## 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	こめに	5
	1.	1	サービスリニューアル	0
2		カス	、タマコントロールサイトへの接続 1	1
	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1	1
	2.	2	初回ログイン時の操作	1
	2.	3	カスタマコントロールサイトのパスワード変更1	2
3		プリ	リセット設定	4
	3.	1	ファイアウォールルール	4
	3.	2	ファイアウォールポリシー設定項目1	7
	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 2	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)2	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)3	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) 3	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)4	10
	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)	13
	4.	8	SNAT 設定方法(表示形式:シーケンス別の場合) 4	17
	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	の
	場	¦合)	εε	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)5	6
	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)5	;9
	4.	12	DNAT 設定方法(表示形式:シーケンス別の場合)	i5
5		アド	*レスの設定方法	/2
	5.	1	アドレスの追加	/2
	5.	2	アドレスの変更	/4
	5.	3	アドレスの削除	/6
6		アド	*レスグループの設定方法	17
	6.	1	アドレスグループの追加	17
	6.	2	アドレスグループの変更	18
	6.	3	ホワイトリスト・ブラックリストへの設定8	30
		1	Src Black list への設定方法	30
		2	Dst Black list への設定方法	\$1
		3	Src White list への設定方法	\$2

# Master'sONE<sup>®</sup>

	4	1)	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	÷	ナー	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	ł	ヒキ	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	ł	ヒキ	ュリティプロファイル : Web フィルタ	91
9	. 1	V	Web フィルタの設定	92
		Ι.	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	I. スタティック URL フィルタ(URL フィルタ)	94
10	ł	ヒキ	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
1	0.	1	アプリケーションコントロールの設定	97
		Ι.	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	ł	ヒキ	ュリティプロファイル:IPS(侵入防止)1	03
12	ł	ヒキ	ュリティプロファイル : アンチスパム(E メールフィルタ) 1	04
1	2.	1 E	E メールフィルタの設定1	04
	(1	1)	プロトコルごとのスパム検知数1	05
		2)	ローカルスパムフィルタリング1	05
13	겯	ふち いちちょう ひちょう ひちょう ひちょう ひちょう ひちょう ふうしょう ふうしょう ふうしょう ふうしょう ふうしょう ふうしょう ふうしょう ひょう ひょう ひょう ひょう ひょう ひょう ひょう ひょう ひょう ひ	キュリティ機能の有効・無効 1	07
1	3.	1 :	各セキュリティ機能の有効化 1	07
1	3.	2 ÷	各セキュリティ機能の無効化1	08
14	5	ダッ	シュボード 1	10
1	4.	1 י	ウィジェット 1	10
15	F	ort	iView	11
1	5.	1 F	FortiView 送信元	11
1	5.	2 F	FortiView 宛先	11
1	5.	3 F	FortiView アプリケーション1	11
1	5.	4 F	FortiViewWeb サイト1	11
16	F	コグ	&レポート 1	12
1	6.	1 🛙	転送トラフィックログ1	13
1	6.	2 -	セキュリティイベント	14
	(1	1)	アンチウイルス1	15
		2)	Web フィルタ1	16

## Master'sONE<sup>•</sup>

3	③ アプリケーションコントロール	117
(4	④ IPS(侵入防止)	118
(5	⑤ アンチスパム (E メールフィルタ)	118
16.3	3 各種ログの取得方法	119
ע 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	2 グラフ	121
18 Q8	J&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。

	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

表 1-1. お客さま権限一覧.

※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。

内容						
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	不可					
	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				

表 1-2. お客さま設定変更不可一覧.

※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



Copyright (c) 2024 NTT PC Communications Incorporated, All Right Reserved.



#### ・セキュリティプロファイル



#### ・システム



Copyright (c) 2024 NTT PC Communications Incorporated, All Right Reserved.



#### ・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。



11

- 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。

ユーリ泊	
パスワード	
ログイン	

#### 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。

TEST-NWUTM-FGOLA	≡ Q.	X	DOM: 🗙 user01 • >_ 🕢 • 🗘 • 😝 user01 •
Øッシュポード →	➡ ウィジェット追加		
	CPU 197- i- XモU 2005 1005 728 728 728 728	U 19- I	
<ul> <li>● セキュリティファブリック &gt;</li> <li>■ ログ&amp;レポート &gt;</li> </ul>	50% 20% 0% 0% 0% 0% 0% 0% 0% 0% 0%		
	現在の使用状況 0%	現在の使用状況 0%	
	47α(2, ¬Σ) 40- L		_
	10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 1		
			0

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		×
▲ 現在の管理者フ になります。	ウウントのパスワードを変更すると再ログインが必要	
ユーザ名	biu00000	
旧パスワード	۲	
新しいパスワード	۲	
パスワードの再入力	۲	
	ОК <b>‡</b> т	ンセル



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)
- 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)
- 1) 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	パイト	タイプ		
□ ¾ LAN (port18 vlan101) → ¾ WAN (vlan2001.emv1)												
NTTPC Monitor Rule	100.88.18.0/29	😑 all	🐻 always	🖬 ALL	✔ 許可	160.248.241.1/32	ss. no-inspection	🙁 無効化済み	0 B	スタンダート		
Src Black Rule	🐴 Src Black list	😑 all	🐻 always	🖬 ALL	⊘ 拒否			🕏 すべて	0 B	スタンダート		
Dst Black Rule	🚍 all	🐴 Dst Black list	🐻 always	ALL ALL	⊘ 拒否			🕏 すべて	0 B	スタンダート		
Src White Rule	🐴 Src White list	😑 all	🐻 always	🖬 ALL	✔ 許可	160.248.241.1/32	55L no-inspection	🛛 すべて	0 B	スタンダート		
Dst White Rule	🗐 all	🖷 Dst White list	🐻 always	🖬 ALL	✔ 許可	160.248.241.1/32	ss. no-inspection	🕏 すべて	117.90 kB	スタンダート		
ALL_ICMP	🚍 all	😑 all	🐻 always	ALL_ICMP	✔ 許可	160.248.241.1/32	ss. no-inspection	🕏 すべて	0 B	スタンダート		
LAN -> WAN	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	🖻 all	o always	I ALL	✔ 許可	B 160.248.241.1/32	AV default WEB default APP default SEL certificate-inspection	🛛 ಕನ್ನ	13.64 MB	スタンダート		
□ 暗黙 1												
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 ⑪「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.



	ポリシー名	用途	デフォルト設定
1	NTTPC モニタール 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	<ul> <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、空の状態で提供致します。</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> <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、空の状態で提供致します。</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> <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、空の状態で提供致します。</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> <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、空の状態で提供致します。</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> <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> <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> <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願います。</li> </ul>	有効
9	webfilter- policy-*	<ul> <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*	- 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

表 3-1. プリセットのファイアウォールルール一覧.

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。

11 暗黙の拒否

Copyright (c) 2024 NTT PC Communications Incorporated, All Right Reserved.

上記①~⑩に合致しない通信を明示的に拒否します。

有効



#### 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		
□ 1월 LAN (port18.vlan101) → 1월 WAN (vlan2001.emv1) 7												
NTTPC Monitor Rule	100.88.18.0/29	💷 all	🐻 always	🖬 ALL	✔ 許可	160.248.241.1/32	ss. 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	55L no-inspection	🕏 すべて	0 B	スタンダード		
Dst White Rule	🗐 all	壇 Dst White list	🐻 always	🖬 ALL	✔ 許可	160.248.241.1/32	ss. 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	ss. no-inspection	🕏 すべて	0 B	スタンダード		
LAN -> WAN	10.0.0/8	🚍 all	🖸 always	🖬 ALL	✔ 許可	160.248.241.1/32	AV default	📀 すべて	15.29 MB	スタンダード		
	1/2.168.0.0/12		Γ)	•		• 、	WEB default			M/S		
A)	- U)	E)	F)	G)	H)	1)	ss. certificate-inspection	N)	L)	M)		
□ 暗黙 ①												
暗黙の拒否	🗐 all	🔳 all	🐻 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	То	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	38 LAN (port18.vian101)	38 WAN (vlan2001.emv1)	100.88.18.0/29	🖾 all	🗔 always	🗵 ALL	✔ 許可	@ 160.248.241.1/32	551 no-inspection	😵 無効化済み	өв	スタンダード
Src Black Rule	) LAN (port18.vian101)	35 WAN (vlan2001.emv1)	👼 Src Black list	🖭 all	🗔 always	🖳 ALL	⊘ 拒否			すべて	oв	スタンダード
Dst Black Rule	Se LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	😑 all	👼 Dst Black list	🕼 always	🖳 ALL	⊘ 拒否			すべて	0 B	スタンダード
Src White Rule	) LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	疆 Src White list	🖻 all	🕼 always	🗵 ALL	✔ 許可	@ 160.248.241.1/32	ssu no-inspection	◎ すべて	ΘB	スタンダード
Dst White Rule	3§ LAN (port18.vian101)	35 WAN (vlan2001.emv1)	😑 all	😼 Dst White list	😡 always	😰 ALL	✔ 許可	160.248.241.1/32	ss no-inspection	すべて	117.90 kB	スタンダード
ALL_ICMP	3 LAN (port18.vlan101)	3§ WAN (vlan2001.emv1)	😐 all	😑 all	😺 always	ALL_ICMP	✔ 許可	9 160.248.241.1/32	551 no-inspection	🛛 すべて	0 B	スタンダード
Lan -> Wai <b>A</b> )	38 LAN (port 18 <b>B)</b> 101)	28 WAN (vlan 20 <b>())</b> mv 1)	<ul> <li>■ 10.0.0.0</li> <li>■ 172.16.0.0</li> <li>■ 172.168.0.0/16</li> </ul>	<sup>⊡</sup> "E)	<sup>® alway</sup> F)	<sup>.</sup> ¶ <b>G</b> )	´Ħ)	<sup>® 160.248.</sup> <b>₽)</b> <sup>1/32</sup>	default J)	° ⁵∕ <b>K</b> )	<u>15.29 мв</u> <b>L)</b>	スタン <b>M)</b> ド
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。
- 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。 H)
- 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。) I)
- 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。 J)
- K) ログを取得するか否かが設定されています。
- 対象のポリシーに合致した通信量が表示されています。 L)
- 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。

TEST-NWUTM-FG01A •	≡ <b>Q</b>								DM: 🙆 user01 •	>_ <b>0 ·</b> ↓ ·	😫 user01 🕶
🙆 ダッシュボード 🔹 🔉	+新規作成 / 編録	毛 >_ CLIで編集		ペリシーのルックア	ップ 検索			Q 🗎 エクスポ	-ト・ インター	フェースペアビュー 👂	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	1571	タイプ
🖹 ポリシー&オブジェクト 🗸 🗸	🖃 🧏 LAN (port18.vlar	101) → 38 WAN (vlar	12001.emv1) 🧭								
ファイアウォールポリシー 🏠	NTTPC Monitor Rule	100.88.18.0/29	🖾 all	😡 always	🖪 ALL	✔ 許可	160.248.241.1/32	ss. no-inspection	😂 無効化済み	oв	スタンダ
アドレス	Src Black Rule	🖥 Src Black list	🖾 all	la always	😰 ALL	⊘ 拒否			すべて	0 B	スタンダ
インターネットサービスデ ータベーマ	Dst Black Rule	🗉 all	🖥 Dst Black list	😡 always	🗷 ALL	⊘ 拒否			⊘ すべて	oв	スタンダ
+	Src White Rule	🖥 Src Whitelist	🖻 all	😡 always	😰 ALL	✔ 許可	160.248.241.1/32	ss. no-inspection	すべて	0 B	スタンダ
パーチャルコロ	Dst White Rule	🗉 all	看 Dst White list	😡 always	🖪 ALL	✔ 許可	160.248.241.1/32	ss. no-inspection	🕏 すべて	945.64 kB	スタンダ
A セキュリティブロファイル >	ALL_ICMP	🗉 all	🖾 all	😡 always	ALL_ICMP	✔ 許可	160.248.241.1/32	ss. no-inspection	🗢 すべて	ОB	スタンダ
■ cq エリノハレ CDノ ハル V な システム >	ii lan -> wan 🖉	■ 10.0.0.0/8	🖬 all	🗴 always	😰 ALL	✔ 許可	160.248.241.1/32	AV default	🛛 すべて	74.69 MB	スタンダ
<ul> <li>● セキュリティファブリック &gt;</li> </ul>		<ul> <li>172.168.0.0/12</li> <li>192.168.0.0/16</li> </ul>						APP default			
ビログ&レポート >								ssu certificate-inspection			
	日暗愁 1										
	暗黙の拒否	🖽 all	🖾 all	👩 always	ALL ALL	⊘ 拒否			◎ 有効化済み	104 B	

変更後適用を押下すると反映されます。

TEST-NWUTM-FG01A +	≡ <b>Q</b>							VDOM: 💩 u	ser01 • >_ (	<b>∂•</b> Д• Өuser01•
🙆 ダッシュポード 🔹 🔉	+新規作成 ● 編集 >- 0	:山で編集   自 削除	Q ポリシーの	ルックアップ オ	検索			Q 🗎 エクスポート・	インターフェース	ペアビュー シーケンス別
ネットワーク >	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
💄 ポリシー&オブラエクト 🔹 🗸	🖻 🔆 LAN (port38 vian103) — 🛠 WAN (vian2001 envi) 🕐									
ファイアウォールポリシー 🏠	NTTPG Monitor Rule	100.88.18.0/29	🗄 all	👩 always	E ALL	✔ 許可	(2) 160.248.241.1/32	ss no-inspection	😂 無効化済み	0 B
アドレス	Src Black Rule	覆 Src Blacklist	🗄 all	😡 always	I ALL	⊘ 拒否			◎ すべて	0 B
インターネットサービスデ ータベース	Dst Black Rule	🗄 all	量 DstBlacklist	la always	I ALL	⊘ 拒否			◎ すべて	0 B
+-Pz	Src White Rule	🍯 Src White list	🗉 all	😡 always	E ALL	✔ 許可	@ 160.248.241.1/32	584 no-inspection	◎ すべて	0 B
バーチャルル	Dst White Rule	🗄 all	看 Dst White list	😡 always	E ALL	✔ 許可	@ 160.248.241.1/32	551 no-inspection	◎ すべて	945.64 kB
▲ セキュリティプロファイル >	ALL_ICMP	🗄 all	🗄 all	😡 always	ALL_ICMP	✔ 許可	(2) 160.248.241.1/32	ss no-inspection	◎ すべて	0 B
	Mah site	10.0.0/8	₽ all	👩 always	I ALL	✔ 許可	160.248.241.1/32	AV default	🛛 すべて	74.69 MB
<ul> <li>シーンシー</li> <li>クーンシー</li> <li>クーン</li> <li>クーン</li></ul>	(Heb Side	<ul> <li>1/2.168.0.0/12</li> <li>192.168.0.0/16</li> </ul>						APP default		
ビログ&レポート >	適用 キャンセル							sst certificate-inspection		
	□ 暗黙 1									
	暗黙の拒否	🔄 all		lø always	I ALL	⊘ 拒否			◎ 有効化済み	104 B

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。

TEST-NWUTM-FG01A +	≡ Q								VDOM: 🚳 user	-01• ≻ <b>_ @•</b> ↓• ⊕user01•
🙆 ダッシュボード 🔹 🔉	<b>十</b> 新規作成		編集	Q ポリシーの/	レックアップ	検索		Q 🗎 エク	マスポート・ イ	エントリを選択 🗙
ネットワーク >	Ū.	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	Q 検索 + 新規作成
💄 ポリシー&オブジェクト 🛛 🗸	t18.vlan101) → 3	WAN (vlan 2001.em)	(1) <b>7</b>							▲ 限定ビュー
ファイアウォールポリシー 🏠	or Rule	100.88.18.0/29		👩 always	I ALL	✔ 許可	@ 160.248.241.1/32	sst no-inspection	😂 無効化済み	■ アンチウイルスプロファイル(4)
アドレス		殭 Src Black list		👩 always	I ALL	⊘ 拒否		マンエウノルフプロファノル	a distanción	AV default AV defaultのクローン実験用
インターネットサービスデ ータベース		🗉 all	👼 Dst Black list	😡 always	I ALL	⊘ 拒否		メンテンイルスンロンアイル 機能セット	dersuit プロキシベース	AV g-default
サービス	2	糧 Src White list	🗄 all	l <b>g</b> always	I ALL	✔ 許可	(2) 160.248.241.1/32	スコープ	VDOM	
15-25-11-10	2	🖂 all	覆 Dst White list	😡 always	R ALL	✔ 許可	@ 160.248.241.1/32	リファレンス	1	E default
		🗐 all	🗄 all	😡 always	ALL_ICMP	✔ 許可	@ 160.248.241.1/32		-	■ WEBフィルタプロファイル(11)
• C+IUTAJUJYAN >		10.0.0/8	🖻 all	🕼 always	I ALL	✔ 許可	160.248.241.1/32	/ MR		₩60 ★Web)Mailブロック
<ul> <li>システム</li> <li>&gt;</li> </ul>		172.16.0.0/12						wie default		wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww
🔕 セキュリティファブリック ゝ		192.168.0.0/16						APP default		WED Base Profile
ビログをレポート >								Sil certificate-intraction		WEE Base Profileのクローン実験
								適用 キャンセル		wee default
										wse defaultのクローン実験用
		🖂 all	🖂 all	d always	I ALL	⊘ 拒否			◎ 有効化済み	wee g-default

Copyright (c) 2024 NTT PC Communications Incorporated, All Right Reserved.



表 3-2.	ファイア	゙ウォールルー	-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 ォールアドレスもしくはファイアウォ 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 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 ォールアドレスもしくはファイアウォ 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	always			
9	サービス	任意:制御対象のプロトコルタイプ(U 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				
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				
		- 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		
16	セキュリティ	- 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		
	ノロノアイル	- 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			
47		- 許可トラフィックをログ	すべての セッション			
17	ロキンクオフション	- 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/ 定	無効化を指	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。

Copyright (c) 2024 NTT PC Communications Incorporated, All Right Reserved.



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。

	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 <sup>*</sup>	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 <sup>%</sup>
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
		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	アプリケーションコント	アプリケーションコント
16	ヤキュリティプロファイル	ロール:無効	ロール:無効	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	ロギングナプション	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

表 3-2. ファイアウォールルールの設定項目(1/3).

※ 初期設定時は、未定義のリストを提供



	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	©ALL_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 <sup>%</sup>	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
		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
16	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 : 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
		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
17	ロギングオプション	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

表 3-2. ファイアウォールルールの設定項目(2/3).

※ 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	⊘LAN -> WAN	®webfilter-policy-*	©user-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	
		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	
	セキュリティプロ	アフリケーションコント   ロール:有効	アフリケーションコン トロール: 有効	アフリケーションコント   ロール : 有効	
16	ファイル	IPS(侵入防止):無効	IPS(侵入防止):無効	IPS(侵入防止):無効	$\square$
		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	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

Copyright (c) 2024 NTT PC Communications Incorporated, All Right Reserved.



#### 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。

	設定項目	設定内容	デフォルト設定
		アンチウイルススキャ ン	ブロック
	アンチウイルス	機能セット	プロキシベース
			HTTP:有効
			SMTP:無効
			P0P3:無効
		インスペクションされ	IMAP:無効
		るプロトコル	FTP:無効
1			CIFS:無効
I			MAPI:無効
			SSH:無効
			コンテンツ無害化:無効
		ATP プロテクションオ プション	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	FortiGuard アウトブレイク防止データ ベースを使用: 無効 <sup>+</sup>
		ク防止	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(1/3).



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						
		機能セット	プロキシベース						
			項目	カテゴリ					
			ローカルカテゴ リ : 無効	custom1		Custom2	2		
			違法性の高いサ	薬物乱用	ハッキング		違法または非 倫理的		
			イト:ブロック	差別	明示的机	は暴力	盗作		
		FortiGuard カテゴ リベースのフィル タ設定		児童虐待					
			アダルト/成人コ ンテンツ : ブロ	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		
			ック	ポルノ	出会い	Ŕ	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: 詐欺	レング	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						
2	WEB フィルタ		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 URI	URL フィルタ:無効						
		フィルタ	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					
			レーティングエラー	-発生時に Web サイ	イトを許す	可:無効			
		レーティングオプ	ドメインまたは IP	アドレスで URL を	レーティ	ング:無	劾		
		ション	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
		カテゴリ	すべてモニタ
		ネットワークプロトコルの 強制	
3	アプリケーションコ	アプリケーションとフィル タのオーバーライド	なし
	ントロール		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
		オプション	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
		悪意のある URL をブロック	有効
			タイプ : フィルタ
			アクション : デフォルト
4	IPS (侵入防止)	IPS シグネチャとフィルタ	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
		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
			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]
		プロトコルごとのスパム検 知数	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]
5	アンチスパム		IP アドレスチェック:有効
Ŭ	(E メールフィルタ)		URL チェック :有効
		FortiGuard スパムフィルタ リング	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
			HELO DNS ルックアップ:無効
		ローカルスパムフィルタリ ング	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。



- 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 (po	🗄 🔰 LAN (port:18 vlan101) — 🗚 WAN (vlan2001.emv1) 🕖										
〒 暗黙 ①											



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

TEST-NWUTM-FG01A 🔹	≡ Q						VDOM: 🚭 user01 🔹	>_ ଡ - ♀ - ⊖ user01 -
🗗 ダッシュボード 🔹 🔉	➡新規作成		■ 削除 Q 市	パリシーのルックア	ップ検索			Q
	目 エクスポー	-ト・ インターフェースペン	7ビュー シーケン	ス別				
🛃 ポリシー&オブジェクト 🗸 🗸	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
ファイアウォールポリシー 🟠	🖃 3월 LAN (po	rt18.vlan101) → ೫೫ WAN (vla	n2001.emv1) 7					
	NTTPC Monif	tor Rule 🗐 100.88.18.0/29	💷 all	🖸 always	🖬 ALL	✔ 許可	160.248.241.1/	ss. no-inspection 🤇
インターネットサービスデ ータベース	Src Black Rule	e 🖷 Src Black list	😑 all	🖸 always	🖬 ALL	⊘ 拒否		٩
サービス	Dst Black Rul	ポリシー	Dst Black li	🕞 always	🖬 ALL	⊘ 拒否		٥
パーチャルIP	Src White Ru	設定ステータス・	😑 all	lo always	🖬 ALL	✔ 許可	160.248.241.1/	ssu no-inspection
🔒 セキュリティプロファイル ゝ	Dst White Ru	▼名前でフィルタ・・	🐴 Dst White I	lo always	🖬 ALL	✔ 許可	160.248.241.1/	ssu no-inspection
* 5254 >	ALL_ICMP	4b⊐ピ–	💷 all	o always	ALL_ICMP	✔ 許可	160.248.241.1/	ss. no-inspection
- <i>③</i> セキュリティファブリック <b>&gt;</b>	LAN -> WAN		🗐 all	🚺 always	🖬 ALL	✔ 許可	160.248.241.1/	AV default
■ ログ&レポート >		▼ 望のホリシーを挿入 →						APP default
		間一致するログを表示						ssu certificate-inspection
	🛨 暗黙 1	■FortiViewで表示する						
		✔ 編集						
	<	>_ CLIで編集						•
FURTIDET v7.2.7	0 セキュリテ	自 ポリシー削除						🚯 更新済み: 09:46:45 🤇

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。

TEST-NWUTM-FG01A 👻	≡ Q					,	/DOM: 🗅 user01 🕶	>_ ? · ∴ · ⊖ user01 ·
🙆 ダッシュボード 🔉 👌	➡新規作成 🖌	編集 >_ CLIで編集	<b>菌</b> 削除 Q 力	ペリシーのルックア	ップ検索			Q
🕁 ネットワーク 🍡 👌	■ エクスポート・	インターフェースペス	7ビュー シーケン	ス別				
🖹 ポリシー&オブジェクト 🗸 🗸	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
ファイアウォールポリシー 🏠	E 왜 LAN (port 18	vlan101) → ೫ WAN (vlar	12001.emv1) (7)					
	NTTPC Monitor R	ule 🔳 100.88.18.0/29	💷 all	🖸 always	д ALL	✔ 許可	160.248.241.1/	55. no-inspection
インターネットサービスデ ータベース	Src Black Rule	🖷 Src Black list	💷 all	🐻 always	🖬 ALL	⊘ 拒否		٥
サービス	Dst Black Rule	ポリシー	Dst Black li	🖸 always	🖬 ALL	⊘ 拒否		٩
バーチャルIP	Src White Rule	設定 ステータス	▶ all	🖸 always	🖬 ALL	✔ 許可	(a) 160.248.241.1/	ss. no-inspection
🔺 セキュリティプロファイル 👂	Dst White Rule	▼ 名前 でフィルタ	<ul> <li>Dst White I</li> </ul>	🖸 always	🖬 ALL	✔ 許可	160.248.241.1/	ss. no-inspection
<ul> <li>         ・システム         ・         ・         ・</li></ul>	ALL_ICMP	@⊐Ľ-	all	🖸 always	ALL_ICMP	✔ 許可	160.248.241.1/	551 no-inspection
🐠 セキュリティファブリック ゝ	LAN -> WAN		<ul> <li>・ ・ 上へ</li> </ul>	🖸 always	🖫 ALL	✔ 許可	160.248.241.1/	AV default
<u>Ш</u> ログ&レポート >		▼ 空のボリシーを挿入	• • • • •					APP default
		じったいます。						ss. certificate-inspection
	田 暗黙 ①	■FortiViewで表示する						
		● 編集						
		>_ CLIで編集						4
	0 セキュリティレ	會 ポリシー削除						🚯 更新済み: 09:46:45 🖸

#### ④ 作成したポリシーをダブルクリックする。

🐺 TEST-NWUTM-FG01A 🛛 👻	≡ Q						'DOM: 💁 user01 - 🔹 💙	- 🛛 • 🗘 • 😝 user0
🙃 ダッシュボード 🔉	+新規作成 🖋 編集	毛 >_ CLIで編集	<b>創除</b> Q ポ	リシーのルックア	ップ検索			Q
♣ ネットワーク	■ エクスポート▼	インターフェースペス	7ビュー シーケン	ス別				
💄 ポリシー&オブジェクト 🗸 🗸	久前	送信录	一一一一	フケジュール	++-1-1-1-7	アクション	NIAT	ヤキュリティプロファイバ
			9676	X) 91-10	9-LX	799999	NAI	242974909747
アドレス	E 3 LAN (port 18.vlar	101) → ₩ WAN (via	12001.emv1) (8)			4 B/r =7		
インターネットサービスデ	Ste Black Bule	100.88.18.0/29	) all	Lo always		✓ 計可	(a) 160.248.241.1/32	no-inspection
	Src Black Rule	SFC Black list	🚍 all	Lo always		<ul> <li>✓ 推告</li> <li>▲ 振雨</li> </ul>		
サービス	Dst Black Rule	gan an	DST BIACK list			●推賞	Q 440 340 344 4733	
パーチャルIP	Src white Rule	Sic write list	an an	Lo always		✓ i+-ŋ	160.246.241.1/32	se no-inspection
セキュリティプロファイル ゝ	Dst white Rule	all 📃	Dst White list	Lo always		✔ 許可	160.248.241.1/32	sa no-inspection
• システム <b>&gt;</b>	ALL_ICMP	🚆 all	😑 all	lo always	L ALL_ICMP	✔ 許可	(ii) 160.248.241.1/32	55L no-inspection
🔊 セキュリティファブリック ゝ	<u>.</u>	10.0.0.0/8 172.16.0.0/12	😑 all	🗗 always	🖬 ALL	✔ 許可	160.248.241.1/32	AV default
<u>u</u> ログ&レポート >		192.168.0.0/16						APP default
								ss. certificate-inspectio
	LAN -> WAN	10.0.0/8	🔲 all	lo always	🖬 ALL	✔ 許可	160.248.241.1/32	AV default
		1/2.16.0.0/12 192.168.0.0/16						WEB default
FCIRTINET v7.2.7	0 セキュリティレーテ	インク問題						0% 😰 更新済み: 13:09:10

