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

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。

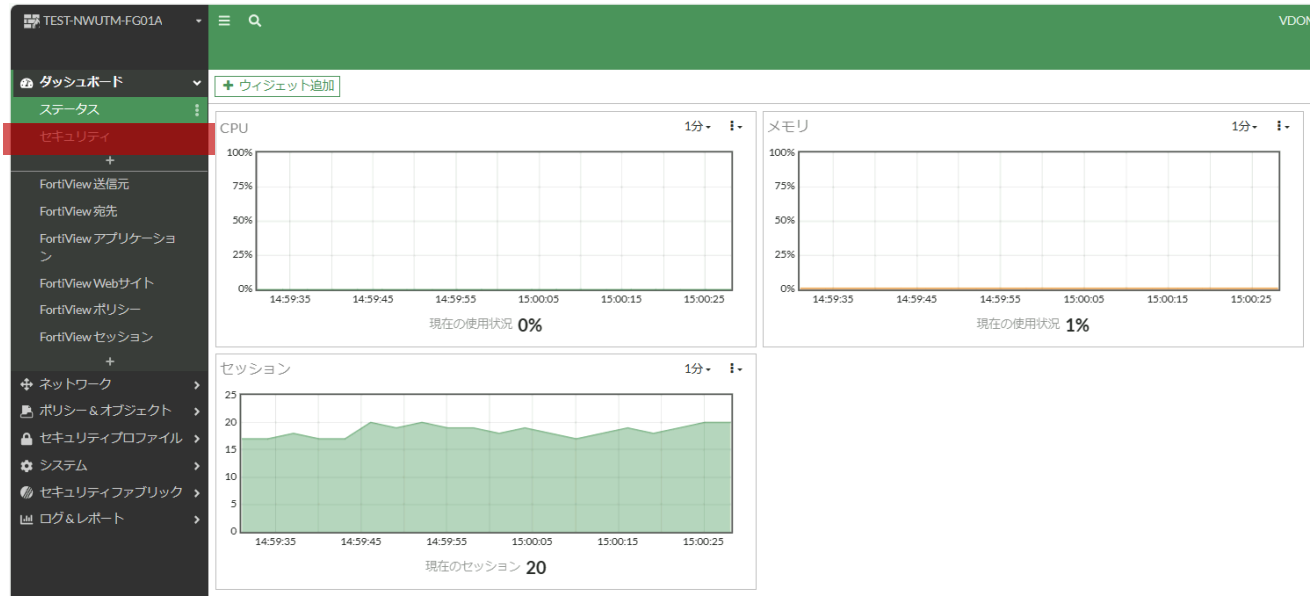
下記箇所を操作すると不具合の原因となりますので行わないでください。

■設定不可な機能

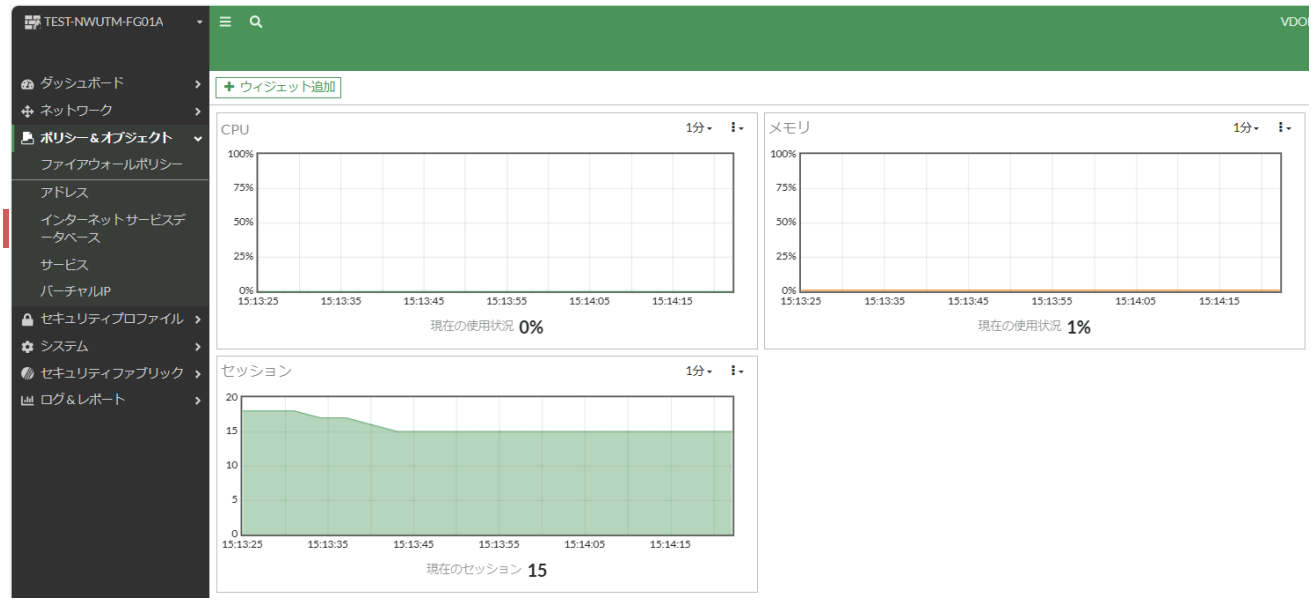
カスタマコントロールで設定不可な機能は以下のとおりです。

※赤で網掛けされた箇所を設定変更しないでください。

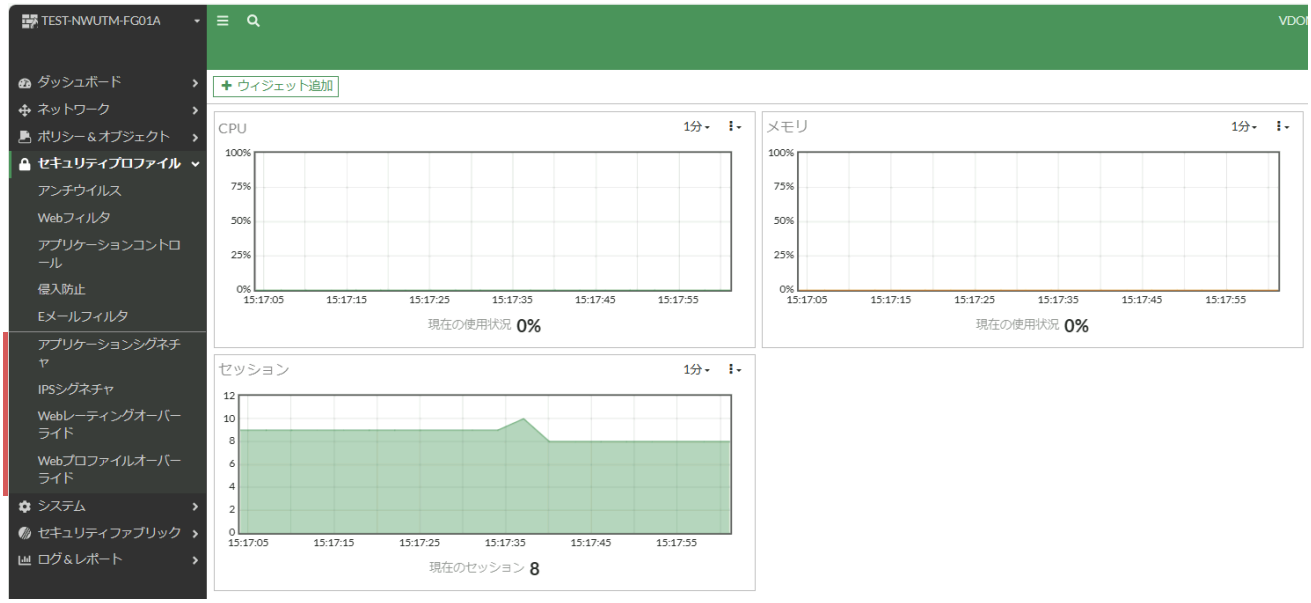
・ダッシュボード



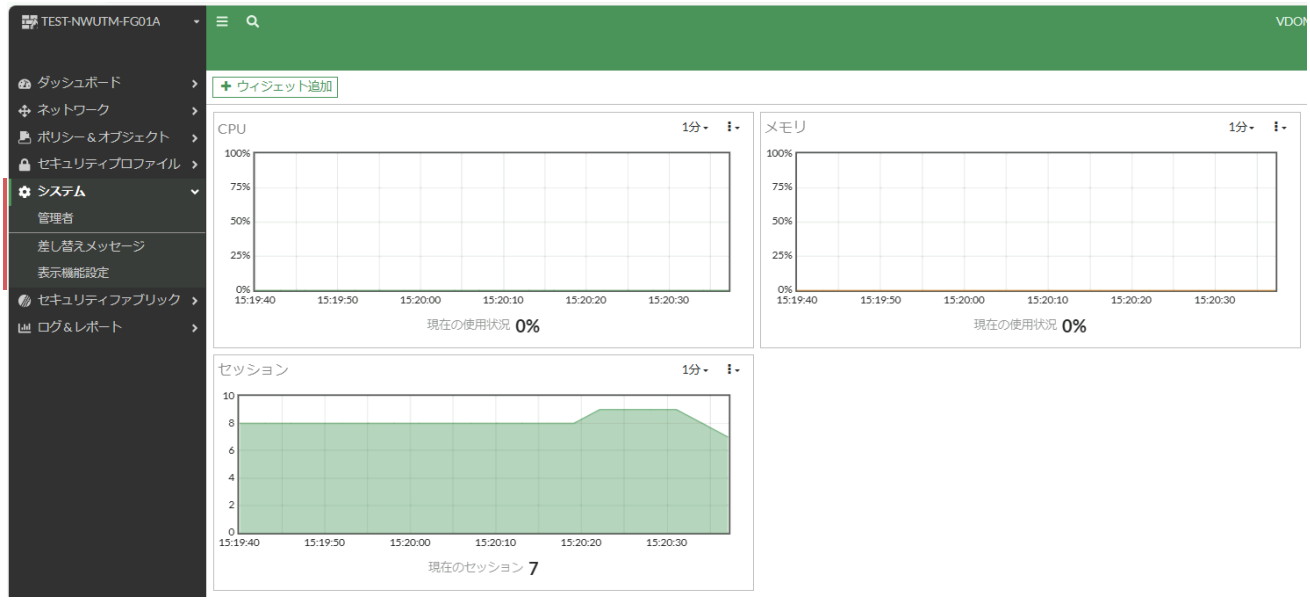
・ポリシー＆オブジェクト



・セキュリティプロファイル

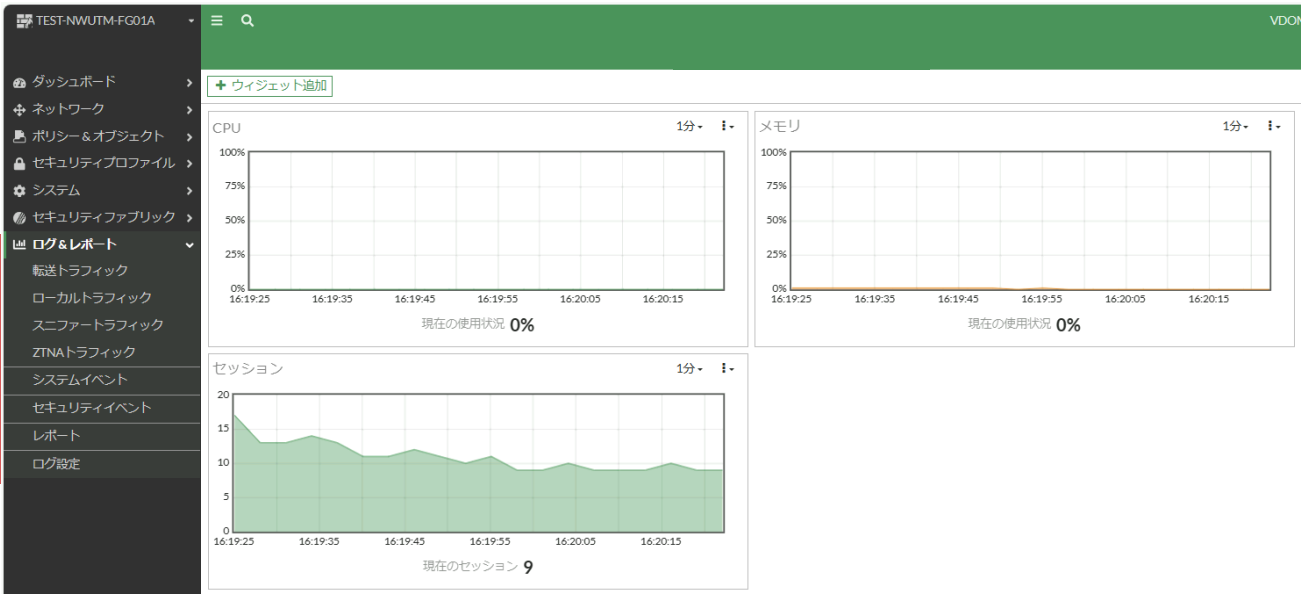


・システム



・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

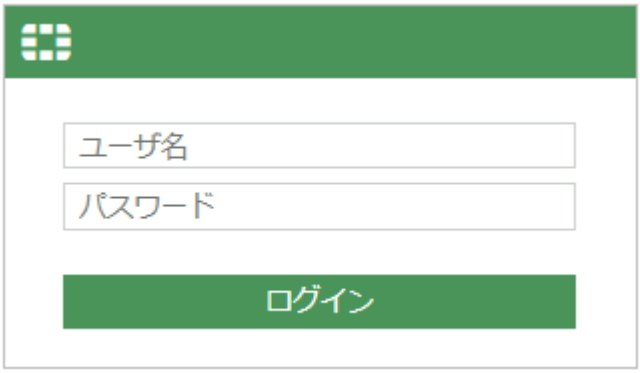
ブラウザから カスタマコントロールの URL にアクセスします。

※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

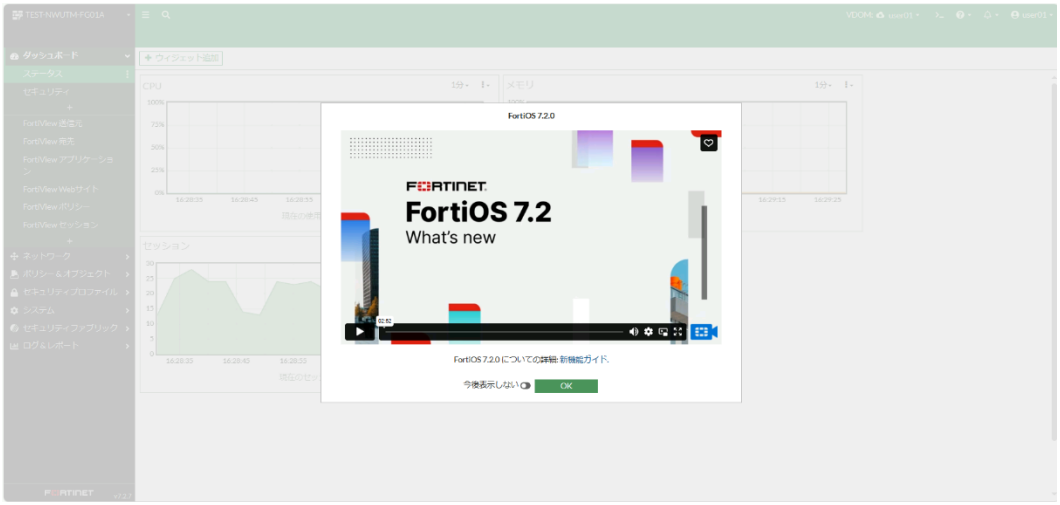
カスタマコントロールサイトのログイン画面が表示されますので、ユーザ名、パスワードを入力し、ログインをクリックします。

※ 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 へはお客さま 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。



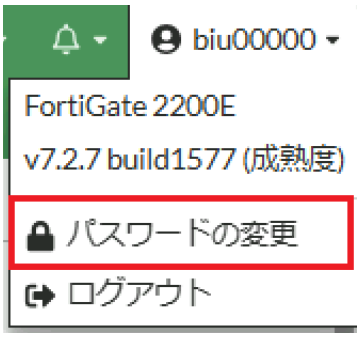
以下のような画面表示となっていれば初回ログイン時の操作は完了です。

2.3　カスタマコントロールサイトのパスワード変更

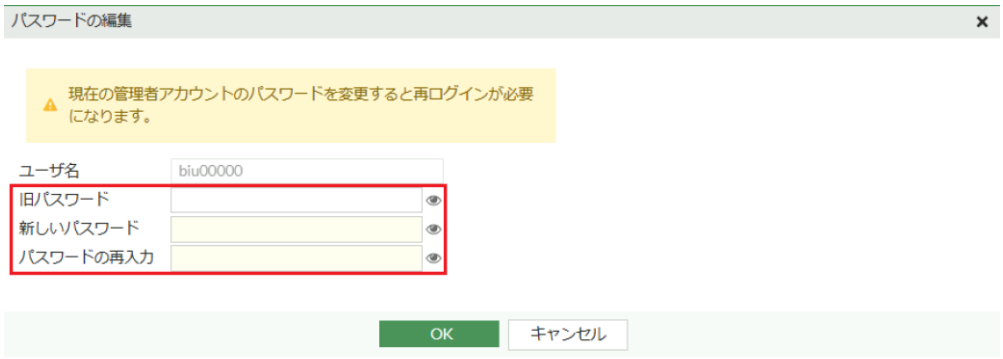
ログイン後、カスタマコントロールサイト右上ユーザ名「biu00000」をクリックします。

※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。



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 NTTPC モニタルール(NTTPC 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 (port18.vlan101) → WAN (vlan2001.emv1)										
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	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 SSL certificate-inspection	すべて	13.64 MB	スタンダード
暗黙										
暗黙の拒否	all	all	always	ALL	拒否			有効化済み	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。

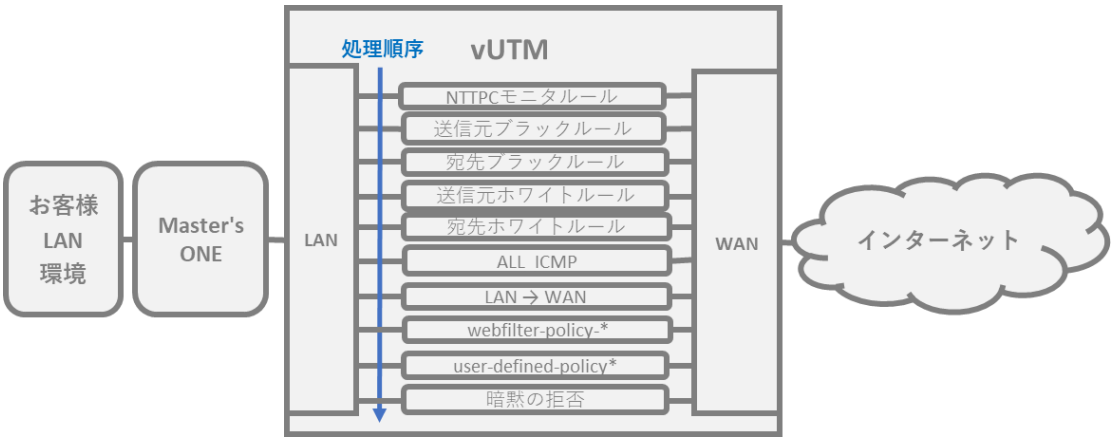


図 3-2. プリセットのファイアウォールポリシー概要図.

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 ルール	- 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。 ※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。	有効
②	送信元ブラックルール	- 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。 - 初期設定時、Src Black list は、空の状態で提供致します。 - 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。	有効
③	宛先ブラックルール	- 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。 - 初期設定時、Dst Black list は、空の状態で提供致します。 - 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。	有効
④	送信元ホワイトルール	- 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。 - 初期設定時、Src White list は、空の状態で提供致します。 - 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。	有効
⑤	宛先ホワイトルール	- 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。 - 初期設定時、Dst White list は、空の状態で提供致します。 - 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。	有効
⑥	ALL_ICMP	- 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。 ※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。	有効
⑦	WindowsUpdate Bandwidth Control	- 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。 ※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。	有効
⑧	LAN→WAN	- 基本となるファイアウォールルールとなります。 - 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。 ※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願います。	有効
⑨	webfilter-policy-*	- 基本となるファイアウォールルールとなります。 - 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。 - 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。	有効
⑩	user-defined-policy*	- 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。	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。

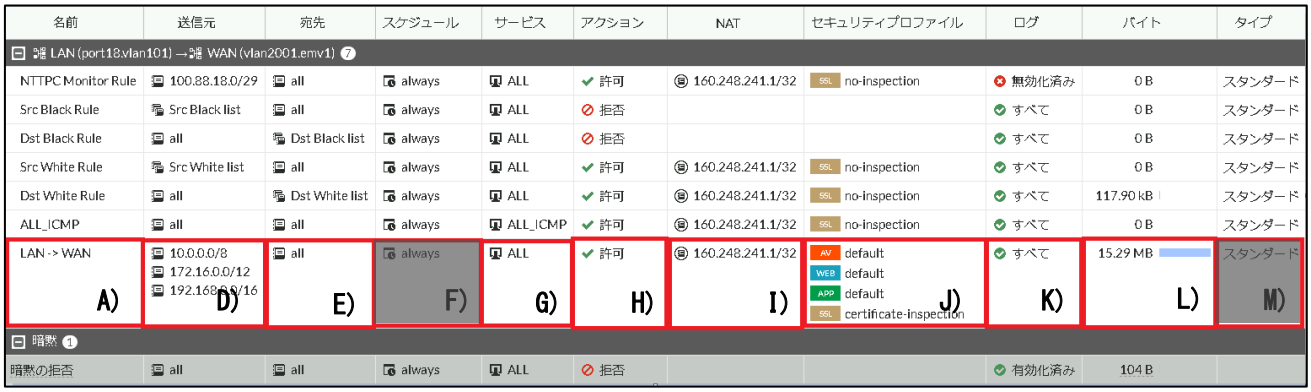


図 3-2.　インターフェースペアビューのファイアウォールポリシー.

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。)

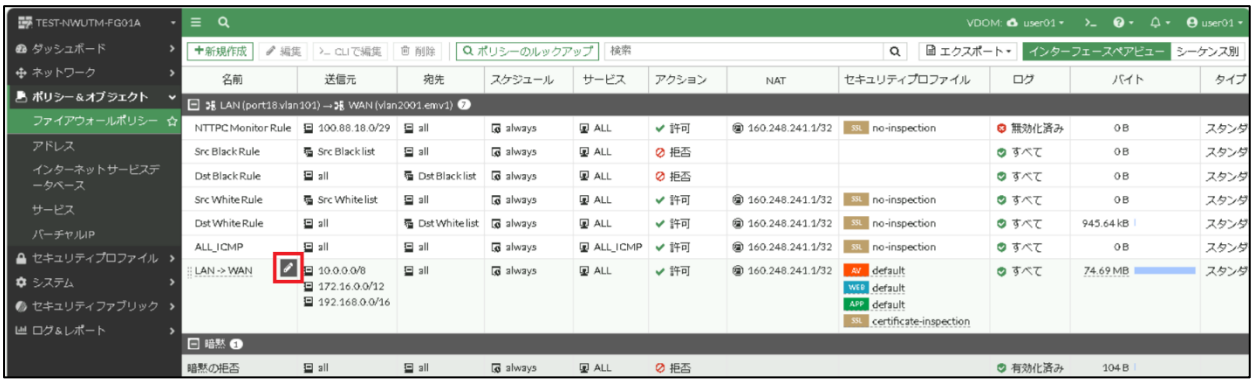
J)　対象の送信元または宛先への通信に対してチェックするセキュリティを設定できます。

K)　ログを取得するか否かが設定されています。

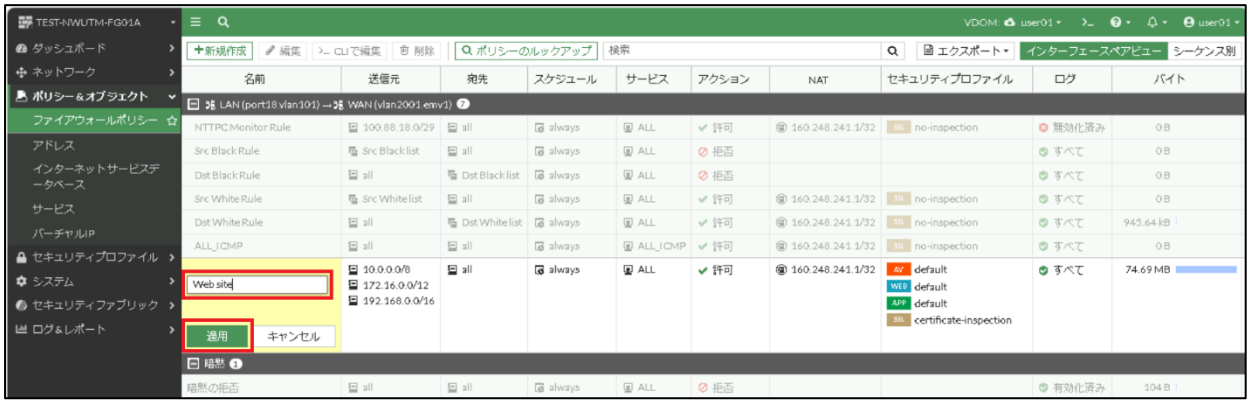
L)　対象のポリシーに合致した通信量が表示されています。

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。

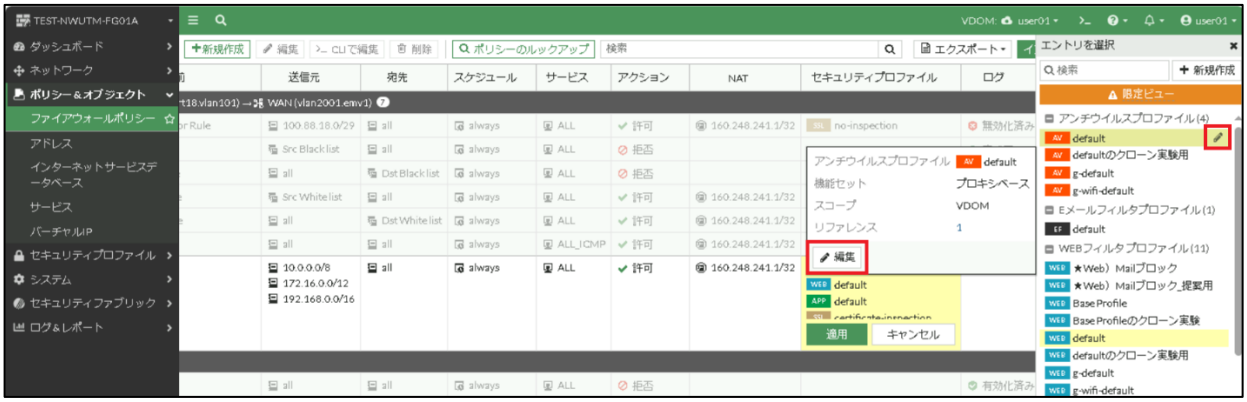


表 3-2. ファイアウォールルールの設定項目.

	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)
		- アンチスパス(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：機器によってかっこ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		
		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‡
			外部マルウェアブロックリストを使用：無効‡

表 3-3. セキュリティ機能概要(2/3).

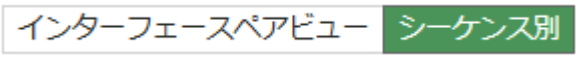
	設定項目	設定内容	デフォルト設定			
2	WEB フィルタ	機能セット	プロキシベース			
		FortiGuard カテゴリベースのフィルタ設定	項目	カテゴリ		
			ローカルカテゴリ：無効	custom1	Custom2	
			違法性の高いサイト：ブロック	薬物乱用	ハッキング	違法または非倫理的
				差別	明示的な暴力	盗作
				児童虐待		
			アダルト/成人コンテンツ：ブロック	その他のアダルトマテリアル	ギャンブル	ヌードとワイセツ
				ポルノ	出会い系	マリファナ
			セキュリティリスクの高いサイト:ブロック	悪意のある Web サイト	フィッシング詐欺	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のチェック　：有効
			スパム報告：有効
		ローカルスパムフィルタリング	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

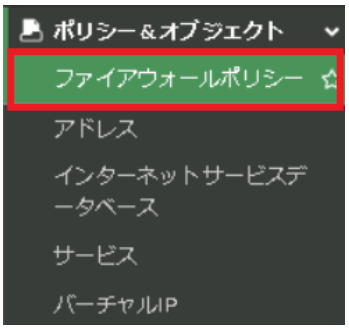
本章では、ファイアウォールルール、NAT の設定方法について解説しています。
ファイアウォールポリシーでは、インターフェースペアビューとシーケンス別の 2 種類の表示方法がありますのでファイアウォールポリシーのメニューを押下後、画面上部の表記を確認してから設定方法をご確認ください。



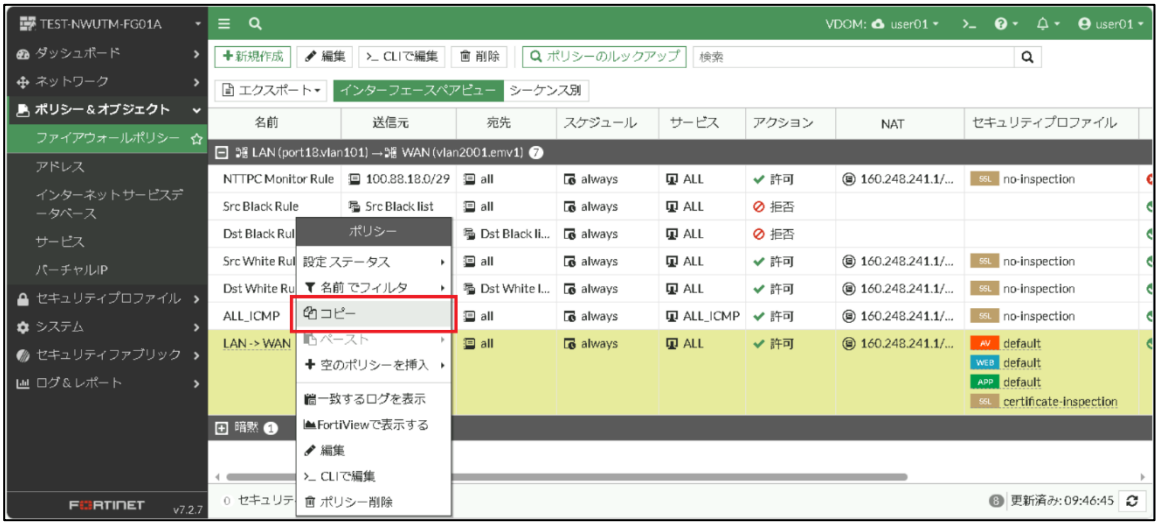
また、表示形式は変更されても構いませんが下記のようにインターフェースペアビューがグレーアウトされて表示切替ができない場合もございます。

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）

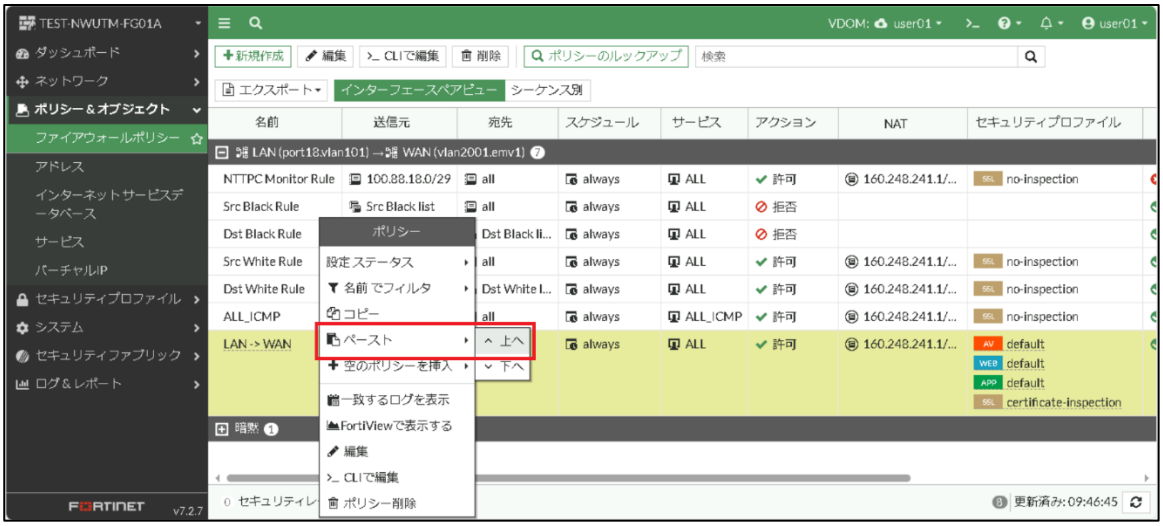
①　左のメニューからポリシー&オブジェクト->ファイアウォールポリシーを選択する。
※ルールの表示がされていない場合は+ボタンを押下して表示させてください。



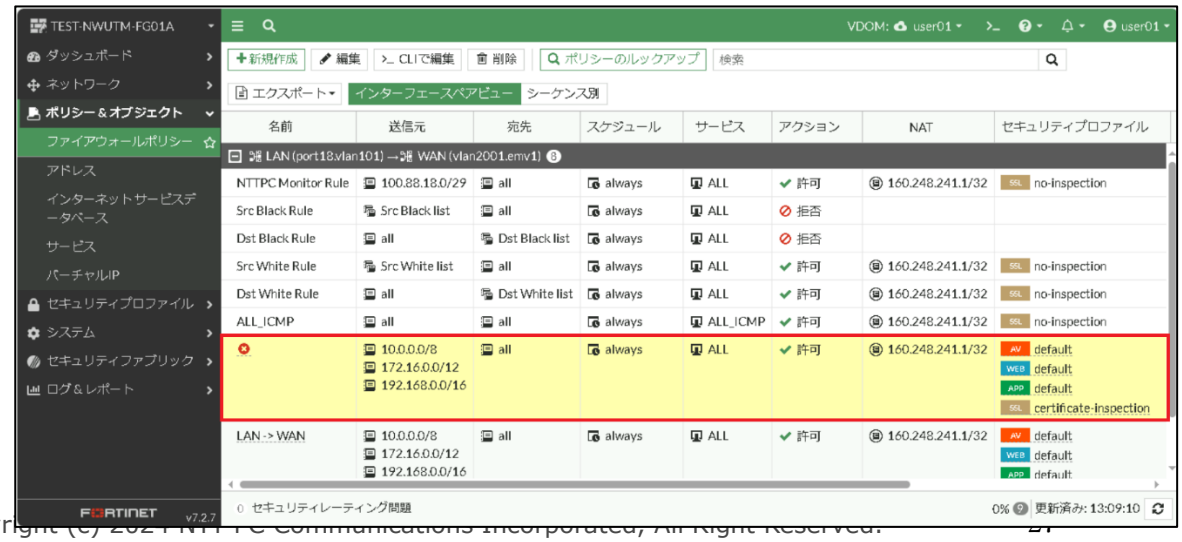
② LAN→WAN 又は、webfilter-policy-*を右クリックし、コピーを押下する。



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。



④ 作成したポリシーをダブルクリックする。

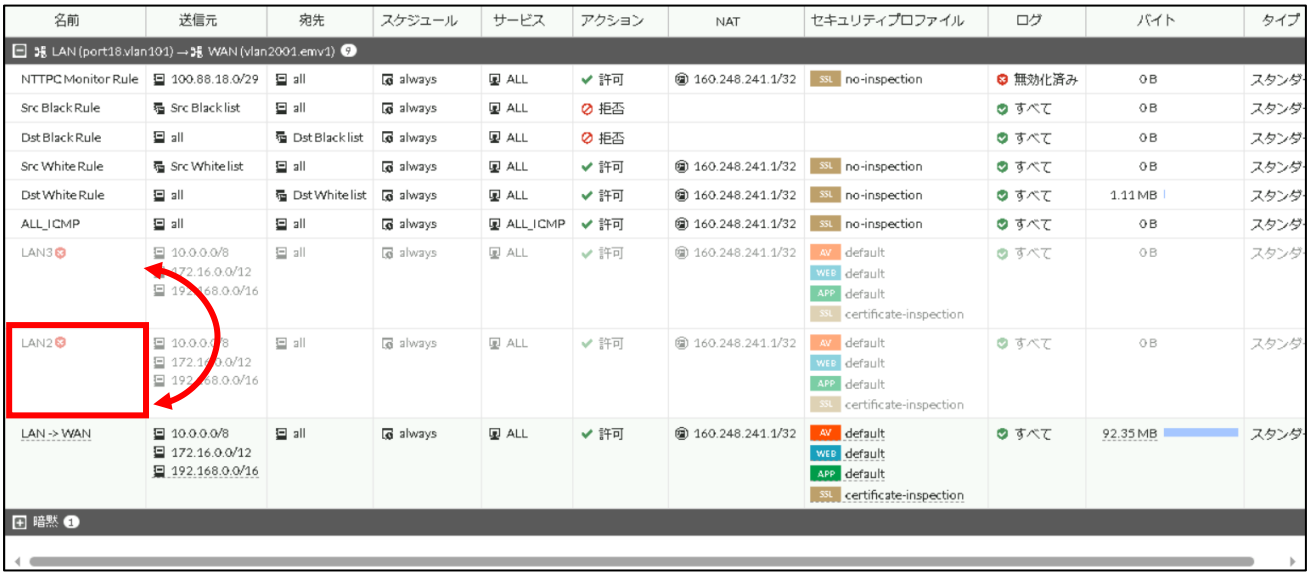


⑤ 名前、送信元、宛先、サービス、セキュリティプロファイルを設定し OK を押下する。
※コメントにコピー元の名前が入るので消すか任意のコメントを記入してください。
※セキュリティプロファイルで使用して良いプロファイルは表 4.1 を参照

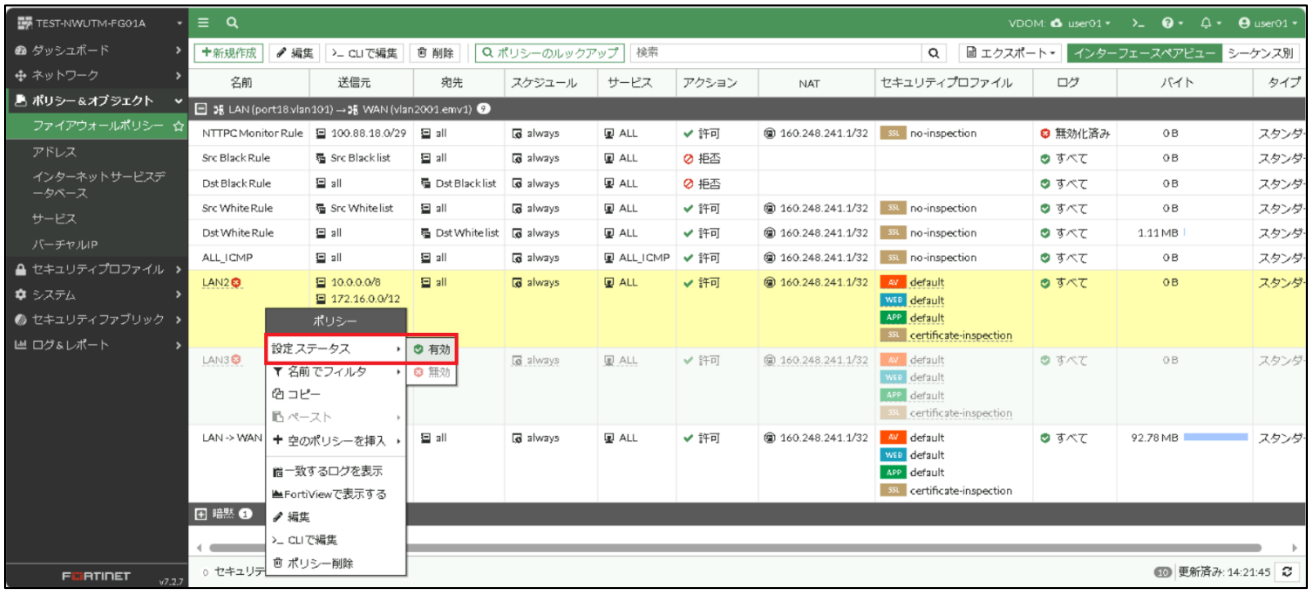
「+」を押下すると右側にリストが表示されるので追加したい分をクリックする。
消すアドレスがある場合は「×」をクリックすると消えます。
送信元、宛先で追加したいものがない場合は 5.1 項を参照
サービスで追加したいものがない場合は 7.1 項を参照

