International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Review on Internet Usage Control Using Access Control Techniques

R. Sangeetha

Assistant Professor, Department of Information Technology, Hindusthan College of Arts and Science, Coimbatore, Tamil Nadu, India

ABSTRACT

The contact list is a group of statements. Each statement defines a pattern that would be found in an IP packet. As each packet comes through an interface with an associated access list, the list is scanned from top to bottom in the exact order that it was entered—for a pattern that matches the incoming packet. Access list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information .Cisco provides basic traffic filtering capabilities with access control lists .Access lists can be configured for all routed network protocols (IP, AppleTalk, and so on) to filter the packets of those protocols as the packets pass through a router. When creating an access list, you define criteria that are applied to each packet that is processed by the router; the router decides whether to forward or block each packet on the basis of whether or not the packet matches the criteria. Typical criteria you define in access lists are packet source addresses, packet purpose addresses, and upper-layer protocol of the packet. However, each protocol has its own specific set of criteria that can be clear. For a single access list, you can define multiple criteria in multiple, separate access list statements. Each of these statements should reference the same identifying name or number, to tie the statements to the same access list. You can have as many criteria statements as you want, limited only by the available memory. Of course, the more statements you have, the more hard it will be to comprehend and manage your access lists. Placement and understanding of the traffic flow is important to understand up front before you configure an ACL on a router interface.

Keywords : Network Traffic, Network Security, Protocols, Standard ACL, Extended ACL

I. INTRODUCTION

ACLs, known for their ability to filter traffic as it either comes into or leaves an interface, can also be used for other purposes, including restricting remote access(virtual type terminal, or VTY) to an IOS device, filtering routing information, prioritizing traffic with queuing, triggering phone calls with dial-on-demand routing(DDR), changing the administrative distance of routes, and specifying traffic to be protected by an IPSec VPN, among many others.

ACLs are basically a set of commands, grouped together by a number or name, that are used to filter traffic entering or leaving an interface. ACL commands define specifically which traffic is permitted and denied. ACLs are created in Global Configuration mode.By default, switches break up collision domains and routers break up broadcast domains.By creating virtual local area network (VLAN), broadcast domains break up in a pure switched internetwork. A VLAN is a logical group of network users and resources connected administratively defined ports on a switch. When VLANS created, It will be the ability to create smaller broadcast domains within a layer 2 switched internetworks by assigning different ports on the switch to different sub networks. A VLAN is treated like its own subnet or broadcast domain, meaning that frames broadcast onto the network are only switched between the ports logically grouped within the same VLAN.

II. III. PROBLEM DEFINITION

VLANs were initially intended to allow net- work administrators to connect a group of hosts in the same broadcast domain, independent of their physical location. However, today's enter- prise administrators use VLANs for a variety of other purposes, most notably for better scalability and flexible specification of policies. However, enterprise administrators have seen many problems of VLANs because VLANs are used for other functions they were not designed for. Understandably, VLANs are at best an incomplete solution for some of these problems. As a result, managing VLANs is one of the most challenging tasks they face.

So there are some useful motivations that motivates to use VLANs:

1)To reduce overhead by limiting the size of each broadcast domain.

2)Better security by putting sensitive devices on separate VLAN. Also making traffic special traffic separate than main.

ACLs are basically statements that are grouped together by either a name or number. Within this group of statements, when a packet is processed by an ACL, the IOS will go through certain steps in finding a match against the ACL statements. ACLs are processed top-down by the IOS. Using a top-down approach, a packet is compared to the first statement in the ACL, and if the IOS finds a match between the packet and the statement, the IOS will execute one of two actions included with the statement: permit or deny. If the IOS doesn't find a match of packet contents to the first ACL statement, the IOS will proceed to the next statement in the list, again going through the same matching process. If the second statement matches the packet contents, the IOS executes one of the two The workstations, hubs, and repeaters together form a LAN segment. A LAN segment is also known as a collision domain since collisions remain within the segment. The area within which broadcasts and multicasts are confined is called a broadcast domain or LAN. Thus a LAN can consist of one or more LAN segments. Defining broadcast and collision domains in a LAN depends on how the workstations, hubs, switches, and routers are physically connected together. This means that everyone on a LAN must be located in the same area

VLAN's offer a number of advantages over traditional LAN's. They are:

- Performance
- Formation of virtual workgroups
- Simplified administration
- Reduced cost
- Security

III. ROUTING PROTOCOL SECURITY

Routing security has received varying levels of attention over the past several years and has recently begun to attract more attention specifically around BGP on the public Internet. Despite this new attention, however, the area most open to attack is often not the Internet's BGP tables but the routing systems within your own enterprise network. An enterprise routing infrastructure can easily be attacked with MITM and other attacks designed to corrupt or change the routing tables with the following results:

- Traffic redirection—In this attack, the adversary is able to redirect traffic, enabling the attacker to modify traffic in transit or simply sniff packets.
- Traffic sent to a routing black hole—Here the attacker is able to send specific routes to null0,

effectively kicking IP addresses off of the network.

