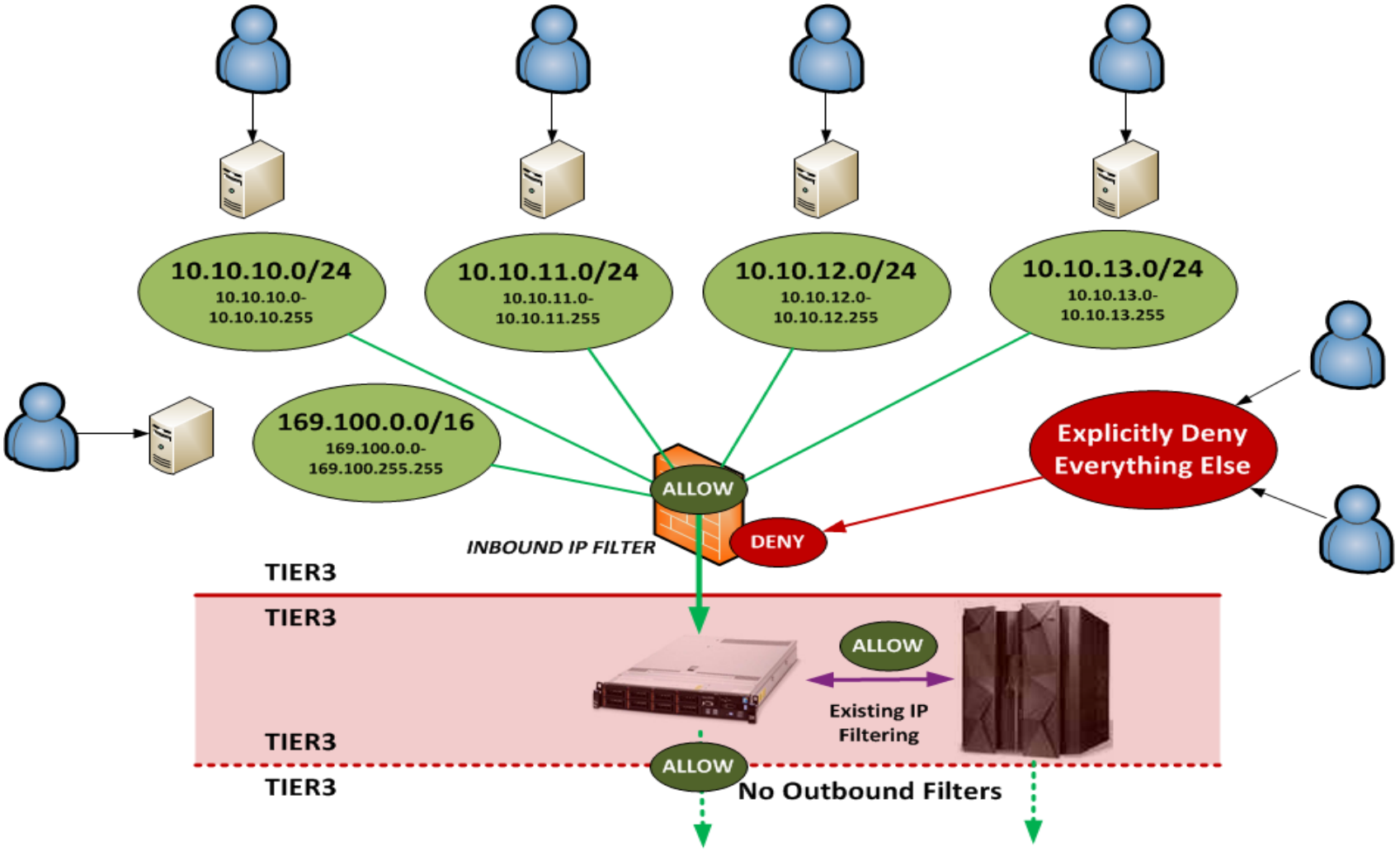
# JPMC Request to IBM for Multi-Factor Authentication (MFA) Support

*9/28/2016 – Version 2*

***JPMC has decided to make a couple adjustments to the originally communicated plan for MFA on IBM HMCs:***

- Instead of using HTTPS Proxies to control all inbound traffic presented to the zSeries HMCs; JPMC will instead have several network "segments" behind firewalls where user workstations will reside.
- These network segments will be designated as administrative user workstations built for the exclusive purpose of performing administrative tasks on all JPMC infrastructures.
- Designated JPMC users who require access to perform these type of tasks (including any work on an IBM HMC) will be authenticated via Strong MFA from their current workstation session into another workstation session within the secure network segment ("C2" Network – Command & Control).
- It is because of this that we ask that IBM modify the network whitelist to support the following (see diagram for details):
    - Allows the customer to specify IP Subnet Addresses with mask (x.x.x.x/xx) in addition to the currently allowable IP Host Addresses (x.x.x.x)
    - Provide support for up to at least a dozen "allow" IP statements to be configured & active. Subnets can range in size from */16 to */31.
    - Log all network traffic that is blocked/filtered by the whitelist within a log on the HMC, which can be viewable & exported as required by the customer.
    - (future) Customer can manually modify the IP whitelist with the proper authority role directly on the HMC, rather than IBM physically configuring the whitelist onsite.




- HMC Remote Access on Port 443 (HTTPS) must be restricted at the SUBNET IP Address level; not simply the host IP Address level.
- Inbound Remote Access to the HMCs will originate from roughly a dozen IP Subnets (ranging in size from */16 subnets to */24 subnets).
- Customer will have the ability to modify IP Filter/Whitelist rules with proper HMC role authority via HMC Remote Web Access Interface.
- HMC Firewall/Filter will log all DENY events to track un-authorized IP Address. This log will be customer accessible given proper HMC role authority.