Misconfiguration or Ineffectiveness of Time-Based ACLs for Web Access Restriction in Cisco Networks

Problem Description

Time-Based Access Control Lists (Time-Based ACLs), which are defined to control and restrict internet traffic at certain time intervals in the corporate network infrastructure, cannot fulfil the expected filtering function despite the configuration accuracy. This technical failure allows unauthorised web access by users outside working hours, creating a situation that contradicts information security principles, network policies and access management strategies. The aim is to ensure that users have internet access only during certain time periods in corporate networks and to prevent web traffic during off-hours.

Prerequisites

CLI (command-line) access to the Cisco router

The NTP server is correctly configured and accessible

Command of IP access control list (ACL) logic

Affected OSI Layers

Layer 3 (Network Layer): IP-based access controls are performed by ACL (Access Control List) rules defined on the router or switch.

Layer 7 (Application Layer): For application protocols such as HTTP/HTTPS, filtering can be done based on the destination domain address or port.

Diagnosis

If feedback is received that users continue to access the web on the corporate network outside working hours, it is understood that time-based access control lists (Time-Based ACL) are not activated in the defined time periods.

The technical review carried out to analyse this situation includes the following steps:

Firstly, access control rules were examined with the show access-lists command; it was evaluated whether IP address and port-based restrictions were defined appropriately.

-The show time-range command was then used to check whether the relevant time ranges had been defined and correctly associated with the ACL rules. In most cases, it was observed that the definition of time-range was missing or incorrect, or that it was not associated with the ACL.

-Finally, the system clock on the router was checked with the show clock command; it was determined that synchronisation with the NTP server could not be achieved or the clock information was manually configured incorrectly.

As a result of these findings, it was assessed that the internet access problems observed at Layer 7 were caused by incomplete or incorrect implementation of the time-based access control mechanisms defined at Layer 3.

Root Cause: The root cause of the problem is that the time-range configuration, which enables access restrictions based on time periods, is missing or incorrectly defined. Even if the ACL rule is written correctly, these rules will not become active if they are not associated with a time range. In addition, incorrect router clock or failed NTP synchronisation can cause time-based rules not to work as expected.

Admin Guide:

