dispersive technologies™

For Your Eyes Only: Protecting Data-in-Motion with Dispersive™ Virtualized Networks

Dispersive Technologies' software and cloud-based virtualized networks deliver mission-critical communications over the public Internet to help organizations reduce costs, streamline and secure operations, and perform more efficiently.

Dispersive Technologies, 2555 Westside Parkway, Suite 500, Alpharetta, GA 30004
Offices in: Dallas | Denver | Washington, D.C.
Main: 1-844-403-5850 | Sales: 1-844-403-5851 | info@dispersivegroup.com

Introduction

The Internet is under siege with criminals and nation-states working to access, manipulate and exfiltrate data transiting the Internet. To counter these threats and protect data-in-motion from prying eyes and crooks, Dispersive Technologies developed a technique that leverages approaches traditionally used to secure military radio frequency (RF) communications. This technique augments encryption and strengthens network security for standards-based public and private Internet Protocol (IP) networks. It applies the concepts of direct spread and frequency hop communications and the principles of interleaving, red-herring and protocol dispersion. As an added benefit, the solution that incorporates these approaches (Dispersive™ Virtualized Networks, or Dispersive™ VN) also enhances network speed, improves network reliability and typically reduces networks costs. This paper will focus on describing the security features of Dispersive™ Virtualized Networks and supplements information found in the companion white paper, "An Introduction to Dispersive™ Virtualized Networks."

Component Definition

Dispersive™ Virtualized Networks comprise a number of different components that collaborate and route traffic in ways that significantly enhance network speed, security and reliability. These components are:

SoftSwitch: Server-based network management software which hosts the trusted peer database, stores communication protocols and route information, and authenticates all network components and their allowed services /service levels. The SoftSwitch also tracks the changing identity of mobile devices to ensure that communications continue without interruption when devices are moving.

Client: Software which: (i.) allows an edge device to send and receive data via the Dispersive™ VN; (ii.) configures devices automatically; and, (iii.) sets the parameters for device communications. Client software can typically reside on any IP-enabled device.

Figure 1: Dispersive™ VN Components

Deflect: Software which relays traffic between Dispersive™ VN Clients and/or Gateways.

Gateway Server: Software which allows an edge server to handle communications for multiple devices at a physical location so they can send and receive data via a Dispersive™ VN.

Interface Server: Software which allows Dispersive™ VN Clients to use services on hosts outside a Dispersive™ VN.

DART: Brower-based user interface tool which is installed on the Dispersive™ VN SoftSwitch and used to administer a Dispersive™ VN.

Figure 2 depicts a notional network that incorporates these components.

