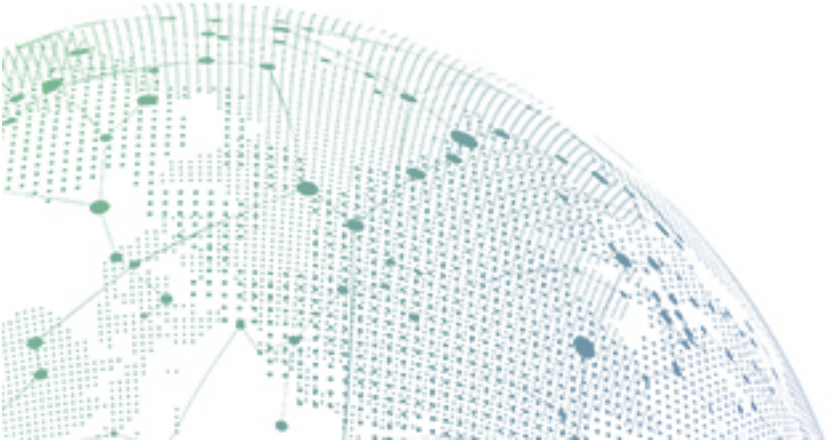
SANGFOR

NGAF

AntiDoS & DdoS Configuration

Version 8.0.5



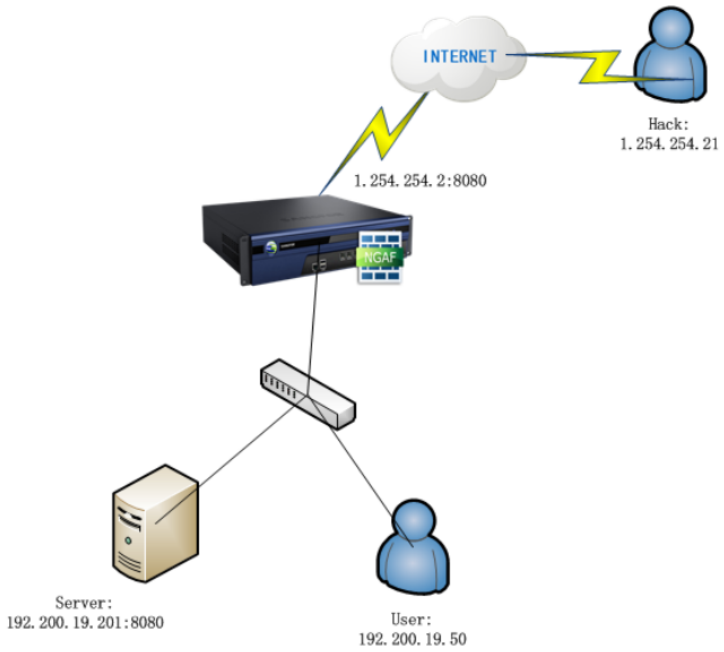
Change Log

Date	Change Description
Oct 26,2018	Version 8.0.5 document release.

