FortiGate の情報取得

FortiOS v2.80 用

以下の情報を弊社宛に送付ください。
これらの情報をメーカへ送り原因追求、解析を致します。

１．基本ステータス

・問い合わせ対象の状況やネットワーク構成図

障害発生日時

IP アドレスや機器構成、インターフェースなどがわかる全体図を送付ください。

再現手順（まずは御社でご確認いただいている範囲でお願いします。）

・Log の取得（ログ設定により取得できない可能性がございます。）

WebUI より

システム[メニュ]→ログ&リポート[メニュ]→ログアクセス[メニュ]→

トラフィックログ[画面タブ]にて TrafficLog の取得

イベント[画面タブ]にて EventLog の取得

アタック[画面タブ]にて AttackLog の取得

アンチウィルス[画面タブ]にて Anti-virusLog の取得

※ ログは“ Raw データに変換”を行い取得をお願いします。

※ syslog で取得している場合はそちらの取得をお願いします。

※ syslog で取得できない場合は HDD から各ログを RAW データで取得お願いします。

・Config ファイルの取得

WebUI より

[システム]→[メンテナンス]→[バックアップと復元]→[システム設定]→[バックアップ]→

システム設定：バックアップ→システム設定をダウンロードする にて Config の取得

全ての設定ファイル：バックアップ→全ての設定ファイルをバックアップする にて Config の取得（この時パスワードは未入力でお願いします)

・**Debug ログの取得**

WebUI より

システム[メニュ]→ステータス[メニュ]→ステータス[画面タブ]→バックアップ→システム設定：バックアップ[項目]→デバッグログのダウンロードにて Debug ログの取得

※debug.log はバイナリデータのため文字化けが発生します。デコードを行うために、コピー&ペーストでなく「右クリックで対象をファイルに保存」で取得お願いします。

ファイル名が” debug[1].log”このような場合取得が失敗しています。

[1]←こちらがでないよう取得お願いします。

HA 構成の場合には以下の場所よりデバックログを取得いたします。

WebUI にログイン後

System > Config > HA > Cluster Members(ボタンをクリック) >

画面右『Download Debug Log』を表示されている全てのクラスターメンバ分

「右クリックで対象をファイルに保存」で取得お願いします。

次のコマンドを Console(シリアル)経由にて実行、取得してください。

HA(冗長)を使用されている場合は全ての機器から取得願います。

*Active 機のみログインが可能な状態で、Standby 機へのログインを実施する方法になります。

execute ha manage [?] ←先コマンドで[？] キーを入力すると HA メンバーの Index が表示されます。

この時表示されたメンバーのインデックスを入力し、Standby にログインします。

(例)

FG-01# execute ha manage

<id> please input peer box index.

<1> Subsidary unit FG100A390750xxxx

FG-01# execute ha manage 1

FG-02$ ←ドルマークに Standby 機のホスト名が表示されれば成功です。

・取得した時間の確認

execute time

execute date

・取得した時間の確認

show (Backup 側のみ)

・ステータスの確認

get system status

get system global

・CPU 負荷率、Memory 空き容量の確認

get system performance (事象発生中数回実行ください)

diagnose hardware sysinfo memory

diagnose hardware sysinfo slab

・デーモンの状況

diagnose sys top（一定時間で更新表示）CTRL + C で解除

※事象発生中約 3 分実行ください。

・System Monitor

diagnose sys matrix

※1 分間に 1 回行い、合計 3 回実行してください。

・**NIC / Ethernetの状況**

diagnose netlink device list

diagnose netlink interface list

diagnose hardware deviceinfo nic [インターフェース名]

※すべてのポートを取得してください。

get system interface

get system interface [インターフェース名]

※ すべてのポートを取得してください。

・**ルーティング / セッション情報**

diagnose netlink ip list

diagnose netlink neighbor list

get router info routing_table

diagnose netlink route list

diagnose sys session stat

diagnose netlink brctl name host root.b

・**HA の設定、動作状況等の確認**

＊HA 使用している場合取得願います

get system ha

diagnose sys ha ldb

diagnose sys ha mac

diagnose sys ha showcsum

diagnose sys ha stats

diagnose sys ha status

diagnose sys ha diffcsum (Backup 側のみ)

diagnose sys ha checksync (Backup 側のみ)

・　**シグネチャアップデート設定、状況の確認、デバッグ情報**

＊ライセンスを使用している場合取得願います

diagnose sys autoupdate status

diagnose sys autoupdate versions

diagnose test update info

・Fortiguard Webfilter AntiSpam 情報

＊ライセンスを使用している場合マスター側のみ取得願います

diagnose spamfilter fortishield statistics list

diagnose debug rating

diagnose webfilter catblock statistics list

execute ping update.fortiguard.net

execute ping antispam.fortiguard.net

execute ping webfilter.fortiguard.net

execute ping www.fortinet.com

*コマンドによってはメーカ診断コマンドも含まれるため内容についてお答えできかねる場合があること、予めご了承ください。