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

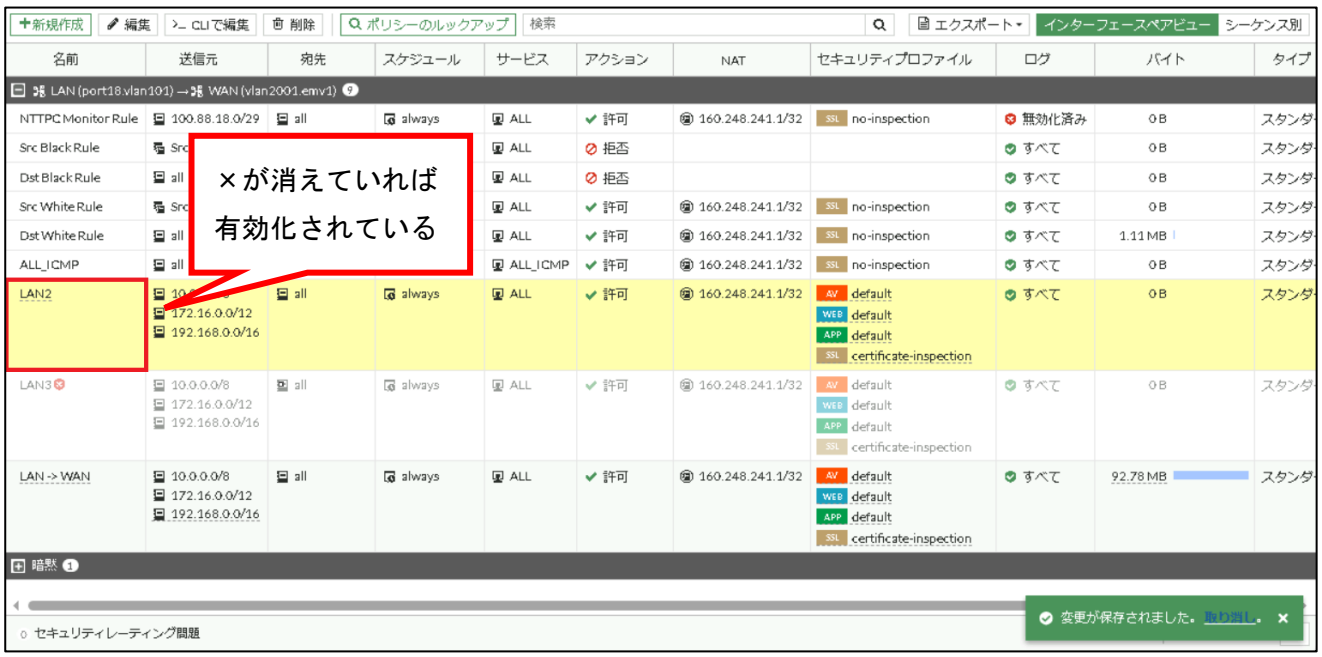
⑥　作成したルールを ALL_ICMP より下の投入したい場所に名前部分でドラッグ&ドロップし移動させる。



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。

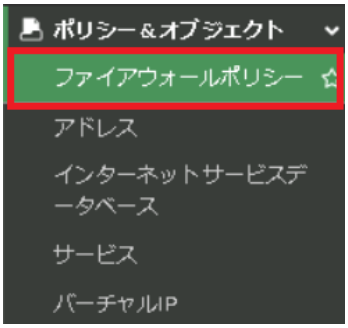


⑧　ルールが有効になったことを確認する。

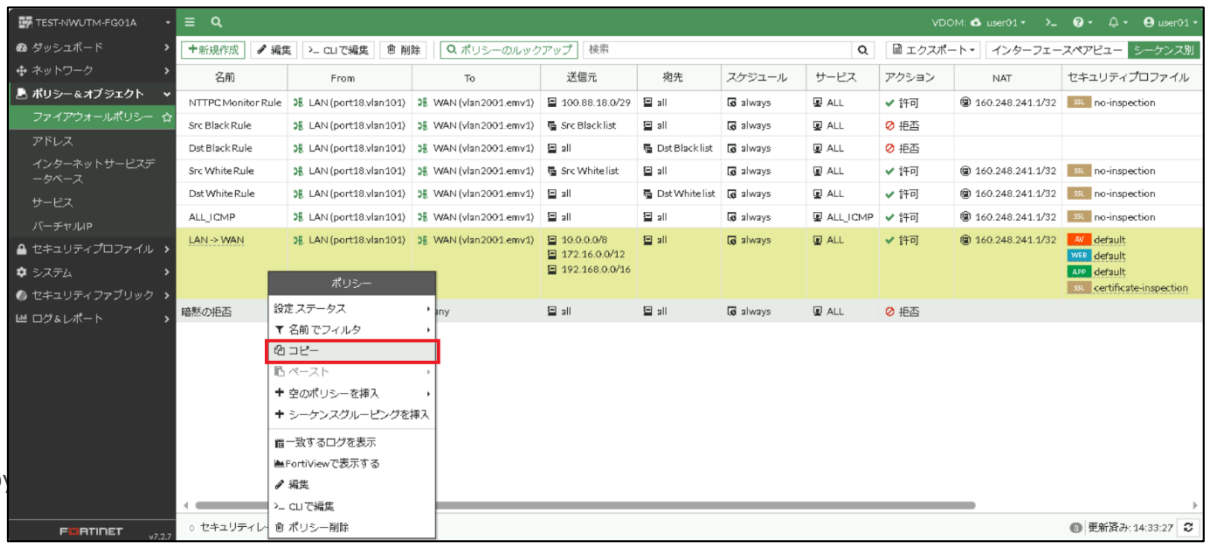


4.2　ファイアウォールルールの追加（表示形式:シーケンス別の場合）

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。

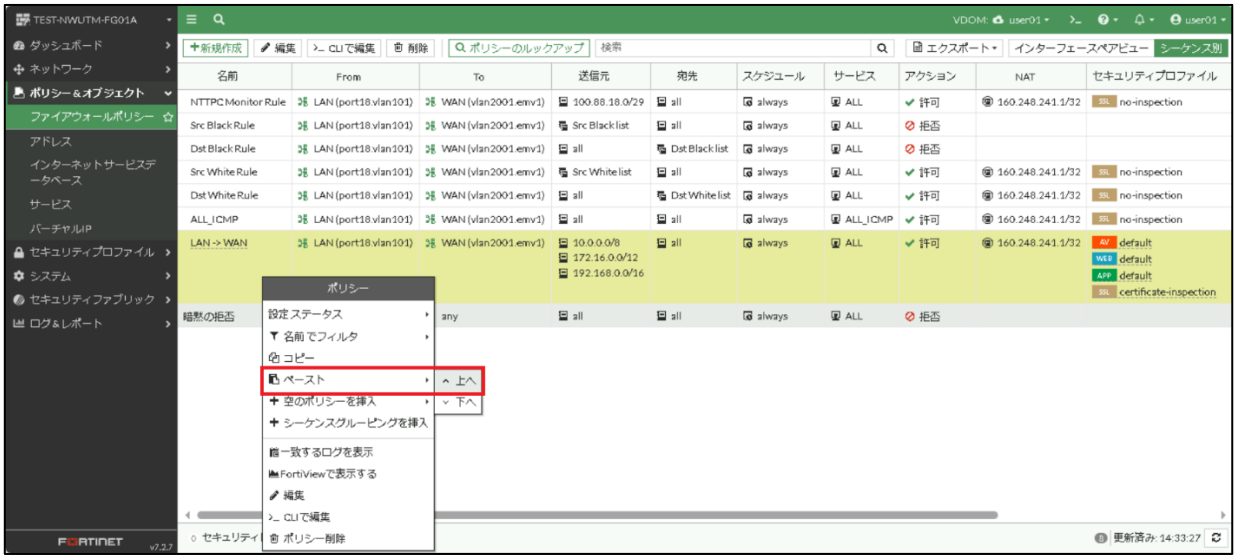


②　LAN→WAN 又は、webfilter-policy-*を右クリックし、コピーを押下する。

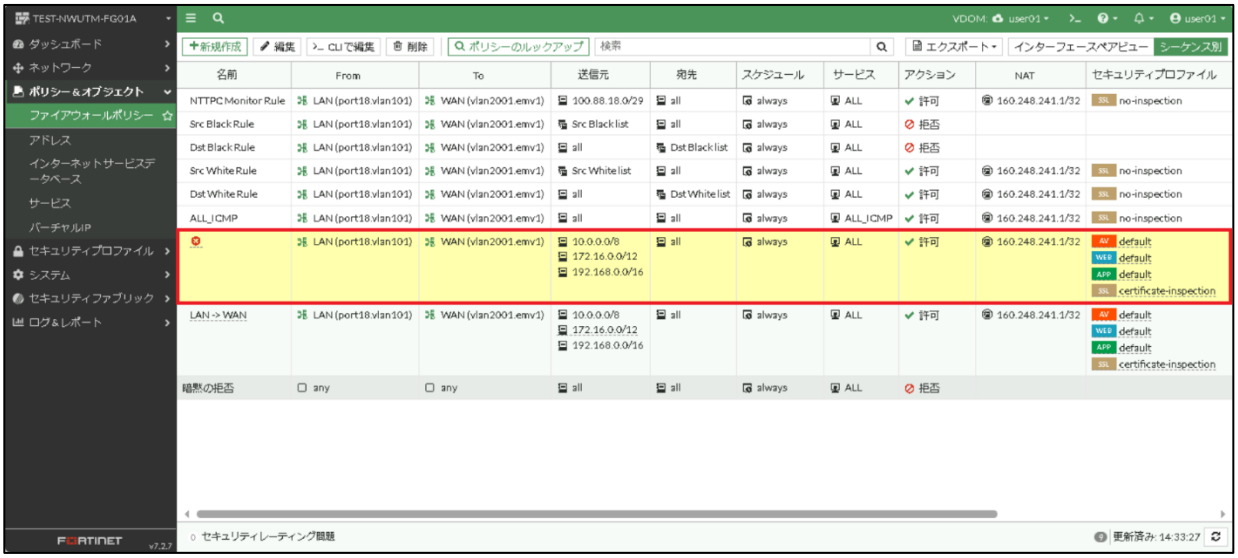


Copy

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。



④　作成したポリシーをダブルクリックする。

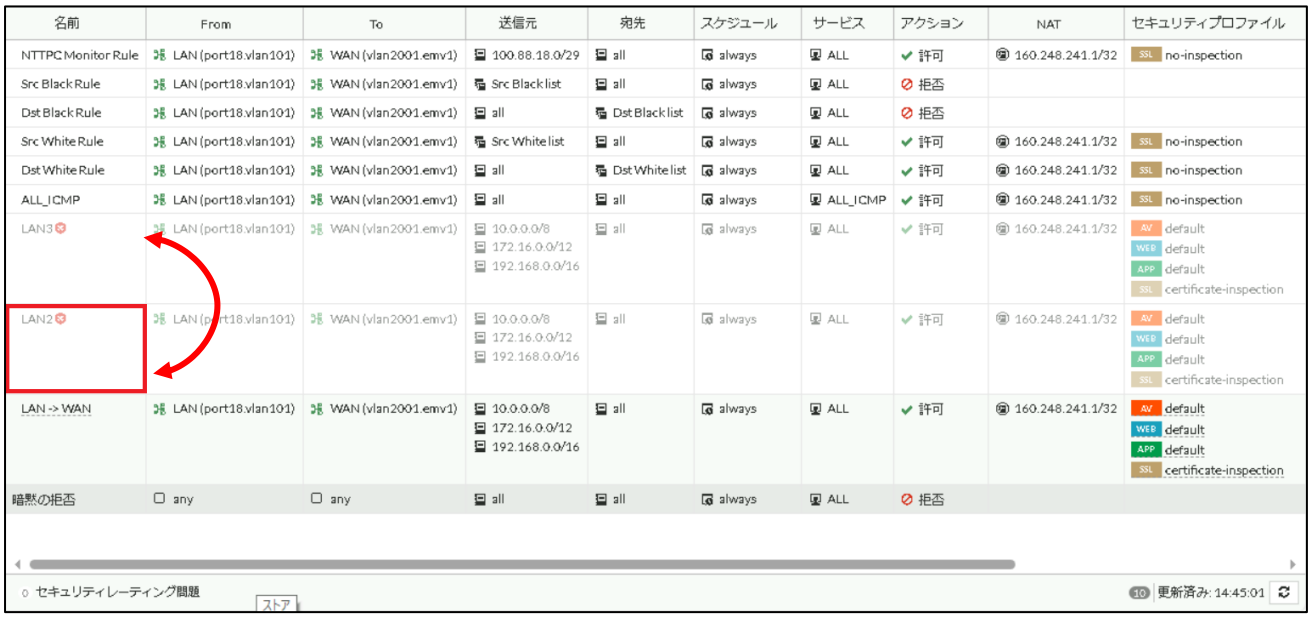


⑤ 名前、送信元、宛先、サービス、セキュリティプロファイルを設定し OK を押下する。
※コメントにコピー元の名前が入るので消すか任意のコメントを記入してください。
※セキュリティプロファイルで使用して良いプロファイルは表 4.1 を参照

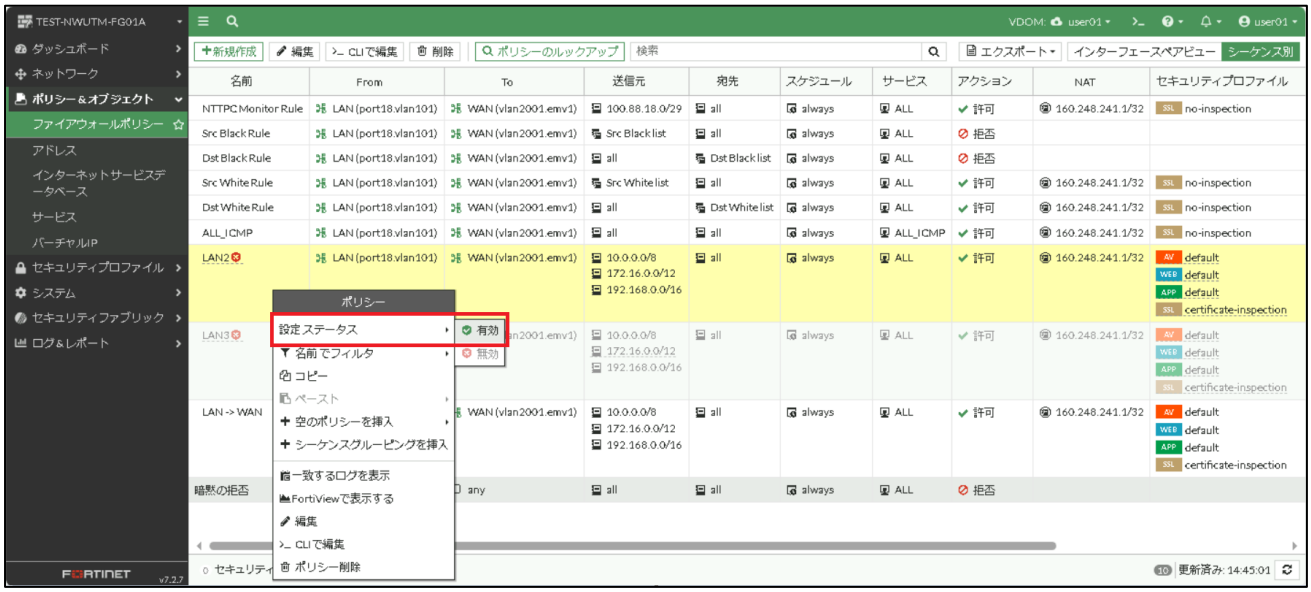
「+」を押下すると右側にリストが表示されるので追加したい分をクリックする。
消すアドレスがある場合は「×」をクリックすると消えます。
送信元、宛先で追加したいものがない場合は 5.1 項を参照
サービスで追加したいものがない場合は 7.1 項を参照

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

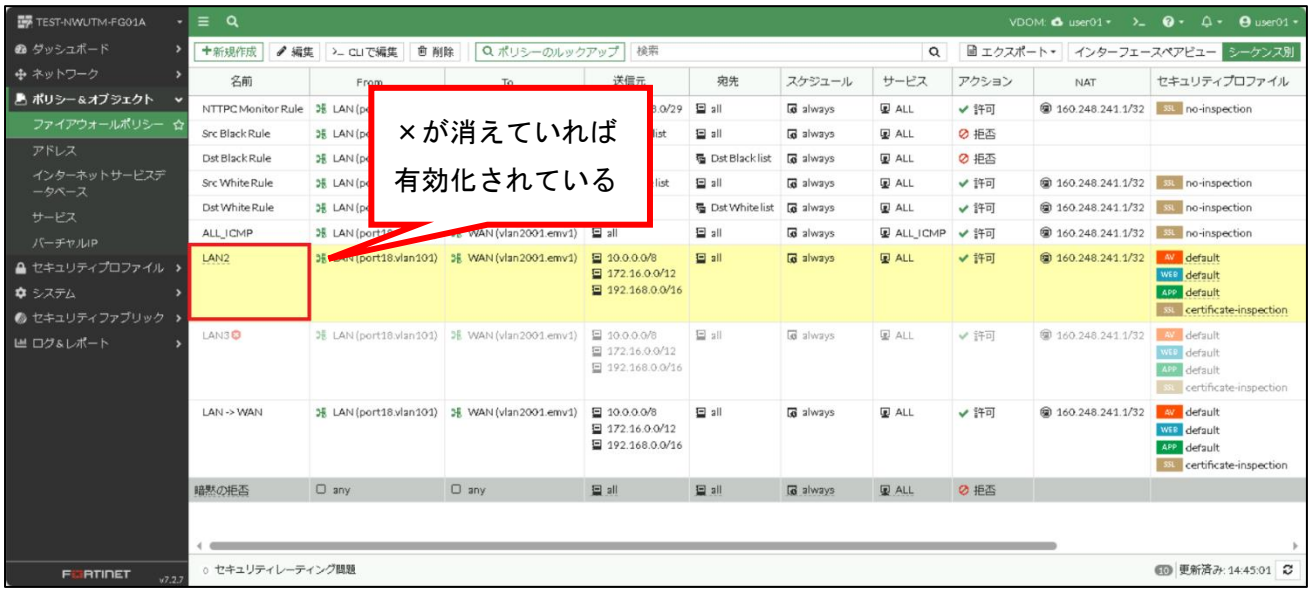
⑥　作成したルールを ALL_ICMP より下の投入したい場所に名前部分でドラッグ&ドロップし移動させる。



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。

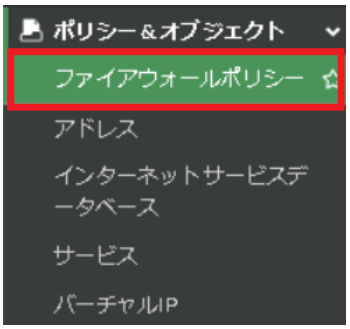


⑧　ルールが有効になったことを確認する。

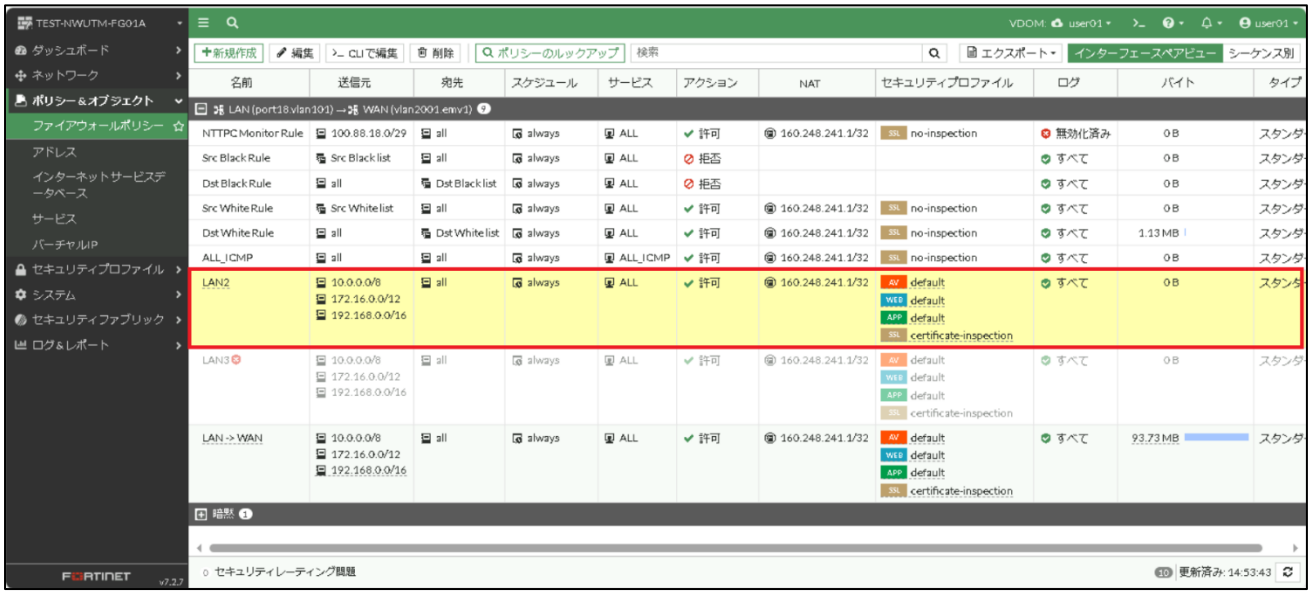


4.3　ファイアウォールルールの変更（表示形式：インターフェースペアビューの場合）

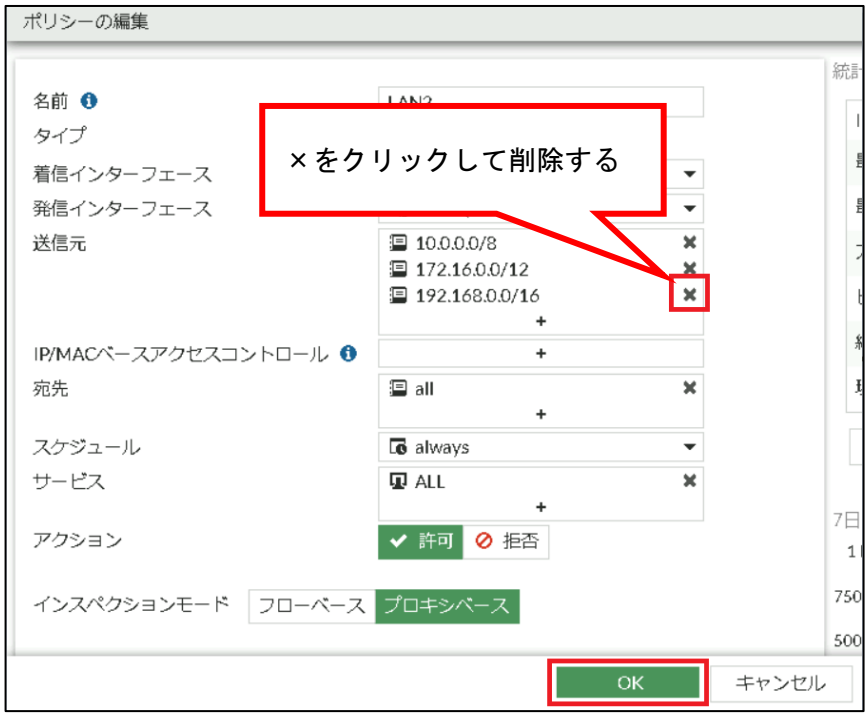
① 左のメニューからポリシー&オブジェクト->ファイアウォールポリシーを選択する。



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。



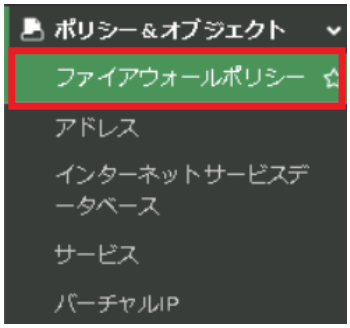
③　変更したい箇所の設定の変更をし、OK を押下する。
※変更可能な個所は下記図 4-1 を参照願います。



④　変更完了後、正しく変更されたことを確認します。

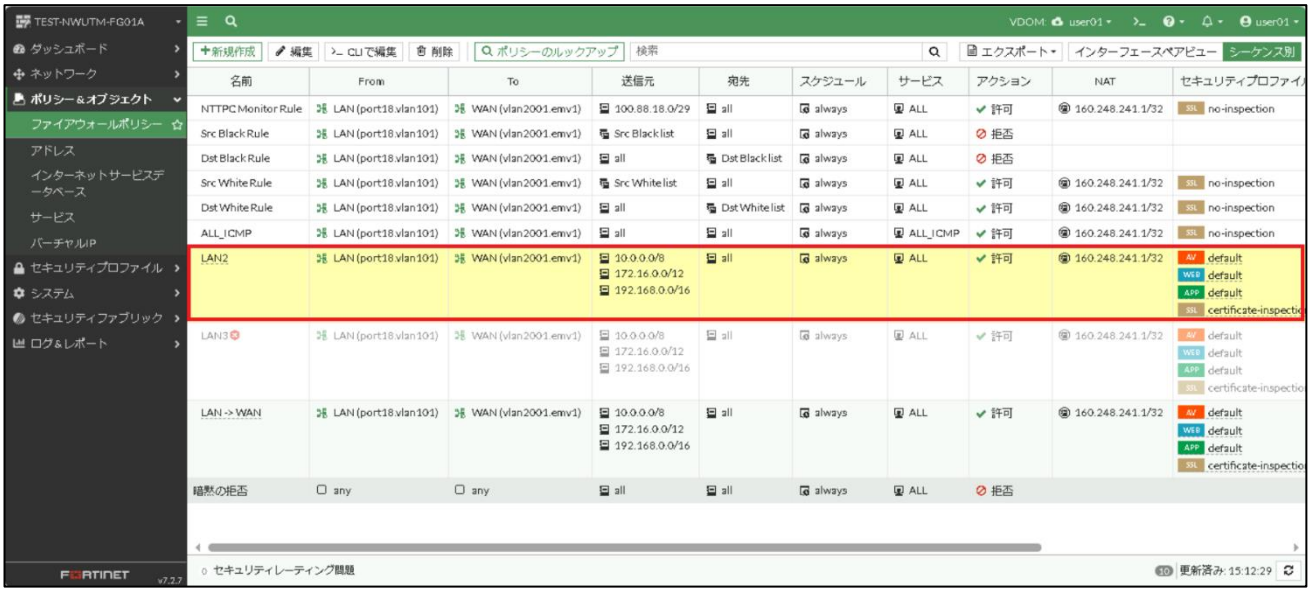
4.4　ファイアウォールルールの変更（表示形式：シーケンス別の場合）

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。



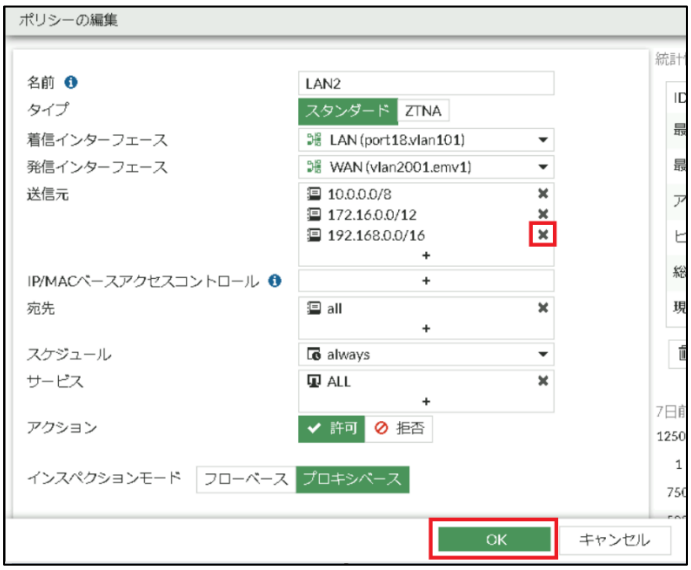
② 変更したいポリシーをダブルクリックします。

例：送信元の 192.168.0.0/16 を削除したい場合。

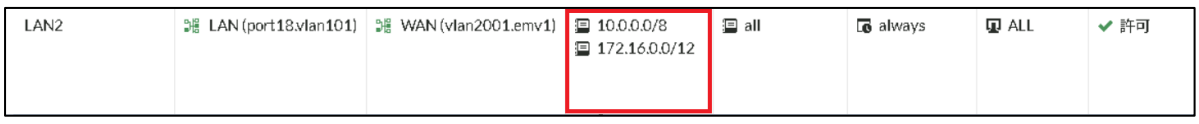


③ 変更したい箇所の設定の変更をし、OK を押下する。

変更可能な個所は下記図 4-1 を参照願います。



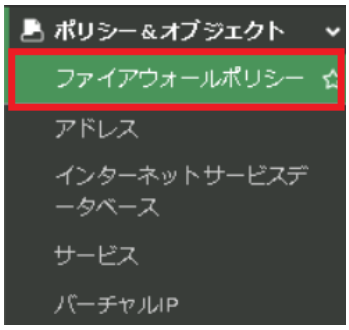
④ 変更完了後、正しく変更されたことを確認します。



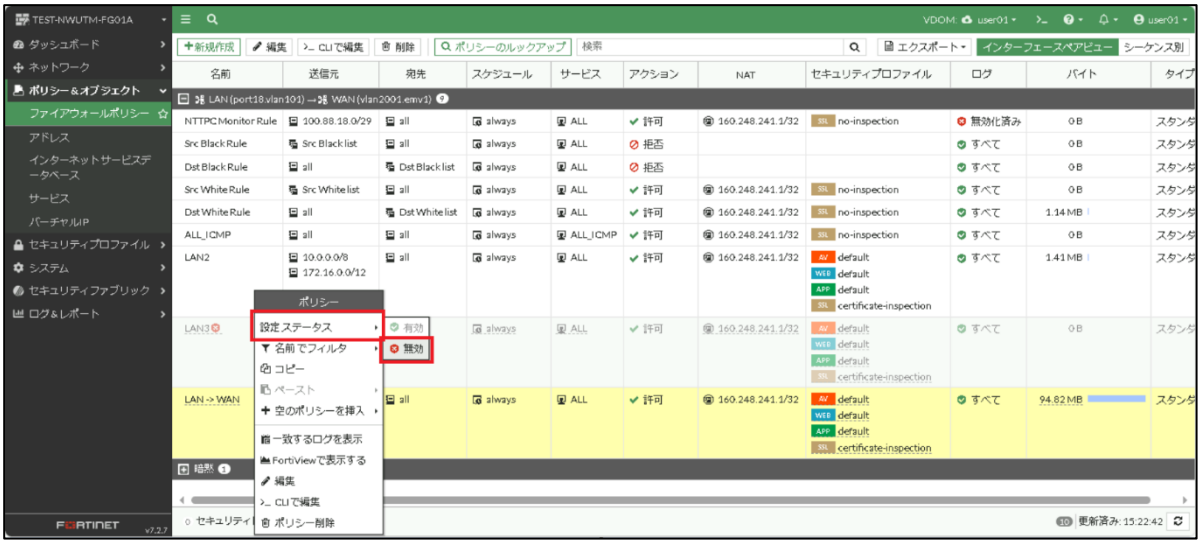
4.5　ファイアウォールルールの無効化・削除（表示形式：インターフェースペアビューの場合）

①　ファイアウォールルールの無効化

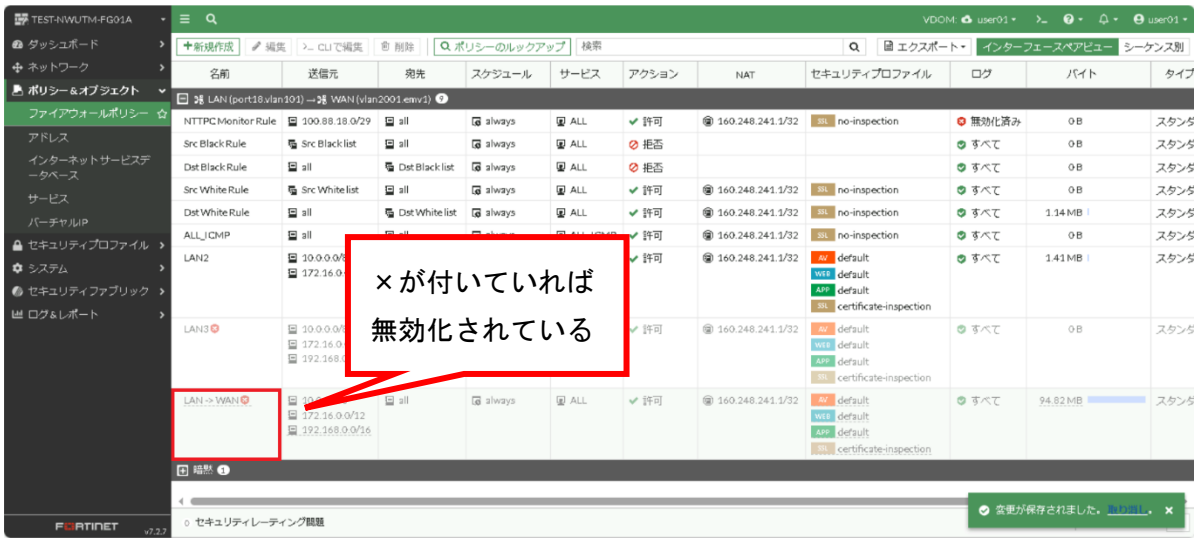
I.　左のメニューからポリシー&オブジェクト->ファイアウォールポリシーを選択する。



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。

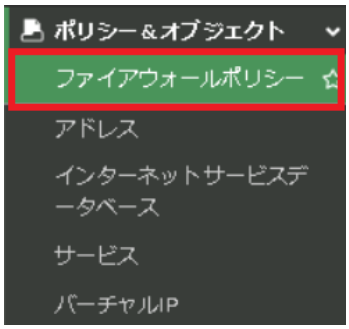


III.　ルールが無効になっていることを確認する。

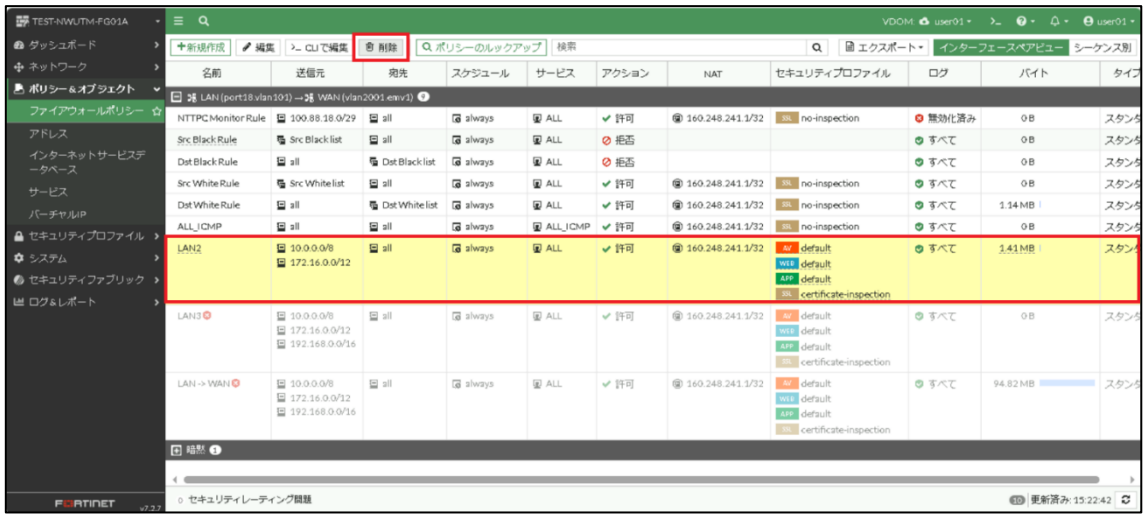


② ファイアウォールルールの削除

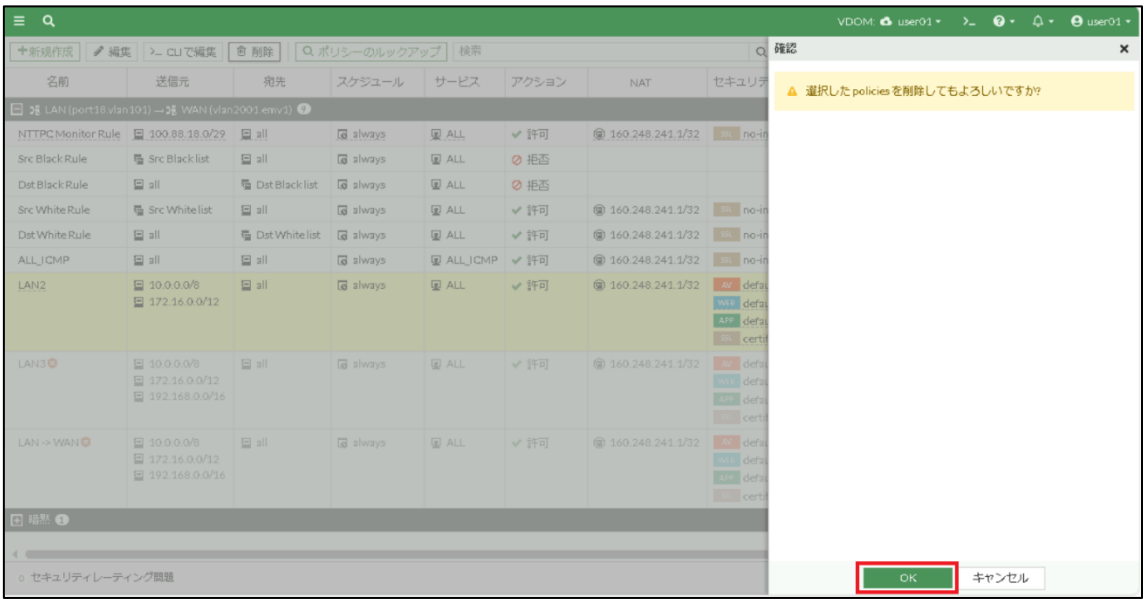
I. 左のメニューからポリシー&オブジェクト->ファイアウォールポリシーを選択する。



