Check Point
SOFTWARE TECHNOLOGIES LTD

Keep Gateways Updated Offline with Private ThreatCloud

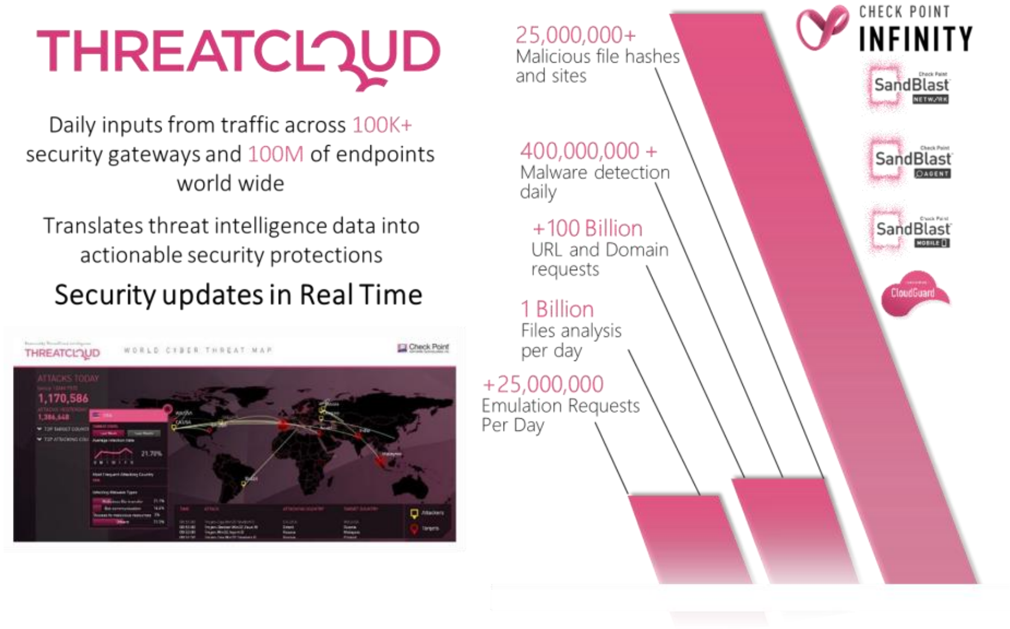
BUSINESS DRIVERS FOR KEEPING GATEWAYS CONSISTENTLY UPDATED

There are plenty of harmful malware attacks that take advantage of software vulnerabilities in common applications, such as operating systems and browsers. To counter these threats security solutions need to be updated in time so as to take advantage of the latest defense mechanisms.

Traditionally, threat prevention products such as Anti-Virus or IPS have relied on intelligence packages periodically pushed to the enforcement points. It has also been possible to schedule updates once a day and even deliver them manually. However, today security assets need to be updated constantly, including when they protect highly critical resources not connected to the Internet.

WHAT IS THE PUBLIC THREATCLOUD?

Threat prevention is driven by threat intelligence.

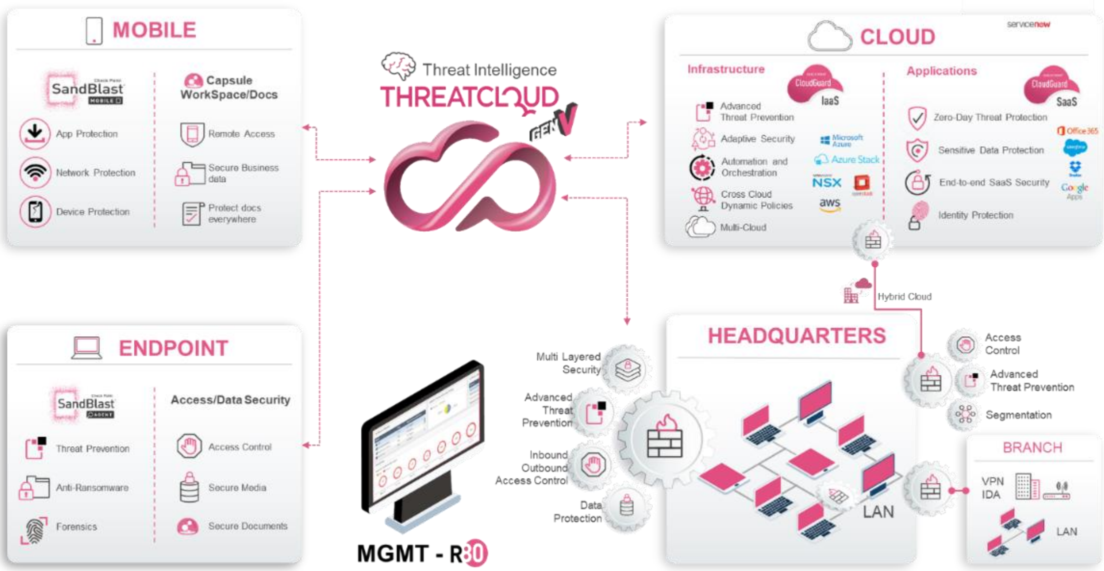


Check Point's ThreatCloud is a large data repository in the cloud that feeds security gateways, endpoint security agents, as well as mobile and cloud security platforms with up-to-the-second security intelligence:

- Collects information from over 100,000 GW’s and millions of endpoints worldwide.
- Handles requests regarding over 100 billion web pages and 1 billion files per day.
- Handles tens of millions of file emulation requests per day.
- Detects hundreds of millions of malicious events per day.
- Holds records of tens of millions of malicious files and websites, and updates over 1 million records per day from a wide variety of intelligence feeds coming from advanced in-house malware and threat research, AI algorithms and automated processes, partnerships and open sources.

