GARLAND TECHNOLOGY
See every bit, byte, and packet®

tenable®

Indentify Vulnerable Traffic with Tenable® and Garland Technology

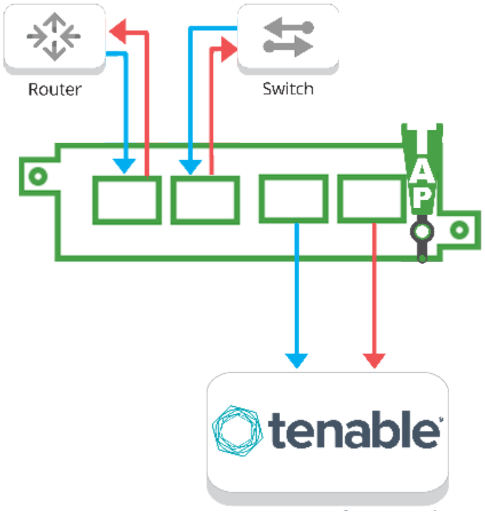
A Joint Solution from Tenable® and Garland Technology

Detect and Decrypt Deep Packet Traffic to the Edge of Your Network Infrastructure

When securing your network, obtaining useful data to reduce vulnerabilities is the epicenter of an infrastructure. Issues arise when encrypted packet level files are missed, so the importance of gaining 100% visibility in your network traffic helps to eliminate blind spots throughout the network. Since encrypted files are difficult to detect, complex security devices require active scanning and non-intrusive monitoring.

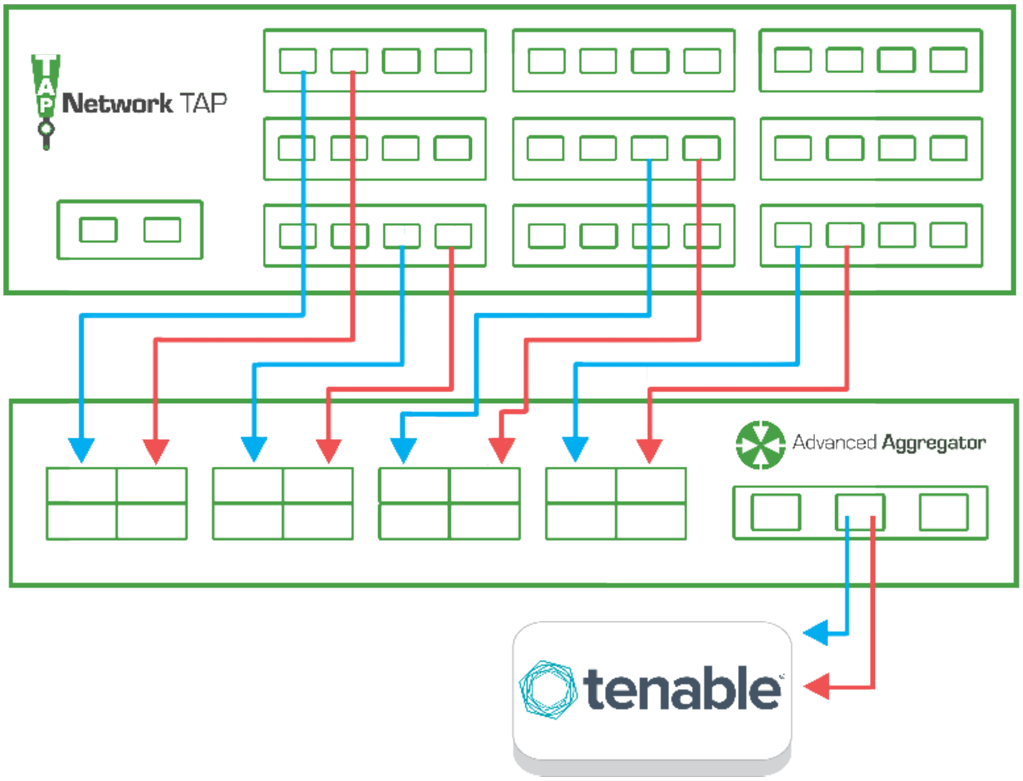
For optimal data collection and continuous visibility, Nessus Network Monitor and Garland Technology's Edgesafe™ Bypass Network TAP provide a fully comprehensive solution. The solution delivers a full platform of network access and completes active scanning and non-intrusive passive monitoring. At the edge, they provide a stream of visibility and continuous monitoring through encrypted traffic and deep packet inspection.

