



Cisco Branch Office Router Comparative Assessment

Cisco ISR1111-8P/1117-4P

Huawei AR201/1220E/169FGW-L

Hewlett Packard Enterprise MSR954-W/1003



DR180731D

21 August 2018

Miercom

www.miercom.com

Contents

1.0 Executive Summary	3
2.0 Products Tested	5
3.0 How We Did It	8
4.0 Maximum WAN Throughput.....	10
5.0 Wireless LAN Features and Ease of Use.....	13
6.0 Security: Router Packet Inspection and Threat Analysis	17
7.0 Cisco SD-WAN: Tool for WAN Configuration and Management.....	20
About "Miercom Performance Verified" Testing.....	24
About Miercom	24
Use of This Report.....	24

1.0 Executive Summary

Miercom was engaged by Cisco Systems to independently compare the performance and key features of leading branch-office routers from: Cisco Systems (it's ISR1111-8P and ISR1117-4P models); Huawei Technologies Co., Ltd (the AR201, AR1220E and AR169FGW-L models); and Hewlett Packard Enterprise Co. (models MSR954-W and MSR1003).

The tested routers were all configured exactly per the vendors' documentation and best practices, and all ran the latest available operating software versions. Each tested branch-office router connected via WAN link with an appropriate "remote peer" router from the same vendor. Testing was conducted in the summer of 2018 in a well-equipped lab on the West Coast, using the latest test system from Spirent Communications.

In addition to throughput testing, "soft" aspects of the routers were examined, including: WiFi features, set-up and management; and data capture for traffic analysis.

Key Findings and Observations:

- **Cisco ISR1111-8P consistently delivered highest average IPSec encrypted WAN throughput at 365 Mbps and the ISR1117-4P followed with 281 Mbps. Huawei routers delivered 84 to 245 Mbps, and HP Enterprise routers delivered 59 to 68 Mbps.**
- **Huawei routers exhibited wide variability in throughput for the same test; the Huawei AR1220E delivered throughput varying by more than 100 percent.**
- **Cisco's NetFlow ability to capture complete traffic flows without compromising performance makes a big difference in the ability to analyze traffic and spot threats. Huawei and HP Enterprise only sample traffic.**
- **Cisco ISR1100 routers deliver the richest set of Wi-Fi features using its built-in Mobility Express architecture, and delivers the best, integrated, scalable and easy-to-use Wi-Fi deployment and management.**
- **Unlike competing routers, Cisco ISR1100 routers offer integrated, feature-rich and scalable SD-WAN**
- **Cisco's unique Encrypted Threat Analytics (ETA) capability identifies the threats (e.g. malware, Trojans, botnets) hidden inside encrypted traffic, such as HTTPS, without infringing privacy. HPE and Huawei both lack this capability.**

With throughput performance and wireless support that outpaces competitive branch-office routers from Huawei and HP Enterprise, we proudly award the **Miercom Performance Verified** certification to Cisco's Integrated Services Router ISR1100 Series, branch-office routers models ISR1111-8P and ISR1117-4P, which effectively deliver a "branch-in-a-box" solution.



Robert Smithers

CEO

Miercom

2.0 Products Tested

Cisco Systems, Huawei Technologies Co., Ltd and Hewlett Packard Enterprise Co. all offer routers designed for SMB (small-to-medium business) environments, as well as for branch-office settings that would be part of a larger enterprise network. This testing and analysis focused on the branch office. The branch office environment entails a particular set of network requirements:

- The need for straightforward remote administration.
- A high degree of remotely administered security, including data capture, threat detection and mitigation.
- Support for one or more high-speed, secure WAN links. Typically, WAN links send data encrypted to the organization's headquarters, or to some other intermediate access and routing point, as well as decrypt incoming data.
- The ability of the branch-office router to interact effectively and efficiently with an appropriate upstream "peer" router.
- Ideally, the branch-office router will also deliver WiFi service to the branch office, including, as necessary, the administration of multiple wireless Access Points (APs).

Cisco Routers (*Cisco IOS XE version 16.07.01*)

Two branch office routers were selected from the Cisco Integrated Service Routers ISR1100 Series. This router comes in a variety of configurations, ranging from 4 or 8 LAN ports, built-in Wi-Fi, LTE uplink capabilities. Numerous models of this series deliver Power over Ethernet (PoE) and PoE+ to endpoints, including APs. The integral IOS XE operating software handles WAN services, VLANs, various WAN-link redundancy and failover options, and most recently, Software-Defined WAN (SD-WAN) support.

WAN links can be secured with IPSec Triple-DES (Data Encryption Standard) and the Advanced Encryption Standard (AES), as well as other encryption algorithms. IPSec capacity can be increased with a remote, performance-on-demand license upgrade. The ISR1100 reportedly handles data encryption/decryption at up to 350 Mbps.

Besides LAN and WAN interfaces, the ISR1100 Series supports the latest WiFi IEEE 802.11ac standard via a built-in, dual-radio 2x2 MIMO integrated AP. What's more, the ISR1100 can also act as a WLAN controller for other external APs, handling up to 50 APs. ISR1100 supports Cisco's Mobility Express WLAN architecture which offers the enterprise class feature richness without compromising the security & scalability. These WiFi capabilities are integral with the ISR1100 Series; no additional licenses are required.

Cisco ISR1111-8P router. The ISR1111 provides two WAN ports – one a Gigabit Ethernet (GbE) port and the other a GbE/SFP “Combo” port – supporting either a GbE copper or SFP (small-form-pluggable) fiber link. In addition, this branch-office router provides eight GbE LAN ports. Four GbE links can deliver PoE to endpoints or two can deliver high-powered PoE+. Two multiband swivel-mount dipole antennas are included.



Source: Cisco Systems

Cisco ISR1117-4P router. While similar in most respects to the ISR1111, the ISR1117 has four GbE LAN ports, two of which can deliver PoE or one can deliver PoE+. The ISR1117 also support the option to connect using ADSL2, VA-DSL, VDSL2+ etc.



Source: Cisco Systems

With all these connectivity options, Cisco ISR1100 offers most flexibility, scalability and investment protection compared to the competition.

Huawei Routers *(software version 5.160 with Patch ARV200R007SPH020)*

Huawei describes its AR100, AR120, AR160 and AR200 Series as fixed interface routers for branch offices and small businesses. Like the Cisco models tested, these Huawei routers provide four or eight LAN ports and two WAN/uplink ports.

Unlike the Cisco ISR1100 Series, which supports both a built-in WiFi Access Point and Wireless LAN Controller, the Huawei routers can function either as a Wireless LAN Controller or a WiFi AP, but not both. To switchover from AP to controller, a restart of the device is required. In addition, a separate, additional license is required for each AP supported.

Huawei AR201 router. The AR201 reportedly delivers up to 150 Mbps of WAN bandwidth. It provides two WAN ports and eight LAN ports, which can alternately be configured as WAN interfaces. If the WiFi controller is enabled, up to eight APs can be managed.



Source: Huawei Technologies

Huawei AR1220E router. This router features two GbE Combo ports and eight GbE LAN ports, which can alternately be configured as WAN ports. The vendor says the router supports embedded hardware encryption and 400 Mbps of WAN bandwidth. If the WiFi controller is enabled, up to 12 APs can be managed.



Source: Huawei Technologies

Huawei AR169FGW-L router. Like the AR201, this branch router claims WAN bandwidth support up to 150 Mbps. If the WiFi controller is enabled, up to eight APs can be managed. The router has one WAN GbE Combo port and four LAN ports, which can alternately be configured as WAN interfaces.



Source: Huawei Technologies

Hewlett Packard Enterprise (HPE) Routers

Hewlett Packard Enterprise (HPE) advertises that its MSR95x Series routers deliver up to 300,000 pps (packets per second) of throughput. With minimum 64-byte packets, that equates to about 150 Mbps. The other HPE router tested, the MSR1003, has a bit more horsepower and boasts a 500,000 pps throughput, about 250 Mbps.

