icon cloud solutions

ICON CLOUD DATA CENTER COMPLIANCE AND CONTINUITY

Document Version: ICSCO Feb. 2024

TABLE OF CONTENTS

1. Service Overview

This document outlines the ICON Cloud Solutions redundancy and failover provisions as well as security measures ensuring operation and uptime. ICON Cloud Solutions has taken a great deal of care in the design of this hosted solution as well as the provisioning of each individual deployment to ensure its run-time operation and business continuity.

1.1 ICON Cloud Solutions Background

ICON Cloud Solutions, LLC (ICON) specializes in providing and deploying hosted voice, unified communications and collaboration, and monitoring and alerting solutions in the cloud. With extensive experience designing and developing voice, messaging, video and mobility technology, we offer flexible solutions for businesses looking to make the move to the cloud.

ICON has over 35 years of experience in the communications industry as a manufacturer, embedded code developer and distributor of communication technologies. Our engineering staff consists of SIP engineers, embedded code engineers, software and Windows based application engineers and advanced LAN/WAN network engineers.

A private hosted phone system instance with a dedicated virtual CPU is deployed in ICON's data center for each customer. This private solution provides security and flexibility enabling each customer to have a customizable deployment. This deployment may include multi-site applications and the support of non-VoIP devices such as analog and digital telephones through integrated IP Media Gateways.

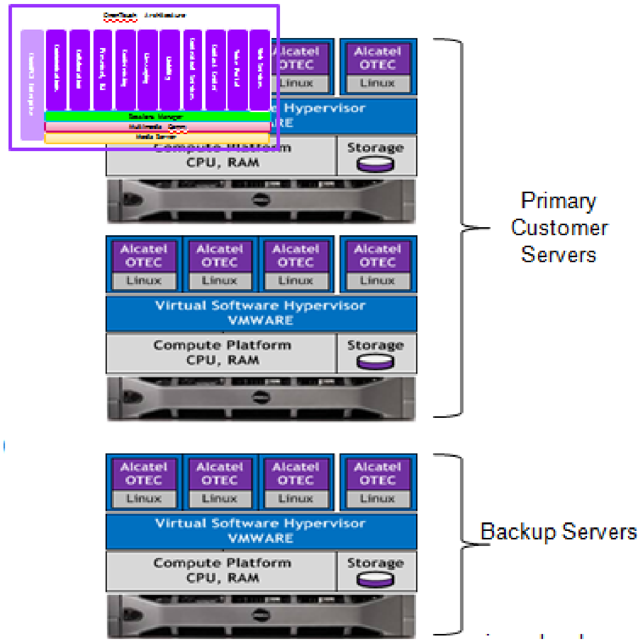


Figure 1 Dedicated Customer Instance

Each dedicated instance is also supported by a redundant back-up server. Additionally, the hosted solution may be configured with an on-premises IP media gateway. The IP media gateway supports multiple local interfaces for connection to paging devices, analog and digital telephones (Alcatel platforms only) and a diverse array of local trunks from POTS to digital PRI's.

Certain of our hosted systems may also be economically configured with a redundant server/appliance that provides local telephony survivability. Should a location lose its Internet connectivity, the redundant on-site server/appliance will take over the call control and allow the system to operate on local services.

2. Data Center – Compliance and Continuity

2.1 Data Bank Holdings

ICON hosts its services in data centers operated by DataBank, www.databank.com, with our primary facility at 400 South Akard Street, Dallas TX. ICON operates and manages our own dedicated co-location suite within these facilities.

DataBank employs on-site, dedicated security staff to manage surveillance and monitor all secure areas, parking and the building perimeter. DataBank strictly adheres to a rigorous set of controls and processes throughout the data center footprint.