CONTENT

Chapter 1 Scenario

Case Environment



NGAF Public IP 1.254.254.2 port 8080 DNAT to Server 192.200.19.201 port 8080

Hacker's PC MAC is 74:de:2b:e8:8c:29

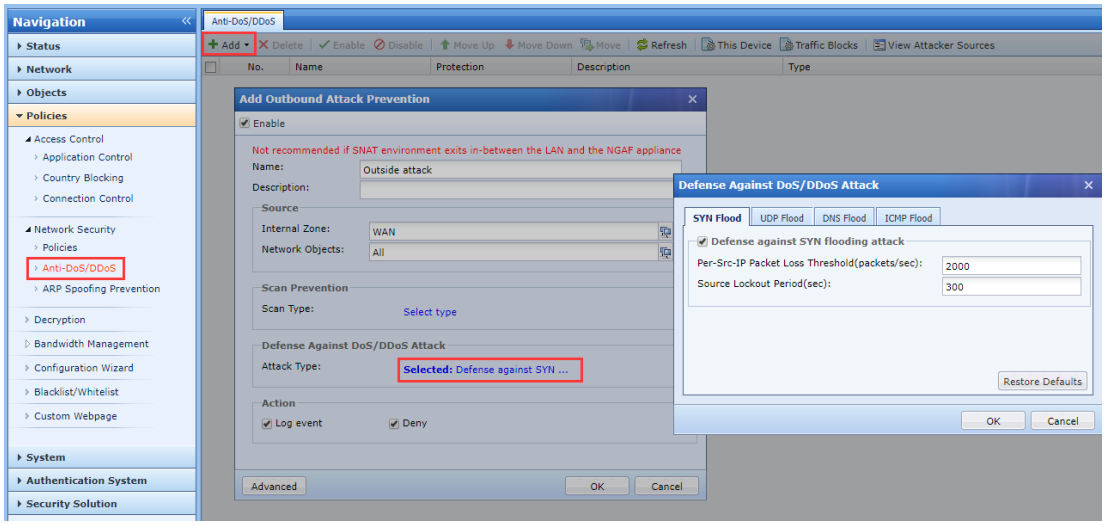
Chapter 2 Configuration

1. Types of Deniel of Attack

    1.1. Outbound attack

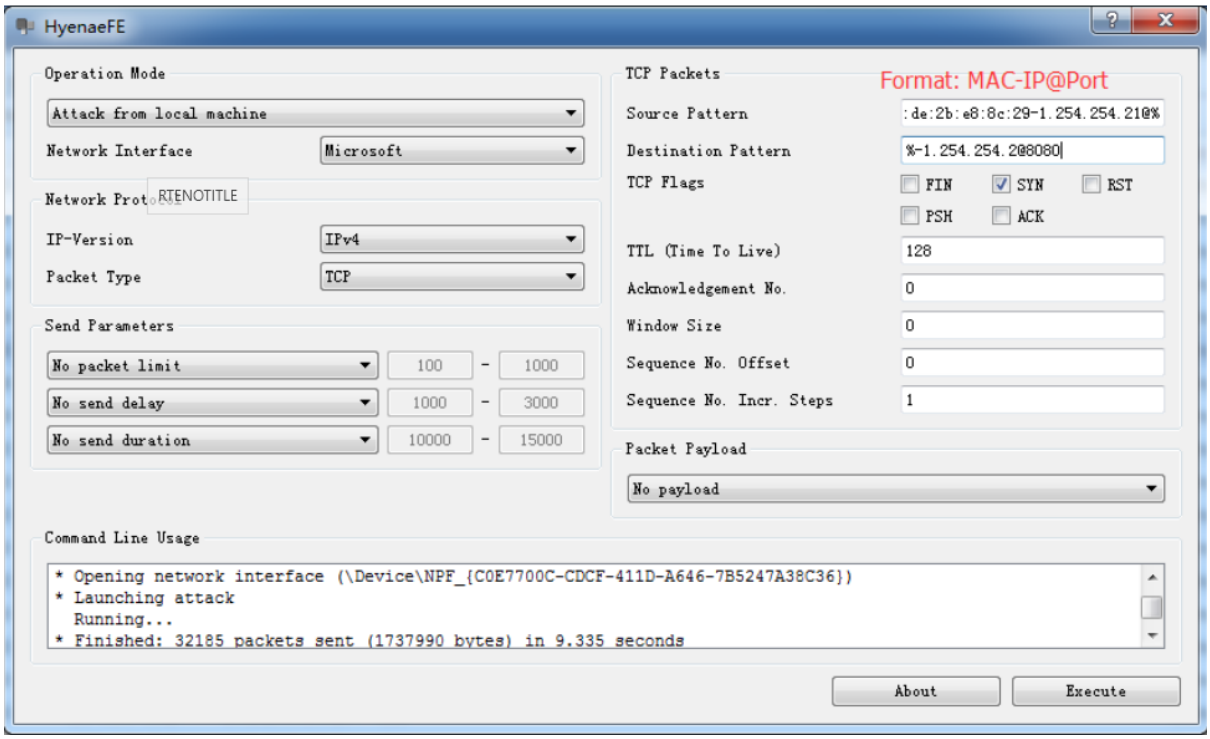
        Prevent attacker attack firewall internal network.

NGAF Anti-Dos/DDos outside attack policy

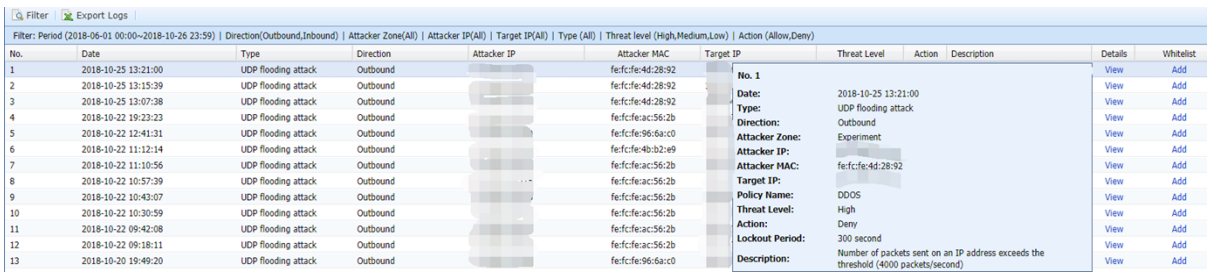


Note: Source zone of the outbound policy is: WAN (external zone)