The HPE routers tested do also offer integral APs, although WiFi support in the models tested is limited to 802.11n and only 2.4-GHz frequency support. Cisco routers by comparison support the latest 802.11ac Wave 2 standard's 5-GHz frequency band. There is no option with either of the HPE routers for an integral Wireless LAN Controller.

HPE MSR954-W router. This small branch router provides a Combo WAN port (with GbE and SFP ports) and another GbE WAN port, plus four GbE LAN ports. The router was tested with software version 7.1.064, Release 0605P20 software.



Source: Hewlett Packard Enterprise

HPE MSR1003 router. This small branch office router features two GbE WAN ports and eight GbE LAN ports. The vendor says the router includes embedded hardware encryption accelerator for improved encryption performance. The router was tested running software version 5.20.106, Release 2516P13 software.



Source: Hewlett Packard Enterprise

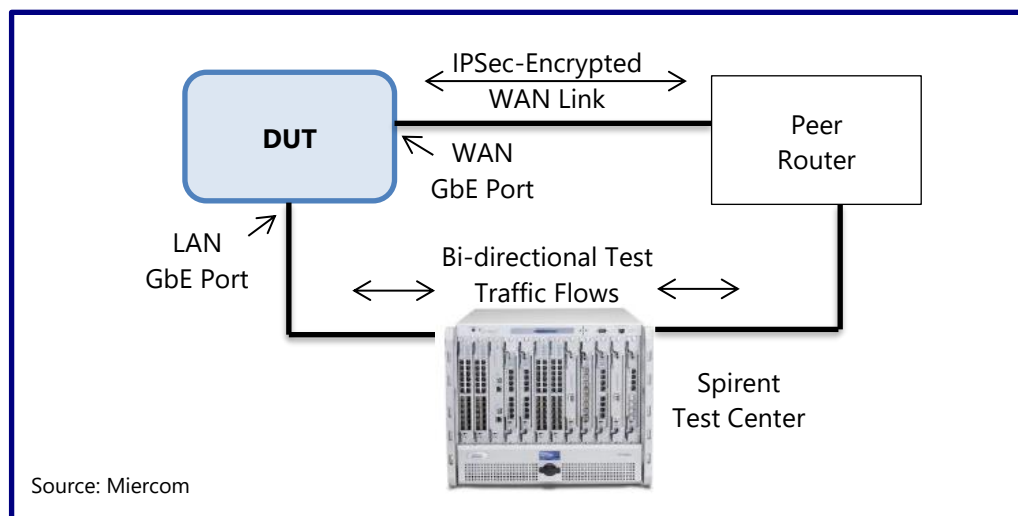
3.0 How We Did It

The testing for this comparative analysis included both “hard” performance measurement and “softer” test components, where aspects including security and WiFi ease of use were assessed.

Based on the branch office deployment, all router performance was compared using maximum bi-directional throughput over a GbE WAN link, which all tested routers support (except the Huawei AR201, which is FastEthernet). To reflect realistic private networks with branch offices and data centers, all traffic was secured with IPSec encryption.

Each vendors’ test bed configurations were set up side-by-side to run throughput tests in parallel. Each test bed was built according to the topology shown below.

Figure 1: Test Topology



At the uplink end of the WAN connection was another one of the same vendor’s routers, typically a larger one, to simulate a headquarters data center site. Being the more powerful router with higher throughput, we could then be confident that the Device Under Test (DUT) is the source when heavy traffic reached the point where packets would be dropped. These larger routers for each respective test bed were the Cisco ASR1002X, the Huawei AR3260 and the HPE MSR4080.

Identical tests were run in all three test bed configurations. First, we ran 100 UDP (User Datagram Protocol) bi-directional flows over the IPSec-encrypted WAN link for 30 seconds. This “ramp up” established the flows in an equilibrium state. Then the one-minute throughput test would be run, and afterwards the test would ramp down for one minute until traffic flow dropped to zero.

Tests were compliant with RFC 2544, to discover the highest rate of traffic before packet loss occurred. Traffic was issued in both directions from the Spirent Test Center, and all traffic was routed back to the test system to determine packet loss.

The Spirent Test Center benchmarked multiple runs of a standard IPSec throughput test, using IMIX traffic. This traffic was not random but compromised of a precise mix and length of packets, shown in the table below. Sixty percent of the packets were short, with IP lengths of just 72 or 74 bytes. A quarter of the packets had mid-size length of 576 bytes, and the remaining 16 percent were large 1400-byte packets.

Figure 2: IMIX Test Traffic Composition

iMIX Distribution	Frame Length Mode	IP Total Length	Default Ethernet	POS Length	Weight	Percentage (%)
IPSEC	FIXED	72	90	80	5,867	58.67
IPSEC	FIXED	74	92	82	200	2
IPSEC	FIXED	576	594	584	2,366	23.66
IPSEC	FIXED	1,400	1,418	1,408	1,567	15.67

While repeated throughput tests could yield different results, most variations were minor. But in a few cases, this variation was substantial. To resolve this issue, the throughput test was run 20 times, and the average throughput was recorded.

4.0 Maximum WAN Throughput

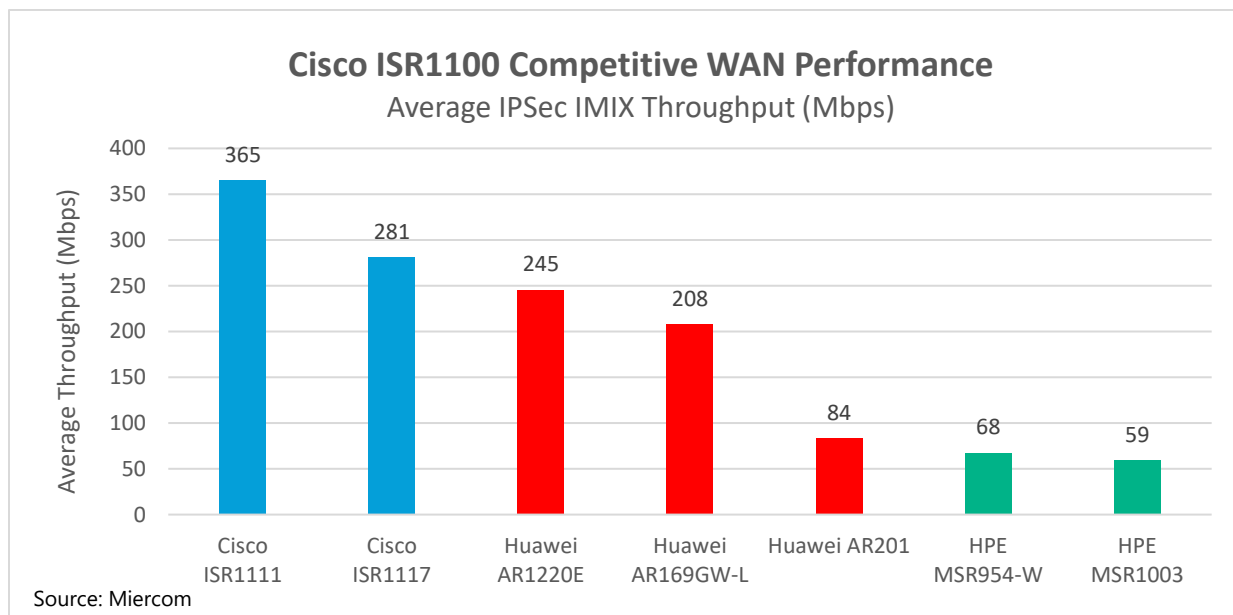
The maximum throughput rate of each branch office router; that is, the highest volume of data that the router can forward, bi-directionally, before packets are dropped or lost.

This test was conducted by the Spirent Test Center in accordance with RFC 2544. Three test-bed networks were assembled, one for each vendor's routers.

