Ref: P015	TLS Denial of Service & Blackmail Policy

Introduction:
Denial-of-service (DoS) attacks typically floods our servers, systems or networks with traffic in order to overwhelm the TLS server resources and make it difficult or impossible for legitimate users to use them. While an attack that crashes a server can often be dealt with successfully by simply rebooting the system, flooding attacks can be more difficult to recover from.
Our IT department suggests the following may indicate such an attack:
Degradation in network performance, especially when attempting to open files stored on the network or accessing websites;

Inability to reach a particular website;

Difficulty in accessing any website; and

A higher than usual volume of spam email.

Experts recommend a number of strategies for TLS Limited as a company to defend against a denial-of-service attack, starting with preparing an incident response **(See below)** plan well in advance of any attack. Once there is suspicion that a DoS attack is underway, enterprises should contact Pyranet (ISP) to determine whether the incident is an actual DoS attack or degradation of performance caused by some other factor. The ISP can help mitigate the attack by rerouting or throttling malicious traffic and using load balancers to reduce the effect of the attack.

Preparing for DoS Attacks

You can't prevent DoS assaults. The fact is that cybercriminals are going to attack. Some are going to hit their targets, regardless of the defenses we have in place.

However, there are steps we can take to spot a brewing storm, including:

- Monitoring your traffic to look for abnormalities, including unexplained traffic spikes and visits from suspect IP address and geolocations. All of these could be signs of attackers performing "dry runs" to test your defenses before committing to a full-fledged attack. Recognizing these for what they are can help you prepare for the onslaught to follow.
- Keep an eye on social media (particularly Twitter) and public wastebins (e.g., Pastebin.com) for threats, conversations and boasts that may hint on an incoming attack.
- Consider using third-party DDoS testing (i.e., pen testing) to simulate an attack against your IT infrastructure so you can be prepared when the moment of truth arrives. When you undertake this, test against a wide variety of attacks, not just those with which you are familiar.
- Create a response plan and a rapid response team, whose job is to minimize the impact of an assault. When you plan, put in place procedures for your customer support and communication teams, not just for your IT professionals.

What do we need to do – our approach.

This first step in preparing TLS Limited is to deal with a DoS incident is to assess your risk. Important basic questions include:

- **Which infrastructure assets need protection?**
- **What are the soft spots, or single points of failure do we have within our systems?**
- **What is required to take them down?**
- **How and when will we know we have been targeted? Will it be too late?**
- **What are the impacts (financial and otherwise) of an extended outage?**

Armed with this information, it's then time to prioritize TLS Limited concerns, examining various mitigation options within the framework.

If you're running a commercial website or online applications (e.g., SaaS applications, online banking, e-commerce), you're probably going to want 24×7, always-on protection. A large law firm, on the other hand, may be more interested in protecting its infrastructure—including email servers, FTP servers, and back office platforms—than its website. This type of business may opt for an "on demand" solution.

The second step is to choose the method of deployment. The most common and effective way to deploy on-demand DoS protection for your core infrastructure services across an entire subnet is via border gateway protocol (BGP) routing. However, this will only work on demand, requiring you to manually activate the security solution in case of an attack.

Consequently, if you're in need of an always-on DoS protection for your web application, you should use DNS redirection to reroute all website traffic (HTTP/HTTPS) through your DoS protection provider's network (usually integrated with a content delivery network,). The advantage of this solution is that most CDNs offer on-call scalability to absorb volumetric attacks, at the same time minimizing latency and accelerating content delivery.

Incident Response Steps (Overview)

1. Preparation: Establish contacts, define procedures, and gather tools to save time during an attack.
2. Analysis: Detect the incident, determine its scope, and involve the appropriate parties.
3. Mitigation: Mitigate the attack's effects on the targeted environment.
4. Wrap-up: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Incident Response - General Considerations

- Denial of Service (DoS) attacks often take the form of flooding the network with unwanted traffic; some attacks focus on overwhelming resources of a specific system.
- It will be very difficult to defend against the attack without specialized equipment or your ISP's help.
- Often, too many people participate during incident response; limit the number of people on the team.
- DDoS incidents may span days. Consider how your team will handle a prolonged attack. Humans get tired.
- Understand your equipment's capabilities in mitigating a DDoS attack. Many under-appreciate the capabilities of their devices, or overestimate their performance.

Prepare for a Future Incident

If you do not prepare for a DoS incident in advance, you will waste precious time during the attack.

