



Cisco Systems Digital Network Architecture
VS
HPE/Aruba Mobile-First Campus



DR170402F

April 2017

Miercom
www.miercom.com

Contents

1 - Executive Summary	3
2 – Product Overview	4
Cisco Software	5
HPE Aruba Software	6
3 – Resilient Network Infrastructure	8
Stacking Technologies.....	8
Configuration Observations.....	9
Test Set-up	10
Results.....	13
Resilient Network Infrastructure Summary.....	14
4 - Simplified Network Operations.....	15
Cisco Quality of Service (QoS) using EasyQoS	15
HPE-Aruba SDN Applications	16
Feature Comparison	16
HPE-Aruba VAN Controller Applications	19
Results.....	20
Simplified Network Operation Summary	20
5 - Network Infrastructure Security (Traffic Analysis)	21
Cisco vs HPE-Aruba Traffic-Analysis Technology	21
Making the pieces work together	22
Threats From Within	23
Network as an Enforcer.....	24
Network Infrastructure Security Summary	25
6 - Summary.....	26
7 - About Miercom Performance Verified Testing	27
8 - About Miercom	27
9 - Use of This Report	27

1 - Executive Summary

Miercom was engaged by Cisco Systems to independently configure, operate and then assess aspects of competitive campus-network infrastructures from Cisco Systems and from Hewlett Packard Enterprise (HPE). The goal was to assemble the products of each vendor strictly according to their recommended designs, and using their respective software for campus-wide network management, control, configuration and monitoring.

Tests were conducted in three areas:

1. Resiliency, focusing on competitive architecture robustness
2. Simplifying operations, such as network-wide QoS deployment, and
3. Security, including traffic analysis for threat detection and mitigation

Key Findings and Observations:

- **Full data capture.** With a custom ASIC and using NetFlow, 100 percent of Cisco network data can be captured, with no impact on switch forwarding performance. HPE-Aruba products use a sampling technique, and can capture no more than 2 percent of packets for analysis.
- **Faster failure recovery.** Cisco modular stacking recovered from every failure scenario in less than one second, with no impact on application traffic. HPE-Aruba recovery took up to 120 seconds; almost all connections dropped and had to be re-established.
- **Policy Automation.** Cisco EasyQoS has built-in best-practice QoS policies, supports over 1,300 applications for policy control, and can apply policies end-to-end across the entire network, including switching, routing and wireless. Most details are handled automatically under the covers. HPE-Aruba's network configuration through HPE VAN and Network Optimizer application handles wired devices only; requires a separate application for wireless devices; marks traffic only at edge devices.
- **Solid security.** Cisco StealthWatch and other tools deliver granular traffic analysis, use the network as both a security sensor and enforcer, provide a complete solution to identify threats and anomalies and take immediate action to secure the entire campus network.

Based on the results of our testing and analysis, comparing the campus-wide network architectures and wares of Cisco and HP Enterprise, we proudly award the **Miercom Performance Verified Certification** to Cisco's campus network designs and related packages for monitoring, management and control.

Robert Smithers

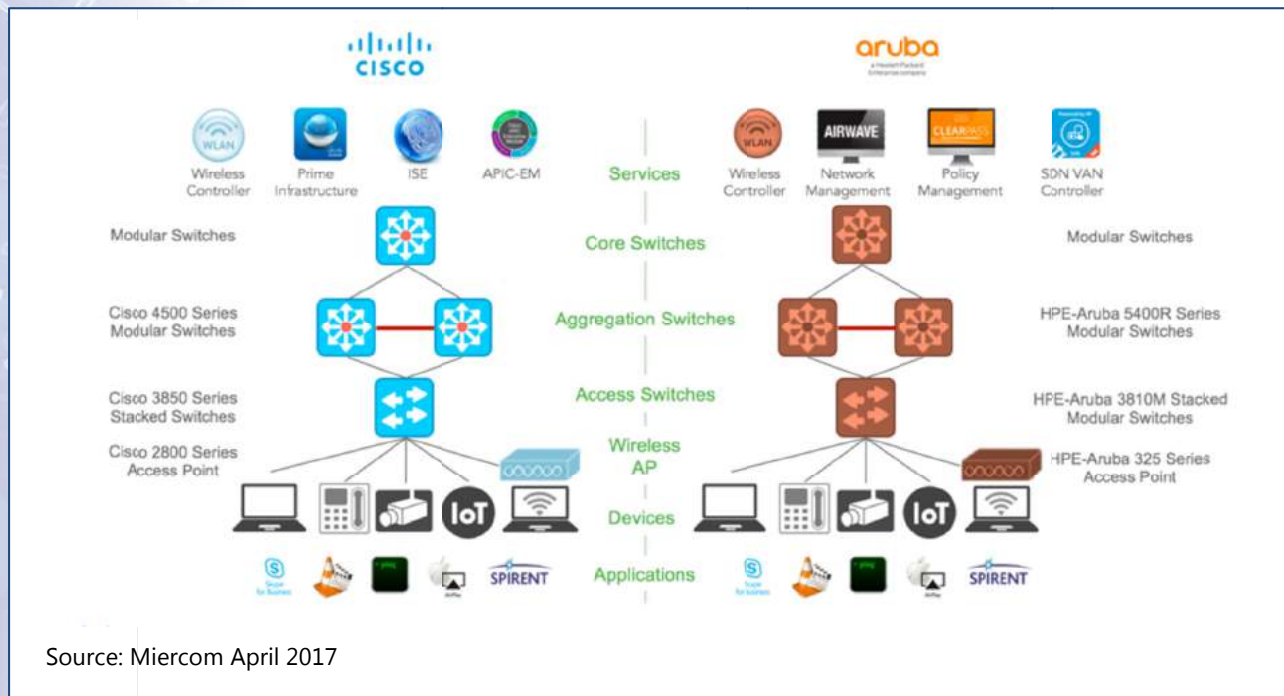
CEO
Miercom



2 – Product Overview

Two model campus networks were assembled for this testing. Miercom engineers ensured that the competitive campus topologies, all the products and their configurations, represented the latest and most appropriate apples-to-apples offerings from both Cisco Systems and HPE-Aruba, including the products from HPE's acquisition of Aruba Networks in 2015. The graphic below summarizes the key components from both vendors. All are discussed in more detail later in this report.

The Big Picture: Comparable Campus-Network Components Tested



The campus networks we built and tested featured three-tier architectures – appropriate for a campus-wide network infrastructure. Each consisted of: an access layer, for both wired and wireless devices; an aggregation level featuring resiliency and survivable switch redundancy; and a resilient core switching level.

A Spirent SPT-N11U Mainframe Chassis, with test modules running version 4.67 code, was employed for the generation of test traffic.

The latest publically available software versions for both vendors were applied in all cases. The individual switches and software packages comprising the two competitive campus networks are described more in the following test sections. Here are the key software components and versions that were tested, the latest available in both cases as of the March 2017 testing.

Cisco Software

Cisco switches ran the latest version 16.3.1 of IOS software code. Cisco wireless equipment ran version 8.3 code, Cisco's Prime Infrastructure network-management ran version 3.1. StealthWatch version 6.8 (see [StealthWatch](#)) was used for analysis of captured network traffic. StealthWatch's advanced security analytics uncover sophisticated attacks on the network infrastructure.

A key automation and orchestration platform used in the Cisco topology was APIC-EM – the Cisco Application Policy Infrastructure Controller Enterprise Module (see [APIC-EM](#)). APIC-EM, a central part of Cisco's Digital Network Architecture, delivers software-defined networking to the enterprise, branch, campus, and WAN. Version 1.4 of APIC-EM was run in our tests.

