



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

Comparison of Static Policy Enforcement Techniques of NAC

Shalvi Dave¹, Bhushan Trivedi², Jimit Mahadevia³

¹Indus University, ²GLS ICT, ³Cyberoam Pvt. Ltd.

Ahmedabad, Gujarat, India

Abstract: To secure any network today, prominent techniques used are firewalls, IDS, IPS and vulnerability assessment. To unify all these endpoint security methods, NAC is used. Network Access Control aims to do exactly what the name implies—control access to a network with policies, including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do.

In this paper, we have first described all the static enforcement policies of NAC. Then a detailed comparison is shown between all the static policies with their advantages and disadvantages. The main aim of this comparative study is to provide a security system, which can identify threats after the host is authorized and authenticated in the network. Such dynamic access prevention requires detection based on anomalies rather than static NAC policies. Techniques such as VLAN Steering can then be used for dynamic access prevention.

Keywords: VLAN Steering, Static NAC, Network access control

I. Introduction

Implementing secure network has become an increasingly serious problem. To secure the data on network there are different methods and architecture which are used. NAC (Network Admission Control) is application access control. Before NAC, authentication is only way to determining the packet is allow in network or not. NAC is mainly used for role based access [2]. Its combines user authentication, end-point security assessment, and access control. As compared to this, firewall provides access control but it only knows monitors and filters the traffic based on the IP address. NAC differs from firewall because it is focused on the host and provides security policy on host identity.

NAC is a set of technologies and defined processes, whose aim is to control access to the network allowing only authorized and compliant host to access and operate on a network. NAC is described in two ways: Static and Dynamic. The static policy is also called Network Admission Control. The term admission refers to policy enforcement at the time of configuring a host in the network with a valid IP after successful authentication and authorization. This is done using a set of pre-defined rules or signatures.

Network Admission control implements a static policy implementation, which is achieved using:

- Host Assessment
- Validation
- Enforcement

Host assessment is a fundamental part of determining the state of a host and the kind of access it should be allowed. For Host Assessment, NAC uses either Agent-Based system or Agent-Less system. NAC provides the above endpoint assessment capabilities to determine the security posture of connecting devices.

HOST ASSESSMENT: AGENT-BASED

The agent-based capability requires the installation of a software agent on the end system. Host assessment using agent-based system can be done by either using persistent agent or dissolvable agent. In both the cases, the assessment is generally performed by the agent, rather than offloaded to other sources.

HOST ASSESSMENT: AGENT-LESS

The agent-less capability does not require the installation of a software security agent on the end system and is typically used for end systems such as guest PCs. Agent-less assessment scans for operating system and application vulnerabilities. An example of agent-less system uses Remote Procedure Call[1]. A server on the network runs scans using RPC or WMI on the target computer. The server needs the host's administrator credentials to run the scan, as well as access to the host. Another example is vulnerability scan where a server performs a vulnerability-assessment scan on the host. The VA scans attempts to identify the OS, services running and any vulnerability.

POLICY ENFORCEMENT

After successful host assessment and validation, NAC implements static policy enforcement. Static policy enforcement is only performed for in-band NAC which is also known as pre-connect policy enforcement.

Pre-connect mechanisms are applied before an endpoint is allowed to join the network and to send and receive traffic. Endpoint compliance posture checking and user authentication are examples of pre-connect mechanisms. Based on the posture status and user identity, a decision can be made as to whether to allow the endpoint to access the network at all. Certain parts of the network may be off-limits to, if even visible at all by, unauthorized clients. Traffic anomaly detection, intrusion detection using threat signatures, and activity monitoring are examples of post-connect mechanisms [3].

In this paper, I present various NAC static policy enforcement methods used for successful intrusion detection. Then a detailed comparison is done for all the static enforcement methods.

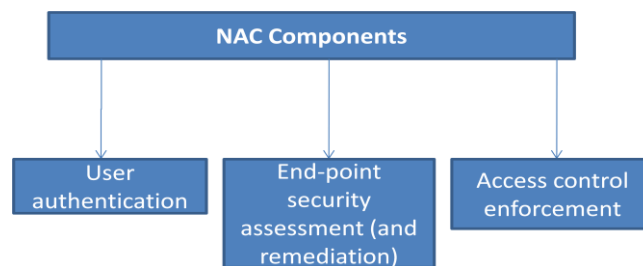
II. RELATED WORK

NAC is the open-architecture and standards-based approach for admission or access control. Lots of research has been done to implement a secure network like client data protection, AAA, Managed and unmanaged device and Intrusion Detection [4]. The application access control (NAC) is very simple and less complex technology compare to other technologies because it is Role based Access which use policies for host. The policies are either static or dynamic such as 802.1x, DHCP, ARP management, VLAN Steering. Almost all IDS/IPS use static policy enforcement techniques using signature based or rule-based detection.

