

Link Oregon

**Built for Innovation.
Powered by Community.**



Link Oregon DDoS Mitigation Capabilities

Presenter: Stephen Fromm

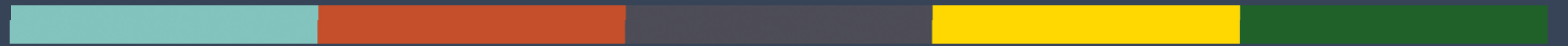
Hey, what is your DDoS protection solution again?”

AGENDA

- Link Oregon Mitigation Toolbox
- Network Telemetry & Detection
- BGP Flowspec & Mitigation
- Volumetric mitigation with Radware



LINK OREGON



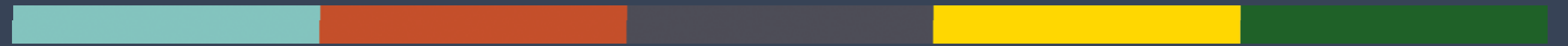
MITIGATION TOOLBOX

OUR MITIGATION TOOLBOX

- *Defense in depth* - No single tool is a cure-all.
- [Team Cymru](#) Bogon and [UTRS](#) feeds
- ACLs on interfaces & BGP peerings to sanitize accepted routes
- RTBH - Remote Trigger Black Hole
- BGP Flowspec with Kentik
- Volumetric attack mitigation with Radware
- BGP communities for traffic engineering
- <https://www.linkoregon.org/tech/bgp/>