II. 削除したいルールをクリックし、削除をクリックする。



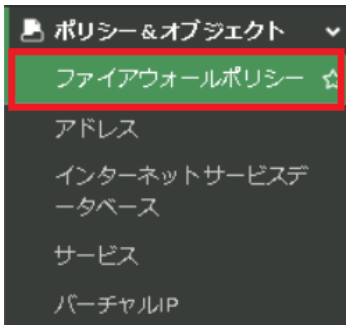
III. 確認画面が表示されるので OK を押下する。



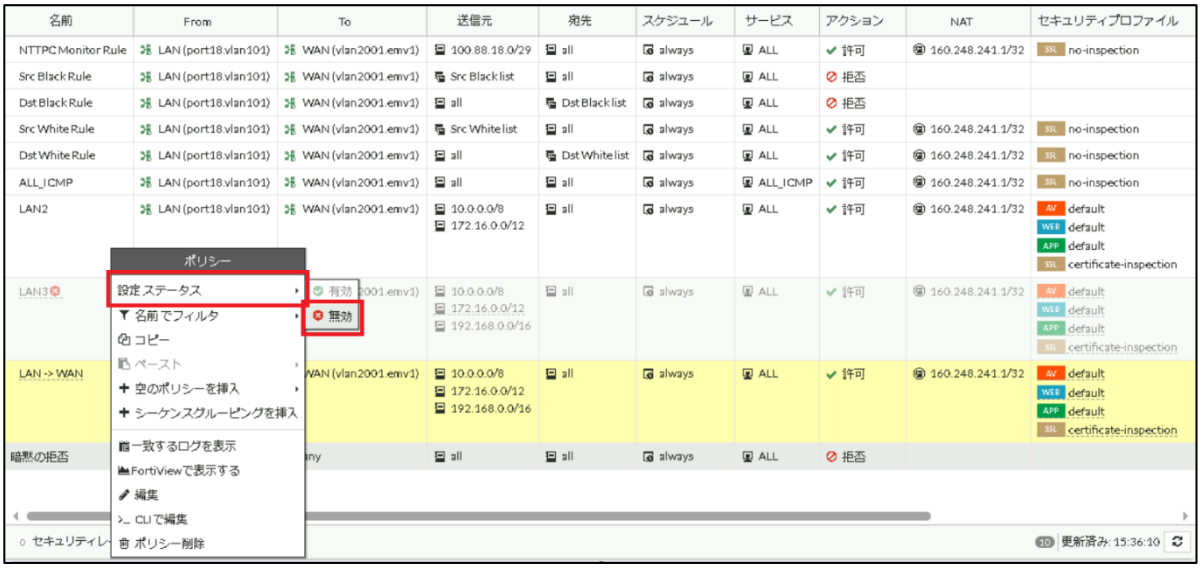
4.6　ファイアウォールルールの無効化・削除（表示形式：シーケンス別の場合）

①　ファイアウォールルールの無効化

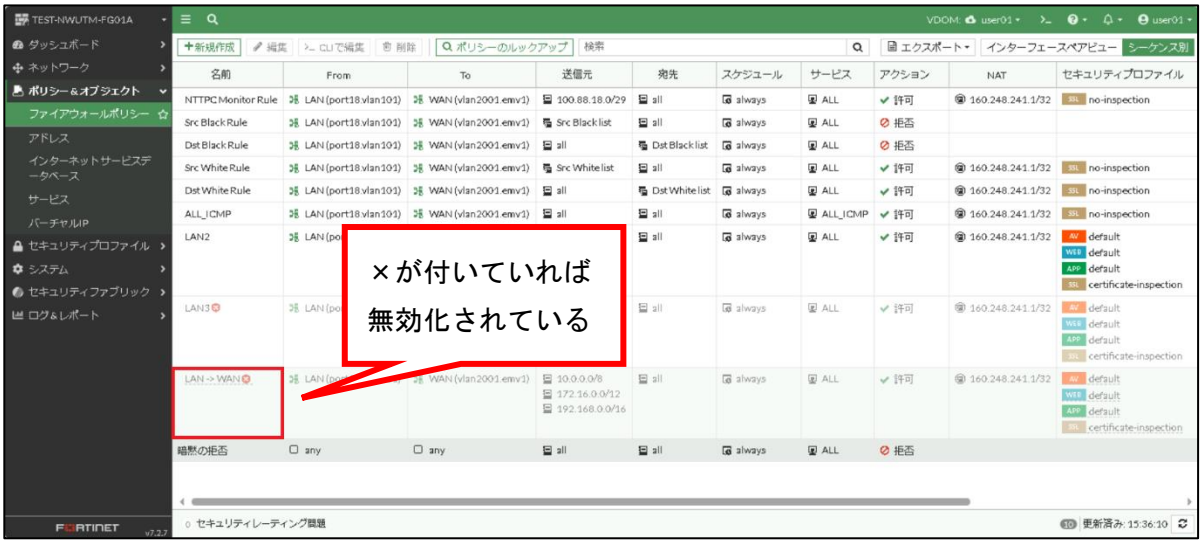
I.　左のメニューからポリシー&オブジェクト->ファイアウォールポリシーを選択する。



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。

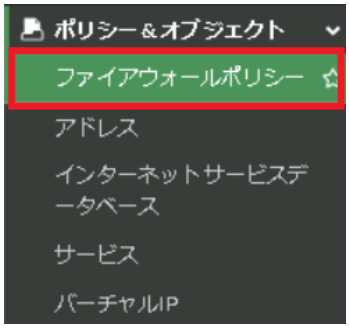


III.　ルールが無効になっていることを確認する。

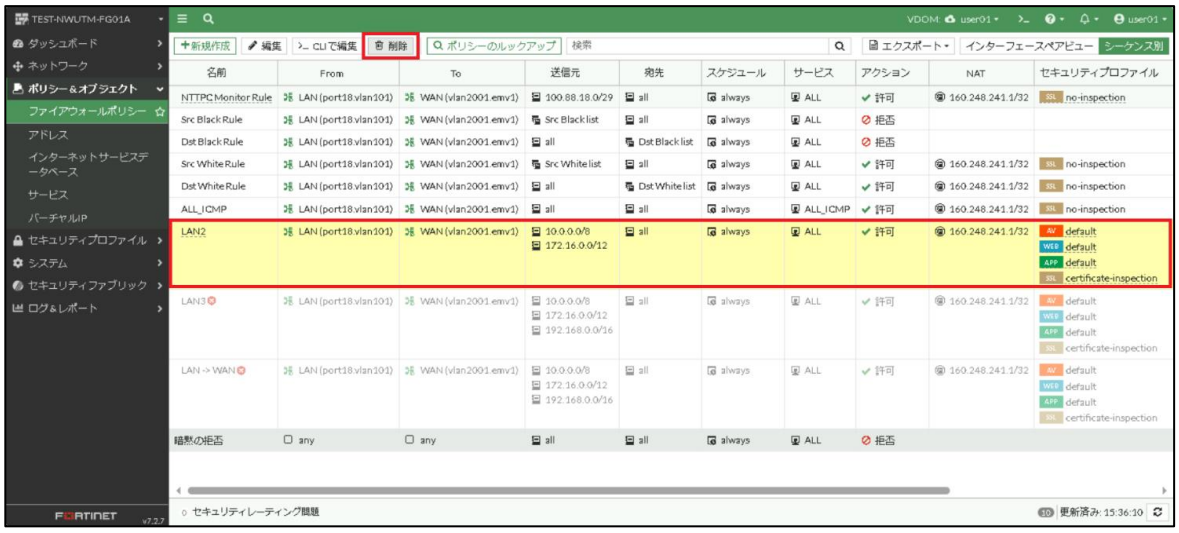


② ファイアウォールルールの削除

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。

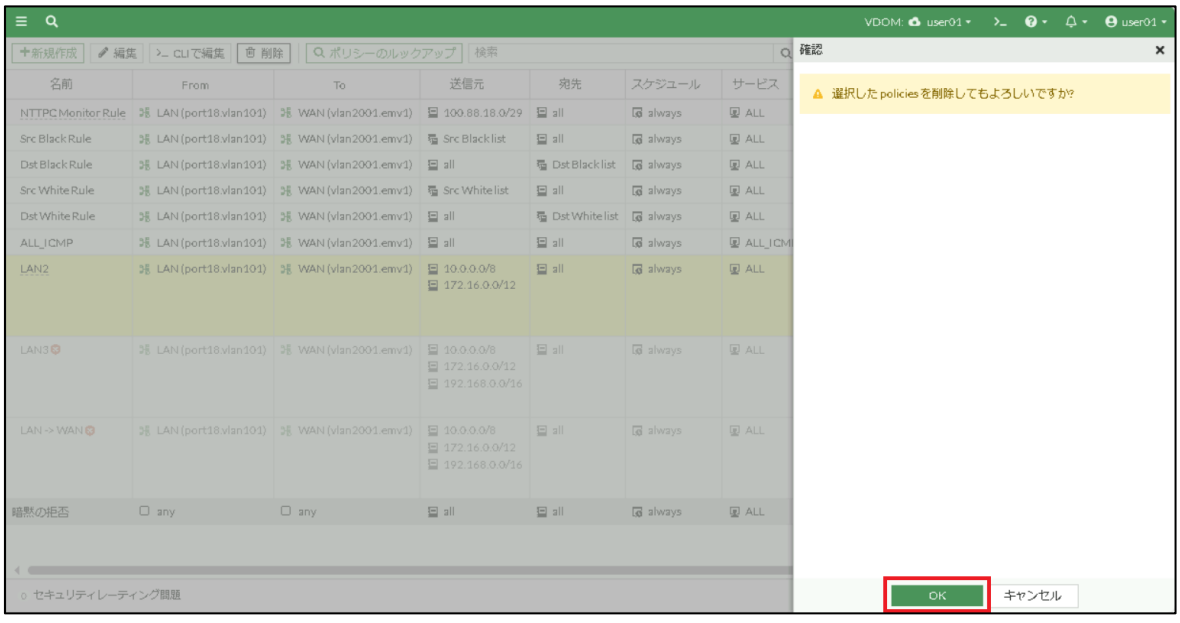


表 4-1.　ファイアウォールルールの設定項目

	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、動作しょうはできません。
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	

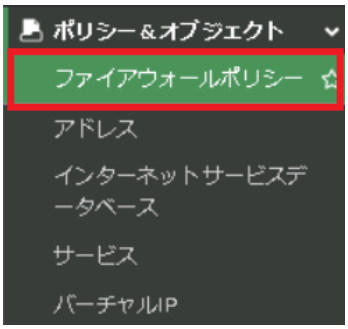
※　上記以外の設定をした場合、動作保証はできません。

※　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。

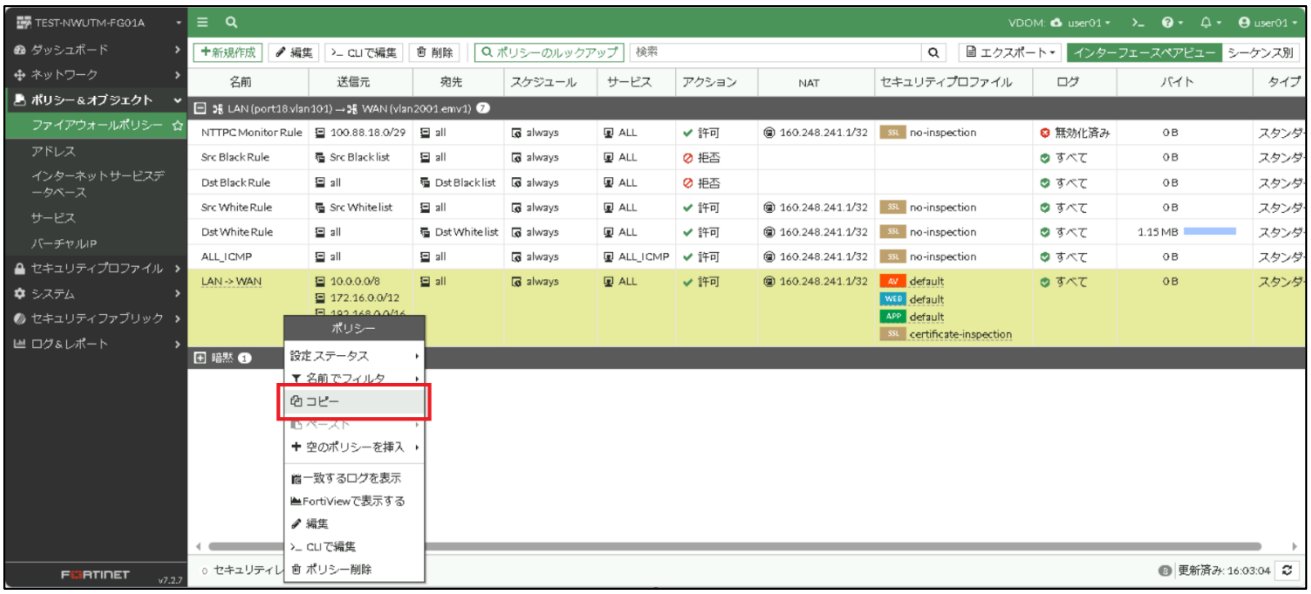
※　水色の網掛け部分に関しては DNAT 使用時のみ変更できるパラメータになります。

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）

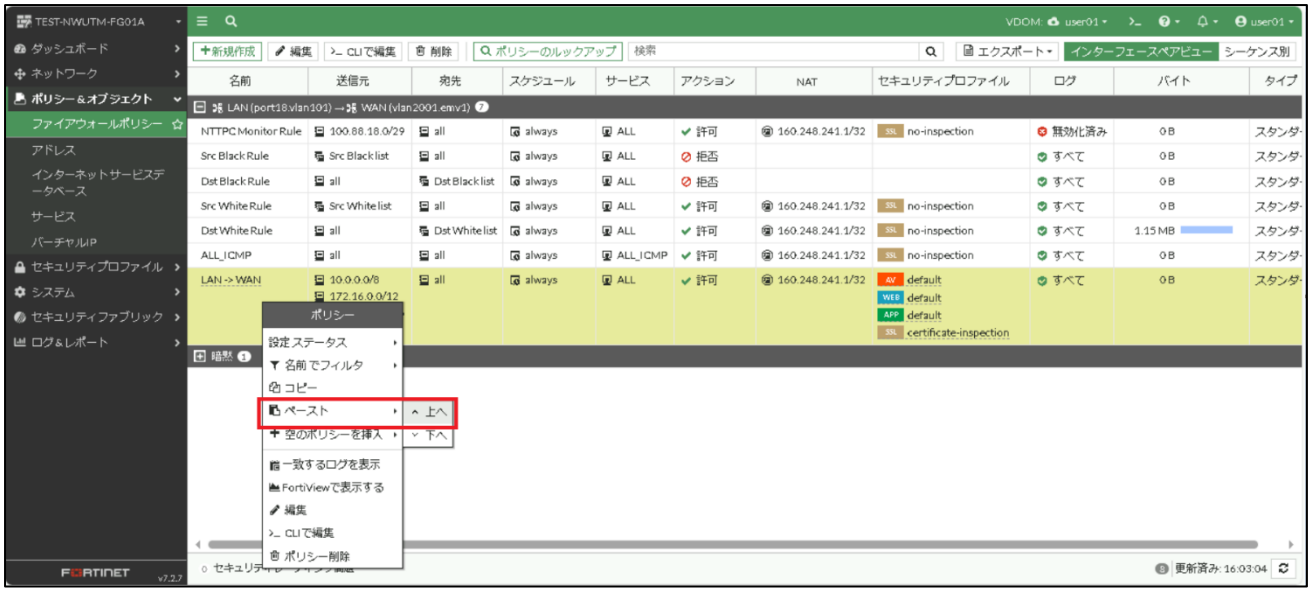
① 左メニューよりポリシー&オブジェクト→ファイアウォールポリシーを選択する。



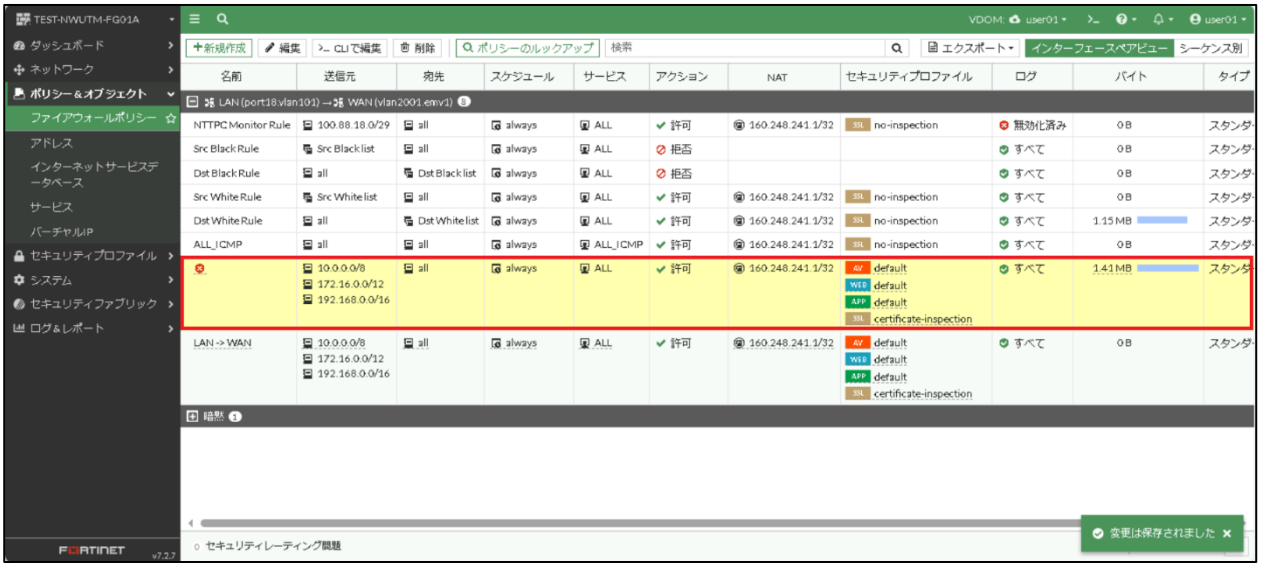
② LAN→WAN を右クリックし、コピーを押下する。



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。



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して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。

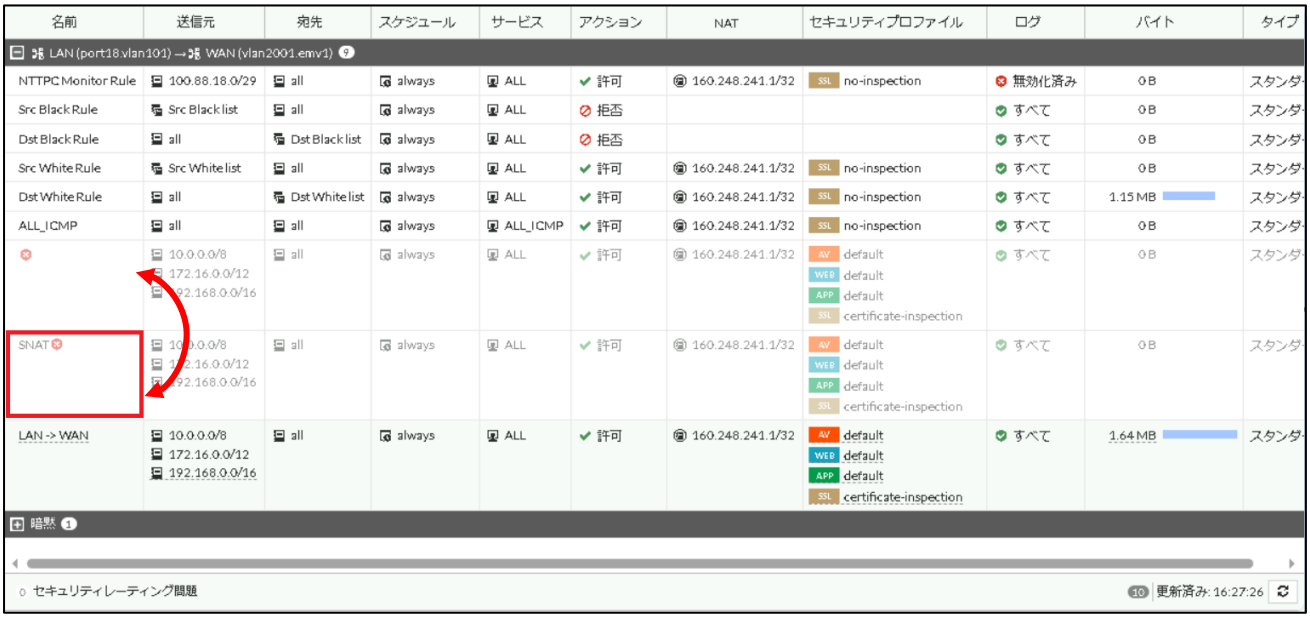
「＋」を押下し右側のリストから追加グローバル IP をクリックする。

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。

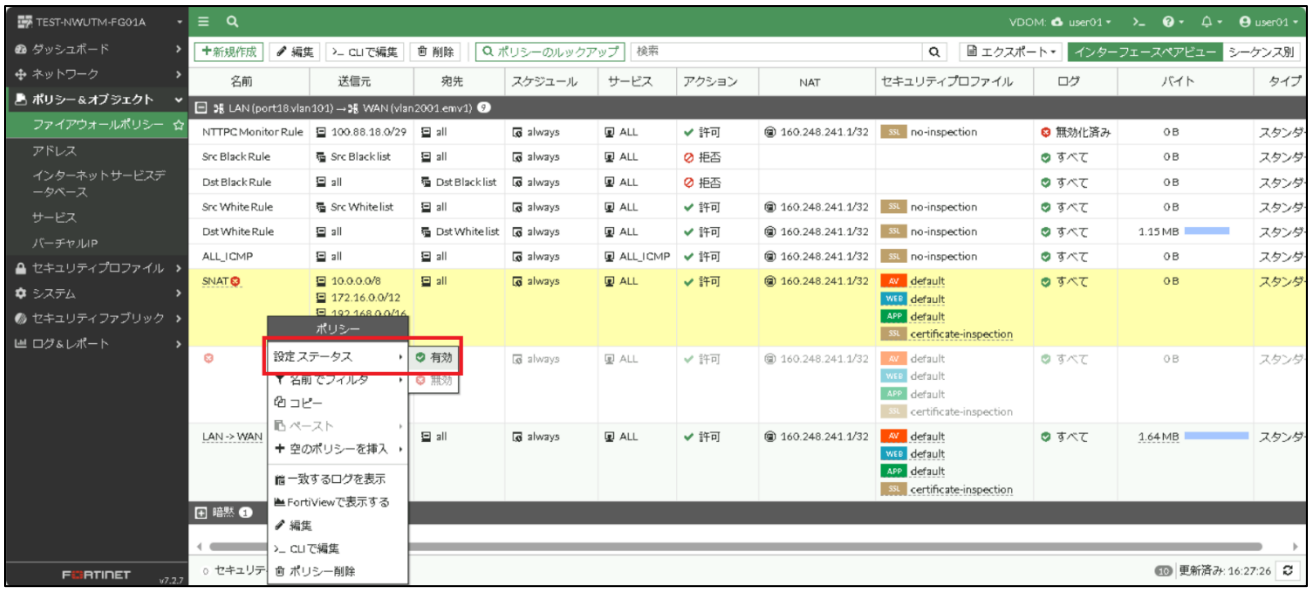
使用しないセキュリティ機能はトグルをクリックし無効化にしてください。

詳細は 13 章を参照

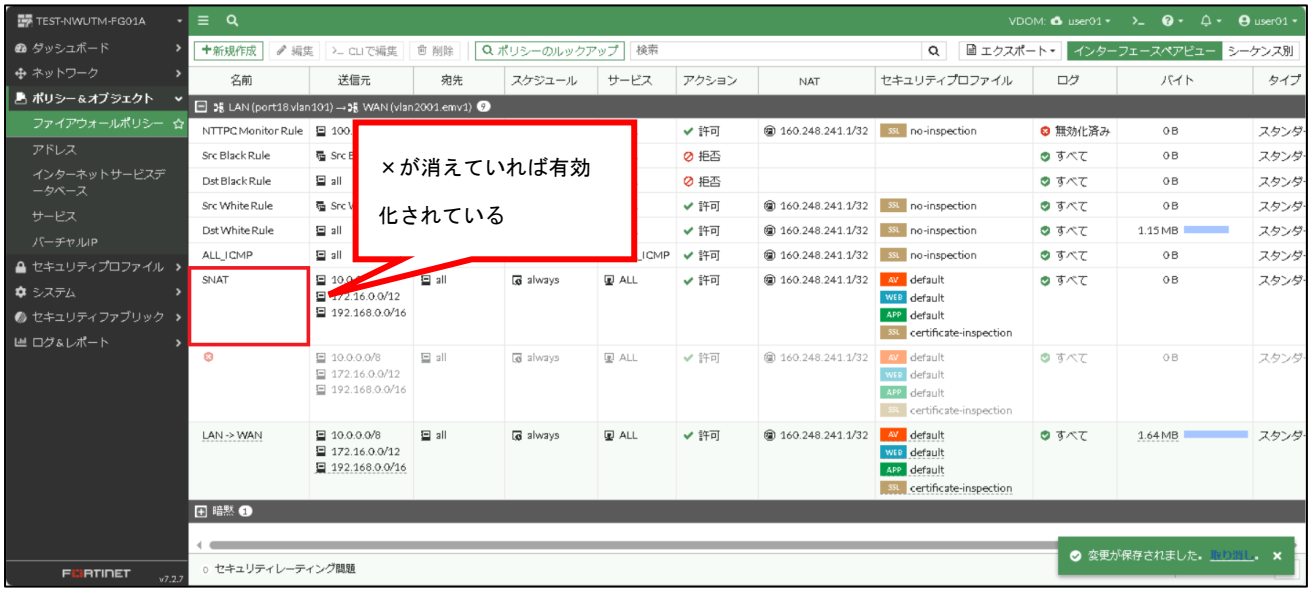
⑥　作成したルールを ALL_ICMP より下の投入したい場所に名前部分でドラッグ&ドロップし移動させる。



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。

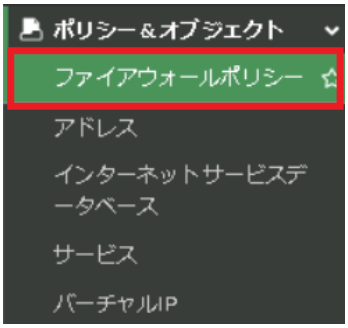


⑧　ルールが有効になったことを確認する。

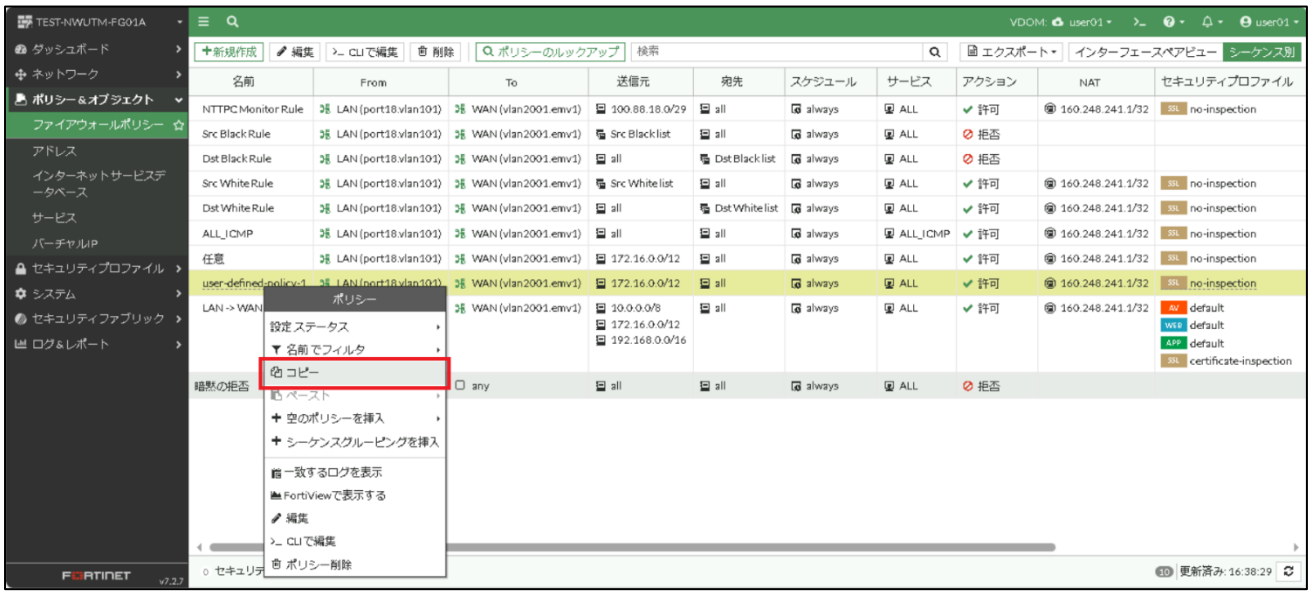


4.8　SNAT 設定方法（表示形式：シーケンス別の場合）

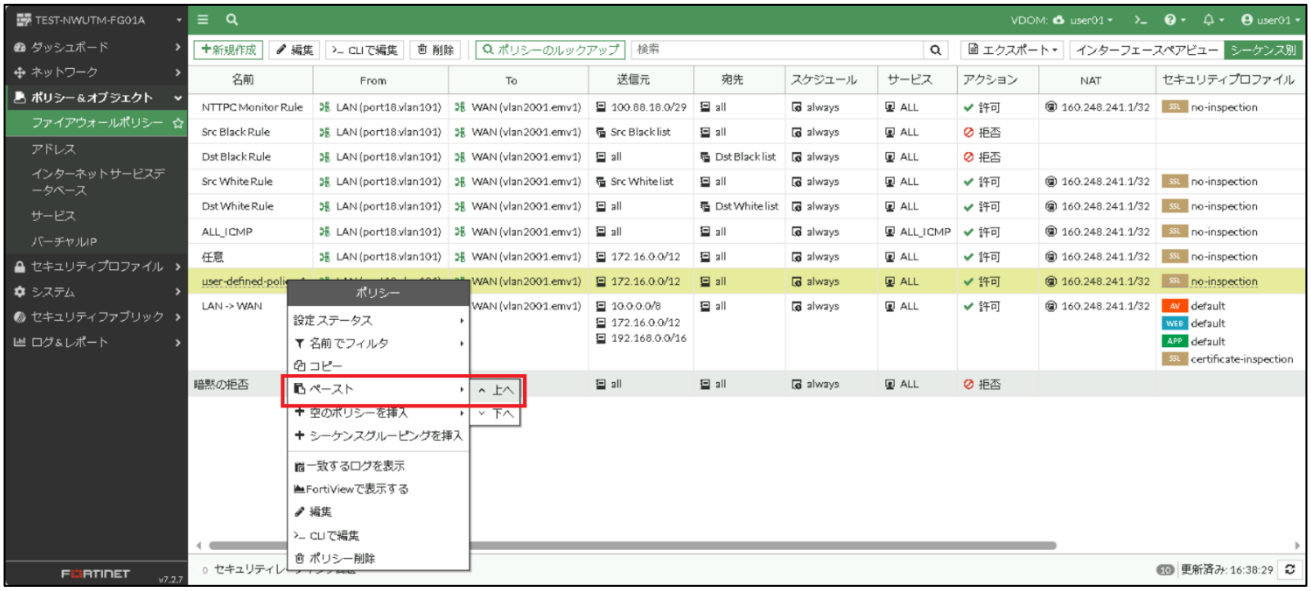
①　左メニューよりポリシー&オブジェクト→ファイアウォールポリシーを選択する。



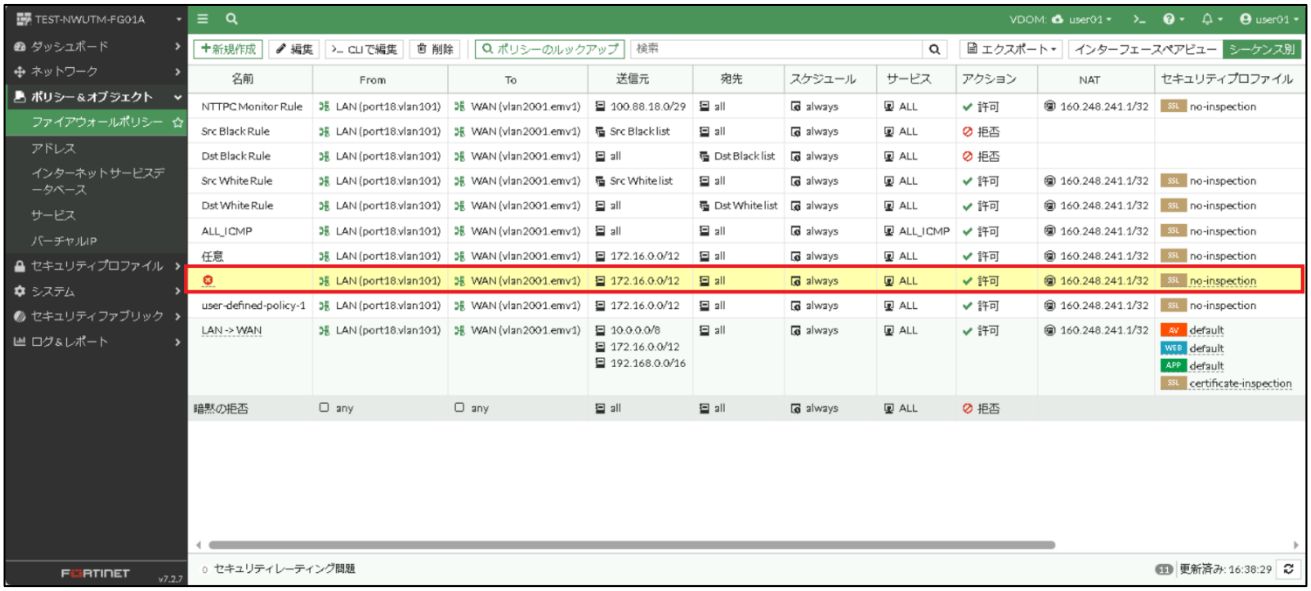
② user-defined-policy-1 を右クリックし、コピーを押下する。



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。



④　作成したポリシーをダブルクリックする。



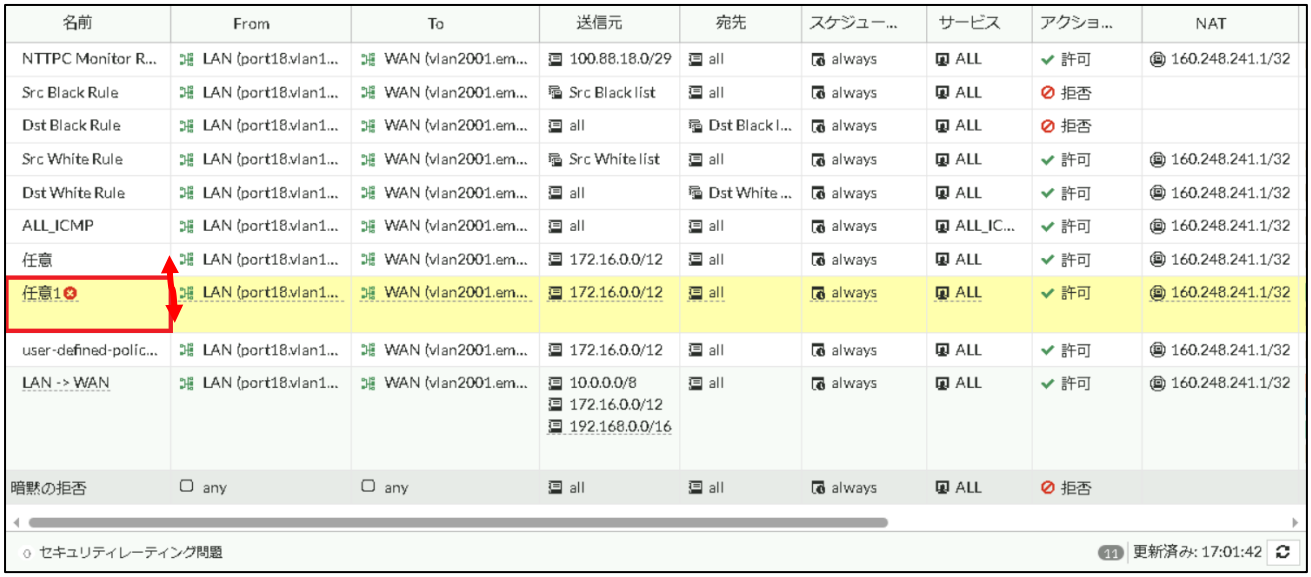
⑤ 名前、送信元、宛先、サービス、IP プール、セキュリティプロファイル、コメント（任意）を設定し OK を押下する。

※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。

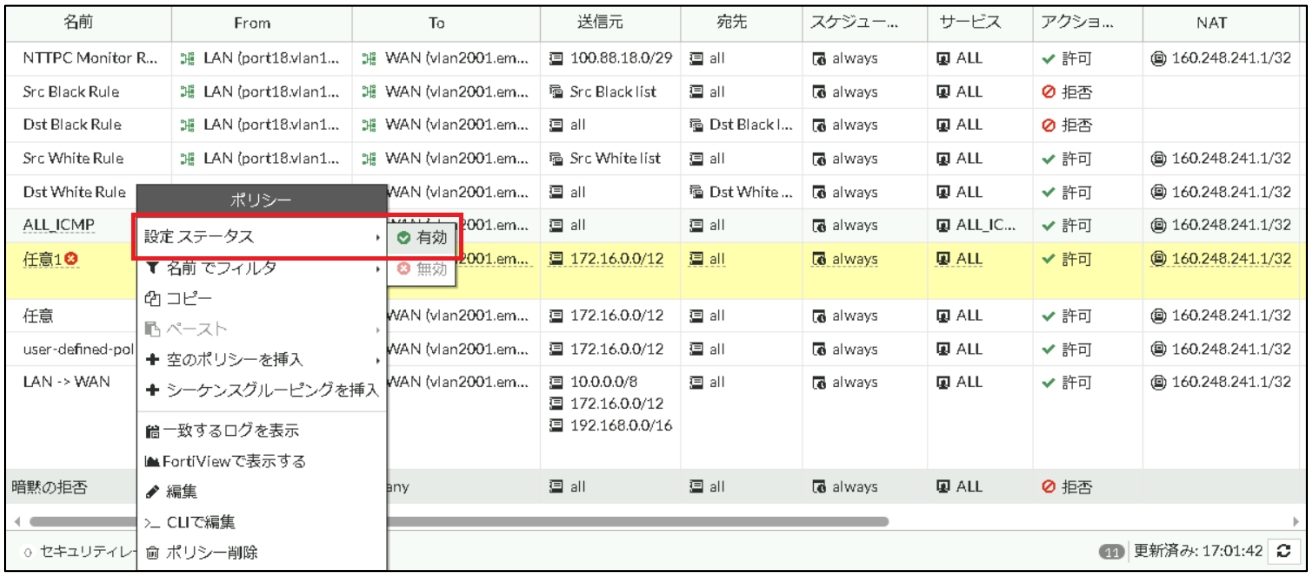
※コメントにコピー元の名前が入るので消すか任意のコメントを記入してください。

※セキュリティプロファイルで使用して良いプロファイルは表 4.1 を参照

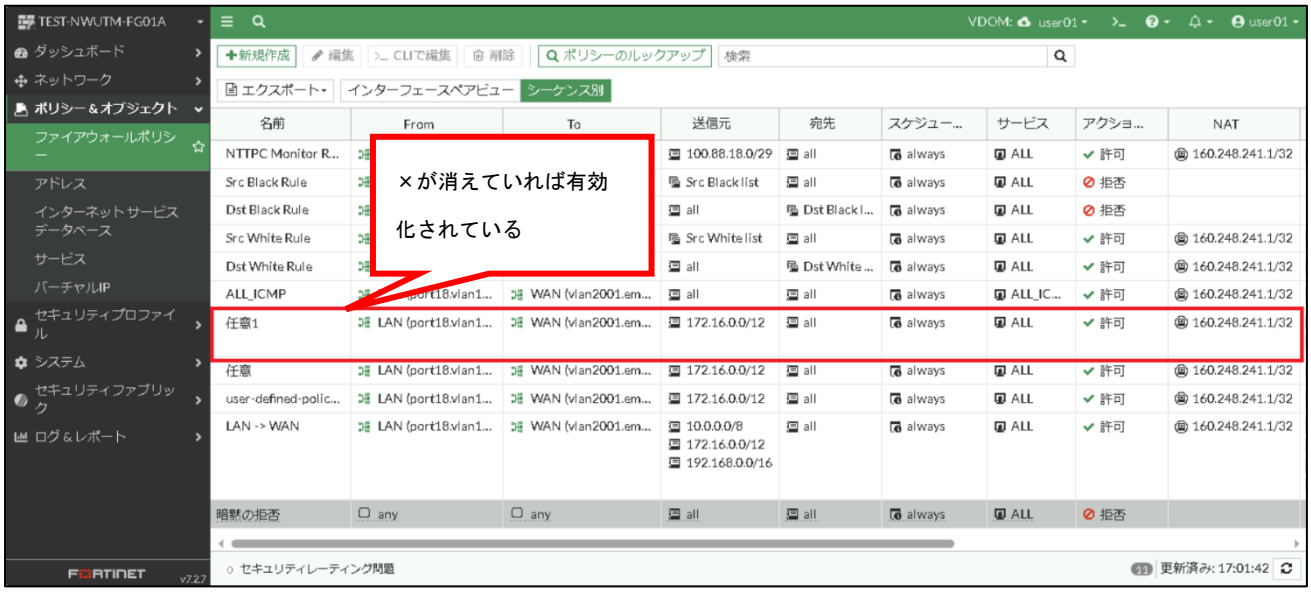
⑥　作成したルールを ALL_ICMP または DNAT が設定されていればそれより下の投入したい場所に名前部分でドラッグ&ドロップし移動させる。



