

ビジネスインターネット接続サービス  
UTM タイプ  
カスタマコントロール利用マニュアル

第 3.2 版  
NTTPC コミュニケーションズ

2024 年 10 月 25 日

## 内容

1	はじめに	5
1.1	サービスリニューアル	10
2	カスタマコントロールサイトへの接続	11
2.1	カスタマコントロールサイトへのログインについて	11
2.2	初回ログイン時の操作	11
2.3	カスタマコントロールサイトのパスワード変更	12
3	プリセット設定	14
3.1	ファイアウォールルール	14
3.2	ファイアウォールポリシー設定項目	17
3.3	セキュリティ機能	23
4	ファイアウォールルールの設定方法	26
4.1	ファイアウォールルールの追加（表示形式：インターフェースペアビューの場合）	26
4.2	ファイアウォールルールの追加（表示形式：シーケンス別の場合）	30
4.3	ファイアウォールルールの変更（表示形式：インターフェースペアビューの場合）	35
4.4	ファイアウォールルールの変更（表示形式：シーケンス別の場合）	36
4.5	ファイアウォールルールの無効化・削除（表示形式：インターフェースペアビューの場合）	38
4.6	ファイアウォールルールの無効化・削除（表示形式：シーケンス別の場合）	40
4.7	SNAT 設定方法（表示形式：インターフェースペアビューの場合）	43
4.8	SNAT 設定方法（表示形式：シーケンス別の場合）	47
4.9	DNAT 申込時の送信元初期設定“none”の変更方法（表示形式：インターフェースペアビューの場合）	53
4.10	DNAT 申込時の送信元初期設定“none”の変更方法（表示形式：シーケンス別の場合）	56
4.11	DNAT 設定方法（表示形式：インターフェースペアビューの場合）	59
4.12	DNAT 設定方法（表示形式：シーケンス別の場合）	65
5	アドレスの設定方法	72
5.1	アドレスの追加	72
5.2	アドレスの変更	74
5.3	アドレスの削除	76
6	アドレスグループの設定方法	77
6.1	アドレスグループの追加	77
6.2	アドレスグループの変更	78
6.3	ホワイトリスト・ブラックリストへの設定	80
①	Src Black list への設定方法	80
②	Dst Black list への設定方法	81
③	Src White list への設定方法	82

④	Dst White list への設定方法.....	83
6.4	アドレスグループの削除 .....	84
7	サービスの設定方法 .....	85
7.1	サービスの追加 .....	85
7.2	サービスの変更 .....	86
7.3	サービスの削除 .....	88
8	セキュリティプロファイル：アンチウイルス.....	89
8.1	アンチウイルスの設定 .....	90
9	セキュリティプロファイル：Web フィルタ .....	91
9.1	Web フィルタの設定 .....	92
I.	FortiGuard カテゴリベースのフィルタ .....	92
II.	スタティック URL フィルタ（無効な URL をブロック） .....	93
III.	スタティック URL フィルタ（URL フィルタ） .....	94
10	セキュリティプロファイル：アプリケーションコントロール.....	96
10.1	アプリケーションコントロールの設定.....	97
I.	カテゴリ .....	97
II.	アプリケーションとフィルタのオーバーライド .....	98
11	セキュリティプロファイル：IPS（侵入防止）.....	103
12	セキュリティプロファイル：アンチスパム（Eメールフィルタ） .....	104
12.1	Eメールフィルタの設定 .....	104
①	プロトコルごとのスパム検知数 .....	105
②	ローカルスパムフィルタリング .....	105
13	各セキュリティ機能の有効・無効 .....	107
13.1	各セキュリティ機能の有効化 .....	107
13.2	各セキュリティ機能の無効化 .....	108
14	ダッシュボード .....	110
14.1	ウィジェット .....	110
15	FortiView .....	111
15.1	FortiView 送信元.....	111
15.2	FortiView 宛先.....	111
15.3	FortiView アプリケーション .....	111
15.4	FortiViewWeb サイト .....	111
16	ログ&レポート .....	112
16.1	転送トラフィックログ .....	113
16.2	セキュリティイベント .....	114
①	アンチウイルス .....	115
②	Web フィルタ.....	116

③	アプリケーションコントロール .....	117
④	IPS（侵入防止） .....	118
⑤	アンチスパム（Eメールフィルタ） .....	118
16.3	各種ログの取得方法 .....	119
17	リアルタイムレポートの閲覧 .....	120
17.1	グラフフィルタ .....	120
17.2	グラフ .....	121
18	Q&A .....	122

## 1 はじめに

本マニュアルでは「ビジネスインターネット接続」の UTM カスタマコントロールについて、お客さまアカウントにて設定できる項目を解説します。

本マニュアルで使用している IP アドレスは、RFC で定義されている例示用の IP アドレスとなりますので、設定の際はお客さまの環境に応じて指定してください。

お客さまにて閲覧、設定できる一覧は表 1-1. の通りです。

表 1-1. お客さま権限一覧.

内容		閲覧・設定
ダッシュボード	ステータス	閲覧可能
	FortiView	閲覧可能
ポリシー&オブジェクト	ファイアウォールポリシー	設定可能
	アドレス	設定可能
	サービス	設定可能
	バーチャル IP	設定可能
セキュリティプロファイル	アンチウイルス	設定可能
	Web フィルタ	設定可能
	アプリケーションコントロール	設定可能
	IPS (侵入防止)	閲覧可能
	アンチスパム (Eメールフィルタ)	設定可能
ログ&レポート	転送トラフィック	閲覧可能
	システムイベント	閲覧可能
	セキュリティイベント	閲覧可能

※本マニュアルに記載がある推奨設定以外の設定を行うことにより、意図しない動作が発生する可能性もあります。

お客さまにて、設定できない一覧は表 1-2. の通りです。

下記メニューにて、設定を実施された場合の UTM の動作保証は致しかねます。

表 1-2. お客さま設定変更不可一覧.

内容		設定変更
ダッシュボード	ステータス	不可
	セキュリティ	不可
	ネットワーク	不可
	ユーザ&デバイス	不可
セキュリティファブリック		不可
システム		不可
ポリシー&オブジェクト	インターネットサービスデータベース	不可
セキュリティプロファイル	アプリケーションシグネチャ	不可
	IPS シグネチャ	不可
	Web レーティングオーバーライド	不可
	Web プロファイルオーバーライド	不可
ログ&レポート	ローカルトラフィック	不可
	スニファートラフィック	不可
	ログ設定	不可

※各章にて灰色で網掛けされているメニューについても設定変更等された場合、動作保証は致しかねます。

下記箇所を操作すると不具合の原因となりますので行わないでください。

### ■設定不可な機能

カスタマコントロールで設定不可な機能は以下のとおりです。

※赤で網掛けされた箇所を設定変更しないでください。

#### ・ダッシュボード



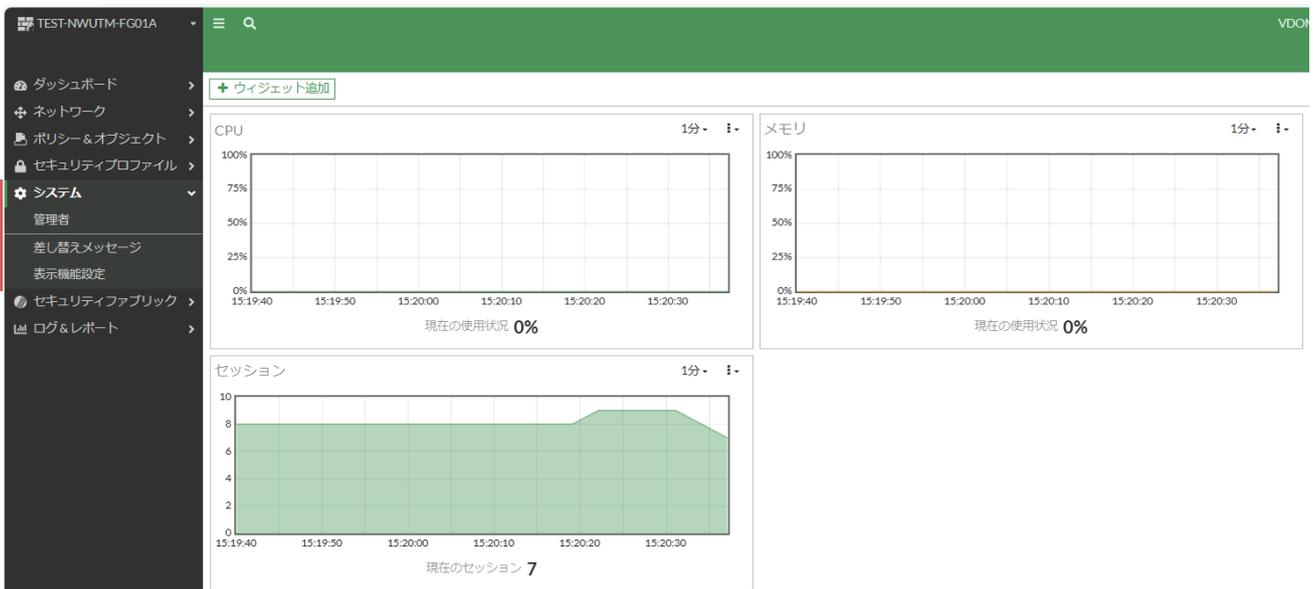
#### ・ポリシー&オブジェクト



## ・セキュリティプロファイル



## ・システム



## ・セキュリティファブリック



## ・ログ&レポート



## 1.1 サービスリニューアル

ビジネスインターネット接続サービスは 2022 年 7 月 22 日にリニューアルしました。本マニュアルはリニューアル後にサービスをご契約いただいたお客さま向けに作成しております。

サービスリニューアル前にご契約いただいたお客さまは一部の設定や表示が異なる場合があります。

## 2 カスタマコントロールサイトへの接続

### 2.1 カスタマコントロールサイトへのログインについて

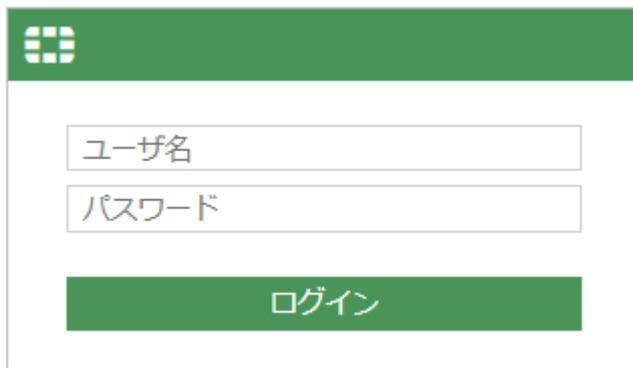
ブラウザから カスタマコントロールの URL にアクセスします。

※IP アドレスは別途、開通通知もしくは、Master' s ONE サービス登録内容のご案内記載の情報をご確認ください。

例 : <https://10.255.28.3>

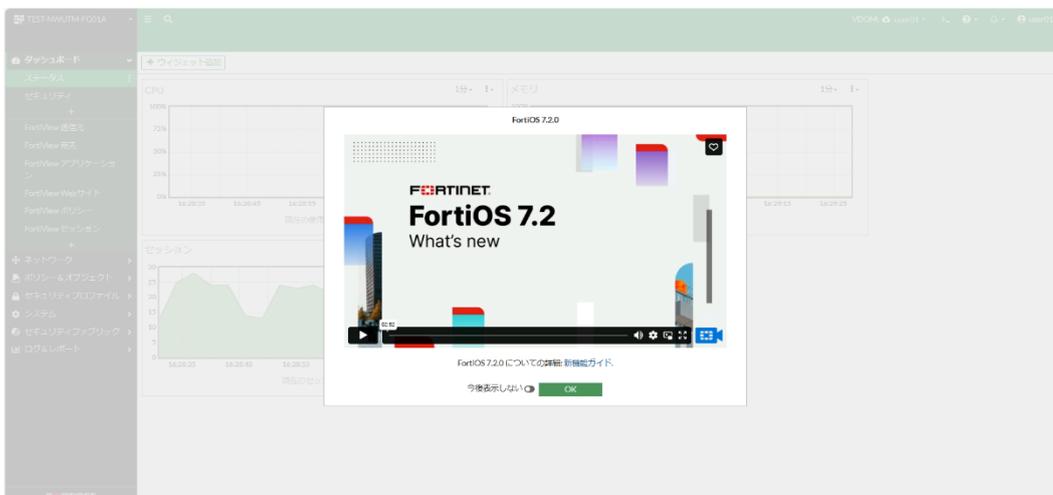
カスタマコントロールサイトのログイン画面が表示されますので、ユーザ名、パスワードを入力し、ログインをクリックします。

※ 初期アクセスにおいて、証明書エラーの画面が表示されますが、サイト自体の問題はございません。また UTM へはお客様 VPN 内と管理セグメントからしかアクセスできません。



### 2.2 初回ログイン時の操作

以下のような画面が表示されるため「今後表示しない」のトグルをオンにし OK を押下します。



以下のような画面表示となっていれば初回ログイン時の操作は完了です。



### 2.3 カスタマコントロールサイトのパスワード変更

ログイン後、カスタマコントロールサイト右上ユーザ名「biu00000」をクリックします。



※実際には「biu00000」ではなく、サービスIDが記載されています。

表示されたプルダウンから「パスワードの変更」をクリックします。



現在のパスワード、新しいパスワードを 2 回入力し、「OK」をクリックします。

パスワードの編集 ×

**△** 現在の管理者アカウントのパスワードを変更すると再ログインが必要になります。

ユーザ名	biu00000
旧パスワード	<input type="password"/>
新しいパスワード	<input type="password"/>
パスワードの再入力	<input type="password"/>

### 3 プリセット設定

ビジネスインターネット接続サービスにてプリセットされたファイアウォールルールやセキュリティ機能の設定概要について記載します。

プリセットのファイアウォールルールを利用することで、様々な通信要件に対して簡易な設定変更により、セキュリティ機能の有効化・無効化を実現することが可能です。

実際の設定方法については、各章をご覧ください。

#### 3.1 ファイアウォールルール

ビジネスインターネット接続サービスでは、予め 8 つのファイアウォールルールがプリセットされています。(サービスリニューアル前に契約したお客さまは 8 つ以上あります。)

- ① NTPC モニタルール (NTPC Monitor Rule) (サービスリニューアル後に契約したお客さまのみ)
- ② 送信元ブラックルール (Src Black Rule)
- ③ 宛先ブラックルール (Dst Black Rule)
- ④ 送信元ホワイトルール (Src White Rule)
- ⑤ 宛先ホワイトルール (Dst White Rule)
- ⑥ ALL\_ICMP
- ⑦ WindowsUpdate Bandwidth Control (サービスリニューアル前に契約した一部のお客さまのみ)
- ⑧ LAN→WAN (サービスリニューアル後に契約したお客さまのみ)
- ⑨ webfilter-policy\* (サービスリニューアル前に契約したお客さまのみ)
- ⑩ user-defined-policy\* (サービスリニューアル前に契約したお客さまのみ)
- ⑪ 暗黙の拒否

名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト	タイプ
LAN (port12.vlan101) → WAN (vlan2001.emv1)										
NTPC Monitor Rule	100.88.18.0/29	all	always	ALL	許可	@ 160.248.241.1/32	no-Inspection	無効化済み	0 B	スタンダード
Src Black Rule	Src Black list	all	always	ALL	拒否			すべて	0 B	スタンダード
Dst Black Rule	all	Dst Black list	always	ALL	拒否			すべて	0 B	スタンダード
Src White Rule	Src White list	all	always	ALL	許可	@ 160.248.241.1/32	no-Inspection	すべて	0 B	スタンダード
Dst White Rule	all	Dst White list	always	ALL	許可	@ 160.248.241.1/32	no-Inspection	すべて	117.90 kB	スタンダード
ALL_ICMP	all	all	always	ALL_ICMP	許可	@ 160.248.241.1/32	no-Inspection	すべて	0 B	スタンダード
LAN → WAN	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	@ 160.248.241.1/32	AV default WEB default APP default certificate-Inspection	すべて	13.64 MB	スタンダード
暗黙の拒否										
暗黙の拒否	all	all	always	ALL	拒否			無効化済み	104 B	

図 3-1. プリセットのファイアウォールポリシー。

ルールは、記載順に処理され、通信要件に合致するルールにて通信が制御されます。

プリセットされたファイアウォールルールのパラメータの追加・変更にて運用して頂くことを推奨します。

上記の⑧「LAN→WAN」ルール ⑨「webfilter-policy-\*」ルール ⑩「user-defined-policy\*」においては、インターネット向けの通信に対して、お客様自身で、きめ細かくセキュリティ機能を適用することが可能です。

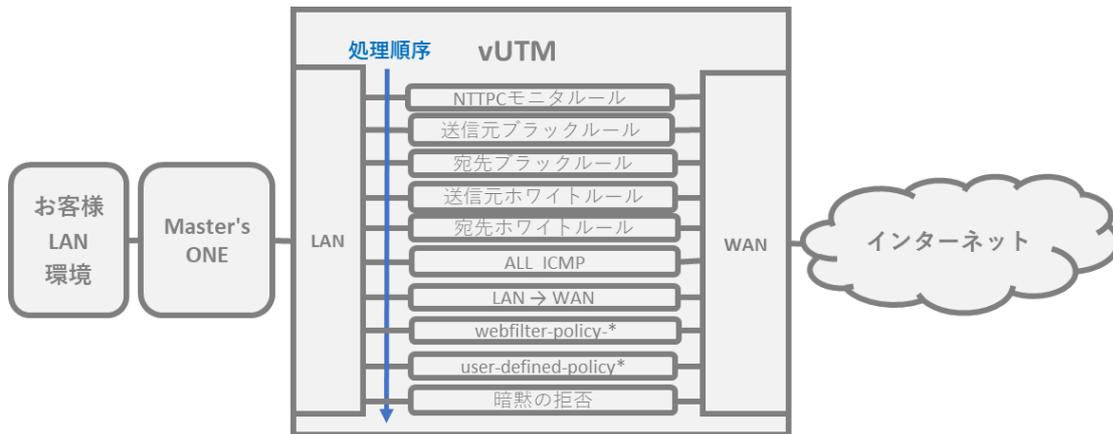


図 3-2. プリセットのファイアウォールポリシー概要図.

表 3-1. プリセットのファイアウォールルール一覧.

	ポリシー名	用途	デフォルト設定
①	NTTPC モニタールール	<ul style="list-style-type: none"> <li>- UTMの死活監視や様々な通信が正常にできるか確認するためのルールになります。</li> <li>※このルールについては、削除や設定の変更を絶対にしないでください。</li> </ul>	有効
②	送信元ブラックルール	<ul style="list-style-type: none"> <li>- アドレスグループ (Src Black list) に送信元 IP アドレスを追加することにより、当該通信を拒否することが可能です。</li> <li>- 初期設定時、Src Black list は、空の状態を提供致します。</li> <li>- 業務上どこにも通信させたくないクライアント端末等を Src Black list に適用することで、対象の通信を拒否することが可能です。</li> </ul>	有効
③	宛先ブラックルール	<ul style="list-style-type: none"> <li>- アドレスグループ (Dst Black list) に宛先 IP アドレスを追加することにより、当該通信を拒否することが可能です。</li> <li>- 初期設定時、Dst Black list は、空の状態を提供致します。</li> <li>- 業務上接続させたくないWEBサイト等を Dst Black list に適用することで、対象の通信を拒否することが可能です。</li> </ul>	有効
④	送信元ホワイトルール	<ul style="list-style-type: none"> <li>- アドレスグループ (Src White list) に送信元 IP アドレスを追加することにより、当該通信の全セキュリティ機能を無効化することが可能です。</li> <li>- 初期設定時、Src White list は、空の状態を提供致します。</li> <li>- セキュリティを無効にしたいお客様端末の IP アドレスを Src White list に適用することで、セキュリティ機能を無効化することが可能です。</li> </ul>	有効
⑤	宛先ホワイトルール	<ul style="list-style-type: none"> <li>- アドレスグループ (Dst White list) に宛先 IP アドレスを追加することにより、当該通信の全セキュリティ機能を無効化することが可能です。</li> <li>- 初期設定時、Dst White list は、空の状態を提供致します。</li> <li>- 信頼のある宛先 IP アドレスを Dst White list に適用することで、セキュリティ機能を無効化することが可能です。</li> </ul>	有効
⑥	ALL_ICMP	<ul style="list-style-type: none"> <li>- サーバ、ネットワーク機器、業務端末などの間で通信が正常にできているか死活監視をするルールになります。</li> <li>※このルールについては、削除や設定の変更を絶対にしないでください。</li> </ul>	有効
⑦	WindowsUpdate Bandwidth Control	<ul style="list-style-type: none"> <li>- サービスで定める特定アプリケーションの通信を制御するためのルールになります。</li> <li>※このルールについては、削除や設定の変更を絶対にしないでください。</li> </ul>	有効
⑧	LAN→WAN	<ul style="list-style-type: none"> <li>- 基本となるファイアウォールルールとなります。</li> <li>- VPN 内のプライベートアドレス (10.0.0.0/8、172.16.0.0/12、192.168.0.0/16) を送信元 IP アドレスとして、全てのインターネット接続の通信を対象にセキュリティ機能を適用します。</li> <li>※webfilter-policy-*をご利用のお客様につきましては送信元のプライベートアドレスが異なりますのでご注意ください。</li> </ul>	有効
⑨	webfilter-policy-*	<ul style="list-style-type: none"> <li>- 基本となるファイアウォールルールとなります。</li> <li>- VPN 内のプライベートアドレス (お客様ごとに異なる) を送信元 IP アドレスとして、全てのインターネット接続の通信を対象にセキュリティ機能を適用します。</li> <li>- サービスリニューアル前 UTM のルールを引き継いだルールになります。</li> </ul>	有効
⑩	user-defined-policy*	<ul style="list-style-type: none"> <li>- サービスリニューアル前 UTM のファイアウォールルールを引き継いだルールになります。</li> </ul>	有効
⑪	暗黙の拒否	上記①～⑩に合致しない通信を明示的に拒否します。	有効

各ファイアウォールルールの設定項目に関しては以下の通りとなります。

※灰色の網掛け部分に関しては変更出来ないパラメータとなります。

### 3.2 ファイアウォールポリシー設定項目

プリセットされているファイアウォールポリシーの各項目の概要、設定方法は以下の通りです。

名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト	タイプ
NTT PC Monitor Rule → WAN (vlan2001.emv1)										
NTT PC Monitor Rule	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	no-inspection	無効化済み	0 B	スタンダード
Src Black Rule	Src Black list	all	always	ALL	拒否			すべて	0 B	スタンダード
Dst Black Rule	all	Dst Black list	always	ALL	拒否			すべて	0 B	スタンダード
Src White Rule	Src White list	all	always	ALL	許可	160.248.241.1/32	no-inspection	すべて	0 B	スタンダード
Dst White Rule	all	Dst White list	always	ALL	許可	160.248.241.1/32	no-inspection	すべて	117.90 kB	スタンダード
ALL_ICMP	all	all	always	ALL_ICMP	許可	160.248.241.1/32	no-inspection	すべて	0 B	スタンダード
<b>A)</b>	<b>D)</b> 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	<b>E)</b>	<b>F)</b>	<b>G)</b>	<b>H)</b>	<b>I)</b>	<b>J)</b> AV default WEB default APP default SSL certificate-inspection	<b>K)</b>	<b>L)</b> 15.29 MB	<b>M)</b>
暗黙の拒否										
暗黙の拒否	any	any	always	ALL	拒否			有効化済み	104 B	

図 3-2. インターフェースペアビューのファイアウォールポリシー。

名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト	タイプ
NTT PC Monitor Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	no-inspection	無効化済み	0 B	スタンダード
Src Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src Black list	all	always	ALL	拒否			すべて	0 B	スタンダード
Dst Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Dst Black list	all	always	ALL	拒否			すべて	0 B	スタンダード
Src White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src White list	all	always	ALL	許可	160.248.241.1/32	no-inspection	すべて	0 B	スタンダード
Dst White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Dst White list	all	always	ALL	許可	160.248.241.1/32	no-inspection	すべて	117.90 kB	スタンダード
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/32	no-inspection	すべて	0 B	スタンダード
<b>A)</b>	<b>B)</b>	<b>C)</b>	<b>D)</b> 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	<b>E)</b>	<b>F)</b>	<b>G)</b>	<b>H)</b>	<b>I)</b>	<b>J)</b> AV default WEB default APP default SSL certificate-inspection	<b>K)</b>	<b>L)</b> 15.29 MB	<b>M)</b>
暗黙の拒否												
暗黙の拒否	any	any	all	all	always	ALL	拒否			有効化済み	104 B	

図 3-3. シーケンス別のファイアウォールポリシー。

- A) 各ポリシーの名前が記載されています。
- B) 送信元インターフェースが設定されています。
- C) 宛先インターフェースが設定されています。
- D) 送信元 IP またはアドレスグループが設定されています。
- E) 宛先 IP またはアドレスグループが設定されています。
- F) ポリシーの適用期間が設定されています。 **※サービス仕様外の為変更しないでください。**
- G) 使用するプロトコルが設定されています。
- H) 対象の送信元または宛先への通信を許可するのか拒否するのかが設定されています。
- I) インターネット接続する際のグローバル IP が設定されています。(DNAT 使用時は空白です。)
- J) 対象の送信元または宛先への通信に対してチェックするセキュリティを設定できます。
- K) ログを取得するか否かが設定されています。
- L) 対象のポリシーに合致した通信量が表示されています。
- M) ポリシーのタイプがスタンダードで設定されています。 **※サービス仕様外の為変更しないでください。**

対象のポリシーの A) ~K) の変更したい箇所にカーソルを合わせると鉛筆マークが表示されます。その鉛筆マークをクリックすることによって簡単に名前や設定を変更することが可能となります。



変更後適用を押下すると反映されます。



J)については、鉛筆マークをクリックすると右側に各プロファイルが表示されますので、対象のプロファイルの右側にある鉛筆マークもしくは編集をクリックすることにより設定変更が可能となります。



表 3-2. ファイアウォールルールの設定項目.

	設定項目	設定内容	参考項目	
1	名前	任意：ポリシー名を記載		
2	タイプ	スタンダード		
3	着信インターフェース	LAN (portB. vlan101) ※他インターフェースでは動作保証不可		
4	発信インターフェース	WAN (vlan3101. emv1) ※他インターフェースでは動作保証不可		
5	送信元	任意 IP アドレス：予め設定されているファイアウォールアドレスもしくはファイアウォールアドレスグループを指定する	5章：ファイアウォールアドレス 6章：ファイアウォールアドレスグループ	
6	IP/MAC ベースアクセスコントロール	ZTNA タグを使用して、デバイスの MAC/IP アドレスに基づいたアクセスを許可する		
7	宛先	任意 IP アドレス：予め設定されているファイアウォールアドレスもしくはファイアウォールアドレスグループを指定する	5章：ファイアウォールアドレス 6章：ファイアウォールアドレスグループ	
8	スケジュール	always		
9	サービス	任意：制御対象のプロトコルタイプ (UDP, TCP) 及び宛先ポート番号を指定	7章：ファイアウォールサービス	
10	アクション	ACCEPT/DENY：当該通信の許容/拒否を指定		
11	インスペクションモード	固定：プロキシベース		
12	NAT	固定：有効		
13	IP プール設定	ダイナミック IP プールを使う		
14	送信元ポートの保持	無効		
15	プロトコルオプション	固定：g-default		
16	セキュリティ プロファイル	- アンチウイルス	有効/無効	9章：アンチウイルス
		- WEB フィルタ	有効/無効	12章：WEB フィルタ
		- アプリケーションコントロール	有効/無効	13章：アプリケーションコントロール
		- IPS (侵入防止)	有効/無効	11章：IPS (侵入防止)
		- アンチスパム (Eメールフィルタ)	有効/無効	10章：Eメールフィルタ
		- SSL インスペクション*	有効/無効	
17	ロギングオプション	- 許可トラフィックをログ	すべてのセッション	
		- セッション開始時にログを生成	無効	
		- パケットをキャプチャ	無効	
18	コメント	任意		
19	有効化設定	ファイアウォールポリシーの有効化/無効化を指定	8章：ファイアウォールポリシーの有効化	

※ SSL インスペクション：有効化の際は「certificate-inspection」もしくは「certificate-inspection2」を利用。「certificate-inspection2」の場合、SSL 証明書の検査ができなかったとき、エラーと判定しなくなります。

※着信、発信インターフェース：機器によってカッコ内の数字が異なります。

プリセットされているファイアウォールルールの設定内容は以下の通り。

※ 灰色の網掛け部分に関しては変更出来ないパラメータとなります

※ 水色の網掛け部分に関しては変更しないことを推奨としております。  
変更することで予期しない動作を起こす可能性があります。

表 3-2. ファイアウォールルールの設定項目 (1/3).

設定項目	①NTTPC モニタルール	②送信元ブラックルール	③宛先ブラックルール
1 名前	NTTPC Monitor Rule	Src Black Rule	Dst Black Rule
2 タイプ	スタンダード	スタンダード	スタンダード
3 着信インターフェース	LAN(portB.vlan101)	LAN(portB.vlan101)	LAN(portB.vlan101)
4 発信インターフェース	WAN(vlan3101.emv1)	WAN(vlan3101.emv1)	WAN(vlan3101.emv1)
5 送信元 IP アドレス	100.88.18.0/29	Src Black list*	all
6 IP/MAC ベースアクセスコントロール	なし	なし	なし
7 宛先 IP アドレス	all	all	Dst Black list*
8 スケジュール	always	always	always
9 サービス	ALL	ALL	ALL
10 アクション	ACCEPT	DENY	DENY
11 インспекションモード	フローベース	フローベース	フローベース
12 NAT	有効	有効	有効
13 IP プール設定	ダイナミック IP プール	ダイナミック IP プール	ダイナミック IP プール
14 送信元ポートの保持	無効	無効	無効
15 プロトコルオプション	g-default	g-default	g-default
16 セキュリティプロファイル	アンチウイルス：無効	アンチウイルス：無効	アンチウイルス：無効
	WEB フィルタ：無効	WEB フィルタ：無効	WEB フィルタ：無効
	アプリケーションコントロール：無効	アプリケーションコントロール：無効	アプリケーションコントロール：無効
	IPS(侵入防止)：無効	IPS(侵入防止)：無効	IPS(侵入防止)：無効
	Eメールフィルタ：無効	Eメールフィルタ：無効	Eメールフィルタ：無効
	SSL インспекション：無効	SSL インспекション：無効	SSL インспекション：無効
17 ログイングオプション	許可トラフィックをログ：すべてのセッション		
	セッション開始時にログを生成：無効		
18 コメント	NTTPC 監視用(削除厳禁)	なし	なし
19 有効化設定	有効	有効	有効

※ 初期設定時は、未定義のリストを提供

表 3-2. ファイアウォールルールの設定項目 (2/3).

	設定項目	④送信元ホワイトルール	⑤宛先ホワイトルール	⑥ALL_ICMP
1	名前	Src White Rule	Dst white Rule	ALL_ICMP
2	タイプ	スタンダード	スタンダード	スタンダード
3	着信インターフェース	LAN(portB. vlan101)	LAN(portB. vlan101)	LAN(portB. vlan101)
4	発信インターフェース	WAN(vlan3101. emv1)	WAN(vlan3101. emv1)	WAN(vlan3101. emv1)
5	送信元 IP アドレス	Src white list*	all	10. 0. 0. 0/8 172. 16. 0. 0/12 192. 168. 0. 0/16
6	IP/MAC ベースアクセスコントロール	なし	なし	なし
7	宛先 IP アドレス	all	Dst White list*	all
8	スケジュール	always	always	always
9	サービス	ALL	ALL	ALL_ICMP
10	アクション	ACCEPT	ACCEPT	ACCEPT
11	インスペクションモード	フローベース	フローベース	フローベース
12	NAT	有効	有効	有効
13	IP プール設定	ダイナミック IP プール	ダイナミック IP プール	ダイナミック IP プール
14	送信元ポートの保持	無効	無効	無効
15	プロトコルオプション	g-default	g-default	g-default
16	セキュリティプロファイル	アンチウイルス：無効	アンチウイルス：無効	アンチウイルス：無効
		WEB フィルタ：無効	WEB フィルタ：無効	WEB フィルタ：無効
		アプリケーションコントロール：無効	アプリケーションコントロール：無効	アプリケーションコントロール：無効
		IPS(侵入防止)：無効	IPS(侵入防止)：無効	IPS(侵入防止)：無効
		Eメールフィルタ：無効	Eメールフィルタ：無効	Eメールフィルタ：無効
		SSL インスペクション：無効	SSL インスペクション：無効	SSL インスペクション：無効
17	ロギングオプション	許可トラフィックをログ：すべてのセッション	許可トラフィックをログ：すべてのセッション	許可トラフィックをログ：すべてのセッション
		セッション開始時にログを生成：無効	セッション開始時にログを生成：無効	セッション開始時にログを生成：無効
18	コメント	なし	なし	なし
19	有効化設定	有効	有効	有効

※ 初期設定時は、未定義のリストを提供

表 3-2. ファイアウォールルールの設定項目 (3/3).

	設定項 6	⑦LAN → WAN	⑧webfilter-policy*	⑨user-defined-policy*	⑩暗黙の拒否
1	名前	LAN → WAN	webfilter-policy*	user-defined-policy	暗黙の拒否
2	タイプ	スタンダード	スタンダード	スタンダード	
3	着信インターフェース	LAN(portB.vlan101)	any	any	any
4	発信インターフェース	WAN(vlan3101.emv1)	any	any	any
5	送信元 IP アドレス	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	サービスリニューアル前 UTM の設定に基づく	サービスリニューアル前 UTM の設定に基づく	all
6	IP/MAC ベースアクセスコントロール	なし	なし	なし	
7	宛先 IP アドレス	all	all	サービスリニューアル前 UTM の設定に基づく	any
8	スケジュール	always	always	always	always
9	サービス	ALL	サービスリニューアル前 UTM の設定に基づく	サービスリニューアル前 UTM の設定に基づく	
10	アクション	ACCEPT	ACCEPT	サービスリニューアル前 UTM の設定に基づく	DENY
11	インスペクションモード	プロキシベース	プロキシベース	プロキシベース	
12	NAT	有効	有効	有効	
13	IP プール設定	ダイナミック IP プール	ダイナミック IP プール	ダイナミック IP プール	
14	送信元ポートの保持	無効	無効	無効	
15	プロトコルオプション	g-default	g-default	g-default	
16	セキュリティプロファイル	アンチウイルス：有効	アンチウイルス：サービスリニューアル前 UTM の設定に基づく	アンチウイルス：無効	
		WEB フィルタ：有効	WEB フィルタ：有効	WEB フィルタ：無効	
		アプリケーションコントロール：有効	アプリケーションコントロール：有効	アプリケーションコントロール：有効	
		IPS(侵入防止)：無効	IPS(侵入防止)：無効	IPS(侵入防止)：無効	
		Eメールフィルタ：無効	Eメールフィルタ：無効	Eメールフィルタ：無効	
		SSL インスペクション：無効	SSL インスペクション：無効	SSL インスペクション：無効	
17	ロギングオプション	許可トラフィックをログ：すべてのセッション	許可トラフィックをログ：すべてのセッション	許可トラフィックをログ：すべてのセッション	
		セッション開始時にログを生成：無効	セッション開始時にログを生成：無効	セッション開始時にログを生成：無効	
18	コメント	なし	なし	なし	
19	有効化設定	有効	有効	有効	有効

### 3.3 セキュリティ機能

ファイアウォールルール「⑧LAN→WAN」のセキュリティ機能においては、一般的なOA端末がインターネットでの通信を実施する際のセキュリティ脅威を検知・ブロック可能とするようにデフォルト設定されています。

各セキュリティ機能における設定概要は以下の通りです。

※灰色の網掛け部分に関しては設定変更をしないでください。

設定変更された場合動作保証は致しかねます。

表 3-3. セキュリティ機能概要(1/3).

設定項目	設定内容	デフォルト設定	
1 アンチウイルス	アンチウイルススキャン	ブロック	
	機能セット	プロキシベース	
	インスペクションされるプロトコル	HTTP	有効
		SMTP	無効
		POP3	無効
		IMAP	無効
		FTP	無効
		CIFS	無効
		MAPI	無効
		SSH	無効
	ATP プロテクションオプション	コンテンツ無害化	無効
		Windows 実行ファイルをウイルスと扱う	無効
		モバイルマルウェアプロテクションを含む	有効
	ウイルスアウトブレイク防止	FortiGuard アウトブレイク防止データベースを使用	無効 <sup>‡</sup>
		外部マルウェアブロックリストを使用	無効 <sup>‡</sup>

表 3-3. セキュリティ機能概要 (2/3).

設定項目	設定内容	デフォルト設定			
2 WEB フィルタ	機能セット	プロキシベース			
	FortiGuard カテゴリベースのフィルタ設定	項目	カテゴリ		
		ローカルカテゴリ：無効	custom1	Custom2	
		違法性の高いサイト：ブロック	薬物乱用	ハッキング	違法または非倫理的
			差別	明示的な暴力	盗作
			児童虐待		
		アダルト/成人コンテンツ：ブロック	その他のアダルトマテリアル	ギャンブル	ヌードとワイセツ
			ポルノ	出会い系	マリファナ
		セキュリティリスクの高いサイト：ブロック	悪意のある Web サイト	フィッシング詐欺	スパム URL
		未評価：モニタ	未評価		
		上記以外のサブカテゴリ：モニタ			
	カテゴリ使用クォータ				
	ユーザにブロックされたカテゴリのオーバーライドを許可する				
	スタティック URL フィルタ	無効な URL をブロック：無効			
		URL フィルタ：無効			
		FortiSandbox により検知された悪意のある URL をブロック：無効			
		コンテンツフィルタ：無効			
	レーティングオプション	レーティングエラー発生時に Web サイトを許可：無効			
		ドメインまたは IP アドレスで URL をレーティング：無効			
		HTTP POST アクション：許可			
Cookie を削除：無効					

表 3-3. セキュリティ機能概要 (3/3).

設定項目	設定内容	デフォルト設定
3 アプリケーションコントロール	カテゴリ	すべてモニタ
	ネットワークプロトコルの強制	
	アプリケーションとフィルタのオーバーライド	なし
	オプション	デフォルト以外のポートで検知されたアプリケーションをブロック：無効 DNS トラフィックの許可とログ：有効 HTTP ベースアプリケーションの差し替えメッセージ：無効
4 IPS (侵入防止)	悪意のある URL をブロック	有効
	IPS シグネチャとフィルタ	タイプ：フィルタ
		アクション：デフォルト
		パケットロギング：無効
		ステータス：デフォルト
	フィルタ：重大度 5 以上	
ボットネット C&C	ボットネットサイトへの発信接続をスキャン：ブロック	
5 アンチスパム (E メールフィルタ)	機能セット	プロキシベース
	スパム検知とフィルタリングを有効化	有効
	プロトコルごとのスパム検知数	IMAP：スパムアクション：タグ、タグ挿入箇所：サブジェクト、タグ形式：[Spam]
		POP3：スパムアクション：タグ、タグ挿入箇所：サブジェクト、タグ形式：[Spam]
		SMTP：スパムアクション：タグ、タグ挿入箇所：サブジェクト、タグ形式：[Spam]
	FortiGuard スパムフィルタリング	IP アドレスチェック：有効
		URL チェック：有効
		E メール内のフィッシング URL を検知：有効
		E メールチェックサムをチェック：有効
	ローカルスパムフィルタリング	スパム報告：有効
HELO DNS ルックアップ：無効		
リターン E メール DNS チェック：無効		
	ブラック/許可リスト：有効	

#### 4 ファイアウォールルールの設定方法

本章では、ファイアウォールルール、NAT の設定方法について解説しています。

ファイアウォールポリシーでは、インターフェースペアビューとシーケンス別の 2 種類の表示方法がありますのでファイアウォールポリシーのメニューを押下後、画面上部の表記を確認してから設定方法をご確認ください。

インターフェースペアビュー シーケンス別

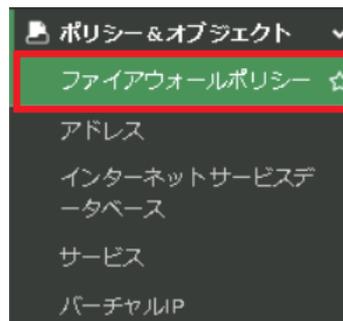
また、表示形式は変更されても構いませんが下記のようにインターフェースペアビューがグレーアウトされて表示切替ができない場合もございます。

インターフェースペアビュー シーケンス別

##### 4.1 ファイアウォールルールの追加（表示形式:インターフェースペアビューの場合）

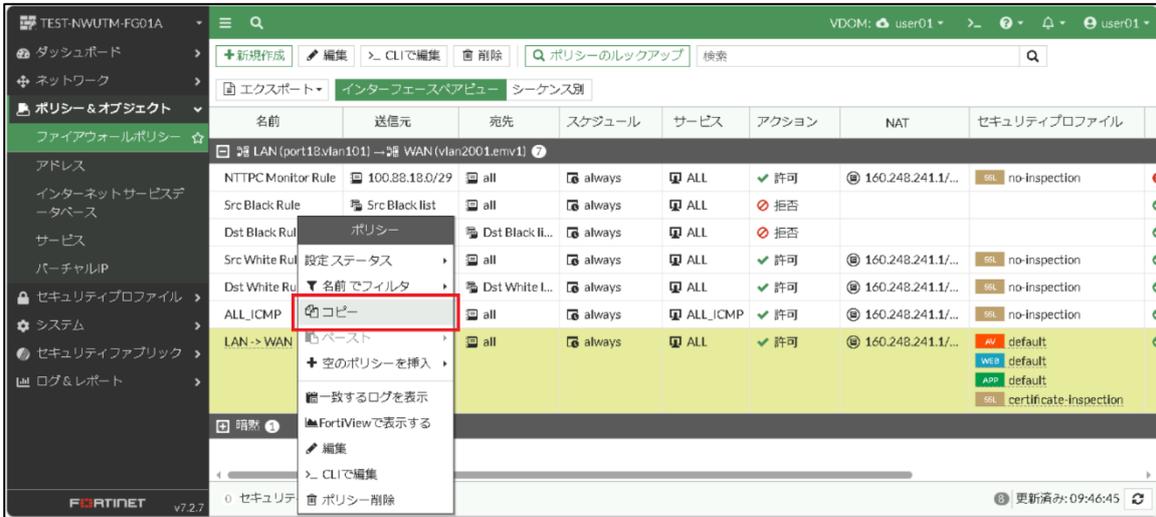
- ① 左のメニューからポリシー&オブジェクト->ファイアウォールポリシーを選択する。

※ルールの表示がされていない場合は+ボタンを押下して表示させてください。



名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト	タイプ
 LAN (port18.vlan101) → WAN (vlan2001.emv1) 										
  										

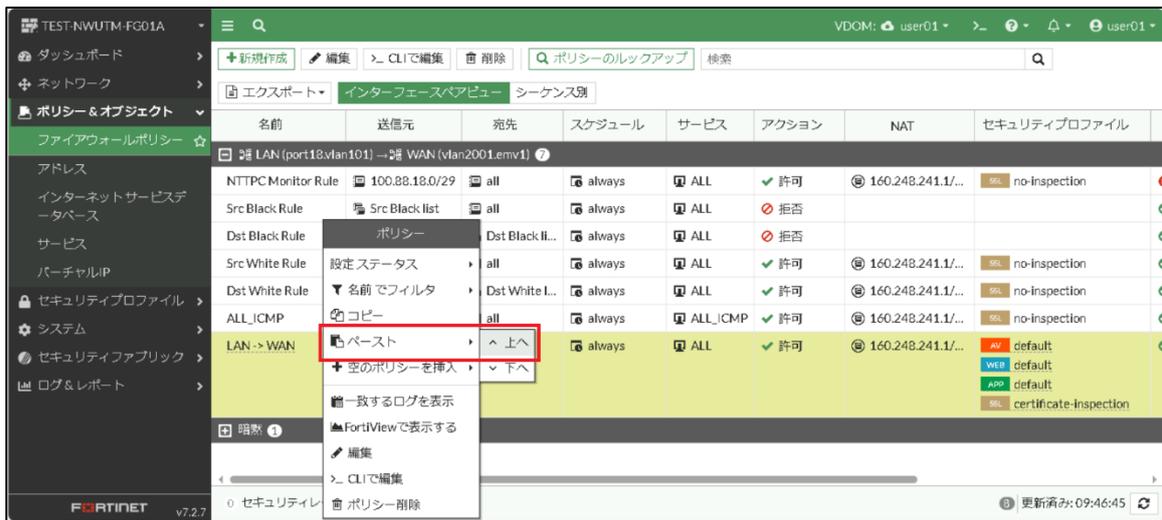
② LAN→WAN 又は、webfilter-policy-\*を右クリックし、コピーを押下する。



The screenshot shows the Fortinet FortiGate GUI. The left sidebar is expanded to 'Policy & Objects'. The main area displays a table of policies. The 'LAN->WAN' policy is selected, and a context menu is open over it. The 'Copy' option is highlighted in red.

