Smart solutions for smart networks

Version 1.0

ISS2150

MCC Firewall Information Security

Description

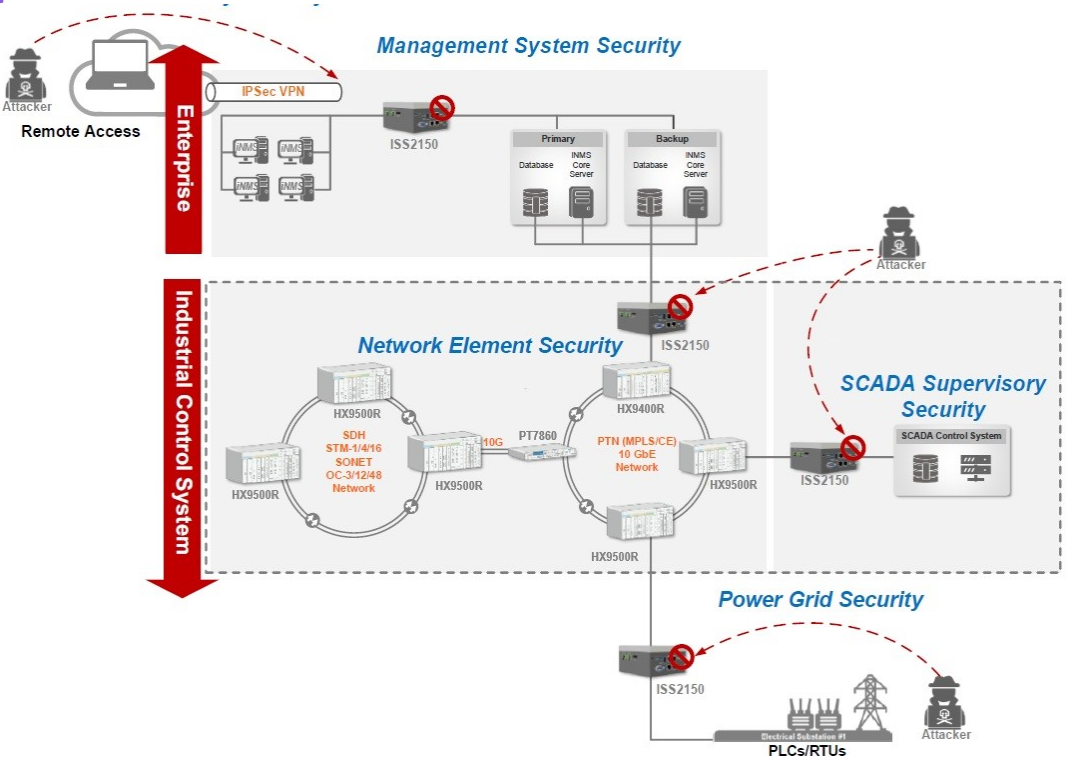
The application of digital information processing and communications in mission critical infrastructure is getting more complicated. It has led to numerous vulnerabilities and significant security issues. It reveals the cyber security threats and the importance of solutions on cyber security against intruders. Abundant attack cases have proven that unauthorized users have the capability to access and manipulate sensitive data from a protected network domain. ISS-2150-NCA MCC Firewall is aimed to manage and enhance the network security of the Mission Critical Infrastructure by utilizing the firewall to isolate security zones between different network areas to better protect and block the inbound information flow.

Features

- All-in-one Firewall/NAT/VPN/Router/IPS
- Stateful firewall that monitors connection states and identifies potential traffic risks
- Full-function NAT includes Source NAT, Destination NAT, Static NAT, and Dynamic NAT
- Secure remote access tunnel with IPSec VPN
- Supports both static routing and dynamic routing.
- Industrial-grade Intrusion Prevention/Detection System (IPS/IDS) for ICS network
- Supports SYN cookies to prevent Denial-of-Service (DoS) attacks.
- Supports Quality of Service (QoS) in networking to manage traffic and guarantee the performance of critical applications.
- Supports a variety of connectivity methods, such as Link Aggregation/Failover, to suit OT networking requirements.
- The high availability design supports automatic hardware failover.
- Supports RESTful API for easy system integration.
- Supports Deep Packet Inspection (DPI)*, offering enhanced network connection management beyond the capabilities of traditional layer 4 firewalls.
- Compliant with the IEC 61850-3 industrial standards (IEC model)
- The fanless design can greatly operate in extreme conditions with restricted airflow