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。



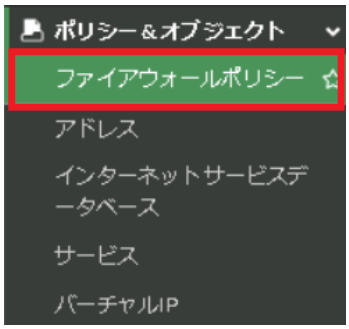
⑧　ルールが有効になったことを確認する。



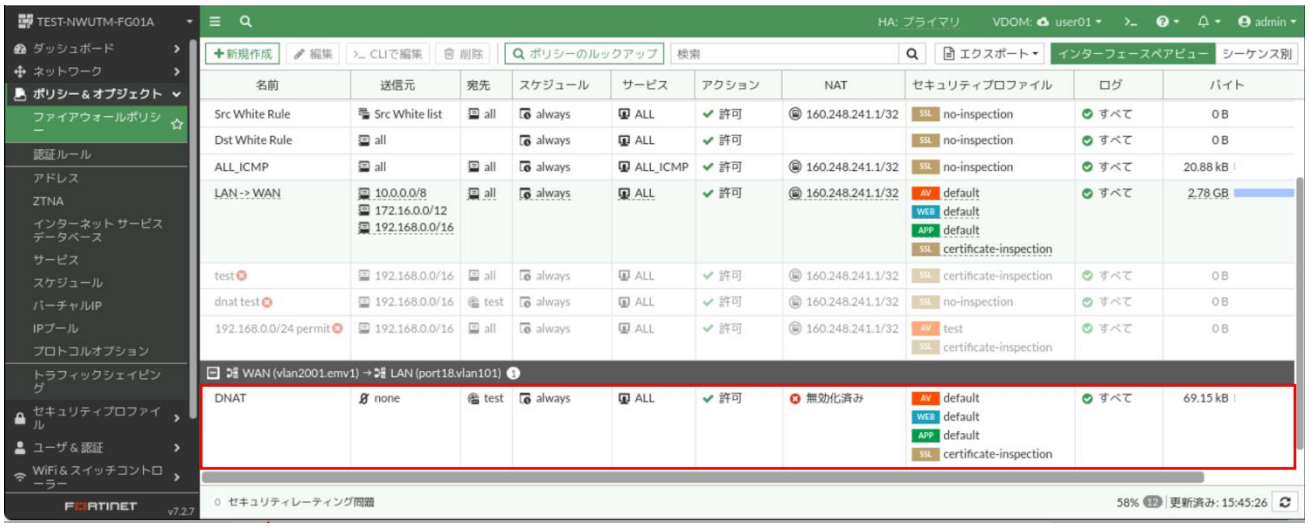
4.9 DNAT 申込時の送信元初期設定"none"の変更方法（表示形式：インターフェースペアビューの場合）

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

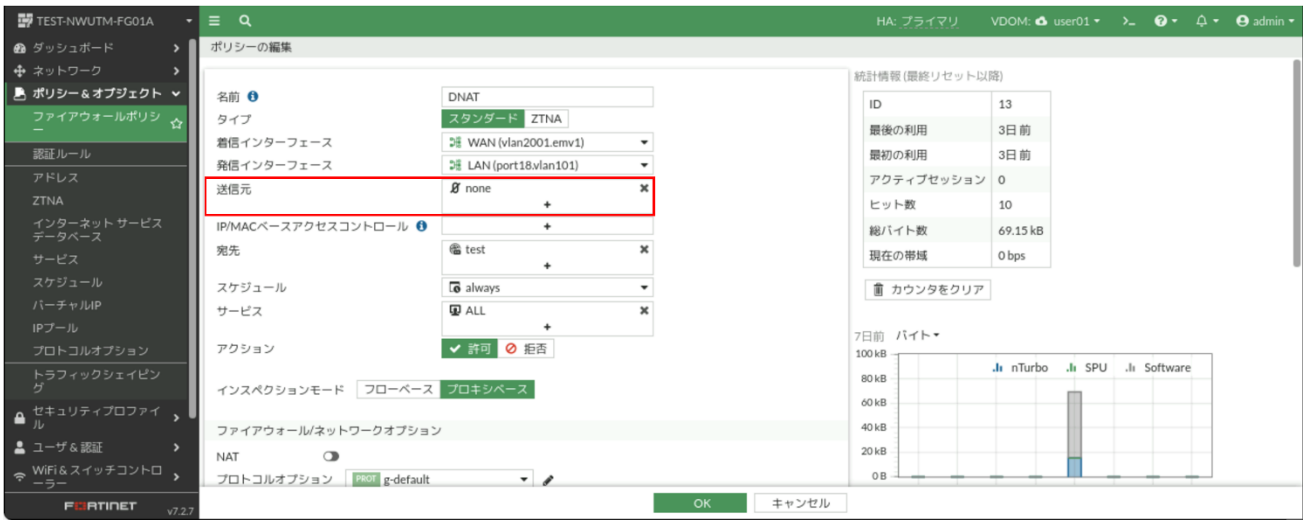
① 左メニューよりポリシー&オブジェクト→ファイアウォールポリシーを選択する。



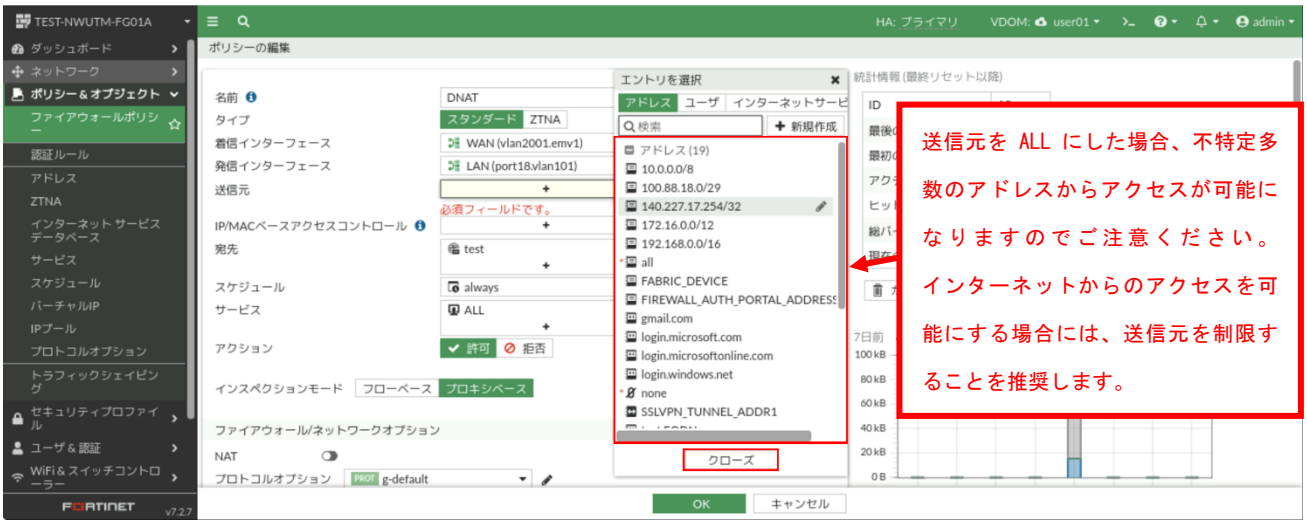
② お申込により作成された DNAT のポリシーをダブルクリックする。



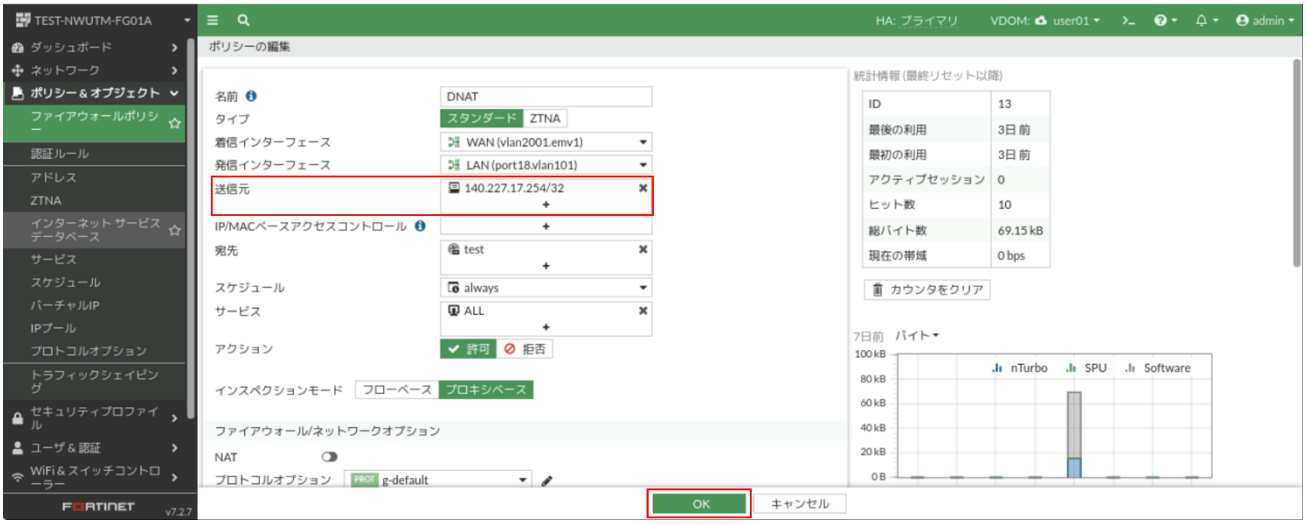
③　送信元が「none」となっていることを確認し、「none」の右の×を押下する。



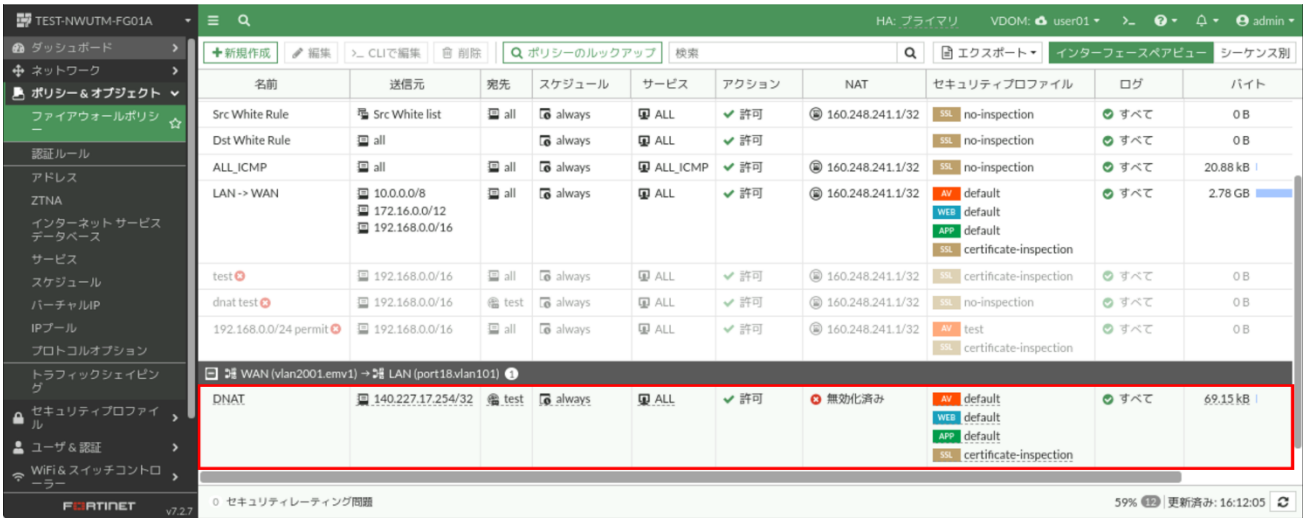
④　「エントリを選択」から通信を行う送信元アドレスを選択しクローズを押下する。



⑤　送信元が問題ないことを確認し OK ボタンを押下する。

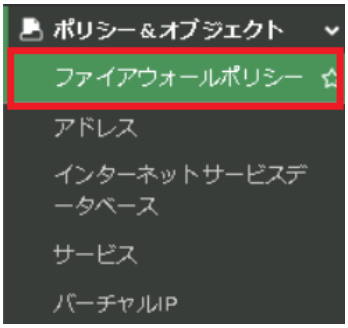


⑥　送信元の欄が問題なく設定されていることを確認する。

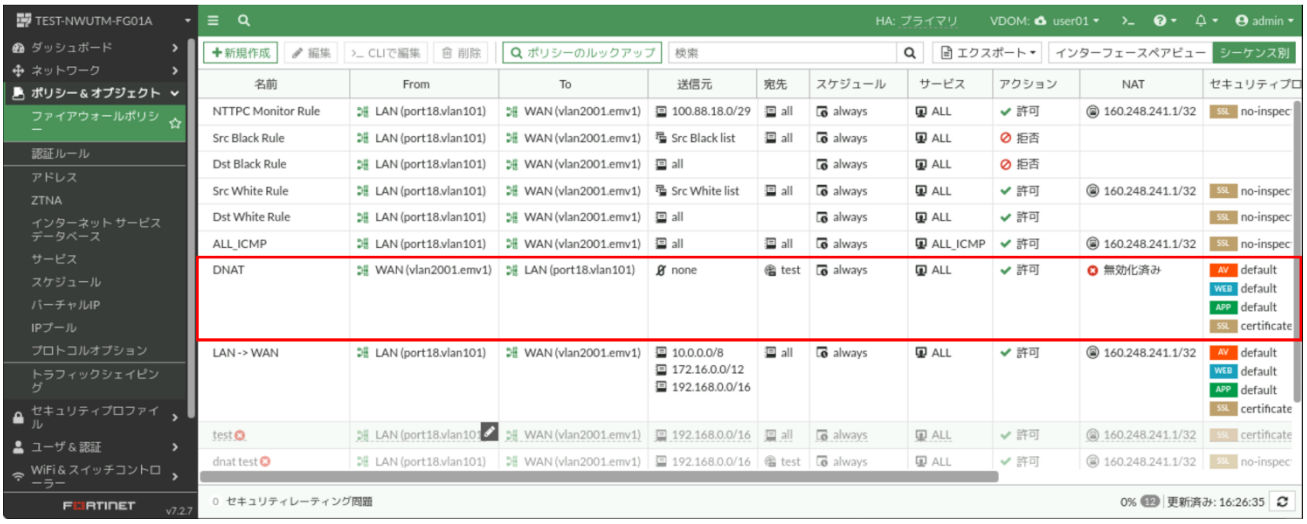


4.10 DNAT 申込時の送信元初期設定"none"の変更方法（表示形式：シーケンス別の場合）

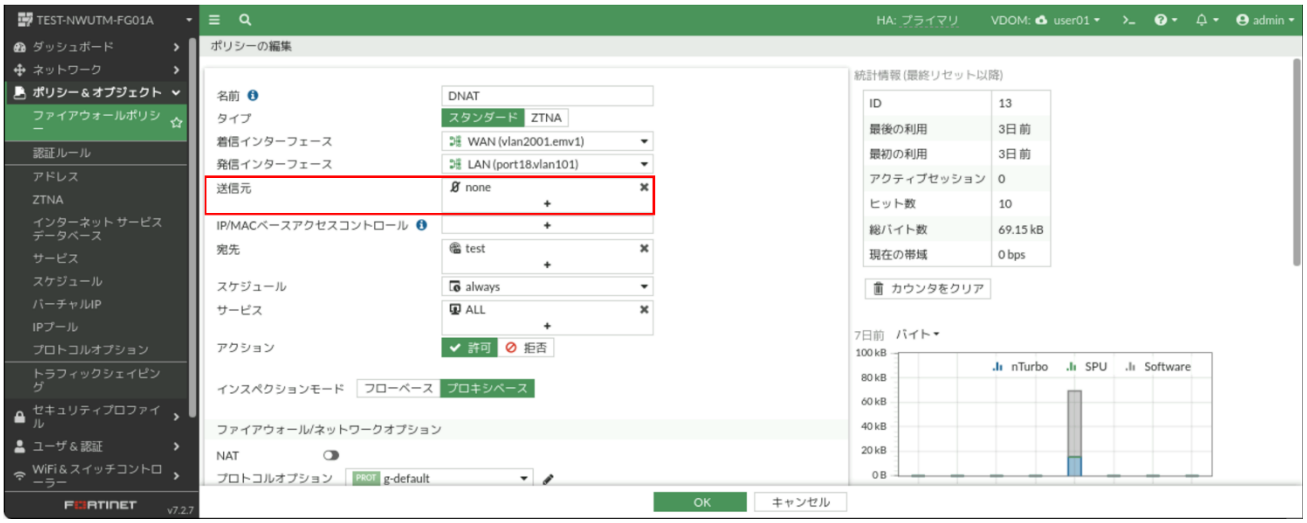
① 左メニューよりポリシー&オブジェクト→ファイアウォールポリシーを選択する。



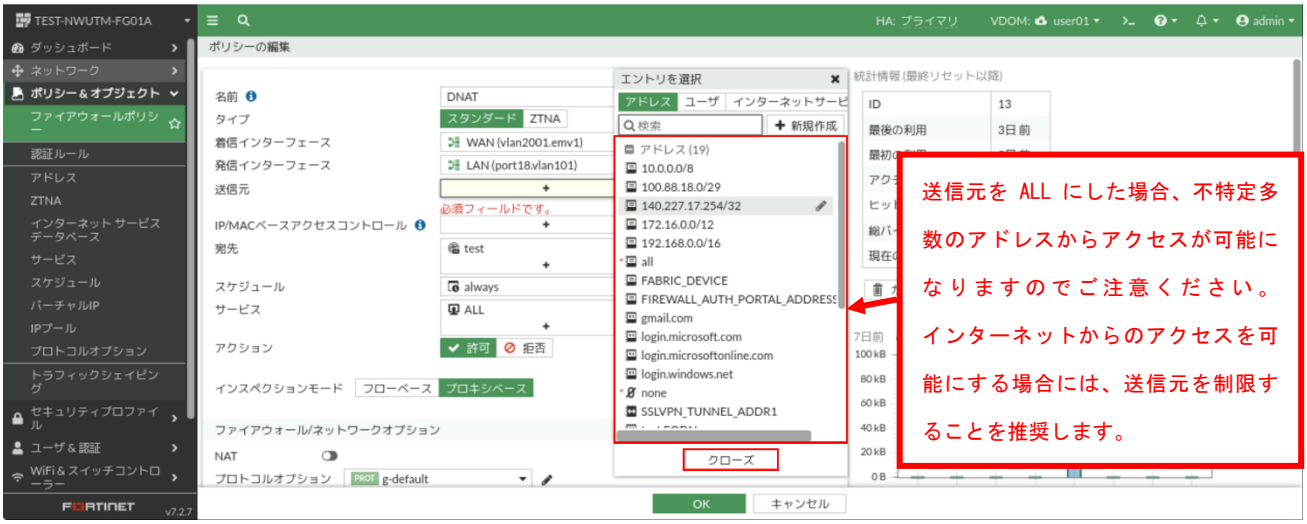
② お申込により作成された DNAT のポリシーをダブルクリックする。



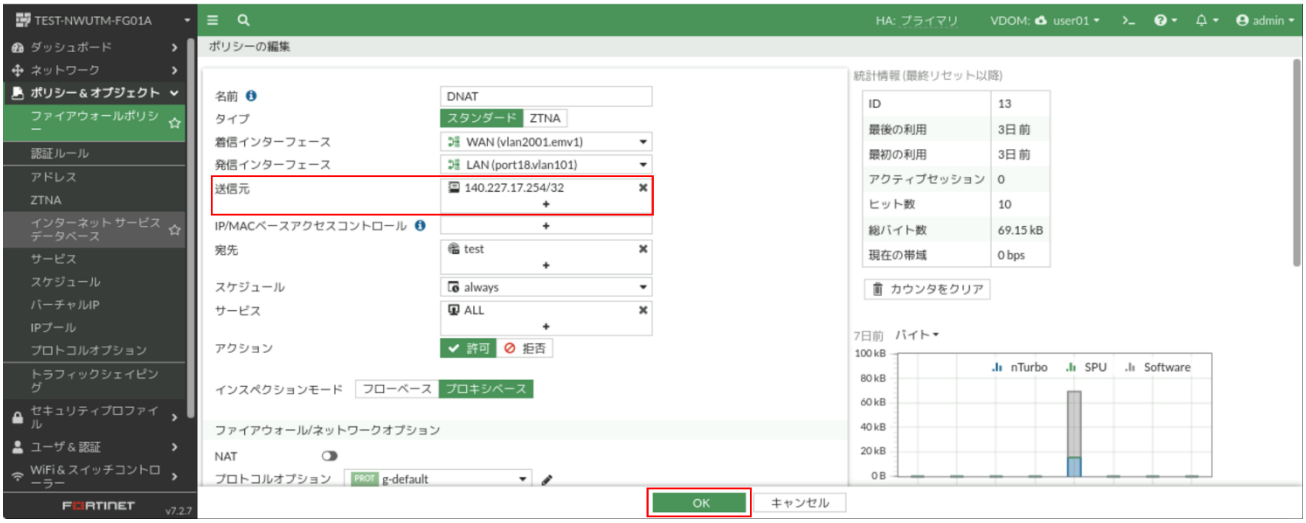
③　送信元が「none」となっていることを確認し、「none」の右の×を押下する。



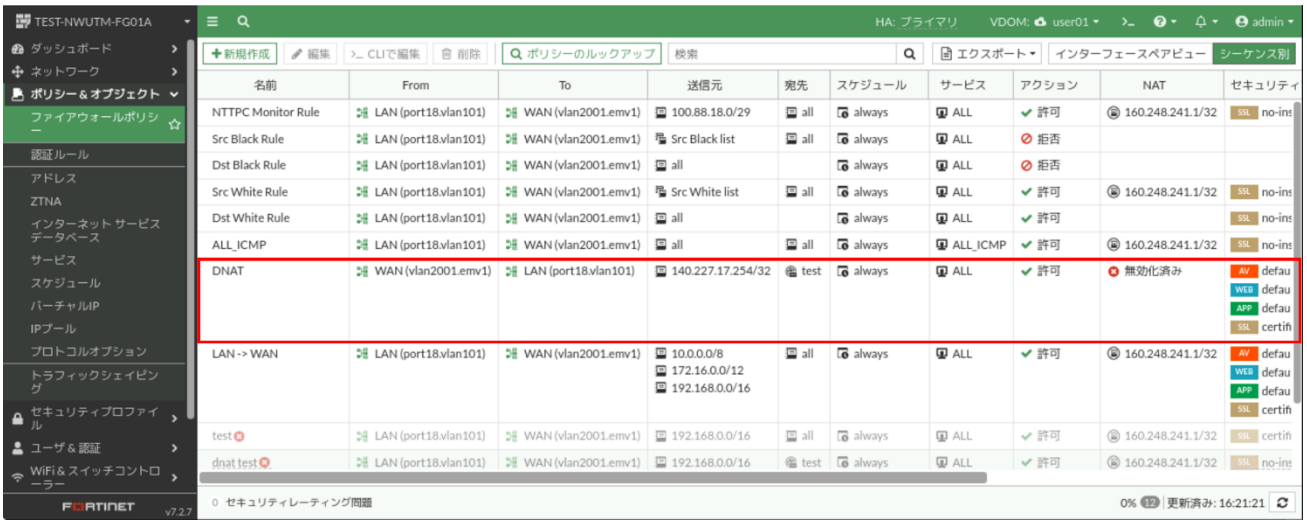
④　「エントリを選択」から通信を行う送信元アドレスを選択しクローズを押下する。



⑤　送信元が問題ないことを確認し OK ボタンを押下する。



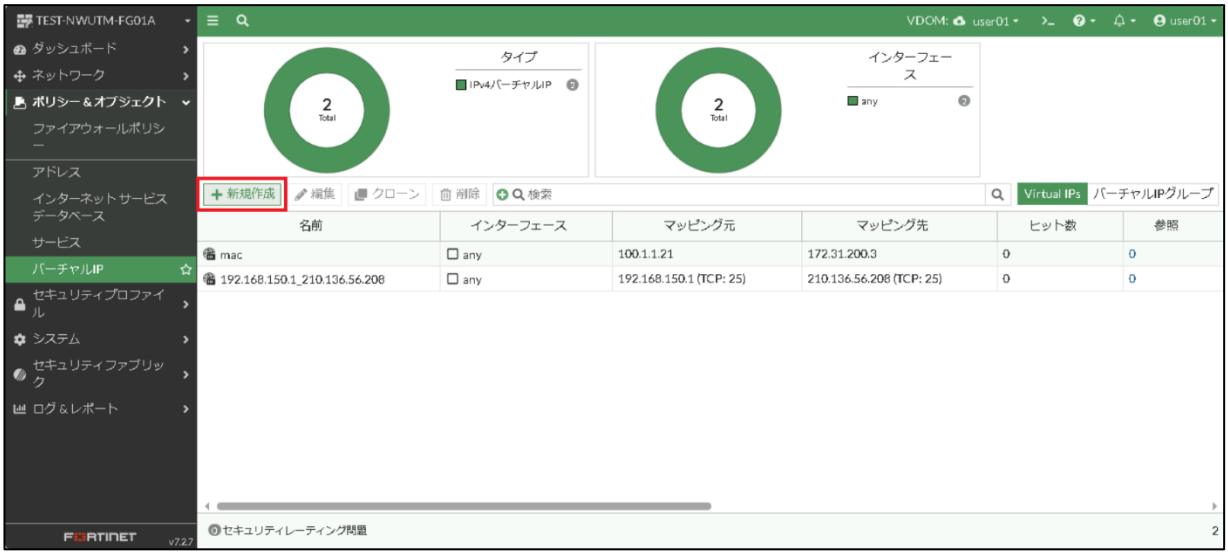
⑥　送信元の欄が問題なく設定されていることを確認する。



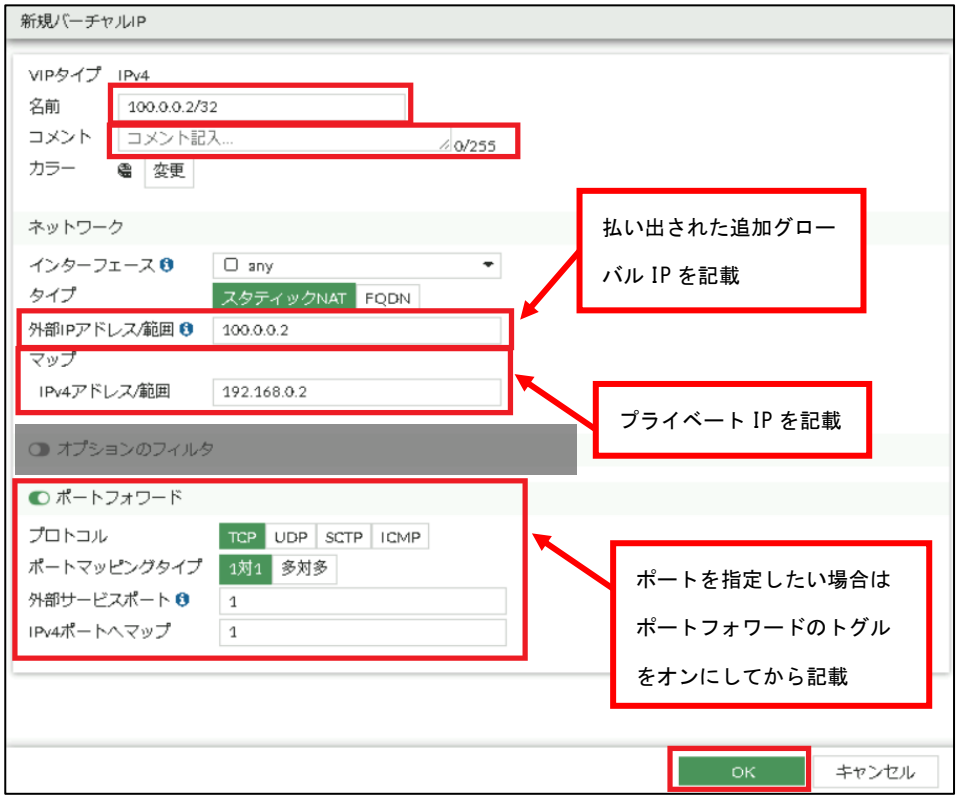
4.11 DNAT 設定方法（表示形式：インターフェースペアビューの場合）

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。

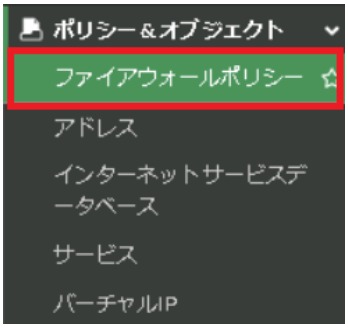
② 新規作成を押下する。



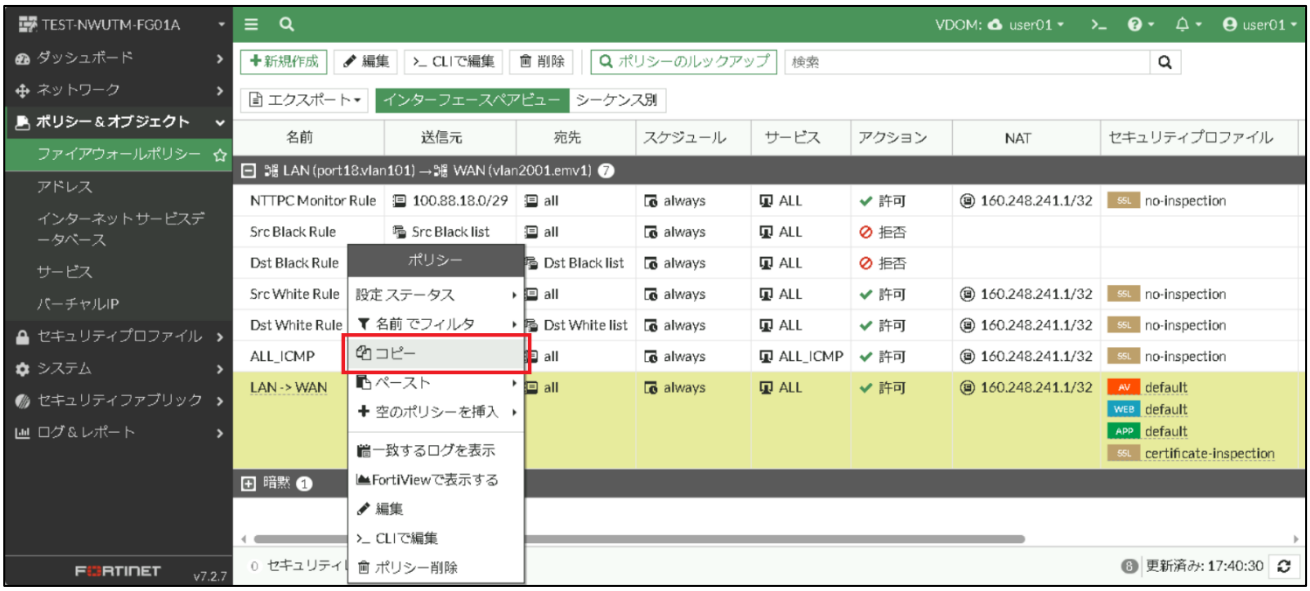
③　名前、外部 IP アドレス/範囲、マップされた IP アドレス/範囲を記載する。
※タイプはスタティック NAT であること
また、ポートフォワードを設定したい場合はポートフォワードのトグルをオンにし、入力を行う。
最後に OK を押して設定を完了する。



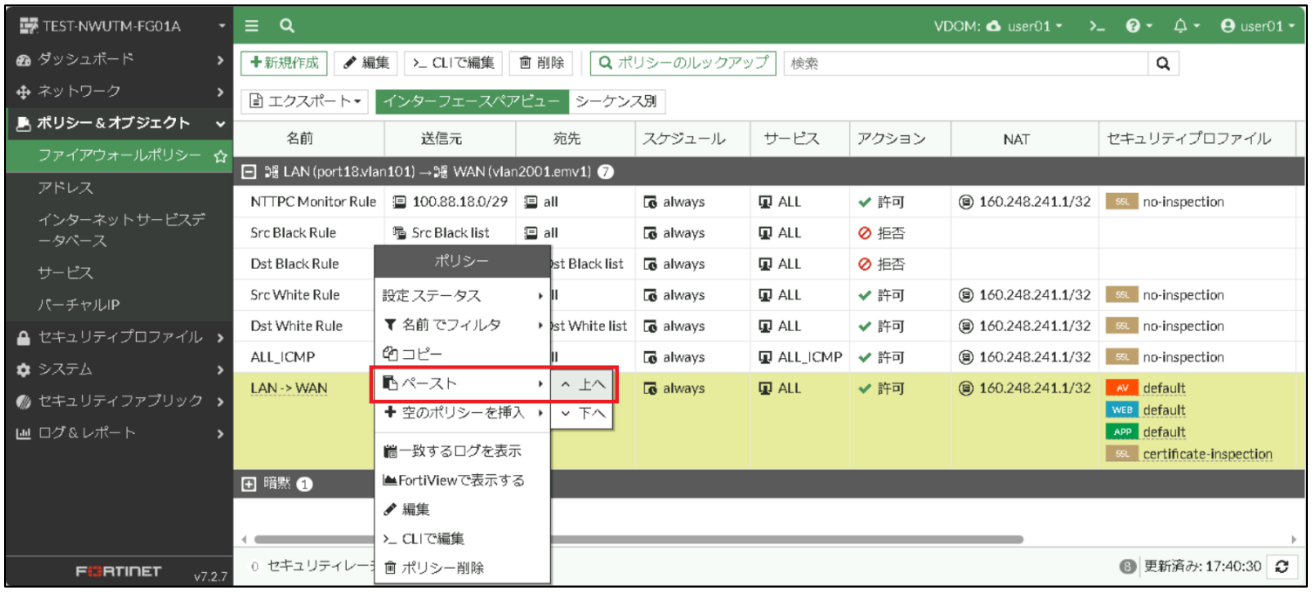
④　左メニューよりポリシー&オブジェクト→ファイアウォールポリシーを選択する。



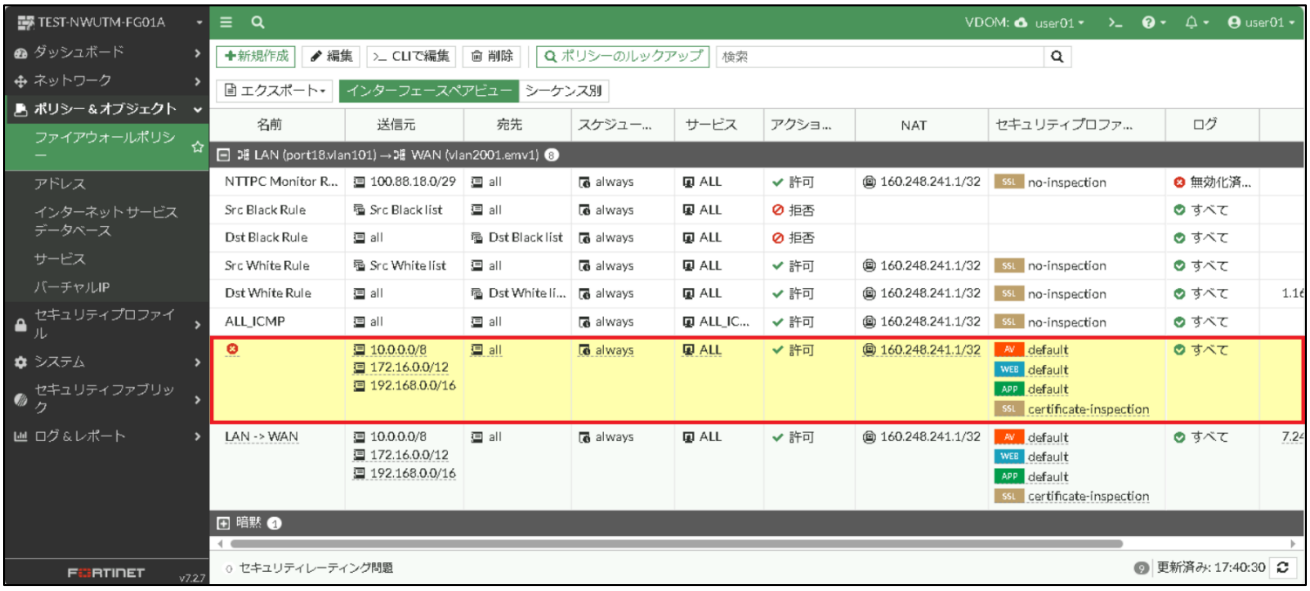
⑤　LAN→WAN を右クリックし、コピーを押下する。



⑥　再度 LAN→WAN を右クリックし、ペースト→上へを押下する。

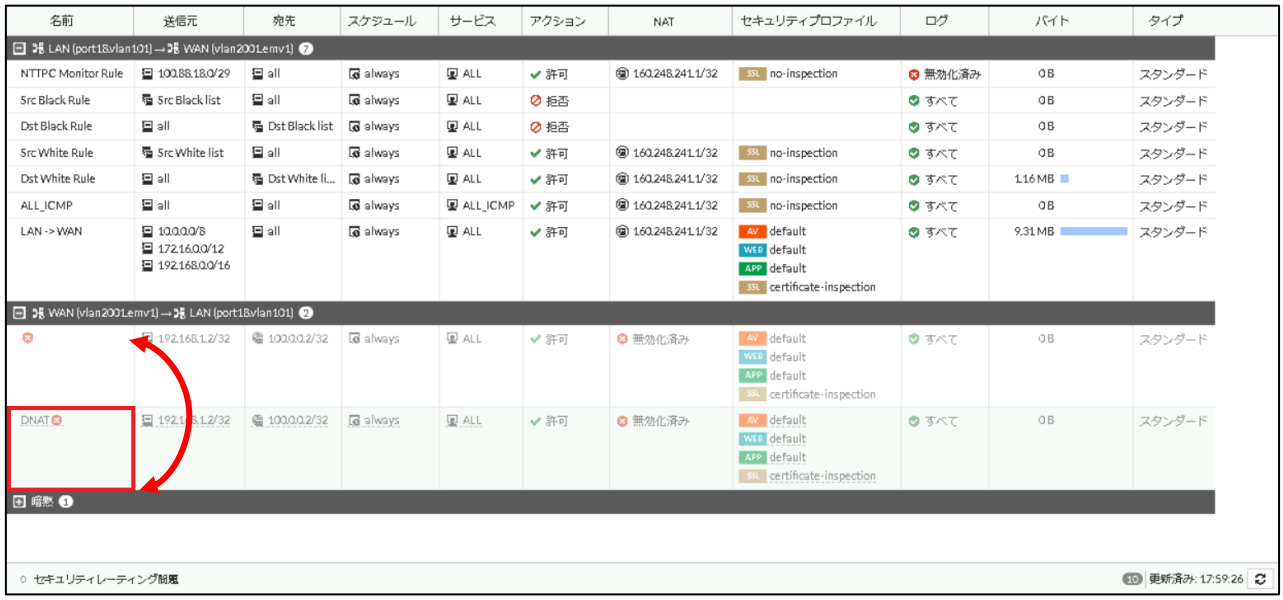


⑦　作成したポリシーをダブルクリックする。

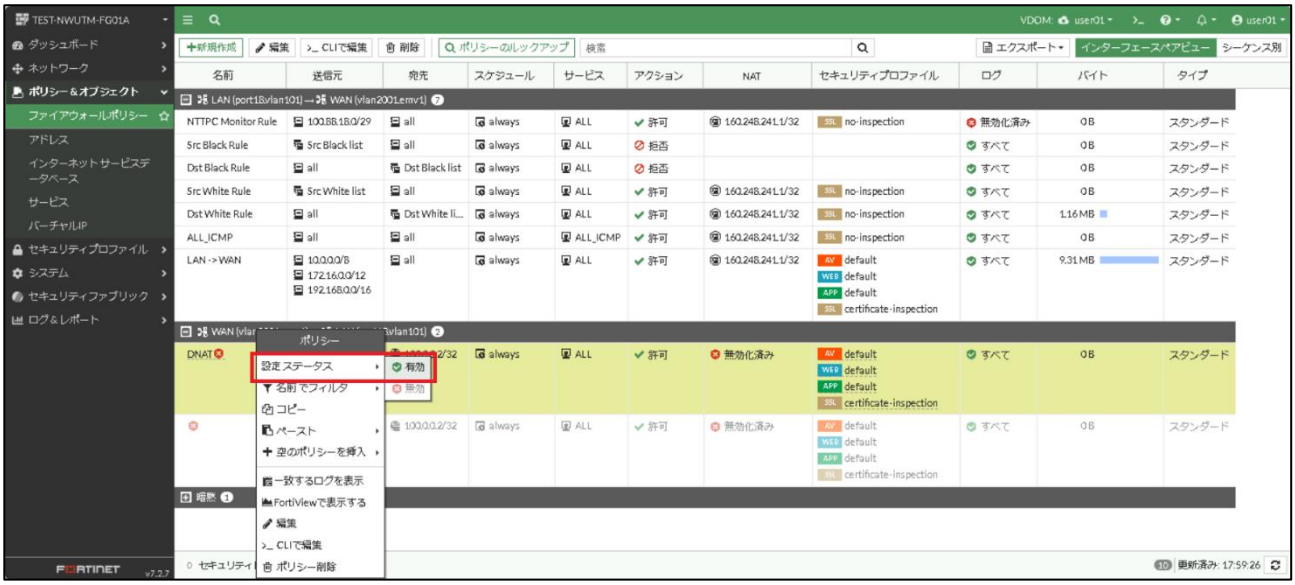


⑧ 名前、発信インターフェース、着信インターフェース、送信元、宛先（バーチャル IP)、サービス、NAT、セキュリティプロファイル、コメント（任意）を設定し OK を押下する。
※DNAT を使用する場合は宛先を DNAT 用の追加グローバル IP を設定します。
※DNAT の宛先に指定されたサーバがインターネット向けにルーティングされていない場合は有効化してください。