Results

The average maximum performance of the branch office routers tested, based on 20 test runs for each router, is shown below. The average Cisco performance is higher than for either the Huawei or HPE routers tested.

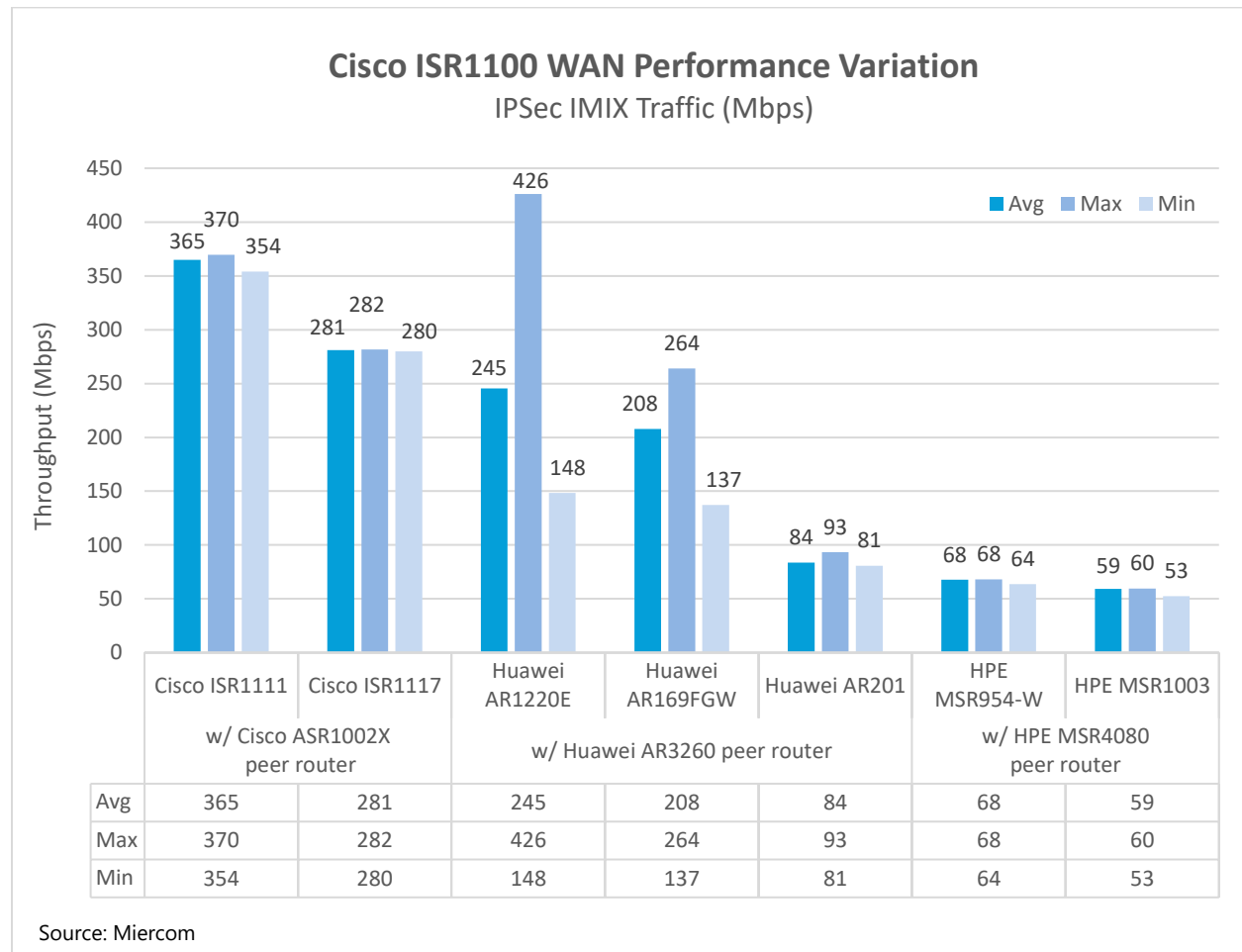
Figure 3: Cisco ISR1100 Competitive WAN Performance



The Cisco ISR1111-8P delivered the highest average maximum throughput of all the routers tested, 365 Mbps – 33 percent higher than its closest competitive product. Second was the Cisco ISR1117-4P, which delivered an average max throughput of 281 Mbps. Two of the Huawei branch-office routers, the AR1220E and the AR169GW-L, delivered good average max-throughput performance, 245 and 208 Mbps, respectively. The HP Enterprise branch-office routers tested, the MSR954-W and MSR1003, turned in much lower average max throughputs, with just 68 and 59 Mbps, respectively.

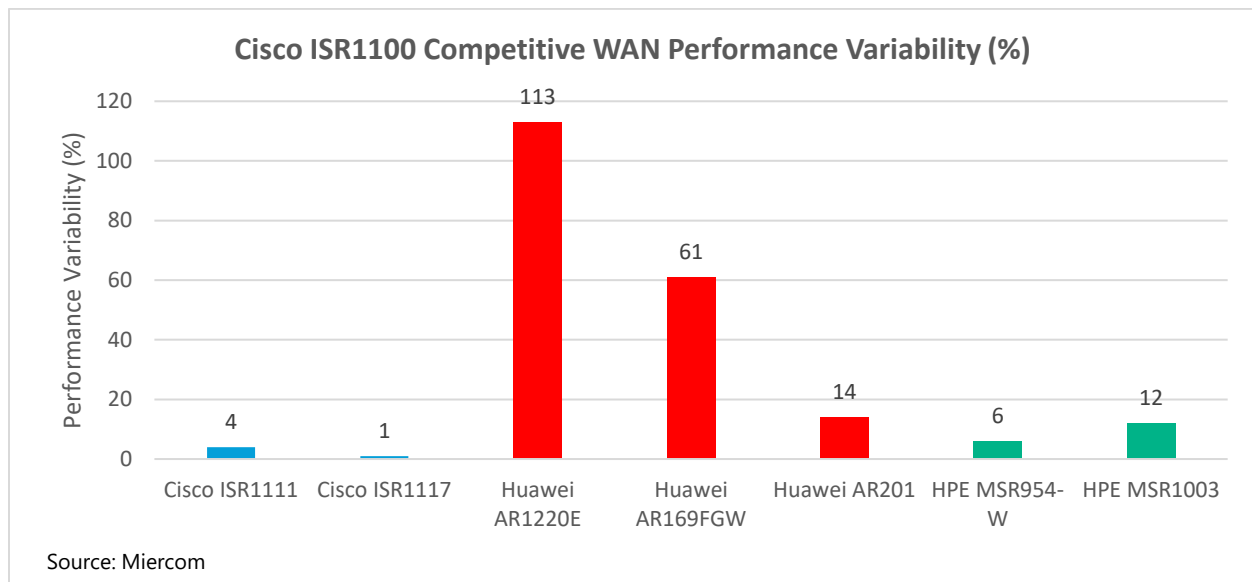
Branch office routers perform a lot of complex processing during these max-throughput-performance-over-WAN-link tests – I/O, buffering, table look-ups, queuing, forwarding, and encryption/decryption, to name a few. This is exacerbated with variable-sized packets, and with traffic approaching the overload point. Some variability from test run to test run is to be expected. But pointing the finger at the cause of such throughput variability is a difficult chore; it is likely a complex mix of factors.

Figure 4: Cisco ISR1100 Competitive WAN Average, Minimum and Maximum Performance



The chart above shows the average, minimum and maximum throughput of each router for the 20 test runs. We discovered in early performance testing that some routers, notably Huawei's two top performers, exhibited wide variation in maximum throughput.

Figure 5: Cisco ISR1100 Competitive WAN Performance Variability (%)



* Calculated as the min-max delta / avg throughput. Results rounded to nearest whole integer.

