Technical White Paper

Executive Summary

The Tempered Networks solution is a network segmentation product based on the International Society of Automation (ISA) TR100.15.01 architecture. The solution is used to create private overlay networks on top of shared network infrastructure. In the parlance of Internet Engineering Task Force (IETF) Requests for Comments (RFCs), each private overlay network is a Virtual Private LAN Service (VPLS).

A Tempered Networks environment is comprised of a scalable orchestration engine (HIPswitch Conductor™), industrial and data-center grade security appliances (HIPswitches) and a management console and user interface (SimpleConnect®). Users interact with their deployment through the SimpleConnect web-based user interface. HIPswitches are used to implement a private overlay network and several independent private overlay networks can be managed by the combination of a HIPswitch Conductor and a SimpleConnect user interface. Each private overlay network can be delegated to different users, yet the governance of the entire solution is centralized and retained by the administrator. The Tempered Networks solution therefore provides the enterprise with "Private Networks as a Service".

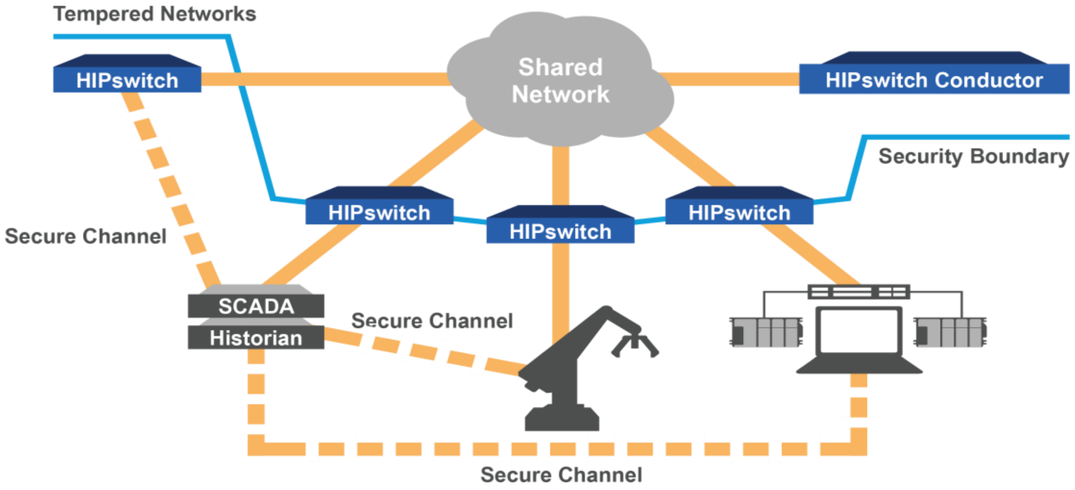


FIGURE 1: EXAMPLE PRIVATE OVERLAY NETWORK IMPLEMENTATION USING THE TEMPERED NETWORKS SOLUTION.

The Trusted Computing Group (TCG) has developed an architecture for network access control (NAC) called Trusted Network Connect (TNC). TNC has a protocol for network security coordination called Interface for Metadata Access Points (IF-MAP). IF-MAP acts as a clearinghouse for security policy and configuration metadata, and uses a publish/subscribe semantic to deliver real-time metadata updates to subscribed clients. TCG has specified Metadata for Industrial Control Systems (ICS) Security to standardize the orchestration control channel between the HIPswitches and the HIPswitch Conductor.

Referenced Standards

International Society of Automation (ISA)
ISA TR 100.15.01 (2012) - Backhaul Architecture Model: Secured Connectivity over Untrusted or Trusted Networks: [https://www.isa.org/store/products/product-detail/?productId=116759]

Trusted Computing Group (TCG)
TCG IF-MAP Binding for SOAP v2.1r15 (2012) – IF-MAP for Network Security Coordination: [https://www.trustedcomputinggroup.org/resources/tnc_ifmap_binding_for_soap_specification]

TCG IF-MAP Metadata for ICS Security (2014) – IF-MAP Metadata for Industrial Control Systems Security: [https://www.trustedcomputinggroup.org/resources/tnc_ifmap_metadata_for_ics_security]

TCG Architects Guide: ICS Security Using TNC Technology (2013) – Whitepaper: [http://www.trustedcomputinggroup.org/resources/architects_guide_ics_security_using_tnc_technology]

Internet Engineering Task Force (IETF)
IETF draft-ietf-hip-rfc5201-bis-11 (2014) – Host Identity Protocol Version 2 (HIPv2): [http://tools.ietf.org/html/draft-ietf-hip-rfc5201-bis-19]