## 👫 Master'sONE°

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





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.vlar	n101) → 🕫 WAN (vlar	12001.emv1) 🥑								
NTTPC Monitor Rule	100.88.18.0/29	🖻 all	🕫 always	I ALL	✔ 許可	160.248.241.1/32	ssu no-inspection	😂 無効化済み	0.8	スタンダ・
Src Black Rule	🖥 Src Black list	🖻 all	🕫 always	I ALL	⊘ 拒否			🥏 すべて	0.8	スタンダ・
Dst Black Rule	🗐 all	👼 Dst Black list	😡 always	🖳 ALL	⊘ 拒否			🗢 すべて	ОB	スタンダ・
Src White Rule	🖥 Src White list	🖻 all	👩 always	I ALL	✔ 許可	160.248.241.1/32	ssu no-inspection	🕏 すべて	0.8	スタンダ・
Dst White Rule	😑 all	👼 Dst White list	👩 always	I ALL	✔ 許可	160.248.241.1/32	ssu no-inspection	🕏 すべて	1.11 MB	スタンダ
ALL_ICMP	😑 all	🖻 all	🔊 always	ALL_ICMP	✔ 許可	(2) 160.248.241.1/32	ssu no-inspection	🗢 すべて	0.8	スタンダ・
LAN3 😡	<ul> <li>☐ 10.0.0.0/8</li> <li>↓ 172.16.0.0/12</li> <li>☐ 192.168.0.0/16</li> </ul>	🗐 all	😡 always	I ALL	✔ 許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	🎯 すべて	ОB	スタンダー
LAN2 💱	<ul> <li>☑ 10.0.0.0<sup>18</sup></li> <li>☑ 172.14 0.0/12</li> <li>☑ 192.468.0.0/16</li> </ul>	😑 all	😡 always	ह्य ALL	✔ 許可	(a) 160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	🕏 কৃশ্বে	ОB	スタンダー
LAN -> WAN	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	🖻 all	👩 always	🖳 ALL	✔ 許可	160.248.241.1/32	M         default           WEB         default           APP         default           SR         certificate-inspection	🕏 রুশ্বে	92.35 MB	スタンダ・
● 暗黙 ①										>

#### 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。

TEST-NWUTM-FG01A +	≡ Q.							VDC	DM: 🙆 user01 •	>_ <b>0</b> · 4 · (	<b>9</b> user01 •
🙆 ダッシュボード 🔹 🔉	+新規作成 🖋 編	実 >_ CLIで編集	意 削除 🔍 7	ペリシーのルックア	ップ検索			Q 🗎 エクスポー	-ト・ インター	フェースペアビュー 📀	ーケンス別
ネットワーク >	名前	送信元	宛先	スケジュール	サービス	アクション	TAN	セキュリティプロファイル	ログ	バイト	タイプ
💄 ポリシー&オブジェクト 🗸 🗸	🖃 🕫 LAN (port18.vla	n101) → <b>35</b> WAN (vlar	n2001.emv1) 🥑								
ファイアウォールポリシー 🏠	NTTPC Monitor Rule	100.88.18.0/29	🗉 all	😡 always	🖪 ALL	✔ 許可	(2) 160.248.241.1/32	ssu no-inspection	🟮 無効化済み	0 B	スタンダ・
アドレス	Src Black Rule	👼 Src Black list	🗉 all	😡 always	🖪 ALL	⊘ 拒否			🛛 すべて	oв	スタンダ・
インターネットサービスデ ータベース	Dst Black Rule	🖻 all	🗟 Dst Black list	😡 always	😰 ALL	⊘ 拒否			すべて	ОB	スタンダ・
#_P7	Src White Rule	🖷 Src Whitelist	😑 all	👩 always	😰 ALL	✔ 許可	160.248.241.1/32	551 no-inspection	🛛 すべて	0 B	スタンダ・
バーチャルル	Dst White Rule	🖭 all	看 Dst White list	😡 always	😰 ALL	✔ 許可	160.248.241.1/32	ss. no-inspection	🗢 すべて	1.11 MB	スタンダ・
A セキュリティブロファイル、	ALL_ICMP	😑 all	🖻 all	👩 always	ALL_ICMP	✔ 許可	(2) 160.248.241.1/32	ssu no-inspection	🛛 すべて	0 B	スタンダ・
		⊑ 10.0.0.0/8 ⊑ 172.16.0.0/12 ポリシー	🖻 all	👩 always	ALL	✔ 許可	a) 160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	🛛 রুশ্বে	08	スタンダ・
	LAN3 Q 上AN3 Q マ 名前 凸 コヒ 尼 ペー	テータス ・ 1でフィルタ ・ 	<ul> <li>● 有効</li> <li>◎ 無効</li> </ul>	🔏 always	I ALL	✔ 許可	(a) 160.248.241.1/32	AV default WEE default APP default SU certificate-inspection	🕲 इंर्ल्स्ट	08	スタンダ・
	LAN -> WAN + 空の 能一致 座Fort	Dポリシーを挿入 ・ するログを表示 iViewで表示する	🔄 all	👩 always	D ALL	✔ 許可	160.248.241.1/32	W default WE0 default APP default SSC certificate-inspection	🕏 রুশ্বে	92.78 MB	スタンダ・
	● 暗黙 ③ / 編録 ↓ CLI	と で編集 リシー削除									
	○ セキュリ <u>デ</u>									14:	21:45 2



⑧ ルールが有効になったことを確認する。

+新規作成 / 編集	ミン- CLIで編集	● 削除 ♀ ;	ポリシーのルックフ	マップ 検索			Q 🗎 エクスポー	ート・ インター	・フェースペアビュー	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	タイプ
🖃 🧏 LAN (port18.vlar	101) → 🕽 WAN (vlar	12001.emv1) 🥑								
NTTPC Monitor Rule	100.88.18.0/29	😑 all	😡 always	🖳 ALL	✔ 許可	160.248.241.1/32	ssu no-inspection	😂 無効化済み	ов	スタンダ・
Src Black Rule	疆 Src			I ALL	🖉 拒否			🗢 すべて	ОB	スタンダ・
Dst Black Rule	≌ ≕ × が	バネてし	いれば	I ALL	🖉 拒否			🗢 すべて	ов	スタンダ
Src White Rule	疆 Src	11 1		I ALL	✔ 許可	160.248.241.1/32	ssu no-inspection	🗢 すべて	ОB	スタンダ・
Dst White Rule	▣ 페 有郊	北されて	いる	ALL	✔ 許可	160.248.241.1/32	ssu no-inspection	🕏 すべて	1.11 MB	スタンダ・
ALL_ICMP	😑 all			ALL_ICMP	✔ 許可	(2) 160.248.241.1/32	ssu no-inspection	🗢 すべて	ов	スタンダ
LAN2	<ul> <li>□ 10</li> <li>□ 172.16.0.0/12</li> <li>□ 192.168.0.0/16</li> </ul>	⊑ all	😡 always	الم ALL	✔ 許可	(a) 160.248.241.1/32	AV default VEB default APP default SE certificate-inspection	🛛 কৃশ্বে	oв	スタンダー
LAN3 🛱	<ul> <li>□ 10.0.0.0/8</li> <li>□ 172.16.0.0/12</li> <li>□ 192.168.0.0/16</li> </ul>	o all	😡 always	图 ALL	✔ 許可	(a) 160.248.241.1/32	AV default WEB default APP default SL certificate-inspection	すべて	ΟB	スタンダー
LAN -> WAN	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	🔄 all	😡 always	1 ALL	✔ 許可	(a) 160.248.241.1/32	AV default WEB default APP default SI certificate-inspection	🕏 র্শেত	92.78 MB	- スタンダ・
<ul> <li>● 暗黙 ①</li> <li></li> <li></li></ul>	イング問題								『保存されました。 <u></u>	))). ×

- 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。

	TEST-NWUTM-FG01A 🔹	≡ Q.								OM: 🙆 user01 - 💦 🔪	0 • ↓ • O user01 •
	🛛 ダッシュボード 🔹 🔉	+新規作成 ✔ 編	実 >_ cuで編集 歯 削	<b>Q</b> ポリシーのルック	アップ 検索			Q	■ エクスポ	ート・ インターフェー	スペアビュー シーケンス別
	🖶 ネットワーク 🔹 🔉	名前	From	То	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
	🖹 ポリシー&オブジェクト 🛛 🗸	NTTPC Monitor Rule	E DE LAN (port18.vlan101)	>§ WAN (vlan2001.emv1)	100.88.18.0/29	😑 all	😡 always	ALL ALL	✔ 許可	160.248.241.1/32	ss no-inspection
		Src Black Rule	LAN (port18.vlan101)	> WAN (vlan2001.emv1)	🖥 Src Black list	🖂 all	always	ALL	⊘ 拒否		
		Dst Black Rule	H LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	🖻 all	🖥 Dst Black list	G always	ALL	⊘ 拒否		
	インターネットサービスデ	Src White Rule	H LAN (port18.vlan101)	> WAN (vlan2001.emv1)	👼 Src White list	🖻 all	o always	ALL	✔ 許可	160.248.241.1/32	ss. no-inspection
		Dst White Rule	H LAN (port18.vlan101)	> WAN (vlan2001.emv1)	😫 all	🖥 Dst White list	👩 always	ALL	✔ 許可	160.248.241.1/32	ss. no-inspection
	9-EX	ALL_ICMP	3 LAN (port18.vlan101)	58 WAN (vlan2001.emv1)	🖬 all	🗉 all	læ always	ALL_ICMP	✔ 許可	160.248.241.1/32	ss. no-inspection
	ハーチャルルP ▲ セキュリティプロファイル >	LAN -> WAN	36 LAN (port18.vlan101)	35 WAN (vlan 2001.emv1)	<ul> <li>10.0.0.0/8</li> <li>172 16 0.0/12</li> </ul>	🗄 all	👩 always	I ALL	✔ 許可	(160.248.241.1/32)	AV default
	<ul><li></li></ul>				<ul> <li>192.168.0.0/16</li> </ul>						APP default
	をキュリティファブリック							_			sectificate-inspection
	ビログ&レポート >	暗黙の拒否	g庄 人デーダス ▼ 夕前 アコノ⊫ わ	iny	E all	😑 all	lo always	I ALL	⊘ 拒否		
			<ul> <li>Am C ノイルタ</li> <li>A コピー</li> </ul>	- <b>1</b>							
			B ペースト								
			▶ 空のポリシーを挿入	,							
		•	▶ シーケンスグルーピングを	揮入							
		r	al一致するログを表示								
~			■FortiViewで表示する								
Copy			✔ 編集								
		4 <b>— — — &gt;</b>	_ CLI で編集							-	Þ
		○ セキュリティレー (	町 ポリシー削除								⑤ 更新済み: 14:33:27 2



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。

TEST-NWUTM-FG01A 🔹	≡ Q.							VDO	M: 🗳 user01 • 💦 >_	Ø• ↓• Øuser01•
🙆 ダッシュボード 🔹 🔉	+新規作成 🖋	編集 >_ CLIで編集   自 削	余 ペポリシーのルック	アップ検索			Q	■ エクスポー	-ト・ インターフェー	スペアビュー シーケンス別
<ul> <li>ホットワーク</li> <li></li> </ul>	名前	From	То	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
💄 ポリシー&オブジェクト 🗸 🗸	NTTPC Monitor R	ule 🕃 LAN (port18.vlan101)	98 WAN (vlan2001.emv1)	100.88.18.0/29	🗉 all	😡 always	🛛 ALL	✔ 許可	160.248.241.1/32	sst no-inspection
ファイアウォールポリシー 🏠	Src Black Rule	3€ LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	🖥 Src Black list	🖽 all	l always	I ALL	⊘ 拒否		
	Dst Black Rule	35 LAN (port18.vian101)	WAN (vlan2001.emv1)	🖻 all	🖥 DstBlacklist	👩 always	😰 ALL	⊘ 拒否		
インターネットサービスデ ータベース	Src White Rule	35 LAN (port18.vian101)	₩AN (vlan2001.emv1)	🖥 Src White list	🖽 all	😡 always	🖪 ALL	✔ 許可	(2) 160.248.241.1/32	ss. no-inspection
サービス	Dst White Rule	3€ LAN (port18.vian101)	S WAN (vlan 2001.emv1)	🖻 all	看 Dst White list	👩 always	🕑 ALL	✔ 許可	160.248.241.1/32	ss. no-inspection
バーチャルP	ALL_ICMP	3€ LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	🔄 211	🖾 all	😡 always	ALL_ICMP	✔ 許可	160.248.241.1/32	ss. no-inspection
セキュリティプロファイル >	LAN -> WAN	38 LAN (port18.vian101)	SE WAN (vlan2001.emv1)	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> </ul>	🖽 all	😡 always	I ALL	✔ 許可	160.248.241.1/32	AV default
• 52754 >		ポリシー		192.168.0.0/16						APP default
🕼 セキュリティファブリック ゝ	101575 I	みた ステータス		E all	E all	E abuma		<b>0</b> 15不		se cerancate-inspection
□□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	暗然の地合い	▼ 名前でフィルタ	any	<b>2</b> 30	<b>2</b> 30	ug always	I ALL	❷ 把告		
	é	8⊐ピ–								
		<b>ひ</b> ペースト	· ~ 上へ							
	•	╋ 空のポリシーを挿入	・ ~ 下へ							
	·	<ul> <li>シーケンスグルーピングを挿</li> </ul>	~							
		<b>虐一致するログを表示</b>								
		■FortiViewで表示する								
	í	✔ 編集								
	· · · · · · · · · · · · · · · · · · ·	- CLIで編集								►
	<ul> <li>セキュリティー</li> </ul>	卣 ポリシー削除								💿 更新済み: 14:33:27 💈

④ 作成したポリシーをダブルクリックする。

TEST-NWUTM-FG01A •	≡ Q,							VDC	)M: 💁 user01 • 🛛 >_	Ø• ↓• ⊖ user01•
🙆 ダッシュボード 🔹 🔸	+新規作成 / 編集	E >_ CLIで編集 自削	除 Q ポリシーのルック	アップ検索			Q	■ エクスポー	-ト・ インターフェー	スペアビュー シーケンス別
<ul> <li>ホットワーク</li> <li>&gt;</li> </ul>	名前	From	То	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
💄 ポリシー&オブジェクト 🔹 🗸	NTTPC Monitor Rule	3 LAN (port18.vlan101)	35 WAN (vlan2001.emv1)	100.88.18.0/29	🖻 all	læ always	I ALL	✔ 許可	160.248.241.1/32	58 no-inspection
ファイアウォールポリシー 🏫	Src Black Rule	HAN (port18.vlan101)	SE WAN (vian2001.emv1)	👼 Src Black list	🖻 all	la always	I ALL	⊘ 拒否		
アドレス	Dst Black Rule	H LAN (port18.vlan101)	WAN (vlan 2001.emv1)	🗉 all	🖥 Dst Black list	👩 always	I ALL	⊘ 拒否		
インターネットサービスデ ータベース	Src White Rule	3€ LAN (port18.vlan101)	₩AN (vlan2001.emv1)	👼 Src White list	😫 all	🖬 always	I ALL	✔ 許可	160.248.241.1/32	ssu no-inspection
#	Dst White Rule	₩ LAN (port18.vlan101)	₩AN (vlan2001.emv1)	🖽 all	🖥 Dst White list	lo always	I ALL	✔ 許可	160.248.241.1/32	ss no-inspection
バーチャルロ	ALL_ICMP	3 LAN (port18.vlan101)	5 WAN (vlan2001.emv1)	🖻 all	🖻 all	😡 always	ALL_ICMP	✔ 許可	9 160.248.241.1/32	ss no-inspection
▲ セキュリティプロファイル >	<u>0</u>	35 LAN (port18.vlan101)	SE WAN (vian2001.emv1)	10.0.0/8	🖻 all	😡 always	P ALL	✔ 許可	160.248.241.1/32	AV default
■				<ul> <li>1/2.168.0.0/12</li> <li>192.168.0.0/16</li> </ul>						APP default
<ul> <li>セキュリティファブリック &gt;</li> </ul>										ssa certificate-inspection
ビログ&レポート >	LAN -> WAN	38 LAN (port18.vlan101)	35 WAN (vian 2001.emv1)	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	E all	😡 always	I ALL	✔ 許可	團 160.248.241.1/32	AV default WED default APP default SSL certificate-inspection
	暗黙の拒否	🗆 any	🗆 any	🖾 all	🖻 all	👩 always	I ALL	⊘ 拒否		
										>
	○ セキュリティレーティ	ィング問題								🕲 更新済み: 14:33:27 🙄

## 👫 Master's ONE°

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





33

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	То	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	3 LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	100.88.18.0/29	🗉 all	😡 always	🖳 ALL	✔ 許可	160.248.241.1/32	ssL no-inspection
Src Black Rule	35 LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	👼 Src Black list	🖻 all	🗔 always	ALL	⊘ 拒否		
Dst Black Rule	38 LAN (port18.vlan101)	₩AN (vlan2001.emv1)	🖬 all	👼 Dst Black list	😡 always	🖳 ALL	🖉 拒否		
Src White Rule	38 LAN (port18.vlan101)	₩AN (vlan2001.emv1)	疆 Src White list	🖾 all	😡 always	🖳 ALL	✔ 許可	160.248.241.1/32	ssL no-inspection
Dst White Rule	38 LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	🗉 all	🖥 Dst White list	😡 always	🖳 ALL	✔ 許可	160.248.241.1/32	sst no-inspection
ALL_ICMP	38 LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	🖬 all	😫 all	😡 always	ALL_ICMP	✔ 許可	160.248.241.1/32	ssL no-inspection
LAN3 😡	35 LAN (port18.vlan101)	38 WAN (vlan 2001.emv1)	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	望 all	😡 always	I ALL	✔ 許可	₪ 160.248.241.1/32	<ul> <li>✓ default</li> <li>✓ default</li> <li>▲ APP default</li> <li>SSL certificate-inspection</li> </ul>
LAN2 💱	38 LAN (pyrt18.vlan101)	35 WAN (vlan 2001.emv1)	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	😑 all	😡 always	로 ALL	✔ 許可	₪ 160.248.241.1/32	AV default WEP default APP default SSL certificate-inspection
LAN -> WAN	3€ LAN (port18.vlan101)	38 WAN (vlan 2001.emv1)	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	🖅 all	😡 always	😨 ALL	✔ 許可	(g) 160.248.241.1/32	Me default default APP default St. certificate-inspection
暗黙の拒否	🗆 any	🗆 any	🗉 all	🖾 all	🗔 always	🖳 ALL	⊘ 拒否		
<ul> <li>セキュリティレーデ</li> </ul>	イング問題							_	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。

TEST-NWUTM-FG01A 🔹	≡ Q.							VDC	)M: 🔷 user01 • 🛛 >_	0 • ↓ • O user01 •
🙆 ダッシュボード 🔹 🔉	◆新規作成 🖋	編集 >_ CLIで編集 🛛 削	象 ペポリシーのルック	アップ検索			Q	■ エクスポー	-ト・ インターフェー	スペアビュー シーケンス別
	名前	From	То	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
占 ポリシー&オブジェクト 🗸	NTTPC Monitor Ru	ile 📲 LAN (port18.vlan101)	98 WAN (vlan 2001.emv1)	100.88.18.0/29	🖻 all	😡 always	I ALL	✔ 許可	160.248.241.1/32	ssu no-inspection
ファイアウォールボリシー ☆	Src Black Rule	SE LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	👼 Src Black list	🚍 all	🖪 always	I ALL	⊘ 拒否		
	Dst Black Rule	😹 LAN (port18.vlan101)	3§ WAN (vlan2001.emv1)	🗉 all	🖥 Dst Black list	🖪 always	I ALL	⊘ 拒否		
インターネットサービスデ ータベース	Src White Rule	😹 LAN (port18.vlan101)	3§ WAN (vlan2001.emv1)	🖥 Src White list	😑 all	😡 always	I ALL	✔ 許可	160.248.241.1/32	ssu no-inspection
サービス	Dst White Rule	3 LAN (port18.vlan101)	08 WAN (vlan2001.emv1)	🚍 all	👼 Dst White list	😡 always	I ALL	✔ 許可	160.248.241.1/32	ssu no-inspection
バーチャルア	ALL_ICMP	3 LAN (port18.vlan101)	38 WAN (vlan 2001.emv1)	🗉 all	🖾 all	😡 always	ALL_ICMP	✔ 許可	160.248.241.1/32	ssu no-inspection
▲ セキュリティプロファイル >		೫ LAN (port18.vlan101) ポリシー	5§ WAN (vlan 2001.emv1)	<ul> <li>■ 10.0.0.0/8</li> <li>■ 172.16.0.0/12</li> <li>■ 192.168.0.0/16</li> </ul>	물 all	😡 always	ALL	✔ 許可	160.248.241.1/32	W default WEB default APP default SSL certificate-inspection
ビログ&レポート >	LAN3 Q 證:	定ステータス 名前でフィルタ コピー	<ul> <li>● 有効 in 2001.emv1)</li> <li>● 無効</li> </ul>	달 10.0.0.0/8 달 172.16.0.0/12 달 192.168.0.0/16	멸 all	😡 always	R ALL	✔ 許可	160.248.241.1/32	WED     default       MED     default       APP     default       SSL     certificate-inspection
	LAN -> WAN +	ハースト 空のポリシーを挿入 シーケンスグルーピングを挿入 一致するログを集ます。	WAN (vlan 2001.emv1)	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	🔄 all	😡 always	🖳 ALL	✔ 許可	160.248.241.1/32	default web default APP default sst certificate-inspection
	暗黙の拒否	スッシーンで扱い FortiViewで表示する	D any	🖻 all	🖻 all	😡 always	I ALL	⊘ 拒否		
	A	編集 CLIで編集							-	Þ
	○ セキュリティ 箇	ポリシー削除								🔞 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。

TEST-NWUTM-FG01A •	≡ Q.							VD	30M: 💁 user01 • 🛛 >_	0 • ↓ • ⊖ user01 •
🙆 ダッシュボード 🔹 🔉	+新規作成 / 編集	毛 >_ CLIで編集 自 削	除 Q ポリシーのルック	7アップ 検索			Q	■ エクスポ	ペート・ インターフェー	スペアビュー シーケンス別
	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
💄 ポリシー&オブジェクト 🔹	NTTPC Monitor Rule	38 LAN (pe		3.0/2	9 🖬 all	G always	😰 ALL	✔ 許可	@ 160.248.241.1/32	ss. no-inspection
ファイアウォールポリシー 合	Src Black Rule	JE LANIN ×ガ	「消えていれ	ば list	🔁 all	😡 always	ALL	⊘ 拒否		
アドレス	Dst Black Rule	28 LAN (pr			😼 Dst Black list	lo always	I ALL	⊘ 拒否		
インターネットサービスデ ータベース	Src White Rule	38 LAN (P 有效	」化されてい	NG list	🖻 all	la always	😰 ALL	✔ 許可	160.248.241.1/32	53L no-inspection
+	Dst White Rule	DE LAN (pe			👼 Dst White list	la always	😰 ALL	✔ 許可	160.248.241.1/32	ss no-inspection
バーチャルロ	ALL_ICMP	3 LAN (port10	wAN (vlan2001.emv1)	🖃 all	🖬 all	😡 always	ALL_ICMP	✔ 許可	160.248.241.1/32	ss no-inspection
▲ セキュリティプロファイル >	LAN2	Di Loov (port18.vian101)	38 WAN (vlan 2001.emv1)	■ 10.0.0.0/8	😫 all	😡 always	ALL	✔ 許可	160.248.241.1/32	AV default
• 5274 >				172.168.0.0/12	6					APP default
セキュリティファブリック >										ss. certificate-inspection
ビログ&レポート >	LAN3 8	38 LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	■ 10.0.0.0/8	🖾 all	G always	ALL	✔ 許可	@ 160.248.241.1/32	AV default
				■ 172.168.0.0/12 ■ 192.168.0.0/1	6					APP default
										ss certificate-inspection
	LAN -> WAN	3 LAN (port18.vlan101)	₩ WAN (vlan 2001.emv1)	10.0.0/8	🖬 all	G always	ALL ALL	✔ 許可	160.248.241.1/32	av default
				<ul> <li>172.16.0.0/12</li> <li>192.168.0.0/1</li> </ul>	6					APP default
										ss certificate-inspection
	暗黙の拒否	🗆 any	🗆 any	🔳 all	🚊 all	la always	I ALL	⊘ 拒否		
	0 セキュリティレーテ・	ィング問題								🔟 更新済み: 14:45:01 💈

Master'sONE<sup>®</sup>

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。



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。

TEST-NWUTM-FG01A +	≡ Q.								DM: 💁 user01 •	>_ ଡ- ≏-	<b>9</b> user01 •
🙆 ダッシュボード 🔹 🔉	+新規作成 / 編集	毛 >_ CLIで編集	自 削除 🔍 7	ペリシーのルックア	<b>'</b> ップ 検索			Q 🗟 エクスポ	ート・ インター	フェースペアビュー 👂	ーケンス別
<ul> <li>ホットワーク</li> <li></li> </ul>	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
占 ポリシー&オブジェクト 🗸 🗸	🖃 🎀 LAN (port18.vlar	101) → 升 WAN (vlar	12001.emv1) 🥑								
ファイアウォールポリシー 🏠	NTTPC Monitor Rule	100.88.18.0/29	🖸 all	👩 always	😰 ALL	✔ 許可	(2) 160.248.241.1/32	ssu no-inspection	😡 無効化済み	0 B	スタンダ・
アドレス	Src Black Rule	🖥 Src Black list	🖻 all	😡 always	I ALL	⊘ 拒否			すべて	ов	スタンダ・
インターネットサービスデ ータベース	Dst Black Rule	🚍 all	🖥 Dst Black list	😡 always	I ALL	⊘ 拒否			♥ すべて	0 B	スタンダ
+-127	Src White Rule	疆 Src White list	🖻 all	👩 always	I ALL	✔ 許可	160.248.241.1/32	<sup>551</sup> no-inspection	🗢 すべて	0 B	スタンダ・
パーチャルロ	Dst White Rule	🖻 all	👼 Dst White list	👩 always	I ALL	✔ 許可	160.248.241.1/32	ssu no-inspection	♥ すべて	1.13 MB	スタンダ
A セキュリティプロファイル、>	ALL_ICMP	🔄 all	🖻 all	👩 always	ALL_ICMP	✔ 許可	160.248.241.1/32	ssu no-inspection	🕏 すべて	0 B	スタンダ・
	LAN2	■ 10.0.0.0/8	🖻 all	👩 always	I ALL	✔ 許可	160.248.241.1/32	AV default	🔿 কৃশ্ব	0 B	スタンち
<ul> <li>セキュリティファブリック</li> </ul>		192.168.0.0/12						APP default			
ビログ&レポート >								ssi certificate-inspection			
	LAN3 😳	E 10.0.0.0/8	🖻 all	😡 always	I ALL	✔ 許可	@ 160.248.241.1/32	A/ default	◎ すべて	ОB	スタンダ・
		192.168.0.0/16						APP default			
								ss certificate-inspection			
	LAN -> WAN	10.0.0.0/8	🖻 all	😡 always	I ALL	✔ 許可	160.248.241.1/32	AV default	🕏 すべて	93.73 MB	スタンダ
		192.168.0.0/16						APP default			
								sst certificate-inspection			
	< C										
	<ul> <li>セキュリティレーテ・</li> </ul>	ィング問題								11 更新済み:14	:53:43 2



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。

ポリシーの編集				
				統計
名前 🚯	LAN2			
タイプ	<i></i>			
着信インターフェース	×をクリック	して削除する	•	h
発信インターフェース		_	-	Ē
送信元	■ 10.0	.0.0/8 160.0/12	×	5
	<b>192</b>	168.0.0/16	×	ł
IP/MACベースアクセスコン	~□−ル 3	+		*
宛先	🗐 all		×	Ę
		+		
スケジュール	Lo alwa	ys	•	
サービス	🖬 ALL		×	
マクション.				7日
1000				11
インスペクションモード	7ローベース プ <u>ロキシ</u>	バース		750
				500
			ОК	キャンセル

