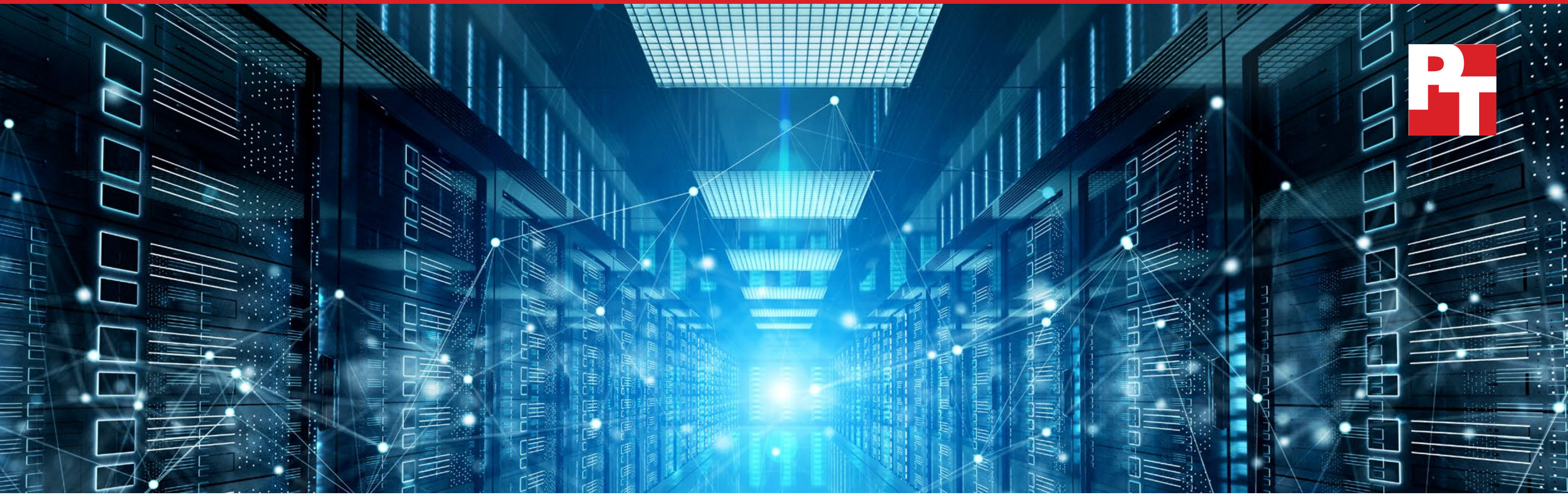
A Principled Technologies report: Hands-on testing. Real-world results.



Equinix Network Edge virtual network services demonstrated strong performance across several multi-cloud connectivity use cases

Multi-cloud and multi-vendor testing covered routing large numbers of UDP packets per second while also delivering high bandwidth with TCP packets

Organizations reaping the benefits of multi-cloud deployments can streamline even further by virtualizing networking between cloud deployments to place infrastructure closer to end-users and ensure top application performance. Network Edge provides virtual network services to help organizations unite infrastructure across multiple cloud vendors without traditional hardware-based networking as they add or acquire cloud instances.

We set up VMs on two different cloud platforms—Amazon Web Services (AWS) and Microsoft Azure—and used Network Edge to privately integrate virtual network services across both platforms. From numerous possible use cases, we selected three example virtual devices to complete three sets of tests: Cisco CSR 1000v with the AX software package, Versa FlexVNF, and Fortinet FortiGate VM Series. We found that Network Edge would be able to support up to 2,591 voice over IP (VoIP) sessions (based on routing up to 129K packets per second (PPS) in UDP tests with sub-0.005% packet loss) and provided strong throughput in TCP tests. Plus, we were able to deploy both Network Edge and order the high-speed private connections to the public clouds in only a few clicks, which improves time to value. These results show that Network Edge can provide virtual networking service in several use cases for organizations looking to offload network services and simplify their cloud infrastructure.

