

Secure Access with VPN Technology in Industrial Networks

A Technical Brief GarrettCom[®], Inc. March 2010

Preface – An Overview of the DX Industrial Router Product Line

The Magnum DX Industrial Router family provides secure networking solutions for power utility substations, transportation systems and other rugged environments. Various models of the DX family enable Layer 2 and Layer 3 data networking, SCADA transport, remote device access, physical surveillance solutions, metering and other applications. The following list highlights some of the DX family features and qualifications for industrial secure access applications:

- IP router and firewall
- Integrated WAN, Serial and LAN interfaces
- Designed for use in secure NERC CIP compliant environments
- Ethernet switch with fiber Ethernet connectivity
- Serial-IP terminal server
- T1/E1 and DDS options with integral CSU/DSU
- Substation-hardened for harsh environments, IEC 61850-3 and IEEE 1613

The Magnum DX family of products also supports a very broad set of security related features. The DX cyber security capabilities cover both electronic perimeter protection for remote sites and management security for the DX product itself. The DX family provides a stateful IP firewall, IP address translation (NAT/PAT) and encryption options via IPsec, SSH port forwarding and serial port SSL VPNs, as well as various logging capabilities. DX management security includes encrypted interfaces (HTTPS, SSH, SFTP and SNMPv3), multi-level user IDs with strong form passwords, authentication via RADIUS, and extensive local and/or remote logging and alerting.

But, because advanced security applications are essential in many industrial markets, GarrettCom has put a major focus on delivering a complete and robust set of security features in the DX product software. This document outlines the IPsec and VPN capabilities available in the DX series of Industrial Router product family, and the benefits these features and capabilities provide to industrial customers.

The Need for Secure Access and VPN Technology

It is well documented that cyber security threats continue to rise. While these threats used to be somewhat limited to attempts to access financial data, recent data indicates that cyber attacks now cut across all business sectors. Security vendor Symantec recently revealed that 75% of organizations witnessed some form of cyber attack during 2009. As a result of this threat, industries involved with managing assets that can affect public safety, or industries that need to protect critical capital assets that can be compromised through unauthorized access, must now embrace new precautions in conducting operations.

Some U.S. industries even face federal mandates requiring protection against cyber threats. The North American Electric Reliability Corporation (NERC) introduced Critical Infrastructure Protections (CIPs) as mandatory regulations that spell out required protections to the bulk electric grid. While power utilities now face this issue by mandate, many other industries are well served to incorporate technologies to protect their facilities and infrastructure, as the consequences of doing nothing can be severe.

While there are many technologies and business practices to manage cyber security, including firewalls, virus and malware scanning, “Triple A” security (authentication, authorization and accounting), multi-level passwords, physical security and secure access (cryptography), this paper addresses one most critical component of this equation – secure access. Secure access should be used whenever control messaging, protection messaging, configuration sessions, SCADA traffic, or other secure data will traverse networks where security could be compromised. Interception, or worse, unauthorized introduction of mischief into such traffic, could severely impact critical infrastructure operation with many possibly disastrous results. So, for many applications, ensuring authenticity and security of networked connections is critical.

Of the various technologies used for secure access, IPsec and VPN technologies are by far the most widely used and most broadly applicable set of standards available to create secure connections across networks that can conceivably be compromised. Because of the importance of VPN and IPsec technologies in managing secure connections, GarrettCom continues to invest in these areas to provide interoperable, feature-rich and robust access security.

Explaining Virtual Private Networks (VPNs)

A virtual private network, or VPN, is a network that is layered onto a more general network using specific protocols or methods to make this overlay communications “private”. Thus the term, *virtual private network*. VPN sessions can be established using various techniques and then tunneled across the transport network in an encapsulated, typically encrypted and secure format, making it for practical purposes “invisible” and secure. The level of security obtained in a VPN network depends on the protocols used, the methods of authentication used in establishing the connection, and the presence and strength of any encryption algorithm used.

The term VPN can be used to describe many different network configurations and protocols. Non-secure VPNs can be used to transport, prioritize and allocate bandwidth for various customers over a multi-purpose transport network. Secure VPNs, however, do use transport and session negotiation protocols, as well as authentication and cryptography, to create secure connections over “exposed” (public, semi-public, or otherwise accessible) communications paths.

The most common use for secure VPNs is to establish remote access sessions between a VPN device, or endpoint, on one end of the “exposed” network, to another VPN device on the other end (for example across the internet). VPN sessions can be established as end-point to end-point sessions, to create a secure path between two devices or applications, or to establish a secure tunnel between two locations that can be used by many devices or end points. These alternatives

are configurable in rich VPN solution implementations. Secure VPN protocols include L2TP, IPsec, SSL/TLS VPN (with SSL/TLS) or PPTP (with MPPE). Because IPsec has enjoyed such thorough development through IETF support, and because IP is the basis for such a high percentage of communications traffic, it is an extremely robust solution in industrial networks for secure VPN access and is, in most cases, it is completely transparent to applications.