IETF draft-henderson-hip-vpls-06 (2013) – HIP-based Virtual Private LAN Service (HIPLS): [http://tools.ietf.org/html/draft-henderson-hip-vpls-07]

Theory of Operation

Shared Network communications

HIPswitches connect to the shared network infrastructure using standard services and interfaces. Typically, HIPswitches obtain a shared network IP address using DHCP and rendezvous with the HIPswitch Conductor using DNS. Using an HTTPS SOAP IF-MAP connection, the HIPswitches obtain their private overlay network configuration, security policies, peer HIPswitch network rendezvous, and other management metadata from the HIPswitch Conductor.

In response to private overlay network communications between devices, the HIPswitches establish HIP tunnels to one another. Therefore, private overlay network communications are encrypted and integrity protected as they traverse the shared network. Since private overlay network communications are hidden from the shared network, the IP addressing of devices in the private overlay network are independent of the IP addresses of the HIPswitches on the shared network.

Private Overlay Network communications

Each HIPswitch has a ***unique*** cryptographic identity in the form of an RSA 2048-bit key pair. Default Tempered Networks signed certificates are "baked in" to each HIPswitch and HIPswitch Conductor and a private overlay network is a whitelist of HIPswitch cryptographic identities. The list of identities is provided to the members of each private overlay network and each HIPswitch authenticates and authorizes peer HIPswitches against this whitelist of allowed peers.

A HIPswitch acts as a bump-in-the-wire device that connects to a Local Area Network (LAN) segment with one network interface and a shared network infrastructure with a second (or optionally several) network interface. The HIPswitch's network interface on the LAN segment is configured as a transparent bridge and therefore has no IP address on the private side, nor is any configuration change required on the local devices.

When the private overlay network is configured, the user must specify the IP addresses of local devices on the LAN segment attached to a local HIPswitch. When a device behind the local HIPswitch attempts to communicate with a device behind a remote HIPswitch, the HIPswitches use the Host Identity Protocol (HIP) Base Exchange to establish a mutually-authenticated certificate-based ESP-protected tunnel between each other. Device packets are encrypted and encapsulated, then sent over the shared network to the peer HIPswitch.

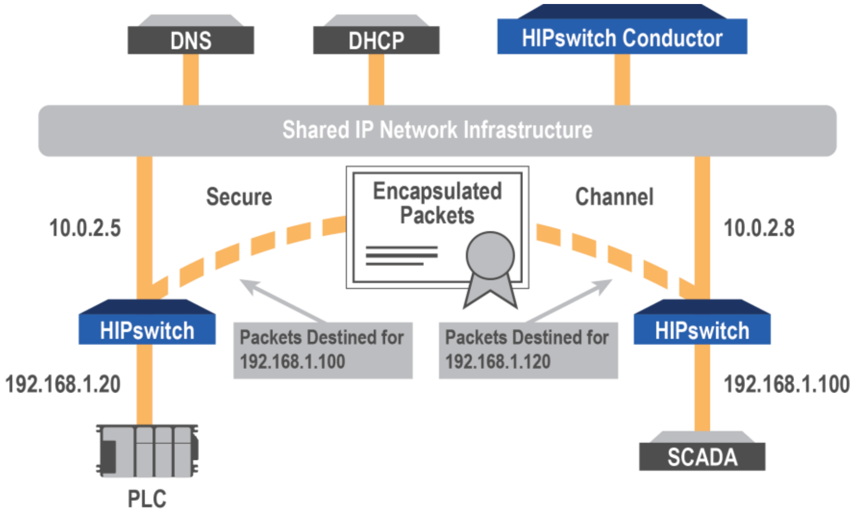
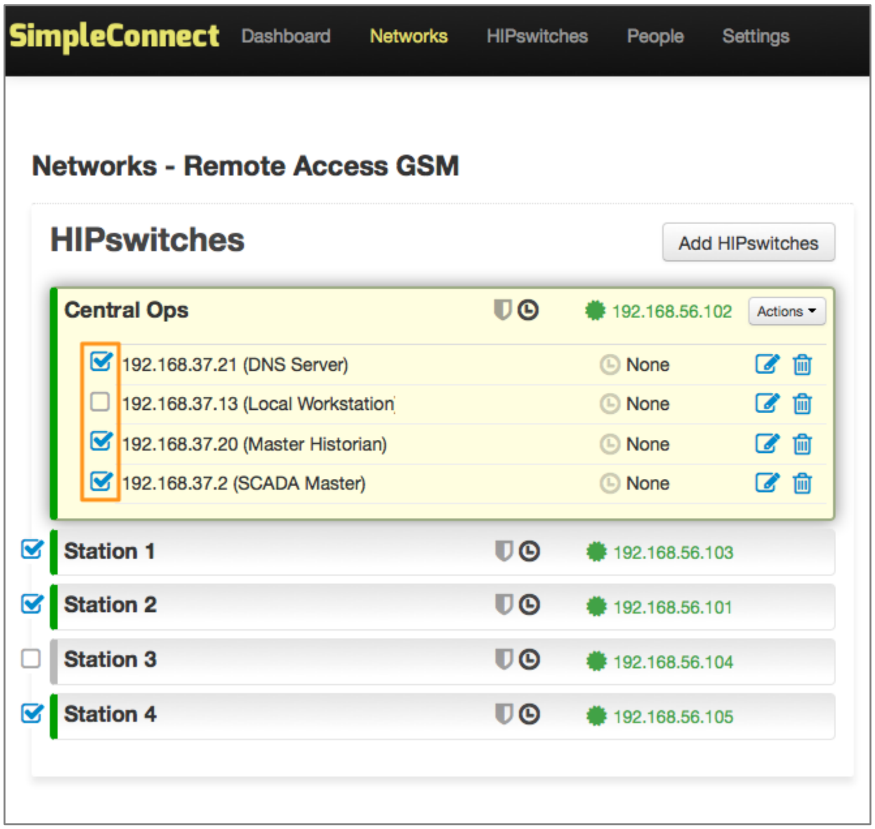