④ 変更完了後、正しく変更されたことを確認します。

LAN2	10.0.0/8	💷 all	🕟 always	🖪 ALL	✔ 許可	160.248.241.1/	AV defai
	172.16.0.0/12						WEB defai
							APP defai
							ssi 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。

TEST-NWUTM-FG01A 🔹	≡ Q.								t 🗗 user01 - 🔪 🤅	→ ↓ - ⊖ user01 -
🙆 ダッシュボード 🔹 🔉	▶ 新規作成 ● 編集	E >_ CLIで編集 自 削	象 ペポリシーのルックス	アップ 検索			Q	■ エクスポート	・ インターフェースハ	マアビュー シーケンス別
	名前	From	То	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
💄 ポリシー&オブジェクト 🗸 🗸	NTTPC Monitor Rule	3 LAN (port18.vlan101)	38 WAN (vlan 2001.emv1)	100.88.18.0/29	🖾 all	lo always	ALL	✔ 許可	160.248.241.1/32	Si no-inspection
ファイアウォールポリシー 合	Src Black Rule	SE LAN (port18.vlan101)	38 WAN (vlan 2001.emv1)	👼 Src Black list	🖾 all	😡 always	ALL	⊘ 拒否		
アドレス	Dst Black Rule	😹 LAN (port18.vlan101)	SE WAN (vlan 2001.emv1)	🖻 all	🖥 DstBlacklist	🖬 always	I ALL	⊘ 拒否		
インターネットサービスデ ータベース	Src White Rule	38 LAN (port18.vlan101)	35 WAN (vlan 2001.emv1)	👼 Src White list	🖾 all	lo always	ALL	✔ 許可	160.248.241.1/32	ss. no-inspection
# FZ	Dst White Rule	35 LAN (port18.vlan101)	38 WAN (vlan 2001.emv1)	🖻 all	👼 Dst White list	la always	I ALL	✔ 許可	160.248.241.1/32	ss. no-inspection
バーチャルア	ALL_ICMP	) LAN (port18 vlan 101)	38 WAN (vlan 2001.emv1)	🖾 all	😫 all	😡 always	ALL_ICMP	✔ 許可	160.248.241.1/32	ss. no-inspection
	LAN2	35 LAN (port18.vlan101)	38 WAN (vlan 2001.emv1)	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	될 all	😡 always	ALL	✔ 許可	(g) 160.248.241.1/32	AV default WEB default APP default SRL certificate-inspectio
ビログ&レポート >	LAN3 Ş	98 LAN (port18.vlan101)	28 WAN (vlan 2001.emv1)	<ul> <li>☐ 10.0.0.0/8</li> <li>☐ 172.16.0.0/12</li> <li>☐ 192.168.0.0/16</li> </ul>	🔄 all	læ always	all	✔ 許可	160.248.241.1/32     160.248.241.1/32	44 default WE9 default A99 default S81 certificate-inspection
	LAN -> WAN	58 LAN (port18.vlan101)	3§ WAN (vlan 2001.emv1)	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	ile 🖬	la always	I ALL	✔ 許可	160.248.241.1/32	W default WEB default APP default SL certificate-inspectio
	暗黙の拒否	🗆 any	🗆 any	🗉 all	🗐 all	😡 always	ALL	⊘ 拒否		
										>
	0 セキュリティレーティ	ィング問題							<b>E</b> <u></u>	●更新済み: 15:12:29 2

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。

ポリシーの編集		統計
名前 🚯	LAN2	луца
タイプ	スタンダード ZTNA	1
着信インターフェース	≫≣ LAN (port18.vlan101) ▼	ł
発信インターフェース	₩ WAN (vlan2001.emv1) -	1
送信元	■ 10.0.0.0/8 ¥ ■ 172.16.0.0/12 ¥ ■ 192.168.0.0/16 ¥	1
IP/MACペースアクセスコントロール 🜖	+	ł
宛先	⊡ all ¥ +	3
スケジュール	🐻 always 👻	
サービス	ALL ×	
アクション	✔ 許可 🖉 拒否	7日 125
インスペクションモード フローベース	プロキシペース	7
	ок ≠1	ャンセル

#### ④ 変更完了後、正しく変更されたことを確認します。

LAN2	聞 LAN (port18.vlan101)	〕 WAN (vlan2001.emv1)	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> </ul>	😑 all	🖸 always	д ALL	✔ 許可

Master'sONE°

- 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。

TEST-NWUTM-FG01A -									M: 💁 user01 •	>_ 😗 - 🗘 -	🖰 user01 •
Ø ダッシュボード >	+新規作成	<ul> <li>編集 &gt;- CLIで編集</li> </ul>	會 削除 🔍 ポ	リシーのルックア	ップ検索			Q 目 エクスポー	ト・インターン	フェースペアビュー 💈	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	タイプ
🖹 ポリシー&オブジェクト 🔹 🗸	E 🧏 LAN (port:	18.vlan 101) → 3€ WAN (vlan	2001.emv1) 🥑								
ファイアウォールポリシー 🏠	NTTPCMonitor	Rule 🔄 100.88.18.0/29	🖬 all	👩 always	😰 ALL	✔ 許可	160.248.241.1/32	ss no-inspection	😫 無効化済み	ов	スタンダ
	Src Black Rule	🖷 Src Black list	🗉 all	😡 always	😰 ALL	⊘ 拒否			<ul> <li>すべて</li> </ul>	oв	スタンダ
インターネットサービスデ ータベーフ	Dst Black Rule	🖽 all	看 Dst Black list	😡 always	🕑 ALL	⊘ 拒否			◎ すべて	oв	スタンダ
+	Src White Rule	👼 Src White list	🗉 all	👩 always	🖪 ALL	✔ 許可	160.248.241.1/32	sa no-inspection	◎ すべて	oв	スタンダ
ノ こへ パーチャルD	Dst White Rule	🖻 all	疆 Dst White list	👩 always	😰 ALL	✔ 許可	160.248.241.1/32	ss no-inspection	♥ すべて	1.14 MB	スタンダ
▲ ヤキュリティプロファイル →	ALL_ICMP	🖽 all	🖻 all	🕫 always	ALL_ICMP	✔ 許可	@ 160.248.241.1/32	ss no-inspection	◎ すべて	ов	スタンダ
	LAN2	■ 10.0.0.% ■ 172.16.0.0/12 ポリシー	면 all	😡 always	I ALL	✔ 許可	160.248.241.1/32	44 default WE0 default APP default S8. certificate-inspection	🛛 রুশ্বে	1.41 MB	スタンダ
	LAN3 😡	設定ステータス ▼名前でフィルタ ゆ コピー	<ul> <li>有効</li> <li>算数</li> </ul>	.always	ILA I	✔ 許可	160.248.241.1/32	AV default WSB default APP default SSL certificate-inspection	♥ すべて	ΟB	スタンダ
	LAN → WAN	<ul> <li>         ・ロスト         ・         ・         ・</li></ul>	ile 🖻	👩 always	I ALL	✔ 許可	◙ 160.248.241.1/32	A/ default WEB default APP default SR certificate-inspection	🕏 রুশ্বে	94.82 MB	■ スタンダ
	● 暗黙 ⑤	■ FortiViewで表示する									
FERTINET V7.2.7	○ セキュリティ	ョポリシー削除			_					10 更新済み:15	22:42

### III. ルールが無効になっていることを確認する。

TEST-NWUTM-FG01A -	≡ Ϙ,								M: 💁 user01 •	>_ @• ∴•	9 user01 •
🕰 ダッシュボード 🔹 💙	+新規作成 / 編集	毛 >_ CLIで編集	◎ 削除 ♀ ポ	リシーのルックア	ップ 検索			Q 🗟 エクスポー	-ト・ インター:	フェースペアビュー	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	タイプ
🖹 ポリシー&オブジェクト 🗸 🗸	E 😹 LAN (port18.vla	n 101) → <b>3</b> 8 WAN (vlar	12001.emv1) 🤊								
ファイアウォールポリシー 🏠	NTTPC Monitor Rule	100.88.18.0/29	🗆 all	👩 always	I ALL	✔ 許可	160.248.241.1/32	ssu no-inspection	😝 無効化済み	θB	スタンダ
アドレス	Src Black Rule	🖥 Src Black list	😑 all	👩 always	ALL	⊘ 拒否			すべて	OВ	スタンダ
インターネットサービスデ ータベーフ	Dst Black Rule	🖾 all	🖥 Dst Black list	lo always	ALL	⊘ 拒否			すべて	oв	スタンダ
+-P7	Src White Rule	🖥 Src White list	🗉 all	👩 always	ALL	✔ 許可	160.248.241.1/32	ss no-inspection	◎ すべて	θB	スタンダ
バーチャルル	Dst White Rule	🖻 all	🖷 Dst White list	👩 always	ALL ALL	✔ 許可	160.248.241.1/32	ssu no-inspection	◎ すべて	1.14 MB	スタンダ
▲ ヤキュリティプロファイル >	ALL_IGMP	🖻 all		C. alumn		✔ 許可	160.248.241.1/32	ssu no-inspection	◎ すべて	ОB	スタンダ
	LAN2	10.0.0.0/8     172.16.0.     172.17	× が付 l	いてい	れば	✔ 許可	160.248.241.1/32	W default WE default AP default SL certificate-inspection	🔊 রন্দে	1.41 MB	スタンダ
	LAN3 😳	<ul> <li>□ 10.0.0.0/i</li> <li>□ 172.16.0.</li> <li>□ 192.168.0</li> </ul>	無効化:	されて	いる	✔ 許可	160.248.241.1/32	AV     default       WG0     default       APP     default       SL     certificate-inspection	🕲 इंग्रेट	ОВ	スタンダ
	LAN -> WAN 🖗	<ul> <li>□ 10.1</li> <li>□ 172.16.0.0/12</li> <li>□ 192.168.0.0/16</li> </ul>	<u> </u>	[₫ always	I ALL	✔ 許可	160.248.241.1/32	AV default WEB default APP default SI certificate-inspection	すべて	94.82.MB	スタンダ
	田 新 1										
FEIRTIDET	○ セキュリティレーテ	イング問題							<ul> <li>         ・ 変更が     </li> </ul>	保存されました。 🔃	······································



- 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。

TEST-NWUTM-FG01A +	≡ <b>Q</b>										😫 user01 •
🙆 ダッシュボード 🔹 🔹	+新規作成 / 編集	と )- CLIで編集	宮 削除 🔍 パ	「リシーのルックア	ップ検索			Q 🗟 エクスポー	-ト・ インター:	フェースペアビュー	シーケンス別
キャットワーク >	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
💄 ポリシー&オブシェクト 🔹	E 🧏 LAN (port18.vlar	101)	12001.emv1) 🤊								
ファイアウォールポリシー 合	NTTPC Monitor Rule	100.88.18.0/29	🖸 all	👩 always	😰 ALL	✔ 許可	160.248.241.1/32	ss. no-inspection	🟮 無効化済み	oв	スタンち
アドレス	Src Black Rule	🖥 Src Black list	🖻 all	👩 always	ALL ALL	⊘ 拒否			◎ すべて	ов	スタンち
インターネットサービスデ ータベース	Dst Black Rule	🗉 all	🖥 Dst Black list	la always	ALL S	⊘ 拒否			<ul> <li>すべて</li> </ul>	ов	スタンタ
#-127	Src White Rule	🖶 Src Whitelist	🖾 all	🐻 always	I ALL	✔ 許可	160.248.241.1/32	<sup>SSL</sup> no-inspection	◎ すべて	ов	スタンタ
バーチャルア	Dst White Rule	🖸 all	🖥 Dst White list	👩 always	I ALL	✔ 許可	160.248.241.1/32	ss. no-inspection	◎ すべて	1.14 MB	スタンタ
▲ ヤキュリティプロファイル >	ALL_ICMP	E all		👩 always	ALL_ICMP	✔ 許可	160.248.241.1/32	ss. no-inspection	◎ すべて	ОB	スタンタ
	LAN2	<ul> <li>■ 10.0.0.0/8</li> <li>■ 172.16.0.0/12</li> </ul>	E all	d always	ALL	✔ 許可	160.248.241.1/32	W     default       WEE     default       APP     default       SN     certificate-inspection	🕲 রেশ্বে	1.41 MB	スタンパ
	LAN3 🗘	<ul> <li>□ 10.0.0.0/8</li> <li>□ 172.16.0.0/12</li> <li>□ 192.168.0.0/16</li> </ul>	🖻 all	👩 always	🗑 ALL	✔ 許可	(a) 160.248.241.1/32	AV default WED default APP default SE certificate-inspection	<ul> <li>कर्त्त्</li> </ul>	ΟB	スタンち
	LAN -> WAN 😳	<ul> <li>□ 10.0.0.0/8</li> <li>□ 172.16.0.0/12</li> <li>□ 192.168.0.0/16</li> </ul>	E all	🗔 always	🗑 ALL	✔ 許可	(a) 160.248.241.1/32	W default will default APP default SS certificate-inspection	すべて	94.82 MB	スタンち
	● 暗黙 1										
											- ·
	○ セキュリティレーティ	ィング問題								(1) 更新済み:1	5:22:42

#### III. 確認画面が表示されるので OK を押下する。

≡ Q.								VDOM: 🛆 user01 • >_ 🕢 • 🗘 • 😝 user01 •
▶ 新規作成 🥒 編集	実 >_ CLIで編集 [	會 削除   Q ポ					0	確認 ×
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	▲ 選択した policies を削除してもよろしいですか?
🖃 🧏 LAN (port18.vla		2001.emv1) 🧐						
NTTPC Monitor Rule	100.88.18.0/29		👩 always	I ALL	✔ 許可	@ 160.248.241.1/32	ssi no-ir	
Src Black Rule	👼 Src Black list	🖻 all	😡 always	🕑 ALL	⊘ 拒否			
DstBlackRule	😑 all	覆 Dst Black list	😡 always	🗷 ALL	⊘ 拒否			
Src White Rule	🖷 Src White list	😑 all	😡 always	I ALL	✔ 許可	@ 160.248.241.1/32	sst no-ir	
Dst White Rule	🖅 all	👼 Dst White list	😡 always	I ALL	✔ 許可	() 160.248.241.1/32	SSL no-ir	
ALL_ICMP	🖅 all	🖃 all	😡 always	ALL_ICMP	✔ 許可	@ 160.248.241.1/32	ssu no-ir	
LAN2	<ul> <li>☐ 10.0.0.0/8</li> <li>☐ 172.16.0.0/12</li> </ul>	🔄 all	😡 always	ALL	✔ 許可	இ 160.248.241.1/32	AV defa WEP defa APP defa SSL certi	
LAN3 🗘	<ul> <li>☐ 10.0.0.0/8</li> <li>☐ 172.16.0.0/12</li> <li>☐ 192.168.0.0/16</li> </ul>	IIe 🖻	😡 always	I ALL		இ 160.248.241.1/32		
LAN -> WAN 🕄	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	i all	læ always	I ALL		ⓐ 160.248.241.1/32		
○ セキュリティレーテ	ィング問題							ок キャンセル



- 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	То	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	e 🕃 LAN (port18.vian101)	VIAN (vlan2001.emv1)	100.88.18.0/29	🖾 all	lo always	I ALL	✔ 許可	160.248.241.1/32	ss no-inspection
Src Black Rule	3€ LAN (port18.vian101)	₩AN (vlan2001.emv1)	👼 Src Black list	🖽 all	lo always	🖳 ALL	⊘ 拒否		
Dst Black Rule	SE LAN (port18.vian101)	VIAN (vlan2001.emv1)	🖬 all	🖥 Dst Black list	🖪 always	🖳 ALL	⊘ 拒否		
Src White Rule	SE LAN (port18.vlan101)	VAN (vlan2001.emv1)	🖥 Src White list	😄 all	👩 always	🖳 ALL	✔ 許可	@ 160.248.241.1/32	ssu no-inspection
Dst White Rule	SE LAN (port18.vlan101)	># WAN (vlan2001.emv1)	🖻 all	🐴 Dst White list	🖪 always	I ALL	✔ 許可	160.248.241.1/32	ssu no-inspection
ALL_ICMP	35 LAN (port18.vian101)	36 WAN (vlan2001.emv1)	😑 all	🖾 all	😡 always	ALL_ICMP	✔ 許可	160.248.241.1/32	ssu no-inspection
LAN2	第 LAN (port18.vian101) ポリシー	5§ WAN (vlan2001.emv1)	<ul> <li>⊒ 10.0.0.0/8</li> <li>⊒ 172.16.0.0/12</li> </ul>	🔄 all	😡 always	ALL	✔ 許可	160.248.241.1/32	W default W60 default APP default ss certificate-inspection
LAN3 🖗 📲	設定ステータス 【 名前でフィルタ 凹 コピー	• ◎ 有効 (001.emv1) • ◎ 無効	<ul> <li>□ 10.0.0.0/8</li> <li>□ 172.16.0.0/12</li> <li>□ 192.168.0.0/16</li> </ul>	편 all	la always	I ALL	✔ 許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection
LAN -> WAN	3 ペースト ▶ 空のポリシーを挿入 ▶ シーケンスグルーピングを打	, WAN (vlan 2001.emv1) 事入	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	🔁 all	👩 always	🛛 ALL	✔ 許可	a 160.248.241.1/32	AV default VEB default APP default
暗黙の拒否	<sup>8</sup> 一致するログを表示 ■FortiViewで表示する ✔ 編集	iny	2 all	1 all	👩 always	D ALL	❷ 拒否		so certificate-inspection
<ul> <li>セキュリティレ</li> </ul>	_ CLIで編集 剤 ポリシー削除								<ul> <li>更新済み: 15:36:10</li> </ul>

### III. ルールが無効になっていることを確認する。

TEST-NWUTM-FG01A •	≡ α,								90M: 🗙 user01 • 🛛 >_	
	+新規作成 / 編5	も   ~ cuで編集   密 削	除 Q ポリシーのルック	フアップ 検索			Q	目 エクスボ	ート・ インターフェー	スペアビュー シーケンス別
	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
🛃 ポリシー&オブジェクト 🗸 🗸	NTTPC Monitor Rule	3 LAN (port18.vlan101)	3 WAN (vian 2001.emv1)	100.88.18.0/29	🗉 all	G always	ALL	✔ 許可	9 160.248.241.1/32	334 no-inspection
ファイアウォールポリシー 🏠	Src Black Rule	28 LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	🖥 Src Black list	🗉 all	always	ALL	⊘ 拒否		
アドレス	Dst Black Rule	3 LAN (port18.vlan101)	H WAN (vian2001.emv1)	🖸 all	🖥 Dst Black list	🖬 always	I ALL	⊘ 拒否		
インターネットサービスデ ータベーフ	Src White Rule	) LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	👼 Src Whitelist	🖻 all	🖬 always	ALL	✔ #可	(2) 160.248.241.1/32	sst no-inspection
#	Dst White Rule	35 LAN (port18.vlan101)	38 WAN (vlan 2001.emv1)	🖻 all	🖥 Dst White list	😡 always	ALL	✔ 許可	160.248.241.1/32	ssu no-inspection
バーチャルロ	ALL_ICMP	3E LAN (port18.vlan101)	35 WAN (vlan2001 emv1)	🖾 all	🗉 all	🐼 always	ALL_ICMP	✔ 許可	160.248.241.1/32	sst no-inspection
▲ ヤキュリティプロファイル >	LAN2	28 LAN (po			🖻 all	😡 always	ALL	✔ 許可	160.248.241.1/32	AV default
		× +	がけいてい	わげ						APP default
セキュリティファブリック >		~ /.		1612						ss certificate-inspection
ビログムレポート >	LAN3 🛱	3등 LAN (po	か化されて	いる	🖬 all	😡 always	I ALL	✔ 許可	160.248.241.1/32	44 default
		75.2		0.0						App default
1										m certificate-inspection
	LAN -> WAN Q	28 LAN (port	28 WAN (vlan 2001.emv1)	E 10.0.0.0/8	🗉 all	la always	@ ALL	✔ 許可	160.248.241.1/32	w default
				E 192.168.0.0/16						APP default
										an certificate-inspection
	暗黙の拒否	🗆 any	🗆 any	🔄 all	🖬 all	G always	I ALL	⊘ 拒否		
	<								_	•
	0 セキュリティレーテ	イング問題								🔟 更新済み: 15:36:10 🗘



- 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。

TEST-NWUTM-FG01A -	≡ Q,	-						VD	0M: 💁 user01 • 🔹 🔪	Ø• ↓• ⊖ user01•
🙆 ダッシュポード 🔹 🔸	+新規作成 / 編録	毛 >_ CLIで編集 自 削	除 Q ポリシーのルック	フアップ 検索			Q	■ エクスポ	ート・ インターフェー	スペアビュー シーケンス別
<ul> <li>ホットワーク</li> <li>&gt;</li> </ul>	名前	From	То	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
🗏 ポリシー&オブシェクト 🗸	NTTPC Monitor Rule	35 LAN (port18.vlan101)	35 WAN (vlan2001.emv1)	100.88.18.0/29	🖬 all	la always	I ALL	✔ 許可	160.248.241.1/32	Si no-inspection
ファイアウォールポリシー 合	Src Black Rule	3 LAN (port18.vlan101)	3 WAN (vlan2001.emv1)	🖥 Src Blacklist	🖾 all	lo always	I ALL	⊘ 拒否		
アドレス	Dst Black Rule	38 LAN (port18.vian101)	38 WAN (vlan2001.emv1)	🖻 all	🖥 Dst Black list	always	ALL	⊘ 拒否		
インターネットサービスデ ータベース	Src White Rule	3 LAN (port18.vian101)	38 WAN (vlan2001.emv1)	🖥 Src White list	🗳 all	lo always	ALL	✔ 許可	160.248.241.1/32	ss. no-inspection
#-PZ	Dst White Rule	38 LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	🔄 all	👼 Dst White list	læ always	I ALL	✔ 許可	160.248.241.1/32	ss. no-inspection
バーチャルア	ALL_ICMP	3 LAN (port18.vlan101)	38 WAN (vlan 2001.emv1)	🖻 all	🗉 all	😡 always	ALL_ICMP	✔ 許可	160.248.241.1/32	Si no-inspection
	LAN2	3§ LAN (port18.vlan101)	3§ WAN (vlan 2001.emv1)	<ul> <li>■ 10.0.0.0/8</li> <li>■ 172.16.0.0/12</li> </ul>	🖻 all	😡 always	ALL	✔ 許可	160.248.241.1/32     160.248.241.1/32     160.248.241.1/32     160.248.241.1/32     160.248.241.1/32     160.248.241.1/32     160.248.241.1/32     160.248.241.1/32     160.248.241.1/32     160.248.241.1/32     160.248.241.1/32	We default we default APP default ss. certificate-inspection
■ ログ&レポート >	LAN3 🖗	3등 LAN (port18.vian101)	38 WAN (vlan 2001. emv1)	<ul> <li>☐ 10.0.0.0/8</li> <li>☐ 172.16.0.0/12</li> <li>☐ 192.168.0.0/16</li> </ul>	🔄 all	læ always	2 ALL	✔ 許可	160.248.241.1/32     160.248.241.1/32	AV default WE default APP default SSL certificate-inspection
	LAN -> WAN 🍪	38 LAN (port18.vian101)	38 WAN (vlan2001.emv1)	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	🖸 all	😡 always	I ALL	✔ 許可	160.248.241.1/32	W default W0 default APP default SX certificate-inspection
	暗黙の拒否	🗆 any	🗆 any	🖻 all	🖬 all	lo always	I ALL	⊘ 拒否		
									_	•
	0 セキュリティレーテ	ィング問題								15:36:10 2

#### III. 確認画面が表示されるので OK を押下する。

≡ Q.									💁 user01 🕶		<b>8</b> - 1		\rm 🛛 user01
★新規作成 ● 編集	匙 >= cuで編集 🗋 首 削	除 Q ポリシーのルック				Q	確認						×
名前	From	То	送信元	宛先	スケジュール	サービス	▲ 選択	Rした polici	iesを削除して	もよろし	<i>,</i> いですか	i?	
NTTPC Monitor Rule	38 LAN (port18.vlan101)	38 WAN (vlan2001.emv1)		🗉 all	😡 always	🗷 ALL							
Src Black Rule	3% LAN (port18.vlan101)	₩ WAN (vlan2001.emv1)	覆 Src Blacklist	🗉 all	😡 always	I ALL							
Dst Black Rule	35 LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	🗉 all	覆 DstBlacklist	😡 always	🖳 ALL							
Src White Rule	38 LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	疆 Src White list	🖽 all	👩 always	🖳 ALL							
Dst White Rule	38 LAN (port18.vlan101)	3§ WAN (vlan2001.emv1)	😑 all	覆 DstWhitelist	👩 always	🖳 ALL							
ALL_ICMP	🧏 LAN (port18.vlan101)	95 WAN (vlan2001.emv1)	🗐 all	🗉 all	😡 always	ALL_ICM							
LAN2	25 LAN (port18.vlan101)	35 WAN (vlan2001.emv1)	달 10.0.0.0/8 달 172.16.0.0/12	聖 all	😡 always	I ALL							
LAN3 🗘			<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	🔄 all	😡 always	I ALL							
Lân -> Wan 🕄			<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	i all	😡 always	I ALL							
暗黙の拒否	🗆 any	🗆 any	🗉 all	🖽 all	👩 always	I ALL							
○ セキュリティレーテ・	イング問題				<u>.</u>				ок	+	ャンセル		



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。
		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
16	セキュリティプロファイ ル	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		許可トラフィックをログ : す べてのセッション	
17	4777777737	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。

TEST-NWUTM-FG01A -									OM: 🙆 user01 🕶	>_ ଡ- ⊅-	😝 user01 -
🙆 ダッシュボード 🔹 🕨	+新規作成 ✔ 編	実 ン_ CLIで編集	自 削除 Q 7	ペリシーのルックア	<b>ップ</b> 検索			Q 🗟 エクスポ	ート・ インター	フェースペアビュー 🗦	レーケンス別
<ul> <li>キャットワーク</li> <li>&gt;</li> </ul>	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
🖹 ポリシー&オブジェクト 🔹 🗸	🖃 🕫 LAN (port18.vla	n 101) → 35 WAN (vla	n2001.emv1) 🧭								
ファイアウォールポリシー 🏠	NTTPC Monitor Rule	100.88.18.0/29	🖻 all	😡 always	I ALL	✔ 許可	@ 160.248.241.1/32	ss. no-inspection	😝 無効化済み	ОB	スタンダ・
アドレス	Src Black Rule	👼 Src Blacklist	🗉 all	😡 always	I ALL	⊘ 拒否			すべて	0 B	スタンダ・
インターネットサービスデ ータベーフ	Dst Black Rule	🖾 all	🖥 Dst Black list	lo always	I ALL	⊘ 拒否			すべて	ов	スタンダ・
+	Src White Rule	疆 Src White list	🖬 all	🐼 always	I ALL	✔ 許可	160.248.241.1/32	ss. no-inspection	すべて	ов	スタンダ・
ノ こへ バーチャルロ	Dst White Rule	😑 all	👼 Dst White list	😡 always	I ALL	✔ 許可	160.248.241.1/32	ss. 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	ss. no-inspection	🛛 すべて	ОB	スタンダ・
<ul> <li>➡ SAFA</li> </ul>	LAN -> WAN	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> </ul>	🖻 all	😡 always	😰 ALL	✔ 許可	160.248.241.1/32	AV default WEB default	🙂 রুশ্বে	ОB	スタンダ・
🧔 セキュリティファブリック ゝ		ポリシー						APP default			
■ ログ&レポート >	設定ス	テータス・						xx certificate-inspection			
	▼名前	iでフィルター・									
	@ ⊐Ŀ	-									
	<b>B</b> ~-	·z ·	▲ 上へ								
	<b>-</b> 空전	ホリシーを挿入 ・	* 下へ								
	龍一致	するログを表示									
	🛎 Fort	iViewで表示する									
	♂ 編集	i									
	>_ CLI	で編集		_	_	_					-
	o セキュリティレーク	シー削除 								📵 更新済み:1	6:03:04