III. Static policy enforcement methods for Intrusion detection

There are various static methods used to implement admission control. NAC have three main basic component such as user authentication, End Point Security Assessment and Access Control Enforcement.

Basic NAC Component



POLICY ENFORCEMENT

Policy enforcement is done in many ways. It is the duty of network administrator or a security manager to choose a method that should be applied. Enforcement is performed at two stages: Layer2 or Layer 3.

Layer 3:

- Creates isolated shared islands (subnets).
- Quarantine of an element is done using ip route.
- Some methods detect the elements on Layer3 only like DHCP

Layer 2:

- Manipulating ARP tables.
- Some elements may only generate Layer 2 Traffic
- Appliances will need to be plugged into switches in each layer 2 switch domain (to provide a server in the authentication VLANs for endpoint compliance checks and user login)

Enforcement at any layer requires specialized software also known as agent software.

The most commonly used NAC Enforcement Methods are:

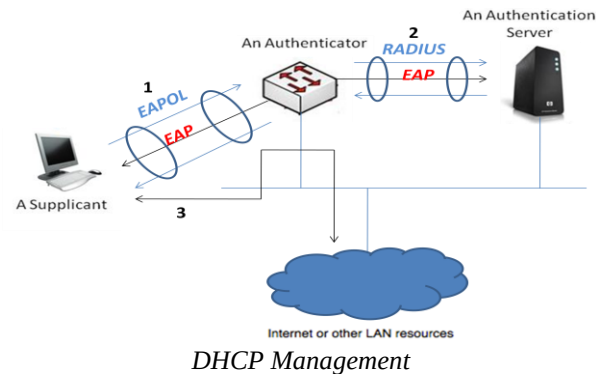
802.1x:

The most secure authentication method for NAC is based on 802.1X, the IEEE standard for authentication over local area networks. In an 802.1X environment, the user's device is not connected to the network – wired or wireless until the authentication is successful. Without authentication, the user doesn't get an IP address, can't sniff traffic, and certainly can't attack anyone or anything else on the network [2]. 802.1X authentication involves three parties:

A Supplicant: The supplicant is a client device (such as a laptop). Which provides credentials to the authenticator.

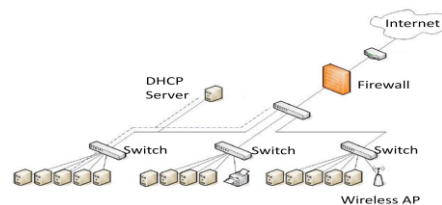
The Authenticator: It is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols. The authenticator acts like a security guard to a protected network.

An Authentication Server: Information is got by Authenticator its forward to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.



The **Dynamic Host Configuration Protocol (DHCP)** is an auto configuration protocol used on IP networks. Computers that are connected to IP networks must be configured before they can communicate with other computers on the network. DHCP is a protocol used by networked devices (clients) to obtain various parameters necessary for the clients to operate in an Internet Protocol (IP) network. By using this protocol, system administration workload greatly decreases, and devices can be added to the network with minimal or no manual configurations.

- DHCP allows a computer to be configured automatically
- Eliminating the need for intervention by a network administrator

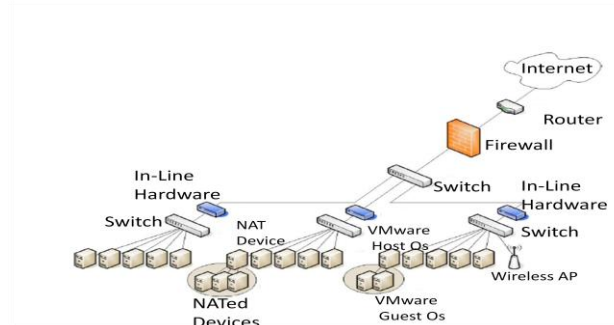


FILTERING USING DHCP

DHCP Filtering is used as a security measure against unauthorized DHCP servers. A known attack can occur when an unauthorized DHCP server responds to a client that is requesting an IP address. The unauthorized server can configure the gateway for the client to be equal to the IP address of the server. At that point, the client sends all of its IP traffic destined to other networks to the unauthorized machine, giving the attacker the possibility of filtering traffic for passwords or employing a 'man-in-the-middle' attack.

INLINE BLOCK

An in-line device must think about traffic shaping, catching attack command-and-control sequences, and detecting inappropriate user access. In-line NAC puts an appliance as a bump in the wire, usually between the access switch and the distribution switch. Each NAC Server only operates in one of those two modes. When in-line, the NAC Appliance filters user traffic, applies access control policies, and checks endpoint security status. The benefit of in-line NAC is that if no other enforcement method is available, in-line blocking is still an option.



