



# IAM

## Anti-DOS attack Troubleshooting Guide

Version 12.0.18



## Change Log

Date	Change Description
June 3, 2019	Version 12.0.18 document release.

# CONTENT

Chapter 1 Normal traffic is intercepted by IAM .....	1
--	---

# Chapter 1 Normal traffic is intercepted by IAM

- Start **Troubleshooting** first to check if it is a packet blocked by the anti-DOS attack module. If the **Action** column shows **dosck**, it means that the anti-DOS attack module intercepts the packet.

The screenshot displays a network management interface. In the foreground, a 'Filter' dialog box is open, showing the following configuration:

- IP Address (Packet Drop)**: Specified IP: 192.168.19.217
- Protocol**: (Empty)
- Improve logs readability**
- Turn on passthrough as well**
- IP Address**: 192.168.19.217
- Advanced**: (Button)
- Enable** and **Cancel**: (Buttons)

In the background, a table of network traffic logs is visible. The table has the following columns: No., Time, Src IP->Dst IP, Protocol, Data Flow, Size, Line, Application, Rule, Source, Packet Drop Tag, and Action. The logs show multiple entries for IP 192.168.19.217, all with the action 'dosck'.

No.	Time	Src IP->Dst IP	Protocol	Data Flow	Size	Line	Application	Rule	Source	Packet Drop Tag	Action
1	14:59:33	192.168.19.217:50494 -> 192.168.19.89:4433	udp	eth0 -> NULL	74(B)	Line1	Others	-	dosck	DROPFLAG_empty	dosck
2	14:59:33	192.168.19.217:50491 -> 192.168.19.89:4433	udp	eth0 -> NULL	74(B)	Line1	Others	-	dosck	DROPFLAG_empty	dosck
3	14:59:33	192.168.19.217:50493 -> 192.168.19.89:4433	udp	eth0 -> NULL	74(B)	Line1	Others	-	dosck	DROPFLAG_empty	dosck
4	14:59:33	192.168.19.217:50492 -> 192.168.19.89:4433	udp	eth0 -> NULL	74(B)	Line1	Others	-	dosck	DROPFLAG_empty	dosck
5	14:59:33	192.168.19.217:50494 -> 192.168.19.89:4433	udp	eth0 -> NULL	74(B)	Line1	Others	-	dosck	DROPFLAG_empty	dosck
6	14:59:33	192.168.19.217:50493 -> 192.168.19.89:4433	udp	eth0 -> NULL	74(B)	Line1	Others	-	dosck	DROPFLAG_empty	dosck
7	14:59:33	192.168.19.217:50491 -> 192.168.19.89:4433	udp	eth0 -> NULL	74(B)	Line1	Others	-	dosck	DROPFLAG_empty	dosck
8	14:59:33	192.168.19.217:50494 -> 192.168.19.89:4433	udp	eth0 -> NULL	74(B)	Line1	Others	-	dosck	DROPFLAG_empty	dosck
9	14:59:33	192.168.19.217:50492 -> 192.168.19.89:4433	udp	eth0 -> NULL	74(B)	Line1	Others	-	dosck	DROPFLAG_empty	dosck
10	14:59:33	192.168.19.217:50493 -> 192.168.19.89:4433	udp	eth0 -> NULL	74(B)	Line1	Others	-	dosck	DROPFLAG_empty	dosck
11	14:59:33	192.168.19.217:50491 -> 192.168.19.89:4433	udp	eth0 -> NULL	74(B)	Line1	Others	-	dosck	DROPFLAG_empty	dosck
12	14:59:33	192.168.19.217:50494 -> 192.168.19.89:4433	udp	eth0 -> NULL	74(B)	Line1	Others	-	dosck	DROPFLAG_empty	dosck

- Query the IP address intercepted by the anti-DOS attack module in the system log to determine the traffic of these IPs.

No.	Module	Type	Time	Details
1	Inside DoS attack(dosckctl)	Info	14:37:22	msg0059: Config has been updated, driver enable
2	Inside DoS attack(dosckctl)	Warning	14:36:58	wrn0228: Defending against UDP attacks (eth0, more than 1000 packets/sec): 192.168.19.217:60393(FE:FC:FE:57:9F:08) --> 192.168.19.89:4433
3	Inside DoS attack(dosckctl)	Warning	14:36:58	wrn0253: Unlocking source IP address(192.168.19.217)
4	Inside DoS attack(dosckctl)	Warning	14:35:56	wrn0228: Defending against UDP attacks (eth0, more than 1000 packets/sec): 192.168.19.217:60327(FE:FC:FE:57:9F:08) --> 192.168.19.89:4433
5	Inside DoS attack(dosckctl)	Info	14:34:47	msg0059: Config has been updated, driver enable
6	Inside DoS attack(dosckctl)	Info	14:33:53	msg0059: Config has been updated, driver enable
7	Inside DoS attack(dosckctl)	Warning	14:30:13	wrn0228: UDP attack from bypass IP address(eth0, more than 1000 packets/sec): 192.168.19.217:60253(FE:FC:FE:57:9F:08) --> 192.168.19.89:3389
8	Inside DoS attack(dosckctl)	Warning	14:30:13	wrn0253: Unlocking source IP address(192.168.19.217)
9	Inside DoS attack(dosckctl)	Warning	14:29:05	wrn0228: Defending against UDP attacks (eth0, more than 1000 packets/sec): 192.168.19.217:60208(FE:FC:FE:57:9F:08) --> 192.168.19.89:3389
10	Inside DoS attack(dosckctl)	Info	14:28:52	msg0059: Config has been updated, driver enable
11	Inside DoS attack(dosckctl)	Info	14:28:44	msg0059: Config has been updated, driver enable
12	Inside DoS attack(dosckctl)	Info	14:28:32	msg0059: Config has been updated, driver enable
13	Inside DoS attack(dosckctl)	Info	14:22:23	msg0059: Config has been updated, driver enable

- Please check if the traffic exceeds the limit of the IAM anti-DOS attack module. The judgment criteria of IAM are as follows. A general device does not generate a large number of data packets within 1s.

