Standard-Front-End-Profil an clientseitige Entitäten gebunden. Mit diesem Profil können Sie Einstellungen für die Verwaltung der clientseitigen Verbindungen konfigurieren. Für SSL-Interception müssen Sie ein SSL-Profil erstellen und SSL-Interception (SSLi) im Profil aktivieren. Eine Standardverschlüsselungsgruppe ist an dieses Profil gebunden, Sie können jedoch weitere Verschlüsselungen entsprechend Ihrer Bereitstellung konfigurieren. Sie müssen ein SSLi-Zertifizierungsstellenzertifikat an dieses Profil binden und dann das Profil an einen Proxyserver binden. Für das SSL-Interception sind die wesentlichen Parameter in einem Profil diejenigen, die verwendet werden, um den OCSP-Status des Ursprungsserverzertifikats zu überprüfen, die Clientneuverhandlung auszulösen, wenn der Ursprungsserver eine Neuverhandlung anfordert, und das Ursprungsserverzertifikat vor der Wiederverwendung der Front-End-SSL-Sitzung zu überprüfen. Sie müssen das Standard-Backend-Profil verwenden, wenn Sie mit den Ursprungsservern kommunizieren. Legen Sie alle serverseitigen Parameter, wie etwa Verschlüsselungssammlungen, im standardmäßigen Backend-Profil fest. Ein benutzerdefiniertes Back-End-Profil wird nicht unterstützt.

Beispiele für die am häufigsten verwendeten SSL-Einstellungen finden Sie unter Beispielprofil am Ende dieses Abschnitts.

Die Verschlüsselungs-/Protokollunterstützung unterscheidet sich vom internen und externen Netzwerk. In den folgenden Tabellen ist die Verbindung zwischen den Benutzern und einer SWG-Appliance das interne Netzwerk. Das externe Netzwerk befindet sich zwischen der Appliance und dem Internet.

Tabelle 1: Verschlüsselungs-/Protokoll -Unterstützungsmatrix für das interne Netzwerk

(Verschlüsselung/Protokoll)/Plattform	MPX (N3)*	VPX
TLS 1.1/1 .2	12.1	12.1
ECDHE/DHE (Beispiel TLS1-ECDHE-RSA-AES128-SHA)	12.1	12.1
AES-GCM (Beispiel TLS1.2-AES128-GCM-SHA256)	12.1	12.1
SHA-2-Chiffre (Beispiel TLS1.2-AES-128-SHA256)	12.1	12.1
ECDSA (Beispiel TLS1-ECDHE-ECDSA-AES256-SHA)	12.1	12.1

Tabelle 2: Verschlüsselung/Protokoll-Unterstützungsmatrix für das externe Netzwerk

(Verschlüsselung/Protokoll)/Plattform	MPX (N3)*	VPX
TLS 1.1/1 .2	12.1	12.1
ECDHE/DHE (Beispiel TLS1-ECDHE-RSA-AES128-SHA)	12.1	12.1
AES-GCM (Beispiel TLS1.2-AES128-GCM-SHA256)	12.1	12.1
SHA-2-Chiffre (Beispiel TLS1.2-AES-128-SHA256)	12.1	12.1
ECDSA (Beispiel TLS1-ECDHE-ECDSA-AES256-SHA)	12.1	Nicht unterstützt

* Verwenden Sie den Befehl **sh hardware** (show hardware), um festzustellen, ob Ihre Appliance über N3-Chips verfügt.

Beispiel:

```
sh hardware

Platform: NSMPX-22000 16\*CPU+24\*IX+12\*E1K+2\*E1K+4*CVM N3 2200100

Manufactured on: 8/19/2013

CPU: 2900MHZ

Host Id: 1006665862

Serial no: ENUK6298FT

Encoded serial no: ENUK6298FT

Done
<!--NeedCopy-->
```

Hinzufügen eines SSL-Profils und Aktivieren der SSL-Interception mit der Citrix SWG-CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Argumente:

sslInterception:

Aktivieren oder deaktivieren Sie SSL-Interception für Sitzungen.

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

ssliReneg:

Aktivieren oder deaktivieren Sie die auslösende Clientneuverhandlung, wenn eine Neuverhandlungsanforderung vom Ursprungsserver empfangen wird.

Mögliche Werte: ENABLED, DISABLED

Standardwert: ENABLED

ssliOCSPCheck:

Aktivieren oder Deaktivieren der OCSP-Prüfung für ein Ursprungsserver-Zertifikat.

Mögliche Werte: ENABLED, DISABLED

Standardwert: ENABLED

ssliMaxSessPerServer:

Maximale Anzahl von SSL-Sitzungen, die pro dynamischem Ursprungsserver zwischengespeichert werden sollen. Für jede vom Client empfangene SNI-Erweiterung wird eine eindeutige SSL-Sitzung erstellt. Die übereinstimmende Sitzung wird für die Wiederverwendung von Serversitzungen verwendet.

Standardwert: 10

Mindestwert: 1

Maximalwert: 1000

Beispiel:

```
add ssl profile swg_ssl_profile  -sslinterception ENABLED

Done

sh ssl profile swg_ssl_profile

1)    Name: swg_ssl_profile (Front-End)

                SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1
                    .1: ENABLED  TLSv1.2: ENABLED

                Client Auth: DISABLED

                Use only bound CA certificates: DISABLED

                Strict CA checks:                                 NO

                Session Reuse: ENABLED
                    Timeout: 120 seconds

                DH: DISABLED

                DH Private-Key Exponent Size Limit: DISABLED
                    Ephemeral RSA: ENABLED
                    Refresh Count: 0

                Deny SSL Renegotiation
                    ALL

                Non FIPS Ciphers: DISABLED

                Cipher Redirect: DISABLED

                SSL Redirect: DISABLED

                Send Close-Notify: YES

```



```
                Strict Sig-Digest Check: DISABLED

                Push Encryption Trigger: Always

                PUSH encryption trigger timeout:             1 ms

                SNI: DISABLED

                OCSP Stapling: DISABLED

                Strict Host Header check for SNI enabled SSL sessions:
                                        NO

                Push flag:            0x0 (Auto)

                SSL quantum size:                            8 kB

                Encryption trigger timeout           100 mS

                Encryption trigger packet count:               45

                Subject/Issuer Name Insertion Format: Unicode

                SSL Interception: ENABLED

                SSL Interception OCSP Check: ENABLED

                SSL Interception End to End Renegotiation: ENABLED

                SSL Interception Server Cert Verification for Client
                   Reuse: ENABLED

                SSL Interception Maximum Reuse Sessions per Server:  10

                Session Ticket: DISABLED              Session Ticket
                   Lifetime: 300 (secs)

                HSTS: DISABLED

                HSTS IncludeSubDomains: NO

                HSTS Max-Age: 0

                ECC Curve: P_256, P_384, P_224, P_521

1)            Cipher Name: DEFAULT Priority :1

                Description: Predefined Cipher Alias

Done
<!--NeedCopy-->
```


Binden eines Zertifizierungsstellenzertifikats für SSL-Interception an ein SSL-Profl mit der Citrix SWG-CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiel:

```
bind ssl profile swg_ssl_profile -ssliCACertkey swg_ca_cert

Done

sh ssl profile swg_ssl_profile

1)            Name: swg_ssl_profile (Front-End)

                SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1
                   .1: ENABLED  TLSv1.2: ENABLED

                Client Auth: DISABLED

                Use only bound CA certificates: DISABLED

                Strict CA checks:                                NO

                Session Reuse: ENABLED
                   Timeout: 120 seconds

                DH: DISABLED

                DH Private-Key Exponent Size Limit: DISABLED
                   Ephemeral RSA: ENABLED
                   Refresh Count: 0

                Deny SSL Renegotiation
                   ALL

                Non FIPS Ciphers: DISABLED

                Cipher Redirect: DISABLED

                SSL Redirect: DISABLED

                Send Close-Notify: YES

                Strict Sig-Digest Check: DISABLED

                Push Encryption Trigger: Always

                PUSH encryption trigger timeout:             1 ms

                SNI: DISABLED
```



```
40
41                  OCSP Stapling: DISABLED
42
43                  Strict Host Header check for SNI enabled SSL sessions:
                                NO
44
45                  Push flag:            0x0 (Auto)
46
47                  SSL quantum size:                              8 kB
48
49                  Encryption trigger timeout           100 mS
50
51                  Encryption trigger packet count:                45
52
53                  Subject/Issuer Name Insertion Format: Unicode
54
55                  SSL Interception: ENABLED
56
57                  SSL Interception OCSP Check: ENABLED
58
59                  SSL Interception End to End Renegotiation: ENABLED
60
61                  SSL Interception Server Cert Verification for Client
                       Reuse: ENABLED
62
63                  SSL Interception Maximum Reuse Sessions per Server:  10
64
65                  Session Ticket: DISABLED              Session Ticket
                       Lifetime: 300 (secs)
66
67                  HSTS: DISABLED
68
69                  HSTS IncludeSubDomains: NO
70
71                  HSTS Max-Age: 0
72
73                  ECC Curve: P_256, P_384, P_224, P_521
74
75  1)            Cipher Name: DEFAULT Priority :1
76
77                  Description: Predefined Cipher Alias
78
79  1)            SSL Interception CA CertKey Name: swg_ca_cert
80
81  Done
82  <!--NeedCopy-->
```

Binden eines Zertifizierungsstellenzertifikats für SSL-Interception an ein SSL-Profl mit der Citrix SWG-GUI

1. Navigieren Sie zu **System** > **Profile** > **SSL-Profil**.

2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie einen Namen für das Profil an.
4. Aktivieren Sie **SSL-Interception für Sitzungen**.
5. Klicken Sie auf **OK**.
6. Klicken Sie unter **Erweiterte Einstellungen** auf **Zertifikatschlüssel**.
7. Geben Sie einen SSLi CA-Zertifikatschlüssel an, der an das Profil gebunden werden soll.
8. Klicken Sie auf **Auswählen** und dann auf **Binden**.
9. Optional können Sie Verschlüsselungen entsprechend Ihrer Bereitstellung konfigurieren.
    - Klicken Sie auf das Symbol Bearbeiten, und klicken Sie dann auf **Hinzufügen**.
    - Wählen Sie eine oder mehrere Verschlüsselungsgruppen aus, und klicken Sie auf den Pfeil nach rechts.
    - Klicken Sie auf **OK**.
10. Klicken Sie auf **Fertig**.

Binden eines SSL-Profils an einen Proxyserver mit der Citrix SWG-GUI

1. Navigieren Sie zu **Secure Web Gateway** > **Proxyserver**, und fügen Sie einen neuen Server hinzu, oder wählen Sie einen zu ändernden Server aus.
2. Klicken Sie im **SSL-Profil**auf das Symbol Bearbeiten.
3. Wählen Sie in der Liste **SSL-Profil** das SSL-Profil aus, das Sie zuvor erstellt haben.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **Fertig**.

Beispielprofil:

```
Name: swg_ssl_profile (Front-End)

                SSLv3: DISABLED              TLSv1.0: ENABLED  TLSv1
                   .1: ENABLED  TLSv1.2: ENABLED

                Client Auth: DISABLED

                Use only bound CA certificates: DISABLED

                Strict CA checks:                                NO

                Session Reuse: ENABLED
                   Timeout: 120 seconds

                DH: DISABLED

```



```
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
```



```
                  HSTS Max-Age: 0

                  ECC Curve: P_256, P_384, P_224, P_521

1)            Cipher Name: DEFAULT Priority :1

                  Description: Predefined Cipher Alias

1)            SSL Interception CA CertKey Name: swg_ca_cert
<!--NeedCopy-->
```

SSL-Richtlinieninfrastruktur für SSL-Interception

April 26, 2021

Eine Richtlinie verhält sich wie ein Filter für eingehenden Datenverkehr. Richtlinien auf der Citrix Secure Web Gateway (SWG) -Appliance definieren, wie Proxy-Verbindungen und -Anforderungen verwaltet werden. Die Verarbeitung basiert auf den Aktionen, die für diese Richtlinie konfiguriert sind. Das heißt, Daten in Verbindungsanforderungen werden mit einer Regel verglichen, die in der Richtlinie angegeben ist, und die Aktion wird auf Verbindungen angewendet, die der Regel (Ausdruck) entsprechen. Nachdem Sie eine Aktion für die Richtlinie definiert und die Richtlinie erstellt haben, binden Sie sie an einen Proxyserver, sodass sie für den Datenverkehr gilt, der durch diesen Proxyserver fließt.

Eine SSL-Richtlinie für das SSL-Interception wertet eingehenden Datenverkehr aus und wendet eine vordefinierte Aktion auf Anforderungen an, die einer Regel (Ausdruck) entsprechen. Eine Entscheidung zum Abfangen, Umgehen oder Zurücksetzen einer Verbindung wird basierend auf der definierten SSL-Richtlinie getroffen. Sie können eine von drei Aktionen für eine Richtlinie konfigurieren: INTERCEPT, BYPASS oder RESET. Geben Sie beim Erstellen einer Richtlinie eine Aktion an. Um eine Richtlinie in Kraft zu setzen, müssen Sie sie an einen Proxyserver auf der Appliance binden. Um anzugeben, dass eine Richtlinie für das SSL-Interception vorgesehen ist, müssen Sie den Typ (Bindpunkt) als INTERCEPT_REQ angeben, wenn Sie die Richtlinie an einen Proxyserver binden. Wenn Sie die Bindung einer Richtlinie aufheben, müssen Sie den Typ als INTERCEPT_REQ angeben.

> **Hinweis:**
>
> Der Proxyserver kann nur dann abfangen, wenn Sie eine Richtlinie angeben.

Interception des Datenverkehrs kann auf jedem SSL-Handshake-Attribut basieren. Am häufigsten wird die SSL-Domäne verwendet. Die SSL-Domäne wird normalerweise durch die Attribute des SSL-Handshake angezeigt. Hierbei kann es sich um den Wert Server Name Indicator handeln, der aus

der SSL-Client-Hallo (falls vorhanden) extrahiert wurde, oder um den aus dem Ursprungsserverzertifikat extrahierten Wert (Server Alternate Name, SAN) handeln. Die SSLi-Richtlinie in Citrix SWG stellt ein spezielles Attribut namens DETECTED_DOMAIN dar, das es den Kunden erleichtert, Interceptionrichtlinien basierend auf der SSL-Domäne aus dem Ursprungsserverzertifikat zu erstellen. Der Kunde kann den Domänennamen mit einer Zeichenfolge, einer URL-Liste (URL-Gruppe oder`patset`) oder einer von der Domäne abgeleiteten URL-Kategorie abgleichen.

Erstellen einer SSL-Richtlinie mit der Citrix SWG-CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiele:

Die folgenden Beispiele beziehen sich auf Richtlinien mit Ausdrücken, die das`detected_domain` Attribut verwenden, um nach einem Domänennamen zu suchen.

Traffic zu einem Finanzinstitut wie XYZBANK nicht abfangen

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

Erlauben Sie einem Benutzer nicht, über das Unternehmensnetzwerk eine Verbindung zu YouTube herzustellen.

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

Abfangen des gesamten Benutzerverkehrs.

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

Wenn der Kunde die detected_domain nicht verwenden möchte, kann er jedes der SSL-Handshake-Attribute verwenden, um die Domäne zu extrahieren und abzuleiten.

Beispielsweise wird kein Domänenname in der SNI-Erweiterung der Client-Hello Message gefunden. Der Domänenname muss dem Ursprungsserverzertifikat entnommen werden. Die folgenden Beispiele beziehen sich auf Richtlinien mit Ausdrücken, die im Antragstellernamen des Ursprungsserverzertifikats nach einem Domänennamen suchen.

Abfangen des gesamten Benutzerverkehrs zu jeder Yahoo Domain.


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

Abfangen des gesamten Nutzerverkehrs für die Kategorie “Shopping/Retail”.

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

Abfangen des gesamten Benutzerdatenverkehrs an eine nicht kategorisierte URL.

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

Die folgenden Beispiele beziehen sich auf Richtlinien, die der Domäne mit einem Eintrag in einem URL-Satz entsprechen.

Fangen Sie den gesamten Benutzerverkehr ab, wenn der Domänenname in SNI mit einem Eintrag im URL-Set “top100”übereinstimmt.

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

Fangen Sie den gesamten Benutzerverkehr des Domänennamens ab, wenn das Ursprungsserverzertifikat mit einem Eintrag im URL-Set “top100”übereinstimmt.

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

Erstellen einer SSL-Richtlinie für einen Proxyserver mit der SWG-GUI

1. Navigieren Sie zu **Secure Web Gateway > SSL > Richtlinien**.
2. Klicken Sie auf der Registerkarte **SSL-Richtlinien** auf **Hinzufügen**, und geben Sie die folgenden Parameter an:
   - Richtlinienname
   - Richtlinienaktion —Wählen Sie zwischen Abfangen, Umgehen oder Zurücksetzen aus.
   - Ausdruck
3. Klicken Sie auf **Erstellen**.

Binden einer SSL-Richtlinie an einen Proxyserver mit der SWG-CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiel:

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

Binden einer SSL-Richtlinie an einen Proxyserver mit der Citrix SWG-GUI

1. Navigieren Sie zu **Secure Web Gateway > Virtuelle Proxy-Server**.
2. Wählen Sie einen virtuellen Server aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie unter **Erweiterte Einstellungen** auf **SSL-Richtlinien**.
4. Klicken Sie in das Feld **SSL-Richtlinie** .
5. **Wählen Sie unter Richtlinie**auswählen eine zu bindende Richtlinie aus.
6. Wählen Sie unter **Typ**die Option **INTERCEPT_REQ**aus.
7. Klicken Sie auf **Bin** den und dann auf **OK** .

Aufheben der Bindung einer SSL-Richtlinie an einen Proxyserver mit der Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

SSL-Ausdrücke, die in SSL-Richtlinien für SWG verwendet werden

Ausdruck	Beschreibung
`CLIENT.SSL.CLIENT_HELLO.SNI.*`	Gibt die SNI-Erweiterung in einem Zeichenfolgenformat zurück. Bewerten Sie die Zeichenfolge, um zu sehen, ob sie den angegebenen Text enthält. Beispiel: client.ssl.client_hello.sni.contains ("xyz.com")
`CLIENT.SSL.ORIGIN_SERVER_CERT.*`	Gibt ein Zertifikat zurück, das von einem Back-End-Server empfangen wird, in einem Zeichenfolgenformat. Bewerten Sie die Zeichenfolge, um zu sehen, ob sie den angegebenen Text enthält. Beispiel: client.ssl.origin_server_cert.subject.contains("xyz.com")
`CLIENT.SSL.DETECTED_DOMAIN.*`	Gibt eine Domäne entweder aus der SNI-Erweiterung oder aus dem Ursprungsserverzertifikat in einem Zeichenfolgenformat zurück. Bewerten Sie die Zeichenfolge, um zu sehen, ob sie den angegebenen Text enthält. Beispiel: client.ssl.detected_domain.contains("xyz.com")

Zertifikatspeicher für SSL-Interception

April 26, 2021

Ein SSL-Zertifikat, das integraler Bestandteil jeder SSL-Transaktion ist, ist ein digitales Eingabeformular (X509), das ein Unternehmen (Domain) oder eine Person identifiziert. Ein SSL-Zertifikat wird von einer Zertifizierungsstelle ausgestellt. Eine Zertifizierungsstelle kann privat oder öffentlich sein. Zertifikate, die von öffentlichen Zertifizierungsstellen ausgestellt werden, wie z. B. Verisign, werden von Anwendungen, die SSL-Transaktionen durchführen, vertrauenswürdig. Diese Anwendungen verwalten eine Liste der Zertifizierungsstellen, denen sie vertrauen.

Als Forward Proxy führt eine Citrix Secure Web Gateway (SWG) -Appliance Verschlüsselung und Entschlüsselung des Datenverkehrs zwischen einem Client und einem Server durch. Es fungiert

als Server für den Client (Benutzer) und als Client für den Server. Bevor eine Appliance HTTPS-Datenverkehr verarbeiten kann, muss sie die Identität eines Servers überprüfen, um betrügerische Transaktionen zu verhindern. Daher muss die Appliance als Client für den Ursprungsserver das Ursprungsserverzertifikat überprüfen, bevor sie es akzeptiert. Um das Serverzertifikat zu überprüfen, müssen alle Zertifikate (z. B. Stamm- und Zwischenzertifikate), die zum Signieren und Ausstellen des Serverzertifikats verwendet werden, auf der Appliance vorhanden sein. Ein Standardsatz von Zertifizierungsstellenzertifikaten ist auf einer Appliance vorinstalliert. Citrix SWG kann diese Zertifikate verwenden, um fast alle gängigen Ursprungsserver-Zertifikate zu überprüfen. Dieser Standardsatz kann nicht geändert werden. Wenn Ihre Bereitstellung jedoch mehr Zertifizierungsstellenzertifikate erfordert, können Sie ein Bündel solcher Zertifikate erstellen und das Paket in die Appliance importieren. Ein Bundle kann auch ein einzelnes Zertifikat enthalten.

Wenn Sie ein Zertifikatpaket in die Appliance importieren, lädt die Appliance das Paket vom Remotestandort herunter und installiert es nach der Überprüfung, ob das Paket nur Zertifikate enthält, auf der Appliance. Sie müssen ein Zertifikatpaket anwenden, bevor Sie es zum Überprüfen eines Serverzertifikats verwenden können. Sie können ein Zertifikatpaket auch exportieren, um es zu bearbeiten oder als Backup an einem Offline-Speicherort zu speichern.

Importieren und Anwenden eines Zertifizierungsstellenzertifikatbündels mit der Citrix SWG CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

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

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

ARGUMENTS:

Nome:

Name, der dem importierten Zertifikatspaket zugewiesen werden soll. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Die folgende Anforderung gilt nur für die CLI:

Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “meine Datei”oder ‘meine Datei’).

Maximale Länge: 31

src:

URL zur Angabe des Protokolls, des Hosts und des Pfads, einschließlich des Dateinamens, zum Zertifikatpaket, das importiert oder exportiert werden soll. Beispiel: `http://www.example.com/cert\\_bundle\\_file`.

HINWEIS: Der Import schlägt fehl, wenn sich das zu importierende Objekt auf einem HTTPS-Server befindet, der Clientzertifikatauthentifizierung für den Zugriff erfordert.

Maximale Länge: 2047

Beispiel:

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

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

```
show ssl certbundle

            Name : swg-certbundle(Inuse)

            URL : http://www.example.com/cert_bundle

    Done
<!--NeedCopy-->
```

Importieren und Anwenden eines Zertifizierungsstellenzertifikatbündels mit der Citrix SWG-GUI auf die Appliance

1. Navigieren Sie zu **Secure Web Gateway** > **Erste Schritte** > **Zertifikatpakete** .
2. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie ein Zertifikatspaket aus der Liste aus.
   - Um ein neues Zertifikatpaket hinzuzufügen, klicken Sie auf + und geben Sie einen Namen und eine Quell-URL an. Klicken Sie auf **OK**.
3. Klicken Sie auf **OK**.

Entfernen eines Zertifizierungsstellenzertifikatpakets aus der Appliance mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

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


Beispiel:

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

Exportieren eines Zertifizierungsstellenzertifikatpakets aus der Appliance mit der Citrix SWG CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

ARGUMENTS:

Nome:

Name, der dem importierten Zertifikatspaket zugewiesen werden soll. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Die folgende Anforderung gilt nur für die CLI:

Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “meine Datei”oder ‘meine Datei’).

Maximale Länge: 31

src:

URL zur Angabe des Protokolls, des Hosts und des Pfads, einschließlich des Dateinamens, zum Zertifikatpaket, das importiert oder exportiert werden soll. Beispiel: `http://www.example.com/cert\\_bundle\\_file`.

HINWEIS: Der Import schlägt fehl, wenn sich das zu importierende Objekt auf einem HTTPS-Server befindet, der Clientzertifikatauthentifizierung für den Zugriff erfordert.

Maximale Länge: 2047

Beispiel:

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

Importieren, Anwenden und Überprüfen eines CA-Zertifikatpakets aus dem Mozilla CA-Zertifikatspeicher

Geben Sie an der Eingabeaufforderung Folgendes ein:


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

Geben Sie Folgendes ein, um das Bündel anzuwenden:

```
> apply certbundle mozilla_public_ca
Done
<!--NeedCopy-->
```

Geben Sie Folgendes ein, um das verwendete Zertifikatbündel zu überprüfen:

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

Einschränkung

Zertifikatpakete werden in einem Cluster-Setup oder auf einer partitionierten Appliance nicht unterstützt.

SSL-Fehler beim automatischen Lernen

April 26, 2021

Die Citrix SWG-Appliance fügt der SSL-Umgehungsliste eine Domäne hinzu, wenn der Lernmodus aktiviert ist. Der Lernmodus basiert auf der SSL-Warnmeldung, die von einem Client oder einem Ursprungsserver empfangen wird. Das heißt, das Lernen hängt davon ab, dass der Client oder Server eine Warnmeldung sendet. Es gibt keine Erkenntnisse, wenn keine Warnmeldung gesendet wird. Die Appliance lernt, ob eine der folgenden Bedingungen erfüllt ist:

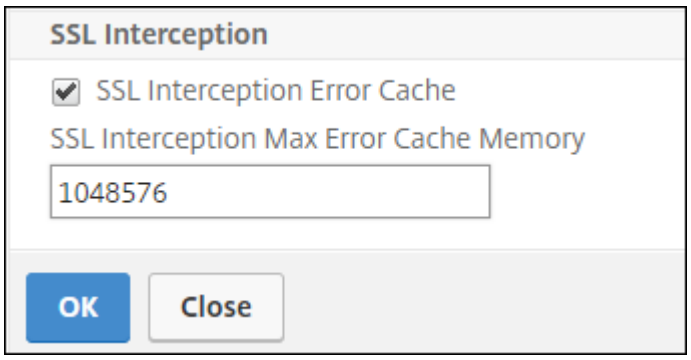
1. Eine Anforderung für ein Clientzertifikat wird vom Server empfangen.
2. Eine der folgenden Warnungen wird als Teil des Handshake empfangen:
    - BAD_CERTIFICATE
    - UNSUPPORTED_CERTIFICATE
    - CERTIFICATE_REVOKED
    - CERTIFICATE_EXPIRED
    - CERTIFICATE_UNKNOWN
    - UNKNOWN_CA (Wenn ein Client das Anheften verwendet, sendet er diese Warnmeldung, wenn er ein Serverzertifikat erhält.)

- HANDSHAKE_FAILURE

Um das Lernen zu aktivieren, müssen Sie den Fehlercache aktivieren und den dafür reservierten Speicher angeben.

Aktivieren des Lernens mit der Citrix SWG-GUI

1. Navigieren Sie zu **Secure Web Gateway** > **SSL** .
2. Klicken Sie **unter Einstellungen**auf **Erweiterte SSL-Einstellungen ändern**.
3. Wählen Sie in **SSL-Interception** die Option **SSL-Interception-Fehlercache** aus.
4. Geben Sie in **SSL Interception Max Error Cache Memory** den Speicher (in Byte) an, der reserviert werden soll.



5. Klicken Sie auf **OK**.

Aktivieren des Lernens mit der Citrix SWG CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Argumente:

ssliErrorCache:

```
1           Aktivieren oder deaktivieren Sie dynamisches Lernen, und
               speichern Sie die erlernten Informationen, um nachfolgende
                Entscheidungen zu treffen, um Anforderungen abzufangen
               oder zu umgehen. Wenn diese Option aktiviert ist, führt
               die Appliance eine Cache-Suche durch, um zu entscheiden,
               ob die Anforderung umgangen werden soll.
2
3           Mögliche Werte: `ENABLED, DISABLED`
4
5           Standardwert: `DISABLED`
```


ssliMaxErrorCacheMem:

```
Geben Sie den maximalen Speicher in Byte an, mit dem die gelernten Daten zwischengespeichert werden können. Dieser Speicher wird als LRU-Cache verwendet, so dass die alten Einträge nach Erschöpfung des eingestellten Speicherlimits durch neue Einträge ersetzt werden. Der Wert 0 entscheidet automatisch über den Grenzwert.

Standardwert: 0

Mindestwert: 0

maximaler Wert: 4294967294
```

Benutzeridentitätsverwaltung

April 26, 2021

Immer mehr Sicherheitsverstöße und die wachsende Beliebtheit mobiler Geräte haben die Notwendigkeit betont, sicherzustellen, dass die Nutzung des externen Internets den Unternehmensrichtlinien entspricht und nur autorisierte Benutzer auf externe Ressourcen zugreifen, die vom Unternehmenspersonal bereitgestellt werden. Identity Management ermöglicht dies, indem die Identität einer Person oder eines Geräts überprüft wird. Es bestimmt nicht, welche Aufgaben der Einzelne übernehmen kann oder welche Dateien der Einzelne sehen kann.

Eine SWG-Bereitstellung (Secure Web Gateway) identifiziert den Benutzer, bevor der Zugriff auf das Internet gewährt wird. Alle Anfragen und Antworten des Benutzers werden überprüft. Benutzeraktivität wird protokolliert, und Datensätze werden zur Berichterstellung in das Citrix Application Delivery Management (ADM) exportiert. In Citrix ADM können Sie die Statistiken zu Benutzeraktivitäten, Transaktionen und Bandbreitenverbrauch anzeigen.

Standardmäßig wird nur die IP-Adresse des Benutzers gespeichert, Sie können jedoch die Citrix SWG-Appliance so konfigurieren, dass weitere Details über den Benutzer aufgezeichnet werden. Mithilfe dieser Identitätsinformationen können Sie für bestimmte Benutzer umfassendere Internetnutzungsrichtlinien erstellen.

Die Citrix ADC-Appliance unterstützt die folgenden Authentifizierungsmodi für eine explizite Proxy-Konfiguration.

- **Lightweight Directory Access Protocol (LDAP)**. Authentifiziert den Benutzer über einen externen LDAP-Authentifizierungsserver. Weitere Informationen finden Sie unter LDAP-Authentifizierungsrichtlinien.

- **RADIUS**. Authentifiziert den Benutzer über einen externen RADIUS-Server. Weitere Informationen finden Sie unter RADIUS-Authentifizierungsrichtlinien.
- **TACACS +**. Authentifiziert den Benutzer über einen externen TACACS-Authentifizierungsserver (Terminal Access Controller Access-Control System). Weitere Informationen finden Sie unter Authentifizierungsrichtlinien.
- **Verhandeln**. Authentifiziert den Benutzer über einen Kerberos-Authentifizierungsserver. Wenn bei der Kerberos-Authentifizierung ein Fehler auftritt, verwendet die Appliance die NTLM-Authentifizierung. Weitere Informationen finden Sie unter Authentifizierungsrichtlinien aushandeln.

Für transparenten Proxy wird derzeit nur IP-basierte LDAP-Authentifizierung unterstützt. Wenn eine Clientanforderung empfangen wird, authentifiziert der Proxy den Benutzer, indem er einen Eintrag für die Client-IP-Adresse im Active Directory überprüft und eine Sitzung basierend auf der IP-Adresse des Benutzers erstellt. Wenn Sie jedoch ssoNameAttribute in einer LDAP-Aktion konfigurieren, wird eine Sitzung mit dem Benutzernamen anstelle der IP-Adresse erstellt. Klassische Richtlinien werden für die Authentifizierung in einem transparenten Proxy-Setup nicht unterstützt.

> **Hinweis**
>
> Für einen expliziten Proxy müssen Sie den LDAP-Anmeldenamen auf `sAMAccountName` festlegen. Für transparenten Proxy müssen Sie den LDAP-Anmeldenamen auf `networkAddress` und `attribute1` auf `sAMAccountName` festlegen.

Beispiel für expliziten Proxy:

```
add authentication ldapAction swg-auth-action-explicit -serverIP
    10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
    CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
    freebsd123$ -ldapLoginName sAMAccountName
<!--NeedCopy-->
```

Beispiel für transparenten Proxy:

```
add authentication ldapAction swg-auth-action-explicit -serverIP
    10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
    CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
    freebsd123$ -ldapLoginName networkAddress -authentication disable -
    Attribute1 sAMAccountName
<!--NeedCopy-->
```

Einrichten der Benutzerauthentifizierung mit der Citrix SWG-CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication vserver <vserver name> SSL

```



```
3 bind ssl vserver <vserver 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 vserver <vserver name> -policy <string> -priority <
     positive_integer>
10
11 set cs vserver <name> -authn401 ON -authnVsName <string>
12 <!--NeedCopy-->
```

Argumente:

Servername:

Name des virtuellen Authentifizierungsservers, an den die Richtlinie gebunden werden soll.

Maximale Länge: 127

serviceType:

Protokolltyp des virtuellen Authentifizierungsservers. Immer SSL.

Mögliche Werte: SSL

Standardwert: SSL

Name der Aktion:

Name für die neue LDAP-Aktion. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und nur Buchstaben, Zahlen und Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), at (@), Gleich (=), Doppelpunkt (:) und Unterstrich enthalten. Kann nicht geändert werden, nachdem die LDAP-Aktion hinzugefügt wurde. Die folgende Anforderung gilt nur für die CLI:

Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “Meine Authentifizierungsaktion”oder ‘Meine Authentifizierungsaktion’).

Maximale Länge: 127

serverIP:

IP-Adresse, die dem LDAP-Server zugewiesen ist.

ldapBase:

Basis (Knoten), von dem aus LDAP-Suchen gestartet werden sollen. Wenn der LDAP-Server lokal ausgeführt wird, lautet der Standardwert von base dc = netscaler, dc = com. Maximale Länge: 127

ldapBindDn:

Vollständiger Distinguished Name (DN), der zum Binden an den LDAP-Server verwendet wird.

Standard: `cn=Manager,dc=netscaler,dc=com`

Maximale Länge: 127

ldapBindDnPassword:

Kennwort für die Bindung an den LDAP-Server.

Maximale Länge: 127

ldapLoginName:

LDAP-Anmeldenamen-Attribut. Die Citrix ADC-Appliance verwendet den LDAP-Anmeldenamen, um externe LDAP-Server oder Active Directories abzufragen. Maximale Länge: 127

Richtlinienname:

Name für die erweiterte Authentifizierungsrichtlinie. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und nur Buchstaben, Zahlen und Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), at (@), Gleich (=), Doppelpunkt (:) und Unterstrich enthalten. Kann nicht geändert werden, nachdem die Authentifizierungsrichtlinie erstellt wurde. Die folgende Anforderung gilt nur für die CLI:

Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. "meine Authentifizierungsrichtlinie"oder 'meine Authentifizierungsrichtlinie').

Maximale Länge: 127

rule:

Name der Regel oder eines Standardsyntaxausdrucks, mit dem die Richtlinie bestimmt, ob versucht wird, den Benutzer beim AUTHENTICATION-Server zu authentifizieren.

Maximale Länge: 1499

action:

Name der Authentifizierungsaktion, die ausgeführt werden soll, wenn die Richtlinie übereinstimmt.

Maximale Länge: 127

priority:

Positive Ganzzahl, die die Priorität der Richtlinie angibt. Eine niedrigere Zahl gibt eine höhere Priorität an. Richtlinien werden in der Reihenfolge ihrer Prioritäten ausgewertet, und die erste Richtlinie, die der Anforderung entspricht, wird angewendet. Muss innerhalb der Liste der Richtlinien eindeutig sein, die an den virtuellen Authentifizierungsserver gebunden sind.

Mindestwert: 0

Maximalwert: 4294967295

Beispiel:

```
add authentication vserver swg-auth-vs SSL

Done

bind ssl vserver explicit-auth-vs -certkeyName ns-swg-ca-certkey

Done

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

Done

add authenticationpolicy swg-auth-policy -rule true -action swg-auth-
    action-explicit

    Done

bind authentication vserver swg-auth-vs -policy swg-auth-policy -
    priority 1

Done

set cs vserver testswg -authn401 ON -authnVsName swg-auth-vs

Done
<!--NeedCopy-->
```

Aktivieren der Benutzernamenprotokollierung mit der Citrix SWG-CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Argumente:

`AAAUserName`

Aktivieren Sie die AppFlow AAA-Benutzernamenprotokollierung.

Mögliche Werte:`ENABLED, DISABLED`

Standardwert:`DISABLED`

Beispiel:


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

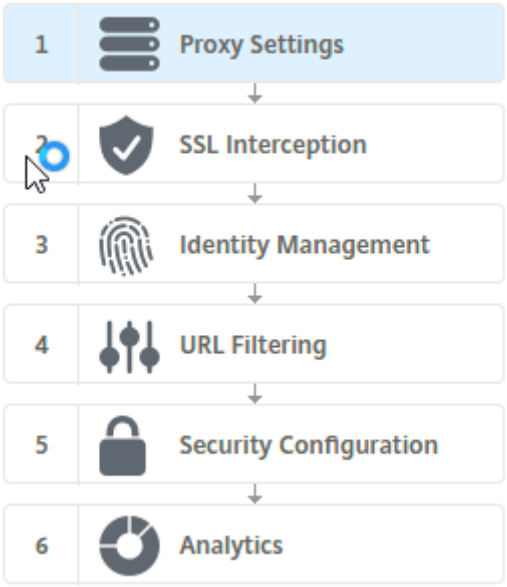
URL-Filterung

April 26, 2021

Die URL-Filterung ermöglicht die richtlinienbasierte Steuerung von Websites mit der in URLs enthaltenen Informationen. Mit dieser Funktion können Netzwerkadministratoren den Benutzerzugriff auf bösartige Websites im Netzwerk überwachen und kontrollieren.

Erste Schritte

Wenn Sie ein neuer Benutzer sind und URL-Filter konfigurieren möchten, müssen Sie die anfängliche SWG-Setup abschließen. Um mit der URL-Filterung zu beginnen, müssen Sie sich zuerst beim Citrix SWG-Assistenten anmelden. Der Assistent führt Sie durch eine Reihe von Konfigurationsschritten, bevor Sie die URL-Filterrichtlinien anwenden.



> **Hinweis**
>
> Bevor Sie beginnen, stellen Sie sicher, dass auf Ihrer Appliance eine gültige URL Threat Intelligence Feature-Lizenz installiert ist. Wenn Sie eine Testversion verwenden, achten Sie darauf, eine gültige Lizenz zu erwerben, um diese Funktion weiterhin auf der SWG-Appliance zu nutzen.

Anmelden beim SWG-Assistenten

Der Citrix SWG-Assistent führt Sie durch eine Reihe vereinfachter Konfigurationsaufgaben, und im rechten Bereich wird die entsprechende Flowsequenz angezeigt. Mit diesem Assistenten können Sie URL-Filterrichtlinien auf eine URL-Liste oder eine vordefinierte Liste von Kategorien anwenden.

Schritt 1: Konfigurieren von Proxy-Einstellungen

Sie müssen zuerst einen Proxy-Server konfigurieren, über den der Client auf das SWG-Gateway zugreift. Dieser Server ist vom Typ SSL und arbeitet im expliziten oder transparenten Modus. Weitere Hinweise zur Konfiguration des Proxyservers finden Sie unter Proxy-Modi.

Schritt 2: Konfigurieren von SSL-Interception

Nach der Konfiguration des Proxyservers müssen Sie den SSL-Interceptionproxy so konfigurieren, dass verschlüsselten Datenverkehr auf der Citrix SWG-Appliance abgefangen wird. Im Falle der URL-Filterung fängt der SSL-Proxy den Datenverkehr ab und blockiert die URL auf der Sperrliste, während der gesamte andere Datenverkehr umgangen werden kann. Weitere Hinweise zum Konfigurieren der SSL-Interception finden Sie unter SSL-Interception.

Schritt 3: Konfigurieren der Identitätsverwaltung

Ein Benutzer wird authentifiziert, bevor er sich am Unternehmensnetzwerk anmelden darf. Die Authentifizierung bietet die Flexibilität, spezifische Richtlinien für einen Benutzer oder eine Gruppe von Benutzern basierend auf ihren Rollen zu definieren. Weitere Informationen zur Benutzerauthentifizierung finden Sie unterVerwaltung der Benutzeridentifizierung

Schritt 4: URL-Filterung konfigurieren

Der Administrator kann eine URL-Filterrichtlinie entweder mit der URL-Kategorisierungsfunktion oder mit der URL-Listenfunktion anwenden.

URL-Kategorisierung. Steuert den Zugriff auf Websites und Webseiten, indem der Datenverkehr anhand einer vordefinierten Liste von Kategorien gefiltert wird.

URL-Liste. Steuert den Zugriff auf Websites und Webseiten auf der Sperrliste, indem der Zugriff auf URLs verweigert wird, die sich in einem URL-Satz befinden, der in die Appliance importiert wurde.

Schritt 5: Konfigurieren der Sicherheitskonfiguration

Mit diesem Schritt können Sie eine Reputationsbewertung konfigurieren und Benutzern erlauben, den Zugriff auf die Websites zu steuern, indem Sie den Zugriff verweigern, wenn die Bewertung zu niedrig ist. Ihre Reputationsbewertung kann zwischen 1 und 4 liegen, und Sie können den Schwellenwert konfigurieren, bei dem die Punktzahl inakzeptabel wird. Bei Bewertungen, die den Schwellenwert überschreiten, können Sie eine Richtlinienaktion auswählen, um Datenverkehr zuzulassen, zu blockieren oder umzuleiten. Weitere Informationen finden Sie unter Sicherheitskonfiguration.

Schritt 6: Konfigurieren von SWG-Analysen

Mit diesem Schritt können Sie SWG-Analysen aktivieren, um den Webverkehr zu kategorisieren, die URL-Kategorie in den Benutzertransaktionsprotokollen zu protokollieren und Traffic-Analysen anzuzeigen. Weitere Informationen zu SWG Analytics finden Sie unterAnalytics.

Schritt 7: Klicken Sie auf Fertig, um die Erstkonfiguration abzuschließen und die Verwaltung der URL-Filterkonfiguration fortzusetzen

URL-Liste

April 26, 2021

Mit der URL-Listenfunktion können Unternehmenskunden den Zugriff auf bestimmte Websites und Websitekategorien steuern. Das Feature filtert Websites, indem eine Responder-Richtlinie angewendet wird, die an einen URL-Abgleichsalgorithmus gebunden ist. Der Algorithmus gleicht die eingehende URL mit einem URL-Satz ab, der aus bis zu einer Million (1.000.000) Einträgen besteht. Wenn die eingehende URL-Anforderung mit einem Eintrag in der Gruppe übereinstimmt, verwendet die Appliance die Responderrichtlinie, um die Anforderung (HTTP/HTTPS) auszuwerten und den Zugriff darauf zu steuern.

URL-Set-Typen

Jeder Eintrag in einem URL-Satz kann eine URL und optional deren Metadaten (URL-Kategorie, Kategoriegruppen oder andere verwandte Daten) enthalten. Bei URLs mit Metadaten verwendet die Appliance einen Richtlinienausdruck, der die Metadaten auswertet. Weitere Informationen finden Sie unter URL-Satz.

Citrix SWG unterstützt benutzerdefinierte URL-Sets. Sie können auch Mustersätze verwenden, um URLs zu filtern.

Benutzerdefinierter URL-Satz. Sie können einen benutzerdefinierten URL-Satz mit bis zu 1.000.000 URL-Einträgen erstellen und als Textdatei in Ihre Appliance importieren.

Musterset Eine SWG-Appliance kann Patternsätze verwenden, um URLs zu filtern, bevor der Zugriff auf Websites gewährt wird. Ein Mustersatz ist ein Zeichenfolge-Matching-Algorithmus, der nach einer genauen Übereinstimmung zwischen einer eingehenden URL und bis zu 5000 Einträgen sucht. Weitere Informationen finden Sie unter Musterset.

Jede URL in einem importierten URL-Satz kann eine benutzerdefinierte Kategorie in Form von URL-Metadaten aufweisen. Ihre Organisation kann das Set hosten und die SWG-Appliance so konfigurieren, dass das Set regelmäßig aktualisiert wird, ohne dass ein manueller Eingriff erforderlich ist.

Nach der Aktualisierung des Satzes erkennt die Citrix ADC-Appliance automatisch die Metadaten, und die Kategorie steht als Richtlinienausdruck zur Verfügung, um die URL auszuwerten und eine Aktion wie Zulassen, Blockieren, Umleiten oder Benachrichtigen des Benutzers anzuwenden.

Erweiterte Richtlinienausdrücke, die mit URL-Sets verwendet werden

In der folgenden Tabelle werden die grundlegenden Ausdrücke beschrieben, die Sie zum Auswerten des eingehenden Datenverkehrs verwenden können.

1. `.URLSET_MATCHES_ANY` - Gibt `TRUE` zurück, wenn die URL genau mit einem Eintrag im URL-Satz übereinstimmt.
2. `.GET_URLSET_METADATA()` - Der Ausdruck `GET_URLSET_METADATA()` gibt die zugeordneten Metadaten zurück, wenn die URL einem Muster innerhalb des URL-Sets entspricht. Eine leere Zeichenfolge wird zurückgegeben, wenn keine Übereinstimmung vorhanden ist.
3. `.GET_ URLSET_METADATA().EQ(<METADATA)- .GET_ URLSET_METADATA().EQ (<METADATA)`
4. `.GET_URLSET_METADATA ().TYPECAST_LIST_T(',').GET(0).EQ()` - Gibt `TRUE` zurück, wenn die übereinstimmenden Metadaten am Anfang der Kategorie sind. Dieses Muster kann verwendet werden, um separate Felder innerhalb von Metadaten zu codieren, aber nur mit dem ersten Feld übereinstimmen.
5. `HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL)` - Verbindet die Host- und URL-Parameter, die dann als Abgleich verwendet werden können.

Responder-Aktionstypen

> **Hinweis:** In der Tabelle wird `HTTP.REQ.URL` als `<URL expression>` verallgemeinert.

In der folgenden Tabelle werden die Aktionen beschrieben, die auf eingehenden Internetverkehr angewendet werden können.

Responderaktion	Beschreibung
Zulassen	Erlauben Sie der Anforderung, auf die Ziel-URL zuzugreifen.
Redirect	Leiten Sie die Anforderung an die URL um, die als Ziel angegeben ist.
Blockieren	Verweigern Sie die Anfrage.

Voraussetzungen

Sie müssen einen DNS-Server konfigurieren, wenn Sie einen URL-Satz von einer Hostnamen-URL importieren. Dies ist nicht erforderlich, wenn Sie eine IP-Adresse verwenden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiel:

```
1 add dns nameServer 10.140.50.5
```

Konfigurieren einer URL-Liste

Zum Konfigurieren einer URL-Liste können Sie den Citrix SWG-Assistenten oder die Citrix ADC-Befehlszeilenschnittstelle (CLI) verwenden. Auf der Citrix SWG-Appliance müssen Sie zuerst die Responderrichtlinie konfigurieren und dann die Richtlinie an einen URL-Satz binden.

Citrix empfiehlt, dass Sie den Citrix SWG-Assistenten als bevorzugte Option zum Konfigurieren einer URL-Liste verwenden. Verwenden Sie den Assistenten, um eine Responder-Richtlinie an einen URL-Satz zu binden. Alternativ können Sie die Richtlinie an einen Mustersatz binden.

Konfigurieren einer URL-Liste mit dem Citrix SWG-Assistenten

So konfigurieren Sie URL-Liste für HTTPS-Datenverkehr mit der Citrix SWG-GUI:

1. Melden Sie sich bei der Citrix SWG-Appliance an, und navigieren Sie zur Seite **Secured Web Gateway**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:

    a) Klicken Sie auf **Secured Web Gateway-Assistent**, um eine neue SWG-Konfiguration mit URL-Listen-Funktion zu erstellen.

b) Wählen Sie eine vorhandene Konfiguration aus, und klicken Sie auf **Bearbeiten**.

3. Klicken Sie im Abschnitt **URL-Filterung** auf **Bearbeiten**.
4. Aktivieren Sie das Kontrollkästchen **URL-Liste**, um die Funktion zu aktivieren.
5. Wählen Sie eine **URL-Listenrichtlinie** aus, und klicken Sie auf **Binden**.
6. Klicken Sie auf **Weiter** und dann **Fertig**.

Weitere Informationen finden Sie unter Erstellen einer URL-Listenrichtlinie.

Konfigurieren einer URL-Liste mit der Citrix SWG-CLI

Gehen Sie folgendermaßen vor, um eine URL-Liste zu konfigurieren.

1. Konfigurieren Sie einen virtuellen Proxyserver für HTTP- und HTTPS-Datenverkehr.
2. Konfigurieren Sie SSL-Interception zum Abfangen des HTTPS-Datenverkehrs.
3. Konfigurieren Sie eine URL-Liste, die einen URL-Satz für HTTP-Datenverkehr enthält.
4. Konfigurieren Sie die URL-Liste mit URL-Satz für HTTPS-Datenverkehr.
5. Konfigurieren Sie einen privaten URL-Satz.

> **Hinweis**
>
> Wenn Sie bereits eine SWG-Appliance konfiguriert haben, können Sie die Schritte 1 und 2 überspringen und mit Schritt 3 konfigurieren.

Konfigurieren eines virtuellen Proxyservers für den Internetverkehr Die Citrix SWG-Appliance unterstützt transparente und explizite virtuelle Proxyserver. Gehen Sie folgendermaßen vor, um einen virtuellen Proxyserver für den Internetverkehr im expliziten Modus zu konfigurieren:

1. Fügen Sie einen virtuellen SSL-Proxyserver hinzu.
2. Binden Sie eine Responderrichtlinie an den virtuellen Proxyserver.

So fügen Sie mit der Citrix SWG-CLI einen virtuellen Proxyserver hinzu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add cs vserver <name> <serviceType> <IPAddress> <port>
<!--NeedCopy-->
```

Beispiel:

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

So binden Sie eine Responderrichtlinie mit der Citrix SWG-CLI an einen virtuellen Proxyserver:


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

> **Hinweis**
>
> Wenn Sie den SSL-Interceptor bereits als Teil der Citrix SWG-Konfiguration konfiguriert haben, können Sie das folgende Verfahren überspringen.

Konfigurieren der SSL-Interception für HTTPS-Datenverkehr Gehen Sie folgendermaßen vor, um SSL-Interception für HTTPS-Datenverkehr zu konfigurieren:

1. Binden Sie ein Zertifizierungsstellen-Schlüsselpaar an den virtuellen Proxyserver.
2. Aktivieren Sie das standardmäßige SSL-Profil.
3. Erstellen Sie ein Front-End-SSL-Profil, binden Sie es an den virtuellen Proxyserver und aktivieren Sie SSL-Interception im Front-End-SSL-Profil.

