



CASE STUDY

State of Nebraska

93 State Agencies Protected by Unified Threat Management Appliances – Power in Unity

Situation

The [State of Nebraska's Office of the Chief Information Officer](#) (CIO) acts as an Internet solution provider (ISP) to all state agencies. Its mission statement is "To serve the citizens of Nebraska by providing premier information technology leadership, policy and operations which facilitate an effective, responsive and efficient government." That vision is based on four priorities: education, economic vitality, efficiency in government and protection of families. They are also proud to state that they believe in "Power in Unity".

When it came time to replace their previous Check Point network security solution, the Office of the CIO furthered their belief in "Power in Unity". Because of its per user licensing model for Web filtering and anti-virus, the Check Point solution proved to be too costly to maintain on such a large network. They wanted and needed to reduce capital costs associated with maintaining the network. In addition, the State wanted a more comprehensive network security solution that offered multiple functionalities within a single appliance.

"When we decided to replace our previous network security solution we knew that we had to better manage new threats," said Brad Weakly, State Information Security Officer for the Office of the CIO. "Our previous solution wasn't giving us the necessary protection that we wanted and needed to offer our agencies."

Solution

After looking at multiple network security vendors, the Office of the CIO competitively selected the Fortinet multi-threat solution to protect its entire network for a number of reasons.

The Office of the CIO found that the FortiGate Web interface is extremely easy to use and it offers a consistent graphical user interface (GUI) across the [FortiGate](#) product line. No matter the size of the appliance, the GUI is the same and as a result, less time is needed to learn new interfaces. The command line interface (CLI) was also very easy to use which gives network administrators who prefer CLI more direct control to the product line. The built-in ability to easily monitor network traffic convinced the administrator that they were off to a great start with the FortiGate product.

Deploying a multi-threat security appliance also allowed the Office of the CIO to have firewall, IPS, antivirus, SSL VPN and Web content filtering in one appliance which translates into a single vendor to work with, reduced maintenance costs and the ability to configure virtual domains to meet the specific needs of each agency.

With the multiple functions in the FortiGate products, the Nebraska Office of the CIO can deploy the same product for different applications. The deployment of the FortiGate products can be simplified into three different applications:

- Clustered FortiGate appliances dedicated for site-to-site VPN connections for all remote agencies
- VDOMs for individual agency Internet and multi-threat security functionality
- VDOM as the center of distributed agency's routing and proxy server

Challenges

- Find a more economic solution
- Better manage new and increasing network security threats

Objectives

- Deploy an easy-to-use network security solution
- Reduce IT spending
- Provide network security to specific agency requirements

Deployment

FortiGate-30Bs
FortiGate-60Cs
FortiGate-80Cs
FortiGate-110s
FortiGate-310B
FortiGate-3810A
FortiAnalyzer

Industry

Government

By consolidating our network security infrastructure to one vendor, we have been able to avoid expenses of up to \$100,000 - \$200,000 a year while increasing the security functionality offered to agencies.

- Brad Weakly

State Information
Security Officer

State of Nebraska

“With multiple functionalities within a single FortiGate appliance you would expect each one to be sub par,” added Gavin Bingman, State Network Engineer for the Office of the CIO. “However, Fortinet’s individual security functionalities are constantly on the top 5 of our list. The sum of the top 5 in all areas is a lot greater than any best of breed solutions and we didn’t have to give up any performance by having everything all in one.”

At the core of the CIO’s office is a pair of [FortiGate-3810A](#) appliances in high availability (HA) mode. The Fortinet appliances are serving as the firewall for the Lincoln, NE based office as well as a second layer of protection for all state agencies. The virtual domain (VDM) functionality of the FortiGate appliances is allowing the State to segregate each agency yet offer firewall protection as well as additional security functionality as required by each individual agency.

Also at the headquarters is a [FortiAnalyzer](#) appliance which is allowing the IT staff to view traffic logs, Web filtering logs and event logs for the entire network. In addition, the IT staff can also do remote set-up and troubleshooting.

The Office of the CIO creates a VDM for each of the individual agency with a basic set of network policies. Each individual agency with its own IT staff is given control to their VDM to manage the day to day network and the rules set up for that particular location. On top of the individual agency’s network policy, the Office of CIO has another layer of global network policy that allows them to have full control on the state network. This hierarchical approach provides the maximum security for the state and flexibility that is essential to the individual agency. When the individual agency needs help with setting up its network, security functionality or troubleshooting issues, the Office of the CIO can effectively assist them because of the clear demarcation between policies.

The comprehensive list of features in the FortiGate appliance also allows the Office of CIO to provide additional functions to the individual agency when it is needed. For example, if the local agency Web proxy service is down, the Office of the CIO can quickly provide the backup service through the FortiGate without installing any new equipment.

Success

The Office of the CIO has seen dramatic success since standardizing on FortiGate appliances. Segregating the network via virtual domains has allowed the State to maintain better control of the network while making network management much easier. If a new agency needs to be added to the network, it can easily be done remotely. Truck rolls are no longer needed and the cumbersome task of managing multiple agencies is now simplified with Fortinet’s virtual domains. Network breaches that could have taken down the entire network are no longer a valid concern because different networks now have their own rules and protection policies.