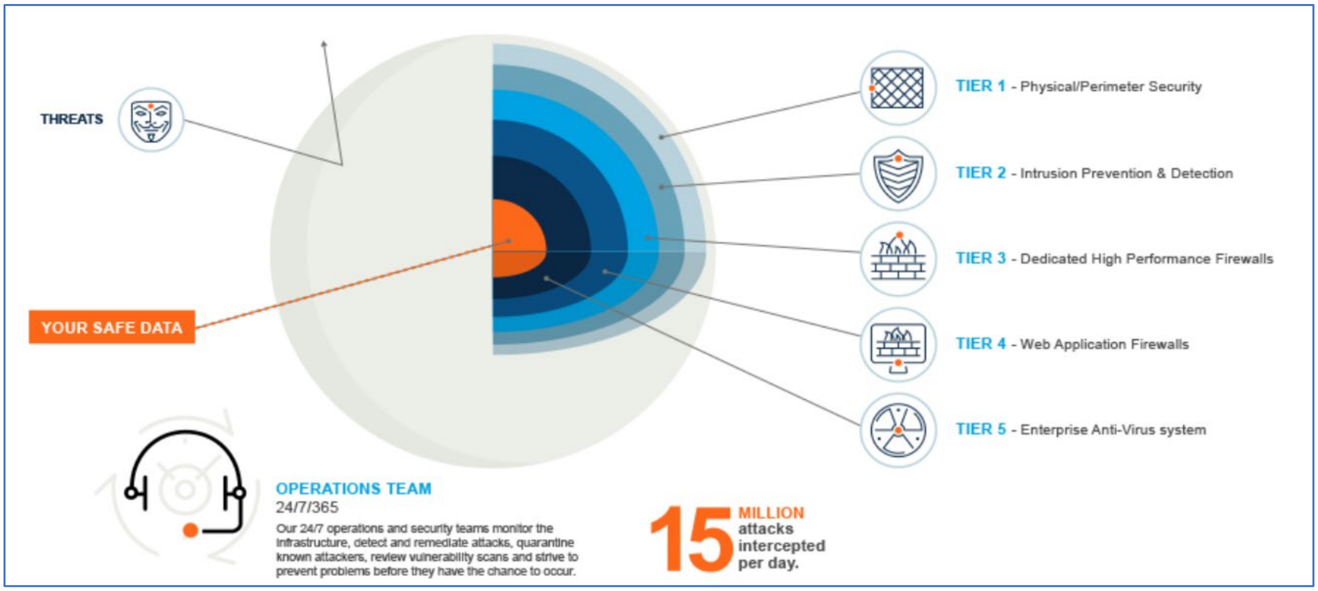
Every data center is managed, maintained and certified in SSAE-18 audits, performed annually at all sites.

2.2 Power Redundancy and Configuration

The solution is powered by a 100% uptime 2N (A+B) power configuration. This configuration provides separate redundant power grids serving each shelf within our suite. The configuration is further supported by on-site back-up power facilities.

2.3 Security

Each data center, as well as its critical infrastructure is protected with multiple layers of security. A five-tier model is utilized to negate both physical and cyber threats.


THREATS
YOUR SAFE DATA
TIER 1 - Physical/Perimeter Security
TIER 2 - Intrusion Prevention & Detection
TIER 3 - Dedicated High Performance Firewalls
TIER 4 - Web Application Firewalls
TIER 5 - Enterprise Anti-Virus system
OPERATIONS TEAM
24/7/365
15 MILLION attacks intercepted per day.

Our 24/7 operations and security teams monitor the infrastructure, detect and remediate attacks, quarantine known attackers, review vulnerability scans and strive to prevent problems before they have the chance to occur.

Figure 5 Data Center Security Tiers

TIER 1 – PHYSICAL/PERIMETER SECURITY

Data centers with guards, cameras and biometric entry prevent physical incursions.

Redundant Tier 1 Internet carriers connected to border routers and firewalls filter known threats, automated attacks, malicious traffic, DDoS filters, bogon IP addresses, bad ports and untrusted networks.

TIER 2 – INTRUSION PREVENTION & DETECTION

DataBank's IPS provides deep packet inspection in real time at multi 10 gigabit speeds blocking packets and application attacks. Rules are updated daily and include most zero-day exploits.

Machines that have launched attacks against DataBank customers or that have been associated with cyber criminals are quarantined and not permitted into the DataBank network.

TIER 3 – DEDICATED FIREWALLS/VLANS

Dedicated high-performance ASA firewalls are used to achieve complete isolation between environments.

TIER 4 – WEB APPLICATION FIREWALLS

DataBank's web application firewalls protect your data from hackers as they try to exploit weaknesses in code. Every web request is inspected for Cross Site Scripting, SQL Injection, Path Traversal and 400+ other attacks.

TIER 5 – ENTERPRISE ANTI-VIRUS SYSTEM

An enterprise-class anti-virus system uses the latest anti-virus software combined with a host intrusion prevention system and central reporting to detect and remove viruses and malware from your servers before they can ever execute.

2.4 Network Connectivity

The ICON hosted phone system network connectivity is anchored around a carrier-neutral model, and diverse multi-carrier environments. Top-tier connectivity options and architecture ensures the deployment maintains maximum connectivity. The network services provide flexible and high capacity bandwidth with transport options built to deliver 99.999% uptime.

The network connectivity is triple redundant through three independent Tier 1 internet carriers.

