"How do I secure and manage an out-of-band connection to network devices?"

Challenge

Due to security concerns, many companies no longer allow dial-up connectivity to their voice and data networks. However, when IP connectivity is unavailable, dial-up is the only means to offer remote, administrative support. This presents a quandary for service providers / remote administrators that require out-of-band access to troubleshoot equipment and maintain service levels.

ION offers a solution that enables emergency, out-of-band connectivity, while meeting companies' strict security requirements.

Key Solution Benefits

ION recommends a solution that balances a service provider's need for access with an enterprise's need for high system availability and security. With ION's technology, service providers can:

- **Meet enterprise security policies** by offering a solution that complies with customer requirements, as well as security regulations (for example, FDIC and PCI) and legislation (for example, GLBA, HIPAA, and SOX).
- **Deliver consistently high service levels** by quickly restoring connectivity and/or diagnosing and correcting equipment problems.
- **Easily enable out-of-band connectivity**, as a single ION appliance connects service providers to all types of endpoint devices (for example, routers and servers).
- **Offer audit capabilities for enterprise customers** through ION's built-in reporting features that details: who logged in, where they went, and what they did.

"How do I secure and manage an out-of-band connection to network devices?"
www.ion-networks.com
Page 1 of 9

- **Remotely reboot devices**, which eliminates the need for a technician's onsite visit, reducing both downtime and truck rolls. However, to eliminate potential risks that could come with this type of functionality, ION adds layers of security to protect against unauthorized reboots.
- **Offer two-factor authentication and encryption**, a frequent requirement to meet government and industry standards.
- **Quick set up** of customer premise-based ION appliances, through easy, wizard-driven installation**.**
- **Manage thousands of customer sites worldwide**, each with highly varying security and connectivity requirements, using a single, highly scalable platform.

"How do I secure and manage an out-of-band connection to network devices?"
www.ion-networks.com
Page 2 of 9

Key Solution Elements

Required

Administrative Access Point

ION SA5600 – Secure Site Appliance
The ION SA5600 is an administrative Site Appliance used by service providers and owners of distributed networks for both in-band and out-of-band access to a variety of devices.

OR

ION SM110 – Secure Modem
The ION SM110 is an administrative access point used by service providers and owners of distributed networks for emergency out-of-band access to a single device.

Tokens

ION ST520 – Soft Token
ION's single-use, free tokens with multi-factor authentication eliminate the use of passwords, which can be easily compromised. The ION Soft Token solution supports several methods of authentication, including password, pager, and ION 520 authentication. The ION's ST520 employs strong two-factor triple-DES challenge/response authentication and is compatible with Windows® platforms, RIM® Blackberry devices, and Palm® OS PDAs.
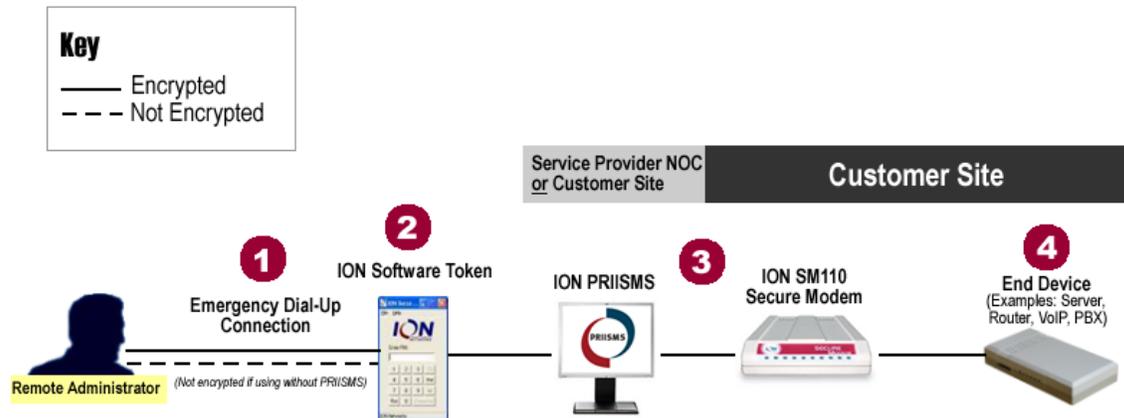
Highly Recommended

Management Software

ION PRIISMS - Secure Administrative Gateway
ION PRIISMS is a secure web-based application that provides centralized control over the 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-band or out-of-band, remotely or from a central Network Operations Center (NOC).

