

次世代ファイアウォール USG シリーズ設定例

USG シリーズの UTM 機能の推奨設定とその設定方法

はじめに

USG シリーズには様々な UTM 機能が搭載されています。各 UTM 機能の概要と弊社としての推奨設定は下表のとおりです。

名称	概要	推奨設定
App Patrol	USG シリーズを通したネットワークを使用するアプリケーションの動作禁止・許可を設定します。	使用します。 Youtube, Facebook, Skype, Twitter, Dropbox の使用を禁止し、ログを取る例を示します。
Contents Filter	Web アクセスの禁止・許可を設定します。設定はカテゴリ単位で行います。	使用します。 設定方法の説明で、設定例を示します。
IDP	外部からの不正アクセスを検知し、遮断します。	使用します。 設定はデフォルトとします。
Anti-Virus	マルウェアの脅威から包括的かつリアルタイムにネットワークを保護します。	使用します。 設定はデフォルトとします。
Anti-Spam	送信者を評価することにより、スパムメールを判断します。スパムと判定したメールは、自動削除・タグをつけて受信等の設定を選択できます。	使用します。 スパムメールについてはタグをつけてそのまま受信します。（誤検知によりスパムでないメールが削除されることを防ぐため。） 必要に応じて White List を使用します。
SSL Inspection	SSL 通信で通信する両者の間に入り、通信の内容を復号して各 UTM 機能を適用し、再暗号化して送信します。	現状では使用しません。

App Patrol の設定方法

App Patrol の設定方法を説明します。LAN ゾーンから Facebook, Skype, Twitter, Youtube, Dropbox の使用を禁止し、ログを取る設定にするには、以下のようにします。

1. アプリケーションオブジェクトの作成

Configuration -> Object -> Application で、制御したいアプリケーションを選択し、アプリケーションオブジェクトを作成します。

2. アプリケーションプロファイルの作成

Configuration -> UTM Profile -> App Patrol で、1. で作成したアプリケーションオブジェクトに対する制御内容(許可/不許可)を選択します。

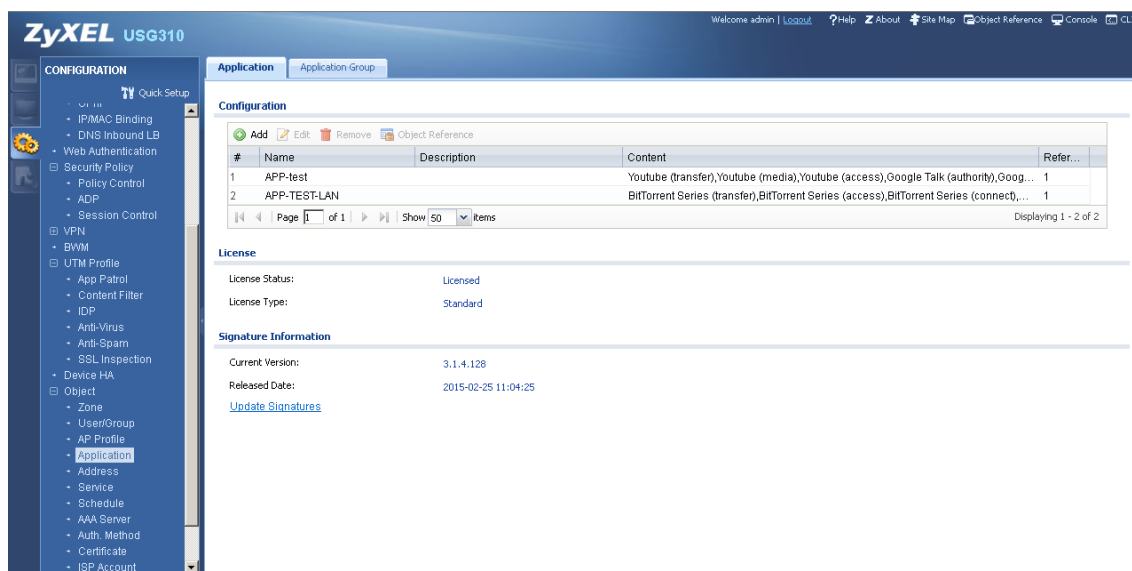
3. ポリシーコントロールの設定

Configuration -> Security Policy -> Policy Control でポリシーコントロールルールを選択し、そのルールに対して2. で作成したアプリケーションプロファイルを適用するように設定します。

詳しくは、以下の通りです。

1. アプリケーションオブジェクトの作成

- ① Configuration -> Object -> Application を開きます。
- ② Configuration の下の Add をクリックします。Add Application Rule 画面が開きます。



- ③ Add Application Rule 画面で、Add をクリックします。Add Application Object 画面が開きます。

Add Application Rule

Name:

Description: (Optional)

Add Remove

#	Category	Application
---	----------	-------------

Page 1 of 1 | Show 50 items | No data to display

OK Cancel

- ④ Add Application Object 画面で、Query の Search で By Service を選択し、Youtube と入力して Search をクリックします。
- ⑤ Query Result で全てにチェックを入れ、OK をクリックします。

Add Application Object

Query

Search:

Query Result

#	<input checked="" type="checkbox"/>	Category	Application
1	<input checked="" type="checkbox"/>	Streaming Media	Youtube (transfer)
2	<input checked="" type="checkbox"/>	Streaming Media	Youtube (media)
3	<input checked="" type="checkbox"/>	Streaming Media	Youtube (access)

Page 1 of 1 | Show 50 items | Displaying 1 - 3 of 3

- ⑥ Add Application Rule 画面に戻るので、Name 欄に適当な名称(ここでは Youtube)を入力し、OK をクリックします。

Add Application Rule

Name:

Description: (Optional)

#	Category	Application
1	Streaming Media	Youtube (transfer)
2	Streaming Media	Youtube (media)
3	Streaming Media	Youtube (access)

Page 1 of 1 | Show 50 items | Displaying 1 - 3 of 3

OK Cancel

- ⑦ Application Object 一覧画面に戻るので、Youtube が追加されていることを確認します。

ZyXEL USG310

CONFIGURATION

- Quick Setup
- IP/MAC Binding
- DNS Inbound LB
- Web Authentication
- Security Policy
- Policy Control
- ADP
- Session Control
- VPN
- BWM
- UTM Profile
- App Patrol
- Content Filter
- IDP
- Anti-Virus
- Anti-Spam
- SSL Inspection
- Device HA
- Object
- Zone
- User/Group
- AP Profile
- Application**
- Address
- Service
- Schedule
- AAA Server
- Auth. Method
- Certificate
- ISP Account

Application | Application Group

Configuration

#	Name	Description	Content	Refer...
1	APP-test		Youtube (transfer), Youtube (media), Youtube (access), Google Talk (authority), Goog...	1
2	APP-TEST-LAN		BitTorrent Series (transfer), BitTorrent Series (access), BitTorrent Series (connect,...	1
3	Youtube		Youtube (transfer), Youtube (media), Youtube (access)	0

Page 1 of 1 | Show 50 items | Displaying 1 - 3 of 3

License

License Status: Licensed

License Type: Standard

Signature Information

Current Version: 3.1.4.128

Released Date: 2015-02-25 11:04:25

[Update Signatures](#)

- ⑧ 同様に、Facebook, Skype, Twitter, Dropbox のアプリケーションオブジェクトを作成します。

ZyXEL USG310 Welcome admin | Logout ? Help Z About Site Map Object Reference Console CLI