ThreatCloud combines global coverage with the ability to create controlled intelligence data flows. This intelligence powers Check Point threat prevention, and is used to identify emerging outbreaks and threat trends. Since processing is done in the cloud, millions of signatures and malware samples can be investigated in real time.

ThreatCloud updates network, endpoints, cloud, and mobile



ThreatCloud's knowledgebase is dynamically updated using attack information from multiple sources:

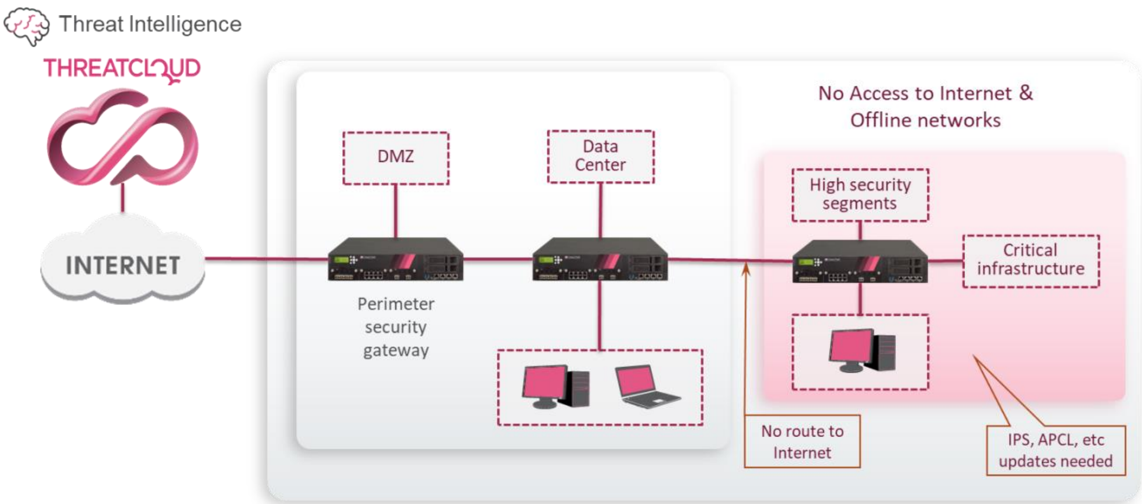
- Worldwide gateways and endpoints.
- Check Point's Threat Emulation cloud.
- Feeds from a network of global threat sensors.
- Check Point's research labs and the industry's best malware feeds.

External feeds are filtered using the FP (false positive) Checker to avoid the contamination of the production cloud intelligence. Corresponding security threat information is then shared among all enforcement points simultaneously.

WHAT ARE THE CHALLENGES TO ACCESSING CLOUD SERVICES OFFLINE?

ThreatCloud is able to efficiently distribute big data threat intelligence throughout global enterprises, to all enforcement points on networks, hosts, mobile devices and local clouds. However, due to individual enterprise network segmentation restrictions, the result is that some enforcement points become forbidden or technically unable to access the Internet, creating a challenge for any solution that leverages ThreatCloud data and it's services.

Such scenarios are ever present, especially among large enterprises and with customers in the financial and government sectors. Reasons cited include: security (e.g. IT/OT separation in ICS networks), operational (e.g. complex proxy configurations in zoned networks), regulatory, latency (over slow Internet pipes), guaranteed service, and more. Currently, the Check Point network Security Gateways that can operate in these environments are Firewall, VPN, and DLP (Data Loss Prevention). Although offline update solutions are available for some blades such as IPS, Application Control and Threat Emulation, these options are complicated and operationally expensive.



The presenting challenge is therefore how to allow customers to enjoy cloud services offline. The Private ThreatCloud (PTC) is intended to support a complete ecosystem of Check Point solutions, where all cloud access is internal to the customer's environment. The PTC update is unidirectional from the Public ThreatCloud; without anything being transmitted out of the customer environment on to the Internet. Furthermore the PTC supports integration with high assurance 3rd party uni-directional gateways (data diode).

