



Citrix Secure Web Gateway 12.1

Machine translated content

Disclaimer

このコンテンツの正式なバージョンは英語で提供されています。Cloud Software Group ドキュメントのコンテンツの一部は、お客様の利便性のみを目的として機械翻訳されています。Cloud Software Group は機械翻訳されたコンテンツを管理していないため、誤り、不正確な情報、不適切な用語が含まれる場合があります。英語の原文から他言語への翻訳について、精度、信頼性、適合性、正確性、またはお使用の Cloud Software Group 製品またはサービスと機械翻訳されたコンテンツとの整合性に関する保証、該当するライセンス契約書またはサービス利用規約、あるいは Cloud Software Group とのその他すべての契約に基づき提供される保証、および製品またはサービスのドキュメントとの一致に関する保証は、明示的か黙示的かを問わず、かかるドキュメントの機械翻訳された範囲には適用されないものとします。機械翻訳されたコンテンツの使用に起因する損害または問題について、Cloud Software Group は責任を負わないものとします。

Contents

リリースノート	3
サポートされているハードウェアおよびソフトウェアプラットフォーム	3
ライセンス要件	4
インストール	9
Citrix ADC MPX および VPX SWG アプライアンスの使用開始	10
Citrix ADC SDX アプライアンス上の SWG インスタンスの使用を開始する	13
プロキシモード	14
SSL インターセプション	16
SSL プロファイル	17
SSL 代行受信のための SSL ポリシーインフラストラクチャ	26
SSL インターセプション証明書ストア	29
SSL エラーの自動学習中	33
ユーザー ID 管理	35
URL フィルタリング	39
URL リスト	41
URL パターンのセマンティクス	48
URL カテゴリのマッピング	48
ユースケース: カスタム URL セットを使用した URL フィルタリング	49
URL の分類	52
セキュリティ構成	64
URL レピュテーションスコア	64
ICAP を使用したリモートコンテンツ検査	66
インラインデバイスとして IPS または NGFW との統合	77

Analytics	125
ユースケース: 企業のインターネットアクセスをコンプライアンスとセキュリティで保護する	126
ユースケース: ICAP を使用したリモートマルウェア検査による企業ネットワークの安全性の確保	141
ハウツー記事	155
URL 分類ポリシーの作成方法	155
URL リストポリシーの作成方法	157
例外的な URL をホワイトリストに登録する方法	160
アダルトカテゴリーのウェブサイトをブロックする方法	161
システム	163
ネットワーク	164
AppExpert	164
SSL	165
よくあるご質問	166

リリースノート

May 1, 2021

Citrix Secure Web Gateway 製品のリリースノートは、Citrix ADC アプライアンスのメインリリースノートに記載されています。「[Citrix ADC リリースノート](#)」を参照してください。

サポートされているハードウェアおよびソフトウェアプラットフォーム

May 1, 2021

Citrix Secure Web Gateway (SWG) アプライアンスは、現在、ハードウェアアプライアンスおよび仮想アプライアンスとして使用できます。詳細仕様については、www.citrix.com で入手可能なデータシートに記載されています。マウスポインタを [製品] の上に置き、[ネットワーク] リストで [**Citrix Secure Web Gateway**] を選択します。

SWG アプライアンスをインストールする前に、正しいライセンスがあることを確認してください。高可用性セットアップの各アプライアンスには、独自のライセンスが必要です。ライセンスについては、「[ライセンス要件](#)」を参照してください。高可用性の詳細については、[高可用性の概要](#)を参照してください。

ハードウェアアプライアンス (**MPX**)

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

仮想アプライアンス (**VPX**)

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

ハードウェアアプライアンス (SDX)

SWG インスタンスは、「SDX 2-Instance Add-On Pack for Secure Web Gateway」ライセンスをインストールすることで、どの SDX プラットフォームでもプロビジョニングできます。1 つのライセンスインストールで、SDX アプライアンスに 2 つの SWG インスタンスをプロビジョニングできます。ライセンスを追加することで、アプライアンス上でさらに多くの SWG インスタンスをプロビジョニングできます。Citrix SWG インスタンスのプロビジョニングの詳細については、「[Citrix ADC インスタンスのプロビジョニング](#)」を参照してください。

ライセンス要件

May 1, 2021

ライセンスにより、Citrix Secure Web Gateway (SWG) アプライアンスの一連の機能にアクセスできます。

Citrix ライセンスフレームワークを使用すると、Citrix 製品から最大限の価値を引き出すことに集中できます。ライセンスの割り当てプロセスは非常に簡単です。SWG 構成ユーティリティ (GUI) では、ハードウェアシリアル番号 (HSN) またはライセンスアクティベーションコード (LAC) を使用してライセンスを割り当てることができます。ライセンスがローカルコンピュータにすでに存在する場合は、アプライアンスにアップロードできます。

ライセンスの返却や再割り当てなど、その他のすべての機能については、ライセンスポータルを使用する必要があります (必要に応じて、初期ライセンス割り当てにも使用できます)。ライセンスポータルの詳細については、「<http://support.citrix.com/article/CTX131110>」を参照してください。

展開の必要に応じて、ライセンスを部分的に割り当てることができます。たとえば、ライセンスファイルに 10 個のライセンスが含まれていて、現在の要件が 6 つのライセンスだけの場合は、6 つのライセンスを割り当てて、後で追加のライセンスを割り当てることができます。ライセンスファイルに存在するライセンスの合計数を超えるライセンスを割り当ててはできません。

SWG アプライアンスを使用する前に、GUI または CLI を使用して次のライセンスをインストールする必要があります。

- **Citrix Secure Web Gateway** ライセンス

- Citrix SWG プラットフォームライセンスは、MPX SWG アプライアンスを使用し、XenServer、VMware ESX、Microsoft Hyper-V、Linux-KVM などの異なるハイパーバイザーに VPX インスタンスをデプロイするための最小要件です。
- SDX プラットフォームの場合、Citrix ADC SDX アプライアンスで Citrix SWG インスタンスをプロビジョニングするには、SDX 10K 同時セッション SWG アドオンパックライセンスが少なくとも 1 つ必要です。

- **URL** 脅威インテリジェンス機能ライセンス。このライセンスは、URL フィルタリング、URL 分類、および URL レピュテーションスコア機能を使用する場合に必要です。

前提条件

ハードウェアシリアル番号またはライセンスアクティベーションコードを使用してライセンスを割り当てるには、次の手順を実行します。

- アプライアンスを介してパブリックドメインにアクセスできる必要があります。たとえば、アプライアンスは www.citrix.com にアクセスできる必要があります。ライセンス割り当てソフトウェアは、ライセンスの Citrix ライセンスポータルに内部的にアクセスします。パブリックドメインにアクセスするには、プロキシサーバーを使用するか、DNS サーバーをセットアップし、Citrix ADC アプライアンス上で NSIP アドレスまたはサブネット IP (SNIP) アドレスを構成します。
- ライセンスはハードウェアにリンクされているか、有効なライセンスアクティベーションコード (LAC) が必要です。ライセンスを購入すると、Citrix から電子メールで LAC が送信されます。

高可用性セットアップのアプライアンスのライセンス

高可用性 (HA) ペアのアプライアンスごとに、個別のライセンスを購入する必要があります。両方のアプライアンスに同じ種類のライセンスがインストールされていることを確認します。

Citrix ADC SDX アプライアンスでは、同じアプライアンス上の 2 つの SWG インスタンス間で高可用性 (HA) セットアップを構成できます。ただし、異なる Citrix ADC SDX アプライアンス上の 2 つの SWG インスタンス間で HA セットアップを構成することをお勧めします。

ライセンスの割り当てとインストール

GUI を使用して、ライセンスの割り当てとインストールを行うことができます。CLI を使用してライセンスをインストールするには、ライセンスを `/nsconfig/license/` ディレクトリにコピーする必要があります。

Citrix SWG GUI を使用してライセンスを割り当てる

1. Web ブラウザで、Citrix SWG アプライアンスの IP アドレスを入力します。
2. **[User Name]** ボックスと **[Password]** ボックスに管理者資格情報を入力します。
3. **[構成]** タブで、**[システム]** > **[ライセンス]** に移動します。
4. 詳細ウィンドウで、**[ライセンスの管理]** をクリックし、**[新しいライセンスの追加]** をクリックして、次のいずれかのオプションを選択します。
 - シリアル番号を使用します。ソフトウェアはアプライアンスのシリアル番号を内部的に取得し、この番号を使用してライセンスを表示します。
 - ライセンスアクティベーションコードを使用します。購入したライセンスのライセンスアクティベーションコード (LAC) が Citrix から電子メールで送信されます。テキストボックスにライセンスアクティブ化コードを入力します。

Citrix ADC アプライアンスでインターネット接続を構成しない場合は、プロキシサーバーを使用できます。
[プロキシサーバー経由で接続] を選択し、プロキシサーバーの IP アドレスとポートを指定します。

5. [ライセンスの取得] をクリックします。
6. ライセンスの割り当てに使用するライセンスファイルを選択します。
7. [Allocate] 列に、割り当てるライセンスの数を入力します。次に、[取得] をクリックします。
8. [Reboot] をクリックして、ライセンスを有効にします。
9. [再起動] ダイアログボックスで、[OK] をクリックします。

Citrix SWG GUI を使用してライセンスをインストールする

1. Web ブラウザで、Citrix SWG アプライアンスの IP アドレスを入力します (例: <http://192.168.100.1>)。
2. [User Name] ボックスと [Password] ボックスに管理者資格情報を入力します。
3. [構成] タブで、[システム] > [ライセンス] に移動します。
4. 詳細ウィンドウで、[ライセンスの管理] をクリックします。
5. [新しいライセンスの追加] をクリックし、[ライセンスファイルのアップロード] を選択します。
6. [Browse] をクリックします。ライセンスファイルの場所に移動し、ライセンスファイルを選択して [開く] をクリックします。
7. [Reboot] をクリックしてライセンスを適用します。
8. [再起動] ダイアログボックスで、[OK] をクリックします。

Citrix SWG CLI を使用してライセンスをインストールする

1. PuTTY などの SSH クライアントを使用して、Citrix SWG アプライアンスへの SSH 接続を開きます。
2. 管理者の資格情報を使用して、アプライアンスにログオンします。
3. シェルプロンプトに切り替えて、新しいライセンスファイルを nsconfig ディレクトリのライセンスサブディレクトリにコピーします。サブディレクトリが存在しない場合は、ファイルをコピーする前に作成してください。

例:

```
1 login: nsroot
2
3 Password: nsroot
4
5 Last login: Mon Aug 4 03:37:27 2008 from 10.102.29.9
```

```
6
7   Done
8
9   > shell
10
11  Last login: Mon Aug  4 03:51:42 from 10.103.25.64
12
13  root@ns# mkdir /nsconfig/license
14
15  root@ns# cd /nsconfig/license
16 <!--NeedCopy-->
```

新しいライセンスファイルをこのディレクトリにコピーします。

注

CLI では、ライセンスをアクティブ化するためにアプライアンスの再起動を求めるプロンプトは表示されません。**reboot-w** コマンドを実行してシステムをウォームリポートするか、**reboot** コマンドを実行してシステムを正常にリポートします。

ライセンスされた機能の確認

機能を使用する前に、ライセンスが機能をサポートしていることを確認してください。

Citrix SWG GUI を使用してライセンスされた機能を検証する

1. Web ブラウザで、Citrix SWG アプライアンスの IP アドレスを入力します (例: <http://192.168.100.1>)。
2. **[User Name]** ボックスと **[Password]** ボックスに管理者資格情報を入力します。
3. [システム]> [ライセンス] に移動します。
画面には、ライセンスされた各機能の横に緑色のチェックマークが付いています。

Citrix SWG CLI を使用してライセンスされた機能を検証する

1. PuTTY などの SSH クライアントを使用して、Citrix SWG アプライアンスへの SSH 接続を開きます。
2. 管理者の資格情報を使用して、アプライアンスにログオンします。
3. コマンドプロンプトで `sh ns license` コマンドを入力して、ライセンスでサポートされている機能を表示します。

例:

```
1 > sh license
2
3 License status:
4
```



```
5 Web Logging: NO
6
7 Surge Protection: NO
8
9 Load Balancing: YES
10
11 ...
12
13 Forward Proxy: YES
14
15 SSL Interception: YES
16
17 Model Number ID: 25000
18
19 Licensing mode: Local
20
21 完了
```

機能を有効または無効にする

Citrix Secure Web Gateway アプライアンスを初めて使用する場合、この機能を使用するには、その機能を有効にする必要があります。機能を有効にする前に設定すると、警告メッセージが表示されます。設定は保存されますが、機能が有効になるまで適用されません。

Citrix SWG GUI を使用して機能を有効にする

1. Web ブラウザで、Citrix SWG アプライアンスの IP アドレスを入力します（例: <http://192.168.100.1>）。
2. **[User Name]** ボックスと **[Password]** ボックスに管理者資格情報を入力します。
3. [システム] > [設定] > [拡張機能の設定] に移動します。
4. 有効にする機能（転送プロキシ、SSL インターセプト、URL フィルタリングなど）を選択します。

Citrix SWG CLI を使用して機能を有効にする

コマンドプロンプトで次のコマンドを入力して、機能を有効にして構成を確認します。

```
enable feature <FeatureName>
```

```
show feature
```

次に、SSL 代行受信、フォワードプロキシ、および URL フィルタリング機能を有効にする例を示します。

```
1 > enable feature forwardProxy sslinterception urlfiltering
2
3 Done
4
```

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

注

機能のライセンスキーを使用できない場合、その機能について次のエラーメッセージが表示されます。

エラー: 機能がライセンスされていません

インストール

May 1, 2021

企業を保護するための構成を開始する前に、Citrix Secure Web Gateway (SWG) アプライアンスを適切にインストールし、インターネットにアクセスできる必要があります。

ハードウェアアプライアンスのインストールと初期設定については、[SWG ハードウェアの設定](#)を参照してください。

Citrix SWG 仮想アプライアンス (VPX) は、異なる仮想化プラットフォームでサポートされています。

サポートされているハイパーバイザーおよび VPX アプライアンスの展開手順については、[Citrix ADC VPX インスタンスを展開する](#)を参照してください。

Citrix ADC MPX および VPX SWG アプライアンスの使用開始

May 1, 2021

ハードウェア (MPX) アプライアンス (MPX) またはソフトウェア (VPX) アプライアンスをインストールし、初期設定を実行すると、そのアプライアンスを Secure Web Gateway アプライアンスとして構成してトラフィックを受信できるようになります。

重要:

- OCSP チェックでは、証明書の有効性をチェックするためにインターネット接続が必要です。NSIP アドレスを使用してインターネットからアプライアンスにアクセスできない場合は、アクセス制御リスト (ACL) を追加して、NSIP アドレスからサブネット IP (SNIP) アドレスに NAT を実行します。SNIP はインターネットからアクセスできる必要があります。例:

```

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

```

- ドメイン名を解決する DNS ネームサーバーを指定します。詳しくは、「[初期構成](#)」を参照してください。
- アプライアンスの日付が NTP サーバと同期していることを確認します。日付が同期されていない場合、アプライアンスはオリジンサーバー証明書の有効期限が切れているかどうかを効果的に検証できません。

Citrix SWG アプライアンスを使用するには、次のタスクを実行する必要があります。

- エクスプリシットモードまたはトランスペアレントモードでプロキシサーバーを追加します。
- SSL インターセプションを有効にします。
 - SSL プロファイルを設定します。
 - SSL ポリシーをプロキシサーバーに追加してバインドします。
 - SSL インターセプション用の CA 証明書とキーのペアを追加およびバインドします。

注: 透過プロキシモードで構成された Citrix SWG アプライアンスは、HTTP および HTTPS プロトコルのみをインターセプトできます。telnet などの他のプロトコルをバイパスするには、プロキシ仮想サーバーに次のリッスンポリシーを追加する必要があります。

仮想サーバは、HTTP および HTTPS の着信トラフィックのみを受け入れるようになりました。

```

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

```

配置によっては、次の機能を設定する必要がある場合があります。

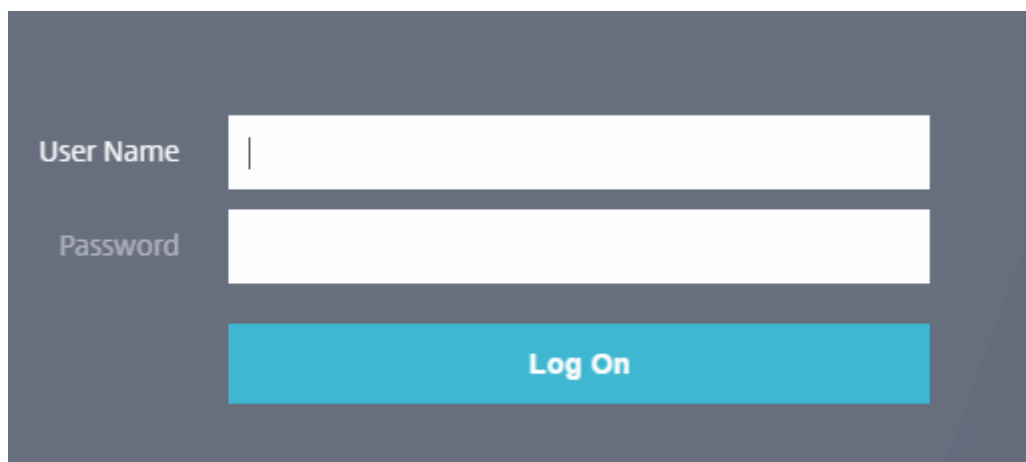
- 認証サービス（推奨） –ユーザーを認証します。認証サービスを使用しない場合、ユーザーアクティビティはクライアント IP アドレスに基づきます。
- URL フィルタリング–カテゴリ、レピュテーションスコア、URL リストによって URL をフィルタリングします。
- 分析-Citrix Application Delivery Management（ADM）でのユーザーアクティビティ、ユーザーリスクインジケータ、帯域幅消費、トランザクションの分類を表示します。

注: SWG は、一般的な HTTP および HTTPS 標準の大部分を実装し、それに続く類似製品を実装しています。この実装は、特定のブラウザを念頭に置いて行われ、最も一般的なブラウザと互換性があります。SWG は、一般的なブラウザと Google Chrome、Internet Explorer、Mozilla Firefox の最近のバージョンでテストされています。

Secure Web Gateway ウィザード

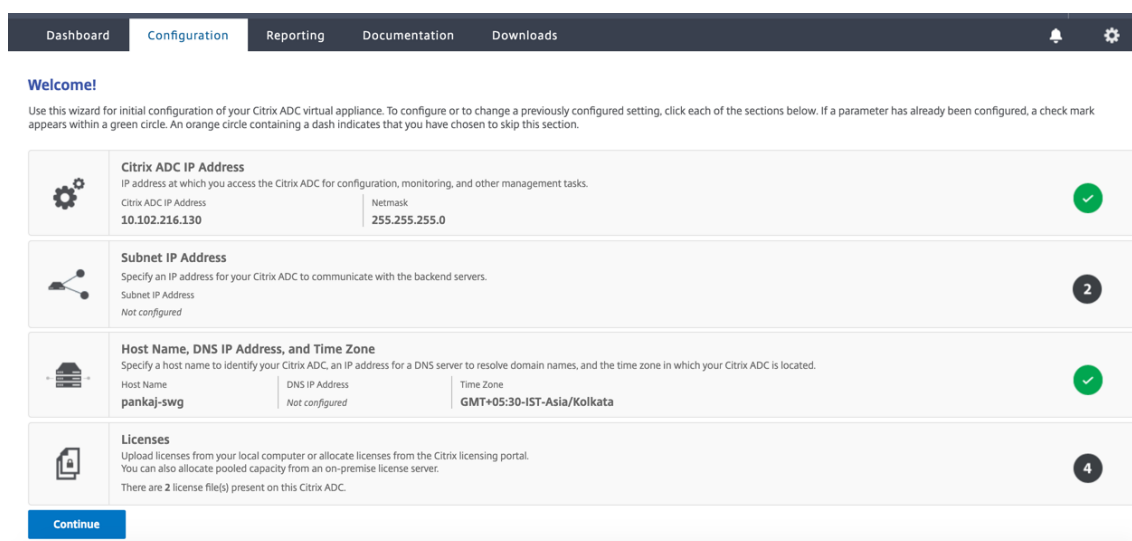
SWG ウィザードでは、Web ブラウザーを使用して SWG 展開全体を管理するためのツールを管理者に提供します。これにより、お客様が SWG サービスを迅速に起動するように導き、明確に定義された一連の手順に従って構成を簡素化できます。

1. Web ブラウザーを開き、初期設定時に指定した NSIP アドレスを入力します。初期設定の詳細については、[初期構成](#)を参照してください。
2. ユーザー名とパスワードを入力します。



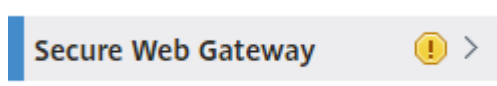
The image shows a login form with a dark gray background. On the left, the labels "User Name" and "Password" are displayed in a light gray font. To the right of each label is a white rectangular input field. Below the input fields is a prominent blue button with the text "Log On" in white. The entire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

3. サブネット IP（SNIP）アドレスを指定していない場合は、次の画面が表示されます。

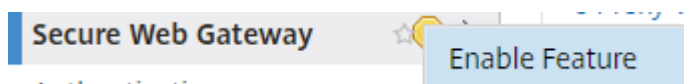


[サブネット IP アドレス] に、IP アドレスとサブネット・マスクを入力します。緑色の円で囲まれたチェックマークは、値が設定されていることを示します。

- [ホスト名]、[DNS IP アドレス]、および [タイムゾーン] で、DNS サーバーの IP アドレスを追加してドメイン名を解決し、タイムゾーンを指定します。
- [続行] をクリックします。
- (オプション) 次のように、感嘆符が表示される場合があります。



このマークは、機能が有効でないことを示します。機能を有効にするには、機能を右クリックし、[機能を有効にする] をクリックします。



- ナビゲーションペインで、[Secure Web Gateway] をクリックします。[はじめに] で、[Secure Web Gateway ウィザード] をクリックします。



- ウィザードの手順に従って、配置を設定します。

透過プロキシサーバーへのリッスンポリシーの追加

1. [**Secure Web Gateway**] > [プロキシサーバー] に移動します。透過プロキシサーバーを選択し、[**Edit**] をクリックします。
2. [基本設定] を編集し、[その他] をクリックします。
3. [リッスンプライオリティ] に 1 を入力します。
4. [リッスンポリシー式] に、次の式を入力します。

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

この式は、HTTP および HTTPS トラフィックの標準ポートを想定しています。HTTP の場合は 8080、HTTPS の場合は 8443 など、異なるポートを設定した場合は、これらのポートを反映するように式を変更します。

制限事項

SWG は、クラスタ設定、管理パーティション、および Citrix ADC FIPS アプライアンスではサポートされていません。

Citrix ADC SDX アプライアンス上の SWG インスタンスの使用を開始する

May 1, 2021

Citrix ADC SDX アプライアンスは、複数の仮想 Citrix ADC インスタンスをプロビジョニングおよび管理できるマルチテナントプラットフォームです。SDX アプライアンスは、単一の管理者がアプライアンスを構成および管理し、各ホストされたインスタンスの管理をテナントに委任できるようにすることで、クラウドコンピューティングおよびマルチテナンシーの要件に対応します。SDX アプライアンスを使用すると、アプライアンス管理者は、各テナントに次の利点を提供できます。それらは以下の通りです：

- 1つの完全なインスタンス。各インスタンスには、次の権限があります。
 - 専用の CPU およびメモリリソース
 - エンティティ用の別のスペース
 - リリースを実行し、選択したビルドへの独立性
 - ライフサイクルの独立性
- 完全に隔離されたネットワーク。特定のインスタンスに対するトラフィックは、そのインスタンスにのみ送信されます。

Citrix ADC SDX アプライアンスをまだインストールしていない場合は、アプライアンスのインストールについては、[ハードウェアの取り付け](#)を参照してください。

Citrix ADC SDX アプライアンスの初期構成を実行するには、管理サービスを使用する必要があります。詳しくは、「[管理サービスユーザーインターフェイスの使用開始](#)」を参照してください。

Citrix ADC SDX アプライアンスの Citrix SWG インスタンスは、Citrix ADC VPX インスタンスのプロビジョニングと同じ方法でプロビジョニングできます。SDX アプライアンスで SWG インスタンスをプロビジョニングするには、「SDX-10K 同時セッション SWG アドオンパック」ライセンスをインストールする必要があります。このライセンスは VPX 用の SDX インスタンスパックに似ていますが、SWG インスタンスには排他的です。Citrix ADC インスタンスの Provisioning の詳細については、「[Citrix ADC インスタンスのプロビジョニング](#)」を参照してください。

トラフィックを受信するように Citrix SWG インスタンスを設定するには、「[Citrix SWG アプライアンスの使用開始](#)」の手順に従います。

プロキシモード

May 1, 2021

Citrix Secure Web Gateway (SWG) アプライアンスは、インターネットおよび SaaS アプリケーションに接続するためのクライアントのプロキシとして機能します。プロキシとして、すべてのトラフィックを受け入れ、トラフィックのプロトコルを決定します。トラフィックが HTTP または SSL でない限り、そのまま宛先に転送されます。アプライアンスはクライアントから要求を受信すると、要求を傍受し、ユーザー認証、サイトの分類、リダイレクトなどのアクションを実行します。ポリシーを使用して、許可するトラフィックとブロックするトラフィックを決定します。

アプライアンスは、クライアントとプロキシの間で、もう一方はプロキシとオリジンサーバー間の 2 つの異なるセッションを維持します。プロキシは、ユーザーが定義したポリシーを使用して、HTTP および HTTPS トラフィックを許可またはブロックします。したがって、財務情報などの機密データをバイパスするポリシーを定義することが重要です。アプライアンスは、トラフィック管理ポリシーを作成するために、レイヤ 4 からレイヤ 7 へのトラフィック属性とユーザ ID 属性の豊富なセットを提供します。

SSL トラフィックの場合、プロキシはオリジンサーバーの証明書を確認し、サーバーとの正当な接続を確立します。次に、サーバー証明書をエミュレートし、Citrix SWG にインストールされた CA 証明書を使用して署名し、作成したサーバー証明書をクライアントに提示します。SSL セッションを正常に確立するには、信頼された証明書として CA 証明書をクライアントのブラウザに追加する必要があります。

アプライアンスは、透過および明示的なプロキシモードをサポートします。明示的なプロキシモードでは、組織が設定をクライアントのデバイスにプッシュしない限り、クライアントはブラウザで IP アドレスを指定する必要があります。このアドレスは、SWG アプライアンス上で構成されているプロキシサーバーの IP アドレスです。すべてのクライアント要求は、この IP アドレスに送信されます。明示的なプロキシの場合は、タイプ PROXY のコンテンツスイッチング仮想サーバを設定し、IP アドレスと有効なポート番号を指定する必要があります。

透過プロキシは、名前が示すように、クライアントに対して透過的です。つまり、クライアントは、プロキシサーバーが要求を仲介していることを認識していない可能性があります。SWG アプライアンスはインライン展開で構成され、すべての HTTP および HTTPS トラフィックを透過的に受け入れます。トランスペアレントプロキシの場合、IP アドレスおよびポートとしてアスタリスク (*) を使用して、タイプ PROXY のコンテンツスイッチング仮想サーバを設定する必要があります。GUI で Secure Web Gateway ウィザードを使用する場合、IP アドレスとポートを指定する必要はありません。

注

透過プロキシモードで HTTP および HTTPS 以外のプロトコルを代行受信するには、リッスンポリシーを追加し、プロキシサーバーにバインドする必要があります。

Citrix SWG CLI を使用して SSL 転送プロキシを構成する

コマンドプロンプトで、次のように入力します。

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

引数:

名前:

プロキシサーバーの名前。ASCII 英数字またはアンダースコア (_) 文字で始まり、ASCII 英数字、アンダースコア、ハッシュ (#)、ピリオド (.)、スペース、コロン (:)、アットマーク (@)、等しい (=)、およびハイフン (-) 文字のみを含める必要があります。CS 仮想サーバの作成後は変更できません。

次の要件は、CLI だけに適用されます。

名前に 1 つ以上のスペースが含まれている場合は、名前を二重引用符または一重引用符で囲みます (「my server」や「my server」など)。

これは必須の引数です。最大長: 127

IPAddress:

プロキシサーバーの IP アドレス。

port:

プロキシサーバーのポート番号。最小値:1

明示的なプロキシの例:

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

透過プロキシの例:

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


Citrix SWG GUI を使用して透過プロキシサーバーにリッスンポリシーを追加する

1. [**Secure Web Gateway**] > [プロキシサーバー] に移動します。透過プロキシサーバーを選択し、[**Edit**] をクリックします。
2. [**基本設定**] を編集し、[**その他**] をクリックします。
3. [**リッスンプライオリティ**] に **1** を入力します。
4. [**リッスンポリシー式**] に、次の式を入力します。

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

注

この式は、HTTP および HTTPS トラフィックの標準ポートを想定しています。HTTP の場合は 8080、HTTPS の場合は 8443 など、異なるポートを設定している場合は、上記の式を変更して、これらのポートを指定します。

SSL インターセプション

May 1, 2021

SSL インターセプト用に構成された Citrix Secure Web Gateway (SWG) アプライアンスは、プロキシとして機能します。SSL/TLS トラフィックを傍受および復号化し、暗号化されていない要求を検査し、管理者がコンプライアンスルールとセキュリティチェックを適用できるようにします。SSL インターセプトでは、インターセプト、ブロック、または許可するトラフィックを指定するポリシーを使用します。たとえば、銀行などの金融ウェブサイトへのトラフィックは傍受してはならないが、他のトラフィックは傍受でき、ブラックリストに登録されたサイトを特定してブロックすることができます。トラフィックを傍受する一般的なポリシーを 1 つ構成し、一部のトラフィックをバイパスするより具体的なポリシーを構成することをお勧めします。

クライアントと Citrix SWG プロキシは、HTTPS/TLS ハンドシェイクを確立します。SWG プロキシは、サーバーと別の HTTPS/TLS ハンドシェイクを確立し、サーバー証明書を受信します。プロキシは、クライアントに代わってサーバー証明書を検証し、オンライン証明書状態プロトコル (OCSP) を使用してサーバー証明書の有効性をチェックします。サーバー証明書を再生成し、アプライアンスにインストールされている CA 証明書のキーを使用して署名し、クライアントに提示します。したがって、クライアントと Citrix ADC アプライアンスの間で 1 つの証明書が使用され、アプライアンスとバックエンドサーバー間で別の証明書が使用されます。

重要

再生成されたサーバー証明書がクライアントによって信頼されるように、サーバー証明書の署名に使用される CA 証明書は、すべてのクライアントデバイスにプレインストールする必要があります。

インターセプトされた HTTPS トラフィックの場合、SWG プロキシサーバはアウトバウンドトラフィックを復号化し、クリアテキスト HTTP 要求にアクセスし、任意のレイヤ 7 アプリケーションを使用してトラフィックを処理できます。たとえば、プレーンテキスト URL を調べて、企業ポリシーと URL レピュテーションに基づいてアクセスを許可またはブロックします。ポリシーの決定がオリジンサーバへのアクセスを許可する場合、プロキシサーバは、再暗号化された要求を宛先サービス (オリジンサーバ上の) に転送します。プロキシは、オリジンサーバからの応答を復号化し、クリアテキストの HTTP 応答にアクセスし、オプションで任意のポリシーを応答に適用します。プロキシは応答を再暗号化し、クライアントに転送します。ポリシーがオリジンサーバへの要求をブロックする場合、プロキシは HTTP 403 などのエラー応答をクライアントに送信できます。

SSL インターセプトを実行するには、以前に構成したプロキシサーバに加えて、SWG アプライアンス上で次の設定を行う必要があります。

- SSL プロファイル
- SSL ポリシー
- CA 証明書ストア
- SSL エラーの自動学習とキャッシュ

SSL プロファイル

May 1, 2021

SSL プロファイルは、暗号やプロトコルなどの SSL 設定の集まりです。プロファイルは、異なるサーバに共通の設定がある場合に役立ちます。各サーバに同じ設定を指定する代わりに、プロファイルを作成し、プロファイルに設定を指定し、プロファイルを別のサーバにバインドできます。カスタムフロントエンド SSL プロファイルが作成されない場合、既定のフロントエンドプロファイルは、クライアント側のエンティティにバインドされます。このプロファイルを使用すると、クライアント側の接続を管理するための設定を構成できます。SSL インターセプションの場合は、SSL プロファイルを作成し、プロファイルで SSL インターセプション (SSLi) を有効にする必要があります。デフォルトの暗号グループはこのプロファイルにバインドされますが、展開に合わせてさらに多くの暗号を設定できます。SSLi CA 証明書をこのプロファイルにバインドし、プロファイルをプロキシサーバにバインドする必要があります。SSL インターセプションの場合、プロファイルの重要なパラメーターは、オリジナル・サーバ証明書の OCSP ステータスの確認、オリジナル・サーバが再ネゴシエーションを要求した場合のクライアントの再ネゴシエーションのトリガー、フロントエンドの SSL セッションを再利用する前にオリジナル・サーバ証明書の検証に使用されるパラメーターです。オリジンサーバと通信するときは、デフォルトのバックエンドプロファイルを使用する必要があります。デフォルトのバックエンドプロファイルで、暗号スイートなどのサーバ側パラメータを設定します。カスタムバックエンドプロファイルはサポートされません。

最も一般的に使用される SSL 設定の例については、このセクションの最後の「サンプルプロファイル」を参照してください。

暗号/プロトコルのサポートは、内部ネットワークと外部ネットワークによって異なります。次の表では、ユーザーと SWG アプライアンス間の接続は内部ネットワークです。外部ネットワークは、アプライアンスとインターネットの

間にあります。

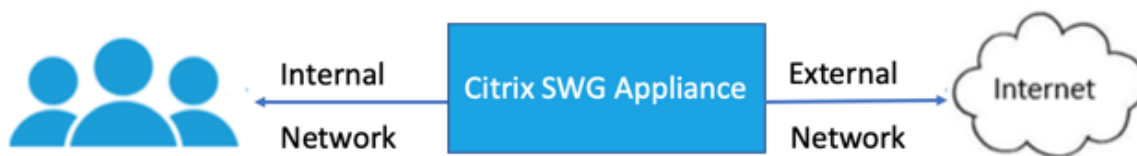


表 1: 内部ネットワークの暗号/プロトコルサポートマトリックス

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

表 2: 外部ネットワークの暗号/プロトコルサポートマトリックス

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

* **sh hardware** (show hardware) コマンドを使用して、アプライアンスに N3 チップがあるかどうかを確認します。

例:

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

Citrix SWG CLI を使用して SSL プロファイルを追加し、SSL インターセプトを有効にする

コマンドプロンプトで、次のように入力します。

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

引数:

sslInterception:

SSL セッションのインターセプションを有効または無効にします。

設定可能な値: ENABLED, DISABLED

デフォルト値: 無効

ssliReneg:

オリジンサーバーから再ネゴシエーション要求を受信したときのクライアント再ネゴシエーションのトリガーを有効または無効にします。

設定可能な値: ENABLED, DISABLED

デフォルト値:ENABLED

ssliOCSPCheck:

オリジンサーバー証明書の OCSP チェックを有効または無効にします。

設定可能な値: ENABLED, DISABLED

デフォルト値:ENABLED

サーバごとの最大サイズ:

動的オリジンサーバごとにキャッシュされる SSL セッションの最大数。クライアント hello メッセージでクライアントから受信した SNI 拡張ごとに、一意の SSL セッションが作成されます。一致するセッションは、サーバーセッションの再利用に使用されます。

デフォルト値:10

最小値:1

最大値:1000

例:

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

```
36
37     PUSH encryption trigger timeout:           1 ms
38
39     SNI: DISABLED
40
41     OCSP Stapling: DISABLED
42
43     Strict Host Header check for SNI enabled SSL sessions:
44         NO
45
46     Push flag:           0x0 (Auto)
47
48     SSL quantum size:           8 kB
49
50     Encryption trigger timeout           100 mS
51
52     Encryption trigger packet count:           45
53
54     Subject/Issuer Name Insertion Format: Unicode
55
56     SSL Interception: ENABLED
57
58     SSL Interception OCSP Check: ENABLED
59
60     SSL Interception End to End Renegotiation: ENABLED
61
62     SSL Interception Server Cert Verification for Client
63         Reuse: ENABLED
64
65     SSL Interception Maximum Reuse Sessions per Server: 10
66
67     Session Ticket: DISABLED           Session Ticket
68         Lifetime: 300 (secs)
69
70     HSTS: DISABLED
71
72     HSTS IncludeSubDomains: NO
73
74     HSTS Max-Age: 0
75
76     ECC Curve: P_256, P_384, P_224, P_521
77
78     1) Cipher Name: DEFAULT Priority :1
79         Description: Predefined Cipher Alias
80 Done
81 <!--NeedCopy-->
```