名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル
NTTPC Monitor Rule	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/...	no-inspection
Src Black Rule	Src Black list	all	always	ALL	拒否		
Dst Black Rule	Dst Black list	all	always	ALL	拒否		
Src White Rule	Src White list	all	always	ALL	許可	160.248.241.1/...	no-inspection
Dst White Rule	Dst White list	all	always	ALL	許可	160.248.241.1/...	no-inspection
ALL_ICMP	all	all	always	ALL_ICMP	許可	160.248.241.1/...	no-inspection
LAN->WAN	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/...	AV default WEB default APP default SSL certificate-inspection

③ 再度 LAN→WAN 又は、webfilter-policy-\*を右クリックし、ペースト→上へを押下する。



The screenshot shows the Fortinet FortiGate GUI. The left sidebar is expanded to 'Policy & Objects'. The main area displays a table of policies. The 'LAN->WAN' policy is selected, and a context menu is open over it. The 'Paste Up' option is highlighted in red.

名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル
NTTPC Monitor Rule	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/...	no-inspection
Src Black Rule	Src Black list	all	always	ALL	拒否		
Dst Black Rule	Dst Black list	all	always	ALL	拒否		
Src White Rule	Src White list	all	always	ALL	許可	160.248.241.1/...	no-inspection
Dst White Rule	Dst White list	all	always	ALL	許可	160.248.241.1/...	no-inspection
ALL_ICMP	all	all	always	ALL_ICMP	許可	160.248.241.1/...	no-inspection
LAN->WAN	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/...	AV default WEB default APP default SSL certificate-inspection

④ 作成したポリシーをダブルクリックする。



The screenshot shows the Fortinet FortiGate GUI. The left sidebar is expanded to 'Policy & Objects'. The main area displays a table of policies. The 'LAN->WAN' policy is highlighted with a red box.

名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル
NTTPC Monitor Rule	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	no-inspection
Src Black Rule	Src Black list	all	always	ALL	拒否		
Dst Black Rule	Dst Black list	all	always	ALL	拒否		
Src White Rule	Src White list	all	always	ALL	許可	160.248.241.1/32	no-inspection
Dst White Rule	Dst White list	all	always	ALL	許可	160.248.241.1/32	no-inspection
ALL_ICMP	all	all	always	ALL_ICMP	許可	160.248.241.1/32	no-inspection
LAN->WAN	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection

- ⑤ 名前、送信元、宛先、サービス、セキュリティプロファイルを設定し OK を押下する。  
 ※コメントにコピー元の名前が入るので消すか任意のコメントを記入してください。  
 ※セキュリティプロファイルで使用する良いプロファイルは表 4.1 を参照

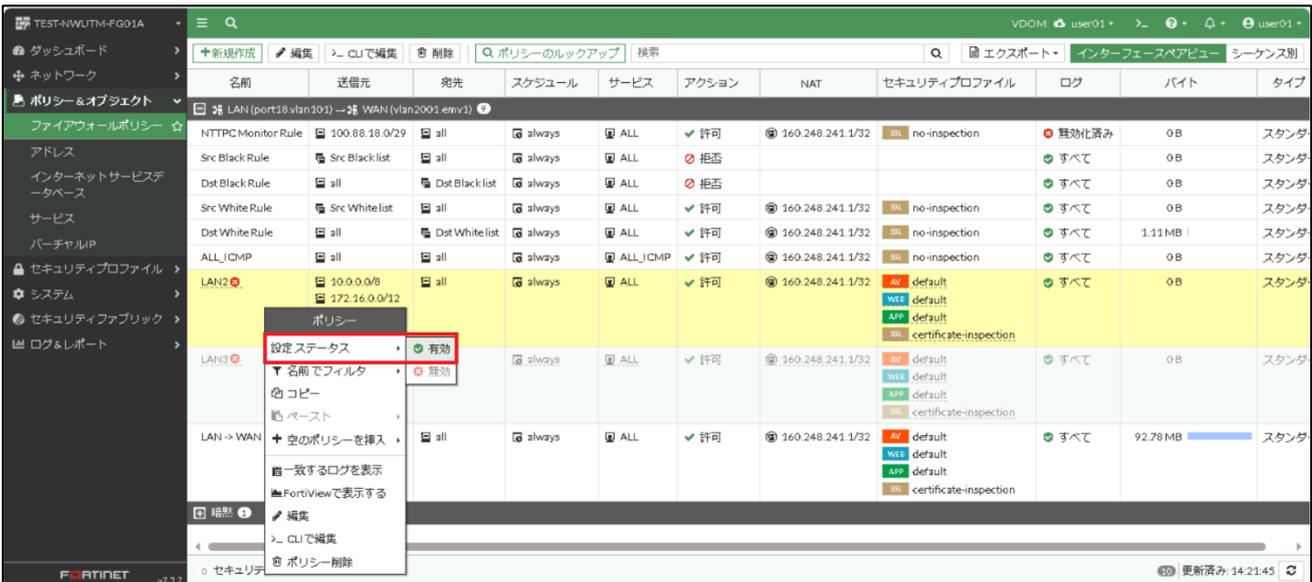
「+」を押下すると右側にリストが表示されるので追加したい分をクリックする。  
 消すアドレスがある場合は「x」をクリックすると消えます。  
 送信元、宛先で追加したいものがない場合は 5.1 項を参照  
 サービスで追加したいものがない場合は 7.1 項を参照

セキュリティ機能を有効化したい場合は各セキュリティ機能のトグルをクリックしてください。  
 使用しないセキュリティ機能はトグルをクリックし無効化にしてください。  
 詳細は 13 章を参照

- ⑥ 作成したルールを ALL\_ICMP より下の投入したい場所に名前部分でドラッグ&ドロップし移動させる。

名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト	タイプ
NTTPC Monitor Rule	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	無効化済み	0B	スタンダ
Src Black Rule	Src Black list	all	always	ALL	拒否			すべて	0B	スタンダ
Dst Black Rule	all	Dst Black list	always	ALL	拒否			すべて	0B	スタンダ
Src White Rule	Src Whitelist	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	0B	スタンダ
Dst White Rule	all	Dst Whitelist	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	1.11 MB	スタンダ
ALL_ICMP	all	all	always	ALL_ICMP	許可	160.248.241.1/32	SSL no-inspection	すべて	0B	スタンダ
LAN3	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて	0B	スタンダ
LAN2	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて	0B	スタンダ
LAN->WAN	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて	92.35 MB	スタンダ

- ⑦ 対象のルールを右クリックし設定ステータス→有効を押下する。



名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト	タイプ
NTTPC Monitor Rule	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	無効化済み	0B	スタンダ
Src Black Rule	Src Black list	all	always	ALL	拒否			すべて	0B	スタンダ
Dst Black Rule	all	Dst Black list	always	ALL	拒否			すべて	0B	スタンダ
Src White Rule	Src Whitelist	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	0B	スタンダ
Dst White Rule	all	Dst Whitelist	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	1.11 MB	スタンダ
ALL_ICMP	all	all	always	ALL_ICMP	許可	160.248.241.1/32	SSL no-inspection	すべて	0B	スタンダ
LAN2	10.0.0.0/8 172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて	0B	スタンダ
LAN3	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて	0B	スタンダ
LAN->WAN	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて	92.78 MB	スタンダ

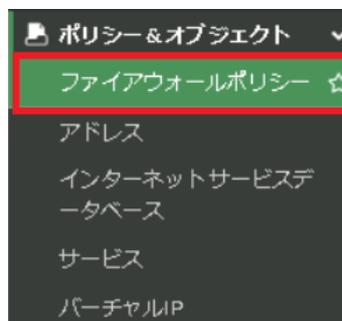
⑧ ルールが有効になったことを確認する。

名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト	タイプ
NTTPC Monitor Rule	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	no-inspection	無効化済み	0B	スタング
Src Black Rule	all	all	always	ALL	拒否			すべて	0B	スタング
Dst Black Rule	all	all	always	ALL	拒否			すべて	0B	スタング
Src White Rule	all	all	always	ALL	許可	160.248.241.1/32	no-inspection	すべて	0B	スタング
Dst White Rule	all	all	always	ALL	許可	160.248.241.1/32	no-inspection	すべて	1.11 MB	スタング
ALL_ICMP	all	all	always	ALL_ICMP	許可	160.248.241.1/32	no-inspection	すべて	0B	スタング
LAN2	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	default default default certificate-inspection	すべて	0B	スタング
LAN3	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	default default default certificate-inspection	すべて	0B	スタング
LAN->WAN	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	default default default certificate-inspection	すべて	92.78 MB	スタング

×が消えていれば有効化されている

4.2 ファイアウォールルールの追加（表示形式：シーケンス別の場合）

① 左のメニューからポリシー&オブジェクト->ファイアウォールポリシーを選択する。

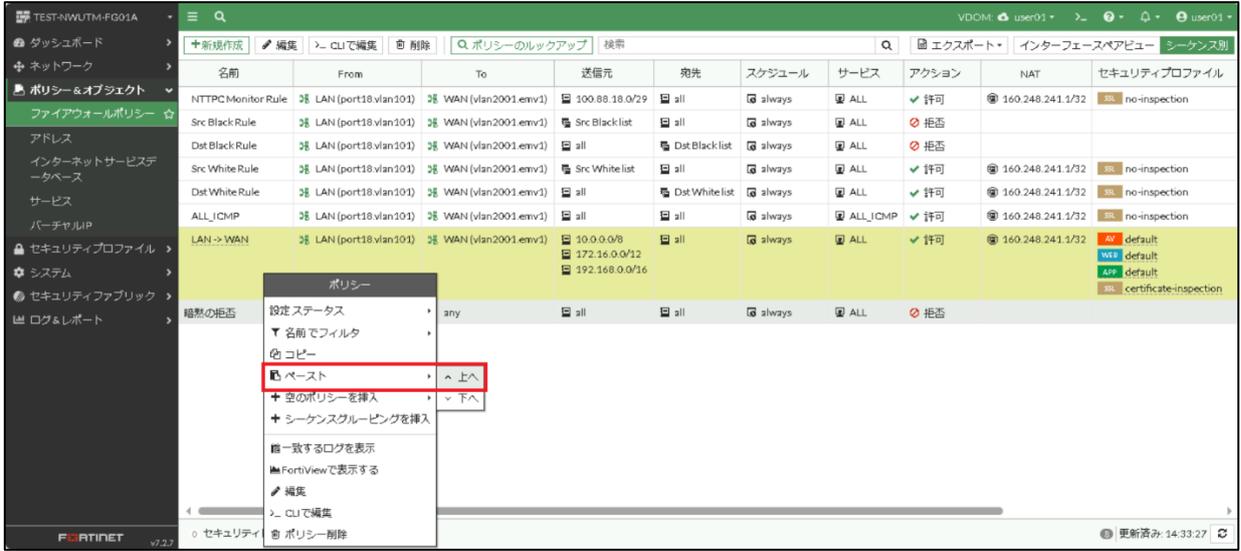


② LAN->WAN 又は、webfilter-policy-\*を右クリックし、コピーを押下する。

名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル
NTTPC Monitor Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	no-inspection
Src Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src Blacklist	all	always	ALL	拒否		
Dst Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Dst Blacklist	all	always	ALL	拒否		
Src White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src Whitelist	all	always	ALL	許可	160.248.241.1/32	no-inspection
Dst White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Dst Whitelist	all	always	ALL	許可	160.248.241.1/32	no-inspection
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/32	no-inspection
LAN->WAN	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	default default default certificate-inspection

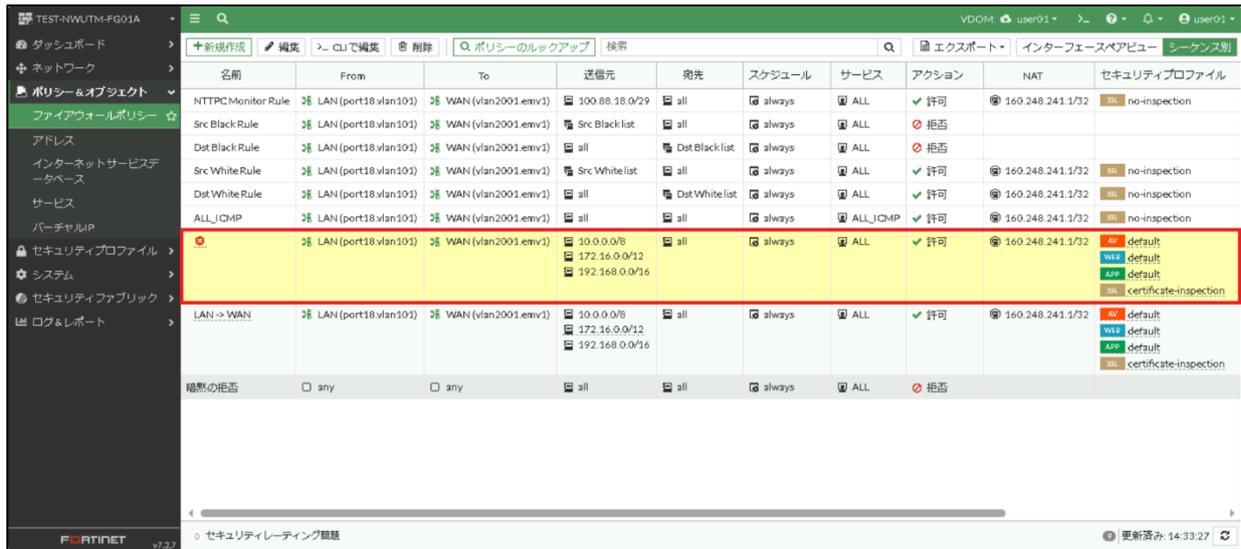
コピー

③ 再度 LAN→WAN 又は、webfilter-policy-\*を右クリックし、ペースト→上へを押下する。



名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル
NTTTPC Monitor Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	no-inspection
Src Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src Black list	all	always	ALL	拒否		
Dst Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst Black list	always	ALL	拒否		
Src White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src White list	all	always	ALL	許可	160.248.241.1/32	no-inspection
Dst White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst White list	always	ALL	許可	160.248.241.1/32	no-inspection
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/32	no-inspection
LAN -> WAN	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection
拒否の拒否	any		all	all	always	ALL	拒否		

④ 作成したポリシーをダブルクリックする。



名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル
NTTTPC Monitor Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	no-inspection
Src Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src Black list	all	always	ALL	拒否		
Dst Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst Black list	always	ALL	拒否		
Src White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src White list	all	always	ALL	許可	160.248.241.1/32	no-inspection
Dst White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst White list	always	ALL	許可	160.248.241.1/32	no-inspection
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/32	no-inspection
LAN -> WAN	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection
拒否の拒否	any	any	all	all	always	ALL	拒否		

- ⑤ 名前、送信元、宛先、サービス、セキュリティプロファイルを設定し OK を押下する。  
 ※コメントにコピー元の名前が入るので消すか任意のコメントを記入してください。  
 ※セキュリティプロファイルで使用する良いプロファイルは表 4.1 を参照

ポリシーの編集

名前

タイプ スタンダード ZTNA

着信インターフェース LAN (port18.vlan101)

発信インターフェース WAN (vlan2001.emv1)

送信元

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- 

IP/MACベースアクセスコントロール

宛先

- all
- 

スケジュール always

サービス

- ALL
- 

アクション 許可 拒否

インスペクションモード フローベース プロキシベース

ファイアウォール/ネットワークオプション

NAT

IPプール設定 発信インターフェースのアドレスを使用 ダイナミックIPプールを使う

- 160.248.241.1/32
- 

送信元ポートの保持

プロトコルオプション PROT default

セキュリティプロファイル

- アンチウイルス  AV default
- Webフィルタ  WEB default
- ビデオフィルタ
- アプリケーションコントロール  APP default
- IPS
- Eメールフィルタ

SSLインスペクション SSL certificate-inspection

ロギングオプション

許可トラフィックをログ  セキュリティイベント すべてのセッション

セッション開始時にログを生成

コメント  21/1023

このポリシーを有効化

「+」を押下すると右側にリストが表示されるので追加したい分をクリックする。  
 消すアドレスがある場合は「×」をクリックすると消えます。  
 送信元、宛先で追加したいものがない場合は 5.1 項を参照  
 サービスで追加したいものがない場合は 7.1 項を参照

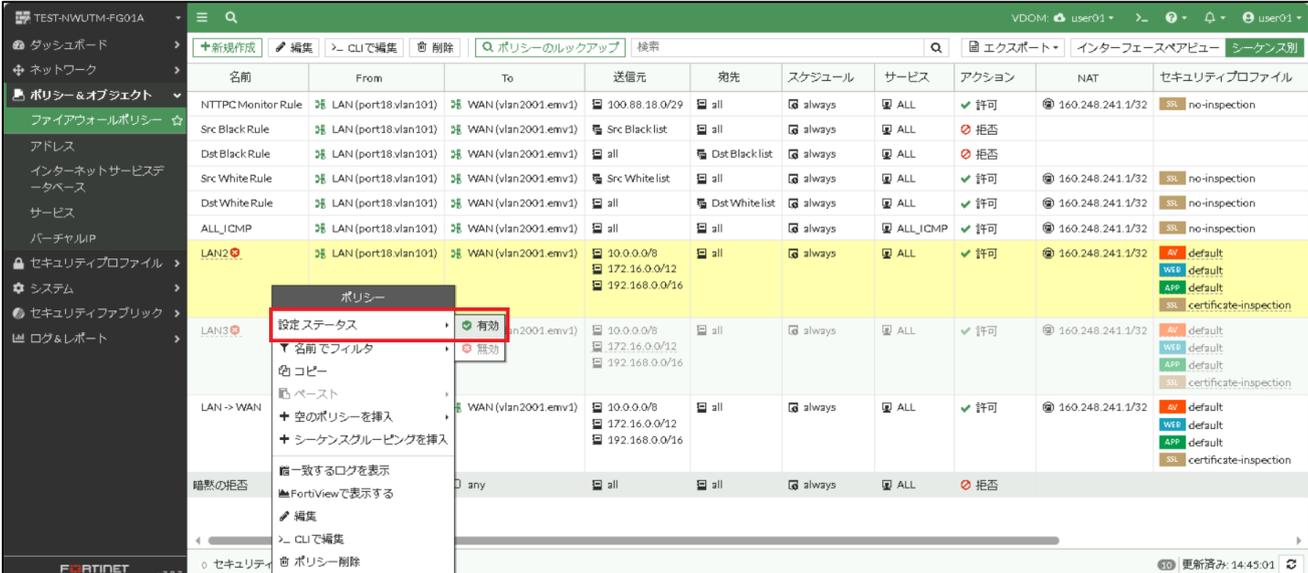
セキュリティ機能を有効化したい場合は各セキュリティ機能のトグルをクリックしてください。  
 使用しないセキュリティ機能はトグルをクリックし無効化にしてください。  
 詳細は 13 章を参照

- ⑥ 作成したルールを ALL\_ICMP より下の投入したい場所に名前部分でドラッグ&ドロップし移動させる。

名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル
NTTTPCMonitor Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection
Src Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src Black list	all	always	ALL	拒否		
Dst Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst Black list	always	ALL	拒否		
Src White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src White list	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection
Dst White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst White list	always	ALL	許可	160.248.241.1/32	SSL no-inspection
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/32	SSL no-inspection
LAN3	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection
LAN2	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection
LAN->WAN	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection
暗黙の拒否	any	any	all	all	always	ALL	拒否		

0 セキュリティレーティング問題 ストア 10 更新済み: 14:45:01

- ⑦ 対象のルールを右クリックし設定ステータス→有効を押下する。



名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル
NTTTPCMonitor Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection
Src Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src Black list	all	always	ALL	拒否		
Dst Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst Black list	always	ALL	拒否		
Src White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src White list	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection
Dst White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst White list	always	ALL	許可	160.248.241.1/32	SSL no-inspection
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/32	SSL no-inspection
LAN2	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection
LAN3	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection
LAN->WAN	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection
暗黙の拒否	any	any	all	all	always	ALL	拒否		

0 セキュリティレーティング問題 ストア 10 更新済み: 14:45:01

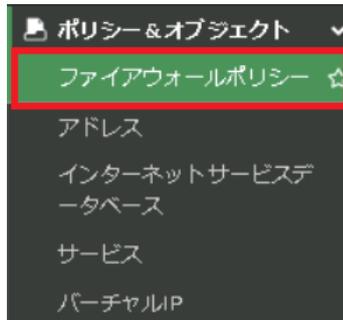
⑧ ルールが有効になったことを確認する。

The screenshot shows the Fortinet security policy configuration page. A table lists several rules. The 'LAN2' rule is highlighted with a red box. A callout box with Japanese text points to the 'LAN2' rule, stating: "×が消えていれば有効化されている" (If the 'x' disappears, the rule is activated).

名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル
NTTPC Monitor Rule	LAN (p		10.0.0.0/24	all	always	ALL	許可	160.248.241.1/32	no-inspection
Src Black Rule	LAN (p			all	always	ALL	拒否		
Dst Black Rule	LAN (p			Dst Black list	always	ALL	拒否		
Src White Rule	LAN (p			all	always	ALL	許可	160.248.241.1/32	no-inspection
Dst White Rule	LAN (p			Dst White list	always	ALL	許可	160.248.241.1/32	no-inspection
ALL_ICMP	LAN (port18	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/32	no-inspection
LAN2	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection
LAN3	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection
LAN->WAN	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection
暗黙の拒否	any	any	all	all	always	ALL	拒否		

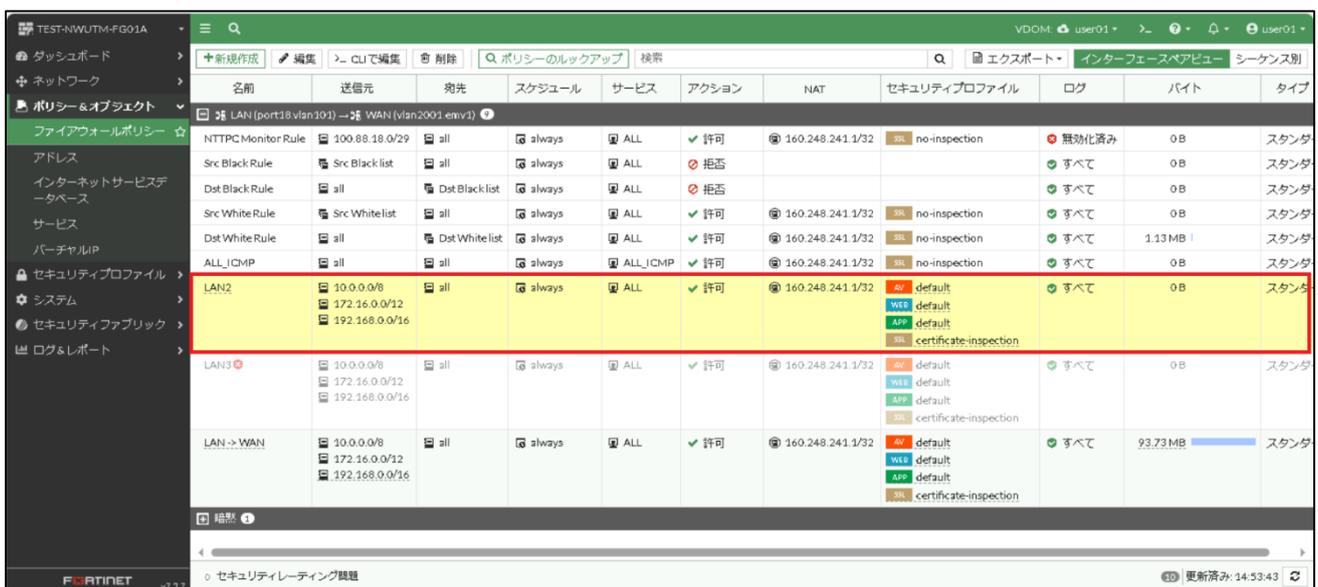
### 4.3 ファイアウォールルールの変更（表示形式：インターフェースペアビューの場合）

- ① 左のメニューからポリシー&オブジェクト->ファイアウォールポリシーを選択する。



- ② 変更したいポリシーをダブルクリックします。

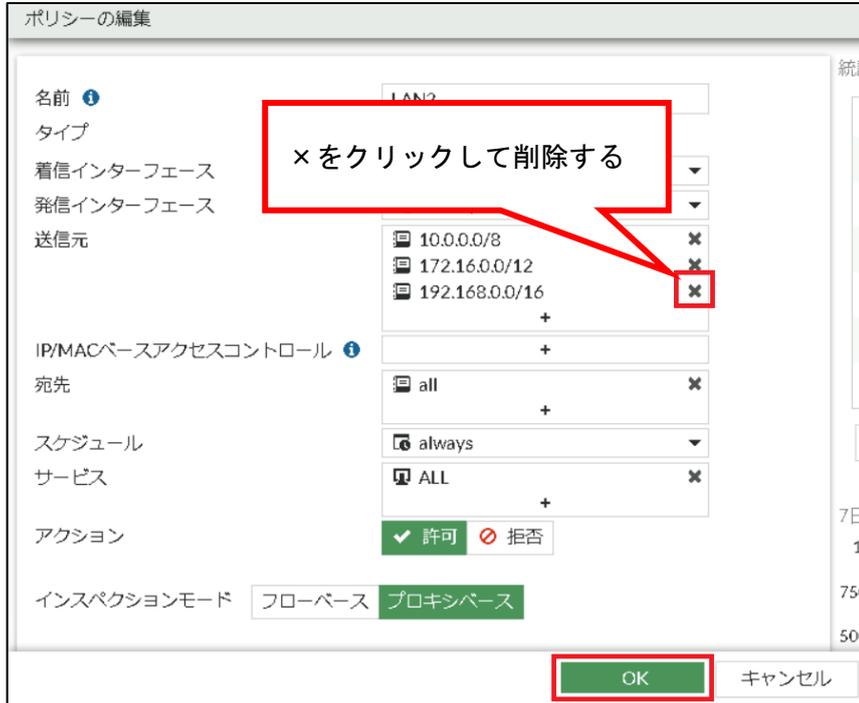
例：送信元の 192.168.0.0/16 を削除したい場合。



名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト	タイプ
NTTPC Monitor Rule	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	no-inspection	無効化済み	0B	スタンダ
Src Black Rule	Src Black list	all	always	ALL	拒否			すべて	0B	スタンダ
Dst Black Rule	all	Dst Black list	always	ALL	拒否			すべて	0B	スタンダ
Src White Rule	Src White list	all	always	ALL	許可	160.248.241.1/32	no-inspection	すべて	0B	スタンダ
Dst White Rule	all	Dst White list	always	ALL	許可	160.248.241.1/32	no-inspection	すべて	1.13 MB	スタンダ
ALL_ICMP	all	all	always	ALL_ICMP	許可	160.248.241.1/32	no-inspection	すべて	0B	スタンダ
LAN2	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	default default default certificate-inspection	すべて	0B	スタンダ
LAN3	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	default default default certificate-inspection	すべて	0B	スタンダ
LAN->WAN	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	default default default certificate-inspection	すべて	93.73 MB	スタンダ

- ③ 変更したい箇所の設定の変更をし、OK を押下する。

※変更可能な個所は下記図 4-1 を参照願います。

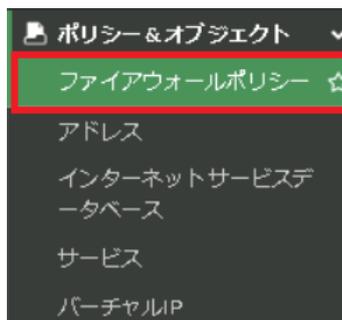


- ④ 変更完了後、正しく変更されたことを確認します。

LAN2	<input checked="" type="checkbox"/> 10.0.0.0/8 <input checked="" type="checkbox"/> 172.16.0.0/12	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> 許可	<input checked="" type="checkbox"/> 160.248.241.1/...	<input checked="" type="checkbox"/> AV defat <input checked="" type="checkbox"/> WEB defat <input checked="" type="checkbox"/> APP defat <input checked="" type="checkbox"/> SSL certif
------	---	---	--	---	--	---	--

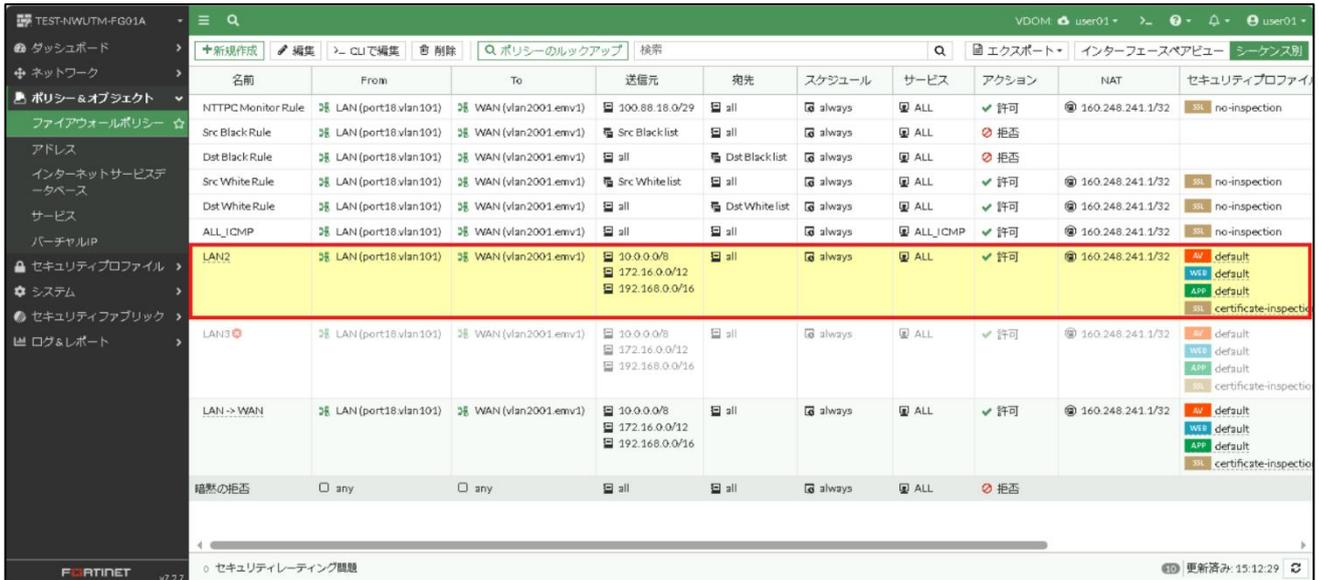
#### 4.4 ファイアウォールルールの変更（表示形式：シーケンス別の場合）

- ① 左のメニューからポリシー&オブジェクト->ファイアウォールポリシーを選択する。



② 変更したいポリシーをダブルクリックします。

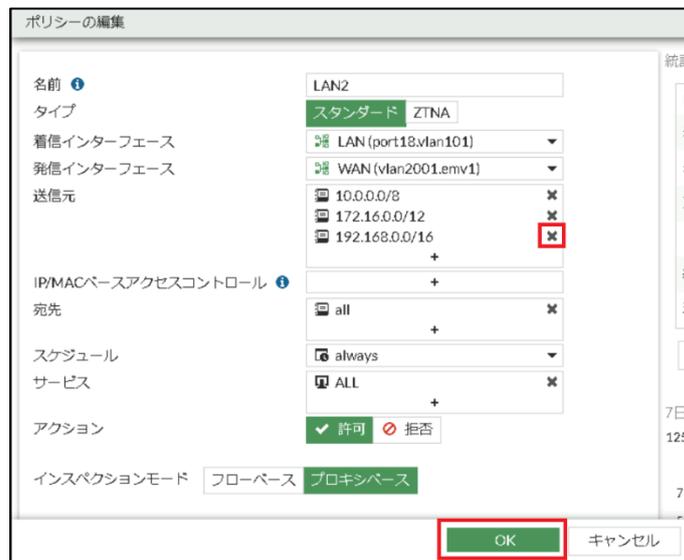
例：送信元の 192.168.0.0/16 を削除したい場合。



名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル
NTTFC Monitor Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	no-inspection
Src Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src Black list	all	always	ALL	拒否		
Dst Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst Black list	always	ALL	拒否		
Src White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src White list	all	always	ALL	許可	160.248.241.1/32	no-inspection
Dst White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst White list	always	ALL	許可	160.248.241.1/32	no-inspection
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/32	no-inspection
LAN2	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	default default certificate-inspect
LAN3	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	default default default certificate-inspect
LAN->WAN	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	default default default certificate-inspect
無条件の拒否	any	any	all	all	always	ALL	拒否		

③ 変更したい箇所の設定の変更をし、OK を押下する。

変更可能な箇所は下記図 4-1 を参照願います。



ポリシーの編集

名前: LAN2

タイプ: スタンダード ZTNA

着信インターフェース: LAN (port18.vlan101)

発信インターフェース: WAN (vlan2001.emv1)

送信元: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16

宛先: all

スケジュール: always

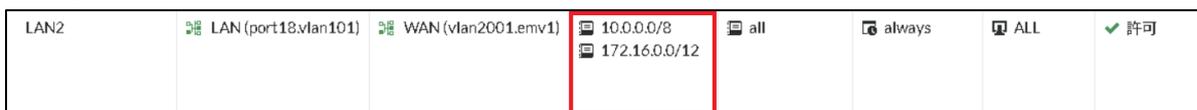
サービス: ALL

アクション: 許可

インスペクションモード: フローベース, プロキシベース

OK

④ 変更完了後、正しく変更されたことを確認します。

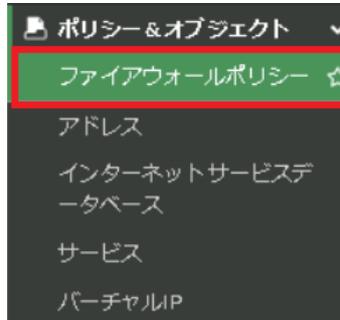


LAN2	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12	all	always	ALL	許可		
------	----------------------	---------------------	-----------------------------	-----	--------	-----	----	--	--

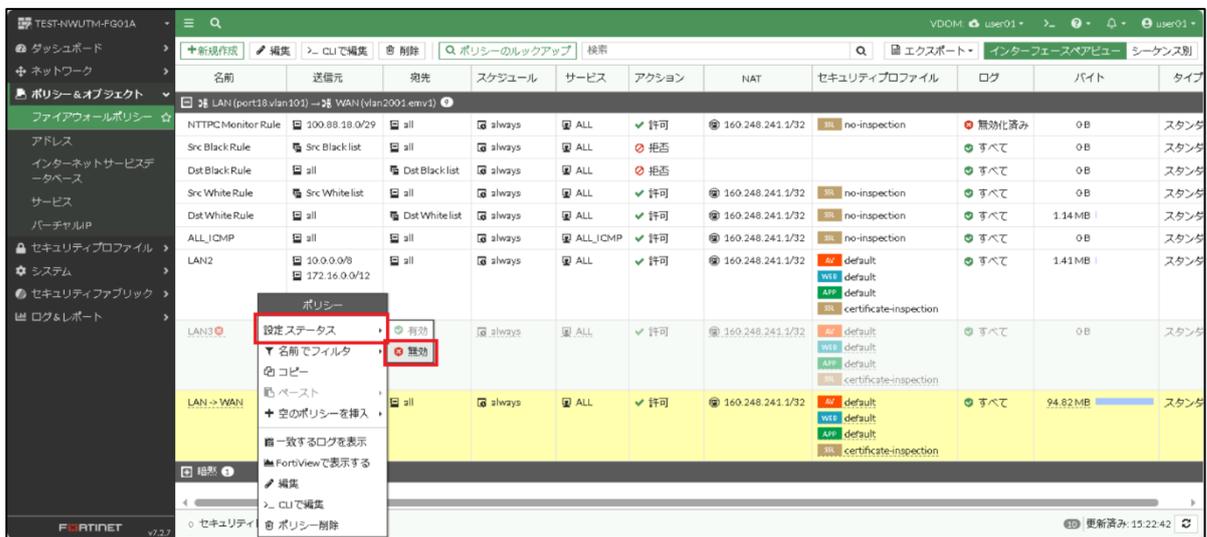
#### 4.5 ファイアウォールルールの無効化・削除（表示形式：インターフェースペアビューの場合）

##### ① ファイアウォールルールの無効化

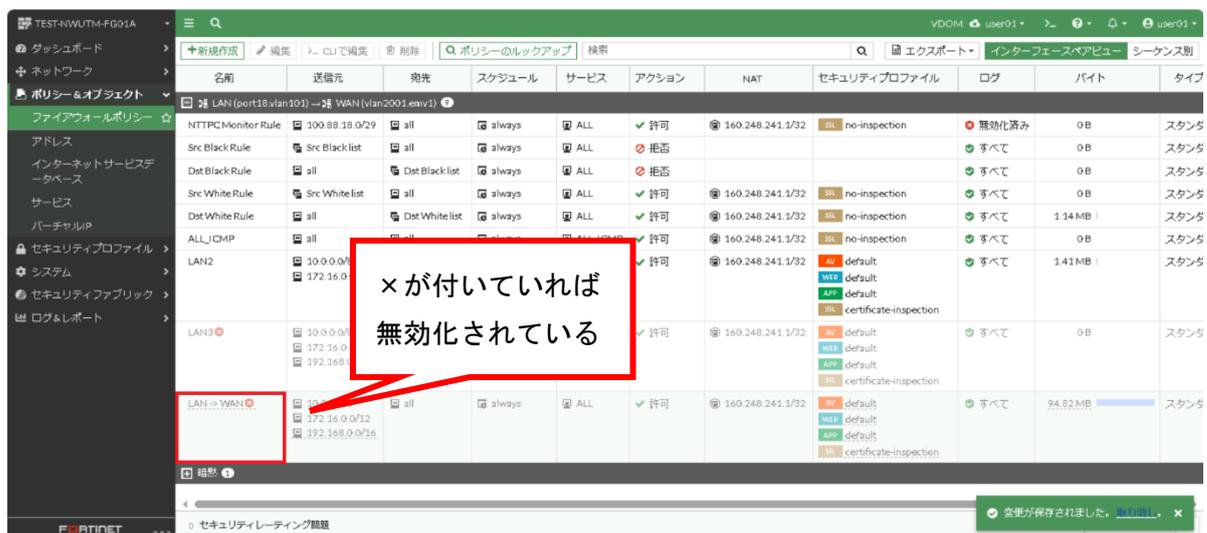
I. 左のメニューからポリシー&オブジェクト->ファイアウォールポリシーを選択する。