So binden Sie mit der Citrix SWG-CLI ein Zertifizierungsstellen-Schlüsselpaar an den virtuellen Proxyserver:

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

So konfigurieren Sie ein Front-End-SSL-Profil mit der Citrix SWG-CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl parameter -defaultProfile ENABLED

add ssl profile <name> -sslInterception ENABLED -ssliMaxSessPerServer <
    positive_integer>
<!--NeedCopy-->
```

So binden Sie ein Front-End-SSL-Profil mit der Citrix SWG-CLI an einen virtuellen Proxyserver

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Konfigurieren einer URL-Liste durch Importieren eines URL-Sets für HTTP-Datenverkehr Hinweise zum Konfigurieren eines URL-Sets für HTTP-Datenverkehr finden Sie unterURL-Satz.

Explizite Subdomain-Übereinstimmung durchführen Sie können jetzt eine explizite Subdomain-Übereinstimmung für einen importierten URL-Satz durchführen. Dazu wird dem Befehl **`import`** `policy URLset` ein neuer Parameter subdomainExactMatch hinzugefügt.

Wenn Sie den Parameter aktivieren, führt der URL-Filteralgorithmus eine explizite Subdomain-Übereinstimmung aus. Wenn beispielsweise die eingehende URL `news.example.com` ist und der Eintrag im URL-Satz, `example.com`erkennt der Algorithmus die URLs nicht als übereinstimmend.

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiel

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

Konfigurieren eines URL-Sets für HTTPS-Datenverkehr So konfigurieren Sie einen URL-Satz für HTTPS-Datenverkehr mit der Citrix SWG-CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiel:

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

So konfigurieren Sie einen URL-Satz für HTTPS-Datenverkehr mit dem Citrix SWG-Assistenten
Citrix empfiehlt, dass Sie den Citrix SWG-Assistenten als bevorzugte Option zum Konfigurieren einer URL-Liste verwenden. Verwenden Sie den Assistenten, um einen benutzerdefinierten URL-Satz zu importieren und an eine Responderrichtlinie zu binden.

1. Melden Sie sich bei der **Citrix SWG-Appliance** an und navigieren Sie zu **Secured Web Gateway > URL-Filter > URL-Listen.**
2. Klicken Sie im Detailbereich auf **Hinzufügen.**
3. Geben Sie auf der Seite **URL-Listenrichtlinie** den Richtliniennamen an.
4. Wählen Sie eine Option aus, um einen URL-Satz zu importieren.
5. Aktivieren Sie auf der Registerkarte **URL-Listenrichtlinie** das Kontrollkästchen **URL-Satz importieren**, und geben Sie die folgenden URL-Set-Parameter an.

a) URL-Set-Name —Name des benutzerdefinierten URL-Sets.
b) URL: Die Webadresse des Standorts, an dem auf den URL-Satz zugegriffen werden soll.
c) Überschreiben —Überschreiben Sie einen zuvor importierten URL-Satz.
d) Trennzeichen: Eine Zeichenfolge, die einen CSV-Dateidatensatz begrenzt.
e) Zeilentrenner —In der CSV-Datei verwendetes Zeilentrenner.
f) Intervall —Intervall in Sekunden, abgerundet auf die nächste Anzahl von Sekunden, die 15 Minuten entspricht, bei der der URL-Satz aktualisiert wird.
g) Private Set: Option, um das Exportieren des URL-Sets zu verhindern.
h) Kanarische URL —Interne URL zum Testen, ob der Inhalt des URL-Sets vertraulich behandelt werden soll. Die maximale Länge der URL beträgt 2047 Zeichen.

6. Wählen Sie eine Responder-Aktion aus der Dropdownliste aus.
7. Klicken Sie auf **Erstellen** und **Schließen**.

Konfigurieren eines privaten URL-Sets Wenn Sie einen privaten URL-Satz konfigurieren und den Inhalt vertraulich behandeln, kennt der Netzwerkadministrator möglicherweise die in der Sperrliste enthaltenen URLs nicht. In solchen Fällen können Sie eine Canary-URL konfigurieren und sie dem URL-Satz hinzufügen. Mit der Canary-URL kann der Administrator den privaten URL-Satz für jede Lookup-Anfrage anfordern. Beschreibungen der einzelnen Parameter finden Sie im Assistentenabschnitt.

So importieren Sie einen URL-Satz mit der Citrix SWG-CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiel:

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

Importierte URL-Satz anzeigen

Sie können nun zusätzlich zu den hinzugefügten URL-Sets importierte URL-Sets anzeigen. Dazu wird dem Befehl show “urlset ein neuer Parameter “importiert hinzugefügt. Wenn Sie diese Option aktivieren, zeigt die Appliance alle importierten URL-Sets an und unterscheidet die importierten URL-Sets von den hinzugefügten URL-Sets.

Geben Sie an der Eingabeaufforderung Folgendes ein:

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


Beispiel

```
show policy urlset -imported
```

Auditprotokoll-Messaging konfigurieren

Mit der Auditprotokollierung können Sie eine Bedingung oder eine Situation in einer beliebigen Phase des URL-Listenprozesses überprüfen. Wenn eine Citrix ADC-Appliance eine eingehende URL empfängt und die Responderrichtlinie über einen erweiterten Richtlinienausdruck URL-Sets verfügt, erfasst das Auditprotokoll-Feature URL-Set-Informationen in der URL und speichert die Details als Protokollnachricht für jedes Ziel, das durch die Auditprotokollierung zulässig ist.

1. Die Protokollmeldung enthält die folgenden Informationen:
2. Zeitstempel.
3. Protokollnachrichtentyp.
4. Die vordefinierten Protokollstufen (Critical, Error, Notice, Warning, Informational, Debug, Alert und Emergency).
5. Protokollieren von Nachrichteninformationen, wie URL-Set-Name, Richtlinienaktion, URL.

Um die Auditprotokollierung für URL-Listenfunktion zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

1. Auditprotokoll aktivieren.
2. Aktion “Auditprotokoll erstellen”
3. Legen Sie die Richtlinie für URL-Listen-Responder mit Auditprotokoll-Nachrichtenaktion fest.

Weitere Informationen finden Sie unter Auditprotokollierung.

URL-Muster-Semantik

April 26, 2021

Die folgende Tabelle zeigt die URL-Muster, die zum Angeben der Liste der Seiten verwendet werden sollen, die gefiltert werden sollen. Beispielsweise entspricht das Muster www.example.com/bar nur einer Seite unter www.example.com/bar. Um alle Seiten zu vergleichen, deren URL mit ‘www.example.com/bar’beginnt, fügen Sie am Ende der URL ein Sternchen (*) hinzu.

Semantik für URL-Muster, um Metadatenzuordnung anzupassen

Die Musterübereinstimmende Semantik ist in einem Tabellenformat verfügbar. Weitere Informationen finden Sie unter der Seite Mustersemantik.

Zuordnungs-URL-Kategorien

April 26, 2021

Eine Liste von Drittanbieterkategorien und Kategoriegruppen. Weitere Informationen finden Sie auf der Seite URL-Kategoriezuordnung.

Anwendungsfall: URL-Filterung mithilfe benutzerdefinierter URL-Sets

April 26, 2021

Wenn Sie ein Unternehmenskunden sind, der nach einer Möglichkeit zum Steuern des Zugriffs auf bestimmte Websites und Websitekategorien sucht, können Sie dies tun, indem Sie einen benutzerdefinierten URL-Satz verwenden, der an eine Responderrichtlinie gebunden ist. Die Netzwerkinfrastruktur Ihres Unternehmens kann einen URL-Filter verwenden, um den Zugriff auf bösartige oder gefährliche Websites wie Websites mit Erwachsenen, Gewalt, Spielen, Drogen, Politik oder Jobportalen zu blockieren. Zusätzlich zum Filtern der URLs können Sie eine benutzerdefinierte Liste von URLs erstellen und in die SWG-Appliance importieren. Beispielsweise könnten die Richtlinien Ihrer Organisation dazu führen, den Zugriff auf bestimmte Websites wie soziale Netzwerke, Shoppingportale und Jobportale zu blockieren.

Jede URL in der Liste kann eine benutzerdefinierte Kategorie in Form von Metadaten enthalten. Die Organisation kann die Liste der URLs als URL-Satz auf der Citrix SWG-Appliance hosten und die Appliance so konfigurieren, dass sie den Satz regelmäßig aktualisiert, ohne dass ein manueller Eingriff erforderlich ist.

Nach der Aktualisierung des Satzes erkennt die Citrix ADC-Appliance automatisch die Metadaten, und die Responderrichtlinie verwendet die URL-Metadaten (Kategoriedetails), um die eingehende URL auszuwerten und eine Aktion wie Zulassen, Blockieren, Umleiten oder Benachrichtigen des Benutzers anzuwenden.

Um diese Konfiguration in Ihrem Netzwerk zu implementieren, können Sie die folgenden Aufgaben ausführen:

1. Importieren eines benutzerdefinierten URL-Sets
2. Hinzufügen eines benutzerdefinierten URL-Sets
3. Konfigurieren einer benutzerdefinierten URL-Liste im Citrix SWG-Assistenten

So importieren Sie einen benutzerdefinierten URL-Satz mit der Citrix SWG-CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

```
Richtlinie importieren urlset test1 — url http://10.78.79.80/alytra/
    top-1k.csv
```

So fügen Sie mit der Citrix SWG-CLI einen benutzerdefinierten URL-Satzhinzu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

add urlset <urlset_name>

```
Add urlset test1
```

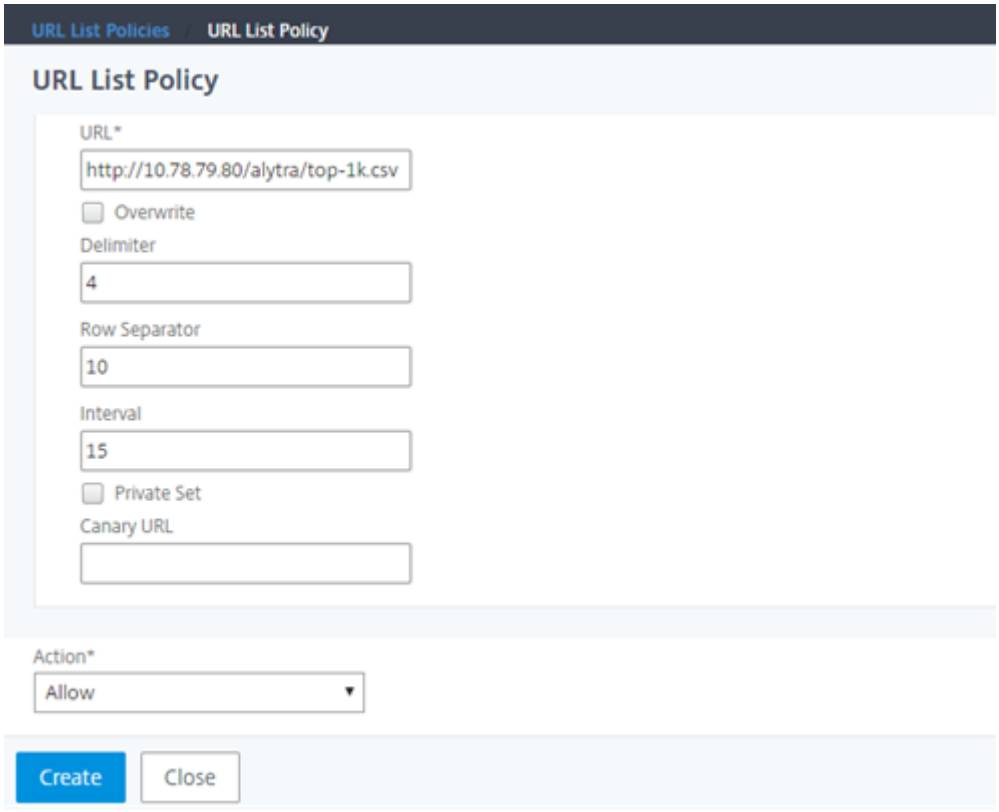
Konfigurieren einer URL-Liste mit dem Citrix SWG-Assistenten

Citrix empfiehlt, dass Sie den Citrix SWG-Assistenten als bevorzugte Option zum Konfigurieren einer URL-Liste verwenden. Verwenden Sie den Assistenten, um einen benutzerdefinierten URL-Satz zu importieren und an eine Responderrichtlinie zu binden.

1. Melden Sie sich bei der **Citrix SWG-Appliance** an und navigieren Sie zu **Secured Web Gateway > URL-Filter > URL-Listen.**
2. Klicken Sie im Detailbereich auf **Hinzufügen.**
3. Geben Sie auf der Seite **URL-Listenrichtlinie** den Richtliniennamen an.
4. Wählen Sie eine Option aus, um einen URL-Satz zu importieren.
5. Aktivieren Sie auf der Registerkarte **URL-Listenrichtlinie** das Kontrollkästchen **URL-Satz importieren**, und geben Sie die folgenden URL-Set-Parameter an.

    a) URL-Set-Name —Name des benutzerdefinierten URL-Sets.
    b) URL: Die Webadresse des Standorts, an dem auf den URL-Satz zugegriffen werden soll.
    c) Überschreiben —Überschreiben Sie einen zuvor importierten URL-Satz.
    d) Trennzeichen: Eine Zeichenfolge, die einen CSV-Dateidatensatz begrenzt.
    e) Zeilentrenner —In der CSV-Datei verwendetes Zeilentrenner.
    f) Intervall—Intervall in Sekunden, abgerundet auf die nächsten 15 Minuten, in denen die URL-Einstellung aktualisiert wird.
    g) Private Set: Option, um das Exportieren des URL-Sets zu verhindern.
    h) Canary-URL—Interne URL zum Testen, ob der Inhalt des URLs vertraulich behandelt werden soll. Die maximale Länge der URL beträgt 2047 Zeichen.

6. Wählen Sie eine Responder-Aktion aus der Dropdownliste aus.
7. Klicken Sie auf **Erstellen** und **Schließen**.



Metadatensemantik für benutzerdefinierte URL-Sets

Um einen benutzerdefinierten URL-Satz zu importieren, fügen Sie die URLs zu einer Textdatei hinzu und binden Sie sie an eine Responderrichtlinie, um URLs für soziale Netzwerke zu blockieren.

Im Folgenden finden Sie Beispiele für URLs, die Sie der Textdatei hinzufügen können:

cnn.com,News

bbc.com,News

google.com,Search Engine

yahoo.com,Search Engine

facebook.com,Social Media

twitter.com,Social Media

Konfigurieren einer Responderrichtlinie zum Blockieren von Social-Media-URLs mit der 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\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-Kategorisierung

April 26, 2021

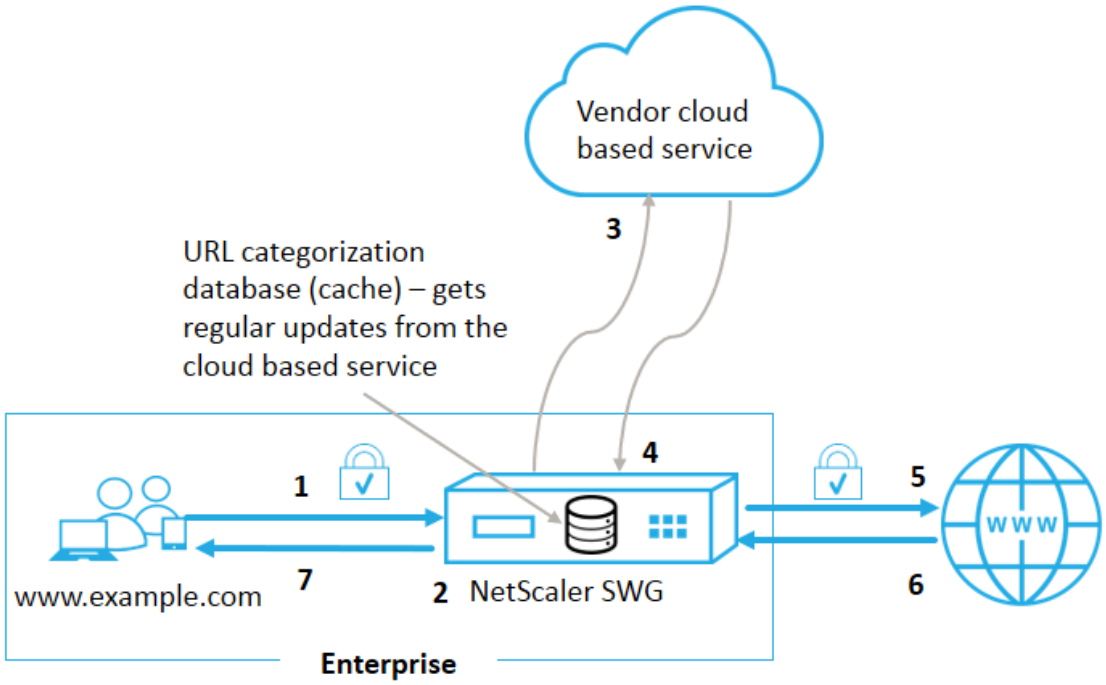
Die URL-Kategorisierung schränkt den Benutzerzugriff auf bestimmte Websites und Websitekategorien ein. Als abonnierter Dienst, der von Citrix Secure Web Gateway (SWG) angeboten wird, ermöglicht es Unternehmenskunden, den Webverkehr mithilfe einer kommerziellen Kategorisierungsdatenbank zu filtern. Die Datenbank verfügt über eine große Anzahl (Milliarden) von URLs, die in verschiedene Kategorien eingeteilt sind, wie soziale Netzwerke, Glücksspiele, Erwachseneninhalte, neue Medien und Shopping. Zusätzlich zur Kategorisierung verfügt jede URL über eine Reputationsbewertung, die auf dem historischen Risikoprofil der Website basiert. Um Ihren Datenverkehr zu filtern, können Sie erweiterte Richtlinien basierend auf Kategorien, Kategoriegruppen (z. B. Terrorismus, illegale Drogen) oder Scores für Site-Reputation konfigurieren.

Beispielsweise können Sie den Zugriff auf gefährliche Websites wie Websites sperren, die bekanntermaßen mit Malware infiziert sind, und selektiv den Zugriff auf Inhalte wie Inhalte für Erwachsene oder Unterhaltungs-Streaming-Medien für Unternehmensbenutzer einschränken. Sie können auch die Transaktionsdetails des Benutzers und die Details des ausgehenden Datenverkehrs erfassen, um die Analyse des Webverkehrs auf dem Citrix ADM-Server zu überwachen.

Citrix ADC lädt Daten vom vorkonfigurierten `NetSTAR` Gerät hoch oder lädt sie herunter `nsv10.netstar-inc.com` und `incompasshybridpc.netstar-inc.com` wird standardmäßig als Cloud-Host für Cloud-Kategorisierungsanfragen verwendet. Die Appliance verwendet ihre NSIP-Adresse als Quell-IP-Adresse und 443 als Zielport für die Kommunikation.

Funktionsweise der URL-Kategorisierung

Die folgende Abbildung zeigt, wie Citrix SWG-URL-Kategorisierungsdienst in eine kommerzielle URL-Kategorisierungsdatenbank und Cloud-Dienste für häufige Updates integriert ist.



Die Komponenten interagieren wie folgt:

1. Ein Client sendet eine Internet-gebundene URL-Anforderung.
2. Der Citrix SWG-Proxy wendet eine Richtlinienerzwingung auf die Anforderung an, basierend auf den Kategoriedetails (z. B. Kategorie, Kategoriegruppe und Site-Reputation-Bewertung), die aus der URL-Kategorisierungsdatenbank abgerufen wurden. Wenn die Datenbank die Kategoriedetails zurückgibt, springt der Prozess zu Schritt 5.
3. Wenn die Datenbank die Kategorisierungsdetails übersieht, wird die Anforderung an einen cloudbasierten Suchdienst gesendet, der von einem Anbieter der URL-Kategorisierung verwaltet wird. Die Appliance wartet jedoch nicht auf eine Antwort. Stattdessen wird die URL als nicht kategorisiert markiert und eine Richtliniendurchsetzung durchgeführt (Sprung zu Schritt 5). Die Appliance überwacht weiterhin das Feedback der Cloud-Abfrage und aktualisiert den Cache, sodass zukünftige Anforderungen von der Cloud-Suche profitieren können.
4. Die SWG-Appliance empfängt die URL-Kategoriedetails (Kategorie, Kategoriegruppe und Reputationsbewertung) vom cloudbasierten Dienst und speichert sie in der Kategorisierungsdatenbank.
5. Die Richtlinie erlaubt die URL und die Anforderung wird an den Ursprungsserver gesendet. Andernfalls wird eine benutzerdefinierte HTML-Seite von der Appliance gelöscht, umgeleitet oder reagiert.
6. Der Ursprungsserver antwortet mit den angeforderten Daten an die SWG-Appliance.
7. Die Appliance sendet die Antwort an den Client.

Anwendungsfall: Internetnutzung im Rahmen von Corporate Compliance für Unternehmen

Sie können die URL-Filter-Funktion verwenden, um Compliance-Richtlinien zu erkennen und zu implementieren, um Websites zu blockieren, die gegen die Unternehmenskonformität verstoßen. Dies können Websites wie Erwachsene, Streaming-Medien, soziale Netzwerke sein, die als unproduktiv angesehen werden oder eine übermäßige Internetbandbreite in einem Unternehmensnetzwerk verbrauchen. Die Sperrung des Zugriffs auf diese Websites kann die Produktivität der Mitarbeiter verbessern, die Betriebskosten für die Bandbreitennutzung senken und den Gemeinkosten des Netzwerkverbrauchs reduzieren.

Voraussetzungen

Die URL-Kategorisierungsfunktion funktioniert nur auf einer Citrix SWG-Plattform, wenn sie über einen optionalen Abonnementdienst mit URL-Filterfunktionen und Bedrohungsinformationen für Citrix Secure Web Gateway verfügt. Mit dem Abonnement können Kunden die neuesten Bedrohungskategorien für Websites herunterladen und diese Kategorien dann auf dem Secure Web Gateway durchsetzen. Das Abonnement ist sowohl für Hardware-Appliances als auch für Software (VPX) von Secure Web Gateway verfügbar.
Bevor Sie das Feature aktivieren und konfigurieren, müssen Sie die folgenden Lizenzen installieren:
CNS_WEBF_SSERVER_Retail.lic

CNS_XXXXX_SERVER_SWG_Retail.lic.

Wobei XXXXX der Plattformtyp ist, zum Beispiel: V25000

Ausdrücke der Responderrichtlinie

In der folgenden Tabelle sind die verschiedenen Richtlinienausdrücke aufgeführt, mit denen Sie überprüfen können, ob eine eingehende URL zugelassen, umgeleitet oder blockiert werden muss.

1. <text>. URL_CATEGORIZE (<min_reputation>, <max_reputation>) - Gibt einURL_CATEGORY Objekt zurück. Wenn größer als 0<min_reputation> ist, enthält das zurückgegebene Objekt keine Kategorie mit einer niedrigeren Reputation als<min_reputation> . Wenn größer als 0<max_reputation> ist, enthält das zurückgegebene Objekt keine Kategorie mit einer höheren Reputation als<max_reputation> . Wenn die Kategorie nicht rechtzeitig aufgelöst wird, wird der undef-Wert zurückgegeben.
2. <url_category>. CATEGORY() - Gibt die Kategoriezeichenfolge für dieses Objekt zurück. Wenn die URL keine Kategorie hat oder wenn die URL falsch formatiert ist, lautet der zurückgegebene Wert “Unbekannt”.

3. <url_category>. CATEGORY_GROUP() - Gibt einen String zurück, der die Kategoriegruppe des Objekts identifiziert. Dies ist eine Gruppierung von Kategorien auf höherer Ebene, die bei Operationen nützlich ist, die weniger detaillierte Informationen über die URL-Kategorie erfordern. Wenn die URL keine Kategorie hat oder wenn die URL falsch formatiert ist, lautet der zurückgegebene Wert "Unbekannt".
4. <url_category>. REPUTATION() - Gibt den Reputationswert als Zahl von 0 bis 5 zurück, wobei 5 den risikoreichsten Ruf angibt. Wenn die Kategorie Unbekannt lautet, beträgt der Reputationswert 1.

Arten von Richtlinien:

1. Richtlinie zum Auswählen von URLs, die sich in der Kategorie Suchmaschine befinden -add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL). URL_CATEGORIZE(0,0). CATEGORY().EQ("Search Engine")
2. Richtlinie zum Auswählen von URLs, die sich in der Kategorie Erwachsene befinden -add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL). URL_CATEGORIZE(0,0). CATEGORY_GROUP().EQ("Adult")'
3. Richtlinie zum Auswählen von Anfragen für Suchmaschinen-URLs mit einer Reputationsbewertung unter 4 -add responder policy p2 'HTTP.REQ.HOSTNAME.APPEND (HTTP. REQ.URL).URL_CATEGORIZE(4,0).HAS_CATEGORY("Search Engine")
4. Richtlinie zum Auswählen von Anfragen für Suchmaschinen- und Shopping-URLs -add responder policy p3 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL). URL_CATEGORIZE(0,0).CATEGORY().EQ ("good_categories")
5. Richtlinie zum Auswählen von Anfragen für Suchmaschinen-URLs mit einer Reputationsbewertung von mindestens 4 -add responder policy p5 'CLIENT.SSL .DETECTED_DOMAIN.URL_CATEGORIZE(4,0). CATEGORY().EQ("Search Engines")
6. Richtlinie zum Auswählen von URLs, die sich in der Kategorie Suchmaschine befinden und mit einem URL-Set vergleichen - ' 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-Richtlinientypen

Es gibt zwei Arten von Richtlinien, die in der URL-Kategorisierungsfunktion verwendet werden, und jeder dieser Richtlinientypen wird im Folgenden erläutert:

Richtlinientyp	Beschreibung
URL-Kategorie	Kategorisieren Sie den Web-Traffic und lassen Sie den Datenverkehr basierend auf den Blockaden der Auswertung zu.
URL-Reputationsbewertung	Bestimmt die Reputationsbewertung der Website und ermöglicht es Ihnen, den Zugriff basierend auf dem vom Administrator festgelegten Schwellenwert für die Reputationsbewertung zu steuern.

URL-Kategorisierung konfigurieren

Gehen Sie folgendermaßen vor, um die URL-Kategorisierung auf einer Citrix SWG-Appliance zu konfigurieren:

1. URL-Filterung aktivieren.
2. Konfigurieren Sie einen Proxyserver für den Webverkehr.
3. Konfigurieren Sie SSL-Interception für Webverkehr im expliziten Modus.
4. Konfigurieren Sie Shared Memory, um den Cache-Speicher zu begrenzen.
5. Konfigurieren Sie URL-Kategorisierungsparameter.
6. Konfigurieren Sie die URL-Kategorisierung mit dem Citrix SWG-Assistenten.
7. Konfigurieren Sie URL-Kategorisierungsparameter mit dem SWG-Assistenten.
8. Konfigurieren des Seeddatenbankpfads und des Cloud-Servernamens

Schritt 1: URL-Filterung aktivieren

Um die URL-Kategorisierung zu aktivieren, aktivieren Sie die URL-Filterfunktion und aktivieren Sie Modi für die URL-Kategorisierung.

So aktivieren Sie die URL-Kategorisierung mit der Citrix SWG: CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Schritt 2: Konfigurieren eines Proxyservers für Webverkehr im expliziten Modus

Die Citrix SWG-Appliance unterstützt transparente und explizite virtuelle Proxyserver. Gehen Sie folgendermaßen vor, um einen virtuellen Proxyserver für SSL-Datenverkehr im expliziten Modus zu kon-

figurieren:

1. Fügen Sie einen Proxyserver hinzu.
2. Binden Sie eine SSL-Richtlinie an den Proxyserver.

So fügen Sie mit der Citrix SWG-CLI einen Proxyserver hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiel:

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

Binden einer SSL-Richtlinie an einen virtuellen Proxyserver mit der Citrix SWG-CLI

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

Schritt 3: Konfigurieren von SSL-Interception für HTTPS-Datenverkehr

Gehen Sie folgendermaßen vor, um SSL-Interception für HTTPS-Datenverkehr zu konfigurieren:

1. Binden Sie ein Zertifizierungsstellen-Schlüsselpaar an den virtuellen Proxyserver.
2. Konfigurieren Sie das standardmäßige SSL-Profil mit SSL-Parametern.
3. Binden Sie ein Front-End-SSL-Profil an den virtuellen Proxyserver und aktivieren Sie SSL-Interception im Front-End-SSL-Profil.

So binden Sie ein Zertifizierungsstellen-Schlüsselpaar mit der Citrix SWG-CLI an den virtuellen Proxyserver

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

So konfigurieren Sie das standardmäßige SSL-Profil mit der Citrix SWG-CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


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

Binden eines Front-End-SSL-Profils an einen virtuellen Proxyserver mit der Citrix SWG-CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Schritt 4: Konfigurieren von Shared Memory, um den Cache-Speicher zu begrenzen

So konfigurieren Sie Shared Memory zur Begrenzung des Cache-Speichers mit der Citrix SWG-CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Dabei wird die für das Zwischenspeichern konfigurierte Speichergrenze auf 10 MB festgelegt.

Schritt 5: Konfigurieren von URL-Kategorisierungsparametern

So konfigurieren Sie die URL-Kategorisierungsparameter mit der Citrix SWG-CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiel:

```
Set urlfiltering parameter  – urlfilt_hours_betweenDB_updates 20
<!--NeedCopy-->
```

Schritt 6: Konfigurieren der URL-Kategorisierung mit dem Citrix SWG-Assistenten

So konfigurieren Sie die URL-Kategorisierung mit der Citrix SWG-GUI

1. Melden Sie sich bei der Citrix SWG-Appliance an, und navigieren Sie zur Seite **Secured Web Gateway**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:

a) Klicken Sie auf **Secured Web Gateway Wizard**, um eine neue Konfiguration zu erstellen.
b) Wählen Sie eine vorhandene Konfiguration aus, und klicken Sie auf **Bearbeiten**.

3. Klicken Sie im Abschnitt **URL-Filterung** auf **Bearbeiten**.
4. Aktivieren Sie das Kontrollkästchen **URL-Kategorisierung**, um die Funktion zu aktivieren.
5. Wählen Sie eine **URL-Kategorisierungs** richtlinie aus, und klicken Sie auf **Binden** .
6. Klicken Sie auf **Weiter** und dann **Fertig**.

Weitere Informationen zur URL-Kategorisierungsrichtlinie finden Sie unterErstellen einer URL-Kategorisierungsrichtlinie.

Schritt 7: Konfigurieren von URL-Kategorisierungsparametern mit dem SWG-Assistenten

So konfigurieren Sie URL-Kategorisierungsparameter mit der Citrix SWG-GUI

1. Melden Sie sich bei der **Citrix SWG-** Appliance an, und navigieren Sie zu **Secured Web Gateway > URL-Filterung** .
2. Klicken Sie auf der Seite **URL-Filterung** auf den Link **URL-Filtereinstellungen ändern** .
3. Geben **Sie auf der Seite URL-Filterparameter konfigurieren** die folgenden Parameter an.

a) Stunden zwischen DB-Updates. URL-Filterung Stunden zwischen Datenbankaktualisierungen. Mindestwert: 0 und Maximalwert: 720.
b) Tageszeit für die Aktualisierung der DB. URL-Filterung Tageszeit für die Aktualisierung der Datenbank.
c) Cloud-Host. Der URL-Pfad des Cloud-Servers.
d) Seed-DB-Pfad. Der URL-Pfad des Seed-Datenbank-Lookup-Servers.

4. Klicken Sie auf **OK** und **schließen**.

Beispielkonfiguration:

```
enable ns feature LB CS SSL IC RESPONDER AppFlow URLFiltering

enable ns mode FR L3 Edge USNIP PMTUD

set ssl profile ns_default_ssl_profile_frontend -denySSLReneg NONSECURE
    -sslInterception ENABLED -ssliMaxSessPerServer 100

add ssl certKey swg_ca_cert -cert ns_swg_ca.crt -key ns_swg_ca.key

set cache parameter -memLimit 100

add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180

add responder action act1 respondwith ""HTTP/1.1 200 OK\r\n\r\n" + http
   .req.url.url_categorize(0,0).reputation + "\n""

```



```
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-->
```

Konfigurieren des Seeddatenbankpfads und des Cloud-Servernamens

Sie können nun den Seed-Datenbankpfad und den Namen des Cloud-Lookup-Servers für die manuelle Einstellung des Cloud-Lookup-Servers und des Seed-Datenbankpfads konfigurieren. Dazu werden zwei neue Parameter, CloudHost und SeedDBPath, dem Befehl URL-Filterparameter hinzugefügt.

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiel

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

Die Kommunikation zwischen einer Citrix ADC Appliance und erfordert NetSTAR möglicherweise einen Domänennamenserver. Sie können mit einer einfachen Konsole oder Telnet-Verbindung von

der Appliance aus testen.

Beispiel:

```
root@ns# telnet nsv10.netstar-inc.com 443
Trying 1.1.1.1...
Connected to nsv10.netstar-inc.com.
Escape character is '^]'.

root@ns# telnet incompasshybridpc.netstar-inc.com 443
Trying 10.10.10.10...
Connected to incompasshybridpc.netstar-inc.com.
Escape character is '^]'.
<!--NeedCopy-->
```

Auditprotokoll-Messaging konfigurieren

Mit der Auditprotokollierung können Sie eine Bedingung oder eine Situation in einer beliebigen Phase des URL-Kategorisierungsprozesses überprüfen. Wenn eine Citrix ADC Appliance eine eingehende URL erhält und die Responder Policy einen URL-Filterausdruck hat, sammelt die Überwachungsprotokoll-funktion URL-Set-Informationen in der URL und speichert sie als Protokollmeldungen für jedes Ziel, das durch die Audit-Protokollierung zulässig ist.

- Quell-IP-Adresse (die IP-Adresse des Clients, der die Anforderung gestellt hat).
- Ziel-IP-Adresse (die IP-Adresse des angeforderten Servers).
- Angeforderte URL, die das Schema, den Host und den Domänennamen (http://www.example.com.
- URL-Kategorie, die das URL-Filterframework zurückgibt.
- URL-Kategoriegruppe, die vom URL-Filterframework zurückgegeben wurde.
- URL-Reputationsnummer, die vom URL-Filterframework zurückgegeben wurde.
- Von der Richtlinie durchgeführte Auditprotokollaktion.

Um die Überwachungsprotokollierung für die URL-Liste zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

1. Auditprotokoll aktivieren.
2. Aktion “Auditprotokoll erstellen”
3. Legen Sie die Richtlinie für URL-Listen-Responder mit Auditprotokoll-Nachrichtenaktion fest.

Weitere Informationen finden Sie unter Auditprotokollierung.

Speichern von Fehler mit SYSLOG-Messaging

Bei einem Ausfall auf Systemebene verwendet die Citrix ADC-Appliance in jeder Phase des URL-Filter-Prozesses den Auditprotokollmechanismus, um Protokolle in der Datei ns.log zu speichern.

Die Fehler werden als Textnachrichten im SYSLOG-Format gespeichert, sodass ein Administrator sie später in chronologischer Reihenfolge des Ereignisses anzeigen kann. Diese Protokolle werden auch zur Archivierung an einen externen SYSLOG-Server gesendet. Weitere Informationen finden Sie unter Artikel CTX229399.

Wenn beispielsweise ein Fehler auftritt, wenn Sie das URL-Filter-SDK initialisieren, wird die Fehlermeldung im folgenden Nachrichtenformat gespeichert.

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

Die Citrix ADC-Appliance speichert die Fehlermeldungen in vier verschiedenen Fehlerkategorien:

- **Download-Versagen**. Wenn ein Fehler auftritt, wenn Sie versuchen, die Kategorisierungsdatenbank herunterzuladen.
- **Integrationsfehler**. Wenn ein Fehler auftritt, wenn Sie ein Update in die vorhandene Kategorisierungsdatenbank integrieren.
- **Fehler bei der Initialisierung** Wenn ein Fehler auftritt, wenn Sie die URL-Kategorisierungsfunktion initialisieren, Kategorisierungsparameter festlegen oder einen Kategorisierungsdienst beenden.
- **Fehler beim Abrufen**. Wenn ein Fehler auftritt, wenn die Appliance die Kategorisierungsdetails der Anforderung abruft.

URL-Kategorisierungsergebnis über die Befehlsschnittstelle anzeigen

Mit der URL-Kategorisierung können Sie eine URL eingeben und Kategorisierungsergebnisse (z. B. Kategorie, Gruppe und Reputationsbewertung) aus der NetStar-URL-Kategorisierungsdatenbank eines Drittanbieters abrufen.

Wenn Sie eine URL eingeben, ruft die URL-Filterfunktion das Kategorisierungsergebnis auf der Befehlsschnittstelle ab und zeigt es an. Wenn Sie weitere URLs eingeben, schließt die Appliance ältere URLs aus der Liste aus und zeigt das Ergebnis für die letzten drei URLs an.

Um das Ergebnis der URL-Kategorie bis zu drei URLs anzuzeigen, führen Sie die folgenden Schritte aus:

1. URL-Kategorisierungs-URL hinzufügen
2. Anzeigen von URL-Kategorisierungsdetails bis zu drei URLs
3. Löschen Sie URL-Kategorisierungsdaten.

So fügen Sie URL-Filter-Kategorisierungs-URL hinzu

Um eine URL hinzuzufügen und ihre Kategorisierungsdetails abzurufen, gehen Sie folgendermaßen vor: Geben Sie

an der Eingabeaufforderung Folgendes ein:

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

Beispiel:

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

So zeigen Sie URL-Kategorisierungsdetails bis zu drei URLs an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
> show urlfiltering categorization
```

Beispiel:

```
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-->
```

Beispielkonfiguration:

```
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
```



```
Done

add urlfiltering categorization -url www.in.gr
Done
show urlfiltering categorization
Url: http://www.google.com      Categorization: Search Engines &
   Portals,Search,1
Url: http://www.citrix.com      Categorization: Computing & Internet,
   Computing & Internet,1
Url: http://www.in.gr   Categorization: Search Engines & Portals,Search
   ,1 Done
<!--NeedCopy-->
```

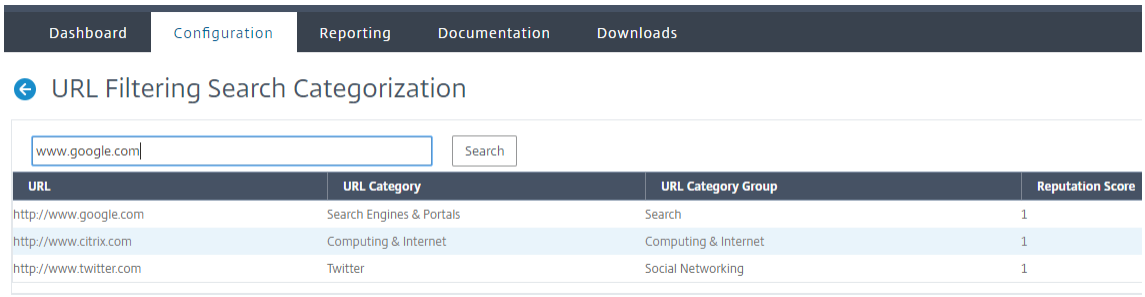
So löschen Sie URL-Kategorisierungsergebnis

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
clear urlfiltering categorization
done

show urlfiltering categorization
done
<!--NeedCopy-->
```

URL-Kategorisierungsergebnis über die GUI-Schnittstelle anzeigen

1. Erweitern Sie im Navigationsbereich **Secure Web Gateway** > **URL-Filterung**.
2. Klicken Sie im Detailbereich im Abschnitt **Extras** auf den Link **URL-Filtersuchkategorisierung**.
3. Geben Sie auf der Seite **Kategorisierung der URL-Filtersuche** eine URL-Anforderung ein, und klicken Sie auf **Suchen**.



4. Die Appliance zeigt das Kategorieergebnis für die angeforderte URL und für die beiden vorherigen URL-Anforderungen an.

Sicherheitskonfiguration

April 29, 2020

Mit der Funktion Sicherheitskonfiguration können Sie die Sicherheitsrichtlinie zum Filtern von URLs konfigurieren. Der Artikel "URL Reputation Score"enthält Details zu Konzepten und Konfiguration für das Filtern von URLs basierend auf der Reputationsbewertung.

Sie können ICAP für die Remote-Inhaltsprüfung verwenden.

URL-Reputationsbewertung

Die URL-Kategorisierungsfunktion verwendet den URL-Reputationswert, um richtlinienbasierte Kontrolle zu bieten, um hochriskante Websites zu blockieren. Weitere Informationen finden Sie unter URL-Reputationsbewertung.

Verwenden von ICAP für die Remote-Content-Inspektion

HTTPS-Datenverkehr wird abgefangen, entschlüsselt und an die ICAP-Server zur Inhaltsüberprüfung für Antischadwareprüfungen und zur Verhinderung von Datenlecks gesendet.

URL-Reputationsbewertung

April 26, 2021

Die URL-Kategorisierungsfunktion bietet richtlinienbasierte Steuerung, um URLs in der Sperrliste einzuschränken. Sie können den Zugriff auf Websites basierend auf URL-Kategorie, Reputationsbewertung oder URL-Kategorie und Reputationsbewertung steuern. Wenn ein Netzwerkadministrator einen Benutzer überwacht, der auf hochriskante Websites zugreift, kann er eine Responderrichtlinie verwenden, die an die URL-Reputationsbewertung gebunden ist, um solche riskanten Websites zu blockieren.

Nach Erhalt einer eingehenden URL-Anforderung ruft die Appliance die Kategorie- und Reputationsbewertung aus der URL-Kategorisierungsdatenbank ab. Basierend auf der von der Datenbank zurückgegebenen Reputationsbewertung weist die Appliance Websites eine Reputationsbewertung zu. Der Wert kann zwischen 1 und 4 liegen, wobei 4 der risikoreichste Typ von Websites ist, wie in der folgenden Tabelle dargestellt.

URL-Reputationsbewertung	Reputationskommentar
1	Saubere Website
2	Unbekannte Website
3	Potenziell gefährlich oder mit einer gefährlichen Site verbunden
4	Bösartige Website

Anwendungsfall: Filtern nach URL-Reputationsbewertung

Betrachten Sie eine Unternehmensorganisation mit einem Netzwerkadministrator, der Benutzertransaktionen und Netzwerkbandbreitenverbrauch überwacht. Wenn Malware in das Netzwerk gelangen kann, muss der Administrator die Datensicherheit verbessern und den Zugriff auf bösartige und gefährliche Websites kontrollieren, die auf das Netzwerk zugreifen. Um das Netzwerk vor solchen Bedrohungen zu schützen, kann der Administrator die URL-Filterfunktion so konfigurieren, dass der Zugriff nach URL-Reputationsbewertung zugelassen oder verweigert wird.

Weitere Hinweise zur Überwachung des ausgehenden Datenverkehrs und der Benutzeraktivitäten im Netzwerk finden Sie unterSWG-Analysen.

Wenn ein Mitarbeiter der Organisation versucht, auf eine Website für soziale Netzwerke zuzugreifen, erhält die SWG-Appliance eine URL-Anforderung und fragt die URL-Kategorisierungsdatenbank ab, um die URL-Kategorie als soziale Netzwerke und eine Reputationsbewertung 3 abzurufen, die auf eine potenziell gefährliche Website hinweist. Die Appliance überprüft dann die vom Administrator konfigurierte Sicherheitsrichtlinie, z. B. den Zugriff auf Websites mit einer Reputationsbewertung von 3 oder mehr blockieren. Anschließend wendet er die Richtlinienaktion an, um den Zugriff auf die Website zu kontrollieren.

Um dieses Feature zu implementieren, müssen Sie die URL-Reputationsbewertung und die Sicherheitsschwellenstufen mit dem Citrix SWG-Assistenten konfigurieren.

Konfigurieren der Reputationsbewertung mit der Citrix SWG-GUI:

Citrix empfiehlt, den Citrix SWG-Assistenten zum Konfigurieren der Reputationsbewertung und der Sicherheitsstufen zu verwenden. Basierend auf dem konfigurierten Schwellenwert können Sie eine Richtlinienaktion auswählen, um Datenverkehr zuzulassen, zu blockieren oder umzuleiten.

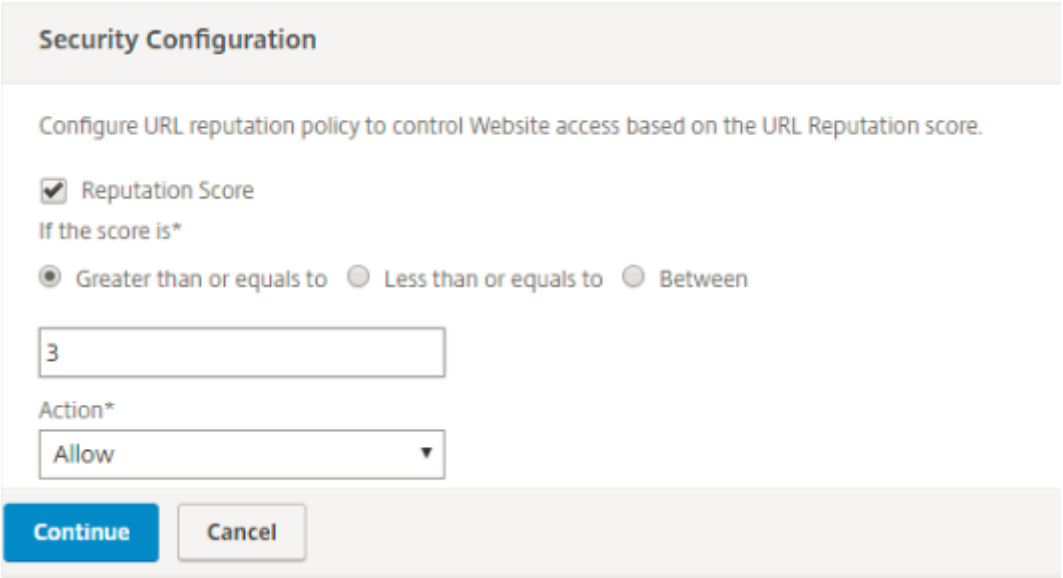
1. Melden Sie sich bei der **Citrix SWG-** Appliance an, und navigieren Sie zu **Secure Web Gateway** .
2. Klicken Sie im Detailbereich auf **Secured Web Gateway-Assistent**.
3. Geben Sie auf der Seite **Secure Web Gateway-Konfiguration** die Einstellungen des SWG-Proxy-Servers an.

4. Klicken Sie auf **Weiter**, um andere Einstellungen wie SSL-Interception und Identifizieren der Verwaltung anzugeben.
5. Klicken Sie auf **Weiter**, um den Abschnitt **Sicherheitskonfiguration** aufzurufen.
6. Aktivieren Sie im Abschnitt **Sicherheitskonfiguration** das Kontrollkästchen **Reputationsbewertung**, um den Zugriff basierend auf der URL-Reputationsbewertung zu steuern.
7. Wählen Sie die Sicherheitsstufe aus, und geben Sie den Schwellenwert für die Reputationsbewertung an:

    a) Größer als oder gleich —Zulassen oder Blockieren einer Website, wenn der Schwellenwert größer oder gleich N ist, wobei N zwischen 1 und 4 liegt.
    b) Kleiner als oder gleich —Zulassen oder Blockieren einer Website, wenn der Schwellenwert kleiner oder gleich N ist, wobei N zwischen 1 und 4 liegt.
    c) Zwischen —Erlaubt oder blockiert eine Website, wenn der Schwellenwert zwischen N1 und N2 liegt und der Bereich zwischen 1 und 4 liegt.

8. Wählen Sie eine Responder-Aktion aus der Dropdownliste aus.
9. Klicken Sie auf **Weiter** und schließen.

Die folgende Abbildung zeigt den Abschnitt Sicherheitskonfiguration des Citrix SWG-Assistenten. Aktivieren Sie die Option URL Reputation Score, um die Richtlinieneinstellungen zu konfigurieren.



Verwenden von ICAP für die Remote-Content-Inspektion

April 26, 2021

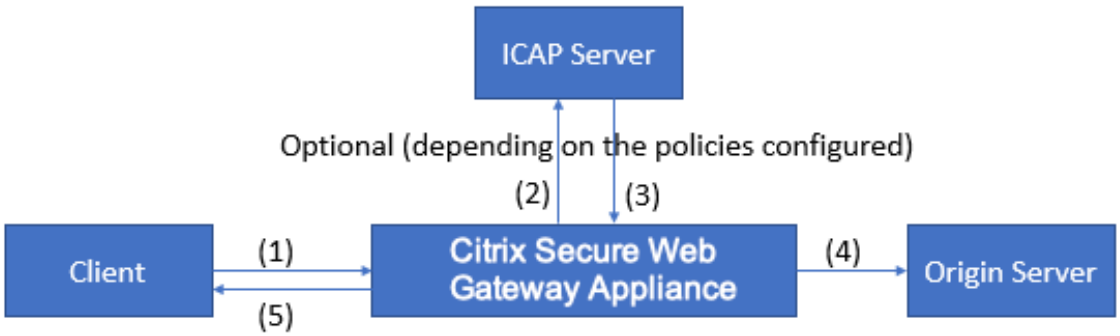
Internet Content Adaptation Protocol (ICAP) ist ein einfaches, leichtes offenes Protokoll. Es wird in der Regel verwendet, um HTTP-Nachrichten zwischen dem Proxy und den Geräten zu transportieren, die Antischadsoftware-Unterstützung und Schutz vor Datenlecks bereitstellen. ICAP hat eine Standardschnittstelle für die Content-Anpassung geschaffen, um eine größere Flexibilität bei der Verteilung von Inhalten zu ermöglichen und einen Mehrwertdienst bereitzustellen. Ein ICAP-Client leitet HTTP-Anfragen und -Antworten zur Verarbeitung an einen ICAP-Server weiter. Der ICAP-Server führt eine gewisse Transformation für Anforderungen durch und sendet Antworten an den ICAP-Client mit entsprechenden Aktionen für die Anforderung oder Antwort zurück.

Verwenden von ICAP auf der Citrix Secure Web Gateway-Appliance

> **Hinweis**
>
> Für die Inhaltsprüfung ist eine SWG Edition-Lizenz erforderlich.

Die Citrix Secure Web Gateway (SWG) -Appliance fungiert als ICAP-Client und verwendet Richtlinien für die Interaktion mit ICAP-Servern. Die Appliance kommuniziert mit ICAP-Servern von Drittanbietern, die sich auf Funktionen wie Antischadsoftware und Data Leak Prevention (DLP) spezialisiert haben. Wenn Sie ICAP auf einer SWG-Appliance verwenden, werden auch verschlüsselte Dateien gescannt. Sicherheitsanbieter haben diese Dateien früher umgangen. Die Appliance führt SSL-Interception durch, entschlüsselt den Client-Datenverkehr und sendet ihn an den ICAP-Server. Der ICAP-Server prüft auf Viren-, Malware- oder Spyware-Erkennung, Datenleckkontrolle oder andere Content-Anpassungsdienste. Die Appliance fungiert als Proxy, entschlüsselt die Antwort vom Ursprungsserver und sendet sie zur Überprüfung im Klartext an den ICAP-Server. Konfigurieren Sie Richtlinien, um den Datenverkehr auszuwählen, der an die ICAP-Server gesendet wird.

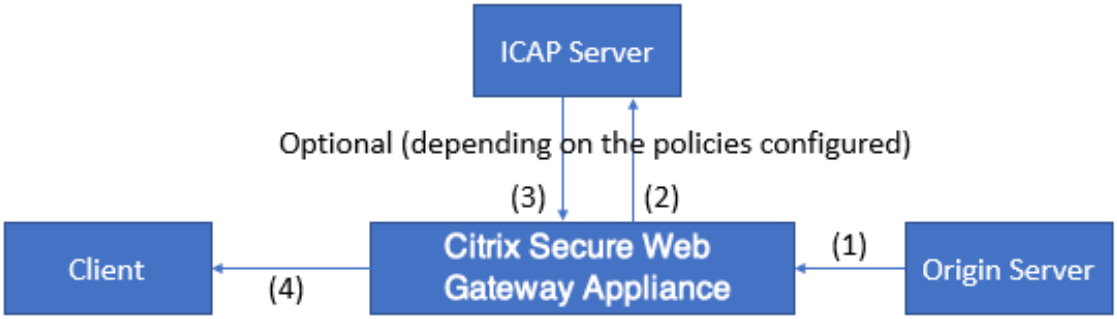
Der Anforderungsmodusablauf funktioniert wie folgt:



(1) Die Citrix SWG-Appliance fängt Anforderungen vom Client ab. (2) Die Appliance leitet diese Anforderungen basierend auf den auf der Appliance konfigurierten Richtlinien an den ICAP-Server weiter. (3) Der ICAP-Server antwortet mit der Meldung “Keine Anpassung erforderlich”, Fehler oder geänderte Anforderung. Die Appliance leitet entweder (4) den Inhalt an den vom Client angeforderten

Ursprungsserver weiter, oder (5) gibt eine entsprechende Nachricht an den Client zurück.

Der Antwortmodusablauf funktioniert wie folgt:



(1) Der Ursprungsserver reagiert auf die Citrix SWG-Appliance. (2) Die Appliance leitet die Antwort auf den ICAP-Server weiter, basierend auf den auf der Appliance konfigurierten Richtlinien. (3) Der ICAP-Server antwortet mit der Meldung "Keine Anpassung erforderlich", Fehler oder geänderte Anforderung. (4) Abhängig von der -Antwort vom ICAP-Server, leitet die Appliance entweder den angeforderten Inhalt an den Client weiter oder sendet eine entsprechende Nachricht.

Konfigurieren von ICAP auf der Citrix Secure Web Gateway-Appliance

In den folgenden Schritten wird erläutert, wie Sie ICAP auf der Citrix SWG-Appliance konfigurieren.

1. Aktivieren Sie die Funktion zur Inhaltsüberprüfung.
2. Konfigurieren Sie einen Proxy-Server.
3. Konfigurieren Sie einen TCP-Dienst, der den ICAP-Server darstellt. Um eine sichere Verbindung zwischen der SWG-Appliance und dem ICAP-Dienst herzustellen, geben Sie den Diensttyp als SSL_TCP an. Weitere Informationen zu sicherem ICAP finden Sie im Abschnitt Secure ICAP weiter unten auf dieser Seite.
4. Fügen Sie optional einen virtuellen Lastausgleichsserver hinzu, um den Lastausgleich der ICAP-Server zu ermöglichen, und binden Sie den ICAP-Dienst an diesen virtuellen Server.
5. Konfigurieren Sie ein benutzerdefiniertes ICAP-Profil. Das Profil muss den URI oder den Dienstpfad für den ICAP-Dienst und den ICAP-Modus (Anforderung oder Antwort) enthalten. Es gibt keine ICAP-Standardprofile, die den HTTP- und TCP-Standardprofilen ähneln.
6. Konfigurieren Sie eine Inhaltsinspektionsaktion und geben Sie den ICAP-Profilnamen an. Geben Sie den Namen des virtuellen Lastenausgleichs oder den TCP/SSL_TCP -Dienstnamen im Parameter Servername an.
7. Konfigurieren Sie eine Richtlinie zur Inhaltsüberprüfung, um den Client-Datenverkehr auszuwerten und an den Proxyserver zu binden. Geben Sie die Inhaltsüberprüfungsaktion in dieser Richtlinie an.

Konfigurieren von ICAP mit der Befehlszeilenschnittstelle

Konfigurieren Sie die folgenden Entitäten:

1. Aktivieren Sie das Feature.

   ```
   enable ns feature contentInspection
   ```

2. Konfigurieren Sie einen Proxy-Server.

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

   Beispiel:

   ```
   add cs vserver explicitswg PROXY 192.0.2.100 80
   ```

3. Konfigurieren Sie einen TCP-Dienst für die Darstellung der ICAP-Server.

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

   Geben Sie den Diensttyp als SSL_TCP für eine sichere Verbindung mit dem ICAP-Server an.

   Beispiel:

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

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

4. Konfigurieren Sie einen virtuellen Lastenausgleichsserver.

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

   Beispiel:

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

   Binden Sie den ICAP-Dienst an den virtuellen Lastenausgleichsserver.

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

   Beispiel:

   ```
   bind lb vserver lbicap icap_svc
   ```

5. Fügen Sie ein benutzerdefiniertes ICAP-Profil hinzu.

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

   Beispiel:

   ```
   add icapprofile icapprofile1 -uri /example.com -Mode REQMOD
   ```

   Parameter

   Name

Name für ein ICAP-Profil. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), At-Zeichen (@), Gleichheitszeichen (=) und Bindestrich (-) enthalten.

CLI-Benutzer: Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. "mein ICAP-Profil"oder 'mein ICAP-Profil').

Maximale Länge: 127

uri

URI, der den ICAP-Dienstpfad darstellt.

Maximale Länge: 511 Zeichen

Modus

ICAP-Modus. Verfügbare Einstellungen funktionieren wie folgt:

- REQMOD: Im Anforderungsänderungsmodus leitet der ICAP-Client eine HTTP-Anforderung an den ICAP-Server weiter.
- RESPMOD: Im Antwortänderungsmodus leitet der ICAP-Server eine HTTP-Antwort vom Ursprungsserver an den ICAP-Server weiter.

  Mögliche Werte: REQMOD, RESPMOD

6. Konfigurieren Sie eine Aktion, die ausgeführt werden soll, wenn die Richtlinie true zurückgibt.

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

Beispiel:

```
add contentInspection action CiRemoteAction -type ICAP -serverName
 lbicap -icapProfileName icapprofile1
```

7. Konfigurieren Sie eine Richtlinie zum Auswerten des Datenverkehrs.

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

Beispiel:

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

8. Binden Sie die Richtlinie an den Proxyserver.

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

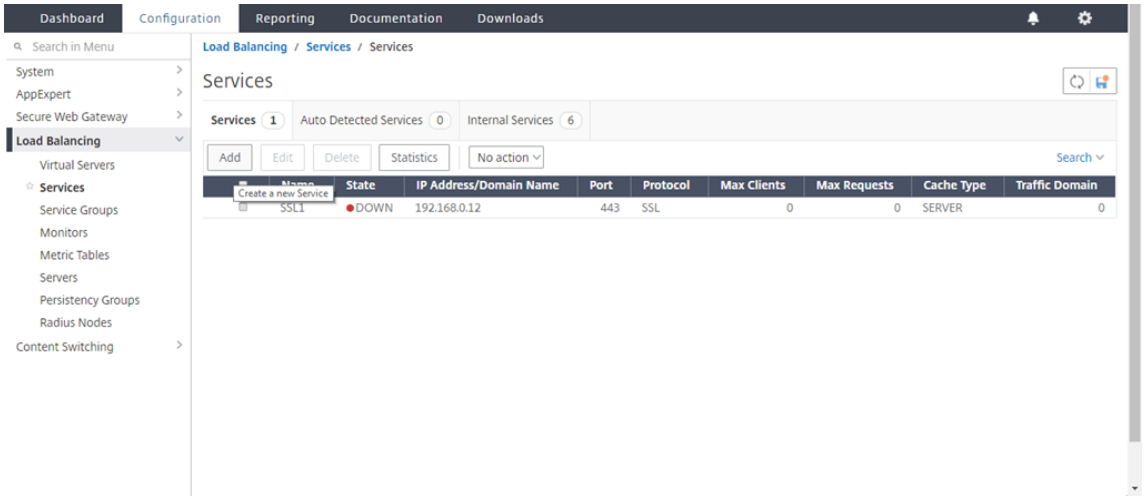

Beispiel:

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

Konfigurieren von ICAP mit der GUI

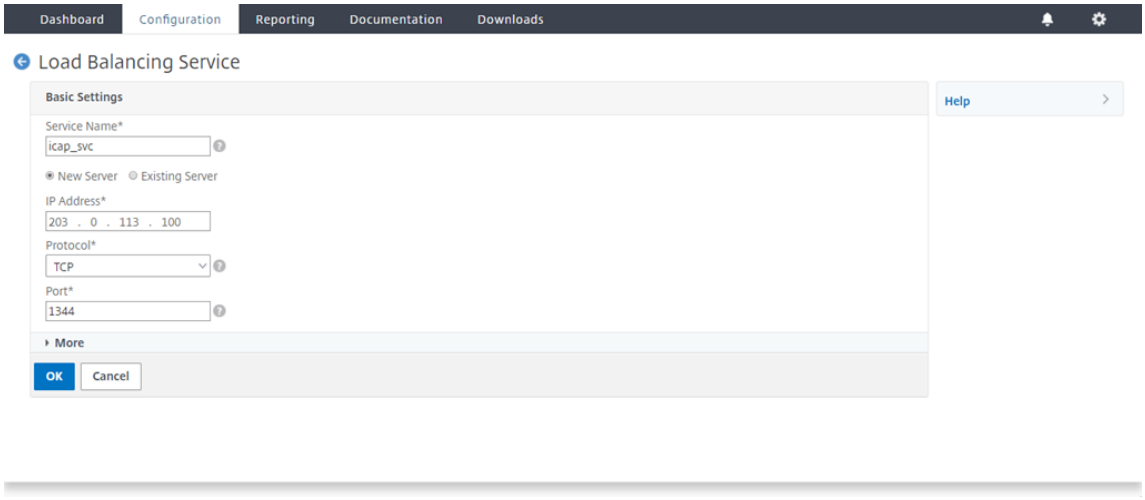
Gehen Sie wie folgt vor:

1. Navigieren Sie zu **Load Balancing** > **Services**, und klicken Sie auf **Hinzufügen**.



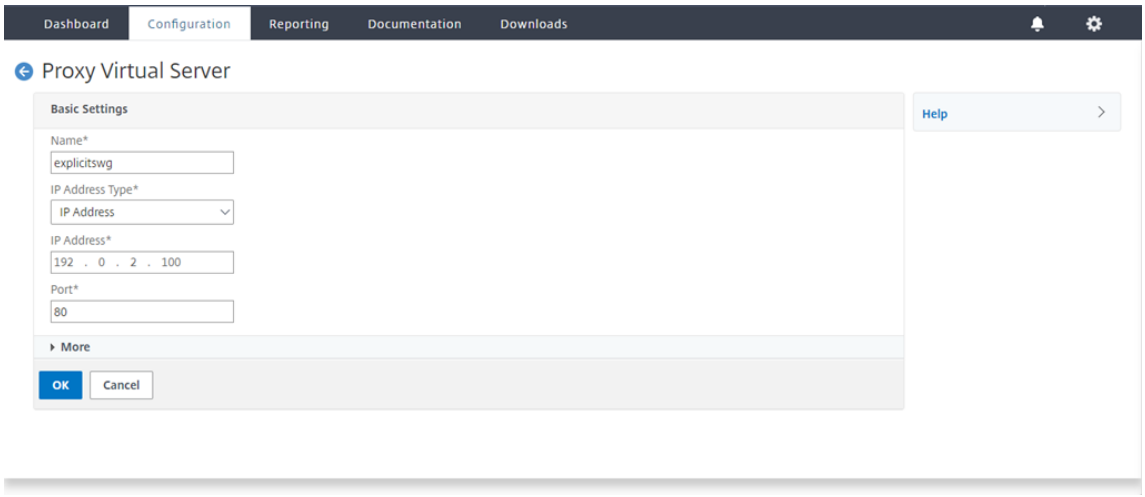
2. Geben Sie einen Namen und eine IP-Adresse ein. Wählen Sie unter **Protokoll** die Option **TCP**aus. Geben Sie in **Port** den Wert **1344**ein. Klicken Sie auf **OK**.

   Für eine sichere Verbindung zu den ICAP-Servern wählen Sie TCP_SSL-Protokoll und geben Sie den Port als 11344 an.

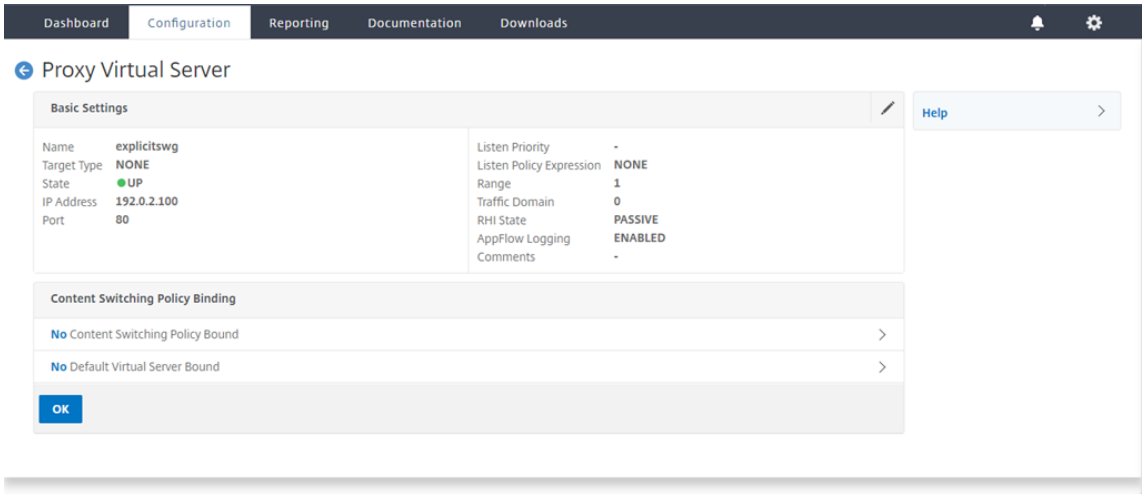


3. Navigieren Sie zu **Secure Web Gateway** > **Virtuelle Proxy-Server**. Fügen Sie einen virtuellen Proxyserver hinzu, oder wählen Sie einen virtuellen Server aus, und klicken Sie auf **Bearbeiten**.

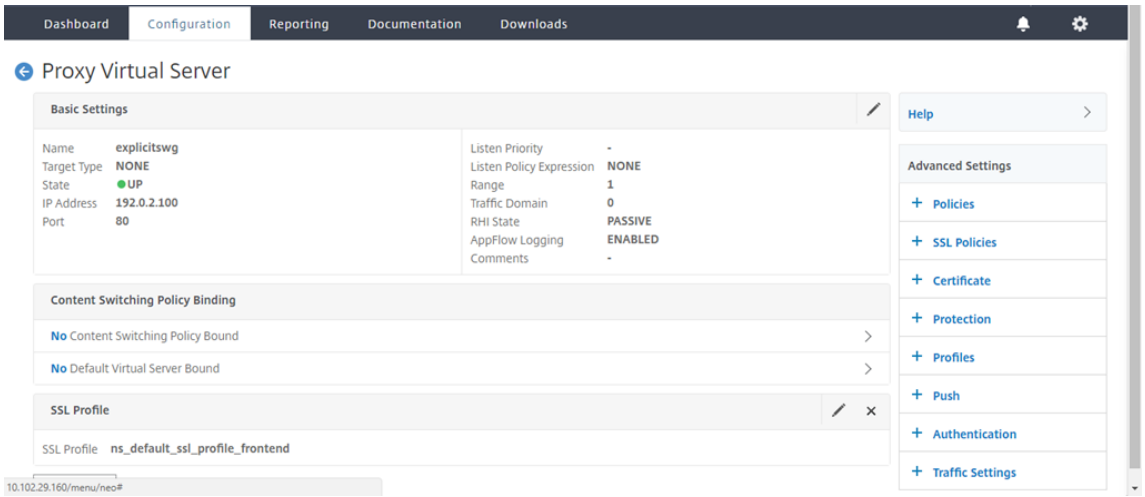
Klicken Sie nach der Eingabe von Details auf **OK**.



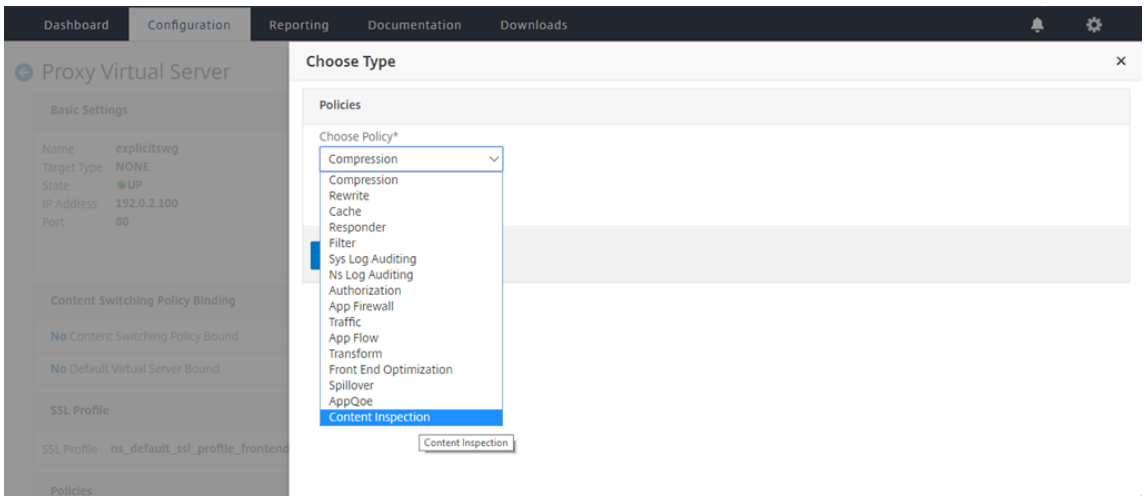
Klicken Sie erneut auf **OK**.



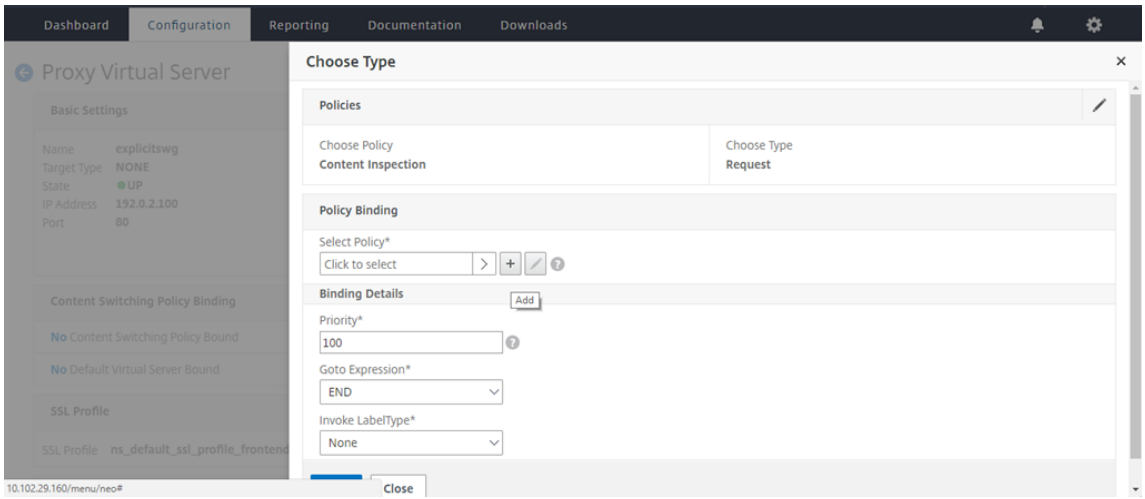
4. Klicken Sie unter **Erweiterte Einstellungen** auf **Richtlinien**.



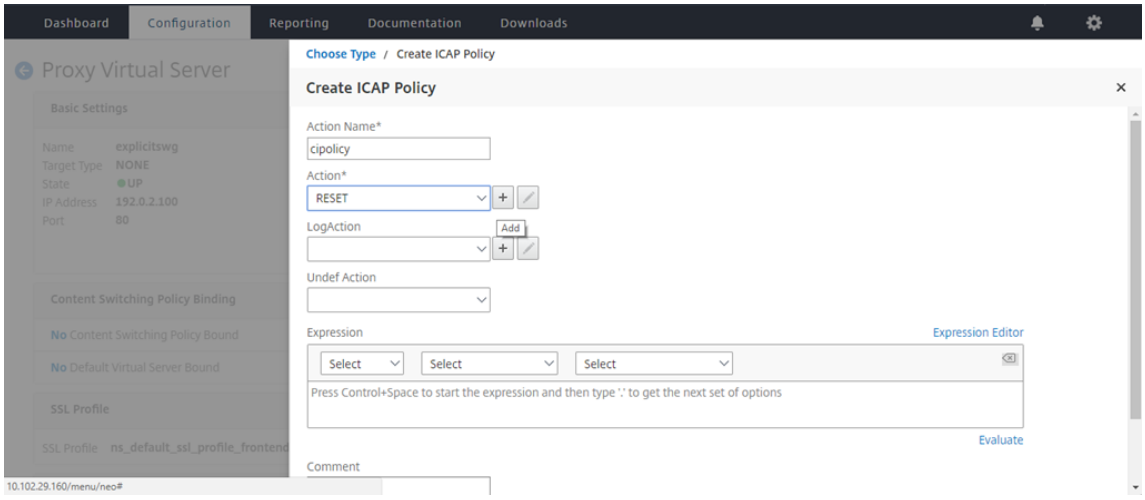
5. Wählen Sie unter **Richtlinie auswählen** die Option **Inhaltsüberprüfung** aus. Klicken Sie auf **Weiter**.



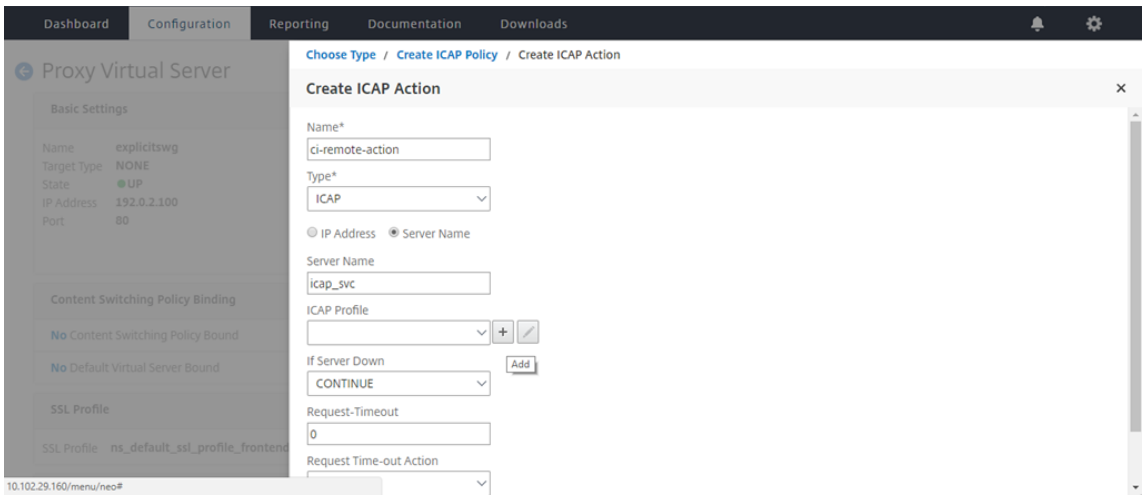
6. Klicken Sie unter **Richtlinie auswählen** auf das +-Zeichen, um eine Richtlinie hinzuzufügen.



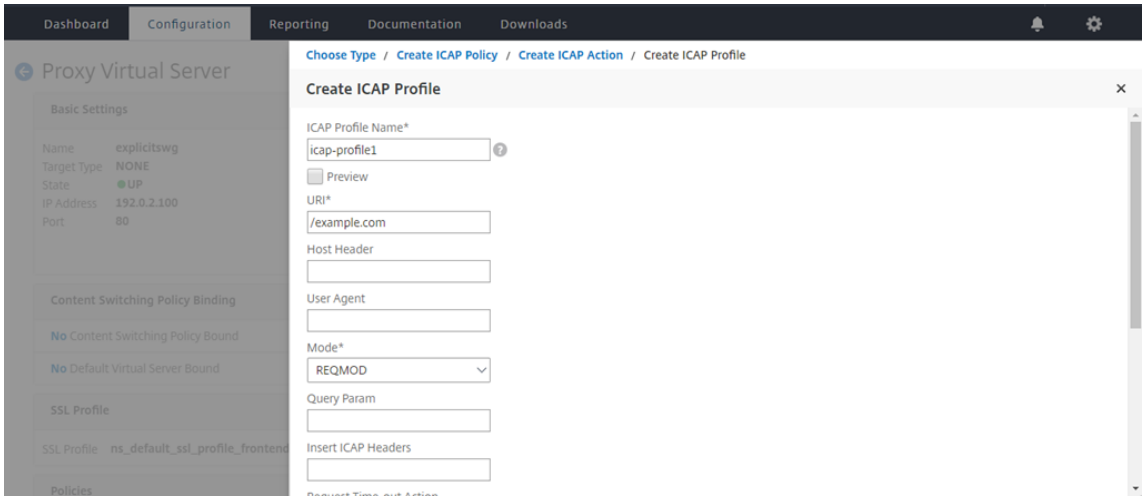
7. Geben Sie einen Namen für die Richtlinie ein. Klicken Sie in **Aktion** auf das +-Zeichen, um eine Aktion hinzuzufügen.



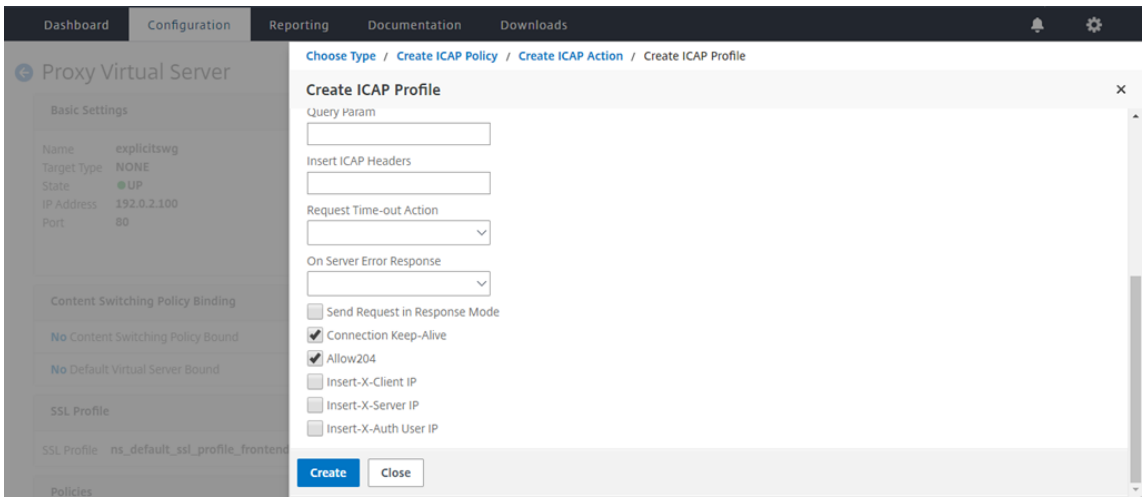
8. Geben Sie einen Namen für die Aktion ein. Geben Sie unter **Servername** den Namen des zuvor erstellten TCP-Dienstes ein. Klicken Sie im **ICAP-Profil** auf das +-Zeichen, um ein ICAP-Profil hinzuzufügen.



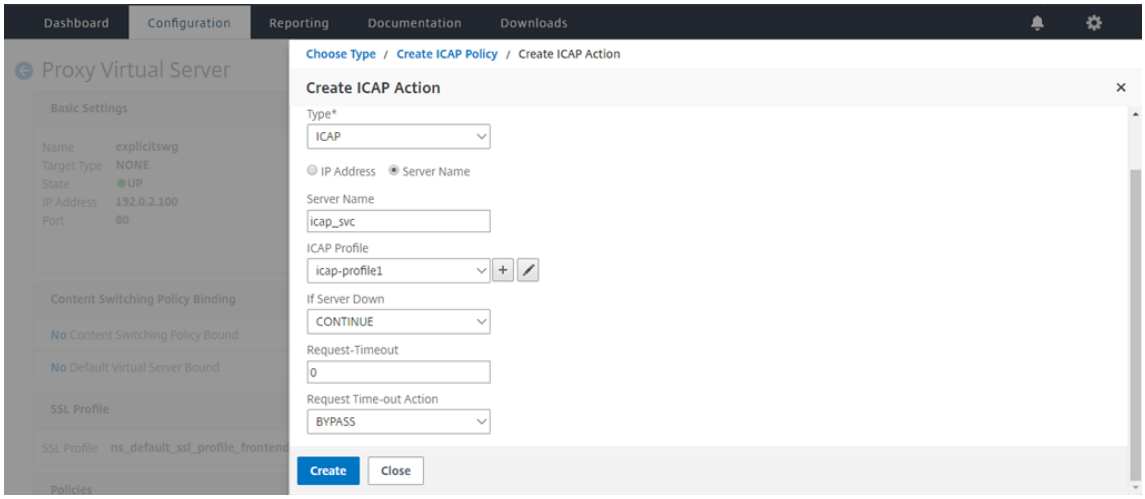
9. Geben Sie einen Profilnamen ein, URI. Wählen Sie unter **Modus** die Option **REQMOD** aus.



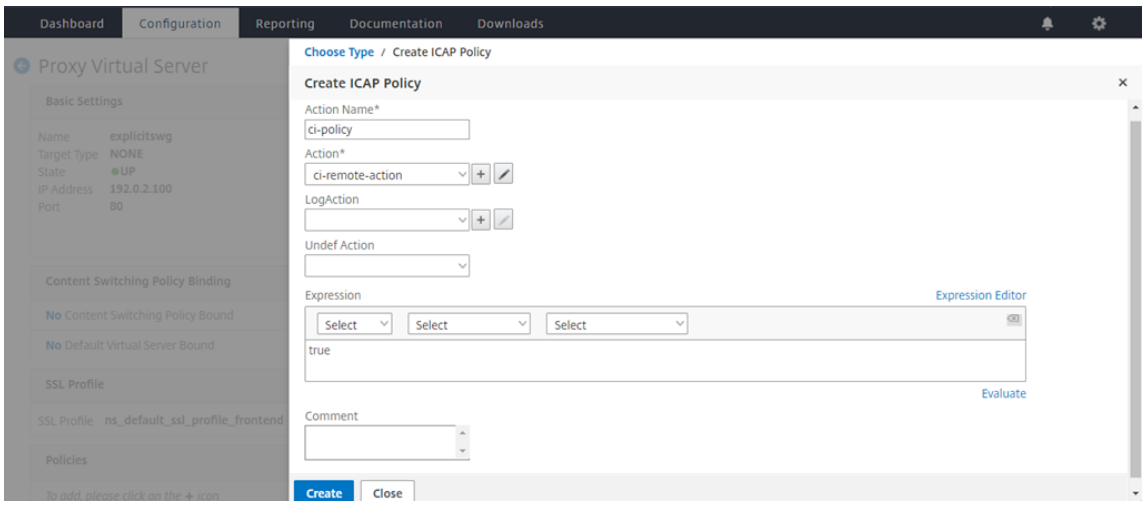
10. Klicken Sie auf **Erstellen**.



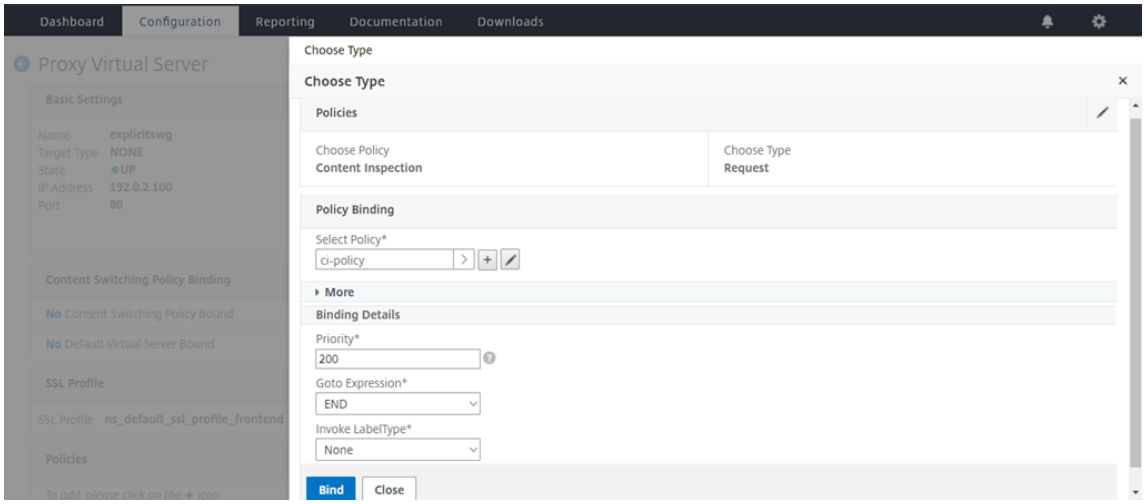
11. Klicken Sie auf der Seite **ICAP-Aktion erstellen** auf **Erstellen**.



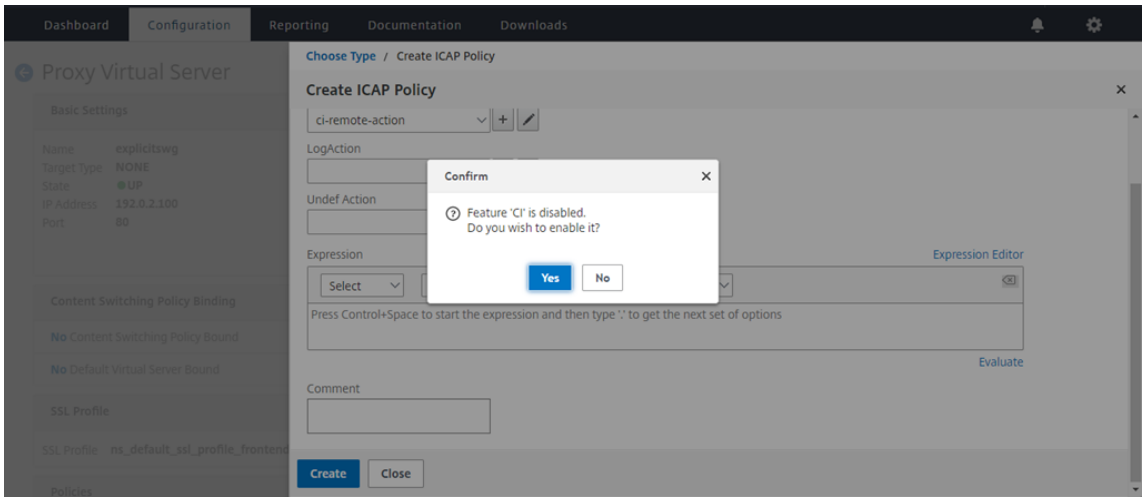
12. Geben Sie auf der Seite **ICAP-Richtlinie erstellen** im **Ausdruckseditor** “true”ein. Klicken Sie dann auf **Erstellen**.



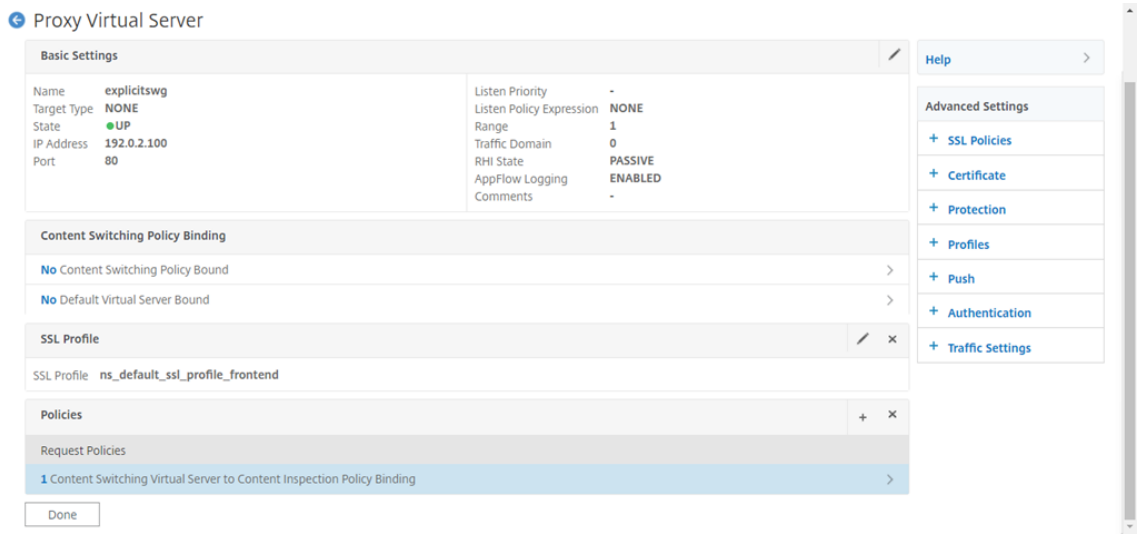
13. Klicken Sie auf **Bind**.



14. Wählen Sie **Ja**aus, wenn Sie dazu aufgefordert werden, die Inhaltsüberprüfungsfunktion zu aktivieren.



15. Klicken Sie auf **Fertig**.



Sicheres ICAP

Sie können eine sichere Verbindung zwischen der SWG-Appliance und den ICAP-Servern herstellen. Erstellen Sie dazu einen SSL_TCP-Dienst anstelle eines TCP-Dienstes. Konfigurieren Sie einen virtuellen Lastausgleichsserver vom Typ SSL_TCP. Binden Sie den ICAP-Dienst an den virtuellen Lastenausgleichsserver.

Konfigurieren Sie sicheres ICAP mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiel:

```
add service icap_svc 203.0.113.100 SSL_TCP 1344

add lbvserver lbicap SSL_TCP 0.0.0.0 0

bind lb vserver lbicap icap_svc
<!--NeedCopy-->
```

Konfigurieren Sie sicheres ICAP mit der GUI

1. Navigieren Sie zu **Lastenausgleich** > **Virtuelle Server**, und klicken Sie auf **Hinzufügen** .

2. Geben Sie einen Namen für den virtuellen Server, die IP-Adresse und den Port an. Geben Sie das Protokoll als SSL_TCP an.
3. Klicken Sie auf **OK**.
4. Klicken Sie in den Abschnitt **Load Balancing Virtual Server Service Binding**, um einen ICAP-Dienst hinzuzufügen.
5. Klicken Sie auf +, um einen Dienst hinzuzufügen.
6. Geben Sie einen Dienstnamen, eine IP-Adresse, ein Protokoll (SSL_TCP) und einen Port an (der Standardport für sicheres ICAP ist 11344).
7. Klicken Sie auf **OK**.
8. Klicken Sie auf **Fertig**.
9. Klicken Sie auf **Bind**.
10. Klicken Sie zweimal auf **Weiter** .
11. Klicken Sie auf **Fertig**.

Einschränkungen

Die folgenden Funktionen werden nicht unterstützt:

- ICAP-Antwort-Caching.
- X-Auth-User-URI-Header wird eingefügt.
- Einfügen der HTTP-Anforderung in die ICAP-Anforderung in RESPMOD.

Integration mit IPS oder NGFW als Inline-Geräte

April 26, 2021

Sicherheitsgeräte wie Intrusion Prevention System (IPS) und Next Generation Firewall (NGFW) schützen Server vor Netzwerkangriffen. Diese Geräte können den Live-Datenverkehr überprüfen und werden in der Regel im Layer 2-Inline-Modus bereitgestellt. Citrix Secure Web Gateway (SWG) bietet Sicherheit für Benutzer und das Unternehmensnetzwerk beim Zugriff auf Ressourcen im Internet.

Eine Citrix SWG-Appliance kann in ein oder mehrere Inline-Geräte integriert werden, um Bedrohungen zu verhindern und erweiterten Sicherheitsschutz zu bieten. Bei den Inline-Geräten kann es sich um ein beliebiges Sicherheitsgerät wie IPS und NGFW handeln.

Einige Anwendungsfälle, in denen Sie von der Citrix SWG-Appliance und der Inline-Geräteintegration profitieren können, sind:

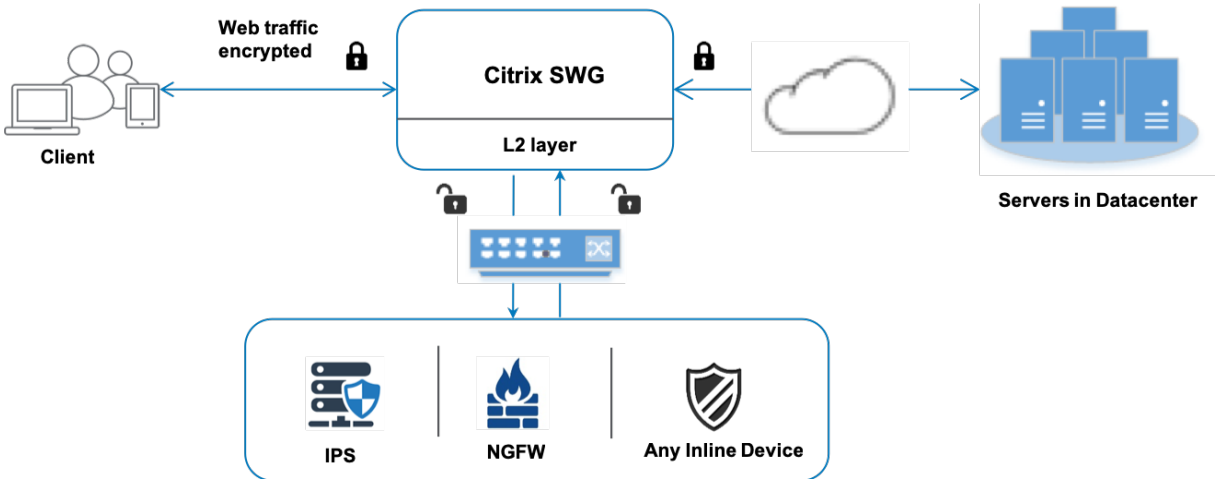
- **Überprüfen des verschlüsselten Datenverkehrs:** Die meisten IPS- und NGFW-Appliances umgehen verschlüsselten Datenverkehr, wodurch Server anfällig für Angriffe werden können.

Eine Citrix SWG-Appliance kann Datenverkehr entschlüsseln und zur Überprüfung an die Inline-Geräte senden. Diese Integration erhöht die Netzwerksicherheit des Kunden.

- **Entladen von Inline-Geräten aus der TLS/SSL -Verarbeitung:** Die TLS/SSL -Verarbeitung ist teuer, was zu einer hohen CPU-Auslastung in IPS- oder NGFW-Appliances führen kann, wenn sie auch den Datenverkehr entschlüsseln. Eine Citrix SWG-Appliance hilft beim Auslagern der TLS/SSL -Verarbeitung von Inline-Geräten. Inline-Geräte können daher ein höheres Verkehrsaufkommen untersuchen.
- **Inline-Geräte laden: Wenn Sie mehrere Inline-Geräte** für die Verwaltung von hohem Datenverkehr konfiguriert haben, kann eine Citrix SWG-Appliance den Lastausgleich ausgleichen und den Datenverkehr gleichmäßig auf diese Geräte verteilen.
- **Intelligente Auswahl des Datenverkehrs:** Statt den gesamten Datenverkehr zur Inspektion an das Inline-Gerät zu senden, führt die Appliance eine intelligente Auswahl des Datenverkehrs durch. Beispielsweise wird das Senden von Textdateien zur Überprüfung an die Inline-Geräte übersprungen.

Citrix SWG-Integration mit Inline-Geräten

Das folgende Diagramm zeigt, wie eine Citrix SWG in Inline-Sicherheitsgeräte integriert ist.



Wenn Sie Inline-Geräte in die Citrix SWG-Appliance integrieren, interagieren die Komponenten wie folgt:

1. Ein Client sendet eine Anforderung an eine Citrix SWG-Appliance.
2. Die Appliance sendet die Daten an das Inline-Gerät zur Inhaltsüberprüfung basierend auf der Richtlinienbewertung. Bei HTTPS-Datenverkehr entschlüsselt die Appliance die Daten und sendet sie zur Inhaltsüberprüfung im Klartext an das Inline-Gerät.

> **Hinweis:**
>
> Wenn zwei oder mehr Inline-Geräte vorhanden sind, gleicht die Appliance die Geräte aus und sendet den Datenverkehr.

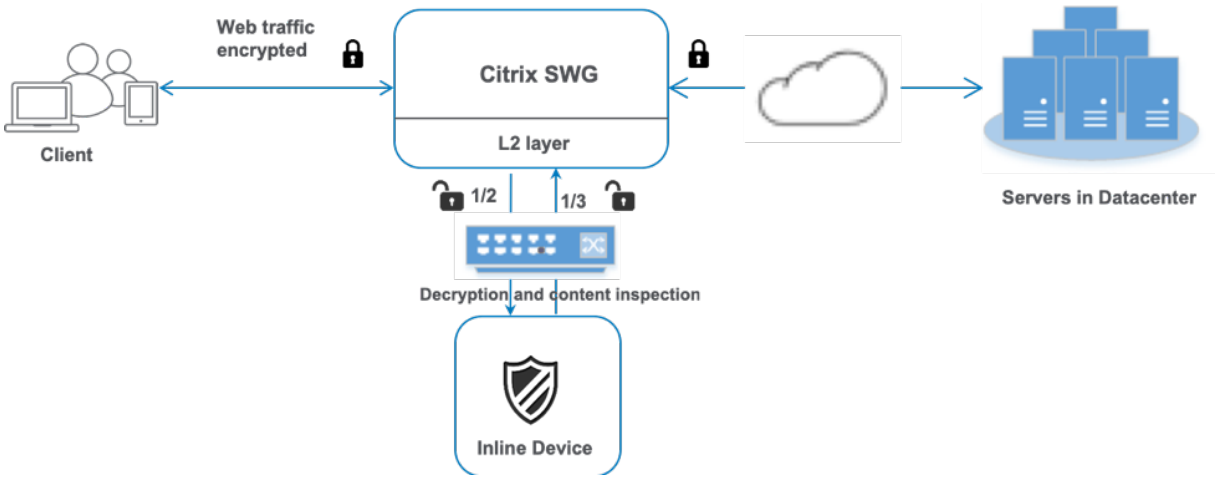
3. Das Inline-Gerät prüft die Daten auf Bedrohungen und entscheidet, ob die Daten gelöscht, zurückgesetzt oder an die Appliance gesendet werden sollen.
4. Wenn Sicherheitsbedrohungen vorliegen, ändert das Gerät die Daten und sendet sie an die Appliance.
5. Bei HTTPS-Datenverkehr verschlüsselt die Appliance die Daten erneut und leitet die Anforderung an den Backend-Server weiter.
6. Der Backend-Server sendet die Antwort an die Appliance.
7. Die Appliance entschlüsselt die Daten erneut und sendet sie zur Überprüfung an das Inline-Gerät.
8. Das Inline-Gerät prüft die Daten. Wenn Sicherheitsbedrohungen vorliegen, ändert das Gerät die Daten und sendet sie an die Appliance.
9. Die Appliance verschlüsselt die Daten erneut und sendet die Antwort an den Client.

Konfigurieren der Inline-Geräteintegration

Sie können eine Citrix SWG-Appliance mit einem Inline-Gerät wie folgt konfigurieren:

Szenario 1: Verwenden eines einzelnen Inline-Geräts

Um ein Sicherheitsgerät (IPS oder NGFW) in den Inline-Modus zu integrieren, müssen Sie die Inhaltsprüfung und die MAC-basierte Weiterleitung (MBF) im globalen Modus auf der SWG-Appliance aktivieren. Fügen Sie anschließend ein Inhaltsinspektionsprofil, einen TCP-Dienst, eine Inhaltsüberprüfungsaktion für Inline-Geräte hinzu, um den Datenverkehr basierend auf der Inspektion zurückzusetzen, zu blockieren oder zu löschen. Fügen Sie außerdem eine Richtlinie zur Inhaltsüberprüfung hinzu, die von der Appliance verwendet wird, um die Teilmenge des Datenverkehrs zu bestimmen, die an die Inline-Geräte gesendet werden soll. Konfigurieren Sie schließlich den virtuellen Proxyserver mit aktivierter Layer-2-Verbindung auf dem Server und binden Sie die Inhaltsüberprüfungsrichtlinie an diesen virtuellen Proxyserver.



Gehen Sie wie folgt vor:

1. Aktivieren Sie den MAC-basierten Weiterleitungsmodus (MPF).
2. Aktivieren Sie die Funktion zur Inhaltsüberprüfung.
3. Fügen Sie ein Inhaltsinspektionsprofil für den Service hinzu. Das Inhaltsinspektionsprofil enthält die Inline-Geräteeinstellungen, die die SWG-Appliance in ein Inline-Gerät integrieren.
4. (Optional) Fügen Sie einen TCP-Monitor hinzu.

   > **Hinweis:**
   >
   > Transparente Geräte haben keine IP-Adresse. Um Integritätsprüfungen durchzuführen, müssen Sie daher einen Monitor explizit binden.

5. Fügen Sie einen Dienst hinzu. Ein Dienst stellt ein Inline-Gerät dar.
6. (Optional) Binden Sie den Dienst an den TCP-Monitor.
7. Fügen Sie eine Inhaltsinspektionsaktion für den Service hinzu.
8. Fügen Sie eine Richtlinie zur Inhaltsüberprüfung hinzu, und geben Sie die Aktion an.
9. Fügen Sie einen virtuellen HTTP- oder HTTPS-Proxyserver (Content Switching) hinzu.
10. Binden Sie die Richtlinie zur Inhaltsüberprüfung an den virtuellen Server.

Konfiguration über die CLI Geben Sie die folgenden Befehle an der Eingabeaufforderung ein. Beispiele werden nach den meisten Befehlen angegeben.

1. MBF aktivieren.

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


2. Aktivieren Sie das Feature.

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

3. Fügen Sie ein Inhaltsinspektionsprofil hinzu.

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

Beispiel:

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

4. Fügen Sie einen Dienst hinzu. Geben Sie eine Dummy-IP-Adresse an, die keinem der Geräte gehört, einschließlich der Inline-Geräte. Setzen Sie `use source IP address` (USIP) auf YES. Setzen Sie `useproxyport` auf NO. Schalten Sie den Integritätsmonitor aus. Aktivieren Sie die Integritätsüberwachung nur, wenn Sie diesen Dienst an einen TCP-Monitor binden. Wenn Sie einen Monitor an einen Dienst binden, setzen Sie die Option TRANSPARENT im Monitor auf ON.

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

Beispiel:

```
add service ips_service 198.51.100.2 TCP * -healthMonitor YES -
    usip YES -useproxyport NO -contentInspectionProfileName ipsprof

<!--NeedCopy-->
```

5. Fügen Sie eine Inhaltsüberprüfungsaktion hinzu.

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

Beispiel:

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

6. Fügen Sie eine Richtlinie zur Inhaltsüberprüfung hinzu.


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

Beispiel:

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

7. Fügen Sie einen virtuellen Proxyserver hinzu.

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

Beispiel:

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

8. Binden Sie die Richtlinie an den virtuellen Server.

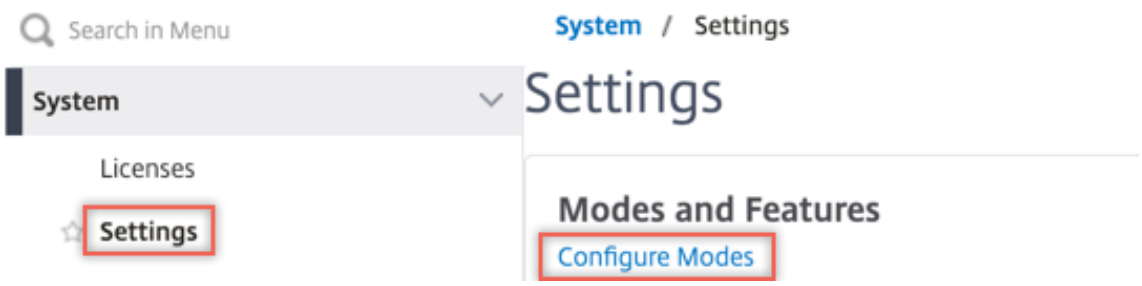
```
bind cs vserver <name> -policyName <string> -priority <
   positive_integer> -gotoPriorityExpression <expression> -type
   REQUEST
<!--NeedCopy-->
```

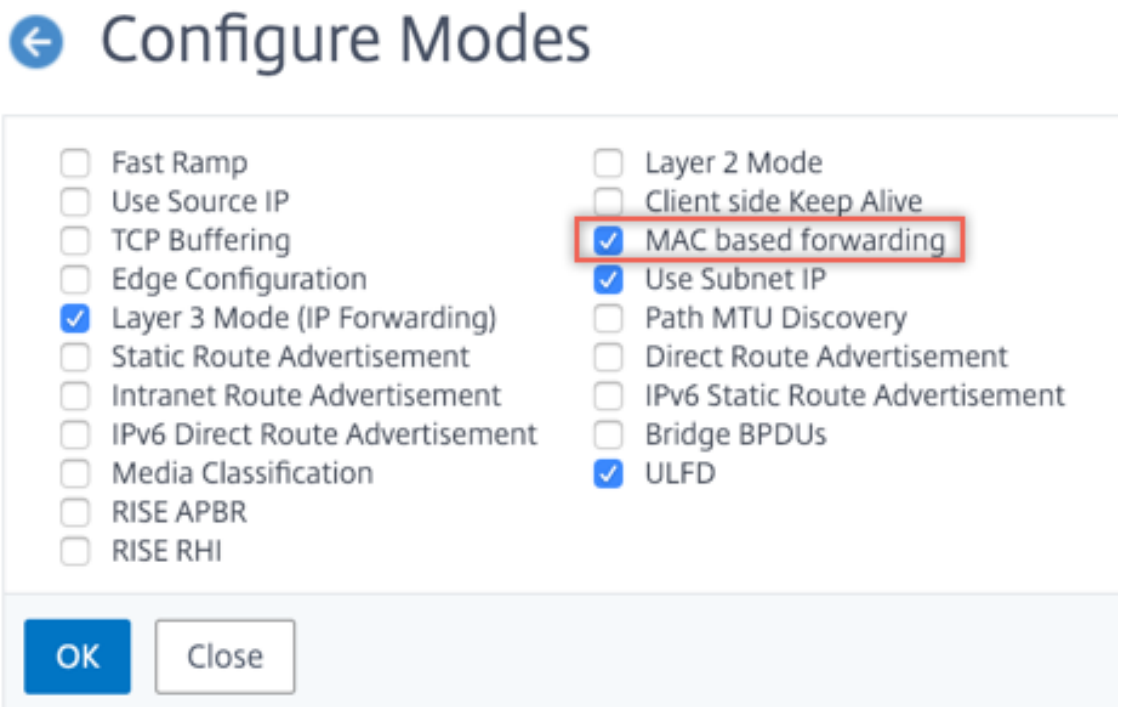
Beispiel:

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

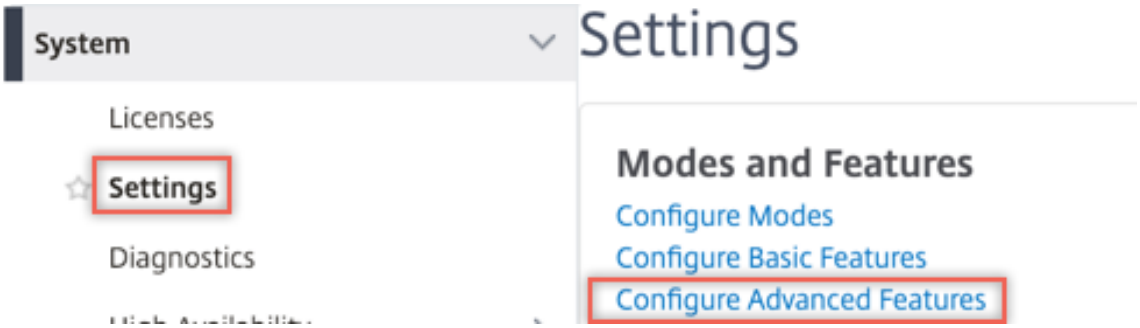
Konfiguration über die GUI

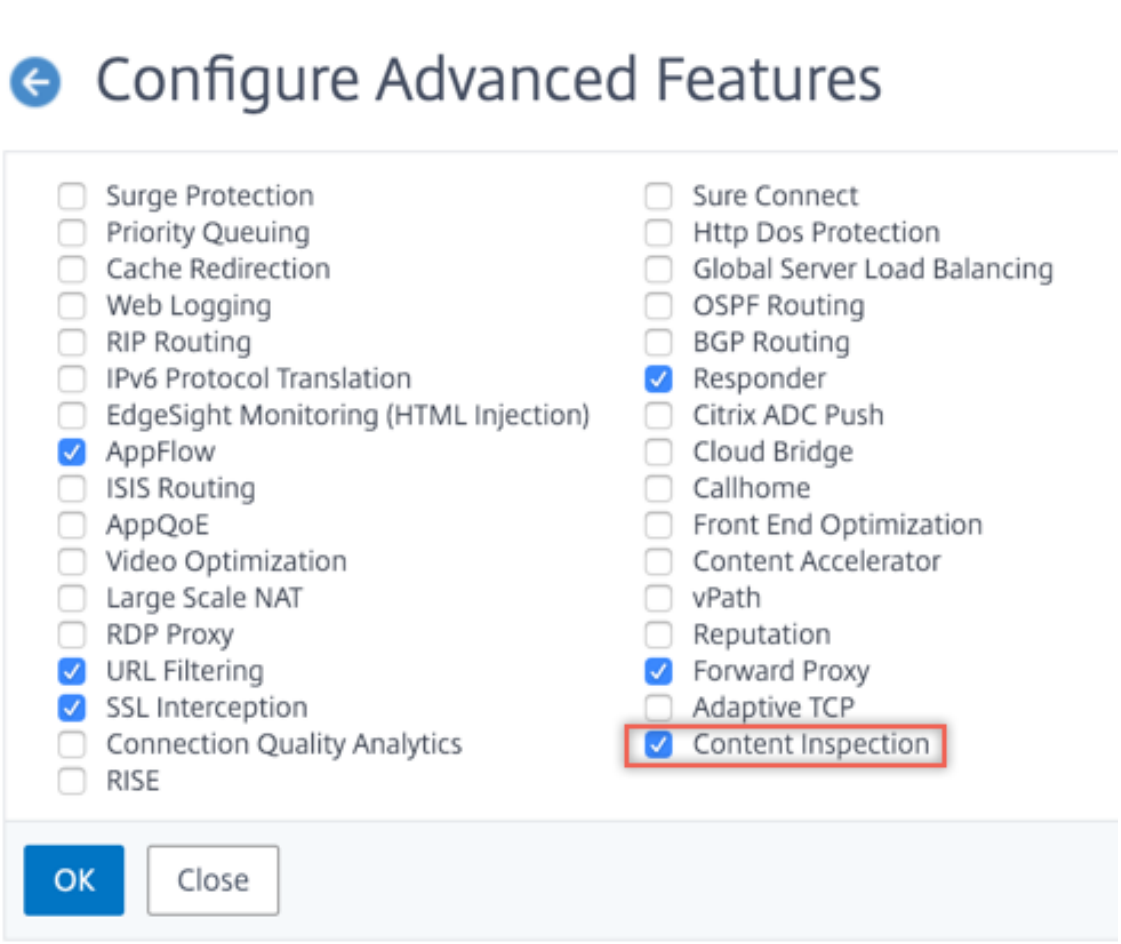
1. Navigieren Sie zu **System > Einstellungen**. Klicken Sie unter **Modi und Features** auf **Modi konfigurieren**.



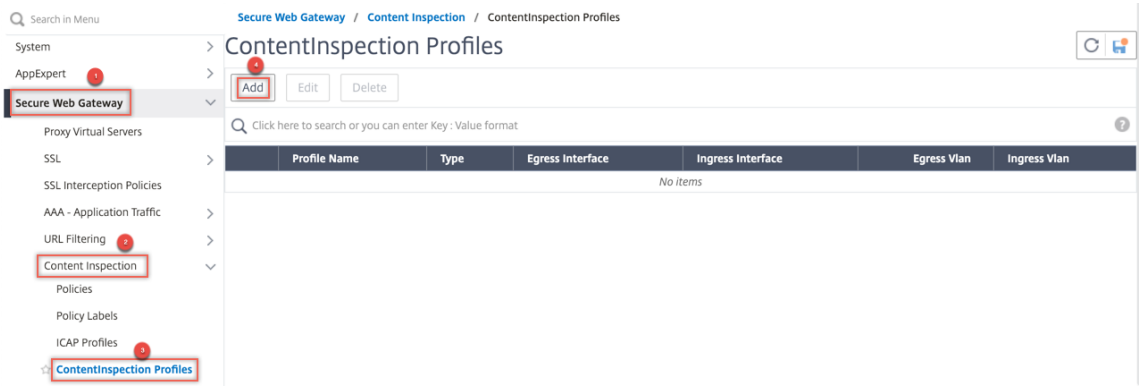


2. Navigieren Sie zu **System > Einstellungen**. Klicken Sie unter **Modi und Features** auf **Erweiterte Funktionen konfigurieren**.



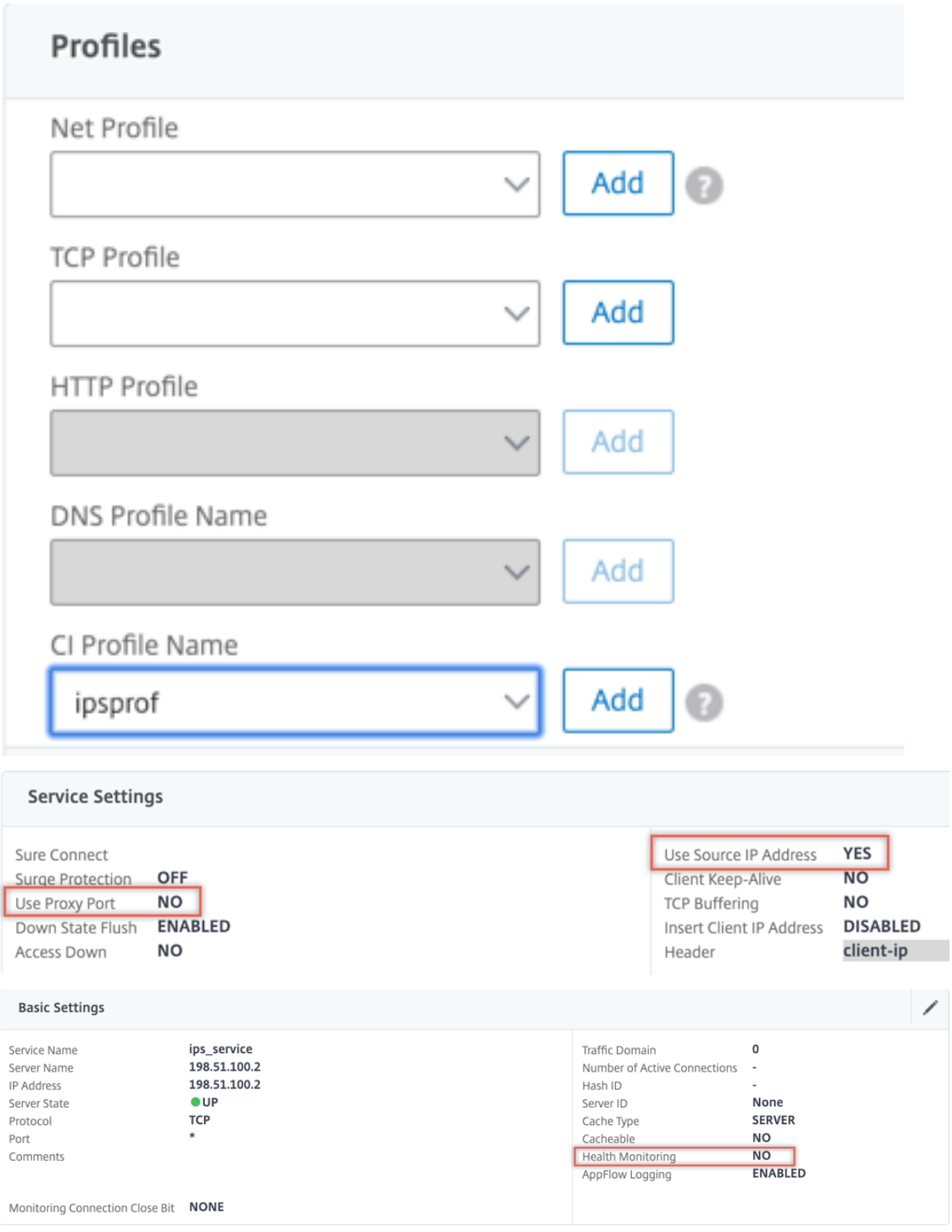


3. Navigieren Sie zu **Secure Web Gateway > Content Inspection > Content Inspection Profile**. Klicken Sie auf **Hinzufügen**.

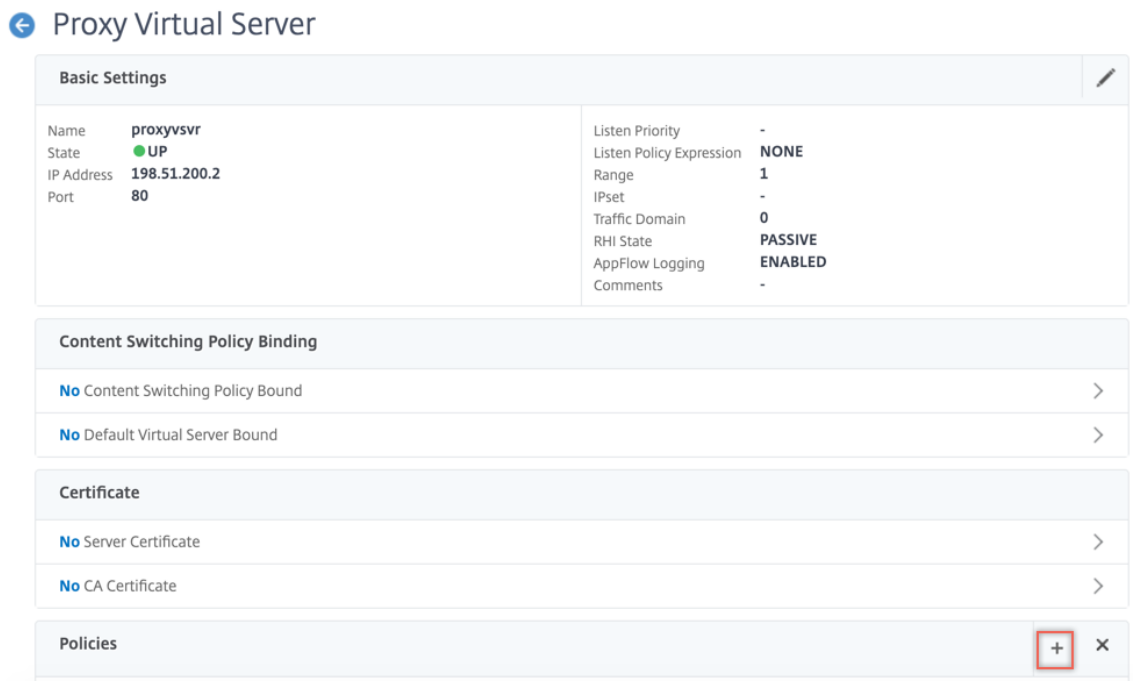


4. Navigieren Sie zu **Load Balancing > Services > Hinzufügen** und fügen Sie einen Service hinzu. Klicken Sie unter **Erweiterte Einstellungen** auf **Profile**. Wählen Sie in der Liste **CI-Profilname** das zuvor erstellte Content-Inspektionsprofil aus. Legen Sie unter **Diensteinstellungen** die Option **Quell-IP-Adresse verwenden** auf Ja und **Proxyport verwenden** auf Nein fest. Legen Sie in den **Grundeinstellungen** die **Integritätsüberwachung** auf Nein fest. Aktivieren Sie die In-

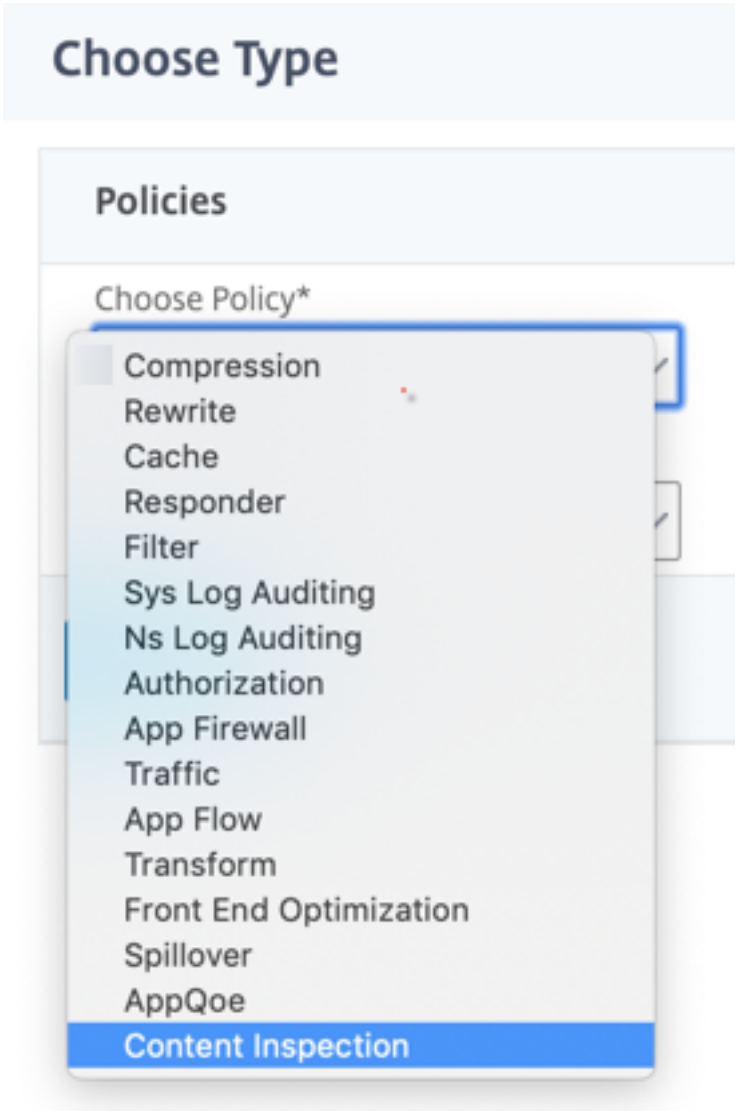
tegritätsüberwachung nur, wenn Sie diesen Dienst an einen TCP-Monitor binden. Wenn Sie einen Monitor an einen Dienst binden, setzen Sie die Option TRANSPARENT im Monitor auf ON.



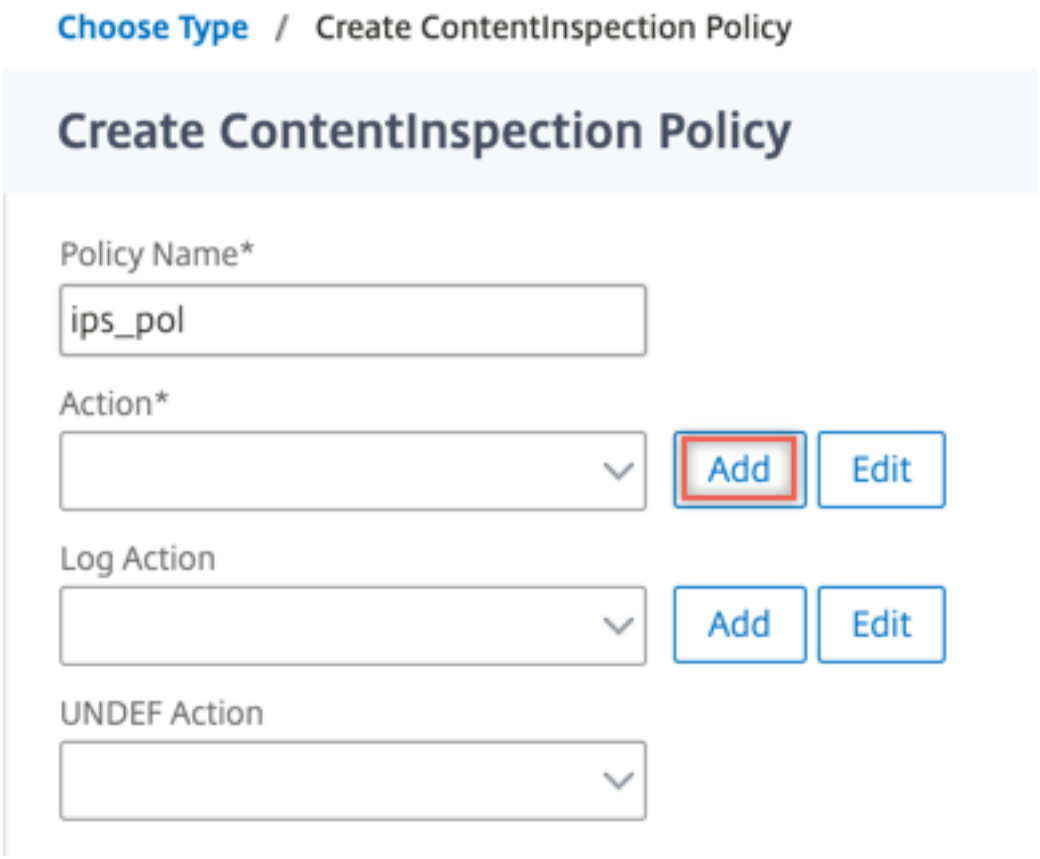
5. Navigieren Sie zu **Secure Web Gateway > Virtuelle Proxyserver > Hinzufügen**. Geben Sie einen Namen, eine IP-Adresse und einen Port an. Wählen Sie unter **Erweiterte Einstellungen** die Option **Richtlinien**aus. Klicken Sie auf das +-Zeichen.



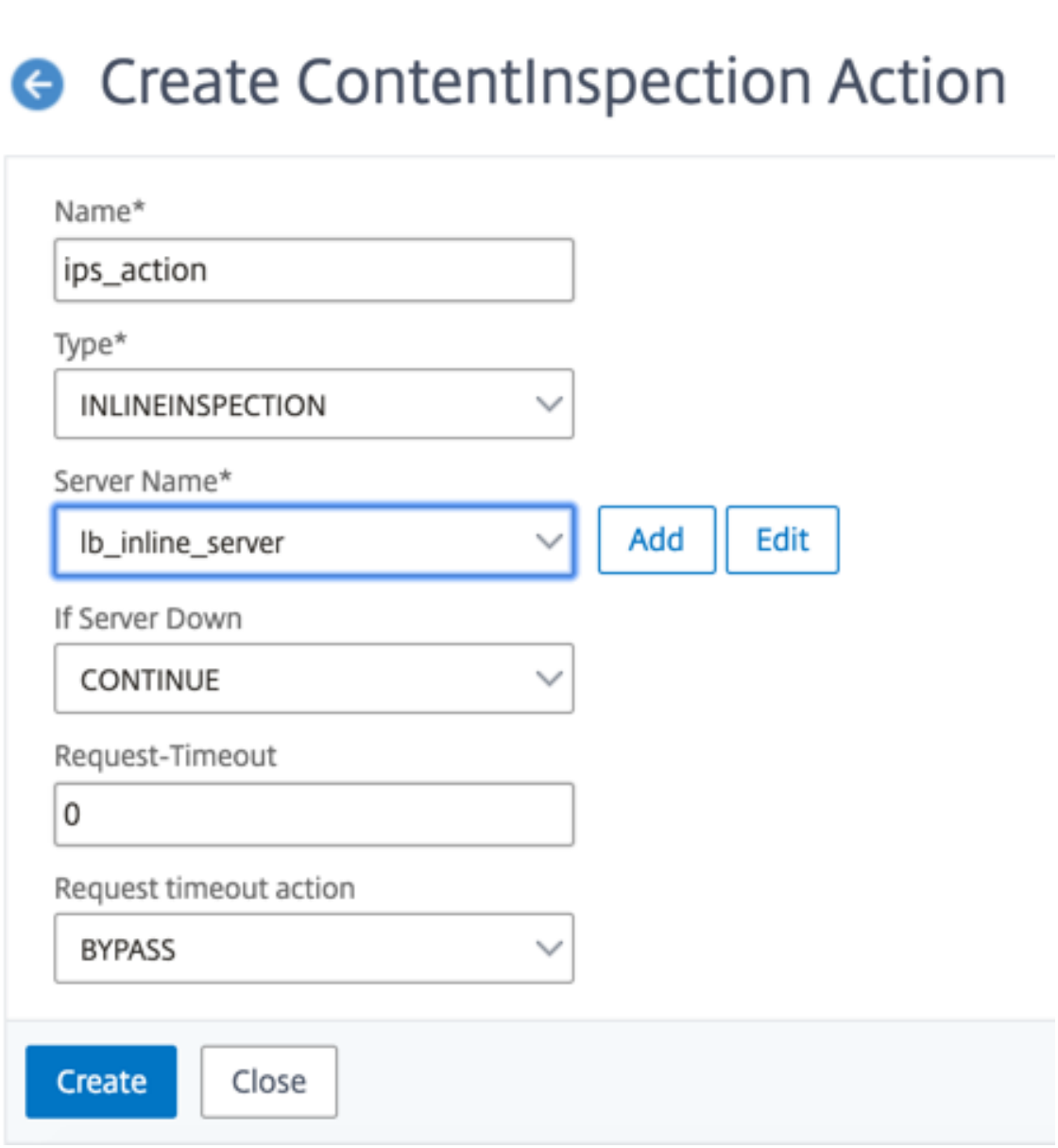
6. Wählen Sie unter **Richtlinie auswählen** die Option **Inhaltsüberprüfung** aus. Klicken Sie auf **Weiter**.



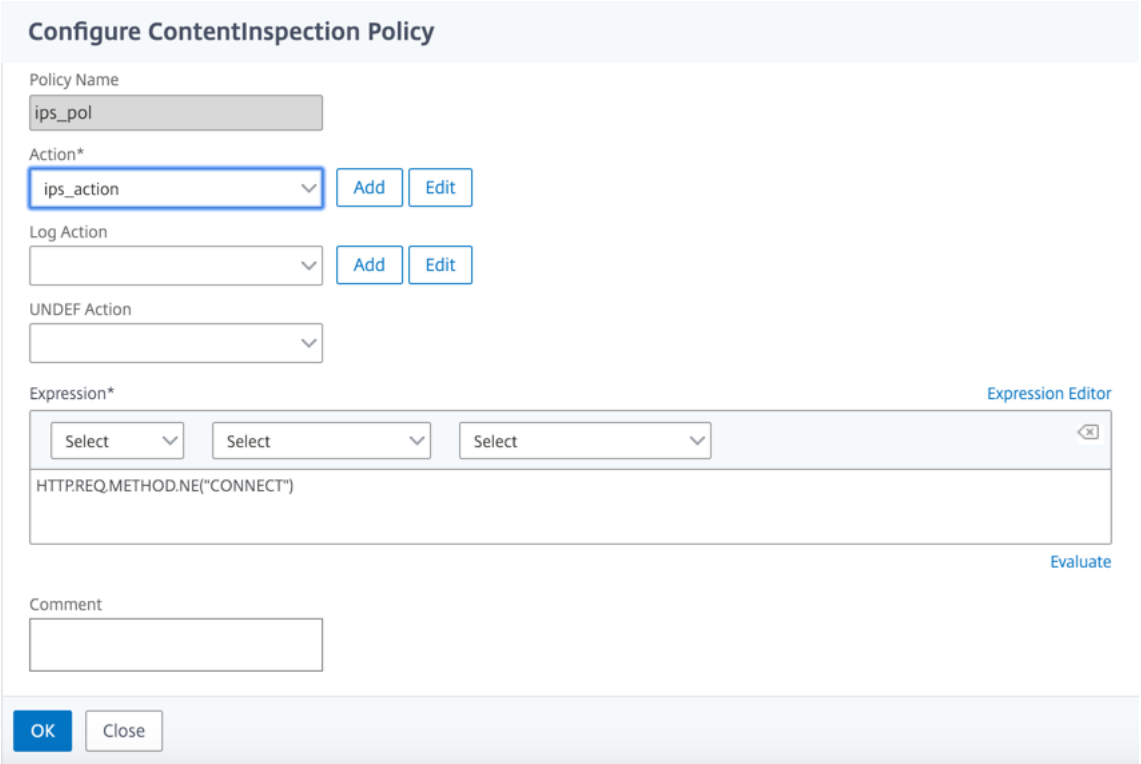
7. Klicken Sie auf **Hinzufügen**. Geben Sie einen Namen an. Klicken Sie unter **Aktion** auf **Hinzufügen**.



8. Geben Sie einen Namen an. Wählen Sie unter **Typ** die Option **INLINEINSPECTION** aus. Wählen Sie **unter Servername**den zuvor erstellten TCP-Dienst aus.



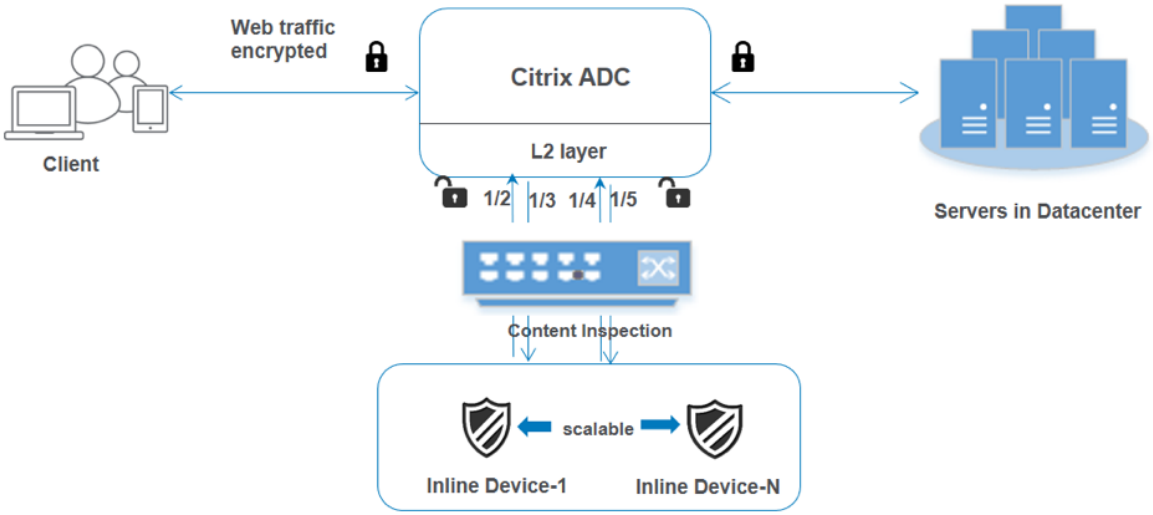
9. Klicken Sie auf **Erstellen**. Geben Sie die Regel an, und klicken Sie auf **Erstellen**.



10. Klicken Sie auf **Bind**.
11. Klicken Sie auf **Fertig**.

Szenario 2: Lastausgleich mehrerer Inline-Geräte mit dedizierten Schnittstellen

Wenn Sie zwei oder mehr Inline-Geräte verwenden, können Sie die Geräte mit verschiedenen Contentinspektionsdiensten mit dedizierten Schnittstellen ausgleichen. In diesem Fall gleicht die Citrix SWG-Appliance die Teilmenge des Datenverkehrs aus, der über eine dedizierte Schnittstelle an jedes Gerät gesendet wird. Die Teilmenge wird basierend auf den konfigurierten Richtlinien festgelegt. Beispielsweise werden TXT- oder Bilddateien möglicherweise nicht zur Überprüfung an die Inline-Geräte gesendet.



Die Basiskonfiguration bleibt dieselbe wie in Szenario 1. Sie müssen jedoch für jedes Inline-Gerät ein Inhaltsinspektionsprofil erstellen und die Eingangs- und Ausgangsschnittstelle in jedem Profil angeben. Fügen Sie einen Dienst für jedes Inline-Gerät hinzu. Fügen Sie einen virtuellen Lastausgleichsserver hinzu, und geben Sie ihn in der Inhaltsüberprüfungsaktion an. Führen Sie die folgenden zusätzlichen Schritte aus:

1. Fügen Sie Content-Inspektionsprofile für jeden Service hinzu.
2. Fügen Sie einen Dienst für jedes Gerät hinzu.
3. Fügen Sie einen virtuellen Lastenausgleichsserver hinzu.
4. Geben Sie den virtuellen Lastausgleichsserver in der Inhaltsüberprüfungsaktion an.

Konfiguration über die CLI Geben Sie die folgenden Befehle an der Eingabeaufforderung ein. Beispiele werden nach jedem Befehl angegeben.

1. MBF aktivieren.

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

2. Aktivieren Sie das Feature.

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

3. Profil 1 für Service 1 hinzufügen.

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



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

Beispiel:

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

4. Profil 2 für Service 2 hinzufügen.

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

Beispiel:

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

5. Service 1 hinzufügen. Geben Sie eine Dummy-IP-Adresse an, die keinem der Geräte gehört, einschließlich der Inline-Geräte. Setzen Sie `use source IP address` (USIP) auf YES. Setzen Sie `useproxyport` auf NO. Schalten Sie den Integritätsmonitor aus. Aktivieren Sie die Integritätsüberwachung nur, wenn Sie diesen Dienst an einen TCP-Monitor binden. Wenn Sie einen Monitor an einen Dienst binden, setzen Sie die Option TRANSPARENT im Monitor auf ON.

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

Beispiel:

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

6. Service 2 hinzufügen. Geben Sie eine Dummy-IP-Adresse an, die keinem der Geräte gehört, einschließlich der Inline-Geräte. Setzen Sie `use source IP address` (USIP) auf YES. Setzen Sie `useproxyport` auf NO. Schalten Sie den Integritätsmonitor aus. Aktivieren Sie die Integritätsüberwachung nur, wenn Sie diesen Dienst an einen TCP-Monitor binden. Wenn Sie einen Monitor an einen Dienst binden, setzen Sie die Option TRANSPARENT im Monitor auf ON.

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


Beispiel:

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

7. Fügen Sie einen virtuellen Lastenausgleichsserver hinzu.

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

Beispiel:

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

8. Binden Sie die Dienste an den virtuellen Lastenausgleichsserver.

