Ports that are blocked by Allied Telesis Capital Corporation - (As of 5/23/2017)

Port	Transport	Protocol	Inbound/Outbound	Reason
25	TCP	SMTP	Both	Simple Mail Transfer Protocol (SMTP)—used for e-mail routing between mail servers. An industry recommendation to block due to infected computers sending spam email.
68	UDP	BOOTP, DHCP	Inbound	Designed to prohibit a customer's misconfigured network device from impersonating an ISP's DCHP server.
67	UDP	BOOTP, DHCP	Outbound	Designed to prohibit a customer's misconfigured network device from impersonating an ISP's DCHP server.
111	UDP	RPC	Both	Portmapper is vulnerable to DDoS(denial of service) attacks.
135-139	TCP/UDP	NetBIOS	Both	NetBIOS services allow file sharing over networks. When improperly configured, they can expose critical system files or give full file system access (run, delete, copy) to any malicious intruder connected to the network.
161-162	TCP/UDP	SNMP	Both	SNMP is vulnerable to DDoS(denial of service) attacks.
445	TCP	MS-DS, SMB	Both	Microsoft-DS SMB file sharing - Vulnerable to attacks, exploits and malware.(Sasser and Nimda worms.)
520	TCP/UDP	RIP	Both	Routing Information Protocol (RIP) - Vulnerable to various attacks.
1080	TCP	SOCKS	Outbound	Socket Secure (SOCKS) - Vulnerable to viruses, worms and DoS attacks.
1900	UDP	UPNP	Outbound	Universal Plug and Play (uPnP) - Vulnerable to attacks and exploits.
6080	TCP	HTTP	Inbound	Modem management access