

# JUNIPER NETWORKS UAC AND SA SERIES SSL VPN APPLIANCES INTEGRATE OPSWAT OESIS FRAMEWORK

## Managing Network Security for High-Performance Businesses

### Challenge

Defining a security policy that grants only protected endpoints network access, determining what security applications are running, and ensuring that they are fully patched and up-to-date.

### Solution

Juniper Networks Unified Access Control and SA Series SSL VPN Appliances together with OPSWAT OESIS Framework provide a solution that assesses the health level of an endpoint and enables customers to easily define security policies and effectively monitor devices attempting to enter their network.

### Benefits

- Accurately assess the endpoint health state
- Ensure only protected users are accessing network resources
- Manage user security applications through a single interface

System administrators have the task of securing their networks from outside and inside threats. When infected endpoints connect to the network, they unsuspectingly spread their infections to other improperly protected devices. The detection of security applications is imperative to network administrators, who not only need to implement security policies but also need to determine whether or not the endpoints trying to gain access to their networks are healthy and protected. In order to accomplish this task, the installed security application must, at a minimum 1) have its processes running; 2) have real-time protection enabled; and 3) be current with the latest released version.

In addition to admission control, networks also need post-admission monitoring and enforcement policies. The endpoint user must meet the security standard upon admission and continue to meet the network's security standards thereafter.

### The Challenge

There are countless cyber-threats including malware, spyware, adware, and crimeware that have become commonplace—making any unprotected computer or network vulnerable. Businesses need to accurately assess the security level of an endpoint to prevent viruses from distorting data, hackers from gaining access to sensitive financial information, and a multitude of spam from eating away valuable time and resources. On the one hand, it is fortunate that hundreds of security applications exist to protect endpoints from these threats. On the other hand, this provides an interesting challenge for system administrators writing security policies and attempting to manage this large number of applications. In addition, new threats are constantly born, and security applications have the challenge of continually updating their software to provide the detection and remediation necessary to eliminate these new threats. Administrators in turn must keep track of the large number of security applications and their patch/update release schedules.

The ideal solution is a two-pronged approach. The first would provide administrators the ability to detect and manage the wide variety of security applications and also control their common features through a single interface, regardless of the vendor. The second would include a system that monitors and collects application update information from vendors. This information would then be used to cross-reference what is being detected on the endpoints.



## UAC, SA Series, and OPSWAT Endpoint Security Integration Solution

Juniper Networks® Unified Access Control (UAC) delivers the access control, visibility, and monitoring of applications and users needed to more effectively and efficiently address regulatory compliance, while mitigating risk and exposure to today's rapidly evolving threat landscape. Juniper Networks SA Series SSL VPN Appliances provide secure, remote access capabilities for a variety of end-user groups including employees, partners, and customers. By leveraging the OPSWAT OESIS® framework, Juniper is able to extend the existing endpoint assessment capabilities of its UAC and SA Series solutions by adding robust application management for endpoint security solutions. This integration enables customers to easily define policies and assess the health of their endpoint security to effectively monitor devices attempting to access their network.

### Features and Benefits

Together, UAC and SA Series solutions along with OPSWAT's OESIS framework provide high-performance organizations with many of the following robust management capabilities.

- Detecting the presence of security applications
- Classifying the security applications
- Determining whether or not their processes are running
- Checking the real-time protection state
- Determining the last scan time
- Determining application currency by checking:
  - The age of the definition file
  - The application version
  - The engine version
  - The information reported by OESIS® Local and cross-referencing with security vendor data collected by OESIS® Monitor

### Solution Components

By integrating OPSWAT's OESIS framework into Juniper Networks Unified Access Control and SA Series appliances, organizations have an added level of assurance that their systems are protected from outside and inside threats. System administrators have the ability to classify, check and monitor the health of security applications protecting endpoints before enabling their access

to enterprise networks, both remote access as well as access on the LAN. The OESIS framework is comprised of both OESIS Local and OESIS Monitor, providing network security administrators the ability to cross reference what is being detected on the endpoint with what is being reported by security vendors to ensure security application currency and policy compliance.

### Endpoint Health Assessment and Security Application Management

When deployed together, UAC, SA Series, and OPSWAT OESIS framework provide detection and management capabilities to system administrators. This integrated solution allows them to ensure that endpoints logging into the network are healthy and protected with the most current versions of their respective security applications.

### Next Steps

For more information about Juniper Networks UAC, visit [www.juniper.net/uac](http://www.juniper.net/uac).

For more information about Juniper Networks SSL VPN solutions, visit [www.juniper.net/sa-series](http://www.juniper.net/sa-series).

For more information about OPSWAT OESIS, visit [www.opswat.com/products.shtml](http://www.opswat.com/products.shtml).

### About OPSWAT

Founded in 2002, OPSWAT is the world leader in development tools and data services that power solutions managing security features of endpoint applications. OPSWAT also founded OESISOK™, an open industry-wide certification program that verifies the interoperability of endpoint security applications with products from market-leading technology vendors. OPSWAT Inc. is headquartered in San Francisco, California, with an additional office in Herzliya, Israel.

### 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.