2.5 Security and Compliance FedRAMP

DataBank conducts regular independent security audits in accordance to industry, FedRAMP and FISMA requirements. FedRamp audit requirements include:

- Security Information and Event Management (SEIM)
- FIPS 140-2 compliant encryption
- Dual Factor Authentication
- Patch Management
- Antivirus
- Backup Services
- Network, Internal, and External Vulnerability Scanning
- Host-based Intrusion Prevention
- Intrusion Detection
- Intrusion Prevention
- Web Application Firewalls
- Log Offloading
- Configuration Scanning
- PIV/CAC Cards

2.6 SSAE 18 Compliance

The SSAE 18 is the gold standard within the industry and an integral part of DataBank's business model and security offering. Cyber security is a key strategic initiative across industries and safeguarding data is of paramount importance to our customers. This is especially the case for our clients in industries with high levels of regulatory scrutiny. SOC 2 standards are based on the proven SysTrust-derived standards of Availability, Security, Confidentiality, Privacy, and Processing Integrity.

As a provider of data center services to some of the largest publicly traded companies in the world, DataBank commits to perform a rigorous SSAE-18 audit in every one of their data center facilities. Certification includes service auditor reports on the fairness of management's description of the service organization's system controls, design, and operating effectiveness over a one-year period. Audits are conducted by an impartial independent third party. The verification agency is the American Institute of Certified Public Accountants (AICPA) which conducts the audit to assure that the control activities described in a service provider's audit are suitably designed to meet specified control objectives, and that those controls are in place and operating effectively. These reports are generally required by a variety of customers and their own auditors. Our compliance includes testing of managed services for operating systems and application level environments across control considerations, including user access, network monitoring and performance, backups, etc. This is where it's critical to communicate with all intended parties regarding the contents of such a report as expectations need to be met for comprehensive reporting.

By performing these audits proactively and delivering them to clients, DataBank saves them an enormous amount of both manpower and capital which would otherwise need to be performed by them. Performing these audit reports also allows for a de facto standard to be met in performing first-hand verification in conjunction with financial statement audits such as FISMA, FedRAMP, or Sarbanes-Oxley compliance.

3. Backhaul Performance and Geo-Redundancy

ICON provides connectivity for our customer to the Public Switched Telephone Network (PSTN) for the processing of local, long distance and international calls. ICON utilizes Tier 1 backhaul carriers to process these calls.

These carriers have highly geo-redundant networks to insure maximum uptime and processing of calls. The diagram below represents one of these redundant networks and the different data centers within it.