Citrix SWG CLI を使用して **SSL** インターセプト **CA** 証明書を **SSL** プロフルにバインドする

コマンドプロンプトで、次のように入力します。

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

例:

```
1 bind ssl profile swg_ssl_profile -ssliCACertkey swg_ca_cert
2
3 Done
4
5 sh ssl profile swg_ssl_profile
6
7 1)          Name: swg_ssl_profile (Front-End)
8
9             SSLv3: DISABLED                TLSv1.0: ENABLED  TLSv1
             .1: ENABLED  TLSv1.2: ENABLED
10
11            Client Auth: DISABLED
12
13            Use only bound CA certificates: DISABLED
14
15            Strict CA checks:                                NO
16
17            Session Reuse: ENABLED
             Timeout: 120 seconds
18
19            DH: DISABLED
20
21            DH Private-Key Exponent Size Limit: DISABLED
             Ephemeral RSA: ENABLED
             Refresh Count: 0
22
23            Deny SSL Renegotiation
             ALL
24
25            Non FIPS Ciphers: DISABLED
26
27            Cipher Redirect: DISABLED
28
29            SSL Redirect: DISABLED
30
31            Send Close-Notify: YES
32
33            Strict Sig-Digest Check: DISABLED
34
35            Push Encryption Trigger: Always
36
37            PUSH encryption trigger timeout:                1 ms
38
39            SNI: DISABLED
40
41            OCSP Stapling: DISABLED
```

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

Citrix SWG GUI を使用して **SSL** インターセプト **CA** 証明書を **SSL** プロフルにバインドする

1. [システム]>[プロファイル]>[**SSL** プロファイル]に移動します。
2. [追加] をクリックします。
3. プロファイルの名前を指定します。

4. **SSL** セッションインターセプションを有効にします。
5. **[OK]** をクリックします。
6. **[詳細設定]** で、**[証明書キー]** をクリックします。
7. プロファイルにバインドする **SSLi CA 証明書キー**を指定します。
8. **[選択]** をクリックし、**[バインド]** をクリックします。
9. オプションで、展開に合わせて暗号を設定します。
 - **編集**アイコンをクリックし、**[追加]** をクリックします。
 - 1つ以上の暗号グループを選択し、右矢印をクリックします。
 - **[OK]** をクリックします。
10. **[完了]** をクリックします。

Citrix SWG GUI を使用して **SSL** プロファイルをプロキシサーバーにバインドする

1. **[Secure Web Gateway]** > **[プロキシサーバー]** に移動し、新しいサーバーを追加するか、変更するサーバーを選択します。
2. **[SSL プロファイル]** で、**[編集]** アイコンをクリックします。
3. **[SSL プロファイル]** リストで、前に作成した SSL プロファイルを選択します。
4. **[OK]** をクリックします。
5. **[完了]** をクリックします。

サンプルプロファイル:

```
1 Name: swg_ssl_profile (Front-End)
2
3         SSLv3: DISABLED           TLSv1.0: ENABLED  TLSv1
         .1: ENABLED  TLSv1.2: ENABLED
4
5         Client Auth: DISABLED
6
7         Use only bound CA certificates: DISABLED
8
9         Strict CA checks:                               NO
10
11        Session Reuse: ENABLED
         Timeout: 120 seconds
12
13        DH: DISABLED
14
15        DH Private-Key Exponent Size Limit: DISABLED
         Ephemeral RSA: ENABLED
         Refresh Count: 0
16
```

17	Deny SSL Renegotiation	
	ALL	
18		
19	Non FIPS Ciphers: DISABLED	
20		
21	Cipher Redirect: DISABLED	
22		
23	SSL Redirect: DISABLED	
24		
25	Send Close-Notify: YES	
26		
27	Strict Sig-Digest Check: DISABLED	
28		
29	Push Encryption Trigger: Always	
30		
31	PUSH encryption trigger timeout:	1 ms
32		
33	SNI: DISABLED	
34		
35	OCSP Stapling: DISABLED	
36		
37	Strict Host Header check for SNI enabled SSL sessions:	
	NO	
38		
39	Push flag:	0x0 (Auto)
40		
41	SSL quantum size:	8 kB
42		
43	Encryption trigger timeout	100 mS
44		
45	Encryption trigger packet count:	45
46		
47	Subject/Issuer Name Insertion Format: Unicode	
48		
49	SSL Interception: ENABLED	
50		
51	SSL Interception OCSP Check: ENABLED	
52		
53	SSL Interception End to End Renegotiation: ENABLED	
54		
55	SSL Interception Maximum Reuse Sessions per Server:	10
56		
57	Session Ticket: DISABLED	Session Ticket
	Lifetime: 300 (secs)	
58		
59	HSTS: DISABLED	
60		
61	HSTS IncludeSubDomains: NO	
62		
63	HSTS Max-Age: 0	
64		
65	ECC Curve: P_256, P_384, P_224, P_521	
66		

```
67 1)          Cipher Name: DEFAULT Priority :1
68
69          Description: Predefined Cipher Alias
70
71 1)          SSL Interception CA CertKey Name: swg_ca_cert
72 <!--NeedCopy-->
```

SSL 代行受信のための SSL ポリシーインフラストラクチャ

May 1, 2021

ポリシーは、着信トラフィックに対するフィルタのように動作します。Citrix Secure Web Gateway (SWG) アプライアンスのポリシーは、プロキシ接続と要求の管理方法を定義するのに役立ちます。処理は、そのポリシーに対して設定されているアクションに基づきます。つまり、接続要求のデータはポリシーで指定された規則と比較され、規則に一致する接続にアクションが適用されます (式)。ポリシーのアクションを定義し、ポリシーを作成したら、プロキシサーバーにバインドして、そのプロキシサーバーを通過するトラフィックに適用されます。

SSL インターセプションの SSL ポリシーは、着信トラフィックを評価し、ルール (式) に一致する要求に事前定義されたアクションを適用します。接続の代行受信、バイパス、またはリセットは、定義された SSL ポリシーに基づいて決定されます。ポリシーに対して、INTERCEPT、BYPASS、または RESET の 3 つのアクションのいずれかを設定できます。ポリシーの作成時にアクションを指定します。ポリシーを有効にするには、アプライアンスのプロキシサーバーにポリシーをバインドする必要があります。ポリシーが SSL インターセプションを対象とするように指定するには、プロキシサーバーにポリシーをバインドするときに、タイプ (バインドポイント) を INTERCEPT_REQ として指定する必要があります。ポリシーのバインドを解除するときは、タイプを INTERCEPT_REQ として指定する必要があります。

注:

プロキシサーバーは、ポリシーを指定した場合にだけ、インターセプトを決定できます。

トラフィックインターセプションは、任意の SSL ハンドシェイク属性に基づいて行うことができます。最も一般的に使用されるのは SSL ドメインです。SSL ドメインは通常、SSL ハンドシェイクの属性によって示されます。これは、SSL Client Hello メッセージから抽出されたサーバー名インジケータ値 (存在する場合)、または元のサーバー証明書から抽出されたサーバー別名 (SAN) 値になります。Citrix SWG の SSLi ポリシーでは、DETECTED_DOMAIN という特別な属性が表示されます。これにより、お客様はオリジンサーバー証明書からの SSL ドメインに基づいてインターセプトポリシーを簡単に作成することができます。顧客は、ドメイン名を文字列、URL リスト (URL セットまたは *patset*)、またはドメインから派生した URL カテゴリと照合できます。

Citrix SWG CLI を使用して SSL ポリシーを作成する

コマンドプロンプトで、次のように入力します。

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

例:

次の例は、`detected_domain` 属性を使用してドメイン名をチェックする式を持つポリシーの例です。

XYZBANK などの金融機関へのトラフィックを傍受しない

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

ユーザーが企業ネットワークから YouTube に接続することを許可しないでください。

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

すべてのユーザトラフィックをインターセプトします。

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

お客様が `detected_domain` を使用したくない場合は、任意の SSL ハンドシェイク属性を使用してドメインを抽出および推測できます。

たとえば、ドメイン名が、クライアントの hello メッセージの SNI 拡張に見つかりません。ドメイン名は、オリジンサーバー証明書から取得する必要があります。次の例は、オリジンサーバー証明書のサブジェクト名でドメイン名をチェックする式を持つポリシーの例です。

任意の Yahoo ドメインへのすべてのユーザトラフィックを傍受します。

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

カテゴリ「ショッピング/小売」のすべてのユーザトラフィックをインターセプトします。

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

未分類 URL へのすべてのユーザトラフィックをインターセプトします。

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

次の例は、URL セットのエントリに対してドメインを照合するポリシーの例です。

SNI のドメイン名が URL セット「top100」のエントリと一致する場合、すべてのユーザートラフィックをインターセプトします。

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

オリジンサーバー証明書が URL セット「top100」のエントリと一致する場合、ドメイン名のすべてのユーザートラフィックをインターセプトします。

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

SWG GUI を使用してプロキシサーバーへの SSL ポリシーを作成する

1. [**Secure Web Gateway**] > [**SSL**] > [**ポリシー**] に移動します。
2. [**SSL ポリシー**] タブで、[**追加**] をクリックし、次のパラメータを指定します。
 - ポリシー名
 - ポリシーアクション: 代行受信、バイパス、またはリセットから選択します。
 - 式
3. [**作成**] をクリックします。

SWG CLI を使用して SSL ポリシーをプロキシサーバーにバインドする

コマンドプロンプトで、次のように入力します。

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

例:

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

Citrix SWG GUI を使用して SSL ポリシーをプロキシサーバーにバインドする

1. [**Secure Web Gateway**] > [**プロキシ仮想サーバー**] に移動します。
2. 仮想サーバを選択し、[**Edit**] をクリックします。
3. [**詳細設定**] で、[**SSL ポリシー**] をクリックします。
4. [**SSL ポリシー**] ボックスの内側をクリックします。

5. 「ポリシーの選択」で、バインドするポリシーを選択します。
6. 「タイプ」で「**INTERCEPT_REQ**」を選択します。
7. [バインド]をクリックし、[OK]をクリックします。

コマンドラインを使用して **SSL** ポリシーをプロキシサーバーにバインド解除する

コマンドプロンプトで、次のように入力します。

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

SWG の SSL ポリシーで使用される SSL 式

式	説明
<code>CLIENT.SSL.CLIENT_HELLO.SNI.*</code>	SNI 拡張を文字列形式で返します。文字列を評価して、指定したテキストが含まれているかどうかを確認します。 例： <code>client.ssl.client_hello.sni.contains("xyz.com")</code>
<code>CLIENT.SSL.ORIGIN_SERVER_CERT.*</code>	バックエンドサーバーから受け取った証明書を、文字列形式で返します。文字列を評価して、指定したテキストが含まれているかどうかを確認します。例： <code>client.ssl.origin_server_cert.subject.contains("xyz.com")</code>
<code>CLIENT.SSL.DETECTED_DOMAIN.*</code>	SNI 拡張またはオリジンサーバー証明書からドメインを文字列形式で返します。文字列を評価して、指定したテキストが含まれているかどうかを確認します。例： <code>client.ssl.detected_domain.contains("xyz.com")</code>

SSL インターセプション証明書ストア

May 1, 2021

SSL 証明書は、SSL トランザクションの不可欠な部分であり、会社 (ドメイン) または個人を識別するデジタルデータフォーム (X509) です。SSL 証明書は、認証局 (CA) によって発行されます。CA は、プライベートまたはパブリック

クにできます。Verisign などのパブリック CA によって発行された証明書は、SSL トランザクションを実行するアプリケーションによって信頼されます。これらのアプリケーションは、信頼する CA の一覧を維持します。

Citrix Secure Web Gateway (SWG) アプライアンスは、フォワードプロキシとして、クライアントとサーバー間のトラフィックの暗号化と復号化を実行します。これは、クライアント（ユーザー）のサーバーとして、およびサーバーのクライアントとして機能します。アプライアンスは HTTPS トラフィックを処理する前に、不正なトランザクションを防ぐために、サーバーの ID を検証する必要があります。したがって、オリジンサーバーのクライアントとして、アプライアンスはオリジンサーバー証明書を受け入れる前にオリジンサーバー証明書を確認する必要があります。サーバーの証明書を確認するには、サーバー証明書の署名と発行に使用されるすべての証明書（ルート証明書と中間証明書など）がアプライアンスに存在する必要があります。デフォルトの CA 証明書セットは、アプライアンス上にプレインストールされています。Citrix SWG は、これらの証明書を使用して、ほぼすべての共通オリジンサーバー証明書を検証できます。この既定のセットは変更できません。ただし、展開でさらに多くの CA 証明書が必要な場合は、そのような証明書のバンドルを作成し、そのバンドルをアプライアンスにインポートできます。バンドルには、単一の証明書を含めることもできます。

証明書バンドルをアプライアンスにインポートすると、アプライアンスはリモートの場所からバンドルをダウンロードし、バンドルに証明書のみが含まれていることを確認した後、アプライアンスにインストールします。証明書バンドルを使用してサーバ証明書を検証するには、事前に証明書バンドルを適用する必要があります。また、証明書バンドルをエクスポートして編集したり、オフラインの場所にバックアップとして保存したりすることもできます。

Citrix SWG CLI を使用してアプライアンスに **CA** 証明書バンドルをインポートして適用する

コマンドプロンプトで、次のように入力します。

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

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

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

要点:

名前:

インポートした証明書バンドルに割り当てる名前。ASCII 英数字またはアンダースコア (_) 文字で始まり、ASCII 英数字、アンダースコア、ハッシュ (#)、ピリオド (.)、スペース、コロン (:)、アットマーク (@)、等しい (=)、およびハイフン (-) 文字のみを含める必要があります。次の要件は、CLI だけに適用されます。

名前に 1 つ以上のスペースが含まれる場合は、名前を二重引用符または一重引用符で囲みます (「 my file 」 や 「 my file 」 など)。

Maximum Length: 31

src:

インポートまたはエクスポートする証明書バンドルへのプロトコル、ホスト、およびパス（ファイル名を含む）を指定する URL。たとえば、`http://www.example.com/cert_bundle_file`などです。

注: インポートするオブジェクトがアクセスにクライアント証明書認証を必要とする HTTPS サーバー上にある場合、インポートは失敗します。

最大の長さ:2047

例:

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

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

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

Citrix SWG GUI を使用してアプライアンスに **CA** 証明書バンドルをインポートして適用する

1. [**Secure Web Gateway**] > [はじめに] > [証明書バンドル] に移動します。
2. 次のいずれかを行います:
 - リストから証明書バンドルを選択します。
 - 新しい証明書バンドルを追加するには、「+」をクリックし、名前とソース URL を指定します。[**OK**] をクリックします。
3. [**OK**] をクリックします。

CLI を使用して **CA** 証明書バンドルをアプライアンスから削除する

コマンドプロンプトで、次のように入力します。

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

例:


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

Citrix SWG CLI を使用してアプライアンスから CA 証明書バンドルをエクスポートする

コマンドプロンプトで、次のように入力します。

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

要点:

名前:

インポートした証明書バンドルに割り当てる名前。ASCII 英数字またはアンダースコア (_) 文字で始まり、ASCII 英数字、アンダースコア、ハッシュ (#)、ピリオド (.)、スペース、コロン (:)、アットマーク (@)、等しい (=)、およびハイフン (-) 文字のみを含める必要があります。次の要件は、CLI だけに適用されます。

名前に 1 つ以上のスペースが含まれる場合は、名前を二重引用符または一重引用符で囲みます (「my file」や「my file」など)。

Maximum Length: 31

src:

インポートまたはエクスポートする証明書バンドルへのプロトコル、ホスト、およびパス (ファイル名を含む) を指定する URL。たとえば、http://www.example.com/cert_bundle_fileなどです。

注: インポートするオブジェクトがアクセスにクライアント証明書認証を必要とする HTTPS サーバー上にある場合、インポートは失敗します。

最大の長さ:2047

例:

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

Mozilla CA 証明書ストアから CA 証明書バンドルをインポート、適用、検証する

コマンドプロンプトで、次のように入力します。

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

バンドルを適用するには、次のように入力します。

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

使用中の証明書バンドルを確認するには、次のように入力します。

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

制限事項

証明書バンドルは、クラスタ設定またはパーティション化されたアプライアンスではサポートされません。

SSL エラーの自動学習中

May 1, 2021

学習モードがオンの場合、Citrix SWG アプライアンスは SSL バイパスリストにドメインを追加します。ラーニングモードは、クライアントまたはオリジナルサーバから受信した SSL アラートメッセージに基づいています。つまり、学習は、アラートメッセージを送信するクライアントまたはサーバによって異なります。アラートメッセージが送信されない場合、ラーニングは行われません。アプライアンスは、次のいずれかの条件が満たされているかどうかを学習します。

1. クライアント証明書の要求がサーバから受信されます。
2. ハンドシェイクの一環として、次のいずれかのアラートが受信されます。
 - BAD_CERTIFICATE
 - UNSUPPORTED_CERTIFICATE
 - CERTIFICATE_REVOKED
 - CERTIFICATE_EXPIRED
 - CERTIFICATE_UNKNOWN
 - UNKNOWN_CA (クライアントがピン接続を使用している場合、サーバ証明書を受信すると、この警告メッセージを送信します)。
 - HANDSHAKE_FAILURE

学習を有効にするには、エラーキャッシュを有効にし、このために予約されたメモリを指定する必要があります。

Citrix SWG GUI を使用して学習を有効にする

1. [**Secure Web Gateway**] > [**SSL**] に移動します。

2. [設定] で、[**SSL** 詳細設定の変更] をクリックします。
3. 「**SSL** インターセプション」で、「**SSL** インターセプションエラー・キャッシュ」を選択します。
4. 「**SSL** インターセプション最大エラーキャッシュメモリ」で、予約するメモリ（バイト単位）を指定します。

5. [OK] をクリックします。

Citrix SWG CLI を使用して学習を有効にする

コマンドプロンプトで次のように入力します。

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

引数:

ssliErrorCache:

- 1 ダイナミックラーニングを有効または無効にし、学習した情報をキャッシュして、要求の代行受信またはバイパスに関するその後の決定を行います。有効にすると、アプライアンスはキャッシュ検索を実行して、要求をバイパスするかどうかを決定します。
- 2
- 3 指定可能な値: `ENABLED, DISABLED`
- 4
- 5 デフォルト値: `DISABLED`

ssliMaxErrorCacheMem:

- 1 学習したデータのキャッシュに使用できる最大メモリをバイト単位で指定します。このメモリは LRU キャッシュとして使用されるため、設定されたメモリ制限を使い果たした後、古いエントリが新しいエントリに置き換えられます。値 0 を指定すると、自動的に制限が決定されます。
- 2
- 3 デフォルト値: 0
- 4
- 5 最小値: 0
- 6
- 7 最大値: 4294967294

ユーザー ID 管理

May 1, 2021

セキュリティ侵害が増え、モバイルデバイスの人気が高まるにつれて、外部インターネットの使用が企業ポリシーに準拠し、許可されたユーザーのみが企業の従業員によってプロビジョニングされた外部リソースにアクセスできるようにする必要性が強調されています。ID 管理では、個人またはデバイスの ID を検証することによって、これを実現できます。これは、個人が取ることができるタスクや個人が参照できるファイルを決定するものではありません。

Secure Web Gateway (SWG) 展開では、インターネットへのアクセスを許可する前にユーザーを識別します。ユーザーからのすべての要求と応答が検査されます。ユーザーアクティビティがログに記録され、レポート用に Citrix Application Delivery Management (ADM) にレコードがエクスポートされます。Citrix ADM では、ユーザーのアクティビティ、トランザクション、帯域幅消費に関する統計を表示できます。

デフォルトでは、ユーザーの IP アドレスのみが保存されますが、ユーザーの詳細を記録するように Citrix SWG アプライアンスを構成し、この ID 情報を使用して特定のユーザーに対してより豊富なインターネット使用ポリシーを作成できます。

Citrix ADC アプライアンスは、明示的なプロキシ構成に対して次の認証モードをサポートしています。

- **ライトウェイトディレクトリアクセスプロトコル (LDAP)**。外部 LDAP 認証サーバーを介してユーザーを認証します。詳しくは、「[LDAP 認証ポリシー](#)」を参照してください。
- **RADIUS**。外部 RADIUS サーバーを介してユーザーを認証します。詳しくは、「[RADIUS 認証ポリシー](#)」を参照してください。
- **TACACS+**。外部ターミナルアクセスコントローラアクセスコントロールシステム (TACACS) 認証サーバーを介してユーザーを認証します。詳しくは、「[認証ポリシー](#)」を参照してください。
- **Negotiate**。Kerberos 認証サーバーを使用してユーザーを認証します。Kerberos 認証にエラーがある場合、アプライアンスは NTLM 認証を使用します。詳しくは、「[認証ポリシーのネゴシエート](#)」を参照してください。

透過プロキシの場合、現在 IP ベースの LDAP 認証だけがサポートされています。クライアント要求を受信すると、プロキシはアクティブディレクトリ内のクライアント IP アドレスのエントリをチェックすることによってユーザーを認証し、ユーザー IP アドレスに基づいてセッションを作成します。ただし、LDAP アクションで `ssoNameAttribute` を構成すると、IP アドレスの代わりにユーザー名を使用してセッションが作成されます。トランスペアレントプロキシ設定では、従来のポリシーは認証ではサポートされません。

注

明示的なプロキシの場合は、LDAP ログイン名を `sAMAccountName` に設定する必要があります。透過プロキシの場合、LDAP ログイン名を `networkAddress` に設定し、`attribute1` を `sAMAccountName` に設定する必要があります。

明示的なプロキシの例:

```

1 add authentication ldapAction swg-auth-action-explicit -serverIP
  10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
  CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
  freesd123$ -ldapLoginName sAMAccountName
2 <!--NeedCopy-->

```

透過プロキシの例:

```

1 add authentication ldapAction swg-auth-action-explicit -serverIP
  10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
  CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
  freesd123$ -ldapLoginName networkAddress -authentication disable -
  Attribute1 sAMAccountName
2 <!--NeedCopy-->

```

Citrix SWG CLI を使用してユーザー認証を設定する

コマンドプロンプトで次のように入力します。

```

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

```

引数:

仮想サーバ名:

ポリシーをバインドする認証仮想サーバの名前。

最大長: 127

serviceType:

認証仮想サーバのプロトコルタイプ。Always SSL.

指定可能な値:SSL

デフォルト値: SSL

アクション名:

新しい LDAP アクションの名前。文字、数字、またはアンダースコア文字 (_) で始まり、文字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、スペース ()、アットマーク (@)、等しい (=)、コロン (:)、およびアンダースコア文字のみを含める必要があります。LDAP アクションが追加された後は変更できません。次の要件は、CLI だけに適用されます。

名前に 1 つ以上のスペースが含まれる場合は、名前を二重引用符または一重引用符で囲みます (「認証アクション」や「認証アクション」など)。

最大長: 127

serverIP:

LDAP サーバに割り当てられた IP アドレス。

ldapBase:

LDAP 検索を開始するベース (ノード)。LDAP サーバがローカルで実行されている場合、base のデフォルト値は dc=netScaler、dc=com です。最大長: 127

ldapBindDn:

LDAP サーバーへのバインドに使用される完全識別名 (DN)。

デフォルト: `cn=Manager,dc=netScaler,dc=com`

最大長: 127

ldapBindDnPassword:

LDAP サーバへのバインドに使用するパスワード。

最大長: 127

ldapLoginName:

LDAP ログイン名属性。Citrix ADC アプライアンスは、LDAP ログイン名を使用して、外部 LDAP サーバーまたは Active Directory のクエリを実行します。最大長: 127

ポリシー名:

事前認証ポリシーの名前。文字、数字、またはアンダースコア文字 (_) で始まり、文字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、スペース ()、アットマーク (@)、等しい (=)、コロン (:)、およびアンダースコア文字のみを含める必要があります。認証ポリシーの作成後は変更できません。次の要件は、CLI だけに適用されます。

名前に 1 つ以上のスペースが含まれる場合は、名前を二重引用符または一重引用符で囲みます (「認証ポリシー」や「認証ポリシー」など)。

最大長: 127

rule を次のように設定します。

AUTHENTICATION サーバーでユーザーを認証するかどうかを決定するためにポリシーが使用する規則の名前、またはデフォルトの構文式。

最大長さ:1499

action。

ポリシーが一致した場合に実行される認証アクションの名前。

最大長: 127

priority:

ポリシーのプライオリティを指定する正の整数。数値が小さいほど、プライオリティが高くなります。ポリシーは優先度の順に評価され、要求に一致する最初のポリシーが適用されます。認証仮想サーバにバインドされたポリシーのリスト内で一意である必要があります。

最小値:0

最大値:4294967295

例:

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

Citrix SWG CLI を使用してユーザー名ログを有効にする

コマンドプロンプトで、次のように入力します。

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

引数:

AAAUserName

AppFlow AAA ユーザー名のロギングを有効にします。

設定可能な値: **ENABLED**, **DISABLED**

デフォルト値: **DISABLED**

例:

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

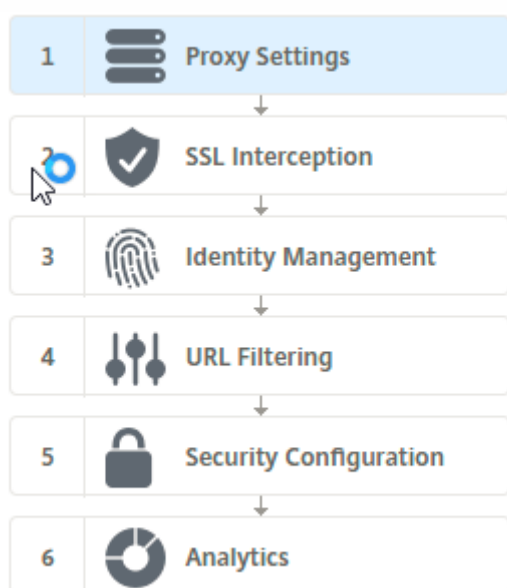
URL フィルタリング

May 1, 2021

URL フィルタリングは、URL に含まれる情報を使用して、Web サイトのポリシーベースの制御を提供します。この機能は、ネットワーク管理者がネットワーク上の悪意のある Web サイトへのユーザーアクセスを監視および制御するのに役立ちます。

導入

新しいユーザーで URL フィルタリングを構成する場合は、最初の SWG セットアップを完了する必要があります。URL フィルタリングを開始するには、まず Citrix SWG ウィザードにログオンする必要があります。ウィザードでは、URL フィルタリングポリシーを適用する前に、一連の構成手順を実行します。



注

開始する前に、有効な URL 脅威インテリジェンス機能ライセンスがアプライアンスにインストールされていることを確認してください。試用版を使用している場合は、SWG アプライアンスでこの機能を引き続き使用するには、有効なライセンスを購入してください。

SWG ウィザードにログインする

Citrix SWG ウィザードでは、一連の簡単な構成タスクを実行でき、右側のペインには対応するフローシーケンスが表示されます。このウィザードを使用して、URL フィルタリングポリシーを URL リストまたは定義済みのカテゴリの一覧に適用できます。

手順 1: プロキシ設定を構成する

まず、クライアントが SWG ゲートウェイにアクセスするためのプロキシサーバーを設定する必要があります。このサーバーは SSL タイプであり、明示的または透過的模式で動作します。プロキシサーバーの設定の詳細については、[プロキシモード](#)を参照してください。

ステップ 2: SSL インターセプションを設定する

プロキシサーバーを構成したら、Citrix SWG アプライアンスで暗号化されたトラフィックをインターセプトするように SSL インターセプトプロキシを構成する必要があります。URL フィルタリングの場合、SSL プロキシはトラフィックを傍受し、ブラックリストに登録された URL をブロックしますが、他のすべてのトラフィックはバイパスできます。SSL インターセプションの設定の詳細については、[SSL インターセプション](#)を参照してください。

ステップ 3: ID 管理を構成する

ユーザーは、エンタープライズネットワークへのログオンを許可される前に認証されます。認証では、役割に基づいて、ユーザーまたはユーザーのグループに対して特定のポリシーを柔軟に定義できます。ユーザー認証の詳細については、「[ユーザー識別管理](#)」を参照してください。

手順 4: URL フィルタリングを構成する

管理者は、URL 分類機能または URL リスト機能を使用して、URL フィルタリングポリシーを適用できます。

URL の分類。 事前に定義されたカテゴリのリストに基づいてトラフィックをフィルタリングすることにより、Web サイトや Web ページへのアクセスを制御します。

URL リスト。 アプライアンスにインポートされた URL セット内の URL へのアクセスを拒否することで、ブラックリストに登録された Web サイトおよび Web ページへのアクセスを制御します。

手順 5: セキュリティ構成を構成する

この手順では、レピュテーションスコアを設定し、スコアが低すぎる場合にアクセスを拒否することで、ユーザーがウェブサイトへのアクセスを制御できるようにします。レピュテーションスコアは 1 ~4 の範囲で、スコアが許容できないしきい値を設定できます。しきい値を超えるスコアの場合は、トラフィックを許可する、ブロック、またはリダイレクトするポリシーアクションを選択できます。詳しくは、「[セキュリティ設定](#)」を参照してください。

ステップ 6: SWG 分析を構成する

このステップでは、ウェブトラフィックの分類、ユーザトランザクションログの URL カテゴリのログ、トラフィック分析の表示を行うための SWG 分析をアクティブ化できます。SWG アナリティクスの詳細については、「[Analytics](#)」を参照してください。

手順 7: **[完了]** をクリックして初期設定を完了し、**URL** フィルタリング設定の管理を続行します

URL リスト

May 1, 2021

URL リスト機能を使用すると、企業のお客様は、特定の Web サイトおよび Web サイトのカテゴリへのアクセスを制御できます。この機能は、URL 照合アルゴリズムにバインドされたレスポンスポリシーを適用して Web サイトをフィルタリングします。このアルゴリズムは、着信 URL を、最大 100 万 (1,000,000) のエントリで構成される URL セットと照合します。着信 URL 要求がセット内のエントリと一致する場合、アプライアンスは応答側ポリシーを使用して要求 (HTTP/HTTPS) を評価し、その要求へのアクセスを制御します。

URL セットのタイプ

URL セット内の各エントリには、URL と、必要に応じてそのメタデータ (URL カテゴリ、カテゴリグループ、またはその他の関連データ) を含めることができます。メタデータを含む URL の場合、アプライアンスはメタデータを評価するポリシー式を使用します。詳しくは、「[URL セット](#)」を参照してください。

Citrix SWG は、カスタム URL セットをサポートしています。パターンセットを使用して URL をフィルタリングすることもできます。

カスタム URL セット。最大 1,000,000 個の URL エントリを含むカスタマイズされた URL セットを作成し、それをテキストファイルとしてアプライアンスにインポートできます。

パターンセット。SWG アプライアンスは、Web サイトへのアクセスを許可する前に、パターンセットを使用して URL をフィルタリングできます。パターンセットは、着信 URL と最大 5000 エントリの間で完全に一致する文字列を検索する文字列マッチングアルゴリズムです。詳しくは、「[パターンセット](#)」を参照してください。

読み込んだ URL セットの各 URL には、URL メタデータの形式でカスタムカテゴリを設定できます。組織では、セットをホストし、手動で介入することなく SWG アプライアンスを定期的に更新するように SWG アプライアンスを設定できます。

セットが更新されると、Citrix ADC アプライアンスはメタデータを自動的に検出し、URL を評価し、許可、ブロック、リダイレクト、通知などのアクションを適用するためのポリシー式としてカテゴリを使用できます。

URL セットで使用される高度なポリシー式

次の表に、着信トラフィックの評価に使用できる基本的な式を示します。

1. `.URLSET_MATCHES_ANY` -URL が URL TRUE セット内のエントリと完全に一致した場合に評価されません。
2. `.GET_URLSET_METADATA()` -URL が URL セット内の任意のパターンと完全に一致する場合、`GET_URLSET_METADATA()` 式は、関連付けられたメタデータを返します。一致しない場合は、空の文字列が返されます。
3. `.GET_URLSET_METADATA().EQ(<METADATA)` - `.GET_URLSET_METADATA().EQ(<METADATA)`
4. `.GET_URLSET_METADATA().TYPECAST_LIST_T(' , ').GET(0).EQ() - TRUE` 一致するメタデータがカテゴリの先頭にある場合に評価されます。このパターンは、メタデータ内の個別のフィールドをエンコードするために使用できますが、最初のフィールドのみに一致します。
5. `HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL)` -ホストパラメータと URL パラメータを結合します。このパラメータは、一致のためにとして使用することができます。

レスポンスのアクションの種類

注: 表では、HTTP.REQ.URL は<URL expression>として一般化されています。

次の表に、着信インターネットトラフィックに適用できるアクションを示します。

レスポンドのアクション	説明
許可	リクエストにターゲット URL へのアクセスを許可します。
リダイレクト	ターゲットとして指定された URL にリクエストをリダイレクトします。
ブロック	要求を拒否します。

前提条件

ホスト名の URL から URL セットをインポートする場合は、DNS サーバを設定する必要があります。IP アドレスを使用する場合は必須ではありません。

コマンドプロンプトで、次のように入力します。

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

例:

```
1 add dns nameServer 10.140.50.5
```

URL リストを構成する

URL リストを構成するには、Citrix SWG ウィザードまたは Citrix ADC コマンドラインインターフェイス (CLI) を使用します。Citrix SWG アプライアンスでは、レスポンドポリシーを構成してから、ポリシーを URL セットにバインドする必要があります。

Citrix SWG ウィザードを使用して、URL リストを構成することをお勧めします。ウィザードを使用して、レスポンドポリシーを URL セットにバインドします。または、ポリシーをパターンセットにバインドすることもできます。

Citrix SWG ウィザードを使用して URL 一覧を構成する

Citrix SWG GUI を使用して HTTPS トラフィックの URL リストを構成するには:

1. Citrix SWG アプライアンスにログオンし、セキュアな **Web** ゲートウェイ のページに移動します。
2. 詳細ウィンドウで、次のいずれかの操作を行います。

- a) [セキュアな **Web** ゲートウェイ] をクリックして、URL リスト機能を備えた新しい SWG 設定を作成します。
 - b) 既存の構成を選択し、[**Edit**] をクリックします。
3. [URL フィルタリング] セクションで、[編集] をクリックします。
 4. 機能を有効にするには、[URL リスト] チェックボックスをオンにします。
 5. URL リスト ポリシーを選択し、[バインド] をクリックします。
 6. [続行] をクリックし、[完了] をクリックします。

詳しくは、「[URL リストポリシーの作成方法](#)」を参照してください。

Citrix SWG CLI を使用して URL リストを構成する

URL リストを設定するには、次の手順を実行します。

1. HTTP および HTTPS トラフィック用のプロキシ仮想サーバーを構成します。
2. HTTPS トラフィックを代行受信するための SSL インターセプションを設定します。
3. HTTP トラフィック用の URL セットを含む URL リストを設定します。
4. HTTPS トラフィックに設定された URL を含む URL リストを設定します。
5. プライベート URL セットを設定します。

注

SWG アプライアンスをすでに設定している場合は、手順 1 と 2 をスキップし、ステップ 3 で設定できます。

インターネットトラフィック用のプロキシ仮想サーバーの構成 Citrix SWG アプライアンスは、透過的かつ明示的なプロキシ仮想サーバーをサポートします。エクスプリシットモードでインターネットトラフィック用のプロキシ仮想サーバーを構成するには、次の手順を実行します。

1. プロキシ SSL 仮想サーバーを追加します。
2. レスポンダーポリシーをプロキシ仮想サーバーにバインドします。

Citrix SWG CLI を使用してプロキシ仮想サーバーを追加するには：

コマンドプロンプトで、次のように入力します。

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

例：

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

Citrix SWG CLI を使用してレスポンダーポリシーをプロキシ仮想サーバーにバインドするには：

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

注

Citrix SWG 構成の一部として SSL インターセプタをすでに構成している場合は、次の手順を省略できます。

HTTPS トラフィックの **SSL** インターセプションの設定 HTTPS トラフィックの SSL インターセプションを設定するには、次の手順を実行します。

1. CA 証明書とキーのペアをプロキシ仮想サーバにバインドします。
2. デフォルトの SSL プロファイルを有効にします。
3. フロントエンド SSL プロファイルを作成し、プロキシ仮想サーバにバインドし、フロントエンド SSL プロファイルで SSL インターセプションを有効にします。

