**National University of Computer and Emerging Sciences**

****

**FINAL COURSE PROJECT**

**CYBER SECURITY**

|  |  |
| --- | --- |
| Course Instructor | DR. Arshad Ali |
| Teacher Assistant | Maida Sajid |
| Section | BCS-6A |
| Semester | Spring 2024 |
| Participants: | Mashhood Ahsan 21L-5406  Rafay Ul Haq 21L-5383  Haris 21L-7526  Huraira 21L-7586 |

# List of Figures

Catalog

**[List of Figures 2](#_Toc1362)**

**[Network Security Implementation and Analysis using Packet Tracer 4](#_Toc23796)**

**[Introduction: 4](#_Toc18836)**

**[Objectives: 6](#_Toc29390)**

**[Major Design Areas and Functional Areas 7](#_Toc3261)**

**[ Network Devices 8](#_Toc5452)**

**[ IP Addresses 13](#_Toc29434)**

**[CYBER SECURITY PROTOCOLS 15](#_Toc17547)**

**[FIREWALL 15](#_Toc24057)**

**[VLAN 16](#_Toc15743)**

**[SSL Encryption 17](#_Toc22763)**

**[Monitor network traffic, identify anomalies, and generate 28](#_Toc24670)**

**[alerts for potential security incidents. 28](#_Toc26069)**

**[Conclusion and Recommendations: 34](#_Toc18224)**

# 

# Network Security Implementation and Analysis using Packet Tracer

# 

# Introduction:

In today's digital age, network security stands as a paramount concern for organizations across industries, with educational institutions being no exception. As universities increasingly rely on interconnected systems to facilitate communication, collaboration, and the exchange of vital information, ensuring the integrity, confidentiality, and availability of data becomes imperative.

This project delves into the realm of network security within the context of a university environment, leveraging Cisco Packet Tracer to craft a robust infrastructure capable of withstanding modern cyber threats. By adhering to the objectives outlined by Cisco, this endeavor seeks to fortify the network against unauthorized access, data breaches, and other malicious activities.

At its core, the project endeavors to achieve several key objectives. Firstly, it aims to design a comprehensive network topology tailored to the needs of a typical university setting, accommodating various departments, administrative offices, and end-user devices. This topology serves as the foundation upon which subsequent security measures are implemented.

Central to the project's mission is the implementation of stringent access control mechanisms. Through the strategic deployment of firewall rules, VLAN segmentation, and access lists, the network's traffic flow is regulated, and unauthorized access to critical resources is restricted. Moreover, encryption protocols such as SSL/TLS or IPsec are employed to safeguard data traversing the network, ensuring confidentiality and integrity.

In addition to proactive measures, the project also focuses on the deployment of intrusion detection and prevention systems (IDPS) to detect and thwart malicious activities in real-time. Network monitoring tools are leveraged to scrutinize traffic patterns, identify anomalies, and generate alerts, enabling swift response to potential security incidents.

Furthermore, the project emphasizes the development of robust incident response procedures and policies, empowering stakeholders to effectively mitigate security breaches and minimize their impact on the network.

Ultimately, the project culminates in a comprehensive analysis of the implemented security measures, evaluating their efficacy in safeguarding against common cybersecurity threats and vulnerabilities. Through meticulous documentation and analysis, insights are gleaned, strengths are identified, weaknesses are addressed, and recommendations for further enhancement are proposed.

By undertaking this endeavor, the university not only fortifies its network infrastructure against evolving cyber threats but also fosters a culture of cybersecurity awareness and preparedness among its stakeholders. In an era defined by digital transformation and interconnectedness, safeguarding the integrity and confidentiality of data remains paramount, and this project serves as a testament to the university's commitment to upholding these principles.

# **Objectives:**

The primary objective of the proposed network is to modernize and fortify the existing infrastructure of the university's network. This modernization effort aims to enhance the network's capabilities and increase its flexibility to adapt to evolving technological landscapes while ensuring robust security measures are in place.

Specifically, the objectives include:

1. Modernization: Update the existing network architecture to align with contemporary standards and best practices in network design and security.

2. Enhanced Capabilities: Implement advanced networking technologies and protocols to improve the performance, reliability, and scalability of the network.

3. Flexibility:Design a flexible network topology that can accommodate future growth, technological advancements, and changes in organizational requirements.

4. Security: Strengthen the network's security posture by implementing comprehensive security measures, including access control mechanisms, encryption protocols, intrusion detection and prevention systems, and incident response procedures.

5. Resilience: Ensure the resilience of the network infrastructure by incorporating redundancy, failover mechanisms, and disaster recovery strategies to mitigate the impact of potential disruptions or cyber attacks.

6. User Experience: Prioritize user experience by optimizing network performance, minimizing downtime, and providing seamless connectivity for students, faculty, staff, and other stakeholders.

7. \*\*Compliance:\*\* Ensure compliance with relevant regulatory requirements and industry standards pertaining to network security and data privacy.

By achieving these objectives, the university aims to establish a modern, secure, and resilient network infrastructure that can support its academic, administrative, and research activities effectively and efficiently. This network transformation initiative reflects the university's commitment to staying at the forefront of technological innovation while safeguarding the integrity and confidentiality of its digital assets.

# Major Design Areas and Functional Areas

The existing system is a very basic system. University mainly comprises of three main sections as

1. Labs

2. Exam Center

3. Office

All the hosts are assigned with static IPs and are assigned in the order in which it where set up. No support for dynamic IP allocations. Even though the working is divided into three major sectors all the

host, multimedia devices are connected in a single network.

# Network Devices

- Cisco PT Routers

- Cisco PT switches

- PC PT

- Server- PT FTP

-Server-PT- WEB

-Server -PT DNS

-Printer-PT

-1941 Router

-1950-24 Router

-Server-PT SysLog

-Laptop-PT

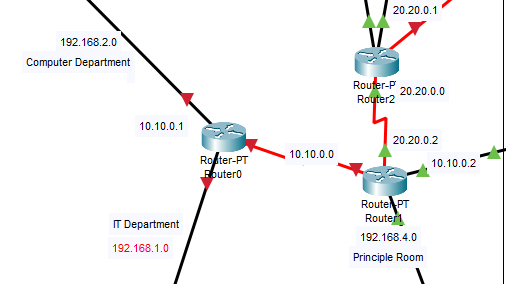
-5505 ASA1

Picture of whole network:

[C:\Users\abc\Pictures\Screenshots\Screenshot (14).png](C:\\Users\\abc\\Pictures\\Screenshots\\Screenshot (14).png)

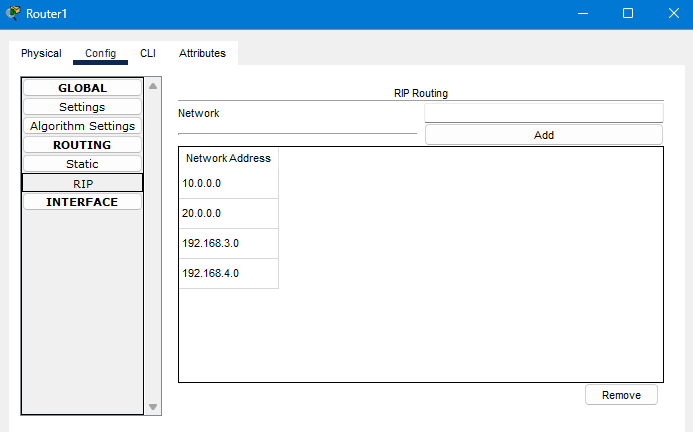
* **Routers**

1-Connectivity between Labs , Offices and Server rooms.

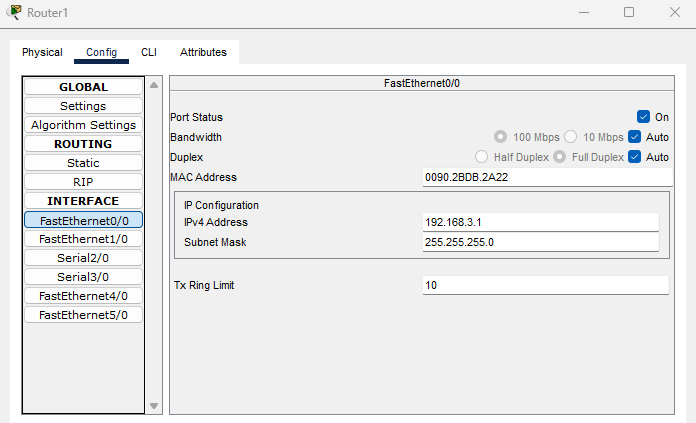


Demonstrating connectivity of R**outer 1**

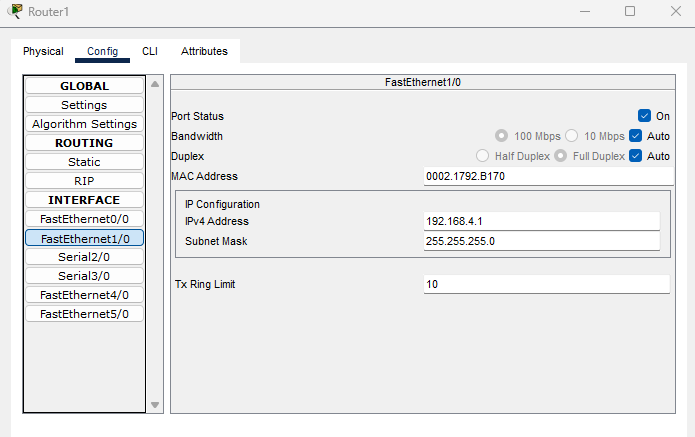
* **RIP Table:**



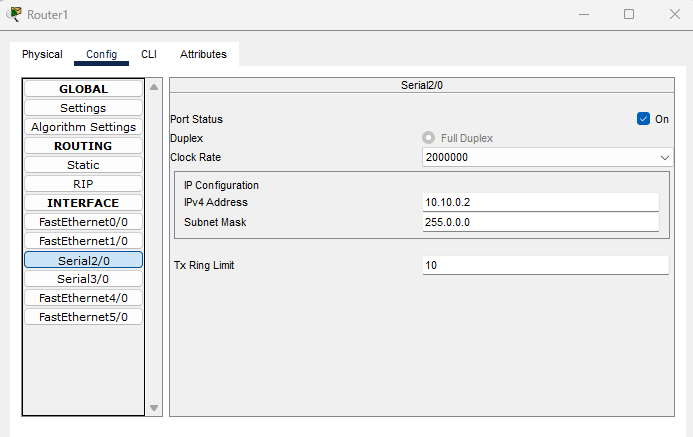
* Linked with others room



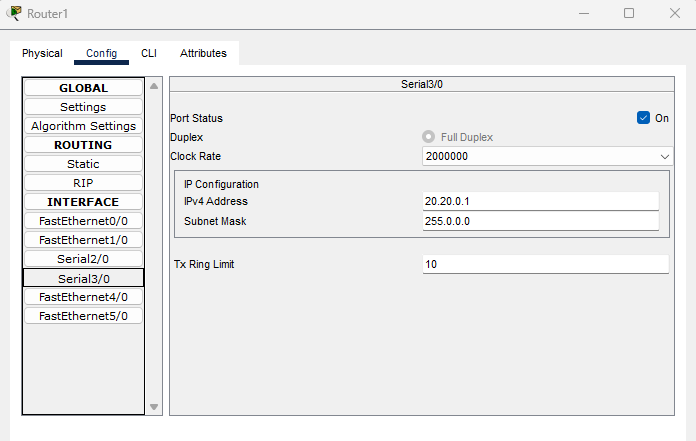
* Linked with Principal room:



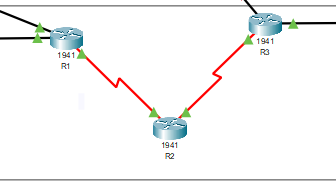
* Linked with router 0



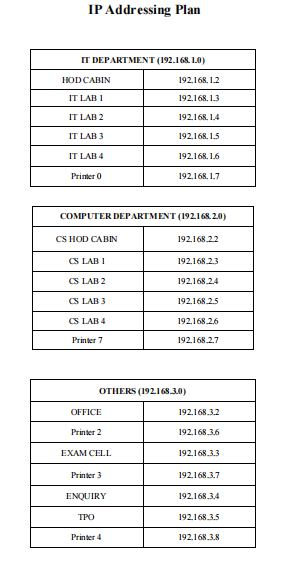
* Linked with router 1:

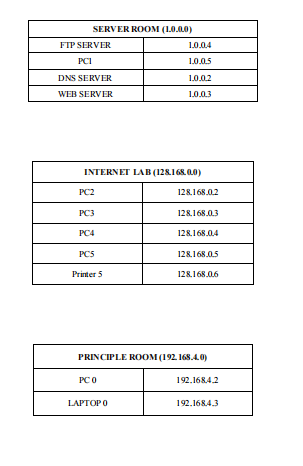


2-IDPS network connectivity routers



# IP Addresses





# CYBER SECURITY PROTOCOLS

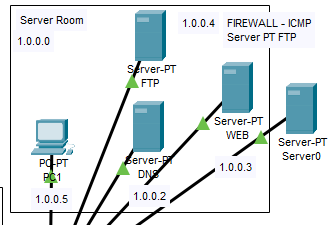
# FIREWALL

- Firewalls are deployed at network boundaries to enforce access control policies and filter traffic based on predefined rules.

