International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.054 ISSN: 2581-4621

The Network Management Appliance

Dr.Koshidgewar Bhasker G
H.O.D (Computer Science), Vai. Dhunda Maharaj Deglurkar College, Degloor, Dt. Nanded (M.S)- INDIA
ORCID ID -0000-0003-3747-0420

***Abstract*—** Network and computer systems have become a critical asset to all organizations. These complex networks must connect several different hardware, software and data platforms seamlessly. This complexity makes it difficult to reliably manage and secure the network and its attached systems while maintaining availability to authorized users. Traditional approaches including the use of VLANs, ACLs, firewalls, and proxies are complicated and make it hard to maintain consistent control across the enterprise. Several tools have been developed to help administrators audit and configure these devices. Despite these efforts, networks still remain unsecure and difficult to manage. This paper looks at a radical new centralized approach to network management called Ethane. Ethane provides direct control over the policy for the entire network by exploiting the capabilities of dumb switches connected to a central controller. An easily readable policy language allows network rules to be explicitly defined. Once we describe how the transport layer is secured, we'll look at how Ethane can be combined with virtualization techniques to provide a thorough defense through all system layers. The system not only blocks malicious traffic, it allows users and administrators to view the system as an organizational appliance.

Keywords-centralized management; natural policy language; network management; security; virtualization;

I. INTRODUCTION

Network and computer systems have become a critical asset to educational, commercial, government, and military organizations. These networks and computer systems have become quite complicated as they connect numerous types of hardware, operating systems and software to support many different types of users with varying levels of responsibilities and access to the system. This complexity makes it difficult to reliably secure the network and its attached systems while maintaining availability to authorized users. Network management not only encompasses managing the transport infrastructure (the network), but also its attached systems [1]. One important facet of network management, network security, has garnered a lot of attention in recent years as attacks cause more and more problems for companies. Today, large commercial organizations spend around 20% of their IT budget on security [2] while military officials describe the threat of a network intrusion as one thing keeping them up at night [3].

With the importance of the management and security of the network so clear, it is not surprising there are numerous methodologies and products available to assist the network administrator exert control over their network. One approach, called Ethane [4] [5], takes a centralized approach to manage network traffic. Ethane solves the problem of having many differing rule sets distributed across the enterprise with varying scopes to the point it is unclear if a network flow should be allowed. Under Ethane, each switch is extremely simple and falls under the control of a centralized controller that is responsible for deciding if traffic is allowed based on the network's policy written using the proprietary language FSL. FSL defines, nouns, representing users and other network objects, conditions, that constrain how these nouns operate, and actions (such as allow) to take when the condition is met. The rules on a central controller allow an administrator to quickly change policy and ensure it is implemented over the whole network without exception. Controlling the flow of traffic over the network is vital to its overall security and efficiency.

As an example, pretend a host on the network wants to connect to a web server on the same network. When the host first generates a request to connect to the web server, the switch sees the

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.054 ISSN: 2581-4621

traffic as an unidentified flow and forwards the traffic to the controller. The controller checks the network policy and determines if the flow is authorized. In this case, the controller grants permission and forwards the packet back to the switch with instructions on what path to route all subsequent packets within that flow. The remainder of the traffic in this exchange does not pass through the controller because the ingress switch and all other switches in the path to the web server have a flow entry, provided by the controller, instructing how to handle the traffic. The switches will maintain this flow is allowed until permission is revoked by the controller or the absence of traffic causes the flow entry to timeout.

In addition to the advantage of having a central management point for network policy, we see several other advantages in this design. First, it is very easy for Ethane to record the source, path, and destination for all traffic on the network. Because all traffic is first routed through the controller, including logon and address request, it is easy to tie traffic to a specific user, on a specific machine, connected to a specific switch. Second, Ethane is aware of the complete network topology and controls the path of traffic. This means specific flows of traffic can be flowed over explicit network paths depending on their sensitivity and priority. Lastly, and arguably most importantly, we see that Ethane is backwards compatible with existing networks hardware and topology. Ethane switches are regular switches with modified firmware to allow them to communicate and make routing decisions based on instructions from the controller. All header information needed by a regular switch is left intact, allowing an Ethane switch to co-exist on the same network with a regular switch.

While Ethane has several advantages, and has proven its viability in an operational 300 host network, it is still susceptible to some common network attacks like spoofing or bandwidth exhaustion [5]. Ethane only addresses half of the network management/security problem: what to do with traffic once it's on the network. Ethane does nothing to prevent hosts from generating nefarious traffic in the first place. In the next section we'll review work related to Ethane and securing network traffic. Afterwards we'll look at how we can combine the techniques used by Ethane with other technologies to further secure the network. We'll then discus the limitations of this new approach and conclude the paper.

