FireCircle: GRNET's approach to advanced network security services' management via bgp flow-spec and NETCONF

Leonidas Poulopoulos (leopoul@noc.grnet.gr) Network Applications Developer	*Michalis Mamalis (mmamalis@noc.grnet.gr) Network Administrator*	Andreas Polyrakis (apolyr@noc.grnet.gr) Technical coordinator
Greek Research & Technology Network (GRNET) NOC 56, Mesogeion Ave. 11527 Athens, Greece		

Keywords: bgp-flowspec, security, DDOS, service, NETCONF

Security is a major concern of today's networks and in particular reactive protection against Denial of Service attacks. In this paper a new security provisioning service is presented based on bgp.flow-spec as described in RFC 5575 [1]. This service, named "FireCircle" is designed and implemented in-house by GRNET Network Operations Center, using open-source tools and platforms. GRNET (Greek Research and Technology Network) provides Internet connectivity and services to all Greek Universities and academic and research institutes.

Attackers typically use compromised systems, "zombies", that are relatively easy to control. In large numbers, zombies, pose a serious threat to modern networks. Take for example an army of zombies that numbers 500 bots originating from different domains. They can easily produce 100 MB of attack traffic through a 2Mbps ADSL line. This number has quite often increased to magnitudes that significantly affect the performance of the network. To date, attack mitigation is carried out mainly by two security approaches. The first approach is to deploy old style access lists either close to the server, resulting in valuable resources already wasted, or to the ingress point of the target domain. In the latter case uplink bandwidth is also wasted while the administrative overhead and large response times together with the coarse nature of access lists renders the mitigation actions ineffective. An improvement is based on a technique known as Remote Triggered Black-Hole (RTBH). Using BGP as a security tool, the receiving router translates a BGP community into a discard Next-Hop. The coarse actions that are implemented by RTBH, render the victim unreachable to the entire Internet, thus terminating in itself the DDOS attack. The positive side of RTBH is that the network administrators have successfully mitigated the flood of inter-domain traffic but even in this case the uplink remains flooded with attack traffic. An enhancement to existing approaches would be the deployment of a security tool that would allow firewalling rules to be propagated to different domains independent of unicast routing, while allowing for n-tuple of matching and filtering actions..

GRNET's operations team, driven by the need to provide advanced security services has designed and implemented its own in-house security provisioning platform, FireCircle, using readily available Open-Source software. GRNET's operations team approach towards security provisioning is the usage of flow specification NLRIs to successfully convey filtering information amongst neighboring domains. The most profound interdomain application of this approach is the deployment of the security service to domains interconnected through GEANT, for traffic flows that the victim AS wishes to drop. In this case, a downstream NREN can advertise an n-tuple filter encoded in the flow specification NLRI that contains the destination addresses from the address-space that it owns.

FireCircle aims to narrowing the gap between network management and security services. GRNET's customers and neighboring domains joining the "circle" can potentially incorporate firewall-on-demand. As the "circle" grows DDOS attacks can be terminated or blocked really close to their source in a timely manner, thus preserving network performance and security. For example, imagine the mechanism being activated in GRNET's upstream, GEANT. A hypothetical DDOS attack sourced behind an NREN-X, towards GRNET, could be blocked upon entrance on the GEANT network, i.e on GEANT's port where NREN-X is connected. Taking the example one step further, in the case that NREN-X exchanges family flow NLRIs with GEANT, the attack will be blocked right at the source with minimum administrative effort.

FireCircle deployment is based on BGP family flow supporting hardware (RFC 5575). GRNET's NOC has deployed a hardware box (Juniper EX4200) that is layer 3 capable and supports BGP and address family flow. This box is located in one of GRNET's data centers and conveys flow information through external BGP sessions with GRNET border routers. A first (coarse) level of trust is applied on the BGP sessions and is based on the well established trust of unicast routing. To allow for automation we have mitigated a more strict authorization model to the web front-end as described in the following section. Therefore a filter is applied on the routers that allow all GRNET customers rules to be accepted on the flow routing table.

