**Cybersecurity Incident Report: Network Traffic Analysis**

**Introduction**  
Upon receiving multiple customer complaints regarding the inability to access the website *yummyrecipesforme.com*, our cybersecurity team initiated an investigation. The error message displayed was *"destination port unreachable."* Initial analysis using *tcpdump* revealed critical issues with DNS resolution, specifically involving UDP and ICMP traffic. This report outlines the findings, analysis, and potential causes of the incident.

### **Part 1: Problem Identification in DNS and ICMP Traffic**

The investigation began with a review of the network traffic logs. The logs showed that when users attempted to access *yummyrecipesforme.com*, their browsers sent DNS queries via the **UDP protocol** to the DNS server at **203.0.113.2:53**. However, instead of a successful resolution, the server responded with an **ICMP error message**: *"udp port 53 unreachable."*

Key observations from the log include:

* **DNS Query Structure**: Each log entry starts with a UDP packet containing a DNS request (e.g., query ID \*35084\* and the *"A?"* flag, indicating a request for an A record mapping).
* **ICMP Error Response**: Following each query, the server returned an ICMP packet stating that port 53 was unreachable. Since port 53 is exclusively used for DNS, this suggests a fundamental failure in DNS service delivery.

**Interpretation**:  
The consistent ICMP errors indicate that the DNS server is either **unavailable** or **not accepting requests on port 53**. This could stem from:

* A **server outage** (e.g., crash, maintenance, or DoS attack).
* A **network misconfiguration** (e.g., firewall blocking port 53).

The presence of DNS query flags (*"A?"*) confirms that the requests were legitimate, ruling out client-side issues.

### **Part 2: Incident Analysis and Root Cause Investigation**

**Timeline and Initial Reports**  
The issue was first detected today at **1:24 p.m.** (log timestamp: \*13:24:32.192571\*). Customers reported the *"destination port unreachable"* error when attempting to load the website. The cybersecurity team was alerted and began analyzing traffic using *tcpdump*.

**Current Status**  
The team is actively investigating the DNS server and firewall configurations to identify the root cause. Service restoration is pending further diagnostics.

**Findings from Packet Analysis**  
The *tcpdump* logs revealed:

1. **Outbound UDP Packets**: DNS queries from user devices to \*203.0.113.2:53\*.
2. **Inbound ICMP Errors**: Every query was met with *"udp port 53 unreachable,"* confirming the server’s inability to process requests.

**Next Steps**  
To resolve the issue, the team will:

1. **Verify DNS Server Status**:
   1. Check if the server is online and responsive.
   2. Review logs for crashes or unusual activity (e.g., traffic spikes).
2. **Audit Firewall Rules**:
   1. Ensure port 53 is not blocked by a misconfigured rule.
3. **Assess for DoS Attacks**:
   1. Analyze traffic patterns for signs of flooding or malicious payloads.

**Suspected Root Causes**  
Two primary hypotheses are under consideration:

1. **Denial-of-Service Attack**:
   1. An attacker may have flooded the DNS server, rendering it unresponsive.
2. **Configuration Error**:
   1. A recent firewall update or DNS server misconfiguration might have inadvertently blocked port 53.

### **Conclusion and Recommendations**

The inability to reach port 53 on the DNS server has disrupted access to *yummyrecipesforme.com*. While the exact cause is still under investigation, the evidence points to either a **DoS attack** or a **configuration error**.

**Recommended Actions**:

1. **Immediate**:
   1. Restart the DNS server if it is unresponsive.
   2. Temporarily whitelist port 53 in the firewall to test connectivity.
2. **Long-term**:
   1. Implement DoS protection mechanisms (e.g., rate limiting).
   2. Document firewall changes to prevent future misconfigurations.

**Final Notes**:  
Further diagnostics are required to confirm the root cause. The team will provide updates upon completing the firewall audit and server health checks.