SG3600LM, SG3600LG, SG3600LJ

V8.0, V8.2, V8.3

InterSecVM/SG V4.0

syslog 転送設定手順書

NEC
2019 年 10 月　第 3 版

目次

1. はじめに

1.1 本書について

本手順書は、SG シリーズのsyslog転送の設定手順書です。

1.2 用語説明

本書で使用する用語を表 1.2-1 に示します。

表 1.2-1 syslog 転送の用語説明

用語	説明
syslog	システムの動作状況やメッセージなどの記録（ログ）を取るプログラム。ネットワークを通じて他のコンピュータとログを送受信する機能もあり、そのためのプロトコルは syslog プロトコルとして RFC 3164 で標準化されている。
syslog サーバ	syslog を転送するときの送信先サーバ
システムログ	OS やソフトウェアなど、全体を管理する中核的なシステムが記録している動作履歴のこと。

1.3 機能概要

SGのsyslog転送は、特定のログをシステムログに出力し、出力したログを任意のサーバ（syslog サーバ）に転送する機能です。

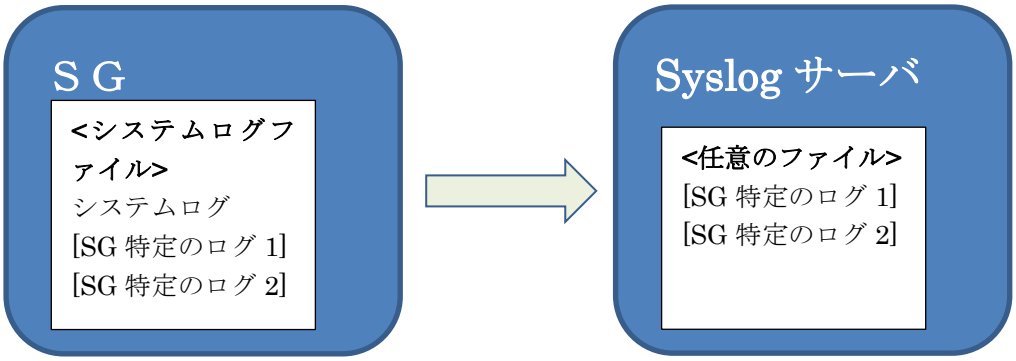

図 1.3-1 syslog 転送イメージ図

syslog転送の設定を行うことにより、SGの特定のログがシステムログに出力され、且つ、その特定のログのみsyslogサーバに転送することができます。本転送にはrsyslogの転送機能を使用します。

サポートしている通信プロトコルは、TCP、UDPです。syslog転送の暗号化はサポートしていません。

尚、SG のシステムログには出力せずに、syslog サーバに転送することも可能です。InterSecVM/SG は容量の関係上、本設定が必須となります。

2. SGのログの種類

syslog転送の対象となるログは、下記の種類（イベント種別）です。

表 1.3-1 ログの種類

分類	イベント種別	ログの内容
通信関連	SYN-SCAN 検出	SYN SCAN 攻撃を検出したときのログです。
	SYN-FLOOD 検出	SYN FLOOD 攻撃を検出したときのログです。
	PING-SWEEP 検出	PING SWEEP 攻撃を検出したときのログです。
	パケット受付	登録されたFWルールのうち、「処理：許可」「記録：アラート＋ログ」として登録したルールに該当する通信が発生した場合のログです。
	パケット拒否	登録された FW ルールのうち、「処理：破棄、拒否」「記録：アラート＋ログ」として登録したルールに該当する通信が発生した場合のログです。
	通信ログ（上記以外）	非公開(※)
通信関連以外	ユーザ認証	グループルールのユーザ認証画面で、ログインに失敗したときのログです。
	ファイル改ざん監視	非公開(※)
	プロセス監視	非公開(※)
	その他（上記以外）	非公開(※)

(※) 障害発生時に、サポート窓口より設定をご依頼させていただく場合があります。
それ以外で使用されても問題はありませんが、本ログの詳細は公開していません。

3. 設定方法

3.1 SG の設定方法

SGへのsyslog転送の為の設定は、下記の流れとなります。尚、syslogサーバに転送のみ行い、ＳＧのシステムログの出力は抑制したい場合は、下記の④も実施ください。

① システムログへの出力設定 （WBMC(WebManagementConsole)で設定）
② 通信ログ設定 （WBMC(WebManagementConsole)で設定）
③ syslog 転送の設定 （コンソールで設定）
④ (SG3600 任意, InterSecVM/SG 必須)SG のシステムログへの出力抑制 （コンソールで設定）

