Network Standards and Remote Support

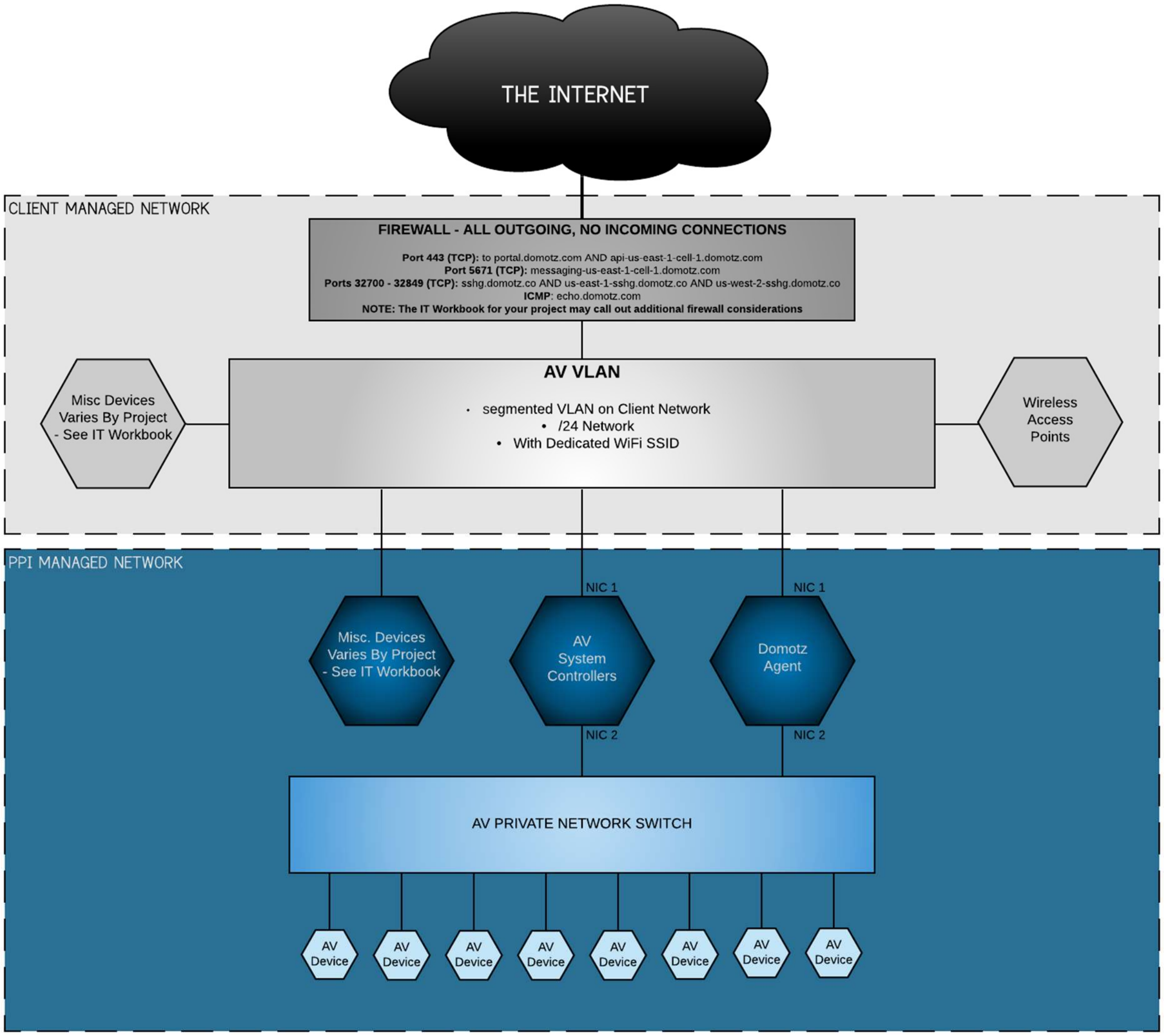
Introduction

PPI's standard networking approach allows PPI to provide a consistent and reliable AV network while easing networking coordination by segmenting the most, if not all, AV LAN traffic from our client's production networks. All devices not requiring internet or local network connectivity will be solely connected to a private network switch managed and maintained by PPI. Any devices that do require internet or local LAN connectivity will connect to a dedicated, segmented "AV VLAN" on the client's network. This "AV VLAN" shall be as isolated as much as possible from the client's production network for security purposes; in some cases, complete isolation can be accomplished on this network segment.