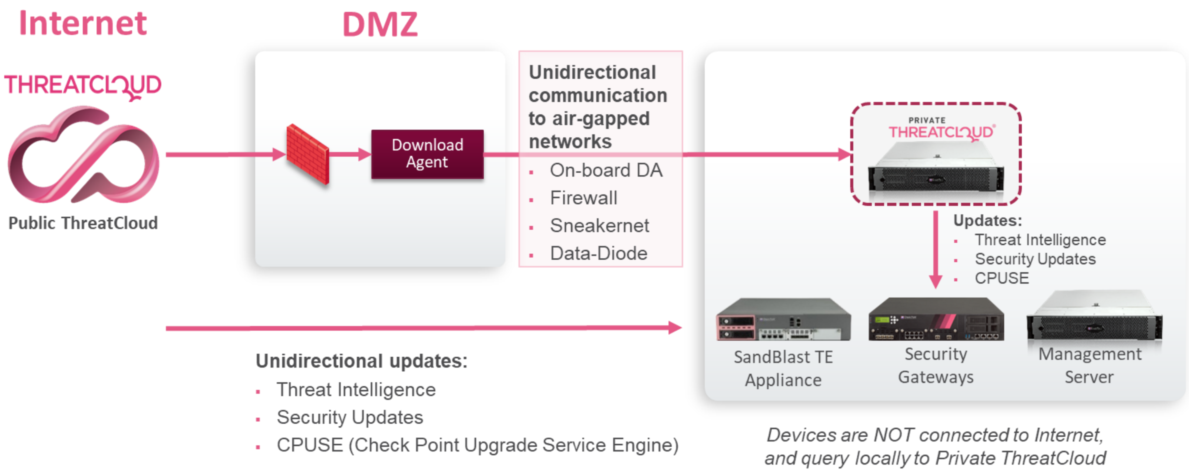
What is the Private ThreatCloud?

The Private ThreatCloud provides a solution for customers who's Security Gateways or other Check Point devices do not connect directly to the Internet. With the Private ThreatCloud, users receive continuous protection as cloud services are extended offline and into other compartmentalized environments.

The Private ThreatCloud is updated by the Check Point Public ThreatCloud. Check Point devices can therefore use the Private ThreatCloud to get updates instead of connecting directly to the Internet through their gateways.

Furthermore, the Private ThreatCloud Download Agent mediates between the Internet and the Private ThreatCloud. For example, the Private ThreatCloud Download Agent first downloads updates from the Public ThreatCloud and then pushes them to the Private ThreatCloud.

The Private ThreatCloud Download Agent can be installed on the same appliance as the Private ThreatCloud, on a separate appliance, or on a Virtual Machine (VM). Communication between the Download Agent and the Private ThreatCloud is completely unidirectional, supporting multiple connectivity mechanisms between the Download Agent and the Private ThreatCloud to suit the needs of different customer categories.



What does a ThreatCloud Appliance offer?

There are currently four main services offered by the ThreatCloud Appliance:

1. Private ThreatCloud – Responds to real-time reputation queries from Check Point Antivirus (AV), Anti-Bot and URL Filtering.
2. Package updates – Serves update package requests for IPS, Application Control, Anti-Bot, and local Sandblast appliances.
3. Upgrades using Gaia OS **CPUSE (sk92449)** – Serves Check Point gateway software update queries.
4. Private Sandblast threat indicators – File hashes detected by local Sandblast appliances are added as custom indicators for serving AV blades.

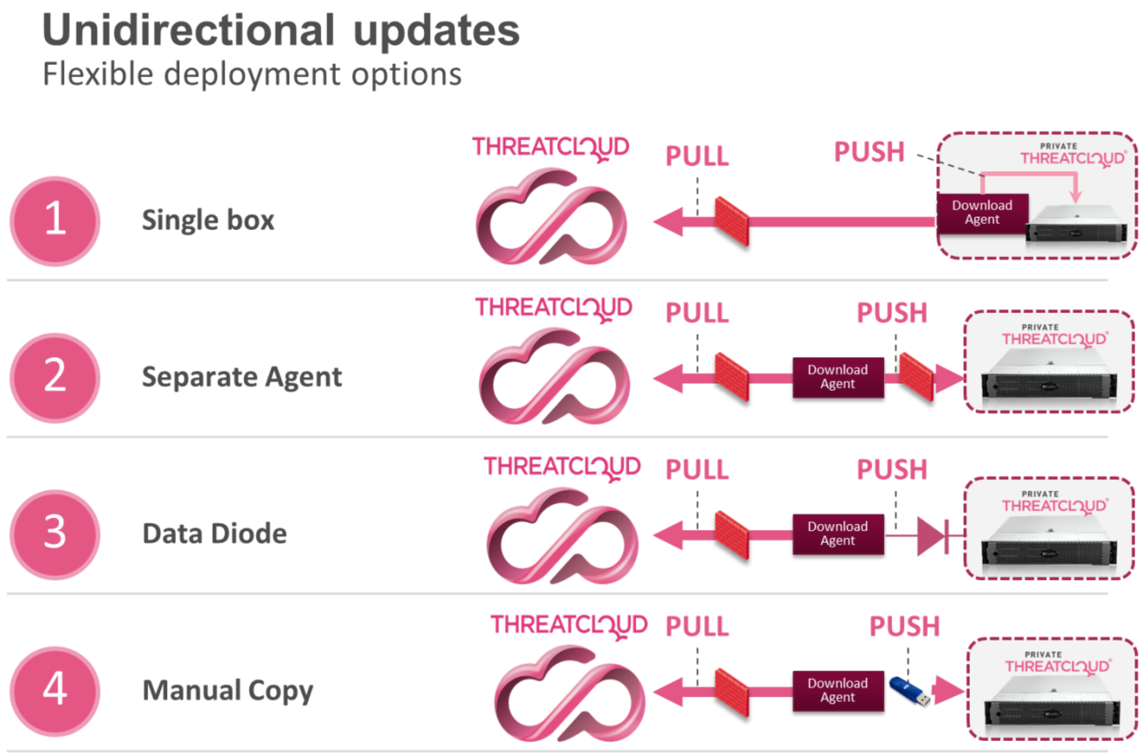
How does a ThreatCloud Appliance function?

