Keeping the Internet Flowing: How IXPs Handle DDoS

José Alberto Nistal

22/05/2025 – ESNOG33

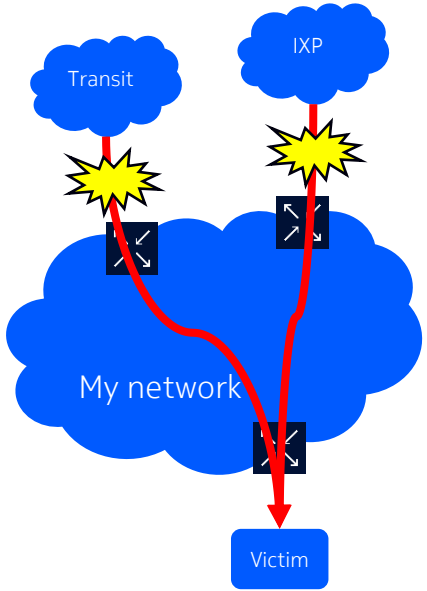
 © 2025 Nokia

Agenda

- The need for DDoS mitigation in IXPs
- Basic concepts: The RTBH mechanism
- Approaches to DDoS mitigation in IXPs
- Recap

© 2025 Nokia

The need for DDoS mitigation in IXPs



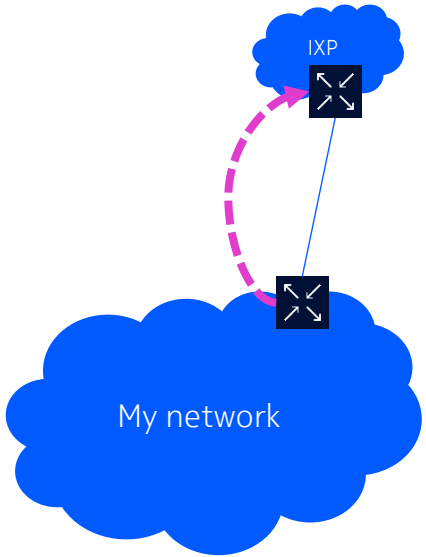
- DDoS traffic comes from everywhere: transit, IXPs, etc.
- Blocking DDoS at edge works very well (if you have enough upstream bandwidth)
- In small and medium ISPs, upstream links may get congested
- Need for upstream mitigation
- Transit providers generally offer DDoS protection
- Up to now, IXPs didn’t

© 2025 Nokia

Basic concepts: The RTBH mechanism

Remotely Triggered Black Hole

- We advertise a BGP route that includes the victim's IP address
  - This can be an existing route or a new, temporary one
  - Ideally /32 although other lengths may be needed for carpet-bomb attacks
- This route is tagged with the BLACKHOLE community
  - Preferred 65535:666 as defined by RFC 7999
  - Other communities can be used instead
- The upstream network (IXP) discards all traffic destined for this prefix

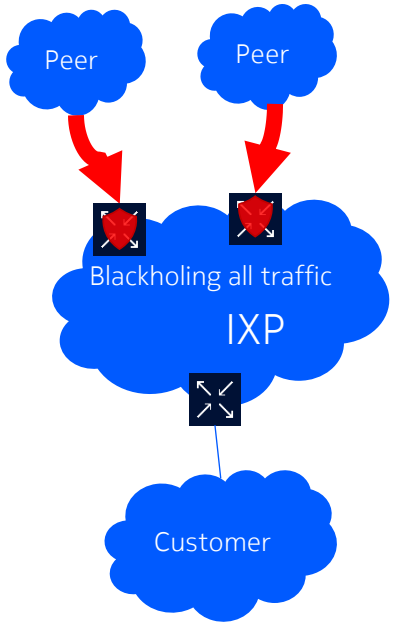


© 2025 Nokia

How do IXPs handle DDoS?

Approach 1: Blackholing

- Supported by most IXPs today, including CATNIX, DE-CIX and ESPANIX
- Customer needs to detect the attack and request the blackholing to the IXP using BGP
- All or nothing mitigation: the IXP discards all traffic destined for this prefix, including good and bad traffic



© 2025 Nokia

How do IXPs handle DDoS?

Approach 2: Blackholing Advanced

- Introduced by DE-CIX
- Customer can drop, shape or whitelist specific protocols and ports using extended BGP communities
- Customer needs to detect the attack and request the required actions to the IXP using BGP
- Reasonably selective on what to drop, shape or whitelist
- Very hard to implement

Rule	Drop Community	Shape Community (5Mbps)
All traffic	RT:6695:4200000000	RT:6695:4200000001
UDP	RT:6695:4200000002	RT:6695:4200000003
UDP, source port = 0 (unassigned)	RT:6695:4200000004	RT:6695:4200000005
UDP, source port = 19 (CharGen)	RT:6695:4200000006	RT:6695:4200000007
UDP, source port = 53 (DNS)	RT:6695:4200000008	RT:6695:4200000009
UDP, source port = 123 (NTP)	RT:6695:4200000010	RT:6695:4200000011
UDP, source port = 389 (LDAP)	RT:6695:4200000012	RT:6695:4200000013
UDP, source port = 11211 (Memcached)	RT:6695:4200000014	RT:6695:4200000015