- The firewall rules effectively control traffic flow and restrict unauthorized access to network resources, mitigating the risk of external threats.

**A**pplied IMCP firewall on FTP server room to stop these attcaks:

* ICMP Flood Attacks
* Ping of Death Attacks
* ICMP Tunneling Attacks
* ICMP Redirect Attacks
* ICMP Evasion and Reconnaissance
* ICMP Time Exceeded Attacks



# VLAN

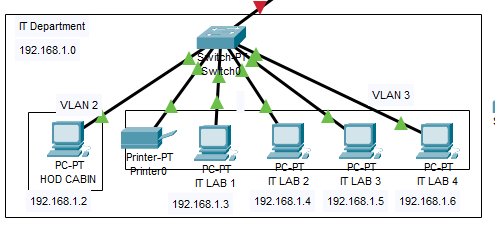
VLANs (Virtual Local Area Networks)

VLANs have been effectively implemented to segment the network into distinct broadcast domains, enhancing network security by isolating traffic and restricting unauthorized access between network segments.

- VLANs provide granular control over network traffic, reducing the risk of lateral movement by potential attackers.

It is applied on IT department. It can stops attcaks such as

* VLAN Hopping Attack
* ARP Spoofing/Poisoning
* MAC Flooding Attack
* VLAN Double Tagging Attack
* DHCP Spoofing Attack



# SSL Encryption

SSL encryption is implemented to secure data in transit between network devices, ensuring confidentiality and integrity.

- SSL encryption protocols such as TLS provide robust encryption mechanisms for protecting sensitive data transmitted over the network.

- Regular updates and patches are essential to address vulnerabilities in SSL implementations and maintain the security of encrypted connections.

It protects from:

Sure, here are the types of attacks SSL/TLS helps protect against:

1. Man-in-the-Middle (MITM) Attacks

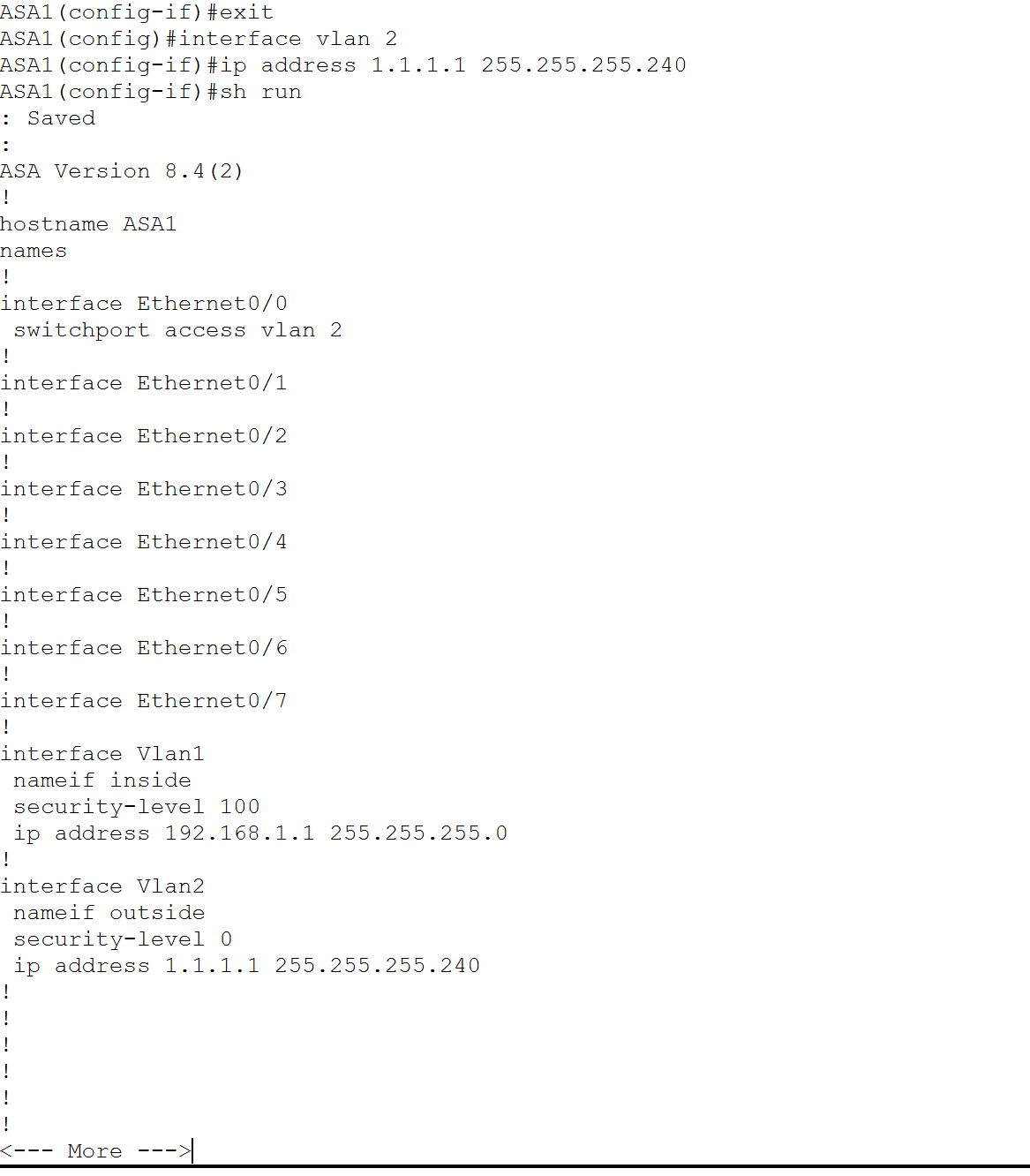
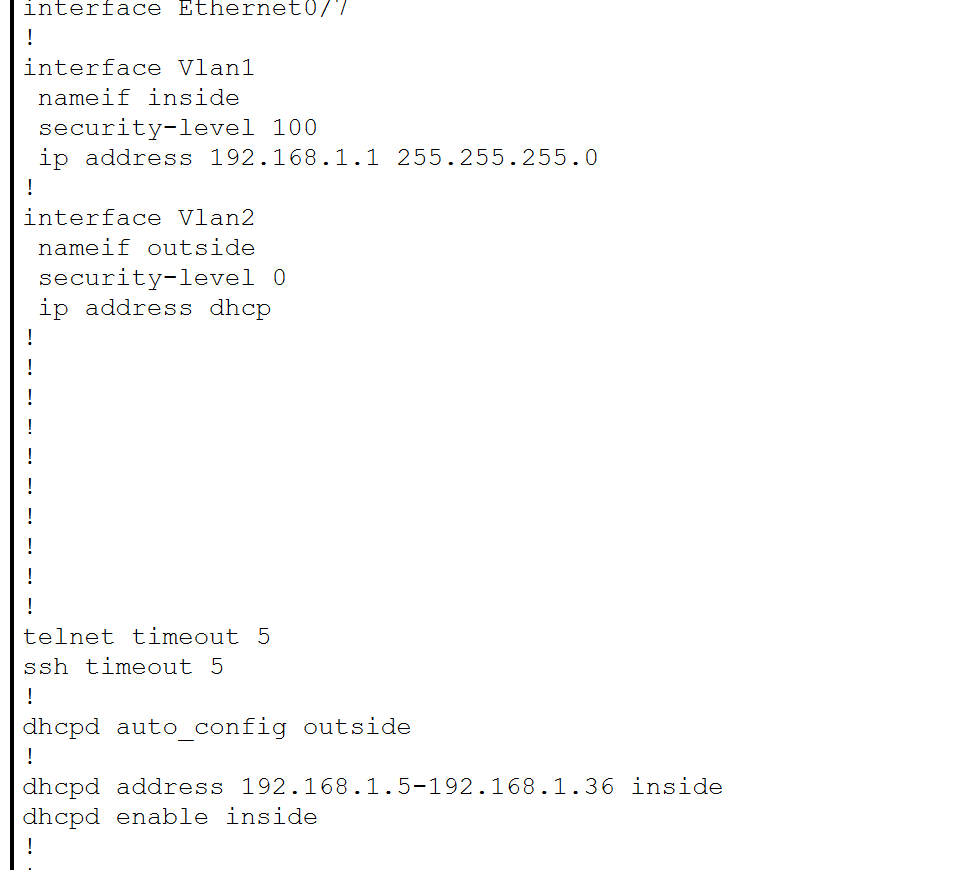
2. Eavesdropping