The Private ThreatCloud running on Gaia OS is updated from the Check Point Public ThreatCloud. It is an on-premises hardware platform, which runs ThreatCloud technologies and contains up-to-date data residing on the Public ThreatCloud. Security Gateways and other Check Point Devices can easily use the Private ThreatCloud locally, instead of using the Public ThreatCloud directly.

In addition to the aforementioned components, the Private ThreatCloud is bundled with the Download Agent software component.

Enterprises can choose from the following deployment options:

- Single Box – The Private ThreatCloud and Download Agent are installed on the same appliance.
- Unidirectional – The Download Agent is installed on a different appliance / Virtual Machine than the Private ThreatCloud. Administrators can then:
  - Use a Check Point Security Gateway to enforce one-way updates.
  - Position a 3rd party certified data diode between these two components.
  - Manually transfer the data from the Download Agent to the Private ThreatCloud using offline media.



What is the Private ThreatCloud Environment?

It is important to understand the different hosts that can be connected to as part of the installation:

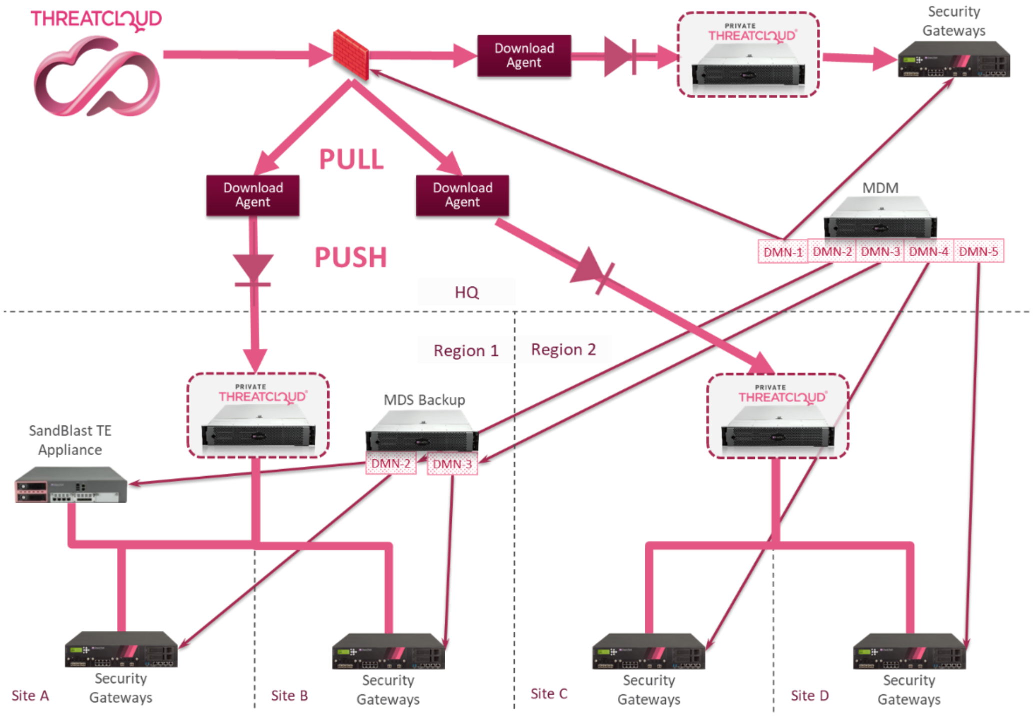
- The Private ThreatCloud: Replies to queries from Security Gateways or other Check Point devices for updates.
- The Download Agent: Downloads updates from the Public ThreatCloud and pushes them to the Private ThreatCloud. In a single box deployment, the Download Agent is on the same appliance as the Private ThreatCloud. In a unidirectional deployment, the Download Agent is on a separate appliance or VM.
- Security Gateways or other Check Point devices: Receives updates from the Private ThreatCloud. They must be configured as a client to the Private ThreatCloud[1].

Please note that the Download Agent must have HTTP or SSL access to some Check Point domains. Application Control rules can be used to allow outgoing connections only to these domains.

[1] Security Gateways and other Check Point devices must be R75.40 or higher to get updates from the Private ThreatCloud.

DEPLOYMENT EXAMPLES

Enterprise with Regional Centers



The above is an example of a large organization using Multi-Domain Management (MDM).

