

Galaxy Team Implements Next Generation Threat Extraction Appliance Solution for a leading Indian FMCG Company

Our Customer is a leading manufacturer of oleo chemicals for use in various industries. It manufactures edible oils, Vanaspati and bakery fats. It has its headquarters in India and exports its products to several countries.

The customer's IT team was using a single Fortigate firewall on perimeter of their network as the gateway to Internet. With an increase in network traffic due to stellar business growth over the years, they needed a more secure, scalable and reliable solution in a fault-tolerant architecture, with all the firewall rules optimized and benchmarked to best industry practices.

THE SOLUTION: -

After a rigorous evaluation and assessment activity with help from Galaxy, customer decided to replace legacy firewall with Check Point NGTX gateways in cluster. This provides best-in-class security, and also protects their internal servers and user systems from external attacks. Galaxy recommended a Security Management pre-defined system managing 2 gateways and 5 blades Solution. We also suggested a 12600 Next Generation Threat Extraction Appliance Solution.

Galaxy Business Solutions team worked on: -

- Understanding and gathering complete information of current network architecture and policy configuration
- New appliances configuration, policy and routing migration based on current setup
- Policy review and verification
- Scheduling connection of these new appliances to the production network and rigorous testing of all traffic
- Creating IPsec VPN and testing the connectivity
- Enabling of new security blades and policy configuration based on requirements
- Monitoring the above setup

THE BENEFITS: -

12600 Security Appliance Provides Comprehensive Security

Customer relies on the Check Point 12600 Appliance with Firewall, Intrusion Prevention (IPS), IPsec VPN, Application Control, Antivirus, Anti-Bot, URL Filtering, Email Security, advanced next-gen zero-day threat prevention, Threat Emulation and Threat Extraction Software Blades to provide robust network protection and accessibility to network resources. With features including hot-swappable redundant power supplies and hard drives as well as high-availability technologies such as Check Point ClusterXL and Load-Sharing, the 12600 appliances provide the customer with a high level of business continuity and serviceability. Moreover, with a number of Software Blades at its disposal, the customer can easily add new layers of protection and functionality as and when needed to change and evolve.

Integrated IPS Software Blade Provides Unrivaled Network Protection

The Check Point IPS Software Blade provides Sinopec with comprehensive, integrated protection against malicious and unwanted network traffic. Incorporated with various advanced technologies and up to 6 GBPS of IPS throughput, the IPS Software Blade delivers dynamic threat protection to secure the customer network from potential threats.

Advanced Management Solution Enhances Visibility and Control

With the Check Point Smart-1 205 security management appliance, the customer is able to administer network policy management, track and analyze events, run reports and more, from a single user interface. Moreover, with Management Software Blades such as Smart Event and Smart Reporter, it can centrally monitor all its Check Point devices to get a complete visual picture of changes to gateways, remote users, and security activities. This enables administrators to immediately identify changes in network traffic flow patterns and stop malicious activity

CONCLUSION

Galaxy team conducted an assessment of customer's network architecture and policy configuration setup, and drew up a thorough project plan to configure new appliances, policies and routing migration. We meticulously completed the migration & testing activity over the assigned weekend to ensure a minimal downtime. Likewise, we also provided monitoring and support services, resulting in enhanced network security and customer satisfaction.