Managing Enterprise Network and Security Policy

By
David Hurst
CTO, Lisle Technology Partners

Introduction

With the global threat environment more acute than ever, network security has become a *sine qua non* for doing business for most public and private enterprises. Network security above all requires the ability to set (i.e who should be able to communicate with whom) and validate (who does communicate with whom) network policy. In addition, it requires the ability to identify and fix network vulnerabilities, conduct network audits for statutory compliance, quantify risk and use it to set the level of risk necessary for conducting normal business operations, set up processes for defense in depth in an evolving threat environment, and manage changes to the network while preserving or enhancing the level of security.

"Such approaches break down very quickly, because at their core they do not handle the fundamental problem of providing a complete analysis of the network."

Managing Network Policy

Network security is such a multi-faceted problem that it is not surprising that current solutions in the marketplace follow different approaches. As an example, to figure out network reachability, logs of network devices such as firewall and router logs are analyzed to trace the routes packets have taken. Obviously, the results are not comprehensive because only a limited number of logs can be examined, and in the ones that are examined certain packet traversal that are potentially dangerous may not have occurred. Another approach to the problem is a firewall audit. In this procedure, firewall configurations, which specify pass/deny policies for packets in that firewall, are analyzed. In enterprise networks, packets traverse multiple network devices so a large number of configurations need to be examined in *ad hoc* manner.

Such approaches break down very quickly, because at their core they do not handle the fundamental problem of providing a complete analysis of the network. The dictum *know your network* is fundamental to tackling not just network policy, but all the other related issues such as vulnerability, risk assessment, remediation, and change management. In its broadest interpretation, knowing your network means knowing the topology of the network, and path based policies, i.e., the comprehensive set of allow and deny policies for the network. By comprehensive we mean, all possible allow (or deny) packet traversal from any source, to any destination, using any protocol, and via any source port and any destination port. Within the ambit of the term comprehensive, we include hosts within the

enterprise network, external hosts such as that of a business partner, or any public site on the Internet. It includes wireless data and VOIP access as well. If we cast policy analysis as a mathematical computation, a comprehensive solution could be referred to as mathematically complete.

Athena Verify™ uses this approach as the foundation of its approach to network security. Athena calculates a comprehensive set of network policy statements based on configuration files imported directly from network devices, and lays out the correct network topology and connectivity based on the analysis of the data in a non-invasive manner. It is then almost instantaneous to verify polices between any two points in the network. The policy editor not only reveals policy but also provides comprehensive detail regarding the policy route and the specific rules in configuration files that led to the policy. Complex network address translation schemes are handled as well. Deny policies have just as much useful information as allow policies. Athena treats deny policies as duals of pass policies providing the same information and in the same format. Tracing the route of a deny policy, it is possible to locate the device and the device rule that disallows the packet. This is very useful in situations where policy changes are contemplated.

"It is then almost instantaneous to verify polices between any two points in the network."

Check Point FW-1, Cisco IOS, Cisco PIX Version 5, Linux IP tables/Chains, Juniper Netscreen, Cisco Catalyst, etc. are all network devices that have a significant market presence and can be expected in any enterprise network. Each of these devices use different rule languages to set policy. Athena reduces this babble of configurations to a common syntax so that network policy evaluation can proceed in a uniform manner across network devices of any type. Once a policy is calculated its path can be linked to rules that are back annotated to the device specific language.

Managing Security Policy

Network policy largely pertains to network reachability, but security policy is concerned with network policies taken as a whole. Security policy grapples with issues of vulnerability (to attack), effectiveness of defense, and risk and seeks to calibrate them through quantitative measures. Such measures are the key tool in evaluating security controls, meeting audit and regulatory compliance, maintaining a minimum-security posture, and enabling continuous improvement processes. Security policy will then be in lock step with corporate IT control policies while addressing the following key issues: how effective are the policy controls that have been put in place, and how does one quantify the risk to the critical assets in the enterprise. The issue of risk arises from the need to allow various degrees of network access inside and outside the enterprise network to support various business processes.

