| USE CASE |

Assure High Quality End-User Experience Over Webex With NETSCOUT

The essence of business continuity is to mitigate corporate risk including keeping people productive during unplanned disruptions. Recent events have forced employees to work from remote sites and as a result, straining IT and collaboration services such as Cisco Webex and Microsoft Teams. Performance problems have erupted. What can the IT organization do to assure high-quality voice and video service delivery?

Two uses cases are described below. The first use case leverages nGeniusONE Service Assurance Platform to analyze Cisco Webex from full VPN users, i.e. remote users who must use a VPN for all their traffic. The second use case describes how nGeniusPULSE is used for visibility into the availability and responsiveness of the Webex service and into the bandwidth available to the internet for both VPN and non-VPN connections. While both use cases focus on Cisco Webex, the same NETSCOUT solutions can be used to isolate the root cause of voice and video quality problems for other collaboration services including Microsoft Teams.

Performance Issue

When packets are dropped using Webex Meetings, for any reason, it means that the voice and video quality are degraded. Remote users may connect in various ways, with some required to pass all their traffic across a VPN and others not. VPNs may be implemented differently, and remote users might have a soft telephony client available or may not. Peak usage times may lead to VPN infrastructure becoming saturated, and this can be the cause of call degradation as often as network issues.

Impact

When Webex is used and call degradation occurs, participants can become distracted from the business at hand, or worse, the meeting dissolves. Poor performance has painful cost consequences as well, including lost revenue, wasted time trying to identify and solve the problem, and reduced productivity.

Use Case 1: Visibility and Troubleshooting Webex for VPN-Based Users

Before the unplanned disruption forced employees to work remotely, they came together in physical meeting rooms on the enterprise campus. Now the IT organization must support people dispersed geographically and enable hundreds, if not thousands, of remote home offices to collaborate in real time. As a result, teams have come together using Webex.

- Employees in engineering and marketing are using full VPN to connect corporate resources, i.e. all their traffic flows over the VPN. The laptops of workers in marketing are configured to connect to VPN1, while workers in engineering connect to VPN2. (See Figure 1)

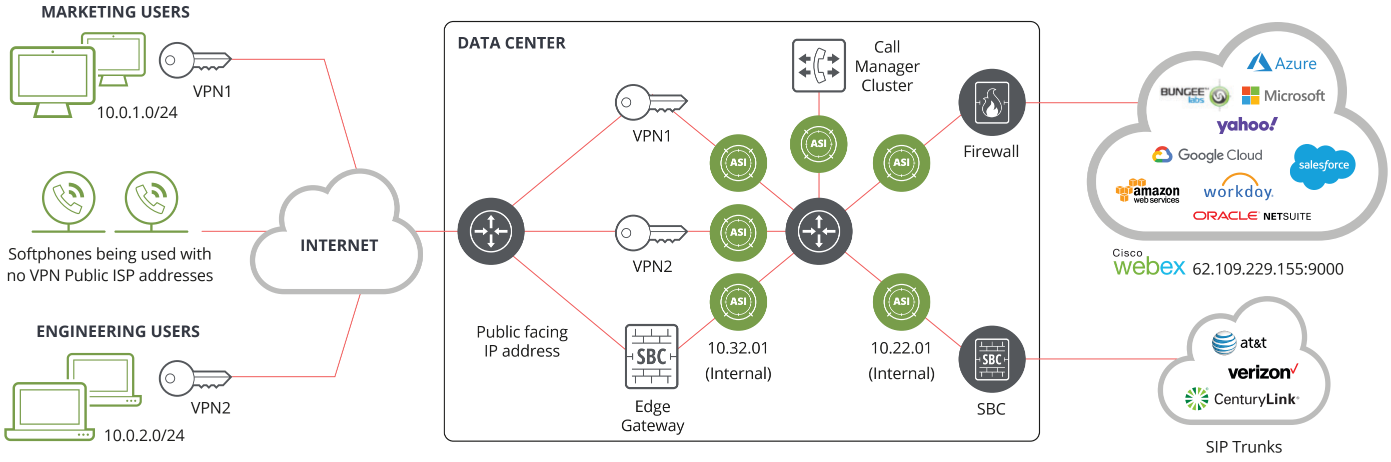


Figure 1: Two groups of remote workers using Webex over full VPN and some users using soft telephony clients over the internet. The green ASI icons show NETSCOUT monitoring locations.