Citrix SWG CLI を使用して CA 証明書とキーのペアをプロキシ仮想サーバにバインドするには:

コマンドプロンプトで、次のように入力します。

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

Citrix SWG CLI を使用してフロントエンド SSL プロファイルを構成するには:

コマンドプロンプトで、次のように入力します。

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

Citrix SWG CLI を使用してフロントエンド SSL プロファイルをプロキシ仮想サーバにバインドするには

コマンドプロンプトで、次のように入力します。

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

HTTP トラフィックの **URL** セットをインポートして **URL** リストを構成する HTTP トラフィックの URL セットを設定する方法については、[URL セット](#)を参照してください。

明示的なサブドメイン一致の実行 インポートされた URL セットに対して明示的なサブドメイン照合を実行できるようになりました。これを行うには、新しいパラメータ「subdomainExactMatch」が `import policy URLset` コマンドに追加されます。

パラメータを有効にすると、URL フィルタリングアルゴリズムは明示的なサブドメイン一致を実行します。たとえば、着信 URL が `news.example.com` で、URL セットのエントリが `example.com` の場合、アルゴリズムは URL と一致しません。

コマンドプロンプトで、次のように入力します。

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

例

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

HTTPS トラフィック用の **URL** セットを構成する Citrix SWG CLI を使用して HTTPS トラフィック用の URL セットを構成するには

コマンドプロンプトで次のように入力します。

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

例:

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

Citrix SWG ウィザードを使用して **HTTPS** トラフィック用の **URL** セットを構成するには Citrix SWG ウィザードを使用して、URL リストを構成することをお勧めします。ウィザードを使用して、カスタム URL セットをインポートし、レスポンスポリシーにバインドします。

1. **Citrix SWG** アプライアンスにログオンし、セキュアな **Web** ゲートウェイ > **URL** フィルタリング > **URL** リストに移動します。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [**URL** リストポリシー] ページで、ポリシー名を指定します。
4. URL セットをインポートするオプションを選択します。
5. [**URL** リストポリシー] タブページで、[**URL** セットのインポート] チェックボックスをオンにし、次の URL セットパラメータを指定します。
 - a) URL セット名-カスタム URL セットの名前。
 - b) URL: URL セットにアクセスする場所の Web アドレス。
 - c) 「上書き」(Overwrite)-以前にインポートした URL セットを上書きします。
 - d) Delimiter: CSV ファイルレコードを区切る文字シーケンス。

- e) 行区切り文字—CSV ファイルで使用される行区切り文字。
 - f) [Interval]: URL セットが更新される 15 分に最も近い秒数に切り捨てられた間隔 (秒単位)。
 - g) プライベートセット—URL セットのエクスポートを防止するオプション。
 - h) カナリア URL—URL セットのコンテンツが機密扱いかどうかをテストするための内部 URL。URL の最大長は 2047 文字です。
6. ドロップダウンリストから応答者のアクションを選択します。
 7. 【作成】して【閉じる】をクリックします。

プライベート URL セットの構成 プライベート URL セットを設定し、その内容を秘密にしておくと、ネットワーク管理者はセット内のブラックリスト URL を知らないことがあります。そのような場合は、カナリアの URL を設定し、URL セットに追加できます。管理者は Canary URL を使用して、すべてのルックアップ要求で使用するプライベート URL セットをリクエストできます。各パラメータの説明については、ウィザードのセクションを参照してください。

Citrix SWG CLI を使用して URL セットをインポートするには:

コマンドプロンプトで、次のように入力します。

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

例:

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

インポートされた **URL** セットを表示

追加された URL セットに加えて、読み込んだ URL セットも表示できるようになりました。これを行うには、新しいパラメータ「インポート」が「show urlset」コマンドに追加されます。このオプションを有効にすると、アプライアンスはインポートされたすべての URL セットを表示し、インポートされた URL セットと追加された URL セットを区別します。

コマンドプロンプトで、次のように入力します。

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

例

```
show policy urlset -imported
```


監査ログメッセージの構成

監査ログを使用すると、URL リストプロセスのどのフェーズでも条件や状況を確認できます。Citrix ADC アプライアンスが受信 URL を受信すると、レスポンスポリシーに URL セットの詳細ポリシー式がある場合、監査ログ機能によって URL セットの情報が収集され、監査ログで許可されるターゲットのログメッセージとして詳細が保存されます。

1. ログメッセージには、次の情報が含まれています。
2. タイムスタンプ。
3. ログメッセージのタイプ。
4. 定義済みのログレベル (重大、エラー、通知、警告、情報、デバッグ、アラート、緊急)。
5. URL セット名、ポリシーアクション、URL などのログメッセージ情報。

URL リスト機能の監査ログを設定するには、次のタスクを実行する必要があります。

1. 監査ログを有効化。
2. 監査ログメッセージの作成アクション。
3. [監査ログメッセージ] アクションで URL リストレスポンスポリシーを設定します。

詳細については、[監査ログ](#)を参照してください。

URL パターンのセマンティクス

May 1, 2021

次の表に、フィルタリングするページのリストを指定するために使用する URL パターンを示します。たとえば、`www.example.com/bar` というパターンは、`www.example.com/bar` の 1 ページだけに一致します。URL が `'www.example.com/bar'` で始まるすべてのページを一致させるには、URL の末尾にアスタリスク (*) を追加します。

メタデータマッピングにマッチする **URL** パターンのセマンティクス

パターンマッチングセマンティクスは、テーブル形式で使用できます。詳細については、[パターンセマンティクスpdf](#) ページを参照してください。

URL カテゴリのマッピング

May 1, 2021

サードパーティのカテゴリとカテゴリグループのリスト。詳細については、[URL カテゴリのマッピングページ](#)を参照してください。

ユースケース: カスタム URL セットを使用した URL フィルタリング

May 1, 2021

特定の Web サイトや Web サイトのカテゴリへのアクセスを制御する方法を探している企業のお客様は、レスポンスポリシーにバインドされたカスタム URL セットを使用できます。組織のネットワークインフラストラクチャでは、URL フィルターを使用して、アダルト、暴力、ゲーム、薬物、政治、求人ポータルなど、悪意のある Web サイトや危険な Web サイトへのアクセスをブロックできます。URL のフィルタリングに加えて、カスタマイズされた URL のリストを作成し、SWG アプライアンスにインポートできます。たとえば、組織のポリシーで、ソーシャルネットワーキング、ショッピングポータル、求人ポータルなどの特定の Web サイトへのアクセスをブロックするよう求められる場合があります。

リスト内の各 URL は、メタデータの形式でカスタムカテゴリを持つことができます。組織では、Citrix SWG アプライアンス上で URL セットとして URL のリストをホストし、手動で介入することなく定期的にセットを更新するようにアプライアンスを構成できます。

セットが更新されると、Citrix ADC アプライアンスはメタデータを自動的に検出し、レスポンスポリシーは URL メタデータ (カテゴリの詳細) を使用して着信 URL を評価し、許可、ブロック、リダイレクト、通知などのアクションを適用します。

この設定をネットワークに実装するには、次のタスクを実行します。

1. カスタム URL セットのインポート
2. カスタム URL セットの追加
3. Citrix SWG ウィザードでカスタム URL 一覧を構成する

Citrix SWG CLI を使用してカスタム **URL** セットをインポートするには:

コマンドプロンプトで、次のように入力します。

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

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

Citrix SWG CLI を使用してカスタム **URL** セットを追加するには:

コマンドプロンプトで、次のように入力します。

```
add urlset <urlset_name>
```

```
1 Add urlset test1
```

Citrix SWG ウィザードを使用して URL 一覧を構成する

Citrix SWG ウィザードを使用して、URL リストを構成することをお勧めします。ウィザードを使用して、カスタム URL セットをインポートし、レスポンスポリシーにバインドします。

1. **Citrix SWG** アプライアンスにログインし、セキュアな **Web** ゲートウェイ > **URL** フィルタリング > **URL** リストに移動します。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [**URL** リストポリシー] ページで、ポリシー名を指定します。
4. URL セットをインポートするオプションを選択します。
5. [**URL** リストポリシー] タブページで、[**URL** セットのインポート] チェックボックスをオンにし、次の URL セットパラメータを指定します。
 - a) URL セット名-カスタム URL セットの名前。
 - b) URL: URL セットにアクセスする場所の Web アドレス。
 - c) 「上書き」(Overwrite)-以前にインポートした URL セットを上書きします。
 - d) Delimiter: CSV ファイルレコードを区切る文字シーケンス。
 - e) 行区切り文字-CSV ファイルで使用される行区切り文字。
 - f) 間隔: URL セットが更新される、最も近い 15 分に四捨五入された秒単位の間隔。
 - g) プライベートセット-URL セットのエクスポートを防止するオプション。
 - h) Canary URL: URL セットのコンテンツの機密を保持するかどうかをテストするための内部 URL。URL の最大長は 2047 文字です。
6. ドロップダウンリストから応答者のアクションを選択します。
7. [作成] して [閉じる] をクリックします。

The screenshot shows the 'URL List Policy' configuration page. At the top, there are tabs for 'URL List Policies' and 'URL List Policy'. The main heading is 'URL List Policy'. Below this, there are several input fields and checkboxes:

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

Below these fields is an **Action*** dropdown menu set to 'Allow'. At the bottom, there are two buttons: 'Create' (in blue) and 'Close'.

カスタム **URL** セットのメタデータのセマンティクス

カスタム URL セットをインポートするには、URL をテキストファイルに追加し、レスポンスポリシーにバインドして Social ネットワーキング URL をブロックします。

次に、テキストファイルに追加できる URL の例を示します。

cnn.com,News

bbc.com,News

google.com,Search Engine

yahoo.com,Search Engine

facebook.com,Social Media

twitter.com,Social Media

Citrix ADC CLI を使用してソーシャルメディア **URL** をブロックするようにレスポンスポリシーを構成する

レスポンスアクションを追加 `act_url_unauthorized respondwith "HTTP/1.1 451 Unavailable For Legal Reasons\r\n\r\nURL is NOT authorized\r\n"`

```
レスポンスポリシーを追加 pol_url_meta_match 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).GET_URLSET_ME  
"u1" ).EQ( "Social Media" )' act_url_meta_match
```

URL の分類

May 1, 2021

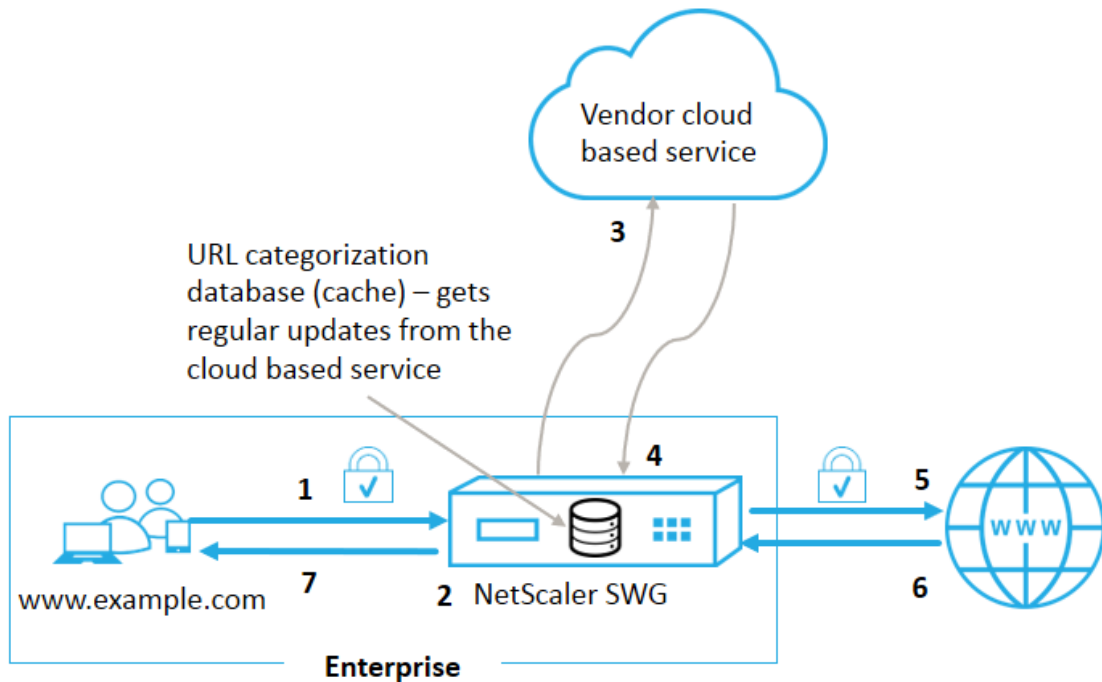
URL の分類は、特定の Web サイトおよび Web サイトのカテゴリへのユーザーアクセスを制限します。この機能により、Citrix Secure Web Gateway (SWG) が提供するサブスクリプションサービスとして、企業のお客様は、商用分類データベースを使用して Web トラフィックをフィルタリングできます。データベースには、ソーシャルネットワーキング、ギャンブル、アダルトコンテンツ、新しいメディア、ショッピングなど、さまざまなカテゴリに分類された URL が数十億個あります。分類に加えて、各 URL には、サイトの履歴リスクプロファイルに基づいて最新のレピュテーションスコアがあります。トラフィックをフィルタリングするには、カテゴリ、カテゴリグループ（テロリズム、違法薬など）、またはサイトレピュテーションスコアに基づいて高度なポリシーを構成できます。

たとえば、マルウェアに感染していることがわかっているサイトなど、危険なサイトへのアクセスをブロックし、エンタープライズユーザーのアダルトコンテンツやエンターテインメントストリーミングメディアなどのコンテンツへのアクセスを選択的に制限できます。また、ユーザーのトランザクションの詳細と送信トラフィックの詳細をキャプチャして、Citrix ADM サーバー上の Web トラフィック分析を監視することもできます。

Citrix ADC は、事前構成された NetSTAR デバイス `nsv10.netstar-inc.com` および `incompasshybridpc.netstar-inc.com` からデータをアップロードまたはダウンロードし、クラウド分類要求のデフォルトでクラウドホストとして使用されます。アプライアンスは、NSIP アドレスを送信元 IP アドレスとして使用し、443 を通信の宛先ポートとして使用します。

URL 分類の仕組み

次の図は、頻繁に更新するために、Citrix SWG URL 分類サービスを、商用 URL 分類データベースおよびクラウドサービスと統合する方法を示しています。



コンポーネントは次のように相互作用します。

1. クライアントは、インターネットにバインドされた URL 要求を送信します。
2. Citrix SWG プロキシは、URL カテゴリ化データベースから取得したカテゴリの詳細（カテゴリ、カテゴリグループ、サイトレピュテーションスコアなど）に基づいて、リクエストにポリシー適用を適用します。データベースがカテゴリの詳細を返す場合、プロセスは手順 5 にジャンプします。
3. データベースで分類の詳細が失われると、要求は URL 分類ベンダーが管理するクラウドベースの検索サービスに送信されます。ただし、アプライアンスは応答を待たずに、URL が未分類としてマークされ、ポリシーの強制が実行されます（ステップ 5 に進みます）。アプライアンスは、クラウドクエリーフィードバックを監視し続け、キャッシュを更新して、今後の要求がクラウドルックアップの恩恵を受けることができますようにします。
4. SWG アプライアンスは、クラウドベースのサービスから URL カテゴリの詳細（カテゴリ、カテゴリグループ、レピュテーションスコア）を受け取り、カテゴリ化データベースに保存します。
5. ポリシーでは URL が許可され、リクエストはオリジンサーバーに送信されます。それ以外の場合、アプライアンスはカスタム HTML ページを使用してドロップ、リダイレクト、または応答します。
6. オリジンサーバーは、要求されたデータで SWG アプライアンスに応答します。
7. アプライアンスは応答をクライアントに送信します。

ユースケース: 企業コンプライアンスに基づくインターネット使用

URL フィルタリング機能を使用して、コンプライアンスポリシーを検出して実装し、企業のコンプライアンスに違反するサイトをブロックできます。これらは、成人、ストリーミングメディア、非生産的と見なされるか、またはエンタープライズネットワークで過剰なインターネット帯域幅を消費するソーシャルネットワーキングなどのサイトです。これらの Web サイトへのアクセスをブロックすると、従業員の生産性が向上し、帯域幅使用の運用コストが削減され、ネットワーク消費のオーバーヘッドが削減されます。

前提条件

URL 分類機能は、Citrix SWG プラットフォームで、Citrix Secure Web Gateway の URL フィルタリング機能と脅威インテリジェンスを備えたオプションのサブスクリプションサービスがある場合にのみ機能します。このサブスクリプションでは、Web サイトの最新の脅威カテゴリをダウンロードし、Secure Web Gateway でそれらのカテゴリを適用できます。このサブスクリプションは、ハードウェアアプライアンスとソフトウェア (VPX) バージョンの Secure Web Gateway の両方で使用できます。

機能を有効にして設定する前に、次のライセンスをインストールする必要があります。

CNS_WEBF_SSERVER_Retail.lic

CNS_XXXXX_SERVER_SWG_Retail.lic.

ここで、XXXXX はプラットフォーム・タイプです (例: V25000)。

レスポンスポリシー式

次の表に、着信 URL を許可、リダイレクト、またはブロックする必要があるかどうかを確認するために使用できるさまざまなポリシー式を示します。

1. `<text>. URL_CATEGORIZE (<min_reputation>, <max_reputation>)` - `URL_CATEGORY` オブジェクトを返します。`<min_reputation>` が 0 より大きい場合、返されるオブジェクトには、`<min_reputation>` より低いレピュテーションのカテゴリは含まれません。`<max_reputation>` が 0 より大きい場合、返されるオブジェクトには、`<max_reputation>` より高いレピュテーションのカテゴリは含まれません。カテゴリがタイムリーに解決に失敗した場合は、`undef` 値が返されます。
2. `<url_category>. CATEGORY ()` - このオブジェクトのカテゴリ文字列を返します。URL にカテゴリがない場合、または URL の形式が正しくない場合、戻り値は「Unknown」になります。
3. `<url_category>. CATEGORY_GROUP ()` - オブジェクトのカテゴリグループを識別する文字列を返します。これは、カテゴリのより高いレベルのグループです。これは、URL カテゴリに関する詳細情報を必要としない操作に役立ちます。URL にカテゴリがない場合、または URL の形式が正しくない場合、戻り値は「Unknown」になります。
4. `<url_category>. REPUTATION ()` - レピュテーションスコアを 0 ~ 5 の数値として返します。5 は最もリスクの高いレピュテーションを示します。カテゴリが「不明」の場合、評価値は 1 です。

ポリシータイプ:

1. 検索エンジンカテゴリにある URL のリクエストを選択するポリシー--`add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY().EQ("Search Engine")`
2. アダルトカテゴリグループの URL に対するリクエストを選択するためのポリシー--`add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY_GROUP().EQ("Adult")'`
3. レピュテーションスコアが 4 未満の検索エンジンの URL に対するリクエストを選択するポリシー--`add responder policy p2 'HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL).URL_CATEGORIZE(4,0).HAS_CATEGORY("Search Engine")`
4. 検索エンジンとショッピング URL のリクエストを選択するポリシー--`add responder policy p3 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY().EQ ("good_categories")`
5. レピュテーションスコアが 4 以上の検索エンジンの URL に対するリクエストを選択するためのポリシー--`add responder policy p5 'CLIENT.SSL.DETECTED_DOMAIN.URL_CATEGORIZE(4,0).CATEGORY().EQ("Search Engines")`
6. 検索エンジンカテゴリにある URL のリクエストを選択し、URL セットと比較するためのポリシー--`'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")'`

レスポンスポリシーの種類

URL 分類機能で使用されるポリシーには 2 つのタイプがあり、これらのポリシータイプを以下に説明します。

ポリシーの種類	説明
URL のカテゴリ	Web トラフィックを分類し、評価結果に基づいてトラフィックをブロック、許可、またはリダイレクトします。
URL レピュテーションスコア	Web サイトのレピュテーションスコアを決定し、管理者が設定したレピュテーションスコアのしきい値レベルに基づいてアクセスを制御できるようにします。

URL 分類の構成

Citrix SWG アプライアンス上で URL の分類を構成するには、次の手順を実行します。

1. URL フィルタリングを有効にします。
2. Web トラフィック用のプロキシサーバーを構成します。

3. 明示モードで Web トラフィックの SSL インターセプションを設定します。
4. キャッシュメモリを制限するように共有メモリを構成します。
5. URL 分類パラメータを設定します。
6. Citrix SWG ウィザードを使用して、URL の分類を構成します。
7. SWG ウィザードを使用して URL 分類パラメータを構成します。
8. シードデータベースパスとクラウドサーバー名の設定

ステップ 1: URL フィルタリングを有効にする

URL 分類を有効にするには、URL フィルタリング機能を有効にし、URL 分類のモードを有効にします。

Citrix SWG を使用して URL の分類を有効にするには: CLI

コマンドプロンプトで、次のように入力します。

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

手順 2: 明示モードで Web トラフィック用のプロキシサーバーを構成する

Citrix SWG アプライアンスは、透過的かつ明示的なプロキシ仮想サーバーをサポートします。明示モードで SSL トラフィック用のプロキシ仮想サーバーを設定するには、次の手順を実行します。

1. プロキシサーバーを追加します。
2. SSL ポリシーをプロキシサーバーにバインドします。

Citrix SWG CLI を使用してプロキシサーバーを追加するには

コマンドプロンプトで、次のように入力します。

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

例:

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

Citrix SWG CLI を使用して SSL ポリシーをプロキシ仮想サーバーにバインドする

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

ステップ 3: HTTPS トラフィックの SSL インターセプションを設定する

HTTPS トラフィックの SSL インターセプションを設定するには、次の手順を実行します。

1. CA 証明書とキーのペアをプロキシ仮想サーバにバインドします。
2. SSL パラメータを使用してデフォルトの SSL プロファイルを設定します。
3. フロントエンド SSL プロファイルをプロキシ仮想サーバにバインドし、フロントエンド SSL プロファイルで SSL インターセプションを有効にします。

Citrix SWG CLI を使用して CA 証明書とキーのペアをプロキシ仮想サーバにバインドするには

コマンドプロンプトで、次のように入力します。

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

Citrix SWG CLI を使用してデフォルトの SSL プロファイルを構成するには

コマンドプロンプトで、次のように入力します。

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

Citrix SWG CLI を使用してフロントエンド SSL プロファイルをプロキシ仮想サーバにバインドする

コマンドプロンプトで、次のように入力します。

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

手順 4: キャッシュメモリを制限するように共有メモリを構成する

Citrix SWG CLI を使用してキャッシュメモリを制限するように共有メモリを構成するには

コマンドプロンプトで、次のように入力します。

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

ここで、キャッシュ用に構成されたメモリ制限は 10 MB に設定されます。

ステップ 5: URL 分類パラメーターの設定

Citrix SWG CLI を使用して URL 分類パラメータを構成するには

コマンドプロンプトで、次のように入力します。

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

例:

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

手順 6: Citrix SWG ウィザードを使用して URL の分類を構成する

Citrix SWG GUI を使用して URL の分類を構成するには

1. Citrix SWG アプライアンスにログオンし、セキュアな **Web** ゲートウェイ のページに移動します。
2. 詳細ウィンドウで、次のいずれかの操作を行います。
 - a) [セキュアな **Web** ゲートウェイウィザード] をクリックして、新しい構成を作成します。
 - b) 既存の構成を選択し、[**Edit**] をクリックします。
3. [**URL** フィルタリング] セクションで、[編集] をクリックします。
4. この機能を有効にするには、[**URL** 分類] チェックボックスをオンにします。
5. **URL** 分類 ポリシーを選択し、[バインド] をクリックします。
6. [続行] をクリックし、[完了] をクリックします。

URL 分類ポリシーの詳細については、「[URL 分類ポリシーの作成方法](#)」を参照してください。

手順 7: SWG ウィザードを使用した URL 分類パラメーターの構成

Citrix SWG GUI を使用して URL 分類パラメータを構成するには

1. **Citrix SWG** アプライアンスにログオンし、「セキュアな **Web** ゲートウェイ」>「**URL** フィルタリング」の順に選択します。
2. [**URL** フィルタ] ページで、[**URL** フィルタ設定の変更] リンクをクリックします。
3. 「**URL** フィルタ・パラメータの設定」 ページで、次のパラメータを指定します。
 - a) DB 更新間隔 (時間)。URL データベース更新間のフィルタリング時間。最小値:0、最大値:720。
 - b) DB を更新する時刻。URL フィルタリングでデータベースを更新する時刻。
 - c) クラウドホスト。クラウドサーバーの URL パス。
 - d) シード DB パス。シードデータベース参照サーバーの URL パス。
4. [**OK**] をクリックして [閉じる] をクリックします。

設定例:

```
1 enable ns feature LB CS SSL IC RESPONDER AppFlow URLFiltering
2
3 enable ns mode FR L3 Edge USNIP PMTUD
4
5 set ssl profile ns_default_ssl_profile_frontend -denySSLReneg NONSECURE
  -sslInterception ENABLED -ssliMaxSessPerServer 100
6
7 add ssl certKey swg_ca_cert -cert ns_swg_ca.crt -key ns_swg_ca.key
8
9 set cache parameter -memLimit 100
10
11 add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180
12
13 add responder action act1 respondwith ""HTTP/1.1 200 OK\r\n\r\n" + http
  .req.url.url_categorize(0,0).reputation + "\n"
14
15 add responder policy p1 "HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.eq("
  Shopping/Retail") || HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.eq("
  Search Engines & Portals
16
17 ")" act1
18
19 bind cs vserver starcs_PROXY -policyName p1 -priority 10 -
  gotoPriorityExpression END -type REQUEST
20
21 add dns nameServer 10.140.50.5
22
23 set ssl parameter -denySSLReneg NONSECURE -defaultProfile ENABLED -
  sigDigestType RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-
  SHA512 -ssliErrorCache ENABLED
24
25 -ssliMaxErrorCacheMem 100000000
26
27 add ssl policy pol1 -rule "client.ssl.origin_server_cert.subject.
  URL_CATEGORIZE(0,0).CATEGORY.eq("Search Engines & Portals")" -
  action INTERCEPT
28
29 add ssl policy pol3 -rule "client.ssl.origin_server_cert.subject.ne("
  citrix")" -action INTERCEPT
30
31 add ssl policy swg_pol -rule "client.ssl.client_hello.SNI.
  URL_CATEGORIZE(0,0).CATEGORY.ne("Uncategorized")" -action INTERCEPT
32
33 set urlfiltering parameter -HoursBetweenDBUpdates 3 -
  TimeOfDayToUpdateDB 03:00
34 <!--NeedCopy-->
```

シードデータベースパスとクラウドサーバー名の設定

クラウド検索サーバー名とシードデータベースパスを手動で設定するために、シードデータベースパスとクラウドルックアップサーバー名を構成できるようになりました。これを行うには、URL フィルタリングパラメータコマンドに、「CloudHost」と「seedDBPath」という 2 つの新しいパラメータが追加されます。

コマンドプロンプトで、次のように入力します。

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

例

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

Citrix ADC アプライアンスと NetSTAR の間の通信には、ドメインネームサーバーが必要な場合があります。アプライアンスからの単純なコンソールまたは Telnet 接続を使用してテストできます。

例:

```
1 root@ns# telnet nsv10.netstar-inc.com 443
2 Trying 1.1.1.1...
3 Connected to nsv10.netstar-inc.com.
4 Escape character is '^]'.
5
6 root@ns# telnet incompasshybridpc.netstar-inc.com 443
7 Trying 10.10.10.10...
8 Connected to incompasshybridpc.netstar-inc.com.
9 Escape character is '^]'.
10 <!--NeedCopy-->
```

監査ログメッセージの構成

監査ログを使用すると、URL 分類プロセスのどのフェーズでも条件や状況を確認できます。Citrix ADC アプライアンスが着信 URL を受信すると、レスポンスポリシーに URL フィルタリング式がある場合、監査ログ機能によって URL セット情報が収集され、監査ログで許可されるターゲットのログメッセージとして保存されます。

- 送信元 IP アドレス（要求を行ったクライアントの IP アドレス）。
- 宛先 IP アドレス（要求されたサーバの IP アドレス）。
- スキーマ、ホスト、ドメイン名 (<http://www.example.com>) を含む要求された URL。
- URL フィルタリングフレームワークが返す URL カテゴリ。
- URL フィルタリングフレームワークが返した URL カテゴリグループ。
- URL フィルタリングフレームワークが返した URL レピュテーション番号。
- ポリシーによって実行された監査ログアクション。

URL リスト機能の監査ログを設定するには、次の作業を完了する必要があります。

1. 監査ログを有効化。
2. 監査ログメッセージの作成アクション。
3. [監査ログメッセージ] アクションで URL リストレスポンスポリシーを設定します。

詳細については、[監査ログ](#)を参照してください。

SYSLOG メッセージングを使用した障害エラーの保存

URL フィルタリングプロセスのどの段階でも、システムレベルの障害が発生した場合、Citrix ADC アプライアンスは監査ログメカニズムを使用してログを ns.log ファイルに保存します。エラーは、SYSLOG 形式のテキストメッセージとして保存されるため、管理者は後でイベントの発生を時系列で表示できます。これらのログは、アーカイブのために外部 SYSLOG サーバにも送信されます。詳しくは、「[記事 CTX229399](#)」を参照してください。

たとえば、URL フィルタリング SDK を初期化するときにエラーが発生した場合、エラーメッセージは次のメッセージ形式で格納されます。

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

Citrix ADC アプライアンスは、4 つの異なる障害カテゴリにエラーメッセージを格納します。

- ダウンロードに失敗しました。分類データベースをダウンロードしようとしたときにエラーが発生した場合。
- 統合の失敗。既存の分類データベースに更新を統合するときにエラーが発生した場合。
- 初期化に失敗しました。URL 分類機能の初期化時にエラーが発生した場合は、分類パラメータを設定するか、分類サービスを終了します。
- 取得に失敗しました。アプライアンスがリクエストの分類の詳細を取得するときにエラーが発生した場合。

コマンドインターフェイスによる **URL** 分類結果の表示

URL 分類を使用すると、NetStar サードパーティの URL 分類データベースから URL を入力し、分類結果（カテゴリ、グループ、評価スコアなど）を取得できます。

URL を入力すると、URL フィルタリング機能は、コマンドインターフェイスで分類結果を取得して表示します。さらに URL を入力すると、アプライアンスはリストから古い URL を除外し、最新の 3 つの URL の結果を表示します。

URL カテゴリの結果を 3 つまで表示するには、次の手順を実行します。

1. URL カテゴリ化 URL の追加
2. URL 分類の詳細を最大 3 つの URL まで表示します。
3. URL 分類データをクリアします。

URL フィルタリング分類 **URL** を追加するには

URL を追加し、その分類の詳細を取得するには、次の操作を行います。

コマンドプロンプトで、次のように入力します。

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

例:

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

URL 分類の詳細を **3** つまで表示するには

コマンドプロンプトで、次のように入力します。

```
> show urlfiltering categorization
```

例:

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

設定例:

```
1 add urlfiltering categorization -url www.facebook.com
2 Done
3 show urlfiltering categorization
4 Url: http://www.facebook.com    Categorization: Facebook,Social
   Networking,1
5 Done
6
7 add urlfiltering categorization -url www.google.com
8 Done
9 show urlfiltering categorization
10 Url: http://www.facebook.com   Categorization: Facebook,Social
   Networking,1
11 Url: http://www.google.com     Categorization: Search Engines &
   Portals,Search,1
12 Done
13
14 add urlfiltering categorization -url www.citrix.com
15 Done
16 show urlfiltering categorization
17 Url: http://www.facebook.com   Categorization: Facebook,Social
   Networking,1
```

```

18 Url: http://www.google.com      Categorization: Search Engines &
    Portals,Search,1
19 Url: http://www.citrix.com      Categorization: Computing & Internet,
    Computing & Internet,1
20 Done
21
22 add urlfiltering categorization -url www.in.gr
23 Done
24 show urlfiltering categorization
25 Url: http://www.google.com      Categorization: Search Engines &
    Portals,Search,1
26 Url: http://www.citrix.com      Categorization: Computing & Internet,
    Computing & Internet,1
27 Url: http://www.in.gr          Categorization: Search Engines & Portals,Search
    ,1 Done
28 <!--NeedCopy-->

```

URL 分類の結果をクリアするには

コマンドプロンプトで、次のように入力します。

```

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

```

GUI インターフェイスによる URL 分類結果の表示

1. ナビゲーションペインで、[**Secure Web Gateway**] > [**URL フィルタリング**] を展開します。
2. 詳細ウィンドウで、[ツール] セクションの [**URL フィルタ検索分類**] リンクをクリックします。
3. [**URL フィルタ検索分類**] ページで、URL 要求を入力し、[検索] をクリックします。

4. アプライアンスは、要求された URL および前の 2 つの URL 要求のカテゴリ結果を表示します。

セキュリティ構成

May 1, 2021

セキュリティ構成機能を使用すると、URL をフィルタリングするためのセキュリティポリシーを構成できます。「URL レピュテーションスコア」トピックでは、レピュテーションスコアに基づいて URL をフィルタリングするための概念および構成の詳細を提供します。

リモートコンテンツ検査には、ICAP を使用できます。

URL レピュテーションスコア

URL 分類機能は、URL レピュテーションスコアを使用して、ポリシーベースの制御を提供し、危険性が高い Web サイトをブロックします。詳しくは、「[URL レピュテーションスコア](#)」を参照してください。

ICAP を使用したリモートコンテンツ検査

HTTPS トラフィックは傍受され、復号化され、ICAP サーバに送信され、マルウェア対策チェックおよびデータ漏洩防止のためのコンテンツ検査が行われます。

URL レピュテーションスコア

May 1, 2021

URL 分類機能は、ポリシーベースの制御を提供し、ブラックリスト URL を制限します。URL カテゴリ、レピュテーションスコア、URL カテゴリとレピュテーションスコアに基づいて Web サイトへのアクセスを制御できます。ネットワーク管理者は、危険性が高い Web サイトにアクセスするユーザーを監視する場合、URL レピュテーションスコアにバインドされたレスポンスポリシーを使用して、そのような危険な Web サイトをブロックできます。

着信 URL 要求を受信すると、アプライアンスは URL 分類データベースからカテゴリとレピュテーションスコアを取得します。データベースから返されたレピュテーションスコアに基づいて、アプライアンスはウェブサイトにはレピュテーションレーティングを割り当てます。値の範囲は 1 ~ 4 です。4 は、次の表に示すように、最もリスクのある Web サイトのタイプです。

URL レピュテーション評価	評価コメント
1	クリーンサイト
2	不明なサイト

URL レピュテーション評価	評価コメント
3	潜在的に危険な、または危険なサイトに所属している
4	悪質なサイト

ユースケース:URL レピュテーションスコアによるフィルタリング

ユーザーのトランザクションとネットワーク帯域幅の消費を監視するネットワーク管理者を持つ企業組織を考えてみましょう。マルウェアがネットワークに入る可能性がある場合、管理者はデータのセキュリティを強化し、ネットワークにアクセスする悪意のある危険なウェブサイトへのアクセスを制御する必要があります。このような脅威からネットワークを保護するために、管理者は URL レピュテーションスコアによるアクセスを許可または拒否するように URL フィルタリング機能を設定できます。

ネットワーク上の発信トラフィックとユーザアクティビティのモニタリングの詳細については、[SWG Analytics](#)を参照してください。

組織の従業員がソーシャルネットワーキング Web サイトにアクセスしようとする時、SWG アプライアンスは URL 要求を受信し、URL 分類データベースに照会して、URL カテゴリをソーシャルネットワーキングとして取得し、潜在的に危険な Web サイトを示すレピュテーションスコア 3 を取得します。アプライアンスは、レピュテーション評価が 3 以上のサイトへのアクセスをブロックするなど、管理者が設定したセキュリティポリシーをチェックします。次に、ポリシーアクションを適用して、Web サイトへのアクセスを制御します。

この機能を実装するには、Citrix SWG ウィザードを使用して URL レピュテーションスコアとセキュリティしきい値レベルを構成する必要があります。

Citrix SWG GUI を使用してレピュテーションスコアを構成する:

Citrix SWG ウィザードを使用して、レピュテーションスコアとセキュリティレベルを構成することをお勧めします。設定されたしきい値に基づいて、トラフィックを許可する、ブロック、またはリダイレクトするポリシーアクションを選択できます。