3.1.1 アラートのシステムログへの出力設定

下記の手順にて出力するログの種類を指定し、システムログの出力の設定を行います。

① 「ファイアウォール ＞ 詳細設定 ＞ アラートアクション設定」画面を開いてください。
② “通知方法-SYSLOG 出力”のファシリティは「LOCAL0」、レベルは「ALERT」を指定してください。
③ システムログに出力したいイベント種別の”通知イベント-イベント種別-SYSLOG チェックボックス “をチェックしてください。
④ 更新ボタンを押下してください。

図 3.1-1 出力ログ指定

3.1.2 通信ログ設定

通信ログの「SYN-FLOOD検出」、「PING-SWEEP検出」、「パケット受付」、「パケット拒否」出力時は、下記の設定も実施してください。

●「SYN-FLOOD 検出」、「PING-SWEEP 検出」

① 「ファイアウォール > かんたん設定」で「再設定」を押下します。
② 「次へ」を押下して画面を進めていき、“不正アクセス対策レベルを選択します”という文言が画面上部に表示されましたら、「ベーシック」もしくは 「アドバンス」を選択し、「次へ」を押下してください。

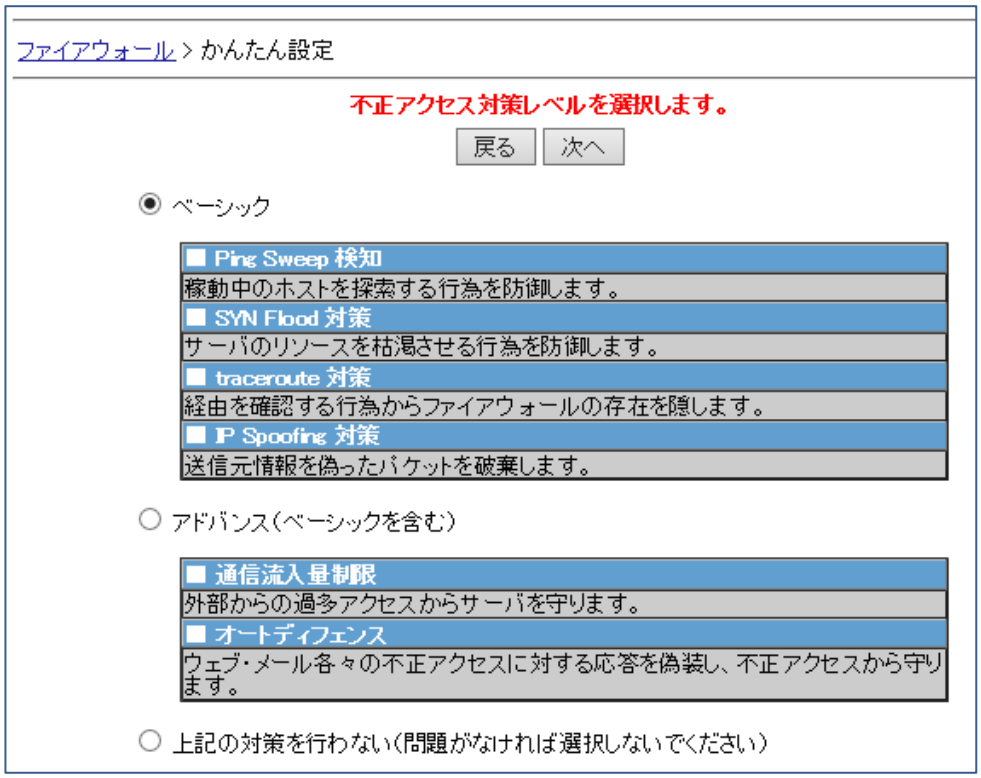

図 3.1-2 かんたん設定の設定

③ その後、“下記のように設定してよろしいですか？”という文言が画面上部に表示されましたら、「設定」を押下してください。

●「パケット受付」、「パケット拒否」

ファイアウォール > 詳細設定の「■ルール設定」の各種設定において、“記録”は「アラート+ログ」を指定してください。

・サイト共通ルール

「ファイアウォール > 詳細設定 > ルール設定（サイト共通） > ルール設定追加」画面
「ファイアウォール > 詳細設定 > ルール設定（サイト共通） > ルール設定更新」画面

・グループルール

「ファイアウォール > 詳細設定 > ルール設定(グループ) > グループルール > 設定追加」画面
「ファイアウォール > 詳細設定 > ルール設定(グループ) > グループルール > 設定更新」画面

