A Survey of Enterprise Middlebox Deployments

Justine Sherry
Sylvia Ratnasamy

Electrical Engineering and Computer Sciences
University of California at Berkeley

Technical Report No. UCB/EECS-2012-24
http://www.eecs.berkeley.edu/Pubs/TechRpts/2012/EECS-2012-24.html

February 9, 2012

A Survey of Enterprise Middlebox Deployments

Background

In November 2011, we surveyed 57 enterprise network administrators, primarily from the NANOG network operators group, regarding network appliances or so-called 'middleboxes.' We designed our survey with the goal of bridging the gap between research and practice, by allowing the experiences and concerns of network administrators to inform the direction of our research. We asked operators about the number of middleboxes they deployed, what the challenges are in managing middleboxes, how much middleboxes cost, and what causes middleboxes to fail. Not only has the survey data driven some of our own research, but we hope that once published some of our conclusions will be able to guide others in the research community.

With this report, we aim to give back to the operator community by reporting on our findings and conclusions. We hope that you find our data useful. Any comments or feedback to us would be greatly appreciated; you can contact Justine Sherry at:

justine@eecs.berkeley.edu

1. THE SURVEY

A wide body of work in the networking research community focuses on challenges with middleboxes. 'Middlebox' is an academic term, typically defined as *'any intermediary box performing functions apart from normal, standard functions of an IP router on the data path between a source host and destination host'* [4]; in industry most of these devices are instead termed 'network appliances.' Researchers have focused on a diverse set of issues related to middleboxes: making middlebox-laden networks easier to manage [3], designing new middleboxes, *e.g.* for intrusion detection [6], building general-purpose middleboxes from off-the-shelf hardware [7], removing middleboxes from networks entirely [5], *etc.* However, we found that concrete, academic data on typical middlebox deployments and their challenges was unavailable. When descriptions of middlebox deployments were available, they typically only reflected the experiences of a single enterprise.

To fill this gap, we conducted a survey of 57 enterprise network administrators regarding their networks, including the number of middleboxes deployed and challenges faced in administering them. To the best of our knowledge, this is the *first large-scale survey* of middlebox deployments in the research community. Our dataset includes 19 small (fewer than 1k hosts) networks, 18 medium (1k-10k hosts) networks, 11 large (10k-100k hosts) networks, and 7 very large (more than 100k hosts) networks. Our respondents were drawn primarily from the NANOG network operator's group and university networks; 62.9% described their role as an engineers, 27.7% described their role as technical management, and the rest described their role as 'other.'

Our analysis led us to four major conclusions to inform future research:

- Middlebox deployments are large – on par with the number of L3 infrastructure – and incur high capital expenses (§2). capex
- Middleboxes have complex management requirements, leading to high operational expenses and administrative headaches (§3) opex
- Overloads and failures lead to a need to overprovision middleboxes for scalability and fault-tolerance (§4).
- Upgrading to new features is often bound to purchasing new hardware, limiting the ability to quickly deploy new features (§5).

We discuss each of these challenges as follows.

2. MIDDLEBOX DEPLOYMENTS

Our data illustrates that typical enterprise networks are a complex ecosystem of firewalls, IDSes, web proxies, and other devices. Figure 1 shows a box plot of the number of middleboxes deployed in networks of all sizes, as well as the number of routers and switches for comparison. Across all network sizes, the number of middleboxes is on par with the number of routers in a network! The average very large network in our data set hosts 2850 L3 routers, and 1946 total middleboxes; the average small network in our data set hosts 7.3 L3 routers and 10.2 total middleboxes.[1]

We also observe trends between different types of middleboxes Security appliances (IP and Application Firewalls, IDS/IPS) tend to be more common than performance-improving appliances (WAN Optimizers, Proxies, and Application gateways) except in very large networks, where performance improving appliances are more common, although with high variance in deployment.

These deployments are not only large, but are also costly, requiring high up-front investment in hardware: thousands to millions of dollars in physical equipment. Figure 2 displays five year expenditures on middlebox hardware against

[1]Even 7.3 routers and 10.2 middleboxes represents a network of a substantial size. Our data was primarily surveyed from the NANOG network operators group, and thus does not include many of the very smallest networks (*e.g.* homes and very small businesses with only tens of hosts).

