Table of Contents

INTRODUCTION........................................................................................................................................................................ 2
SOLUTION AND ADVANTAGES .................................................................................................................................................... 2
INTEGRATION OF FIREWALL AND IPS SOLUTION .................................................................................................................. 2
CONFIGURATION ........................................................................................................................................................................... 5
  OPSEC SAM APPLICATION FOR DEFENSE CENTER / INTRUSION SENSOR ................................................................. 5
  CONNECTING DEFENSE CENTER WITH CHECK POINT SERVER ............................................................................ 6
  CONFIGURING FIREWALL RESPONSES ............................................................................................................................. 8
CONCLUSION .............................................................................................................................................................................. 12
APPENDIX I: DESCRIPTION OF FILTERS ............................................................................................................................... 13

Table of Figures

Figure 1: Interaction between firewall and sensor through defense center ................................................................. 3
Figure 2: Logical Diagram of Integration ............................................................................................................................... 4
Figure 3: OPSEC Application for Defense Center / Intrusion Sensor ........................................................................ 5
Figure 4: Adding an Instance for response to a compliance event ............................................................................... 6
Figure 5: Instance Properties ............................................................................................................................................... 7
Figure 6: Adding OPSEC Peer for response to an intrusion event ................................................................................. 7
Figure 8: Remediation Properties ......................................................................................................................................... 9
Figure 9: Adding Response to Compliance Rules ............................................................................................................. 10
Figure 10: Adding Response to Intrusion Rules ................................................................................................................ 11
Figure 11: Response Properties .......................................................................................................................................... 11
Introduction

Firewalls provide protection between the external networks and internal networks by blocking potentially malicious traffic from entering the internal network infrastructure. However, inherently firewalls need to allow SMTP/email, FTP, SIP/VoIP calls and other protocols with minimal payload security inspection. This also allows external threat-sources to infect internal end-points and use them as threat sources.

Firewall’s deep packet inspection capabilities are not as strong as an Intrusion Prevention solution. Nokia Intrusion Prevention provides the flexibility to interact with Nokia Firewall, providing the most effective strategy for threat mitigation at both the perimeter and deep within the core. This paper explains the interaction between Nokia Intrusion Prevention and Nokia Firewall.

Solution and Advantages

The interaction between firewalls and intrusion sensors will help strong policy enforcement and mitigate attacks and denial of service at the borders of a network; saving resources and avoiding any compromise of the internal network. The interaction provides a mechanism for intrusion sensors to invoke specific firewall rules on a temporary or permanent basis that will block or drop connections traversing the firewall.

An example of Policy Enforcement:
If a corporate policy is not to allow peer-to-peer applications then intrusion sensor’s rules can be enabled that identify this traffic inside the network. These rules then instruct the firewall to prevent further communication between that peer-to-peer client and host for a period of time thus rendering the application useless.

An example of Threat Mitigation:
Usually intrusion sensors can more effectively detect DoS or DDoS attacks than regular firewalls. In such a case, the intrusion sensors would notice any attack missed by a firewall and could instruct the firewall to deny access thus preventing an inadvertent compromise of hosts or intellectual properties on that network.

The interaction between Nokia Intrusion Prevention and Nokia Firewalls also allows for the validation of firewall policies by the intrusion sensors and if desired, enforcement of those policies. This solution is easily implemented without introducing additional costs making firewalls more robust without effecting performance.

Integration of firewall and IPS solution

Sourcefire Defense Center for Nokia is used to manage and correlate data from all the intrusion sensors deployed in the network. Defense Center is configured to interact with the firewall whenever a particular rule is triggered. The interaction takes place in when an event is generated by either Intrusion Prevention & Detection Policy rule or by Compliance Policy rule.
Initially the Nokia Check Point firewalls and the Defense Center must be configured so that they communicate with each other.

Each Check Point firewall that needs to interact with a Defense Center must be configured with a Check Point Suspicious Activity Monitor application/object (OPSEC SAM). This object in the Firewall management server represents a Defense Center.

The Defense Center should be configured with all the firewalls that it will send responses to:

- Responding to the events triggered by the Intrusion Prevention and Detection Policy, an OPSEC peer is created in the policy and the response for each firewall
- Responding to the events triggered by the Compliance Policy, a Check Point OPSEC SAM instance is created in the Policy & Response for each firewall

Figure 1: Interaction between firewall and sensor through defense center
Rules in both Intrusion Prevention and Detection Policy or Compliance Policy are configured to send events to the P&R system if that particular rule is matched or triggered.

- Defense Center’s Policy & Response system then executes responses to the triggered rules. Such a response is called a remediation event.
- Defense Center runs a remediation module (e.g.: Check Point Firewall module, Nessus Scanner etc.) when a compliance policy is violated.
- The Defense Center sends a Check Point Firewall response when rules that are configured for an Intrusion Sensor managed by the Defense Center are triggered.
- The Defense Center sends a Check Point Firewall response by invoking the Check Point Remediation module when a compliance policy is violated.