- Router DoS—Attacking the routing process can result in a crash of the router or a severe degradation of service.
- Routing protocol DoS—Similar to the attack previously described against a whole router, a routing protocol attack could be launched to stop the routing process from functioning properly.
- Unauthorized route prefix origination—This attack aims to introduce a new prefix into the route table that shouldn't be there. The attacker might do this to get a covert attack network to be routable throughout the victim network.

There are four primary attack methods for these attacks:

- Configuration modification of existing routers
- Introduction of a rogue router that participates in routing with legitimate routers
- Spoofing a valid routing protocol message or modifying a valid message in transit
- Sending of malformed or excess packets to a routing protocol process

These four attack methods can be mitigated in the following ways:

- To counter configuration modification of existing routers, you must secure the routers.
- This includes not only the configuration of the router but also the supporting systems it makes useof, such as TFTP servers. See Chapter 5, "Device Hardening," for more information.
- Anyone can attempt to introduce a rogue router, but to cause damage, the attacker needs the other routing devices to believe the information that is sent. This can most easily be blocked by adding message authentication to your routing protocol. More on this subject can be found in the next section. Additionally, the routing protocol message types can be blocked by ACLs from networks with no need to originate them.
- Message authentication can also help prevent the spoofing or modification of a valid routing protocol message. In addition, the transport layer protocol (such as TCP for BGP) can further complicate message spoofing because of the difficulty in guessing pseudorandom initial sequence numbers (assuming a remote attacker).
- Excess packets can be stopped through the use of traditional DoS mitigation techniques, which are discussed later in the chapter. Malformed packets, however, are nearly impossible to stop without the participation of the router vendor. Only through exhaustive testing and years of field use do routing protocol implementations correctly deal with most malformed messages. This is an area of computer security that needs increased attention, not just in routing protocols but in all network applications.

IV. ACCESS CONTROL LIST

An access control list (ACL) is a list of access control entries (ACE). Each ACE in an ACL identifies a trustee and specifies the access rights allowed, denied, or audited for that trustee. The security descriptor for a securable object can contain two types of ACLs: a DACL and a SACL.

A discretionary access control list (DACL) identifies the trustees that are allowed or denied access to a securable object. When a process tries to access a securable object, the system checks the ACEs in the object's DACL to determine whether to grant access to it. If the object does not have a DACL, the system grants full access to everyone. If the object's DACL has no ACEs, the system denies all attempts to access the object because the DACL does not allow any access rights.

The system checks the ACEs in sequence until it finds one or more ACEs that allow all the requested access rights, or until any of the requested access rights are denied. For more information, see How DACLs Control Access to an Object. For information about how to properly create a DACL, see Creating a DACL.

A system access control list (SACL) enables administrators to log attempts to access a secured object. Each ACE specifies the types of access attempts by a specified trustee that cause the system to generate a record in the security event log. An ACE in a SACL can generate audit records when an access attempt fails, when it succeeds, or both. For more information about SACLs, see Audit Generation and SACL Access Right.

Do not try to work directly with the contents of an ACL. To ensure that ACLs are semantically correct, use the appropriate functions to create and manipulate ACLs. For more information, see Getting Information from an ACL and Creating or Modifying an ACL.

i) SIMPLIFYING ACCESS CONTROL POLICIES

VLANs provide an effective way to enforce access control by directing inter-VLAN traffic through routers. In addition, by allowing administrators to assign related hosts to IP addresses in the same subnet, VLANs simplify access control configuration by making packet classification rules more concise.

Imposing Access Control Policies — VLANs provide a way to restrict communication between hosts. In Fig. 1, router 3 (R3) can apply access control lists (ACLs) to limit the traffic between hosts H3 and H4 that belong to different VLANs.

Concise Access Control Lists — Routers and firewalls apply ACLs based on the five-tuple of the source and destination IP addresses, the source and destination TCP/UDP port numbers, and the protocol. Wildcards enable shorter lists of rules for permitting and denying traffic, which simplifies ACL configuration and also makes efficient use of the limited high-speed memory (e.g., TCAMs) for applying the rules. VLANs enable more compact ACLs by allowing administrators to group hosts with common access control policies into a common IP subnet. For example, campus 3 identifies user machines through a small number of IP prefixes (corresponding to the faculty and student VLANs), allowing concise ACLs for traffic sent by user machines (e.g., to ensure only SMTP traffic is allowed to reach the email servers on the infra- structure VLAN).

