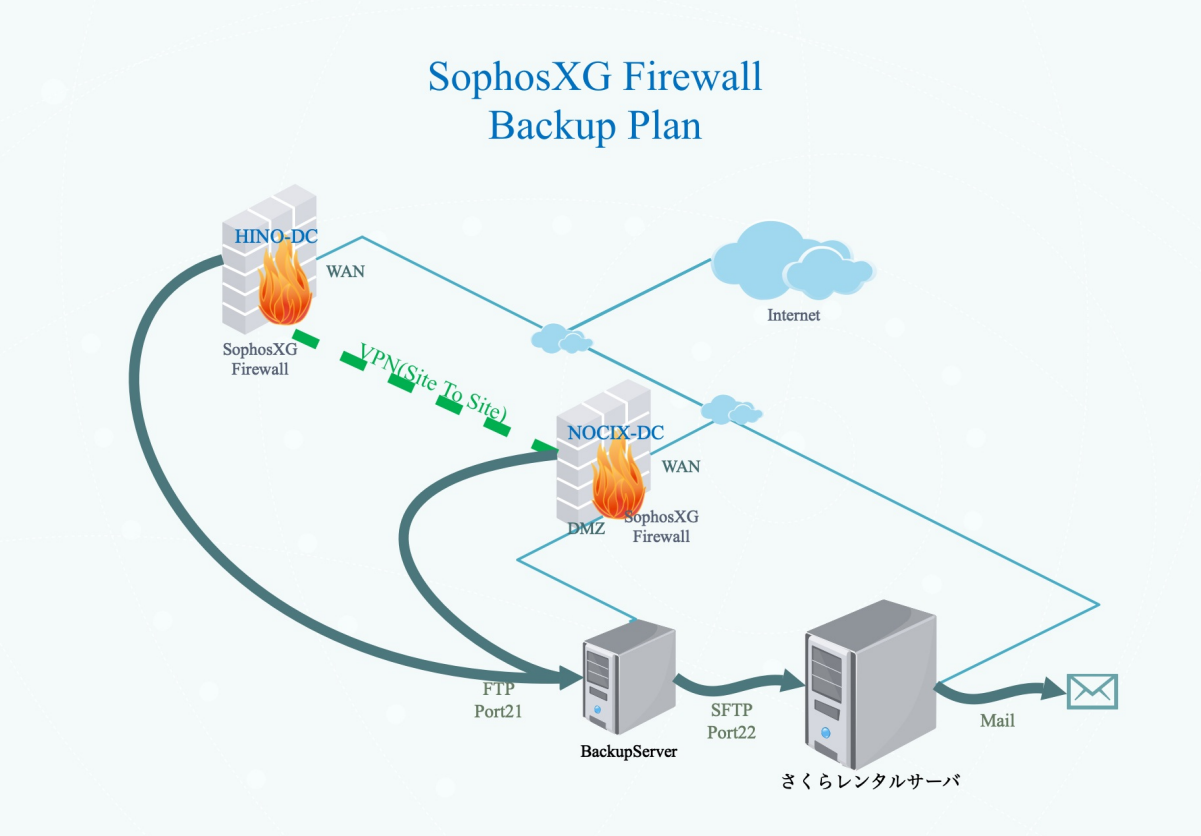
Table of Contents

URL一覧

- Ssh_Attack_Reporter
- phpmyadmin
- Blog
- Zabbix

バックアップ構成概要



各拠点のSophosXGのコンフィグのバックアップを次の３箇所に日次で作成する。

- バックアップサーバ
- さくらレンタルサーバ
- 管理用メールボックス

バックアップは下記の要項で実施する。

1. SophosXG標準機能で、日次でバックアップへFTPでアップロードする。
2. バックアップサーバもSophosXG影響下にいる為、SophosXGのコンフィグをさくらレンタルサーバへもアップロードする。（バックアップサーバ上のCronでSFTPでバックアップするシェルスクリプトを実行）
3. さくらレンタルサーバのメールサーバを使い、圧縮したSophosXGのコンフィグをメールで送付する。

バックアップ構成設定値

SophosXG設定値

項目	設定値（NOCIX-DC）	設定値（HINO-DC）
バックアップモード	FTP	FTP
バックアップのプレフィックス	NOCIX	HINO
FTPサーバのIP	172.16.16.99	172.16.16.99
ユーザー名	localadm	localadm
パスワード	**********	**********
FTPパス	glanz	glanz
頻度	毎日	毎日
スケジュール	00:00	00:00

バックアップサーバ

項目	設定値	備考
SophosXGコンフィグ格納ディレクトリ	/home/localadm/glanz/	-
バックアップ保管日数	6ヶ月	-
さくらレンタルサーバへのアップロード用バッチ	/root/scripts/DAILY_BACKUP_SCRIPT.sh	-
SophosXGコンフィグ送信先メールアドレス	shinji@k636174.net	-
その他	Cron設定状況は【バックアップサーバ】を参照	

専用サーバ契約情報

仮想基盤

仮想マシン

仮想マシン一覧

- [MAIN]monkey2018.k636174.net
- [MAIN]glanz.k737184.net
- [MAIN]ansible.k636174.net
- [MAIN]blog.k636174.net
- [MAIN]drive.k636174.net
- [MAIN]fsv.k636174.net
- [MAIN]gitlab.k636174.net
- [MAIN]syslog.k636174.net
- [MAIN]honeypot.k636174.net
- [SophosXG]

バックアップサーバ

仮想マシン設定情報

項目	設定値
仮想マシン名	[MAIN]glanz.k636174.net
インストールOS	CentOS Linux release 7.6.1810 (Core)
IPアドレス	172.16.16.99
コア数	8コア
メモリ	2046MB
アタッチネットワーク	DMZ
ディスク	16GB(スパース)
主な用途	バックアップ用途

OS設定値

項目	設定値
ホスト名	glanz.k636174.net
IPアドレス	172.16.16.99

Cron設定状況

実行日時（間隔）	実行するコマンド
* * * * *	php /var/www/mf_reporter/artisan schedule:run >> /dev/null 2>&1
* * 30 * *	/root/scripts/sar_k636174_net_certbot.sh
30 0 * * *	/root/scripts/DAILY_BACKUP_SCRIPT.sh

稼働サービス

- SSH
- vsftpd
- mariadb
- ZabbixAgent
- rsyslog

DAILY_BACKUP_SCRIPT.sh

```
#!/bin/bash

# Variable
TARGET_HOST=k636174.sakura.ne.jp
TARGET_USER=k636174
DEST_DIR=/home/k636174/Backup/`hostname`/
```

```
SOURCE_DIR=/home/localadm/`hostname`

# CREATE DIRECTORY
mkdir -p $SOURCE_DIR/server_status/
chown -R localadm:localadm $SOURCE_DIR

# Server Status
ps -ef > $SOURCE_DIR/server_status/`hostname`_`date +%Y%m%d_%H-%M-%S`.txt

# SophosXG Config Backup
find $SOURCE_DIR -type f -mmin -60 -exec scp '{}' $TARGET_USER@$TARGET_HOST:$DEST_DIR ';'
```