

SECURITY ASSESSMENT AND RISK MITIGATION

Service Overview

Attacks on enterprise and service provider networks are increasing at an unprecedented rate. In fact, security experts state that attacks are no longer measured by the number of events per week, but rather by the number of events that occur simultaneously. To protect your customers as well as your business investments, your organization must be able to maintain network security—and to react quickly if attacked. Juniper Networks Security Assessment and Risk Mitigation service can help you reduce network vulnerabilities, prevent attacks and mitigate the disruptions they cause.

Service Description

Through the Juniper Networks® Security Assessment and Risk Mitigation program, your organization receives access to Juniper Networks Professional Services IP security experts who perform a router security assessment of your network. These consultants analyze network design and configuration for security exposures, and architect solutions appropriate for established security policies and procedures.

The Security Assessment and Risk Mitigation program is offered in five phases. Your organization can take advantage of the entire program or choose individual elements to meet your specific network security requirements.

Phase 1: Vulnerability Analysis

Our experts work with your business, design, security and operations teams to gather information about the current network topology, security requirements, traffic profiles and business demands for existing and planned network services. We then review existing detailed designs and configurations, identify immediate internal and external vulnerabilities, and create a security profile for your network that is documented in a vulnerability analysis document.

Phase 2: Network Security Architecture

Our Professional Services consultants work with you to develop high-level security solutions for each tier of your network. They prepare a network security architecture document that includes the monitoring, detection and suppression capabilities required across your network. Plans for future network expansion are evaluated for potential security risks. Juniper Networks also reviews and recommends appropriate incident response practices for your network.

Phase 3: Mitigation and Implementation Plan

Our experts generate configuration templates for Juniper Networks Junos® operating system-based devices and document-specific requirements for individual network elements. Monitoring and detection parameters are defined, incident response techniques are documented, and a network security implementation plan is provided for the new configurations.

Phase 4: Predeployment Validation

Juniper Professional Services consultants develop a detailed test plan with your security and operations teams to verify that the network security implementation plan provides the level of protection required. The test plan is executed in a lab with the help of your

operations team, and the configurations are fine-tuned to ensure your network's security. In addition to validating the recommended security measures, the testing minimizes the inherent risk of introducing changes to your production network. Upon successful completion, the final configurations are worked into the production implementation plan.

Phase 5: New Configuration Deployment and Final Testing

Our experts work with your security and operations teams to deploy the new Junos OS configurations into your live network according to the production implementation plan. As the configurations are deployed, final testing is performed to confirm the functional and operational integrity of the network and verify the effectiveness of the changes.

Table 1: Features and Benefits

Feature	Feature Description	Benefit
Vulnerability analysis	Security profile and recommendations	Proactively identifies the network security risks and overall vulnerability to attack
Network security architecture	Design document and practices	Ensures consistent level of security across various network tiers and elements
Mitigation and implementation plan	Detailed implementation plan and configurations that carefully consider operational impact of network changes	Increases network availability due to reduced network vulnerability and exposure
Predeployment validation	Test plan, results and final configurations	<ul style="list-style-type: none"> Ensures minimal operational impact to the network Ensures well-understood, predictable results of changes
New configuration deployment and testing	Implementation of all steps contained in the Network Security Implementation Plan in your production network	Ensures that all steps contained in network security implementation plan are compliant with the new network security architecture
Knowledge transfer	Informal transfer of knowledge throughout the period of engagement	Prepares your staff to independently continue the security analysis work and implementation of network security changes

Table 2: Service Specifications

Juniper Responsibilities	Customer Responsibilities
<p>Provide a Juniper Professional Services consultant, who will work both onsite and remotely as appropriate.</p> <p>Depending on which program components you choose, provide the following deliverables:</p> <ul style="list-style-type: none"> Vulnerability analysis document Network security architecture document Network security implementation plan Test plan Test results Production implementation plan Security closure report Project closure workshop 	<ul style="list-style-type: none"> Provide a designated project manager or point of contact to interface with Juniper Networks on day-to-day issues and coordination of resources Provide access to appropriate members of your business, design, security and operations teams Provide external access to the Internet, internal access to your Intranet, and access to your network equipment that the consultant will support Provide access to any applications, databases and internal technical resources

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit www.juniper.net/us/en/products-services.

Ordering Information

The Juniper Networks Firewall Migration Service is available globally. Please contact your local Juniper Partner or Juniper Networks account manager for details.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at 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

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 2011 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.