

SMART GRID SECURITY SOLUTION

Comprehensive Network-Based Security for Smart Grids

Challenge

Smart Grid operators must guard against international security threats from hackers, cyber terrorists, and rogue states; secure sensitive data; minimize data transfer bottlenecks that degrade performance; centralize management and reporting; and minimize cybersecurity incidents, all while controlling rising operational costs.

Solution

Juniper Networks Smart Grid security solution improves productivity with fewer security risks while significantly reducing total cost of ownership (TCO). This solution is built on the world's most dynamic, scalable, and interactive security infrastructure featuring real-time threat defense and unparalleled network-wide visibility and control.

Benefits

- Meets unique Smart Grid application requirements
- Comprehensive security that identifies, mitigates, and reports on even the most sophisticated attack
- Delivers network-wide and granular policy-based access control
- Reduces cost of ownership with lower CapEx and OpEx compared to disparate point products
- Enhances compliance via network-wide, real-time visibility

Today's global industrial infrastructure includes thousands of electric utilities, water/wastewater management companies, oil and gas suppliers, chemical manufacturers, and other related facilities. The control and monitoring system networks that operate these critical infrastructures are among the most attractive targets for hackers, cyber terrorists, and rogue states. As organizations rely more on off-the-shelf operating systems and Internet-based remote access to carry out production tasks, traditional control networks are open to the worms, viruses, and application-level attacks that proliferate online. Additionally, government mandates to update aging power generation and distribution networks, to add intelligence to these networks, and to implement a Smart Grid, creates a plethora of new security concerns and challenges that must be addressed and overcome.

The Smart Grid represents an advanced telecommunications/electric grid with sensors and smart devices linking all aspects of the grid, from generator to consumer, in order to deliver enhanced operational capabilities that:

- Provide consumers with the information and tools necessary to be responsive to electricity grid conditions through the use of electric devices and new services
- Ensure efficient use of the electric grid, optimizing current assets while integrating emerging technologies such as renewable and storage devices
- Enhance reliability by protecting the grid from cyber and natural attacks, increasing power quality, and promoting early detection and a self-correcting, self-healing grid

The Challenge

Smart Grid operators must guard against a wide range of security threats such as hackers, cyber terrorists, and rogue states, as well as unintentional actions. Operators must also secure sensitive data, minimize data transfer bottlenecks at various network security points that degrade performance, and centralize management and reporting to improve the overall health of the network, including compliance, and data correlation and analysis. And they must do all of this while controlling rising operational costs.

Operators must also improve connectivity between networks, whether wireless or wireline-based, and they must strengthen network security, since there are millions of potential vulnerabilities in the network. A lack of governing standards makes it more difficult to identify who is responsible for security, which adds to the vulnerability of network equipment such as network sensors and meters to hacking and terrorist attack.

Overcoming these challenges is made even more urgent in light of an expected shortage in electricity generation. Electricity rates are expected to double in the next 5 to 10 years, plans for new generating plants are not being approved due to environmental concerns, and alternate energy sources aren't expected to meet demand or be cost-effective. In addition, costs for maintaining

or replacing networks are prohibitive, and power outages and disturbances cost the U.S. economy \$25 to \$180 billion annually. Employee training costs are also expected to rise, as roughly one-third of the current workforce approaches retirement in the next five years.