APIC-EM features various operational modes and applications running on the base platform, several of which played key roles in the testing we applied. The APIC-EM includes these functions/applications:

- Discovery – APIC-EM queries the network to discover the network topology.
- Device and Host Inventory – gives access to all the devices connected on the network.
- Path Trace – displays details of the network path taken between any two devices.
- Network Plug & Play – lets the administrator pre-configure, or use the best-practices configuration, for a secure push-button deployment of newly connected devices (switches, Access Points, wireless controllers etc.).
- EasyQoS – configures QoS policies and assigns them to devices on the network, providing end-to-end quality of service across multiple layers of wired and wireless platform. It also comes with a library of best-practice policies for a long list of applications.
- IWAN – Intelligent WAN (IWAN) Application simplifies WAN deployments by providing a highly intuitive, policy-based interface that simplifies SD WAN management, allows faster deployment for branch offices, and over reduces WAN complexity and costs.

Cisco NetFlow (see [NetFlow](#)) is the next-generation in flow technology allowing optimization of the network infrastructure, reducing operation costs, improving capacity planning and security incident detection. NetFlow provides valuable information about network users and applications, peak usage times, and traffic routing. Although a Cisco invention, NetFlow data collection is also now widely used in third-party packages for IP traffic-flow analysis.

Another common component supported on many Cisco platforms is TrustSec (see [TrustSec](#)) which is software-defined segmentation that organizes endpoints into logical groups, called security groups. Security groups are assigned based on business decisions, using criteria beyond just an IP address or traditional ACLs. They are easier for administrators to understand and

manage, and the number of group-based rules is dramatically less than an equivalent set of rules based on IP addresses.

For Cisco configuration and best-practices guides:

- Cisco CVD (Cisco Validated Design Program) guide, see [Guide](#)

HPE Aruba Software

The devices selected for the HPE-Aruba campus topology and their configuration were as specified in HPE-Aruba public documents and guides (see links below). As noted, HPE in 2015 acquired leading wireless vendor Aruba Networks, which brought its products, software and technology into the HPE product fold. And, as we discovered in our testing, Aruba's wares – while innovative and generally good performers – have not been fully assimilated into a cohesive, unified HPE product architecture.

The primary HPE-Aruba network-management package we used, as recommended by HPE-Aruba, was AirWave, version 8.2. The code level for the HPE-Aruba wired switching devices was version KB.16.03, and the version for HPE-Aruba wireless devices was 6.5. It's noteworthy that HPE's legacy – and now somewhat competing – management platform, IMC (Intelligent Management Center), which purports to deliver comprehensive management across campus core and data center networks – mainly for the FlexNetwork product line, was also examined for use in this testing.

A primary HPE platform for software defined networking, used was HPE SDN VAN – HP Enterprise's Software-Defined Network (SDN) Virtual Application Networks (VAN) Controller Software, version 2.7, with added licenses for applications like Network Optimizer, Network Protector and Network Visualizer.

Even though Cisco APIC-EM EasyQoS application supports over 1300 applications, HPE's Network Optimizer application is limited to only Skype for Business. To make fair apples-to-apples comparison, we tested only the Skype for Business application on both vendors. Skype for Business, 2016 version was used for the testing. For configuration details see Skype for Business [Guide](#).

For more information on these packages, as well as HPE-Aruba's best-practices for network design, configuration and deployment, see the below links.

- Network Optimizer on HPE-Aruba's VAN Controller [Link](#)
- Aruba reference designs [Guide](#) and Aruba [Solutions Exchange](#) for configurations
- Aruba VRD (Validated Reference Design) guide, see [Guide](#)

Test Cases

Testing was conducted in three areas:

Resilient Network Infrastructure,
including the survivability of these vendors' modular switches in a multi-level campus network.

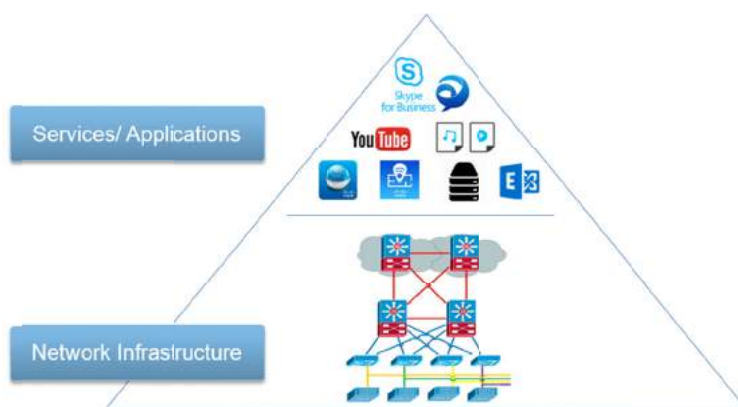
Simplified Operations,
examining the ability to readily apply features like Quality of Service (QoS) across entire end-to-end campus infrastructure.

Network Infrastructure Security,
on traffic analysis for detecting threats.

3 – Resilient Network Infrastructure

In these tests, we analyzed Cisco’s and HPE-Aruba’s solutions – which we deployed and configured based on their best-practice recommendations. In addition, we evaluated the end user’s application experience and captured the pertinent view from the network administrator’s perspective.

As illustrated in the diagram below, a strong and resilient backbone is essential to supporting business services and critical applications. For both the Cisco and HPE-Aruba configurations, we tested the underlying networks’ support of various applications across several events where one of the two VSS (Cisco) and VSF (HPE-Aruba) systems would fail and have to recover.



A strong backbone is essential to offer a resilient underlying network infrastructure to build reliable business services and critical applications.

Stacking Technologies

Cisco 4507-E

Cisco offers resilient options using either a switch stack (switch modules that interconnect via direct backplane cabling) or modular front plane stacking through a virtual switching system (VSS), which makes deployment and troubleshooting easier for support staff.

Customers can merge their modular switches into a VSS arrangement, with options for redundant supervisors in each member switch. The result is a high availability configuration that’s managed as a single logical device.

HPE-Aruba 5406R

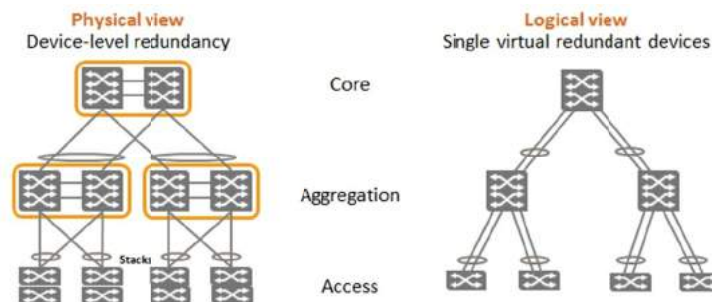
HPE-Aruba's Virtual Switching Framework (VSF) technology assembles multiple physical devices into one virtual logical device which provides high availability. Virtual Switching Framework (VSF) allows supported switches connected to each other through Ethernet connections (copper or fiber) to behave like a single-chassis switch.

HPE VSF is supported on Aruba 5400R series switches and Aruba 2930F switches.

Key drawbacks of HPE-Aruba's VSF are:

- Only one management module is supported per chassis (lacks chassis level redundancy);
- and VSF is supported only on new v3 modules.

Modular Stacking: Physical-Logical Views



Configuration Observations

Cisco can scale its modular stacking across the aggregation and core platforms making it simpler and consistent to configure and manage.

