HOW TO PREVENT DDOS ATTACKS IN A SERVICE PROVIDER ENVIRONMENT

The frequency and sophistication of Distributed Denial of Service attacks (DDoS) on the Internet are rapidly increasing. Most of the earliest DDoS attacks were simply arbitrary attempts by hackers to gain simple notoriety. However, they have evolved into serious criminal operations that threaten to attack businesses with significant financial and operational implications.

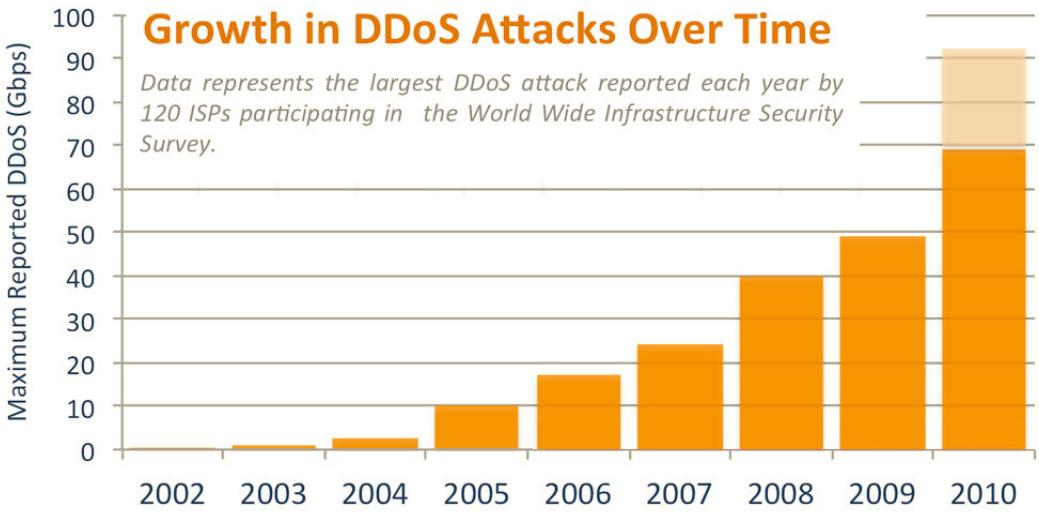
INTRODUCTION

Service providers are under mounting pressure to prevent, monitor and mitigate DDoS attacks directed toward their customers and their infrastructure. DDoS attacks on businesses are increasing at an alarming rate. Network security has now evolved to become a critical part of business success. A secure network infrastructure moulds the foundation for service delivery in all businesses, large and small. For network service providers and carriers, network security has always been important but today it strongly influences network design considerations and technology purchasing decisions more than ever before. Enterprise customers increasingly want their service providers to protect their network assets from large DDoS attacks and other security threats.

The sheer number and capability of botnets grows dramatically each year as well as the sophistication of application attack toolsets. HOIC and its succeeding generations of volunteer based, botnet controlled PCs will almost certainly evolve to pose a significant Internet-wide threat. However, traditionally the DDoS threat has come more from increasingly professional criminal hackers than volunteer activists or “hacktivists” The Internet is part of the critical national infrastructure but is unique in that it has no customary borders to safeguard it from attacks.

Attacks that are seen every day on the Internet include direct attacks, remote controlled attacks, reflective attacks, worms, and viruses. Specific attacks directed at a service provider’s infrastructure can be very damaging and cause wide spread outages. This paper covers these attacks and discusses techniques to prevent attacks including good security policies, new/updated product security testing, patch management, spoofed packet dropping (uRPF) and firewall/IDS/IPS deployment in a service provider environment. Protection of the provider’s infrastructure is another key aspect and is addressed in this paper.

Figure 1 the following graph plots the growth DDoS flooding attacks over the last decade



DDoS Attack Vectors in 2010 (Source – Arbor Networks)

DDOS ATTACKS

DDoS attacks can be classified as logic attacks and resource exhaustion flooding attacks. Logic attacks exploit security vulnerabilities to cause a server or service to crash or significantly reduce performance.

Resource exhaustion flooding attacks cause the server's or network's resources to be consumed to the point where the service is no longer responding or the response is significantly reduced.