The Cisco routers' throughput variability was small, only about 1 to 4 percent. HPE's variability was a little more, 6 to 12 percent, still within the reasonable realm, especially since these are maximum-load throughputs. Variability with the Huawei routers was significant. Planning for traffic loads and flows becomes nearly impossible when the maximum throughput varies from 137 to 426 Mbps. In other words, with an average max throughput of 245 Mbps, the actual throughput realized could be 100 Mbps more or less, for reasons that for now remain unknown.

5.0 Wireless LAN Features and Ease of Use

The facilities, interfaces and processes offered for setting up and managing the wireless features of these branch-office routers.

Each router package was examined to learn what WiFi capabilities are integral or optionally offered. Then one by one, our engineers familiarized themselves with the interfaces and processes offered for setting up and administering each router's WiFi, using the vendor's documentation and on-line resources.

Results

The WiFi offerings embodied in the three vendors' branch-office routers are quite diverse. The below table compares and contrasts some of the key WiFi support differences. Not all the WiFi capabilities shown are available for all the other router models, including Cisco where the most basic ISR1100 models come without WiFi.

Table 1: Wireless Features and Ease of Use Comparison

	Cisco	Huawei	HPE
Built-in AP	Yes	Yes	Yes
Built-in Wireless LAN Controller	Yes, works concurrently with AP	Configured as a controller or AP, not both; restart required to switch modes	No; no built-in controller functionality; external controller required
IEEE 802.11ac support	Yes, latest Wave 2	802.11ac Wave 1	802.11n, 2.4 GHz only
Max APs controlled	50	12	Separate controller required
Additional cost per AP?	No	Yes; an additional license per AP is required	N/A
Wireless IPS (intrusion prevention system)	Yes	Limited (CLI only)	No
Multiple SSIDs	Yes	Yes	No
Application Visibility & Control	Built-in DPI engine. No licenses	Requires additional licenses	Extremely limited signature database (~200)

In our evaluation of the set-up, management and monitoring of WiFi, we concluded it is much easier and straightforward to perform for the Cisco routers than either Huawei or HP Enterprise. This is mainly due to a new Cisco WiFi architecture called Mobility Express. Below are our observations and notes of the vendors' WiFi configuration and management.

Huawei WiFi Configuration Process and Observations

These are the steps for WiFi configuration of the AP in Huawei routers:

1. Power up router; run basic router configuration (i.e., IP address, etc) via CLI
2. Enable the GUI (graphical user interface) for the router
3. Log into router's Web page and select mode of WiFi operation (built-in AP or limited controller functionality). Router will reboot while switching mode of WiFi operation
4. Configure Wireless Controller using Wizard
5. Configure SSID parameters using separate wizard
6. Configure device and user behavior using another wizard (generic settings for the entire router for user contracts, service profiles etc.)

Notes:

- There are various wizards for different configurations
- Enterprise features are noticeably absent
- Default settings are not useful (i.e., best practices are not implemented by default)
- Security features are limited (i.e., there is a limited, CLI-driven Wireless Intrusion Prevention System, WIPS)
- The GUI processes in general mirrors the CLI.

HP Enterprise WiFi Configuration Process and Observations

These are the steps for WiFi configuration of the AP in Huawei routers:

1. Power up router; Basic router configuration (i.e., IP address, etc) via CLI
2. Enable the GUI (graphical user interface) for the router
3. Log into router's Web page and navigate to LAN>WLAN configuration
4. Configure AP parameter (Frequency, channels, transmit power etc.)
5. Configure WLAN parameters (Only SSID name and password)

Notes:

- Very basic set-up; no advanced features; even some usual config options are absent
- Enterprise features (e.g. rogue/interferer detection, WIPS, multiple-SSID, Guests SSID/portal, AP groups, RF-profiles, user profiling, bandwidth contracts, application contracts) are noticeably absent
- No best practices settings are enabled by default
- Each AP (router) is configured as a standalone unit; there's no multi-AP control/ management.

Cisco WiFi Configuration Process and Observations

These are the steps for WiFi configuration of the AP in the Cisco routers:

1. Power up router; connect to “CiscoAirProvision” SSID. Default password is password.
2. Either from browser, access ‘mobility express’ URL: <http://mobilityexpress.cisco/screens/day0-config.html> or use ‘Cisco Wireless’ App from Apple or Android devices
3. Go through the set-up wizard; Confirm the settings (Mobility Express will automatically reboot)
4. Connect second and subsequent APs in the same Layer-2 domain. (The new AP will automatically join the Master AP as a subordinate AP).
5. Monitor and control wirelessly by connecting to the Master AP.

Notes:

- Best practices are enabled by default (good, practical settings are already input).
- WiFi controller and support for 50 APs are included and integral; no extra costs.
- Screens are intuitive (see below). Initial deployment is fast and simple.

Figure 6: Cisco Mobility Express: Integrated WiFi and AP Management Interface



Source: Miercom

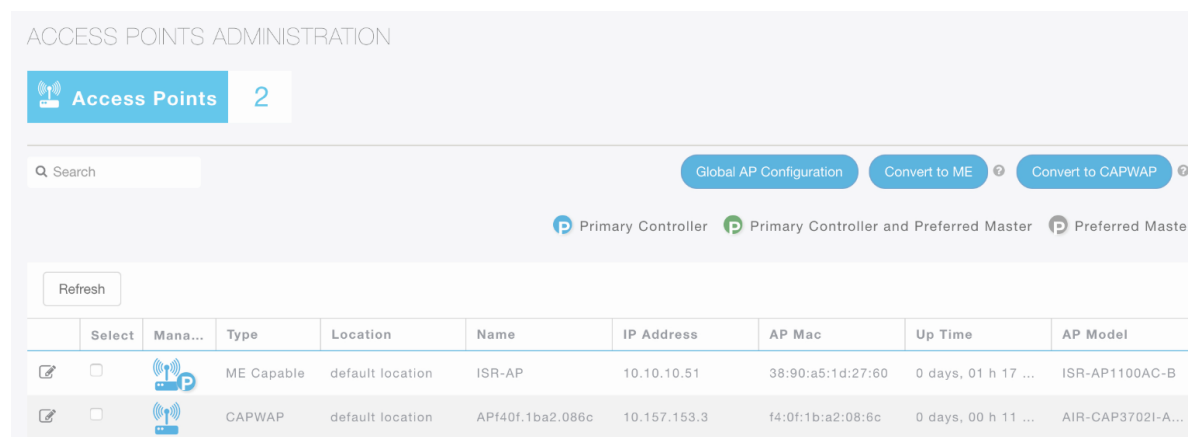
The Cisco Mobility Express single pane interface provides one-step access to the total WiFi picture.

From the top-level interface, the administrator can readily step down into functions including:

- Software upgrade
- AP / Radio Frequency details
- AP / Master Controller Configuration
- SSID configuration
- Local user management.