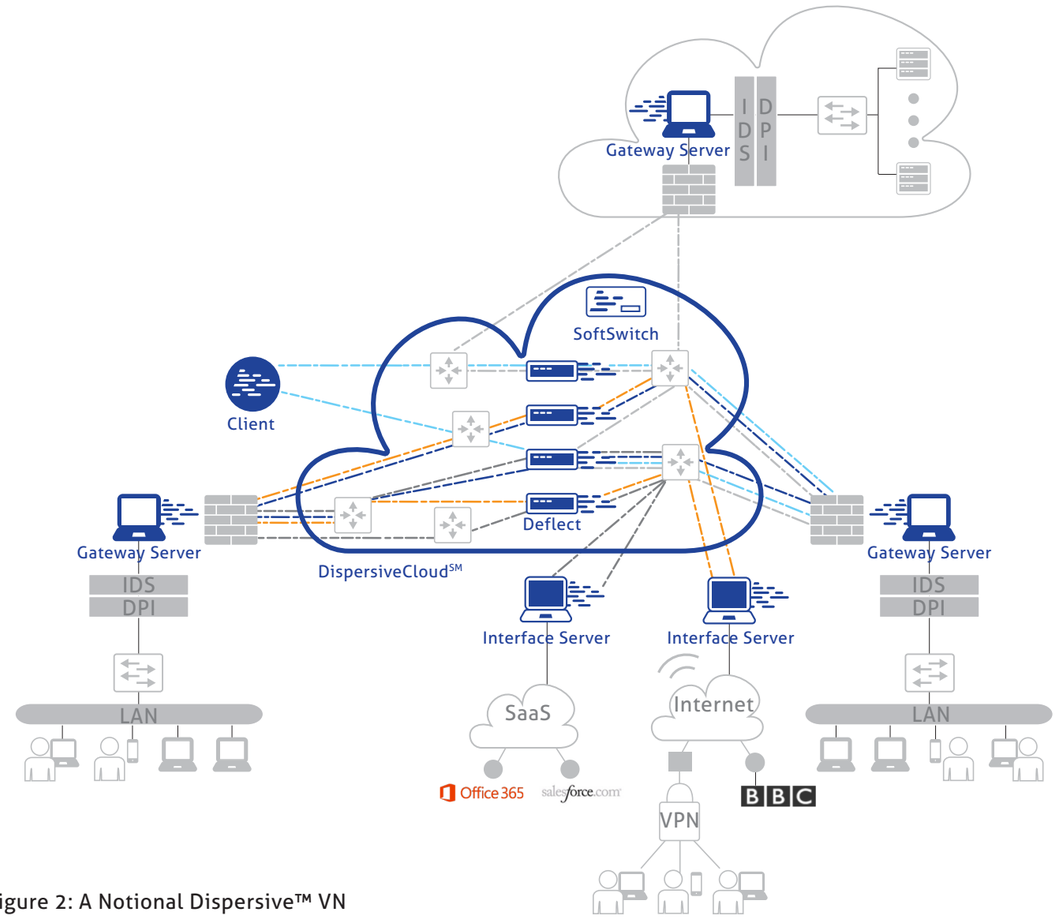
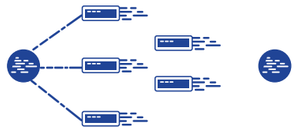
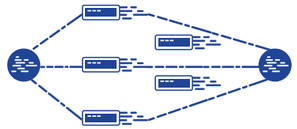


Figure 2: A Notional Dispersive™ VN

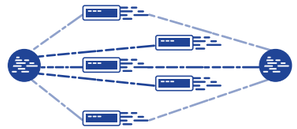
How Dispersive™ VN Transfers Data



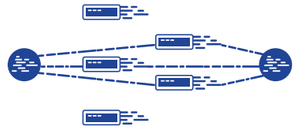
Client splits data and sends it as non-duplicated data packets.



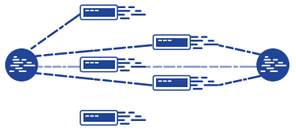
Data packets travel across parallel independent paths.



Data streams dynamically roll to optimum paths.



Degraded paths drop.



Rolling repeats.

Figure 3

Solution Overview

Dispersive™ VN software performs several key functions that combine to significantly enhance network speed, security and reliability. As visualized in Figure 3, Dispersive™ VN software:

1. Divides session layer IP traffic into smaller, non-duplicated independent packet streams;
2. Rolls these independent paths dynamically based on:
   a. Bandwidth availability
   b. Quality of line
   c. Measured time delay on each independent packet stream
   d. Other factors important to the customer
3. Reassembles the data at the receiving Client.

The Dispersive™ approach of sending data over multiple (up to 250), simultaneous, rolling paths takes inspiration from spread spectrum communications systems, which have been traditionally used to secure military RF communications. (See Appendix A for more information.) This approach differs fundamentally from the way data transits standard Internet networks, where devices are forced by routers to send data to other devices along a single path. The one stream /one path method used in standard Internet networks creates a single point of failure due to congestion and router failures, and provides one big target for man-in-the-middle attacks. By distributing packet data over multiple paths, Dispersive™ VN software significantly increases the number of paths on which a hacker would have to "camp" to intercept even one message in its entirety. By rolling paths across device IP ports, carrier channels or any combination of the two, Dispersive™ VNs introduce a pseudo-randomness that adds complexity to the collection problem, further reducing the probability of successful intercept.

Additional features further strengthen the security of the transmission and render intercepts meaningless. Each path utilizes a unique and one-time encryption key. Each transmission utilizes a unique protocol to randomly rearrange the bits in each packet stream and insert false data (interleaving and red herring, respectively). Each channel can use UDP[1] or TCP[2] or a combination of UDP and TCP ("protocol dispersion"). This unpredictable pattern of packet sequencing results in streams being undecipherable to anyone other than authorized receiving Clients.

