Security Monitoring of Critical Infrastructure

Deployment Scenario: Out-Of-Band Visibility Architecture

Monitoring of critical building infrastructures and industrial control systems (ICS) has become a key concern over the last several years for two reasons — cost control and unrelenting security threats. Security breaches continue to remain a persistent challenge for both data center providers and enterprises monitoring their networks, even as the expenditures on network security appliances increases.

Consistent monitoring and the installation of simple network visibility solutions can produce clear cost reductions. Critical pieces of network data exposed by a visibility solution and analyzed in either real time or near real time, prevent the loss of building functionalities like power outages, air conditioning outages, and equipment damage.

This solution brief presents a clear strategy for the network operation center (NOC) and security operations center (SOC) personnel to create visibility into critical infrastructure and ICS data networks.

Solution Components

- Keysight network packet brokers
- Keysight taps
- Keysight BreakingPoint
- Network monitoring tools

Benefits

- Remote access 24 x 7 to critical infrastructure and control systems
- Cost reduction because of faster alerting of system problems
- Deployment of n+1 survivability for ICS monitoring tools
- Testing and validation of critical infrastructure against security threats

KEYSIGHT TECHNOLOGIES

Solution Overview

This solution enables you to:

- Improve operational security across your network
- Create a monitoring architecture for your critical infrastructure components
- Extend Ethernet connectivity to remote equipment and equipment closets within your network

Sixty-eight percent of security and risk managers reported losing confidential information or experiencing disruption over the past year.

Improvement of Network Security Is Critical

Network security optimization is an ongoing and critical task. For instance, the Ponemon Institute, report titled "The State of Cybersecurity in the Oil & Gas Industry" says that "68 percent of security and risk managers reported losing confidential information or experiencing disruption over the past year."

Examples of vulnerable systems include heating, ventilation and air conditioning (HVAC), building power distribution systems, and communication systems. For example, modern versions of HVAC systems need continual monitoring to stay energy efficient and ensure building occupants are comfortable. Frequent monitoring is necessary because there are numerous environmental sensors and motorized control systems within HVAC systems. Proper monitoring helps maintain a consistent temperature to reduce energy and maintenance costs.

Also, many building and system control and data acquisition (SCADA) systems remain unhardened against the multitude of security threats that exist. These threats include:

- Third-party remote and wireless access since contractors may have lax security processes
- Proprietary appliances and sensors with potentially outdated software which are prone to vulnerabilities, the use of default/easy passwords, and the lack of encryption safeguards
- Insufficient attention from NOC/SOC personnel due to auxiliary nature of critical infrastructure networks to their daily tasks
- The common practice of rotating technical personnel that are servicing critical infrastructure equipment — this provides wider access to the physical infrastructure including the network and USB ports
- Malware insertion through dedicated attacks that take control of critical infrastructure for criminal and nation-state security attacks

Malware and cyberattacks can easily interfere with command and control of critical data infrastructure and also result in successful ransomware attacks that can cost thousands, if not millions, of dollars.

Monitoring and Testing Critical Infrastructure

A three-pronged approach can solve these issues.

Prong 1: The first prong of the strategy is to place Ethernet-based taps into buildings and enclosures. Taps give building personnel and network managers (DevOps and SecOps teams) easy access to data from critical infrastructure systems.

Prong 2: After tap installation, a network packet broker (NPB), like the Keysight Vision ONE, aggregates data from the various taps. The NPB can capture, filter, and regenerate specific pieces of data as necessary and pass that data to the specific application monitoring tools. For example, Security Matters and Claroty are two types of tools that perform data examination. Data segmentation allows the DevOps and SecOps teams to see only the information that they need while removing extraneous data.

The NPB also provides the internal ability to load balance data before sending it to multiple tools. This enables IT personnel to deploy n+1 survivability. The traffic load is divided evenly across the number of allocated tools. Should one or more of the data monitoring tools fail, the data spreads evenly across the remaining number of tools. Proper tool dimensioning ensures there is no loss of data.

Figure 1 outlines the solution's process.

The NPB will capture, filter, and regenerate specific pieces of data as needed and pass that data on to individual application monitoring tools (like Security Matters and Claroty) for data examination.

