ION Networks
120 Corporate Blvd
South Plainfield, NJ 07080
Phone: +1 908.546.3900
Email: IONsales@apitech.com
www.apitech.com

api technologies corp.

ION Solutions

The Challenge...

*You depend on **3rd party service providers** to ensure your mission critical system's availability and sustainability. To meet your requirements, the provider requires always-on access, for 24/7 monitoring, periodic maintenance, patches/system updates, & emergency access when trouble occurs...*

You need to get the most from your service providers… and they need secure access.

*Universal access via the Internet gives your service provider the best means to quickly delivery reliable services...Sounds great, but what about hackers trolling the Internet looking for opportunities? You need to ensure your service provider's access is secure from both internal and external threats. Your service provider is trusted, but the provider still needs to be verified and monitored. Balancing service provider access without compromising security… **this is the ION Solution.** You depend on **3rd party service providers** to ensure your mission critical system's availability… **this is the ION Solution.***

What Threatens Traditional VPN Access?

1. Internal misbehavior… whether by accident, negligence, or design, people inside your system can cause damage.
2. External attackers… People and/or bots breaking into your system to steal information or leave viruses when security solution implemented poorly or weak passwords are used.
3. Real time visibility in what is going on in your network… now and after problem resolution.

How Service Providers Utilizing ION Provide Solutions for You...

1. Accessing your system to fix issues and provide upgrades, no truck roll required. Multiple access platforms including in- and out-of-band.
2. Providing you with the ability to lock anyone out at any time, both internal personnel and external technicians.
3. Providing you with the ability to observe all activity through recorded sessions and live streaming of activity.
4. Three-strike access auto-lock out for dial-up access.

The Solution

ION Networks is the most trusted name in remote device management and secure access technology for defense and commercial applications. The ION solution enables service providers, equipment manufacturers, government and military agencies, and corporations to remotely manage, monitor, and secure critical voice and data networks.

This ensures the "privileged" system administrator can access systems without compromising security. Only trusted users can access these systems. This requires a comprehensive solution that secures all privileged user connections, whether the user is an employee, an equipment manufacturer, or 3rd party consultant/service provider.

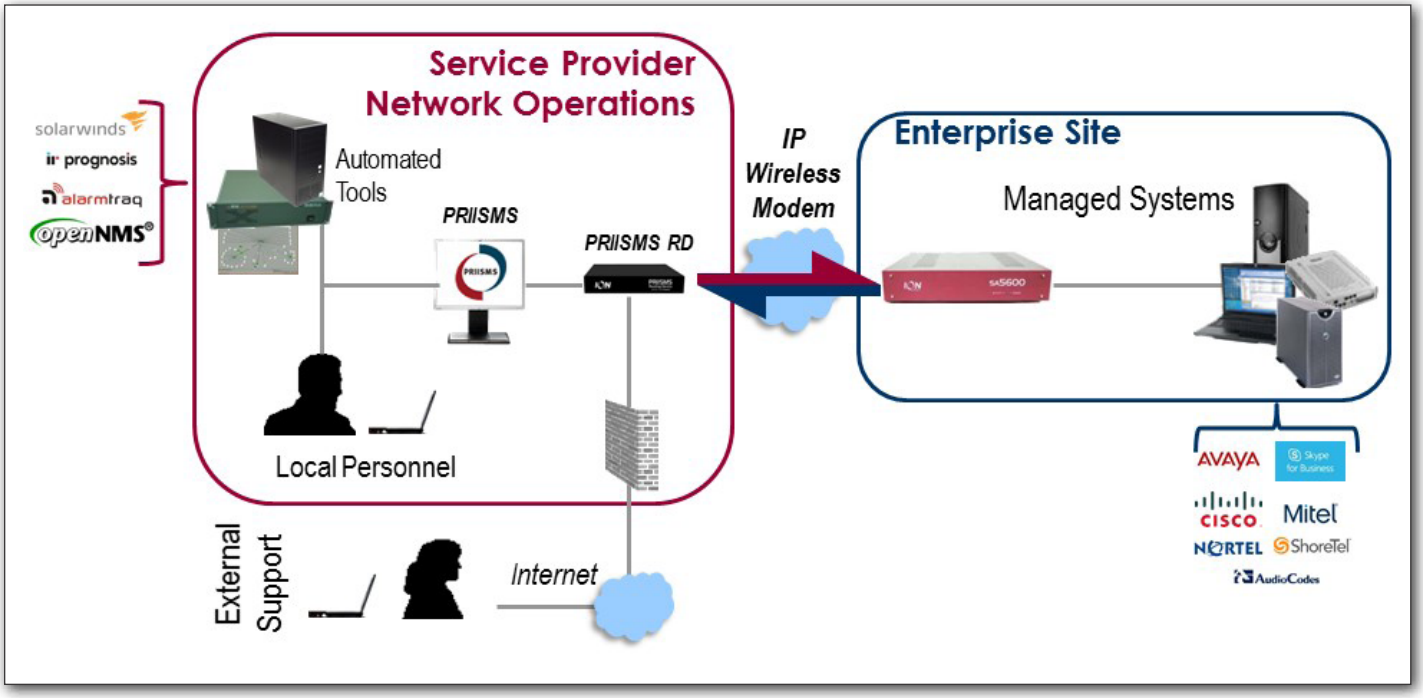
…You need a solution that is flexible to handle any type of connection or application needed to manage a device.

