Solano Community College

Firewall Management Department Policy

Purpose

The purpose of this policy is to define the requirements and management of district firewalls

Scope

This IT policy applies to Solano Community College Windows workstations and servers, and network firewalls

Definitions

Firewall – A device, software, or combination of both to allow and deny access

Next Generation Firewall (NGFW) – A firewall with advanced features that can do URL filtering, threat detection, and traffic classification beyond static rules based on IP and port

Process

Windows

All Windows machines, both physical and virtual, are required to have the operating system firewall enabled, selectively allowing access to services provided on these machines.

On Windows clients, File and Print Sharing are disabled by default. Remote Desktop and Remote Assistance is enabled by default.

Network

For firewall appliances at the network edge, a NGFW will be used utilizing:

- URL filtering blocking access from internal users to known bad actors, known malware sites, and sites with illegal content
- Real-time threat detection based on known threat signatures, and advanced intelligence to detect threat behavior not yet defined by a signature
- Traffic classification to detect applications running on protocols and ports inappropriately
- Serves as a termination point to VPN access
- Firewall changes will be made by the network staff only. Requests for firewall changes must either come through a helpdesk ticket, or at the request of a department head or Vice President. Typical endw users cannot request the changes without further approvals

- The main administrator password will be kept secured and meet length requirements

Revision History

Version:	Date:	Description:
1.0	10/7/2022	Initial document