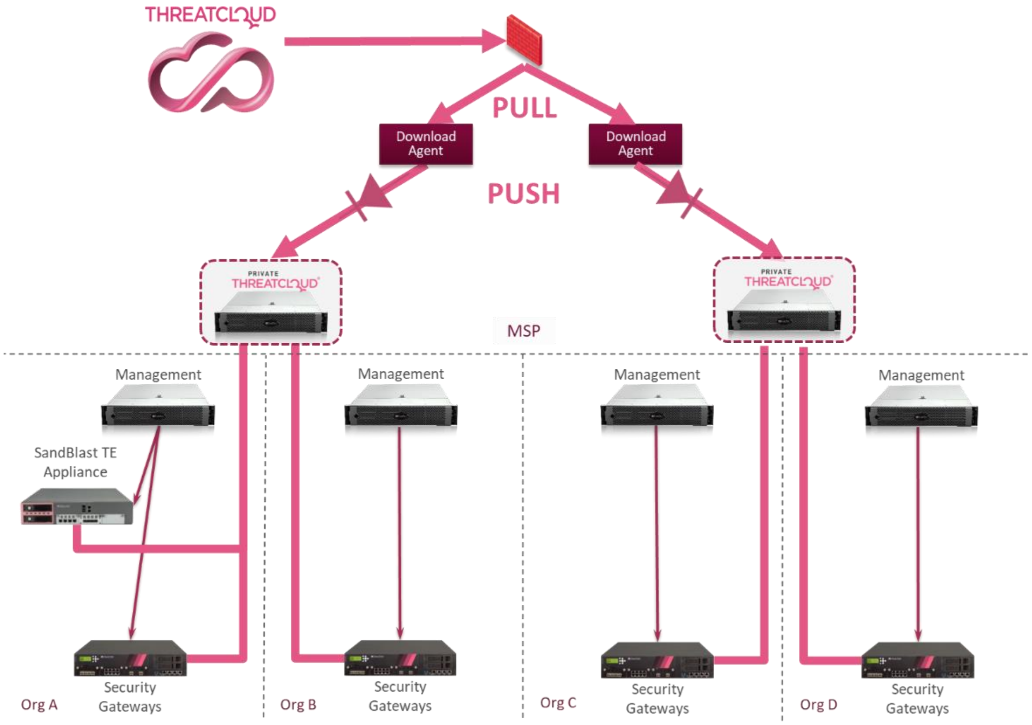
There are many Security Gateways distributed geographically (HQ and many remote sites grouped to Regions).

Some of the Regions have MDS Backups (Management Domains DMN-2 and DMN-3 are active at the Region 1).

Each Region has its own Private ThreatCloud appliance (PTC) to serve gateways close to it.

Important: It is not possible to configure only one Domain to work with the Private ThreatCloud R80.20, i.e. it is only possible to configure all Domains or none.

MSP / Vertical Solution



This graphic illustrates an enterprise (MSP) providing updates to multiple organizations.

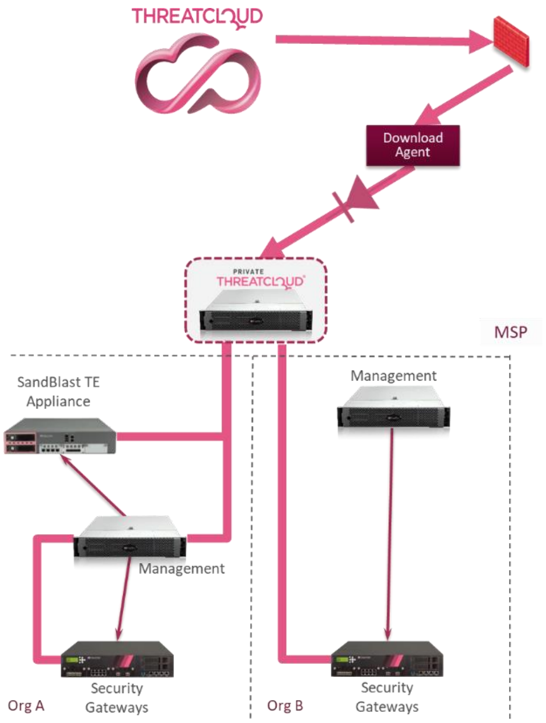
It might add its own value and intelligence feeds, and it is also possible for them to add indicators of compromise (IoCs) manually or by using scripts.

For example, the Central Bank distributes updates to many banks, adding financial IoCs specific for their governing country.

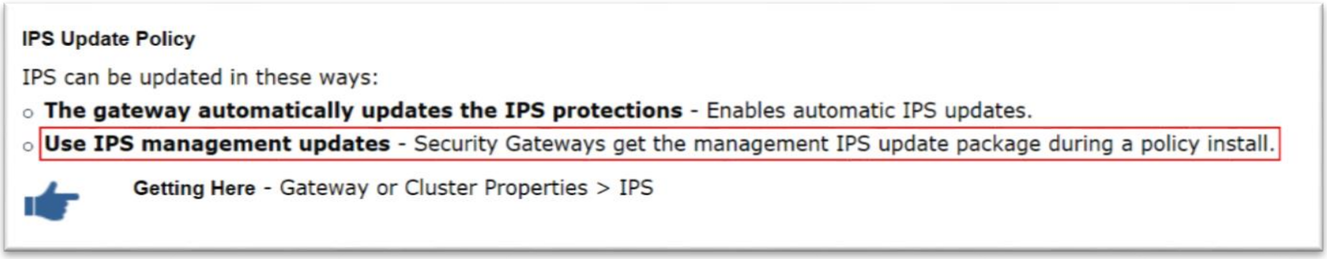
Simplified Configuration

Sometimes only Internet gateways require a full scope of updates while most internal gateways require only IPS updates.