Service providers with ION solutions provide end-users the ability to grant third party and internal users access for remote management of voice and data systems. By not keeping you waiting for a service provider to come on location to resolve issues, they are minimizing your downtime. The provider can also offer increased security measures by recording system activity and protecting against hacker threats to sensitive information with auto-lockout modem functionality.

Products Overview

The ION solution is comprised of an access gateway called PRIISMS and multi-function security appliances that enable local security and connectivity to remote devices.

We have made significant investments into FIPS and Common Criteria certification to ensure the security foundation of our solution has been vetted by a third party testing organization. Additionally, ION Networks regularly updates software based on newly discovered vulnerabilities and keeps up to date with updates to Open Source components. ION Networks can be trusted.



What is PRIISMS…

ION PRIISMS (Proactive Remote Integrated Intelligent Secure Management Solution) is a secure web-based gateway application that provides centralized control over security and administrative access policies of distributed and complex network device environments. Service providers/network administrators can configure, troubleshoot, and manage consolidated or geographically dispersed critical network devices, in- or out-of-band, remotely or from a central Network Operations Center (NOC). The PRIISMS architecture provides a scalable solution ensuring the highest of availability for an unlimited number of connections.

PRIISMS is a simple to use platform that provides a robust set of security features ensuring only trusted users can access the management interfaces of mission critical systems. In addition, PRIISMS provides the most comprehensive set of audit capabilities documenting what device(s) a privileged user accessed, and what changes they made with recorded sessions. PRIISMS provides the ability to control who can get access to specific devices and confidence with transparent knowledge of what was done be it device access via SSH, Web, RDP, or a propriety client.

ION™ PRIISMS

- Single-sign-on technician access for remote endpoint management
- M2M automatic connectivity
- ION devices central manager
- Software, virtual machine or hardware appliance

Products Overview

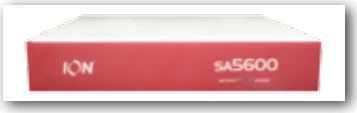
The appliances… ION has a range of hardware and virtual machine (VM) security appliances to meet the unique needs of both VoIP and IT deployments. Secure appliances provide flexible and adaptable connectivity solutions via diverse networks or physical connectivity to devices through console ports or networks such as the PSTN, Cellular, or broad band networks. Utilizing the ION VM security appliance enables secure remote access to systems in cloud network environments.

ION™ Secure Virtual Machine

- Eliminates the cost of physical appliances
- Ensures privileged administrators access only permitted Cloud based systems utilizing VPN tunneling technology
- Cost-effective and scalable solution for small and large deployments
- Compatible with VMware, ESXI Server and Microsoft Hypervisor

ION™ SA5600 Secure Appliance

- High-performance, Enterprise-secure appliance
- Easy connectivity, highly scalable solution
- Modem, Internet, or wireless connectivity device



ION™ SA5610-SAL Avaya SAL Edition

- Plug-and-play SAL Gateway appliance
- Installs in under 10 minutes*
- Complete SAL Gateway installation without the headache of building from scratch
- Supports SAL Gateway and SLAMON