LINK OREGON

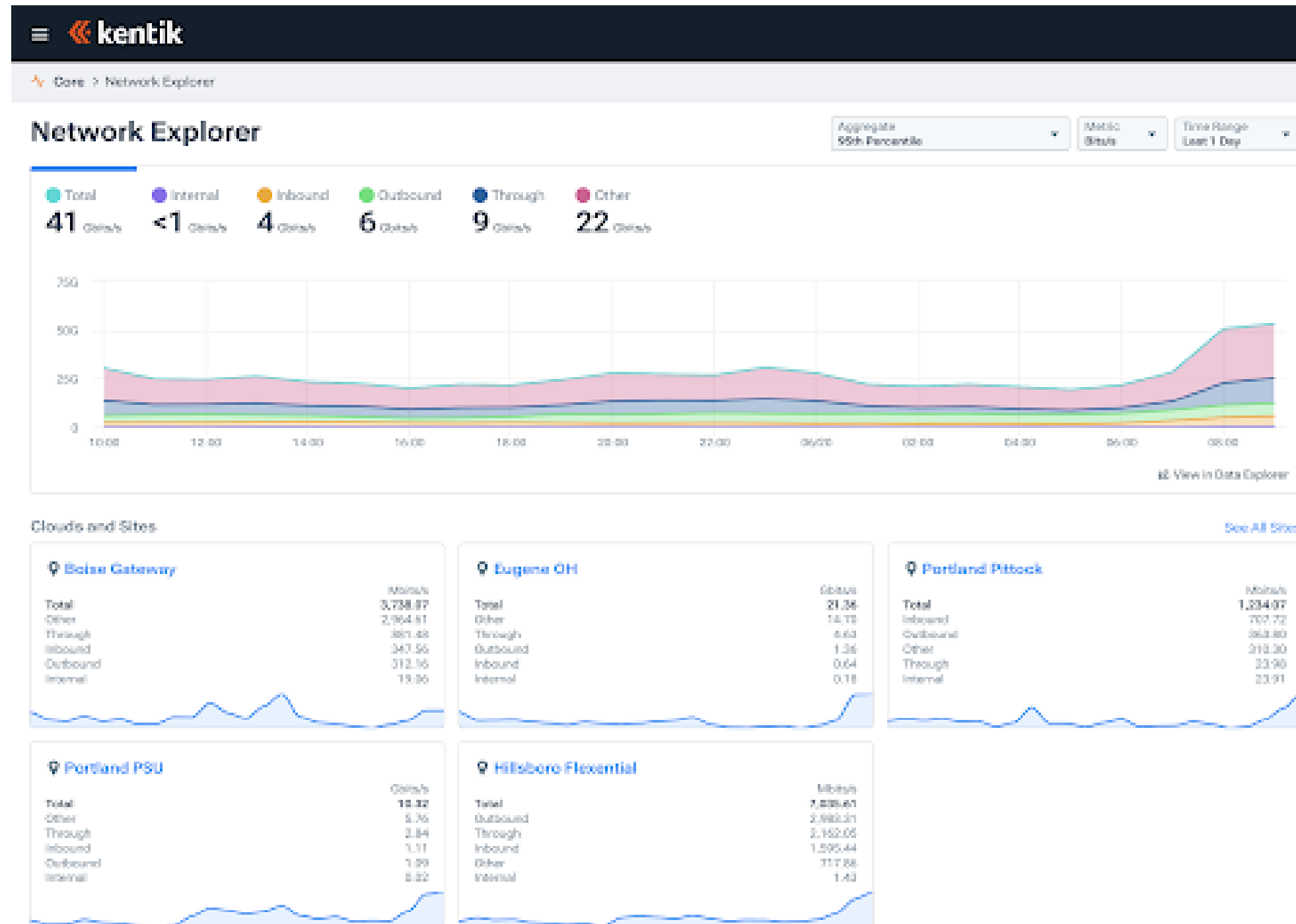


NETWORK TELEMETRY & DETECTION

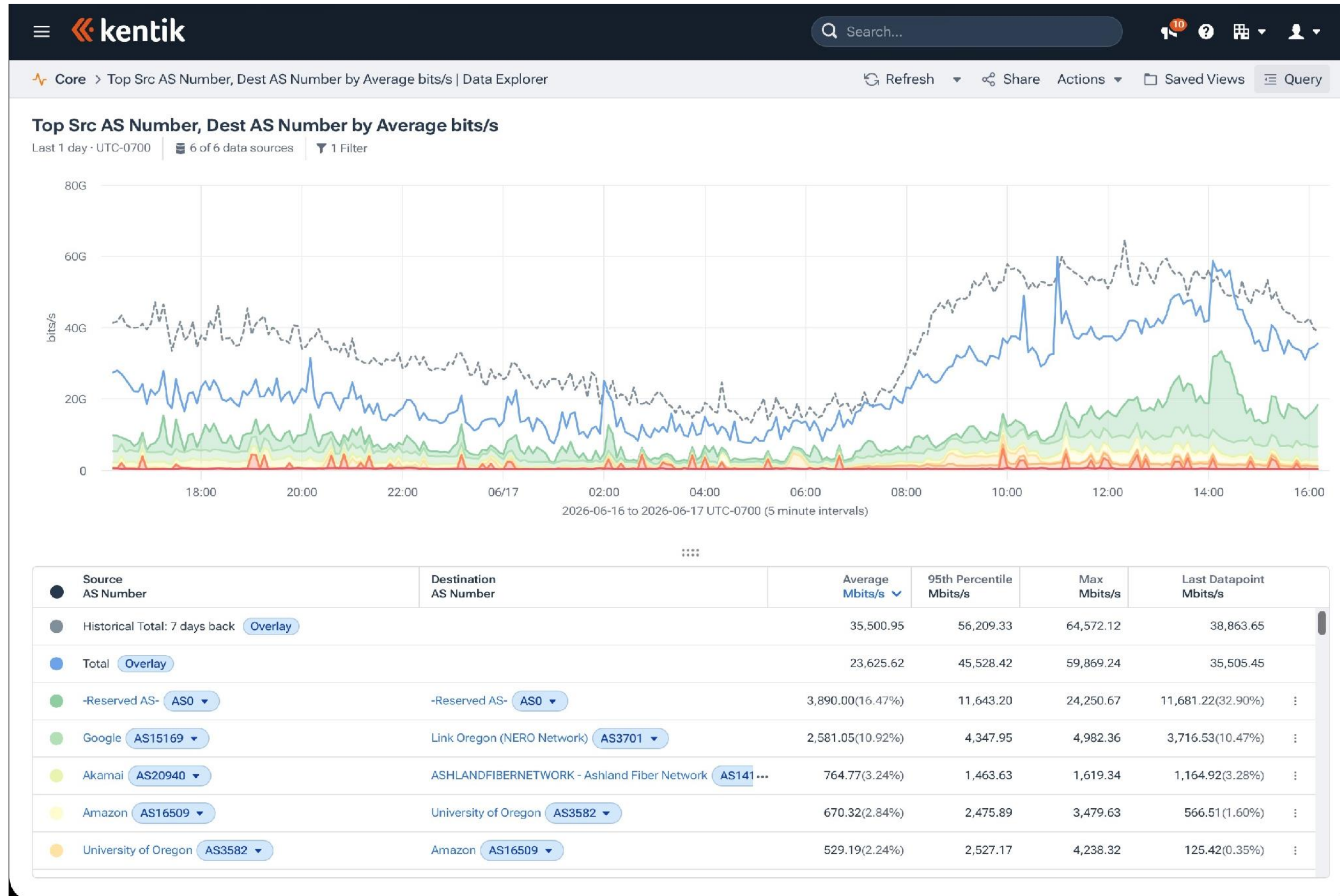
KENTIK & NETWORK TELEMETRY

- Network Telemetry sent to Kentik
 - Local agent SNMP queries Link Oregon routers
 - Send sFlow data with BGP extension enabled
 - Includes AS hop, BGP community, and other BGP attributes
 - BGP peer with Kentik as a route-reflector-client
- Ability to visualize network telemetry
- Visualize peering and interconnection data
- Default reports and ability to create custom reports
- **Ability to create portals for members**

VISUALIZE NETWORK TELEMETRY



STANDARD FEATURES FOR INSPECTING NETFLOW



KENTIK MEMBER PORTAL

- Link Oregon can create Portals for Members
- Members can view their traffic across Link Oregon Backbone
- Member view limited to their networks
- Traffic Analysis and DDoS Investigation

MEMBER PORTAL

The screenshot displays the LINK OREGON Member Portal interface. At the top left is the LINK OREGON logo. The main heading is "Explore Your Network" with a star icon. Below this is a "Library" tab. The interface is divided into two main sections: "ALERT DASHBOARDS" and "EXPLORER DASHBOARDS".

ALERT DASHBOARDS

- Attack**: Use this view to dig into a specific insight or alarm associated with potentially malicious network activity. LINKOR Tentant Views Package.