```
bind lb vserver <LB_VSERVER_NAME> <service_name>
bind lb vserver <LB_VSERVER_NAME> <service_name>
<!--NeedCopy-->
```

Beispiel:

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

9. Geben Sie den virtuellen Lastausgleichsserver in der Inhaltsüberprüfungsaktion an.

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

Beispiel:

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

10. Fügen Sie eine Richtlinie zur Inhaltsüberprüfung hinzu. Geben Sie die Inhaltsinspektionsaktion in der Richtlinie an.

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

Beispiel:

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE("
   CONNECT")" -action ips_action
```



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

11. Fügen Sie einen virtuellen Proxyserver hinzu.

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

Beispiel:

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

12. Binden Sie die Richtlinie zur Inhaltsüberprüfung an den virtuellen Server.

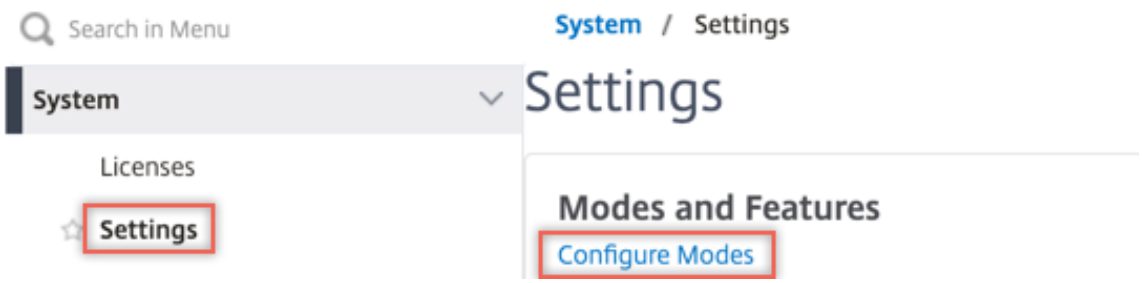
```
bind cs vserver <name> -policyName <string> -priority <
    positive_integer> -gotoPriorityExpression <expression> -type
    REQUEST
<!--NeedCopy-->
```

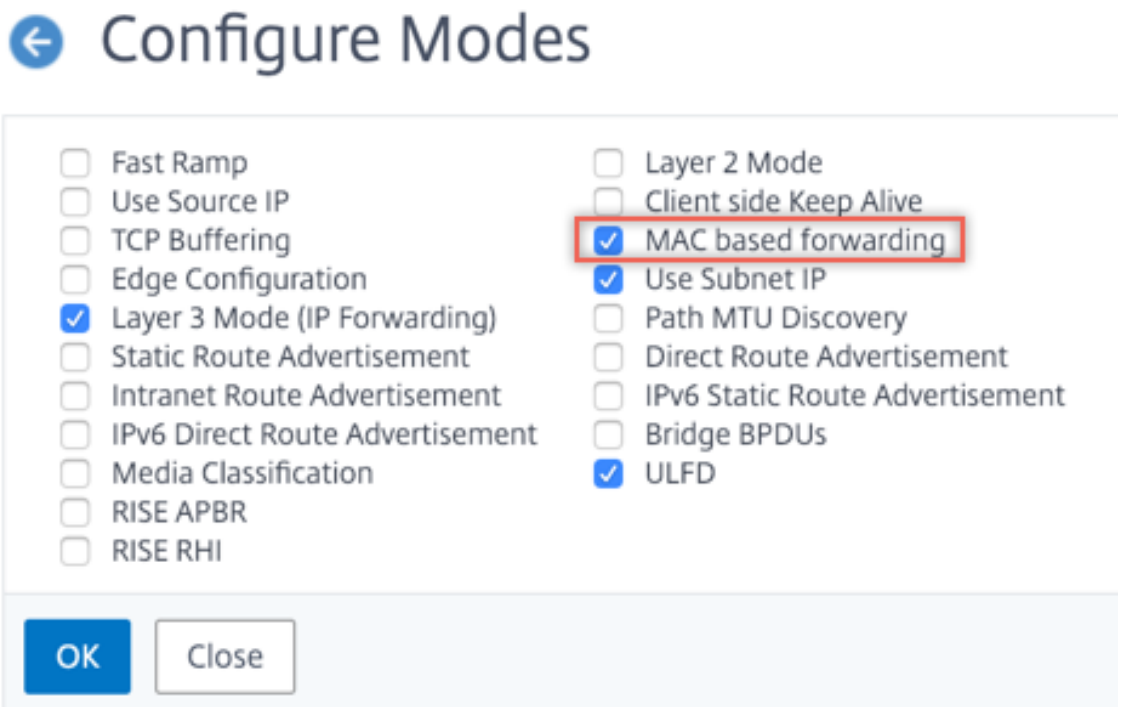
Beispiel:

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

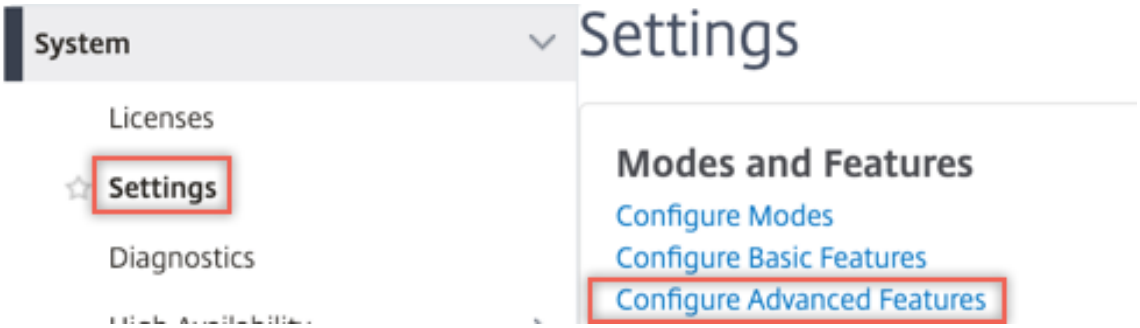
Konfiguration über die GUI

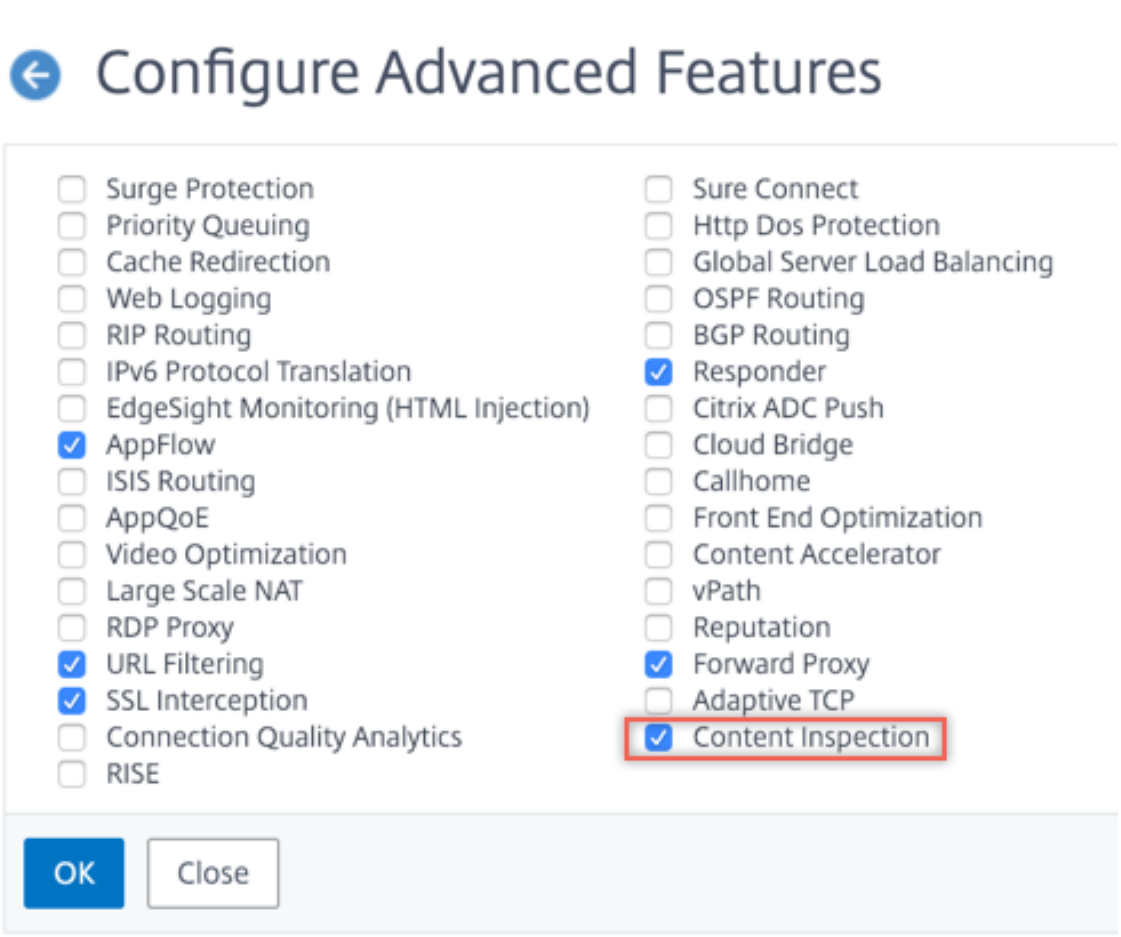
1. Navigieren Sie zu **System > Einstellungen**. Klicken Sie unter **Modi und Features** auf **Modi konfigurieren**.



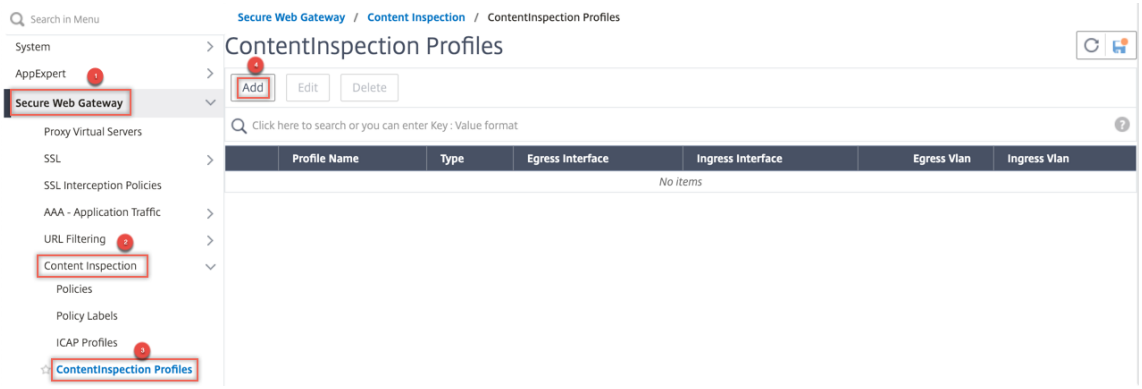


2. Navigieren Sie zu **System > Einstellungen**. Klicken Sie unter **Modi und Features** auf **Erweiterte Funktionen konfigurieren**.

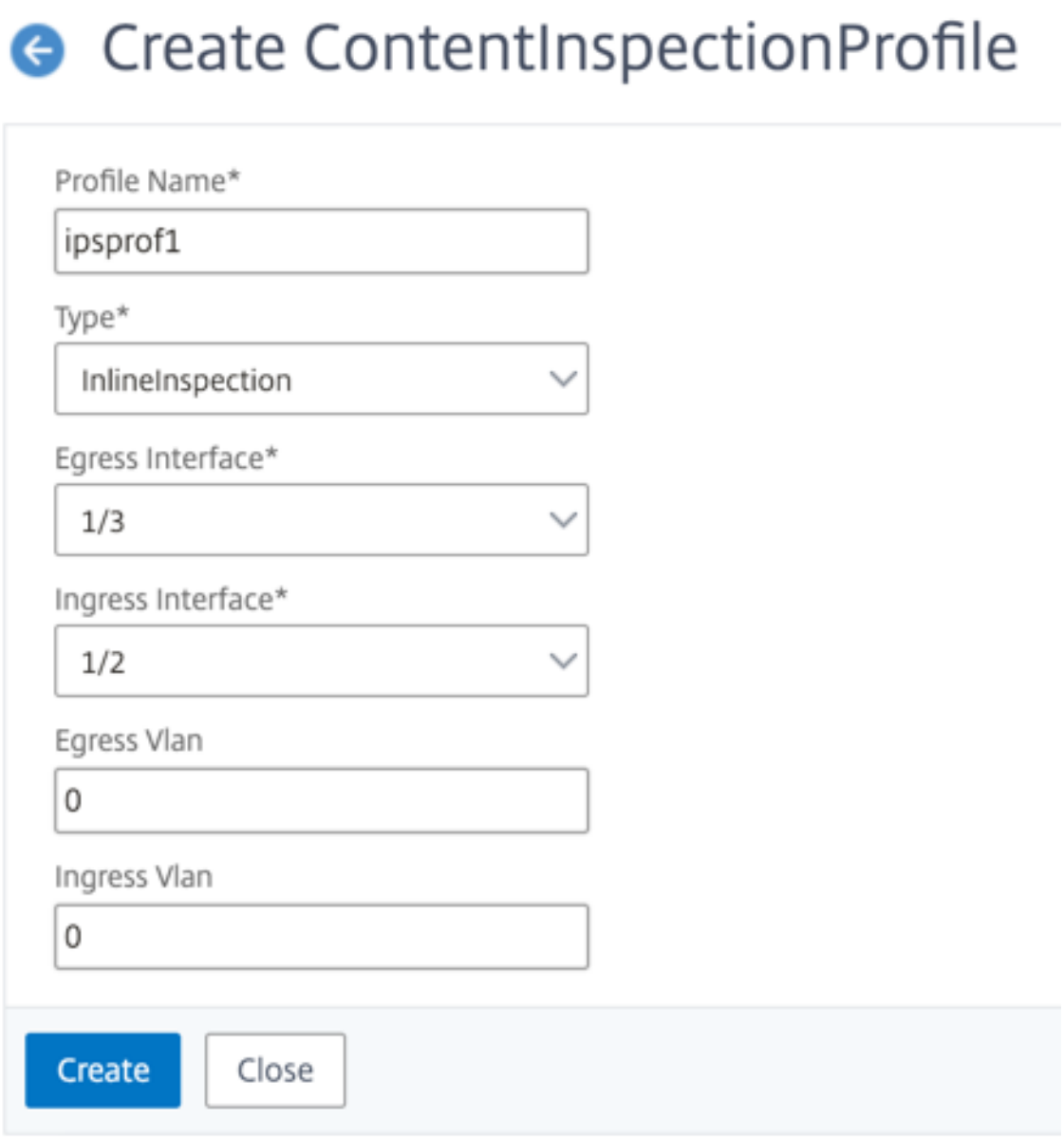




3. Navigieren Sie zu **Secure Web Gateway > Content Inspection > Content Inspection Profile**. Klicken Sie auf **Hinzufügen**.

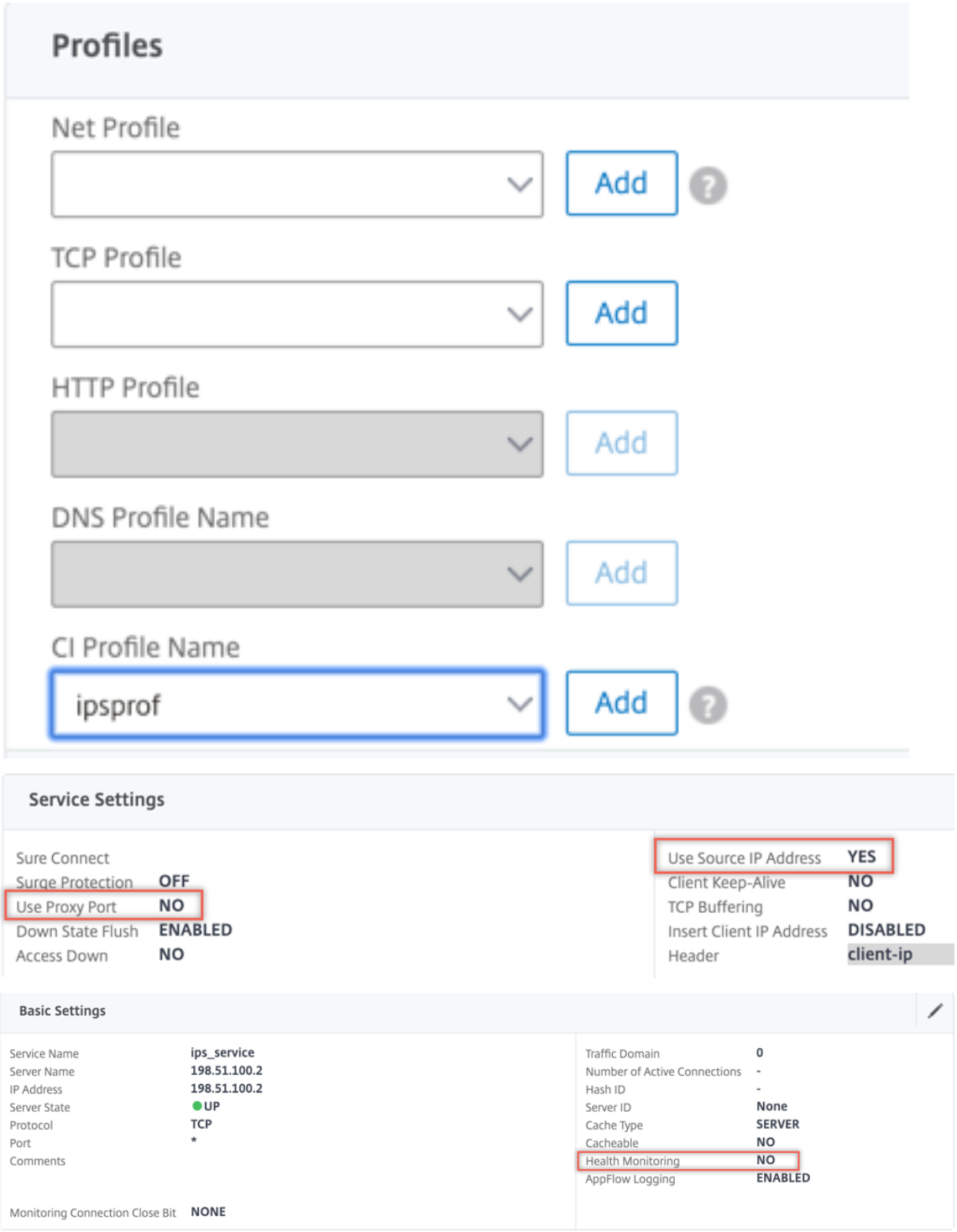


Geben Sie die Eingangs- und Ausgangsschnittstellen an.



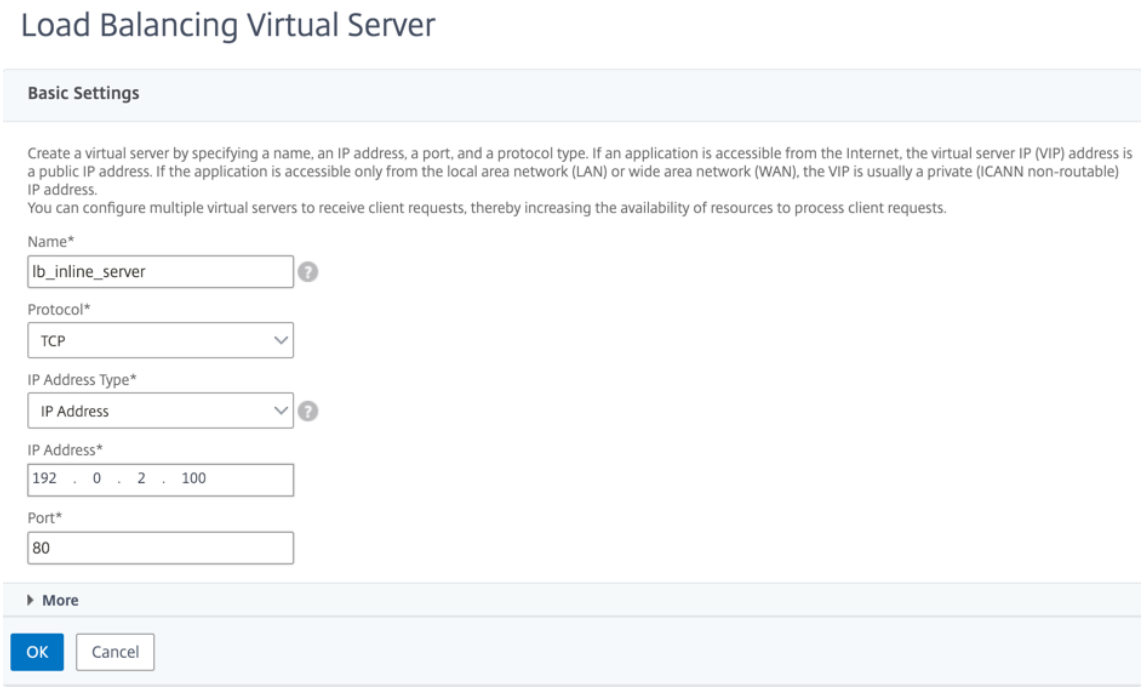
Erstellen Sie zwei Profile. Geben Sie im zweiten Profil eine andere Eingangs- und Ausgangsschnittstelle an.

4. Navigieren Sie zu **Load Balancing > Services > Hinzufügen** und fügen Sie einen Service hinzu. Klicken Sie unter **Erweiterte Einstellungen** auf **Profile**. Wählen Sie in der Liste **CI-Profilname** das zuvor erstellte Content-Inspektionsprofil aus. Legen Sie unter **Diensteinstellungen** die Option **Quell-IP-Adresse verwenden** auf Ja und **Proxyport verwenden** auf Nein fest. Legen Sie in den **Grundeinstellungen** die **Integritätsüberwachung** auf Nein fest. Aktivieren Sie die Integritätsüberwachung nur, wenn Sie diesen Dienst an einen TCP-Monitor binden. Wenn Sie einen Monitor an einen Dienst binden, setzen Sie die Option TRANSPARENT im Monitor auf ON.



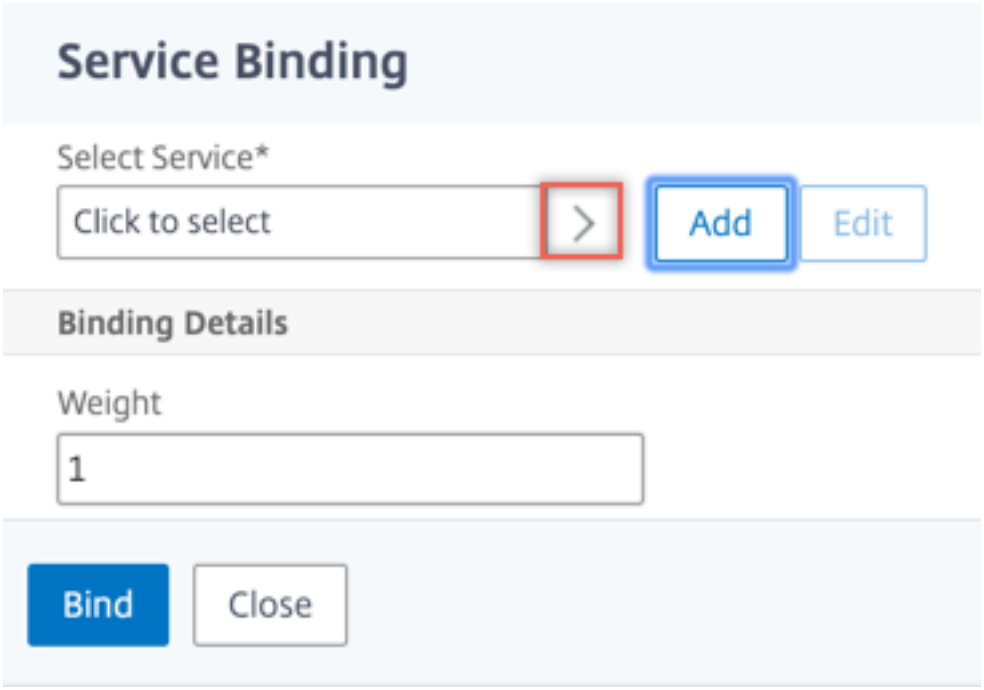
Erstellen Sie zwei Dienste. Geben Sie Dummy-IP-Adressen an, die keinem der Geräte gehören, einschließlich der Inline-Geräte.

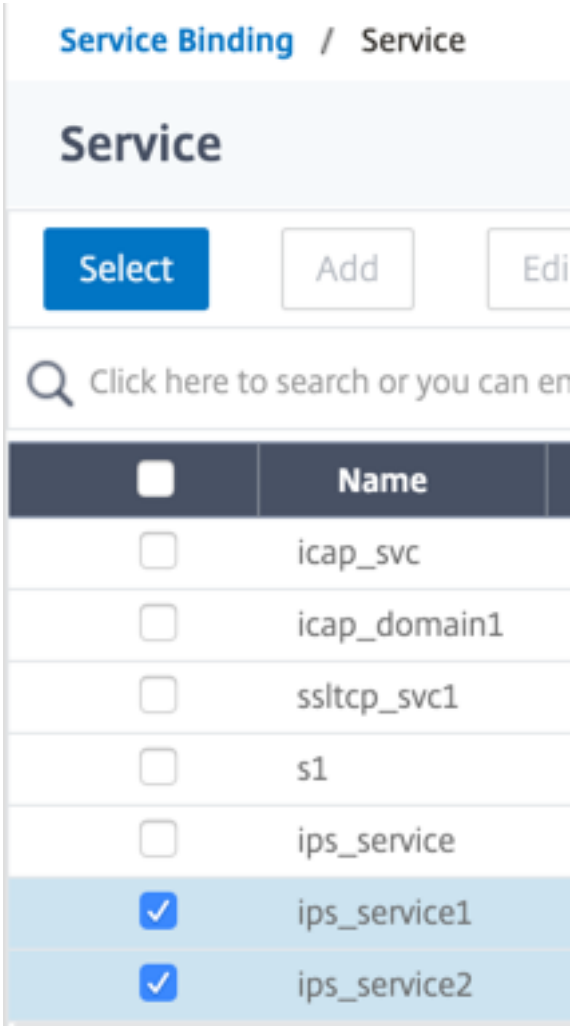
5. Navigieren Sie zu **Lastenausgleich > Virtuelle Server > Hinzufügen**. Erstellen Sie einen virtuellen TCP-Load Balancing Server.

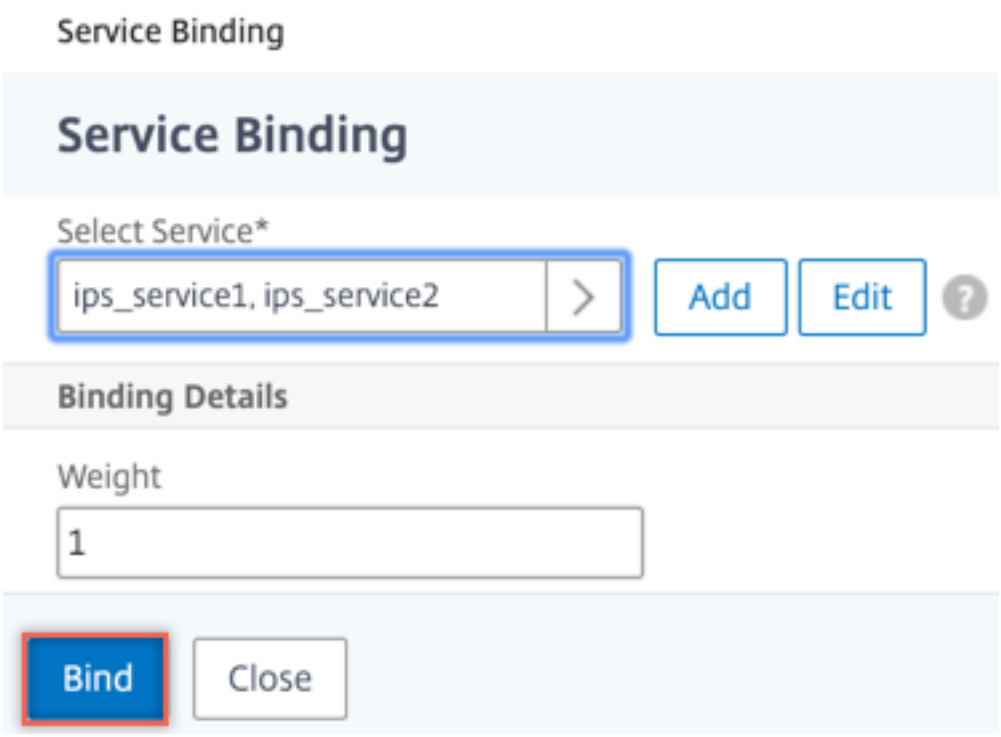


Klicken Sie auf **OK**.

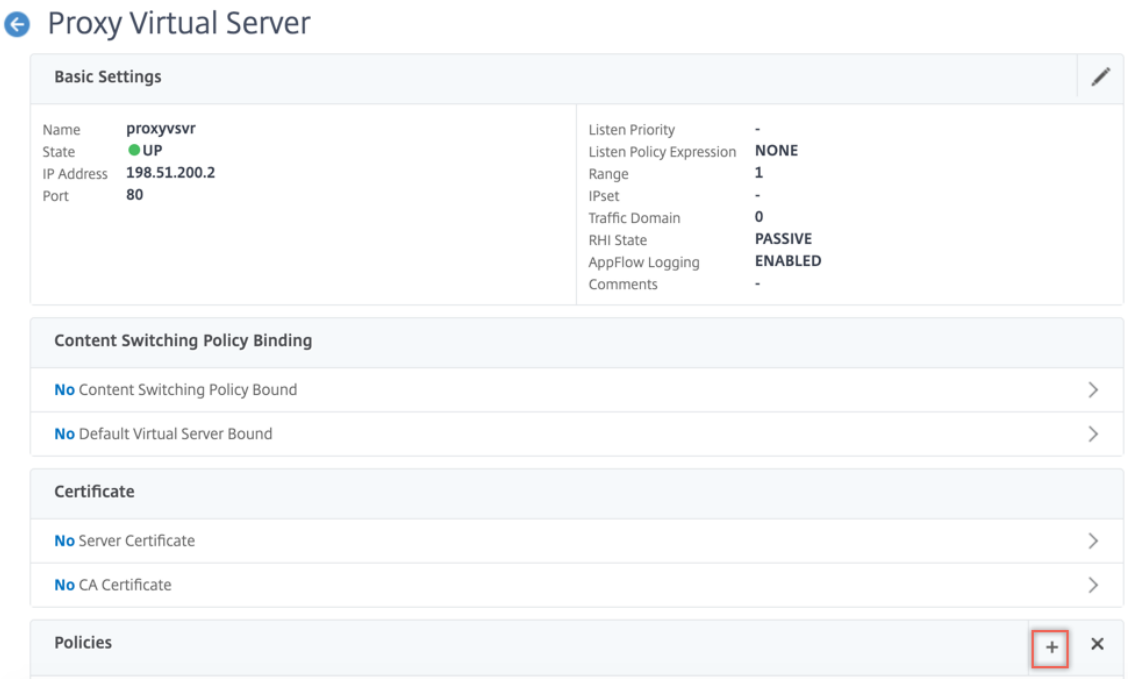
6. Klicken Sie in den Abschnitt **Load Balancing Virtual Server Service Binding**. Klicken Sie unter **Dienstbindung** auf den Pfeil unter **Dienst auswählen**. Wählen Sie die beiden zuvor erstellten Dienste aus, und klicken Sie auf **Auswählen**. Klicken Sie auf **Bind**.



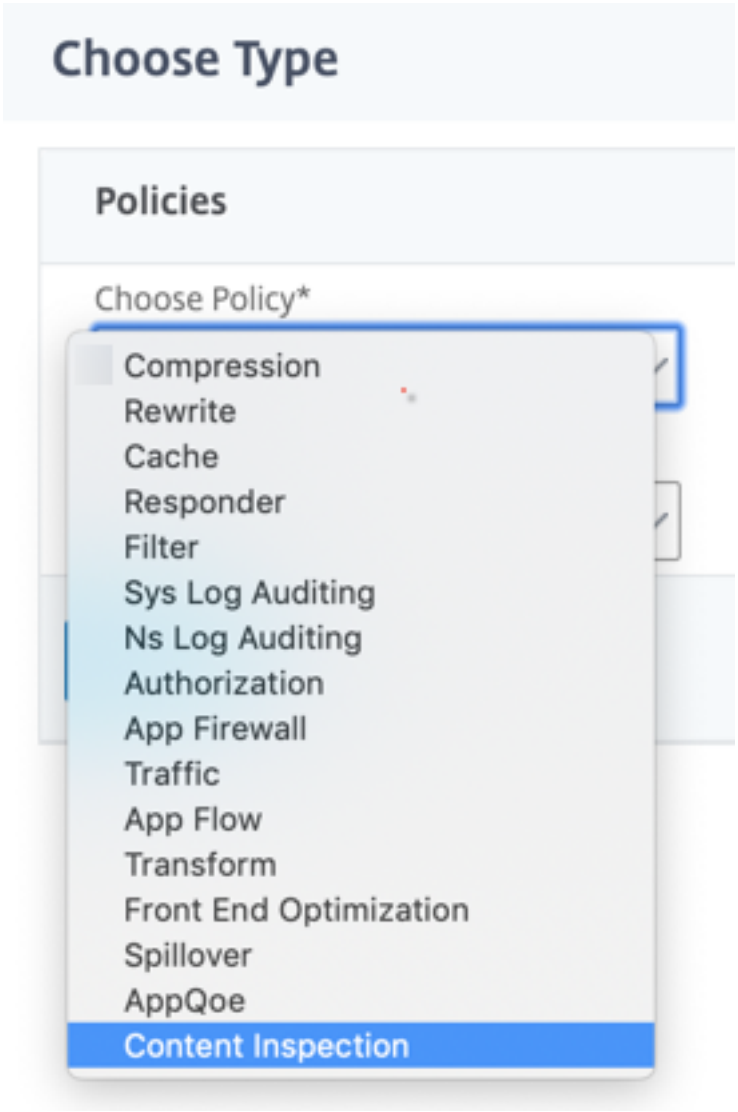




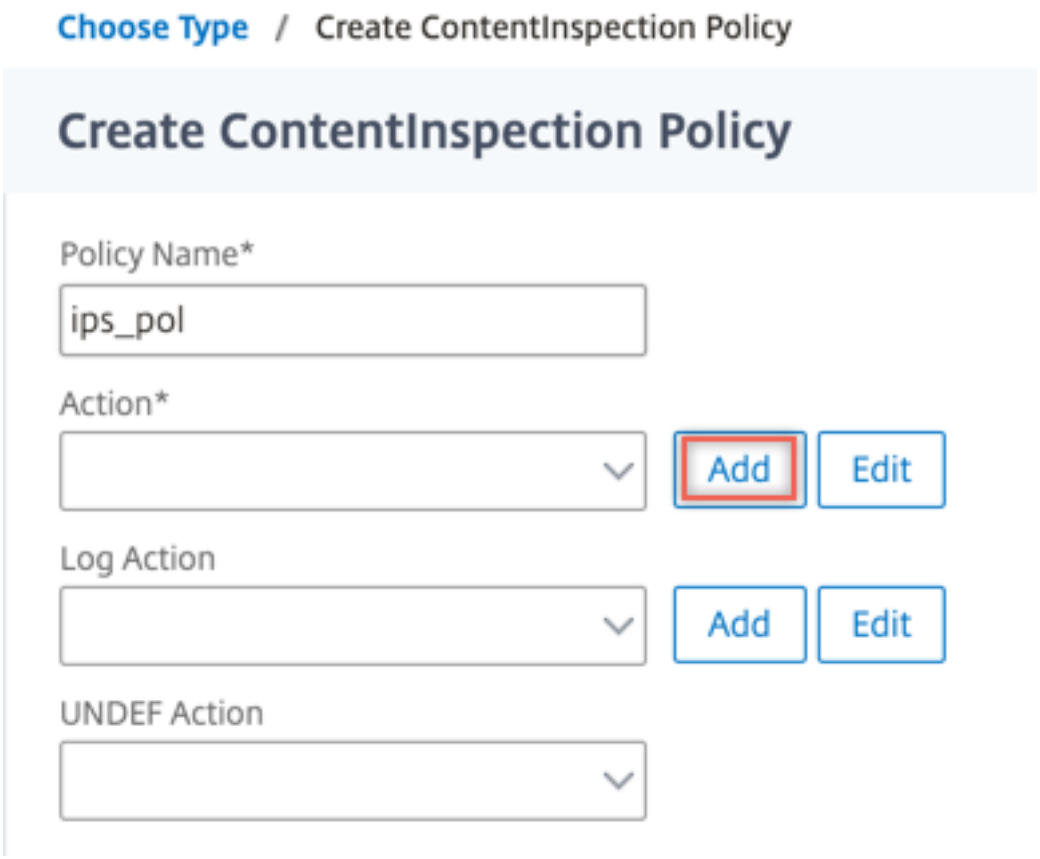
7. Navigieren Sie zu **Secure Web Gateway > Virtuelle Proxyserver > Hinzufügen**. Geben Sie einen Namen, eine IP-Adresse und einen Port an. Wählen Sie unter **Erweiterte Einstellungen** die Option **Richtlinien**aus. Klicken Sie auf das +-Zeichen.



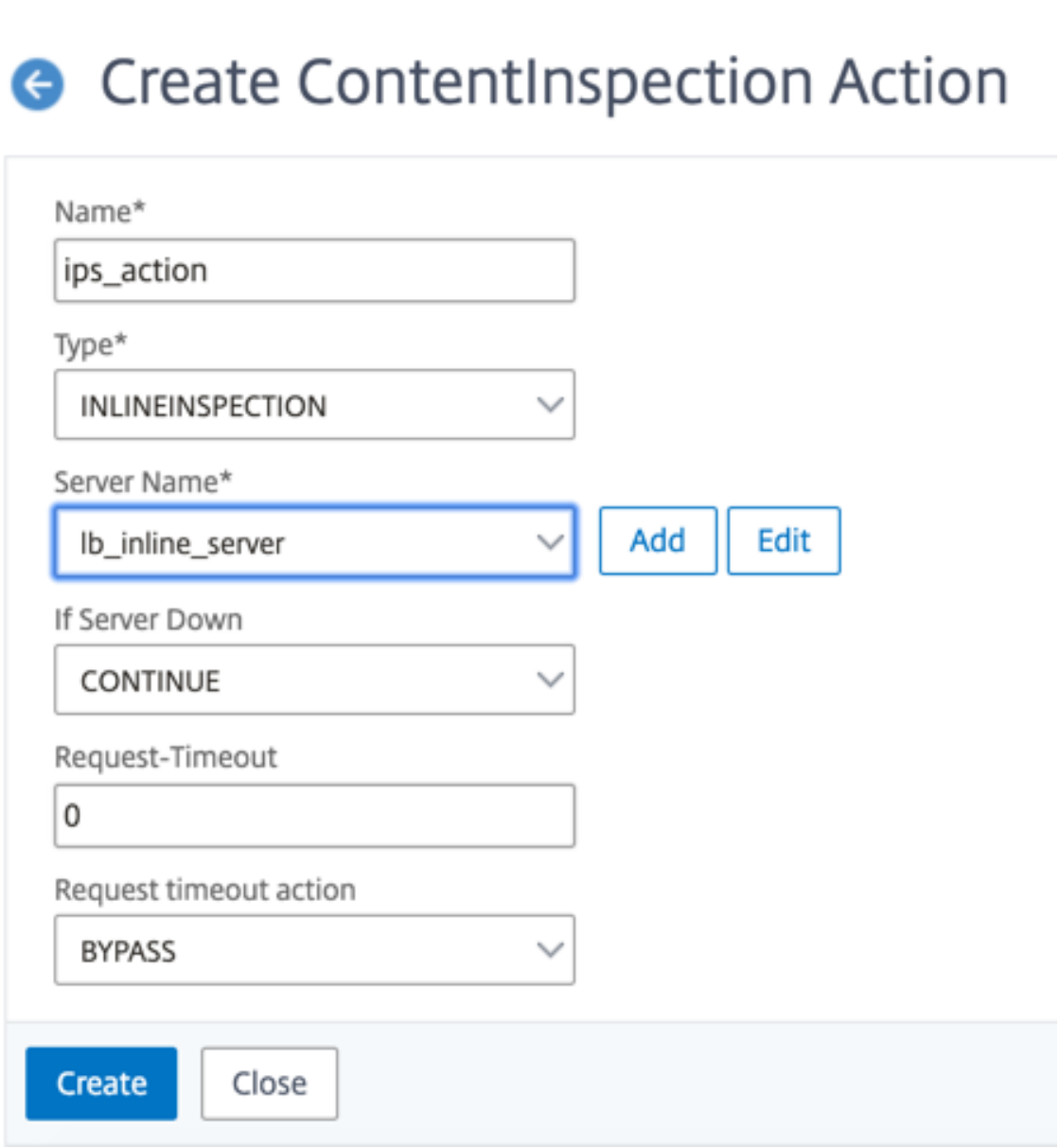
8. Wählen Sie unter **Richtlinie auswählen** die Option **Inhaltsüberprüfung** aus. Klicken Sie auf **Weiter**.



