HOW A FORTUNE 20 ENERGY & PETROLEUM COMPANY PROTECTS ITS NEXT-GEN EXTRANET WITH A SOFTWARE-DEFINED SECURITY FABRIC

Customer Success Story

big switch networks

With over $110 billion in revenues (2016), the Fortune 20 Energy & Petroleum Company is not only one of the world's largest integrated energy companies, it's also one of the most innovative when it comes to network design. The Company's extranet, which connects more than 20 locations worldwide, uses Big Switch Networks' Big Monitoring Fabric™ (Big Mon) Inline to deliver highly advanced, compliant cybersecurity and performance monitoring capabilities while reducing expenditures on third-party appliances by 50 percent.

Integrated energy company gains agility while reducing cybersecurity risk and monitoring costs

The energy giant's use of a software-defined security fabric is the brainchild of the Company's Team Lead for Field Telecom Services, Western U.S. At the outset of the network renovation project, he recalls, "*our extranet design had been in place for many years. With new cloud providers coming on board, and a global initiative to better protect our resources with more cybersecurity appliances, we realized that the extranet design was not capable of handling our emerging requirements.*"

> *"It was crucial to be able to add new tools on the fly without having to recable all of our network.With the old extranet, when we wanted to remove or add a tool we had to schedule an outage, work within a change window and cable everything around the device.*
>
> **- TEAM LEAD**
> **Field Telecom Services, Western U.S.**

CHALLENGE

- Meet today's business needs: Design a new extranet that could provide better performance, security and monitoring insights
- Gain agility: Be able to drop/add appliances, reroute traffic and direct specific streams without cumbersome cabling
- Reduce costs: Find a better way to connect monitoring and security tools to the network, to eliminate the need for multiple pairs

SOLUTION

- Big Monitoring Fabric Inline
- Symantec (Blue Coat) SSL Visibility Appliance
- Sourcefire IPS
- FireEye Threat Protection Platform (FireEye NX Series)

RESULTS

- Better business agility through faster adaption to change
- Reduced cybersecurity risk through the ability to add new tools quickly
- Enhanced monitoring through granular traffic direction
- Easier management through graphical user interface
- Reduced appliance costs by 50%
- Achieved scale-out DMZ security at 20+ global data centers

The Old Way: Physically Cabled Devices

The Team Lead led the review to better understand how the extranet could integrate new cybersecurity technologies and provide more monitoring capabilities, with a flexible design to allow components to be easily added and removed. "It was crucial to be able to add new tools on the fly without having to recable all of our network," he says. "With the old extranet, when we wanted to remove or add a tool we had to schedule an outage, work within a change window and cable everything around the device."

In addition, the previous network design necessitated multiple pairs of each new monitoring or cyber security appliance. "We had multiple paths in and out for redundancy, so it was a very expensive set-up."

The Next-Generation: Software-Defined Security Fabric

Finding an alternative network design proved to be a challenge. The Team Lead explains, "Traditionally, big enterprises get off the shelf products and try to integrate them as best as they can. In a network our size that strategy doesn't work because we have a lot of external connections to third parties, internet providers and other entities. Being able to manage security and monitoring at a high multiple of external connections is tough without a fabric technology like Big Switch."

SPECIFICALLY, THE NEW EXTRANET WOULD NEED TO:

- Handle numerous cybersecurity appliances to provide intrusion prevention, malware detection, and traffic decryption capabilities. These devices would need to be easily added to, or removed from, the production network.
- Allow the cyber team to inspect traffic as it traverses the network, and be able to make copies of the traffic dynamically, for quick analysis "on the fly."
- In the event of network outages or performance issues, support easy device removal and traffic re-routing to allow troubleshooting around the device.

To meet its overarching goals of visibility, granularity, and control over the security tools located in the extranet's DMZ, the Company chose Big Switch's Big Mon Inline. Now in production, the Team Lead recalls, "After a very extensive six-plus month effort with a lot of design phases, we looked at solutions from numerous vendors, including Big Switch. We did lab testing, a proof of concept implementation and a small pilot."

"We have rolled out BMF Inline across multiple sites across the globe. It's a very critical, integral part of our design, and so far we've had great success. With Big Switch's software-defined security fabric we have been able to deliver on, and exceed, our monitoring and operational requirements."