- DDoS Investigation**: Use this view to understand graphical and tabular data about an attack. (Note: Use this view with a DDoS Policy in the alerting system). LINKOR Tentant Views Package.
- UDP Attack**: LINKOR Tentant Views Package.
- TCP Attack**: LINKOR Tentant Views Package.
- Inbound DDoS**: Use this view to investigate inbound DDoS attacks. Quickly diagnose and understand attack impacts to inform mitigation actions and reporting. LINKOR Tentant Views Package.

EXPLORER DASHBOARDS

- Pivot**: This dashboard is used throughout Data Explorer when you explode a given time series into multiple dimensions. LINKOR Tentant Views Package.
- Site Explorer**: SELECT A SITE. Includes a text input field and a "Go" button. LINKOR Tentant Views Package.
- Interface Explorer**: SELECT AN INTERFACE. Includes a text input field and a "Go" button. LINKOR Tentant Views Package.
- Connectivity Explorer**: SELECT A CONNECTIVITY TYPE. Includes a dropdown menu with "Select a value..." and a "Go" button. LINKOR Tentant Views Package.
- Prefix Explorer**: ENTER AN PREFIX/LEN. Includes a text input field and a "Go" button. LINKOR Tentant Views Package.
- IP Explorer**: ENTER AN IP. Includes a text input field and a "Go" button. LINKOR Tentant Views Package.
- ASN Explorer**: SELECT AN AS NUMBER. Includes a text input field and a "Go" button. LINKOR Tentant Views Package.

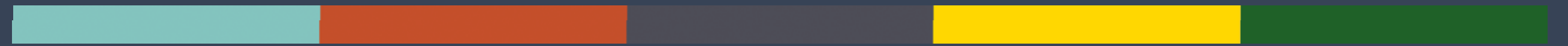
At the bottom left of the interface, it says "GENERAL PURPOSE".

KENTIK MEMBER PORTAL (cont...)

