



VCL-5001

NETWORK TRAFFIC SNIFFER

Introduction

VCL's "Beyond the Firewall" Cyber Security Solution does not negate or invalidate the role of the "Firewall" in any manner. The Firewall still remains the primary element of defence against cyber-attacks. However, cyber-attacks succeed because firewalls get breached. The deployment of VCL's "Beyond the Firewall" Cyber Security Solution provides the "next-line-of-defence" against firewall breaches, resulting in the enhanced network security and resilience against cyber-attacks.



VCL's "Beyond the Firewall" Cyber Security Solution is very different from other security solutions that report a network security breach long after the event – when the damage has already been done.

We provides a comprehensive "Beyond the Firewall" Cyber Security Solution that is designed to assist organizations to detect, prevent and secure their networks against firewall breaches and cyber- attacks – while they occur. All elements of the VCL "Beyond the Firewall" Cyber Security Solution function in real-time to alert the network administrator against a network security breach and to also automatically take a series of appropriate 'counter-measures' in accordance with the organization's custom defined network security policy.

The VCL-5001, Network Traffic Sniffer is one such "Beyond the Firewall" Cyber Security element that detects firewall breaches, network intrusions and cyber-attacks in "real-time". It also provides the user, the data to conduct forensic analysis and trace the attack route which assists the user to identify the points of network vulnerability.

Inbound and Outbound Traffic Monitoring: The VCL-5001, Network Traffic Sniffer provides the network administrator the ability to continuously scan inbound and outbound traffic and to generate an alert if an unauthorized data transmission is taking place from any of the Servers or IEDs such RTUs, PMUs, Bay Control Units, etc. which may be considered a potential data breach and security threat. This feature is especially useful in detecting "moles" or "malicious firmware" in any of the Servers or IEDs that could have been compromised and may be unlawfully transmitting data to any destination (i.e. IP address) which has not been included in the network administrator's authorized-list. It becomes a useful tool in enhancing cyber-security of Banks and other financial infrastructure, Sub-Stations, SCAD Networks and Oil and Gas Pipelines.

VCL-5001: Network Traffic Sniffer Use-Cases and Capabilities

IRIG-B Format

- VCL Network Traffic Sniffer detect network intrusions and abnormal data transmission patterns that could potentially result in Data Theft, Ransomware Attacks, Denial of Service (DoS) and Cyber-Attacks that are aimed to bring-down the target network.
- Flags unusual traffic flows for both inbound and outbound traffic to unauthorized IP addresses by alerting the network administrator about such anomalies.
- Provide a warning mechanism of an impending cyber-attack to Utilities which use “**Protection Relays**” and RTUs (Remote Terminal Units) by alerting the network administrator if such devices are being accessed from un-authorized IP addresses.
- Allows the network administrator to implement a series of completely customized defensive ‘counter-measures’ which shall be automatically initiated in the event of a network breach, in accordance with the organization’s network security policy.
- Defensive counter-measures may include automatic physical isolation of the complete network (or physical isolation of specified sensitive devices from the network) and generating a series of audio and visual alarms when used in conjunction with the VCL-2702, Network Kill-Switch, in the event that a network-security breach has been detected.
- Defensive counter-measures may also include re-routing the entire network to an alternate secured transmission link and generating a series of audio and visual alarms when used in conjunction with the **VCL-2778: SafeComm-E: 1+1 ethernet Failover Protection/AB Fallback Switch**
- Provides a full-featured, secured network management interface. Compatible with VCL-UNMS (Unified Network Management System) for remotely monitoring all the VCL-5001: Network Traffic Sniffer installed in the network over a secured communication link.

Ordering Information

Reference	Description
VCL-5001	VCL-5001 Network Traffic Sniffer 19-inch Rack Mount, 3U High



CXR
T 02 37 62 87 90
www.cxr.com

17 Rue de l'Ornette 28410 Abondant France
contact@cxr.com

Smart Solutions for Smart Networks

Information contained in this document is not contractual. CXR improves its products continuously. Specifications may change without notice.