3. Data Tampering

4. Spoofing

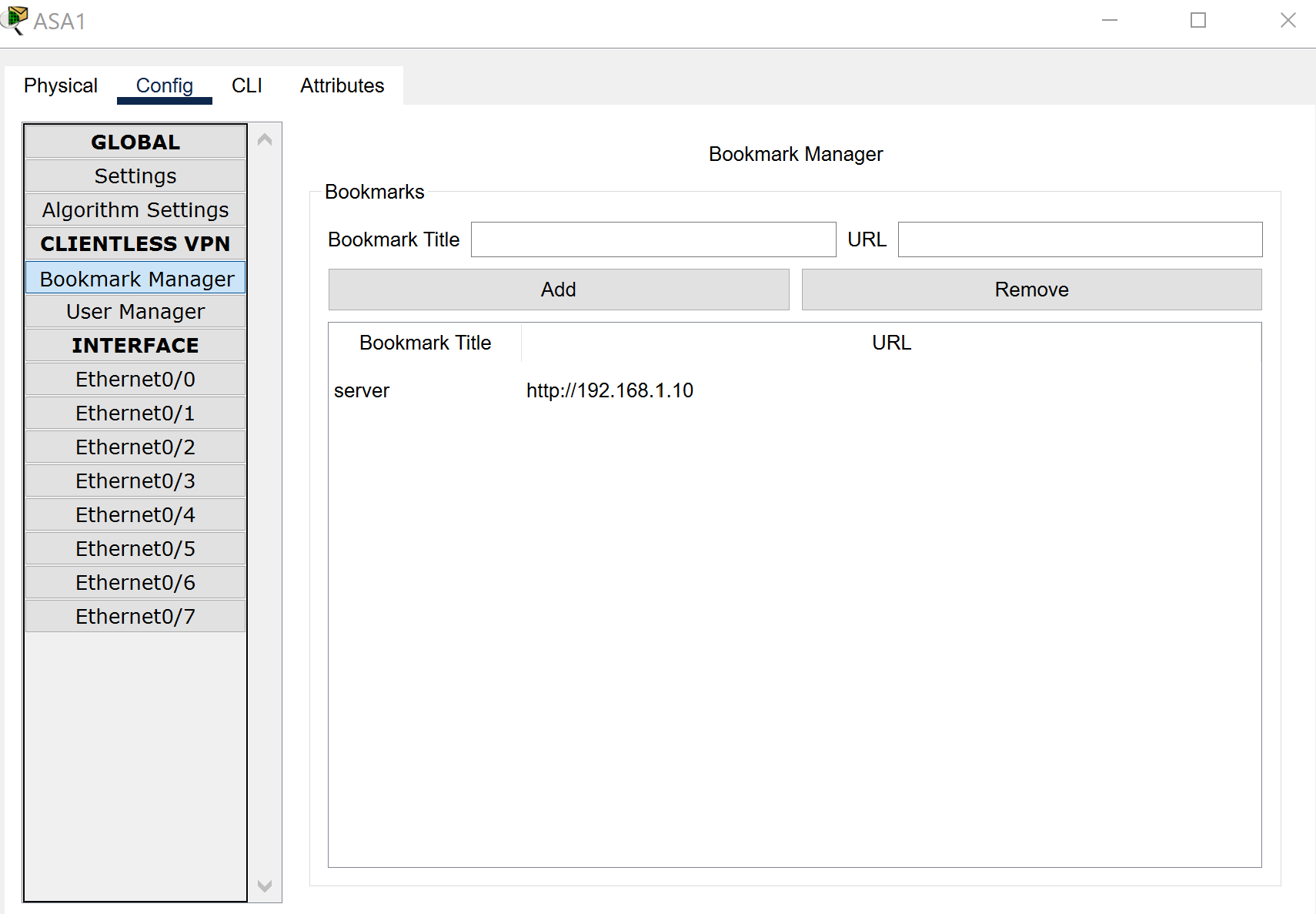
5. Session Hijacking

Initializing network security 5505:-

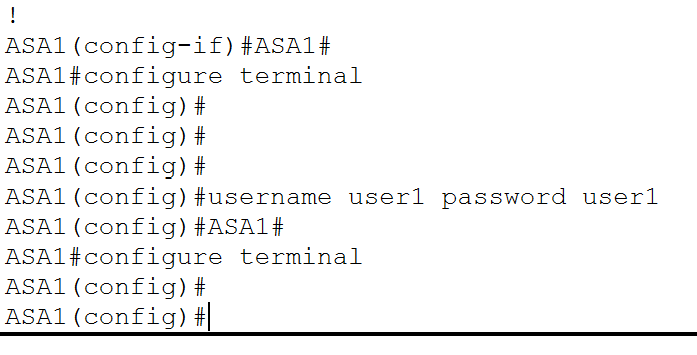


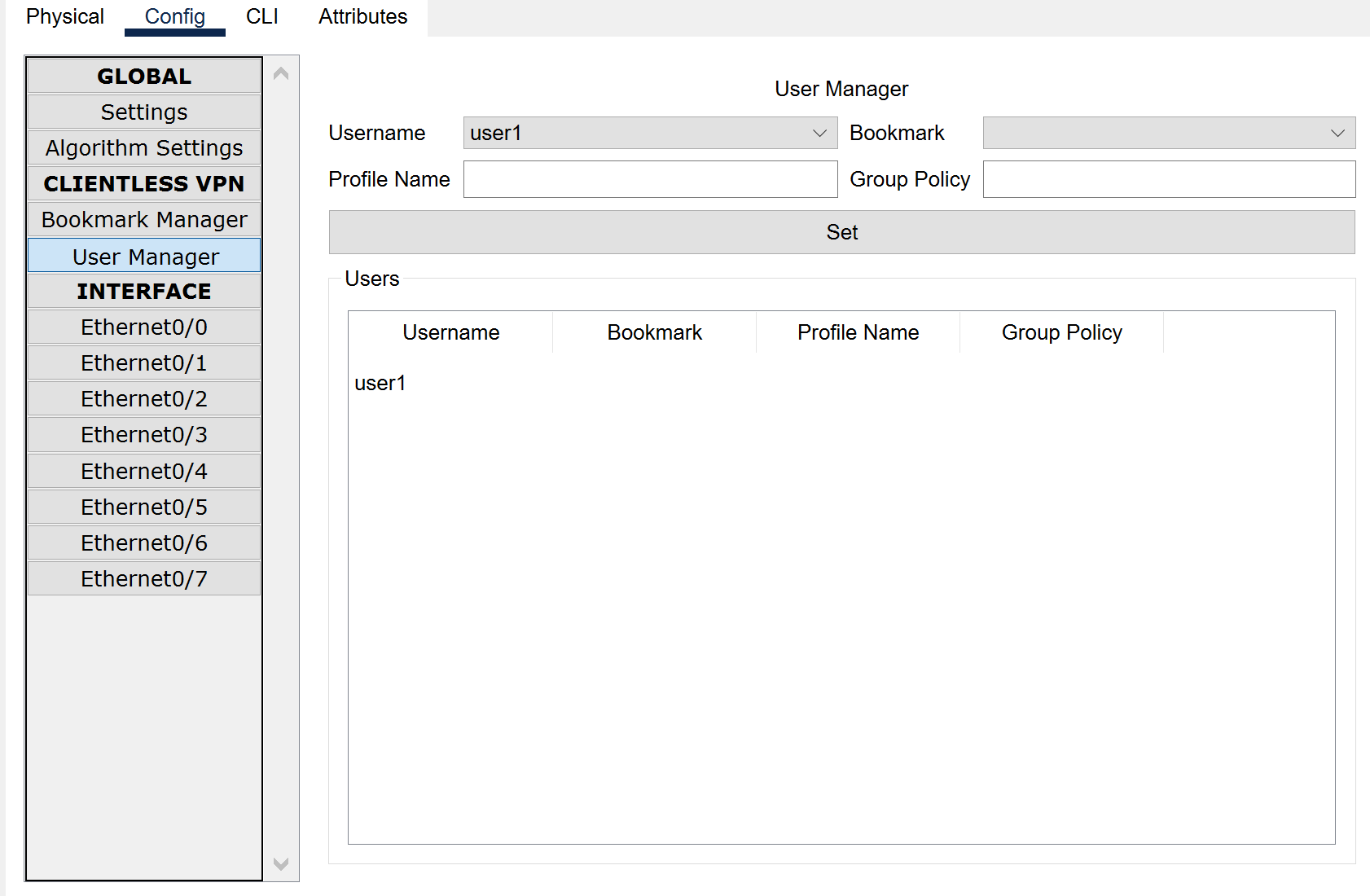
Both ips added

Now adding server site as bookmark:

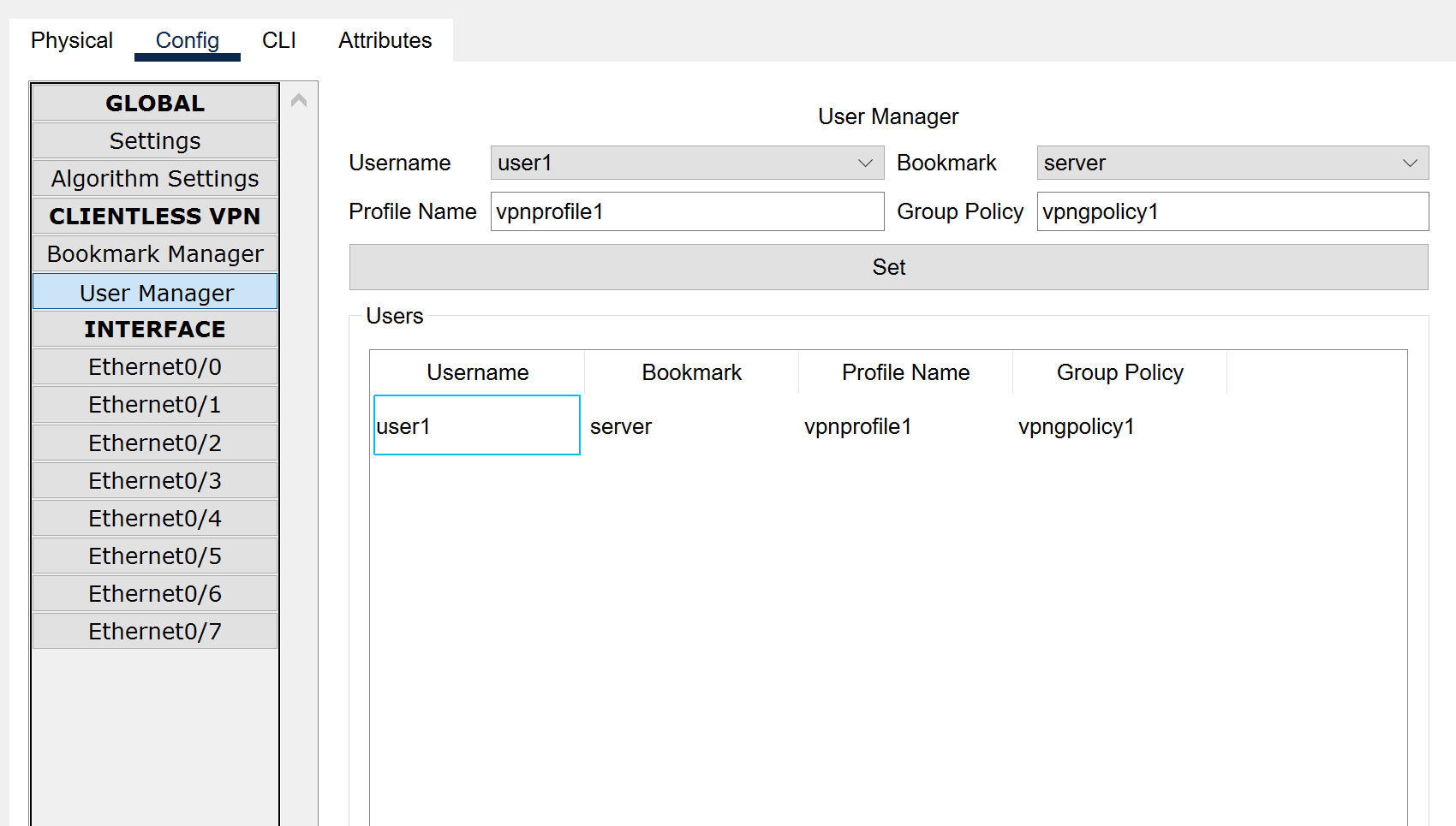


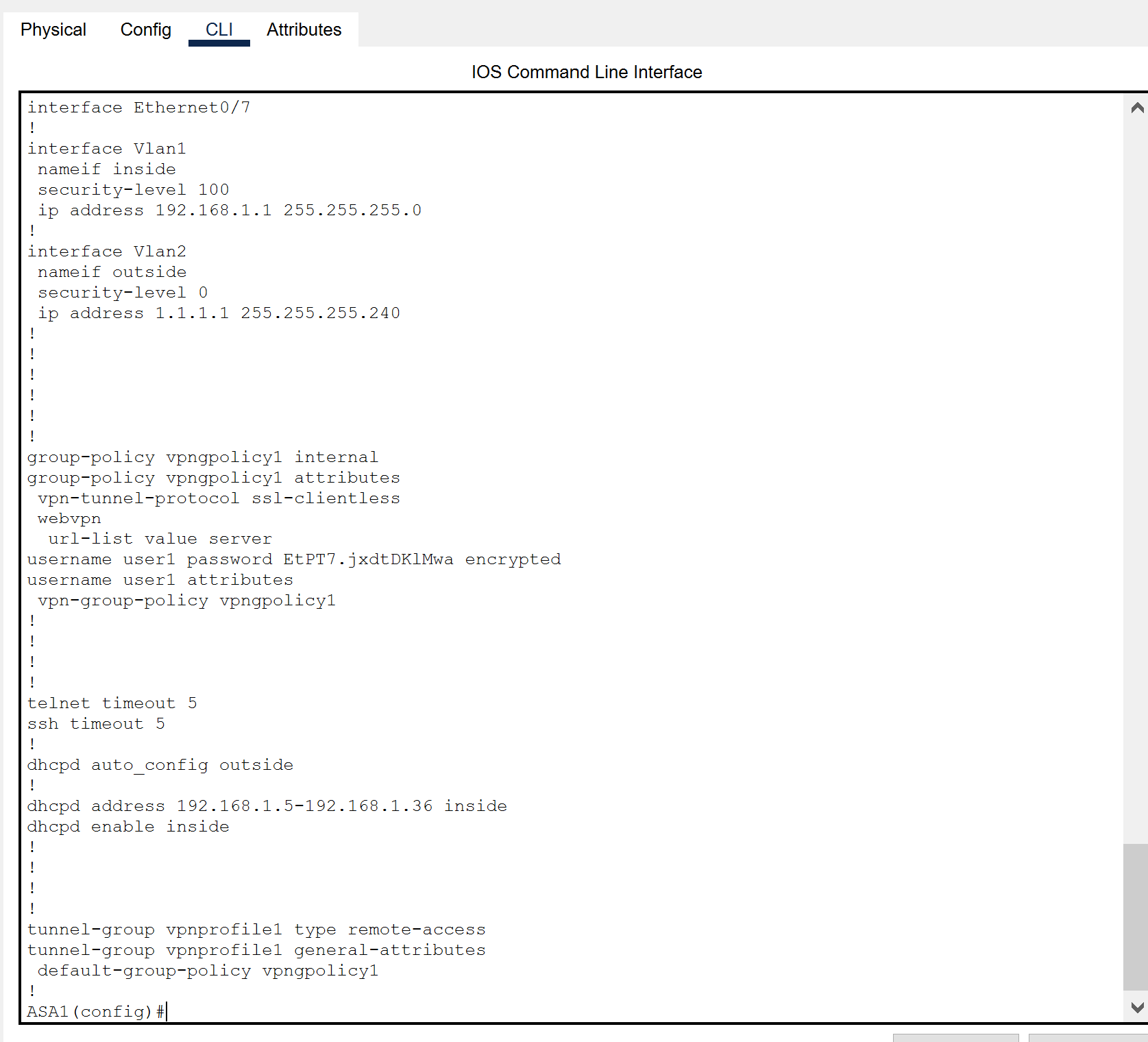
Now adding user into user manager:



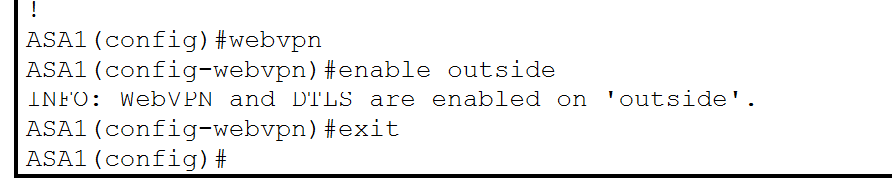


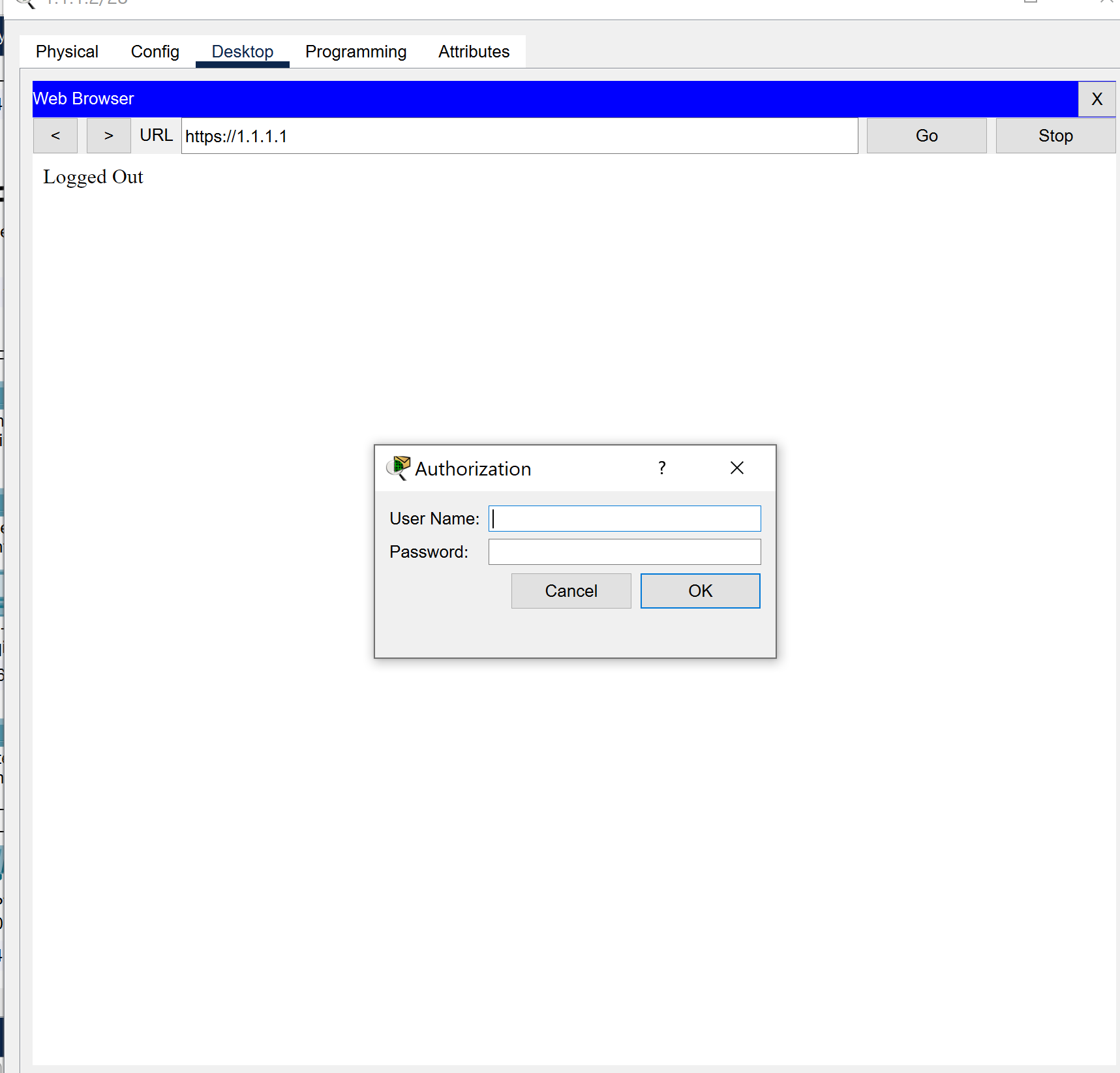
Setting Vpn:



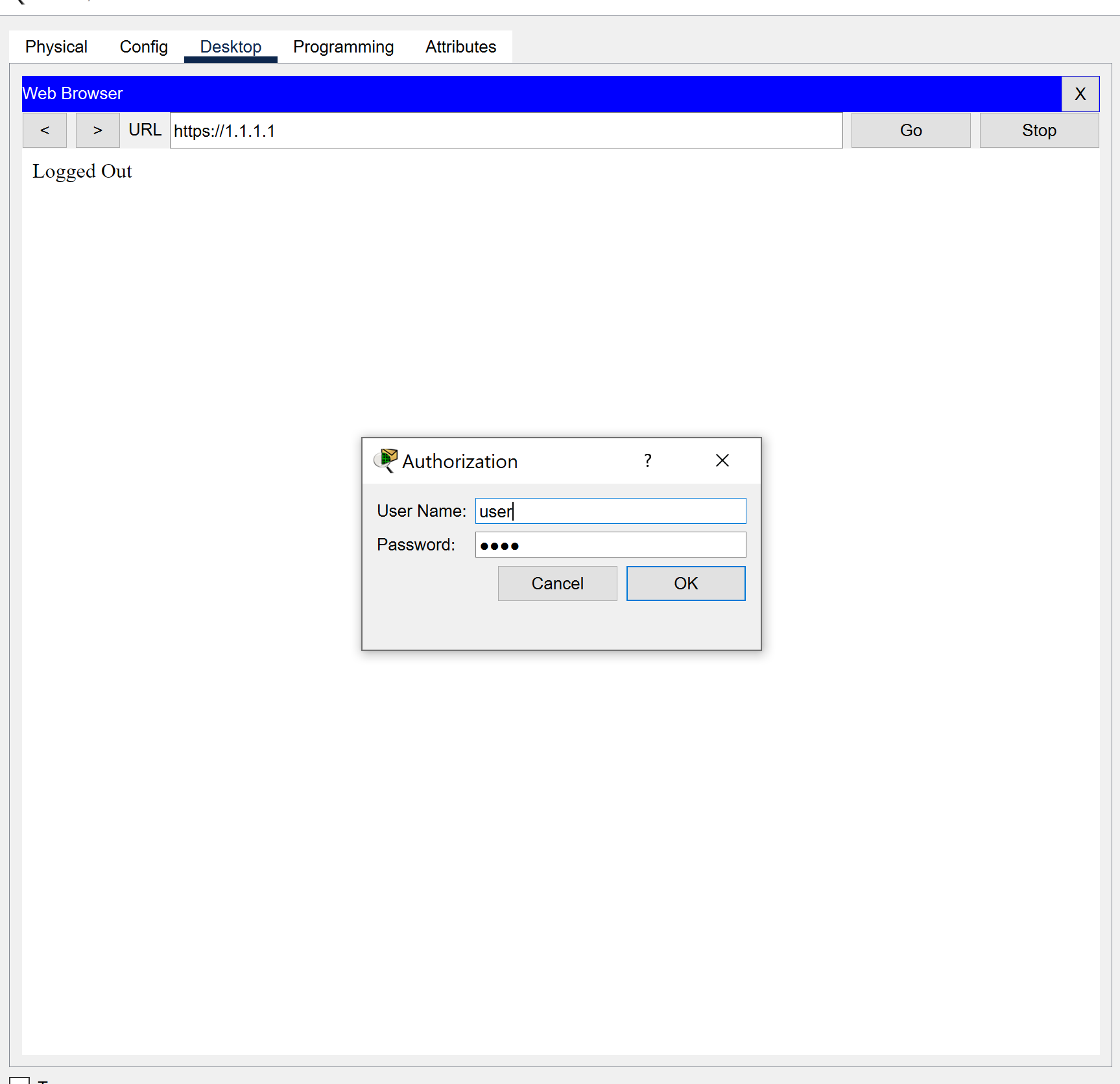


Enable vpn:

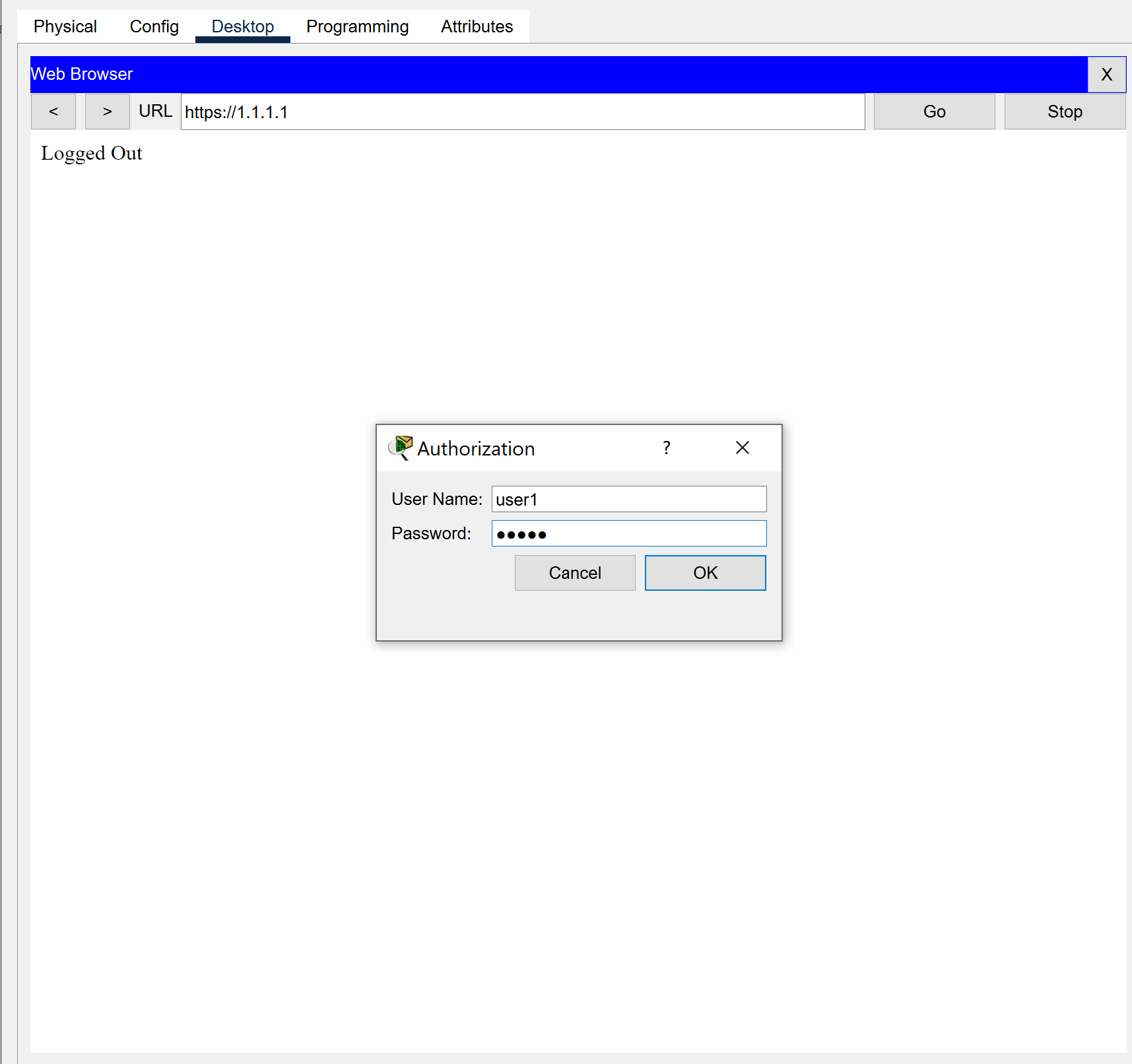
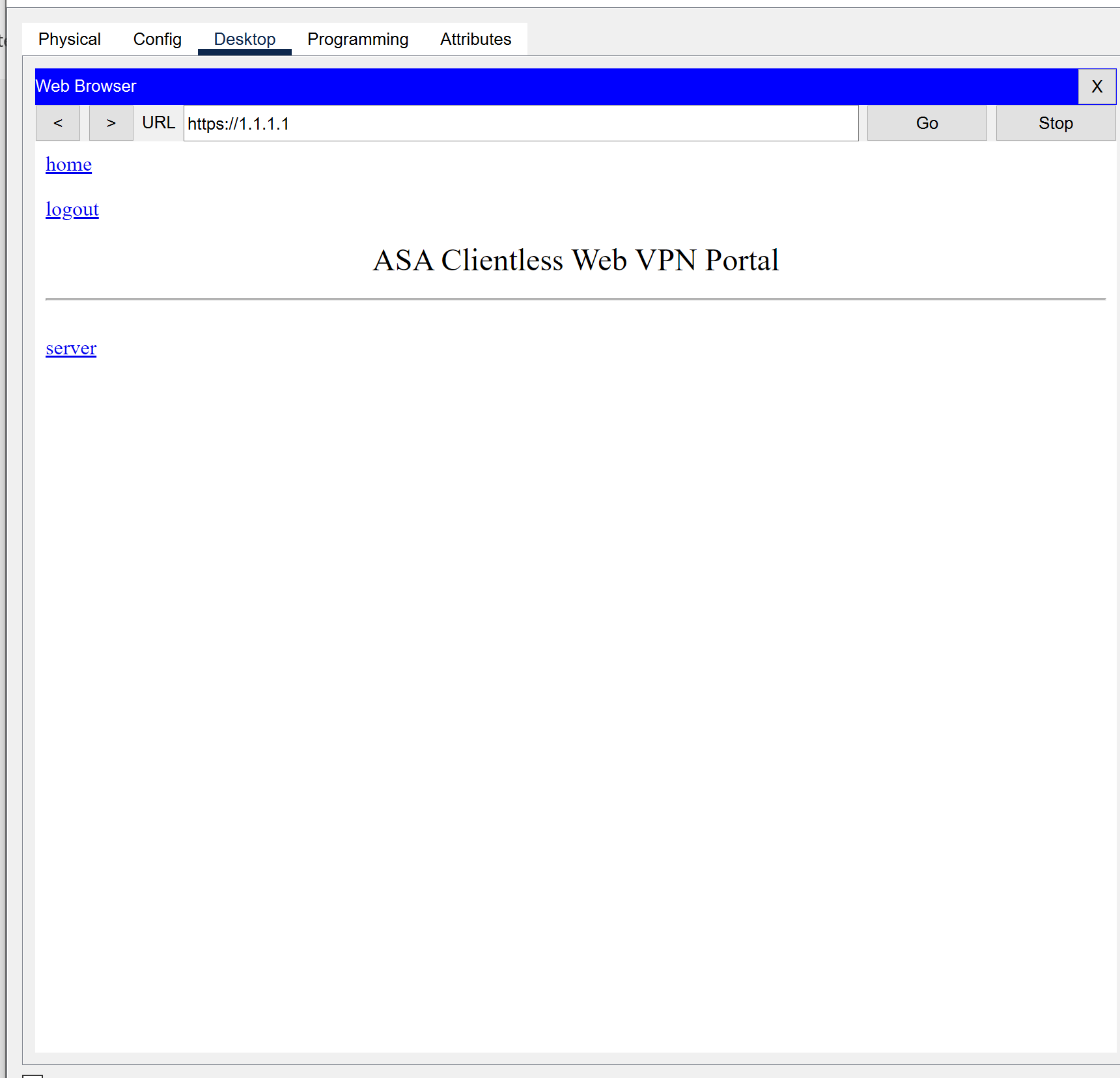