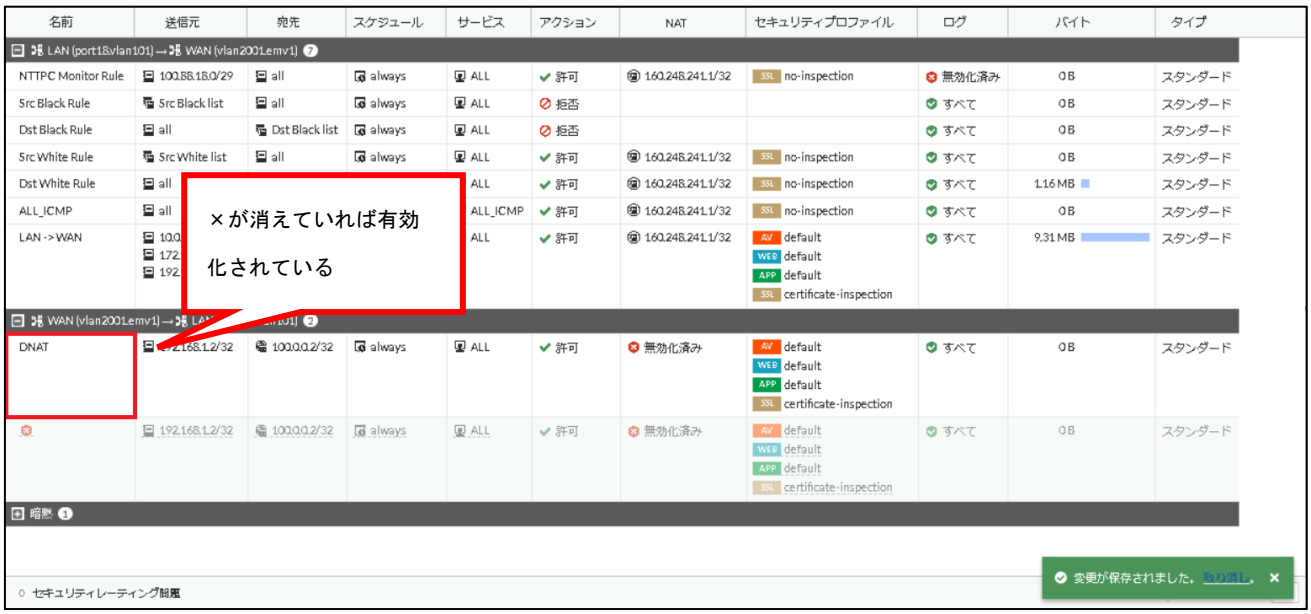
⑨　作成したルールを WAN→LAN 内で投入したい場所に名前部分でドラッグ&ドロップし移動させる。（DNAT が複数行ある場合）



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。

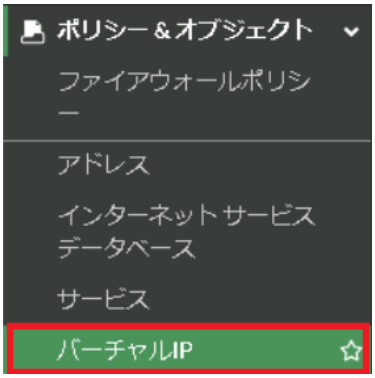


⑪　ルールが有効になったことを確認する。

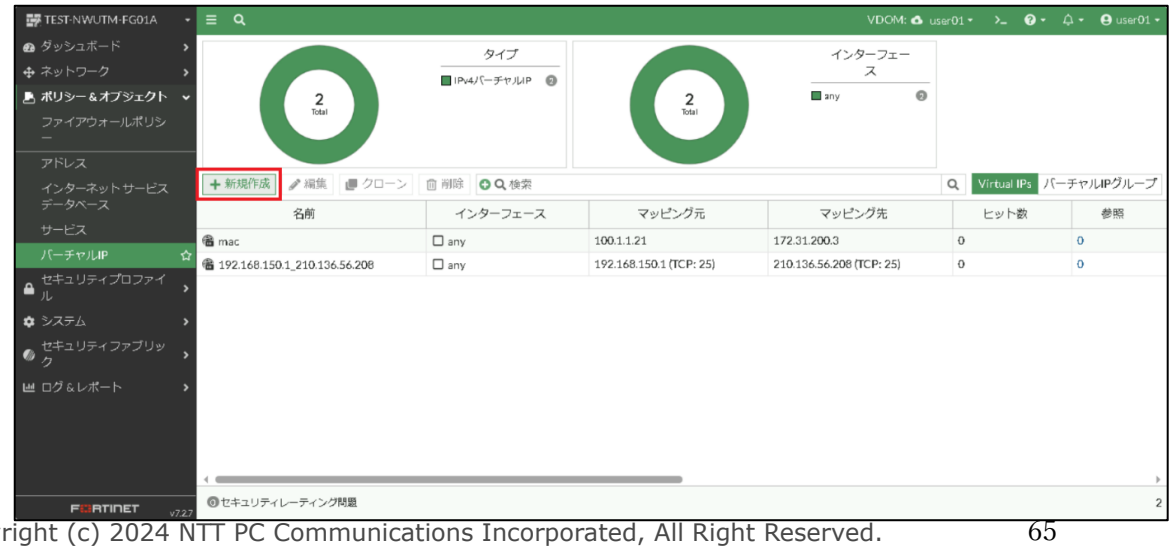


4.12 DNAT 設定方法（表示形式：シーケンス別の場合）

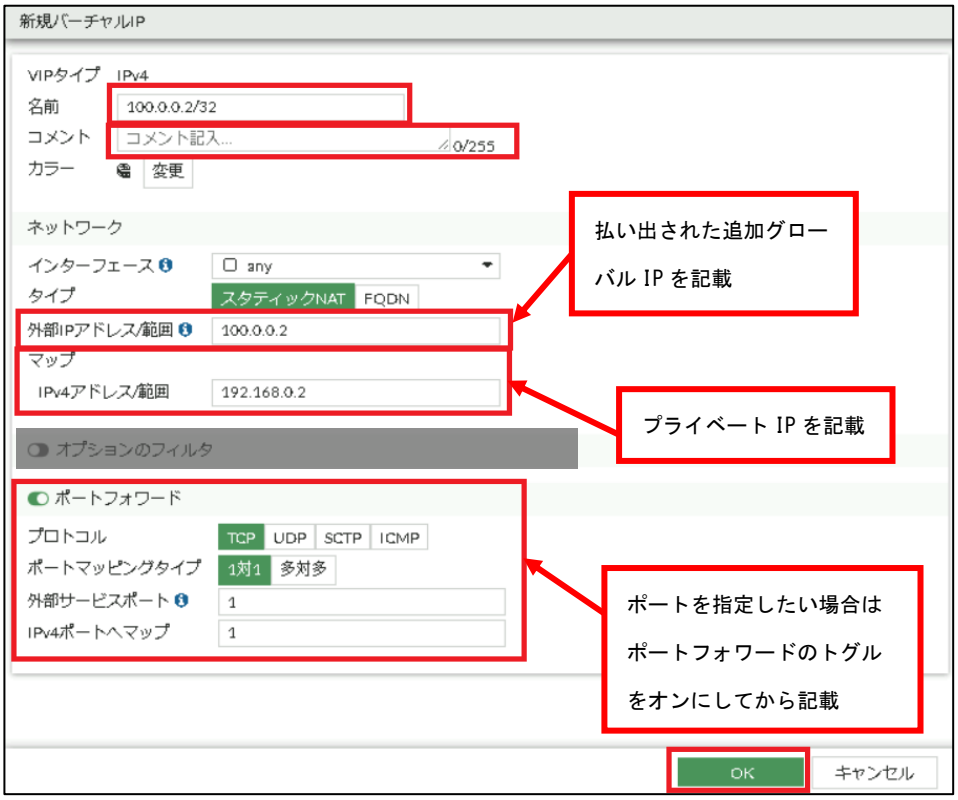
①　左メニューよりポリシー&オブジェクト→バーチャル IP を選択する。



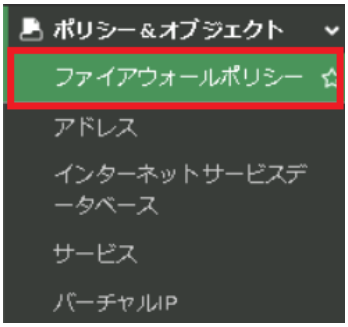
②　新規作成を押下する。



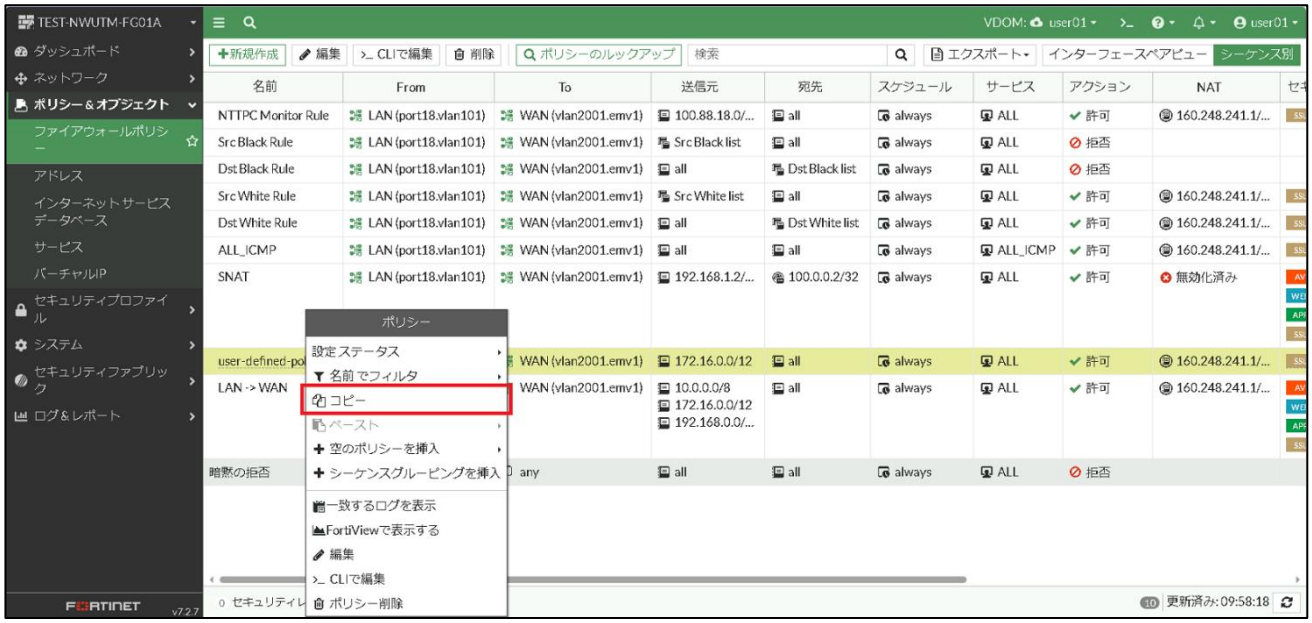
③　名前、外部 IP アドレス/範囲、マップされた IP アドレス/範囲を記載して OK を押下する。
※タイプはスタティック NAT であること
また、ポートフォワードを設定したい場合はポートフォワードのトグルをオンにし、入力を行う。
最後に OK を押して設定を完了する。



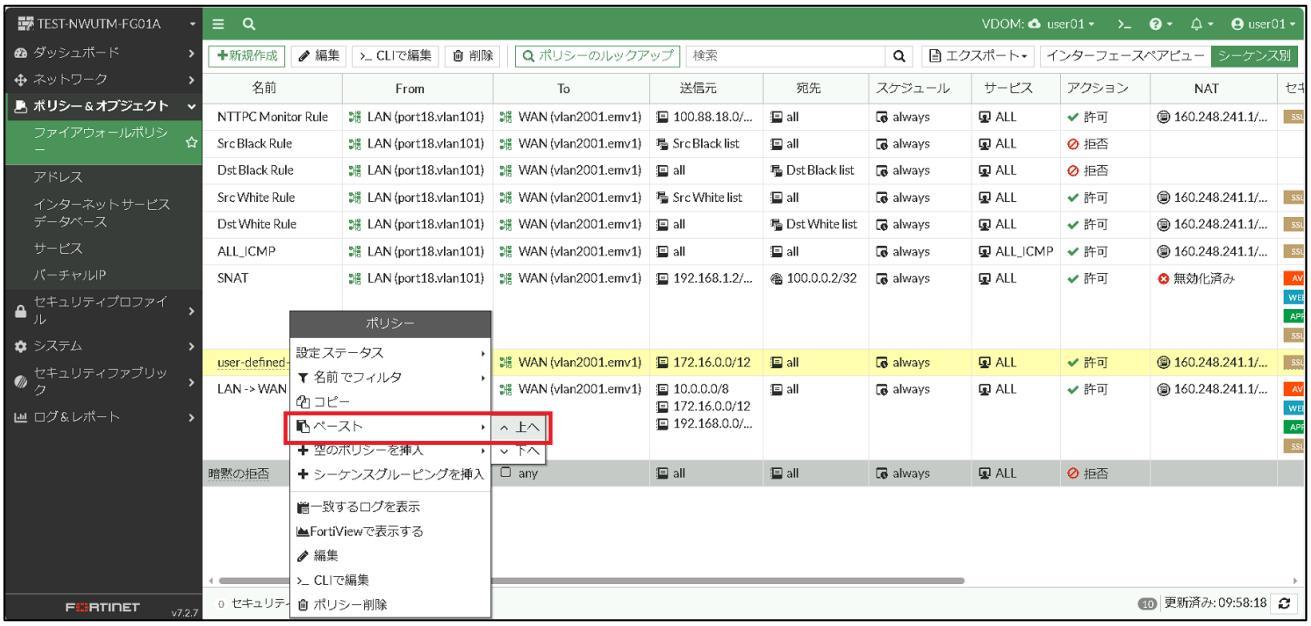
④　左メニューよりポリシー&オブジェクト→ファイアウォールポリシーを選択する。



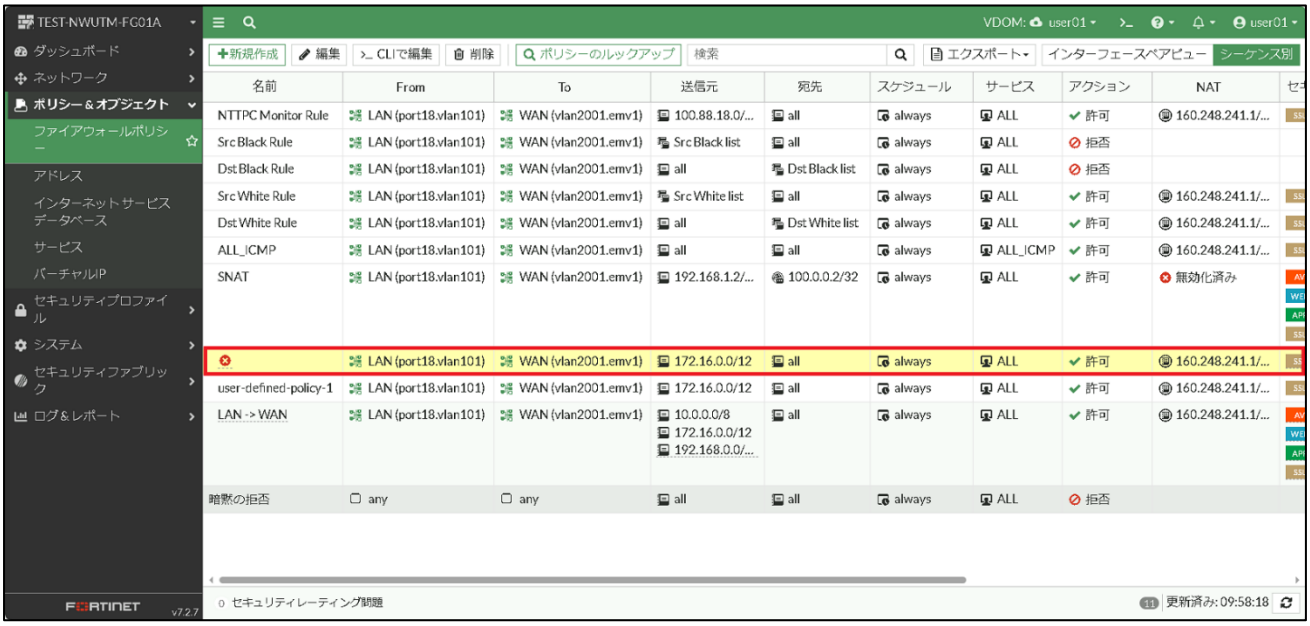
⑤　user-defined-policy-1 を右クリックし、コピーを押下する。



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。



⑦　作成したポリシーをダブルクリックする。



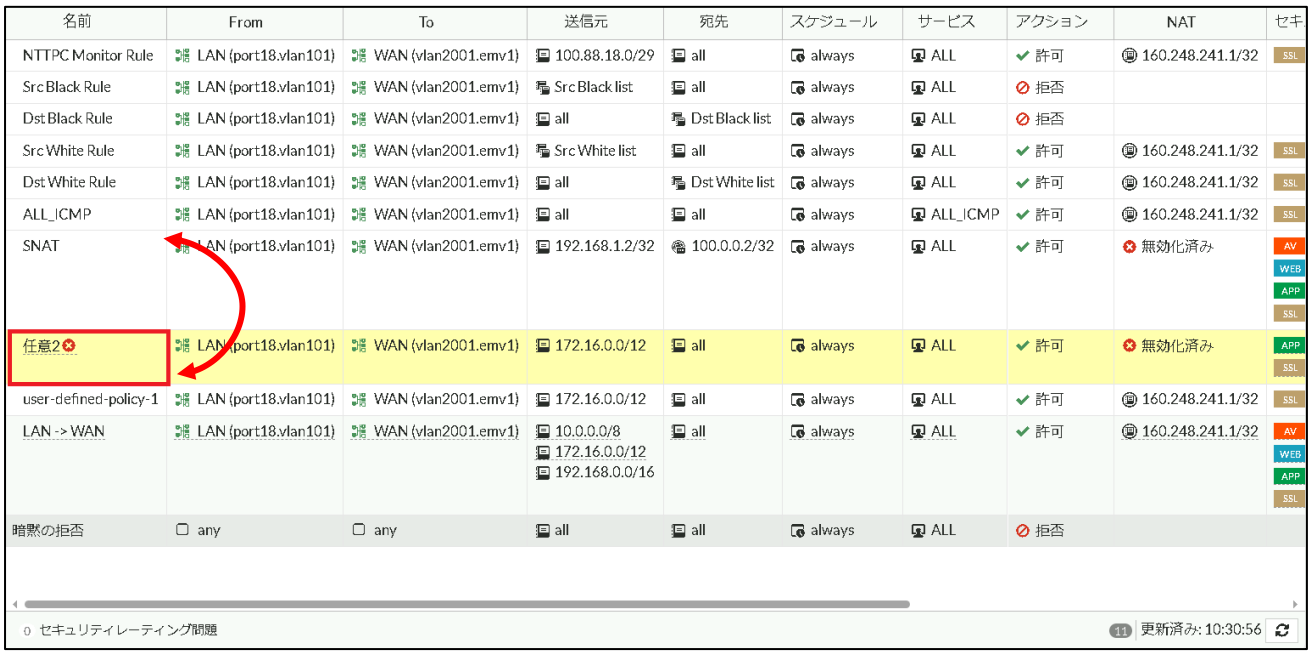
⑧ 名前、送信元、宛先（バーチャル IP）、サービス、NAT、セキュリティプロファイル、コメント（任意）を設定し OK を押下する。
※DNAT を使用する場合は宛先を DNAT 用の追加グローバル IP を設定します。
※DNAT の宛先に指定されたサーバがインターネット向けにルーティングされていない場合は有効化してください。

「+」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。

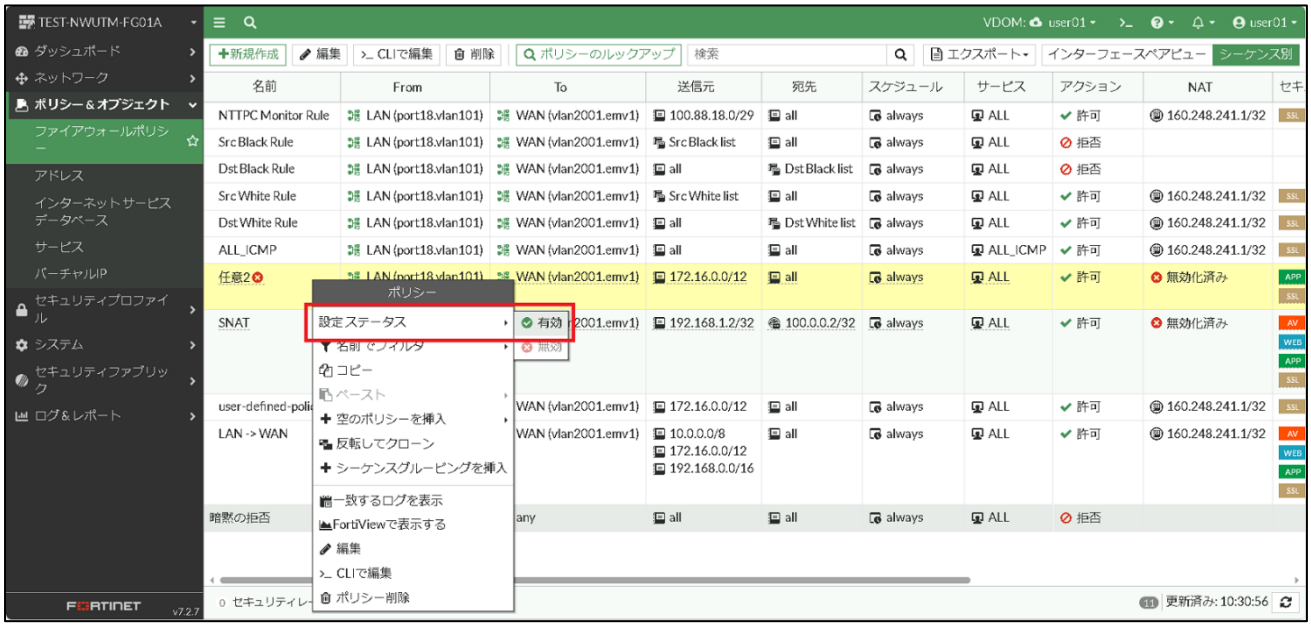
DNAT を使用する場合は必ず無効化（※）

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

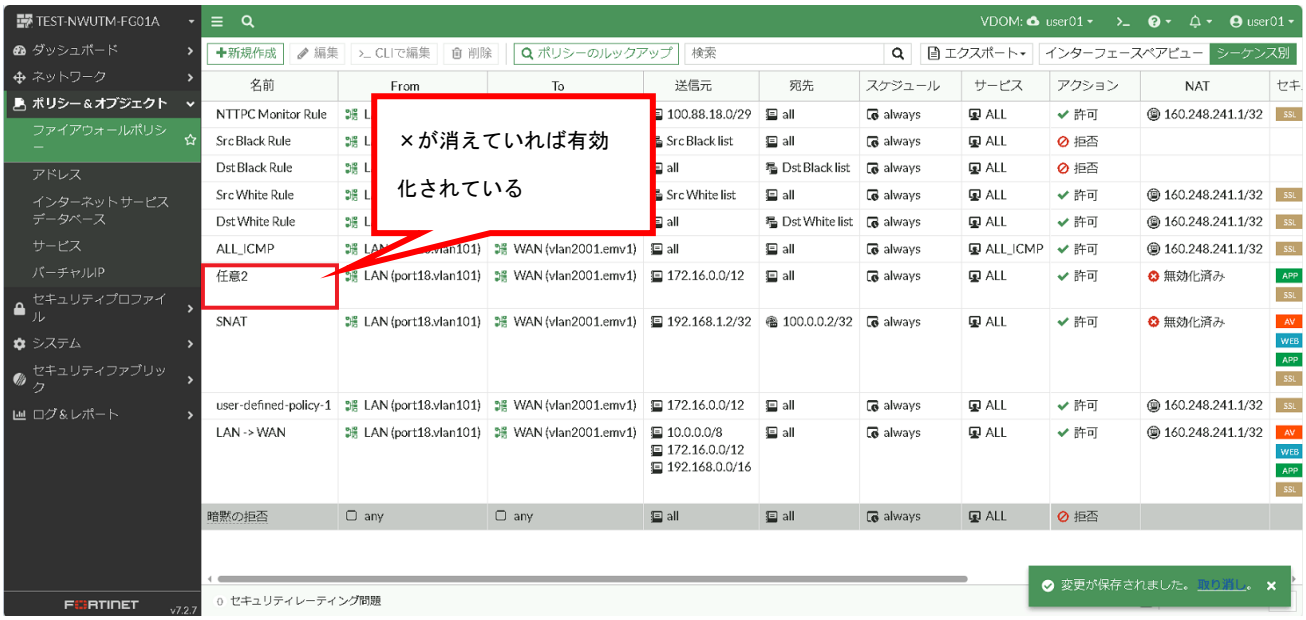
⑨　作成したルールを ALL_ICMP より下、SNAT より上の投入したい場所に名前部分でドラッグ&ドロップし移動させる。