1. **Citrix SWG** アプライアンスにログオンし、**Secure Web Gateway** に移動します。
2. 詳細ウィンドウで、[セキュアな **Web** ゲートウェイウィザード] をクリックします。
3. **Secure Web Gateway** の構成ページで、SWG プロキシサーバーの設定を指定します。
4. [**Continue**] をクリックして、SSL インターセプションなどの他の設定を指定し、管理を識別します。
5. [続行] をクリックして、[セキュリティ構成] セクションにアクセスします。
6. 「セキュリティ構成」セクションで、「レピュテーションスコア」チェックボックスを選択して、URL レピュテーションスコアに基づいてアクセスを制御します。
7. セキュリティレベルを選択し、レピュテーションスコアのしきい値を指定します。
 - a) より大きい、または等しい: しきい値が N 以上の場合、Web サイトを許可またはブロックします。N の範囲は 1 ~4 です。
 - b) 以下-しきい値が N 以下の場合、Web サイトを許可またはブロックします。N の範囲は 1 ~4 です。

- c) [In from]: しきい値が N1 ~N2 の間で、1 ~4 の範囲の場合に、Web サイトを許可またはブロックします。
8. ドロップダウンリストから応答者のアクションを選択します。
 9. [続行] をクリックして閉じる。

次の図は、Citrix SWG ウィザードの [セキュリティの構成] セクションを示しています。[URL レピュテーションスコア] オプションを有効にして、ポリシー設定を構成します。

Security Configuration

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

Reputation Score

If the score is*

Greater than or equals to Less than or equals to Between

3

Action*

Allow

Continue Cancel

ICAP を使用したリモートコンテンツ検査

May 1, 2021

Internet Content Adaptation Protocol (ICAP) は、シンプルで軽量のオープンプロトコルです。通常、プロキシと、マルウェア対策のサポートおよびデータ漏洩防止サービスを提供するデバイス間で HTTP メッセージを転送するために使用されます。ICAP は、コンテンツ配信の柔軟性を高め、付加価値サービスを提供するために、コンテンツ適応のための標準インターフェイスを作成しました。ICAP クライアントは、HTTP 要求と応答を ICAP サーバに転送して処理します。ICAP サーバーは、要求に対して何らかの変換を実行し、要求または応答に対して適切なアクションを使用して ICAP クライアントに応答を返します。

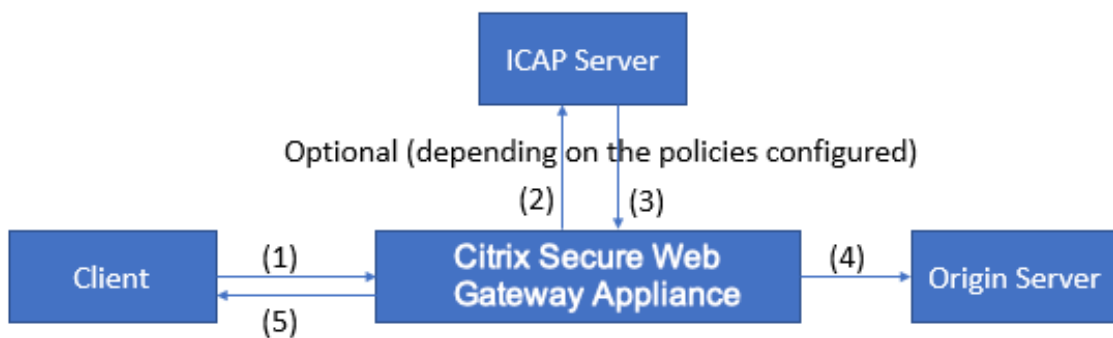
Citrix Secure Web Gateway アプライアンスでの ICAP の使用

注

コンテンツ検査機能を使用するには、SWG Edition ライセンスが必要です。

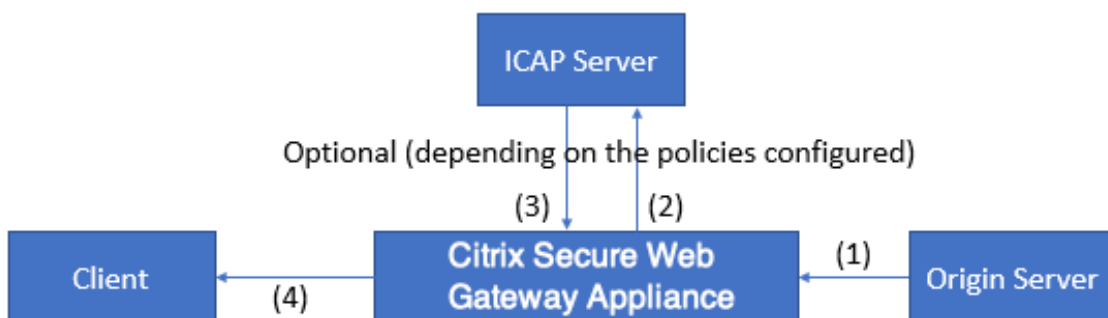
Citrix Secure Web Gateway (SWG) アプライアンスは ICAP クライアントとして機能し、ポリシーを使用して ICAP サーバーと通信します。アプライアンスは、マルウェア対策やデータ漏洩防止 (DLP) などの機能を専門とするサードパーティの ICAP サーバーと通信します。SWG アプライアンスで ICAP を使用すると、暗号化されたファイルもスキャンされます。セキュリティベンダーは、以前にこれらのファイルをバイパスしました。アプライアンスは SSL インターセプトを実行し、クライアントトラフィックを復号化し、ICAP サーバーに送信します。ICAP サーバーは、ウイルス、マルウェア、スパイウェアの検出、データリーク検査、またはその他のコンテンツ適応サービスをチェックします。アプライアンスはプロキシとして機能し、オリジンサーバからの応答を復号化し、それをプレーンテキストで ICAP サーバに送信して検査します。ICAP サーバに送信されるトラフィックを選択するためのポリシーを設定します。

要求モードフローは次のように動作します。



(1) Citrix SWG アプライアンスは、クライアントからの要求をインターセプトします。(2) アプライアンスは、アプライアンスに構成されたポリシーに基づいて、これらの要求を ICAP サーバーに転送します。(3) ICAP サーバーは、「適応不要」、エラー、または変更要求を示すメッセージで応答します。アプライアンスは、(4) クライアントが要求したオリジンサーバーにコンテンツを転送するか、(5) クライアントに適切なメッセージを返します。

応答モードフローは次のように動作します。



(1) オリジンサーバーは Citrix SWG アプライアンスに応答します。(2) アプライアンスは、アプライアンスに構成されたポリシーに基づいて、応答を ICAP サーバーに転送します。(3) ICAP サーバーは、「適応不要」、エラー、または変更要求を示すメッセージで応答します。(4) 応答を受信した場合、アプライアンスは要求されたコンテンツをクライアントに転送するか、適切なメッセージを送信します。

Citrix Secure Web Gateway アプライアンスでの ICAP の構成

次の手順では、Citrix SWG アプライアンス上で ICAP を構成する方法について説明します。

1. コンテンツ検査機能を有効にします。
2. プロキシサーバを設定します。
3. ICAP サーバを表す TCP サービスを設定します。SWG アプライアンスと ICAP サービスの間の安全な接続を確立するには、サービスタイプを `SSL_TCP` として指定します。セキュリティで保護された ICAP の詳細については、このページの「セキュリティで保護された ICAP」セクションを参照してください。
4. 必要に応じて、負荷分散仮想サーバを追加して、ICAP サーバーの負荷を分散し、ICAP サービスをこの仮想サーバにバインドします。
5. カスタム ICAP プロファイルを設定します。プロファイルには、ICAP サービスの URI またはサービスパス、および ICAP モード (要求または応答) を含める必要があります。HTTP および TCP のデフォルトプロファイルに似た ICAP デフォルトプロファイルはありません。
6. コンテンツインスペクションアクションを設定し、ICAP プロファイル名を指定します。サーバー名パラメーターに、負荷分散仮想サーバー名または TCP/SSL_TCP サービス名を指定します。
7. クライアントトラフィックを評価し、プロキシサーバにバインドするようにコンテンツインスペクションポリシーを設定します。このポリシーでコンテンツ検査アクションを指定します。

CLI を使用した ICAP の設定

次のエンティティを構成します。

1. 本機能を有効にします。

```
enable ns feature contentInspection
```

2. プロキシサーバを設定します。

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

例:

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

3. ICAP サーバを表すように TCP サービスを設定します。

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

ICAP サーバーとの安全な接続の場合、サービスタイプを `SSL_TCP` として指定します。

例:

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

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

4. 負荷分散仮想サーバーを構成します。

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

例:

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

ICAP サービスを負荷分散仮想サーバーにバインドします。

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

例:

```
bind lb vserver lbicap icap_svc
```

5. カスタム ICAP プロファイルを追加します。

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

例:

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

パラメーター

名前

ICAP プロファイルの名前。ASCII 英数字またはアンダースコア (_) 文字で始まり、ASCII 英数字、アンダースコア、ハッシュ (#)、ピリオド (.)、スペース、コロン (:)、アットマーク (@)、等号 (=)、ハイフン (-) のみを含める必要があります。

CLI ユーザー: 名前に 1 つ以上のスペースが含まれている場合は、名前を二重引用符または一重引用符で囲みます (「my icap profile」 や 「my icap プロファイル」 など)。

最大長: 127

uri

ICAP サービスパスを表す URI。

最大長:511 文字

モード

ICAP モード。使用可能な設定は次のように機能します。

- REQMOD: 要求変更モードでは、ICAP クライアントは HTTP 要求を ICAP サーバーに転送します。
- RESPMOD: 応答変更モードでは、ICAP サーバーはオリジンサーバーから ICAP サーバーに HTTP 応答を転送します。

可能な値:REQMOD、RESPMOD

6. ポリシーが true を返した場合に実行するアクションを設定します。

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

例:

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

7. トラフィックを評価するポリシーを設定します。

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

例:

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

8. ポリシーをプロキシサーバーにバインドします。

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

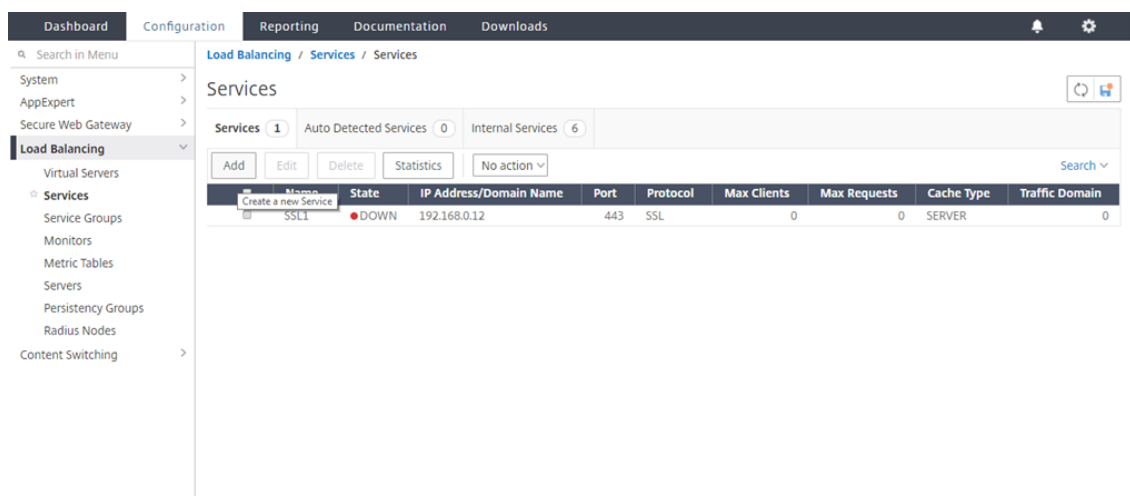
例:

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

GUI を使用して ICAP を構成する

次の手順を実行します。

1. [負荷分散] > [サービス] に移動し、[追加] をクリックします。



- 名前と IP アドレスを入力します。「プロトコル」で、「**TCP**」を選択します。[ポート] に **1344** と入力します。[**OK**] をクリックします。

ICAP サーバへのセキュア接続の場合は、TCP_SSL プロトコルを選択し、ポートを 11344 と指定します。

The screenshot shows the 'Load Balancing Service' configuration window. The 'Basic Settings' section is visible, containing the following fields:

- Service Name*: icap_svc
- IP Address Type: New Server Existing Server
- IP Address*: 203 . 0 . 113 . 100
- Protocol*: TCP
- Port*: 1344

At the bottom, there are 'OK' and 'Cancel' buttons. A 'Help' button is also present on the right side of the window.

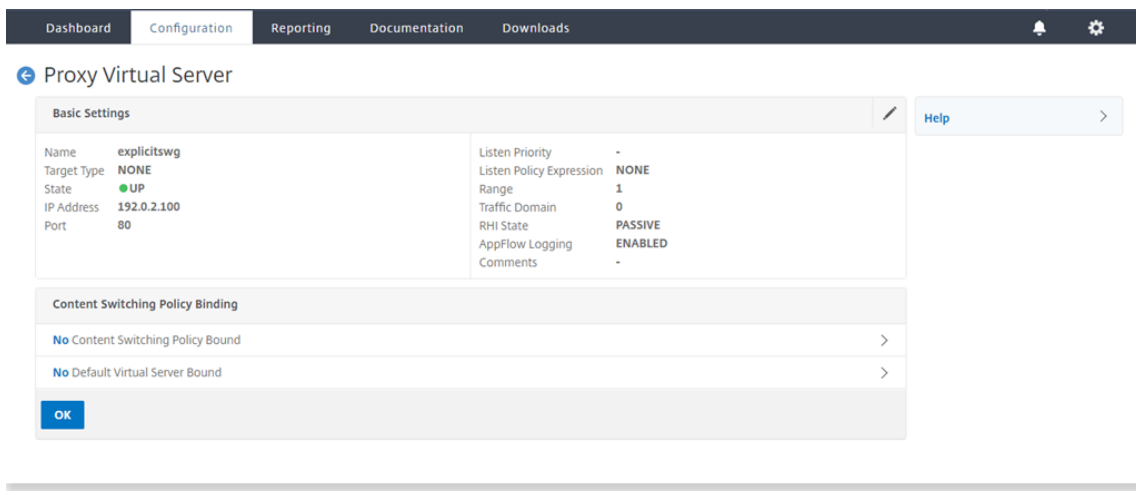
- [**Secure Web Gateway**] > [プロキシ仮想サーバー] に移動します。プロキシ仮想サーバーを追加するか、仮想サーバーを選択して「編集」をクリックします。詳細を入力したら、[**OK**] をクリックします。

The screenshot shows the 'Proxy Virtual Server' configuration window. The 'Basic Settings' section is visible, containing the following fields:

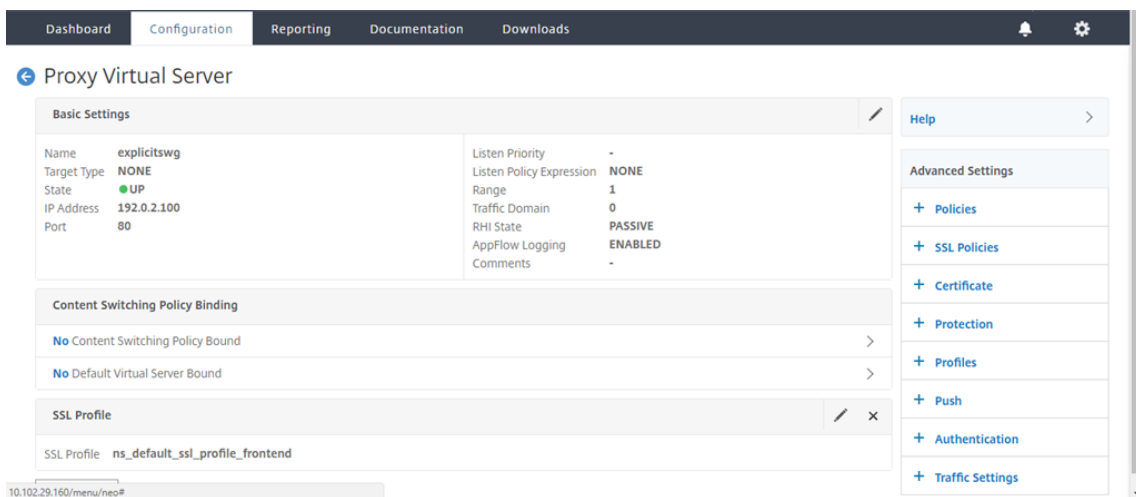
- Name*: explicitSWG
- IP Address Type*: IP Address
- IP Address*: 192 . 0 . 2 . 100
- Port*: 80

At the bottom, there are 'OK' and 'Cancel' buttons. A 'Help' button is also present on the right side of the window.

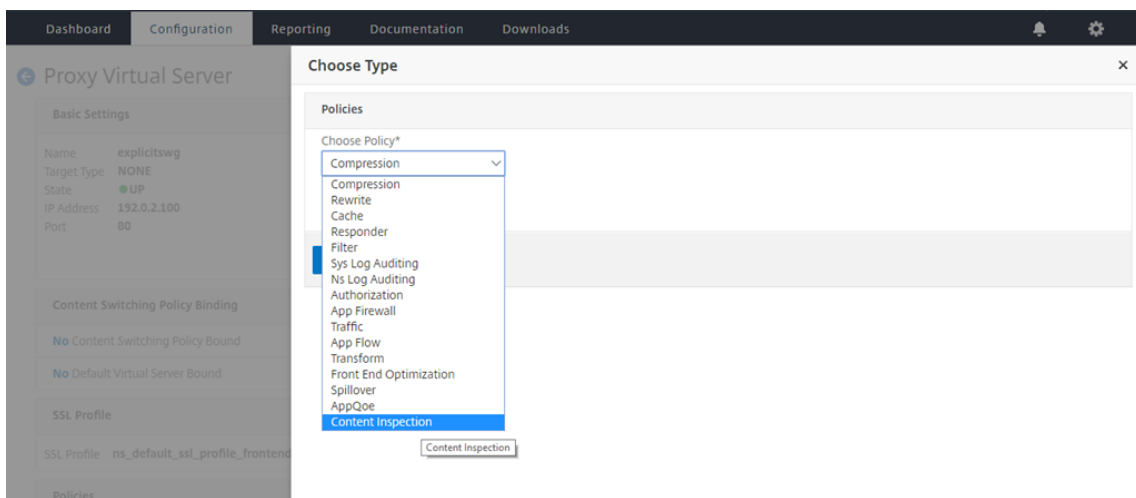
もう一度 [**OK**] をクリックします。



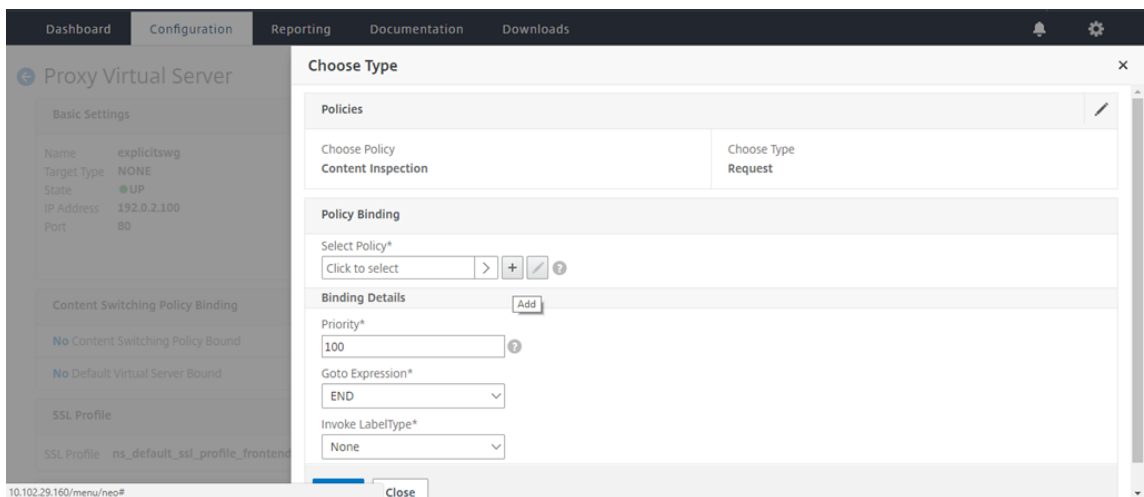
4. [詳細設定] で、[ポリシー] をクリックします。



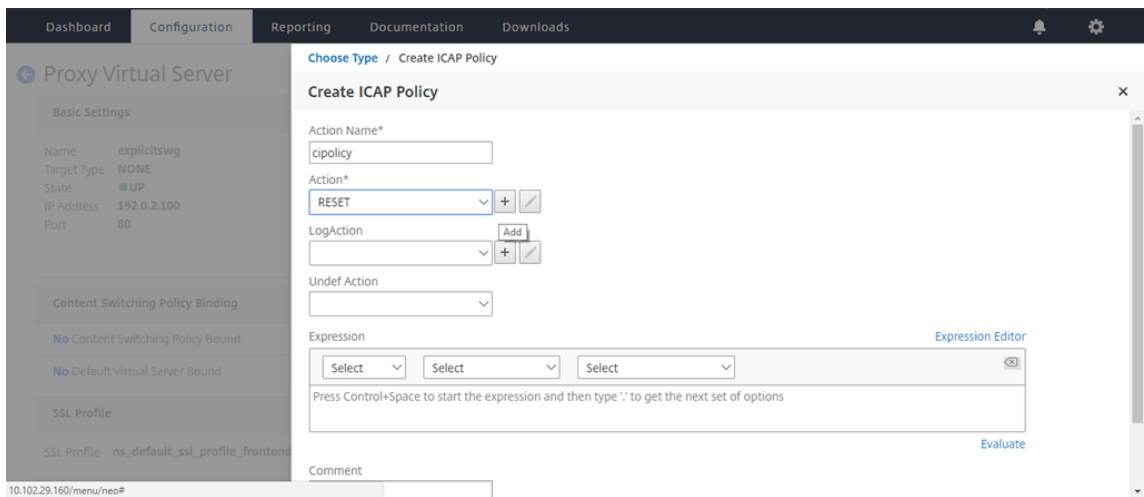
5. 「ポリシーの選択」で、「コンテンツ検査」を選択します。[続行] をクリックします。



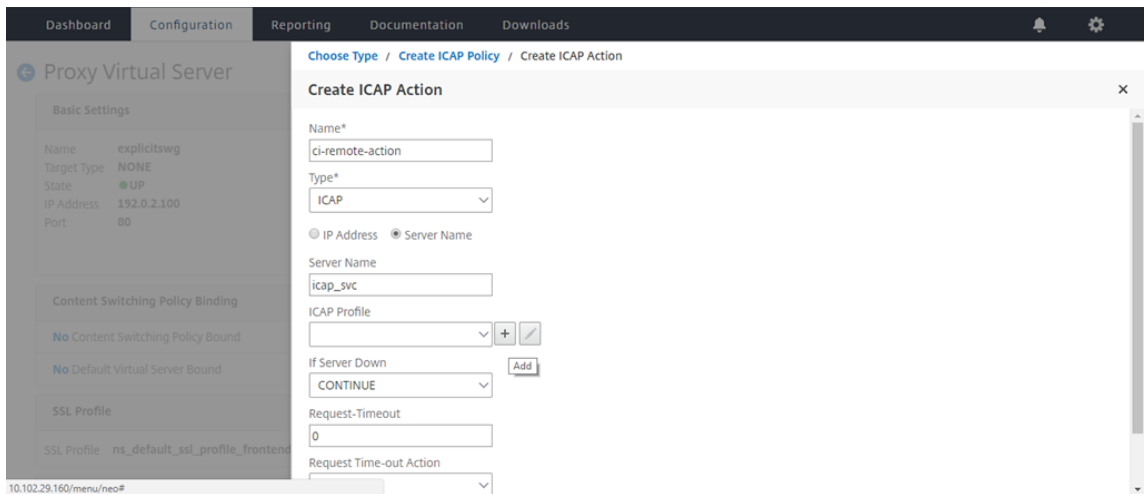
6. [ポリシーの選択] で、[+] 記号をクリックしてポリシーを追加します。



7. ポリシーの名前を入力します。[アクション]で、[+]記号をクリックしてアクションを追加します。



8. アクションの名前を入力します。[サーバー名]に、以前に作成した TCP サービスの名前を入力します。ICAP プロファイルで、「+」記号をクリックして ICAP プロファイルを追加します。

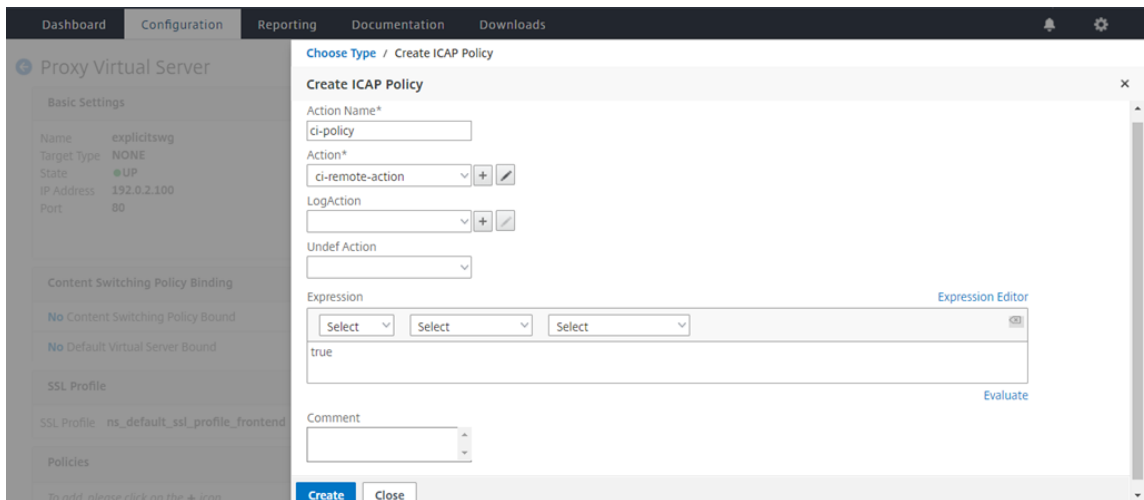


9. プロファイル名「URI」を入力します。「モード」で「REQMOD」を選択します。

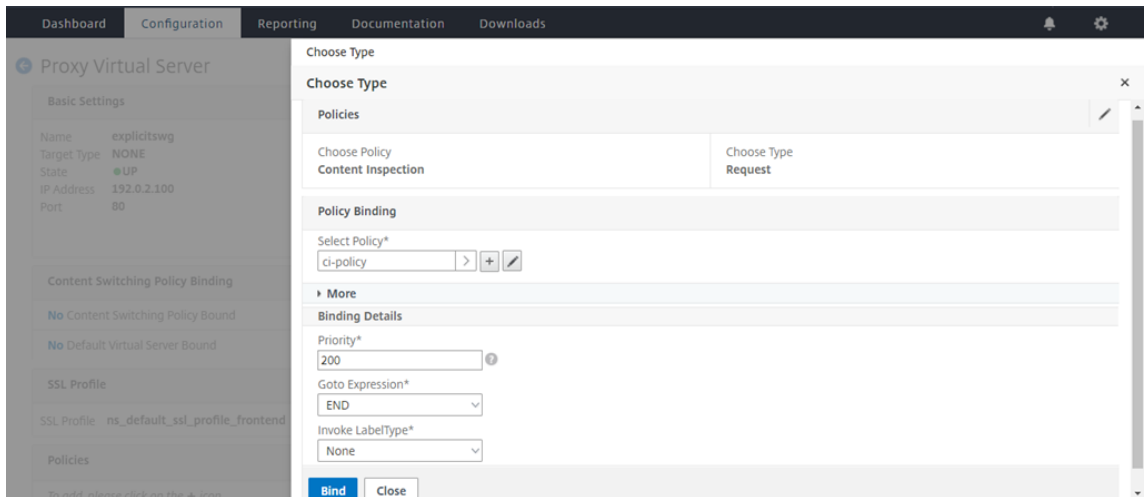
10. [作成] をクリックします。

11. 「ICAP アクションの作成」 ページで、「作成」 をクリックします。

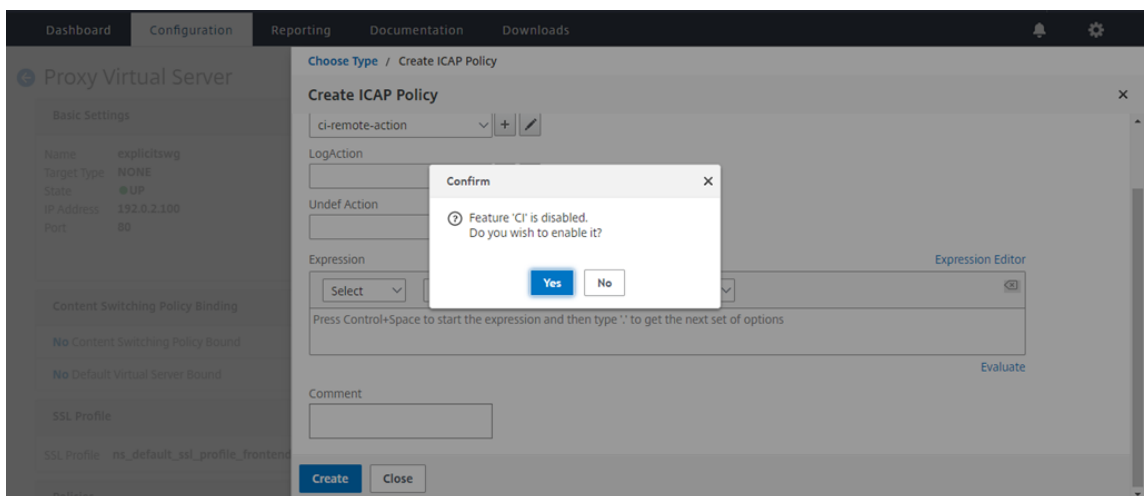
12. **ICAP** ポリシーの作成 ページで、式エディター に true と入力します。次に、[作成] をクリックします。



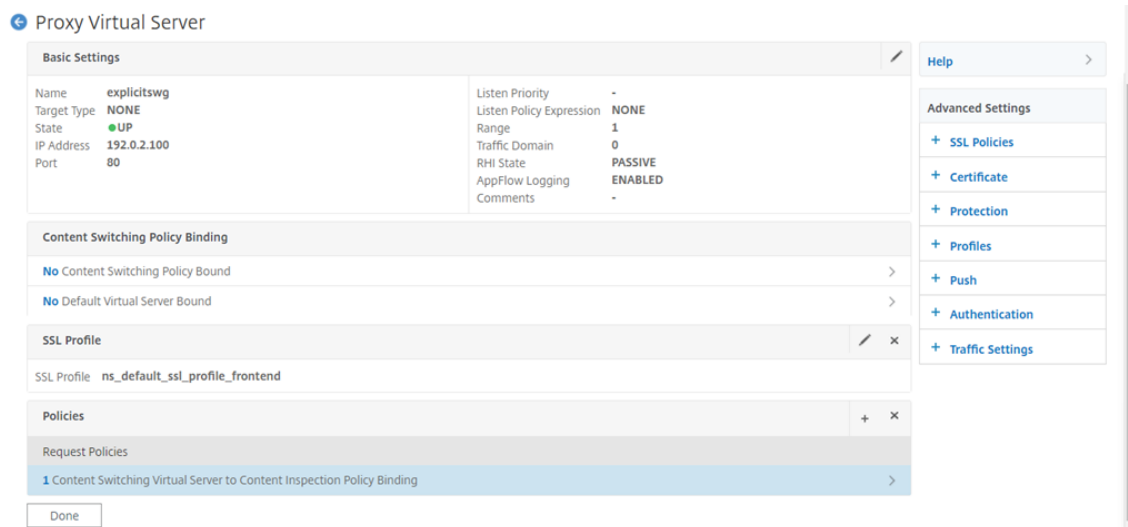
13. [バインド] をクリックします。



14. コンテンツ検査機能を有効にするように求められたら、[はい] を選択します。



15. [完了] をクリックします。



安全な ICAP

SWG アプライアンスと ICAP サーバー間の安全な接続を確立できます。これを行うには、TCP サービスの代わりに SSL_TCP サービスを作成します。SSL_TCP タイプの負荷分散仮想サーバーを構成します。ICAP サービスを負荷分散仮想サーバーにバインドします。

CLI を使用したセキュア ICAP の設定

コマンドプロンプトで、次のように入力します。

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

例:

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

GUI を使用したセキュア ICAP の設定

1. [負荷分散] > [仮想サーバー] に移動し、[追加] をクリックします。
2. 仮想サーバーの名前、IP アドレス、およびポートを指定します。SSL_TCP としてプロトコルを指定します。

3. **[OK]** をクリックします。
4. [負荷分散仮想サーバーサービスのバインド] セクション内をクリックして、ICAP サービスを追加します。
5. 「+」 をクリックしてサービスを追加します。
6. サービス名、IP アドレス、プロトコル (SSL_TCP)、およびポート (セキュア ICAP のデフォルトポートは 11344) を指定します。
7. **[OK]** をクリックします。
8. [完了] をクリックします。
9. [バインド] をクリックします。
10. [続行] を 2 回クリックします
11. [完了] をクリックします。

制限事項

次の機能はサポートされていません。

- ICAP 応答キャッシング。
- X-認証ユーザー URI ヘッダーを挿入しています。
- RESPMOD の ICAP 要求に HTTP 要求を挿入します。

インラインデバイスとして **IPS** または **NGFW** との統合

May 1, 2021

侵入防止システム (IPS) や次世代ファイアウォール (NGFW) などのセキュリティデバイスは、ネットワーク攻撃からサーバーを保護します。これらのデバイスはライブトラフィックを検査でき、通常はレイヤ 2 インラインモードで展開されます。Citrix Secure Web Gateway (SWG) は、インターネット上のリソースにアクセスする際に、ユーザーとエンタープライズネットワークのセキュリティを提供します。

Citrix SWG アプライアンスは、1 つ以上のインラインデバイスと統合して、脅威を防止し、高度なセキュリティ保護を提供します。インラインデバイスには、IPS や NGFW などの任意のセキュリティデバイスを使用できます。

Citrix SWG アプライアンスおよびインラインデバイス統合を使用すると、次のようなユースケースが利用できます。

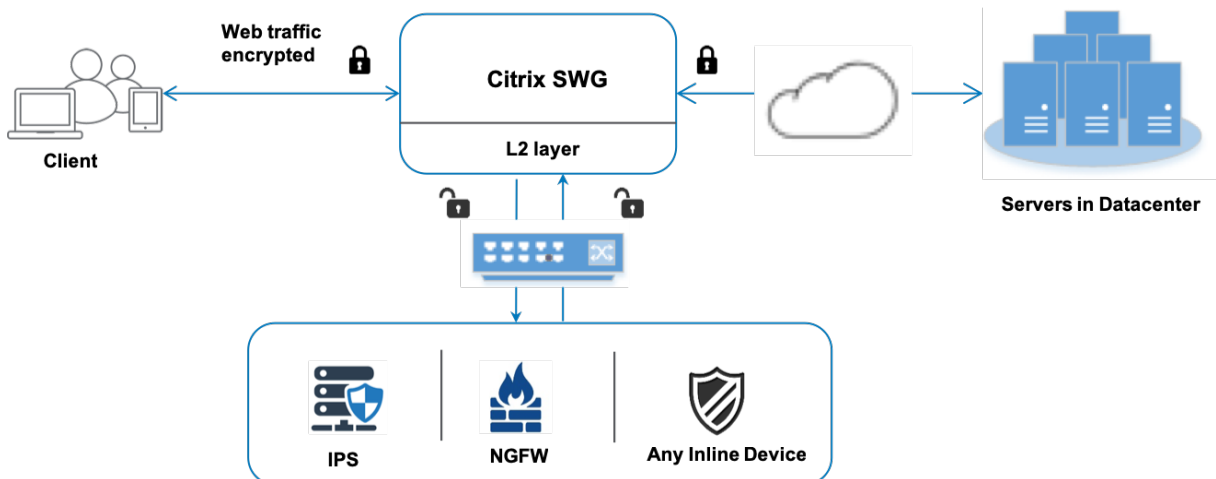
- **暗号化されたトラフィックの検査:** ほとんどの IPS および NGFW アプライアンスは暗号化されたトラフィックをバイパスするため、サーバーが攻撃に対して脆弱になる可能性があります。Citrix SWG アプライアンスは、トラフィックを復号化し、検査のためにインラインデバイスに送信できます。この統合により、お客様のネットワークセキュリティが強化されます。
- **TLS/SSL 処理からのインラインデバイスのオフロード:** TLS/SSL 処理はコストがかかり、IPS または NGFW アプライアンスがトラフィックを復号化すると CPU 使用率が高くなる可能性があります。Citrix SWG アプ

