An Application Note from the Experts in Business-Critical Continuity

Secure Remote Monitoring of the Critical System Infrastructure

Liebert.

EMERSON™
Network Power

TABLE OF CONTENTS

Introduction

Enterprises seeking to improve the availability of business-critical systems can now utilize the Internet to dynamically control service access into their protected networks, while still shielding their assets from ongoing security threats.

Liebert, through its partnership with ComBrio, has pioneered the use of this technology in delivering robust remote monitoring of the critical system infrastructure to provide early detection and faster response to problems that could affect the availability of business-critical systems.

This white paper describes how this service is delivered with particular focus on network security.

The Liebert Virtual Ntegrity Infrastructure (VNI) solution consists of three components that work together to create a unique, policy-based Secure Connection between the Liebert command center and customer location.

Liebert Virtual Ntegrity Infrastructure Components

The Liebert Virtual Ntegrity Infrastructure (VNI) solution consists of three components that work together to create a unique, policy-based Secure Connection between the Liebert command center and customer location.

1. Virtual Ntegrity Gateway - Compact hardware appliance placed within the enterprise private network or DMZ that collects information from devices being monitored and provides remote access to devices being managed.
2. Virtual Ntegrity Administrator - Server located at the Liebert High Availability Response Center that monitors information reported from the Virtual Ntegrity Gateways at enterprise locations, and dynamically applies rules and policies upon remote access requests.
3. Virtual Ntegrity Manager - Server located at Liebert High Availability Response Center accepts mutually consented Secure Connection between a Liebert device on the enterprise network and a specially trained Liebert Customer Engineer. Upon completion of remote access needs, all policies and rules are removed leaving no open path for security vulnerability.

Secure Proactive Monitoring

The Virtual Ntegrity Infrastructure provides a unique method to assure security to the enterprise network for both proactive monitoring and on-demand network device access.

This closed architecture assures customers that visibility and access to their critical network elements is restricted only to authorized Liebert personnel.

The Virtual Ntegrity Gateway continuously monitors the health of the target devices on the enterprise network it has been provisioned to manage, and sends its heartbeat via an encrypted out-bound initiated SSL session back to the Liebert High Availability Response Center (HARC).

These heartbeats are sent once a minute to the Virtual Ntegrity Administrator. Upon delivery confirmation of the heartbeat, the SSL session is completely removed until the next scheduled update; so with every heartbeat, an SSL session is dynamically set up and taken down. Delivering these heartbeats with dynamic SSL sessions, versus a permanent (nailed-up) connection, eliminates the risk of a "man-in-the-middle" attack. This, in turn, eliminates the ability for anyone to capture session information for reuse or mimic.

VNI status heartbeats utilize a "push" method of information flow where all communications are securely initiated and driven from the Virtual Ntegrity Gateway at the enterprise location to the Virtual Ntegrity Administrator in the Liebert High Availability Response Center. This allows for remote monitoring without the concern of security vulnerability due to inbound holes placed in firewalls between the enterprise network and the Liebert High Availability Response Center.

Secure Remote Device Connectivity

In the event an authorized Liebert Customer Engineer needs to access a monitored network device at the enterprise location, the Secure Connection allows the Engineer to setup an on-demand IPsec-based session to the target device from the High Availability Response Center. Similar to VNI's status heartbeats, IPsec sessions on the Secure Connection are initiated by the Virtual Ntegrity Gateway upon request from a Virtual Ntegrity Administrator, again requiring no open inbound holes in the firewall of the enterprise network.

When a Secure Connection request is initiated, the Virtual Ntegrity Administrator defines and distributes the unique dynamic routing policies and rules to the Virtual Ntegrity Manager and customer's Virtual Ntegrity Gateway. These rules define the IPsec session from the target device to the authenticated Engineer making the Secure Connection request. The visibility of a Secure Connection is limited only to the target device, eliminating the access risk to unauthorized network devices on the enterprise network.

Upon completion of a remote management session over a Secure Connection, closure of a Secure Connection will automatically remove the unique session rules and policies that were assigned for the Secure Connection from both end points, leaving no risk for reuse by man-in-the-middle attacks.