This standard package may also include a remote monitoring and support option, which provides PPI withessential remote support capabilities. If this is deployed PPI will be able to monitor AV systems and to receive real-time alerts whenever an issue is detected. This also allows PPI engineers to remotely access, service, and troubleshoot the AV systems, significantly reducing response time, sometimes, when coupled with proactive monitoring, fixing issues before they're noticed by end users. PPI uses the Domotz Pro platform for this purpose.

Is there a typical network topology diagram?

Below is a diagram showing the typical network topology:

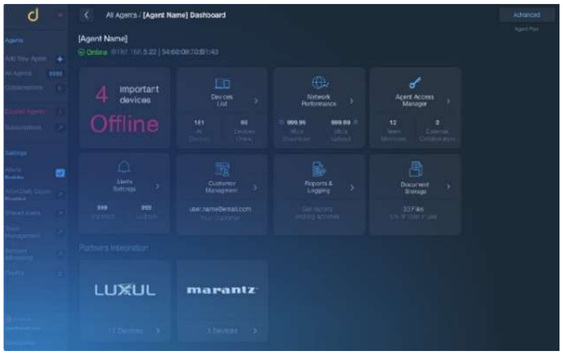


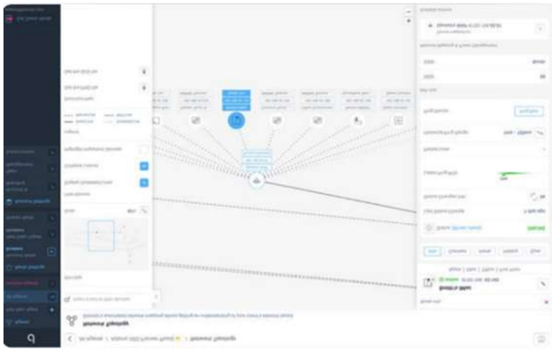
THE INTERNET
CLIENT MANAGED NETWORK
FIREWALL - ALL OUTGOING, NO INCOMING CONNECTIONS
Port 443 (TCP): to portal.domotz.com AND api-us-east-1-cell-1.domotz.com
Port 5671 (TCP): messaging-us-east-1-cell-1.domotz.com
Ports 32700 - 32849 (TCP): sshg.domotz.co AND us-east-1-sshg.domotz.co AND us-west-2-sshg.domotz.co
ICMP: echo.domotz.com
NOTE: The IT Workbook for your project may call out additional firewall considerations
AV VLAN
• segmented VLAN on Client Network
• /24 Network
• With Dedicated WiFi SSID
Misc Devices Varies By Project - See IT Workbook
Wireless Access Points
PPI MANAGED NETWORK
NIC 1
NIC 1
Misc. Devices Varies By Project - See IT Workbook
AV System Controllers
Domotz Agent
NIC 2
NIC 2
AV PRIVATE NETWORK SWITCH
AV Device
AV Device
AV Device
AV Device
AV Device
AV Device
AV Device
AV Device

To view Full-scale version of this diagram, click HERE

What is Domotz?

Domotz Pro is a network monitoring and remote technical support system that gives PPI control over and access to devices on the AV VLAN and Private AV Network. Domotz detects and monitors IP devices on the network, giving remote access to devices, providing network health analysis tools, and the ability to get notified in the event that a devices' connectivity changes. This, coupled with PPI's custom control system programming that provides additional hooks and alerts into the Domotz platform, combines to create a robust, detailed, and complete monitoring and support package for your AV systems.





All this is compiled and displayed on easy to read dashboards and reports, allowing dispatch and service teams to quickly identify problems to assign for resolution, and then efficiently diagnose, troubleshoot, and resolve them.

What hardware will be installed onto the AV VLAN?

Most installation will have the following 2 components installed onto the AV VLAN:

- **A Domotz Network Agent:**, a custom-built Orange Pi PC running the Ubuntu Core OS, will be installed. This device has 2 network interface cards. One NIC for connecting to the "AV VLAN", and the second NIC connected to the private PPI AV Network. The connection to the AV VLAN's singular purpose is to provide internet access to the Domotz Network Agent

- **An AV Control Processor, typically Crestron:** This device also has 2 network interface cards, connecting to the AV VLAN and the private PPI AV network the same way the Domotz Agent does. The AV Control Processor's connection to the AV VLAN is less about internet access, and more about communication to common auxiliary AV system components on the network, such as:
  - Connection to tablet-based AV control touch panels, mainly iPads, connected to a client provided AV SSID
  - Connection to 3rd party systems such as:
    - Lighting and Shade Systems
    - Building Information Management (BIM) Systems
    - Room Scheduling Systems

Most smaller systems will require only 2 IP addresses for the AV systems themselves; one for the Network Agent and one for the AV Control Processor.