- The computer audio feature built into the Webex client is used by all remote employees. However, they also have access to a soft telephony client, which can be used to make calls within the enterprise and to the PSTN. Calls from soft clients are managed by a call manager cluster located in the data center. Calls to the PSTN are routed to a SIP trunk by a session border controller (SBC). In addition to soft client calls made over the VPN connections, there are a small number of users who make calls from their soft telephony client when they are not connected to VPN. These calls enter the data center via an edge gateway and are then handled identically to calls made over a VPN connection.
- The engineering department is under strict instructions not to use video for Webex meetings, whereas the use of video for Webex meetings is ubiquitous within marketing. As a result, the infrastructure providing VPN1, is becoming saturated at peak hours, with the result that packets are dropped. This means that the voice and video quality of Webex meetings and telephony calls made from the marketing team are degraded.

How NETSCOUT Helps Assure Webex Performance

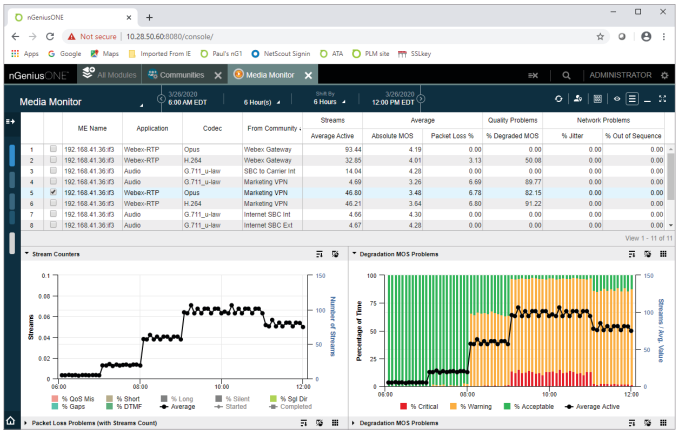
The nGeniusONE® Service Assurance platform with Adaptive Service Intelligence™ (ASI) technology provides rapid and clear insights based on rich analysis, metrics and views into applications, service enablers, server transactions, user communities, and the network. For this Webex use case, nGeniusONE offers top-down contextual workflows, reducing mean-time-to-knowledge to triage performance problems more quickly. NETSCOUT® instrumentation, including InfiniStreamNG® (ISNG) and vSTREAM™ software and hardware appliances, use the ASI technology to provide deeper visibility into the interactions of the many components of Webex and other services and applications.

The visibility provided by the ISNG appliance (note the ASI icon in Figure 1) at each of the VPN concentrator locations provides insight into how the VPN bandwidth is being used – for example, which corporate applications are being accessed and which common websites are being visited. The ISNG appliances also analyze the audio and video components of all Webex sessions, providing insight into the quality of the end-user experience being delivered along with detailed troubleshooting metrics.

The ISNG appliances also provide visibility of voice traffic at the SBC serving the SIP trunk and the edge gateway connected to the internet. Additionally, all SIP signaling traffic at the call manager cluster responsible for handling the soft clients is analyzed.

One way to improve troubleshooting efficiency is to use the Client Community feature in nGeniusONE to group related traffic together. Hence, all traffic coming over VPN1 and VPN2 is separately identified, along with the traffic flowing to and from the SBC, edge gateway and external Webex servers. This grouping provides critical visibility into the traffic flowing within the corporate network and the end-user experience of employees.

nGeniusONE Media Monitor. One of the powerful features of nGeniusONE is the "Media Monitor" view. The Media Monitor views in nGeniusONE are designed to allow problems to be rapidly identified, triaged and isolated. Figure 2 shows a screen shot from the Media Monitor with a filter applied to show the media traffic arriving from the marketing team.



