



# NGAF

## AntiDoS & DdoS Configuration

Version 8.0.5

---

## Change Log

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

---

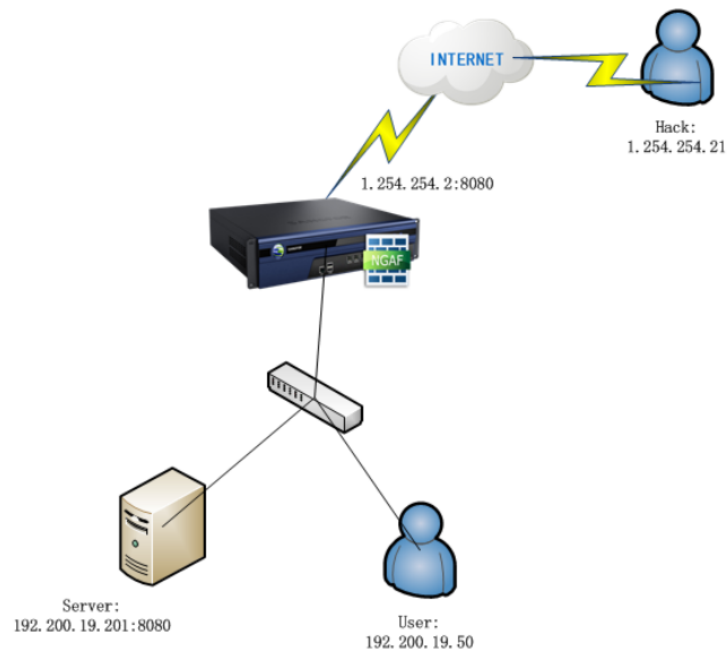
## CONTENT

<b>Chapter 1 Scenario .....</b>	<b>4</b>
<b>Chapter 2 Configuration .....</b>	<b>4</b>
<b>Chapter 3 Detail configuration.....</b>	<b>7</b>
3.1 Outside attack policy.....	7
3.2 Inside attack policy.....	11
3.3 Anti-Dos/Ddos logs.....	12

