

# NUCLEAR PLANT CONTROL SYSTEM CYBER VULNERABILITIES AND RECOMMENDATIONS TOWARD SECURING THEM

Enabling Comprehensive Network-  
Based Security for Control Systems

## Table of Contents

Executive Summary .....	3
Introduction .....	3
Threats to the Control System Network .....	3
NRC March 2009 Security Enhancements .....	5
Seven-Step Plan for Plant Control System Cyber Security .....	5
Step 1 – Identifying Critical Assets .....	6
Step 2 – Profiling the Network .....	6
Step 3 – Creating and Managing Policies Across the Network .....	6
Step 4 – Creating a Strong Defense Perimeter .....	7
Step 5 – Ensuring Identity Management and Rogue Device Mitigation .....	7
Step 6 – Setting Up Secure Remote Access .....	8
Step 7– Monitoring and Reporting .....	8
Conclusion .....	9
About the Contributing Author .....	9
About Juniper Networks .....	10

## Table of Figures

Figure 1: Seven-step plan for plant control system cyber security .....	6
Figure 2: Nuclear power plant network security architecture .....	8

## Executive Summary

The nuclear energy industry is one of the few industries whose security program is regulated by the federal government. The U.S. Nuclear Regulatory Commission (NRC) holds nuclear power plants to the highest security standards of any American industry. Each of the nuclear power plants within the U.S. has extensive security measures in place to protect the facility from intruders.

The increasing reliance on computer systems and networks within control systems at nuclear power plants has presented new potential security threats—referred to as cyber security—that include such threats as viruses, worms, and unauthorized access. The potential effects such cyber security threats might pose to the real-time visibility and control, along with real-time response and deployment of needed resources in a plant on a daily basis, are not acceptable.

This paper helps control network and security managers better understand the cyber security challenges within today's nuclear power plants and what the actual threats are. The document then briefly reviews the key enhancements to cyber security required by the recent NRC Security Rule 7354, and presents a seven-step plan that can help address meeting these requirements by enabling a comprehensive network-based security solution.

## Introduction

For nuclear power plants, the digital computers and communication systems and networks are a strategic asset. Some key cyber security challenges in maintaining the safety and availability of nuclear plants are in the areas of interoperability, scalability, performance, usability, and manageability.

From a security perspective, many current security solutions lack the ability to adapt and respond proactively in real time to constantly evolving unintentional incidents and intentional threats such as hacking, scanning, denial-of-service (DoS) attacks, new exploits in applications, worms, and viruses, to name a few. Further, the lack of tight integration between security products such as firewalls and intrusion prevention systems (IPS), in combination with disparate features, creates a challenge to the job of adequately addressing security incidents.

Security and IT administrators are also faced with the challenge of making sure that the products they deploy scale to support ever-increasing network traffic and a diverse user population, while at the same time maintaining fast, reliable, and secure access to applications and network resources. Often this results in a compromise, where adding extra security degrades performance of the service or vice versa. Performance, interoperability, and scalability are also an issue, especially when service is required under heavy traffic load such as during an off-normal event or plant scram.

Finally, because existing solutions consist of a mix of different products and technologies that are not tightly integrated, administrators are faced with the challenge of understanding and managing multiple security products and management systems. This challenge grows exponentially when one tries to identify the root cause of an incident, where reports and logs need to be viewed from multiple systems and several hundred devices that are spread over many locations. This makes forensic analysis difficult at best, and leaves the network extremely vulnerable.

## Threats to the Control System Network

A primary source of cyber attacks against control systems originates via the WAN, the Internet, and trusted third-party or remote connections. While internal threats are still significant and one of the top areas of concern for plant managers, increasing numbers of targeted threats are originating from external sources. This mirrors the current threat trend in traditional IT systems.

Internal threats can come from a number of different sources, including attacks by disgruntled employees and contractors or accidental infection from a device accessing the network without the latest protection and unknowingly spreading a virus, worm, or other attack. However, user error and unintended consequences of routine actions actually represent the greatest risks, causing many cyber-related incidents in industrial environments. A local or remote user might access the wrong systems and make changes to them; IT personnel can perform a network penetration test that degrades performance or renders a system inoperable; or a user might download or send large files over the network and impact control traffic performance.