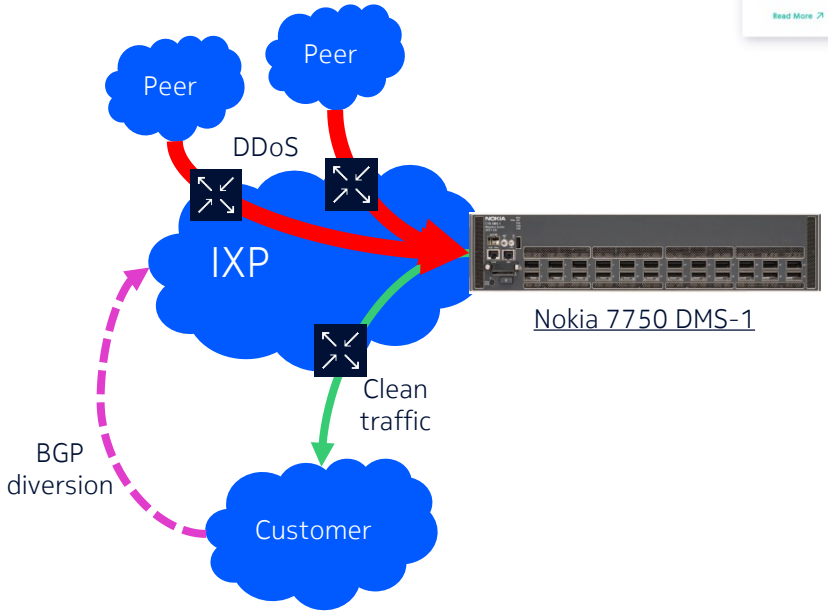
© 2025 Nokia

How do IXPs handle DDoS?

Approach 3: On demand scrubbing

Link to press release

- Introduced by LINX
- Customer detects the attack and requests cleaning using BGP communities
- Traffic is diverted to the scrubber, which analyzes the traffic and performs the required cleaning
- Clean traffic is routed back to customer

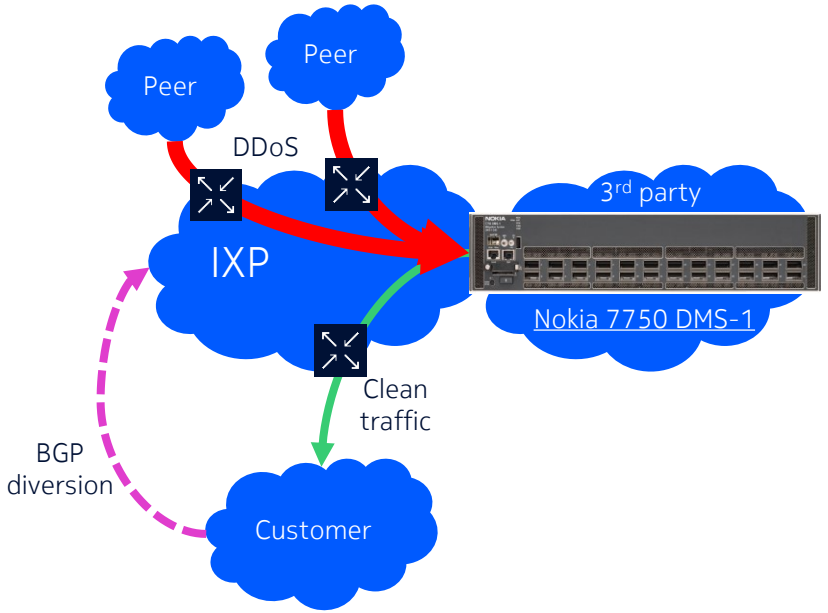


© 2025 Nokia

How do IXPs handle DDoS?

Approach 4: On demand scrubbing provided by 3rd party

- 3rd party takes care of scrubber/cleaning
- Customer detects the attack and requests cleaning using BGP communities
- Traffic is diverted to 3rd party for cleaning
- Clean traffic is routed back to customer

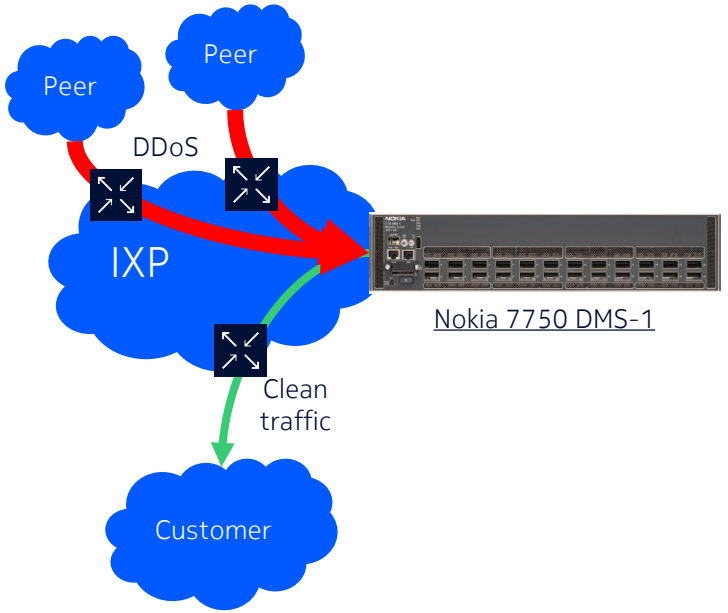


© 2025 Nokia

How do IXPs handle DDoS?

