FortiGate 情報取得ガイド FortiOS v4.0 向け

本資料の情報を弊社宛に送付ください。 取得頂いた情報をメーカへ送り原因追求、解析を致します。

v1.7



- 1. お問い合わせ対象のネットワーク構成図(必須)
 - ・ IP アドレス体系、機器構成などが把握出来る全体図を送付下さい。(例:図1)



2. エスカレーション用基本情報(必須)

以下の3つの情報を弊社までご連絡願います。

2.1 障害情報 (必須)

状況を把握する為、可能な限り詳細に障害に関する情報を連絡願います。
(例)
1.初めに障害が発生した日時
2. 障害の原因が FG にあると判断した切り分け情報
3. 障害復旧の前後で、FG 及び FG 以外の設定変更有無
4. 障害が復旧するまでに行っていた作業内容

5. 問題再現性の有無・頻度・可能であれば再現手順

2.2 Log の取得 (必須)

FortiGate は以下ポイントにログの出力が行えます。(モデル・環境によって異なります。) ・本体メモリ・HDD(搭載機の場合)・FortiAnalyzer・syslog お客様環境で使用されているポイントより可能な限り事象の発生前 (正常時のログ)、発生中、発生後を含む範囲のログを提供願います。 >>取得方法を後述します

2.3 本体ステータス (必須)

機器の状態を正確に把握するため機器にて機器のコンフィグ・コマンドを実行し、 情報の収集を願います。

>> 取得方法を後述します

2.2 Log の取得 -- 取得方法-

・HDD、FortiAnalyzer、syslog が稼働している場合

->いずれかの機器からログを取得願います

・上記に該当しない場合

->FortiGateの本体メモリからログを取得願います

ヒント: VDOM 環境のログ取得方法

System Dashboard Dashboard Dashboard Dashboard Dashboard Dashboard Dashboard Dashboard Dashboard Dashboard Dashboard Dashboard Dashboard Dashboard Dashboard Dashboard Dashboard Dashboard Dashboard Dashboard	左記図の①をクリックする事によって、WebUIの VDOM を切 り替える事が可能です。
UTM Log&Report Current VDOM Global	

■ HDD からの取得

*VDOM 環境の場合、ログは VDOM 毎に記録されています。

 FortiGate の WebUI にて Log&Report > Log Access にアクセス 事象に該当する種類のログ(イベント・antivirus 等) をクリックし (図 2-1-①)にて Disk を選択(図 2-2-①) "Raw データに変換"(図 2-2-②)をクリック ログを範囲選択・コピーペーストし取得願います 	Log&Report
*イベントログは必ず取得願います。その他機能のログは事象に応じて取得願います。 *事象発生時間帯のログを取得してください。	 Log Config Log Setting Alert E-mail Event Log Log Access Application Control DLP Email Filter Attack Web Filter AntiVirus Event Traffic

			1	3	2	
2 Refresh	ា Clear All Filters	Column Settings	• Disk C Memory	HA Cluster: FG30	€ F	Formatted C Raw
# 🍸 Date	🝸 Time 🛛 🍸 Leve	el 🛛 🝸 Sub Type	VID V Source	V Destination	🝸 Service 🛛 🍸 Sent	t 🝸 Received
			No entries fo	und.		

図 2-2 (ログ取得の画面-HDD)

■ FortiAnalyzer による取得-

-WebUI による取得-

1. FortiAnalyzer の WebUI にて TOP の Statistics(図 3-1-①)にアクセス

2. 該当デバイスから事象に該当する種類のログ(イベント・antivirus 等)をクリック(図 3-2-①-②) *イベントログは必ず取得願います。その他機能のログは事象に応じて取得願います。

- 3. Download(図 3-2-③)をクリック
- 4. CSV、圧縮を有効にしてファイルをダウンロード(図 3-3-①)
 - * HA環境の場合ログは統合されているため特別なログ取得手順は御座いません

Statistics (Since 2010-04-27 12:02:30)								
Sessions	9 current sessions	[Details]						
Logs & Reports		(1)						
Logs	7 new log files for 1 devices	[Details]						
Log Volume	82.06 MB/day for past 7 Day	[Details]						
Reports	0 reports generated for 0 devices	[Details]						

図 3-1 (ログ取得の画面-FortiAnalyzer)

	(3							
道 Dele	te 🖳 Display	📥 Download	🖑 Import	Device Type:	FortiGate		Show Log File Names		
		Log F	iles			#	From	То	Size (bytes)
– N	o Group				1	10	Thu Apr 8 14:36:28 2010	Thu May 13 18:42:51 2010	486,601,655
\square	FG300B)		6	Thu May 13 16:19:21 2010	Thu May 13 18:42:51 2010	442,068,115
	Attack					0			0
	Email Filter					0			0
	Event					1	Thu May 13 16:19:21 2010	Thu May 13 18:42:51 2010	10,967
	TM IM					0			0
E 2	Traffic					5	Thu May 13 17:07:11 2010	Thu May 13 17:19:38 2010	442,057,148
Г							Thu May 13 17:19:22 2010	Thu May 13 17:19:38 2010	22,626,519
							Thu May 13 17:18:08 2010	Thu May 13 17:19:22 2010	104,857,615
							Thu May 13 17:15:50 2010	Thu May 13 17:18:08 2010	104,857,612
							Thu May 13 17:10:54 2010	Thu May 13 17:15:50 2010	104,857,708
							Thu May 13 17:07:11 2010	Thu May 13 17:10:54 2010	104,857,694
	AntiVirus					0			0
	VoIP					0			0
	🔽 Web Filter					0			0
	DLP					0			0
	Application Complexity	ontrol				0			0
	Network Scar	ı				0			0