Preventing Source IP Address Spoofing — Source IP address spoofing is a serious security problem, since spoofing allows attackers to evade detection or shift blame for their attacks to others. Assigning host addresses from a com- mon IP prefix simplifies the preventive filtering of packets with spoofed source IP addresses. Hosts in the same VLAN are assigned IP addresses from the same subnet(s). This allows network administrators to configure ACLs at the VLAN's gateway router to drop any packets with source IP addresses from other prefixes. Campus 3 does precisely that.

Supporting Quality of Service — Classifying packets based on IP prefixes applies not only to access control, but also to quality of service (QoS) policies. For example, administrators can configure a router to place IP packets in differ- ent queues (with different priority levels) based on the source or destination IP prefix, if hosts are grouped into VLANs based on their QoS requirements. None of the campuses in our study apply these kinds of QoS policies.

ii) DE-CENTRALIZING NETWORK MANAGEMENT

VLANs allow administrators to delegate some management tasks to individual departments. VLANs also simplify network troubleshooting by allowing an administrator to observe connectivity from any part of the campus simply by trunking a port to a VLAN.

iii) CONVENTIONAL LOCAL AREA NETWORKS

In a traditional local area network (LAN), hosts are connected by a network of hubs and switches. The switches cooperate to construct a spanning tree for delivering traffic. Each switch forwards Ethernet frames based on its destination MAC address. If the switch contains no forwarding-table entry for the frame's destination MAC address, the switch floods each frame over the entire spanning tree. A switch learns how to reach a MAC address by remembering the incoming link for frames sent by that MAC address and creating a mapping between the MAC address and that port.

To connect to the rest of the enterprise net- work (and the rest of the Internet), the island of Ethernet switches connects to IP routers that forward traffic to and from remote hosts. Each host interface in the LAN has an IP address from a common IP prefix (or set of prefixes). Traffic sent to an IP address in the same subnet stays within the LAN; the sending host uses the Address Resolution Protocol (ARP) to determine the MAC address associated with the destination IP address. For traffic destined to remote IP addresses, the host forwards the packets to the gateway router, which forwards packets further toward their destinations.

V. COMMUNICATION WITHIN A VLAN

Administrators use VLANs to construct network segments that behave logically like a convention- al LAN but are independent of the physical locations of the hosts; for example, hosts H1 and H3 in Fig. 1 both belong to VLAN1. As in a conventional physical LAN, the switches in a VLAN construct a spanning tree, and use flood- ing and learning to forward traffic between hosts. For example, the switches S3, S4, and S5 form a spanning tree for VLAN2.

VI. COMMUNICATION BETWEEN VLANS

Each host has an IP address from an IP prefix (or prefixes) associated with its VLAN; IP routers forward packets based on these prefixes, over paths computed in the routing protocol (e.g., Open Shortest Path First [OSPF] or Rout- ing Information Protocol [RIP]). For example, when sending traffic to H4, host H3 forwards the packets to its gateway router R2, since the destination IP address belongs to a different prefix. R2 would then look up the destination IP address to forward the packet to H4 in VLAN2. If H4 sends an IP pack- et to H1, then H4's router R3 forwards the pack- et based on the IP routing protocol toward the router announcing H1's IP prefix, and that router would then forward the packet over the spanning tree for VLAN1.

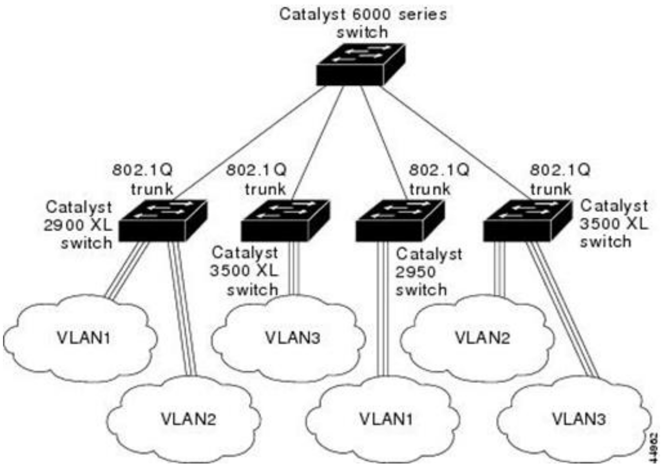

Figure 1 . Communication Between Vlans

VII. ADVANTAGES OF USING ACL

There are several advantages to using Router ACL. Create the access list before applying it to an interface (or elsewhere), because if you apply a nonexistent access list to an interface and then proceed to configure the access list, the first statement is put into effect, and the implicit deny statement that follows could cause you immediate access problems. Use the statement permit any any if you want to allow all other packets not already denied. Using the statement permit any any in effect avoids denying all other packets with the implicit deny statement at the end of an access list. Do not make your first access list entry permit any any because all traffic will get through; no packets will reach the subsequent testing. In fact, once you specify permit any any, all traffic not already denied will get through.