CONFIGURATION Quick Setup

- Licensing
- Wireless
- Network
 - Interface
 - Routing
 - DDNS
 - NAT
 - HTTP Redirect
 - ALG
 - UPnP
 - IP/MAC Binding
 - DNS Inbound LB
- Web Authentication
- Security Policy
- VPN
- BWM
- UTM Profile
- Device HA
- Object
- Zone
- User/Group
- AP Profile
- Application**
- Address
- Service
- Schedule
- AAA Server
- Auth. Method
- Certificate

Application Application Group

Configuration

Add Edit Remove Object Reference

#	Name	Description	Content	Refer...
1	APP-test		Youtube (transfer), Youtube (media), Youtube (access), Google Talk (authority), Goo...	1
2	APP-TEST-LAN		BitTorrent Series (transfer), BitTorrent Series (access), BitTorrent Series (connect), ...	1
3	Youtube		Youtube (transfer), Youtube (media), Youtube (access)	1
4	Facebook		Facebook (authority), Facebook (access)	0
5	Skype		Skype (authority), Skype (media), Skype (connect)	0
6	Twitter		Twitter (authority), Twitter (access)	0
7	Dropbox		Dropbox (authority), Dropbox (access), Dropbox LanSync (connect)	0

Page 1 of 1 Show 50 Items Displaying 1 - 7 of 7

License

License Status: Licensed

License Type: Standard

Signature Information

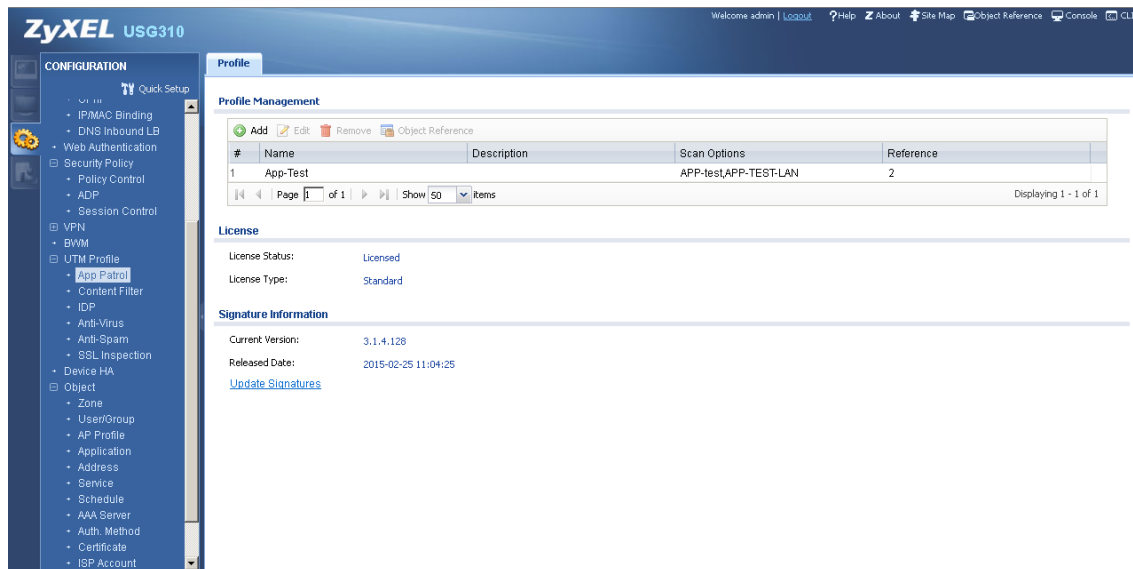
Current Version: 3.1.4.131

Released Date: 2015-03-18 11:29:02

[Update Signatures](#)

2. Application Profile の作成

- ① Configuration -> UTM Profile -> App Patrol を開きます。
- ② Profile Management の Add をクリックします。Add Rule 画面が開きます。



- ③ Add Rule 画面の Profile Management で、Add をクリックします。Add Application 画面が開きます。

Add rule

General Settings

Name:

Description:

Profile Management

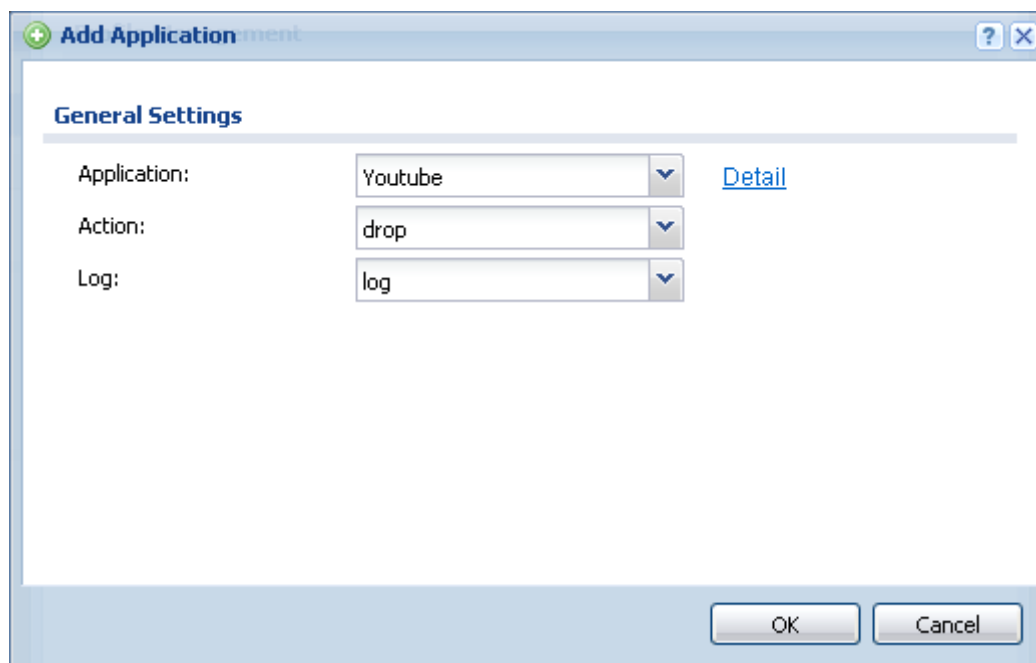
Add Edit Remove

#	Application	Action	Log
---	-------------	--------	-----

Page 1 of 1 | Show 50 items | No data to display

OK Cancel

- ④ Add Application 画面で、Application で Youtube を、Action で drop を選択して OK をクリックします。



- ⑤ 同様に、Facebook, Skype, Twitter, Dropbox を設定します。

- ⑥ Add Rule 画面で Profile Management 欄に Youtube が追加されたことを確認して、Name に適当な名前(この例では App_sample)を入力して OK をクリックします。

Add rule

General Settings

Name: App_sample

Description:

Profile Management

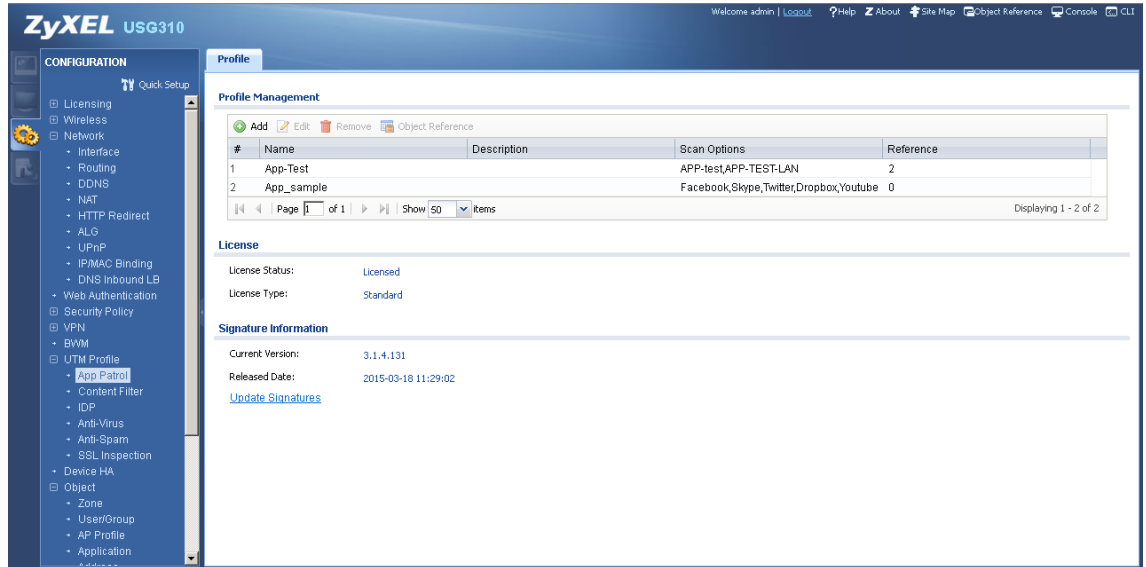
Add Edit Remove

#	Application	Action	Log
1	Youtube	drop	log
2	Facebook	drop	log
3	Skype	drop	log
4	Twitter	drop	log
5	Dropbox	drop	log

Page 1 of 1 Show 50 items Displaying 1 - 5 of 5

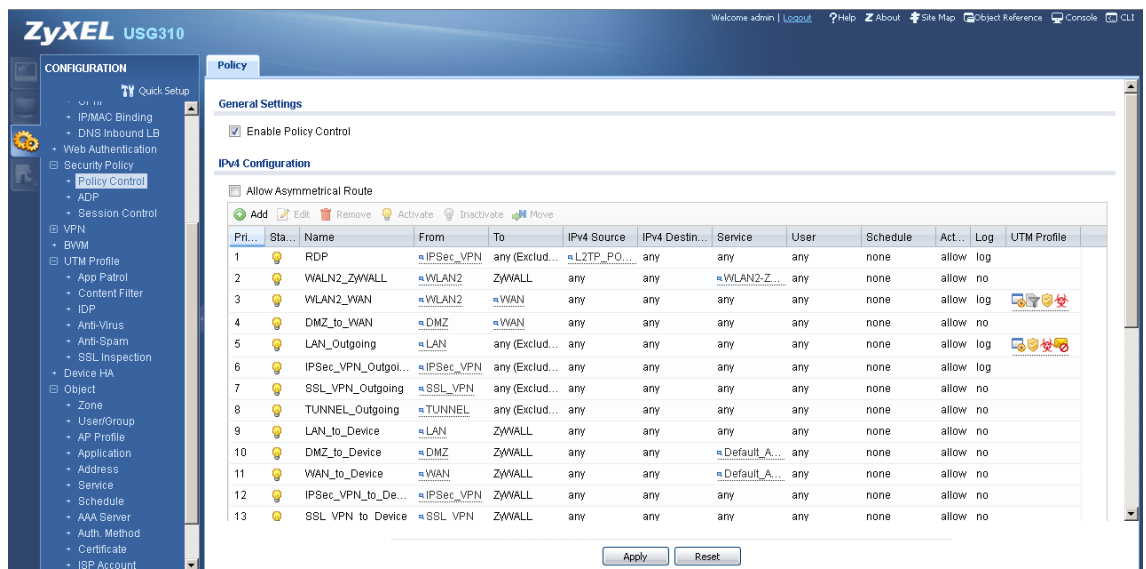
OK Cancel

- ⑦ Application Profile 一覧に戻るので、一覧に App_sample が追加されていることを確認します。



3. Policy Control の設定

- ① Configuration -> Security Policy -> Policy Control を開きます。
- ② LAN_Outgoing を選択して Edit をクリックします。



- ③ UTM Profile で Application Patrol にチェックを入れ、App_sample を選択します。OK をクリックします。

The screenshot shows the 'Edit Policy5' dialog box with the 'UTM Profile' tab selected. The 'General Settings' section at the top has the following values: User: any, Schedule: none, Action: allow, and Log matched traffic: log. The 'UTM Profile' section contains a list of security features with checkboxes and dropdown menus. The 'Application Patrol' checkbox is checked and set to 'App_sample'. The other features are also checked and have specific profiles selected. The 'Log' column for all features is set to 'by profile'. At the bottom right, there are 'OK' and 'Cancel' buttons.

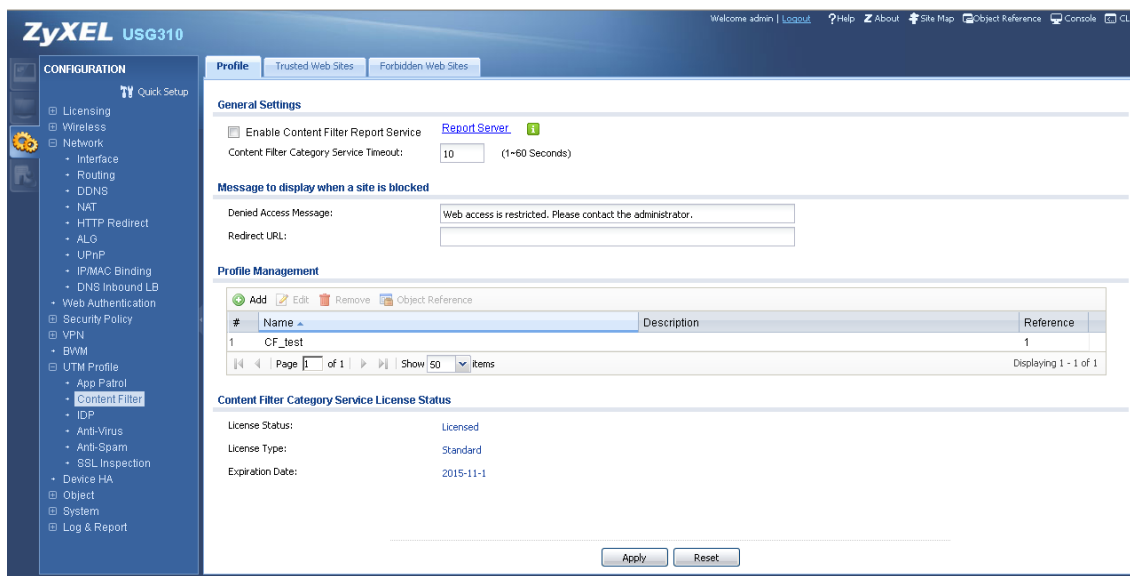
Feature	Setting	Log
Application Patrol	App_sample	by profile
Content Filter	CF_sample	by profile
IDP	SPF5583	by profile
Anti-Virus	AV-test	by profile
Anti-Spam	Anti-Spam-test	by profile
SSL Inspection	none	by profile

