dispersive®

DISPERSIVE® VIRTUALIZED NETWORK

Standard approaches to networking all have one crucial flaw in common: they all use a single path to transfer data. To avoid this single point of compromise and congestion, a Dispersive® Virtualized Network does things differently.

I. INTRODUCTION

In theory, the Internet offers enterprises a universal and comparatively inexpensive way to connect users, devices and sites. In practice, the Internet falls short of this promise: security risks abound[1] and the 'best effort' nature of the Internet causes less-than-acceptable application performance in many parts of the world.[2]

This paper describes how a Dispersive® Virtualized Network (Dispersive® VN), more than any other software solution, overcomes the deficiencies of Internet communications.

Section II introduces the concept of a Dispersive® VN and details the techniques a Dispersive® VN employs to simultaneously optimize security and performance.

Section III provides an overview of how this approach compares with alternatives and presents test data from a third-party evaluator to validate performance improvement claims.

Section IV concludes the paper with a review of the benefits Dispersive® VN provides to our communications service provider (CSP) partners.

AUTHORS

Douglas V. Dimola

Delia J. Smith, Dispersive Networks
Vice President, Product and Marketing

[1] Verizon. *2017 Data Breach Investigations Report*. April 2017.

[2] Bjarne Munch and Danellie Young. *How to Architect Your Internet Services for Best Performance*, (ID: G00319889). March 22, 2017. Retrieved from Gartner Database.

II. DISPERSIVE® VN OVERVIEW

Dispersive® VN Components

A Dispersive® VN comprises software components that collaborate and route traffic to significantly enhance network speed, security and reliability. These components are:

Controller. Server-based network management system that hosts the trusted peer database and authenticates all network components and their services.

Deflect. Software that relays traffic between clients or edge endpoints, acting as a waypoint within the network. This is the mechanism by which a Dispersive® VN establishes multiple, independent paths.

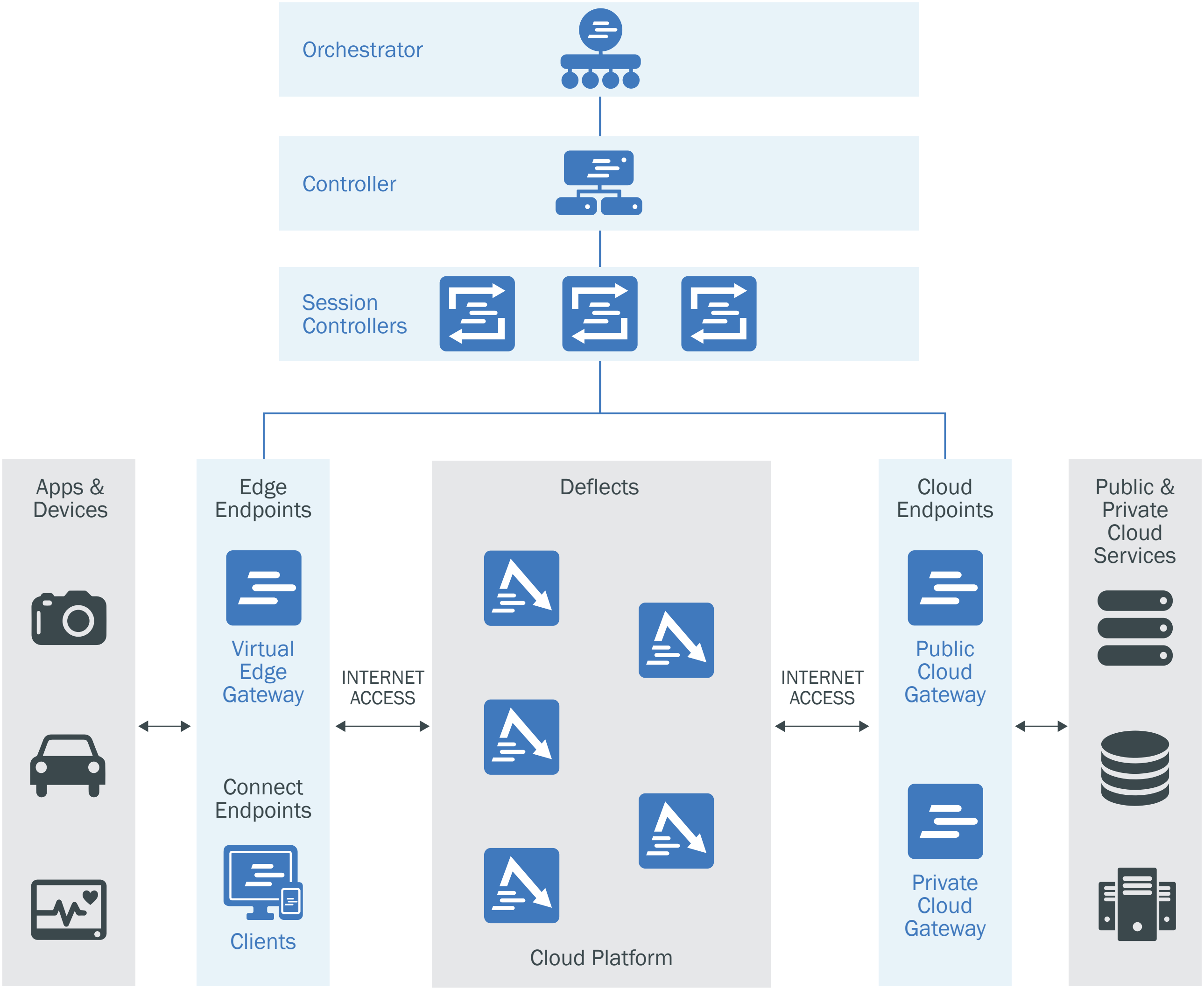
Endpoint app. Software that resides at the network access layer, enabling an edge device to send and receive data via a Dispersive® VN. Installs on most commodity hardware, including mobile phones, laptops, servers, and certain Internet of Things devices that have an OS and are IP enabled.