# ④ 作成したポリシーをダブルクリックする。

TEST-NWUTM-FG01A 🔹	≡ Q.							VD	OM: 💁 user01 🔹	≻ <b>_ 0</b> • ∴•	<b>e</b> user01 •
🙆 ダッシュボード 🔹 🔉	+新規作成 🖌 編集	ミ >_ CLIで編集	● 削除 Q 7	ポリシーのルックア	<b>ッ</b> プ 検索			Q 目 エクスポ	ート・ インター	フェースペアビュー 💈	ーケンス別
<ul> <li></li></ul>	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
🖹 ポリシー&オブジェクト 🛛 🗸	🖃 💃 LAN (port18.vlar	101)	12001.emv1) 🛞								
ファイアウォールポリシー 🏠	NTTPC Monitor Rule	100.88.18.0/29	🖸 all	😡 always	I ALL	✔ 許可	160.248.241.1/32	ssu no-inspection	😝 無効化済み	0 B	スタンダ・
	Src Black Rule	🖥 Src Blacklist	🖽 all	👩 always	😰 ALL	⊘ 拒否			<ul> <li>すべて</li> </ul>	ОB	スタンダ・
インターネットサービスデ ータベーフ	DstBlackRule	🖻 all	👼 Dst Black list	😡 always	🖪 ALL	⊘ 拒否			すべて	ОB	スタンダ・
+=ビ7	Src White Rule	🖥 Src White list	🖾 all	🕼 always	😰 ALL	✔ 許可	160.248.241.1/32	sst no-inspection	◎ すべて	ОB	スタンダ・
	Dst White Rule	🖻 all	👼 Dst White list	👩 always	I ALL	✔ 許可	160.248.241.1/32	ssu 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	ssu no-inspection	すべて	ОB	スタンダ・
	0	<ul> <li>■ 10.0.0.0/8</li> <li>■ 172.16.0.0/12</li> <li>■ 192.168.0.0/16</li> </ul>	🖳 all	🕢 always	ALL	✔ 許可	160.248.241.1/32	AV default ViE default APP default SE certificate-inspection	🕲 রুশ্বে	1.41MB	- スタンダ・
	LAN -> WAN	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>		🐱 always	🖳 ALL	✔ 許可	160.248.241.1/32	AV default WE default APP default SL certificate-inspection	🕏 র্বে	ов	スタンダ・
	田 ::::::::::::::::::::::::::::::::										
	4									<ul> <li>         か雨(+炭友之か)     </li> </ul>	= .1°. ¥
	○ セキュリティレーティ	ィング問題								BERGARIT CIT	

Master'sONE°

45

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。

※IF シールが SNAF のアドレス設定になりよりので追加ウローバル IF 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 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.vlar	101) → 38 WAN (vlar	12001.emv1) 🤊								
NTTPC Monitor Rule	100.88.18.0/29	😐 all	👩 always	🖳 ALL	✔ 許可	160.248.241.1/32	ssu no-inspection	😂 無効化済み	oв	スタンダ・
Src Black Rule	👼 Src Black list	😐 all	👩 always	🖳 ALL	⊘ 拒否			🗢 すべて	0.8	スタンダ・
Dst Black Rule	🖾 all	😼 Dst Black list	😡 always	I ALL	⊘ 拒否			🗢 すべて	0.8	スタンダ・
Src White Rule	🍓 Src White list	🖻 all	😡 always	🖳 ALL	✔ 許可	160.248.241.1/32	ssu no-inspection	🗢 すべて	0 B	スタンダ・
Dst White Rule	🖬 all	👼 Dst White list	🗔 always	🖳 ALL	✔ 許可	160.248.241.1/32	ssu 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	ssu no-inspection	🗢 すべて	0.8	スタンダ・
8	<ul> <li>□ 10.0.0.0/8</li> <li>□ 172.16.0.0/12</li> <li>□ 192.168.0.0/16</li> </ul>	🔄 all	👩 always	I ALL	✔ 許可	(a) 160.248.241.1/32	AV default WEB default APP default SL certificate-inspection	⊘ すべて	OB	スタンダ・
SNAT 🖗	<ul> <li>■ 100.0.0/8</li> <li>■ 112.16.0.0/12</li> <li>▼ 192.168.0.0/16</li> </ul>	🔄 all	👩 always	I ALL	✔ 許可	ⓐ 160.248.241.1/32	AV default WEB default APP default SL certificate-inspection	♥ すべて	ОB	スタンダー
LAN -> WAN	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	🔁 all	🖪 always	I ALL	✔ 許可	160.248.241.1/32	AV default WEB default APP default SL certificate-inspection	🕏 র্শবে	1.64 MB	スタンダ・
田 ::::::::::::::::::::::::::::::::										
0 セキュリティレーテ	イング問題								の 更新済み	16:27:26
0 21 20010 0	1.5.5.000								SOB10407.	10.27.20 V

### 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。

TEST-NWUTM-FG01A +	≡ Q							VD	OM: ❹ user01 •	≻ <b>_ 0</b> • ¢•	<b>9</b> user01 -
🙆 ダッシュボード 🔹 🔉	+新規作成	編集 >_ CLIで編集	會 削除 🔍 7	ポリシーのルックア	マップ 検索			Q 目 エクスポ	ート・ インター	フェースペアビュー シ	ーケンス別
<ul> <li>         キットワーク      </li> </ul>	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	ノバイト	タイプ
💄 ポリシー&オブジェクト 🗸 🗸	🖃 🔏 LAN (port18	vlan101) → 35 WAN (vla	n2001.emv1) 🥑								
ファイアウォールポリシー ☆	NTTPC Monitor R	ule 🔄 100.88.18.0/29	🖻 all	👩 always	I ALL	✔ 許可	160.248.241.1/32	ssu no-inspection	😡 無効化済み	oв	スタンダ・
アドレス	Src Black Rule	👼 Src Black list	🗉 all	👩 always	ALL	⊘ 拒否			すべて	ОB	スタンダ・
インターネットサービスデ ータベーフ	Dst Black Rule	😑 all	🖥 Dst Black list	😡 always	I ALL	⊘ 拒否			すべて	0 B	スタンダ・
+	Src White Rule	👼 Src Whitelist	🖬 all	😡 always	I ALL	✔ 許可	160.248.241.1/32	ss. no-inspection	🗢 すべて	0 B	スタンダ・
ノーモヤルロ	Dst White Rule	😑 all	👼 Dst White list	👩 always	I ALL	✔ 許可	160.248.241.1/32	ss. no-inspection	すべて	1.15 MB	スタンダ・
	ALL_ICMP	🖾 all	😑 all	👩 always	ALL_ICMP	✔ 許可	(2) 160.248.241.1/32	ss. no-inspection	🕏 すべて	ОВ	スタンダ・
	SNAT 😡	<ul> <li>□ 10.0.0.0/8</li> <li>□ 172.16.0.0/12</li> <li>□ 192.168.0.0/16</li> <li>ポリシー</li> </ul>	E all	👩 always	I ALL	✔ 許可	இ 160.248.241.1/32	default vre default APP default ss certificate-inspection	🛛 রুশ্বে	oв	スタンダ・
	© 12: ▼ අ	をステータス ・ 名前でフィルタ ・ コピー	<ul> <li>● 有効</li> <li>○ 訊効</li> </ul>	👩 always	I ALL	✔ 許可	ⓐ 160.248.241.1/32	AV default VCO default APP default SSL certificate-inspection	🕏 রন্দে	ОB	スタンダ・
	LAN->WAN +	ペースト , 空のポリシーを挿入 , 一致するログを表示	\Xi all	😡 always	ALL	✔ 許可	160.248.241.1/32	AV default WE0 default APP default SSL certificate-inspection	🕏 র্শবে	1.64 MB	■ スタンダ・
		FortiViewで表示する 編集 CLIで編集									
	○ セキュリテ 竜	ポリシー削除								10 更新済み:16	27:26



⑧ ルールが有効になったことを確認する。

TEST-NWUTM-FG01A •	≡ Q.							VD	OM: 💁 user01 •	> <b>_ 0 •</b> ∴ •	😝 user01 🗸
Ø ダッシュボード >	+新規作成 @ 編\$	嵬 >_ CLIで編集	歯 削除 🔍 🕽	ポリシーのルックア	アップ 検索			Q 🗎 エクスポ	ート・ インター	フェースペアビュー 💈	レーケンス別
	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	タイプ
💄 ポリシー&オブジェクト 🗸 🗸	🖃 🗏 LAN (port18.vlar	n 101) → <b>35</b> WAN (vlar	12001.emv1) 🥑								
ファイアウォールポリシー 合	NTTPC Monitor Rule	🗉 100.				✔ 許可	160.248.241.1/32	ssu no-inspection	😡 無効化済み	0 B	スタンダ・
アドレス	Src Black Rule	≣ Src B v th	ジョティー	んげちか		⊘ 拒否			🛛 すべて	0B	スタンダ・
インターネットサービスデ ータベース	Dst Black Rule		いれんしい	いいより刈		⊘ 拒否			すべて	0 B	スタンダ・
#-F2	Src White Rule	<sup>≣ Src V</sup> 化力	ちれている			✔ 許可	160.248.241.1/32	ssu no-inspection	♥ すべて	0 B	スタンダ・
バーチャルア	Dst White Rule		.1000	,		✔ 許可	(2) 160.248.241.1/32	ssi no-inspection	🕏 すべて	1.15 MB	スタンダ・
▲ セキュリティプロファイル <b>&gt;</b>	ALL_ICMP	🗉 all			_ICMP	✔ 許可	160.248.241.1/32	ssu no-inspection	◎ すべて	0 B	スタンダ・
•         •           •         •	SNAT	<ul> <li>□ 10.01</li> <li>□ 172.16.0.0/12</li> </ul>	🚍 all	😡 always	ALL	✔ 許可	160.248.241.1/32	AV default WEB default	🗢 すべて	ОB	スタンダ・
		192.168.0.0/16						APP default sst certificate-inspection			
	0	<ul> <li>□ 10.0.0.0/8</li> <li>□ 172.16.0.0/12</li> <li>□ 192.168.0.0/16</li> </ul>	Ξ all	😡 always	R ALL	✔ 許可	ⓐ 160.248.241.1/32	AV default WEP default APP default SL certificate-inspection	すべて	ОВ	スタンダ・
	LAN -> WAN	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	🔄 all	🕡 always	😰 ALL	✔ 許可	160.248.241.1/32	AV default WEP default APP default SSL certificate-inspection	🕏 すべて	1.64 MB	スタンダ・
	∃ 暗黙 1										
	○ セキュリティレーテ	ィング問題								保存されました。 <u>101</u> 5	. ×

- 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。

TEST-NWUTM-FG01A +	≣ Q,									VDOI	M: ❹ user01 • >_	Ø• ↓• ⊕ user01•
🙆 ダッシュボード 🔹 🔸	+新規作成	✔ 編集	>_ CLIで編集	<b>自</b> 削降		アップ 検索			Q	目 エクスポー	ト・ インターフェー	スペアビュー シーケンス別
♣ ネットワーク	名前		From		То	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
💄 ポリシー&オブジェクト 🗸 🗸	NTTPC Moni	itor Rule	S LAN (port18.)	lan101)	3 WAN (vian2001.emv1)	100.88.18.0/29	🖻 all	😡 always	🗷 ALL	✔ 許可	160.248.241.1/32	ssu no-inspection
ファイアウォールポリシー 🌣	Src Black Rul	le	3€ LAN (port18.v	lan101)	35 WAN (vlan 2001.emv1)	🖥 Src Blacklist	🖽 all	😡 always	🛛 ALL	⊘ 拒否		
アドレス	Dst Black Ru	le	DE LAN (port18.)	lan 101)	SE WAN (vlan2001.emv1)	😑 all	🖥 Dst Black list	🕫 always	I ALL	⊘ 拒否		
インターネットサービスデ ータベース	Src White Ru	le	35 LAN (port18.)	lan101)	35 WAN (vlan2001.emv1)	🖥 Src White list	😑 all	😡 always	🖳 ALL	✔ 許可	160.248.241.1/32	ssu no-inspection
サービス	Dst White Ru	ıle	CAN (port18.)	lan 101)	₩AN (vlan2001.emv1)	😐 all	霫 Dst White list	😡 always	🖳 ALL	✔ 許可	160.248.241.1/32	ss. no-inspection
バーチャルル	ALL_ICMP		35 LAN (port18.v	lan101)	3 WAN (vlan 2001.emv1)	🗐 all	🖻 all	😡 always	ALL_ICMP	✔ 許可	160.248.241.1/32	ss no-inspection
🔒 セキュリティプロファイル ゝ	任意		3€ LAN (port18.v	lan101)	3 WAN (vlan2001.emv1)	172.16.0.0/12	🖻 all	😡 always	😰 ALL	✔ 許可	160.248.241.1/32	ssu no-inspection
	user-defined	-policy-1	1 LAN (port18) #LLS	an101)	> WAN (vlan 2001.emv1)	172.16.0.0/12	😫 all	😡 always	🖳 ALL	✔ 許可	(2) 160.248.241.1/32	SSL no-inspection
セキュリティファブリック     ・      ・     ・      ・      ・      ・      ・      ・      ・      ・      ・      ・      ・      ・      ・      ・      ・      ・      ・      ・     ・      ・	LAN -> WAN	10中 7日			35 WAN (vlan 2001.emv1)	10.0.0.0/8	🖻 all	😡 always	🖳 ALL	✔ 許可	160.248.241.1/32	W default
■ログ&レポート >		▼ 名前 :	でフィルタ			92.168.0.0/16						APP default
		むコピ-	-		_							ss certificate-inspection
	暗黙の拒否	16 ×->	スト	•	🗆 any	🖃 all	🖻 all	😡 always	I ALL	⊘ 拒否		
		+ 空の7	ポリシーを挿入	•								
		+ 2-3	テンスグルーピング	を挿入								
		龍一致す	るログを表示									
		🛎 FortiV	iewで表示する									
	-	>_ CU 7	編集								-	•
	○ セキュリテ	自 ポリ:	シー削除									11) 更新済み: 16:38:29 📿

### 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。

TEST-NWUTM-FG01A 🔹	≡ Q.							VDOI	M: 🔹 user01 • 🛛 >_	<b>3</b> • ↓ • <b>9</b> user01 •
🙆 ダッシュボード 🔹 🔉	+新規作成 🖌 編集	E >_ CLIで編集 自	劉除 Q ポリシーのルック	アップ 検索			Q	■ エクスポー	ト・ インターフェー	スペアビュー シーケンス別
<ul> <li>キャットワーク</li> <li>・</li> </ul>	名前	From	То	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
💄 ポリシー&オブジェクト 🗸 🗸	NTTPC Monitor Rule	😹 LAN (port18.vlan10	I) 38 WAN (vlan 2001.emv1)	100.88.18.0/29	🗐 all	😡 always	🖳 ALL	✔ 許可	160.248.241.1/32	ss. no-inspection
ファイアウォールポリシー 🏠	Src Black Rule	5 LAN (port18.vlan10	I) 35 WAN (vlan 2001.emv1)	👼 Src Black list	🖾 all	👩 always	I ALL	⊘ 拒否		
アドレス	Dst Black Rule	😹 LAN (port18.vian10	I) 38 WAN (vlan 2001.emv1)	🖽 all	👼 Dst Black list	🖬 always	I ALL	⊘ 拒否		
インターネットサービスデ ータベース	Src White Rule	😹 LAN (port18.vlan10	I) 35 WAN (vlan 2001.emv1)	👼 Src White list	🖾 all	🖬 always	I ALL	✔ 許可	160.248.241.1/32	ssu no-inspection
#_PZ	Dst White Rule	😹 LAN (port18.vlan10	i) 38 WAN (vlan2001.emv1)	🖻 all	看 Dst White list	🖬 always	I ALL	✔ 許可	160.248.241.1/32	ss. no-inspection
バーチャルア	ALL_ICMP	😹 LAN (port18.vlan10	i) 35 WAN (vlan2001.emv1)	😑 all	🖾 all	😡 always	ALL_ICMP	✔ 許可	160.248.241.1/32	ss no-inspection
A ヤキュリティプロファイル >	任意	😹 LAN (port18.vlan10	I) 35 WAN (vlan2001.emv1)	172.16.0.0/12	🖽 all	👩 always	I ALL	✔ 許可	160.248.241.1/32	ss. no-inspection
	user-defined-poli		WAN (vlan 2001.emv1)	172.16.0.0/12	😑 all	🖬 always	😰 ALL	✔ 許可	160.248.241.1/32	ssi no-inspection
◆ フィンス ② セキュリティファブリック → 巴 ログ&レポート →	LAN -> WAN 設加 で	ホッシン ミステータス 名前 でフィルタ コピー	WAN (vlan 2001.emv1)	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	E all	🕢 always	I ALL	✔ 許可	160.248.241.1/32	W     default       WEE     default       APP     default       SSL     certificate-inspection
	暗黙の拒否	ペースト	· • FV	🗉 all	🗉 all	🖬 always	ALL	⊘ 拒否		
	+ + B- 2	空のボリシーを挿入 シーケンスグルーピング 一致するログを表示 FortiViewで表示する 編集 Culで編集 ポリミー 細味	* 下へ						-	•
	○ セキュリティレーテ									🔟 更新済み: 16:38:29 🖸



## ④ 作成したポリシーをダブルクリックする。

TEST-NWUTM-FG01A -	≡ Q							VDO	M: 💁 user01 • 🛛 >_	
🙆 ダッシュボード 🔹 🔉	+新規作成 🥒 編集	- CLIで編集  首 削加	Q ポリシーのルック	アップ 検索			Q	■ エクスポー	ト・インターフェー	スペアビュー シーケンス別
ホットワーク >	名前	From	То	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
💄 ポリシー&オブジェクト 🗸 🗸	NTTPC Monitor Rule	3 LAN (port18.vlan101)	3 WAN (vlan2001.emv1)	100.88.18.0/29	😫 all	la always	🗷 ALL	✔ 許可	160.248.241.1/32	ss no-inspection
ファイアウォールポリシー 🏫	Src Black Rule	SE LAN (port18.vian101)	58 WAN (vlan2001.emv1)	🖥 Src Black list	🖬 all	always	I ALL	⊘ 拒否		
アドレス	Dst Black Rule	3 LAN (port18.vlan101)	SE WAN (vlan2001.emv1)	🗐 all	🖥 Dst Black list	😡 always	I ALL	⊘ 拒否		
インターネットサービスデ ータベース	Src White Rule	35 LAN (port18.vlan101)	3€ WAN (vlan2001.emv1)	👼 Src White list	🖴 all	lo always	😰 ALL	✔ 許可	160.248.241.1/32	ssu no-inspection
#-PZ	Dst White Rule	) LAN (port18.vlan101)	3€ WAN (vlan2001.emv1)	🗄 all	🖥 Dst White list	🖬 always	I ALL	✔ 許可	160.248.241.1/32	ss no-inspection
バーチャルP	ALL_ICMP	3 LAN (port18.vian101)	35 WAN (vlan2001.emv1)	🖹 all	🗄 all	😡 always	ALL_ICMP	✔ 許可	160.248.241.1/32	ssu no-inspection
▲ セキュリティプロファイル <b>&gt;</b>	任意	35 LAN (port18.vian101)	3€ WAN (vlan2001.emv1)	172.16.0.0/12	😫 all	👩 always	😰 ALL	✔ 許可	160.248.241.1/32	ssu no-inspection
	0	35 LAN (port18.vlan101)	3€ WAN (vlan2001.emv1)	172.16.0.0/12	🖻 all	🖬 always	🛛 ALL	✔ 許可	160.248.241.1/32	ss. no-inspection
セキュリティファブリック     ・      ・     ・     ・     ・     ・     ・      ・     ・     ・      ・      ・     ・      ・      ・	user-defined-policy-1	35 LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	172.16.0.0/12	🖻 all	🖬 always	I ALL	✔ 許可	160.248.241.1/32	ss. no-inspection
<ul><li>ビログ&amp;レポート &gt;</li></ul>	LAN-> WAN	35 LAN (port18.vlan191)	58 WAN (vlan 2001.emv1)	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	n all	👩 always	🖳 ALL	✔ 許可	160.248.241.1/32	AV default VEB default APP default SSL certificate-inspection
	暗黙の拒否	🗆 any	🗆 any	🖻 all	🖻 all	🕼 always	I ALL	⊘ 拒否		
										•
	○ セキュリティレーティ	ング問題								🗊 更新済み: 16:38:29 📿



 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



Copyright (c) 2024 NTT PC Communications Incorporated, All Right Reserved.

50



## 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	То	送信元	宛先	スケジュー	サービス	アクショ	NAT
NTTPC Monitor R	💥 LAN (port18.vlan1	💥 WAN (vlan2001.em	100.88.18.0/29	📃 all	🐻 always	😰 ALL	✔ 許可	(a) 160.248.241.1/32
Src Black Rule	꽤 LAN (port18.vlan1	14 WAN (vlan2001.em	🚡 Src Black list	💷 all	🖪 always	🖬 ALL	❷ 拒否	
Dst Black Rule	ዡ LAN (port18.vlan1	1 WAN (vlan2001.em	📃 all	疆 Dst Black I	🐻 always	🖪 ALL	⊘ 拒否	
Src ₩hite Rule	⊯ LAN (port18.vlan1	ዡ WAN (vlan2001.em	🚡 Src White list	🔲 all	🐻 always	д ALL	✔ 許可	(2) 160.248.241.1/32
Dst White Rule	꽤 LAN (port18.vlan1	꽤 WAN (vlan2001.em	🔄 all	🖥 Dst White	🖪 always	🖪 ALL	✔ 許可	@ 160.248.241.1/32
ALL_ICMP	💥 LAN (port18.vlan1	1 WAN (vlan2001.em	📃 all	🔲 all	🐻 always	ALL_IC	✔ 許可	@ 160.248.241.1/32
任意	🗯 LAN (port18.vlan1	꽤 WAN (vlan2001.em	⊒ 172.16.0.0/12	🖻 all	🖬 always	🛛 ALL	✔ 許可	(2) 160.248.241.1/32
任意10	ා표 LAN (port18.vlan1	₩AN (vlan2001.em	172.16.0.0/12	🗐 all	🖪 always	🔲 ALL	✔ 許可	(a) 160.248.241.1/32
user-defined-polic	꽤 LAN (port18.vlan1	꽤 WAN (vlan2001.em	⊒ 172.16.0.0/12	🗉 all	🖪 always	🛛 ALL	✔ 許可	(a) 160.248.241.1/32
LAN -> WAN	꽤 LAN (port18.vian1	3를 WAN (vlan2001.em	<ul> <li>10.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	遭 all	🐻 always	д ALL	✔ 許可	(a) 160.248.241.1/32
暗黙の拒否	🗆 any	🗆 any	🗉 all	🗉 all	🖸 always	ALL ALL	⊘ 拒否	
								Þ
0 セキュリティレーティ	ング問題						11 5	更新済み: 17:01:42 오

### 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	То	送信元	宛先	スケジュー	サービス	アクショ	NAT
NTTPC Monitor	R 🏦 LAN (port18.vlan1	먦 WAN (vlan2001.em	100.88.18.0/29	💷 all	🐻 always	😡 ALL	✔ 許可	B 160.248.241.1/32
Src Black Rule	꽤 LAN (port18.vlan1	왜 WAN (vlan2001.em	🚡 Src Black list	🖽 all	🐻 always	🛛 ALL	⊘ 拒否	
Dst Black Rule	3를 LAN (port18.vlan1	ዡ WAN (vlan2001.em	🗉 all	😼 Dst Black I	🐻 always	🖪 ALL	⊘ 拒否	
Src White Rule	₩ LAN (port18.vlan1	೫ WAN (vlan2001.em	🚡 Src White list	💷 all	🐻 always	🖪 ALL	✔ 許可	160.248.241.1/32
Dst White Rule	ポリシー	WAN (vlan2001.em	🗉 all	ବ Dst White	🐻 always	🛛 ALL	✔ 許可	160.248.241.1/32
ALL_ICMP	設定 ステータス	▶ ◎ 有効	🗉 all	🖽 all	🐻 always	ALL_IC	✔ 許可	160.248.241.1/32
任意18	▼ 名前 でフィルタ	◆ 日初 ◆ ② 無効 <sup>2001.em…</sup>	172.16.0.0/12	📃 all	d always	🛛 ALL	✔ 許可	160.248.241.1/32
任意	砲 ⊐ピー	WAN (vlan2001.em	⊒ 172.16.0.0/12	🗉 all	🐻 always	🕼 ALL	✔ 許可	160.248.241.1/32
user-defined-pol	■ へースト ● 空のポリシーを挿入	WAN (vlan2001.em	172.16.0.0/12	💷 all	🖪 always	🖪 ALL	✔ 許可	(a) 160.248.241.1/32
LAN -> WAN	<ul> <li>▲ シーケンスグルーピングを排</li> </ul>	挿入 WAN (vlan2001.em	<ul><li>10.0.0/8</li><li>172.16.0.0/12</li></ul>	🗉 all	🖪 always	😰 ALL	✔ 許可	160.248.241.1/32
	間一致するログを表示		192.168.0.0/16					
	I■ FortiViewで表示する							
暗黙の拒否	✔ 編集	any	🔳 all	🗏 all	🐻 always	🚇 ALL	❷ 拒否	
-	>_ CLIで編集							Þ
0 セキュリティレー	◎ ポリシー削除						11 5	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。

TEST-NWUTM-FG01A	- ≡ Q					VI	DOM: 🐽 user0	91 <b>• &gt;_ ()</b>	• 🗘 • 🕒 user01 •
	◆新規作成 》 編創		除 Q ポリシーのルック	クアップ 検索			Q		
	■ エクスポート・	インターフェースペアビュ	ー シーケンス別						
▶ ポリシー&オブジェクト 、	名前	From	То	送信元	宛先	スケジュー	サービス	アクショ	NAT
ファイアウォールポリシ ー	NTTPC Monitor R	DB		100.88.18.0/29	🔲 all	🐻 always	🖬 ALL	✔ 許可	(a) 160.248.241.1/32
アドレス	Src Black Rule	🔹 ×が消えて	いれば有効	🐴 Src Black list	🖽 all	🐻 always	ALL	⊘ 拒否	
インターネットサービス	Dst Black Rule	DE	_	💷 all	璮 Dst Black I	🐻 always	D ALL	❷ 拒否	
データベース	Src White Rule	🦼 化されてい	<sub>ି</sub> ବ	壇 Src White list	💷 all	🐻 always	D ALL	✔ 許可	(a) 160.248.241.1/32
サービス	Dst White Rule	DB		🖾 all	훰 Dst White	🐻 always	🖬 ALL	✔ 許可	(a) 160.248.241.1/32
バーチャルIP	ALL_ICMP	DF	₩AN (vlan2001.em	💷 all	💷 all	👩 always	ALL_IC	✔ 許可	(a) 160.248.241.1/32
● <sup>セキュリティプロファイ</sup> 、	任意1	₩ LAN (port18.vian1	₩ WAN (vian2001.em	172.16.0.0/12	🖫 all	🐻 always	😡 ALL	✔ 許可	160.248.241.1/32
<ul><li>システム</li></ul>	任意	꽤 LAN (port18.vlan1	p∄ WAN (vlan2001.em	172.16.0.0/12	💷 all	🐻 always	🖪 ALL	✔ 許可	(a) 160.248.241.1/32
セキュリティファブリッ     ク     ク	user-defined-polic	₩ LAN (port18.vlan1	1월 WAN (vlan2001.em	172.16.0.0/12	💷 all	🐻 always	ALL .	✔ 許可	160.248.241.1/32
 ■ ログ&レポート	LAN -> WAN	D≣ LAN (port18.vian1	D≣ WAN (vian2001.em	<ul> <li>10.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	遭 all	🐻 always	D ALL	✔ 許可	<sup>(a)</sup> 160.248.241.1/32 <sup>(b)</sup>
	暗黙の拒否	O any	🗆 any	🔲 all	🔲 all	🐻 always	🛛 ALL	❷ 拒否	
	0 セキュリティレーティ 7	ング問題						<b>m</b>	更新済み: 17:01:42 🖸



