SDi Resilience: Heavy Traffic and DoS Attacks

This report presents the findings from a study conducted by Bastionne to demonstrate the robustness, efficiency, and security capabilities of our Secure Digital Interaction (SDi) technology. The study aims to illuminate SDi's ability to manage heavy traffic loads and block illegitimate access attempts under a simulated Distributed Denial of Service (DDoS) scenario, while maintaining secure and efficient operations of legitimate processes. Conducted within an Azure cloud Virtual Network (VNet) environment, the study involved the use of SDi to protect and facilitate gameplay of the Ninvaders game, under conditions that simulated both normal and extreme cybersecurity threats.

Network Setup

Cloud Environment

Azure Cloud VNet with two 1GB, general compute, Ubuntu Virtual Machines (VMs). See the diagram on the next page for an overview of the setup.

Applications and Hardware

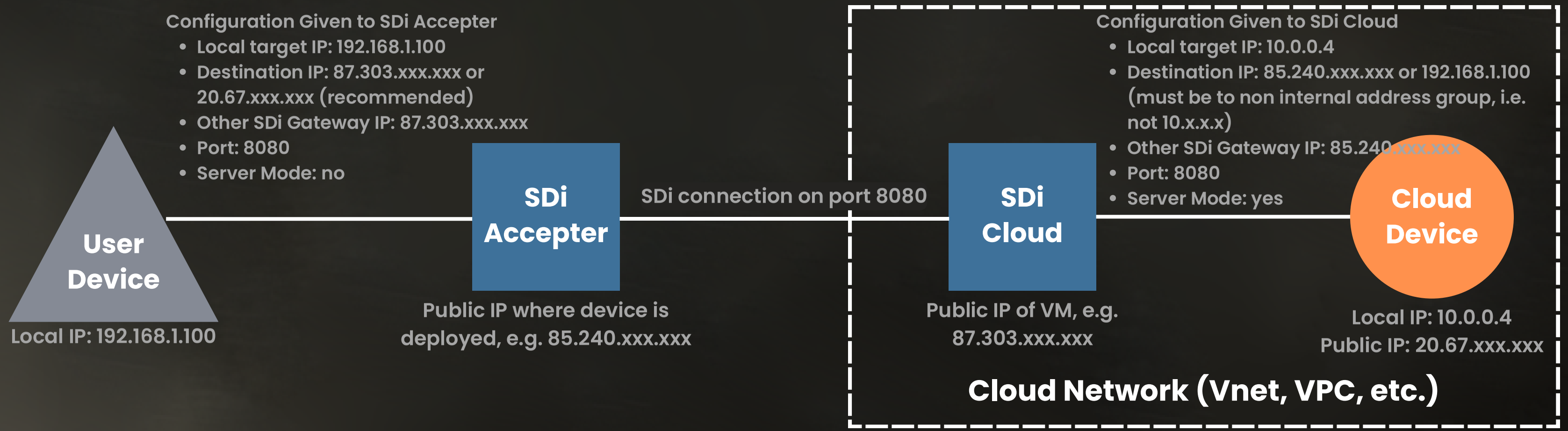
Ninvaders game installed on one VM. Two instances of SDi, one instance installed on the other Azure Ubuntu VM, the other on a physical machine in the corporate network (HP 255 G8). Paired with SSH to access the VMs for deployment and gameplay. Indeed, this means that traffic was doubly encrypted, further denoting the performance of SDi. Finally, tcpdump was used to monitor trafic to and from the machines.

Simulation Parameters

The scenario scaled from one to eight instances of the game, simulating legitimate user traffic. Concurrently, the VNet was bombarded with up to 2 million packets per minute of mixed legitimate and illegitimate traffic, simulating a high-scale illegitimate access attempt and a Distributed Denial of Service (DDoS) scenario.