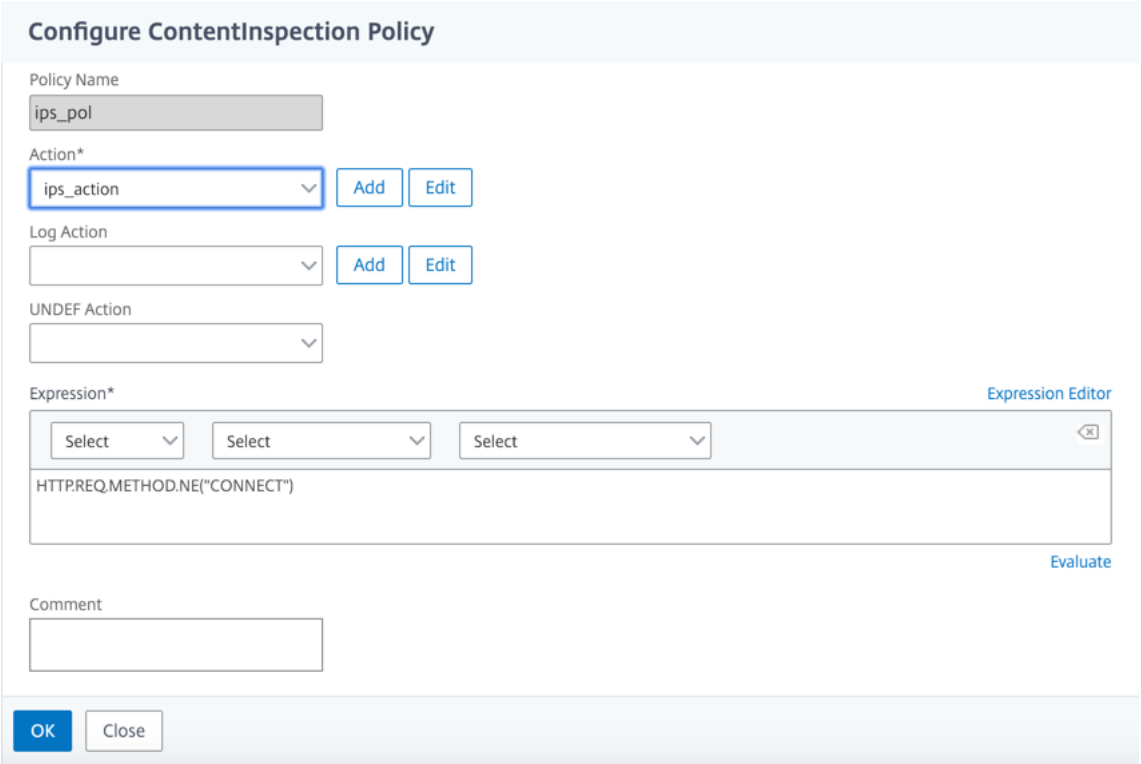
9. Klicken Sie auf **Hinzufügen**. Geben Sie einen Namen an. Klicken Sie unter **Aktion** auf **Hinzufügen**.



10. Geben Sie einen Namen an. Wählen Sie unter **Typ** die Option **INLINEINSPECTION** aus. Wählen Sie unter **Servername** den zuvor erstellten virtuellen Lastenausgleichsserver aus.



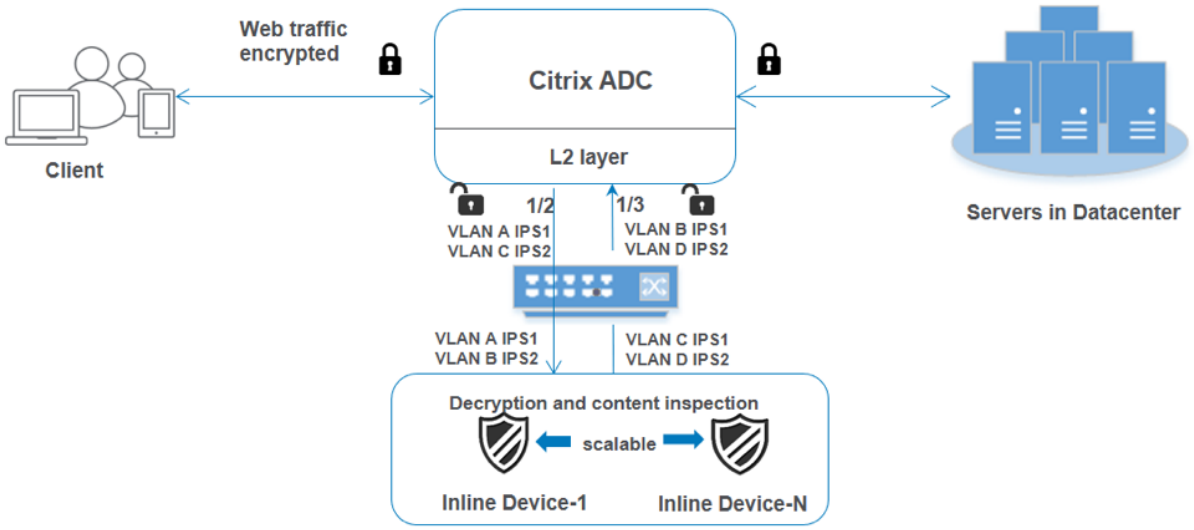
11. Klicken Sie auf **Erstellen**. Geben Sie die Regel an, und klicken Sie auf **Erstellen**.



12. Klicken Sie auf **Bind**.
13. Klicken Sie auf **Fertig**.

Szenario 3: Lastausgleich mehrerer Inline-Geräte mit gemeinsamen Schnittstellen

Wenn Sie zwei oder mehr Inline-Geräte verwenden, können Sie die Geräte mit verschiedenen Contentinspektionsdiensten mit gemeinsam genutzten Schnittstellen ausgleichen. In diesem Fall gleicht die Citrix SWG-Appliance die Teilmenge des Datenverkehrs aus, der über eine gemeinsame Schnittstelle an jedes Gerät gesendet wird. Die Teilmenge wird basierend auf den konfigurierten Richtlinien festgelegt. Beispielsweise werden TXT- oder Bilddateien möglicherweise nicht zur Überprüfung an die Inline-Geräte gesendet.



Die Basiskonfiguration bleibt dieselbe wie in Szenario 2. Binden Sie für dieses Szenario die Schnittstellen an verschiedene VLANs, um den Datenverkehr für jedes Inline-Gerät zu trennen. Geben Sie die VLANs in den Content-Inspektionsprofilen an. Führen Sie die folgenden zusätzlichen Schritte aus:

1. Binden Sie die freigegebenen Schnittstellen an verschiedene VLANs.
2. Geben Sie die Ein- und Ausgangs-VLANs in den Content-Inspektionsprofilen an.

Konfiguration über die CLI Geben Sie die folgenden Befehle an der Eingabeaufforderung ein. Beispiele werden nach jedem Befehl angegeben.

1. MBF aktivieren.

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

2. Aktivieren Sie das Feature.

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

3. Binden Sie die freigegebenen Schnittstellen an verschiedene VLANs.

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

Beispiel:

```
bind vlan 100  – ifnum 1/2 tagged
bind vlan 200  – ifnum 1/3 tagged
```



```
bind vlan 300 –ifnum 1/2 tagged
bind vlan 400 –ifnum 1/3 tagged
<!--NeedCopy-->
```

4. Profil 1 für Service 1 hinzufügen. Geben Sie die Ein- und Aus-VLANs im Profil an.

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

Beispiel:

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

5. Profil 2 für Service 2 hinzufügen. Geben Sie die Ein- und Aus-VLANs im Profil an.

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

Beispiel:

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

6. Service 1 hinzufügen.

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

Beispiel:

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

7. Service 2 hinzufügen.

```
add service <service_name>  <IP> TCP <Port> -
    contentinspectionProfileName <Name>  -healthMonitor NO  -usip
    YES –useproxyport NO
```



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

Beispiel:

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

8. Fügen Sie einen virtuellen Lastenausgleichsserver hinzu.

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

Beispiel:

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

9. Binden Sie die Dienste an den virtuellen Lastenausgleichsserver.

```
bind lb vserver <LB_VSERVER_NAME> <service_name>
bind lb vserver <LB_VSERVER_NAME> <service_name>
<!--NeedCopy-->
```

Beispiel:

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

10. Geben Sie den virtuellen Lastausgleichsserver in der Inhaltsüberprüfungsaktion an.

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

Beispiel:

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

11. Fügen Sie eine Richtlinie zur Inhaltsüberprüfung hinzu. Geben Sie die Inhaltsinspektionsaktion in der Richtlinie an.

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

Beispiel:


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

12. Fügen Sie einen virtuellen Proxyserver hinzu.

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

Beispiel:

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

13. Binden Sie die Richtlinie zur Inhaltsüberprüfung an den virtuellen Server.

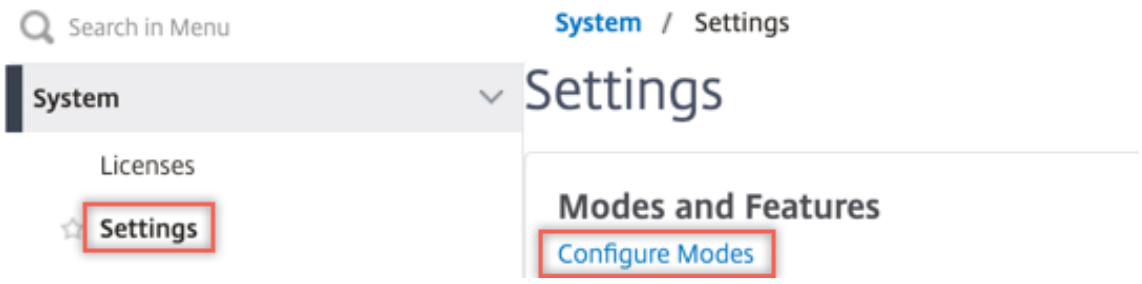
```
bind cs vserver <name> -policyName <string> -priority <
    positive_integer> -gotoPriorityExpression <expression> -type
    REQUEST
<!--NeedCopy-->
```

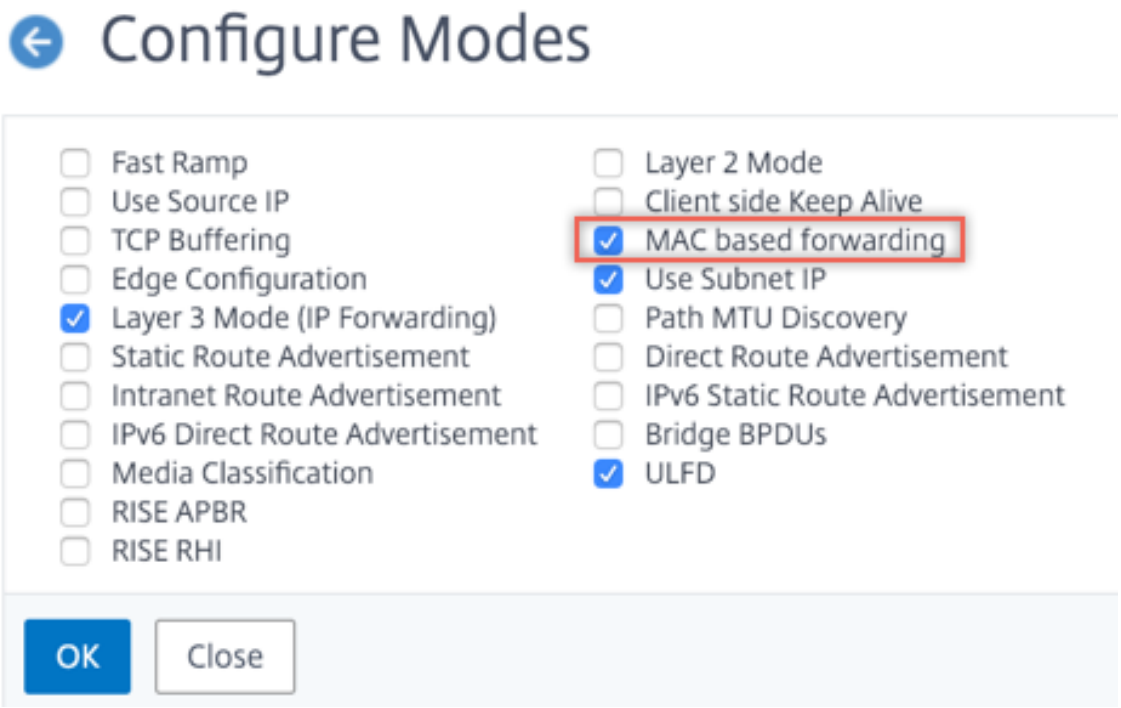
Beispiel:

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

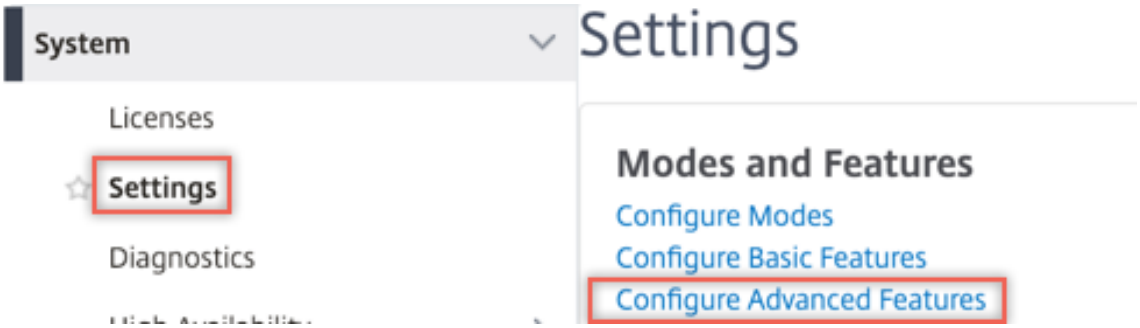
Konfiguration über die GUI

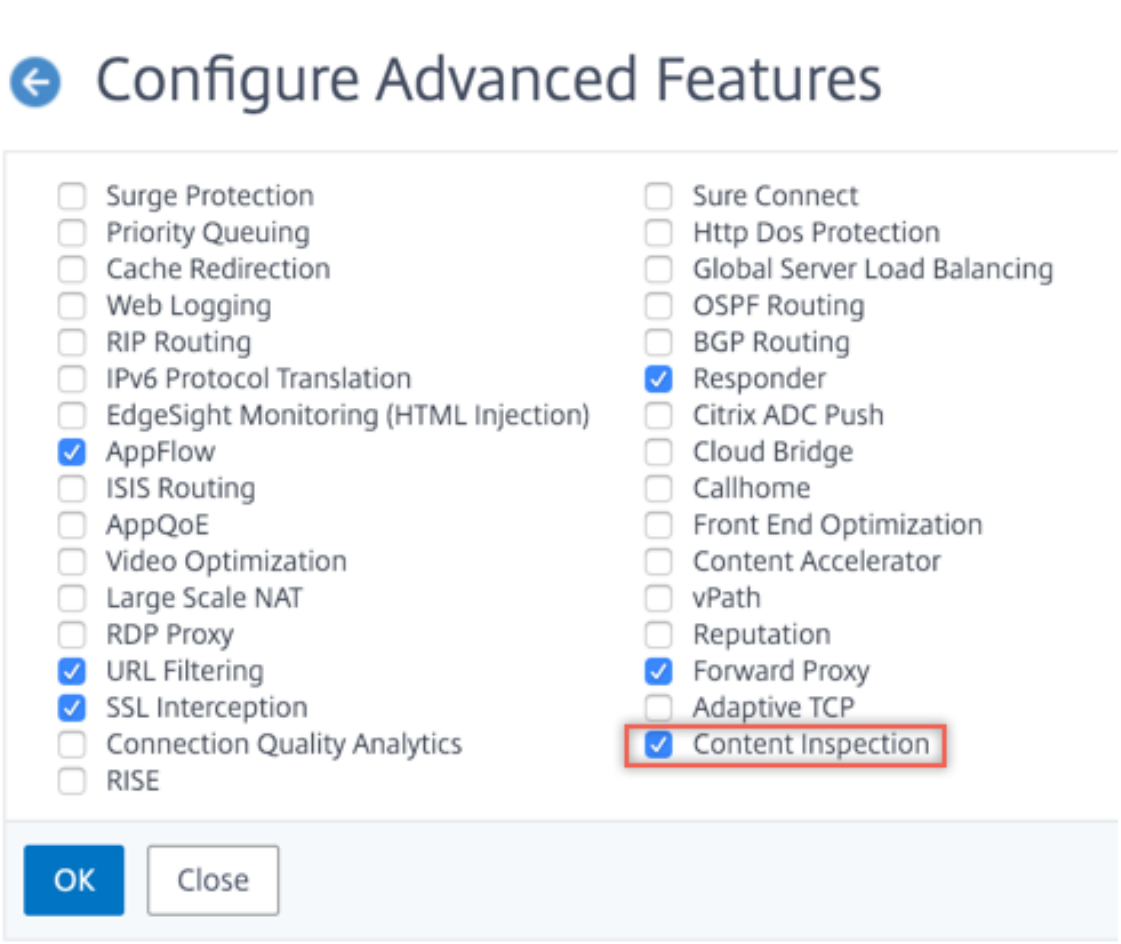
1. Navigieren Sie zu **System > Einstellungen**. Klicken Sie unter **Modi und Features** auf **Modi konfigurieren**.



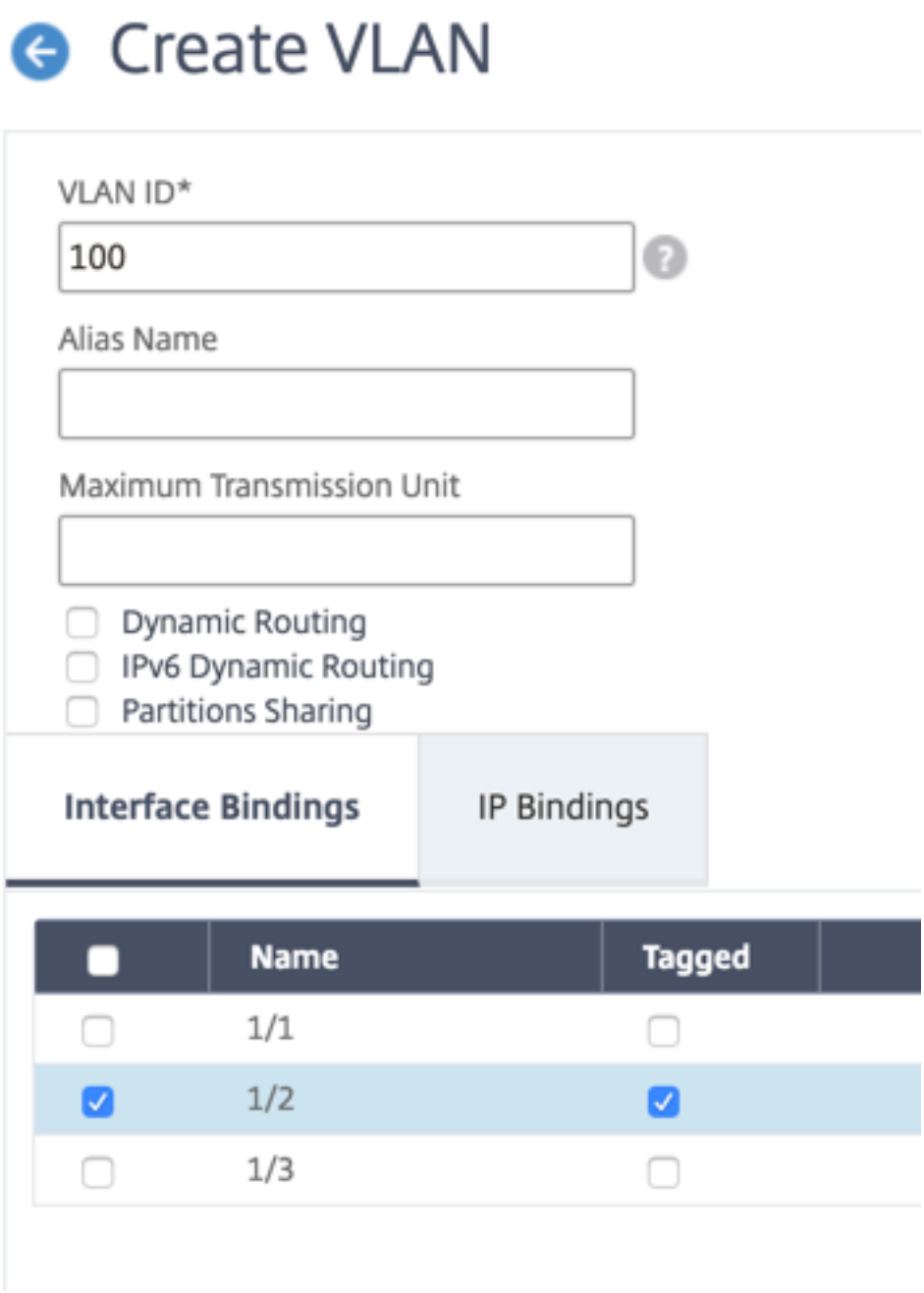


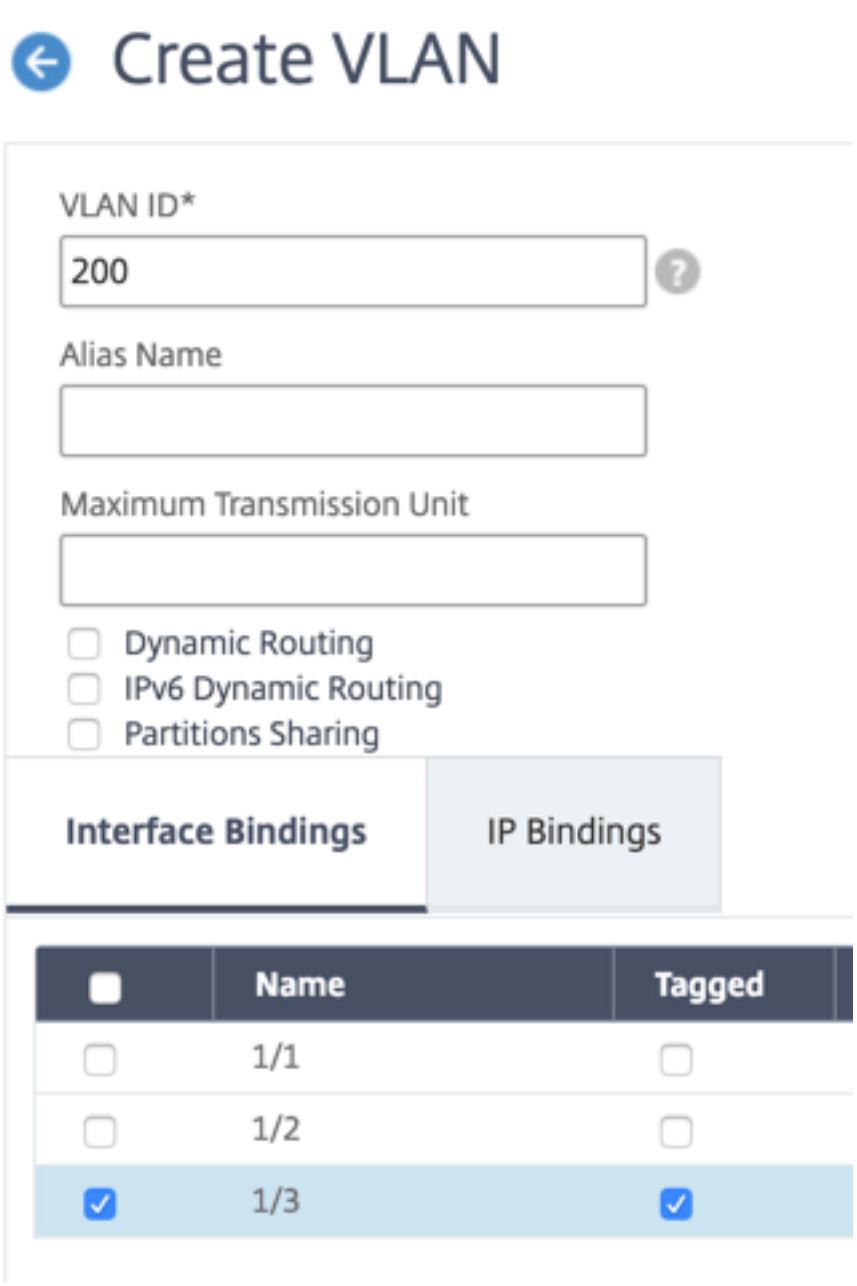
2. Navigieren Sie zu **System > Einstellungen**. Klicken Sie unter **Modi und Features** auf **Erweiterte Funktionen konfigurieren**.

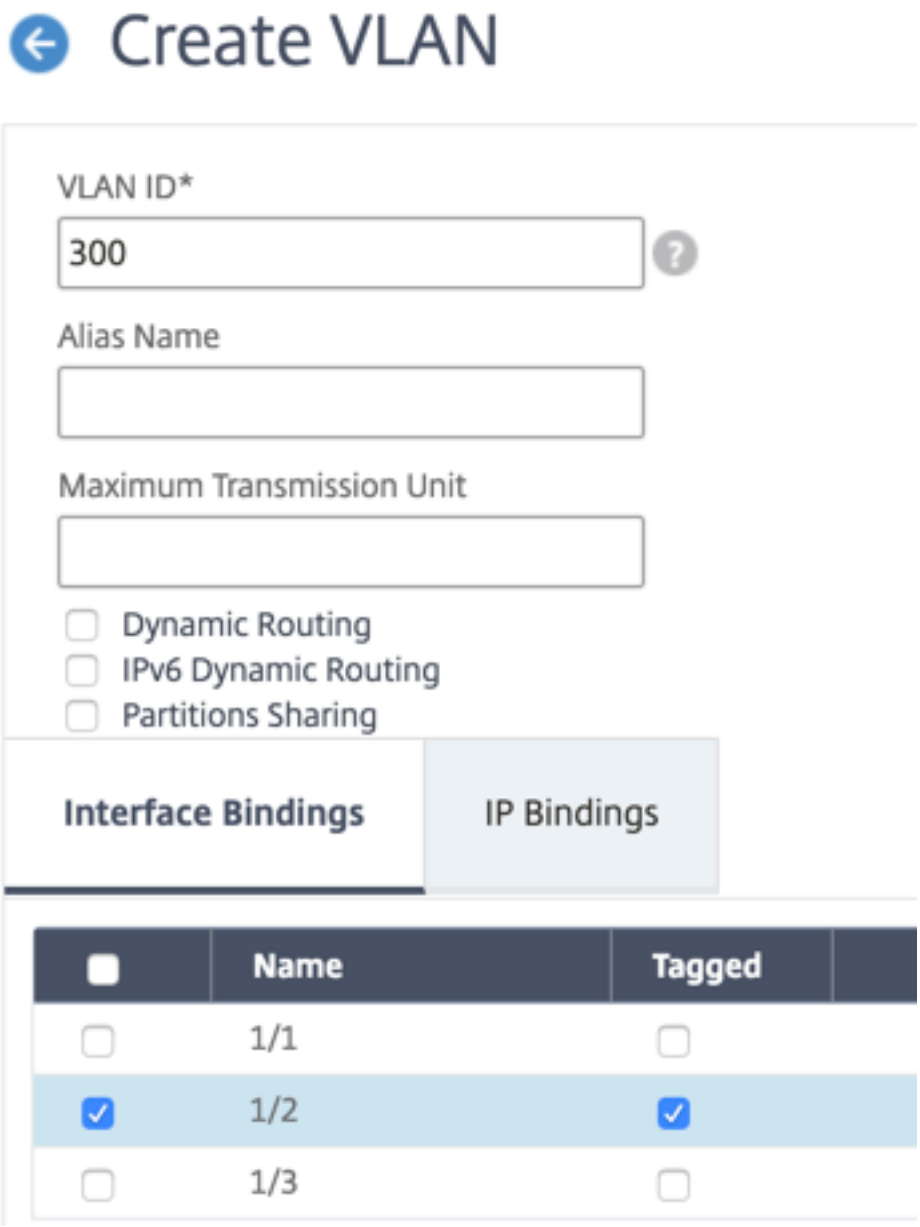


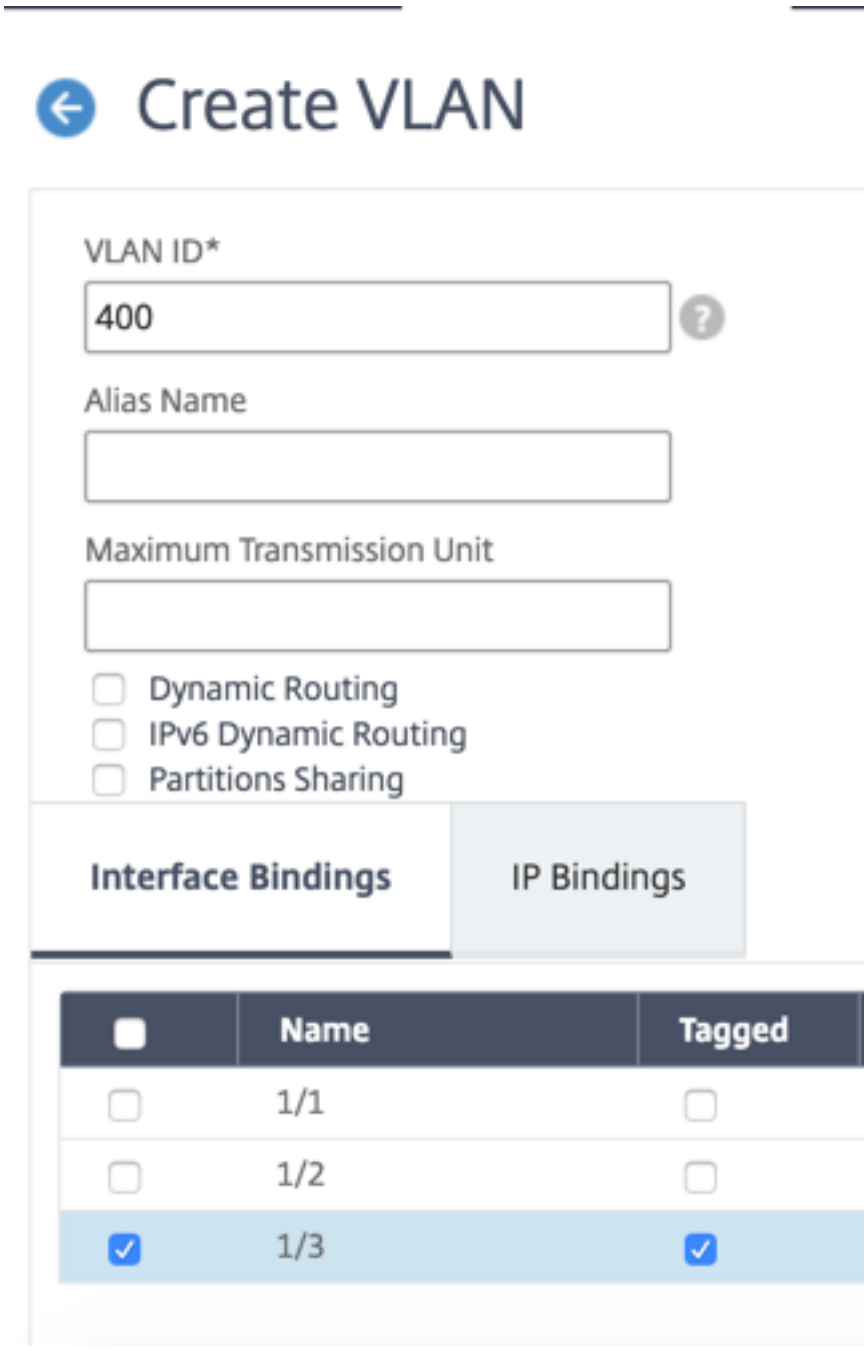


3. Navigieren Sie zu **System > Netzwerk > VLANs > Hinzufügen**. Fügen Sie vier VLANs hinzu und markieren Sie sie den Schnittstellen.

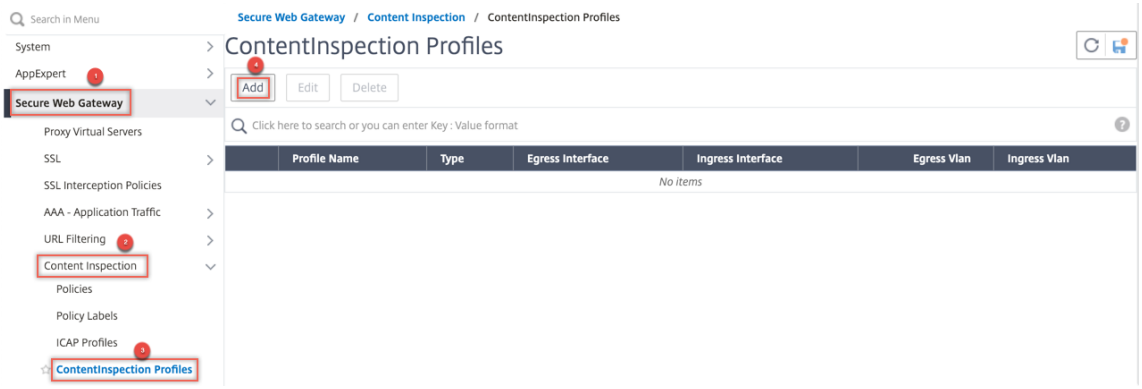




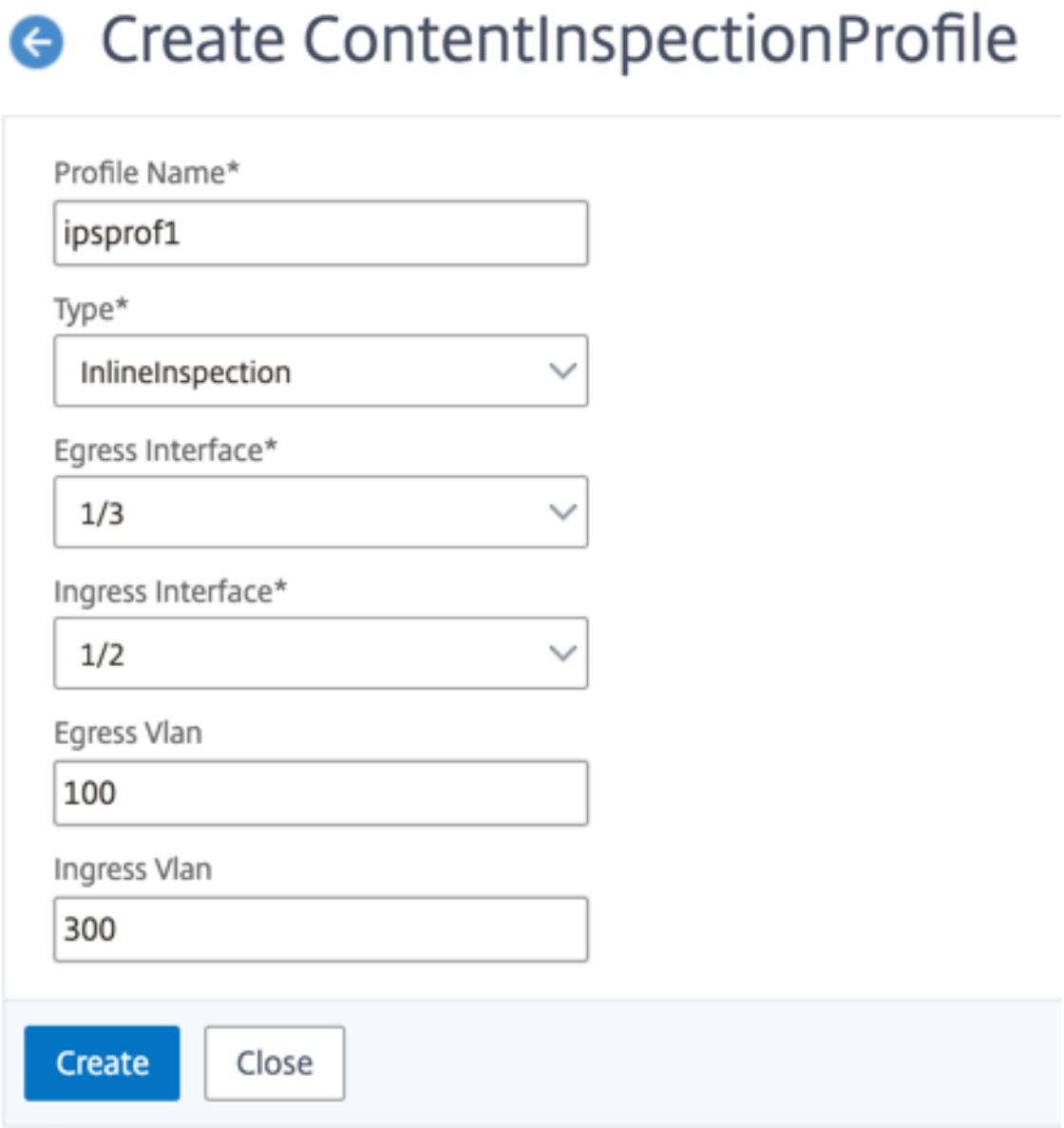




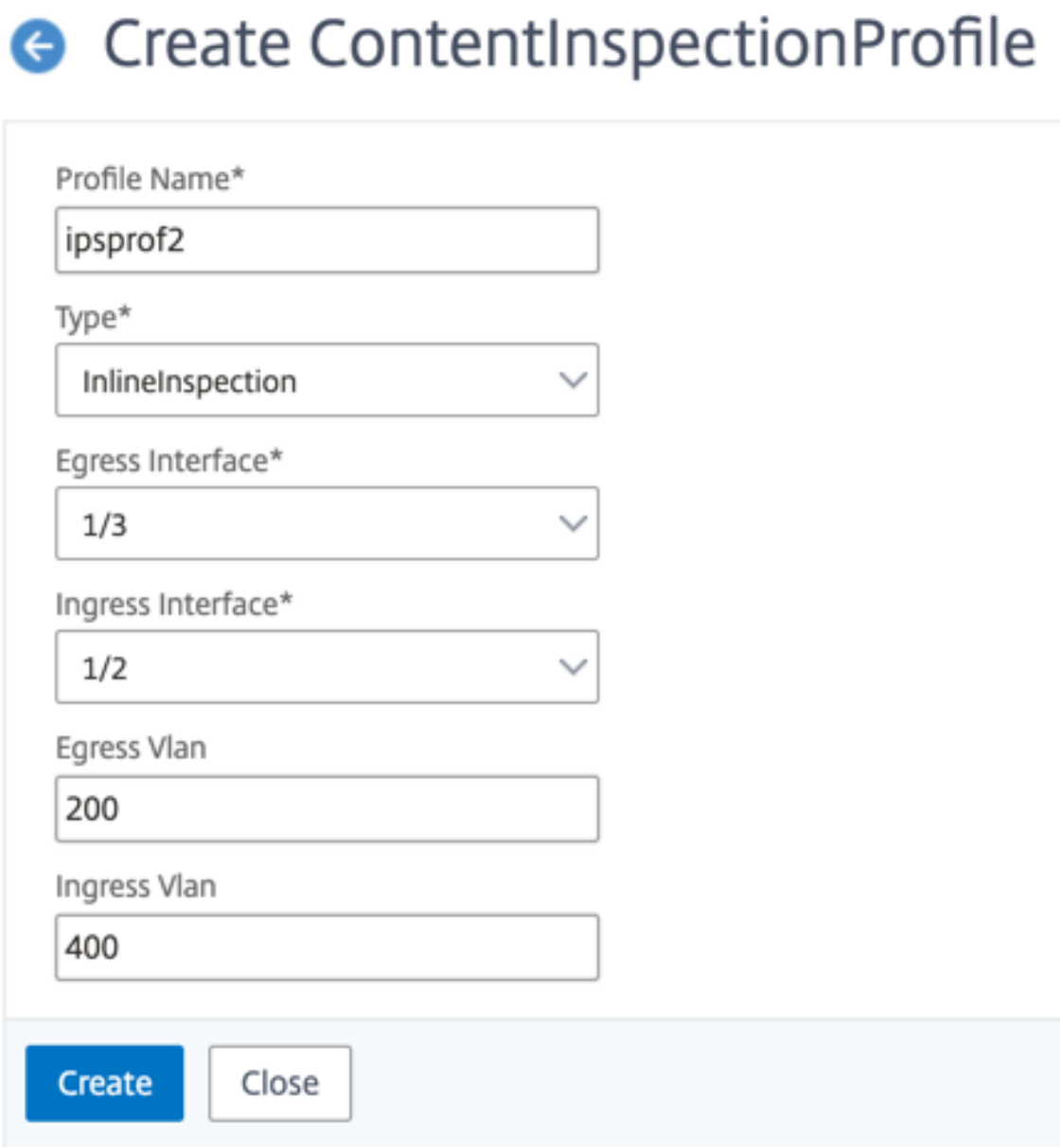
4. Navigieren Sie zu **Secure Web Gateway > Content Inspection > Content Inspection Profile**. Klicken Sie auf **Hinzufügen**.



Geben Sie die Ein- und Aus-VLANs an.

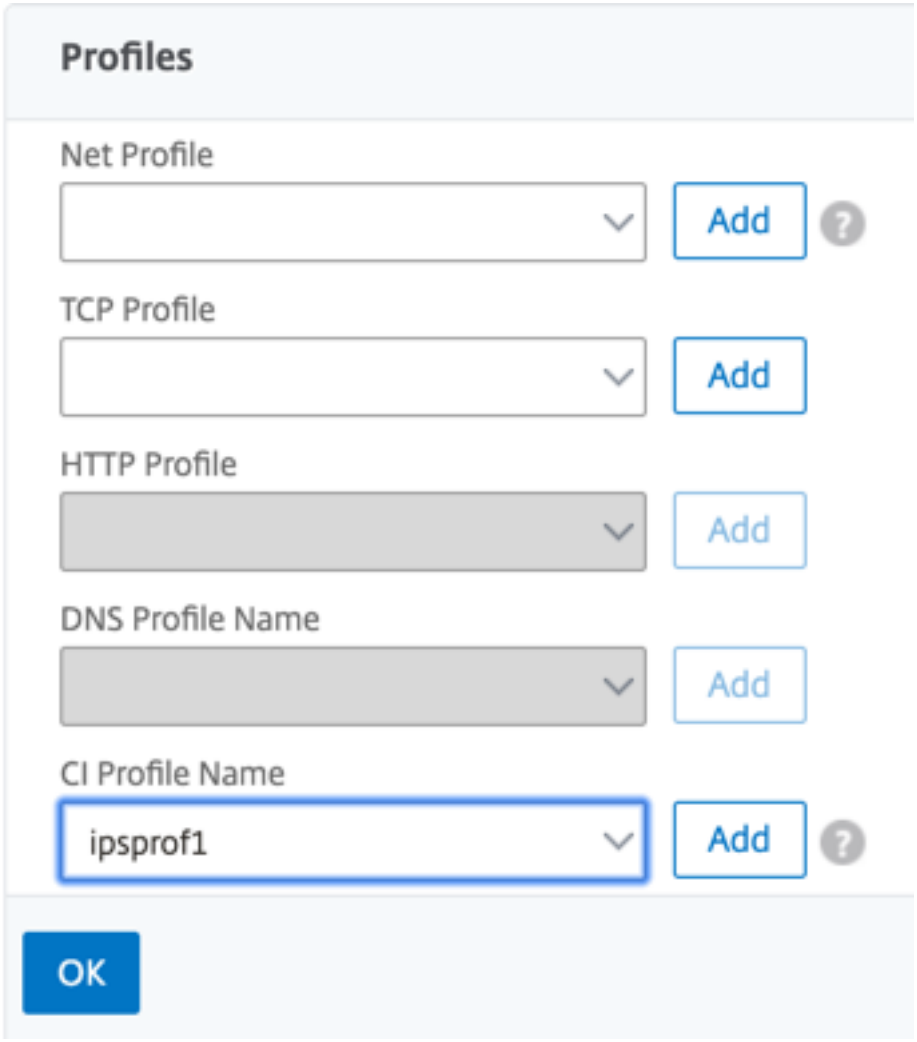


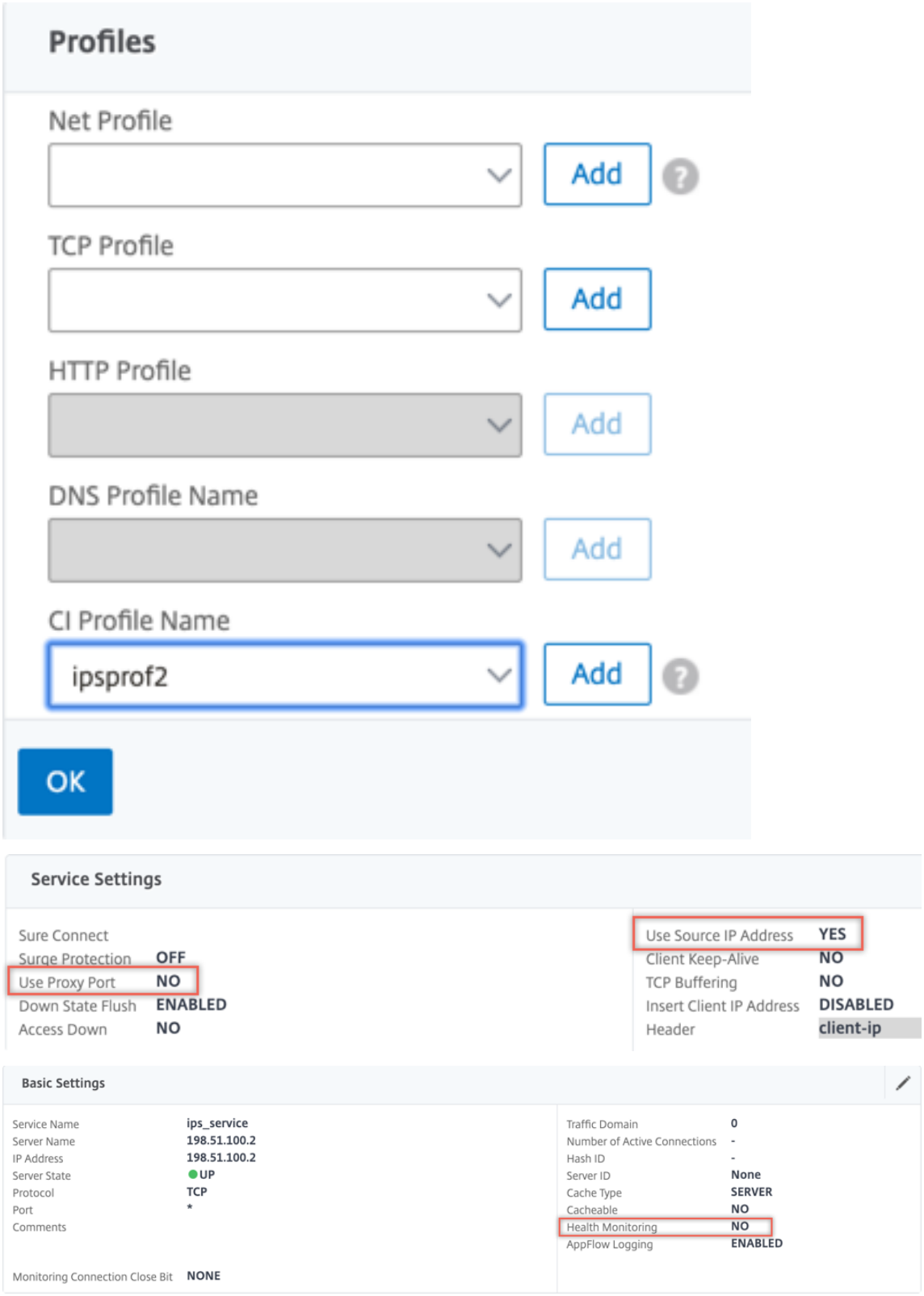
Erstellen Sie weitere Profile. Geben Sie im zweiten Profil ein anderes Ingress- und Egress-VLAN an.



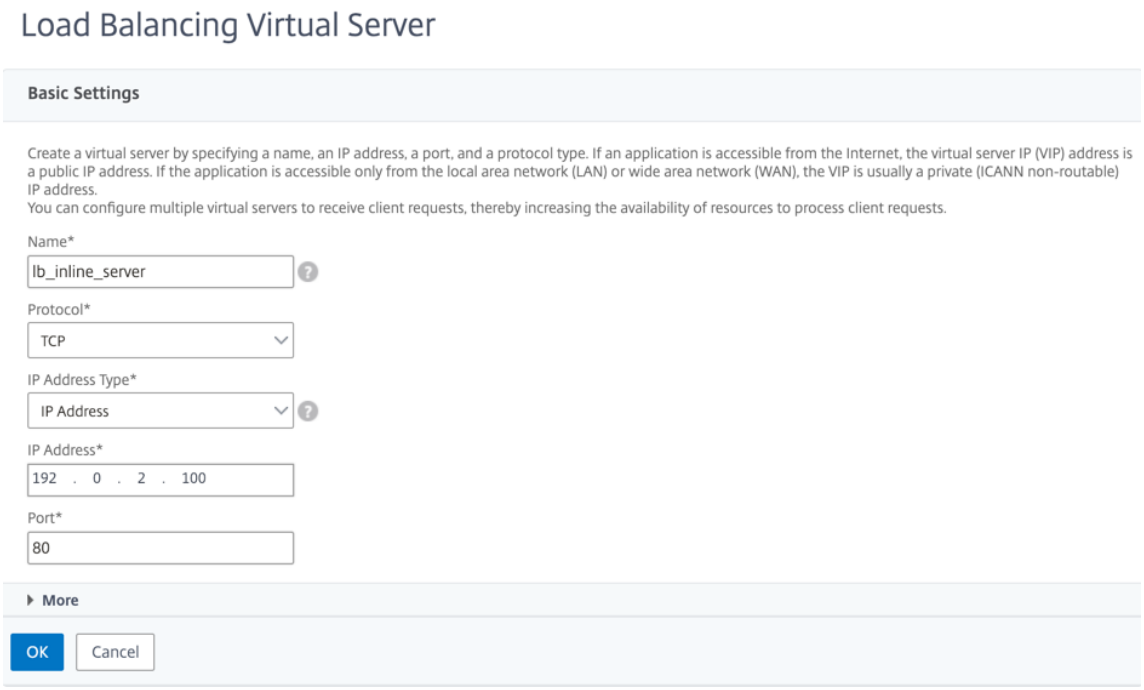
5. Navigieren Sie zu **Load Balancing > Services > Hinzufügen** und fügen Sie einen Service hinzu. Klicken Sie unter **Erweiterte Einstellungen** auf **Profile**. Wählen Sie in der Liste **CI-Profilname** das zuvor erstellte Content-Inspektionsprofil aus. Legen Sie unter **Diensteinstellungen** die Option **Quell-IP-Adresse verwenden** auf Ja und **Proxyport verwenden** auf Nein fest. Legen Sie in den **Grundeinstellungen** die **Integritätsüberwachung** auf Nein fest.

   Erstellen Sie zwei Dienste. Geben Sie Dummy-IP-Adressen an, die keinem der Geräte gehören, einschließlich der Inline-Geräte. Geben Sie Profil 1 in Dienst 1 und Profil 2 in Dienst 2 an.



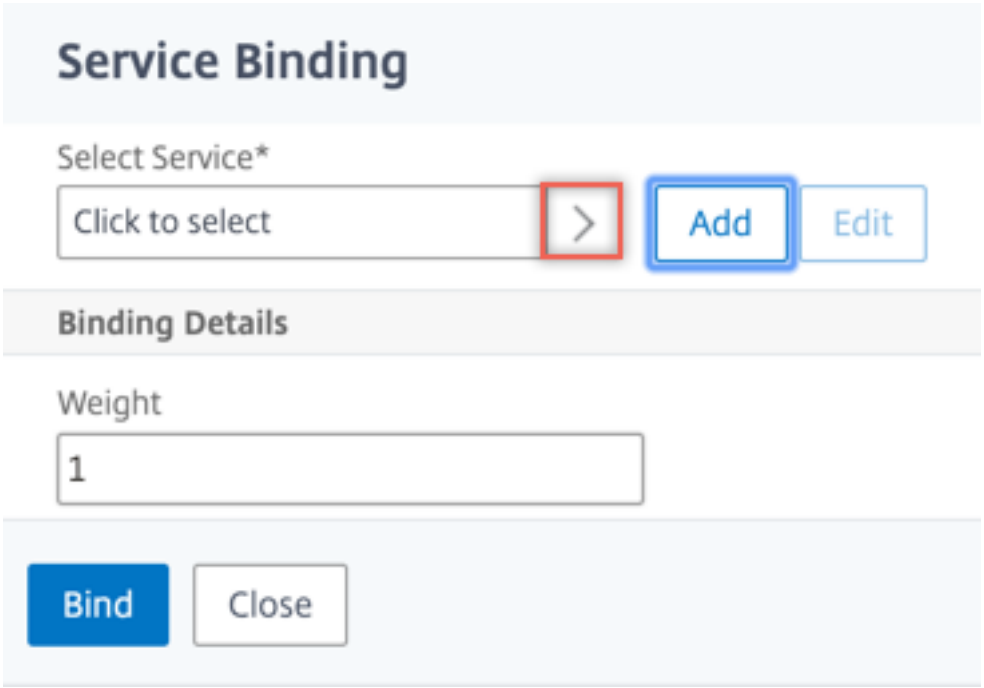


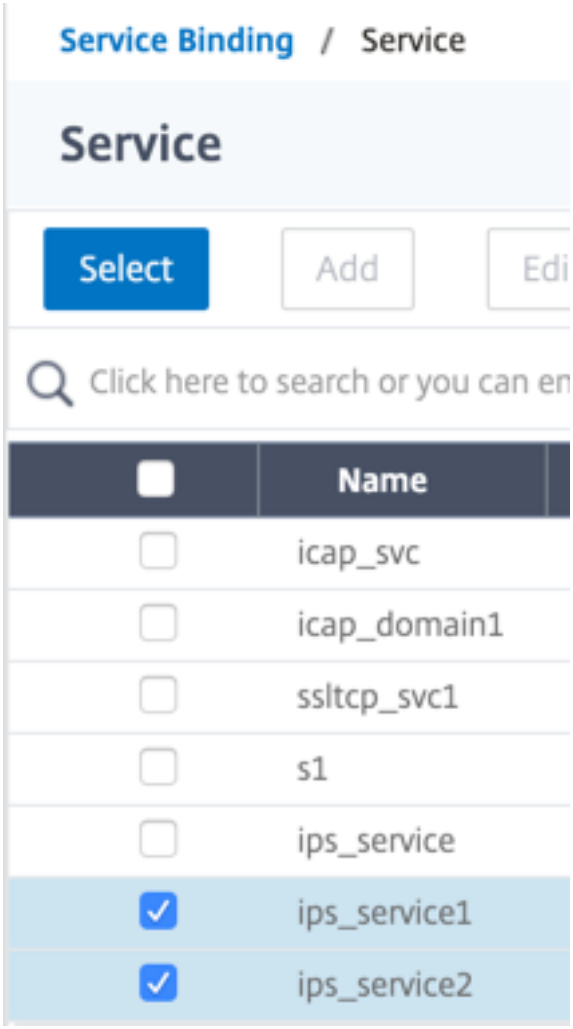
6. Navigieren Sie zu **Lastenausgleich > Virtuelle Server > Hinzufügen**. Erstellen Sie einen virtuellen TCP-Load Balancing Server.

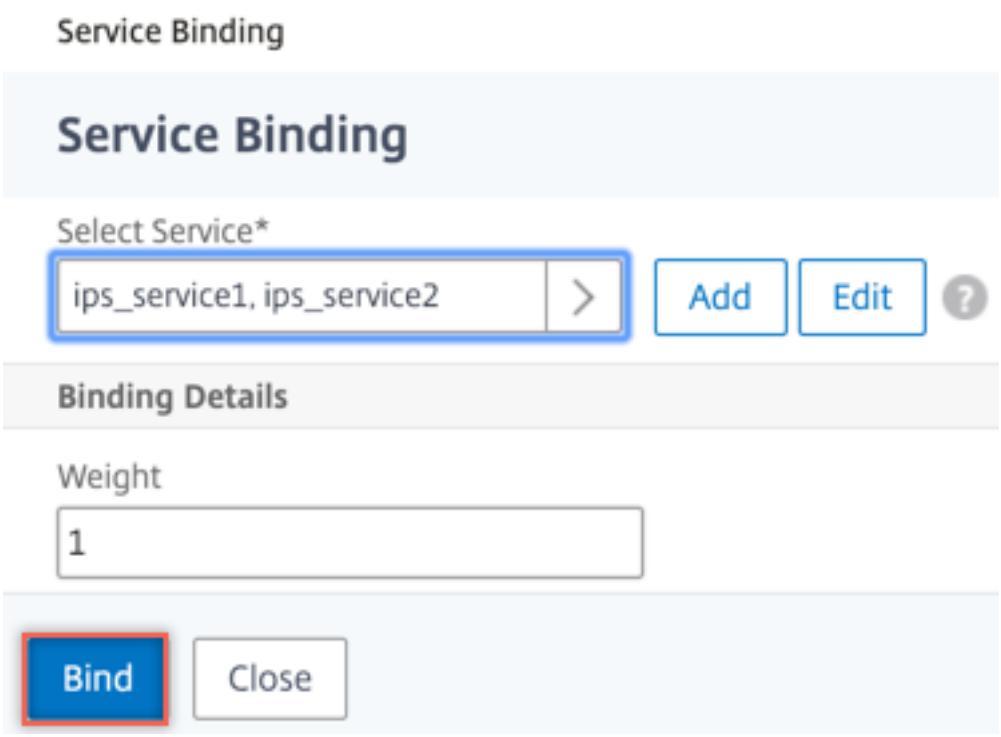


Klicken Sie auf **OK**.