FIGURE 2: END-TO-END COMMUNICATIONS EXAMPLE

Although both the ISA architecture document and the TCG ICS Metadata specification refer to the private overlay network as a full layer 2 VPLS, the Tempered Networks solution currently implements a layer 2/3 overlay network; i.e. ARP is the only tunneled layer 2 traffic. The default network topology within a private overlay network is a single broadcast domain. The Tempered Networks solution also supports routing and network address translation (NAT) in the private overlay network by allowing the HIPswitch to function as a default gateway to local devices.

Communications Policies

The Tempered Networks solution currently supports the definition and enforcement of three kinds of communications policies: HIPswitch-level (peer) policies, device-level (host) policies and ports and protocol (SPI) policies. HIPswitch-level policies specify the set of peers within the private overlay network with whom a given HIPswitch is authorized to establish HIP tunnels. Device-level policies instruct a HIPswitch whether to allow or deny a device on the local LAN segment from communicating with remote devices. The screenshot in Figure 3 shows an example of configuring device-level policies for a selected HIPswitch.



Networks - Remote Access GSM

HIPswitches

Central Ops 192.168.56.102

☑ 192.168.37.21 (DNS Server) None

☐ 192.168.37.13 (Local Workstation None

☑ 192.168.37.20 (Master Historian) None

☑ 192.168.37.2 (SCADA Master) None

☑ Station 1 192.168.56.103

☑ Station 2 192.168.56.101

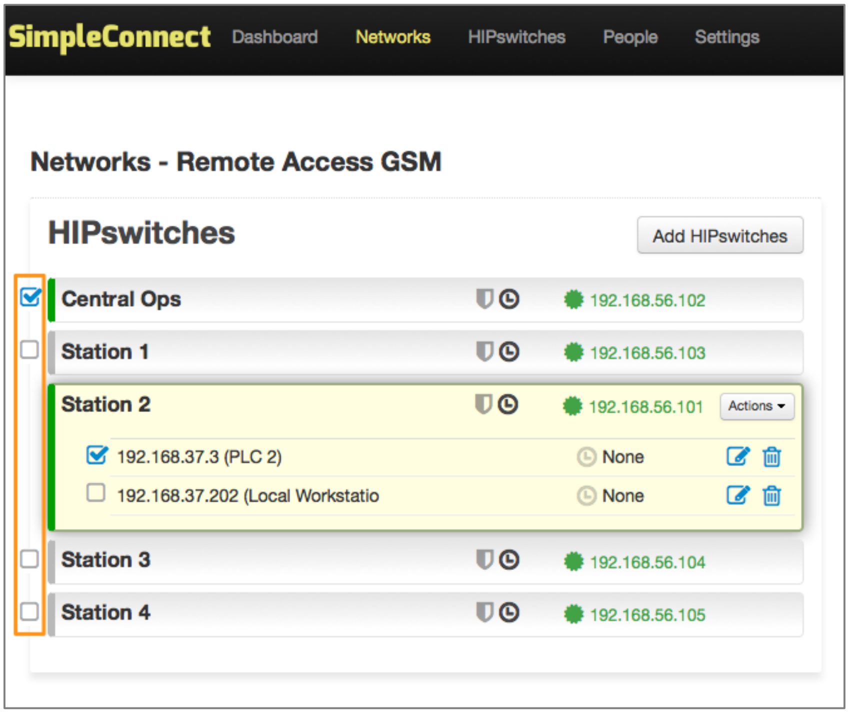
☐ Station 3 192.168.56.104

☑ Station 4 192.168.56.105

FIGURE 3: SCREENSHOT SHOWING DEVICE-LEVEL POLICY CONFIGURATION FOR A GIVEN HIPSWITCH. (THE ORANGE BOX HAS BEEN ADDED FOR EMPHASIS)

For end-to-end communications between a local and remote device, there must be an allowed device policy for each device with its local HIPswitch, and allowed HIPswitch policy between the two respective HIPswitches. As an example consider Figure 2: there must be device policy for the HMI and HIPswitch 1, device policy for the Server and HIPswitch 2, and HIPswitch-HIPswitch policy between HIPswitch 1 and HIPswitch 2.

These HIPswitch-level policies can result in policies anywhere from full-mesh to limited point-to-point. An example of HIPswitch-level policies is shown in the screenshot in Figure 4.



Networks - Remote Access GSM

HIPswitches

☑ Central Ops 192.168.56.102
☐ Station 1 192.168.56.103
Station 2 192.168.56.101
☑ 192.168.37.3 (PLC 2) None
☐ 192.168.37.202 (Local Workstatio None
☐ Station 3 192.168.56.104
☐ Station 4 192.168.56.105

FIGURE 4: SCREENSHOT SHOWING HIPSWITCH-HIPSWITCH POLICY CONFIGURATION.
(THE ORANGE BOX HAS BEEN ADDED FOR EMPHASIS)