Use DOS/DDos attack tool Hyenae send SYN flood to 1.254.254.2@80

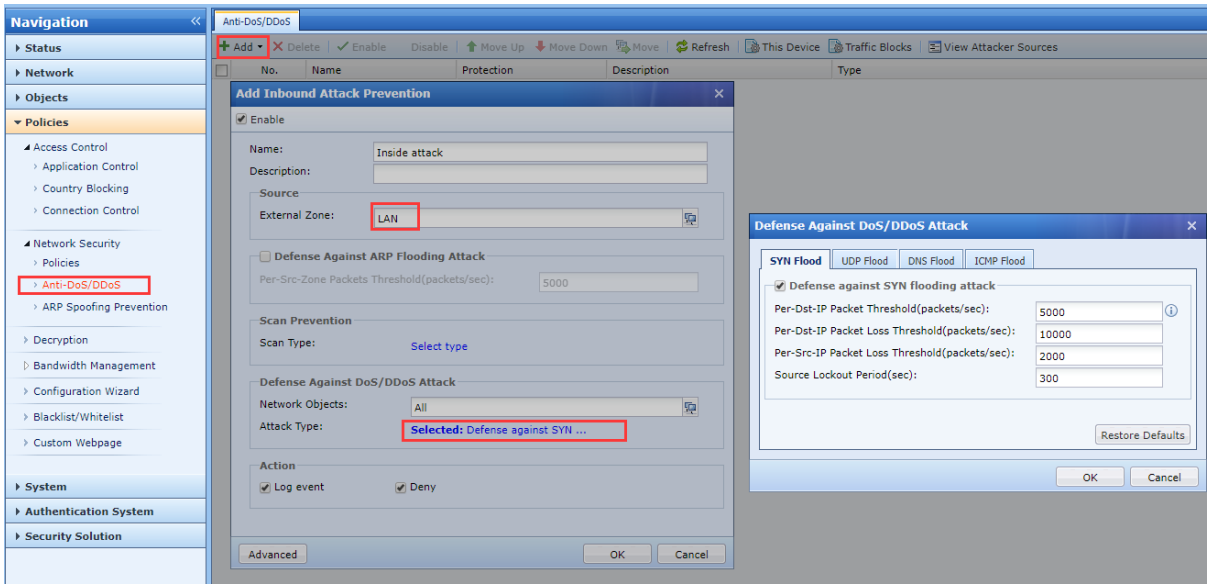


NGAF Record in logs



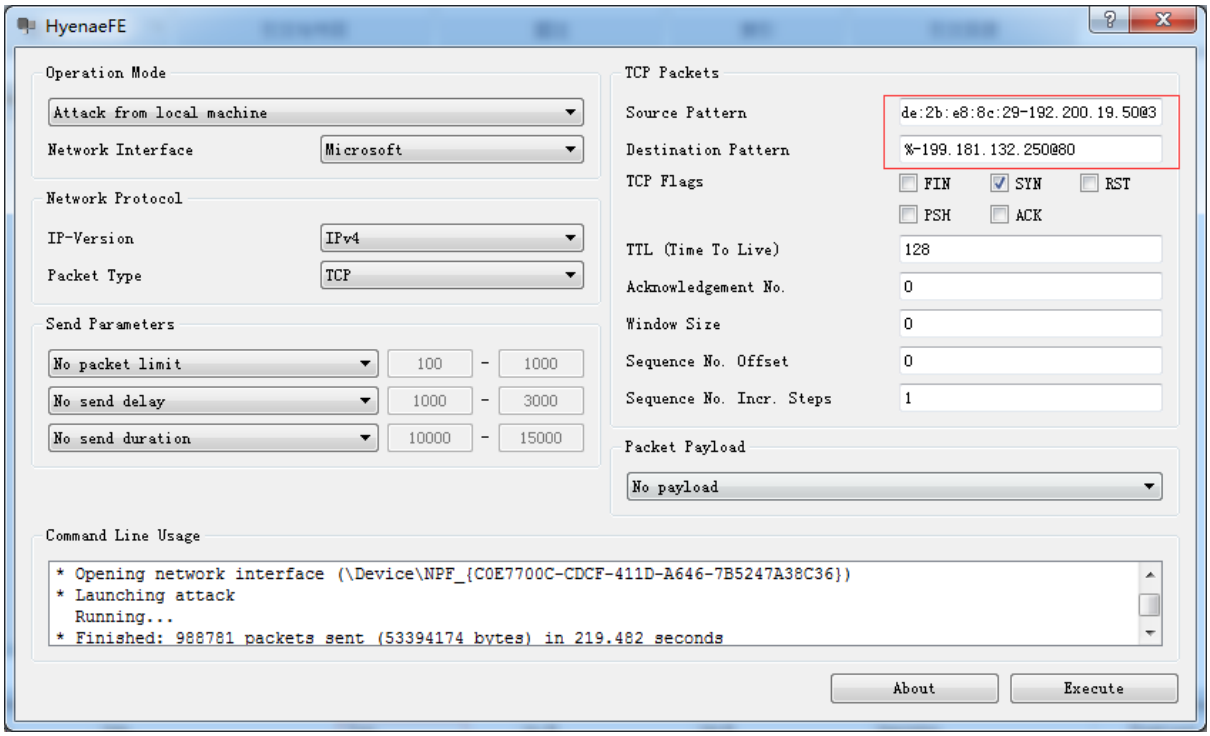
1.2. Inbound Attack

Prevent internal users attack outside network.