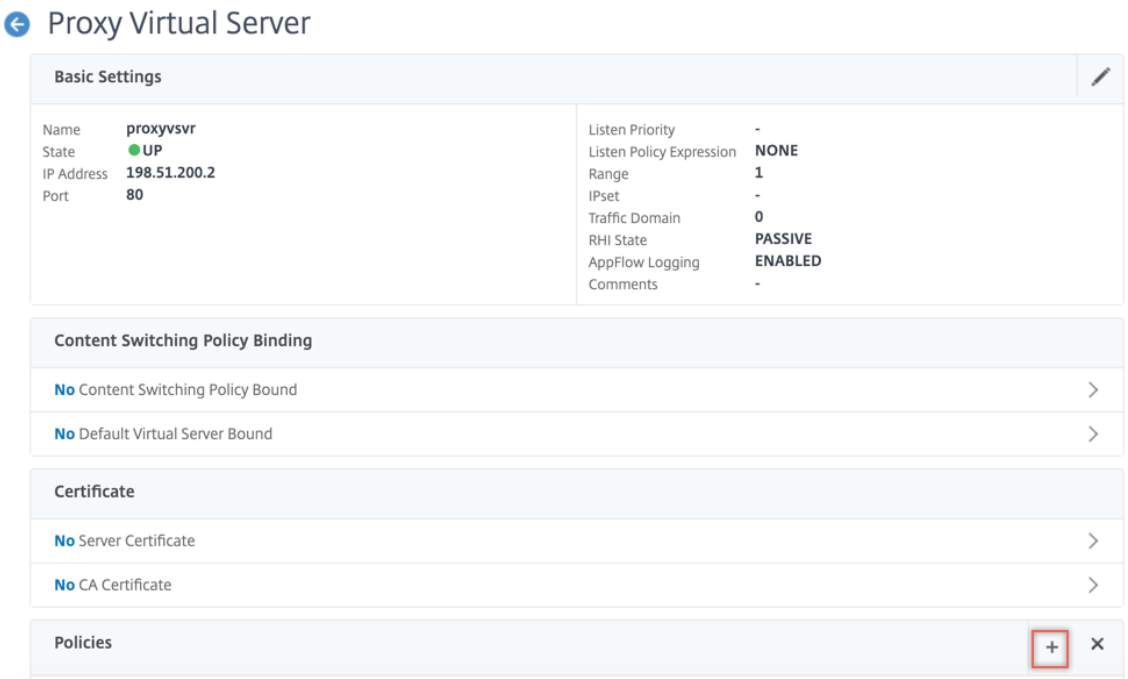
7. Klicken Sie in den Abschnitt **Load Balancing Virtual Server Service Binding**. Klicken Sie unter **Dienstbindung** auf den Pfeil unter **Dienst auswählen**. Wählen Sie die beiden zuvor erstellten Dienste aus, und klicken Sie auf **Auswählen**. Klicken Sie auf **Bind**.



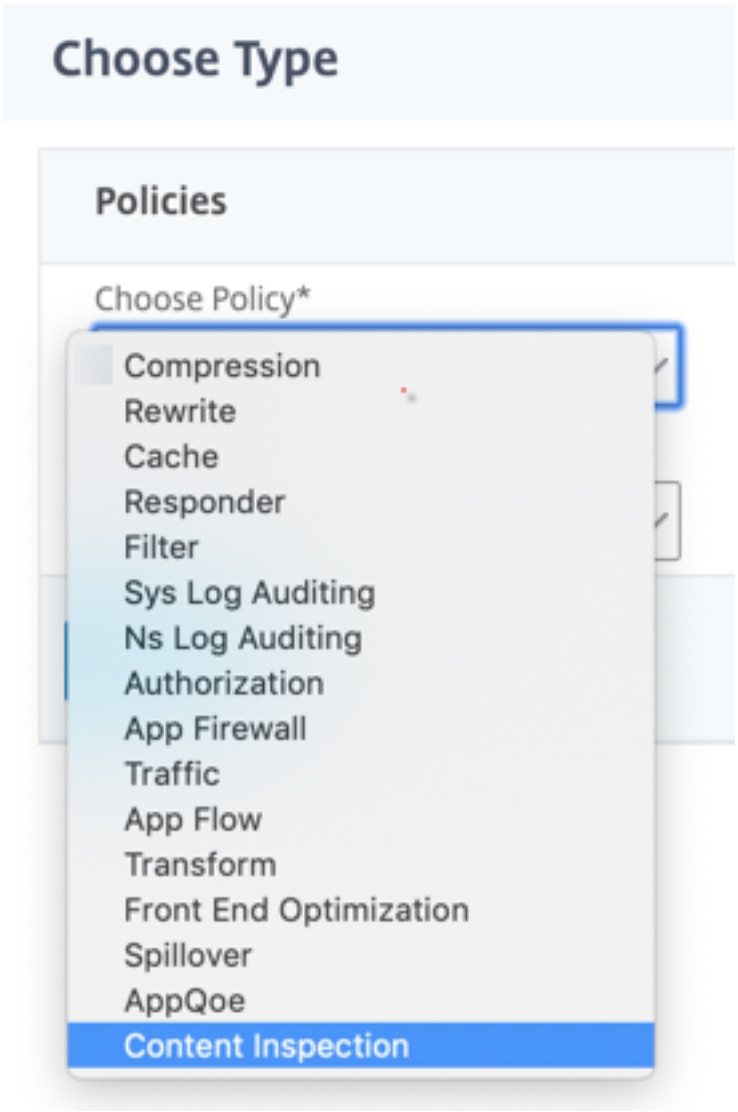




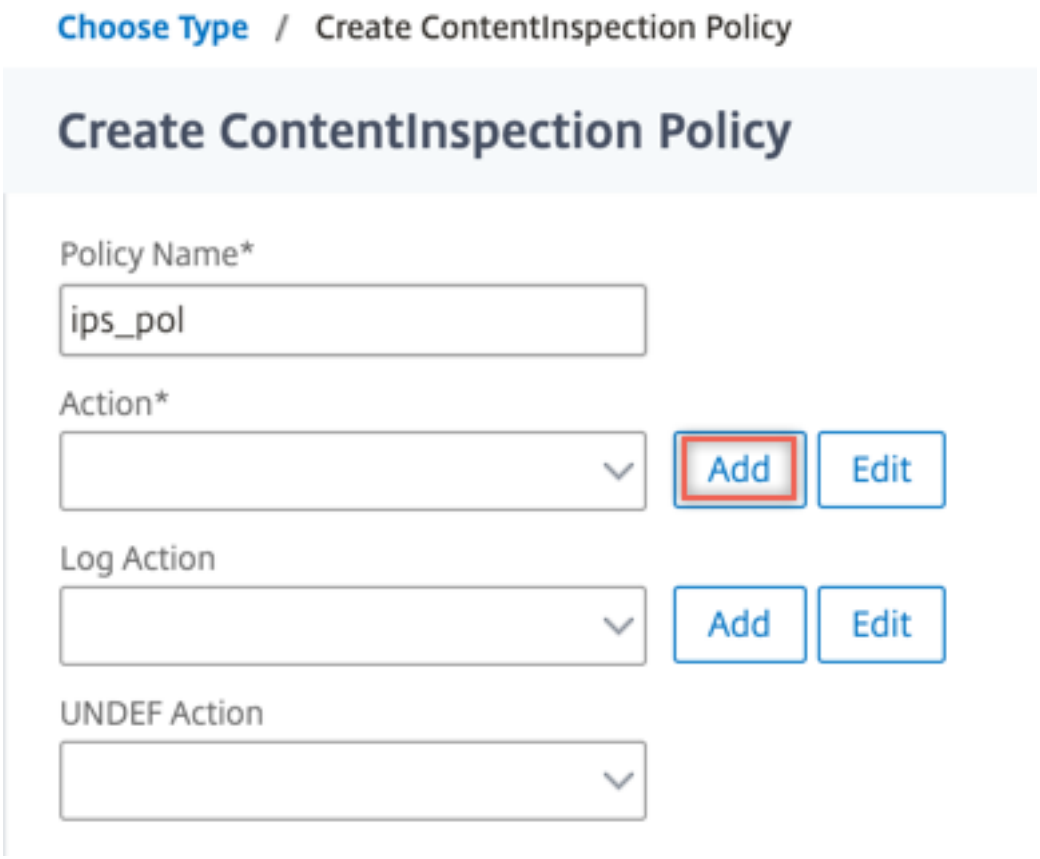
8. Navigieren Sie zu **Secure Web Gateway > Virtuelle Proxyserver > Hinzufügen**. Geben Sie einen Namen, eine IP-Adresse und einen Port an. Wählen Sie unter **Erweiterte Einstellungen** die Option **Richtlinien**aus. Klicken Sie auf das +-Zeichen.



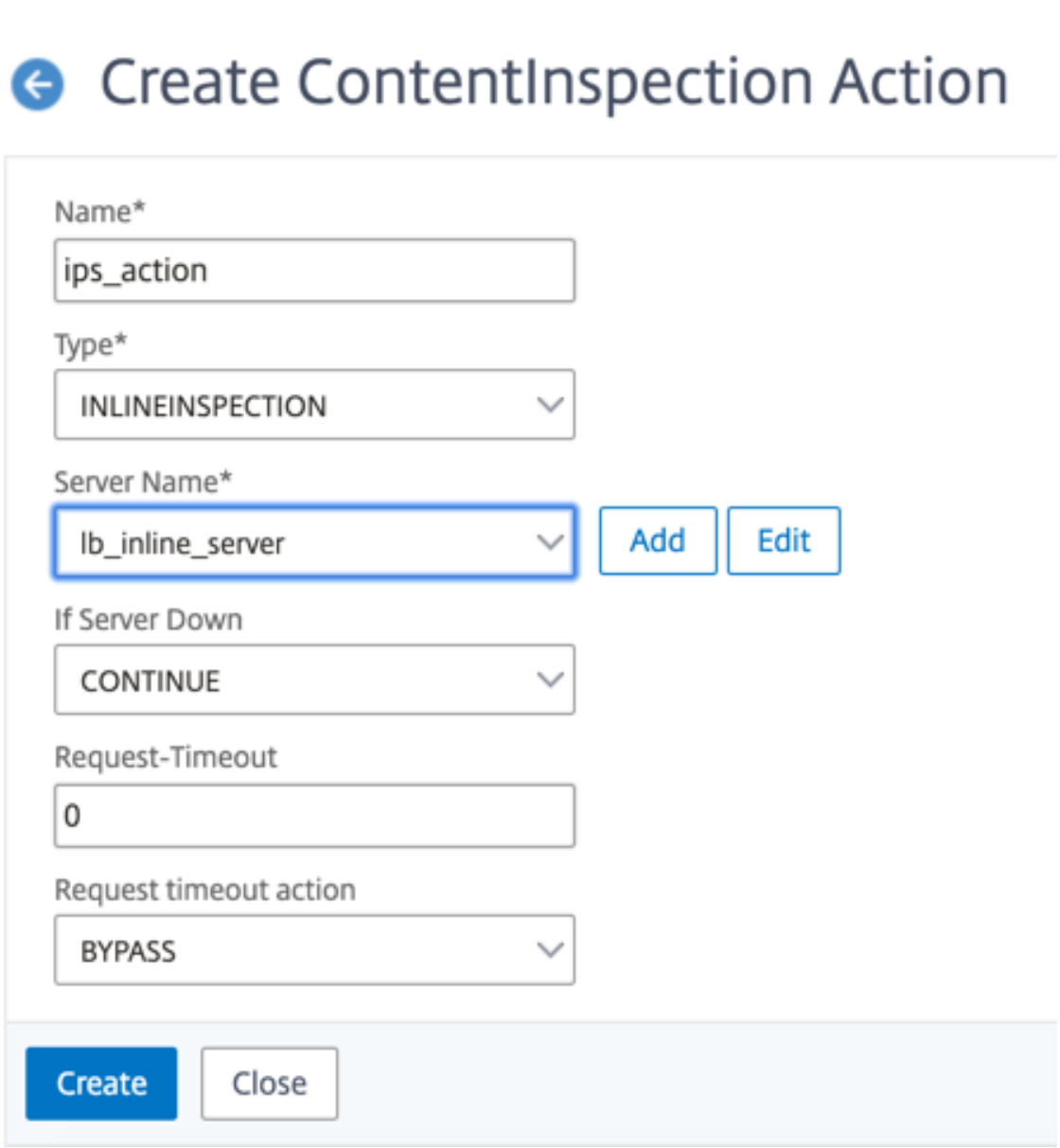
9. Wählen Sie unter **Richtlinie auswählen** die Option **Inhaltsüberprüfung** aus. Klicken Sie auf **Weiter**.



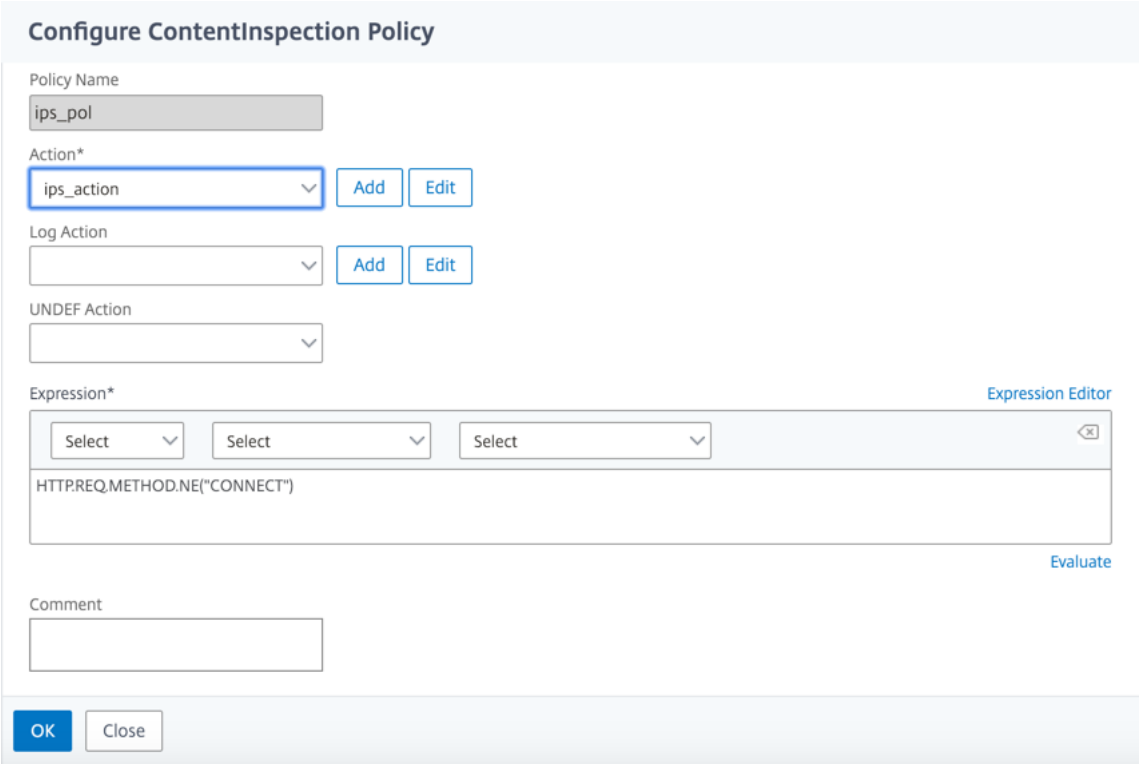
10. Klicken Sie auf **Hinzufügen**. Geben Sie einen Namen an. Klicken Sie unter **Aktion** auf **Hinzufügen**.



11. Geben Sie einen Namen an. Wählen Sie unter **Typ** die Option **INLINEINSPECTION** aus. Wählen Sie unter **Servername** den zuvor erstellten virtuellen Lastenausgleichsserver aus.



12. Klicken Sie auf **Erstellen**. Geben Sie die Regel an, und klicken Sie auf **Erstellen**.



13. Klicken Sie auf **Bind**.
14. Klicken Sie auf **Fertig**.

Analytics

April 26, 2021

In der Citrix SWG-Appliance werden alle Benutzerdatensätze und nachfolgenden Datensätze protokolliert. Wenn Sie Citrix Application Delivery Management (ADM) in die Citrix SWG-Appliance integrieren, werden die protokollierten Benutzeraktivitäten und die nachfolgenden Datensätze in der Appliance mit dem Logstream nach Citrix ADM exportiert.

Citrix ADM stellt Informationen über die Aktivitäten der Nutzer zusammen, z. B. besuchte Websites und die verbrauchte Bandbreite. Außerdem werden Bandbreitennutzung und erkannte Bedrohungen wie Malware und Phishing-Sites gemeldet. Mit diesen Schlüsselmetriken können Sie Ihr Netzwerk überwachen und Korrekturmaßnahmen mit der Citrix SWG-Appliance durchführen. Weitere Informationen finden Sie unter Citrix Secure Web Gateway-Analyse.

So integrieren Sie die Citrix SWG-Appliance in Citrix ADM:

1. Aktivieren Sie in der Citrix SWG-Appliance bei der Konfiguration von Secure Web Gateway Analytics und geben Sie die Details der Citrix ADM-Instanz an, die Sie für Analysen verwenden

möchten.

2. Fügen Sie in Citrix ADM die Citrix SWG-Appliance als Instanz zu Citrix ADM hinzu. Weitere Informationen finden Sie unter Neue Instanzen zu Citrix ADM hinzufügen.

Anwendungsfall: Konformität und Sicherheit des Internetzugangs im Unternehmen

April 26, 2021

Der Direktor der Netzwerksicherheit in einer Finanzorganisation will das Unternehmensnetzwerk vor externen Bedrohungen aus dem Web in Form von Malware schützen. Um dies zu tun, muss der Director Sichtbarkeit gewinnen, um sonst verschlüsselten Datenverkehr umgehen und den Zugriff auf bösartige Websites kontrollieren zu können. Der Direktor ist verpflichtet, Folgendes zu tun:

- Abfangen und Überprüfen des gesamten Datenverkehrs, einschließlich SSL/TLS (verschlüsselter Datenverkehr), der in das Unternehmensnetzwerk eingeht und aus diesem herausgeht.
- Übergehen Sie Interception von Anfragen an Websites, die sensible Informationen enthalten, wie z. B. finanziellen Benutzerinformationen oder E-Mails.
- Blockieren Sie den Zugriff auf schädliche URLs, die als schädliche oder nicht erwachsene Inhalte identifiziert wurden.
- Identifizieren Sie Endbenutzer (Mitarbeiter) im Unternehmen, die auf bösartige Websites zugreifen, und blockieren Sie den Internetzugriff für diese Benutzer oder sperren Sie die schädlichen URLs.

Um all das zu erreichen, kann der Director einen Proxy auf allen Geräten in der Organisation einrichten und ihn auf das Citrix Secure Web Gateway (SWG) verweisen, das als Proxyserver im Netzwerk fungiert. Der Proxyserver fängt den gesamten verschlüsselten und unverschlüsselten Datenverkehr ab, der durch das Unternehmensnetzwerk fließt. Es fordert zur Benutzerauthentifizierung auf und ordnet den Datenverkehr einem Benutzer zu. URL-Kategorien können angegeben werden, um den Zugriff auf illegale/schädliche, adulte, Malware und SPAM-Websites zu blockieren.

Konfigurieren Sie die folgenden Entitäten, um das oben genannte zu erreichen:

- DNS-Namensserver zum Auflösen von Hostnamen.
- Subnet IP (SNIP) -Adresse, um eine Verbindung mit den Ursprungsservern herzustellen. Die SNIP-Adresse sollte Internetzugang haben.
- Proxyserver im expliziten Modus, um den gesamten ausgehenden HTTP- und HTTPS-Datenverkehr abzufangen.
- SSL-Profil zum Definieren von SSL-Einstellungen, wie Verschlüsselungen und Parameter, für Verbindungen.

- Zertifizierungsstellen-Schlüsselpaar, um das Serverzertifikat für SSL-Interception zu signieren.
- SSL-Richtlinie zur Definition der Websites, die abgefangen und umgangen werden sollen.
- Authentifizierung virtueller Server, Richtlinie und Aktion, um sicherzustellen, dass nur gültige Benutzer Zugriff gewährt werden.
- Appflow-Collector zum Senden von Daten an das Citrix Application Delivery Management (ADM).

Für diese Beispielkonfiguration werden sowohl CLI- als auch GUI-Prozeduren aufgelistet. Die folgenden Beispielwerte werden verwendet. Ersetzen Sie sie durch gültige Daten für IP-Adressen, SSL-Zertifikat und Schlüssel sowie LDAP-Parameter.

Name	In der Beispielkonfiguration verwendete Werte
NSIP-Adresse	192.0.2.5
Subnetz-IP-Adresse	198.51.100.5
IP-Adresse des virtuellen LDAP-Servers	192.0.2.116
IP-Adresse des DNS-Nameservers	203.0.113.2
IP-Adresse des Proxyservers	192.0.2.100
MAS-IP-Adresse	192.0.2.41
Zertifizierungsstellenzertifikat für SSL-Interception	ns-swg-ca-certkey (Zertifikat: ns_swg_ca.crt und Schlüssel: ns_swg_ca.key)
LDAP-Basis-DN	CN = Benutzer, DC = CTXNSSFB, DC = COM
LDAP-Bindung DN	CN = Administrator, CN = Benutzer, DC = CTXNSSFB, DC = COM
LDAP-Bind-DN-Kennwort	zzzzz

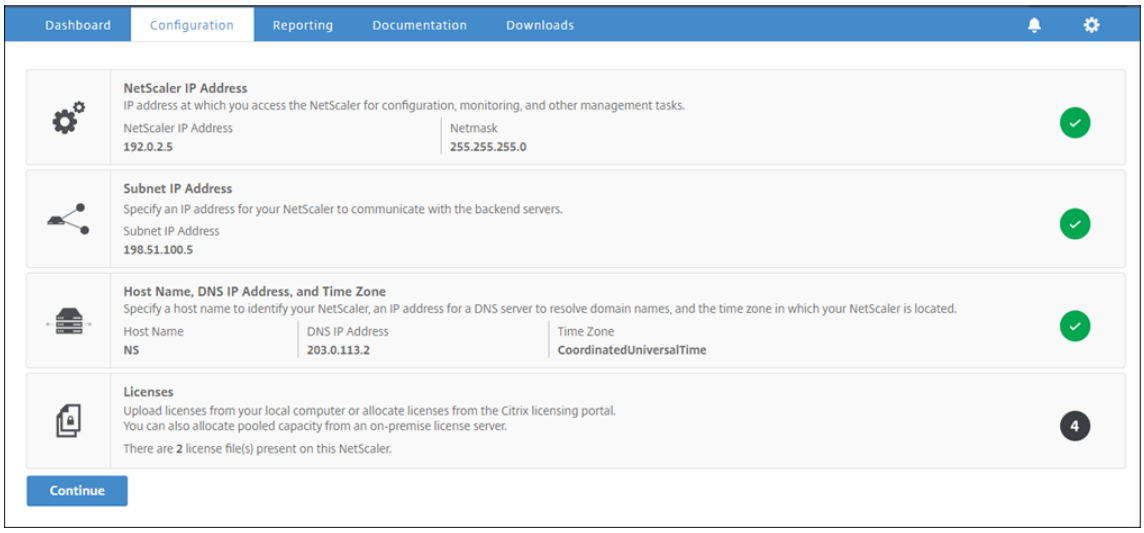
Konfigurieren von Interception und Überprüfung des Datenverkehrs zum und vom Unternehmensnetzwerk mit dem Secure Web Gateway-Assistenten

Das Erstellen einer Konfiguration für Interception und Überprüfungg von verschlüsseltem Datenverkehr zusätzlich zu dem anderen Datenverkehr zu und von einem Netzwerk erfordert die Konfiguration von Proxyeinstellungen, SSLi-Einstellungen, Benutzerauthentifizierungseinstellungen und URL-Filtereinstellungen. Die folgenden Verfahren enthalten Beispiele für die eingegebenen Werte.

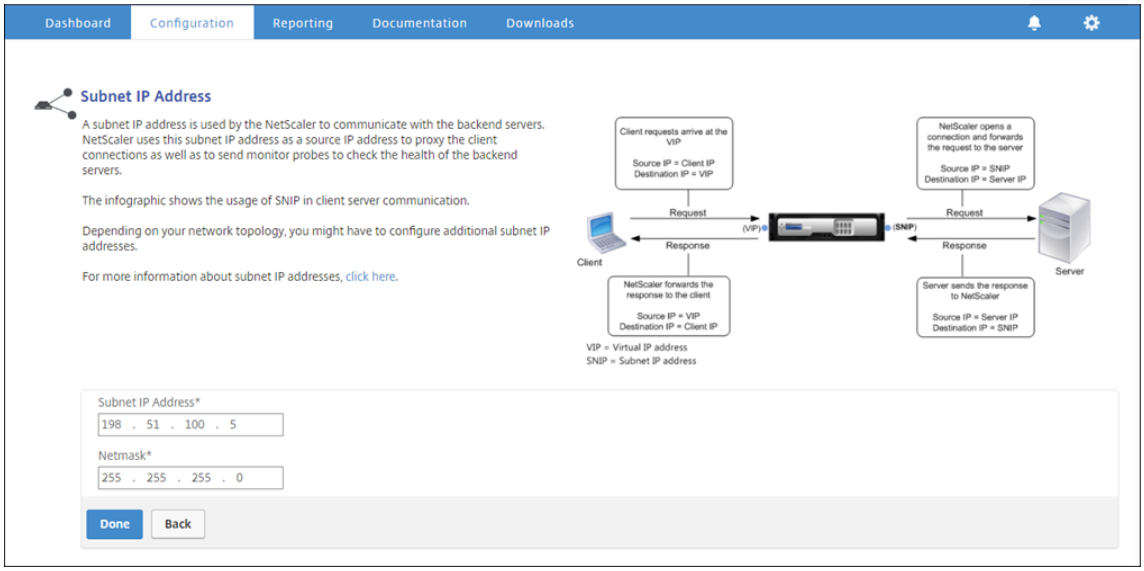
Konfigurieren der SNIP-Adresse und des DNS-Namensservers

1. Geben Sie in einem Webbrowser die NSIP-Adresse ein. Beispiel: `http://192.0.2.5`.

2. Geben Sie im Feld **User Name** und **Password** die Administratoranmeldeinformationen ein. Der folgende Bildschirm wird angezeigt.

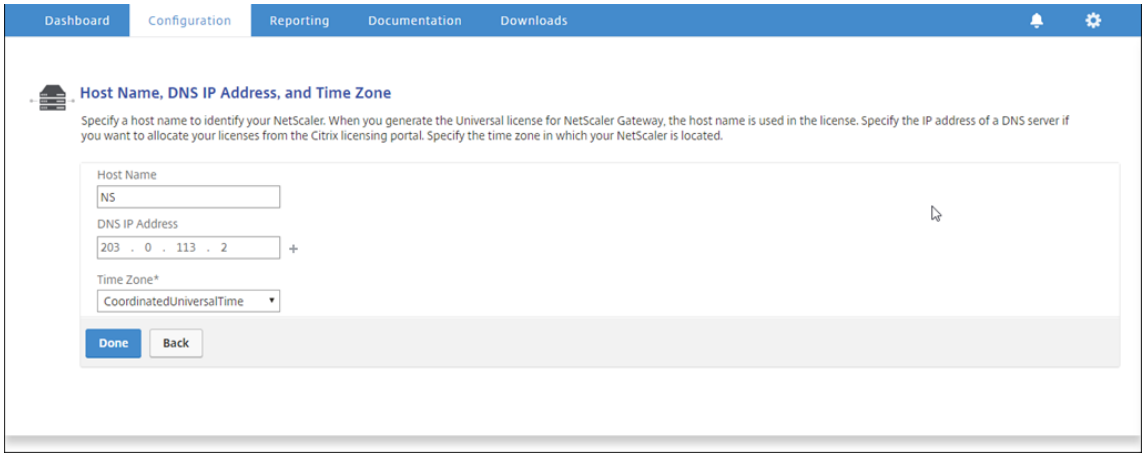


3. Klicken Sie in den Abschnitt **Subnetz-IP-Adresse**, und geben Sie eine IP-Adresse ein.



4. Klicken Sie auf **Fertig**.

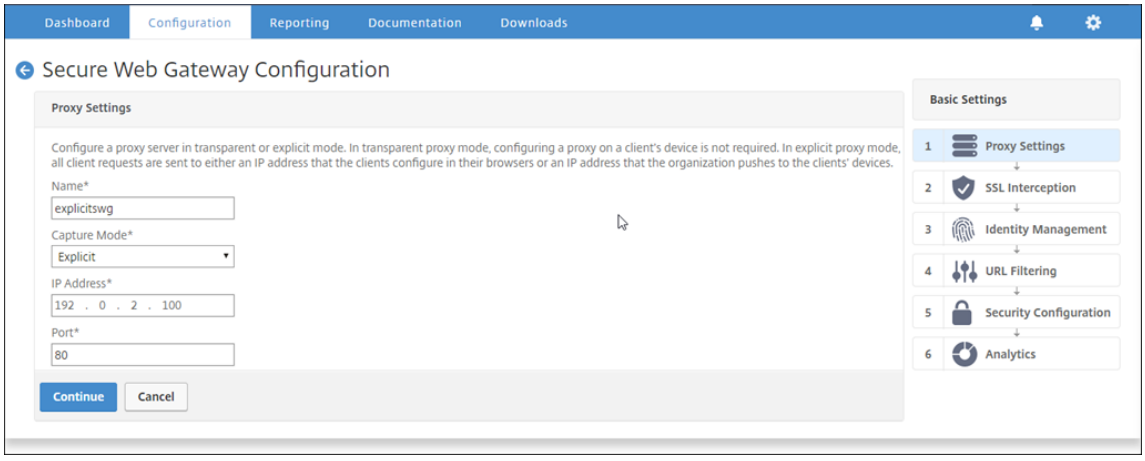
5. Klicken Sie in den Abschnitt **Hostname, DNS-IP-Adresse und Zeitzone**, und geben Sie Werte für diese Felder ein.



6. Klicken Sie auf **Fertig**, und klicken Sie dann auf **Weiter**.

Konfigurieren der Proxy-Einstellungen

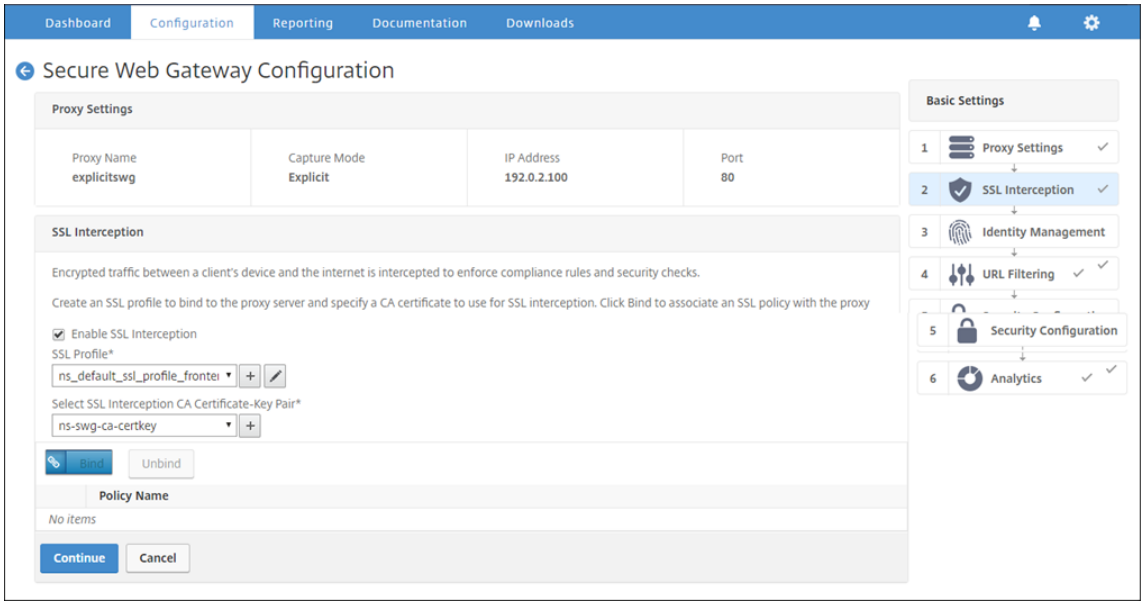
1. Navigieren Sie zu **Secure Web Gateway** > **Secure Web Gateway-Assistent**.
2. Klicken Sie auf **Erste Schritte** und dann auf **Weiter**.
3. Geben Sie im Dialogfeld **Proxyeinstellungen** einen Namen für den expliziten Proxyserver ein.
4. Wählen Sie für **den AufnahmemodusExplizit**aus
5. Geben Sie eine IP-Adresse und Portnummer ein.



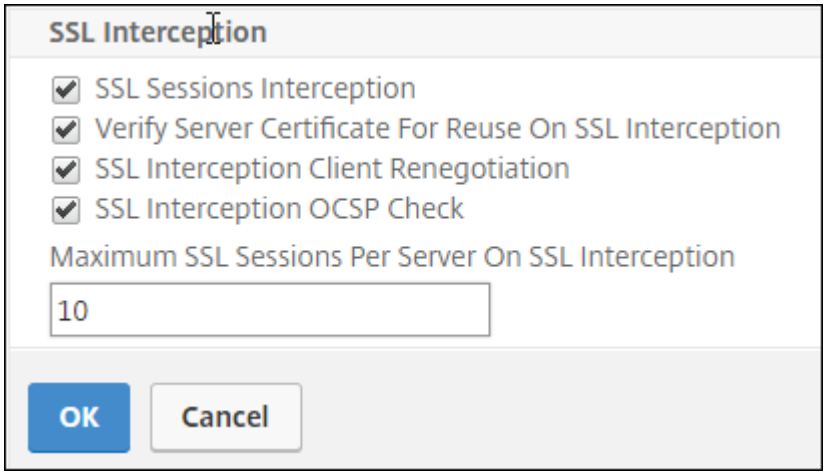
6. Klicken Sie auf **Weiter**.

Konfigurieren der Einstellungen für SSL-Interception

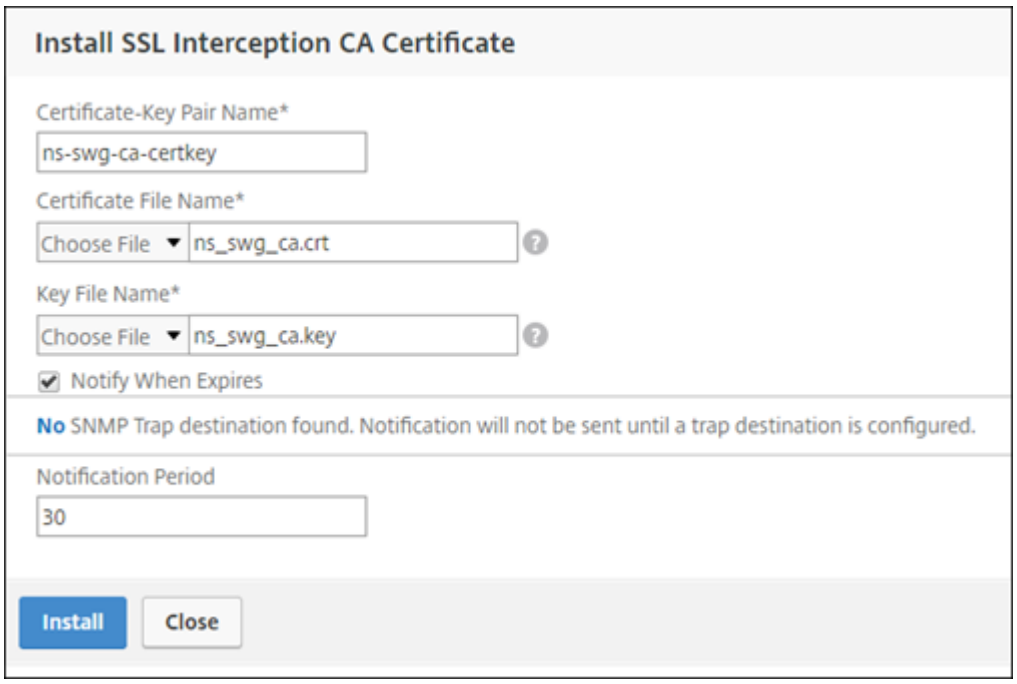
1. Wählen Sie **SSL-Interception aktivieren** aus.



2. Klicken Sie im **SSL-Profil** auf "+", um ein neues Front-End-SSL-Profil hinzuzufügen und **SSL-Sitzungsinterception** in diesem Profil zu aktivieren.

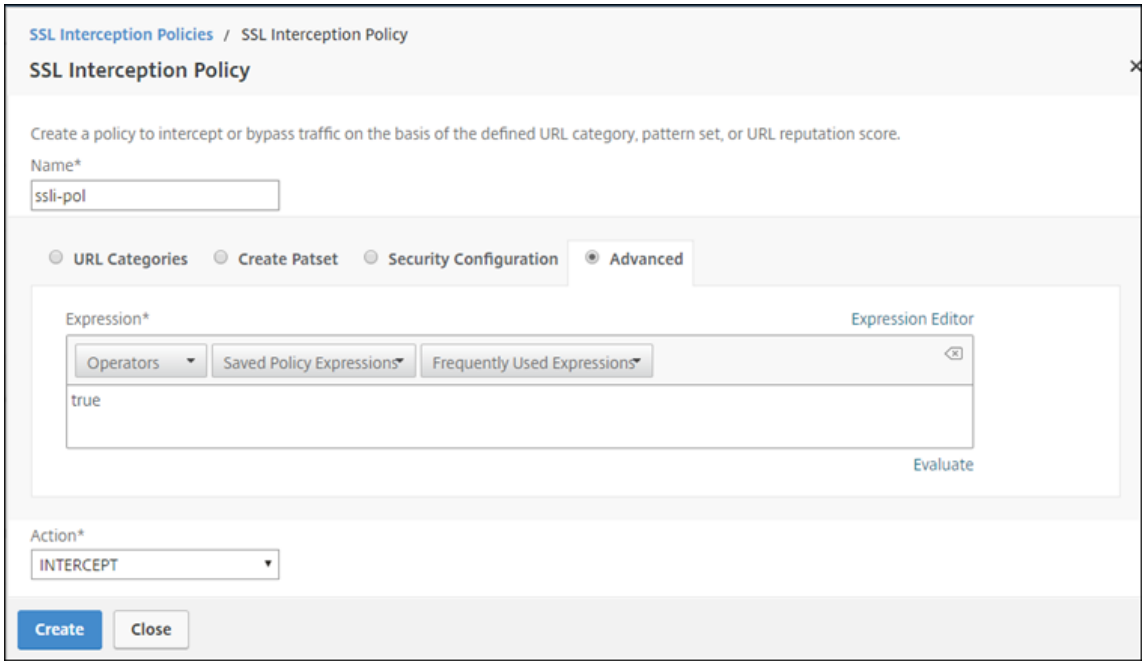


3. Klicken Sie auf **OK** und dann auf **Fertig**.
4. Klicken **Sie in Select SSL Interception CA Certificate-Key Pair**auf „+", um ein CA-Zertifikatschlüsselpaar für das SSL-Abfangen zu installieren.

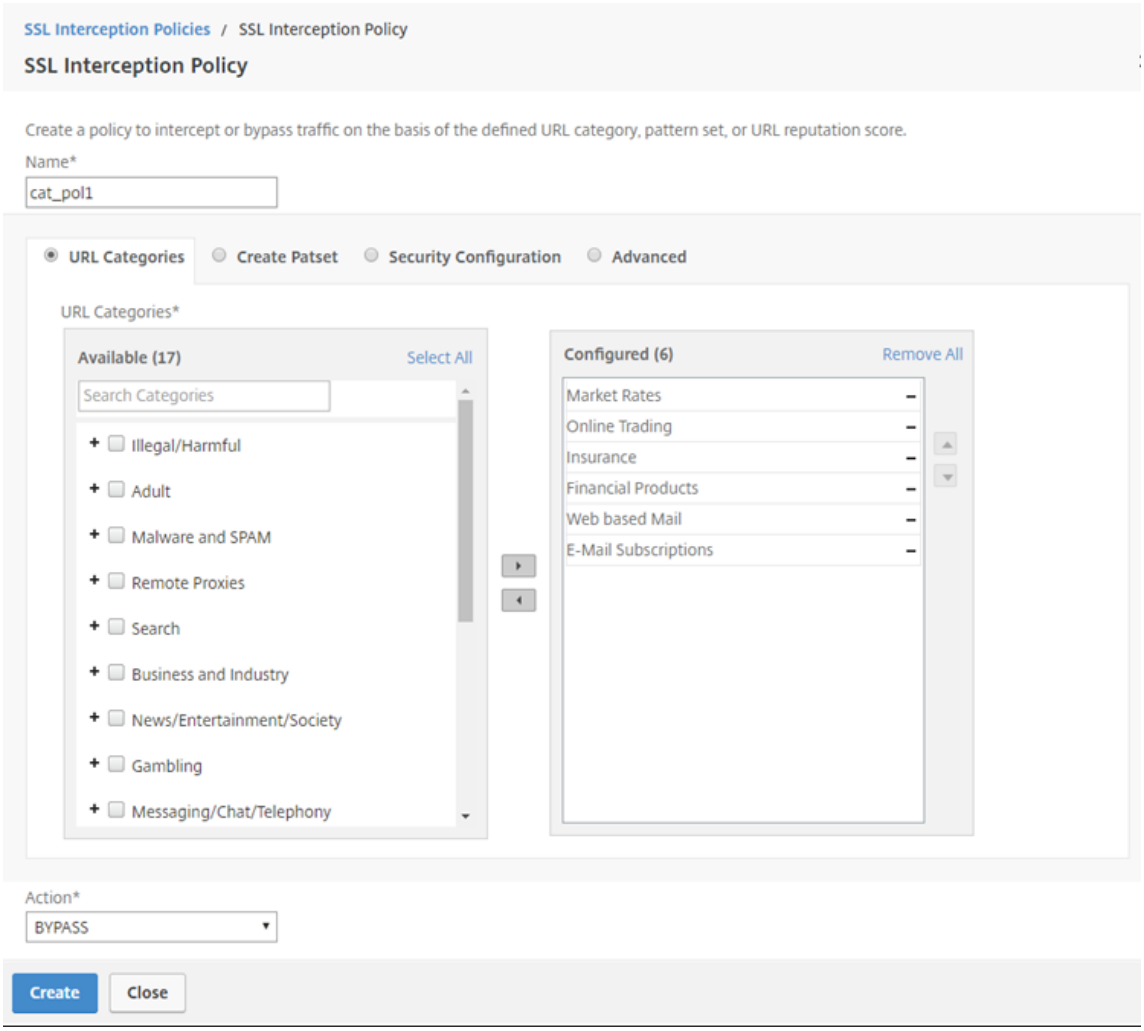


5. Klicken Sie auf **Installieren** und dann auf **Schließen**.
6. Fügen Sie eine Richtlinie hinzu, um den gesamten Datenverkehr abzufangen. Klicken Sie auf **Binden** und dann auf **Hinzufügen** .

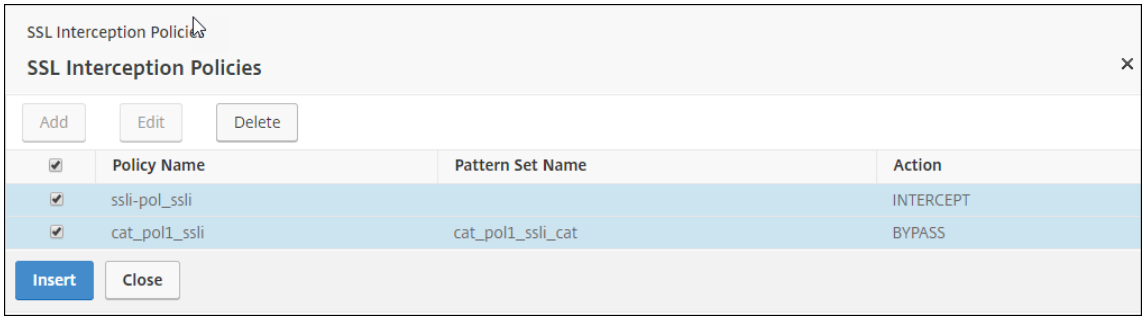
7. Geben Sie einen Namen für die Richtlinie ein, und wählen Sie **Erweitert** aus. Geben Sie im Ausdrucksеditor true ein.
8. Wählen Sie unter **Aktion** die Option **INTERCEPT** aus.



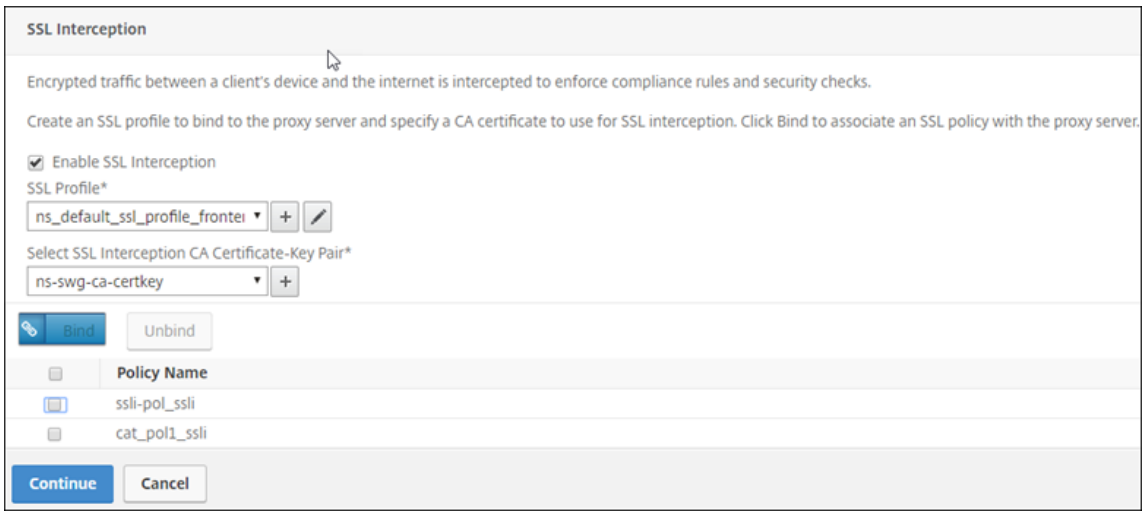
9. Klicken Sie auf **Erstellen** und dann auf **Hinzufügen**, um eine weitere Richtlinie hinzuzufügen, um vertrauliche Informationen zu umgehen.
10. Geben Sie einen Namen für die Richtlinie ein, und klicken Sie unter **URL-Kategorien** auf **Hinzufügen**.
11. Wählen Sie die Kategorien **Finanzen** und **E-Mail** aus, und verschieben Sie sie in die Liste **Konfiguriert**.
12. Wählen Sie unter **Aktion** die Option **BYPASS** aus.



13. Klicken Sie auf **Erstellen**.
14. Wählen Sie die beiden zuvor erstellten Richtlinien aus, und klicken Sie auf **Einfügen**.

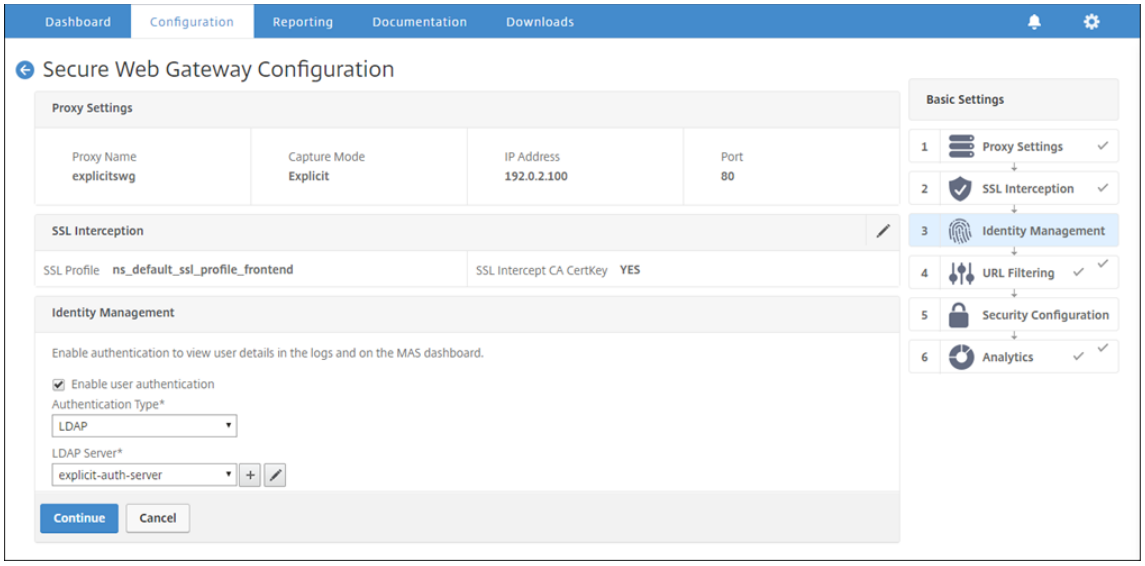


15. Klicken Sie auf **Weiter**.

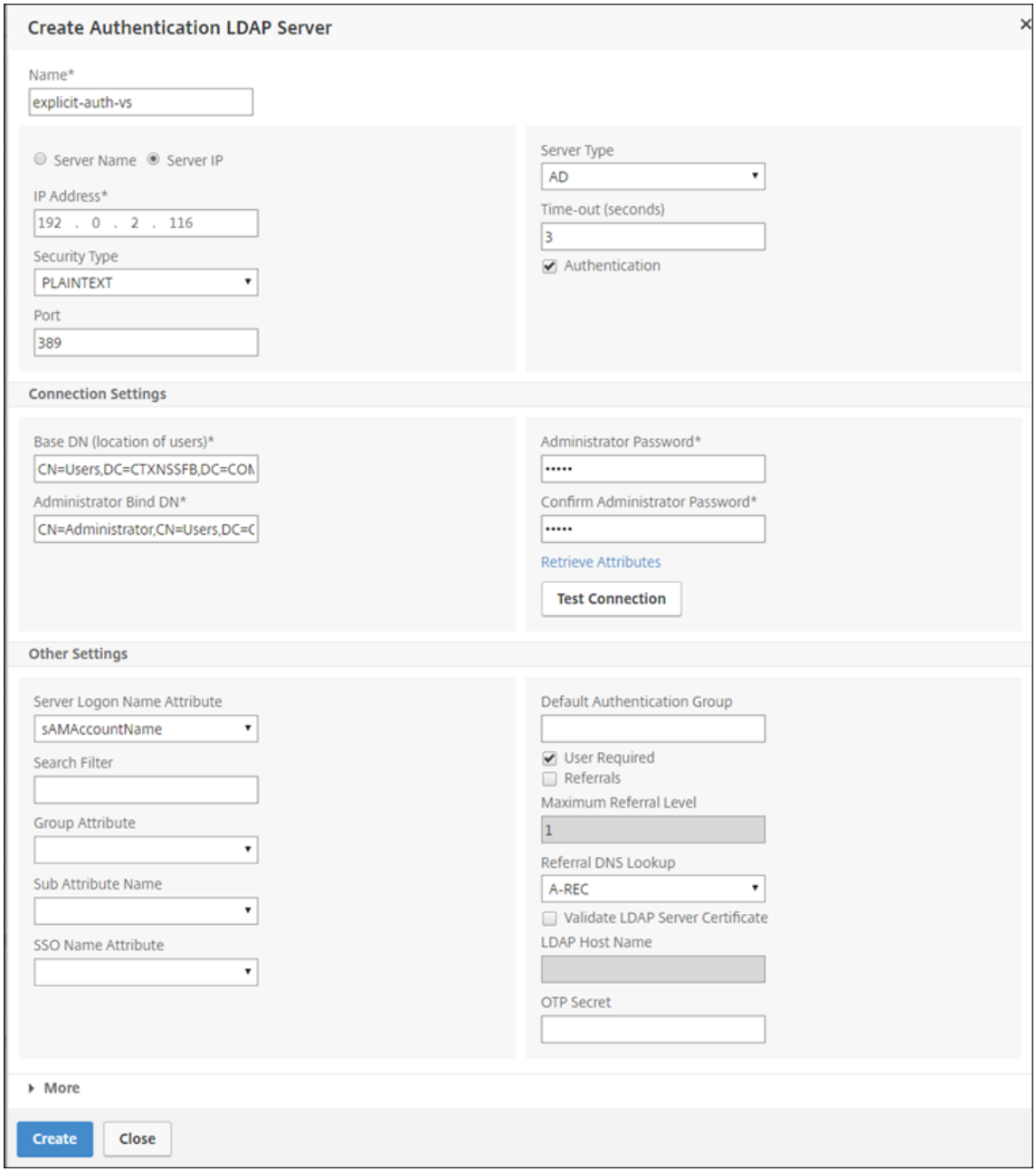


Konfigurieren der Benutzerauthentifizierungseinstellungen

1. Wählen Sie **Benutzerauthentifizierung aktivieren**aus. Wählen Sie im Feld **Authentifizierungstyp** die Option **LDAP** aus.



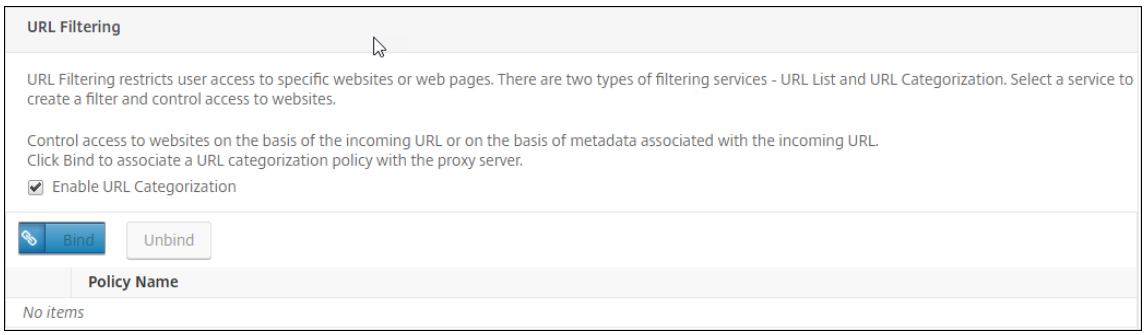
2. Fügen Sie LDAP-Serverdetails hinzu.



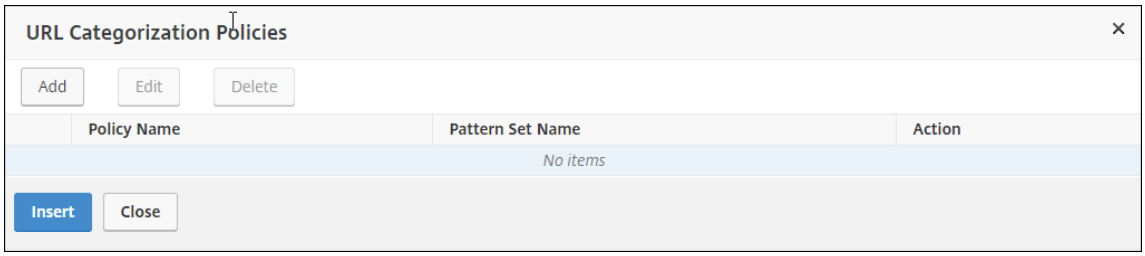
3. Klicken Sie auf **Erstellen**.
4. Klicken Sie auf **Weiter**.

Einstellungen für die URL-Filterung konfigurieren

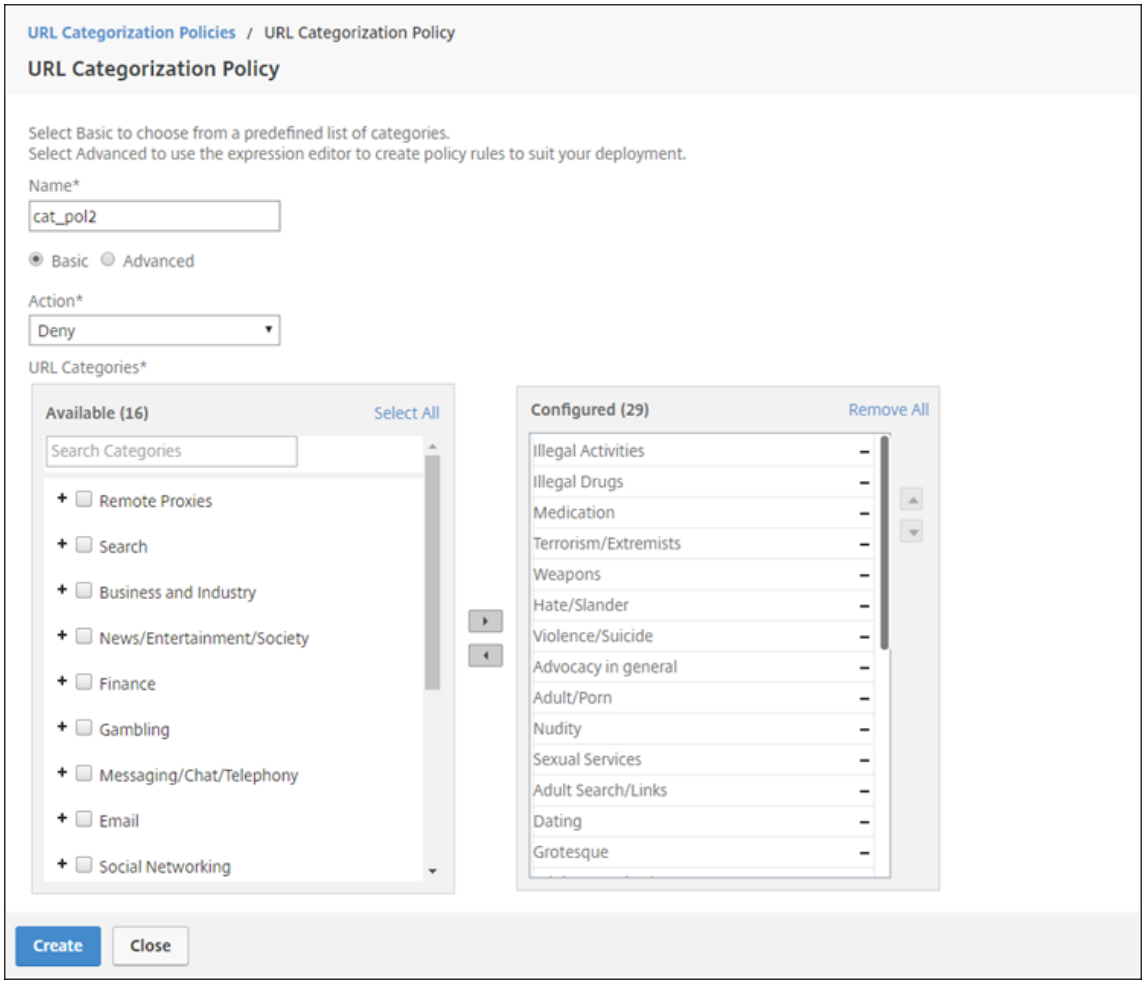
1. Wählen Sie **URL-Kategorisierung aktivieren aus,** und klicken Sie dann auf **Binden** .