Although all access lists end with an implicit deny statement, we recommend use of an explicit deny statement (for example, deny ip any any). On most platforms, you can display the count of packets denied by issuing the show access-list command, thus finding out more information about who your access list is disallowing. Only packets denied by explicit deny statements are counted, which is why the explicit deny statement will yield more complete data for you. While you are creating an access list or after it is created, you might want to delete an entry.

You cannot delete an entry from a numbered access list; trying to do so will delete the entire access list. If you need to delete an entry, you need to delete the entire access list and start over. You can delete an entry from a named access list. Use the no permit or no deny command to delete the appropriate entry. In order to make the purpose of individual statements more scannable and easily understood at a glance, you can write a helpful remark before or after any statement by using the remark command.

If you want to deny access to a particular host or network and find out if someone from that network or host is attempting to gain access, include the log keyword with the corresponding deny statement so that the packets denied from that source are logged for you.

i) Cost and Time Reduction

VLANs can reduce the migration cost of stations going from one group to another. Physical reconfiguration takes time and is costly. Instead of physically moving one station to another segment or even to another switch, it is much easier and quicker to move it by using software.

ii) Creating Virtual Work Groups

VLANs can be used to create virtual work groups. For example, in a campus environment, professors working on the same project can send broadcast messages to one another without the necessity of belonging to the same department. This can reduce traffic if the multicasting capability of IP was previously used.

iii)Security

VLANs provide an extra measure of security. People belonging to the same group can send broadcast message with the guaranteed assurance that users in other groups will not receive these messages.

VIII. CONCLUSION

The use of access control lists to filter traffic within a routed network is a critical network security practice. ACL’s provide network administrators with the ability to monitor vulnerable ports and block known malicious traffic at key points within a network. The access control lists in place at the ingress and egress points of a network are a key part of the first line of defense. The filtering strategy in place at the network edges reduces many of the risks associated with direct network attacks.

Access control lists in place at the WAN and LAN level will guard against compromised or infected systems from attacking vulnerable systems on other subnets or at other sites. There should be several access control lists in the router’s configuration for use on a daily basis, or waiting to be used to block infected hosts or malicious traffic.

Network security administrators should be aware of the current vulnerabilities so that ACL’s can be updated and waiting in a router’s configuration before an actual attack begins. This practice can help isolate an attack quickly and save hundreds of man hours that would be required to battle a full scale outbreak.

IX. REFERENCES

[1]. MAdFraud: Investigating Ad Fraud in Android Applications.

[2]. Mining Personal Context-Aware Preferences for Mobile Users.

[3]. A Flexible Generative Model for Preference Aggregation.

[4]. Opinion spam and analysis. In Proceedings of the 2008 International Conference on Web Search and Networking, WSDM ’08, pages 219-230, 2008.

[5]. D. M. Blei, A. Y. Ng, and M. I. Jordan. Lantent dirichlet allocation. Journal of Machine Learning Research, pages 993-1022, 2003.

[6]. Y. Ge, H. Xiong, C. Liu, and Z.-H. Zhou. A taxi driving fraud detection system. In Proceedings of the 2011 IEEE 11th International Conference Neural Networks, ICNN ’11, pages 181-190, 2011.

[7]. N. Spirin and J. Han, "Survey on web spam detection: Principles and algorithms," SIGKDD Explor. Newslett., vol. 13, no. 2, pp. 50-64, May2012.

[8]. E.-P. Lim, V.-A. Nguyen, N. Jindal, B. Liu, and H. W. Lauw, "Detecting product review spammers using rating behaviors," in Proc.19thACMInt. Conf. Inform. Knowl. Manage., 2010, pp. 939-948.

[9]. W.Dzwinel et al Non multidimensional scaling and visualization of earth quake cluster over space and feature space, nonlinear processes in geophysics 12[2005] pp1-12.

[10]. C.Lomnitz. Fundamentals of Earthquake prediction [1994].

[11]. B.Gutenberg & C.H. Richtro, Earthquake magnitude, intensity, energy & acceleration bulseism soc. Am 36, 105-145 [1996].

[12]. C.Brunk, J.Kelly & Rkohai "Mineset An integrate system for Visual Data Mining" 1997.

[13]. http://www.dotnetspider.com.

[14]. Xia Qianfang and Ye Xiaohua;National Media Coverage of SARS Crisis (February to May 2003)[J];Journalism & Communication;2003-02.

[15]. Tian Weiguang and Li Xiguang;Political Bias of Media Coverage on China SARS by the US Media[J];Journalism & Communication;2003-02