Pocket Guide

Create DoS Bypass Rule

Product: Sophos XG Firewall
## Contents

**Overview** ........................................................................................................... 3

**Prerequisite** ......................................................................................................... 3

**Configuration** .................................................................................................... 4

Create a DoS Bypass Rule ....................................................................................... 4

**Result** .................................................................................................................. 5

**Copyright Notice** .................................................................................................. 6
Create DoS Bypass Rule

**Overview**
This guide describes the steps to create a DoS bypass rule in Sophos XG Firewall.

You can create a rule to bypass DoS inspection for traffic of certain protocols between the specified source and destination ports and networks. XG Firewall allows you to bypass DoS rules when the specified source is not a threat to your network. By default, VPN traffic is subjected to DoS inspection.

**Prerequisite**
You must have read-write permissions on the SFOS Admin Console for the relevant features.
**Configuration**

Log in to the SFOS Admin Console.

**Create a DoS Bypass Rule**

- Go to Protect > Intrusion Prevention > DoS & Spoof Protection.
- Under DoS Bypass Rule, click Add.

![DoS Bypass Rule](image)

- Select IP Family.
- Enter Source IP/Netmask.
- Enter Destination IP/Netmask.
- Select Protocol. Traffic belonging to this protocol between the specified source and destination will be bypassed.
- Enter Source Port.
- Enter Destination Port.

Note: To bypass traffic, enter *.

![Add DoS Bypass Rule](image)

Click Save.
Result
You have created a DoS bypass rule.
Copyright Notice

Copyright 2016-2018 Sophos Limited. All rights reserved. Sophos is a registered trademark of Sophos Limited and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.