ライセンスは、TLS/SSL 処理をインラインデバイスからオフロードするのに役立ちます。その結果、インラインデバイスは大量のトラフィックを検査できます。

- インラインデバイスの負荷分散: 負荷の高いトラフィックを管理するために複数のインラインデバイスを構成した場合、Citrix SWG アプライアンスは、これらのデバイスにトラフィックを均等に分散してトラフィックを分散できます。
- トラフィックのスマート選択: アプライアンスは、検査のためにすべてのトラフィックをインラインデバイスに送信する代わりに、トラフィックのスマートな選択を行います。たとえば、インラインデバイスへの検査用のテキストファイルの送信はスキップされます。

インラインデバイスとの Citrix SWG の統合

次の図は、Citrix SWG がインラインセキュリティデバイスとどのように統合されているかを示しています。



インラインデバイスを Citrix SWG アプライアンスに統合すると、コンポーネントは次のように相互作用します。

1. クライアントが Citrix SWG アプライアンスに要求を送信します。
2. アプライアンスは、ポリシー評価に基づいてコンテンツ検査のためにデータをインラインデバイスに送信します。HTTPS トラフィックの場合、アプライアンスはデータを復号化し、コンテンツ検査のためにプレーンテキストでインラインデバイスに送信します。

注:

2 つ以上のインラインデバイスがある場合、アプライアンスはデバイスの負荷分散を行い、トラフィックを送信します。

3. インラインデバイスは、データの脅威を検査し、データをドロップ、リセット、またはアプライアンスに戻すかどうかを決定します。
4. セキュリティ上の脅威がある場合、デバイスはデータを修正してアプライアンスに送信します。

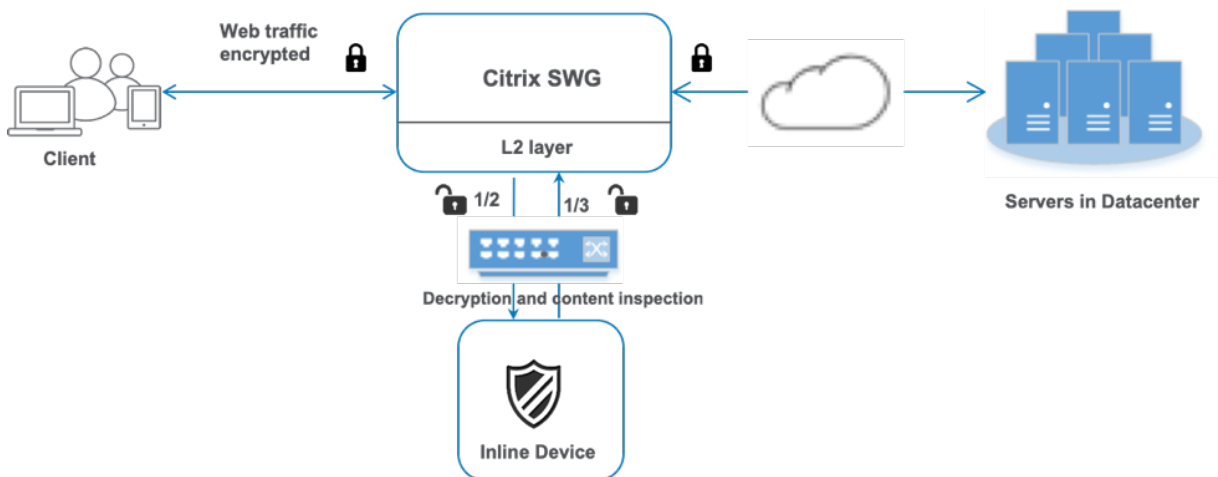
5. HTTPS トラフィックの場合、アプライアンスはデータを再暗号化し、要求をバックエンドサーバーに転送します。
6. バックエンドサーバーは応答をアプライアンスに送信します。
7. アプライアンスは再びデータを復号化し、検査のためにインラインデバイスに送信します。
8. インラインデバイスがデータを検査します。セキュリティ上の脅威がある場合、デバイスはデータを修正してアプライアンスに送信します。
9. アプライアンスはデータを再暗号化し、応答をクライアントに送信します。

インラインデバイス統合の設定

インラインデバイスを持つ Citrix SWG アプライアンスは、次の 3 つの異なる方法で構成できます。

シナリオ 1: 単一のインラインデバイスを使用する

セキュリティデバイス（IPS または NGFW）をインラインモードで統合するには、SWG アプライアンスでグローバルモードでコンテンツ検査と MAC ベース転送（MBF）を有効にする必要があります。次に、コンテンツインスペクションプロファイル、TCP サービス、インラインデバイスのコンテンツインスペクションアクションを追加して、インスペクションに基づいてトラフィックをリセット、ブロック、またはドロップします。また、インラインデバイスに送信するトラフィックのサブセットを決定するためにアプライアンスが使用するコンテンツ検査ポリシーを追加します。最後に、サーバ上でレイヤ 2 接続を有効にしてプロキシ仮想サーバを設定し、コンテンツ検査ポリシーをこのプロキシ仮想サーバにバインドします。



次の手順を実行します。

1. MAC ベース転送（MPF）モードを有効にします。
2. コンテンツ検査機能を有効にします。

3. サービスのコンテンツ検査プロファイルを追加します。コンテンツインスペクションプロファイルには、SWG アプライアンスとインラインデバイスを統合するインラインデバイス設定が含まれます。

4. (任意) TCP モニタを追加します。

注:

トランスペアレントデバイスには IP アドレスがありません。したがって、ヘルスチェックを実行するには、モニターを明示的にバインドする必要があります。

5. サービスを追加します。サービスは、インラインデバイスを表します。
6. (任意) サービスを TCP モニタにバインドします。
7. サービスのコンテンツインスペクションアクションを追加します。
8. コンテンツ検査ポリシーを追加し、アクションを指定します。
9. HTTP または HTTPS プロキシ (コンテンツスイッチング) 仮想サーバーを追加します。
10. コンテンツ検査ポリシーを仮想サーバにバインドします。

CLI を使用した設定 コマンドプロンプトで次のコマンドを入力します。例はほとんどのコマンドの後に示されています。

1. MBF を有効にします。

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

2. 本機能を有効にします。

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

3. コンテンツ検査プロファイルを追加します。

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

例:

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

4. サービスを追加します。インラインデバイスを含むどのデバイスにも所有されていないダミー IP アドレスを指定します。 `use source IP address (USIP)` を YES に設定します。 `useproxyport` を NO に

設定します。ヘルスマニタの電源を切ります。このサービスを TCP モニターにバインドする場合のみ、ヘルスマニタリングをオンにします。モニタをサービスにバインドする場合は、モニタの TRANSPARENT オプションを ON に設定します。

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

例:

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

5. コンテンツインスペクションアクションを追加します。

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

例:

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

6. コンテンツ検査ポリシーを追加します。

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

例:

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

7. プロキシ仮想サーバーを追加します。

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

例:

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

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

8. ポリシーを仮想サーバにバインドします。

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

例:

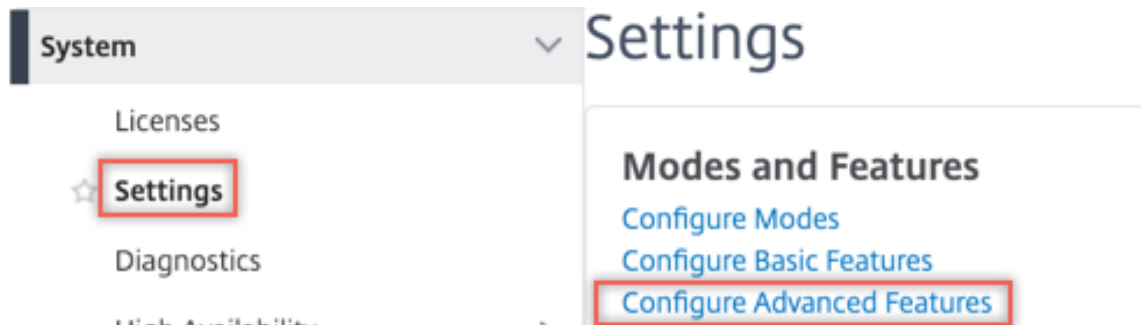
```
1 bind cs vserver explicitcs -policyName ips_pol -priority 1 -
  gotoPriorityExpression END -type REQUEST
2 <!--NeedCopy-->
```

GUI を使用した設定

1. **System > Settings** に移動します。[モードと機能] で、[モードの構成] をクリックします。

The screenshot shows the Citrix Secure Web Gateway GUI. In the top left, there is a search bar labeled 'Search in Menu'. The main navigation area shows 'System' selected, with a dropdown menu containing 'Licenses' and 'Settings' (highlighted with a red box). To the right, the 'Settings' page is displayed, with 'Modes and Features' selected, and a 'Configure Modes' link (highlighted with a red box) is visible. Below this, the 'Configure Modes' dialog box is shown, featuring a list of configuration options. The 'MAC based forwarding' option is checked and highlighted with a red box. Other checked options include 'Layer 3 Mode (IP Forwarding)', 'Use Subnet IP', and 'ULFD'. At the bottom of the dialog, there are 'OK' and 'Close' buttons.

2. **System > Settings** に移動します。[モードと機能] で、[高度な機能の構成] をクリックします。

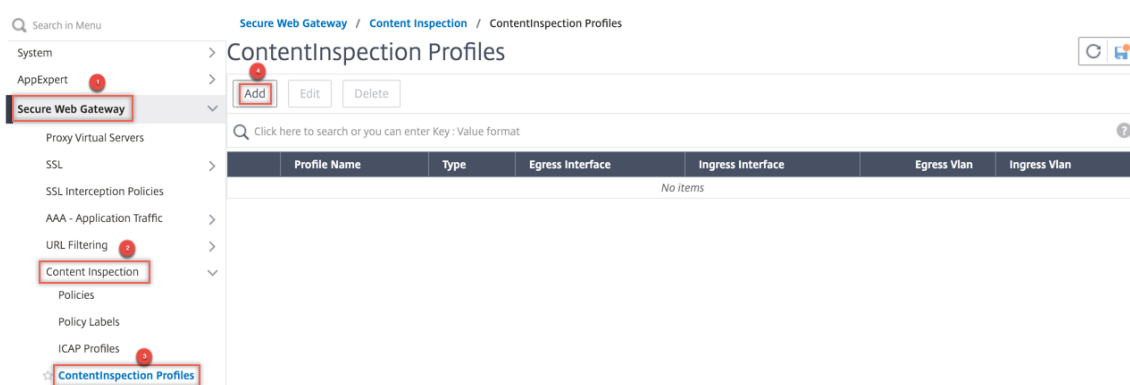


← Configure Advanced Features

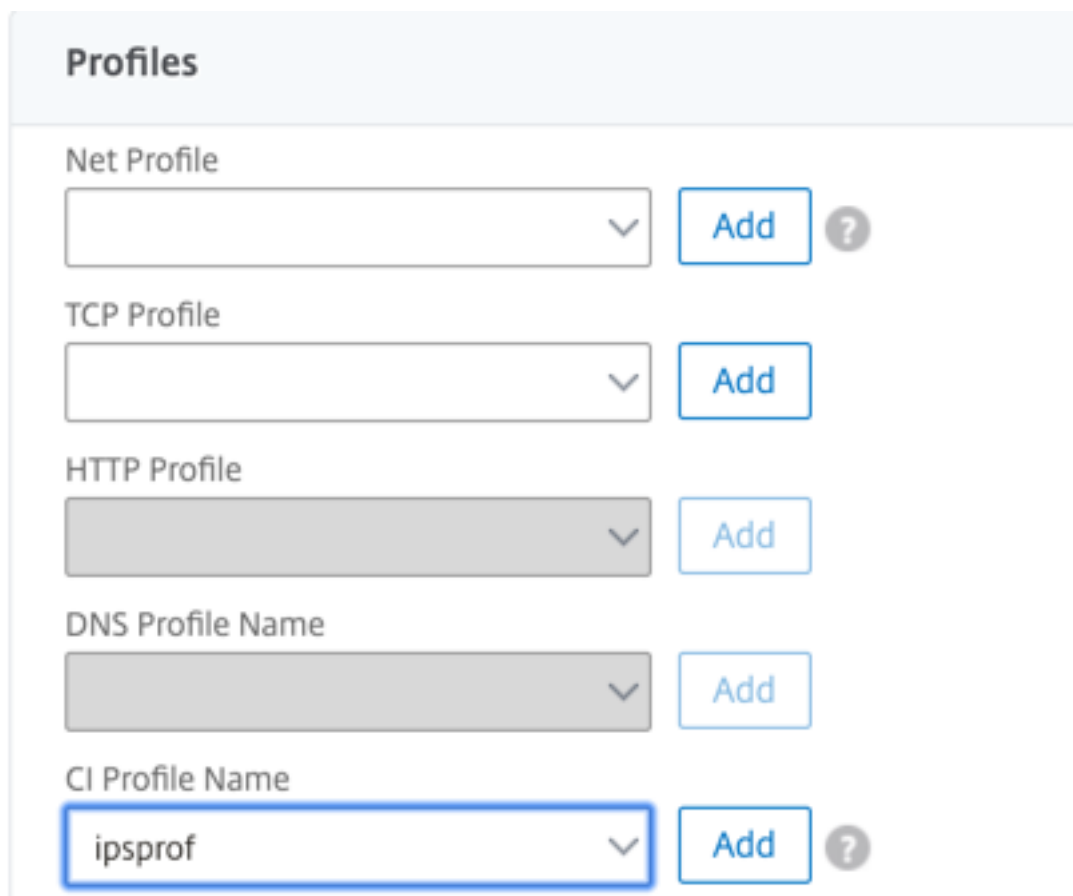
<input type="checkbox"/> Surge Protection	<input type="checkbox"/> Sure Connect
<input type="checkbox"/> Priority Queuing	<input type="checkbox"/> Http Dos Protection
<input type="checkbox"/> Cache Redirection	<input type="checkbox"/> Global Server Load Balancing
<input type="checkbox"/> Web Logging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

OK Close

3. **[Secure Web Gateway] > [コンテンツ検査] > [コンテンツ検査プロファイル]** に移動します。[追加] をクリックします。



4. [負荷分散] > [サービス] > [サービスの追加と追加] に移動します。[詳細設定] で、[プロファイル] をクリックします。[CI プロファイル名] リストで、以前に作成したコンテンツ検査プロファイルを選択します。[サービス設定] で、[ソース IP アドレスを使用] を [はい]、[プロキシポートを使用] を [いいえ] に設定します。[基本設定] で、[ヘルスマonitoring] を [いいえ] に設定します。このサービスを TCP モニターにバインドする場合のみ、ヘルスマonitoring をオンにします。モニタをサービスにバインドする場合は、モニタの TRANSPARENT オプションを ON に設定します。



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

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

5. [Secure Web Gateway] > [プロキシ仮想サーバー] > [追加] に移動します。名前、IP アドレス、およびポートを指定します。[詳細設定] で、[ポリシー] を選択します。「+」記号をクリックします。

← Proxy Virtual Server

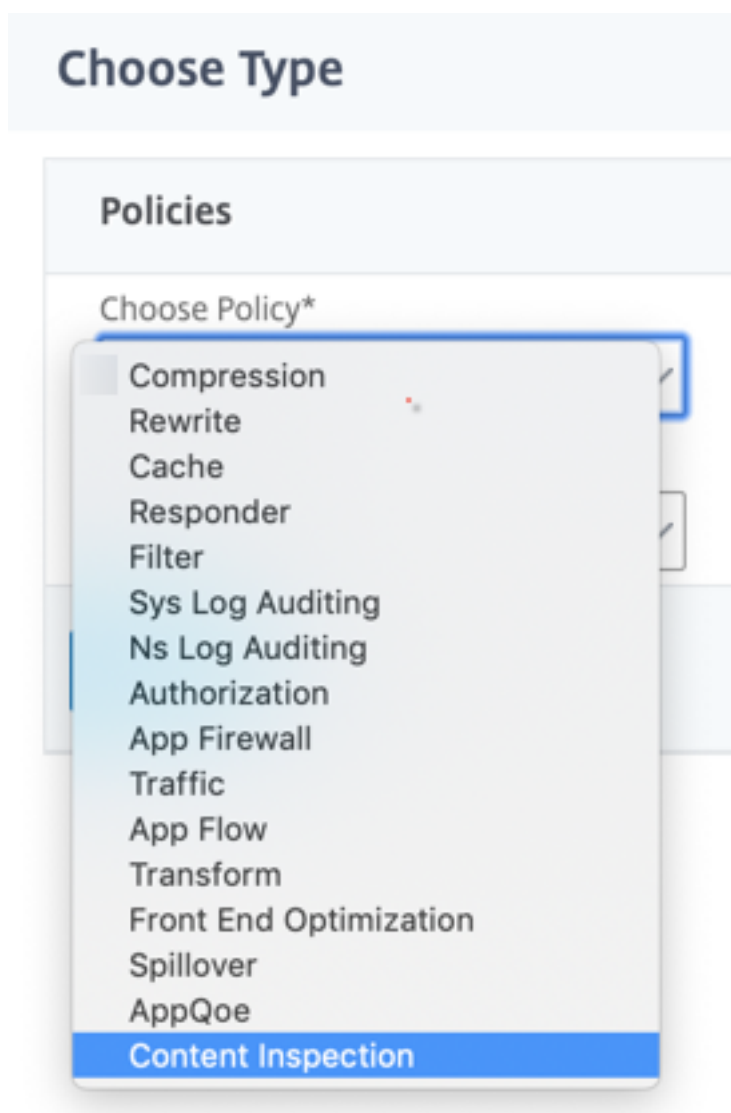
Basic Settings	
Name	proxysvr
State	● UP
IP Address	198.51.200.2
Port	80
Listen Priority	-
Listen Policy Expression	NONE
Range	1
IPset	-
Traffic Domain	0
RHI State	PASSIVE
AppFlow Logging	ENABLED
Comments	-

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

Certificate	
No Server Certificate	>
No CA Certificate	>

Policies	
	+ ×

6. [ポリシーの選択] で [コンテンツ検査] を選択します。[続行] をクリックします。



7. [追加] をクリックします。名前を指定します。「アクション」で、「追加」をクリックします。

[Choose Type](#) / Create ContentInspection Policy

Create ContentInspection Policy

Policy Name*

Action*

Log Action

UNDEF Action

- 名前を指定します。「タイプ」で「**INLINEINSPECTION**」を選択します。「サーバー名」で、以前に作成した TCP サービスを選択します。

← Create ContentInspection Action

Name*

Type*

Server Name*

If Server Down

Request-Timeout

Request timeout action

9. [作成] をクリックします。ルールを指定し、[Create] をクリックします。

Configure ContentInspection Policy

Policy Name
ips_pol

Action*
ips_action [Add] [Edit]

Log Action
[Add] [Edit]

UNDEF Action
[Add] [Edit]

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

Comment
[Text Area]

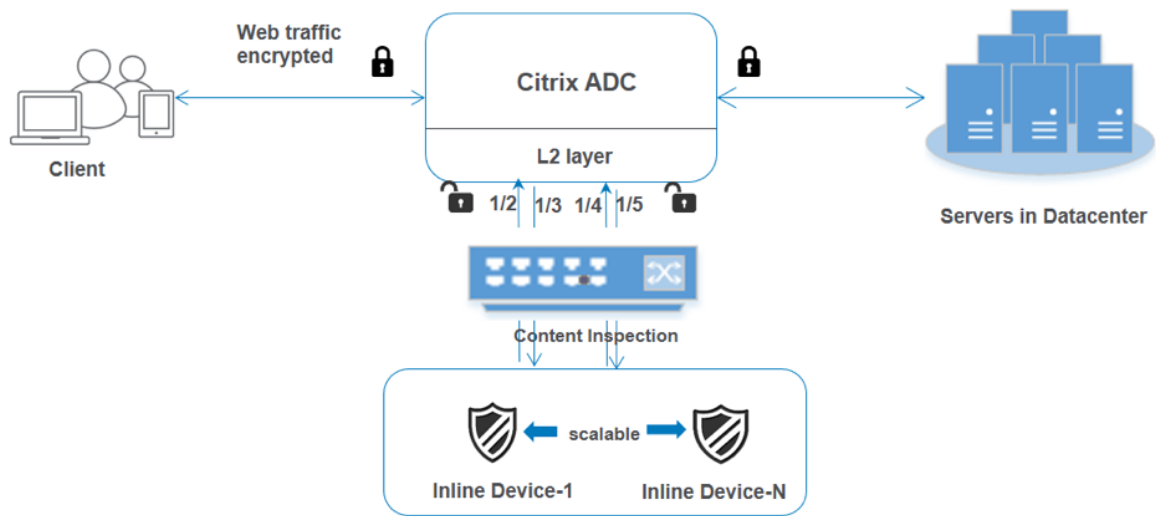
[OK] [Close]

10. [バインド] をクリックします。

11. [完了] をクリックします。

シナリオ 2: 専用インターフェイスを持つ複数のインラインデバイスの負荷分散

2 つ以上のインラインデバイスを使用している場合は、専用のインターフェイスで異なるコンテンツインスペクションサービスを使用して、デバイスを負荷分散できます。この場合、Citrix SWG アプライアンスは、専用インターフェイスを介して各デバイスに送信されるトラフィックのサブセットの負荷分散を行います。サブセットは、設定されたポリシーに基づいて決定されます。たとえば、TXT ファイルやイメージファイルは、検査のためにインラインデバイスに送信されない場合があります。



基本設定は、シナリオ 1 と同じままです。ただし、インラインデバイスごとにコンテンツ検査プロファイルを作成し、各プロファイルで入力および出力インターフェイスを指定する必要があります。インラインデバイスごとにサービスを追加します。負荷分散仮想サーバを追加し、コンテンツインスペクションアクションで指定します。次の追加手順を実行します。

1. サービスごとにコンテンツ検査プロファイルを追加します。
2. デバイスごとにサービスを追加します。
3. 負荷分散仮想サーバを追加します。
4. コンテンツインスペクションアクションで負荷分散仮想サーバを指定します。

CLI を使用した設定 コマンドプロンプトで次のコマンドを入力します。各コマンドの後に例が示されています。

1. MBF を有効にします。

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

2. 本機能を有効にします。

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

3. サービス 1 のプロファイル 1 を追加します。

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

例:

```

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

```

4. サービス 2 のプロファイル 2 を追加します。

```

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

```

例:

```

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

```

5. サービス 1 を追加します。インラインデバイスを含むどのデバイスにも所有されていないダミー IP アドレスを指定します。use source IP address (USIP) を YES に設定します。useproxyport を NO に設定します。ヘルスマニタの電源を切ります。このサービスを TCP モニターにバインドする場合のみ、ヘルスマニタリングをオンにします。モニタをサービスにバインドする場合は、モニタの TRANSPARENT オプションを ON に設定します。

```

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

```

例:

```

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

```

6. サービス 2 を追加します。インラインデバイスを含むどのデバイスにも所有されていないダミー IP アドレスを指定します。use source IP address (USIP) を YES に設定します。useproxyport を NO に設定します。ヘルスマニタの電源を切ります。このサービスを TCP モニターにバインドする場合のみ、ヘルスマニタリングをオンにします。モニタをサービスにバインドする場合は、モニタの TRANSPARENT オプションを ON に設定します。

```

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

```

例:

```

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

```

7. 負荷分散仮想サーバーを追加します。

```

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

```

例:

```

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

```

8. サービスを負荷分散仮想サーバーにバインドします。

```

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

```

例:

```

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

```

9. コンテンツインスペクションアクションで負荷分散仮想サーバを指定します。

```

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

```

例:

```

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

```

10. コンテンツ検査ポリシーを追加します。ポリシーでコンテンツインスペクションアクションを指定します。

```

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

```

例:

```

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

```

11. プロキシ仮想サーバーを追加します。

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

例:

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

12. コンテンツ検査ポリシーを仮想サーバにバインドします。

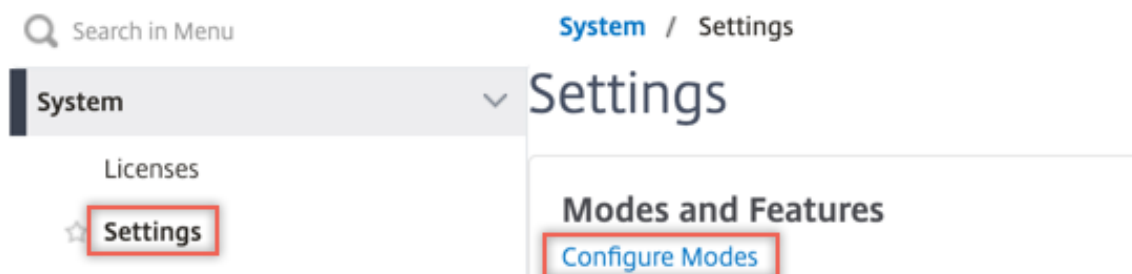
```
1 bind cs vserver <name> -policyName <string> -priority <
  positive_integer> -gotoPriorityExpression <expression> -type
  REQUEST
2 <!--NeedCopy-->
```

例:

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

GUI を使用した設定

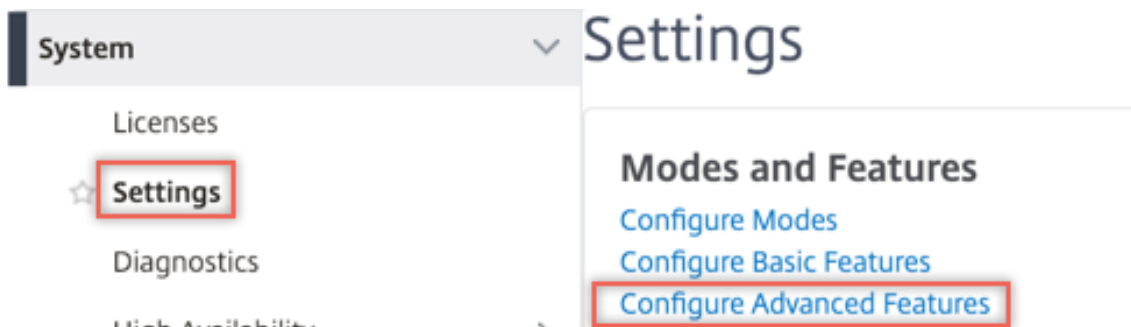
1. **System > Settings** に移動します。[モードと機能] で、[モードの構成] をクリックします。



← Configure Modes

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

2. **System > Settings** に移動します。[モードと機能] で、[高度な機能の構成] をクリックします。



← Configure Advanced Features

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

OK Close

3. [Secure Web Gateway] > [コンテンツ検査] > [コンテンツ検査プロファイル] に移動します。[追加] をクリックします。

Secure Web Gateway / Content Inspection / ContentInspection Profiles

ContentInspection Profiles

Add Edit Delete

Click here to search or you can enter Key: Value format

Profile Name	Type	Egress Interface	Ingress Interface	Egress Vlan	Ingress Vlan
No items					

入力および出カインターフェイスを指定します。

← Create ContentInspectionProfile

Profile Name*

Type*

Egress Interface*

Ingress Interface*

Egress Vlan

Ingress Vlan

2つのプロファイルを作成します。2番目のプロファイルで、異なる入力および出力インターフェイスを指定します。

4. [負荷分散] > [サービス] > [サービスの追加と追加] に移動します。[詳細設定] で、[プロファイル] をクリックします。[CI プロファイル名] リストで、以前に作成したコンテンツ検査プロファイルを選択します。[サービス設定] で、[ソース IP アドレスを使用] を [はい]、[プロキシポートを使用] を [いいえ] に設定します。[基本設定] で、[ヘルスマモニタリング] を [いいえ] に設定します。このサービスを TCP モニターにバインドする場合のみ、ヘルスマモニタリングをオンにします。モニタをサービスにバインドする場合は、モニタの TRANSPARENT オプションを ON に設定します。

Profiles

Net Profile
 Add ?

TCP Profile
 Add

HTTP Profile
 Add

DNS Profile Name
 Add

CI Profile Name
 Add ?

Service Settings

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

Basic Settings

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

2つのサービスを作成します。インラインデバイスを含むどのデバイスにも所有されていないダミー IP アドレスを指定します。

5. [負荷分散] > [仮想サーバー] > [追加] に移動します。TCP 負荷分散仮想サーバーを作成します。

Load Balancing Virtual Server

Basic Settings

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

Name*

Protocol*

IP Address Type*

IP Address*

Port*

▶ More

[OK] をクリックします。

6. [負荷分散仮想サーバーサービスのバインド] セクション内をクリックします。「サービス・バインド」で、「サービスの選択」の矢印をクリックします。前に作成した2つのサービスを選択し、[Select] をクリックします。[バインド] をクリックします。

Service Binding

Select Service*

Binding Details

Weight

Service Binding / Service

Service

Select Add Edi

🔍 Click here to search or you can en

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

Service Binding

Service Binding

Select Service*

ips_service1, ips_service2 > Add Edit ?

Binding Details

Weight

1

Bind Close

7. [Secure Web Gateway] > [プロキシ仮想サーバー] > [追加] に移動します。名前、IP アドレス、およびポートを指定します。[詳細設定] で、[ポリシー] を選択します。「+」記号をクリックします。

← Proxy Virtual Server

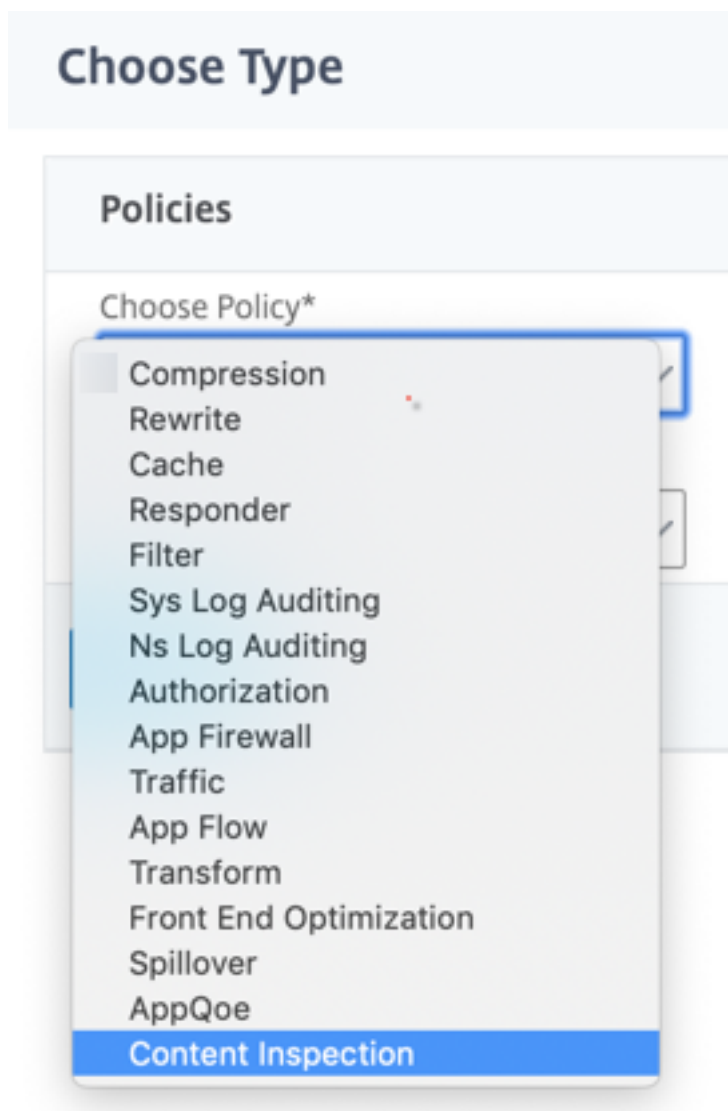
Basic Settings	
Name	proxyvsvr
State	● UP
IP Address	198.51.200.2
Port	80
Listen Priority	-
Listen Policy Expression	NONE
Range	1
IPset	-
Traffic Domain	0
RHI State	PASSIVE
AppFlow Logging	ENABLED
Comments	-

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

Certificate	
No Server Certificate	>
No CA Certificate	>

Policies	
	+ x

8. [ポリシーの選択] で [コンテンツ検査] を選択します。[続行] をクリックします。



9. [追加] をクリックします。名前を指定します。「アクション」で、「追加」をクリックします。

[Choose Type](#) / Create ContentInspection Policy

Create ContentInspection Policy

Policy Name*

Action*

Log Action

UNDEF Action

- 名前を指定します。「タイプ」で「**INLINEINSPECTION**」を選択します。「サーバー名」で、以前に作成した負荷分散仮想サーバーを選択します。

← Create ContentInspection Action

Name*

Type*

Server Name*

If Server Down

Request-Timeout

Request timeout action

11. [作成] をクリックします。ルールを指定し、[Create] をクリックします。

Configure ContentInspection Policy

Policy Name
ips_pol

Action*
ips_action [Add] [Edit]

Log Action
[Add] [Edit]

UNDEF Action
[Add] [Edit]

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

Comment

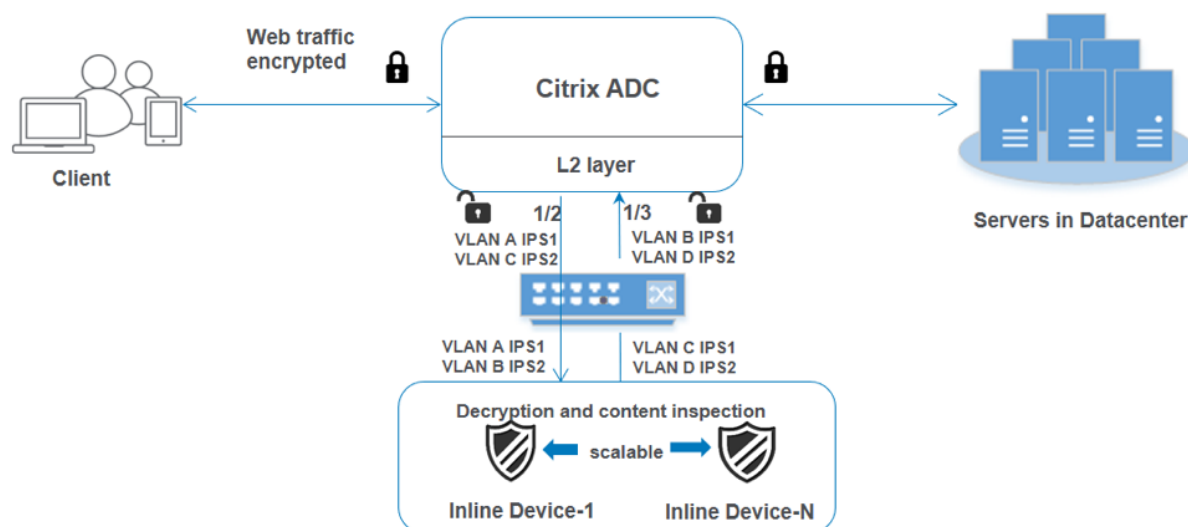
[OK] [Close]

12. [バインド] をクリックします。

13. [完了] をクリックします。

シナリオ 3: 共有インターフェイスを持つ複数のインラインデバイスの負荷分散

2 つ以上のインラインデバイスを使用している場合は、共有インターフェイスで異なるコンテンツインスペクションサービスを使用して、デバイスを負荷分散できます。この場合、Citrix SWG アプライアンスは、共有インターフェイスを介して各デバイスに送信されるトラフィックのサブセットの負荷分散を行います。サブセットは、設定されたポリシーに基づいて決定されます。たとえば、TXT ファイルやイメージファイルは、検査のためにインラインデバイスに送信されない場合があります。



基本設定は、シナリオ 2 と同じままです。このシナリオでは、インターフェイスを異なる VLAN にバインドして、各インラインデバイスのトラフィックを分離します。コンテンツインスペクションプロファイルで VLAN を指定します。次の追加手順を実行します。

1. 共有インターフェイスを異なる VLAN にバインドします。
2. コンテンツ検査プロファイルで入力 VLAN と出力 VLAN を指定します。

CLI を使用した設定 コマンドプロンプトで次のコマンドを入力します。各コマンドの後に例が示されています。

1. MBF を有効にします。

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

2. 本機能を有効にします。

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

3. 共有インターフェイスを異なる VLAN にバインドします。

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

例:

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

4. サービス 1 のプロファイル 1 を追加します。プロファイルで入力 VLAN と出力 VLAN を指定します。

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

例:

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

5. サービス 2 のプロファイル 2 を追加します。プロファイルで入力 VLAN と出力 VLAN を指定します。

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

例:

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

6. サービス 1 を追加します。

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

例:

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

7. サービス 2 を追加します。

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

例:

```

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

```

8. 負荷分散仮想サーバーを追加します。

```

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

```

例:

```

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

```

9. サービスを負荷分散仮想サーバーにバインドします。

```

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

```

例:

```

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

```

10. コンテンツインスペクションアクションで負荷分散仮想サーバを指定します。

```

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

```

例:

```

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

```

11. コンテンツ検査ポリシーを追加します。ポリシーでコンテンツインスペクションアクションを指定します。

```

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

```

例:

```

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

```

12. プロキシ仮想サーバーを追加します。

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

例:

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

13. コンテンツ検査ポリシーを仮想サーバにバインドします。

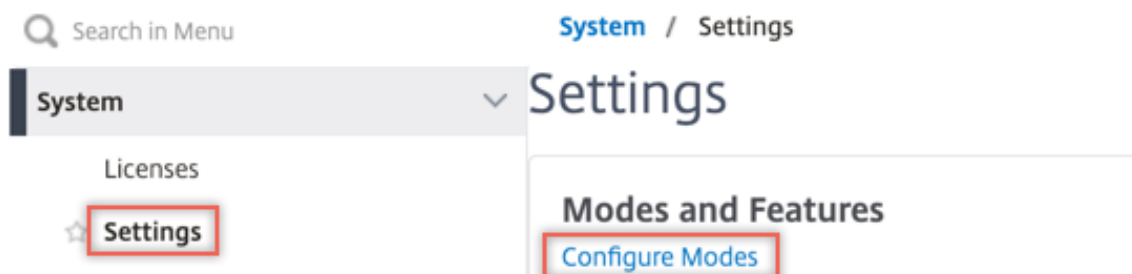
```
1 bind cs vserver <name> -policyName <string> -priority <
  positive_integer> -gotoPriorityExpression <expression> -type
  REQUEST
2 <!--NeedCopy-->
```

例:

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

GUI を使用した設定

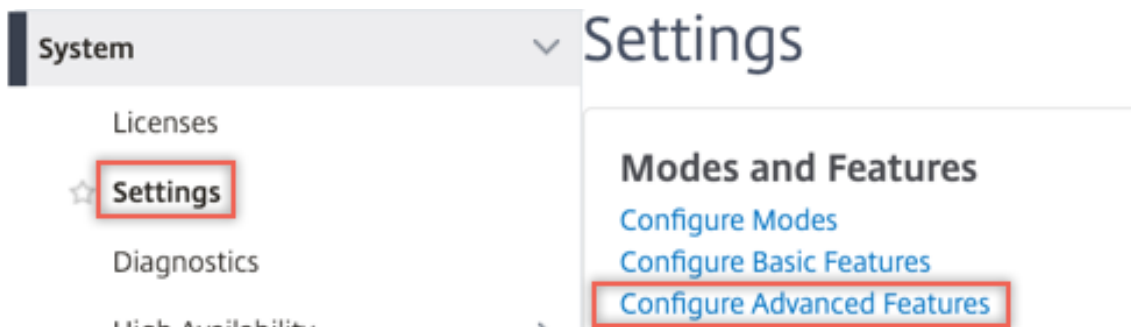
1. **System > Settings** に移動します。[モードと機能] で、[モードの構成] をクリックします。



← Configure Modes

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

2. **System > Settings** に移動します。[モードと機能] で、[高度な機能の構成] をクリックします。



← Configure Advanced Features

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

3. [システム] > [ネットワーク] > [VLAN] > [追加] に移動します。4つのVLANを追加し、インターフェイスにタグを付けます。

← Create VLAN

VLAN ID*

100 ?