---

## 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

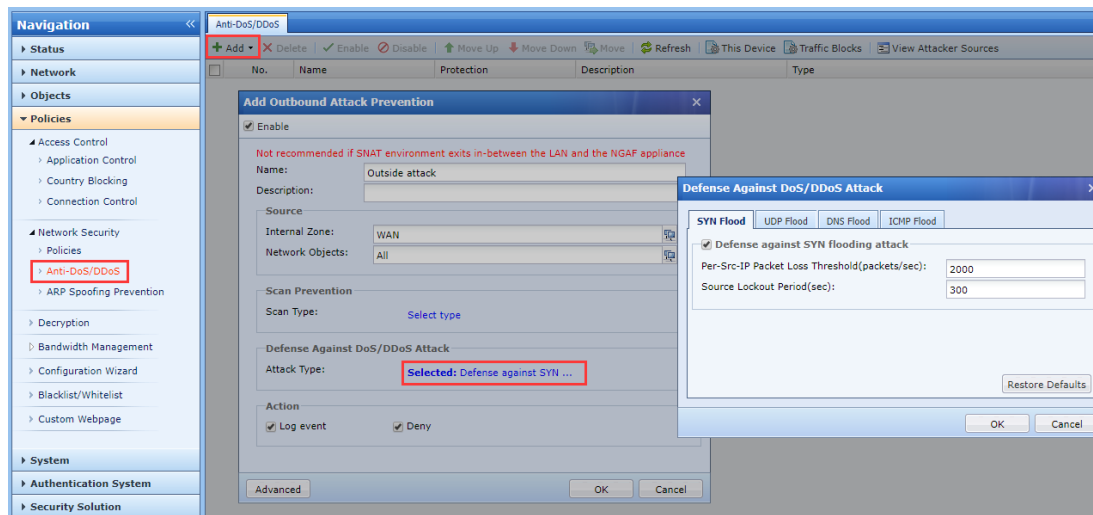
## Chapter 2 Configuration

### 1. Types of Deniel of Attack

#### 1.1. Outbound attack

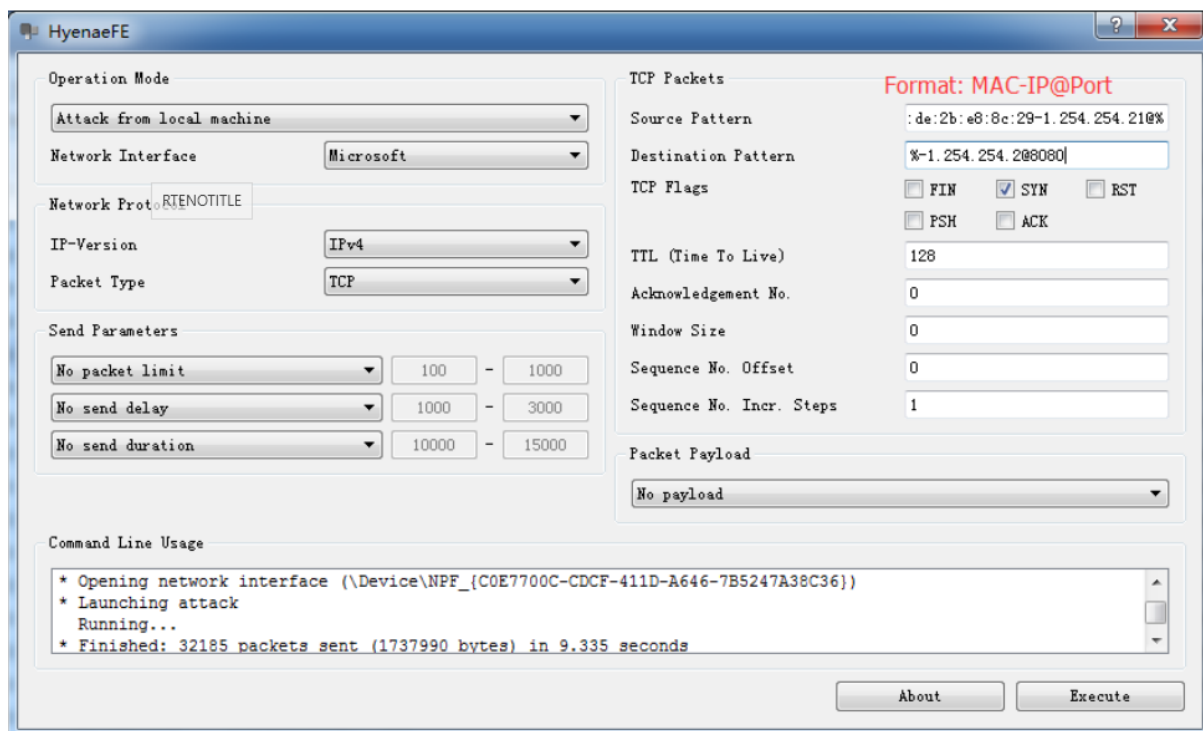
Prevent attacker attack firewall internal network.