Network Diagram

REGULAR CONFIGURATION USER TO CLOUD



Local IP: 192.168.1.100

Configuration Given to SDi Accepter
- Local target IP: 192.168.1.100
- Destination IP: 87.303.xxx.xxx or 20.67.xxx.xxx (recommended)
- Other SDi Gateway IP: 87.303.xxx.xxx
- Port: 8080
- Server Mode: no

Public IP where device is deployed, e.g. 85.240.xxx.xxx

Configuration Given to SDi Cloud
- Local target IP: 10.0.0.4
- Destination IP: 85.240.xxx.xxx or 192.168.1.100 (must be to non internal address group, i.e. not 10.x.x.x)
- Other SDi Gateway IP: 85.240.xxx.xxx
- Port: 8080
- Server Mode: yes

Public IP of VM, e.g. 87.303.xxx.xxx

Local IP: 10.0.0.4
Public IP: 20.67.xxx.xxx

Cloud Network Settings of SDi Cloud VM:
Allow inbound tcp access on port 8080 from 85.240.xxx.xxx.

Cloud Network Settings of Cloud Device:
Disable non cloud network inbound access to Cloud device.

Findings

Traffic Management

SDi successfully managed escalating traffic loads from multiple game instances without degradation in performance or security.

Security Efficacy

Throughout the connection, SDi adeptly differentiated between legitimate and illegitimate traffic, ensuring uninterrupted service for authorised users while blocking and blacklisting offending machines.

Encryption and Security Standards

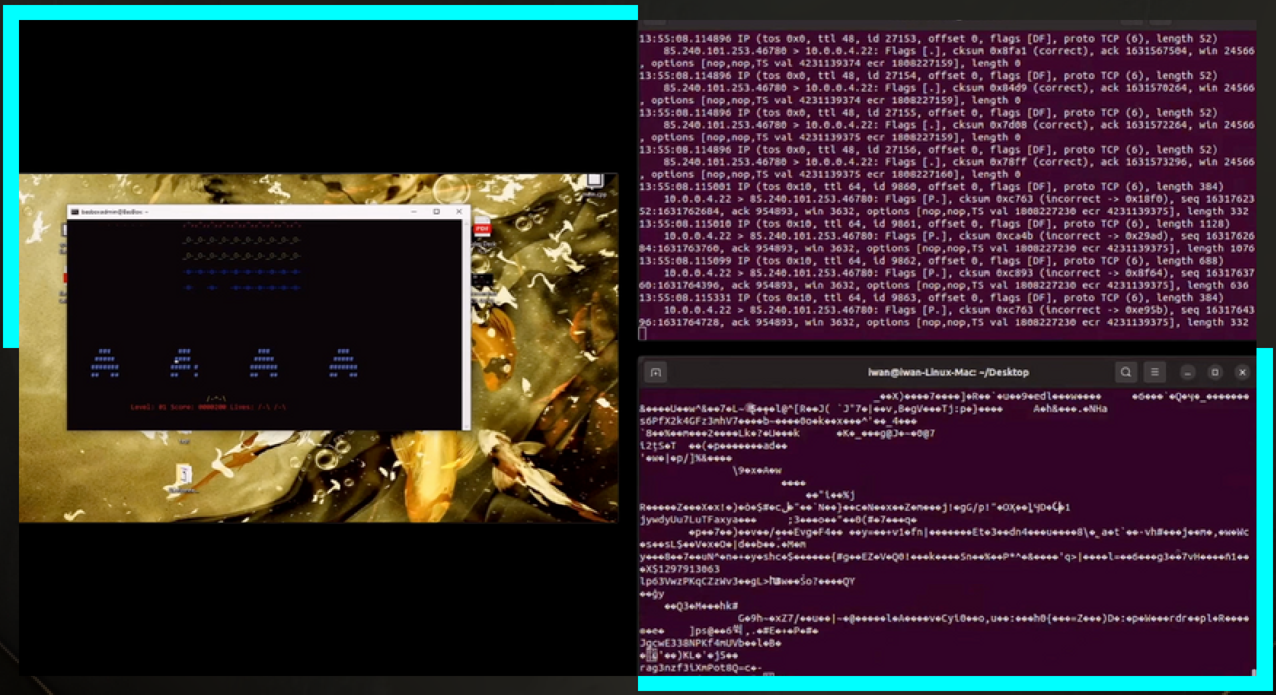
Utilising tcpdump, we verified that all traffic was encrypted to a quantum-secure standard. This encryption covered not just the gameplay data but all digital interactions to the VNet, showcasing SDi's comprehensive security measures, including Machine Identity Management (MIM), Perimeter VPN tunneling, and Secure Access Service Edge (SASE).

