Lumeta ESI

SOLUTION BRIEF

Lumeta ESI IPv6 Discovery

In today's globally distributed IT landscape it is becoming critical to identify and properly manage devices utilizing IPv6. With IPv6 infiltrating data centers and externally exposed devices such as smart phones, tablets, and POS systems it is essential to understand that networks are still open to the same vulnerabilities as IPv4 networks. There may also be even more at risk due to the fact that these IPv6 networks are not yet as widely patrolled and monitored.

IPv6 Benefits

The good news is that IPv6 has been built from the ground up with security in mind. Many security features that have been added after the fact or are deemed optional in IPv4 are integrated into IPv6 as fundamental requirements. IPv6 core security features include:

- IPv6 encrypts traffic and checks packet integrity to provide VPN-like protection for standard Internet traffic
- Internet Protocol Security (IPsec), which is optional in IPv4, is an integral and mandatory part of IPv6, making man-in-the-middle attacks much more difficult for hackers
- IPv6 simplifies and speeds up data transmission by handling packets more efficiently, and removing the need to check packet integrity
- The availability and abundance of global IPv6 addresses enables businesses to create specific services for targeted users and connected devices

IPv6 Challenges

While having a large number of IP addresses benefits organizations from an IT management point of view, it also creates exposure to cyber criminals and malicious devices. Not only will criminals be able to switch IP addresses frequently – making it difficult to track and trace them – but many existing security controls that rely on blacklisting malicious IP addresses will cease to be effective.

As a result, there is a potential to create security holes during the transition process. The most likely place for this to occur is in the creation of usage and security policies for IPv6. The lack of operational expertise also makes it more likely that an IT manager will inadvertently create a security hole while writing those new policies.

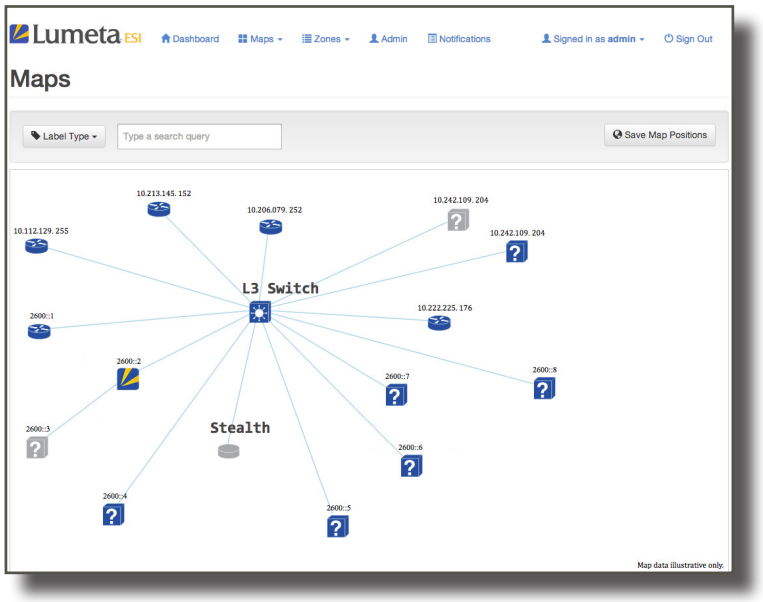
IT teams are also faced with public address management at a grand scale and must figure out how to prevent internal users from creating secure tunnels to the outside, which may create a corporate liability.

While the mandatory encryption of IPv6 traffic should reduce the seriousness of data breaches that occurs it also presents a challenge to government and commercial organizations who, once the transition to IPv6 is complete, will find their network traffic monitoring capabilities severely diminished.

Lumeta ESI IPv6 Solution

Lumeta ESI delivers foundational intelligence to power real-time network situational awareness of the entire enterprise. It automatically discovers and monitors the entire enterprise and creates comprehensive, detailed network topology maps – in real-time. ESI yields accurate network and device intelligence, while issuing alerts and notifications as the enterprise changes and evolves. This foundational intelligence is a critical underpinning for IPv6 network vulnerability management strategies to be truly effective.

Lumeta's IPv6 Discovery passively monitors ICMPv6/NDP traffic, as well as OSPF route/infrastructure updates providing a clear understanding of network paths and devices. This passive monitoring then allows for a highly targeted scan-based assessment of newly discovered IPv6 devices.



You can choose to toggle among IP address, system name, MAC address, and device type labels to quickly see all identifiers associated with a particular node. Its Search capability enables you to highlight map elements that meet your search criteria and its Save Map Positions button enables you to preserve a map with its elements positioned as you've defined.

ESI improves the quality of network provisioning, fault monitoring and service-level reporting/verification by using IPv6 Discovery to:

- Identify IPv6-enabled devices, both native and dual-stacked
- Find IPv6 routes and paths on the network
- Collect attributes of native IPv6 network equipment
- Deliver IPv6 discovery results in real-time
- Locate unwanted IPv6 devices and routes
- Identify unintentionally configured IPv6 devices
- Secure and manage policy-compliant IPv6 equipment

Vulnerability Management Integration

Most security products can't scan and discover the IPv6 address space because it is simply too large. These products support IPv6, but need to know the specific address in order to run a vulnerability scan on it. ESI enhances and feeds vulnerability scanners such to discover the unknown IPv6 addresses.

Doing this gives them the ability to:

- Identify and monitor IPv6 network connections and devices
- Understand all aspects of the IPv6 network environment – physical, mobile, virtualized, cloud (private, public and hybrid)
- Expose potential problems, such as unplanned IPv6 Internet connections, unmanaged devices and unsecured ports
- Monitor IPv6 networks in real-time for instant visibility – and quick response

Lumeta Corporation | 300 Atrium Drive, Suite 302 | Somerset, NJ 08873 USA | +1.732.357.3500 | www.lumeta.com