図 3-2 (ログ取得の画面-FortiAnalyzer)

Download Log File
CSV Compress with gzip
OK Cancel

図 3-3 (ログ取得の画面-FortiAnalyzer)

■ メモリでの取得の場合

*VDOM 環境の場合、ログは VDOM 毎に記録されています。 そのため、ログの取得時には管理 VDOM および問題のある VDOM から取得してください。 TFTP もしくは WebUI より取得願います。

-TFTP による取得 (TFTP 利用可能環境の場合は推奨)

CLI(コンソール・TELNET・SSH)にて以下のコマンドを実行する事で、機器のメモリに保存 されているログを出力します。

[TFTP]

execute backup memory alllogs tftp <TFTP サーバ IP アドレス> text

*HA環境の場合、Standby機のログ情報も同時に取得出来ます。

-WebUI による取得-



図	4-1 (ログ取得の画面-メモリ)
---	-------------------------	---

Log&Report

_					\bigcirc			3			2		
ſ	🥏 Refresh	📋 Clear Al	l Filters	Column Settings	Oisk (Memory		HA Cluster: FG	530		For	matted 🔿 R	aw
	# 🍸 Date	🝸 Time	T Leve	el 🛛 🝸 Sub Type	T ID	V Source	-	Destination	Y Service	Y	Sent	💎 Received	d
						No entries fo	unc	1.					

図 4-2 (ログ取得の画面-メモリ)

2.3 本体ステータスの取得 –取得方法-

■ Config ファイルの取得

WebUI より

- 1. TOP 画面中の system information > System Configuration [Backup]をクリック(図 5-1-①)
- 2. Config の取得 *暗号化・パスワードは入力せずにデフォルトのまま取得してください。

System Information	n	
Serial Number	F(
Uptime	0 003(0) 11 1001(0) 0 1111(0)	
System Time	Fri May 14 10:10:19 2010 [Change]	
HA Status	Active-Passive [Configure]	
Cluster Name	FGT-HA	
Cluster Members	FG300	(Master)
Firmware Version	v4.0, [Upd:	
System Configuration	Lost Dockup: Thu May 13 17:23:09 2010 [Backup] [Restore]	
FortiClient Version	Unknown	
Operation Mode	NAT [Change]	
Virtual Domain	Disabled [Enable]	
Current Administrators	1 [Details]	
Current User	admin [Change Password]	

図 5-1 (config 取得の画面)

■ CLI 情報の取得

冗長・VDOM 構成に操作方法

以下コマンドを Console(シリアル)・Telnet・SSH のいずれかにて実行取得してください。 *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。

注意:HA環境の場合、全ての機器から情報を取得してください。 注意:VDOM環境の場合、VDOM毎の情報取得が必要になりますので、指定してある階層 で実行願います。

- HA Standby へのログイン方法-

(例)

FG-01# execute ha manage

<id> please input peer box index.

<1> Subsidary unit FG100A390750xxxx

FG-01# execute ha manage 1

FG-02\$ ←Standby 機のホスト名が表示されれば成功です。

-仮想(VDOM)環境での CLI 操作方法-

・Global 階層への移動方法
(例)
FG-01# ←ログインした状態
config global
(global) # ←グローバル階層
・VDOM 階層への移動方法
(例)
FG-01# ←ログインした状態
config vdom

(vdom) # edit xxx←vdom 名を入力

((VDOM 名) #←VDOM 階層

<u>取得コマンド表</u>

 ステータスの確認 (Global 階層で実施) get system status get system global

・サポート情報

(root vdom 階層で実施) diagnose debug crashlog read diagnose log alertconsole list

 CPU 負荷率、Memory 空き容量の確認 (Global 階層で実施) get system performance status
 ※可能な場合正常時・事象発生中に複数回実行してください。
 diagnose hardware sysinfo memory

・デーモンの状況 (Global 階層で実施)
 diagnose sys top 2 CTRL + C で解除
 ※可能な場合正常時・事象発生中に1分実行してください。

デーモンの詳細 (Global階層で実施)
 diagnose test application proxyworker 4
 diagnose hardware sysinfo shm
 diagnose test application http 4
 diagnose test application ftpd 4
 diagnose test application smtp 4
 diagnose test application pop3 4
 diagnose test application scanunit 4

 NIC / Ethernetの状況 (Global階層で実施) get hardware 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。 ・ルーティング / セッション情報

(Global 階層で実施) get sys session-info statistics

(vdom 階層で実施) get system arp get router info routing-table database (NAT/Route モードのみ表示) diagnose ip route list diagnose ip rtcache list diagnose netlink brctl name host root.b (TP モードのみ表示) diagnose netlink brctl list (TP モードのみ表示)

・HAの設定・動作状況等の確認(Global階層で実施)

※HA 構成を組んでいる場合

diagnose sys ha status diagnose sys ha dump 1 show full-configuration system ha

 ・VPN 情報 (vdom 階層で実施)
 *VPN を使用している場合 get vpn status tunnel list

・ライセンスの確認

* ライセンス(AV・IPS・WebFilter・AntiSpam)を使用している場合 (Global 階層で実施) get system auto-update status get system auto-update versions get webfilter ftgd-statistics get webfilter status ※上記コマンドは1分間に1回行い、合計3回実行してください。 diagnose spamfilter fortishield servers ※上記コマンドは1分間に1回行い、合計3回実行してください。

(rootvdom 階層で実施) diagnose test update info exe ping update.fortiguard.net (Master 機で実行) exe ping service.fortiguard.net (Master 機で実行)