"How do I secure and manage an out-of-band connection to network devices?"
www.ion-networks.com
Page 3 of 9

How it Works

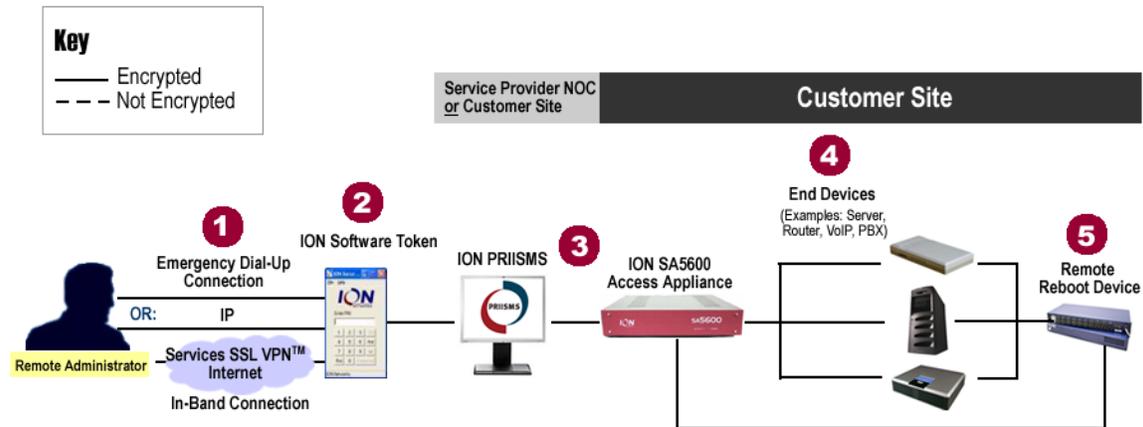## Out-of-Band Access Using ION's SM110 Secure Modem

Step 1: Remote Administrator initiates an emergency dial-up connection.

Step 2: Remote Administrator is prompted to authenticate (challenge/response) via a token, such ION's free ST520 software token or RSA Security®'s SecurID®.

Step 3: PRIISMS system directs Remote Administrator to the endpoint device. ION's SM110 Secure Modem provides access to the device. PRIISMS keeps a log of the entire session. If using SM110 Secure Modem without PRIISMS, login/logout and administrative changes are stored on the device for reporting purposes.

Step 4: Remote Administrator has administration rights to the device.

"How do I secure and manage an out-of-band connection to network devices?"
www.ion-networks.com
Page 4 of 9

Out-of-Band Access Using ION's SA5600 Site Appliance

Step 1: Remote Administrator initiates an emergency dial-up connection (out of band) or a Services SSL VPN™ or Internet connection (in band), using a Web browser or terminal application, such as Secure Shell or ProComm.

Step 2: Remote Administrator is prompted to authenticate (challenge/response) via a token, such ION's free ST520 software token or RSA Security®'s SecurID®.

Step 3: PRIISMS reviews the Remote Administrator's privileges, and then directs the Remote Administrator to appropriate device(s). ION's SA5600 Site Appliance provides access to the device(s). PRIISMS keeps a log of the entire session, which is stored in PRIISMS and on the SA5600 Site Appliance.

Step 4: Remote Administrator has administration rights to the device.

Step 5 (Optional): If needed, a reboot router connected to ION's SA5600 Site Appliance, can be used to reboot selected endpoint devices.

"How do I secure and manage an out-of-band connection to network devices?"
www.ion-networks.com
Page 5 of 9

Frequently Asked Questions

Why is dial-up access still a necessity?

Business runs on the Internet. The longer Internet access is down, the more severely business is impacted. Simply put: dial-up is the fastest way to restore Internet connectivity. Allowing a service provider remote, emergency, out-of-band access to troubleshoot and reboot systems enables the quick restoration of service levels, without having to wait hours or even days for an onsite visit from a technician.

I am a service provider with an enterprise client who sees modems as a security risk. How can I convince them otherwise?

Many clients are phasing out the use of modems. This poses a challenge for service providers, as dial-up is a necessary means to restore service when Internet connectivity is unavailable. Traditional modems can pose security risks. However, ION's SM110 Secure Modem provides unparalleled security, authentication, and audit capabilities unavailable in traditional modems. ION technology is an essential element in managed services delivery, as it enables service providers to quickly restore service levels in the event of an outage.

Why incorporate ION technology?

Maintain High Service Levels – Granting access to a service provider or remote administrator enables them to resolve issues quickly, vastly improving network uptime.

Security Compliance – ION's tools, the first to be approved by the US Department of Defense for network access security, provide a way for customers to comply with enterprise security policies, as well as security-related regulations and legislation. Two-factor authentication and embedded encryption provide unparalleled protection. Detailed reports, down to keystroke level, offer a clear audit trail for forensic analysis / auditors.

Access Control – Precisely control network access. Limit who can connect to critical voice and data systems, when they can access these assets, where they can go, and what they can do.

Scalability – For service providers: Manage thousands of customers, each with hundreds of endpoints. For the enterprise: Manage hundreds of sites and the service providers and remote administrators who require access.

"How do I secure and manage an out-of-band connection to network devices?"
www.ion-networks.com
Page 6 of 9

Mature Technology & Extensive Experience – Since 1982, ION has been the trusted name in remote administrative management and secure access technology. More than half of the world's top telecommunications firms rely on ION technology to ensure quality service for their customers. With over 50,000 devices deployed worldwide, ION's products are currently in use in over 35 countries.

Should I use the SA5600 Site Appliance or the SM110 Secure Modem?

