Table of Contents

1 Introduction......................................................................................................................... 5
  1.1 About this document ........................................................................................................ 5
  1.2 Prerequisites .................................................................................................................. 5
  1.3 Additional Documentation .......................................................................................... 5

2 Overview ............................................................................................................................ 6
  2.1 SOAP .......................................................................................................................... 6
  2.2 Transport ..................................................................................................................... 6
  2.3 Authentication & Access Control ................................................................................... 6
  2.4 Addressing ................................................................................................................... 6
  2.5 Example ....................................................................................................................... 7
  2.6 Filter Semantics .......................................................................................................... 8
  2.7 Identifiers .................................................................................................................... 8
  2.8 Building Web Service Requests from the SMC GUI .................................................... 9

3 Reference .......................................................................................................................... 11
  3.1 getDSCTraffic ............................................................................................................. 11
    3.1.1 Request ................................................................................................................ 11
    3.1.2 Response .............................................................................................................. 12
  3.2 getFlows .................................................................................................................... 13
    3.2.1 Request ................................................................................................................ 13
    3.2.2 Response .............................................................................................................. 21
  3.3 getSecurityEvents ....................................................................................................... 27
    3.3.1 Request ................................................................................................................ 27
    3.3.2 Response .............................................................................................................. 29
  3.4 getHostSnapshot ......................................................................................................... 31
    3.4.1 Request ................................................................................................................ 31
    3.4.2 Response .............................................................................................................. 32
  3.5 getHostInformation ...................................................................................................... 49
    3.5.1 Request ................................................................................................................ 49
    3.5.2 Response .............................................................................................................. 53
  3.6 getHostGroups ............................................................................................................ 58
    3.6.1 Request ................................................................................................................ 58
    3.6.2 Response .............................................................................................................. 58
  3.7 setHostGroups .............................................................................................................. 59
    3.7.1 Request ................................................................................................................ 59
    3.7.2 Response .............................................................................................................. 60
  3.8 updateExporters .......................................................................................................... 60
    3.8.1 Request ................................................................................................................ 60
    3.8.2 Response .............................................................................................................. 63
  3.9 removeExporters .......................................................................................................... 63
    3.9.1 Request ................................................................................................................ 63
    3.9.2 Response .............................................................................................................. 64
  3.10 updateExporterSNMPConfiguration ........................................................................... 64
    3.10.1 Request ................................................................................................................ 64
    3.10.2 Response .............................................................................................................. 66
  3.11 addHostGroup .......................................................................................................... 66
    3.11.1 Request ................................................................................................................ 66
    3.11.2 Response .............................................................................................................. 67
  3.12 addHostGroups ......................................................................................................... 67
    3.12.1 Request ................................................................................................................ 68
    3.12.2 Response .............................................................................................................. 69
  3.13 addHostGroupIPRange ............................................................................................. 69

NOTE: ‘getCIEEvents’ is deprecated and has been replaced with ‘getSecurityEvents’ in version 6.

5. The getCIEEvents’ service will not be supported in future releases. ......................... 27
  5.1 Request ...................................................................................................................... 27
  5.2 Response ................................................................................................................... 29

6. Building Web Service Requests from the SMC GUI .................................................... 9
5 Examples of Accessing SMC Web Services

3.13.1 Request ........................................................................................................... 69
3.13.2 Response .......................................................................................................... 69
3.14 addHostGroupIPRanges ........................................................................................ 69
3.14.1 Request ............................................................................................................. 70
3.14.2 Response .......................................................................................................... 70
3.15 removeHostGroup ................................................................................................. 70
3.15.1 Request ............................................................................................................. 70
3.15.2 Response .......................................................................................................... 71
3.16 removeHostGroupIPRange .................................................................................... 71
3.16.1 Request ............................................................................................................. 71
3.16.2 Response .......................................................................................................... 71
3.17 setHostGroupIPRange ........................................................................................... 71
3.17.1 Request ............................................................................................................. 71
3.17.2 Response .......................................................................................................... 72
3.18 getDomain ............................................................................................................. 72
3.18.1 Request ............................................................................................................. 72
3.18.2 Response .......................................................................................................... 72
3.19 addDomain ............................................................................................................ 72
3.19.1 Request ............................................................................................................. 72
3.19.2 Response .......................................................................................................... 76
3.20 removeDomain ....................................................................................................... 77
3.20.1 Request ............................................................................................................. 77
3.20.2 Response .......................................................................................................... 77

4 Appendix .................................................................................................................. 78
4.1 Date & Time Filtering .......................................................................................... 78
4.1.1 Time Range Selection ..................................................................................... 78
4.1.2 Time Window Selection .................................................................................. 78
4.1.3 Day Selection .................................................................................................. 79
4.1.4 Day Range Selection ....................................................................................... 79
4.1.5 Active Time Selection ..................................................................................... 79
4.1.6 First-Last Time Selection ............................................................................... 80
4.2 Device Filtering ................................................................................................... 81
4.2.1 Device List Selection ....................................................................................... 81
4.2.2 Exporter Selection ......................................................................................... 81
4.2.3 Interface Selection .......................................................................................... 81
4.3 Host Filtering ....................................................................................................... 82
4.3.1 Host Group Selection ...................................................................................... 82
4.3.2 IP Address Range Selection ......................................................................... 82
4.3.3 IP Address List Selection ............................................................................... 82
4.3.4 IP Address Selection ...................................................................................... 83
4.3.5 VM Selection .................................................................................................. 83
4.3.6 Host Pair Selection ......................................................................................... 83
4.4 Service Profile Status ......................................................................................... 84
4.5 Alarm Types .......................................................................................................... 85
4.6 Security Event Types ........................................................................................... 89
4.6.1 In previous versions, these were known as CI Events .................................. 89
4.7 ICMP Types ......................................................................................................... 91

5 Examples of Accessing SMC Web Services

5.1 Using 'wget' .......................................................................................................... 93
5.1.1 'getDomain' request example ....................................................................... 93
5.1.2 'getHostSnapshot' request ............................................................................ 93
5.2 Using 'curl' ........................................................................................................... 94
5.2.1 'getHostInformation' request ...................................................................... 94
5.2.2 'getSecurityEvents' request ......................................................................... 94
5.3 Using 'python' ...................................................................................................... 95
5.3.1 'addDomain' request ..................................................................................... 95
1 Introduction

1.1 About this document

This document aims to explain the operation of the StealthWatch Management Console (SMC) Web Service that is present in this version of the SMC product. This guide supports Stealthwatch Enterprise v6.10.x and v7.0.x.

1.2 Prerequisites

It is assumed that the reader is familiar with the following concepts:

- Extensible Markup Language (XML)
- XML Schema Definition (XSD)
- Web Services Description Language (WSDL) version 1.1
- Simple Object Access Protocol (SOAP) version 1.2

1.3 Additional Documentation

While this document serves as a guide to users of the SMC Web Service, the following documents provide the full formal specification of the SMC Web Service:

- SMC Web Service WSDL Definition (sws.wsdl)
- SMC Web Service XML Message Types (sws-message.xsd)
- SMC XML Data Record Types (sws-record.xsd)
- SMC XML Types (sws.xsd)

There is the server-side and the client-side version of these documents. A client should be initialized with the client-side version of the documents. All of the files are located in the following two files. The URL for each file is included.

- Web Services API Schema - Client
  
  https://lancope.my.salesforce.com/sfc/p/#300000000QWy/a/3800000008snF/VhoOCKF_Db3TjpEB_XS2rvcttoeddYFPr41BUUmxm4

- Web Services - Server
  
  https://lancope.my.salesforce.com/sfc/p/#300000000QWy/a/3800000008stX/_LN3Y1NhzFsFBzM78pBnyGoInpEDFM62zbDlkFkOOw
2 Overview

2.1 SOAP

The SMC Web Service uses a single type of binding for service endpoints, or ports, that use the SOAP to transfer XML payloads between the client and the server. The encoding that is used for the XML payload within the SOAP messages is constrained in the following ways:

- The input message has a single part (soap:body has only one child)
- The part is an element
- The element has the same name as the operation
- The element's complex type has no attributes

This style of SOAP-WSDL binding is often termed "document/literal wrapped" and is illustrated in the proceeding examples.

2.2 Transport

The SMC Web Service uses HTTPS (HTTP with TLS) as the transport for the SOAP messages.

2.3 Authentication & Access Control

The SMC Web Service delegates authentication of the client to the HTTP transport. Specifically, the SMC Web Service utilizes HTTP Basic Authentication. The client should use credentials that have been set up on the SMC through the SMC Web Start Client.

Access to data and operations through the SMC Web Service is then restricted by the Data Role and Function Roles assigned to that user.

Please refer to the SMC Online Help for instructions on creating and managing SMC users and roles.

2.4 Addressing

The SMC Web Service WSDL describes the HTTP address for the ports in the following fashion:

```xml
<wsdl:port name="flowsPort" binding="tns:flowsBinding">
  <soap:address location="http://WWW.LANCOPE.COM/smc/swsService/flows" />
</wsdl:port>
```

When addressing this service port in the real world there are two things to note:

1. While the URLs in the WSDL specify the HTTP protocol the SMC Web Service actually uses HTTPS.
2. The URLs in the WSDL specify WWW.LANCOPE.COM as the host. This should be substituted with the IP address or host name of the SMC.

For example, to access the service port defined above for an SMC at 192.168.1.100, the actual URL that the client would use would be:

https://192.168.1.100/smc/swsService/flows
2.5 Example

Let us say that the client would like to access the `getFlows` operation in the `flowsPort` service port. The pertinent part of the WSDL would be:

```xml
<wsdl:message name="getFlowsRequest">
    <wsdl:part name="parameters" element="getFlows" />
</wsdl:message>

<wsdl:message name="getFlowsResponse">
    <wsdl:part name="parameters" element="getFlowsResponse" />
</wsdl:message>

<wsdl:portType name="flows">
    <wsdl:operation name="getFlows">
        <wsdl:input message="tns:getFlowsRequest"  />
        <wsdl:output message="tns:getFlowsResponse" />
    </wsdl:operation>
</wsdl:portType>

<wsdl:binding name="flowsBinding" type="tns:flows">
    <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http" />
    <wsdl:operation name="getFlows">
        <wsdl:input>
            <soap:body use="literal" />
        </wsdl:input>
        <wsdl:output>
            <soap:body use="literal" />
        </wsdl:output>
    </wsdl:operation>
</wsdl:binding>

<wsdl:service name="swsService">
    <wsdl:port name="flowsPort" binding="tns:flowsBinding">
        <soap:address location="http://WWW.LANCOPE.COM/smc/swsService/flows" />
    </wsdl:port>
</wsdl:service>
```

The URL to HTTP POST the request to would be:

```
https://192.168.1.100/smc/swsService/flows
```

The request would be:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<soapenc:Envelope xmlns:soapenc="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:getFlows="http://www.LANCOPE.COM">
    <soapenc:Body>
        <getFlows>
            <!--request payload XML -->
        </getFlows>
    </soapenc:Body>
</soapenc:Envelope>
```
The response would be:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<soapenc:Envelope xmlns:soapenc="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:ns="http://www.example.com">
    <soapenc:Body>
        <getFlowsResponse>
            <!—response payload XML •–>
            </getFlowsResponse>
        </soapenc:Body>
    </soapenc:Envelope>
```

### 2.6 Filter Semantics

The request XML payload to the SMC Web Service is termed a filter and contains a description of the constraints to be placed on the returned results.

It is important to note that, in general the contents of the filters are interpreted through AND logic: the returned results must satisfy ALL of the supplied constraints.

However, in certain cases some sub-set of constraints may follow OR logic: the returned results must satisfy AT LEAST ONE of the supplied constraints. These cases will be highlighted in the proceeding reference section.

### 2.7 Identifiers

The XML documents used in the SMC Web Service use numeric identifiers for various resources or entities. Common numerical IDs used are:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>The ID of a Domain.</td>
<td>Integer</td>
</tr>
<tr>
<td>device-id</td>
<td>The ID of a StealthWatch FlowCollector appliance.</td>
<td>Integer</td>
</tr>
<tr>
<td>host-group-id</td>
<td>The ID of a Host Group.</td>
<td>Integer</td>
</tr>
<tr>
<td>host-group-ids</td>
<td>The IDs of a Host Group. This is a comma-separated list of Host Group IDs</td>
<td>String</td>
</tr>
<tr>
<td>spi</td>
<td>The ID of a service as defined by the Service Definitions.</td>
<td>Integer</td>
</tr>
<tr>
<td>application-id</td>
<td>The ID of an application as defined by the Application Definitions.</td>
<td>Integer</td>
</tr>
</tbody>
</table>

If the user of the SMC Web Service would like to convert these IDs into string names of the resources, then the user must:

1. Launch the SMC Graphical User Interface (GUI) through Java Web Start.
2. Select the Domain of interest from the tree on the left.
3. Right-click and select “Properties”.
4. Select the tab named “Export”.
5. Make sure the option “Export All configuration” is selected.
6. Click “Export” and select a file location.
7. Open the exported XML file in your favorite text editor.
The exported XML file will contain the current configuration of the Domain and may serve as a lookup for the IDs listed above.

2.8 Building Web Service Requests from the SMC GUI

It is possible to extract the XML required for a Web Service call from the SMC GUI. This way you may use the SMC GUI to build and fine-tune a query and then cut-and-paste the generated XML into the code or script that is making the Web Service call.

In order to achieve this, the Java Web Start Console must be visible while the SMC GUI is running:

On Windows:

1. From the “Start” menu, select “Control Panel”.
2. Double-click the “Java” item to open the Java control panel.
3. On the “Advanced” tab, make sure that “Java console” -> “Show console” is enabled.

On Mac OS X:

1. Open the folder “Applications” -> “Utilities” -> “Java”
2. Launch the “Java Preferences” application
3. On the “Advanced” tab, make sure that “Java console” -> “Show console” is enabled.

When you next launch the SMC GUI using Java Web Start, a console window will appear that will show logging information. Part of this information will be the XML for any queries that the SMC GUI is making to
the SMC Server. You can cut-and-paste this XML into the code or script that will make the Web Service call.
3 Reference

3.1 getDSCPTraffic

3.1.1 Request
The request takes the form of a `<dscp-traffic-filter>` XML element

```xml
<dscp-traffic-filter domain-id="104" />
<date-selection>
  :
</date-selection>
<device-selection>
  <interface-selection
device-id="602" exporter-ip="10.10.10.10"
  interface-id="2" />
</device-selection>
</dscp-traffic-filter>
```

The `<dscp-traffic-filter>` element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>ID of the Domain to be queried.</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>

The following sections describe the sub-elements of the `<dscp-traffic-filter>`. These sub-elements must appear in the order described above. The `<date-selection>` sub-element is optional, but the `<device-selection>` sub-element is required.

3.1.1.1 Date and Time Filtering
The request may, optionally, filter the returned records based on date and time:

```xml
<date-selection>
  :
</date-selection>
```

The `<date-selection>` element may contain any of the following sub-elements:

- `time-range-selection`
- `time-window-selection`
- `day-selection`

See 4.1 for more information.

NOTE: If the `<date-selection>` XML is missing, the date/time filter will default to the last 12 hours.

3.1.1.2 Device Filtering
The request will filter the returned records based on the exporter/interface selection. This is a required element:

```xml
<device-selection>
```
<interface-selection . . . />
</device-selection>

The **device-selection** element must contain the sub-element:

- **interface-selection**

  See 4.2.3 for more information.

### 3.1.2 Response

The response takes the form of a **dscp-traffic-list** element that contains zero or more **dscp-traffic** elements:

```xml
<dscp-traffic-list>
  <dscp-traffic
    domain-id="116"
    device-id="130"
    retention="300"
    exporter-ip="10.10.10.10"
    if-index="2"
    time="2012-07-12T12:30:00Z"
    dscp="10"
    traffic-in"46296"
    traffic-out"47214" />
</dscp-traffic-list>
```

The **dscp-traffic** element contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>The ID of the Domain in which the traffic was reported.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>device-id</td>
<td>The ID of the StealthWatch FlowCollector which reported this traffic.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>retention</td>
<td>The time duration (in seconds) of the reported traffic.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>exporter-ip</td>
<td>The exporter that observed this traffic.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>if-index</td>
<td>The interface of the exporter that observed this traffic.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>time</td>
<td>The end time that the traffic was observed.</td>
<td>ISO8601</td>
<td>Date</td>
</tr>
<tr>
<td>dscp</td>
<td>The DSCP(differentiated services code point) value associated with this traffic.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>traffic-in</td>
<td>Traffic reported as bps that is received by an interface on a DiffServ-aware router in the monitored network.</td>
<td>Long</td>
<td>Optional</td>
</tr>
<tr>
<td>traffic-out</td>
<td>Traffic reported as bps that is sent by the interface on a DiffServ-aware router in the monitored network.</td>
<td>Long</td>
<td>Optional</td>
</tr>
</tbody>
</table>
3.2 getFlows

3.2.1 Request

The request takes the form of a `flow-filter` XML element:

```xml
<flow-filter max-rows="100"
  domain-id="104"
  remove-duplicates="true"
  order-by="TOTAL_PACKETS"
  order-by-desc="true" />

<date-selection>
  :
</date-selection>

<device-selection>
  :
</device-selection>

<host-selection>
  :
</host-selection>

<services>. .</services>

<ports>. .</ports>

<protocols>. .</protocols>

<applications>. .</applications>

<traffic>
  :
</traffic>

<network-performance>
  :
</network-performance>

<as-numbers>. .</as-numbers>

<dscps>. .</dscps>

<vlan-ids>. .</vlan-ids>

<mpls-labels>. .</mpls-labels>

<client-ports>. .</client-ports>

<query>
  :
</query>

<flow-action.denied</flow-action>
</flow-filter>
```
The **flow-filter** element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>ID of the Domain to be queried.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>max-rows</td>
<td>The maximum number of rows to be returned in the response.</td>
<td>Integer</td>
<td>Optional Default of 2000</td>
</tr>
<tr>
<td>remove-duplicates</td>
<td>De-duplicate flows capability</td>
<td>Boolean</td>
<td>Optional Default of false</td>
</tr>
<tr>
<td>order-by</td>
<td>Valid values are:</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>TOTAL_BYTES,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOTAL_PACKETS,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOTAL_BYTE_RATE,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOTAL_PACKET_RATE,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CLIENT_BYTES,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CLIENT_PACKETS,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CLIENT_BYTE_RATE,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CLIENT_PACKET_RATE,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SERVER_BYTES,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SERVER_PACKETS,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SERVER_BYTE_RATE,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SERVER_PACKET_RATE,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RTT_MINIMUM,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RTT_AVERAGE,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RTT_MAXIMUM,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SRT_MINIMUM,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SRT_AVERAGE,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SRT_MAXIMUM,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CONNECTIONS,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RETRANSMITS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>order-by-desc</td>
<td>This specified whether order-by value is processed in descending(true) or ascending(false) order</td>
<td>Boolean</td>
<td>Required if order-by exists</td>
</tr>
<tr>
<td>include-interface-data</td>
<td>Allows you to determine whether or not interface data is included in your flow query.</td>
<td>Boolean</td>
<td>Optional Default of true</td>
</tr>
</tbody>
</table>

The following sections describe the sub-elements of the **flow-filter**. These sub-elements are optional and must appear in the order described above.

### 3.2.1.1 Date and Time Filtering

**NOTE:** If the `<date-selection>` xml is missing, the date/time filter will default to the last 5 minutes.

The request may, optionally, filter the returned records based on date and time:

```xml
<date-selection>
```
The \textit{date-selection} element must contain one of the following sub-elements:

- \textit{time-range-selection}
  See 4.1.1 for more information.
- \textit{time-window-selection}
  See 4.1.2 for more information.
- \textit{day-selection}
  See 4.1.3 for more information.

\subsection{3.2.1.2 Device Filtering}

The request may, optionally, filter the returned records based on the associated device or devices:

\begin{verbatim}
<device-selection> :
</device-selection>
\end{verbatim}

The \textit{device-selection} element must contain one of the following sub-elements:

- \textit{device-list-selection}
  See 4.2.1 for more information.
- \textit{exporter-selection}
  See 4.2.2 for more information.
- \textit{interface-selection}
  See 4.2.3 for more information.

