



Stealthwatch Endpoint Concentrator

Extending network visibility to the Endpoint

Cisco AnyConnect Network Visibility Module

Enhanced Endpoints
Context



Collector & Reporting
Cisco / Partners



ENHANCE NETFLOW RECORDS WITH ENDPOINT/USER DATA WITH
APPLICATION ACTIVITY

VISIBILITY



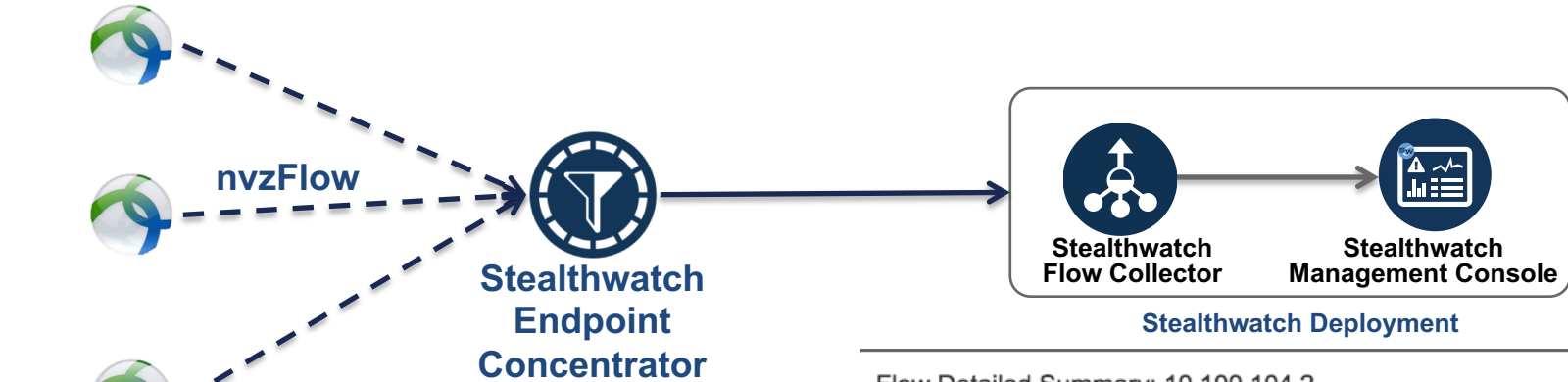
AUDITING



ANALYTICS



Stealthwatch Endpoint Visibility Solution



AnyConnect
with Network
Visibility
Module

Attributing a flow to:

- Process name
- Process hash
- Process account
- Parent process name
- Parent process hash
- Parent process account

Flow Detailed Summary: 10.100.104.2

Search Subject Details

Packets: 1.25K
Packet Rate: 416pps
Bytes: 1.74MB
Byte Rate: 607.51Kbps
Percent Transfer: 100%
Host Groups: Catch All
TrustSec Name: Group 1
TrustSec SGT: 27

Totals

Packets: 1.25K
Packet Rate: 416pps
Bytes: 1.74MB
Byte Rate: 607.51Kbps
Search Subject/Peer Ratio: all search
subject
RTT: 0s
SRT: 0s

Peer Details

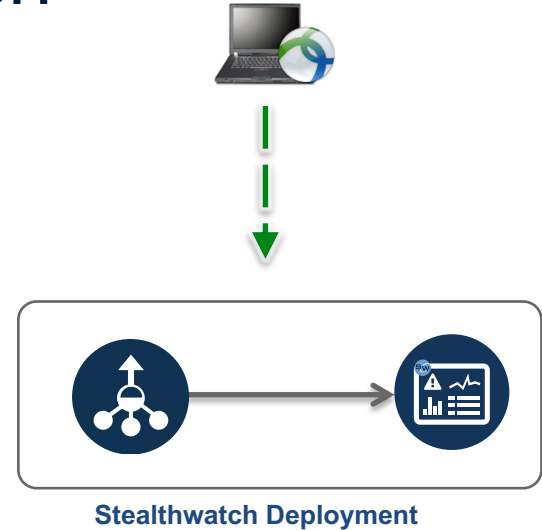
Packets: 0
Packet Rate: 0pps
Bytes: 0B
Byte Rate: 0bps
Percent Transfer: 0%
Host Groups: Catch
All
TrustSec Name: Group 2
TrustSec SGT: 52