Routed up to

129K

packets per second which could support

2,591

VoIP sessions

Tested using Cisco CSR 1000v (IPBase) with UDP G.711 codec sized packets

Delivered up to

1,144.1 Mbps

bi-directional throughput

Tested using Fortinet FortiGate VM Series (IPSEC) with TCP 1350B

Virtualizing network services with Network Edge

Virtualizing networking is another step in the move to software-defined infrastructure. By using Network Edge to connect network services virtually—even across multiple cloud vendors—organizations can avoid some of the CAPEX costs and complexity that physical networking hardware adds to cloud-based services and realize a faster time to market.

According to Equinix, "Network Edge provides virtual network services that run on a modular infrastructure platform, optimized for instant deployment and interconnection of network services."[1] Network Edge provides such features as direct access with SSH and whitelisting flexibility, custom routing in CLI, VPN termination, and 256-bit IPSEC encryption.[2] Virtualizing with Network Edge can help organizations scale VPN capacity rapidly to enable their remote workforce, integrate cloud and IT services, and securely add new sites to an existing network as needed.

To learn more about Network Edge, visit https://www.equinix.com/services/edge-services/network-edge/.

Testing overview

Multi-cloud deployments have a lot to offer modern organizations, but typically require networking equipment to link them and ensure that workloads run seamlessly. In our tests, we set up instances in both AWS and Microsoft Azure and used Network Edge to privately provide virtual network services between them. We logged into the Cloud Exchange portal, and with just a few clicks deployed not only the Network Edge device itself, but ordered the high-speed private connections to the public clouds housing our target VMs.

We tested both UDP and TCP traffic bi-directionally using a common UDP codec packet size and two typical TCP payload sizes. Codecs, or coder-decoders, are "algorithms used to encode data, such as an audio or video clip" that must be decoded when played back.[3] The test sizes we used were:

- UDP (real-time, speedy apps, e.g., video conferencing, internet gaming)
  - G.711 (simulated), 218B: Widely used audio codec used for Voice Over IP (VoIP).
- TCP (secure apps, e.g., file transfers, email, websites)
  - 1350B TCP (Note: Max packet size is 1,500B; we ran the final stream at 1,350B due to inconsistent performance within AWS cloud at 1,500B)
  - Internet Mix (IMIX)

Because organizations have different security protocols in place, we completed tests two ways: 1) without IP security (IPBase) and 2) with IPSEC, a secure network protocol that utilizes virtual private network (VPN) encryption to keep data secure. Because encryption occurs through a VPN while transmitting the codecs, IPSEC test results reflect the overhead that encryption places on systems.

For our testing, we selected an example device from three categories: routers, SD-WAN, and firewalls. The devices we tested are examples of virtual network functions (VNFs) Equinix offers, which includes partners such as Cisco, Juniper, Palo Alto Networks, CloudGenix, Fortinet, Versa, and VeloCloud. Network Edge provides customers with virtualized network resources from the vendors they're used to. We performed three sets of tests using both IPBase and IPSEC, each set of tests using a different routing device: Cisco CSR 1000v virtual router, Versa FlexVNF SD-WAN, and Fortinet FortiGate VM Series Firewall. The following sections show the data we collected across these devices. For complete detail about how we set up and performed our tests, read the accompanying document, the science behind the report.

How Network Edge worked with the Cisco CSR 1000v virtual router device

According to Cisco, CSR 1000V Series routers such as the Cisco CSR 1000v we tested can "serve as a secure single-tenant router in a multitenant, shared-resource public cloud environment."[4] Please note that in our tests, we used a 1GB license, which placed boundaries on speeds; 10GB IPBase licenses are available and could make it possible to achieve higher rates.

In conjunction with the Cisco CSR 1000v, we found that Network Edge could support up to 2,591 simultaneous VoIP sessions[5] using the G.711 codec, as the solution routed up to 129,000 packets per second and stayed under the threshold of 0.005% packet loss. For TCP tests, Network Edge with the Cisco solution offered bandwidth ranging from 902 to 970 Mbps, showing that Network Edge united instances across clouds from multiple vendors while delivering fast transmission.

Hosting VoIP services across multiple cloud vendors

Both private companies and government are turning to cost-efficient, cloud-hosted VoIP services, with analysts predicting a 12 percent compound annual growth rate through 2025.[6] Organizations setting up call centers for surveys or other robust communication needs require assurance that hosting VoIP services across multiple clouds won't slow down connections.