There is also a wide range of external threats to control systems. These range from accidental infection by a guest laptop to deliberate attacks. Today's hackers are now more often motivated by profit, with groups looking for opportunities for extortion or theft that provide a quick payoff. Such targeted intrusions are increasingly difficult to detect, which is a key reason for achieving complete visibility across the corporate network. These types of threats can include:

1. *Malicious Code (Malware)*: Malware includes the broad range of software designed to infiltrate or damage computing systems without user knowledge or consent. The most well-known forms of malware include the following:
  - a. *Viruses* manipulate legitimate users into bypassing authentication and access control mechanisms in order to execute malicious code. Virus attacks are often untargeted and can spread rapidly between vulnerable systems and users. They damage systems and data, or decrease availability of infected systems by consuming excessive processing power or network bandwidth.
  - b. A *worm* or self-replicating program uses the network to send copies of itself to other nodes without any involvement from a user. Worm infections are untargeted and often create availability problems for affected systems. They might also carry a malicious code to launch a distributed attack from the infected hosts. There has been at least one case of a worm affecting a nuclear plant.
  - c. The *trojan* is a type of virus in which the malicious code is hidden behind a functionality desired by the end user. Trojan programs circumvent confidentiality or control objectives and can be used to gain remote access to systems, gather sensitive information, or damage systems and data.
2. *Denial-of-Service Attack*: DoS attacks have become notorious over the past few years when used by attackers to flood network resources, such as critical servers or routers, in several major organizations with the goal of obstructing communication and decreasing the availability of critical systems. A similar attack can be easily mounted on a targeted control system, making it unusable for a critical period of time. An unintentional denial-of-service incident has occurred to at least one nuclear plant.
3. *Rogue Devices*: In wireless networks, an unauthorized access point might be inserted into the control system. This can be done in a non-malicious manner, which inadvertently provides an unknown access point. It can also be done maliciously to provide false or misleading data to the controller, which can cause it to issue errant commands such as triggering a fail-safe device or changing operator screens to provide erroneous information.
4. *Reconnaissance Attacks*: Reconnaissance attacks enable the first stage of the attack life cycle by probing. This serves to provide a more focused life cycle and improve the odds of success in the attacker's favor.
5. *Eavesdropping Attacks*: The goal of an eavesdropper is to violate the confidentiality of communications by "sniffing" packets of data on the control network or by intercepting wireless transmissions. Advanced eavesdropping attacks, also known as "man-in-the-middle" (MITM) or path insertion attacks, are typically leveraged by a hacker as a follow-up to a network probe or protocol violation attack.
6. *Collateral Damage*: This type of impact is typically unplanned or materializes as an unforeseen or unplanned side effect of techniques being used for the primary attack. An example is the impact that bulk scanning or probing traffic can have on link and bandwidth availability. Or, if a network is not properly configured, unintended traffic—such as large downloads, streaming video, or penetration tests—can consume excessive bandwidth and result in unacceptable levels of network "noise" and slowed performance. Jitter is a significant, and usually undesired, factor in the design of almost all communications links. Since field controllers are sensitive to jitter, network noise can be detrimental to performance.
7. *Unauthorized Access Attacks*: These are attempts to access assets that the attacker is not privileged or authorized to use. This implies that the attacker has some form of limited or unlimited control over the system.
8. *Unauthorized Use of Assets, Resources, or Information*: In this type of incident, an asset, service, or data is used by someone authorized to use that particular asset, but not in the manner being attempted.

The faster a threat can be recognized, the more quickly with which it can be dealt. Preventing the behavior of the attacks and intrusions once the hacker is inside is the key to network security. There are many "back doors" and potential weak links in industrial control system networks. Typically, these include misconfigured devices, undocumented connections, wireless networks without proper security configurations, and open unguarded ports. A primary vector of concern is the compromise of data that can alter the operation of field devices or mislead an operator into taking inappropriate action.

Perhaps the greatest threat of all is the lack of understanding within the industrial organizations—in both operations and IT departments—as to the seriousness of the problem. Even control system vendors still are not designing technologies for security. In fact, many are instead including vulnerable applications and technologies such as Microsoft IIS, Bluetooth wireless communications, and wireless modems in their latest offerings.