\subsection{3.2.1.3 Host Filtering}

The request may, optionally, filter the returned records based on the associated host or hosts, Host Groups, VM servers, VMs, IP Address Ranges:

\begin{verbatim}
<host-selection> :
</host-selection>
\end{verbatim}

The \textit{host-selection} element must contain the following sub-element:

- \textit{host-pair-selection}
  See 4.3.6 for more information.

\subsection{3.2.1.4 Services Filtering}

The request may, optionally, filter the returned records based on the user-defined services:

\begin{verbatim}
<services exclude="false">1,2,3,4,26</services>
\end{verbatim}

The \textit{services} element contains a comma separated list of SPIs (service profile ids). By looking at the exported configuration, you can determine the SPI. Find the \textit{services-definitions} element, then find the \textit{service} name attribute of the \textit{services} element that you are looking for. The associated profile attribute will contain the SPI needed for this filter.

The \textit{services} element supports the following attribute:
### 3.2.1.5 Ports Filtering

The request may, optionally, filter the returned records based on the UDP/TCP port:

```
<ports exclude="true">53/tcp,53/udp</ports>
```

The `ports` element contains a comma separated list of port/protocol values. The value for the protocol portion is either TCP or UDP. The value for the port is the actual port number.

The `ports` element supports the following attribute:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>exclude</td>
<td>Specify whether to include (=false) or exclude (=true) the flows with the ports/protocols specified.</td>
<td>Boolean</td>
<td>Optional Default is ‘false’</td>
</tr>
</tbody>
</table>

NOTE: If the exclude attribute is ‘false’, then a flow is considered to match this constraint if it matches AT LEAST ONE of the specified ports/protocols. If the exclude attribute is ‘true’, then a flow is considered to match this constraint if it the flow does NOT match any of the ports/protocols.

### 3.2.1.6 Protocols Filtering

The request may, optionally, filter the returned records based on the IP protocol:

```
<protocols exclude="true">6,34,114</protocols>
```

The `protocols` element contains a comma-separated list of protocol numbers. The values for the protocol numbers are the actual raw value.

The `protocols` element supports the following attribute:
### Name | Description | Type | Use
--- | --- | --- | ---
eclude | Specify whether to include (=false) or exclude (=true) the flows with the protocols specified. | Boolean | Optional Default is ‘false’

**NOTE:** If the exclude attribute is ‘false’, then a flow is considered to match this constraint if it matches AT LEAST ONE of the specified protocols. If the exclude attribute is ‘true’, then a flow is considered to match this constraint if it the flow does NOT match any of the protocols specified.

#### 3.2.1.7 Applications Filtering

The request may, optionally, filter the returned records based on the user-defined applications:

```xml
<applications exclude="false">129,165,124</applications>
```

The `applications` element contains a comma separated list of Application IDs. By looking at the exported config, you can determine the application id. Find the `application-list` element, and then find the `name` attribute of the `application` element that you are looking for. The associated `id` attribute will contain the application id needed for this filter.

The `applications` element supports the following attribute:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
</table>
eclude | Specify whether to include (=false) or exclude (=true) the flows with the applications specified | Boolean | Optional Default is ‘false’ |

**NOTE:** If the exclude attribute is ‘false’, then a flow is considered to match this constraint if it matches AT LEAST ONE of the specified applications. If the exclude attribute is ‘true’, then a flow is considered to match this constraint if it the flow does NOT match any of the applications specified.

#### 3.2.1.8 Traffic Statistics Filtering

The request may, optionally, filter the returned records based on traffic statistics:

```xml
<traffic>
  <client>
    <bytes-range low-value="100" high-value="20000" />
    <packets-range low-value="100" high-value="20000" />
  </client>
  <server>
    <bytes-range high-value="20000" />
    <packets-range low-value="100" high-value="20000" />
  </server>
  <total>
    <bytes-range low-value="100" />
    <packets-range low-value="100" high-value="20000" />
  </total>
</traffic>
```

The `traffic` element contains constraints on the byte and packets count on the flow for the client, server or total. Each constraint must contain one or more of the following attributes:
The attributes are interpreted as follows:

- If the low-value is not present, then the constraint is interpreted as LESS THAN the high-value.
- If the high-value is not present, then the constraint is interpreted as GREATER THAN the low-value.
- If both attributes are preset, then the constraint is interpreted as BETWEEN the two values.

3.2.1.9 Network Performance Statistics Filtering

The request may, optionally, filter the returned records based on network performance statistics:

```xml
<network-performance>
  <total-connections low-value="1" high-value="2" />
  <total-retransmissions low-value="1" high-value="2" />
  <round-trip-time>
    <min low-value="1" high-value="2" />
    <avg low-value="1" high-value="2" />
    <max low-value="1" high-value="2" />
  </round-trip-time>
  <server-response-time>
    <min low-value="1" high-value="2" />
    <avg low-value="1" high-value="2" />
    <max low-value="1" high-value="2" />
  </server-response-time>
</network-performance>
```

The network-performance element contains constraints on the performance statistics maintained for each flow. Each constraint must contain one or more of the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>low-value</td>
<td>Lower bound for the constraint.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>high-value</td>
<td>Upper bound for the constraint.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
</tbody>
</table>

The attributes are interpreted as follows:

- If the low-value is not present, then the constraint is interpreted as LESS THAN the high-value.
- If the high-value is not present, then the constraint is interpreted as GREATER THAN the low-value.
- If both attributes are preset, then the constraint is interpreted as BETWEEN the two values.

NOTE: The unit for the time values is milliseconds.
3.2.1.10 Autonomous System Number (ASN) Filtering
The request may, optionally, filter the returned records based on ASN:

\[
<\text{as-numbers exclude="true"}>11</\text{as-numbers}>
\]

The `as-numbers` element simply contains a comma-separated list of the ASNs of interest.

The `as-numbers` element supports the following attribute:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>exclude</td>
<td>Specify whether to include (=false) or exclude (=true) the as-numbers.</td>
<td>Boolean</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default is 'false'</td>
</tr>
</tbody>
</table>

NOTE: If the `exclude` attribute is 'false', then a flow is considered to match this constraint if it matches AT LEAST ONE of the specified as-numbers. If the `exclude` attribute is 'true', then a flow is considered to match this constraint if the flow does NOT match any of the as-numbers specified.

NOTE: This constraint should only be used if the device selected in the `device-selection` is a StealthWatch FlowCollector for NetFlow appliance. Otherwise an error will be returned.

3.2.1.11 Differentiated Services Code Point (DSCP) Filtering
The request may, optionally, filter the returned records based on DSCP:

\[
<dscps>28,18,12</dscps>
\]

The `dscps` element simply contains a comma-separated list of the DSCPs of interest.

The `dscps` element supports the following attribute:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>exclude</td>
<td>Specify whether to include (=false) or exclude (=true) the dscps.</td>
<td>Boolean</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default is 'false'</td>
</tr>
</tbody>
</table>

NOTE: If the `exclude` attribute is 'false', then a flow is considered to match this constraint if it matches AT LEAST ONE of the specified DSCPs. If the `exclude` attribute is 'true', then a flow is considered to match this constraint if the flow does NOT match any of the DSCPs specified.

3.2.1.12 Virtual LAN IDs Filtering
The request may, optionally, filter the returned records based on Virtual LAN IDs:

\[
<vlan-ids>1,2,3</vlan-ids>
\]

The `vlan-ids` element simply contains a comma-separated list of the Virtual LAN IDs of interest.
The `vlan-ids` element supports the following attribute:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>exclude</td>
<td>Specify whether to include (=false) or exclude (=true) the VLAN IDs.</td>
<td>Boolean</td>
<td>Optional Default is 'false'</td>
</tr>
</tbody>
</table>

NOTE: If the exclude attribute is 'false', then a flow is considered to match this constraint if it matches AT LEAST ONE of the specified VLAN IDs. If the exclude attribute is 'true', then a flow is considered to match this constraint if the flow does NOT match any of the VLAN IDs specified.

### 3.2.1.13 MPLS Labels Filtering

The request may, optionally, filter the returned records based on MPLS labels

```
<mpls-labels>9321,45782</mpls-labels>
```

The `mpls-labels` element simply contains a comma-separated list of the Virtual LAN IDs of interest.

The `mpls-labels` element supports the following attribute:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>exclude</td>
<td>Specify whether to include (=false) or exclude (=true) the MPLS labels.</td>
<td>Boolean</td>
<td>Optional Default is 'false'</td>
</tr>
</tbody>
</table>

NOTE: If the exclude attribute is 'false', then a flow is considered to match this constraint if it matches AT LEAST ONE of the specified MPLS labels. If the exclude attribute is 'true', then a flow is considered to match this constraint if the flow does NOT match any of the MPLS labels specified.

### 3.2.1.14 Client Ports Filtering

The request may, optionally, filter the returned records based on MPLS labels:

```
<client-ports>53921,65421</client-ports>
```

The `client-ports` element simply contains a comma-separated list of the client ports of interest.

The `client-ports` element supports the following attribute:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>exclude</td>
<td>Specify whether to include (=false) or exclude (=true) the client ports.</td>
<td>Boolean</td>
<td>Optional Default is 'false'</td>
</tr>
</tbody>
</table>

NOTE: If the exclude attribute is 'false', then a flow is considered to match this constraint if it matches AT LEAST ONE of the specified client ports. If the exclude attribute is 'true', then a flow is considered to match this constraint if the flow does NOT match any of the client ports specified.

### 3.2.1.15 Payload Filtering

The request may, optionally, filter the returned records based contents of the payload:
<query>
  <payload-match-all>get</payload-match-all>
  <payload-match-any>ssh</payload-match-any>
  <payload-not-match-all>dns</payload-not-match-all>
</query>

The query element supports 3 sub-elements for matching text in payloads as seen above in the sample, and are described below.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>payload-match-all</td>
<td>This element will appear for each string in match request. All strings must be found for this flow to be selected</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>payload-match-any</td>
<td>This element will appear for each string in match request. If any one of the strings are found, this flow will be selected</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>payload-not-match-all</td>
<td>This element will appear for each string in match request. All strings must match in order for the flow to be ignored</td>
<td>String</td>
<td>Optional</td>
</tr>
</tbody>
</table>

NOTE: Both client and server payloads are examined in the query.

3.2.1.16 Flow Action
The request may, optionally, filter the returned records based on the Cisco ASA flow-action of permitted or denied:

    <flow-action>permitted</flow-action>

The flow-action element simply contains one of 2 values: permitted or denied.

3.2.2 Response
The response takes the form of a flow-list element that contains zero or more flow elements:

    <flow-list>
      <flow>
        <client>...
          ...
        </client>
        <server>...
          ...
        </server>
        <application>...
          ...
        </application>
      </flow>
    </flow-list>

The flow element contains the following attributes:
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>A unique number that identifies the flow.</td>
<td>Long</td>
<td>Required</td>
</tr>
<tr>
<td>domain-id</td>
<td>The ID of the Domain in which the observation was made.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>device-id</td>
<td>The ID of the StealthWatch FlowCollector appliance that made this observation.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>start-time</td>
<td>The time at which this flow began. ISO8601 Date</td>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>last-time</td>
<td>The time at which this flow was last observed to be active. ISO8601 Date</td>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>active-duration</td>
<td>The number of seconds the flow has been active.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>protocol</td>
<td>The protocol number</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>service-id</td>
<td>The id of the service that this flow is using as defined by the Service Definitions for the Domain.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>application-id</td>
<td>The application that this flow is using as defined by the Application Definitions for the Domain.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>service</td>
<td>The UDP or TCP port number that defines the service used by this flow.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>connections</td>
<td>The number of TCP connections that occur during a flow.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>retransmits</td>
<td>The number of TCP packets that were retransmitted during the flow.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>vlan-id</td>
<td>The number identifying a virtual LAN associated with the flow.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>mpls-label</td>
<td>The Multi-Protocol Label Switching label associated with the flow.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>total-bytes</td>
<td>The total payload bytes transmitted by both client and server.</td>
<td>Long</td>
<td>Optional</td>
</tr>
</tbody>
</table>

The **client** and **server** sub-elements will both exist and can look like this:

```
<client> or <server>
  <flags. . ./>
  <payload. . ./>
  <interface-list>
  <interface. . ./>
  ...
  </interface-list>
</client> or </server>
```

The **client** and **server** sub-elements contain the following attributes:
### Name | Description | Type | Use
--- | --- | --- | ---
ip-address | The IP address of the host. | String | Required
xlate-ip-address | The translated IP address (i.e., as altered by a network address translation device) of the host. | String | Optional
host-name | The name of the host. | String | Optional
country | The country that the host belongs to. | String | Optional
host-group-ids | The comma separated list of Host Group IDs of the Host Groups that the host belongs to. | String | Required
vserver-id | The VM server id on which this host exists. | Integer | Optional
vserver-ip-address | The VM server ip-address on which this host exists. | String | Optional
vserver-name | The VM server name on which this host exists. | String | Optional
vmachine-id | The virtual machine id associated with the host. | Integer | Optional
vmachine-name | The virtual machine name associated with the host. | String | Optional
mac-address | The MAC address observed for this host. | String | Optional
port | The last TCP or UDP port number used by the host to receive packets. | Integer | Required
xlate-port | The port used by the translated host. | Integer | Required
bytes | The number of bytes sent by the host. | Long | Required
packets | The number of packets sent by the host. | Packets | Required
asn | The ASN associated with the client/server. NOTE: this attribute will only have a meaningful value if a StealthWatch FlowCollector for NetFlow observed the flow. | Long | Optional

There are 3 sub-elements that may be included in the client and the server sub-elements, the flags sub-element, the interface-list sub-element and the payload sub-element. These will be described in the sections below.

#### 3.2.2.1 Flags
Each of the client and server elements also contains a flags sub-element that contains the following attributes:

### Name | Description | Type | Use
--- | --- | --- | ---
syn | The number of TCP packets sent by the host with the SYN header flag set. | Integer | Optional
### 3.2.2 Exporters

Both the `client` and `server` elements may contain an `interface-list` element that describes the interfaces that have seen this flow in the given direction:

```xml
<flow>
  <id>120448</id>
  <domain-id>117</domain-id>
  <device-id>118</device-id>
  <start-time>2011-04-07T11:48:30Z</start-time>
  <last-time>2011-04-07T11:48:30Z</last-time>
  <active-duration>0</active-duration>
  <protocol>17</protocol>
  <service-id>64</service-id>
  <application-id>170</application-id>
  <service>1027</service>
  <client>
    <ip-address>11.11.166.53</ip-address>
    <host-group-ids>61627</host-group-ids>
    <country>US</country>
    <port>63081</port>
    <bytes>4314800</bytes>
    <packets>700</packets>
    <asn>46554</asn>
    <flags syn="0" syn-ack="0" rst="0" fin="0"/>
    <interface-list>
      <interface>
        <exporter-ip>10.10.10.10</exporter-ip>
        <if-index>1</if-index>
        <direction>OUTBOUND</direction>
        <bytes>1401408</bytes>
        <packets>216</packets>
      </interface>
      <interface>
        <exporter-ip>10.10.10.10</exporter-ip>
        <if-index>2</if-index>
        <direction>OUTBOUND</direction>
        <bytes>4314800</bytes>
        <packets>700</packets>
      </interface>
    </interface-list>
  </client>
  <server>
    <ip-address>12.12.173.120</ip-address>
    <host-group-ids>61627</host-group-ids>
    <country>US</country>
    <port>1027</port>
    <bytes>1401408</bytes>
    <packets>216</packets>
    <asn>47440</asn>
    <flags syn="0" syn-ack="0" rst="0" fin="0"/>
    <interface-list>
      <interface>
        <exporter-ip>10.10.10.10</exporter-ip>
        <if-index>1</if-index>
        <direction>INBOUND</direction>
        <bytes>4314800</bytes>
        <packets>700</packets>
        <dscp>0</dscp>
      </interface>
    </interface-list>
  </server>
</flow>
```
The interface element contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>exporter-ip</td>
<td>The IP address of the NetFlow or sFlow exporter that observed this flow.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>if-index</td>
<td>The index number of the interface that this flow traversed.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>dscp</td>
<td>The DSCP associated with the client/server. NOTE: this attribute will only have a meaningful value if a StealthWatch FlowCollector for NetFlow observed the flow.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>direction</td>
<td>The direction is one of 2 values: INBOUND for data received by the interface, or OUTBOUND for data sent by the interface.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>bytes</td>
<td>The total number of bytes sent by this interface</td>
<td>Long</td>
<td>Optional</td>
</tr>
<tr>
<td>packets</td>
<td>The total number of packets sent by this interface</td>
<td>Long</td>
<td>Optional</td>
</tr>
<tr>
<td>min-ttl</td>
<td>The smallest number of host/links over which the first packet from this host may be routed.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>max-ttl</td>
<td>The largest number of host/links over which the first packet from this host may be routed.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>flow-action</td>
<td>If the exporter type is Cisco ASA then this value will be present and values will be either 'permitted' or 'denied'</td>
<td>String</td>
<td>Optional</td>
</tr>
</tbody>
</table>

3.2.2.3 Packet Data

There may be additional data in the flow describing actual packet data sampled from the flow:

```
<flow
   id="80049"
   domain-id="117"
   device-id="118"
   start-time="2011-04-07T08:10:34Z"
   last-time="2011-04-07T08:15:16Z"
   active-duration="282000"
   protocol="6"
   service-id="3"
   application-id="39"
   service="80"
   connections="1"
   retransmits="0">
```
Both the client and server elements contain a payload element that contains the first 26 bytes from the first packet observed from that host. The data is provided in ASCII format.

### 3.2.2.4 Application Data

The application element is a sub-element of the flow element and can contain the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>flowsensor</td>
<td>The id of the application that was discovered by the Flowsensor application discovery process.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>nbar</td>
<td>The id of the application that was discovered by examining the CISCO netflow data.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>packetshaper</td>
<td>The id of the application that was discovered by examining the data sent by the PacketShaper Appliance.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
</tbody>
</table>

**NOTE:** The ID’s returned above are explicit to the source of the application discovery.
3.2.2.5 Performance Statistics

The \texttt{rtt} and \texttt{srt} elements are both sub-elements of the \texttt{flow} element. Each of these elements can contain the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min</td>
<td>The average of the least amounts of time in milliseconds.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>Max</td>
<td>The average of the greatest amounts of time in milliseconds</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>Avg</td>
<td>The average amount of time in milliseconds</td>
<td>Integer</td>
<td>Optional</td>
</tr>
</tbody>
</table>

3.3 getSecurityEvents

\textbf{NOTE:} \texttt{getCiEvents} is deprecated and has been replaced with \texttt{getSecurityEvents} in version v6.5. The \texttt{getCiEvents} service will not be supported in future releases.

3.3.1 Request

The request takes the form of a \texttt{security-event-filter} XML element:

\begin{verbatim}
<security-event-filter max-rows="2000" domain-id="104">
  <date-selection>
  : 
  </date-selection>
  <device-selection>
  : 
  </device-selection>
  <host-selection>
  : 
  </host-selection>
  <types> .. </types>
  <ports> .. </ports>
  <hit-count .. />
  <ci-points .. />
</security-event-filter>
\end{verbatim}

The \texttt{security-event-filter} element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>ID of the Domain to be queried.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>max-rows</td>
<td>The maximum number of rows to be returned in the response.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
</tbody>
</table>

The following sections describe the sub-elements of the \texttt{security-event-filter}. These sub-elements are optional and must appear in the order described above.

3.3.1.1 Date and Time Filtering

The request may, optionally, filter the returned records based on time:

\begin{verbatim}
<date-selection>
\end{verbatim}
The `date-selection` element must contain one of the following sub-elements:

- `active-time-selection`
  See 4.1.5 for more information.
- `first-last-time-selection`
  See 4.1.6 for more information.

### 3.3.1.2 Device Filtering

The request may, optionally, filter the returned records based on the associated device or devices:

```xml
<device-selection> 
  
</device-selection>
```

- `device-list-selection`
  See 4.2.1 for more information.

### 3.3.1.3 Host Filtering

The request may, optionally, filter the returned records based on associated the host or hosts:

```xml
<host-selection> 
  
</host-selection>
```

The `host-selection` element can contain the `host-pair-selection`. See 4.3.6 for more information.

### 3.3.1.4 Security Event Type Filtering

The request may, optionally, filter the returned records based on Security Event type:

```xml
<types>50,49,2,20,23,44</types>
```

The `types` element is simply a comma separated list of Security Event Type IDs. See 4.6 for the list of Security Events and the corresponding IDs.