II. RELATED WORK

The conventional approach to handling network management has been to setup the routing algorithms, firewalls, and proxy servers according to industry best practices and manufactures recommendations for the services you wish to support. Most companies claim this configuration information is well defined and recorded in some company document; however research often refutes these claims. The problem is numerous manufactures and pieces of hardware are all configured differently and at different points of the networks evolution. Such inconsistency often leads to rule holes and redundancies. One researcher [6] took the rule sets of 37 firewalls and analyzed them for common errors that were against industry practices and manufacturer recommendations. Errors, such as allowing insecure firewall management and allowing any service on an inbound rule were present in nearly 80% of the firewalls.

As a result the research developed AlgoSec, a tool that analyzes the access control devices on a network for these common configuration errors. The need for this tool exhibits the central strength of an Ethane network: policy is not spread across multiple devices, but instead lies in one place. AlgoSec has the burden of having to learn how to communicate and interpret rules for each device it supports. The large number of sources and formats creates a large opportunity for errors. When errors are inevitably found, the configuration must be changed on a large number of devices. While such an auditing tool may be useful on an Ethane network for audits, it would only have to analyze the controller and understand one language, FSL. Should a problem be found, the fix is implemented in one place.

Other research [7] [8] ignored the security-specific aspect of network devices altogether in a bid to understand the path of network traffic in general. The researchers analyzed over 8,000

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.054 ISSN: 2581-4621

configuration files of various networks to build graphs of the routing paths. It is important to know how traffic flows on a network so you can provide the security and service that traffic deserves. This is difficult to do in a typical network where each section may be left to decide its own best path. This also makes it difficult to audit the path a specific packet of traffic flow traversed for troubleshooting or security reasons. In contrast, Ethane handles network paths explicitly, allowing the controller to specify every node along the path. Should a link go offline or a new link come online, the change in network path is not changed until the controller explicitly plots a new path for the traffic. Such a system makes tracing traffic paths as simple as looking in the audit log of the controller.

The centralized approach to network management is not a new idea. Research like the Clean Slate 4D approach also advocates centralizing network decision making [9]. In this approach, the researches define four planes: decision, dissemination, discovery, and data that are used to manage a network. The idea is to replace control protocols like OPSF, IS-IS, and EIGRP with one standard protocol that runs on a central manager. They argue this simplifies the network management and increases the scalability and clarity of the network. This allows administrators to better specify the service that is given to flows of traffic by allowing them to specify the service directly, rather than create the service environment by manipulating settings on many different devices. The research only outlines principles such a network would operate on and doesn't define any protocols or specific methods to implement the idea. Ethane embraces many of these ideas and practically demonstrates such a network has potential in the enterprise environment.

Research closely resembling the architecture of Ethane called SANE, also advocates a centralized management approach [10]. However, SANE advocates a clean slate approach where many common services like DNS are replaced by SANE services. This offers the advantage of being able to design a network to the exact needs of an organization at the expense of quick migration from the network's current status. Another major difference in this approach is the requirement to explicitly publish services in a SANE network, so they can be advertized to hosts. Ethane, on the other hand, relies on typical network service advertising and only controls the connection to those services.

III. SOLUTION

Ethane and similar techniques only address half of the network security problem: what to do with traffic once it exists on the network. They remain vulnerable to malicious logic that takes advantage of a previously authorized flow—perhaps by attempting to consume all available bandwidth or tunnel undesirable traffic. These vulnerabilities are hard to overcome using an approach to security that only focuses on the transport medium and not the entire system down to individual hosts. I propose a solution that pairs a centrally managed transport system, like Ethane, that connects users to a centrally managed virtual host system. This allows us to limit user's ability to generate malicious traffic, by limiting what they have access to on the host system. Any traffic that is not generated by this central host system is then easily identified and dropped by rules on the centrally managed transport system.

Many organizations try to maintain control over their individual hosts through the use of standard disk images, group policy, and other administrative controls. Over time, the standardization obtained through such techniques gradually fades due to inconsistent software updates, unsuccessful configuration changes and user input. These variances can introduce vulnerabilities and malicious logic onto the network. Often times the failure cannot be traced back to a single source do to the exploit corrupting the evidence, intentionally or by happenstance. For this reason, I view it as a necessity to refresh the host provided to the user each time the user accesses the system. In the system, hosts are virtual machines served off a virtualization server to a user. That is to say a virtualization service, like Citrix or VMware View, provides the host to the user via a software

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.054 ISSN: 2581-4621

client. This means the user can join the network with any device capable or running the software client. Let's look at an example to further define the points I've made.

Sarah arrives at work with a laptop loaded with the system's software client installed. Any traffic from the laptop is sent to the Ethane controller as an unidentified flow. Ethane denies all traffic from the laptop except that generated by the virtualization client (qualified by port number for this example). Ethan allows traffic from Sarah's virtualization client to talk to the virtualization server. The virtual server provides a basic authentication challenge that forces Sarah to enter a username/password. Once verified, the server logs her session has begun and sets up Sarah's virtual machine based on her assigned disk image, access level, and settings. It is important to note here that Sarah's laptop and virtualization client only allow her basic input and output like keyboard, mouse, monitor, sound, etc. All processing, storage, and network connectivity (from the virtual machine) is provided on the server's side. When the virtual machine generates request for network resources, the request emanates from the virtual server, not Sarah's laptop. These requests are sent through the Ethane controller and are allowed because the controller is configured to permit traffic to flow from the virtualization server to other network servers. As a result, Sarah can only access the network from her laptop through the virtualization client. The only services she is able to access are those available from her desktop image.

