Encrypted Traffic Visibility

10 Things to Ask Your Vendor

This checklist will help you formulate requirements when designing a packet broker network for encrypted traffic visibility and security monitoring. Because comprehensive visibility requires more than a single hardware or software product, we recommend you establish a set of criteria to clarify requirements for your security monitoring solution and to avoid any blind spots.

In order to ensure what you are considering meets your requirements, consider these questions:

1. Describe Your Solution for Passive and Active Inline Deployment.

Security solutions operate in passive (ex. IDS) out-of-band or active (ex. IPS, WAF) inline mode. Look for a solution supporting both configurations and is capable of performing both positive and negative health checks. Also consider what is required to make security system changes, or to install additional devices. Ensure that this can be done without taking the production network offline.

2. How Do You Ensure Your Architecture Does Not Slow the Production Network and Monitoring Tools?

Consider how network performance changes as security monitoring tools are added to the network. Look for a solution that does application level performance checks, so you can ensure that monitoring tools don't introduce unacceptable latency. The solution should also allow to set latency to trigger an action, such as routing around the tool or failing over to a redundant tool, to ensure that security does not become a bottleneck or a single point of failure.

3. Does Your Solution Support 1G, 10G, 40G and 100G Networks?

With digital transformation, enterprise networks are quickly migrating to 40G and 100G networks. Ensure the solution can support varying network speeds and traffic patterns without degrading network and security monitoring tool performance.

4. Describe Your Solutions Performance and Scalability?

SSL/TLS encryption and decryption require high computing resources. Most solutions do not scale well and become cost prohibitive for enterprise-wide security monitoring, resulting in security blind spots. Look for a solution that operates at line rate, required connections per second with broad set of cypher suites with linear scaling architecture.

5. How Do You Ensure Privacy and Policy Management?

SSL/TLS is used primarily to ensure end-to-end security between two end points. Decryption must not compromise the privacy expectations from secure connections. Look for a solution that provides easy-to-use policy management and configuration to ensure security posture is maintained between the end points. Look for the ability to select what traffic is decrypted or bypassed and that no personal data is visible to security monitoring tools in clear text.

6. Does Your Solution Support All Protocols and Applications?

SSL/TLS is predominantly used by HTTPS but there are many other protocols such as SMTP, FTP, SIPS and custom applications leverage SSL/TLS for secure communications. These applications could also operate on any TCP port. Ask your provider to ensure their solution can automatically identify and decrypt traffic across all protocols and applications.

7. Does Your Solution Support All SSL/TLS Versions and Cipher Suites?

There are several versions of TLS with TLS 1.1 and 1.2 being used widely. TLS 1.3 has been recently introduced for greater security; many organizations are migrating to it. Additionally, there are many cipher suites available for encryption and enterprises select a subset of cipher suites to implement in their systems. Look for a solution that has a broader cipher suite and TLS 1.0-1.3 and SSL 3.0 support.

8. Does Your Solution Provide High-Availability and Failover Mechanisms?

Security systems are usually deployed in passive (out-of-band) or active (inline) mode. It is imperative that decryption solutions are highly available to ensure continuous security monitoring and uninterrupted network connectivity. It is even more critical for inline deployments where any failure will disrupt network connectivity. Inline security tools may also become inoperable or slow down due to traffic load causing network connectivity outages or performance degradation. Ensure solution supports high availability, fail-safe mechanisms and health checks with bypass to meet expected SLAs.

9. Describe Your Company's Visibility Product Suite.

Decryption is one component that makes up security and service monitoring solutions. Decrypting traffic blindly, without knowing how the clear traffic is used by security and service monitoring tools unnecessarily increase security risks and costs. Ensure the solution provider has a broad understanding of enterprise security and service monitoring needs and offers a comprehensive portfolio. This would help avoid vendor finger pointing and achieve best end-to-end experience.

10. Describe Your Company's Customer Support Services.

A product's value is greatly diminished without adequate support, maintenance, and continuous innovation to address changing customer needs. Solution architecture design, deployment, and on-going support are essential for any successful implementation. Look for a vendor with world-class support services across your operating regions, R&D investments, and technology innovations.

NETSCOUT Solution for Encrypted Traffic Visibility

Key Capabilities

Passive and active deployment configuration

- All applications and protocols with automatic identification of SSL/TLS traffic
- SSH3.0, TLS 1.0-1.3 including hundreds of cipher suites
- Decrypt once and feed many security monitoring tools
- Supports unlimited network segments

Privacy and Policy Management

- Policy based decryption with granular filters and action rules to drop, reject and bypass
- Flexible policy management with support for common names, SAN, SNI, ALPN, TLS version
- Mask confidential or private data for HIPPA, PCI and other regulatory compliance

High performance, scalability and availability

- Line rate 20G and 40G performance and horizontal scalability
- More than 2 million simultaneous connections with 40,000 new connections per second
- Health and latency checks of active inline tools
- Power safe bypass protection for uninterrupted network connectivity

Easy Management and Operations Console

- System administration with configurable access privileges
- Detail logs for system access, performance and system load with configurable alerts and notifications
- Comprehensive decryption/re-encryption logs with certificate, protocol and cipher suite details and fast log search queries

About NETSCOUT nGenius Decryption Appliance

NETSCOUT® nGenius® Decryption Appliance enables visibility into encrypted traffic for pervasive, high-performance security monitoring with policy management for privacy. nGenius Decryption Appliance decrypts traffic flows from the network to the security systems and monitoring tools. Our customers use nGenius Decryption Appliance to enhance both their service assurance platform and cybersecurity deployments so that they can gain visibility into encrypted traffic, increase security monitoring tool performance, and reduce total cost of security monitoring tools.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

© 2020 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, Arbor Networks, the Arbor Networks logo, ATLAS, InfiniStream, InfiniStreamNG, nGenius, and nGeniusONE are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. Third-party trademarks mentioned are the property of their respective owners.