Customer Case Study

Top Natural Gas Provider Safeguards Industrial Control and SCADA systems

Secure provisioning and anytime, anywhere access to vulnerable industrial assets.

Customer Needs

- Network segmentation
- Simplified identity management
- Less dependence on IT for SCADA controls
- Network bandwidth capacity improvement
- Secure remote access
- SCADA network redundancy
- Shared customer control provisioning

Solution

- Micro-segmentation
- Identity management overlay transparent to existing infrastructure
- HIPswitch protects each pipeline-metering skid

Benefits

- Anytime, anywhere contractor access to authorized SCADA controls
- OT provisioning freedom
- Reduced IT support workload
- Recovered network bandwidth through broadcast storm reduction

In a world where cyber-attacks are becoming daily occurrences, there are growing concerns about attacks on supervisory control and data acquisition (SCADA) systems.

SCADA is what allows organizations to control and monitor mechanized processes locally or remotely. It's the backbone of many modern industries including energy, food and beverage, manufacturing, oil and gas, power, recycling, transportation, water, and waste-water—in other words, services that keep society up and running. Most troubling, an attack on SCADA systems could become life threatening if, for instance, it shut down a town's water supply or crippled its power distribution infrastructure.

With today's prevalence of cyber-attacks, in addition to the specific targeting of SCADA, industrial organizations are worried that they could endanger thousands, even millions of citizens.

A leading North American provider of oil and natural gas services recently failed an infrastructure security audit. With only a flat Layer 2 network, they were very exposed and ripe for attack. The network lacked segmentation and had duplicate IP addresses from mergers and acquisitions. The radio networks used for control and telemetry readings were congested with broadcast storms. Inadequate redundancy guaranteed calamity in the event of a critical failure. And, multiple downstream refineries shared the natural gas liquid (NGL) pipeline control infrastructure. In short, the audit exposed a ticking time bomb in the form of the network.

Both the operational technology (OT) and information technology (IT) teams were aware of the many problems but, as with many businesses, department objectives, processes, and budgets were not aligned. OT provisioning and change requests took forever to process, raising tension between the teams, meanwhile the problems sat unaddressed.

The company signed a contract with a well-known global management consulting company to design a solution. It mainly consisted of next-generation firewall and VPN technology. But OT remained unconvinced, seeing that approach as overly complicated and expensive. Furthermore, IT would have to remain involved, exacerbating trouble ticket responsiveness.

 |

TEMPERED NETWORKS

Enter Tempered Network's Identity-Defined Networking (IDN) solution.

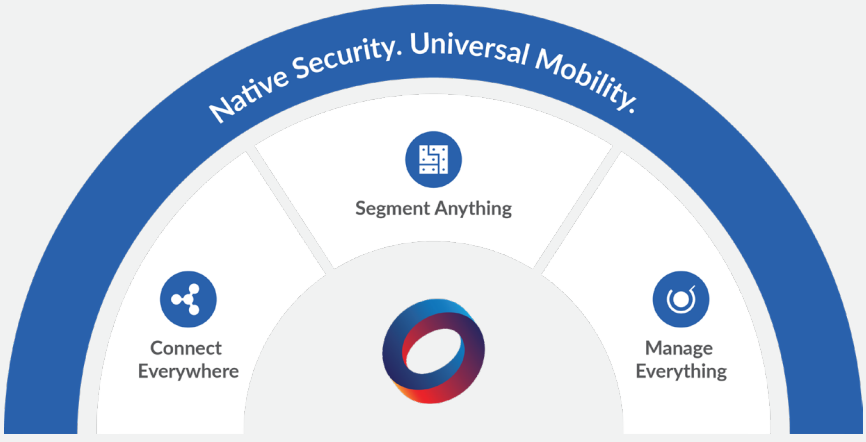
IDN is a secure networking architecture based on centralized orchestration of crypto-IDs, where only verified, trusted endpoints can communicate with each other. With IDN, connection, segmentation, encryption and cloaking of critical assets and networks become flexible, secure, and simple. Best of all, IDN is deployed as a transparent overlay to existing network infrastructure—no rip and replace.

IDN enabled much-needed security and operational control at a fraction of the cost of traditional NGFW/VPN approaches. Fundamental problems were solved immediately with micro-segmentation and Layer 3 routing became configurable with no impact to existing Layer 2 infrastructure. And, OT was able to take control of network adds, moves, and changes.

Seeing the promise and possibilities after deployment, IT decided to adopt IDN for an OSPF implementation that improved the efficiency of the radio network.

The project made use of HIPswitches, provisioned at each pipeline-metering skid. Since HIPswitches only allow identity-defined inbound connections, all network switching infrastructure behind them were cloaked from unauthorized view, heightening security. And field techs—using trusted, verified devices—can access the control network from a car or the field, anywhere, anytime.

With Tempered Network's IDN, OT service level has reached new heights. The client passed the next audit with flying colors and is far more secure against a potential SCADA attack—all at a fraction of the cost of traditional networking solutions.



Experience the same simplicity, security, and cost-savings that our customers achieved.

To learn more or schedule a no obligation demo, email info@temperednetworks.com or visit www.temperednetworks.com