- There are 25 dashboards available
- Ranges from Traffic Overview, to Top Talkers, to DDoS Investigation
- Includes visualizations and tabular data
- <https://portal.kentik.com>
- **Please reach out with any questions**



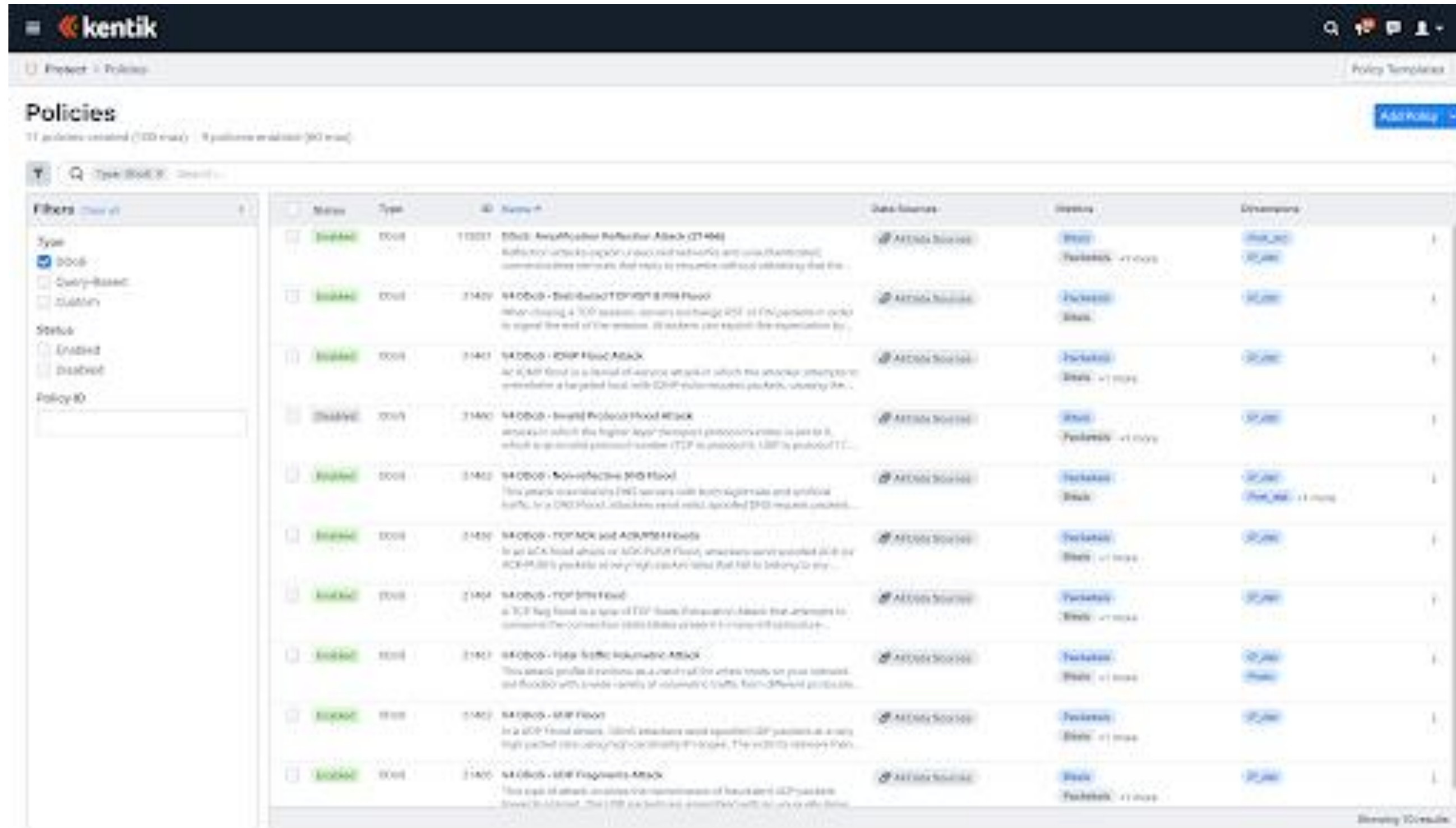
LINK OREGON



DDoS DETECTION & MITIGATION

KENTIK AND DDoS MITIGATION

Baked in DDoS Detection & Reporting



The screenshot shows the Kentik interface for managing DDoS mitigation policies. The page title is "Policies" and it indicates that 11 policies are created and 9 are evaluated. A search bar is present above the table. On the left, there are filters for Type (DDoS, Query-based, Custom), Status (Enabled, Disabled), and Policy ID. The main table lists various DDoS mitigation policies with columns for Name, Type, ID, Name, Description, Data Sources, Status, and Dynamic.

