CHECK POINT + INDENI
PREEMPTIVE MAINTENANCE
OF CRITICAL SERVICES

BENEFITS

When deploying top of class network security equipment, organizations need to make sure configurations are done correctly and consistently. By using indeni with Check Point firewalls, network security operations teams can be alerted to misconfigurations before they result in service downtime.

- Become a proactive organization
- Conduct regular preemptive maintenance
- Backup configurations
- Track device inventory and configuration changes

CHALLENGE

When deploying best-in-class network and network security products, it is important to consider how to protect the investment: how to ensure best practices are followed, configurations are in check and the products' performance is tracked as needs change. Today's solutions, mostly simple SNMP monitoring, are incapable of delivering true, in depth visibility.

Network and network security operations teams find themselves scrambling whenever downtime occurs. The day to day behavior is reactive and root cause analysis is done after the fact. To be able to deliver on the business goals, operations teams need to become proactive.

SOLUTION

indeni is the only solution in the market that has an onboard, ever expanding, crowd sourced knowledge base that is used to compare network device configurations to best practices. indeni's knowledge is built through its users, their networks, its vendor partners and public sources.

The integration of indeni with Check Point management servers and gateways allows network security operations teams to constantly validate their environments' configuration against an ever growing set of best practices. Some best practices come from Check Point's own knowledge base while others are from the practices learned in the field by other users and the service providers they work with. In addition, indeni conducts automated root cause analyses whenever an issue actually occurs.
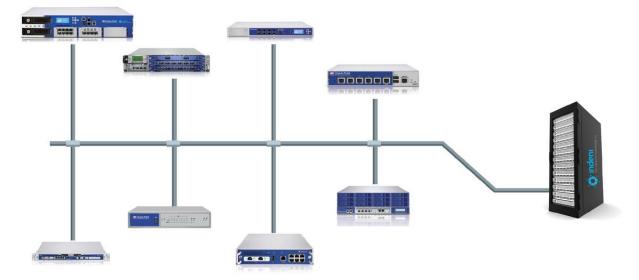
indeni logs into Check Point devices using SSH and collects data 24/7 by running commands administrators commonly run manually; commands such as "ifconfig -a", "cpstat fw", "fw ctl get int <kernel_param>" and more. indeni also collects and analyzes files such as objects_5_0.C, fwkern.conf and others. When indeni finds a configuration issue, an alert is issued describing the issue and the best course of action. In many cases, indeni refers to the relevant SecureKnowledge article in Check Point's support center.

Configuration data pulled in by indeni is also stored for backup purposes, inventory reporting and configuration change tracking. This ensures that the network operations team can track its growing inventory on an ongoing basis as well as review configuration changes and restore backups when needed.

```
# ifconfig –a
# cpstat fw
# fw ctl get int <kernel_param>
```

… and more. indeni also collects and analyzes files such as objects_5_0.C, fwkern.conf and others.

indeni Maintains and Tunes Your Check Point Infrastructure

indeni's ability to collect vast amounts of knowledge and instrumentalize it is unique in the market. indeni is a leader in the number of automated checks for network equipment that its software is capable of executing. The number of checks grows on a regular basis, further securing indeni's position in the field of automated root cause analysis.

indeni is also unique in how easy it is to deploy and maintain. Deployed within less than 60 minutes on a virtual machine and very little tuning required means there is no need to watch another tool. Once running, indeni sends alerts in email messages or SNMP traps. The logic is tuned constantly by indeni's R&D to ensure alerts are only produced when immediate action is necessary. Alerts are not sent more than once, avoiding alert fatigue.

IN SUMMARY

Check Point plays a leading role in securing corporate networks and the Internet. An important part of this role is monitoring networks to see the breadth and depth of threats targeting our current and future customers using a comprehensive suite of threat prevention technologies that adapt as threats evolve. The Check Point integrated next generation solution prevents advanced threats and malware. This includes stopping application-specific attacks, botnets, targeted APT attacks and zero-day threats.

With Check Point providing the security protection and indeni providing maintenance of this top of class network security solution, customers can rest assured that they are protected and secure from the latest threats.

About Check Point

Check Point Software Technologies Ltd., the worldwideleader in securing the Internet, provides customers with uncompromised protection against all types of threats. Check Point first pioneered the industry with FireWall-1 and its patented stateful inspection technology. Today, Check Point continues to develop new innovations based on the Software Blade Architecture. The Software Blade Architecture provides flexible simple, and easy to deploy security modules that enable customers to select the security they need to build a custom Check Point security gateway solution. For more information, visit www.checkpoint.com.

About indeni

Thus far, keeping track of network devices was limited solely to acquiring data through common protocols (SNMP, SSH, telnet, etc.) and analyzing the data using basic mechanisms (graphing, regular expression checking, etc.). Think about this - how useful is a pretty graph displayed in a NOC? indeni is riding the technological trends that enabled companies like New Relic, Box and others to succeed. Collection of enormous amounts of data from customer networks and public sources, analyzing it using cutting edge science, generating complex knowledge and producing actionable bottom lines for our customers. More information is available at. For more information, visit www.indeni.com.