IETF 108 bmwg

draft-ietf-bmwg-ngfw-performance-03

draft-ietf-bmwg-ngfw-performance-03

- Current draft is draft-ietf-bmwg-ngfw-performance-03
- Upcoming changes and updates
  - Adding CVE Test to Security Effectiveness section
  - Following KPIs to be measured
    - Number of blocked CVEs
    - Number of bypassed (nonblocked) CVEs
    - Background traffic performance (verify if the background traffic is impacted while sending CVE toward DUT/SUT)
    - Accuracy of DUT/SUT statistics in term of attack reporting

draft-ietf-bmwg-ngfw-performance-03

- Security Features list (Network IPS)
  - SSL Inspection
  - Anti-Malware
  - Anti-Botnet
  - Logging and Reporting
  - Application Identification
  - Deep Packet Inspection
  - Anti-Evasion
- Security Features list (NGFW)
  - Outlined in current draft – no significant changes

draft-ietf-bmwg-ngfw-performance-03

- Test Equipment Config Parameters (Network IPS)
  - Current req’ts outlined in 4.3.1.2 and 4.3.2.2 remain
  - Background traffic to requires even distribution of HTTP and HTTPS
  - Based on maximum DUT/SUT throughput or results determined in section 7.3 and 7.7
  - CVE traffic transmission Rate: Y CVEs per second (e.g. Y=10)
  - Generate each CVE multiple times (sequentially) at Y CVEs per second (e.g. generate CVE traffic for 3 minutes)
- Test Equipment Config Parameters (NGFW)
  - Outlined in current draft – no significant changes

draft-ietf-bmwg-ngfw-performance-03

- Test Results Validation Criteria (Network IPS)
  - Number of failed Application transaction in the background traffic MUST be less than 0.01% of attempted transactions
  - Number of Terminated TCP connections of the background traffic (due to unexpected TCP RST sent by DUT/SUT) MUST be less than 0.01% of total initiated TCP connections in the background traffic
  - During the sustain phase, traffic should be forwarded at a constant rate
  - False positive MUST NOT occur in the background traffic
- Test Results Validation Criteria (NGFW)
  - Outlined in current draft – no significant changes

draft-ietf-bmwg-ngfw-performance-03

- Measurement (Network IPS)
    - Mandatory KPIs:
        - Blocked CVEs: It should be represented in following ways:
            - number of blocked CVEs out of total CVEs
            - percentage of blocked CVEs
        - Unblocked CVEs: It should be represented in following ways:
            - Number of unblocked CVEs out of total CVEs
            - percentage of unblocked CVEs
        - Background traffic behavior: it should represent one of the followings ways:
            - No impact (traffic transmission at constant rate)
            - minor impact (e.g. small spikes- +/- 100 Mbit/s)
            - heavily impacted (large spikes and reduced the background throughput > 100 Mbit/s)
        - DUT/SUT statistics regarding attacks
- Measurement (NGFW)
    - Outlined in current draft – no significant changes

draft-ietf-bmwg-ngfw-performance-03

- Test Procedures and Expected Results (Network IPS)
  - Background traffic
  - CVE Emulation
- Test Procedures and Expected Results(NGFW)
  - Outlined in current draft – no significant changes