II. 無効化したいルールを右クリックし、設定ステータス->無効をクリックする。

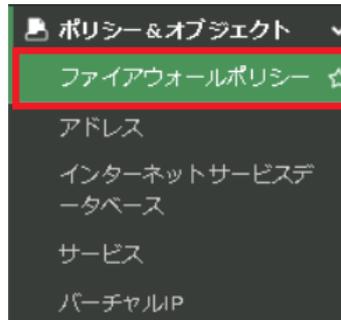


III. ルールが無効になっていることを確認する。

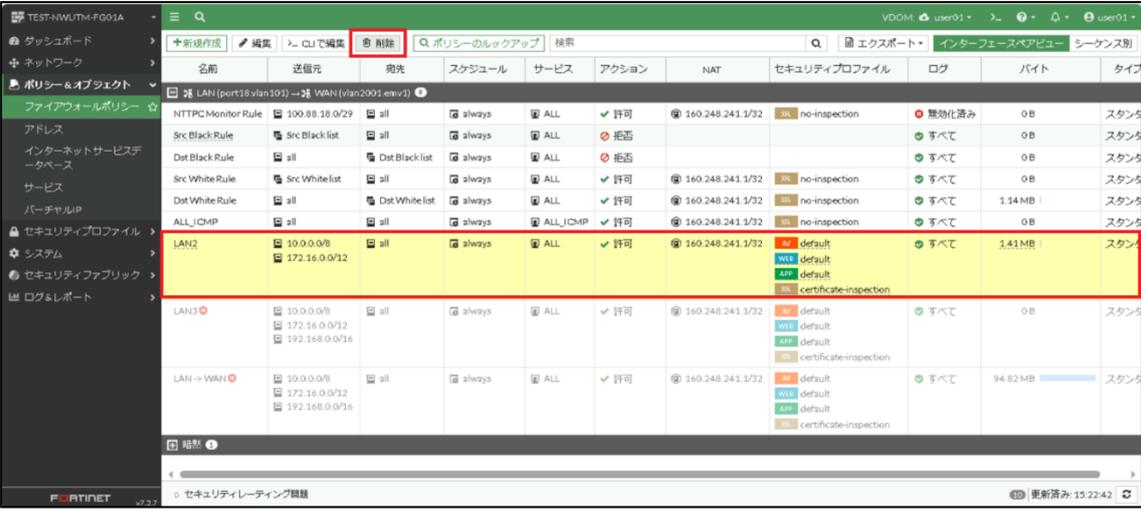


## ② ファイアウォールルール削除

I. 左のメニューからポリシー&オブジェクト->ファイアウォールポリシーを選択する。

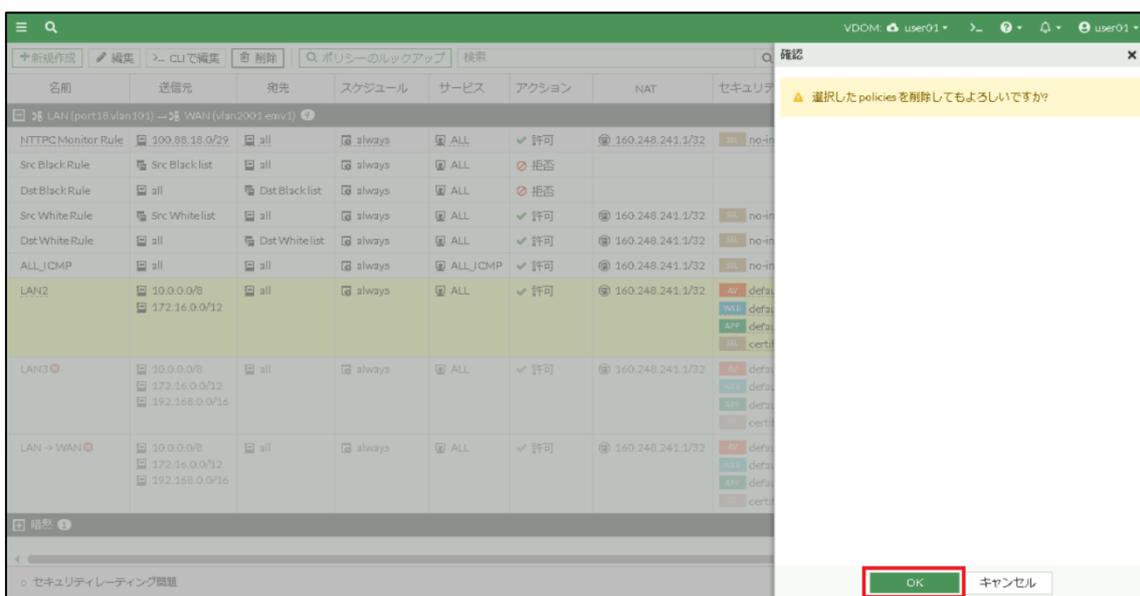


II. 削除したいルールをクリックし、削除をクリックする。



名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト	タイプ
NTTFC Monitor Rule	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	no-inspection	無効化済み	0B	スタンダ
Src Black Rule	Src Black list	all	always	ALL	拒否			すべて	0B	スタンダ
Dst Black Rule	Dst Black list	all	always	ALL	拒否			すべて	0B	スタンダ
Src White Rule	Src White list	all	always	ALL	許可	160.248.241.1/32	no-inspection	すべて	0B	スタンダ
Dst White Rule	Dst White list	all	always	ALL	許可	160.248.241.1/32	no-inspection	すべて	1.14 MB	スタンダ
ALL_Icmp	all	all	always	ALL_Icmp	許可	160.248.241.1/32	no-inspection	すべて	0B	スタンダ
LAN2	10.0.0.0/8 172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32	default default certificate-inspection	すべて	1.41 MB	スタンダ
LAN3	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	default default default certificate-inspection	すべて	0B	スタンダ
LAN -> WAN	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	default default default certificate-inspection	すべて	94.82 MB	スタンダ

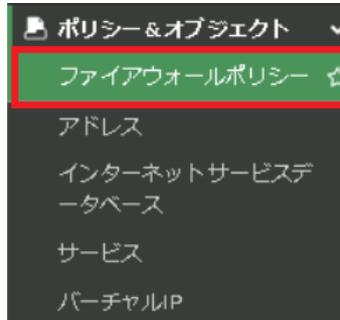
III. 確認画面が表示されるので OK を押下する。



#### 4.6 ファイアウォールルールの無効化・削除（表示形式：シーケンス別の場合）

##### ① ファイアウォールルールの無効化

I. 左のメニューからポリシー&オブジェクト->ファイアウォールポリシーを選択する。



II. 無効化したいルールを右クリックし、設定ステータス->無効をクリックする。

名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル
NTTPC Monitor Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	no-inspection
Src Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src Black list	all	always	ALL	拒否		
Dst Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst Black list	always	ALL	拒否		
Src White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src White list	all	always	ALL	許可	160.248.241.1/32	no-inspection
Dst White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst White list	always	ALL	許可	160.248.241.1/32	no-inspection
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/32	no-inspection
LAN2	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32	default default default certificate-inspection
LAN3	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	default default default certificate-inspection
LAN->WAN	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	default default default certificate-inspection
暗黙の拒否	any	any	any	all	always	ALL	拒否		

Context menu for 'LAN3' rule:

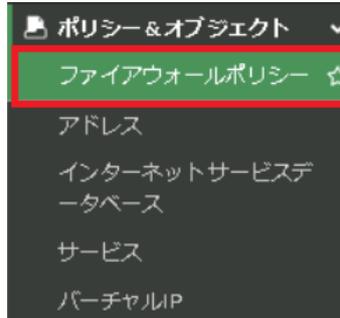
- 設定ステータス (設定ステータス)
- 名前でフィルタ
- コピー
- ペースト
- 空のポリシーを挿入
- シーケンスグループを挿入
- 一致するログを表示
- FortiViewで表示する
- 編集
- CLIで編集
- セキュリティ
- ポリシー削除

III. ルールが無効になっていることを確認する。

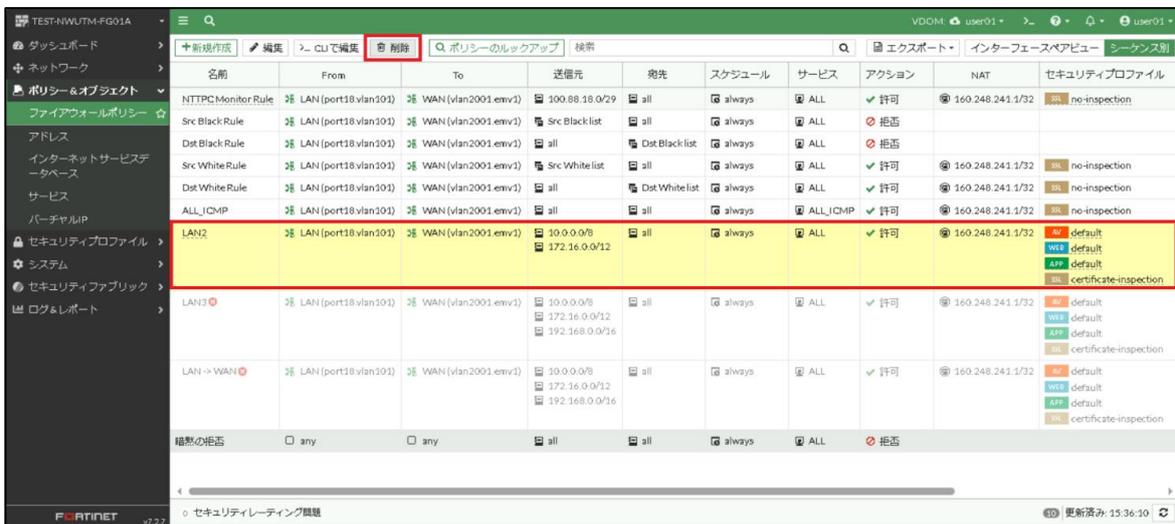
名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル
NTTPC Monitor Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	no-inspection
Src Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src Black list	all	always	ALL	拒否		
Dst Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst Black list	always	ALL	拒否		
Src White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src White list	all	always	ALL	許可	160.248.241.1/32	no-inspection
Dst White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst White list	always	ALL	許可	160.248.241.1/32	no-inspection
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/32	no-inspection
LAN2	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	default default default certificate-inspection
LAN3	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	default default default certificate-inspection
LAN->WAN	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	default default default certificate-inspection
暗黙の拒否	any	any	any	all	always	ALL	拒否		

## ② ファイアウォールルールの削除

I. 左のメニューからポリシー&オブジェクト->ファイアウォールポリシーを選択する。



II. 削除したいルールをクリックし、削除をクリックする。



III. 確認画面が表示されるので OK を押下する。

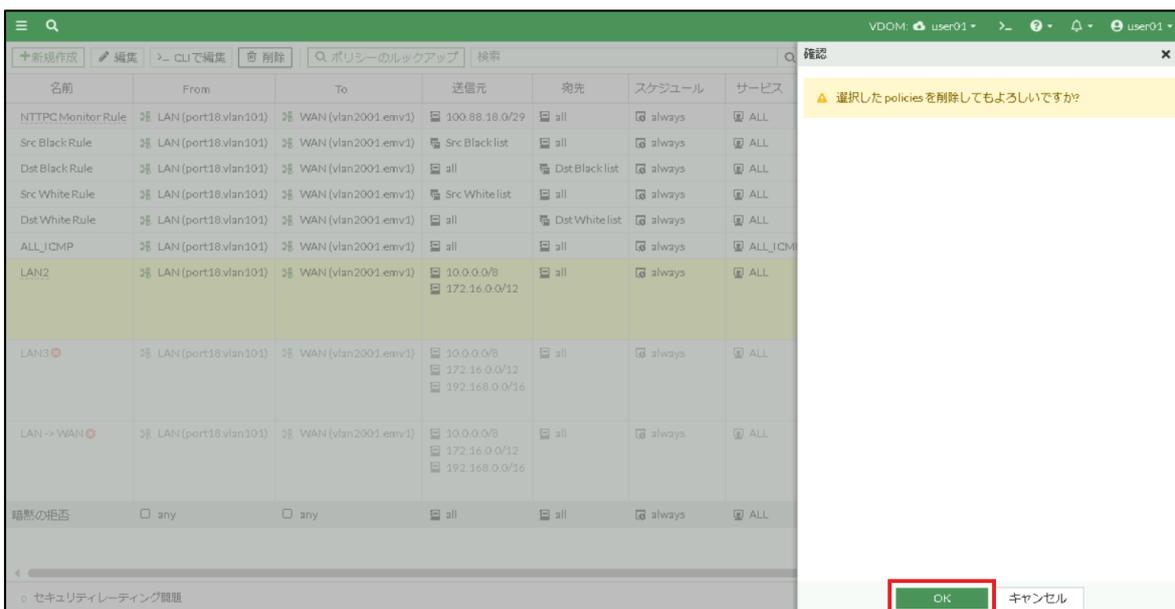


表 4-1. ファイアウォールルールの設定項目

	設定項目	変更内容	備考
1	名前	任意	
2	タイプ	スタンダード	
3	着信インターフェース	LAN(portB.vlan101)	LAN(portB.vlan101) もしくは WAN(vlan3101.emv1)
4	発信インターフェース	WAN(vlan3101.emv1)	WAN(vlan3101.emv1) もしくは LAN(portB.vlan101)
5	送信元	任意	アドレスの作成方法は 5.1 項参照
6	IP/MAC ベースアクセスコントロール	なし	
7	宛先	任意	アドレスの作成方法は 5.1 項参照
8	スケジュール	always	
9	サービス	任意	サービスの作成方法は 7.1 項参照
10	アクション	ACCEPT/DENY	
11	インスペクションモード	プロキシベース	
12	NAT	有効	
13	IP プール設定	ダイナミック IP プールを使用	
14	送信元ポートの保持	無効	
15	プロトコルオプション	g-default	g-default 以外を使用した場合、動作しようはできません。
16	セキュリティプロファイル	アンチウイルス:有効/無効	※有効の場合、default のみ選択可
		Eメールフィルタ:有効/無効	※有効の場合、default のみ選択可
		IPS(侵入防止):有効/無効	※有効の場合、g-default のみ選択可
		WEB フィルタ:有効/無効	※有効の場合、default のみ選択可
		アプリケーションコントロール:有効/無効	※有効の場合、default のみ選択可
17	ロギングオプション	許可トラフィックをログ:すべてのセッション	
		セッション開始時にログを生成:無効	
18	コメント	任意	
19	有効化設定	有効/無効	

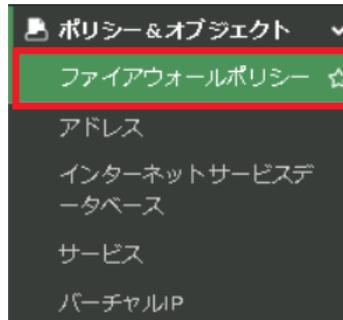
※ 上記以外の設定をした場合、動作保証はできません。

※ 灰色の網掛け部分に関しては変更出来ないパラメータとなります。

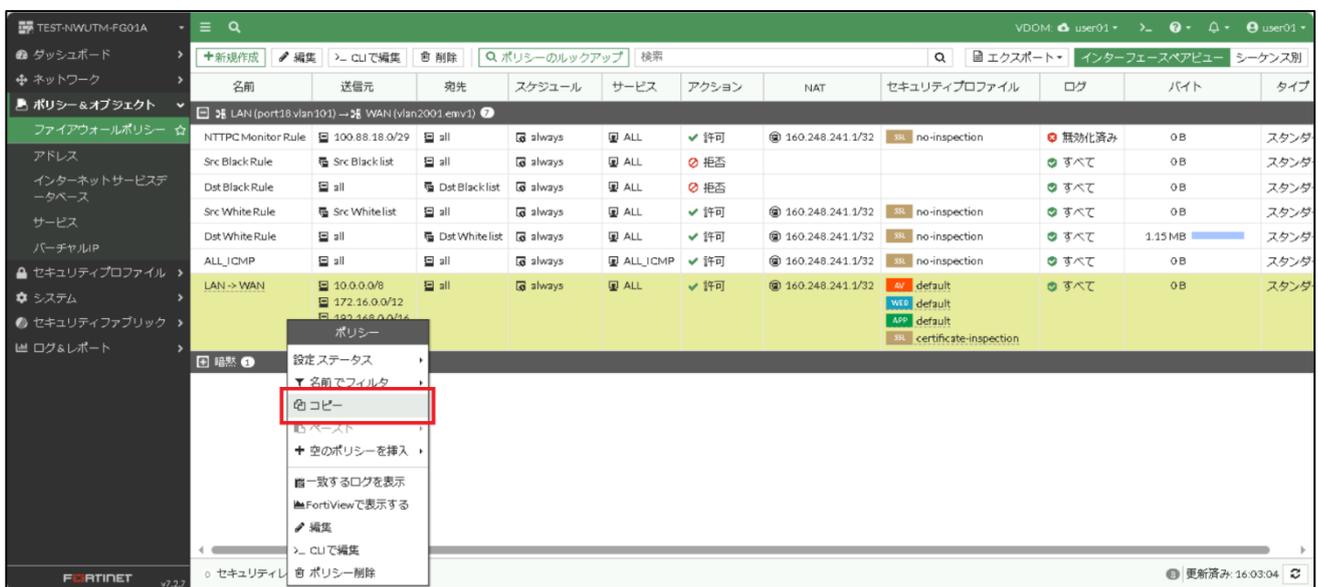
※ 水色の網掛け部分に関しては DNAT 使用時のみ変更できるパラメータとなります。

#### 4.7 SNAT 設定方法（表示形式：インターフェースペアビューの場合）

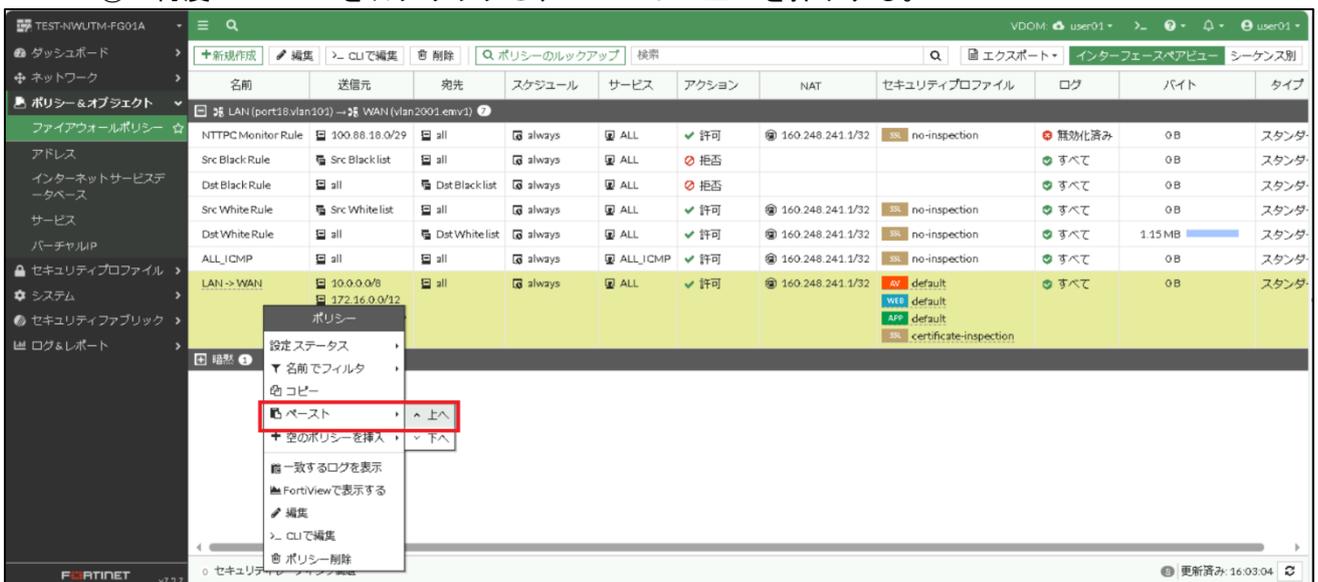
- ① 左メニューよりポリシー&オブジェクト→ファイアウォールポリシーを選択する。



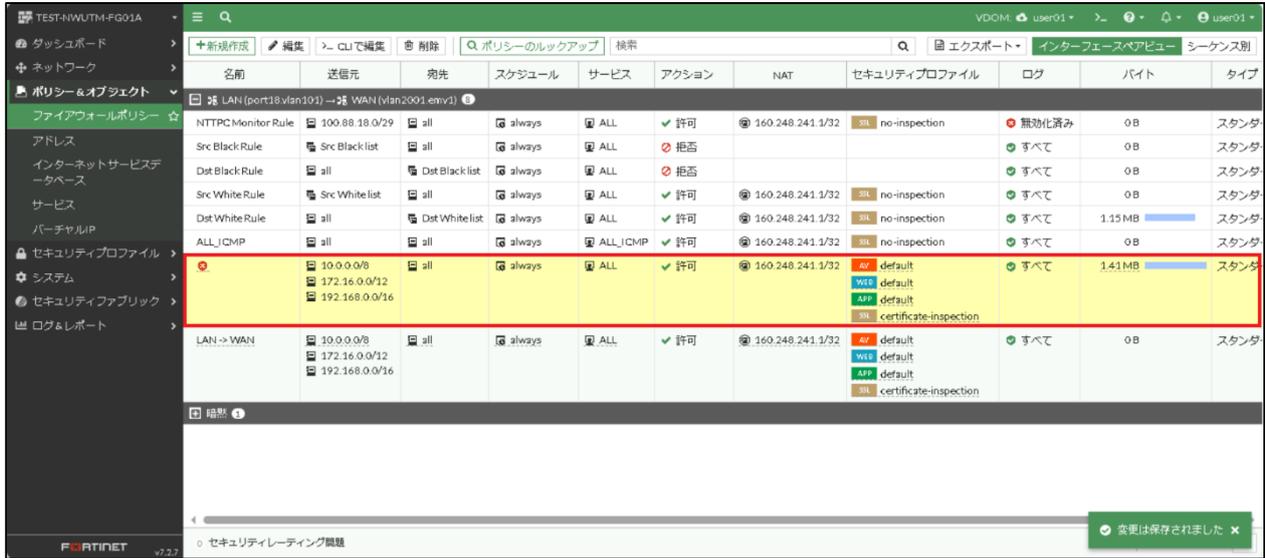
- ② LAN→WAN を右クリックし、コピーを押下する。



- ③ 再度 LAN→WAN を右クリックし、ペースト→上へを押下する。



④ 作成したポリシーをダブルクリックする。



名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト	タイプ
LAN (port18.vlan101) → WAN (vlan2001-emb1)										
NTPC Monitor Rule	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	無効化済み	0B	スタンプ
Src Black Rule	Src Black list	all	always	ALL	拒否			すべて	0B	スタンプ
Dst Black Rule	Dst Black list	all	always	ALL	拒否			すべて	0B	スタンプ
Src White Rule	Src White list	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	0B	スタンプ
Dst White Rule	Dst White list	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	1.15 MB	スタンプ
ALL ICMP	all	all	always	ALL ICMP	許可	160.248.241.1/32	SSL no-inspection	すべて	0B	スタンプ
	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて	1.41 MB	スタンプ
LAN → WAN	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて	0B	スタンプ

- ⑤ 名前、送信元、宛先、サービス、IP プール、セキュリティプロファイル、コメント（任意）を設定し OK を押下する。

※IP プールが SNAT のアドレス設定になりますので追加グローバル IP を設定する。

※コメントにコピー元の名前が入るので消すか任意のコメントを記入してください。

※セキュリティプロファイルで使用する良いプロファイルは表 4.1 を参照

「+」を押下すると右側にリストが表示されるので追加したい分をクリックする。

消すアドレスがある場合は「×」をクリックすると消えます。

送信元、宛先で追加したいものがない場合は 5.1 項を参照

サービスで追加したいものがない場合は 7.1 項を参照

すでに設定されているアドレスを「×」で消す。

「+」を押下し右側のリストから追加グローバル IP をクリックする。

セキュリティ機能を有効化したい場合は各セキュリティ機能のトグルをクリックしてください。

使用しないセキュリティ機能はトグルをクリックし無効化にしてください。

詳細は 13 章を参照

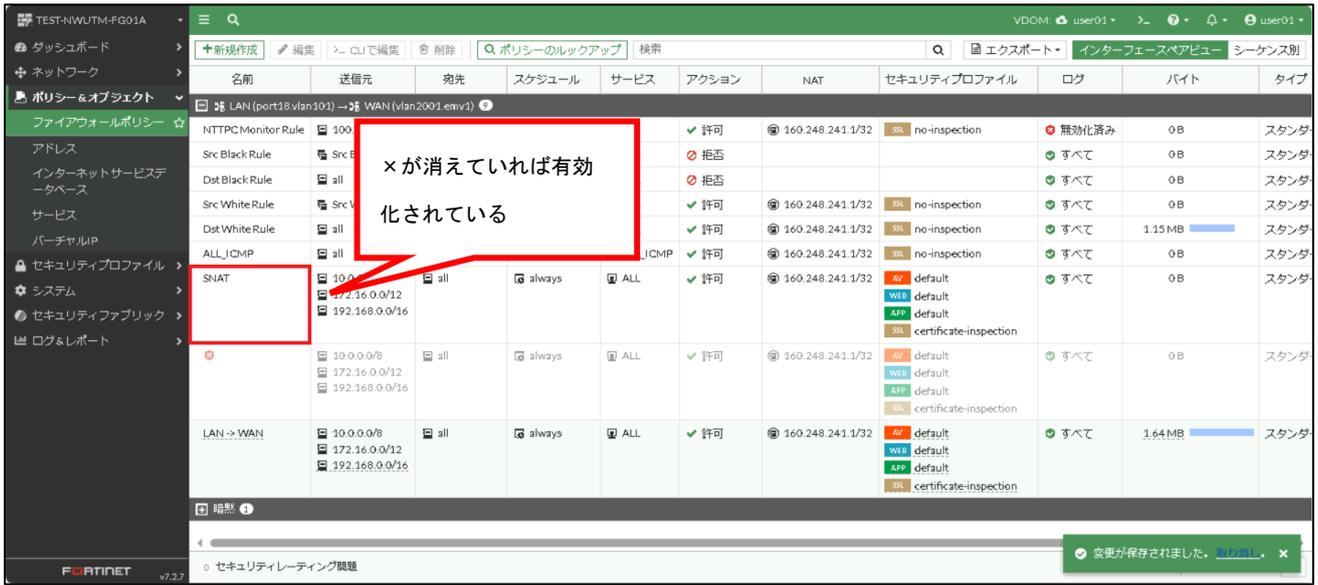
⑥ 作成したルールを ALL\_ICMP より下の投入したい場所に名前部分でドラッグ&ドロップし移動させる。

名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト	タイプ
LAN (port18.vlan101) → WAN (vlan2001.emv1)										
NTTTCMonitor Rule	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	無効化済み	0B	スタンダ
Src Black Rule	Src Black list	all	always	ALL	拒否			すべて	0B	スタンダ
Dst Black Rule	all	Dst Black list	always	ALL	拒否			すべて	0B	スタンダ
Src White Rule	Src White list	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	0B	スタンダ
Dst White Rule	all	Dst White list	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	1.15 MB	スタンダ
ALL_ICMP	all	all	always	ALL_ICMP	許可	160.248.241.1/32	SSL no-inspection	すべて	0B	スタンダ
SNAT	10.0.0.0/8	all	always	ALL	許可	160.248.241.1/32	AV default	すべて	0B	スタンダ
	WEB default									
	SSL certificate-inspection									
LAN → WAN	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて	1.64 MB	スタンダ

⑦ 対象のルールを右クリックし設定ステータス→有効を押下する。

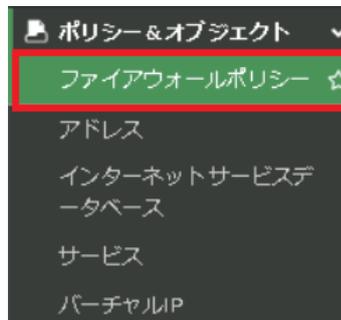
名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト	タイプ
LAN (port18.vlan101) → WAN (vlan2001.emv1)										
NTTTCMonitor Rule	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	無効化済み	0B	スタンダ
Src Black Rule	Src Black list	all	always	ALL	拒否			すべて	0B	スタンダ
Dst Black Rule	all	Dst Black list	always	ALL	拒否			すべて	0B	スタンダ
Src White Rule	Src White list	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	0B	スタンダ
Dst White Rule	all	Dst White list	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	1.15 MB	スタンダ
ALL_ICMP	all	all	always	ALL_ICMP	許可	160.248.241.1/32	SSL no-inspection	すべて	0B	スタンダ
SNAT	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default	すべて	0B	スタンダ
							WEB default			
							SSL certificate-inspection			
LAN → WAN	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて	1.64 MB	スタンダ

⑧ ルールが有効になったことを確認する。

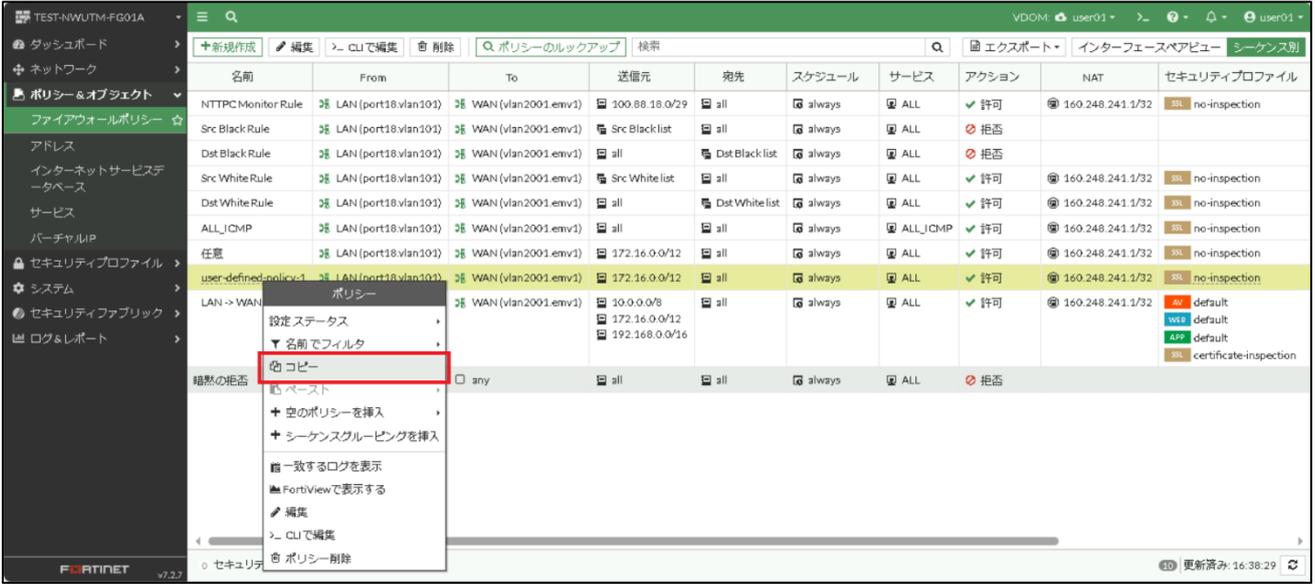


4.8 SNAT 設定方法（表示形式：シーケンス別の場合）

- ① 左メニューよりポリシー&オブジェクト→ファイアウォールポリシーを選択する。

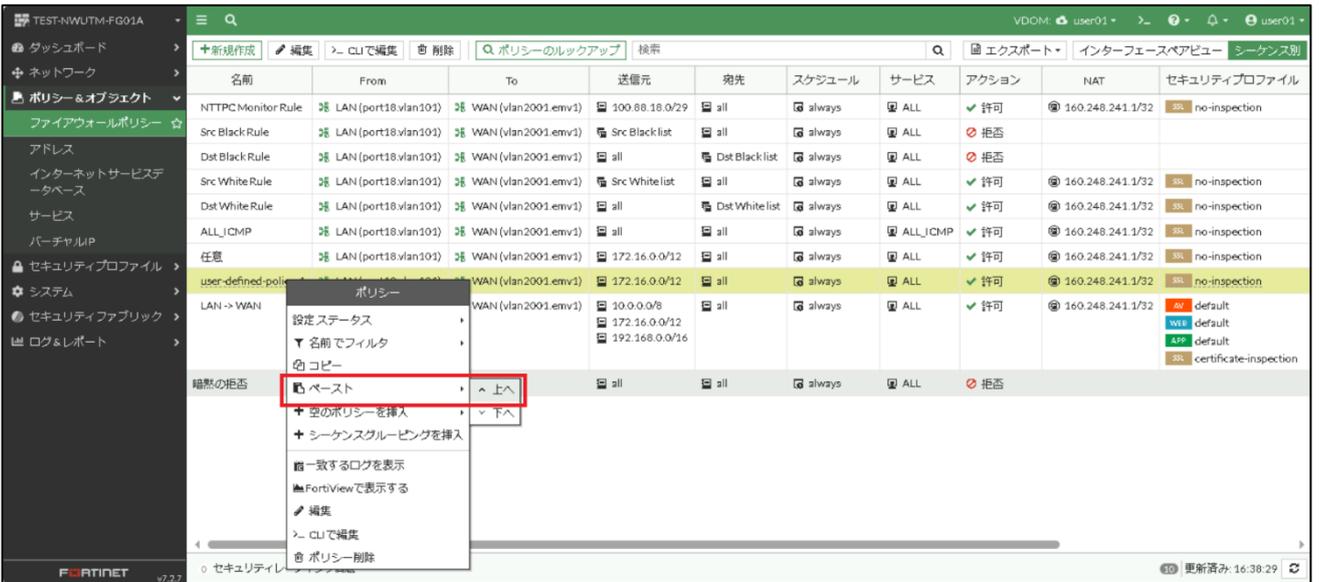


② user-defined-policy-1 を右クリックし、コピーを押下する。



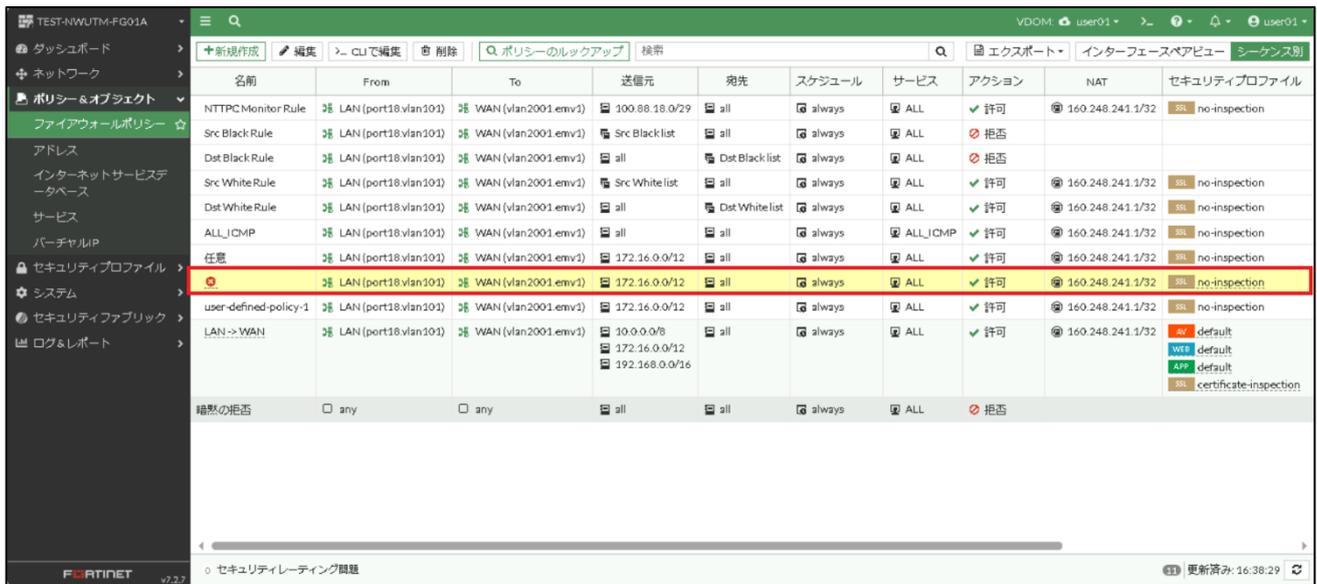
名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル
NTTTPC Monitor Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	no-inspection
Src Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src Black list	all	always	ALL	拒否		
Dst Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst Black list	always	ALL	拒否		
Src White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src White list	all	always	ALL	許可	160.248.241.1/32	no-inspection
Dst White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst White list	always	ALL	許可	160.248.241.1/32	no-inspection
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/32	no-inspection
任意	LAN (port18.vlan101)	WAN (vlan2001.emv1)	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32	no-inspection
user-defined-policy-1	LAN (port18.vlan101)	WAN (vlan2001.emv1)	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32	no-inspection
LAN -> WAN		WAN (vlan2001.emv1)	10.0.0.0/8	all	always	ALL	許可	160.248.241.1/32	default
			172.16.0.0/12						default
			192.168.0.0/16						certificate-inspection
暗黙の拒否		any	all	all	always	ALL	拒否		

③ 再度 user-defined-policy-1 を右クリックし、ペースト→上へを押下する。



名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル
NTTTPC Monitor Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	no-inspection
Src Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src Black list	all	always	ALL	拒否		
Dst Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst Black list	always	ALL	拒否		
Src White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src White list	all	always	ALL	許可	160.248.241.1/32	no-inspection
Dst White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst White list	always	ALL	許可	160.248.241.1/32	no-inspection
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/32	no-inspection
任意	LAN (port18.vlan101)	WAN (vlan2001.emv1)	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32	no-inspection
user-defined-policy-1	LAN (port18.vlan101)	WAN (vlan2001.emv1)	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32	no-inspection
LAN -> WAN		WAN (vlan2001.emv1)	10.0.0.0/8	all	always	ALL	許可	160.248.241.1/32	default
			172.16.0.0/12						default
			192.168.0.0/16						certificate-inspection
暗黙の拒否		any	all	all	always	ALL	拒否		

④ 作成したポリシーをダブルクリックする。



The screenshot shows the Fortinet Firewall Policy configuration interface. The 'Policy' tab is selected, and the 'user-defined-policy-1' policy is highlighted with a red border. The table below represents the data shown in the interface.

名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル
NTTPC Monitor Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection
Src Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src Blacklist	all	always	ALL	拒否		
Dst Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst Blacklist	always	ALL	拒否		
Src White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src White list	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection
Dst White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst White list	always	ALL	許可	160.248.241.1/32	SSL no-inspection
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/32	SSL no-inspection
任意	LAN (port18.vlan101)	WAN (vlan2001.emv1)	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection
user-defined-policy-1	LAN (port18.vlan101)	WAN (vlan2001.emv1)	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection
LAN->WAN	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	SSL certificate-inspection AV default WEB default APP default
暗黙の拒否	<input type="checkbox"/> any	<input type="checkbox"/> any	all	all	always	ALL	拒否		

- ⑤ 名前、送信元、宛先、サービス、IP プール、セキュリティプロファイル、コメント（任意）を設定し OK を押下する。

※IP プールが SNAT のアドレス設定になりますので追加グローバル IP を設定する。

※コメントにコピー元の名前が入るので消すか任意のコメントを記入してください。

※セキュリティプロファイルで使用する良いプロファイルは表 4.1 を参照

The screenshot shows the 'ポリシーの編集' (Policy Edit) screen. Key sections include:

- 名前:** 任意1
- タイプ:** スタンドアード ZTNA
- 発信インターフェース:** LAN (port18.vlan101)
- 発信インターフェース:** WAN (vlan2001.enw1)
- 送信元:** 172.16.0.0/12
- 宛先:** all
- スケジュール:** always
- サービス:** ALL
- アクション:** 許可 (checked), 拒否
- ファイアウォールネットワークオプション:**
  - NAT: ON
  - IPプール設定: 発信インターフェースのアドレスを使用 (selected), ダイナミックIPプールを使う
  - 送信元ポートの保持: ON
  - プロトコルオプション: default
- セキュリティプロファイル:**
  - アンチウイルス: OFF
  - Webフィルタ: OFF
  - ビデオフィルタ: OFF
  - アプリケーションコントロール: ON, APP default
  - IPS: OFF
  - Eメールフィルタ: OFF
- SSLインスペクション:** certificate-inspection
- ロギングオプション:**
  - 許可トラフィックをログ: ON, セキュリティイベント, すべてのセッション
  - セッション開始時にログを生成: ON
- コメント:** (Copy of LAN -> WAN) (Copy of 8) (Copy of user-defined-policy-1) / 65/1023
- このポリシーを有効化:** ON

Red boxes and arrows highlight the following elements:

- Source IP field:** A red box around '172.16.0.0/12' with an arrow pointing to a text box explaining that clicking '+' shows a list and clicking 'x' removes the address.
- Destination field:** A red box around 'all' with an arrow pointing to a text box explaining that clicking '+' shows a list and clicking 'x' removes the address.
- Service field:** A red box around 'ALL' with an arrow pointing to a text box explaining that clicking '+' shows a list and clicking 'x' removes the address.
- IP Pool Setting:** A red box around the 'ダイナミックIPプールを使う' option with an arrow pointing to a text box explaining that clicking '+' adds a global IP from the list.
- Security Profile:** A red box around the 'アプリケーションコントロール' toggle with an arrow pointing to a text box explaining that clicking the toggle turns security features on/off.
- Comment field:** A red box around the comment text with an arrow pointing to a text box explaining that the comment contains the source name and should be deleted or replaced.