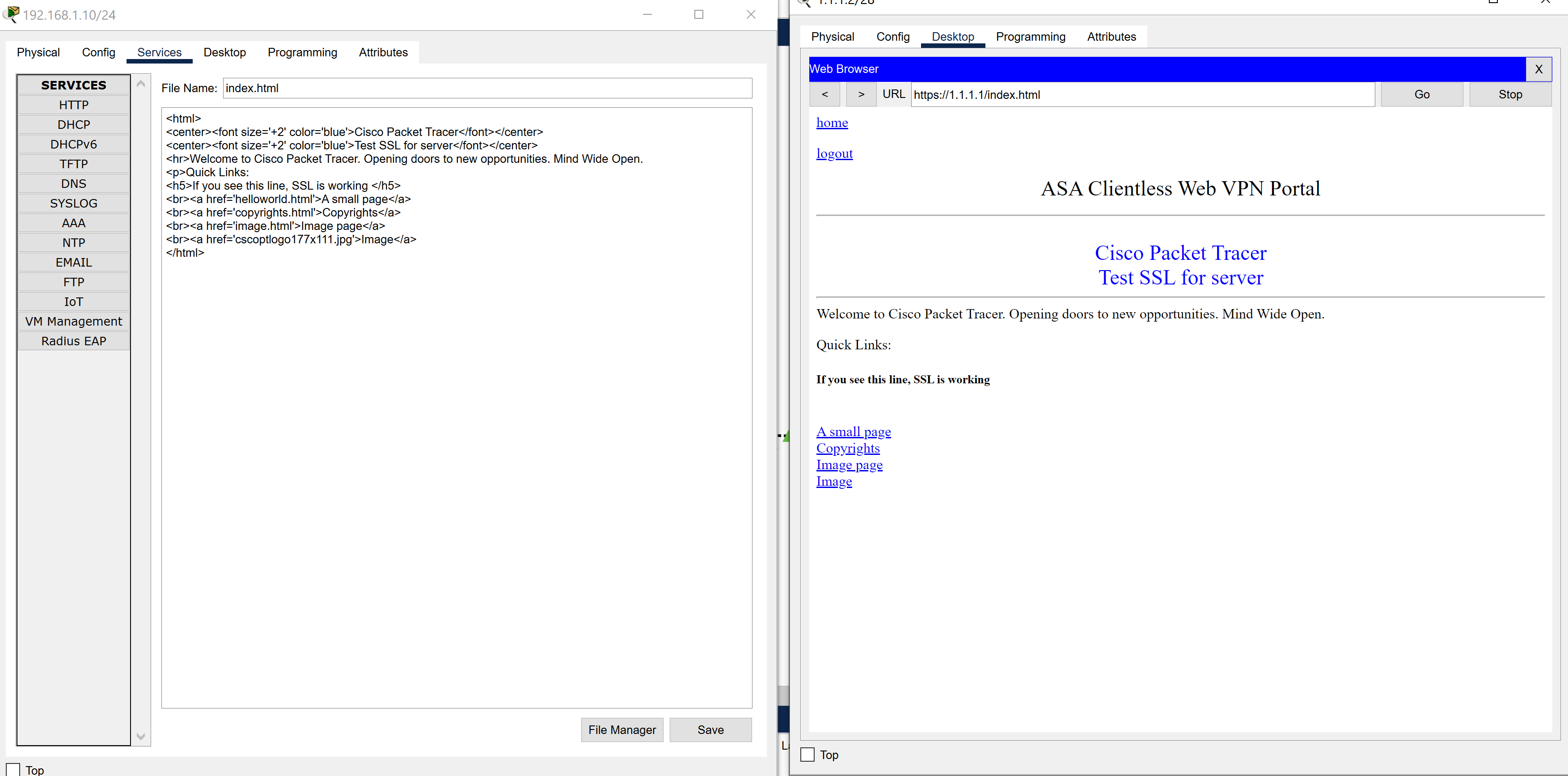
Now access server using password and user:  


Wrong details = no entry



Right details= enter

🡪

Now change page on server side and see if change is reflected to ensure ssl is working:  


**IDPS**

Intrusion Detection and Prevention Systems (IDPS):

- IDPS sensors are deployed strategically within the network to monitor traffic and detect suspicious activities or security policy violations.

- The IDPS effectively detects known attack signatures and anomalous behavior, providing real-time alerts for potential security incidents.

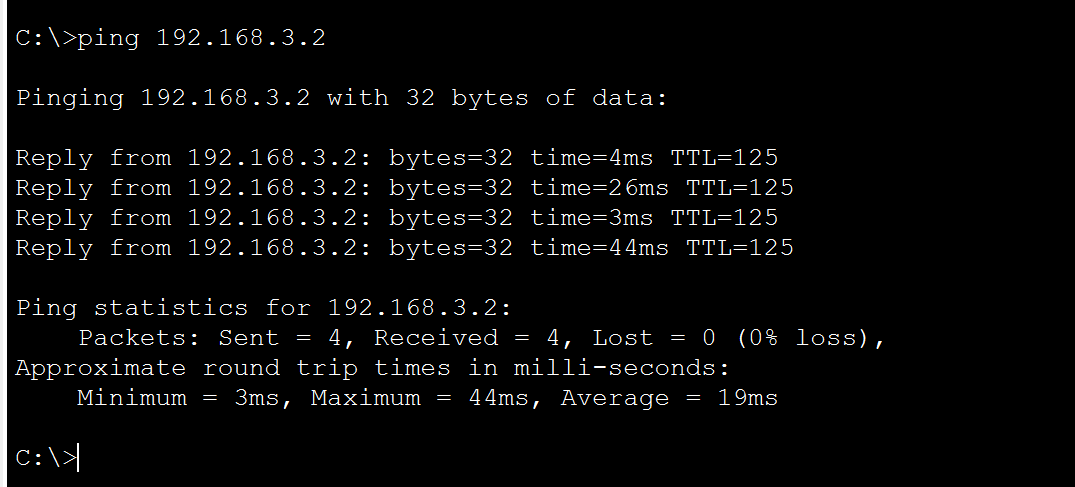
- Continuous monitoring and fine-tuning of IDPS configurations are essential to maintain accuracy and minimize false positives.

First check if ping from inside in ping from outside is working:

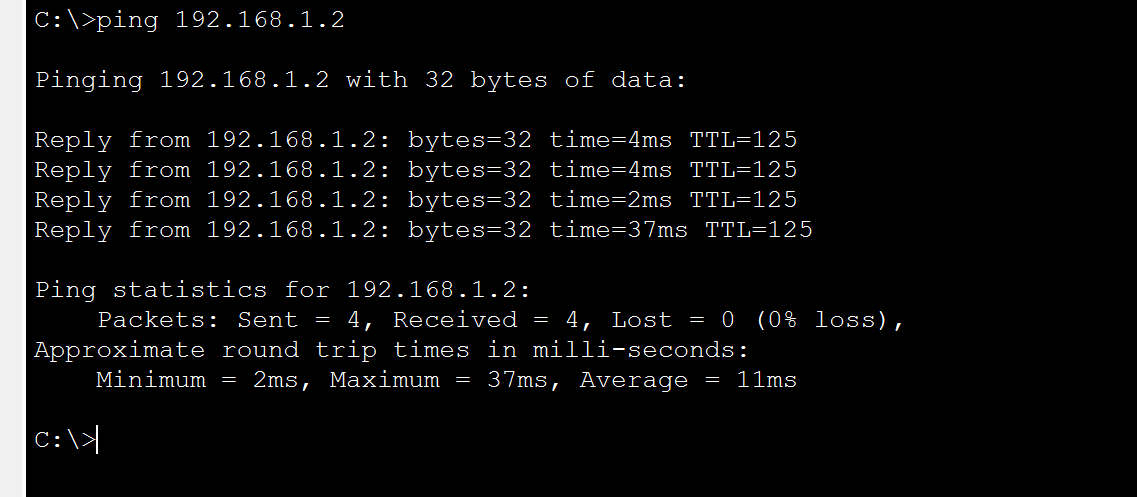
Inside: 128.168.1.2

Outside: 192.168.3.2

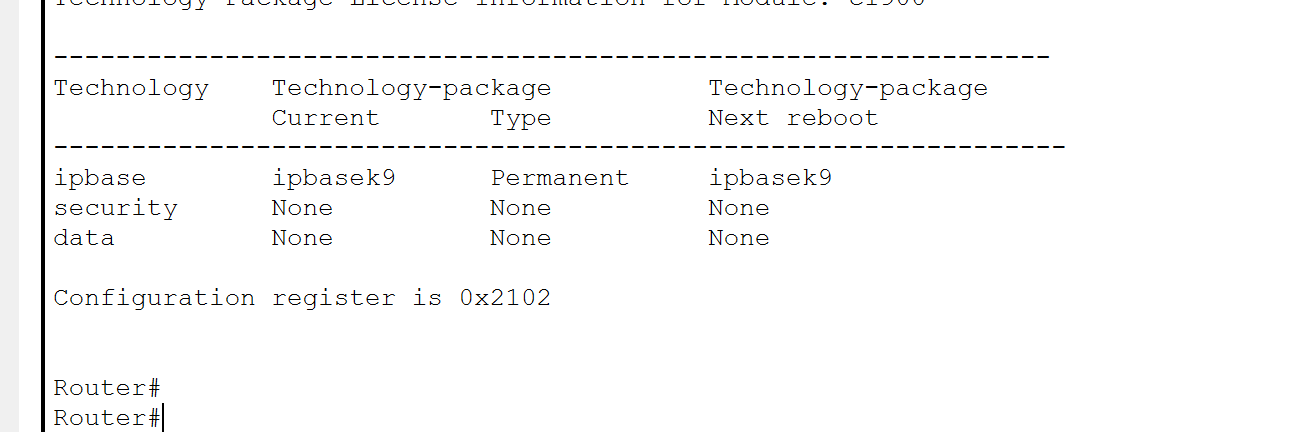
Inside to outside:



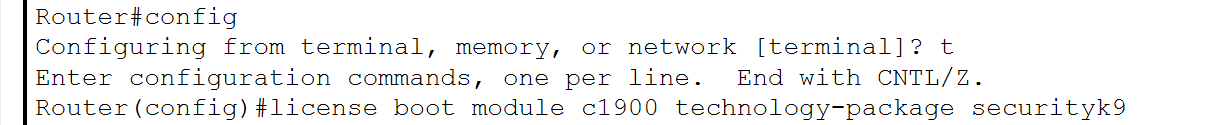
Outside to Inside:



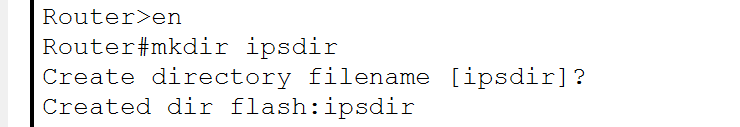
Now check security settings on Router1:-



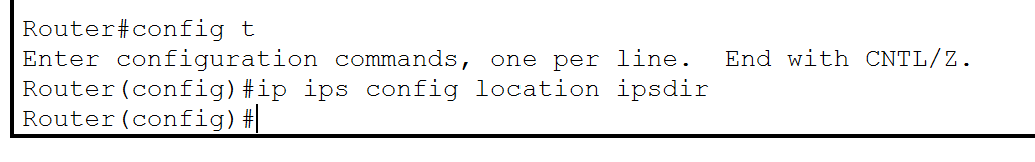
Not Enabled so we will enable security package. Then reboot router once.