ION™ SA600 Service Access Point

- Console terminal server, modem and wireless
- Ideal solution for legacy PBX monitoring and access

ION™ SA500 Service Access Point

- Ideal device for SME deployments for IP Office, BCM, or Suretel
- Low cost Internet service delivery platform

ION™ SA5600-IA2 DoD/Gov Edition

- JITC/IA approved
- Dial-up, IP and console access
- Built-in two factor authentication
- Encrypted link
- CAC/PIV/SIPR card authentication

JITC/IA Certified

ION™ SM110 Secure Modem

- Eliminate weak passwords securing critical network elements
- Ideal for mission critical router console for OOB access

Appliance Overview	Secure VM	SA500	SA600	SA5600	SA5600-SAL
Internet	√	√	√	√	√
Out of band	X	X	Modem/Cellular	Modem	Modem
Console Server (Router/ PBX)	X	X	√	√	√
IP Endpoints	6-400+	6-24	6-24	64-400	64-400
	SME/Enterprise	*SME*	*SME*	*Enterprise*	*Enterprise (AVAYA)*

1. HOW IS THE CONNECTION SECURE?

With proven encryption backed by FIPS and Common Criteria Certifications

Services SSL VPN™ Simplifies Connectivity by Harnessing HTTPS to Easily Traverse Complex Enterprise Networks:

There is no need to reconfigure firewalls or navigate through complex IT environments because the Services SSL VPN™ uses standard HTTPS ports to initiate a secure tunnel between the enterprise customer and service provider As soon as the ION appliance (hardware of virtual machine) is placed on the customer site, it automatically establishes a connection from inside the network to the service provider's Network Operations Center (NOC). The customer sees and treats the connection just as it would an employee browsing the Internet. This makes it easy for service providers to connect to customer premise equipment using a variety of connectivity methods, including (but not limited to): broadband (ADSL/DSL/Cable modems) or leverage existing customer's Internet connectivity.

Bi-Directional Connectivity via the Internet Enables Delivery of Revenue-Generating, Proactive Managed Services:

Services SSL VPN™ is the first of its kind to create bi-directional, encrypted tunnels, which originate within the customer's network. This means service providers can have always-on, Internet connectivity to customer devices, enabling the delivery of key site data (for example, alarms and traps) in real time. As a result, the service provider can consistently monitor equipment and conduct proactive maintenance. This is a service option previously unavailable with traditional SSL VPN connectivity. Customers benefit from higher service levels, while service providers benefit from the additional, revenue-generating service options they can deliver.

Encryption Details

- OpenVPN tunnel
  - Government strength encryption - AES 128 CBC Minimum
  - TLS 1.2
- ION or user supplied PKI certificates
  - ION Supplied certificates: 2048 bit, SHA512, RSA
- ION Services SSLVPN is very secure and easy to setup. Like browsing to a secure website using port 443.
- Unlike your typical IPSec or SSLVPN tunnel the ION solution provides the enterprise customer with greater visibility and control over their services providers access (see below)

FAQS

2. HOW ARE ONLY AUTHORIZED PEOPLE ALLOWED TO ACCESS THE EQUIPMENT?

With Strong Two-Factor Authentication

- All traffic to protected devices traverses the appliance or VM adjacent to the device. Only authenticated, authorized users will have the ability to communicate with the device.
- The solution provides two factor authentication at PRIISMS solution and the appliance.
- The solution is role based for controlling user access to specific devices.

Figure 1. Secure connection using ION's two factor authentication.