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

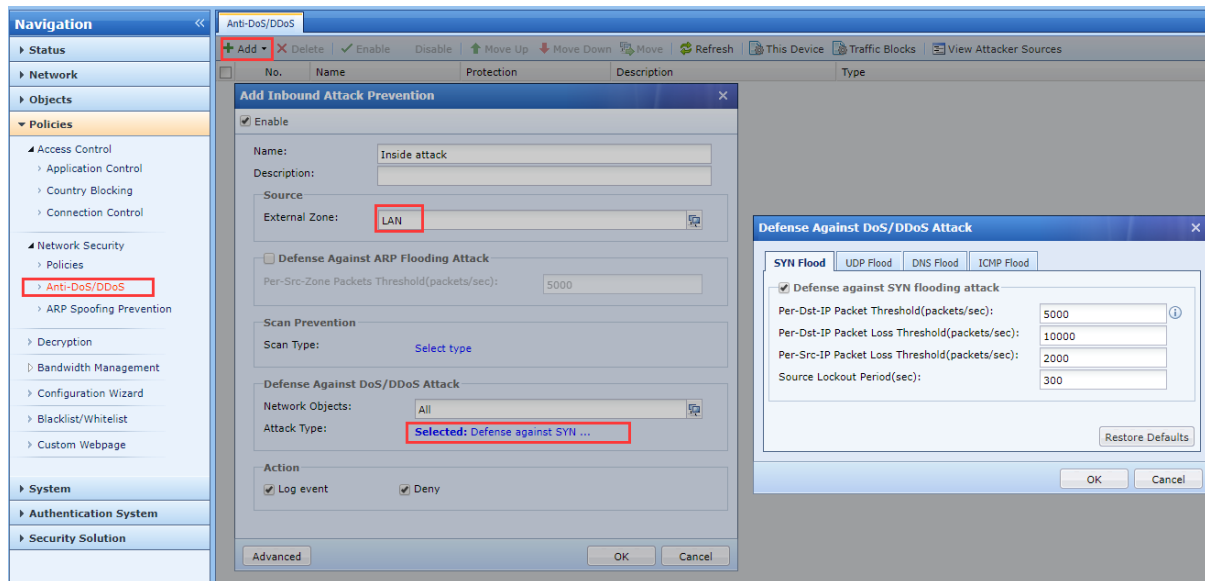


NGAF Record in logs

No.	Date	Type	Direction	Attacker IP	Attacker MAC	Target IP	Threat Level	Action	Description	Details	Whitelist
1	2018-10-25 13:21:00	UDP flooding attack	Outbound		fe1cfe4d:28:92	No. 1					
2	2018-10-25 13:15:39	UDP flooding attack	Outbound		fe1cfe4d:28:92						
3	2018-10-25 13:07:38	UDP flooding attack	Outbound		fe1cfe4d:28:92						
4	2018-10-22 19:23:23	UDP flooding attack	Outbound		fe1cfe4d:28:92						
5	2018-10-22 12:41:31	UDP flooding attack	Outbound		fe1cfe4d:28:92						
6	2018-10-22 11:12:14	UDP flooding attack	Outbound		fe1cfe4d:28:92						
7	2018-10-22 11:10:56	UDP flooding attack	Outbound		fe1cfe4d:28:92						
8	2018-10-22 10:57:39	UDP flooding attack	Outbound		fe1cfe4d:28:92						
9	2018-10-22 10:43:07	UDP flooding attack	Outbound		fe1cfe4d:28:92						
10	2018-10-22 10:30:59	UDP flooding attack	Outbound		fe1cfe4d:28:92						
11	2018-10-22 09:42:08	UDP flooding attack	Outbound		fe1cfe4d:28:92						
12	2018-10-22 09:18:11	UDP flooding attack	Outbound		fe1cfe4d:28:92						
13	2018-10-20 19:49:20	UDP flooding attack	Outbound		fe1cfe4d:28:92						