		ME Name	Application	Codec	From Community	Streams	Average		Quality Problems	Network Problems	
						Average Active	Absolute MOS	Packet Loss %	% Degraded MOS	% Jitter	% Out of Sequence
1	□	192.168.41.36:if3	Webex-RTP	Opus	Webex Gateway	93.44	4.19	0.00	0.00	0.00	0.00
2	□	192.168.41.36:if3	Webex-RTP	H.264	Webex Gateway	32.85	4.01	3.13	50.08	0.00	0.00
3	□	192.168.41.36:if3	Audio	G.711_u-law	SBC to Carrier Int	14.04	4.28	0.00	0.00	0.00	0.00
4	□	192.168.41.36:if3	Audio	G.711_u-law	Marketing VPN	4.69	3.26	6.69	89.77	0.00	0.00
5	☑	192.168.41.36:if3	Webex-RTP	Opus	Marketing VPN	46.80	3.48	6.78	82.15	0.00	0.00
6	□	192.168.41.36:if3	Webex-RTP	H.264	Marketing VPN	46.21	3.64	6.80	91.22	0.00	0.00
7	□	192.168.41.36:if3	Audio	G.711_u-law	Internet SBC Int	4.66	4.30	0.00	0.00	0.00	0.00
8	□	192.168.41.36:if3	Audio	G.711_u-law	Internet SBC Ext	4.67	4.28	0.00	0.00	0.00	0.00

View 1 - 11 of 11

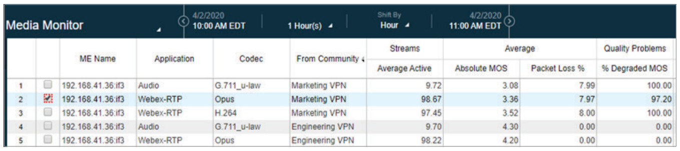
Figure 2: nGeniusONE Media Monitor showing voice traffic over a 14-hour period between 6am and 8pm. The Degradation MOS Problems graph shows the percentage of streams with a quality problem.

An application called "Webex-RTP" has been defined in nGeniusONE to label traffic to and from the Webex servers in the cloud. The traffic under the application name "Audio" is the VoIP traffic from the soft clients.

The voice component of Webex sessions is encoded with the OPUS codec; the soft telephone client traffic is encoded with the G.711 codec. Figure 3 shows a detail of the nGeniusONE Media Monitor table for the 9am to 10am busy hour showing that all traffic from the marketing VPN, i.e. Webex H.264 video, Webex Opus voice and Soft-client G.711 voice, has quality problems.

Inspection of the table in Figure 3 instantly shows that the engineering team is only generating audio traffic. Whereas, it can clearly be seen that the marketing team is also generating video traffic with the H.264 video codec. The Media Monitor table also shows that almost 100% of the RTP sessions coming from the marketing team VPN have degraded quality ("% Degraded MOS"), i.e. they are classified as Warning or Critical in the graph in Figure 2, due to an average packet loss of ~8%.

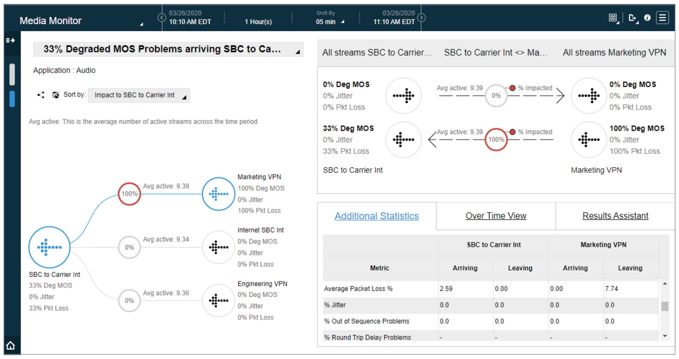
Even though Webex media traffic is transported using the encrypted SRTP protocol, ISNG appliances can analyze and measure metrics such as end-user experience (MOS), packet loss, jitter, along with several key performance indicators such as IP QoS marking problems, one-way calls, and short calls.