- ⑥ 作成したルールを ALL\_ICMP または DNAT が設定されていればそれより下の投入したい場所に名前部分でドラッグ&ドロップし移動させる。

名前	From	To	送信元	宛先	スケジュー...	サービス	アクション...	NAT
NTTPC Monitor R...	LAN (port18.vlan1...	WAN (vlan2001.em...	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32
Src Black Rule	LAN (port18.vlan1...	WAN (vlan2001.em...	Src Black list	all	always	ALL	拒否	
Dst Black Rule	LAN (port18.vlan1...	WAN (vlan2001.em...	all	Dst Black l...	always	ALL	拒否	
Src White Rule	LAN (port18.vlan1...	WAN (vlan2001.em...	Src White list	all	always	ALL	許可	160.248.241.1/32
Dst White Rule	LAN (port18.vlan1...	WAN (vlan2001.em...	all	Dst White ...	always	ALL	許可	160.248.241.1/32
ALL_ICMP	LAN (port18.vlan1...	WAN (vlan2001.em...	all	all	always	ALL_IC...	許可	160.248.241.1/32
任意	LAN (port18.vlan1...	WAN (vlan2001.em...	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32
任意1	LAN (port18.vlan1...	WAN (vlan2001.em...	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32
user-defined-pol...	LAN (port18.vlan1...	WAN (vlan2001.em...	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32
LAN -> WAN	LAN (port18.vlan1...	WAN (vlan2001.em...	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32
暗黙の拒否	any	any	all	all	always	ALL	拒否	

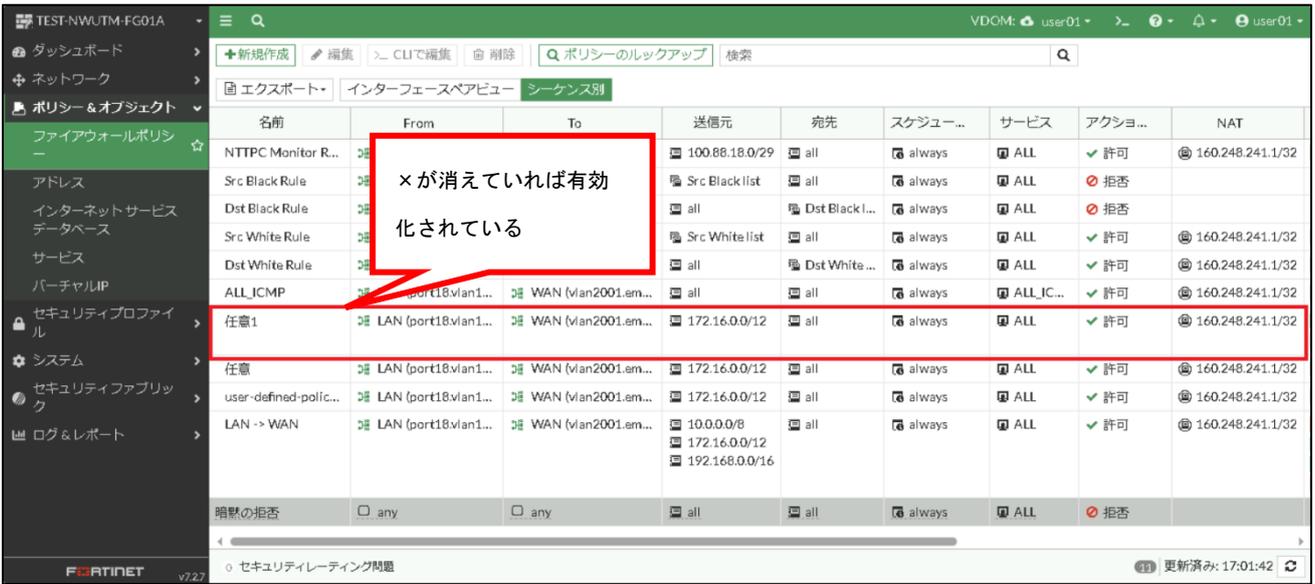
更新済み: 17:01:42

- ⑦ 対象のルールを右クリックし設定ステータス→有効を押下する。

名前	From	To	送信元	宛先	スケジュー...	サービス	アクション...	NAT
NTTPC Monitor R...	LAN (port18.vlan1...	WAN (vlan2001.em...	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32
Src Black Rule	LAN (port18.vlan1...	WAN (vlan2001.em...	Src Black list	all	always	ALL	拒否	
Dst Black Rule	LAN (port18.vlan1...	WAN (vlan2001.em...	all	Dst Black l...	always	ALL	拒否	
Src White Rule	LAN (port18.vlan1...	WAN (vlan2001.em...	Src White list	all	always	ALL	許可	160.248.241.1/32
Dst White Rule	LAN (port18.vlan1...	WAN (vlan2001.em...	all	Dst White ...	always	ALL	許可	160.248.241.1/32
ALL_ICMP	LAN (port18.vlan1...	WAN (vlan2001.em...	all	all	always	ALL_IC...	許可	160.248.241.1/32
任意1	LAN (port18.vlan1...	WAN (vlan2001.em...	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32
任意	LAN (port18.vlan1...	WAN (vlan2001.em...	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32
user-defined-pol...	LAN (port18.vlan1...	WAN (vlan2001.em...	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32
LAN -> WAN	LAN (port18.vlan1...	WAN (vlan2001.em...	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32
暗黙の拒否	any	any	all	all	always	ALL	拒否	

更新済み: 17:01:42

⑧ ルールが有効になったことを確認する。



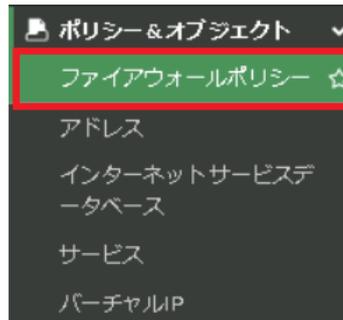
名前	From	To	送信元	宛先	スケジュー...	サービス	アクション...	NAT
NTTPC Monitor R...			100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32
Src Black Rule			Src Black list	all	always	ALL	拒否	
Dst Black Rule			all	Dst Black l...	always	ALL	拒否	
Src White Rule			Src White list	all	always	ALL	許可	160.248.241.1/32
Dst White Rule			all	Dst White ...	always	ALL	許可	160.248.241.1/32
ALL_ICMP	port18.vlan1...	WAN (vlan2001.em...	all	all	always	ALL_IC...	許可	160.248.241.1/32
任意1	LAN (port18.vlan1...	WAN (vlan2001.em...	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32
任意	LAN (port18.vlan1...	WAN (vlan2001.em...	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32
user-defined-polic...	LAN (port18.vlan1...	WAN (vlan2001.em...	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32
LAN -> WAN	LAN (port18.vlan1...	WAN (vlan2001.em...	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32
暗黙の拒否	any	any	all	all	always	ALL	拒否	

×が消えていれば有効化されている

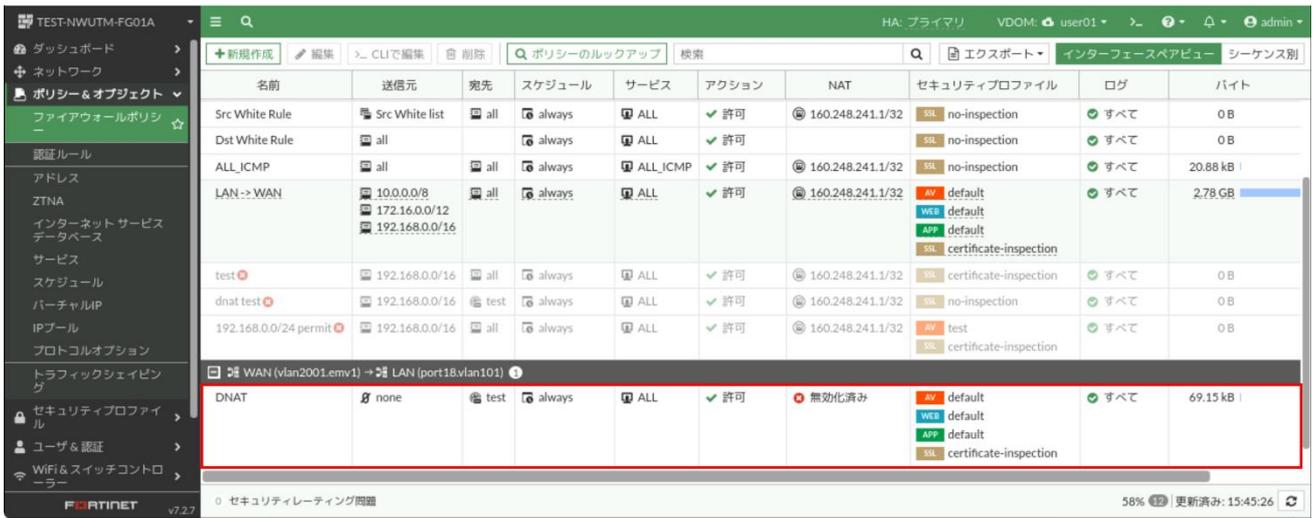
#### 4.9 DNAT 申込時の送信元初期設定“none”の変更方法（表示形式：インターフェースペアビューの場合）

DNAT をお申込みいただいた場合、DNAT のファイアウォールポリシーが作成されます。  
送信元の初期設定は“none”となっておりますので送信元を設定してください

- ① 左メニューよりポリシー&オブジェクト→ファイアウォールポリシーを選択する。

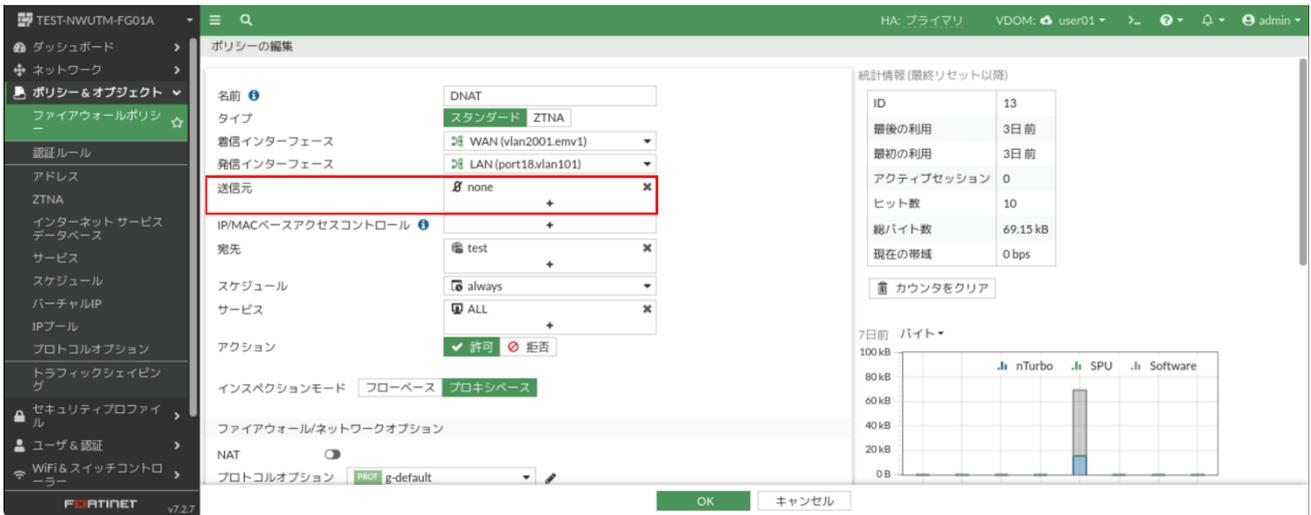


- ② お申込により作成された DNAT のポリシーをダブルクリックする。

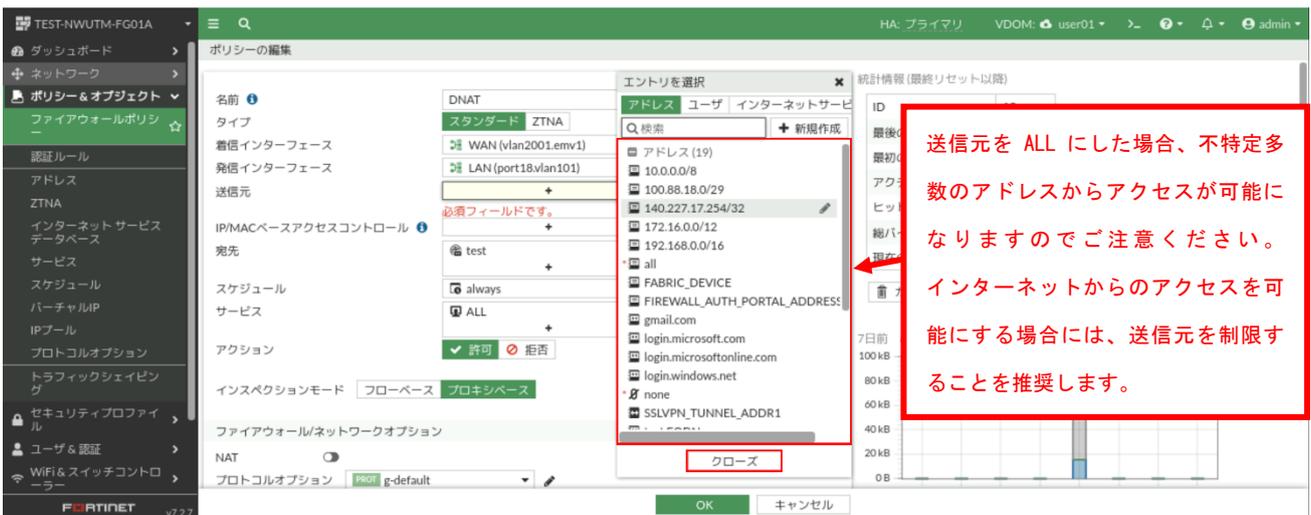


名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト
Src White Rule	Src White list	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	0 B
Dst White Rule	all		always	ALL	許可		SSL no-inspection	すべて	0 B
ALL_ICMP	all	all	always	ALL_ICMP	許可	160.248.241.1/32	SSL no-inspection	すべて	20.88 kB
LAN->WAN	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて	2.78 GB
test	192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	SSL certificate-inspection	すべて	0 B
dnat test	192.168.0.0/16	test	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	0 B
192.168.0.0/24 permit	192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV test SSL certificate-inspection	すべて	0 B
WAN (vlan2001.emv1) → LAN (port18.vlan101)									
DNAT	none	test	always	ALL	許可	無効化済み	AV default WEB default APP default SSL certificate-inspection	すべて	69.15 kB

③ 送信元が「none」となっていることを確認し、「none」の右の×を押下する。



④ 「エントリーを選択」から通信を行う送信元アドレスを選択しクローズを押下する。



⑤ 送信元が問題ないことを確認し OK ボタンを押下する。



ポリシーの編集

名前: DNAT

タイプ: スタンダード ZTNA

着信インターフェース: WAN (vlan2001.emv1)

発信インターフェース: LAN (port18.vlan101)

送信元: 140.227.17.254/32

宛先: test

スケジュール: always

サービス: ALL

アクション: 許可

インスペクションモード: フローベース プロキシベース

ファイアウォール/ネットワークオプション

NAT: 有効

プロトコルオプション: PROT g-default

統計情報 (最終リセット以降)

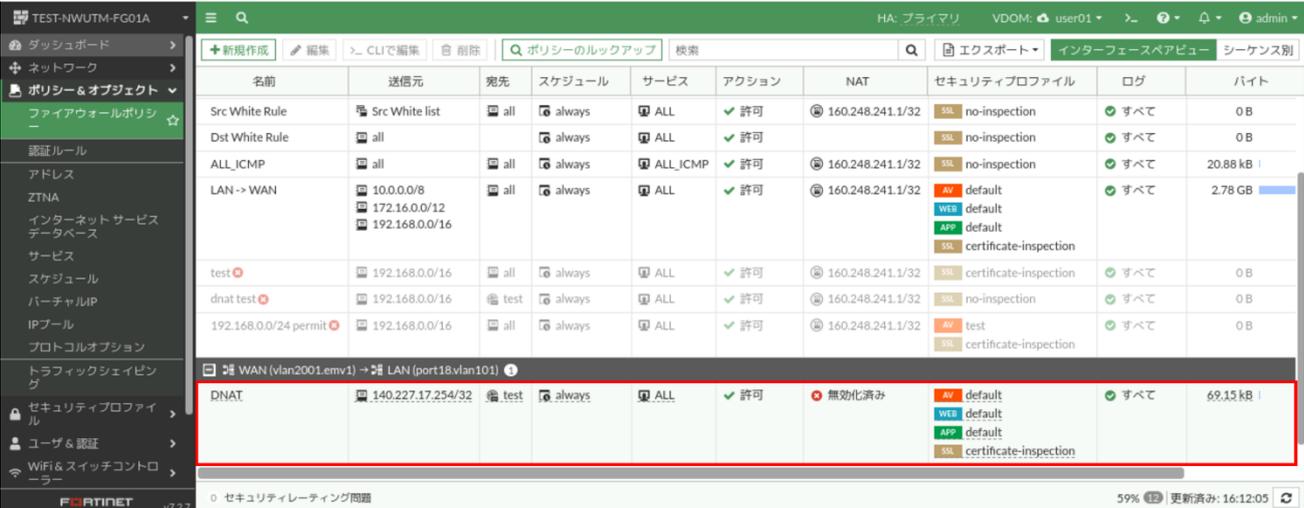
ID	13
最後の利用	3日前
最初の利用	3日前
アクティブセッション	0
ヒット数	10
総バイト数	69.15 kB
現在の帯域	0 bps

7日前 バイト

100kB  
80kB  
60kB  
40kB  
20kB  
0B

OK キャンセル

⑥ 送信元の欄が問題なく設定されていることを確認する。



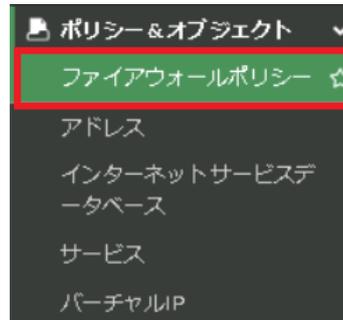
新規作成 編集 CLIで編集 削除 ポリシーのルックアップ 検索 エクスポート インターフェースレビュー シーケンス別

名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト
Src White Rule	Src White list	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	0 B
Dst White Rule	all		always	ALL	許可		SSL no-inspection	すべて	0 B
ALL_ICMP	all	all	always	ALL_ICMP	許可	160.248.241.1/32	SSL no-inspection	すべて	20.88 kB
LAN -> WAN	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて	2.78 GB
test	192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	SSL certificate-inspection	すべて	0 B
dnat test	192.168.0.0/16	test	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	0 B
192.168.0.0/24 permit	192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV test SSL certificate-inspection	すべて	0 B
WAN (vlan2001.emv1) -> LAN (port18.vlan101)									
DNAT	140.227.17.254/32	test	always	ALL	許可	無効化済み	AV default WEB default APP default SSL certificate-inspection	すべて	69.15 kB

0 セキュリティレーティング問題 59% 更新済み: 16:12:05

#### 4.10 DNAT 申込時の送信元初期設定“none”の変更方法（表示形式：シーケンス別の場合）

- ① 左メニューよりポリシー&オブジェクト→ファイアウォールポリシーを選択する。



- ② お申込により作成された DNAT のポリシーをダブルクリックする。

名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロ
NTTTPC Monitor Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	no-inspec
Src Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src Black list	all	always	ALL	拒否		
Dst Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL	拒否		
Src White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src White list	all	always	ALL	許可	160.248.241.1/32	no-inspec
Dst White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL	許可		no-inspec
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/32	no-inspec
DNAT	WAN (vlan2001.emv1)	LAN (port18.vlan101)	none	test	always	ALL	許可	無効化済み	default default certificate
LAN->WAN	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	default default certificate
test	LAN (port18.vlan101)	WAN (vlan2001.emv1)	192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	certificate
dnat test	LAN (port18.vlan101)	WAN (vlan2001.emv1)	192.168.0.0/16	test	always	ALL	許可	160.248.241.1/32	no-inspec

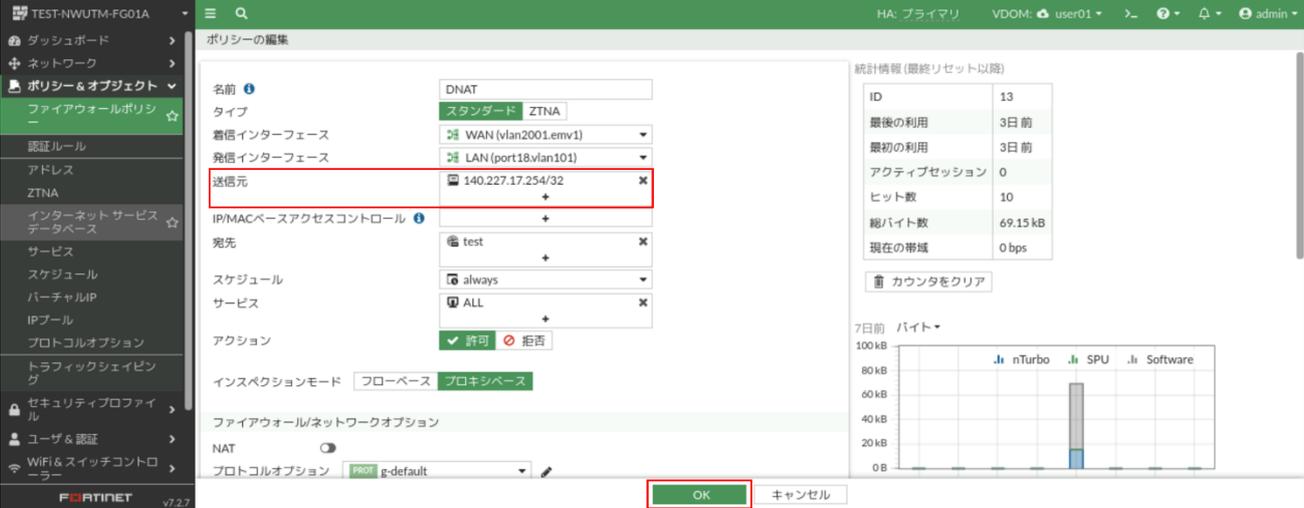
③ 送信元が「none」となっていることを確認し、「none」の右の×を押下する。

The screenshot shows the 'ポリシーの編集' (Edit Policy) page in Fortinet's management interface. The '送信元' (Source) field is highlighted with a red box and contains the value 'none'. To the right of this field is a small 'X' icon. The interface also shows other configuration options like 'タイプ' (Type), '着信インターフェース' (Destination Interface), and '発信インターフェース' (Source Interface). On the right side, there is a '統計情報' (Statistics) panel showing various metrics like ID, last used, and hit count.

④ 「エントリを選択」から通信を行う送信元アドレスを選択しクローズを押下する。

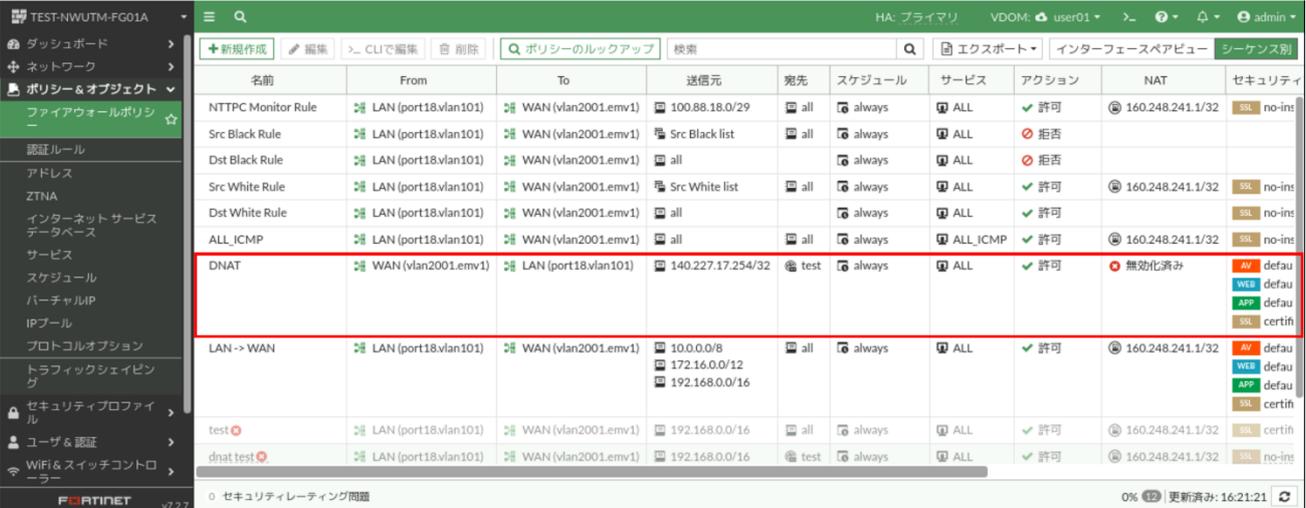
This screenshot shows the same policy configuration page as above, but with the 'エントリを選択' (Select Entry) dialog box open. The dialog has columns for 'アドレス' (Address), 'ユーザ' (User), and 'インターネットサービス' (Internet Service). A list of IP addresses and domains is displayed. A red box highlights the 'クローズ' (Close) button at the bottom of the dialog. To the right of the dialog, a red text box contains the following warning: '送信元を ALL にした場合、不特定多数のアドレスからアクセスが可能になりますのでご注意ください。インターネットからのアクセスを可能にする場合には、送信元を制限することを推奨します。' (When the source is set to ALL, access will be possible from an unspecified number of addresses, so please be careful. When enabling access from the Internet, it is recommended to restrict the source.)

⑤ 送信元が問題ないことを確認し OK ボタンを押下する。



Policy Editor Screenshot: A DNAT rule is being edited. The '送信元' (Source) field is set to '140.227.17.254/32'. The '宛先' (Destination) is 'test'. The 'アクション' (Action) is '許可' (Allow). The 'OK' button is highlighted in red.

⑥ 送信元の欄が問題なく設定されていることを確認する。

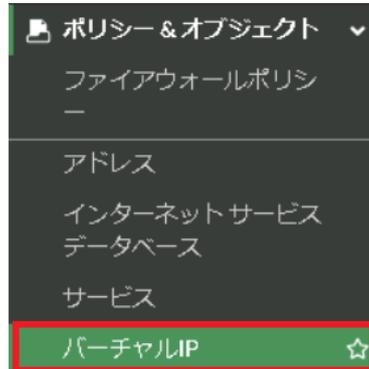


Policy List Screenshot: A table of policies is shown. The '送信元' (Source) column is highlighted in red. The table contains the following data:

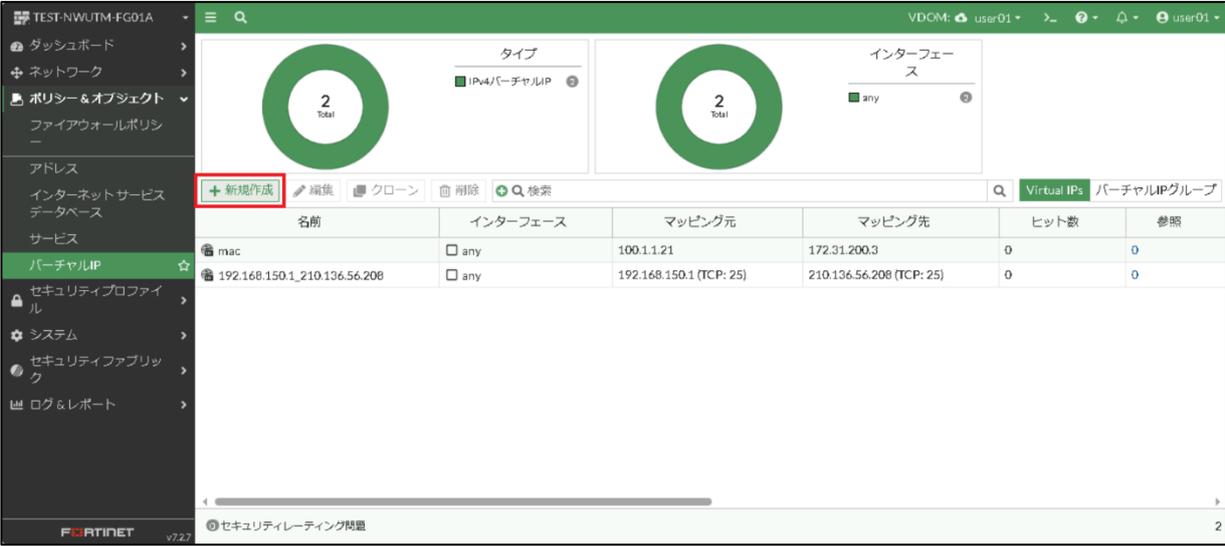
名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティ
NTTPC Monitor Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	SSL no-ins
Src Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src Black list	all	always	ALL	拒否		
Dst Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL	拒否		
Src White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src White list	all	always	ALL	許可	160.248.241.1/32	SSL no-ins
Dst White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL	許可		SSL no-ins
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/32	SSL no-ins
DNAT	WAN (vlan2001.emv1)	LAN (port18.vlan101)	140.227.17.254/32	test	always	ALL	許可	無効化済み	AV defau, WEB defau, APP defau, SSL certif
LAN->WAN	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV defau, WEB defau, APP defau, SSL certif
test	LAN (port18.vlan101)	WAN (vlan2001.emv1)	192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	SSL certif
dnat test	LAN (port18.vlan101)	WAN (vlan2001.emv1)	192.168.0.0/16	test	always	ALL	許可	160.248.241.1/32	SSL no-ins

#### 4.11 DNAT 設定方法（表示形式：インターフェースペアビューの場合）

- ① 左メニューよりポリシー&オブジェクト→バーチャル IP を選択する。



- ② 新規作成を押下する。



名前	インターフェース	マッピング元	マッピング先	ヒット数	参照
mac	<input type="checkbox"/> any	100.1.1.21	172.31.200.3	0	0
192.168.150.1_210.136.56.208	<input type="checkbox"/> any	192.168.150.1 (TCP: 25)	210.136.56.208 (TCP: 25)	0	0

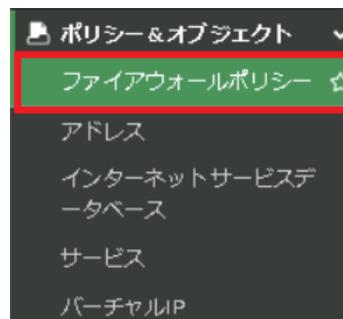
- ③ 名前、外部 IP アドレス/範囲、マップされた IP アドレス/範囲を記載する。

※タイプはスタティック NAT であること

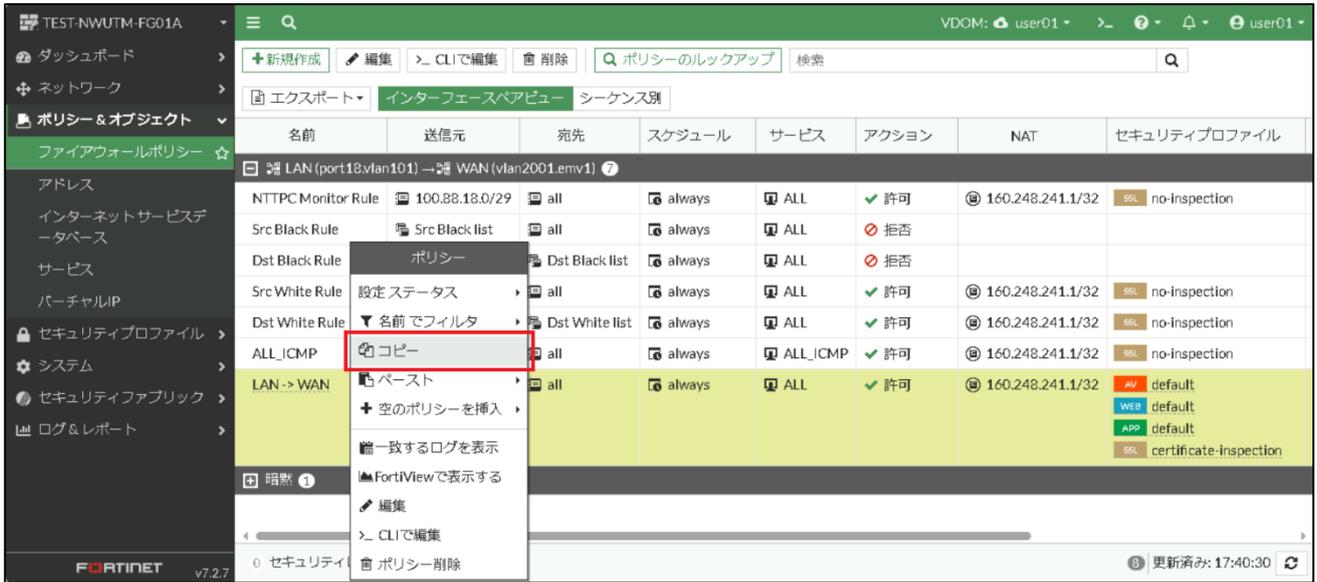
また、ポートフォワードを設定したい場合はポートフォワードのトグルをオンにし、入力を行う。

最後に OK を押して設定を完了する。

- ④ 左メニューよりポリシー&オブジェクト→ファイアウォールポリシーを選択する。



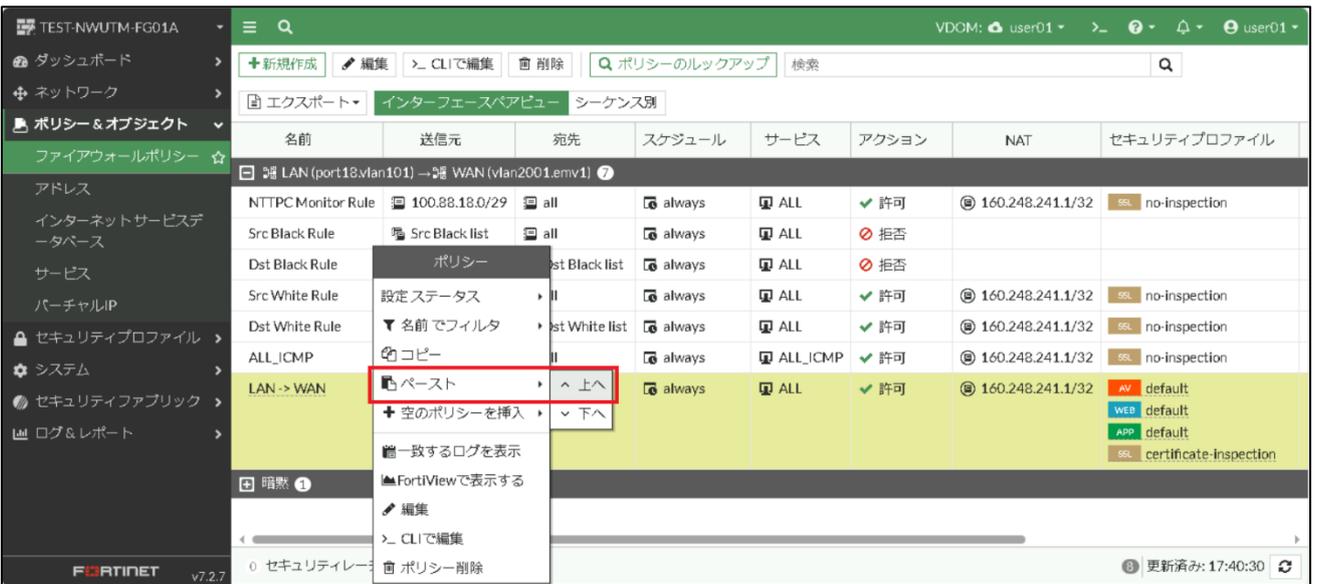
⑤ LAN→WAN を右クリックし、コピーを押下する。



The screenshot shows the Fortinet FortiGate GUI for a device named TEST-NWUTM-FG01A. The left sidebar shows the navigation menu with 'ファイアウォールポリシー' (Firewall Policy) selected. The main area displays a table of firewall policies. The 'LAN -> WAN' policy is highlighted in yellow. A context menu is open over this policy, with the 'コピー' (Copy) option selected and highlighted in red.

名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル
NTTPC Monitor Rule	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	no-inspection
Src Black Rule	Src Black list	all	always	ALL	拒否		
Dst Black Rule	Dst Black list	all	always	ALL	拒否		
Src White Rule		all	always	ALL	許可	160.248.241.1/32	no-inspection
Dst White Rule		all	always	ALL	許可	160.248.241.1/32	no-inspection
ALL_ICMP		all	always	ALL_ICMP	許可	160.248.241.1/32	no-inspection
LAN -> WAN		all	always	ALL	許可	160.248.241.1/32	AV: default WEB: default APP: default SSL: certificate-inspection

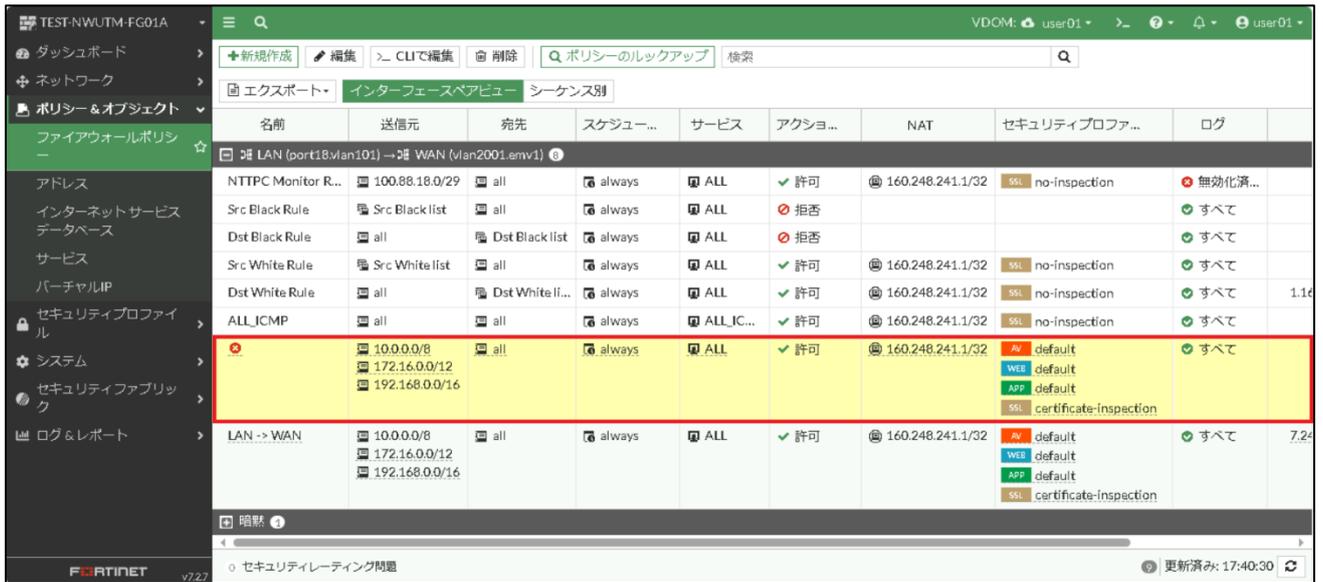
⑥ 再度 LAN→WAN を右クリックし、ペースト→上へを押下する。



The screenshot shows the Fortinet FortiGate GUI for a device named TEST-NWUTM-FG01A. The left sidebar shows the navigation menu with 'ファイアウォールポリシー' (Firewall Policy) selected. The main area displays a table of firewall policies. The 'LAN -> WAN' policy is highlighted in yellow. A context menu is open over this policy, with the 'ペースト' (Paste) and '上へ' (Up) options selected and highlighted in red.

名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル
NTTPC Monitor Rule	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	no-inspection
Src Black Rule	Src Black list	all	always	ALL	拒否		
Dst Black Rule	Dst Black list	all	always	ALL	拒否		
Src White Rule		all	always	ALL	許可	160.248.241.1/32	no-inspection
Dst White Rule		all	always	ALL	許可	160.248.241.1/32	no-inspection
ALL_ICMP		all	always	ALL_ICMP	許可	160.248.241.1/32	no-inspection
LAN -> WAN		all	always	ALL	許可	160.248.241.1/32	AV: default WEB: default APP: default SSL: certificate-inspection

⑦ 作成したポリシーをダブルクリックする。



The screenshot shows the Fortinet Master's ONE interface for a device named 'TEST-NWUTM-FG01A'. The left sidebar contains navigation menus for Dashboard, Network, Policy & Objects, Security Profiles, System, Security Applications, and Logs & Reports. The main area displays a table of security policies under the 'インターフェースペアビュー' (Interface Pair View) tab. The table columns include Name, Source, Destination, Schedule, Service, Action, NAT, Security Profile, and Log. The 'ALL\_ICMP' policy is highlighted with a red border. Below the table, there is a '暗黙' (Implicit) section and a status bar at the bottom indicating a security rating issue and the last update time.

