

Magnum Secure Networking

Magnum Secure Networking is a focused initiative of GarrettCom that addresses cyber security requirements of power utilities, transportation systems, pipeline operations and other critical infrastructure sectors. Built around a Magnum Secure Networks Framework of key products and technologies, the initiative also includes marketing, Professional Services, cooperative vulnerability and needs assessments and a growing set of industry partnerships aimed at providing comprehensive solutions for both risk mitigation and compliance management.

The **Magnum Secure Networks Framework (MSNF)** consists of several functional building blocks and secure networking protocols. The MSNF can be implemented using various combinations of GarrettCom and partner products.

MSNF functional building blocks include:

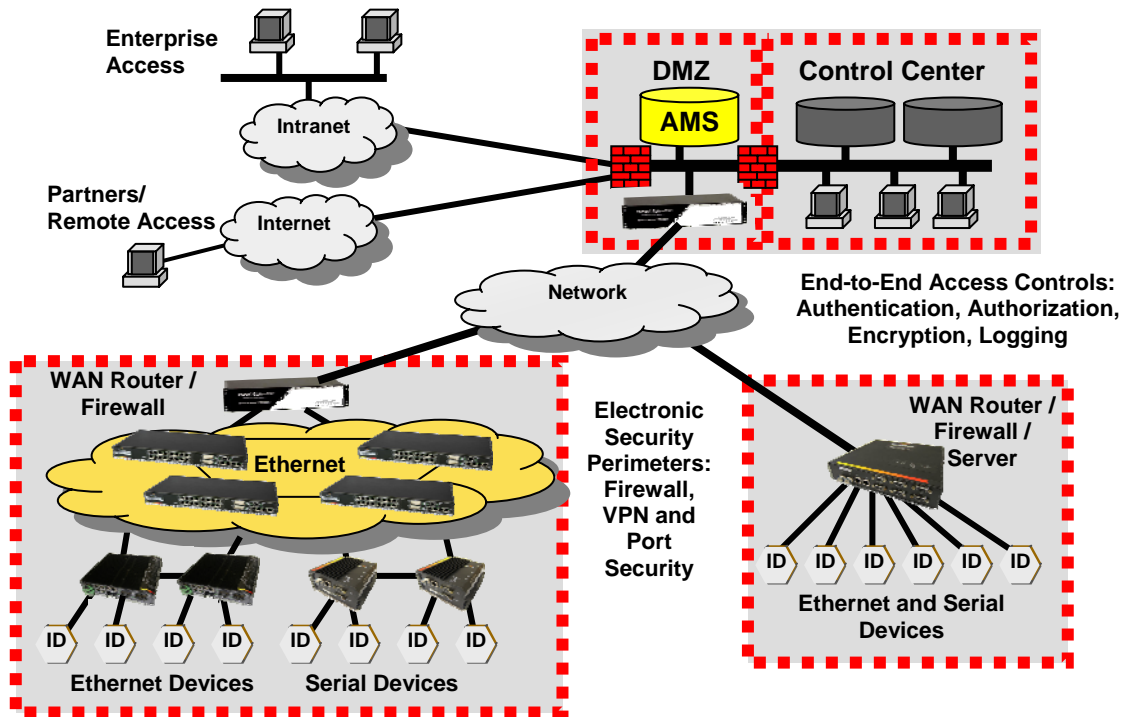
- Secure Network Management
- WAN Perimeter Security
- Serial and Ethernet Port Security
- Access Control
- Network back-up and recovery
- Legacy non-routable protocol secure transport

Secure Network Management requires each network element to implement secure management interfaces requiring rigorous authentication/authorization and both local logging and remote event notification regarding status, configuration change and network security events. Key secure management protocols and features include SSH/SSL for console access, SNMPv3, secure FTP and syslog remote logging.

Enforcement of an effective Electronic Security Perimeter requires WAN Perimeter Security, using IP Firewall and IP VPN technologies, as well as both physical and virtual port security within the perimeter. VLAN, static MAC security, and 802.1x technologies can provide Ethernet port security, while static Serial-IP and filters, serial-port SSL and serial-port VLANs can provide serial-port security. Firewall technology and/or SSL can be extended within a local site to ensure end-to-end connection security.