With 450 compliance and configured templates to audit against CIS benchmark and best practices, Nessus Network Monitor leads security vulnerability scanning for encrypted traffic. With Garland Technology creating visibility at the edge, this duo dynamically equips your network infastructure to see every packet.



Single Source Deployment for Monitoring Performance

Deploy the Garland Technology Edgesafe™ Bypass Network TAP to effectively create complete visibility by passing the data traffic into the Tenable® Nessus Network Monitor sensor. The sensor capture relevant data through de-duplication and advanced filtering techniques to create comprehensive DNS logs needed to detect vulnerabilities in the network. This seamless integration provides a sensor that filters data traffic from a single link to monitor small networks and network segments.



Scalable Security at the Perimeter of Your Network Infrastructure

A robust framework in a multi-network ecosystem supplies an impactful deployment to sensors across the entire network infrastructure, all the way to the edge. The data traffic is managed and monitored through Nessus Network Monitor, providing continuous complete visibility with the PacketMax™ Advanced Aggregator. The scalable modular solution allows for future growth with port efficiency and reducing overall cost per-port.

The Nessus Network Monitor connects to the network segment via a Network TAP to have a full, continuous view of network traffic providing the most optimal data collection. The network is tapped using Garland Technology's failsafe, Bypass TAP feeding multiple links into Garland's PacketMax™ Advanced Aggregator, which will take in links to load balance into the Nessus Network Monitor.

Garland Technology Network TAPs and Packet Brokers

Garland Technology provides a full platform of network access products including a range of network TAPs and Network Packet Broker devices, supporting the entire wire spectrum from 10/100M copper to 1G/10G/40G/100G.

Key Capabilities

- Complete network visibility by passing all live wire data
- Ensure no dropped packets for out-of-band tools
- Quality standard, all TAPs are tested with live network data and validated
- 100% failsafe packet capture – all network TAPs are tested and validated, and have built-in failsafe and/or heartbeat technology
- Reliable traffic aggregation, load balancing, and filtering – full control over traffic behavior and flexibility for aggregation and regeneration

Tenable's Cyber Exposure Platform

Cyber Exposure is an emerging discipline for managing and measuring cybersecurity risk in the digital era. Cyber Exposure transforms security from static and siloed visibility into cyber risk to dynamic and holistic visibility across the modern attack surface. Cyber Exposure translates raw vulnerability data into business insights to help security teams prioritize and focus remediation based on business risk. Cyber Exposure provides executives and boards of directors with a way to objectively measure cyber risk to help guide strategic decision making. Just as other functions have a system of record - including ITSM for IT and CRM for Sales - Cyber Exposure solutions will provide Security with a system of record to help them effectively manage and measure cyber risk.

Key Capabilities

- Live discovery of any digital asset across any computing environment
- Continuous visibility into where an asset is secure, or exposed, and to what extent
- Prioritization of remediation based on business risk
- Benchmarking of cyber exposure compared to industry peers and best in class organizations
- Measurement of cyber exposure as a key risk metric for strategic decision support.

About Tenable

Tenable®, Inc. is the Cyber Exposure company. Over 27,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 25 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

Have Questions? sales@garlandtechnology.com | +1 716.242.8500 | garlandtechnology.com

Garland Technology is an industry leader delivering network products and solutions for enterprises, service providers, and government agencies worldwide. Since 2010, Garland Technology has developed the industry's most reliable test access points (TAPs), enabling data centers to address IT challenges and gain complete network visibility. For more information, or learn more about the inventor of the first bypass TAP, visit GarlandTechnology.com or @GarlandTech.

GARLAND TECHNOLOGY

See every bit, byte, and packet®