How to disable SecureXL for specific IP addresses

Solution ID	sk104468
Product	SecureXL
Version	All
OS	Gaia, SecurePlatform, SecurePlatform 2.6, Crossbeam XOS
Platform / Model	All
Date Created	29-Jan-2015
Last Modified	22-Jun-2016

Solution

Background

Disabling SecureXL allows to see the complete connection in FW Monitor, which may be required for troubleshooting purposes.

Disabling SecureXL for traffic sent from/to specific IP addresses might be needed when it is not possible to disable SecureXL completely due to high traffic load on Security Gateway.

Procedure

1. For R76, R75.45 and lower: Contact Check Point Support to get a Hotfix that will add this feature.
   A Support Engineer will make sure the Hotfix is compatible with your environment before providing the Hotfix.
   For faster resolution and verification, please collect CPinfo files from the Security Management Server and Security Gateways involved in the case.

2. Connect to command line on the Security Management Server / Multi-Domain Security Management Server that manages the involved Security Gateway / Cluster.

3. Log in to Expert mode.

4. In the relevant table.def file, define the IP addresses, whose traffic should not be accelerated:

   Note: For locations of these files, refer to sk98339 - Location of 'table.def' files on Security Management Server.

   A. Search for this section (located near the end of this file):

```
/*
 * The following tables force TCP and UDP connections to be
 * forwarded to the firewall according to their tuples.
 *
 * src          Source IP address
 * dst          Destination IP address
 * dport        Destination port
 */
/* tcp_f2f_ports = { <dport> }; */
/* udp_f2f_ports = { <dport> }; */
/* tcp_f2f_conns = { <src, dest, dport> }; */
/* udp_f2f_conns = { <src, dest, dport> }; */
```

   B. Add a new section with the relevant IP addresses under the above section:

```
f2f_addresses =
{
<IP_ADDRESS_1> ,
<IP_ADDRESS_2> ,
<IP_ADDRESS_3>
};
```

   Important Notes:

   - Currently, network addresses are not supported - only separate IP addresses can be specified (you can use any IPs generator (even Microsoft Excel) to quickly generate all the required IP addresses)
   - Each IP address must be enclosed in < >
   - IP addresses must be separated by comma - except after the last IP address in this list

   C. Save the changes in the file.

5. Connect with SmartDashboard to Security Management Server / Domain Management Server.

6. Install the policy onto the relevant Security Gateway / Cluster object.

7. Verify that the IP addresses you defined in the relevant table.def file were transferred to Security Gateway / each cluster member by the policy installation:

```
[Expert@HostName]# fw tab -t f2f_addresses
```

The output should show the defined IP addresses in Hexadecimal network order format.

Example: If you defined IP 192.168.100.200, then the output should show C0A864C8.