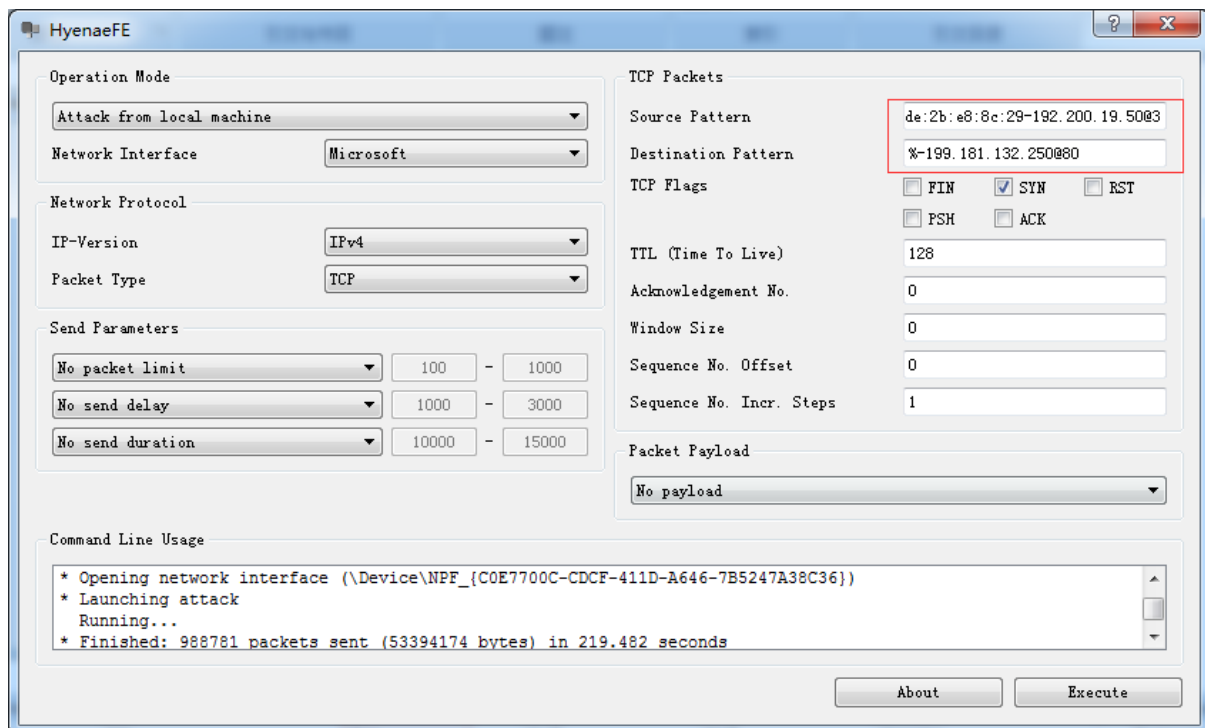
## 1.2. Inbound Attack

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	Detail
1	2015-11-25 18:02:49	Inside DoS attack	192.200.19.50	199.181.132.250	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			<a href="#">View</a>

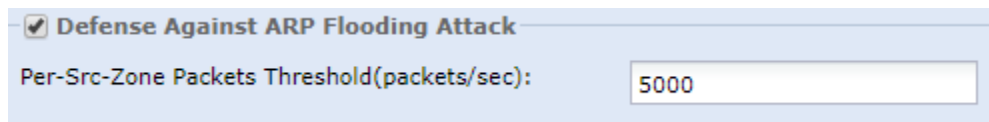
---

## Chapter 3 Detail configuration

### 3.1 Outside attack policy

Policy zone chose WAN zone.

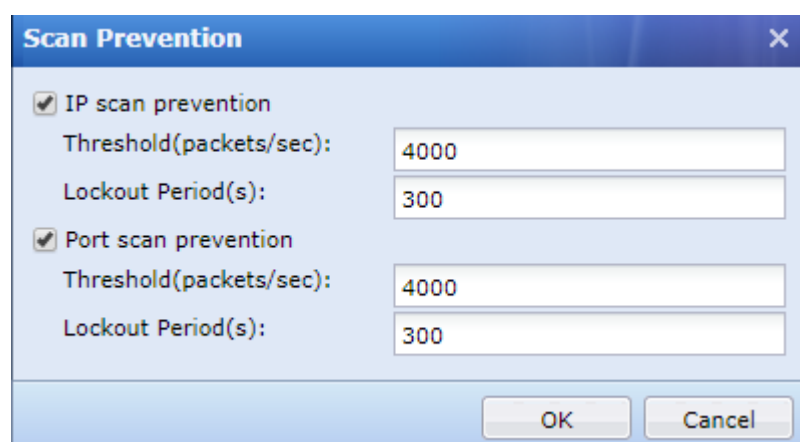
#### Defense against ARP flooding attack



☒ **Defense Against ARP Flooding Attack**

Per-Src-Zone Packets Threshold(packets/sec):

