Scenario
Customer desires to upgrade their boundary architecture and solutions to meet current threats and extend options for secure business communications.

Current Architecture
Customer's boundaries are a mix of stateful inspection and proxy firewalls from two firewall vendors. There are web and mail content proxy servers, and a separate DMZ with web servers with business applications available to external clients.

Requirements
Customer has had numerous malware events, arising from targeted phishing attacks as well as indiscriminate drive by downloads from web sites. The incidents were disruptive to operations and one incident had to be publicly reported as it involved a customer's Personally Identifiable Information (PII). The customer is also concerned about proprietary data being exfiltrated by malware as well as by employees. Regulations and a desire to expand their web services are pulling the customer towards ISO 27001 compliance. Developing better boundary architecture will be a major step toward that compliance goal

Initial Assessment
After reviewing requirements the following is discussed:

- What is the budget for implementation/training and for ongoing maintenance?
- What products /solutions do you have now (in production and in development)?
- Describe your security organization; how is the boundary managed and by whom?
- How committed are you to multiple security products?
- Where is your company security policy, and is the boundary security policy documented within?
- Please confirm what standards and regulations that you need to comply with (FISMA, ICD 503, NIST 800-53, HIPAA, PCI, Sarbanes/Oxley, GLB, FFIEC, etc.)

The desire is to design a solution that fits with the customers' existing product lines and the skillsets of those who will be maintaining the solutions. For example, if the customer's security support staff is used to dealing with Cisco security solutions and if a Cisco solution meets the requirements, then it would be recommended.

Frequently customers have products that can be leveraged to do more than what they were aware of when purchased; an example would be a load balancer that can also terminate SSL sessions, or a firewall that has IPS functions that have never been utilized.

Layered Security
The issue of defense in depth is often misunderstood as purchasing products which provide the same function from multiple vendors. That is vendor diversity. Defense in depth is a layered approach to security, starting from layer 8 (the human being), and moving to securing the

application through secure coding practices and testing, down through to the session layer (authenticating client to server and server to server communication), to the operating system (hardening the OS) and encrypting data in transit and restricting who can communicate with what (network security). In other words, when architecting a solution, using multiple vendors is acceptable, as long as they are interchangeable solutions, but not stacked up and performing the same function. For example, if two firewalls are in line in a boundary, both examining the same traffic with the same rules the client is wasting resources and creating a situation that is more difficult to manage. If vendor diversity is desired, perhaps one vendor product would work better as an internal firewall and another vendor's firewall would be better on the network edge.

Recommended Solutions

After examining the existing infrastructure and interviewing staff, the following options were suggested:

Deploy a 'NextGen' firewall, which would provide the following solutions to the customer's boundary requirements:

- Application awareness, a feature of NextGen firewalls, permits granular control and visibility into what traffic is entering and leaving the enterprise. Meld the rules to the company's security policy to the ruleset and consider tightening up what can now be seen and controlled (such as uploads to file sharing sites, games and chat on social networking sites, etc.).
- User and group awareness is another feature of NextGen firewalls. By tying these into the enterprise LDAP directories, the customer can create rules by user and group and not by hostname/IP address. Wherever the user goes within the workplace, the rules on the firewall permit or deny access by userid, not by the IP address of the workstation, smartphone, or laptop. The resulting rules are easier to understand and manage, when maintaining the firewall.
- NextGen firewalls also can act as man-in-the-middle proxies for SSL decryption, something that would go a long way to detecting and blocking malware at the edge of the network, not at the endpoint. SSL decryption also permits the inspection of what applications are being shunted across SSL, and what data is being sent out. This is critical to ensure that Malware is caught and data is not being exfiltrated across encrypted connections.
- NextGen firewalls have data loss prevention (DLP) functionality, which can be used to examine traffic for certain words and phrases or certain types of files. As the customer is concerned about data being exfiltrated, enabling DLP is a mitigation strategy.
- Antivirus is an option on most firewalls, NextGen and existing stateful firewalls. Kaizen encourages the customer to enable antivirus on specific file types, using a *different* antivirus vendor than the product currently used on their existing mail/spam content filter. One antivirus vendor will never catch all the malware, using two good products increases the odds of blocking more viruses.