Athena implements a policy controls evaluation engine that uses policy data to evaluate the various policy controls implemented in

the network. This evaluation can be scored and weighted to establish policy baselines. Such evaluations and scoring are invaluable in setting up a baseline and subsequent updates for trend analysis, reporting, and in a continuous improvement process. Issues, such as calculating the impact of a planned policy change or deciding which policy improvement to be carried out next, can use this analysis in a very meaningful manner. An issue related to security policy is the network quality in terms of industry standards and practices or perhaps as compared to industry peers. Evaluations of policy controls, like Athena's, make possible such comparisons.

Athena uses the calculated network policy data to evaluate and enforce corporate and regulatory security policy. Let us take a simple example of security policy and its evaluation *vis a vis* network policy. Consider the security policy on VOIP, which may be to segregate VOIP data from other data in the network. Given the network policy computation above, Athena can evaluate if indeed VOIP data is segregated from the rest of the data. Indeed, it can go further and, in tandem with the above, also calculate that inbound VOIP traffic is allowed from a specific external source, or that network policies do not restrict traffic to only VOIP enabled devices in the network. This may be deliberate policy introduced in order to support business process or it may be inadvertent policy implementation that needs to be remediated. In the former, an element of risk has been introduced.

"Examples of legislative and regulatory frameworks include SOX, GLBA, COBIT, ISO, FFEIC, AICPA, etc. Security policy must be in compliance with these standards…"

Defense in depth is another design principle used in network security policy. Basically it specifies that a layered system of defenses be established so that the network as a whole does not succumb to a single attack. High value corporate assets should be situated at the core of the network. Athena can be used to analyze, and subsequently design, network topologies to identify the layers involved in such a defense. Athena also provides support for threat simulation, whereby threats can be evaluated not only in terms of their primary impact, i.e. the sub-network and hosts that can be compromised, but also in terms of a staged attack, whereby the compromised hosts can be used to mount an attack on other network hosts, and so on until high value sub-networks risk compromise. It should be noted that all such analysis is done off-line, without injecting any test data packets into the active network.

Public and private enterprises face a host of legislative, regulatory or IT control frameworks compliance requirements, a significant number of which apply to network security. Examples of legislative and regulatory frameworks include SOX, GLBA, COBIT, ISO, FFEIC, AICPA, etc. Security policy must be in compliance with these standards, which often resolves into individual policy statements cross referencing line items in the standards. Athena can evaluate security policy statements and reference it to individual line items in compliance standards.

Aiding Security Management Processes

Many enterprises have set up security management processes for handling day-to-day issues related to security. These processes are tasked to handle change management and remediation in a manner that does not disrupt company processes, while ensuring that the changes do not introduce new vulnerabilities. Today these processes suffer from the same information deficit regarding the network; hence decisions need to be taken without the assurance that it will not worsen network security. Athena, with its complete enunciation of network policies, is well positioned to remedy this situation.

Athena is capable of a wide variety of hypothesis testing, wherein various change scenarios can be quantitatively evaluated at the network policy level (will the change block any existing communication path that we want to keep open?) and at the security policy level (will the change increase the vulnerability of the network to attacks or is a regulatory compliance line item being violated). It can also compare policies set at an earlier date with the current policy in order to track additional changes in network policy that may result from the new policies.

About The Author

David is a founding partner of Lisle Technology Partners and has been a technology entrepreneur for over 25 years, having formed and developed multiple successful technology start-ups. As a LisleTech partner, David does strategic business and software development consulting for early stage and start-up technology companies, preparing them for successful venture capital funding and product launching.

Previously, he was a founder and CTO of Athena Security, Inc., which was acquired by Solarwinds (NYSE:SWI) in August 2012. At Athena, he developed innovative technology to help organizations analyze existing network security policy and enable a policy-driven approach to govern and execute changes to network perimeter security configurations. David has been passionate about security since the early '90s when he founded and operated an ISP in Chicago and defended it against malicious hackers.

For more information about this topic, please contact:

Lisle Technology Partners, LLC
650 Warrenville Road
Lisle, IL 60532
Phone: 630-629-0600
FAX: 630-629-2429
Web: http://www.lisletech.com
Email: info@lisletech.com

For more papers from Lisle Technology Partners, see http://www.lisletech.com/whitepapers.html