Cyber Security

with

Galaxy 635 IP Filters

GALAXY
CONTROL SYSTEMS

ACCESS
EXCELLENCE

JAN 2018

IP Filters are strengthening Galaxy's Cyber Security.

Our primary cyber security strategy is to make our access controllers virtually invisible on clients' networks. Several years ago, Galaxy added IP filtering capabilities to its 635 CPU to alleviate network related conditions that could interfere with functionality.

As a result of this and numerous other safeguards and best practices we've initiated, Galaxy Systems maintains the highest levels of certification to supply the US government with our access solutions. Most notable is Galaxy's compliance with the United States Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) process, which requires companies and organizations to apply risk management best practices to IT systems by implementing defined activities, general tasks and a management structure with processes designed to maintain the information assurance posture throughout the system's life cycle.

- Default settings for IP Filters is OFF.
- The controller enclosure *Tamper Switch must be closed* for activated IP Filters to take effect.
- Activated IP Filters will affect access to the 635 CPUs embedded web server. When all filters are activated, the embedded web server will be unreachable unless the controller enclosure Tamper Switch is open.
- Galaxy recommends leaving IP Filters in the default settings unless the controller is experiencing problems staying on the network.
- Galaxy recommends activating all the IP Filters on 635 controllers that are experiencing problems staying on the network.

Definitions

- Syn packets: Normally, when a client attempts to start a TCP connection to a server, the client and server exchange a series of messages. The client requests a connection by sending a SYN (synchronize) message to the server. The server responds with a SYN-ACK back to the client.
- BROADCAST packets: In computer networking, broadcasting refers to transmitting a packet directed to every device on the network.
- MAC Address: The IP address is an address bound network device (e.g. computer, controller, router) via software. The MAC Address is a hardware address unique to the network adapter on the device.
- ARP: Address Resolution Protocol is used to link IP addresses to the MAC addresses. A networked device will maintain an ARP table listing the IP address and associated MAC address of each device on its segment of a network.
- Gratuitous ARPs: A Gratuitous ARP is a sort of advance notification. It updates the ARP cache of other systems before they ask for it (no ARP request)or to update outdated info.
- UDP packets: Uniform Datagram Protocol provides an unreliable packet delivery systems built on top of the IP protocol. Because of this, the amount of data that can be sent in a UDP packet is limited to the amount that can be contained in a single IP packet.

Galaxy IP Filters Explained

- Ignore Syn Packets: When enabled, the embedded web server will be unavailable.
- Ignore all BROADCAST packets: When enabled, all BROADCAST traffic will be discarded.
- Ignore all BROADCAST packets except for APR and Galaxy Control Systems: When enabled, all BROADCAST traffic will be discarded except for the standard ARP messages and GALAXY proprietary packets.
- Use MAC filtering when connected to event server: When enabled, this activates a mechanism where the MAC address of the Galaxy Event Server is found during the initial handshake. Then it is used to reject packets from all other MAC addresses.
- Send periodic gratuitous ARPs: Some network hardware assumes that all devices will participate in ARP messaging. If they do not see an ARP message froma device within a set period, the network decide will begin to ignore the device. Enabling this setting causes the CPU to periodically issue an ARP to prevent this from happening.
- Ignore UDP packets: Enabling this setting causes the CPU to ignore all UPD traffic at the network level. This includes malformed UPD packets that are addressed to the CPU.