## NRC March 2009 Security Enhancements

The NRC endorsed cyber security guidelines in 2005 and by May 2008 all 104 operations nuclear power plants in the U.S. had implemented them voluntarily. In March 2009, the NRC issued “enhancements” to cyber security—Nuclear Regulations 10 CFR 73.54 “Protection of digital computer and communication systems and networks.” This rule stated the following:

- By November 23, 2009 every one of the 104 U.S. plants and companies seeking to license new plants must submit a comprehensive cyber security plan including a proposed implementation schedule.
- These cyber security plans must include measures to:
  - Ensure the capability for timely detection and response to cyber attacks
  - Mitigate the consequences of such attacks
  - Correct exploited vulnerabilities
  - Restore the affected systems, networks, and equipment
- The rule also imposes new requirements pertaining to individuals who have electronic means to interfere with plant safety, security, or emergency preparedness such as enhanced psychological assessments.

The actions laid out in this security rule state that to accomplish its objectives, the licensee will:

- Analyze digital computer and communication systems and networks and identify those assets that must be protected against cyber attacks
- Establish, implement, and maintain a cyber security program for the protection of these assets
- Incorporate the cyber security program as a component of the physical protection program to emerging threats that take advantage of gaps between disparate devices to cause disruption and downtime

The draft NRC Regulatory Guide 5-71 identifies the NIST standards as an acceptable program to meet the NRC Security Rule.

## Seven-Step Plan for Plant Control System Cyber Security

To address the security needs of nuclear power plant control networks, it is essential to begin with a layered defense-in-depth approach that enables administrators to monitor the network at every level. Primary concerns for a control system network manager include:

- Assuring the integrity of the data
- Securing remote access
- Validating and authenticating every device and user on the control system network

A systematic approach to security begins with reducing the vulnerable surface of the industrial control system network. The first stage is the creation of control system-specific policies that detail which devices, what protocols, and which applications can run on the network; who and what have access to these devices and from where; and what are the types of operations a user (or a role) is allowed to perform. The next stage is to identify the appropriate locations to implement the policy. This can be through the appropriate configuration of controls on devices already present on the network, and by adding various network elements. Such network elements are required to create a security perimeter, provide additional enforcement points, and segment the network for fault containment. The third stage is to monitor the implementation of the policy to ensure these controls are effective, locate any violations, and then feed back into the policy any corrections based on observed network behavior. Security is a continuous process and requires diligent monitoring, reviewing, and adjusting to be effective. The following sections explain each of these stages and discuss existing technologies that can be used for securing typical control networks.

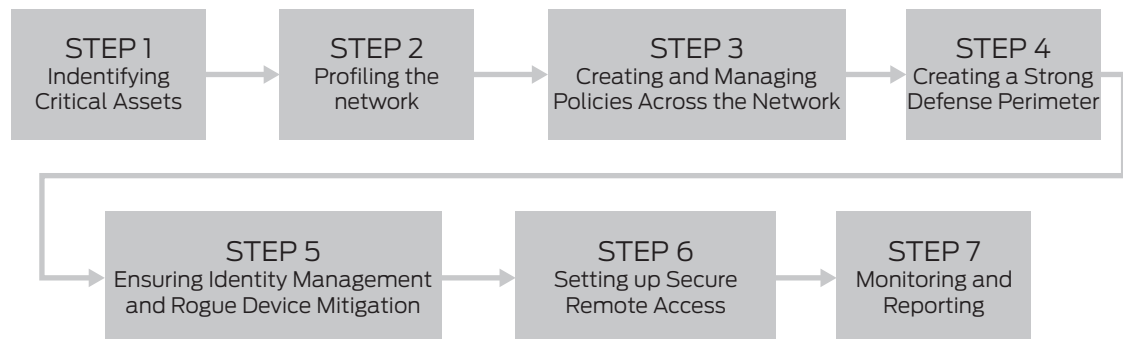


Figure 1: Seven-step plan for plant control system cyber security

### Step 1 – Identifying Critical Assets

Policy creation begins with identifying assets that need protection and the requisite level of protection. On a control system network these are real-time servers, field devices, and peripherals such as printers and network routers and switches. The primary vector of most concern is the compromise of communication that can alter the operation of field devices. In order to gain a foothold behind a firewall, attackers typically target non-essential appliances that are most vulnerable. Hence, any network-enabled device on the control network must be considered critical for security.

Since most servers on the control network run standard operating systems and applications, they must be guarded against common cyber threats. Such threats include intentional as well as unintentional DoS attacks through packet floods, irregular packets, protocol anomalies, buffer overflows, worms, trojans, and spyware.