3. HOW DO WE KNOW WHAT EQUIPMENT CAN BE ACCESSED?

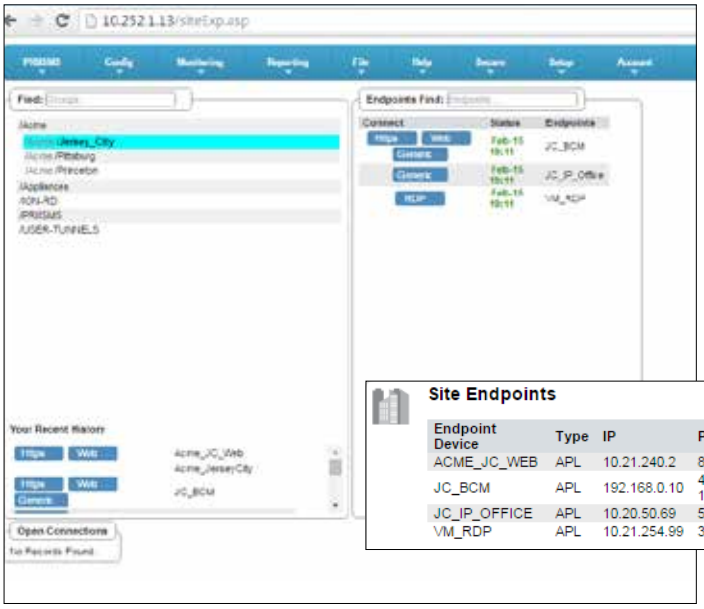


Figure 2. Unlocked screen

ION End-Point Table Controls Access

- The secure appliance is a gateway device located at the customer premises and is under the control of client. The client works with the service provider to define the equipment set (referred to as the endpoint table).
- The equipment set can be frozen by the end user by restricting the service provider role in the appliance. Access to the equipment is strictly defined in the appliance and is enforced by access to the appliance as well as IPTables rules. The IPTable rules are abstracted into the appliance as the endpoint table.

Site Endpoints

Endpoint Device	Type	IP	Port
ACME_JC_WEB	APL	10.21.240.2	8080
JC_BCM	APL	192.168.0.10	443,22,443,59000,5989 6000,8000,1:65000,22,80 443,59000,5989,6000,8000 1:65000,80 161:163,8000,161:163,8000
JC_IP_OFFICE	APL	10.20.50.69	50794,50802:50814,69 161:162
VM_RDP	APL	10.21.254.99	3389

Figure 3. Service Provider accessible point.

4. HOW CAN WE CONTROL WHEN OUR SERVICE PROVIDER IS ALLOWED TO ACCESS OUR EQUIPMENT BUT NOT AFFECT THEIR ABILITY TO MONITOR OUR DEVICES?

Endpoints Find: Endpoints...

Connect	Status	Endpoints in Group: /ABC Corp/ABC Chicago
Connect	Dec-29 11:04	ABC Chicago
	Dec-29 11:04	ABCChicagoWeb
	Dec-29 11:04	Avaya IP Office
	Dec-29 11:04	BCM Chicago
	Dec-29 11:04	RDP-VM

Figure 4. Locks clearly indicate to the service provider that access is blocked, eliminating the guess work determining if access is down or restricted.

End-Point Locking - The ION Solution Allows You To Enable and Disable Service Provider Access

- The access to equipment is restricted in the appliance to the equipment defined in the endpoint table. A further restriction is possible with a feature called endpoint locking. If enabled, endpoint locking will block and notify the service provider, without removing the equipment definition. Even though endpoint locking is enabled, the equipment will still be able to send out data (i.e. SNMP traps).

5. HOW CAN WE PROVIDE AN AUDIT OF OUR SERVICE PROVIDERS' ACCESS?

In The Appliance System Log

- The ION appliance logs are tamper-proof (read only) tracking all user's access and activities; who, date, time, duration, successful or unsuccessful.
- These events can be sent to a Security Operation Center (SOC) system (syslog or SNMP).