・LDAP グループルール

「ファイアウォール > 詳細設定 > ルール設定(LDAP グループ) > LDAP グループルール > 設定追加」画面

下記はサイト共通ルールの場合の手順です。

① 「「ファイアウォール > 詳細設定 > ルール設定（サイト共通)」で、「挿入」「追加」、もしくは、対象となるルールを選択します。

② 編集画面の「■記録」にて、「アラート+ログ」を指定してください。その他の項目は、適切な値を入力ください。

③ 「登録」を押下ください。

図 3.1-3 サイト共通ルール画面での記録設定箇所

④ 「「ファイアウォール > 詳細設定」にて「編集結果を適用」を押下ください。

3.1.3 syslog 転送の設定

設定を行うために、SGにコンソール接続、またはSSH接続の何れかでログインしてください。

下記は root 権限で実行してください。

1 vi などのエディタで/etc/rsyslog.conf を開いてください。

2 /etc/rsyslog.conf に以下の設定を追加してください。（★行追加）

```
# ### end of the forwarding rule ###
# Save sudo messages
local2.*                        /var/log/sudo.log
# Save racoon messages
local4.*                        /var/log/racoon/messages
# Save hasg messages
local5.*                        /var/log/hasg/hasg.log
local0.alert    @192.168.10.100:514        →★追加
local0.alert    @@server.example.net:514       →★追加
```

＜フォーマット＞

●UDP 通信の場合

local0.alert　　@[syslog サーバの IP アドレス or FQDN]:[syslog 転送のポート番号]

●TCP 通信の場合

local0.alert　　@@[syslog サーバの IP アドレス orFQDN]:[syslog 転送のポート番号]

（補足）

・local0.alert は固定です。

・syslog 転送のポート番号は一般的に 514 ですが、syslog サーバの設定に依存します。

・複数の syslog サーバに転送する場合は、並べて記載してください。

例)

```
local0.alert        @192.168.10.148:514
local0.alert        @192.168.10.149:514
```

・syslog サーバを FQDN で記載する場合、DNS で IP アドレスが引ける状態としてください。

3 下記のコマンドを実行してください。

```
service rsyslog restart
```

3.1.4 (SG3600 任意, InterSecVM/SG 必須)SG のシステムログへの出力抑制

syslogサーバに転送のみ行い、SGのシステムログの出力は抑制したい場合は下記の手順を実施ください。
設定を行うために、SGにコンソール接続、またはSSH接続の何れかでログインしてください。

