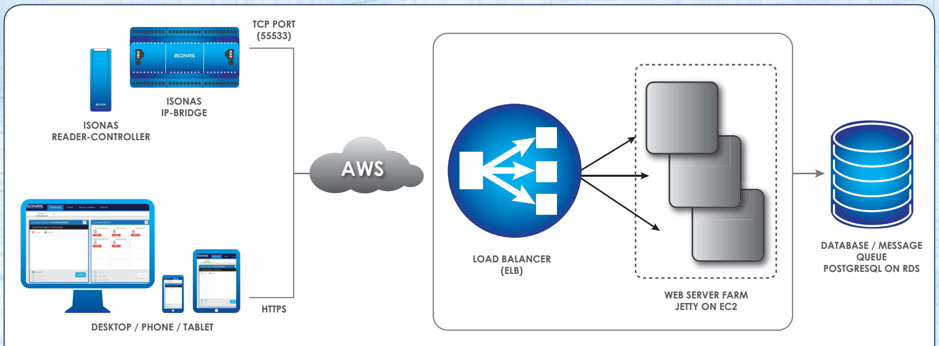
ISONAS™
PURE IP ACCESS CONTROL

# HOW DO YOU KNOW ACCESS CONTROL IN THE CLOUD IS SECURE?

## HERE ARE 9 BEST PRACTICES YOU SHOULD ENSURE YOUR CLOUD PROVIDER IS USING.

Access Control as a Service (ACaaS) has grown into a mainstream product offering from many access control manufacturers and the product offering is gaining significant growth in the market. With the adoption of this technology, end users and integrators need to ask several pertinent questions. It is extremely important to understand the security of the communications, the quality of service, who the provider of the cloud service is, the redundancy of the servers, disaster recovery, scalability of the platform and finally the stability and availability of the service. With this information end users and system integrators can make a sound decision on which product to select and if the provider can be trusted to deliver the critical action of physically opening and closing doors successfully. At ISONAS, we take each of these issues very seriously and have worked tirelessly to provide the most transparent service to a customer while leading the industry in security and scalability. When selecting an Access Control as a Service provider, we recommend looking for the following best practices to ensure clarity in the decision making process.

Defense in depth is important.



ISONAS PURE ACCESS CLOUD INFRASTRUCTURE

### 1. OVERALL STRUCTURE

Where is the platform hosted? Amazon Web Services has created a business solely around hosting services. ISONAS Pure Access Cloud is hosted on a complex structure within Amazon Web Services. We chose AWS because of their best in class cyber security infrastructure and their extensive global flexibility in hosting and deployment of Pure Access.

### 2. PERIMETER SECURITY

Does the platform have perimeter security?  Typical first line of defense is through the firewall that can deny or allow traffic. Networks should be surrounded by firewalls and reverse proxy units which protect the systems within. Intrusion detection and prevention measures should be set up to alert and mitigate potential risks before they can get into the network. All perimeter security logs should be reviewed daily as well as alerting on key terms for a rapid response to threats. At ISONAS, we measure and monitor 430 individual metrics 24/7 with real time alerting to our technical team and we use an industry leading service to provide this comprehensive level of IT infrastructure monitoring.

### 3. INTERNAL SECURITY

How the cloud provider manages their internal systems is a good reflection on how they manage additional systems and will prevent another avenue for an attack. Systems should be under a Network Access Control Layer as well as local firewalls limiting only the required ports for operation to be active and only responsive to specified networks. As a second layer of protection, Host Intrusion Detection and Prevention act as a threat reduction as well as Antivirus and Malware mitigation. Internal team access to systems should be group based and only granted on an as needed basis via a secure password manager portal where access can be granted and revoked at any time.

### 4. ENCRYPTION

One of the most basic pieces of security is ensuring the web application has an SSL (Secure Sockets Layer). An SSL establishes an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private. Pure Access Cloud utilizes SSL encryption governed by the reverse proxy. Even the passwords used by the web servers to access the database are encrypted to mitigate against data leakage. Automated file watchers keep a close eye on configuration details in the servers to ensure no access is granted without administration approval. All information on ISONAS hardware is encrypted using AES-256 bit algorithms. Communication between Pure Access Cloud and each connected access point can also be AES 256 bit encrypted.

