

# COORDINATED THREAT CONTROL

---

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

## Table of Contents

Introduction .....	1
Threats .....	1
Benefits of Coordinated Threat Control .....	1
Design Considerations .....	2
Description and Deployment Scenario .....	3
Configuration .....	3
Communication Setup .....	3
Action Setup .....	6
Logging .....	7
Summary .....	7
About Juniper Networks .....	8

## Table of Figures

Figure 1: IDP Series configuration .....	4
Figure 2: One-time password (OTP) .....	4
Figure 3: IVE—new sensor .....	5
Figure 4: IVE—IDP Series connected .....	5
Figure 5: Example of sensor expressions .....	6
Figure 6: SA Series actions .....	6
Figure 7: SA Series logging .....	7

## Introduction

This document provides details on the functionality of Coordinated Threat Control features available on the Juniper Networks® IDP Series Intrusion Detection and Prevention Appliances and Juniper Networks SA Series SSL VPN Appliances. In addition to the background and implementation details, deployment and sample configuration information are also provided.

Employing a traditional layered security approach, where an intrusion protection system is positioned behind the SSL VPN gateway in order to identify and block attacks, is not flexible enough to provide true network protection. The inherent problem with such an approach is that all user traffic appears as if it were initiated from the same IP address (the SSL VPN device). Even with Network Connect, IP addresses from the pool of addresses being reused by different users are not an accurate enough indicator to identify who the real user/attacker is. It would be possible to derive some conclusions by manually analyzing SSL and IDP logs, but for all intents and purposes, this is both impractical and a virtually impossible task to perform on a daily basis.

Coordinated Threat Control, on the other hand, enables Juniper Networks SA Series SSL VPN Appliances and IDP Series Intrusion Detection and Prevention Appliances to correlate the user's identity or session from the SSL VPN with the threat detection capabilities of the IDP Series. This effectively identifies, stops, and remediates users who pose network or application-level threats within the remote access deployment. With this technology, when the IDP Series appliance detects a security event (be it a threat or any traffic that breaks an administrator configured policy), it can, in addition to blocking that threat, signal the SA Series device in real time. The SA Series then uses the information from the IDP Series appliance to identify the user session that is the source of the undesired traffic, and can take actions on the endpoint that include terminating the user session, disabling the user's account or mapping the user into a quarantine role, or simply notifying the administrator via Syslog.

Administrators can configure the quarantine role to provide users with a lower level of access and inform them why they have been quarantined and what they should do next. Administrators can 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 appliance.

Coordinated Threat Control is supported on standalone IDP Series appliances running version 3.2R2 and above (with the exception of 4.0R1) and the SA Series running IVE 5.3R1 and above.

## Threats

Customers normally leverage SSL VPN gateway technology to provide application/database access to third parties such as customers or partners. While this solution may be robust, many risks still exist, including:

- In most cases, in order to keep costs down, organizations deploy weak authentication (for example, simple password protection) to their partners and customers. Given the nature of such authentication, there is a very real concern that credentials will be compromised by an unauthorized party.
- Also, there is an ever present threat from malicious partners and/or customers. Once customers, partners, or some other party who manages to obtain credentials successfully authenticates, they can freely mount attacks against resources to which they have been authorized access.
- Then there is a genuine risk that the endpoint security policy will not be able to identify malicious code that is possibly even unknown to the end user even though it is running on his/her machine.
- Last but not least, threats can exist from attack proliferation targeted against business partners from the customer's very own server(s), if infected or compromised.

## Benefits of Coordinated Threat Control

Juniper's Coordinated Threat Control solution for employee and partner remote access provides three main benefits:

1. *Comprehensive threat detection and prevention.* Utilizing proven and market leading technology, the IDP Series can detect and block most network worms based on software vulnerabilities, trojans, malware (including response side or server-client malware), zero day attacks with protocol or traffic anomaly detection, attacks from user to application and from application to user (for example, propagation from a server side endpoint), and spyware/adware/keyloggers.

