【MVS】通过F5 iRule实现Virtual Servers虚服务DNAT与SNAT转换日志信息发送到远程日志主机

网络相关 设备管理 **胡伟** 3天前 发表

问题描述

【MVS】通过F5 iRule实现Virtual Servers虚服务DNAT与SNAT转换日志信息发送到远程日志主机

解决方法

目标

- 捕捉并记录客户端IP、端口、SNAT IP、端口、原始目的地IP、端口和服务器IP、端口信息。
- 记录虚拟服务器名称。
- 将日志信息发送到本地日志和远程日志主机。

iRule代码

以下是实现上述目标的iRule代码：

```
when CLIENT_ACCEPTED {
    # 获取虚拟服务器名称
    set vs_name [virtual]

    # 设置全局变量来保存客户端和原始目的地信息
    set client_ip [IP::client_addr]
    set client_port [TCP::client_port]
    set original_dst_ip [IP::local_addr]
    set original_dst_port [TCP::local_port]

    # 初始SNAT处理，如果没有SNAT则设置为空
    if { [IP::client_addr] ne [IP::remote_addr] } {
        set snat_ip [IP::remote_addr]
        set snat_port [TCP::remote_port]
    } else {
        set snat_ip $client_ip
        set snat_port $client_port
    }
}

when SERVER_CONNECTED {
    # 捕获服务器的IP和端口
    set server_ip [IP::remote_addr]
    set server_port [TCP::remote_port]

    # 综合记录所有信息，包括VS名称和SNAT信息
    set log_msg "VS Name - $vs_name; Client IP - $client_ip, Port - $client_port; SNAT IP - $snat_ip, Port - $snat_port; Original Destination IP - $original_dst_ip, Port - $original_dst_port; Server IP - $server_ip, Port - $server_port"

    # 本地日志记录
    log local0. $log_msg

    # 发送到远程日志主机
    log 192.168.254.120 local0. $log_msg
}
```

详细解析

- **CLIENT_ACCEPTED事件：**
  - 获取并存储虚拟服务器名称。
  - 捕获客户端的IP和端口。

- 捕获原始的目的地IP和端口。
- 检测并存储SNAT后的IP和端口。如果没有进行SNAT，则保持SNAT IP和端口为客户端的IP和端口。

- **SERVER_CONNECTED事件：**
- 捕获服务器的IP和端口。
- 综合所有信息，格式化为日志消息字符串。
- 使用log local0.命令记录日志到本地。
- 使用log <远程IP> local0.命令将日志消息发送到远程日志主机，替换其中的192.168.254.120为远程日志主机的IP地址。

应用和验证

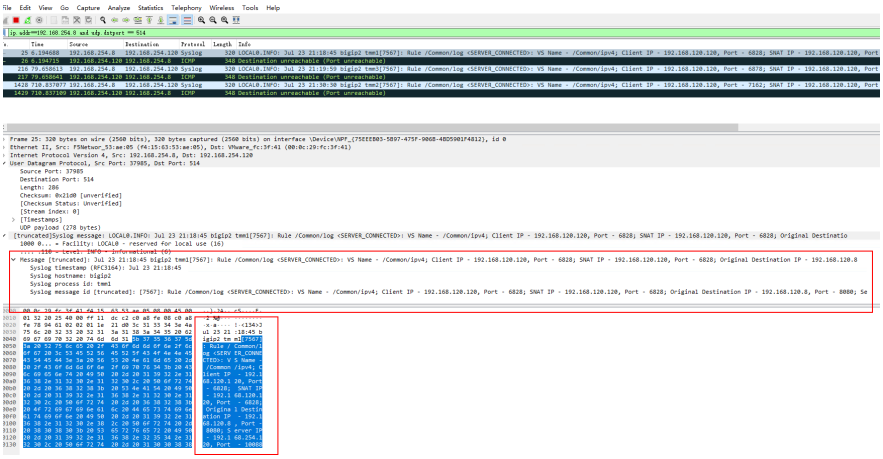
1. **应用iRule：**
- 在F5管理控制台上，创建并应用上述iRule到相应的虚拟服务器。确保使用的虚拟服务器和iRule创建过程正确无误。

1. **验证日志记录：**
- 本地日志：通过命令tail -f /var/log/ltm实时查看日志文件，确保日志信息已记录。
- 远程日志：在远程日志主机上配置syslog接收器，并确保F5设备与远程主机网络连通。检查远程主机上的日志文件，确保日志信息已成功转发。

日志示例

成功配置后，日志条目应类似于以下内容：

> Tue Jul 23 21:01:57 PDT 2024 info bigip2 tmm3[7567] Rule /Common/log <SERVER_CONNECTED>: VS Name - /Common/test_vs; Client IP - 192.168.120.120, Port - 6204; SNAT IP - 192.168.120.121, Port - 6204; Original Destination IP - 192.168.120.8, Port - 8080; Server IP - 192.168.254.120, Port - 10088



优点

- **集中管理：** 将日志信息发送到集中式日志管理系统，便于统一查看和分析。
- **纠错和排障：** 详细的日志信息有助于快速识别和解决网络问题。
- **安全监控：** 实时记录和监控网络流量，提升安全性。

注意事项

- **性能影响：** 大量日志记录可能会影响F5设备的性能，建议在生产环境中控制日志数量和频率。
- **网络设置：** 确保F5设备与远程日志主机之间的网络路径可达，且防火墙允许相关的SYSLOG流量。
- **隐私和安全：** 日志中可能包含敏感信息，应在日志传输过程中确保其安全性，例如使用加密通道。

总结

通过应用上述iRule，可以在F5设备上详细记录并集中管理网络流量日志信息。在实际操作中，除了记录和转发日志外，还需要考虑日志的安全传输和存储，以确保日志信息的机密性和完整性。这对于大规模网络环境中的故障排查和安全监控至关重要。