Orchestrator. Browser-based user interface tool installed on the controller and used to administer a Dispersive® VN.

Session controllers. Software that confirms two endpoints are allowed to communicate, establishes communication protocols for each session, and notifies the destination to initiate a call out.

Figure 1 shows these components in a sample network diagram.

Figure 1: Dispersive® VN Sample Network Diagram



The Dispersive® Virtualized Network

A Dispersive® VN is a carrier-grade, software-defined network that overlays the Internet. It virtualizes networking and routes traffic in ways that overcome some of the limitations of the Internet such as path congestion induced packet loss, latency, and jitter.

Dispersive's endpoint app installs on edge devices. When an application launches an Internet session, Dispersive's endpoint app intercepts the packet stream at Layer 2, 3, or 4. The endpoint app then communicates with the session controllers, which tell the source and destination which deflects to use. Once edge endpoints call out to the deflects, the app on the source device splits the single packet stream into multiple, non-duplicated packet streams, applies security rules, and sends each stream on a different, independent Internet path using deflects as intermediate waypoints.

On the destination device, the endpoint app receives the streams, authenticates the transmission, decrypts the packets and begins reassembly. If the app detects a bad or missing packet, it asks the source to retransmit only that packet on a new path. Upon receipt, the endpoint app puts the packet in the appropriate position before presenting the stream to the application. This all occurs without application awareness or active participation: Dispersive's application acceleration and performance-enhancing proxy techniques allow the application to operate with reduced packet loss, mitigating the effects of latency on the application.

Figure 2 illustrates the steps a Dispersive® VN follows when endpoints are communicating.

III. COMPARISON BETWEEN DISPERSIVE® VN AND LEGACY NETWORKS

Legacy networks rely on only one path to transfer data. That presents serious problems.

If that path degrades, data packets are lost. If the path is congested, transfer speeds slow and connections drop. If that one path is hacked, all data is compromised.

A Dispersive® VN replaces one-path networks with a solution that divides packet streams into multiple independent streams. It then sends each stream down its own independent path. No one path carries all the data. And streams can automatically change paths if necessary.

It's a software-defined network that conquers the security AND performance problems associated with the Internet.

A Dispersive® VN Improves Security

The "defense in motion" philosophy behind a Dispersive® VN makes IP-based communications more secure than ever. These security features include:

Shifted attack surface. By forcing endpoint devices to call out to network deflects rather than to each other, a Dispersive® VN moves the attack surface outside the enterprise network. It also eliminates the need to create static holes in your firewall to host services and facilitate connections.

