ManageEngine Firewall Analyzer





2024年改訂

■著作権について

本ガイドの著作権は、ゾーホージャパン株式会社が所有しています。

■注意事項

本ガイドの内容は、改良のため、予告なく変更することがあります。 ゾーホージャパン株式会社は本ガイドに関しての一切の責任を負いかねます。 当社はこのガイドを使用することにより引き起こされた偶発的もしくは間接的な損害に ついても責任を負いかねます。

■商標一覧

文中の社名、商品名等は各社の商標または登録商標である場合があります。 Windowsは、米国およびその他の国における米国Microsoft Corp. の登録商標です。 ManageEngineは、ZOHO Corporation Pvt.Ltd社の登録商標です。 なお、本ガイドでは、(R)、TM表記を省略しています。 目次

1		はじめに	
	1.1	Firewall Analyzerについて	6
	1.2	本ガイドについて	6
	1.3	本ガイドの目的と対象読者	6
2		動作環境	
	2.1	ハードウェア要件	7
	2.2	OS要件	8
	2.3	Webブラウザー要件	8
	2.4	ポート要件	
3		FWAのセットアップ	
	3.1	インストーラーのダウンロード	
	3.2	インストール手順(Windows)	
	3.3	インストール手順(Linux)	
	3.4	アンインストール手順	
4		起動と停止	
	4.1	起動、停止に関する注意事項	
	4.2	Windows(起動)	
	4.3	Windows(停止)	
	4.4	Linux(起動)	
	4.5	Linux(停止)	
5		初期設定	
	5.1	Webクライアントへのアクセス	
	5.2	ライセンス適用(保守ユーザー向け)	
	5.3	ログインパスワードの更新とメールサーバー設定	
	5.4	装置登録	
	5	.4.1 FWAにsyslogを直接転送	
	5	.4.2 ファイルインポート	
	5.5	アーカイブ設定	
6		レポート	
	6.1	FWAレポート	
	6	.1.1 イントラネット設定	
	6.2	プロキシレポート	
	6.3	VPNレポート	
	6.4	カスタムレポート(スケジュールレポート)	

6.4.1 スケジュール設定方法	
6.4.2 レポートフィルター	
6.4.3 レポートタイプ	
7 アラートプロファイル設定	48
7.1 通知テンプレートの作成	
7.2 アラートプロファイルの作成	
7.3 通常アラート	
7.4 異常アラート	
7.5 带域	
7.6 SNMP設定	
8 アラート	
8.1 アラート	
8.2 可用性アラート	
8.3 セルフ監視	
9 ルール管理	
9.1 装置ルール設定	
9.2 ルール管理	
9.2.1 概要	
9.2.2 最適化	
9.2.3 クリーンアップ	
9.2.4 並べ替え	
9.2.5 影響	
9.2.6 管理	
9.2.7 比較	
9.2.8 期限切れ通知	
10 コンフィグバックアップ	
10.1 コンフィグバックアップのスケジュール設定手順	
10.2 バックアップ監査	
10.3 比較	
11 ログ検索	
11.1 生ログ設定	
11.2 生ログ検索	
11.3 集約検索	
12 ユーザー管理とロール権限	
12.1 ユーザー管理	
12.2 ロール権限	
12.3 パスワードポリシー	

13 各メニュータブの説明	
13.1 ダッシュボード	
13.1.1 ダッシュボードの新規作成	
13.1.2 ウィジェットの追加、編集、削除	
13.2 インベントリ	
13.2.1 スナップショット画面	
13.3 アラート	
13.4 レポート	
13.5 ルール管理	
13.6 コンプライアンス	
13.7 検索	
13.8 ツール	
13.9 設定	
13.10 サポート(米国)	
14 お問い合わせ窓口と関連資料	
14.1 お問い合わせ窓口	
14.2 関連資料	

1はじめに

1.1 Firewall Analyzerについて

ManageEngine Firewall Analyzerは、マルチベンダーのUTM・ファイアウォール、プロ キシサーバーのログを収集し、一元的に管理するツールです。

収集したログの統計的な可視化や、特定のログを検知した際のアラート発報、ファイア ウォールに設定されているルールの整理、管理を実現します。

1.2 本ガイドについて

本ガイドでは、Firewall Analyzer(以下、FWA)のインストール方法から導入時に必要 な初期設定、製品機能の概要について記載します。 本ガイドは、ビルド12.7.124(2024年1月24日リリース)をもとに作成しています。

FWAのリリースビルドについては、以下をご参照ください。 <u>https://www.manageengine.jp/products/Firewall_Analyzer/support.html#eol</u>

本ガイドに記載の範囲は、FWAの基本的な操作方法です。 一部機能は、本ガイドでは取り扱っておりません。

FWAのユーザーマニュアルは、以下をご参照ください。 <u>https://www.manageengine.jp/products/Firewall_Analyzer/help/</u>

1.3 本ガイドの目的と対象読者

本ガイドは、FWAを購入された方やこれから評価版を使用される方が、本製品の概要 を手早く理解し、ご利用を開始するまでの学習時間を短縮することを目的としていま す。

2動作環境

2.1 ハードウェア要件

最小のハードウェア要件は、以下の通りです。

- CPU: Quad Core 3.5 GHz/ 8 threads以上
- メモリ:8GB以上
- ハードディスク:90GB以上

FWAではログの流量やログの保存期間に応じて、サイジング情報を設定しています。 サイジングの目安は以下をご確認ください。 *ログ流量=1秒間のパケット数

メモリ要件

ログ流量	メモリ
500ログ/秒まで	8GB
500ログ/秒以上	16GB

ハードディスク(保存期間)

ログ流量	1日	1週間	1か月	3か月	6か月	1年間
500ログ/秒	12GB	38GB	100GB	210GB	320GB	630GB
100ログ/秒	18GB	65GB	150GB	400GB	720GB	1.2TB
300ログ/秒	40GB	150GB	440GB	1TB	1.5TB	2.5TB
500ログ/秒	90GB	300GB	720GB	1.8TB	3.4TB	6TB
1000ログ/秒	180GB	640GB	1.4TB	3.5TB	6TB	10.5TB
2000ログ/秒	364GB	1.31TB	3.03TB	7.2TB	13.5TB	21.1TB
3000ログ/秒	546GB	1.97TB	4.5TB	10.8TB	20.3TB	31.6TB

※上記のサーバーサイジングは、OSリソースを考慮しておりません。

※ハードディスクサイズ:アーカイブ+インデックス+データベースサイズ=合計サイズ

*製品のご利用に際し、専用サーバーでご利用いただくことを推奨しています(その他のアプリケーションが同サーバー上で稼働している場合、十分なリソースを確保できない場合があります)。

※ご購入前に、評価版でのご利用環境の検証を推奨します。

※対象装置のsyslogを、サードパーティーのsyslogサーバー経由でFWAサーバーに転送 することは非推奨の構成です。トラブルシューティングの状況に応じて、対象装置から

の直接転送(弊社推奨構成)をご案内する場合がございますので、あらかじめご了承く ださい。

*FWAの機能で、ログ流量を確認することができます。

https://www.manageengine.jp/support/kb/Firewall_Analyzer/?p=2189

2.2 OS要件

FWAのOS要件は、以下の通りです。

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Red Hat Enterprise Linux 8~9.4
- CentOS Stream 9
- Ubuntu Server 20.04 LTS
- Ubuntu Server 22.04 LTS

*64bit版をご利用ください。

*評価期間中のみ、クライアントOSを使用することが可能ですが、スペックや稼働状況 によって動作が遅くなる可能性がございます。なお、<u>本番の運用環境では上記のサー</u> <u>バーOSをご利用ください。</u>

*AWSやAzureなどのクラウド環境、VMwareやHyper-V、XenServerなどの仮想化環境上でも、上記対応OS上であれば運用可能です。ただし、性能に関しては、必ず評価版を利用して製品性能を十分に検証した上で、お客様の性能要件を満たすか確認してください。

2.3 Webブラウザー要件

FWAのWebUIにアクセスする際は、以下のブラウザーをご利用ください。

- Google Chrome(最新版)
- Mozilla Firefox(最新版)
- Microsoft Edge(最新版)

2.4 ポート要件

FWAで使用するポート番号について、以下の表をご確認ください。

用途	ポート番号
WabIII 按結	8060/8061 (TCP)
Web01]安心	HTTP/HTTPS
DB接続	13306 (TCP)
(PostgreSQL)	
SSHD	22 (TCP)
syslogサーバー	1514 (UDP)
ログファイルのインポート	21 (FTP : TCP)
	22(SFTP/SCP:TCP)

3FWAのセットアップ

3.1 インストーラーのダウンロード

WindowsまたはLinux用のインストーラーは、以下のURLからダウンロードしてください。

https://www.manageengine.jp/products/Firewall_Analyzer/download.html

インストール後30日間は、評価版としてすべての機能を使用できます。30日の評価期 間が終了後、正規ライセンスを適用しない場合、自動的に停止します。

3.2 インストール手順(Windows)

インストーラーファイルをダウンロード後、 以下の手順で、Windows環境にFWAをインストールします。

1. インストーラーファイル「ManageEngine_FirewallAnalyzer_64bit.exe」を、イン ストールサーバーに配置

2. 右クリックから管理者権限で実行

以下、インストールウィザードに沿ってインストールを行います。



3. ライセンス条項(英語)を承諾後、[Yes]をクリック

ManageEngine Firewall	×
Please read the following license agreement carefully.	ME
Press the PAGE DOWN key to see the rest of the agreement.	
TERMS OF SALE FOR MANAGEENGINE SOFTWARE PRODUCTS 1. Your Acceptance of the Terms of Sale Thank you for visiting the Zoho Corporation Private Limited ("we" or "Zoho") website, www.manageengine.com (the "Website"). This document ("Terms of Sale") is a legal agreement between you or the entity that you represent ("you") and Zoho, and governs your download and purchase of ManageEngine software products from the Website. PLEASE NOTE THAT YOUR USE OF THE WEBSITE TO DOWNLOAD A SOFTWARE PRODUCT CONSTITUTES ACCEPTANCE OF THE TERMS OF SALE, AND TERMS AND CONDITIONS OF THE END USER LICENSE AGREEMENT PROVIDED BELOW. IF YOU DO NOT AGREE TO THE TERMS OF SALE, OR TERMS OF THE END USER LICENSE	~
Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install ManageEngine Firewall, you must accept this agreement. InstallShield	
< <u>B</u> ack <u>Y</u> es <u>N</u>	0

4. インストールディレクトリパスを指定

デフォルトでは、「C:\Program Files\ManageEngine\OpManager」にインス トールされます。

ManageEngine Firewall	×
Destination Folder	
Select a folder where the application will be installed	ME
Click Next to install in this folder.	
To install in a different folder, click Browse and select another folder.	
You can choose not to install ManageEngine Firewall by clicking Cancel to exit the Installation Wizard	
Destination Folder	
C:¥Program Files¥ManageEngine¥OpManager Brow	/se
InstallShield	
< <u>B</u> ack <u>N</u> ext >	Cancel

 5. WebUIに接続するためのWebサーバー用ポート番号を指定 デフォルトポート番号:8060(HTTP)、8061(HTTPS)

ManageEngine Firewall	×
Port Selection Panel Enter the HTTP and HTTPS ports	ME
Firewall uses 8060 as the default HTTP port a different port please specify the same here	and 8061 as HTTPS Port. If you want to run it on
HTTP Port	8060
HTTPS Port	8061
InstallShield	
	< Back Next > Cancel

6. お客様情報(Registration for Technical Support)を入力 ※スキップ可

ManageEngine Firewall		×
Registration for Technical Support (O Enter Your Details below	ptional)	ME
Name		
E-mail Id		
Phone		
Company Name		
Country	-Select-	~
By clicking 'Next', you agree to ou	r <u>Privacy Policy</u> .	
	< <u>B</u> ack <u>N</u> ext >	Skip

 7. 使用するデータベースを選択し、 [Next] をクリック FWAには、PostgreSQLがバンドルされています。
 *MS SQLを選択する場合、お客様の方で別途ご用意してください。

ManageEngine Firewall			\times
Select the backend database for Firewall			
Firewall supports SQL Server version 2008 and	above		ME
Click next to continue			
POSTGRESQL (Bundled with the Product)			
○ MSSQL			
InstallShield			
	< Back	Next >	Cancel

 アンチウイルスソフトに関するダイアログを確認 インストールサーバー上で、アンチウイルスソフトやバックアップソフトを使用 する場合、データベースの動作に影響を及ぼす可能性があるため、インストール ディレクトリ「ManageEngine」全体をアンチウイルスソフトやバックアップソ

フトの対象から除外してください。

ManageEngine Firewall	×
Select the backend database for Firewall Firewall supports SQL Server version 2008 and above	ME
ManageEngine Firewall	×
Antivirus scanners interfering with database files may a functioning of database. Define exception for the C:¥Users¥Administrator¥Desktop¥FWA¥125334¥OpMa directories in the antivirus scanners.	ffect normal anager
	ОК
InstallShield	Cancel

9. [InstallShield Wizard Complete] が表示されると、インストール完了です。 [Start Server] にチェックを入れた状態で [Finish] をクリックすると、サービ スとしてFWAが起動します。

ManageEngine Firewall	
	InstallShield Wizard Complete The InstallShield Wizard has successfully installed ManageEngine Firewall. Click Finish to exit the wizard.
	 □ View Readme ✓ Start Server Firewall will start now once you click finish.
	Technical support: fwanalyzer-support@manageengine.com
	< Back Finish Cancel

3.3 インストール手順(Linux)

インストーラーファイルをダウンロード後、 以下の手順で、Linux環境にFWAをインストールします。

- 1. インストーラーファイル「ManageEngine_FirewallAnalyzer_64bit.bin」を、イン ストールサーバーに配置
- 以下のコマンドを参考に、インストーラーファイルに実行権限を付与 コマンド: chmod a+x <file-name>
- 3. 以下を実行し、インストールを開始 ./ManageEngine_NetworkConfigurationManager_64bit.bin

[root€]# ./ManageEngine_FirewallAnalyzer_64bit.bin Preparing to install Extracting the JRE from the installer archive Unpacking the JRE Extracting the installation resources from the installer archive Configuring the installer for this system's environment	
Launching installer	
Graphical installers are not supported by the VM. The console mode will be used ins	stead
ManageEngine FireWallAnalyzer (created with InstallAnywhere)	
Preparing CONSOLE Mode Installation	
Introduction	
Welcome to the InstallShield Wizard for ManageEngine FireWallAnalyzer.	
A comprehensive Network, Systems, and Applications Management product that is easy-to-install, easy-to-use, and extremely affordable.	
For help on installation, refer to <u>http://manageengine.</u> com/products/opmanager/help/installation_guide/index.html	
The InstallShield Wizard will install ManageEngine Fire₩allAnalyzer on your computer. To continue, click Next.	
PRESS <enter> TO CONTINUE: []</enter>	

4. ライセンス条項(英語)を確認後、[Y]を入力して続行

14. GENERAL:

If you are a resident of the United States or Canada, this Agreement shall be governed by and interpreted in all respects by the laws of the State of California, without reference to conflict of laws' principles, as such laws are applied to agreements entered into and to be performed entirely within California between California residents. If you are a resident of any other country, this Agreement shall be governed by and interpreted in all respects by the laws of the Republic of India without reference to conflict of laws' principles, as such laws are applied to agreements entered into and to be performed entirely within the Republic of India between residents of the Republic of India. If you are a resident of the United States or Canada, you agree to submit to the personal jurisdiction of the courts in the Northern

PRESS <ENTER> TO CONTINUE:

District of California. If you are a resident of any other country, you agree to submit to the personal jurisdiction of the courts in Chennai, India. This Agreement constitutes the entire agreement between the parties, and supersedes all prior communications, understandings or agreements between the parties. Any waiver or modification of this Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this Agreement is found invalid or unenforceable, the remainder shall be interpreted so as to reasonable effect the intention of the parties. You shall not export the Licensed Software or your application containing the Licensed Software except in compliance with United States export regulations and applicable laws and regulations.

DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N):

- 5. お客様情報(Registration for Technical Support)を任意に入力 ※[N]を入力し、スキップ可
- インストールディレクトリパスとWebUIに接続するためのWebサーバー用ポート 番号を指定
 - ・デフォルトパス:/opt/ManageEngine/OpManager
 - ・デフォルトポート番号:8060(HTTP)、8061(HTTPS)



インストール情報を確認し、Enterをクリック
 「Firewall Analyzer has been successfully installed」が表示されると、インストール完了です。



3.4 アンインストール手順

起動停止方法は、以降の「<u>4起動と停止</u>」をご参照ください。

<u>Windowsの場合</u>

以下の手順で、アンインストールを実施します。

- 1. FWAを停止後、Windowsサーバーの[コントロールパネル] → [プログラムと 機能]を表示
- 2. 「ManageEngine Firewall Analyzer」を選択し、アンインストールを実行
- 3. アンインストール処理が完了後、インストールディレクトリ「ManageEngine」 を削除

*インストールディレクトリを削除できない場合には、タスクマネージャーから関連プロセスを停止させた後、削除してください。

<u>Linuxの場合</u>

以下の手順でアンインストールを実施します。

1. FWAを停止

2. インストールディレクトリ「ManageEngine」を削除

4起動と停止

4.1 起動、停止に関する注意事項

- 定期点検やメンテナンス等により、サーバーを再起動する場合、事前にFWAを 停止した上で実施するようお願いします。
- 製品が停止されていない状態でのサーバー停止は、製品データベースの破損につ ながる恐れがあります。
- アプリケーション起動/停止、サービス起動/停止は、いずれか1つの方法で実施してください。
 アプリケーション起動を実施した場合には、アプリケーション停止を、サービス起動を実施した場合には、サービス停止の実施をお願いします。

4.2 Windows (起動)

※タスクマネージャーで、以下のプロセスが稼働していないことを事前に確認してくだ さい。

- java.exe
- wrapper.exe
- · postgres.exe
- FirewallAnalyzer Traylcon / OpManager Traylcon

<u>アプリケーション起動</u>

- 1. コマンドプロンプトを管理者権限で起動
- 2. FWAインストールディレクトリ/bin/に遷移
- 3. 「run.bat」を実行

モジュールの読み込みが開始されます。

読み込みが完了すると、以下のようなメッセージが表示されます。

Server started in :: [37028 ms] Connect to: [http://localhost:8060]

HTTPSによる接続の場合は、以下のメッセージが表示されます。

Server started in :: [37028 ms] Connect to: [https://localhost:8061]

<u>サービス起動</u>

インストール手順に沿ってインストールすると、FWAはWindowsサービスとして自動 で登録されます。

- Windowsの[コントロールパネル]→[管理ツール]→[サービス]を選択 [管理ツール]が見つからない場合は、services.mscより[サービス]を起動
- 2. サービス一覧に「ManageEngine OpManager」が存在することを確認
- 3. サービス「ManageEngine OpManager」を選択し、「サービスの開始」をクリック

しばらくしてWebUIにアクセスできるようになります。

4.3 Windows (停止)

<u>アプリケーション停止</u>

- 1. コマンドプロンプトを管理者権限で起動
- 2. FWAインストールディレクトリ/bin/に遷移
- 3. 以下2つのコマンドを順に実行 shutdown.bat stopPgSQL.bat

