Stanford | University IT
Information Security Office

Position Paper - Creating firewall rules open to the world

Position Title	
Position Audience	Stanford Faculty, Staff, and Students
Contact	Information Security Office (https://stanford.service-now.com/it_services?id=sc_cat_item&sys_id=f7ae081a13bce2008a9175c36144b0ad)
Position Release Date	December 2018
Last Update	Initial Posting

Problem Statement

University systems that are exposed to the public Internet are subject to continuous scanning for and exploitation of vulnerabilities by adversaries, which significantly increases the risk of compromise. This exposure most often occurs via firewall rules that allow greater access than necessary.

ISO Position

Do not expose management services such as RDP and SSH to the entire internet, and refrain from using global access rules such as “allow source Any” in firewall configurations. This applies to both network and host-based firewalls. The Information Security Office may inquire about broadly permissive firewall rules and is available for consultation if you have a question about a firewall rule’s overall risk.