If your organization is currently evaluating vendors for VoIP service across multiple clouds, our tests show that using Network Edge virtual network services with the Cisco CSR 1000v device to connect instances in AWS and Azure can reduce complexity while providing near-zero packet loss and strong PPS routing.

Table 1: Network performance statistics we gathered using various codecs and security protocols while testing Network Edge with the Cisco CSR 1000v virtual router. Source: Principled Technologies.

	Byte size and protocol (bi-directional)	Bandwidth (Mbps)	Packets per second (PPS)	Packet loss (%)
Cisco CSR 1000v (IPBase)	UDP G.711 218B	226.0	129,990	0.004050%
	TCP 1350B	970.9		
	TCP IMIX†	930.4		

	Byte size and protocol (bi-directional)	Bandwidth (Mbps)	Packets per second (PPS)	Packet loss (%)
Cisco CSR 1000v (IPSEC)	UDP G.711 218B	129.0	73,994	0.003355%
	TCP 1350B	931.0		
	TCP IMIX†	902.6		

† TCP IMIX testing ran using 12 simultaneous streams consisting of (7) at 64B, (4) at 512B, and (1) at 1,350B. Refer to the science for more details.

How Network Edge worked with the Versa FlexVNF SD-WAN device

Organizations seeking virtual wide area network (WAN) architecture might choose a Versa FlexVNF device that focuses on traffic shaping and traffic prioritization such as Versa FlexVNF SD-WAN. According to Versa Networks, "Versa FlexVNF SD-WAN reduces cost through WAN flexibility and simplifies operations with centralized provisioning, management, policy control and application visibility."[7]

In conjunction with the Versa FlexVNF SD-WAN device, we found that Network Edge could support up to 961 simultaneous VoIP sessions using the G.711 codec, as the solution routed up to 47,000 PPS and stayed under the threshold of 0.005% packet loss. This strong performance and low packet loss can reduce interruptions in voice calls, conferencing, and internet gaming. With Versa FlexVNF SD-WAN, Network Edge offered even stronger bandwidth than with the Cisco device, on both IPBase and IPSEC protocols, achieving between 974 and 1,953 Mbps.

Table 2: Network performance statistics we gathered using various codecs and security protocols while testing Network Edge with the Versa FlexVNF SD-WAN device. Source: Principled Technologies.

	Byte size and protocol (bi-directional)	Bandwidth (Mbps)	Packets per second (PPS)	Packet loss (%)
Versa FlexVNF (IPBase)	UDP G.711 218B	83.8	47,997	0.000600%
	TCP 1350B	1,941.3		
	TCP IMIX†	1,953.6		

	Byte size and protocol (bi-directional)	Bandwidth (Mbps)	Packets per second (PPS)	Packet loss (%)
Versa FlexVNF (IPSEC)	UDP G.711 218B	59.2	33,998	0.000875%
	TCP 1350B	1,104.5		
	TCP IMIX†	974.4		

Pushing virtualization even further to reduce complexity

Modern organizations have embraced virtualizing servers, storage, and more to reduce complexity and save on hardware purchases. But wide area networks that connect branch offices haven't changed much, and still run on outdated telecom networks and proprietary hardware.

Organizations looking to virtualize their networking can do so with Network Edge and a Versa FlexVNF SD-WAN device, which together provide a virtualized, cloud-native WAN experience offering strong performance for UDP codecs and TCP.

UDP and TCP: A primer

User Datagram Protocol, or UDP, is a transport layer protocol that doesn't require an end-to-end connection or verification of transmission. Real-time apps where speed and timing are a priority, like video conferencing or computer gaming, use UDP.

Transmission Control Protocol, or TCP, is more reliable than UDP and requires three-way handshakes and verification that packets are transmitted and received at a destination with no errors, in the correct order. As such, TCP requires more overhead. Web sites, file transfers, and email, all of which require reliability but rely less on timing, use TCP.

† TCP IMIX testing ran using 12 simultaneous streams consisting of (7) at 64B, (4) at 512B, and (1) at 1,350B. Refer to the science for more details.