以上となります。

Contents Filter の設定方法

Contents Filter の設定方法を説明します。LAN ゾーンから業務に関係ないウェブサイトへのアクセスをブロックするように設定するには、以下のようにします。

- ① Configuration -> UTM Profile -> Content Filter で Profile タブを開きます。
- ② Profile Management で Add をクリックします。



- ③ Add Filter Profile 画面が開くので、Category Service タブを選択します。
- ④ General Settings で Name にこの Profile を識別するための任意の名称を半角英数字で設定(ここでは CF_sample とする)し、Enable Content Filter Category Service にチェックを入れます。
- ⑤ Action When Category Server Is Unavailable は Pass に設定します。

The screenshot shows the 'Edit Filter Profile CF_sample' dialog box with the 'Category Service' tab selected. The 'General Settings' section includes fields for License Status (Licensed), License Type (Standard), Name (CF_sample), and Description (Optional). The 'Enable Content Filter Category Service' checkbox is checked. Below it, four actions are listed with dropdown menus and checkboxes: 'Action for Unsafe Web Pages' (Warn, Log), 'Action for Managed Web Pages' (Block, Log), 'Action for Unrated Web Pages' (Warn, Log), and 'Action When Category Server Is Unavailable' (Pass, Log). The 'Select Categories' section has 'Select All Categories' and 'Clear All Categories' checkboxes. The 'Security Threat (unsafe)' section has checkboxes for 'Anonymizers', 'Botnets', and 'Compromised', all of which are checked. The dialog box has 'OK' and 'Cancel' buttons at the bottom right.

Edit Filter Profile CF_sample

Category Service Custom Service

General Settings

License Status: Licensed

License Type: Standard

Name: CF_sample

Description: (Optional)

☒ Enable Content Filter Category Service

Action for Unsafe Web Pages:	Warn	<input checked="" type="checkbox"/> Log
Action for Managed Web Pages:	Block	<input checked="" type="checkbox"/> Log
Action for Unrated Web Pages:	Warn	<input checked="" type="checkbox"/> Log
Action When Category Server Is Unavailable:	Pass	<input checked="" type="checkbox"/> Log

Select Categories

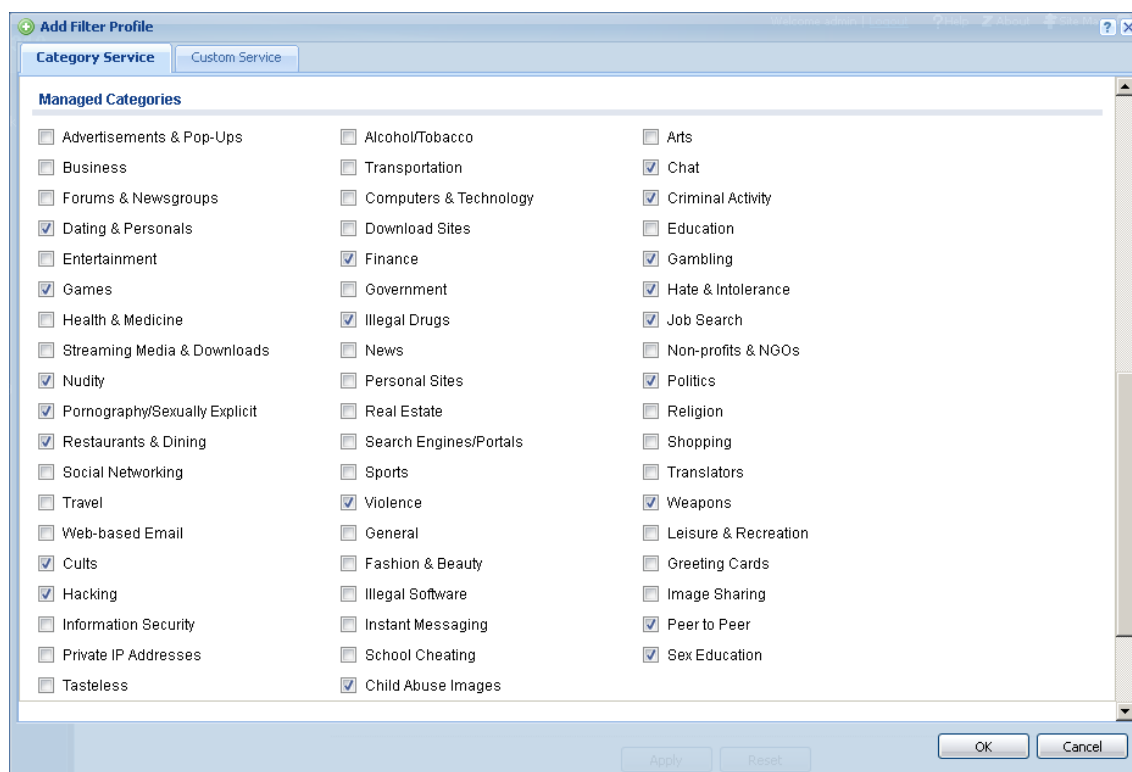
☐ Select All Categories ☐ Clear All Categories

Security Threat (unsafe)