Explaining Internet Protocol Security (IPsec)

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used to protect data flows between a pair of hosts (e.g. computer users or servers), between a pair of security gateways (e.g. routers or firewalls), or between a security gateway and a host.[1] ¹

So, IPsec is a framework that uses an extensive implementation of RFC components for securely establishing end-to-end authentication, and to negotiate a variety of authentication and cryptographic algorithms to secure traffic using the secure VPN connection. Because IPsec runs at the IP layer, or Layer 3, it can be used to secure a variety of different applications and services.

In this protocol suite, different authentication and data cryptography algorithms are supported to allow for selection of algorithms appropriate to a given use. Relatively “weak” algorithms use significantly less processing power, but may be appropriate for many types of secure access needs. More sophisticated or “strong” authentication and cryptography algorithms may be more desirable for other needs requiring heightened levels of security. It is important that the “strength” of the algorithms used to securely establish authentication and the “strength” of the algorithm being used for encryption and decryption are balanced because security can depend on the “weakest link” in the security used. For example, if weak authentication is used with strong crypto algorithms, and the authentication is cracked, it is simple to decrypt the “secure” method.

GarrettCom has deployed a wide range of both authentication algorithms as well as encryption algorithms to address the various needs of customers needing secure IPsec communications. While GarrettCom continues to add new algorithms as they emerge, the following cryptography algorithms are supported in the current release of MNS-DX software, or available for support based on customer demand:

Cryptography Algorithms	Currently Supported	Subsequent Release or Customer Demand
SYMMETRIC CRYPTO:		
DES-56-CBC	X	

¹ Kent (BBN Corp) and R. Atkinson (@Home Network). ""RFC 2406 IP Encapsulating Security Payload (ESP)". Internet Engineering Task Force (IETF). <http://www.ietf.org/rfc/rfc2406.txt>.

3DES-168-CBC	X	
Blowfish—CBC	X	
AES-128-CBC	X	
AES-192-CBC>	X	
AES-256-CBC	X	
ASYMMETRIC CRYPTO:		
Diffie-Hellman Groups 1, 2, 5, 14	X	
DHE with Perfect Forward Secrecy (PFS)	X	
RSA		X
ECDSA		X
ECDH		X
SUITE B CRYPTO:		
Suite-B-GCM-128		X
Suite-B-GCM-256		X
Suite-B-GMAC-128		X
Suite-B-GMAC-256		X

Similar to the addition of new cryptography algorithms, GarrettCom continues to add new authentication algorithms as they emerge. The following authentication algorithms are supported in the current release of MNS-DX software, or available for support based on customer demand:

Authentication and Integrity	Currently Supported	Subsequent Release or Customer Demand
Certificate-based (X.509) authentication	X	
HMAC-SHA1-96		X
HMAC-MD5-128	X	
HMAC-SHA1-160	X	
HMAC-MD5-96		X
MD2		X
MD4		X
MD5	X	
SHA1	X	
SHA-224	X	
SHA-256	X	
SHA-384	X	
SHA-512	X	

This rich set of cryptography algorithms and authentication methods provide many options for medium- to very-strong security. While GarrettCom has developed capability to deliver substantial algorithms beyond what is supported in current software releases, new algorithms will be introduced based on customer demand as some algorithms are rarely used, some are already obsolete, while others are emerging.

Interoperability

In order to establish secure VPNs using IPsec, one of the most important aspects of any implementation is the interoperability of that implementation with other available products in the market. While, this would seem straightforward as VPN connections over IPsec use industry standards (RFCs) to establish the solution infrastructure and underlying code, and standards based authentication and encryption algorithms for security. For various reasons, incompatibility between VPN products from disparate suppliers is often seen.

The biggest factor in delivering broadly compatible secure VPN IPsec solutions is in developing products with complete – not partial – implementation of the RFCs called out in the standards. Solutions that provide partial RFC implementations may enjoy apparent interoperability under many interoperability scenarios, but the danger with partial implementations is that changes to other network equipment – within the bounds of the standards – can cause products with partial implementations to fail. This is particularly troublesome when this happens in the field in mission critical applications. While it is reasonable to selectively support some secure VPN IPsec features or protocols, it is critical to support all of the underlying code that is required by the features that it does support.

GarrettCom’s implementation of secure VPNs using IPsec provides full implementations of all of the RFCs and supporting code for every feature that is released into product. While GarrettCom continues to add support for new features into the product, the following table provides a view of the RFCs currently in use in the products, as well as a list of what is implemented and available for release based on customer demand. Again, this list represents full implementation of these standards.