We observed a product gap in HPE-Aruba's core-switching solution. If users require additional scaling in a three-tier architecture (to support more routes, Access Control Lists (ACLs), 10/40 Gig link density etc.), HPE's answer is to deploy its FlexNetwork 10500 series switch in the core.

Unfortunately, from a modular-stacking perspective, FlexNetwork 10500 switches do not support the VSF architecture. Rather, they support the H3C IRF (Intelligent Resilient Framework) technology. IRF is quite different from VSF. Indeed, while HPE claims IRF uses open standard protocols, we observed that it employs two proprietary protocols instead.

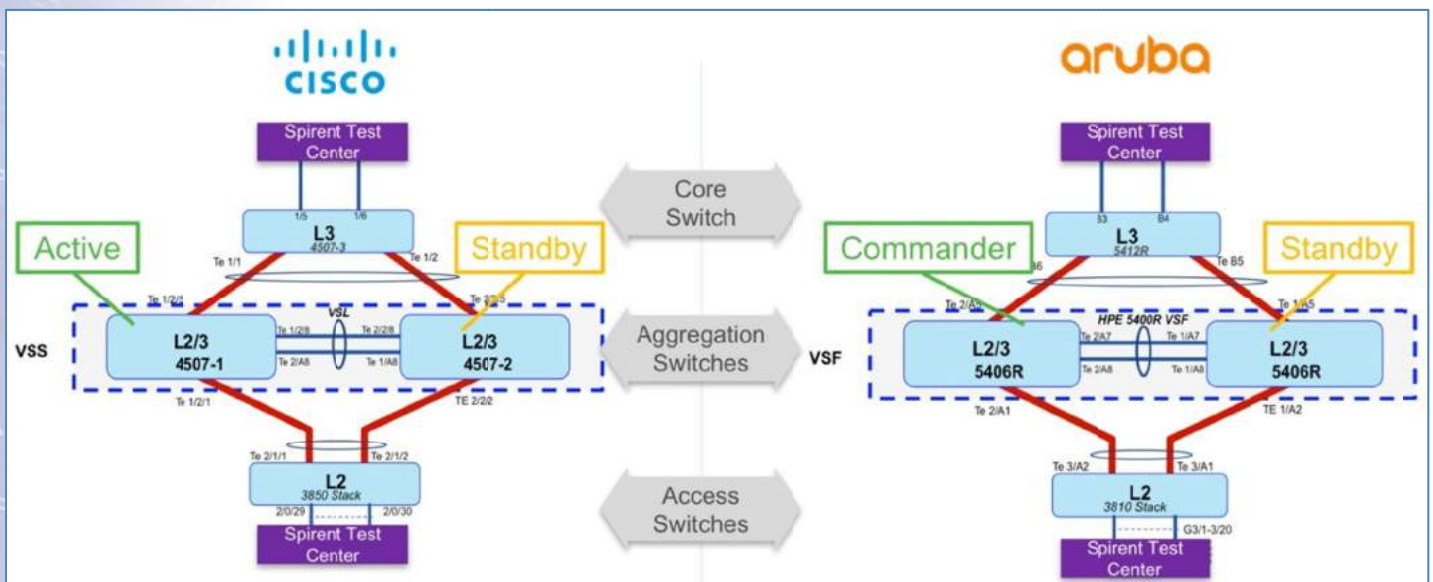
So if the user is deploying a mix of HPE-Aruba and HPE-FlexNetwork products due to high scale requirements, as recommended in previous HPE's Mobile First Campus Design, there are some significant caveats:

- The administrator has to understand, configure and manage two separate resiliency features running on two separate operating systems to achieve high availability across a pair of distribution (VSF-based) switches and core (IRF-based) switches.
- Two completely separate and disjointed management platforms are then required for deploying, monitoring, managing, troubleshooting and reporting: AirWave, for the HPE-Aruba product portfolio and IMC for the HPE-H3C product portfolio.

Test Set-up

Shown below are the physical topologies for the Cisco and HPE-Aruba network. The objective of the test was to determine the resiliency of the network across several possible outages like power failure, device failure or link error and recovery scenarios.

Network Topology

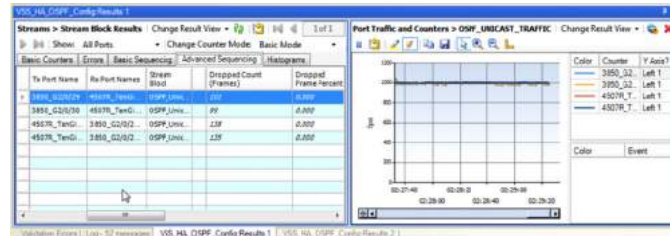


In this test, the Spirent Test Center system is set to generate bidirectional traffic across entire network infrastructure using 1000 OSPF routes. Spirent traffic flows are used to quantify the disruption that various fail scenarios cause to the clients connected via this network infrastructure.

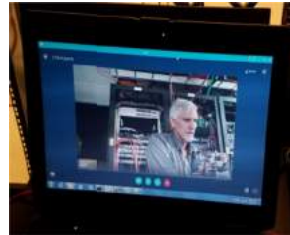
Clients attached to the wired and wireless network then ran following applications:

- ICMP pings, using Colasoft ping software
- Skype for Business Audio/Video/Desktop Sharing Call
- Video streaming using VLC Media Player
- Apple screen mirroring using apple AirPlay

Spirent Data



Skype Audio/ Video/ Desktop Sharing Call, Video Streaming and Ping



Apple Screen Mirroring



Test Objective

Compare the failover time seen when Active/ Standby switches are failed in the modular stacking configuration. How is the network downtime characterized?

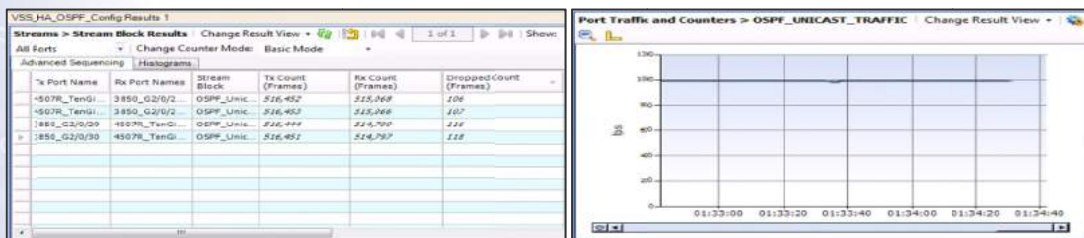
- Network Level
 - Layer 3 unicast failover times with bidirectional traffic over L2-L3 network
 - Unicast uses OSPF routing protocol with 1000 routes emulated by Spirent traffic generator
 - DUTs/SUTs are configured with OSPF graceful restart protocol extensions
- Device Level
 - Connectivity of network attached devices like Wireless Access Point, IP Phones, Video Cameras and IoT devices like Apple TV
 - Connectivity of user devices like Wired Laptop and Wireless Laptop
- Application Level
 - Ping
 - Voice/ Video/ Collaboration (Skype for Business)
 - Video Streaming (VLC)
 - Screen Mirroring (AirPlay)

The failure-recovery scenarios tested were:

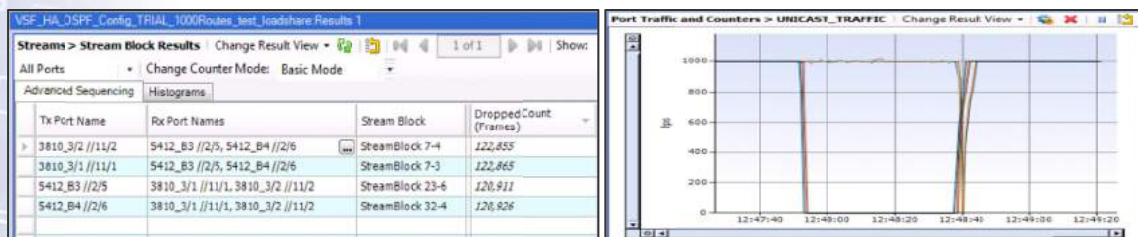
1. Unplanned Downtime – Active/Commander device goes down due to an unexpected power failure or an unexpected hardware failure of the Active/Commander
2. Unplanned Downtime – Standby goes down due to a power failure
3. Stack Link Failure – link between the VSS / VSF boxes is disconnected, simulating a link-connectivity or cable failure
4. Planned Downtime – Standby gets a software reboot, such as for a routine maintenance upgrade

In each of these tests scenarios, the Spirent Test Center issued a bi-directional traffic at 1,000pps (packets per second). The dropped packet count from the Spirent output was used to determine the duration of downtime across the network infrastructure as the system recovered from the power or connection loss.

Cisco

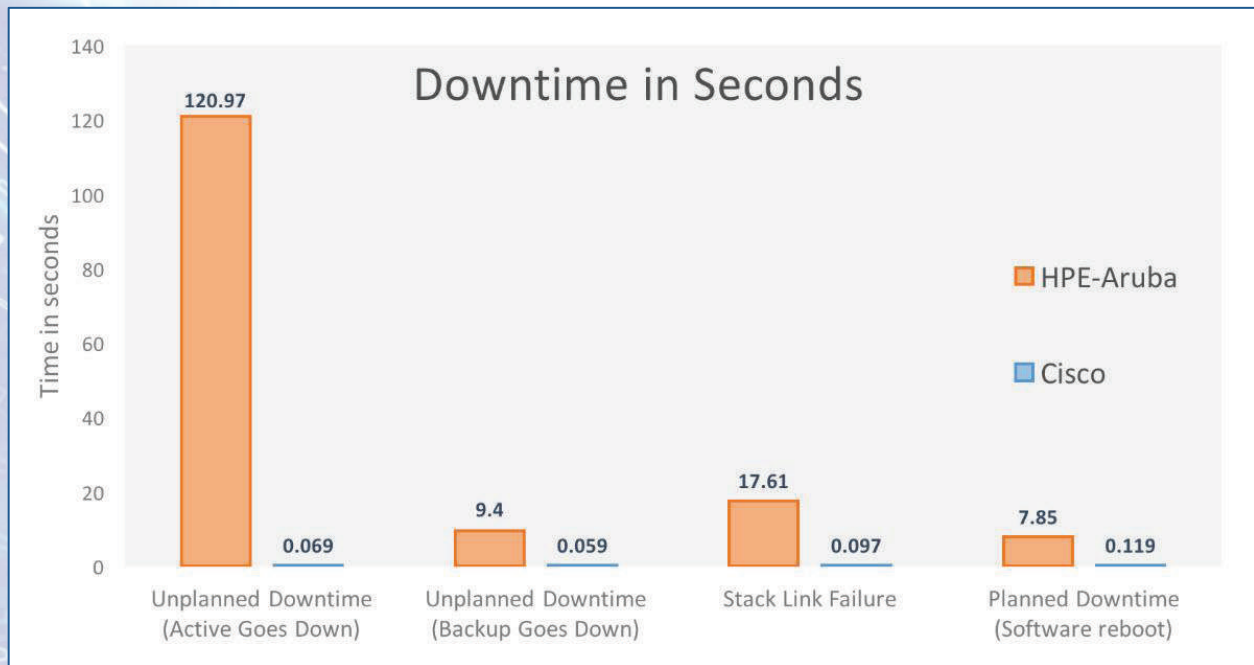


HPE-Aruba



Results

The results from the failure-recovery tests are shown in the graph below.



Source: Miercom April 2017

These tests were run multiple times and generally gave consistent results across the runs. The results shown here represent a typical run.

HPE-Aruba exhibits significant outage of over 120 seconds during unplanned downtime, which results in:

- Network downtime (causing business disruption, lost revenue and user productivity).
- Unacceptable impact on the infrastructure devices for wired and wireless like access points, phones, IoT devices, surveillance cameras and video endpoints.
- Poor application experience especially on time sensitive applications – failure of voice/video calls, IP Phones, video streaming services and screen mirroring.

Resilient Network Infrastructure Summary

In all cases, the Cisco infrastructure recovered from each failure scenario with sub-second downtime, as calculated by the Spirent dropped-packet method. What's more, and just as importantly, all the test applications showed no discernable disruption in service.

The HPE-Aruba infrastructure downtimes were significantly longer in all of the tested scenarios. What's more, HPE-Aruba wireless clients experienced significant impacts on the applications – due mainly, we observed, to the HPE-Aruba APs (Access Points) losing connection to their wireless controller during each failure. The Colasoft ping stream suffered ping drops in all tests except for the shortest 7.85 seconds downtime during planned downtime simulation using software reboot. The Skype, the video streaming and the Apple screen-mirroring applications dropped their connections in all cases while the VSF network infrastructure was recovering.

Cisco's robust modular stacking architecture was able to demonstrate sub-second failover for L3 Traffic. Cisco maintained end-to-end network connectivity for wired and wireless clients without impacting application performance and end-user experience

The Aruba Mobile-First Campus infrastructure failed to maintain connectivity for wired and wireless, impacting end-user experience and network outage for over a minute

Cisco's mature and proven stacking technology demonstrated superiority over Aruba stacking technology.

4 - Simplified Network Operations

In this testing, we sought to compare the vendors' infrastructures and applications in terms of performing complex configuration and operations across various network elements, locations, branches, and so on. By enabling the user to apply such measures simply and transparently across multiple platforms on an end-to-end basis requires less staff expertise and can save significant time and costs.

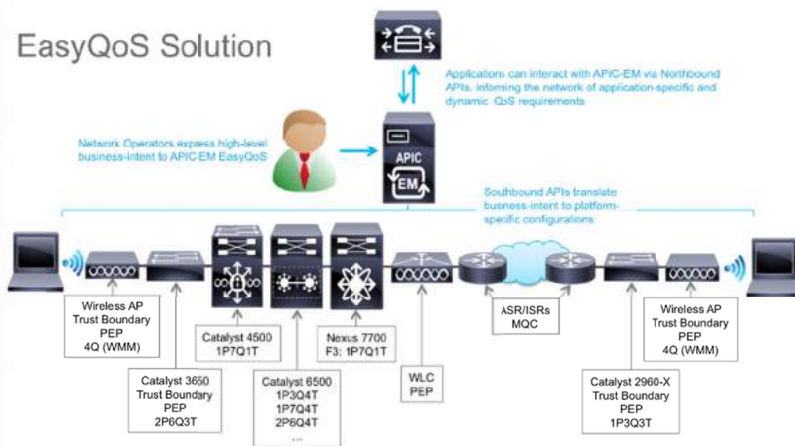
Collectively, such end-to-end operations and network-wide configuration have been termed SDN, (Software-Defined Networking). SDN has long been used to describe service-provider network operations, where custom network settings can be centrally and readily defined, in terms of bandwidth allocation, resilience, Quality of Service (QoS), and so on. Much of the same SDN capabilities are also now available to enterprise networks.

