MOCANA

# Mocana CyberWall™

## Embedded Network Access Controls for Device Security

The Mocana® CyberWall™ Client provides embedded and lightweight network access controls for Mocana TrustEdge™-enabled distributed IoT devices with TrustCenter-based management for tamper-resistant delivery of policies. Network layer access controls (i.e., allow, deny rules) may be provisioned by packet header (source/destination MAC address, IP address, port number), network interface type, and destination domain-based dynamic filters. CyberWall comprises the Mocana TrustCenter™ CyberWall (TCCW) Studio and the Mocana TrustEdge Protection CyberWall (TPCW) Client (see Figure 1 below).

## Mocana CyberWall Services Architecture

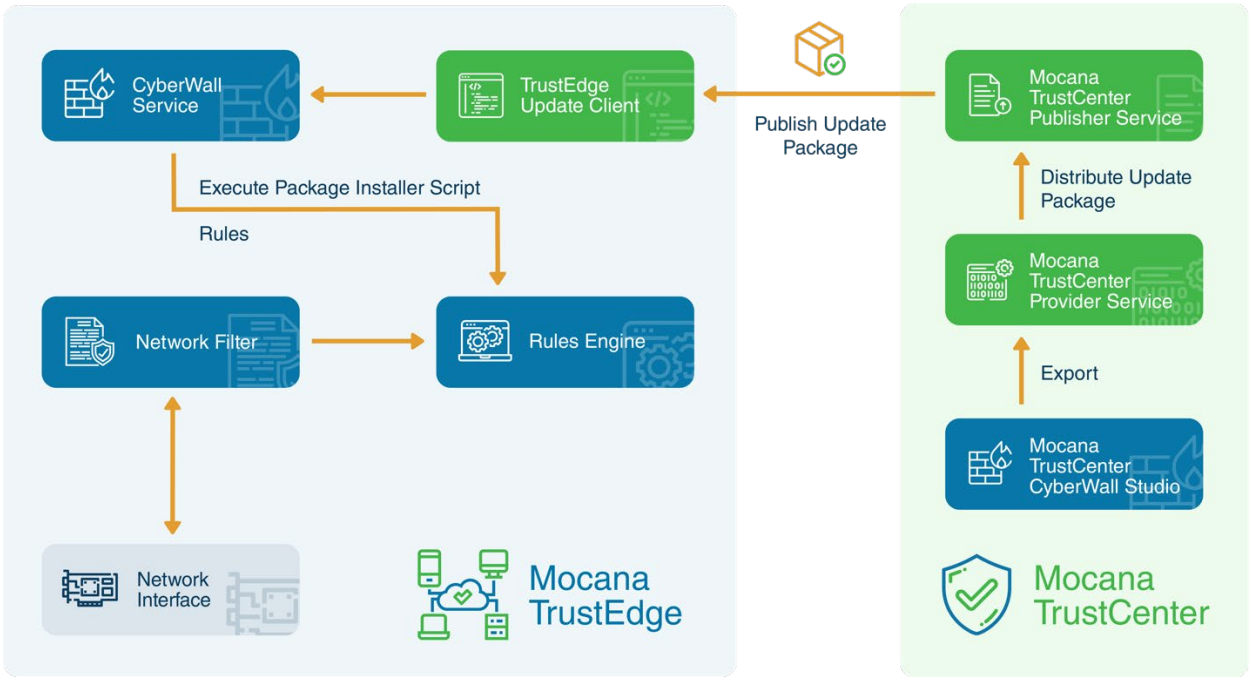


Figure 1. Mocana CyberWall Services Architecture

## Benefits

- Enable light-weight embedded network access controls to protect IoT devices across verticals
- Apply tamper-proof rule updates with supply chain validation
- Provide security controls required to meet compliance standards (NERC-CIP, ISA 62443)

## Security Features

- Integrated with the Mocana TrustCenter™ Update Service (TCUS) and Mocana TrustEdge™ Protection Update Client (TPUC) for tamper-resistance rule updates.
- Small memory footprint on the device.
- Network access controls with rules for enforcement based on input interface (LAN, WAN, Wi-Fi), output interface (LAN, WAN, Wi-Fi, PPP, Cell), protocol type (UDP, TCP, ICMP, AH, ESP), source/destination MAC address, source/destination IP address, subnet or address range, source/destination port, and destination domain.
- Policies associated to Mocana TrustCenter device types.
- Files (rules and configuration) digitally signed by Mocana TrustCenter for tamper resistance.
- DNS parser for domain-based rules to inspect inbound packets from UDP/port 53 (DNS responses), extract domain names (CNAME, ALIAS records), extract IP addresses (A records), hash/remove/add new IP addresses to domain tables, and update the IP hash table with new IP hashes.
- Enables use of granular pinholes with default deny.
- No reliance on the open-source community libraries.
- CyberWall Studio installs as a Docker container, a virtual machine or native application.
- CyberWall Client installs as a native lightweight service and network filter on the device.

## Supported Device Types

- Edge gateways
- Network devices
- Network servers
- HMI workstations
- Medical systems
- Aviation systems
- Automotive systems
- Industrial control systems

## About Mocana

Mocana protects more than 100 million devices worldwide and is trusted by the largest aerospace, industrial, energy, healthcare, and communications companies. Find out more at www.mocana.com.

**Mocana Corporation**
1735 North First Street, Suite 306
San Jose, CA 95112
tel (415) 617-0055 toll free (866) 213-1273
**sales@mocana.com**

 Revised June 28, 2021 