Features and Capabilities	Currently Supported	Subsequent Release or Customer Demand
Full (not partial) RFC Compliance:		
RFC-2401, Security Architecture for the Internet Protocol	X	
RFC-2402/4302, IP Authentication Header	X	
RFC-2403/4303, The Use of HMAC-MD5-96 within ESP and AH	X	
RFC-2404, The Use of HMAC-SHA-1-96 within ESP and AH	X	
RFC-2405/4305, The ESP DES-CBC Cipher Algorithm With Explicit IV	X	
RFC-2406/4305, IP Encapsulating Security Payload (ESP)	X	
RFC-2407, The Internet IP Security Domain of Interpretation for ISAKMP	X	
RFC-2408, Internet Security Association and Key Management Protocol (ISAKMP)	X	

RFC-2409, The Internet Key Exchange (IKE)	X	
RFC-2410, The NULL Encryption Algorithm and Its Use With IPsec	X	
RFC-2451, The ESP CBC-Mode Cipher Algorithms	X	
RFC-3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile		X
RFC-3602, The AES-CBC Cipher Algorithm and Its Use with IPsec	X	
RFC-3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers	X	
RFC-3715, IPsec-Network Address Translation (NAT) Compatibility Requirements		X
RFC-3748, Extensible Authentication Protocol (EAP)		X
RFC-3947, Negotiation of NAT-Traversal in IKE		X
RFC-3948, UDP Encapsulation of IPsec ESP Packets		X
RFC 4106: The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)		X
RFC-4306, Internet Key Exchange (IKEv2) Protocol		X
RFC-4434, The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)		X
RFC 4543: The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH		X
RFC-4555, IKEv2 Mobility and Multihoming NanoSec™		X
RFC-4718, IKEv2 Clarifications and Implementation Guidelines		X
RFC 4753: ECP Groups for IKE and IKEv2		X
RFC 4754: IKE and IKEv2 Authentication Using ECDSA		X
RFC 4868: Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec	X	
RFC 4869: Suite B Cryptographic Suites for IPsec		X
OCSP integrated with IKE for On Line Certificate Status check		X
ModeConfig: draft-dukes-ike-mode-cfg-02.txt		X
XAUTH: draft-ietf-ipsec-isakmp-xauth-06.txt		X
Certificate Management RFCs Supported:		
IETF Draft: draft-nourse-scep-14.txt		X
X.509 v3 certificate		X
X.509 v2 CRL format		X
RFC-2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP		X
RFC-3280, X.509 certificate and CRL profiles		X

It is clear from this list that the secure VPN requirements commonly needed are all already supported in the GarrettCom implementation. However, the core software of GarrettCom's DX product family contains full implementations of the RFCs and specifications listed above in anticipation of future needs. Product release of these additional capabilities and features will be driven by market demand and customer requests.

Full RFC implementation notwithstanding, interoperability testing is also essential. It is always possible that one company's product code has nuances in implementation that do meet the standards, yet they do not behave quite like others, requiring one product or the other to make allowances for optimum interoperability. To address this, GarrettCom has performed interoperability testing with other key providers of secure VPN IPsec solutions. In cases where adherence to standards allows, GarrettCom products have been tuned to optimize interoperability performance with other OEM products. This testing and product tuning improves the overall robustness of the GarrettCom product offering, and can significantly improve a customer's experience in interworking disparate equipment.

To further validate interoperability, GarrettCom has participated in the LEMNOS project. The LEMNOS project is sponsored by the U.S. Department of Energy (DOE), and establishes the DOE National SCADA Test Bed (NSTB). In short, the NSTB is a multi-laboratory resource to bring together product manufactures with government test resources to evaluate, research and help design cyber security solutions. This is particularly focused on the energy sector to reduce the risk of disruptions due to cyber attack. In 2009, GarrettCom successfully participated in the LEMNOS security project and validated the DX compatibility with other LEMNOS certified products. GarrettCom is continuing to invest in this interoperability program in 2010 (and on-going) as a means of assuring continued interoperability.

Summary

GarrettCom maintains a serious commitment to providing best-in-class routing, firewall, and security features. Our focus on delivering robust IPsec and VPN capabilities is only one part of our overall strategy to provide our customers with full-featured and high-availability networking solutions. GarrettCom's secure VPN solution has been tested for interoperability with other key solution providers and is supported by a full implementation of the RFCs used to support the broad set of features and capabilities offered. While its feature content and product capabilities will continue to evolve with changing market needs, the Magnum DX family of Industrial Routers has a rich set of routing, firewall, and secure VPN capabilities ready to meet mission critical and demanding applications now.

