.TW DNS Security: NOC & ISP collaboration

Cheng-Yi Chen & Tszheng Guo,
TWNIC
Defense against DDoS attacks with ISPs

Guo Tszheng
outline

• Filter action
  – Block DNS query traffic from abroad
  – Filter traffic with white list
• Increasing response capacity
  – Set-up the hidden DNS
.tw DNS face DDoS attack

Attack traffic from Abroad

Traffic through cache

Domestic attack traffic

Avoid traffic pass edge router

.tw authoritative DNS server
Filter action—Block DNS query traffic from abroad

- .TW DNS service domestic users majorly, local user availability is the first priority
- There are .TW DNS servers distribute globally, include local and abroad.
- When suffer DDoS attack, block the DDoS attack traffic from abroad on the border router to ensure domestic user can reach .TW DNS.
- According to past experience the action can filter out 95% traffic.
Block attack traffic on the border router

Attack traffic from Abroad

Traffic through cache

Domestic attack traffic
Filter action-
Filter traffic with white list

• Authoritative DNS server only service recursive DNS server, traffic from end user is abnormal.
• We analysis the DNS query log to find out which IPs are cache DNS servers and put they into white list, then configure the edge router to limit the bandwidth usage which DNS query traffic come from the IPs not in white list.
Filter by white list

Domestic attack traffic

Attack traffic from Abroad

Traffic through cache
Increasing response capacity
-Set-Up the hidden DNS

- Hidden DNS server is an DNS server only service Taiwan ISP’s cache server.
- When .TW DNS suffer DDoS attack, The ISP can configure their cache DNS servers to forward .tw queries to hidden DNS to make sure the .tw DNS availability.
Enable hidden DNS

Normal query traffic

Domestic attack traffic

Attack traffic from Abroad

Traffic through cache
DNS Network Operation Center (DNSNOC)

Cheng-Yi Chen
Outlines

• System Architecture
  – Probes

• Parameters

• Introduction of probes
  – Bandwidth
  – System
  – Alive、Response

• System overview
System Architecture (1)

Colocation A
- Switch
- Load balancer
- DNS
- Other Service

DDoS
Botnet
Attack

Probe based Cyber Security System
- Alert
- Record
- Bandwidth
- Alive
- System
- Response
System Architecture (2) - Probes

Colocation A
- switch
- Load balancer
- Machine/Device
- DNS

Probes
- Machine / Device
- Colocation A
- Colocation B
- Colocation C

System Architecture
- Probes
--bandwidth
-_alive
--system

Alert
- Probe based Cyber Security System
- Receiver
- MsgLog
- Processes
- Data Storage
- Backup

Response
- TCP/UDP
- DNS
- Web
- Mail

Alert
- Probe based Cyber Security System
- Receiver
- MsgLog
- Processes
- Data Storage
- Backup