Logic attacks will be evaluated based on their effect on the network infrastructure and critical network services (DNS, BGP, RADIUS, etc). A complete discussion of logic attacks is very broad and outside the scope of this paper.

Flooding attacks can be evaluated by their amplification factor. The amplification factor is the amount each source packet is multiplied by before reaching the victim. For example, in a direct flooding attack, for each source packet transmitted by the attacker, one packet is received at the victim's site. In a smurf reflective attack, each packet is reflected off a set of hosts that send multiple packets to the victim site. A smurf attack can achieve an amplification factor in the hundreds. In other words, for each source attack packet sent, hundreds of packets are received by the victim.

PREVENTION

Knowledge of DDoS tactics and methods is a fundamental key in implementing methods to prevent attacks. No service provider will be able to prevent all attacks. The goal is to raise the bar for people to launch attacks with;

POLICIES AND PROCEDURES. Security policies and procedures should be developed and in place to ensure that Company and best practices are followed. Security policies are a very important part of a service provider's overall security architecture and are critical for stopping abusive users. A service provider's Acceptable Use Policy (AUP) is a key tool for removing abusive customers from their network.

Service providers should also establish an Incident Response Team (IRT) that is responsible for responding to attacks. The IRT should develop procedures concerning:

- Who should be notified?
- What data needs to be collected (for possible law-enforcement action, later)?
- What responsive measures should be employed to protect the infrastructure or service?
- What is the escalation path for critical decisions?

DNS CONSIDERATIONS. One use for IPS systems is to protect DNS servers as the rate of false positive reactions will be much lower than for multi-purpose systems. An IPS can also be used to deny legitimate but unwanted traffic to DNS servers to reduce the load on the servers.

MANAGEMENT AND CONTROL PLANE PROTECTION. Protection of the management and control planes is critical for the successful operation of an ISP. It is easier to discuss both topics together because the router configuration to protect both is similar in many ways. Authenticated and encrypted protocols are preferred for router management. Protocols must be accepted only from trusted hosts. Steps to protect the control plane include: protection of the route engine using filters, authentication and integrity verification of routing protocol updates, rate limiting of diagnostic protocols and filtering of routing prefix updates sent from customers and peers.

ROUTER ENGINE PROTECTION. Router engines have limited bandwidth and resources compared with the data plane they control. The router engine should be protected from mistrusted sources to limit resource exhaustion attacks on the router itself and to limit reflective attacks from the router. Only required services and protocols should be turned on.

MONITORING

The next step in DDoS protection is monitoring for attacks. It is difficult to mitigate an attack without good information about the characteristics of the attack. The mitigation techniques used will depend on the level of pain and inconvenience your customer is willing to put up with.

NETFLOW MONITORING. Netflow is a very useful tool in monitoring traffic patterns and DoS/DDoS attacks.
Developed by Cisco in 1996, a flow is defined as having the following seven unique attributes:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Layer 3 protocol type
- TOS byte (DSCP)
- Input logical interface (ifIndex)

Each unique flow is counted in the router. The flow data can be exported to a separate collection and correlation system. Netflow is unidirectional and is currently only available on the router ingress interface. To monitor traffic in both directions all router interfaces must be monitored, including uplinks to the core routers.

MITIGATION

When a customer or the network infrastructure is under attack, monitoring is important for quick identification of the attack characteristics and entry points. Good mitigation techniques are a required part of a service provider's security architecture. Below are some examples of mitigation that can be adopted in a service provider environment.

