UPTIME. ALL THE TIME. GUARANTEED.

www.vistnet.com

DDoS Protection Company

Anti-DDoS ACTION PLAN

for

Hosting Providers – a Guideline

prepared by

Vistnet Corporation Ltd.

This document aims to provide hosting vendors with general guidelines for adequate reaction to DDoS Floods. The information provided below is of general nature and is intended to orientate. A standard hosting topology use case is discussed at more length for a more detailed outline on possible actions when under a DDoS attack.

Vistnet are happy to provide further information and advice on mitigation techniques on a case-by-case basis, so please feel free to contact us at **sales@vistnet.com** with your specifics.

STEPS TO PROTECT AGAINST DDoS FLOODS

STEP 1:
Determine The Scope Of The Attack

Find out which services are being targeted. Is it client webserver(s), DNS servers, mail servers, network nodes, etc.?

Usually this is done by checking the NMS for traffic spikes on switch ports, congestions, CPU/RAM usage spikes on all machines and network nodes. In the absence of an NMS or its inaccessibility this is done by checking each node and link separately.

If possible, determine the type of the attack (what protocol is being used) and how it compromises the targeted service.

STEP 2:
Take Basic Measures To Block The DDoS Attack

After determining the target and type of the attack try finding the source using packet sniffer tools to see the source IP addresses of the packets.

If applicable, try blocking the traffic as near to its source as possible. If the source is within the DC that your equipment is located, contact on-site personnel with evidence and ask them to block the attack before your uplink or terminate the misbehaving customer.

If the source cannot be determined, ask your upstream provider if they can provide details on where the malicious traffic is originating and whether it can be blocked before entering your networks.