<u>サービス停止</u>

1. Windowsの [コントロールパネル] → [管理ツール] → [サービス] を選択

管理ツールが見つからない場合は、services.mscより[サービス]を起動

- 2. サービス一覧に「ManageEngine OpManager」が存在することを確認
- 3. サービス「ManageEngine OpManager」を選択し、「サービスの停止」をク リック

*停止後、タスクマネージャーで以下のプロセスが残存していないことを確認してくだ さい。

- java.exe
- wrapper.exe
- postgres.exe
- FirewallAnalyzer Traylcon / OpManager Traylcon

4.4 Linux (起動)

<u>アプリケーション起動</u>

- 1. 管理者権限(root)で、インストールサーバーにアクセス
- 2. FWAインストールディレクトリ/bin/に遷移
- 「./run.sh」を実行
 モジュールの読み込みが開始されます。

読み込みが完了すると、以下のようなメッセージが表示されます。

Server started in :: [37028 ms] Connect to: [http://localhost:8060]

HTTPSによる接続の場合は、以下のメッセージが表示されます。

Server started in :: [37028 ms] Connect to: [https://localhost:8061]

<u>サービス起動</u>

以下の手順で、サービス登録および起動を行います。

- 1. 管理者権限(root)で、インストールサーバーにアクセス
- 2. FWAインストールディレクトリ/bin/に遷移
- 3. 以下のコマンドを実行し、サービスとして登録 ./linkAsService.sh
- 4. 以下のコマンドを参考に起動 systemctl start OpManager.service

起動後のステータスは、以下のコマンドで参照します。 systemctl status OpManager.service

4.5 Linux (停止)

<u>アプリケーション停止</u>

- 1. 管理者権限(root)で、インストールサーバーにアクセス
- 2. FWAインストールディレクトリ/bin/に遷移
- 3. 以下2つのコマンドを順に実行 ./shutdown.sh ./stopPgSQL.sh

<u>サービス停止</u>

- 1. 管理者権限(root)で、インストールサーバーにアクセス
- 以下のコマンドを参考に停止 systemctl stop OpManager.service

停止後のステータスは、以下のコマンドで参照します。 systemctl status OpManager.service

5 初期設定

5.1 Webクライアントへのアクセス

FWAを起動後、Webクライアントへアクセスします。

 「<u>2.3 Webブラウザー要件</u>」に記載のブラウザーを開き、以下のいずれかのURL でアクセス http://<ホスト名/サーバーIPアドレスまたはlocalhost>:8060

. https://<ホスト名/サーバーIPアドレスまたはlocalhost>:8061 ※「8060」および「8061」はデフォルトのポート番号です。

2. ログイン画面の表示を確認後、ユーザー名、パスワードを入力 デフォルト: admin/admin

Firewall Analyzer	
✓ ログイン状態の維持 パスワードを忘れた場合	

5.2 ライセンス適用(保守ユーザー向け)

FWAをご契約したユーザー様には、当社ライセンス担当よりご契約内容に応じたライセンスファイル(.xml)をご提供します。

ライセンスファイルを受領後、以下の手順でライセンス適用を行います。

- 1. FWAにログイン後、画面右上のシルエットアイコンをクリック
- [ライセンス登録] タブをクリックし、[参照] で、適用するライセンスファイ ルを選択
- 3. [ライセンス登録]をクリックし、適用

ライセンスファイルを初めて適用すると、HTTPSの有効化および反映のための再起動 を強制するメッセージが表示されます。 [アプリケーションの再起動] をクリックし製 品を再起動後、HTTPSを使用して製品UIにアクセスしてください。

III Firewall Analyzer		\$ ₽ Q ♠ ♥
ダッシュボード インベントリ アラー	レポート ルール管理 コンプライアンス 検索 ツール 設定 サポート(米国)	:
メールサーバー設定 ま マン マン マン マン メールサーバーの正しい設定は、パス ドを忘れた際やその他のメール通知受け 必須です	メールサーバー設定 サーバー名 ポート番号 タイムアウト(の) に ほに 正記動が必要です (の)	
パスワード変更 パスワード変更 ほをれていません Firewall Analyzerと監視するネットワー セキュリティ向上のため、デフォルト ワードの変更は必須となっています		
 2要素認証 2要素認証 セキュリティを確保するため、2要素認 有効化を推奨します。 	セキュ: * * Webアクセスは、HTTPSでのみ利用可能です。アブリケーションを再 起動してください。 * ・ * アブリケーションの再起動 保存	
	解説 ナレッジベース 1. Office 365メールサーバーの設定方法は? 2. Gmailメールサーバーの設定方法は?	

再起動後、メールサーバー設定、adminユーザーのデフォルトパスワードの変更、2要素認証の有効化を推奨する画面が表示されます。

その後、画面右上のシルエットアイコンの [製品] タブでご契約情報(ライセンスタイ プ、会社名、監視可能装置数、有効期限等)を確認してください。

・ご契約内容およびライセンス発行に関するご不明点は、当社ライセンス担当窓口まで ご連絡ください。

連絡先:jp-license@zohocorp.com

・ [設定] → [一般設定] → [セキュリティ設定] → [SSL設定] でHTTPS接続を無効 化することができます。無効化後、製品を再起動します。

5.3 ログインパスワードの更新とメールサーバー設定

FWAにログイン後、adminユーザーアカウントのログインパスワードの更新とメール サーバーの設定を実施します。

※保守ユーザーの場合、ライセンスファイルを適用後に以降の設定が強制されます。

<u>ログインパスワードの変更について</u>

[設定]→[一般設定]→[ユーザー管理]→[ユーザー]画面でadminユーザーをク リックし、新規のパスワードを設定してください。

🔢 Firewall Analyze	er
ダッシュボード インベン	ントリ アラート レポート ルール管理 コンプライアンス 検索 ツール 設定 サポート(米国)
一般設定 ディスカバリー	FWAサーバー システム 設定 セキュリティ その他
メールサーバー設定	フーザー情報を編集
SMSサーバー設定	
ユーザー管理	2
認証	ユーザー設定 詳細
SSH設定	ユーザーロール、認証情報、連絡先詳細を入力して ユーザーにアクセスを許可する装置を設定します
システム設定	ください
リブランディング	アップロード
スナップショット設定	
セルフ監視	役割 ① ユーザータイプ
セキュリティ設定	管理者 マ ローカル認証 マ
プライバシー設定	ユーザー名・ Email ID・
サードパーティ製品の統合	admin
	現在のパスワード・
	パスワード・パスワードポリシーの設定パスワードの再入力・
	Phone Number Phone Number タイムソーン(NFAレルート用)
	キャンオル 四方
	モレンビルはオ

※評価版をご利用の場合、デフォルトパスワードを変更せず7日間以上ログインしていないと、アカウントがロックされログインできなくなります。

<u>メールサーバー設定について</u>

[設定]→[一般設定]→[メールサーバー設定]画面で、ご利用環境のメールサーバーを設定します。

[テストメールの送信]オプションより、設定したメールサーバーの有効性を確認する ためのテストを行うことができます。

🔢 Firewall Analyzer	r								A	i (2 🔺	¢ 😩
ダッシュボード インベント	リアラート	レポート	ルール管理	コンプライフ	シス も	「索 ツール	197E	サポート				:
一般設定 ディスカバリー	FWAサーバー	システム	設定	セキュリティ	その他							
メールサーバー設定 SMSサーバーPDPま	メールサーバー	設定										
プロキシサーバー設定	プライマリメ-	・ルサーバー	セカンダリ	メールサーバー								
OAuthプロバイダー	サーバー名			ボート番号		タイムアウト(#	步)					
ユーザー管理				25		100		? ヘルプ				
総証 サーバー設定	送信元メールアドレ notification@opma	マス (任意項目) inager.com		宛先メール	アドレス		3	oAuthiは、パズワードの代わりにアクセストークンを使用して、 アプリケーションにユーザーアカウントを登録する安全な場面方法 です。Firenal Analyzerは、統可プロパイダーへの統可リクエスト				
SSH設定 システム設定	認证設定 (任意項目	1)						○、必要な場合を増払します。必須コレバオターほンウエストを 検証した後、ユーザーにプロンプトを表示し、アブリケーションの リクエストを認可するかどろかを確認します。ユーザーの確認急、 アプリケーションにアクセストークンが何を訪れ、APIリクエスト				
リブランディング スナップショット設定	認証タイプ ● Basic OA	uth						に使用できるようになります。 要件: ! リダイレクトURLを使用して、クライアントロ/クライアン トシークレット/営びBURLのやセストークンURL/スコープを、認証				
セルフ監視 セキュリティ設定	ユーザー名			パスワード				プロバイダーから感嘆します。MicrosofWoogle Authenticatorの サーバーに対応しています。これるのプロバイダーからアクセスト ークンを生成する方法については、こちらをご覧ください。				
プライバシー設定	セキュアな接続 🤉											
サートハーティ製品の統合 フェールオーバーサーバー	SSLの有効化	TLS 有効化	なし									
	テストメールの	送信										
					キャン	セル 🖗	存					

- ■メールサーバーを設定する目的
- ・定期的なレポートファイルをメールで受信
- ・特定の条件に該当するログを検知した際のアラートメール通知
- ・ログインパスワードを失念した場合、ログイン画面の[パスワードを忘れた場合]よ
- り、指定したメールアドレス宛にパスワードリセット用リンクを通知

■保守ユーザーの場合

ライセンスファイルを適用後、メールサーバー設定およびパスワード更新専用の画面が 自動で表示されます。

5.4 装置登録

FWAに装置を登録する方法は以下の2つがあります。

● FWAにsyslogを直接転送

管理対象装置のsyslog転送先として、FWAのインストールサーバーを指定します。

 ファイルインポート 管理対象装置のsyslogファイルをインポートします。

FWAがログを受信後、「インベントリ」→「装置」画面に自動で装置が追加されます。

※新規インストール後はUIにアクセスすると、装置追加方法のポップアップが表示され ますが、上記1つ目の方法による装置追加を推奨しています。

5.4.1 FWAにsyslogを直接転送

管理対象装置からsyslogを直接転送する場合、以下の2点を設定します。

- syslogサーバー設定(FWA側の設定)
- syslog転送の設定(管理対象装置側の設定)

FWAのsyslogサーバー設定は以下の手順で実施します。

- 1. [設定] → [FWAサーバー] → [syslogサーバー] を表示
- 2. 画面右上の [追加] をクリック
- 3. 任意のプロファイル名、使用するsyslog用ポート番号を入力
- 4. 設定を保存後、プロファイル名、ポート番号が [syslogサーバー] 一覧に追加さ れることを確認

ステータスが[アップ]になっていることを確認してください。[ダウン]の場合、 サーバー上で既にポートが占有されている状態のため、ポートの開放または別ポート番 号の追加が必要です。

🚻 Firewall Analyze	er			1 🛱 Q 🔺 🌣 💲
ダッシュボード インベン	トリ アラート レポート ルール	管理 コンプライアンス 検索 ツール	段定 サポート FWAマニュアル	:
一般設定 ディスカバリー	FWAサーバー システム 設定	セキュリティ その他		
syslogサーバー				
装置ルール	syslogサーバー			ライブパケットカウント 追加
除外条件	メモ: 次のボートでファイアウォールからこのサー	パーにSyslogを転送します。 <u>こちらをクリックして</u> ファイア!	ウォールを設定します。	
認証プロファイル	surlegtt=/[=	#_ \ # =	7=-27	マクション、 ライブruelooドユーアー
接続診断	system y	八 1 圖 7	~ ~ ~~	, , , , , , , , , , , , , , , , , , ,
可用性アラート	SysLogServer-1	1514	アップ	
装置情報	Demo	514	アップ	Ш II 🔍

その後管理対象装置側で、syslog転送先(FWAのインストールサーバー/ポート番号) を設定します。

以下のページでは各ベンダーごとに参考となる設定内容を記載していますが、 コマンドや設定内容の詳細については、ご利用のベンダー様にご確認ください。

・管理対象装置の設定

https://www.manageengine.jp/products/Firewall_Analyzer/help/firewalldevices_configuration.html

*サードパーティベンダーのsyslogサーバーを中継して転送する構成は、弊社では推奨 していません。FWAで問題が発生した際の調査状況に応じて、それ以上の調査が叶わ ず、FW装置からFWAへの直接転送(弊社推奨構成)をご案内する場合がございますの で、あらかじめご了承ください。

5.4.2 ファイルインポート

ログ転送の他、対象装置のログファイルをインポートして取り込む方法があります。 以下の手順でログファイルをインポートします。

- 1. [設定] → [システム] → [ログファイルのインポート] を表示
- 2. 画面右上の [ログのインポート] をクリック
- 以下のオプションよりインポートタイプを選択し、インポートを実施
 ・ローカルホスト
 - ・リモートホスト

<u>ローカルホスト</u>

FWAに接続している端末上(インストールサーバー含む)にログファイルが存在する 場合、本オプションよりインポートを実施します。

ローカルホスト画面では、以下の3つのオプションから選択します。

• ファイル

項目

説明

ファイルの場所	ローカル内に保管されているファイルの場所を指定します。 テキストファイルまたはZipファイルをインポート可能です。 ※ファイルサイズ:最大1GB
未解析/ジャンクレコー	FWAで解析不可なログが含まれている場合、そのレコードはス
ドは無視する	キップし、解析可能なレコードのみを参照します。
	仮想ファイアウォールと物理ファイアウォールを分ける際に使用
次を仮想ファイア	します。
ウォールとする(※)	チェックがない場合、インポートされる装置は物理装置として識
	別されます。
ログファイルを既存の 装置にマッピング	インポート対象の装置がFWAに既に追加されている場合、対象装 置にマージするようインポートします。

🔢 Firewall Analyz	zer								1	4	Q	A <	* 3
ダッシュボード インパ	ベントリ アラート	レポート	ルール管理	コンプライアンス	検索	ツール	設定	サポート(米国)					:
一般設定 ディスカバリー	- FWAサーバー	システム 詰	焼 セキュリ	ティ その他									
ログファイルのインポート													
プロトコルグループ	ログファイルの	Dインボート				グのインボ-	-ト						×
アーカイブファイル	□ ファイル名	リモートホン	ト プロトコル	ステータス	٠	ローカルホスト	עד-	- トホスト					
レポートカスタマイズ DNS						スケジュール	ディレク	フトリ					
業務時間					۰	ファイル							
装置グループ	解説 F/	Q			ファー	イルの場所							
	1. 既存のファィ	、 アウォールやプロキ	シサーバーについて	、ログファイルをイン	ť-			参照					
	2. リモートホス 3. ローカルホス	、トからの「ログのィ 、トからの「ログのィ	ンポート」を、スク ンポート」を、スク	「ジュールするには? 「ジュール実行するには	?	未解析/ジャンク	7レコードは	無視する					
	4.1ディレクト 5.スケジュール	リ内の複数ログファ· ・インポートを開始・	イルをインポートす [.] 停止するには?	るには?		次を仮想ファイ	アウォールさ	とする					
						ログファイルを	既存の装置に	こマッピング 👔					
										キャンセ	JL	インオ	∜−ト

• スケジュール

項目	説明
ファイルの提所	ローカル内に保管されているファイルの場所(パス含む)を指定
	します。
時間間隔(分)、開始	ファイルの参照間隔と開始時刻を指定します。
動的にファイル名を変	日時等、インポート対象のファイル名が動的に変化する場合に
更する	チェックを入れ、ファイル名の変更パターンを入力します。
未解析/ジャンクレコー	FWAで解析不可なログが含まれている場合、そのレコードはス

ドは無視する	キップし、解析可能なレコードのみを参照します。
次を仮想ファイア ウォールとする(※)	仮想ファイアウォールと物理ファイアウォールを分ける際に使用 します。 チェックがない場合、インポートされる装置は物理装置として識 別されます。
ログファイルを既存の 装置にマッピング	インポート対象の装置がFWAに既に追加されている場合、対象装 置にマージするようインポートします。

Filewall Allaly	zer		A 🛄 Q 🔺 🌣 🌡
ダッシュポード イン	ベントリ アラート レポート ルール管理 コンプライアンス	検索 ツール 設定 サポート(米	国)
一般設定 ディスカバリ	ー FWAサーバー システム 設定 セキュリティ その他		
ログファイルのインポート			
プロトコルグループ	ロクファイルのインホート	ロクのインホート	~
アーカイブファイル	□ ファイル名 リモートホスト プロトコル ステータス	 ローカルホスト リモートホスト 	
レポートカスタマイズ			
DNS		スケジュール ディレクトリ	
業務時間		ファイル	
装置グループ	解説 FAQ	ファイルの場所	
	1.既存のファイアウォールやプロキシサーバーについて、ログファイルをインボー	絶対パスとファイル名を入力してください	
	2. リモートホストからの「ログのインボート」を、スケジュールするには?	時間間隔(分)	開始:
	3.ローカルホストからの「ログのインポート」を、スケジュール実行するには?	取得間隔を分単位で指定	時 ▼ 分 ▼
	4.1ティレクトリ内の復数ログファイルをインボートするには?		
		動的にファイル名を変更する	
		✓ 未解析/ジャンクレコードは無視する	
		次を10度ファイア・フォールと9 る	
			キャンセル インホート

• ディレクトリ

項目	説明
ファイルの場所	ファイルが保管されているディレクトリパスを指定
未解析/ジャンクレコー	FWAで解析不可なログが含まれている場合、そのレコードはス
ドは無視する	キップし、解析可能なレコードのみを参照します。
	仮想ファイアウォールと物理ファイアウォールを分ける際に使用
次を仮想ファイア	します。
ウォールとする(※)	チェックがない場合、インポートされる装置は物理装置として識
	別されます。



インストールサーバー上から直接FWAのWebUIにアクセスした場合、[スケジュール] と[ディレクトリ]オプションが表示されます。 リモート端末から接続した場合、こ れら2つのオプションは表示されません。

<u>リモートホスト</u>

ログファイルがローカル端末上ではなくリモート端末上にある場合、本オプションより インポートを実施します。

リモートホスト画面では、以下の項目を指定します。

項目	説明
ホスト名/IPアドレス	リモート端末のホスト名もしくはIPアドレスを入力
ユーザー名、パスワード	リモート端末にアクセスするための認証情報を入力
	アクセス時のプロトコルを選択
プロトコル	• FTP
	· SFTP/SSH
ポート	プロトコル選択時に自動的にポートが反映されます。必要に応じ
	て変更してください。
時間間隔(分)、開始	ファイルの参照間隔と開始時刻を指定します。
ファイルの場所	リモート端末に保管されているファイルの場所を指定

	*ファイルサイズ:最大2GB
動的にファイル名を変更	日時等、インポート対象のファイル名が動的に変化する場合に
する	チェックを入れ、ファイル名の変更パターンを入力します。
未解析/ジャンクレコード	FWAで解析不可なログが含まれている場合、そのレコードはス
は無視する	キップし、解析可能なレコードのみを参照します。
	仮想ファイアウォールと物理ファイアウォールを分ける際に使用
次を仮想ファイアウォー	します。
ルとする(※)	チェックがない場合、インポートされる装置は物理装置として識
	別されます。
ログファイルを既存の装	インポート対象の装置がFWAに既に追加されている場合、対象
置にマッピング	装置にマージするようインポートします。

(*)