Here are the key differences:

SA5600 Site Appliance	SM110 Secure Modem
Out-of-Band & In-Band Connectivity	Out-of-Band Connectivity
2, 4 or 8 Ports	1 Port
Full Audit Capabilities (On Device)	Limited Audit Capabilities (On Device)
Login Attempts	Login Attempts
Access Logs	Access Logs
Keystroke Logs	Keystroke Logs (with PRIISMS)
End-to-End Encryption	No Encryption

Is PRIISMS required?

PRIISMS is ION's management platform. Using PRIISMS, you can centrally manage the user profiles of hundreds of technicians on thousands of devices. Combined with the SA5600 Site Appliance / SM110 Secure Modem, PRIISMS offers enhanced management, monitoring, and auditing functionality. As such, it is highly recommended, but not required, that customers use the SA5600 Site Appliance or SM110 Secure Modem in conjunction with PRIISMS.

I currently use a server-based Authentication, Authorization and Access (AAA) solution (for example, TACACS or RADIUS). How will the inclusion of ION technology impact this?

When an outage occurs, AAA servers (RADIUS or TACACS) have no way to authenticate users. As a result, they use password-based authentication during an outage. This, an inherent security risk, conflicts with enterprise security policies. ION's embedded two-factor authentication ensures that only the people you choose can access your network during an outage. Therefore, ION technology acts as a complement to your current solution.

However, some customers have found that ION's PRIISMS combined with the SA5600 Site Appliance or SM110 Secure Modem provides a highly secure,

"How do I secure and manage an out-of-band connection to network devices?"
www.ion-networks.com
Page 7 of 9

highly scalable alternative to a AAA solution, as ION uses free, software-based tokens that are supported on a variety of end devices (for example, laptops and PDAs). For more information, speak with your ION representative or e-mail info@ion-networks.com.

What vendor devices can a technician access and manage using ION's SA5600 Site Appliance and/or the SM110 Secure Modem?

Supported devices include (but are not limited to) those manufactured by the following providers:

APC	Fujitsu	Nortel
Alcatel	HP	Oracle
Avaya	IBM	Siemens
Cisco	InRange	Sycamore
Dell	Juniper	Sun
EMC	Lucent	
Ericsson	NEC	

What's embedded challenge and response?

All of ION's devices come equipped with embedded challenge and response technology. This ensures that, in the event of network outage, two-factor authentication is not dependent on any other device and is always on. There is no reliance on weak or static passwords at any time.

Why would I want to give my service provider reboot access?

Sometimes problems are as easy to resolve as rebooting a router. The service provider does not always know who the appropriate contact is at a remote location. Also, this contact may lack the technical proficiency to locate and reboot the device in question. By allowing a service provider access and reboot capabilities, the service provider is able to resolve issues quickly and maintain high service levels.

How will the incorporation of ION technology help organizations comply with the Sarbanes-Oxley Act (SOX)?

From an information technology perspective, SOX requires organizations to ensure the security, reliability, and accuracy of the systems that manage and report financial data. This also extends to the organizations that may manage the systems that host this data, for example service providers and vendor technicians. ION technology helps give service providers the access needed to provide consistent service levels, while helping the enterprise clearly identify

"How do I secure and manage an out-of-band connection to network devices?"
www.ion-networks.com
Page 8 of 9

users (via authentication and challenge/response), enable the secure transmission of sensitive data, and provide a highly detailed audit trail.

How will the incorporation of ION technology help organizations comply with the Health Insurance Portability and Accountability Act (HIPAA)?

HIPAA requires strict monitoring and control of information assets. ION's two-factor authentication, AES encryption, and unparalleled audit and reporting capabilities help organizations comply with these requirements.

How will the incorporation of ION technology help organizations comply with Payment Card Industry (PCI) data security requirements?

ION technology helps to meet PCI's strict data security standards. ION's embedded two-factor authentication eliminates static or vendor-supplied default passwords. ION also gives the enterprise the capability to track and monitor all access to network resources and cardholder data, using PRIISMS / ION's in-depth reporting capabilities. Additionally, ION's AES encryption protects sensitive information that travels over public networks.

How will the incorporation of ION technology help organizations comply with Federal Deposit Insurance Corporation (FDIC) information technology security requirements?

The FDIC requires the encryption of sensitive information. ION's built-in AES encryption meets this requirement. Additionally, contractors (for example, service providers and outside consultants) must be audit-ready at all times. ION's detailed reporting features, down to keystroke level, allow a clear view into all maintenance activities done by a contractor on a customer's behalf.

About ION Networks, Inc.

ION Networks, Inc. (OTCBB: IONN.OB) is the most trusted name in remote administrative management and secure access technology. ION's suite of tools enables service providers, government and military agencies, and corporate IT resources to remotely manage, monitor, and secure critical voice and data networks. More than half of the world's top telecommunications firms rely on ION technology to ensure quality service for their customers. With over 50,000 devices deployed worldwide, ION's products are currently in use in over 35 countries. For more information, visit www.ion-networks.com or call 800.722.8986 (US), +1 908.546.3900 (International).

"How do I secure and manage an out-of-band connection to network devices?"
www.ion-networks.com
Page 9 of 9