dispersive

CISO GUIDE: LOOKING BEYOND THE VPN

White Paper

Business networking must evolve to meet the demands of the digital enterprise. The Dispersive™ Virtual Network enables this evolution with a highly secure alternative to VPN.

I. INTRODUCTION

Since its inception in the early '90s, Virtual Private Networks (VPNs) have been the de facto standard for remote workers and third party partners to securely access the enterprise network. However, VPNs weren't designed to handle the 21st century business challenges of big data, cloud computing, mobile workforces and the Internet of Things. As a result, a VPN can't deliver the secure, reliable and high-performance connectivity your employees need to collaborate and your customers need to transact business with you.

This paper describes how a Dispersive™ Virtual Network (DVN) overcomes the deficiencies of legacy VPNs and establishes a new, best-of-breed standard for remote connectivity.

Section II provides background information on VPNs and details some of their known vulnerabilities and weaknesses.

Section III describes how the Dispersive™ Virtual Network compares with VPNs. This section also includes test data from a third-party evaluator to substantiate claims that the Dispersive™ Virtual Network provides security without performance compromise.

Section IV concludes the paper by describing several uses cases where the Dispersive™ Virtual Network replaced a VPN.

AUTHORS

Rick Conklin, Dispersive Networks
Vice President, Engineering

Douglas V. Dimola

II. VPN OVERVIEW

Enterprises typically rely on VPNs to secure communication links between endpoints in an effort to protect data and network services from cyber threats. Enterprises may allow VPN nodes to communicate directly, or may require them to communicate via a VPN concentrator, which routes messages and services between the nodes.

VPN Vulnerabilities

As detailed in our companion white papers, both implementations are vulnerable to a range of threats. For instance, the single path VPNs use exposes organizations to DoS/DDoS threats as well as man-in-the-middle collection activities.

Another known VPN vulnerability relates to the way VPNs establish trusted relationships with devices. Typically, a device will first obtain the IP address of a network resource through DNS. With this information, communication from the device will pass the firewall and traverse the stack to the session layer (Layer 5), where the device is then authenticated and authorized. Allowing a device access to network resources before it is authenticated can negatively impact network security.

Enterprises that use a VPN concentrator face additional risks, including resource starvation attacks in which hackers direct multiple devices at the VPN concentrator to consume its compute cycles and limit its ability to authenticate and authorize network access. Additionally, enterprises using a VPN concentrator must punch a hole in the firewall of the demilitarized zone so VPN clients can connect to the network. However, every time a remote user connects to the VPN concentrator, the connection reveals the IP address and port for the firewall hole. (IP headers include this information to correctly route packets across networks.) And, as the breaches at Fortune 100 companies and The Office of Personnel Management demonstrate, hackers can combine this knowledge with compromised credentials to gain access to the network and its extended services.

VPN Disadvantages

VPN disadvantages contribute to organizational inefficiencies. VPNs require active management and maintenance of PKI certificates. They introduce packet loss and latency problems across locations, long distances and devices; this results in frequently dropped and choppy calls, which frustrates end-users.

III. COMPARISON BETWEEN THE DISPERSIVE™ VIRTUAL NETWORK AND LEGACY VPN

Legacy VPNs 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.

The Dispersive™ Virtual Network replaces one-path VPNs 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.

The Dispersive™ Virtual Network Improves Security

The "defense-in-motion" philosophy behind a Dispersive™ Virtual Network makes IP-based communications more secure than any VPN. Specific ways that the Dispersive™ Virtual Network protects data better than a VPN include:

Path-level encryption. Dispersive™ Virtual Networks use very fast, industry-standard ephemeral AES 256-bit encryption for each path.[1] 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.

Eavesdropping protection. By splitting traffic across multiple paths, encrypting each path with a different ephemeral key known only to the source and destination, and rolling communications streams periodically, the Dispersive™ Virtual Network inhibits passive eavesdropping (also known as "Eve") attacks.