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。



⑪　ルールが有効になったことを確認する。

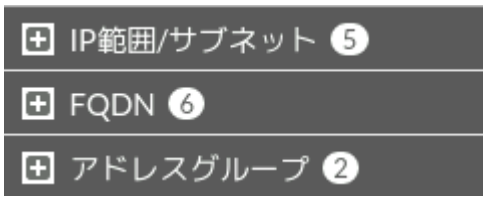


5　アドレスの設定方法

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。

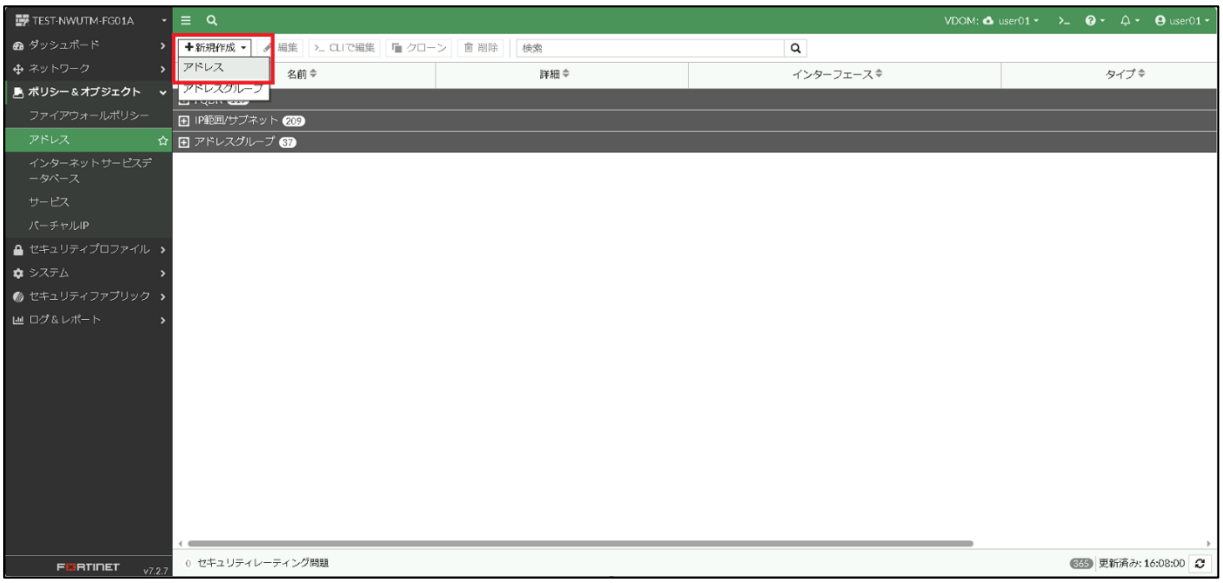
※「＋」を押下すると一覧が表示されます。



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

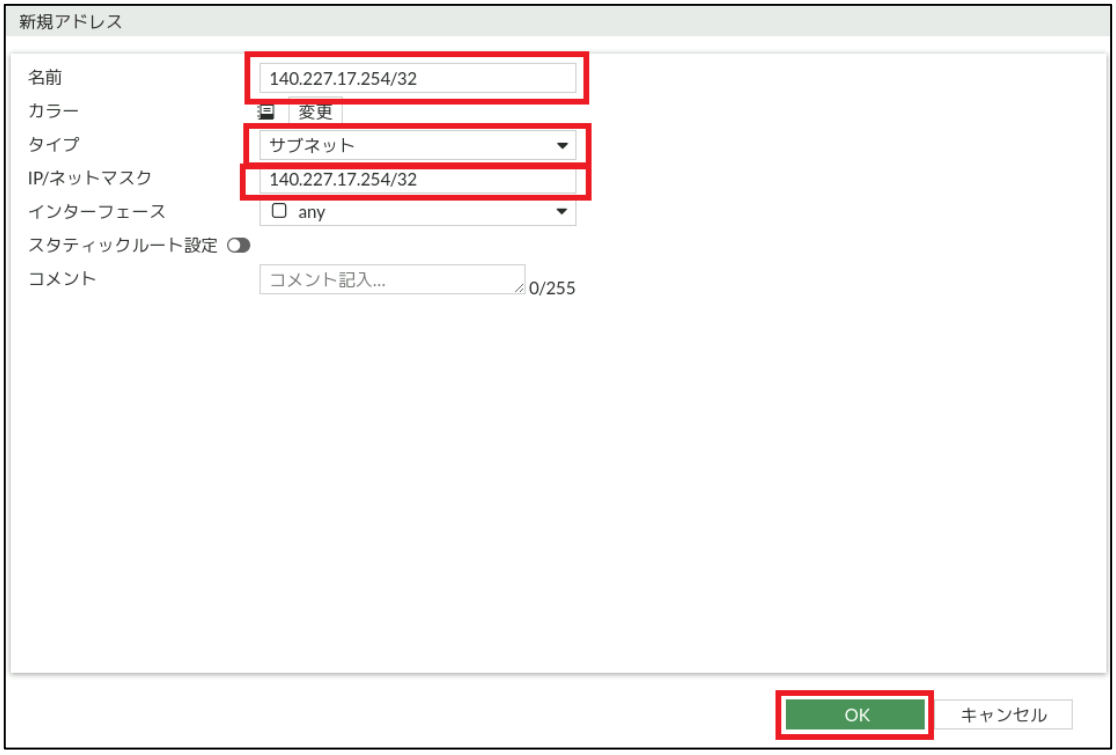
I.　サブネットの場合は、IP/ネットマスクを記載して OK を押下する。

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



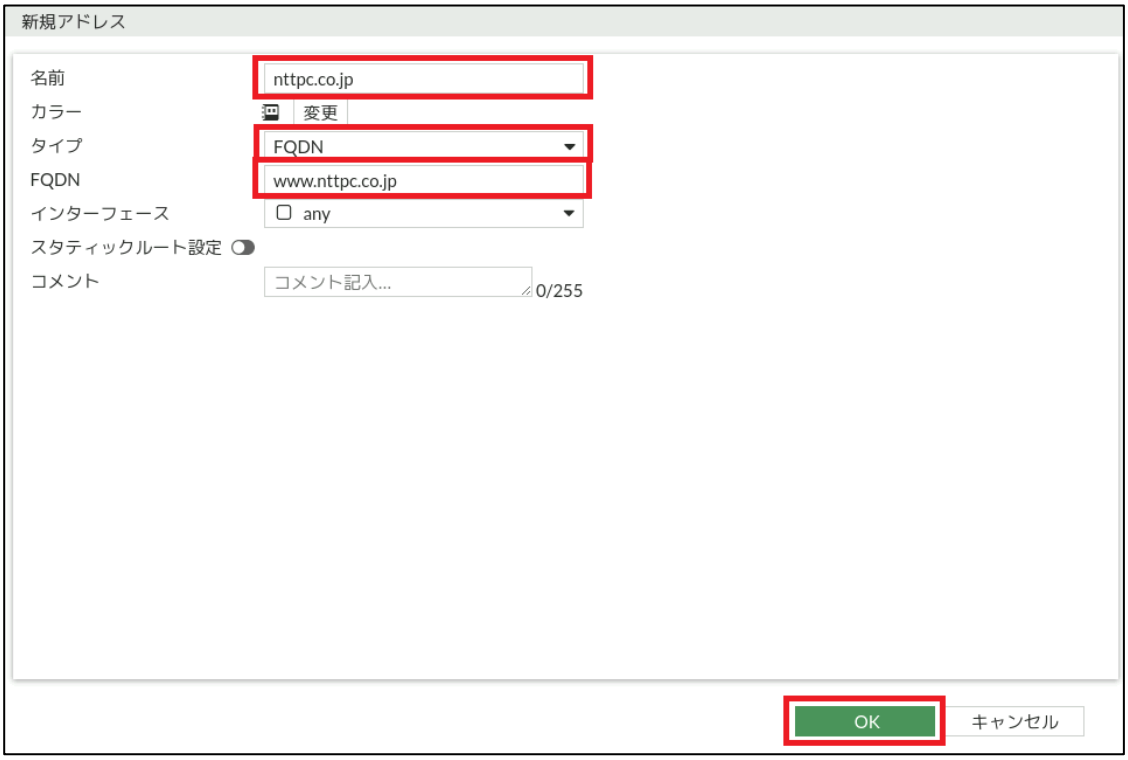
II. FQDN の場合は、FQDN を記載して OK を押下する。

例：https://www.nttpc.co.jp を追加する場合

名前：nttpc.co.jp

タイプ：FQDN

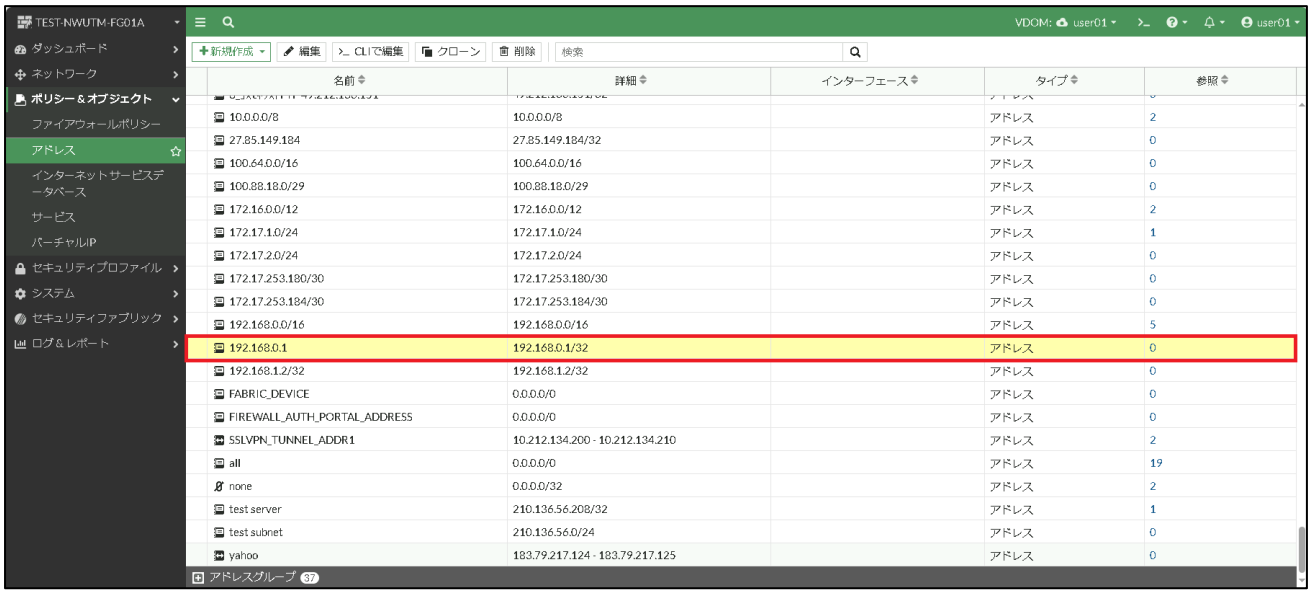
FQDN：www.nttpc.co.jp



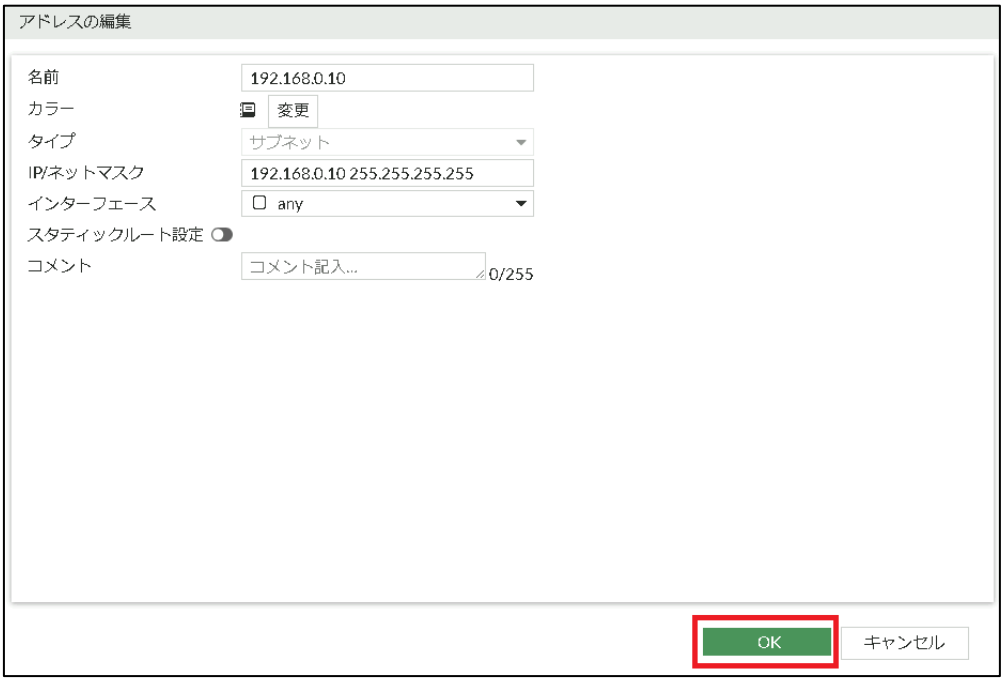
5.2　アドレスの変更

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。



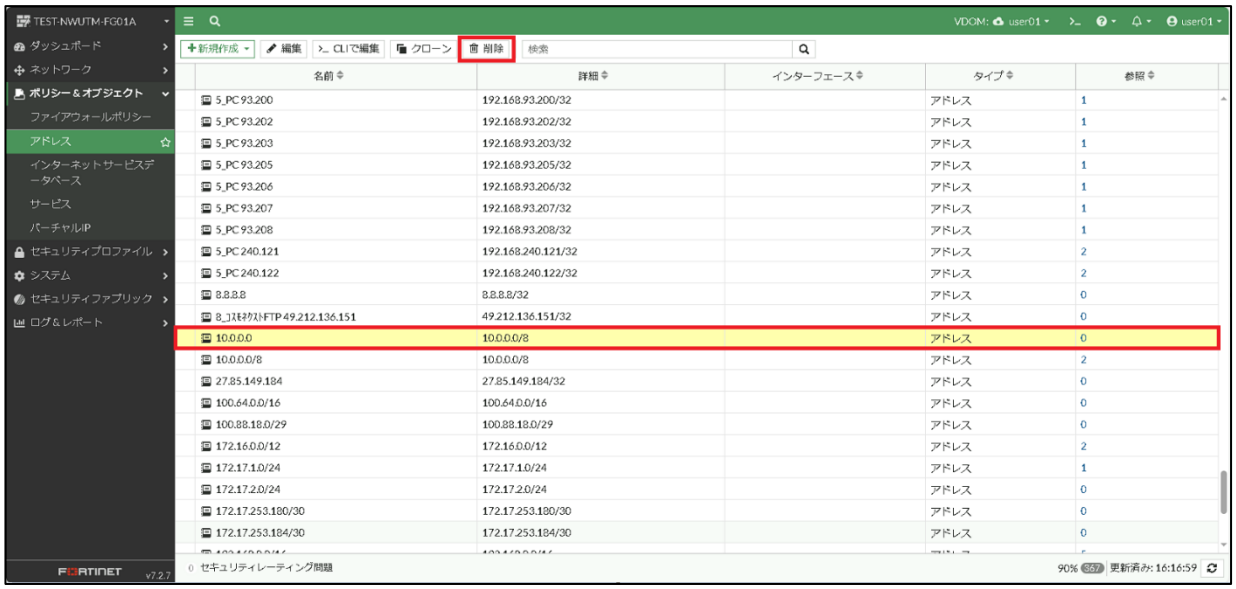
③ 変更箇所の変更をして OK を押下する。



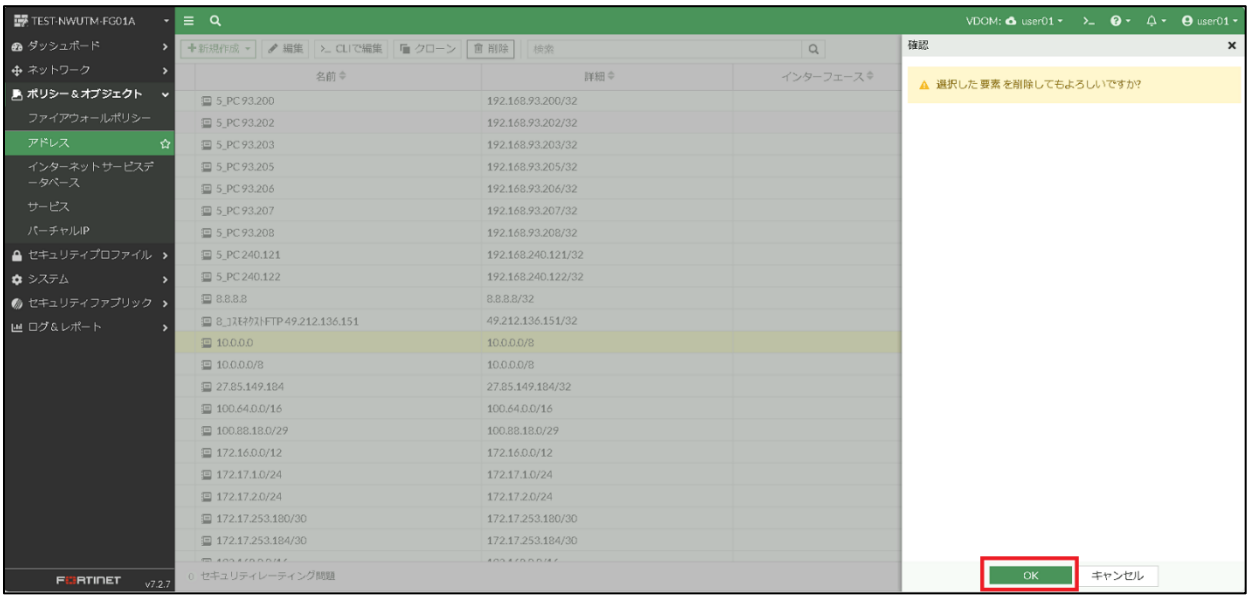
5.3　アドレスの削除

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。



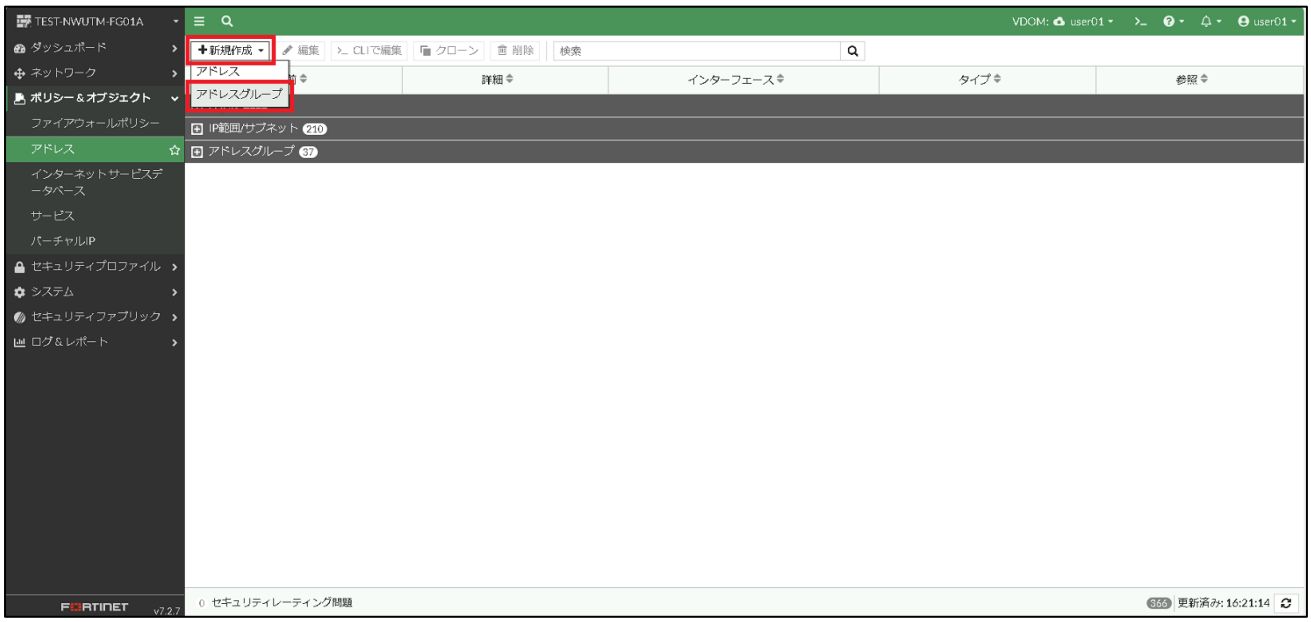
6　アドレスグループの設定方法

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。

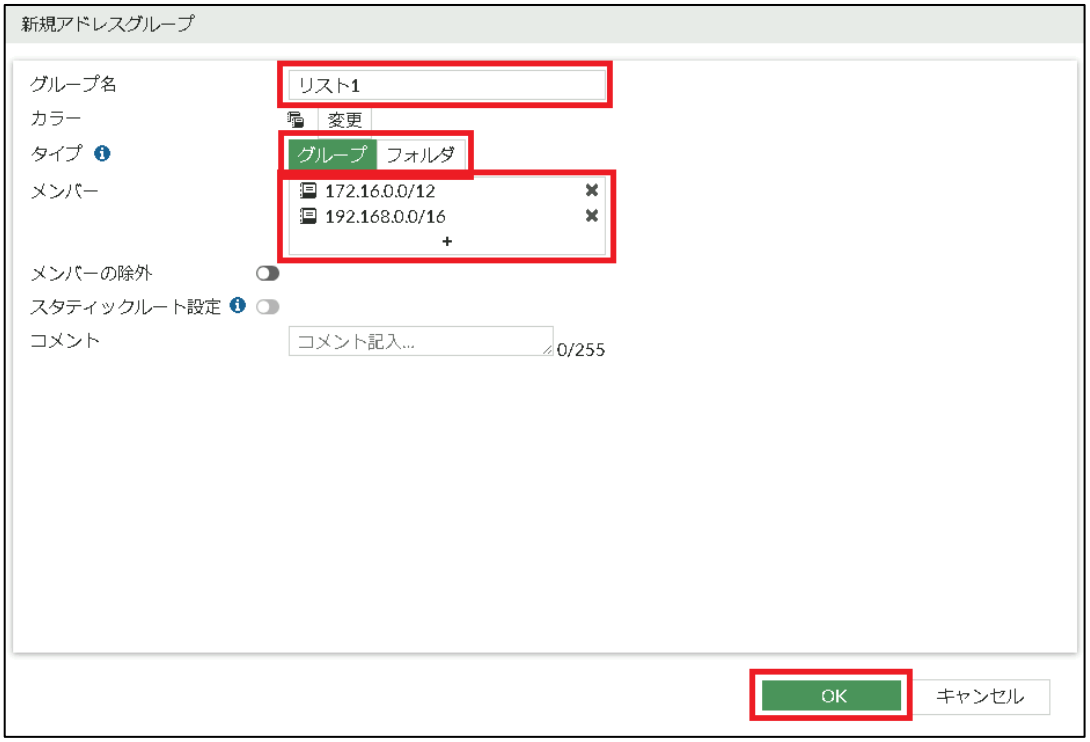
6.1　アドレスグループの追加

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。

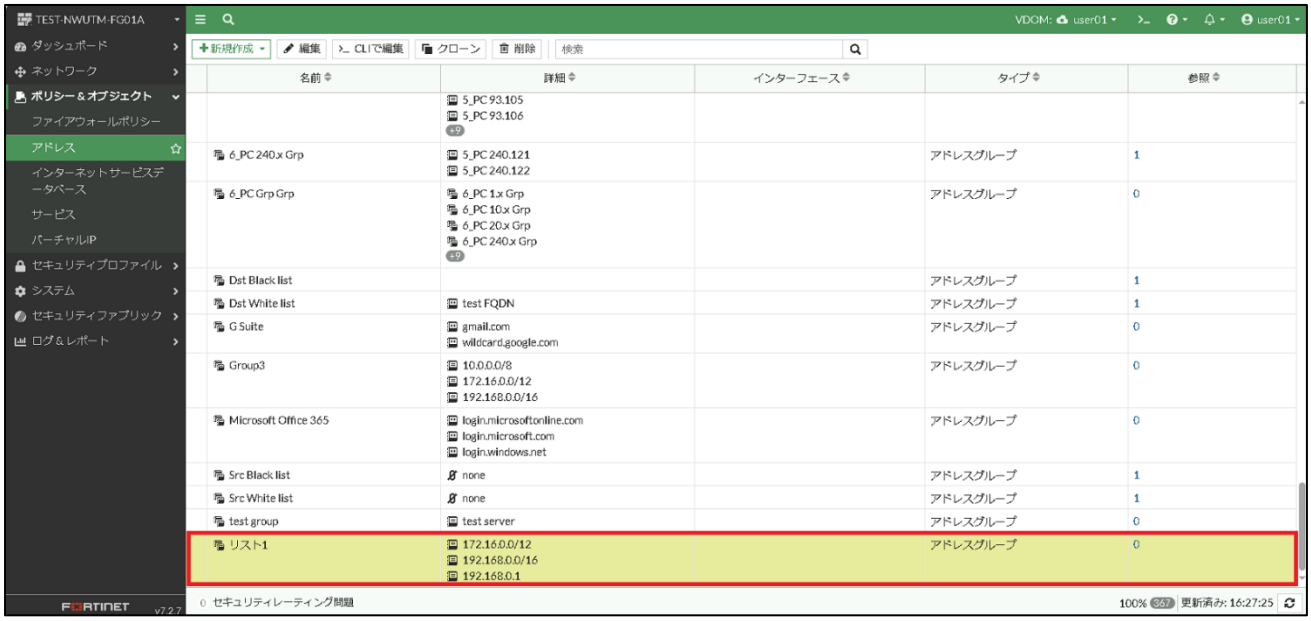


例：172.16.0.0/12 と 192.168.0.0/16 のようなセグメントが違うアドレスをメンバーに設定することにより 1 グループとして利用することが可能となります。
※メンバーは 5.2 項で登録したアドレスを使用します。

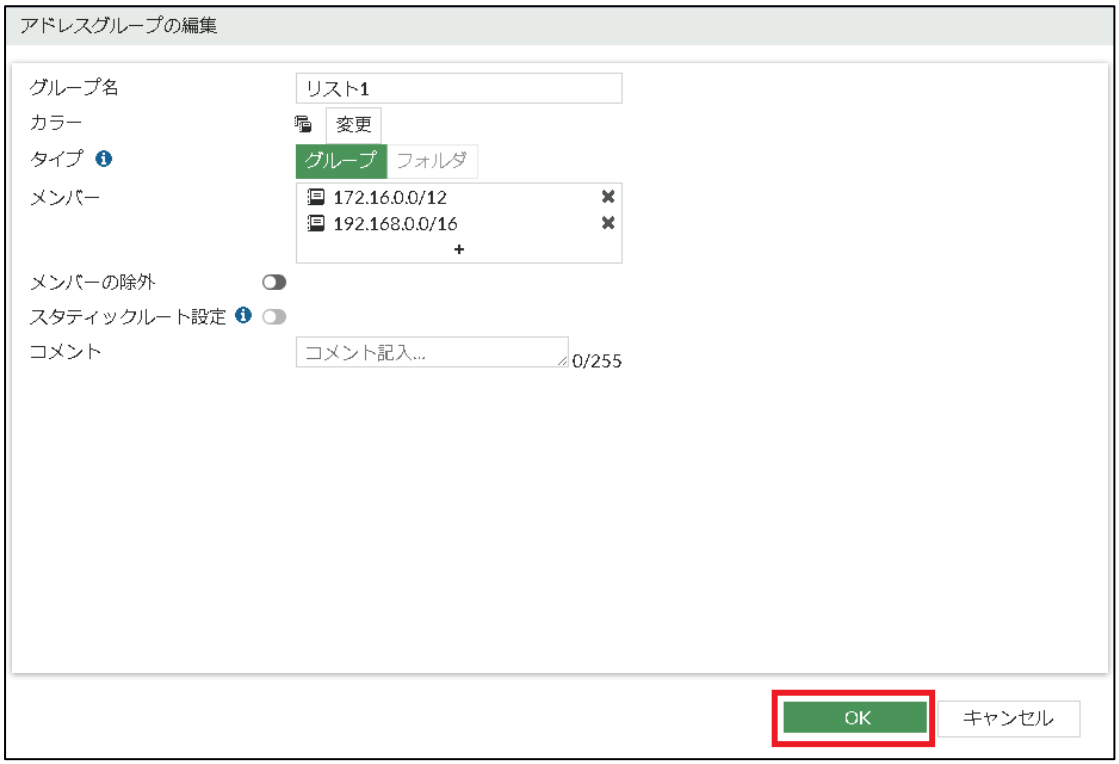
6.2　アドレスグループの変更

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。



③ 変更したいメンバーを変更し、OK クリックします。

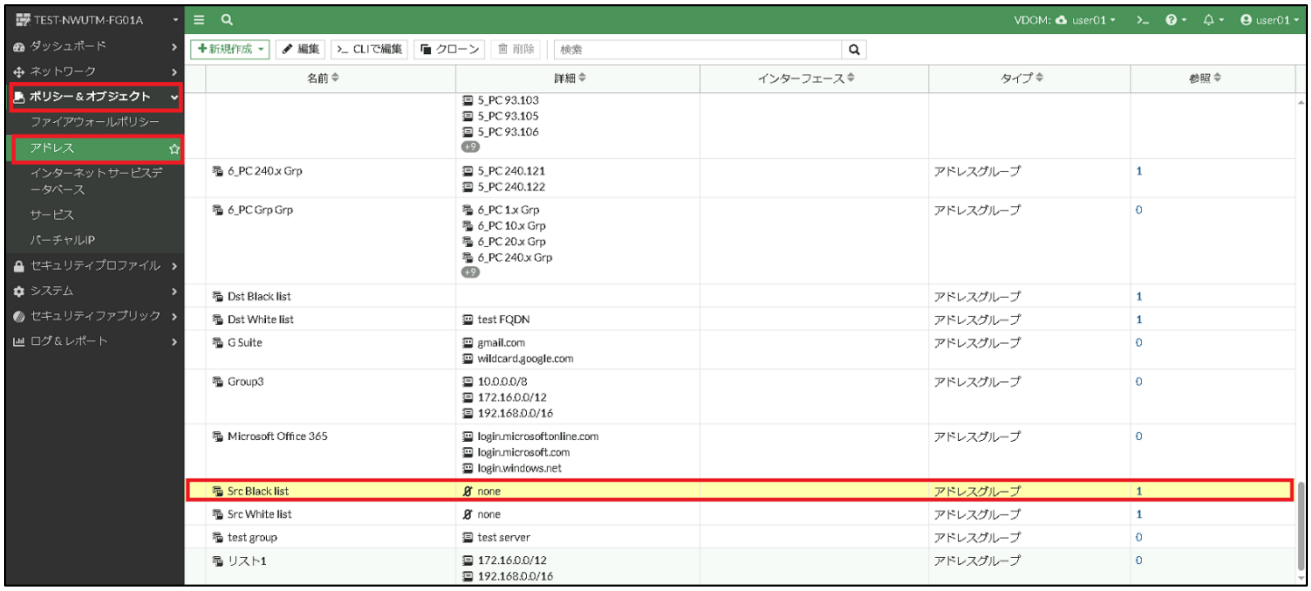


6.3　ホワイトリスト・ブラックリストへの設定

①　Src Black list への設定方法

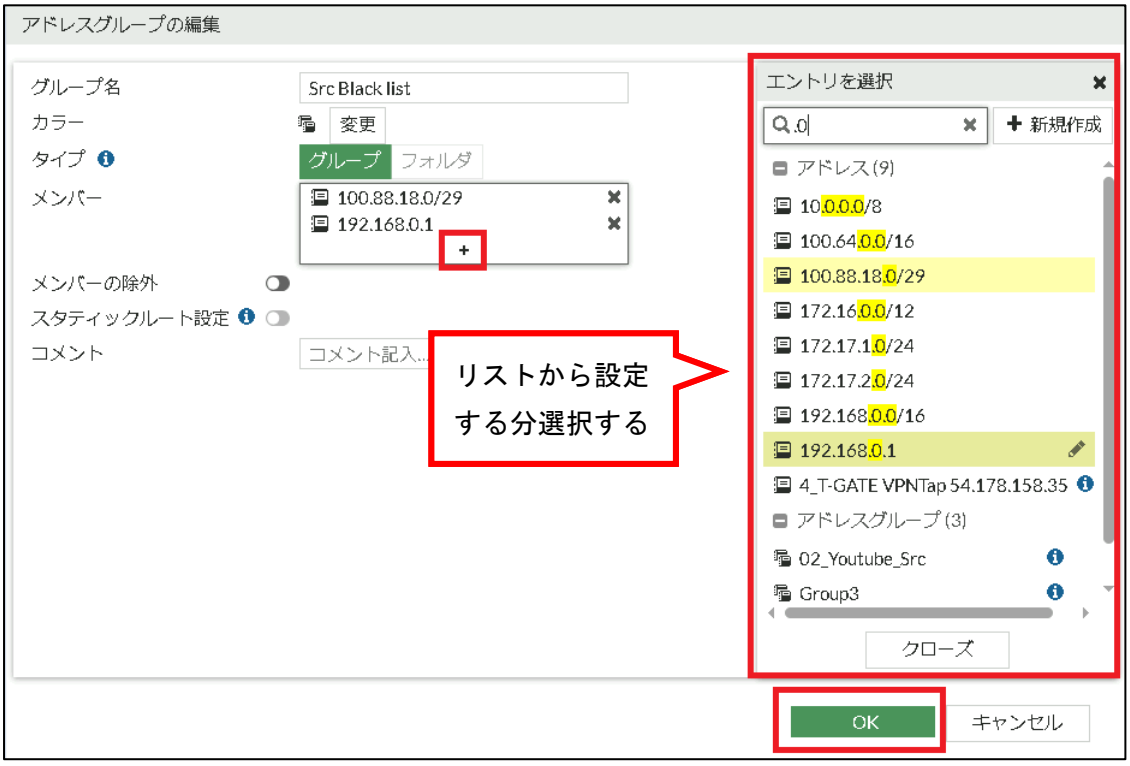
※業務上どこにも通信させたくないクライアント端末などを設定するリストになります。

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。



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。

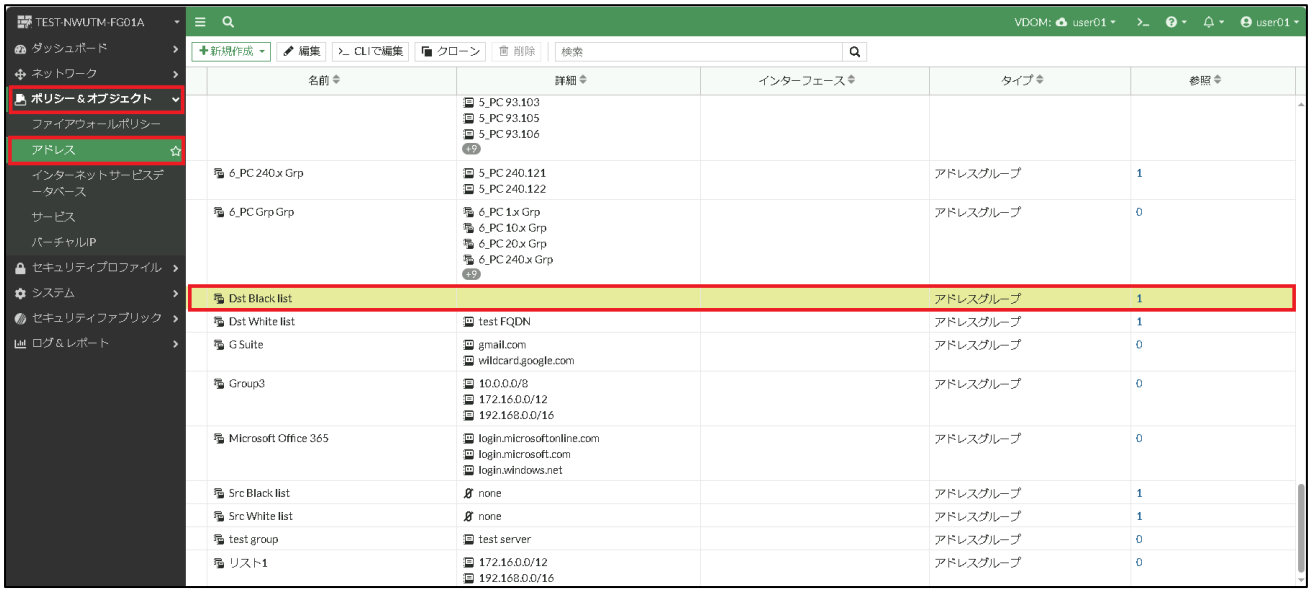
III. 投入したい分選択したら OK を押下する。



② Dst Black list への設定方法

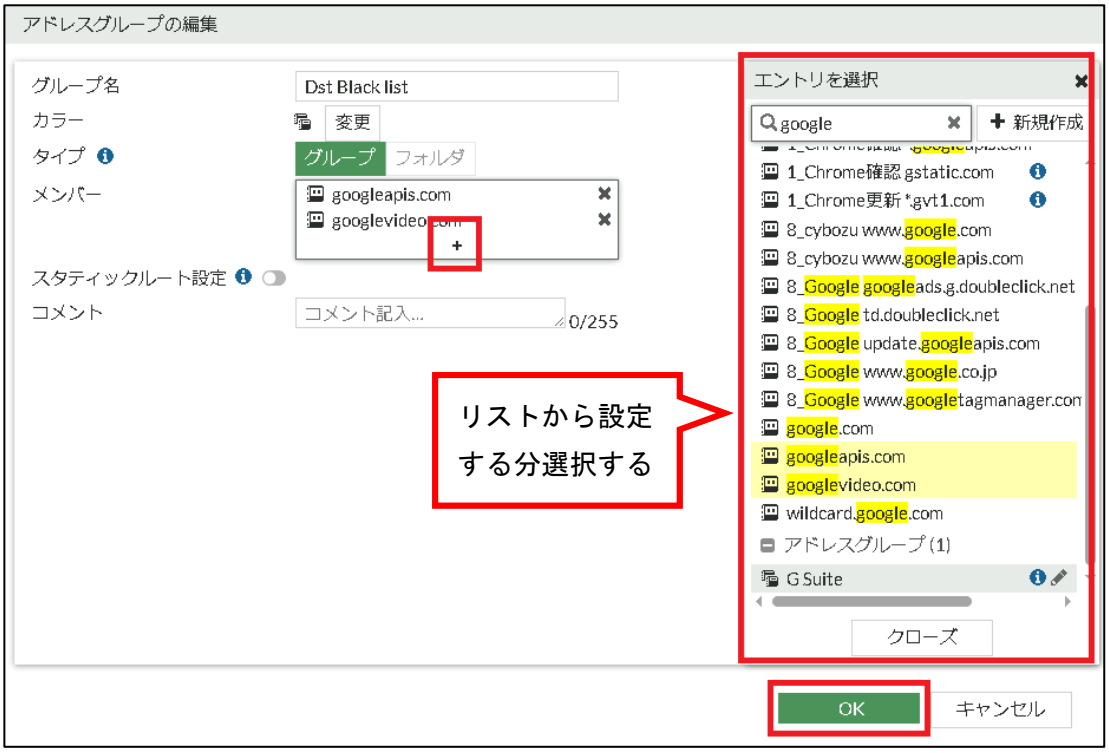
※業務上接続させたくない Web サイトなどを設定するリストになります。

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。



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。

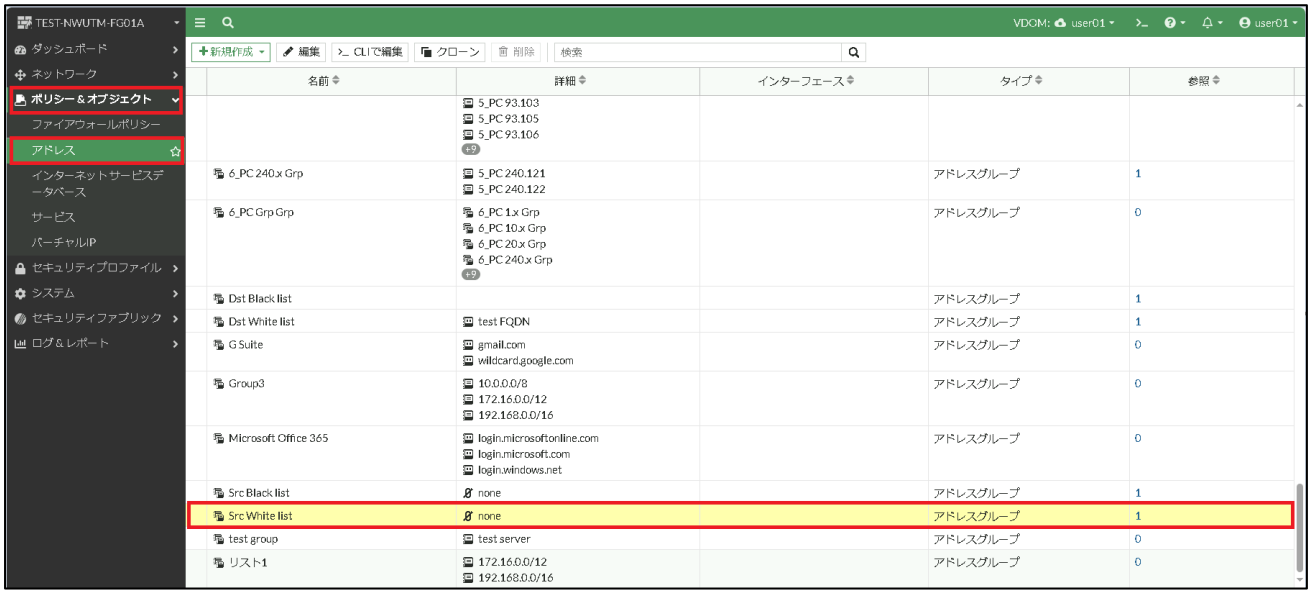
III. 投入したい分選択したら OK を押下する。



③ Src White list への設定方法

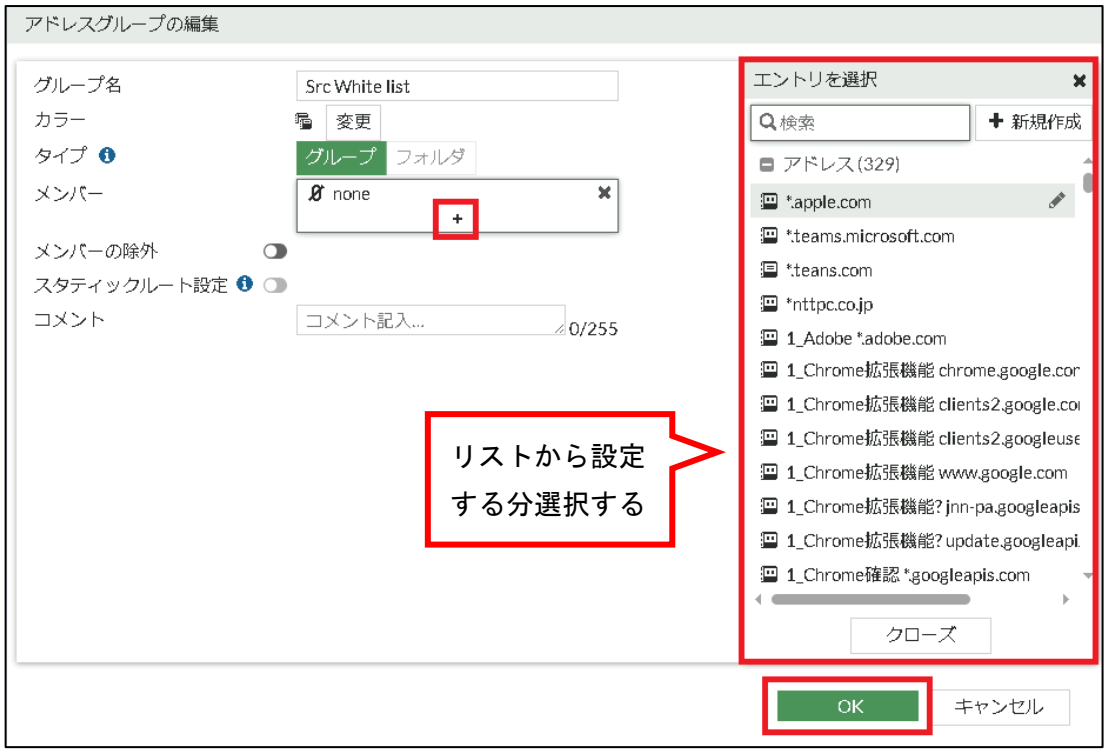
※セキュリティ機能を無効にし、通信を行いたいクライアント端末などを設定するリストになります。

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。



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。

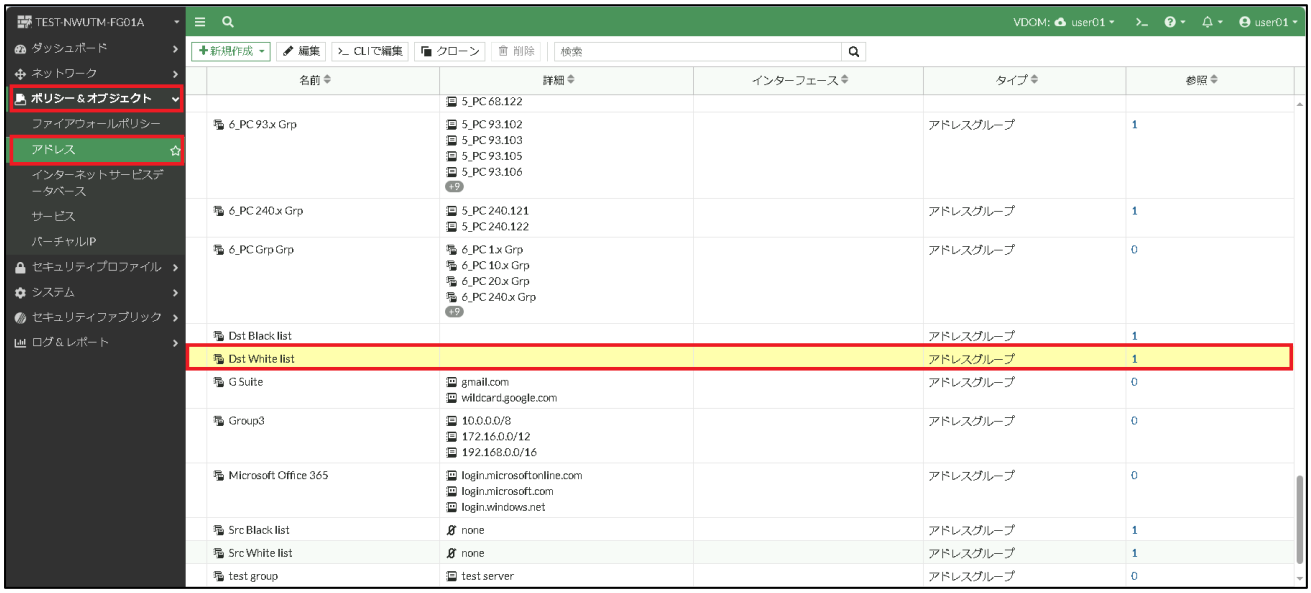
III. 投入したい分選択したら OK を押下する。



④ Dst White list への設定方法

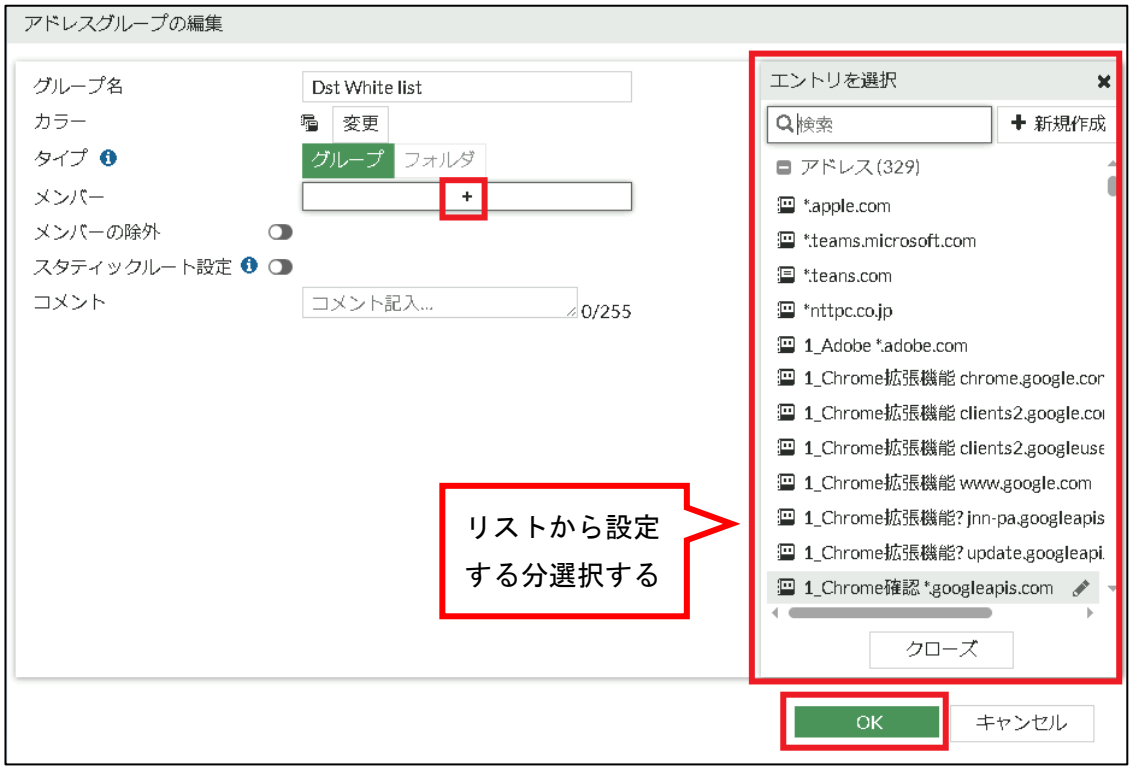
※信頼のある Web サイトなどを設定することにより、セキュリティ機能を無効にした状態で通信をすることができるリストです。

