REDSPAM

SOLUTION OVERVIEW
redspam.com

Client On-boarding

Technical concept and details

Why RedSpam?

▶ PERFORMANCE

RedSpam's **True Dynamic Mitigation™** is a unique combination of industry-leading hardware and patent-pending software that offers unprecedented protection. Attacks are blocked close to source and genuine traffic is never compromised. Monitoring, early threat detection and seamless integration of 3-way mitigation combine to deliver a robust service.

▶ EXPERIENCE

RedSpam's technical team has been successfully defending DDoS attacks in the most demanding environments.

▶ CLOUD BASED, TRANSPARENT SERVICE

RedSpam provides protection within minutes through DNS or BGP re-routing. RedSpam do not need to access the clients' security certificates, the hardware is unaffected, complexity or risks of integrating new hardware into your systems is minimised.

Example BGP Solution Overview

Ampito's RedSpam DDoS Monitoring and Mitigation Solution has two UK cleaning centres located in Global Switch 2 and InterXion data-centres. A fast BGP conversion is provided by peering at Tier 1 with Level 3 and Global Crossing or by accommodating COLT's demarcation points in our racks. The scrubbing centre design is based on geographical redundancy providing high availability and dilution of DDoS attacks.

RedSpam suggests that a direct circuit will be the most appropriate on-boarding method for the BGP based solution. Alternatively, a GRE solution could be implemented (typically utilised for proof of concept and while awaiting circuit provision).

A. BGP Redirection Proposed Solution

1. Client and RedSpam domains complete the BGP peering process, including registration with RIPE NCC.
2. Client and RedSpam will agree on two VLANs; one VLAN dedicated to the BGP peering process, and one VLAN dedicated to delivering clean return traffic to the client by RedSpam.
3. Note that control of the BGP routing announcements associated with the client /24 is a requirement for any BGP based monitoring and mitigation solution.
4. In the event of an attack, the client will advertise the /24 prefix to RedSpam and the client will cease announcing it.
5. During an attack, RedSpam will advertise upstream the received /24 prefix and traffic will then be redirected to the RedSpam cleaning centres.
6. The RedSpam threat mitigation system will further inject a /32 route for the individual IP under DDoS attack into the local routing table for on-ramping traffic to the mitigation engine. All other /32's are routed straight through.
7. Once the traffic is cleaned, it will be off-ramped and delivered to the client via the clean return VLAN.to their websites, this information can be made available through the x-forwarded-for (XFF) header.
8. Please find a diagram on page 3.

B. GRE Option – Proof of Concept Redirection Solution

1. The GRE solution will follow the same steps as above, but two GRE tunnels will be established instead of 2 VLANs. One GRE tunnel will be used for BGP peering and the other for delivering clean return traffic (after it has been through the mitigation engine).

This can be a fully automated process (the client can chose between an automated and a manual process); the client can permanently advertise its prefix to RedSpam and, in case of an attack, the RedSpam NOC will update the required prefix-lists in order for the route/routes to be advertised upstream and thus redirect the traffic to the cleaning centres. Alternatively, if the client requires a manual element/interaction, it can advertise the /24 route to RedSpam only when under an attack.

C. Attack Detection and Mitigation Mechanisms

1. RedSpam will sample the client's traffic using flow technology.

2. The client and RedSpam will jointly build a detection template to determine which alerts will be categorised as low, medium, and high.

3. For the misuse detection template, the following values can be set: number of accepted ICMP, IP Fragment, IP NULL, IP Private, TCP NULL, TCP RST, TCP SYN, UDP, Total Traffic.

4. A profiled detection template will also be completed as part of the on-boarding process.

5. When the thresholds are met, the RedSpam system will automatically start the mitigation process according to a pre-defined mitigation template.

6. The client and RedSpam will agree the counter-measures that will be used during automitigation (these can always be manually overwritten by human intervention during an attack): IPv4 Address Filter Lists, IPv4 Black/White Lists, IP Location Filter Lists, Zombie Detection, TCP SYN Authentication, DNS Scoping, DNS Authentication, TCP Connection Reset, Payload Regular Expression, Source /24 Baselines, Protocol Baselines, DNS Malformed, DNS Rate Limiting, DNS NXDomain Rate Limiting, DNS Regular Expression, HTTP Malformed, HTTP Scoping, HTTP Rate Limiting, HTTP/URL Regular Expression, SIP Malformed, SIP Request Limiting, Shaping, IP Location Policing, SSL Negotiation, Slowloris style slow HTTP attacks, GeoIP.

7. Note that the mitigation template is generally amended by RedSpam technical staff during an attack as the majority of DDoS attacks contain multiple attack vectors (i.e. several vectors within the same attack), therefore additional counter-measures need to be enforced in real-time in order to mitigate the attack.

8. During the attack the clean return traffic will be delivered to the client via the established VLAN.

9. Once the attack stops, RedSpam will cease advertising the /24 client route and the traffic will be handed back to the client routers.

Why RedSpam?

▶ FIXED PRICE

Whatever the level of attack, you only pay the price agreed for the service. RedSpam does not charge for size, number of, or duration of attacks and provides same-day, fixed price quotations for the protection level required.

