TISSUE ANALYTICS
SIMPLIFYING WOUNDCARE

Perimeter Firewall Policy

Version: 1.0
Effective Date: 11/18/16

Author: Joshua Budman, Chief Technology Officer

Disclaimer: This policy was created by Tissue Analytics, Inc. for the sole use of its employees and clients.

Overview

The perimeter firewall protects the company's private network and servers from unwanted traffic or potentially harmful intruders. Robustness of the firewall setup ensures that servers used by Tissue Analytics, Inc. (TA) are fully safe and secure. This is especially important since said servers are involved in the storage of patient protected health information (PHI). Thus, Tissue Analytics works with Amazon Web Services (AWS) to develop best practices in firewall setup to ensure the safety and security of its application's network.

Purpose

The purpose of this policy is to establish standards for the setup of the perimeter firewall protecting the network and database used by TA's web application. Effective implementation of this policy will minimize unauthorized or unwanted access to TA's proprietary information and technology as well as any client-associated PHI.

Scope

All employees, contractors, consultants, temporary and other workers at TA and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated or leased by TA or registered under a TA-owned internal network domain.

This policy specifies requirements for equipment on the internal TA network. More specifically, for secure configuration of equipment external to TA on Amazon Web Services, see *Amazon Web Services: Overview of Security Processes* by consulting http://aws.amazon.com/security/ for the latest version of this whitepaper. For specifics on the AWS ad hoc perimeter firewall setup one can consult http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security.html.

Policy

4.1 General Requirements

4.1.1 In order to ensure HIPAA-compliant storage of PHI, TA must use the AWS Virtual Private Cloud (VPC) service for all of its servers. This is described in detail in the *Privacy Policy.*

4.1.2 Each TA VPC must be equipped with a security group that controls both inbound and outbound traffic for associated elastic compute cloud (EC2) instances.

4.1.3 Each VPC must be equipped with Access Control Lists (ACLs) that control both inbound and outbound traffic for subnetworks

4.2 Configuration Requirements

4.2.1 IP anti-spoofing protocols must be implemented at the network layer of each instance. Specifically, RFC 2827 limits remote spoof attempts and RFC 1918 to perform packet filtering.

4.2.2 All network communication is conducted through TCP/IP (Transmission Control Protocol/Internet Protocol) port 43 and Internet Control Message Protocol (ICMP) is restricted

4.2.3 Each VPC security group is configured to eliminate superfluous network communication. Furthermore, no VPC peering is performed.

Policy Compliance

5.1 Compliance Measurement

The Information Security team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions
Any exception to the policy must be approved by the Information Security team in advance.

Related Standards, Policies and Processes

- Server Audit Policy
- Amazon Web Services: Overview of Security Processes
- Privacy Policy

Definitions and Terms

- **Amazon Web Services (AWS):** A collection of remote computing services that together make up a cloud computing platform, offered over the Internet by amazon.com.
- **Virtual Private Cloud (VPC):** On-demand configurable pool of shared computing resources allocated with a cloud environment but providing physical isolation between different organizations.
- **Elastic Compute Cloud (EC2):** A web service that provides resizable compute capacity in the cloud.
- **Transmission Control Protocol/Internet Protocol (TCP/IP):** Basic communication language of the Internet. It can also be used as a communication protocol in a private network.
- **Internet Control Message Protocol (ICMP):** The messaging protocol used by network devices to send error messages.

Revision History

Date of Change	Version Number	Responsible	Summary of Change