Overview

Industrial control systems (ICS) such as Supervisory Control and Data Acquisition (SCADA) systems and Human Readable Interfaces (HMIs) are a critical component of monitoring and controlling industrial infrastructure processes across the energy, nuclear, and critical manufacturing sectors. They combine hardware, software, and network connectivity to help you precisely monitor, control and visualize every aspect of your operations.

These advances in smart sensor technology and wireless networking are made possible by the blending of operational technologies (OT) and open-protocol information technologies (IT). Despite the benefits, the convergence of OT/IT means that organizations are highly susceptible to lateral attacks from these connected systems, such as those instigated against the Ukrainian power grid in 2015. HMIs are an attractive target since they are installed on a network-enabled location and are a vital component for controlling the entire SCADA system. If you can control the HMI, then you can take over the key industrial processes.

Using off-the-shelf hacking tools, hackers bypass perimeter defenses such as firewalls, intrusion detection systems, and application level privileges to gain access to the control system LAN.

Furthermore, software-based VPNs (used by engineers and even remote third-party vendor support teams to access the control system LAN) are easily bypassed by sophisticated attacks, especially on untrustable endpoints. An attacker will attempt to take over a machine and wait for the legitimate user to VPN into the control system LAN and piggyback on the connection. In systems with password only authentication, the attackers can easily steal the user credentials and access the control system network from their own PC.

Once in, attackers take advantage of an additional vulnerability to take control of the ICS. In ICS networks, asset owners often do not secure the data that flows between servers, resources, and devices because they assume the data resides on a “protected” network. With more and more organizations connecting ICS networks with business systems, security issues arise from this assumed trust, including the ability for an attacker to reroute data in transit on a network (aka a man-in-the-middle attack), to capture and analyze critical traffic in plaintext.

Organizational Challenges

- Improve network and system security without significant cost and disruption
- Manage internal and third-party threats when opening the network to remote workers, vendors, and support teams using untrustable devices
- Quickly and simply establish and manage secure site-to-site and remote connections
- Simultaneously protect critical assets against external and internal threats
- Cost-effectively scale to meet growing networking requirements

Technical Challenges

- Establish quick and secure connections, without IT intervention and overhead
- Protect IT, IIoT, and OT networks without degrading performance and availability
- Counteract the vulnerabilities inherent in software or virtual security solutions
- Minimize impact on existing infrastructure and user experience
- Prevent malware from propagating once on network
format, or the ability to reverse engineer control protocols to gain command over control communications.

Yet, there remains no practical or effective strategy to mitigate imminent threats to critical industrial operations while addressing their unique performance, reliability, and safety requirements – until now.

**The Blue Ridge Networks Solution**

Blue Ridge Networks’ Autonomous Network Segmentation (ANS) solution is a self-contained cybersecurity ecosystem that protects organizations from vulnerabilities posed by connected devices, networks, and people by establishing cryptographically isolated network segments within an organization’s networking environment and eliminating the entry point for cyber-attacks.

Based on the Zero Trust methodology, ANS provides the highest level of security autonomously – seamlessly protecting your most critical infrastructure and allowing your IT teams to focus on other tasks. ANS enables secure connectivity across the enterprise – wherever it’s needed, without costly or time-consuming IT overhead.

Using public or private clouds, and with support for any communication media, ANS enables secure connectivity for industrial and building automation systems (BAS) and allows infrastructure managers to access, monitor, and control building assets. Support for the system integrity of SCADA/HMI has never been easier or quicker to deploy.

**How it Works**

ANS is an operationally transparent and versatile overlay solution that enables industrial organizations to seamlessly connect, isolate, contain, cloak, and manage users and devices over any transport, anywhere in the world – with minimal network configuration changes. This concept of network segmentation, enforced by encryption, and the establishing of secure enclaves is a core recommendation of NIST Special Publication 800-82 (Rev 2) Guide to Industrial Control System Security.

The ANS ecosystem is comprised of the BorderGuard hardware that serves as the orchestration engine and root of trust for the entire ANS ecosystem, and RemoteLink and EdgeGuard devices that extend proven security architecture to dispersed offices, remote sites and users, and more.

The ANS ecosystem uses built-in mandatory public key cryptography to automatically authenticate the identity of each appliance. Rather than monitor packets based on known-threats and pre-determined rules, ANS stresses autonomous cryptographic proof over content dependence. Each network packet must provide cryptographic evidence that it originates from a trusted ANS appliance and known closed user group before being decrypted and forwarded to the user. Once deployed, the products don’t trust anyone or anything else, establishing cryptographically isolated network segments within an organization’s networking environment and eliminating the entry point for cyber-attacks.

**Key Benefits**

- **Increased Efficiency** – Minimal IT configuration and resourcing and independence from traditional IT tools increases efficiency of both OT staff and users and drastically decreases operational expenses.

- **Tried and Tested** – Originally developed to protect high value critical operations and assets for the US Government.

- **Reduced Network Complexity** – Allows you to protect your critical operations autonomously without dependence on complex traditional IT solutions like firewalls, VPNs, Access Control Lists, and VLANs.

