

An Abnormal Traffic Cleaning System

Yang Li^{1,a,*}, Yanlian Zhang^{2,b}

¹DIGITAL CHINA(CHINA)LIMITED, Beijing, China

²China Flight test establishment , Xi'an 710089,China,

^{a,*} digital9898@sina.com

Keywords: Abnormal Traffic, Cleaning, Detection, Traffic Re-injection

Abstract. Abnormal traffic cleaning system is proposed, which includes a cleaning platform, a detection platform and a management platform. The cleaning platform is mainly deployed through the bypass to guide the flow of the attacked object to the cleaning equipment. According to the protection strategy, the attack traffic is cleaned and normal traffic, the detection platform complete the detection of traffic for the attack, the management platform to provide cleaning equipment, testing equipment, state monitoring. The system can effectively clean the abnormal traffic and improve the security of the network.

1. Introduction

With the development of network technology and network economy, the importance of network to enterprises and individuals is increasing. At the same time, the network security vulnerabilities are also being increased, the importance of network security issues is also growing. In the metropolitan area network side for enterprise customers to carry out traffic cleaning services to achieve the defences of DDoS attacks, can meet the dual needs of customers. The traffic cleaning service is a kind of network security service for the government and enterprise customers who rent the IDC service and monitor, alarm and protect against the DOS /DDOS attack.

2. Architecture of Traffic Cleaning System

Abnormal traffic cleaning system includes cleaning platform, detecting platform and management platform. These parts of the function may be implemented by a device, or each part of the function realize by a single device.

The cleaning platform is mainly deployed through the bypass. It uses the routing protocol to route the attacked objects from the routing device to the cleaning device. According to the protection strategy, the abnormal traffic can be distinguished from the normal traffic to realize the cleaning of the attack traffic and the return of the normal traffic. And feedback the cleaning results to the management platform for unified management and presentation.

The detection platform can use splitting, mirroring, or traffic information collection, and can detect the attack traffic based on the traffic baseline policy. After the test platform runs for a period of time in the network, it can form a set of traffic distribution similar to the actual network according to the traffic situation in the actual network. The automatic learning generation or manual configuration forms the traffic baseline. When an attack is detected, an alarm is generated to the management platform.

Management platform provide cleaning equipment, testing equipment, state monitoring, and unified policy management, user management, device management and other functions, to provide users with cleaning statements query portal, can send and receive instructions to achieve linkage with other platforms.

Traffic cleaning system can interact with external detection alarm system, unified scheduling platform; form a multi-level traffic cleaning system.

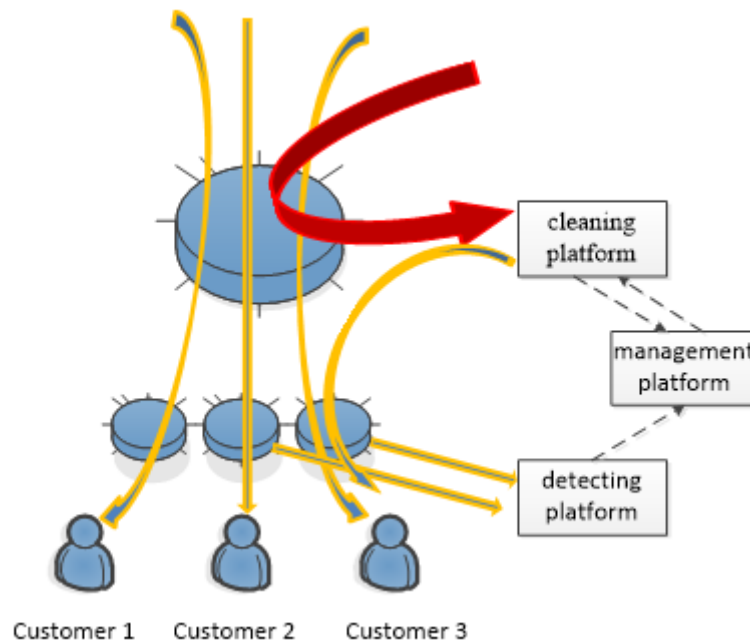


Figure 1 architecture of traffic cleaning system

3. Traffic Cleaning Function

3.1 Traffic Cleaning

Support clean typical traffic-based attacks, the cleaning of the attack types should include: Syn flood, ICMP flood, UDP flood, Ack flood, TCP connections flooded, DNS flood, HTTP post flood, Https flood. Support clean typical reflection attacks, including at least DNS reply flood, NTP flood and so on.