We compared the management and enforcement of operational policies between Cisco and HPE-Aruba to gauge the capability and ease of use involved with effective management of the two competitive network foundations. Our testing focused on applying QoS configurations and settings across the network.

Cisco Quality of Service (QoS) using EasyQoS

In Cisco's controller-led networking, end-to-end network quality of service is accomplished using EasyQoS, an application that runs on Cisco's APIC-EM (Application Policy Infrastructure Controller- Enterprise Module).

EasyQoS is designed to make as transparent as possible the otherwise complex configuration of priority queues across network platforms, both wired and wireless. EasyQoS provides end-to-end orchestration of QoS in the Enterprise network, implementing consistent QoS policies. The application features a fairly straightforward GUI with built-in recommended best practices for applying QoS policies. The operator expresses the business relevance of applications and the EasyQoS/APIC-EM does much of the rest under the hood.



HPE-Aruba SDN Applications

HPE's equivalent application to Cisco's EasyQoS is the Network Optimizer, which runs on HPE's VAN (Virtual Applications Network) SDN controller. Our experience with Optimizer showed some features and functions lacking when compared to EasyQoS. For example:

- In a campus deployment, the network administrator has to perform separate configurations for wired and wireless. For example, wired configuration using HPE VAN SDN Controller, and the wireless configuration using Aruba Wireless Mobility Controller (Aruba VRD). In a HPE-Aruba wired and wireless environment, there is duplication of effort for policy creation, operations and management.
- The Network Optimizer application addresses a fairly narrow QoS window. It supports QoS only on wired, edge/access switches (no wireless), and only marks DSCP (Differentiated Services Code Point) traffic at the edge.
- For Skype for Business end-to-end QoS, the administrator needs to configure VAN Controller and Mobility Controller separately to achieve same results. Moreover the administrator needs to make sure every hop throughout the network and WAN are honoring correct DSCP markings.

HPE does sponsor an SDN App Store, which we explored to make sure we weren't missing any other applications or automated-management capabilities. We found just three HPE-branded, homegrown applications: the Network Optimizer, and two others called Protector and Visualizer.

We noted that *third-party* applications are not tested, validated or supported by HPE. What's more, many of the partner applications are fairly old and apparently work only on older HPE platforms.

Feature Comparison

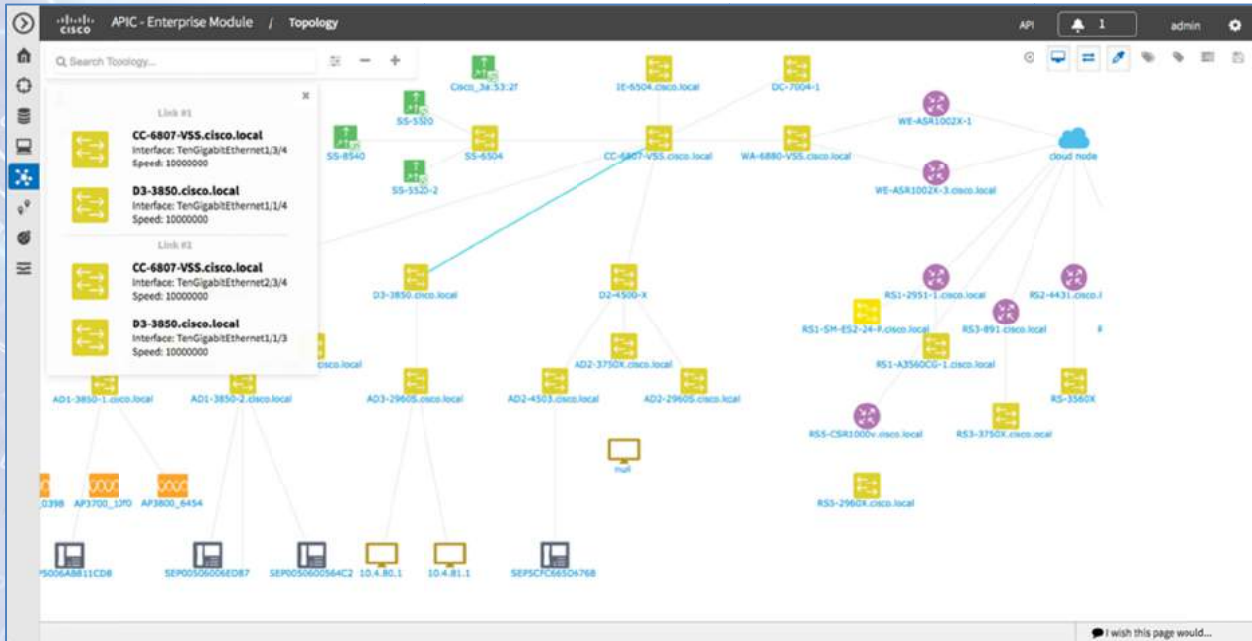
Our assessment of the two competing software packages – EasyQoS (APIC-EM) and Network Optimizer (HPE VAN) – covered the following functional areas, in all cases using the standard best practices from the current released documentation for each product:

1. Policy Creation and Management – the ease of creating and managing policies
2. Policy Enforcement – consistently applying policies across every network device (access, aggregation and core switches, wired as well as wireless and routers)
3. Breadth of Coverage – the number of supported applications/traffic types for policy control, and investment protection for future applications

The task we undertook, then, was to create and apply end-to-end QoS policies, for multiple applications, across multi-tiered switching and wireless networks portions.

QoS Configuration, via Cisco APIC-EM

The process starts with the Topology View of the Cisco APIC-EM SDN Controller (shown below), consisting of entire network including switches, routers, wireless controllers and access points.



EasyQoS - Application Registry

Cisco offers a built-in application registry with more than 1300 applications which includes business applications like Jabber, Spark, Skype for Business and consumer applications like YouTube, Netflix, AirPlay etc. Cisco also offers ability to add customized applications like internal web services, file hosting or video hosting services.

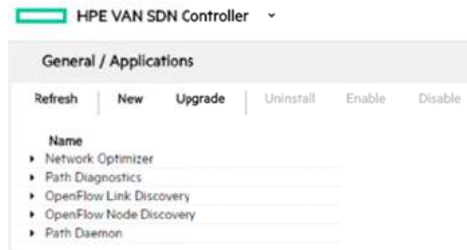
The screenshot displays the Cisco APIC-EM EasyQoS Application Registry interface. The interface is divided into several sections: POLICY SCOPIES, APPLICATION REGISTRY, POLICIES, and ADVANCED SETTINGS. The APPLICATION REGISTRY section is active, showing a list of applications categorized by traffic class and control/voice/video/data. The 'telepresence-media' application is highlighted. The right side of the interface shows details for the 'telepresence-media' application, including its traffic class, group, description, and associated policies.

Scope	Policy Name	Relevance
CVD	BUSINESS_RELEVANT_CVD_Policy	Business-Relevant
EasyQoS_Lab	EasyQoS_Lab_Policy	Business-Relevant
EasyQoS_Lab	EasyQoS_Wireless_Poli	Business-Relevant

HPE-Aruba VAN Controller Applications

HPE VAN SDN Controller

A fairly lean set of applications can be found under the HPE VAN Controller package (see below), one of which is the Network Optimizer for applying QoS policies.



HPE VAN Controller Topology View – Only Switches and Hosts (not wireless and routers)

Similar to Cisco's Topology View, HPE VAN provides a topology view that includes switches and hosts. But wireless equipment including Access Points (APs) and routers are not included. However, the topology view misses comprehensive information about device version, connectivity, link details etc.



