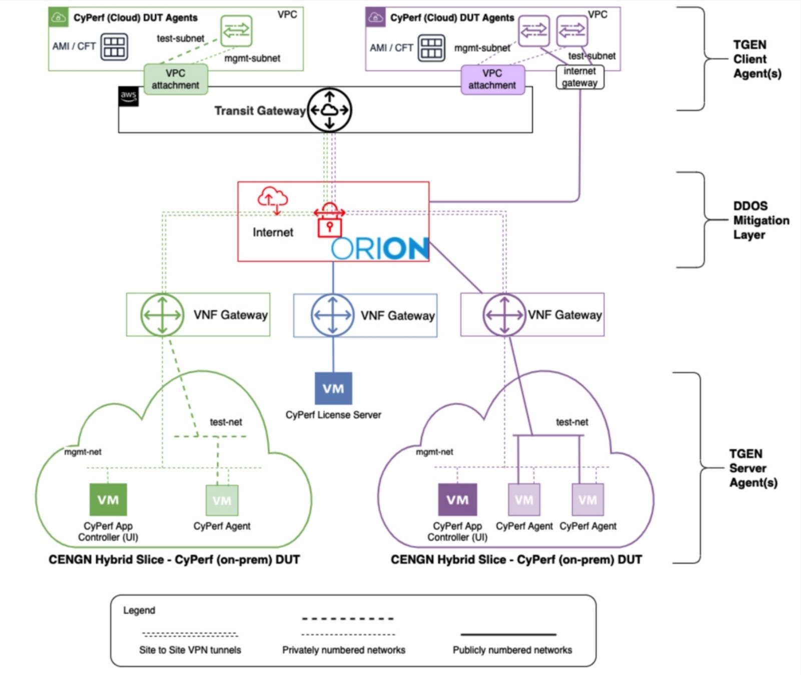
EINPRESSWIRE

CENGN Demonstrates ORION DDoS Mitigation System Using Keysight’s CyPerf

This project was the first to use a test solution that re-creates realistic workloads and DDoS attacks on production-level physical and cloud environments.



OTTAWA, ONTARIO, CANADA, December 6, 2021 /EINPresswire.com/ -- Summary

The rate of cybercrimes in the form of distributed denial-of-service (DDoS) attacks and widespread botnet activities has escalated in recent times, with over 10 million DDoS attacks launched in 2020 (Source: NETSCOUT). The number of malicious attacks continues to grow with the rollout of 5G technologies, which has accelerated the use of advanced Internet of Things (IoT) and cloudification of processes that provide more avenues for cyberthreats.

As part of its security strategy, CENGN continuously validates its protection mechanisms. In this project, the CENGN Testbed’s hybrid cloud environment was used in combination with Keysight’s CyPerf test traffic simulator to measure the effectiveness of ORION’s DDoS mitigation solution deployed upstream to CENGN’s public network.

Keysight’s CyPerf product is the industry’s first cloud-native traffic simulator. CyPerf simulates realistic application workloads and malicious attacks across various physical and cloud environments, delivering unrivalled insights into end-user experience, security posture, and distributed hybrid network performance bottlenecks.

ORION’s DDoS Threat and Mitigation system detects volumetric, state-exhaustion, asymmetric, computational, vulnerability and network-layer attacks. The detection component identifies unusual and suspicious network traffic from cyber attackers and botnets that cause a denial of service. The mitigation function helps monitor network traffic, automatically mitigating DDoS threats while also providing alerts and data reporting if an attack were to happen.

This project simulated various DDoS attacks towards CENGN’s environment using Keysight’s CyPerf cloud test traffic simulator and ORION’s DDoS threat mitigation system to demonstrate the value of both products.

Project Details

The topology involved in this project is presented in the following diagram.

Testbed Overview

The CENGN Testbed is a multi-vendor, multi-site infrastructure leveraging the ORION DDoS threat mitigation service. ORION DDoS Threat Protection monitors traffic on the ORION network, detecting and mitigating DDoS threats, providing alerts and reporting when an attack happens. To prove the effectiveness of the threat mitigation system, this project took advantage of CENGN’s hybrid cloud validation services and Keysight’s CyPerf test solution to generate diverse application traffic profiles embedded with DDoS threats.