下記は root 権限で実行してください。

1 vi などのエディタで/etc/rsyslog.conf を開いてください。

2 /etc/rsyslog.conf に以下の設定を追加してください。（**太文字部分**）

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none;local2.none;local4.none;local5.none;local6.*;local0.none          /var/log/messages
```

3 下記のコマンドを実行してください。

service rsyslog restart

4. ログフォーマット

4.1 通信関連のログ

通信関連のログのフォーマットは下記です。

表 4.1-1 通信ログフォーマット

出力例

Sep 8 11:58:57 174-LM806 floga_actd[5981]: [ALT_ATTACK],Accepted.,a2,INPUT,NEW,0,eth0,,,00:24:21:03:da:00,ff:ff:ff:ff:ff:ff,192.168.10.239,192.168.10.255,229,0x00,0x00,129,14497,,,,0,UDP,,138,138,,,,,,,,,,,,,,,209,,,,,,,,

フォーマット

月 日 時刻 ホスト名 floga_actd [PID]: [ALT_ATTACK],%0,%1,%2,%3,%4,**%5,%6,**%7,**%8,%9,%10,%11,%12,%13,%14,%15,%16,%17,%18,%19,%20,%21,**%22,**%23,%24,**%25,%26,%27,%28,%29,%30,%31,%32,%33,%34,%35,%36,%37,%38,%39,%40,**%41**,%42,%43,%44,%45,%46,%47,%48,%49

※上記の**青太文字**以外は、デバッグ用情報となります。

グループ	NO.	意味
raw	%0	イベント文字列 イベント種別 / イベント文字列 SYN-SCAN 検出 / SYN-SCAN. SYN-FLOOD 検出 / SYN-FLOOD. PING-SWEEP 検出 / PING-SWEEP. パケット受付 / Accepted パケット拒否 / Dropped/Rejected 通信ログ（上記以外） / （開発者向け情報の為詳細は非公開）
	%1	ルール ID
	%2	スタック中のどのフックポイントでの処理
	%3	ctinfo_name
	%4	PF によってパケット構造体に付けられた整数値のマーク。10 進。
I/F	%5	入力インタフェース名
	%6	出力インタフェース名
	%7	欠番
	%8	ソース Ethernet MAC アドレス %02x:%02x:%02x:%02x:%02x:%02x
	%9	デスト Ethernet MAC アドレス %02x:%02x:%02x:%02x:%02x:%02x
IP	%10	送信元 IP アドレス
	%11	宛先 IP アドレス
	%12	Total Length： 全パケット長(バイト)。10 進整数。
	%13	ToS フィールド先頭から数えて 0～2 ビット 0x%02X
	%14	ToS フィールド先頭から数えて 3～6 ビット 0x%02X
	%15	Time To Live。10 進整数。
	%16	IP パケットの ID。10 進整数。
	%17	Flags の未使用ビット。"CE" or ""。現状立つこと無し。
	%18	Flags の Don't Fragment ビット. "DF" or ""
	%19	Flags の More Fragments ビット. "MF" or ""
	%20	Flagment Offset。10 進。
	%21	プロトコル ："TCP", "UDP", "ICMP", "ESP", "AH" or 番号(10 進整数)。
	%22	欠番
TCP/UDP	%23	ソースポート番号。10 進整数。
	%24	デストポート番号。10 進整数。

	%25	ウィンドウサイズ 10 進。
	%26	Reserved フィールド先頭から数えて 0～3 ビット 0x%02x
	%27	Reserved フィールド先頭から数えて 4 ビット "CWR" or ""
	%28	Reserved フィールド先頭から数えて 5 ビット "ECE" or ""
	%29	Control Flag URG ビット。"URG" or ""
	%30	Control Flag ACK ビット。"ACK" or ""
	%31	Control Flag PSH ビット。"PSH" or ""
TCP	%32	Control Flag RST ビット。"RST" or ""
	%33	Control Flag SYN ビット。"SYN" or ""
	%34	Control Flag FIN ビット。"FIN" or ""
	%35	Urgent pointer. 10 進。
	%36	シーケンス番号 10 進。
	%37	ACK 番号 10 進。
	%38	欠番
	%39	TCP ステート
UDP	%40	UDP パケット長 10 進。
	%41	タイプ 10 進
	%42	コード 10 進
	%43	echo, echo-reply の場合の ID。10 進
ICMP	%44	echo, echo-reply の場合のシーケンス番号。10 進
	%45	parameter problem の場合の parameter 10 進。
	%46	redirect の場合のゲートウェイ IP アドレス
	%47	destination unreachable 等の場合の MTU。10 進。
ESP,AH	%48	ESP, AH の場合の SPI。
予備	%49	欠番

4.2 通信関連以外のログ

通信関連以外のログのフォーマットは下記です。

●ユーザ認証

表 4.2-1 ユーザ認証ログフォーマット

出力例	
Sep 8 10:27:26 174-LM806 floga_actd[13777]: [ALT_ATTACK], <usr1> locked out. (from 192.168.10.48)	
フォーマット	
月 日 時刻 ホスト名 floga_actd [プロセス番号]: [ALT_ATTACK], <%0> locked out. (from %1)	
NO.	意 味
%0	ユーザ名
%1	アクセス端末の IP アドレス

5. 注意・制限事項

・ SG3600 の場合、アラートのシステムログへの出力設定を行う場合、1日100Mbyteを超えないようログの出力内容をご調整ください。もしくは、SGのシステムログへの出力抑制の設定を実施お願いいたします。システムログにはサイズの上限がございません。その為、システムログの肥大化が続いた場合は、SGに深刻な問題が発生する場合がございます。
尚、InterSecVM/SG は容量の関係上、SG のシステムログへの出力抑制の設定は必須となります。

・ システムログの機能（rsyslog）では、5秒に200以上のログが発生した場合、出力が抑制され下記のメッセージが表示されます。また抑制されたログは、syslogサーバには転送されません。
例）Sep 15 11:24:23 LG806-184 rsyslogd-2177: imuxsock begins to drop messages from pid 11950 due to rate-limiting

・ syslogサーバの再起動や、syslogサーバとSG間で通信障害が発生した場合に、syslog転送が停止しているときは、SGにコンソール接続、またはSSH接続の何れかでログイン

・rsyslog.confはバックアップ対象外です。リストア時必要に応じて、rsyslog.confを再設定ください。

以上