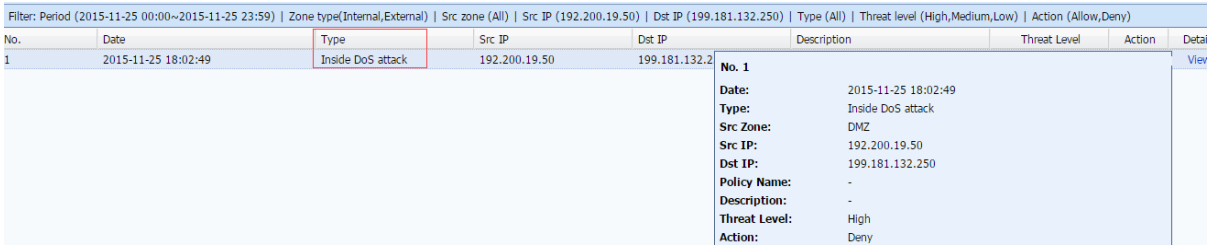


Note: Source zone of the inbound policy is LAN/DMZ

Use DOS/DDos attack tool Hyenae send SYN flood to 192.200.19.201@80



NGAF Record in logs

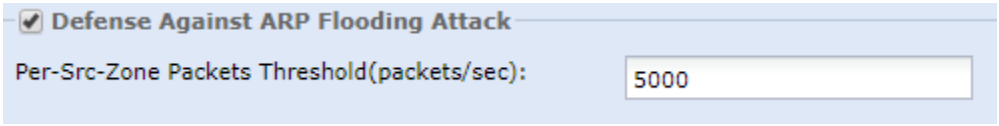

Filter: Period (2015-11-25 00:00~2015-11-25 23:59) | Zone type(Internal,External) | Src zone (All) | Src IP (192.200.19.50) | Dst IP (199.181.132.250) | Type (All) | Threat level (High,Medium,Low) | Action (Allow,Deny)
No.
Date
Type
Src IP
Dst IP
Description
Threat Level
Action
1
2015-11-25 18:02:49
Inside DoS attack
192.200.19.50
No. 1
Date: 2015-11-25 18:02:49
Type: Inside DoS attack
Src Zone: DMZ
Src IP: 192.200.19.50
Dst IP: 199.181.132.250
Policy Name: -
Description: -
Threat Level: High
Action: Deny

Chapter 3 Detail configuration

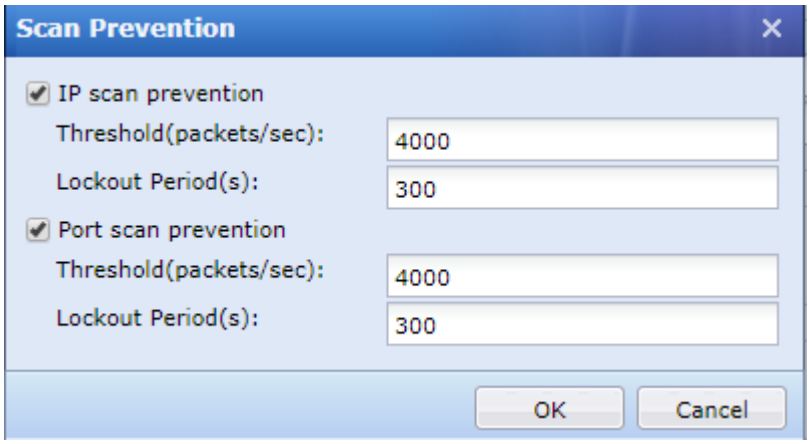
3.1 Outside attack policy

Policy zone chose WAN zone.