Name	Type	ID	Name	Description	Data Sources	Status	Dynamic
11001	DDoS	11001	DDoS - Amplifier Reflector Attack (DRAM)	Amplifier/reflector attacks exploit network architecture to send thousands of malicious requests that reply to requests without verifying that the...	ATTN: SOURCE	Block	Block, IP
11409	DDoS	11409	SYN Flood - Distributed Denial of Service Flood	When closing a TCP session, servers exchange SYN and ACK packets in order to signal the end of the session. If someone can exploit the negotiation by...	ATTN: SOURCE	Block	Block, IP
11411	DDoS	11411	SYN Flood - SYN Flood Attack	An SYN flood is a form of denial of service attack in which the attacker attempts to overwhelm a targeted host with SYN connection requests, causing the...	ATTN: SOURCE	Block	Block, IP
11410	DDoS	11410	SYN Flood - Slow Poison Flood Attack	Attack in which the higher layer transport protocols' state is set to 0, which is equivalent to a closed socket (TCP is FIN_WAIT_2, UDP is FIN_WAIT_2...	ATTN: SOURCE	Block	Block, IP
11412	DDoS	11412	SYN Flood - Non-reflective SYN Flood	This attack overwhelms DNS servers with both legitimate and spoofed traffic. In a DNS flood, attackers send valid, spoofed DNS requests to...	ATTN: SOURCE	Block	Block, IP, IP, IP
11413	DDoS	11413	SYN Flood - TCP ACK and ACK RST Floods	In an ACK flood attack or ACK RST flood, attackers send spoofed ACK or ACK RST packets to the target server and cause the host to believe the...	ATTN: SOURCE	Block	Block, IP
11414	DDoS	11414	SYN Flood - TCP SYN Flood	A TCP flag found in a type of DDoS attack that causes the attacker to consume the connection state table of the target system...	ATTN: SOURCE	Block	Block, IP
11415	DDoS	11415	SYN Flood - High Traffic Volumetric Attack	This attack profile is common as a result of other types of your targeted, but flooded with a wide variety of volumetric traffic from IP-based providers...	ATTN: SOURCE	Block	Block, IP
11416	DDoS	11416	SYN Flood - SYN Flood	In a SYN flood attack, client machines send spoofed SYN packets to a very high port on the target's IP address. The victim receives many...	ATTN: SOURCE	Block	Block, IP
11417	DDoS	11417	SYN Flood - SYN Fragment Attack	This type of attack involves the transmission of large sized SYN packets from multiple sources. The SYN packets are spoofed with the victim's IP...	ATTN: SOURCE	Block	Block, IP

DDoS DETECTION– TYPES OF ATTACKS

- Total Traffic Volumetric Attack
- Amplification Reflection Attack
- ICMP Flood Attack
- UDP Flood
- UDP Fragments Attack
- And more ...

DDoS DETECTION– Continued

- Build filters of what to include/exclude
- Example: DDoS Amplification Reflection filters
 - 19/udp
 - 53/udp
 - 123/udp
 - 161/udp
 - 162/udp
 - Others per [CISA](#)
- Link Oregon NOC uses Kentik API to report detected and mitigated events to members

BGP FLOWSPEC

- Kentik supports several platforms for mitigation
- Link Oregon is using BGP Flowspec, [RFC-5575](#)
- Use BGP to disseminate rules for traffic flow specifications

BGP FLOWSPEC RULES

- Flowspec rule can match on (not exhaustive):
 - Source and/or destination IP
 - Protocol
 - Source and/or destination port
 - DSCP
 - TCP Flags
 - Packet Length
- Filters are typically inferred from the triggered DDoS Policy

BGP FLOWSPEC ACTIONS

- Options for Flowspec actions
 - Rate Limit
 - Discard
 - Mark DSCP
 - Route-Target redirect
 - Next-hop redirect
- Link Oregon approach is to rate limit
 - This is typically *bytes/sec*
 - Endeavour to *do no harm*
- Can take more aggressive stance when working with customer

