FIREWALL POLICY

Team 00



Security Policies

StormSurge Software

**Firewall Policy**

**Application Filter**

**1. Overview**

Our overall objective is to keep our employees secure when using our services. This can be a difficult task as there are many different methods of attack a mal-intended individual can use to gain access to data in which is not intended to be seen by the public.

**2. Purpose**

Instituting a firewall policy is essential as in the case that an employee accidentally clicks a malignant link or be convinced to navigate to a page that they should not be accessing. This is a severe problem as in the event an employee navigates to a page with a keylogger or other such malware in it this could impact the entire corporation. This impact could bring about a class-action lawsuit or severe reputable damage.

**3. Scope**

This policy includes the allowance and denial of many network protocols and services that are extremely critical or dangerous to everyday workflow.

**The allowed services are as follows:**

3.1 DNS

3.1.1 This service is used to translate domain names (I.E google.com) to IP addresses. DNS is incredibly important to secure as if this service is tampered with, a simple google search could mean a devastating attack or breach on the company.

3.2 NTP

3.2.1 This protocol is used to synchronize all clocks so any encrypted transaction is not blocked because of the time difference.

3.3 ICMP

3.3.1 This protocol is used to test the connectivity between two computers. This can be extremely beneficial in configuration as if a host is not responding as expected or at all, ICMP can be used to verify a host is online and active on a specific location.

3.4 SSL

3.4.1 This protocol establishes a secure encrypted link between two hosts. Normally a client and server. This link could for email, websites or FTP servers.

3.5 General Internet

3.5.1 This allowance provides the ability to access the open internet.

3.6 MS-Update

3.6.1 This allowance provides the ability to download Microsoft and Windows updates.

3.7 Apt-get

3.7.1 This allowance provides the apt-get repositories on debian systems to update and install new applications..

3.8 Yum

3.8.1 This package manager is used on RHEL like operating systems to update and install applications and services.

3.9 Kaspersky/Kaspersky Netagent

3.9.1 This allowance will allow Kaspersky Signature and Application updates in addition to access to the Kaspersky website.

3.10 Git/Github

3.10.1 Git is a Version Control System (VCS) that can track the additions and subtractions to projects and files. Github is a resource to store Git repositories for use with multiple individuals or on multiple locations.

**All other services and protocols will be implicitly blocked.**

**Additional Network Security Measures:**

3.11 Wildfire

3.11.1 Wildfire takes most files that are passed into the network and passes them to the Wildfire cloud to be analyzed for suspicious or malicious activity. These test results will be sent back to the network to either accept the file into the network or block it entirely.

3.12 SSL Splicing

3.12.1 SSL Splicing allows encrypted traffic in the network to be decrypted and investigated.

3.13 Antivirus

3.13.1 A network antivirus piggybacks on SSL Splicing in the sense that it will investigate any traffic in the network for any malicious or suspicious activity.

3.14 Antispyware

3.14.1 Network antispyware will investigate all network traffic to ensure that no spyware is active or trying to gain access

3.15 File Blocking

3.15.1 Blocking certain types of files within the network will limit the possibility of a malicious or otherwise unnecessary file being downloaded.

3.16 Zone Protection

3.16.1 Zone protection will block against network intelligence reconnaissance, malformed packets, SYN Floods and mismatched TCP packets. All of which can introduce problems or possible vulnerability.