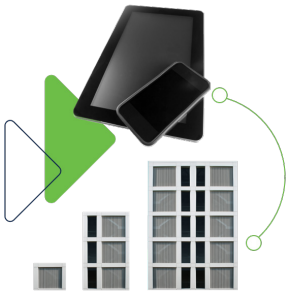
CISCO
SECURE

White Paper
Cisco Public

Extending Zero Trust to the Network Through Visibility and Security Analytics

Continuous network traffic monitoring with Cisco Secure Network Analytics to detect malicious behavior and take dynamic policy decisions

Table of Contents



The challenge

The need for Zero Trust has stemmed from the modern enterprise challenges surrounding the increasing network complexity as well as the evolving threat landscape. The move to the cloud, users accessing the network from any location and any device, rise in encrypted traffic and the growing number of Internet of Things (IoT) have blurred the lines around the traditional network perimeter. At the same time, attacker tactics are evolving such as logging into the network with compromised credentials versus breaking in, being motivated to persist within the network versus stealing data and getting out and hiding malware in encrypted traffic.

The role of visibility and security analytics within a Zero Trust network

Forrester has stated that the network is one of the key components of the Zero Trust eXtended (ZTX) Ecosystem[2]. And that a main tenet of any secure network has always been increased visibility. The report further highlights the importance of deploying a Network Analysis and Visibility (NAV) tool to implement a Zero Trust network. These solutions, also categorized as Network Traffic Analysis (NTA) or Network Detection and Response (NDR), provide the ability to detect any kind of malicious activity using network traffic for faster threat detection and response.

Cisco Secure Network Analytics (formerly Stealthwatch) is one such solution, that provides enterprise-wide visibility, from the private network to the public cloud by collecting network telemetry. It then applies advanced security analytics in the form of behavioral modeling and machine learning to pinpoint anomalies and further reduce them to critical alerts in order to detect advanced threats in real-time. With a single, agentless solution, you get comprehensive threat monitoring, even in encrypted traffic.

Secure Network Analytics was designed with the ideology of continuously verifying all network activity, regardless of location, to ensure it's "normal", so that any anomalous activity could be detected immediately in case of a compromise. Following are some more details on how the solution is implemented to extend Zero Trust to the network.

What is Zero Trust?

Zero Trust is an approach to help achieve more pragmatic security for today's world. It is a security architecture and enterprise methodology, not a technology or tool, designed to effectively orchestrate today's challenging combination of technologies, practices and policies. It represents an evolution in our approach to security, focused on delivering a comprehensive, interoperable, holistic solution approach that integrates multiple vendors' products and services.

A Zero Trust Architectural Framework involves restricting access to system, application and data resources to those users and devices that are specifically validated as needing access. It will then continuously authenticate their identity and security posture to ensure proper authorization for each resource to provide continued, ongoing access[1]

Contextual network-wide visibility

Secure Network Analytics is able to ingest and analyze telemetry from network devices such as routers, switches and firewalls. It can also natively collect telemetry from the public cloud infrastructure. Secure Network Analytics uses **entity modeling** to classify all the devices or entities connected to the network such as servers, printers, etc. to efficiently determine normal behavior of these entities so it can alarm on any anomalies. Another unique capability of Secure Network Analytics is that it stitches traffic flows following asymmetric paths through the network together, to represent the client-server communication. This means that Secure Network Analytics can not only detect a threat, but provide **additional contextual information** about the source of the threat, like where else it might have propagated laterally, which user has been compromised, and provide other information such as location, device type, timestamp, etc. Secure Network Analytics can also store telemetry for a certain period of time to forensically investigate past or long-running events. In addition to network telemetry, Secure Network Analytics integrates with other solutions to infuse user and application data, web information, etc. for faster threat investigation and response.