This closed architecture assures customers that visibility and access to their critical network elements is restricted only to authorized Liebert personnel.

Traceability and Audit Trail

Every Secure Connection session is logged, providing for an audit trail of who, where, what, and when a remote session was performed.

The Liebert Virtual Ntegrity Infrastructure supports regulatory compliance. Every Secure Connection session is logged, providing for an audit trail of who, where, what, and when a remote session was performed. This assures that both the enterprise being monitored and Liebert have information transfer traceability to meet internal and external audit requirements.

Security Standards

The Liebert Virtual Ntegrity Infrastructure uses standard, proven protocols to ensure the highest level of end-to-end security and authenticity. Secure Sockets Layer (SSL) is used to transport the VNI heartbeats and IPsec is used for the tunnel between the Virtual Ntegrity Manager and Virtual Ntegrity Gateways.

The utilization of IPsec provides authentication and encryption at the IP (Internet Protocol) level. This requires a higher-level protocol (IKE) to set things up for the IP-level services Encapsulating Security Payload (ESP). SSL secures a single application socket. IPsec encrypts everything between two hosts.

With this approach, IPsec can be used behind any Network Address Translation (NAT) device by converting ESP into UDP. Additionally, the dual channel closed system (SSL and IPsec) combination guarantees the authenticity of the connection.

The Virtual Ntegrity Infrastructure incorporates the following security standards and policies:

Encapsulating Security Payload (ESP)

The encryption in the ESP encapsulation protocol is done with a block cipher, DES. Two versions of DES are used in the industry for encryption: DES and Triple DES (3DES). The default block cipher used by the VNI is 3DES.

Internet Key Exchange (IKE)

The IKE protocol sets up IPsec connections after negotiating appropriate parameters (algorithms to be used, keys, and connection lifetimes) for them. This is accomplished by exchanging packets on UDP port 500 between the devices in the VNI.

Whether systems are operating in the data center, a network closet or the warehouse floor, mission-critical power and cooling technologies should be employed to ensure resistance to failure and the ability to adapt to increases in criticality.

Two-Phase IKE Negotiations

Phase one
The two gateways negotiate and set up a two-way Internet Security Association and Key Management Protocol (ISAKMP) Security Association (SA), which they can then use to handle phase two negotiations. One such SA between a pair of gateways can handle negotiations for multiple tunnels.

Phase two
Using the ISAKMP SA, the gateways negotiate IPsec (ESP) SAs as required. IPsec SAs are unidirectional (a different key is used in each direction) and are always negotiated in pairs to handle two-way traffic. There may be more than one pair defined between two gateways.

Both phases use the UDP protocol and port 500 for their negotiations.

After both IKE phases are complete, IPsec SAs carry the encrypted data. These use the ESP protocols. The RSA algorithm is a very widely used public key cryptographic technique. It is used in IPsec as one method of authenticating gateways for Diffie-Hellman key negotiation. The VNI uses a custom matched pair system using 2192 bits per key in the Virtual Ntegrity Gateway and the Virtual Ntegrity Manager.

Firewall Provisioning

All firewall changes required to implement the Virtual Ntegrity Infrastructure are outbound only. No inbound firewall ports are necessary for this solution. The following ports are required by Liebert:

- UDP Port 4500: used for port floating in NAT traversal
- UDP Port 500: used for IKE IPsec key exchange
- TCP Port 443: used for SSL communication and monitoring

Summary

Liebert Virtual Ntegrity Infrastructure provides a unique, secure, remote access solution that utilizes the best of multiple encryption technologies to achieve a high level of security while at the same time takes the burden off customers to deploy and manage the service. In addition, this solution incorporates various deployment methods, ensuring compliance with our customer's security policies and requirements.

Liebert Corporation
1050 Dearborn Drive
P.O. Box 29186
Columbus, Ohio 43229
800.877.9222 (U.S. & Canada Only)
614.888.0246 (Outside U.S.)
Fax: 614.841.6022

www.liebert.com

Printed in U.S.A. 0106 AN106