The Tempered Networks solution also has the capability to define and enforce Stateful Packet Inspection (SPI) policies for device communications through a HIPswitch. In addition to standard best-practice policies (bogon packet, syn flooding), HIPswitch firewall policies support policies based on:

- Source device IP Address
- Destination device IP Address
- Source Port
- Destination Port
- Protocol

Public Key Infrastructure (PKI)

Out-of-the-box HIPswitches and HIPswitch Conductors ship from Tempered Networks with unique Tempered Networks signed X.509 certificates that are based on RSA 2048-bit public/private key pairs. As described in the TCG ICS Security standard, the Common Name

(CN) of each certificate is also the BHI Unique ID (UID). The UID is printed in text and barcode on the label of each device.

As some customers will prefer to provision customer-signed certificates on HIPswitches or HIPswitch conductors, the Tempered Networks solution supports the complete lifecycle management of customer-signed certificates onto each HIPswitch. Once a customer-signed certificate is provisioned onto a HIPswitch, the HIPswitch will use the customer certificate to authenticate to the HIPswitch Conductor and to peer HIPswitches. Additionally, HIPswitches will use their customer certificates to authenticate to WiFi 802.11i EAP-TLS networks configured via the HIPswitch Conductor.

IF-MAP Service

IF-MAP enables the (network) real-time coordination of network configuration and security policy metadata. The HIPswitch Conductor hosts the IF-MAP service for a deployment. IF-MAP provides a publish-subscribe semantic on a graph-based database and was purpose-built for network security coordination. HIPswitches and HIPswitch Conductors connect to IF-MAP using a SOAP web service over HTTPS connections.

Based on user input through the SimpleConnect UI, the HIPswitch Conductor publishes private overlay network configurations to IF-MAP. Each HIPswitch searches the IF-MAP graph to determine the following:

- Private overlay network memberships
- List of peer HIPswitches within its private overlay network(s)
- List of local devices that will be allowed to communicate through this HIPswitch
- List of remote devices associated with peer HIPswitches
- DHCP-assigned IP addresses of peer HIPswitches
- X.509 certificates for peer HIPswitches

Furthermore, each HIPswitch subscribes to changes in the above metadata. When changes occur, the IF-MAP service provides the changes to the relevant subscribed HIPswitches. Since IF-MAP only sends deltas to the configuration, and since each HIPswitch only receives configuration that is relevant to its operation, the data model has excellent scaling properties. HIPswitches cache their current configuration to persistent flash in order to remain operational in the event the HIPswitch Conductor is offline.

