SECTION 40 66 16

FIREWALL HARDWARE

PART 1 GENERAL

1.1 SCOPE OF WORK

A. Scope:

1. CONTRACTOR shall provide all labor, materials, equipment and incidentals as shown, specified and required to furnish and install network security and firewall devices as part of a fully functional control system network based on an Ethernet platform.

B. Related Sections:

1. Section 40 63 43: Programmable Logic Process Controllers.
2. Section 40 66 13: Switches and Routers.

1.2 QUALITY ASSURANCE

A. Standards, Codes and Regulations:
1. Construction of control system network and the installation and interconnection of all equipment and devices mounted within shall comply with applicable provisions of the following standards, codes and regulations:
   a. National Fire Protection Association 79, Annex “D” Standards, (NFPA).
   b. National Electrical Code, (NEC).
   c. National Electrical Manufacturer's Association Standards, (NEMA).
   d. International Society of Automation (ISA), ISA-99 standards.
   e. Underwriters’ Laboratory, Inc., (UL).
   f. International Electrotechnical Commission (IEC).
   g. Institute of Electrical and Electronics Engineers (IEEE).
   h. State and Local code requirements.
   i. Where any conflict arises between codes or standards, the more stringent requirement shall apply.

PART 2 PRODUCTS

2.1 NETWORK SECURITY DEVICE

****
NTS: INCLUDE 2.1.B.2 FOR GIGABIT SPEED NETWORKS. INCLUDE 2.1.B.7 FOR VPN CAPABILITY. INCLUDE 2.1.B.14 FOR CIFS MONITORING.
****

A. General: Provide network security devices as shown on the drawings to segregate networks and to protect critical PLCs from cyber security intrusions or failure due to unintentional traffic storm.

B. Features:

1. Copper ports shall be 10/100 base-T(X), auto-negotiation and auto-crossing. Ports shall be configurable to be enabled/disabled via the management interface.
2. Minimum of two (2) Small Form-factor Pluggable (SFP) fiber optic ports for one (1) fiber pair capable of supporting 1000 Mbps full duplex communication.
3. Supply voltage range of 9 VDC to 30 VDC, nominal 24 VDC. Capable of accepting redundant power inputs. Power connections shall be pluggable.
4. Device shall have a transparent or stealth mode that drops all unsolicited traffic from the unprotected side to the protected side of the network. Device shall support stateful inspection as a firewall.

****
NTS: DELETE 2.1.B.5 IF FULL FIREWALL FILTERING CAPABILITIES ARE NOT REQUIRED FOR THE APPLICATION. DELETE 2.1.B.6 IF SWITCH AND DMZ PORT ARE NOT REQUIRED FOR THE APPLICATION
****

5. Firewall rules shall be configurable by the user and include inspection on Source/Destination IP address, MAC address, protocols and/or Source/Destination TCP/UDP port.
6. Provide 4-port unmanaged or managed 10/100 Mbps integrated switch with DMZ port for further network segregation.
7. Support protection against IP Spoofing, Denial of Service and Syn Flood Protection.
8. Support Virtual Private Network (VPN) functionality up to 250 licenses with ability to act as client or server of VPN requests. IPSec shall be the supported VPN protocol with encryption meeting the military standard of AES-256. Provide hard-wired contact to initiate VPN tunnel.
9. Support static routing between two or more networks.
10. Support One (1) to One (1) Network Address Translation (NAT) routing.
11. Support dynamic device addressing via BootP.
12. Support the use of Rapid Spanning Tree 802.1w in transparent firewall mode. Redundancy will be integral to device and not dependent on separate management device.

13. Supports multiple VLANs.
14. Supports the use of SNMP management, up to v3 for maximum security.
15. Supports Common Internet File System (CIFS) monitoring to monitor the modification of selected files and sending alerts when files have been modified. Provide license for CIFs monitoring.
16. Two LEDs for indicating port status.
17. DIN Rail mountable.
18. Alarm contact to indicate malfunction with power supply unit or loss of port communication.
19. Capable of being configured via integrated web server working with standard browsers, including Internet Explorer ™ and Chrome ™. Configuration of device requires username and password authentication. Capable of accepting a SD card for securely storing configuration file of device.
20. Operating temperature of -20 C to 60 degrees C.