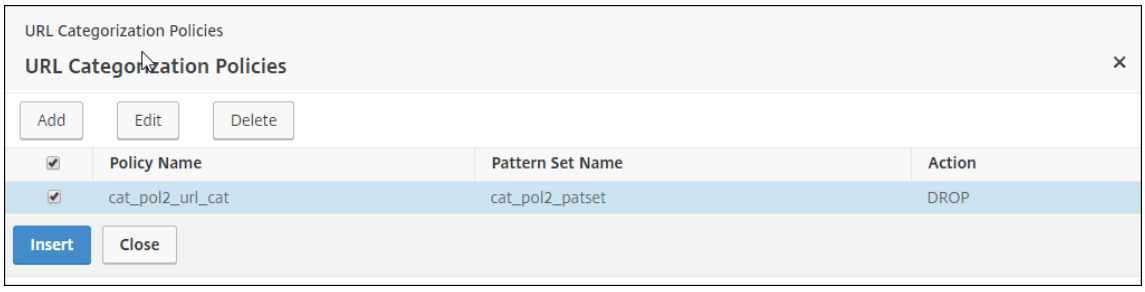
2. Klicken Sie auf **Hinzufügen**.



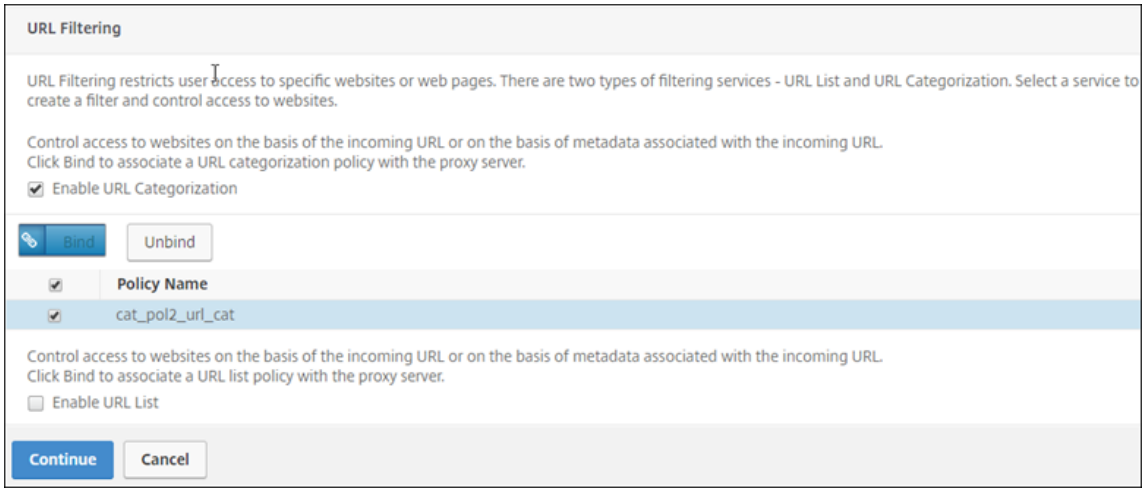
3. Geben Sie einen Namen für die Richtlinie ein. Wählen Sie **unter Aktion**die Option **Verweigern**aus. Wählen Sie **unter URL-Kategorien**die Option **Illegal/Schädlich**, **Erwachsene**sowie **Malware und SPAM**aus und verschieben Sie sie in die Liste **Konfiguriert**.



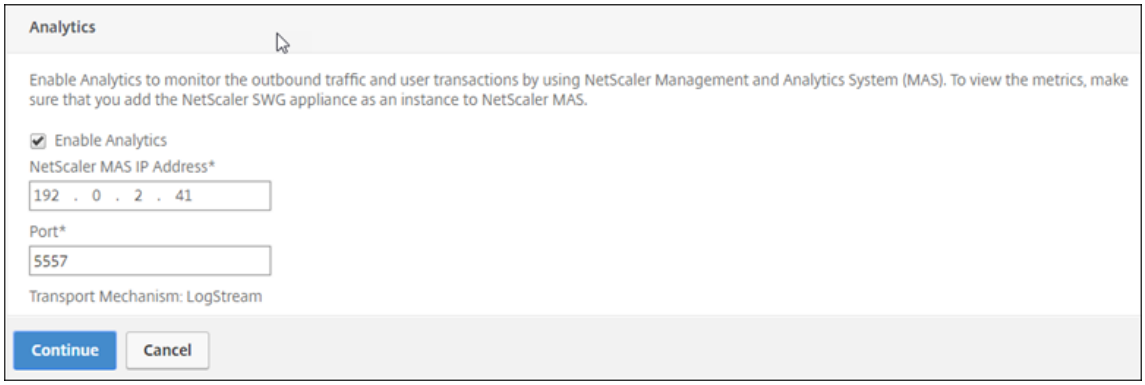
4. Klicken Sie auf **Erstellen**.
5. Wählen Sie die Richtlinie aus, und klicken Sie dann auf **Einfügen**.



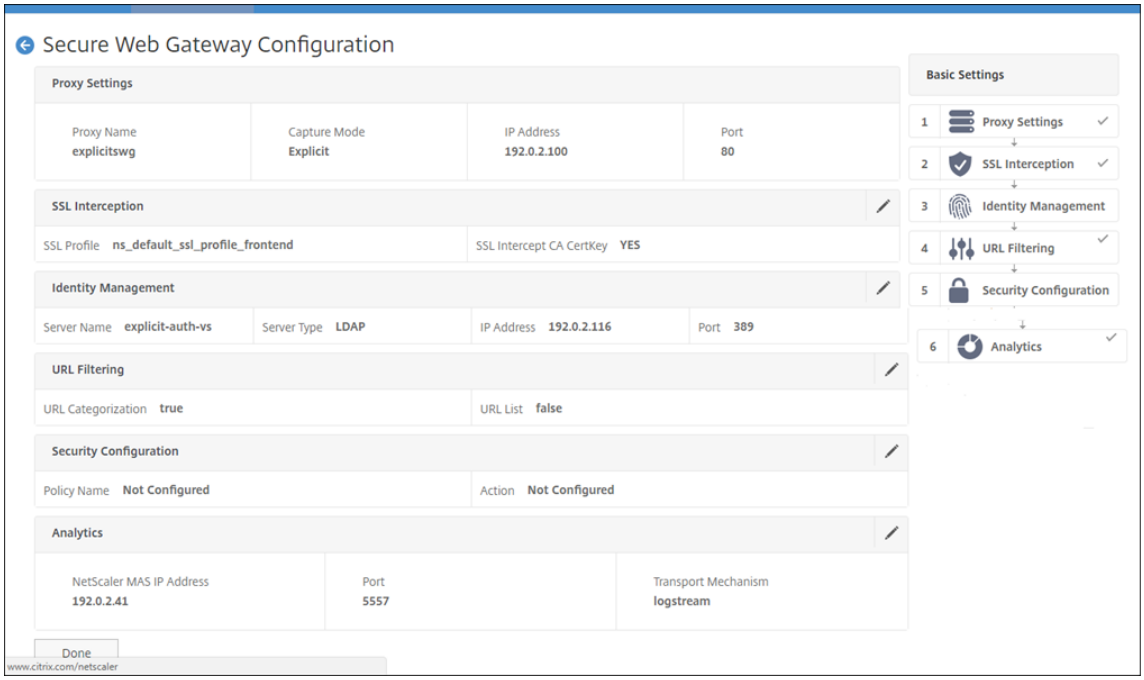
6. Klicken Sie auf **Weiter**.



7. Klicken Sie auf **Weiter**.
8. Klicken Sie auf **Analytics aktivieren**.
9. Geben Sie die IP-Adresse von Citrix ADM ein, und geben Sie für **Port**5557 an.



10. Klicken Sie auf **Weiter**.
11. Klicken Sie auf **Fertig**.



Verwenden Sie Citrix ADM, um Schlüsselmetriken für Benutzer anzuzeigen und Folgendes zu bestimmen:

- Surfverhalten der Benutzer in Ihrem Unternehmen.
- URL-Kategorien, auf die die Benutzer in Ihrem Unternehmen zugreifen.
- Browser, die für den Zugriff auf die URLs oder Domänen verwendet werden.

Verwenden Sie diese Informationen, um festzustellen, ob das System des Benutzers mit Malware infiziert ist, oder verstehen Sie das Bandbreitenverbrauchsmuster des Benutzers. Sie können die Richtlinien auf Ihrer Citrix SWG-Appliance optimieren, um diese Benutzer einzuschränken oder weitere Websites zu blockieren. Weitere Informationen zum Anzeigen der Metriken auf MAS finden Sie im Anwendungsfall “Inspecting Endpoints”in MAS Anwendungsfälle.

> **Hinweis**
>
> Legen Sie die folgenden Parameter mit der CLI fest.

```
set syslogparams -sslInterception ENABLED

set cacheparameter -memLimit 100

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


CLI-Beispiel

Das folgende Beispiel enthält alle Befehle, die zum Konfigurieren von Interception und der Überprüfung des Datenverkehrs zum und vom Unternehmensnetzwerk verwendet werden.

Allgemeine Konfiguration:

```
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-->
```

Authentifizierungskonfiguration:

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

Proxyserver- und SSL-Interceptionkonfiguration:

```
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-->
```

Konfiguration der URL-Kategorien:

```
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-Konfiguration zum Abrufen von Daten in 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-->
```


Anwendungsfall: Sicherung des Unternehmensnetzwerks durch Verwendung von ICAP für die Remote-Malware-Inspektion

April 26, 2021

Die Citrix Secure Web Gateway (SWG) -Appliance fungiert als Proxy und fängt den gesamten Client-Datenverkehr ab. Die Appliance verwendet Richtlinien, um den Datenverkehr auszuwerten und leitet Clientanforderungen an den Ursprungsserver weiter, auf dem sich die Ressource befindet. Die Appliance entschlüsselt die Antwort vom Ursprungsserver und leitet den Nur-Text-Inhalt für eine Antischadwareprüfung an den ICAP-Server weiter. Der ICAP-Server antwortet mit der Meldung "Keine Anpassung erforderlich", Fehler oder geänderte Anforderung. Abhängig von der Antwort des ICAP-Servers wird der angeforderte Inhalt entweder an den Client weitergeleitet oder eine entsprechende Nachricht gesendet.

Für diesen Anwendungsfall müssen Sie eine allgemeine Konfiguration, Proxy- und SSL-Interceptionkonfiguration sowie eine ICAP-Konfiguration auf der Citrix SWG-Appliance durchführen.

Allgemeine Konfiguration

Konfigurieren Sie die folgenden Entitäten:

- NSIP-Adresse
- Subnetz-IP-Adresse (SNIP)
- DNS-Namensserver
- Zertifizierungsstellenschlüsselpaar zum Signieren des Serverzertifikats für SSL-Interception

Proxyserver- und SSL-Interceptionkonfiguration

Konfigurieren Sie die folgenden Entitäten:

- Proxyserver im expliziten Modus, um den gesamten ausgehenden HTTP- und HTTPS-Datenverkehr abzufangen.
- SSL-Profil zum Definieren von SSL-Einstellungen, wie Verschlüsselungen und Parameter, für Verbindungen.
- SSL-Richtlinie zum Definieren von Regeln zum Abfangen von Datenverkehr. Auf true gesetzt, um alle Clientanforderungen abzufangen.

Weitere Informationen finden Sie in den folgenden Artikeln:

- Proxy-Modi
- SSL-Interception

In der folgenden Beispielkonfiguration befindet sich der Antischadsoftware-Erkennungsdienst unter www.example.com.

Allgemeine Beispielkonfiguration:

```
add ns ip 192.0.2.5 255.255.255.0

add ns ip 198.51.100.5 255.255.255.0 -type SNIP

add dns nameServer 203.0.113.2

add ssl certKey ns-swg-ca-certkey -cert ns_swg_ca.crt -key ns_swg_ca.
    key
<!--NeedCopy-->
```

Beispiel-Proxyserver und SSL-Interceptionkonfiguration:

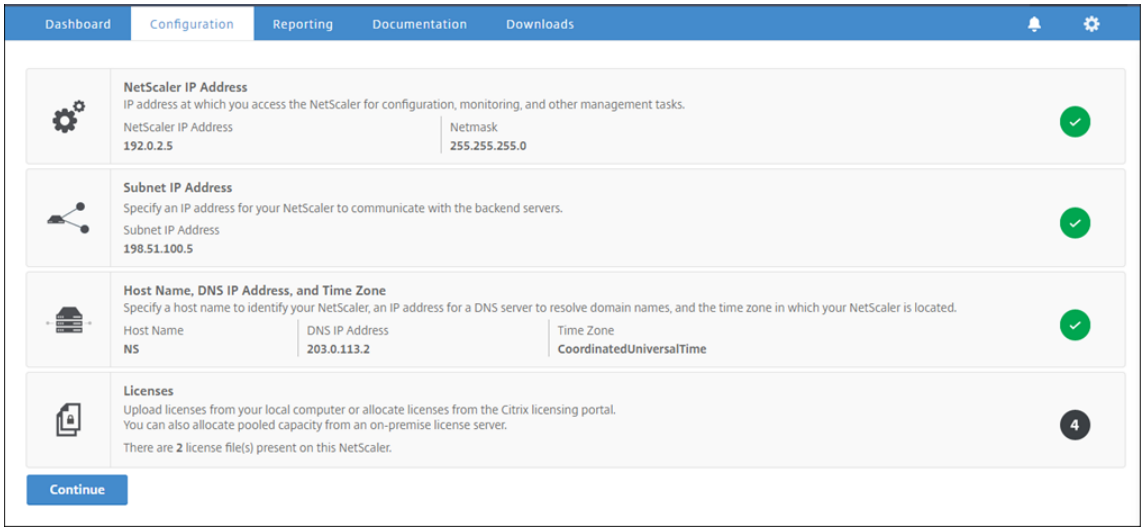
```
add cs vserver explicitswg PROXY 192.0.2.100 80 –Authn401 ENABLED –
    authnVsName explicit-auth-vs

set ssl parameter -defaultProfile ENABLED

add ssl profile swg_profile -sslInterception ENABLED

bind ssl profile swg_profile -ssliCACertkey ns-swg-ca-certkey

set ssl vserver explicitswg -sslProfile swg_profile

add ssl policy ssli-pol_ssli -rule true -action INTERCEPT

bind ssl vserver explicitswg -policyName ssli-pol_ssli -priority 100 -
    type INTERCEPT_REQ
<!--NeedCopy-->
```

Beispiel-ICAP-Konfiguration:

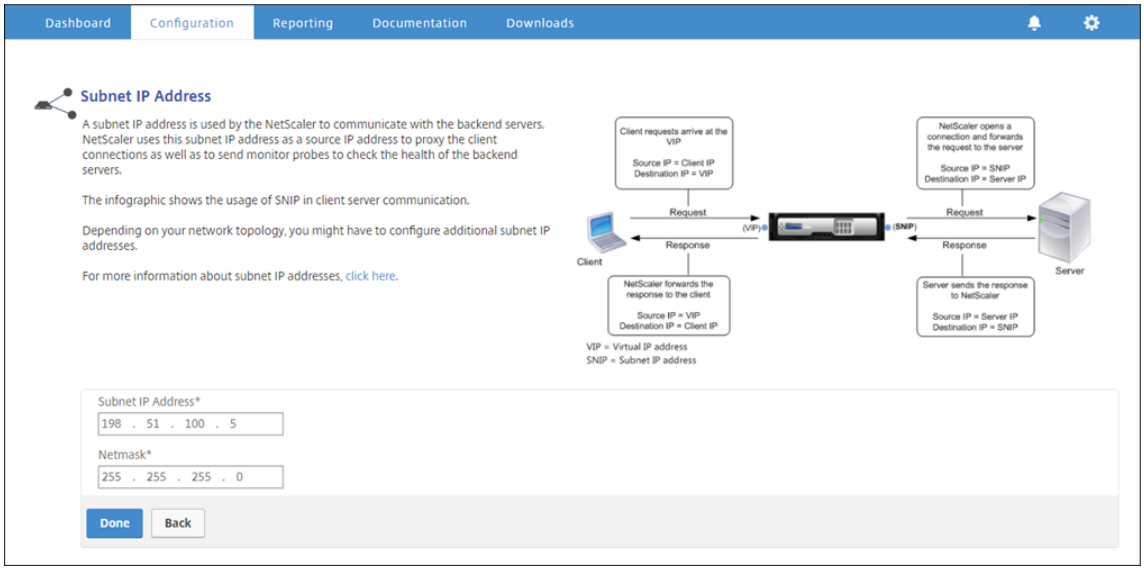
```
add service icap_svc 203.0.113.225 TCP 1344

enable ns feature contentinspection

add icapprofile icapprofile1 -uri /example.com -Mode RESMOD

add contentInspection action CiRemoteAction -type ICAP -serverName
    icap_svc -icapProfileName icapprofile1

add contentInspection policy CiPolicy -rule "HTTP.REQ.METHOD.NE("
    CONNECT")" -action CiRemoteAction

bind cs vserver explicitswg -policyName  CiPolicy -priority 200 -type
    response
<!--NeedCopy-->
```


Konfigurieren der SNIP-Adresse und des DNS-Namensservers

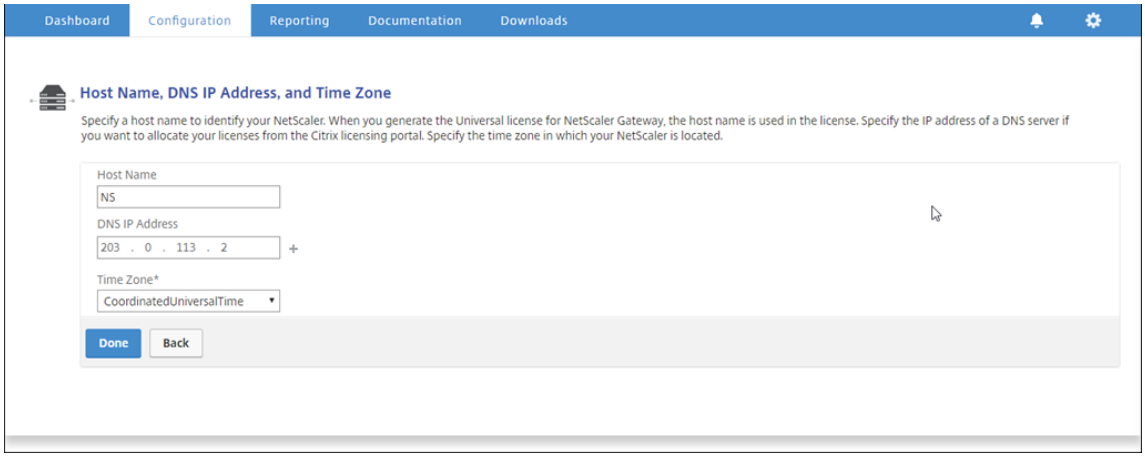
1. Geben Sie in einem Webbrowser die NSIP-Adresse ein. Beispiel: `http://192.0.2.5`.
2. Geben Sie im Feld **User Name** und **Password** die Administratoranmeldeinformationen ein. Der folgende Bildschirm wird angezeigt. Wenn der folgende Bildschirm nicht angezeigt wird, fahren Sie mit dem Abschnitt Proxy-Einstellungen fort.



3. Klicken Sie in den Abschnitt **Subnetz-IP-Adresse**, und geben Sie eine IP-Adresse ein.



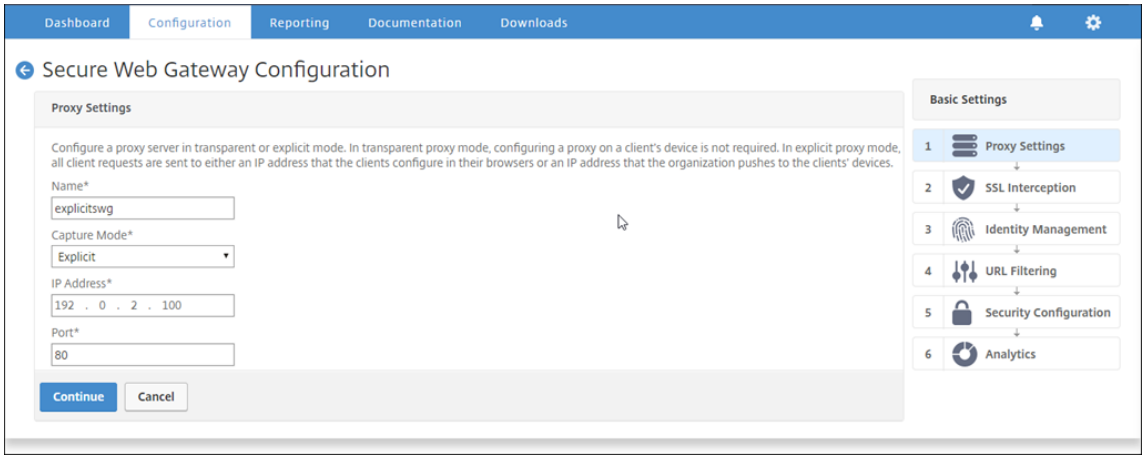
4. Klicken Sie auf **Fertig**.
5. Klicken Sie in den Abschnitt **Hostname, DNS-IP-Adresse und Zeitzone**, und geben Sie Werte für diese Felder ein.



6. Klicken Sie auf **Fertig**, und klicken Sie dann auf **Weiter**.

Konfigurieren der Proxy-Einstellungen

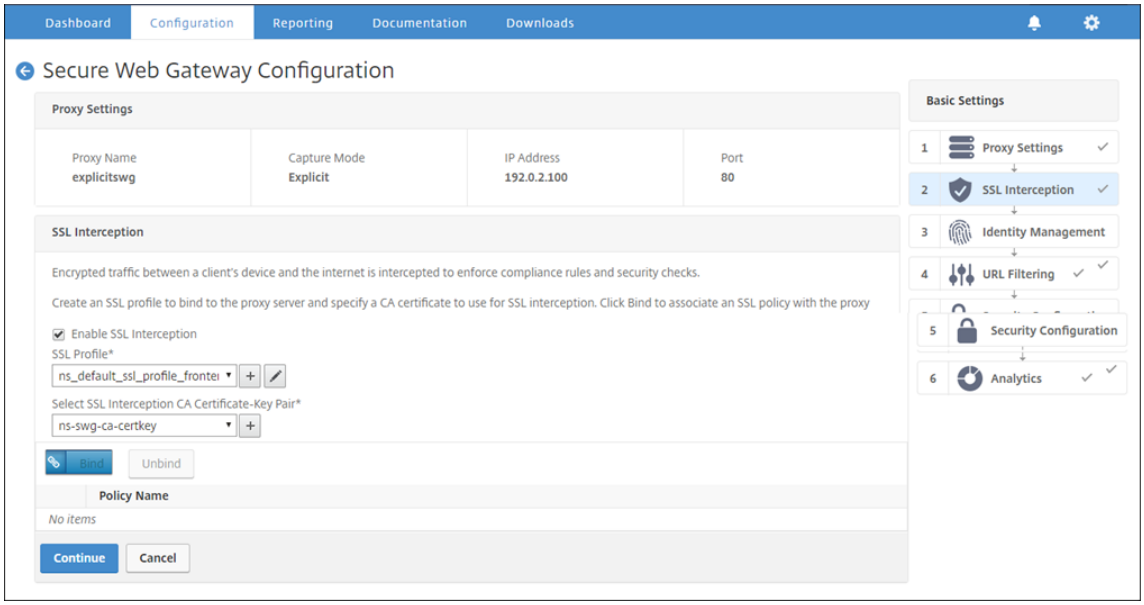
1. Navigieren Sie zu **Secure Web Gateway** > **Secure Web Gateway-Assistent**.
2. Klicken Sie auf **Erste Schritte** und dann auf **Weiter**.
3. Geben Sie im Dialogfeld **Proxyeinstellungen** einen Namen für den expliziten Proxyserver ein.
4. Wählen Sie für **den AufnahmemodusExplizit**aus
5. Geben Sie eine IP-Adresse und Portnummer ein.



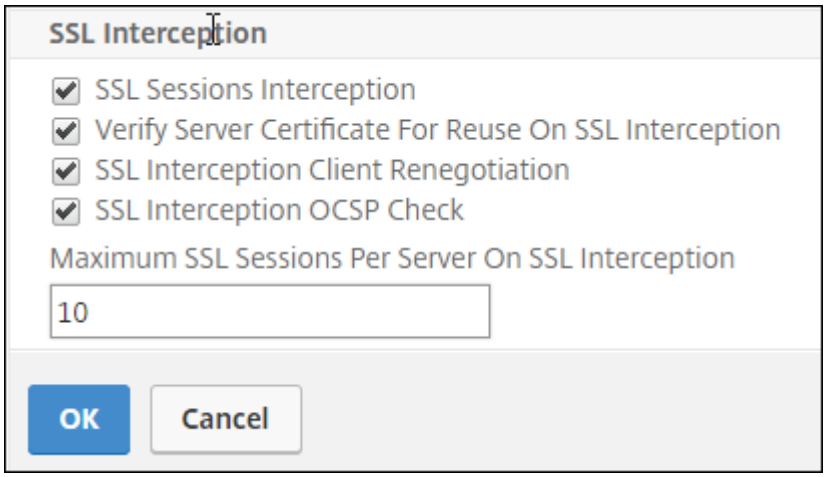
6. Klicken Sie auf **Weiter**.

Konfigurieren der Einstellungen für SSL-Interception

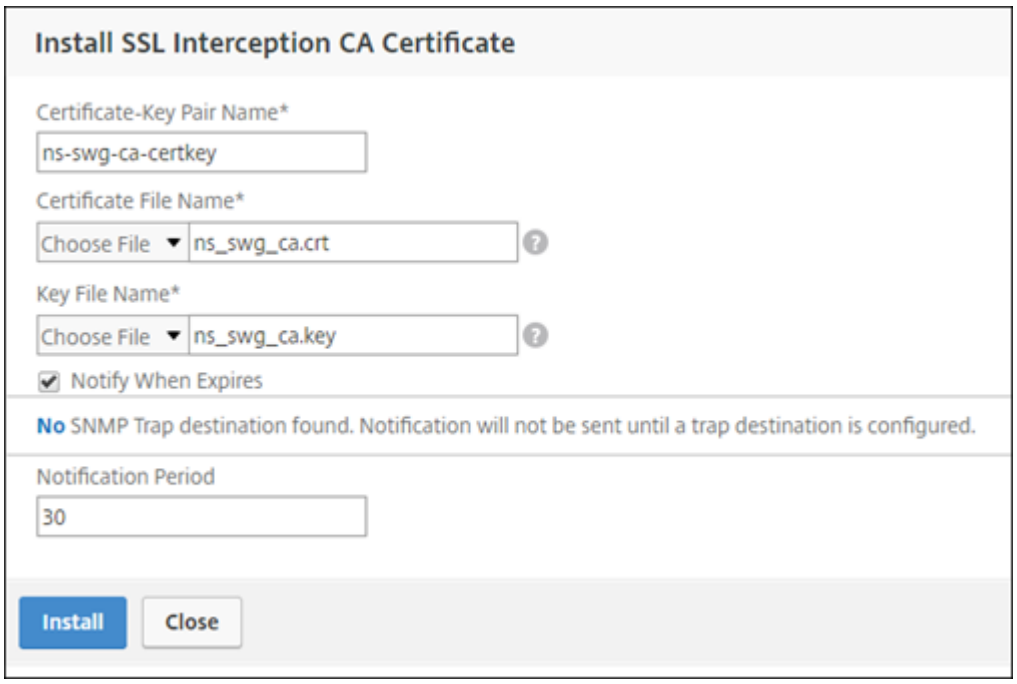
1. Wählen Sie **SSL-Interception aktivieren** aus.



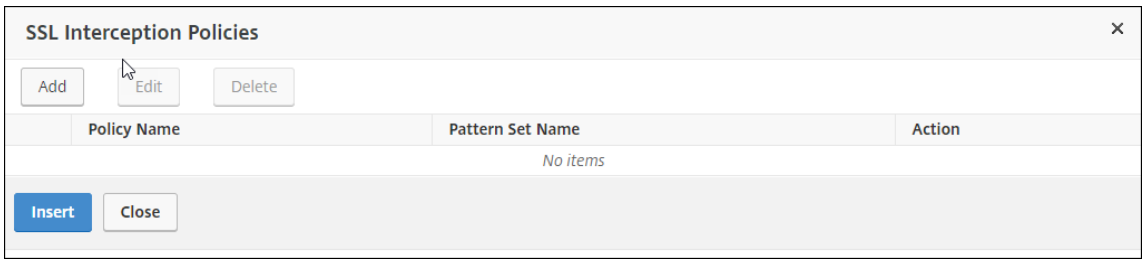
2. Wählen Sie im **SSL-Profil** ein vorhandenes Profil aus oder klicken Sie auf +, um ein neues Front-End-SSL-Profil hinzuzufügen. Aktivieren Sie **SSL Sessions Interception** in diesem Profil. Wenn Sie ein vorhandenes Profil auswählen, überspringen Sie den nächsten Schritt.



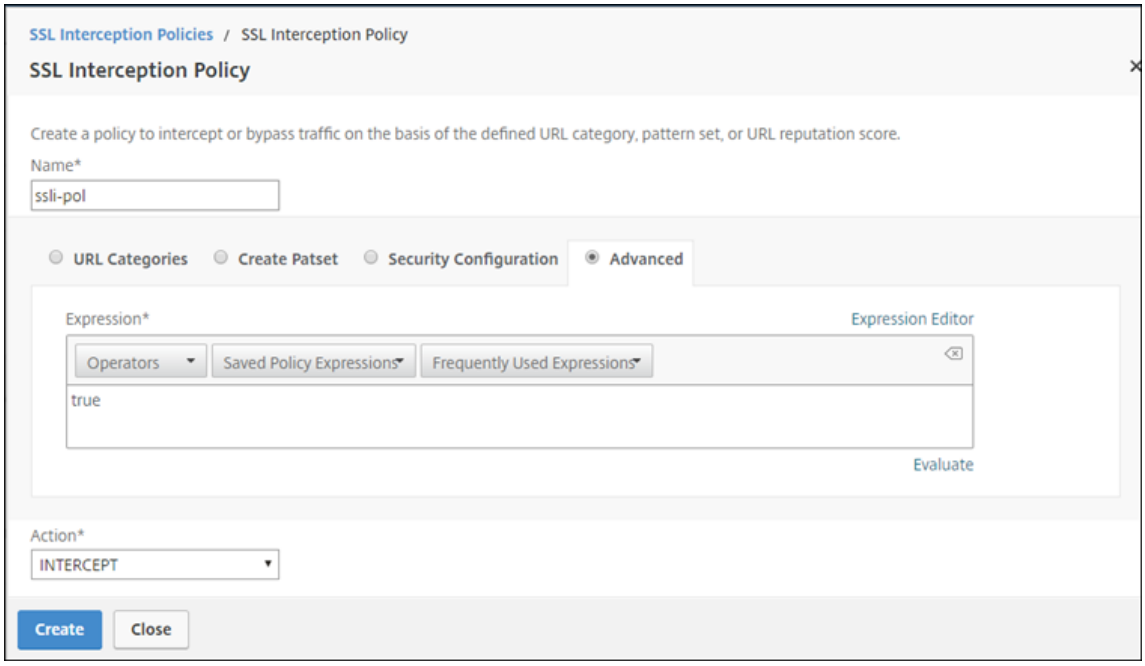
3. Klicken Sie auf **OK** und dann auf **Fertig**.
4. Wählen Sie unter **Select SSL Interception CA Certificate-Key Pair**ein vorhandenes Zertifikat aus, oder klicken Sie auf “+”, um ein CA-Zertifikatschlüsselpaar für SSL-Interception zu installieren. Wenn Sie ein vorhandenes Zertifikat auswählen, überspringen Sie den nächsten Schritt.



5. Klicken Sie auf **Installieren** und dann auf **Schließen**.
6. Fügen Sie eine Richtlinie hinzu, um den gesamten Datenverkehr abzufangen. Klicken Sie auf **Bind**. Klicken Sie auf **Hinzufügen**, um eine neue Richtlinie hinzuzufügen oder eine vorhandene Richtlinie auszuwählen. Wenn Sie eine vorhandene Richtlinie auswählen, klicken Sie auf **Einfügen**, und überspringen Sie die nächsten drei Schritte.



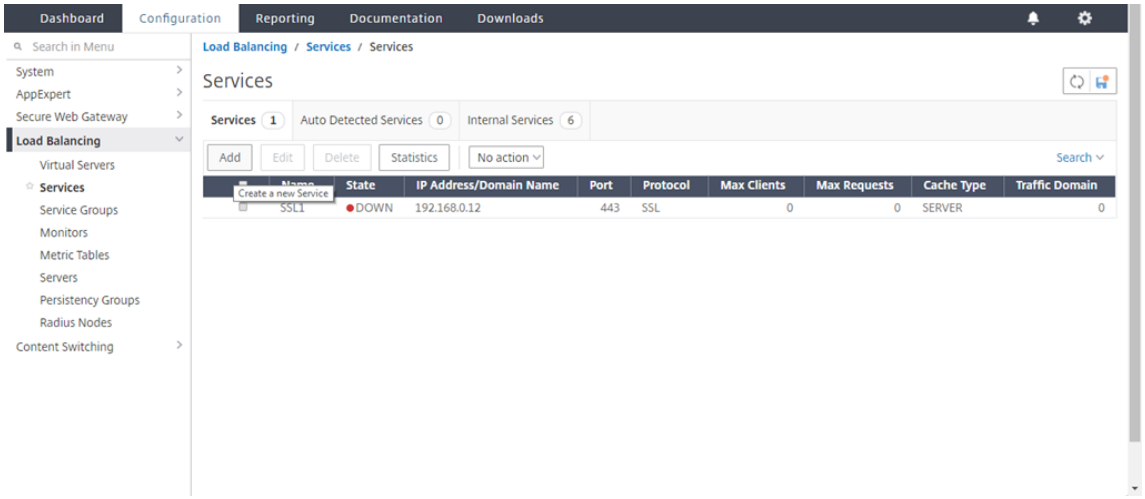
7. Geben Sie einen Namen für die Richtlinie ein, und wählen Sie **Erweitert** aus. Geben Sie im Ausdruckseditor true ein.
8. Wählen Sie unter **Aktion** die Option **INTERCEPT** aus.



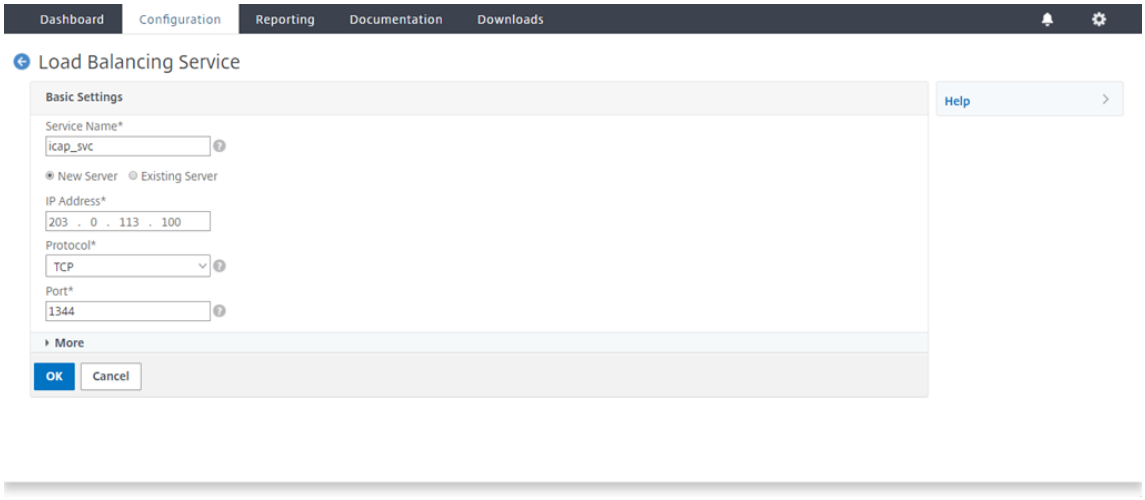
9. Klicken Sie auf **Erstellen**.
10. Klicken Sie viermal auf **Fortfahren**, und klicken Sie dann auf **Fertig**.

Konfigurieren der ICAP-Einstellungen

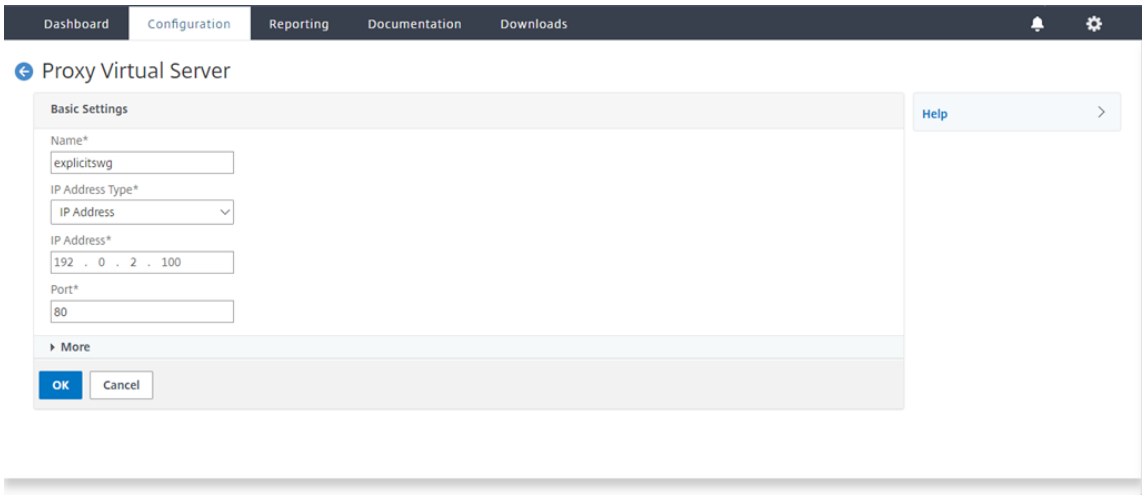
1. Navigieren Sie zu **Load Balancing** > **Services**, und klicken Sie auf **Hinzufügen**.



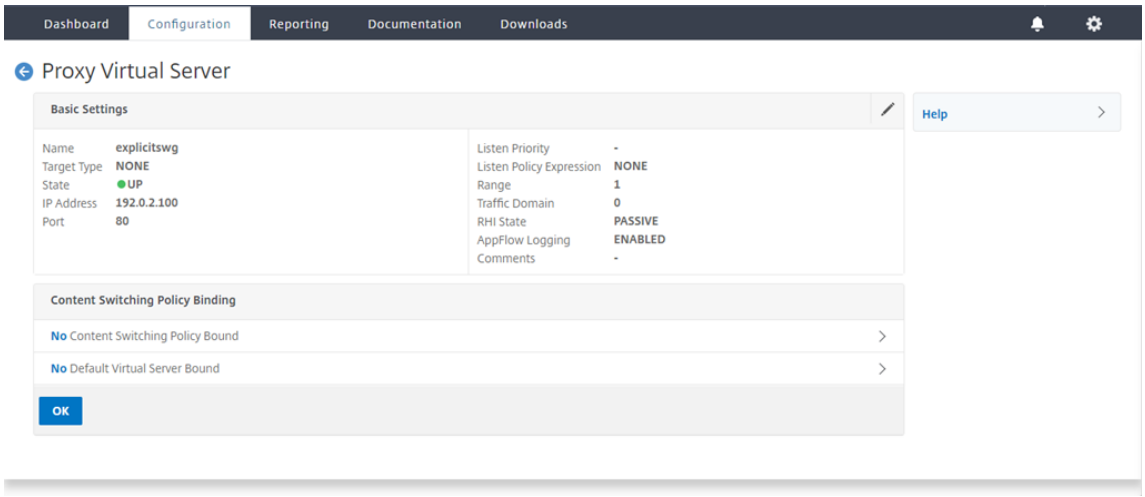
2. Geben Sie einen Namen und eine IP-Adresse ein. Wählen Sie unter **Protokoll** die Option **TCP**aus. Geben Sie in **Port** den Wert **1344**ein. Klicken Sie auf **OK**.



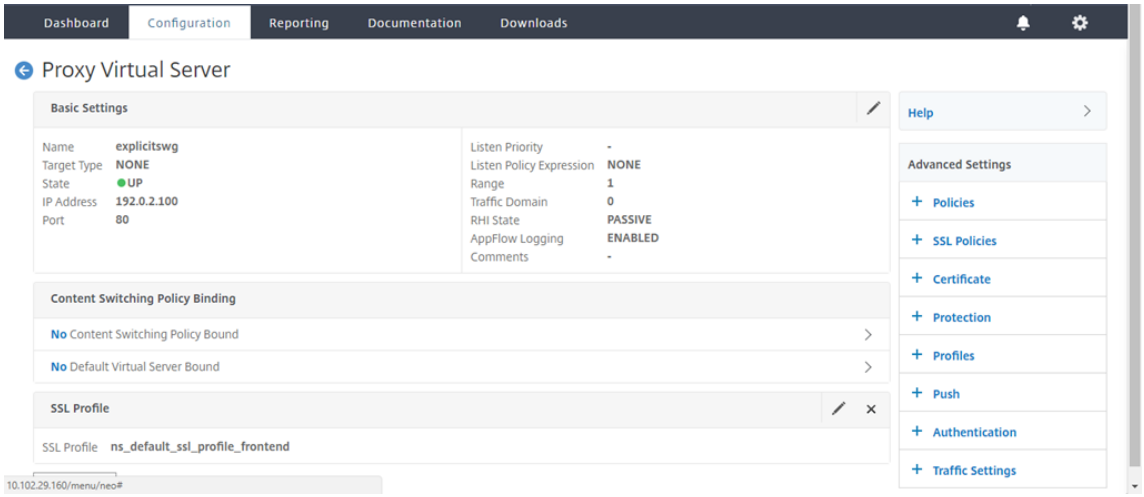
3. Navigieren Sie zu **Secure Web Gateway** > **Virtuelle Proxy-Server**. Fügen Sie einen virtuellen Proxyserver hinzu, oder wählen Sie einen virtuellen Server aus, und klicken Sie auf **Bearbeiten**. Klicken Sie nach der Eingabe von Details auf **OK**.



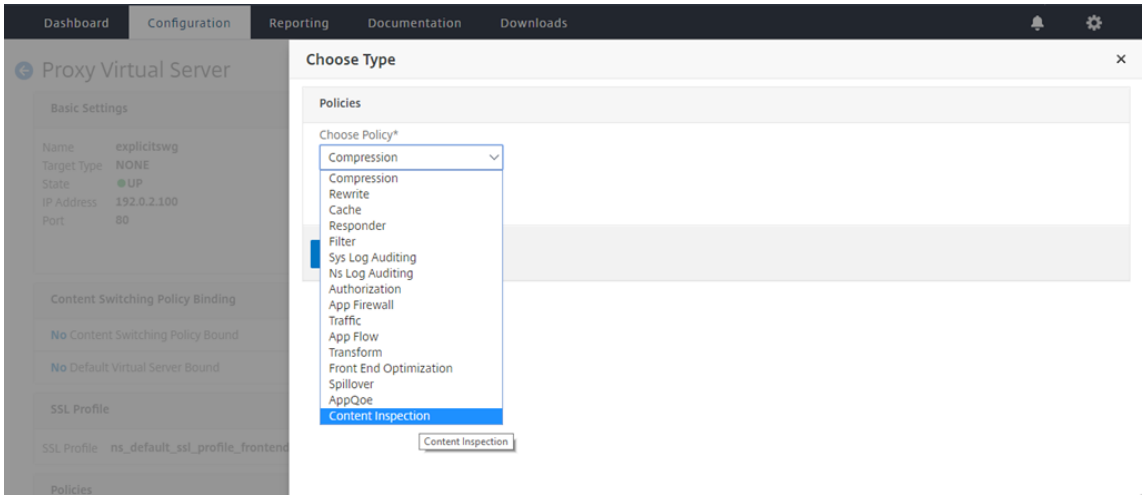
Klicken Sie erneut auf **OK**.



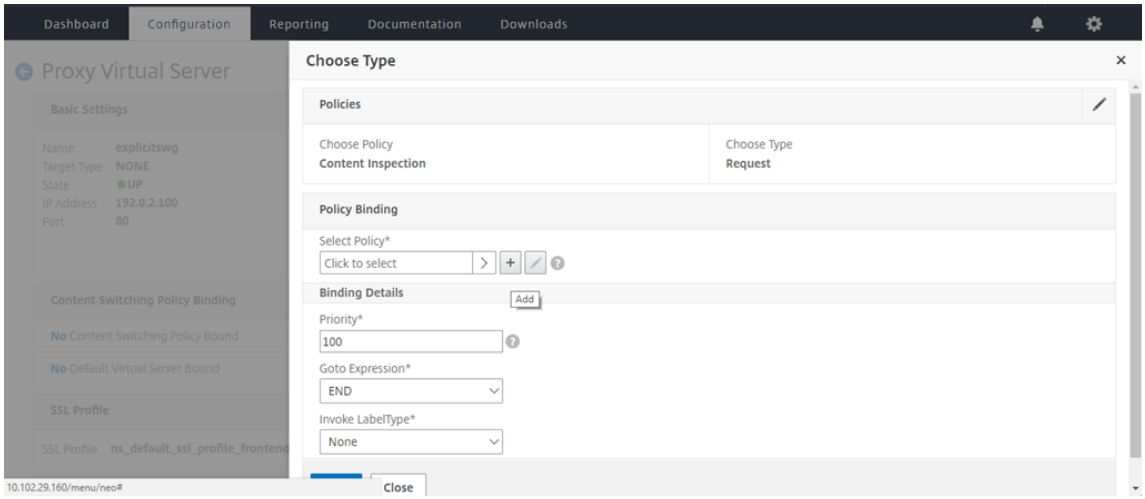
4. Klicken Sie unter **Erweiterte Einstellungen** auf **Richtlinien**.



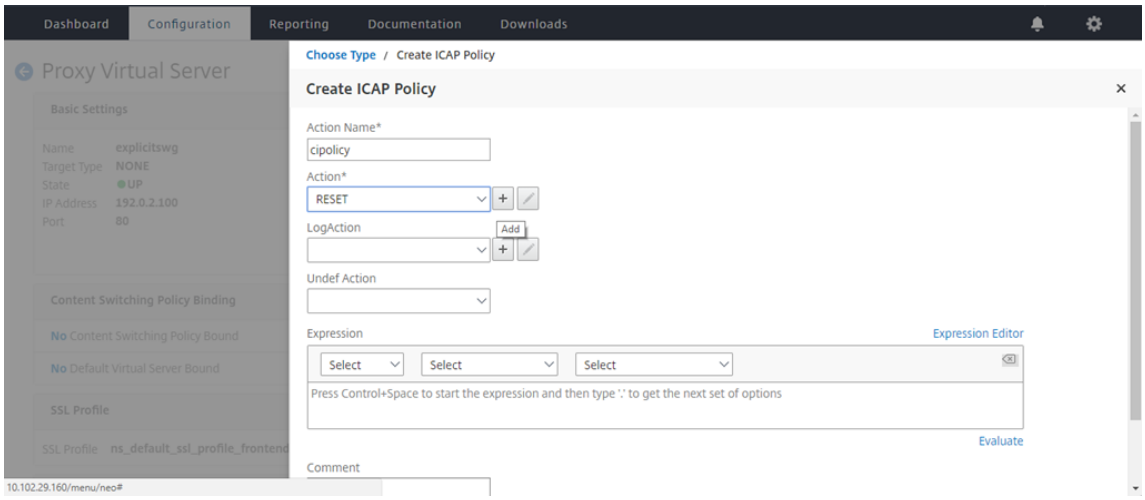
5. Wählen Sie unter **Richtlinie auswählen** die Option **Inhaltsüberprüfung** aus. Klicken Sie auf **Weiter**.



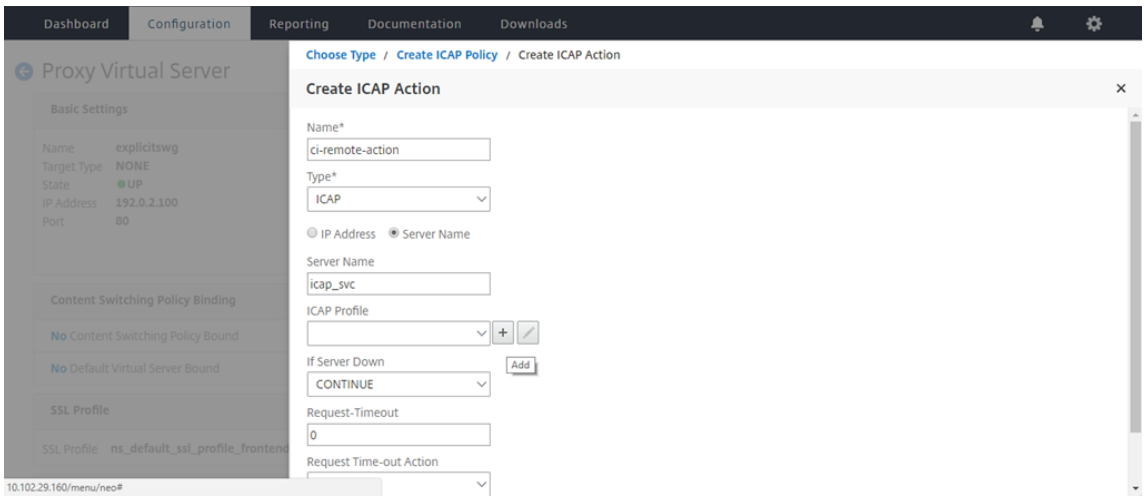
6. Klicken Sie unter **Richtlinie auswählen** auf das +-Zeichen, um eine Richtlinie hinzuzufügen.



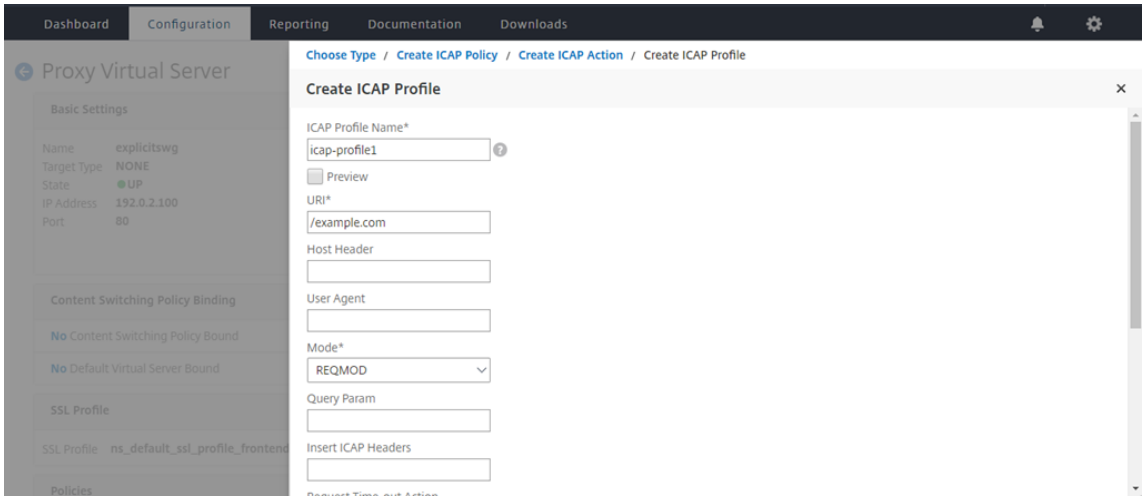
7. Geben Sie einen Namen für die Richtlinie ein. Klicken Sie in **Aktion** auf das +-Zeichen, um eine Aktion hinzuzufügen.



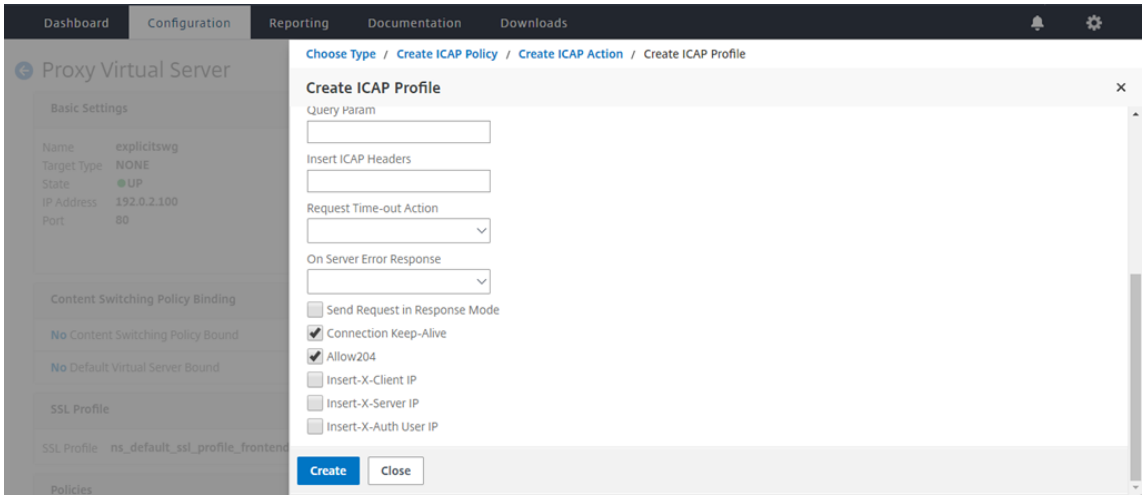
8. Geben Sie einen Namen für die Aktion ein. Geben Sie unter **Servername** den Namen des zuvor erstellten TCP-Dienstes ein. Klicken Sie im **ICAP-Profil** auf das +-Zeichen, um ein ICAP-Profil hinzuzufügen.



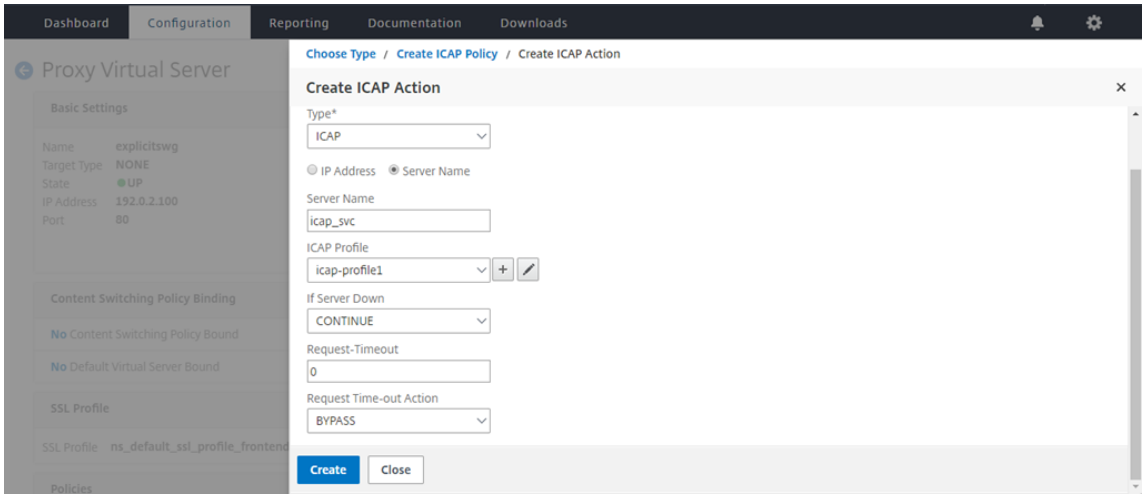
9. Geben Sie einen Profilnamen ein, URI. Wählen Sie unter **Modus** die Option **REQMOD** aus.



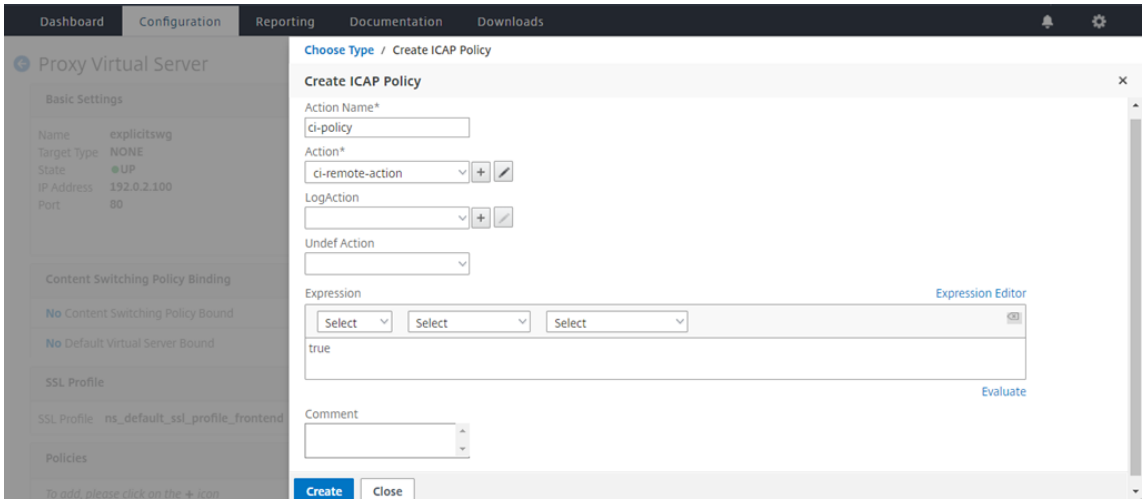
10. Klicken Sie auf **Erstellen**.



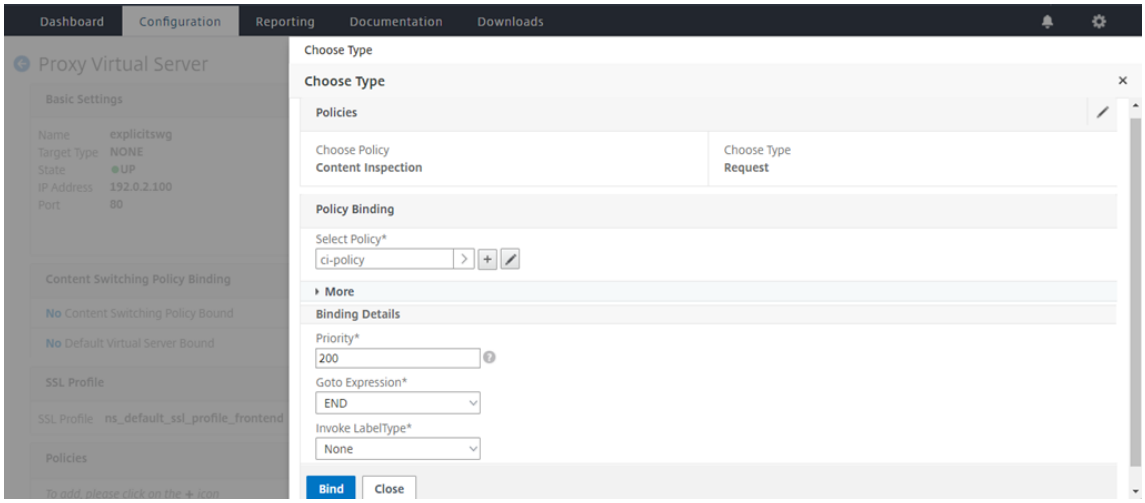
11. Klicken Sie auf der Seite **ICAP-Aktion erstellen** auf **Erstellen**.



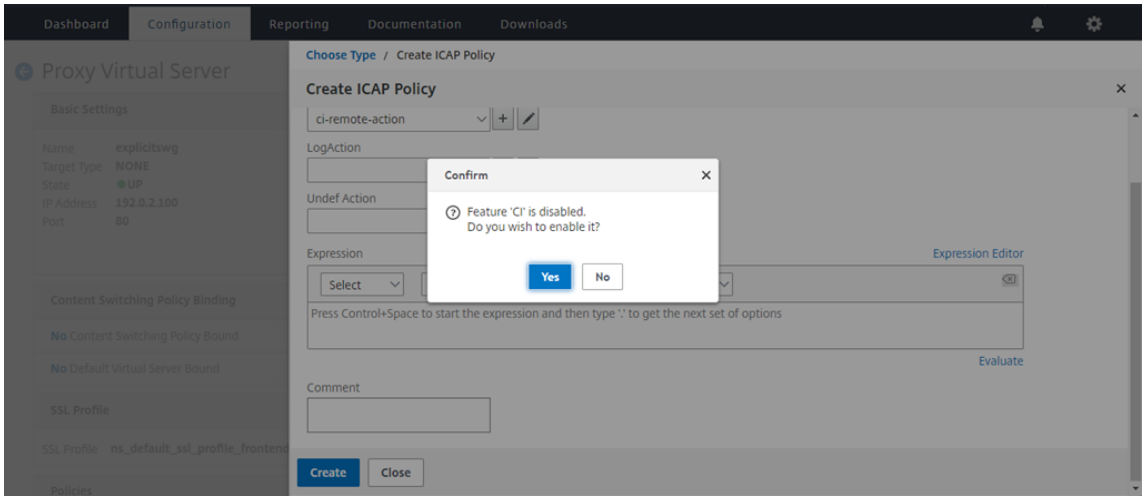
12. Geben Sie auf der Seite **ICAP-Richtlinie erstellen** im **Ausdruckseditor** “true”ein. Klicken Sie dann auf **Erstellen**.



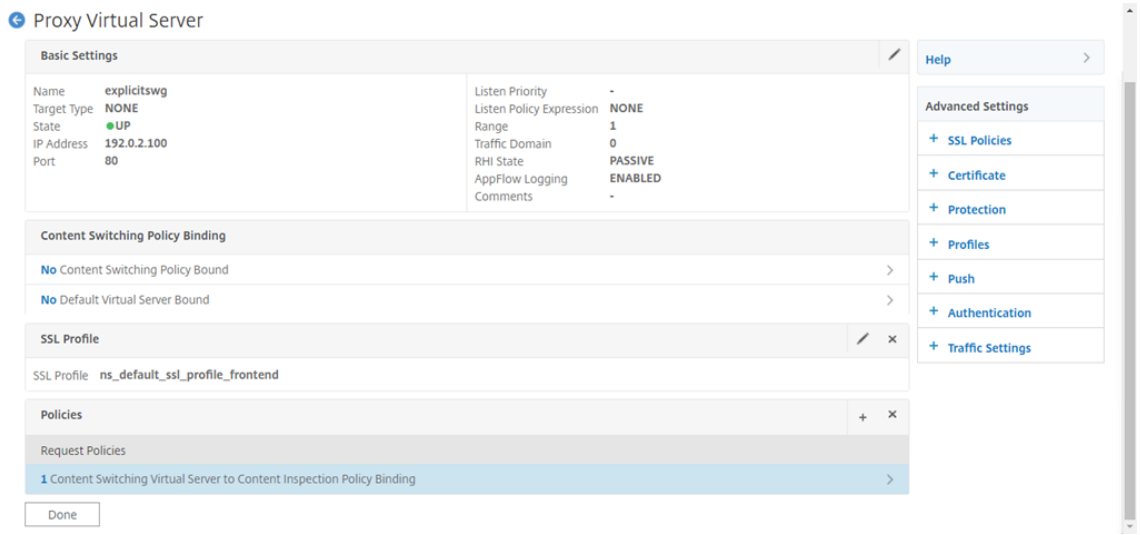
13. Klicken Sie auf **Bind**.



14. Wenn Sie aufgefordert werden, die Funktion zur Inhaltsprüfung zu aktivieren, wählen Sie **Ja** aus.



15. Klicken Sie auf **Fertig**.



Beispiel für ICAP-Transaktionen zwischen der Citrix SWG-Appliance und dem ICAP-Server in RESPMOD

Anforderung von der Citrix SWG-Appliance an den ICAP-Server:

```
RESPMOD icap://10.106.137.15:1344/resp ICAP/1.0

Host: 10.106.137.15

Connection: Keep-Alive

Encapsulated: res-hdr=0, res-body=282

HTTP/1.1 200 OK

Date: Fri, 01 Dec 2017 11:55:18 GMT

Server: Apache/2.2.21 (Fedora)

Last-Modified: Fri, 01 Dec 2017 11:16:16 GMT

ETag: "20169-45-55f457f42aee4"

Accept-Ranges: bytes

Content-Length: 69

Keep-Alive: timeout=15, max=100

Content-Type: text/plain; charset=UTF-8

X5O!P%@AP[4\PZX54(P^)7CC)7 }
 $EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
<!--NeedCopy-->
```


Antwort vom ICAP-Server auf die Citrix SWG-Appliance:

```
ICAP/1.0 200 OK

Connection: keep-alive

Date: Fri, 01 Dec, 2017 11:40:42 GMT

Encapsulated: res-hdr=0, res-body=224

Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$

ISTag: "9.8-13.815.00-3.100.1027-1.0"

X-Virus-ID: Eicar_test_file

X-Infection-Found: Type=0; Resolution=2; Threat=Eicar_test_file;

HTTP/1.1 403 Forbidden

Date: Fri, 01 Dec, 2017 11:40:42 GMT

Cache-Control: no-cache

Content-Type: text/html; charset=UTF-8

Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$

Content-Length: 5688

<html><head><META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset
    =UTF-8"/>

...