1. Ensuring Clock Synchronisation

    R1(config)# ntp server 192.168.1.10

    R1# show clock

2. Defining the Time Interval

    R1(config)# time-range MESAISAATI

    R1(config-time-range)# periodic weekdays 08:00 to 18:00

3. Defining ACL Rules

    R1(config)# access-list 100 deny tcp any any eq www time-range MESAISAATI

    R1(config)# access-list 100 permit ip any any

4. Applying ACL to the Interface

    R1(config)# interface FastEthernet0/0

    R1(config-if)# ip access-group 100 in

5. Validation Commands

R1# show access-lists 100

R1# show time-range

R1# show clock

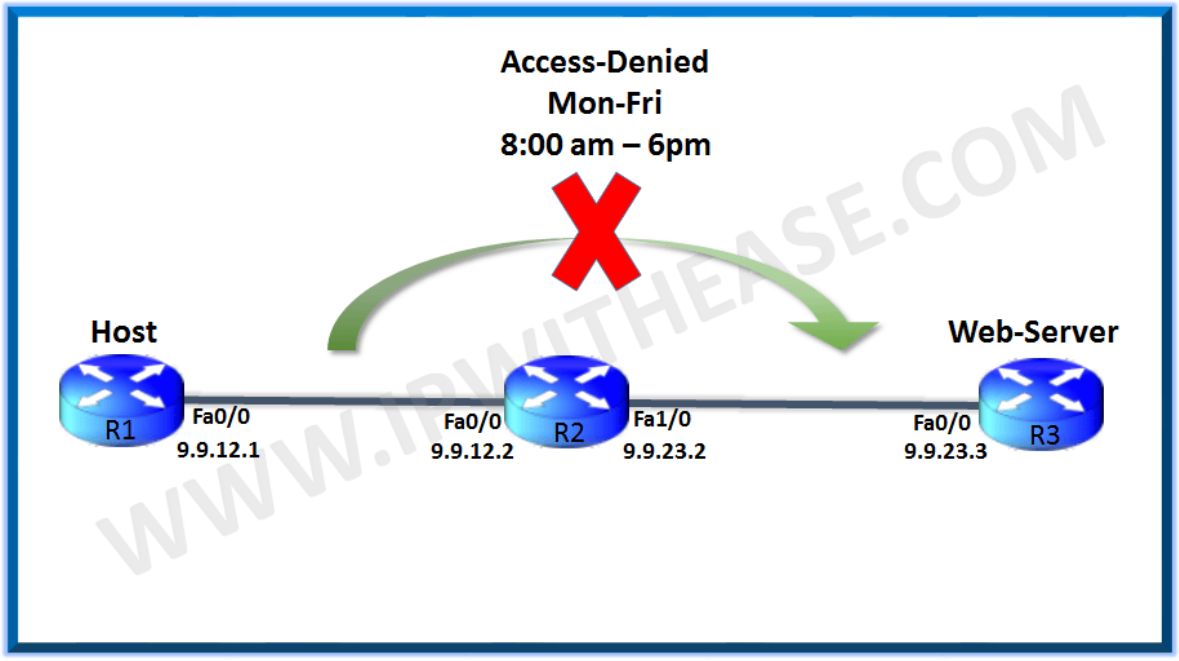
Expected Result:

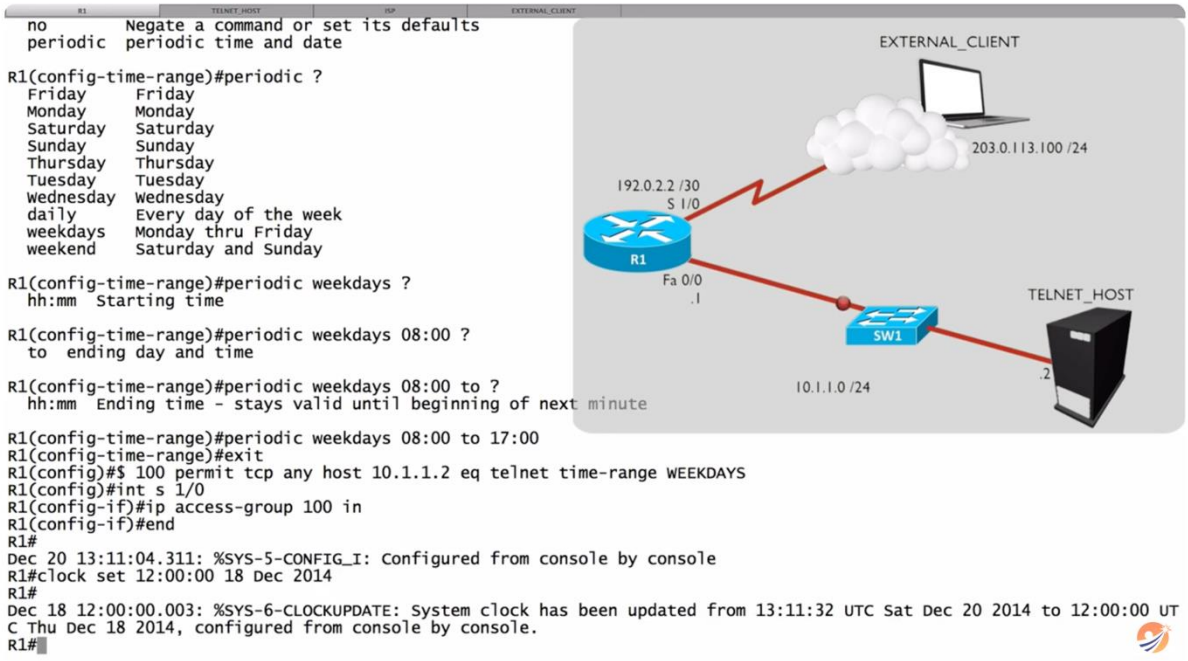
Outside office hours (18:00 - 08:00), users should be blocked from accessing the web; during office hours, access should be allowed. If the router clock is correct and ACLs are configured correctly, time-based filtering will work as expected.