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。



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。

TEST-NWUTM-FG01A 🔹	≣ Q						HA:	プライマリ VDOM: 🌢 น	ser01 • >_ (	9 • 🗘 • \varTheta admin •
🙆 ダッシュボード 🔹 🔹	◆新規作成 🖋 編集	> CLIで編集	削除	Q ポリシーのル・	ックアップ 検討	穀		Q 🖹 エクスポート・	インターフェースペ	アピュー シーケンス別
⊕ ネットワーク     →	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
ファイアウォールポリシ 🔥	Src White Rule	🖷 Src White list	🔳 all	lo always	D ALL	✔ 許可	(@ 160.248.241.1/32	ssu no-inspection	<ul> <li>কুর্বের্টের বিশ্ব বিশ্</li></ul>	0 B
	Dst White Rule	🔄 all		lo always	ALL ALL	✔ 許可		ss. no-inspection	⊙ すべて	0 B
認証ルール	ALL_ICMP	🗐 all	🔳 all	lo always	ALL_ICMP	✔ 許可	@ 160.248.241.1/32	55L no-inspection	◎ すべて	20.88 kB
ZTNA	LAN -> WAN	10.0.0/8	💻 all	o always	ALL ALL	✔ 許可	160.248.241.1/32	AV default	⊘ すべて	2.78.GB
インターネット サービス データベース		172.16.0.0/12 192.168.0.0/16						WEB default		
サービス		<b>E</b> 400.470.0.0747	H			A 10/17	@ 4/0 040 044 4/00	ssc certificate-inspection	A 12.17	
スケジュール	test	≦ 192.168.0.0/16	Se all	Lo always	W ALL	▼ 計円	₩ 160.248.241.1/32	certificate-inspection	0 9 ~ C	0.B
バーチャルル	dnat test 😒	192.168.0.0/16	le test	lo always	ALL ALL	✔ 許可	160.248.241.1/32	ss. no-inspection	◎ すべて	0 B
IPプール	192.168.0.0/24 permit 😂	192.168.0.0/16	🗐 all	to always	I ALL	✔ 許可	@ 160.248.241.1/32	AV test	◎ すべて	0 B
プロトコルオプション								st certificate-inspection		
トラフィックシェイピン	🖃 🇯 WAN (vlan2001.emv	1) → 🏙 LAN (port18.)	vlan101) (	1						
→ セキュリティプロファイ 、 ル	DNAT	Ø none	test	👩 always	ALL	✔ 許可	◎ 無効化済み	AV default	⊘ すべて	69.15 kB
💄 ユーザ & 認証 🔹 💙								sst certificate-inspection		
♥ WiFi&スイッチコントロ > -ラー								· · · ·		
FERTINET V7.2.7	0 セキュリティレーティング	何問題							58% 🖽	更新済み: 15:45:26 2



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。

TEST-NWUTM-FG01A 🔹	≡ Q.			HA: プライマリ	VDOM: 💁 user01 🕶	>_ 🕜 -	4 - 🛛 admin	-
🙆 ダッシュボード 🔉 🕻	ポリシーの編集							
💠 ネットワーク 💦 👌				統計情報(最終リセット以	降)			
💄 ポリシー&オブジェクト 🗸	名前 🚯	DNAT		ID	13			I
ファイアウォールポリシ _	タイプ	スタンダード ZTNA		最後の利田	3日前			I
波証 ルール	着信インターフェース	Die WAN (vlan2001.emv1)		最初の利用	3日前			I
	発信インターフェース	滩 LAN (port18.vlan101)	,	アクティブセッション	0			I
ZTNA	送信元	Ø none >	1	アンティンピッション	10			I
インターネット サービス	IP/MACベースアクセスコントロール 🜖	+	4	総バイト数	69.15 kB			
テーダベースサービス	宛先	lest >	t i i i i i i i i i i i i i i i i i i i	現在の帯域	0 bps			
スケジュール	スケジュール	+		童 カウンタをクリア				
バーチャルIP	サービス	ALL >		B 77776777				
IPプール		+		7日前 パイト・				
プロトコルオプション	アクション	✓ 許可 Ø 拒否		100 kB			_	
トラフィックシェイピン グ	インスペクションモード フローベース	プロキシベース		80 kB	.lı nTurbo .lı SPU	J .lı Software	_	
● <sup>セキュリティプロファイ</sup> →	ファイアウォール/ネットワークオプション	,		40 kB				
💄 ユーザ&認証 🔹 🔸	NAT 🕕			20 kB				
♥ WiFi&スイッチコントロ ーラー	プロトコルオプション PROT g-default	- 1		ОВ	<u>+</u> +			_
			OK キャンセル	]				

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。

TEST-NWUTM-FG01A 🔹	≡ Q.			HA: 7	プライマリ	VDOM: 🕹 user01 🔹	≻_ ଡ•	🗘 🔹 🤨 admin 🔹
🙆 ダッシュボード 🔹 🕨	ポリシーの編集							
🕂 ネットワーク 💦 💙			エントリを選択 🗙	統計情報()	最終リセット以	(降)		I
💄 ポリシー&オプジェクト 🗸	名前 🕄	DNAT	アドレス ユーザ インターネットサート					
ファイアウォールポリシ 	タイプ	スタンダード ZTNA	Q.検索 + 新規作成	開始の				
認証 11 11.	着信インターフェース	Di WAN (vlan2001.emv1)	アドレス (19)	#R(150)	送信元	を ALL にし7	と場合、	不特定多
	発信インターフェース	Di LAN (port18.vlan101)		現 約 0				
	送信元	+	100.88.18.0/29	193	数のア	ドレスからフ	7クセス7	が可能に
インターネット サービス	IP/MACベースアクセスコントロール Ø	必須フィールドです。 +	⊒ 140.227.17.254/32 ■ 172.16.0.0/12	E91				
データベース	宛先	lest	192.168.0.0/16	総八い	なりま	ミすのでごネ	È 意 く だ	ぎさい。
サービス	,	+	•🖃 all	HE ZT /				
スケジュール	スケジュール	lo always		前オ	インタ	ーネットから	ヮのアク・	セスを可
バーチャルIP	サービス	ALL ALL	gmail.com					
IPプール	703-24		Iogin.microsoft.com	7日前	能にす	る場合には、	送信元	を制限す
プロトコルオプション	70939	✓ 計可 🔮 拒否	login.microsoftonline.com	100 kB				
トラフィックシェイピン グ	インスペクションモード フローベース	プロキシペース	☑ login.windows.net	80 kB	ること	を推奨します	0	
▲ セキュリティプロファイ 、			SSLVPN_TUNNEL_ADDR1	60 kB				
• <i>n</i>	ファイアウォール/ネットワークオプション	/	The second	40 kB				
🛓 ユーザ & 認証 🔹 🔹	NAT 🔿		クローズ	20 kB				
	プロトコルオプション PROT g-default	- <i>d</i>		ОВ	+ +	÷ ÷ • •		-
			OK キャンセル					



⑤ 送信元が問題ないことを確認し OK ボタンを押下する。

TEST-NWUTM-FG01A 🔹	≡ Q.				HA: プライマリ	VDOM: 💁 user01 🔻	>_ @• 4	수 🔹 😖 admin 🕶
🙆 ダッシュボード 🔹 🔰	ポリシーの編集							
ネットワーク >					統計情報(最終リセット以	降)		
💄 ポリシー&オブジェクト 🗸	名前 🚯	DNAT			ID	13		
ファイアウォールポリシ _	タイプ	スタンダード ZTNA			帰後の利田	3日前		
寝証ルール	着信インターフェース	Di WAN (vlan2001.emv1)	•		最初の利用	3日前		
	発信インターフェース	3륜 LAN (port18.vlan101)	-		アクティブセッション	0		
ZTNA	送信元	140.227.17.254/32	×		トット数	10		
インターネット サービス 🔥	IP/MACベースアクセスコントロール 🚯	+			総パイト教	40 15 kB		
データベース ど	宛先	🖀 test	×		おバイト奴	O has		
サービス		+			現任の市場	obps		
スケジュール	スケジュール	lo always	-		創 カウンタをクリア			
ハーチャルド	サービス	I ALL	×					
プロトコルオプション	アクション	✓ 許可 Ø 拒否			7日前 バイト・			
トラフィックシェイピン		An Int			100 KB	.lı nTurbo .lı SPU	J .lı Software	
ビッシュ シンティビン グ	インスペクションモード フローベース	プロキシベース			80 kB			
▲ セキュリティプロファイ 、					60 kB			
್ರಿ – ಈ ವಿಶಾಸ <b>ು</b>	ファイアウォール/ネットワークオプション	/			40 kB			
WiFi&スイッチコントロ	NAT O				20 kB			
<u>^ -</u> ,-	プロトコルオプション PROT g-default	- 1			08	+ + 4	+ + +	
FURTINET V7.2.7			ОК	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。

TEST-NWUTM-FG01A 🔹	≡ Q.						HA: プラ	<u> </u>	• >_ @•	🗘 🔹 😝 admin 🕶
🕰 ダッシュボード >	+新規作成	>_ CLIで編集   自 削開	R Q	ポリシーのルックフ	アップ 検索		Q	🖹 エクスポート 🕶 インタ	ーフェースペアビ	ュー シーケンス別
⊕ ネットワーク     >	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
ファイアウォールポリシ 🏑	Src White Rule	彊 Src White list	💷 all	lo always	🖳 ALL	✔ 許可	3 160.248.241.1/32	ss. no-inspection	すべて	0 B
- M	Dst White Rule	🔄 all		o always	🖬 ALL	✔ 許可		ss. no-inspection	すべて	0 B
 	ALL_ICMP	🔲 all	💷 all	o always	ALL_ICMP	✔ 許可	3 160.248.241.1/32	ss. no-inspection	🛛 すべて	20.88 kB
ZTNA	LAN -> WAN	10.0.0/8	💷 all	o always	🖬 ALL	✔ 許可	(a) 160.248.241.1/32	AV default	🕑 すべて	2.78 GB
インターネット サービス データベース		1/2.168.0.0/12						APP default		
サービス								ss. certificate-inspection		
スケジュール	test 🙁	192.168.0.0/16	🗐 all	lo always	I ALL	✔ 許可	ⓐ 160.248.241.1/32	ss. certificate-inspection	🛛 すべて	0 B
バーチャルIP	dnat test 😢	⊒ 192.168.0.0/16	🖀 test	🗔 always	I ALL	✔ 許可	160.248.241.1/32	ss. no-inspection	🔿 すべて	0 B
IPプール	192.168.0.0/24 permit 🔇	192.168.0.0/16	💷 all	lo always	🖳 ALL	✔ 許可	ⓐ 160.248.241.1/32	AV test	⊘ すべて	0 B
プロトコルオプション								ss. certificate-inspection		
トラフィックシェイピン	🖃 🗯 WAN (vlan2001.emv	1) → 🏦 LAN (port18.vlan	101) 1							
ッ ▲ <sup>セキュリティプロファイ</sup> 、	DNAT	140.227.17.254/32	test	o always	🖳 ALL	✔ 許可	😮 無効化済み	V default	🕑 すべて	69.15 kB
💄 ユーザ & 認証 🔹 🔸								SSL certificate-inspection		
≈ WiFi&スイッチコントロ −ラ−	-									
	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。

TEST-NWUTM-FG01A 🛛 🗸	≡ Q.							VDOM: 🙆 user	01 <b>- &gt;_ @-</b> 4	4 • 😐 admin •
🙆 ダッシュボード 🔹 🔹	◆新規作成 🖋 編集	>_ CLIで編集 🛛 自 削除	Q ポリシーのルックアッ	プ検索			<b>Q</b> 🖹 エクス	ポート・イン	ターフェースペアピュー	シーケンス別
⊕ ネットワーク     →	名前	From	То	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
ファイアウォールポリシ	NTTPC Monitor Rule	Di LAN (port18.vlan101)	) WAN (vlan2001.emv1)	100.88.18.0/29	🔳 all	o always	ALL	✔ 許可	160.248.241.1/32	ss. no-inspec
	Src Black Rule	Di LAN (port18.vlan101)	왜 WAN (vlan2001.emv1)	彊 Src Black list	🗉 all	lo always	ALL	⊘ 拒否		
	Dst Black Rule	맭 LAN (port18.vlan101)	먥 WAN (vlan2001.emv1)	🗉 all		o always	ALL	⊘ 拒否		
ZTNA	Src White Rule	왜 LAN (port18.vlan101)	VAN (vlan2001.emv1)	🖥 Src White list	🔳 all	o always	ALL	✔ 許可	3 160.248.241.1/32	ss. no-inspec
インターネット サービス	Dst White Rule	3용 LAN (port18.vlan101)	渊 WAN (vlan2001.emv1)	🗉 all		lo always	😰 ALL	✔ 許可		ss. no-inspec
データベース	ALL_ICMP	왜 LAN (port18.vlan101)	跳 WAN (vlan2001.emv1)	😑 all	🗉 all	lo always	ALL_ICMP	✔ 許可	160.248.241.1/32	ss. no-inspec
スケジュール	DNAT	₩ WAN (vlan2001.emv1)	嘂 LAN (port18.vlan101)	Ø none	🖀 test	o always	ALL	✔ 許可	🛚 無効化済み	AV default
バーチャルル										APP default
IPプール										ss. certificate
プロトコルオプション	LAN -> WAN	Di LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	10.0.0/8	🗉 all	lo always	ALL	✔ 許可	160.248.241.1/32	AV default
トラフィックシェイピン グ				1/2.168.0.0/12						APP default
▲ セキュリティプロファイ 、										ss. certificate
ニール ユーザ& 認証 >	test 🙆	💥 LAN (port18.vlan101 🖋	調 WAN (vlan2001.emv1)	192.168.0.0/16	📃 all	lo always	I ALL	✔ 許可	@ 160.248.241.1/32	ss. certificate
■ WiFi&スイッチコントロ	dnat test 🙁	💥 LAN (port18.vlan101)	₩ WAN (vlan2001.emv1)		🖀 test	to always	I ALL	✔ 許可	ⓐ 160.248.241.1/32	ss. no-inspec
	0 セキュリティレーティング問題         0% (1) 更新済み: 16:26:35 2									



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。

TEST-NWUTM-FG01A 🔹	≡ Q.				HA: プライマリ	VDOM: 💁 user0	1 <del>-</del> >_	Ø -	۰ ټ	⊖ admin •
🙆 ダッシュボード 🔉	ポリシーの編集									
🕂 ネットワーク 💦 👌					統計情報(最終リセット以	降)				I
💄 ポリシー&オブジェクト 🗸	名前 🚯	DNAT			ID	13				
ファイアウォールポリシ _	タイプ	スタンダード ZTNA			最後の利田	3日前				
家証 ルー ル	着信インターフェース	Diff WAN (vlan2001.emv1)	•		最初の利用	3日前				
	発信インターフェース	Diff LAN (port18.vlan101)	•		アクティブセッション	0				
ZTNA	送信元	Ø none	×		アンティンとランコン	10				
インターネット サービス	IP/MACベースアクセスコントロール 🚯	+			シバント教	10 15 kP				
データベース	宛先	lest	×		おバイト奴	09.13 KB				
サービス	1010	+			現住の帝珠	0 bps				
スケジュール	スケジュール	🐻 always	•		創 カウンタをクリア					
バーチャルIP	サービス	I ALL	×							
IPブール プロトコルオプション	アクション	◆ お可 Ø 垢香			7日前 バイト・					
	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,				100 kB	.lı nTurbo .lı	SPU .lı	Software	e	
ゲージョンチッシンシェイビン	インスペクションモード フローベース	プロキシベース			80 kB	-				
▲ セキュリティプロファイ 、					60 kB					
	ファイアウォール/ネットワークオプション	/			40 kB					
▲ ユーザム認証 >	NAT 🔿				20 kB					
	プロトコルオプション PROT g-default	- /			ОВ		-	+ •	-	
FERTINET V7.2.7			ок	キャンセル	]					

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。

TEST-NWUTM-FG01A 🔹	≡ <b>Q</b>					DOM: 🤷 user01 🔻	>_ ?-	¢• 6	🧿 admin 👻
🙆 ダッシュボード 🔉	ポリシーの編集								
🕂 ネットワーク 💦 💙			エントリを選択	<ol> <li>統計情報(最終)</li> </ol>	終リセット以降)				I
💄 ポリシー&オブジェクト 🖌	名前 🕄	DNAT	アドレス ユーザ インターネットサー	E ID	1	13			
ファイアウォールポリシ 🕁	タイプ	スタンダード ZTNA	Q 检索 + 新規作成	見後の利用					
ETET II II	着信インターフェース	DE WAN (vlan2001.emv1)	P アドレス (19)	慶復の利用	8 3				
	発信インターフェース	Di LAN (port 18.vlan 101)	10.0.0/8	銀初0					
	送信元	+	100.88.18.0/29	703	送信元を	ALL (CL)	た場合、	不特定	主多
		必須フィールドです。	I 40.227.17.254/32	ヒット					
インターネット リーヒス データベース	IP/MACペースアクセスコントロール 3	+	= 1/2.16.0.0/12 = 192.168.0.0/16	総バー	数のアト	、 レスからこ	アクセス	が可能	能に
サービス	郊先	test +	*I all	現在の					
スケジュール	スケジュール	lo always	FABRIC_DEVICE	<b>1</b>	なりま	すのでご	主音く	ださし	N
バーチャルIP	サービス	ALL .	FIREWALL_AUTH_PORTAL_ADDRESS			, , , , , , , , , , , , , , , , , , , ,			°
IPプール		+	gmail.com	7日前	インター	-ネットから	このアク	カスオ	후 피
プロトコルオプション	アクション	✓ 許可 Ø 拒否	Iogin.microsoftonline.com	100 kB	122				
トラフィックシェイピン			login.windows.net	80 kB	能にする	く得合にけ	洋信元	た生眠	見せ
	インスペクションモード フローベース	プロキシベース	* Ø none	60 kB	HEIC 9 'a			1 C 101 19	K 9
	ファイアウォール/ネットワークオプション	1	SSLVPN_TONNEL_ADDR1	40 kB	スーレた	(推将) ます			
💄 ユーザ&認証 🔹 💙				20 kB	<i>م د د خ</i>	雅美しより	0		
⇔ WiFi&スイッチコントロ		- 0	20-X	0B		_			
<u> </u>	groeiaut					1			
FERTIDET V7.2.7			OK = ++>セル						



### ⑤ 送信元が問題ないことを確認し OK ボタンを押下する。

TEST-NWUTM-FG01A •						VDOM: 🙆 user0	1• ≻_ @• 4	🗘 🔹 🤒 admin 🗣
🙆 ダッシュポード 🔹 🔰	ポリシーの編集							
🕂 ネットワーク 💦 👌					統計情報 (最終リセット以	降)		I
💄 ポリシー&オブジェクト 🗸	名前 🚯	DNAT			ID	13		
ファイアウォールポリシ _	タイプ	スタンダード ZTNA			最後の利用	3日前		
認証ルール	着信インターフェース	Di WAN (vlan2001.emv1)	•		最初の利用	3日前		
	発信インターフェース	Di LAN (port18.vlan101)	•		東京のの不可用	0		
	送信元	140.227.17.254/32	×		アジティンセッション	0		
インターネットサービス		+			ビット数	10		
データベース	ржаск-хуроехцорга-ло о	₹ Æ tect	×		総バイト数	69.15 kB		
サービス	98.75	+	<u> </u>		現在の帯域	0 bps		
スケジュール	スケジュール	lo always	•		創 カウンタをクリア			
バーチャルIP	サービス	ALL	×					
IPプール		+			7日前 バイト・			
プロトコルオプション	アクション	✓ 計刊 🥑 拒否			100 kB	l nTurbo di	SPU .l. Software	7
トラフィックシェイピン グ	インスペクションモード フローベース	プロキシベース			80 kB	_		
▲ セキュリティプロファイ 、					60 kB			
■ <i>I</i> U	ファイアウォール/ネットワークオプション	/			40 kB			-
💄 ユーザ & 認証 🔹 ゝ	NAT 🛈				20 kB			
<sup>〒 WiFi&amp;スイッチコントロ</sup> →	プロトコルオプション PROT g-default	- <i>d</i>			0B	÷ ÷ 🗏		
			ОК	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。

TEST-NWUTM-FG01A 🔹	≡ ۹.					HA: プラ・	<u>רדי</u> עסמ	OM: 💁 user01 🕶	>_ 0• ∴•	🕒 admin 🕶
	+新規作成 ● 編集	>_ CLIで編集 🛛 🖻 削除	Q ポリシーのルックアップ	プ検索		Q	🖹 エクスポー	ト・ インター	フェースペアビュー	シーケンス別
⊕ ネットワーク     >     ■     ポリシー&オブジェクト      ∨	名前	From	То	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
ファイアウォールポリシ 🏑	NTTPC Monitor Rule	18 LAN (port18.vlan101)	Se WAN (vlan2001.emv1)	100.88.18.0/29	🔳 all	o always	ALL	✔ 許可	3 160.248.241.1/32	ssL no-ins
- H	Src Black Rule	🔠 LAN (port18.vlan101)	해 WAN (vlan2001.emv1)	🖥 Src Black list	🗉 all	lo always	ALL	⊘ 拒否		
認証ルール	Dst Black Rule	📲 LAN (port18.vlan101)	3용 WAN (vlan2001.emv1)	🗉 all		o always	ALL	⊘ 拒否		
ZTNA	Src White Rule	📲 LAN (port18.vlan101)	에 WAN (vlan2001.emv1)	彊 Src White list	💷 all	lo always	🖸 ALL	✔ 許可	3 160.248.241.1/32	ssu no-ins
インターネット サービス	Dst White Rule	📲 LAN (port18.vlan101)	VAN (vlan2001.emv1)	💷 all		o always	ALL	✔ 許可		ssi no-ins
データベース	ALL_ICMP	🔠 LAN (port18.vlan101)	₩ WAN (vlan2001.emv1)	🖃 all	💷 all	lo always	ALL_ICMP	✔ 許可	3 160.248.241.1/32	ssu no-ins
シービス スケジュール	DNAT	3륜 WAN (vlan2001.emv1)	3븝 LAN (port18.vlan101)	140.227.17.254/32	🍘 test	o always	ALL	✔ 許可	🔕 無効化済み	AV defau
バーチャルIP										APP defau
IPプール										ssi certifi
プロトコルオプション	LAN -> WAN	📲 LAN (port18.vlan101)	왜 WAN (vlan2001.emv1)	10.0.0/8	💷 all	🚺 always	ALL	✔ 許可	160.248.241.1/32	AV defau
トラフィックシェイピン グ				<ul> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>						MEB defau APP defau
▲ セキュリティプロファイ 、										ssi certifi
、 ▲ ユーザ&認証 →	test 🙁	먦 LAN (port18.vlan101)	왜 WAN (vlan2001.emv1)	192.168.0.0/16	🔲 all		ALL	✔ 許可	160.248.241.1/32	ssi certifi
- WiFi&スイッチコントロ >	dnat test 😣	Di LAN (port18.vlan101)	DE WAN (vlan2001.emv1)	192.168.0.0/16	lest	lo always	I ALL	✔ 許可	160.248.241.1/32	ssi no-ins
	0 セキュリティレーティング問題 0% 😨 更新済み: 16:21:21 C									



- 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)
  - ・ 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。

TEST-NWUTM-FG01A -	≡ Q			VDOM: 🔂 use	r01• >_ 🕜 • 4	) - 🕒 user01 -
🙆 ダッシュボード 💦 👌		タイプ		インターフェー		
♣ ネットワーク		■IPv4バーチャルIP ②		ス		
💄 ポリシー&オブジェクト 🗸	2	-	2	any 💿		
ファイアウォールポリシ ー	Total		lotal			
アドレス						
インターネットサービス	◆ 新規作成	前 削除 ● Q, 検索	1		Q Virtual IPs 八一	チャルIPクループ
	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	參照
	🖀 mac	🗆 any	100.1.1.21	172.31.200.3	0	0
バーチャルIP 🏠	192.168.150.1_210.136.56.208	🗆 any	192.168.150.1 (TCP: 25)	210.136.56.208 (TCP: 25)	0	0
<ul> <li>システム</li> </ul>						
<ul> <li></li></ul>						
■ ログ&レポート >						
						>
	● ビキエリディレーディング問題					2



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

新規ハーナヤルIP	
VIPタイプ IPv4 名前 100.0.0.2/32 コメント コメント記入 /0/2 カラー 電 変更	55
ネットワーク	払い出された追加グロー
インターフェース 🕄 🗆 any タイプ スタティックNAT FORM	・ バル IP を記載
外部IPアドレス/範囲 🖲 100.0.0.2	
マップ IPv4アドレス/範囲 192.168.0.2	
● オプションのフィルタ	ノフィヘート IP を記載
● ポートフォワード	
プロトコル TCP UDP SCTP ICMP	
ポートマッピングタイプ 1対1 多対多	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
	ок キャンセル

最後にOKを押して設定を完了する。

を行う。

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。

TEST-NWUTM-FG01A	= Q					v	'DOM: 📤 user01 • 🔹 🗘	- 🛛 • 🗘 • \varTheta user01 •
孢 ダッシュボード	+新規作成	✔ 編集 >_ CLIで編集	<b>會</b> 削除 Q ポ	リシーのルックア	'ップ 検索			Q
🕂 ネットワーク 🔹	■ エクスポート	-▼ インターフェースペス	7ビュー シーケン	ス別				
💄 ポリシー&オブジェクト 🔹		送信元	宛先	スケジュール	サービス	アクション	NAT	ヤキュリティプロファイル
ファイアウォールポリシー 🖌			0004 41 8	X) ) 1 /V	5 27	/ // 1/	1051	
アドレス	E 🕷 LAN (port)	18.Vian101) → 3/8 VVAN (Viar	12001.emv1) 🅖				-	
インターネットサービスデ	NTTPC Monitor	Rule 🗐 100.88.18.0/29	💷 all	o always	🖬 ALL	✔ 許可	160.248.241.1/32	ss. no-inspection
ータベース	Src Black Rule	🖷 Src Black list	😑 all	o always	д ALL	⊘ 拒否		
サービス	Dst Black Rule	ポリシー	🗟 Dst Black list	🖸 always	🖬 ALL	⊘ 拒否		
パーチャルIP	Src White Rule	設定ステータス	🗉 all	o always	д ALL	✔ 許可	160.248.241.1/32	ss. no-inspection
▲ セキュリティプロファイル >	Dst White Rule	▼ 名前 でフィルタ	🗟 Dst White list	🖸 always	🖬 ALL	✔ 許可	(a) 160.248.241.1/32	ss. no-inspection
■ = - =	ALL_ICMP	<b>4</b> 1⊐ピ−	🗊 all	🖸 always	ALL_ICMP	✔ 許可	(a) 160.248.241.1/32	ss. no-inspection
	LAN -> WAN	▶ペースト	💷 all	🖸 always	🖳 ALL	✔ 許可	(a) 160.248.241.1/32	AV default
⑦ セキュリティファフリック >		◆ 空のポリシーを挿入						WEB default
<b>回</b> ログ&レポート <b>)</b>								APP default
		間一致するロクを表示						55L certificate-inspection
	∃ 暗黙 1	I≜FortiViewで表示する						
		✔ 編集						
		>_ CLIで編集						•
FCRTINET v7.2.	0 セキュリティ	■ ポリシー削除						🚯 更新済み: 17:40:30 🕃

