## **DNS and ICMP Traffic Analysis Report**

### **Summary of the Problem Found in the DNS and ICMP Traffic Log**

#### **Summary of the Problem:**

* **Affected Protocol:** UDP
* **ICMP Error Message:** "udp port 53 unreachable"
* **Affected Port:** 53 (used for DNS services)
* **Most Likely Issue:** The DNS server was not available or was not listening on port 53.

#### **DNS and ICMP Logs:**

13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)

13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)

13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)

13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 150

### **Analysis of the Data and Proposed Solution**

#### **Analysis of the Data:**

* **Incident Time:** 13:24:32, 13:26:32, and 13:28:32
* **Detection of the Incident:** Clients reported being unable to access [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com) and observed the "destination port unreachable" error.
* **IT Team Actions:**
  + Verified the website and confirmed the error.
  + Used tcpdump to capture network traffic and analyze packets.
* **Key Findings:**
  + UDP requests from IP 192.51.100.15 to DNS server 203.0.113.2 showed that UDP port 53 was unreachable.
  + ICMP responses confirmed that port 53 was not available on the DNS server.

#### **Proposed Solution:**

1. **Verify the DNS Server:**
   * Ensure that the DNS server at IP 203.0.113.2 is operational and listening on port 53.
   * Check DNS server logs for possible configuration issues or service failures.
2. **Check Network Configuration:**
   * Confirm that there are no firewall blocks preventing access to port 53.
   * Review firewall rules on the DNS server and within the company's network to ensure UDP traffic to port 53 is allowed.
3. **Update and Restart DNS Service:**
   * If the DNS server was inactive, restart the service and check if the issue persists.
   * Ensure that the DNS server is properly configured to handle name resolution requests.
4. **Monitor Traffic:**
   * Continue monitoring DNS and ICMP traffic to ensure the issue is resolved and does not recur.

### **Conclusion**

The analysis of DNS and ICMP traffic indicates that the main issue was the DNS server at IP 203.0.113.2 not being available on UDP port 53, which prevented the resolution of the domain name [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com). The solution involves verifying and correcting the availability of the DNS server and its network configuration, as well as ensuring that traffic to port 53 is allowed. After implementing these solutions, continuous monitoring is recommended to confirm that the issue is fully resolved and does not reoccur.

## **Reporte de Análisis de Tráfico DNS e ICMP (spanish)**

### **Resumen del Problema en el Tráfico DNS e ICMP**

#### **Resumen del Problema:**

* **Protocolo Afectado:** UDP
* **Mensaje de Error ICMP:** "udp port 53 unreachable"
* **Puerto Afectado:** 53 (usado para servicios DNS)
* **Causa Probable:** El servidor DNS no estaba disponible o no estaba escuchando en el puerto 53.

#### **Registros DNS e ICMP:**

13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)

13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)

13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)

13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 150

### **Análisis de los Datos y Solución Propuesta**

#### **Análisis de los Datos:**

* **Hora del Incidente:** 13:24:32, 13:26:32, y 13:28:32
* **Detección del Incidente:** Clientes reportaron la imposibilidad de acceder a [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com) y observaron el error "puerto de destino inalcanzable."
* **Acciones del Equipo de TI:**
  + Se verificó el sitio web y se confirmó el error.
  + Se utilizó tcpdump para capturar el tráfico de red y analizar los paquetes.
* **Hallazgos Clave:**
  + Las solicitudes UDP desde la IP 192.51.100.15 al servidor DNS 203.0.113.2 indicaron que el puerto UDP 53 estaba inalcanzable.
  + Respuestas ICMP confirmaron que el puerto 53 no estaba disponible en el servidor DNS.

#### **Solución Propuesta:**

1. **Verificar el Servidor DNS:**
   * Asegurarse de que el servidor DNS 203.0.113.2 esté operativo y escuchando en el puerto 53.
   * Revisar los registros del servidor DNS para detectar posibles problemas de configuración o fallos en el servicio.
2. **Revisar la Configuración de Red:**
   * Confirmar que no haya bloqueos de firewall que impidan el acceso al puerto 53.
   * Verificar las reglas de firewall en el servidor DNS y en la red de la empresa para asegurar que el tráfico UDP hacia el puerto 53 esté permitido.
3. **Actualizar y Reiniciar el Servicio DNS:**
   * Si el servidor DNS estaba inactivo, reiniciar el servicio y verificar si el problema persiste.
   * Asegurarse de que el servidor DNS esté correctamente configurado para manejar las solicitudes de resolución de nombres.
4. **Monitorear el Tráfico:**
   * Continuar monitoreando el tráfico DNS e ICMP para asegurarse de que el problema se haya resuelto y no vuelva a ocurrir.

### **Conclusión**

El análisis del tráfico DNS e ICMP indica que el problema principal se debe a que el servidor DNS en la IP 203.0.113.2 no estaba disponible en el puerto UDP 53, lo que impidió la resolución del nombre de dominio [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com). La solución incluye verificar y corregir la disponibilidad del servidor DNS y su configuración de red, así como asegurar que el tráfico hacia el puerto 53 esté permitido. Tras implementar estas soluciones, se recomienda un monitoreo continuo para confirmar que el problema esté completamente resuelto y que no se repita en el futuro.