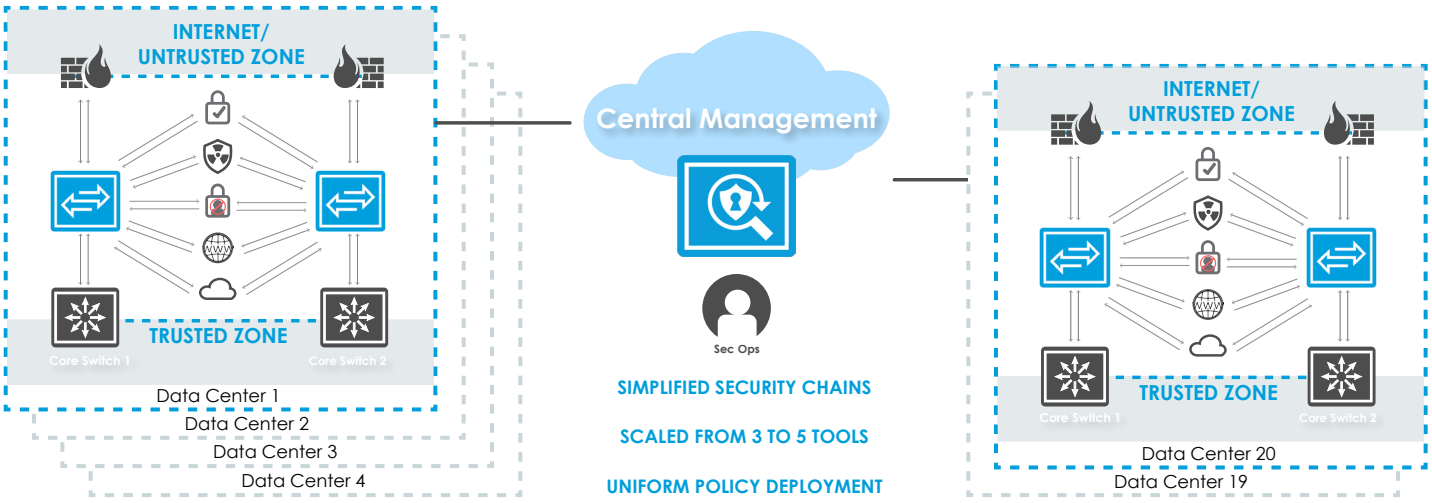
New Agility and Improved Network Performance

The biggest change the Team Lead sees with the new extranet is the flexibility in how the Company can manage its cybersecurity and monitoring tools. He explains, "By flexibility, I mean we have a large, distributed team, with different initiatives happening all the time; there's no way we can anticipate upcoming tools we may want to use. Because the security environment can change overnight with new threats, it was crucial for us to be able to add new tools on-the-fly, without having to recable all of our network, and without having to worry about breaking something when we added or removed a tool."

In terms of performance monitoring, the Company primarily uses security tools and performance analytics tools to gauge, for example, how long packets are taking to traverse the network. *"When someone starts complaining that something is slow, we can quickly go back and see what happened, and figure out what the problem is. We didn't have those capabilities before, because it was too difficult to collect streaming data from every endpoint. Now that we are aggregating all traffic to BMF Inline as a single point of presence; from there, we can collect traffic and present it to any tool we want."*

Having the flexibility to send certain traffic to specific tools is a critical for the Company and *"is instrumental in how Big Switch has designed their product,"* the Team Lead says, allowing network analysts to pick and choose traffic flows based on any given requirement.

"Before, since the devices were physically cabled up, we did not have that flexibility; we were physically constrained from splitting traffic streams. With BMF Inline we have a taken a huge load off the devices, sending only legitimate traffic to them, whereas before we were sending everything. This is more efficient, and reduces license fees that we pay to the tool vendors, since we need fewer devices to handle the reduced capacity."



Simplifying Network Management

The Company uses the Big Switch software-defined controller to gain a single pane of view, managing multiple deployments from one interface. *"This speeds up deployment, helps operations, and eases our compliance activities because we manage and push everything from one centralized view,"* the Team Lead says, continuing, *"Big Switch's graphical representation turns network management upside down, in a good way. The network has always been managed with command line [CLI]-based syntax, but now, anybody can look at the Big Switch controller and understand how the traffic is being routed from the network to different appliances and back out."*

Previously, when a network outage occurred, *"we had to pull diagrams, call people who worked on the project, and get people on site to tell us how a cable is connected. Now anyone on our team can just look at the interface and it makes sense. The visualization really helps to put it all together. Big Switch has done a great job with the UI design and has really differentiated themselves in this area."*

Unexpected Cost Savings

The Company's previous extranet model necessitated multiple pairs of appliances to cover multiple paths into and out of the network. The Team Lead says, *"It was very expensive, and difficult to monitor asymmetric traffic. Now, with an aggregated view of all traffic, we just have to buy and maintain just one set of tools. Over a network of our size, that's a significant savings."*

He concludes, *"What's more, if there's a failure condition we can work around it, and if one path fails we can always send the same traffic to the appliance again. BMF Inline opens more doors to other opportunities that we didn't anticipate. In the networking world, Big Switch is a breath of fresh air."*

big switch networks

Big Monitoring Fabric is a network visibility fabric that leverages high performance, open Ethernet switches to provide pervasive security, monitoring and visibility of an organization's network traffic. Using an SDN-centric architecture, Big Mon enables a scale-out fabric for enterprise-wide monitoring, a single pane of glass for operational simplicity, and multi-tenancy for multiple IT teams to perform network monitoring using tenant-specific inline or out-of-band tools and policies.

Big Mon Inline enables pervasive security in the DMZ, addressing challenges faced by traditional solutions. Big Mon consists of a Big Mon Controller and open HW switches deployed in HA configuration. Leveraging the Controller as the central point of management, Big Mon configures policies that create paths through the inline tools. The solution supports load balancing across multiple instances of the same tool and chaining of a set of tools on a per-policy basis.

To learn more about Big Monitoring Fabric, register for BSN Labs to get hands-on experience via our self-paced labs modules. To register (it's free): http://labs.bigswitch.com