		ME Name	Application	Codec	From Community	Streams	Average		Quality Problems
						Average Active	Absolute MOS	Packet Loss %	% Degraded MOS
1	□	192.168.41.36:if3	Audio	G.711_u-law	Marketing VPN	9.72	3.08	7.99	100.00
2	☑	192.168.41.36:if3	Webex-RTP	Opus	Marketing VPN	98.67	3.36	7.97	97.20
3	□	192.168.41.36:if3	Webex-RTP	H.264	Marketing VPN	97.45	3.52	8.00	100.00
4	□	192.168.41.36:if3	Audio	G.711_u-law	Engineering VPN	9.70	4.30	0.00	0.00
5	□	192.168.41.36:if3	Webex-RTP	Opus	Engineering VPN	98.22	4.20	0.00	0.00

Figure 3: Detail of the nGeniusONE Media Monitor table for the 9am to 10am busy hour showing that all traffic from the marketing VPN, i.e. Webex H.264 video, Webex OPUS voice and Soft-Client G.711 voice, has quality problems.

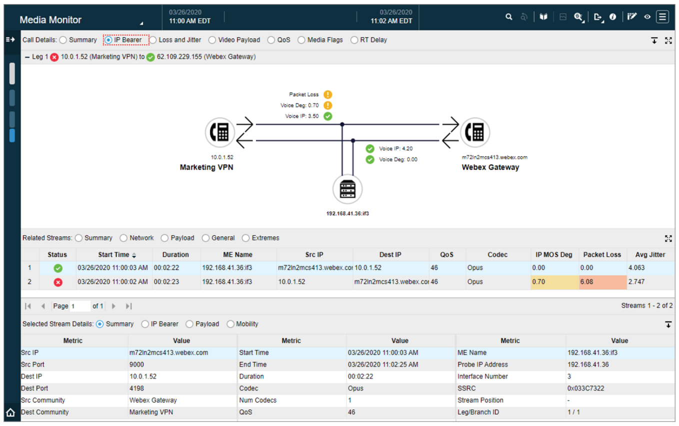
Further evidence that the Marketing VPN is degrading the quality of their media is found in the Media Monitor Conversation view. Figure 4 shows the view for all traffic seen at the SIP Trunk SBC. The pane on the left shows the source of all voice streams flowing towards the SIP trunk. It can clearly be seen that only the traffic from the marketing VPN is degraded. By contrast, the traffic from the engineering VPN and VoIP calls arriving at the Internet facing SBC have no problems.



	SBC to Carrier Int		Marketing VPN	
Metric	Arriving	Leaving	Arriving	Leaving
Average Packet Loss %	2.59	0.00	0.00	7.74
% Jitter	0.0	0.0	0.0	0.0
% Out of Sequence Problems	0.0	0.0	0.0	0.0
% Round Trip Delay Problems	-	-	-	-

Figure 4: nGeniusONE Media Conversation view showing which voice traffic going to the SIP trunk has degraded quality, in this case the traffic from the Marketing VPN is saturated by Webex video traffic.

nGeniusONE Individual Call View. nGeniusONE collects detailed metrics about RTP sessions and, in the case of internal voice and video calls, the SIP signaling. Figure 5 shows the nGeniusONE Individual Call view, which provides a visual summary of the health of a media session, in this case the audio component of a Webex session between a user on the Marketing VPN and the cloud-based Webex server. The purpose of this view is to provide a clear, visual summary of any issues, such as, the presence of packet loss coming from the Marketing VPN connection.