Support cleaning of application-level non-traffic-based attacks, at least should include HTTP slow request attacks, CC attacks. Supports common DOS attack packet cleaning, include Smurf, Land, deformity package, and TearDrop.

3.2 Cleaning limit

According to the user policy, it is defined that when the total traffic rate of the protection object exceeds a certain threshold value, random discarding is carried out, and the flow rate after cleaning is limited below the threshold value.

3.3 Black hole cleaning

It is recommended to use the route traction command to implement the black hole policy when the total traffic rate exceeds a certain threshold. This tells the neighbour router to directly flood all the traffic. Black hole routing instructions should support the use of BGP protocol.

3.4 Cleaning feature

According to the characteristics of the attack (such as IP header, TCP header, TCP payload, UDP header and UDP payload, source port, destination port, etc.) to define the precise filtering policy, support the analysis of typical protocol fields, and apply the attack feature to the protection object .

3.5 Protection strategy

Protection policy for the protection object should be configured. The protection objects should be distinguished by IP addresses. A default protection object policy should be supported to support the creation of a unified protection policy (the default protection policy) for protected objects that do not have explicit IP protection.

The protection strategy should include the following:

- Support the defence flow threshold and rate of a specific protocol
- Support the use of specific cleaning algorithm (including whether the source calibration, etc.)
- Support the cleaning strategy when exceeding the protection threshold (traffic rate limit, sub-protocol speed limit, black hole routing, etc.)

- Configure the cleaning features of specific attack packets
- Supports IP address blacklist function based on attack source geographic information (optional), and blacklist IP address traffic directly intercepts.

3.6 Traffic traction

The traffic cleaning device has a neighbour relationship with the router, and dynamically sends a route advertisement to the upstream (neighbour) router to dynamically draw the traffic of the protected object to the cleaning device. The traffic clean-up platform support dynamic routing traction using the BGP-4 protocol. Traffic cleaning and draining can support OSPF, IS-IS, MPLS LSP, MPLS VPN and other forms of traffic traction requirements.

Traffic tracing supports specifying a traffic traction policy for each protection object. It supports setting the mask length for different bits in traffic advertisement for protection objects. The BGP peering policy support the configuration of BGP community, AS path, and other basic attributes. And can configure route-map, prefix-list, and other route filtering modes.

The cleaning platform support BGP route advertisements with different attribute parameters for different neighbouring routers. The router can advertise only a route advertisement to a specific neighbour router (not all neighbour routers) to cooperate with the router in the network.

3.7 Traffic injected

The traffic injected through policy routing, MPLS VPN, MPLS LSP, GRE, and Layer 2 injection will be injected into the network.

3.8 Traffic balance

Diversion and re-injection of two-way links should be supported through link aggregation, equivalent routing and other forms of drainage, re-injection flow load sharing.

3.9 Cleaning source authentication

The source IP address of the specified attack type should be authenticated according to the user protection policy. The IP address of the source IP address to be authenticated should be used as the source authentication whitelist. No longer need to perform source authentication. The whitelist should have a certain aging time.

The number of IP addresses of the whitelist entries must be selected according to the deployment requirements. The total number of whitelist entries should be at least 100,000.

4. Detection function

The detection device support traffic detection by means of one or more means based on traffic information or per packet detection.