Predictive threat analytics

Attackers use multiple methods to compromise your security so why should you employ just one defense technique? Secure Network Analytics uses a three-pronged approach to detect advanced threats before they turn into a high impact incident:

- The first is **behavioral modeling**. Secure Network Analytics constantly observes network activities to create a baseline of normal behavior, and alarms on any anomalies using close to 100 different heuristics. It also has knowledge of known bad behavior that it alarms on. So, if attackers are using lost or stolen credentials to gain access, or if you are dealing with a malicious employee involved in hoarding or exfiltrating sensitive data, Secure Network Analytics can alert on it right away. **That is why it is necessary to continuously verify network activity, even after proper access has been granted.**
- Secondly, Secure Network Analytics applies a funnel of **machine learning** techniques to reduce large amount of telemetry to anomalies, to eventually high-fidelity threat detections. So, your security team can now focus on investigating critical threats. This cloud-based machine learning engine can also determine malicious servers across the world and flags any communication to these, in order to detect unknown or targeted attacks.
- And lastly, Secure Network Analytics uses **global threat intelligence** powered by the industry-leading Cisco Talos platform to correlate local threats globally, and thwart attackers' rinse-and-repeat tactics of infecting multiple victims with the same malware. All these analytical techniques work together to identify early indicators of compromise like constant pinging/beaconing, port scanning, communications to malicious domains.

Analyzing encrypted traffic

The rapid rise in encrypted traffic is changing the threat landscape. With more than 80% of the web traffic being encrypted today, this leaves a huge blind spot for the organizations. Today, most technologies rely on decryption-based monitoring, but this method is not only time and resource intensive, but also compromises data privacy and security.

NIST recently released a draft publication, SP 800-207: Zero Trust Architecture (ZTA)[3], an overview of a new approach to network security. NIST also recognizes that in ZTA, all traffic should be inspected, logged and analyzed to identify and respond to network attacks against the enterprise. But some enterprise network traffic may be difficult to monitor, as it comes from third-party systems or applications that cannot be examined due to encrypted traffic.

In this situation, NIST recommends collecting encrypted traffic metadata and analyzing it to detect malware or attackers on the network. It also references Cisco's research on machine learning techniques for encrypted traffic (section 5.4, page 22).

Cisco encrypted traffic analytics was developed using the same Cisco research, wherein Secure Network Analytics ingests enhanced metadata and analyzes it to detect threats in encrypted traffic and also ensure cryptographic compliance, without any decryption.

Simplifying segmentation and policy monitoring

With the visibility provided by Secure Network Analytics into all communications occurring within and outside the organization, smarter policies can be created without disrupting critical mission workflows. Also, custom security alerts can be created within Secure Network Analytics to trigger when these policies are violated. For example, if a guest user tries to access a sensitive data server, or traffic is seen flowing to a country marked as suspicious by the organization. In this way, organizations can ensure that the security policies they have set in other tools are actually working. And lastly, through the integration with Cisco Identity Services Engine (ISE), Secure Network Analytics can set the appropriate policy on the suspicious device based on the severity of the threat, in order to contain the threat immediately.

Cisco Zero Trust

Cisco Zero Trust provides a comprehensive approach to securing all access across your applications and environment, from any user, device and location. It protects your workforce, workloads and workplace.

Cisco was recently named a leader in The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q4 2019 – read the report to learn more about our position as a leader.

"The enterprise can collect metadata about the encrypted traffic and use that to detect possible malware communicating on the network or an active attacker. Machine learning techniques [Anderson] can be used to analyze traffic that cannot be decrypted and examined. Employing this type of machine learning would allow the enterprise to categorize traffic as valid or possibly malicious and subject to remediation."

Conclusion

Knowing who is connected to the network and what they are doing in order to detect malicious behavior immediately is an important component of implementing Zero Trust for the network.

Cisco Secure Network Analytics can help organizations implement this in a simple and scalable manner by ingesting network telemetry and analyzing it to generate high-fidelity critical alerts, without the need to deploy any sensors or probes.

Next steps:

Get started on your journey to extend Zero Trust to the network. Sign up for a free 2-week visibility assessment today!

Learn more at:

Cisco Secure Network Analytics

Sources: 1. White paper: Zero Trust 101

2. Forrester report "The Zero Trust eXtended (ZTX) Ecosystem: Networks"

3. Draft (2nd) NIST Special Publication 800-207: Zero Trust Architecture