Time-based ACLs

- To implement time-based ACLs:
  - Create a time range that defines specific times of the day and week.
  - Identify the time range with a name and then refer to it by a function.
  - The time restrictions are imposed on the function itself.

Step 1	R1(config)#**time-range EVERYOTHERDAY** R1(config-time-range)#**periodic Monday Wednesday Friday 8:00 to 17:00**
Step 2	R1(config)#**access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq telnet time-range EVERYOTHERDAY**
Step 3	R1(config)#**interface s0/0/0** R1(config-if)#**ip access-group 101 out**

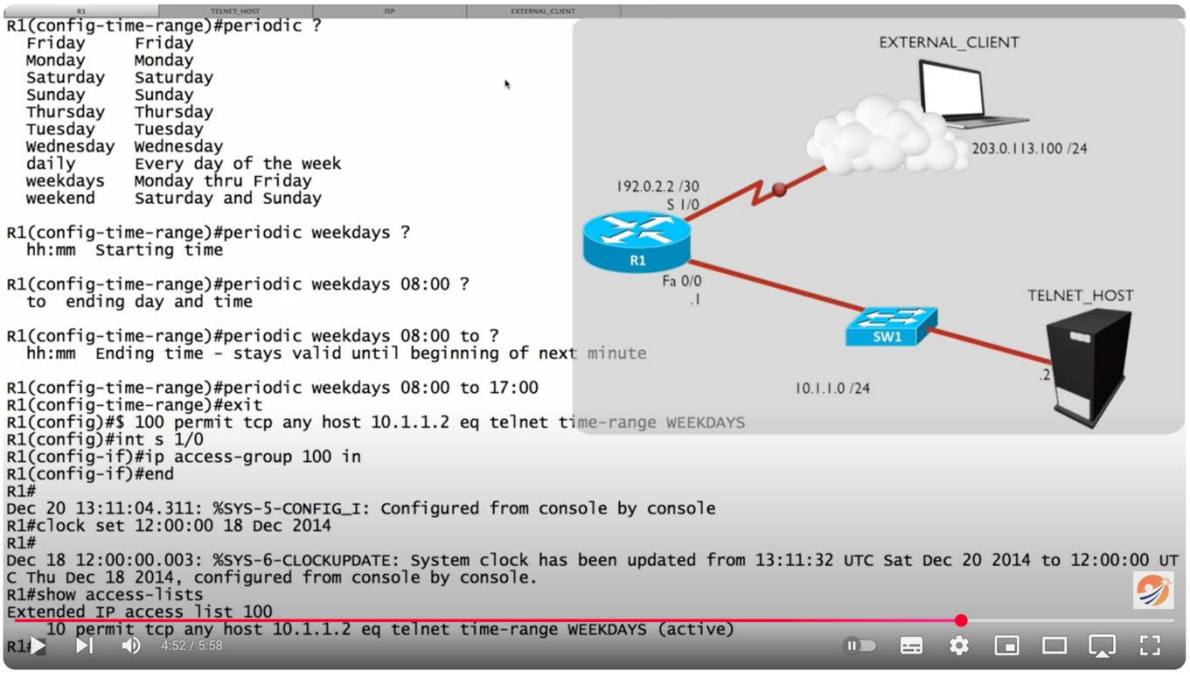




Cisco IOS: Time-Based Access Control Lists (ACLs)