The HIPswitches connect to the shared network infrastructure using DHCP, however static IP addressing of the HIPswitches is also possible. Using DHCP reduces the administrative burden to establish private overlay networking, but does introduce the challenge of network rendezvous. To enable network rendezvous in real time, the HIPswitches publish their DHCP-assigned shared network IP address to IF-MAP.

The HIPswitch Conductor coordinates several other powerful features using IF-MAP. The availability of HIPswitch firmware updates are delivered via IF-MAP, along with the digital signature validating the authenticity of the firmware update. Additional functionality coordinated via IF-MAP includes:

- HIPswitch and HIPswitch Conductor central logging service
- HIPswitch WiFi network settings
- Device MAC detection
- Device activity reporting
- Initiation and download of HIPswitch packet captures
- Initiation and download of HIPswitch diagnostic information

Standards-Based Solution

The Tempered Networks solution is based on the architecture model described in ISA TR100.15.01. This model describes a HIPswitch as a Backhaul Interface (BHI). BHIs connect to a shared network called the Backhaul Network.

The ISA model describes a communication interface between BHIs (IF2), which is typically a tunneling mechanism to enable communications between local devices (CCDs). The Tempered Networks solution implements IF2 using the Host Identity Protocol (HIP) published by the IETF as RFCs 5601 and 5602. HIP provides an identity-based key exchange that is more efficient than ISAKMP and has additional benefits. An additional HIP VPLS informational RFC describes the private overlay network approach using HIP.

The ISA model also describes a Configuration Interface (IF5). The Tempered Networks solution implements IF5 using standards from the Trusted Computing Group. Specifically, the Interface for Metadata Access Points (IF-MAP) is a specification to enable highly-scalable network security coordination. TCG has also published a standard that defines the IF-MAP metadata for Industrial Control Systems Security.

Together these standards provide the network architecture and security models upon which the Tempered Networks solution is built. These documents represent years of work by The Boeing Company, Juniper Networks, Infoblox, Mitre, NSA, Lumeta, Great Bay, Yokogawa, Oak Ridge National Labs, Tempered Networks, and many others. Reading these standards to gain deeper insight into the architecture and security model of the Tempered Networks solution is strongly recommended.

Implementation Details

HIPswitch Communications and Services

HIPswitches communicate on the shared network using standard ports and protocols. HIPswitches use DHCP or static addressing to obtain an IP address from the shared network, and can use DNS resources if configured. HIPswitches can rendezvous with the HIPswitch Conductor through either dynamic or static mechanisms:

- Dynamically with DNS SRV records
- Static Hostname / IP Address configuration of the HIPswitch Conductor IF-MAP Service URI

HIPswitches establish HTTPS connections to the HIPswitch IF-MAP Service on TCP port 8096. If central logging is configured, the HIPswitches will send UDP syslog messages to the configured syslog host and port. HIPswitches also establish HIP Security Associations using UDP-encapsulated IP Protocol 139, and use the UDP-encapsulated ESP protocol for the encrypted and encapsulated traffic. The only listening service on the HIPswitch is the service for establishing HIP Security Associations and receiving ESP packets. This service listens on UDP/10500.

The default security algorithms used by the HIPswitches for HIP tunnels are:

- RSA 2048 bit asymmetric keys for peer authentication
- X.509 certificates with AES-256/SHA-2 digital signatures
- AES-256 per-packet symmetric keys (as of v1.9)
- SHA-1 per-packet HMAC

The HIP ESP tunnels are established with the following parameters:

- Security Association (SA) lifetime: 172,800 seconds (48 hours)
- Diffie Helman (DH) exchange: group 3
- DH lifetime: 900 seconds
- Unused SA lifetime: 600 seconds
- SA establishment packet timeout: 10 seconds
- SA cookie puzzle difficulty (Denial of Service mitigation): 10 (hardest - most protection)

Each HIPswitch implements a stateful firewall to protect itself from other systems on the shared network. The basic firewall configuration performs TCP SYN flood protection, bogon packet filtering, rate limiting, and HIP service restriction to known peers.

HIPswitch Conductor Communications and Services

The HIPswitch Conductor typically uses static IP addressing for its connection to the shared network, though DHCP configuration is also an option. If central logging is configured, the HIPswitches and HIPswitch Condcutor will send UDP syslog messages to the configured syslog host and port.