[次を仮想ファイアウォールとする] オプションは、VDOMのsyslogファイルをイン ポートする場合に有効化します。

・FWAに既に装置が追加されている場合

本オプションを有効化し、FWAに追加されている既存装置のIPアドレスを入力してイン ポートしてください。

・FWAに装置が追加されていない場合

初めにVDOMのsyslogファイルをインポートし装置追加を行います。それ以降は本オプ ションを有効化の上、追加した装置のIPアドレスを入力してVDOMのsyslogファイルを インポートしてください。

*本オプションを有効化した場合、IPアドレスの入力が必須です。IPアドレスの入力な しにインポートを実施すると、エラーが発生します。

*入力したIPアドレスが、FWAの [インベントリ] 画面に存在しない場合、新規装置と して追加されます。

🏭 Firewall Analyzer 🔗 🗘 🔍 🌲 🕸 🔮					
ダッシュボード インペ 一般設定 ディスカバリー	ントリ アラート レポート ルール管理 コンプライアンス 検索 ツール FWAサーバー システム 設定 セキュリティ その地	20定 サポート(米国)		1	
- 他校 ディスカバレー ログフィルのインボート ブロトコル/レーブ クーカイブブイル レポートカスタマイズ DNS 展開治想 構造グループ	Wukth-Vic 5.252. 設定 ではコリアイ そのき ログファイルのインボート ロ ファイル名 リモートホスト ファールス ステータス MRE FQ 日 日本のカボストやちの「ログタインボートトき」、スクジュールギスでは2 ユーカホボストやちの「ログタインボート」を、スクジュールギスでは2 ユーカホボストやちの「ログタインボート」を、スクジュールギスにな? シスクジュールギンホートを見合いた。 シレモートホストやうの「ログタインボート」を、スクジュールギスには2 シスクジュールインボートを見合いた。 シスクジュールインボートを見合いた。 シスクジュールインボートを見合いた。 シスクジョールインボートを見合いた。	インボート接座 サイズ データがありません	を認知	ユーザー名 ポート 21 ・ 略称: 問 ・ 分 ・ ・	

5.5 アーカイブ設定

FWAは管理対象装置のログを受信後、インストールディレクトリ内にアーカイブファ イルを作成し、定期的にZip化します。

本設定では、受信したログの保存期間やZipファイルの作成間隔を設定します。

・設定画面

[設定] → [システム] → [アーカイブファイル] → [アーカイブ設定]

アーカイブ設定画面には、以下の設定項目があります。

項目	説明	
ファイル作成間隔	管理対象装置からsyslogを受信し、ログファイルを作成する間隔 を指定します。 作成されたアーカイブファイルは、アーカイブ先のhotフォル ダーに保存されます。 *デフォルト:12時間	
Zipファイル作成間隔	 ディスク容量の圧迫を防ぐために、ログファイルのZip化を行う 間隔を指定します。 作成されたZipファイルは、アーカイブ先のcoldフォルダーに保存されます。 ※デフォルト:24時間 	
Zipファイル佐成開始時刻	Zipファイル作成の開始時刻	
--------------------	--	
	*デフォルト:0時0分	
	受信した生ログの保存期間を指定します。	
	期間:1週間、1か月、2か月、3か月、6か月、1年、無期限	
ログ保存期間	*デフォルト:無期限	
	*本設定は、[設定]→[設定]→[データ保存]の[ログアー	
	カイブ]期間と連動しています。	
	生ログのアーカイブファイルの保存先を設定します。	
アーカイブ先変更	チェックを入れると保存先を変更できます。	
	デフォルト:ManageEngine/OpManager/server/default/archive	
ナロガインゴックフ担託	生ログのインデックスファイルの保存先を設定します。	
エロワイフノックス場所	チェックを入れると保存先を変更できます。	
を変更	デフォルト: ManageEngine/OpManager/server/default/indexes	
ートレンジョンマイルな作品	アーカイブ先のhotフォルダーに保存されているアーカイブファ	
フッヽZipノア1ルでTF成 	イルを、即時的にZip化します	

アーカイブ先(archiveフォルダー配下)には、管理対象装置ごとにフォルダーが作成 されており、さらに以下の3つのフォルダーが存在します。

・hotフォルダー

ログを受信してからZipファイルが作成されるまでの最新の生ログが保存されます。

・coldフォルダー

hotフォルダーの生ログデータをZip化したZipファイルが保存されます。

・warmフォルダー

データ参照時に、対象期間の生ログデータを一時的に保管します。1日経過するとwarmフォルダーからは削除されます。

🔢 Firewall Analyzer						Я	¢ Q	A © 3
ダッシュボード インベント 一般設定 ディスカバリー	トリ アラート レポート ルール管理 FWAサーバー システム 設定 セキ:	コンプライアンス 検索 ツール ユリティ その他	設定サポート(米国)					:
ログファイルのインボート プロトコルグループ	アーカイブファイル				アーカイブ設定			×
アーカイブファイル	□ 装置	ファイル名	開始時刻	アーカ				
レポートカスタマイズ	FGT100D186_Sim	/opt/ManageEngine/OpManager/server/default/arc hive/FGT100D186 Sim/cold/FGT100D186 Sim 20	Sun, 19 Jun 2022 00:03	Mon, 20	✓ 生ログアーカイブ			
DNS 樂歌時間		22_06_20_00_04_07.zlp			ファイル作成閣隔:	12.0	B	÷
装置グループ	SRXTest	/opt/ManageEngine/OpManager/server/default/arc hive/SRXTest/cold/SRXTest_2022_06_20_00_04_29. zip	Sun, 19 Jun 2022 00:05	Mon, 20	Zipファイル作成闢構 👔	24.0	B	÷
			Sun, 19 Jun 2022 00:49	Mon, 20	Zipファイル作成開始時刻: 💿	0 時 0	ś	9
				ログ保存期間: ③	無期限	•	*	
	SRXTest	/opt/ManageEngine/OpManager/server/default/arc hive/SRXTest/cold/SRXTest_2022_06_19_00_03_56. zip	Sat, 18 Jun 2022 00:05	Sun, 19				
	GT100D186_Sim	/opt/ManageEngine/OpManager/server/default/arc Sat, 18 Jun 2022 00:03 htwl=CfT100D186_Simicoldi/FCT100D186_Sim_20 22,06,19,00,03,43.stp	アーカイブ先変更 Sun, 19 (Click here for steps to configure network mapped drive.)					
					/opt/ManageEngine/OpManager/server/defau	It/archive		
			Sat, 18 Jun 2022 00:40	Sun, 19				
				生ログインデックス場所を変更	anad datum 3			
	SRXTest	/opt/ManageEngine/OpManager/server/default/arc Fri, 17 Ju hive/SRXTest/cold/SRXTest 2022 06 18 00 03 53	Fri, 17 Jun 2022 00:04 Sat, 18 .	Sat, 18 .	Circk here for steps to configure network map	aped or ive.)		
		zip			/opt/ManageEngine/OpManager/server/defau	lt/indexes		
	GT100D186_Sim	/opt/ManageEngine/OpManager/server/default/arc hive/FGT100D186_Sim/cold/FGT100D186_Sim_20	Fri, 17 Jun 2022 00:03	Sat, 18 .				
		22_06_18_00_03_34.zip			キャンセ	し 今すぐZipファイル	しを作成	保存
			Fri, 17 Jun 2022 00:33	Sat, 18 .				

6レポート

FWAでは、ファイアウォールやプロキシサーバーから受信したログを解析し、各種レ ポートタイプごとに解析データを可視化します。 FWAに実装されている各種レポートタイプについて記載します。

6.1 FWAレポート

[レポート]→[FWAレポート]では、以下のレポートタイプが実装されています。

レポートタイプ	説明
トラフィックレポート	ファイアウォールを通過(permit/accept)した送受信トラ フィック量に基づいた帯域使用率を表示します。
プロトコル使用レポート	ファイアウォールを通過(permit/accept)してトラフィックを 生成しているプロトコルグループの帯域幅使用率を表示します。
Web使用レポート	ファイアウォールを通過(permit/accept)してトラフィックを 生成しているプロトコルグループの内、Webプロトコルグループ

	に特化した帯域幅使用率を表示します。
メール使用レポート	ファイアウォールを通過(permit/accept)してトラフィックを 生成しているプロトコルグループの内、メールプロトコルグルー プに特化した帯域幅使用率を表示します。
FTP使用レポート	ファイアウォールを通過(permit/accept)してトラフィックを 生成しているプロトコルグループの内、ファイル転送プロトコル グループに特化した帯域幅使用率を表示します。
Telnet使用レポート	ファイアウォールを通過(permit/accept)してトラフィックを 生成しているプロトコルグループの内、Telnetプロトコルグルー プに特化した帯域幅使用率を表示します。
ストリーミング・チャッ トサイトレポート	ファイアウォールを通過(permit/accept)してトラフィックを 生成しているプロトコルグループの内、ストリーミングとチャッ トサイト通信に関する帯域幅使用率を表示します。 事前に、後述のイントラネット設定を行う必要があります。
イベント概要レポート	ファイアウォールが生成したイベント(重要度)の概要を表示し ます。
ファイアウォールルール レポート	使用頻度の高いルールや使用されていないルール情報を表示しま す。
受信・送信トラフィック レポート	インバウンドトラフィック(LANに流入するトラフィック)とア ウトバウンドトラフィック(LANから出力されるトラフィック) を分離している場合のトラフィック状況を表示します。 事前に「 <u>6.1.1 イントラネット設定</u> 」を行う必要があります。
イントラネットレポート	内部ホスト(LAN内部のホスト)からのトラフィック情報を表示 します。 事前に「 <u>6.1.1 イントラネット設定</u> 」を行う必要があります。

インターネットレポート	外部ホスト(LAN外部のホスト)からのトラフィック情報を表示 します。 事前に「 <u>6.1.1 イントラネット設定</u> 」を行う必要があります。
セキュリティレポート	ファイアウォールに設定されているルールによって拒否(Deny)された通信を表示します。
ウイルスレポート	ウイルスに関する通信に特化してログ情報を表示します。
攻撃レポート	攻撃に関する通信に特化してログ情報を表示します。
Spamレポート	Spamに関する通信に特化してログ情報を表示します。
プロトコルトレンドレ ポート	各プロトコルグループごとに、使用状況のトレンドを時系列で表 示します。
トラフィックトレンドレ ポート	通信量のトレンドを時系列で表示します。
イベントトレンドレポー ト	イベント数のトレンドを時系列で表示します。
管理者レポート	ファイアウォールのログイン、ログオフ、ログイン拒否に関連す るレポートを表示します。
URLレポート	syslogに含まれるURLのカテゴリを取得し、許可、拒否状況をカ テゴリ単位で表示します。

FWAレポート画面では、以下の各操作を実行することができます。 以下、トラフィックレポート例

1. 出力日時の変更

*トレンドレポートでは、日時指定はできません。

- 送信元、宛先、プロトコルに関するフィルター設定
 ※画面左上の[装置名]で[すべての装置]を選択した場合は表示されません。
- 3. レポート全体のPDF、XLSX、CSVファイル出力、メール送信
- 4. スケジュール出力設定
- 5. DNSによる名前解決(インストールサーバーからアクセス可能なDNSサーバーに DNS解決を行います)
- 6. レポート内のウィジェット単位のPDF、XLSX、CSVファイル出力、メール送信
- 7. 通信の詳細確認(該当ホストやプロトコルを深掘りして、詳細な通信内容を表示 します)



6.1.1 イントラネット設定

組織のネットワーク環境におけるIPアドレス(LAN)を、イントラネットとインター ネットに区別するための設定を行います。

・設定画面

[設定]→[設定]→[イントラネット]

[イントラネット設定] 画面では、FWAに追加されている装置が一覧で表示されます。

装置個別または画面右上の[全装置設定]より、複数装置に一括で設定することができ ます。

対象装置を指定後、イントラネットとして設定するネットワーク範囲を以下の項目より 指定します。

- IPアドレス 単一のホスト/IPアドレスを指定します。
- IPネットワーク
 特定のネットワークを設定する場合に、IPアドレスと対応するサブネットマスクを指定します。
- IPレンジ

IPアドレスを範囲指定する場合に、開始と終了のIPアドレス、対応するサブネットマスクを指定します。

III Firewall Analyzer				1 🔅 Q 🔺 🌣 💲
ダッシュポード インペン	トリ アラート レポート ルール管理 コンプライアンス	検索 ツール 設定 サポート(米国)		:
一般設定 ディスカバリー	FWAサーバー システム 設定 セキュリティ その他			
イントラネット データ保存	イントラネット		イントラネットの設定	×
ライセンス管理	装置名	イントラネット設定	使用可能な装置	選択済みの装置
リボジトリ 除外ホスト	FGT100D186_SIm	IP Range : Start IP :192.168.2.1 End IP :192.168.2.200		FGT100D186_Sim SRXTest
	SRXTest	IP Network : Network :192.168.1.1 Net Mask :255.255.255.0		4
	新課 FAQ		IPレンジ ▼ 開始IPアドレス 終了II	アアドレス 255 255 255 0 🗴
	1. Firewall Analyzerで、イントラネットを設定するには?		追加その他	
				キャンセル 保存

6.2 プロキシレポート

プロキシサーバーのアクセスログを、各カテゴリに分けて収集、可視化します。 [レポート]→[プロキシレポート]では、以下の各レポートタイプが実装されていま す。

レポートタイプ	説明
URLレポート	プロキシサーバーのログに含まれるURLとそのカテゴリ情報をレ ポート化します。
プロキシ使用レポート	プロキシサーバーのキャッシュとステータスコードの使用情報に ついて表示します。
Webサイト詳細レポート	プロキシサーバー経由でアクセスした、Webサイト、ドメイン、 Webページなどの情報を表示します。
トップトーカーレポート	プロキシサーバー経由で通信を行っている上位のホストとユー ザー情報(LAN/WAN)を表示します。

[FWAレポート]と同様に、[プロキシレポート]でも以下の各操作を実施します。

1. 出力日時の変更

- 2. 送信元、宛先、プロトコルに関するフィルター設定
- 3. レポート全体のPDF、XLSX、CSVファイル出力、メール送信
- 4. レポート内のウィジェット単位のPDF、XLSX、CSVファイル出力、メール送信
- 5. スケジュール出力設定
- 6. DNSによる名前解決(インストールサーバーからアクセス可能なDNSサーバーに DNS解決を行います)
- 7. 通信の詳細確認(該当ホストやサイトを深掘りして、詳細な通信内容を表示しま す)

6.3 VPNレポート

収集したVPNログを各カテゴリに分けて可視化します。 [レポート]→ [VPNレポート]には、以下の各レポートタイプが実装されています。

レポートタイプ	説明
アクティブVPNユーザー	リアルタイムでVPN通信を行っているアクティブなユーザーを表

レポート	示します。
VPNセッションレポート	VPN通信が発生したユーザーとそのセッション情報を表示します。
トップユーザーレポート	VPN接続の回数(ヒット数)が多いユーザー情報を表示します。
VPN Usageレポート	VPN接続が行われていたアクティブなセッション数を時系列の折 れ線グラフとして表示します。
VPN Statusレポート	アクティブVPNユーザーレポートが、指定した期間におけるオン ラインのVPN情報(ユーザー名、IP、VPN接続時刻、経過時間) を表示するのに対し、 VPN Statusレポートでは、時間軸のアクティブVPNユーザーの セッション数を表示します。
VPN概要レポート	ー定の期間(日、1時間)のVPNセッション数に焦点をあて、 VPN使用状況を表示します。
VPNレポート	ファイアウォール経由のVPN通信に関するユーザー(上位のユー ザー、VPN接続失敗ユーザー)や使用統計などの情報を表示しま す。
VPNトレンドレポート	VPN接続に成功した一定期間のセッション数に関して、折れ線グ ラフの時系列形式でセッション数を表示します。 *既にセッションがクローズしているVPNセッションが表示対象 です。
アクティブVPNトレンド レポート	VPNトレンドレポートと同様、VPN接続に成功した一定期間の セッション数に関して、折れ線グラフの時系列形式でセッション 数を表示します。 *VPNトレンドレポートの場合、既にセッションがクローズして

いるVPNセッションを表示対象としますが、本レポートの場合、
一定の時間帯でVPNセッションがアクティブなセッション数を表
示します。

6.4 カスタムレポート(スケジュールレポート)

FWAに実装されている各種レポートタイプをスケジュールで定期出力します。

6.4.1 スケジュール設定方法

以下の手順で設定します。

- [レポート]→ [カスタムレポート]→ [レポートプロファイル] 右上の [追加] をクリック
- 2. プロファイル名を任意に入力し、対象装置を選択
- 3. レポートフィルターを任意に指定
- 4. 出力するレポートタイプを選択
 ※ [ウィジェットのカスタマイズ] で [はい] を選択することで、レポート内の
 任意のウィジェットを指定することができます。

🔢 Firewall Analyze	er					*	QI	A 🗘 😩
ダッシュボード インベ	ントリ アラート レポート ルール管理	コンプライアンス 検索 ツ	ール 設定	サポート(米国)				:
カスタムレポート FWAレ	ポート プロキシレポート VPNレポート APIアク	セスー般						
レポートプロファイル スケジュールリスト	レポートプロファイルを追加							
レポートフィルター	プロファイル名							
レポートタイプ								
	✓ すべての装置選択済み(選択した項目を編集)							
	フィルター							
	レポート	レポート	を追加					
	ウィジェットのカスタマイズ: 🌒 いいえ 🔵 はい							
	検索							
	□ すべて選択		1					
	□ トラフィックレポート							
	プロトコル使用レポート							
	── Web使用レポート							
	□ メール使用レポート							
	□ FTP使用レポート							
	 Telnet使用レポート 							

- 5. スケジュールを [有効] にし、レポートタイプ (PDF、CSV、XLS) を選択
- レポートを生成するスケジュール(毎時、日次、週次、月次、1回、カスタム)
 を設定
- メール通知を任意に設定
 ※メール通知を行う場合には、事前に「5.3メールサーバー設定」を設定してくだ

さい。

8. 設定を保存

*保存後、レポートプロファイル一覧に、設定したプロファイルが追加されていることを確認してください。

III Firewall Anal	yzer		A 🛱 Q 🛊 🌣 🍔
ダッシュボード イン	レベントリ アラート	レポート ルール管理 コンプライアンス 検索 ツール 設定 サポート(米国)	:
カスタムレポート FV	/Aレポート プロキシレポー!	ト VPNレポート APIアクセス 一般	
レポートプロファイル	レポートプロファイ	イルを追加	
スケジュールリスト			
レポートフィルター	レポートタイプ	PDF +	
レポートタイプ	指定した時間		
	毎時	以下の指定した時刻より1時間毎にレポートを作成する	
	日次	日時(日)レポート作成	
	週次	10 * 時 00 * 分	
	月次	期間レポート作成:	
	10	18時間的 *	
	+= 5 /		
	リスタム	28 2月 2023 10-00-E8 仁裕 IST	
	3811079 - 77 - P689 . 2	10 V2 2022 100000 T TT 10 10 10	
	✓ メール通知		
	帝先:	(複数のメールアドレスに送る場合、コンマ	
		「」」で区切りを入れてください)	
	件名:	1.4-1.2 228	
	メモ:		