HPE Network Optimizer

HPE-Aruba requires the user to create manual profiles for various QoS configurations, compared to Cisco EasyQoS which uses built-in best practices. Moreover these configurations are valid only for edge switches which again forces administrator to create similar policies separately on wireless controllers.

VAN SDN Controller and Network Optimizer have knowledge of wired users connected to a switch. They apply the policy on the switch using OpenFlow to configure a specific remarking rule for the Skype for Business traffic flow. It's up to the administrator to configure and maintain similar device policies beyond the edge switches.

Results

Ease of creating policies – We concluded that Cisco EasyQoS, along with other pertinent Cisco APIC-EM applications, such as Path Trace, provides a straightforward, single site to configure and apply policies for QoS control – for both wired and wireless network portions. With HPE-Aruba, two discrete applications are required to implement QoS control: VAN for wired network portions, and Mobility Controller for wireless.

End-to-end policies – The Cisco APIC-EM addresses policies for every wired-wireless-WAN device in the network. HPE-Aruba application applies policies only at the network's access edge.

Variety of supported applications/traffic types – The Cisco EasyQoS environment includes support for over 1,300 applications/traffic types, providing investment protection for users' future traffic types. The HPE-Aruba application supports only one – Skype for Business.

Unified Management – Based on HPE-Aruba's VRD guide, if customers require additional scale, HPE-Aruba requires another piece of management platform to manage multiple VAN SDN Controllers. IMC is recommended as the standard management tool for VAN, and a separate module (SDN Manager) is required for installation to manage a cluster of VAN controllers. Whereas the rest of the network requires AirWave management platform which creates duplication, additional licensing and platform lifecycle management.

Simplified Network Operation Summary

For the criteria and objectives we assessed, the Cisco EasyQoS application clearly far exceeds the capabilities of HPE-Aruba's Network Optimizer, especially in consolidated support of both wired and wireless network equipment and portions, in the ability to apply policies on an end-to-end basis, and in the scope of applications and traffic types already defined and supported.

Cisco's EasyQoS is capable of configuring QoS across 40 network devices (including routers, switches, and wireless APs and devices) for over 1,300 applications/Traffic types, and across six different device operating systems. In one of our tests, more than 25,500 lines of configuration commands were pushed out to network nodes in one minute – all under the covers and transparently to the network administrator. The EasyQoS solution provides a simplified, business-drive model.

Except for edge-access switches, HPE-Aruba requires customers to provision QoS manually within the infrastructure. That is where the bulk of QoS-configuration complexity lies, and is critical to achieving consistent end-to-end QoS across the router/switch/wireless infrastructure.

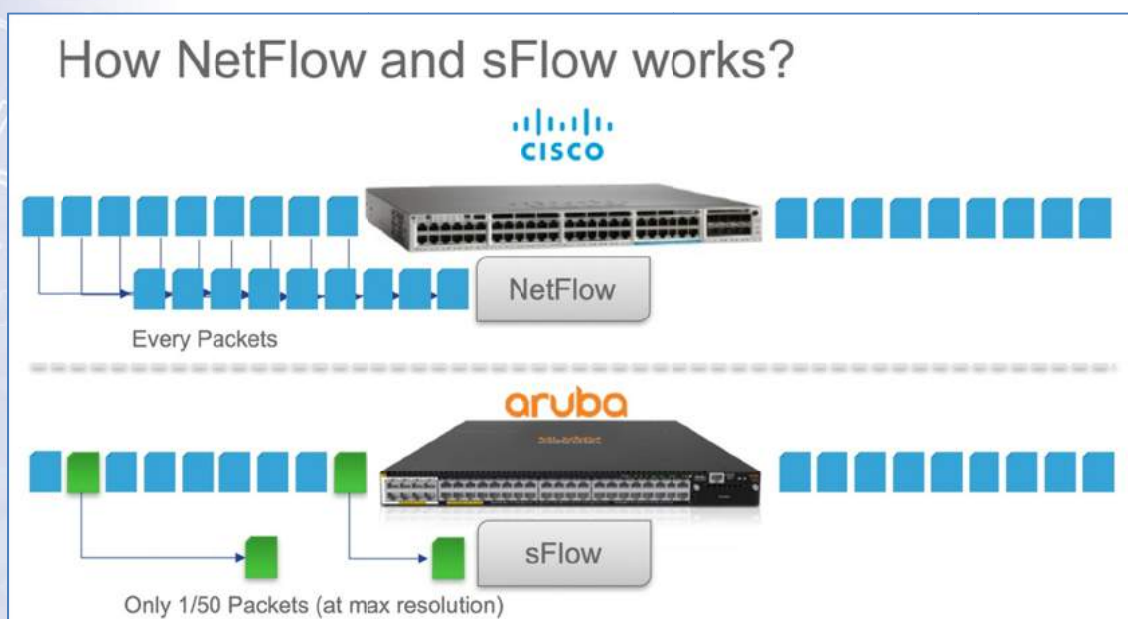
There are multiple congestion points across the network as some links are naturally oversubscribed. This is not addressed by HPE-Aruba's VAN/Network Optimizer application. In addition, Network Optimizer cannot dynamically prioritize other business critical traffic types, such as Oracle, SAP or Salesforce.

5 - Network Infrastructure Security (Traffic Analysis)

Cisco vs HPE-Aruba Traffic-Analysis Technology

Cisco's NetFlow technology is supported across many wired-wireless-routing platforms. Cisco Catalyst family of switches leverage Cisco's UADP (Unified Access Data Plane) custom ASIC (Application-Specific Integrated Circuit) to enable full NetFlow and real-time traffic analysis without impacting switching performance. This allows monitoring of 100 percent of the packet flow through all Cisco UADP based switches on the network.

By comparison, HPE-Aruba samples traffic to be captured using sFlow, which collects at best one out of every 50 passing packets. This difference is illustrated in the figure below.



This key difference enables Cisco traffic monitoring and analysis to gain a much more granular view, which can be further processed for accurate threat analysis. That's because many of today's threats – notably malware, worms and similar executable files – are communicated over many packets. By observing the entire sequence of suspect packets, analytic software can better view the context of suspect threats, match signatures of known threats, and more accurately spot and isolate them.

Cisco's network-security portfolio (Cisco Security Solutions) contains various tools which, collectively, help secure the network infrastructure. Some of this work together; others work independently.