C. Product and manufacturer:

1. Phoenix Contact, mGuard Series.
2. Or approved equal.

2.2 CELLULAR NETWORK SECURITY DEVICE

****
NTS: EDIT 2.2.B.4 FOR MANAGED OR UNMANAGED CAPABILITIES. INCLUDE 2.2.B.5 IF USING MANAGED SWITCH MODEL, ELSE DELETE. INCLUDE 2.2.B.10 FOR VPN CAPABILITY. INCLUDE 2.2.B.16 FOR CIFS MONITORING.
****

A. General: Provide cellular network security devices as shown on the drawings to provide secure remote access to critical PLCs.

B. Features:

1. Copper ports shall be 10/100 base-T(X), auto-negotiation and auto-crossing. Ports shall be configurable to be enabled/disabled via the web-based management interface.
2. Supply voltage range of 9 VDC to 30 VDC, nominal 24 VDC. Capable of accepting redundant power inputs. Power connections shall be pluggable.
3. Cellular modem shall support LTE cellular technologies in a single device for a Verizon or AT&T network.
4. Provide 4-port unmanaged or managed 10/100 Mbps integrated switch.
5. Provide DMZ and WAN port for further network segregation. Provide failover redundancy between wired WAN port and cellular WAN port.
6. Provide integrated Global Positioning System functionality.
7. Device shall have a transparent or stealth mode that drops all unsolicited traffic from the unprotected side to the protected side of the network. Device shall support stateful inspection as a firewall.

****
NTS: DELETE 2.2.B.8 IF USING 2000 MODEL WHERE FULL FIREWALL FILTERING CAPABILITIES ARE NOT REQUIRED FOR THE APPLICATION.
****

8. Firewall rules shall be configurable by the user and include inspection on Source/Destination IP address, MAC address, protocols and/or Source/Destination TCP/UDP port.
9. Support protection against IP Spoofing, Denial of Service and Syn Flood Protection.
10. Support Virtual Private Network (VPN) functionality up to 250 licenses with ability to act as client or server of VPN requests. IPSec shall be the supported VPN protocol with encryption meeting the military standard of AES-256. Capable of initiating VPN via hard-wired contact or remotely through SMS text message.
11. Support static routing between two or more networks.
12. Support One (1) to One (1) Network Address Translation (NAT) routing.
13. Support dynamic device addressing via BootP and DHCP.
14. Supports multiple VLANs.
15. Supports the use of SNMP management, up to v3 for maximum security.
16. Supports Common Internet File System (CIFS) monitoring to monitor the modification of selected files and sending alerts when files have been modified. Provide license for CIFs monitoring.
17. Two LEDs for indicating port status.
18. DIN Rail mountable.
19. Alarm contact to indicate malfunction with power supply unit or loss of port communication.
20. Capable of being configured and updating firmware via integrated web server working with standard browsers, including Internet Explorer ™ and Chrome ™. Configuration of device requires username and password authentication. Capable of accepting a SD card for securely storing configuration file of device.
21. Alerts can be sent to defined list of recipients via pre-configured SMS text message.
22. Alerts can be sent to defined list of recipients via SMTP (email) message.
23. Operating temperature of -20 C to 60 degrees C.

C. Product and manufacturer:

1. Phoenix Contact, TC mGuard Series.
2. Or approved equal.

2.3 SPARE PARTS

A. Provide the following control system network component spare parts:

1. One of each type of network security device provided for project.

PART 3 EXECUTION

3.1 ENVIRONMENTAL CONDITIONS

A. The control system network will be used in a water or wastewater treatment facility environment where there will be high energy AC fields, DC control pulses, and varying ground potentials between the transducers or input contact locations and the system components. The system design shall be adequate to provide proper protection against interferences from all such possible situations.

END OF SECTION