2. *Correlated threat information.* With the ability to correlate session identity and threat detection, Juniper can reliably identify the source of attacks and provide administrators with unmatched visibility into security events. This goes above and beyond anything available, even an “all in one” security router. Specifically, Juniper’s solution can provide:
  - Full access to identity/user information in authentication servers and directories
  - Extensive end-user device information from “Host Checker” that can inform administrators of the type of device (OS, browser or other) and the presence of endpoint security software
  - Access history from SA Series logs that can show administrators which resources and applications a user has utilized
  - Detailed threat information from the IDP Series that helps administrators understand the nature and impact of the threat
  - Overall profile of application-layer traffic through the IDP Series Enterprise Security Profiler
3. *Coordinated threat response.* As before, administrators can use the IDP Series to not only detect threats but also to block them from reaching the intended victim. Now, administrators can also use the SA Series to take action on the source of the threat as well as the threat itself. Taking action on the source of a threat is a very valuable way to mitigate security threats. The specific actions the SA Series appliance can take include:
  - Terminating the user’s session
  - Disabling the user’s account so that the user cannot authenticate to the SA Series again until his/her account is re-enabled
  - Quarantining the user by mapping him/her to a new role, either temporarily or permanently

## Design Considerations

Today’s SSL VPN gateways (including the SA Series) are not equipped with technology capable of mitigating Web-based application threats such as malicious code injection (cmd, SQL), buffer overflow, parameter change/forceful browse, Cross-Site Scripting (XSS) and loss of confidential information (social security number, credit card number, and so on).

The IDP Series, on the other hand, has been designed with exactly that purpose in mind—to provide protection against many variants of these threats through signatures for Web applications, as well as through traffic and protocol anomaly detection.

In addition to providing protection for an enterprise’s own Web applications, the IDP Series can also provide protection for an enterprise’s portal partner devices. For instance, the IDP Series can prevent the propagation of attacks to partners when a company’s own server is infected. It can also stop spyware from “phoning home,” and it can provide protection when a server is retrieving data from a third party as part of a Web application.

The next big concern for customers in regards to SSL VPN gateways revolves around the nature of the Network Connect (Layer 3 SSL VPN) access method which, like IPsec, provides full network access via an encrypted tunnel into the corporate network. This deployment practice presents real threats that range anywhere from worms, hacker attacks, trojans and spyware/malware to many known and unknown (zero day) attacks that leverage vulnerabilities in packaged applications.

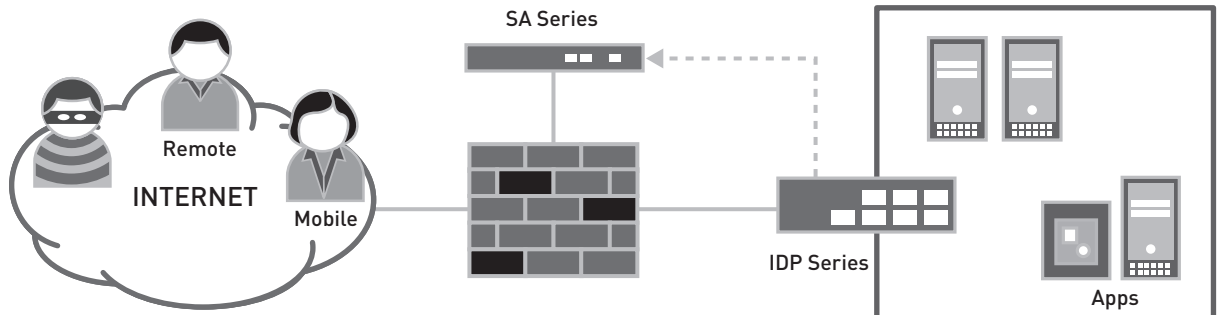
The IDP Series has been specifically designed to:

- Protect against attacks from user to application and from application to user
- Detect and block network worms based on software vulnerabilities
- Detect and block trojans (non-file-based)
- Detect and block communications of spyware/malware
- Detect and block zero-day attacks through the use of anomaly detection
- Stop attack proliferation