Media Monitor
03/26/2020
11:00 AM EDT
03/26/2020
11:02 AM EDT
Call Details: ○ Summary ● IP Bearer ○ Loss and Jitter ○ Video Payload ○ QoS ○ Media Flags ○ RT Delay
– Leg 1 ✕ 10.0.1.52 (Marketing VPN) to ✓ 62.109.229.155 (Webex Gateway)
Packet Loss !
Voice Deg: 0.70 !
Voice IP: 3.50 ✓
10.0.1.52
Marketing VPN
Voice IP: 4.20 ✓
Voice Deg: 0.00 ✓
m72ln2mcs413.webex.com
Webex Gateway
192.168.41.36:if3
Related Streams: ○ Summary ○ Network ○ Payload ○ General ○ Extremes
Page 1 of 1
Streams 1 - 2 of 2
Selected Stream Details: ● Summary ○ IP Bearer ○ Payload ○ Mobility

	Status	Start Time	Duration	ME Name	Src IP	Dest IP	QoS	Codec	IP MOS Deg	Packet Loss	Avg Jitter
1	✓	03/26/2020 11:00:03 AM	00:02:22	192.168.41.36:if3	m72ln2mcs413.webex.coı	10.0.1.52	46	Opus	0.00	0.00	4.063
2	✕	03/26/2020 11:00:02 AM	00:02:23	192.168.41.36:if3	10.0.1.52	m72ln2mcs413.webex.coı	46	Opus	0.70	6.08	2.747

Metric	Value	Metric	Value	Metric	Value
Src IP	m72ln2mcs413.webex.com	Start Time	03/26/2020 11:00:03 AM	ME Name	192.168.41.36:if3
Src Port	9000	End Time	03/26/2020 11:02:25 AM	Probe IP Address	192.168.41.36
Dest IP	10.0.1.52	Duration	00:02:22	Interface Number	3
Dest Port	4198	Codec	Opus	SSRC	0x033C7322
Src Community	Webex Gateway	Num Codecs	1	Stream Position	-
Dest Community	Marketing VPN	QoS	46	Leg/Branch ID	1 / 1

Figure 5: nGeniusONE Single Call view showing how the voice component of a Webex session from the Marketing team is degraded as it leaves the VPN.

Use Case 2: Visibility and Troubleshooting Webex for Non-VPN-Based Users

NETSCOUT has an approach to assure quality performance when an enterprise has employees that do not use VPN for Webex. Combined with nGeniusONE, nGenius®PULSE expands visibility by routinely and automatically monitoring applications and services for performance and availability, while also verifying the health of the underlying infrastructure that delivers those services. nGeniusPULSE uses hardware- and software-based active agents, called nPoints, to simulate user actions.

NETSCOUT nPoints can be configured to perform synthetic business transaction testing to a designated web service. They can also be configured to perform bandwidth tests to a specified iPerf reflector or between two nPoints. The results of the tests can be seen in the nGeniusPULSE application, and in nGeniusONE if the synthetic test traffic is sent over a VPN connection and therefore passes one or more locations in the data center monitored by an ISNG appliance.

Business Transaction Testing. The purpose of the business transaction testing is to establish if the target service, in this case Webex, is available and responsive. In addition to the network delay to the server, the test results shown in the nGeniusPULSE server provide a breakdown of the response time and any error codes for various phases of the server connection, including:

- DNS request
- TLS session handshake
- Navigate to enterprise.Webex.com
- Login to enterprise.Webex.com
- Start Webex meeting
- Wait in meeting
- End meeting
- Logout of Webex.com

Figure 6 shows nGeniusPULSE server results of Webex business transaction testing.