### Step 2 – Profiling the Network

In order to create a comprehensive policy, the network administrator (typically a role performed by a control systems engineer) needs a tool that can collate information from all subnets. Since a majority of devices are vulnerable to disruption from active scans using tools such as Nessus, passive scanning and identification is currently the only viable option to discover and identify all devices detected on the network.

This profiler tool needs to log all network activity into tables that provide information about device types, operating systems, protocols, applications, and network peers. The profiler can be used to establish a baseline that can track the servers and control devices on the network, as well as the protocols and services those components use to communicate.

By immediately locating new components on the network, an administrator can ensure that those components are protected and can track their status. The profiler should use passive fingerprinting to provide an inventory of operating systems and software applications, their versions, and what components use them. As new versions or security updates are announced, an administrator is able to determine if the network is affected, locate the affected components, and identify remediation as appropriate.

### Step 3 – Creating and Managing Policies Across the Network

Once devices, networks, applications, and users have been identified, a network management system is required, which preferably can be used as a centralized management system to create and manage policies across all security devices.

Through rule-based policies, an administrator can create policies tailored to the type of devices being protected on a particular subnet or VLAN. Such tailored policies improve efficiency while reducing the number of events an administrator has to address. For example, a Windows-targeted worm attacking a Linux host might not be a critical event.

The network management system should also support dynamic groups of attack objects. An administrator can define a dynamic group based on OS or protocol set, such as DCS, and stay up-to-date on protection without having to manually address each vulnerability.

#### Step 4 – Creating a Strong Defense Perimeter

Given the need to access control networks from the corporate network or, in some cases, from the Internet, it is essential to create a strong defense perimeter. A perimeter firewall must create at least three security zones—a secure zone for the control system network elements, a demilitarized zone (DMZ), and an insecure zone.

Even if all access to the control network is through the corporate network, the perimeter firewall must treat the corporate network as insecure and have a mutually non-trusting policy. The DMZ contains secure access authentication devices, workstations, and servers that are accessible from the insecure network. Any device in the secure zone should be accessible only through one of the DMZ devices. By ensuring that the devices in the DMZ are properly protected and continuously monitored, a control network administrator can significantly reduce the probability of a network-based attack. As previously mentioned, it is key that the perimeter device not only provide security zones and flow-based firewalls, it must also detect protocols and applications it is protecting.

An integrated, purpose-built firewall/IPsec VPN security solution is recommended that can be used to secure control system networks. This device should offer robust firewall capabilities for control system-specific protocols (for example, Modbus, DNP3, etc), providing the first line of defense from network attacks. Additionally, it should have upgraded capabilities for full IPS support to secure the control system network from the latest application-level exploits and attacks.

#### Step 5 – Ensuring Identity Management and Rogue Device Mitigation

The most likely vector for an intrusion in a control system network is unintentional inappropriate use. An employee or contractor might plug in a laptop to perform routine tasks without realizing that it has picked up a worm or spyware. (This has already occurred in nuclear plants). The worm can then start scanning the control system network, and cause outages on devices such as PLCs due to unexpected traffic. This scenario is even more likely with the proliferation of wireless access points. Control over access points through authentication of every user and health-checking of every device is essential to ensure security within the perimeter.

A network access control (NAC) solution should combine user identity, device security, state, and location information for session-specific access control by user, enforced throughout the network. This NAC system should be an open-standards-based solution built on field-tested, best-in-class security and networking products. With strong authentication enforced, access to the network and resources within the network can be closely controlled. Control over the resources accessible by particular users can minimize the proliferation of worms and other malware, which might have been inadvertently introduced to the network.

One of the primary concerns in augmenting control system networks is to ensure that inline security devices do not impact the network's performance or availability. Therefore, we suggest to use a device that provides a passive intrusion detection service (IDS) with a sniffer mode—combined with a NAC policy server—that enables the creation of policies to restrict access at the application level. For example, if a contractor sends a Modbus write command to change PLC setpoints, the Juniper Networks IDP Profiler notifies the NAC appliance about the unauthorized activity. The NAC appliance can then signal to any 802.1X-compliant switch or firewall that the contractor's access must be terminated or quarantined. Meanwhile, an event is logged for administrators to follow up.

The NAC solution should minimize the need for an administrator to create numerous access control lists (ACLs) across the control system network to provision the appropriate level of access for each user. The IDP Profiler can also provide usage information for every session on the control system network for compliance monitoring and forensics. In addition, Juniper Networks IC Series Unified Access Control Appliances can be deployed locally to the control center with federation of identities enabled from the corporate network to the control network. This allows control system network administrators to have complete control over permitted users and their access privileges regardless of their privilege levels on the corporate network without a dual sign-on.