...

</body></html>
<!--NeedCopy-->
```

Anleitungsartikel

April 26, 2021

Im Folgenden finden Sie einige Konfigurationsanweisungen oder funktionale Anwendungsfälle, die als Artikel How to verfügbar sind, mit denen Sie Ihre SWG-Bereitstellung verwalten können.

URL-Filterung

Erstellen einer URL-Kategorisierungsrichtlinie

Erstellen einer URL-Listenrichtlinie

Wie man eine außergewöhnliche URL auf die Positivliste setzt

So blockieren Sie Websites für Erwachsene Kategorie

Erstellen einer URL-Kategorisierungsrichtlinie

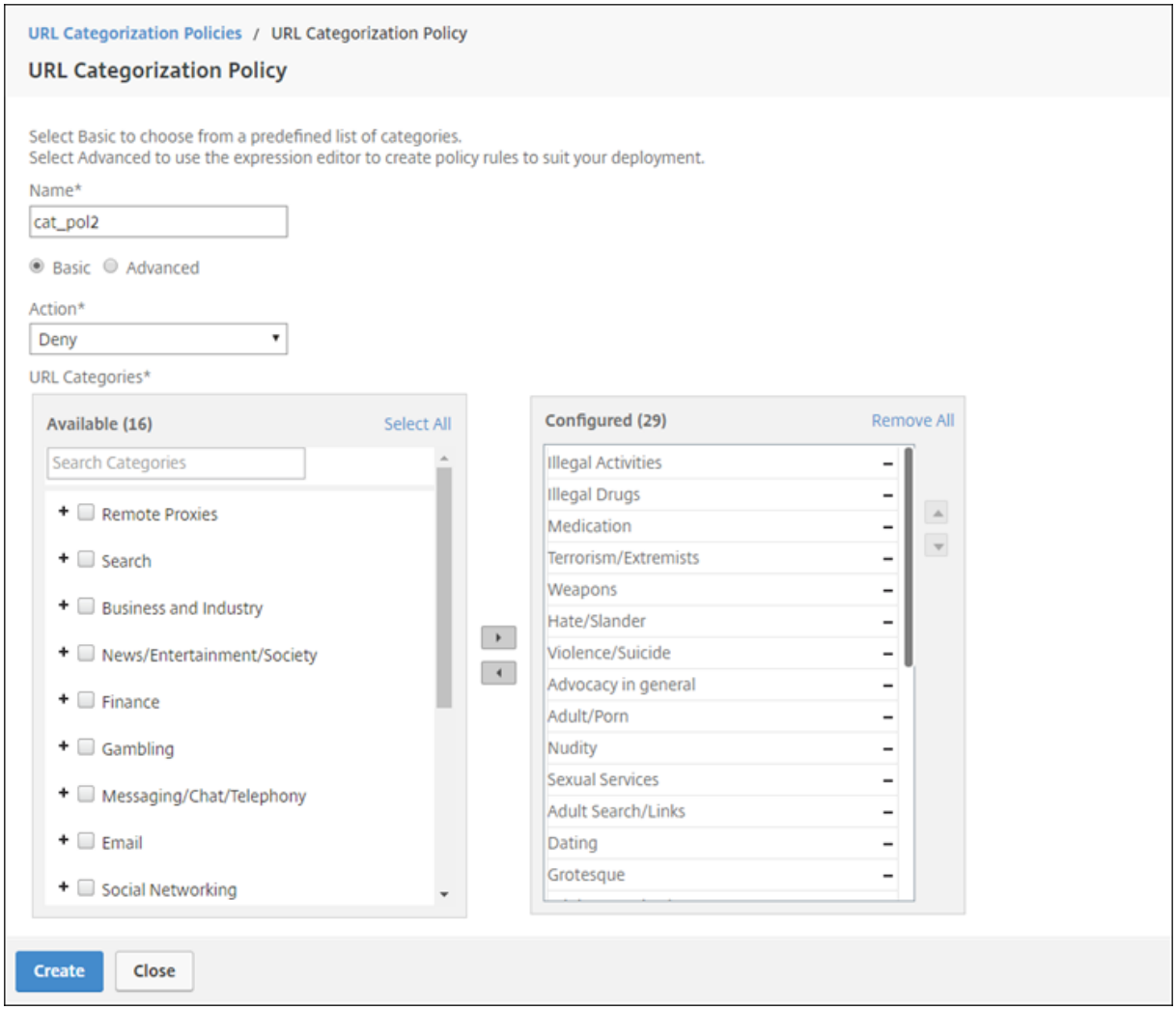
April 26, 2021

Als Netzwerkadministrator können Sie bestimmte Kategorien von Websites für den Benutzerzugriff blockieren. Sie können dies ausführen, indem Sie eine URL-Kategorisierungsrichtlinie erstellen und die Richtlinie mit einer vordefinierten Liste von Kategorien binden, die Sie den Zugriff einschränken möchten.

Beispielsweise möchten Sie den Zugriff auf alle Websites sozialer Netzwerke gemäß den Organisationsrichtlinien einschränken. In einem solchen Szenario müssen Sie eine Kategorisierungsrichtlinie erstellen und die Richtlinie an die vordefinierte Liste der Kategoriewebsites für soziale Netzwerke binden.

So erstellen Sie URL-Kategorisierungsrichtlinie mit der grundlegenden Methode:

1. Melden Sie sich bei der **Citrix SWG-** Appliance an und navigieren Sie zu **Secured Web Gateway > URL-Filterung > URL-Kategorisierung** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**, um auf die Seite **URL-Kategorisierungsrichtlinie** zuzugreifen und die folgenden Parameter anzugeben.
    a) **URL-Kategorisierungsrichtlinie**. Name der Responder-Richtlinie.
    b) **Grundlegend**. Wählen Sie Konfigurieren mit einer vordefinierten Liste von Kategorien aus.
    c) **Aktion**. Eine Aktion zum Steuern des Zugriffs auf die URL.
    d) **URL-Kategorien** Eine vordefinierte Liste von Kategorien, die ausgewählt und zu einer konfigurierten Liste hinzugefügt werden sollen.
3. Klicken Sie auf **Erstellen** und **Schließen**.

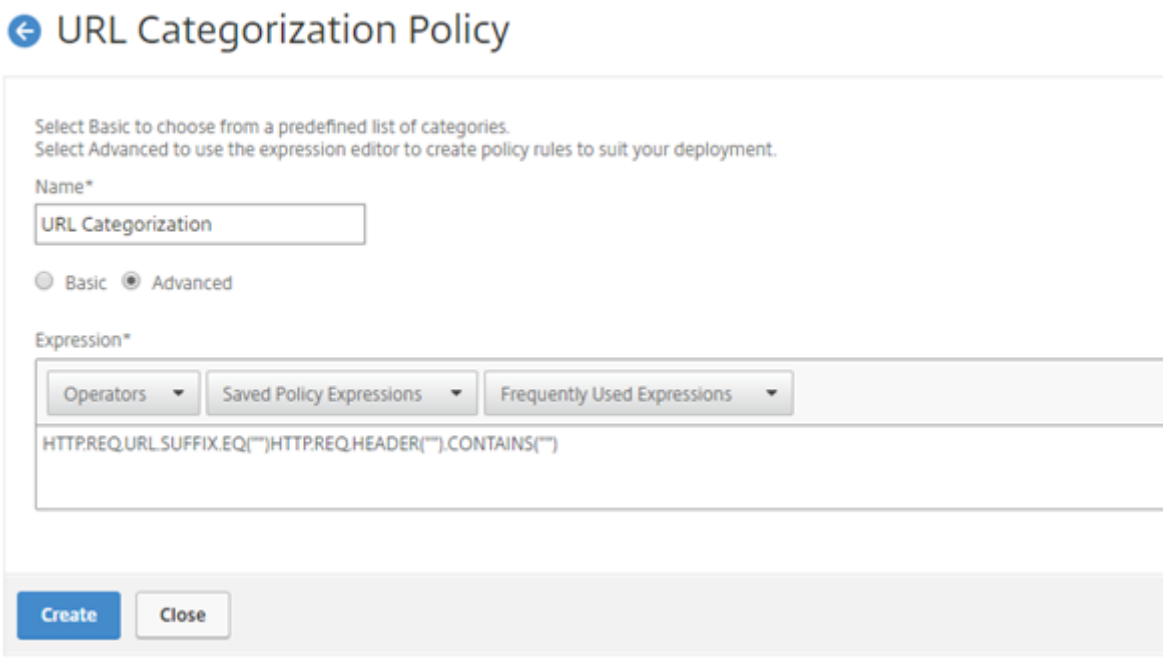


So erstellen Sie URL-Kategorisierungsrichtlinie mit der erweiterten Methode:

1. So konfigurieren Sie eine neue URL-Kategorisierungsrichtlinie mit der erweiterten Kategorisierung.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie auf der Seite **URL-Kategorisierungsrichtlinie** die folgenden Parameter an.

    a) **URL-Kategorisierungsrichtlinie**. Name der Responder-Richtlinie.
    b) **Fortgeschritten**. Konfigurieren Sie die Richtlinie mithilfe benutzerdefinierter Ausdrücke.

4. Klicken Sie auf **Erstellen** und **Schließen**.



Erstellen einer URL-Listenrichtlinie

April 26, 2021

Als Netzwerkadministrator können Sie bestimmte Kategorien von Websites für den Benutzerzugriff blockieren. Sie können dies ausführen, indem Sie URL-Listenrichtlinie erstellen und die Richtlinie mit einem URL-Satz verknüpfen, der als Textdatei in die Appliance importiert wird. Der URL-Satz ist eine Sammlung von Websites, die Sie lieber filtern möchten.

Beispielsweise möchten Sie den Zugriff auf alle Malware-Websites gemäß den Organisationsrichtlinien einschränken. In einem solchen Szenario müssen Sie eine URL-Listenrichtlinie erstellen und die Richtlinie an einen URL-Satz binden, der in die Appliance importiert wird.

So konfigurieren Sie eine URL-Listenrichtlinie:

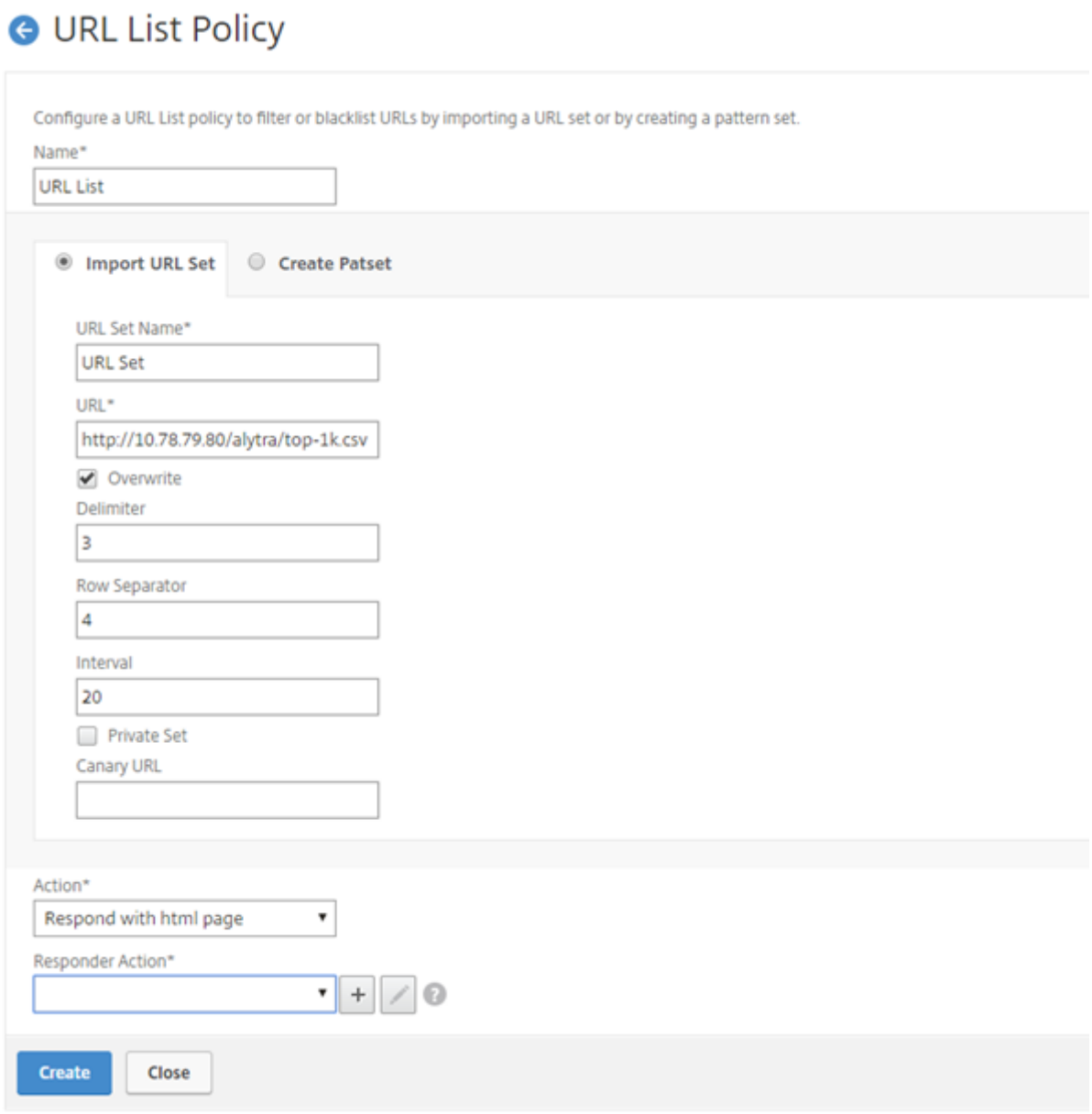
1. Melden Sie sich bei der **Citrix SWG-Appliance** an, und navigieren Sie zu **Secured Web Gateway > URL-Filterung > URL-Listen** .
2. Klicken Sie im Detailbereich auf **Hinzufügen.**
3. Geben Sie auf der Seite **URL-Listenrichtlinie** den Richtliniennamen an.
4. Wählen Sie eine Option aus, um einen URL-Satz zu importieren oder einen Mustersatz zu erstellen, und führen Sie dann eine der Verfahren aus, die dem letzten Schritt dieses Verfahrens folgen.
5. Wählen Sie eine Responder-Aktion aus der Dropdownliste aus.

6. Klicken Sie auf **Erstellen** und **Schließen**.

So importieren Sie einen benutzerdefinierten URL-Satz oder einen URL-Satz von Drittanbietern:

1. Aktivieren Sie auf der Registerkarte **URL-Listenrichtlinie** das Kontrollkästchen **URL-Satz importieren**, und geben Sie die folgenden URL-Set-Parameter an.

    a) **URL-Set-Name**—Name des URL-Sets.
    b) **URL**—Webadresse des Standorts, an dem auf den URL-Set zugegriffen werden soll.
    c) **Überschreiben**—Überschreibt den zuvor importierten URL-Satz.
    d) **Trennzeichen**—Zeichensequenz, die einen CSV-Dateidatensatz begrenzt.
    e) **Zeilentrenner**—In der CSV-Datei verwendetes Zeilentrennzeichen.
    f) **Intervall**—Intervall in Sekunden, abgerundet auf die nächsten 15 Minuten, in denen die URL-Einstellung aktualisiert wird.
    g) **Private Set**—Option, um das Exportieren des URL-Sets zu verhindern.
    h) **Canary-URL**—Interne URL zum Testen, ob der Inhalt des URLs vertraulich behandelt werden soll. Die maximale Länge der URL beträgt 2047 Zeichen. Weitere Informationen zu Canary URL finden Sie unter Konfigurieren eines privaten URL-Sets.

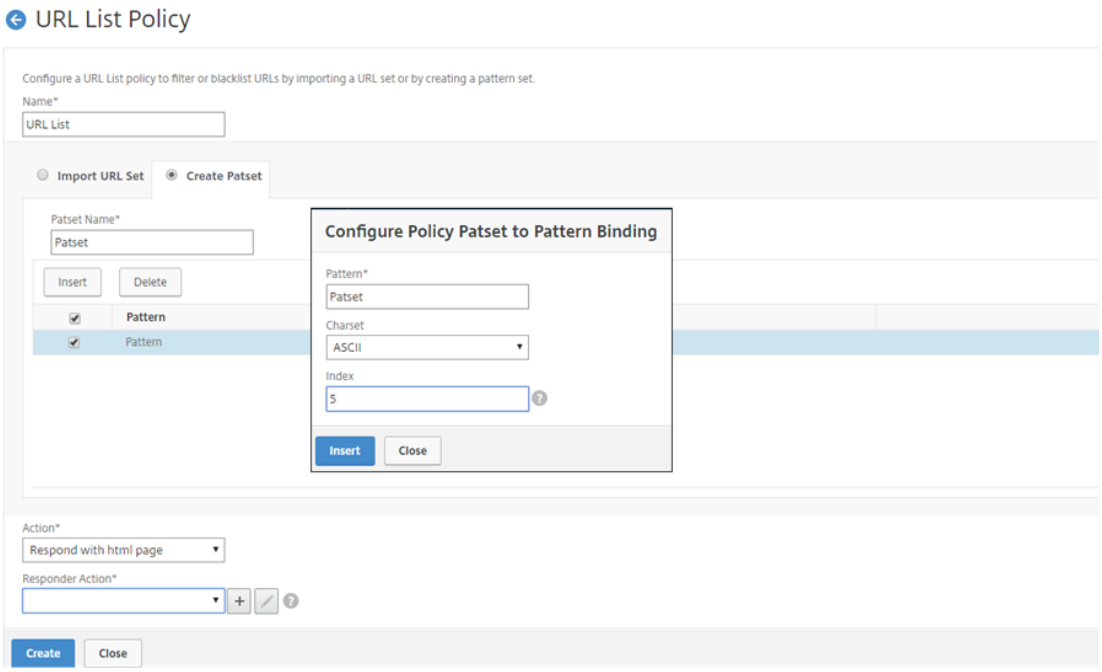


So erstellen Sie einen Mustersatz:

1. Geben Sie auf der Registerkarte **Muster erstellen** einen Namen für den Mustersatz ein.
2. Klicken Sie auf **Einfügen**, um ein Muster zu erstellen.
3. Legen Sie auf der Seite **Richtlinienpatset an Musterbindung konfigurieren** die folgenden Parameter fest.

    a) **Muster**—Zeichenkette, die ein Muster darstellt
    b) **Zeichensatz**—Zeichensatztyp: ASCII- oder UTF_8-Format
    c) **Index**—Vom Benutzer zugewiesener Indexwert, von 1 bis 4294967290

4. Klicken Sie auf **Einfügen**, um den Mustersatz hinzuzufügen, und klicken Sie dann auf **Schließen**.



Wie man eine außergewöhnliche URL auf die Positivliste setzt

April 26, 2021

Wenn Sie einen URL-Filter zum Sperren einer Kategorie von Websites verwenden, müssen Sie möglicherweise eine Positivliste oder eine bestimmte Website als Ausnahme zulassen. Wenn Sie beispielsweise die Sperrliste von Gaming-Websites bevorzugen, aber nur die Positivliste bevorzugenwww.supersports.com, müssen Sie ein Patset mit einer URL-Listenrichtlinie erstellen und dann die Richtlinie an den Proxyserver mit einer höheren Priorität als andere gebundene Richtlinien.

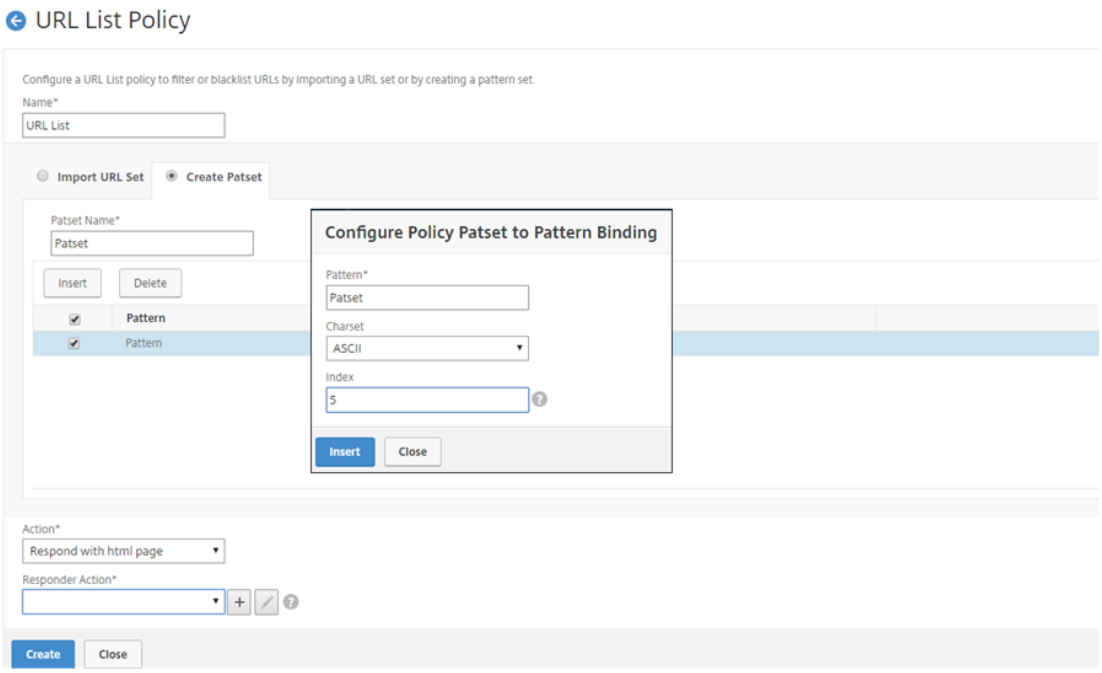
So erstellen Sie einen Mustersatz mit dem Citrix SWG-Assistenten

1. Melden Sie sich bei der **Citrix SWG-Appliance** an und navigieren Sie zu **Secured Web Gateway > URL-Filter > URL-Listen.**
2. Klicken Sie im Detailbereich auf **Hinzufügen.**
3. Geben Sie auf der Seite **URL-Listenrichtlinie** den Richtliniennamen an.
4. Wählen Sie eine Option aus, um einen URL-Satz zu importieren oder einen Mustersatz zu erstellen.
5. Geben Sie auf der Registerkarte **Muster erstellen** einen Namen für den Mustersatz ein.
6. Klicken Sie auf **Einfügen**, um ein Muster zu erstellen.

7. Legen **Sie auf der Seite Richtlinienpatset an Musterbindung konfigurieren** die folgenden Parameter fest.

   a) **Muster**—Eine Zeichenfolge, die ein Muster darstellt.
   b) **Charset**—Der Zeichensatztyp definiert als ASCII- oder UTF_8-Format.
   c) **Index**—Ein vom Benutzer zugewiesener Indexwert (von 1 bis 4294967290)

8. Klicken Sie auf **Ein** fügen, um den Mustersatz hinzuzufügen, und klicken Sie auf **Schließen** .



So legen Sie die Priorität des Richtlinienausdrucks mit der Citrix SWG-GUI fest:

1. Melden Sie sich bei der **Citrix SWG**-Appliance an, und navigieren Sie zu **Secure Web Gateway > Virtual Proxy-Server**.
2. Wählen Sie auf der Detailseite einen Server aus, und klicken Sie auf **Bearbeiten**.
3. Gehen Sie auf der Seite **Virtuelle Proxyserver** zum Abschnitt **Richtlinien** und klicken Sie auf das Bleistiftsymbol, um die Details zu bearbeiten.
4. Wählen Sie die von Ihnen erstellte Patset-Richtlinie aus, und geben Sie auf der Seite **Richtlinienbindung** den Prioritätswert an, der niedriger ist als andere gebundene Richtlinien.
5. Klicken Sie auf **Binden** und **Fertig**.

So blockieren Sie die Website der Erwachsenenkategorie

April 26, 2021

Als Enterprise-Kunde möchten Sie möglicherweise Websites blockieren, die zur Kategorie Erwachsene gehören. Dies geschieht durch Konfigurieren einer Responder-Richtlinie, die Anforderungen einer Erwachsenenkategorie auswählt und den Zugriff auf solche URLs in der Sperrliste blockiert.

URL-Kategorisierung konfigurieren, um Websites zu blockieren, die zur Kategorie Erwachsener gehören

So konfigurieren Sie eine Richtlinie und blockieren Sie Websites für Erwachsene mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

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

Beispiel:

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

Konfigurieren der URL-Kategorisierung zum Blockieren von Websites für Erwachsene mit dem Citrix SWG-Assistenten

So blockieren Sie Kategorien für Erwachsene mit dem Citrix SWG-Assistenten

1. Melden Sie sich bei der **Citrix SWG-** Appliance an, und navigieren Sie zu **Secure Web Gateway** .
2. Klicken Sie im Detailbereich auf **Secured Web Gateway-Assistent**.
3. Geben Sie auf der Seite **Secure Web Gateway-Konfiguration** die Einstellungen des SWG-Proxy-Servers an.
4. Klicken Sie auf **Weiter**, um andere Einstellungen wie SSL-Interception und Identifizieren der Verwaltung anzugeben.
5. Klicken Sie auf **Weiter**, um auf den Abschnitt **URL-Filterung** zuzugreifen.
6. **Aktivieren Sie das Kontrollkästchen URL-Kategorisierung** aktivieren, um die Funktion zu aktivieren.
7. Klicken Sie auf Binden, um auf den Schieberegler für **URL-Kategorisierungsrichtlinien** zuzugreifen.
8. Wählen Sie eine Richtlinie aus, und klicken Sie auf **Einfügen**, um die Richtlinie zu binden.
9. Wählen Sie die Responder-Richtlinie aus, um Websites für Erwachsene zu blockieren.

10. Um eine neue Richtlinie hinzuzufügen, klicken Sie auf **Hinzufügen**, um auf die Seite **URL-Kategorisierungsrichtlinie auf** zurufen, und führen Sie eine der folgenden Aktionen aus.

    a) Klicken Sie auf **Hinzufügen**, um eine Richtlinie mit der grundlegenden Kategorisierung zu konfigurieren.

        i. Geben Sie auf der Seite **URL-Kategorisierungsrichtlinie** die folgenden Parameter an.

            A. URL-Kategorisierungsrichtlinie. Name der Responder-Richtlinie.
            B. Grundlegend. Konfigurieren Sie die Richtlinie mit der grundlegenden Konfigurationsmethode.
            C. Aktion. Eine Aktion zum Steuern des Zugriffs auf die URL.
            D. URL-Kategorien Wählen Sie in der vordefinierten Liste die Kategorie Erwachsene aus.

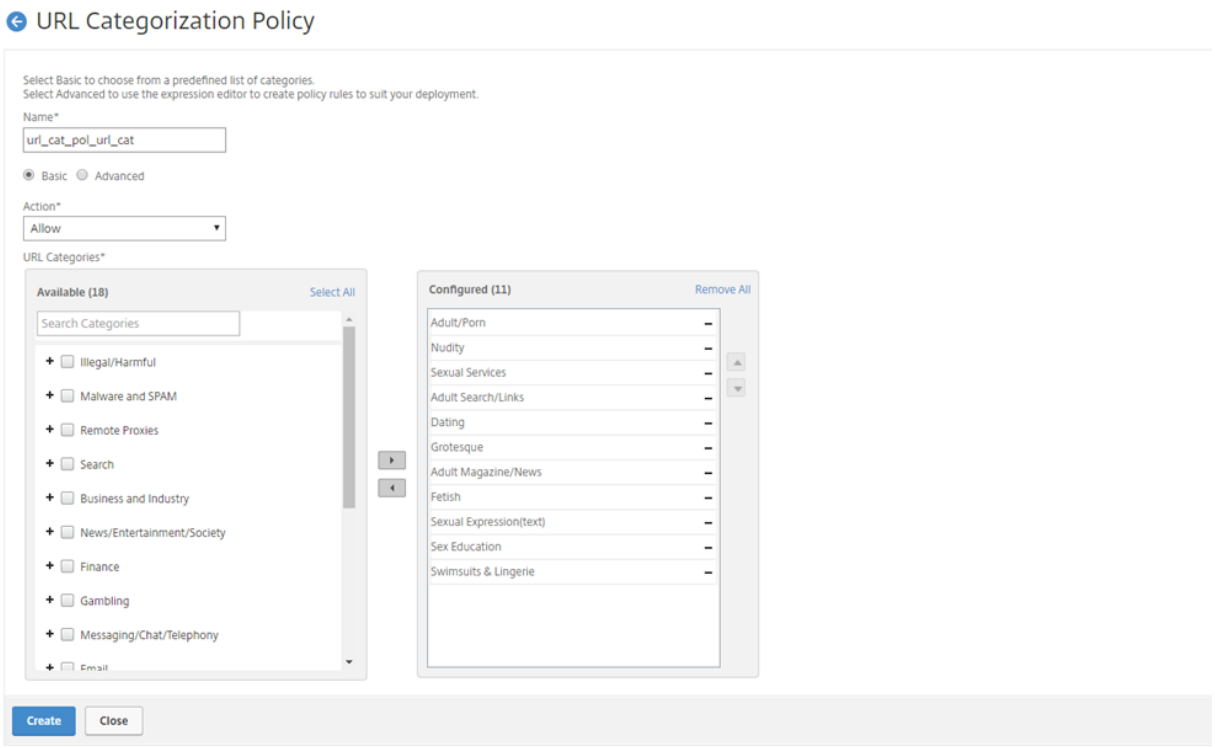
11. Klicken Sie auf **Erstellen** und **Schließen**.

    a) Klicken Sie auf **Hinzufügen**, um eine neue URL-Kategorisierungsrichtlinie mit der erweiterten Kategorisierung zu konfigurieren.

        i. Geben Sie auf der Seite **URL-Kategorisierungsrichtlinie** die folgenden Parameter an.

            A. **URL-Kategorisierungsrichtlinie**. Name der Responder-Richtlinie.
            B. **Fortgeschritten**. Konfigurieren Sie die Richtlinie, um Anforderungen der Kategorie Erwachsene zu blockieren.

12. Klicken Sie auf **Erstellen** und **Schließen**.



System

April 29, 2020

Die Systemfunktionen enthalten konzeptionelle Informationen und Konfigurationsanweisungen, die Sie bei der Konfiguration einer Citrix SWG-Appliance möglicherweise verweisen möchten.

In der folgenden Tabelle werden die Features in einer Citrix SWG-Appliance beschrieben.

Grundlegende Operationen- Betriebs- und Konfigurationsdetails einer Citrix ADC-Appliance auf Systemebene.

Authentifizierung und Autorisierung- Konfigurationsdetails beim Erstellen von Benutzern, Benutzergruppen und Befehlsrichtlinien sowie beim Zuweisen von Richtlinien zu Benutzerkonten

TCP-Konfiguration- Konfigurationsdetails des TCP-Profils und der TCP-Funktionen auf einer Citrix ADC-Appliance.

HTTP-Konfiguration- Konfigurationsdetails zum HTTP-Profil und HTTP-Funktionen auf einer Citrix ADC-Appliance.

SNMP- Ein Netzwerkverwaltungsprotokoll, das die Citrix ADC-Appliance überwacht und umgehend auf Probleme auf der Appliance reagiert.

Auditprotokollierung- Ein Standardprotokoll zum Protokollieren von Citrix ADC-Appliance-Zuständen und Statusinformationen, die von verschiedenen Modulen im Kernel und in den Daemons auf Benutzerebene erfasst werden. Für die Überwachungsprotokollierung können Sie SYSLOG- oder NSLOG-Protokoll oder beides verwenden.

Call Home- Ein Benachrichtigungssystem zur Überwachung und Behebung kritischer Fehlerbedingungen auf einer Citrix SWG-Appliance.

Reporting-Tool- Eine webbasierte Schnittstelle, auf die von einer Citrix SWG-Appliance zugegriffen wird, um Systemleistungsberichte als Diagramme anzuzeigen.

Netzwerke

April 29, 2020

Die folgenden Artikel enthalten konzeptionelle Referenzinformationen und Konfigurationsanweisungen für Netzwerkfunktionen, die Sie möglicherweise auf einer Citrix SWG-Appliance konfigurieren möchten.

- IP-Adressierung von Citrix ADC-eigenen IP-Adressen und deren Konfigurationsdetails.

- Schnittstellen Zugriff und Konfiguration der Citrix SWG-Appliance.
- Zugriffssteuerungslisten (ACL) Verschiedene Arten von Zugriffskontrolllisten, die auf Citrix ADC-Appliances verwendet werden, mit Konfigurationsdetails.
- IP-Routing Die verschiedenen IP-Routingprotokolle, die auf einer Citrix ADC-Appliance verwendet werden.
- Internetprotokoll Version 6 (IPv6) Internetprotokollunterstützung auf einer Citrix ADC-Appliance und Funktionsweise der Appliance als IPv6-Knoten.
- VXLAN Virtual eXtensible Local Area Network (VXLAN) -Unterstützung in der Citrix ADC-Netzwerkinfrastruktur und wie VXLAN Layer 2-Netzwerke auf eine Layer 3-Infrastruktur überlagert, indem Layer-2-Frames in UDP gekapselt werden -Pakete.

AppExpert

April 26, 2021

Die folgenden Artikel enthalten konzeptionelle Informationen und Konfigurationsanweisungen für AppExpert-Features, die Sie möglicherweise auf einer Citrix SWG-Appliance konfigurieren möchten.

Mustersätze und Datensätze - Richtlinienausdrücke zum Ausführen von String-Matching-Operationen auf einem großen Satz von String-Mustern.

Abhängig vom Mustertyp, den Sie abgleichen möchten, können Sie eines der folgenden Features verwenden, um Musterabgleich zu implementieren:

- Ein Mustersatz ist ein Array von indizierten Mustern, die für die Zeichenfolgenabgleich während der Standardauswertung von Syntaxrichtlinien verwendet werden. Beispiel für einen Mustersatz: imagetypes {svg, bmp, png, gif, tiff, jpg}.
- Ein Datensatz ist eine spezielle Form von Mustersatz. Es ist ein Array von Mustern des Typs Zahl (Integer), IPv4-Adresse oder IPv6-Adresse.

Variablen - Objekte, die Informationen in Form von Token speichern und von Responder-Richtlinienaktionen verwendet werden.

Variablen sind von zwei Typen wie unten angegeben:

- Singleton-Variablen. Kann einen einzelnen Wert von einem der folgenden Typen haben: ulong und text (max-size). Der ulong-Typ ist eine 64-Bit-Ganzzahl ohne Vorzeichen, der Texttyp ist eine Folge von Bytes und max-size ist die maximale Anzahl von Bytes in der Sequenz.

- Variablen zuordnen. Karten enthalten Werte, die mit Schlüsseln verknüpft sind: Jedes Schlüssel-Wert-Paar wird als Karteneintrag bezeichnet. Der Schlüssel für jeden Eintrag ist innerhalb der Karte eindeutig.

Richtlinien und Ausdrücke- Richtlinien steuern den Webverkehr, der in eine Citrix SWG-Appliance eintritt. Eine Richtlinie verwendet einen logischen Ausdruck, der auch als Regel bezeichnet wird, um Anforderungen, Antworten oder andere Daten auszuwerten und wendet eine oder mehrere Aktionen an, die durch das Ergebnis der Auswertung bestimmt werden. Alternativ kann eine Richtlinie ein Profil anwenden, das eine komplexe Aktion definiert.

Responder- Richtlinie, die Antworten basierend darauf sendet, wer die Anforderung sendet, von wo aus sie gesendet wird, und andere Kriterien mit Auswirkungen auf die Sicherheit und die Systemverwaltung. Die Funktion ist einfach und schnell zu bedienen. Durch das Vermeiden des Aufrufs komplexerer Funktionen reduziert es die CPU-Zyklen und den Zeitaufwand für die Verarbeitung von Anforderungen, die keine komplexe Verarbeitung erfordern. Wenn Sie beim Umgang mit sensiblen Daten wie Finanzinformationen sicherstellen möchten, dass der Client eine sichere Verbindung zum Durchsuchen einer Website verwendet, können Sie die Anforderung mit dem HTTPS-Protokoll auf eine sichere Verbindung umleiten.

Neuschreiben- Richtlinie, die Informationen in den Anforderungen und Antworten umschreibt, die von der Citrix SWG-Appliance verarbeitet werden. Das Umschreiben kann helfen, den Zugriff auf den angeforderten Inhalt bereitzustellen, ohne unnötige Details zur tatsächlichen Konfiguration der Website anzuzeigen.

URL-Sets- Erweiterte Richtlinienausdrücke zum Sperren einer Million URL-Einträge. Um den Zugriff auf eingeschränkte Websites zu verhindern, verwendet eine Citrix SWG-Appliance einen speziellen URL-Abgleichsalgorithmus. Der Algorithmus verwendet einen URL-Satz, der eine Liste von URLs bis zu einer Million (1.000.000) Einträge in der Sperrliste enthalten kann. Jeder Eintrag kann Metadaten enthalten, die URL-Kategorien und Kategoriegruppen als indizierte Muster definieren. Die Appliance kann auch regelmäßig URLs von hochsensiblen URLs herunterladen, die von Internet-Durchsetzungsbehörden (mit Regierungswebsites) oder unabhängigen Internetorganisationen verwaltet werden.

SSL

April 29, 2020

Die folgenden Artikel enthalten konzeptionelle Referenzinformationen und Konfigurationsanweisungen für SSL-Features, die Sie möglicherweise auf einer Citrix SWG-Appliance konfigurieren möchten.

- Zertifikate
- Zertifikatsperrlisten (CRL)
- SSL-Richtlinien
- OCSP-Responder

FAQ

April 26, 2021

F: Welche Hardwareplattformen werden für Citrix Secure Web Gateway (SWG) unterstützt?

A. Citrix SWG ist auf den folgenden Hardwareplattformen verfügbar:

- 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
- Alle Cavium N2 und N3 basierten SDX-Plattformen

F: Welche zwei Erfassungsmodi kann ich beim Erstellen eines Proxys auf der SWG-Appliance festlegen?

A. Die SWG-Lösung unterstützt explizite und transparente Proxy-Modi. Im expliziten Proxymodus müssen die Clients eine IP-Adresse und einen Port in ihren Browsern angeben, es sei denn, die Organisation verschiebt die Einstellung auf das Gerät des Clients. Diese Adresse ist die IP-Adresse eines Proxy-Servers, der auf der SWG-Appliance konfiguriert ist. Transparenter Proxy ist, wie der Name schon sagt, für den Client transparent. Die SWG-Appliance ist in einer Inline-Bereitstellung konfiguriert, und die Appliance akzeptiert transparent den gesamten HTTP- und HTTPS-Datenverkehr.

F: Verfügt Citrix SWG über einen Konfigurationsassistenten?

A. Ja. Der Assistent befindet sich auf dem SWG-Knoten im Konfigurationsdienstprogramm.

F: Welche Citrix ADC-Funktionen werden bei der Konfiguration von Citrix SWG verwendet?

A. Responder, AAA-TM, Content Switching, SSL, Forward-Proxy, SSL-Interception und URL-Filterung.

F: Welche Authentifizierungsmethoden werden von Citrix SWG unterstützt?

A. Im expliziten Proxymodus werden die Authentifizierungsmethoden LDAP, RADIUS, TACACS + und NEGOTIATE unterstützt. Im transparenten Modus wird nur die LDAP-Authentifizierung unterstützt.

F: Muss das Zertifizierungsstellenzertifikat auf dem Clientgerät installiert werden?

A. Ja. Die Citrix SWG-Appliance emuliert das Ursprungsserverzertifikat. Dieses Serverzertifikat muss von einem vertrauenswürdigen Zertifizierungsstellenzertifikat signiert sein, das auf den Geräten der Clients installiert werden muss, damit der Client dem regenerierten Serverzertifikat vertrauen kann.

F: Kann ich eine Citrix ADC Platform-Lizenz auf der Citrix SWG-Plattform verwenden?

A. Nein. Die Citrix SWG-Plattform erfordert eine eigene Plattformlizenz.

F: Wird HA für eine Citrix Secure Web Gateway-Bereitstellung unterstützt?

A. Ja.

F: Welche Datei enthält die Protokolle für Citrix SWG?

A. In der Datei ns.log werden Citrix SWG-Informationen aufgezeichnet. Sie müssen die Protokollierung mit der CLI oder GUI aktivieren. Geben Sie an der Eingabeaufforderung: **set syslogparams -ssli Enabled**ein.

Navigieren Sie in der GUI zu **System** > **Auditing** . Klicken Sie **unter Einstellungen**auf **Auditing Syslog-Einstellungen ändern**. Wählen Sie **SSL-Interception**aus.

F: Welche nsconmsg-Befehle kann ich verwenden, um Probleme zu beheben?

A. Sie können einen oder beide der folgenden Befehle verwenden:

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

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

F: Wie erhalte ich Updates, wenn das Zertifikatspaket integriert ist?

A. Das neueste Bundle ist im Build enthalten. Wenden Sie sich an den Citrix Support, um Updates zu erhalten.

F: Können Daten auf Citrix ADM von Citrix SWG erfasst werden?

A. Ja. Sie müssen **Analytics** im Secure Web Gateway-Assistenten aktivieren.

Wichtig: Stellen Sie sicher, dass Sie denselben 12.0-Build für MAS und SWG verwenden.

F: Was ist URL-Filterdienst?

A. URL-Filter ist ein Webinhaltsfilter, der den Zugriff auf eine Liste mit eingeschränkten Websites und Webseiten steuert. Der Filter schränkt den Benutzerzugriff auf unangemessene Inhalte im Internet basierend auf URL-Kategorie, Kategoriegruppen und Reputationsbewertung ein. Ein Netzwerkadministrator kann den Webverkehr überwachen und den Benutzerzugriff auf hochriskante Websites blockieren. Sie können das Feature mithilfe von URL-Kategorisierung oder URL-Listenfunktion

basierend auf der Richtliniendurchsetzung implementieren. Weitere Informationen finden Sie unter URL-Filterung.

F: Wie passt die URL-Filterung in Citrix SWG?

EIN. Die URL-Filterung nutzt die Citrix SWG-Appliance, um den Zugriff auf bestimmte Websites zu steuern. Die SWG-Appliance am Rand des Netzwerks fungiert als Proxy, um den Webverkehr abzufangen und Aktionen wie Authentifizierung, Inspektion, Zwischenspeicherung und Umleitung auszuführen. Der Filter steuert dann den Zugriff auf Websites mit der URL-Kategorisierung oder URL-Listenfunktion mit Richtliniendurchsetzung.

F: Wie oft wird die URL-Kategorisierungsdatenbank aktualisiert?

A. Wenn Sie die URL-Kategorisierungsfunktion verwenden, um den Zugriff auf eingeschränkte Websites zu steuern, müssen Sie die Kategorisierungsdatenbank regelmäßig mit den neuesten Daten aus dem cloudbasierten Vendor Service aktualisieren. Um die Datenbank zu aktualisieren, können Sie mit der Citrix SWG-GUI die URL-Filterparameter wie Stunden zwischen DB-Updates oder Time of Day to Update DB konfigurieren.

F: Welche Anwendungsfälle sind heute am besten für den URL-Filterdienst geeignet?

EIN. Im Folgenden werden einige der angestrebten Anwendungsfälle für Unternehmenskunden aufgeführt:

- URL-Filterung nach URL-Reputationsbewertung
- Kontrolle der Internetnutzung im Rahmen der Corporate Compliance für Unternehmen
- URL-Filterung mithilfe benutzerdefinierter URL-Liste

F: Gibt es ein Speicherlimit für das Caching im URL-Kategorisierungsdienst?

A. Ja. Das Speicherlimit für das Caching ist auf 10 GB festgelegt und Sie können es nur über die CLI-Schnittstelle konfigurieren.

F: Was gibt die URL-Kategorisierungsdatenbank zurück, wenn keine Kategorie mit der eingehenden Anforderung übereinstimmt?

A. Wenn die eingehende Anforderung nicht mit einer Kategorie übereinstimmt oder die URL falsch formatiert ist, markiert die Appliance die URL als Nicht kategorisiert und sendet die Anforderung an den cloudbasierten Dienst, der vom Kategorisierungsanbieter verwaltet wird. Die Appliance überwacht weiterhin das Feedback der Cloud-Abfrage und aktualisiert den Cache, sodass zukünftige Anforderungen von der Cloud-Suche profitieren können.

F: Was ist eine URL-Reputationsbewertung und wie steuern Sie den Zugriff auf bösartige Websites basierend auf der Reputationsbewertung?

A. Eine URL-Reputationsbewertung ist eine Bewertung, die Citrix SWG einer Website zuweist. Der Wert kann zwischen 1 und 4 liegen, wobei 4 eine bösartige Website und 1 eine saubere Website ist. Wenn ein Netzwerkadministrator einen Benutzer überwacht, der auf hochriskante Websites zugreift, wird der

Zugriff auf solche Websites basierend auf der URL-Reputationsbewertung und der Sicherheitsstufe gesteuert, die Sie auf der Citrix SWG-Appliance konfiguriert haben. Weitere Informationen finden Sie unter URL-Reputationsbewertung.

F: Wenn Sie Websites mit einem URL-Satz filtern, aber eine bestimmte Website falsch filtern, was ist der Prozess, um außergewöhnliche Websites zu ermöglichen?

EIN. URL-Filterung verwendet eine Responder-Richtlinie, um den Zugriff auf Websites zu steuern. Um eine bestimmte URL als Ausnahme auf die Positivliste zu setzen, erstellen Sie im SWG-Assistenten eine Patset-Richtlinie und fügen Sie die außergewöhnliche URL mit der Aktion Zulassen hinzu. Nachdem Sie die Richtlinie erstellt haben, beenden Sie den Assistenten, und führen Sie die folgenden Schritte aus:

So ändern Sie die Priorität eines Richtlinienausdrucks mit der Citrix SWG-GUI:

1. Melden Sie sich bei der **Citrix SWG**-Appliance an, und navigieren Sie zu **Secure Web Gateway > Virtual Proxy-Server**.
2. Wählen Sie auf der Detailseite einen Server aus, und klicken Sie auf **Bearbeiten**.
3. Gehen Sie auf der Seite **Virtuelle Proxyserver** zum Abschnitt **Richtlinien** und klicken Sie auf das Bleistiftsymbol, um die Details zu bearbeiten.
4. Wählen Sie die Patset-Richtlinie aus, und geben Sie auf der Seite **Richtlinienbindung** den Prioritätswert an, der niedriger ist als andere gebundene Richtlinien.
5. Klicken Sie auf **Binden** und **Fertig**.

F: Welche Vorteile bietet die Verwendung der Citrix SWG-URL-Filterfunktion?

A. URL-Filterfunktion ist einfach zu implementieren, zu konfigurieren und zu verwenden. Es bietet folgende Vorteile und ermöglicht Unternehmenskunden:

- Überwachen des Webverkehrs und der Benutzertransaktion
- Filtern Sie Malware und Internet-Bedrohungen.
- Kontrollieren Sie den unbefugten Zugriff auf bösartige Websites.
- Durchsetzen von Sicherheitsrichtlinien für Unternehmen, um den Zugriff auf eingeschränkte Daten zu kontrollieren.

F: Wie kann ich eine URL-Listenrichtlinie bearbeiten, wenn Sie eine URL-Listenfunktion zum Filtern von Websites verwenden?

A. Sie können eine URL-Listenrichtlinie über den Citrix SWG-Assistenten ändern, indem Sie die importierte Liste überschreiben oder löschen, die an die Responderrichtlinie gebunden ist.

F: Was enthalten die Metadaten, die einer URL zugeordnet sind?

A. Jedem URL in der Kategorisierungsdatenbank sind Metadaten zugeordnet. Die Metadaten enthalten Informationen zu URL-Kategorie, Kategoriegruppe und Reputationsbewertung. Wenn es sich bei

der URL beispielsweise um ein Shopping-Portal handelt, sind die Metadaten Shopping, Shopping/Retail und 1.

Verwenden Sie die folgenden Ausdrücke, um diese Werte für die eingehende URL abzurufen. Die Ausdrücke sind unten angegeben:

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

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

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

F: Welche Art von Lizenz und Abonnement benötigen Sie für die URL-Kategorisierungsfunktion?

A. Die URL-Kategorisierungsfunktion erfordert einen URL Threat Intelligence-Abonnementdienst (verfügbar für ein Jahr oder drei Jahre) mit Citrix SWG-Edition.

F: Wie kann ich die URL-Filterung konfigurieren?

A. Es gibt zwei Möglichkeiten, URL-Filterung zu konfigurieren. Sie können dies entweder über die Citrix SWG-Befehlsschnittstelle oder über den Citrix SWG-Assistenten tun. Citrix empfiehlt, dass Sie den Assistenten zum Konfigurieren von Filterrichtlinien verwenden.

F: Welche URL-Kategorien können Sie blockieren?

A. Die URL-Kategorisierungsdatenbank enthält Millionen von URLs mit Metadaten. Der Administrator kann eine Responder-Richtlinie konfigurieren, um zu entscheiden, welche URL-Kategorien gesperrt werden können und welche URL-Kategorien für den Benutzerzugriff zugelassen werden können. Informationen zur URL-Kategoriezuordnung finden SieZuordnungskategorienauf Seite.

F: Was müssen wir tun, wenn wir nicht auf Origin Server zugreifen können, die WebSocket verwenden, wieWhatsApp

Sie müssen WebSocket im Standard-HTTP-Profil aktivieren.

Geben Sie bei der CLI Folgendes ein:

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

Was ist ICAP?

ICAP steht für Internet Content Adaption Protocol.

Welche Version von Citrix SWG unterstützt ICAP?

ICAP wird in Citrix SWG Version 12.0 Build 57.x und höher unterstützt.

Welche beiden ICAP-Modi werden von Citrix SWG unterstützt?

Request modification (`REQMOD`) mode und response modification (`RESPMOD`) mode werden unterstützt.

Was ist der Standardport für ICAP?

`1344.`