BEHAVIORAL SECURITY THREAT DETECTION STRATEGIES FOR DATA CENTER SWITCHES AND ROUTERS

Ram (Ramki) Krishnan, *Brocade Communications*

Dilip Krishnaswamy, *IBM Research*

Dave Mcdysan, *Verizon*
AGENDA

• Introduction

• Layer 2-4 DDoS detection/mitigation strategies

• Behavioral Security Threat Detection Assists

• Emerging Research Topics in NFV
Introduction
Motivation

The DDoS Threat Spectrum

Bolstered by favorable economics, today’s global botnets are using distributed denial-of-service (DDoS) attacks to target firewalls, web services, and applications, often simultaneously. This DDoS threat spectrum includes conventional network attacks, HTTP and SSL floods, and an emerging wave of low-bandwidth threats, plus the new threat vectors likely to target emerging service platforms.

by David Holmes
Senior Technical Marketing Manager

## Simple Network Attack Summary

<table>
<thead>
<tr>
<th>Attack</th>
<th>Target Vector</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYN flood</td>
<td>Stateful flow tables</td>
<td>Fake TCP connection setup overflows tables in stateful devices</td>
</tr>
<tr>
<td>Conn flood</td>
<td>Stateful flow tables</td>
<td>Real, but empty, connection setup overflows tables in stateful devices</td>
</tr>
<tr>
<td>UDP flood</td>
<td>CPU, bandwidth</td>
<td>Floods server with UDP packets, can consume bandwidth and CPU, can also target DNS servers and VOIP servers</td>
</tr>
<tr>
<td>Ping flood</td>
<td>CPU</td>
<td>Floods of these control messages can overwhelm stateful devices</td>
</tr>
<tr>
<td>ICMP fragments</td>
<td>CPU, memory</td>
<td>Hosts allocate memory to hold fragments for reassembly and then run out of memory</td>
</tr>
<tr>
<td>Smurf attack</td>
<td>Bandwidth</td>
<td>Exploits misconfigured routers to amplify an ICMP flood by getting every device in the network to respond with an ICMP broadcast</td>
</tr>
<tr>
<td>Christmas tree</td>
<td>CPU</td>
<td>Packets with all flags set except SYN (to avoid SYN flood mitigation) consume more CPU than normal packets</td>
</tr>
<tr>
<td>SYN/ACK, ACK, &amp; ACK/PUSH floods</td>
<td>CPU</td>
<td>SYN-ACK, ACK, or ACK/PUSH without first SYN cause host CPUs to spin, checking the flow tables for connections that aren’t there</td>
</tr>
<tr>
<td>LAND</td>
<td>CPU</td>
<td>Identical source and target address IPs consume host CPU as they process these invalid addresses</td>
</tr>
<tr>
<td>Fake TCP</td>
<td>Stateful flow tables</td>
<td>TCP sessions that look real, but are only recordings of previous TCP sessions; enough can consume flow tables and avoid SYN flood detection</td>
</tr>
</tbody>
</table>

Additional types of attacks*

- DNS attacks
  - UDP floods
  - Legitimate queries (NSQUERY) - hierarchical lookup to resolve names
  - Legitimate queries against non-existent hosts (NXDOMAIN)

- HTTP attacks
  - Floods - over 80% of DDoS attacks appear to be HTTP floods
    - Repeat request, Recursive gets for web pages
  - Low-bandwidth HTTP denial of service attacks
    - Slowloris – sends enough data (5 bytes) every 299 secs to keep connections active – fills up connections table
    - Slowpost – starts an HTTP post and fills data slow – can impact online Java gaming applications for example
    - HashDos – creates form variable names that map to the same hash value, posting a request containing the names, CPU time in handling collisions
  - SSL renegotiation – exploits asymmetry in crypto computation between client and server (significantly more computation at server)

Multi-tenant Virtualized DC

Issues Today

Present Mode of Operation

Need expensive dedicated DDoS appliance for L2-L7 DDoS detection/mitigation

Switches /Routers support only static firewall rule (L2-L4 ACL) configuration – scalability issues in protecting all servers
Layer 2/3/4 Flow Categorization

Short-lived Large Flows
Search Applications etc.

Long-lived Large Flows
Hadoop, File transfers, Tunnels etc.

Flexible – Any layer 2/3/4 fields
Observability, Controllability, Scalability
Key to Real-time SDN/NFV Analytics

Short-lived Small Flows
Chat (Twitter), Short form video content (Video clips) etc.

Long-lived Small Flows
Long form video content (Catch up episodes, Movies) etc.

Issues in learning all flows (NetFlow/IPFIX etc.) Flow cache size; CPU utilization
LONG-LIVED LARGE FLOWS

Real-time Automatic Recognition

Recognition External (Collector) e.g. sFlow-RT
E.g. FTP, Observation Interval – 2s
Minimum Bandwidth Threshold – above 10% link bandwidth

Recognition Sampling technologies (minimal router overhead)
e.g. sFlow, sampled NetFlow/IPFIX

HW Switches/Routers

Recognition Programmable Parameters
Observation Interval; Minimum Bandwidth Threshold

In-line line-rate techniques (faster detection)
e.g. FTP, Observation Interval – 200ms
Minimum Bandwidth Threshold – above 10% link bandwidth – IPFIX std. in progress, new IEs