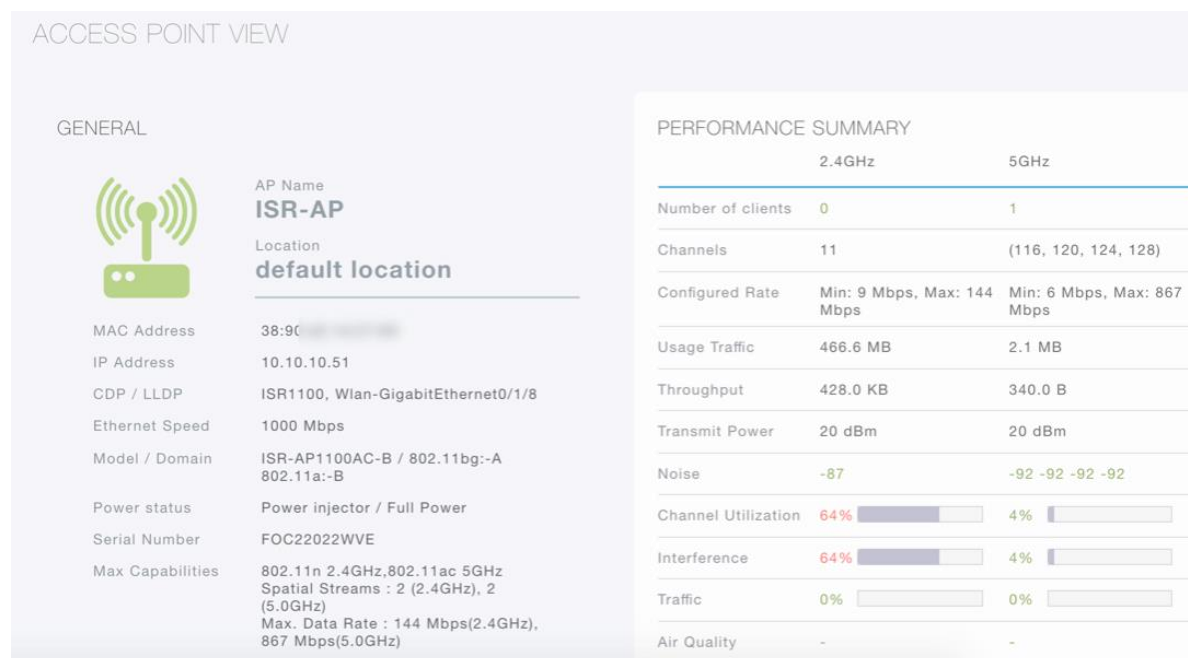
Some of the additional Cisco Mobility Express GUIs are shown below:

Figure 7: Cisco Mobility Express Access Point Management



Source: Miercom

Figure 8: Cisco Mobility Express Access Point Details



Source: Miercom

6.0 Security: Router Packet Inspection and Threat Analysis

This test examined the capabilities and tools offered to users for monitoring traffic and for identifying security threats and application usage. We examined each router for its forensic analysis capabilities and interfaces, including optional applications. Their ability to provide clear and accurate traffic analytics was comparatively assessed.

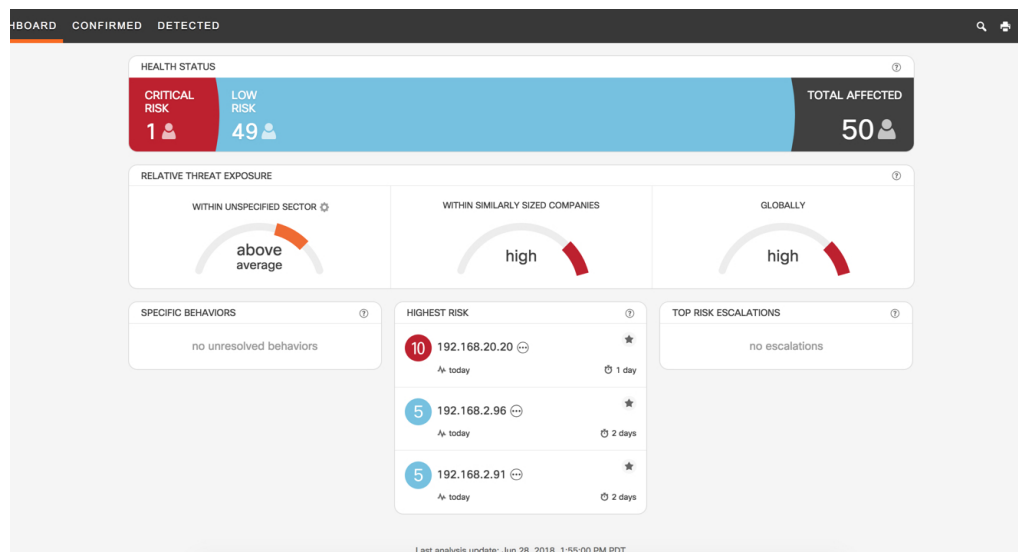
Results

The key to providing complete and accurate forensic data analytics is the ability to view all passing data. It is critical to see every packet to capture security threats like malware.

A key difference we found: Cisco's NetFlow can capture 100 percent of packets without compromising the routing performance and, using additional Cisco tools like Stealthwatch and AMP, provides a more complete view of applications in use and traffic types. This monitoring allows recognition and evaluation of possible threats, as well as continually updated templates to recognize new known threats or in-house policy changes.

By comparison, Huawei and HPE offer applications and capabilities including NetStream and sFlow. These capture on a sampling basis – at most just 1 packet of every 50 (a maximum of 2 percent of all packets). Subsequently, for threat analysis, the limited capture capability of Huawei and HPE means fewer threats will be recognized, from their signature catalog of known threats.

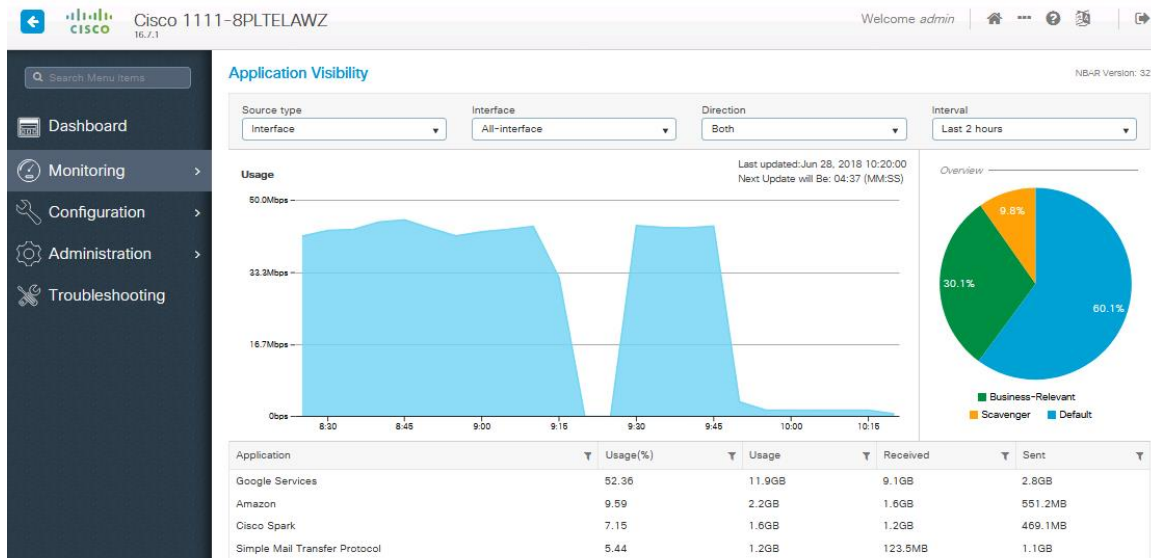
Figure 9: Cisco ISR1100 Health Status Dashboard



Source: Miercom

The dashboard gives a full view of risks and threats. A key differentiator for Cisco is its ability to detect inside encrypted traffic flows like HTTPS without compromising privacy. Besides threats, a graphical summary of application usage can be revealing.