Software-defined perimeter. The Dispersive® VN uses off-network, two-factor authentication and authorizes devices and users before granting them access to network services. The approach allows enterprises to virtually air gap devices, applications and users to enhance data protection.

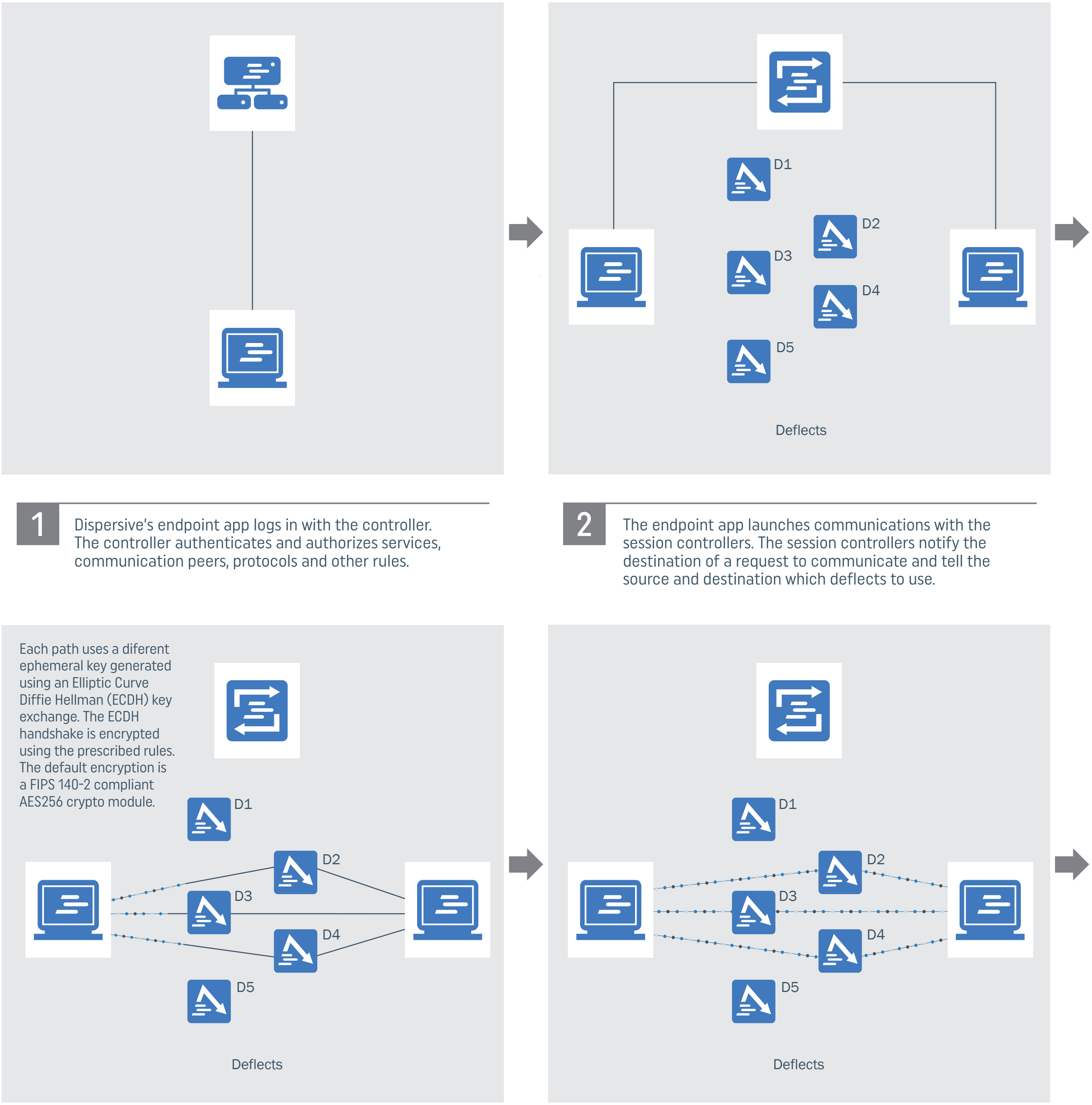
Unattributable networking. To confound hackers, a Dispersive® VN can hop across any range of ports and mask points of origin and destination by veiling IP addresses, ports and geographic operations.