A remediation handler is a typical task handler in the Defense Center that calls specific loadable modules on the trigger of a rule. These handlers are passed information about the policy that triggered the rule, the rule that was triggered and the network information (ip, port, protocol, etc.) of the hosts that caused the exception.

The handler can then use this information to communicate with the firewalls to create a network intervention to address the intrusion or compliance exception. The network intervention can take many forms as necessary, which will be described in the next section.
Configuration

The following are the main steps involved in configuring the interaction between Nokia Intrusion Prevention and Nokia Firewalls:

- Configure a Check Point OPSEC SAM application in the Check Point server that communicates with the Defense Center / Intrusion Sensor
- After configuring the Check Point application, configure the connection between the Defense Center / Intrusion Sensor and the Check Point server
- Configure the firewall responses to existing rules within a custom policy, and then apply that policy to the Intrusion Sensor

OPSEC SAM Application for Defense Center / Intrusion Sensor

An OPSEC SAM Application is created for Defense Center (for responding to compliance events) and for Intrusion Sensors (for responding to intrusion events). The Application is created in the SmartDashboard’s ‘Manage Menu’
The main things to consider in the above snapshot are,

- In the host field in the above snapshot, **Defense Center** information needs to be added to respond to compliance events.
- In the host field in the above snapshot, **Intrusion Sensor** information needs to be added to respond to intrusion events.
- The Defense Center pushes the response configuration to managed Intrusion Sensors by applying policies that contain the OPSEC Response settings, but does so by managing the peer trust between the Intrusion Sensor and the firewall.
- To establish peer trust Secure Internal Communication needs to be established by using the same key between OPSEC Application and Defense Center.

**Connecting Defense Center with Check Point Server**

There are two type of events that the Defense Center can respond to, so there are two places where Check Point information needs to be configured depending on the type of the event.

**Compliance Event:**
A remediation instance is created for each firewall, to which the Defense Center will be sending responses.

![Policy & Response > Responses > Remediations](Image)

**Figure 4: Adding an Instance for response to a compliance event**

A new instance is added for each firewall. Each instance is created with the firewall details as shown in the snapshot Figure 5. The instance is configured with remediation, which is then added to the desired compliance policy rule.
Intrusion Events:
A peer is created for each firewall, to which the Defense Center will be sending responses.

The trust is managed by Defense Center between the Intrusion Sensors and Check Point Server using the same Activation Key / SIC key.
Configuring Firewall Responses

Responses for Compliance Violations:

Remediation for each instance is created, based on the type of response you want to send to the firewall when compliance policies are violated.

• “OPSEC Block To/From Destination IP/Network Remediations” to block all traffic sent to or received from the destination host or network in a compliance event
• “OPSEC Block To Destination Service Remediations” to block service traffic to the destination host in a compliance event. The blocked service is determined by the protocol and port in the event
• “OPSEC Block To/From Source IP/Network” to block all traffic sent to or received from the source host or network in a compliance event
• “OPSEC Block To Source Service” to block service traffic to the source host in a compliance event. The blocked service is determined by the protocol and port in the event

Available Remediation Types for CheckPoint OPSEC SAM (Select an Instance to Configure a Remediation)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block To/From Destination IP/Network</td>
<td>No description provided</td>
</tr>
<tr>
<td>Block To Destination Service</td>
<td>No description provided</td>
</tr>
<tr>
<td>Block To/From Source IP/Network</td>
<td>No description provided</td>
</tr>
<tr>
<td>Block to Source Service</td>
<td>No description provided</td>
</tr>
</tbody>
</table>

Figure 7: Remediation Types
Each remediation can be configured with the type of response and logging level, which are explained in the tables 1 and 2. A timeout can also be specified, which specifies the life of that particular firewall filter.

**TABLE 1: TYPE OF ACTION FOR REMEDIATION**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify</td>
<td>All connection attempts are logged as specified by the logging attribute. Traffic is not impeded.</td>
</tr>
<tr>
<td>Inhibit</td>
<td>All connection attempts are rejected. Existing connections will continue to function.</td>
</tr>
<tr>
<td>Inhibit and Close</td>
<td>All connection attempts are rejected. Existing connections are closed.</td>
</tr>
<tr>
<td>Drop</td>
<td>All connection attempts are dropped. Existing connections will continue to function.</td>
</tr>
<tr>
<td>Drop and Close</td>
<td>All connection attempts are dropped. Existing connections are closed.</td>
</tr>
<tr>
<td>Log Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Log w/Alert</td>
<td>Keeps more detailed logs along with the event that caused the firewall response</td>
</tr>
<tr>
<td>Log</td>
<td>Performs detailed logging, but does not store the event that caused the firewall response</td>
</tr>
<tr>
<td>None</td>
<td>Does not log firewall responses to this rule</td>
</tr>
</tbody>
</table>

The configured remediation response is added independently to a specific rule in the compliance policy as shown in Figure 9.