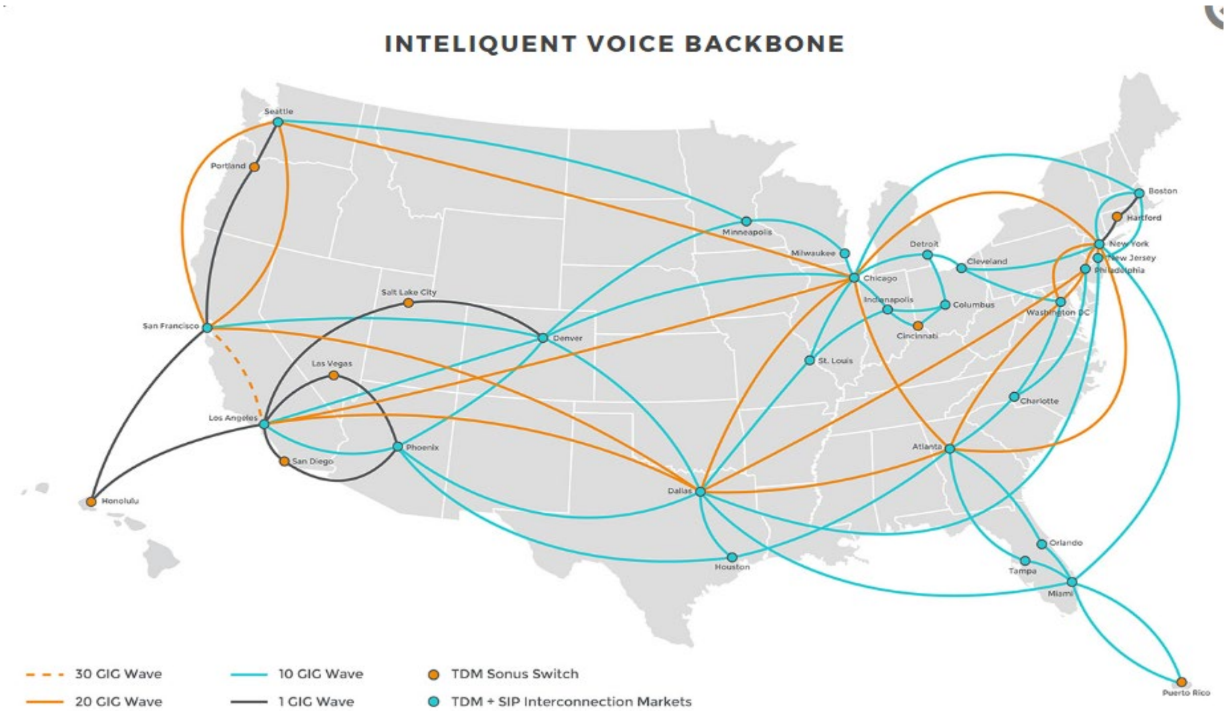


Figure 6 Geo-redundant Telephone Network

4. Service Quality

ICON is committed to providing the best communications experience from our hosted solutions. This begins with a focus on providing superior voice quality through well-designed connectivity from our host to our customer's site(s).

4.1 VPN Tunnel Configuration – Voice Quality

As an option or requirement based on the system configuration, ICON provides the services over a VPN tunnel established between our cloud host and the customer site. The benefit of a VPN is measurable in the capability of the configuration to deliver consistently superior voice quality when compared to the "open internet" connectivity provided by most hosted companies.

This quality of service is illustrated in the chart below with the ICON VPN Tunnel quality represented in purple. The measurement in this chart is what is known as a Mean Opinion Score or MOS Score which is used to measure Voice over IP quality.

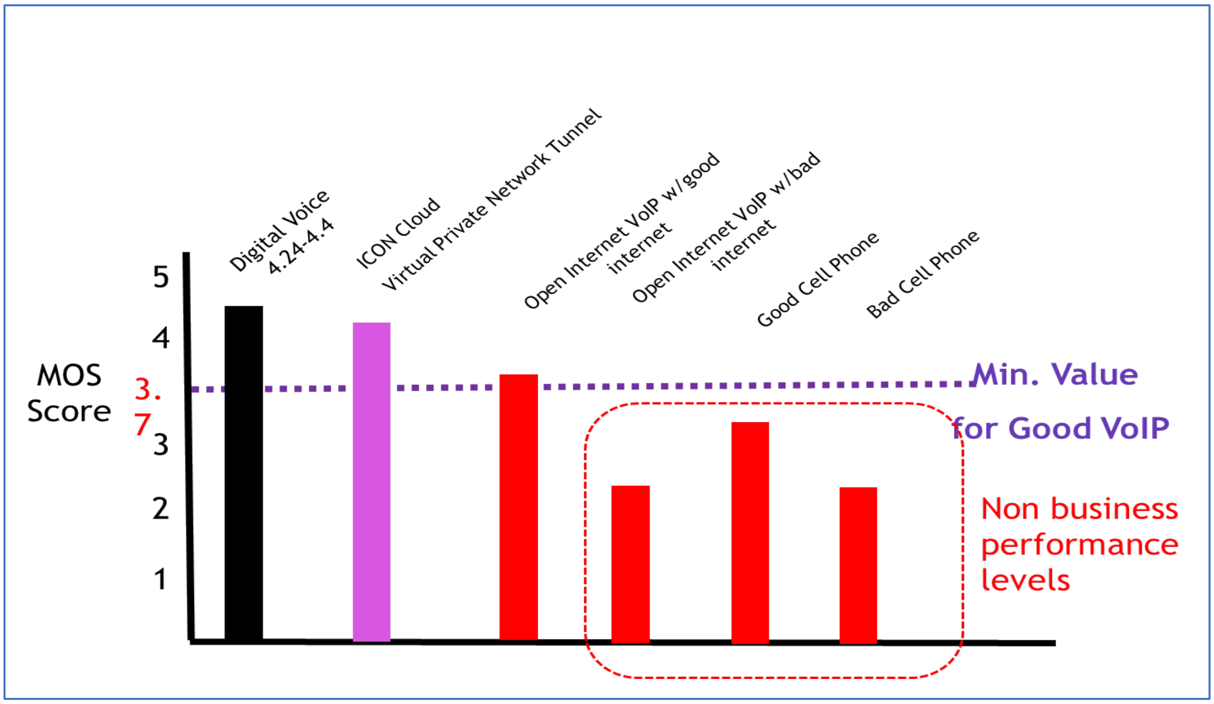


Figure 7 Voice Quality Rankings

4.2 VPN Tunnel Configuration – Minimized Bandwidth Utilization

Another significant benefit of ICON's VPN service configuration is the minimization of bandwidth required for communication. Intercom calls (station-to-station calls) on many hosted solutions actually take up twice the bandwidth of a call to an outside customer. This is because they travel up to the cloud and then back down to the other stations.