[1] UDP is an acronym for "User Datagram Protocol," a connectionless transport protocol (handshake not required) to exchange messages on an Internet Protocol ("IP") network; packets can arrive in an unordered sequence.
[2] TCP is an acronym for "Transmission Control Protocol," a connection-oriented transport protocol (handshake required) to exchange messages on an IP network; packets arrive in an ordered sequence.

Divide and conquer. It's more than a military strategy. It's how Dispersive Technologies strengthens networks.

Dispersive™ VNs: Protecting Data-in-Motion

In combination, the techniques discussed above enable Dispersive™ VNs to protect data-in-motion by thwarting a range of man-in-the-middle attacks. Such attacks occur when a hacker monitors, intercepts, and/or alters packet streams transiting a network.

Specific examples of the type of man-in-the-middle attacks that Dispersive™ VNs defeat include: (i.) data intercept/data exfiltration; (ii) public key intercept; (iii.) packet injection; and (iv.) denial of service (DoS). These attacks, and the ways in which Dispersive™ VNs defeat them, are described in more detail below.

Data Intercept/Data Exfiltration

In traditional networks, hackers who insert themselves into the communications channel can eavesdrop on transmissions (data intercept) and copy it (data extraction) for later use and manipulation (including brute force decryption.) As depicted in Figure 4, Dispersive™ VNs significantly increase the complexity of the hacker's collection problem. A hacker would have to camp on multiple, rolling paths in order to capture 100% of the packets in just one message. The hacker would then have to sift through all the packets and properly sequence them to identify which ones belong to which message. This sifting requires Dispersive™ VN software on a device registered as one that is trusted. To sequence the packets, the hacker would also have to know the message's unique reassembly code, which is established between Clients when communications are initiated and which are specific to communicating devices and messages. As an additional security measure to protect against data exfiltration, Dispersive™ VNs can be configured to: (i.) intercept all application traffic; (ii.) force this traffic on to a Dispersive™ VN; (iii.) force all Internet traffic to route via an interface server. This server can be loaded with applications specified by the IT department and can include white and black listing, deep packet inspection, etc. to protect against data exfiltration from the Client device. This is especially useful in protecting against data exfiltration caused by an employee clicking on the infamous "bad email link" during a phishing attack.

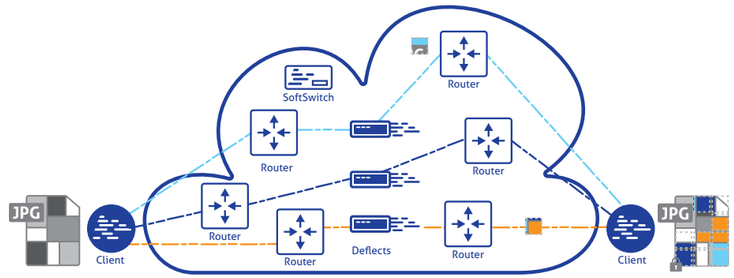


Figure 4: A hacker would have to "camp" on multiple lines to intercept an entire transmission.

Public/Private Key Intercept

Public keys are widely used to establish secure communications over an open network, but are susceptible to intercept. When this occurs, the man-in-the-middle can impersonate the parties, sending forged messages that rely on the man-in-the-middle's private key rather than the private keys of the trusted parties. This allows the man-in-the-middle to read and alter messages.To reduce this risk, Dispersive™ VNs arbitrarily split the application encryption key over multiple independent paths; this makes intercept dramatically more difficult. By protecting the transmission of the initial public key, Dispersive™ VNs thwart public key intercept in ways that mimic the defeat of data intercept/data exfilitration. (See above section.)

Packet Injection

When a hacker inserts forged or spoofed packets into an established communication ("packet injection"), he introduces an ability to disrupt and compromise the session. This creates opportunities to: hack WiFi access points; monitor and censor traffic (by injecting TCP reset packets to block undesired traffic); commit financial fraud (by injecting a script that brings users to a phishing website posing as an online bank) or commit corporate espionage (by using packet injection to deploy backdoors to launch packet sniffing attacks to allow data theft.) To defeat this type of attack, Dispersive™ VNs calculate hash values for each independent path as well as for the full buffer; if the hash values

do not match, Dispersive™ VNs discard the corrupt packets (sending it to the Deep Packet Inspection system for further analysis) and request re-transmission of the missing packets.