Process name: malware.exe
File SHA Hash: 6ca13d52ca70c883e0f0bb101e425a89e8624de51db2d2392593af6a84118090

AnyConnect NVM & Stealthwatch

nvzFlow differs from traditional IPFIX:

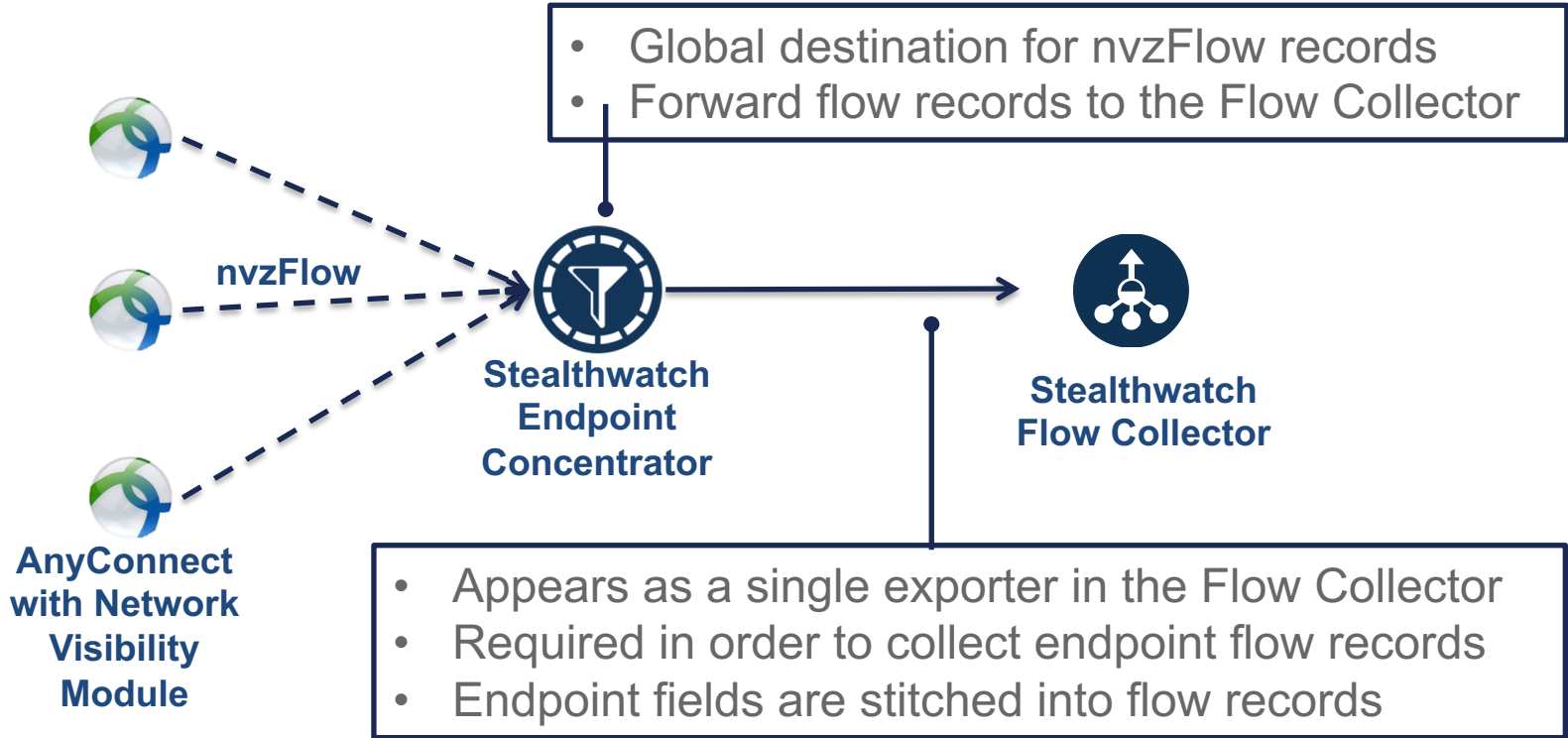
- Records are bi-directional
- Records produced only at end of flow
- Records created when client only
- No packet counts
- Byte counts are Layer 4 counts
- IP Address represents local network



