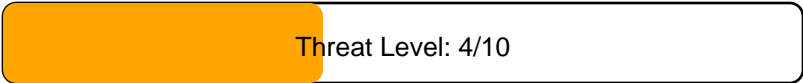


# Network Traffic Security Analysis Report

## Overall Threat Assessment



## Table of Contents

Placeholder for table of contents	0
-----------------------------------	---

# Executive Summary

## Network Traffic Analysis Security ReportExecutive Summary

Two instances of **TCP connect scan activity** detected from internal IP 10.7.5.101 to external IPs (64.185.227.156 and 162.241.169.155).

No direct attack packets (TCP/UDP/ICMP/ARP) observed in the analyzed traffic sample.

Evidence suggests potential network reconnaissance activity targeting external systems.

Risk Assessment

### Critical TCP Scan Patterns:

**High severity:** Repeated SYN flag usage with window sizes >1024 (indicates potential evasion attempt of legacy IDS systems)

**Internal host at risk:** Source IP 10.7.5.101 shows suspicious outbound behavior suggesting possible compromise

### External Targeting Risk:

Connections to non-standard IPs (64.185.227.156 and 162.241.169.155) require verification of business purpose

Threat Observations

### Scan Characteristics:

Both detections (packets #3 and #26) occurred within 3 seconds (19:57:27 - 19:57:30 UTC)

Consistent use of TCP protocol with SYN flag manipulation

Abnormal window size configuration (exceeding 1024 bytes) to bypass basic detection mechanisms

### Operational Context:

Source port/destination port data missing - **limits pattern analysis**

No payload data provided - unable to confirm scan objectives

All detections originated from internal network space (10.7.5.0/24)

Recommendations

### Immediate Containment:

**Quarantine host 10.7.5.101** for forensic analysis

Block outbound connections to detected external IPs at firewall level

### Network Hardening:

Implement TCP window size normalization on border firewalls

Update IDS/IPS signatures to detect SYN scans with window sizes >1024

### Investigation Priorities:

Review DNS logs for domain resolution patterns from 10.7.5.101

Conduct endpoint analysis of source device for rootkits/C2 tools

Validate business justification for communication with external IPs

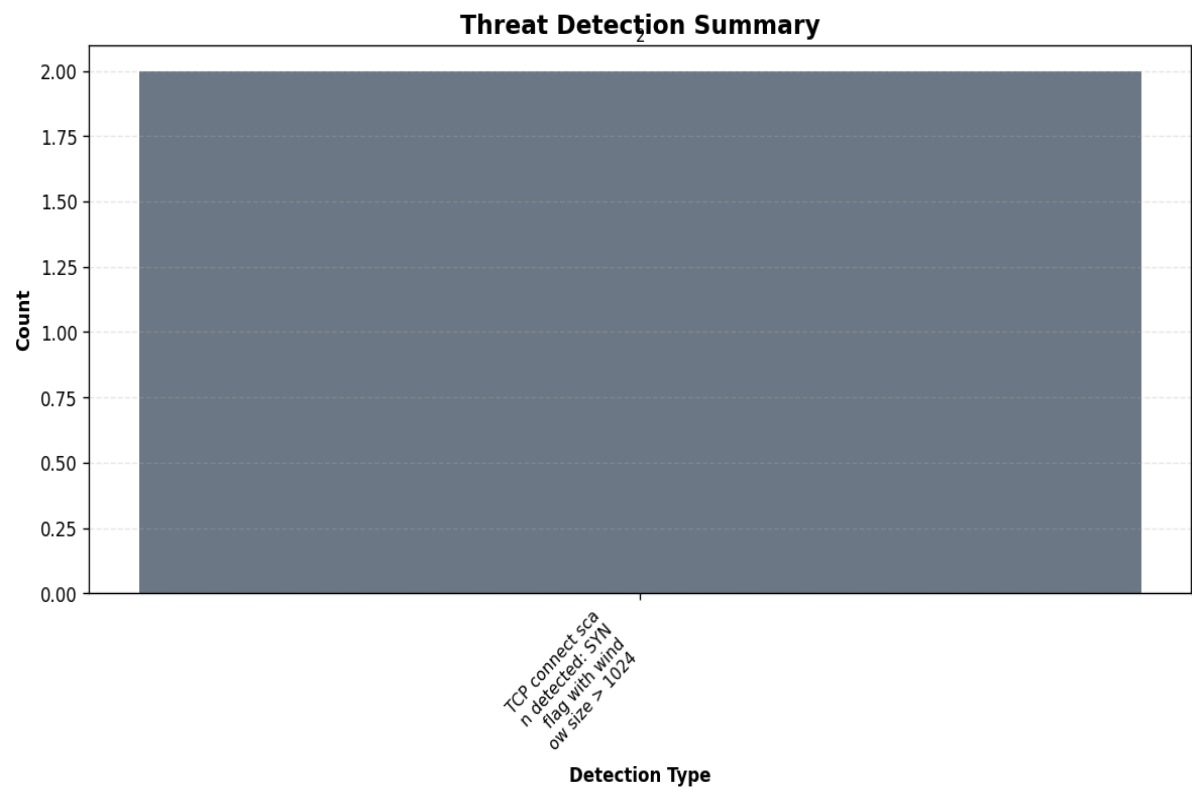
**Preventive Controls:**

Deploy network segmentation for critical internal subnets

Enable egress filtering with explicit allow-list policies

Implement continuous monitoring for SYN flood patterns from internal hosts

# Threat Detection Summary



## Detection Details

Detection Type	Count
TCP connect scan detected: SYN flag with window size > 1024	2

## Source/Destination Analysis

IP Address	As Source	As Destination	Total
10.7.5.101	2	0	2
64.185.227.156	0	1	1
162.241.169.155	0	1	1

***Event Timeline***

Time	Packet #	Protocol	Detection
19:57:27.313	3	TCP	TCP connect scan detected: SYN  flag with window size > 1024
19:57:30.359	26	TCP	TCP connect scan detected: SYN  flag with window size > 1024

## Appendix: Raw Traffic Analysis Data

```
{
  "detection_counts": {
    "TCP connect scan detected: SYN flag with window size > 1024": 2
  },
  "attack_stats": {
    "tcp_packets": 0,
    "udp_packets": 0,
    "icmp_packets": 0,
    "arp_packets": 0
  },
  "top_threats": [
    {
      "packet_number": 3,
      "timestamp": "2023-07-05T19:57:27.313166",
      "minute": "2023-07-05 19:57",
      "protocols": [
        "TCP"
      ],
      "src_ip": "10.7.5.101",
      "dst_ip": "64.185.227.156",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "TCP connect scan detected: SYN flag with window size > 1024"
      ]
    },
    {
      "packet_number": 26,
      "timestamp": "2023-07-05T19:57:30.359542",
      "minute": "2023-07-05 19:57",
      "protocols": [
        "TCP"
      ],
      "src_ip": "10.7.5.101",
      "dst_ip": "162.241.169.155",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "TCP connect scan detected: SYN flag with window size > 1024"
      ]
    }
  ]
}
```

*This report was automatically generated by DeepSeek AI*

*Filename: security\_report\_20250410\_152332.pdf*

*SHA-256 Hash: e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855*

*Generated on: 2025-04-10 15:24:24*