## ⑥ 再度 LAN→WAN を右クリックし、ペースト→上へを押下する。

TEST-NWUTM-FG01A -	≡ Q					VI	DOM: 💁 user01 • 🔹 🔸	- 🛛 • 🗘 • 🔒 user01 •
🙃 ダッシュボード 💦 👌	➡新規作成 🖋 編	集 >_ CLIで編集	<b>會</b> 削除 Q ポ	リシーのルックア	ップ検索			Q
	■ エクスポート・	インターフェースペア	<b>パビュー シーケン</b>	ス別				
💄 ポリシー&オブジェクト 🗸 🗸	名前	送信元	宛失	スケジュール	サービス	アクション	NAT	ヤキュリティプロファイル
ファイアウォールポリシー 🕁	E SELAN (port18vl	an101) → ₩ WAN (vian	2001 emv1) 7	X0 9 ± 10	J EX	/ // 1/	1001	
アドレス	NTTPC Monitor Rule	100.88.18.0/29	🗉 all	always	🗊 ALL	✔ 許可	160.248.241.1/32	55L no-inspection
インターネットサービスデ	Src Black Rule	🖷 Src Black list	🚍 all	lo always	I ALL	⊘ 拒否		
ー·ジベーへ サードフ	Dst Black Rule	ポリシー	st Black list	🖸 always	🖬 ALL	⊘ 拒否		
バーチャルIP	Src White Rule	設定ステータス	• II	😈 always	🖬 ALL	✔ 許可	160.248.241.1/32	ss. no-inspection
▲ ヤキュリティプロファイル <b>&gt;</b>	Dst White Rule	▼ 名前 でフィルタ	<ul> <li>st White list</li> </ul>	lo always	д ALL	✔ 許可	160.248.241.1/32	55L no-inspection
▲ システム >	ALL_ICMP	<b>@</b> ⊐Ľ–	u .	🖸 always	ALL_ICMP	✔ 許可	160.248.241.1/32	ss. no-inspection
	LAN -> WAN	<b>心</b> ペースト	・ <u>~</u> 上へ	🖸 always	🖬 ALL	✔ 許可	160.248.241.1/32	AV default
₩ ログ&レポート >		◆ 空のポリシーを挿び	入・ ~ 下へ					APP default
		<b>間</b> 一致するログを表示	ŧ					ss. certificate-inspection
	田 暗黙 ①	▲FortiViewで表示する	5					
		● 編集						
EMBTIDET	↓ ● 0 セキュリティレー:	>_ CLI C編集						③ 更新済み: 17:40:30 2
	0 セキュリティレー	會 ポリシー削除						🚯 更新済み: 17:40:30 🤰



## ⑦ 作成したポリシーをダブルクリックする。

TEST-NWUTM-FG01A 🗸	≡ ۹	E Q											
🗛 ダッシュボード 🔹 🔉	◆新規作成 ◆ 編	集 >_ CLIで編集	◎ 削除 Q オ	ペリシーのルックフ	アップ検索			Q					
	□ エクスポート・	インターフェースペ	アビュー シーケン	レス別									
■ ポリシー&オブジェクト マ フライアウォールゼリシュ	名前	送信元	宛先	スケジュー	サービス	アクショ	NAT	セキュリティプロファ	ログ				
-	🖃 🎜 LAN (port18.vla	n101) → 🎟 WAN (via	an2001.emv1) 🛞										
アドレス	NTTPC Monitor R	100.88.18.0/29	💷 all	🐻 always	🖪 ALL	✔ 許可	@ 160.248.241.1/32	ssu no-inspection	😢 無効化済				
インターネットサービス	Src Black Rule	🚡 Src Black list	💷 all	🖬 always	🕼 ALL	⊘ 拒否			🛛 すべて				
データベース	Dst Black Rule	🔲 all	🗟 Dst Black list	🖬 always	🕼 ALL	⊘ 拒否			🛛 すべて				
サービス	Src White Rule	🐵 Src White list	💷 all	🖬 always	🖬 ALL	✔ 許可	(2) 160.248.241.1/32	ssi no-inspection	🛛 すべて				
バーチャルIP	Dst White Rule	🔄 all	🖻 Dst White li	🖬 always	🕼 ALL	✔ 許可	@ 160.248.241.1/32	ssi no-inspection	🛛 すべて	1.16			
	ALL_ICMP	🔲 all	🔲 all	🐻 always	ALL_IC	✔ 許可	@ 160.248.241.1/32	ssu no-inspection	🛛 すべて				
	0	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	🖳 all	G always		✔ 許可	<sup>(1)</sup>	Av default wea default APP default SSL certificate-inspection	🕈 রুর্নেে				
■ ログ&レポート >	LAN -> WAN	<ul> <li>10.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	🔄 all	🐻 always	🛛 ALL	✔ 許可	(a) 160.248.241.1/32	AV default WEE default APP default SSL certificate-inspection	🛛 র্বেে	7.24			
	❶ 暗黙 ①												
		ハンガロ原							■ 毎日の 「 日本の な」、 17、40、31				
	0 ビキエリティレーティ	「ノン回題						<b>1</b>	と初月の7.17:40:31				

Master's ONE°

 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)

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 (port18vlan	101) → 🕽 WAN (vlan2	001.emv1) 🧷								
NTTPC Monitor Rule	100.88.18.0/29	🚍 all	😡 always	🖳 ALL	✔ 許可	160.248.241.1/32	ssu no-inspection	😵 無効化済み	OB	スタンダード
5rc Black Rule	🖥 5rc Black list	\Xi all	😡 always	🖳 ALL	🖉 拒否			🕏 すべて	OB	スタンダード
Dst Black Rule	🖃 all	🖥 Dst Black list	😡 always	🖳 ALL	🖉 拒否			🥏 すべて	OB	スタンダード
5rc White Rule	😼 Src White list	\Xi all	😡 always	🖳 ALL	✔ 許可	160.248.241.1/32	ssu no-inspection	🕏 すべて	OB	スタンダード
Dst White Rule	🖃 all	👼 Dst White li	🖬 always	🖳 ALL	✔ 許可	160.248.241.1/32	ssu 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	ssu no-inspection	🕏 すべて	OB	スタンダード
LAN -> WAN	<ul> <li>⊒ 10.0.0.0/8</li> <li>⊒ 172.16.0.0/12</li> <li>⊒ 192.168.0.0/16</li> </ul>	🔄 all	😡 always	▣ ALL	✔ 許可	160.248.241.1/32	AV default VEB default APP default SSL certificate-inspection	🕏 র্বশবে	9.31 MB	スタンダード
🖃 🧏 WAN (vlan2001.e	emv1) → 👫 LAN (port1	.8.vlan101) <sub>2</sub>								
Θ.	192168.1.2/32	@ 100.0.0.2/32	la always	모 ALL	✔ 許可	😂 無効化済み	AV default VEE default APP default SL certificate-inspection	🕏 রুশ্বে	OB	スタンダード
DNAT 😒	<u>■</u> 1921/812/32	(a) 100.0.0.2/32	😡 always	ALL ALL	✔ 許可	😵 無効化済み	Av default wes default APP default ss certificate-inspection	🕏 इंग्रेट	OB	スタンダード
	- بر 100 per									<b>四 王が文山</b> 17:00 22
v erij 274 2-24	1.2.2.10.352									957(),907. 17.39.20 V

## 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。

TEST-NWUTM-FG01A +	≡ Ϙ,								VDO	M: 🝊 user01 → 🔶	<b>Θ •</b>
🙆 ダッシュボード 🔹 🔸	十新規作成	✔ 編集 >_ CLIで編集	自剤除(Qヵ	(リシーのルックア	<b>シップ</b> 検索			۹	■ エクスポー	-ト・ インターフェー	-スペアビュー シーケンス別
キャットワーク >	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	07	バイト	タイプ
▶ ポリシー&オブジェクト 🗸	E 18 LAN (port:	18vlan101) → 35 WAN (vlan2	001.emv1) 7								
ファイアウォールポリシー 合	NTTPC Monitor	r Rule 🗧 100.88.18.0/29	🖬 all	🗔 always	😰 ALL	✔ 許可	@ 160.248.241.1/32	ss. no-inspection	😝 無効化済み	OB	スタンダード
アドレス	5rc Black Rule	🐴 5rc Black list	🖬 əll	G always	😰 ALL	⊘ 拒否			🛛 কৃৎবে	OB	スタンダード
インターネットサービスデ	Dst Black Rule	🖽 all	🖥 Dst Black list	😡 always	😰 ALL	⊘ 拒否			<ul> <li>すべて</li> </ul>	ОB	スタンダード
	Src White Rule	👼 Src White list	🗳 all	lo always	😰 ALL	✔ 許可	@ 160.248.241_1/32	38 no-inspection	🗢 কৃশবে	OB	スタンダード
ジービス バーチャルIP	Dst White Rule	🖾 əll	層 Dst White li	lo always	😰 ALL	✔ 許可	@ 160.248.241.1/32	ssu no-inspection	🗢 রুদের	1.16 MB 🔳	スタンダード
	ALL_ICMP	🖾 əll	🖬 əll	lo always	ALL_ICMP	✔ 許可	160.248.241.1/32	ss. no-inspection	S 3775	OB	スタンダード
	LAN -> WAN	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	E all	læ always	I ALL	✔ 許可	(2) 160.248.241.1/32	44 default WED default APP default SSL certificate-inspection	🗢 রুশ্বে	9.31 MB	■ スタンダード
₩ D2&U#-N >	🖃 🧏 WAN (vlar		Tvlan101) 🙄								
	DNAT 🤤	ホッシー 設定ステータス ・ ▼名前でフィルタ ・ 内コピー	<ul> <li>○ 有効</li> <li>2/32</li> <li>○ 有効</li> </ul>	lo always	🗑 ALL	✔ 許可	S 無効化済み	AV default WEB default APP default SSL certificate-inspection	চস্ফ 🕲	OB	スタンダード
	0	<ul> <li>レースト・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>	@ 100.0.0.2/32	😡 always	ALL ALL	✔ 許可	S 無効化済み	AV default W69 default APP default SU certificate-inspection	오 इन्ट्र	OB	スタンダード
	由 暗黙 1	▶FortiViewで表示する									
		✔ 編集									
		>_ CLIで編集									
	0 セキュリティ	歯 ポリシー削除									① 更新済み: 17:59:26 2



① 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&vlar	101) → 🕽 WAN (vlan2	001.emv1) 🤈								
NTTPC Monitor Rule	100.88.18.0/29	🗉 all	👩 always	🖳 ALL	✔ 許可	@ 160.248.241.1/32	ssu no-inspection	😂 無効化済み	OB	スタンダード
5rc Black Rule	🖥 5rc Black list	🗳 all	😡 always	🖳 ALL	🖉 拒否			🕏 すべて	OB	スタンダード
Dst Black Rule	😑 all	🖥 Dst Black list	🗔 always	🖳 ALL	🖉 拒否			🕏 すべて	OB	スタンダード
5rc White Rule	🖥 5rc White list	🖻 all	🗔 always	모 ALL	✔ 許可	@ 160.248.241.1/32	sst no-inspection	🛛 すべて	OB	スタンダード
Dst White Rule	🖻 all			ALL	✔ 許可	@ 160.248.241.1/32	ssi no-inspection	🔮 すべて	1.16 MB 🔳	スタンダード
ALL_ICMP	<sup>⊑ all</sup> × ກ່	消えていれ	1.ば有効	ALL_ICMP	✔ 許可	160.248.241.1/32	ssu no-inspection	🕏 すべて	OB	スタンダード
LAN ->WAN	■ 100 ■ 172 ■ 192 化さ	れている		ALL	✔ 許可	160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	🔊 কর্শেব	9.31 MB	スタンダード
🖃 🔀 WAN (vlan 2001.	emv1)→3 <mark>8</mark> LA <sup>br</sup>									
DNAT	E	100.0.0.2/32	Go always	🛛 ALL	✔ 許可	〇 無効化済み	AV default VEE default APP default SSL certificate-inspection	🕏 রশবে	OB	スタンダード
8	☐ 192.168.1.2/32	∰ 100.0.0.2/32	log always	ALL ALL	✔ 許可	(2) 無効化済み	AV default WEB default APP default SSL certificate-inspection	🦁 রস্তে	OB	スタンダード
田 暗黙      1										
									o 亦再が足が	station and a
○ セキュリティレーテ	ィング問題								2 SOTA	

- 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。



新規作成を押下する。

TEST-NWUTM-FG01A	• ≡ Q				VDOM: 🔂 us	er01• >_ 🕜•	4 • 🔒 user01 •
<ul> <li></li></ul>	*	2 Total	タイプ IPuJバーチャルIP	2 Total	インターフェー ス ■ 20y		
インターネットサービス	+ 新規作成	🖋 編集 🔳 クローン	前 削除 ○ Q 検索			Q Virtual IPs パー	ーチャルIPグループ
		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
サービス	🖀 mac		🗆 any	100.1.1.21	172.31.200.3	0	0
バーチャルIP	☆ 🖀 192.168.15	0.1_210.136.56.208	🗆 any	192.168.150.1 (TCP: 25)	210.136.56.208 (TCP: 25)	0	0
<sup>■</sup> ル ◆ システム ● セキュリティファブリッ ク	> >						
₩ ログ&レポート	`						Þ
	0 セキュリティ	ィレーティング問題					2

Copyright (c) 2024 NTT PC Communications Incorporated, All Right Reserved.



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。

新規バーチャルIP	
VIPタイプ IPv4 名前 100.0.0.2/32 コメント コメント記入 0/255 カラー 魯 変更	
ネットワーク	払い出された追加グロー
インターフェース ()     □ any       タイプ     スタティックNAT_FODN	バル IP を記載
外部IPアドレス/範囲 100.0.0.2	
マップ IPv4アドレス/範囲 192.168.0.2	
オプションのフィルタ	フライベート IP を記載
● ポートフォワード	
プロトコル TCP UDP SCTP ICMP ポートマッピングタイプ 4対4 条対条	
ハートマッピンジョイン コメゴ シバシ 外部サービスポート 0 1	ポートを指定したい場合は
IPv4ポートヘマップ 1	ポートフォワードのトグル
1	をオンにしてから記載
	ок キャンセル

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。





TEST-NWUTM-FG01A 🚽	≡ Q.						VDOM: 🚭 us	er01 - >_	Ø• ↓• Øuser	01 -
🙆 ダッシュボード 🔹 🔸	+新規作成 ● 編集	■ >_ CLIで編集	Q ポリシーのルックア	タップ 検索		Q 🖹 I	クスポート・イ	ンターフェース	ペアビュー シーケンス	ス別
♣ ネットワーク >	名前	From	То	送信元	宛先	スケジュール	サービス	アクション	NAT	セ
ポリシー&オブジェクト	NTTPC Monitor Rule	😹 LAN (port18.vlan101)	📽 WAN (vlan2001.emv1)	■ 100.88.18.0/	🗉 all	G always	I ALL	✔ 許可	() 160.248.241.1/	55
ファイアウォールボリシ ー	Src Black Rule	😹 LAN (port18.vlan101)	😹 WAN (vlan2001.emv1)	唱 Src Black list	🗉 all	🕼 always	I ALL	⊘ 拒否		
アドレス	Dst Black Rule	🗯 LAN (port18.vlan101)	₩ WAN (vlan2001.emv1)	💷 all	😼 Dst Black list	G always	I ALL	⊘ 拒否		
インターネットサービス	Src White Rule	🚟 LAN (port18.vlan101)	VAN (vlan2001.emv1)	唱 Src White list	🚍 all	🕼 always	ALL	✔ 許可	() 160.248.241.1/	55
データベース	Dst White Rule	🎥 LAN (port18.vlan101)	I WAN (vlan2001.emv1)	🚍 all	🖷 Dst White list	G always	ALL ALL	✔ 許可	@ 160.248.241.1/	55
サービス	ALL_ICMP	🗯 LAN (port18.vlan101)	Sil WAN (vlan2001.emv1)	🖭 all	🚍 all	🕼 always	ALL_ICMP	✔ 許可	@ 160.248.241.1/	55
バーチャルIP	SNAT	3# LAN (port18.vlan101)	p∰ WAN (vlan2001.emv1)	192.168.1.2/	@ 100.0.0.2/32	🕢 always	I ALL	✔ 許可	🙁 無効化済み	AN WE
<ul> <li>ル</li> <li>⇒ システム</li> <li>&gt;</li> <li>↓</li> <li>セキュリティファブリッ</li> </ul>	user-defined-po	ボリシー ステータス 2前 でつくリタ	B WAN (vlan2001.emv1)	172.16.0.0/12	💷 all	🕼 always	😨 ALL	✔ 許可	@ 160.248.241.1/	55
♥ク > ■ログ&レポート >	LAN -> WAN	コピー ペースト Pのポリシーを挿入	WAN (vlan2001.emv1)	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/</li> </ul>	🖭 all	🕢 always	ل ALL	✔ 許可	160.248.241.1/	AV WE AP SS
	暗黙の拒否 <b>+</b> シ	マーケンスグルーピングを挿入	) any	🗐 all	🖃 all	G always	ALL	⊘ 拒否		
	₩ ■Fc ● 第 <	致するログを表示 xrtiViewで表示する a集 LLで編集								Þ
	<ol> <li>0 セキュリティレ 自 オ</li> </ol>	ペリシー削除							10 更新済み: 09:58:18	Ø

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。

🐨 TEST-NWUTM-FG01A 🛛 🗸	≡ Q.						VDOM: 🚭 us	ær01 • >_	😧 • 🗘 • 🔒 user	01 -
🙆 ダッシュボード 🔹 🔉	+新規作成 🥒 編集	■ CLIで編集 ● 削除	Q ポリシーのルックア	ップ 検索		Q 🗎 I/	フスポート・ イ	ンターフェース	ペアビュー シーケンス	ス別
	名前	From	То	送信元	宛先	スケジュール	サービス	アクション	NAT	セキ
ポリシー&オブジェクト	NTTPC Monitor Rule	해 LAN (port18.vlan101)	譜 WAN (vlan2001.emv1)	100.88.18.0/	💷 all	🐻 always	🕢 ALL	✔ 許可	() 160.248.241.1/	SSL
ファイアウォールボリシ -	Src Black Rule	웲 LAN (port18.vlan101)	譜 WAN (vlan2001.emv1)	🖷 Src Black list	💷 all	🐻 always	I ALL	⊘ 拒否		
アドレス	Dst Black Rule	3용 LAN (port18.vlan101)	譜 WAN (vlan2001.emv1)	🗉 all	🖷 Dst Black list	🕞 always	😡 ALL	⊘ 拒否		
インターネットサービス	Src White Rule	譜 LAN (port18.vlan101)	I WAN (vlan2001.emv1)	🖷 Src White list	💷 all	🕞 always	🕢 ALL	✔ 許可	() 160.248.241.1/	SSL
データベース	Dst White Rule	먦 LAN (port18.vlan101)	端 WAN (vlan2001.emv1)	😑 all	🐴 Dst White list	🕞 always	I ALL	✔ 許可	3 160.248.241.1/	SSL
サービス	ALL_ICMP	📲 LAN (port18.vlan101)	₩ WAN (vlan2001.emv1)	🚍 all	💷 all	🐻 always	ALL_ICMP	✔ 許可	3 160.248.241.1/	SSL
バーチャルIP	SNAT	tAN (port18.vlan101) №	Stan (vlan2001.emv1)	■ 192.168.1.2/	@ 100.0.0.2/32	🕞 always	🕢 ALL	✔ 許可	🕴 無効化済み	AV
▲ セキュリティプロファイ ル		ポリシー								APP SSL
	user-defined- 設定ス	テータス・	₩ WAN (vlan2001.emv1)	■ 172.16.0.0/12	💷 all	🕞 always	🕢 ALL	✔ 許可	(2) 160.248.241.1/	SSL
● <sup>C+⊥9</sup> 1 <sup>→</sup> 2 <sup>→</sup> 2 <sup>→</sup>	LAN->WAN	・ ・	嘂 WAN (vlan2001.emv1)	10.0.0/8	💷 all	🕞 always	😰 ALL	✔ 許可	() 160.248.241.1/	AV
■ ログ&レポート >	LE 10 LE ペー L 1 空の		<ul> <li>▲ 上へ</li> <li>▼ 下へ</li> </ul>	<ul> <li>172.16.0.0/12</li> <li>192.168.0.0/</li> </ul>						APF SSL
	暗黙の拒否 + シー	ケンスグルーピングを挿入	🗆 any	🔳 all	💷 all	🐻 always	😨 ALL	⊘ 拒否		
	iii一致  ▲Forti ✔ 編集	するログを表示 Viewで表示する								
F#RTINET	<ul> <li>セキュリテ・ 値 ポリ</li> </ul>	<sup>ご确未</sup> Iシー削除						6	更新済み: 09:58:18	8



## ⑦ 作成したポリシーをダブルクリックする。

FG01A 🔹	≡ Q						VDOM: 🔂 us	er01 - >_		-
🛯 ダッシュボード 🔹 🔸	+新規作成 ℓ 編集	>_ CLIで編集 💼 削除	· <b>Q</b> ポリシーのルックア	/ップ 検索		Q 🗎 I/	7スポート・ イ	ンターフェース	ペアビュー シーケンス別	I
♣ ネットワーク	名前	From	То	送信元	宛先	スケジュール	サービス	アクション	NAT	23
▶ ポリシー&オブジェクト ∨	NTTPC Monitor Rule	🍀 LAN (port18.vlan101)	₩ WAN (vlan2001.emv1)	⊑ 100.88.18.0/	🗐 all	🕞 always	🕢 ALL	✔ 許可	@ 160.248.241.1/	551
ファイアウォールポリシ -	Src Black Rule	:# LAN (port18.vlan101)	₩ WAN (vlan2001.emv1)	🖷 Src Black list	💷 all	🐻 always	🖬 ALL	⊘ 拒否		
アドレス	Dst Black Rule	38 LAN (port18.vlan101)	₩ WAN (vlan2001.emv1)	😑 all	🐴 Dst Black list	🐻 always	😨 ALL	⊘ 拒否		
インターネットサービス	Src White Rule	38 LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	🐴 Src White list	💷 all	🕞 always	🖬 ALL	✔ 許可	160.248.241.1/	SSL
データベース	Dst White Rule	38 LAN (port18.vlan101)	₩ WAN (vlan2001.emv1)	💷 all	🐴 Dst White list	🕞 always	д ALL	✔ 許可	() 160.248.241.1/	550
サービス	ALL_ICMP	28 LAN (port18.vlan101)	3 WAN (vlan2001.emv1)	😑 all	💷 all	🐻 always	ALL_ICMP	✔ 許可	160.248.241.1/	SSL
バーチャルIP	SNAT	2# 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
▲ セキュリティプロファイ >										APP
										551
◆ /// · · · · · · · · · · · · · · · · ·	0	🍀 LAN (port18.vlan101)	🗯 WAN (vlan2001.emv1)	😑 172.16.0.0/12	😑 all	🗔 always	😰 ALL	✔ 許可	160.248.241.1/	<b>S</b> 5
• <b>` ` ` `</b> }	user-defined-policy-1	😹 LAN (port18.vlan101)	₩ WAN (vlan2001.emv1)	172.16.0.0/12	😑 all	🕟 always	😰 ALL	✔ 許可	160.248.241.1/	SSL
<ul> <li>■ ログ&amp;レポート</li> <li>&gt;</li> </ul>	LAN -> WAN	Sig LAN (port18.vlan101)	38 WAN (vlan2001.emv1)	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/</li> </ul>	🔁 all	🕢 always	n All	✔ 許可		AV WE APP SSL
	暗黙の拒否	🗆 any	any	😑 all	💷 all	🐻 always	I ALL	⊘ 拒否		
										+
FERTINET v7.2.7	0 セキュリティレーティ	ング問題						6	▶ 更新済み:09:58:18 2	1



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。





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	То	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)	3# WAN (vlan2001.emv1)	100.88.18.0/29	😑 all	🐻 always	🕢 ALL	✔ 許可	160.248.241.1/32	SSL
Src Black Rule	📲 LAN (port18.vlan101)	3 WAN (vlan2001.emv1)	🖷 Src Black list	💷 all	🐻 always	😰 ALL	⊘ 拒否		
Dst Black Rule	Sill LAN (port18.vlan101)	3# WAN (vlan2001.emv1)	🖃 all	🖷 Dst Black list	🐻 always	😰 ALL	⊘ 拒否		
Src White Rule	📲 LAN (port18.vlan101)	3 WAN (vlan2001.emv1)	墙 Src White list	💷 all	🐻 always	😨 ALL	✔ 許可	160.248.241.1/32	SSL
Dst White Rule	📲 LAN (port18.vlan101)	3 WAN (vlan2001.emv1)	🖃 all	🖷 Dst White list	🐻 always	😰 ALL	✔ 許可	160.248.241.1/32	SSL
ALL_ICMP	Stand (port18.vlan101)	3# WAN (vlan2001.emv1)	😑 all	💷 all	🐻 always	ALL_ICMP	✔ 許可	() 160.248.241.1/32	SSL
SNAT	📲 LAN (port18.vlan101)	調 WAN (vlan2001.emv1)	192.168.1.2/32	100.0.2/32	🐻 always	n All	✔ 許可	😢 無効化済み	AV WEB APP SSL
任意28	嘂 LAN,port18.vlan101)	歸 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	과용 LAN (port18.vlan101)	3룹 WAN (vlan2001.emv1)	<ul> <li>10.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	😑 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		
4									•
0 セキュリティレーティ	ング問題							111   史新済み: 10:30:56	C

### 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。

🖬 TEST-NWUTM-FG01A 🛛 👻	≡ Q						VDOM: 🚭 🛛	user01 - >_	영 • 슈 • 😁 user	r01 -
🙆 ダッシュボード 🔹 🔉	+新規作成 ● 編	集 >_ CLIで編集 🔒 削除	Q ポリシーのルックフ	アップ 検索		Q 🗎 I	クスポート・	インターフェース	マペアビュー シーケン	ス別
	名前	From	То	送信元	宛先	スケジュール	サービス	アクション	NAT	セキ
ポリシー&オプジェクト マ	NTTPC Monitor Rule	e DE LAN (port18.vlan101)	🕷 WAN (vlan2001.emv1)	100.88.18.0/29	😑 all	尾 always	🖸 ALL	✔ 許可	() 160.248.241.1/32	SSL
ファイアウォールポリシ - <b>な</b>	Src Black Rule	DE LAN (port18.vlan101)	🗯 WAN (vlan2001.emv1)	🖷 Src Black list	🚍 all	🐻 always	🖬 ALL	⊘ 拒否		
アドレス	Dst Black Rule	DE LAN (port18.vlan101)	WAN (vlan2001.emv1)	💷 all	🐴 Dst Black list	🐻 always	😨 ALL	⊘ 拒否		
インターネットサービス	Src White Rule	聞 LAN (port18.vlan101)	調 WAN (vlan2001.emv1)	🖷 Src White list	🚍 all	🕼 always	I ALL	✔ 許可	160.248.241.1/32	SSL
データベース	Dst White Rule	D語 LAN (port18.vlan101)	調 WAN (vlan2001.emv1)	💷 all	1 Dst White list	🐻 always	I ALL	✔ 許可	(160.248.241.1/32)	SSL
サービス	ALL_ICMP	聞 LAN (port18.vlan101)	調 WAN (vlan2001.emv1)	💷 all	🚍 all	Co always	ALL_ICMP	✔ 許可	160.248.241.1/32	SSL
バーチャルIP	任意20	5≣ LAN (port18 vlan101) +#u s	WAN (vlan2001.emv1)	172.16.0.0/12	😑 all	G always	ALL	✔ 許可	🔕 無効化済み	APP
▲ セキュリティプロファイ >		ホリシー								SSL
	SNAT	定 ステータス	・ ② 有効 (2001.emv1)	192.168.1.2/32	€ 100.0.0.2/32	Co always	ILA 😨	✔ 許可	🕴 無効化済み	AV
		「名則 Cノイルタ								APP
∅ 2	4									SSL
■ ログ&レポート >	user-defined-poli	▶ 空のポリシーを挿入	WAN (vlan2001.emv1)	172.16.0.0/12	🚍 all	🕞 always	🕢 ALL	✔ 許可	160.248.241.1/32	SSL
	LAN -> WAN	反転してクローン	WAN (vlan2001.emv1)	10.0.0.0/8	😐 all	🐻 always	ALL	✔ 許可	160.248.241.1/32	AV
	-	<ul> <li>シーケンスグルーピングを挿</li> </ul>	7	192.168.0.0/12						APP
	i i i i i i i i i i i i i i i i i i i									SSL
	暗黙の拒否	■FortiViewで表示する	any	💷 all	🚍 all	🐻 always	🖬 ALL	⊘ 拒否		
		▶ 編集								
	· >	_ CLIで編集								•
	○ セキュリティレ- 〔	) ポリシー削除							10:30:56 更新済み: 10:30:56	C



