Internet Usage Control Using Access Control Techniques

18CSS202J- Computer Communication Project Report

Submitted by

Anushka Priya (RA2011003010555)
Abhijeet Kumar Jha (RA2011003010549)
Shruti Srivastava (RA2011003010553)

Submitted to

Ms. M. Vaidhehi

Assistant Professor, Department of Computing Technologies

in partial fulfilment for the award of the degree of

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE ENGINEERING

SCHOOL OF COMPUTING

COLLEGE OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR - 603203

JUNE 2022

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR-603203

BONAFIDE CERTIFICATE

Certified that 18CSC202J minor project report titled **"Internet Usage Control Using Access Control."** is the bonafide work of **"Anushka Priya (**RA2011003010555) , **Abhijeet Kumar Jha(**RA2011003010549), **Shruti Srivastava(**RA2011003010553)**"** who carried out the minor project work under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate

SIGNATURE	**SIGNATURE**
MS.M.VAIDHEHI	M PUSHPALATHA
CC Faculty	**HEAD OF THE DEPARTMENT**
Assistant Professor	Professor
Dept. of Computer Technologies	Dept. of Computer Technologies

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.

INDEX

OBJECTIVE OF THE PROJECT

Problem statement- On a network infrastructure, there are 100 users. All the users access internet through a Cisco router. It was observed that the internet usage was very high which created problems like slow internet, expensive internet bills etc. To solve the problem, the network has to be redesigned which would allow only browsing traffic and all other traffic bound to the internet should be blocked.

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.

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 topdown 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:

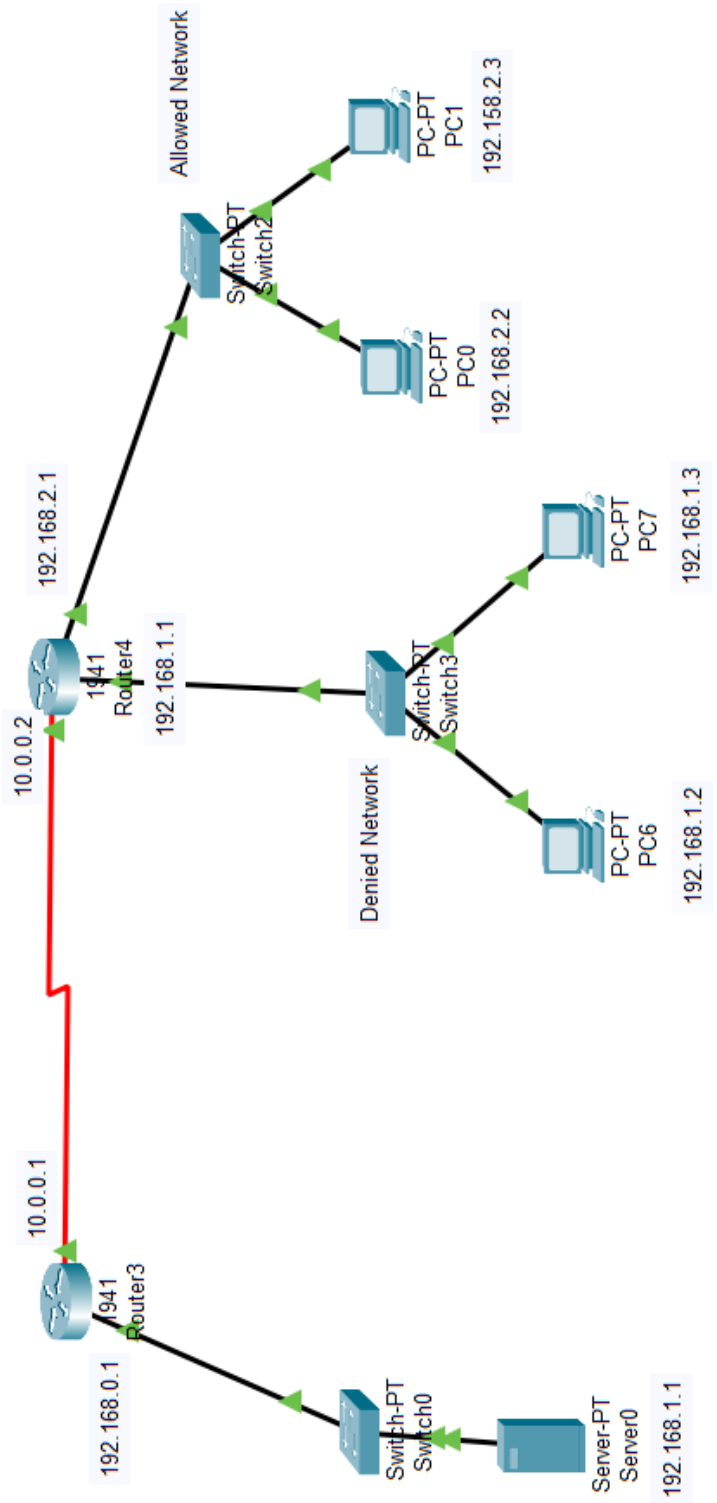
- Performance
- Formation of virtual workgroups
- Simplified administration
- Reduced cost
- Security

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.