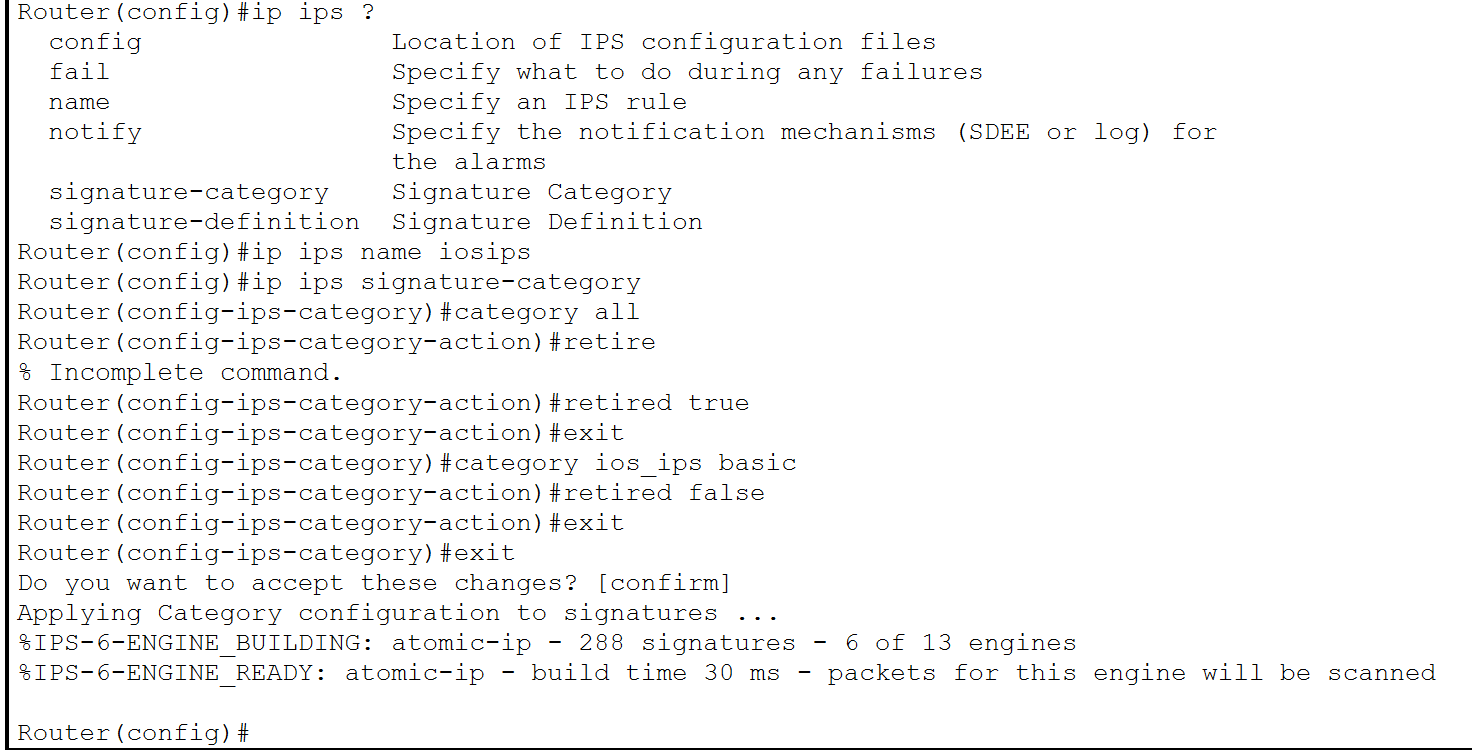
Now make directory for storing detections.



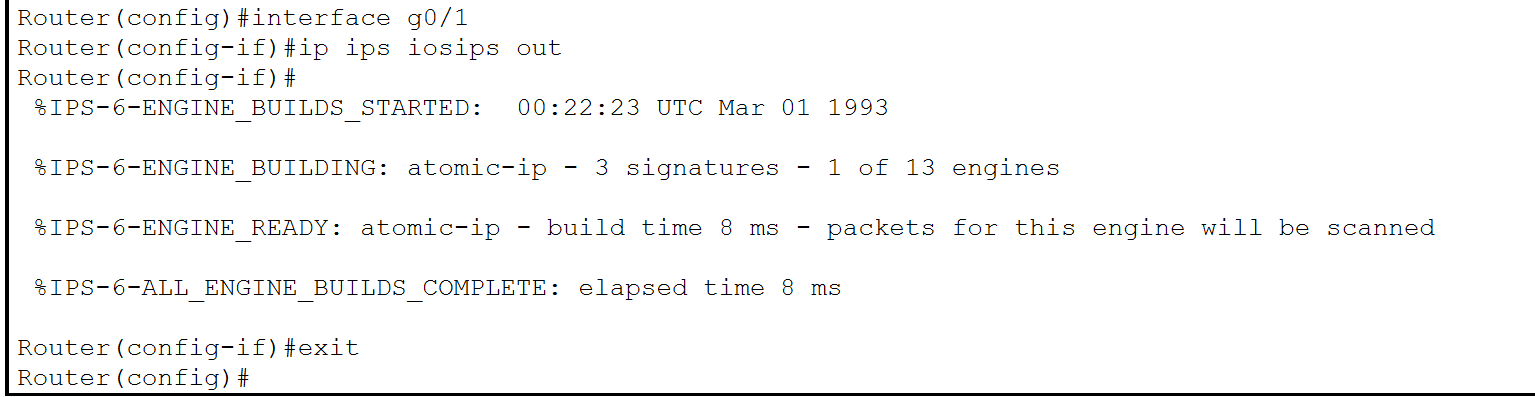
Now configure router to store in this directory.



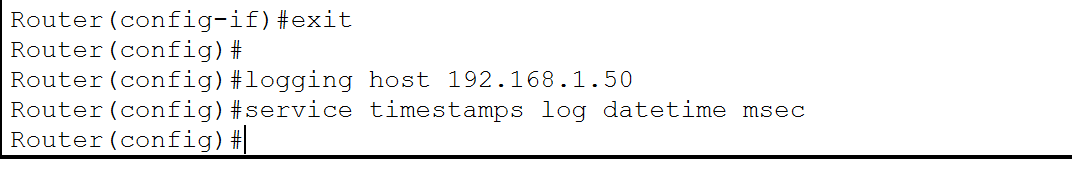
Now specify ips rule:-



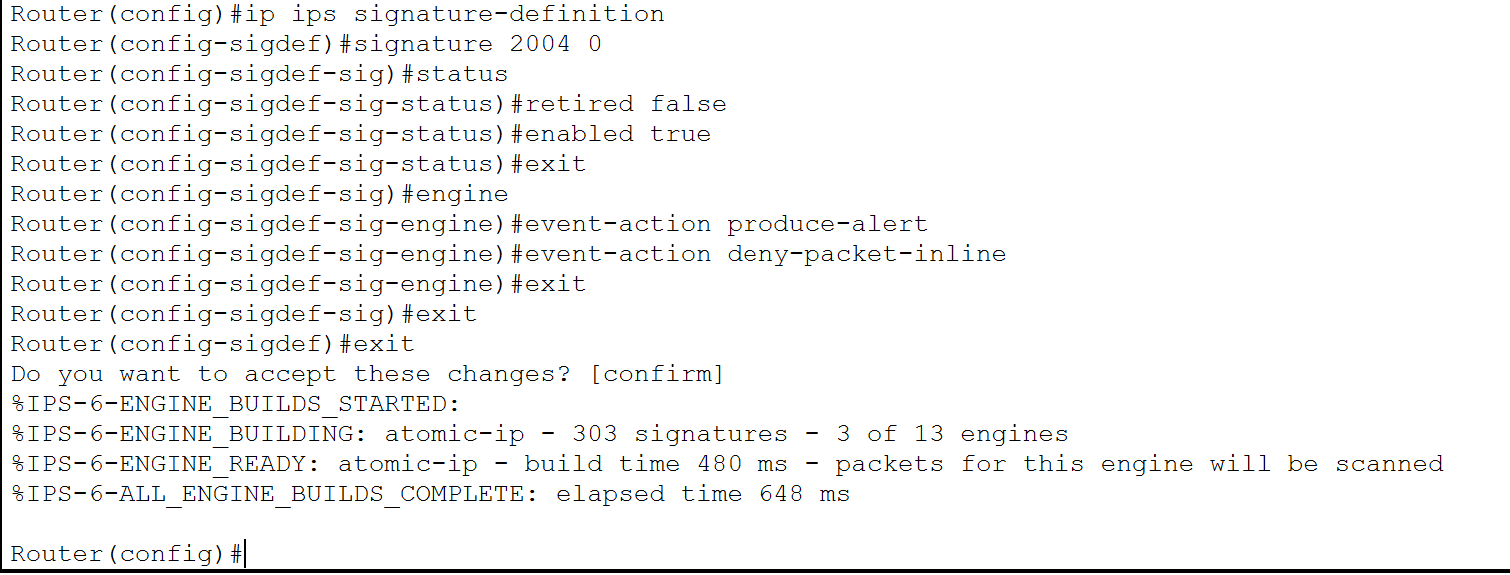
Now apply this rule to g0/1 port so we can scan traffic coming from outside:-



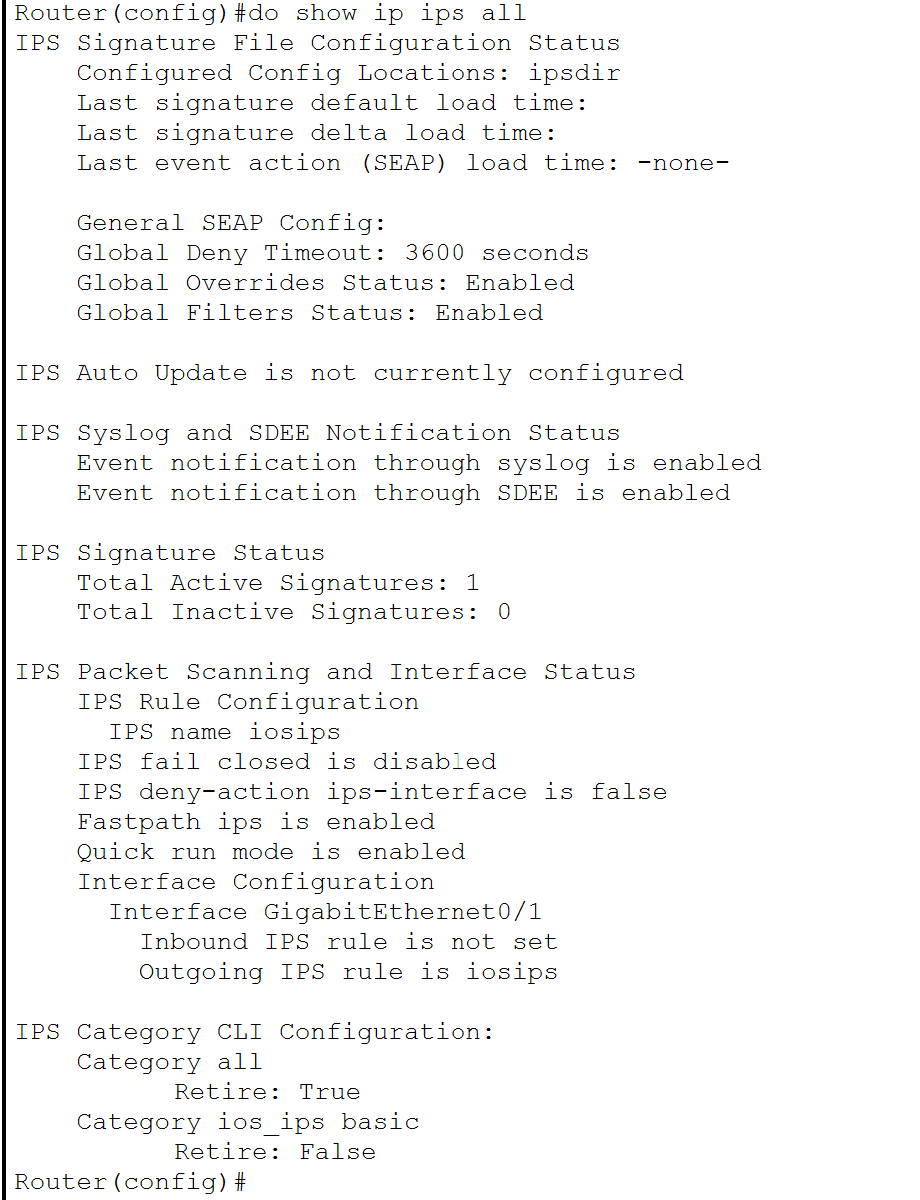
Now configure the traffic logs to be stored in server SysLog:-



Now set the signature statuses and add actions to produce an alert and deny the packet:-



Now check if everything has been done correctly:-



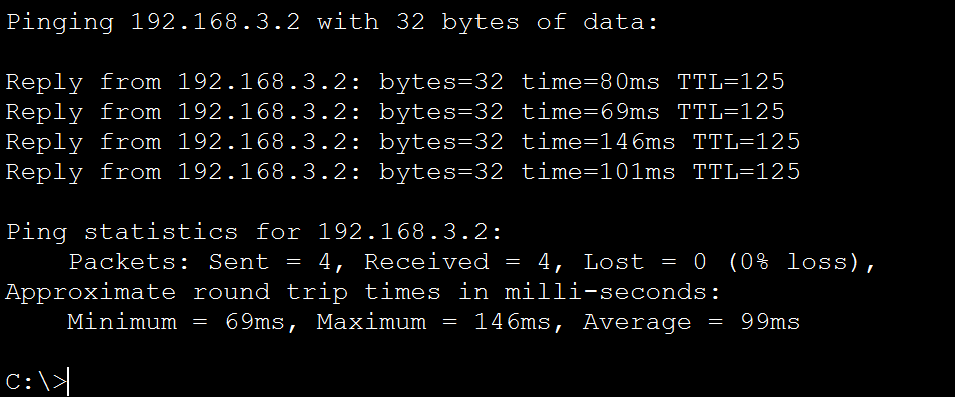
As you can see, location is configured as ipsdir, event notifications are enabled, ip rule for outbound is active. Now traffic can go from inside to outside but not from outside to inside. If we receive from outside on router 1, packet will be denied and an event log will be stored in syslog on our server.