・設定したスケジュールは、 [レポート] → [カスタムレポート] → [スケジュールリ スト] で、ステータスを有効化/無効化できます。

・レポートファイルの保存先は、[設定]→[その他]→[ユーザー設定]→[スケ ジュールレポート保存場所]で指定します。

6.4.2 レポートフィルター

カスタムレポートでプロファイルを作成する際に指定するフィルターを設定します。 フィルター内容は、包含または除外から選択し、プロトコル、送信元/宛先IPアドレ ス、イベント、ユーザー情報を条件に指定します。 レポートフィルター設定により、出力するレポートに含める情報やレポートから除外す る情報を指定します。

III Firewall Analyz	er					A 📄	Q 🛊 🌣 🐍
ダッシュボード インベ	ントリ アラート レポート ルール	言理 コンプライアンス 検索 ツール	設定 サポート(米国)				:
カスタムレポート FWAL レポートプロファイル		APIアクセス 一般					~
スケジュールリスト					追加 ノイルター:		^
レポートフィルター	フィルター名:	タイプ		アクション	フィルター名	フィルタータイプ	
レホートタイン			データがありません		test	23/7/09-	¥
					以下のプロトコルを含める		
					以下の送信元IPアドレス/ホストを含める		
					シングル		
					開始IPアドレス		
					検了IPアドレス・・		
					192.168.1.1>192.168.2.100		
					以下の宛先を含める		
					以下のイベントを含める		
					以下のユーザーを含める		
						キャンセル	Ok

レポートフィルター機能は、カスタムレポートの他に、FWAレポート、プロキシレ ポート、VPNレポートの画面上からも指定できます。

6.4.3 レポートタイプ

各種レポートに含まれる情報(プロトコル、URL、イベント、VPN、ルール、攻撃、ウ イルス、Spam、ホスト、サーバー)に関して、必要な情報のみを選択し、レポートに 出力することができます。

レポートの表示形式は、グラフとテーブル、グラフ、テーブルから選択することができ、グラフを選択した場合には、さらに円グラフや棒グラフを選択することができます。

III Firewall Analy:	zer					1 🗔 Q	A & &
ダッシュボード イン・	ベントリ アラート レポート	ルール管理 コンプライアン	ス 検索 ツール 設定	サポート(米国)			:
	レポート プロキシレポート VPRL レポートタイプ レポート名	ल-⊢ антроед —е	L#-1947	7-9%802W	レポートタイプス レポート名 地田 お示 グラフタイプ メ地 グループ化県件 町/(増え基準	を選択する レポート対象 プロトコル クガランをテーブル グラフ テ・ ログラフ ・ ログラフ ・ ログ ログ ・ ログ ・ ログ ログ ・ ログ ・ ログ ・ ログ ログ ・ ログ ログ ログ ログ ログ ログ ログ ロ	-J)L
					テーブル設定		
						キャンセル	Ok

作成したレポートタイプは、カスタムレポートのレポートプロファイル追加画面のレ ポート一覧に表示されます。

7アラートプロファイル設定

セキュリティ対策や通信の監視を目的に、条件に合致したログイベントが発生した際に 管理者にアラートを通知します。

7.1 通知テンプレートの作成

アラート発生時のアクションを事前にテンプレートとして定義し、アラートプロファイ ルを作成する際に使用します。

- 1. [設定]→[その他]→[通知テンプレート]右上の[追加]をクリック
- 作成するテンプレートタイプを選択 メール、チャット(Slack連携)、syslogプロファイル、トラッププロファイル 等
- 通知先など、各テンプレートタイプに応じた必要項目を入力し、保存 ※以下はメール通知の設定例です。

🔛 Firewall Analyze	r									
ダッシュボード インベン	・トリ アラート	レポート ノ	レール管理	コンプ	ライアンス	検索	ツール	設定	サポート(米国)	
一般設定 ディスカバリー	FWAサーバー	システム 設定	セキ	ニリティ	その他					
SNMP設定	通知テンプレート	> >-11.								
アラートプロファイル	アラート発生時、メールで	通知します。								
ユーザー名-IPマッピング	テンプレート名									
ユーザー設定										
通知テンプレート										
	送信元メールアドレス									
	notification@opmanag	er.com								
	宛先メールアドレス 🤉									
	メール形式									
	● プレーンテキスト	HTML 💽 i	両方							
	() ()			14. 17						
	行る	ヨート1 プロファイル	·* \$54	作石変数						
	054504 705		2. 9FW	変動の通知						
	メッセージ		?	メッセージョ	数					
	プロファイル名: \$Fw 条件: \$FwaField(crite	aField(profileName) ria)		変数の選択			Ŧ			
	詳細:\$FwaField(alert	Msg)								
	厚る			キャンヤル	テスト実行	Ŧ	保存			
	17.2			11200			PRIT			

保存した通知テンプレートは、[通知テンプレート]画面の一覧に追加されます。

7.2 アラートプロファイルの作成

通知テンプレートを作成後、以下の手順でアラートプロファイルを作成します。

1. [設定] → [その他] → [アラートプロファイル] 右上の [追加] をクリック

- 2. プロファイル名を任意に入力
- 3. プロファイルタイプを以下から選択
 - ・通常アラート
 - ・異常アラート
 - ・帯域

*各プロファイルタイプについては、後述の内容をご確認ください。

プロファイルを適用する対象装置を選択
 ※デフォルトではすべての装置が選択されています。

5. [アラート条件の定義] で以下のいずれかを選択

・カスタム:任意の条件を指定します。

・事前定義:各種イベントタイプ(VPN、重要度、攻撃、セキュリティ、ウイル ス、SPAM、管理)に対して、事前にアラート条件を実装しています。

- 6. [しきい値設定]の項目でアラートの優先度、アラート間隔を設定
- 7. 1度のみ通知を送信

アラート発生時に毎回通知を行うか、任意のタイミングで1度のみ通知するか選 択します。

通知を有効にする
 [通知テンプレート]機能で作成したテンプレートを選択します。

7.3 通常アラート

アラート条件を任意にカスタマイズして設定します。 ※前述、「アラートプロファイルの作成」に記載の内容と同様の手順で作成します。

🔢 Firewall Analyz	er
ダッシュボード インベ	シトリ アラート レポート ルール管理 コンプライアンス 検索 ツール 設定 サポート(米国)
一般設定 ディスカバリー	FWAサーバー システム 設定 セキュリティ その他
SNMP設定	アラートプロファイルの追加
アラートプロファイル	
ユーザー名-IPマッピング	プロファイル名 プロファイルタイプ
ユーザー設定	道常アラート
Notification Templates	✓ すべての装置選択済み(選択した項目を編集)
	アラート条件の定義
	● Predefined ● カスタム
	● いずれかの条件に合致 (OR) ── 以下のすべてに一致
	重要度 ▼ 次に等 ▼
	しきい値設定
	優先度: 重大 ▼
	アラート闇隔: イベント生成 分
	管理者副り当て admin y
	しきい値の週用範囲: 💿 すべての選択した装置 🤍 選択したそれぞれの装置
	1度のみ通知を送信 今日 🔹
	Enable Notification
	Template Type テンプレート名
	すべてのテンプレート ▼ 値を選択してください ▼ +
	キャンセル 保存

7.4 異常アラート

NBA (Network Behavior Analysis:ネットワーク動作解析)のようにトラフィックの何らかの異常を検知する場合に選択します。

前述、「アラートプロファイルの作成」の手順4以降の流れを記載します。

- 1. 対象装置を選択
- 2. [アラート条件の定義] で以下の中からレポートタイプを選択し、各条件を設定 ・トラフィックレポート
 - ・攻撃レポート
 - ・ウイルスレポート
 - ・VPNレポート

・URLレポート

- ・ルールレポート
- 3. しきい値設定

対象期間や重要度、異常の有無を確認する時間間隔を指定

- 1度のみ通知を送信
 アラート発生時に毎回通知を行うか、任意のタイミングで1度のみ通知するか選択します。
- 5. 通知を有効にする

[通知テンプレート]機能で作成したテンプレートを選択します。

🔢 Firewall Analyze	r	
ダッシュボード インベン	・トリ アラート レポ	ドート ルール管理 コンプライアンス 検索 ツール 整定 サポート(米国)
一般設定 ディスカバリー	FWAサーバー システム	ム 設定 セキュリティ その他
SNMP設定 アラートプロファイル	アラートプロファイルの	2)追加
ユーザー名-IPマッピング	プロファイル名	プロファイルタイプ
ユーザー設定		風常アラート ▼
通知テンプレート	✓ すべての装置選択済み(選	諸 択した項目を編集)
	アラート条件の定義	
	● 事前定義 ── カスタム	
	異常レポートタイプ	トラフィックレポート
	事前定義 alert	Working Hour Traffic +
	日時	次に等しい * 異説時間 *
	送信元	次に等しい ・ CIDRおよびCSV形式での記述も可能です
	プロトコル	次に等しい *
	宛先	次に等しい ・ CIDRおよびCSV形式での記述も可能です
	ユーザー	次に等しい *
	アプリケーション	次に等しい *
	送信元の国名	次に等しい * 国を選択 *
	宛先の国名	次に等しい * 国を選択 *
	alert 説明 : Alarm occur for Traffic consu	umed in Working Hour
	しきい値設定	
	期間 1時間 🔻	· 、 合計トラフィ… ▼ : すべて ▼ 超過 MB ▼
	しきい値を超えた場合に生成す 要度:	「るアラートの重 重大 *

7.5 帯域

対象装置のインターフェースで使用する帯域の異常を検知します。 前述、「アラートプロファイルの作成」の手順4以降の流れを記載します。

- 1. 対象装置を選択
- 2. アラート条件の定義
 - ・対象のインターフェース

・トラフィックタイプ(受信トラフィック、送信トラフィック、合計トラフィック)

- ・トラフィックの条件、値
- 3. しきい値設定
 - ・優先度
 - ・アラート間隔
 - ・1度のみ通知を送信(任意)
 - ・通知を有効にする(任意)

🔢 Firewall Analyze	er	# 🖾 Q 🔺 🌣
ダッシュポード インベン	ントリ アラート レポート ルール管理 コンプライアンス 検索 ツール 副注 サポート(米田)	
一般設定 ディスカバリー	FWAサーバー システム 設定 セキュリティ その他	
SNMP設定	アラートプロファイルの追加	
アラートプロファイル		
ユーザー名-IPマッピング	プロファイル名 プロファイルタイプ	
ユーザー設定	市域、	
通知テンプレート	観査を道沢してください	
	SRVIķĒ +	
	アラート条件の定義	
	100.16384 マ 受信トラフィック マ マ Gbps マ	
	しきい価級定	
	每午宴•	
	アラート構築: イベント生成 分	
	オーナー割り当て admin v	
	✓ 1度のみ通知を送信 今日 ▼	
	✓ 通知を有効にする	
	テンプレートタイプ テンプレート名	
	すべてのテンプレート * 僅を選択してください * 🛨	
	キャンセル 病母	

帯域アラートを設定するには、後述の「7.6 SNMP設定」を事前に登録する必要があります。

7.6 SNMP設定

FWAでSNMP設定を有効化することにより、以下の機能でSNMPを使用した情報取得を 行います。

- ダッシュボード ファイアウォールライブトラフィック、ファイアウォールインターフェースライ ブトラフィック
- インベントリ
 [帯域] → [ライブトラフィック]
- 帯域アラート
 [設定]→[その他]→[アラートプロファイル]

ダッシュボード、インベントリ配下の上記データについては、syslogの情報をもとに データ表示することも可能です。 SNMP設定を有効にすることで、SNMPをもとに帯域データが取得されます。

以下の手順でSNMP設定を有効化します。

- 1. [設定] → [その他] → [SNMP設定] 画面右上の [追加] をクリック
- 2. 以下の各情報を設定
 - ・装置名:SNMP設定を行う対象装置を選択
 - ・SNMPバージョン:v1/v2/v3から選択

*v3を選択すると、さらに認証設定を入力する画面が表示されます。

- ・SNMPコミュニティ:対象装置に設定されているSNMPコミュニティ名を入力
- SNMPポート:SNMPポート番号を入力
- インターフェースライブレポートにチェックし、更新間隔(1分/5分/10分)を 選択(任意)
- [テスト]をクリックし、入力したSNMP情報に誤りがないことを確認し[保存]

III Firewall Analyze	er				1 🗭 Q 🔺 🌣 🎖
ダッシュボード インベン	ントリ アラート レポート	ルール管理 コンプライアンス 検索	ツール 設定 サポート(米国)		
一般設定 ディスカバリー	FWAサーバー システム	設定 セキュリティ その他			
SNMP設定 アラートプロファイル	SNMP股定			SNMP設定を編集する	×
ユーザー名·IPマッピング	装置名	バージョン	ステータス	装置名	IPアドレス:
ユーザー設定	SRXTest	v2		SRXTest	· 192.168.
通知テンプレート				SNMPバージョン	
	FAQ			V2	*
		りるレポートの内容は2		SNMPコミュニティ	SNMP#
	2.自社のファイアウォールMI	B情報をFirewall Analyzerに取り込むには?		1000	161
				1.#_1.の理想	
				レポート名	インターフェースライブレポート
				更新間隔	5分 *
					[インターフェースライブレポートへ適用]
					キャンセル、テフト

8アラート

FWAで発報されたアラートの確認画面について記載します。

8.1 アラート

「7 アラートプロファイル設定」を設定後、条件に該当するログを検知すると、[ア ラート]タブにアラートが発報され、一覧で表示されます。

その他「8.3 セルフ監視」により発生したアラートも同様にアラート一覧に追加されます。

アラートは、アラートプロファイル設定で指定したアラートの重要度に応じて、色分け で表示されます。

画面左の重要度のアイコンをクリックすることで、重要度に該当するアラートのみが表 示されます。

アラートタブには以下の3つのタブが存在します。

- 発生中のアラート
 アラートプロファイルやセルフ監視により発生したアラートの内、アラートがクリアされていない、発生中のアラートを一覧で表示します。
- すべてのアラート
 アラートプロファイルやセルフ監視により発生したすべてのアラートを一覧で表

示します。セルフ監視のしきい値違反やクリアは、1つのアラートとして集約されます。

• イベント

アラートプロファイルやセルフ監視により発生したすべてのアラートを一覧で表 示します。セルフ監視のしきい値違反やクリアのアラートは、個々のイベントと して表示されます。

III Fin	ewall Analyzer] 🖪 Q		\$
ダッシュ	ボード インベントリ アラート	レポート ルール管理	コンプライアンス 検索	ツール	設定 サポート(米国)					
発生中のフ	アラート すべてのアラート イベント									
	すべてのアラート (53)			î↓					+	Ê ;
53	est_vmx: Number of Mits exce FG1001	个明 不割目 に 里八	1483							
	e test_VPN: Number of Hits exce FG100	不明 未割当て 重大	1年前	Fi	reWall Analyzer ディスク空き容量のし	っきい値違反がクリアされました。現在の値は 10	GBです			
	etest_VPN: Number of Hits exce FG100	不明 未割当て 重大	1年前	Sy	stem					
"	etest_VPN: Number of Hits exce FG1001	不明 未割当て 重大	1年前	17	ルフ監視 :: 確認解除 :: クリア					
2	e test_VPN: Number of Hits exce FG1001	不明 未割当て 重大	1年前							
	e test_VPN: Number of Hits exce FG1001	不明 未割当て 重大	1年前		511202212.55.14 +8055					
0	etest_VPN: Number of Hits exce FG100	不明 未割当て 重大	1年前		イベント ワークフロー メモ	QE	図 ki ele 3 ページ中 [>= M	EM 50	▼を表示
~	e test_VPN: Number of Hits exce FG100	不明 未割当て 重大	1年前		メッセージゥ			ステ	ータス	
•	e test_VPN: Number of Hits exce FG100	不明 未割当て 重大	1年前		FireWall Analyzer ディスク空き容量が 4GB で	す。しきい値(5GB)違反です		8 I	it	
2	e test_VPN: Number of Hits exce FG1001	不明 未割当て 重大	1年前		FireWall Analyzer ディスク空き容量のしきい	直違反がクリアされました。現在の値は13GB です		00	יטד	
	e test_VPN: Number of Hits exce FG100	不明 未割当て 重大	1年前		FireWall Analyzer ディスク空き容量が 3GB で	す。しきい値(5GB)違反です		6 I	大	
	e test_VPN: Number of Hits exce FG1001	不明 未割当て 重大	1年前		FireWall Analyzer ディスク空き容量のしきい	直違反がクリアされました。現在の値は 15GB です		00	יטד	
	e test_VPN: Number of Hits exce FG1001	不明 未割当て 重大	1年前		FireWall Analyzer ディスク空き容量が 3GB で	す。しきい値(5GB)違反です		01	达	
	e test_VPN: Number of Hits exce FG1001	不明 未割当て 重大	1年前	1	FireWall Analyzer ディスク空き容量のしきい	直違反がクリアされました。現在の値は 7GB です		00	עי	
	• test_VPN: Number of Hits exce FG100	不明 未割当て 重大	1年前		FireWall Analyzer ディスク空き容量が 2GB で	す。しきい値(5GB)違反です		(3) #	i大	
	e test_VPN: Number of Hits exce FG100	不明 未割当て 重大	1年前		FireWall Analyzer ディスク空き容量のしきい	直違反がクリアされました。現在の値は6GB です		00	יעד	
	etest_VPN: Number of Hits exce FG100	不明 未割当て 重大	1年前		FireWall Analyzer ディスク空き容量が 3GB で	す。しきい値(5GB)違反です		(3) ii	大	
	etest_VPN: Number of Hits exce FG100	不明 未割当て 重大	1年前		FireWall Analyzer ディスク空き容量のしきい	直違反がクリアされました。現在の値は 9GB です		00	עי	
	etest_VPN: Number of Hits exce FG100	不明 未割当て 重大	1年前		FireWall Analyzer ディスク空き容量が 4GB で	す。しきい値(5GB)違反です		0 1	达	
	etest_VPN: Number of Hits exce FG1001	不明 未割当て 重大	1年前		FireWall Analyzer ディスク空き容量のしきい	直違反がクリアされました。現在の値は5GBです		00	עד	
	est_VPN: Number of Hits exce FG1001	不明 未割当て 重大	1年前		FireWall Analyzer ディスク空き容量が 2GB で	す。しきい値(5GB)違反です		0 1	i大	
	etest_VPN: Number of Hits exce FG1001	不明 未割当て 重大	1年前		FireWall Analyzer ディスク空き容量のしきい	直違反がクリアされました。現在の値は8GB です		0 2	עי	
	 ポーリングに応答しました 192.168 } 	不明 未割当て クリア	1年前	2	FireWall Analyzer ディスク空き容量が 4GB で	す。しまい値(5GB)遍反です		0 1	达	
		1 ページ目 100 マ	53 件中 1 - 53 を表示							

対象のアラートをクリックすることで、アラートが発生するトリガーとなった通信情報 や条件が表示されます。

8.2 可用性アラート

対象装置から一定時間ログを受信していない場合に、アラートを発報し管理者にメール 通知します。

以下の手順で、可用性アラートを設定します。

1. [設定] → [FWAサーバー] → [可用性アラート] を表示し、画面右上の [追 加] をクリック

2. 以下の各項目を設定

·対象装置

・x分間ログがありません(15分、30分、1時間、2時間、6時間、12時間、1 日)

※指定した時間、対象装置からログ受信がない場合に、アラートを発報します。
・アラート発生時のアクション(メール送信)