Alias Name

Maximum Transmission Unit

- Dynamic Routing
- IPv6 Dynamic Routing
- Partitions Sharing

Interface Bindings

IP Bindings

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

← Create VLAN

VLAN ID*



Alias Name

Maximum Transmission Unit

- Dynamic Routing
- IPv6 Dynamic Routing
- Partitions Sharing

Interface Bindings

IP Bindings

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

← Create VLAN

VLAN ID*

300



Alias Name

Maximum Transmission Unit

- Dynamic Routing
- IPv6 Dynamic Routing
- Partitions Sharing

Interface Bindings

IP Bindings

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

← Create VLAN

VLAN ID*

 ?

Alias Name

Maximum Transmission Unit

Dynamic Routing

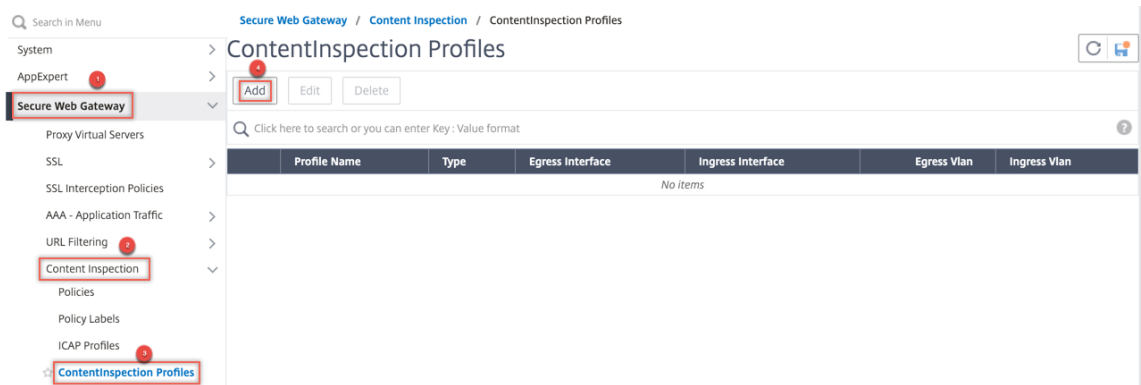
IPv6 Dynamic Routing

Partitions Sharing

Interface Bindings IP Bindings

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

4. **[Secure Web Gateway]** > **[コンテンツ検査]** > **[コンテンツ検査プロファイル]** に移動します。[追加] をクリックします。



入力 VLAN と出力 VLAN を指定します。

← Create ContentInspectionProfile

Profile Name*

Type*

Egress Interface*

Ingress Interface*

Egress Vlan

Ingress Vlan

別のプロファイルを作成します。2 番目のプロファイルで異なる入力 VLAN と出力 VLAN を指定します。

← Create ContentInspectionProfile

Profile Name*

Type*

Egress Interface*

Ingress Interface*

Egress Vlan

Ingress Vlan

5. [負荷分散] > [サービス] > [サービスの追加と追加] に移動します。[詳細設定] で、[プロファイル] をクリックします。[CI プロファイル名] リストで、以前に作成したコンテンツ検査プロファイルを選択します。[サービス設定] で、[ソース IP アドレスを使用] を [はい]、[プロキシポートを使用] を [いいえ] に設定します。[基本設定] で、[ヘルスマモニタリング] を [いいえ] に設定します。

2 つのサービスを作成します。インラインデバイスを含むどのデバイスにも所有されていないダミー IP アドレスを指定します。サービス 1 でプロファイル 1 を指定し、サービス 2 でプロファイル 2 を指定します。

Profiles

Net Profile

 ?

TCP Profile

HTTP Profile

DNS Profile Name

CI Profile Name

 ?

Profiles

Net Profile

TCP Profile

HTTP Profile

DNS Profile Name

CI Profile Name

Service Settings

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

Basic Settings

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

6. [負荷分散] > [仮想サーバー] > [追加] に移動します。TCP 負荷分散仮想サーバーを作成します。

Load Balancing Virtual Server

Basic Settings

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

Name*

Protocol*

IP Address Type*

IP Address*

Port*

▶ More

[OK] をクリックします。

7. [負荷分散仮想サーバーサービスのバインド] セクション内をクリックします。「サービス・バインド」で、「サービスの選択」の矢印をクリックします。前に作成した2つのサービスを選択し、[Select] をクリックします。[バインド] をクリックします。

Service Binding

Select Service*

Binding Details

Weight

Service Binding / Service

Service

Select Add Edit

🔍 Click here to search or you can enter a filter

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

Service Binding

Service Binding

Select Service*

ips_service1, ips_service2 > Add Edit ?

Binding Details

Weight

1

Bind Close

8. [Secure Web Gateway] > [プロキシ仮想サーバー] > [追加] に移動します。名前、IP アドレス、およびポートを指定します。[詳細設定] で、[ポリシー] を選択します。「+」記号をクリックします。

← Proxy Virtual Server

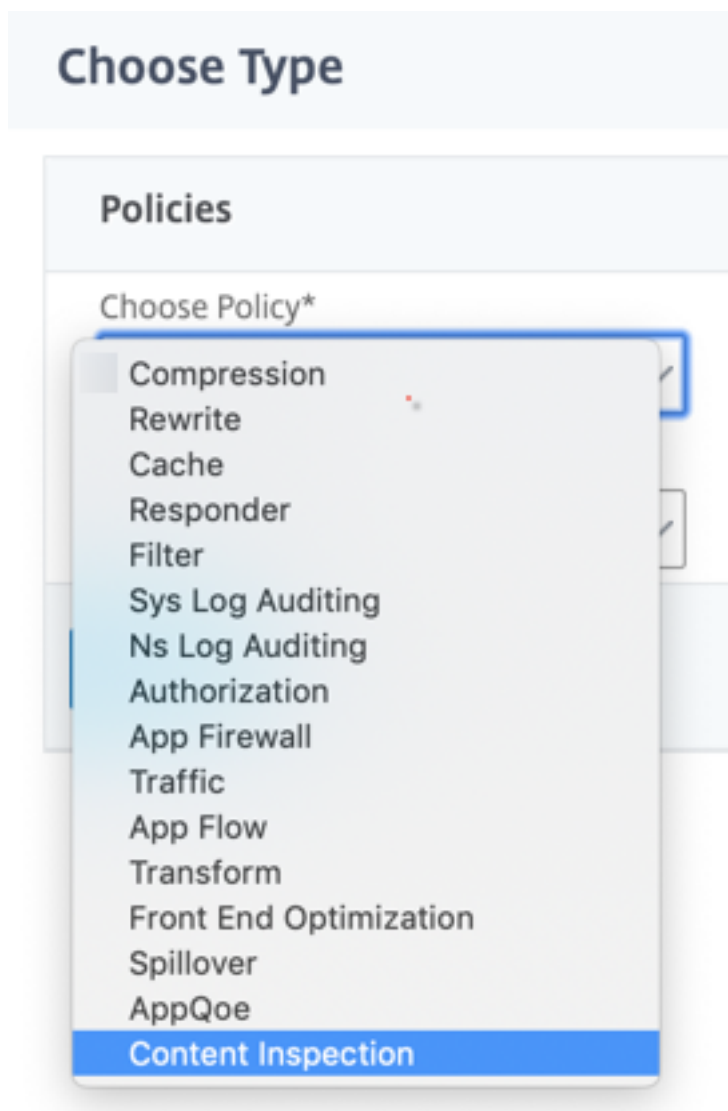
Basic Settings	
Name	proxysvr
State	● UP
IP Address	198.51.200.2
Port	80
Listen Priority	-
Listen Policy Expression	NONE
Range	1
IPset	-
Traffic Domain	0
RHI State	PASSIVE
AppFlow Logging	ENABLED
Comments	-

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

Certificate	
No Server Certificate	>
No CA Certificate	>

Policies	
	+ x

9. [ポリシーの選択] で [コンテンツ検査] を選択します。[続行] をクリックします。



10. [追加] をクリックします。名前を指定します。「アクション」で、「追加」をクリックします。

[Choose Type](#) / Create ContentInspection Policy

Create ContentInspection Policy

Policy Name*

Action*

Log Action

UNDEF Action

- 名前を指定します。「タイプ」で「**INLINEINSPECTION**」を選択します。「サーバー名」で、以前に作成した負荷分散仮想サーバーを選択します。

← Create ContentInspection Action

Name*

Type*

Server Name*

If Server Down

Request-Timeout

Request timeout action

12. [作成] をクリックします。ルールを指定し、[Create] をクリックします。

Configure ContentInspection Policy

Policy Name
ips_pol

Action*
ips_action Add Edit

Log Action
Add Edit

UNDEF Action

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

Comment

OK Close

13. [バインド] をクリックします。

14. [完了] をクリックします。

Analytics

May 1, 2021

Citrix SWG アプライアンスでは、すべてのユーザーレコードと後続のレコードがログに記録されます。Citrix Application Delivery Management (ADM) を Citrix SWG アプライアンスに統合すると、ログに記録されたユーザーアクティビティとアプライアンス内の後続のレコードは、ログストリームを使用して Citrix ADM にエクスポートされます。

Citrix ADM は、訪問した Web サイトや消費された帯域幅など、ユーザーのアクティビティに関する情報を照合して表示します。また、帯域幅の使用量と検出された脅威（マルウェアやフィッシングサイトなど）をレポートします。これらの主要なメトリックを使用して、ネットワークを監視し、Citrix SWG アプライアンスで修正アクションを実行できます。詳しくは、「[Citrix Secure Web Gateway 分析](#)」を参照してください。

Citrix SWG アプライアンスと Citrix ADM を統合するには：

1. Citrix SWG アプライアンスで、Secure Web Gateway を構成するときに、分析を有効にし、分析に使用する Citrix ADM インスタンスの詳細を指定します。

2. Citrix ADM で、Citrix SWG アプライアンスをインスタンスとして Citrix ADM に追加します。詳しくは、「[Citrix ADM への新しいインスタンスの追加](#)」を参照してください。

ユースケース: 企業のインターネットアクセスをコンプライアンスとセキュリティで保護する

May 1, 2021

金融組織のネットワークセキュリティのディレクターは、マルウェアの形で Web から来る外部の脅威から企業ネットワークを保護したいと考えています。これを行うには、ディレクターは、そうでなければ暗号化されたトラフィックをバイパスし、悪意のある Web サイトへのアクセスを制御することを可視化する必要があります。ディレクターは、次のことを行う必要があります。

- 企業ネットワークに出入りする SSL/TLS（暗号化されたトラフィック）を含むすべてのトラフィックを傍受し、調べます。
- ユーザーの財務情報や電子メールなどの機密情報を含むウェブサイトへのリクエストの傍受をバイパスします。
- 有害またはアダルトコンテンツを提供していると識別された有害な URL へのアクセスをブロックします。
- 悪意のある Web サイトにアクセスしている企業内のエンドユーザー（従業員）を特定し、これらのユーザーのインターネットアクセスをブロックするか、有害な URL をブロックします。

上記のすべてを実現するために、ディレクターは組織内のすべてのデバイスにプロキシを設定し、Citrix Secure Web Gateway (SWG) をポイントします。SWG (SWG) は、ネットワーク内でプロキシサーバーとして機能します。プロキシサーバーは、企業ネットワークを通過する暗号化および暗号化されていないすべてのトラフィックを代行受信します。ユーザ認証を要求し、トラフィックをユーザに関連付けます。URL カテゴリを指定して、違法/有害、アダルトサイト、マルウェアおよびスパム Web サイトへのアクセスをブロックすることができます。

上記を実現するには、次のエンティティを設定します。

- DNS ネームサーバーを使用してホスト名を解決します。
- サブネット IP (SNIP) アドレスを使用して、オリジナルサーバーとの接続を確立します。SNIP アドレスはインターネットにアクセスできる必要があります。
- エクスプリシットモードのプロキシサーバーで、すべてのアウトバウンド HTTP および HTTPS トラフィックを代行受信します。
- SSL プロファイルを使用して、接続の SSL 設定（暗号やパラメータなど）を定義します。
- SSL インターセプション用のサーバ証明書に署名するための CA 証明書とキーのペア。
- SSL ポリシーを使用して、傍受およびバイパスする Web サイトを定義します。
- 仮想サーバ、ポリシー、およびアクションを認証し、有効なユーザのみにアクセスを許可します。
- Appflow コレクターを使用して、Citrix Application Delivery Management (ADM) にデータを送信します。

この設定例では、CLI と GUI の両方の手順がリストされています。次のサンプル値が使用されます。IP アドレス、SSL 証明書とキー、および LDAP パラメータの有効なデータに置き換えます。

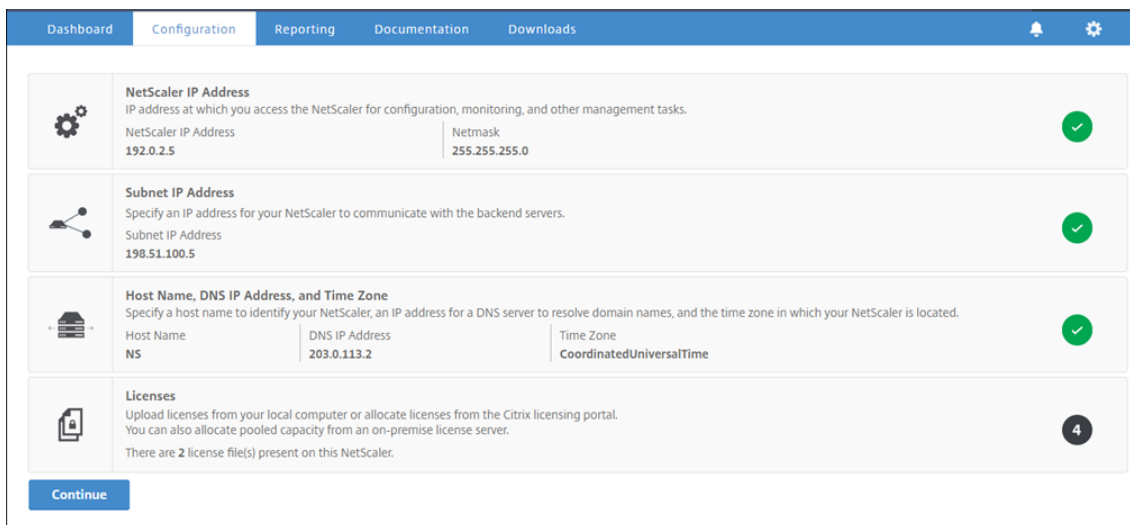
Name	サンプル設定で使用される値
NSIP アドレス	192.0.2.5
サブネット IP アドレス	198.51.100.5
LDAP 仮想サーバの IP アドレス	192.0.2.116
DNS ネームサーバの IP アドレス	203.0.113.2
プロキシサーバー IP アドレス	192.0.2.100
MAS IP アドレス	192.0.2.41
SSL インターセプション用の CA 証明書	ns-swg-ca-certkey (certificate: ns_swg_ca.crt and key: ns_swg_ca.key)
LDAP ベース DN	CN=Users,DC=CTXNSSFB,DC=COM
LDAP バインド DN	CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM
LDAP バインド DN パスワード	zzzzz

Secure Web Gateway ウィザードを使用して、企業ネットワークとの間で送受信されるトラフィックの代行受信と検査を設定します

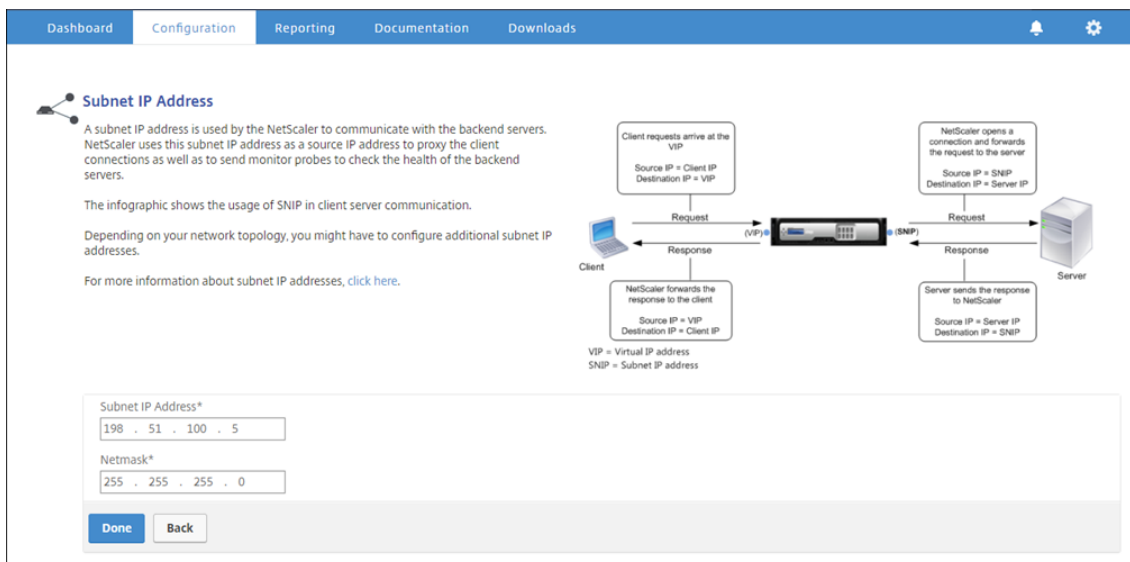
ネットワークとの間で送受信される他のトラフィックに加えて、暗号化されたトラフィックを傍受および検査するための設定を作成するには、プロキシ設定、SSLi 設定、ユーザ認証設定、および URL フィルタリング設定を構成する必要があります。次に、入力した値の例を示します。

SNIP アドレスと **DNS** ネームサーバーの構成

1. Web ブラウザで、NSIP アドレスを入力します。たとえば、<http://192.0.2.5>などです。
2. **[User Name]** ボックスと **[Password]** ボックスに管理者資格情報を入力します。次の画面が開きます。



3. [サブネット IP アドレス] セクションをクリックし、IP アドレスを入力します。



4. [完了] をクリックします。

5. [ホスト名]、[DNS IP アドレス]、[タイムゾーン] セクションをクリックし、これらのフィールドに値を入力します。

The screenshot shows the 'Host Name, DNS IP Address, and Time Zone' configuration page. The page has a blue header with navigation tabs: Dashboard, Configuration, Reporting, Documentation, and Downloads. Below the header, there is a title 'Host Name, DNS IP Address, and Time Zone' and a brief instruction: 'Specify a host name to identify your NetScaler. When you generate the Universal license for NetScaler Gateway, the host name is used in the license. Specify the IP address of a DNS server if you want to allocate your licenses from the Citrix licensing portal. Specify the time zone in which your NetScaler is located.' The form contains three input fields: 'Host Name' with the value 'NS', 'DNS IP Address' with the value '203 . 0 . 113 . 2', and 'Time Zone*' with a dropdown menu set to 'CoordinatedUniversalTime'. At the bottom of the form are two buttons: 'Done' and 'Back'.

6. [完了]、[続行] の順にクリックします。

プロキシ設定を構成する

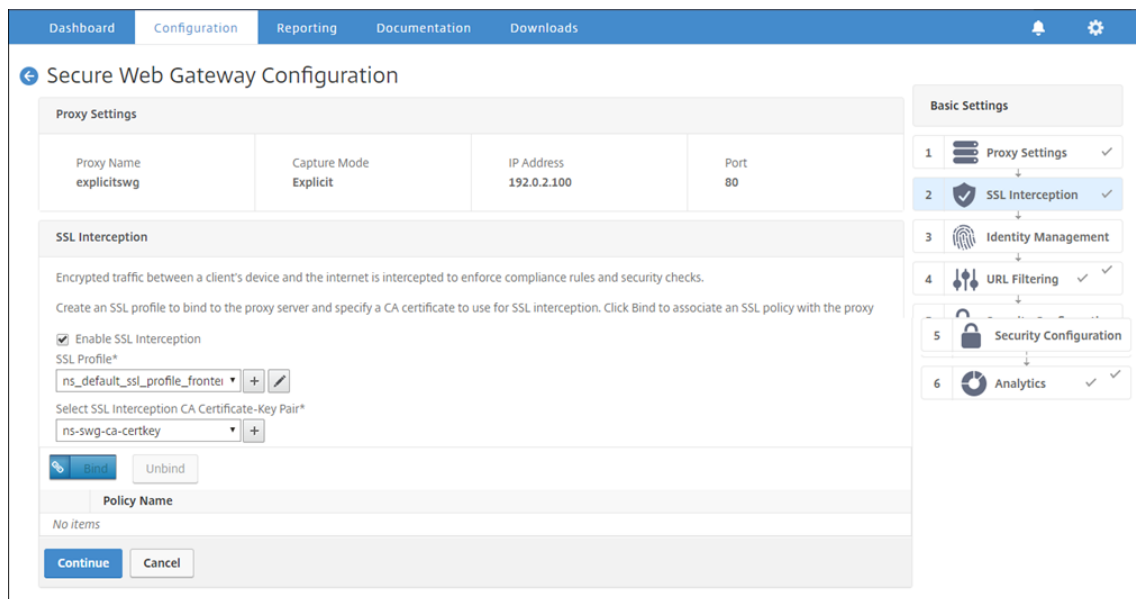
1. [**Secure Web Gateway**] > [**Secure Web Gateway ウィザード**] に移動します。
2. [はじめに] をクリックし、[続行] をクリックします。
3. [プロキシ設定] ダイアログボックスで、明示的なプロキシサーバーの名前を入力します。
4. [キャプチャモード] で、[明示的] を選択します。
5. IP アドレスとポート番号を入力します。

The screenshot shows the 'Secure Web Gateway Configuration' page. The page has a blue header with navigation tabs: Dashboard, Configuration, Reporting, Documentation, and Downloads. Below the header, there is a title 'Secure Web Gateway Configuration' and a sub-section 'Proxy Settings'. The 'Proxy Settings' section contains a brief instruction: 'Configure a proxy server in transparent or explicit mode. In transparent proxy mode, configuring a proxy on a client's device is not required. In explicit proxy mode, all client requests are sent to either an IP address that the clients configure in their browsers or an IP address that the organization pushes to the clients' devices.' The form contains four input fields: 'Name*' with the value 'explicitswg', 'Capture Mode*' with a dropdown menu set to 'Explicit', 'IP Address*' with the value '192 . 0 . 2 . 100', and 'Port*' with the value '80'. At the bottom of the form are two buttons: 'Continue' and 'Cancel'. On the right side of the page, there is a 'Basic Settings' sidebar with a list of settings: 1. Proxy Settings, 2. SSL Interception, 3. Identity Management, 4. URL Filtering, 5. Security Configuration, and 6. Analytics.

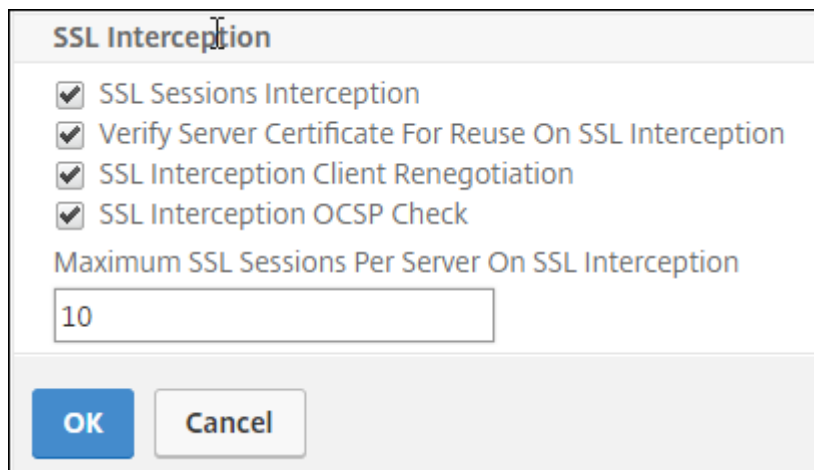
6. [続行] をクリックします。

SSL インターセプション設定の構成

1. [**SSL インターセプトを有効にする**] を選択します。



2. 「**SSL** プロファイル」で、「+」をクリックして新しいフロントエンド SSL プロファイルを追加し、このプロファイルで **SSL** セッションインターセプトを有効にします。



3. [OK] をクリックし、[完了] をクリックします。
4. [**SSL** インターセプト **CA** 証明書とキーペアの選択] で、[+] をクリックして、SSL インターセプト用の CA 証明書とキーのペアをインストールします。

Install SSL Interception CA Certificate

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

Certificate File Name*
Choose File ▼ ns_swg_ca.crt ?

Key File Name*
Choose File ▼ ns_swg_ca.key ?

Notify When Expires

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

Notification Period
30

Install **Close**

5. [インストール] をクリックし、[閉じる] をクリックします。
6. すべてのトラフィックを代行受信するポリシーを追加します。[バインド] をクリックし、[追加] をクリックします。

SSL Interception Policies ×

Add Edit Delete

Policy Name	Pattern Set Name	Action
No items		

Insert **Close**

7. ポリシーの名前を入力し、[詳細設定] を選択します。式エディタで true と入力します。
8. [アクション] で、[インターセプト] を選択します。

SSL Interception Policies / SSL Interception Policy

SSL Interception Policy

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

Name*

ssli-pol

URL Categories Create Patset Security Configuration Advanced

Expression*

Expression Editor

Operators Saved Policy Expressions Frequently Used Expressions

true

Evaluate

Action*

INTERCEPT

Create Close

9. **[Create]** をクリックし、**[Add]** をクリックして、機密情報をバイパスする別のポリシーを追加します。
10. ポリシーの名前を入力し、**[URL カテゴリ]** で **[追加]** をクリックします。
11. 「財務」および「電子メール」カテゴリを選択し、「構成済み」リストに移動します。
12. [アクション] で **[BYPASS]** を選択します。

SSL Interception Policies / SSL Interception Policy

SSL Interception Policy

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

Name*

URL Categories
 Create Patset
 Security Configuration
 Advanced

URL Categories*

Available (17) Select All

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

Configured (6) Remove All

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

Action*

13. [作成] をクリックします。

14. 前に作成した 2 つのポリシーを選択し、[Insert] をクリックします。

SSL Interception Policies

SSL Interception Policies

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

15. [続行] をクリックします。

SSL Interception

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

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

Enable SSL Interception

SSL Profile*
ns_default_ssl_profile_frontend + ✎

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

Bind Unbind

Policy Name
ssli_pol_ssli
cat_pol1_ssli

Continue Cancel

ユーザー認証設定の構成

1. [ユーザー認証を有効にする] を選択します。[認証タイプ] フィールドで、[LDAP] を選択します。

Dashboard Configuration Reporting Documentation Downloads

Secure Web Gateway Configuration

Proxy Settings

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

SSL Interception

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

Identity Management

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

Enable user authentication

Authentication Type*
LDAP

LDAP Server*
explicit-auth-server + ✎

Continue Cancel

Basic Settings

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

2. LDAP サーバの詳細を追加します。

Create Authentication LDAP Server

Name*
explicit-auth-vs

Server Name Server IP

IP Address*
192 . 0 . 2 . 116

Security Type
PLAINTEXT

Port
389

Server Type
AD

Time-out (seconds)
3

Authentication

Connection Settings

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

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

Administrator Password*
.....

Confirm Administrator Password*
.....

[Retrieve Attributes](#)

Test Connection

Other Settings

Server Logon Name Attribute
sAMAccountName

Search Filter

Group Attribute

Sub Attribute Name

SSO Name Attribute

Default Authentication Group

User Required
 Referrals

Maximum Referral Level
1

Referral DNS Lookup
A-REC

Validate LDAP Server Certificate

LDAP Host Name

OTP Secret

► More

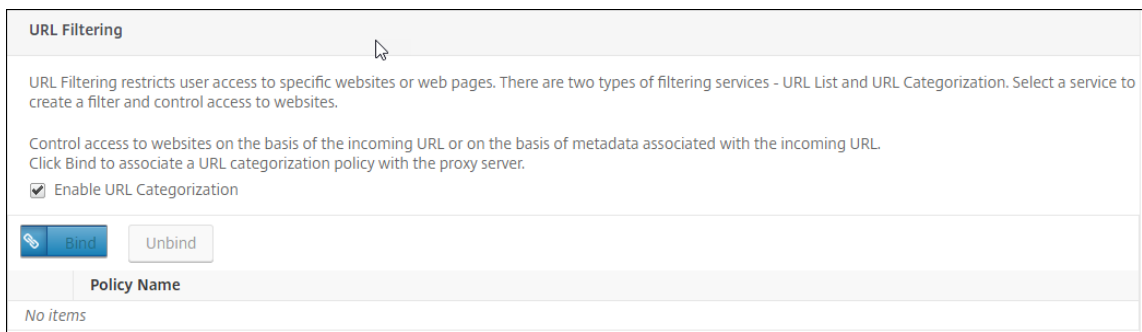
Create **Close**

3. [作成] をクリックします。

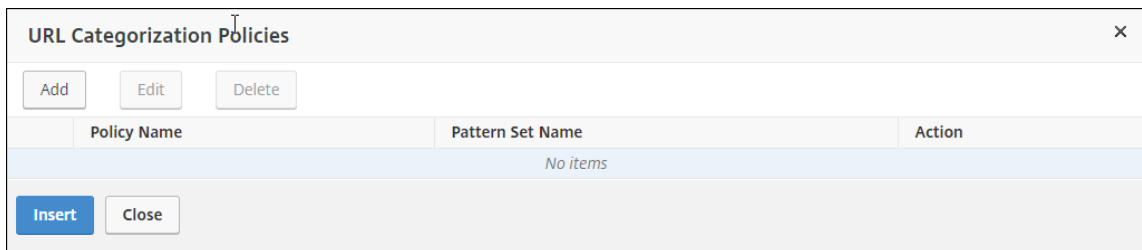
4. [続行] をクリックします。

URL フィルタリング設定の構成

1. [URL の分類を有効にする] を選択し、[バインド] をクリックします。



2. [追加] をクリックします。



3. ポリシーの名前を入力します。[アクション] で、[拒否] を選択します。[URL カテゴリ] で、[不正/有害]、[アダルト]、[マルウェアとスパム] を選択し、[構成済み] リストに移動します。

URL Categorization Policies / URL Categorization Policy

URL Categorization Policy

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

Name*

Basic Advanced

Action*

URL Categories*

Available (16) Select All

Search Categories

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

Configured (29) Remove All

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

4. [作成] をクリックします。

5. ポリシーを選択し、[Insert] をクリックします。

URL Categorization Policies

URL Categorization Policies

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

6. [続行] をクリックします。

URL Filtering

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

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

Enable URL Categorization

Enable URL List

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

Continue **Cancel**

7. [続行] をクリックします。
8. [アナリティクスの有効化] をクリックします。
9. Citrix ADM の IP アドレスを入力し、[ポート] に 5557 と指定します。

Analytics

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

Enable Analytics

NetScaler MAS IP Address*

192 . 0 . 2 . 41

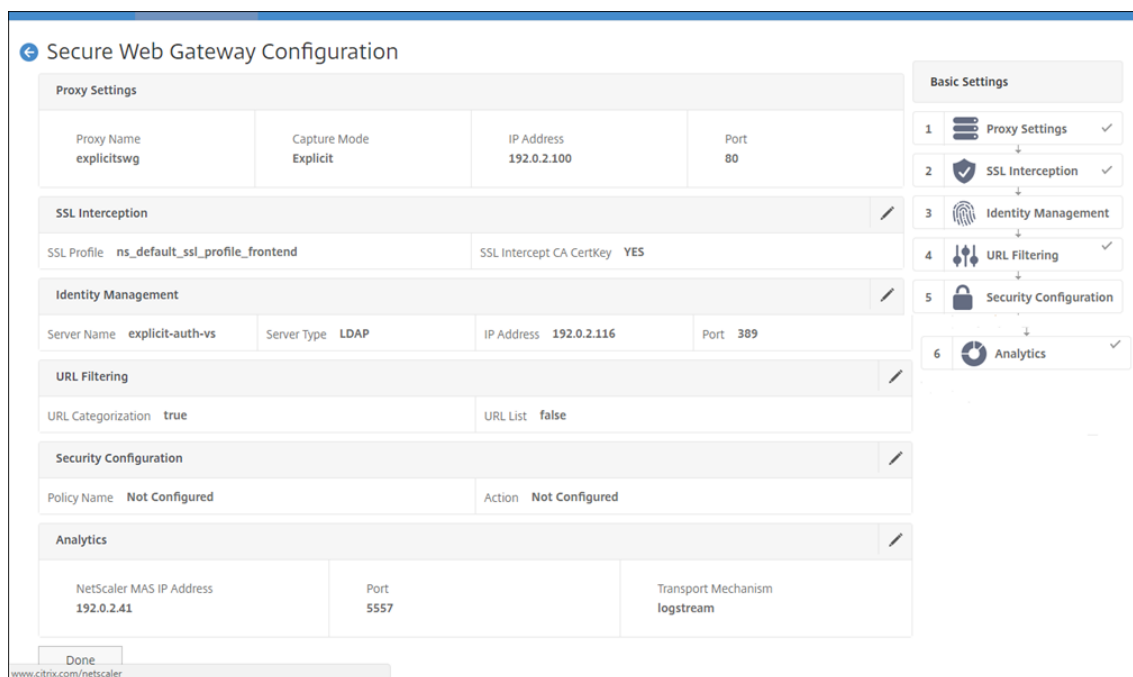
Port*

5557

Transport Mechanism: LogStream

Continue **Cancel**

10. [続行] をクリックします。
11. [完了] をクリックします。



Citrix ADM を使用して、ユーザーの主要なメトリックを表示し、次の項目を決定します。

- 企業内のユーザーのブラウズの動作。
- 社内ユーザーがアクセスした URL カテゴリ。
- URL またはドメインへのアクセスに使用された Web ブラウザー。