Defense against ARP flooding attack

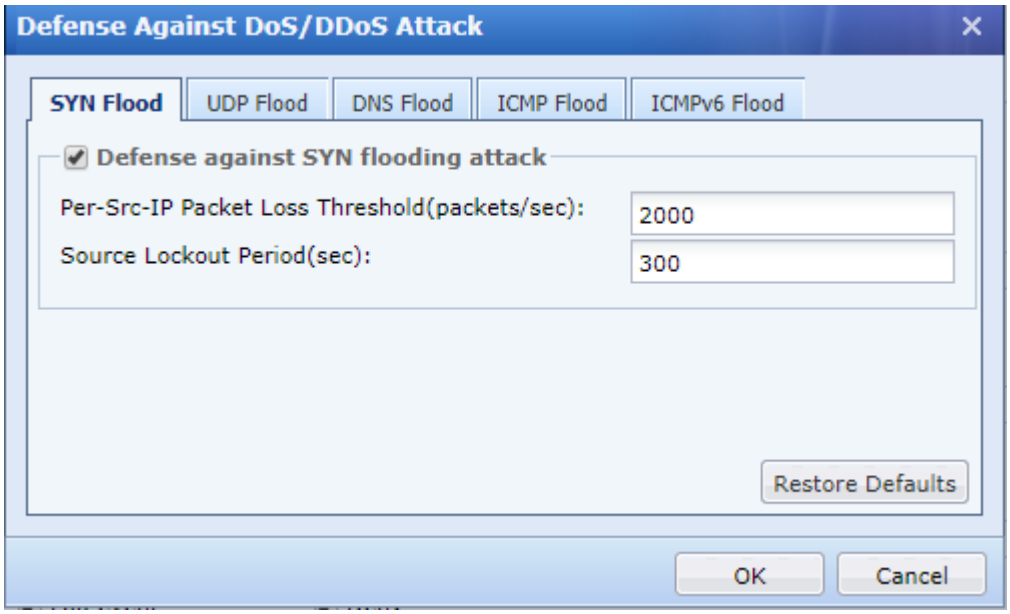


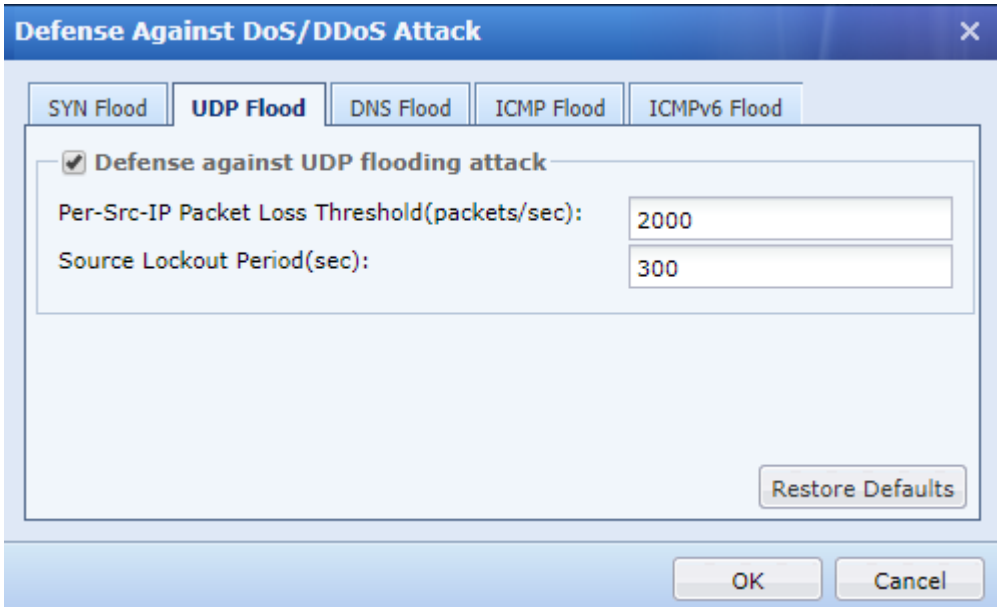
Scan Prevention

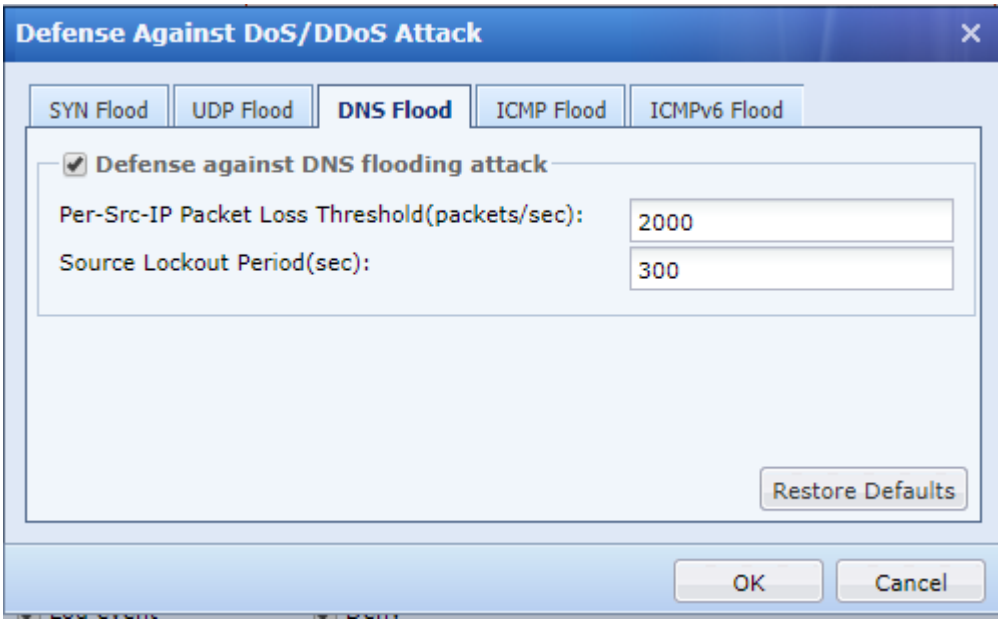


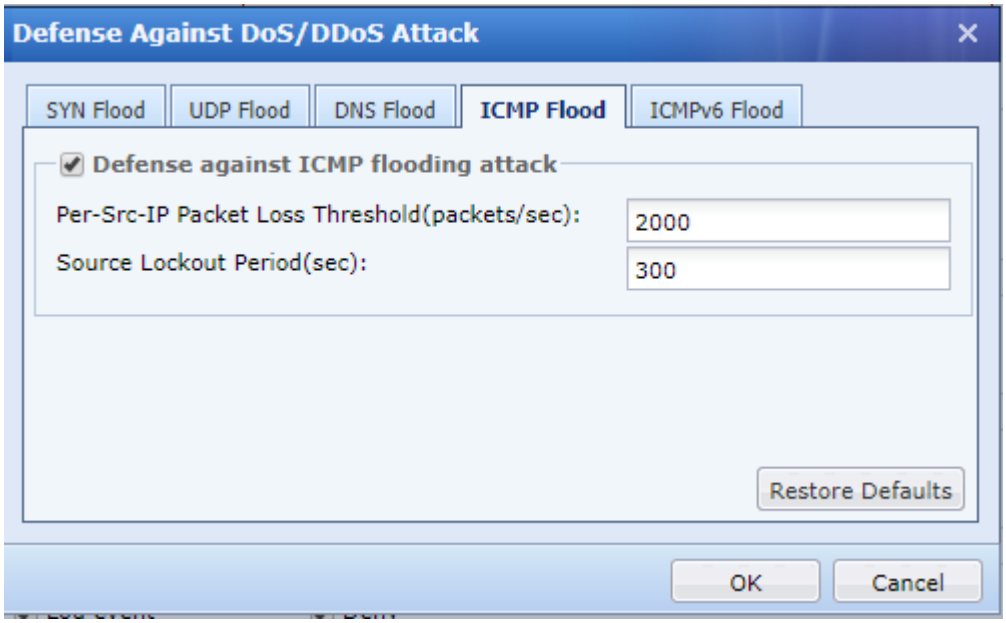
* Only support TCP port scan.

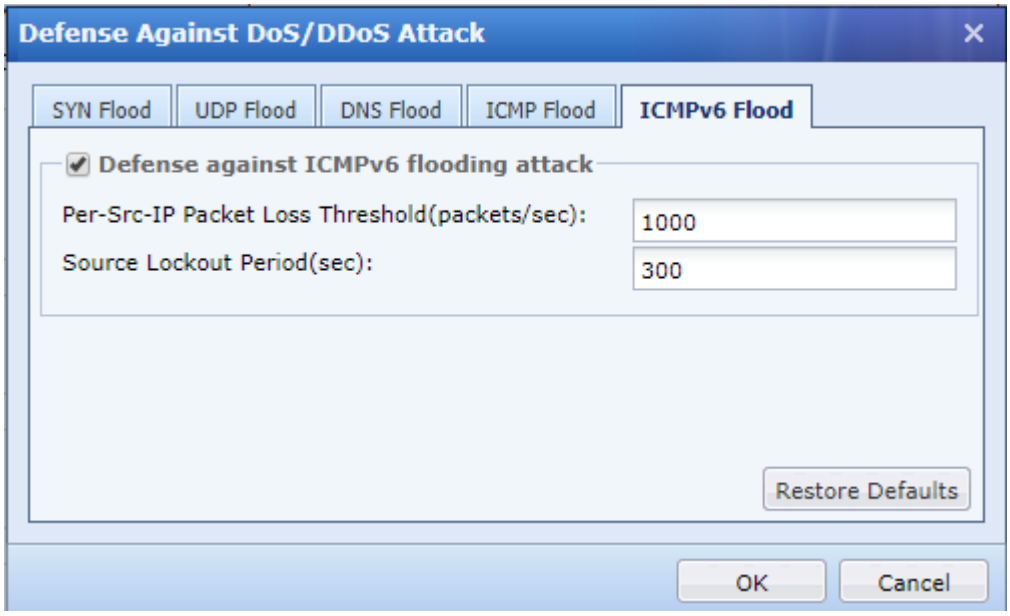