1. 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

Attribution protection. The Dispersive™ Virtual Network utilizes waypoints (called "deflects") that relay traffic between endpoints. By combining this network element with techniques that eliminate inbound listeners on the firewall, the Dispersive™ Virtual Network hides the true source and destination of traffic and from-to relationships. Additionally, the Dispersive™ Virtual Network hides OS fingerprint data and can be configured to hide frame size information. These settings prevent an attacker from gaining any information about the endpoints or nature of traffic traveling on the Dispersive™ Virtual Network. To further confound hackers, the Dispersive™ Virtual Network can hop across any range of ports. It can also mask origin and destination by veiling IP addresses, ports and geographic operations through the use of strategically located deflects.

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

Malicious phoning home protection. The Dispersive™ Virtual Network only allows communication between trusted peers. As such, the Dispersive™ Virtual Network can block surreptitious communication between applications, devices and malicious third parties. It can also be configured to route all traffic via third-party scanners before leaving the corporate network for enhanced security.

Port scan protection. Dispersive encourages network administrators to expose only UDP ports to the public, untrusted portion of the network and to open TCP ports (i.e., a TCP listen port) only on trusted, internal networks (including the local IP address 127.0.0.1). In this mode, adversaries see no open TCP ports or port banners. TCP services are still available to authorized peers, but only after they have been authenticated and authorized by the Dispersive™ Virtual Network.

Viable trust relationship. The Dispersive™ Virtual Network authenticates devices (with support for two-way signed certificates and multi-level authentication) before allowing them access to the enterprise network or its services. This process, which establishes the trusted relationship only after authentication, differs from typical VPNs, which provide network access to devices before authenticating them.

Notably, the Dispersive™ Virtual Network meets the requirements for a software defined perimeter:

1. The Dispersive™ Virtual Network verifies users, devices and roles before granting access to protected systems.
2. The Dispersive™ Virtual Network uses cryptographic verification to ensure the security model is followed.
3. The Dispersive™ Virtual Network uses proven public domain security controls in its approach to achieve items 1 and 2 (above).

DoS/DDoS protection. Port scan protection and viable trust relationships provide a basis for fast processing and early discard, two defenses against DoS/DDoS attack. The Dispersive™ Virtual Network can also augment other security measures (such as deep packet inspection tools) to make resources less vulnerable to an application layer DDoS attack and can effectively shift the secure perimeter to Dispersive's cloud-hosted resources. Additionally, all elements of the Dispersive™ Virtual Network can be redundant, which helps protect against resource starvation attacks. Finally, with its ability to aggregate bandwidth from multiple carriers across multiple NICs, a Dispersive™ Virtual Network can help mitigate the impact of DoS/DDoS attacks on one specific carrier.

Microsegmentation The Dispersive™ Virtual Network segments networks by service and assigns rights to access services to individual users and devices. Users are only granted access to those specific services for which they are authorized. Users do not gain access to the full enterprise LAN. Users do not have the ability to inject multicast packets or frames into the multicast domain to discover resources on the LAN.

The Dispersive™ Virtual Network Improves Performance

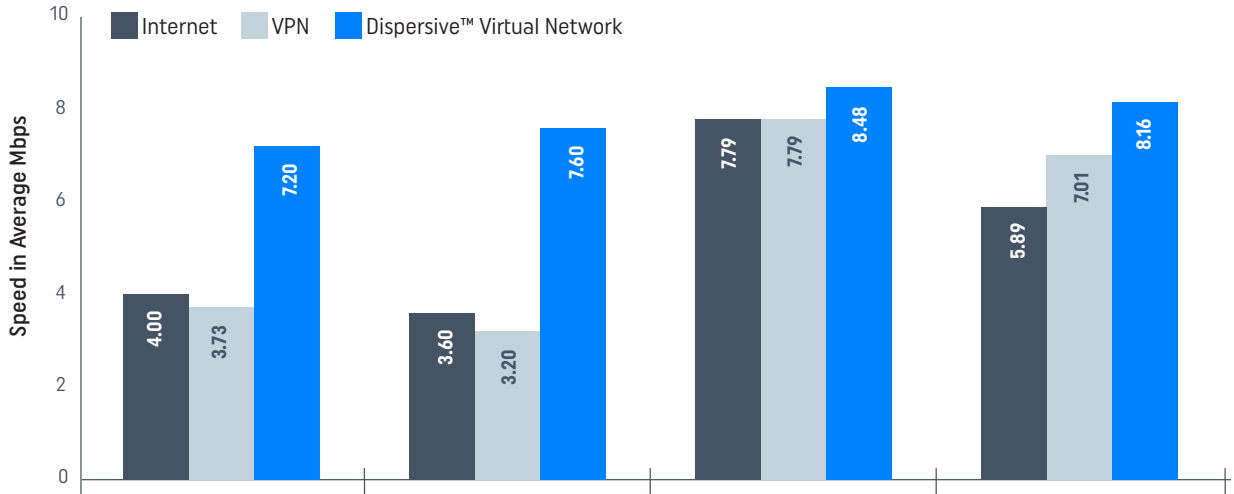
Third party test results reveal that the Dispersive™ Virtual Network out performs legacy VPNs, particularly in high latency environments. (See Figure 1.) This is due to a combination of techniques, which include:

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. The Dispersive™ Virtual Network 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 the Dispersive™ Virtual Network 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. The Dispersive™ Virtual Network does this without application awareness; the application consequently maintains the maximum transmission window.

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

Figure 1: Performance Comparison and Analysis of Dispersive™ Virtual Networks



File Size	1 MB	1 MB	10 MB	10 MB
Speed (Mbps)	10	10	10	10
Error Rate	0.02%	0.02%	0.02%	0.02%
RTT (msec)	200	300	200	300

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

IV. SELECT DISPERSIVE™ VIRTUAL NETWORK USE CASES

The Dispersive™ Virtual Network Improves Quality of Experience for Sales People

One of Dispersive's customers provides food service and cleaning supplies to various markets. Its salespeople spend a lot of time visiting hospitals, restaurants and other facilities. Getting to these locations was easy. Getting the applications and materials these road warriors needed to succeed was the problem. The Citrix remote desktop and app virtualization on which they relied would often lock up and freeze. With a high frequency of support calls diverting the IT staff from more strategic matters, the customer turned to Dispersive for help.

In just a few weeks, two Citrix servers were decommissioned and replaced with Dispersive™ Connect. End-user satisfaction now stands at an astounding 99%. Better yet, the company's senior IT administrator observes, "It' so simple... I don't have to do much to support it. I just sit back and focus on other activities. Citrix required constant attention and touch to keep it working. With Dispersive, it just works."

The Dispersive™ Virtual Network Secures Connections for a Managed Security Service Provider

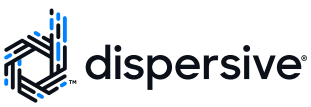
One of Dispersive's customers is a managed security service provider (MSSP) that protects over 1 million users in two dozen countries. Prior to implementing Dispersive™ Virtual Network, the MSSP relied on a legacy IPSEC VPN to manage security services for its customers. Today, the MSSP feels the enhanced security provided by Dispersive™ Virtual Networks is a competitive differentiator. They have introduced a software-defined perimeter, microsegmentation, and a call-out only approach that eliminates the need for customers to have static firewall holes.

The Dispersive™ Virtual Network Speeds International Backhaul for Security Analysis

One of Dispersive's customers has dozens of locations worldwide. It backhauls traffic from these locations to a handful of centralized facilities to conduct deep packet inspection (DPI) and other security analyses. While it traditionally relied on VPN over MPLS for this back-haul, network congestion and costs prompted this Fortune 100 enterprise to evaluate alternatives. Within weeks of implementing a Dispersive™ Virtual Network between locations in the U.S. and Asia-Pacific, IT administrators noticed enhanced network performance and are planning to extend the service to incorporate thousands of end-users.

CONCLUSION

The Dispersive™ Virtual Network overcomes the deficiencies of legacy VPNs and establishes a new, best-of-breed standard for remote connectivity. It tightens security, improves network reliability and reduces CAPEX costs. Users have a higher quality experience. Network administrators have an easier time managing the network. Given these benefits, isn't it time for you to look beyond the VPN?



13560 Morris Road, Suite 3350
Alpharetta, GA 30004

1.844.403.5850
dispersive.io