Implications to Stealthwatch:

- Each endpoint is an exporter
- End of flow impacts “near real-time” analysis
- Lack of packet counts impact multiple algorithms
- “local network” address not relevant to enterprise
- Not all host transactions captured (only client)

Introducing the Endpoint Concentrator



Deployment Model 1: Trusted Network

Client with AnyConnect NVM



NetFlow-Enabled Network Device



Server



nvzFlow records sent to Endpoint Concentrator when Trusted Network Detected



Stealthwatch Endpoint Concentrator

NetFlow from Network devices



Stealthwatch Flow Collector

Per-User License Applied at the SMC



Stealthwatch Management Console

Endpoint flow records are sent to the Flow Collector

Endpoint fields are stitched into the conversational flow record

Deployment Model 2: Full Tunnel VPN

Client with AnyConnect NVM



ASA



Server



nvzFlow records sent to Endpoint Concentrator

NSEL from ASA

Per-User License Applied at the SMC

Stealthwatch Endpoint Concentrator

Stealthwatch Flow Collector

Stealthwatch Management Console

Endpoint flow records are sent to the Flow Collector

Endpoint fields are stitched into the conversational flow record

Attributing Activity to a Process

Process and file details associated with the communication to Known C&C Server:

- Process Name
- File Hash
- Parent Process Name
- Parent File Hash

Flow Detailed Summary: 10.100.10.131

Search Subject Details

Packets:
4
Packet Rate:
0.01pps
Bytes:
1.38KB
Byte Rate:
5.23bps
Percent Transfer:
0.44%
NAT:
128.107.78.50
Host Groups:
Main Campus VPN

Totals

Packets:
762
Packet Rate:
2.81pps
Bytes:
312.84KB
Byte Rate:
1.18Kbps
Subject Byte Ratio:
0.44%
RTT:
0s
SRTT:
0s

Peer Details

Packets:
758
Packet Rate:
2.8pps
Bytes:
311.46KB
Byte Rate:
1.18Kbps
Percent Transfer:
99.56%
Host Groups:
United States

Process Name:

taskhost.exe

File Hash:

473866333D2241BAD6918D21EBCBE8F8EEA9344D816788
300BCA290A89FBD3DD

Parent Process Name:

services.exe

Parent File Hash:

8EA41124A4E97732C5DAA616457FBA7111CB38986F3427F
A776ED00BC1407171

Endpoint Concentrator Specifications

DESCRIPTION	PID	Memory	vCPU	Max Users	Max Endpoints	Max Flows Per Second Output
Endpoint Concentrator VE	L-ST-EP	8GB	2	8,888	13,333	20,000
Endpoint Concentrator 1010	Coming Soon					

Endpoint Concentrator

These are the requirements for the Endpoint Concentrator 1000:

Reserved CPU	Reserved Memory	Maximum FPS Rate
2	8 GB	20,000



The capacity of your Flow Collector should be taken into consideration in determining the number of Endpoint Concentrators needed for your deployment.