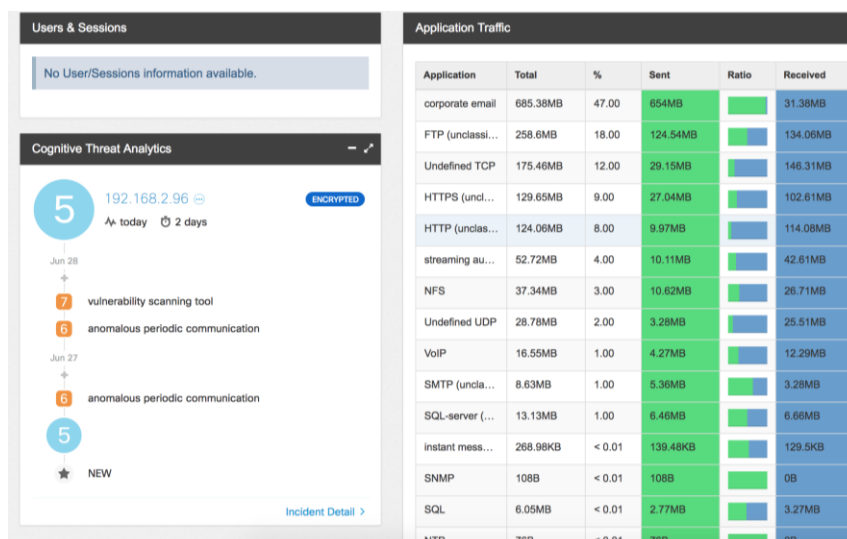
Figure 10: Cisco ISR1100: Application Visibility Monitoring



Source: Miercom

Application visibility monitoring lets the user keep a real-time eye on application usage, which may indicate internal policy problems or perhaps an outside incursion.

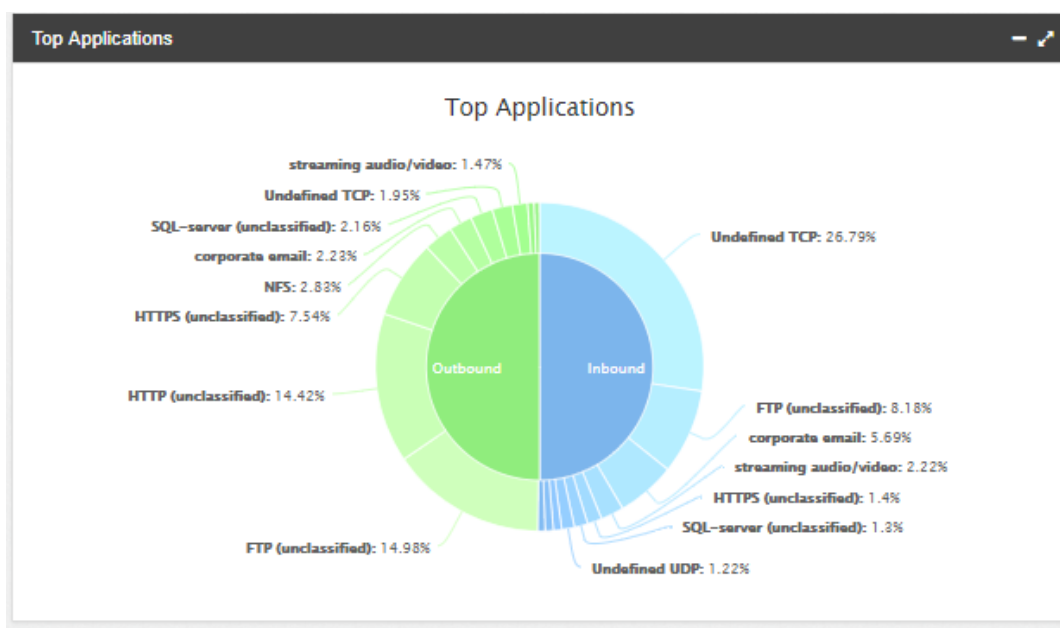
Figure 11: Cisco StealthWatch Application Risk Assessment



Source: Miercom

Expanding the StealthWatch application screen provides a risk assessment to highlight possible risks. A simple numeric indicator, in this case a "5," indicates a moderate vulnerability that may bear more watching and perhaps investigation going forward.

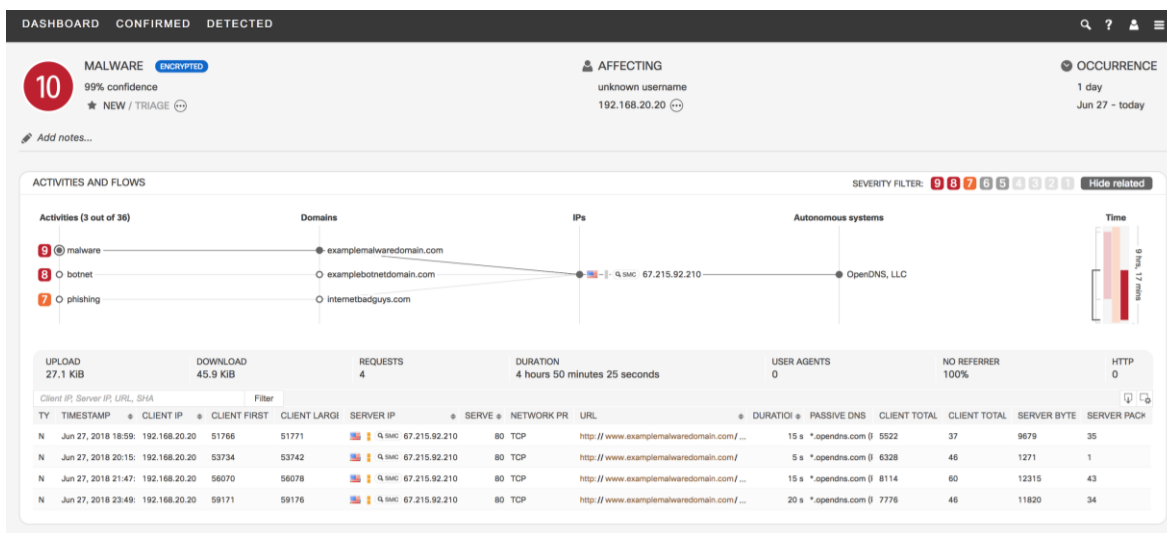
Figure 12: Application Monitoring



Source: Miercom

In this Application Monitoring view, application details are graphically shown. This screen shows the most used applications over time, a valuable metric for IT and network planning.

Figure 13: Malware Detection



Source: Miercom

In this view, Malware Detection tracks known malware on an ongoing basis and can readily identify traffic that matches the signatures of this malware. Here a malware attack has been identified with high confidence – along with indications of who is being attacked and where that attack originated.

7.0 Cisco SD-WAN: Tool for WAN Configuration and Management

A set of software features incorporated into the Cisco 1100 Series routers, which simplifies and facilitates the configuration of Software-Defined Wide Area Networks (SD-WANs). The SD-WAN package was developed by Viptela, which Cisco acquired in 2017.

Software-defined networking, or SDN, refers to a network approach that separates control and data planes, and provides centralized tools for simplified configuration management, service orchestration and monitoring. SD-WAN is the term applied to the package that Cisco has now incorporated into routers including the ISR1100 "edge," branch office routers.

Specifically, several key components of SD-WAN were exercised for this study:

- vManage – the SD-WAN management interface,
- Push updates on templates for policies,
- Secure shell (ssh) access to branch-router consoles,
- Two-step upgrades: upgrade and activate,
- vAnalytics – to provide access to the whole network's status, and
- Application-aware routing policies.