For such cases, it is possible to download updates directly from the Management Server/ Multi Domain Management server. It is necessary to configure such Management Server as a client to the Private ThreatCloud.



In the configuration above, the Sandblast TE Appliances keep receiving updates directly from the MSP Private ThreatCloud appliance, while internal Security Gateway downloads IPS updates from the Organizational Management Server, which acts as a client.



IPS Update Policy

IPS can be updated in these ways:

- ○ **The gateway automatically updates the IPS protections** - Enables automatic IPS updates.
- ○ **Use IPS management updates** - Security Gateways get the management IPS update package during a policy install.

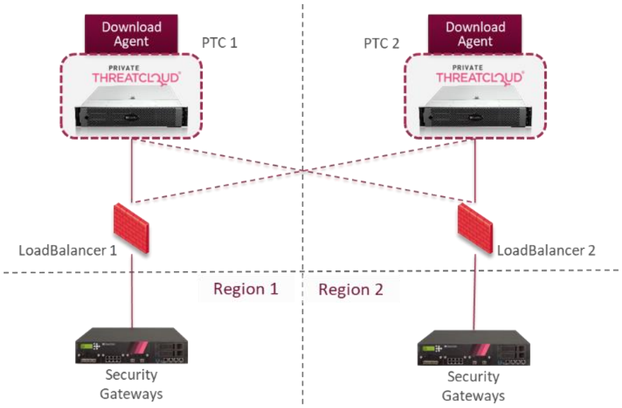
Getting Here - Gateway or Cluster Properties > IPS

Availability and Scalability

Transactions in the cloud are inherently stateless. All ThreatCloud Appliances in a private cloud maintain the same data so that each request can be serviced by a different ThreatCloud Appliance[2] (the exception is the Sandblast Cloud service, which requires stickiness between cloud consumer and the ThreatCloud Appliance). This characteristic allows the use of multiple load balancing and high availability options. Typically, larger enterprises will install ThreatCloud appliances at regional data centers and configure their gateways to access the closest cloud appliance by default, with remote cloud appliances picking up the load in case of failure.

A Load Balancer can also be used to distribute connections from Security Gateways to the Private ThreatCloud Appliance.

[2] Any discrepancies in PTCs' configurations (for example caused by manual IoCs addition or by other means) should be avoided.



It can be either a 3rd party load balancer or a Check Point ConnectControl feature, which is included in all Check Point gateways (either via the appliance or running on a virtual machine).

See CONNECTCONTROL - SERVER LOAD BALANCING and SK31162: SUPPORTED CONFIGURATIONS FOR CONNECTCONTROL - SERVER LOAD BALANCING or relevant 3rd party load balancer documentation