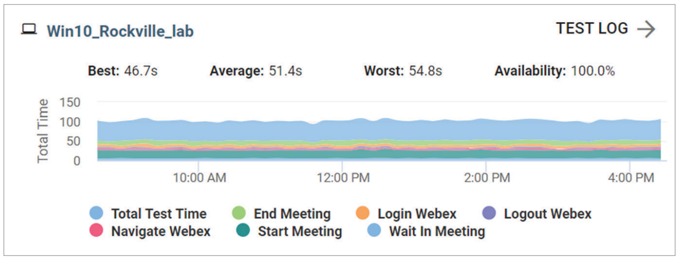
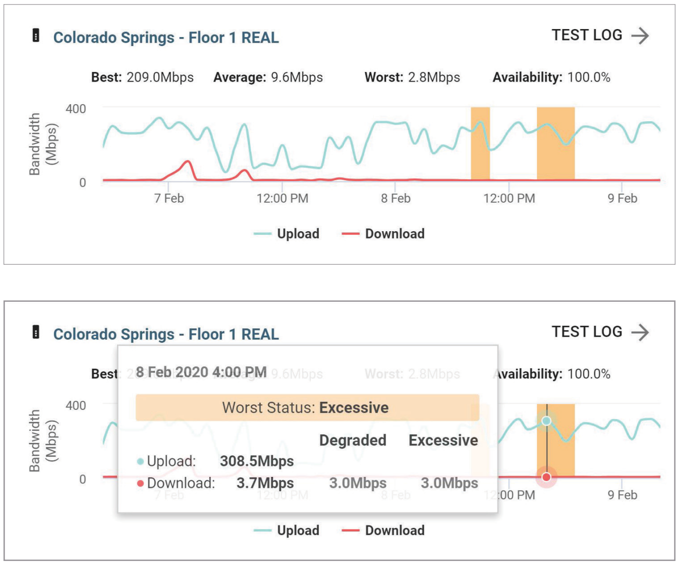


Figure 6: nGeniusPULSE server showing results of Webex business transaction testing.

If the traffic is also seen in the data center by an ISNG appliance, then nGeniusONE will show the delay between the client and the data center and the delay between data center and the Webex server, along with other detailed TCP statistics. Performing business transaction testing at regular intervals ensures that any degradation in the responsiveness of a service, or a complete outage, are detected quickly and can be reported to the service provider, e.g. Webex. In the case of collaboration services such as Webex, different geographical areas are serviced by different servers, hence it is advisable to deploy nPoints at multiple locations, including all geographies where employees are known to be working from.

Bandwidth Testing. nPoints can also perform bandwidth testing to a designated iPerf reflector, which is built into the nPoints or can be installed at any location on the Internet. Bandwidth tests can also be made between pairs of nPoints. The objective of bandwidth tests is to troubleshoot connection issues affecting specific remote workers, e.g. problems with the local Wi-Fi or the connection provided by their Internet Service Provider (ISP). Candidates for this type of testing include remote employees with repeated connection problems and VIP users, such as executives and users with mission-critical roles.

Since Webex is connected to the internet via major peering points, it is necessary that the iPerf reflector be installed at a location with a high-bandwidth internet connection, e.g. a co-location site or a public cloud availability zone. nGeniusPULSE bandwidth tests are shown in Figure 7.


Colorado Springs - Floor 1 REAL

Best: 209.0Mbps Average: 9.6Mbps Worst: 2.8Mbps Availability: 100.0%

8 Feb 2020 4:00 PM

Worst Status: Excessive

		Degraded	Excessive
Upload:	308.5Mbps		
Download:	3.7Mbps	3.0Mbps	3.0Mbps

Figure 7: nGeniousPULSE showing the results of bandwidth tests made to an iPerf reflector.

Remediation

NETSCOUT understands the complexity of collaboration services. With nGeniusONE and nGeniusPULSE, performance monitoring and analysis pinpointed Webex meeting problems. After identifying the root cause along the service delivery path, IT professionals can take remediation steps to assure the highest quality Webex user experience. That can include increasing bandwidth, optimizing endpoints, changing QoS settings, or reconfiguring Webex servers. In the cases described above, the obvious course of action would be to advise remote employees from the marketing team to refrain from using video until their VPN capacity can be increased.

Summary

NETSCOUT can help get people back to work quickly when there are unplanned disruptions. That includes assuring collaboration services with remote teammates and management. As the use cases demonstrate, NETSCOUT solutions can be used to monitor, analyze, and troubleshoot collaboration services such as Cisco Webex or Microsoft Teams. With NETSCOUT, the IT organization sees what is really going on in their complex environment so they can then take the right corrective action in real-time to keep the services available and at the highest performance and quality levels.

LEARN MORE

For further information about NETSCOUT Unified Communications and Collaboration solutions, please visit:

https://www.netscout.com/solutions/unified-communications-collaboration

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us