Network Topology Diagram



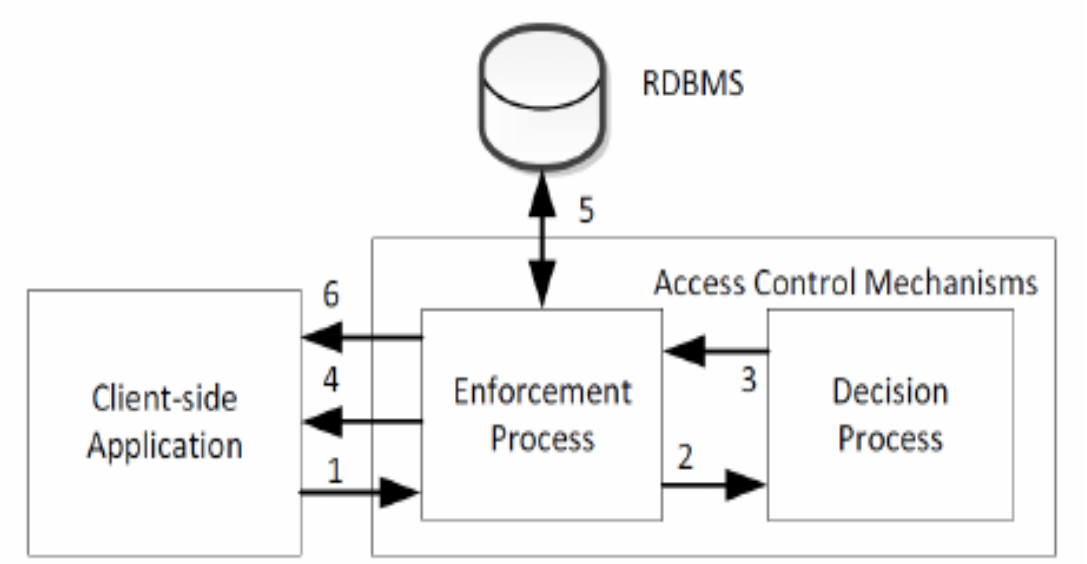
TCP/IP addressing

Device	Interface	IP Address	Subnet Mask	Gateway
Server0	Fa 0/0	192.168.0.2	255.255.255.0	192.168.0.0
PC6	Fa 0/0	192.168.1.2	255.255.255.0	192.168.1.0
PC7	Fa 0/0	192.168.1.3	255.255.255.0	192.168.1.0
PC0	Fa 0/0	192.168.2.2	255.255.255.0	192.168.2.0
PC1	Fa 0/0	192.168.2.3	255.255.255.0	192.168.2.0
Router3	Gig 0/0	192.168.0.1	255.255.25.0	-
Router3	Se 0/1/0	10.0.0.1	255.0.0.0	-
Router4	Gig 0/0	192.168.1.1	255.255.255.0	-
Router4	Gig 0/1	192.168.2.1	255.255.255.0	-
Router4	Se 0/1/0	10.0.0.2	255.0.0.0	-

Network Design strategy

- Web browsing traffic would comprise of the protocols http, https and dns. http and https is used by browsers and dns is used for resolving website names into IP address.
- Without DNS, name resolution would fail and browsing would not work.
- An access list is configured on the E0 interface as inbound which would allow only the protocols listed above and all other traffic is blocked.

Block Diagram



Router Configuration

- An extended ACL is configured on the E0 interface as inbound, the detail of which is shown below.
- Router(config)# #access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq 80
- Router(config)# #access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq 443
- Router(config)# #access-list 101 permit udp 192.168.1.0 0.0.0.255 any eq 53
- Router(config)#interface FastEthernet 0/0
- Router(config-if)#ip access-group 101

Router Configuration Explained

- The first line configures the ACL to allow TCP port 80 for http communication
- The second line configures the ACL to allow TCP port 443 for allowing https communication
- The 3rd line configures the ACL to allow TCP port 443 for allowing https communication
- The 4th line goes to the interface of the router
- The 5th line applies the ACL as inbound.
- The implicit deny functionality of Cisco ACL would ensure that all other protocols are denied automatically.
- The configurations would ensure that only http, https and dns traffic is allowed from the network 192.168.1.0/24 to the E0 interface through which packets bound for the internet travel.
- This would ensure that users would be unable to access any other type of traffic apart from the protocols listed above.

INFERENCES FROM THE RESULT

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 defence. 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.

REFERENCES

- Behrouz A. Forouzan “Data Communications and Networking” 5th ed., 2010
- Todd Lammle, CCNA Study Guide, 7th ed. 2011
- Cisco Networking Academy
- Geeks for Geeks