ICON's solution processes these calls as peer to peer calls over the customer network. This means the voice stays on net thus utilizing significantly less bandwidth. The diagram below is an illustration of this.

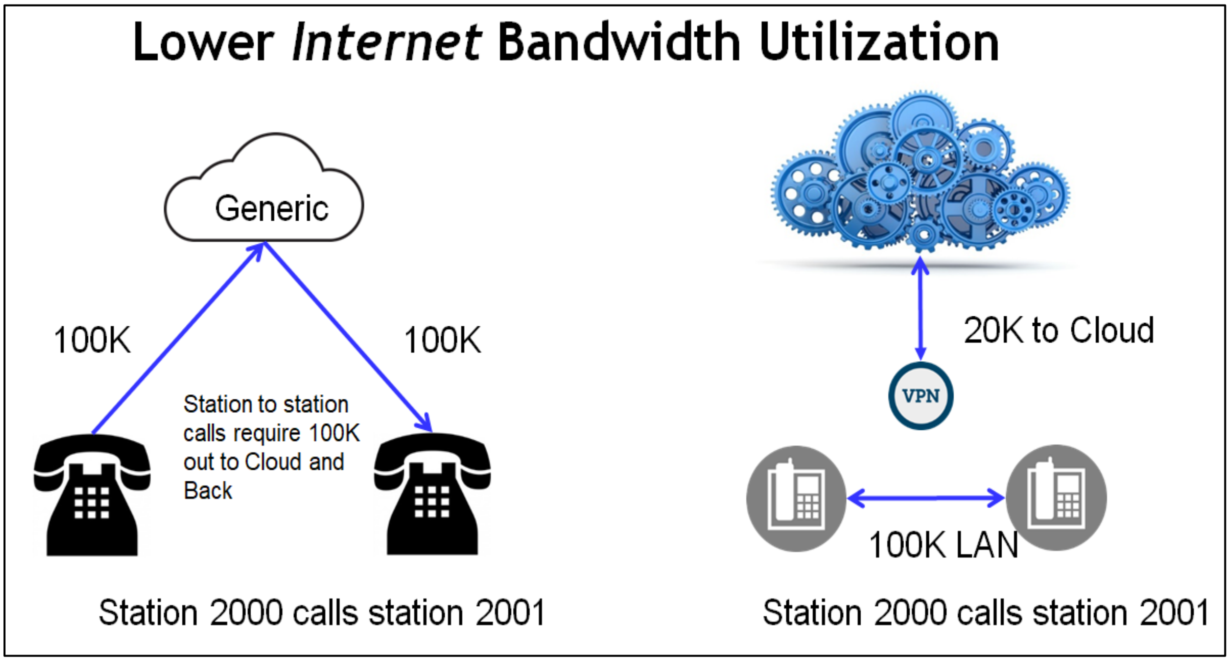
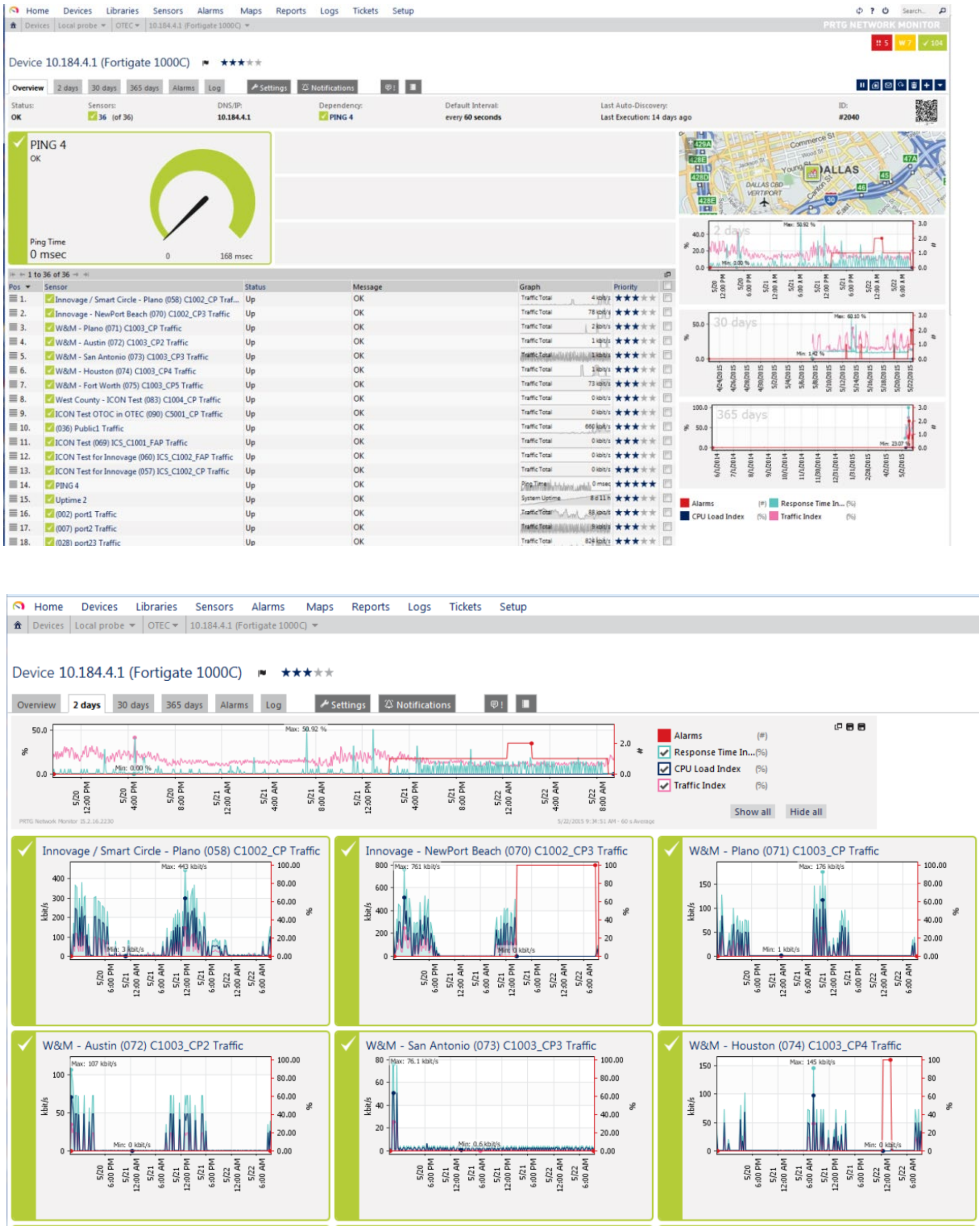