Models

Supported models: Smart-1 5050 | 5150

Licensing options from 50 up to 2000 gateways

TECHNICAL DETAILS

How to manage the Private ThreatCloud

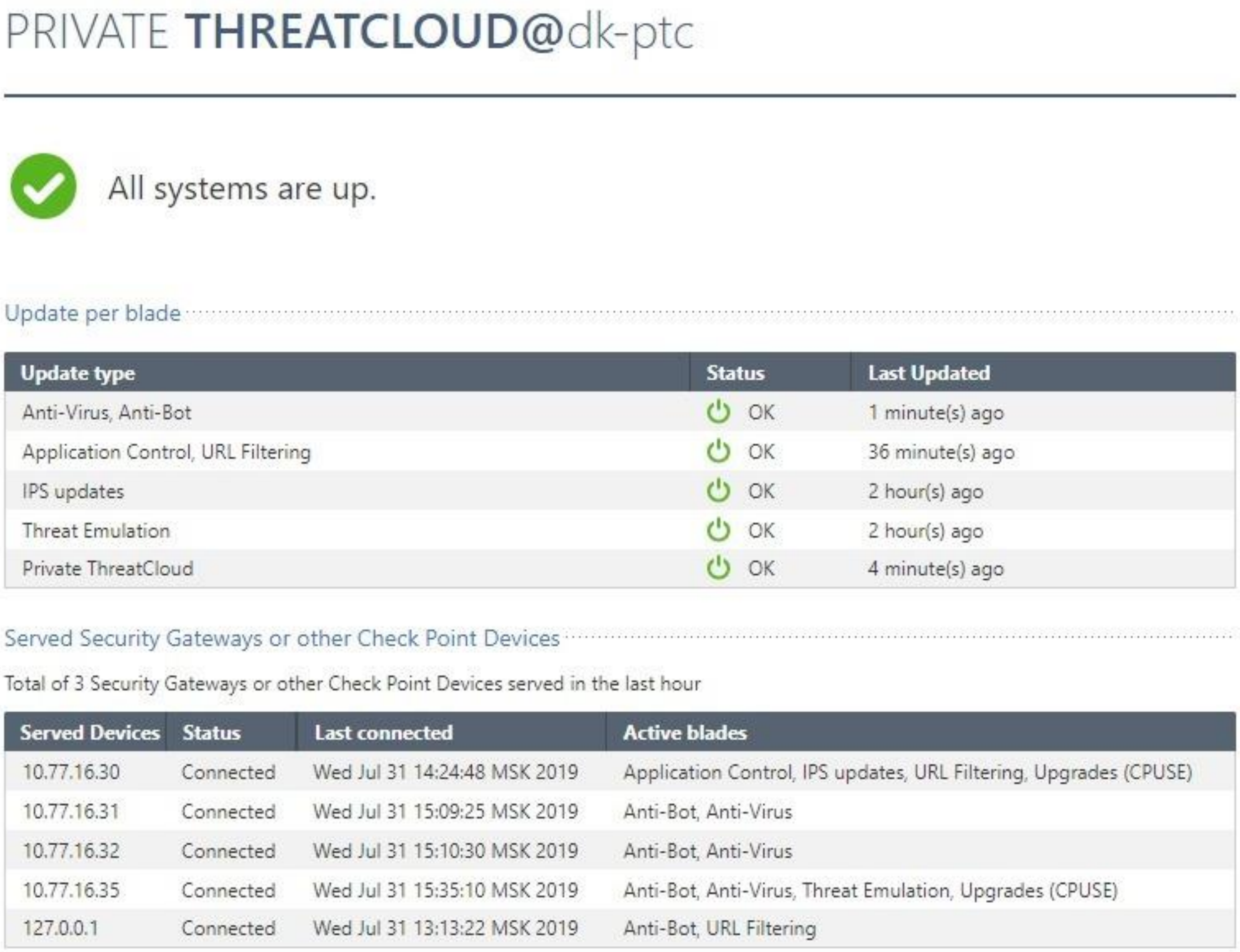
Starting from R80.20, the Private ThreatCloud is installed on a dedicated Management Server, which manages **only the Private ThreatCloud** (the Gateways that connect to the Private ThreatCloud as clients must be managed by a different Management Server).

The Download Agent can be installed on a Gateway or Management Server, however it is highly recommended to install it on a Gateway.

It is possible to monitor both Private ThreatCloud Download Agent (download process, etc.) as well as Private ThreatCloud's state.

Both GUI and CLI are available, which provides for easy and effective management leveraged with automation when needed.

PTC monitoring overview example: GUI



PRIVATE **THREATCLOUD@**dk-ptc

All systems are up.

Update per blade

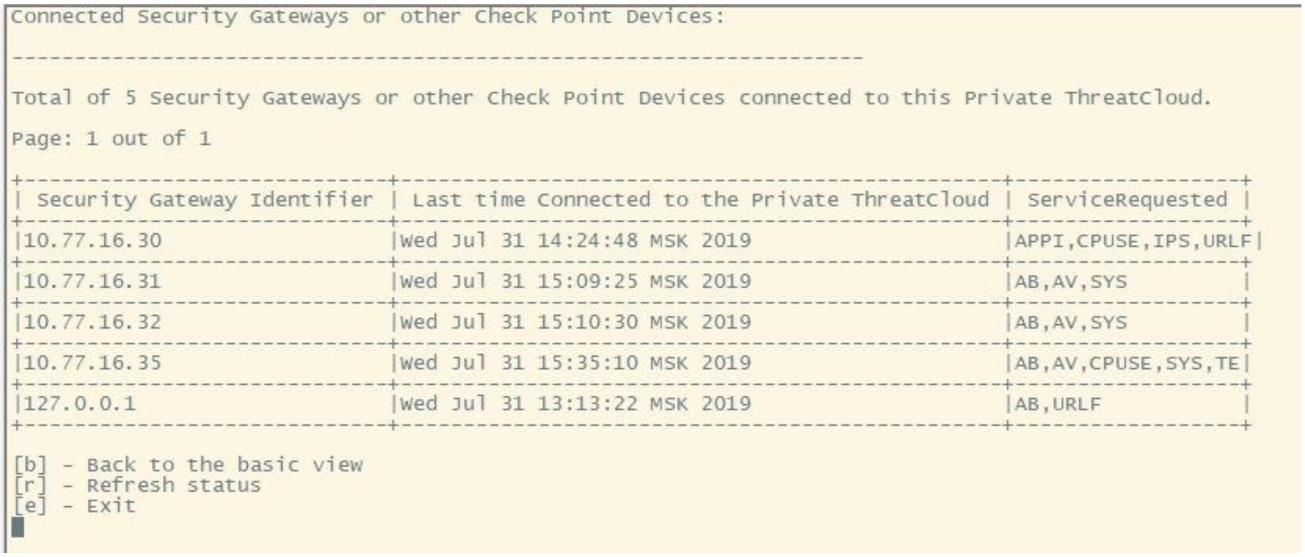
Update type	Status	Last Updated
Anti-Virus, Anti-Bot	⏻ OK	1 minute(s) ago
Application Control, URL Filtering	⏻ OK	36 minute(s) ago
IPS updates	⏻ OK	2 hour(s) ago
Threat Emulation	⏻ OK	2 hour(s) ago
Private ThreatCloud	⏻ OK	4 minute(s) ago

