Issues with Network Address Translation for SCTP

David Hayes
dahayes@swin.edu.au
Centre for Advanced Internet Architectures (CAIA)
Swinburne University of Technology

Outline

Overview of SCTP NAT
Alias_sctp data structures
  Lookup tables
  Timer Q
NAT state inconsistencies
Lookup table conflicts
Alias_sctp performance
Alias_sctp Interface
Some practical observations
Conclusions
Overview of SCTP NAT

Why is SCTP NAT different?

- Multiple control chunks
  - And parameters
  - DoS – processing chunks and parameters

<table>
<thead>
<tr>
<th>SCTP Header</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Chunk 1 Header</td>
</tr>
<tr>
<td>Parameter 1</td>
</tr>
<tr>
<td>Parameter 2</td>
</tr>
<tr>
<td>Parameter 3</td>
</tr>
<tr>
<td>Parameter 4</td>
</tr>
<tr>
<td>Data Chunk 1 Header</td>
</tr>
<tr>
<td>Parameter 1</td>
</tr>
<tr>
<td>Parameter 2</td>
</tr>
<tr>
<td>Data Chunk 2 Header</td>
</tr>
</tbody>
</table>
Overview of SCTP NAT

Why is SCTP NAT different?

- Multiple control chunks
  - And parameters
  - DoS – processing chunks and parameters
- Multi-homing
  - Can change on the fly
  - NAT state inconsistencies
  - DoS - Memory when tracking
Overview of SCTP NAT

Gleaning association state information

- INIT ↔ INIT-Ack exchange
Overview of SCTP NAT

Gleaning association state information

- INIT ↔ INIT-Ack exchange

Local

Global

Hash Table

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>$h^{-1}$</td>
<td>$h$</td>
<td></td>
</tr>
</tbody>
</table>

Assoc state

Association State

- local – vtag, port, address
- global – vtag, port, [address list]
- state – [Idle, ···, UP, ···, Closing]
- expiration time
- pointers for:
  - local and global lookup tables
  - timer Q

Alias_sctp data structures

Lookup tables — Global and Local
Alias_sctp data structures

Lookup tables — Global and Local

Hash Table

<table>
<thead>
<tr>
<th></th>
<th>assoc</th>
<th>assoc</th>
<th>assoc</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>g1</td>
<td>g1</td>
<td>g1</td>
</tr>
<tr>
<td>2</td>
<td>g2</td>
<td>g2</td>
<td>g2</td>
</tr>
<tr>
<td>3</td>
<td>g3</td>
<td>g3</td>
<td></td>
</tr>
</tbody>
</table>

Timer Queue

- Circular Q
- Time in seconds
- \( n = \text{maxtime} \)
exp updated continually
Location in Q only changed if earlier

exp > current
assoc
exp
assoc
exp
assoc
exp
n+1
1 2

current

exp > current
assoc
exp
assoc
exp
assoc
exp
There is no state inconsistency when global IP addresses are not tracked.
NAT State Inconsistencies
When tracking global IP addresses

There is no state inconsistency when global IP addresses are not tracked.

Caia Seminar
http://www.caia.swin.edu.au
dahayes@swin.edu.au
September 11, 2008
There is no state inconsistency when global IP addresses are not tracked

Lookup table conflicts
General model of lookup table process

Is it necessary to track global IP addresses?

- $\Lambda$ association arrival rate
- $R\Lambda$ association retry rate
- $m$ lookup table size
- $\lambda = \Lambda/m$ and $r = r/m$
- $1/\mu$ average association holding time
Lookup table conflicts
Single element model

\[
\lambda + r\lambda
\]

\[
\mu
\]

Solving the balance equations

\[
P[\text{conflict}] = P[1] = \left(1 + \left(\frac{\mu}{2\lambda}\right)^2\right)^{\frac{1}{2}} - \frac{\mu}{2\lambda}
\]

Lookup table conflicts
Two scenarios

- No global IP address tracking

Vtag only
- All local hosts always use the same source and destination ports
- Conflict when two hosts coincidentally choose the same vtag
- \(m = 2^{32} - 1\)

vtag and port
- All local hosts always use the same destination port, but random source port.
- Conflict when two hosts coincidentally choose the same vtag and port.
- \(m = (2^{32} - 1)(2^{16} - 1024)\)