### 3.3.1.5 Port Filtering

The request may, optionally, filter the returned records based on TCP or UDP port number:

```xml
<ports>33-55/udp,77/tcp</ports>
```

The `ports` element contains a comma separated list of port/protocol values. The value for the protocol portion is either TCP or UDP. The value for the port is the actual port number.

### 3.3.1.6 Hit Count Filtering

The request may, optionally, filter the returned records based on the number of hits that occurred.

```xml
<hit-count low-value="10" high-value="200" />
```
The hit-count sub-element contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>low-value</td>
<td>Lower bound for the constraint.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>high-value</td>
<td>Upper bound for the constraint.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
</tbody>
</table>

The attributes are interpreted as follows:

- If the low-value is not present, then the constraint is interpreted as LESS THAN the high-value.
- If the high-value is not present, then the constraint is interpreted as GREATER THAN the low-value.
- If both attributes are preset, then the constraint is interpreted as BETWEEN the two values.

### 3.3.1.7 Concern Index Filtering

The request may, optionally, filter the returned records based on the value of the value of the Concern Index.

```xml
<ci-points low-value="3" high-value="4" />  
```

The ci-points sub-element contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>low-value</td>
<td>Lower bound for the constraint.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>high-value</td>
<td>Upper bound for the constraint.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
</tbody>
</table>

The attributes are interpreted as follows:

- If the low-value is not present, then the constraint is interpreted as LESS THAN the high-value.
- If the high-value is not present, then the constraint is interpreted as GREATER THAN the low-value.
- If both attributes are preset, then the constraint is interpreted as BETWEEN the two values.

### 3.3.2 Response

The response takes the form of a security-event-list element that contains zero or more security-event elements:

```xml
<security-event-list>  
  <security-event  
    domain-id="117"  
    device-id="118"  
    start-time="2011-04-07T04:01:56Z"  
    last-time="2011-04-07T16:43:56Z"  
    ci-points="492984"  
    total-hits="988">  
    <source  
      ip-address="128.9.160.132"  
      host-group-ids="61627"  
      host-name="jar.isi.edu"  
      country="US" />
  </security-event>
</security-event-list>
```
<target
    ip-address="209.182.184.0"
    host-group-ids="1519"
    country="US" />
<details-list>
    <details type="21" hit-count="984" ci-points="49984" />
    <details type="1" hit-count="4" ci-points="0" />
</details-list>
</security-event>
</security-event-list>

The `security-event` element contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Unique ID assigned to the Security Event: NOT IN real output</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>domain-id</td>
<td>The ID of the Domain in which the observation was made.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>device-id</td>
<td>The ID of the StealthWatch FlowCollector appliance that made this observation.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>start-time</td>
<td>The time at which this Security Event began.</td>
<td>ISO8601</td>
<td>Required</td>
</tr>
<tr>
<td>last-time</td>
<td>The time at which this Security Event was last observed to be active.</td>
<td>ISO8601</td>
<td>Required</td>
</tr>
<tr>
<td>ci-points</td>
<td>The total number of Concern Index points that were generated by the Security Event.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>total-hits</td>
<td>The total number of hits generated during the Security Event.</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>

The `source` and `target` sub-elements contain the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>The IP address of the host.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>host-name</td>
<td>The name of the host.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>country</td>
<td>The country that the host belongs to.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>host-group-ids</td>
<td>The IDs of the Host Groups that the host belongs to.</td>
<td>String</td>
<td>Required</td>
</tr>
</tbody>
</table>

The `details-list` element contains one or more `details` elements that break down the Security Event by type. Each `details` element contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>The ID of the Security Event type. See 4.6 for more information.</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>
hit-count | The number of hits for this particular Security Event type. | Integer | Required
---|---|---|---
ci-points | The Concern Index points for this particular Security Event type. | Integer | Required

3.4 getHostSnapshot

3.4.1 Request
The request takes the form of a `host-filter` XML element:

```xml
<host-filter domain-id="104">
  <date-selection>:
  </date-selection>
  <device-selection>:
  </device-selection>
  <host-selection>:
  </host-selection>
</host-filter>
```

The `host-filter` element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
</table>
| domain-id | ID of the Domain to be queried.          | Integer | Required

The following sections describe the sub-elements of the `host-filter`. These sub-elements are optional and must appear in the order described above.

3.4.1.1 Date and Time Filtering
The request may, optionally, filter the returned records based on time:

```xml
<date-selection>:
  </date-selection>
```

The `date-selection` element must contain one of the following sub-elements:

- `day-selection`
  See 4.1.3 for more information.

3.4.1.2 Device Filtering
The request may, optionally, filter the returned records based on the associated device or devices:

```xml
<device-selection>:
  </device-selection>
```

The `device-selection` element must contain one of the following sub-elements:
• device-list-selection
  See 4.2.1 for more information.

3.4.1.3 Host Filtering
The request must specify the host of interest:

```xml
<host-selection>
  <ip-address-selection value="10.202.4.131"/>
</host-selection>
```

The `host-selection` element must contain one of the following sub-elements:

• ip-address-selection
  See 4.3.4 for more information.

3.4.2 Response
The response takes the form of a `host-snapshot` element:

```xml
<host-snapshot
domain-id="117"
ip-address="10.202.15.73"
host-group-ids="154,1545"
host-name="vcenter.lancope.local"
country="XR"
time="2011-04-07T17:47:40Z">
<status-list>
  :
</status-list>
<host-information-list>
  :
</host-information-list>
<security-list>
  :
</security-list>
<touched-list>
  :
</touched-list>
<traffc-list>
  :
</traffic-list>
<ci-events>
  :
</ci-events>
<flows>
  :
</flows>
<exporters>
  :
</exporters>
<alarm-counts-list>
  :
</alarm-counts-list>
<alarm-list>
  :
</alarm-list>
<identity-session-list>
  :
```
The host-snapshot element contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>The ID of the Domain in which the observation was made.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>ip-address</td>
<td>The IP address of the host.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>host-name</td>
<td>The name of the host.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>country</td>
<td>The country that the host belongs to.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>host-group-ids</td>
<td>The IDs of the Host Groups that the host belongs to.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>time</td>
<td>The timestamp of when the request was made</td>
<td>ISO8601 Date</td>
<td></td>
</tr>
</tbody>
</table>

The optional sub-elements contain various information regarding the behavior of the host during the time specified in the filter and will be described in the subsequent sections.

### 3.4.2.1 Status

The response may contain a status-list element:

```xml
<status-list>
  <status
domain-id="104"
device-id="117"
value="active"
first-seen="2010-12-12T20:09:45Z"
last-seen="2011-02-06T18:21:00Z">
    <mac-address value="00:1e:13:80:d0:c0" vendor="Unknown Vendor"/>
  </status>
  :  
:  
</status-list>
```

The status element contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>The ID of the Domain in which the observation was made.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>device-id</td>
<td>The ID of the StealthWatch FlowCollector appliance that made this observation.</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>
value | The current status of the host. | Enumeration of “active”, “inactive” or “phantom” | Required
---|---|---|---
first-seen | The time at which this host was first observed. | ISO8601 Date | Required
last-seen | The time at which this host was last observed. | ISO8601 Date | Required

Optionally, there could be `mac-address` sub-element that contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>The MAC address observed for this host.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>vendor</td>
<td>The name of the vendor that is assigned this MAC address.</td>
<td>String</td>
<td>Optional</td>
</tr>
</tbody>
</table>

### 3.4.2.2 Host Information

The response may contain a `host-information-list` element:

```xml
<host-information-list>
  <host-information
domain-id="117"
device-id="118"
ip-address="10.202.15.73" host-group-ids="154,1545" host-name="vcenter.lancope.local"
country="XR">
    <service-profile-status>
      <server>1:S60256,S60264,S3,012489/tcp</server>
      <client>1:S4,S1,S29,S48,S23,S36,S14,S34,S3</client>
    </service-profile-status>
    <application-activity>
      <server>,186,170,169,168,</server>
      <client>,51,186,171,187,184,185,190,188,58,</client>
    </application-activity>
    <os>1897979539</os>
  </host-information>
</host-information-list>
```

The `host-information` element contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>The ID of the Domain in which the observation was made.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>device-id</td>
<td>The ID of the StealthWatch FlowCollector appliance that made this observation.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>ip-address</td>
<td>The IP address of the host.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>host-group-ids</td>
<td>The IDs of the Host Groups that the host belongs to.</td>
<td>String</td>
<td>Required</td>
</tr>
</tbody>
</table>
### 3.4.2.3 Security

The response may contain a `security-list` element:

```xml
<security-list>
  <security domain-id="104" device-id="117"
    concern-index value="8875685" threshold="1000000"/>
  <target-index value="15910" threshold="50000"/>
  <file-sharing-index value="91161000" threshold="500000"/>
</security-list>
```

The `security` element contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>The ID of the Domain in which the observation was made.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>device-id</td>
<td>The ID of the StealthWatch FlowCollector appliance that made this observation.</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>

Each sub-element of the `security` element describes the status of the Concern Index, Target Index and File Sharing Index for the host and contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>The current value of the index.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>threshold</td>
<td>The alarm threshold that is currently in effect for the index.</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>

### 3.4.2.4 Touched

The response may contain a `touched-list` element:

```xml
<touched-list>
  <touched domain-id="115" device-id="252"
    been-touched="false" has-touched="true"/>
</touched-list>
```
The `touched` element contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>The ID of the Domain in which the observation was made.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>device-id</td>
<td>The ID of the StealthWatch FlowCollector appliance that made this observation.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>been-touched</td>
<td>Indicates if this host has communicated with a host with High Concern Index.</td>
<td>Boolean</td>
<td>Required</td>
</tr>
<tr>
<td>has-touched</td>
<td>Indicates if this host has a High Concern Index value and has communicated with other hosts.</td>
<td>Boolean</td>
<td>Required</td>
</tr>
</tbody>
</table>

### 3.4.2.5 Traffic

The response may contain a `traffic-list` element:

```xml
<traffic-list>
  <traffic domain-id="117" device-id="118">
    <five-min threshold="100000000" udp-percent="2">
      <in max-bps="119976" />
      <out max-bps="8424" />
    </five-min>
    <day threshold="3000000000" data-loss-threshold="0">
      <in>
        total-bytes="4656110"
        total-packets="5633"
        total-data-bytes="4431414"
      </in>
      <out>
        total-bytes="739394"
        total-packets="3682"
        total-data-bytes="593242"
      </out>
      data-loss="0" />
    </day>
  </traffic>
</traffic-list>
```

The `traffic` element contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>The ID of the Domain in which the observation was made.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>device-id</td>
<td>The ID of the StealthWatch FlowCollector appliance that made this observation.</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>

The `traffic` element contains 2 sub-elements: `five-min` and `day`. 
The 5-min element contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold</td>
<td>The current value for the 'High Traffic in 5 min' setting</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>udp-percent</td>
<td>The percentage of traffic that used the UDP protocol</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>

The 5-min element contains 2 sub-elements: **in** and **out**. Each of these contains the following attribute:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-bps</td>
<td>The highest number of bits per second the host has received(in) or sent(out) for any 5 minute interval over the last 24 hours</td>
<td>Integer</td>
<td>Optional</td>
</tr>
</tbody>
</table>

The day element contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold</td>
<td>The current value for the &quot;High Total Traffic in 24 hrs&quot; setting</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>data-loss-threshold</td>
<td>The threshold for the Suspect Data Loss alarm, as set on the policy.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
</tbody>
</table>

The day element contains 2 sub-elements: **in** and **out**. Each of these contain the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total-bytes</td>
<td>The total number of bytes that the host has sent(out) or received(in), including the IP and TCP header, over the last 24 hours.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>Total-packets</td>
<td></td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>Total-data-bytes</td>
<td>The total number of bytes of payload information that the host has sent(out) or received(in) over the last 24 hours.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>Total-loss</td>
<td>The cumulative amount of suspected data loss by the host on the corresponding appliance since the last archive hour.</td>
<td>Integer</td>
<td>Optional 'out' element only</td>
</tr>
</tbody>
</table>

3.4.2.6 CI Events

The response may contain a **ci-events** element:

```
<ci-events>
  <source-high-ci-list>
    <ci-event ..>
  ...
</source-high-ci-list>
</ci-events>
```
The ci-events element may contain 3 sub-elements that contain lists of CI Events in the format described in 3.3.2.

### 3.4.2.7 Flows

The response may contain a flows element:

```xml
<flows>
  <most-recent>
    <flow connected="10.202.25.46"
       connected-host-group-ids="154,1545"
       start-time="2011-04-07T21:34:16Z"
       last-time="2011-04-07T21:34:16Z"
       protocol="tcp"
       service="https"
       service-id="4"
       bytes-sent="4506"
       bytes-received="2324"
       pkts-sent="20"
       pkts-received="22"
       average-bps="0"
       role="Server"
       total-conn="1"
       total-retrans="1"
       min-rtt="1"
       max-rtt="1"
       avg-rtt="1"
       min-srt="3"
       max-srt="3"
       avg-srt="3"
  
    </flow>
  
    <flow ..> ...
  
  </most-recent>

  <highest-traffic>
    <flow ..> ...
  
  </highest-traffic>

</flows>
```

The flow element contains the following attributes:
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>The IP address of the other host in the flow.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>connected-host-group-ids</td>
<td>The IDs of the Host Groups that the other host belongs to.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>connected-vm</td>
<td>The IP address of the host with which the subject host communicated during the flow.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>start-time</td>
<td>The time at which this flow began.</td>
<td>ISO8601 Date</td>
<td>Required</td>
</tr>
<tr>
<td>last-time</td>
<td>The time at which this flow was last observed to be active.</td>
<td>ISO8601 Date</td>
<td>Required</td>
</tr>
<tr>
<td>protocol</td>
<td>The IP protocol used in the flow.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>service</td>
<td>The service used in the flow.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>service-id</td>
<td>The service used in the flow.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>bytes-sent</td>
<td>The number of bytes sent by this host.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>bytes-received</td>
<td>The number of bytes received by this host.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>pkts-sent</td>
<td>The number of bytes sent by this host.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>pkts-received</td>
<td>The number of bytes received by this host.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>average-bps</td>
<td>The average rate of traffic (in bits per second) between the hosts in the flow.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>role</td>
<td>The role of this host in the flow.</td>
<td>Enumeration of &quot;Client&quot;, &quot;Server&quot; or &quot;Undetermined&quot;</td>
<td>Required</td>
</tr>
<tr>
<td>total-conn</td>
<td>The Total TCP Connections from the first SYN to the last ACK that occur during the flow.</td>
<td>Long</td>
<td>Optional</td>
</tr>
<tr>
<td>total-retrans</td>
<td>The percentage of TCP packets that were retransmitted during the flow</td>
<td>Long</td>
<td>Optional</td>
</tr>
<tr>
<td>min-rtt</td>
<td>The Minimum Round-Trip Time (in milliseconds) required for all the TCP connections to occur in the flow.</td>
<td>Long</td>
<td>Optional</td>
</tr>
<tr>
<td>max-rtt</td>
<td>The Maximum Round-Trip Time (in milliseconds) required for all the TCP connections to occur in the flow.</td>
<td>Long</td>
<td>Optional</td>
</tr>
<tr>
<td>avg-rtt</td>
<td>The Average Round-Trip Time (in milliseconds) required for all the TCP connections to occur in the flow.</td>
<td>Long</td>
<td>Optional</td>
</tr>
<tr>
<td>min-srt</td>
<td>The Minimum Server Response Time (in milliseconds) between the first client request and the first server response among.</td>
<td>Long</td>
<td>Optional</td>
</tr>
</tbody>
</table>
### 3.4.2.8 Exporters

The response may contain an `exporters` element:

```xml
<exporters>
  <closest-interface-list>
    <closest-interface
      domain-id="115"
      device-id="252"
      exporter-ip="11.9.102.4"
      if-index="833"
      confidence="100"/>
    <closest-interface ../>
  </closest-interface-list>
  <active-source-list>
    <interface-status
      domain-id="115"
      device-id="252"
      exporter-ip="11.8.1.101"
      if-index="9">
      <inbound
        current-bps="662"
        maximum-bps="1293"
        average-bps="0"
        current-pps="0"
        maximum-pps="0"
        average-pps="0"
        current-util="0"
        maximum-util="0"/>
      <outbound
        current-bps="662"
        maximum-bps="0"
        average-bps="0"
        current-pps="0"
        maximum-pps="0"
        average-pps="0"
        current-util="0"
        maximum-util="0"/>
    </interface-status>
    <interface-status ../>
    ...
  </active-source-list>
</exporters>
```
The exporters element contains the following sub-elements:

- closest-interface-list
  Determination of which Exporter and Interface is closest to the host.
- active-source-list
  List of Interfaces that have seen inbound traffic with this host as the source.
- active-dest-list
  List of Interfaces that have seen outbound traffic with this host as the destination.
- today-list
  List of Interfaces that have seen any traffic to or from this host.

The closest-interface-list element contains one or more closest-interface elements that each has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>The ID of the Domain in which the observation was made.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>device-id</td>
<td>The ID of the StealthWatch FlowCollector appliance that made this observation.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>exporter-ip</td>
<td>The IP address of the exporter that observed this host.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>if-index</td>
<td>The index number of the Interface that passed traffic for this host.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>confidence</td>
<td>The confidence level, in percent, with the closest interface determination.</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>

The active-source-list, active-dest-list and today-list all contain one or more interface-status elements that each have the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>The ID of the Domain in which the observation was made.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>device-id</td>
<td>The ID of the StealthWatch FlowCollector appliance that made this observation.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>exporter-ip</td>
<td>The IP address of the exporter that observed this host.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>if-index</td>
<td>The index number of the Interface that passed traffic for this host.</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>
In addition, the `interface-status` element contains an `inbound` and `outbound` element that each has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>current-bps</td>
<td>The current traffic rate (in bits per second) through the interface.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>maximum-bps</td>
<td>The highest traffic rate (in bits per second) through the interface over the time period requested.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>average-bps</td>
<td>The average traffic rate (in bits per second) through the interface over the time period requested.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>current-pps</td>
<td>The current packet rate (in packets per second) through the interface.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>maximum-pps</td>
<td>The highest packet rate (in packets per second) through the interface over the time period requested.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>average-pps</td>
<td>The average packet rate (in packets per second) through the interface over the time period requested.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>current-util</td>
<td>The current interface utilization (in percent).</td>
<td>Double</td>
<td>Required</td>
</tr>
<tr>
<td>maximum-util</td>
<td>The highest interface utilization (in percent) over the time period requested.</td>
<td>Double</td>
<td>Required</td>
</tr>
</tbody>
</table>

### 3.4.2.9 Alarm Counts

The response may contain an `alarm-counts-list` element:

```xml
<alarm-counts-list>
  <alarm-counts domain-id="104" device-id="117" source="13" target="0">
    <details alarm-type="7" source="11" target="0"/>
    <details alarm-type="16" source="2" target="0"/>
  </alarm-counts>
  ...
  <alarm-counts ..>
  ...
</alarm-counts-list>
```

The `alarm-counts-list` element contains one or more `alarms-counts` elements that have the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>The ID of the Domain in which the observation was made.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>device-id</td>
<td>The ID of the StealthWatch FlowCollector appliance that made this observation.</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>
source | The number of alarms active during the requested time period, where this host was the Source. | Integer | Required
---|---|---|---
target | The number of alarms active during the requested time period, where this host was the Target. | Integer | Required

Each `details` sub-element of the `alarm-counts` element then breaks down the counts by Alarm Type and has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>alarm-type</td>
<td>The ID of the Alarm Type.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>source</td>
<td>The number of alarms active during the requested time period, where this host was the Source.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>target</td>
<td>The number of alarms active during the requested time period, where this host was the Target.</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>

### 3.4.2.10 Alarms

The response may contain an `alarm-list` element:

```xml
<alarm-list>
  <alarm
    domain-id="101"
    device-id="103"
    id="2V-13BN-VMSF-XY9K-K"
    type="35"
    start-time="2011-03-09T23:34:00Z"
    end-time="2011-03-10T00:19:00Z"
    active="false">
    <source ip-address="192.168.1.40"
      host-group-ids="11,28"
      country="US"/>
    <target ip-address="192.168.1.50"
      host-group-ids="11,25"
      country="XR"/>
  </alarm>
  ...
</alarm-list>
```

The `alarm-list` element contains one or more `alarm` elements that have the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>The ID of the Domain in which the observation was made.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>device-id</td>
<td>The ID of the StealthWatch FlowCollector appliance that made this observation.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>id</td>
<td>The globally unique ID of the alarm.</td>
<td>String</td>
<td>Required</td>
</tr>
</tbody>
</table>
The `alarm` element contains a `source` and/or `target` sub-element that each has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>The IP address of the host.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td><code>host-name</code></td>
<td>The name of the host.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td><code>country</code></td>
<td>The country that the host belongs to.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td><code>host-group-ids</code></td>
<td>The IDs of the Host Groups that the host belongs to.</td>
<td>String</td>
<td>Required</td>
</tr>
</tbody>
</table>

### 3.4.2.11 Identity Session

The response may contain an `identity-session-list` element:

```xml
<identity-session-list>
  <identity-session
domain-id="101"
device-id="170"
ip-address="192.168.3.100"
host-group-ids="11,15"
host-name="some.hostname.local."
country="XR"
calendar-start-time="2011-03-10T12:31:26Z"
calendar-end-time="2011-03-10T18:06:28Z"
active="false"
username="bob"
_vlan="v-1234"
device-type="phone"
ad-domain="ms-domain"
vpn-ip="10.202.1.96">
  <mac-address value="00:ab:cd:ef:12:34" vendor="Acme Inc."/>
  <network-access-device ip-address="192.168.1.10"
    name="ms-activedirectory"
    interface="interface-name"/>
  <user-groups identity="group1" security="group2"/>
  <server ip-address="10.202.1.1" name="dev"/>
</identity-session>
</identity-session-list>
```

The `identity-session-list` element contains one or more `identity-session` elements that have the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>domain-id</code></td>
<td>The ID of the Domain in which the observation was made.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Use</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>device-id</td>
<td>The ID of the Cisco ISE appliance that made this observation.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>ip-address</td>
<td>The IP address of the host.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>host-name</td>
<td>The name of the host.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>host-group-ids</td>
<td>The IDs of the Host Groups that the host belongs to.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>country</td>
<td>The country that the host belongs to.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>start-time</td>
<td>The time at which the session started.</td>
<td>ISO8601 Date</td>
<td>Required</td>
</tr>
<tr>
<td>end-time</td>
<td>The time at which the session ended.</td>
<td>ISO8601 Date</td>
<td>Optional</td>
</tr>
<tr>
<td>active</td>
<td>Indication if the session was active at the time of the request.</td>
<td>Boolean</td>
<td>Required</td>
</tr>
<tr>
<td>username</td>
<td>The username used for this session.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>vlan</td>
<td>The user’s assigned VLAN</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>device-type</td>
<td>The endpoint’s device type as detected by the NAC profiler.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>ad-domain</td>
<td>The user’s Active Directory domain</td>
<td>String</td>
<td>Optional</td>
</tr>
</tbody>
</table>

The `identity-session` element contains four sub-elements that describe the authentication server and Windows domain used for the session.