Note that additional hardware, requiring further IP addresses, may be required based on the size, complexity, and scope of your AV systems. Additional requirements, if any, will be coordinated by PPI's engineering team during the installation phase of the project.

How will networking information for my project be coordinated?

PPI will submit a document called the "IT Workbook", custom built for your project, that will outline all devices being installed onto the network, both client and PPI managed. This document will be submitted during the planning phase of the project for coordination purposes and again at the end of the project for record as part of our usual closeout process.

This document will also make general network architecture suggestions as well as list out any firewall adjustments that may be required for the system as specified. Generally speaking, firewall adjustments, outside of Domotz outbound connections to the internet, listed below, are only ever necessary if it has been requested that the AV system will communicate with outside systems like lighting, shades, BMS, scheduling platforms, etc.

Once the IT workbook has been submitted, PPI engineers will schedule coordination calls and efforts with all relevant project stakeholders and IT department members to review the workbook in detail, discuss the network deployment strategy, and answer any questions there may be. Every network is different, and this process is meant to be highly collaborative to ensure that decisions made regarding the network are understood and approved by all.

How is PPI gaining access to the AV systems remotely?

We will be using the Domotz platform to create a secure VPN tunnel into the Network Agent, which then allows for connection to devices on the AV networks. Domotz Pro's remote connection establishes a secure channel (encrypted overlay network) between the agent and Domotz Cloud services. A separate HTTPS channel is established between application and Domotz Cloud Services. The entire communication from end to end is encrypted.

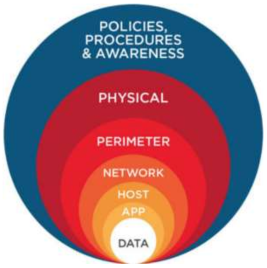
What adjustments need to be made to my firewall?

The Domotz Platform uses the below ports for OUTBOUND connections to the internet at the specified addresses:

Port	Type	To	Description
443	TCP	api-us-east-1-cell-1.domotz.com	Domotz Updates
443	TCP	portal.domotz.com	Initial Connection and API Dispatcher
5671	TCP	messaging-us-east-1-cell-1.domotz.com	Domotz Agent Commands from Domotz Cloud
32700 - 57699	TCP	sshg.domotz.co, us-east-1-sshg.domotz.co us-east-1-02-sshg.domotz.co ap-southeast-2-sshg-domotz.co us-west-2-sshg.domotz.co	Remote Connection/VPN
N/A	ICMP	echo.domotz.com	Internet Heartbeat

Is remote access and support secure?

Security is a core pillar of the Domotz platform and has been built from the ground up with security as a top priority. Enterprise grade best practices are in place to protect customers networks and data:



- Defense in Depth
    - Defense in Depth (layered defensive mechanisms), and Defense in Breadth (multiple and automated security controls) are the pillars of our cyber defense strategy. Comprehensive and layered physical, technical, and administrative controls are in place to protect data and to block threats before they can reach endpoints. As today's cyberthreats are evolving and growing rapidly, we continuously review and enhance our defenses. Security patches to both Ubuntu core and Domotz software are automatically updated.
- Security Standards and Practices
    - Domotz has adopted CIS Control® as a global standard and a set of recognized best practices for securing IT systems and data against the most pervasive attacks and threats. Domotz is also part of the OWASP community and uses a number of OWASP tools and resources, as well as OWASP's education and training programs.
- Physical & Data Centers Security
    - Domotz servers are hosted on Amazon Web Services (AWS), state-of-the-art data centers with electronic surveillance, multi-factor access control, and 24-7 security guard protection. The data centers are ISO 27001, ISO 27017, and ISO 27018 certified, and undergo regular SOC 2 Type II audits.
- Data Security
    - Domotz has adopted the best administrative, physical, and technical industry-standards to protect the confidentiality of data and the security of credentials stored in the system.
    - Domotz uses strong cryptography and security protocols for data in transit and at rest. Cryptographic keys are managed, secured, restricted, and rotated according the recommendations of National Institute of Standards and Technology to NIST SP 800-57 Part 1 Recommendation for the management of encryption keys.

In addition to Domotz's security practices, PPI has put the following measures in place to ensure no un-vetted or unauthorized user ever has access to the platforms or systems:

- All users are only added to the PPI-Domotz platform by invitation from PPI ownership
- All PPI users only use their PPI domain email for their Domotz login
- All users have a forced two-factor authentication policy enacted
- All PPI users have a randomly generated password for their Domotz Login

With these measures in place we believe that we can have a stable and secure remote connection to manage and service our audiovisual equipment, and our customers need not worry about the security of our methods.

For additional information, Domotz's security whitepaper is available HERE (direct PDF download)