Kevin Wallace Training, LLC
155 B abone
Abone ol

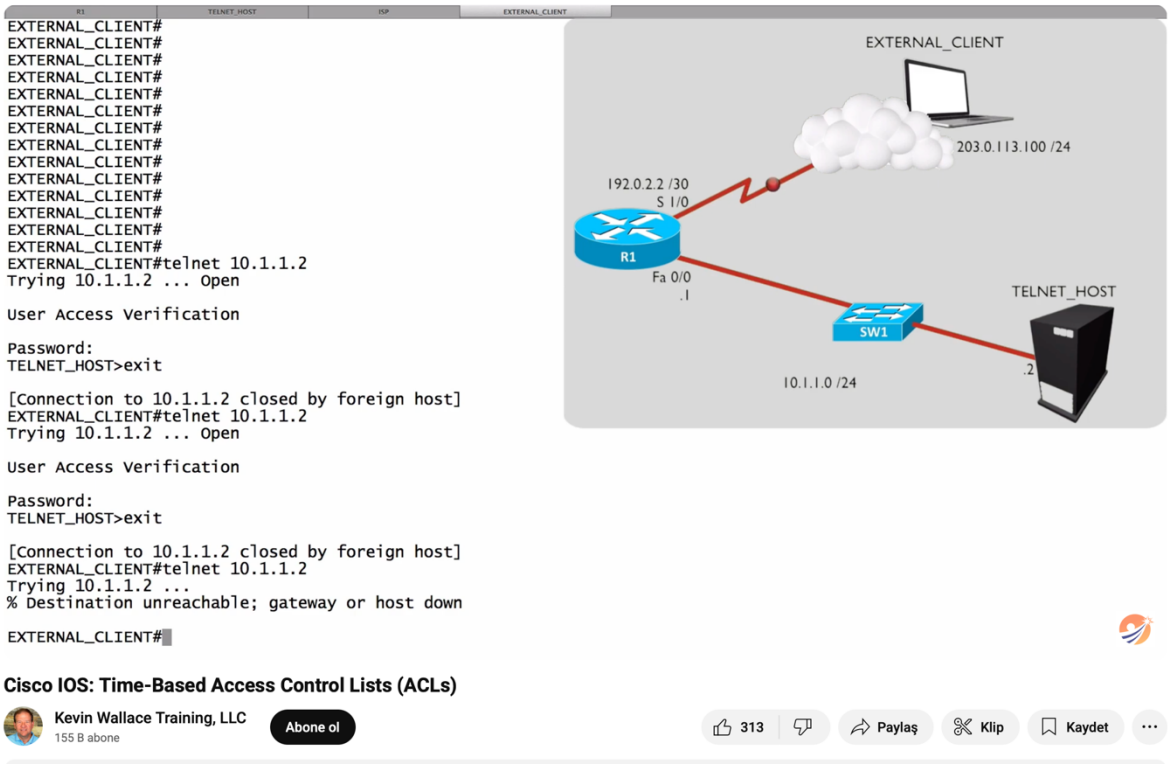
313 Paylaş Klip Kaydet



Cisco IOS: Time-Based Access Control Lists (ACLs)

Kevin Wallace Training, LLC
Abone ol

313 Paylaş Klip Kaydet



Conclusion

When the Time-Based ACL is successfully implemented:

Out of Time Slot (When Access is Free): When the defined time slot is not active, the access list (ACL) is not activated. Ping commands and web accesses (HTTP/HTTPS) from user devices to the target server are successfully executed. Network traffic continues uninterrupted.

Within Time Range (When Access is Restricted): ACL is activated automatically when the defined time-range becomes active. The rules specified in the access list are activated and prevent the related devices from accessing the target IP address. In this case, ping tests fail. Access via web browser fails (page cannot be displayed).

Verification and Monitoring Commands:

With the -show access-lists command, it can be checked whether the relevant ACL is active.

With the -show time-range command, it is observed whether the time range is valid or not.

When the ACL is activated by updating the clock, access is cut off immediately.

Access is restored when the clock is set back or out of the time interval.