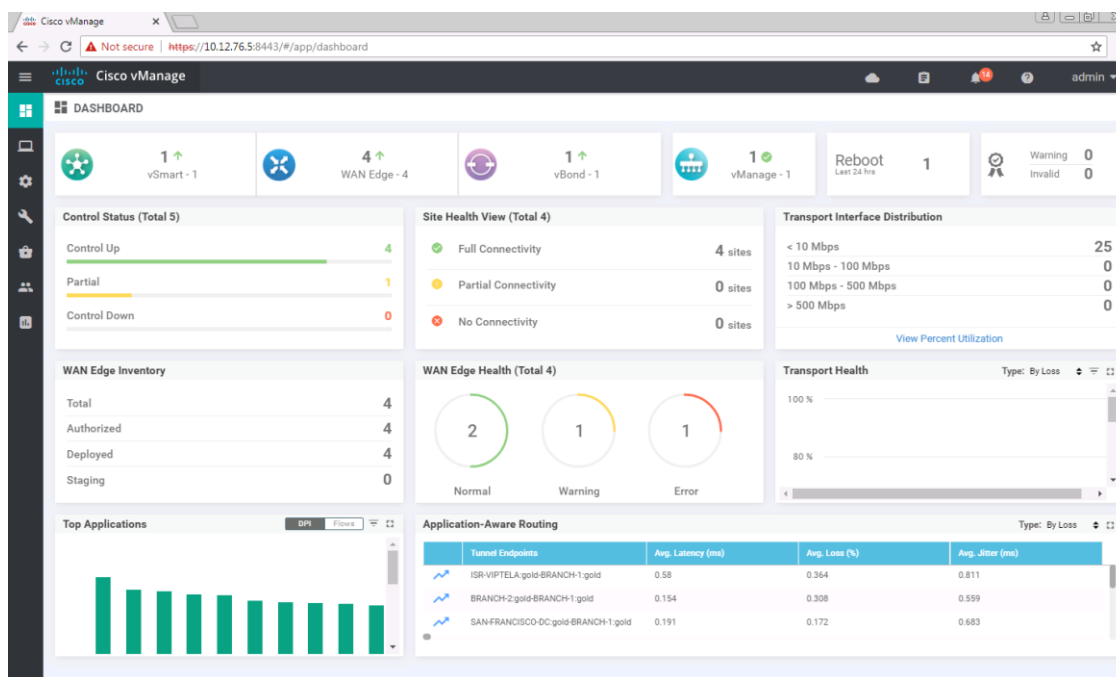
Results

Huawei and HPE both support configuration of complex WANs. But this is invariably done on these vendors' routers by correctly applying dozens, sometimes hundreds, of arcane CLI-like commands, a job normally entrusted to very highly trained, hard-to-find and expensive network specialists.

The Cisco SD-WAN software and router comprise a hardware appliance that sits at the perimeter of a site, such as remote office, branch office, campus, or data center. They participate in establishing a secure virtual overlay network over a mix of WAN transports. With SD-WAN the routers provide essential features of routing, forwarding, security, encryption, Quality of Service(QoS), policy and configuration management.

Cisco views the incorporation of features like SD-WAN as part of a transformation from an interconnected-hardware-centric network approach to a more business-centric model, focusing on the nature of business communications: Who needs to talk to whom and what functions do they need to perform.

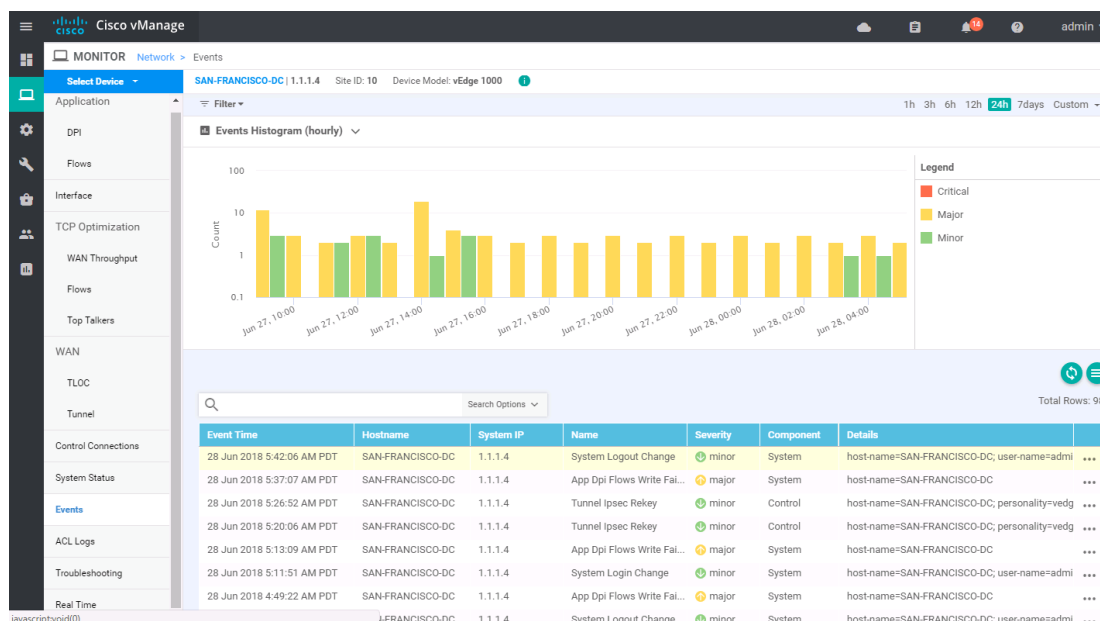
Figure 14: Dashboard View



Source: Miercom

The top-level vManage interface shows details of any particular applet of interest.

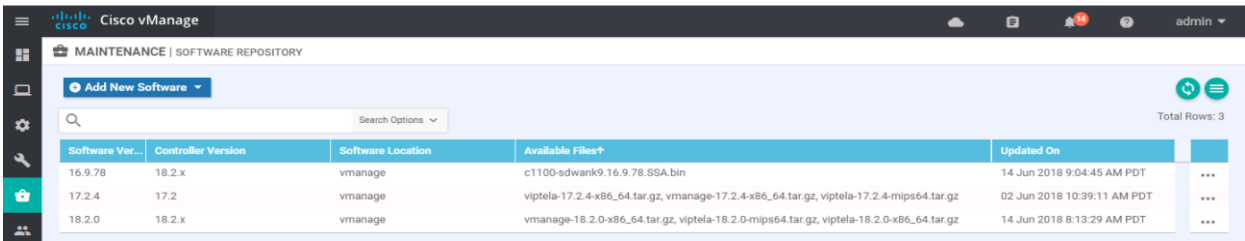
Figure 15: Events Histogram



Source: Miercom

This histogram of network events allows the user can drill down into any area for more detail.

Figure 16: Software Maintenance



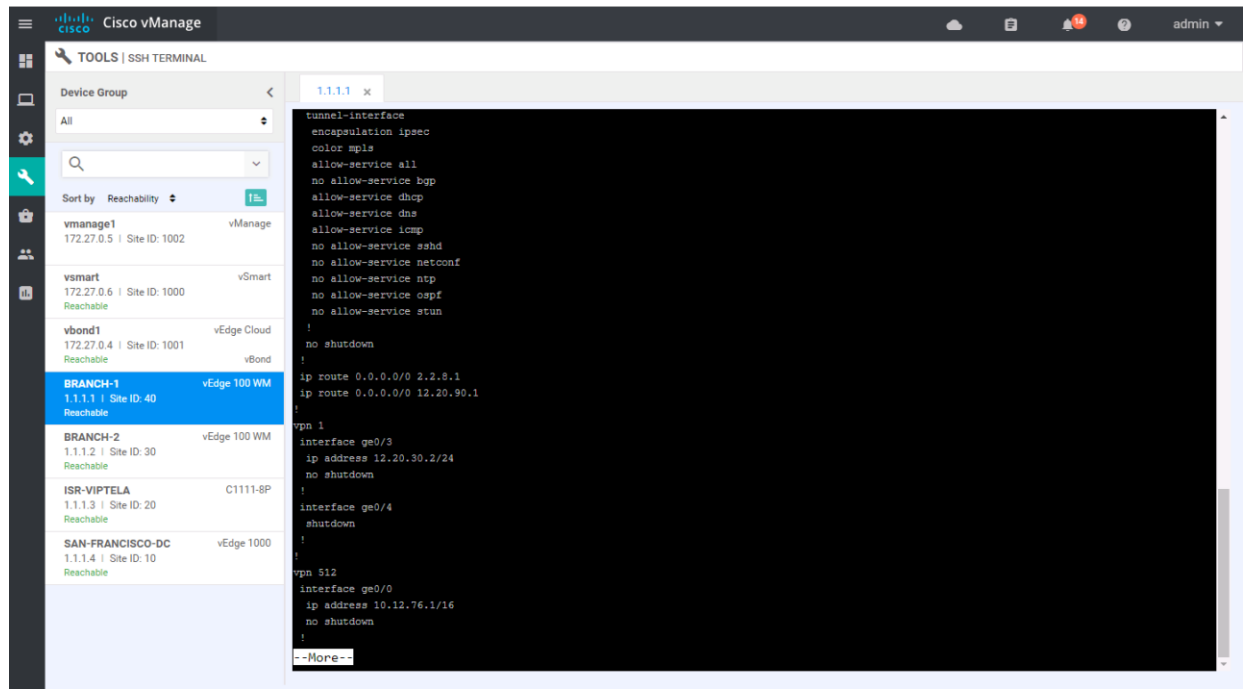
The screenshot shows the Cisco vManage 'MAINTENANCE | SOFTWARE REPOSITORY' page. It includes a search bar, a table of software versions, and a sidebar with navigation icons. The table lists software versions, controller versions, software locations, available files, and update dates.

