26 May 2016

Check Point APIs

R80

Reference Guide

Check Point
SOFTWARE TECHNOLOGIES LTD.

Introducing Check Point APIs

Check Point APIs let system administrators and developers make changes to the security policy with CLI tools and web-services. You can use an API to:

- Use an automated script to perform common tasks
- Integrate Check Point products with 3rd party solutions
- Create products that use and enhance the Check Point solution

Overview

R80 Management API

R80 Security Management Servers support hundreds of API calls to let you perform many tasks that are usually done with the SmartConsole. These are the procedures you can use to make API calls:

- SmartConsole CLI - From SmartConsole, you can open a CLI window end enter API commands
- mgmt_cli Tool - Runs in Expert mode and lets you enter commands from a Windows or Linux computer

  Note - You must enter the username and password with the mgmt_cli tool procedure
- Gaia CLI - Log in to the Gaia operating system with an administrator account on the Security Management Server and enter API commands
- Web Services - Send HTTPS Post requests to the Security Management Server

For more about how to use the R80 Management API, go to the Check Point Community https://community.checkpoint.com/welcome and see the *Management API Reference* https://sc1.checkpoint.com/documents/R80/APIs/index.html#introduction.

Sample Command with SmartConsole CLI

You can use the `add host` command to create a new host and then publish the changes.

```
> add host name "Sample_Host" ip-address "192.0.2.3"
> publish
```

R77 Threat Prevention API

The Check Point Threat Prevention Web Service API lets you control these Threat Prevention products:

- Threat Emulation
- Anti-Virus
- Threat Extraction

The Threat Prevention API is a cloud service, with dynamic updates for feature extensions. This API uses JSON requests and responses for functionality similar to NGTX and TX appliances.

For more how to use the R77 Threat Prevention API, see the *Threat Prevention API Reference Guide* http://supportcontent.checkpoint.com/documentation_download?ID=43199.

Sample Command of the Threat Prevention API:

This is an example Request to send a web service query to the databases for Threat Emulation and Anti-Virus results of the file with the specified MD5 signature. The query outputs the results to XML and PDF formats, for Threat Emulation, on all the supported images.

```
{
    "request": [
        {
            "md5": "8dfa1440953c3d93daafeae4a5daa326",
            "features": [
                "te",
                "av"
            ],
            "te": {
                "reports": [
                    "xml",
                    "pdf"
                ]
            }
        }
    ]
}
```

OPSEC SDK

The OPSEC SDK contains APIs for commands that were originally used with SecurePlatform. You can also use these commands on the Gaia operating system. The OPSEC APIs can open and monitor connections between the Security Management Server and gateways and other hosts and objects. The OPSEC SDK is very powerful and accesses the tables in the Security Management Server database.

For more about how to use the OPSEC SDK, go to sk63026 http://supportcontent.checkpoint.com/solutions?id=sk63026.

Sample Command with OPSEC SDK

You can use the `cp_conf sic state` command to show the SIC status for a gateway or host.

```
> cp_conf sic state
```

Output - `Trust State: Trust established`

Identity Awareness Web Services APIs

The Identity Awareness Web Services APIs lets you use REST protocol over HTTPS to add, remove, and show the status of these identity parameters:

- User name
- IP address
- Computer name
- SmartConsole user groups
- Identity Awareness Access Roles

For example, you can use the API to add a new user to an Access Role, or allow a user to connect to the internal network from a different IP address.

Check Point is planning to release the Identity Awareness APIs with R80.10.

Threat Prevention Intelligence API

You can use Custom Indicators to identify malicious activity related to the Check Point Threat Prevention Software Blades. Anti-Virus and Anti-Bot use this information to detect and prevent malicious activity based on your indicators.

An API for this feature is planned for a version after R80.10.