In this hybrid scenario, the first phase of the project (green) entailed traffic generation between public and on-premises cloud slices, via a site-to-site virtual private network (VPN) tunnel interconnecting Amazon Web Services (AWS) transit gateway and CENGN’s virtual network function (VNF) customer gateway.

The second phase (purple) generated aforementioned traffic via the internet – a direct connection to the public cloud resource, facilitated via AWS elastic internet protocols (IPs).

Both traffic scenarios were built around safe and malicious DDoS traffic profiles to monitor, detect and alert on preconfigured throughput (from 100Mbps to 1Gbps) and connection rate (20000 cps) thresholds.

Test Case(s)

The following pre-selected DDoS attack signatures were used as part of the execution of this joint project:

- IPv4 Blocklists
- TCP SYN and ACK Authentications
- HTTP Malforms
- HTTP Reflection and Amplifications

The test approach was conducted in two phases:

Phase 1: Execution of sixteen (16) test cases to analyze TCP SYN, TCP ACK, Malform HTTP, and IPv4 Blocklist attacks for bidirectional traffic – refer to Appendix 1 for more details. In addition to the initial scope, three (3) additional test cases with UDP Floods were performed. Details of the test cases are available in Appendix 2.
Phase 2: Execution of HTTP Reflection/Amplification attack test cases. Details are presented in Appendix 3.

Test Results

Prior to covering the detailed test results, CyPerf’s implicit value became apparent in the ease of simulating versatile traffic profiles, helping with the efficiency of bidirectional security attacks and auto-mitigation verification of inbound DDoS attacks.

Outlined is a quick summary of the test outcomes:

- IPv4 Blocklists: The IPv4 blocklist was simulated leveraging HTTP-GET traffic with a mix of blocklisted and safe predefined IPs. The outcome of this test was a resounding 100% auto filtering of the blocklisted source IPs which cleaned up the traffic to only allow passage of whitelist IPs within the traffic flow. The visual representation reflects on the type of traffic being accepted or discarded depending on the traffic profile simulated by CyPerf.
- TCP SYN and ACK Authentications: For this test, we focused on both inbound and outbound authentications. As depicted below, we experienced a complete bidirectional detection of all excessive application and illegitimate traffic. In addition, leveraging auto mitigation, the detected traffic was dropped.
- HTTP Malforms: In simulating the HTTP malform traffic, we preconfigured HTTP request to medium/high sensitive levels and observed consistent detection and prevention of bad requests.

- UDP Flooding: CENGN simulated UDP flood with its hybrid connection to AWS via IPsec. As a result, the spoofed UDP data packets were effectively detected, generating alerts for further mitigation action.
- HTTP Reflection and Amplifications: In this test, a flexible regex-based countermeasure was deployed so generated URL expressions were examined on inspected HTTP requests, all detected attack signatures were filtered through auto mitigation.

Test Summary

This level of success was achieved thanks to a close collaboration between CENGN, ORION and Keysight. Our organizations worked together to plan and define the levels of detection to mitigation mapping against certain types of threat signatures as well as adjusted ORION's protection configurations and CyPerf's attack volumes for proper testing.

This collaborative project was the first of its kind as it leveraged a test solution that re-creates realistic workloads and DDoS attacks on production-level physical and cloud environments. This expanded Keysight's CyPerf tool coverage, which had an initial focus towards software-defined wide area networking (SD-WAN) solution validation.

Overall, CENGN gathered relevant experience around CyPerf's functionality while improving its security posture through proper validation going beyond generic or default configuration. As a next step, CENGN will be incorporating this type of testing as a potential offering to augment our already wide set of commercialization validation services for Canada's startups and scaleups.

The ORION-CENGN NGNP Partnership

The CENGN Testbed is a multisite hybrid cloud infrastructure that leverages the ORION Network. This infrastructure acts as the digital backbone of innovation in Ontario, hosting the Next Generation Network Program (NGNP).

The NGNP is a Government of Ontario program offered through a partnership between CENGN and the Ontario Centre of Innovation (OCI) that provides small and medium-sized enterprises across Ontario access to the infrastructure they need to test their tech products and solutions for market readiness. Through the NGNP, CENGN also uses its testbed to deliver skill development and training in cloud computing and networking technologies to help meet the growing demand of Canadian professionals in digital technology.