The `mac-address` element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>The MAC address of the host requesting the DHCP lease.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>vendor</td>
<td>The name of the vendor that has been assigned the MAC address.</td>
<td>String</td>
<td>Optional</td>
</tr>
</tbody>
</table>

The `network-access-device` element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>The IP address of the endpoint’s network attachment device.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>name</td>
<td>The DNS name of the endpoint’s network attachment device.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>interface</td>
<td>Then endpoint’s network attachment port.</td>
<td>String</td>
<td>Optional</td>
</tr>
</tbody>
</table>

The `user-groups` element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>identity</td>
<td>The user’s provisioned group (OU in LDAP, for instance)</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>security</td>
<td>The user’s TrustSec SGT group</td>
<td>String</td>
<td>Optional</td>
</tr>
</tbody>
</table>

The `server` element has the following attributes:
### 3.4.2.12 User Activity

The response may contain a `user-activity-list` element:

```xml
<user-activity-list>
  <user-activity>
    domain-id="101"
    device-id="170"
    ip-address="192.168.3.100"
    host-group-ids="11,15"
    host-name="some.hostname.local."
    country="XR"
    start-time="2011-03-10T12:31:26Z"
    end-time="2011-03-10T18:06:28Z"
    active="false"
    username="bob">
      <server ip-address="192.168.1.10" name="ms-activedirectory"/>
      <domain name="AD" controller="MSACTDIR"/>
  </user-activity>
  ...
</user-activity-list>
```

The `user-activity-list` element contains one or more `user-activity` elements that have the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>The ID of the Domain in which the observation was made.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>device-id</td>
<td>The ID of the StealthWatch IDentity appliance that made this observation.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>ip-address</td>
<td>The IP address of the host.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>host-name</td>
<td>The name of the host.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>host-group-ids</td>
<td>The IDs of the Host Groups that the host belongs to.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>country</td>
<td>The country that the host belongs to.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>start-time</td>
<td>The time at which the login session started.</td>
<td>ISO8601 Date</td>
<td>Required</td>
</tr>
<tr>
<td>end-time</td>
<td>The time at which the login session ended.</td>
<td>ISO8601 Date</td>
<td>Optional</td>
</tr>
<tr>
<td>active</td>
<td>Indication if the session was active at the time of the request.</td>
<td>Boolean</td>
<td>Required</td>
</tr>
<tr>
<td>user-name</td>
<td>The username used for this session.</td>
<td>String</td>
<td>Required</td>
</tr>
</tbody>
</table>
The user-activity element contains two sub-elements that describe the authentication server and Windows domain used for the session. The server element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>The IP address of the server providing the authentication data.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>name</td>
<td>The name given to the server providing the authentication data.</td>
<td>String</td>
<td>Required</td>
</tr>
</tbody>
</table>

The domain element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name of the Windows domain that the user logged into.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>controller</td>
<td>The name of the Windows domain controller associated with the domain that the user logged into.</td>
<td>String</td>
<td>Optional</td>
</tr>
</tbody>
</table>

3.4.2.13 DHCP Lease

The response may contain dhcp-lease-list element:

```xml
<dhcp-lease-list>
  <dhcp-lease>
    domain-id="101"
    device-id="391"
    ip-address="192.168.3.100"
    host-group-ids="11"
    host-name="some.hostname.local."
    country="XR"
    start-time="2011-12-11T05:45:57Z"
    end-time="2011-12-18T05:48:13Z"
    active="false">
    <server name="dhcptest1"/>
    <client mac-address="00:ab:cd:ef:12:34" vendor="Acme Inc."/>
  </dhcp-lease>
  ...
  <dhcp-lease>
  ...
</dhcp-lease-list>
```

The dhcp-lease-list element contains one or more dhcp-lease elements that have the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>The ID of the Domain in which the observation was made.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>device-id</td>
<td>The ID of the StealthWatch IDentity appliance that made this observation.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>ip-address</td>
<td>The IP address of the host.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>host-name</td>
<td>The name of the host.</td>
<td>String</td>
<td>Optional</td>
</tr>
</tbody>
</table>
The \texttt{host-group-ids} element contains two sub-elements that describe the DHCP lease assigning server and the client that requested the lease. The \texttt{server} element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name given to the server assigning the DHCP leases.</td>
<td>String</td>
<td>Required</td>
</tr>
</tbody>
</table>

The \texttt{client} element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address</td>
<td>The MAC address of the host requesting the DHCP lease.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>vendor</td>
<td>The name of the vendor that has been assigned the MAC address.</td>
<td>String</td>
<td>Optional</td>
</tr>
</tbody>
</table>

### 3.4.2.14 Host Notes

The response may contain a \texttt{host-notes-list} element:

```xml
<host-note-list>
  <host-note
    domain-id="104"
    ip-address="10.202.4.131"
    host-group-ids="11"
    country="XR",
    time="2011-02-05T20:10:18Z",
    user="admin">This host needs to be tracked.</host-note>
  ...
</host-note-list>
```

The \texttt{host-note-list} element contains one or more \texttt{host-note} elements that have the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>The ID of the Domain in which the observation was made.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>ip-address</td>
<td>The IP address of the host.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>host-name</td>
<td>The name of the host.</td>
<td>String</td>
<td>Optional</td>
</tr>
</tbody>
</table>
### host-group-ids

The IDs of the Host Groups that the host belongs to.

- **Type**: String
- **Use**: Required

### country

The country that the host belongs to.

- **Type**: String
- **Use**: Required

### time

The time at which the note was added.

- **Type**: ISO8601
- **Use**: Required

### user

The name of the user that added the note

- **Type**: String
- **Use**: Required

The text content of the `host-note` element is the actual text of the note.

### 3.5 `getHostInformation`

#### 3.5.1 Request

The request takes the form of a `host-information-filter` XML element:

```xml
<host-information-filter domain-id="101">
  <date-selection>...</date-selection>
  <device-selection>...</device-selection>
  <host-selection>...</host-selection>
  <server-service-list ..></server-service-list>
  <server-application-list ..></server-application-list>
  <client-service-list ..></client-service-list>
  <client-application-list ..></client-application-list>
  <operating-system ..>..</operating-system>
  <alarms ..>..</alarms>
  <alerts ..>..</alerts>
  <ci-events ..>..</ci-events>
</host-information-filter>
```

The `host-information-filter` element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>ID of the Domain to be queried.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>max-rows</td>
<td>The maximum number of rows to be returned in the response.</td>
<td>Integer</td>
<td>Optional Default of 2000</td>
</tr>
</tbody>
</table>

The following sections describe the sub-elements of the `host-information-filter`. These sub-elements are optional and must appear in the order described above.

#### 3.5.1.1 Date and Time Filtering

The request may, optionally, filter the returned records based on time:
The `date-selection` element must contain one of the following sub-elements:

- `day-range-selection`
  See 4.1.4 for more information.

### 3.5.1.2 Device Filtering

The request may, optionally, filter the returned records based on the associated device or devices:

```xml
<device-selection>
  :
</device-selection>
```

The `device-selection` element must contain one of the following sub-elements:

- `device-list-selection`
  See 4.2.1 for more information.

### 3.5.1.3 Host Filtering

The request may, optionally, filter the returned records based on the associated host or hosts, Host Groups, VM servers, VMs, IP Address Ranges:

```xml
<host-selection>
  :
</host-selection>
```

The `host-selection` element must contain one of the following sub-elements:

- `host-group-selection`
  See 4.3.1 for more information.
- `ip-address-range-selection`
  See 4.3.2 for more information.
- `ip-list-selection`
  See 4.3.3 for more information.
- `vm-list-selection`
  See 4.3.5 for more information.
- `host-pair-selection`
  See 4.3.6 for more information.

### 3.5.1.4 Service Filtering

The request may, optionally, filter the returned records based on the TCP/UDP services observed for a host as a Client and/or Server

```xml
<server-service-list operator="AND">
  <profiled-service-list>
    <profiled-service profile-index="93" />
    <profiled-service profile-index="76" />
  </profiled-service-list>
  <custom-service-list>
    <custom-service protocol="tcp" port-number="123-456" />
    <custom-service protocol="udp" port-number="100-102" />
  </custom-service-list>
</server-service-list>
```
The server-service-list and client-service-list elements contain the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>operator</td>
<td>Specifies how a host is matched to the specified services.</td>
<td>Enumeration of &quot;AND&quot; or &quot;OR&quot;</td>
<td>Required</td>
</tr>
</tbody>
</table>

The server-service-list and client-service-list contains 2 list elements that specify the services of interest in one of two ways.

The profiled-service-list element contains profiled-service elements. The element specifies a service as defined in the Service Definitions for the Domain and contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile-index</td>
<td>The index as specified in the Service Definitions for the Domain.</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>

The custom-service-list element contains custom-service elements. The element specifies a service using the protocol and port/port-range and contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol</td>
<td>The protocol of the service.</td>
<td>Enumeration of &quot;tcp&quot; or &quot;udp&quot;</td>
<td>Required</td>
</tr>
<tr>
<td>port-number</td>
<td>The port/port-range associated with this service. e.g. &quot;8080&quot;, &quot;100-200&quot;</td>
<td>String</td>
<td>Required</td>
</tr>
</tbody>
</table>

### 3.5.1.5 Protocol Filtering

Protocol filtering is now done with the profiled-service element, instead of a separate XML tag.

For example, in order to add a filter by protocol of 4, add the constant 60000 to the raw protocol number to get 60004 for the profile-index of the profiled-service element.

To filter by ICMP type, you add the constant 60256 to the raw ICMP type. See 4.7 for a list of ICMP Types.
### 3.5.1.6 Operating System Filtering

The request may, optionally, filter the returned records based on the operating system that the host is using:

\[
<\text{operating-system} \text{ operator}="\text{AND}">503331,1493595250</\text{operating-system}>
\]

The `operating-system` elements contain the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>operator</td>
<td>Specifies how a host is matched to the specified OSs.</td>
<td>Enumeration of &quot;AND&quot; or &quot;OR&quot;</td>
<td>Required</td>
</tr>
</tbody>
</table>

The `operating-system` element simply contains a comma-separated list of the operating system codes of interest.

**NOTE:** This constraint should only be used if the device selected in the `device-selection` is a FlowCollector for sFlow appliance.

### 3.5.1.7 Alarm Filtering

The request may, optionally, filter the returned records based on the type of Alarms that have been active for a host:

\[
<\text{alarms} \text{ operator}="\text{AND}">1,20,7</\text{alarms}>
\]

The `alarms` elements contain the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>operator</td>
<td>Specifies how a host is matched to the specified Alarm types.</td>
<td>Enumeration of &quot;AND&quot; or &quot;OR&quot;</td>
<td>Required</td>
</tr>
</tbody>
</table>

The `alarms` element simply contains a comma-separated list of the Alarm type IDs of interest. See 4.5 for more information.

### 3.5.1.8 Alert Filtering

The request may, optionally, filter the returned records based on the type of Alerts that have been active for a host:

\[
<\text{alerts} 2,9,27</\text{alarms}>
\]

The `alerts` elements contain the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>operator</td>
<td>Specifies how a host is matched to the specified Alert types.</td>
<td>Enumeration of &quot;AND&quot; or &quot;OR&quot;</td>
<td>Required</td>
</tr>
</tbody>
</table>

The `alerts` element simply contains a comma-separated list of the Alert type IDs of interest. See Error! Reference source not found. for more information.
3.5.1.9 CI Event Filtering

The request may, optionally, filter the returned records based on the type of CI Events that have been active for a host:

```xml
<ci-events>33,37,43</ci-events>
```

The `ci-events` elements contain the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>operator</td>
<td>Specifies how a host is matched to the specified CI Event types.</td>
<td>Enumeration of &quot;AND&quot; or &quot;OR&quot;</td>
<td>Required</td>
</tr>
</tbody>
</table>

The `ci-events` element simply contains a comma-separated list of the CI Event type IDs of interest. See 4.6 for more information.

3.5.2 Response

The response takes the form of a `host-information-list` element that contains zero or more `host-information` elements:

```xml
<host-information-list>
  <host-information
      domain-id="102"
      device-id="104"
      ip-address="10.202.10.20"
      host-group-ids="11"
      host-name="somehostname.something.com"
      country="XR"
      time="2011-08-11T20:19:34Z"
      mac-address="00:0b:db:08:a8:79">
    <service-profile-status>
    </service-profile-status>
    <application-activity>
    </application-activity>
    <os>..</os>
    <traffic>
    </traffic>
    <total-traffic ../>
    <high-traffic ../>
    <low-traffic ../>
    <concern-index ../>
    <target-index ../>
    <file-sharing-index ../>
    <new-flows-initiated ../>
    <new-flows-served ../>
    <max-flows-initiated ../>
    <max-flows-served ../>
    <syns-received ../>
    <syns ../>
    <udp ../>
    <icmp ../>
    <ci-events> .. </ci-events>
    <closest-interface ../>
  </host-information>
</host-information-list>
```
The *host-information* element contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>The ID of the Domain to which this host belongs.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>device-id</td>
<td>The ID of the StealthWatch FlowCollector appliance that made this observation.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>ip-address</td>
<td>The IP address of the host.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>host-name</td>
<td>The name of the host.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>country</td>
<td>The country that the host belongs to.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>host-group-ids</td>
<td>The IDs of the Host Groups that the host belongs to.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>vserver-id</td>
<td>The VM server id on which this host exists.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>vserver-ip-address</td>
<td>The VM server ip-address on which this host exists.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>vserver-name</td>
<td>The VM server name on which this host exists.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>vmachine-id</td>
<td>The virtual machine id associated with the host.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>vmachine-name</td>
<td>The virtual machine name associated with the host.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>time</td>
<td>The time associated with this observation</td>
<td>ISO8601</td>
<td>Date</td>
</tr>
<tr>
<td>mac-address</td>
<td>The MAC address observed for this host.</td>
<td>String</td>
<td>Optional</td>
</tr>
</tbody>
</table>

The optional sub-elements contains various information regarding the behavior of the host during the time specified in the filter.

### 3.5.2.1 Service Profile

The response may contain a *service-profile-status* element that describes the services that have been observed for the host as either a Server or Client:

```xml
<service-profile-status>
  <server>1:S16,S22</server>
  <client>1:S12,S23,S27,S80</client>
</service-profile-status>
```

See 4.4 for details of the format.
3.5.2.2 Application Activity
The response may contain an application-activity element that describes the applications that have been observed for the host as either a Server or Client:

```
<application-activity>
  <server>,169,</server>
  <client>,51,171,169,184,168,81,175,39,53,41,44,</client>
</application-activity>
```

The server or client sub-elements simply contain a comma-separated list of the application-ids as defined in the Services and Applications Configuration Dialog.

3.5.2.3 Alarms
The response may contain an alarms element that describes the alarms that have been observed for the host:

```
<alarms>24,32</alarms>
```

The alarms element simply contains a comma-separated list of the host alarm ids. See 4.5 table for list of valid alarm ids.

3.5.2.4 Alerts
The response may contain an alerts element that provides the alerts that have been observed for the host:

```
<alerts>5,22,28</alerts>
```

The alerts element simply contains a comma-separated list of the alert ids. See the Error! Reference source not found. table for list of valid alert ids.

3.5.2.5 Operating System
The response may contain an os element that describes the Operating Systems that have been observed for the host:

```
<os>1897979539</os>
```

NOTE: This element may only be present if a FlowCollector for sFlow appliance made the observation.

3.5.2.6 Traffic Statistics
The response will contain a traffic element that describes the inbound and outbound traffic observed for the host:

```
<traffic>
  <in bytes="281869267" packets="1955487" max="64720"></in>
  <out bytes="338649938" packets="2299743" max="64760"></out>
</traffic>
```

NOTE: This element may only be present if an FlowCollector for sFlow appliance made the observation.

The traffic element contains an in and out element that contains the following attributes:
### Name | Description | Type | Use
--- | --- | --- | ---
bytes | The total number of payload bytes inbound/outbound to the host during the day. | Long | Required
packets | The total number of IP packets inbound/outbound to the host during the day. | Long | Required
max | The maximum observed inbound/outbound traffic rate (bits per second) during the day. | Integer | Required

#### 3.5.2.7 Policy Statistics
The response will contain a number of elements that describe the statistics that are tracked with respect to a number of the alarms:

```xml
<total-traffic max="620519205"/>
<data-loss max="1262"/>
<high-traffic max="126212" average="84379"/>
<low-traffic max="3874" average="84379"/>
<concern-index max="0"/>
<target-index max="0"/>
<file-sharing-index max="0"/>
<br new-flows-initiated max="0" average="0"/>
<br new-flows-served max="0" average="0"/>
<br max-flows-initiated max="0" average="0"/>
<br max-flows-served max="0" average="0"/>
<br syns-received max="0" average="0"/>
<br ipv6 max="0" average="0"/>
<br ipv4 max="0" average="0"/>
</xml>

Each element may contain the following attributes:

### Name | Description | Type | Use
--- | --- | --- | ---
max | The maximum value for that statistic observed during the day. | Long | Required
average | The mean value for that statistic observed during the day | Long | Optional

The following table describes the statistics tracked by each element for the day:

### Element Name | Description | Units
--- | --- | ---
total-traffic | Amount of traffic in both directions for the host for the day. | Bytes
data-loss | The cumulative amount of suspected data loss by host. | Bytes
concern-index | Concern index value for the host. | Points
low-traffic | Lowest rate of traffic in both directions for the host for a period of time. | Bits per second
high-traffic | Highest rate of traffic in both directions for the host for a period of time. | Bits per second
max | The maximum observed inbound/outbound traffic rate (bits per second) during the day. | Bits per second
```
3.5.2.8 Concern Index Events
The response may contain a ci-event element. This is a comma-separated list of ci-events that contributed to the Concern Index points.