How Network Edge worked with the Fortinet FortiGate VM Series device

Organizations that seek to virtualize networking and require an additional security focus may be interested in Network Edge with a Fortinet FortiGate VM Series device. According to Fortinet, "Next-generation firewalls filter network traffic to protect an organization from external threats. Maintaining features of stateful firewalls such as packet filtering, VPN support, network monitoring, and IP mapping features, NGFWs also possess deeper inspection capabilities that give them a superior ability to identify attacks, malware, and other threats."[8]

With the Fortinet FortiGate VM Series device, we found that Network Edge could support up to 720 simultaneous VoIP sessions using the G.711 codec, as the solution routed up to 35,000 PPS and stayed under the threshold of 0.005% packet loss. Network Edge again provided strong bandwidth during TCP testing, ranging from 964 to 1,940 Mbps. These results show that organizations with high security needs that use Fortinet with their multi-cloud deployments can virtualize further by adding Network Edge.

Secure websites give consumers confidence to make purchases

Hosting applications that handle sensitive information—be it government data, health data, or financial data—have different security concerns than companies offering VoIP services. They require strong bandwidth for encrypted TCP traffic to ensure that this vital data is protected in flight and at rest.

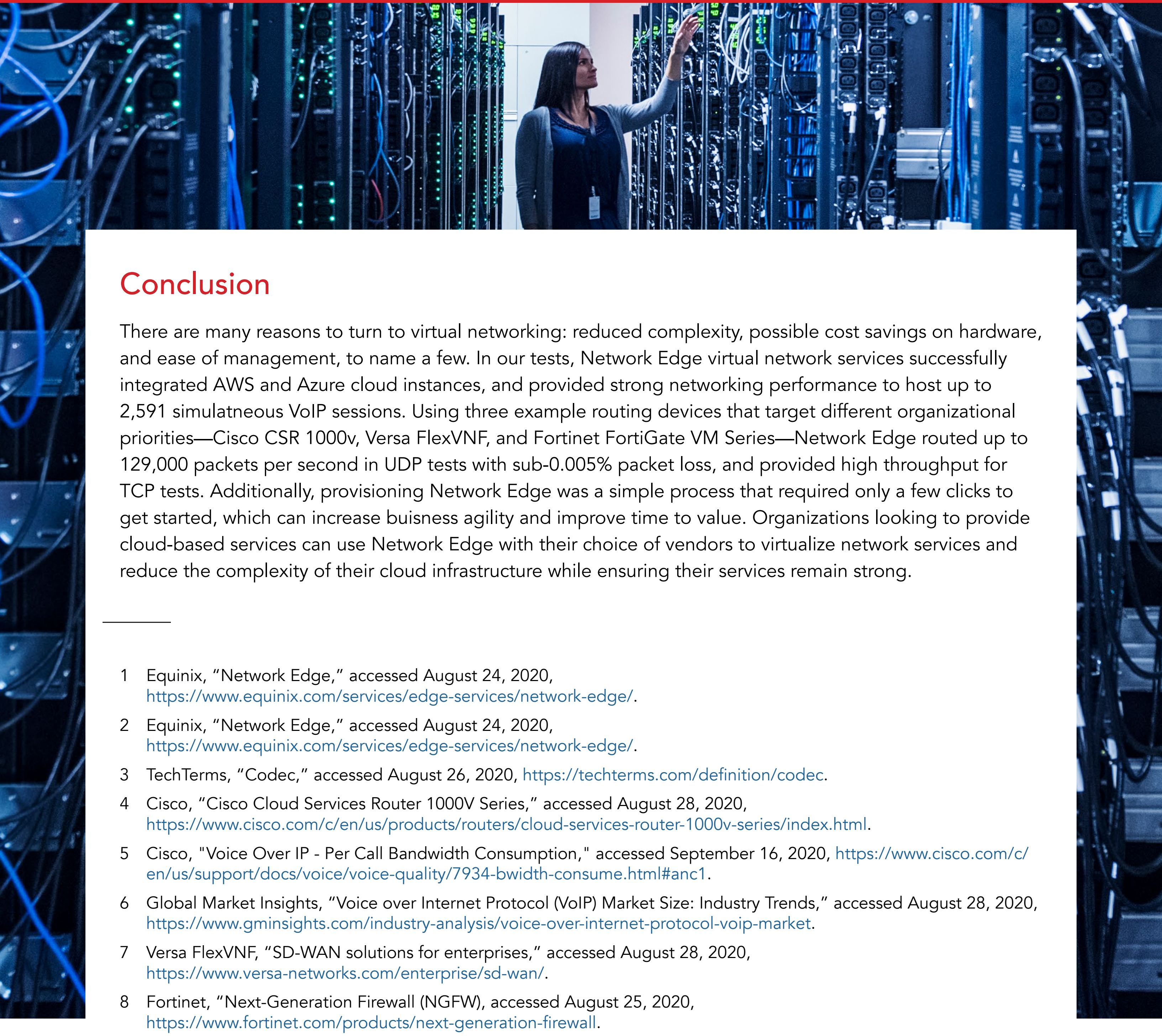
Network Edge and Fortinet Firewall devices together can provide additional security and fast performance while also reducing complexity by virtualizing network services.