Served Security Gateways or other Check Point Devices

Total of 3 Security Gateways or other Check Point Devices served in the last hour

Served Devices	Status	Last connected	Active blades
10.77.16.30	Connected	Wed Jul 31 14:24:48 MSK 2019	Application Control, IPS updates, URL Filtering, Upgrades (CPUSE)
10.77.16.31	Connected	Wed Jul 31 15:09:25 MSK 2019	Anti-Bot, Anti-Virus
10.77.16.32	Connected	Wed Jul 31 15:10:30 MSK 2019	Anti-Bot, Anti-Virus
10.77.16.35	Connected	Wed Jul 31 15:35:10 MSK 2019	Anti-Bot, Anti-Virus, Threat Emulation, Upgrades (CPUSE)
127.0.0.1	Connected	Wed Jul 31 13:13:22 MSK 2019	Anti-Bot, URL Filtering

PTC monitoring overview example: CLI



```
Connected Security Gateways or other Check Point Devices:

------------------------------------------------------------------

Total of 5 Security Gateways or other Check Point Devices connected to this Private ThreatCloud.

Page: 1 out of 1

+------------------------------+------------------------------------------------+------------------+
| Security Gateway Identifier  | Last time Connected to the Private ThreatCloud | ServiceRequested |
+------------------------------+------------------------------------------------+------------------+
|10.77.16.30                   |Wed Jul 31 14:24:48 MSK 2019                    |APPI,CPUSE,IPS,URLF|
+------------------------------+------------------------------------------------+------------------+
|10.77.16.31                   |Wed Jul 31 15:09:25 MSK 2019                    |AB,AV,SYS         |
+------------------------------+------------------------------------------------+------------------+
|10.77.16.32                   |Wed Jul 31 15:10:30 MSK 2019                    |AB,AV,SYS         |
+------------------------------+------------------------------------------------+------------------+
|10.77.16.35                   |Wed Jul 31 15:35:10 MSK 2019                    |AB,AV,CPUSE,SYS,TE|
+------------------------------+------------------------------------------------+------------------+
|127.0.0.1                     |Wed Jul 31 13:13:22 MSK 2019                    |AB,URLF           |
+------------------------------+------------------------------------------------+------------------+

[b] - Back to the basic view
[r] - Refresh status
[e] - Exit
```

How to Configure Check Point Devices to Use the Private ThreatCloud

Trust must be established between the Security Management / Domain Management Server and the Security Gateways that connect to the Private ThreatCloud. To download updates directly from the Management Server / Multi Domain Management server, it must be configured as a client to the Private ThreatCloud.

Gateways do not require installation of any extra packages. Only Management Server / Multi-Domain Management require a special RPM. A gateway's redirection to the Private ThreatCloud is configured from the Management Server. If a proxy server has been previously used for updates, the administrator will need to remove the proxy configurations on all objects or they can configure the DNS to resolve some domains to the Private ThreatCloud IP address.

Indicators of Compromise

It is possible to import custom indicators to the PTC to share them with all connected gateways and they will be enforced without any further actions (no policy installation is required).

Custom indicators can be added/deleted in the following ways:

- Over REST from the Private ThreatCloud appliance
- Via STIX/TAXII packages from the Download Agent

Adding a custom indicator via POST

Send a POST message to the URL: `http://<ptc ip>/ptcd/customIndicators/add`

Adding a custom indicator via CLI

There is a script available on the Private ThreatCloud appliance:

```
add_indicator <indicator> <protection_name> [<confidence>] [<severity>]
```

Private ThreatCloud (PTC) supports custom indicators of the following types: *hash/domain/url/ip.*

STIX/TAXII

PTC supports indicators from STIX/TAXII servers[3]. Once the TAXII configuration is complete, the TAXII server will be polled periodically for new STIX packages

How to Schedule Large Downloads and Software Updates

CPUSE and Threat Emulation require very large updates. The Private ThreatCloud can be configured to a time at which downloads for these updates will start. A daily or weekly update can be set up, or the downloads can be set at intervals (i.e. every two days).

Using the download schedule, the Private ThreatCloud Download Agent requests new updates from the Public ThreatCloud at the most optimal time. Once an update is found, the Private ThreatCloud Download Agent will download until all the pakages reach the ThreatCloud.

[3] Was tested with the TAXII stand implementation of TAXII server.

These downloads may take several hours, depending on the available ISP bandwidth.

ADDITIONAL MATERIALS

For the latest details regarding Private ThreatCloud see:

sk149692 R80.20 Private ThreatCloud

sk125693 Private ThreatCloud Custom Indicators and STIX/TAXII support

Simplified Updates

In some cases it is possible to have offline updates without Private ThreatCloud. See:

sk93724 IPS and Application Control blade (Account Services authorization is required).

sk92509 Offline updates for Threat Emulation images and engine.