   <ci-events>
     Addr_Scan/udp, Suspect_UDP_Activity/udp, ICMP_Port_Unreach,
   </ci-events>

3.5.2.9 Exporters
The response may contain the following elements:

   <closest-interface
     domain-id="102"
     device-id="104"
     exporter-ip="10.202.4.72"
     if-index="1"
     confidence="98"/>
   <interface-list>
     <interface
       domain-id="102"
       device-id="104"
       exporter-ip="10.202.4.72"
       if-index="1"/>
     ...
   </interface-list>

The closest-interface element contains the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>The ID of the Domain in which the observation was made.</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>
The `interface-list` element contains one or more `interface` elements that each have the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>The ID of the Domain in which the observation was made.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>device-id</td>
<td>The ID of the StealthWatch FlowCollector appliance that made this observation.</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>exporter-ip</td>
<td>The IP address of the exporter that observed this host.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>if-index</td>
<td>The index number of the Interface that passed traffic for this host.</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>

### 3.6 `getHostGroups`

This Web Services request allows the user to get the current Host Group structure for a given Domain.

#### 3.6.1 Request

The request takes the form of a `domain` XML element:

```xml
<domain id="115" />
```

The `domain` element contains the single `id` attribute that specifies that domain of interest.

#### 3.6.2 Response

The response takes the form of a `host-group-tree` element:

```xml
<domain id="115">
  <host-group-tree>
    <inside-hosts>
      <host-group id="23" name="Host Group A">
        <ip-address-ranges>10.202.</ip-address-ranges>
        <ip-address-ranges>10.203.</ip-address-ranges>
        ...
        <host-group id="24" name="Host Group A1">
          <ip-address-ranges>...</ip-address-ranges>
          ...
        </host-group>
        ...
      </host-group>
      ...
    </inside-hosts>
  </host-group-tree>
</domain>
```
<outside-hosts>
  <host-group id="19" name="AOL IM">
    <ip-address-ranges>64.12.24-26.</ip-address-ranges>
    <ip-address-ranges>64.12.28-29.</ip-address-ranges>
  </host-group>
</outside-hosts>

<host-group id="62001" name="Command & Control Servers" />
<host-group id="65" name="Top-Level Host Group-1">
  <ip-address-ranges>32.12.24-26.</ip-address-ranges>
  <ip-address-ranges>32.12.28-29.</ip-address-ranges>
</host-group>
</host-group-tree>
</domain>

The host-group-tree element must contain the inside-hosts and outside-hosts elements. The
host-group-tree will also contain a host-group element named "Command & Control Servers".
These elements may then contain a nested tree of host-group elements.

The attributes for the inside-hosts element and the outside-hosts element are the same as the host-
group element. These attributes are omitted in the sample above for brevity.

The top-level host groups are host-group elements that come after the host-group element named
"Command & Control Servers."

3.7 setHostGroups

This call allows the user to replace the current host group structure for a given domain.

3.7.1 Request

The request takes the form of a domain element:

<domain id="115">
  <host-group-tree>
    <inside-hosts>
      <host-group id="23" name="Host Group A">
        <ip-address-ranges>10.202.</ip-address-ranges>
        <ip-address-ranges>10.203.</ip-address-ranges>
      </host-group>
      :
      <host-group id="24" name="Host Group A1">
        <ip-address-ranges>...</ip-address-ranges>
      </host-group>
      :
    </inside-hosts>
    <outside-hosts>
      <host-group id="19" name="AOL IM">
        <ip-address-ranges>64.12.24-26.</ip-address-ranges>
        <ip-address-ranges>64.12.28-29.</ip-address-ranges>
      </host-group>
      <host-group id="65" name="Top-Level Host Group-1">
        <ip-address-ranges>32.12.24-26.</ip-address-ranges>
        <ip-address-ranges>32.12.28-29.</ip-address-ranges>
      </host-group>
    </outside-hosts>
  </host-group-tree>
</domain>
The `domain` element must contain the `id` attribute to specify the Domain of interest. The domain specified must already exist.

The `host-group-tree` element must then follow. The `host-group-tree` element must contain the `inside-hosts` and `outside-hosts` elements. These elements may then contain a nested tree of host-group elements.

**NOTE:** Host Group IDs must be larger than 1 and less than 60000. Any Host Groups specified with IDs outside of this range will be ignored.

**NOTE:** The Countries host group will not be replaced if this call is made. In addition, if the Command & Control Servers host group exists in the tree, it will be replaced.

**WARNING:** Host Groups statistics are stored by using the 'id' as a key. When using the setHostGroups Web Service call, do not change the 'id' number of existing host groups because doing so could cause access to historical data for those groups to be inhibited. If 'id' numbers are reassigned from one group to another, retrieval of historical data for the group may contain records from the host group to which the 'id' was previously assigned.

### 3.7.2 Response

The response will simply echo the request providing that the call has successfully completed. It will include all attributes showing the defaults taken.

### 3.8 updateExporters

#### 3.8.1 Request

The request takes the form of a `domain` element:

```xml
<domain id="101">
  <swa-list>
    <swa id="415">
      <exporter-list auto-add="true">
        <exporter ip="10.9.1.1" exporter-type="flow-sensor">
          <snmp>...
        </snmp>
        <interface if-index="2" name="if-1" description="if-1" speed-in="1000000000" speed-out="1000000000" threshold-in="90" threshold-out="90" />
        ...
      </exporter>
      ...
    </swa>
    ...
  </swa-list>
</domain>
```

60
The `domain` element must contain the `id` attribute to specify the Domain of interest.

The `swa-list` element should contain a list of `swa` elements that specify, using the `id` attribute, the StealthWatch FlowCollector devices to be configured.

Each `swa` element should contain an `exporter-list` element that has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-add</td>
<td>Indicates if the StealthWatch FlowCollector for sFlow should accept data from any exporter (true) or only those specified (false).</td>
<td>Boolean</td>
<td>Optional</td>
</tr>
</tbody>
</table>

The `exporter-list` element contains a list of `exporter` elements that specify, using the `ip` element, which exporters are to be updated or added. The `exporter` element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>IP Address of the exporter to be updated</td>
<td>IP Address</td>
<td>Required</td>
</tr>
<tr>
<td>exporter-type</td>
<td>Specifies the type of exporter. Valid values are: 'exporter', 'flowsensor'</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>Username</td>
<td>Username for communication credentials, if exporter-type='flowsensor'.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>Password</td>
<td>Password for communication credentials, if exporter-type='flowsensor'.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>hybrid-pair-ip</td>
<td>IP Address of the hybrid pair, if exporter-type='exporter'.</td>
<td>IP Address</td>
<td>Optional</td>
</tr>
<tr>
<td>ignore-v5-egress</td>
<td>Ignore egress values when computing interface traffic statistic, if exporter-type='exporter'.</td>
<td>Boolean</td>
<td>Options</td>
</tr>
</tbody>
</table>

The `exporter` element may contain a `snmp` element that specifies if and how the SMC should poll the exporter using the SNMP protocol. This element can take one of 2 forms:

A reference to an SNMP configuration already in the system:

```
<snmp enabled="true">
  <snmp-configuration-ref name="Device Profile #1"/>
</snmp>
```

or an inline SNMP configuration to be used by this exporter alone:

```
<snmp enabled="true">
  <snmp-configuration
    name="SNMP Config A"
    port="161"
    version="2"
    polling-interval="5"
  />
</snmp>
```
```xml
<snmp
    community="public"
    use-ifXTable="true"
    use-catos-mib="false"
    username="user1"
    auth-password="password1"
    priv-password="password2"
    security-level="0"
    auth-method="0"
    priv-method="0" />
</snmp>
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name given to the configuration</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>port</td>
<td>The UDP port that the SNMP requests should be sent.</td>
<td>Short</td>
<td>Optional.</td>
</tr>
<tr>
<td>version</td>
<td>The version of the SNMP protocol to use.</td>
<td>&quot;1&quot;, &quot;2&quot; or &quot;3&quot;</td>
<td>Optional. Default is &quot;1&quot;.</td>
</tr>
<tr>
<td>polling-interval</td>
<td>The number of minutes between each poll. (&quot;0&quot; corresponds to never poll)</td>
<td>Integer</td>
<td>Mandatory</td>
</tr>
<tr>
<td>community</td>
<td>The community string. Used in SNMP v1 and 2c only.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>use-if-Xtable</td>
<td>Indicates if the if-Xtable MIB should be queried on the exporter.</td>
<td>Boolean</td>
<td>Optional. Default is &quot;false&quot;</td>
</tr>
<tr>
<td>use-catos-mib</td>
<td>Indicates if the CatOS MIB should be queried on the exporter.</td>
<td>Boolean</td>
<td>Optional. Default is &quot;false&quot;</td>
</tr>
<tr>
<td>username</td>
<td>USM user name. Used in SNMP v3 only.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>auth-method</td>
<td>USM authentication protocol.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>priv-method</td>
<td>USM privacy protocol.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>auth-password</td>
<td>USM authentication key.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>priv-password</td>
<td>USP privacy key.</td>
<td>String</td>
<td>Optional</td>
</tr>
</tbody>
</table>
The **exporter** element may then contain a number of **interface** elements that represent the interfaces to be updated/added. These elements contain the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>if-index</td>
<td>The interface ID or Index.</td>
<td>Integer</td>
<td>Mandatory</td>
</tr>
<tr>
<td>name</td>
<td>A string name for the interface.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>description</td>
<td>A string description for the interface.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>speed-in</td>
<td>The inbound speed of the interface in bits per second.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>speed-out</td>
<td>The outbound speed of the interface in bits per second.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>threshold-in</td>
<td>The inbound threshold of the interface. If traffic rises above this percentage of inbound speed an &quot;Exporter Utilization Inbound Exceeded&quot; alarm is generated.</td>
<td>Percent</td>
<td>Optional</td>
</tr>
<tr>
<td>threshold-out</td>
<td>The outbound threshold of the interface. If traffic rises above this percentage of outbound speed an &quot;Exporter Utilization Outbound Exceeded&quot; alarm is generated.</td>
<td>Percent</td>
<td>Optional</td>
</tr>
</tbody>
</table>

### 3.8.2 Response
The response is empty.

### 3.9 removeExporters

#### 3.9.1 Request
The request takes the form of a **domain** element:

```xml
<domain id="101">
  <swa-list>
    <swa id="415">
      <exporter-list>
        <exporter ip="10.9.1.1" />
      </exporter-list>
    </swa>
    <swa id="416">
      <exporter-list/>
    </swa>
    ...
  </swa-list>
</domain>
```

The **domain** element must contain the **id** attribute to specify the Domain of interest.

The **swa-list** element should contain a list of **swa** elements that specify, using the **id** attribute, the StealthWatch FlowCollector devices to be configured.
The exporter-list element contains a list of exporter elements that specify, using the ip element, which exporters are to be removed.

The exporter element contains the following attributes (removeExporters required attribute):

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>IP Address of the exporter</td>
<td>IP Address</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>

3.9.2 Response
The response is empty.

3.10 updateExporterSNMPConfiguration

3.10.1 Request
The request takes the form of a domain element:

```xml
<domain id="101">
  <snmp-configuration-list timeout="5000" retries="3">
    <snmp-configuration
      name="SNMP Config A"
      port="161"
      version="2"
      polling-interval="5"
      community="public"
      use-ifXTable="true"
      use-catos-mib="false"
      username="user1"
      auth-password="password1"
      priv-password="password2"
      security-level="0"
      auth-method="0"
      priv-method="0" />
  </snmp-configuration-list>
</domain>
```

The domain element must contain the id attribute to specify the Domain of interest.

The domain element contains a snmp-configuration-list element. The snmp-configuration-list element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-configuration-name</td>
<td>The name of the SNMP configuration settings that the SMC will use when querying the Exporter when the default SNMP configuration is specified.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>time-out</td>
<td>The amount of time in milliseconds that the SMC waits when querying an exporter before aborting the attempt.</td>
<td>Integer</td>
<td>Optional, Default is &quot;5000&quot;</td>
</tr>
</tbody>
</table>
The `retries` element contains the number of attempts that the SMC makes after the first attempt to query an exporter fails. It is an integer, with a default value of "3".

The `snmp-configuration-list` element contains a list of `snmp-configuration` elements. Each `snmp-configuration` element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name given to the configuration</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>port</td>
<td>The UDP port that the SNMP requests should be sent.</td>
<td>Short</td>
<td>Optional. Default is &quot;161&quot;</td>
</tr>
<tr>
<td>version</td>
<td>The version of the SNMP protocol to use.</td>
<td>&quot;1&quot;, &quot;2&quot; or &quot;3&quot;</td>
<td>Optional. Default is &quot;1&quot;</td>
</tr>
<tr>
<td>polling-interval</td>
<td>The number of minutes between each poll.</td>
<td>Integer</td>
<td>Mandatory</td>
</tr>
<tr>
<td>community</td>
<td>The community string. Used in SNMP v1 and 2c only.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>use-if-Xtable</td>
<td>Indicates if the if-Xtable MIB should be queried on the exporter.</td>
<td>Boolean</td>
<td>Optional. Default is &quot;false&quot;</td>
</tr>
<tr>
<td>use-catos-mib</td>
<td>Indicates if the CatOS MIB should be queried on the exporter.</td>
<td>Boolean</td>
<td>Optional. Default is &quot;false&quot;</td>
</tr>
<tr>
<td>username</td>
<td>USM user name. Used in SNMP v3 only.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>auth-method</td>
<td>USM authentication protocol.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>priv-method</td>
<td>USM privacy protocol.</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>auth-password</td>
<td>USM authentication key. Used in SNMP v3 only.</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>priv-password</td>
<td>USM privacy key. Used in SNMP v3 only.</td>
<td>String</td>
<td>Optional</td>
</tr>
</tbody>
</table>
3.10.2 Response
The response is empty.

3.11 addHostGroup
This Web Services request adds a new host group. The new host group may be added as any of the following types of host groups:

- Top-level host group
- Sub-host group under Inside Hosts or Outside Hosts
- Sub-host group to any existing host group, except for the following host groups:
  - Catch All
  - Command & Control Servers
  - Countries.

3.11.1 Request
The request takes the form of a `host-group` element:

```xml
<host-group domain-id="101" id="1" ...
<ip-address-ranges>10.201.3.0-10</ip-address-ranges>
<ip-address-ranges>10.202.</ip-address-ranges>
>
</host-group>
```

The `host-group` element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>ID of the Host Group of interest</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>domain-id</td>
<td>ID of the Domain of interest</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>Name</td>
<td>Name of Host Group</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>parent-id</td>
<td>ID of the Parent. Omit if adding top-level Host Group</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>host-baselines</td>
<td>Indicates if hosts in this Host Group will have individual policies</td>
<td>Boolean</td>
<td>Optional Default is false</td>
</tr>
<tr>
<td>suppress-excluded-services</td>
<td>Allows for disabling CI Events using excluding services</td>
<td>boolean</td>
<td>Optional Default is true</td>
</tr>
<tr>
<td>inverse-suppression</td>
<td>Disable Flood alarms and CI Events when a Host in this Host Group is the target</td>
<td>Boolean</td>
<td>Optional Default is true</td>
</tr>
<tr>
<td>host-trap</td>
<td>Enable ‘trapping’ of hosts that scan unused addresses in this Host Groups</td>
<td>Boolean</td>
<td>Optional Default is true</td>
</tr>
</tbody>
</table>

The `host-group` element must contain a `domain-id` attribute to specify the Domain of interest.

In order to add a top-level Host Group, omit the `parent-id` attribute.

In order to add a Host Group to the Inside-Hosts, set the `parent-id` to 1.
In order to add a Host Group to the Outside-Hosts, set the parent-id to 0.

In order to add a Host Group as a sub-group to another Host Group, use the exported configuration xml file to determine the correct parent-id element.

The ip-address-ranges element contains a string that represents an IP Address or a range of IP Addresses.

This operation will add, subject to validation, the Host Group as specified in the host-group element.

### 3.11.2 Response

The response will return XML in the same format as the request. Note that the value for the Host Group id has been assigned and returned in the response. Any optional elements not entered in the request will be returned in the response showing the default values assigned.

### 3.12 addHostGroups

This Web Services request adds multiple new host groups. The new host groups may be added as any of the following types of host groups:

- Sub-host group under Inside Hosts or Outside Hosts
- Sub-host group to any existing host group, except for the following host groups:
  - Catch All
  - Command & Control Servers
  - Countries

For memory considerations, we recommend you limit the number of new host groups to 3000 per request.
3.12.1 Request
The request takes the form of a `host-group` element:

```
<sub-group-tree domain-id="101">
  <host-group id="84">
    <host-group domain-id="101" id="1" ...>
      <ip-address-ranges>10.201.3.0-10</ip-address-ranges>
      <ip-address-ranges>10.202.</ip-address-ranges>
    </host-group>
  </host-group>
  ...
</sub-group-tree>
```

The `sub-host-group` element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>ID of the Domain of interest</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>

The `host-group` element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>ID of the Host Group of interest</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>domain-id</td>
<td>ID of the Domain of interest</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>Name</td>
<td>Name of Host Group</td>
<td>String</td>
<td>Optional</td>
</tr>
<tr>
<td>parent-id</td>
<td>ID of the Parent. Omit if adding top-level Host Group</td>
<td>Integer</td>
<td>Optional</td>
</tr>
<tr>
<td>host-baselines</td>
<td>Indicates if hosts in this Host Group will have individual policies</td>
<td>Boolean</td>
<td>Optional</td>
</tr>
<tr>
<td>suppress-excluded-services</td>
<td>Allows for disabling CI Events using excluding services</td>
<td>boolean</td>
<td>Optional</td>
</tr>
<tr>
<td>inverse-suppression</td>
<td>Disable Flood alarms and CI Events when a Host in this Host Group is the target</td>
<td>Boolean</td>
<td>Optional</td>
</tr>
<tr>
<td>host-trap</td>
<td>Enable ‘trapping’ of hosts that scan unused addresses in this Host Group</td>
<td>Boolean</td>
<td>Optional</td>
</tr>
</tbody>
</table>

The top level `host-group` elements do not need to contain any attributes except an id for a host group that already exists. This will be the parent host group for all the host groups defined within it.

If an `id` attribute contains an id that is not already in use, then the specified id will be used for the new host group. If an `id` attribute contains an id that is already in use, then a new id will be assigned to the new host group.

The `ip-address-ranges` element contains a string that represents an IP Address or a range of IP Addresses.
This operation will add, subject to validation, the Host Groups as specified in the host-group elements. A validation error in any host groups will result in the entire file being rejected.

3.12.2 Response
The response will return XML in the same format as the request. Note that the value for the Host Group id has been assigned and returned in the response. Any optional elements not entered in the request will be returned in the response showing the default values assigned.

3.13 addHostGroupIPRange
This Web Services request will add IP Address Ranges to an existing Host Group.

3.13.1 Request
The request takes the form of a host-group element:

```
<host-group id="34" domain-id="101" ...>
  <ip-address-ranges>10.202.1.</ip-address-ranges>
  <ip-address-ranges>10.203.1.</ip-address-ranges>
  ...:
</host-group>
```

The host-group element for this request accepts the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>ID of the Host Group of interest</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>domain-id</td>
<td>ID of the Domain of interest</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>

The host-group element must contain a domain-id attribute to specify the Domain of interest.

The host-group element also contains zero or more ip-address-ranges elements.

The ip-address-ranges element contains a string that represents an IP Address or a range of IP Addresses.

This operation will add, subject to validation, the Host Group IP Ranges as specified in the host-group element.

**NOTE:** IP address ranges cannot be added to either the Countries or the Command & Control Servers host groups.

3.13.2 Response
The response will return XML for the entire host-group element and all its configured ip-address-ranges.

3.14 addHostGroupIPRanges
This Web Services request will add IP Address Ranges to multiple existing Host Groups.
3.14.1 Request

The request takes the form of multiple `host-group` elements:

```xml
<multiple-host-groups>
  <host-group id="34" domain-id="101" ...>
    <ip-address-ranges>10.202.1.</ip-address-ranges/>
    <ip-address-ranges>10.203.1.</ip-address-ranges/>
  ...
  </host-group>
</multiple-host-groups>
```

The `host-group` elements for this request accepts the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>ID of the Host Group of interest</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>domain-id</td>
<td>ID of the Domain of interest</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>

The `host-group` element must contain a `domain-id` attribute to specify the Domain of interest.

The `host-group` element also contains zero or more `ip-address-ranges` elements.

The `ip-address-ranges` element contains a string that represents an IP Address or a range of IP Addresses.

This operation will add, subject to validation, the Host Group IP Ranges as specified in the `host-group` elements.

**NOTE:** IP address ranges cannot be added to either the Countries or the Command & Control Servers host groups.

3.14.2 Response

The response will return XML for the entire `host-group` element and all its configured `ip-address-ranges`.

3.15 removeHostGroup

This Web Service request will remove the Host Group specified by the `host-group` element attributes of `domain-id` and `id`.

3.15.1 Request

The request takes the form of a `host-group` element:

```xml
<host-group id="34" domain-id="101">
</host-group>
```

The `host-group` element for this request accepts the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>ID of the Host Group of interest</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>domain-id</td>
<td>ID of the Domain of interest</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>
The **host-group** element must contain a **domain-id** attribute to specify the Domain of interest and an **id** attribute to specify the Host Group of interest.

This operation will remove, if present, the Host Group specified by the **domain-id** and **id**. Note that Command & Control Servers and its subordinate host groups cannot be removed.

### 3.15.2 Response

The response is empty.

### 3.16 removeHostGroupIPRange

#### 3.16.1 Request

The request takes the form of a **host-group** element:

```xml
<host-group id="34" domain-id="101">
  <ip-address-ranges>10.202.1.</ip-address-ranges>
  <ip-address-ranges>10.201.2.1</ip-address-ranges>
</host-group>
```

The **host-group** element must contain a **domain-id** attribute to specify the Domain of interest and an **id** attribute to specify the Host Group of interest.

This operation will remove, if present, the IP address ranges as specified in the **ip-address-ranges** elements. Note that IP address ranges cannot be removed from host groups subordinate to Command & Control Servers.

#### 3.16.2 Response

The response will return XML for the entire **host-group** element and all its configured **ip-address-ranges**.

### 3.17 setHostGroupIPRange

#### 3.17.1 Request

The request takes the form of a **host-group** element:

```xml
<host-group id="34" domain-id="101">
  <ip-address-ranges>"10.202.1."</ip-address-ranges>
  <ip-address-ranges>"10.203.1."</ip-address-ranges>
</host-group>
```

The **host-group** element must contain a **domain-id** attribute to specify the Domain of interest and an **id** attribute to specify the Host Group of interest.

This operation will replace the existing IP address ranges for the Host Group, subject to validation, with those specified in the **ip-address-ranges** elements.

**NOTE:** IP address ranges cannot be defined for either the Countries or the Command & Control Servers host groups.
3.17.2 Response
The response will return XML in the same format as the request that contains the currently configured IP
address ranges for the Host Group.

3.18 getDomain
This Web Services request allows the user to get the current configuration of a Domain as specified by
the id attribute.

3.18.1 Request
The request takes the form of a domain element:

```xml
<domain id="101" />
```

The domain element has the following required attribute:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>ID of the Domain of interest</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>

This operation will return subject to validation, the Domain group as specified in the host-group element.

3.18.2 Response
The response will return XML in the same format as the request. Note that the value for the Host Group
id has been assigned and returned in the response. Any optional elements not entered in the request will
be returned in the response showing the default values assigned.

3.19 addDomain
This Web Services request will add a new Domain.

3.19.1 Request
The request takes the form of a domain element:

```xml
<domain name="SMC A" reset-hour="4">
  <as-configuration ... />
  <host-group-tree ... />
  <policy-list ... />
  <swa-list ... />
  <external-device-list ... />
  <swa-id-list ... />
  <cisco-ise-list ... />
  <alarm-configuration ... />
  <service-definitions ... />
  <application-definitions ... />
  <intergroup-locking-list ... />
  <snmp-configuration-list ... />
  <group-pair-list ... />
  <map-list ... />
</domain>
```

The sub-elements of the domain element are shown above for reference.
For the addDomain request, the following attributes are available:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name of the domain</td>
<td>String</td>
<td>Optional Default is ‘Domain_xxx’ where xxx is the generated domain id.</td>
</tr>
<tr>
<td>reset-hour</td>
<td></td>
<td>Short</td>
<td>Required. Valid values are 0-23. Default is 4.</td>
</tr>
</tbody>
</table>

This operation will add, subject to validation, the Domain. A domain id is automatically assigned.

The sub-elements are discussed below.

3.19.1.1 Autonomous System Number Configuration

The as-configuration element contains the internal-as-numbers element. This element consists of a comma-separated list of as numbers.

```xml
<as-configuration>
  <internal-as-numbers>10986,12058,,47896,48148,59274</internal-as-numbers>
</as-configuration>
```

3.19.1.2 Host Group Tree

The host-group-tree element consists of the inside-hosts element, outside-hosts element, and host-group elements that are referred to as top-level host groups. Command & Control Servers host-group elements in the request will be ignored, but any Command & Control Servers host groups in an existing domain on the SMC will be automatically added to your new domain. Top-level host groups are not identified with either the Inside, Outside, or Command & Control Servers host groups.

See 3.11 for details of the host-group element.

3.19.1.3 Policy Configuration

It is recommended to export a domain, then extract the entire sections of this for creating the new domain. Better yet, is to just use the exported XML for your new domain making any changes to the exported XML.

3.19.1.4 SWA Device Configuration

The swa-list element should contain a list of swa elements that specify the StealthWatch FlowCollector devices to be configured.
3.19.1.5 SWA Identity Device Configuration

The `<swa-id-list>` element should contain a list of `<swa-id>` elements that specify the SWA Identity devices to be configured.

```xml
<swa-id-list>
  <swa-id
    id="2104"
    name="test"
    ip-address="10.202.1.217"
    username="admin"
    password="xxxxxxxx"
    port="2393"
  />
</swa-id-list>
```

The `<swa-id>` element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto-assigned when added</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>name</td>
<td>User provided name</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>ip-address</td>
<td>User provided ip address</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>username</td>
<td>Name used to authenticate with the SWA Identity appliance</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>Password</td>
<td>Pass used to authenticate with the SWA Identity appliance</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>port</td>
<td>Port number used by the SWA Identity appliance</td>
<td>Integer</td>
<td>Optional</td>
</tr>
</tbody>
</table>

3.19.1.6 Cisco ISE Configuration

The `<cisco-ise-list>` element contains a list of `<cisco-ise>` elements that specify the Cisco ISE appliances to be configured. Your license will limit the number of Cisco ISE devices you are allowed to add. Any devices over that limit will be ignored.

```xml
<cisco-ise-list>
  <cisco-ise
    id="2143"
    name="Cisco ISE"
    ip-address="10.203.6.2"
    username="choward"
    password="xxxxxxxx"
    time-zone-id="Africa/Cairo"
  />
</cisco-ise-list>
```

The `<cisco-ise>` element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto-assigned when added</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>name</td>
<td>User provided name</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>ip-address</td>
<td>User provided ip address</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>username</td>
<td>Name used to authenticate with the ISE</td>
<td>String</td>
<td>Required</td>
</tr>
</tbody>
</table>
Password | Pass used to authenticate with the ISE | String | Required
---|---|---|---
time-zone-id | User provided configuration. It will default to "etc/UTC" | String from combo box which is populated with a text file provided by Cisco. | Optional

### 3.19.1.7 External Devices Configuration

The `external-device-list` element should contain a list of `external-device` elements that specify the External devices to be configured.

```xml
<external-device-list>
  <external-device id="122" name="ISS/RealSecure Test" ip-address="10.203.6.6" type="realsecure">
    <property-list>
      <property key="value" value="test"/>
    </property-list>
  </external-device>
</external-device-list>
```

The `external-device` element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>External device id</td>
<td>Integer</td>
<td>Required</td>
</tr>
<tr>
<td>ip-address</td>
<td>User provided name</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>type</td>
<td>Valid values are: realsecure snort syslog</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>name</td>
<td>User provided name</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>property-list</td>
<td>User configured properties dependent on types</td>
<td>Name/Value pair</td>
<td>Optional</td>
</tr>
</tbody>
</table>

### 3.19.1.8 Alarm Configuration

The `alarm-configuration` element is used to change the severity of the individual alarms and consists of an `alarm-severity` sub-element for each alarm that is to be changed.

```xml
<alarm-configuration>
  <alarm-severity id="36" value="major"/>
  <alarm-severity id="40" value="critical"/>
</alarm-configuration>
```
The alarm-severity element has the following attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>ID of alarm type. See 4.5 table for list of alarms and ids.</td>
<td>String</td>
<td>Required</td>
</tr>
<tr>
<td>value</td>
<td>Valid values are based on the: critical, major, minor, trivial, information</td>
<td>String</td>
<td>Required</td>
</tr>
</tbody>
</table>

3.19.1.9 Service-Definitions

The service-definitions element contains 1 sub-elements. The services element then contains service elements. It is recommended to export a domain, then extract the entire sections of this for creating the new domain. Better yet, is to just use the exported XML for your new domain making any changes to the exported XML.

3.19.1.10 Application Definitions

The applications-definitions element contains 2 sub-elements: classification-list and application-list. It is recommended to export a domain, then extract the entire sections of this for creating the new domain. Better yet, is to just use the exported XML for your new domain making any changes to the exported XML.

3.19.1.11 Host Locking Configuration

The Host Locking Configuration is defined using the intergroup-locking-list element which contains a group-pair element. It is recommended to export a domain that contains configuration similar to what you desire, then extract the entire sections of this for creating the new domain. Better yet, is to just use the exported XML for your new domain making any changes to the exported XML.

3.19.1.12 SNMP Configuration

The snmp-configuration-list element contains an snmp-configuration sub-element for each configuration needed. It is recommended to export a domain, then extract the entire sections of this for creating the new domain. Better yet, is to just use the exported XML for your new domain making any changes to the exported XML.

3.19.1.13 Host Group Relationships Configuration

The Host Group Relationship configuration is tightly coupled with the Map configuration. It is recommended to export a domain, then extract the entire sections of this for creating the new domain. Better yet, is to just use the exported XML for your new domain making any changes to the exported XML.

3.19.2 Response

The response will return XML is the same format as the request. Note that the value for the Domain id has been assigned and returned in the response. Any optional elements not entered in the request will be returned in the response showing the default values assigned.
3.20 removeDomain

This Web Services request will remove the domain as specified by the supplied \textit{id} attribute of the domain to be removed.

3.20.1 Request

The request takes the form of a \texttt{domain} element:

\[
\texttt{<domain id="101" />}
\]

The \texttt{domain} element has the following required attribute:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>ID of the Domain of interest</td>
<td>Integer</td>
<td>Required</td>
</tr>
</tbody>
</table>

The \texttt{domain} element must contain an \texttt{id} attribute to specify the Domain of interest.

3.20.2 Response

The response is empty
4 Appendix

4.1 Date & Time Filtering

The general form of date and time filtering in a request filter consists of a date-selection element:

```xml
<date-selection>:
</date-selection>
```

The following sections will describe the various constructs that may be contained within the date-selection element.

4.1.1 Time Range Selection

This form of filtering simply matches records that fall between a start and end time:

“Match all records between 10th March 2011 4AM GMT and 10th March 2011 5AM GMT”

```xml
<date-selection>
  <time-range-selection start="2011-03-10T04:00:00Z"
                        end="2011-03-10T05:00:00Z"/>
</date-selection>
```

“Match all records after 10th March 2011 4AM GMT”

```xml
<date-selection>
  <time-range-selection start="2011-03-10T04:00:00Z"/>
</date-selection>
```

“Match all records before 10th March 2011 4AM GMT”

```xml
<date-selection>
  <time-range-selection end="2011-03-10T04:00:00Z"/>
</date-selection>
```

Notice that if the start element is not specified the start time is assumed to be epoch and if the end element is not specified the end time is assumed to be the time of the request (“now”).

4.1.2 Time Window Selection

This form of filtering matches all records that fall in a time window of fixed length that ends at the time of the request (“now”):

“Match all records from the last 1 hour”

```xml
<date-selection>
  <time-window-selection duration="3600000"/>
</date-selection>
```

The duration attribute is the size of the time window in milliseconds.
4.1.3 Day Selection
This form of filtering matches all records that fall within a specified day. A day, in this context, runs from
the Domain's reset hour to reset hour:

“Match all records from the day (24 hours) starting 10th March 2011 12AM GMT”

```xml
<date-selection>
  <day-selection start="2011-03-10T00:00:00Z"/>
</date-selection>
```

“Match all records from the day (24 hours) starting 3 days ago”

```xml
<date-selection>
  <day-selection days-before="3"/>
</date-selection>
```

“Match all records from today”

```xml
<date-selection>
  <day-selection/>
</date-selection>
```

Note that if either the start or days-before attribute is not specified, the selection is interpreted as between
the last reset hour and now (“today”).

4.1.4 Day Range Selection
This form of filtering matches all records that fall within a specified range of days. A day, in this context,
runs from the Domains reset hour to reset hour:

“Match all records for the 7 days ending with the day that started 10th March 2011 12AM GMT”

```xml
<date-selection>
  <day-range-selection last-day="2011-03-10T00:00:00Z" day-count="7"/>
</date-selection>
```

“Match all records for the last 7 day”

```xml
<date-selection>
  <day-range-selection day-count="7"/>
</date-selection>
```

Notice that if the day start-time is not specified, the selection is interpreted as between the last reset hour
and now (“today”).

4.1.5 Active Time Selection
As of this writing, the only SOAP request supporting the active time selection is getSecurityEvents.

Certain data records hold to the concept of being active during some period of time. These records hold
this information in a start time and an end time.

When requesting these types of data, it is often useful to specify the time these records were active in the
request. Simply wrapping a time-range-selection, time-window selection or day-selection with
an active-time-selection element does this:
“Match all records that were active between 10th March 2011 4AM GMT and 10th March 2011 5AM GMT”

```xml
<date-selection>
  <active-time-selection>
    <time-range-selection start="2011-03-10T04:00:00Z" end="2011-03-10T05:00:00Z"/>
  </active-time-selection>
</date-selection>
```

“Match all records that were active after 10th March 2011 4AM GMT”

```xml
<date-selection>
  <active-time-selection>
    <time-range-selection start="2011-03-10T04:00:00Z"/>
  </active-time-selection>
</date-selection>
```

“Match all records that were active before 10th March 2011 4AM GMT”

```xml
<date-selection>
  <active-time-selection>
    <time-range-selection end="2011-03-10T04:00:00Z"/>
  </active-time-selection>
</date-selection>
```

“Match all records that were active in the last 1 hour”

```xml
<date-selection>
  <active-time-selection>
    <time-window-selection duration="3600000"/>
  </active-time-selection>
</date-selection>
```

“Match all records that were active in the day (24 hours) starting 10th March 2011 12AM GMT”

```xml
<date-selection>
  <active-time-selection>
    <day-selection start="2011-03-10T00:00:00Z"/>
  </active-time-selection>
</date-selection>
```

“Match all records that were active today”

```xml
<date-selection>
  <active-time-selection>
    <day-selection/>
  </active-time-selection>
</date-selection>
```

### 4.1.6 First-Last Time Selection

As of this writing, the only SOAP request supporting first-last time selection is getCiEvents.

Requests for data that contain both a start and end time (see 4.1.4) may also filter on these times independently:
Match all records that started active in the day (24 hours) starting 10th March 2011 12AM GMT and stopped being active in the last 1 hour

```
<date-selection>
  <first-last-time-selection>
    <first>
      <day-selection start="2011-03-10T00:00:00Z"/>
    </first>
    <last>
      <time-window-selection duration="3600000"/>
    </last>
  </first-last-time-selection>
</date-selection>
```

If the first or last elements are not present then the start active or end active times are unconstrained.

### 4.2 Device Filtering

The general form of device filtering in a request filter consists of a `device-selection` element:

```
<device-selection>
  ...
</device-selection>
```

The following sections will describe the various constructs that may be contained within the `device-selection` element.

#### 4.2.1 Device List Selection

This form of filtering allows the request to list the devices that the response will contain data from:

"Match all records that were observed by devices with IDs 111, 112 and 113"

```
<device-selection>
  <device-list-selection>
    <device device-id="111"/>
    <device device-id="112"/>
    <device device-id="113"/>
  </device-list-selection>
</device-selection>
```

#### 4.2.2 Exporter Selection

This form of filtering allows the request to specify an Exporter of interest:

"Match all records that were observed by the flow exporter 192.168.1.2, that is attached to device 111"

```
<device-selection>
  <interface-list-selection>
    <interface device-id="111" exporter-ip="192.168.1.2"/>
  </interface-list-selection>
</device-selection>
```

#### 4.2.3 Interface Selection

This form of filtering allows the request to specify an Interface of interest:
“Match all records that refer to interface #12, on the flow exporter 192.168.1.2, that is attached to device 111”

```xml
<device-selection>
  <interface-list-selection>
    <interface
      device-id="111"
      exporter-ip="192.168.1.2"
      interface-id="12" />
  </interface-list-selection>
</device-selection>
```

4.3 Host Filtering

The general form of host filtering in a request filter consists of a `host-selection` element:

```xml
<host-selection>
</host-selection>
```

The following sections will describe the various constructs that maybe contained within the `host-selection` element.

4.3.1 Host Group Selection

This form of filtering simply matches records that concern hosts in a particular Host Group:

“Match all records that refer to hosts in Host Group #10”

```xml
<host-selection>
  <host-group-selection host-group-id="10"/>
</host-selection>
```

4.3.2 IP Address Range Selection

This form of filtering matches records that concern hosts that have IP address in some range:

“Match all records that refer to hosts with IP address that start in 10.168.”