☒ Anonymizers ☒ Botnets ☒ Compromised

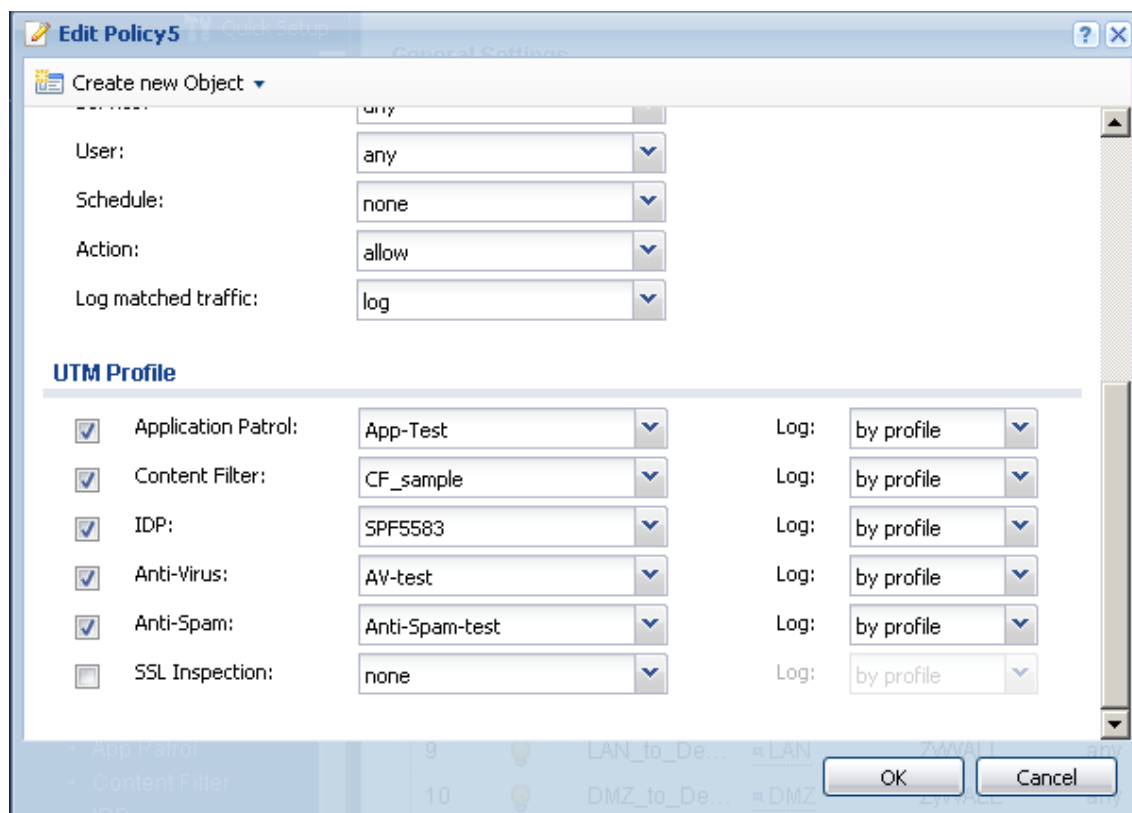
OK Cancel

- ⑥ Managed Categories で、アクセスをブロックしたいカテゴリにチェックを入れます。
下図は、設定の一例です。



- ⑦ OK をクリックします。

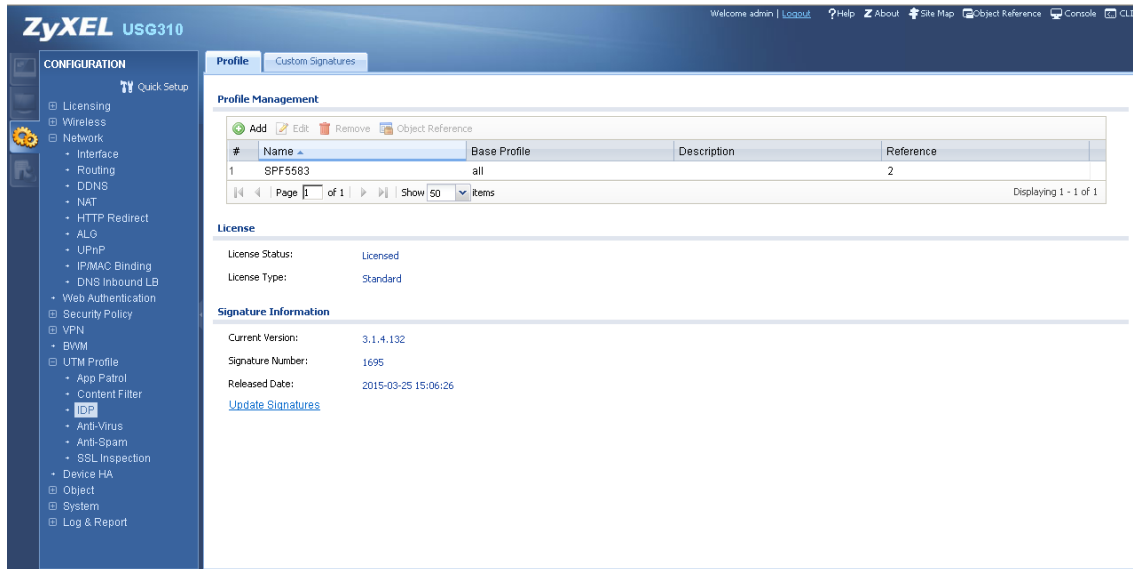
- ⑧ Configuration -> Security Policy -> Policy Control を開きます。
- ⑨ from: LAN, to: any (Excluding ZyWALL) のルールを選択し、Edit をクリックします。
- ⑩ Edit Policy#のウィンドウが開くので、UTM Profile で Contents Filter にチェックを入れ、CF_sample を選択して OK をクリックします。



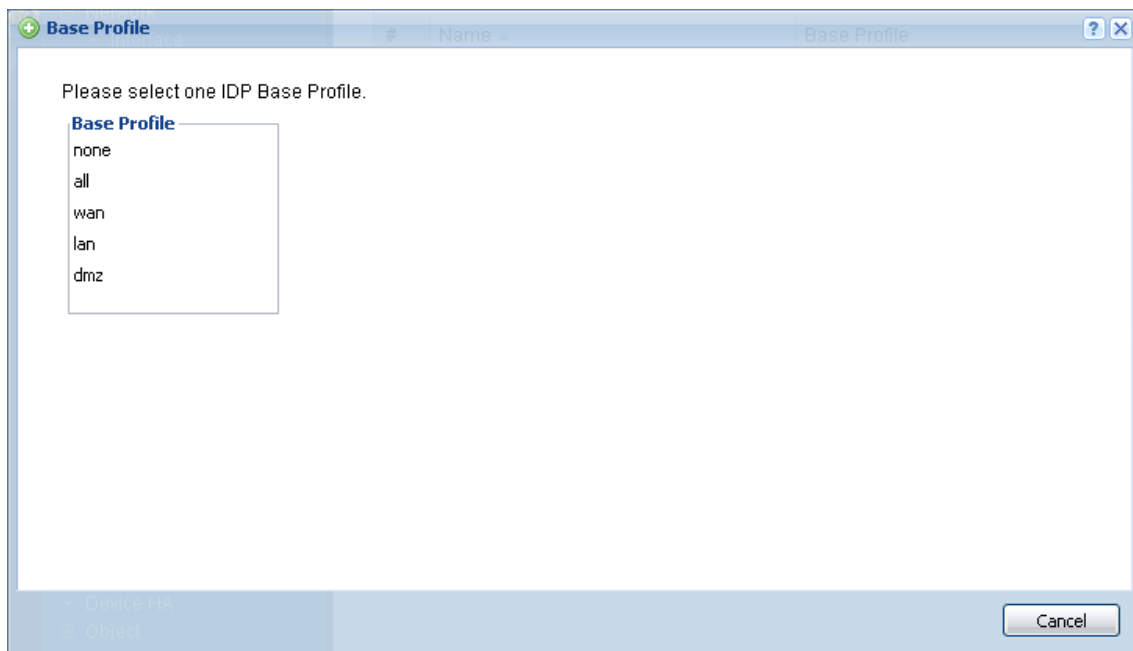
以上となります。

IDP の設定方法

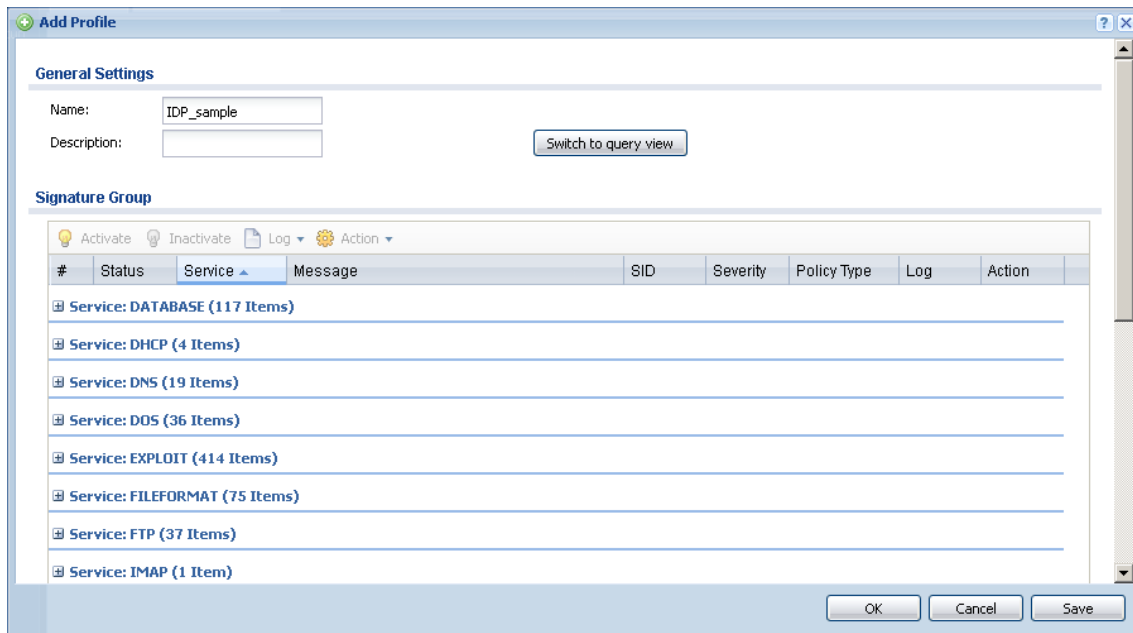
- ① Configuration -> UTM Profile -> IDP を開き、Profile タブを選択します。
- ② Profile Management で Add をクリックします。