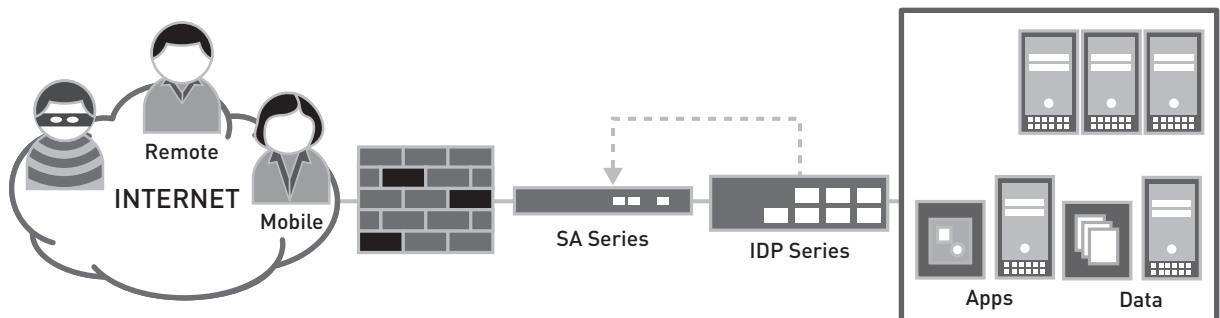
## Description and Deployment Scenario

There are several different deployment options that exist when it comes to Coordinated Threat Control or IDP Series/SA Series integration. The following examples show two of the most commonly deployed scenarios:

1. *Split Deployment:* In this scenario, the customer is using the SA Series for extended enterprise access and the IDP Series appliance for security for all perimeter traffic including but not limited to the traffic coming from the SA Series.



2. *Internal Deployment:* In this scenario, only encrypted SSL traffic terminated at the SA Series has access to the rest of the network and the IDP Series appliance will be inspecting only traffic coming through the SA Series.



There are other possible scenarios like the SA Series and IDP Series in the DMZ, additional IDP Series appliances on an internal network, and others. Instead of being deployed inline, the IDP Series appliance can also be configured in Sniffer mode. Most of these deployment scenarios depend on specific requirements as well as the existing network design (whether there is a DMZ network, how traffic is routed from in and out of the internal network—either via DMZ or is there other traffic not traversing the SA Series, and so on).

The main idea behind any deployment scenario is to make sure encrypted traffic which is terminated at the the SSL VPN device, are inspected by the IDP Series appliance as it continues to internal networks. This way, in the case of malicious content, the IDP Series appliance will signal the SA Series, which in turn implements appropriate restrictive measures as listed above.

### Configuration

This section describes detailed steps required for:

- **Communication Setup**—configuring and establishing a communication channel between the SA Series and IDP Series
- **Action Setup**—configuring the SA Series to perform specific actions upon receiving signal from the IDP Series appliance

### Communication Setup

Communication settings that are required to establish a control session between Coordinated Threat Control components are configured on both the IDP Series appliance and SA Series device. Coordinated Threat Control uses Transport Layer Security (TLS) as the cryptographic protocol to provide secure communication which allows the IPS Sensor to signal the SA Series about relevant security events. Configuration is handled on the SA Series side, but the IDP Series administrator must provide the SA Series administrator with the one-time password (OTP) generated by the sensor in order to establish communications between the devices.

This is done through Appliance Configuration Manager (ACM). After successful login into the Web browser session with the sensor and after selecting ACM, the administrator selects “Configure IDP IVE Server Communication” link which brings up the following configuration page:

**Configure NetScreen-Security Manager Communication**

In this step, you can configure the Sensor to use a NetScreen-Security Manager. Configuration fields in this page are optional.

Additionally, the One Time Password may be reset to authenticate communication between the Sensor and NetScreen-Security Manager.

Provide the requested information below to configure the Sensor to use a NetScreen-Security Manager.

Reset One Time Password?

New One Time Password :  (password is displayed)

Device ID :

Primary NetScreen-Security Manager IP :  Port No:

Secondary NetScreen-Security Manager IP :  Port No:

**Configure IDP IVE Server Communication**

IVE one-time password (IVE OTP) may be reset by the user which is used to authenticate certificates of IDP and IVE.

Reset IVE OTP?