この情報を使用して、ユーザーのシステムがマルウェアに感染しているかどうかを判断するか、ユーザーの帯域幅消費パターンを理解します。Citrix SWG アプライアンスのポリシーを微調整して、これらのユーザーを制限したり、さらに一部のウェブサイトブロックしたりできます。MAS でのメトリックスの表示の詳細については、[MAS ユースケース](#)の「エンドポイントの検査」ユースケースを参照してください。

注

CLI を使用して、次のパラメータを設定します。

```

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

```

CLI の例

次に、企業ネットワークとの間で送受信されるトラフィックのインターセプションと検査を設定するために使用されるすべてのコマンドの例を示します。

一般的な構成:

```
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-->
```

認証の設定:

```
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-->
```

プロキシサーバと **SSL** インターセプションの設定:

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

URL カテゴリの設定:

```
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-->
```

Citrix ADM にデータをプルするための **AppFlow** 構成:

```
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-->
```

ユースケース:**ICAP** を使用したリモートマルウェア検査による企業ネットワークの安全性の確保

May 1, 2021

Citrix Secure Web Gateway (SWG) アプライアンスはプロキシとして機能し、すべてのクライアントトラフィックを代行受信します。アプライアンスは、ポリシーを使用してトラフィックを評価し、リソースが存在するオリジンサーバーにクライアント要求を転送します。アプライアンスはオリジンサーバーからの応答を復号化し、プレーンテキストのコンテンツを ICAP サーバーに転送してマルウェア対策チェックを行います。ICAP サーバーは、「適応不要」、

エラー、または変更要求を示すメッセージで応答します。ICAP サーバーからの応答に応じて、要求されたコンテンツがクライアントに転送されるか、適切なメッセージが送信されます。

このユースケースでは、Citrix SWG アプライアンスで、一般的な構成、プロキシおよび SSL インターセプト関連の構成、および ICAP 構成を実行する必要があります。

一般的な構成

次のエンティティを構成します。

- NSIP アドレス
- サブネット IP (SNIP) アドレス
- DNS ネームサーバー
- SSL インターセプションのためにサーバ証明書に署名するための CA 証明書とキーのペア

プロキシサーバと **SSL** インターセプションの設定

次のエンティティを構成します。

- エクスプリシットモードのプロキシサーバで、すべてのアウトバウンド HTTP および HTTPS トラフィックを代行受信します。
- SSL プロファイルを使用して、接続の SSL 設定（暗号やパラメータなど）を定義します。
- SSL ポリシーを使用して、トラフィックを代行受信するためのルールを定義します。すべてのクライアント要求をインターセプトするには、true に設定します。

詳細については、次のトピックを参照してください。

- [プロキシモード](#)
- [SSL インターセプション](#)

次の構成例では、マルウェア対策検出サービスが www.example.com にあります。

一般的な設定例:

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

プロキシサーバと **SSL** インターセプション設定の例:

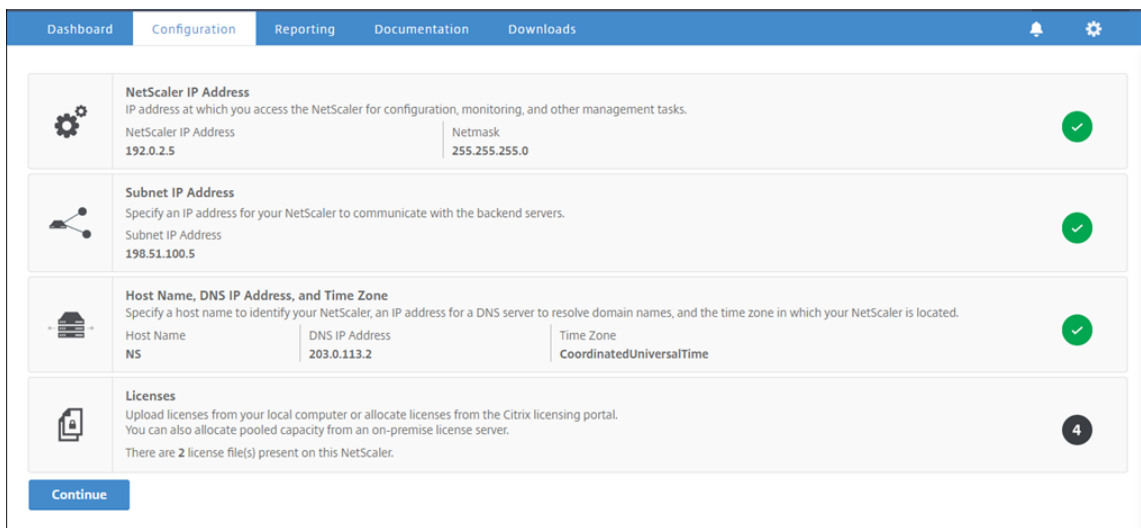
```
1 add cs vserver explicitSWG PROXY 192.0.2.100 80 - Authn401 ENABLED -  
  authnVsName explicit-auth-vs  
2  
3 set ssl parameter -defaultProfile ENABLED  
4  
5 add ssl profile swg_profile -sslInterception ENABLED  
6  
7 bind ssl profile swg_profile -ssliCACertkey ns-swg-ca-certkey  
8  
9 set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

ICAP 設定の例:

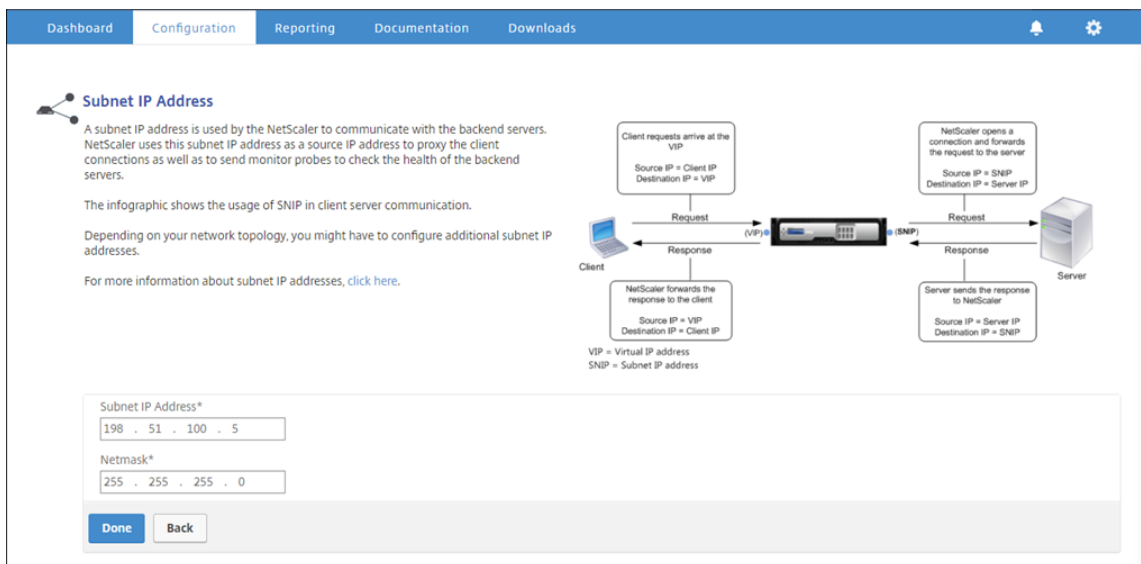
```
1 add service icap_svc 203.0.113.225 TCP 1344  
2  
3 enable ns feature contentinspection  
4  
5 add icaprofile icaprofile1 -uri /example.com -Mode RESMOD  
6  
7 add contentInspection action CiRemoteAction -type ICAP -serverName  
  icap_svc -icapProfileName icaprofile1  
8  
9 add contentInspection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

SNIP アドレスと DNS ネームサーバーの構成

1. Web ブラウザで、SNIP アドレスを入力します。たとえば、<http://192.0.2.5>などです。
2. **[User Name]** ボックスと **[Password]** ボックスに管理者資格情報を入力します。次の画面が開きます。次の画面が表示されない場合は、プロキシ設定セクションに進んでください。



3. [サブネット IP アドレス] セクションをクリックし、IP アドレスを入力します。



4. [完了] をクリックします。

5. [ホスト名]、[DNS IP アドレス]、[タイムゾーン] セクションをクリックし、これらのフィールドに値を入力します。

The screenshot shows the 'Host Name, DNS IP Address, and Time Zone' configuration page. The page has a navigation bar with 'Dashboard', 'Configuration', 'Reporting', 'Documentation', and 'Downloads'. Below the navigation bar, there is a title 'Host Name, DNS IP Address, and Time Zone' and a brief instruction: 'Specify a host name to identify your NetScaler. When you generate the Universal license for NetScaler Gateway, the host name is used in the license. Specify the IP address of a DNS server if you want to allocate your licenses from the Citrix licensing portal. Specify the time zone in which your NetScaler is located.' The form contains three input fields: 'Host Name' with the value 'NS', 'DNS IP Address' with the value '203 . 0 . 113 . 2', and 'Time Zone*' with a dropdown menu set to 'CoordinatedUniversalTime'. At the bottom of the form are two buttons: 'Done' and 'Back'.

6. [完了]、[続行] の順にクリックします。

プロキシ設定を構成する

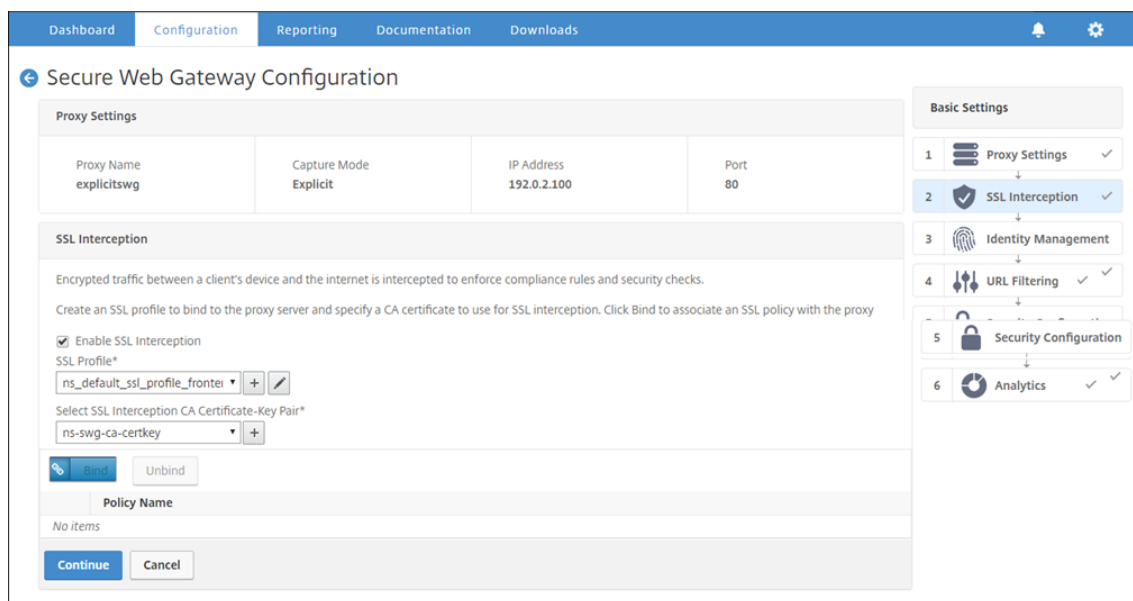
1. [**Secure Web Gateway**] > [**Secure Web Gateway ウィザード**] に移動します。
2. [はじめに] をクリックし、[続行] をクリックします。
3. [プロキシ設定] ダイアログボックスで、明示的なプロキシサーバーの名前を入力します。
4. [キャプチャモード] で、[明示的] を選択します。
5. IP アドレスとポート番号を入力します。

The screenshot shows the 'Secure Web Gateway Configuration' page. The page has a navigation bar with 'Dashboard', 'Configuration', 'Reporting', 'Documentation', and 'Downloads'. Below the navigation bar, there is a title 'Secure Web Gateway Configuration' and a sub-section 'Proxy Settings'. The 'Proxy Settings' section contains a brief instruction: 'Configure a proxy server in transparent or explicit mode. In transparent proxy mode, configuring a proxy on a client's device is not required. In explicit proxy mode, all client requests are sent to either an IP address that the clients configure in their browsers or an IP address that the organization pushes to the clients' devices.' The form contains four input fields: 'Name*' with the value 'explicitswg', 'Capture Mode*' with a dropdown menu set to 'Explicit', 'IP Address*' with the value '192 . 0 . 2 . 100', and 'Port*' with the value '80'. At the bottom of the form are two buttons: 'Continue' and 'Cancel'. On the right side of the page, there is a 'Basic Settings' sidebar with a list of settings: 1. Proxy Settings, 2. SSL Interception, 3. Identity Management, 4. URL Filtering, 5. Security Configuration, and 6. Analytics.

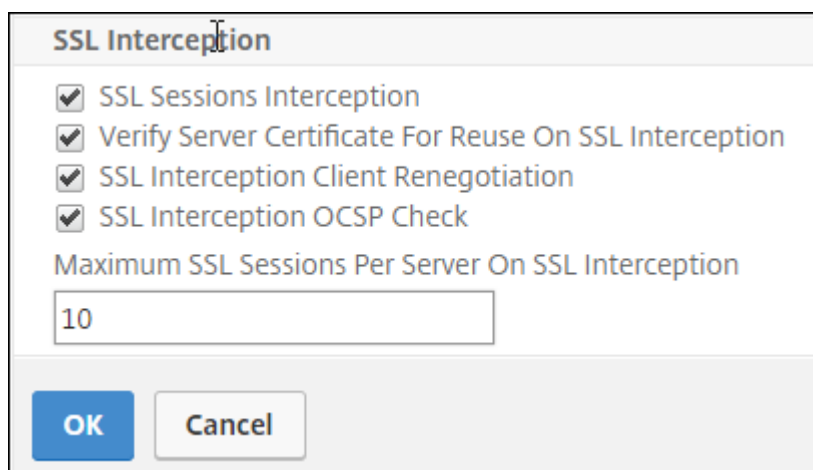
6. [続行] をクリックします。

SSL インターセプション設定の構成

1. [**SSL インターセプトを有効にする**] を選択します。



2. 「**SSL** プロファイル」で、既存のプロファイルを選択するか、「+」をクリックして新しいフロントエンド SSL プロファイルを追加します。このプロファイルで **SSL** セッションインターセプトを有効にします。既存のプロファイルを選択する場合は、次の手順をスキップします。



3. [OK] をクリックし、[完了] をクリックします。
4. [**SSL** インターセプト **CA** 証明書とキーペアの選択] で、既存の証明書を選択するか、[+] をクリックして SSL インターセプト用の CA 証明書とキーのペアをインストールします。既存の証明書を選択した場合は、次の手順をスキップします。

Install SSL Interception CA Certificate

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

Certificate File Name*
Choose File ▼ ns_swg_ca.crt ?

Key File Name*
Choose File ▼ ns_swg_ca.key ?

Notify When Expires

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

Notification Period
30

Install **Close**

5. [インストール] をクリックし、[閉じる] をクリックします。
6. すべてのトラフィックを代行受信するポリシーを追加します。[バインド] をクリックします。[Add] をクリックして新しいポリシーを追加するか、既存のポリシーを選択します。既存のポリシーを選択した場合は、[Insert] をクリックし、次の3つの手順をスキップします。

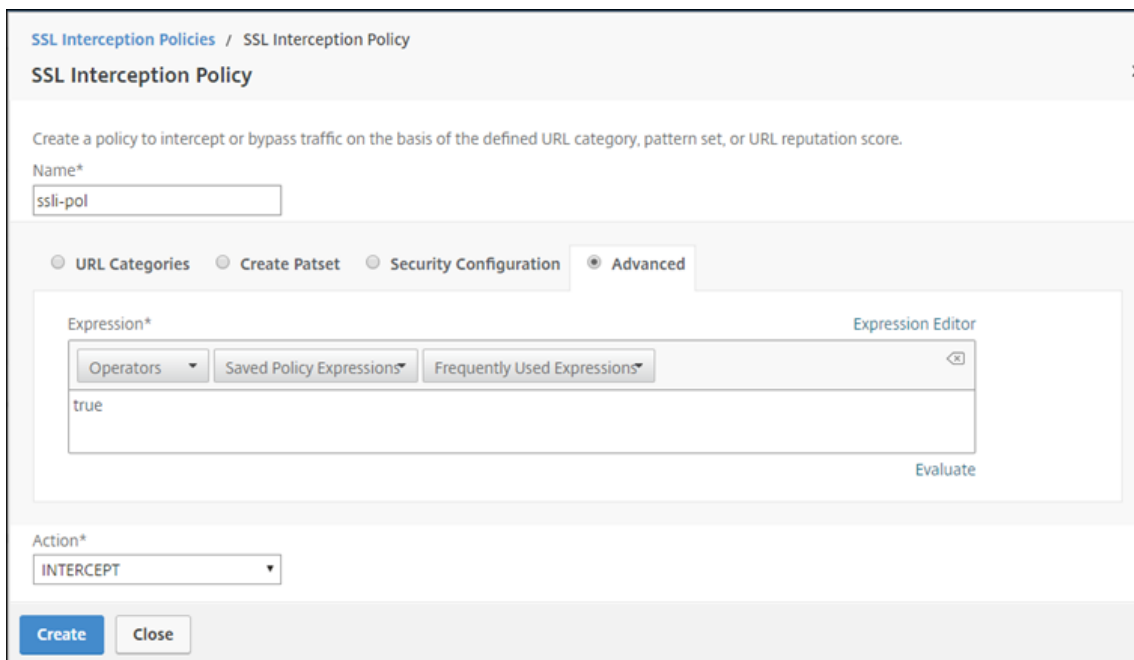
SSL Interception Policies ×

Add Edit Delete

Policy Name	Pattern Set Name	Action
No items		

Insert **Close**

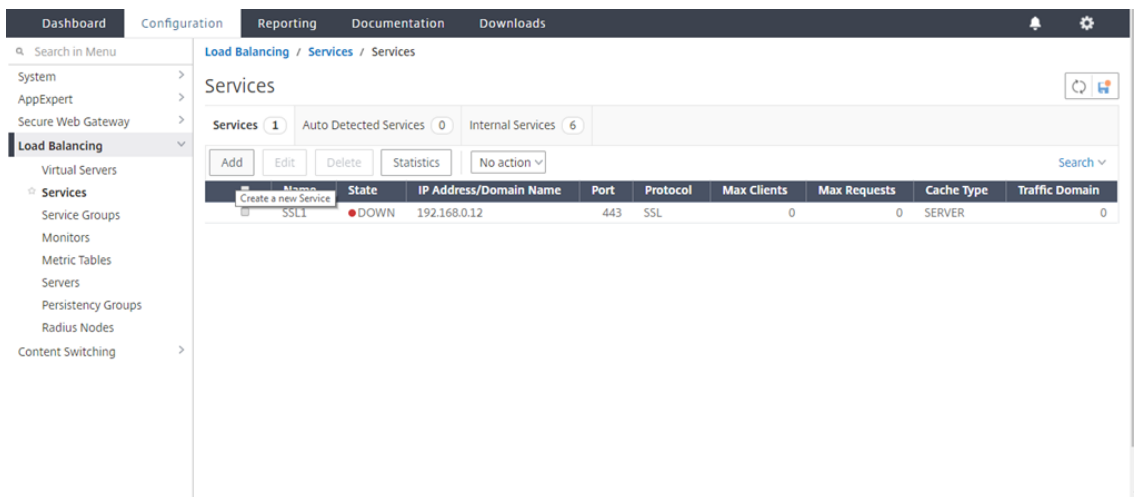
7. ポリシーの名前を入力し、[詳細設定] を選択します。式エディタで true と入力します。
8. [アクション] で、[インターセプト] を選択します。



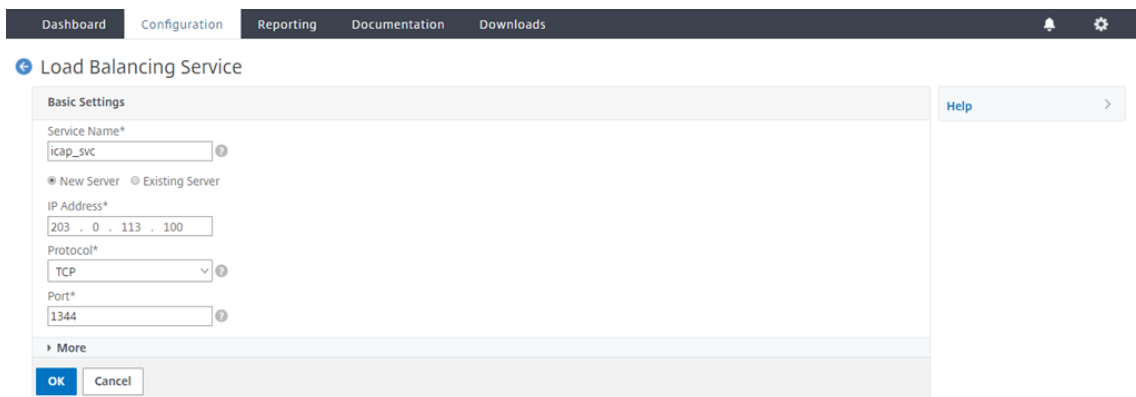
9. [作成] をクリックします。
10. [続行] を 4 回クリックし、[完了] をクリックします。

ICAP の設定を構成する

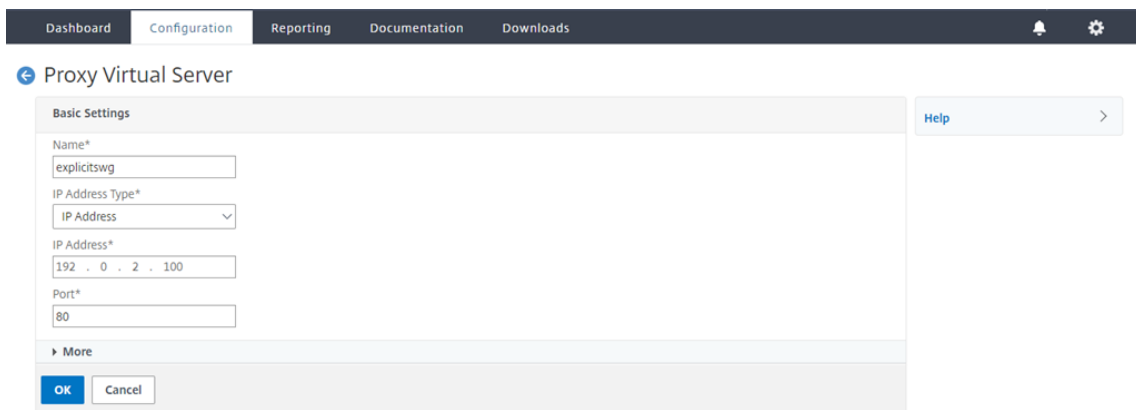
1. [負荷分散] > [サービス] に移動し、[追加] をクリックします。



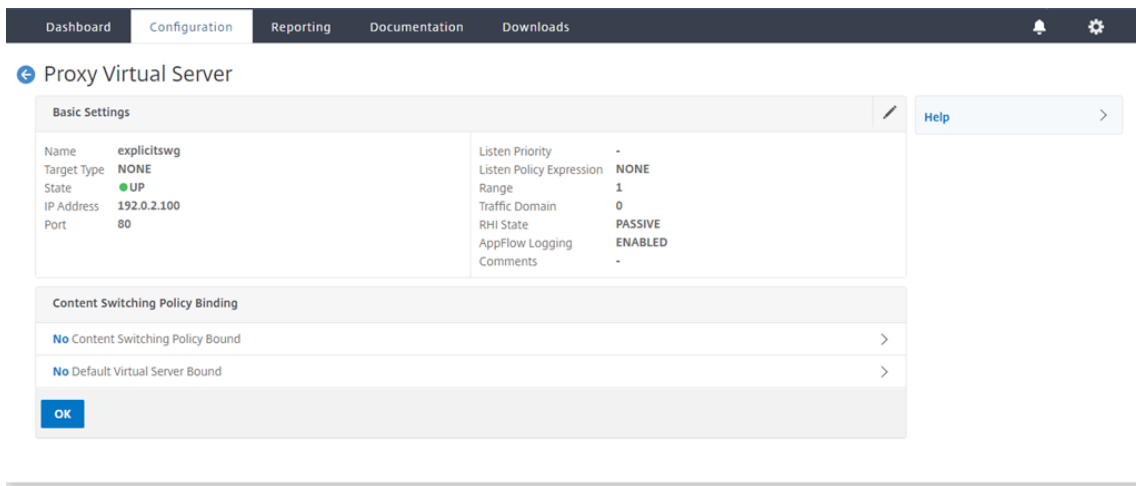
2. 名前と IP アドレスを入力します。「プロトコル」で、「TCP」を選択します。[ポート] に **1344** と入力します。[OK] をクリックします。



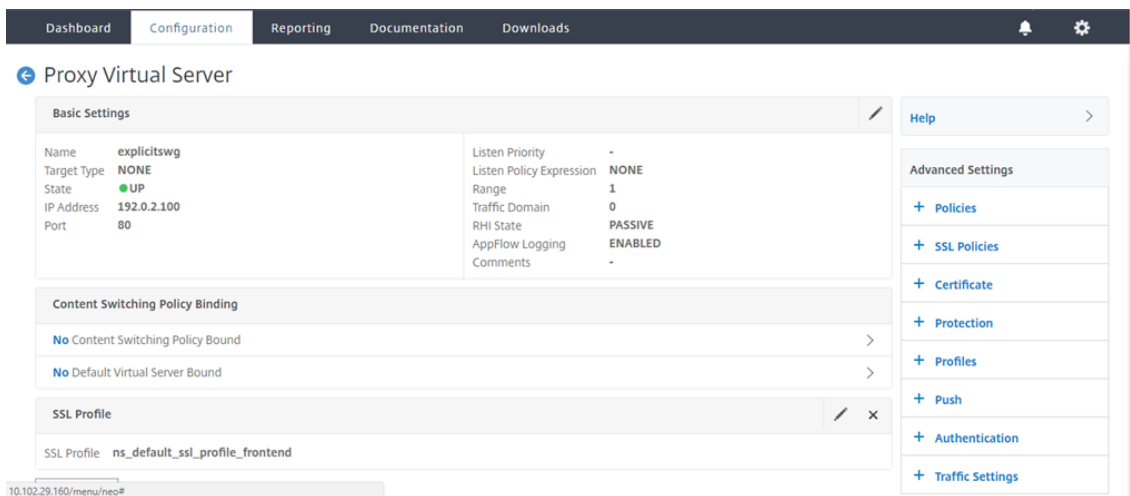
3. [**Secure Web Gateway**] > [プロキシ仮想サーバー] に移動します。プロキシ仮想サーバーを追加するか、仮想サーバーを選択して「編集」をクリックします。詳細を入力したら、[**OK**] をクリックします。



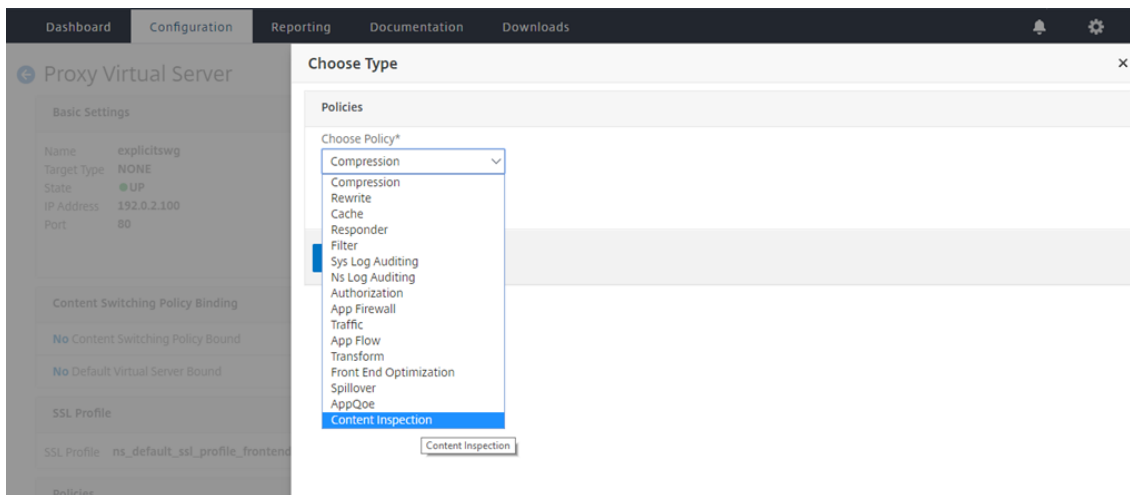
もう一度 [**OK**] をクリックします。



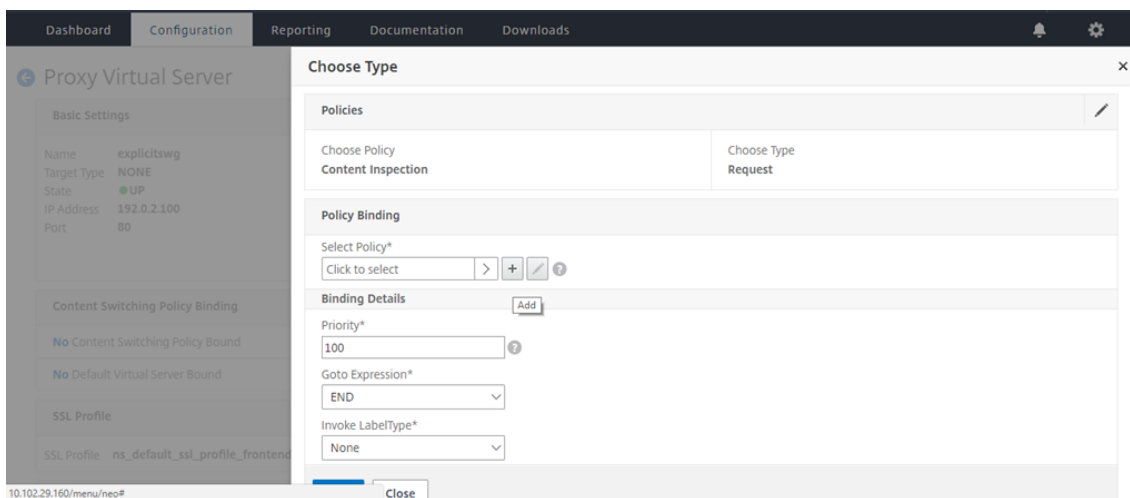
4. [詳細設定] で、[ポリシー] をクリックします。



5. 「ポリシーの選択」で、「コンテンツ検査」を選択します。[続行] をクリックします。



6. [ポリシーの選択] で、[+] 記号をクリックしてポリシーを追加します。



7. ポリシーの名前を入力します。[アクション] で、[+] 記号をクリックしてアクションを追加します。

Dashboard Configuration Reporting Documentation Downloads

Choose Type / Create ICAP Policy

Proxy Virtual Server

Basic Settings

Name explicitSWG
Target Type NONE
State UP
IP Address 192.0.2.100
Port 80

Content Switching Policy Binding

No Content Switching Policy Bound

No Default Virtual Server Bound

SSL Profile

SSL Profile ns_default_ssl_profile_frontend

10.102.29.160/menu/neo#

Create ICAP Policy

Action Name*
cipolicy

Action*
RESET

LogAction
Add

Undef Action

Expression
Select Select Select

Press Control+Space to start the expression and then type ':' to get the next set of options

Comment

8. アクションの名前を入力します。[サーバー名] に、以前に作成した TCP サービスの名前を入力します。ICAP プロファイルで、「+」記号をクリックして ICAP プロファイルを追加します。