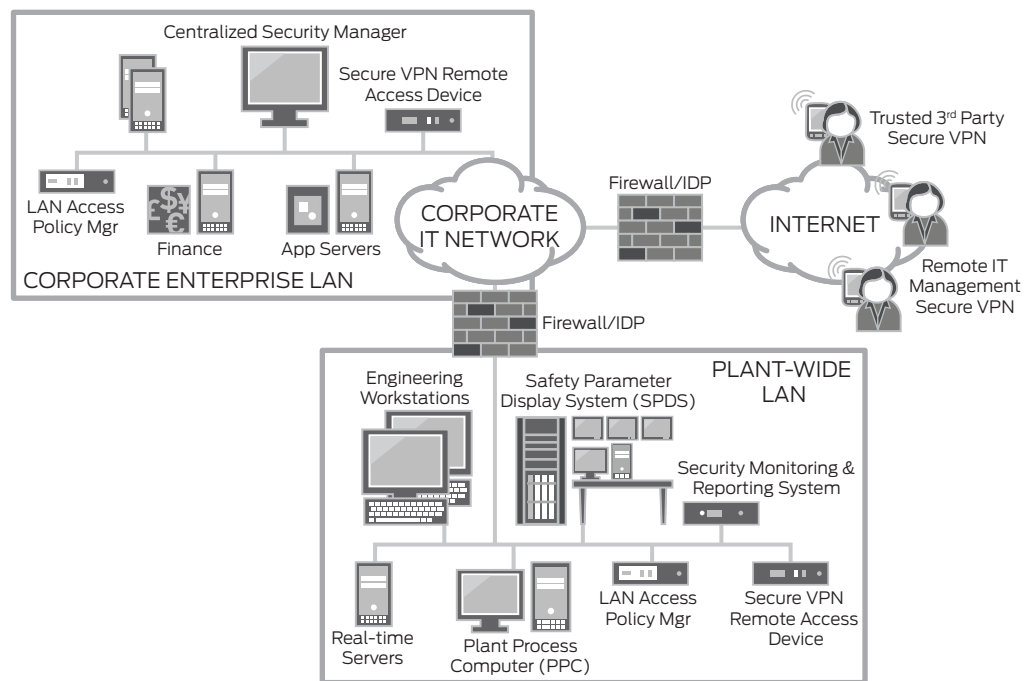


Figure 2: Nuclear power plant network security architecture

### Step 6 – Setting Up Secure Remote Access

Remote access is enabled for several reasons. A plant operator/engineer might remotely monitor equipment status; corporate engineering might need to collect plant data; or a vendor might have to diagnose and fix operational problems. In order to minimize the probability of unintentional misuse or tampering, users should be limited only to functions for which they are authorized. For example, a vendor logging in to update a patch must not be able to run any control system commands. If a contractor's laptop contains spyware, or his antivirus is not up to date, that contractor should not be allowed access to the control system network.

A VPN appliance based on SSL, the security protocol found in all standard Web browsers, is what we recommend. The use of SSL VPNs eliminates the need for client-software deployment, changes to internal servers, and costly ongoing maintenance and desktop support. Enhanced remote access methods enable the enterprise to provision access by purpose for virtually any resource. The level of access can also be dynamically adjusted based on the condition of the remote access device, such as the timestamp of the most recent antivirus definition files.

### Step 7– Monitoring and Reporting

Once access policies are defined, firewalls, switches, and intrusion prevention devices can act as enforcement points as well as monitoring stations for flagging any policy violation. The IDP Profiler information, combined with user information from the NAC and SSL/VPN devices, provides insight into who is using the network, what applications they are running, and from where they came.

The IDP Profiler provides session context at the granularity of individual control system protocol commands and the values being set. This information can be used to create a baseline of expected communications. The administrator can establish a policy of acceptable communication and have the management system send an alert on any violations of policy. For example, a point-to-point connection initiated to/from the control system network, or an IRC command being sent to a machine designated as a real-time data collection server, could automatically trigger an alert and notify the control system network administrator of these policy violations.

The network administrator should also have a monitoring and reporting tool to help keep track of the services running in the DCS network and alert to any new services being deployed or changes in the behavior of the existing services. Changes to the network or behavior of existing services might indicate an attack has gained access to the equipment or that an employee might be using the systems inappropriately, causing risk to the organization.

