About Lumeta Traffic

Packet Rates

If you know you have a low-bandwidth link on your network and want to avoid taxing it, take advantage of Lumeta's packet rate control. This feature enables you to throttle a packet rate for an interface to the value you specify.

The recommended packet rate is between 500 and 5000.

The packet-rate pertains to the interface level (per interface, per system), which is to say the rate is per interface, not per collector.

To change an interface's packet rate, use the Lumeta command-line interface (CLI) command **`system interface packetrate <n>`** where <n> is some integer for the packet rate.

When the packet rate changes, the notifications at your Lumeta GUI (Settings > Notifications > System tab) will be COLLECTOR_UPDATED event with the descriptor "Interface Packet Rate Changed." To see the current packet rate in the CLI, use the `system interface list <iface>` command where <iface> is the name of the interface.

Scan Rates

Limit rescanning to a frequency appropriate to the type of discovery you are running. Recommended rescan (RI) intervals:

- Passive monitoring – Not Applicable
- Base rescan interval on size of network
- Criticality of fresh data
- Longest RI should be no more than 3X your shortest RI

Benefits of compliance:

- Smooth rescans
- Productive scanning
- Accommodates bandwidth constraints

Consequences of non-compliance:

- Scanning never stops
- Yields non-productive scanning

Communication

The communication among the Lumeta Command Center and one or more Lumeta Scouts is TLS/SSL-secured over port 443.

Protocols/Ports: HTTPS:443

Encryption & Authentication

Certificate Types

- Certificate Authority (CA) Cert
- Server Cert
- User Cert

Lumeta Authentication Methods

- Smart Card (CAC)
- User ID and Password
- SSH Key

Lumeta Encryption Methods

- Public Key Infrastructure (PKI)
- TLS/SSL 443 Levels

Encryption & Authentication Algorithms & Strength

- **Cryptographic Protocol:** TLS v 1.1 and 1.2
- **Ciphers, key strength in bold:** DHE-RSA-AES**256**-SHA, AES**256**-SHA, DHE-RSA-AES**192**-SHA, AES**192**-SHA, DHE-RSA-AES**128**-SHA, AES**128**-SHA

Bandwidth & Other Architectural Considerations

1. Does your network have perimeters to monitor?
2. Does your network have enclaves to secure from internal attacks?
3. Does your network have bandwidth limitations?
4. Do you want to gather broadcast information?
5. From which point will you have visibility into a zone?
6. From which point can you gain an “outside-in” perspective?
7. From which point can you service the requests of multiple collectors?

Bandwidth

Lumeta's Consumption of Bandwidth

Lumeta disperses/distributes packets during network scans so that bandwidth impact is negligible; Lumeta scans generally go unnoticed by IDSs.

Visibility & Perspective

- Outbound, from Scout - What can this Scout “see” from its outpost?
- Inbound, from Scout to Command Center - What can this Scout tell us

Scout Deployment Considerations

Recommended Deployment Areas:

- Place Scouts where there is maximum visibility.
- Place Scouts where there is maximum perspective.

Typical Deployment Areas:

- Deploy one Scout in Area 0 (i.e., OSPF) for passive listening.
- Place Scouts in remote network locations such as overseas.
- Place a Scout in cloud environments such as AWS.

about how our network is “seen” from a different location.

SSL/TLS 443 is required for Scout/Command Center connectivity.

- Scouts can connect to Command Centers
- Command Centers can connect to Scouts

Adjust firewalls before deploying Lumeta. Validate connectivity using your preferred troubleshooting tools.

- Validate SSL Access
- Test for SSH Access
- Ping test connectivity from your Command Center’s perspective, not from your workstation’s perspective. Browse to Settings > Support Tools > Ping Test.

To validate visibility and perspective . . .

1. Target the network where the Scout was deployed.
    a. Configure Target list to include local network
    b. Configure Target list to ensure visibility to remote networks
2. Assign additional Scout interfaces to organize visibility.

Adjusting Collector Configurations

If your scan has gone out-of-bounds—to a business affiliate’s network or the Internet . . .

- Adjust Maximum Hops – Path
- Adjust Discovery Space > Update the Stop or Avoid list
- Adjust your Eligible list

If discovery is taking longer than your rescan interval . . .

- Disable Trace to Hosts – Path
- Disable Trace Discovered Routes – Path

If the scan is encroaching on your business affiliate’s hosts . . .

1. Put affiliate’s CIDR in Stop list
2. Modify Eligible list
3. Disable Target Discovered Routes – Host

If you’re not finding all of your forwarding devices under management . . .

- Change CIDR Expansion – Path
- Make your expansion list more granular (e.g., change CIDR from /24 to /28)
- Make sure your SNMP credentials are set correctly

If your scan is taking too long . . .
•Skip BGP Routes – SNMP