Industry-standard encryption. Dispersive® VNs use very fast, industry-standard ephemeral AES 256-bit encryption for each path.[3] The encryption keys for each path are generated on the fly by the endpoints. These keys are only known to the endpoints—deflects neither know nor store the keys. Keys are generated every time a path changes or when a time limit is reached.

In addition, Dispersive® VNs thwart man-in-the-middle attacks because an individual path is only used for a few minutes and only contains a fraction of the traffic.

[3] Standard encryption modules are FIPS-140-2 compliant, with accreditation dates of: February 22, 2014; September 18, 2015; and February 26, 2016. See: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2014.htm#2081

Figure 2: Packet Flow in a Dispersive® Virtualized Network



1 Dispersive's endpoint app logs in with the controller. The controller authenticates and authorizes services, communication peers, protocols and other rules.

2 The endpoint app launches communications with the session controllers. The session controllers notify the destination of a request to communicate and tell the source and destination which deflects to use.

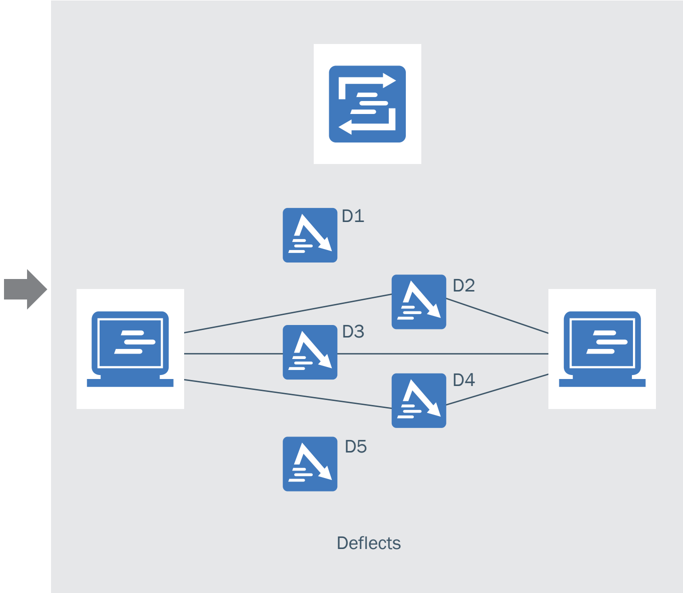
Each path uses a diferent ephemeral key generated using an Elliptic Curve Diffie Hellman (ECDH) key exchange. The ECDH handshake is encrypted using the prescribed rules. The default encryption is a FIPS 140-2 compliant AES256 crypto module.

5 The endpoint app on the **source** device:

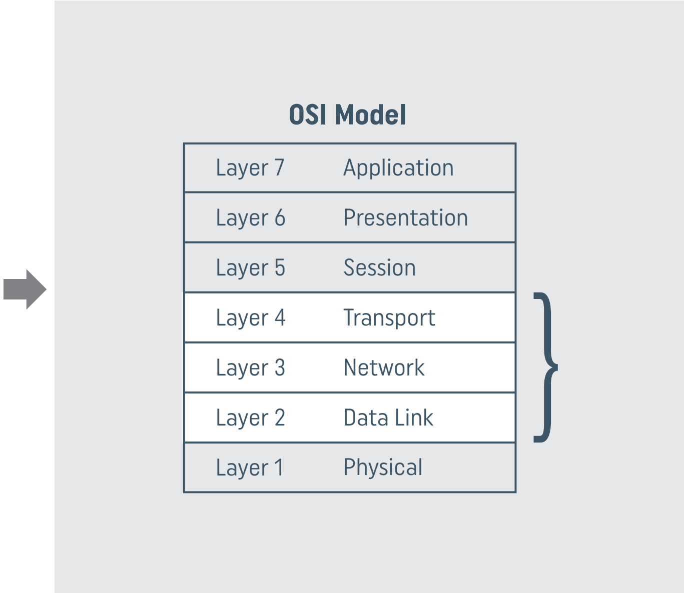
- Divides session-layer IP traffic into smaller, non-duplicated packet streams
- Applies security rules to each stream
- Sends each packet stream along a different, independent path by using deflects as intermediate waypoints