#### Rules:

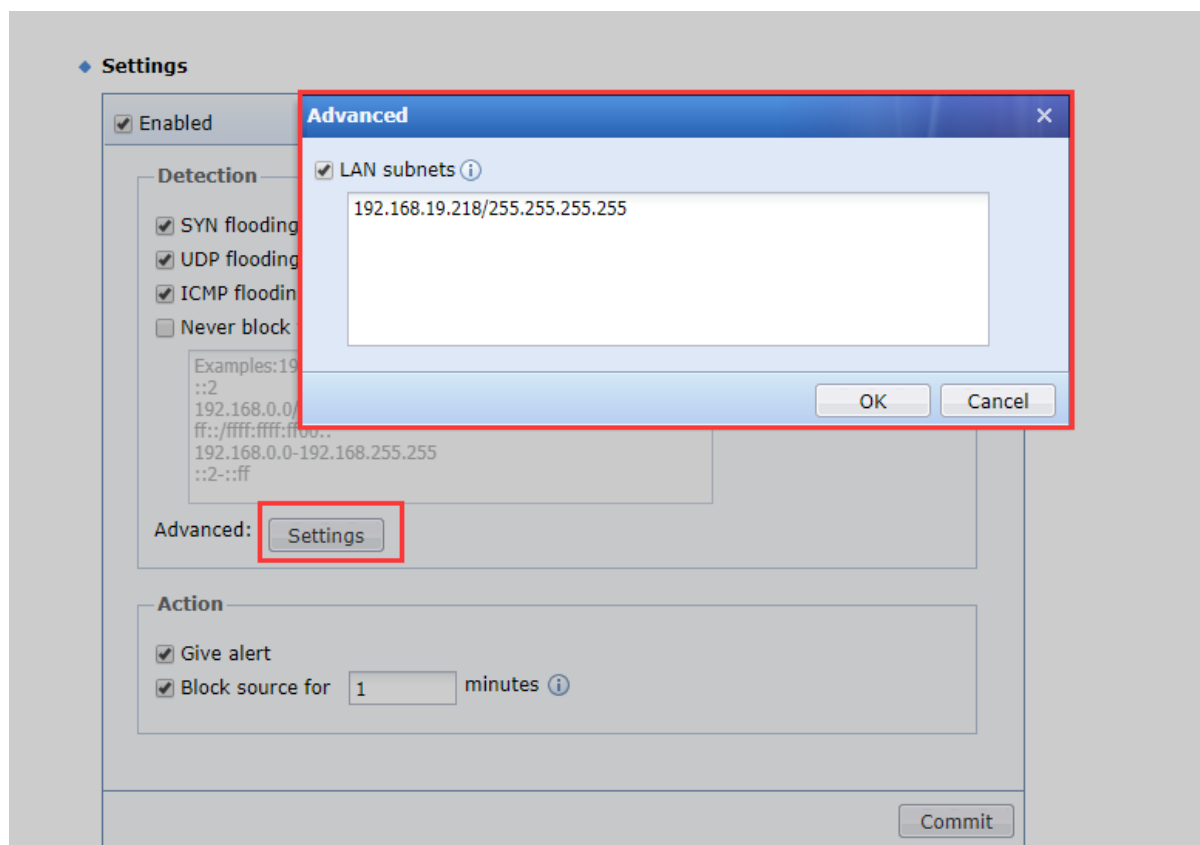
The number of udp upstream packets that are consecutive and consistent in size according to source ip and target ip in 1 second. If more than **1000**, it is judged as udp dos attack.

Within 1 second, according to the source ip and the target ip, the difference between the number of packets SYN packets and ACK packets of the tcp handshake is more than **1000**, and it is determined to be tcp dos attack.

The total number of ICMP ping packets is counted by source ip and target ip in 1 second , and the total number reaches **1000**, which is judged as ICMP dos attack.

## Chapter 2 Check if the configuration is correct

- Regarding the configuration of the anti-DOS attack module, if you want to fill in the LAN subnet, you must fill in the complete subnet segment of all the intranets, otherwise the anti-DOS attack module will intercept the data packet.



- If some network devices on the intranet have relatively large traffic, you can consider adding the IP of this device to the exclusion list.

Enabled

**Detection**

- SYN flooding
- UDP flooding
- ICMP flooding
- Never block the internal IP addresses below. ⓘ

Examples:192.168.0.1  
::2  
192.168.0.0/255.255.255.0  
ff::/ffff:ffff:ff00::  
192.168.0.0-192.168.255.255  
::2-::ff

Advanced:

**Action**

- Give alert
- Block source for  minutes ⓘ



**SANGFOR**

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