SECURITY AND NETWORK MANAGEMENT

Saranya J,
Assistant Professor,
Department of Computer Science,
Sri Krishna Adithya College of Arts and Science,
Kovaipudhur, Coimbatore, India.

Vaishnavi A.B,
B.Sc., (Information Technology),
Department of Computer Science,
Sri Krishna Adithya College of Arts and Science,
Kovaipudhur, Coimbatore, India.

Anusha Mary Sunny Thomas,
B.Sc., (Information Technology),
Department of Computer Science,
Sri Krishna Adithya College of Arts and Science,
Kovaipudhur, Coimbatore, India.

Abstract: Network management is challenging. To operate maintain and secure a communication network, network operators must grapple with low level vendor specific configuration to implement complex high level network policies. Despite many previous proposals to make network easier to manage, many solutions to network management problems amount to stop gap solutions because of the difficulty of changing the underlying infrastructure .A new paradigm in networking, software defined networking (SDN)advocates separating the data plane and the control plane, making network switches in a data plane simple packet forwarding devices and leaving a logically centralized software program to control the behaviour of the entire network.

Keywords: Network, Security Managements, Attacks

I.INTRODUCTION

Network security has become synonymous with complex network architecture, administrative nightmares and increased threat exposure. Myriad security point deployments, diverse management consoles, and complex and outdated security policies spread across multiple rule bases make effective network management and good visibility into network traffic nearly impossible.

Network security management empowers you with easy to implement, consolidated policy creation and management. Set up and control firewalls centrally with industry-leading functionality and efficient rule base and gain insight into network-wide threats while correlating information across your entire network .Today's sophisticated and multidimensional cyber attacks call for complex countermeasures. Many security solutions are limited in scope and offer no integration with other solutions. Security teams need to manage multiply security deployments, and an overwhelming amount of network data ,with very limited resources.

II.SECURITY MANAGEMENT

Today's IT security team are faced with rapidly mutating threads at every possible point of entry-from the perimeter to the desktop from mobile to the cloud. Fuelled by the past evolution of the thread landscape and changes and network and security architectures, network security managements far more challenging and complex than just a few hours ago.

Security terms must support internal and external complains mandates, enable new service, optimise performance, ensure availability and support the ability to troubleshoot efficiently on demand-with no room for error. That's a lot to balance when managing network security.

Here are four essential bet practices for network security management.

1. **Network security management requires macro view:** organization need a holistic view of their network with disparate vendor devices and hosts, security teams need a normalized ,comprehensation view of the network with including: routing rules ,access rules ,NAT, VPN, etc, .hosts, including all products (and versions),services, vulnerabilities and patches and asserts, including assert groupings and classifications. With a comprehensive view of the network, security teams can view host in the network ,as well as configurations, classifications and other pertinent information. A network map or model is a both useful visualization tool under diagonal tool providing analyses that is the only possible when considering an overall view. Eg: Security and complains teams can use this macro view to see how data would move between points on the network.

   Additionally ,it highlights information that is missing, such as host access control list(ACL)data and more. Sophisticated analytics can be conducted quickly and accurately in a model based environment, without disrupting the live network. Access path analyses helps to validate changes and can troubleshoot outages or connectivity issues, enhancing visibility and improving security process. "what-if" analyses indicates both accessible and blocked destinations for designed data.

2. **Daily device management requires an micro view:** Although the macro view is needed to see how all the pieces of the network fit together ,network administrators must also be able to drill down in the details for a particular device, easily accessing information on rules, access policies and configuration complains.amd this information must be consider within the frame work of the border network, including context such as segments or zones, routing, routers, switches, intrusion prevention system(IPS),and firewalls.

   Information must be provided in a digestible fashion. The network components that impact the device will undoubtedly come from various vendors, creating data of different vendor languages that must be deciphered, correlated, and optimized to allow administrators to stream line rule sets. Eg: administrators need to be able to block are limit access by application and view violations of this access policies.

   Daily or weekly reviews of all devices on the network is unattainable with a manual process, and reviewing device configuration less frequently puts network security and complains at risk. Automating policy complains helps ensure complains and constituency, and preserves IT resources. Ideally, a networking modelling tool that provides a macro view should also allow administrators drill into a micro view of each device, providing information on users, applications, vulnerabilities, and more. This allows administrators to see the boarder network view and then focus in on a particular devices for management.

3. **Simulate attacks for context-aware risk assessment :**Merely knowing the network vulnerabilities and their criticality is insufficient for understanding the true level of risk to an organization. Today's attacks of an incorporate multiple steps that cross several different networks zones, and an isolated view of any of this steps could appear innocuous.

   Attack simulation technology automatically looks at the holistic network –business assets ,known threats and vulnerabilities-and identifies what would happen if the condition were combined. Attacks simulation can also evaluate potential options to block an attack to providing intelligence for decision support. Understanding the like hood of an attack and its potential impact against valuable targets is the key to assessing which vulnerabilities and threats post to the most risk.

   Attack simulation looks at network context asset critically, business metrics and existing security controls when determining the impact of a potential attack. Eg: If an asset runs an application that is crucial to maintain the business and require continuous availability the level vulnerability that threatens to disable this asset might be high level risk to this particular business.

   The impact of developing a particular security control must also be considered keeping an IPS continually on active mode can impact network performance. Attack simulation tools enable security tools to the target use of their IPS protection, activation ally necessary signatures ,maximizing performance, and prioritizing vulnerabilities.

4. **Secure change management is critical:** once a network is in complains, a secure change management process is needed to maintain continuous complains and validate that planned changes do not introduce new risk. Secure change management incorporates risk assessment in orchestrated, standardised process, flags changes outside of this structure, allows administrators to reconcern flagged changes and troubleshoots where need. Secure change management verifies that changes were implemented and intended, identifies when a change has un intended consequences, and highlights unapproved changes.

   Eg: A change management process can flag when a network change expose vulnerabilities, when a fire wall change open access to risky services, or when there is an unauthorised access path from a partner to an internal zone. More importantly, to maintain network security, change management processors can be used to determine the impact of a proposed change before implementing the change.

   Implanting this four best practices for network security management can reduce risk across the network. With visibility on both the network and device level, tremendous amounts of data are translated into intelligence into deciphers complicated network security transactions into manageable, actionable information. With this insight, attack simulation can then prioritize vulnerabilities and eliminate the vectors hat are most critical to the organization, protecting business services and data. Finally, change management can automate and optimize security processors to improve security and reduce the security work load.

   A network management system (NMS) is a set of hard ware and\or software tools that allow an IT professional to supervise the individual components of a network within a larger network management frame work.

Network management system components assist with:

- Network device discovery-identifying that devices are present on a network.
- Network device monitoring-monitoring at the device level to determine the health of network components and the extent to which their performance matches capacity plans and intra – enterprise service level agreements(SLAs)
- Network performance analyses-tracking performance indicators such as band width utilization, packet loss ,latency availability and uptime of routers, switches and other simple network management protocol(SNMP)-enabled services.
- Intelligent notifications-configurable alerts that will respond to specific network sceneries by paging, e-mailing, calling o texting a network administrator.

III.CONCLUSION

Security teams need to manage multiply security deployments, and an overwhelming amount of network data , with very limited resources. Network security management empowers you with easy to implement, consolidated policy creation and management.

IV.REFERENCES

[1]. *https://en.wikipedia.org/wiki/**Network_security***

[2]. www.interhack.net/pubs/**network-security**

[3]. https://en.wikipedia.org/wiki/Book:**Network_Security_and_Management**