1. Contact our ISP to understand the paid and free DoS mitigation it offers and what process you should follow.
2. Create a whitelist of the source IPs and protocols you must allow if prioritising traffic during an attack. Include your big customers, critical partners, etc.
3. Confirm DNS time-to-live (TTL) settings for the systems that might be attacked. Lower the TTLs, if necessary, to facilitate DNS redirection if the original IPs get attacked.
4. Establish contacts for your ISP, law enforcement, IDS, firewall, systems, and network teams. (See TLS Limited emergency policy)
5. Document your IT infrastructure details, including business owners, IP addresses and circuit IDs; prepare a network topology diagram and an asset inventory.
6. Understand business implications (e.g., money lost) of likely DoS attack scenarios.
7. If the risk of a DoS attack is high, consider purchasing specialized DDoS mitigation products or services.
8. Collaborate with your BCP/DR planning team, to understand their perspective on DDoS incidents.
9. Harden the configuration of network, OS, and application components that may be targeted by DDoS.
10. Baseline your current infrastructure's performance, so you can identify the attack faster and more accurately.

Analyse the Attack

- Understand the logical flow of the DoS attack and identify the infrastructure components affected by it.

- Review the load and logs of servers, routers, firewalls, applications, and other affected infrastructure.
- Identify what aspects of the DoS traffic differentiate it from benign traffic (e.g., specific source IPs, destination ports, URLs, TCP flags, etc.).
- If possible, use a network analyser (e.g. tcpdump, ntop, Aguri, MRTG, a NetFlow tool) to review the traffic.

Mitigate the Attack's Effects

- While it is very difficult to fully block DoS attacks, you may be able to mitigate their effects.
- Attempt to throttle or block DoS traffic as close to the network's "cloud" as possible via a router, firewall, load balancer, specialized device, etc.
- Terminate unwanted connections or processes on servers and routers and tune their TCP/IP settings.
- If possible, switch to alternate sites or networks using DNS or another mechanism. Blackhole DDoS traffic targeting the original IPs.
- If the bottle neck is a particular a feature of an application, temporarily disable that feature.
- If possible, add servers or network bandwidth to handle the DoS load. (This is an arms race, though.)
- If possible, route traffic through a traffic-scrubbing service or product via DNS or routing changes.
- If adjusting defences, make one change at a time, so you know the cause of the changes you may observe.
- Configure egress filters to block the traffic your systems may send in response to DoS traffic, to avoid adding unnecessary packets to the network.

Wrap-Up the Incident and Adjust

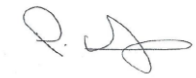
- Consider what preparation steps you could have taken to respond to the incident faster or more effectively.
- If necessary, adjust assumptions that affected the decisions made during DoS incident preparation.
- Assess the effectiveness of your DoS response process, involving people and communications.
- Consider what relationships inside and outside your organizations could help you with future incidents.

Guidance & policy for TLS on the Blackmail side

While there have been instances where DoS attackers demand payment and try to blackmail victims within TLS limited to end the attacks, financial profit is not usually the

motive behind this type of attack, However if such an event was to happen whereby monies are being asked for our policy would be to involve the police as soon as possible. In many cases, the attackers wish to cause harm to TLS Limited as an organisation or an individual targeted in the attack; in other cases, the attackers are simply attempting to sabotage the system or organisation, causing the greatest damage or inconvenience to the greatest number of people at work. When a perpetrator of a DoS attack is identified, the reasons for an attack may also be revealed.

Paul Chamley



Managing Director

Ref: P015	TLS Denial of Service & Blackmail Policy

Revision History

Revision	Date	What has changed?	Who has written it?	Who has approved it?
00	**25/05/2015**	**First Issue**	**QE&SH Manager**	**MD**
01	**27/01/2016**	**Reviewed**	**QE&SH Manager**	**MD**
02	**19/01/2017**	**Reviewed**	**QE&SH Manager**	**MD**
03	**26/05/2020**	**Reviewed, updated to new document control format, name & signature of MD added**	**Systems Manager**	**MD**
04	**26/05/2021**	**Reviewed nd TA logo added**	**Systems Manager**	**MD**
05	**26/05/2022**	**Reviewed**	**Systems Manager**	**MD**
06	**24/01/2023**	**New TLS Group Logo added**	**Systems Manager**	**MD**
07	**17/01/2024**	**Annual review**	**Systems Manager**	**MD**
08	**17/01/2025**	**Annual review**	**Systems Manager**	**MD**
09	**17/01/2026**	**Review**	**Systems Manager**	**MD**

Ref: P015	TLS Denial of Service & Blackmail Policy