White paper

Cisco Stealthwatch Cloud: Private Network Monitoring

Performance Metrics for Stealthwatch Cloud Sensor

Introduction

Cisco Stealthwatch Cloud improves security and incident response across the distributed network – from the private network and branch office to the public cloud. Providing comprehensive visibility and high-precision alerts with low noise, Stealthwatch Cloud enables organizations to accurately detect threats in real time, regardless of whether an attack is taking place on the network, in the cloud, or across both environments. Stealthwatch Cloud is a cloud-based, Software-as-a-Service (SaaS)-delivered solution, detecting ransomware and other malware, data exfiltration, network vulnerabilities, and role changes that indicate compromise.

Stealthwatch Cloud consists of two primary offerings: **Public Cloud Monitoring and Private Network Monitoring.**

Public Cloud Monitoring can be used in combination with Private Network Monitoring or Cisco Stealthwatch Enterprise (on-premises appliance-based version of Stealthwatch) to provide visibility and threat detection across the entire network, such as AWS, GCP, and Microsoft Azure infrastructures. It is a cloud-delivered, and truly cloud-native solution that can be deployed easily and quickly.

Cisco Stealthwatch Cloud Private Network Monitoring provides visibility and threat detection for the on-premises network, delivered from a cloud-based SaaS solution. It is the perfect solution for organizations that want better awareness and security within their on-premises environments while reducing capital expenditure and operational overhead. It works by deploying a lightweight appliance, referred to as the Stealthwatch Cloud Sensor, in a virtual machine or server that can consume a variety of native sources of telemetry or extract metadata from network packet flow. It encrypts this metadata and sends it to the Stealthwatch Cloud analytics platform for analysis. Stealthwatch Cloud consumes metadata only. The packet payloads are never retained or transferred outside the network.

In this document, validated performance metrics for the Stealthwatch Cloud Sensor are presented.