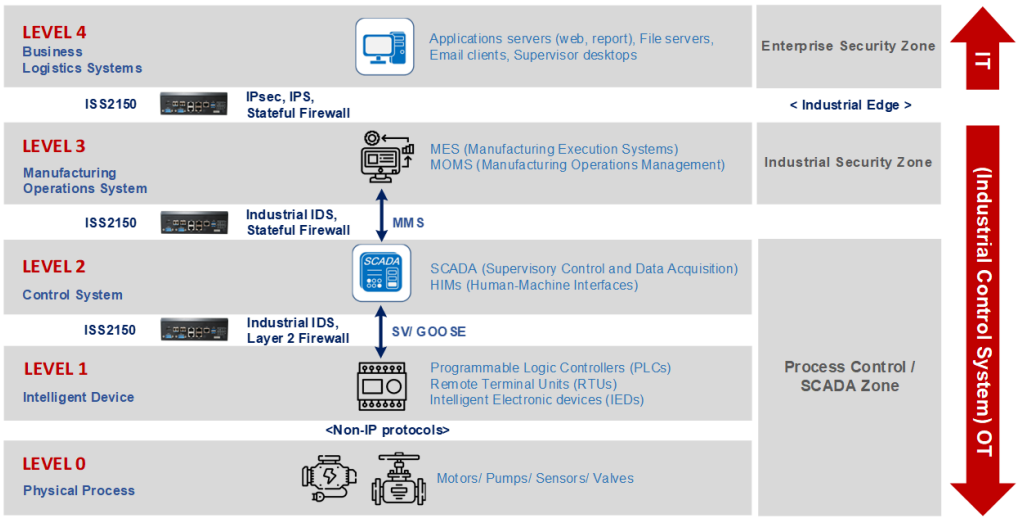
CXR Networks

Application Illustrations



Mission Critical Communications Network for SCADA & Teleprotection

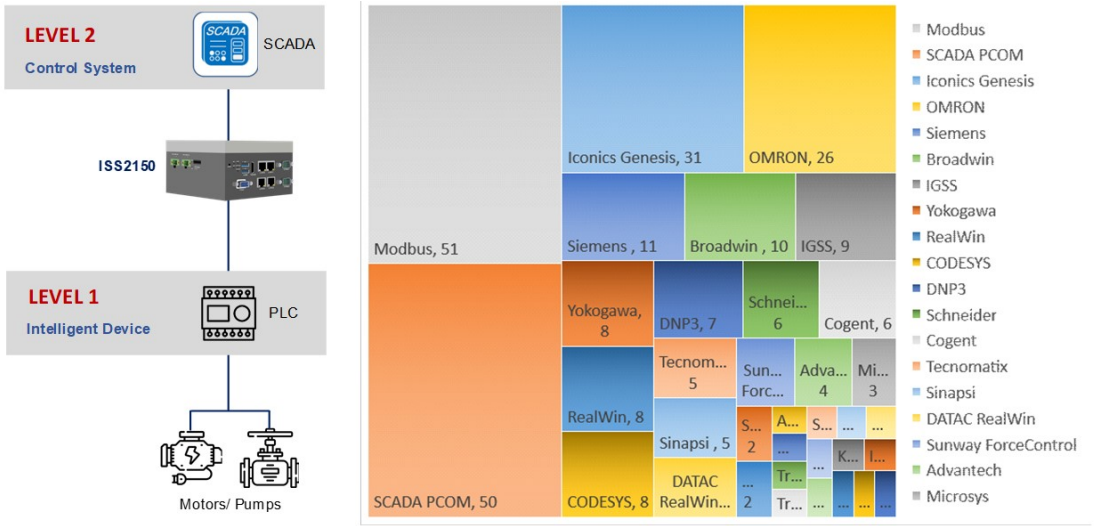
The ISS-2150-NCA firewall in this application protects critical systems by controlling and monitoring network traffic to block unauthorized access and cyber threats. It is placed at gate keepers, such as the Management System Security and SCADA Supervisory Security edges, to secure sensitive areas like the NMS Core Server and SCADA control systems. The firewall enforces strict access rules, inspects network packets, and prevents attacks on PLCs/RTUs and other critical components. Its role is to ensure secure communication, protect against intrusions, and maintain the reliability of the mission-critical network.