Lower *Internet* Bandwidth Utilization
Generic
100K
100K
Station to station calls require 100K out to Cloud and Back
Station 2000 calls station 2001
20K to Cloud
VPN
100K LAN
Station 2000 calls station 2001

Figure 8 Reduced Per Call Bandwidth Requirement

4.3 Service and Uptime Monitoring

ICON utilizes several different service monitoring software programs to ensure uninterrupted operation of our services. These applications provide real-time monitoring of packet transmission, QoS statistics and connectivity with our customer instances. Our support staff is immediately alerted to conditions that may negatively affect the quality of services enabling them to take immediate steps to minimize and correct the issue. The screen captures below provide a sample of the activity and information analyzed.



Home Devices Libraries Sensors Alarms Maps Reports Logs Tickets Setup
Devices | Local probe | OTEC | 10.184.4.1 (Fortigate 1000C)
PRTG NETWORK MONITOR
Overview | 2 days | 30 days | 365 days | Alarms | Log | Settings | Notifications
PING 4
OK
Ping Time
0 msec
0
168 msec
DALLAS
2 days
30 days
365 days
Alarms
Response Time In...
CPU Load Index
Traffic Index

Device 10.184.4.1 (Fortigate 1000C) ★★★☆☆

Status: OK
Sensors: 36 (of 36)
DNS/IP: 10.184.4.1
Dependency: PING 4
Default Interval: every 60 seconds
Last Auto-Discovery: Last Execution: 14 days ago
ID: #2040

