

Packet Tracer Lab 15 Solution Guide

Internal Portal Access Failure

Incident ID: INC-1015

Objective

This lab focuses on identifying and restoring access to an internal web application following scheduled security policy updates.

Although users can browse the internet and resolve DNS successfully, the internal BridgeOpsOne Corporate Portal is inaccessible.

The objective is to troubleshoot the issue using a structured methodology, identify the root cause, restore application access, and validate successful operation.

Root Cause

An extended ACL named **LAN_SECURITY** was applied inbound on **GigabitEthernet0/0.10**.

The ACL contained the following entry:

```
deny tcp any host 192.168.20.100 eq www
```

As a result:

- DNS continued functioning.
- ICMP connectivity remained operational.
- Internet browsing remained operational.
- HTTP traffic to the internal web server was blocked.

Symptoms Observed

- Users successfully receive IP configuration.
- Default gateway reachable.

BridgeOpsOne

- Internal DNS resolution successful.
- Internal server responds to ping.
- Public website accessible.
- Internal portal fails to load (Request Timeout).

Troubleshooting Process

Step 1 — Verify IP Configuration

From PC-HR:

ipconfig

Verify:

- Valid IP address
 - Valid subnet mask
 - Valid default gateway
 - Correct DNS server
-

Step 2 — Verify Gateway Connectivity

Example:

ping 192.168.10.1

This should succeed.

Step 3 — Verify DNS Resolution

Example:

ping portal.bridgeops.local

Successful hostname resolution confirms the issue is not DNS-related.

Users should observe that the hostname resolves to:

BridgeOpsOne

192.168.20.100

This confirms DNS is functioning correctly.

Step 4 — Compare Application Behavior

Verify:

`http://bridgeopsone.com`

Loads successfully. This comparison demonstrates that HTTP is functioning to external resources while the issue is isolated to the internal application.

Then test:

`http://portal.bridgeops.local`

The request times out.

This confirms the issue is isolated to the internal application.

Step 5 — Verify Connectivity to the Server

Example:

`ping 192.168.20.100`

Ping succeeds, confirming the server is reachable over Layer 3.

This confirms Layer 3 connectivity exists.

Step 6 — Review Security Policy

Access R-MAIN.

Use:

`show access-lists`

Identify:

`deny tcp any host 192.168.20.100 eq www`

Then review the running configuration.

BridgeOpsOne

Packet Tracer Note: The command `show run interface g0/0.10` is not supported. Instead, use:

`show run`

or

`show run | section GigabitEthernet0/0`

Locate the following configuration:

```
interface GigabitEthernet0/0.10
ip access-group LAN_SECURITY in
```

This confirms the ACL is actively filtering traffic from the user VLAN.

Commands Used

```
ipconfig
ping
show ip interface brief
show access-lists
show running-config
configure terminal
interface g0/0.10
no ip access-group LAN_SECURITY in
write memory
```

Resolution

Access R-MAIN:

```
conf t
interface g0/0.10
no ip access-group LAN_SECURITY in
end
write memory
```

BridgeOpsOne

Validation

Successful resolution should include:

- Internal portal loads successfully.
- Public website remains accessible.
- DNS resolution successful.
- Successful ping to the internal server.
- Users regain access to internal web resources.

Key Takeaways

- Connectivity and application access are not always the same.
- Successful ping tests do not guarantee application functionality.
- ACLs can selectively block specific protocols while allowing other traffic.
- Always compare working and non-working services before making assumptions.
- Verify security policies as part of structured troubleshooting.
- Packet Tracer does not support show run interface; use show run or show run | section instead.