ARP MANAGEMENT

ARP Management is also called “ARP spoofing” or “man-in-the-middle.” The Address Resolution Protocol is used to tell other hosts which IP addresses are assigned to a MAC address. These assignments are held in an ARP table on each host and updated periodically. This method manages a host’s ARP table by dynamically sending ARP tables with different IP-to-MAC mappings.

WALLED GARDEN

ARP maps IP address to MAC addresses. Similarly, DNS maps host names to IP addresses. Wildcard DNS will respond to any DNS query with an IP address, effectively redirecting hosts to a specific server.

IV. COMPARISON OF NAC ENFORCEMENT METHODS

All the static NAC enforcement methods have different characteristics. For example DHCP is detects threats at Layer 3 and some other methods work on Layer 2. Filtering of traffic is done in different ways by all the methods. The methods are using the combination of network access device and the software which is either agent based or agent less. In static method the detection of element or attack is checked by pre-defined policy [1]. Some methods which are using same features like DHCP and ARP management, works with any host that uses DNS. 802.1x is authentication based method which is implementing protocols such as RADIUS and EAP. The following table shows a detailed comparison of each static policy used by NAC:

Methods	PROS	CONS
802.1x	- Highest security standards and authentication based Multiprotocol. - In 802.1x Authentication and authorization occurs before a host even accesses the network. Multiple authentication schemes are supported, and 802.1X is designed to be extensible as new technology arrives. - Centralized administration, Good scalability, Real time detection, High level of security this are characteristics of 802.1x - Very familiar model to end-users ,broadest platform support, handles - Guest user best. - Hosts that do not support 802.1x can be granted access to the network using manually configured exception by MAC address. - Implementing RADIUS and EAP protocol	- For compliance check must use an agent software - Some times its difficult or complex to deploy - All elements on the network must be configured to use 802.1x - Difficult manageability. Not all of networking element can support 802.1x and Not all of the elements residing on the network are 802.1x capable (AS-400, Printers etc.) - It is possible to spoof the MAC address of an exception element is order to receive the same access that element has to enterprise network. - The cost for implementing a solution which is based on 802.1x is currently HIGH (time, resources, infrastructure, upgrade, etc.)
DHCP	- DHCP is easy to install and configure. Because DHCP is well supported, it will work with any host that uses DHCP to request an IP address. - Easy to intercept requests for IP assignment. - Fewer devices are required because it only needs to be in-line with the DHCP server. - It is Easy and fast to deploy.	- Control is easily bypassed by devices assigning a static IP. - Detected elements are only those using DHCP. - Won’t catch devices behind a NAT device (i.e. routing WAP). - Detection of elements is done at Layer 3 only. - An element can connect to the network without being detected. Access to at least the local subnet will not be restricted
ARP	ARP is used in any IP host and will always work without any configuration changes to hosts.	Cannot solve the problem of network traffic.
Inline Block	- An in-line device checks traffic shaping and catch attack. - Elements detection is performed at layer 3.	- Deployment is time consuming. Deployment must involve a network re-architecture. - Some elements may only generate layer 2 traffic. Elements can infect and entering on their local subnet and cannot be stopped. Elements detection is checked only at layer 3.
Walled Garden	Like DHCP and ARP management, this method works with any host that uses DNS. Often, the user ends up at a Web page, where he has to authenticate or accept an agreement. Relies on the fact that users will eventually use a Web browser and thus be redirected to a Web page.	Not widely used.

V CONCLUSION

All the NAC policy enforcement methods described above only provides threat management statically during the time of host admission. After a host is successfully given network access, if there is any threat, it cannot be detected using static methods. After successful host admission, intrusion can be detected by traffic monitoring. This is possible using IDS logged data as evidence and using anomaly based detection with VLAN Steering to detect threat dynamically and put the infected host in quarantine area. The key to successful policy

implementation lies in combining IDS logged data with IPS and prevent attacks before they occur in the network.

The above study of static enforcement methods was carried out basically as a pre-requisite to understand the need for dynamic access control. From the above mentioned methods, the most popular methods used are 802.1x and DHCP. For simplicity, DHCP is the most suited policy enforcement method whereas for complex security measures 802.1x is well suited.

REFERENCES

- [1] Porras, P and Neumann P 1997. EMERALD :Event monitoring enabling responses to anomalous live disturbances.
- [2] D. Wagner and P. Soto. Mimicry Attacks on Host-Based Intrusion Detection Systems. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 255–264, Washington DC, USA, Nov2002.
- [3] Zamboni, D and Spafford, E 1999. New directions for the AAPHID architecture. In *Recent Advances in Intrusion Detection*.
- [4] Polla D, McConnel,J, Johnson T Marconi, 1998. A frame work for co-operative intrusion detection. In *Proceedings of the national conference on Computer security system*.