By combining these two paradigms, we've created a very secure system that has some advantages over Ethane alone. The first advantage is we've significantly limited the possible source/destination pairs for traffic on the network. User machines are only allowed to talk to the virtualization server via their virtualization client and the virtualization server is the only device allowed to talk to other servers. This well defined network pattern allows the administrator to easily anticipate and plan for network load. More money can be spent to the greatest effect. Such traffic patterns also eliminate the possibility for the end user's machine (Sarah's laptop in the above scenario), from tunneling any illegitimate data through the network because all traffic flows toward the virtualization server and will not be relayed if misunderstood. The virtual images allow software vulnerabilities, updates, and configuration to be fixed on one image vs. hundreds of machines. In essence, the network becomes an appliance to the user, allowing them access to a well-defined set of applications and services and nothing else.

IV. CONCLUSION

Today's networks and computer systems have become quite complicated as they connect numerous types of hardware, operating systems and software to support many different types of users with varying levels of responsibilities and access to the system. This complexity makes it difficult to reliably secure the network and its attached systems while maintaining availability to authorized users. I propose the centralized management of transport and host systems is the answer to this problem. Centralized management allows policy to be made and maintained with greater accuracy across the enterprise without exception. Unfortunately limitations and caveats do exist. The most glaring is the system I've outlined has never been tried in practice. The main components, desktop virtualization, and Ethane have been proven separately, but not in concert together. The lack of a tangible deployment mean there are several gaps in the specifics needed to make this idea a reality. My goal is to provide the template for deployments in the future, and allow other researchers to explore specific implementation strategies.

The method also suffers the draw backs of its component methods. For example, much research is to be done on how to replicate and accommodate the failure of one or more controllers in a centrally managed system like Ethane. Virtualization faces similar challenges as well as some that impact the experience of the end user. For example, some applications, like multimedia content creation and CAD/CAM software, are not easily virtualized. While progress has been made over recent years, many would argue not enough to do away with dedicated machines to run theses tasks. These exceptions complicate a policy we've gone through great strides to simplify. Finally, most

DOI:10.46647/ijetms.2023.v07i01.054 ISSN: 2581-4621

organizations simply do not like being the guinea pig for new technologies. This will make it hard to find networks willing to try the new methods, particularly because the new solution is not quickly adapted to existing networks.

REFERENCES

[1] M. Subramanian, Network management Principles and Practice. Boston: Addison Wesley, 2006, pp. 35-36.
[2] J Leyden, "Security spending soars." The Register [Online] October 11, 2007. [Cited: March 20, 2010] http://www.theregister.co.uk/2007/10/11/comptia_security_survey/.
[3] U.S. Department of Defense**,** "Cybersecurity Seizes More Attention, Budget Dollars." in Defence Talk. [Online] February 8, 2010. [Cited: March 23, 2010.] http://www.defencetalk.com/network-security-budget-dollars-24057/.
[4] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker, "Ethane: Taking control of the enterprise," in Proc. SIGCOMM, Kyoto, Japan, Aug. 2007, pp. 1-12.
[5] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker, 2009. Rethinking enterprise network control. IEEE/ACM Trans. Netw. 17, 4 (Aug. 2009), 1270-1283..
[6] A. Wool, "A quantitative study of firewall configuration errors," Computer, vol. 37, no. 6, pp. 62–67, 2004.
[7] G. Xie, J. Zhan, D. A. Maltz, H. Zhang, A. Greenberg, and G. Hjalmtysson, "Routing design in operational networks: A look from the inside," in Proc. SIGCOMM, Sep. 2004, pp. 27–40.
[8] D. Caldwell, A. Gilbert, J. Gottlieb, A. Greenberg, G. Hjalmtysson, and J. Rexford, "The cutting edge of IP router configuration," Comput. Commun. Rev., vol. 34, no. 1, pp. 21–26, 2004.
[9] A. Greenberg, G. Hjalmtysson, D. A. Maltz, A. Myers, J. Rexford, G. Xie, H. Yan, J. Zhan, and H. Zhang, "A clean slate 4D approach to network control and management," Comput. Commun. Rev., vol. 35, no. 5, pp. 41–54, Oct. 2005.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.
[10] M. Casado, T. Garfinkel, A. Akella, M. J. Freedman, D. Boneh, N. McKeown, and S. Shenker, "SANE: A protection architecture for enterprise networks," in Proc. USENIX Security Symp., Aug. 2006, vol. 15, Article No. 10.