- ③ Base Profile ウィンドウが開くので、all を選択します。(※)



- ④ Add Profile ウィンドウが開くので、Name にこの Profile を識別するための任意の名称を半角英数字で設定し、OK をクリックします。(※)



※ これはデフォルトの設定です。カスタマイズ方法についての詳細はユーザーズガイドを参照してください。

- ⑤ Configuration -> Security Policy -> Policy Control を開きます。
- ⑥ from: LAN, to: any (Excluding ZyWALL) のルールを選択し、Edit をクリックします。
- ⑦ Edit Policy#のウィンドウが開くので、UTM Profile で IDP にチェックを入れ、作成した Profile 名を選択して OK をクリックします。

Anti-Virus の設定方法

- ① Configuration -> UTM Profile -> Anti-Virus を開き、Profile タブを選択します。
- ② Profile Management で Add をクリックします。

The screenshot displays the ZyXEL USG310 web management interface. The left sidebar shows the 'CONFIGURATION' menu with 'Anti-Virus' selected under 'UTM Profile'. The main content area is titled 'Profile Management' and includes a table with one entry named 'AV-test'. Below the table, the 'License' section shows 'Licensed' status and 'Standard' type. The 'Signature Information' section displays version 2.0.1.135, signature number 684077, and release date 2015-03-25 09:39:58, with a link to 'Update Signatures'.

ZyXEL USG310 Welcome admin | Logout ? Help Z About Site Map Object Reference Console CLI

CONFIGURATION Quick Setup

- Licensing
- Wireless
- Network
 - Interface
 - Routing
 - DDNS
 - NAT
 - HTTP Redirect
 - ALG
 - UPnP
 - IP/MAC Binding
 - DNS Inbound LB
- Web Authentication
- Security Policy
- VPN
- BWM
- UTM Profile
 - App Patrol
 - Content Filter
 - IDP
 - Anti-Virus**
 - Anti-Spam
 - SSL Inspection
- Device HA
- Object
- System
- Log & Report

Profile Management

Add Edit Remove Object Reference

#	Name	Description	Reference
1	AV-test	New Create	2

Page 1 of 1 | Show 50 Items | Displaying 1 - 1 of 1

License

License Status: Licensed
License Type: Standard

Signature Information

Current Version: 2.0.1.135
Signature Number: 684077
Released Date: 2015-03-25 09:39:58
[Update Signatures](#)

https://192.168.5.1/ext-js/web-pages/index/index.html

- ③ Add Rule 画面が開くので、Name にこの Profile を識別するための任意の名称を半角英数字で設定し、OK をクリックします。(※)

※ これはデフォルトの設定です。カスタマイズ方法についての詳細はユーザーズガイドを参照してください。

Add Rule

Configuration

Name:

Description: (Optional)

Actions When Matched

☒ Destroy infected file

Log: ▼

File decompression

☒ Enable file decompression (ZIP and RAR)

☐ Destroy compressed files that could not be decompressed

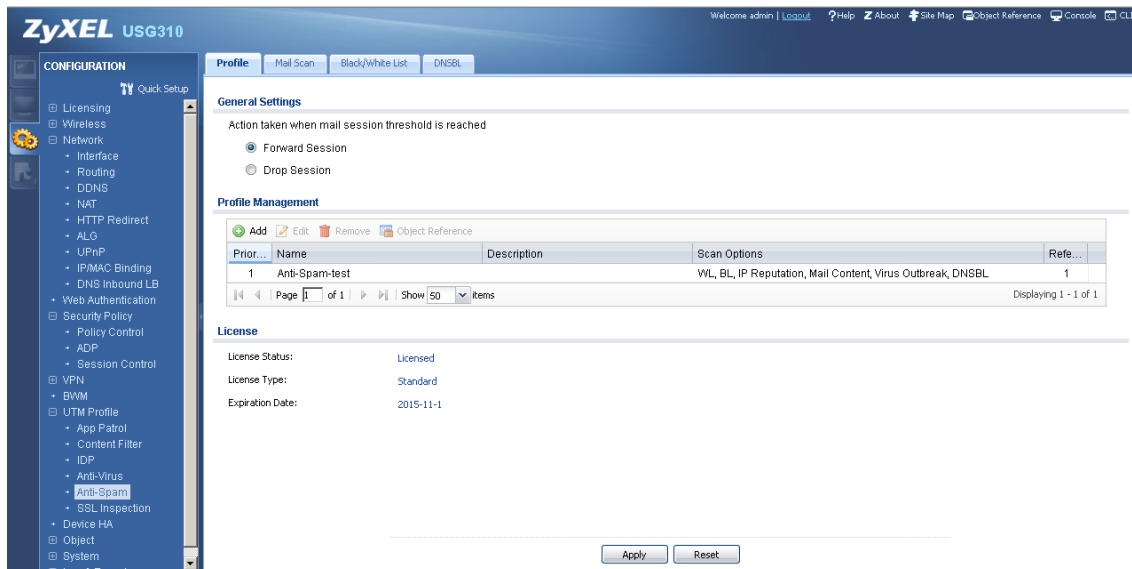
OK Cancel

- ④ Configuration -> Security Policy -> Policy Control を開きます。
- ⑤ from: LAN, to: any (Excluding ZyWALL) のルールを選択し、Edit をクリックします。
- ⑥ Edit Policy#のウィンドウが開くので、UTM Profile で Anti-Virus にチェックを入れ、作成した Profile 名を選択して OK をクリックします。

Anti-Spam

Anti-Spam の設定方法

- ① Configuration -> UTM Profile -> Anti-Spam を開き、Profile タブを選択します。
- ② Profile Management で Add をクリックします。



- ③ Add Rule 画面が開くので、Name にこの Profile を識別するための任意の名称を半角英数字で設定し、OK をクリックします。(※)

※ これはデフォルトの設定です。カスタマイズ方法についての詳細はユーザーズガイドを参照してください。

Add rule

General Settings

Name: AS_sample

Description:

Log: log

Scan Options

☒ Check White List

☒ Check Black List

☒ Check IP Reputation (SMTP only)

