indeni

Keeping Check Point VSX Firewalls Healthy

White Paper

Visibility is Key

Normally, Check Point VSX firewalls are deployed in the core of the network. Basically, where all the cool stuff happens. The reason being VSX's flexibility and ability to segment traffic into separate virtual devices. However, as the VSX devices are so critical, visibility into their health is critical.

With normal Check Point firewalls, you want to track hardware health, performance, software configurations, clustering, CoreXL and SecureXL behavior, and much more. With VSX firewalls, you want to do ALL that, but on a per Virtual System basis. Since each Virtual System has its own firewall configurations, you want to collect data for each of them.

Keeping track of all of these different items is crucial. For example:

- CoreXL defines how the traffic load will be balanced across CPU cores in the device. When operating in a VSX setup, each VS needs to have enough cores to do its job. If it doesn't, it will begin dropping potentially critical traffic. To avoid such a situation, the core allocation and CPU usage per VS must be watched constantly.
- SecureXL is a means of accelerating traffic through the firewall. Each VS has its own setting and sometimes one or two VSs may have it disabled by user error. It's important to identify such a situation and turn SecureXL back on.

All of the above examples ares ones Indeni is uniquely positioned to help with.

An administrator responsible for Check Point VSX is required to handle more data and complexity than with a regular Check Point firewall. To do that job well, the administrator needs complete visibility and a lot of data at their fingertips.

Making Visibility Possible

Great, so I can just leverage SNMP-based monitoring for this, right?

Historically, this has been difficult. In recent versions, Check Point has done considerable work to make it easier to do through SNMP. With R80.20 you can leverage a monitoring system like SolarWinds NPM to gain insight to some of the basic metrics you care about. However, this is still fairly limited, as most items you want to look for are outside the scope of SNMP-based monitoring with VSX. Examples include:

- Deep resource usage per VS beyond just CPU and memory.
- Verification of best practices published by Check Point.
- Security posture analysis (such as the lockdown of insecure protocols).
- Gold configuration verification (NTP, AAA, syslog and other device-level configurations).
- Kernel debug accidently left on.
- Cluster-level configuration mismatch.

The result is that many Check Point customers find themselves unable to leverage their current monitoring system to gain true visibility into VSX firewalls.

So SSH?

SSH is still the way to go with collecting data from Check Point firewalls and even more so with VSX. Whether you are looking for basic CPU or memory utilization per VS, or more elaborate status and configuration information, SSH is the most reliable method to get the information.

NOTE: Check Point is making more and more APIs available in recent versions. As these evolve, they may replace the SSH collection method.

To get access to this data and analyze it, you would need to build your own set of scripts for executing SSH commands at regular intervals and parsing their output. Here's an idea how. The SSH output may change from version to version of Check Point's firewall, so you'll need to update the scripts along the way. Also, in reality, you need to poll several hundred different metrics and configurations to get the visibility needed to operate a VSX firewall cluster successfully. This can become draining, time intensive and hard to keep up with. What's more, you want to be able to easily direct operations teams to the solution when a problem is identified.

Luckily, Indeni has chosen to take on this challenge.

How Does Indeni Help?

Indeni has a community of Check Point experts who look for every possible metric or configuration that needs to be collected and analyzed. They utilize Indeni's platform's capabilities to actually implement the collection and analysis, providing users with a powerful solution for ensuring Check Point firewalls operate as intended.

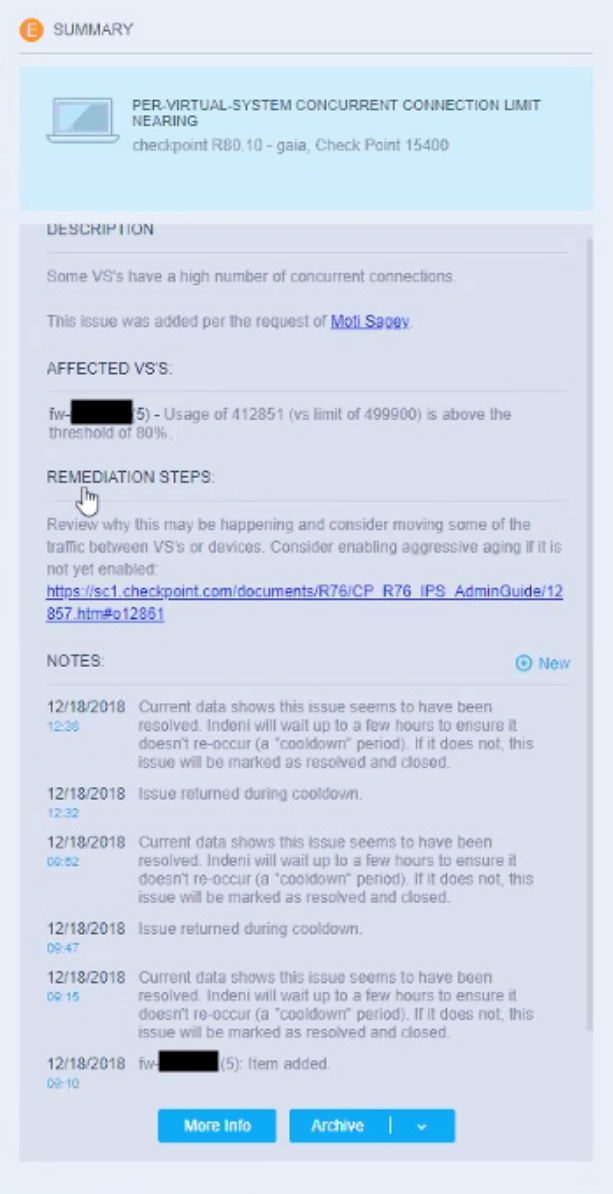
Customers with large Check Point VSX deployments often purchase Indeni. These customers have shared the main capabilities of Indeni they found useful with Check Point VSX and these are included below.