Software Ver...	Controller Version	Software Location	Available Files†	Updated On
16.9.78	18.2.x	vmanage	c1100-sdwank9.16.9.78.SSA.bin	14 Jun 2018 9:04:45 AM PDT
17.2.4	17.2	vmanage	viptela-17.2.4-x86_64.tar.gz, vmanage-17.2.4-x86_64.tar.gz, viptela-17.2.4-mips64.tar.gz	02 Jun 2018 10:39:11 AM PDT
18.2.0	18.2.x	vmanage	vmanage-18.2.0-x86_64.tar.gz, viptela-18.2.0-mips64.tar.gz, viptela-18.2.0-x86_64.tar.gz	14 Jun 2018 8:13:29 AM PDT

Source: Miercom

Another component is access to the software repository, which shows software versions and when last updated.

Figure 17: Centralized Remote Management



The screenshot shows the Cisco vManage 'TOOLS | SSH TERMINAL' page. It features a sidebar with a list of devices and their reachability status, and a main terminal window displaying network configuration commands for a vEdge 100 WM device.

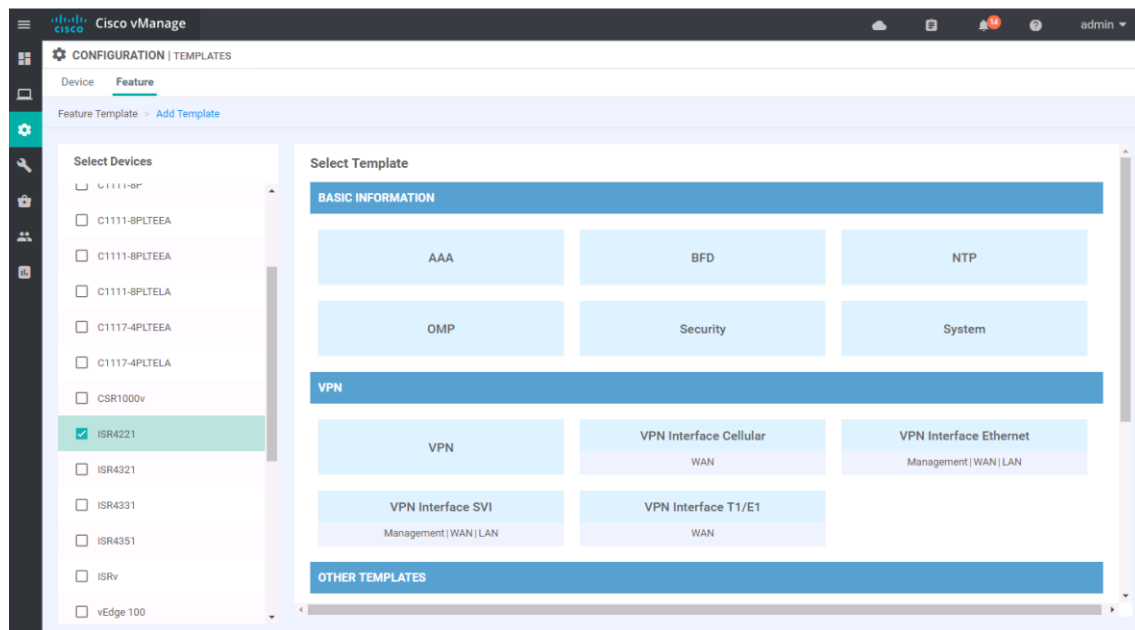
Device Group	Device Name	IP Address	Site ID	Reachability
All	vmanage1	172.27.0.5	1002	Reachable
	vsmart	172.27.0.6	1000	Reachable
	vbond1	172.27.0.4	1001	Reachable
	BRANCH-1	1.1.1.1	40	Reachable
	BRANCH-2	1.1.1.2	30	Reachable
	ISR-VIPTELA	1.1.1.3	20	Reachable
	SAN-FRANCISCO-DC	1.1.1.4	10	Reachable

```
tunnel-interface
encapsulation ipsec
color mpls
allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
!
no shutdown
!
ip route 0.0.0.0/0 2.2.8.1
ip route 0.0.0.0/0 12.20.90.1
!
vpn 1
interface ge0/3
ip address 12.20.30.2/24
no shutdown
!
interface ge0/4
shutdown
!
vpn 512
interface ge0/0
ip address 10.12.76.1/16
no shutdown
!
--More--
```

Source: Miercom

A recurrent problem for network management is accessing dozens of remote branch office routers. This interface provides centralized, quick secure shell (SSH) command-line access to any remote router.

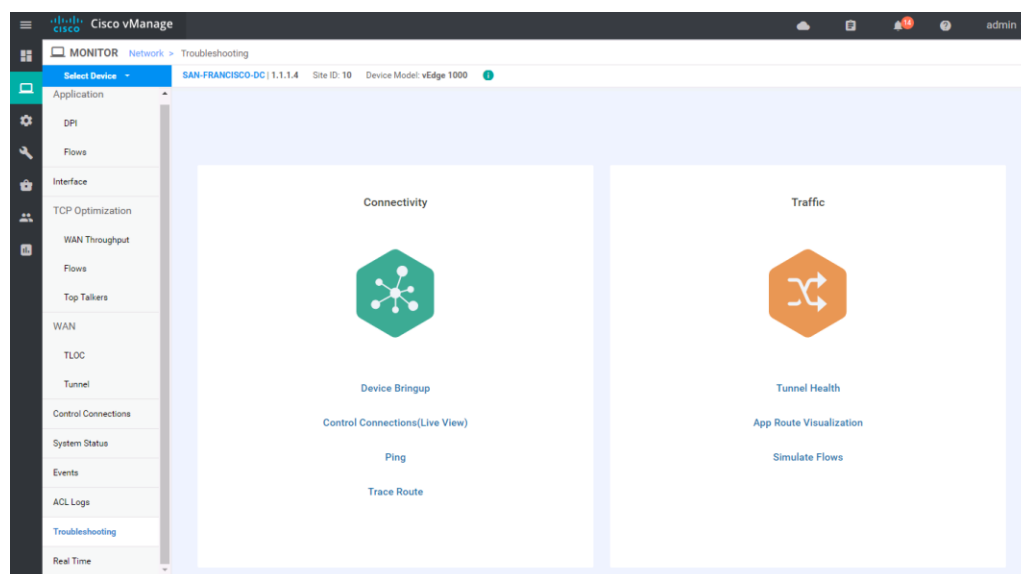
Figure 18: Configuration Templates



Source: Miercom

This interface is a real help to WAN router configuration. By selecting the appropriate template and the target router, the user can readily set the router's parameters for any WAN component – VPN, T1/E1, security, and a host of different protocols. This goes a long way to alleviating the complexity of today's software-defined WAN configurations.

Figure 19: Network Troubleshooting



Source: Miercom

This high-level network troubleshooting interface gives options on the left, and then drill-down points on the right, in this case based on connectivity or traffic.

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.

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.

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.