Approach 5: Automated scrubbing

- Customer does not need to detect the attack, it is detected automatically by the IX
- Traffic is diverted to the scrubber, which analyzes the traffic and performs the required cleaning
- Clean traffic is routed back to customer

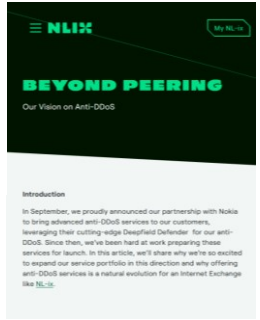


© 2025 Nokia

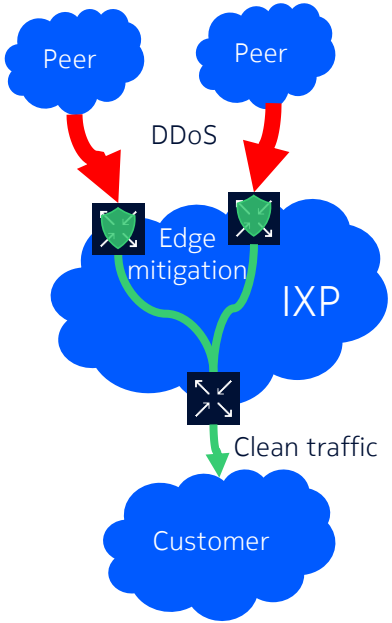
How do IXPs handle DDoS?

Approach 6: Automated edge mitigation

Link to blog post



- Introduced by NL-ix
- Customer does not need to detect the attack, it is detected automatically by the IX
- No scrubbing appliance needed, no diversion needed
- DDoS is mitigated by the existing network devices
- Clean traffic is routed normally



© 2025 Nokia

DDoS protection model recap

Customer's perspective

	Blackholing	Blackholing Advanced	On-demand scrubbing	On-demand scrubbing (3rd)	Automated scrubbing	Automated edge mitigation
Who detects	Customer	Customer	Customer	Customer	IXP	IXP
Mitigation	All or nothing	Complex	Full	Full	Full	Full
Automation	Partial	Partial	Partial	Partial	Full	Full
Scalability	Peering capacity	Peering capacity	2.8 Tbps	2.8 Tbps	2.8 Tbps	Peering capacity

© 2025 Nokia

DDoS protection model recap

IXP's perspective

	Blackholing	Blackholing Advanced	On-demand scrubbing	On-demand scrubbing (3rd)	Automated scrubbing	Automated edge mitigation
Network requirements	Basic equipment	Powerful filtering	Basic equipment	Basic equipment	Basic equipment	Powerful filtering
Integration requirements	Easy	Medium	Easy	Easy	Easy	Easy
Customer perception	Poor	Medium	Good	Good	Good	Good
Cost	Low	Low	Medium	Low (3rd party)	Medium	Medium
Revenue	None	None	Good	Medium	Good	Good

© 2025 Nokia


NOKIA

Copyright and confidentiality

The contents of this document are proprietary and confidential property of Nokia. This document is provided subject to confidentiality obligations of the applicable agreement(s).

This document is intended for use by Nokia's customers and collaborators only for the purpose for which this document is submitted by Nokia. No part of this document may be reproduced or made available to the public or to any third party in any form or means without the prior written permission of Nokia. This document is to be used by properly trained professional personnel. Any use of the contents in this document is limited strictly to the use(s) specifically created in the applicable agreement(s) under which the document is submitted. The user of this document may voluntarily provide suggestions, comments or other feedback to Nokia in respect of the contents of this document ("Feedback").

Such Feedback may be used in Nokia products and related specifications or other documentation. Accordingly, if the user of this document gives Nokia Feedback on the contents of this document, Nokia may freely use, disclose, reproduce, license, distribute and otherwise commercialize the feedback in any Nokia product, technology, service, specification or other documentation.

Nokia operates a policy of ongoing development. Nokia reserves the right to make changes and improvements to any of the products and/or services described in this document or withdraw this document at any time without prior notice.

The contents of this document are provided "as is". Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy, reliability or contents of this document. NOKIA SHALL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT or for any loss of data or income or any special, incidental, consequential, indirect or direct damages howsoever caused, that might arise from the use of this document or any contents of this document.

This document and the product(s) it describes are protected by copyright according to the applicable laws.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.