```xml
<host-selection>
  <ip-address-range-selection value="10.168." />
</host-selection>
```

4.3.3 IP Address List Selection

This form of filtering matches records that concern hosts that have one of the listed IP addresses:

“Match all records that refer to hosts with IP addresses 192.168.1.10 and 192.168.1.20”

```xml
<host-selection>
  <ip-address-list-selection>
    <ip-address value="192.168.1.10" />
    <ip-address value="192.168.1.20" />
  </ip-address-list-selection>
</host-selection>
```
4.3.4 IP Address Selection
This form of filtering matches records that concern the host with the specified IP addresses: This form is used for single host filtering such as needed for Host Snapshot.

“Match all records that refer to the host with IP address 192.168.1.20”

<host-selection>
  <ip-address-selection value="192.168.1.10" />
</host-selection>

4.3.5 VM Selection
This form of filtering matches records that concern specific VM Hosts and/or hosts on specific VM Servers. This is in the form of the vm-list-selection sub-element. The vm-list-selection has 2 sub-elements that allow for specifying VM Servers using the vmserver-list sub-element, and/or the vm-list sub-element for specifying VM Hosts. The vm-list-selection element can contain both the vmserver-list sub-element and the vm-list sub-element

“Match all records that refer to the hosts with vm-id of 55 or vm-server-id of 52”

<host-selection>
  <vm-list-selection>
    <vmserver-list>
      <vmserver
        id="52"
        device-id="113"
        server-ip-address="10.202.15.68" />
    </vmserver-list>
    <vm-list>
      <vm
        id="55"
        device-id="113"
        server-ip-address="10.202.15.68" />
    </vm-list>
  </vm-list-selection>
</host-selection>

4.3.6 Host Pair Selection
Certain data records refer to 2 hosts and some relationship between them. Examples of the type of data are:

- Flows
- CI Events

An example of this query would be:

“Match all records that refer between host 192.168.1.10 and host 192.168.1.20”

<host-pair-selection direction="BETWEEN_SELECTION_1_SELECTION_2">
  <selection-1>
    <ip-address-selection value="192.168.1.10" />
  </selection-1>
  <selection-2>
    <ip-address-selection value="192.168.1.20" />
  </selection-2>
</host-pair-selection>
The host-pair-selection element may contain a selection-1 and/or selection-2 which, in turn, contain a host selection. If either of these elements is unspecified, then they are interpreted as “all hosts”. Possible contents of selection-1 and selection-2 are:

- host-group-selection
  See 4.3.1 for more information.
- ip-address-range-selection
  See 4.3.2 for more information.
- ip-address-list-selection
  See 4.3.3 for more information.
- ip-address-selection
  See 4.3.4 for more information.
- vm-list-selection
  See 4.3.5 for more information.

The direction attribute that has the following possible values:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SELECTION_1_A_SELECTION_2_Z</td>
<td>Hosts that match selection 1 are in role A And Hosts that match selection 2 are in role Z</td>
</tr>
<tr>
<td>SELECTION_1_Z_SELECTION_2_A</td>
<td>Hosts that match selection 1 are in role Z And Hosts that match selection 2 are in role A</td>
</tr>
<tr>
<td>BETWEEN_SELECTION_1_AND_SELECTION_2</td>
<td>Hosts that match selection 1 are in either role A or Z And Hosts that match selection 2 are in either role A or Z</td>
</tr>
</tbody>
</table>

The roles are defined as follows:

<table>
<thead>
<tr>
<th>Record</th>
<th>Role A</th>
<th>Role Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow</td>
<td>Client</td>
<td>Server</td>
</tr>
<tr>
<td>Alarm</td>
<td>Source</td>
<td>Target</td>
</tr>
<tr>
<td>CI Event</td>
<td>Source</td>
<td>Target</td>
</tr>
</tbody>
</table>

### 4.4 Service Profile Status

The service profile status is encoded into a string format:

1:P28,T1 2:S1,S48,U3 3:P2 5:0902/tcp

The string is made up of up to five sections separated by a white space. Each section starts with a number (“1”, “2”, “3”, “4”, or “5”) that represents the status, followed by a colon (”:”) and then a comma (”,”) separated list of service description.

The possible states:

<table>
<thead>
<tr>
<th>Number</th>
<th>Policy</th>
<th>Observed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Explicitly allowed in profile</td>
<td>Observed</td>
</tr>
<tr>
<td>ID</td>
<td>Explicitly allowed in profile</td>
<td>Not Observed</td>
</tr>
<tr>
<td>----</td>
<td>-------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>2</td>
<td>Explicitly disallowed in profile</td>
<td>Observed</td>
</tr>
<tr>
<td>3</td>
<td>Explicitly disallowed in profile</td>
<td>Not Observed</td>
</tr>
<tr>
<td>4</td>
<td>Not specified in profile. Implicitly disallowed.</td>
<td>Observed</td>
</tr>
</tbody>
</table>

The service descriptions start with a single letter code ("S", "P", "T", "U", "O") followed by a string that gives further detail.

The possible service codes and details are:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>Profiled TCP or UDP Service as described in Service Definitions</td>
<td>Index into Service Definitions e.g. S1, S43</td>
</tr>
<tr>
<td>P</td>
<td>Profiled protocol as described in Service Definitions</td>
<td>Index into Service Definitions e.g. P1, P4</td>
</tr>
<tr>
<td>O</td>
<td>Unprofiled service</td>
<td>Port and protocol e.g. 902/tcp, 1000/udp</td>
</tr>
</tbody>
</table>

### 4.5 Alarm Types

**NOTE:** Some previously used alarms are now obsolete and no longer listed in this file.

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Host Lock Violation</td>
</tr>
<tr>
<td>5</td>
<td>SYN Flood</td>
</tr>
<tr>
<td>6</td>
<td>UDP Flood</td>
</tr>
<tr>
<td>7</td>
<td>ICMP Flood</td>
</tr>
<tr>
<td></td>
<td>Event Description</td>
</tr>
<tr>
<td>---</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>8</td>
<td>Packet Flood</td>
</tr>
<tr>
<td>9</td>
<td>High Volume Email</td>
</tr>
<tr>
<td>10</td>
<td>Mail Relay</td>
</tr>
<tr>
<td>11</td>
<td>Spam Source</td>
</tr>
<tr>
<td>12</td>
<td>Mail Rejects</td>
</tr>
<tr>
<td>13</td>
<td>Watch Port Active</td>
</tr>
<tr>
<td>14</td>
<td>New Host Active</td>
</tr>
<tr>
<td>15</td>
<td>High Target Index</td>
</tr>
<tr>
<td>16</td>
<td>High Total Traffic</td>
</tr>
<tr>
<td>17</td>
<td>Max Flows Initiated</td>
</tr>
<tr>
<td>18</td>
<td>New Flows Initiated</td>
</tr>
<tr>
<td>19</td>
<td>SYNS Received</td>
</tr>
<tr>
<td>20</td>
<td>High File Sharing Index</td>
</tr>
<tr>
<td>24</td>
<td>Suspect UDP Activity</td>
</tr>
<tr>
<td>25</td>
<td>MAC Address Violation</td>
</tr>
<tr>
<td>26</td>
<td>Half Open Attack</td>
</tr>
<tr>
<td>28</td>
<td>Touched</td>
</tr>
<tr>
<td>29</td>
<td>Low Traffic</td>
</tr>
<tr>
<td>30</td>
<td>High Traffic</td>
</tr>
<tr>
<td>31</td>
<td>Watch Host Active</td>
</tr>
<tr>
<td>32</td>
<td>High Concern Index</td>
</tr>
<tr>
<td>33</td>
<td>Suspect Long Flow</td>
</tr>
<tr>
<td>34</td>
<td>Trapped Host</td>
</tr>
<tr>
<td>35</td>
<td>Worm Activity</td>
</tr>
<tr>
<td>36</td>
<td>Worm Propagation</td>
</tr>
<tr>
<td>37</td>
<td>Max Flows Served</td>
</tr>
<tr>
<td>38</td>
<td>New Flows Served</td>
</tr>
<tr>
<td>39</td>
<td>Beaconing Host</td>
</tr>
<tr>
<td>40</td>
<td>Suspect Data Loss</td>
</tr>
<tr>
<td>41</td>
<td>Bot Infected Host - Attempted C&amp;C Activity</td>
</tr>
<tr>
<td>42</td>
<td>Bot Infected Host - Successful C&amp;C Activity</td>
</tr>
<tr>
<td>43</td>
<td>Bot Command &amp; Control Server</td>
</tr>
<tr>
<td>44</td>
<td>Slow Connection Flood</td>
</tr>
<tr>
<td>45</td>
<td>Data Exfiltration</td>
</tr>
<tr>
<td>46</td>
<td>Command and Control</td>
</tr>
<tr>
<td>47</td>
<td>Policy Violation</td>
</tr>
<tr>
<td>48</td>
<td>Suspect Quiet Long Flow</td>
</tr>
<tr>
<td>49</td>
<td>UDP Received</td>
</tr>
<tr>
<td>50</td>
<td>ICMP Received</td>
</tr>
<tr>
<td>51</td>
<td>Recon</td>
</tr>
<tr>
<td>52</td>
<td>Data Hoarding</td>
</tr>
<tr>
<td>53</td>
<td>High DDOS Target Index</td>
</tr>
<tr>
<td>54</td>
<td>High DDOS Source Index</td>
</tr>
<tr>
<td>55</td>
<td>Port Scan</td>
</tr>
<tr>
<td>Page</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>56</td>
<td>Exploitation</td>
</tr>
<tr>
<td>57</td>
<td>Anomaly</td>
</tr>
<tr>
<td>58</td>
<td>Brute Force Login</td>
</tr>
<tr>
<td>59</td>
<td>Talks to Phantoms</td>
</tr>
<tr>
<td>60</td>
<td>High SMB Peers</td>
</tr>
<tr>
<td>61</td>
<td>SSH Reverse Shell</td>
</tr>
<tr>
<td>62</td>
<td>Fake Application Detected</td>
</tr>
<tr>
<td>63</td>
<td>Scanner Talking</td>
</tr>
<tr>
<td>257</td>
<td>Ping</td>
</tr>
<tr>
<td>258</td>
<td>ICMP TimeOut</td>
</tr>
<tr>
<td>259</td>
<td>TimeOut UDP</td>
</tr>
<tr>
<td>260</td>
<td>TimeOut TCP</td>
</tr>
<tr>
<td>261</td>
<td>Reset UDP</td>
</tr>
<tr>
<td>262</td>
<td>Reset TCP</td>
</tr>
<tr>
<td>263</td>
<td>Bad Flag All</td>
</tr>
<tr>
<td>264</td>
<td>Bad Flag SYN FYN</td>
</tr>
<tr>
<td>265</td>
<td>Bad Flag Reserved (Sflow Only)</td>
</tr>
<tr>
<td>266</td>
<td>Bad Flag RST</td>
</tr>
<tr>
<td>267</td>
<td>Bad Flag ACK</td>
</tr>
<tr>
<td>268</td>
<td>Bad Flag URG</td>
</tr>
<tr>
<td>269</td>
<td>Bad Flag No Flag</td>
</tr>
<tr>
<td>271</td>
<td>Stealth Scan UDP</td>
</tr>
<tr>
<td>272</td>
<td>Stealth Scan TCP</td>
</tr>
<tr>
<td>273</td>
<td>SRC=DES</td>
</tr>
<tr>
<td>276</td>
<td>Addr Scan TCP</td>
</tr>
<tr>
<td>277</td>
<td>Ping Scan</td>
</tr>
<tr>
<td>278</td>
<td>Ping Oversized Packet</td>
</tr>
<tr>
<td>281</td>
<td>Frag Pkt Too Short</td>
</tr>
<tr>
<td>282</td>
<td>Frag Pkt Too Long</td>
</tr>
<tr>
<td>283</td>
<td>Frag Different Sizes</td>
</tr>
<tr>
<td>286</td>
<td>Addr Scan UDP</td>
</tr>
<tr>
<td>289</td>
<td>ICMP Net Unreachable</td>
</tr>
<tr>
<td>290</td>
<td>ICMP Host Unreachable</td>
</tr>
<tr>
<td>291</td>
<td>ICMP Protocol Unreachable</td>
</tr>
<tr>
<td>292</td>
<td>ICMP Port Unreachable</td>
</tr>
<tr>
<td>293</td>
<td>ICMP Frag Needed</td>
</tr>
<tr>
<td>294</td>
<td>ICMP SRC Route Failed</td>
</tr>
<tr>
<td>295</td>
<td>ICMP Dest Network Unknown</td>
</tr>
<tr>
<td>296</td>
<td>ICMP Dest Host Unknown</td>
</tr>
<tr>
<td>297</td>
<td>ICMP Src Host Isolated</td>
</tr>
<tr>
<td>298</td>
<td>ICMP Dest Net Admin</td>
</tr>
<tr>
<td>299</td>
<td>ICMP Dst Host Admin</td>
</tr>
<tr>
<td>300</td>
<td>ICMP Net Unreachable TOS</td>
</tr>
<tr>
<td>301</td>
<td>ICMP Host Unreachable TOS</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>302</td>
<td>ICMP Comm Admin</td>
</tr>
<tr>
<td>303</td>
<td>ICMP Host Precedence</td>
</tr>
<tr>
<td>304</td>
<td>ICMP Precedence Cutoff</td>
</tr>
<tr>
<td>310</td>
<td>Flow Denied</td>
</tr>
<tr>
<td>315</td>
<td>Suspect Data Hoarding</td>
</tr>
<tr>
<td>316</td>
<td>Target Data Hoarding</td>
</tr>
<tr>
<td>317</td>
<td>Connection From TOR Attempted</td>
</tr>
<tr>
<td>318</td>
<td>Connection From TOR Successful</td>
</tr>
<tr>
<td>319</td>
<td>Inside TOR Exit Detected</td>
</tr>
<tr>
<td>513</td>
<td>Connection to TOR Attempted</td>
</tr>
<tr>
<td>514</td>
<td>Connection to TOR Successful</td>
</tr>
<tr>
<td>515</td>
<td>Inside TOR Entry Detected</td>
</tr>
<tr>
<td>516</td>
<td>Connection To Bogon Address Successful</td>
</tr>
<tr>
<td>517</td>
<td>Connection From Bogon Address Successful</td>
</tr>
<tr>
<td>518</td>
<td>Connection To Bogon Address Attempted</td>
</tr>
<tr>
<td>519</td>
<td>Connection From Bogon Address Attempted</td>
</tr>
<tr>
<td>4010</td>
<td>FlowCollector Flow Date Lost</td>
</tr>
<tr>
<td>4020</td>
<td>Interface Utilization Exceeded Inbound</td>
</tr>
<tr>
<td>4030</td>
<td>Interface Utilization Exceeded Outbound</td>
</tr>
<tr>
<td>5010</td>
<td>FlowSensor VE Configuration Error</td>
</tr>
<tr>
<td>5011</td>
<td>FlowSensor Traffic Lost</td>
</tr>
<tr>
<td>5012</td>
<td>FlowSensor RAID Failure</td>
</tr>
<tr>
<td>5013</td>
<td>FlowSensor RAID Rebuilding</td>
</tr>
<tr>
<td>5998</td>
<td>FlowSensor Time Mismatch</td>
</tr>
<tr>
<td>5999</td>
<td>FlowSensor Management Channel Down</td>
</tr>
<tr>
<td>6010</td>
<td>New VM</td>
</tr>
<tr>
<td>6020</td>
<td>V-Motion</td>
</tr>
<tr>
<td>7001</td>
<td>Relationship High Total Traffic</td>
</tr>
<tr>
<td>7002</td>
<td>Relationship High Traffic</td>
</tr>
<tr>
<td>7003</td>
<td>Relationship Low Traffic</td>
</tr>
<tr>
<td>7004</td>
<td>Relationship Max Flows</td>
</tr>
<tr>
<td>7005</td>
<td>Relationship New Flows</td>
</tr>
<tr>
<td>7006</td>
<td>Relationship Round Trip Time</td>
</tr>
<tr>
<td>7007</td>
<td>Relationship Server Response Time</td>
</tr>
<tr>
<td>7008</td>
<td>Relationship TCP Retransmission Ratio</td>
</tr>
<tr>
<td>7009</td>
<td>Relationship SYN Flood</td>
</tr>
<tr>
<td>7010</td>
<td>Relationship UDP Flood</td>
</tr>
<tr>
<td>7011</td>
<td>Relationship ICMP Flood</td>
</tr>
<tr>
<td>9021</td>
<td>FlowCollector Data Deleted</td>
</tr>
<tr>
<td>9022</td>
<td>FlowCollector Database Unavailable</td>
</tr>
<tr>
<td>9023</td>
<td>FlowCollector Database Channel Down</td>
</tr>
<tr>
<td>9040</td>
<td>FlowCollector Log Retention Reduced</td>
</tr>
<tr>
<td>9050</td>
<td>FlowCollector Exporter Count Exceeded</td>
</tr>
<tr>
<td>9051</td>
<td>FlowCollector FlowSensor VE Count Exceeded</td>
</tr>
</tbody>
</table>
### 4.6 Security Event Types

#### 4.6.1 In previous versions, these were known as CI Events

**NOTE:** Some previously used alarms are now obsolete and no longer listed in this file.

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Host Lock Violation</td>
</tr>
<tr>
<td>5</td>
<td>SYN Flood</td>
</tr>
<tr>
<td>6</td>
<td>UDP Flood</td>
</tr>
<tr>
<td>7</td>
<td>ICMP Flood</td>
</tr>
<tr>
<td>8</td>
<td>Packet Flood</td>
</tr>
<tr>
<td>9</td>
<td>High Volume Email</td>
</tr>
<tr>
<td>10</td>
<td>Mail Relay</td>
</tr>
<tr>
<td>11</td>
<td>Spam Source</td>
</tr>
<tr>
<td>12</td>
<td>Mail Rejects</td>
</tr>
<tr>
<td>13</td>
<td>Watch Port Active</td>
</tr>
<tr>
<td>14</td>
<td>New Host Active</td>
</tr>
<tr>
<td>15</td>
<td>High Target Index</td>
</tr>
<tr>
<td>16</td>
<td>High Total Traffic</td>
</tr>
<tr>
<td>17</td>
<td>Max Flows Initiated</td>
</tr>
<tr>
<td>18</td>
<td>New Flows Initiated</td>
</tr>
<tr>
<td>19</td>
<td>SYNS Received</td>
</tr>
<tr>
<td>20</td>
<td>High File Sharing Index</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>24</td>
<td>Suspect UDP Activity</td>
</tr>
<tr>
<td>25</td>
<td>MAC Address Violation</td>
</tr>
<tr>
<td>26</td>
<td>Half Open Attack</td>
</tr>
<tr>
<td>28</td>
<td>Touched</td>
</tr>
<tr>
<td>29</td>
<td>Low Traffic</td>
</tr>
<tr>
<td>30</td>
<td>High Traffic</td>
</tr>
<tr>
<td>31</td>
<td>Watch Host Active</td>
</tr>
<tr>
<td>32</td>
<td>High Concern Index</td>
</tr>
<tr>
<td>33</td>
<td>Suspect Long Flow</td>
</tr>
<tr>
<td>34</td>
<td>Trapped Host</td>
</tr>
<tr>
<td>35</td>
<td>Worm Activity</td>
</tr>
<tr>
<td>36</td>
<td>Worm Propagation</td>
</tr>
<tr>
<td>37</td>
<td>Max Flows Served</td>
</tr>
<tr>
<td>38</td>
<td>New Flows Served</td>
</tr>
<tr>
<td>39</td>
<td>Beaconing Host</td>
</tr>
<tr>
<td>40</td>
<td>Suspect Data Loss</td>
</tr>
<tr>
<td>41</td>
<td>Bot Infected Host - Attempted C&amp;C Activity</td>
</tr>
<tr>
<td>42</td>
<td>Bot Infected Host - Successful C&amp;C Activity</td>
</tr>
<tr>
<td>43</td>
<td>Bot Command &amp; Control Server</td>
</tr>
<tr>
<td>44</td>
<td>Slow Connection Flood</td>
</tr>
<tr>
<td>45</td>
<td>Data Exfiltration</td>
</tr>
<tr>
<td>46</td>
<td>Command and Control</td>
</tr>
<tr>
<td>47</td>
<td>Policy Violation</td>
</tr>
<tr>
<td>48</td>
<td>Suspect Quiet Long Flow</td>
</tr>
<tr>
<td>49</td>
<td>UDP Received</td>
</tr>
<tr>
<td>50</td>
<td>ICMP Received</td>
</tr>
<tr>
<td>51</td>
<td>Recon</td>
</tr>
<tr>
<td>52</td>
<td>Data Hoarding</td>
</tr>
<tr>
<td>53</td>
<td>High DDOS Target Index</td>
</tr>
<tr>
<td>54</td>
<td>High DDOS Source Index</td>
</tr>
<tr>
<td>55</td>
<td>Port Scan</td>
</tr>
<tr>
<td>56</td>
<td>Exploitation</td>
</tr>
<tr>
<td>57</td>
<td>Anomaly</td>
</tr>
<tr>
<td>58</td>
<td>Brute Force Login</td>
</tr>
<tr>
<td>59</td>
<td>Talks to Phantoms</td>
</tr>
<tr>
<td>60</td>
<td>High SMB Peers</td>
</tr>
<tr>
<td>61</td>
<td>SSH Reverse Shell</td>
</tr>
<tr>
<td>62</td>
<td>Fake Application Detected</td>
</tr>
<tr>
<td>63</td>
<td>Scanner Talking</td>
</tr>
<tr>
<td>257</td>
<td>Ping</td>
</tr>
<tr>
<td>258</td>
<td>ICMP TimeOut</td>
</tr>
<tr>
<td>259</td>
<td>TimeOut UDP</td>
</tr>
<tr>
<td>260</td>
<td>TimeOut TCP</td>
</tr>
<tr>
<td>261</td>
<td>Reset UDP</td>
</tr>
</tbody>
</table>
### 4.7 ICMP Types

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Echo Reply</td>
</tr>
<tr>
<td>1</td>
<td>Reserved 1</td>
</tr>
<tr>
<td>2</td>
<td>Reserved 2</td>
</tr>
<tr>
<td>3</td>
<td>Destination Unreachable</td>
</tr>
<tr>
<td>4</td>
<td>Source Quench</td>
</tr>
<tr>
<td>5</td>
<td>Redirect</td>
</tr>
<tr>
<td>6</td>
<td>Alternate Host Address</td>
</tr>
<tr>
<td>7</td>
<td>Reserved 7</td>
</tr>
<tr>
<td>8</td>
<td>Echo Request</td>
</tr>
<tr>
<td>9</td>
<td>Router Advertisement</td>
</tr>
<tr>
<td>10</td>
<td>Router Solicitation</td>
</tr>
<tr>
<td>11</td>
<td>Time Exceeded</td>
</tr>
<tr>
<td>12</td>
<td>Parameter Problem</td>
</tr>
<tr>
<td>13</td>
<td>Timestamp</td>
</tr>
<tr>
<td>14</td>
<td>Timestamp Reply</td>
</tr>
<tr>
<td>15</td>
<td>Information Request</td>
</tr>
<tr>
<td>16</td>
<td>Information Reply</td>
</tr>
<tr>
<td>17</td>
<td>Address Mask Request</td>
</tr>
<tr>
<td>18</td>
<td>Address Mask Reply</td>
</tr>
<tr>
<td>19</td>
<td>Reserved 19</td>
</tr>
<tr>
<td>20</td>
<td>Reserved 20</td>
</tr>
<tr>
<td>21</td>
<td>Reserved 21</td>
</tr>
<tr>
<td>22</td>
<td>Reserved 22</td>
</tr>
<tr>
<td>23</td>
<td>Reserved 23</td>
</tr>
<tr>
<td>24</td>
<td>Reserved 24</td>
</tr>
<tr>
<td>25</td>
<td>Reserved 25</td>
</tr>
<tr>
<td>26</td>
<td>Reserved 26</td>
</tr>
<tr>
<td>27</td>
<td>Reserved 27</td>
</tr>
<tr>
<td>28</td>
<td>Reserved 28</td>
</tr>
<tr>
<td>29</td>
<td>Reserved 29</td>
</tr>
<tr>
<td>30</td>
<td>Traceroute</td>
</tr>
<tr>
<td>31</td>
<td>Datagram Conversion Error</td>
</tr>
<tr>
<td>32</td>
<td>Mobile Host Redirect</td>
</tr>
<tr>
<td>33</td>
<td>Where-Are-You</td>
</tr>
<tr>
<td>34</td>
<td>I-Am-Here</td>
</tr>
<tr>
<td>35</td>
<td>Mobile Registration Request</td>
</tr>
<tr>
<td>36</td>
<td>Mobile Registration Reply</td>
</tr>
<tr>
<td>37</td>
<td>Domain Name Request</td>
</tr>
<tr>
<td>38</td>
<td>Domain Name Reply</td>
</tr>
<tr>
<td>39</td>
<td>Reserved 39</td>
</tr>
<tr>
<td>40</td>
<td>Photuris</td>
</tr>
</tbody>
</table>
5 Examples of Accessing SMC Web Services

Below are some very simplistic examples of using the Web Services API

5.1 Using ‘wget’

Note: As of v6.X, the ‘-auth-no-challenge’ must be included as a ‘wget’ option due to a change to session based authentication by the SMC. Otherwise, a '401 error (unknown authentication scheme)' will result from the SOAP request.

5.1.1 ‘getDomain’ request example

Contents of an example getDomainRequest.xml file:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<soapenc:Envelope
    xmlns:soapenc="http://schemas.xmlsoap.org/soap/envelope/"
>
    <soapenc:Body>
        <getDomain>
            <domain id="117"/>
        </getDomain>
    </soapenc:Body>
</soapenc:Envelope>
```

