Suricata - Bug #3218

ssl_state does the wrong thing

10/04/2019 09:11 PM - Travis Green

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>OISF Dev</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td>4.1.5, 5.0rc1</td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
</tbody>
</table>

Description

The `ssl_state` keyword does not alert on the correct state when specified in the rule.

Example 1: should work with client_hello, but only works with server_hello

```
alert tls any any -> any [465,25,587] (msg:"Test 1 SNI in SMTPS incorrect state (server_hello)"; tls_sni; content:"flagstring";
flow:established,to_server; ssl_state:server_hello; classtype:attempted-admin; sid:1003923; rev:1;)
```

```
alert tls any any -> any [465,25,587] (msg:"Test 1 SNI in SMTPS desired state (client_hello)"; tls_sni; content:"flagstring";
flow:established,to_server; ssl_state:client_hello; classtype:attempted-admin; sid:1003924; rev:1;)
```

```
fast.log:
```

Example 2: should work with client_hello, but only works with server_keyx

```
alert tls any any -> any any (msg:"Test 2 SNI in HTTPS incorrect state (server_keyx)"; tls_sni; content:"www.google.com";
flow:established,to_server; ssl_state:server_keyx; classtype:attempted-admin; sid:1003925; rev:1;)
```

```
alert tls any any -> any any (msg:"Test 2 SNI in HTTPS correct state (client_hello)"; tls_sni; content:"www.google.com";
flow:established,to_server; ssl_state:client_hello; classtype:attempted-admin; sid:1003926; rev:1;)
```

```
fast.log:
```

Example 3: should only alert with server_hello state, instead alerts with client_keyx

```
alert tls any any -> any any (msg:"Test 3 HTTPS certificate incorrect state"; content:"Google Trust Services";
flow:established,to_client; ssl_state:client_keyx; classtype:attempted-admin; sid:1003928; rev:1;)
```

```
alert tls any any -> any any (msg:"Test 3 HTTPS certificate desired state"; content:"Google Trust Services";
flow:established,to_client; ssl_state:server_hello; classtype:attempted-admin; sid:1003929; rev:1;)
```

```
fast.log
```

Tested with:
5.0.0-dev (9340769ad 2019-09-29)
4.1.5 RELEASE (with and without rust)

History

#1 - 10/07/2019 08:57 PM - Andreas Herz
- Assignee set to OISF Dev

06/13/2020 1/2
Can you create some SV tests out of these pcaps/rules?

<table>
<thead>
<tr>
<th>Files</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>slice_smtps.pcap</td>
<td>8.25 KB</td>
<td>10/04/2019</td>
<td>Travis Green</td>
</tr>
<tr>
<td>slice_https.pcap</td>
<td>55.5 KB</td>
<td>10/04/2019</td>
<td>Travis Green</td>
</tr>
</tbody>
</table>