Dashboard Configuration Reporting Documentation Downloads

Choose Type / Create ICAP Policy / Create ICAP Action

Proxy Virtual Server

Basic Settings

Name explicitSWG
Target Type NONE
State UP
IP Address 192.0.2.100
Port 80

Content Switching Policy Binding

No Content Switching Policy Bound

No Default Virtual Server Bound

SSL Profile

SSL Profile ns_default_ssl_profile_frontend

10.102.29.160/menu/neo#

Create ICAP Action

Name*
ci-remote-action

Type*
ICAP

IP Address Server Name

Server Name
icap_svc

ICAP Profile
Add

If Server Down
CONTINUE

Request-Timeout
0

Request Time-out Action

9. プロファイル名「URI」を入力します。「モード」で「REQMOD」を選択します。

Dashboard Configuration Reporting Documentation Downloads

Choose Type / Create ICAP Policy / Create ICAP Action / Create ICAP Profile

Proxy Virtual Server

Basic Settings

Name explicitSWG
Target Type NONE
State UP
IP Address 192.0.2.100
Port 80

Content Switching Policy Binding

No Content Switching Policy Bound

No Default Virtual Server Bound

SSL Profile

SSL Profile ns_default_ssl_profile_frontend

Policies

Create ICAP Profile

ICAP Profile Name*
icap-profile1

Preview

URI*
/example.com

Host Header

User Agent

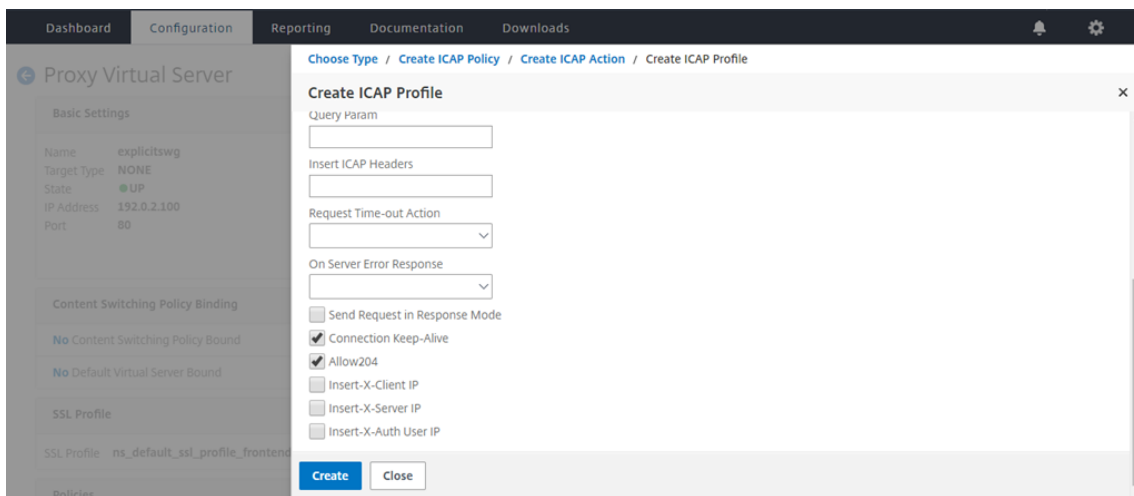
Mode*
REQMOD

Query Param

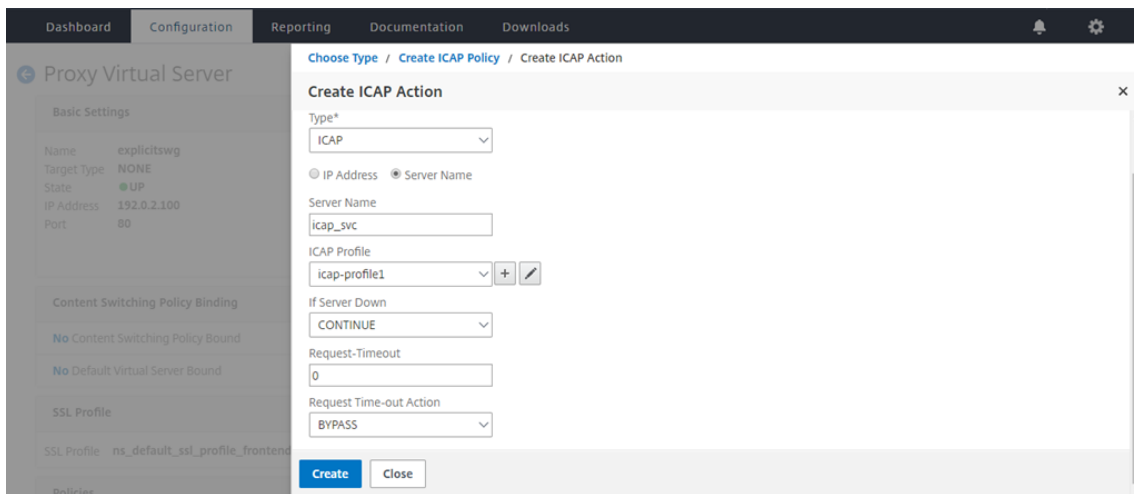
Insert ICAP Headers

Request Time-out Action

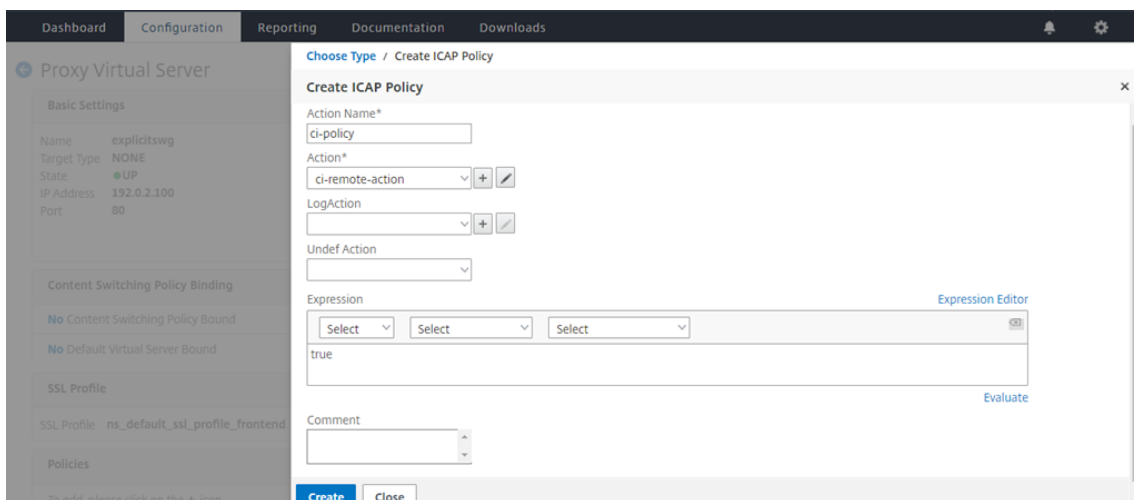
10. [作成] をクリックします。



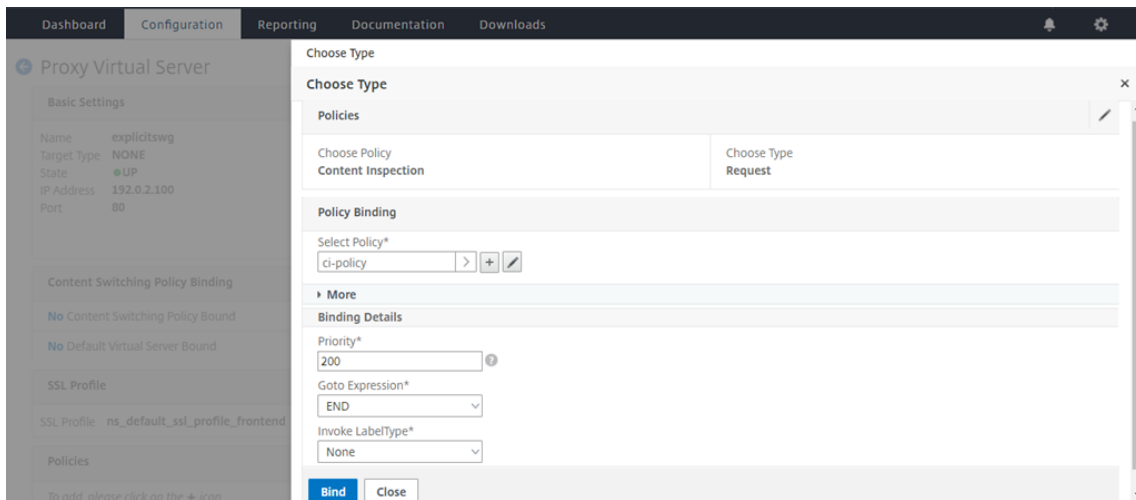
11. 「ICAP アクションの作成」 ページで、「作成」 をクリックします。



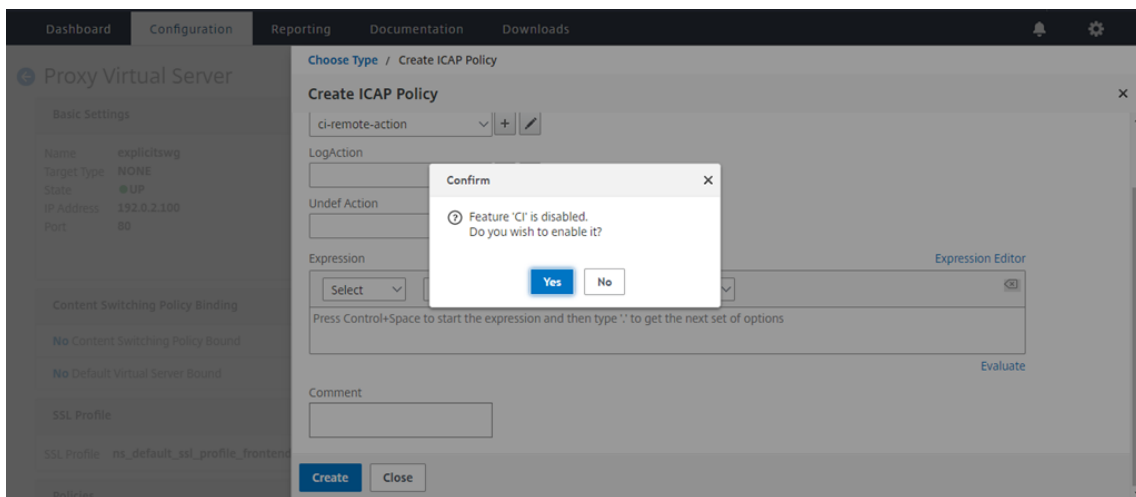
12. ICAP ポリシーの作成 ページで、式エディター に true と入力します。次に、[作成] をクリックします。



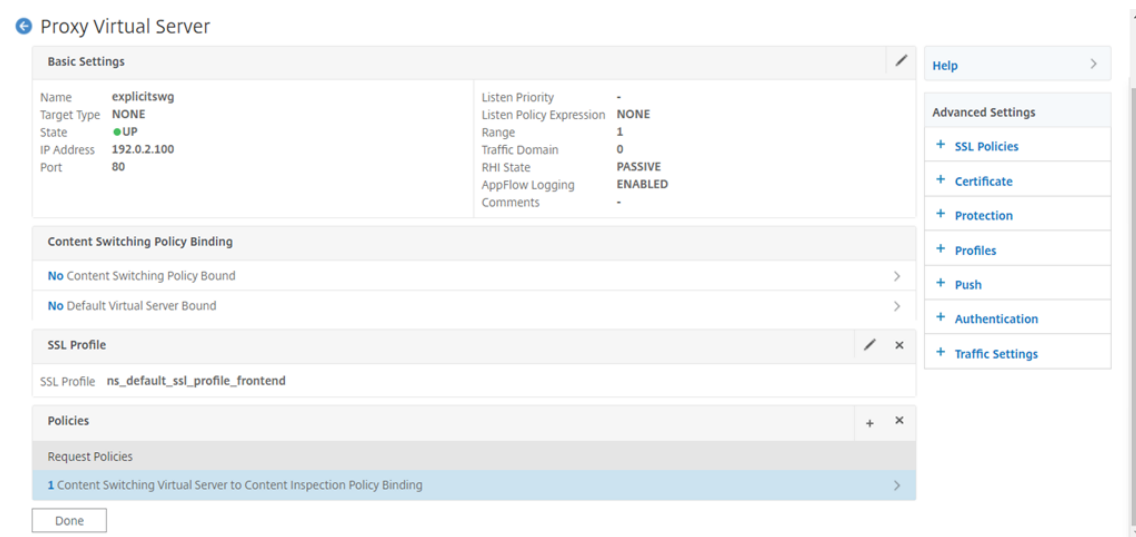
13. [バインド] をクリックします。



14. コンテンツ検査機能を有効にするかどうかを確認するメッセージが表示されたら、[Yes] を選択します。



15. [完了] をクリックします。



RESPMOD の Citrix SWG アプライアンスと ICAP サーバー間のサンプル ICAP トランザクション

Citrix SWG アプライアンスから ICAP サーバーへの要求:

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

ICAP サーバーから Citrix SWG アプライアンスへの応答:

```
1  ICAP/1.0 200 OK
2
3  Connection: keep-alive
4
5  Date: Fri, 01 Dec, 2017 11:40:42 GMT
6
7  Encapsulated: res-hdr=0, res-body=224
8
9  Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$
10
11 IStag: "9.8-13.815.00-3.100.1027-1.0"
12
13 X-Virus-ID: Eicar_test_file
14
15 X-Infection-Found: Type=0; Resolution=2; Threat=Eicar_test_file;
16
17 HTTP/1.1 403 Forbidden
```

```
18
19 Date: Fri, 01 Dec, 2017 11:40:42 GMT
20
21 Cache-Control: no-cache
22
23 Content-Type: text/html; charset=UTF-8
24
25 Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$
26
27 Content-Length: 5688
28
29 <html><head><META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset
    =UTF-8"/>
30
31 ...
32
33 ...
34
35 </body></html>
36 <!--NeedCopy-->
```

ハウツー記事

May 1, 2021

SWG 展開の管理に役立つ「操作方法」記事として、いくつかの設定手順や機能ユースケースを以下に示します。

URL フィルタリング

[URL 分類ポリシーの作成方法](#)

[URL リストポリシーの作成方法](#)

[例外的な URL をホワイトリストに登録する方法](#)

[アダルトカテゴリーのウェブサイトをブロックする方法](#)

URL 分類ポリシーの作成方法

May 1, 2021

ネットワーク管理者は、ユーザーアクセスのために特定のカテゴリの Web サイトをブロックしたい場合があります。これを実行するには、URL 分類ポリシーを作成し、アクセスを制限するカテゴリの事前定義されたリストにポリシーをバインドします。

たとえば、組織のポリシーに従って、すべてのソーシャルネットワーキング Web サイトへのアクセスを制限することができます。このようなシナリオでは、分類ポリシーを作成し、ソーシャルネットワーキングカテゴリウェブサイトの事前定義されたリストにポリシーをバインドする必要があります。

基本的な方法を使用して URL 分類ポリシーを作成するには、次の手順を実行します。

1. **Citrix SWG** アプライアンスにログオンし、[セキュアな Web ゲートウェイ] > [URL フィルタリング] > [URL 分類] に移動します。
2. 詳細ウィンドウで、[追加] をクリックして [URL 分類ポリシー] ページにアクセスし、次のパラメータを指定します。
 - a) **URL 分類ポリシー**。レスポンスポリシーの名前。
 - b) 基本。[定義済みのカテゴリのリストを使用して構成する] を選択します。
 - c) アクション。URL へのアクセスを制御するアクション。
 - d) **URL カテゴリ**。カテゴリの事前定義済みリストを選択して、設定済みリストに追加します。
3. [作成] して [閉じる] をクリックします。

URL Categorization Policies / URL Categorization Policy

URL Categorization Policy

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

Name*
cat_pol2

Basic Advanced

Action*
Deny

URL Categories*

Available (16) Select All

Search Categories

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

Configured (29) Remove All

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

高度な方法を使用して URL 分類ポリシーを作成するには、次の手順を実行します。

1. 高度な分類を使用して新しい URL 分類ポリシーを設定する。
2. [追加] をクリックします。
3. [URL 分類ポリシー] ページで、次のパラメータを指定します。
 - a) **URL 分類ポリシー**。レスポンスポリシーの名前。
 - b) [詳細]。カスタム式を使用してポリシーを設定します。
4. [作成] して [閉じる] をクリックします。

← URL Categorization Policy

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

Name*

Basic Advanced

Expression*

Operators Saved Policy Expressions Frequently Used Expressions

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

Create Close

URL リストポリシーの作成方法

May 1, 2021

ネットワーク管理者は、ユーザーアクセスのために特定のカテゴリの Web サイトをブロックしたい場合があります。これを実行するには、URL List ポリシーを作成し、アプライアンスにテキストファイルとしてインポートされた URL セットにポリシーをバインドします。URL セットは、フィルタを適用する Web サイトのコレクションです。

たとえば、組織のポリシーに従って、すべてのマルウェア Web サイトへのアクセスを制限できます。このようなシナリオでは、URL リストポリシーを作成し、アプライアンスにインポートされた URL セットにポリシーをバインドする必要があります。

URL リストポリシーを設定するには、次の手順を実行します。

1. **Citrix SWG** アプライアンスにログオンし、[セキュアな **Web** ゲートウェイ] > [URL フィルタリング] > [URL リスト] に移動します。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [URL リストポリシー] ページで、ポリシー名を指定します。
4. URL セットをインポートするか、パターンセットを作成するオプションを選択し、この手順の最後の手順に従います。
5. ドロップダウンリストから応答者のアクションを選択します。
6. [作成] して [閉じる] をクリックします。

カスタム URL セットまたはサードパーティ URL セットをインポートする手順は、次のとおりです。

1. [URL リストポリシー] タブページで、[URL セットのインポート] チェックボックスをオンにし、次の URL セットパラメータを指定します。
 - a) **URL セット名**: URL セットの名前。
 - b) **URL**: URL セットにアクセスする場所の Web アドレス。
 - c) **[Overwrite]**: 以前にインポートした URL セットを上書きします。
 - d) **Delimiter**: CSV ファイルレコードを区切る文字シーケンス。
 - e) 行区切り文字—CSV ファイルで使用される行区切り文字。
 - f) 間隔: URL セットが更新される、最も近い 15 分に四捨五入された秒単位の間隔。
 - g) プライベートセット—URL セットのエクスポートを防止するオプション。
 - h) **Canary URL**: URL セットのコンテンツの機密を保持するかどうかをテストするための内部 URL。URL の最大長は 2047 文字です。カナリア URL の詳細については、「プライベート URL セットの構成」セクションを参照してください。

← URL List Policy

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

Name*

Import URL Set Create Patset

URL Set Name*

URL*

Overwrite

Delimiter

Row Separator

Interval

Private Set

Canary URL

Action*

Responder Action*
 + ?

パターンセットを作成するには、次の手順に従います。

1. 「パターンの作成」 (**Create Pattern**) タブページで、パターンセットの名前を入力します。
2. [挿入] をクリックしてパターンを作成します。
3. [パターンバインドへのポリシー・パッチセットの構成] ページで、次のパラメータを設定します。
 - a) パターン: パターンを構成する文字の文字列
 - b) 文字セット: 文字セットのタイプ: ASCII または UTF_8 フォーマット
 - c) インデックス: ユーザによって割り当てられたインデックス値 (1 ~4294967290)
4. [挿入] をクリックしてパターンセットを追加し、[閉じる] をクリックします。

例外的な URL をホワイトリストに登録する方法

May 1, 2021

URL フィルターを使用して Web サイトのカテゴリをブラックリストに登録する場合、特定の Web サイトを例外としてホワイトリストに登録するか、許可する必要があります。たとえば、ゲームの Web サイトをブラックリストに登録したいが、ホワイトリストのみを希望する場合は www.supersports.com、URL リストポリシーでパッチセットを作成し、そのポリシーを他のバインドされたポリシーよりも優先されます。

Citrix SWG ウィザードを使用してパターンセットを作成するには

1. **Citrix SWG** アプライアンスにログオンし、セキュアな **Web** ゲートウェイ > **URL** フィルタリング > **URL** リストに移動します。
2. 詳細ウィンドウで、[追加] をクリックします。
3. [**URL** リストポリシー] ページで、ポリシー名を指定します。
4. URL セットをインポートするか、パターンセットを作成するオプションを選択します。
5. 「パターンの作成」 (**Create Pattern**) タブページで、パターンセットの名前を入力します。
6. [挿入] をクリックしてパターンを作成します。
7. 「パターン・バインディングへのポリシー・パッチセットの構成」 ページで、次のパラメータを設定します。
 - a) パターン: パターンを構成する文字列。
 - b) 文字セット: 文字セットタイプは、ASCII 形式または UTF_8 形式として定義されます。

c) インデックス: ユーザーが割り当てたインデックス値 (1 ~4294967290)

8. 「挿入」 (**Insert**) をクリックしてパターンセットを追加し、「閉じる」 (**Close**) をクリックします。

← URL List Policy

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

Name*
URL List

Import URL Set Create Patset

Patset Name*
Patset

Insert Delete

Patset Name	Pattern	Index
Patset	Pattern	5

Configure Policy Patset to Pattern Binding

Pattern*
Patset

Charset
ASCII

Index
5

Insert Close

Action*
Respond with html page

Responder Action*
+

Create Close

Citrix SWG GUI を使用してポリシー式の優先度を設定するには:

1. **Citrix SWG** アプライアンスにログオンし、[**Secure Web Gateway**] > [プロキシ仮想サーバー] に移動します。
2. 詳細ページで、サーバを選択し、[**Edit**] をクリックします。
3. [プロキシ仮想サーバー] ページで、[ポリシー] セクションに移動し、鉛筆アイコンをクリックして詳細を編集します。
4. 作成したパッチセットポリシーを選択し、「ポリシーバインディング」ページで、他のバインドポリシーよりも低い優先度値を指定します。
5. [バインド] と [完了] をクリックします。

アダルトカテゴリーのウェブサイトをブロックする方法

May 1, 2021

企業のお客様は、アダルトカテゴリーグループに属する Web サイトをブロックすることができます。これは、アダルトカテゴリーに属するリクエストを選択し、そのようなブラックリスト URL へのアクセスをブロックするレスポンスポリシーを設定することによって行われます。

アダルトカテゴリに属する **Web** サイトをブロックするための **URL** 分類の設定

CLI を使用してポリシーを設定し、成人向け **Web** サイトをブロックするには、次の手順を実行します。

コマンドプロンプトで、次のコマンドを入力します。

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

例:

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

Citrix SWG ウィザードを使用してアダルト **Web** サイトをブロックするための **URL** 分類の構成

Citrix SWG ウィザードを使用してアダルトカテゴリをブロックするには

1. **Citrix SWG** アプライアンスにログオンし、**Secure Web Gateway** に移動します。
2. 詳細ウィンドウで、[セキュアな **Web** ゲートウェイウィザード] をクリックします。
3. **Secure Web Gateway** の構成ページで、SWG プロキシサーバーの設定を指定します。
4. [**Continue**] をクリックして、SSL インターセプションなどの他の設定を指定し、管理を識別します。
5. [続行] をクリックして、[**URL** フィルタリング] セクションにアクセスします。
6. 機能を有効にするには、[**URL** 分類を有効にする] チェックボックスをオンにします。
7. [バインド] をクリックして [**URL** 分類ポリシー] スライダにアクセスします。
8. ポリシーを選択し、[**Insert**] をクリックしてポリシーをバインドします。
9. アダルト **Web** サイトをブロックするレスポンスポリシーを選択します。
10. 新しいポリシーを追加するには、[追加] をクリックして [**URL** 分類ポリシー] ページにアクセスし、次のいずれかの操作を行います。
 - a) 基本分類を使用してポリシーを設定するには、[**Add**] をクリックします。
 - i. [**URL** 分類ポリシー] ページで、次のパラメータを指定します。
 - A. URL 分類ポリシー。レスポンスポリシーの名前。
 - B. 基本。基本設定方法を使用してポリシーを設定します。
 - C. アクション。URL へのアクセスを制御するアクション。
 - D. URL カテゴリ。定義済みの一覧から [**アダルトカテゴリ**] を選択します。
11. [作成] して [閉じる] をクリックします。
 - a) 高度な分類を使用して新しい URL 分類ポリシーを構成するには、[追加] をクリックします。
 - i. [**URL** 分類ポリシー] ページで、次のパラメータを指定します。

- A. **URL** 分類ポリシー。レスポンスポリシーの名前。
 B. **[詳細]**。成人カテゴリグループの要求をブロックするポリシーを構成します。

12. **[作成]** して **[閉じる]** をクリックします。

← URL Categorization Policy

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

Name*

Basic Advanced

Action*

URL Categories*

Available (18) Select All

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

Configured (11) Remove All

- Adult/Porn
- Nudity
- Sexual Services
- Adult Search/Links
- Dating
- Grotesque
- Adult Magazine/News
- Fetish
- Sexual Expression(text)
- Sex Education
- Swimsuits & Lingerie

システム

May 1, 2021

システム機能では、Citrix SWG アプライアンスの構成時に参照する可能性のある概念情報と構成手順が提供されません。

次の表では、Citrix SWG アプライアンスの機能について説明します。

[基本操作](#) - Citrix ADC アプライアンスのシステムレベルの操作と構成の詳細。

[認証と承認](#) - ユーザー、ユーザーグループ、コマンドポリシーの作成、およびユーザーアカウントへのポリシーの割り当てに関する設定の詳細

[TCP 構成](#) - Citrix ADC アプライアンス上の TCP プロファイルと TCP 機能の構成の詳細。

[HTTP 構成](#) - Citrix ADC アプライアンスでの HTTP プロファイルと HTTP 機能の構成の詳細。

[SNMP](#) - Citrix ADC アプライアンスを監視し、アプライアンス上の問題に迅速に対応するネットワーク管理プロトコル。

監査ログ -カーネルおよびユーザーレベルデーモン内のさまざまなモジュールによって収集された Citrix ADC アプライアンスの状態とステータス情報をログに記録するための標準プロトコル。監査ログには、SYSLOG または NSLOG プロトコル、またはその両方を使用できます。

Call Home -Citrix SWG アプライアンスの重大なエラー状態を監視および解決するための通知システム。

レポート作成ツール -システムパフォーマンスレポートをグラフで表示するために、Citrix SWG アプライアンスからアクセスする Web ベースのインターフェイス。

ネットワーク

May 1, 2021

以下のトピックでは、Citrix SWG アプライアンスで構成するネットワーク機能の概念的な参照情報と構成手順について説明します。

- **IP アドレッシング** Citrix ADC が所有している IP アドレスとその構成詳細。
- **インターフェイス** Citrix SWG アプライアンスにアクセスして構成する。
- **アクセス制御リスト (ACL)** Citrix ADC アプライアンスで使用されるさまざまな種類のアクセス制御リストと、構成の詳細が表示されます。
- **IP ルーティング** Citrix ADC アプライアンスで使用されるさまざまな IP ルーティングプロトコル。
- **インターネットプロトコルバージョン 6 (IPv6)** Citrix ADC アプライアンスでのインターネットプロトコルのサポート、およびアプライアンスが IPv6 ノードとして機能する方法。
- **VXLAN** Citrix ADC ネットワークインフラストラクチャにおける仮想拡張ローカルエリアネットワーク (VXLAN) のサポート、およびレイヤ 2 フレームを UDP でカプセル化することにより、VXLAN がレイヤ 2 ネットワークをレイヤ 3 インフラストラクチャにオーバーレイする方法パケット。

AppExpert

May 1, 2021

以下のトピックでは、Citrix SWG アプライアンス上で構成する AppExpert 機能の概念情報と構成手順について説明します。

パターンセットとデータセット -文字列パターンの大規模なセットに対して文字列マッチング操作を実行するためのポリシー式。

マッチングするパターンタイプに応じて、次のいずれかの機能を使用してパターンマッチングを実装できます。

- パターンセットは、デフォルトの構文ポリシー評価時に文字列マッチングに使用されるインデックス付きパターンの配列です。パターンセットの例: イメージタイプ {svg、bmp、png、gif、tiff、jpg}。
- データセットは、パターンセットの特殊な形式です。これは、型数 (整数)、IPv4 アドレス、または IPv6 アドレスのパターンの配列です。

変数: トークンの形式で情報を格納し、レスポンスポリシーアクションによって使用されるオブジェクト。

下記のように変数は、2つのタイプがあります:

- シングルトン変数。ulong および text (最大サイズ) のいずれかの型の値を指定できます。ulong 型は符号なし 64 ビット整数で、テキスト型はバイトのシーケンス、max-size はシーケンスの最大バイト数です。
- 変数をマップします。マップはキーに関連付けられた値を保持します。各キーと値のペアはマップエントリと呼ばれます。各エントリのキーは、マップ内で一意です。

ポリシーと表現 -ポリシーは、Citrix SWG アプライアンスに入る Web トラフィックを制御します。ポリシーは、規則とも呼ばれる論理式を使用して要求、応答、またはその他のデータを評価し、評価の結果によって決定される 1つ以上のアクションを適用します。または、ポリシーでプロファイルを適用して、複雑なアクションを定義することもできます。

レスポンス: 要求の送信者、送信元、およびセキュリティとシステム管理に関連するその他の条件に基づいて応答を送信するポリシー。この機能はシンプルで迅速に使用できます。より複雑な機能の呼び出しを避けることで、複雑な処理を必要としない要求の処理に費やされる CPU サイクルと時間を削減できます。財務情報などの機密データを処理するために、クライアントが安全な接続を使用して Web サイトを参照するようにするには、HTTPS プロトコルを使用して安全な接続に要求をリダイレクトできます。

書き換え -Citrix SWG アプライアンスが処理する要求と応答の情報を書き換えるポリシー。書き換えは、ウェブサイトの実際の設定に関する不必要な詳細を公開することなく、要求されたコンテンツへのアクセスを提供するのに役立ちます。

URL セット -100 万の URL エントリをブラックリストする高度なポリシー式。制限された Web サイトへのアクセスを防止するために、Citrix SWG アプライアンスは特殊な URL マッチングアルゴリズムを使用します。このアルゴリズムでは、最大 100 万 (1,000,000) のブラックリストエントリを含む URL セットが使用されます。各エントリには、URL カテゴリとカテゴリグループをインデックス付きパターンとして定義するメタデータを含めることができます。アプライアンスは、インターネット執行機関 (政府の Web サイトを含む) または独立したインターネット組織によって管理される、機密性の高い URL セットの URL を定期的にダウンロードすることもできます。

SSL

May 1, 2021

以下のトピックでは、Citrix SWG アプライアンス上で構成する SSL 機能の概念的な参照情報と構成手順について説明します。

- [証明書](#)
- [証明書失効リスト \(CRL\)](#)
- [SSL ポリシー](#)
- [OCSP レスポンダー](#)

よくあるご質問

May 1, 2021

Q: Citrix Secure Web Gateway (SWG) でサポートされるハードウェアプラットフォームは何ですか？

A. Citrix SWG は、次のハードウェアプラットフォームで利用できます。

- 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
- すべての Cavium N2 および N3 ベースの SDX プラットフォーム

Q. SWG アプライアンスでプロキシを作成するときに設定できる 2 つのキャプチャモードは何ですか？

A. SWG ソリューションでは、明示的なプロキシモードと透過プロキシモードがサポートされています。明示的なプロキシモードでは、組織がクライアントのデバイスに設定をプッシュしない限り、クライアントはブラウザで IP アドレスとポートを指定する必要があります。このアドレスは、SWG アプライアンス上で構成されているプロキシサーバーの IP アドレスです。透過プロキシは、名前が示すように、クライアントに対して透過的です。SWG アプライアンスはインライン展開で構成され、アプライアンスはすべての HTTP および HTTPS トラフィックを透過的に受け入れます。

Q: Citrix SWG には構成ウィザードがありますか？

A. はい。ウィザードは、構成ユーティリティの SWG ノードにあります。

Q: Citrix SWG を構成する際に使用される Citrix ADC 機能はどれですか？

A. レスポンダー、AAA-TM、コンテンツスイッチング、SSL、フォワードプロキシ、SSL インターセプト、および URL フィルタリング

Q: Citrix SWG ではどのような認証方法がサポートされていますか？

A. 明示プロキシモードでは、LDAP、RADIUS、TACACS+、およびネゴシエート認証方式がサポートされます。トランスペアレントモードでは、LDAP 認証だけがサポートされます。

Q: クライアントデバイスに CA 証明書をインストールする必要がありますか？

A. はい。Citrix SWG アプライアンスは、オリジンサーバー証明書をエミュレートします。このサーバー証明書は、再生成されたサーバー証明書を信頼できるように、信頼された CA 証明書によって署名されている必要があります。この証明書は、クライアントのデバイスにインストールされている必要があります。

Q: Citrix SWG プラットフォームで Citrix ADC プラットフォームライセンスを使用できますか？

A. なし Citrix SWG プラットフォームには、独自のプラットフォームライセンスが必要です。

Q: 高可用性は Citrix Secure Web Gateway の展開でサポートされていますか？

A. はい。

Q: Citrix SWG のログが含まれているファイルはどれですか。

A. ns.log ファイルには、Citrix SWG 情報が記録されます。CLI または GUI を使用してロギングを有効にする必要があります。コマンドプロンプトで、「**syslogparams-ssli** 有効」と入力します。

GUI で、[システム]>[監査]に移動します。[設定]で、[監査 **Syslog** 設定の変更]をクリックします。[**SSL** インターセプト]を選択します。

Q: 問題のトラブルシューティングにはどの nsconmsg コマンドを使用できますか？

A. 次のコマンドの一方または両方を使用できます。

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

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

Q: 証明書バンドルが組み込まれている場合、更新はどのように入手できますか。

A. 最新のバンドルがビルドに含まれています。アップデートについては、Citrix サポートにお問い合わせください。

Q: Citrix SWG から Citrix ADM でデータをキャプチャできますか？

A. はい。Secure Web **Gateway** ウィザードでアナリティクスを有効にする必要があります。

重要: MAS と SWG で同じ 12.0 ビルドを使用していることを確認してください。

Q: URL フィルタリングサービスとは何ですか？

A. URL フィルタリングは、制限された Web サイトおよび Web ページのリストへのアクセスを制御する Web コンテンツフィルタです。このフィルタは、URL カテゴリ、カテゴリグループ、評価スコアに基づいて、インターネット上の不適切なコンテンツへのユーザーアクセスを制限します。ネットワーク管理者は、Web トラフィックを監視し、非常に危険な Web サイトへのユーザーアクセスをブロックできます。この機能を実装するには、ポリシー適用に基づいて URL 分類機能または URL リスト機能を使用します。詳細については、[URL フィルタリング](#)を参照してください。

Q: URL フィルタリングは Citrix SWG にどのように適合しますか？

A. URL フィルタリングは、Citrix SWG アプライアンスを使用して特定の Web サイトへのアクセスを制御します。ネットワークのエッジにある SWG アプライアンスは、Web トラフィックをインターセプトし、認証、検査、キャッシュ、リダイレクトなどのアクションを実行するプロキシとして機能します。フィルタは、URL 分類機能または URL リスト機能を使用して、ポリシーを適用して Web サイトへのアクセスを制御します。

Q: URL 分類データベースの更新頻度はどれくらいですか。

A. URL 分類機能を使用して制限された Web サイトへのアクセスを制御する場合は、クラウドベースのベンダーサービスの最新データを使用して分類データベースを定期的に更新する必要があります。データベースを更新するために、Citrix SWG GUI では、「DB の更新間隔時間」や「DB の更新時間」などの URL フィルタリングパラメータを構成できます。

Q: 今日の URL フィルタリングサービスに最適なユースケースは何ですか？

A. 企業のお客様向けのターゲットとなるユースケースの一部を以下に示します。

- [URL レピュテーションスコアによる URL フィルタリング](#)
- [企業コンプライアンス下におけるインターネット利用制御](#)
- [カスタム URL リストを使用した URL フィルタリング](#)

Q: URL 分類サービスでのキャッシュのメモリ制限はありますか？

A. はい。キャッシュのメモリ制限は 10 GB に設定され、CLI インターフェイスだけで設定できます。

Q: 着信要求に一致するカテゴリがない場合、URL 分類データベースは何を返しますか。

A. 着信要求がカテゴリと一致しない場合、または URL の形式が正しくない場合、アプライアンスは URL を「Uncategorized」としてマークし、カテゴリ化ベンダーが管理するクラウドベースのサービスに要求を送信します。アプライアンスは、クラウドクエリーフィードバックを監視し続け、キャッシュを更新して、今後の要求がクラウドルックアップの恩恵を受けることができるようにします。

Q: URL レピュテーションスコアとは何ですか。また、レピュテーションスコアに基づいて悪意のある Web サイトへのアクセスをどのように制御しますか？

A. URL レピュテーションスコアは、Citrix SWG が Web サイトに割り当てる評価です。値の範囲は 1 ~4 です。4 は悪意のある Web サイト、1 はクリーンな Web サイトです。ネットワーク管理者がリスクの高い Web サイトにアクセスするユーザーを監視する場合、そのようなサイトへのアクセスは、Citrix SWG アプライアンスで構成した URL レピュテーションスコアとセキュリティレベルに基づいて制御されます。詳しくは、「[URL レピュテーションスコア](#)」を参照してください。

Q: URL セットを使用してウェブサイトをフィルタリングしても、特定の Web サイトを誤ってフィルタリングした場合、例外的な Web サイトを有効にするプロセスは何ですか。

A. URL フィルタリングは、レスポンスポリシーを使用して Web サイトへのアクセスを制御します。特定の URL を例外としてホワイトリストに登録するには、SWG ウィザードでパッチセットポリシーを作成し、例外の URL を「許可」アクションとともに追加します。ポリシーを作成したら、ウィザードを終了し、次の手順を実行します。

Citrix SWG GUI を使用してポリシー式の優先度を変更するには：

1. **Citrix SWG** アプライアンスにログオンし、[**Secure Web Gateway**] > [プロキシ仮想サーバー] に移動します。
2. 詳細ページで、サーバーを選択し、[**Edit**] をクリックします。
3. [プロキシ仮想サーバー] ページで、[ポリシー] セクションに移動し、鉛筆アイコンをクリックして詳細を編集します。
4. patset ポリシーを選択し、[**Policy Binding**] ページで、他のバインドされたポリシーよりも低いプライオリティ値を指定します。
5. [バインド] と [完了] をクリックします。

Q: Citrix SWG URL フィルタリング機能を使用する主な利点は何ですか？

A. URL フィルタリング機能は、展開、構成、および使用が簡単です。これにより、次のようなメリットがもたらされ、企業のお客様は以下を実現できます。

- Web トラフィックとユーザトランザクションを監視する
- マルウェアやインターネットによるセキュリティ脅威をフィルタリングします。
- 悪意のあるウェブサイトへの不正アクセスを制御します。
- 企業のセキュリティポリシーを適用して、制限されたデータへのアクセスを制御します。

Q: URL リスト機能を使用して Web サイトをフィルタリングしている場合、URL リストポリシーを編集する方法はありますか。

A. Citrix SWG ウィザードを使用して、レスポンスポリシーにバインドされたインポートされたリストを上書きまたは削除することで、URL リストポリシーを変更できます。

Q: URL に関連付けられたメタデータには何が含まれていますか？

A. 分類データベースの各 URL には、それに関連付けられたメタデータがあります。メタデータには、URL カテゴリ、カテゴリグループ、および評価スコア情報が含まれます。たとえば、URL がショッピングポータルの場合、メタデータはそれぞれ [ショッピング]、[ショッピング/小売]、および [1] になります。

次の式を使用して、着信 URL のこれらの値を取得します。式は次のとおりです。

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

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

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

Q: URL 分類機能に必要なライセンスとサブスクリプションの種類は何ですか？

A. URL 分類機能を使用するには、Citrix SWG エディションで URL 脅威インテリジェンスサブスクリプションサービス（1年または3年間利用可能）が必要です。

Q: URL フィルタリングを設定する方法は何ですか？

A. URL フィルタリングを構成するには、2つの方法があります。この操作は、Citrix SWG コマンドインターフェイスまたは Citrix SWG ウィザードを使用して実行できます。ウィザードを使用してフィルタリングポリシーを構成することをお勧めします。

Q: ブロックできる URL カテゴリの種類は何ですか？

A. URL 分類データベースには、メタデータを持つ数百万の URL が含まれています。管理者は、レスポンスポリシーを構成して、ブロックできる URL カテゴリと、ユーザーアクセスを許可する URL カテゴリを決定できます。URL カテゴリのマッピングについては、[カテゴリのマッピング](#) ページを参照してください。

Q. WebSocket を使用するオリジンサーバーにアクセスできない場合はどうしたらいいですか ([whatsapp](#)など)。

デフォルトの HTTP プロファイルで WebSocket を有効にする必要があります。

CLI で、次のように入力します。

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

ICAP って何ですか

ICAP は、インターネットコンテンツ適応プロトコルの略です。

ICAP をサポートしている Citrix SWG のバージョンはどれですか？

ICAP は、Citrix SWG リリース 12.0 ビルド 57.x 以降でサポートされています。

Citrix SWG でサポートされる 2 つの ICAP モードは何ですか？

リクエスト変更 (**REQMOD**) モードと応答変更 (**RESPMOD**) モードがサポートされています。

ICAP のデフォルトポートは何ですか。

1344.



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