名前	送信元	宛先	スケジュー...	サービス	アクション...	NAT	セキュリティプロファ...	ログ
NTTPC Monitor R...	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	no-inspection	無効化済...
Src Black Rule	Src Black list	all	always	ALL	拒否			すべて
Dst Black Rule	all	Dst Black list	always	ALL	拒否			すべて
Src White Rule	Src White list	all	always	ALL	許可	160.248.241.1/32	no-inspection	すべて
Dst White Rule	all	Dst White li...	always	ALL	許可	160.248.241.1/32	no-inspection	すべて
ALL_ICMP	all	all	always	ALL_IC...	許可	160.248.241.1/32	no-inspection	すべて
	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて
LAN -> WAN	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて

暗黙

セキュリティレーティング問題

更新済み: 17:40:30

- ⑧ 名前、発信インターフェース、着信インターフェース、送信元、宛先（バーチャル IP）、サービス、NAT、セキュリティプロファイル、コメント（任意）を設定し OK を押下する。  
 ※DNAT を使用する場合は宛先を DNAT 用の追加グローバル IP を設定します。  
 ※DNAT の宛先に指定されたサーバがインターネット向けにルーティングされていない場合は有効化してください。

「+」を押下すると右側にリストが表示されるので追加したい分をクリックする。  
 消すアドレスがある場合は「×」をクリックすると消えます。  
 送信元、宛先で追加したいものがない場合は 5.1 項を参照  
 送信元を ALL にした場合、不特定多数のアドレスからアクセスが可能になりますのでご注意ください。  
 インターネットからのアクセスを可能にする場合には、送信元を制限することを推奨します。  
 サービスで追加したいものがない場合は 7.1 項を参照  
 宛先には手順③で作成したバーチャル IP を設定する。

セキュリティプロファイルを有効化したい場合は各セキュリティのトグルをクリックしてください。  
 使用しないセキュリティはトグルをクリックし無効化にしてください。  
 詳細は 13 章を参照

DNAT を使用する場合は必ず無効化(※)

- ⑨ 作成したルールを WAN→LAN 内で投入したい場所に名前部分でドラッグ&ドロップし移動させる。(DNAT が複数行ある場合)

名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト	タイプ
LAN [port18/vlan101] → WAN [vlan2001/Lev1]										
NTTPC Monitor Rule	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	無効化済み	0B	スタンダード
Src Black Rule	Src Black list	all	always	ALL	拒否			すべて	0B	スタンダード
Dst Black Rule	all	Dst Black list	always	ALL	拒否			すべて	0B	スタンダード
Src White Rule	Src White list	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	0B	スタンダード
Dst White Rule	all	Dst White list	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	1.16 MB	スタンダード
ALL_ICMP	all	all	always	ALL_ICMP	許可	160.248.241.1/32	SSL no-inspection	すべて	0B	スタンダード
LAN → WAN	100.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて	9.31 MB	スタンダード
WAN [vlan2001/Lev1] → LAN [port18/vlan101]										
	192.168.1.2/32	100.0.0.2/32	always	ALL	許可	無効化済み	AV default WEB default APP default SSL certificate-inspection	すべて	0B	スタンダード
DNAT	192.168.1.2/32	100.0.0.2/32	always	ALL	許可	無効化済み	AV default WEB default APP default SSL certificate-inspection	すべて	0B	スタンダード

- ⑩ 対象のルールを右クリックし設定ステータス→有効を押下する。

名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト	タイプ
LAN [port18/vlan101] → WAN [vlan2001/Lev1]										
NTTPC Monitor Rule	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	無効化済み	0B	スタンダード
Src Black Rule	Src Black list	all	always	ALL	拒否			すべて	0B	スタンダード
Dst Black Rule	all	Dst Black list	always	ALL	拒否			すべて	0B	スタンダード
Src White Rule	Src White list	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	0B	スタンダード
Dst White Rule	all	Dst White list	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	1.16 MB	スタンダード
ALL_ICMP	all	all	always	ALL_ICMP	許可	160.248.241.1/32	SSL no-inspection	すべて	0B	スタンダード
LAN → WAN	100.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて	9.31 MB	スタンダード
WAN [vlan2001/Lev1] → LAN [port18/vlan101]										
DNAT	192.168.1.2/32	100.0.0.2/32	always	ALL	許可	無効化済み	AV default WEB default APP default SSL certificate-inspection	すべて	0B	スタンダード
	100.0.0.2/32	all	always	ALL	許可	無効化済み	AV default WEB default APP default SSL certificate-inspection	すべて	0B	スタンダード

⑪ ルールが有効になったことを確認する。

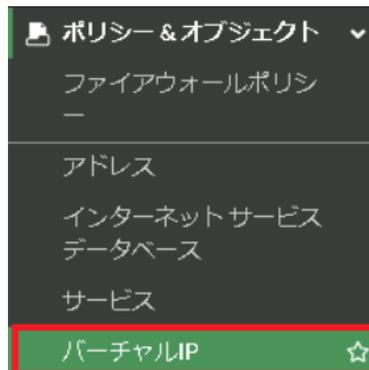
名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト	タイプ
LAN (port1&vlan101) → WAN (vlan2001emv1)										
NTTFC Monitor Rule	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	無効化済み	0B	スタンダード
Src Black Rule	Src Black list	all	always	ALL	拒否			すべて	0B	スタンダード
Dst Black Rule	all	Dst Black list	always	ALL	拒否			すべて	0B	スタンダード
Src White Rule	Src White list	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	0B	スタンダード
Dst White Rule	all	all	always	ALL	許可	160.248.241.1/32	SSL no-inspection	すべて	1.16 MB	スタンダード
ALL_ICMP	all	all	always	ALL_ICMP	許可	160.248.241.1/32	SSL no-inspection	すべて	0B	スタンダード
LAN → WAN	10.0.0.0/24 172.16.0.0/24 192.168.0.0/24	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて	9.31 MB	スタンダード
WAN (vlan2001emv1) → LAN (port1&vlan101)										
DNAT	192.168.1.2/32	100.0.0.2/32	always	ALL	許可	無効化済み	AV default WEB default APP default SSL certificate-inspection	すべて	0B	スタンダード
	192.168.1.2/32	100.0.0.2/32	always	ALL	許可	無効化済み	AV default WEB default APP default SSL certificate-inspection	すべて	0B	スタンダード

×が消えていれば有効化されている

変更が保存されました。 [再読み込み](#) ×

4.12 DNAT 設定方法（表示形式：シーケンス別の場合）

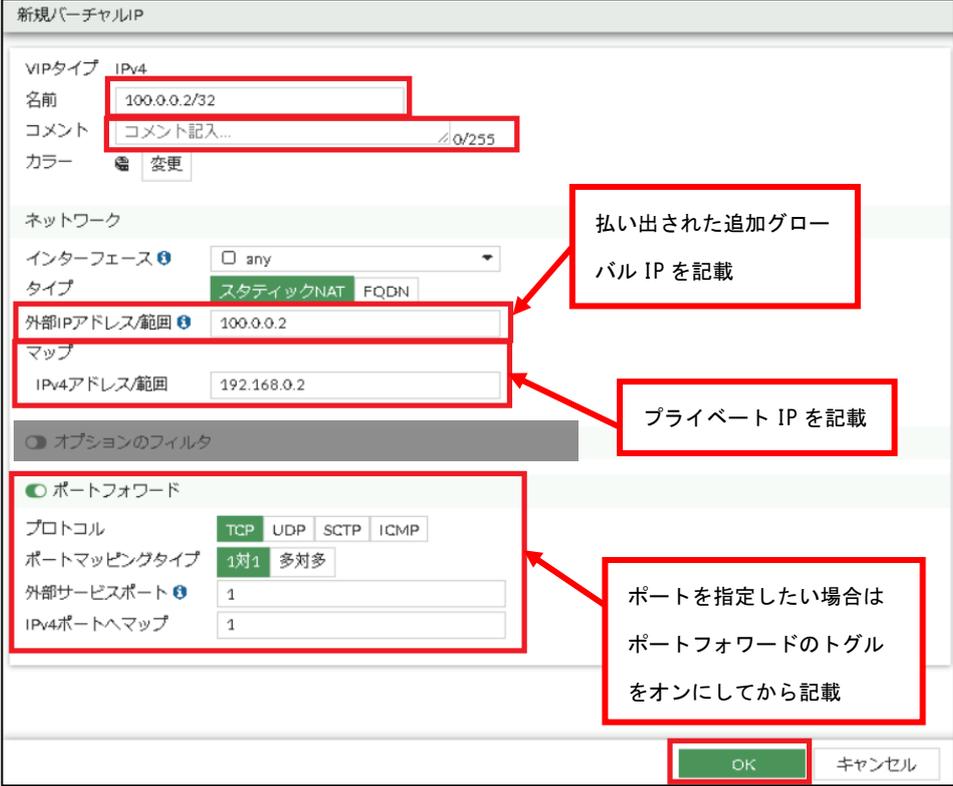
① 左メニューよりポリシー&オブジェクト→バーチャル IP を選択する。



② 新規作成を押下する。

名前	インターフェース	マッピング元	マッピング先	ヒット数	参照
mac	<input type="checkbox"/> any	100.11.21	172.31.200.3	0	0
192.168.150.1_210.136.56.208	<input type="checkbox"/> any	192.168.150.1 (TCP: 25)	210.136.56.208 (TCP: 25)	0	0

- ③ 名前、外部 IP アドレス/範囲、マップされた IP アドレス/範囲を記載して OK を押下する。  
 ※タイプはスタティック NAT であること  
 また、ポートフォワードを設定したい場合はポートフォワードのトグルをオンにし、入力を行う。  
 最後に OK を押して設定を完了する。



The screenshot shows the '新規バーチャルIP' (New Virtual IP) configuration window. Red boxes and arrows highlight specific fields with explanatory text:

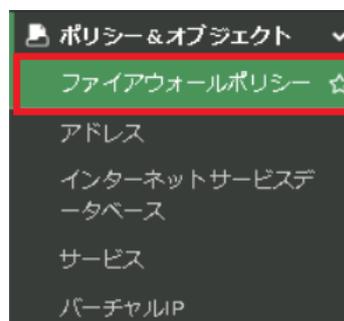
- 名前 (Name):** 100.0.0.2/32
- コメント (Comment):** コメント記入... /0/255
- ネットワーク (Network):**
  - インターフェース (Interface): any
  - タイプ (Type): **スタティックNAT** (Static NAT)
- 外部IPアドレス/範囲 (External IP Address/Range):** 100.0.0.2
- マップ (Map):**
  - IPv4アドレス/範囲 (IPv4 Address/Range): 192.168.0.2
- オプションのフィルタ (Option Filter):**
  - ポートフォワード (Port Forward):** On
  - プロトコル (Protocol): TCP, UDP, SCTP, ICMP
  - ポートマッピングタイプ (Port Mapping Type): 1対1, 多対多
  - 外部サービスポート (External Service Port): 1
  - IPv4ポートへマップ (Map to IPv4 Port): 1

Annotations:

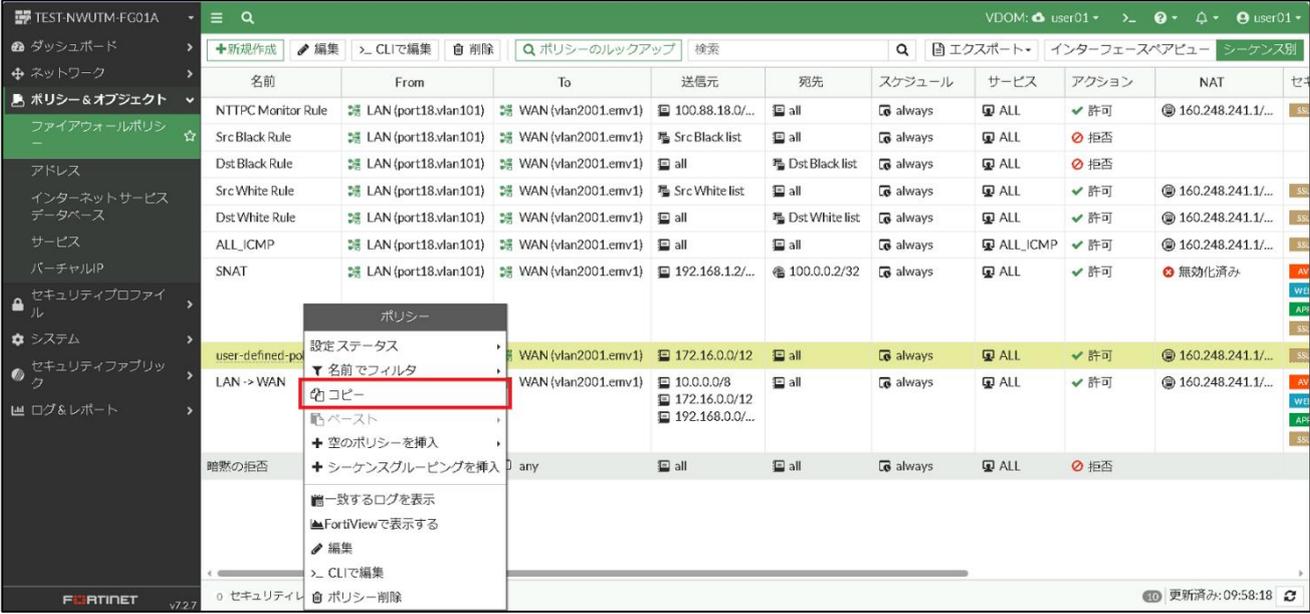
- 払い出された追加グローバル IP を記載 (Record the additional global IP issued)
- プライベート IP を記載 (Record private IP)
- ポートを指定したい場合はポートフォワードのトグルをオンにしてから記載 (If you want to specify a port, turn on the port forward toggle before recording)

Buttons: OK, キャンセル (Cancel)

- ④ 左メニューよりポリシー&オブジェクト→ファイアウォールポリシーを選択する。



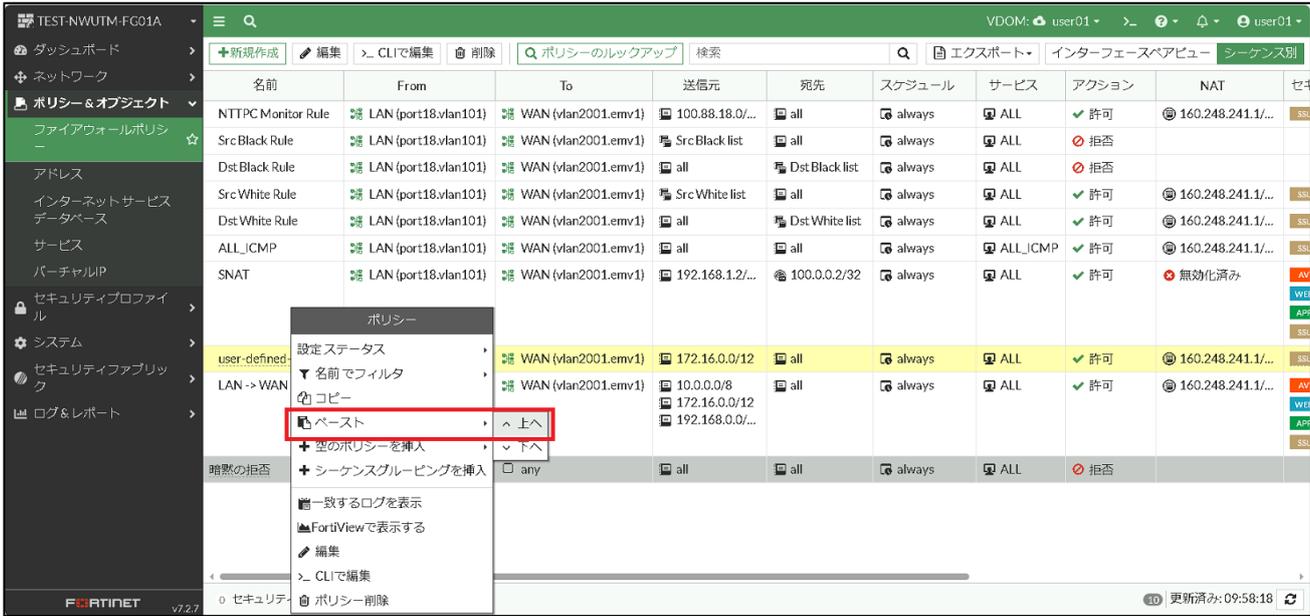
⑤ user-defined-policy-1 を右クリックし、コピーを押下する。



The screenshot shows the Fortinet FortiGate GUI with a table of policies. The 'user-defined-policy-1' row is selected, and a context menu is open over it. The 'コピー' (Copy) option is highlighted in red.

名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セ
NTTPC Monitor Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	100.88.18.0/...	all	always	ALL	許可	160.248.241.1/...	SS
Src Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src Black list	all	always	ALL	拒否		
Dst Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst Black list	always	ALL	拒否		
Src White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src White list	all	always	ALL	許可	160.248.241.1/...	SS
Dst White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst White list	always	ALL	許可	160.248.241.1/...	SS
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/...	SS
SNAT	LAN (port18.vlan101)	WAN (vlan2001.emv1)	192.168.1.2/...	100.0.0.2/32	always	ALL	許可	無効化済み	AV
user-defined-policy-1	LAN (port18.vlan101)	WAN (vlan2001.emv1)	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/...	SS
LAN -> WAN	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8	172.16.0.0/12	192.168.0.0/...	all	許可	160.248.241.1/...	AV
暗黙の拒否		any		all	always	ALL	拒否		

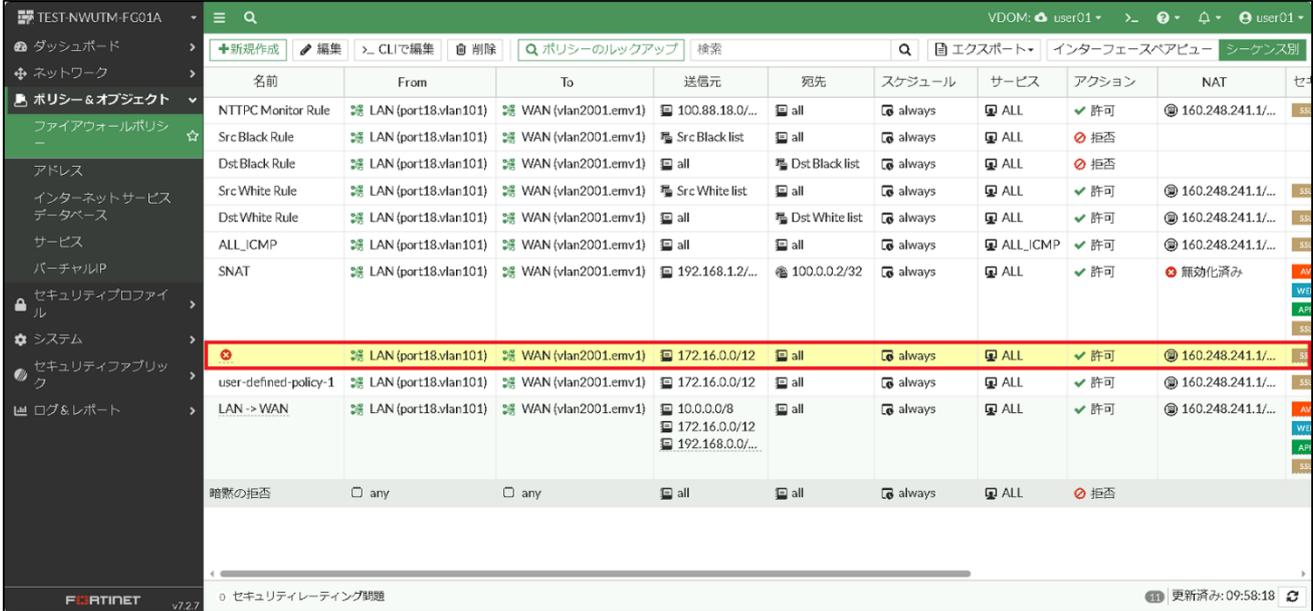
⑥ 再度 user-defined-policy-1 を右クリックし、ペースト→上へを押下する。



The screenshot shows the same Fortinet FortiGate GUI. The 'user-defined-policy-1' row is selected, and a context menu is open over it. The 'ペースト→上へ' (Paste to top) option is highlighted in red.

名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セ
NTTPC Monitor Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	100.88.18.0/...	all	always	ALL	許可	160.248.241.1/...	SS
Src Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src Black list	all	always	ALL	拒否		
Dst Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst Black list	always	ALL	拒否		
Src White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src White list	all	always	ALL	許可	160.248.241.1/...	SS
Dst White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst White list	always	ALL	許可	160.248.241.1/...	SS
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/...	SS
SNAT	LAN (port18.vlan101)	WAN (vlan2001.emv1)	192.168.1.2/...	100.0.0.2/32	always	ALL	許可	無効化済み	AV
user-defined-policy-1	LAN (port18.vlan101)	WAN (vlan2001.emv1)	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/...	SS
LAN -> WAN	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8	172.16.0.0/12	192.168.0.0/...	all	許可	160.248.241.1/...	AV
暗黙の拒否		any		all	always	ALL	拒否		

⑦ 作成したポリシーをダブルクリックする。



The screenshot shows the Fortinet FortiGate GUI with the 'Policy & Object' section selected. A table of firewall policies is displayed, with the 'user-defined-policy-1' row highlighted in red. The table columns include Name, From, To, Source, Destination, Schedule, Service, Action, and NAT.

名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT
NTTPC Monitor Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	100.88.18.0/...	all	always	ALL	許可	@ 160.248.241.1/...
Src Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src Black list	all	always	ALL	拒否	
Dst Black Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst Black list	always	ALL	拒否	
Src White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	Src White list	all	always	ALL	許可	@ 160.248.241.1/...
Dst White Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	Dst White list	always	ALL	許可	@ 160.248.241.1/...
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	@ 160.248.241.1/...
SNAT	LAN (port18.vlan101)	WAN (vlan2001.emv1)	192.168.1.2/...	100.0.0.2/32	always	ALL	許可	無効化済み
	LAN (port18.vlan101)	WAN (vlan2001.emv1)	172.16.0.0/12	all	always	ALL	許可	@ 160.248.241.1/...
user-defined-policy-1	LAN (port18.vlan101)	WAN (vlan2001.emv1)	172.16.0.0/12	all	always	ALL	許可	@ 160.248.241.1/...
LAN -> WAN	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/...	all	always	ALL	許可	@ 160.248.241.1/...
暗黙の拒否	<input type="checkbox"/> any	<input type="checkbox"/> any	all	all	always	ALL	拒否	

- ⑧ 名前、送信元、宛先（バーチャル IP）、サービス、NAT、セキュリティプロファイル、コメント（任意）を設定し OK を押下する。

※DNAT を使用する場合は宛先を DNAT 用の追加グローバル IP を設定します。

※DNAT の宛先に指定されたサーバがインターネット向けにルーティングされていない場合は有効化してください。

ポリシーの編集

名前

タイプ

着信インターフェース

発信インターフェース

送信元

IP/MACベースアクセスコントロール

宛先

スケジュール

サービス

アクション  許可  拒否

インスペクションモード

ファイアウォール/ネットワークオプション

NAT  DNAT を使用する場合は必ず無効化(※)

プロトコルオプション

セキュリティプロファイル

アンチウイルス

Webフィルタ

ビデオフィルタ

アプリケーションコントロール  APP default

IPS

Eメールフィルタ

SSLインスペクション

ロギングオプション

許可トラフィックをログ  セキュリティイベント

セッション開始時にログを生成

コメント  53/1023

このポリシーを有効化

OK キャンセル

「+」を押下すると右側にリストが表示されるので追加したい分をクリックする。  
 消すアドレスがある場合は「×」をクリックすると消えます。  
 送信元、宛先に追加したいものがない場合は 5.1 項を参照  
 送信元を ALL にした場合、不特定多数のアドレスからアクセスが可能になりますのでご注意ください。  
 インターネットからのアクセスを可能にする場合には、送信元を制限することを推奨します。  
 サービスで追加したいものがない場合は 7.1 項を参照  
 宛先には手順③で作成したバーチャル IP を設定する。

セキュリティプロファイルを有効化したい場合は各セキュリティのトグルをクリックしてください。  
 使用しないセキュリティはトグルをクリックし無効化にしてください。  
 詳細は 13 章を参照

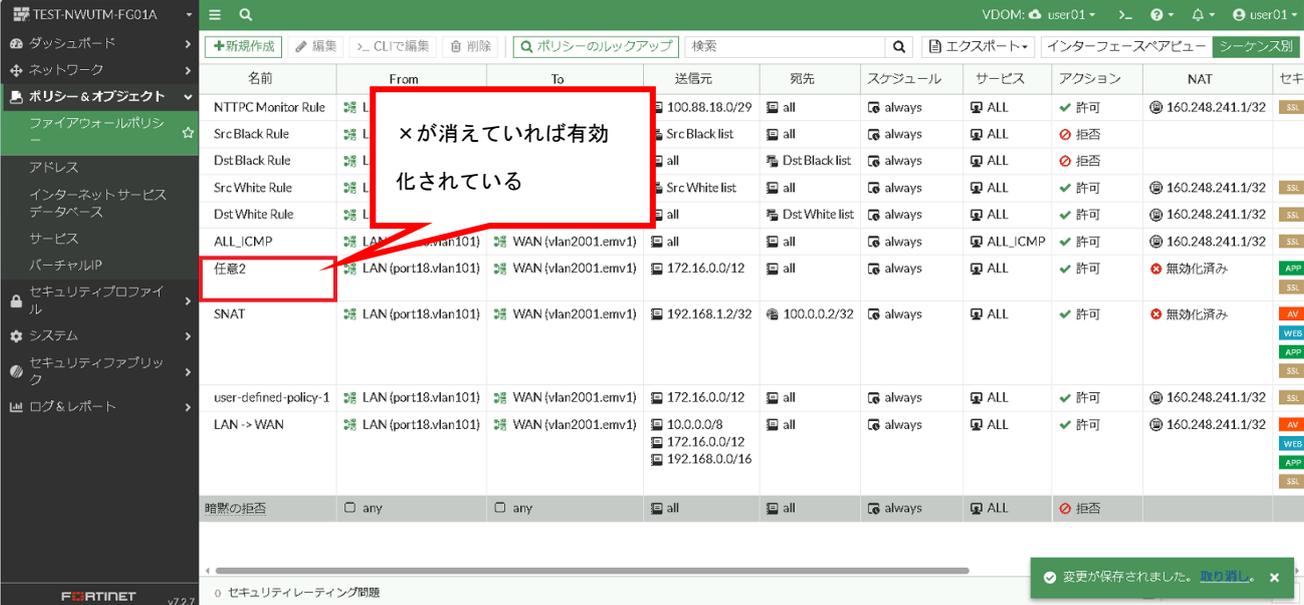
⑨ 作成したルールを ALL\_ICMP より下、SNAT より上の投入したい場所に名前部分でドラッグ&ドロップし移動させる。

名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セキ
NTTPC Monitor Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	SSL
SrcBlack Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	SrcBlack list	all	always	ALL	拒否		
DstBlack Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	DstBlack list	always	ALL	拒否		
SrcWhite Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	SrcWhite list	all	always	ALL	許可	160.248.241.1/32	SSL
DstWhite Rule	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	DstWhite list	always	ALL	許可	160.248.241.1/32	SSL
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/32	SSL
SNAT	LAN (port18.vlan101)	WAN (vlan2001.emv1)	192.168.1.2/32	100.0.0.2/32	always	ALL	許可	無効化済み	AV, WEB, APP, SSL
任意2	LAN (port18.vlan101)	WAN (vlan2001.emv1)	172.16.0.0/12	all	always	ALL	許可	無効化済み	APP, SSL
user-defined-policy-1	LAN (port18.vlan101)	WAN (vlan2001.emv1)	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32	SSL
LAN -> WAN	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV, WEB, APP, SSL
暗黙の拒否	any	any	all	all	always	ALL	拒否		

⑩ 対象のルールを右クリックし設定ステータス→有効を押下する。

The screenshot shows the Fortinet FortiGate GUI. A right-click context menu is open over the '任意2' rule. The menu items include: 名前 フィルタ, コピー, ペースト, 空のポリシーを挿入, 反転してクローン, シーケンスグループリングを挿入, 一致するログを表示, FortiViewで表示する, 編集, CLIで編集, and ポリシー削除. The '設定ステータス' (Set Status) option is highlighted, and its sub-menu is open, showing '有効' (Enabled) as the selected option.

## ⑪ ルールが有効になったことを確認する。



The screenshot shows the Fortinet Firewall Policy configuration interface. A table lists various policies, and the '任意2' rule is highlighted with a red box. A callout box with a red border contains the text: "×が消えていれば有効化されている" (If the 'x' disappears, it means the rule is activated).

名前	From	To	送信元	宛先	スケジュール	サービス	アクション	NAT	セキ
NTTPC Monitor Rule			100.88.18.0/29	all	always	ALL	許可	160.248.241.1/32	SSL
Src Black Rule			Src Black list	all	always	ALL	拒否		
Dst Black Rule			all	Dst Black list	always	ALL	拒否		
Src White Rule			Src White list	all	always	ALL	許可	160.248.241.1/32	SSL
Dst White Rule			all	Dst White list	always	ALL	許可	160.248.241.1/32	SSL
ALL_ICMP	LAN (port18.vlan101)	WAN (vlan2001.emv1)	all	all	always	ALL_ICMP	許可	160.248.241.1/32	SSL
任意2	LAN (port18.vlan101)	WAN (vlan2001.emv1)	172.16.0.0/12	all	always	ALL	許可	無効化済み	APP
SNAT	LAN (port18.vlan101)	WAN (vlan2001.emv1)	192.168.1.2/32	100.0.0.2/32	always	ALL	許可	無効化済み	AV
user-defined-policy-1	LAN (port18.vlan101)	WAN (vlan2001.emv1)	172.16.0.0/12	all	always	ALL	許可	160.248.241.1/32	SSL
LAN -> WAN	LAN (port18.vlan101)	WAN (vlan2001.emv1)	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV WEB APP SSL
暗黙の拒否	<input type="checkbox"/> any	<input type="checkbox"/> any	all	all	always	ALL	拒否		

0 セキュリティレーティング問題

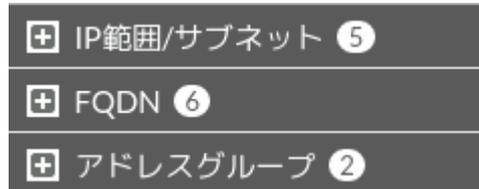
変更が保存されました。 [強制終了](#)

## 5 アドレスの設定方法

本章では、ホワイトリスト、ブラックリスト、ファイアウォールルールの送信元、宛先などに設定するアドレスについて解説しています。

項目として下記3項目ありますが、IP範囲/サブネット、FQDNの2項目が対象となります。

※「+」を押下すると一覧が表示されます。

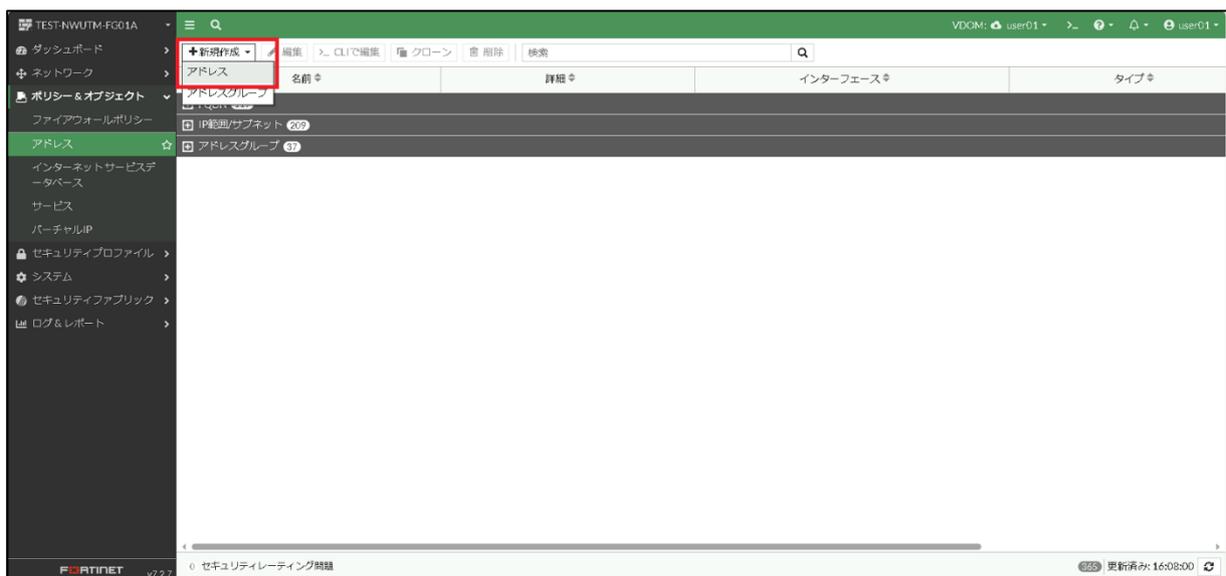


### 5.1 アドレスの追加

- ① 左のメニューからポリシー&オブジェクト->アドレスを選択する。



- ② 新規作成->アドレスを押下する。



③ 名前を記載しタイプにて使用するタイプを選択する。

※タイプについては、サブネット、FQDN を使用すること

I. サブネットの場合は、IP/ネットマスクを記載して OK を押下する。

例：140.227.17.254/32 を追加する場合

名前：140.227.17.254

タイプ：サブネット

IP/ネットマスク：140.227.17.254/32

新規アドレス

名前	<input type="text" value="140.227.17.254/32"/>
カラー	<input type="button" value="変更"/>
タイプ	<input type="text" value="サブネット"/>
IP/ネットマスク	<input type="text" value="140.227.17.254/32"/>
インターフェース	<input type="text" value="any"/>
スタティックルート設定	<input checked="" type="checkbox"/>
コメント	<input type="text" value="コメント記入..."/> 0/255

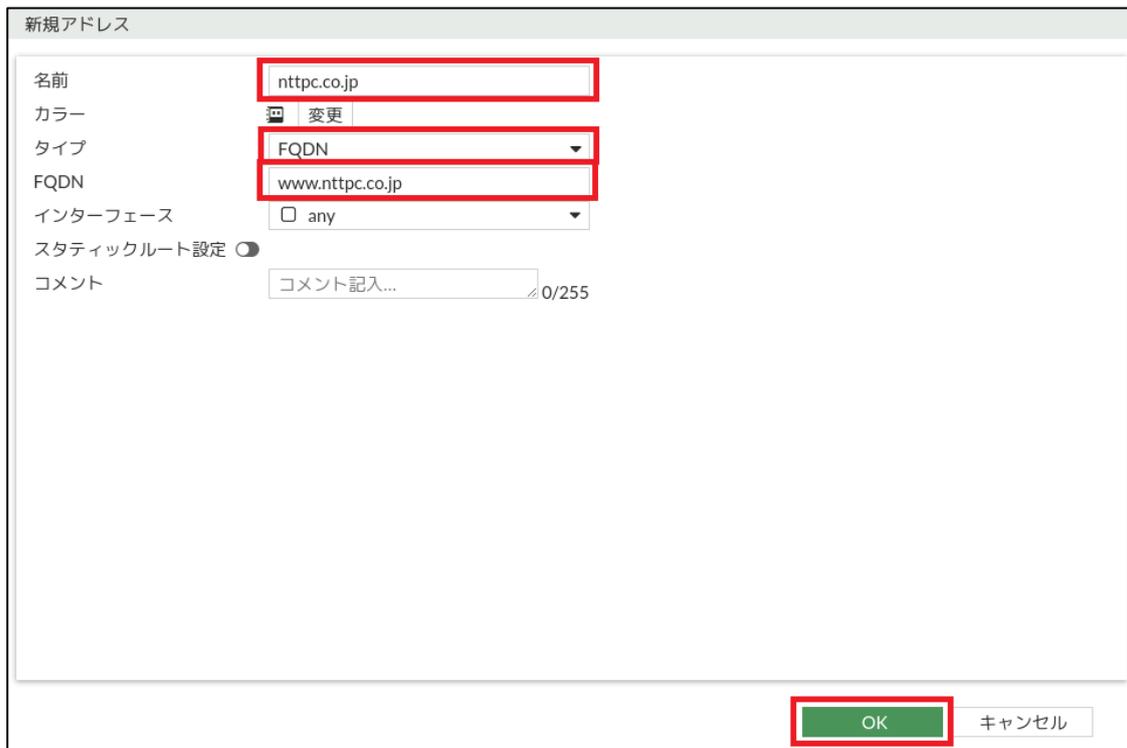
II. FQDN の場合は、FQDN を記載して OK を押下する。

例 : https://www.nttpc.co.jp を追加する場合

名前 : nttpc.co.jp

タイプ : FQDN

FQDN : www.nttpc.co.jp

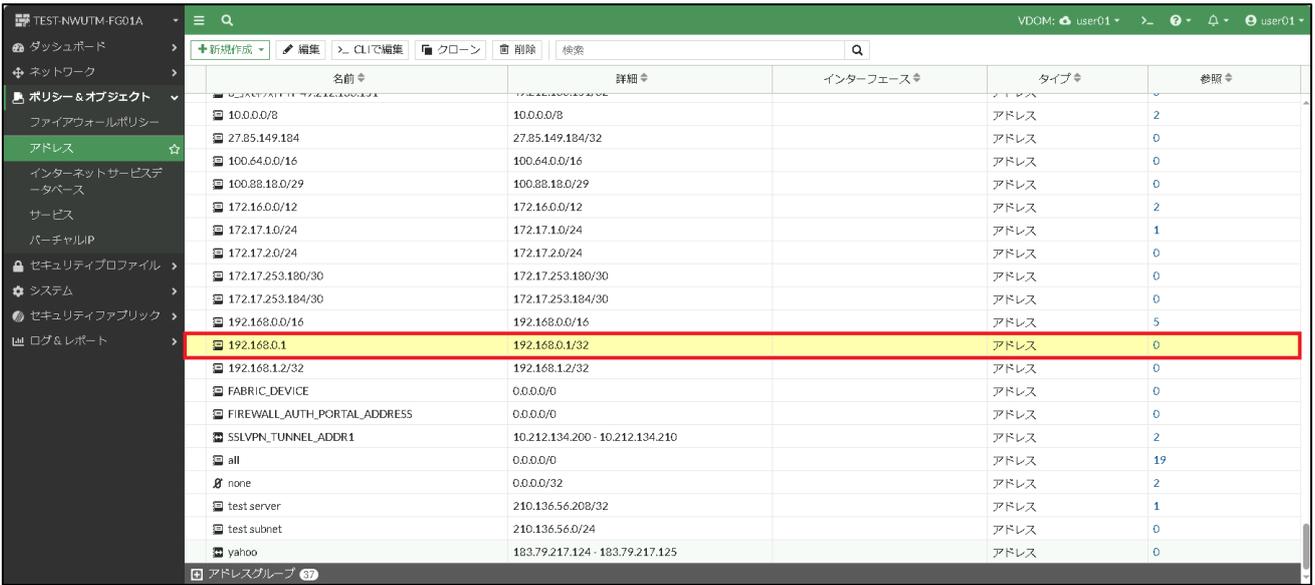


## 5.2 アドレスの変更

① 左のメニューからポリシー&オブジェクト->アドレスを選択する。



② 変更対象のアドレスをダブルクリックする。



名前	詳細	インターフェース	タイプ	参照
10.0.0/8	10.0.0/8		アドレス	2
27.85.149.184	27.85.149.184/32		アドレス	0
100.64.0/16	100.64.0/16		アドレス	0
100.88.18.0/29	100.88.18.0/29		アドレス	0
172.16.0/12	172.16.0/12		アドレス	2
172.17.1.0/24	172.17.1.0/24		アドレス	1
172.17.2.0/24	172.17.2.0/24		アドレス	0
172.17.253.180/30	172.17.253.180/30		アドレス	0
172.17.253.184/30	172.17.253.184/30		アドレス	0
192.168.0/16	192.168.0/16		アドレス	5
192.168.0.1	192.168.0.1/32		アドレス	0
192.168.1.2/32	192.168.1.2/32		アドレス	0
FABRIC_DEVICE	0.0.0/0		アドレス	0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0/0		アドレス	0
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210		アドレス	2
all	0.0.0/0		アドレス	19
none	0.0.0/32		アドレス	2
test server	210.136.56.208/32		アドレス	1
test subnet	210.136.56.0/24		アドレス	0
yahoo	183.79.217.124 - 183.79.217.125		アドレス	0

③ 変更箇所の変更をして OK を押下する。

アドレスの編集

名前

カラー

タイプ

IP/ネットマスク

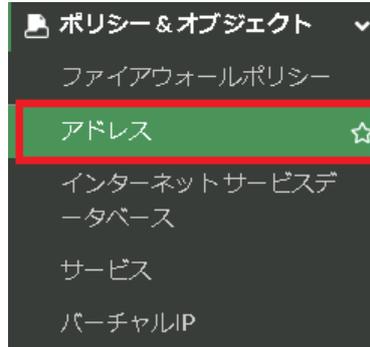
インターフェース

スタティックルート設定

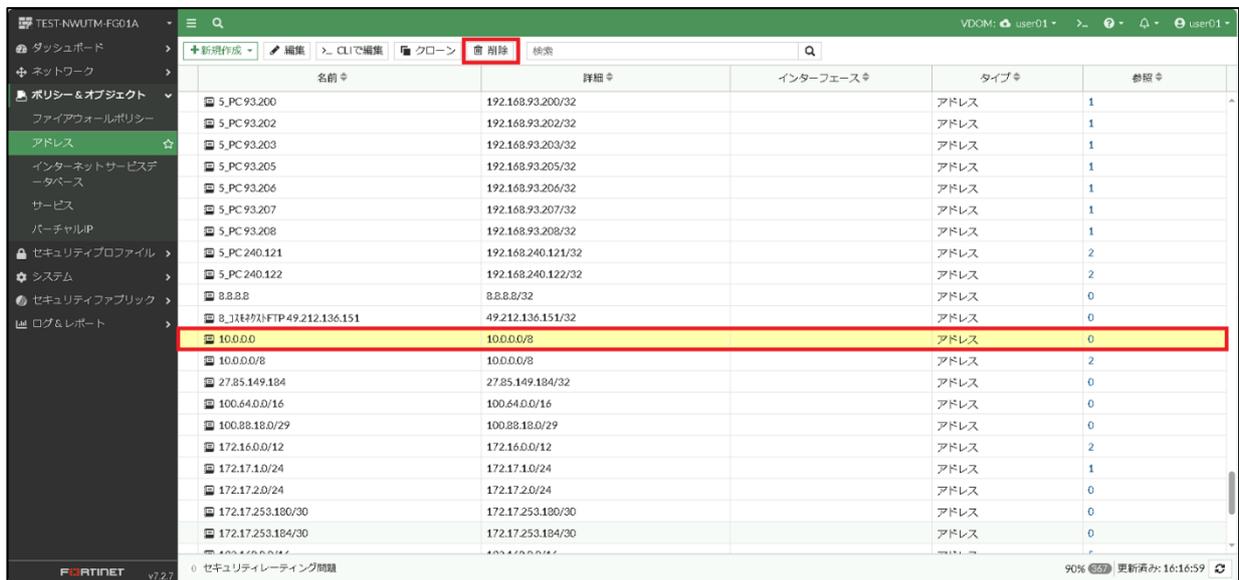
コメント  0/255

### 5.3 アドレスの削除

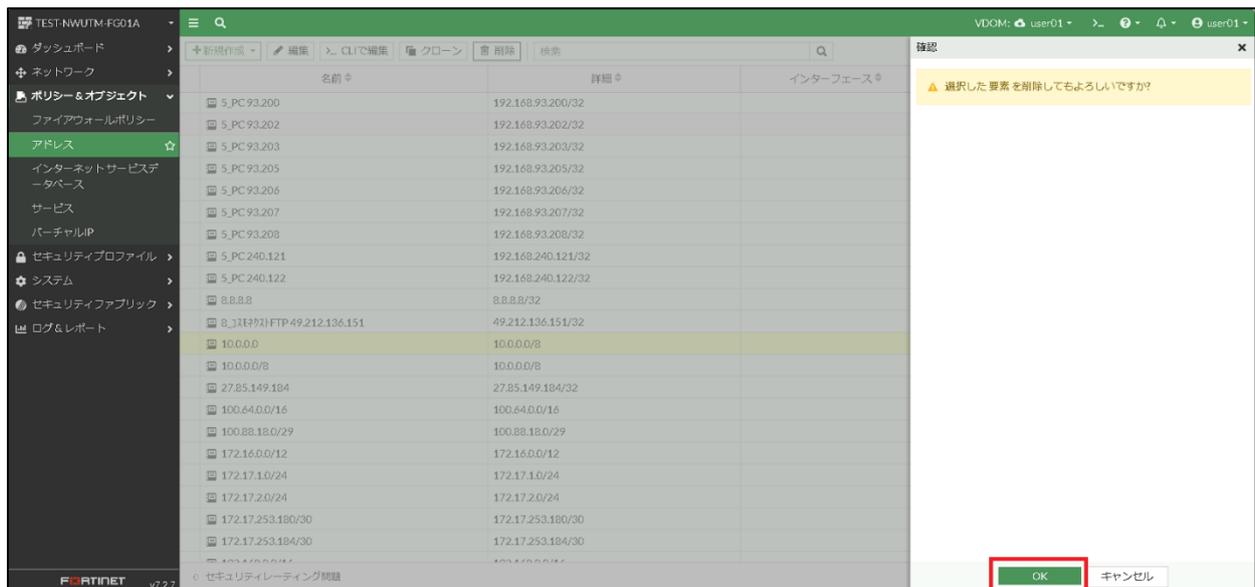
- ① 左のメニューからポリシー&オブジェクト->アドレスを選択



- ② 削除したいアドレスをクリックし、削除をクリックする。



- ③ 確認ウィンドウがでるので、OK をクリックします。

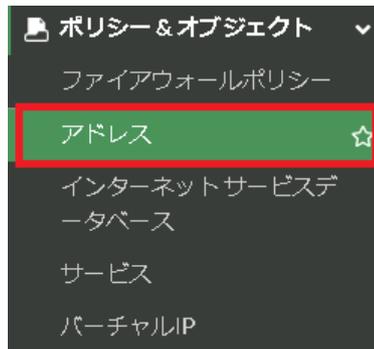


## 6 アドレスグループの設定方法

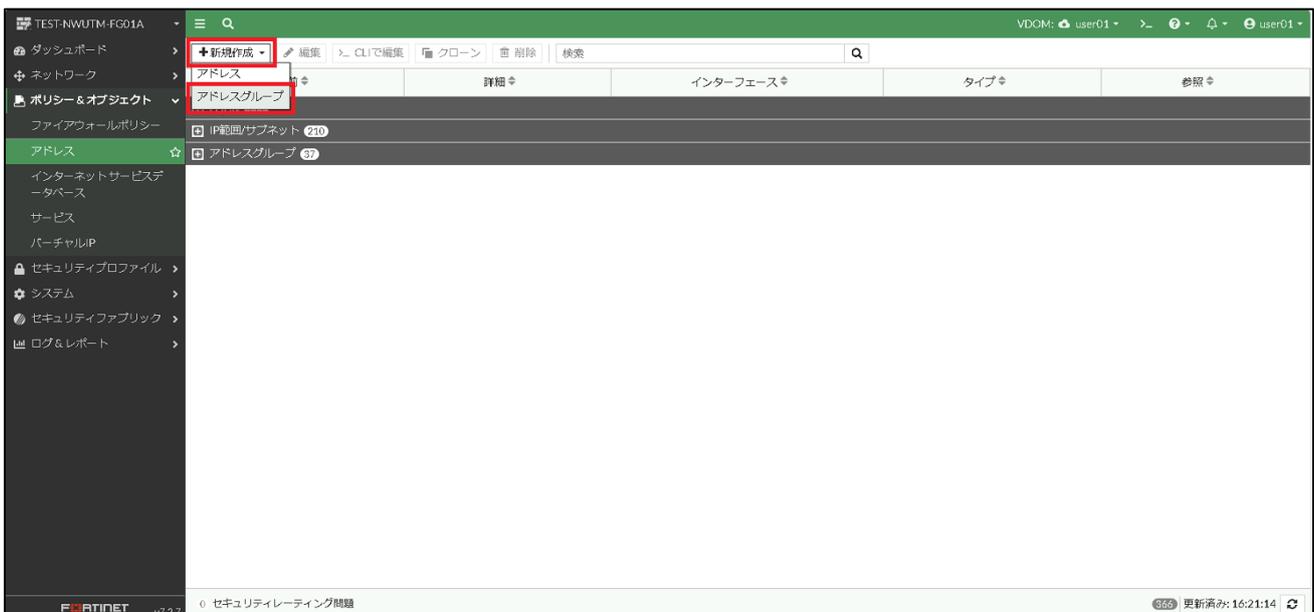
本章では、5章で作成したアドレスをグルーピングする方法、ホワイトリスト、ブラックリストへの設定方法などを解説しています。