3. 各項目を設定後、[保存]をクリック

・可用性アラートが発報された際は、指定したアクション(メール送信)のみが実行され、FWA上の[アラート]には表示されません。

・メール通知アクションの設定にあたり、事前にメールサーバー設定を実施してくださ い。

Firewall Analyzer ダッシュボード インペント!	リ アラート レポート ルール管理 コンフ	プライアンス 検索 ツール	設定 サポート			<i>≰</i> ⊈ Q ≜ ⇔ &
一般設定 ディスカバリー syslogサーバー	FWAサーバー システム 設定 セキュリテ	ィーその他				
装置ルール	可用性アラート				アラート追加	×
除外条件	装置名	メールアドレス	電話番号	BƏMƏMƏRA (使用可能な装置	選択した装置
認証プロファイル	FG	vcom		60		FortiGate-FW
接続診断		a.com		360		
可用性アラート 装置情報			_			✓ FG
	解説 FAQ					FG ~
	1. ファイアウォールからsyslog受信ができない場合に、ア	'ラート発信する設定の方法は?			×分間ログがありません	u 15分 ▼
					✓ メール送	メール
					信尤	(複数のメールアドレスに送る場合、コンマ「」ア反切りたみわてください)
					SMS送信	件名:
						ファイアウォール 可用性 alert [オプション]
						キャンセル 保存

8.3 セルフ監視

FWAのインストールサーバー自体のCPUやディスク空き容量を監視します。

[設定]→[一般設定]→[セルフ監視]画面で、以下の各項目を設定します。

<u>CPU監視</u>

- 監視間隔(5分/10分/15分/30分/60分)
- Java CPU使用率(しきい値%、連続回数、メール通知、アラート表示)
- PostgreSQL CPU使用率(しきい値%、連続回数、メール通知、アラート表示)
- システムCPU(しきい値%、連続回数、メール通知、アラート表示)

<u>ディスク空き容量</u>

- 監視間隔(任意の分数を設定指定)
- Firewall Analyzerのディスク空き容量のアラートを作成する(しきい値GB)

🗰 Firewall Analyzer											A	Ç Q	A @ (
ダッシュボード インベントリ	アラート	レポート	ルール管理	コンプライアンス	検索	ツール	設定	サポート					
一般設定 ディスカバリー	FWAサーバー	システム	設定	セキュリティ そ	の他								
メールサーバー設定 SMSサーバー設定	セルフ監視												
プロキシサーバー設定 OAuth プロバイダー	✔ CPU監視					60	* 分	•	連続回数	JL-K	直面	にアラートを	表示
ユーザー管理	Java CPU使用	×				> 90	%		2	~		~	
1212	PostgreSQL C	PU使用率				> 90	%		2	~		~	
サーバー設定	システムCPU					> 90	%		2	~		\checkmark	
SSH設定	✓ ディスク空き	容量を監視				30	分	2		~		~	
システム設定 リブランディング	Firewall Analy	/zerのディスク空	き容量のアラー	トを作成する		< 5	GB						
スナップショット設定													
セルフ監視											キャン	コル	保存
セキュリティ設定													
プライバシー設定													
サードパーティ製品の統合													

9ルール管理

ファイアウォールに設定されている既存ルール(ポリシー)の関連性を可視化し、ルー ル設定を最適化します。

また、新規ルールを追加する際、既存ルールとの関連性を事前に把握するために使用します。

9.1 装置ルール設定

[ルール管理]機能を使用するために、対象装置のルール、コンフィグ情報を事前に取 得する必要があります。

装置ルールの取得は、[設定]→[FWAサーバー]→[装置ルール]画面右上の[追加]より実施します。

取得方法には以下の3つがあります。

- CLIベース
- ファイルインポート
- API

ベンダーごとの使用可能な方法については、以下のサポートページをご確認ください。 <u>https://www.manageengine.jp/products/Firewall_Analyzer/SupportedFW.html#rule_management</u>

以下の手順で装置ルールを設定します。

<u>CLIベース</u>

- 1. [装置選択]より対象装置を選択し、取得方法 [CLI] を選択
- 2. 対象装置に接続する認証情報(プロトコル、IPアドレス、ログイン名、パスワー ド等)を入力し、[テスト]をクリック

装置認証情報の追加		
装置選択:		取得方法:
SRXTest	*	CLI
認証プロファイル		
選択なし	Ŧ	•
認証: ● プライマリー 追加情報		
プロトコル		ファイアウォールのIPアドレス
SSH	Ŧ	192.168.x.x
ログイン名:		パスワード
admin		•••••
プロンプト	?	
>		

3. 検証に成功後、 [ルール/コンフィグ取得をスケジュール] を任意に設定 以下の例では毎日0時00分に、最新情報を自動で取得します。



<u>ファイルインポート</u>

- 1. [装置選択]より対象装置を選択し、取得方法 [ファイル]を選択
- ルール情報を含むファイルまたはコンフィグ情報を含むファイルを各インポート オプションから選択し、インポートを実施

装置認証情報の追加					
装置選択:		取得方法:			
FortiGate-FW	*	ファイル			~
ルール/コンフィグファイルのインポート					
ルールファイルのインポート 📀					参照
コンフィグファイルのインポート 🔅					参照
			取消	インポート	

<u>API</u>

- 1. [装置選択]より対象装置を選択し、取得方法 [API] を選択
- 2. 対象装置のAPI管理サーバーのURL、認証情報(ユーザー名、パスワード)を入力

装置認証情報の追加					
装置選択:		取得方法	:		
Sonicwall	*	API			*
優先情報					
WebサーバーURL ③					
ユーサー名					
パスワード					
			田道	法反	
			4X/A	進及	

装置ルール設定を保存後、一覧に取得状況が追加されます。

ダッシュボード インベン	ントリ アラート レポート	トルール管理	コンプライアンス 検知	き ツール	設定 サポート(米国)	Help Docs			
一般設定 ディスカバリ	FWAサーバー システム	設定 セキュリティ	その他						
syslogサーバー Check Point	装置ルール							16.00	削除
装置ルール	□ コマンドステータス	装置名	モード	仮想FW	セキュリティ監査	設定保存	最終更新	オンデマンド	編集
除外条件 認証プロファイル	🗆 🔮 成功	zoho-watchguard (WatchGuard Firewall)	CLI		Ф 2022-08-15 20:08	Ф 2022-08-28 20:07	Aug 28, 2022 20:07 PM	0, 20 F	2
接続診断	🗆 🕑 成功	Sophos XG (Sophos XG)	API	-	Ф 2022-08-16 15:04	Ф́ 2022-08-28 15:04	Aug 28, 2022 15:04 PM	9	8
可用性アラート 装置情報	🗆 🥑 成功	CheckPoint (Check Point)	API		Ф 2022-08-16 15:04	¢ 2022-08-28 15:04	Aug 28, 2022 15:04 PM	. e -	8

9.2 ルール管理

「9.1 装置ルール設定」を実施後、[ルール管理] タブより、 ファイアウォールのルール情報に関する各種レポートを確認します。

ベンダーごとのサポート対象機能は、以下のページをご参照ください。 <u>https://www.manageengine.jp/products/Firewall_Analyzer/SupportedFW.html#rule_management</u>

9.2.1 概要

ファイアウォールからルール情報を取得し、現在の設定情報の概要を表示します。 [サマリ] タブでは、以下の各統計情報が表示されます。

レポートタイプ	説明
合計ルール数	該当ファイアウォールで設定されている全てのルール数
許可ルール数	該当ファイアウォールで設定されている全ての許可ルール数
拒否ルール数	該当ファイアウォールで設定されている全ての拒否ルール数
ファイアウォール受信 ルール数	該当ファイアウォールで設定されているインバウンド(受信) ルール数
ファイアウォール送信 ルール数	該当ファイアウォールで設定されているアウトバウンド(送信) ルール数
無効ルール数	無効(非アクティブ)になっているルール数
ロギングが無効のルール 数	ロギング設定が無効になっているルール数
「any」から「any」への 許可ルール数	通信を無制限に許可しているルール数
「any」サービスを許可 しているルール数	サービス「any」を設定しているルール数
双方向ルールカウント	方向(送信元と宛先)の値のみが異なり、他項目の値は同一な ルール数

🗰 Firewall Analyzer		\$ I Q A \$
ダッシュボード インペントリ アラート レポート ルール経費 コンプライアンス 様余 ツール 縦定	サポート	
法法 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)		0 スケジュール 🔳 🕼 🖾
ファイアウォールに設定されているすべてのルールかわかります 現されたポリシー Q 70 のうち1	#581	数
60 et All Belleler 50	合計ルール数	72
V FortiGate-FW Policy 40	許可ルール数	67
30	拒否ルール数	5
20	ファイアウォール受信ルール数	0
	ファイアウォール送信ルール数	0
	無効ルール数	9
	ロギングが無効のルール数	2
and the second	「any」から「any」への許可ルール数	4
¢	^{- 2} ☆ 「any」サービスを許可しているルール数	24
	双方向ルールカウント	0

[セキュリティルールタブ] では、ファイアウォールに設定されているルール情報 (ルール番号/ID、送信元、宛先、送信インターフェース、宛先インターフェース、 サービス、アクション)を一覧で表示します。

[オブジェクト詳細] タブでは、ファイアウォールに設定されているオブジェクト情報 (ネットワークオブジェクト、サービスオブジェクト)を一覧で表示します。

ー覧で表示されるルールの順番は、ファイアウォールのCLIベースで設定されている ルールの順番に沿って表示されます。

9.2.2 最適化

ファイアウォールに設定されているルールの相関関係や使用状況に応じて、最適なルー ル構成を確認します。

以下の各タイプごとに情報を参照します。

タイプ	説明
ポリシー異常	ルール間の相関性を解析し、設定の最適化をサポートします。
	カテゴリ別(冗長性/一般化/相関(コリレーション)/シャドウ/ グループ)に、相関性や重複状況を表示します。
ルールの提案	過度な許可ルール(permit/any)に対して、ルールの使用状況に

	もとづいた推奨設定を表示します。
ポリシーのチューニング	許可ルールのみを表示し、一定期間に使用されているルール情報 をもとにチューニング内容を表示します。
オブジェクト使用	選択した期間に受信したsyslogに応じて、使用されたネットワー クオブジェクト/サービスオブジェクトの概要を表示します。
	また、未使用のネットワークオブジェクト/サービスオブジェク トも表示します。
重複オブジェクト	同じIPアドレス/サービスを持つが、オブジェクト名が異なる ネットワーク/サービスオブジェクトを対象に、重複しているオ ブジェクト情報を一覧で表示します。

Firewall Analyz	ser						
ッシュボード インベン	ントリ アラート レポート	ルール管理 コンプ	ライアンス 検索 ツール 設定 サ	ボート			
(要 - 最適化 - クリ	リーンアップ 並べ替え 影響	管理 比較	期限切れ通知 リスク				
名 rtiGate-FW v	ポリシー異常 ルールの提案	ポリシーのチューニング	オブジェクト使用 重複オブジェクト		O	スケジュール 🔥 💷 🖂 🗳 🖨	
シャドウ、元長、一般化、相関、グループなど、様々なルールの異常を特定するのに殺立ちます。詳細は、ごちらを確認してください							
				Category	Count		
				冗長性	10		
		一般化	0				
10			相關	11			
				シャドウ	0		
				グループ	1		
				ৰ্শন	22		

9.2.3 クリーンアップ

ファイアウォールに設定されているものの、一定期間使用されていないルールやオブ ジェクト、インターフェース情報を表示します。 以下の各タイプごとに情報を参照します。

タイプ	説明
未使用ルール	ー定期間に使用されなかったルール番号/ID、ルール説明(送信 元、宛先、アクション等)を一覧で表示します。

未使用オブジェクト	クトについて、該当のルール名、オブジェクトタイプ、未使用オ ブジェクト数、未使用比率(%)を一覧で表示します。
割り当てのないインター フェース	ルールに割り当てられていない未使用のインターフェース情報 (インターフェース名、IPアドレス、タイプ、モード、許可され たサービス、Vdom、ARP転送)を一覧で表示します。
割り当てのないオブジェ クト	ルールに割り当てられていないオブジェクト情報(オブジェクト 名、オブジェクト詳細、タイプ)を一覧で表示します。

III Fir	ewall A	nalyzer									A [Q A &
ダッシュン 概要	ポード 最達化	インベント クリーン	- リ ア ラート アップ 並べ替え	レポート 影響	ルール管理 管理 比較	コンプライアンス 交 利限切れ遅知	検索	ツール ギ	bite	サポート(米国)		
装置名 SRXTest0		v	未使用ルール 7	未使用オブジ	ェクト 割り当	てのないインターフェース 🔅	2) 割り	当てのないオブジェク	• •		◎ スケジュール	
時間の選択			所定期間に使用されな	いったルールを!	寺定します					開始:202	2-05-17 00:00:00 終了	7 : 2022-05-17 08:57:59
今日		w.	ルール番号/ID							ルール説明		
			All_Internal_Internet							State enabled, Index 8, Scope Policy: 0, Sequence number: 1Source addresses: any Destination addresses: any Action: permit		
			Web-Transaction							State: enabled, Index 4, Scope Policy: D. Sequence number: ISource addresses: Internal-Di- Destination addresses: any Applications: Junos-http, Junos-https://junos-discard, Junos-ymag Source Identifies: any Actions permit, application services, log, count.	łCP	
			internal-25-deny							State: enabled, Index 6, Scope Policy: 0. Sequence number: 3Source addresses: any Destination addresses: 192.168. Application: any Action: deny, log. count		
			internal-test-accept							State: enabled, Index: 9, Scope Policy: 0, Sequence number: 5Source addresses: any Destination addresses: 1921.68. Applications: junos snm:-clear-text Actions permit, los, count		
			internal-26-accept							State: enabled, Index 7, Scope Policy: 0, Sequence number: 4Source addresses: any Destination addresses: 192.168. 192.168. Applications; purces tapa Action: permit, log, count		
			ping							State: enabled, Index 5, Scope Polloy: Q. Sequence number: 2Source addresses: any Destination addresses: any Agolications: Lances-kompail. Junos-komp-ping, Junos-komp6-all Action: permit, log, count		

9.2.4 並べ替え

使用頻度の多いルールの順番を上位に配置することで、ファイアウォール自体の負荷を 低減させることにつながります。

本レポートでは、使用されるルールのヒット数に応じて、最適なルールの配置を提案し ます。

以下の各タイプごとに情報を参照します。

タイプ	説明
	 FWAが対象のファイアウォールから受信するsyslogに含まれる

提案された変更	ルールのヒット数をもとに、現在のポジションからどこのポジ ションに配置することが適切か表示します。
変更完了	ファイアウォールに設定されているルール内の未使用のオブジェ クトについて、該当のルール名、オブジェクトタイプ、未使用オ ブジェクト数、未使用比率(%)を一覧で表示します。

・並べ替えレポートでは、ルール配置の提案のみを行い、FWAからファイアウォール に対する設定変更は行いません。

・ルールに値が設定されていない場合、並べ替え提案の解析プロセスで、解析対象外と なります。

🔢 Firewall Analyzer						〇 045-225-8953 回オンライン相談 ⑤ お見様!	ッ ダウンロー	- F 🛃 💰 Q	A © 8
ダッシュポード インベント	トリ アラート レポー	-ト ルール管理	コンプライアンス 検索	ツール	設定 サポート(米国)	Help Docs			:
板要 最達化 クリーン	アップ 並べ替え 影響	2 管理 比較	期限切れ通知						
装置名		97				6			The set
PaloAlto *	促業されに変更 🐴 変更	296 J 105				لغ		1FD(8939):2018-06-06 15:03:	99.0 <u>9</u> .87
時間の選択	Rule Name		Position (From - To)		Hit Count		Perf. Improvem	ent	
今日 *	NET-2-LAN_112		82 → 1		153		78		
	ME-LEGDMZ-2-NET_68		71 → 2		153		67		
	NET-2-ME-LEGDMZ_125		92 → 3		153		86		
	LAN-2-NET_37		40 → 4		150		35		
	ME-IPSec-SOC-2-CHI		7 → 5		150		2		
	NET-2-LAN_118		86 → 6		150		77		
	LAN-2-NET_52		56 → 7		149		48		
	LAN-2-ME-LEGDMZ_6		10 → 8		123		2		
	LAN-2-ME-LEGDMZ_5		11 → 9		149		2		
	LAN-2-NET_30		34 → 10		148		24		
	NET-2-ME-LEGDMZ_124		91 → 11		148		77		

9.2.5 影響

ファイアウォールに新規ルールを追加する際、既存ルールとの関係や影響範囲を事前に 把握することが重要です。

本機能では、新規に追加予定のルールと既存ルールの関連性を表示します。

以下の流れで影響分析レポートからルールの関連性を確認します。

- 1. 追加予定のルール情報をレポートとして作成
- 2. レポートから既存ルールとの関連性を確認

<u>1.追加予定のルール情報をレポートとして作成</u>

[ルール管理]→[影響]画面で対象装置を選択し、[影響分析]より以下の各情報を 入力

項目	説明
ポリシーでのルール	任意のルール名
ポジション	新規ルールの配置予定の位置を選択
ソース	ファイアウォールに設定されている送信元オブジェクトまたはIP アドレスを指定
宛先	ファイアウォールに設定されている宛先オブジェクトまたはIPア ドレスを指定
送信インターフェース	送信元のインターフェースゾーン
宛先インターフェース	宛先のインターフェースゾーン
サービス	サービス名を選択
アクション	ルールのアクションを選択(Allow/Deny)
ブラックリストにしてい るIPアドレスファイルを 検討対象にする	組織内で重要視しているIPアドレスリストが存在する場合に、 txtまたはcsv形式のファイルを選択
最初に、オブジェクトの 重複確認をする	重複確認を行うルール数を選択(通常はALL)

Firewall A	Analyzer										1	Q 🌲 🌣 🔮
ダッシュボード	インベント	ッリ アラート	レポート	ルール管理	1	コンプライアンス	検索	ノール 設定 サポート(米国)				
概要 最遷化 装置名 FG800	クリーン ・	アップ 並べ替え ルールの影響	影響	管理	比較	期限切れ通知			事前影響確認レポートの	作成		×
		<mark>メモ</mark> : 新規ルールの作成	前に、ルールイ	ンパクト解析	では既存ル	ールを査定し、セキ	ュリティ上の脅威	リスクのあるボート、異常などを特定しま	す ポリシーでのルール			
		ポリシー名			レポート			作成日	ポジション		● デフォルト ─ カスタム	
		test2			レポートの)表示		29-03-2021 11:26:26	ソース		● 指定なし ── 選択	
									宛先		● 指定なし ── 選択	
	FAQ					送信インターフェース		● 指定なし ── 道択				
		1.ルールのインパクト解析問題が必要な理由は? 2.新規ルールのインパクト解析方法は2					宛先インターフェース	(● 指定なし ── 選択			
		3.ルールのインパクト解析レボートで提供される項目は? 4.作成したブラックリストロマドレスタ、ルールのインパクト解析機能にファイルとして決断するに				サービス		指定なし 🖲 選択				
		(2)			使用可能 サービス		選択済み サービス					
									検索		検索	
				mysql								
									SMB-Port			
									5905 zchat		4	
									OP25R			
									アクション	P	Allow *	
									レポート作成中			
									ブラックリストにしているIPア	ドレスフ	2 2 2	

