**DOS attack mitigation**

The attack that degrades or block the availability of a service of users. Endpoint dos can be performed by exhausting the system resources that service is hosted. Attacker can target various layers of application stack that hosted this service like OS layer. Attacking each layer requires different techniques that take advantage of bottlenecks that are unique to the respective components. DOS attack can be performed using single system or multiple systems (botnets) which is commonly referred to distributed DOS (DDOS). DOS attack categorized as Endpoint dos or Network dos.

**Endpoint DOS mitigation:**

ID: M1037

Version: 1.1

Created: 11 June 2019

Last Modified: 17 October 2024

Endpoint DOS can be mitigated by filtering network traffic by follow the following table

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Name** | | **Use** |
| [T1499](https://attack.mitre.org/techniques/T1499) | [Endpoint Denial of Service](https://attack.mitre.org/techniques/T1499) | | Leverage services provided by Content Delivery Networks (CDN) or providers specializing in DOS mitigation to filter traffic upstream from services. Filter boundary traffic by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport. To defend against SYN floods, enable SYN Cookies. |
|  | [.001](https://attack.mitre.org/techniques/T1499/001) | [OS Exhaustion Flood](https://attack.mitre.org/techniques/T1499/001) |
|  | [.002](https://attack.mitre.org/techniques/T1499/002) | [Service Exhaustion Flood](https://attack.mitre.org/techniques/T1499/002) |
|  | [.003](https://attack.mitre.org/techniques/T1499/003) | [Application Exhaustion Flood](https://attack.mitre.org/techniques/T1499/003) |
|  | [.004](https://attack.mitre.org/techniques/T1499/004) | [Application or System Exploitation](https://attack.mitre.org/techniques/T1499/004) |

**Network DOS mitigation:**

ID: M1037

Version: 1.1

Created: 11 June 2019

Last Modified: 17 October 2024

A Network DOS will occur when the bandwidth capacity of the network connection to a system is exhausted due to the volume of malicious traffic directed at the resource or the network connections and network devices the resource relies on. We can also mitigate network dos attack by filtering network traffic by follow the following table.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Name** | | **Use** |
| [T1498](https://attack.mitre.org/techniques/T1498) | [Network Denial of Service](https://attack.mitre.org/techniques/T1498) | | When flood volumes exceed the capacity of the network connection being targeted, it is typically necessary to intercept the incoming traffic upstream to filter out the attack traffic from the legitimate traffic. Such defenses can be provided by the hosting Internet Service Provider (ISP) or by a 3rd party such as a Content Delivery Network (CDN) or providers specializing in DOS mitigation.  Depending on flood volume, on-premises filtering may be possible by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport.  As immediate response may require rapid engagement of 3rd parties, analyze the risk associated to critical resources being affected by Network DOS attacks and create a disaster recovery plan/business continuity plan to respond to incidents. |
|  | [.001](https://attack.mitre.org/techniques/T1498/001) | [Direct Network Flood](https://attack.mitre.org/techniques/T1498/001) |
|  | [.002](https://attack.mitre.org/techniques/T1498/002) | [Reflection Amplification](https://attack.mitre.org/techniques/T1498/002) |

**References:**

[Filter Network Traffic, Mitigation M1037 - Enterprise | MITRE ATT&CK®](https://attack.mitre.org/mitigations/M1037/)