**A DOCUMENT ON BACKUP POLICY**

Backup is the essential part of data protection. No matter how well your system is treated, no matter how much it is taken care of, you cannot guarantee that your data is safe, if it exists only at one place. Backups are necessary in order to recover data from loss due to disk failure, accidental deletion or file corruption. There are many ways of taking backup and just as many types of media to use as well. Backup consists of all the policies and all other user related information. Device facilitates to take back-up only of the system data, either through scheduled automatic backup or using a manual backup. Once the backup is taken, the file for restoring the backup must be uploaded for restoring the configuration. Below are the screen elements with their description:

**Product and Environment**

**Sophos Firewall - All supported versions**



**Backup**

**Backup Mode**

Select how and to whom backup files should be sent.

Available Options:

Local - Backup is taken and stored on the Device itself. FTP - Configure FTP server IP Address (IPv4/IPv6), login credentials and FTP path. Email - Configure Email Address on which backup is to be mailed. You can configure multiple Email Addresses.

**Frequency**

Select the system data backup frequency.

In general, it is best to schedule backup on regular basis. Schedule can be determined depending on how much information is added or modified.

**Available Options:**

Never - Backup will not be taken at all daily - Backup will be taken every day weekly - Backup will be taken every week monthly - Backup will be taken every month.

Schedule: Specify the day/date and time for Daily, Weekly and Monthly backup.

Backup Now: Click to take the backup of system data till date.

****