1 to 36 of 36

Pos	Sensor	Status	Message	Graph	Priority
1.	Innovage / Smart Circle - Plano (058) C1002_CP Traf...	Up	OK	Traffic Total 4 kbit/s	★★★☆☆
2.	Innovage - NewPort Beach (070) C1002_CP3 Traffic	Up	OK	Traffic Total 78 kbit/s	★★★☆☆
3.	W&M - Plano (071) C1003_CP Traffic	Up	OK	Traffic Total 2 kbit/s	★★★☆☆
4.	W&M - Austin (072) C1003_CP2 Traffic	Up	OK	Traffic Total 1 kbit/s	★★★☆☆
5.	W&M - San Antonio (073) C1003_CP3 Traffic	Up	OK	Traffic Total 1 kbit/s	★★★☆☆
6.	W&M - Houston (074) C1003_CP4 Traffic	Up	OK	Traffic Total 1 kbit/s	★★★☆☆
7.	W&M - Fort Worth (075) C1003_CP5 Traffic	Up	OK	Traffic Total 73 kbit/s	★★★☆☆
8.	West County - ICON Test (083) C1004_CP Traffic	Up	OK	Traffic Total 0 kbit/s	★★★☆☆
9.	ICON Test OTOC in OTEC (090) C5001_CP Traffic	Up	OK	Traffic Total 0 kbit/s	★★★☆☆
10.	(036) Public1 Traffic	Up	OK	Traffic Total 660 kbit/s	★★★☆☆
11.	ICON Test (069) ICS_C1001_FAP Traffic	Up	OK	Traffic Total 0 kbit/s	★★★☆☆
12.	ICON Test for Innovage (060) ICS_C1002_FAP Traffic	Up	OK	Traffic Total 0 kbit/s	★★★☆☆
13.	ICON Test for Innovage (057) ICS_C1002_CP Traffic	Up	OK	Traffic Total 0 kbit/s	★★★☆☆
14.	PING 4	Up	OK	Ping Time 0 msec	★★★★★
15.	Uptime 2	Up	OK	System Uptime 8 d 11 h	★★★☆☆
16.	(002) port1 Traffic	Up	OK	Traffic Total 88 kbit/s	★★★☆☆
17.	(007) port2 Traffic	Up	OK	Traffic Total 9 kbit/s	★★★☆☆
18.	(028) port23 Traffic	Up	OK	Traffic Total 824 kbit/s	★★★☆☆

Home Devices Libraries Sensors Alarms Maps Reports Logs Tickets Setup
Devices | Local probe | OTEC | 10.184.4.1 (Fortigate 1000C)
Overview | 2 days | 30 days | 365 days | Alarms | Log | Settings | Notifications
Max: 50.92 %
Min: 0.00 %
Alarms
Response Time In... (%)
CPU Load Index (%)
Traffic Index (%)
Show all
Hide all
Innovage / Smart Circle - Plano (058) C1002_CP Traffic
Innovage - NewPort Beach (070) C1002_CP3 Traffic
W&M - Plano (071) C1003_CP Traffic
W&M - Austin (072) C1003_CP2 Traffic
W&M - San Antonio (073) C1003_CP3 Traffic
W&M - Houston (074) C1003_CP4 Traffic
kbit/s
%

Device 10.184.4.1 (Fortigate 1000C) ★★★☆☆

Figure 9 Service and Uptime Monitoring

5. Disaster Recovery Plan

ICON has established a comprehensive Disaster Recovery Plan in the event of service disruptions. This Distaster Recovery Plan is an internal document for obvious security reasons.

However, highlighted below are some high level details of the processces included within this plan.

5.1 Policy Statement

It is ICON Cloud Solution's policy to maintain a comprehesive Business Continuity Plan for the operations of its cloud services. This plan incorporates the architectural design elements of our cloud services, the operational business processes and policies in place to ensure continued service operation and expedited recovery measures in the event of an unscheduled interuption.

5.2 Recovery Objectives

The recovery objectives of the ICON Cloud solution dictate the following:

Redundant Operations – That we have auto-redundancies for each communication layer at the core data center tier. This includes software, application layer, hardware, and external connectivity layer redundancies.

Advanced Solution Monitoring – Advanced diagnostic and traffic software is utilized that provides real time data, measurement and alerts of system continuity. This includes:

- Application Monitoring Software
- Data core to customer Site connectivity

Emergency Response – 24/7 availability of technical assistance to support cloud services to ensure operation.

5.3 Recovery Strategy

The primary objective of our recovery strategy is to provide operational redundancy of the solution at the core (data centers) with multiple connectivity options to carrier access and to customer premises connectivity.

5.3.1. Dedicated Customer Instance

The ICON Cloud hosted communications software is operated as an individualized, virtual CPU dedicated to each customer. A primary instance for the customer is established as the Primary Data Center instance and provides all of the communications and features of the solution offering.

A redundant instance (customer specific virtual CPU) is also provided as the secondary data center instance. This redundant instance operates on a totally separate server architecture. In the event of disruption of the primary data center instance the secondary data center instance takes over.

5.3.2. Redundant Hardware and Application

Although the hosted communication software is the main communication platform, there are several other applications that operate in conjunction with the software to fully deliver and enable operability. Specifically, a session boarder controller and reverse proxy enable the proper routing of communication packets and the connectivity to mobile devices.

All of these application servers are duplicated within the secondary data center instance.

