Ovum

Verizon offers a zero-trust service with SDP over MPLS

Publication Date: 31 Oct 2019 | Product code: INT005-000048

Rik Turner

Ovum view

Summary

Verizon has launched what it is calling a “zero-trust-as-a-service” offering, whereby it runs software-defined perimeter (SDP) technology over its Private IP enterprise WAN offering based on MPLS networking. By combining SDP and MPLS, Verizon is providing a differentiated, more secure version of SDP, while adding much-needed value to its MPLS offering.

SDP is a replacement for VPNs in the cloud era

SDP is a technology that came out of work done by the Defense Information Systems Agency in the US during the 2000s and is often referred to as the evolution of, and replacement for, virtual private network (VPN) technology for remote access to corporate applications.

VPNs work by enabling client software on remote devices to log into a VPN concentrator on corporate premises to gain access to a company’s network. SDP also has software clients on devices, but these communicate with an SDP controller, which can be on-premises or, more usually, in the cloud, via which they gain access to the specific application they require for a given task, based on a predefined list of authorized users and machines. There are two “tunnels” of secure communication. The first is client-to-controller and the second is controller-to-application, without the blanket network access enabled by VPNs. Access to a second application requires another authentication process, again depending on list of authorized users/devices.

For this reason, SDP is an implementation of zero trust, a philosophy of trusting no-one and granting everyone the least amount of access required at any one moment. This concept also comes out of the US defense sector, although it was brought to general enterprise awareness around 2010 by a tech analyst firm.

The first commercial offerings of SDP involved technology that a customer acquired, installed, and operated themselves, but in recent years, several of the original vendors have been acquired by companies planning service offerings. Akamai acquired Soha, Cyxtera absorbed Cryptzone, and Proofpoint bought Meta Networks, which was already offering SDP as a service. Verizon joined the fray in November 2018 with the acquisition of the assets of SDP pioneer Vidder.

Meanwhile, Zscaler launched a product that was delivered as a service from the outset, and Google implemented SDP for its own workforce (a project called BeyondCorp) and makes it available free to its customers under the name Identity-Aware Proxy. However, the technology only works for assets residing in the Google Cloud Platform.

Verizon’s SDP gateway enables the fastest path to the app

Given its ability to enforce Zero Trust principles, there are now security industry pundits who recommend the use of SDP not only for remote access, but also for all application access, even by employees on the corporate LAN. This argument makes increasing sense, now that applications themselves are moving off company premises and into the cloud.

Verizon’s SDP works by deploying client software containing a digital certificate on the device of each end user to be enrolled in the scheme. The client communicates with an SDP gateway, which is a

1GB server that can reside in a DMZ, on each application server to be accessed via the system, or in the cloud.

When users request access, the gateway checks against their Active Directory or LDAP entry to see what they are authorized to do, as well as validating that their name is on the authorized user list for the particular application they are requesting. It also checks the end user's device to make sure that it has the necessary digital certificate associated with that user.

Verizon says integration with an endpoint security platform such as CrowdStrike or Cylance can add further layers of security, checking that there is no malware on the device, for instance. If therefore, an endpoint in a branch office that has direct internet access via a broadband or wireless link has been compromised, the endpoint security product can raise an alarm and the device can be removed from the authorized user list until it has been remediated.

The carrier makes the point that, unlike competing SDP services, its gateway is not a proxy, so that once the user and device have been authorized for access, the communication can take the fastest path through the Verizon network to the desired resource, rather than being limited to a link to the proxy and the proxy's link to the app.

SDP is a value-add for Verizon's MPLS service

Verizon has embedded the SDP technology inside its customers' MPLS links and, to turn it on, they must deploy the necessary SDP clients and set up the authorized user lists for the applications to be accessed. The carrier already offers SDP as a service on its regular broadband links, but it is the SDP-over-MPLS service that spearheads its zero-trust efforts, and with good reason.

First, because as a private WAN link, MPLS is inherently more secure than the public internet, not to mention having service-level agreements and quality of service capabilities far beyond broadband. Layering SDP on top of MPLS therefore adds a deterministic security dimension for even greater control of who has access to which resources.

Second, the SDP feature adds value to MPLS at a time when the venerable WAN service is coming under fire from the proponents of SD-WAN who argue that it is considerably more expensive on a per-gigabit basis, even after MPLS prices have themselves come down somewhat.

While this is undoubtedly still true, Verizon's strategy is to layer value-adds such as SDP onto its MPLS service, then counter with the argument that enterprises need to consider the total cost of a broadband connection, plus the acquisition cost of SDP technology, plus the salaries they would have to pay to IT professionals to configure, implement, and operate it, and compare this with the cost of SDP over MPLS, all delivered as a service.

To further underscore its argument, Verizon is making the SDP part of the service free for a customer's first 100 employees, after which there is a monthly fee per employee, with volume discounts as the employee count goes up.

Appendix

Author

Rik Turner, Principal Analyst, Infrastructure Solutions

rik.turner@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

CONTACT US

ovum.informa.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Boston
Chicago
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
Paris
San Francisco
Sao Paulo
Shanghai
Singapore
Sydney
Tokyo