Troubleshooting and Tool Report

[ Name ]

## Network Problem Selected

The problem stated here is the inbound connection request from an adversary. This must be considered as a major problem as there is a potential threat of loss of data.

## Troubleshooting Steps

For this we can use the ACL (Access Control Lists). Here we must imply the port guard to block the request as we are getting the requests from a particular port. For further addition we can also use the implicit deny as it can deny all the traffic that has not been explicitly allowed.

## Tool and Description

Your network safety is the fundamental notion of utilizing ACL. Any route without it can enter or depart and become very exposed to undesirable and harmful traffic. You may refuse some router updates or offer traffic flow control to increase safety with ACL, for example. As illustrated in the following picture, the routing device contains an ACL that limits access to C hosting over the financial network, while allowing access to the D holding. ACL enables you to filter packets for individual or group IP addresses or other protocols like TCP and UDP. You may therefore, for instance, prohibit access to a whole network, and let only one, instead of banning an administrator in an engineering team. Or access to Host C might also be limited. If the host C developer requires access to a financial network web server, only port 80 may be activated and everything else can be blocked.

## Tool Operational Use Case

You will need the necessary details when defining an ACL entry.

**Sequence Number**: Identify ACL with a number.

**ACL Name**: define a term for the ACL input. Some routers enable a mix of names and numbers instead than simply a series of numbers.

**Remark**: Some routers let you add comments to the ACL, so you may give extensive explanations.

**Statement**: Reject or permit a certain source based on the wildcard's address and mask. Certain routing devices, like Cisco, prepare a clear declaration of denial at conclusion of each ACL automatically.

**Accord on communications**: Specify if IP, IPX, ICMP, TCP, UDP, NetBIOS and more should be disabled.

**Location or Source**: Set a single IP, Range (CIDR), or all addresses to the source or destination goals.

**Log**: When ACL matches are found, some devices can keep logs.

**Additional Conditions**: Advanced traffic control (ToS), IP startup, and code point (DSCP) priority are used by advanced ACLs.

## Tool Functionality

In order to correctly use ACL, it is important to understand the input and output of the router. All traffic is based on the viewer interface of the router when you establish ACL rules (not other networks). The input flows from the network, external or internal, to the optical router connection, as you can see in the following figure. On the other side, egress traffic flows into the network from the visible connection. To interact with ACL, utilize it at the router interface. As the router hardware makes all transmission and transfer decisions, ACL declarations may be made fast. The source is the first one, and the destination moves backwards when you establish an ACL input. See the example of Cisco Router's extended ACL IP. You must first define the source and then the destination IP when you construct a Deny/Permit rule. Inbound streams are the source of all hosting and networks, and all festivals and networks receive inbound streams.

Diagram

Description automatically generated