## ① ルールが有効になったことを確認する。

TEST-NWUTM-FG01A 🔹	▼ Ξ Q. VDOM: 🌢 user01 ▼ ≻ 😧 • 🖧 ▼ 😌 user01 ▼									
🕰 ダッシュボード 💦 👌	◆新規作成 ● 編集 >_ CLIで編集			マップ 検索 Q 目 エクスポート			クスポート・	<ul> <li>インターフェースペアビュー シーケンス別</li> </ul>		
♣ ネットワーク	名前	From	То	送信元	宛先	スケジュール	サービス	アクション	NAT	セキ
🖹 ポリシー&オブジェクト 🗸 🗸	NTTPC Monitor Rule	3K L		100.88.18.0/29	🗐 all	🐻 always	😰 ALL	✔ 許可	(a) 160.248.241.1/32	SSL
ファイアウォールポリシ _ <b>☆</b>	Src Black Rule	<sup>嘂∟</sup> ×が消え	×が消えていれば有効 化されている		🗉 əll	🐻 always	😰 ALL	⊘ 拒否		
アドレス	Dst Black Rule	3용 L			🐴 Dst Black list	🐻 always	д ALL	⊘ 拒否		
インターネットサービス	Src White Rule	📲 化されて			😑 all	🐻 always	I ALL	✔ 許可	@ 160.248.241.1/32	SSL
データベース	Dst White Rule	3뚢 L			🖷 Dst White list	🐻 always	I ALL	✔ 許可	@ 160.248.241.1/32	SSL
サービス	ALL_ICMP	Stan (Avian101)	聞 WAN (vlan2001.emv1)	🗐 all	🚍 all	🐻 always	ALL_ICMP	✔ 許可	(2) 160.248.241.1/32	SSL
バーチャルIP	任意2 🦯	💥 LAN (port18.vlan101)	DE WAN (vlan2001.emv1)	172.16.0.0/12	🚍 all	🐻 always	🕢 ALL	✔ 許可	🔉 無効化済み	APP
▲ セキュリティプロファイ >					~					SSL
が ☆ システム  >	SNAT	譜 LAN (port18.vlan101)	譜 WAN (vlan2001.emv1)	<b>192.168.1.2/32</b>	100.0.0.2/32	L <b>e</b> always	LEU ALL	✔ 許可	♥ 無効化済み	AV WEB
・ セキュリティファブリッ										APP
● _ · · · · · · · · · · · · · · · · · ·										SSL
■ ログ&レポート >	user-defined-policy-1	Se LAN (port18.vlan101)	WAN (vlan2001.emv1)	172.16.0.0/12	💷 all	🐻 always	I ALL	✔ 許可	(ii) 160.248.241.1/32	SSL
	LAN -> WAN	DE LAN (port18.vlan101)	과품 WAN (vlan2001.emv1)	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	🗐 all	<table-cell> always</table-cell>	😱 ALL	✔ 許可	160.248.241.1/32	AV WEB APP SSL
	暗黙の拒否	🗆 any	🗆 any	🗐 all	🗐 all	🐻 always	I ALL	⊘ 拒否		
	・ 0. ヤキュリティレーティー ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	トノブ問題						⊋ 変更が保存され	れました。 <u>取り消し</u> 。	×
	0 27 2 7 7 7 0 - 7 4	> > (P)/AZ					_			



72

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。


Master's ONE<sup>®</sup>

- 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	140.227.17.254/32
カラー	
タイプ	サブネット ▼
IP/ネットマスク	140.227.17.254/32
インターフェース	🗆 any 🗸 👻
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



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

新規アドレス		
名前	nttpc.co.jp	
カラー	·····································	
タイプ	FQDN	
FQDN	www.nttpc.co.jp	
インターフェース	🗆 any 💌	
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	,

#### 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。





## 変更対象のアドレスをダブルクリックする。

TEST-NWUTM-FG01A 🔹	≡ Q			VDOM: 🙆 user01 -	>_ 0 - ↓ - ⊖ user01 -
🙆 ダッシュボード 🔹 🔸	◆新規作成 ▼ 🖌 編集 ╞ → CLIで編集 📔 クローン	會 削除 使索	Q		
	名前 ≑	詳細⇔	インターフェースキ	タイプ 🗢	参照≑
💄 ポリシー&オブジェクト 🔷 🗸		17.E1E.100.101/0E		TIPA	
・ ファイアウォールポリシー	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
	100.64.0.0/16	100.64.0.0/16		アドレス	0
1 ンターネット リーヒステ ータベース	100.88.18.0/29	100.88.18.0/29		アドレス	0
サービス	172.16.0.0/12	172.16.0.0/12		アドレス	2
パーチャルJP	I72.17.1.0/24	172.17.1.0/24		アドレス	1
	I72.17.2.0/24	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
• システム >	172.17.253.184/30	172.17.253.184/30		アドレス	0
🛞 セキュリティファブリック ゝ	192.168.0.0/16	192.168.0.0/16		アドレス	5
回 ログ&レポート >	⊒ 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	0.0.0.0/0		アドレス	0
	FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0		アドレス	0
	SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210		アドレス	2
	🔄 all	0.0.0.0/0		アドレス	19
	Ø none	0.0.0.0/32		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
	アドレスグループ 37				U

### 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	192.168.0.10
カラー	· 変更
タイプ	サブネット 🗸
IP/ネットマスク	192.168.0.10 255.255.255.255
インターフェース	🗆 any 💌
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



- 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



削除したいアドレスをクリックし、削除をクリックする。

TEST-NWUTM-FG01A 🔹	≡ Q			VDOM: 💁 user01 -	≻_ 😧 • 🎝 • 😝 user01 •
🙆 ダッシュボード 🔹 🕻	◆新規作成 → 🖌 編集 >_ CLIで編集 🕒 クローン 🚺	自 削除 検索	Q		
	名前令	詳細 ⇔	インターフェースキ	タイプキ	参照⇔
🖹 ポリシー&オブジェクト 🗸 🗸	□ 5_PC 93.200	192.168.93.200/32		アドレス	1 *
ファイアウォールポリシー	5_PC 93.202	192.168.93.202/32		アドレス	1
アドレス 🏠	5_PC 93.203	192.168.93.203/32		アドレス	1
	5_PC 93.205	192.168.93.205/32		アドレス	1
ータペース	5_PC 93.206	192.168.93.206/32		アドレス	1
	5_PC 93.207	192.168.93.207/32		アドレス	1
	Image: Example 2 = 5_PC 93.208	192.168.93.208/32		アドレス	1
🔒 セキュリティプロファイル ゝ	E 5_PC 240.121	192.168.240.121/32		アドレス	2
🔹 システム	5_PC 240.122	192.168.240.122/32		アドレス	2
🐠 セキュリティファプリック ゝ	8.8.8.8	8.8.8/32		アドレス	0
■ ログ&レポート >	2.1入モネクストFTP 49.212.136.151	49.212.136.151/32		アドレス	0
	10.0.0.0	10.0.0.0/8		アドレス	0
	10.0.0.0/8	10.0.0.0/8		アドレス	2
	27.85.149.184	27.85.149.184/32		アドレス	0
	100.64.0.0/16	100.64.0.0/16		アドレス	0
	100.88.18.0/29	100.88.18.0/29		アドレス	0
	172.16.0.0/12	172.16.0.0/12		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
		400.470.0.0/47			
FIGRTINET V7.2.7	0 セキュリティレーティング问題			90	% 🐨 史新治が: 16:16:59 🖸

### ③ 確認ウィンドウがでるので、OK をクリックします。

TEST-NWUTM-FG01A -	≡ Q.			VDOM: 🛆 user01 - >_ 😯 - 🎝 - 😝 user01 -
🗈 ダッシュボード 🔹 🔉	➡新規作成 ▼ ● 編集   >_ CLIで編集   ■ クローン	會 削除 検索	Q	確認 ×
	名前令	詳細 ⇔	インターフェース章	
🖹 ポリシー&オブジェクト 🗸 🗸	□ 5 PC 93.200	192.168.93.200/32		▲ 選択した要素を削除してもよろしいですか?
ファイアウォールポリシー	□ 5 PC 93,202	192.168.93.202/32		
アドレス 🏠	□ = - □ 5_PC 93.203	192.168.93.203/32		
インターネットサービスデ	Image: 2000 million = 1000 million = 10000 million = 1000 million = 10000 million = 1000 million = 10000 million = 1000 million = 10000 million = 10000 million = 10000	192.168.93.205/32		
ータペース	Image: 200 million = 100 m	192.168.93.206/32		
サービス	5_PC 93.207	192.168.93.207/32		
パーチャルIP	5_PC 93.208	192.168.93.208/32		
🔒 セキュリティプロファイル ゝ	□ 5_PC 240.121	192.168.240.121/32		
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	5_PC 240.122	192.168.240.122/32		
🕼 セキュリティファプリック ゝ	8.8.8.8	8.8.8.8/32		
U ログ&レポート >	国 8_13 長本の大トFTP 49.212.136.151	49.212.136.151/32		
	10.0.0.0	10.0.0/8		
	10.0.0/8	10.0.0/8		
	27.85.149.184	27.85.149.184/32		
	100.64.0.0/16	100.64.0.0/16		
	100.88.18.0/29	100.88.18.0/29		
	172.16.0.0/12	172.16.0.0/12		
	172.17.1.0/24	172.17.1.0/24		
	172.17.2.0/24	172.17.2.0/24		
	172.17.253.180/30	172.17.253.180/30		
	172.17.253.184/30	172.17.253.184/30		
	0 セキュリティレーティング問題	400.470.0.0747		OK キャンセル



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。

TEST-NWUTM-FG01A 🔹	. ≡ <i>c</i>			VDOM: 🚳 user	01 • ≻_ 😧 • 🗘 • 😝 user01 •
🙆 ダッシュボード 🔹 🔸	+新規作成 → / 編集 >_ CLIで編集	■ クローン	٩		
	アドレス	詳細⇔	インターフェース 🗢	タイプキ	参照≑
🖹 ポリシー&オブジェクト 🗸 🗸	アドレスグループ				
ファイアウォールポリシー	Ⅰ IP範囲/サブネット 210				
アドレス 🏠	ア ➡ アドレスグループ 37				
インターネットサービスデ ータベース					
サービス					
パーチャルIP					
🔒 セキュリティプロファイル ゝ					
<ul> <li>システム</li> <li>&gt;</li> </ul>					
Ø セキュリティファブリック >					
□□ □グ&レポート >					
	0 セキュリティレーティング問題				366 更新済み: 16:21:14 2



 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。

新規アドレスグループ			
グループ名	リスト1		
カラー			
タイプ 🚯	グループ フォルダ	_	
メンバー	□ 172.160.0/12 ¥ □ 192.168.0.0/16 ¥ +		
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		
		ОК	キャンセル

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。

🐺 TEST-NWUTM-FG01A 🛛 🔹	≡ Q.			VDOM: ❹ user01 ▾	>_ @ • △ • ⊕ user01 •
🙆 ダッシュボード 🔹 🔪	+新規作成 → 編集 >_ CLIで編集	クローン 倉 削除 検索	Q		
	名前◆	詳細⇔	インターフェースキ	タイプ 🌣	参照≑
■ ポリシー&オブジェクト マ ファイアウォールポリシー		5_PC 93.105			A
		5_PC 93.106			
アドレス 🔓	1 6_PC 240 x Grp	5_PC 240.121		アドレスグループ	1
インターネットサービスデ		5_PC 240.122			
-9/	叠 6_PC Grp Grp	區 6_PC 1.x Grp 區 6 PC 10.x Grp		アドレスグループ	0
		■ 6_PC 20.x Grp			
バーチャルIP		69 6_PC 2403 Grp			
	🐴 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
<ul> <li></li></ul>	🐴 G Suite	gmail.com mvildcard.google.com		アドレスグループ	0
	墻 Group3	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>		アドレスグループ	0
	看 Microsoft Office 365	<ul> <li>login.microsoftonline.com</li> <li>login.microsoft.com</li> <li>login.windows.net</li> </ul>		アドレスグループ	0
	🐴 Src Black list	Øf none		アドレスグループ	1
	🐴 Src White list	Øf none		アドレスグループ	1
	🖷 test group	test server		アドレスグループ	0
	看 Uスト1	<ul> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> <li>192.168.0.1</li> </ul>		アドレスグループ	0
	0 セキュリティレーティング問題			1	00% 🚳 更新済み: 16:27:25 🕃

### 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	疆 変更	
タイプ 🚯	グループ フォルダ	
-71/2	□ 172.16.0.0/12 ¥ □ 192.168.0.0/16 ¥ +	
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。

TEST-NWUTM-FG01A 🔹	≣ Q. VDOM: Δ use01+ → Ø+ ↓+ Ø use01				
🙆 ダッシュボード 🔹 🔸	◆新規作成 ◆ / 編集 >_ CLIで編集 ● クロ	コーン 前前除 検索	Q		
	名前⇔	詳細 ≑	インターフェース 🌣	タイプ 🗢	参照⇔
🖹 ポリシー&オプジェクト 🗸 🗸		5_PC 93.103			A
ファイアウォールポリシー		5_PC 93.105			
アドレス 🏠		49			
インターネットサービスデ ータベース	叠 6_PC 240 x Grp	<ul> <li>5_PC 240.121</li> <li>5_PC 240.122</li> </ul>		アドレスグループ	1
サービス	糧 6_PC Grp Grp	5_PC 1x Grp		アドレスグループ	0
パーチャルIP		™ 6_PC 10.x Grp			
🔒 セキュリティプロファイル 🔸		雪 6_PC 240.x Grp 69			
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	獨 Dst Black list			アドレスグループ	1
Ø セキュリティファブリック ♪	🚳 Dst White list	👜 test FQDN		アドレスグループ	1
■ ログ&レポート >	階 G Suite	<ul> <li>gmail.com</li> <li>wildcard.google.com</li> </ul>		アドレスグループ	0
	n Group3	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>		アドレスグループ	0
	🐴 Microsoft Office 365	<ul> <li>login.microsoftonline.com</li> <li>login.microsoft.com</li> <li>login.windows.net</li> </ul>		アドレスグループ	0
	🖥 Src Black list	Ø none		アドレスグループ	1
	🐴 Src White list	Ø none		アドレスグループ	1
	🐴 test group	😑 test server		アドレスグループ	0
	局 リスト1	172.16.0.0/12 192.168.0.0/16		アドレスグループ	0

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。
 投入したい分選択したら 0K 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。

TEST-NWUTM-FG01A 🔹				VDOM: 🚭 user01 🔹	>_ 3 • ♀ • • user01 •
🙆 ダッシュボード 🔹 🔉	+新規作成 → 🥒 編集 >_ CLIで編集 📑 クロ	コーン 直 削除   検索	Q		
	名前◆	詳細 ⇔	インターフェースキ	タイプキ	参照◆
島 ポリシー&オブジェクト 🔷 🗸		5_PC 93.103			
ファイアウォールポリシー		5_PC 93.105			
アドレス 🔓		<b>O</b>			
インターネットサービスデ ータベース	№ 6_PC 240 x Grp	<ul> <li>5_PC 240.121</li> <li>5_PC 240.122</li> </ul>		アドレスグループ	1
サービス	😼 6_PC Grp Grp	1 6_PC 1 x Grp		アドレスグループ	0
パーチャルIP		™ 6_PC 10X Grp ™ 6_PC 20X Grp			
🔒 セキュリティプロファイル ゝ		% 6_PC 240.x Grp			
<ul> <li>システム</li> <li>&gt;</li> </ul>	😼 Dst Black list	-		アドレスグループ	1
🐠 セキュリティファブリック ゝ	🐴 Dst White list	👜 test FQDN		アドレスグループ	1
■ ログ&レポート >	7 G Suite	gmail.com     wildcard.google.com		アドレスグループ	0
	🚡 Group3	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>		アドレスグループ	0
	😼 Microsoft Office 365	<ul> <li>login.microsoftonline.com</li> <li>login.microsoft.com</li> <li>login.windows.net</li> </ul>		アドレスグループ	0
	😼 Src Black list	Ø none		アドレスグループ	1
	😼 Src White list	Ø none		アドレスグループ	1
	🚡 test group	test server		アドレスグループ	0
	壇 リスト1	172.16.0.0/12 192.168.0.0/16		アドレスグループ	0

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。
 投入したい分選択したら 0K を押下する。

アドレスグループの編集			
グループ名	Dst Black list		エントリを選択 🗙
カラー	<b>雪</b> 変更		Q google ¥ 并規作成
タイプ 🟮	グループ フォ	ルダ	·····································
メンバー	😐 googleapis.co	om 🗶	□ 1 Chrome更新*gyt1.com ①
	😐 googlevideo	×	S_cybozu www.google.com
		+	🕮 8_cybozu www. <mark>google</mark> apis.com
スタティックルート設定 🛡 🕕			8_Google googleads.g.doubleclick.net
	コメント記人	//255	8 Google td.doubleclick.net
			8 Google www.google.co.jp
		リュレムとも広	S_Google www.googletagmanager.com
		リストから設定	🕮 <mark>google</mark> .com
		する分選択する	googleapis.com
			googlevideo.com
			$ = \mathbf{Z} \mathbb{K} [ \mathbf{Z} \mathbb{Z}^{d} ] = \mathbb{Z}^{d} (1) $
			クローズ
			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。

TEST-NWUTM-FG01A 🔹				VDOM: 🛆 user01 🗸	>_ ? · ∴ · • user01 ·
🙆 ダッシュボード 🛛 🔉	+新規作成 ▼ / 編集 >_ CLIで編集 ● クロ	コーン 自 削除 検索	Q		
	名前 ≑	詳細 🗢	インターフェース 🎈	タイプ 🗢	参照 🕈
🛃 ポリシー&オブジェクト 🗸		□ 5_PC 93.103			
ファイアウォールポリシー		□ 5_PC 93.105 □ 5_PC 93.106			
アドレス 👌		69			
インターネットサービスデ ータベース	ी 6_PC 240 x Grp	<ul> <li>5_PC 240.121</li> <li>5_PC 240.122</li> </ul>		アドレスグループ	1
サービス	糧 6_PC Grp Grp	墙 6_PC 1 x Grp		アドレスグループ	0
パーチャルIP		◎ 6_PC 20 x Grp			
🔒 セキュリティプロファイル ゝ		ធ 6_PC 240.x Grp භ			
<ul> <li>システム</li> <li>&gt;</li> </ul>	Not Black list			アドレスグループ	1
🐠 セキュリティファブリック ゝ	🐴 Dst White list	test FQDN		アドレスグループ	1
■ ログ&レポート >	The G Suite	<ul> <li>gmail.com</li> <li>wildcard.google.com</li> </ul>		アドレスグループ	0
	ng Group3	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>		アドレスグループ	0
	唱 Microsoft Office 365	<ul> <li>login.microsoftonline.com</li> <li>login.microsoft.com</li> <li>login.windows.net</li> </ul>		アドレスグループ	0
	🐴 Src Black list	£6 none		アドレスグループ	1
	🐴 Src White list	Øf none		アドレスグループ	1
	🐞 test group	😑 test server		アドレスグループ	0
	播 リスト1	<ul> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>		アドレスグループ	0

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。
 投入したい分選択したら 0K を押下する。

アドレスグループの編集		
グループ名	Src White list	エントリを選択
カラー	遍 交更	Q.検索 + 新規作成
タイプ 🕕	グループフォルダ	アドレス(329)
メンバー	8 none 🗙	😐 *.apple.com 🖋
メンバーの除外		*teams.microsoft.com
スタティックルート設定 ①		I ≉.teans.com
	コメント記入	😐 *nttpc.co.jp
	0/255	1_Adobe *.adobe.com
		□ 1_Chrome拡張機能 chrome.google.com
		Ⅲ 1_Chrome拡張機能 clients2.google.co
	リフレムと記点	Ⅲ 1_Chrome拡張機能 clients2.googleuse
	リストから設定	I_Chrome拡張機能 www.google.com
	する分選択する	😐 1_Chrome拡張機能? jnn-pa.googleapis
		I_Chrome拡張機能? update.googleapi
		I_Chrome確認 *googleapis.com
		クローズ
		OK キャンセル



- 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。

TEST-NWUTM-FG01A 🔹				VDOM: 📤 user01 🕶	>_ @ • ● user01 •
🙆 ダッシュボード 💦 👌	+新規作成 ▼ / 編集 >_ CLIで編集 「	クローン	Q		
	名前 ≑	詳細 🗢	インターフェース 🕈	タイプ 🗢	参照≑
🛃 ポリシー&オブジェクト 🗸 🗸		5_PC 68.122			A
ファイアウォールポリシー	糧 6_PC 93.x Grp	5_PC 93.102		アドレスグループ	1
アドレス 🔂		E 5_PC 93.103 E 5_PC 93.105			
インターネットサービスデ ータベース		<ul> <li>□ 5_PC 93.106</li> <li>●9</li> </ul>			
サービス	№ 6_PC 240.x Grp	<ul> <li>5_PC 240.121</li> <li>5_PC 240.122</li> </ul>		アドレスグループ	1
パーチャルIP	🐴 6_PC Grp Grp	1 6_PC 1.x Grp		アドレスグループ	0
セキュリティブロファイル >		雪 6_PC 10.x Grp 雪 6_PC 20.x Grp			
• \$775 <b>}</b>		獨 6_PC 240.x Grp			
⑦ セキュリティファブリック >	B. Det Black liet	•		アドレスグリープ	1
■ ログ&レポート >	Det Unite list			アドレスグループ	1
	🐴 G Suite	<ul> <li>gmail.com</li> <li>wildcard.google.com</li> </ul>		アドレスグループ	0
	n Group3	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>		アドレスグループ	0
	囁 Microsoft Office 365	<ul> <li>login.microsoftonline.com</li> <li>login.microsoft.com</li> <li>login.windows.net</li> </ul>		アドレスグループ	0
	🐴 Src Black list	Ø none		アドレスグループ	1
	🐴 Src White list	Ø none		アドレスグループ	1
	🐴 test group	📮 test server		アドレスグループ	0

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。
 投入したい分選択したら 0K を押下する。

グループ名	Dst White list	エントリを選択
カラー	验 変更	Q. 検索 + 新規作成
タイプ 🚯	グループ フォルダ	アドレス(329)
メンバー	+	📟 *apple.com
メンバーの除外		*teams.microsoft.com
スタティックルート設定		I *teans.com
コメント	コメント記入 // 0/255	💷 *nttpc.co.jp
		1_Adobe *.adobe.com
		I 1_Chrome拡張機能 chrome.google.com
		I_Chrome拡張機能 clients2.google.co
		I_Chrome拡張機能 clients2.googleuse
		I_Chrome拡張機能 www.google.com
	リストから設定	定 🔰 📟 1_Chrome拡張機能? jnn-pa.googleapis
		I_Chrome拡張機能? update.googleapi.
	9る分迭択9る	る 🔛 1_Chrome確認 *googleapis.com 🖋
		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。
- 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。

TEST-NWUTM-FG01A 🔹	≡ Q.			VDOM: 🚭 user01 🕶	>_ @ •
🙆 ダッシュボード 🔹 🔉	◆新規作成 → // 編集 >_ CLIで編集 // クロ	>  直 削除  検索	Q		
	名前⇔	詳細令	インターフェースキ	タイプキ	参照令
<ul> <li>■ ポリシー&amp;オブジェクト マ</li> <li>ファイアウォールポリシー</li> <li>アドレス ☆</li> </ul>		<ul> <li>□ 5.PC 93.103</li> <li>□ 5.PC 93.105</li> <li>□ 5.PC 93.106</li> </ul>			A
インターネットサービスデ ータベース	№ 6_PC 240 x Grp	<ul> <li>5_PC 240.121</li> <li>5_PC 240.122</li> </ul>		アドレスグループ	1
サービス パーチャルはР ▲ セキュリティブロファイル →	囁 6_PC Grp Grp	<ul> <li><sup>™</sup> 6_PC 1x Grp</li> <li><sup>™</sup> 6_PC 10x Grp</li> <li><sup>™</sup> 6_PC 20x Grp</li> <li><sup>™</sup> 6_PC 240x Grp</li> </ul>		アドレスグループ	0
<ul><li>システム</li></ul>	ng Dst Black list			アドレスグループ	1
🧶 セキュリティファプリック ゝ	🖷 Dst White list	test FQDN		アドレスグループ	1
■ ログ&レポート >	🐴 G Suite	gmail.com     wildcard.google.com		アドレスグループ	0
	s Group3	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>		アドレスグループ	0
	Sector Microsoft Office 365	<ul> <li>login.microsoftonline.com</li> <li>login.microsoft.com</li> <li>login.windows.net</li> </ul>		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
	雪 リスト1	<ul> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>		アドレスグループ	0
	0 セキュリティレーティング問題			10	00% 🚳 更新済み: 16:54:00 🕃

### ③ 確認ウィンドウがでるので、OK をクリックします。

TEST-NWUTM-FG01A 🔹				VDOM: 🛆 user01 • >_ 🕜 • 🗘 • 😝 user01 •
🙆 ダッシュボード 🔹 🔉	+新規作成 → 🥒 編集 >_ CLIで編集 📔 クロ	コーン 薗 削除   検索	Q	確認 ×
	名前令	詳細 ≎	インターフェース令	
📙 ポリシー&オブジェクト 🗸 🗸		□ 5_PC 93.103		▲ 選択した要素を削除してもようしいですカ?
ファイアウォールポリシー		□ 5_PC 93.105 □ 5 PC 93.106		
アドレス 🏠		0		
インターネットサービスデ ータベース	唱 6_PC 240 x Grp	5_PC 240.121 5_PC 240.122		1
サービス	幅 6_PC Grp Grp	局 6_PC1x Grp		7
パーチャルIP		· 雪 6_PC 20x Grp 雪 6_PC 20x Grp		
🔒 セキュリティプロファイル ゝ		™ 6_PC 240.x Grp ©		
🌣 システム 🔹 🔹	Dst Black list			-
⊘ セキュリティファブリック ゝ	뛐 Dst White list	💷 test FQDN		2
■ログ&レポート >	雪 G Suite	<ul> <li>gmail.com</li> <li>wildcard.google.com</li> </ul>		
	彊 Group3	<ul> <li>□ 10.0.0.0/8</li> <li>□ 172.16.0.0/12</li> <li>□ 192.168.0.0/16</li> </ul>		2
	Nicrosoft Office 365	<ul> <li>login.microsoftonline.com</li> <li>login.microsoft.com</li> <li>login.windows.net</li> </ul>		2
	🐴 Src Black list	& none		2
	🖷 Src White list	ß' none		2
	🐴 testgroup	test server		2
	雪 リスト1	<ul><li>172.16.0.0/12</li><li>192.168.0.0/16</li></ul>		1
	0 セキュリティレーティング問題			OK キャンセル



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。

+ 新規作成 🥒 編集 📕 クローン	<ul> <li>(1) 刑除</li> <li>(1) Q 検索</li> </ul>			٩	サービス サービスグループ
名前 ≑	詳細 ⇔	IP/FQDN ≑	カテゴリ ≑	プロトコルキ	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 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	<b>一般</b>	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 DNS	TCP/53 UDP/53	0.0.0.0	ネットワークサービス	TCP/UDP/SCTP	4
ESP ESP	IP/50		Tunneling	1P	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 🗸	≡ Q	
	● FortiGateの時刻が同期していません。	
🙆 ダッシュボード 💦 👌	新規サービス	
	名前 HTTPS_1	
□ ホリシーをオノシェクト マ ファイアウォールポリシー	コメント コメント記入 20/255 カラー Q 変更	
アドレス	カテゴリ Uncategorized 🔹	
インターネットサービスデ ータベース	プロトコルオプション	
サービス 🏠	プロトコルタイプ TCP/UDP/SCTP ▼	
バーチャルIP 🕁	アドレス IP範囲 FQDN 0.0.0.0	
🔒 セキュリティプロファイル ゝ	宛先ポート TCP ▼ 443 - High	
🔹 ୬ステム 💦 👌		
🕼 セキュリティファブリック ゝ		
ш ログ&レポート >		
	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。