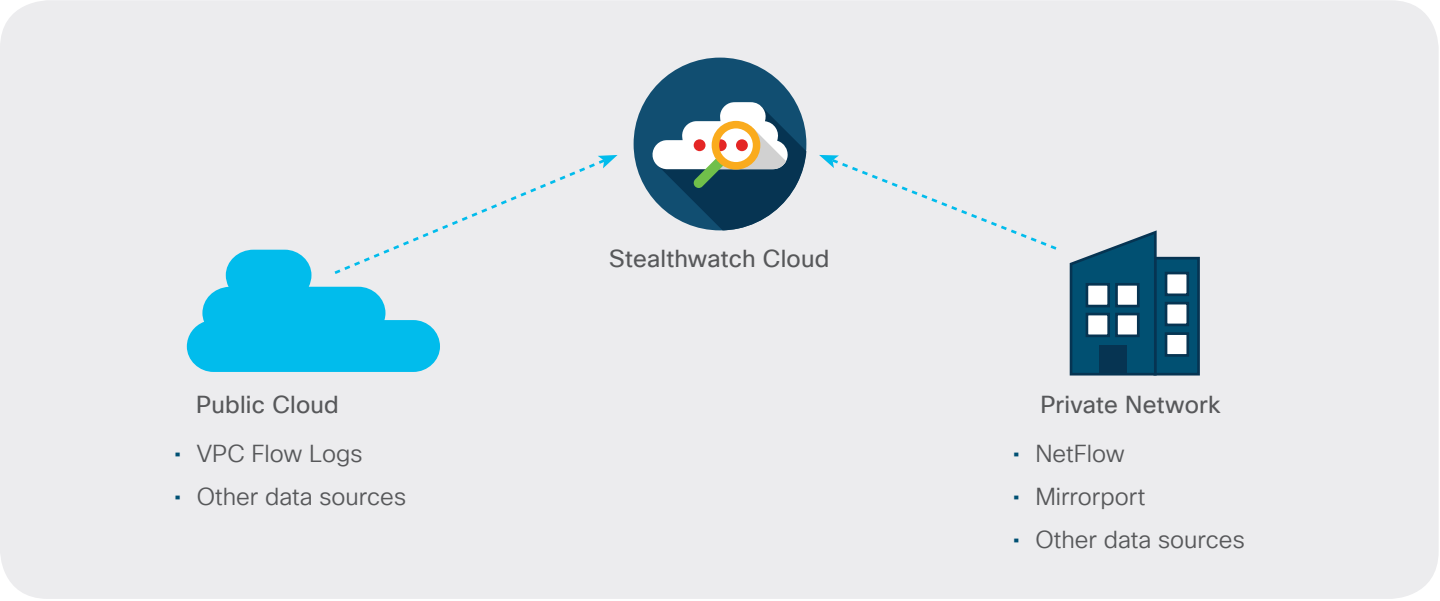

Figure 1. Stealthwatch Cloud monitors cloud as well as private network environments

Deployment Modes

The Stealthwatch Cloud Sensor has two major deployment modes, which are not mutually exclusive:

1. Processing metadata out of a raw traffic flow (ex. SPAN or network TAP)
2. Processing metadata out of NetFlow/IPFIX records

Under test conditions, the two deployment scenarios were tested individually to understand expected behavior. However, it is possible to do both functions simultaneously.

Stealthwatch Cloud Sensor for Private Network Monitoring

In order to monitor on-premises networks, a Stealthwatch Cloud Sensor appliance will need to be installed. This appliance can be installed either as a physical appliance or as a virtual machine leveraging the ISO or OVF distributions. Conceptually, the figure below illustrates the deployment scenario of the Stealthwatch Cloud Sensor, where the on-premises sensor collects telemetry and forwards metadata to the customer's Stealthwatch Cloud instance through an encrypted private tunnel.

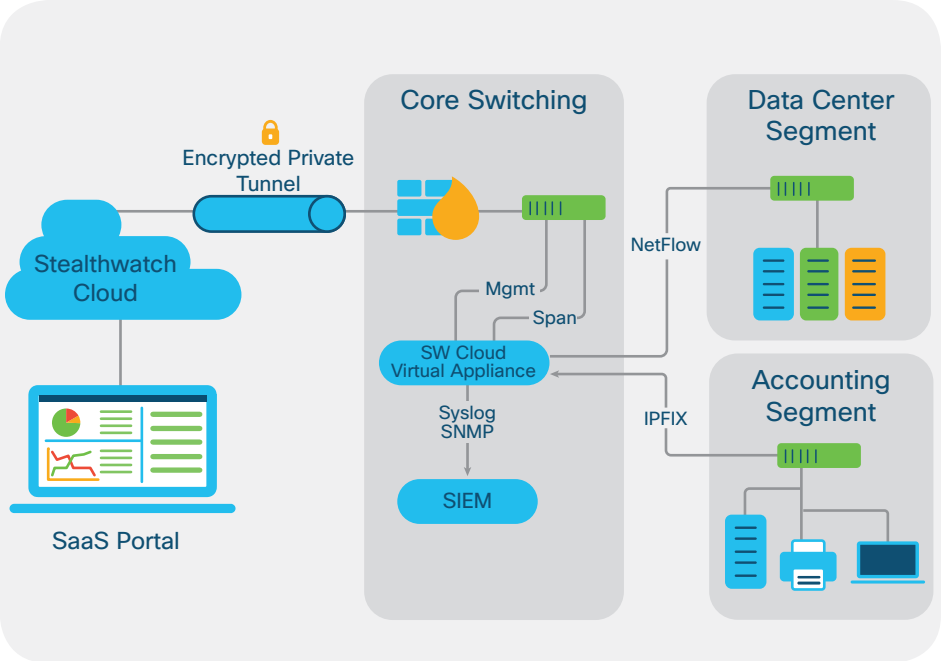

Figure 2. Private Network Monitoring virtual sensor deployment overview

The Stealthwatch Cloud sensor is included in the Stealthwatch Cloud service. Users can download the sensor ISO directly from their customer portal or alternatively the sensor image, which is based on ubuntu Linux, source code and alternative deployment options are available at this URL: https://github.com/obsrvbl/ona.