Now Check pinging again:-

Inside: 128.168.1.2

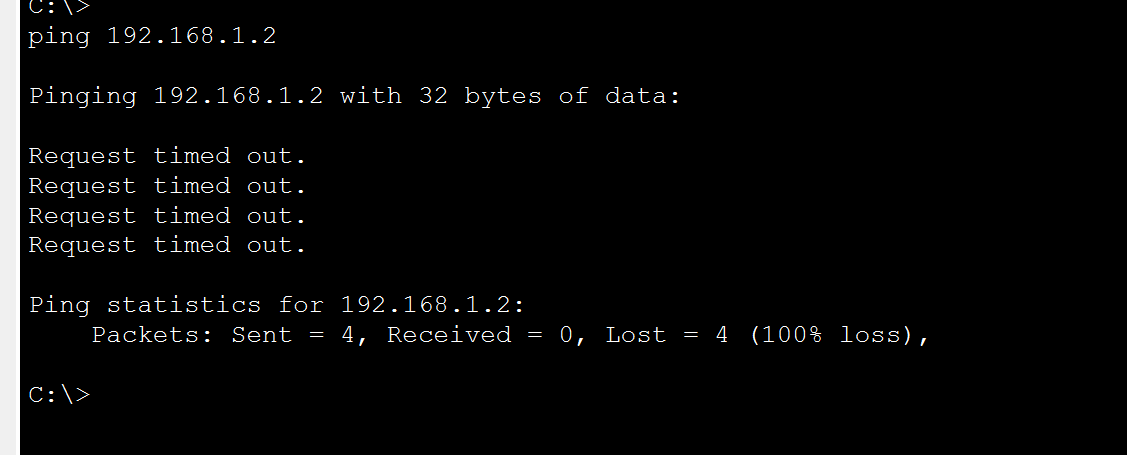
Outside: 192.168.3.2

Inside to outside:



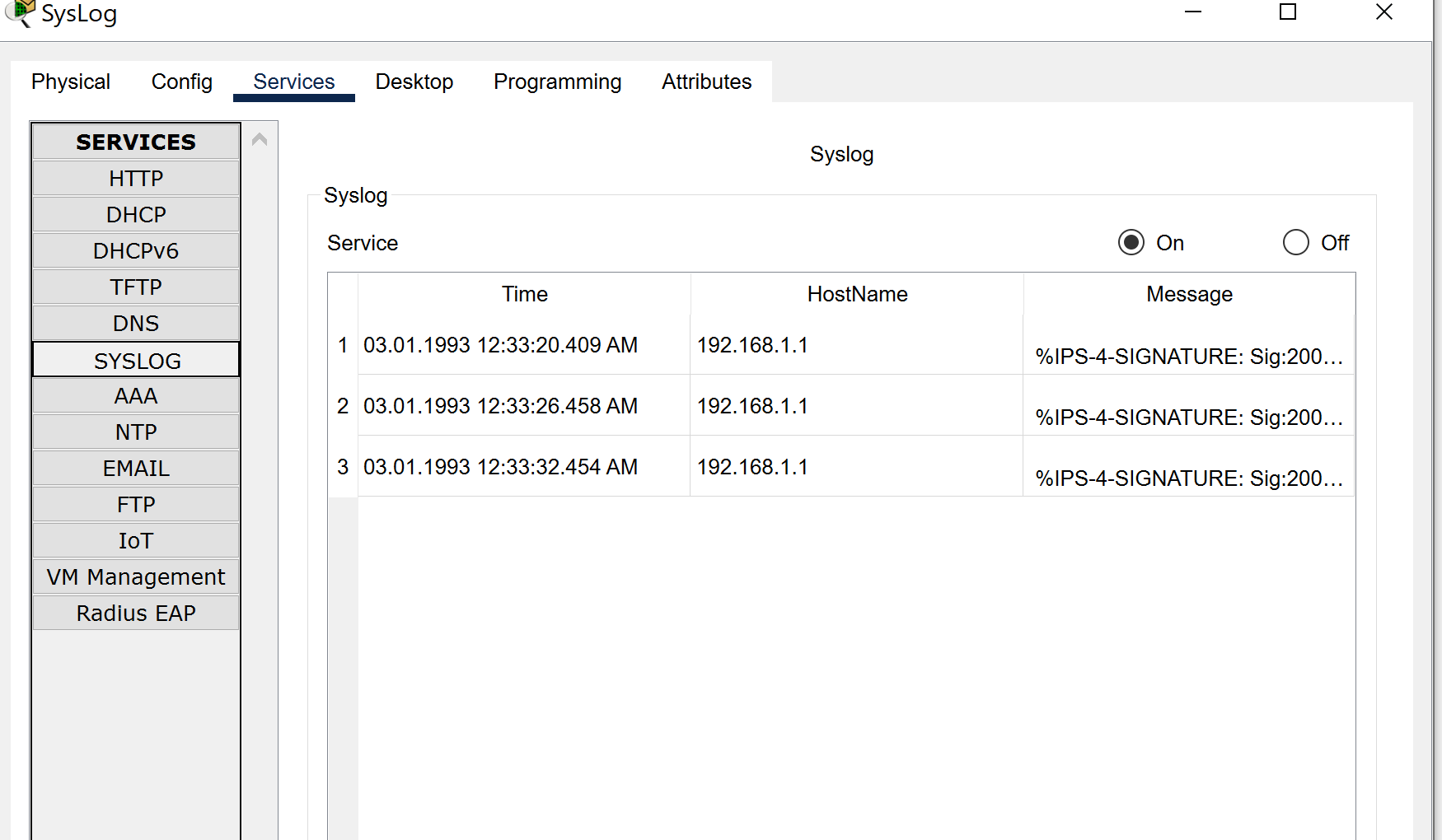
Working!

Outside to Inside:



Doesn’t work!!

Also got stored into our log.



# Monitor network traffic, identify anomalies, and generate alerts for potential security incidents.

**Packet Sniffers:**

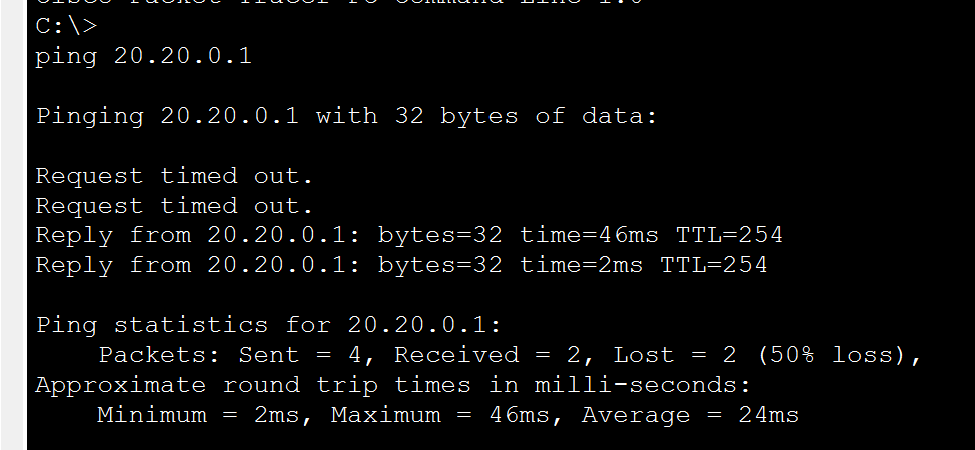
- Packet sniffers are utilized to monitor network traffic and analyze packet contents for signs of malicious activities or security breaches.

- Packet sniffers facilitate the detection of unauthorized network traffic and aid in forensic analysis during security investigations.

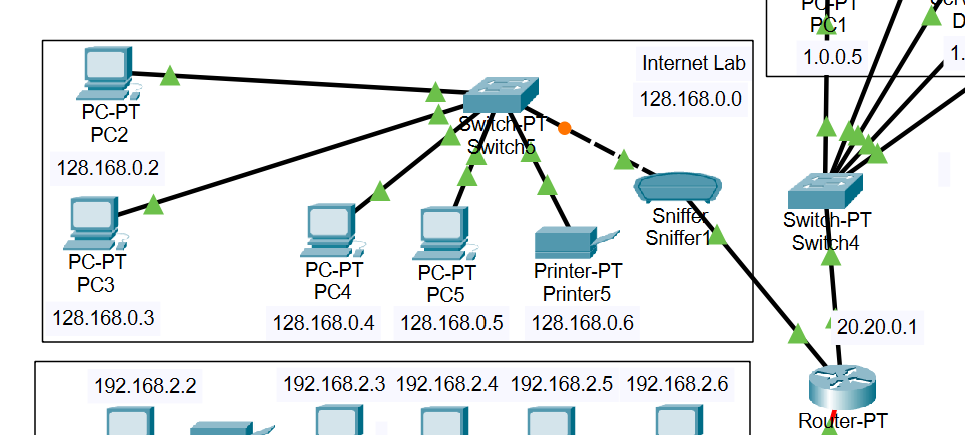
- However, privacy concerns and legal considerations regarding the interception of network traffic must be addressed when deploying packet sniffers.

Tool used: Packet sniffer

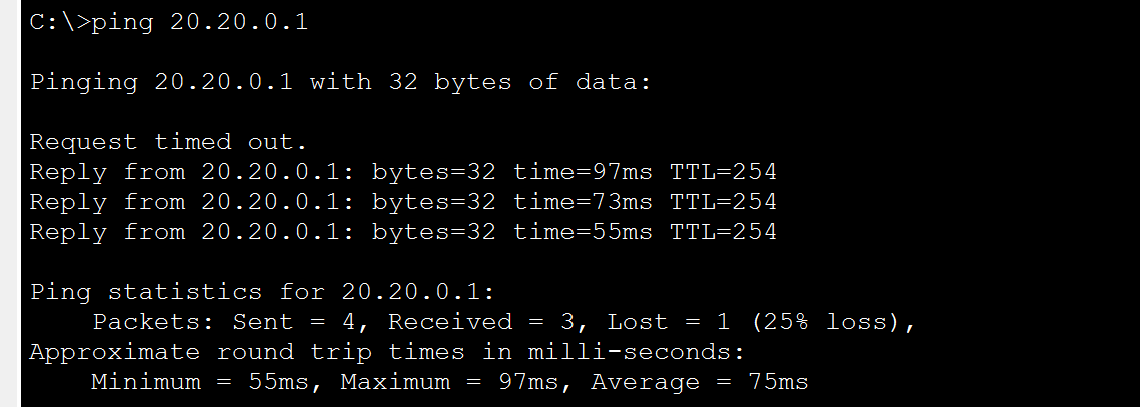
Before adding sniffer:-



Add a sniffing tool between two routers as shown.