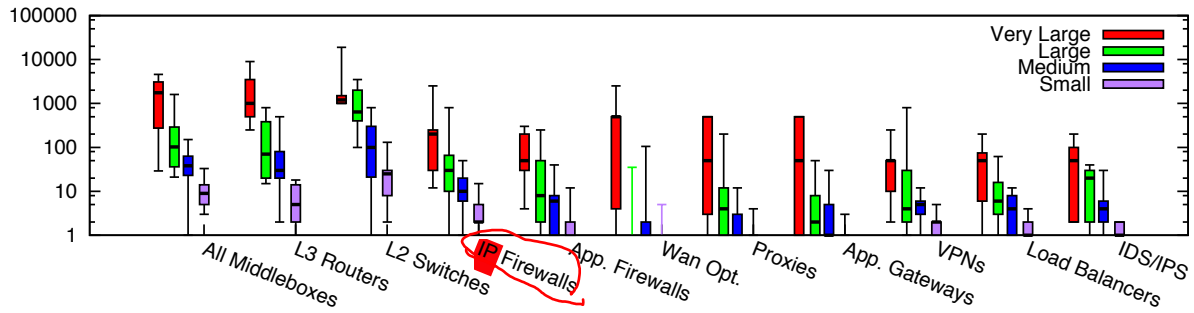

Figure 1: Box plot of middlebox deployments for small (fewer than 1k hosts), medium (1k-10k hosts), large (10k-100k hosts), and very large (more than 100k hosts) enterprise networks. Y-axis is in log scale.

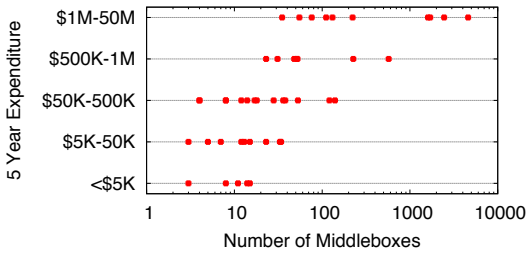

Figure 2: Administrator-estimated spending on middlebox hardware per network.

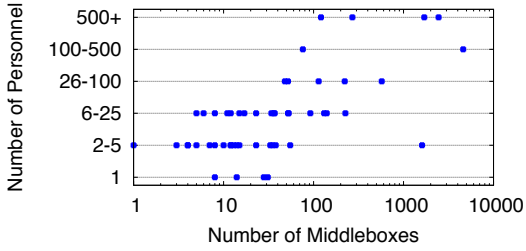

Figure 3: Administrator-estimated number of personnel per network.

the number of actively deployed middleboxes in the network. All of our surveyed very large networks had spent over a million dollars on middlebox hardware in the last five years; the median small network spent between $5,000-50,000 dollars, and the top third of the small networks spent over $50,000.

3. MIDDLEBOX MANAGEMENT

Figure 1 also shows that middleboxes deployments are diverse. Of the eight middlebox categories we present in Figure 1, the median very large network deployed seven categories of middleboxes, and the median small network deployed four categories of middleboxes. Our categories are coarse-grained (*e.g.* Application Gateways include smartphone proxies and VoIP gateways), so these figures represent a *lower bound* on the number of distinct device types in the network.

Managing many heterogeneous devices requires broad expertise and consequently a large management team. Figure 3 correlates the number of middleboxes against the number of networking personnel. Even small networks with only tens of middleboxes typically required a management team of 6-25 personnel. Thus, middlebox deployments incur substantial operational expenses on top of hardware costs.

Understanding the administrative tasks required to manage middleboxes further illuminates why large administrative staffs are needed.

Monitoring and Diagnostics. To make managing tens or hundreds of devices feasible, enterprises deploy network management tools (e.g., [2, 1]) to aggregate exported monitoring data, *e.g.* SNMP.

Configuration. Configuring middleboxes breaks in to three classes of tasks. *Appliance configuration* is installing new rulesets and upgrades, configuring cache sizes, and allocating IP addresses. *Traffic configuration* is ensuring that the right traffic traverses the right middlebox, configuring routing policies such that, *e.g.* port 80 traffic traverses an HTTP proxy. Finally, *policy configuration* is tuning middleboxes to enforce specific policies, *e.g.* that social networking sites are banned by the application firewall.

Training. New appliances require new training for administrators to manage them. One administrator even stated that existing training and expertise was a key question in purchasing decisions:

> Do we have the expertise necessary to use the product, or would we have to invest significant resources to use it?

Another administrator reports that a lack of training limits the benefits from use of middleboxes:

> They [middleboxes] could provide more benefit if there was better management, and allocation of training and lab resources for network devices.