5.3.3. Power Redundancy

As detailed within Section 2 all ICON's equipment is served by an 2N(A+B) grid redundant power source. This ensures if there is a disruption within one of the geographic power grids our equipment would continue operating. This design provides a 100% uptime configuration.

5.3.4. Internet Connectivity

The connectivity between the ICON Cloud hosted service and the customer site may travel via a VPN IPsec tunnel connection over the internet or via dedicated MPLS connection.

In the case of the VPN IPSec connection, ICON's connection to the internet provides triple redundant access through three distinctly different providers. In the event the primary provider encounters a service disruption, connectivity will quickly shift to the alternative providers.

Statistically, over 90% of ICON's customer connections are provided via VPN IPSec tunnels. This vehicle of connectivity has proven to be very reliable due to the quality characteristics as previously mentioned gained from this VPN tunnel configuration.

MPLS circuits may also be provided for connectivity to customer sites. Common configurations for large customers may include an MPLS connection with a back-up VPN

IPsec tunnel. In the event of MPLS interruption the VoIP packets will then be routed over the VPN tunnel.

5.3.5. Backhaul Network Redundancy PSTN

All outbound telephones calls from our customers are processes through Tier 1 carriers with highly redundant networks. This includes local, long distant and international calls. Section 3 provides a map of the various points of presence (POP's) whereby the carriers redundant services are located.

In the event of an outage on a specific link or data center calls are automatically routed to the secondary routes.

5.4 Host Configuration

The diagram below represents the redundant infrastructure of our OTEC hosted service.

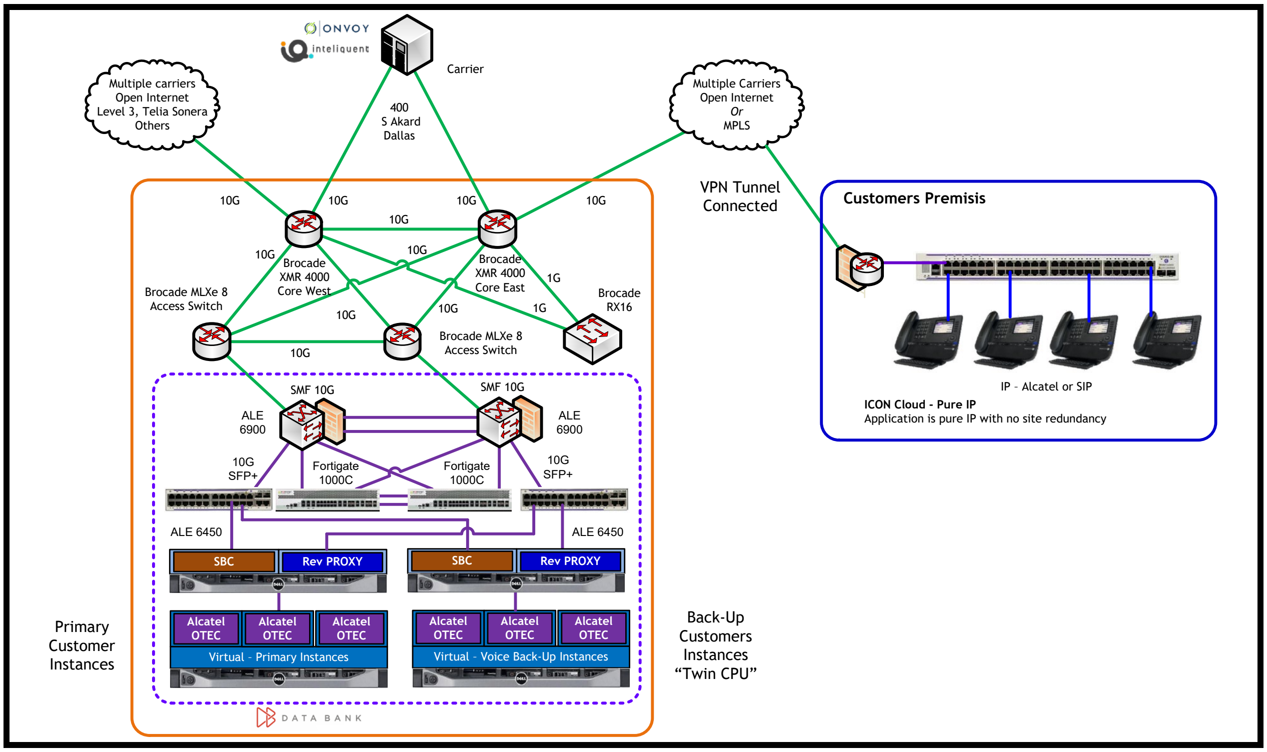


Figure 10 ICON OTEC Redundant Infrastructure