### 6.1 アドレスグループの追加

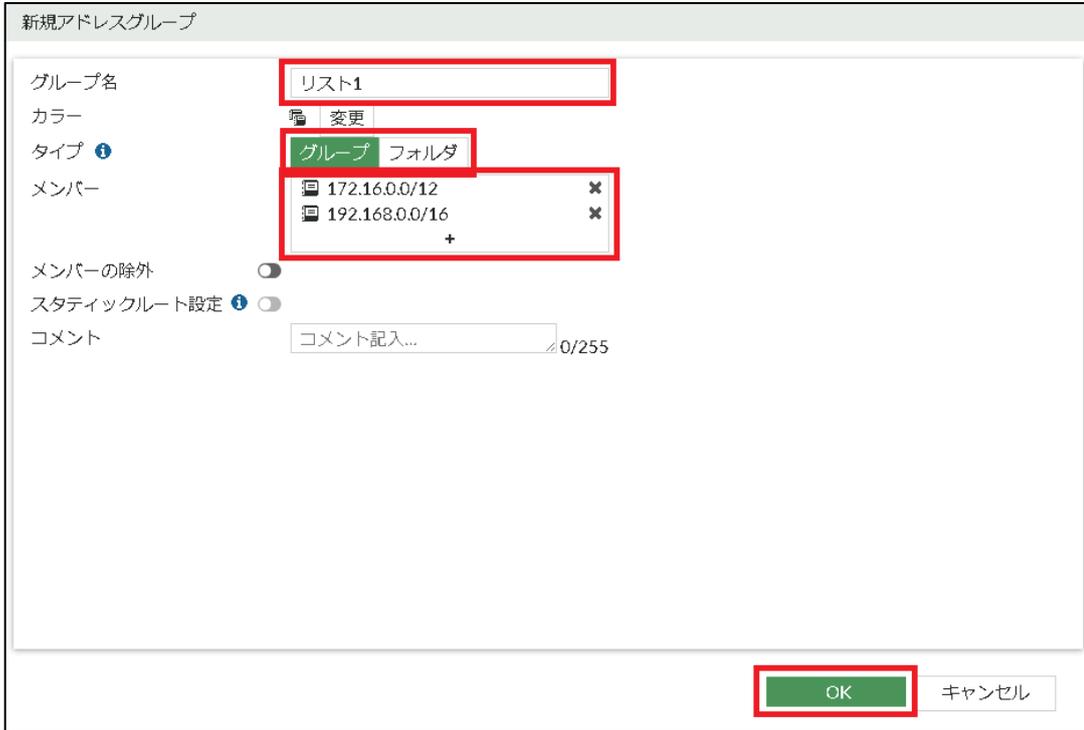
- ① 左のメニューからポリシー&オブジェクト->アドレスを選択する。



- ② 新規作成をクリックし、アドレスグループをクリックします。



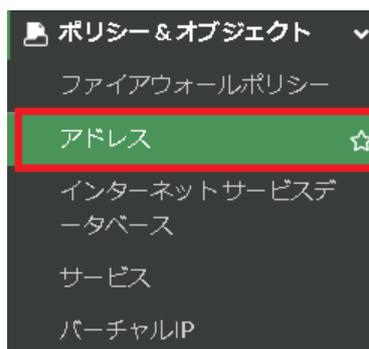
- ③ グループ名を記載、タイプをグループ、メンバーの+を押下して設定する分アドレスをクリックし、OK を押下します。



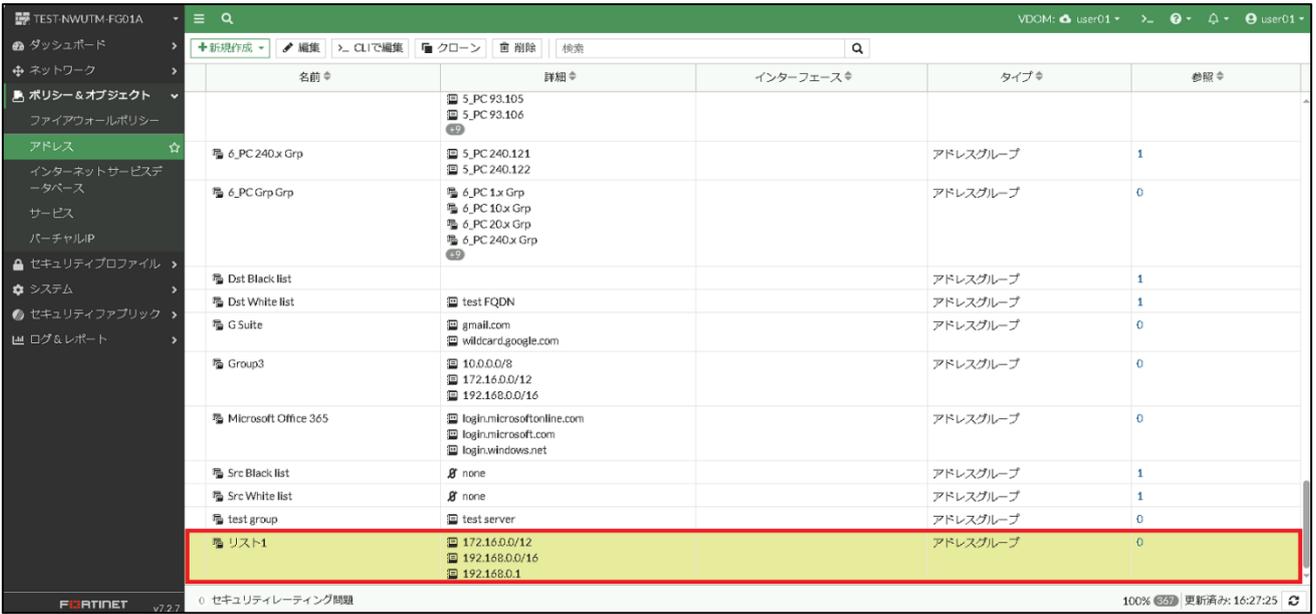
例：172.16.0.0/12 と 192.168.0.0/16 のようなセグメントが違うアドレスをメンバーに設定することにより1グループとして利用することが可能となります。  
※メンバーは5.2項で登録したアドレスを使用します。

## 6.2 アドレスグループの変更

- ① 左のメニューからポリシー&オブジェクト->アドレスを選択

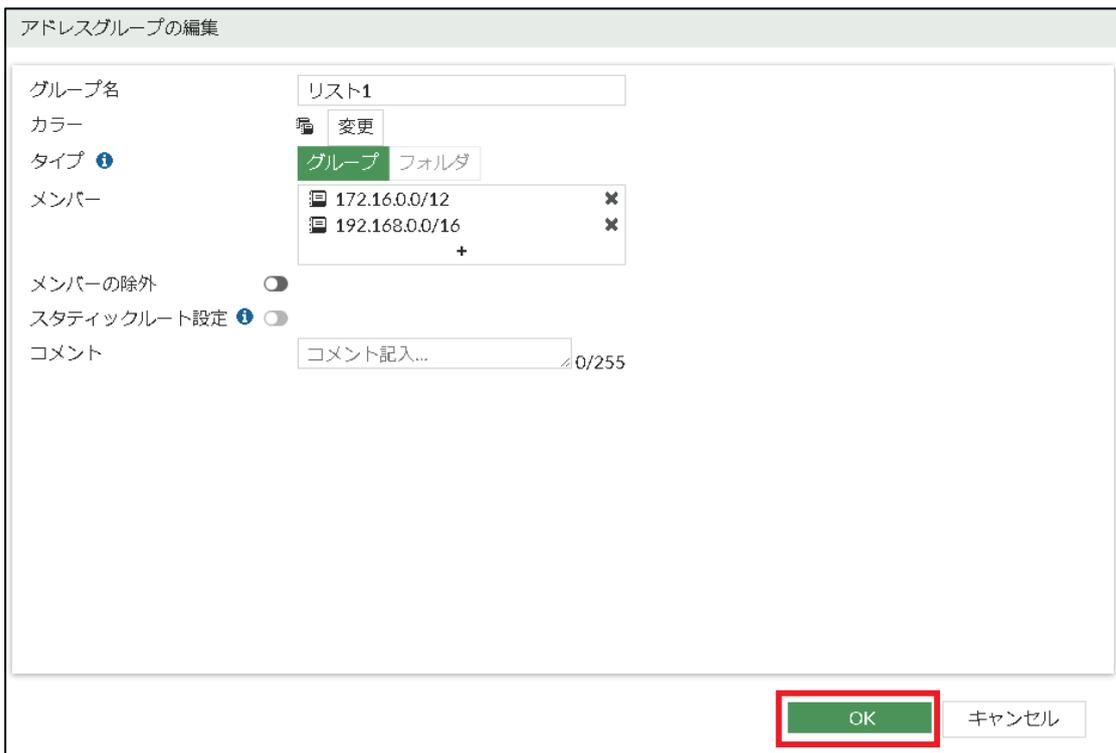


② 変更したいアドレスグループをダブルクリックします。



名前	詳細	インターフェース	タイプ	参照
	5_PC 93.105 5_PC 93.106			
6_PC 240x Grp	5_PC 240.121 5_PC 240.122		アドレスグループ	1
6_PC Grp Grp	6_PC 1x Grp 6_PC 10x Grp 6_PC 20x Grp 6_PC 240x Grp		アドレスグループ	0
Dst Black list			アドレスグループ	1
Dst White list	test FQDN		アドレスグループ	1
G Suite	gmail.com wildcard.google.com		アドレスグループ	0
Group3	10.0.0/8 172.16.0/12 192.168.0/16		アドレスグループ	0
Microsoft Office 365	login.microsoftonline.com login.microsoft.com login.windows.net		アドレスグループ	0
Src Black list	none		アドレスグループ	1
Src White list	none		アドレスグループ	1
test group	test server		アドレスグループ	0
リスト1	172.16.0/12 192.168.0/16 192.168.0.1		アドレスグループ	0

③ 変更したいメンバーを変更し、OK クリックします。



アドレスグループの編集

グループ名: リスト1

カラー: 変更

タイプ: **グループ** フォルダ

メンバー:
 

- 172.16.0/12
- 192.168.0/16
- +

メンバーの除外:

スタティックルート設定:

コメント: コメント記入... /0/255

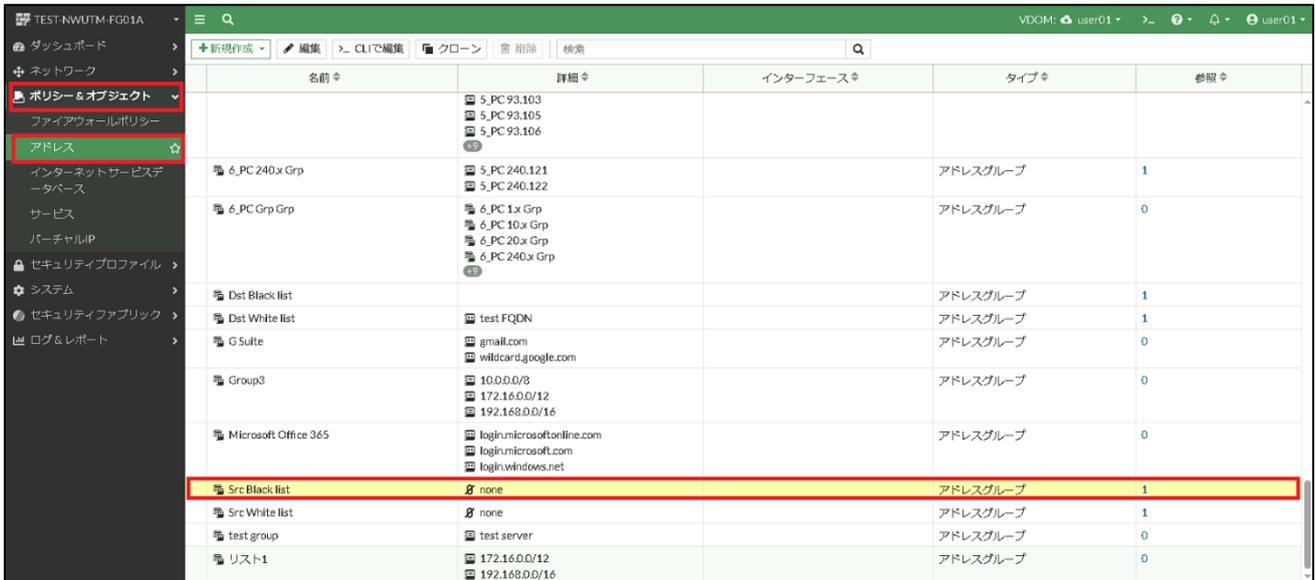
OK キャンセル

### 6.3 ホワイトリスト・ブラックリストへの設定

#### ① Src Black list への設定方法

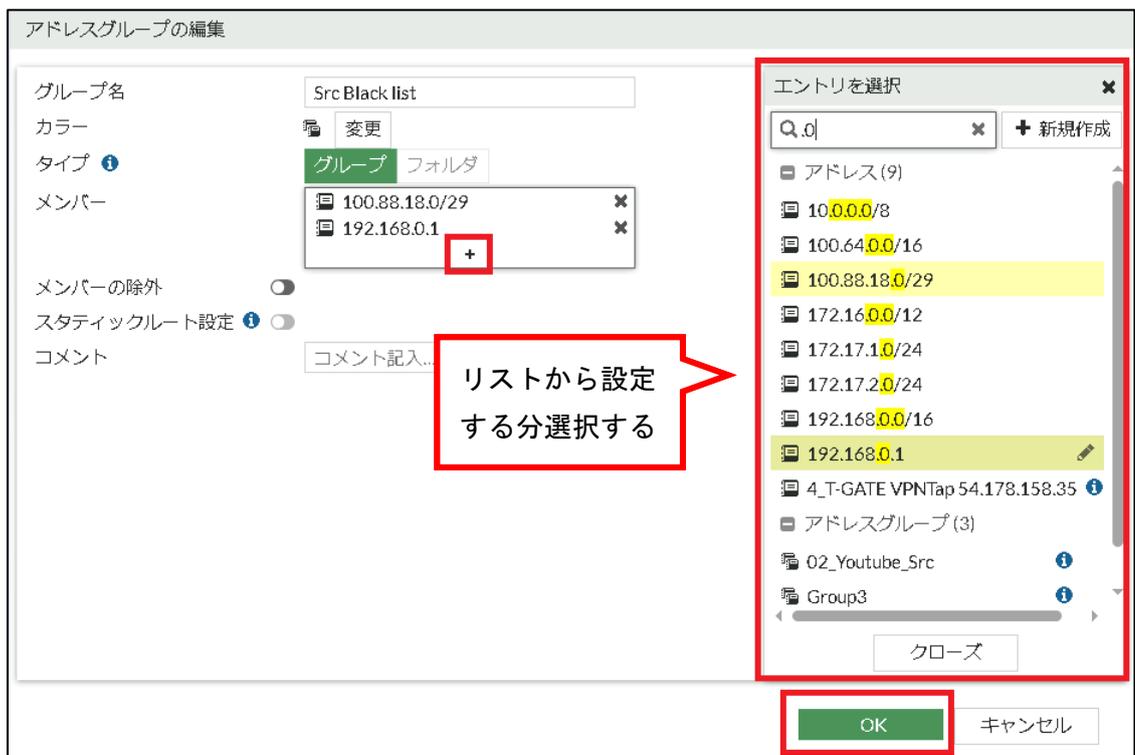
※業務上どこにも通信させたくないクライアント端末などを設定するリストになります。

- I. 左メニューより、ポリシー&オブジェクト→アドレスを選択し、アドレスグループにある Src Black list をダブルクリックする。



名前	詳細	インターフェース	タイプ	参照
6_PC 240x Grp	5_PC 93.103 5_PC 93.105 5_PC 93.106		アドレスグループ	1
6_PC Grp Grp	6_PC 1x Grp 6_PC 10x Grp 6_PC 20x Grp 6_PC 240x Grp		アドレスグループ	0
Dst Black list			アドレスグループ	1
Dst White list	test FQDN		アドレスグループ	1
G Suite	@gmail.com wildcard.google.com		アドレスグループ	0
Group3	10.0.0/8 172.16.0.0/12 192.168.0.0/16		アドレスグループ	0
Microsoft Office 365	login.microsoftonline.com login.microsoft.com login.windows.net		アドレスグループ	0
Src Black list	none		アドレスグループ	1
Src White list	none		アドレスグループ	1
test group	test server		アドレスグループ	0
リスト1	172.16.0.0/12 192.168.0.0/16		アドレスグループ	0

- II. メンバーの+をクリックしリストから対象のアドレスを選択し、メンバーに投入する。
- III. 投入したい分選択したら OK を押下する。



アドレスグループの編集

グループ名: Src Black list

カラー: 変更

タイプ: グループ フォルダ

メンバー: 100.88.18.0/29, 192.168.0.1

メンバーの除外:

スタティックルート設定:

コメント: コメント記入...

リストから設定する分選択する

エントリを選択

検索: Q.0

新規作成

アドレス (9)

10.0.0.0/8

100.64.0.0/16

100.88.18.0/29

172.16.0.0/12

172.17.1.0/24

172.17.2.0/24

192.168.0.0/16

192.168.0.1

4\_T-GATE VPNTap 54.178.158.35

アドレスグループ (3)

02\_Youtube\_Src

Group3

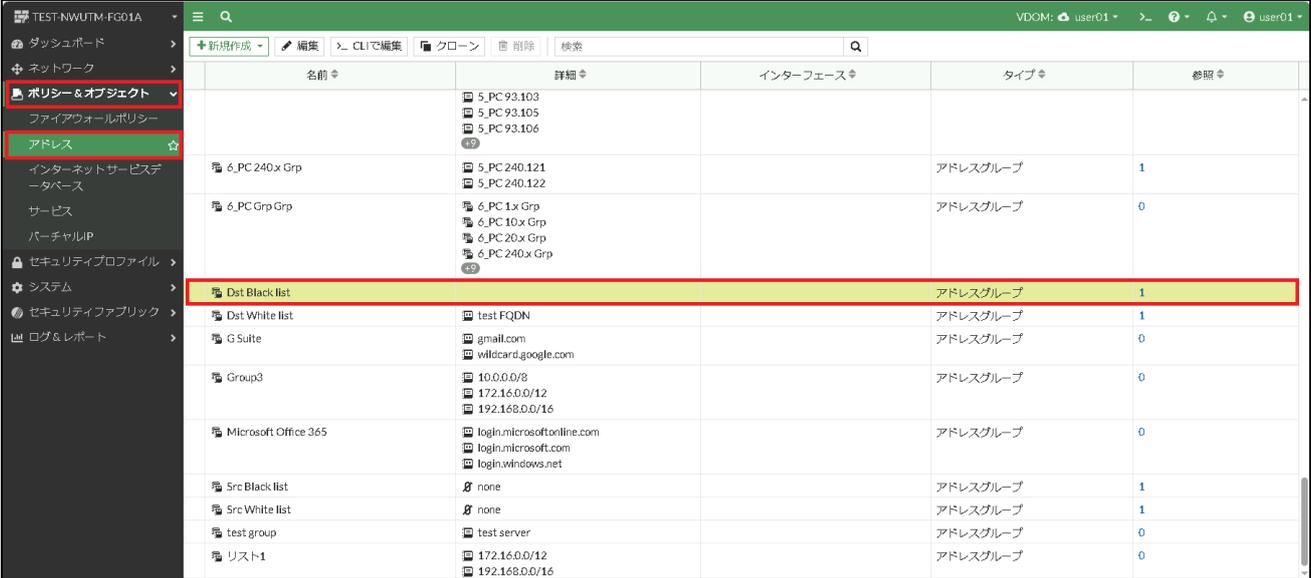
クローズ

OK キャンセル

## ② Dst Black list への設定方法

※業務上接続させたくないWeb サイトなどを設定するリストになります。

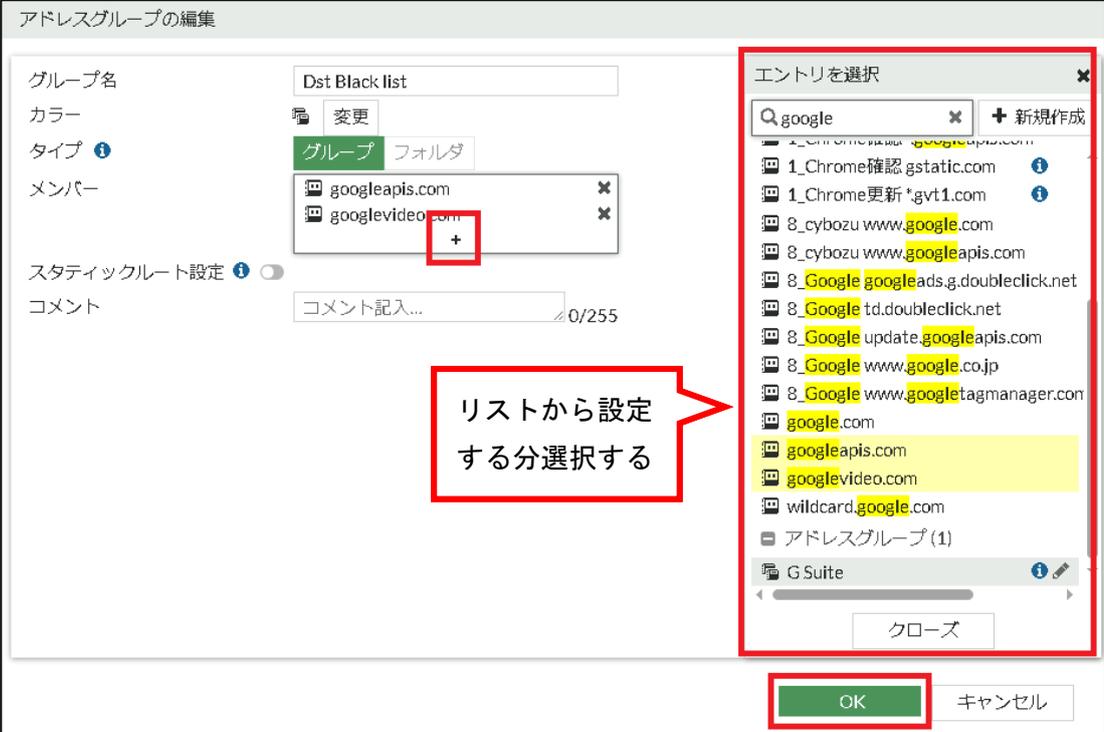
- I. 左メニューより、ポリシー&オブジェクト→アドレスを選択し、アドレスグループにあるDst Black list をダブルクリックする。



名前	詳細	インターフェース	タイプ	参照
6_PC 240x Grp	5_PC 93.103 5_PC 93.105 5_PC 93.106		アドレスグループ	1
6_PC Grp Grp	5_PC 240.121 5_PC 240.122		アドレスグループ	0
<b>Dst Black list</b>			アドレスグループ	1
Dst White list	test FQDN		アドレスグループ	1
G Suite	@gmail.com wildcard.google.com		アドレスグループ	0
Group3	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16		アドレスグループ	0
Microsoft Office 365	login.microsoftonline.com login.microsoft.com login.windows.net		アドレスグループ	0
Src Black list	none		アドレスグループ	1
Src White list	none		アドレスグループ	1
test group	test.server		アドレスグループ	0
リスト1	172.16.0.0/12 192.168.0.0/16		アドレスグループ	0

- II. メンバーの+をクリックしリストから対象のアドレスを選択し、メンバーに投入する。

- III. 投入したい分選択したら OK を押下する。



アドレスグループの編集

グループ名: Dst Black list

カラー: 変更

タイプ: グループ フォルダ

メンバー: googleapis.com, googlevideo.com

スタティックルート設定:

コメント: コメント記入... /0/255

エントリを選択

検索: google

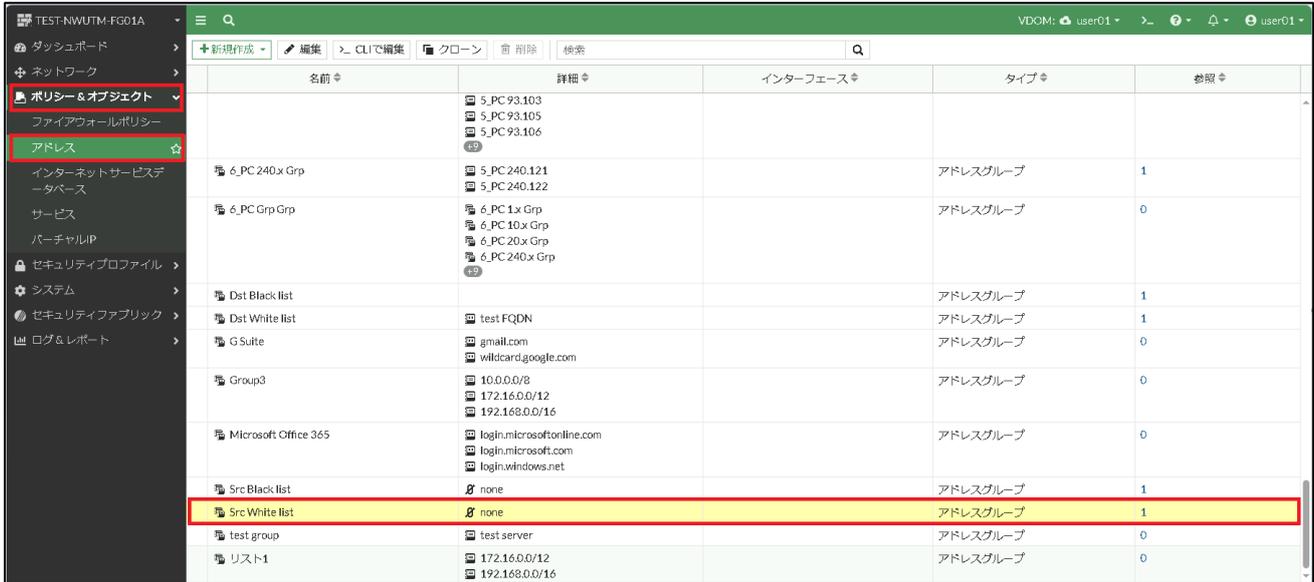
リストから設定する分選択する

OK キャンセル

### ③ Src White list への設定方法

※セキュリティ機能を無効にし、通信を行いたいクライアント端末などを設定するリストになります。

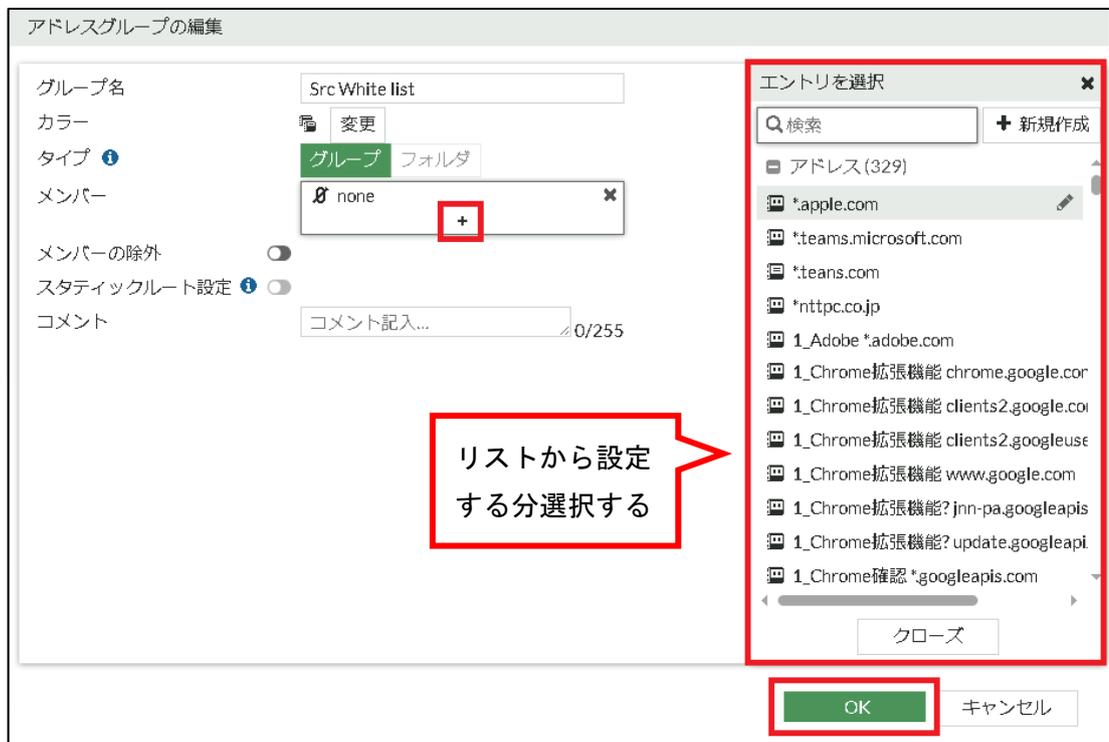
I. 左メニューより、ポリシー&オブジェクト→アドレスを選択し、アドレスグループにある Src White list をダブルクリックする。



名前	詳細	インターフェース	タイプ	参照
	5_PC 93.103 5_PC 93.105 5_PC 93.106			
6_PC 240x Grp	5_PC 240.121 5_PC 240.122		アドレスグループ	1
6_PC Grp Grp	6_PC 1x Grp 6_PC 10x Grp 6_PC 20x Grp 6_PC 240x Grp		アドレスグループ	0
Dst Black list			アドレスグループ	1
Dst White list	test FQDN		アドレスグループ	1
G Suite	gmail.com wildcard.google.com		アドレスグループ	0
Group3	10.0.0/8 172.16.0/12 192.168.0/16		アドレスグループ	0
Microsoft Office 365	login.microsoftonline.com login.microsoft.com login.windows.net		アドレスグループ	0
Src Black list	none		アドレスグループ	1
Src White list	none		アドレスグループ	1
test group	test.server		アドレスグループ	0
リスト1	172.16.0/12 192.168.0/16		アドレスグループ	0

II. メンバーの+をクリックしリストから対象のアドレスを選択し、メンバーに投入する。

III. 投入したい分選択したら OK を押下する。



アドレスグループの編集

グループ名: Src White list

カラー: 変更

タイプ: グループ フォルダ

メンバー: none +

メンバーの除外:

スタティックルート設定:

コメント: コメント記入... 0/255

エントリを選択

検索: + 新規作成

アドレス (329)

- \*apple.com
- \*teams.microsoft.com
- \*teams.com
- \*nttpc.co.jp
- 1\_Adobe \*adobe.com
- 1\_Chrome拡張機能 chrome.google.cor
- 1\_Chrome拡張機能 clients2.google.coi
- 1\_Chrome拡張機能 clients2.googleuse
- 1\_Chrome拡張機能 www.google.com
- 1\_Chrome拡張機能? jnn-pa.googleapis
- 1\_Chrome拡張機能? update.googleapi
- 1\_Chrome確認 \*googleapis.com

クローズ

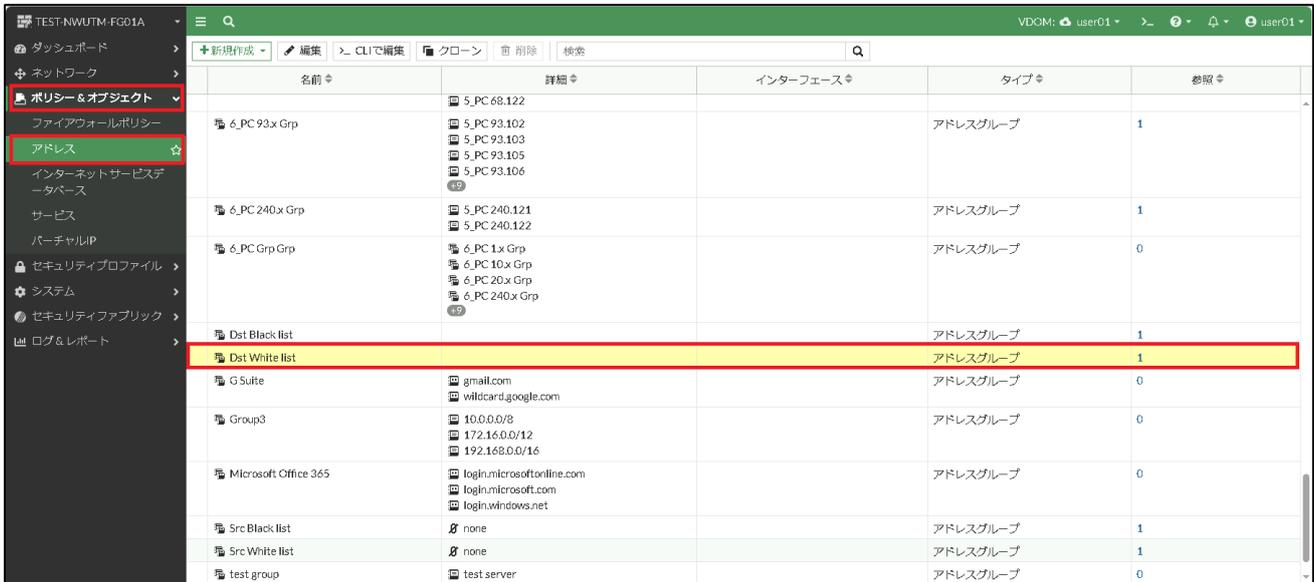
OK キャンセル

リストから設定する分選択する

#### ④ Dst White list への設定方法

※信頼のある Web サイトなどを設定することにより、セキュリティ機能を無効にした状態で通信をすることができるリストです。

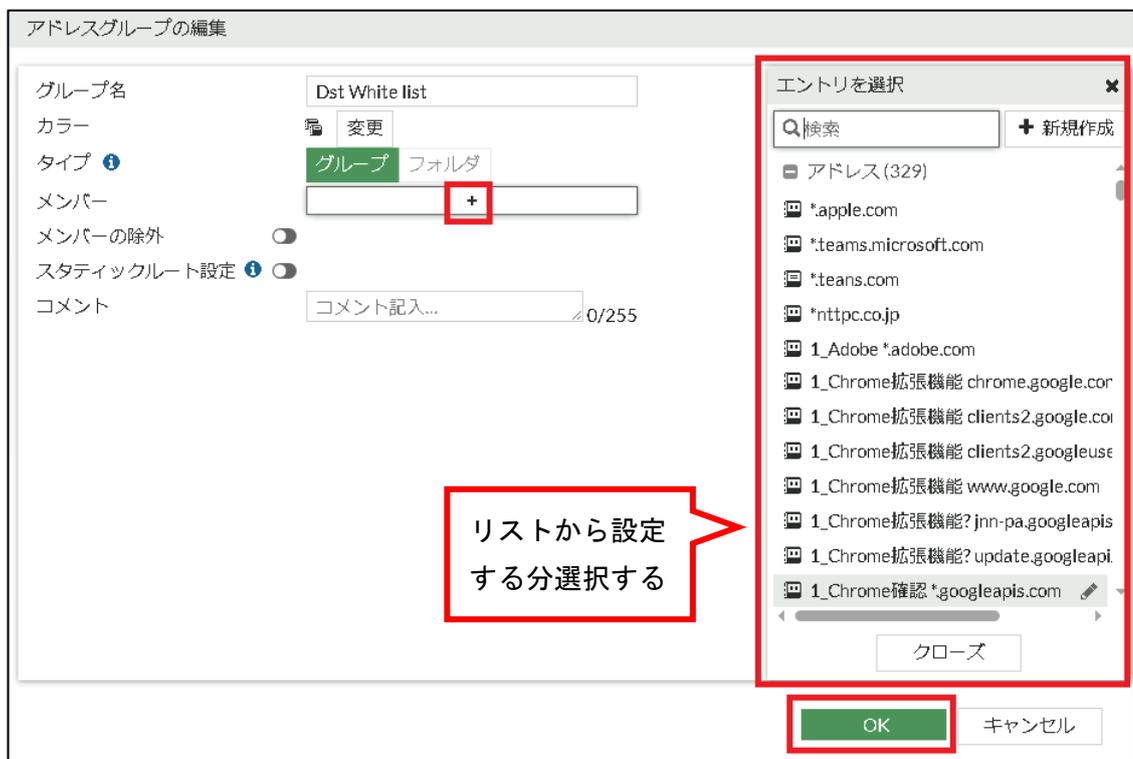
I. 左メニューより、ポリシー&オブジェクト→アドレスを選択し、アドレスグループにある Dst White list をダブルクリックする。



名前	詳細	インターフェース	タイプ	参照
ファイアウォールポリシー				
6_PC 93x Grp	5_PC 68.122 5_PC 93.102 5_PC 93.103 5_PC 93.105 5_PC 93.106		アドレスグループ	1
6_PC 240x Grp	5_PC 240.121 5_PC 240.122		アドレスグループ	1
6_PC Grp Grp	6_PC 1x Grp 6_PC 10x Grp 6_PC 20x Grp 6_PC 240x Grp		アドレスグループ	0
Dst Black list			アドレスグループ	1
Dst White list			アドレスグループ	1
G Suite	gmail.com wildcard.google.com		アドレスグループ	0
Group3	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16		アドレスグループ	0
Microsoft Office 365	login.microsoftonline.com login.microsoft.com login.windows.net		アドレスグループ	0
Src Black list	none		アドレスグループ	1
Src White list	none		アドレスグループ	1
test group	test server		アドレスグループ	0

II. メンバーの+をクリックしリストから対象のアドレスを選択し、メンバーに投入する。

III. 投入したい分選択したら OK を押下する。



アドレスグループの編集

グループ名: Dst White list

カラー: 変更

タイプ: グループ フォルダ

メンバー: +

メンバーの除外:

スタティックルートを設定:

コメント: コメント記入... /0/255

エントリを選択

検索: + 新規作成

- アドレス (329)
- \*apple.com
- \*teams.microsoft.com
- \*teams.com
- \*nttpc.co.jp
- 1\_Adobe \*.adobe.com
- 1\_Chrome拡張機能 chrome.google.co
- 1\_Chrome拡張機能 clients2.google.co
- 1\_Chrome拡張機能 clients2.googleuse
- 1\_Chrome拡張機能 www.google.com
- 1\_Chrome拡張機能? jnn-pa.googleapis
- 1\_Chrome拡張機能? update.googleapi
- 1\_Chrome確認 \*googleapis.com

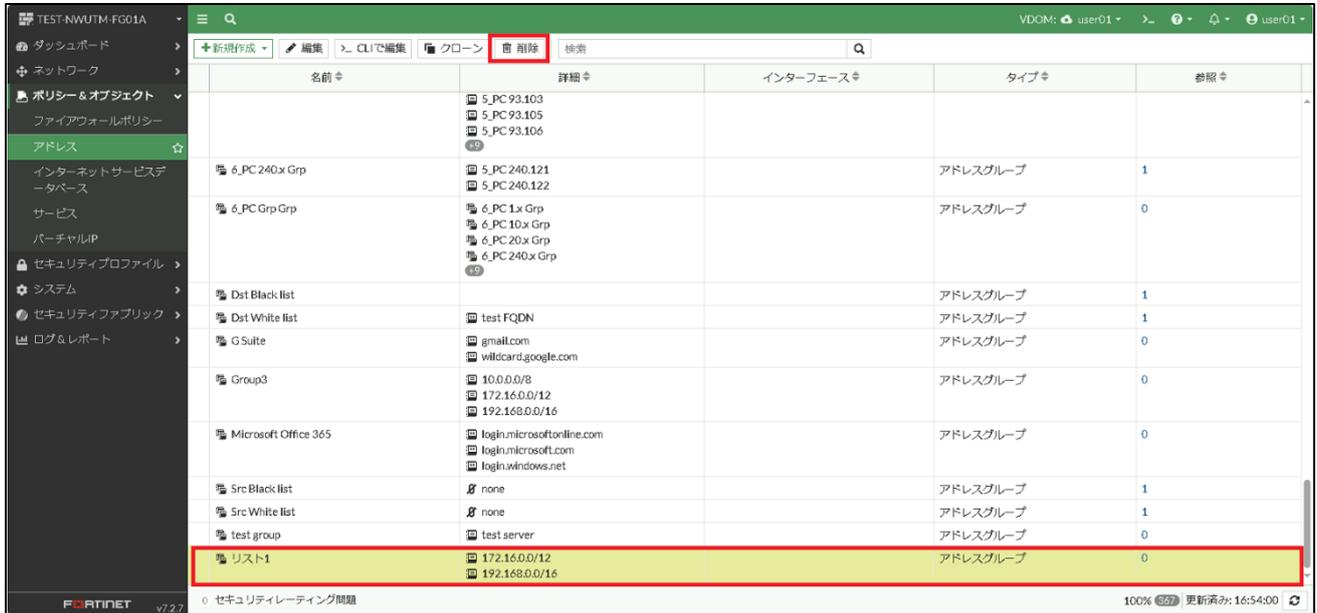
リストから設定する分選択する

クローズ

OK キャンセル

## 6.4 アドレスグループの削除

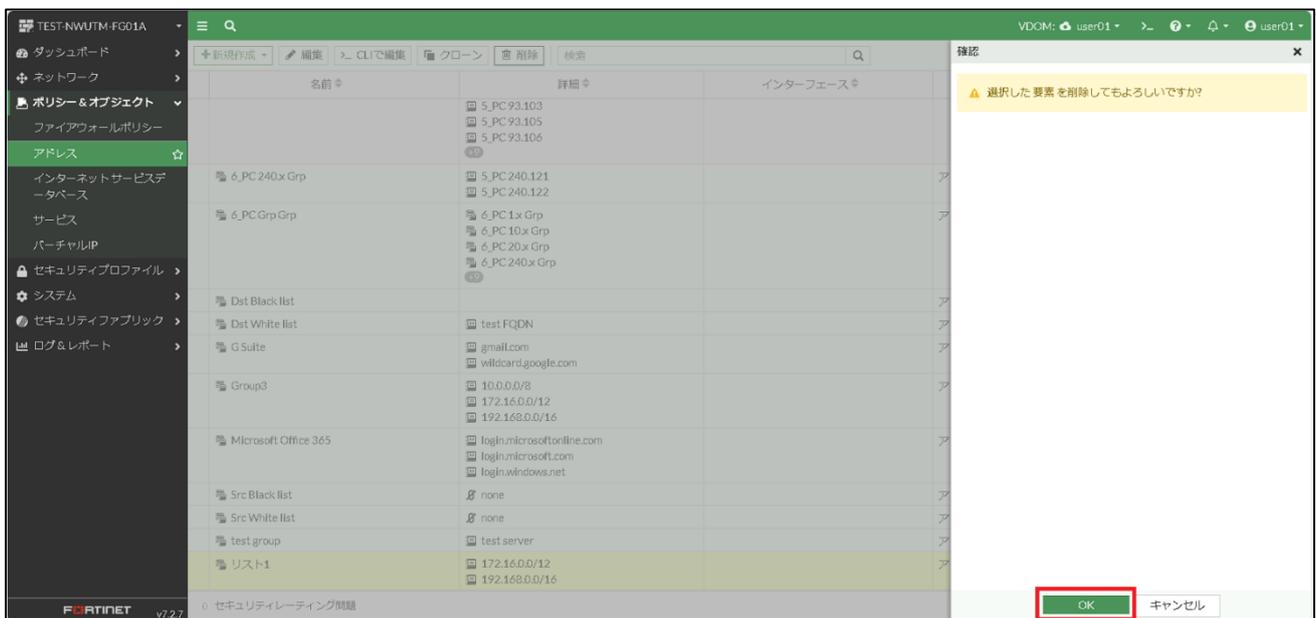
- ① 左のメニューからポリシー&オブジェクト->アドレスを選択する。
- ② 削除したいアドレスグループをクリックし、削除をクリックします。



The screenshot shows the Fortinet web interface with the 'Addresses' section selected in the left-hand menu. The 'Delete' button in the top navigation bar is highlighted in red. The 'リスト1' address group is selected and highlighted in yellow.