SW - Virtual Switches/Routers

Other Methods - User Application Notification
e.g. scheduled backups

SDN AND NFV

SDN – innovation/value added services
SDN + NFV – untapped – key to driving innovation/value added services to the next level

Source: ETSI NFV White Paper
Layer 2-4 DDoS DETECTION/MITIGATION
Future Mode of Operation

DDoS Attacks – Layer 2-4 long-lived large flow! examples below

a. UDP Flood (DNS, SNMP, NTP etc.)
Attack - <Destination IP address>, UDP Protocol, UDP Src Port

b. Classic Large flow (IP 5 tuple), e.g. P2P

OpenFlow-hybrid – QoS actions (Policy) independent of forwarding

Benefits:
- Works on Hybrid OF (future I2RS) capable high speed routers, light-weight sampling techniques
- Attack detection/mitigation – typically couple of seconds
Simulation Results

• Topology:
  • Border Router with Hybrid Openflow, External sFlow Collector with real-time large flow detection application, SDN Controller and DDoS SDN Application
  • Border Router with sFlow sampling rate of 1:2048 and 4x10Gbps Internet Uplinks

• Test:
  • Border Router was subject to 20Gbps of traffic on 2 different uplink ports
  • 1Gbps of UDP flood traffic was sent on one of the uplink ports
  • Values chosen for programmable parameters for UDP flood detection pre-filter – Minimum
    • Bandwidth threshold (bmin) = 800Mbps. Observation Interval (dmin) = 3s.

• Result:
  • The UDP flood attack was detected by the DDoS SDN application in ~5s and was rate-limited to 200Mbps in the Border Router based on a configured policy.
NFV/SDN - LAYER 2-4 DDoS ATTACK DETECTION/MITIGATION

Future Mode of Operation

Benefits:
- Attack detection/mitigation – typically 100s of ms (order of magnitude faster than sampling)
- Flexibility, evolving attacks
- Capacity scale on demand
- Use OF/SDN (future I2RS) to program upstream/other network nodes

Brocade Network Field Day presentation, Brocade’s first ETSI NFV PoC on DDoS mitigation
Simulation Results

- **Topology:**
  - Virtual switch/router was the edge device for 60 virtual servers (each virtual server is a VM).

- **Test:**
  - Virtual switch/router was the subject to 8Gbps of traffic; this traffic was switched to different servers.
  - 500Mbps of UDP flood traffic was continuously sent to a single virtual server.
  - Values chosen for programmable parameters for UDP flood detection pre-filter – Minimum bandwidth threshold ($b_{min}$) = 400Mbps. Observation Interval ($d_{min}$) = 200ms.

- **Result:**
  - Virtual switch/router’s throughput was unaffected.
  - The UDP flood attack was detected by the Virtual switch/router in ~400ms and was rate-limited to 50Mbps based on a configured policy.
Behavioral Security Threat Detection Assists
Layer 7 DDoS Assist

- DC Edge switch/router or Border Router can assist in detecting various Layer 7 DDoS attacks such as HTTP GET Amplification
  - An errant tenant which is being subject to DDoS attack can be detected in the DC Edge switch/router or Border Router. Also, any layer 2-4 DDoS attacks on the errant tenant can be detected in the DC Edge switch/router or Border Router.
  - Tenant traffic can be redirected to a Layer 7 DDoS appliance using a redirection rule specific to the tenant (OpenFlow or vendor specific) in the DC Edge switch/router or Border Router.
  - If the tenant stops misbehaving, the redirection rule specific to the tenant can be removed in the DC Edge switch/router or Border Router.

- Benefits: Substantially reduce the amount of traffic sent to expensive Layer 2-7 Firewall/DDoS appliances.
Flow Aware Sampling

Future Mode of Operation

Automatic recognition of classic Layer 2-4 long-lived flows such as file transfers, video streaming – no sampling

Other flows; sampling at normal rate; potential source of behavioral security threats – examined in External Collector

Benefit - much lesser samples than sampling all flows equally

NFV/SDN possibilities

• Allow the bandwidth $b_{\text{min}}$ and observation interval $d_{\text{min}}$ thresholds to be programmable in a router

• Allow exposure of flow-specific information

• Programmable thresholds for each flow?
  • Higher thresholds for flows whose natural requirements are high
  • Bursty flow with long duration of inactivity can have a longer observation interval
  • Flow requiring a large bandwidth naturally may need a higher bandwidth threshold

• With multiple flows, can consider allocating flows to flow categories $i$, and specifying thresholds for those
  • each flow category $i$ can have a different bandwidth threshold $b_{\text{min},i}$ and observation interval threshold $d_{\text{min},i}$.
NFV/SDN possibilities contd.

• The thresholds for each category $i$ can be exposed via APIs.

• Metadata associated with a flow can be used to extract the flow category to apply the appropriate threshold for a specific flow in a router.

• Additional refinement of the thresholds can be performed for each specific type of attack $j$
  • each DDoS attack $j$ can have attack-specific thresholds $b_{\text{min},i,j}$ and $d_{\text{min},i,j}$ for each flow category $i$. In

• Flow-category and DDoS attack type requirements exposed through APIs
  • Can help with smarter configuration in the system and optimized detection/mitigation – needs further exploration
Other Public Presentations/Demos/PoCs
• Recent recognition for SDN–related work
• ONS SDN Idol Winner – SDN DDoS - Ram (Ramki) Krishnan, Brocade

• ETSI NFV PoC in progress