GarrettCom works with partners such as SubNet Solutions and Bow Networks who provide Access Management Systems for interactive access to industrial devices. By assuring interoperability including Serial-IP services and end-to-end SSL-based encryption, the MSNF provides a complete access control solution that rigorously secures system access, logs activity for compliance management and auditability, and even facilitates end-user productivity and ease-of-use.

Magnum Secure Networking (cont.)



Key products used to implement Magnum Secure Networks include all managed Magnum 6K Ethernet switching products, DynaStar Industrial Routers and Magnum DX Serial Device Routers. These products enable scalable, distributed deployment of highly secured networks, from large-scale multi-device implementations built upon an Ethernet switching core, to highly integrated single-device solutions incorporating many networking functions into a single GarrettCom product.

One major focus of Magnum Secure Networking is power utilities facing mandated compliance with NERC Critical Infrastructure Protection (CIP) standards. The attached table summarizes key GarrettCom CIP solutions.

47823 Westinghouse Drive
Fremont, CA 94539
Phone: 510.438.9071



25 Commerce Way
North Andover, MA
Phone: 978.688.8807

Email: mktg@garrettcom.com
www.GarrettCom.com

5/22/07

Magnum Secure Networking NERC CIP Compliance Solutions

Electronic Security Perimeter -- CIP-005

WAN Firewall	<ul style="list-style-type: none"> ▪ IP / TCP Filters (address/port access control) ▪ IPsec VPN ▪ Frame relay link encryption
Ethernet Port Security	<ul style="list-style-type: none"> ▪ Static MAC security ▪ 802.1x port security ▪ Port groups and tagged VLANs
Serial Port Security	<ul style="list-style-type: none"> ▪ Static Serial-IP and port filtering ▪ Serial-port SSL authentication and encryption ▪ Serial-port VLAN assignment

System/IED Access Control -- CIP-007, -4, -5

Individual Profiles	<ul style="list-style-type: none"> ▪ Central administration of individual user profiles ▪ One place to suspend or edit access rights ▪ Easy navigation / organization of permitted applications for end-user ease-of-use
Strong Authentication	<ul style="list-style-type: none"> ▪ 2-factor authentication via integration w. RSA and/or Enterprise active directory systems ▪ Enforceable strong form passwords and aging ▪ User-to-server security via SSL ▪ Server-to-IED authentication/encryption via SSL or IPsec
Session Logging	<ul style="list-style-type: none"> ▪ Logging of all sessions and access authentication events ▪ Log options for session, transaction, or keystroke ▪ Collection of remote network logs for end-to-end audits

Network Management Security -- CIP-007

Console Security	<ul style="list-style-type: none"> ▪ Strong forms passwords and aging ▪ SSH and HTTPS for authentication/encryption ▪ RADIUS support for authentication
System Security	<ul style="list-style-type: none"> ▪ SNMPv3 for encrypted system management ▪ FTP secured via SSL or IPsec
Event Logging	<ul style="list-style-type: none"> ▪ System logging for port status, access and change events ▪ syslog and SNMP traps for remote event reporting

System Recovery -- CIP-009

Backup Networking	<ul style="list-style-type: none"> ▪ Multi-master, multicast support for Serial SCADA applications ▪ Resilient networking w. frame relay redundancy/backup, dynamic IP routing and VRRP, and Ethernet RSVP
Configuration Backup	<ul style="list-style-type: none"> ▪ Remote backup of all software and configuration files ▪ Scripting support for configuration management

Asset Classification -- CIP-002

“Critical Asset” Transition Options	<ul style="list-style-type: none"> ▪ “SCADA Frame Forwarding” provides ‘non-routable’ alternative for remote SCADA consolidation ▪ Provides transition planning option to avoid classification as Critical Cyber Assets
--	---

47823 Westinghouse Drive
Fremont, CA 94539
Phone: 510.438.9071



25 Commerce Way
North Andover, MA
Phone: 978.688.8807

5/22/07