- **Seamless Integration with Your Existing Infrastructure** – Overlays existing IT infrastructure with little to no modification to the underlying network infrastructure.

- **Simple and Cost-Effective** – Eliminates the need for pre-configuration and traditional IT tools that require staff to manage.

- **Built-in Two-Factor Authentication** – Mitigates the vulnerability of exposure by not requiring a user to depend on a password, or shared secret, for authentication.

- **Managed Services Option** – Further decreases the complexity of secure networking: deploy ANS as a managed service to allow your IT team to focus on more critical tasks.
The ANS ecosystem includes a Management Console that serves as the orchestration engine and security policy enforcement for all ANS appliances and software. The management console allows admins to remotely manage the system and define security policies in one place without impacting its operational mission. The management tier (layer of tunnels) does not intersect with and is cryptographically and operationally separate from any data channels, and their controls do not depend on the data being transferred. The data channels continue to provide secure transport regardless of if the management tier is online. Set up and control of the management channels are associated with the system administration function through the Management Console.

Our security algorithms have been NIST FIPS 140-2 validated and we currently hold Army CoNs for multiple products. In addition, our solutions have been cited as compensating controls for HIPAA and PCI compliance.

Use Cases

Isolate and Contain OT systems
ICS professionals are now leveraging the public internet to enable connectivity of OT systems, but with that connectivity comes the risk of exposing these networks and system to possible attacks which could lead to system breaches and downtime. With ANS, networks protected by the ANS ecosystem are isolated and cloaked from both the IT network and the outside world without impacting system functionality. ANS securely connects OT/ICS system using any protocol to untrustable devices through untrustable communications mediums without the risk that would be inherent in traditional networking environments. Any malware or threat that had previously affected the system is contained within the segment, drastically reducing the possibility of lateral attacks or exfiltration of critical data and credentials.

Ubiquitous Connectivity for OT Systems
While IT networks require the need to widely communicate with other parties of all types, OT systems require specific exclusive, access to only dedicated users. With ANS, organizations can provide remote access to authenticated parties (such as vendor support and maintenance teams) while enforcing policies to eliminate the risk of accidental threats that the user may pose. ANS also allows organizations to continue leveraging shared infrastructure to reap the cost benefits without leaving those systems wide open and susceptible to the risks that a shared infrastructure poses. Organizations can further realize cost savings because unlike traditional network segmentation approaches, ANS doesn’t depend on complex network architecture that relies heavily on internal firewalls, VPNs, Access Control Lists, and VLANs – making it simple and cost efficient to secure critical assets.

Establish Quick and Secure Network Connections
As your organizations scales and building automation systems and operations become more interconnected across departments, buildings, and to remote sites and users in the field, the ANS ecosystem protects and secures network access using autonomous cryptographic authentication of all network communications.

Even previously compromised systems are rendered harmless to surrounded networks as the ANS ecosystem contains and prevents malware from establishing unauthorized communications outside of the isolated network segment.

Securely Open the Enterprise Network to Your Remote Workforce
The ANS ecosystem’s proven security architecture extends to create trusted network segments, or enclaves, in the field. Using mandatory, mutual authentication, remote teams, users, third party vendors and engineers can securely access the network via untrustable devices without the possibility of an attacker entering network sessions via identity spoofing or man-in-middle attacks.

Easy to deploy, ANS securely connects remote networks over any communication medium. No configuration by end users is required. Its simple approach to secure remote access provides field offices, mobile work teams, and even deployed personnel an easy-to-use LAN extension to their enterprise data network.
Industry-Verified & Trusted Security

The ANS ecosystem provides access to a data network while transporting packets over another network. It does this while maintaining mandatory separation of the two networks such that no nodes on either network can communicate with other nodes.

Originally developed to defend highly sensitive networks for the Intelligence Community, Department of Defense (DoD), and other U.S. government customers, the ANS ecosystem is considered the "next best thing to Type-1 (classified)". We proudly meet or exceed all NIST SP800-82 recommendations and are operationally compatible with all industrial IEEE 802.3 protocols.

The ANS ecosystem’s built-in public key trust system protects and complements enterprise VPNs, VDI environments, user authentication methods, SSL platforms, and other system architecture components without disrupting the existing network infrastructure or operational processes.

With over 20 years in deployment, Blue Ridge products have never had a reported breach.

About Blue Ridge Networks

Based in Northern Virginia, Blue Ridge Networks is a visionary cybersecurity pioneer that provides autonomous cybersecurity for the connected world. Blue Ridge Networks’ Autonomous Cybersecurity Suite protects organizations from vulnerabilities posed by connected devices, endpoints, networks, and people. Blue Ridge solutions have protected critical operations for some of the largest US government, financial, healthcare, and other critical infrastructure customers for more than twenty years with no reported breaches.

Contact Us:
1-800-722-1168
sales@blueridgenetworks.com

Headquarters:
14120 Parke Long Court Suite 103
Chantilly VA, 20151