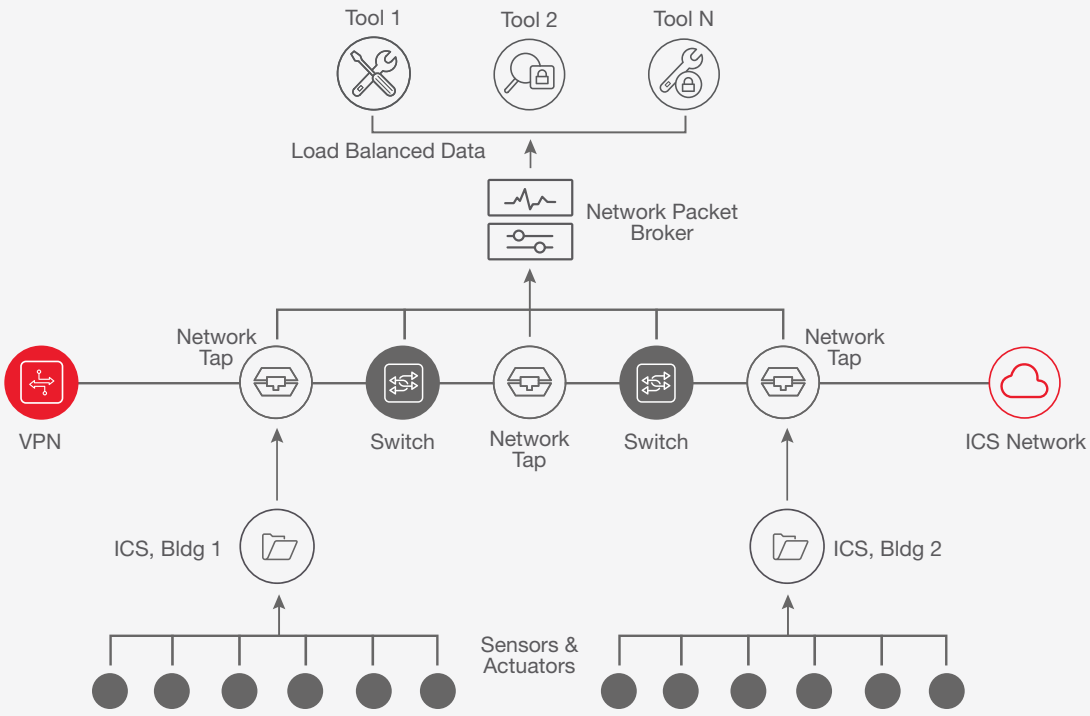

Figure 1. Typical monitoring architecture for critical infrastructure.

Prong 3: The third prong of the solution is to use a security testing device, like Keysight's BreakingPoint, that actively tests critical infrastructure. Figure 2 highlights the tests that include the simulation and introduction of realistic malware into lab-based versions of the infrastructure to determine potential vulnerabilities.

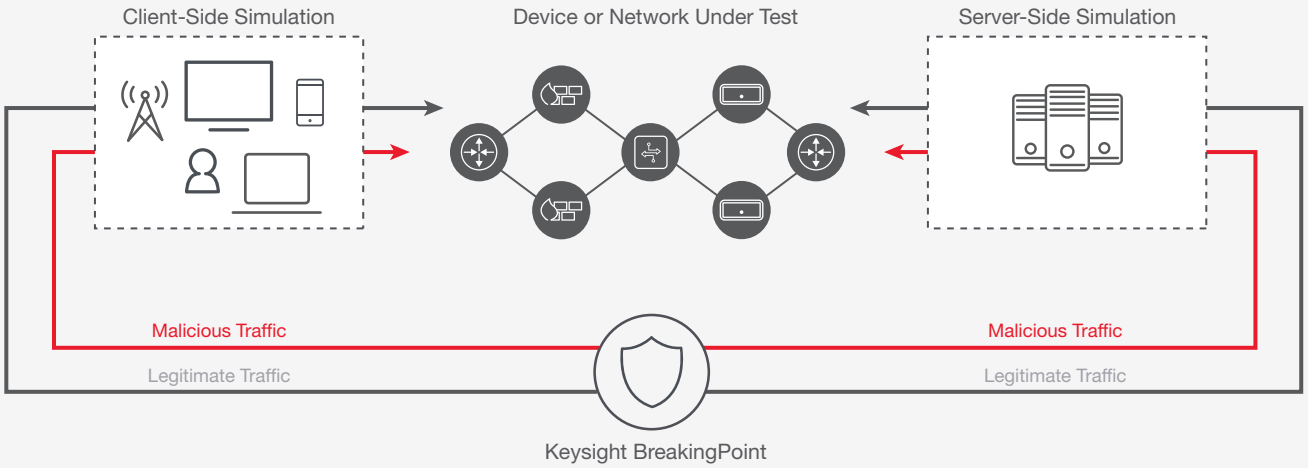

Figure 2. Security testing scenario.

Summary

Network security optimization is a never ending challenge but one that can be made easier with enhanced visibility into your network. One way of doing this is to provide access to network monitoring data via taps, which then feed into network packet brokers which can then filter, deduplicate and otherwise groom data to make more efficient use of security and other tools on your network. Network packet brokers can also help you deliver greater uptime in addition to enabling active security testing.

Visibility Architecture Solutions from Keysight

Keysight's network visibility solution involves using NPBs in conjunction with taps and network threat testing equipment. Learn more about Keysight's Network Packet Brokers, BreakingPoint, and tap technologies, along with our technical partner solutions.