Purdue Model with MCC Firewall

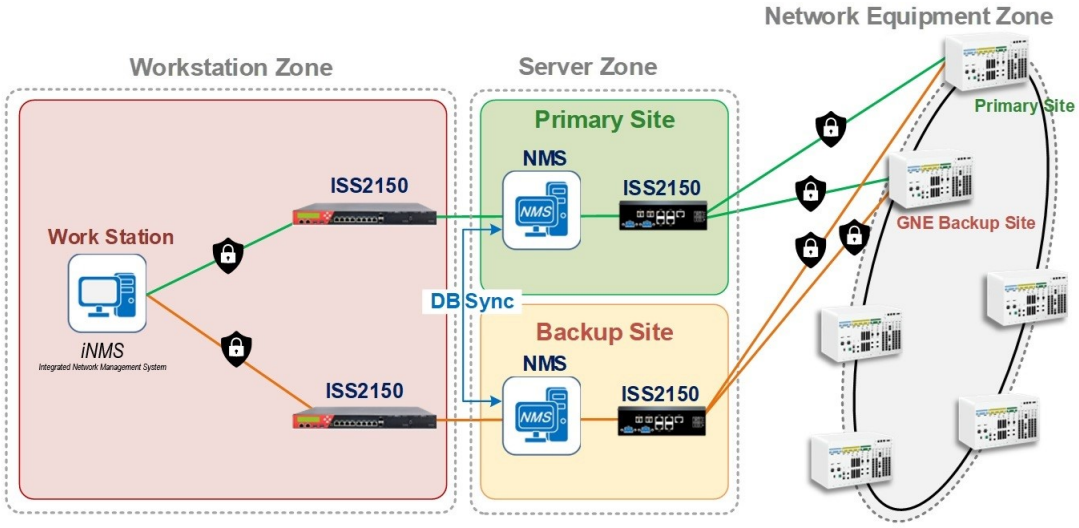
The Purdue model is a structural framework for Industrial Control System (ICS) security that prioritizes segmentation. It has been recognized as a foundational framework for ICS network segmentation, safeguarding Operational Technology (OT) from malware and other forms of attacks. The MCC firewall is seamlessly integrated into the Purdue model, thereby establishing the necessary segmentation barrier.

Application Illustrations



IDS/IPS Function Offered by MCC Firewall to Recognize 275 Industrial Protocols

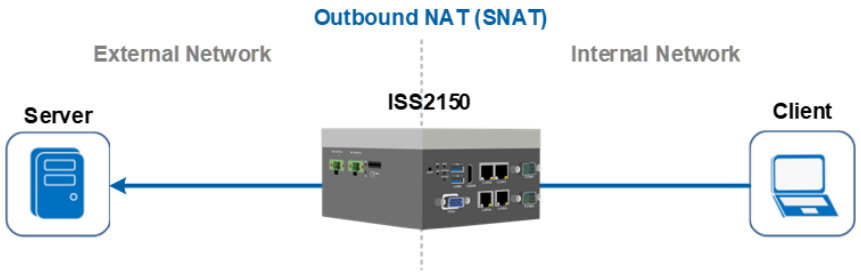
The flow of information within the power grid architecture spans across multiple network areas, presenting challenges in maintaining cybersecurity across these domains. To ensure the protection of the entire power grid, the MCC firewall not only filters network packets to establish security zones but also enhances the IDS/IPS function. This involves examination of network traffic behavior to thwart attacks and prevent malware connections.



DCN (Management Plane) Security Approach

The MCC firewall is specifically designed for the Telecommunication Management Network to bolster the cybersecurity of Data Communication Network (DCN). It can both support high availability and handle a significant number of IPSec connections. This capability is crucial for linking various network equipment to the DCN, ensuring that data remains encrypted. Additionally, IPSec enables power grids to extend their private networks to the internet, creating encrypted, secure zones essential for modern power grid information exchange.

Application Illustrations

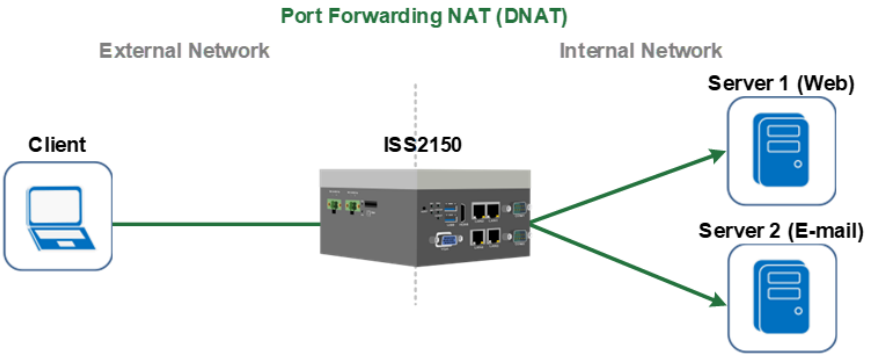


NAT Function

PAT, or Dynamic Port Address Translation, is employed for connections originating from the internal security zone and heading towards the external network. It operates by obscuring the internal devices' source IP addresses, translating them into external addresses—a process commonly recognized in Cisco terminology.

One-to-One NAT Function

One to One NAT, particularly beneficial for connections with fixed IP address prerequisites, is ideal for establishing stable bidirectional connections, especially between servers. In this configuration, the server located within the internal security zone maintains a constant mapping to a specified external address, ensuring a reliable one-to-one correspondence for seamless communication.