Performance under Threat

Even under simulated DDoS attacks, SDi demonstrated exceptional capability in maintaining operational integrity, with no legitimate traffic being erroneously blocked or delayed.

Analysis

The study confirmed SDi's superior design in handling both high volumes of network traffic and sophisticated cyber threats. The ability of SDi to distinguish between legitimate and malicious traffic with precision underlines its value in contemporary cloud environments where security and performance are paramount. The encryption of traffic to quantum-secure standards further reinforces Bastionne's commitment to providing future-proof cybersecurity solutions.



```
13:55:08.114896 IP (tos 0x0, ttl 48, id 27153, offset 0, flags [DF], proto TCP (6), length 52)
    85.240.101.253.46780 > 10.0.0.4.22: Flags [.], cksum 0x8fa1 (correct), ack 1631567504, win 24566
, options [nop,nop,TS val 4231139374 ecr 1808227159], length 0
13:55:08.114896 IP (tos 0x0, ttl 48, id 27154, offset 0, flags [DF], proto TCP (6), length 52)
    85.240.101.253.46780 > 10.0.0.4.22: Flags [.], cksum 0x84d9 (correct), ack 1631570264, win 24566
, options [nop,nop,TS val 4231139374 ecr 1808227159], length 0
13:55:08.114896 IP (tos 0x0, ttl 48, id 27155, offset 0, flags [DF], proto TCP (6), length 52)
    85.240.101.253.46780 > 10.0.0.4.22: Flags [.], cksum 0x7d08 (correct), ack 1631572264, win 24566
, options [nop,nop,TS val 4231139375 ecr 1808227159], length 0
13:55:08.114896 IP (tos 0x0, ttl 48, id 27156, offset 0, flags [DF], proto TCP (6), length 52)
    85.240.101.253.46780 > 10.0.0.4.22: Flags [.], cksum 0x78ff (correct), ack 1631573296, win 24566
, options [nop,nop,TS val 4231139375 ecr 1808227160], length 0
13:55:08.115001 IP (tos 0x10, ttl 64, id 9860, offset 0, flags [DF], proto TCP (6), length 384)
    10.0.0.4.22 > 85.240.101.253.46780: Flags [P.], cksum 0xc763 (incorrect -> 0x18f0), seq 16317623
52:1631762684, ack 954893, win 3632, options [nop,nop,TS val 1808227230 ecr 4231139375], length 332
13:55:08.115010 IP (tos 0x10, ttl 64, id 9861, offset 0, flags [DF], proto TCP (6), length 1128)
    10.0.0.4.22 > 85.240.101.253.46780: Flags [P.], cksum 0xca4b (incorrect -> 0x29ad), seq 16317626
84:1631763760, ack 954893, win 3632, options [nop,nop,TS val 1808227230 ecr 4231139375], length 1076
13:55:08.115099 IP (tos 0x10, ttl 64, id 9862, offset 0, flags [DF], proto TCP (6), length 688)
    10.0.0.4.22 > 85.240.101.253.46780: Flags [P.], cksum 0xc893 (incorrect -> 0x8f64), seq 16317637
60:1631764396, ack 954893, win 3632, options [nop,nop,TS val 1808227230 ecr 4231139375], length 636
13:55:08.115331 IP (tos 0x10, ttl 64, id 9863, offset 0, flags [DF], proto TCP (6), length 384)
    10.0.0.4.22 > 85.240.101.253.46780: Flags [P.], cksum 0xc763 (incorrect -> 0xe95b), seq 16317643
96:1631764728, ack 954893, win 3632, options [nop,nop,TS val 1808227230 ecr 4231139375], length 332
```

Conclusion

The effectiveness of SDi in a high-threat simulation demonstrates its readiness and reliability for real-world applications, particularly in environments vulnerable to heavy digital traffic and potential cyberattacks. Conclusive findings not only validate Bastionne's claims regarding SDi's capabilities but also illustrates its practical benefits in ensuring secure, efficient, and uninterrupted digital interactions under various conditions.