Figure 1: IDP Series configuration

To generate an OTP, the administrator must check the “Reset IVE OTP?” check box and click Next Step. The new IVE OTP will appear on the Final Configuration page at the top, and will be activated once the administrator confirms and applies the changes at the bottom of this page.

**General Configuration**

Hostname: idp200.xy2\_inc.com

Model: NS-IDP-200

Version: 4.1.96964

Config Date: Jul 26, 2007

Config Time: 12:06am

Timezone: PDT

Mode: transparent (enable layer2 bypass)

Serial Number: 0146072006000028

One Time Password: *Already Set*

IVE OTP:

Primary NetScreen-Security Manager IP: 192.168.1.122

Figure 2: One-time password (OTP)

The next step in setting up communication involves configuring the IPS Sensor on the IVE. The administrator selects “New Sensor” from Sensor Configuration Page in IVE Admin UI, and enters the IPS Sensor name, IP address and One-time password. The default Port used is 7103 (TCP).

The screenshot shows the 'New Sensor' configuration page in the IVE Admin UI. The page is titled 'New Sensor' and is part of the 'Sensors' configuration section. The 'Sensor Properties' section includes the following fields:

- Name: IDP200 (Label to reference sensor)
- Hostname: 192.168.1.120 (Hostname or IP address)
- Port: 7103 (Port)
- One-time password: yWES3H7e5Z58jS2GRMyQJ2O11y6W4hby0Z (Used for TLS handshake with sensor)

The 'Monitoring Options' section includes:

- Addresses to monitor: <default> (List of IP addresses to be monitored. (one per line). Examples: <default>, 0.0.0.0/0, 192.168.40.128, 192.168.40.210-245, 192.168.0.0/255.255.0.0, 192.168.10.0/24)
- Severity filter: 3 - Medium

At the bottom, there is a 'Save changes?' section with 'Save Changes' and 'Cancel' buttons.

Figure 3: IVE—new sensor

The administrator can also select which addresses to monitor or leave default settings which include internal IVE interface IPs, aliases, VIPs, Network Connect pools and VLAN addresses, as well as the severity of the events to monitor (for example, which events to ignore based on severity). Administrators will most likely only need to modify this list if the IVE will be issuing/using IP addresses it doesn't yet know about, such as those retrieved from a Dynamic Host Configuration Protocol (DHCP) server like those for NC IPs.

Once the IPS Sensor has been added by selecting “Save Changes” button, in New Sensor configuration page, the IVE will establish a persistent connection to the IPS Sensor using the IP address and the port number specified by the IVE administrator in the IPS configuration page. The OTP is used to encrypt and securely exchange X.509 digital certificates, which will then be used for all IVE-IDP communications going forward. A successfully established connection is indicated on the Sensor Configuration page.

The screenshot shows the 'Configuration' page in the IVE Admin UI, specifically the 'Sensors' tab. The page displays a table of configured sensors. The table has the following columns: Sensor, Address, Enabled, Status, Notes, and IVE.

Sensor	Address	Enabled	Status	Notes	IVE
<input type="checkbox"/> IDP200	192.168.1.120:7103	<input checked="" type="checkbox"/>	Connected	Connected at 2007/07/26 12:19:49 PDT	192.168.1.125

Figure 4: IVE—IDP Series connected

## Action Setup

The SA Series allows the administrator to create IDP-specific policies based on custom expressions.