Table 1: Juniper Networks Security Solutions Meeting Smart Grid Challenges

SMART GRID SECURITY CHALLENGES	ADDRESSING THESE CHALLENGES WITH JUNIPER NETWORKS SECURITY SOLUTIONS
<p>Vulnerabilities and cyber incidents</p> <ul style="list-style-type: none"> • Intentional and unintentional threats/vulnerabilities 	<ul style="list-style-type: none"> • Juniper Networks intrusion prevention system (IPS) technology incorporates multiple detection methodologies to be able to spot known and unknown threats/vulnerabilities, and stop them before they can cause damage. • In addition, Juniper Networks IPS and STRM Series Security Threat Response Managers utilize behavior analysis to ensure that critical assets are operating correctly and are alerting on deviations from established norms which could be an indication of a cyber event. • Furthermore, Juniper's IPS technology interoperates with Juniper Networks SA Series SSL VPN Appliances to ensure that local and remote user roles are enforceable throughout the network, and can automatically quarantine users should they deviate from their defined roles/responsibilities.
<p>Lack of network-wide visibility</p> <ul style="list-style-type: none"> • Various utility operations interconnecting with each other, other utilities, and customers 	<ul style="list-style-type: none"> • STRM Series and IPS solutions allow control center administrators to profile their networks, helping identify critical assets and alerting on changes to network topology. • The STRM Series also includes a robust event correlation engine that provides administrators with a single event view of any incident, plus canned and custom reporting for demonstrating compliance to established policies or regulatory mandates.
<p>Performance bottlenecks</p> <ul style="list-style-type: none"> • At different security points in the network 	<ul style="list-style-type: none"> • Juniper Networks security solutions deliver the performance and reliability required by the world's most demanding environments. • Juniper offers a wide breadth of product offerings designed to meet or exceed the needs of the smallest remote sites to the largest control/distribution centers. • In addition, Juniper Networks WXC Series Application Acceleration Platforms deliver consistent application performance for remote stations and sites.
<p>Rising cost of ownership</p> <ul style="list-style-type: none"> • Different security products for different problems, each with different operating systems and management tools 	<ul style="list-style-type: none"> • Juniper Networks security solutions are managed by a common management platform—Juniper Networks Network and Security Manager (NSM). • NSM provides complete provisioning and device life cycle management for the entire security posture including: Juniper firewall solutions, Juniper IPS solutions, SA Series appliances (local and remote), WXC Series appliances, Juniper Networks EX Series Ethernet Switches, and Juniper Networks J Series Services Routers. • Being able to manage the entire security portfolio from a common, cost-effective management platform greatly reduces the complications and risks associated with implementing costly security solutions. • In addition, by not having to deploy and learn multiple management solutions and work flows, NSM helps reduce configuration errors that can lead to unintentional cyber incidents.
<p>Lack of centralized management and reporting</p> <ul style="list-style-type: none"> • No clear view of overall health of the network, compliance, correlation, and analysis of data 	<ul style="list-style-type: none"> • The STRM Series provides a comprehensive, network-wide view of all critical assets, and logs their activities into a centralized event correlation engine to allow administrators to view a single incident instead of individual log files. • This helps quickly identify what has transpired, while allowing administrators to drill down to see specific log files about the incident in order to gather more information. • In addition, the STRM Series is equipped with a powerful reporting engine that incorporates several canned reports, and allows for custom reports for auditing purposes and for demonstrating compliance with regulatory mandates. • Of course, the STRM Series, like all Juniper security solutions, can be managed by NSM, Juniper's centralized management tool.

The Juniper Networks Smart Grid Security Solution

Juniper Networks® is a leader in network security, with innovative products recognized as the best in their respective categories by analysts from around the world. Furthermore, because they are from Juniper, these products offer something other products don't—the ability to work together within a unified management framework. This tight integration between devices delivers a Smart Grid security solution whose value exceeds the sum of its parts, empowering the network to change based on policies set as variables within the network, users, and threat environments change. Smart Grid entities do not have to compromise productivity for improving risk mitigation, or incur higher network TCO when deploying new services and applications.

The performance and scalability of Juniper's solution improve business operations and employee productivity. Its carrier-class reliability and power efficiency lower TCO. And its end-to-end security mitigates risk, maintaining control system reliability and functional safety.

Features and Benefits

- Smart Grid application awareness enables Juniper's solution components to adapt to meet the requirements of the Smart Grid network infrastructure.
- A single network-wide view for identification, mitigation, and reporting of complex attacks eliminates false positives with a highly advanced correlation system, enabling operators to concentrate on actual security incidents.
- Includes consistent and granular policy-based access control regardless of the location from which operators access the network.
- Unparalleled security and compliance functionality with a low TCO that is achieved by reducing both obvious capital expenditures and hidden operational expenses. CapEx is reduced with products designed to scale via an incremental, pay-as-you-grow model. OpEx is reduced with features such as a single management system that provisions all products in the solution to simplify learning and reduce deployment and provisioning times.
- Centralized management capabilities reduce management complexity, support compliance requirements, and reduce TCO.