KENTIK MITIGATION VIEW

The screenshot displays the Kentik Mitigation View interface. At the top, there is a navigation bar with the Kentik logo, a search bar, and user profile icons. Below the navigation bar, the breadcrumb path is "Protect > Mitigations". The main content area is titled "Mitigations" and includes a "Start a Manual Mitigation" button. A filter bar shows "Group By: None" and a search box with "Status: Waiting, Inactive, Active, Failed". A sidebar on the left contains filters for "Time Range (Local)" (Last 14 days), "Status" (Active, Failed, Waiting, Inactive), "Type", "Source" (Policy, Manual), "Control" (Policy, Manual), "Mitigation ID", "Alert ID", "Method" (No methods selected), "Platform" (No platforms selected), and "Show Tenant Mitigations". The main table lists four mitigation actions, all with a status of "Archived".

<input type="checkbox"/>	Status	Mitigation ID	Policy	Platform	Method	Target	Started (Local)	Min. Time Remaining	<input type="checkbox"/>
<input type="checkbox"/>	Archived	10521	V4 DDoS - No...	LinkOR Flo...	UDP Destinati...	protocol: =17 destination-port...	2026-06-09 16...	None	<input type="checkbox"/>
<input type="checkbox"/>	Archived	10520	V4 DDoS - No...	LinkOR Flo...	UDP Destinati...	protocol: =17 destination-port...	2026-06-05 12...	None	<input type="checkbox"/>
<input type="checkbox"/>	Archived	10519	V4 DDoS - No...	LinkOR Flo...	UDP Destinati...	protocol: =17 destination-port...	2026-06-03 04...	None	<input type="checkbox"/>
<input type="checkbox"/>	Archived	10518	V4 DDoS - No...	LinkOR Flo...	UDP Destinati...	protocol: =17 destination-port...	2026-06-01 18...	None	<input type="checkbox"/>

Showing 4 results

MANUAL MITIGATION TRIGGER VIA KENTIK

The screenshot displays the Kentik web interface for manual mitigation. A modal dialog titled "Start Manual Mitigation" is open, allowing users to configure a new mitigation. The dialog includes the following fields:

- Mitigation Method*:** A dropdown menu showing "ICMP flowspec Rate Limit" with "Platform: LinkOR Flowspec" below it.
- IP/CIDR to Mitigate*:** A text input field.
- Comment:** A text input field.
- Time Before Auto Stop (TTL):** A text input field with the value "5" and a unit dropdown menu set to "minutes". Below this field is the instruction: "Set the TTL to 0 to disable auto stop."
- Tenant:** A dropdown menu with the text "Select a tenant...". Below it is the instruction: "Associate this manual mitigation with a tenant. The mitigation will show as read-only for the tenant."

At the bottom of the dialog are two buttons: "Cancel" and "Add Manual Mitigation".

The background interface shows the "Mitigations" page with a search bar, filters, and a table of mitigation records. The table has columns for "Started (Local)", "Min. Time Remaining", and "Customize". The table contains four rows of data, each representing a mitigation record.

MANUAL MITIGATION FLOWSPEC

```
eugn-oh-pe-02(vrf:Internet_3701)#
eugn-oh-pe-02(vrf:Internet_3701)#
eugn-oh-pe-02(vrf:Internet_3701)#show bgp flow-spec ipv4
BGP Flow Specification rules for VRF Internet_3701
Router identifier 207.98.127.249, local AS number 3701
Rule status codes: # - not installed, M - received from multiple peers

Matching Rule                                     Actions
[REDACTED]*;IT:=8|=3|=0|=4|=5|=9;                Police: 8 Mbps (1 MBps)
eugn-oh-pe-02(vrf:Internet_3701)#
eugn-oh-pe-02(vrf:Internet_3701)#
eugn-oh-pe-02(vrf:Internet_3701)#
eugn-oh-pe-02(vrf:Internet_3701)#
eugn-oh-pe-02(vrf:Internet_3701)#show bgp flow-spec ipv4 detail
BGP Flow Specification rules for VRF Internet_3701
Router identifier 207.98.127.249, local AS number 3701
BGP Flow Specification Matching Rule for [REDACTED]*;IT:=8|=3|=0|=4|=5|=9;
Rule identifier: 139716912222928
Matching Rule:
  Destination Prefix: [REDACTED]
  Source Prefix: *
  ICMP Type: =8 | =3 | =0 | =4 | =5 | =9
Paths: 1 available
Local
  from 208.76.14.223 (208.76.14.223)
    Origin IGP, metric -, localpref 100, weight 0, valid, internal, best
    Actions: Police: 8 Mbps (1 MBps)
eugn-oh-pe-02(vrf:Internet_3701)#
```



