

CA Automic Proxy

At A Glance

CA Automic One Automation platform is the linchpin of your business automation strategy, successfully automating many of your most critical IT processes and giving you complete control from the infrastructure and application layer, right up to the business layer. By managing secured tunnels between the CA Automic One Automation platform and the rest of the network, CA Automic Proxy lowers risk, increases control and reduces network security maintenance costs.

KEY BENEFITS

- Reduces the threat of external hacking attacks and provides a secure automation environment through an additional security layer
- Achieves faster time-to-value for new automation initiatives, and quickly automates new hosts and applications without touching or weakening your firewall
- Simplifies network configuration and reduces maintenance costs

KEY FEATURES

- **Secured tunnels** between the CA Automic One Automation platform and the rest of the network
- **One-way connections** enforced between the secured network and the other segments, no incoming connections
- **Multiplexed communications** that reduce the administrative burden of opening up new firewall ports for each new automation target
- **Seamless fault-tolerance** by adding redundancy with another proxy pair

Business Challenges

As part of your strategy to ensure a continuously secure automation network, you are experiencing exponential growth of network segments—*islands of security* with thousands of uncontrollable tunnels between them. This problem of multiplying open firewall ports is particularly apparent if you control external servers in different, co-located network segments. For every new host, your CA Automic One Automation platform administrator is opening a new network port in your secure automation network, as well as in the externally located target network.

This volume of open firewall ports—thousands in a typical setup—is compounding complexity. Moreover, it is time-consuming to administer, expensive and can quickly undermine your IT governance and compliance strategy.

For instance, every time you need a new port, your security team needs to evaluate, document and give approval to the network team—a significant administrative overhead. Moreover, the security officer will be alarmed by the risk to governance and compliance arising from the rapidly growing number of open firewall ports; each one representing an increased risk of a hacking attack into your secure automation network.

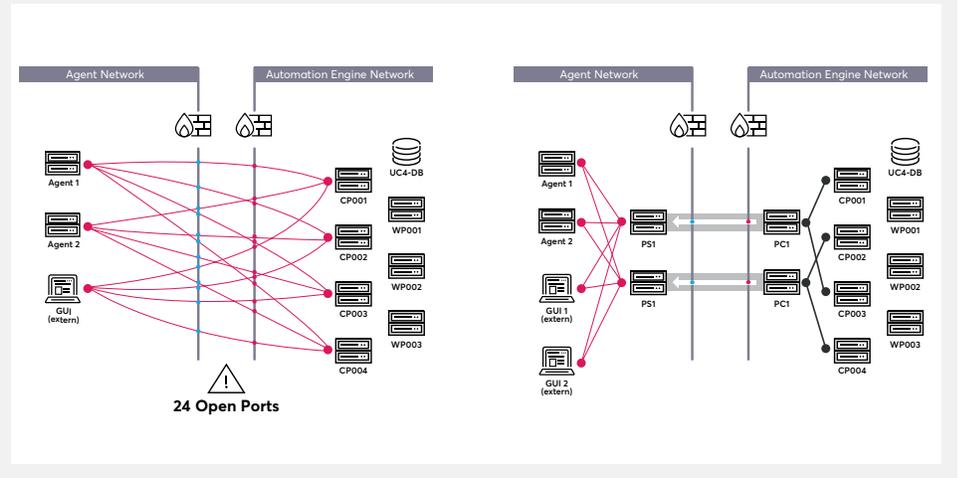
- Network complexity makes it difficult to know which ports are open and why
- Firewall hole monitoring and evaluation extremely difficult to understand
- You are required to open new ports for each connected automation target
- Each target requires an open incoming port in the firewall configuration

Solution Overview

With CA Automic Proxy, you can seal off thousands of firewall ports in your critical network segments and ensure fail-safe communication. This convenient solution removes all incoming open ports from your secure network and adds a transparent application security layer to your communications.

The result is a more secure automation environment, free of threats, with more control and lower network security maintenance costs.

Conventional Automation Engine Network without CA Automic Proxy vs with CA Automic Proxy



Related Products

CA Automic Workload Automation. Deliver the fully automated enterprise with intelligent business automation.

CA Automic Release Automation. Drive Agility and speed to digital business apps and core commercial applications

CA Automic Service Orchestration. Deliver the IT Services your users, applications and infrastructure need, when they need it.

For more information, please visit ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.