'wget' command syntax in a 'bash' shell context:

```
wget --post-file=getDomainRequest.xml --http-user=admin --ht --auth-no-challenge \
http-password=xxxxxxxx --no-check-certificate -O responseDomain.xml \
https://smc1.mydomain.com/smc/swsService/configuration
```

5.1.2 ‘getHostSnapshot’ request

Contents of an example getHostSnapshot.xml file:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<soapenc:Envelope
    xmlns:soapenc="http://schemas.xmlsoap.org/soap/envelope/"
>
    <soapenc:Body>
        <getHostSnapshot>
            <host-filter domain-id="117">
                <host-selection>
                    <ip-address-selection value="10.203.1.110"/>
                </host-selection>
            </host-filter>
        </getHostSnapshot>
    </soapenc:Body>
</soapenc:Envelope>
```

'wget' command syntax in a 'bash' shell context:

```
wget --post-file=getHostSnapshot.xml --http-user=admin --ht --auth-no-challenge \
http-password=xxxxxxxx --no-check-certificate -O reponseHostSnapshot.xml \
https://smc1.mydomain.com/smc/swsService/hosts
```
5.2 Using ‘curl’

5.2.1 ‘getHostInformation’ request

Contents of an example getHostInfo.xml file:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<soapenc:Envelope
xmlns:soapenc="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenc:Body>
    <getHostInformation>
      <host-information-filter max-rows="2000" domain-id="117">
        <date-selection>
          <day-range-selection day-count="1"/>
        </date-selection>
      </host-information-filter>
    </getHostInformation>
  </soapenc:Body>
</soapenc:Envelope>
```

‘curl’ command syntax in a ‘bash’ shell context:

```
curl --tcp-nodelay -m 1 -o responseHostInfo.xml -u admin:mypassword -k -d@getHostInfo.xml \
https://smc1.mydomain.com/smc/swsService/hosts
```

5.2.2 ‘getSecurityEvents’ request

Contents of an example SecurityEventsReq.xml file:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<soapenc:Envelope
xmlns:soapenc="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenc:Body>
    <getSecurityEvents>
      <security-event-filter domain-id="117">
        <host-selection>
          <host-pair-selection direction="BETWEEN_SELECTION_1_SELECTION_2">
            <selection-1>
              <ip-address-list-selection>
                <ip-address value="10.203.1.110"/>
              </ip-address-list-selection>
            </selection-1>
          </host-pair-selection>
        </host-selection>
      </security-event-filter>
    </getSecurityEvents>
  </soapenc:Body>
</soapenc:Envelope>
```

‘curl’ command syntax in a ‘bash’ shell context:

```
curl --tcp-nodelay -m 1 -o SecurityEventsReq.xml -u admin:mypassword -k -d@SecurityEventsReq.xml \
https://smc1.mydomain.com/smc/swsService/security
```
5.3 Using ‘python’

5.3.1 ‘addDomain’ request

This simplistic python script uses a file retrieved via a ‘getDomain’ Web Services call to restore the domain configuration to the SMC.

```python
from lxml import etree
import pycurl

def smcRequest(url, request):
    response_file = open("responseAddDomain.xml", "w")
    co = pycurl.Curl()
    co.setopt(co.UNRESTRICTED_AUTH, 1)
    co.setopt(co.URL, url)
    co.setopt(co.POST, 1)
    co.setopt(co.WRITEDATA, response_file)
    co.setopt(co.INFILESIZE, len(request) + 1)
    co.setopt(co.POSTFIELDS, request)
    co.setopt(co.USERPWD, "admin:mypassword")
    try :
        co.perform()
    except :
        print "POST failed"
        exit(1)
    co.close()
    response_file.close()

    # tidy up the response for human readability
    parsed = etree.parse("responseAddDomain.xml")
    request = header + etree.tostring(parsed, pretty_print = True)
    response_file = open("responseAddDomain.xml", "w")
    response_file.write(request)
    response_file.close()
    return(request)

def addDomain(domain_id, domain_file):
    # assume the 'domain_file' is from a previous "getDomain" request
    try :
        parsed = etree.parse(domain_file)
        request = header + etree.tostring(parsed, pretty_print = True)
    except :
        print "Malformed input file : %s" % domain_file
        exit(1)
    return(request.replace("getDomainResponse","addDomain"))

def main():
    domainID = 117
    xml = addDomain(domainID, "responseDomain.xml")
    url = "https://smc1.mydomain.com/smc/swsService/configuration"
    response = smcRequest(url, xml)
    print response

if __name__ == "__main__":
    main()
```

Index

5-min..........................................................37
access control ...............................................6
active .......................................................44, 45, 46, 48
active time selection .....................................79
active-dest-list ...........................................41
active-source-list .......................................41
active-time-selection...............................15, 28
addDomain..................................................72
addHostGroup ...........................................66, 67
addHostGroupIPRange ...................................69
addressing...................................................6
Alarm Configuration .....................................75
Alarm Filtering ...........................................52
alarm types, table .......................................85
alarm-configuration .....................................75
alarm-counts .............................................43
alarm-counts-list .......................................42
alarm-list ................................................43
alarms ......................................................53, 55
alarms-counts ............................................42
alarm-severity ...........................................75
alarm-type ................................................43
alerts .........................................................53, 55
application .................................................26
Application Definitions ...............................76
application-activity ......................................35, 55
application-id ............................................8, 22
applications ...............................................17
Applications Filtering ..................................17
ascii ..........................................................26
as-configuration .........................................73
asn .............................................................23
ASN filtering ...............................................19
as-numbers ...............................................19
authentication ...........................................6
auth-method ................................................62, 65
auth-password ............................................62, 65
auto-add ....................................................61, 64
Autonomous System Number ......................19
Autonomous System Number Configuration ....73
average .....................................................56
average-bps ...............................................39, 42
average-pps ................................................42
avg-rtt .......................................................39
avg-srt ......................................................40
been-touched ............................................36
bytes .........................................................23, 25, 56
bytes-received ..........................................39
bytes-sent ...............................................39
CI Event Filtering ........................................53
ci-event ......................................................57
ci-events ...................................................37, 53
ci-points ...................................................29, 30, 31
Cisco ISE Configuration .............................74
cisco-ise ...................................................74
cisco-ise-list .............................................74
client .........................................................22, 24, 45, 48
Client Ports Filtering ..................................20
client-ports ...............................................20
client-service-list .....................................51
closest-interface .........................................41, 57
closest-interface-list .................................41
community ...............................................62, 65
Concern Index ..........................................35
Concern Index Events .................................57
Concern Index Filtering ............................29
concern-index .............................................56
data-loss .....................................................56
data-loss-threshold .....................................37
Date & Time Filtering .................................78
Date and Time Filtering ............................49
date-selection ...........................................11, 14, 27, 31, 78
day ...........................................................37
day range selection .....................................79
day selection .............................................79
day-selection .............................................31
description ...............................................63
details .......................................................30, 43
details-list ...............................................30
device filtering ..........................................81
device list selection .................................81
device-id .................................................43, 45, 46, 47, 54, 58
device-list-selection ..................15, 28, 32
device-selection ..........................................11, 15, 28, 31, 52, 81
dhcp-lease ...................................................47, 48
dhcp-lease-list .........................................47
SMC Web Services Programming Guide
<p>| differentia l services code point filtering | 19 |
| direction | 25, 84 |
| domain | 47, 58, 60, 63, 64 |
| domain-id | 8, 12, 14, 22, 27, 30, 31, 33, 34, 35, 36, 41, 42, 43, 44, 46, 47, 48, 49, 54, 57, 58, 66, 68, 69, 70, 71 |
| dscp | 12, 25 |
| DSCP filtering | 19, 20 |
| dscp-list | 19 |
| dscp-traffic | 12 |
| dscp-traffic-filter | 11 |
| dscp-traffic-list | 12 |
| duration | 78 |
| end-time | 44, 45, 46, 48 |
| exclude | 16, 17, 19, 20 |
| exporter | 61, 64 |
| exporter selection | 81 |
| exporter-ip | 12, 25, 41, 58 |
| exporter-list | 61, 64 |
| exporters | 40, 41 |
| Exporters | 24, 57 |
| exporter-selection | 15 |
| exporter-type | 61 |
| External Devices Configuration | 75 |
| external-device | 75 |
| external-device-list | 75 |
| file-sharing-index | 57 |
| filter semantics | 8 |
| fin | 24 |
| first-last-time selection | 80 |
| first-last-time-selection | 15, 28 |
| first-seen | 34 |
| flags | 23 |
| flow | 21, 38 |
| flow-filter | 13, 14 |
| flow-list | 21 |
| flows | 38 |
| flowsensor | 26 |
| getDomain | 72 |
| getFlows | 13 |
| getHostGroups | 58 |
| getHostInformation | 49 |
| getHostSnapshot | 31 |
| getSecurityEvents | 27 |
| has-touched | 36 |
| high-traffic | 56 |
| high-value | 18, 29 |
| hit-count | 29, 31 |
| Host filtering | 82 |
| Host Filtering | 82 |
| Host Group ID | 60 |
| Host Group Relationships Configuration | 76 |
| Host Group Selection | 82 |
| Host Group Tree | 73 |
| Host Locking Configuration | 76 |
| Host Pair Selection | 83 |
| host-baselines | 66, 68 |
| host-filter | 31 |
| host-group | 59, 66, 68, 69, 70, 73 |
| host-group-id | 8 |
| host-group-ids | 8, 23, 30, 33, 34, 44, 45, 46, 48, 49, 54 |
| host-group-selection | 50 |
| host-group-tree | 58, 60, 73 |
| host-information | 34, 53, 54 |
| host-information-filter | 49 |
| host-information-list | 34, 53 |
| host-name | 23, 30, 33, 44, 45, 46, 47, 48, 54 |
| host-note | 48 |
| host-note-list | 48 |
| host-notes-list | 48 |
| host-pair-selection | 15, 28, 50 |
| host-selection | 15, 28, 32, 82 |
| host-snapshot | 32 |
| host-trap | 66, 68 |
| hybrid-pair-ip | 61 |
| icmp | 57 |
| ICMP type | 16 |
| ICMP Types | 91 |
| id | 43, 69, 70, 77 |
| identifiers | 8 |
| if-index | 12, 25, 41, 58, 63 |
| ignore-v5-egress | 61 |
| inside-hosts | 59, 60, 73 |
| interface | 25, 58, 63 |
| Interface Selection | 81 |
| interface-list | 23, 24, 58 |
| interface-selection | 12, 15 |
| interface-status | 41, 42 |
| intergroup-locking-list | 76 |
| internal-as-numbers | 73 |
| inverse-suppression | 66, 68 |
| ip | 64 |
| IP address list selection | 82 |
| IP address range selection | 82 |
| IP Address Ranges | 69 |
| IP address selection | 83 |
| IP protocol | 16 |
| IP Ranges | 69, 70 |
| ip-address | 23, 30, 33, 44, 45, 46, 47, 48, 54 |
| ip-address-range | 71 |
| ip-address-ranges | 67, 68, 69, 70, 71 |
| ip-address-range-selection | 50 |
| ip-address-selection | 32 |
| ip-list-selection | 50 |</p>
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java Web Start</td>
<td>9</td>
</tr>
<tr>
<td>last-seen</td>
<td>34</td>
</tr>
<tr>
<td>last-time</td>
<td>22, 30, 39</td>
</tr>
<tr>
<td>low-traffic</td>
<td>56</td>
</tr>
<tr>
<td>low-value</td>
<td>18, 29</td>
</tr>
<tr>
<td>MAC address</td>
<td>34</td>
</tr>
<tr>
<td>mpls-label</td>
<td>20, 21</td>
</tr>
<tr>
<td>mpls-labels</td>
<td>22</td>
</tr>
<tr>
<td>name</td>
<td>45, 46, 47, 48, 54</td>
</tr>
<tr>
<td>nbar</td>
<td>26</td>
</tr>
<tr>
<td>Network Performance Statistics Filtering</td>
<td>18</td>
</tr>
<tr>
<td>network-performance</td>
<td>18</td>
</tr>
<tr>
<td>new-flows-initiated</td>
<td>57</td>
</tr>
<tr>
<td>new-flows-served</td>
<td>57</td>
</tr>
<tr>
<td>Operating System</td>
<td>55</td>
</tr>
<tr>
<td>Operating System Filtering</td>
<td>52</td>
</tr>
<tr>
<td>operating-system</td>
<td>52</td>
</tr>
<tr>
<td>operator</td>
<td>51, 52, 53</td>
</tr>
<tr>
<td>order-by</td>
<td>14</td>
</tr>
<tr>
<td>order-by-desc</td>
<td>14</td>
</tr>
<tr>
<td>os</td>
<td>55</td>
</tr>
<tr>
<td>outside-hosts</td>
<td>59, 60, 73</td>
</tr>
<tr>
<td>packet data</td>
<td>25</td>
</tr>
<tr>
<td>packets</td>
<td>23, 25, 56</td>
</tr>
<tr>
<td>packetshaper</td>
<td>26</td>
</tr>
<tr>
<td>parent-id</td>
<td>66, 68</td>
</tr>
<tr>
<td>Password</td>
<td>61</td>
</tr>
<tr>
<td>payload</td>
<td>23, 26</td>
</tr>
<tr>
<td>Payload Filtering</td>
<td>20</td>
</tr>
<tr>
<td>payload-match-all</td>
<td>21</td>
</tr>
<tr>
<td>payload-match-any</td>
<td>21</td>
</tr>
<tr>
<td>payload-not-match-all</td>
<td>21</td>
</tr>
<tr>
<td>Policy Configuration</td>
<td>73</td>
</tr>
<tr>
<td>policy statistics</td>
<td>56</td>
</tr>
<tr>
<td>polling-interval</td>
<td>62, 65</td>
</tr>
<tr>
<td>port</td>
<td>23, 62, 65</td>
</tr>
<tr>
<td>port-number</td>
<td>51</td>
</tr>
<tr>
<td>Ports Filtering</td>
<td>16</td>
</tr>
<tr>
<td>prerequisites</td>
<td>5</td>
</tr>
<tr>
<td>priv-method</td>
<td>62, 65</td>
</tr>
<tr>
<td>priv-password</td>
<td>62, 65</td>
</tr>
<tr>
<td>profiled-service</td>
<td>51</td>
</tr>
<tr>
<td>profiled-service-list</td>
<td>51</td>
</tr>
<tr>
<td>profile-index</td>
<td>19, 20, 51</td>
</tr>
<tr>
<td>protocol</td>
<td>39, 51</td>
</tr>
<tr>
<td>Protocol Filtering</td>
<td>51</td>
</tr>
<tr>
<td>protocols</td>
<td>16</td>
</tr>
<tr>
<td>Protocols Filtering</td>
<td>16</td>
</tr>
<tr>
<td>query</td>
<td>21</td>
</tr>
<tr>
<td>removeDomain</td>
<td>77</td>
</tr>
<tr>
<td>remove-duplicates</td>
<td>14</td>
</tr>
<tr>
<td>removeExporters</td>
<td>63</td>
</tr>
<tr>
<td>removeHostGroupIPRange</td>
<td>70, 71</td>
</tr>
<tr>
<td>reset-hour</td>
<td>73</td>
</tr>
<tr>
<td>response</td>
<td>53</td>
</tr>
<tr>
<td>retention</td>
<td>12</td>
</tr>
<tr>
<td>retransmits</td>
<td>22</td>
</tr>
<tr>
<td>retries</td>
<td>65</td>
</tr>
<tr>
<td>role</td>
<td>39</td>
</tr>
<tr>
<td>roles</td>
<td>84</td>
</tr>
<tr>
<td>rst</td>
<td>24</td>
</tr>
<tr>
<td>rtt</td>
<td>27</td>
</tr>
<tr>
<td>security</td>
<td>35</td>
</tr>
<tr>
<td>Security Event Type Filtering</td>
<td>28</td>
</tr>
<tr>
<td>security-event</td>
<td>30</td>
</tr>
<tr>
<td>security-event-filter</td>
<td>27</td>
</tr>
<tr>
<td>security-event-list</td>
<td>29</td>
</tr>
<tr>
<td>security-list</td>
<td>35</td>
</tr>
<tr>
<td>server</td>
<td>22, 24, 45, 47, 48</td>
</tr>
<tr>
<td>server-service-list</td>
<td>51</td>
</tr>
<tr>
<td>service</td>
<td>22, 39</td>
</tr>
<tr>
<td>service codes</td>
<td>85</td>
</tr>
<tr>
<td>Service Filtering</td>
<td>50</td>
</tr>
<tr>
<td>Service Profile</td>
<td>54</td>
</tr>
<tr>
<td>service profile status</td>
<td>84</td>
</tr>
<tr>
<td>Service-Definitions</td>
<td>76</td>
</tr>
<tr>
<td>service-id</td>
<td>22</td>
</tr>
<tr>
<td>service-profile-status</td>
<td>35, 54</td>
</tr>
<tr>
<td>services</td>
<td>15</td>
</tr>
<tr>
<td>Services Filtering</td>
<td>15</td>
</tr>
<tr>
<td>services-definitions</td>
<td>15</td>
</tr>
<tr>
<td>setHostGroupIPRange</td>
<td>71</td>
</tr>
<tr>
<td>setHostGroups</td>
<td>59</td>
</tr>
<tr>
<td>snmp</td>
<td>61</td>
</tr>
<tr>
<td>SNMP Configuration</td>
<td>76</td>
</tr>
<tr>
<td>snmp-configuration</td>
<td>65</td>
</tr>
<tr>
<td>snmp-configuration-list</td>
<td>64, 65, 76</td>
</tr>
<tr>
<td>SOAP</td>
<td>6</td>
</tr>
<tr>
<td>source</td>
<td>30, 43</td>
</tr>
</tbody>
</table>