- Average association lasts 180 s (1/\(\mu\))
- Association arrival rate varies
Lookup table conflicts
$P[\text{conflict}]$ versus $\Lambda$ for $1/\mu = 180$ s

\begin{align*}
\text{vtag only} & \quad \text{vtag and port} \\
1 \times 10^{-01} & \quad 1 \times 10^{-03} & \quad 1 \times 10^{-05} & \quad 1 \times 10^{-07} & \quad 1 \times 10^{-09} \\
1 \times 10^{+01} & \quad 1 \times 10^{+03} & \quad 1 \times 10^{+05} & \quad 1 \times 10^{+07} & \quad 1 \times 10^{+09}
\end{align*}

Caia Seminar
http://www.caia.swin.edu.au
dahayes@swin.edu.au
September 11, 2008

Alias_sctp performance
Experimental setup

High association rate
- 1 500 assoc/s
- Assoc duration 10 s
- 4 addresses in INIT
- With and without global IP address tracking
- Baseline
- Measuring kernel process CPU time
Alias_sctp performance
Results — High association arrival rate

<table>
<thead>
<tr>
<th>kernel</th>
<th>Total</th>
<th>alias_sctp</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mean (s)</td>
<td>Variance (s^2)</td>
</tr>
<tr>
<td>tracking</td>
<td>177.46</td>
<td>0.062</td>
</tr>
<tr>
<td>not tracking</td>
<td>165.52</td>
<td>0.067</td>
</tr>
<tr>
<td>baseline</td>
<td>143.90</td>
<td>0.058</td>
</tr>
<tr>
<td>increase due to tracking</td>
<td>7.2%</td>
<td>—</td>
</tr>
</tbody>
</table>

- Tracking significantly increases in alias_sctp’s work
- Overall 7%

---

Alias_sctp performance
Results — High data rate

<table>
<thead>
<tr>
<th>kernel</th>
<th>Total</th>
<th>alias_sctp</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mean (s)</td>
<td>Variance (s^2)</td>
</tr>
<tr>
<td>tracking</td>
<td>231.63</td>
<td>0.068</td>
</tr>
<tr>
<td>not tracking</td>
<td>229.61</td>
<td>0.063</td>
</tr>
<tr>
<td>baseline</td>
<td>223.15</td>
<td>0.130</td>
</tr>
<tr>
<td>increase due to tracking</td>
<td>0.9%</td>
<td>—</td>
</tr>
</tbody>
</table>

- Not really significant
Alias_sctp performance

Memory usage

State space memory usage

\[ M = 8h + 60n + 12 \sum_{i=1}^{n} g_i \] bytes

<table>
<thead>
<tr>
<th>Memory usage</th>
<th>Tracking</th>
<th>Not tracking</th>
</tr>
</thead>
<tbody>
<tr>
<td>High assoc rate</td>
<td>1.8 \times 10^6 bytes</td>
<td>9.0 \times 10^5 bytes</td>
</tr>
<tr>
<td>High packet rate</td>
<td>2.4 \times 10^5 bytes</td>
<td>1.2 \times 10^5 bytes</td>
</tr>
</tbody>
</table>

Alias_sctp Interface

- ipfw command
- sysctl variables (net.inet.ip.alias.sctp)
  - track_global_addresses
  - param_proc_limit
  - chunk_proc_limit
  - initialising_chunk_proc_limit
  - accept_global_ootb_addip
  - error_on_ootb
  - hashtable_size
  - holddown_timer
  - shutdown_timer
  - up_timer
  - init_timer
  - log_level d
Some practical observations

- freesbie – FreeBSD bootable disk
- cscope – Searchable C source tree database
- svn
- python
  - impacket

Conclusions

**Alias_sctp module**

- FreeBSD ipfw2 kernel based SCTP NAT
- extension to libalias kernel module
- ipfw and sysctl

**SCTP NAT**

- Multiple control streams
  - Limit number of parameters and chunks processed
- Global address tracking
  - Not necessary in any practical implementation
  - Memory usage significant
  - Disable by default
    - Prevents NAT state problems
  - Limit total number of addresses if enabled