SWCAT-Security-V5-m			
L-ST-EP-LIC=	3 days	0.00	1 +
Cisco Stealthwatch Endpoint License			
L-SW-SCA-K9 CP	3 days	1,683.00	1 +
Cisco Stealthwatch Learning Network Virtual Manager Software			

Endpoint License: Term Based Licenses

DESCRIPTION	1 Year License	3 Year License	5 Year License
Cisco Stealthwatch Endpoint License 1 - 99 Hosts	L-ST-EP-1Y-S1	L-ST-EP-3Y-S1	L-ST-EP-3Y-S1
Cisco Stealthwatch Endpoint License 100 - 249 Hosts	L-ST-EP-1Y-S2	L-ST-EP-3Y-S2	L-ST-EP-3Y-S2
Cisco Stealthwatch Endpoint License 250 - 499 Hosts	L-ST-EP-1Y-S3	L-ST-EP-3Y-S3	L-ST-EP-3Y-S3
Cisco Stealthwatch Endpoint License 500 - 999 Hosts	L-ST-EP-1Y-S4	L-ST-EP-3Y-S4	L-ST-EP-3Y-S4
Cisco Stealthwatch Endpoint License 1,000 – 2,999 Hosts	L-ST-EP-1Y-S5	L-ST-EP-3Y-S5	L-ST-EP-3Y-S5
Cisco Stealthwatch Endpoint License 2,500 – 4,999 Hosts	L-ST-EP-1Y-S6	L-ST-EP-3Y-S6	L-ST-EP-3Y-S6
Cisco Stealthwatch Endpoint License 5,000 – 9,999 Hosts	L-ST-EP-1Y-S7	L-ST-EP-3Y-S7	L-ST-EP-3Y-S7
Cisco Stealthwatch Endpoint License 10,000 – 24,999 Hosts	L-ST-EP-1Y-S8	L-ST-EP-3Y-S8	L-ST-EP-3Y-S8
Cisco Stealthwatch Endpoint License 25,000 - 49,999 Hosts	L-ST-EP-1Y-S9	L-ST-EP-3Y-S9	L-ST-EP-3Y-S9
Cisco Stealthwatch Endpoint License 50,000 – 99,999 Hosts	L-ST-EP-1Y-S10	L-ST-EP-3Y-S10	L-ST-EP-3Y-S10
Cisco Stealthwatch Endpoint License 100,000 – 249,999 Hosts	L-ST-EP-1Y-S11	L-ST-EP-3Y-S11	L-ST-EP-3Y-S11

Spare License – L-ST-EP-LIC=

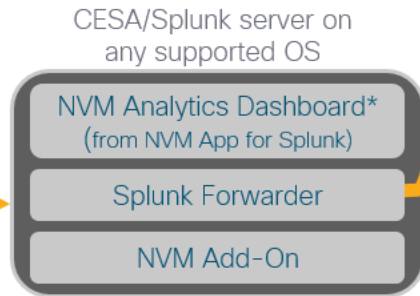
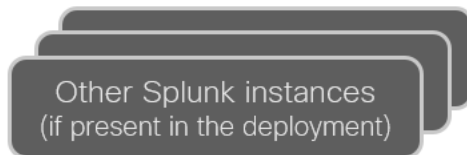
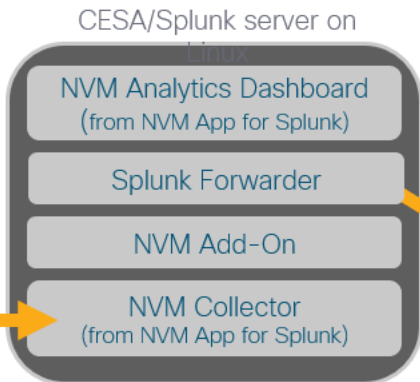
Deployment Architecture

“Integrated Collector”
Option
(when Splunk server is on Linux)



Telemetry
Generated by
AnyConnect NVM

“Separate Collector”
Option
(when Splunk server is not on Linux
or large scale Splunk deployment)



*Analytics Dashboard may also be loaded on a separate server

Cisco Confidential