I'm human

An ACL is essentially a set of rules governing traffic flow based on source and destination IP addresses or port numbers, akin to allowing or blocking packets from entering an interface on a router, switch, firewall etc. Each entry within these access lists, known as ACEs, specifies a specific traffic pattern that should either be granted access or blocked. ACLs play a dual role in networks: they facilitate traffic control and filtering while also serving as a security mechanism for accessing routers via telnet or preferably SSH by only allowing required IP addresses or networks to connect. Other uses of ACLs include management access restriction, route advertisement filtering, debug output filtering, and VPN scenario-related traffic identification for encryption purposes. In essence, ACLs enable the matching of relevant packets for subsequent special operations. On Cisco devices, we have two primary types of ACLs: Standard Access Control Lists and Extended Access Control Lists. Standard ACLs are basic forms that can match packets based on source IP address in the packet header. These are simpler to create but also limited in their packet matching capabilities compared to extended ACLs. Extended ACLs offer more advanced features, including filtering by both source and destination IP addresses or a combination of these along with other fields like TCP/UDP ports etc. Both standard and extended access lists can be written in numbered or named format. While the functionality remains the same regardless of the chosen format—numbered or named—the former is often favored for its readability but is equally as effective as the latter, which is widely used in practice. Both formats are crucial for Cisco certification exams and can achieve the same results when properly configured. For creating ACLs on Cisco routers, it's essential to understand the access list number ranges (Table 1) that dictate standard and extended access lists. Understanding how these work, as demonstrated through configuring examples like those described in Figure 1, is critical for network control and security. This setup involves a single router R1 with two interfaces connected to an internal network and the Internet respectively, aiming to restrict access from the internal network to the Internet via ACLs applied on interface Fa0/0 in the inbound direction. Given text rewritten as: Standard Access List Configuration Examples The standard access control list allows for either permitting or denying traffic from a specific source IP address or IP network. Creating Numbered Standard Access Lists We will start by configuring a numbered standard access list first, followed by a named format. The goal is to allow Bob to access the Internet while blocking all access for Smith and logging unsuccessful attempts by Smith. Example in Numbered Format: ``` R1>enable R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#access-list 1 permit host 192.168.1.3 R1(config)#access-list 1 deny host 192.168.1.7 log ``` In this example, the `host` keyword is used to identify individual hosts, but an inverse mask can also be used to achieve the same result. Applying the Access List to Interface Fa0/0: ``` R1(config)#interface Fa0/0 R1(config-if)#ip access-group 1 in R1(config-if)#end ``` Named Access Lists Named access lists have a number from 1 to 99. When configuring an access list, it is necessary to identify the list with a number, as shown above. It's essential to note that every access list has an implicit deny all at the end of the ACL, even if not specified explicitly. Example in Named Format: ``` R1>enable R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ip access-list standard Filter R1(config-std-nacl)#permit 192.168.1.3 0.0.0.0 R1(config-std-nacl)#deny 192.168.1.7 0.0.0.0 log R1(config-std-nacl)#interface Fa0/0 R1(config-if)#ip access-group Filter in R1(config-if)#end ``` Extended Access Lists Configuration Examples An extended access control list allows for denying or permitting traffic from specific IP addresses and ports, as well as controlling the type of protocol that can be transferred. The range of extended ACLs is from 100 to 199 for numbered ACLs. Example of a Numbered Extended ACL: ``` access-list 110 permit tcp 92.128.2.0 0.0.0.255 any eq 80 ``` This ACL will permit traffic coming from any address on the 92.128.2.0 network towards any destination IP on port 80. The `any` statement is used to allow traffic towards any IP destination on port 80. Configuring Access Control Lists (ACLs) is crucial for network security. The example given shows how to configure a numbered ACL, allowing IP traffic from source network `192.168.1.0/24` to destination network `192.168.2.0/24`. To create an extended access list in numbered format, you must first enable the router and enter configuration mode: `R1>enable R1#configure terminal`. Next, define a permit rule for Bob (host 192.168.1.3) to access web servers on the Internet: `access-list 100 permit tcp host 192.168.1.3 any eq www`. Then, deny all web access for Smith by specifying his host IP address and logging unsuccessful attempts: `deny tcp host 192.168.1.7 any eq www log`. Apply this ACL to interface Fa0/0 in the inbound direction: `interface Fa0/0 R1(config-if)#ip access-group 100 in`. For a named ACL, enable the router and enter configuration mode as before. Then, create an extended access list with the name `Filter` and define the permit rule for Bob: `permit tcp 192.168.1.3 0.0.0.0 any eq www`. Deny all web access for Smith while logging unsuccessful attempts: `deny tcp 192.168.1.7 0.0.0.0 any eq www log`. Apply the named ACL to interface Fa0/0 in the inbound direction using the name of the ACL instead of its number: `ip access-group Filter in`. After setting an ACL, you must specify which direction it operates on the interface (inbound or outbound) and apply it to a specific interface. For example, `interface serial 0 Router(config-if)#ip access-group 111 out` specifies that ACL #111 operates in the outbound direction on the Serial 0 interface. To secure Telnet access to a router via ACLs, you can allow access only for certain hosts or networks while blocking all other attempts. A sample configuration involves creating an ACL with permit rules and then applying it to VTY login lines: `access-list 25 permit 192.168.2.0 0.0.0.255 line vty 0 4 access-class 25 in`. Another example shows allowing a specific management station (10.1.1.1) to access the router via Telnet while blocking all other hosts: `access-list 10 permit host 10.1.1.1 line vty 0 4 access-class 10 in`. We need to manage traffic in a network. Cisco routers have IOS commands that help control traffic effectively. However, PIX firewalls or ASA firewalls have additional security features. Access lists are used to filter out traffic based on configuration rules. When setting up access list rules, we should be careful because if a rule denies traffic and then allows it later, the router will drop the packet earlier. The order of rules matters. There is a difference between standard and extended access lists. Standard lists only filter traffic based on source IP, while extended lists can filter by multiple factors including source and destination IP, protocols, and port numbers. Extended lists are more complex to configure but provide more control over traffic. To create an access list in Cisco, we assign a number from 1 to 99. We then use the "deny" command followed by the IP address range, and the "permit any" command to allow other traffic. However, if we don't include the "permit any" command, the deny rule will block all traffic. To apply an access list to a router's interface, we use the "ip access-group" command. The access list is applied in both inbound and outbound directions, but only one access list can be enabled per interface and direction. List is enabled on router 1's gigabit Ethernet port in the outbound direction to block PC0 traffic reaching router 2. Once active, we verify its functionality by generating traffic through pinging router 2 from a host. The outcome shows destination host unreachable replies. To confirm packet blocking, we use the show access-lists command, which indicates the deny condition blocked four ping packets sent to the router. To filter traffic based on protocol, we configure an extended access list on router 2, blocking PC2's ICMP pings (ping functionality) while permitting all other network traffic. We apply this list in the inbound direction and test it by generating ICMP traffic from PC2. The expected result is that the ping command fails to reach any device in the network. Types of traffic are an essential aspect to consider when testing access-lists, providing a comprehensive evaluation of their effectiveness.

Access control lists. Access control list explanation. What is access control list (acl).