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。



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。

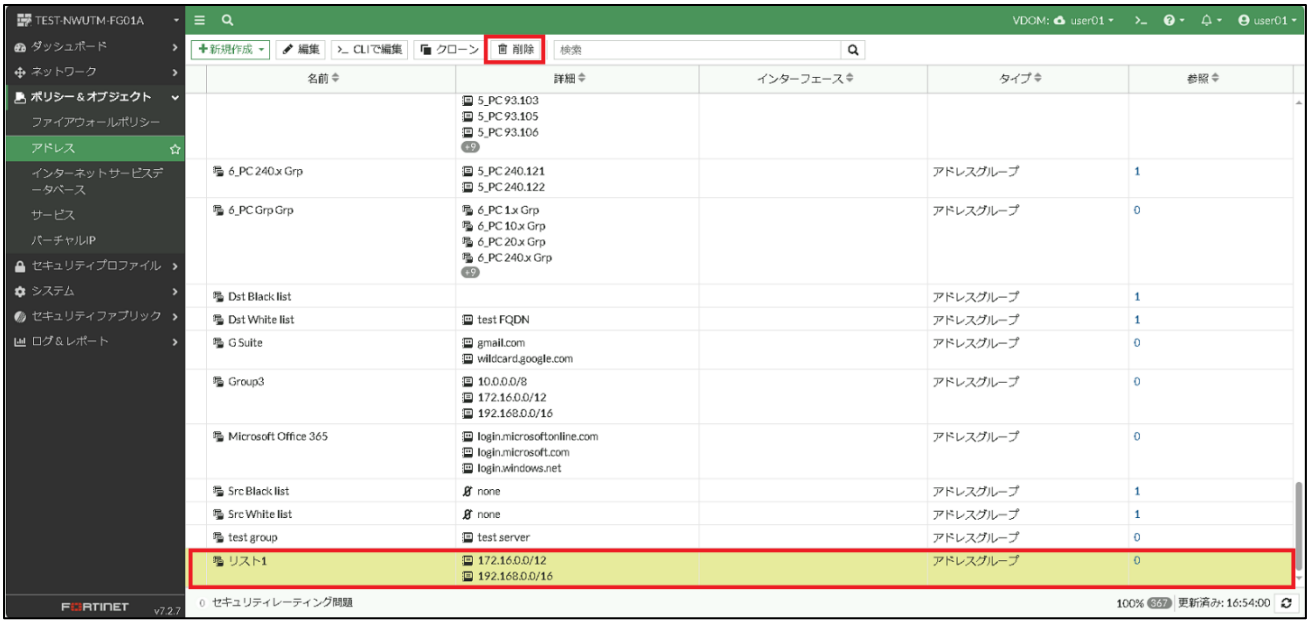
III. 投入したい分選択したら OK を押下する。



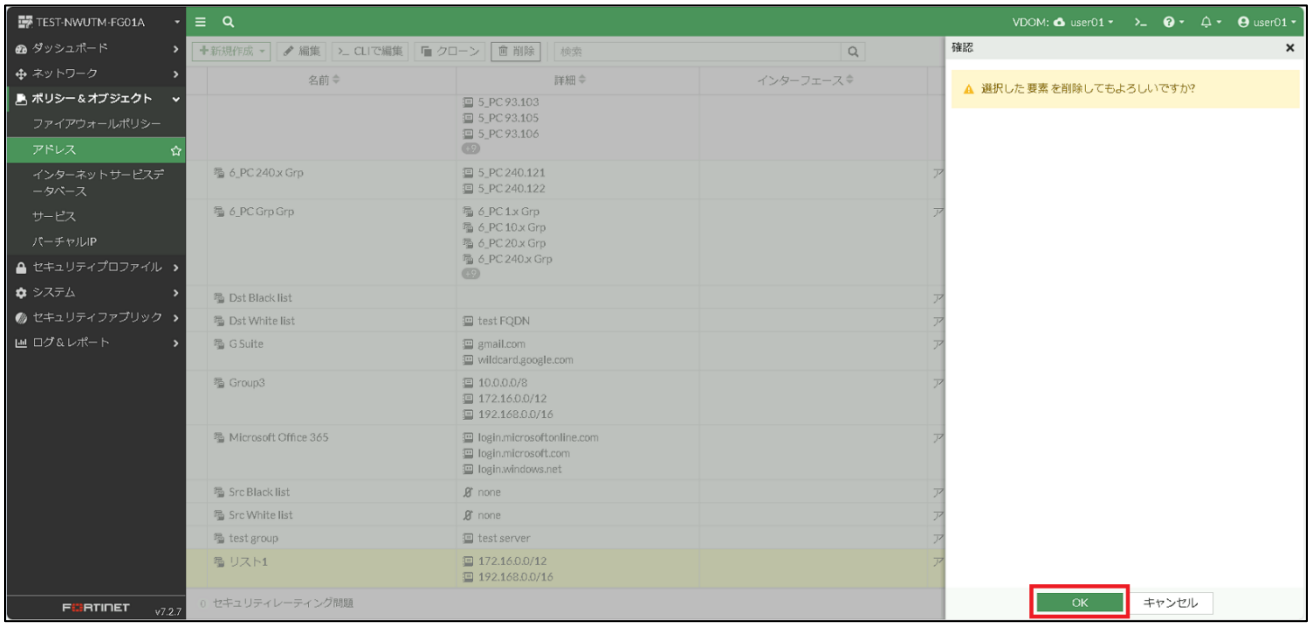
6.4　アドレスグループの削除

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。



③ 確認ウィンドウがでるので、OK をクリックします。

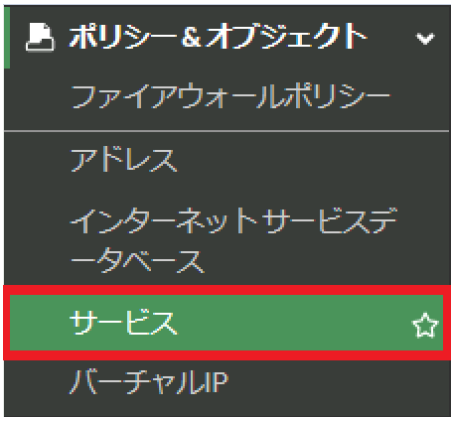


7　サービスの設定方法

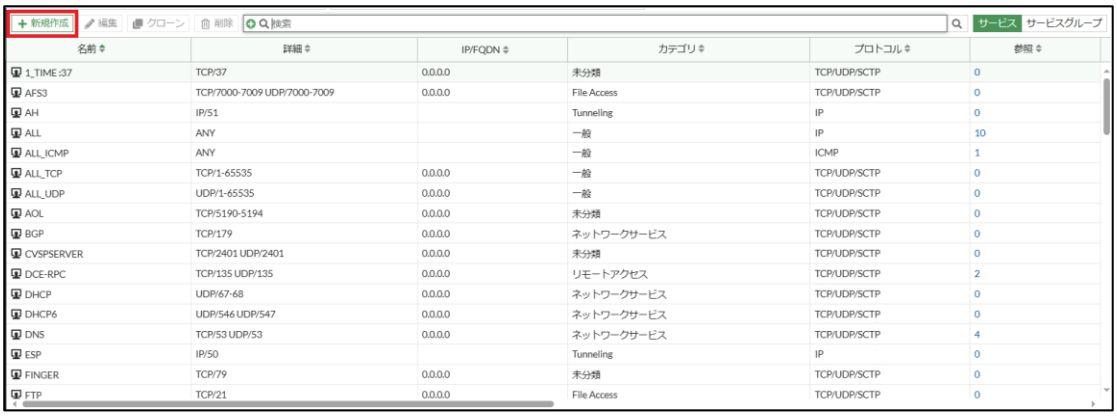
本章では、ファイアウォールルールで設定するサービス（TCP や UDP など）の設定方法について解説しています。

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。

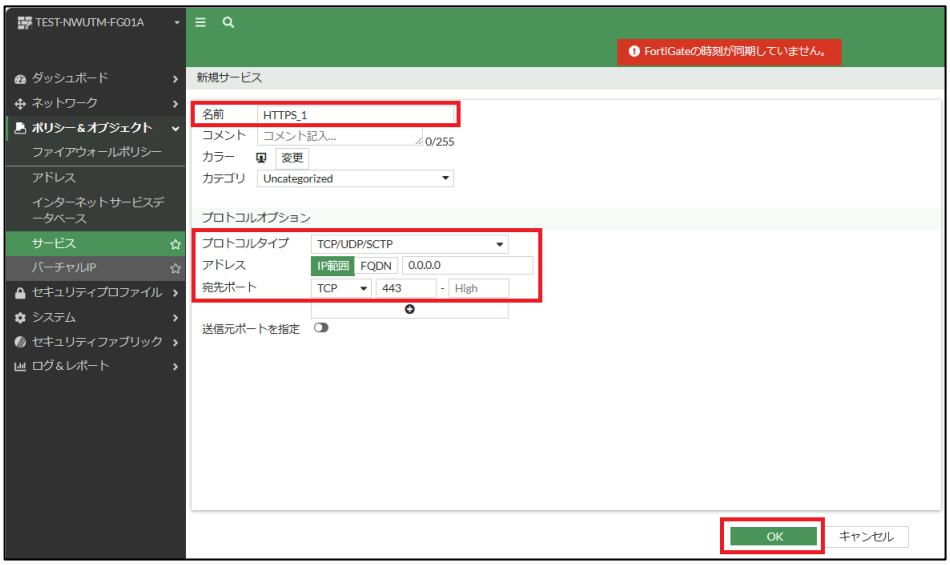


名前	詳細	IP/FQDN	カテゴリ	プロトコル	参照
1_TIME :37	TCP/37	0.0.0.0	未分類	TCP/UDP/SCTP	0
AFS3	TCP/7000-7009 UDP/7000-7009	0.0.0.0	File Access	TCP/UDP/SCTP	0
AH	IP/51		Tunneling	IP	0
ALL	ANY		一般	IP	10
ALL_ICMP	ANY		一般	ICMP	1
ALL_TCP	TCP/1-65535	0.0.0.0	一般	TCP/UDP/SCTP	0
ALL_UDP	UDP/1-65535	0.0.0.0	一般	TCP/UDP/SCTP	0
AOL	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。

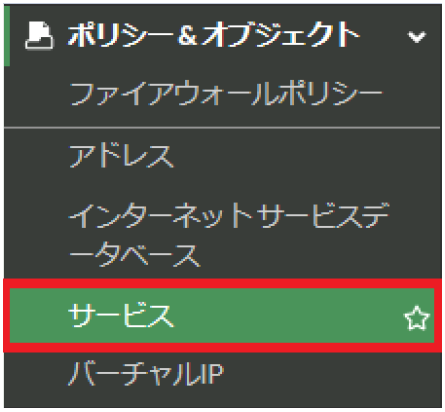
※プロトコルタイプは 3 種類ありますが TCP/UDP/SCTP または既存に設定されている ICMP を使用することを推奨します。

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。



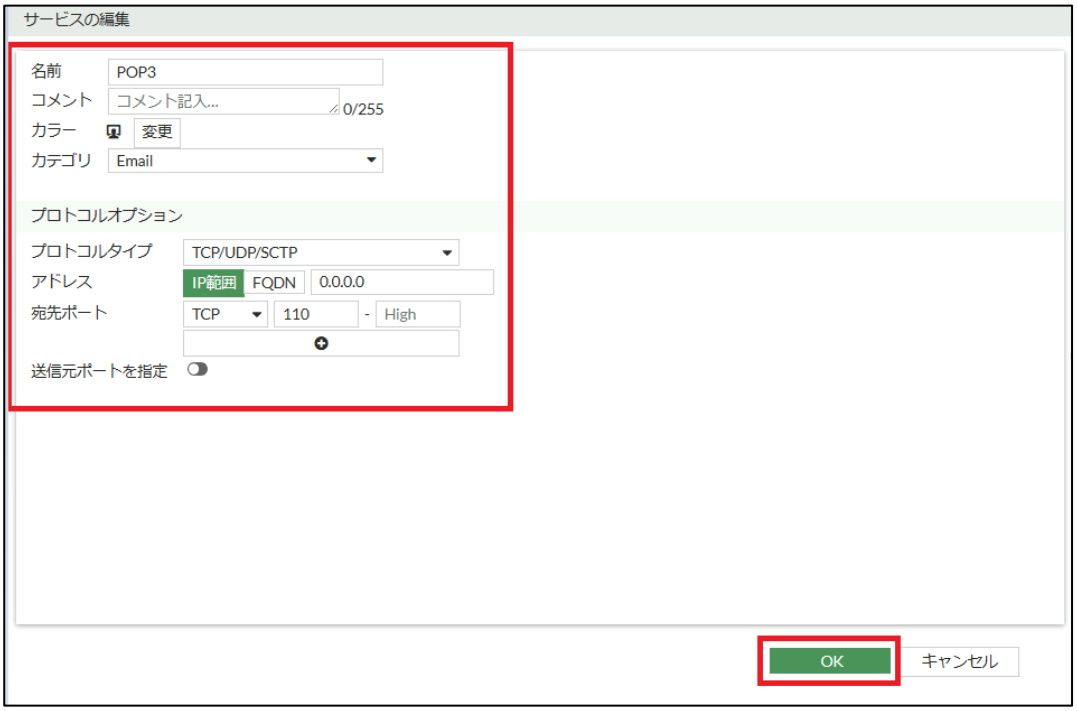
7.2　サービスの変更

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。



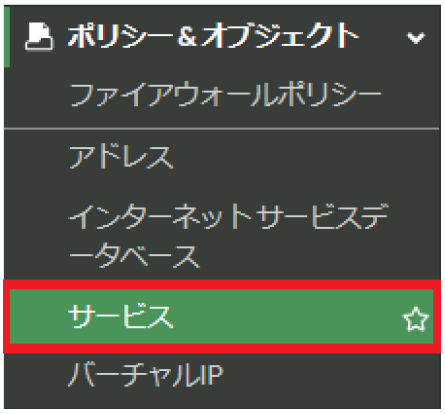
② 変更したいサービスをダブルクリックする。

③ 変更したい項目を変更し、OK をクリックする。



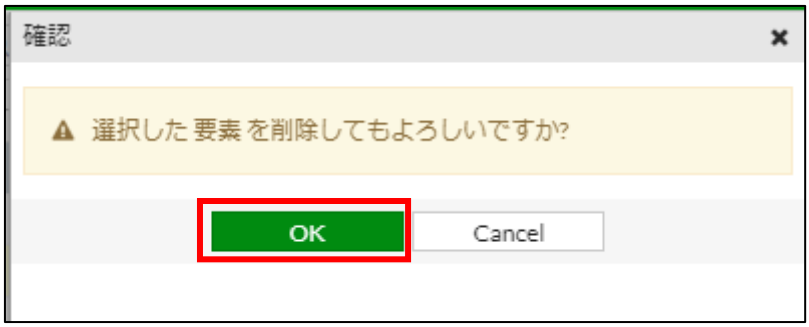
7.3　サービスの削除

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。

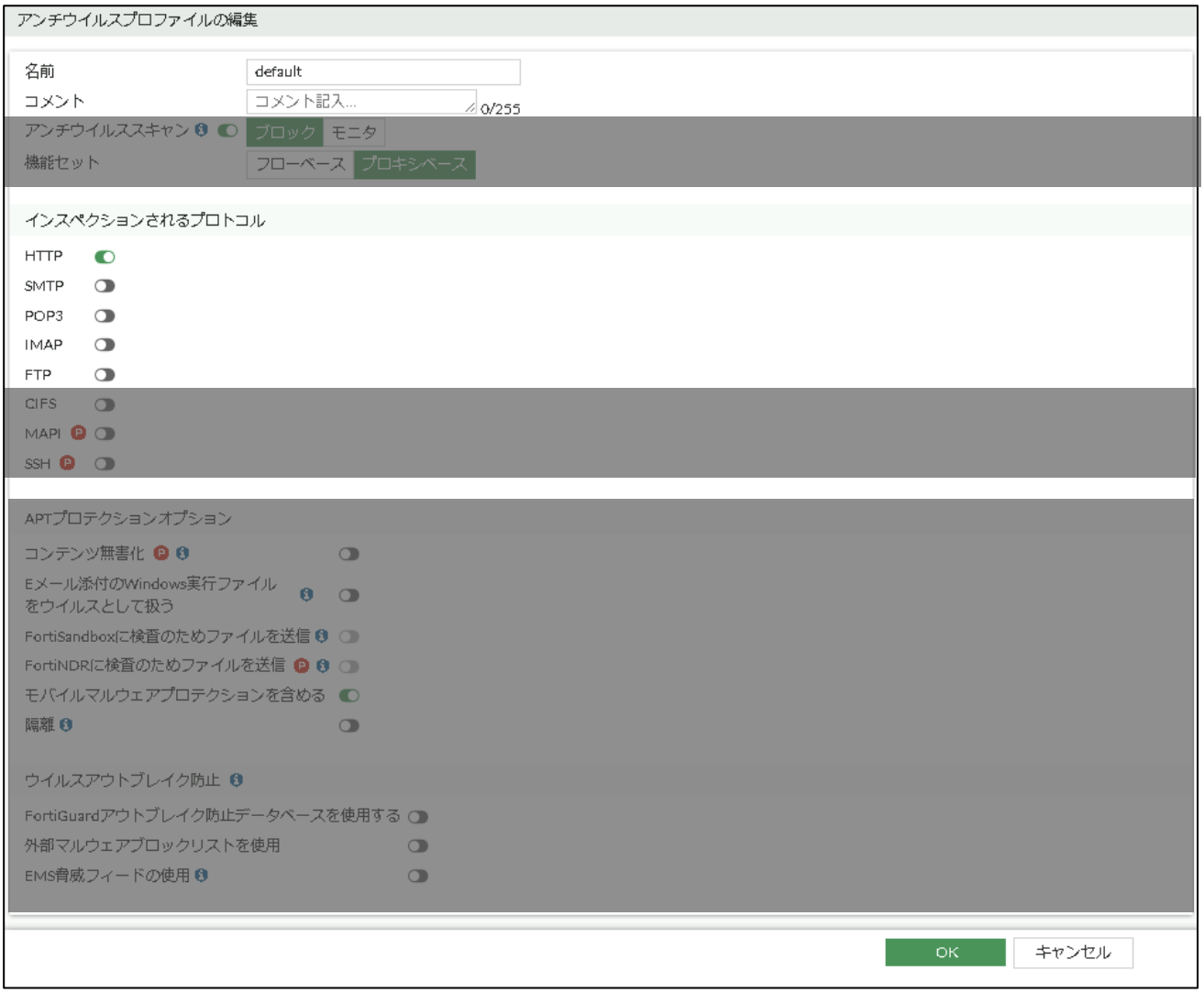
③ 確認ウィンドウがでるので、OK をクリックします。



8　セキュリティプロファイル：アンチウイルス

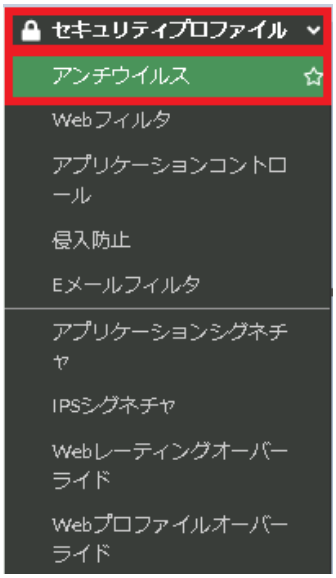
本章では、アンチウイルス機能の設定方法について解説しています。

※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。



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。

③ インスペク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。

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）

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。

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。

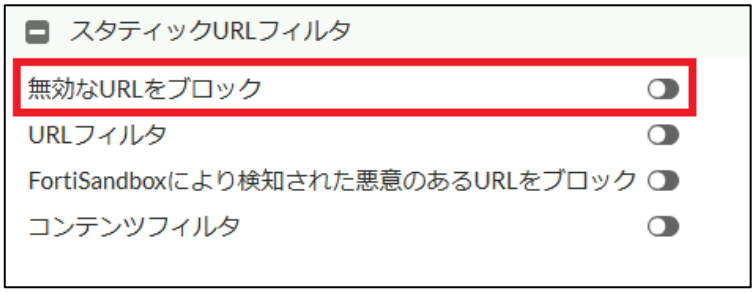
アクションについての詳細は下記のとおりです。

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。

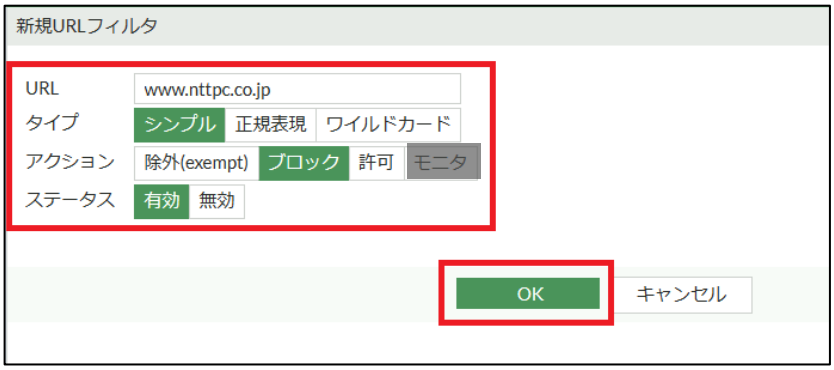
許可：URL フィルタでは許可となるが、その他有効化されているアンチウイルス等のセキュリティチェックが行われます。

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だけをブロックします。
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

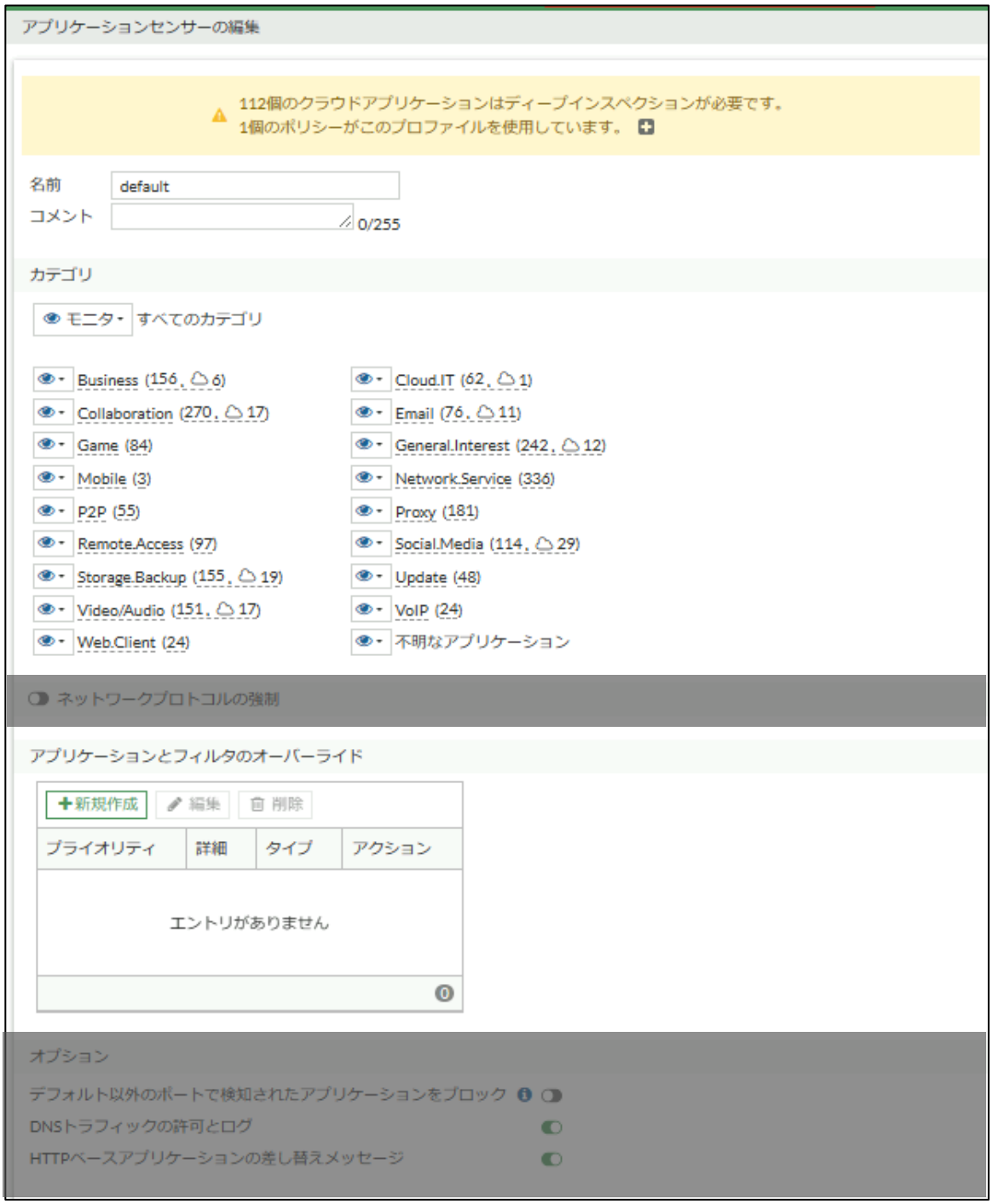
※URL フィルタよりもカテゴリベースのフィルタの方がセキュリティ設定が強いため、カテゴリベースのフィルタでブロックされているものを許可したい場合はアクション除外を使用して設定をしてください。

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。



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。

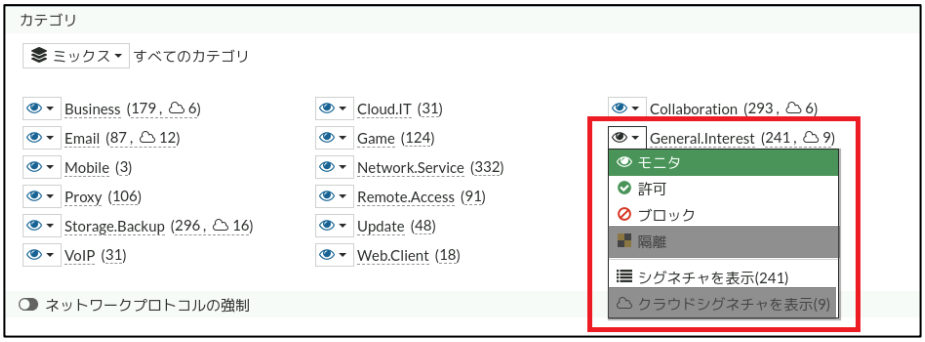
I. カテゴリ

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。



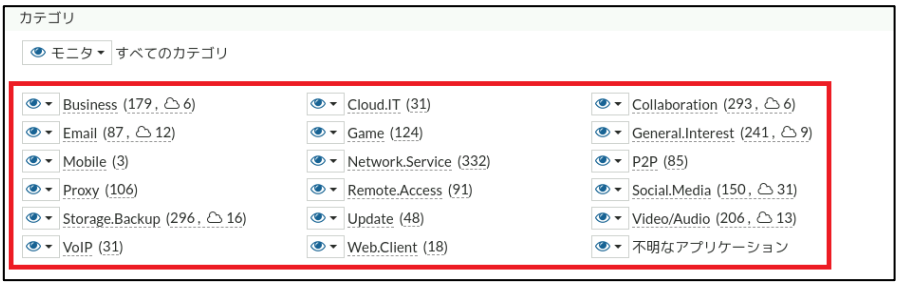
アクションの詳細については下記のとおりです。

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。



II. アプリケーションとフィルタのオーバーライド

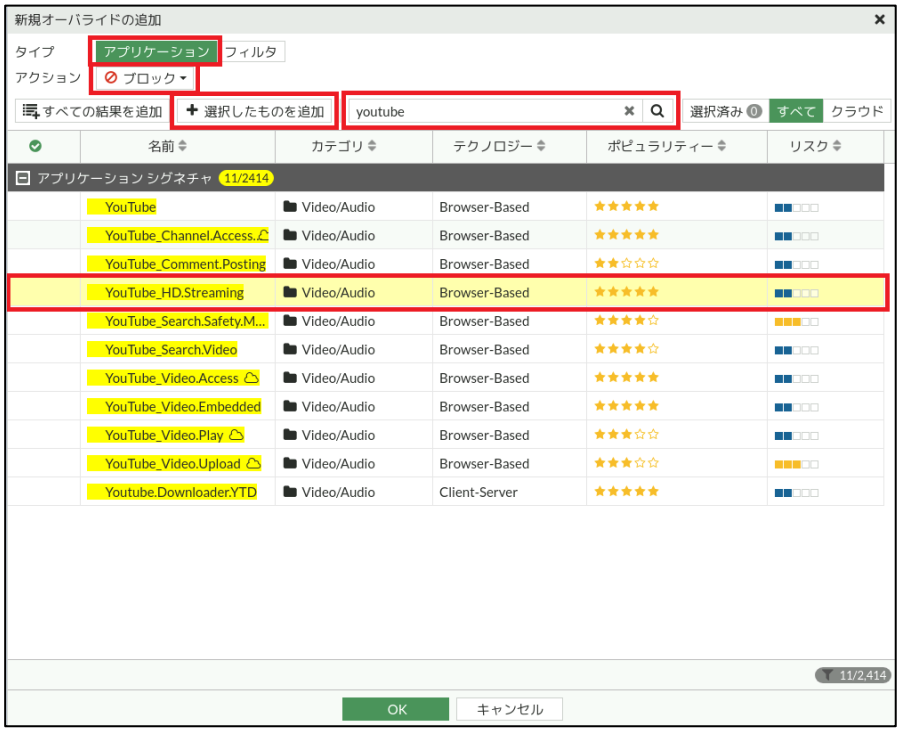
カテゴリとは別に個別にアプリケーション通信の許可、ブロック等の処理を可能とします。