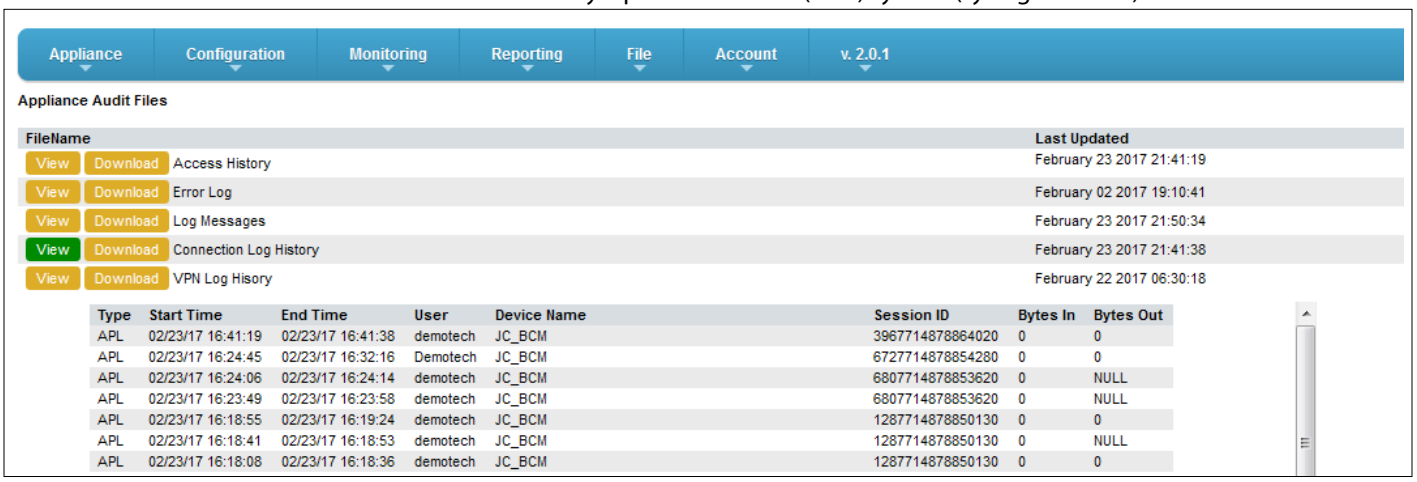


Figure 5. Automated notification email.

6. HOW DO I KNOW THEY ARE ON MY EQUIPMENT?

Automated Notification and Real-Time Monitoring

- The appliance maintains a rich set of alarms. This includes connections and disconnections, logins, etc. It has a capability to dispatch notifications on any or all of these events. Notification can be delivered via email, SNMP or Syslog message. The appliance web page shows all current and historical connections and data usage.

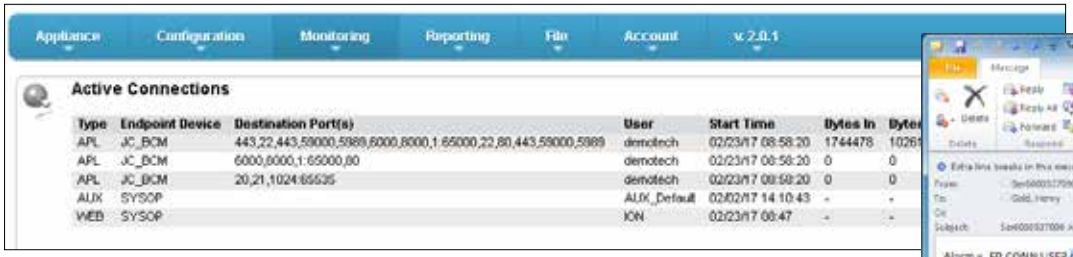
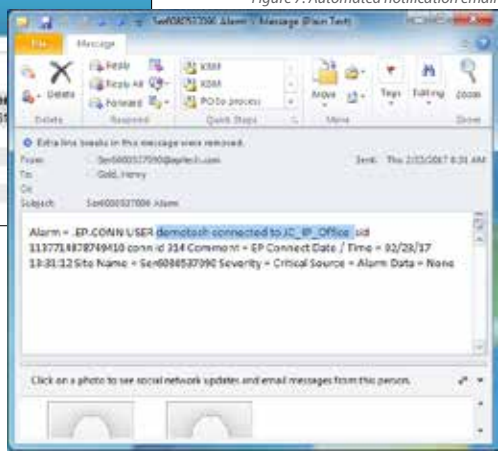


Figure 6. Active Connections

Figure 7. Automated notification email



7. HOW DO I KNOW WHAT THEY DID?

GUI Session Recording

- If your service provider has the PRIISMS+ module, a recording of the technician's session was captured and stored at the service provider. There is an ICON in the connection log indicating that the session was recorded and a request can be sent to download a copy of the recording.
- Recorded sessions capture every system change for root cause analysis or security forensics.

ION Networks
120 Corporate Blvd
South Plainfield, NJ 07080
Phone: +1 908.546.3900
Email: IONsales@apitech.com
www.apitech.com

api technologies corp. *ION Networks is a part of API Technologies Corporation.*