Proxy Load Balancing

RADEXT - IETF 124

draft-dekok-radext-proxy-load-00

InkBridge Networks

TWO PROBLEMS, TWO SOLUTIONS

- Multiple home servers, what if one fails?
  - Packets for ongoing EAP sessions will be sent to servers which cannot process them
  - *define a method for stateless server affinity*
- DoS prevention, where one supplicant / client sends 1000’s of packets/s
  - existing solution is to block source IP, either manually or automatically
  - *define a method for detecting and automatically blocking bad sessions*

InkBridge Networks

SERVER AFFINITY

- Give each home server a unique 8-bit identifier
- Mangle State attribute to/from the home server
  - If the home server is down, don’t send the packet to a different one!
  - **Only works for the proxy next to the home server**
- Near zero-cost for proxy
- avoids sending more traffic to the home server

RATE LIMITING

- When proxying, look at Access-Rejects. If “too many” are received in a short time frame, block packets based on User-Name + Calling-Station-Id
- When receiving packets, look up User-Name + Calling-Station-Id, and synthesize Access-Reject if the user is being blocked
- Additional details are in the draft
- IPR exists, disclosure will be filed shortly (terms are no patent lawsuits)

RATE LIMITING - DETAILS

- In practice, this has been shown to block bad traffic at a high confidence
  - With no impact on “good” traffic
  - Eduroam can see 2000+ PPS of bad traffic from one misbehaving system
- Blocking is only done while the DoS attack is ongoing
  - plus a small window, sub 10 seconds.
- Essentially no chance of affecting normal traffic

RATE LIMITING - EXTENSIONS

- It could be extended to block authentic users who are not authorized for a particular network
  - i.e. “my credentials are OK, but I can’t roam here”
  - The supplicant just keeps trying, because there is no way to signal any backoff
- Using rate limiting here more likely to see problems
  - Blocking on human timescales is more likely to go wrong

QUESTIONS?

- Should be “informational” or even “experimental”