名前	詳細	インターフェース	タイプ	参照
6_PC 240x Grp	5_PC 93.103 5_PC 93.105 5_PC 93.106		アドレスグループ	1
6_PC Grp Grp	6_PC 1x Grp 6_PC 10x Grp 6_PC 20x Grp 6_PC 240x Grp		アドレスグループ	0
Dst Black list			アドレスグループ	1
Dst White list	test fqdn		アドレスグループ	1
G Suite	gmail.com willcard.google.com		アドレスグループ	0
Group3	10.0.0/8 172.16.0/12 192.168.0/16		アドレスグループ	0
Microsoft Office 365	login.microsoftonline.com login.microsoft.com login.windows.net		アドレスグループ	0
Src Black list	none		アドレスグループ	1
Src White list	none		アドレスグループ	1
test group	test server		アドレスグループ	0
リスト1	172.16.0/12 192.168.0/16		アドレスグループ	0

- ③ 確認ウィンドウがでるので、OK をクリックします。



The screenshot shows the Fortinet web interface with the 'Addresses' section selected. A confirmation dialog box is displayed on the right side of the screen, asking '選択した要素を削除してもよろしいですか?' (Are you sure you want to delete the selected items?). The 'OK' button is highlighted in red.

## 7 サービスの設定方法

本章では、ファイアウォールルールで設定するサービス（TCP や UDP など）の設定方法について解説しています。

### 7.1 サービスの追加

- ① 左のメニューからポリシー&オブジェクト->サービスを選



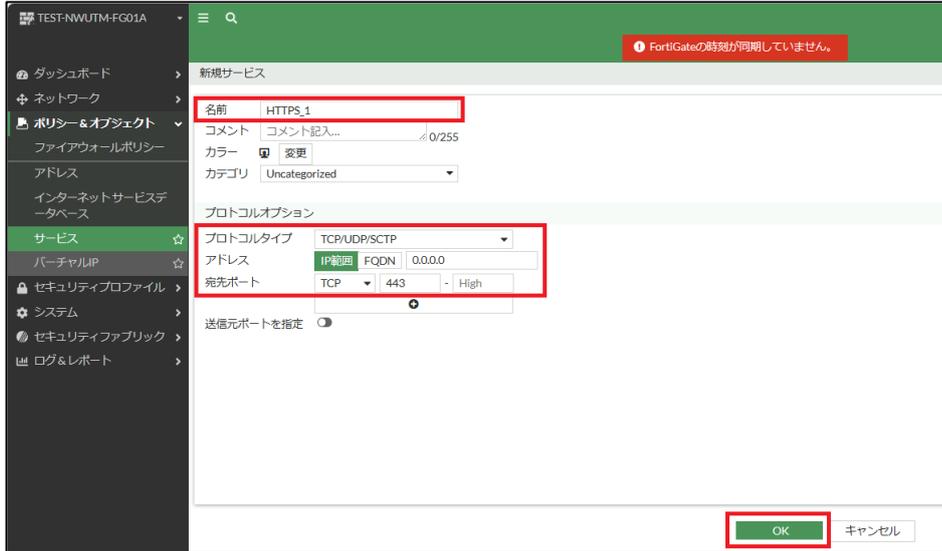
- ② 新規作成を押下する。

名前	詳細	IP/FQDN	カテゴリ	プロトコル	参照
1_TIME:37	TCP/37	0.0.0.0	未分類	TCP/UDP/SCTP	0
AFS3	TCP/7000-7009 UDP/7000-7009	0.0.0.0	File Access	TCP/UDP/SCTP	0
AH	IP/51		Tunneling	IP	0
ALL	ANY		一般	IP	10
ALL_ICMP	ANY		一般	ICMP	1
ALL_TCP	TCP/1-65535	0.0.0.0	一般	TCP/UDP/SCTP	0
ALL_UDP	UDP/1-65535	0.0.0.0	一般	TCP/UDP/SCTP	0
AOL	TCP/5190-5194	0.0.0.0	未分類	TCP/UDP/SCTP	0
BGP	TCP/179	0.0.0.0	ネットワークサービス	TCP/UDP/SCTP	0
CVSPSERVER	TCP/2401 UDP/2401	0.0.0.0	未分類	TCP/UDP/SCTP	0
DCE-RPC	TCP/135 UDP/135	0.0.0.0	リモートアクセス	TCP/UDP/SCTP	2
DHCP	UDP/67-68	0.0.0.0	ネットワークサービス	TCP/UDP/SCTP	0
DHCP6	UDP/546 UDP/547	0.0.0.0	ネットワークサービス	TCP/UDP/SCTP	0
DNS	TCP/53 UDP/53	0.0.0.0	ネットワークサービス	TCP/UDP/SCTP	4
ESP	IP/50		Tunneling	IP	0
FINGER	TCP/79	0.0.0.0	未分類	TCP/UDP/SCTP	0
FTP	TCP/21	0.0.0.0	File Access	TCP/UDP/SCTP	0

③ 名前の記載、プロトコルタイプを選択する。

※プロトコルタイプは 3 種類ありますが TCP/UDP/SCTP または既存に設定されている ICMP を使用することを推奨します。

I. プロトコル TCP/UDP/SCTP を選択した場合はアドレス、宛先ポートを記載し OK を押下する。



TEST-NWUTM-FG01A

FortiGateの時刻が同期していません。

新規サービス

名前: HTTPS\_1

コメント: コメント記入... / 0/255

カラー: 変更

カテゴリ: Uncategorized

プロトコルオプション

プロトコルタイプ: TCP/UDP/SCTP

アドレス: IP範囲 FQDN 0.0.0.0

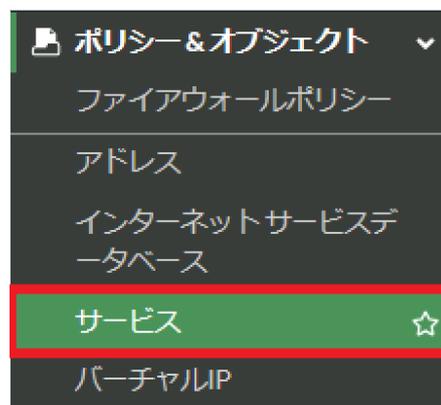
宛先ポート: TCP 443 - High

送信元ポートを指定:

OK キャンセル

## 7.2 サービスの変更

① 左のメニューからポリシー&オブジェクト->サービスを選択する。

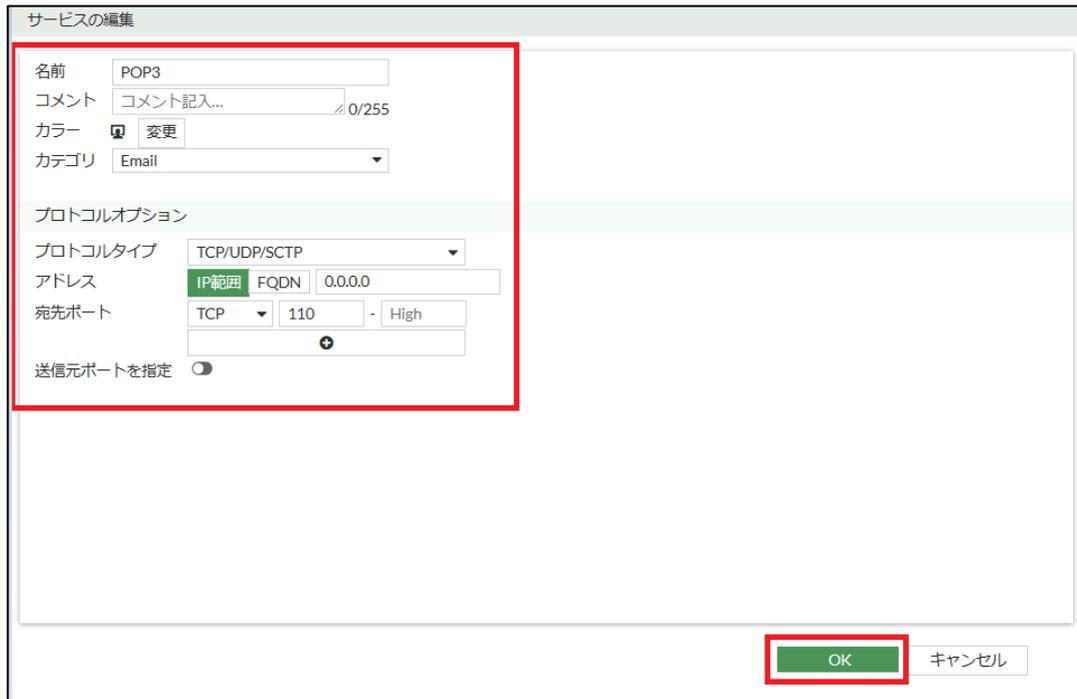


② 変更したいサービスをダブルクリックする。



名前	詳細	IP/FQDN	カテゴリ	プロトコル	詳細
ONC-RPC	TCP/111 UDP/111	0.0.0.0	リモートアクセス	TCP/UDP/SCTP	0
OSPF	IP/89		ネットワークサービス	IP	0
PCAnywhere	TCP/5631 UDP/5632	0.0.0.0	リモートアクセス	TCP/UDP/SCTP	0
PING	ICMP/ANY		ネットワークサービス	ICMP	0
<b>POP3</b>	<b>TCP/110</b>	<b>0.0.0.0</b>	<b>Email</b>	<b>TCP/UDP/SCTP</b>	<b>1</b>
POP3S	TCP/995	0.0.0.0	Email	TCP/UDP/SCTP	1
PPTP	TCP/1723	0.0.0.0	Tunneling	TCP/UDP/SCTP	0
QUAKE	UDP/26000 UDP/27000 UDP/27910 UDP/27960	0.0.0.0	未分類	TCP/UDP/SCTP	0
RADIUS	UDP/1812 UDP/1813	0.0.0.0	認証	TCP/UDP/SCTP	0
RADIUS-CLD	UDP/1645 UDP/1646	0.0.0.0	未分類	TCP/UDP/SCTP	0
RAUDIO	UDP/7070	0.0.0.0	未分類	TCP/UDP/SCTP	0
RDP	TCP/3389	0.0.0.0	リモートアクセス	TCP/UDP/SCTP	0
REXEC	TCP/512	0.0.0.0	未分類	TCP/UDP/SCTP	0
RIP	UDP/520	0.0.0.0	ネットワークサービス	TCP/UDP/SCTP	0
RLOGIN	TCP/513512-1023	0.0.0.0	未分類	TCP/UDP/SCTP	0
RSH	TCP/514512-1023	0.0.0.0	未分類	TCP/UDP/SCTP	0
RTSP	TCP/554 TCP/7070 TCP/8554 UDP/554	0.0.0.0	VoIP, Messaging & Other Applications	TCP/UDP/SCTP	0
SAMBA	TCP/139	0.0.0.0	File Access	TCP/UDP/SCTP	1
SCCP	TCP/2000	0.0.0.0	VoIP, Messaging & Other Applications	TCP/UDP/SCTP	0
SIP	TCP/5060 UDP/5060	0.0.0.0	VoIP, Messaging & Other Applications	TCP/UDP/SCTP	0
SIP-MSNMessenger	TCP/1863	0.0.0.0	VoIP, Messaging & Other Applications	TCP/UDP/SCTP	0
SMB	TCP/445	0.0.0.0	File Access	TCP/UDP/SCTP	1

③ 変更したい項目を変更し、OK をクリックする。



サービスの編集

名前: POP3

コメント: コメント記入... 0/255

カラー:  変更

カテゴリ: Email

プロトコルオプション

プロトコルタイプ: TCP/UDP/SCTP

アドレス: IP範囲 FQDN 0.0.0.0

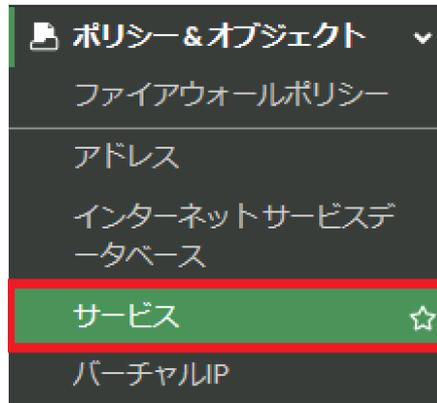
宛先ポート: TCP 110 - High

送信元ポートを指定:

OK キャンセル

### 7.3 サービスの削除

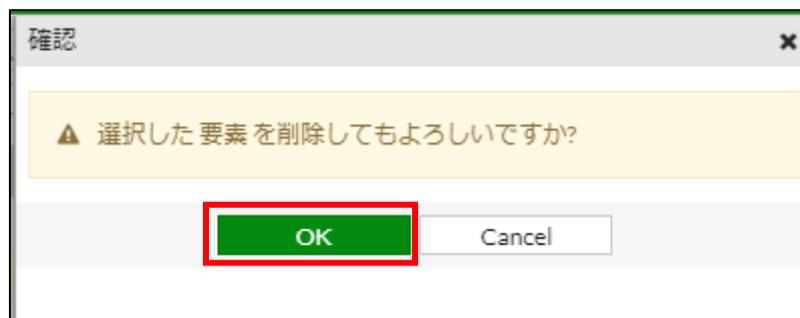
- ① 左のメニューからポリシー&オブジェクト->サービスを選択



- ② 削除するサービスをクリックし削除を押下する。

サービス名	詳細	IP/FQDN
General 5		
ALL	ANY	
<b>ALL_TCP</b>	<b>TCP/1-65535</b>	<b>0.0.0.0</b>
ALL_UDP	UDP/1-65535	0.0.0.0
ALL_ICMP	ANY	
ALL_ICMP6	ANY	

- ③ 確認ウィンドウがでるので、OK をクリックします。



## 8 セキュリティプロファイル：アンチウイルス

本章では、アンチウイルス機能の設定方法について解説しています。

※灰色の網掛け部分に関しては変更出来ないパラメータとなります。

アンチウイルスプロファイルの編集

名前	default
コメント	コメント記入... <span style="float: right;">0/255</span>
アンチウイルススキャン <span style="font-size: small;">?</span>	<input type="radio"/> ブロック <input checked="" type="radio"/> モニタ
機能セット	<input type="radio"/> フローベース <input checked="" type="radio"/> プロキシベース

インスペクションされるプロトコル

HTTP	<input checked="" type="checkbox"/>
SMTP	<input type="checkbox"/>
POP3	<input type="checkbox"/>
IMAP	<input type="checkbox"/>
FTP	<input type="checkbox"/>
CIFS	<input type="checkbox"/>
MAPI <span style="font-size: small;">?</span>	<input type="checkbox"/>
SSH <span style="font-size: small;">?</span>	<input type="checkbox"/>

APTプロテクションオプション

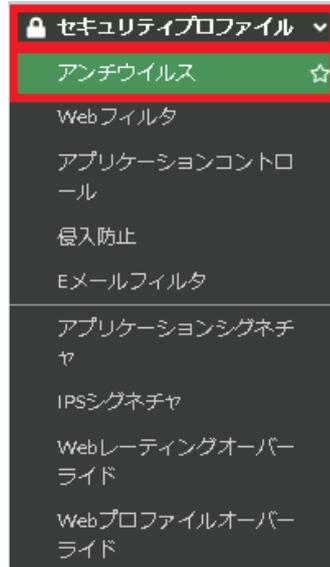
コンテンツ無害化 <span style="font-size: small;">?</span> <span style="font-size: small;">?</span>	<input type="checkbox"/>
Eメール添付のWindows実行ファイルをウイルスとして扱う <span style="font-size: small;">?</span>	<input type="checkbox"/>
FortiSandboxに検査のためファイルを送信 <span style="font-size: small;">?</span>	<input type="checkbox"/>
FortiNDRに検査のためファイルを送信 <span style="font-size: small;">?</span> <span style="font-size: small;">?</span>	<input type="checkbox"/>
モバイルマルウェアプロテクションを含める	<input checked="" type="checkbox"/>
隔離 <span style="font-size: small;">?</span>	<input type="checkbox"/>

ウイルスアウトブレイク防止 ?

FortiGuardアウトブレイク防止データベースを使用する	<input type="checkbox"/>
外部マルウェアブロックリストを使用	<input type="checkbox"/>
EMS脅威フィードの使用 <span style="font-size: small;">?</span>	<input type="checkbox"/>

## 8.1 アンチウイルスの設定

- ① 左メニューよりセキュリティプロファイル→アンチウイルスを選択



- ② default をダブルクリックします。

名前*	コメント*	スコープ*	参照*
g-default	Scan files and block viruses.	グローバル	
g-wifi-default	Default configuration for offloading WiFi traffic.	グローバル	
default		VDOM	2

- ③ インспекションされるプロトコルより監視するプロトコルを選択し有効化または無効化する。

※MAPI、CIFS、SSH は有効化しないでください。



- ④ アンチウイルス内の設定が完了したら画面一番下にある OK を押下する。



## 9 セキュリティプロファイル：Web フィルタ

本章では、Web フィルタ機能の設定方法について解説しています。

※灰色の網掛け部分に関しては変更出来ないパラメータとなります。

Webフィルタプロファイルの編集

名前

コメント  0/255

機能セット フローベース プロキシベース

FortiGuardカテゴリベースのフィルタ

許可
  モニタ
  ブロック
  警告
  認証

名前	アクション
ローカルカテゴリ	
custom1	<input type="radio"/> 無効
custom2	<input type="radio"/> 無効
違法性の高いサイト	
薬物乱用	<input checked="" type="radio"/> モニタ
ハッキング	<input checked="" type="radio"/> モニタ
違法または非倫理的	<input checked="" type="radio"/> モニタ
差別	<input checked="" type="radio"/> モニタ

0%

カテゴリ使用クォータ

+新規作成 編集 削除

カテゴリ	クォータ合計
エントリがありません	

ユーザにブロックされたカテゴリのオーバーライドを許可する

サーチエンジン

スタティックURLフィルタ

無効なURLをブロック

URLフィルタ

FortiSandboxにより検知された悪意のあるURLをブロック

コンテンツフィルタ

レーティングオプション

プロキシオプション

## 9.1 Web フィルタの設定

- ① 左メニューよりポリシー&オブジェクト->ファイアウォールポリシーを選択し、LAN→WAN もしくは webfilter-policy-\* に設定されている web フィルタのセキュリティプロファイルを確認する。(水色で web と白字で記載されているもの)

LAN→WAN	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default <b>WEB default</b> APP default certificate-inspection	すべて	2.18 MB	スタンダー
---------	---	-----	--------	-----	----	------------------	---	-----	---------	-------

- ② 左メニューよりセキュリティプロファイル->Web フィルタを選択し、①で確認したプロファイルをダブルクリックします。(種類として default、Webfilter-profile-\*、Base Profile 等があります。) サービスリニューアル前に契約されたお客様につきましては default 以外の設定になります。

名前	コメント	スコープ	参照
WEB g-default	Default web filtering.	グローバル	
WEB default	Default web filtering.	VDOM	1
WEB g-wifi-default	Default configuration for offloading WiFi traffic.	グローバル	

### I. FortiGuard カテゴリベースのフィルタ

カテゴリの項目は、以下 8 項目になります。

+ ローカルカテゴリ ②
+ 違法性の高いサイト ⑫
+ アダルト/成人コンテンツ ⑮
+ 帯域を消費しやすいサイト ⑥
+ セキュリティリスクの高いサイト ⑥
+ 一般的な関心事 - 個人 ③⑤
+ 一般的な関心事 - ビジネス ⑮
+ 未評価 ①

アクションについての詳細は下記のとおりです。

許可：カテゴリ内のサイトへのアクセスを許可します。

ブロック：カテゴリ内のサイトへのアクセスを遮断し、ログに記録します。

モニタ：カテゴリ内のサイトへのアクセスを許可及びログに記録します。

項目内に表示されているカテゴリをクリックし、アクションを選択しOKを押下する。

※カテゴリを表示させる場合は項目左にある+を押下すると表示されます。

※デフォルト設定についてはP. 15の表3-3を参照してください。

※項目のローカルカテゴリ、未評価については設定変更しないでください。

未評価をブロック設定にした場合、著しくスループットが落ちますのでご注意ください。

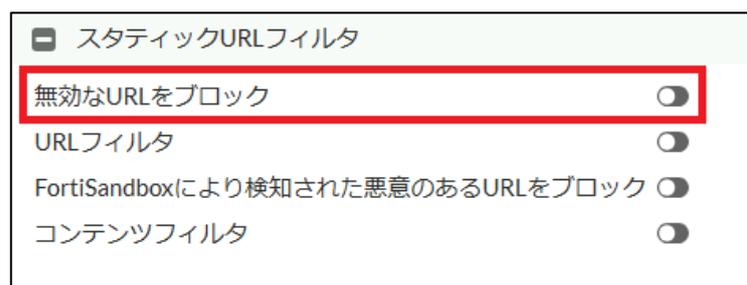
例：過激派グループをブロックにする場合

メインカテゴリより過激派グループをクリックし、ブロックを押下する。



## II. スタティック URL フィルタ（無効な URL をブロック）

この設定を使用して、SSL 証明書の CN フィールドに有効なドメイン名が含まれていない場合に Web サイトをブロックします。



### III. スタティック URL フィルタ (URL フィルタ)

テキストと正規表現を含むパターンで特定の URL を追加することにより、指定された URL またはパターンに一致する Web ページへのアクセスを許可、ブロック、除外、モニタします。

アクションについての詳細は下記の通りです。

除外：対象の URL は許可され、その他のセキュリティチェックもせずに通信を通過させます。

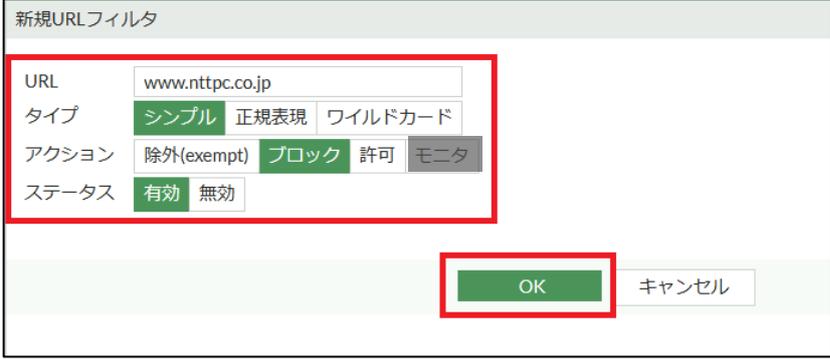
許可：URL フィルタでは許可となるが、その他有効化されているアンチウイルス等のセキュリティチェックが行われます。

ブロック：URL パターンに一致する URL へのアクセスを遮断し、ログに記録します。

例：www.nttpc.co.jp をタイプシンプルでブロックする場合  
URL フィルタを有効化し、新規作成をクリック



URL、タイプ、アクション、ステータスを入力選択し OK をクリック



※UTM は www. nttpc. co. jp に部分一致したものをブロックします。

hoge. nttpc. co. jp などはブロックしません。

ブロックさせたい場合は URL に hoge. nttpc. co. jp を指定するか、タイプ（ワイルドカード）の手順で設定してください。

例：hoge. nttpc. co. jp などのドメインをブロックさせたい場合

URL：\*nttpc. co. jp

タイプ：ワイルドカード

アクション：ブロック

例：正規表現で www. nttpc. co. jp をブロックさせたい場合

URL：^www¥. nttpc¥. co¥. jp/

タイプ：正規表現

アクション：ブロック

※URL フィルタよりもカテゴリベースのフィルタの方がセキュリティ設定が強いため、カテゴリベースのフィルタでブロックされているものを許可したい場合はアクション除外を使用して設定をしてください。

③ Web フィルタ内の設定が完了したら画面一番下にある OK を押下する。



## 10 セキュリティプロファイル：アプリケーションコントロール

本章では、アプリケーションコントロール機能の設定方法について解説しています。

※灰色の網掛け部分に関しては変更出来ないパラメータとなります。

アプリケーションセンサーの編集

**⚠** 112個のクラウドアプリケーションはディープインスペクションが必要です。  
1個のポリシーがこのプロファイルを使用しています。 **+**

名前

コメント  0/255

カテゴリ

モニタ・すべてのカテゴリ

<input checked="" type="checkbox"/> Business (156, ☁️ 6)	<input checked="" type="checkbox"/> Cloud.IT (62, ☁️ 1)
<input checked="" type="checkbox"/> Collaboration (270, ☁️ 17)	<input checked="" type="checkbox"/> Email (76, ☁️ 11)
<input checked="" type="checkbox"/> Game (84)	<input checked="" type="checkbox"/> General.Interest (242, ☁️ 12)
<input checked="" type="checkbox"/> Mobile (3)	<input checked="" type="checkbox"/> Network.Service (336)
<input checked="" type="checkbox"/> P2P (55)	<input checked="" type="checkbox"/> Proxy (181)
<input checked="" type="checkbox"/> Remote.Access (97)	<input checked="" type="checkbox"/> Social.Media (114, ☁️ 29)
<input checked="" type="checkbox"/> Storage.Backup (155, ☁️ 19)	<input checked="" type="checkbox"/> Update (48)
<input checked="" type="checkbox"/> Video/Audio (151, ☁️ 17)	<input checked="" type="checkbox"/> VoIP (24)
<input checked="" type="checkbox"/> Web.Client (24)	<input checked="" type="checkbox"/> 不明なアプリケーション

ネットワークプロトコルの強制

アプリケーションとフィルタのオーバーライド

プライオリティ	詳細	タイプ	アクション
エントリがありません			

**0**

オプション

デフォルト以外のポートで検知されたアプリケーションをブロック **i**

DNSトラフィックの許可とログ

HTTPベースアプリケーションの差し替えメッセージ

## 10.1 アプリケーションコントロールの設定

- ① 左メニューよりセキュリティプロファイル→アプリケーションコントロール→default をダブルクリックします。

名前	コメント	スコープ	参照
g-default	Monitor all applications.	グローバル	
g-wifi-default	Default configuration for offloading WiFi traffic.	グローバル	
default		VDOM	1

### I. カテゴリ

カテゴリを使用すると、カテゴリタイプに基づいてシグネチャのグループを選択することが可能です。

※シグネチャについては対象カテゴリのプルダウンから「シグネチャを表示」を押下すると確認可能です。

※クラウドシグネチャに関しては提供していないシグネチャとなります。

カテゴリより対象カテゴリのプルダウンよりモニタ、許可、ブロックのいずれかのアクションを選択します。



カテゴリ

ミックス すべてのカテゴリ

- Business (179, 6)
- Email (87, 12)
- Mobile (3)
- Proxy (106)
- Storage.Backup (296, 16)
- VoIP (31)
- Cloud.IT (31)
- Game (124)
- Network.Service (332)
- Remote.Access (91)
- Update (48)
- Web.Client (18)
- Collaboration (293, 6)
- General.Interest (241, 9)
  - モニタ
  - 許可
  - ブロック
  - 隔離
  - シグネチャを表示(241)
  - クラウドシグネチャを表示(9)

ネットワークプロトコルの強制

アクションの詳細については下記のとおりです。

許可：カテゴリ内のサイトへのアクセスを許可します

ブロック：カテゴリ内のサイトへのアクセスを遮断し、ログに記録します

モニタ：カテゴリ内のサイトへのアクセスを許可及びログに記録します。

カテゴリは下記 18 項目になります。



カテゴリ

モニタ すべてのカテゴリ

- Business (179, 6)
- Email (87, 12)
- Mobile (3)
- Proxy (106)
- Storage.Backup (296, 16)
- VoIP (31)
- Cloud.IT (31)
- Game (124)
- Network.Service (332)
- Remote.Access (91)
- Update (48)
- Web.Client (18)
- Collaboration (293, 6)
- General.Interest (241, 9)
- P2P (85)
- Social.Media (150, 31)
- Video/Audio (206, 13)
- 不明なアプリケーション

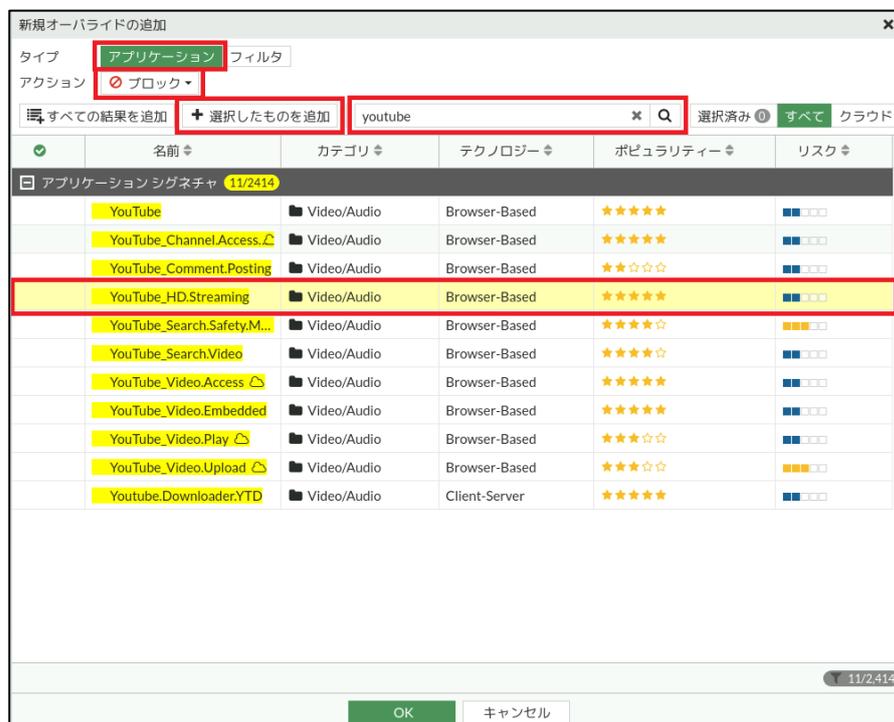
## II. アプリケーションとフィルタのオーバーライド

カテゴリとは別に個別にアプリケーション通信の許可、ブロック等の処理を可能とします。

例：youtube のHD ストリーミングをブロックする場合  
新規作成をクリック



タイプを「アプリケーション」、アクションを「ブロック」に設定します。  
検索ボックスにて「youtube」を入力し検索し、「YouTube\_HD.Streaming」を選択し、「選択したものを追加」を押下する。



対象のシグネチャにチェックがついていることを確認し「OK」をクリック

新規オーバーライドの追加

タイプ **アプリケーション** フィルタ

アクション **ブロック**

すべての結果を追加 youtube \* Q 選択済み すべて クラウド

名前	カテゴリ	テクノロジー	ポピュラリティ	リスク
アプリケーションシグネチャ 11/2414				
YouTube	Video/Audio	Browser-Based	★★★★★	■■■■
YouTube_Channel.Access....	Video/Audio	Browser-Based	★★★★★	■■■■
YouTube_Comment.Posting	Video/Audio	Browser-Based	★★★☆☆	■■■■
<input checked="" type="checkbox"/> YouTube_HD.Streaming	Video/Audio	Browser-Based	★★★★★	■■■■
YouTube_Search.Safety.M...	Video/Audio	Browser-Based	★★★★☆	■■■■
YouTube_Search.Video	Video/Audio	Browser-Based	★★★★☆	■■■■
YouTube_Video.Access	Video/Audio	Browser-Based	★★★★★	■■■■
YouTube_Video.Embedded	Video/Audio	Browser-Based	★★★★★	■■■■
YouTube_Video.Play	Video/Audio	Browser-Based	★★★☆☆	■■■■
YouTube_Video.Upload	Video/Audio	Browser-Based	★★★☆☆	■■■■
Youtube.Downloader.YTD	Video/Audio	Client-Server	★★★★★	■■■■

OK キャンセル

作成されたことを確認する。

プライオリティ	詳細	タイプ	アクション
1	YouTube_HD.Streaming	アプリケーション	<input checked="" type="checkbox"/> ブロック

例：既存の設定に YouTube ビデオアクセスを追加する場合  
追加したい既存のグループをダブルクリックする。

プライオリティ	詳細	タイプ	アクション
1	YouTube_HD.Streaming	アプリケーション	<input checked="" type="checkbox"/> ブロック

検索ボックスにて「youtube」を入力し検索し、「YouTube\_Video.Access」を選択し、「選択したものを追加」を押下する。

オーバーライドの編集

タイプ アプリケーション フィルタ  
 アクション ブロック

すべての結果を追加  選択したものを追加   選択済み 1

<input checked="" type="checkbox"/>	名前	カテゴリ	テクノロジー	ポピュラリティ	リスク
<input type="checkbox"/>	YouTube	Video/Audio	Browser-Based	★★★★★	■■■■
<input type="checkbox"/>	YouTube_Channel.Access.△	Video/Audio	Browser-Based	★★★★★	■■■■
<input type="checkbox"/>	YouTube_Comment.Posting	Video/Audio	Browser-Based	★★★☆☆	■■■■
<input checked="" type="checkbox"/>	YouTube_HD.Streaming	Video/Audio	Browser-Based	★★★★★	■■■■
<input type="checkbox"/>	YouTube_Search.Safety.M...	Video/Audio	Browser-Based	★★★★☆	■■■■
<input type="checkbox"/>	YouTube_Search.Video	Video/Audio	Browser-Based	★★★★☆	■■■■
<input checked="" type="checkbox"/>	YouTube_Video.Access △	Video/Audio	Browser-Based	★★★★★	■■■■
<input type="checkbox"/>	YouTube_Video.Embedded	Video/Audio	Browser-Based	★★★★★	■■■■
<input type="checkbox"/>	YouTube_Video.Play △	Video/Audio	Browser-Based	★★★☆☆	■■■■
<input type="checkbox"/>	YouTube_Video.Upload △	Video/Audio	Browser-Based	★★★☆☆	■■■■
<input type="checkbox"/>	Youtube.Downloader.YTD	Video/Audio	Client-Server	★★★★★	■■■■

アプリケーションシグネチャ 11/2414

OK キャンセル

対象のシグネチャにチェックがついていることを確認し「OK」をクリック

オーバーライドの編集

タイプ **アプリケーション** フィルタ

アクション **ブロック**

すべての結果を追加 youtube

選択済み すべて クラウド

	名前	カテゴリ	テクノロジー	ポピュラリティ	リスク
アプリケーション シグネチャ 11/2414					
	YouTube	Video/Audio	Browser-Based	★★★★★	■■■■■
	YouTube_Channel.Access.∠	Video/Audio	Browser-Based	★★★★★	■■■■■
	YouTube_Comment.Posting	Video/Audio	Browser-Based	★★☆☆☆	■■■■■
✓	YouTube_HD.Streaming	Video/Audio	Browser-Based	★★★★★	■■■■■
	YouTube_Search.Safety.M...	Video/Audio	Browser-Based	★★★★☆	■■■■■
	YouTube_Search.Video	Video/Audio	Browser-Based	★★★★☆	■■■■■
✓	YouTube_Video.Access ∆	Video/Audio	Browser-Based	★★★★★	■■■■■
	YouTube_Video.Embedded	Video/Audio	Browser-Based	★★★★★	■■■■■
	YouTube_Video.Play ∆	Video/Audio	Browser-Based	★★☆☆☆	■■■■■
	YouTube_Video.Upload ∆	Video/Audio	Browser-Based	★★☆☆☆	■■■■■
	Youtube.Downloader.YTD	Video/Audio	Client-Server	★★★★★	■■■■■

11/2414

**OK** キャンセル

追加されたことを確認する。

プライオリティ	詳細	タイプ	アクション
1	YouTube_HD.Streaming YouTube_Video.Access ∆	アプリケーション	ブロック

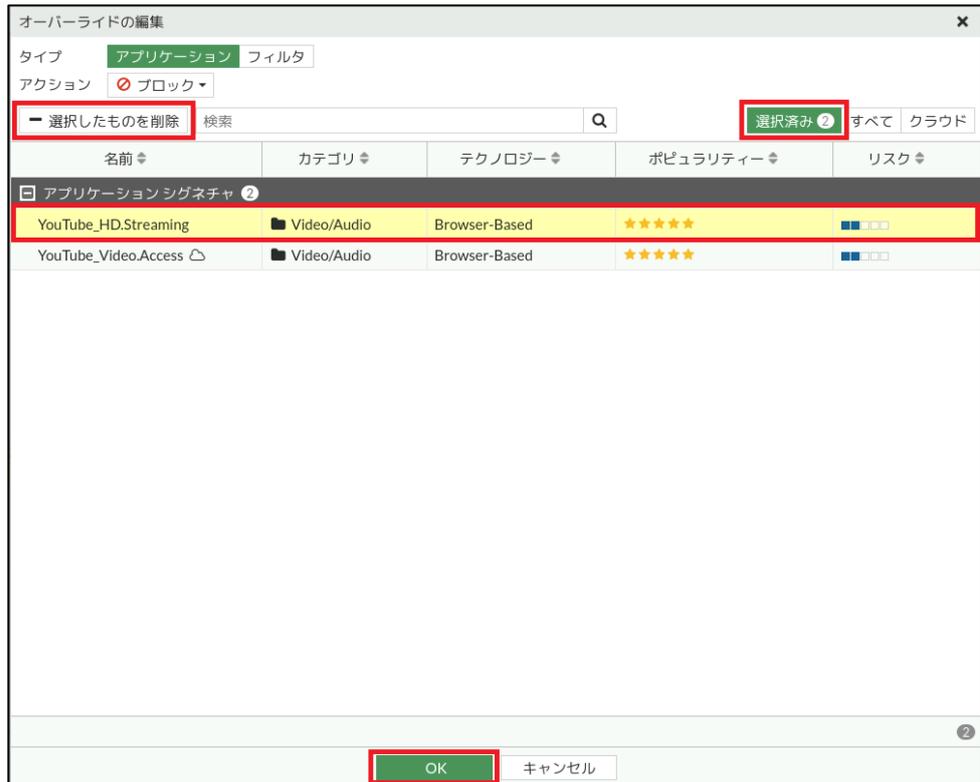
1

例：グループ内のシグネチャを削除する場合  
対象のグループをダブルクリックします。

プライオリティ	詳細	タイプ	アクション
1	YouTube_HD.Streaming YouTube_Video.Access ∆	アプリケーション	ブロック

1

選択済みをクリックし、削除したいシグネチャを選択し、「選択したものを削除」を押下し、OK をクリックする。



対象のシグネチャが削除されたことを確認する。

プライオリティ	詳細	タイプ	アクション
1	YouTube_Video.Access	アプリケーション	ブロック

①

② アプリケーションコントロール内の設定が完了したら画面一番下にある OK を押下する。



## 11 セキュリティプロファイル：IPS（侵入防止）

本章では、侵入防止機能について解説しています。

※こちらの機能については有効もしくは無効の操作のみを行ってください。

設定を変更された場合機能の保証はできません。

※機能の有効・無効については13章を参照ください。

IPSセンサーの編集

名前

コメント

25/255

悪意のあるURLをブロック

IPSシグネチャとフィルタ
 

+新規作成
編集
削除

詳細	除外IP	アクション	パケットロギング
SEV <span style="color: red;">■■■■■</span>		デフォルト	無効化済み

1

ポットネットC&C
 

ポットネットサイトへの発信接続をスキャン
 

無効 **ブロック** モニタ

botnet package に 2458個のIPアドレス。

OK

キャンセル

## 12 セキュリティプロファイル：アンチスパム（Eメールフィルタ）

本章では、Eメールフィルタの設定方法について解説しています。

メールフィルタプロファイルの編集

名前

コメント  35/255

機能セット  フローベース  プロキシベース

スパム検知とフィルタリングを有効化

**■ プロトコルごとのスパム検知**

プロトコル	スパムアクション	タグの挿入箇所	タグ形式
IMAP	転送	サブジェクト	[Spam]
POP3	転送	サブジェクト	[Spam]
SMTP	転送	サブジェクト	[Spam]

**+** FortiGuardスパムフィルタリング

**■** ローカルスパムフィルタリング

HELO DNSレックアップ

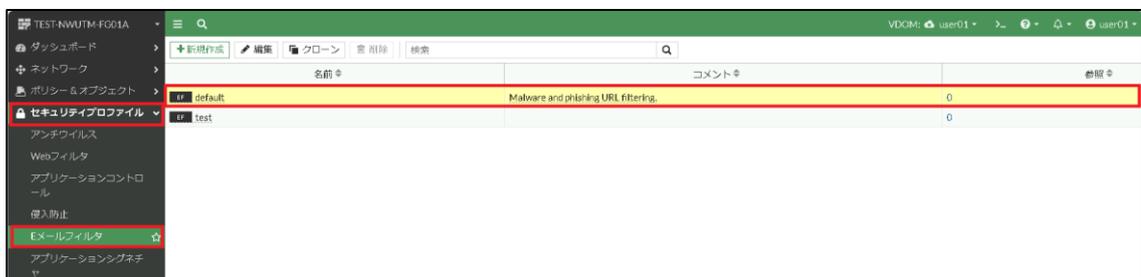
リターンEメールDNSチェック

ブロック/許可リスト

タイプ	パターン	アクション	ステータ...
送信者アドレ...	@nttpc.co.jp	クリアとしてマー...	有効
送信者アドレ...	@securityboss...	クリアとしてマー...	有効
送信者アドレ...	test.com	スパムとしてマー...	無効

### 12.1 Eメールフィルタの設定

左メニューよりセキュリティプロファイル->Eメールフィルタ->default ダブルクリックします。



### ① プロトコルごとのスパム検知数

SMTP、POP3、IMAP プロトコルの 3 プロトコルあり、各プロトコルはセクション分けされているので各セクションでプロトコルのログを破棄（SMTP のみ）、タグ、転送のアクションをスパムアクションより設定できます。

プロトコル	スパムアクション	タグの挿入箇所	タグ形式
IMAP	タグ ▼	サブジェクト ▼	[Spam]
POP3	タグ ▼	サブジェクト ▼	[Spam]
SMTP	タグ ▼	サブジェクト ▼	[Spam]

スパムアクションの詳細は下記のとおりです。

破棄：スパムメールを破棄（ブロック）します。

タグ：件名またはヘッダーに設定されたテキストでスパムメールにタグをつけます。

転送：スパムメールの送受信を許可します。

※スパムアクションでタグを選択した場合、タグの挿入箇所、タグ形式を任意で記載が可能です。

### ② ローカルスパムフィルタリング

電子メールまたは IP サブネットからブラックリスト/許可リストを作成して、電子メールの送受信を遮断または許可することができます。

ブラック/許可リストの新規作成をクリック

タイプ	パターン	アクション	ステータス
送信者アドレス	@nttpc.co.jp	クリアとしてマーク	有効
送信者アドレス	@securityboss.jp	クリアとしてマーク	有効
送信者アドレス	test.com	スパムとしてマーク	無効

図 12-2. スпамフィルタリング設定画面。

タイプ、パターン、アクションを選択入力し、ステータスが有効であることを確認し OK をクリック

図 12-3. スпамフィルタリング設定画面.