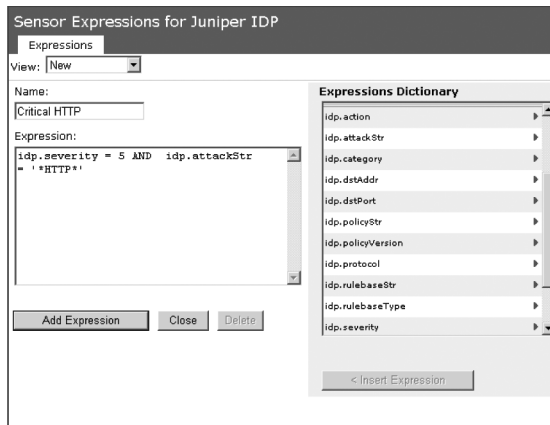


Figure 5: Example of sensor expressions

The administrator then ties these custom IPS attack expressions into the IPS Rule and further identifies the action which is to be performed when a matching event is recognized. The SA Series receives the source and destination IP addresses and port numbers of the attacking machine and the resource against which the attack was launched, along with the attack identifier, severity and time of the attack. Based on the attacker's IP address and port number, the SA Series then uniquely identifies the user's session. As part of defining the IPS policies, the SA Series administrator can choose automatic or manual action for the attacks detected by the IPS Sensor. For manual action, the administrator will have to look at all of the information available on the Active Users page and decide on an action, whereas in the case of an automatic action, the SA Series administrator will have to configure the action in advance while defining the IPS policies.



Figure 6: SA Series actions

As shown in Figure 6, an administrator can configure SA Series to:

1. Ignore the event (just log)—best used for informational attack messages (low severity).
2. Terminate user session—SA Series immediately terminates user session and requires user to sign in to the SA Series again.
3. Disable user account—SA Series disables user profile. User is then unable to sign into SA Series until the administrator re-enables the account (applicable only for local SA Series user accounts).
4. Replace user role (permanently or for active session only)—the SA Series replaces existing user role with another, typically more restrictive role for the duration of the session (unless assignment is selected to be permanent). As part of the process, SA Series can notify user about the event and suggest steps required to remediate the problem.

## Logging

In addition to detailed logs and reports provided by IDP Series management platform (NSM) events, as observed by the SA Series device, are also logged by Juniper Networks NSM Central Manager using the existing SA Series logging mechanism and leveraging existing filtering capabilities.

Note: The SA Series also logs all of the attack responses and actions or role changes it makes.

The screenshot displays the 'Logs' section of the Juniper Networks NSM Central Manager interface. The interface includes a navigation menu on the left, a top header with 'Central Manager on SA1', and a main content area with tabs for Events, User Access, Admin Access, NC Packets, Sensors, Client Logs, SNMP, and Statistics. The Logs section is active, showing a 'View by filter' dropdown set to 'Standard:Standard (default)', a 'Show 200 items' option, and an 'Edit Query' field. Below the query field are buttons for 'Update', 'Reset Query', and 'Save Query...'. Further down are buttons for 'Save Log As...', 'Clear Log', and 'Save All Logs'. A table of logs is displayed with columns for Severity, ID, and Message. The table shows two entries: one with ID IDP24103 and another with ID IDP24107, both dated 2007-08-07 16:04:07.

Severity	ID	Message
Major	IDP24103	2007-08-07 16:04:07 - SA2 - [192.168.1.125] hr(HR)[HR] - User [hr] roles replaced with [Quarantine]
Major	IDP24107	2007-08-07 16:04:07 - SA2 - [192.168.1.125] hr(HR)[HR] - IDP Sensor IDP200 - timestamp=[Tue Aug 7 16:04:05 2007 ] severity=[4] policyStr=[IDP Policy] category=[attack] protocol=[tcp] attackStr=[HTTP:CISCO:IOS-ADMIN-ACCESS] rulebaseStr=[IDS] rulebaseType=[Main Rule Base] srcAddr=[192.168.1.125] srcPort=[32830] dstAddr=[192.168.1.119] dstPort=[80] action=[none] policyVersion=[19] ruleNumber=[2]

Figure 7: SA Series logging

## Summary

One of the missing pieces of traditional remote access end-to-end security stories is the protection of applications and resources to which remote users are provided access. Application protection is a valuable security layer to implement because it can protect against a number of security threats for which the traditional remote access devices do not.

Juniper Networks SA Series SSL VPN Appliances leverage best-in-class IPS technology to provide full protection against a wide range of application and network security threats. This encompasses all of the different types of access that can be provided via the SSL VPN, while at the same time maintains real-time information about the actual user as well as the content being used to mount the attack against internal resources.

This joint solution demonstrates yet another example of how Juniper products can be used to effectively secure and run a high-performance network for a high-performance business.

## 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  
Airsides 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.