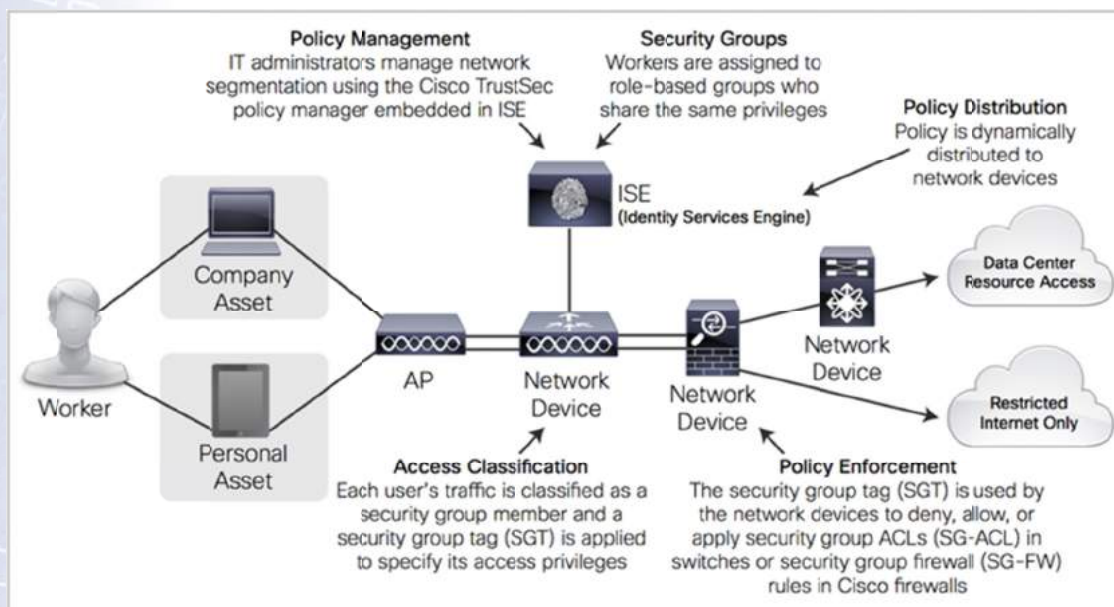
Cisco StealthWatch uses NetFlow or sFlow to provide visibility across the network. Then it employs advanced security analytics to examine flows and uncover attacks. StealthWatch uses the network as a real-time security sensor and enforcer to bolster threat defenses. Discrete Management Console, Collector and Sensor components make up the StealthWatch system.

Cisco Identity Services Engine (ISE), a network-administrator application, enables the creation and enforcement of security and access policies for endpoint devices connected to the network. Its goal is simplify identity management across diverse devices and applications.

Cisco TrustSec, a security capability where a tag (called Security Group Tag) is assigned to a user's or device's traffic when it enters the network, and then the access policy is enforced based on the tag, everywhere in the network infrastructure.

Making the pieces work together

The below graphic illustrates the interaction of the Cisco security elements. Policies, as discussed previously, are dynamically distributed to all network nodes and devices. The Identity Services Engine maintains the information on specific users and groups, resulting in security group tags being applied to each user's traffic. Each device in the network, as a coordinated whole, checks the tag and undertakes the appropriate action.



HPE-Aruba's security approach showed some significant differences. For example:

- HPE-Aruba captures traffic for analysis based on a sampling process (sFlow), which provides traffic analysis with considerably less evidence to sift through which often leads to false alarms or blurred analysis.
- HPE Flow is only supported on switches; there is no flow solution with wireless devices. Cisco NetFlow can capture full streams from any network device.

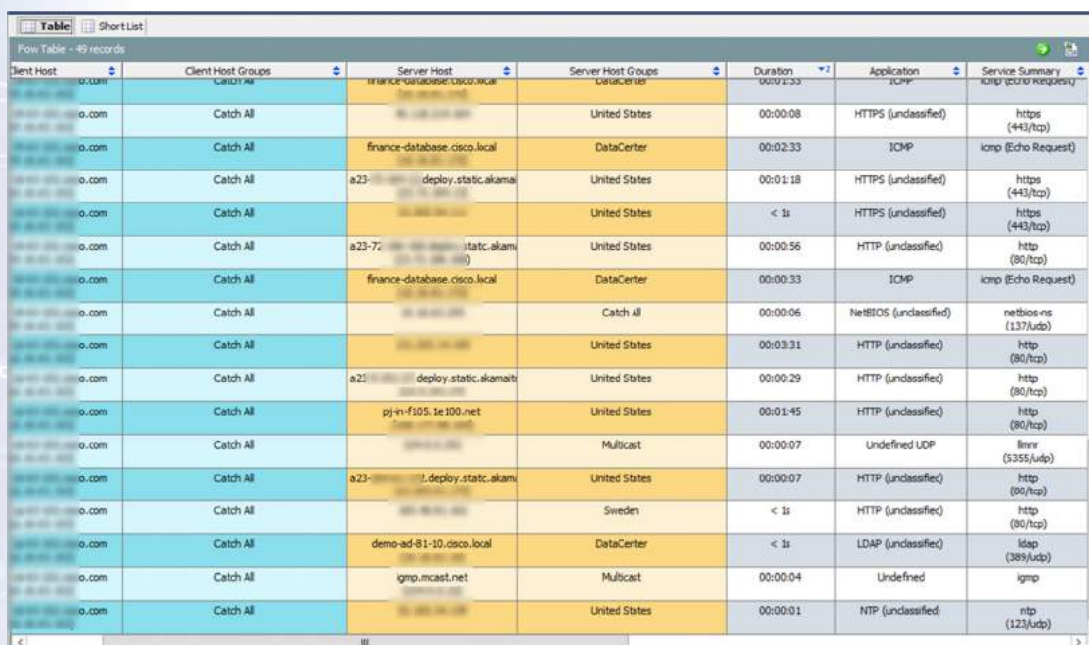
Threats From Within

Security attacks emerge from many unexpected sources – like end-user devices, IoTs (Internet of Things) devices, users themselves, BotNets, ransomware, malware, and so on. Indeed, network compromises can occur from traffic flowing inside a branch or inside the HQ. These are often referred to as East-West traffic flows, since they originate and target nodes within the network, and not necessarily from the outside.

As noted, HPE-Aruba security focuses on access switches, and so internally generated threats can go unnoticed. Granular traffic-flow analysis is extremely important at every level to identify threats and then take corrective actions

Several tests were run with StealthWatch analyzing the captured data from both vendors' campus networks. Several typical threats were included in the packet streams along with generic continuous ping and http traffic. One in particular highlighted this major difference in packet-capture techniques. An nmap port scan was conducted. Such a scan, designed to find open or accessible protocols and ports in network devices and hosts, involves many queries to target systems. When responses are received back, it is clear that certain ports and protocol services are active and open, and these are used for subsequent attacks.

What we found was that with full data capture, via NetFlow, the administrator is presented much more meaningful results. Suspect packets and flows are not just identified as possible threats, but a simple double-click drill-down lets the user gain more detailed information, including the source of the suspect traffic.



Client Host	Client Host Groups	Server Host	Server Host Groups	Duration	Application	Service Summary
o.com	Catch All	finance-database.cisco.local	DataCenter	00:01:33	ICMP	icmp (Echo Request)
o.com	Catch All	finance-database.cisco.local	DataCenter	00:00:08	HTTPS (unclassified)	https (443/tcp)
o.com	Catch All	finance-database.cisco.local	DataCenter	00:02:33	ICMP	icmp (Echo Request)
o.com	Catch All	a23-...-deploy.static.akama	United States	00:01:18	HTTPS (unclassified)	https (443/tcp)
o.com	Catch All	a23-...-deploy.static.akama	United States	< 1s	HTTPS (unclassified)	https (443/tcp)
o.com	Catch All	a23-7-...-stafc.akam	United States	00:00:56	HTTP (unclassified)	http (80/tcp)
o.com	Catch All	finance-database.cisco.local	DataCenter	00:00:33	ICMP	icmp (Echo Request)
o.com	Catch All	o.com	Catch All	00:00:06	NetBIOS (unclassified)	netbios-ns (137/udp)
o.com	Catch All	o.com	United States	00:03:31	HTTP (unclassified)	http (80/tcp)
o.com	Catch All	a21-...-deploy.static.akama	United States	00:00:29	HTTP (unclassified)	http (80/tcp)
o.com	Catch All	pg-y-f105.1e100.net	United States	00:01:45	HTTP (unclassified)	http (80/tcp)
o.com	Catch All	o.com	Multicast	00:00:07	Undefined UDP	linnr (5355/udp)
o.com	Catch All	a23-...-L.deploy.static.akam	United States	00:00:07	HTTP (unclassified)	http (80/tcp)
o.com	Catch All	o.com	Sweden	< 1s	HTTP (unclassified)	http (80/tcp)
o.com	Catch All	demo-ad-81-10.cisco.local	DataCenter	< 1s	LDAP (unclassified)	ldap (389/udp)
o.com	Catch All	igmp.mcast.net	Multicast	00:00:04	Undefined	igmp
o.com	Catch All	o.com	United States	00:00:01	NTP (unclassified)	ntp (123/udp)

