cuculan™

Janus security versus Firewall security

By: cuculan
Date: 12-2022

The deployment of operational technology (OT) devices that control and monitor physical devices is increasing exponentially while the security related to these devices is lagging. Moreover, the convergence of IT and OT in industrial verticals based on the need to access operational data to streamline business decision making is exposing OT devices to bad actors. OT systems have not traditionally received the level of security focus and protection that is commonplace in the IT world such as encryption, zero trust access, micro segmentation, and mutual authentication and are not well positioned to defend against current cyber security threats. Current forecasts estimate that there will be eighteen billion OT devices in use in 2022.

On the other hand, as Information Technologies (IT) that enable the distribution and management of data and information using computers, networks and application software have become critical assets to managing a business, it has also become a critical exposure area for cyber-attacks. The need to protect these assets from access by unauthorized internal as well as external bad actors while ensuring the confidential secure exchange of information to authorized organizations is critical.

It is imperative that every organization understands the key requirements that need to be satisfied to implement a secure environment with the solution that is easily configurable, requires minimum maintenance without the need for sophisticated technical expertise to deploy and manage. These requirements span not only the specific security capabilities required in a comprehensive security solution but also how the solution itself is presented to the user from an ease of use and management perspective.

Below is a comparison between the Janus technology and Firewalls.

The **Janus** solution is a purpose designed device to address these requirements. It brings together the following features in a secure, easy to implement, and low-cost of ownership appliance.

cuculan™

Janus security versus Firewall security

Operations

- ✓ Proactive mutual authentication of network resources
- ✓ Concealment of protected network resources
- ✓ Full encryption of all packets sent across the network
- ✓ Network segmentation/micro segmentation
- ✓ Secure networks from lateral breaches
- ✓ Secure networks from internal attacks
- ✓ Provide hardened security device
- ✓ Provide automatic failover

Management

- ✓ Ease of configuration of network security
- ✓ Minimal maintenance of configured network
- ✓ No third party/cloud tools required
- ✓ No agents required
- ✓ Centralized firmware updates

Implementation

- ✓ Ease of configuration/setup
- ✓ Ease of deployment
- ✓ Centralized configuration

Cost

- ✓ Low cost of entry
- ✓ Low cost of growth
- ✓ All capability contained in the device with no need for additional agents or external management

The fundamental premise of the **Janus** device is that it provides a purpose designed device to address point-to-point and point-to-multipoint security targeted primarily at environments that require resource to resource

security. Its goal is simplicity. As such it is a self-contained hardened device that is simple to set up, easy to maintain, delivers to the requirements described above at a preferred cost to other available solutions.

The Janus device is locked down during the manufacturing process with subsequent access to the device being only through the API. Additionally, access to the API itself is through biometrically authorized administrators.

Set up is completed by simply registering the device via the management application and plugging the device in-line with the resource it protects. A centralized management application assigns the Janus device to its protected resource and the network resources it is authorized to communicate with on the network.

The Janus device is easy to maintain with additions, removals and changes to devices and protected resources on the network managed through the centralized management application.

It is cost effective as it is

- ✓ Self-contained with all features included
- ✓ Does not require deep networking knowledge to manage
- ✓ Does not require installation of agents on protected resources
- ✓ Does not require cloud-based management system
- ✓ Does not require annual subscriptions
- ✓ Requires minimal maintenance driven only by network connectivity changes

A **Firewall** is a general-purpose solution designed to address a wide array of requirements. Firewalls are necessary at the internet/company edge and are well suited for this purpose, but they are not optimal for internal resource-to-resource protection.

Firewalls fail to meet key requirements in a point-to-point or point-to-multipoint environment that require security between resources.

- Firewalls require sophisticated networking management knowledge. Both filtering and encryption is required to fully secure a resource. This is implemented through ACL’s or AI devices in combination with

point-to-point/ point-to-multipoint VPNs. This approach requires multiple steps and needs in-depth security understanding to properly secure resources.

- Firewalls are expensive and, depending on the firewall supplier, may require a cloud-based management service and annual subscription.

- When securing a network resource, a security device is deployed adjacent to, and in-line with, the protected resource to minimize any unprotected network segment. This may require the device to be located outside a security enclosure and physically exposed to unauthorized employees or bad actors. As such, many firewalls allow recovery of the administrator password and the potential of uncontrolled access by bad actors.

When choosing a solution for your IT/OT challenges security professionals should review all solution options and look for the solution that best meets their security requirements from a capability, manageability, and cost perspective. We believe that for point-to-point/multi-point environments the **Janus** solution meets these requirements.