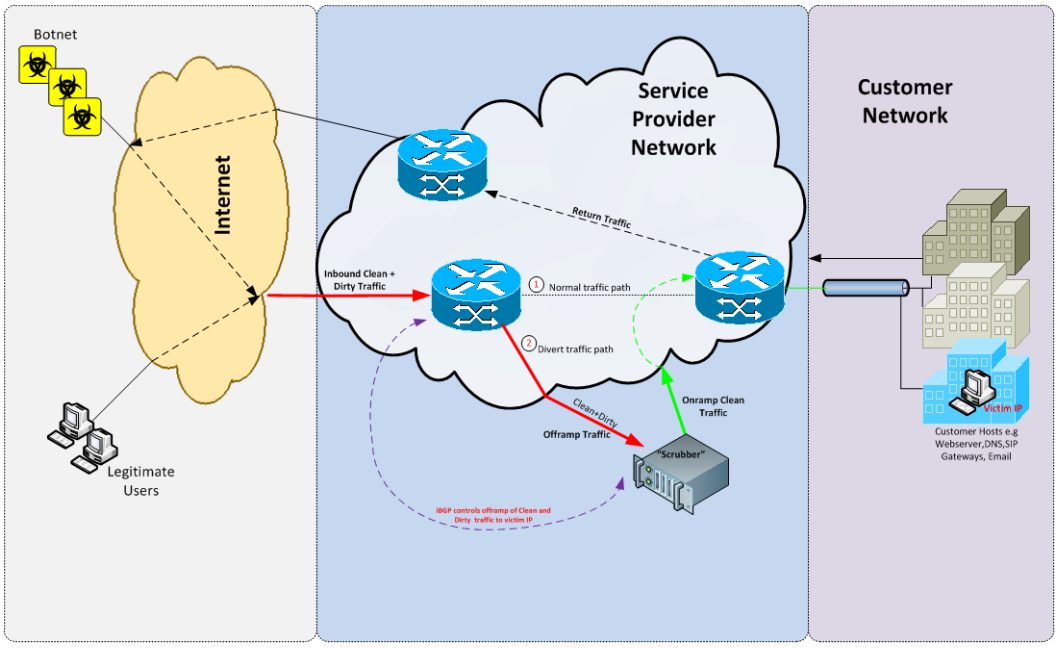
ACCESS CONTROL LISTS (ACLs). Access control lists (ACL) or firewall filters are the first line of defence for a service provider. For a simple DDoS attack directed at a single customer, deployment of an egress ACL on the customer's edge router is an easy way to stop the attack. The problem with this technique is scaling both from a router performance perspective and as the number of attacks managed increases. The management of a large number of temporary ACLs that may have performance impacts on different router hardware and software is non-trivial and can be very labour intensive and error prone. Most service providers have home grown scripts for their router configuration and ACL management.

DESTINATION BASED BLACK HOLE FILTERING. Black hole filtering is an effective, quick and simple technique for dropping attack traffic destined toward a victim. Using iBGP as a trigger mechanism, black hole filtering can be remotely triggered across the

entire perimeter of a provider's network. When an attack occurs, a static route is added to the trigger router to route the /32 IP address under attack to the bogon address block configured in the perimeter routers. The route is injected into iBGP and distributed to all routers in the network. The traffic for the attack is black holed at each ingress router to the network, effectively stopping the attack. This type of black hole filtering is only good to drop traffic based on the destination address.

BLACK HOLE SCRUBBING. Black hole shunting is another variation on the black hole filtering configuration. The difference is that instead of sending the traffic to the null0 or drop interface, the traffic is sent out a different physical interface. A data scrubber residing on the alternate data path can filter out the attack traffic "dirty traffic" from the good customer traffic "Clean traffic" and send the clean traffic to the customer. A number of vendors e.g Arbor Networks do provide products (Scrubber) that are specifically designed to monitor (using Netflow) and mitigate DDoS attacks buy cleaning diverted DDoS suspected traffic from the ingress of service provider Core networks to the scrubber and egress to customer networks.

Figure 2 Illustrates scrubbing technique of DDoS traffic



CONCLUSION

Prevention is always the best measure. Preparation is the key for service providers to mitigate attacks as they happen. Automated DDoS monitoring and reporting should be standard for service providers as reaction times have gone from days to minutes. Customers are beginning to expect the same reliability from the Internet as other critical infrastructures.

Reply
sytel

Sytel Reply UK is the company of the Reply group that is specialised in the Telecommunication, Media and Entertainment (TM&E) markets in the UK and Ireland. The Sytel Reply mission is to support clients during their technology and business innovation processes by planning, developing and managing solutions for Networking, BSS and OSS and Mobile Applications within TM&E service provider market.

Sytel Reply, thanks to its in-depth competence and experience, boasts a team of highly skilled professionals able to manage any end-to-end business and technology transformation programmes.

Sytel Reply UK
www.replyltd.co.uk