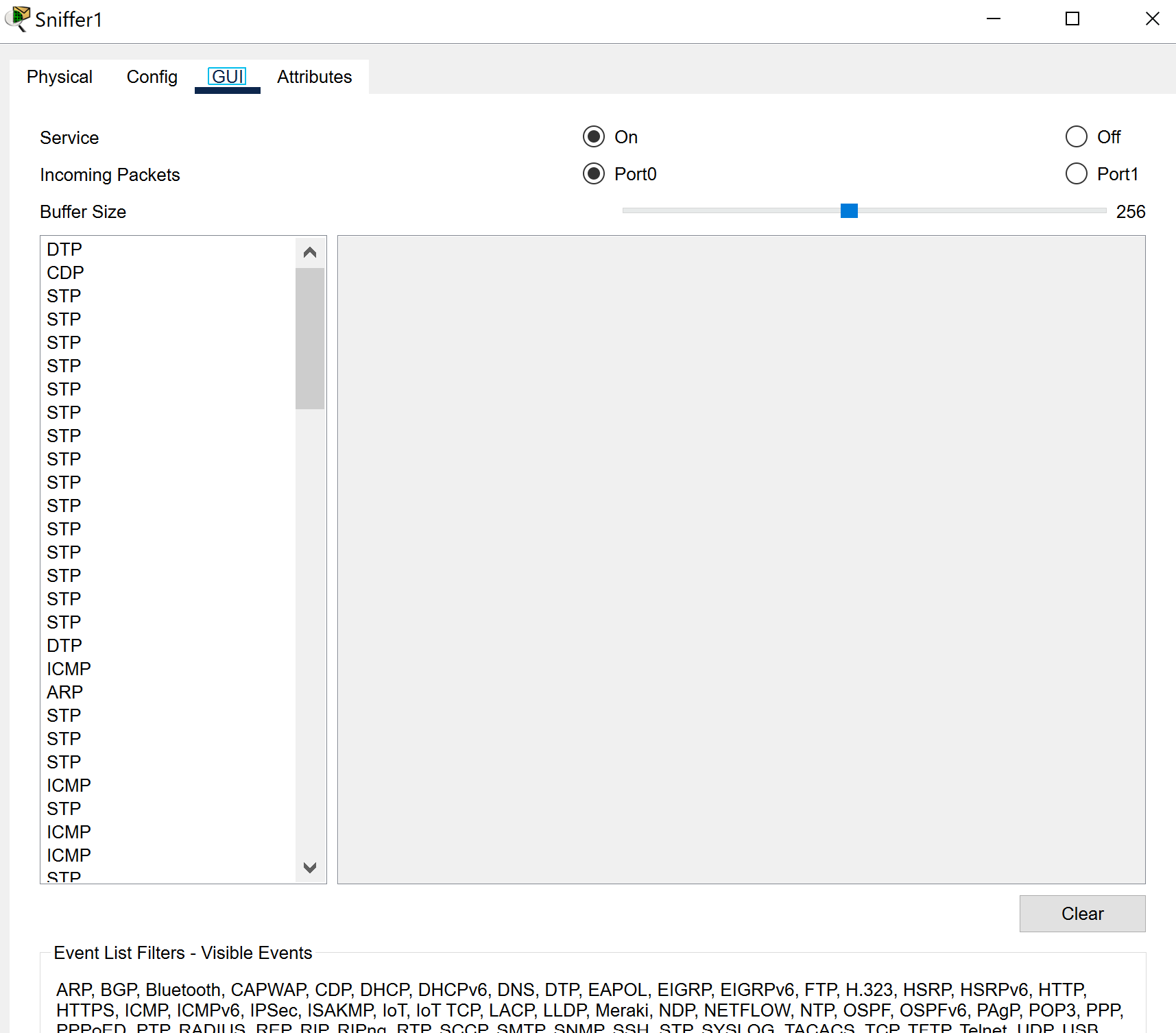


After adding sniffer:-

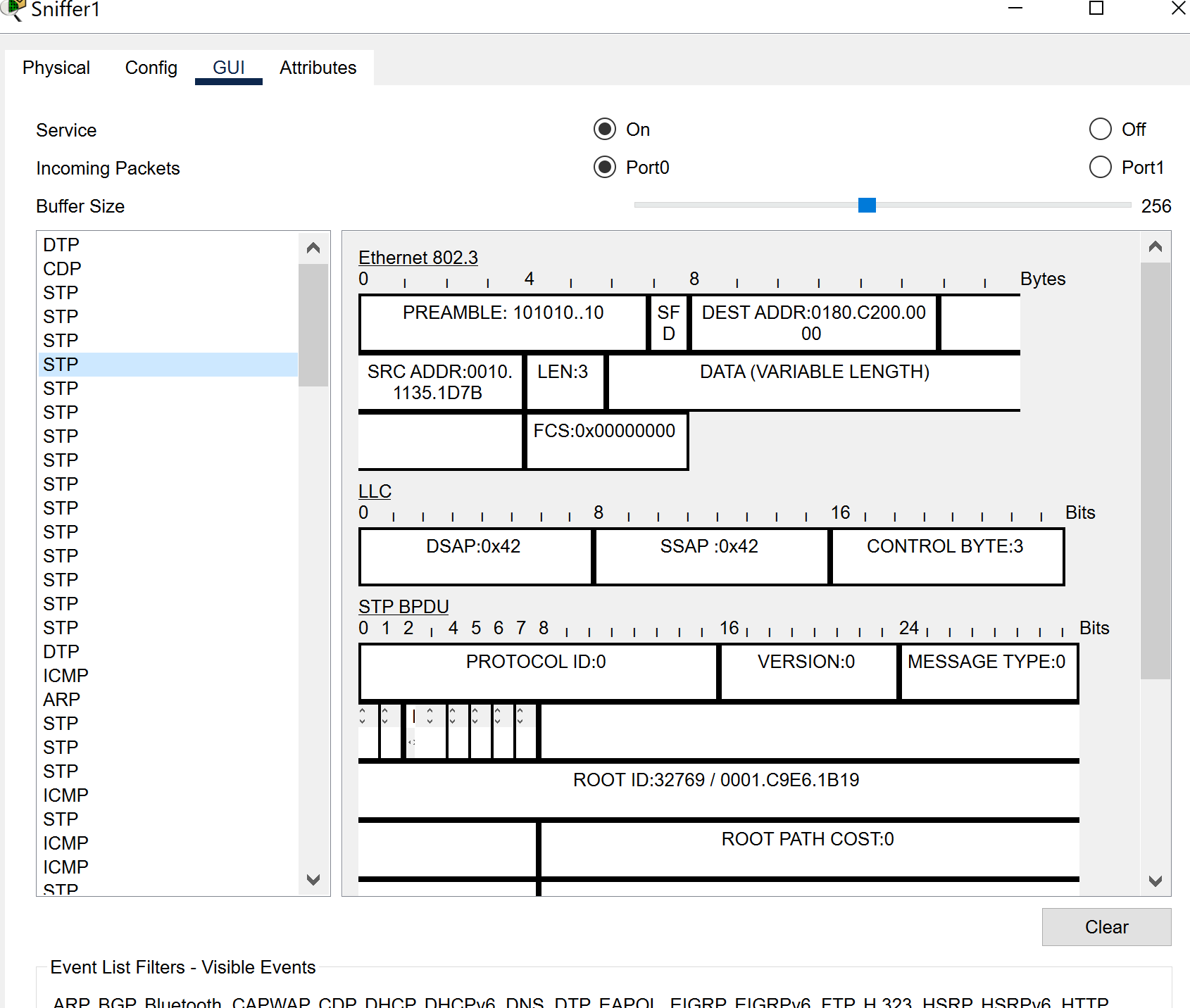


Connection is OK!

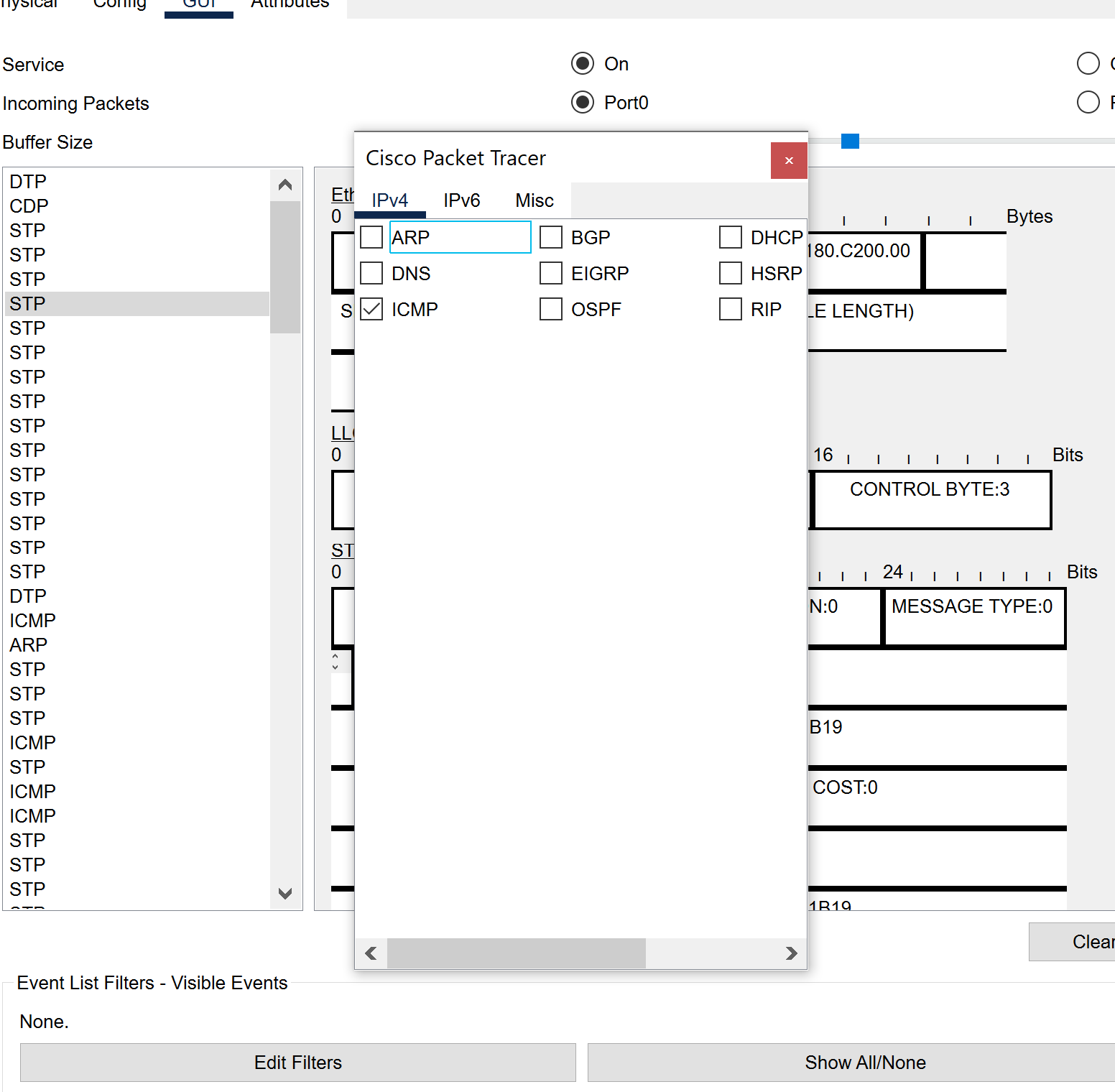
It is showing us traffic as follows:-



You can select a packet and look further into it as follows:-

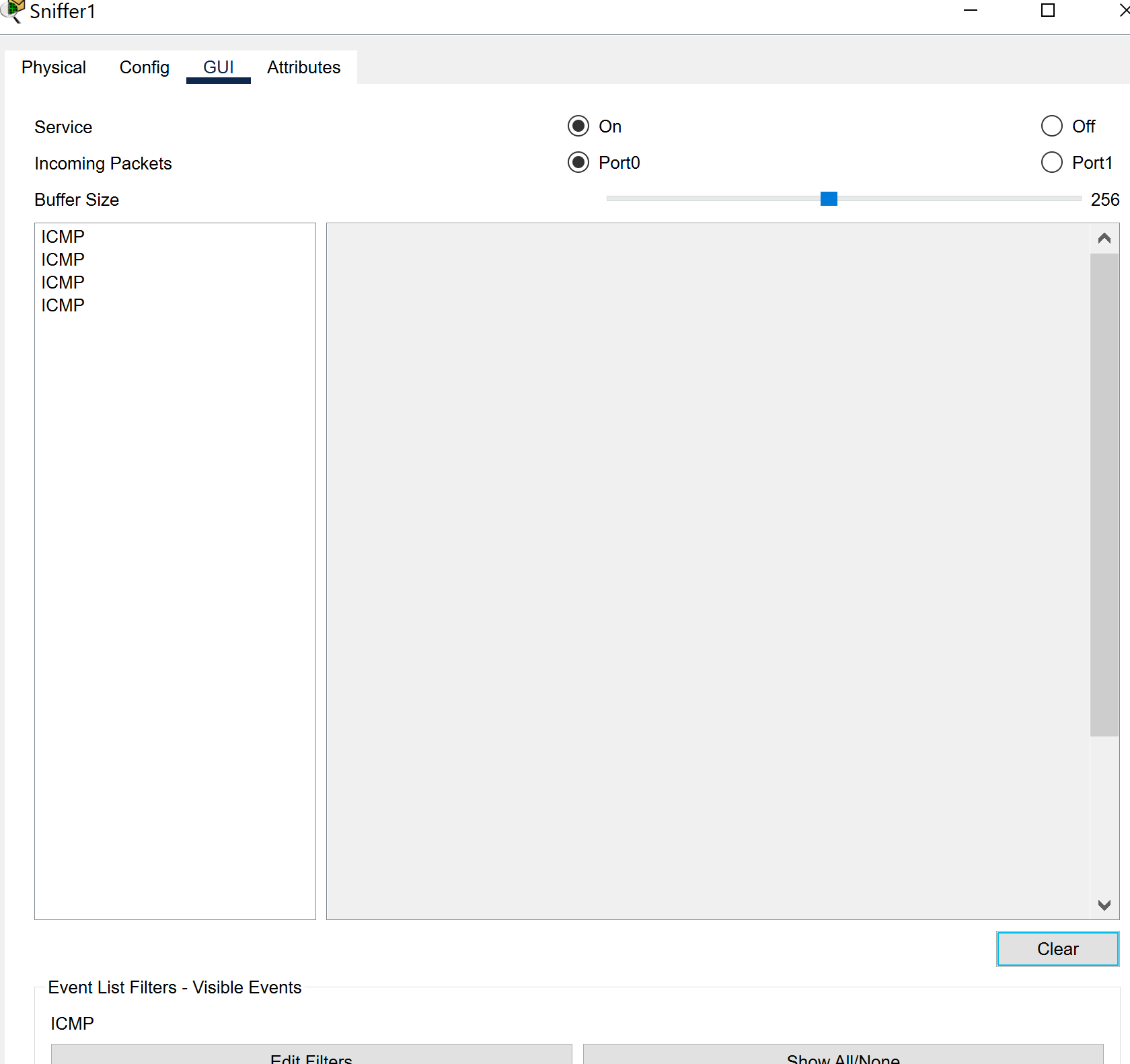


You can also add filters to see only what you want for example to only see ICMP:-



Now clear and ping again.

It now shows only ICMP packets due to filter:-



# Conclusion and Recommendations:

In conclusion, the implemented security measures, including VLAN segmentation, firewalls, IDPS, packet sniffers, and SSL encryption, play a critical role in safeguarding our network against cybersecurity threats. However, to further enhance network security, the following recommendations are proposed:

- Conduct regular audits and reviews of firewall rules, VLAN configurations, and IDPS policies to identify and address security gaps.

- Implement network segmentation best practices to mitigate the risk of VLAN hopping attacks and unauthorized access.

- Enhance monitoring capabilities by integrating packet sniffers with IDPS for comprehensive threat detection and incident response.

- Stay vigilant against emerging threats and vulnerabilities by staying abreast of security advisories and updates related to SSL encryption protocols.