2.レポートから既存ルールとの関連性を確認

生成したレポートには、以下の情報が表示されます。

項目	説明
ルールのインパクト詳細	[影響分析]で設定したルール情報を表示します。
異常詳細	既存ルールとの重複がある場合に表示されます。
ルール並べ替えの提案	既存ルールのヒット数から新規ルールの配置をサポートします。
このルールは、許可の範 囲が広くとられています	Anyを含む場合や、許可設定しているオブジェクトが多い場合 に、高リスクであることを警告します。
セキュリティ脅威の詳細	設定したサービスやインターフェースのセキュリティリスクレベ ルやCVE情報を表示します。
ブラックリスト(要注 意)のIPアドレス分析	新規ルールにブラックリストとして指定したIPアドレスが含まれ ているか表示します。

リスクがあるポート情報	設定したサービス、インターフェースのセキュリティリスク(CVE情報)を表示します。
複数ルールにおけるオブ	追加予定のサービス、送信元/宛先IPアドレスの各オブジェクト
ジェクトの重複性	と既存ポリシーとの重複性を表示します。

9.2.6 管理

CLIまたはAPIで接続を確立しているファイアウォールに対して、FWAから、オブジェ クトやルールの追加/編集/削除を行います。

以下の各タブごとに、オブジェクトの編集や変更を実施します。

タブ	説明
	ネットワークオブジェクトの追加やファイアウォールに設定され ている既存オブジェクトの編集や削除を行います。
ネットワークオブジェク	 ローカルオブジェクト ネットワークオブジェクトの追加設定を行います。
k	 ファイアウォールオブジェクト 既存で設定されているネットワークオブジェクトを編集します。
	追加、編集したオブジェクトは、ローカルオブジェクトまたは、 [レビュー&送信]タブに追加されます。
	*この時点では、ファイアウォールに変更は反映されません。
	サービスオブジェクトの追加やファイアウォールに設定されてい る既存オブジェクトの編集/削除を行います。
サービスオブジェクト	 ローカルオブジェクト サービスオブジェクトの追加設定を行います。
	 ファイアウォールオブジェクト 既存で設定されているサービスオブジェクトを編集します。

	追加、編集したオブジェクトは、ローカルオブジェクトまたは、 [レビュー&送信] タブに追加されます。 *この時点では、ファイアウォールに変更は反映されません。
	ルールの追加や対象装置に設定されている既存ルールの編集/削 除を行います。
セキュリティルール	● ローカルルール 新規ルールの追加設定を行います。
	 ファイアウォールルール 既存で設定されているルールを編集します。
	追加、編集したルールは、ローカルルールまたは、[レビュー& 送信]タブに追加されます。
	 *この時点では、ファイアウォールに変更は反映されません。
レビュー&送信	新規追加、編集、削除予定のオブジェクトやルールは、それぞれ [ローカルオブジェクト]と[ローカルルール]に追加されま す。加えて、[レビュー&送信]タブにも追加されます。
	[レビュー&送信] タブで、対象のオブジェクトまたはルールに チェックを入れて、画面右上の[送信] をクリックすることで、 対象のファイアウォールに設定を送信します。 編集や削除もこのタブから実行できます。
Rule Approval	ルールやオブジェクトの変更の際に、Administrator権限のFWA ユーザー間で承認プロセスを実現します。
	ユーザーが変更リクエストを送信し、承認者が承認、拒否、投入 を行います。
コミット	Palo AltoまたはCheck Pointを管理対象装置としている場合、 [レビュー&送信]タブで送信したオブジェクトやルールは、 [コミット]タブに移動します。
	[コミット]または[インストールポリシー]より、設定を送信します。
Palo AltoまたはCheck Pointをご利用の場合には、以下ページに記載の手順に沿って、 変更内容の送信およびコミットを実施してください。

https://www.manageengine.jp/products/Firewall_Analyzer/help/firewall-ruleadministration.html#review_send

9.2.7 比較

ファイアウォールの2つのコンフィグファイル、または異なるRunningコンフィグバー ジョン(世代)間における、ルールセットの差分を表示します。 追加、変更、削除ポイントを色別に比較します。 以下の各項目ごとに、差分を確認します。

項目	説明
コンフィグファイル間	2つの同一ベンダー/モデルのコンフィグファイルをインポート し、ルールセットを比較します。
コンフィグファイルと最 新runningコンフィグ	ファイアウォールのコンフィグファイルをインポートし、現在稼 働しているルールセット(FWAで取得したRunningコンフィグ) との比較を行います。
runningコンフィグの世代 間	ファイアウォールのコンフィグ設定が変更され、コンフィグバー ジョン(世代)がFWA上に追加されている場合に、変更された ルールセットを差分として表示します。

・ファイアウォールのコンフィグが変更された場合、[コンプライアンス]→[変更管 理]に世代が追加されます。

・コンフィグ世代の差分が、基本設定のみ(ルールセットに関する差分がない)場合、 本機能による比較はできません。

9.2.8 期限切れ通知

ファイアウォールに設定されているルールの有効期限やスケジュール情報を一覧で表示 します。

以下の各タブごとに、アクティブなルールや今後アクティブになるルール、既に期限が 切れているルールなどを表示します。

項目	説明
すべてのスケジュール ルール	週次のスケジュールや、特定の期間の1回のみのスケジュールな ど、ファイアウォールに設定されているスケジュールルールを一 覧で表示します。
アクティブルール	スケジュールルールの内、現在アクティブ状態のルールを一覧で 表示します。また、アクティブなルールの期限が切れた場合に、 通知する機能も搭載されています。
	[自分に通知]では、対象ルールの期限切れ確認時間(日次) や、期限切れになる前後の通知日を指定することができます。 ※繰り返しルールには設定できません。
予定ルール	今後のスケジュールで、アクティブになるルールを一覧で表示し ます。
期限切れルール	設定されたスケジュールに則り、既に有効期限が切れたルールを 一覧で表示します。
繰り返しルール	週次や日次スケジュールなど、定期的にアクティブになるよう設 定されているルールを一覧で表示します。

9.2.9 リスク

ファイアウォールに設定されているルールを分析し、脆弱なリスクが存在するルールを レベル別に表示します。

以下の各タブごとに、対象装置に潜む脆弱性を確認します。

タブ	説明
概要	各リスクレベルの合計数やリスク数のトレンドを色別に表示しま す。
ルール	各ルールごとに、該当するリスク内容を表示します。 ・ルール表示 ルール名/IDを基準に、該当するリスクレベルとその数を一覧で 表示します。 リスク数をクリックすると、ルールに関連するリスク情報と対策 のための推奨事項を確認することができます。 ・リスク表示 リスクレベルを基準に、リスク情報と該当のルール数を一覧で表 示します。 リスク情報をクリックすると、該当のルール一覧が表示されま す。 誤検知としてマークが必要なルールには、[誤検知をマーク]に より該当ルールをホワイトリストとして追加することができま す。 ※誤検知としてマークしたルールは、[除外ルール]から確認で きます。

10 コンフィグバックアップ

ファイアウォールのコンフィグを定期的にバックアップし、差分を比較します。

- ・事前に[装置ルール]を設定している必要があります。
- ・本機能のサポート対象ベンダーは、以下のページをご参照ください。

https://www.manageengine.jp/products/Firewall_Analyzer/SupportedFW.html#complia

・設定画面

[コンプライアンス] → [コンフィグバックアップ]

10.1 コンフィグバックアップのスケジュール設定手順

以下の手順で、スケジュール設定を行います。

- [コンプライアンス]→[コンフィグバックアップ]→[すべてのスケジュール]を表示
- 2. 画面右上の、 [バックアップスケジュールの追加]をクリック
- 3. 任意のスケジュール名を入力し、バックアップ対象の装置を選択
- コンフィグバックアップを実施する周期を選択 選択可能な周期:日次、週次、月次、1回
- 5. [設定とメール通知の保存]の項目で、保存するコンフィグ世代数、メール通知 を設定 選択可能なコンフィグ世代数:最新3バックアップ、最新5バックアップ、最新 10バックアップ、最新バックアップ、すべてのバックアップ ※週次、月次を選択した場合、[すべてのバックアップ]項目を選択できます。 ※1回を選択した場合、最新バックアップのみが選択可能です。
 ※メール通知を有効化した場合、指定したメールアドレスにコンフィグバック アップの実行ステータス(成功、失敗)を通知します。
- 6. [保存]より、設定を保存 保存すると、[すべてのスケジュール]の一覧に設定内容が表示されます。

<u>nce</u>

🔡 Firewall Ar	nalyzer										A	A & 8
ダッシュボード	インベントリ ア	ラート レポート ル	レール管理 コンプライフ	7ンス 検索	ツール 設定	サポート						:
32754728	変更管理 · セキ:	ユリティ監査 監査ログ	コンノイクハックアッノ									
すべてのスケジュー	ル バックアップ監	查 比較						バックアップスケジ	ュールの追加	0		\times
スケジュール名	装置名	ステータス	次回の実行	繰り返し	作成者	最近の変更	バーショ	スケジュール名				
test2	SRX検証		At 06-28-2023, 10 : 15	Once Only	admin	[NA]	late	装置が選択されていません	Q		選択された装置	Q
SRX	SRX検証		At 18:15 on Monday	Weekly	admin	admin	all			\rightarrow	SRX検証	
SRXバックアップ	SRX検証		From 10-18-2023, 11 : 00, everyday	Daily	admin	[NA]	last			4		
								スケジュール:				
								日次 次:	から開始			
								週次	/3-15-2024			
								月次 1	17 19		▼ 時 12	* 分
								10				
								設定とメール通知の保存:				
								バックアップコンフィグの保存	17		最新10バックアップ	v

10.2 バックアップ監査

スケジュールによるコンフィグバックアップの取得日時やステータス、取得したコン フィグファイルのダウンロードを行います。

以下の項目を選択し、参照するデータを指定します。

- 装置名
- スケジュールタイプ(すべてのスケジュール、日次、週次、月次、1回)
- 時間の選択(今日、最新24時間、最新7日間、最新30日間、カスタム)

[コンフィグファイル]のダウンロードリンクより、取得したコンフィグファイルをテ キスト形式でダウンロードします。 [比較]では、取得した別世代のルールまたはコンフィグとの比較を行います。

III Firewall A	Analyzer									1	Q	٨	¢ 😩
ダッシュボード	インベントリ	アラート レ	ポート ルール管	ヨンプライアンス	検索 ツー	ール 設定	サポート						:
コンプライアンス	交更管理	セキュリティ監査	監査ログ コ	ンフィグバックアップ									
装置名 SRX検証	¥	すべてのスケジュール	バックアップ監査	比較									
スケジュールタイプ		バックアップ時刻		スケジュール名		ステータ	2	コンフィグファイル	比較				
すべてのスケジュール	+	2024-03-18 11:00:10		SRXバックアップ		📀 成功		ダウンロード	B 1				
時間の選択		2024-03-17 11:00:08		SRXバックアップ		🔗 इंग्रेज		ダウンロード	5- B				
最新30日間	Ŧ	2024-03-16 11:00:11		SRXバックアップ		📀 成功		ダウンロード	5g ∰				

10.3 比較

スケジュールバックアップで取得したコンフィグ情報をもとに、ルールまたはコンフィ グに焦点をあて、差分比較を行います。

比較対象に関する以下の情報を指定します。

- 装置名:比較対象の装置を選択
- 比較規準:ルールまたはコンフィグを選択
- スケジュールタイプ:比較を行うスケジュールタイプを選択
- 時間の選択:取得したコンフィグ期間を選択
 今日、最新24時間、最新7日間、最新30日間、カスタム
- 比較するコンフィグのバックアップ日次:取得したコンフィグを選択(取得した 日時で表示されます)
- 対象:比較対象のコンフィグを選択(取得した日時で表示されます)
 ※[最新コンフィグ]は、その場で最新のコンフィグを取得し比較対象とします。

ルールまたはコンフィグに差分がある場合には、以下のような差分ページが表示され、 差分内容の詳細を確認します。

🗰 Firewall Analyzer						\$ ₽ Q ♠ ♥
ダッシュボード インベントリ ア	ラート レポート ルール管理	コンプライアンス 検索 ツール 設定 サポート				
コンプライアンス 変更管理 セキ	ニュリティ監査 監査ログ コンフィグ	バックアップ				
すべてのスケジュール バックアップ型	£查 比較			ルールtest_	を修正しました	>
SRX検証			✔ 追加-(0)			道加 🔜 変更 📕 削除
コンフィグファイルのバックアップ時	刻 : 2024-03-16 11:00:11		最新取得	ルールカラム	コンフィグファイルのバックアップ時 刻:2024-03-16 11:00:11	最新取得コンフィグ
ポリシー名	ルール名	比較	ポリシー名	Source	Any	Any
8 -	test			Destination		
				From	Internal	Internal
				То	Internet	Internet
				Service	Any	20231113 junos-aol junos-bgp
				Action	permit	permit
				Status	enabled	enabled
				Log	disable	disable

11 ログ検索

11.1 生ログ設定

FWAが受信する生ログのインデックス設定を実施します。

デフォルトでは、[セキュリティログのインデックスのみ]が有効化されています。 後述の「11.2 生ログ検索」で、トラフィックログの検索を行う場合には、[トラ フィックとセキュリティログのインデックス]を選択して、設定を保存します。

選択した項目に応じて、生ログ検索画面で表示されるオプションが異なります。

<u>[セキュリティログのインデックスのみ]を選択した場合</u>

- タイプ検索
- ファイアウォールの生ログ
- VPNの生ログ
- ウイルス/攻撃の生ログ
- 装置管理の生ログ
- 拒否の生ログ

[トラフィックとセキュリティログのインデックス]を選択した場合

● タイプ検索

```
ファイアウォールの生ログ
プロキシの生ログ
不明なプロトコル
```

- VPNの生ログ
- ウイルス/攻撃の生ログ
- トラフィックログ
- 装置管理の生ログ
- 拒否の生ログ

11.2 生ログ検索

FWAが受信した生ログに対して複数の検索条件を指定し、該当ログを検索します。

III Firewall Anal	yzer			*	Q 🛕 H	¢ 😩
ダッシュボード イン	ベントリ アラート レポート ルール管理	コンプライアンス 検索 ツール 設定	サポート(米国)			:
集約検索生ログ検索	生ログ設定					
使用可能な装置	選択済みの装置					
検索	検索					
	SRXTest					
	1011000100_3					
	4					
タイプ検索	ファイアウォールの生ログ 🔹					
	✓ VPNの生ログ ✓ ウイルス/攻撃の生ログ ✓ トラ	ライックログ 🗸 装置管理の生ログ 🗸 拒否の生ログ				
条件の設定	● すべての条件に合致 ── いずれかの条件に合致					
プロトコル	▼ 次に等しい ▼ ssh	•				
送信元	* 次の文字列 * 192.168.1	♥ ●				
	447.152					
解説 FAQ						
	5、レポートプロファイルを作成するには ?					
2.生ログ検索の結果が	から、レポートプロファイルを作成するには?					
3.ユーザーがアクセン	へしたWebサイト情報をタイムスタンプ含め取得するには?					
4. 断続的なVPN トラ:	フィック情報を取得するには?					

タイプ検索には、以下の種類があります。

- ファイアウォールの生ログ
- プロキシの生ログ
- 不明なプロトコル

また、生ログタイプとして、以下のチェック項目が実装されています。

- VPNの生ログ
- ウイルス/攻撃の生ログ
- トラフィックログ
- 装置管理の生ログ
- 拒否の生ログ

検索条件を指定し[作成]をクリックすると、検索条件に該当する生ログ情報が表示されます。

*プラスアイコンをクリックし、複数の検索条件を指定することも可能です。

検索後は、「フォーマットされたログ」または「生ログ」タブから確認します。

- フォーマットされたログ
 生ログを日時やホスト、ユーザーなど、各カラムごとに分け、視覚的に分かりや
 すい形式で表示します。
- 生ログ
 FWAが受信したログを、加工せずそのままの状態(生ログ)で表示します。

III Firewall A	nalyzer							1 🖾 Q I	A & .
ダッシュボード	インベントリ アラート	レポート ルール管理	コンプライアンス	検索 ツール 設定	サポート(米国)				:
集約検索 生D:	グ検索 生ログ設定								
レポートを検	索				DNSIC	よる名前解決 🔵 🗗 🔐 🗵		伝選択 保存	
フォーマットされ たログ	n <u>生ロ</u> グ								×
Date/Time	Host	User	Protocol	Destination	Severity	Duration	Sent	Received	
19 Jul 2022, 09:14:5	2 192.168.1.63	Chris	ssh	104.20.25.250	notice	2 Mins 52 Secs	475.79 KB	875.94 KB	
19 Jul 2022, 09:14:5	0 192.168.1.49	Khrist	ssh	31.13.69.203	notice	6 Mins 54 Secs	284.24 KB	801.2 KB	
19 Jul 2022, 09:13:2	2 192.168.1.12	Joseph	ssh	64.8.70.102	notice	1 Secs	0 KB	0 KB	
19 Jul 2022, 09:12:4	6 192.168.1.196	Chris	ssh	13.33.235.106	notice	10 Mins 20 Secs	42.92 KB	33.27 KB	
19 Jul 2022, 09:12:0	8 192.168.1.99	Khrist	ssh	31.13.69.203	notice	2 Mins 46 Secs	94.46 KB	658.75 KB	
19 Jul 2022, 09:11:3	1 192.168.1.16	Chris	ssh	104.20.74.90	notice	1 Secs	0 KB	0 KB	
19 Jul 2022, 09:09:0	4 192.168.1.214	Chris	ssh	64.4.54.253	notice	18 Mins 38 Secs	795.57 KB	851.96 KB	
19 Jul 2022, 09:08:5	3 192.168.1.117	samR	ssh	76.76.202.171	notice	1 Secs	0 KB	0 KB	
19 Jul 2022, 09:08:3	2 192.168.1.180	John	ssh	12.183.124.41	notice	11 Mins 58 Secs	338.87 KB	88.92 KB	
19 Jul 2022, 09:07:5	5 192.168.1.97	Joel	ssh	207.46.108.40	notice	3 Mins 16 Secs	356.42 KB	548.1 KB	
19 Jul 2022, 09:06:5	5 192.168.1.62	Chris	ssh	108.174.11.74	notice	17 Mins 27 Secs	560.5 KB	927.75 KB	
19 Jul 2022, 09:04:1	2 192.168.1.109	Joseph	ssh	64.8.70.102	notice	6 Mins 0 Secs	484.74 KB	354.82 KB	
19 Jul 2022, 09:03:2	4 192.168.1.187	John	ssh	12.183.124.41	notice	7 Mins 19 Secs	631.65 KB	741.16 KB	
19 Jul 2022, 09:00:5	9 192.168.1.138	Chris	ssh	204.62.114.50	notice	1 Min 6 Secs	577.38 KB	880.29 KB	
19 Jul 2022, 09:00:4	2 192.168.1.239	Khrist	ssh	31.13.69.203	notice	15 Mins 29 Secs	183.37 KB	774.13 KB	
19 Jul 2022, 09:00:2	6 192.168.1.90	Chris	ssh	13.33.235.106	notice	14 Mins 19 Secs	499.37 KB	454.95 KB	
19 Jul 2022, 08:57:3	7 192.168.1.85	Patrick	ssh	69.63.178.12	notice	1 Secs	0 KB	0 KB	
19 Jul 2022, 08:57:2	4 192.168.1.223	Chris	ssh	192.0.123.245	notice	1 Min 8 Secs	850.67 KB	842.45 KB	
19 Jul 2022, 08:55:5	8 192.168.1.209	Chris	ssh	13.33.235.106	notice	1 Secs	0 KB	0 KB	

```
・画面上部の[保存]より、検索した条件をプロファイルとして保存することができま
す。
*保存したプロファイルは、[レポート]→[カスタムレポート]のプロファイル一覧
```