例：youtube の HD ストリーミングをブロックする場合

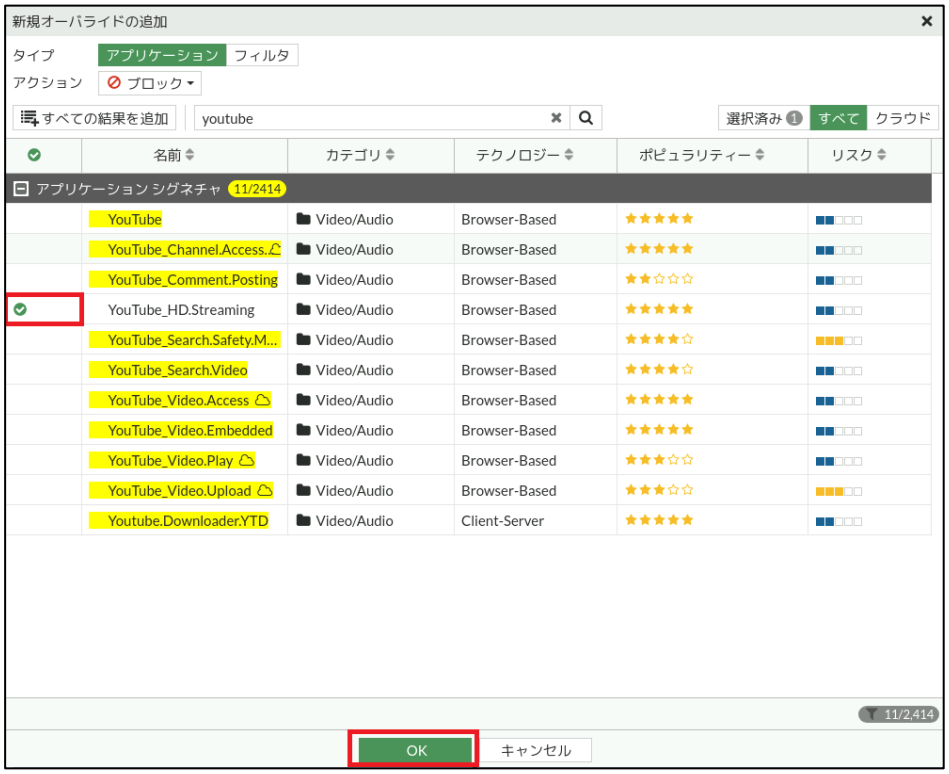
新規作成をクリック

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。



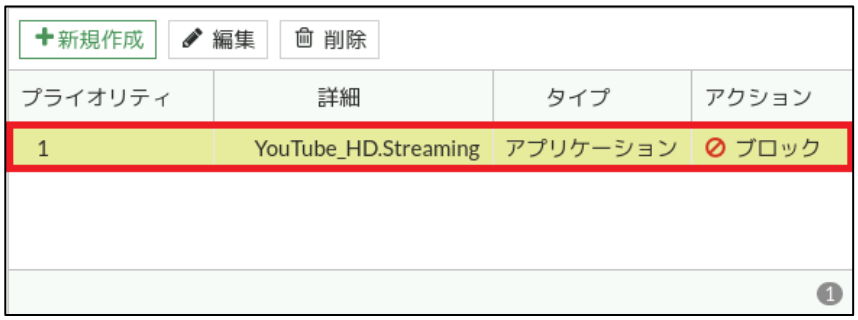
対象のシグネチャにチェックがついていることを確認し「OK」をクリック



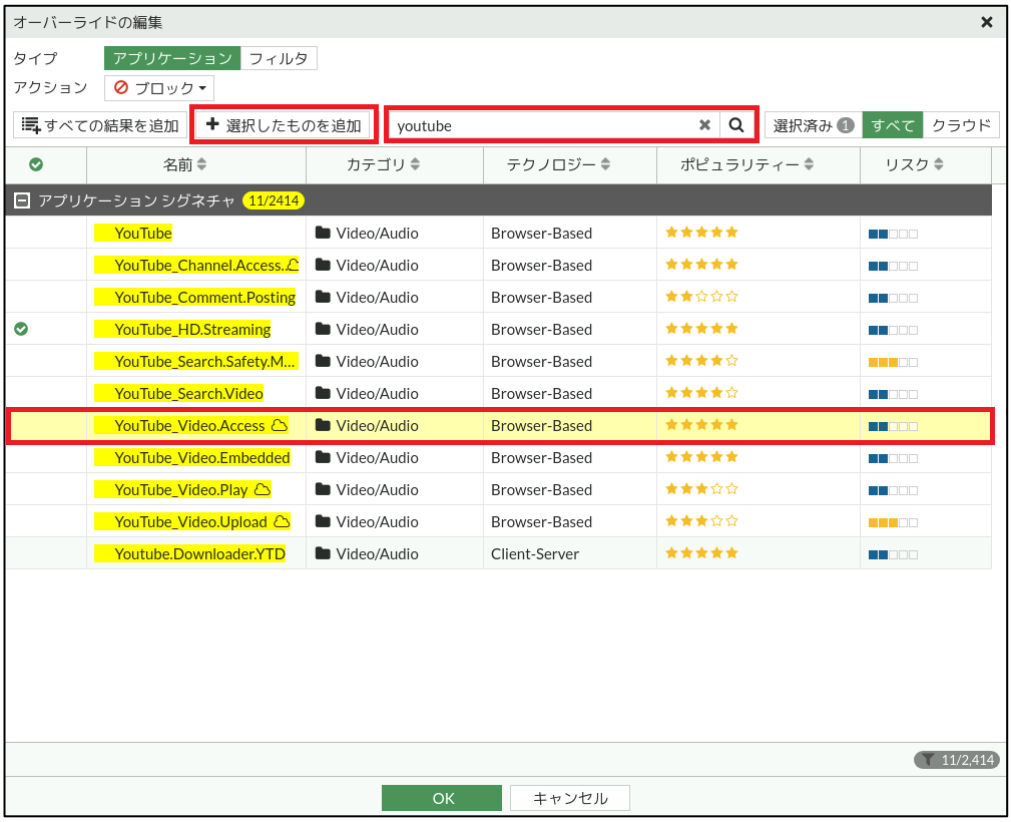
作成されたことを確認する。

例：既存の設定に YouTube ビデオアクセスを追加する場合

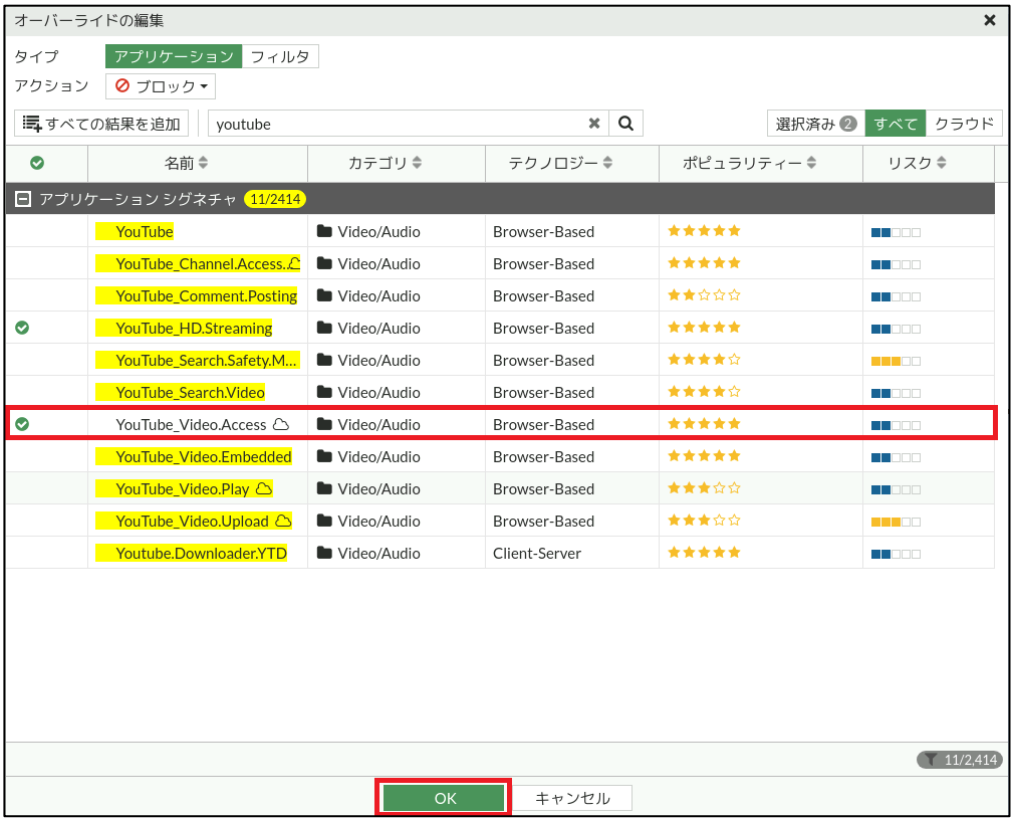
追加したい既存のグループをダブルクリックする。



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。



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

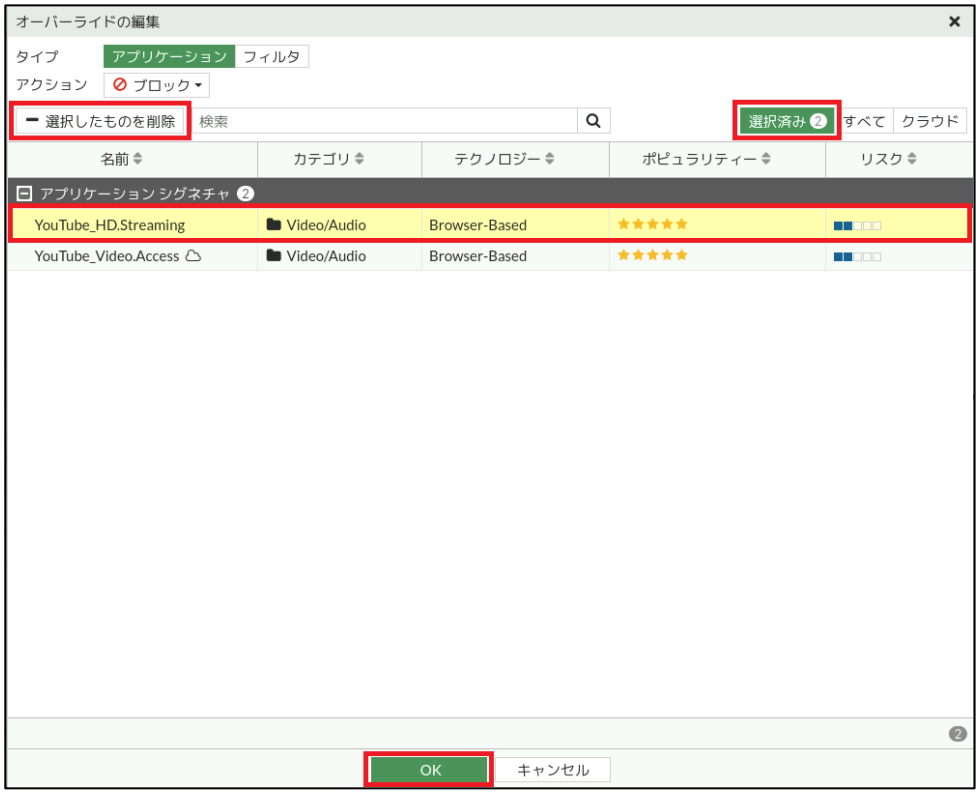


追加されたことを確認する。

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。

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。

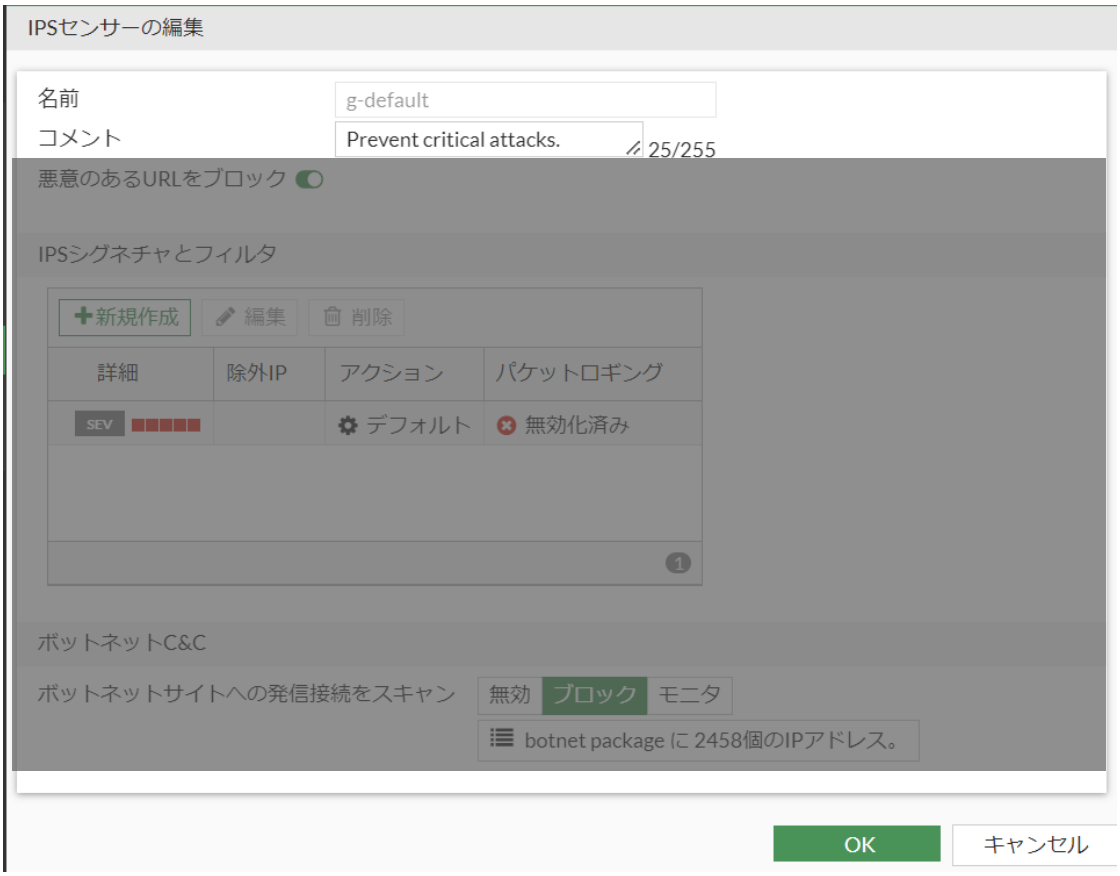
② アプリケーションコントロール内の設定が完了したら画面一番下にある OK を押下する。

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。

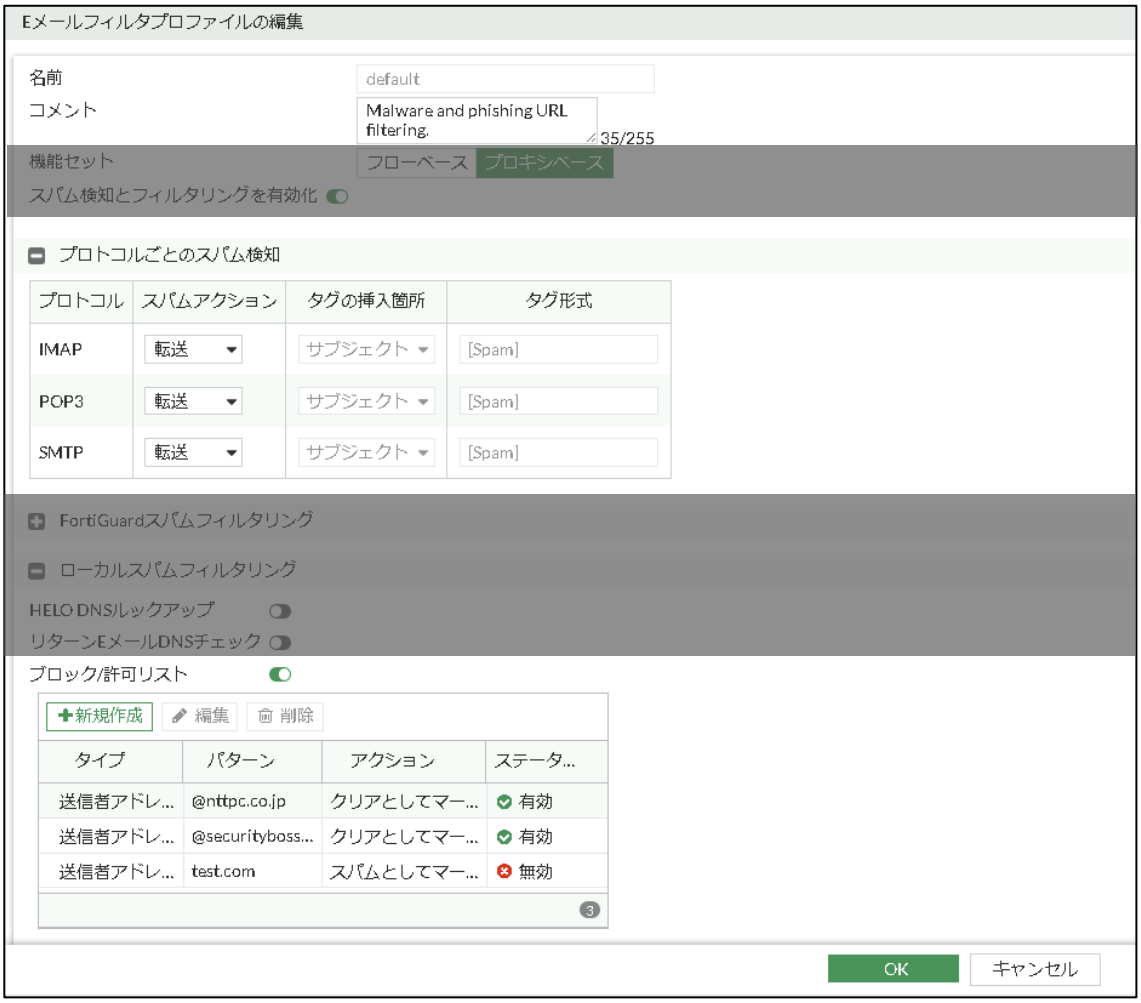
※こちらの機能については有効もしくは無効の操作のみを行ってください。
　設定を変更された場合機能の保証はできません。

※機能の有効・無効については 13 章を参照ください。



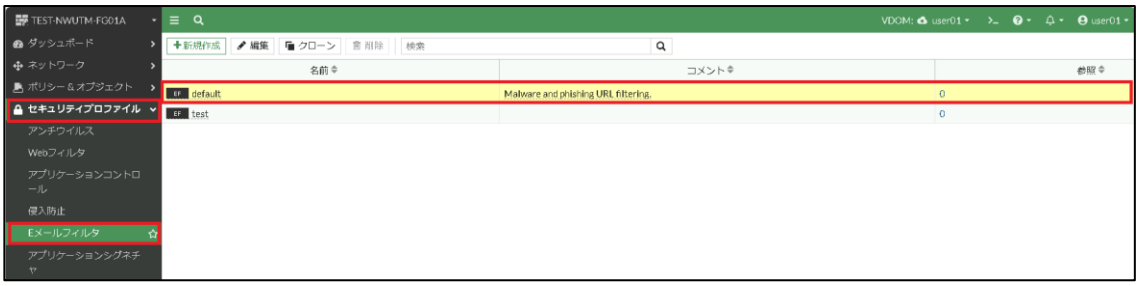
12 セキュリティプロファイル：アンチスパム（E メールフィルタ）

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。



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。

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

図 12-2. スパム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

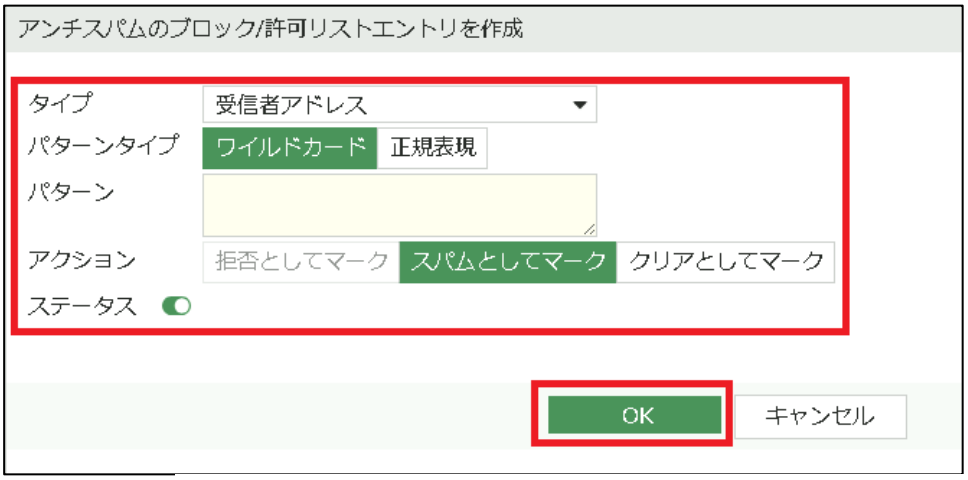


図 12-3. スパムフィルタリング設定画面.

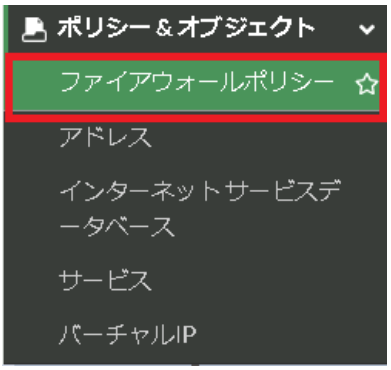
④ E メールフィルタ内の設定が完了したら画面一番下にある OK を押下する。

13 各セキュリティ機能の有効・無効

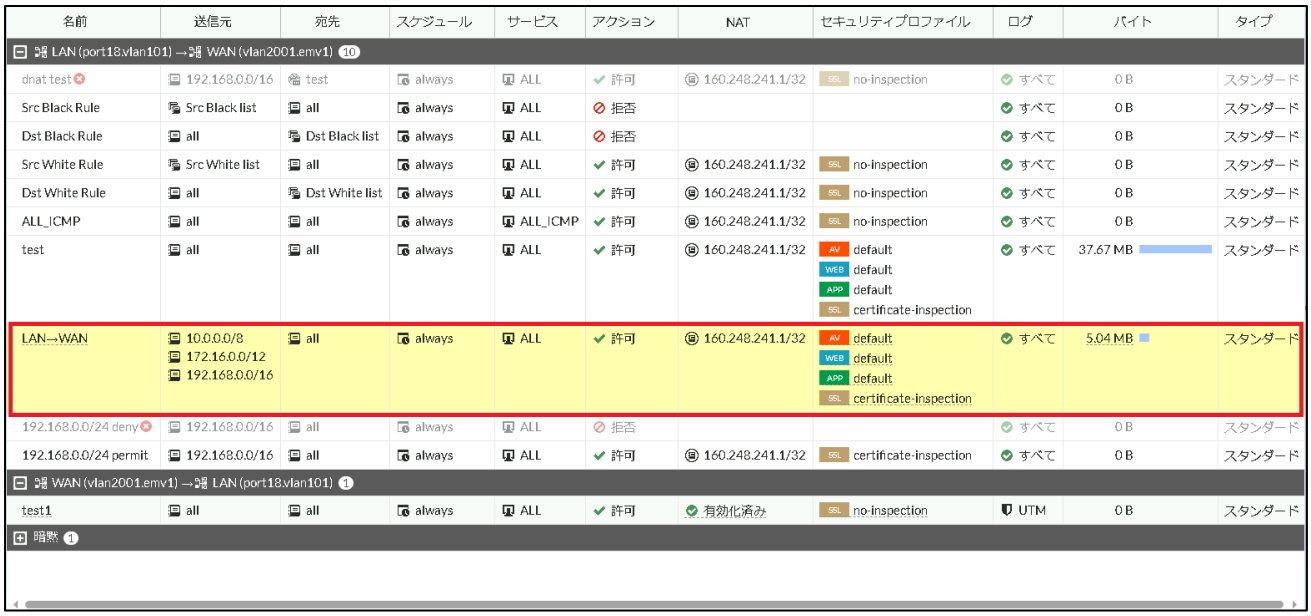
本章では各セキュリティ機能の設定方法について解説しています。

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。

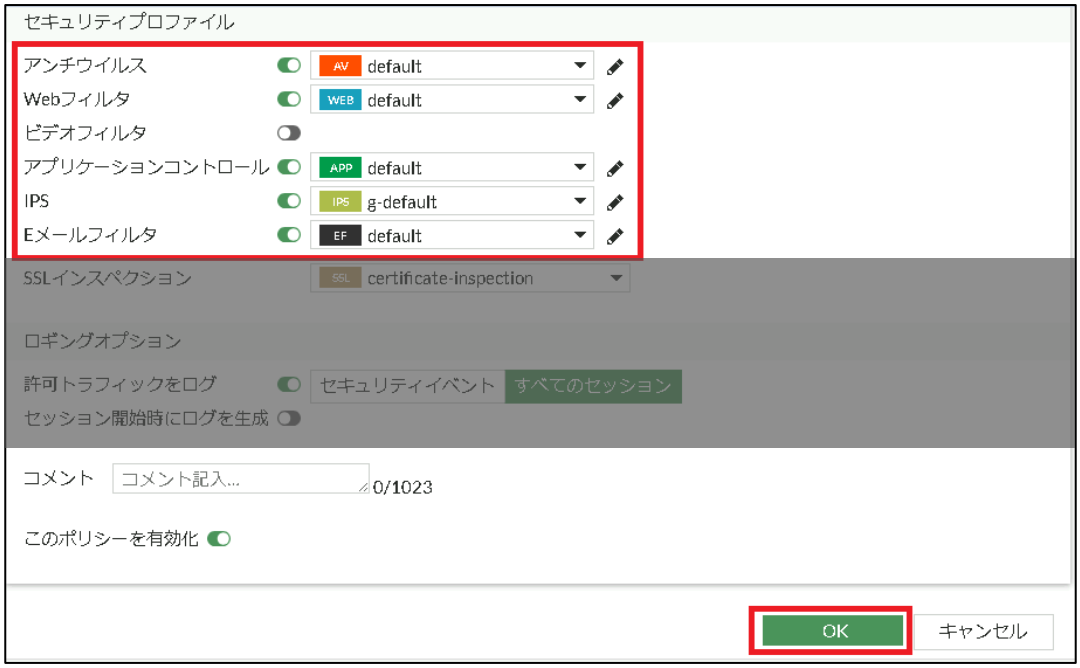


② セキュリティ機能を有効化するルールをダブルクリックする。



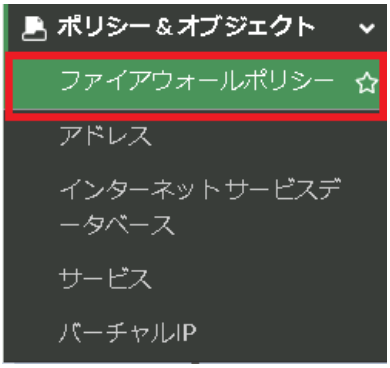
名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト	タイプ
LAN (port18.vlan101) → WAN (vlan2001.emv1) 10										
dnat test	192.168.0.0/16	test	always	ALL	許可	160.248.241.1/32	no-inspection	すべて	0 B	スタンダード
Src Black Rule	Src Black list	all	always	ALL	拒否			すべて	0 B	スタンダード
Dst Black Rule	all	Dst Black list	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_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	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	SSL 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	SSL no-inspection	UTM	0 B	スタンダード
暗黙 1										

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

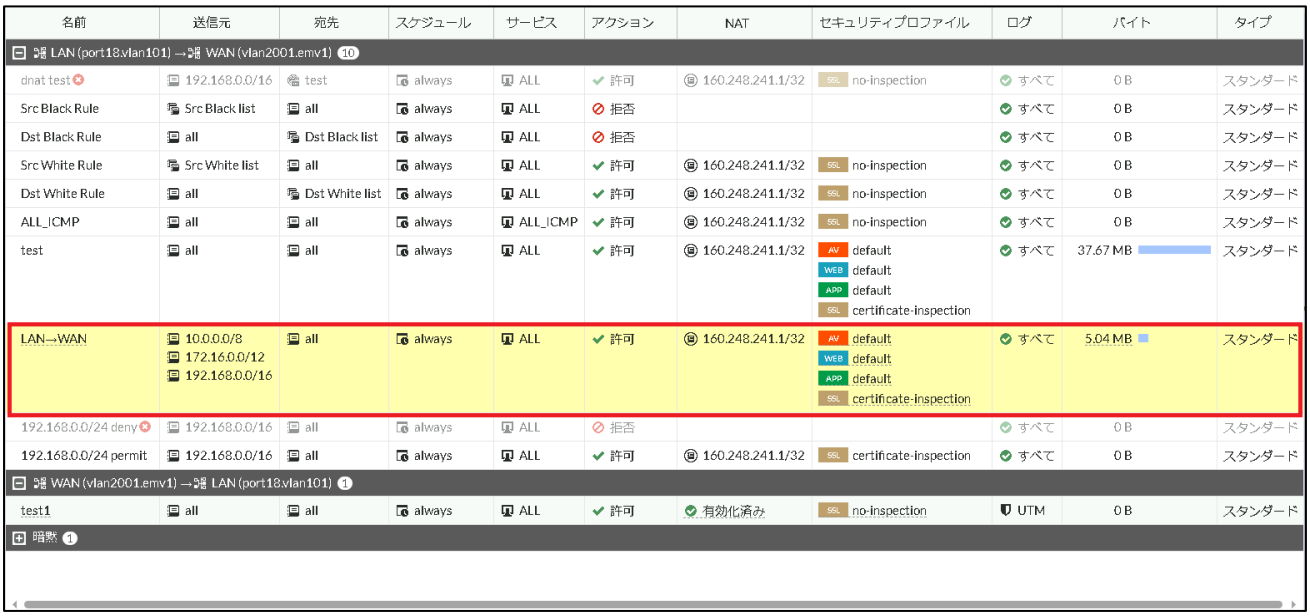


13.2 各セキュリティ機能の無効化

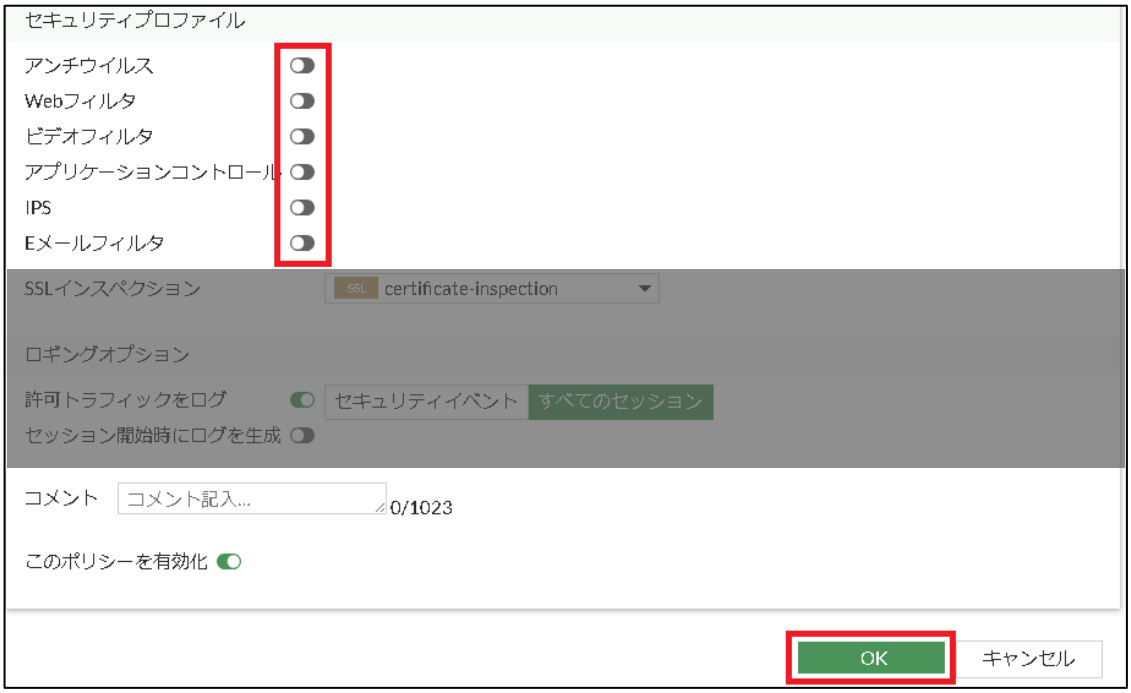
① 左メニューより、ポリシー&オブジェクト→ファイアウォールポリシーを選択する。



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。



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。



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。

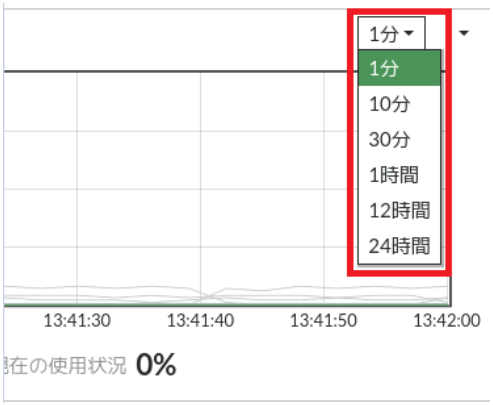
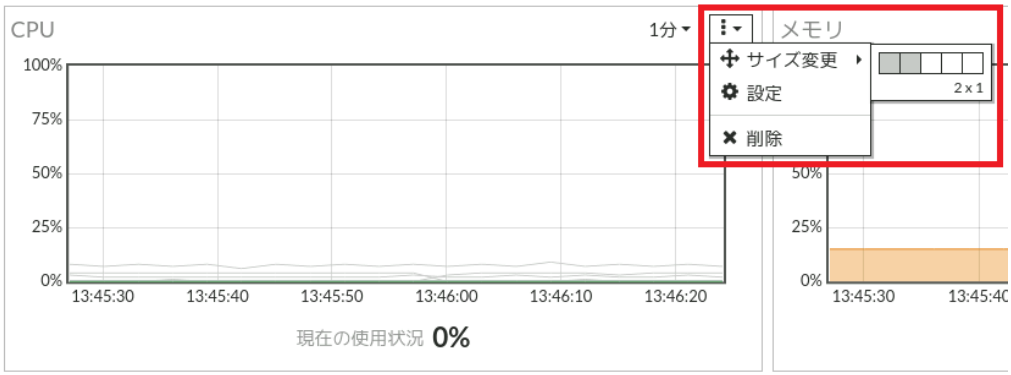


図 14-1. ウイジェット設定画面.

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。

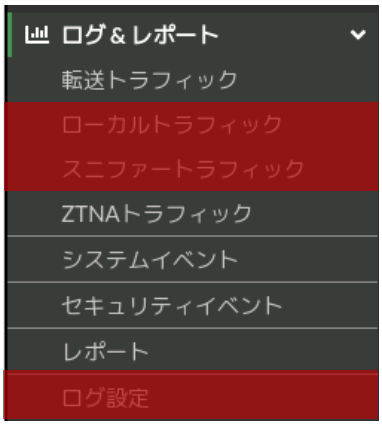
15.4 FortiViewWeb サイト

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:5e:fa: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:5e:fa: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:5e:fa:8c:02	188.172.201.136 (router6.teamviewer.com)	TeamViewer	442.89 kB / 356.79 k
5 分前		192.168.0.2	30:7c:5e:fa:8c:02	210.150.254.130	DNS	75 B / 205 B
5 分前		192.168.0.2	30:7c:5e:fa:8c:02	210.150.254.130	DNS	75 B / 205 B

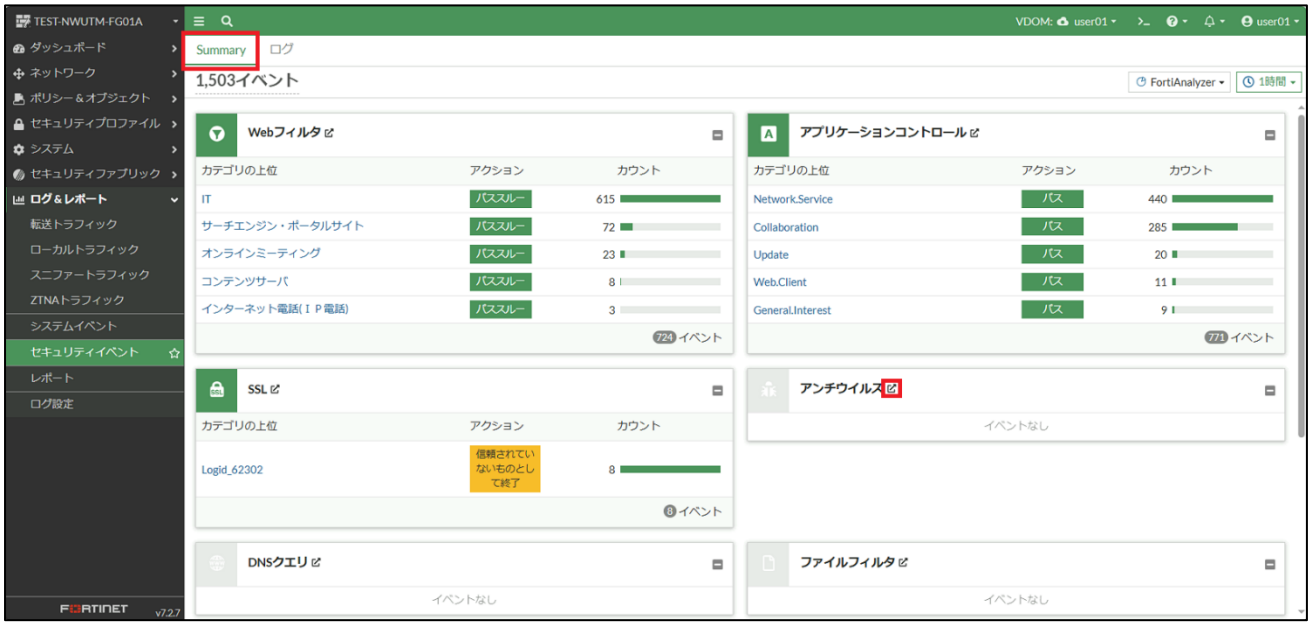
16.2 セキュリティイベント

「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。

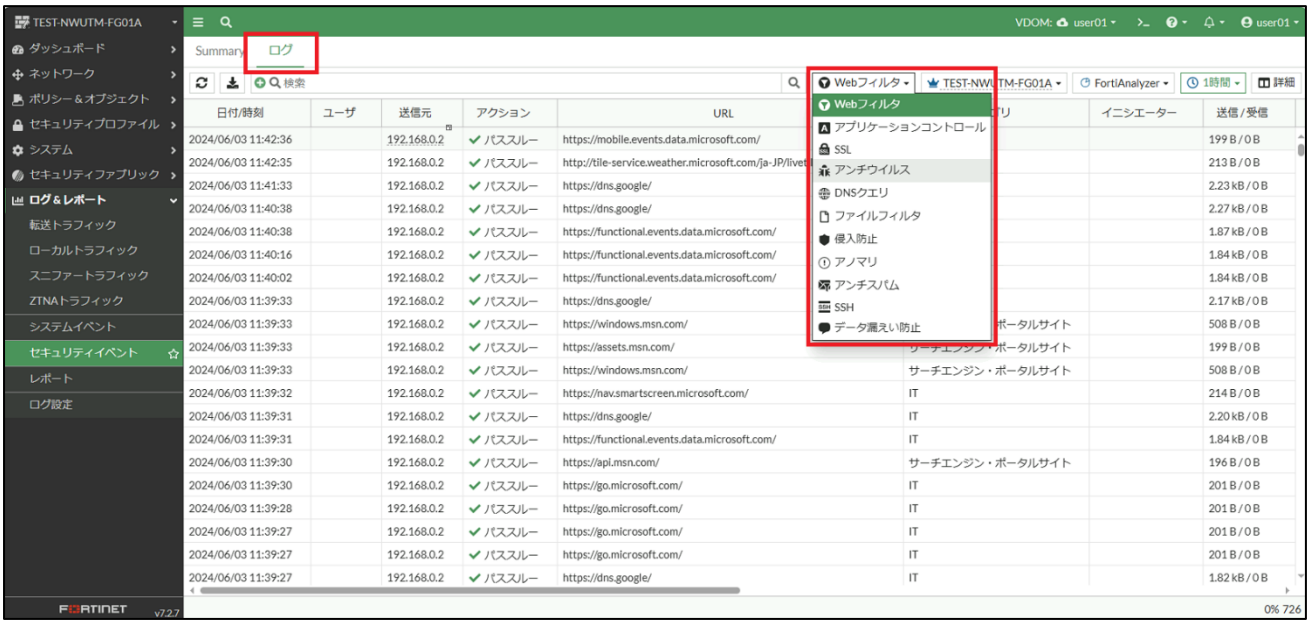
① 左メニューより、ログ&レポート→セキュリティイベントを選択する。

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



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



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、該当の通信の状況が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ございます。

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

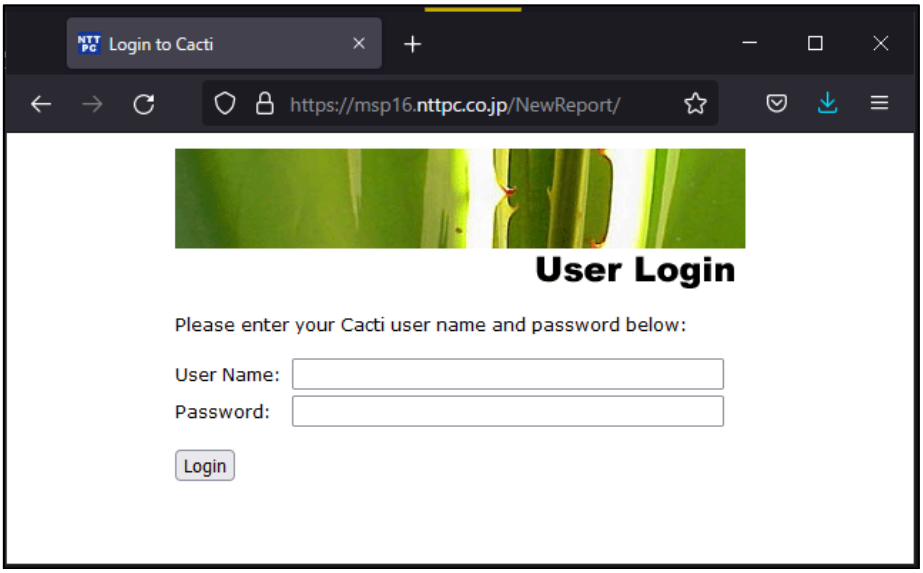


図 17-1. Cacti ログイン画面.

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。

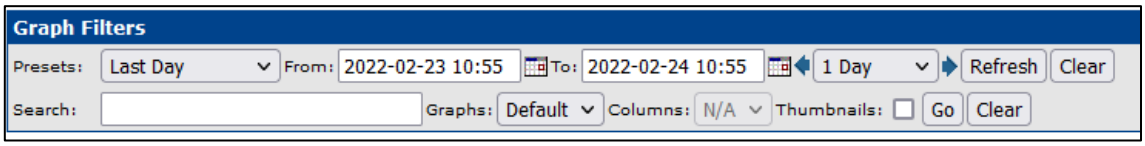


図 17-2. グラフフィルター設定画面.

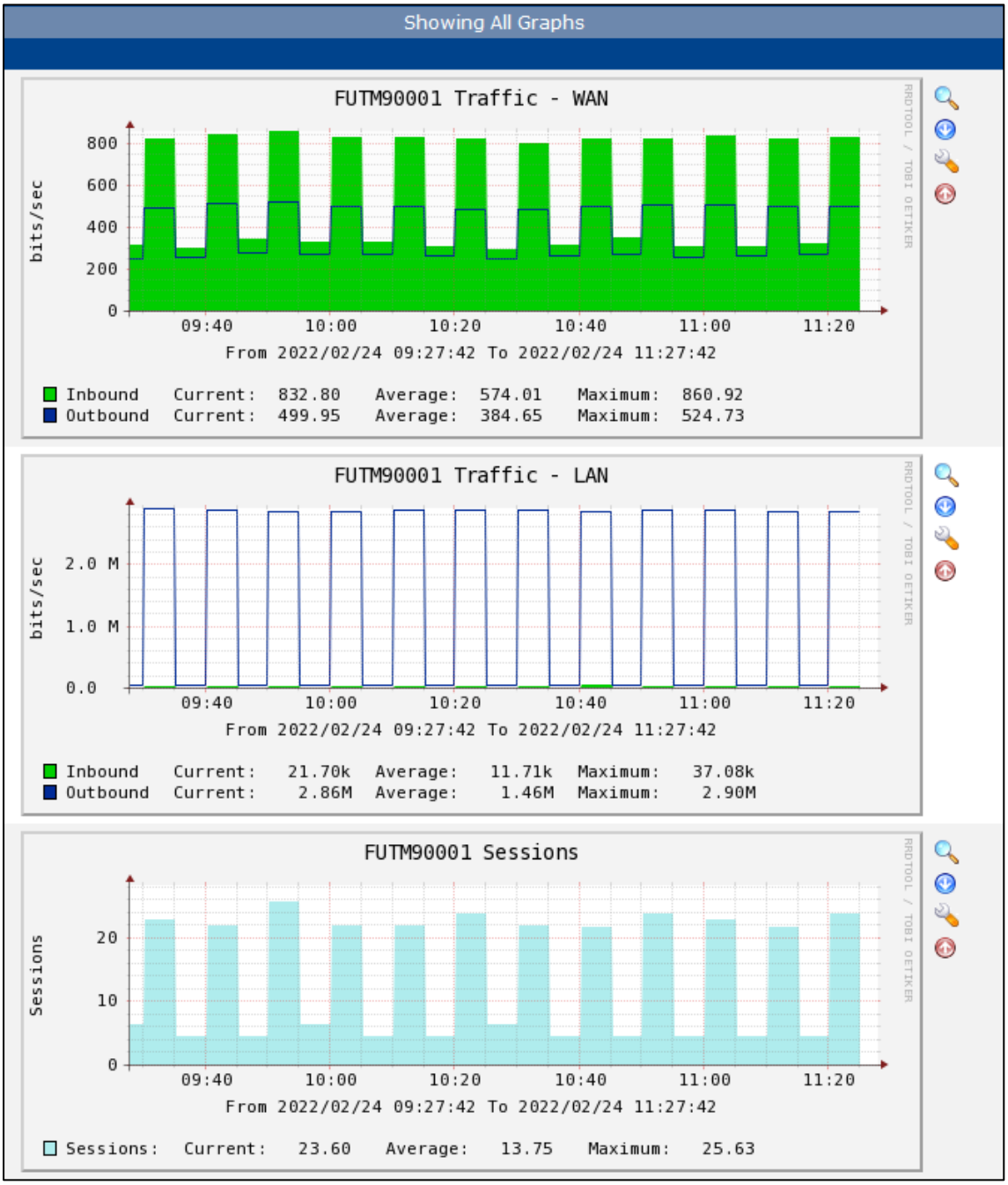
参照方法は下記 2 点になります。

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。