#### Scan Prevention



**Scan Prevention** [X]

☒ **IP scan prevention**

Threshold(packets/sec):

Lockout Period(s):

☒ **Port scan prevention**

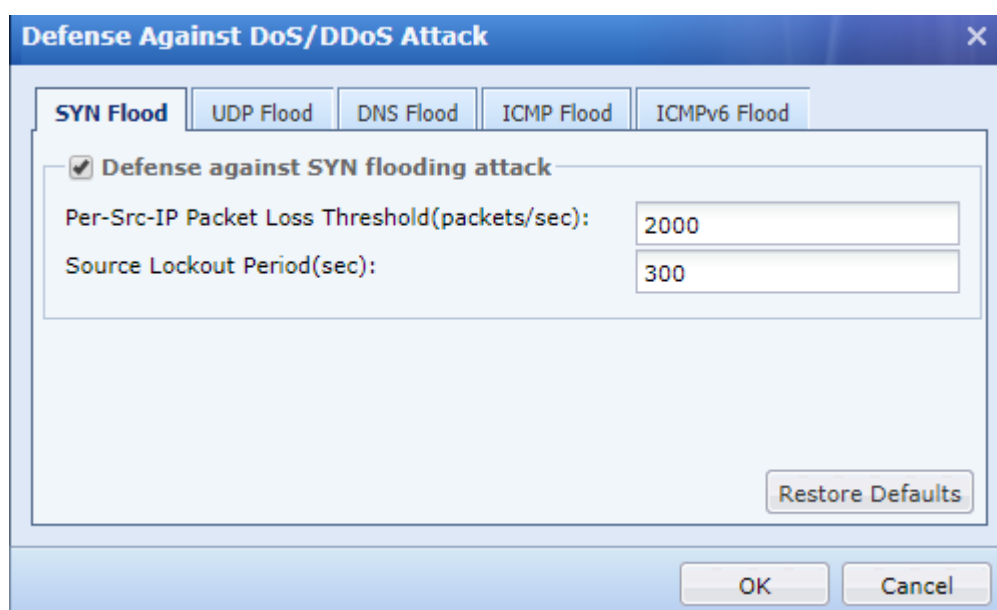
Threshold(packets/sec):

Lockout Period(s):

OK Cancel

\* Only support TCP port scan.

#### Defense against DoS/DDoS Attack



**Defense Against DoS/DDoS Attack** [X]

**SYN Flood** | UDP Flood | DNS Flood | ICMP Flood | ICMPv6 Flood

☒ **Defense against SYN flooding attack**

Per-Src-IP Packet Loss Threshold(packets/sec):

Source Lockout Period(sec):

Restore Defaults

OK Cancel



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

**Defense Against DoS/DDoS Attack** [X]

☒ **Defense against ICMP flooding attack**

Per-Src-IP Packet Loss Threshold(packets/sec):

Source Lockout Period(sec):

**Defense Against DoS/DDoS Attack** [X]

☒ **Defense against ICMPv6 flooding attack**

Per-Src-IP Packet Loss Threshold(packets/sec):

Source Lockout Period(sec):