に追加され、次回以降、保存した条件で検索することができます。 ※[スケジュール]を有効化することで、検索条件に対する検索結果を定期出力しま す。

・ [フォーマットされたログ] タブを表示し、画面上部の [表示カラム選択] から、一 覧に表示するカラム情報を選択することができます。 ※選択可能なカラムは11個までです。

11.3 集約検索

FWAのデータベースに集約されたデータをもとに、データ検索を行います。 検索画面で、対象装置の選択と検索条件を指定します。

III Firew	all Analyz	er												A	♪ C	×	1
ダッシュボー	ドインベ	ד עלי	ラート	レポート	ルール管理	コンプライス	シス	検索	ツール	設定	サポート(米国)						
集約検索	生ログ検索	生ログ設定															
使用可能な装	(E		選	沢済みの装置													
検索			1	発行													
			SI	OXTest													
			F	GT100D186_Sim													
			4														
条件の設定		 	条件に合致) いずれかの	条件に合致												
70 kau		- Voi=661	-	bib.c.													
		× KILWO	*	nttps		••••											
送信元		次の文字	9J *	192.168.1.		× 💿											
				作成													

検索条件を指定し[作成]をクリックすると、検索条件に該当するログ情報が表示され ます。

*プラスアイコンをクリックし、複数の検索条件を指定することも可能です。

検索結果は、以下のタイプごとに表示されます。

- ウイルス詳細
- 攻撃の分析
- URL詳細
- VPN使用率レポート
- プロトコル分析
- アプリケーション詳細

- 帯域詳細
- トリガーとするルール
- Spam詳細 (Spam Detail)

🔢 Firewall A	nalyzer									1 🔅 Q	A & &
ダッシュポード	インベントリ アラート	レポート	ルール管理 コンプライ	イアンス 検索	ツール 設定	サポート					:
集約検索 生ログ	検索 生ログ設定										
レポートを検索	Ā							A B X	① 今日 表示カラム選択	保存	
ウイルス詳細	攻撃の分析	URL 詳細	VPN使用率レポー ト	プロトコル分析	アプリケーション 詳細	带域詳細	トリガーとするル ール	Spam 詳細			×
装置≑	アプリケ	ーション	カテゴリ	۲»	(h	受信八イト(MB)	送信/	(イト(MB)	総バイト(MB)		
FGT100D186_Sim	HTTP.Flas	h	file-transfer	271		102.1	105.8	7	207.97		
FGT100D186_Sim	Google		Serach-Engine	27		12.11	12.42		24.53		
FGT100D186_Sim	Yahoo.We	bmail	web-mail	30		11.89	10.2		22.09		
FGT100D186_Sim	HTTP		web	22		9.26	8.58		17.84		
FGT100D186_Sim	Epic.Gam	es	Game	25		9.19	8.57		17.76		
FGT100D186_Sim	Musical.ly		video/audio	22		10.22	7.07		17.29		
FGT100D186_SIm	DreamBo	к	collaboration	21		8.27	8.36		16.63		
FGT100D186_Sim	Microsoft	Outlook.Office.365	Email	19		8	7.81		15.81		
FGT100D186_Sim	DNS		network-service	16		8.02	5.55		13.57		
FGT100D186_Sim	Facebook		Social-Media	15		6.17	4.29		10.46		
				14.44	1ページ中(1)ページ目	▶ ≥ 50 V				10 件中 1 - 10 を表示	

画面上部の[保存]より、検索した条件をプロファイルとして保存することができま す。

保存したプロファイルは、 [レポート] → [カスタムレポート] のプロファイル一覧に 追加され、次回以降、保存した条件で検索を行うことができます。

12 ユーザー管理とロール権限

FWAを複数人で管理する場合に、ユーザーアカウントごとに権限を作成して付与する ことができます。

*標準で使用可能なユーザーアカウント数は、デフォルトのadminユーザーを含めて2 ユーザーまでです(それ以上の追加は、オプションです)。

12.1 ユーザー管理

[設定]→[一般設定]→[ユーザー管理]→[ユーザー]画面で、ユーザーアカウントを作成します。

デフォルトで、以下の2つの権限が実装されています。

● 管理者

FWAであらゆる操作を実行する権限があります。

オペレーター
 FWAで操作制限のある権限です。ユーザー管理機能の操作など、設定タブ配下の表示項目が制限されます。

操作権限の詳細については、以下のページをご参照ください。

https://www.manageengine.jp/products/Firewall_Analyzer/help/user-managementsettings.html#create_users

以下の手順でユーザーアカウントを作成します。

- 1. [設定]→[一般設定]→[ユーザー管理]→[ユーザー]右上の[ユーザー追 加]をクリック
- 2. [ロール]で、作成するユーザーの権限を選択(管理者、オペレーター、作成したロール権限)

※ロール権限については、次章を確認してください。

- 3. [ユーザータイプ]で、認証タイプを以下より選択
 - ・ローカル認証
 - ・RADIUS認証
 - · AD(Active Directory)認証
- 4. ユーザー名、パスワード、対象ユーザーのメールアドレスを入力し、 [次へ]

🗰 Firewall Analy	zer								\$	-	Q 🌲	4
ダッシュボード インベ	ントリ アラート	レポート	ルール管理	コンプライ	アンス 検索	ツール	設定	サポート				
一般設定 ディスカバリ	ー FWAサーバー	システム	設定	セキュリティ	その他							
メールサーバー設定	フーザー情報を	编生										
SMSサーバー設定	IH+R C	- m##										
プロキシサーバー設定	6			2								
OAuth プロバイダー	フーザー設定			詳細								
ユーザー管理	ユーザーロール、認識	证情報、連絡先詳	細を入力して	 ユーザーにアクセ	スを許可する装置を	設定します						
181E	ください											
サーバー設定	דיש	プロード										
SSH設定												
システム設定	ロール			? ユーザータ	マイプ							
リブランディング	管理者			▼ □−カル	-828E		*					
スナップショット設定	ユーザー名・			Email ID *								
セルフ監視												
セキュリティ設定	パスワード・	パスワー	ドポリシーの副	定 パスワート	ヾの再入力*							
プライバシー設定				8			8					
サードパーティ製品の統合	Phone Number	Mobile	Number	タイムゾー	-ン(NFAレポート	用)						
				Asia/Tok	уо		Ŧ					
					キャンセ	レ次	^					

5. ユーザーに割り当てる装置または装置グループを選択し、保存

III Firewall Analy	zer		1
ダッシュポード イン	ベントリ アラート レポート ル	ノール管理 コンプライアンス 検索 ツール 設定 サポート(米国)	
一般設定 ディスカバリ・	- FWAサーバー システム 設定	セキュリティ その他	
メールサーバー設定	コーザー情報を編集		
SMSサーバー設定			
ユーザー管理			
認証	ユーザー設定	洋網	
SSH設定	ユーザーロール、認証情報、連絡先詳細を入力し	て ユーザーにアクセスを許可する装置を設定します	
システム設定	くたさい		
リブランディング	ファイアウォール	^	
スナップショット設定			
ルフ監視	使用可能な装置		
2キュリティ設定	CheckPoint	Paloato_sim EGT100D186 Sim	
プライバシー設定	SRXtell	→ SquidProxy,Sim	
ナードパーティ製品の統合			
		(
	戻る	キャンセル 保存	

・ローカル認証

FWAで独自に作成、管理するユーザーアカウントです。ローカル認証の場合、パス ワードポリシーを任意に設定することができます。

※パスワードポリシーの設定は、「<u>12.3 パスワードポリシー</u>」をご確認ください。

・RADIUS認証

RADIUS認証を使用して、FWAにログインするユーザーアカウントを作成します。 導入 しているRADIUSサーバーの設定が必要です。RADIUSサーバーの設定については、以下 のページをご参照ください。

https://www.manageengine.jp/products/Firewall_Analyzer/help/user-managementsettings-radius.html

・AD認証

AD認証を使用して、FWAにログインするユーザーアカウントを作成します。 導入して いるドメインサーバーの設定が必要です。ドメインサーバーの設定については、以下の ページをご参照ください。

https://www.manageengine.jp/products/Firewall_Analyzer/help/user-managementsettings-ad.html

12.2 ロール権限

管理者、オペレーター権限に加え、任意の権限名と各機能の権限(Read/Write、Read のみ、アクセス権なし)を付与した独自の権限を作成します。 作成手順は以下の通りです。

- [設定]→[一般設定]→[ユーザー管理]→[ロール]を表示し、画面右上の [Add Role]をクリック
- 2. 権限名として任意の [名前] およびその [説明] を記入
- [共通設定]、[ファイアウォールログ解析]の項目から、権限に付与する操作 を選択し、[保存]
 ※操作権限は、読み取り/書き込み、読み取り、アクセス許可なしから選択しま す。

※権限を保存すると、[ロール]画面の一覧に追加されます。

🔢 Firewall Analyze	er				* • • • • •
ダッシュボード インベン	トリ アラート レポート ルール管理	コンプライアンス 検索 ツール 設	き サポート		:
一般設定 ディスカバリー	FWAサーバー システム 設定	セキュリティ その他			
メールサーバー設定	追加 役割				
SMSサーバー設定	名前				
OAuth プロバイダー	アラートと通知プロファイル				
ユーザー管理	說明				
121E	アラートと通知プロファイルの参照権限	キャンセル保存			
サーバー設定					
SSH股定	▼ 共通設定				
ンステム設定	モジュール	読み取り/書き込み	読み取り	アクセス許可なし	
スナップショット設定	全般設定			~	
セルフ監視	ディスカバリ			~	
セキュリティ設定	アラートの操作		~		
サードパーティ製品の統合	通知プロファイル		 		
	ダッシュボード			~	
	レポート			~	
	ツールセット			~	
	▶ ファイアウォールログ解析				

追加したロール権限は、[設定]→[一般設定]→[ユーザー管理]→[ユーザー]で ユーザーを作成または編集する際の[ロール]に表示されるようになります。

ロール機能で作成可能な操作権限については、以下のページをご参照ください。 <u>https://www.manageengine.jp/products/Firewall_Analyzer/help/role_feature.html#Oper</u> <u>ation_list</u>

12.3 パスワードポリシー

FWAにログインして操作を行うユーザーアカウントの「パスワードレベル」を設定します。

ご利用環境のセキュリティレベルに応じて、ポリシー変更を実施してください。 *ローカル認証で追加したユーザーを対象にポリシーが適用されます。

III Firewall Analyze	er	A 🗔 Q 🔺 🌣 😩
ダッシュボード インベン	ントリ アラート レポート ルール管理 コンプライアンス 検索 ツール 設定 サポート(米国)	:
一般設定 ディスカバリ	FWAサーバー システム 設定 セキュリティ その他	
メールサーバー設定 SMSサーバー設定	ユーザー管理	
ユーザー管理 認証 SSH設定	ユーザー ロール パスワードポリシ	
システム設定 リブランディング	メモ: この協定は「ローカル総証」のユーザーにのみ適用されます 詳細はこちらを参照ください	
スナップショット設定	最短パスワード長 5	
セルフ監視 セキュリティ設定	パスワードの機器を記録する 3 パスワード.	
プライバシー設定	バスワードとユーザー名は同一にはできません 🂽 有効	
サードパーティ製品の統合	パスワードを忘れた場合	
	ユーザーアカウントのロックアウトポリシー C 有効 ①	
	ログイン失敗の最大試行回数 5	
	ロックアウト明語 2 分	
	キャンセル 保守	

各パラメーターについて、以下の表に記載します。

項目	説明
最短パスワード長	設定可能な最短パスワードの長さを設定 デフォルト:5
パスワードの履歴を記録 する	パスワードを変更時に、過去数回の同パスワードの使用を不可に 設定
パスワードとユーザー名 は同一にはできません	ユーザー名、パスワードを同一にしない場合、有効に設定
パスワードを忘れた場合	ログイン画面で、[パスワードを忘れた場合]オプションを表示 /非表示に設定

ユーザーアカウントの ロックアウトポリシー	複数回ログインに失敗した場合のロック設定
 ログイン失敗の最大試行 回数	ロックアウトポリシーを有効にした際の最大試行回数を設定(デ フォルト5回)
ロックアウト期間	ロックアウトポリシーを有効にした際のロック時間を設定(デ フォルト2分)

13 各メニュータブの説明

FWAの画面上部に、各メニュータブが存在します。 各タブで表示される情報や操作可能な機能について記載します。

13.1 ダッシュボード

FWAにログイン後に表示されるホーム画面です。 ダッシュボードで表示する項目(ウィジェット)を任意にカスタマイズすることで、管 理対象装置の一覧や装置、ホストごとのトラフィック状況を1つの画面で把握します。

ダッシュボードには、以下のタブが存在します。

タブ名	機能
概要	管理対象装置の一覧やホスト、アプリケーションごとのトラ フィック状況など、全体の状況を表示します。
ライブトラフィック	装置またはインターフェースごとに、In/Outのトラフィックをリ アルタイムのグラフで表示します。
クラウドコントロール	ファイアウォールを通過するクラウドサービスの使用状況を表示 します。

ユーザー	通信を行っているユーザーに焦点をあて、アクセス状況を表示し ます。
VPN	ファイアウォールを通過するVPN通信のトラフィック使用率、 VPNグループとユーザー情報を表示します。
ルール管理	ファイアウォールに設定されているルールを最適化するための情 報(シャドーイング、冗長性、相関性、グループ化、一般化)を 表示します。
セキュリティ	攻撃、ウイルス、SPAM通信など、ファイアウォールを通過しよ うとする通信の内、セキュリティに関連するデータを表示しま す。
コンプライアンス	業界の各セキュリティ標準や監査要件に対する、ファイアウォー ルに設定されているコンフィグの準拠状況を表示します。

Firewa	all Ana	lyzer												1 I Q	A
ダッシュボード 概要 [、]	5 1 51	バンベントリ プトラフィック	アラー ク ク:	ト レポート ラウドコントロール	ルール管理 ユーザー	コンプライアンス VPN	ス 検索 ルール管理	ツール セキュリティ	設定 サボ コンプライ	ート(米国) アンス	カスタム ~				*
トラフィッ すべての装置	ク統計								セキュリティ 劇 すべての装置 今日	充計					
150000 (BI)) 100000 100000 50000 0				FGT100D186_Sim Resources			Streaming FTP Network Man Network Secu Voip Routing Printer Ucensing Point2Point Nowee Century	agement sity	80000 10 10 10 10 10 10 10 10 10			PGT1000186_SH Event Type			Security Events Attacks Deried Events Virus Port Scans
装置名			送信		受信	合計			装置名 ♥	攻撃	ウイルス	ログオン失	枚 セキュリティイ ベント	拒否イベント	コンフィグ保存
▶ FGT100D1	186_Sim		80.38 GB		80.28 GB	160.6	56 GB		FGT100D186_Sim	18114	17953		36067	18012	
装置一覧					トップNホスト: すべての装置 今日	トラフィック順			トップトロフプリ	1/7-2-3	トニコ <i></i>		トップルナフト・104	915	
装置名 ロ	IPアドレ ス	タイプ	ベンダー	ステータ ス	192.168.1.75	421.3 MB			すべての装置 今日	/-/=/			すべての装置 今日	BUR .	
SRXTest		Firewall	SRX Log Format	(2) 管理対 象外	192.168.1.247	416.2 MB			HTTP.Flash	7.	91.47 GB		200.50.4.39	28 Hits	
SquidProxy _Sim	127.0.0.1	Squid	Unknown CLF	管理対 象外	192.168.1.31	400.84 MB			HTTP	7.	.74 GB		31.13.69.203	19 Hits	
FGT100D1 86_Sim	127.0.0.1	Firewall	FortiGate	♥ 管理	192.168.1.74	399.49 MB			Yahoo.Webmail	[7.	.74 GB		69.63.178.12	16 Hits	
					192.168.1.184	394.49 MB			Microsoft.Outloo	k.O 7.	.71 GB		76.76.202.171	15 Hits	

13.1.1 ダッシュボードの新規作成

以下の手順で新規ダッシュボードを作成します。

1. ダッシュボード画面右上の [+] をクリック

- 2. [ダッシュボードを追加]をクリック
- 任意のダッシュボード名、説明を入力し、 [次へ] をクリック
 ※ダッシュボード名に、特殊文字や空白は使用できません。
- 4. ダッシュボードに追加するウィジェットを選択し、 [次へ] をクリック

🗱 Firewall Analyzer						A	4	Q 🌲	1	₽ .
ダッシュボード インベントリ アラート	レポート ルール管理	コンプライアンス	検索 ツール	設定	サポート(米国)					:
Q 検索ウィジェット										\times
ログ解析										
Compliance by GLBA Standard										
GDPR標準でのコンプライアンス										
HIPAA標準でのコンプライアンス										
ISO標準でのコンプライアンス										
NERC CIP標準でのコンプライアンス										
NIST標準でのコンプライアンス										
PCIDSS標準でのコンプライアンス										
SANS標準でのコンプライアンス										
SOX標準でのコンプライアンス										
アクティブVPNユーザー										
カテゴリ使用率										
セキュリティイベント概要										
セキュリティ統計										
トップN SPAM送信者:ヒット数順										
トップN VPNグループ:トラフィック順										
トップN VPN : トラフィック使用率順										
トップN クラウドアプリケーション										
トップN クラウドサービス										
トップN クラウドユーザー										
トップN ソーシャルメディアサービス										
1										
戻る							<i>≠</i> v>1	211	次へ	

5. ダッシュボードの参照を許可するユーザーアカウントを任意に選択し、[作成]

作成したダッシュボードは、 [ダッシュボード] → [カスタムウィジェット] タブから 選択できます。

また、ダッシュボードを表示し、画面右上の [★] をクリックすると、デフォルトダッ シュボードとして設定することができます。



13.1.2 ウィジェットの追加、編集、削除

ウィジェットの追加

デフォルトダッシュボードにウィジェットを追加するためには、事前設定が必要です。 [設定]→[一般設定]→[システム設定]→[クライアント設定]より、

[デフォルトダッシュボードからウィジェットを追加/削除できるようにする]を有効 化して保存してください。

🔡 Firewall Analyze	er		⊀ ⊡ Q ≜ ⇔ ≗
ダッシュボード インベン	ットリ アラート レポート ルー	し管理 コンプライアンス 検索 ツール 設定 サポート(米国)	:
一般設定 ディスカバリー	FWAサーバー システム 設定	セキュリティ その他	
メールサーバー設定			
SMSサーバー設定	システム設定		
ユーザー管理			
1228E	ハンテマージ シライアンド設定		
SSH股定	デフォルト認証	ローカル設施	
システム設定			
リブランディング	アラート通知	有効 無効	
スナップショット設定	ニフェルトガッシュ ギードからみ ノジュー	● 2015	
セルフ監視	テノオルドラッシュホードからウィシェ ットを追加/削除できるようにする		
セキュリティ設定	ヘルプカード詳細	● 有効 無効	
プライバシー設定			
サードパーティ製品の統合	DBクエリ	有动 💿 無动	
	製品プロモーション	有効 () 無効	
	劇品アシストのお知らせ	有効 () 無効	
	オペレーターにタッシュホートの作成を 許可する	 4xi xi 	
	チャットサポート	有効 新加加	
	他の製品のおすすめ	有効 () 無効	
		08	
		1945f	