▶ FLEXIBILITY

RedSpam believes that every business should have protection from the damage caused by DDoS attacks. However, the needs of organisations differ, so a choice of service packages is offered to suit differing requirements. These are priced to meet a range of budgets, making the protection accessible to all.

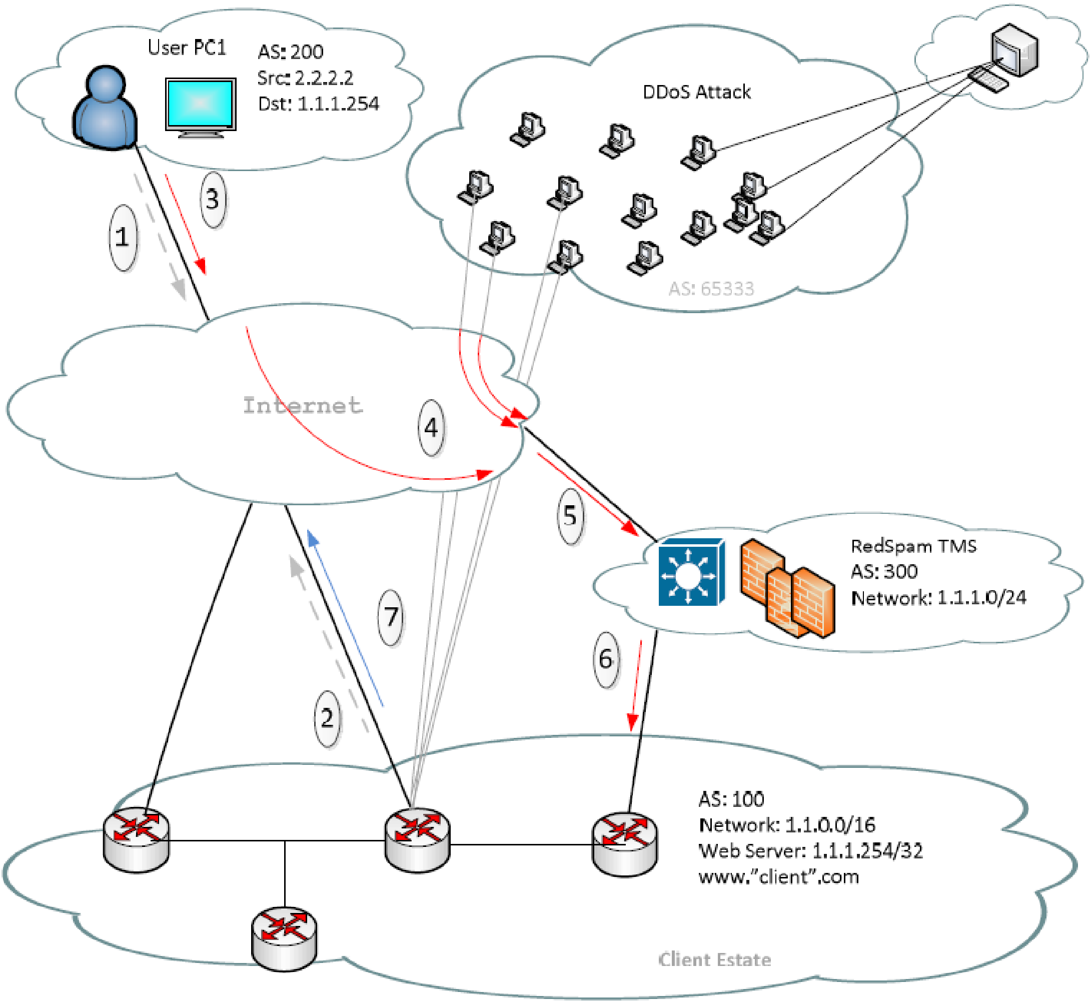
▶ LOCAL PROTECTION

European-based scrubbing ensures no latency problems.

▶ LOCAL 24/7/365 SUPPORT

Telephone support is on-hand from European-based technical experts.

Example Logical Diagram – BGP Integration Solution



Example Logical Diagram – BGP Integration Solution

Normal Circumstances – Network 1.1.0.0/16 is advertised by AS: 100

1. User PC1 sends a http request to 1.1.1.254 for www."client".com

2. Client's Web Server replies to User PC1, destination IP: 2.2.2.2

================================

Client Gets Attacked – Network 1.1.1.0/24 is advertised by AS: 300

3. User PC1 sends a http request to 1.1.1.254 for www."client".com

4. The backbone BGP table is updated with a longer subnetmask for destination 1.1.1.254/24, (ie a better path) advertised by AS: 300

5. All traffic with the destination 1.1.1.254, including the DDoS attack from AS: 65333, is now forwarded to the RedSpam TMS

6. RedSpam TMS mitigates the DDoS attack and separates the dirty traffic form the clean traffic; the clean traffic from 2.2.2.2 is then sent to AS: 100

7. The client Web Server, now fully functional, receives the request from User PC1 and replies accordingly