

# COORDINATED THREAT CONTROL

## Juniper Networks SA Series SSL VPN and IDP Series Intrusion Detection and Prevention Appliances

### Challenge

IT departments face the dilemma of enabling remote access to a diverse group of users while at the same time making sure their corporate network is shielded from accidental or malicious attacks.

### Solution

Coordinated threat control enables Juniper Networks SA Series SSL VPN Appliances and Juniper Networks IDP Series Intrusion Detection and Prevention Appliances to correlate the user's identity (session) from the SSL VPN with the threat detection capabilities of IDP Series.

### Benefits

- Rapid detection of source and correction taken during attack to prevent any further harm
- Enhanced protection of network resources
- Trusted enablement of secure remote access to diverse users
- Increased user productivity with minimal downtime due to network attacks

Today's IT departments have increasing demands for providing secure remote access for employees, partners and customers. The proliferation of users along with the diversity of users, devices and networks is only a part of the challenge. The escalating volume and sophistication of threats from intentional and unintentional attacks contribute to the challenges for extended enterprise access.

### The Challenge

A common theme of frustration for IT departments continue to be the escalating barrage of viruses, trojans, worms and spyware. While the number of these incidents continue to grow, the increasing sophistication of these network attacks are also compounding the frustration even further. To combat these market trends, more and more IT departments are realizing the importance of Intrusion Detection and Prevention (IDP) systems as well as firewalls, logs, password complexity, and other technology and physical security measures to address the rapid growth of threats to any enterprise.

The increased need for remote access for the extended enterprise of employees, partners and customers must be balanced with steps to ensure valuable resources and assets are protected from intentional or unintentional attacks. Granular access capabilities and endpoint security technologies provide the ability for IT to control access to applications and resources. However, while restricting access to only what a user requires is critical, it does not prevent attacks that can come from either unintentional or malicious authenticated users. Some examples include a disgruntled employee/partner or a hacker who has compromised the authentication credentials of a user. Another example is malicious code (for example, spyware) that has not been intercepted or discovered by endpoint security policies. In addition, sometimes practical considerations—such as restrictions as to what partners will allow a company to download to their endpoints—reduce the ability of administrators to utilize endpoint security technologies, further limiting an administrator's security tools.

A common way of adding security to a remote access deployment is to utilize IDP technologies. However, deploying Intrusion Prevention Systems (IPS) behind an SSL VPN can be limiting. When malicious traffic is detected, it can be difficult to correlate the malicious tunneled traffic to a specific user and sometimes impossible to identify a user with intermediated traffic. However, the identification of the user and the source of the malicious traffic are key in maintaining a secure network for the extended enterprise. Valid users whose remote access devices may have been compromised must be notified

and directed to “clean” their devices of any malware. Malicious users on the other hand, must have their access blocked to prevent further network attacks. Containment and restricting any further access are imperative to safeguard all resources.

The challenge is for enterprises to reliably secure each and every session, so that they can deliver high-end user productivity while protecting information assets.

## The Juniper Networks Coordinated Threat Control Solution

Juniper Networks® coordinated threat control provides a solution for overcoming the challenge of balancing extranet access—for full-access remote employees and partners to critical applications—while maintaining a strong security posture around the enterprise’s critical assets.

Coordinated threat control enables SA Series and IDP Series to tie the session identity of the SSL VPN with the threat detection capabilities of the IDP Series to effectively identify, stop, and remediate both network and application-level threats within remote access traffic. With this technology, when the IDP Series detects a threat or any traffic that breaks an administrator-configured rule, it signals the SA Series appliance. The SA Series uses the information from the IDP Series to identify the user session that is the source of undesired traffic.

Utilizing this information, the SA Series is able to take actions on the endpoint including: terminating the user session, disabling the user’s account or mapping the user into a quarantine role. Administrators can configure the quarantine role so that they can provide users with a lower level of access to resources and inform users of why they have been quarantined and what they should do to remove themselves from the quarantined role.

They could also execute additional endpoint security checks or download additional endpoint protection software. The SA Series allows administrators to take action on user sessions either manually by selecting an active user session and executing the desired action, or automatically by creating policies that will execute the desired actions as soon as a signal that matches the policy criteria is received from the IDP Series. With this new functionality, the combined SA Series and IDP Series solution allows administrators to take action by not only blocking attacks before they reach their targets, but also by taking coordinated action against the endpoint that is the source of the attack.

## Features and Benefits

Looking across the requirements of the extended access, it becomes apparent that coordinated threat control provides unique benefits for different use cases. The following provides two example use cases using the coordinated threat control solution.

### Customer Value

In this scenario a user has been granted full network access. With this unfettered access comes the concern that any malware on the user’s machine will also have unlimited access to high-value assets.

In this use case, coordinated threat control provides the administrator with the ability to:

- Detect and drop malicious application-layer traffic (for example, worms, trojans, spyware, keyloggers)
- Control application usage on the endpoint (for example, IM chat clients, peer-to-peer programs)
- Identify source of malicious traffic, unapproved application user and take action on source (for example, disabling/quarantining accounts)
- Log detailed endpoint, user, network and application-layer traffic information for security event mitigation, auditing and compliance

### Partner Access

In this scenario, a business partner has been given access to certain resources on the enterprises network. Since there is little control over the incoming user and the user’s machine, the exposure to attacks is quite high.

In this use case, coordinated threat control provides the administrator with the ability to:

- Provision access to required applications (“provision by purpose”)
- Detect and drop malicious application-layer traffic
- Identify source of malicious traffic and take action on source even when SSL VPN is acting as a proxy
- Log detailed endpoint, user, network and application-layer traffic information for security event mitigation, auditing and compliance

## Solution Components

Juniper Networks SA Series SSL VPN Appliances enable any Web-enabled device such as a corporate laptop, PDA, or kiosk to securely access an organization's resources without the cost and complexity of installing, configuring, and maintaining any client software for each device. The appliances use SSL (Secure Sockets Layer), the security protocol found in all standard Web browsers. SA Series appliances also offer sophisticated partner/customer extranet features that enable controlled access to differentiated users and groups without any infrastructure changes, demilitarized zone (DMZ) deployments, or software agents.

Juniper Networks IDP Series Intrusion Detection and Prevention Appliances provide comprehensive and easy-to-use inline protection that stops network and application-level attacks before they inflict any damage to the network, minimizing the time and costs associated with maintaining a secure network. Using industry-recognized stateful detection and prevention techniques, the IDP Series provides zero-day protection against worms, trojans, spyware, keyloggers and other malware from penetrating the network or spreading from already infected users.

## Summary – Proven Solution to Quickly Detect Malicious Traffic and Take Immediate Action

With coordinated threat control, Juniper Networks provides enterprises with the ability to deploy best-in-class access and threat prevention technologies in a seamless solution that works to provide secure and assured access. With this solution enterprises can continue to service the ever-expanding need for anywhere, anytime access to information with the confidence that their security posture remains uncompromised.

## Next Steps

Please contact a Juniper Networks representative or Juniper's global network of channel partners for any questions about the coordinated threat control solution.

## 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

### 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  
Fax: 35.31.8903.601

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. "Engineered for the network ahead" and JUNOSE are trademarks of Juniper Networks, Inc. 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.

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