☒ Check Mail Content

☒ Check Virus Outbreak

☒ Check DNSBL

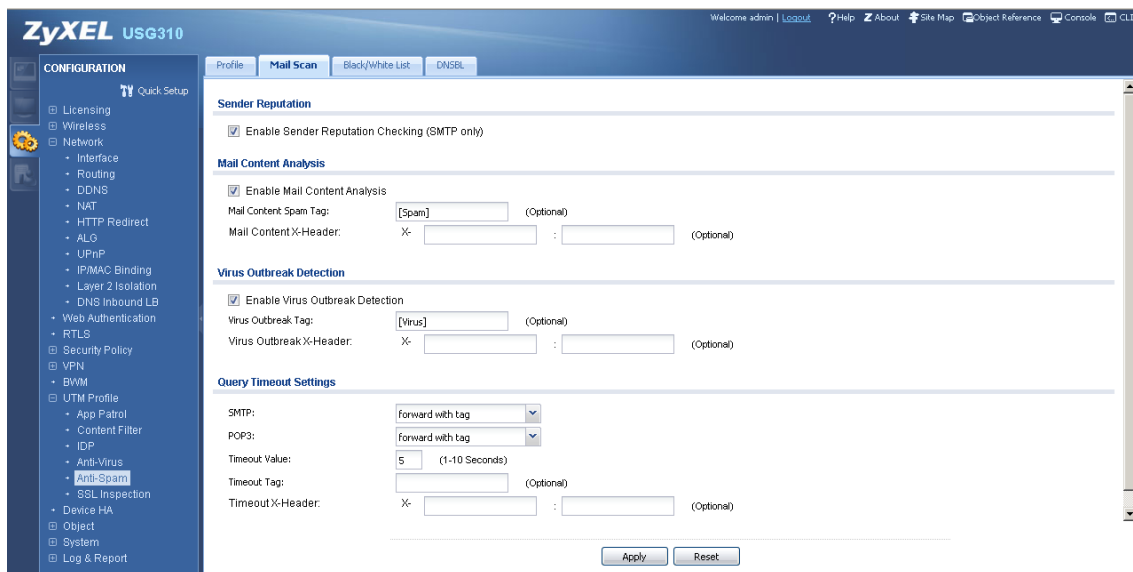
Actions For Spam Mail

SMTP: forward with tag

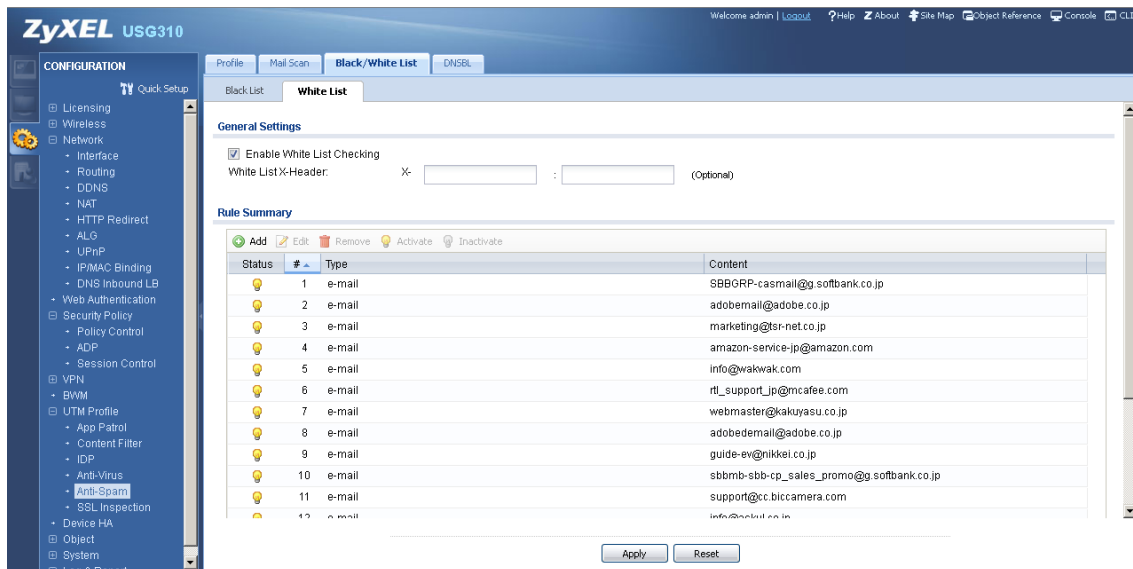
POP3: forward with tag

OK Cancel

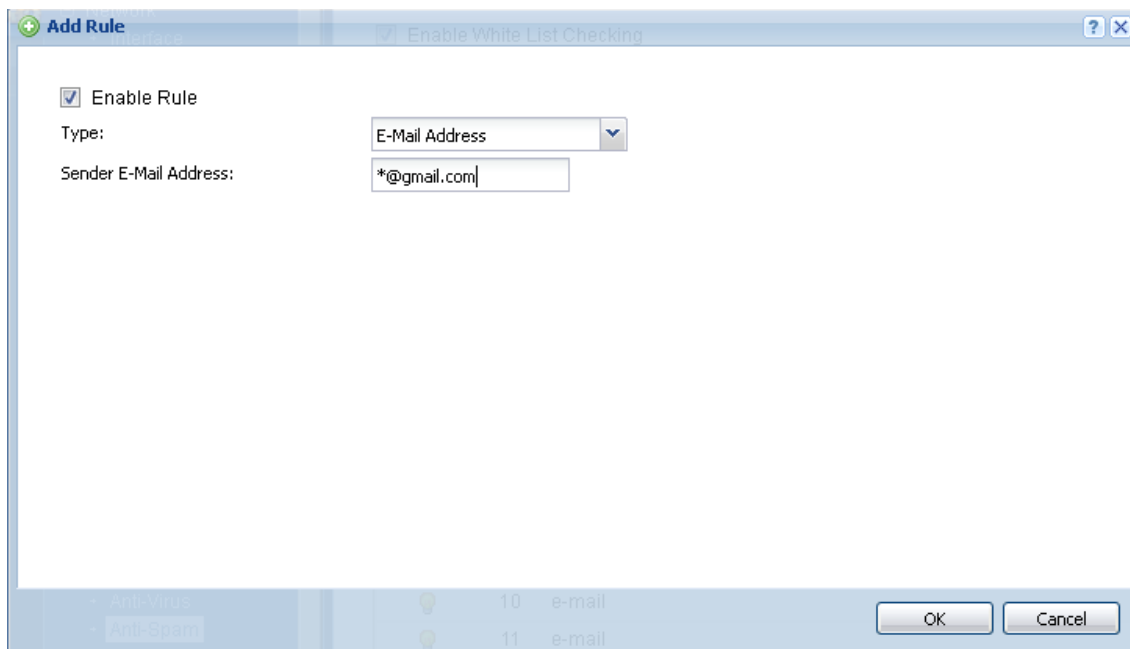
- ④ デフォルトでは、スパムメールの件名の先頭には” [Spam]” という文字列が追加されます。これを変更する場合、Configuration → UTM Profile → Anti-Spam を開き、Mail Scan タブを選択します。
- ⑤ Mail Content Analysis の Mail Content Spam Tag を変更します。例えば、” [SpamMail]” と変更した場合、スパムメールの件名の先頭に” [SpamMail]” という文字列が追加されます。



- ⑥ スパムではないメールがスパムと誤判定される場合、White List に登録することで誤判定を回避することができます。ここでは、xxx@gmail.com（xxx は任意）を全てスパム以外と判定する設定の追加方法を紹介します。
- ⑦ Configuration -> UTM Profile -> Anti-Spam を開き、Black/White List タブを選択し、更に White List タブを選択します。
- ⑧ General Settings で Enable White List Checking にチェックを入れます。
- ⑨ Rule Summary で Add をクリックします。