## Packet-Based Attack

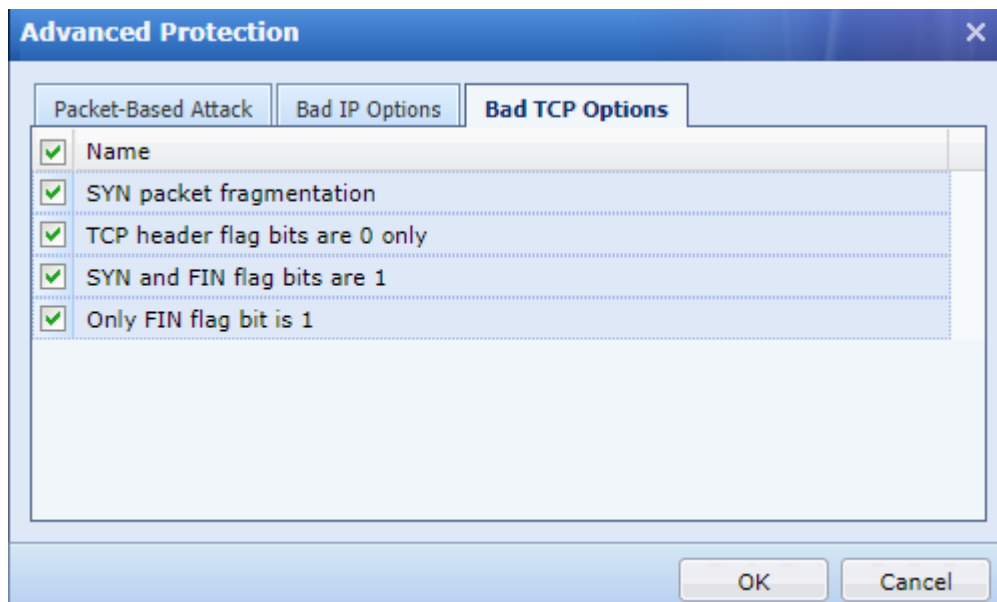
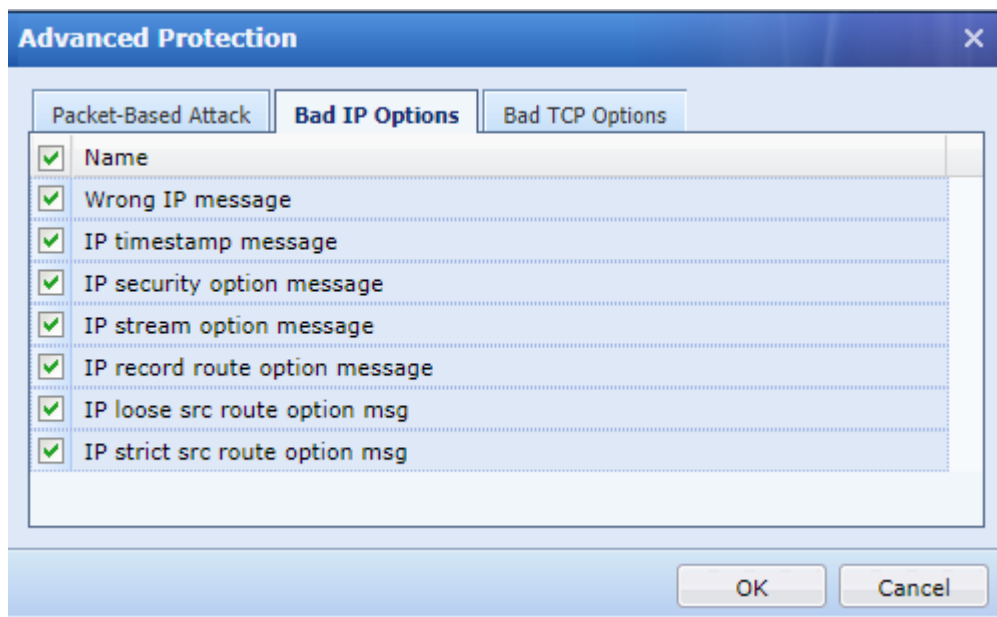
**Packet-Based Attack** [X]

<input type="checkbox"/>	Name
<input type="checkbox"/>	Unknown protocol
<input checked="" type="checkbox"/>	TearDrop attack
<input type="checkbox"/>	Sending IP fragment
<input checked="" type="checkbox"/>	LAND attack
<input checked="" type="checkbox"/>	WinNuke attack
<input checked="" type="checkbox"/>	Smurf attack
<input checked="" type="checkbox"/>	Large size ICMP packet(>1024B)#Ping of death

---

\* 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

Internal IP Address Whitelist

This allows traffic from specified internal IP address or ranges to outside network, to prevent DoS attacks to outside network on forged source IP address.

Settings

Internal IP Address Whitelist

☒ Enable

You may add all the internal IP addresses into the Internal network object, to prevent outbound DoS attacks from them, since access to the Internet from all other IP addresses will be rejected.