The tool should also monitor for other known attack vectors that might go undetected. These might include a system attempting to connect to known hostile hosts or networks, such as those known to run BOTNET command and control channels. The tool should also prioritize and correlate attacks on the DCS network back to the location of origin.

This tool should also provide correlation features, where all the devices monitoring the control system network—such as IPS, firewalls, and antivirus platforms—can be correlated together for a single operational view of the security state of the control system network. The tool should also go beyond the network and also monitor the application logs from the control system, which might indicate certain attack vectors or even system failures.

The monitoring and reporting tool, as well as third-party analyzers such as SecureView, can also provide additional features that offer significant value to a complete security solution, including:

- **Historical Data:** Providing precise point-in-time data supports forensic investigation when researching past events. Many solutions support detailed correlation between multiple events, allowing network managers and security professionals to establish the root cause of an incident.
- **Comprehensive Reporting:** Textual and graphical reports are a vital tool for communicating the status of security-related events to a broad range of personnel—including network managers, facility managers, as well as third parties such as regulatory officials. Reporting solutions provide a framework for establishing consistent, measurable reporting metrics to key constituents.
- **Compliance Management:** With a myriad of ever-changing regulatory requirements from FERC and NRC—as well as pending legislation—the ability to correlate implemented policies and controls to specific statements in regulations, best practices, and SLAs is critical. Juniper security solutions can integrate with third-party tools to map these policies and controls to specific compliance criteria, and provide evidence for auditing events.
- **Asset-Based Risk Management:** Knowing the importance—as well as the potential attack vectors—of devices and systems on control networks is an important first step in the process of securing these components. By establishing key criteria related to these assets—such as value, likelihood of specific threats being realized, and the potential consequence of those threats—network managers can establish security controls that are both effective and efficient.

## Conclusion

The security of nuclear power plants' control system networks is critical to achieving mission objectives. To effectively protect the security of their plants, control system network administrators and network security specialists must have insight into the multiple types and levels of evolving threats to secure their network perimeter, critical resources, and remote access. Adopting the recent NRC security rule helps organizations establish a prioritized baseline for their information security measures and controls.

Taking a systematic, step-by-step approach to network security helps reduce the vulnerabilities of the control system network for nuclear power plants. By first creating system-specific policies, then identifying the appropriate locations to implement the policy, and finally monitoring the implementation of policy, administrators are able to protect against today's highly volatile and damaging cyber security threats.

## About the Contributing Author

Joe Weiss, Managing Partner of Applied Control Solutions (ACS), is an industry expert on control systems and security, with more than 30 years in the energy industry. Before launching ACS, he spent time at the Electric Power Research Institute (EPRI), heading programs including the Nuclear Plant Instrumentation and Diagnostics Program, the Fossil Plant Instrumentation & Controls Program, the Y2K Embedded Systems Program, and initiatives on cyber security for digital control systems. He has provided testimony to five congressional committees, and has served as a regular speaker for numerous industry events and at the NIST/NSA Security Summit.

Mr. Weiss holds two patents and has published more than 60 papers on instrumentation, controls, and diagnostics. He has also written a chapter for *Electric Power Substations Engineering* on "Cyber Security of Substation Control and Diagnostic Systems." He also established and chairs the annual Control System Cyber Security Workshop, and established the International Standards Coordination Meeting on Control System Cyber Security. He has received numerous industry awards, including the EPRI President's Award (2002) and is an ISA Fellow and member of the ISA Engineering, Science, and Technology Policy Committee. He is also the Managing Director of ISA Nuclear Plant Standards. Mr. Weiss is a registered professional engineer in California and a Certified Information Security Manager.

## About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at [www.juniper.net](http://www.juniper.net).

---

### Corporate and Sales Headquarters

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
Phone: 888.JUNIPER (888.586.4737)  
or 408.745.2000  
Fax: 408.745.2100  
[www.juniper.net](http://www.juniper.net)

### APAC Headquarters

Juniper Networks (Hong Kong)  
26/F, Cityplaza One  
1111 King's Road  
Taikoo Shing, Hong Kong  
Phone: 852.2332.3636  
Fax: 852.2574.7803

### EMEA Headquarters

Juniper Networks Ireland  
Airside Business Park  
Swords, County Dublin, Ireland  
Phone: 35.31.8903.600  
EMEA Sales: 00800.4586.4737  
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.