Table 3: Network performance statistics we gathered using various codecs and security protocols while testing Network Edge with the Fortinet FortiGate VM Series device. Source: Principled Technologies.

	Byte size and protocol (bi-directional)	Bandwidth (Mbps)	Packets per second (PPS)	Packet loss (%)
Fortinet FortiGate VM Series (IPBase)	UDP G.711 218B	62.8	35,998	0.000260%
	TCP 1350B	1,921.0		
	TCP IMIX†	1,940.5		

	Byte size and protocol (bi-directional)	Bandwidth (Mbps)	Packets per second (PPS)	Packet loss (%)
Fortinet FortiGate VM Series (IPSEC)	UDP G.711 218B	87.2	49,994	0.002000%
	TCP 1350B	1,144.1		
	TCP IMIX†	964.0		

† TCP IMIX testing ran using 12 simultaneous streams consisting of (7) at 64B, (4) at 512B, and (1) at 1,350B. Refer to the science for more details.



Conclusion

There are many reasons to turn to virtual networking: reduced complexity, possible cost savings on hardware, and ease of management, to name a few. In our tests, Network Edge virtual network services successfully integrated AWS and Azure cloud instances, and provided strong networking performance to host up to 2,591 simulatneous VoIP sessions. Using three example routing devices that target different organizational priorities—Cisco CSR 1000v, Versa FlexVNF, and Fortinet FortiGate VM Series—Network Edge routed up to 129,000 packets per second in UDP tests with sub-0.005% packet loss, and provided high throughput for TCP tests. Additionally, provisioning Network Edge was a simple process that required only a few clicks to get started, which can increase buisness agility and improve time to value. Organizations looking to provide cloud-based services can use Network Edge with their choice of vendors to virtualize network services and reduce the complexity of their cloud infrastructure while ensuring their services remain strong.

[1] Equinix, "Network Edge," accessed August 24, 2020, https://www.equinix.com/services/edge-services/network-edge/.

[2] Equinix, "Network Edge," accessed August 24, 2020, https://www.equinix.com/services/edge-services/network-edge/.

[3] TechTerms, "Codec," accessed August 26, 2020, https://techterms.com/definition/codec.

[4] Cisco, "Cisco Cloud Services Router 1000V Series," accessed August 28, 2020, https://www.cisco.com/c/en/us/products/routers/cloud-services-router-1000v-series/index.html.

[5] Cisco, "Voice Over IP - Per Call Bandwidth Consumption," accessed September 16, 2020, https://www.cisco.com/c/en/us/support/docs/voice/voice-quality/7934-bwidth-consume.html#anc1.

[6] Global Market Insights, "Voice over Internet Protocol (VoIP) Market Size: Industry Trends," accessed August 28, 2020, https://www.gminsights.com/industry-analysis/voice-over-internet-protocol-voip-market.

[7] Versa FlexVNF, "SD-WAN solutions for enterprises," accessed August 28, 2020, https://www.versa-networks.com/enterprise/sd-wan/.

[8] Fortinet, "Next-Generation Firewall (NGFW), accessed August 25, 2020, https://www.fortinet.com/products/next-generation-firewall.

Read the science behind this report at http://facts.pt/A6StLc0 ▶

Principled Technologies®

Facts matter.®

Principled Technologies is a registered trademark of Principled Technologies, Inc.
All other product names are the trademarks of their respective owners.
For additional information, review the science behind this report.

This project was commissioned by Equinix.