The Stealthwatch Cloud Sensor can be deployed and configured by following the instruction in Stealthwatch Cloud Sensor Installation Guide: https://ebooks.cisco.com/story/swc-sensor-install

With the distribution of the Stealthwatch Cloud Sensor as an ISO or Linux packages there is a variety of platforms and options, including a Raspberry Pi, where the sensor can be deployed. Given the variety of deployment Under

test conditions, the two deployment scenarios were tested individually to understand expected behavior. However, it is possible to do both functions simultaneously.

The table below illustrates the results of a set of tests against specific configurations of a virtual Stealthwatch Cloud Sensor, identified by the Config ID number, where the number of virtual CPUs, RAM and allocated disk space was varied, and the performance was observed in terms of NetFlow records collected per second.

Sensor Config ID	vCPU	RAM (GB)	Disk (GB)	Interfaces	Flow Record Collection Rate (Flows per Second FPS)
SWCS-1	2	2	32	1 Gbps Mgmt & NetFlow	80,000
SWCS-2	3	8	32	1 Gbps Mgmt & NetFlow	520,000
SWCS-3	4	32	32	1 Gbps Mgmt & NetFlow	523,000

In the above configurations, steady load of the Stealthwatch Cloud Sensor was observed in all configurations, meaning that the observed flow collection rate can be assumed to be held indefinitely. As can be seen between the observations of SWCS-2 and SWCS-3 configurations, increasing the virtual CPU and RAM configurations does not significantly increase the flow record collection rate and as a result the optimal configuration for NetFlow collection is SWCS-2.

Under a separate round of tests, illustrated in the tables below, the same configurations of a virtual Stealthwatch Cloud Sensor were tested processing raw network traffic, and performance rate was observed for those configurations. In the first table, tests were performed using small packets, where the average packet size was 140 bytes and in the second table larger packets, that were an average of 1400 bytes were used. It is also important to note that in the configurations below, PCI passthrough was enabled for both virtual machine configurations.

Raw network traffic performance metrics for Stealthwatch Cloud Sensor with small packets:

Sensor Config ID	vCPU	RAM (GB)	Disk (GB)	Interfaces	Data Rate (Mbps)	Packet Rate (Packets per Second PPS)
SWCS-1	2	2	32	1 Gbps Mgmt 1 Gbps monitoring	2,500	2,200,000
SWCS-3	4	32	32	1 Gbps Mgmt 1 Gbps monitoring	2,500	2,200,000

Raw network traffic performance metrics for Stealthwatch Cloud Sensor with large packets:

Sensor Config ID	vCPU	RAM (GB)	Disk (GB)	Interfaces	Data Rate (Mbps)	Packet Rate (Packets per Second PPS)
SWCS-1	2	2	32	1 Gbps Mgmt 1 Gbps monitoring	9,400	2,200
SWCS-3	4	32	32	1 Gbps Mgmt 1 Gbps monitoring	9,650	2,200

In the above configurations, as in the earlier tests, steady load of the Stealthwatch Cloud Sensor was observed in all configurations, meaning that the observed flow collection rate can be assumed to be held indefinitely. In the SWCS-3 configuration in both the tables above, the primary limitation was the data rate in the input interface.

Summary

Due to its multitude of distribution and deployment methods, the Cisco Stealthwatch Cloud Sensor has a variety of configuration options that can result in varying performance metrics. This document presented a summary of extensive testing against some of those configurations to provide guidelines to baseline performance expectations.

The optimal configuration, for both the collection of raw network traffic and NetFlow is for the Stealthwatch Cloud Sensor to have at least four (4) virtual CPUs and 32 GB RAM and it was found that resources beyond that amount did not demonstrate any measurable increase in performance.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at http://www.cisco.com/go/offices.