**Figure 9: Adding Response to Compliance Rules**

### Responses for Intrusion Events:

Responses for intrusion events are created by editing Intrusion Prevention and Detection policy. Firewall / OPSEC SAM responses are selected for the desired rules within the policy.

The firewall response must be configured independently for each rule. This configuration is saved separately from the rule within a policy, so that any changes to the rule do not change the configured response. When using the Defense Center, the firewall responses are pushed to the managed Intrusion Sensors when the affected policy is applied.
Most of the parameters shown in the snapshot above in the response configuration such as **Logging**, **Action** and **Timeout** are the same as described in the previous section (Table 1 and Table 2) for responses to compliance events, except for the **Filter Type**.

Filters define parameters of traffic against which the specified action is taken. The supported filters apply information from packets that trigger intrusion rules to traffic at the firewall, and take the specified action against those packets. The available filters are described in **APPENDIX I**.
Conclusion

This interaction of firewall applications with Nokia Intrusion Prevention ultimately enables Nokia Check Point firewalls to perform tasks similar to next generation firewalls and emerging ‘intrusion prevention’ devices without requiring a replacement or overhaul of the current architecture and without adding another single point of failure to your network.

This interaction helps to provide enhanced network security tailored for the specific threats customers encounter on their networks with existing security applications.
## APPENDIX I: Description of Filters

<table>
<thead>
<tr>
<th>Filter Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>Performs the action against network traffic that has the same source IP as the packet that triggered the Snort rule.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Performs the specified action against network traffic that has the same destination IP as the packet that triggered the Snort rule.</td>
</tr>
<tr>
<td>Source or Destination IP</td>
<td>Performs the specified action against network traffic that has either the same source IP or destination IP as that of the packet triggering the Snort rule.</td>
</tr>
<tr>
<td>Source IP, Destination IP, and Service</td>
<td>Performs the specified action against network traffic that has the same source IP, destination IP, IP protocol, and destination port as the packet that triggered the Snort rule.</td>
</tr>
<tr>
<td>Destination IP and Service</td>
<td>Performs the specified action against network traffic that has the same destination IP, IP protocol, and destination port as the packet that triggered the Snort rule.</td>
</tr>
<tr>
<td>Source IP and Protocol</td>
<td>Performs the specified action against network traffic that has the same source IP and IP protocol as the packet that triggered the Snort rule.</td>
</tr>
<tr>
<td>Destination IP and Protocol</td>
<td>Performs the specified action against network traffic that has the same destination IP and IP protocol as the packet that triggered the Snort rule.</td>
</tr>
<tr>
<td>Source Network</td>
<td>Performs the specified action against network traffic identified as coming from the same source network as the packet that triggered the Snort rule, calculated using the Source Network Mask attribute specified in the Check Point OPSEC SAM response configuration.</td>
</tr>
<tr>
<td>Destination Network</td>
<td>Performs the specified action against traffic whose destination address matches the destination network, calculated using the Network Mask attribute, of the packet that triggered the Snort rule.</td>
</tr>
<tr>
<td>Source or Destination Network</td>
<td>Performs the specified action against any packet whose source or destination network, calculated using the Network Mask attribute, matches the address of the packet that triggered the Snort rule.</td>
</tr>
<tr>
<td>Source Network and Protocol</td>
<td>Performs the specified action against any network traffic whose source network, calculated using the source Network Mask attribute, and IP protocol match the source network and IP protocol of the packet that triggered the Snort rule.</td>
</tr>
<tr>
<td>Destination Network and Protocol</td>
<td>Performs the specified action against any network traffic whose destination network, calculated using the Destination Network Mask attribute, and IP protocol match the destination network and IP protocol of the packet that triggered the Snort rule.</td>
</tr>
<tr>
<td>Destination Network and Service</td>
<td>Performs the specified action against any network traffic with the same destination network, calculated using the Destination Network Mask attribute, IP protocol, and destination port as the packet that triggered the Snort rule.</td>
</tr>
<tr>
<td>Source Network, Destination IP and Service</td>
<td>Performs the specified action against any network traffic with the same source network, calculated using the Source Network Mask, destination IP, IP protocol, and destination port and the packet that triggered the Snort rule.</td>
</tr>
<tr>
<td>Source IP, Destination Network and Service</td>
<td>Performs the specified action against any network traffic with the same source IP, destination network, calculated using the destination network mask, IP protocol, and destination port of the packet that triggered the Snort rule.</td>
</tr>
</tbody>
</table>