### 5. DATA PROTECTION

The worst time to find out backups didn't work is when you need them the most so employing backups and snap shots of the database is vital. This will ensure that data cannot be lost due to failure or even accidental deletion. All recovery methods should also be tested on a regular basis to ensure that restore and recovery is fast and accurate if required.

### 6. TESTING

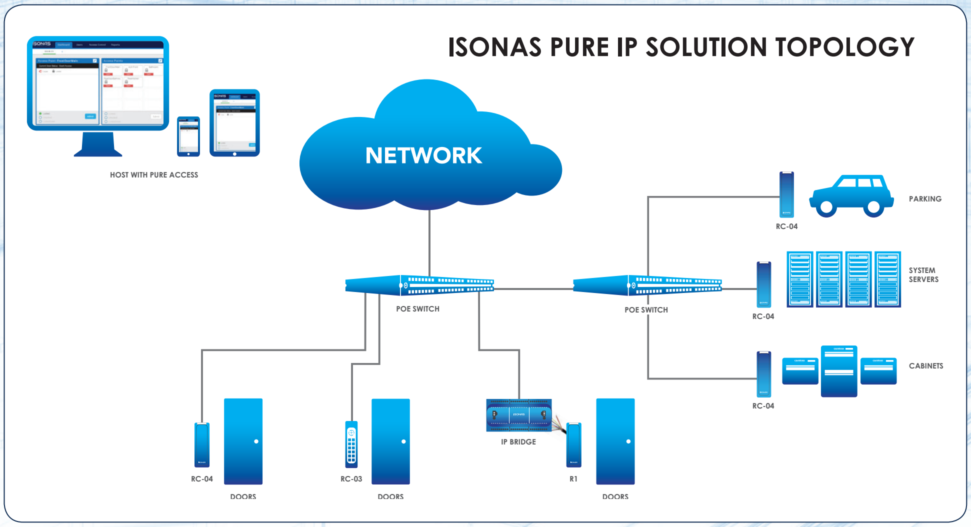
All products should undergo thorough and rigorous automated and manual testing to ensure that the product that is placed in front of customers is stable without issue. ISONAS utilizes 3rd party Penetration Testing on a regular basis to subject our systems and configurations to the highest level of cyber security standards.

### 7. MONITORING

All systems should be monitored heavily. A best practice here at ISONAS is that each server has up to 30 points monitored from services to configuration files to up/down time. Ports are monitored as well as web services. Our services are monitored by Selenium style scripts that not only see if the web services are up but actually log in and click links and log out measuring the performance of the services. These checks are done every 5 minutes from locations in the US and internationally as well as internal network monitors.

### 8. REDUNDANCY AND LOAD BALANCING

As systems scale and grow, there is risk that traffic to the platform could create performance issues, therefore the ability to load balance information is critical to preventing an overload. Systems should be redundantly load balanced using affinity in the virtual IP configuration to ensure a seamless customer experience. In addition, applications should be stateless and share cache information so if a system stops responding the customer will not be affected and it can be repaired without downtime being a factor.


ISONAS PURE IP SOLUTION TOPOLOGY

### 9. SUPPORT PHILOSOPHY

Is there a support program and team in place to assist if there are issues? Here at ISONAS we don't believe in traditional tech departments where there are separate network, server, security, cloud and support teams. We fundamentally believe that a rapidly scaling business and application needs a team that can manage all systems, anytime and anywhere. Our team is empowered and trained to handle all facets of the support process from the customer to SaaS application.

### About ISONAS:

At ISONAS, security is taken seriously. The patented Pure IP hardware products from ISONAS offer a technologically advanced solution that eliminates the panel in access control. Their platform requires the Pure IP RC-04 reader-controller and a category 5 cable to drive data and power to the edge and open and close doors. The combination of their revolutionary hardware and world class software application, Pure Access Cloud, provide customers the ability to scale rapidly and secure their building for less. With the industry leading cloud application and Pure IP hardware along with their technical expertise in SaaS deployment, they have created a product and infrastructure that is extremely easy to use, administer, and manage from any device in any location in the world. When combined with the security, availability, testing, monitoring, redundancy and support there is simply no better choice in the market.