Internal Zone/IP

Internal Zone:

Select

Network Objects:

Select

Others

☐ Allow specified private network segments(10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)

OK

Cancel

### 3.3 Anti-Dos/Ddos logs

Check in internal report center

Navigation Menu

Statistics

Logs

DoS Attack

WAF

Intrusion Prevention

APT

Content Security

Application Control

SSL VPN

Local Security Events

User Login/Logout

Admin Operation

DoS Attack

Specify the following and click Go to retrieve data.

From: 2018-06-01 00:00

To: 2018-10-26 23:59

Direction: ☒ Outbound ☒ Inbound

Attacker Zone: All

Attacker IP: All

Attack Type: All

Threat Level: ☒ High ☒ Medium ☒ Low

Action: ☒ Allow ☒ Deny

Go

Open in new tab

Navigation Menu

Statistics

Logs

DoS Attack

WAF

Intrusion Prevention

APT

Content Security

Application Control

SSL VPN

Local Security Events

User Login/Logout

Admin Operation

DoS Attack

Filter: Period (2018-06-01 00:00~2018-10-26 23:59) | Direction(Outbound,Inbound) | Attacker Zone(All) | Attacker IP(All) | Target IP(All) | Type (All) | Threat level (High,Medium,Low) | Action (Allow,Deny)

No.	Date	Type	Direction	Attacker IP	Attacker MAC	Target IP	Threat Level	Action	Description	Details	Whitelist
1	2018-10-25 13:21:00	UDP flooding attack	Outbound		fecfca4b28-92		High	Deny	Number of packets sent on an IP ...	View	Add
2	2018-10-25 13:15:39	UDP flooding attack	Outbound		fecfca4b28-92		High	Deny	Number of packets sent on an IP ...	View	Add
3	2018-10-25 13:07:38	UDP flooding attack	Outbound		fecfca4b28-92		High	Deny	Number of packets sent on an IP ...	View	Add
4	2018-10-22 19:23:23	UDP flooding attack	Outbound		fecfca56-2b		High	Deny	Number of packets sent on an IP ...	View	Add
5	2018-10-22 12:41:31	UDP flooding attack	Outbound		fecfca56-2b		High	Deny	Number of packets sent on an IP ...	View	Add
6	2018-10-22 11:12:14	UDP flooding attack	Outbound		fecfca4b52-e9		High	Deny	Number of packets sent on an IP ...	View	Add
7	2018-10-22 11:10:56	UDP flooding attack	Outbound		fecfca56-2b		High	Deny	Number of packets sent on an IP ...	View	Add
8	2018-10-22 10:57:39	UDP flooding attack	Outbound		fecfca56-2b		High	Deny	Number of packets sent on an IP ...	View	Add
9	2018-10-22 10:43:07	UDP flooding attack	Outbound		fecfca56-2b		High	Deny	Number of packets sent on an IP ...	View	Add
10	2018-10-22 10:30:59	UDP flooding attack	Outbound		fecfca56-2b		High	Deny	Number of packets sent on an IP ...	View	Add
11	2018-10-22 09:42:08	UDP flooding attack	Outbound		fecfca56-2b		High	Deny	Number of packets sent on an IP ...	View	Add
12	2018-10-22 09:18:11	UDP flooding attack	Outbound		fecfca56-2b		High	Deny	Number of packets sent on an IP ...	View	Add
13	2018-10-20 19:49:20	UDP flooding attack	Outbound		fecfca56-2b		High	Deny	Number of packets sent on an IP ...	View	Add
14	2018-10-20 19:09:01	UDP flooding attack	Outbound		fecfca56-2b		High	Deny	Number of packets sent on an IP ...	View	Add
15	2018-10-20 17:07:29	UDP flooding attack	Outbound		fecfca56-2b		High	Deny	Number of packets sent on an IP ...	View	Add



Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

The information in this document is subject to change without notice.

To obtain the latest version, contact the international service center of SANGFOR Technologies Inc