上記設定を保存後、 [ダッシュボード] 画面右上の [+] アイコンより、表示中のダッシュボードに任意のウィジェットを追加します。

III Firewall Analyzer									1 🗔 Q	
ダッシュポード インベントリ アラート レポート	ト ルール管理 コン	プライアンス 検索	ツール	設定 サボ・	- ト(米国)					:
概要 ライブトラフィック クラウドコントロー トラフィック統計 マハエの発意(+9日 装置名 送信	ル ユーザー 、 受信	VPN ルール管理 合計	セキュリテ	イ コンプライフ セキュリティ統 すべての装置(今日 装置名。	アンス ゴ 計 攻撃	bスタム ∨ ウイルス	ログオン失敗	セキュリ	ダッシュボード ^{ダッシュポードを追加}	J-151y HORENS
▶ FGT1000186_Sim 85.33GB 被面一覧	85.23 GB トップNホスト:トラ すべての発言(今日	170.56 GB フィック順		FGT100D186_Sim トップNアプリ・ すべての装置19日	19227 ケーション:	19062 トラフィック頃		38289 38289 トップNホス	test	× 12 8

<u>ウィジェットの編集、削除</u>

ウィジェットに表示する情報を変更する際は、ウィジェットにカーソルをあて、[編 集]アイコンから編集を行います。

※編集できる内容はウィジェットごとに異なり、ウィジェット名やデータ表示対象期間、データ表示数、対象装置などを指定することができます。

ウィジェットを削除する際は、同様に対象のウィジェットにカーソルをあて、[削除] アイコンから削除します。

ダッシュボード内で、ウィジェットを任意の位置に配置したり、大きさを変更すること ができます。 参照する頻度の高いウィジェットを上部に配置しておくことで、より迅速に情報を把握 します。

III Firewall	Analyzer											1 1	2 🌲 🗉		F (3)
ダッシュボード	インベントリ	アラート レポート	ルール管理	コンプライアンス	検索	ツール	設定 サボ	- ト(米国)							:
概要 ∨	ライブトラフィック	クラウドコントロール	ユーザー	VPN JL-	ール管理	セキュリティ	ィ コンプライフ	アンス	カスタム ~					*	Ē
トラフィック 新 すべての装置 今日	tat.			Ð		-	セキュリティ統 すべての装置1今日	iä†							
装置名	送	E	受信	合計			装置名≑	攻撃	ウイルス	ログオン	夫敗 セキュリティイ	拒否イベント	コンフ	ィグ保存	
▶ FGT100D186_S	im 85.	33 GB	85.23 GB	170.56 GB			FGT100D186_Sim	19227	19062		38289	19120			
装置一覧			トップNホスト:ト すべての装置1今日	~ラフィック順			トップNアプリー すべての装置 今日	ケーショ	ン:トラフィック順		トップNホスト: 攻撃 すべての装置 今日	k)(Ą			

13.2 インベントリ

FWAに追加した装置や使用ユーザーの確認、トラフィックの多い通信状況の参照な ど、

管理対象装置から受信したログ情報にもとづいた詳細な情報を確認することができます。

[インベントリ]には、以下のタブが存在します。

タブ名	説明
装置	FWAに追加されている装置の一覧を表示します。 装置の名前、ライセンス(管理/非管理)、IPアドレス タイプ、ベンダー、アップ/ダウンリンク速度、イントラネット /SNMP設定の各情報を表示します。
インターフェース	FWAに追加された装置のログから取得したインターフェース情報を 表示します。 インターフェース名をクリックすることで、帯域や発生した通信を 表示します。

	FWAに追加された装置のログから取得したユーザー情報を表示しま
¬_+++	す。
y	ユーザー名をクリックすることで、対象ユーザーに関する詳細な通
	信状況を表示します。
	FWAに追加された装置のログから取得したクラウドサービス情報を
クニウドサービフ	表示します。
	クラウドサービス名をクリックすることで、帯域や使用ユーザー情
	報を表示します。
	装置でトリガーとして使用されたルール情報(許可/拒否、ヒット
(古田山 <u>山</u>)	数、トラフィック数)を表示します。
	ルール名をクリックすることで、ルールのトリガーとなった通信情
	報を表示します。

13.2.1 スナップショット画面

[インベントリ]→[装置]画面で装置をクリックすると、スナップショット画面が表示されます。

本画面では、対象装置に関する詳細な情報を参照することができます。

タブ名	説明
	装置情報に加え、受信、送信のトラフィック量を表示します。
概要	アップリンク/ダウンリンクの値を編集アイコンから変更すること
	ができます。
	受信、送信のライブトラフィックを表示します。グラフによる時系
	列データと、最小、最大、平均のトラフィック値を算出したデータ
世代	が表示されます。
'中'地	グラフ上をクリックすることで、該当の時間帯の通信状況(送信
	元、ユーザー、宛先、時刻、ルール番号/ID、プロトコル、重要
	度、期間、送受信バイト)を一覧で表示します。
	トラフィックの多い通信を対象に、ホスト、宛先、プロトコルグ
	ループ、内部サーバー、外部サイト、会話(通信)を一覧で表示し
トップ10	ます。
	対象のホストやプロトコルグループをクリックすることで、より詳
	細な通信情報を表示することができます。
サイト	通信許可、拒否されたWebサイト(URL)情報を表示します。

該当のURL、ヒット数、ヒット率(%)、総バイト(MB)を一覧で確認
します。
対象装置を介して発生した通信のうち、アプリケーション情報を表
示します。
アプリケーション名またはカテゴリ名をクリックすることで、該当
のアプリケーションを使用しているより詳細な通信情報が表示され
ます。
対象装置で許可、拒否された上位のルール(ポリシー)番号を表示
します。
ルール番号をクリックすることで、ルールのヒット数や、ルールに
該当した通信の情報が表示されます。
攻撃やウイルス、拒否された送信元、宛先ホスト情報など、セキュ
リティに関連する情報を一覧で表示します。
攻撃名やホスト名をクリックすることで、該当の通信の詳細(ホス
ト、宛先、プロトコルなど)が表示されます。
対象装置を介して発生したVPN通信の情報(アクティブVPNユー
ザー、VPNセッション、上位VPNレポート)を一覧で表示します。
一覧では、ユーザー名やVPN通信の開始/終了時刻、経過時間、送
信/受信量などが表示されます。
プロキシサーバーを経由したウイルス情報を表示します。
※プロキシサーバーの画面で表示されます。
プロキシサーバーの使用状況(キャッシュコード、ピアステータ
ス、HTTPステータスコード、HTTP操作)を表示します。
※プロキシサーバーの画面で表示されます。

・アプリケーションレポートのサポート対象は、以下の通りです。

Check Point、Cisco Firepower、FortiGate、Juniper SRX、Palo Alto、SonicWall、 Sophos XG、WatchGuard

・「app」レコードを含むsyslogデータを解析対象とします。

Firewall Ar	nalyzer								1			₽
ジ ッシュボード	インペントリ アラート	レポート ルール管理	コンプライア	ンス 検索 ツ・	ール 設定	サポート(米国)						
100D186_Sim	今日 2023-03-03 00:00 to 2023-03-03 10:41						レポートプロファイルを作成	する アラートプロファ	マイルを作成する	t 🖂 [<u>a</u> <	>
$y>_2x=k^-k^ y=k^ k=1$ $2y=2/57/92x$ $k=1$ $y=1$ $k=1$												
装置概要						迷	腹 平均 🔹 🖻 🖂 🖓 🖉					
ホスト名	FGT100D186_Sim			トラフ	イック							
IPアドレス	127.0.0.1			1.77	199							
タイプ	Firewall			21.52Mbps	🔥 21.52мы	IS						
ベンダー	FortiGate			◆ 受信(平均)	送信 (平均)							
ダウンリンク速 度	1000 Mbps 🕼											
アップリンク速 度	1000 Mbps 🕼											
最終パケット受 信時間	Mar 03, 2023 10:42 AM											
ステータス	🕑 管理対象											
装置ルール	未設定			2 %	2 %							
SNMP設定	未設定		8	ー 通しトラフィック(平均)	(注信トラフィック	(亚物)						
イントラネット 設定	未設定		2	(m) 224 22 (TP)	AGIE 1 994 99	(199)						
除外ホスト	未設定											
仮想装置	傳											

13.3 アラート

アラートプロファイルやセルフ監視で発生したイベントを、アラートとして一覧で表示 します。

アラートの発生状況から、問題が発生している装置やそのイベント内容を把握します。

III Fi	rewall Analyzer				
ダッシュ	ュポード インベントリ アラート	レポート ルール管理	コンプライアンス 検索 ツー	-ル 設定 サポート(米国)	:
発生中の	アラート すべてのアラート イベント				
0	すべてのアラート(53)		î↓		+ 🛍 🗙
53	Ust_VPN: Number of Hits exce [FG1001	小明 不割ヨ (里八	14-80	1	
	e test_VPN: Number of Hits exce FG1000	不明 未割当て 重大	1年前	FireWall Analyzer ディスク空き容量のしきい値違反がクリアされました。現在の値は 10GB です	Ľ
	etest_VPN: Number of Hits exce FG1000	不明 未割当て 重大	1年前	System	
51	e test_VPN: Number of Hits exce FG1000	不明 未割当て 重大	1年前	ヤルフ乾視 :: 確認解除 :: クリア	
\bigcirc	e test_VPN: Number of Hits exce FG1000	不明 未割当て 重大	1年前		
\mathbf{O}	e test_VPN: Number of Hits exce FG1000	不明 未割当て 重大	1年前	图 511202212:55:14年期 51	
	e test_VPN: Number of Hits exce FG100	不明 未割当て 重大	1年前	イベント ワークフロー メモ Q画像は443x4-	ジ中 1 ページ目 開始開 50 🗸 を表示
	e test_VPN: Number of Hits exce FG1000	不明 未割当て 重大	1年前	メッセージ	ステータス
\bigcirc	etest_VPN: Number of Hits exce FG1001	不明 未割当て 重大	1年前	FireWall Analyzer ディスク空き容量が 4GB です。しきい値(5GB)違反です	😢 重大
2	e test_VPN: Number of Hits exce FG100	不明 未割当て 重大	1年前	FireWall Analyzer ディスク空き容量のしきい機違反がクリアされました。現在の値は13GB です	📀 クリア
\bigcirc	e test_VPN: Number of Hits exce FG1000	不明 未割当て 重大	1年前	FireWall Analyzer ディスク空き容量が 3GB です。しきい徳(5GB)違反です	(2) 重大
>	etest_VPN: Number of Hits exce FG1000	不明 未割当て 重大	1年前	FireWall Analyzer ディスク空き容量のしきい価違反がクリアされました。現在の価は 15GB です	📀 クリア
	etest_VPN: Number of Hits exce FG1001	不明 未割当て 重大	1年前	FireWall Analyzer ディスク空き容量が 3GB です。しきい値(5GB)違反です	😢 重大
	e test_VPN: Number of Hits exce FG1000	不明 未割当て 重大	1年前	FireWall Analyzer ディスク空き容量のしきい値違反がクリアされました。現在の値は 7GB です	📀 クリア
	etest_VPN: Number of Hits exce FG100[不明 未割当て 重大	1年前	FireWall Analyzer ディスク空き容量が 2GB です。しきい偃(5GB)違反です	(2) 重大
	est_VPN: Number of Hits exce FG100[不明 未割当て 重大	1年前	FireWall Analyzer ディスク空き容量のしきい債違反がクリアされました。現在の値は 6GB です	📀 クリア
	etest_VPN: Number of Hits exce FG1001	不明 未割当て 重大	1年前	FireWall Analyzer ディスク空き容量が 3GB です。 しきい値(5GB)違反です	(2) 重大

13.4 レポート

カスタムレポートやFWAレポート、プロキシレポートなど、各種レポートを表示、 ファイル出力します。 詳しくは、「<u>6 レポート</u>」の章をご参照ください。

13.5 ルール管理

ファイアウォールに設定されているルールについて、 既存ルール間の関連性や新規ルールを追加する際の重複性などを確認し、 最適なルール設定をサポートします。 詳しくは、「<u>9 ルール管理</u>」の章をご参照ください。

13.6 コンプライアンス

ファイアウォールに設定されているルールやコンフィグについて、

SANSやPCI-DSSなどの各業界のセキュリティ標準に対する準拠状況や、コンフィグバックアップ、変更管理を実施します。

コンフィグバックアップについては、「<u>10 コンフィグバックアップ</u>」の章をご参照く ださい。



13.7 検索

任意の検索条件を指定し、該当のログを特定します。

生ログベースの検索と、データベースの集約データを対象とした検索を行います。 詳しくは、「<u>11 ログ検索</u>」の章をご参照ください。

13.8 ツール

Ping、MACアドレス/DNS解決、syslog転送など、各種ツール機能を使用することができます。

🏢 Firewall Analyzer										*	Q 🏚	¢ 💲
ダッシュボード インベントリ アラート	レポート	ルール管理	コンプライアンス	検索	ツール	設定	サポート(米国)					:
pingツール アドレス監視 ネットワーク監視	SNMPツール	Ciscoツール	syslogの転送		pingツール		>					
syslog転送 @#					アドレス監視	ł	>			物先追加		K III IA
受信したsyslogを設定した宛先に転送します					ネットワーク	7監視	>			1010204		1000
宛先ホストゥ				3	snmpツール		>	アクション	٩			
				データがあり	Ciscoツール		>					
					syslogの転送							

13.9 設定

メールサーバー設定やユーザー管理、ログファイルのインポート、アラートプロファイ ル設定など、FWAを運用する上で必要となる各種設定を行います。

🗰 Firewall Analyzer					\$ ₽ Q ♠ ♥ .
ダッシュボード インベントリ	アラート レポート ルール管理 コ	ンプライアンス 検索 ツール	健定 サポート(米国)		:
一般設定	ディスカバリ	FWAサーバー	システム	設定	
☑ メールサーバー設定	③ ファイアウォールの追加	iii syslogサーバー	勘 ログファイルのインボート	鼻 イントラネット	
🖂 sMSサーバー設定	□ ターミナル	Check Point	🛛 プロトコルグループ	◎ データ保存	
▶ ユーザー管理	闘 シミュレーション	▲ 装置ルール	🏾 アーカイブファイル	◎ ライセンス管理	
a6 2222		部外条件	🗅 レポートカスタマイズ	囲 リポジトリ	
── SSH設定		■ 認証プロファイル	DNS DNS	■ 除外ホスト	
📓 システム設定		₩5 接続診断	☑ 業務時間	セキュリティ	
∅ リブランディング		③ 可用性アラート	蟇 装置グループ		
1日 スナップショット設定		▲ 装置情報	→ <i>∞</i> //b		
🖉 セルフ監視			その知道		
衛 セキュリティ設定			圆 SNMP設定		
△ プライバシー設定			む アラートプロファイル		
♥。 サードバーティ製品の統合			国 ユーザー名-IPマッピング		
			▶ ユーザー設定		
			№ 通知テンプレート		

13.10 サポート

本ページは、主に本社サポートやマニュアル(英語)への案内が表示されます。 [コミュニティと詳細]の項目では、インストール環境情報やアップグレード履歴を確 認することができます。

日本国内における正規のサポート窓口や関連資料については、次章をご確認ください。

Firewall Analy	zer									*		Q	₽ ‡
シュポード インベ	ントリ アラート	レポート	ルール管理	コンプライアンス	ス 検索	ツール	設定	サポート					
ポート情報			セル	フサポート				お問い	合わせ				
<mark>サポート</mark> 技術サポートの依頼			• 🗌 Fi	Lーザーガイド irewall Analyzerのヘル	プ情報			• Fire	wall Analyzerサポー	トチームヘメ	ールでお問	い合わせ	ţ
サポート情報ファイル サポート情報ファイルの	レを作成 D作成		ל י ע	・レッジベース リリースノート、使いこ	こなし情報などを掲	載していま	र व	• 当社	サポートチ ー ムに連	絡します			
ログログの閲覧			• 槻 Fi	戦能に関するご要望 irewall Analyzerの機能	要望に関するお問い	い合わせ		製品レ	ビュー				
DBクエリ データベースクエリの実	行		ן • ג	ラブルシュートのも くある技術的な問題の	ヒント(よくある)、トラブルシュー	5 <mark>質問)</mark> トガイドで	ँचे	• Fire Fire ਰੁ	wall Analyzer レビ wall Analyzerについ	ユーサイト て、お客さま	からのご意	観をお待	ちして
スレッドダンプ 作成スレッドダンプ			• \$ \$	レステムパフォーマン レステムパフォーマンス	ンス Rを監視・解析しま	đ							
ミュニティと詳細													
泉 ユーザーコミュニテ		(j) インブ	ストール情報	☐ DB情報	() ボーリング	ÉXE	① アップク	ブレード詳細	₽ フローレー	۲			
ビルド番号	日付												
127124	25 1 2024	07:19:55 午後 JST											
127004	25 1 2024	06:08:32 午後 JST											
126288	2172023	03:12:08 午後 JST											
126110	21 2 2023	03:54:15 午後 JST											

14 お問い合わせ窓口と関連資料

日本国内における正規のお問い合わせ窓口および、FWAのユーザーガイドやナレッジ ベースなどの関連資料について記載します。

14.1 お問い合わせ窓口

製品に関する技術サポート窓口やその他お問い合わせについては、以下のページをご確 認ください。

評価版ユーザーのお問い合わせ窓口 https://www.manageengine.jp/support/trial.html

製品購入後(保守ユーザー)のお問い合わせ窓口

https://www.manageengine.jp/support/purchased.html

保守ユーザー様は、下記のお客様専用ポータル「ManageEngine Community」よりお問い合わせください。

ManageEngine Community
 <u>https://adcommunity.manageengine.jp/jsp/login.jsp</u>

・ManageEngine Communityマニュアル <u>https://jpmeuser.wiki.zoho.com/Me-Community.html</u>

価格、お見積りなどの営業に関するお問い合わせ窓口 https://www.manageengine.jp/purchase/

その他のお問い合わせ窓口

https://www.manageengine.jp/contact.html

14.2 関連資料

オンラインユーザーマニュアル

https://www.manageengine.jp/products/Firewall_Analyzer/help/

ナレッジベース

https://www.manageengine.jp/support/kb/Firewall_Analyzer/

リリース関連情報 <u>https://www.manageengine.jp/products/Firewall_Analyzer/help/release_info.html</u>

簡易版スタートアップガイド

https://www.manageengine.jp/products/Firewall_Analyzer/startup-guide.html

<製品提供元> ゾーホージャパン株式会社 〒220-0012 神奈川県横浜市西区みなとみらい 3-6-1 みなとみらいセンタービル 13 階 ・ホームページ <u>https://www.zoho.co.jp</u>

・Firewall Analyzer製品ページ https://www.manageengine.jp/products/Firewall_Analyzer/