Remote Access VPN in the Cloud Age

White paper

The remote access Virtual Private Network (VPN) has been around for years. Let's see how it's changing in the cloud-enabled age.

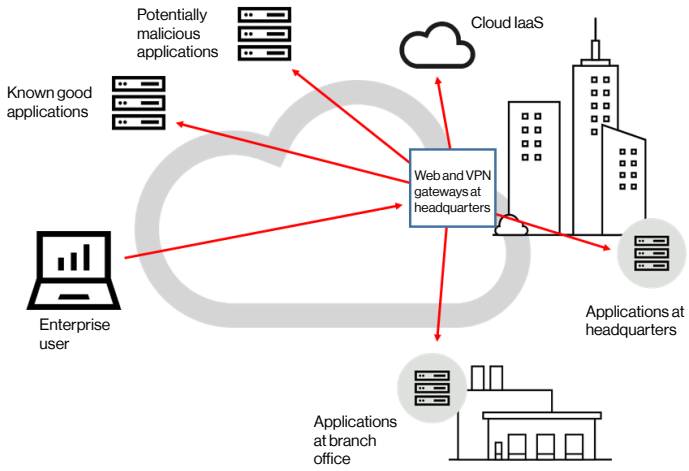
The old-school remote access VPN (circa 1990's) used a traditional VPN and web gateway, where the VPN essentially put the user on the Local Access Network (LAN) and required a security stack to ensure users were not going to bad websites or downloading bad payloads. In Figure 1, we see four different environments that start with known "good" applications like Office 365, Google search, and others. We know that the connection to those applications will be allowed by the security stack, yet the connection must still be hairpinned through the VPN gateway and the web gateway.

The second environment has potentially malicious websites, and those connections need to go through a security stack, but, do all connections (good, bad and questionable) have to be hairpinned through a few locations? We'll see a better way in a minute.

Businesses are now migrating their applications to different cloud environments. But since we're still in the 1990's data flow model, that move creates another hairpinning event where users must first go to the traditional data center before being re-routed to the cloud via a site-to-site VPN.

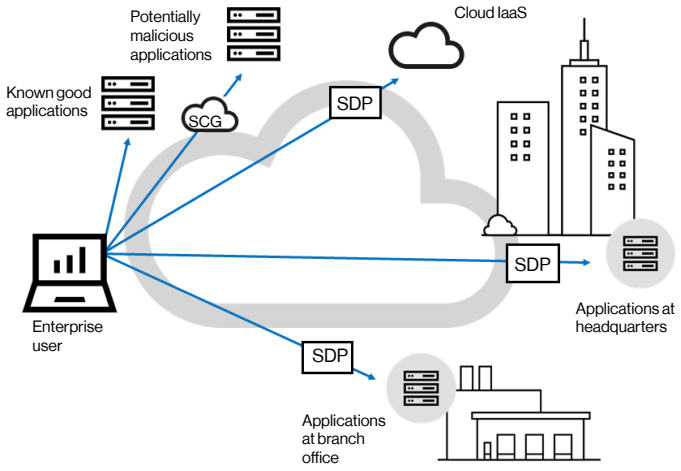
And finally, access to some enterprise applications may still involve hairpinning data through the fixed locations of the VPN gateway out to other locations.

Figure 1: traditional Remote Access VPN and Web Gateway



- Known good applications: hairpin through Web Gateway
- Potentially malicious applications: hairpin through Web Gateway
- Enterprise applications: hairpin through Web Gateway
- Cloud IaaS: hairpin through site-to-site VPN

Figure 2: Verizon Software Defined Perimeter and Secure Cloud Gateway



- Known good applications: whitelisted in PAC; enterprise-specific
- Potentially malicious applications: Secure Cloud Gateway (SCG) has a blacklist and sandbox; includes "unsuitable for work"
- Enterprise applications: Software Defined Perimeter (SDP) is the Zero Trust Architecture. Provides direct access to applications
- Cloud IaaS: Multiple gateways simultaneously. Completely black - Nmap returns filtered

verizon

The alternative shown in Figure 2 consists of the Verizon Software Defined Perimeter (SDP) and the Secure Cloud Gateway. Back to our four environments. We have our known good applications (Office 365 and Google search) that we know users will be allowed to access. With Verizon SDP, these can be whitelisted in the proxy auto-configuration (PAC) file. Installed on each user's computer, the file instructs the computer that it is permitted to go directly to these applications, greatly reducing latency to commonly used websites.

For potentially malicious websites, we still need to put the connection though a security stack. With Secure Cloud Gateway, this is now done in a distributed fashion such that the security stack does not create a huge hairpinning of the connection.

- Access to good ones = fast
- Access to bad ones = blocked

Next, we have our cloud migration. With a traditional remote access VPN, all traffic must hairpin through one gateway typically established at the enterprise data center. Verizon SDP simultaneously enables multiple gateways at multiple locations, so the users can go directly to multiple clouds and the enterprise data center at the same time. And Verizon SDP Gateways are completely black (unlike traditional gateways), meaning that if you try to scan for them you will find that they don't exist. There is no DNS entry for them and if an adversary were to somehow find the IP address of a Gateway, an Nmap scan would return "Filtered" – meaning that Nmap thinks it doesn't exist.

Finally, for enterprise applications Verizon SDP implements the Zero Trust Architecture. [Note: Zero Trust Architecture is defined in the National Institute of Standards and Technology Special Publication 800-207 and that document calls out the Software Defined Perimeter as a preferred implementation of the Zero Trust Architecture] While there are multiple ways to implement the Software Defined Perimeter, Verizon SDP is the fast Zero Trust Architecture as it securely routes traffic directly to the applications.

That takes care of the four environments, so let's look at the security stack itself. Secure Cloud Gateway in Figure 2 is equal to the Web Gateway in Figure 1 since they provide the same decision making process as to whether to allow the user to access a website or not. So, why use the old architecture that adds the often significant delay of hairpinning the traffic for the same security functionality?

The era of the cloud can mean much faster access to applications for your users. Verizon SDP and the Secure Cloud Gateway can make it happen.

Why Verizon.

As an award-winning leader in cybersecurity, we keep up with the rapidly changing nature of cyber threats by processing billions of security events each year, analyzing evolving threats at our global security operations centers, performing forensic investigations for companies around the world, and sharing our knowledge through industry-recognized content like the annual Data Breach Investigations Report.

We differ from other security service providers because our substantial risk and incident experience lets us understand the real-world threats you face and the potential vulnerabilities in each system. And, our years of practical experience in developing and implementing security programs across all industries lets you know that our priority is your long-term success.

Learn more.

For more information on the solutions discussed here, contact your account representative.

verizon