6 The endpoint app on the **destination** device:

- Receives the streams
- Authenticates each packet
- Decrypts the packets
- Reassembles the original packet stream



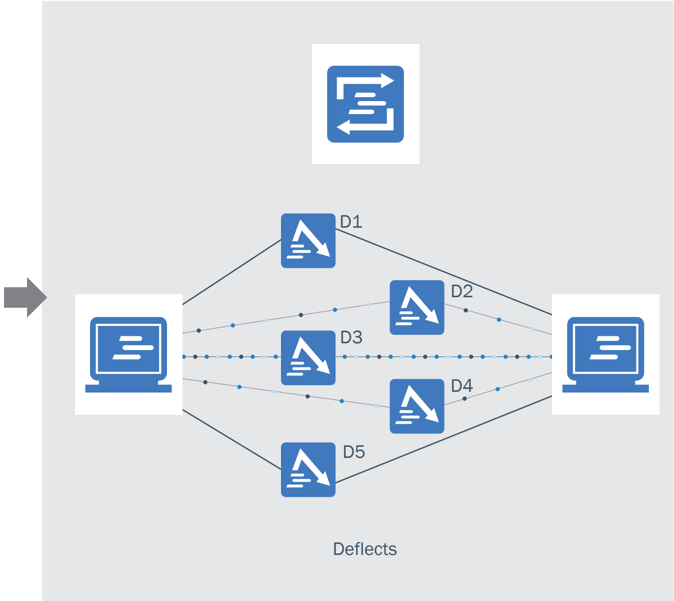
3 The edge endpoints call out to the deflects.



OSI Model

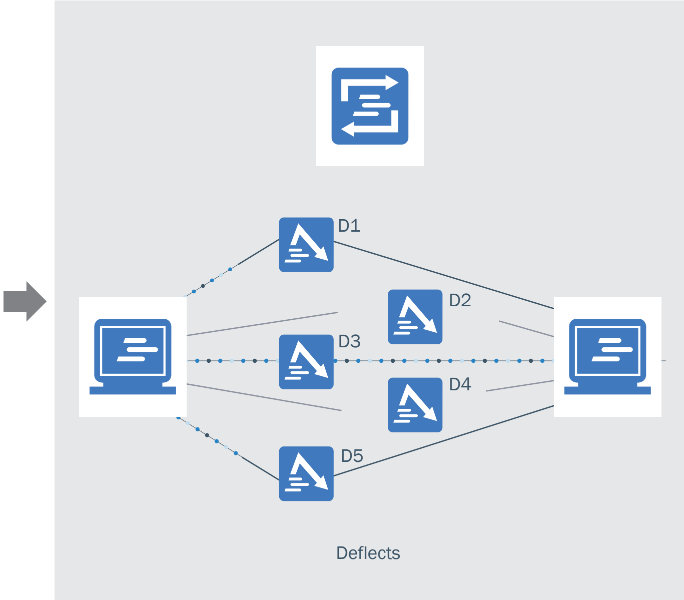
Layer 7	Application
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	Data Link
Layer 1	Physical

4 The endpoint app on the source device intercepts packet streams at Layers 2, 3, or 4.



7 The endpoint app monitors the transmission based on:

- Bandwidth availability
- Quality of line
- Measured time delay, jitter and differential latency
- Security and other customer-specific parameters



8 The endpoints roll these independent paths dynamically when necessary.

A Dispersive® VN Improves Internet Performance

A Dispersive® VN improves Internet performance in high latency environments (see Figure 3 below). This is due to a combination of techniques, which include:

Optimum path selection. With long-term connections, BGP determines the best path when the connection is established. However, that may not be the best path a few minutes later. Furthermore, if the transmission is switched to a dirty fiber, the results are higher error rates and more retransmissions. A Dispersive® VN avoids these path problems by dynamically rolling packet streams away from an impaired path to a new one.

Smarter packet handling. With TCP, when a few packets arrive out of order, the protocol assumes the network is congested and immediately slows transmissions. When packets are lost with TCP, the receiver requests that the sender transmit not only the missing packet, but also any subsequent packets. Only then does the sender slowly increase transmission speed. When a Dispersive® VN experiences a lost packet, only the lost packet is requested. The lost packet is placed at the front of the queue and sent on the next available path. A Dispersive® VN does this without notifying the application, so the application maintains the maximum transmission window.