変更したいサービスをダブルクリックする。

TEST-NWUTM-FG01A	· ≡ Q				VDOM: 🙆 user01 •	_ 🛛 • Д • 😝 user01 •
		0 F	ortiGateの時刻が同期していません。			
🙆 ダッシュボード 🛛 🗧	+ 新規作成 / 編集 🕑 クローン	前 削除 ○ Q 検索			Q	サービス サービスグループ
⊕ ネットワーク	名前≑	\$ <b>羊</b> 紙 \$	IP/FQDN \$	カテゴリ \$	プロトコルキ	夢照⇔
A ボリシー&オプジェクト・	ONC-RPC	TCP/111 UDP/111	0.0.0.0	リモートアクセス	TCP/UDP/SCTP	0
ファイアウォールポリシー	OSPF	IP/89		ネットワークサービス	IP	0
アドレス	PC-Anywhere	TCP/5631 UDP/5632	0.0.0.0	リモートアクセス	TCP/UDP/SCTP	0
インターネットサービスデ ータベーフ	D PING	ICMP/ANY		ネットワークサービス	ICMP	0
**	POP3	TCP/110	0.0.0.0	Eメール	TCP/UDP/SCTP	1
J CA 1	POP3S	TCP/995	0.0.0.0	Eメール	TCP/UDP/SCTP	1
	D PPTP	TCP/1723	0.0.0.0	Tunneling	TCP/UDP/SCTP	0
■ セキュリティブロンアイル :	1 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	ASSE.	TCP/UDP/SCTP	0
セキュリティファブリック:	RADIUS-OLD	UDP/1645 UDP/1646	0.0.0.0	未分類	TCP/UDP/SCTP	0
ビログ&レポート	RAUDIO	UDP/7070	0.0.0.0	未分類	TCP/UDP/SCTP	0
	RDP 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
	D RIP	UDP/520	0.0.0.0	ネットワークサービス	TCP/UDP/SCTP	0
	RLOGIN	TCP/513:512-1023	0.0.0.0	未分類	TCP/UDP/SCTP	0
	RSH	TCP/514:512-1023	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	VolP, Messaging & Other Applications	TCP/UDP/SCTP	0
	SIP 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
	T	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     2     変更       カデゴリ     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 0.0.00 宛先ポート TCP ▼ 110 - High び 送信元ポートを指定 ●	
	ОК +721



- 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

占 ポリシー&オブジェクト	~
ファイアウォールポリシー	
アドレス	
インターネットサービスデ ータベース	
サービス・	습
バーチャルIP	

② 削除するサービスをクリックし削除を押下する。

+ 新規作成・ 🖌 編集  幅 クローン	/ 💼 削除 🍄 カテゴリ設定 検	索
サービス名●	詳細 🌒	IP/FQDN
General 5		
<b>Q</b> ALL	ANY	
ALL_TCP	TCP/1-65535	0.0.0.0
Q 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。

確認		×
A	選択した 要素 を削除してもよろしいですか?	
	OK Cancel	



# 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
アンチウイルススキャン      ①      ブロック      モニタ
機能セット フローベース プロキシベース
インスペクションされるプロトコル
HTTP 💽
SMTP 🕥
POP3 O
FTP O
SSH 🦉 🔘
APTプロテクションオプション
コンテンツ無害化 🤨 🕄 💿 💿 💿
Eメール添付のWindows実行ファイル 😗 🔿
FortiSandboxに検査のためファイルを送信 🖲 🔘
FortiNDRに検査のためファイルを送信 😰 🖲 🕥
モバイルマルウェアプロテクションを含める 🜑
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 🕥
外部マルウェアブロックリストを使用 のうちょう アンドロックリストを使用 のうちょう アンド・シート アンド・シート アンド・シート アンド・シート アンド・シート
EMS脅威フィードの使用 🕴 のうまた のうまた しょうしょう しょう
ОК キャンセル



- 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。

名前車	コメントキ	スコープキ	参照章
W 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	
W default		O VDOM	2

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。

ок	キャンセル



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フィルタブロファイルの編集	
名前 default	
コメント コメント記入	/ 0/255
機能セット フローベース フ	
● FortiGuardカデゴリベースの	フィルタ
<ul> <li>第可</li> <li>第三夕</li> </ul>	ブロック 🔺 警告 👛 認証
名前	アクション
🔲 ローカルカデゴリ 😢	
custom1	<ul> <li>無効</li> </ul>
custom2	<ul> <li>無効</li> </ul>
□ 違法性の高いサイト 😢	
業物乱用	
ハッキング	
違法または非倫理的	
差別	● モニタ ▼
	0% (22)
カテゴリ使用クォータ 🕑 🖯	
◆新規作成 ● 編集 🔒	
カテゴリキ	クォータ合計 🌣
エントリがあ	りません
エントリがあ	りません
エントリが後	りません ()
エントリがる	りません () () () () () () () () () () () () ()
エントリがる ・ ユーザにブロックされたカデ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	りません し ゴリのオーバーライドを許可する
エントリがる コーザにブロックされたカテ ロサーチエンジン	りません し ゴリのオーバーライドを許可する
エントリがる ユーザにブロックされたカテ ロ サーチエンジン ロ スタティックURLフィルタ	りません ① ゴリのオーバーライドを許可する
エントリがる ① ユーザにブロックされたカテ ② 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	ゆません  ゴリのオーバーライドを許可する
エントリがあ ・ ユーザにブロックされたカテ ・ 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	ゆません  ゴリのオーバーライドを許可する  
エントリがる コーザにブロックされたカテ サーチエンジン スタティックURLフィルタ 無効はURLをブロック URLフィルタ FortiSandboxにより検知された夢	ゆません  ゴリのオーバーライドを許可する  急のあるURLをブロック ①
エントリが後 コーザにブロックされたカテ 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により検知された感 コンテンツフィルタ	ゆません し ゴリのオーバーライドを許可する 急のあるURLをブロック ①
エントリが感 コーザにブロックされたカテ 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により検知された感 コンテンツフィルタ しーティングオブション	ゆません ① ゴリのオーバーライドを許可する ③ 急のあるURLをブロック ③



- 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	🗐 all	o always	д ALL	✔ 許可	160.248.241.1/32	AV default	🛛 ಕನ್ನ	2.18 MB	スタンダー
	192.168.0.0/16						APP default ss. certificate-inspection			

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。

+新規作成 ● 編集 ■ クローン 首 削除 検索			
名前♥	◆ イベズロ	スコープ 🗢	参照 🗢
web g-default	Default web filtering.	グローバット	
web default	Default web filtering.	▲ VDOM	1
web g-wifi-default	Default configuration for offloading WiFi traffic.		

 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。



Master's ONE°

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。

♥許可	● モニタ	🖉 ブロック	▲ 警告	▲ 認証
	名前		アク	ション
∃ ローカルオ	カテゴリ 2	)		
□ 違法性の高	いサイト	12		
薬物乱用			⊘₹I	-9
ハッキング			@ =:	_9
違法または非体	倫理的		⊘ ₹1	
差別			@ ==	ニタ
明示的な暴力			@ Ŧ:	_夕
過激派グルー	プ		⊘ ₹1	<b>_</b> 夕
プロキシ回避			⊘ ₹:	_夕
				0% 93

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。

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	7 🕥
コンテンツフィルタ	



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

スタティック	7URLフィルタ			
無効なURLをブロ	]ック 💽			
URLフィルタ				
➡新規作成	☞ 編集 👘	削除検索		Q
URL	タイプ	アクション	ステータス	
	I>	トリがありません		
				0
FortiSandbox(こ	いり検知された悪	意のあるURLをブロッ	ク 🛈	
コンテンツフィノ	L9			



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

新規URLフィル	LA
URL タイプ アクション ステータス	www.nttpc.co.jpシンプル正規表現ワイルドカード除外(exempt)ブロック許可有効無効
	OK キャンセル

※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。

アプリケーションセンサーの編集	
▲ 112個のクラウ 1個のポリシー	ウドアプリケーションはディーブインスペクションが必要です。 -がこのプロファイルを使用しています。 ▐
名前 default コメント	0/255
カテゴリ	
<ul> <li>● モニタ・ すべてのカテゴリ</li> </ul>	
👁 - Business (156 🛆 6)	Cloud.IT (62, (2) 1)
Collaboration (270, △ 17)	👁 - Email (76, 🛆 11)
Game (84)	General.Interest (242, △ 12)
Mobile (3)	• Network.Service (336)
P2P (55)	Proxy (181)
Remote.Access (97)	Social.Media (114, 29)
Storage.Backup (155, △ 19)	• Update (48)
Video/Audio (151, △ 17)	• VoIP (24)
● - Web.Client (24)	●・ 不明なアプリケーション
③ 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・	۲۴
➡新規作成 ● 編集	
ブライオリティ 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	
デフォルト以外のボートで検知されたアプ	リケーションをブロック 🚯 🕥
DNSトラフィックの許可とログ	0
HTTPベースアプリケーションの差し替えメ	(ッセージ の



- 10.1 アプリケーションコントロールの設定

<ul> <li>+新規作成 ◎ 確認 ■ クローン 自 削除 検索</li> <li>Q</li> </ul>				
名前 ♥	コメント 🌩	スコープキ	参照♥	
APP g-default	Monitor all applications.	グローバル		
APP g-wifi-default	Default configuration for offloading WiFi traffic.	グローバル		
APP 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		
<ul> <li>Business (179,          <u>6</u>)</li> <li>Email (87,          <u>12</u>)</li> <li>Mobile (3)</li> <li>Proxy (106)</li> <li>Storage.Backup (296,          <u>16</u>)</li> <li>VolP (31)</li> </ul>	<ul> <li>Cloud.IT (31)</li> <li>Game (124)</li> <li>Network.Service (332)</li> <li>Remote.Access (91)</li> <li>Update (48)</li> <li>Web.Client (18)</li> </ul>	<ul> <li>Collaboration (293, △ 6)</li> <li>General.Interest (241, △ 9)</li> <li>モニタ</li> <li>許可</li> <li>ブロック</li> <li>陽離</li> <li>ジグネチャを表示(241)</li> </ul>
○ ネットワークプロトコルの強制		🗅 クラウドシグネチャを表示(9)

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。

● モニタ・ すべてのカテゴリ		
● ▼ Business (179, △ 6)	✓ Cloud.IT (31)	Solution (293, △ 6)
<ul> <li>●</li></ul>	● - Game (124)	👁 🕶 General.Interest (241, 🛆 9)
● ▼ Mobile (3)	<ul> <li>Network.Service (332)</li> </ul>	● ▼ P2P (85)
Proxy (106)	<ul> <li>Remote.Access (91)</li> </ul>	<ul> <li>Social.Media (150,</li></ul>
<ul> <li>Storage.Backup (296,</li></ul>	<ul> <li>Update (48)</li> </ul>	<ul> <li>Video/Audio (206, △ 13)</li> </ul>
● ▼ VoIP (31)	●	● ▼ 不明なアプリケーション



- 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

7	アプリケーションとフィルタのオーバーライド					
	◆新規作成 🖋 編集 💼 削除					
	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					

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。

新規オーバ	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 🗸						
耳すべて	の結果を追加 🕇 選択したもの	Dを追加 youtube		×Q	選択済み 🛈	すべて	クラウド
۲	名前 🗣	カテゴリ ≑	テクノロジー 🗢	ポピュラリテ	÷	リスク	\$
🗆 アプリ	ケーション シグネチャ <mark>(11/2414</mark> )						
	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	****			
							11/2,414
		ок	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

新規オーバ	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 🗸				
<b>■</b> すべて	の結果を追加 youtube		×Q	選択済み	すべて クラウド
۲	名前 ≑	カテゴリ 🗢	テクノロジー 🖨	ポピュラリティー 🗢	リスク 🗢
🛛 アプリ	ケーション シグネチャ <mark>(11/2414</mark> )				
	YouTube	Video/Audio	Browser-Based	****	
	YouTube_Channel.Access.	Video/Audio	Browser-Based	****	
	YouTube_Comment.Posting	Video/Audio	Browser-Based	★★☆☆☆	
0	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	****	
					11/2.414
					11/2,414
		ОК	キャンセル		

作成されたことを確認する。

+新規作成   ● 削除					
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	🖉 ブロック		
			0		

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。

➡新規作成	編集		
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	⊘ ブロック
			0



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 ▼				
<b>二</b> すべて	の結果を追加 🗕 選択したもの	)を追加 youtube		× Q 選択済み 1	すべて クラウド
•	名前 🗣	カテゴリ 🗢	テクノロジー 🗢	ポピュラリティー 🌲	リスク 🗢
🗉 アプリ	ケーション シグネチャ <mark>(11/2414</mark> )				
	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	<b>★★★</b> ☆☆	
	YouTube_Video.Upload	Video/Audio	Browser-Based	<b>★★★</b> ☆☆	
	Youtube.Downloader.YTD	Video/Audio	Client-Server	****	
					<b>T</b> 11/2,414
		ОК	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 🔻				
<b>調</b> すべて	の結果を追加 youtube		×Q	選択済み 2	すべて クラウド
•	名前 🗣	カテゴリ ≑	テクノロジー 🗢	ポピュラリティー 🖨	リスク 🗢
🛛 アプリク	テーション シグネチャ <mark>11/2414</mark> )				
	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	***	
0	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	****	
					11/2,414
		ОК	キャンセル		

追加されたことを確認する。

◆新規作成 ● 編集 ● 削除					
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。

+新規作成 ● 編集 @ 削除									
プライオリティ	詳細	タイプ	アクション						
1	YouTube_HD.Streaming YouTube_Video.Access 屳	アプリケーション	🖉 ブロック						
			0						



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。

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 🕶				
- 選択したものを削除 検索		Q	選択済み 2	すべて クラウド
名前 ♥	カテゴリ 🗢	テクノロジー 🗢	ポピュラリティー 🗢	リスク 🗢
🖻 アプリケーション シグネチャ 2				
YouTube_HD.Streaming	Video/Audio	Browser-Based	****	
YouTube_Video.Access 🗅	Video/Audio	Browser-Based	****	
				2
		OK キャンセル		

#### 対象のシグネチャが削除されたことを確認する。

➡新規作成 🖋	編集 👜 削除		
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
			0

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	g-default			
コメント	Prevent critica	l attacks. // 25/25	5	
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				
詳細 除外IP	アクション	パケットロギング		
SEV	🌣 デフォルト	😢 無効化済み		
		0		
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	無効 ブロック モニ	9	
		■ botnet package (こ 2	458個のIPアドレス。	
			ОК	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。

Eメールフィルタ	プロファイルの編集						
名前 コメント		default Malware and p	default Malware and phishing URL				
機能セット スパム検知とフ-	ィルタリングを有効化	70-ベース と <b>O</b>	⊿35 プロキシベース	5/255			
Johana	ごとのスパム検知						
วือหวาม ว	びムアクション	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]				
SIMTP	転送 ▼	サブジェクト 👻 🏾 [	Spam]				
🕒 FortiGuard2	マパムフィルタリング	Ž					
🛢 ローカルスノ	ペムフィルタリング						
HELO DNSルック	לעידל 🕥						
リターンEメール ブロック/許可リ	JDNSチェック 🕥 スト 🔹 💽						
➡新規作成	✓ 編集	Ř					
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				
			8				
						ОК	キャンセル

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。

TEST-NWUTM-FG01A •	≡ Q.		VDOM: 🛆 user01 • • >.	- 🛛 • 🗘 • 😝 user01 •
🙆 ダッシュボード 🔹 🔸	●新規作成 ✔ 編集 ■ クローン 言 削除 検索	٩		
ネットワーク >	名前≑	サイベト		参照≑
💄 ポリシー&オブジェクト 🔹 🔉	🐖 default	Malware and phishing URL filtering.	0	
🔮 セキュリティプロファイル 🗸	EF test		0	
アンチウイルス				
Webフィルタ				
アプリケーションコントロ ール				
侵入防止				
Eメールフィルタ 🖒				
アプリケーションシグネチ ヤ				



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	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	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

ローカルスパムコ	フィルタリング		
HELO DNSルックアッ	ນプ 🕕		
リターンEメールDN:	Sチェック 🖜		
ブロック/許可リスト	. 💽		
➡新規作成	▶ 編集		
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
			6

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

アンチスパムのブロ	コック/許可リストエントリを作成
<u> </u>	
91)	受信者アドレス    ▼
パターンタイプ	ワイルドカード 正規表現
パターン	
アクション	拒否としてマーク スパムとしてマーク クリアとしてマーク
ステータス 🜑	
	OK キャンセル

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。

🖹 ポリシー&オブジェクト	~
ファイアウォールポリシー	슜
アドレス	
インターネットサービスデ ータベース	
サービス	
バーチャルIP	

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	パイト	タイプ
🖃 🎀 LAN (port18.vlan10	1) → ാ∰ WAN (vlan20	01.emv1) 10								
dnat test 😳	192.168.0.0/16	🖀 test	🐻 always	🖬 ALL	✔ 許可	(a) 160.248.241.1/32	55. no-inspection	📀 すべて	0 B	スタンダード
Src Black Rule	写 Src Black list	🗐 all	🖸 always	🖬 ALL	⊘ 拒否			🛛 すべて	0 B	スタンダード
Dst Black Rule	💷 all	퉠 Dst Black list	🖸 always	🖬 ALL	⊘ 拒否			🕏 ಕ್ಷನ	0 B	スタンダード
Src White Rule	写 Src White list	💷 all	🐻 always	🖬 ALL	✔ 許可	(a) 160.248.241.1/32	ss. no-inspection	🕏 すべて	0 B	スタンダード
Dst White Rule	🚍 all	🐴 Dst White list	🖸 always	🖬 ALL	✔ 許可	(a) 160.248.241.1/32	ss. 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	55L no-inspection	🕏 কৃ্র্র্ব্ব	0 B	スタンダード
test	⊑ all	⊑ all	🖸 always	n All	✔ 許可	B 160.248.241.1/32	AV default WEB default APP default SSL certificate-inspection	🛛 इंग्रेंट	37.67 MB	- スタンダード
LAN→WAN	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	🗐 all	🖪 always	😱 ALL	✔ 許可		AV     default       WEB     default       APP     default       SSL     certificate-inspection	🕑 র্শবে	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	(a) 160.248.241.1/32	ss. certificate-inspection	📀 すべて	0 B	スタンダード
🖃 🥞 WAN (vlan2001.em	iv1) → 🎀 LAN (port18	svlan101) 1								
test1	💷 all	💷 all	🐻 always	🖬 ALL	✔ 許可	● 有効化済み	55L no-inspection	🛡 ОТМ	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。

※使入防止(IFS)を有効化する場合はg-defaultを迭折する。	IPS)を有効化する場合は g-default を選択	するこ。
------------------------------------	-----------------------------	------

セキュリティプロファイル				
アンチウイルス	🔍 🗛 default	▼ #*		
Webフィルタ	C web default	<b>▼</b> s*		
ビデオフィルタ				
アプリケーションコントロール	L 💽 🔤 default	▼ get		
IPS	💽 📧 g-default	<b>▼</b> #*		
Eメールフィルタ	C EF default	<b>▼ s</b> t		
SSLインスペクション	55L certificate-inspe	ection 💌		
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	<ul> <li>すべてのセッション</li> </ul>		
セッション開始時にログを生成	¢Ο.			
コメント コメント記入	0/1023			
このポリシーを有効化 🜑				
			OK	キャンオル
				++700

- 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。




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	パイト	タイプ
🖃 🇯 LAN (port 18.vlan 10	1) → 3 WAN (vlan20	01.emv1) 10								
dnat test 😳	192.168.0.0/16	lest 🍘	🗔 always	😨 ALL	✔ 許可	3 160.248.241.1/32	551 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	写 Dst Black list	🖸 always	д 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	ss. no-inspection	📀 すべて	0 B	スタンダード
Dst White Rule	😑 all	写 Dst White list	🖸 always	😱 ALL	✔ 許可	160.248.241.1/32	ss. 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	ss. no-inspection	🔮 すべて	0 B	スタンダード
test	😑 all	🗐 all	o always	🖬 ALL	✔ 許可	⑥ 160.248.241.1/32	AV default WEB default AVP default SSL certificate-inspection	🔮 इ॑ぺॅट	37.67 MB	━ スタンダード
LAN→WAN	<ul> <li>10.0.0.0/8</li> <li>172.16.0.0/12</li> <li>192.168.0.0/16</li> </ul>	🚍 all	🐻 always	🖬 ALL	✔ 許可		AV default wee default APP default se certificate-inspection	🔮 কেন্বে	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	ss. certificate-inspection	🔮 すべて	0 B	スタンダード
🖃 🎀 WAN (vlan2001.em	v1) →೫ LAN (port18	.vlan101) (1								
test1	😑 all	😑 all	🖸 always	🖬 ALL	✔ 許可	◎ 有効化済み	ss. no-inspection	🛡 ОТМ	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	sst certificate-inspection
ロギングオプション	
許可トラフィックをログ	<ul> <li>セキュリティイベント すべてのセッション</li> </ul>
セッション開始時にログを生成	
コメント コメント記入	<i>∞</i> 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。



🕺 Master's ONE°

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。



112

### 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	Ø	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	<b>#</b> 30:7c:5e:fa:8c:02	🔜 20.189.173.12 (v10.events.data.microsoft.com)	Hicrosoft.Portal	✔ 768 B / 0 B
5 分前		192.168.0.2	<b>#</b> 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	<b>4</b> 30:7c:5e:fa:8c:02	• 210.150.254.130	DNS	✓ 75 B / 205 B
5 分前		192.168.0.2	<b>#</b> 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。

🐺 TEST-NWUTM-FG01A 🛛 👻					VDOM: 🚭 user01 -	≻_ ଡ• ⊹••	\rm e user01 -
🙆 ダッシュボード 💦 👌	Summary ログ						
	1.503イベント					O FortiAnalyzer •	()1時間 -
🛃 ポリシー&オブジェクト 🔹 🔹						,,	
🔒 セキュリティプロファイル ゝ	Webフィルタ R		_	アプリケーションコントロー	L R		
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$			-				
🐠 セキュリティファブリック ゝ	カテゴリの上位	アクション	カウント	カテゴリの上位	アクション	カウント	
山 ログ&レポート 🗸 🗸 🗸	π	パススルー	615	Network.Service	パス	440	
転送トラフィック	サーチエンジン・ポータルサイト	パススルー	72	Collaboration	パス	285	- 1
ローカルトラフィック	オンラインミーティング	パススルー	23	Update	パス	20	
スニファートラフィック	コンテンツサーバ	パススルー	8	Web.Client	バス	11	
ZTNAトラフィック	インターネット電話(IP電話)	パススルー	3	General.Interest		91	
システムイベント			17A 1121			<b>m</b>	1021
セキュリティイベント 🏠			0.01			-	
レポート ログ設定	🗟 SSL 🗹		•	☆ アンチウイルス 20			•
	カテゴリの上位	アクション	カウント		イベントなし		
	Logid_62302	信頼されてい ないものとし て終了	8				
			③イベント				
	DNSクエリ e	イベントなし		ファイルフィルタビ	イベントなし、		
FCRTINET v727		1.01.40			1.121.00		v

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

TEST-NWUTM-FG01A -	≣ Q							VDOM: 🗗	user01 - >_ 😮	- ¢-	e user01 -
🙆 ダッシュボード 💦 👌	Summary ログ										
					0	😡 Webフィルタ・	TEST-NW	TM-EG01A •	C FortiAnalyzer •	(1時間 -	□詳細
🖹 ポリシー&オプジェクト 🔹 🔉		- 16	14 /= -			🕜 Webフィルタ			(->	144.6	
🛕 セキュリティプロファイル ゝ	日19/時刻	<u>-</u> -9	达信元	アクション	URL	アプリケーション	シコントロール	U.	1=91-9-	达信	/受信
🌣 システム 🔉	2024/06/03 11:42:36		192.168.0.2	✔ パススルー	https://mobile.events.data.microsoft.com/	SSL SSL				199 B /	́0В 🔒
かれたいのです。 かれたいのでは、 かれたいのです。 かれたいのでは、 ないのでは、 ないの	2024/06/03 11:42:35		192.168.0.2	< パススル−	http://tile-service.weather.microsoft.com/ja-JP/livet	泉 アンチウイルス				213 B/	0 B
い ログトレポート ・	2024/06/03 11:41:33		192.168.0.2	✔ パススルー	https://dns.google/	DNSクエリ				2.23 kE	3/0B
	2024/06/03 11:40:38		192.168.0.2	✔ パススルー	https://dns.google/	D ファイルフィルタ	7			2.27 k	3/0B
転达トラノイツク	2024/06/03 11:40:38		192.168.0.2	✔ パススルー	https://functional.events.data.microsoft.com/	● 侵入防止				1.87 kB	3/0B
ローカルトラフィック	2024/06/03 11:40:16		192.168.0.2	✔ パススルー	https://functional.events.data.microsoft.com/	① アノマリ				1.84 kE	3/0B
スニファートラフィック	2024/06/03 11:40:02		192.168.0.2	✔ パススルー	https://functional.events.data.microsoft.com/	塚 アンチスパム				1.84 kE	3/0B
ZTNAトラフィック	2024/06/03 11:39:33		192.168.0.2	✔ パススルー	https://dns.google/	SSH SSH				2.17 kB	3/0B
システムイベント	2024/06/03 11:39:33		192.168.0.2	✔ パススルー	https://windows.msn.com/	● データ漏えい防止	E	ポータルサイト		508 B /	/0B
セキュリティイベント 🏠	2024/06/03 11:39:33		192.168.0.2	✔ パススルー	https://assets.msn.com/		ーナエノシノ・	ポータルサイト		199 B /	/0B
レポート	2024/06/03 11:39:33		192.168.0.2	✔ パススルー	https://windows.msn.com/	t	ナーチエンジン・	ポータルサイト		508 B /	/0B
	2024/06/03 11:39:32		192.168.0.2	✔ パススルー	https://nav.smartscreen.microsoft.com/	п	r			214 B /	/0B
ロク設定	2024/06/03 11:39:31		192.168.0.2	✔ パススルー	https://dns.google/	п	r			2.20 kE	3/0B
	2024/06/03 11:39:31		192.168.0.2	✔ パススルー	https://functional.events.data.microsoft.com/	п	r			1.84 kE	3/0B
	2024/06/03 11:39:30		192.168.0.2	✔ パススルー	https://api.msn.com/	t	ナーチエンジン・	ポータルサイト		196 B /	/0B
	2024/06/03 11:39:30		192.168.0.2	✔ パススルー	https://go.microsoft.com/	п	r			201 B /	/0B
	2024/06/03 11:39:28		192.168.0.2	✔ パススルー	https://go.microsoft.com/	п	r			201 B /	/0B
	2024/06/03 11:39:27		192.168.0.2	✔ パススルー	https://go.microsoft.com/	п	r			201 B/	/0B
	2024/06/03 11:39:27		192.168.0.2	✔ パススルー	https://go.microsoft.com/	11	r			201 B/	/0B
	2024/06/03 11:39:27		192.168.0.2	✔ パススルー	https://dns.google/	IT		1.82 kB/0 B			
	4										°0% 726

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 道		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



117

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	Ø	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)	Hicrosoft.Portal	pass		
5 分前		192.168.0.2	40.90.184.82 (smartscreen-prod.microsoft.com)	Hicrosoft.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	То	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。

C 7 00	<b>、</b> 検索		
日付/時刻	Ø	2	サービス



## 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/

		ogin to C	acti		×	+						-		×
Ļ	$\rightarrow$	С	0	8	https://msp	016. <b>nttp</b>	c.co.jp/N	ewRepor	rt/	٢	\$	${igsidential}$	$\mathbf{F}$	≡
								Use	er L	Log	gin			
		U	lser Na	ence ime:	r your cacu	user na	me and	passwoi	rabe	210W:				
		P	asswo	rd:										
			Login											

#### 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。

Graph Filters								
Presets:	Last Day V From: 2022-02-23 10:55 To: 2022-02-24 10:55 To Refresh Clear							
Search:	Graphs: Default V Columns: N/A V Thumbnails: Go Clear							

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。