LINK OREGON



VOLUMETRIC MITIGATION

VOLUMETRIC MITIGATION WITH RADWARE



- **On-demand** cloud-based DDoS mitigation
- Radware scrubbing service is available through Internet2 agreement
- Contract established in 2022 as part of preparation for *Oregon22*
- Best suited for volumetric attacks and member wants to push the mitigation further upstream
- Needs collaboration with Radware SOC to target less obvious or application-specific vectors

VOLUMETRIC MITIGATION WITH RADWARE (Continued)

- Link Oregon, or partner, BGP announces more specific IP prefix to Radware
- Clean traffic comes back via peering with Internet2/Radware
 - A total of 1G of clean traffic is currently supported
- Tested multiple times in preparation for Oregon22 event
- Successfully used in several real-world member security incidents
- Requires LOA between member and Link Oregon

RADWARE DEDICATED TENANCY

- For a separate recurring fee:
 - Link Oregon members can peer with Radware and directly trigger mitigation
 - Link Oregon gets separate Radware portal to manage mitigations
 - Requires LOA between member and Radware

BGP SIGNAL TO BEGIN MITIGATION

```
port-psu-pe-01(vrf:Internet_3701)#show ip bgp nei 163.253.4.182 advertised-routes detail
BGP routing table information for VRF Internet_3701
Router identifier 207.98.127.252, local AS number 3701
Update wait-install is disabled
BGP routing table entry for 140.211.4.0/24
  Paths: 1 available
    3701
      163.253.4.183 from 207.98.127.254 (207.98.127.254), imported EVPN route, RD
207.98.127.249:15001
  Origin INCOMPLETE, metric -, localpref -, IGP metric -, weight -, tag 0
  Received 00:00:28 ago, valid, internal, best, AS Origin not validated
  Extended Community: Route-Target-AS:3701:15001 Route-Target-AS4:396450:723
TunnelEncap:tunnelTypeMpls
  Rx SAFI: Unicast
```

MORE SPECIFIC ADVERTISED ROUTE

```
route-views>sh ip bgp 140.211.4.0/24
BGP routing table entry for 140.211.4.0/24, version 1259985930
Paths: (14 available, best #3, table default)
  Not advertised to any peer
  Refresh Epoch 1
1351 174 1299 198949 396450 3701
  132.198.255.253 from 132.198.255.253 (132.198.255.253)
    Origin IGP, localpref 100, valid, external
    path 7F16CC07BD98 RPKI State not found
    rx pathid: 0, tx pathid: 0
  Refresh Epoch 1
3356 198949 396450 3701
  4.68.4.46 from 4.68.4.46 (4.69.184.201)
    Origin IGP, metric 0, localpref 100, valid, external, best
    Community: 3356:3 3356:22 3356:100 3356:123 3356:575
3356:903 3356:2011 64777:0 64777:4101 64777:11103 64777:11202
65000:700
  unknown transitive attribute: flag 0xE0 type 0x20 length
0x24
  value 0003 0925 0000 0000 0000 09C4 0006 0CA2
        0000 0000 0000 038E 0006 0CA2 0000 0003
        0000 02D3
  path 7F158C7EB830 RPKI State not found
  rx pathid: 0, tx pathid: 0x0
```