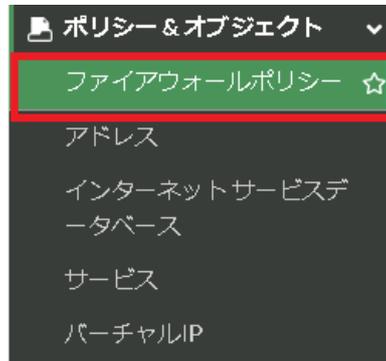
- ④ Eメールフィルタ内の設定が完了したら画面一番下にある OK を押下する。

### 13 各セキュリティ機能の有効・無効

本章では各セキュリティ機能の設定方法について解説しています。

#### 13.1 各セキュリティ機能の有効化

- ① 左メニューより、ポリシー&オブジェクト→ファイアウォールポリシーを選択する。

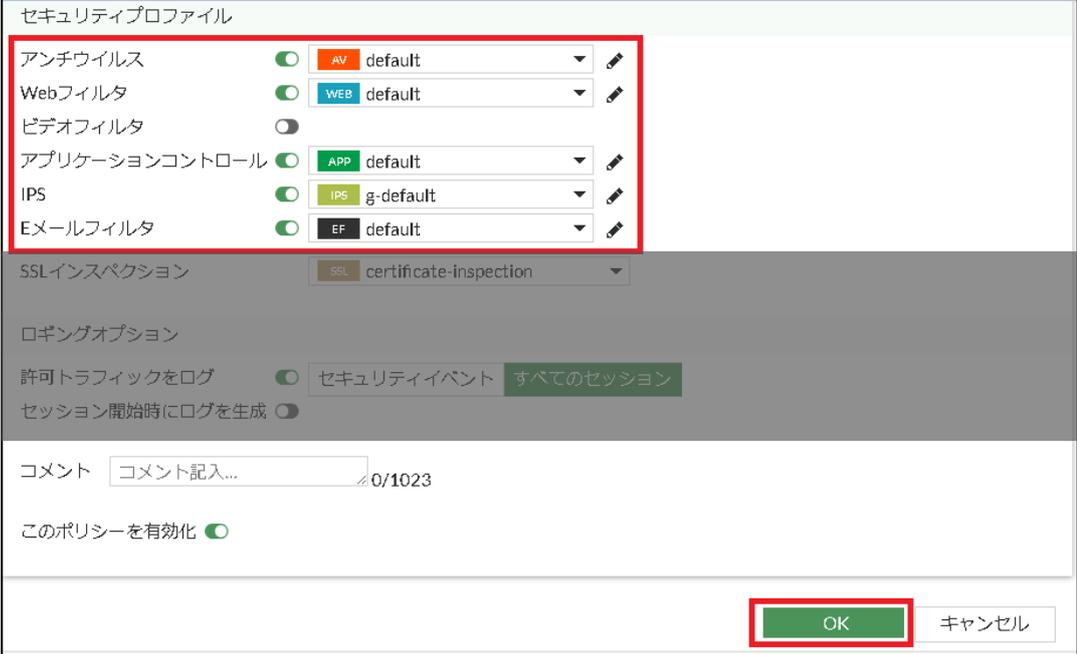


- ② セキュリティ機能を有効化するルールをダブルクリックする。

名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト	タイプ
LAN (port18:vlan101) → WAN (vlan2001:emv1) 10										
dnat test	192.168.0.0/16	test	always	ALL	許可	160.248.241.1/32	no-inspection	すべて	0 B	スタンダード
Src Black Rule	Src Black list	all	always	ALL	拒否			すべて	0 B	スタンダード
Dst Black Rule	all	Dst Black list	always	ALL	拒否			すべて	0 B	スタンダード
Src White Rule	Src White list	all	always	ALL	許可	160.248.241.1/32	no-inspection	すべて	0 B	スタンダード
Dst White Rule	all	Dst White list	always	ALL	許可	160.248.241.1/32	no-inspection	すべて	0 B	スタンダード
ALL_CMP	all	all	always	ALL_CMP	許可	160.248.241.1/32	no-inspection	すべて	0 B	スタンダード
test	all	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて	37.67 MB	スタンダード
LAN→WAN	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて	5.04 MB	スタンダード
192.168.0.0/24 deny	192.168.0.0/16	all	always	ALL	拒否			すべて	0 B	スタンダード
192.168.0.0/24 permit	192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	certificate-inspection	すべて	0 B	スタンダード
WAN (vlan2001:emv1) → LAN (port18:vlan101) 1										
test1	all	all	always	ALL	許可	有効化済み	no-inspection	UTM	0 B	スタンダード

- ③ セキュリティプロファイルより有効化したいセキュリティ機能のトグルを有効化し、default が選択されていることを確認し、OK を押下する。

※侵入防止（IPS）を有効化する場合は g-default を選択すること



セキュリティプロファイル

アンチウイルス	<input checked="" type="checkbox"/>	AV	default
Webフィルタ	<input checked="" type="checkbox"/>	WEB	default
ビデオフィルタ	<input type="checkbox"/>		
アプリケーションコントロール	<input checked="" type="checkbox"/>	APP	default
IPS	<input checked="" type="checkbox"/>	IPS	g-default
Eメールフィルタ	<input checked="" type="checkbox"/>	EF	default

SSLインスペクション SSL certificate-inspection

ロギングオプション

許可トラフィックをログ  セキュリティイベント  すべてのセッション

セッション開始時にログを生成

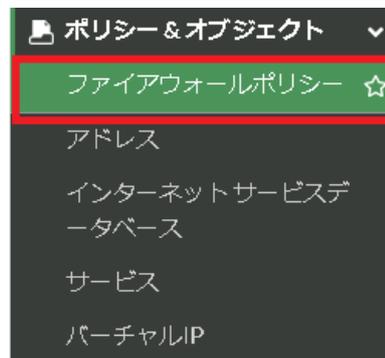
コメント  0/1023

このポリシーを有効化

OK キャンセル

### 13.2 各セキュリティ機能の無効化

- ① 左メニューより、ポリシー&オブジェクト→ファイアウォールポリシーを選択する。



② セキュリティ機能を無効化するルールをダブルクリックする。

名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト	タイプ
LAN (port18.vlan101) → WAN (vlan2001.emv1) 10										
dnat test	192.168.0.0/16	test	always	ALL	許可	160.248.241.1/32	no-inspection	すべて	0 B	スタンダード
Src Black Rule	Src Black list	all	always	ALL	拒否			すべて	0 B	スタンダード
Dst Black Rule	all	Dst Black list	always	ALL	拒否			すべて	0 B	スタンダード
Src White Rule	Src White list	all	always	ALL	許可	160.248.241.1/32	no-inspection	すべて	0 B	スタンダード
Dst White Rule	all	Dst White list	always	ALL	許可	160.248.241.1/32	no-inspection	すべて	0 B	スタンダード
ALL_ICMP	all	all	always	ALL_ICMP	許可	160.248.241.1/32	no-inspection	すべて	0 B	スタンダード
test	all	all	always	ALL	許可	160.248.241.1/32	default AV default WEB default APP default SSL certificate-inspection	すべて	37.67 MB	スタンダード
LAN→WAN	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	すべて	5.04 MB	スタンダード
192.168.0.0/24 deny	192.168.0.0/16	all	always	ALL	拒否			すべて	0 B	スタンダード
192.168.0.0/24 permit	192.168.0.0/16	all	always	ALL	許可	160.248.241.1/32	certificate-inspection	すべて	0 B	スタンダード
WAN (vlan2001.emv1) → LAN (port18.vlan101) 1										
test1	all	all	always	ALL	許可		no-inspection	UTM	0 B	スタンダード
増添 1										

③ セキュリティプロファイルより無効化したいセキュリティ機能のトグルを無効化し、OK を押下する。

セキュリティプロファイル

- アンチウイルス
- Webフィルタ
- ビデオフィルタ
- アプリケーションコントロール
- IPS
- Eメールフィルタ

SSLインスペクション SSL certificate-inspection

ロギングオプション

許可トラフィックをログ  セキュリティイベント  すべてのセッション

セッション開始時にログを生成

コメント  0/1023

このポリシーを有効化

OK
キャンセル

## 14 ダッシュボード

本章では、ダッシュボードにセットされているウィジェットの見方について解説しています。  
 ※左メニューのダッシュボード→ステータスより確認

### 14.1 ウィジェット

#### ① 表示時間の変更

プリセットされているウィジェットは表示する時間幅を変更することができます。  
 変更したいウィジェットの右上にある時間のプルダウンから時間を変更できます。

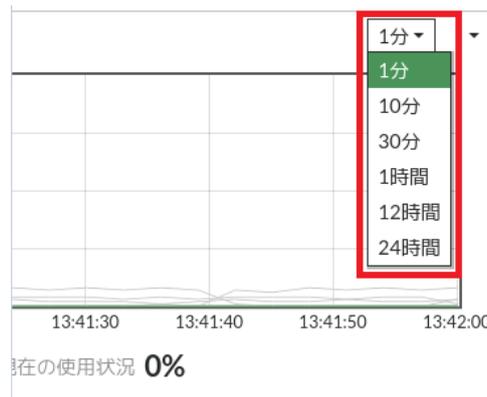
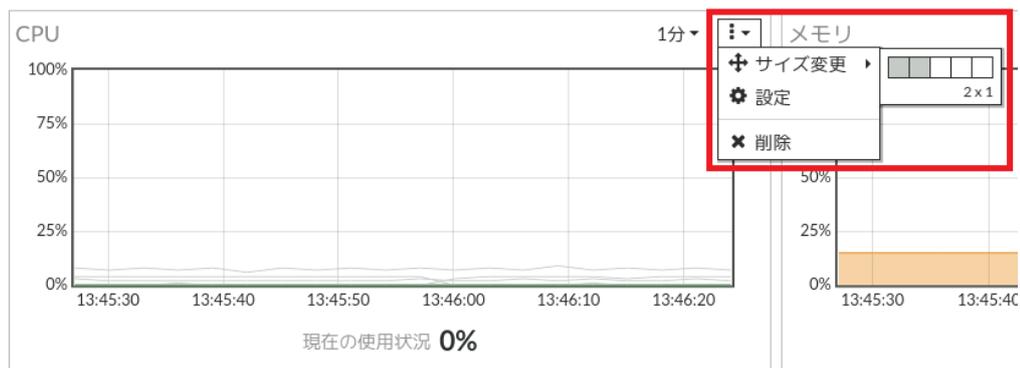


図 14-1. ウィジェット設定画面.

#### ② 表示サイズの変更

プリセットされているウィジェットは表示する画面サイズを変更することができます。  
 変更したいウィジェットの右上にある縦三点リーダーのプルダウンからサイズ変更を選択し  
 表示サイズを変更する。



## 15 FortiView

本章では、FortiView で確認できる通信について解説しています。

左メニューのダッシュボードよりそれぞれのFortiViewのメニューを選択することで「送信元」「宛先」「アプリケーション」「Web サイト」「ポリシー」「セッション」の通信状況を確認することができます。主に上位4メニューを確認していただくと通信状況がわかります。

※参照する際は UTM に多少負荷がかかる場合が有り表示されるまで数分かかりますので、頻繁に見るのはご遠慮ください。



### 15.1 FortiView 送信元

各端末の送信元 IP 別に、デバイス、脅威スコア（UTM によってブロックされたスコア）、バイト数、セッション数の確認ができます。

右上に時間のプルダウンがありますので、直近から最大 7 日間の情報を閲覧することが可能です。

### 15.2 FortiView 宛先

宛先 IP 別にアプリケーション（HTTPS、TCP、UDP など）、バイト数、セッション数の確認ができます。

右上に時間のプルダウンがありますので、直近から最大 7 日間の情報を閲覧することが可能です。

### 15.3 FortiView アプリケーション

アプリケーション別にカテゴリ、リスク、バイト数、セッション数の確認ができます。

右上に時間のプルダウンがありますので、直近から最大 7 日間の情報を閲覧することが可能です。

### 15.4 FortiView Web サイト

ドメイン別にカテゴリ、ブラウズ時間、脅威スコア、バイト数、セッション数の確認ができます。

右上に時間のプルダウンがありますので、直近から最大 7 日間の情報を閲覧することが可能です。

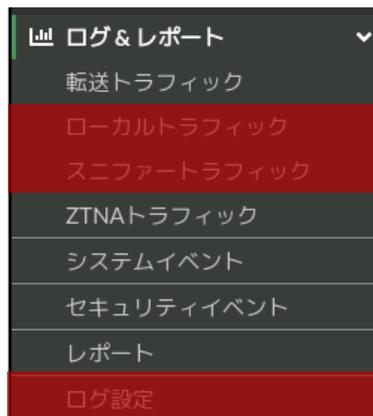
## 16 ログ&レポート

本章では、UTMの通信ログを確認、取得する方法の解説をしています。

それぞれのメニューを選択することで「転送トラフィック」「イベント」「アンチウイルス」「Webフィルタ」「SSL」「アプリケーションコントロール」「IPS(侵入防止)」「アンチスパム(Eメールフィルタ)」の通信ログを確認することができます。

※赤色の網掛け部分に関しては設定変更をしないでください。

設定変更された場合動作保証は致しかねます。



## 16.1 転送トラフィックログ

UTM を通過しようとするすべてのトラフィックログを確認できます。

アクセスしたい Web サイト等にアクセスできない場合などはまずこちらのログを確認してください。

主に確認できる内容は以下です。

- UTM を通過した日時
- 送信元情報
- 宛先情報
- アプリケーション情報
- データ量の情報
- アクション情報（通信が通過したかブロックされたか、どのルールで通過したか）
- セキュリティレベル情報
- セルラー
- その他

送信元、宛先、アクションを確認することにより、該当の通信の通信状況を確認することが可能です。

アクションを確認することにより対象通信が、許可（通信の通過）、ブロック（通信の遮断）されたかを確認することができます。

また、アプリケーションコントロールを確認することによりどのアプリケーションに対して通信を行おうとしているかが確認可能です。

日付/時刻		送信元	デバイス	宛先	アプリケーション名	結果
4 分前		192.168.0.2	 30:7c:5efa:8c:02	 20.189.173.12 (v10.events.data.microsoft.com)	 Microsoft.Portal	✔ 6.53 kB / 6.05 kB
4 分前		192.168.0.2	 30:7c:5efa:8c:02	 20.189.173.12 (v10.events.data.microsoft.com)	 Microsoft.Portal	✔ 768 B / 0 B
5 分前		192.168.0.2	 30:7c:5efa:8c:02	 188.172.201.136 (router6.teamviewer.com)	 TeamViewer	✔ 442.89 kB / 356.79 kB
5 分前		192.168.0.2	 30:7c:5efa:8c:02	 210.150.254.130	 DNS	✔ 75 B / 205 B
5 分前		192.168.0.2	 30:7c:5efa:8c:02	 210.150.254.130	 DNS	✔ 75 B / 205 B

## 16.2 セキュリティイベント

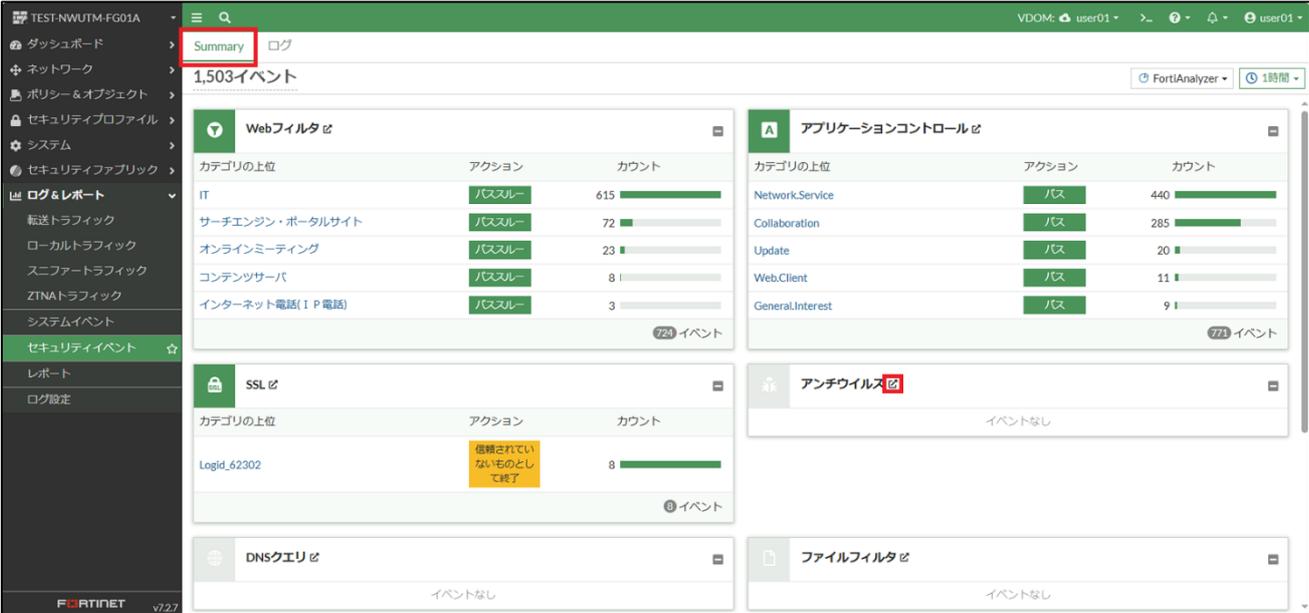
「セキュリティイベント」からそれぞれの項目についてのログを見ることができます。

- ① 左メニューより、ログ&レポート→セキュリティイベントを選択する。



- ② Summary タブまたはログタブからそれぞれのログを見る。

- i. Summary タブを押下し対象のイベントの右側にあるポップアップボタンを押下

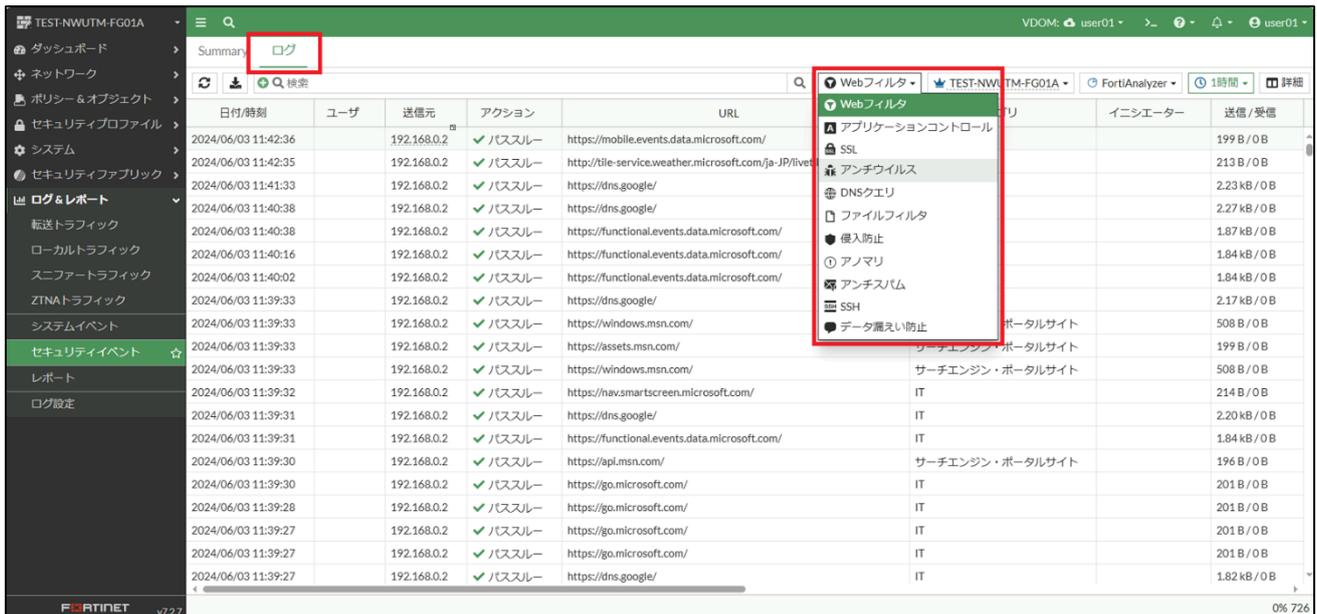


カテゴリの上位	アクション	カウント
IT	パススルー	615
サーチエンジン・ポータルサイト	パススルー	72
オンラインミーティング	パススルー	23
コンテンツサーバ	パススルー	8
インターネット電話 (IP 電話)	パススルー	3
724 イベント		

カテゴリの上位	アクション	カウント
Network.Service	パス	440
Collaboration	パス	285
Update	パス	20
Web.Client	パス	11
General.Interest	パス	9
771 イベント		

カテゴリの上位	アクション	カウント
Logid_62302	接続されていないものとして終了	8
8 イベント		

## ii. ログタブを押下し検索窓の右にあるプルダウンから対象のイベントを選択



The screenshot shows the FortiAnalyzer interface. In the top-left navigation pane, the 'ログ' (Log) tab is highlighted with a red box. In the top-right search area, a dropdown menu is open, also highlighted with a red box, showing various event categories such as 'Webフィルタ', 'アプリケーションコントロール', 'SSL', 'アンチウイルス', 'DNSクエリ', 'ファイルフィルタ', '侵入防止', 'アナマリ', 'アンチスパム', 'SSH', and 'データ漏えい防止'. The main table below displays a list of security events with columns for date/time, user, source IP, action, URL, and traffic volume.

日付/時刻	ユーザ	送信元	アクション	URL	送信/受信
2024/06/03 11:42:36		192.168.0.2	✓ パススルー	https://mobile.events.data.microsoft.com/	
2024/06/03 11:42:35		192.168.0.2	✓ パススルー	http://tile-service.weather.microsoft.com/ja-JP/live/	
2024/06/03 11:41:33		192.168.0.2	✓ パススルー	https://dns.google/	
2024/06/03 11:40:38		192.168.0.2	✓ パススルー	https://dns.google/	
2024/06/03 11:40:38		192.168.0.2	✓ パススルー	https://functional.events.data.microsoft.com/	
2024/06/03 11:40:16		192.168.0.2	✓ パススルー	https://functional.events.data.microsoft.com/	
2024/06/03 11:40:02		192.168.0.2	✓ パススルー	https://functional.events.data.microsoft.com/	
2024/06/03 11:39:33		192.168.0.2	✓ パススルー	https://dns.google/	
2024/06/03 11:39:33		192.168.0.2	✓ パススルー	https://windows.msn.com/	
2024/06/03 11:39:33		192.168.0.2	✓ パススルー	https://assets.msn.com/	
2024/06/03 11:39:33		192.168.0.2	✓ パススルー	https://windows.msn.com/	
2024/06/03 11:39:32		192.168.0.2	✓ パススルー	https://nav.smartscreen.microsoft.com/	
2024/06/03 11:39:31		192.168.0.2	✓ パススルー	https://dns.google/	
2024/06/03 11:39:31		192.168.0.2	✓ パススルー	https://functional.events.data.microsoft.com/	
2024/06/03 11:39:30		192.168.0.2	✓ パススルー	https://api.msn.com/	
2024/06/03 11:39:30		192.168.0.2	✓ パススルー	https://go.microsoft.com/	
2024/06/03 11:39:28		192.168.0.2	✓ パススルー	https://go.microsoft.com/	
2024/06/03 11:39:27		192.168.0.2	✓ パススルー	https://go.microsoft.com/	
2024/06/03 11:39:27		192.168.0.2	✓ パススルー	https://go.microsoft.com/	
2024/06/03 11:39:27		192.168.0.2	✓ パススルー	https://dns.google/	

以下ではセキュリティイベントで見ることができるログの種類について解説します。

## ① アンチウイルス

アンチウイルスでは、監視設定しているプロトコルのブロックされた通信を確認することが可能です。

確認できる項目は下記 8 項目です。

- 日付/時刻
- サービス
- 送信元
- ファイル名
- ウイルス/ボットネット
- ユーザ
- 詳細
- アクション

## ② Web フィルタ

Web フィルタでは、ファイアウォールルールを通過した http または https の通信を確認することができます。

アクションを確認することにより対象通信が、通過 (passthrough)、遮断 (blocked) されたかを確認することができます。

対象トラフィックを選択し詳細を押下することにより、下記の詳細な項目を確認することができます。

- 一般
- 送信元
- 宛先
- アプリケーションコントロール
- データ
- アクション
- セキュリティ
- セルラー
- Web フィルタ
- その他

送信元、宛先、URL、アクションを確認することにより、該当の通信の状況を確認することが可能です。

また、カテゴリ説明を確認することによりどのカテゴリに分類されているか確認することが可能です。

日付/時刻	ユーザ	送信元	アクション	URL	カテゴリ説明	イニシエーター	送信/受信
4分前		192.168.0.2	passthrough	https://smartscreen-prod.microsoft.com/	IT		517 B / 0 B
4分前		192.168.0.2	passthrough	https://smartscreen-prod.microsoft.com/	IT		517 B / 0 B
4分前		192.168.0.2	passthrough	https://settings-win.data.microsoft.com/	IT		214 B / 0 B
4分前		192.168.0.2	passthrough	http://ping.monitor.nttpc.info/	未分類		77 B / 0 B
4分前		192.168.0.2	passthrough	http://ping.monitor.nttpc.info/	未分類		77 B / 0 B

### ③ アプリケーションコントロール

アプリケーションコントロールでは、Web アプリケーションへの通信状況を確認することが可能です。

アクションを確認することにより対象通信が、通過 (pass)、遮断 (block) されたかを確認することができます。

対象トラフィックを選択し詳細を押下することにより、下記の詳細な項目を確認することができます。

- 一般
- 送信元
- 宛先
- アプリケーションコントロール
- アクション
- セキュリティ
- セルラー
- その他

送信元、宛先、アプリケーション、アクションを確認することにより、該当の通信の状況が確認することが可能です。

日付/時刻	送信元	宛先	アプリケーション名	アクション	アプリケーションユーザ	アプリケーション詳細
5 分前	192.168.0.2	51.11.168.232 (settings-win.data.microsoft.com)	MS.Windows.Update	pass		
5 分前	192.168.0.2	40.90.184.82 (smartscreen-prod.microsoft.com)	Microsoft.Portal	pass		
5 分前	192.168.0.2	40.90.184.82 (smartscreen-prod.microsoft.com)	Microsoft.Portal	pass		
6 分前	192.168.0.2	18.182.170.25 (ping.monitor.nttpc.info)	HTTP.BROWSER	pass		

#### ④ IPS（侵入防止）

IPSでは、不正アクセスをしようとする端末の通信状況を確認することが可能です。

アクションを確認することにより対象通信が、検知（detected）、遮断（dropped）されたかを確認することができます。

対象トラフィックを選択し詳細を押下することにより、下記の詳細な項目を確認することができます。

- 一般
- 送信元
- 宛先
- アプリケーションコントロール
- アクション
- セキュリティ
- セルラー
- 侵入防止
- その他

#### ⑤ アンチスパム（Eメールフィルタ）

アンチスパムでは、送られてきたメールの受信状態を確認することが可能です。

アクションを確認することにより対象が、免除（exempted）、タグ付け（tagged）されたかを確認することができます。

対象トラフィックを選択し詳細を押下することにより、下記の詳細な項目を確認することができます。

- 一般
- 送信元
- 宛先
- アプリケーションコントロール
- アクションセキュリティ
- セルラー
- アンチスパムフィルタ
- その他

日付..	ユーザ	送信元	From	To	サブジェクト	アクション
1時間前		192.168.10.10				exempted
1時間前		192.168.10.10				exempted
1時間前		192.168.10.10				tagged

### 16.3 各種ログの取得方法

各ログメニューの左上にあるダウンロードボタンを押下し、しばらく待つとダウンロードされます。



## 17 リアルタイムレポートの閲覧

UTM の WAN 側、LAN 側の通信状況、セッション数を確認することができます。

リアルタイムレポートを確認するには、開通通知書に記載されている URL、ユーザ ID、パスワードからログインする必要があります。

例 : <https://msp16.nttpc.co.jp/NewReport/>

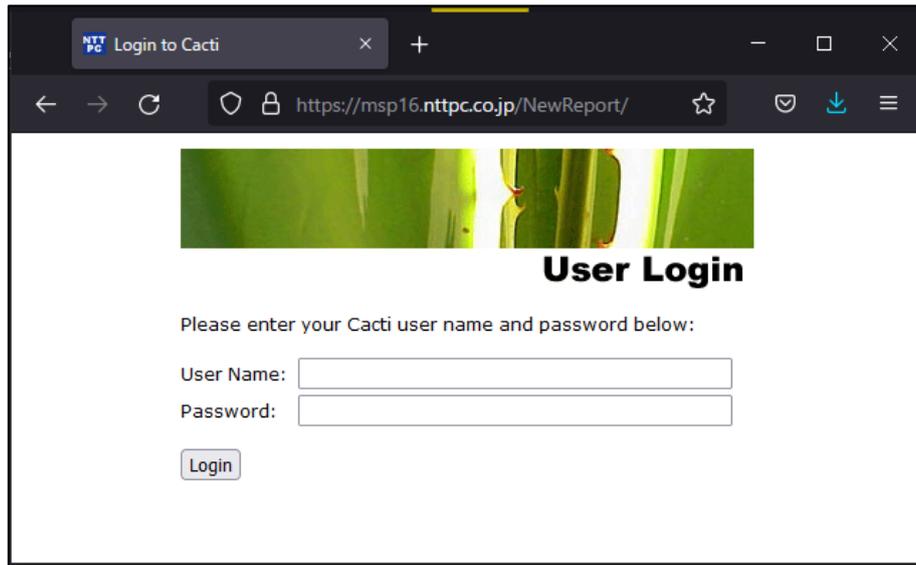


図 17-1. Cacti ログイン画面.

### 17.1 グラフフィルタ

画面上部にあるグラフフィルタより、トラフィック、セッション数を参照したい日時に設定することにより閲覧することが可能となります。

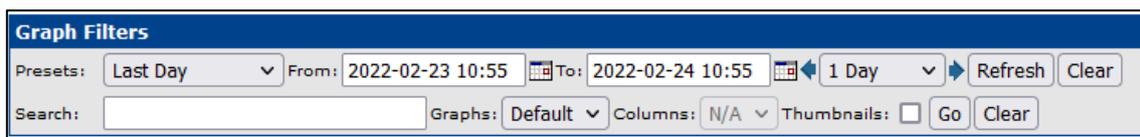


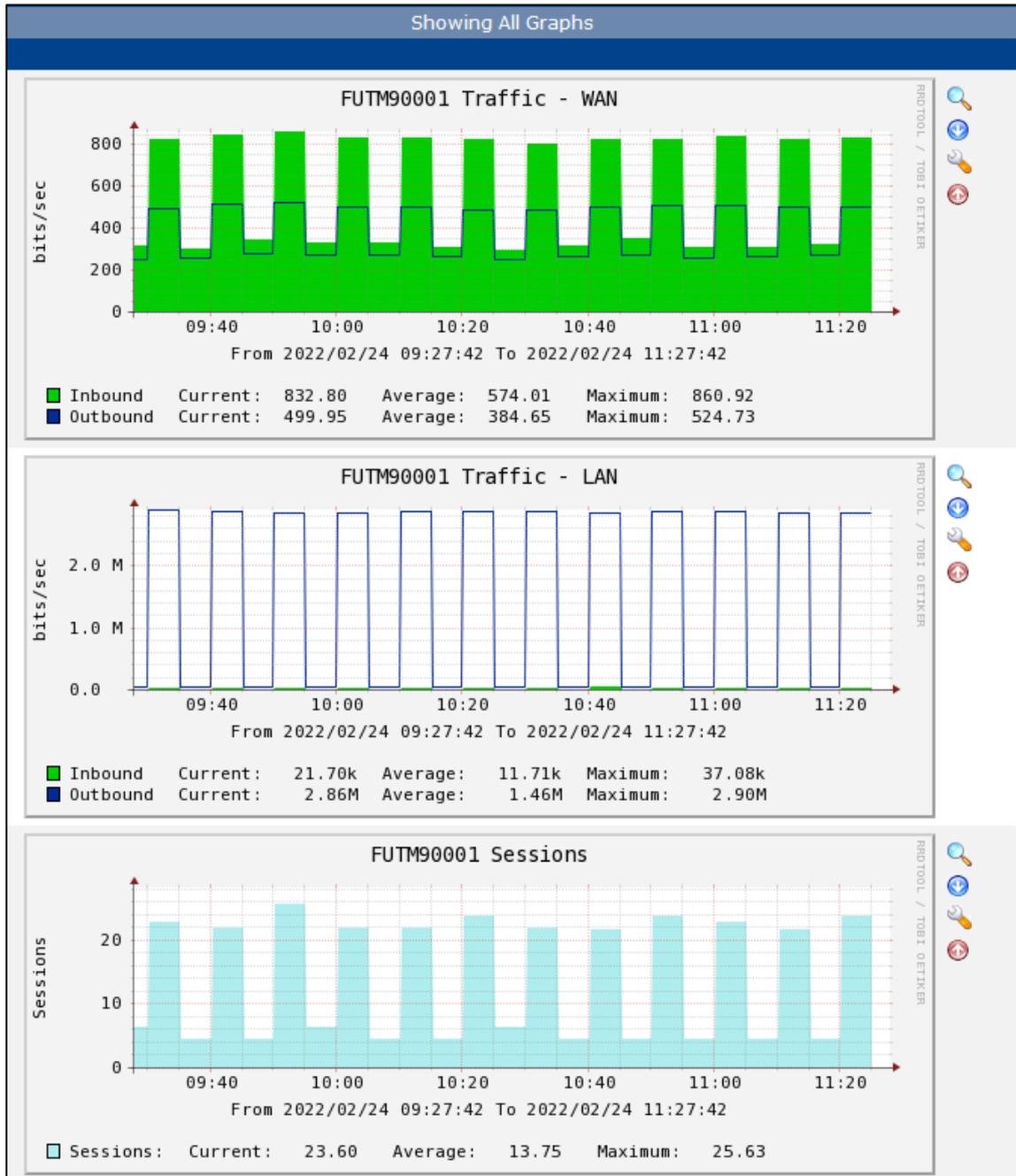
図 17-2. グラフフィルタ設定画面.

参照方法は下記 2 点になります。

- ① Presets のプルダウンから何日間表示させるか選択する。
- ② From、To に日時を入力して、「Refresh」を押下する。

## 17.2 グラフ

グラフフィルタで設定した範囲のトラフィック、セッション数が確認することができます。



トラフィックでは、WAN 側と LAN 側のインバウンドとアウトバウンドの現在、平均、最大の通信状況を確認することができ、セッションでは現在、平均、最大のセッション数を確認することができます。

## 18 Q&A

### ➤ 全般

Q：作業中にブラウザが応答しなくなった。

A：ブラウザをリロードして再読み込みをするか、別の種類のブラウザの使用をお試しください。

### ➤ ファイアウォールアドレス

Q：ポリシー&オブジェクト内のアドレスを削除できない。

A：そのアドレスをグループやポリシーで使用中の場合は削除できません。

最初に使用を解除して下さい。アドレスグループ、サービス、サービスグループについても同様です。

### ➤ ファイアウォールポリシー

Q：ポリシーの編集で、サービスを「HTTP」から「HTTPS」に変更したが、編集後に確認すると、「HTTP」と「HTTPS」の両方が指定されている。

A：ポリシーの編集から、サービスを変更した場合、「変更」ではなく「追加」となるため、名前の右側にある「×」をクリックしてエントリから削除してください。ポリシーのほかの項目、またはアドレスグループ、サービスグループも同様です。

Q：ポリシーが勝手に動いた。

A：ポリシーは、ドラック&ドロップで順番を変更することができます。

その順番によって優先順位が変更されるため、優先順位を変更するとき以外はポリシーを動かさないように注意してください。

Q：ポリシーで通信を拒否したはずなのに、拒否されない。

A：ポリシーは上から順番に評価されます。設定した拒否ポリシーの上側に許可ポリシーがある場合、その許可ポリシーが優先されます。優先順位をご確認ください。