- Data flow based detection: Supports the analysis of the data flow in the traffic, the acquisition format should support a variety of protocol formats, including Netflow V5/V9, Netstream and other protocols, while supporting IPv4 and IPv6 traffic detection.
- DPI based traffic detection: Supports packet-by-packet traffic analysis to detect abnormal traffic events in the network. Supports detection of traffic packets based on detection thresholds, detection features, and so on.
- Dynamic baseline learning: The detection equipment supports the dynamic baseline learning task. It should support dynamic baseline learning at a specified time, support dynamic baseline automatic generation, and support manual adjustment and confirmation of thresholds for dynamic learning.
- Attack event Alarm :Alarm event list Including the alarm ID, alarm type, alarm cause, severity, IP address and port to be attacked, the source IP address of the attack, and the source IP address of the attack source, Start time and so on.

5. Management function

Login Management: B/S mode should support the user login management, multi-user landing at the same time, to support more than one login account or only single sign-on. Support mandatory to

enable https, support the management of IP address restrictions, the command line should support SSH. RADIUS-based authentication should be supported.

User management: It should support a unified operation and maintenance management portal and user service portal capabilities, the system should support the creation of sub-domain for the user to achieve management of the sub-domain management.

Protection object management: The protection object is configured by IP address. It should be configured through IP address. It can be configured by IP address segment plus mask. Supports the object protection strategy of the bulk application, protection object (group) number of not less than 1000.

Device management: support the management of the device group, and to add, delete and modify the devices in the group. The defence group can be built and the protection strategy of the protection object can be unified. The import and export of device configuration information should be supported.

6. Performance requirements

Single Device Throughput: The throughput of a device should meet the throughput requirements according to the actual requirements in different deployment environments. Packet flooding, DNS flood, ICMP flood, UDP flood, mixed flood, HTTP Get Flood, and so on.

Equipment cleaning accuracy: cleaning specifications 90% load, normal traffic and mixed attack traffic according to 1: 9 ratio, the normal business packet loss rate should not be higher than one thousandth, attack traffic leakage blocking rate should not be high One percent.

Cleaning delay requirements: cleaning specifications 90% load conditions, the forwarding delay of not more than 80us.

Reliability Requirement: The overall reliability of the system should reach 99.999% (software and hardware), that is, the system may not interrupt more than 5.26 minutes during the continuous operation for 1 year.

7. External interface

Cleaning system external interface support the establishment of a trusted channel interface to meet the security requirements of transmission, support for domestic encryption algorithm.

Interface between the cleaning system and the third-party detection equipment: The attacking alarm reported by the third-party detection platform Syslog should be supported. The protocol and format of the Syslog interface meet the requirements of RFC3164.

Management system interface with the external dispatch platform include: data reporting interface: to support the cleaning task start / end of the report, reporting the status of cleaning tasks changes. support the cleaning log, traffic log regularly reported, reported cleaning data, traffic data to the scheduling platform. Can support the cleaning capacity is insufficient cleaning business alarm report. Command issuance interface: It can support the protection strategy and drainage policy of cleaning protection object issued by external management platform. Can support the external platform issued the task of cleaning tasks, scheduling cleaning equipment for cleaning, stop cleaning and other operations.

8. Conclusions

An abnormal traffic cleaning system is proposed in this paper, the architecture of the system is provided, which includes a cleaning platform, a detection platform and a management platform. And this system can improve the security of traffic.

References

- [1] Francesco Gargiulo; Carlo Sansone, (2010) Improving Performance of Network Traffic

Classification Systems by Cleaning Training Data, 2010 20th International Conference on Pattern Recognition, 2768 - 2771

[2] Byoung-Koo Kim; Dong-Ho Kang, (2016) Abnormal traffic filtering mechanism for protecting ICS networks 2016 18th International Conference on Advanced Communication Technology, 436 – 440

[3] Sergey Ageev; Yan Kopchak, (2015) Abnormal traffic detection in networks of the Internet of things based on fuzzy logical inference, 2015 XVIII International Conference on Soft Computing and Measurements (SCM), 5 - 8

[4] Tianshu Wu; Kunqing Xie, (2012) A online boosting approach for traffic flow forecasting under abnormal conditions 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, 2555 – 2559

[5] Ayman Mohammad Bahaa-Eldin, (2011) Time series analysis based models for network abnormal traffic detection The 2011 International Conference on Computer Engineering & Systems, 64 - 70