Cisco

Client User Name	Client Host	Client Host Groups	Server Host	Server Host Groups	Duration	Application
dhcp-10.10.10.10	10.10.10.10	Catch All	finance-database.cisco.local	DataCenter	00:03:10	Undefined TCP
dhcp-10.10.10.10	10.10.10.10	DataCenter	dhcp-10.10.10.10	DataCenter	00:03:19	ICMP
dhcp-10.10.10.10	10.10.10.10	Catch All	pj-in-f99.1e100.net	United States	00:00:01	HTTPS (unclassified)
dhcp-10.10.10.10	10.10.10.10	Catch All	pj-in-f94.1e100.net	United States	00:00:01	HTTPS (unclassified)
dhcp-10.10.10.10	10.10.10.10	Catch All	a23.deploy.static.akamai	United States	00:00:02	HTTPS (unclassified)
dhcp-10.10.10.10	10.10.10.10	Catch All		United States	00:01:51	HTTPS (unclassified)
dhcp-10.10.10.10	10.10.10.10	Catch All	demo-ad-81-10.cisco.local	DataCenter	00:01:06	DNS (unclassified)
dhcp-10.10.10.10	10.10.10.10	Catch All	a21.deploy.static.akamai	United States	< 1s	HTTP (unclassified)
dhcp-10.10.10.10	10.10.10.10	Catch All	pj-in-f100.1e100.net	United States	< 1s	HTTPS (unclassified)

HPE-Aruba

The results of the StealthWatch analysis of the HPE-Aruba data capture are much more limited, it turns out. Fewer suspected threats are identified, and few details are included to aid security decisions and corrective action. Most of the results are simply shown as unclassified.

The StealthWatch display below, from the Cisco infrastructure using NetFlow data capture, shows considerable detail on suspected threats. The user can see the size of the threat stream, and can drill down to find the source and apply enforcement action. For example: Port Scan is being identified as a security event

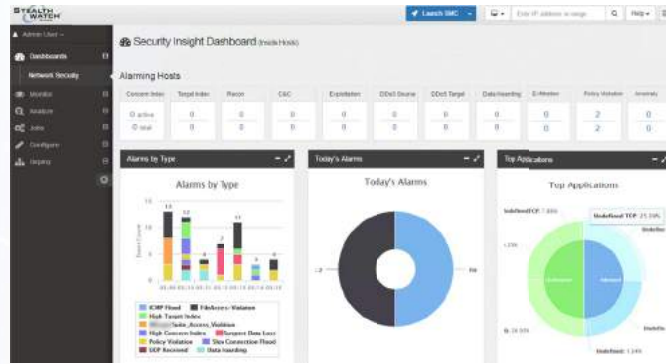
Start Active Time	Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Mar 15, 2017 1:27:18 PM (48s ago)	Catch All	dhcp-10.10.10.10	DataCenter	finance-database.cisco.local	108,036	Port Scan(36)

Cisco infrastructure, with NetFlow capturing 100 percent of traffic, all of the threatening scan packets were caught and identified.

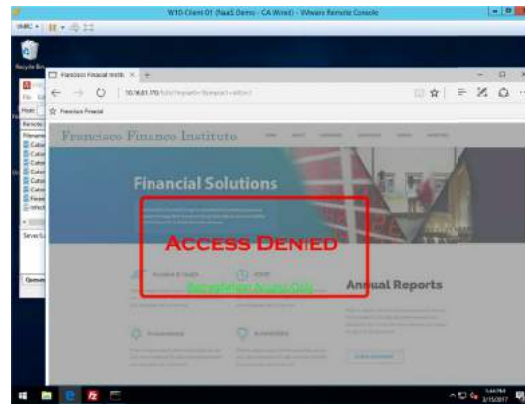
Network as an Enforcer

Once data is collected by the Network as a Sensor, the Network as an Enforcer—enabled by Cisco TrustSec technology—is a software-defined segmentation and response system that enhances your ability to limit the security attack surface and quickly take action to contain threats. The functionality is built into the Cisco networking hardware and gives you the ability to create access and segmentation policies in ISE, which controls the network and allows you to:

- Segment your network into security groups to protect and reduce threat proliferation



- Take immediate action to contain a threat



We used ISE to create a policy to contain the threat so its access can be restricted, removed altogether, or quarantined until it is fixed or remediated. We found that applying enforcement action in the Cisco infrastructure was easier and faster than with HPE-Aruba. In fact, depending on how policies are defined, the TrustSec policy segmentation application can automatically quarantine the offending PC.

Network Infrastructure Security Summary

Cisco's UADP custom ASIC enables full NetFlow captures and real-time traffic analysis without impacting the switching performance. HPE-Aruba states that it offers a flexible, programmable ProVision ASIC. However, their switches were unable to detect multiple events – due, we believe to implementation limitations, as well as the sampling data-capture technology. Since HPE-Aruba cannot identify the threats, they cannot contain the threat.

6 - Summary

Our evaluation found that Cisco offers a robust network infrastructure with impressive resiliency and the ability to apply configuration and security settings across the entire product line, including wired and wireless portions. HPE-Aruba offers similar equipment at the lower, functional layers, but we found serious limitations at the higher control and configuration layers. Most noteworthy, wireless and wired network portions are handled by disjointed control and configuration applications.

Cisco's stacking capabilities offer solid resilience and ability to withstand failures. Our tests found that Cisco supports sub-second failover recovery in all scenarios we tested. This is so quick, in fact, that neither users nor applications are impacted. In the HPE-Aruba infrastructure recovery delays were as long as 120 seconds, and all application connections dropped and had to be reconnected.

Cisco's investment in custom silicon ASICs makes a big difference with NetFlow, where whole data streams can be captured in real-time and security-analyzed, with no impact on regular switch-forwarding performance.

The security tools that comprise Cisco's threat-detection and mitigation portfolio are effective and straightforward to use, using the network as a sensor for threatening traffic, and an enforcer to mitigate threats. We found that, with all security applications at play, we could identify threats and anomalies and take immediate action to secure an entire campus network.

In addition, the Cisco APIC-EM, with numerous applications, offers real-world SDN (Software Defined Networking). We conclude that one of these, EasyQoS, enables end-to-end orchestration of QoS in the enterprise network, making QoS policy definition simple and easy to deploy. The APIC-EM controller does most of the complex and tedious work under the hood.

7 - About Miercom Performance Verified Testing

This report was sponsored by Cisco Systems, Inc. The data was obtained completely and independently by Miercom engineers and lab-test staff as part of our Performance Verified assessment. Testing such as this is based on a methodology that is jointly co-developed with the sponsoring vendor. The test cases are designed to focus on specific claims of the sponsoring vendor, and either validate or repudiate those claims. The results are presented in a report such as this one, independently published by Miercom.

8 - About Miercom

Miercom has published hundreds of network-product-comparison analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

9 - Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Miercom or Cisco Systems, Inc. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.