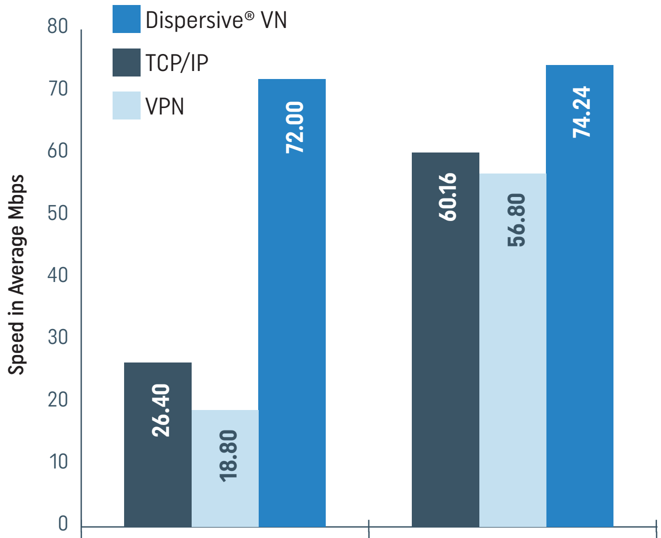
Lower bandwidth overhead. A Dispersive® VN lowers bandwidth consumption by moving away from lossy or congested paths. It also reduces retransmissions by only retransmitting lost packets.

Higher utilization. Dispersive® VN's proprietary intercept and path parallelization techniques increase application link utilization for all forms of communications links (fiber, cable, satellite and cellular).

Independent Test Results

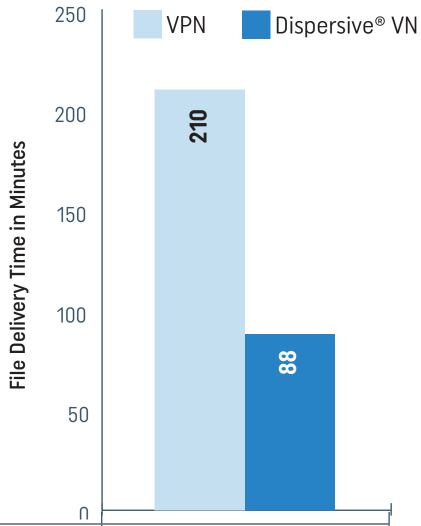
Figure 3 depicts a subset of third-party test results comparing Dispersive® VN and Internet performance across various latencies and types of file transfer.

Figure 3: Performance Comparison and Analysis of Dispersive® Virtualized Networks



File Size	10MB	100 MB
Speed (Mbps)	100	100
Error Rate	0.00%	0.00%
RTT (msec)	200	200

Source: University of New Hampshire Connectivity Research Center. *Performance Comparison and Analysis of Dispersive® Virtualized Networks.* February 2017.



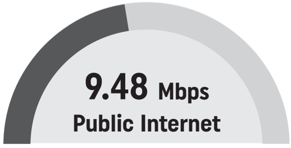
File Size	3.03Gb
Speed (Mbps)	1

Source: Intelligent Waves, Fall 2017. File transfer between Germany and US via BGAN.

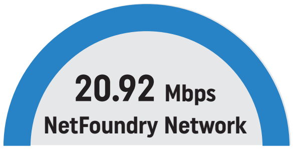
Worldwide Test
US to Asia

File Size: 48.46 MB

Source: NetFoundry, October 2017.