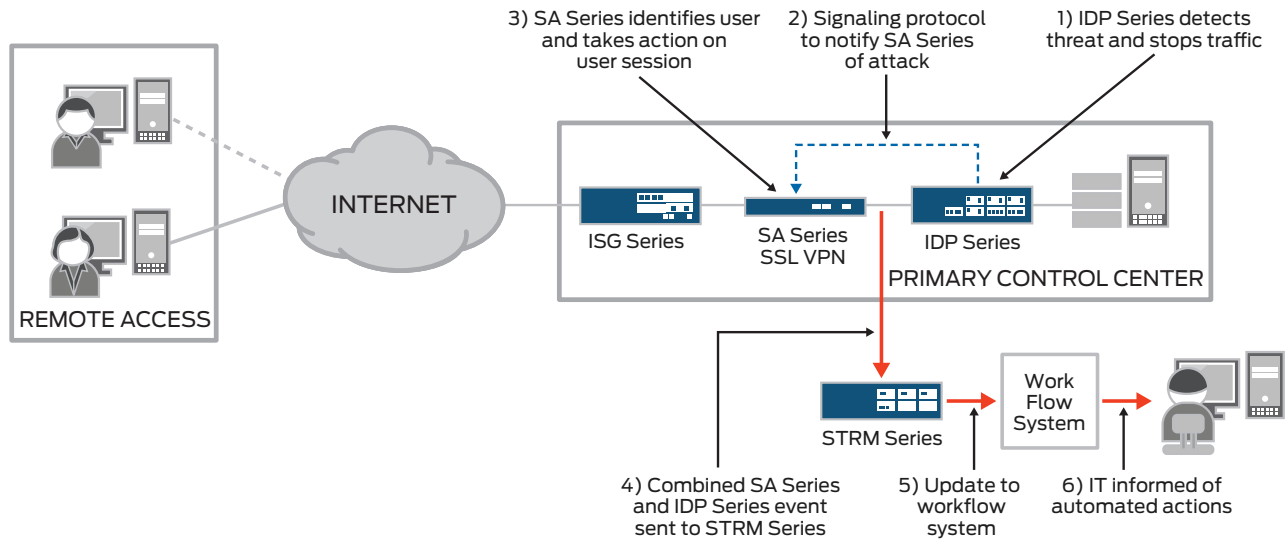


Figure 1: With Juniper's Smart Grid security solution in action, malicious traffic or an out-of-policy action can be thwarted in real time with a complete audit trail of events.

Table 2: Juniper Networks Smart Grid Security Solution Components

JUNIPER SECURITY SOLUTION	FUNCTION
<p>Firewalls</p> <ul style="list-style-type: none"> • Broad product offering (from smallest office to largest control centers) <ul style="list-style-type: none"> – SSG Series Secure Services Gateways – ISG Series Integrated Security Gateways – NetScreen Series Security Systems – SRX Series Services Gateways 	<ul style="list-style-type: none"> • Stateful inspection and logical network segmentation keep critical data streams isolated, while assuring adherence to and enforcement of security policies concerning port and protocol usage. • Application awareness helps identify attacks or malicious activity targeted at common applications. • Provides brute force protection against denial-of-service (DoS) or distributed-denial-of-service (DDoS) attacks. • Unified threat management (UTM) capabilities such as antivirus, antispam, URL filtering, and more provide enhanced protection at regional/remote sites from Internet-related attacks and vulnerabilities.
<p>Intrusion prevention</p> <ul style="list-style-type: none"> • Broad portfolio of stand-alone and integrated solutions <ul style="list-style-type: none"> – IDP Series Intrusion Detection and Prevention Appliances – ISG Series with integrated IPS – SRX Series Services Gateways 	<ul style="list-style-type: none"> • Application/protocol/session/traffic flow awareness. <ul style="list-style-type: none"> – Common synchronous code-division multiple access (SCADA) protocol decoders: MODBUS® Protocol, Inter-control Center Communications Protocol (ICCP), Distributed Network Protocol (DNP3), and more identify attacks using ambiguous traffic or fuzzing techniques for these and other common protocols. – Traffic anomaly detection identifies attacks by comparing incoming traffic volume to established baseline activities. • Multiple detection methods including signatures, protocol anomalies, backdoor, traffic, and more ensures greater threat detection capabilities and provides zero-day coverage against unknown vulnerabilities.
<p>Local and remote user access control</p> <ul style="list-style-type: none"> • Broad portfolio of local and remote access control solutions <ul style="list-style-type: none"> – SA Series SSL VPN Appliances – IC Series Unified Access Control Appliances 	<ul style="list-style-type: none"> • Enforceable business policies per user roles, device, location. • Coordination with Juniper Networks IPS to monitor and validate legitimate user access and thwart malicious activities or quarantine users who are not in compliance with established policies.
<p>Security event correlation and network behavior anomaly detection</p> <ul style="list-style-type: none"> • Purpose-built solutions <ul style="list-style-type: none"> – STRM Series Security Threat Response Managers 	<ul style="list-style-type: none"> • SCADA specific reports for responding to North American Electric Reliability Corporation/ Federal Energy Regulatory Commission (NERC/FERC) critical infrastructure protection (CIP) requirements. • Network/asset profiling and flow analysis identifies what is on the network and how it is communicating. Helps to enforce policies concerning critical assets. • Network behavior anomaly detection (NBAD) alerts on deviations to established network behavior that could indicate an attack or change of network composition.
<p>Data acceleration and encryption</p> <ul style="list-style-type: none"> • Purpose-built solutions <ul style="list-style-type: none"> – WXC Series Application Acceleration Platforms 	<ul style="list-style-type: none"> • Site-to-site optimization and protection. • Patented compression technology provides congestion relief for all IP-based traffic, helping organizations avoid performance bottlenecks and costly WAN upgrades. • Application control allows quality-of-service (QoS) capabilities to be assigned to traffic, ensuring sufficient bandwidth to critical applications as well as adjusting bandwidth allocation and prioritization schemes dynamically.
<p>Central, role-based management</p> <ul style="list-style-type: none"> • Network and Security Manager 	<ul style="list-style-type: none"> • Unified network management and centralized automation of complete device life cycle. • Manage entire security portfolio—firewall, IDP Series/IPS, access control, security event and incident management (SEIM), data acceleration. • Flexible and scalable—can be deployed as software or as dedicated appliances.