Company Overviews

ORION

ORION is a not-for-profit organization dedicated to empowering Ontario researchers, educators, and innovators. ORION fosters a community of more than two million users at more than a hundred universities, colleges, hospitals, and research institutions, as well as many of Ontario's school boards. They enable ground-breaking discoveries and cutting-edge education by connecting institutions and regions through our network, facilitating collaboration, and providing our community with the digital tools and expert support they need to make the world a better place.

Keysight Technologies

Keysight Technologies is the world's leading electronic measurement company, transforming today's measurement experience through wireless, modular, and software solutions innovations. The company provides network, application, and security test solutions to strengthen networks and cloud environments for enterprises, service providers and network equipment manufacturers.

CENGN

CENGN is Canada’s Centre of Excellence in Next Generation Networks. Our mission is to drive technology and industry growth in Canada, enabling economic strength and prosperity, as well as innovation and competitiveness in this high-growth global multi-trillion-dollar industry.

Through our leading-edge technology infrastructure and expertise, and the creation of a globally recognized ecosystem of partners, CENGN helps Canadian small and medium enterprises overcome commercialization barriers and grow. CENGN collaborates with top ICT multinationals, the public sector, financial institutions, and academic partners, to solidify Canada’s leadership in advanced networking for the benefit of all Canadians.

Contact

Rick Penwarden
Senior Communications Manager
CENGN – Canada’s Centre of Excellence in Next Generation Networks
rick.penwarden@cengn.ca

Appendix

Appendix 1

Cycle 1 – Purple Scenario: Inbound and Outbound Traffic Simulation

Back to Test Case(s)

Alert and Mitigation Type	Tests	Simulation	Result/Remark
TCP SYN, TCP ACK (Outbound)	1 – 5	Traffic: HTTP-GET and HTTP-POST	– High-level outgoing alerts were triggered for HTTP requests in tests 2, 4 and 5 when Global Detection thresholds were lowered for the tests – Medium level incoming alerts were triggered for HTTP responses in tests 1 and 2 as warnings. Mitigations were not triggered – High-level incoming alerts and mitigations was triggered for HTTP responses in tests 3 – 5, packet drops for both excessive application traffic and illegitimate traffic were observed
TCP SYN, TCP ACK (Inbound)	6	Traffic: HTTP-GET	– High-level incoming alert and mitigation was triggered – No packet drops of excessive application traffic

– Packet drops of illegitimate traffic were observed
Malform HTTP
(Inbound) 7 – 14 Traffic: HTTP-POST, or Attacks: SQL injection, or DoS – High-level incoming alerts and mitigations were triggered in all tests

– Malformed HTTP Filtering level was set as Medium or High

– Packet drops by Malformed HTTP filter were observed in tests 7 – 10 and 14

– When the source of app traffic was set to be different from the source of attacks, the Malformed HTTP filter detected attacks and dropped attack packets (tests 9 – 10)

– In packet capture for test 10, all attack packets from the attacker were picked by the filter and dropped
IPv4 Blocklist
(Inbound) 15 – 16 Traffic: HTTP-GET incoming from a blocklisted IP – High-level incoming alerts and mitigations were triggered in test 15 and 16, all traffic from blocklisted sources were blocked
Appendix 2
Cycle 1 – Green Scenario: Inbound and Outbound Traffic Simulation
Back to Test Case(s)

Alert and Mitigation Type Tests Simulation Result/Remark
UDP Flood
(Outbound) 1 Traffic: outgoing HTTP-GET – Both incoming and outgoing DoS Host Alerts were triggered during outbound traffic simulation of HTTP application with throughput 100 Mbps
UDP Flood (Inbound) 2-3 Traffic: incoming HTTP-GET – Both incoming and outgoing DoS Host Alerts were triggered during inbound traffic simulation of HTTP application with throughput 100 Mbps
Appendix 3
Cycle 2 – Purple Scenario: Inbound and Outbound Traffic Simulation

Back to Test Case(s)

Alert and Mitigation Type Simulation Result/Remark
HTTP Reflection/Amplification Traffic: HTTP-GET, and HTTP Attack – We established that the earlier deployed Payload regex did not match 100% with the attack traffic simulation

– As a result, we altered to a more flexible regex-based countermeasure that looks at the URL expressions on the HTTP requests inspected

– This was effective and dropped the attack traffic completely

Rick Penwarden
CENGN
+1 613-963-1200 ext. 329
email us here