It is important to note that Indeni is capable of collecting VSX-level data on both standard Gaia-based deployments as well as Scalable Platforms (61000, etc.).

On-going tracking of CPU, memory, number of connections and interface stats, each of them per VS:

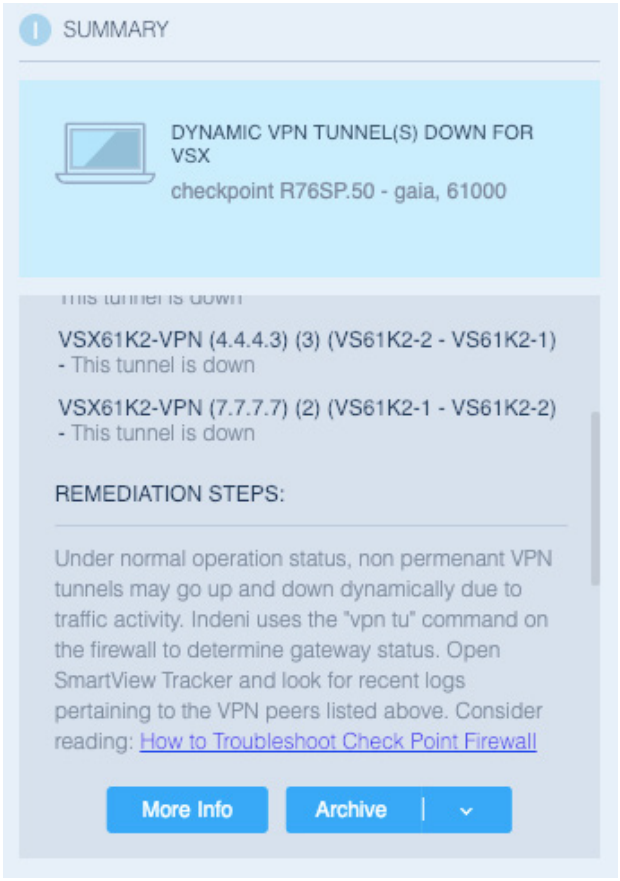
See how this works in the Indeni Knowledge Explorer.

Indeni identifies issues on a per VS level and provides detailed information in the issue notification. This includes the specific metric that is problematic, the affected VS and the history of the situation.



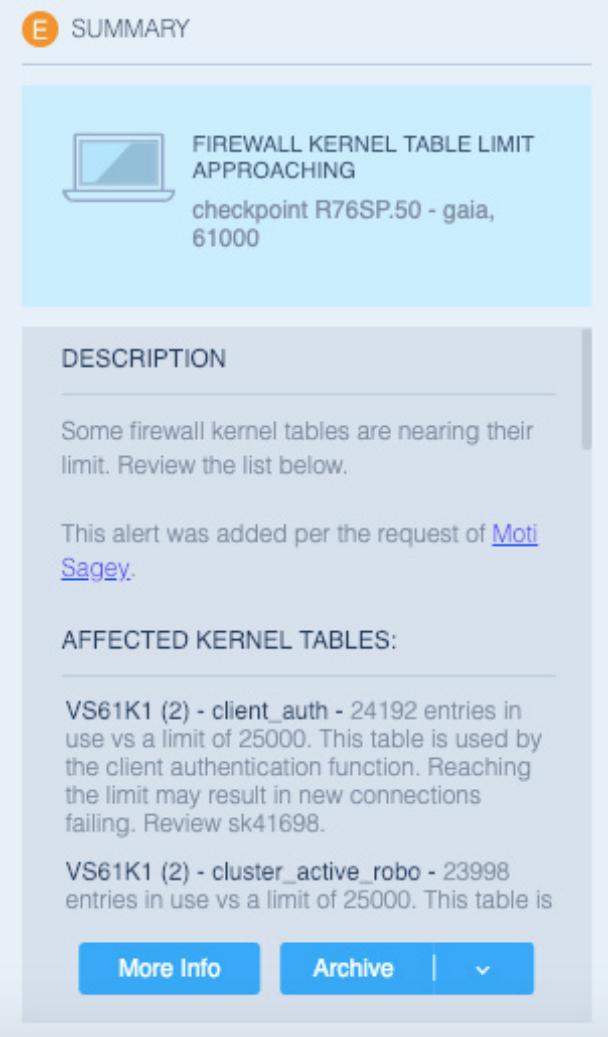
Indeni tracks VPN tunnels on a per VS basis. If a permanent VPN tunnel goes down, you will know. If a non-permanent VPN tunnel is failing to come up, you will know.

VPN tunnel health, per VS:



Indeni tracks many kernel-level parameters, such as the known kernel tables. Each such parameter is tracked per VS and Indeni will let you know if a specific VS is reaching a risky situation.

Kernel table tracking, per VS:



See how this works.

If you are looking for more examples, Indeni has made its knowledge repository public through its Knowledge Explorer, a list of what is available for Check Point is here.

About Indeni

Indeni is the crowd-sourced automation platform for security infrastructure. With the Indeni Automation Platform organizations gain access to living repository of scripts that automate tasks for maintenance, high availability, network visibility, security, compliance, validating vendor best practices and much more. Learn more at www.indeni.com.

Corporate Headquarters
San Francisco, CA USA
Tel: +1-877-778-8991
Email: info@indeni.com

European Headquarters
Tel Aviv, Israel
Tel: +1-809-494-190
Email: info@indeni.com