Elapsed Time: 40.87 seconds

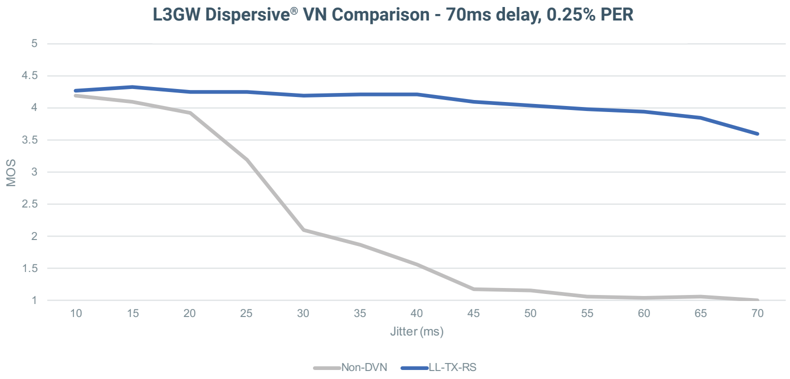


Elapsed Time: 18.53 seconds

Internal Test Results

Figure 4 depicts a subset of our internal results comparing the MOS sores delivered by Dispersive® VN and the open internet.

Figure 4: Internal Test Scores Reveal Superior MOS Scores



IV. DISPERSIVE® VN BENEFITS COMMUNICATION SERVICE PROVIDERS

Technological advances—increasingly powerful computing resources, fast networks, the convergence of IP, mobility and cloud technologies, etc.—are rapidly fueling business transformation. Enterprises now demand real-time connectivity across a variety of device types and from a range of locations . They expect improved network agility. And they pressure their service providers to maintain or reduce costs.

Software-defined networking (SDN) and network virtualization[4] are emerging technologies that promise to deliver a competitive advantage to service providers who deploy them. Elastic scalability, easier and faster provisioning of new services, and delivery of over-the-top (OTT) services are just some of the ways these technologies will increase service provider revenue while reducing churn and operational expenses.

The Dispersive® VN is the first software-defined overlay network that avoids congestion, errors, and vulnerabilities on the Internet. It provides a way for CSPs to rapidly deploy new, highly secure services, avoid middle-mile issues and obtain edge visibility. A Dispersive® VN also allows providers to use existing infrastructure more efficiently, relieving pressure on congested networks.

As a result, the Dispersive® VN increases revenue potential, avoids capital investment, raises margins and enhances network reliability.

Equally importantly, the Dispersive® VN provides a way for service providers to extend their reach into their customer base to create loyalty and reduce churn.

Samples use cases for CSP-partner deployments of Dispersive® VN include:

1. **Security-as-a-service offerings to combat cyberespionage.** Cyberespionage is on the rise. A Dispersive® VN provides a way for CSPs to deploy premium offerings that help combat this threat. Our split-path, multipath, and rolling techniques combine to make packet streams unintelligible to man-in-the-middle interceptors. Additionally, the use of strategically positioned deflects makes traffic patterns less interesting to watchful eyes.
2. **High-bandwidth data services.** High-bandwidth services like hybrid cloud backup, workload migration and data center-to-data center replication have been slow to migrate to the Internet because of performance, reliability and security concerns. However, with a Dispersive® VN, CSPs can eliminate these worries. This gives CSPs an ability to offer premium services that support enterprise digital transformation without any additional investment in capital infrastructure.
3. **IIoT connectivity solutions.** There are many cybersecurity risks for Industrial Internet of Things devices. Four that Dispersive combats are: DoS/DDoS attacks, replay attacks, unauthorized access, and infiltration/exfilitration of data and malware. Network architectures that incorporate an edge-to-edge deployment of Dispersive® VN can combat these threats while opening new revenue streams for CSPs.

[4] The International Telecommunications Union (ITU) defines software-defined networking as "a set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner." [ITU-T Y.3300 (06/2014.)] The ITU defines network virtualization as "a technology that enables the creation of logically isolated network partitions over shared physical networks so that heterogeneous collection of multiple virtual networks can simultaneously coexist over the shared networks. This includes the aggregation of multiple resources in a provider and appearing as a single resource." [ITU-T Y.3011 (01/2012.)]

CONCLUSION

A Dispersive® VN is a carrier-grade, software-only solution that incorporates multipath techniques with other key features to make it possible for enterprises to use the Internet for mission-critical communications.

The network is highly responsive to network availability, communications link errors, and route failures. It detects link errors, rolling away from one set of paths to another set without dropping the overall connection.

Given these and other features, a Dispersive® VN is exceptionally well suited to make the Internet a secure, reliable and high-performance communications platform for CSPs and their enterprise customers.

dispersive®

13560 Morris Road, Suite 3350
Alpharetta, GA 30004

1.844.403.5850
dispersive.io