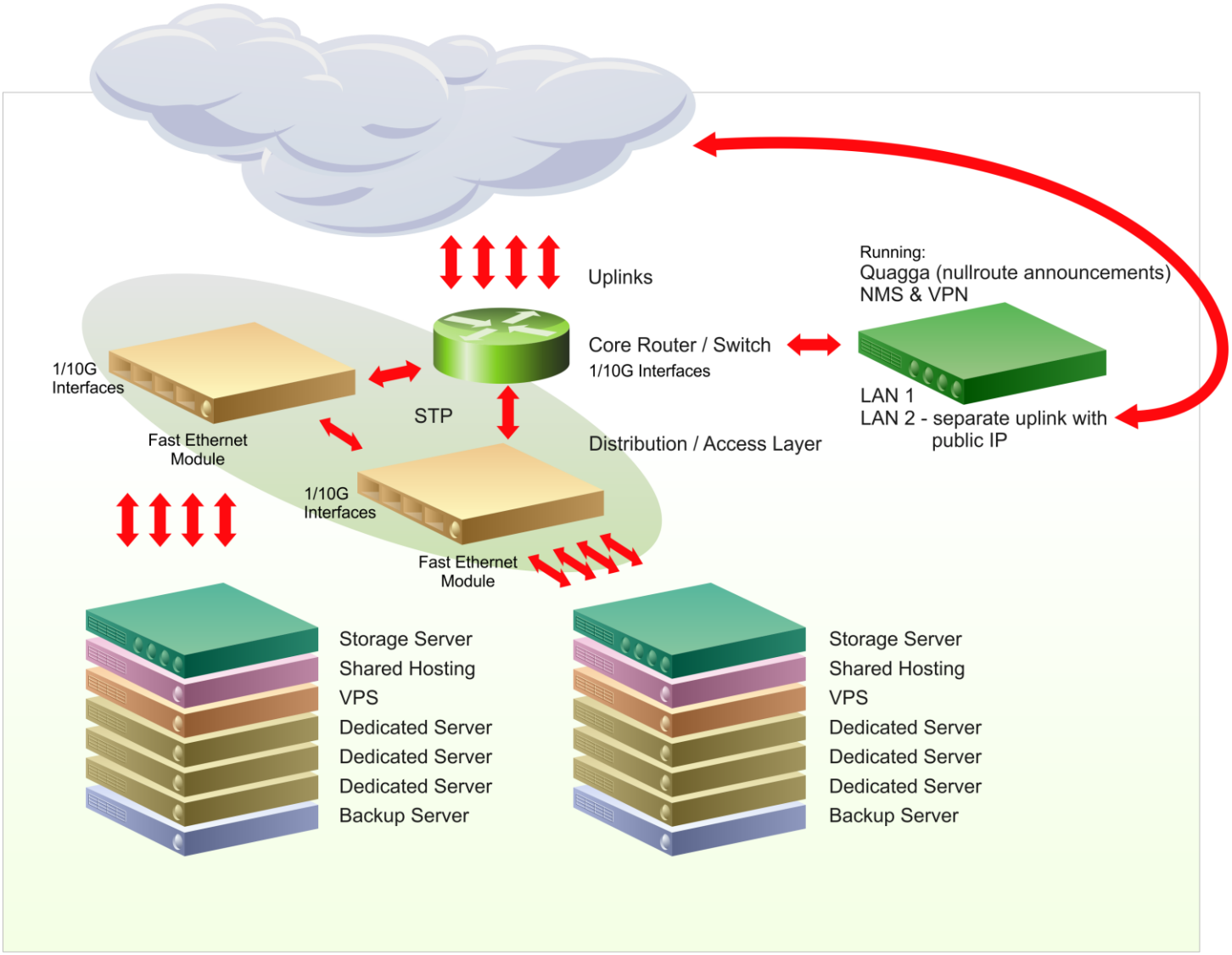
STEP 3:
Get External Help

In case results from the above steps are still not satisfactory, it is best to seek professional help from a DDoS Mitigation Company.

USE CASE: based on a typical hosting vendor topology

Prerequisites: The following use case scenario is to serve as example describing a procedure/guideline of an actual hosting provider's support for dealing with DDoS attacks. It assumes a topology similar to the one described in the topology diagram. Familiarity of the support personnel with the network topology and/or access to the topology diagram as well as privileges to access the network/server nodes is necessary.

TOPOLOGY



STEP 1:
Determine The Scope Of The Attack

- Check the uplink graph for excessive bandwidth consumption. If the uplink is over-flooded, the core switch along with all other nodes will probably be inaccessible from the outside and all services will be affected. In case the attack exceeds your uplink capacity, immediately notify Level 3 support and call upstream providers giving them as much details as you are able to gather.
- If the switch is inaccessible from the outside network use the VPN to access the LAN and telnet to the switch using its private IP address. The management VLAN should be unaffected by the attack. If the switch is still inaccessible, call on-site personnel and third line support immediately.
- Determine who the target of the attack is. Mirror the uplink port on core switch to the backup port to the NMS (Gi0/1/0 -> Gi0/1/2). SSH to the NMS and use tcpdump to determine targeted IPs.
- If no excessive bandwidth consumption is detected and there are no infrastructural problems, check the NMS for any nodes with CPU or RAM consumption spikes, If any, check their web server logs for repeated reoccurring requests from the same IP addresses.

STEP 2:
Take Basic Measures To Block The DDoS Attack

- If a volumetric attack is in place and sources can be easily determined (are not spoofed), call the upstream provider and ask them to temporarily block the subnets/IP's from which the attack is originating.
- If the sources are spoofed and the attack is affecting other customers, null-route the targeted IP (Procedure B08). Lift the announcement every 15 minutes to see if traffic is still coming.
- If the attack is targeting a shared IP address, null-route it and notify all customers. Re-spawn all virtual hosts on one of backup servers BS01-BS03 and start changing DNS A records of the domains, giving each host five minutes to propagate. During this time monitor tcpdump on the new server.
- Once you start seeing attack traffic coming to the server, change the A record of the most recently transferred domain to 127.0.0.1 and proceed with moving the remaining domains one by one. Communication with the customer under attack is covered in Step 3.
- In case of an Application Layer attack, notify the owner of the domain showing logs as evidence. Proceed with step 3.

STEP 3: **Propose Professional Mitigation Service To Affected Customers**	• In the event that none of the above steps give the desired result or an application layer attack is in place (given that the target of the attack has been determined throughout the investigation), notify the owners of the domain under DDoS attack and propose professional assistance from your partners. • Inform customer of the cost of the service and let them know that this is the only way you are able to continue their service referring to specific violations of your TOS. Always include detailed description and logs supporting your claims. • If the customer agrees, notify external vendor's support stating targeted domain and backend IP address for the website. Always change the IP address of targeted domains and provide the fresh IP to external vendor. • Do not set the new IP as A record for the domain. You will receive instructions containing a protected IP address from external vendor's support which in turn must be set as A record for the targeted domain.

ADDITIONAL CONSIDERATIONS

Data Collection & Analysis:	Gathering data from a DDoS Flood can present storage capacity issues, due to the sheer size of accumulated data in a relatively short time. Thus, It is not always feasible to collect all possible data for a flood, especially when it originates from spoofed IP's. When collecting data, keep in mind what portion of it is usable for forensic analysis or for any further meaningful processing.
Setup/Provision Specifics:	While this Action Plan is drafted with maximum uniformity in mind, it is not possible to describe or generalize on all possible topology and running application combinations. Applying the steps described herein may not yield any desired results, as it is always best to take into account the specifics of a given setup, topology, application configuration and qualified personnel availability. As stated above, Vistnet look forward to discussing your needs and provide customized advice to ensure best fit and applicability to particular operational structures.

□