Port Forwarding Function

Diverging from one-to-one NAT, which utilizes a single external IP address, port forwarding offers enhanced flexibility. It allows for mapping one external address to one or multiple internal devices, distinguished by various TCP/UDP connection ports, providing a versatile and adaptable solution.

Product Specifications

Ethernet Connectivity System	Network Interface	8 * RJ45 Ports 10/100/1000Mbps, 2*GbE SFP optical ports
	SNMP	SNMPv1, v2c, v3
	Config Backup & Restore	History & Diff support
	Syslog	Support remote syslog
	User Interface Management	HTTPs, SSH, serial port
Layer 2 Specifications	802.1Q VLAN Support	IEEE 802.1Q max 4096 VLANs
	8021x Support	IEEE 802.1x
	Link Aggregation	IEEE 802.3ad LACP
	Layer 2 Transparent	Bridging
	Spanning Tree-Protocol	IEEE 802.1D (STP), IEEE802.1W (RSTP)
Layer 3 Specifications	Routing	Static route, RIPv1, RIPv2, OSPFv3, BGPv4 Routing among system VLAN/ sub-Interface
	Policy-Based Routing	Support policy-based routing rules
High Availability	Automaitc Hardware Failover	Virtual Ips of the type CARP (Common Access Redundancy Protocol, a.k.a. VRRP)
	Synchronization State Table	PF Sync (packet filter state table synchronization)
	Configuration Synchronization	Yes
IPSec VPN	Support of Tunnels	Site-to-site, hub and spoke, dynamic endpoint
	Internet Key Exchange	IKEv1, IKEv2 (RFC 7296)
	IKE Authentication Algorithms	SHA-1, SHA-256, SHA-384
	Support of Authentication	Pre-sahred key, public key infrastructure (PKI) (X.509), EAP TLS, EAP-MSCHAPv2
	VPN Monitoring	Dead Peer Detection (DPD, RFC 3706)
	Support of Dynamic IP VPN	MOBIKE (RFC 4555)
	Multiple Authentication	IKEv2 (RFC 4739)
	Maximum IPSec Tunnels	300
	Recommendation	
Intrusion Detection System (IDS & IPS)	Intrusion Detection Mode	Detect threats and send real-time alerts
	Intrusion Prevention Mode	Blocks harm traffic and protect zones and applications

Product Specifications

Network Security	Firewall Policies (Maximum)	10.000
	Stateful Packet Inspection	Yes
	Deep Packet Inspection	DPI for application control and visibility
	Network Address Translation (NAT)	Outbound NAT (SNAT) Bidirectional One-to-One NAT (1:1 NAT) Port Forwarding NAT (Destination NAT)
Network Monitoring	NetFlow Explorer	v5, v9
Network Management	Console	DB9S (DCE), female, RS232 connector
	Ethernet	User Interace management: VT-100 GE port, connector: RJ45 SNMP v1/v2c/v3, SSH, support Radius client function Web GUI support
QoS	Traffic Shaping Support	ToS, CoS
Throughput	Throughput	10Gbps
Latency	Latency	200μs
Connection	Packets Per Second	500Kpps
	Concurrent Sessions	500.000.000
	Connections Per Second	50.000
Physical and Environmental	Dimension (W*H*D)	440*44*470 mm
	Temperature	Operating: 0~40°C Storage: -40~85°C
	Humidity	Operating: 10~80% relative humidity, non-condensing Storage: 10~80% at 40°C, non-condensing
	Mounting	19-inch rack mounting
Power Supplies	Power Supplies Connector	Connector types C13
	Power Requirement	Redundant 100-220 VAC power input
Certification		EMC EN55032 Class A, FCC Part 15 Class A, IEC61850-3/ IEEE 1613, EN50121-4

CXR Networks

Ordering Informations

Firewall	MCC OT Firewall
ISS-2150-NCA	ISS2150 MCC Firewall with NAT, VPN, ACL and router all-in-one features. - Datacenter level (high throughput) with dual AC power module - 8 x RJ45 Ports 10/100/1000Mbps , 2 x 10 GbE SFP+ - Operating Temperature: 0 to 40°C - Built-in Syslog client for Log monitoring
Feature Option	
ISS2150-IPS	IPS function for intrusion prevention system including DDoS protection
Maintenance Agreement (MA)	
ISS2150-MA001	Annual software maintenance service on ISS-2150 MCC OT Firewall System for the first year - 5x8 (Monday to Friday from 9:00am to 5:00pm, UTC+08:00) problem remote diagnosis and consulting via email and phone call - MA is renewable on a yearly basis.
NE Management License	
iNET-ISS2150	Each ISS2150 Major NE management license (EN)

CXR Networks
CXR
T +33 (0) 237 62 88 00
www.cxr.com
17 Rue de l'Ornette 28410 Abondant France
contact@cxr.com