- ⑩ Add Rule 画面が開くので、Enable Rule にチェックを入れ、Type で E-Mail Address を選択し、Sender E-Mail Address に*@gmail.com と入力し、OK をクリックします。



- ⑪ Configuration -> Security Policy -> Policy Control を開きます。
- ⑫ from: LAN, to: any (Excluding ZyWALL) のルールを選択し、Edit をクリックします。
- ⑬ Edit Policy#のウィンドウが開くので、UTM Profile で Anti-Spam にチェックを入れ、作成した Profile 名を選択して OK をクリックします。

- ⑭ メーラーの設定(ここでは、Windows Live Mail を例として説明します。他のメーラーをご使用の場合は読み替えてください。)
- ⑮ フォルダータブを選択し、メッセージルールをクリックします。
- ⑯ 新規のメール ルールウィンドウが開くので、条件で「件名に指定した文字列が含まれる場合」、アクションで「指定のフォルダーに移動する」をチェックしてください。

新規のメール ルール

POP 電子メール アカウントの新しいルールを作成します。

注意: Windows Live Hotmail などの IMAP または HTTP の電子メール アカウントに対して、ルールは適用されません。

1 つ以上の条件を選択してください(C):

- ☐ 差出人にユーザーが含まれる場合
- ☒ 件名に指定した文字列が含まれる場合
- ☐ メッセージ本文に指定した文字列が含まれる場合
- ☐ 宛先にユーザーが含まれる場合

1 つ以上のアクションを選択してください(A):

- ☒ 指定のフォルダーに移動する
- ☐ 指定のフォルダーにコピーする
- ☐ 削除する
- ☐ 指定したユーザーに転送する

この説明を編集するには、下線付きの単語をクリックしてください(D):

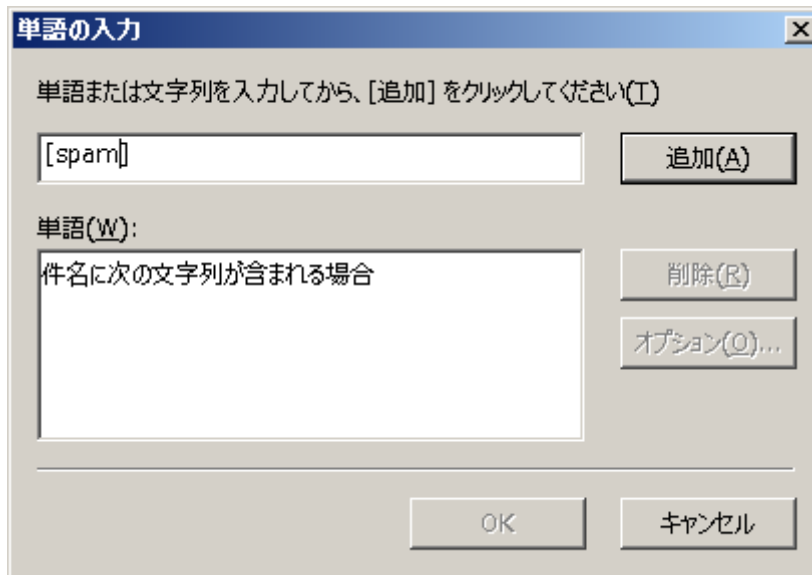
メッセージを受信してから、このルールを適用する
件名に指定した文字列が含まれる場合
指定のフォルダーに移動する

このルールの名前を入力してください(N):

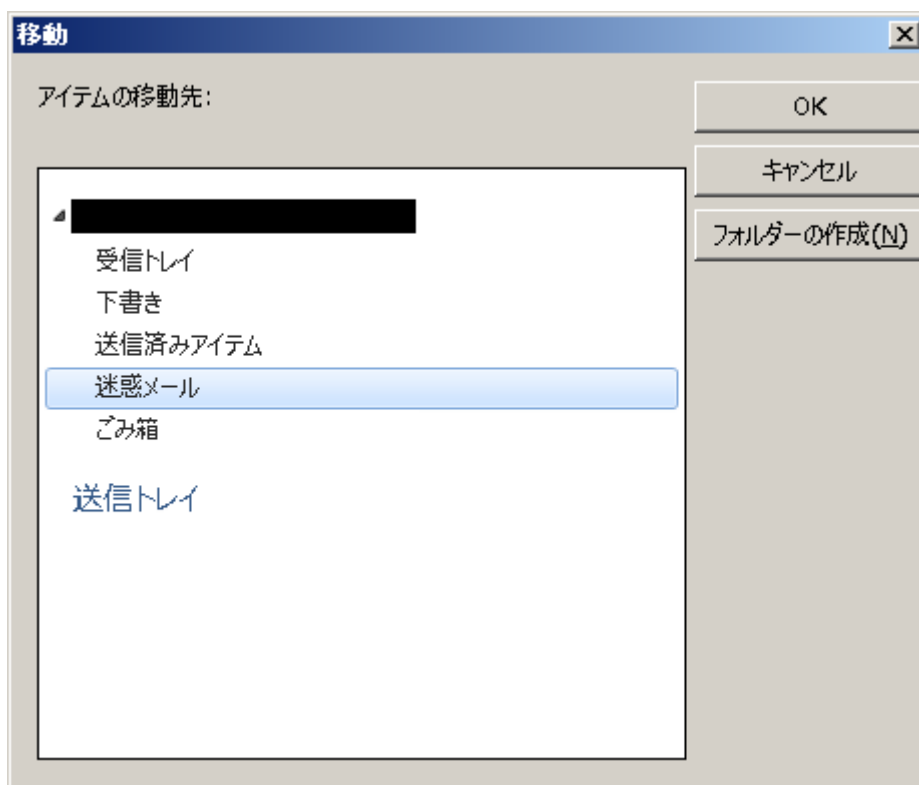
新規の電子メール ルール #1

ルールを保存 キャンセル

- ⑪ 編集テキストボックスで「指定した文字列が含まれる」をクリックしてください。単語の入力ウィンドウが開くので、[spam]と入力して追加をクリックします。(ここでは、手順⑤でスパムメールの件名に追加する文字列を”[Spam]”から変更しなかった場合を説明します。変更した場合はここで指定する文字列も変更してください。)



- ⑫ 編集テキストボックスで「指定のフォルダー」をクリックしてください。移動ウィンドウが開くので、迷惑メールを選択してOKをクリックします。



SSL Inspection の設定方法(弊社では、使用を推奨しません)

- ① Configuration -> UTM Profile -> SSL Inspection を開き、Profile タブを選択します。
- ② Profile Management で Add をクリックします。
- ③ Add Rule 画面が開くので、Name にこの Profile を識別するための任意の名称を半角英数字で設定し、OK をクリックします。(※)
※ これはデフォルトの設定です。カスタマイズ方法についての詳細はユーザーズガイドを参照してください。
- ④ Configuration -> Security Policy -> Policy Control を開きます。
- ⑤ from: LAN, to: any (Excluding ZyWALL) のルールを選択し、Edit をクリックします。
- ⑥ Edit Policy#のウィンドウが開くので、UTM Profile で SSL Inspection にチェックを入れ、作成した Profile 名を選択して OK をクリックします。