Summary—Juniper Networks Smart Grid Security Solution: Improved Productivity with Fewer Security Risks and Lower TCO

Smart Grid operators must guard against a wide range of security threats from hackers, cyber terrorists, rogue states, and unintentional actions. They must secure sensitive data, minimize data transfer bottlenecks that degrade performance, and centralize management and reporting to improve the overall health of the network. And they must do all of this while controlling rising operational costs.

Juniper Networks tight integration between devices delivers a Smart Grid security solution whose value exceeds the sum of its parts. With Juniper's solution, Smart Grid entities no longer need to compromise productivity while improving risk mitigation, or incur higher network TCO when deploying new services and applications.

Next Steps

For more information about Juniper Networks Smart Grid security solution, please contact your Juniper Networks sales representative or visit www.juniper.net.

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.

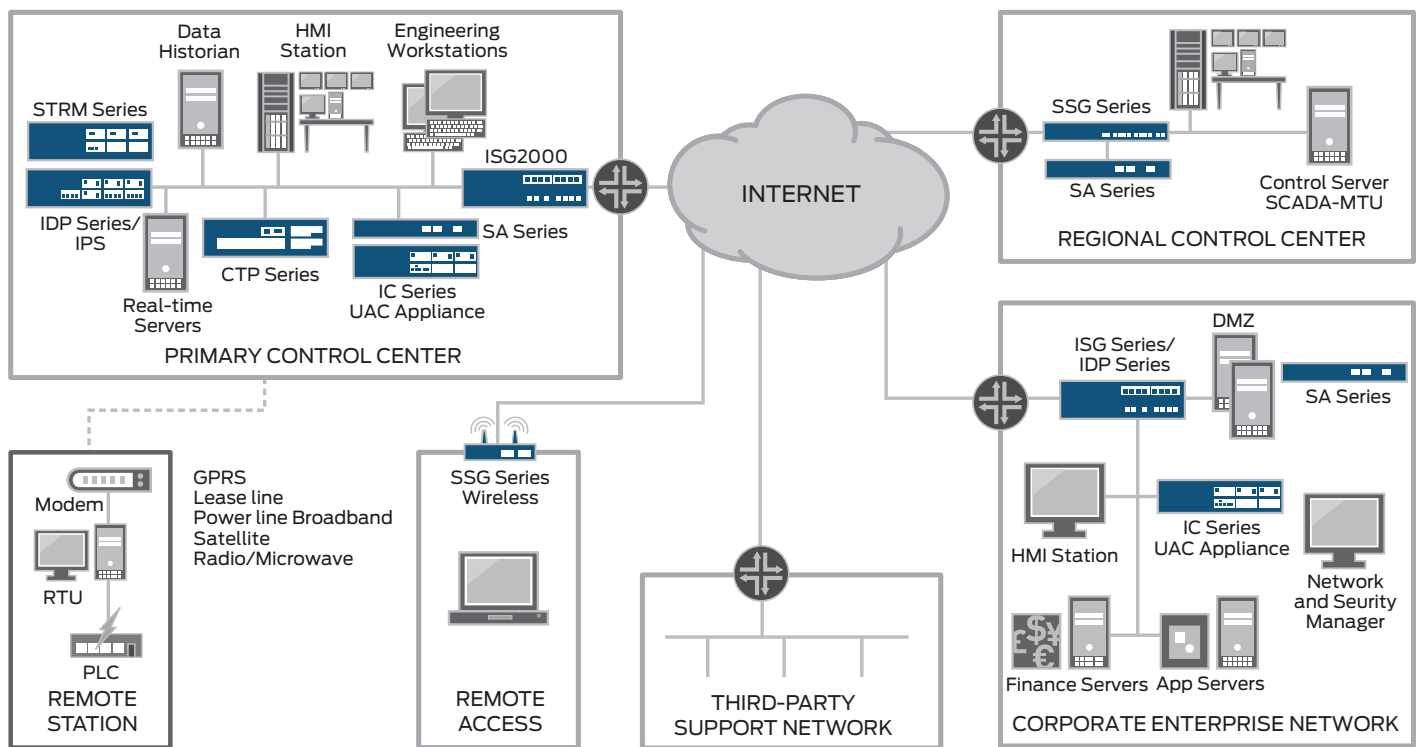


Figure 2: Comprehensive network-based security for Smart Grids

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

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 2010 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.