- Intrusion Prevention System (IPS) is also a function of NextGen firewalls and of some existing firewalls as well. The difference between these and NextGen is the breadth of functionality, speed and performance of IPS versus the older firewalls that are slower, lack functionality, and performance. Reputation based controls, for inbound web, mail traffic are also available on regular and NextGen firewalls. The customer was unaware that the reputation controls were available on the current firewall, and was advised on how to implement the control. This restricts connections to/from known botnet and spambot servers, limiting connections from malware and spam producing servers.
- Kaizen then recommend a NextGen firewall based on our own knowledge, experience, as well as test results from independent labs such as NSS and ICSA.

Closely related, we recommended the customer leverage an existing firewall monitoring and auditing solution for firewall cleanup and change control. Kaizen encouraged the use of the product beyond that of the firewall admins, creating reports for the internal audit and compliance departments. This product also has the ability assess the firewall configurations against the enterprise security policy and to provide artifacts and evidence of monitoring for certain situations that would be extremely useful in obtaining and maintaining an ISO 27001 certification.

Proper deployment of the functions of a NextGen firewall, in conjunction with the customer's existing mail content filtering/spam/malware solution, would go a long way to mitigating the threats from malware and viruses. To take the defense to the next step, and in light of the intrusions that the customer endured in the past year, Kaizen also recommended a zero day malware solution.

- Zero Day malware solutions work on the basis of known behaviors (heuristics) and the ability to create new signatures as new malware is detected, and alert/block on what is found. Some solutions have the ability to run suspected malware on virtual machines, to analyze and assess the code. If it is determined to be malware, a signature is created for future detection and the alert is made, subsequent downloads will be blocked. Malware detected is also packaged for analysis, if so desired. Some solutions can block callbacks to command and control servers on the internet from compromised devices within the enterprise, thus preventing further actions and neutralizing the malware, until the afflicted internal machines can be cleansed or reloaded.

The web servers providing services to external clients are well secured, on hardened Linux apache servers, with no detected application vulnerabilities (SQL injection or cross site scripting, for example). All data communication is SSL encrypted and the existing firewall limits ingress and egress flows. Management of the machines is through a separate management network. Kaizen recommends adding the following options:

- Investigate a third party automated scanning of all internet entry points, web servers especially. This should be done at least on a monthly basis, or done adhoc after any changes are made to the boundaries or the web servers. The scanning service should provide reports of any vulnerability found and the means to mitigate them. Ideally problems should be ranked in order of severity and the service should be up to date on security exploits and threats.

- As the web applications are all written in house, it is recommended that major code updates be reviewed for vulnerabilities by an external party. There are services such as Veracode which examines binary code for possible code exploits. As most intrusions are achieved through application errors, this might be a good direction for the future.

- Investigate strong authentication options for the external clients performing monetary /fiscal transactions on the web servers. There are smartphone enabled applications that can replace the need for separate tokens or fobs. This would not only protect the customer and the external clients from stolen credentials, but greatly enhances the perceived security of the customer to their clients. This can be a marketing/sales enhancer, and keeps the customer on the positive side with the regulators.

- Run an integrity checker like Tripwire on the web servers. Given the hardened and restricted capabilities of the web servers, Tripwire adds that extra bit of certainty that the integrity of the servers is still intact. Another positive stroke for ISO 27001 certification.

Summary

The Kaizen team performed a comprehensive assessment of the customers' existing security posture. With an understanding of customer requirements (regulatory, budgetary, etc.) we made many recommendations to improve their posture. By adopting our layered approach to security, the customer is well positioned to withstand the rigors of regulatory auditors and protect their network and data.