The web platform on which FireCircle operates is developed in Python Django framework. The platform allows for creation, modification and deletion of flow rules via a wizard-like GUI. Authentication is performed via Shibboleth using an appropriate Entitlement attribute, carried only by NOC personnel. This gives the service a federated nature and eliminates any concern that the mechanism is a DDOS by itself. Authorization is based on address space assignments to GRNET's customers. A number of GRNET's clients are assigned a private AS number not allowing in this case the use of RIPE public whois. To address this issue GRNET has implemented a local private whois server where all the records are kept. Each client Institution/University has each own address space allocated by RIPE and also registered by GRNET Hostmaster in appropriate route-object located on the local whois server.

Thus, address space retrieval is accomplished by a python whois client towards the local whois server. The script eventually associates IP space with the customers' AS,

and the customer itself. Each downstream AS is allowed to impose a flow filter as long as the destination address belongs to the address space allocated to that AS.

While existing bgp flow-spec approaches make usage of bgp daemons [2,3], GRNET's implementation is solely based on NETCONF. NETCONF was chosen for being a secure management protocol with clean XML structure and a well defined request/response schema. Furthermore, the hardware that the rules are applied supports NETCONF. On the backend of the tool, a python NETCONF proxy middleware translates user requests to BGP flow rules and vice-versa. The NETCONF middleware applies the produced configuration to the hardware box via a python SSH-NETCONF client. Configuration retrieval is also supported to allow for syncing and reconciliation. Device configuration is mapped to Python classes that can be easily distributed and reused among a variety of applications. Once a request for a new flow rule is placed, configuration is applied to the aforementioned hardware box and is then propagated via BGP to GRNET's routers. What really boosts the deployment of FireCircle is the use of open source tools that map network configuration to service elements. This allows for interdomain deployment as tools can be easily adapted to each domain needs and requirements.

An important aspect of the tool and the service is its application on GRNET's production network. Currently (Nov. 2011), FireCircle is deployed in alpha release and will be soon available as a beta release to GRNET customers. GRNET NOC has already tested the service by simulating and mitigating a number of simulated attacks. Performance tests have shown an average of 30 seconds between flow rule request via the GUI and actual application to the network.

Future plans include a REST API for requesting flow rules via other applications such as security mail parsers (xarf) or threat notifiers and a mobile GUI to ease security management while on the run.

Authors' short bio

Leonidas Poulopoulos received his Diploma in Electrical and Computer Engineering from the University of Patras in 2005 and his M.Sc degree on Computer Science from the Department of Computer Engineering and Informatics (University of Patras) in 2010. Currently, he is with the development team of GRNET NOC.

Michalis Mamalis received his Diploma in Electrical and Computer Engineering from the Democritus University of Thrace in 2002. His diploma thesis focused on the design and implementation of an MMIC board acting as the optical receiver part of an STM-4 optical link. His areas of interest include MPLS, routing protocols, IPv6 and policy based networking. Currently he is with the routers administration team of GRNET NOC.

Andreas Polyrakis, received his Dipl.-Ing. Degree from the Department of Electrical and Computer Engineering, National Technical University of Athens (NTUA), Greece in 1999 and his M.Sc. degree on Computer Science from the University of Toronto,

Canada in 2001. His areas of interest include MPLS, IPv6, routing protocols, QoS in IP environments and policy-based networking. Currently, he is the technical coordinator of GRNET NOC.

References:

1. RFC 5575, *Dissemination of Flow Specification Rules.*
2. ExaBGP route injector, http://code.google.com/p/exabgp/
3. NANOG38, Deployment Experience With BGP Flow Specification, http://www.nanog.org/meetings/nanog38/abstracts.php?pt=MzEzJm5hbm9nMzg=&nm=nanog38