The HIPswitch Conductor hosts the SimpleConnect HTTPS Web UI on TCP/443 and hosts the HTTPS IF-MAP Service on TCP/8096. These are the only listening services on the HIPswitch Conductor.

The HIPswitch Conductor implements a firewall to protect itself from other systems on the shared network. The basic firewall configuration performs TCP SYN flood protection, bogon packet filtering, rate limiting, and opens ports for only the necessary services.

Security Considerations

General Considerations

While we do refer the reader to the Security Model sections in the ISA and TCG documents, which describe the trust model, threat model, and countermeasures, we will address some further considerations here.

IF-MAP represents a coordination point for network and policy configuration and must be adequately protected against unauthorized access and modification. The Tempered Networks solution restricts access to IF-MAP to the following identities:

- The HIPswitch Conductor identity/identities
- Specifically listed factory reset HIPswitches
- HIPswitches that are managed by the HIPswitch Conductor

The HIPswitch Conductor IF-MAP service restricts access to IF-MAP by the client certificate presented in the HTTPS connection. Furthermore, the IF-MAP service has an authorization model that restricts metadata publishing by role and context (i.e. factory reset versus managed HIPswitches). The HIPswitch Conductor identity (and only the unique HIPswitch Conductor identity) is allowed to publish metadata that establishes the security policy configurations (private overlay memberships, HIPswitch-level policies, and device-level policies).

HIPswitch Registration to HIPswitch Conductor

An out-of-the-box or factory reset HIPswitch is allowed to connect to the HIPswitch Conductor IF-MAP service and publish only the metadata that is needed to announce its availability as an unassigned security appliance. These unassigned security appliances appear in the

SimpleConnect user interface, and users can verify that the Unique ID (UID) that appears in the SimpleConnect user interface matches the UID printed on the HIPswitch label.

Once a HIPswitch is added to a private overlay network, the HIPswitch becomes authorized to publish additional metadata for private overlay network communications and policy enforcement.

HIPswitch Revocation

If a HIPswitch is removed from a private overlay network, it will no longer be able to establish security associations to the other HIPswitches in the private overlay network. If a HIPswitch is not a member of any private overlay networks, it will not be able to establish security associations with any other HIPswitches. However, this HIPswitch will still be able to connect to the IF-MAP service with the role of a managed HIPswitch.

However, if a HIPswitch is deactivated or revoked within the SimpleConnect user interface, the identity of the HIPswitch is revoked from any access to the IF-MAP service. If a HIPswitch is lost or stolen, the HIPswitch should be removed from all private overlay networks in addition to being revoked.

HIPswitch Factory Reset

If a HIPswitch is factory reset (by gaining physical access to the HIPswitch and pressing the factory reset button for more than 8 seconds), the HIPswitch erases the following data:

- Cached security policy configuration
- Customer-signed certificate and CA
- Wireless network configurations
- Central logging service
- Static IF-MAP Service configuration
- Static IP Address configuration

After the HIPswitch is factory reset, it attempts to discover and connect to the IF-MAP Service in order to notify the HIPswitch Conductor that it has been reset. Once the HIPswitch Conductor determines that the HIPswitch has been factory reset, the HIPswitch Conductor removes the HIPswitch from all private overlay networks.

HIPswitch Device Security

There is no generally available console access to the HIPswitch. There is an external serial port on some HIPswitch models, however this serial port provides read-only diagnostic data only. The serial port does have a login prompt and the password for each HIPswitch is unique and is a 16 character alphanumeric random password. If desired, console access can be entirely disabled.

Shared Network Firewall

The Conductor and HIPswitches each implement stateful packet filtering on their shared network interface(s).

Next Steps and Call to Action

Best practices suggest comprehensive risk management, tied to a defense in depth cybersecurity implementation, is the appropriate approach for securing ICS. Network segmentation is a foundational building block of a defense in depth, layered security architecture. Standards from ISA are focusing on network segmentation because it can be used to constrain the connectivity for ICS to the absolute minimum, and protect that connectivity over shared network infrastructures. Additional standards from IETF and TCG show how these segmented networks can be efficiently managed at scale.

The Tempered Networks solution is an implementation of industry standards that not only decouples and secures the ICS communications from a shared network, but also decouples the management of the ICS systems from the management of the shared network. This delegated management approach makes it possible for an enterprise to deploy secure private networks as an internal service, while adding robust and flexible security to these critical systems.

Please contact Tempered Networks to learn how to use our solution in your environment.