EXAMPLE- REDIRECTION SCREENCAST

```
stephenf@bstn-03: ~  
Community: 3303:1004 3303:1005 3303:1030 3303:3060 3701:10100 3701:65001 11164:1110 11164:7500  
11164:51240  
path 7F153F32FEB0 RPKI State not found  
rx pathid: 0, tx pathid: 0  
Refresh Epoch 1  
1351 11537 3701  
132.198.255.253 from 132.198.255.253 (132.198.255.253)  
Origin IGP, localpref 100, valid, external  
path 7F16299793F8 RPKI State not found  
rx pathid: 0, tx pathid: 0  
Refresh Epoch 1  
49788 1299 25899 3701 3701 3701  
91.218.184.60 from 91.218.184.60 (91.218.184.60)  
Origin IGP, localpref 100, valid, external  
Community: 1299:1000 1299:35000 1299:55000  
Extended Community: 0x43:100:1  
path 7F15B63F2B50 RPKI State not found  
rx pathid: 0, tx pathid: 0  
Refresh Epoch 1  
3356 3701 3701 3701 3701 3701  
4.68.4.46 from 4.68.4.46 (4.69.184.201)  
Origin IGP, metric 0, localpref 100, valid, external  
Community: 3356:3 3356:22 3356:100 3356:123 3356:575 3356:903 3356:2030 3701:10100 3701:65001  
path 7F16CCED1148 RPKI State not found  
rx pathid: 0, tx pathid: 0  
Refresh Epoch 1  
20080 11537 3701  
198.32.252.33 from 198.32.252.33 (198.32.252.33)  
Origin IGP, localpref 100, valid, external  
Community: 3701:10100 3701:65001 11537:950 20080:6999 20080:8001  
path 7F16203E74C8 RPKI State not found  
rx pathid: 0, tx pathid: 0  
route-views>  
route-views>  
route-views>  
route-views>  
route-views>  
route-views>  
route-views>  
route-views>  
route-views>  
route-views>  
route-views>  
route-views>  
route-views>
```

```
My traceroute [v0.95]  
neptune01.ring.nlnog.net (23.157.160.133) -> 140.211.4.10 (140.211.4.10) 2026-06-19T00:28:09+0000  
Keys: Help Display mode Restart statistics Order of fields quit  
Packets Pings  
Host Loss% Snt Last Avg Best Wrst StDev  
1. AS21700 23.157.160.161 0.0% 112 0.2 0.2 0.1 1.1 0.1  
2. AS21700 23.157.160.4 0.0% 112 0.3 0.3 0.2 0.8 0.1  
3. (waiting for reply)  
4. AS174 be3157.agr21.jfk02.atlas.cogentco.com 0.0% 112 1.2 1.4 1.1 2.0 0.1  
5. AS174 be2606.ccr42.jfk02.atlas.cogentco.com 0.0% 112 1.3 1.4 1.2 2.0 0.1  
6. AS174 port-channel14986.ccr92.cle04.atlas.cogentco.c 0.0% 112 9.2 9.3 9.2 9.6 0.1  
7. AS174 be2718.ccr42.ord01.atlas.cogentco.com 0.0% 112 16.5 16.5 16.3 19.0 0.3  
8. AS174 be5068.ccr32.oma02.atlas.cogentco.com 0.0% 112 24.6 24.8 24.6 25.7 0.2  
9. AS174 be8568.ccr82.den01.atlas.cogentco.com 28.6% 112 36.9 36.4 35.3 39.3 0.6  
10. AS174 be9563.ccr82.slc03.atlas.cogentco.com 67.6% 111 45.9 45.8 44.4 58.2 2.2  
11. AS174 be9528.ccr82.sea08.atlas.cogentco.com 5.4% 111 65.3 64.7 63.4 78.8 1.5  
12. AS174 be9852.ccr22.pdx01.atlas.cogentco.com 0.0% 111 66.8 67.0 66.7 67.5 0.2  
13. AS3701 port-ptck-pe-02.net.linkoregon.org 0.0% 111 66.5 66.6 66.5 66.8 0.1  
14. AS3701 eugn-oh-pe-02.net.linkoregon.org 0.0% 111 69.2 69.3 69.2 69.9 0.1  
15. AS3701 noc-inside.eugn-oh-pe-02.net.linkoregon.org 0.0% 111 69.3 69.3 69.2 70.4 0.1  
16. AS3701 ns1.net.linkoregon.org 0.0% 111 69.5 69.4 69.2 70.4 0.2
```



THANK YOU!



QUESTIONS?