Response
- TCP/UDP
- DNS
- Web
- Mail
Outlines

• System Architecture
  – Probes

• Parameters

• Introduction of probes
  – Bandwidth
  – System
  – Alive 、 Response

• System overview
### Parameters

<table>
<thead>
<tr>
<th>变数</th>
<th>描述</th>
<th>资料类型</th>
<th>预设值</th>
<th>說明</th>
</tr>
</thead>
<tbody>
<tr>
<td>DF-BW(_j^i)</td>
<td>編號 (_i) 機房中編號 (_j) 主機的頻寬探針規則定義(規則定義方程式)</td>
<td>邏輯判斷方程式</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>(\theta_{bw})</td>
<td>頻寬探針偵測頻率(分鐘)</td>
<td>整數 (\geq 1)</td>
<td>預設值=5</td>
<td></td>
</tr>
</tbody>
</table>
| \(R_{jk}^i\) | 編號 \(_i\) 機房中編號 \(_j\) 主機第 \(_k\) 次資料傳輸的平均速度(Mbps) | 實數 \(\geq 0.0\) | 0.0 | 計數器為32位元，若超過最大值將歸零重新計數。
若計數器數值 \(C_1 > C_2\) \(\downarrow\)  \[ R_{jk}^i = \frac{(C_1-C_2) \times 8}{2^{20} \times \theta_{bw} \times 60} \]  
若計數器數值 \(C_2 > C_1\) \(\uparrow\)  \[ R_{jk}^i = \frac{(2^{32}-C_2+C_1) \times 8}{2^{20} \times \theta_{bw} \times 60} \] |
| Week\(_jt\) | 編號 \(_i\) 機房中編號 \(_j\) 主機第 \(_t\) 周的資料傳輸的每周平均速度(Mbps) | 實數 \(\geq 0.0\) | 0.0 | |
| Month\(_jt\) | 編號 \(_i\) 機房中編號 \(_j\) 主機第 \(_t\) 月的資料傳輸的每月平均速度(Mbps) | 實數 \(\geq 0.0\) | 0.0 | |
| PeakR-PerHour\(_j^i\) | 編號 \(_i\) 機房中編號 \(_j\) 主機每小時的最大資料傳輸速度(Mbps) | 實數 \(\geq 0.0\) | 0.0 | |
| PeakR-PerDay\(_j^i\) | 編號 \(_i\) 機房中編號 \(_j\) 主機每天的最大資料傳輸速度(Mbps) | 實數 \(\geq 0.0\) | 0.0 |  \[ PeakR-PerDay\(_j^i\) = \max( PeakR-PerHour\(_j^i\) ) \] |
Outlines

• System Architecture
  – Probes

• Parameters

• Introduction of probes
  – Bandwidth
  – System
  – Alive, Response

• System overview
Bandwidth probe

• Warn value：n * max bandwidth from historical data of same month last year in normal status.

• Error value：m * max bandwidth from historical data of same month last year in normal status. (m>n)

• Red alert： (one of bellowing situation)
  – Machine bandwidth > 80% * Site max bandwidth
  – Machine bandwidth > Error value and Machine bandwidth > 60% * Site max bandwidth

• Yellow warn：
  – Machine bandwidth > Error value or Machine bandwidth > 60% * Site max bandwidth
System probes - Load 、 Memory 、 Proc 、 Disk 、 Syslog

• Load 、 Memory 、 Proc 、 Disk
  – Error value and warn value are based on history log
  – Red alert : query result via SNMP > error value
  – Yellow warn : query result via SNMP > warn value

• Syslog
  – Check syslog : find error and warning record via syslog analysis and domain knowledge.
  – Red alert : error record has appeared in syslog.
    Ex: failed authentication, wrong account …
  – Yellow warn : warning record has appeared in syslog.
    Ex: too many logins …
Outlines

• System Architecture
  – Probes
• Parameters
• Introduction of probes
  – Bandwidth
  – System
  – Alive、Response
• System overview
Alive probe

• Alive
  – Lost ratio：ratio of missing ICMP probe test.
  – Error value：100% lost
  – Warn value：60% lost
  – Red alert：ICMP lost ratio is larger than error value
  – Yellow warn：ICMP lost ratio is larger than warn value, but below error value
Response probe

- **Response**
  - Lost ratio: ratio of missing connection test of service.
  - Error value: 100% lost
  - Warn value: 60% lost
  - Red alert: lost ratio is larger than error value
  - Yellow warn: lost ratio is larger than warn value, but below error value
Outlines

• System Architecture
  – Probes
• Parameters
• Introduction of probes
  – Bandwidth
  – System
  – Alive、Response
• System overview
DNSNOC

DNS Network Operation Center

HiNet  台北是方  遠傳  中研院
台固  亞太  TANet  國高
遠傳台中
中華高雄

Colocation Probes
Search
Query bandwidth and load
Query single probe hostory log

- Last 24 hours
- Last 7 days
- Last 4 weeks
- Last 12 months
Notice process log
THANK YOU