Defense against DoS/DDoS Attack



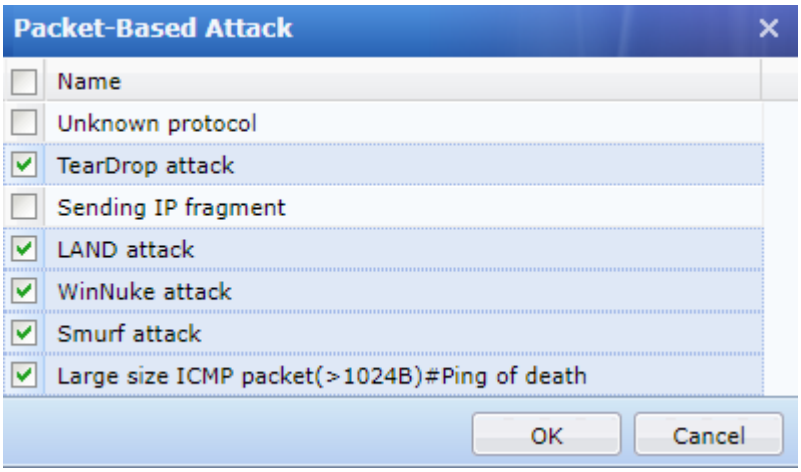

Defense Against DoS/DDoS Attack
SYN Flood
UDP Flood
DNS Flood
ICMP Flood
ICMPv6 Flood
Defense against UDP flooding attack
Per-Src-IP Packet Loss Threshold(packets/sec):
2000
Source Lockout Period(sec):
300
Restore Defaults
OK
Cancel


