Gartner

Research

Publication Date: 12 August 2008 ID Number: G00160362

Q&A: Is It More Secure to Use Firewalls From Two Different Vendors?

Greg Young, John Pescatore

Enterprises should standardize on one firewall platform to minimize self-inflicted configuration errors. It's not more secure to use firewalls from different vendors, instead of one to protect enterprise networks.

© 2008 Gartner, Inc. and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner's research may discuss legal issues related to the information technology business, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice.

ANALYSIS

Is It More Secure to Use Firewalls From Different Vendors at the Different Layers in Our "Demilitarized Zone" (DMZ)?

Two firewall platforms are not better than one. We believe there is a higher risk associated with configuring and managing firewalls from multiple vendors than from a single vendor. Therefore, Gartner advises enterprises that have more than one firewall to standardize on a single vendor platform when the opportunity presents itself (that is, new installations or replacement during a refresh). In choosing a standard firewall, enterprises should consider the experience of their firewall administrators with each platform, scalability, central management and cost.

Years ago, it was often recommended to use two vendors' firewall products. This was done to provide an overlap of capability in case a single product could not be relied on. The argument for this practice was that, if hackers exploit a vulnerability in one firewall, then it's unlikely that they will be able to get through the second firewall — therefore, two firewalls are better than one. This is no longer the case. Two firewall platforms cause more security concerns than they solve.

Most security breaches at the enterprise firewall are caused by misconfigurations, not by exploited vulnerabilities in the product. Firewall vulnerabilities do occur, but they are quite rare and are usually reported to vendors and patched before the public (and, thus, hackers) are aware that they exist. Diligence in patching firewalls, monitoring configuration and assessing the rule base is required to maintain security. Gartner believes that managing the updates for a single platform is less costly and less prone to error than configuring two separate platforms, with two different graphical user interfaces, policies (rules) and architectures.

Debugging a new Internet application (especially Web services) or working with a new trading partner often involves temporarily adding permissive rules to a firewall. Confusion over what protocols are used by the application can cause the administrator to open the firewall and close down services until the application eventually breaks. Performing this process with two different firewall user interfaces is cumbersome and even more prone to error, particularly on the firewall platform with which the administrator is less proficient. Firewall configuration tools are almost exclusively proprietary to a single platform, so they cannot be used to resolve multivendor complexity — or at least not with the degree of granularity required.

The complexity of today's enterprise DMZ also aggravates the task of aligning two rule sets, along with their monitoring and maintenance. Firewall training costs and training times are doubled for a single firewall team, and having multiple teams manage separate firewall products in the same DMZ can breed confusion with the resulting misconfigurations.

Providing an audit review of firewall rules is a common compliance and general security practice, and is made more complex with multiple vendors, as is providing infrastructure support, such as load balancing and failover. Most enterprise firewall vendors have improved their branch-office firewall offerings, so that these remote locations can be well-served with products under the same console as the primary firewalls.

For a small percentage of enterprises, having firewalls from two vendors may be warranted, but this is only where an enterprise has such an extraordinarily low level of acceptable risk that the small risk of a firewall vulnerability is unacceptable. This requires a higher level of staffing, training and oversight in exchange for this risk reduction; otherwise, these enterprises face the higher-risk scenario of misconfiguration described earlier. In many cases, diversity can improve survivability; however, in the case of network firewalls, the benefits of diversity are minimal, and the risks are significant.

© 2008 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

If you have two incumbent vendors, then an immediate change may not be required or urgent. An ideal time to move to a single vendor is when a firewall technology refresh is due or a DMZ redesign is under way. Use the presence of a competitor to drive steep discounts for an incumbent vendor to increase its "wallet share." Where a firewall technology refresh is far in the future, look to the incumbent of the preferred platform to provide sufficient incentives in exchange for giving up the investment in the second vendor's platform. If appropriate to the DMZ design and local security policy, then consider upgrading to a larger, single, virtualized firewall instead of two single appliances as a possible convergence. Plan for the additional work of rule migration because this remains a manual task between firewalls of different vendors.

Key facts are as follows:

- Having two different firewall platforms greatly increases configuration and management problems.
- More than 99% of firewall breaches are caused by firewall misconfigurations, not firewall flaws.
- Debugging an error in firewall rules or a new application can be cumbersome and time-consuming.
- The increasingly complex DMZ is increasing the complexity in firewall rule bases.
- A single vendor relationship can yield greater discounts and lower contract administration overhead.

RECOMMENDED READING

"Magic Quadrant for Enterprise Network Firewalls, 2H07"

© 2008 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

© 2008 Gartner, Inc. and/or its Affiliates. All Rights Reserved.