Denial of Service

Denial-of-service (DoS) attacks are asymmetric, malicious attempts to overwhelm computers and/or network resources and thereby make them unavailable to their intended users. DoS attacks have included assaults that flood network resources to jam bandwidth (e.g., "Smurf" and "Ping") and exploit defects in MAC protocol messages and procedures to consume CPU resources (e.g., "Teardrop" and "Bonk.") Dispersive™ VNs defeat DoS attacks by unknown entities by rejecting requests from non-trusted Clients and rolling independent paths dynamically based on (i.) bandwidth availability; (ii.) quality of line; (iii.) measured time delay and (iv.) other factors important to the customer. Additionally, Dispersive™ VN Clients incorporate firewall systems that dynamically close ports when data transmission ends so ports do not remain open until the network times out. This approach helps defeat attacks on network resources, avoids congestion and dynamically allocates resources to areas of demand. Of note, Dispersive™ VNs can send data across any combination of available network connections—including fixed line POTS (using a modem), cable, wireless and satellite—individually or simultaneously without duplication. This allows Dispersive™ VNs to utilize any available bandwidth, which thwarts Smurf- and Ping-type attacks.

Conclusion

Dispersive™ VNs protect data-in-motion from prying eyes and crooks with a technique that leverages approaches traditionally used to secure military radio frequency (RF) communications. Disperisve Technologies' techniques augment encryption and strengthen network security for standards-based public and private Internet Protocol (IP) networks by applying the concepts of direct spread and frequency hop communications and the principles of interleaving, red-herring and protocol dispersion.

Specifically, Dispersive™ VNs send packet streams over multiple independent paths. Path selection changes continuously and encryption varies from path to path during the session. Each transmission utilizes a unique protocol to randomly rearrange the bits in each packet stream and insert false packets (interleaving and red herring, respectively). Each channel can use UDP or TCP or a combination of UDP and TCP. This unpredictable pattern of packet streams and packet sequencing makes it virtually impossible for man-in-the-middle attackers to know which routes are in use, or collect enough meaningful data to reassemble the communications: streams are undecipherable to anyone other than authorized receiving Clients. Thus, there is significantly reduced risk of data intercept and theft and the confidentiality, integrity and availability of customer data is protected.

Dispersive™ VNs have been tested and approved for use on classified US government networks and have been installed in mission-critical environments that include applications within the power industry and enterprise communication. This solution runs on off-the-shelf hardware and leverages readily available, low-cost broadband Internet connections. Dispersive Technologies' approach allows companies to utilize the public Internet and cloud computing to reduce costs, streamline and secure operations, and perform more efficiently.

Appendix A: Spread Spectrum Overview

Spread spectrum communications systems utilize a wider signal bandwidth than that required for successful transmission. As such, these systems attain a better signal-to-noise ratio, which reduces the probability of interference and intercept when compared with traditional narrowband communications systems.

There are two main types of spread spectrum communications: direct sequence spread spectrum ("direct spread" or "DSSS") and frequency hopping spread spectrum ("frequency hop" or FHSS). Direct spread systems directly modulate the carrier bandwidth with a signal centered at the carrier frequency and spread over the bandwidth. Frequency hopping is a form of spread spectrum communications where the signal moves (or "hops") through the transmission band in a pseudorandom fashion. The two types may be combined to form hybrid systems, and directly influenced the analogous design of Dispersive™ Virtualized Networks on IP-based systems.

The Solution is Dispersive Technologies

Different Drivers. Different Industries.
One Need: Mission-Critical Communications.

"Dispersive™ Virtualized Networks transform the way organizations use the Internet. By operating at the bottom of the network stack, Dispersive™ Virtualized Networks control packet traffic at the most efficient point on the host. This provides signficant advantages for all users of our solutions."

— Robert W. Twitchell, Jr., CEO and Founder, Dispersive Technologies

Find out more: www.dispersivegroup.com

Dispersive Technologies, 2555 Westside Parkway, Suite 500, Alpharetta, GA 30004
Offices in: Dallas | Denver | Washington, D.C.
Main: 1-844-403-5850 | Sales: 1-844-403-5851 | info@dispersivegroup.com

dispersive VN by dispersive technologies