4. OVERLOAD AND FAILURES

Most administrators who described their role as engineering estimated spending between one and five hours per week

	Misconfig.	Overload	Physical/Electric
Firewalls	67.3%	16.3%	16.3%
Proxies	63.2%	15.7%	21.1%
IDS	54.5%	11.4%	34%

Table 1: Fraction of network administrators who estimated misconfiguration, overload, or physical/electrical failure as the most common cause of middlebox failure.

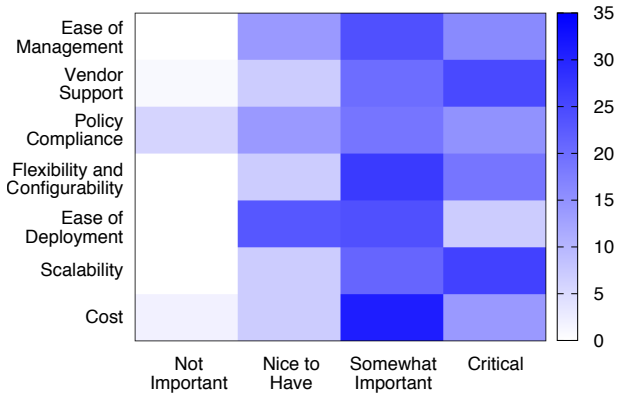

Figure 4: Importance of various factors in comparing middleboxes for purchase.

dealing with middlebox failures; 9% spent between six and ten hours per week. Table 1 shows the fraction of network administrators who labeled misconfiguration, overload, and physical/electrical failures the most common cause of failures in their deployments of three types of middleboxes. Note that this table is *not* the fraction of failures caused by these issues; it is the fraction of administrators who estimate each issue to be the *most common* cause of failure. A majority of administrators stated misconfiguration as the most common cause of failure; in the previous subsection we highlight management complexity which likely contributes to this figure.

On the other hand, many administrators saw overload and physical/electrical problems as the most common causes of errors. For example, roughly 16% of administrators said that overload was the most common cause of IDS and proxy failure, and 20% said that physical failures were the most common cause for proxies. These classes of failures are traditionally resolved by deploying redundant devices for better scalability and fault-tolerance.

5. UPGRADEABILITY

Deploying new features in the network entails deploying new hardware infrastructure. Each time operators negotiate a new deployment, they must select between several offerings, weighing the capabilities of devices offered by numerous vendors – an average network in our dataset contracted with 4.9 vendors. In Figure 4, we show various factors that operators weigh when considering a new appliance. We asked administrators to rank each feature as 'Not Important', 'Nice to Have', 'Somewhat Important', or 'Critical'; Scalability and Vendor Support were the two features most commonly considered critical.

In the median case, enterprises update their middlebox hardware every four years. The four-year upgrade cycle is at the same time both too frequent and too infrequent. Upgrades are too frequent in that every four years, administrators must evaluate, select, purchase, install, and train to maintain new appliances. Upgrades are too infrequent in that administrators are 'locked in' to hardware upgrades to obtain new features. Quoting one administrator:

> Upgradability is very important to me. I do not like it when vendors force me to buy new equipment when a software upgrade could give me additional features.

6. CONCLUSION

We presented data on middlebox deployments from 57 enterprise networks surveyed from the NANOG network operators group. Our data revealed several challenges for the research community to consider: large and costly deployments, complex management requirements, overloads and failures, and limited upgradeability.

If you have any comments, questions, or feedback, please don't hesitate to contact us (`justine@eecs.berkeley.edu`). Finally, we thank you for your help and support for our study!

References

[1] Network monitoring tools. `http://tinyurl.com/nmtools`.

[2] Tivoli Monitoring Software. `http://tinyurl.com/7ycs5xv`.

[3] H. Ballani and P. Francis. Conman: a step towards network manageability. In *SIGCOMM*, 2007.

[4] B. Carpenter and S. Brim. Middleboxes: Taxonomy and issues. RFC 2334.

[5] C. Dixon, H. Uppal, V. Brajkovic, D. Brandon, T. Anderson, and A. Krishnamurthy. ETTM: a scalable fault tolerant network manager. In *NSDI*, 2011.

[6] V. Paxson. Bro: A system for detecting network intruders in real-time. In *Computer Networks*, pages 2435–2463, 1999.

[7] V. Sekar, S. Ratnasamy, M. K. Reiter, N. Egi, and G. Shi. The middlebox manifesto: enabling innovation in middlebox deployment. In *HotNets*, 2011.