Defense Against DoS/DDoS Attack
SYN Flood
UDP Flood
DNS Flood
ICMP Flood
ICMPv6 Flood
Defense against DNS flooding attack
Per-Src-IP Packet Loss Threshold(packets/sec):
2000
Source Lockout Period(sec):
300
Restore Defaults
OK
Cancel



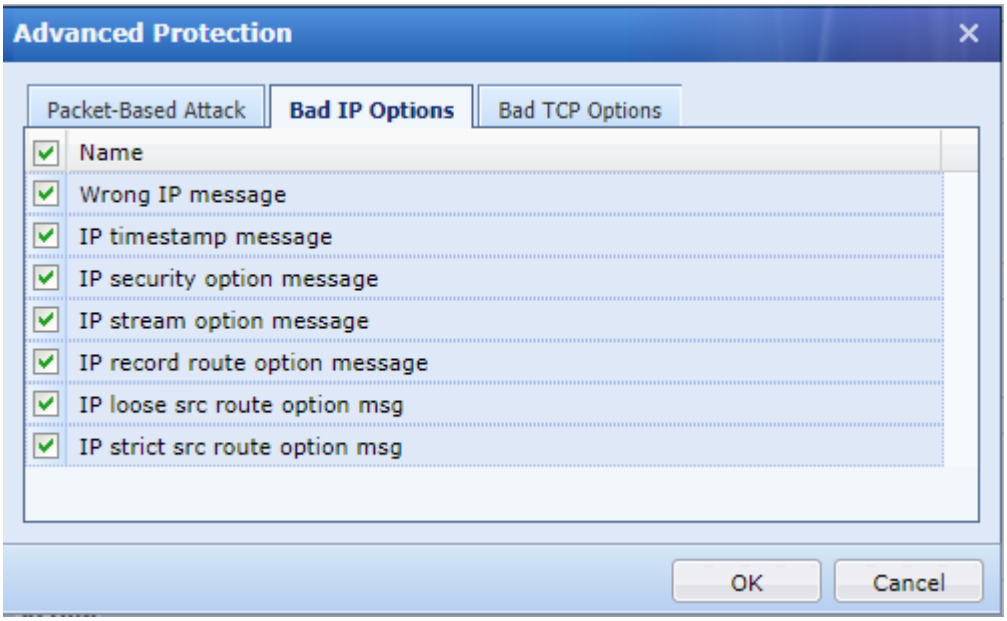


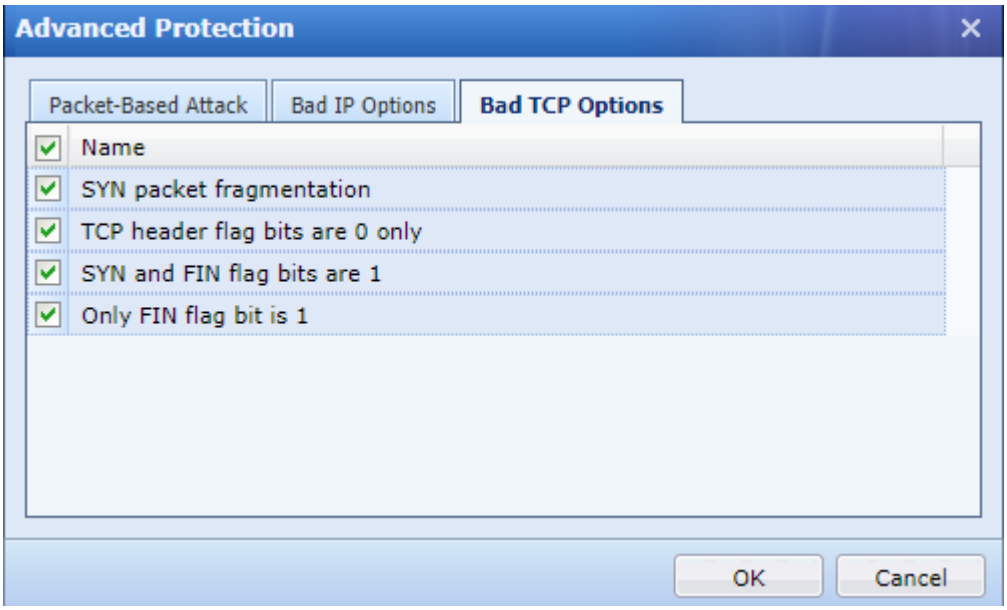
Packet-Based Attack



* Not suggest chose Sending IP fragment, IP fragment exist in normal network.