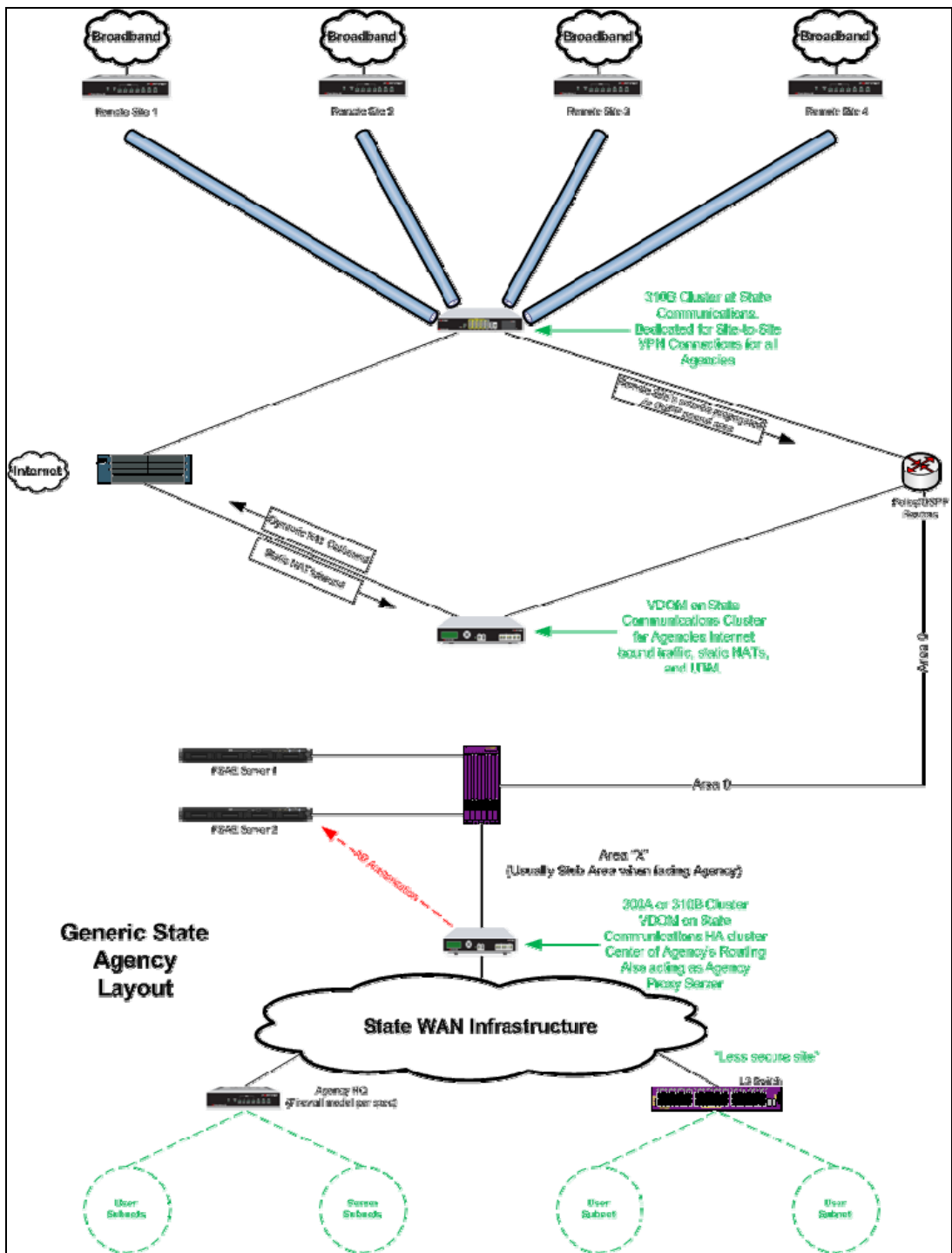
One of the larger benefits of the FortiGate deployment is the visibility that the network staff now has into not just the headquarters’ network, but all the agencies’ network. Previously having to monitor ports per agency site, the team can now watch traffic live and view traffic logs, Web content filtering logs and event logs with ease.

With a simplified GUI, IT managers can easily make changes to any Fortinet appliances without having to learn a new GUI. No matter the size of the appliance the GUI is the same across the product line. This simplifies network management and makes remote management and troubleshooting much easier.

The Office of the CIO has been a long time user of FortiGate products, going back about five years. They are very excited with the constant innovations in the Fortinet product line as new services such as Web proxies, SSL offload and SSL VPN are being offered to the local agencies.

Since deploying the Fortinet solution both internally and at agency sites, the Office of the CIO has seen a reduction in network security costs. No longer do they have to purchase individual point products to meet network security needs. Fortinet’s unified threat approach allows the Office of the CIO to buy appliances and add or remove functionalities as needed without added costs. With a single vendor offering multiple functionalities and one GUI, there are now less headaches associated with working with multiple vendors – headaches that generally lead to extra costs from multiple contracts and multiple points products.

“By consolidating our network security infrastructure to one vendor, we have been able to avoid expenses of up to \$100,000 - \$200,000 a year while increasing the security functionality offered to agencies.” concluded Weakly.



FORTINET

GLOBAL HEADQUARTERS

Fortinet Incorporated
 1090 Kifer Road, Sunnyvale, CA 94086 USA
 Tel +1.408.235.7700
 Fax +1.408.235.7737
 www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE

Fortinet Incorporated
 120 rue Albert Caquot
 06560, Sophia Antipolis, France
 Tel +33.4.8987.0510
 Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE

Fortinet Incorporated
 61 Robinson Road, #09-04 Robinson Centre
 Singapore 068893
 Tel +65-6513-3730
 Fax +65-6223-6784