HIRSCHMANN
A BELDEN BRAND

Secure Remote Access Solution

The Hirschman Solution vs. Traditional VPNs

Release 01 03/2017

Technical Support
https://hirschmann-support.belden.eu.com

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann product site (www.hirschmann.com).

Printed in Germany
Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
Tel.: +49 1805 141538

How to overcome the limitations of traditional VPNs

Although traditional VPNs are widely used and suit the general purpose of interconnecting remote networks quite well, they have some serious drawbacks for remote device monitoring and management. The Secure Remote Access Solution is an Internet based technology that specifically addresses the security and usability requirements of linking service engineers with industrial equipment.

Summary

Traditional VPNs	Secure Remote Access Solution
Multiple installed VPN clients cause conflicts with each other	LinkManager is independent of VPN clients
Connected networks cannot use the same local IP subnet	Works independently of IP subnets
Connections must be pre-configured	Connections can be configured dynamically
Requires advanced routing functions	The system does not use routing internally
Requires special ports and protocols open on a firewall	Only standard web ports need to be open on a firewall
Needs complex VPN firewall rules	Rules are created automatically
Requires certificates from a Certificate Authority	GateManager provides the certificates
Limited logging	Comprehensive logging
Requires a VPN concentrator	GateManager acts as a concentrator

1. VPN clients

Traditional VPNs require clients to be installed on the client PC. These clients usually conflict with each other. With multiple clients installed, it may even be the case that no client works.

The LinkManager client is not a VPN client. As a result, it will not interfere with an existing VPN client. Therefore an engineer can run a traditional VPN client and a LinkManager client on the same PC.

2. Subnet conflicts

Networks connected via traditional VPNs cannot use the same local subnet. But a Machine Builder / System Integrator managing hundreds of customer installations is bound to run into lots of locations using the same subnet addresses. Asking the customers to change their addressing schemes is rarely an option, and juggling with NAT rules to deal with the existing addressing schemes can quite simply be a nightmare.

With the Secure Remote Access Solution all sites could have the same subnet, and all equipment could have the same IP address. The engineer and the remote device are simply linked to each other from an IP perspective at connection.

3. Pre-configured connections are required

Connection between traditional VPN peers cannot be established dynamically upon request, but have to be configured beforehand. This needs involvement of IT personnel, and takes time – every time.

Once the engineer with the LinkManager Client has an account on the GateManager represented by his personal X.509 certificate, the GateManager administrator can by point-and-click associate the account with exactly the site or group of equipment the technician

should have access to. The entry is immediately added to the list of sites available in the LinkManager client.

4. Advanced routing challenges

Connecting two remote networks with traditional VPNs via a central VPN concentrator requires configuration and management of advanced forwarding routing rules. Additionally routing equipment usually needs to be able to support NAT-T and UDP encapsulation.

The Secure Remote Access Solution does not use routing and subsequently no NAT rules are required. IP addresses are simply linked via a central proxy server. Traditional VPNs are suitable for one-to-one or many-to-one connections, but not one-to-many (one engineer to many sites), or many-to-many (many engineers to many sites). The Secure Remote Access Solution easily administers thousands of engineers needing access to thousands of sites, including management of individual access rights, and even limits access to specific types of equipment, or specific protocols/services of equipment.

5. Firewall opening challenges

Traditional IPSec based VPNs require special ports and protocols open in firewalls to communicate through.

All connections from SiteManagers and LinkManagers are established from inside the network to outside, and only standard web ports are used (such as 443). All these encrypted connections are terminated at the central Internet based GateManager server, and through these encrypted connections, the links between engineers and devices are dynamically established.

6. Firewall blocking challenges

VPNs route everything and not just the protocols you need, unless efforts are also put into creating and managing a number of firewall rules.

The device agents defined on the SiteManager are automatically limited to allowing access only to the ports or services defined for the agent type. For example, when defining a Beckhoff PLC agent on the SiteManager, the ports that are opened are TCP ports 987, 5120, 48897-48899 and UDP 48898-48899. Only these are activated when a LinkManager connects to the agent representing the Beckhoff PLC.

7. Certificate management

A good VPN solution is usually based on X.509 certificates that are exchanged or signed by a Certificate Authority (CA). This adds overhead and makes it tedious to set up individual connections.

The GateManager acts as the CA authority for both SiteManagers and LinkManager clients. The Client access is secured by a two factor system (certificate and password), known from web banking solutions. But the X.509 certificate is not only a security measure. The LinkManager certificate includes all the configuration details and thereby eliminates the need for the user to configure anything. Install the LinkManager and the certificate, and the LinkManager will know where to connect to. No additional configuration of the LinkManager is needed.

8. Activity Logging

The principle of traditional VPN is to connect two networks, and have everything accessible between the two peers. Therefore logging is at best only done when establishing the connection. But once connected, nothing is logged.

The GateManager server will not only centrally log who made the connection and to what, but also when the connection was established, and what services were accessed. The log is kept centrally on the GateManager and cannot be deleted by administrators. It can therefore act as evidence in case of legal disputes.

9. Managing the ”Concentrator”

Typical IPSec based VPN solutions require an IT administered concentrator, which requires networking knowledge. Also individual concentrators must typically be installed at each service provider, in order to avoid very complex triangular routing and firewall setups. SSL based VPN solutions overcome some of the issues of IPSec based VPNs, but users are still exposed to advanced routing and firewall configuration rules on hosted solutions.

The ”concentrator” for the Secure Remote Access Solution is a central service in the form of the GateManager server, where each service provider gets an isolated account. Here the administrator issues account certificates, organizes his equipment and users in domain structures and dynamically controls what equipment and which sites each service engineer should have access to. There is no networking or other IT skill sets required.