Abnormal Message Probe

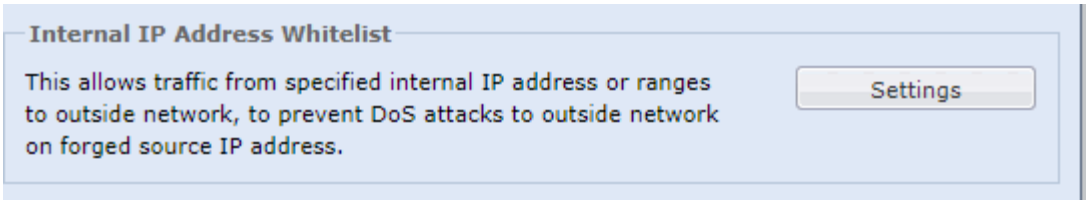


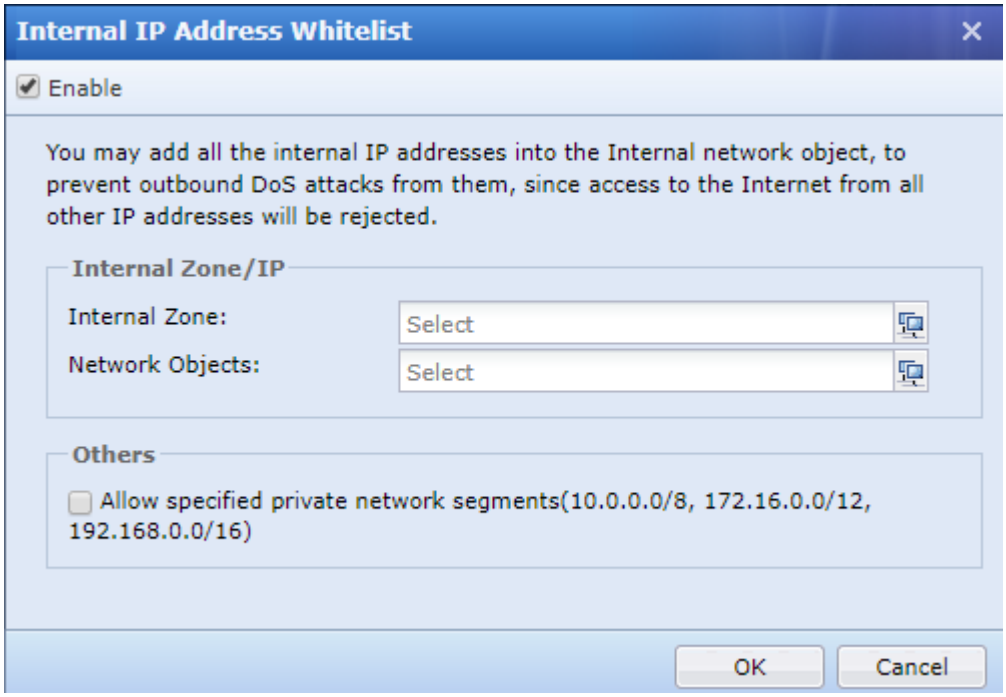


3.2 Inside attack policy

We need to know NGAF connect to intranet through L3 switch or router or L2, whether L3 or router enable SNAT. whether proxy server in intranet, we can exclusion proxy server IP.

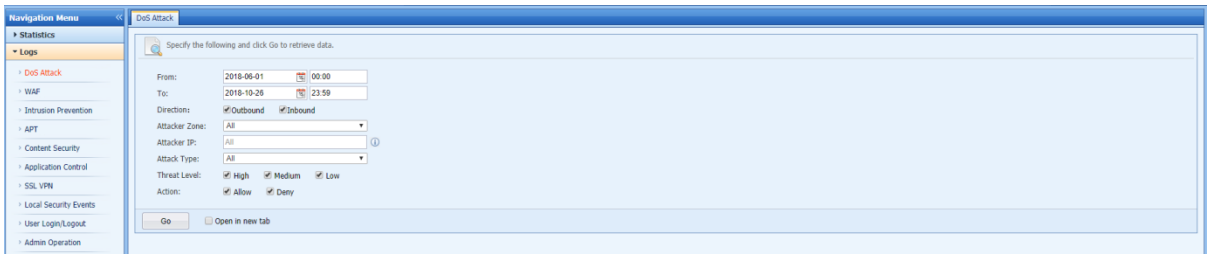
Internal IP Address Whitelist

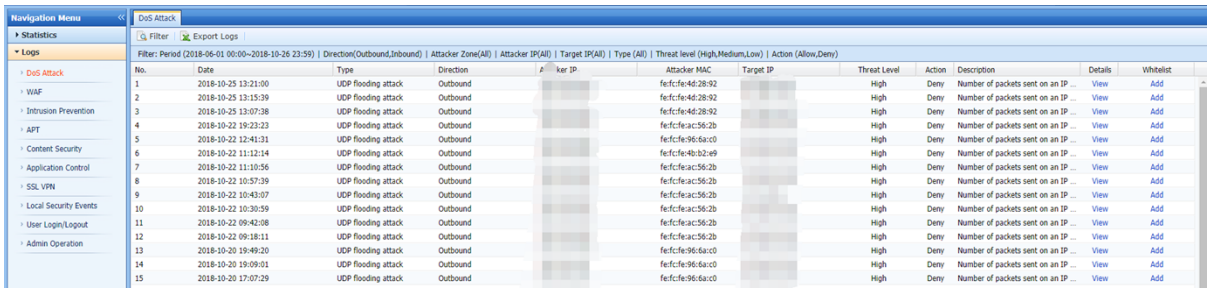




3.3 Anti-Dos/Ddos logs

Check in internal report center





SANGFOR