



REPORT

Layered Access Control Bypass & Cross-Platform Network Stabilization

v1.0.0

Author:

Eldon Gabriel

October 8, 2025



Cybersecurity Professional | IT Security Consultant

TABLE OF CONTENTS

REVISION HISTORY	2
SECTION 1.0: EXECUTIVE SUMMARY	3
1.1 Project Description	3
1.2 Security Conflict.....	4
1.3 Chronology of Network Instability.....	4
2.0 STABILIZATION PROCEDURE	5
3.0 CONCLUSION	6
3.1 Key Takeaways.....	6
3.2 Security Implications and Recommendations.....	6




Disclaimer: This report documents my personal work completing an MCSI lab exercise. It reflects my understanding and configuration of Windows 10 UAC settings in a controlled environment. No MCSI video or lab materials have been posted, shared, or distributed, ensuring compliance with MCSI's policies.



Cybersecurity Professional | IT Security Consultant

REVISION HISTORY

Version	Date	 Author	Description of Changes
v1.0.0	10/08/2025	Eldon G.	Initial draft.





Cybersecurity Professional | IT Security Consultant

SECTION 1.0: EXECUTIVE SUMMARY

1.1 Project Description

This report explains how a complex, three-step connection problem was found and fixed. The issue happened when trying to connect to a Windows 10 virtual machine (VM) using Remote Desktop Protocol (RDP). The VM was running on a macOS system using the UTM virtualization platform in **Bridged Network** mode.

The first problem was a Domain Group Policy Object (GPO) that blocked remote logins. The second problem was network instability in the virtual NIC, which caused the RDP session to drop.

The final solution used a **bidirectional network initialization method** (forced ARP refresh) to keep the virtual NIC stable long enough for the RDP session to connect.

This exercise showed skills in **security policy analysis, network management across different platforms, and troubleshooting virtual machines**—all important for a Cybersecurity & IT Operations Technician.



1.2 Security Conflict

Observation

A Domain Group Policy Object (GPO) stopped the admin account from connecting via RDP. The system showed access-denied errors even with correct credentials.

Resolution

The problem was solved by setting the correct **User Rights Assignment** in `secpol.msc`. This gave the admin account permission to log in remotely, meeting the lab goal.

This approach restored proper access without changing the main domain policy.

1.3 Chronology of Network Instability

Frequent drops caused **Error 0x204** ("We could not connect to the remote PC"). The problem was caused by the virtual NIC not keeping **ARP entries consistent** in Bridged Mode.

Logs showed repeated attempts to connect, followed by **incomplete ARP updates** between the host and guest IP addresses.



2.0 STABILIZATION PROCEDURE

Concept

ICMP packets (pings) were sent both ways to **force the host's ARP cache to update** and keep the UTM Bridged Mode route active. This stopped the connection from dropping.

Procedure

1. From the macOS host, ping the VM IP **192.168.1.58**.
2. From the Windows VM, ping the host IP at the same time.
3. Launch the RDP client while the connection is stable.

Exchanging pings in both directions kept the ARP tables refreshed. This lets the virtual NIC stay active long enough for RDP to finish logging in. It also prevented the NIC from timing out.



3.0 CONCLUSION

3.1 Key Takeaways

This solution shows the ability to analyze and fix problems in both security policies and virtual networks. Solving the GPO restrictions and network instability shows skill in security management, system control, and troubleshooting.

The bidirectional ping method shows how practical solutions can fix hard problems. This report provides clear proof of hands-on problem-solving and professional-level documentation for cybersecurity work.

3.2 Security Implications and Recommendations

- Created effective workarounds for unstable virtual networks.
 - Learned advanced troubleshooting for OS and virtualization issues.
 - Improved skill in finding and solving multi-layered problems.
 - Reinforced professional documentation standards.
 - Always control access and permissions during virtual experiments to avoid privilege problems.
 - Watch host–guest connections for network issues or ARP errors.
 - Use network segmentation and firewalls to reduce the risk of attacks inside the virtual network.
 - Keep records of all configuration changes to allow review or rollback if needed.
-