5 Security Threats The VPN Can't Defend Against

By: Etay Bogner

Enterprise security has been turned on its head as the way we work has morphed from primarily office-based to remote work environments on a more regular basis. Today's employees need to work on the go, whether from home or while traveling and commuting. The rise of the gig economy and a massive expansion of contractors and freelancers in the workforce have added to this remote work environment.

The traditional way that IT approached securing the enterprise was via perimeter security—hence the popularity of virtual private networks (VPNs), which were designed expressly for this purpose. Yet while VPNs could effectively enable and secure remote access in the past when most work was done onsite within company walls, their use has become increasingly risky in a world that includes a preponderance of virtual workers. While corporate VPNs gave remote workers network access to retrieve company data and applications needed to do their work, other network data also became vulnerable.

The fact is that local area network users can't always be "trusted," as is evident by the large number of data breaches affecting organizations of all sizes around the globe. By giving remote users the run of the network, so to speak, a sizable attack surface remains open for exploitation by hackers and attackers.

In 2019, the DHS Cybersecurity and Infrastructure Security Agency (CISA) and the CERT Coordination Center released information on a vulnerability affecting Virtual Private Networks (VPNs). An attacker could exploit this vulnerability to take control of an affected system. There have been instances where VPNs may improperly secure tokens and cookies, allowing malicious actors with the ability to invade and take over control of an end user's system. CISA, the Cybersecurity and Infrastructure Security Agency, encourages users and administrators to review CERT/CC's Vulnerability Notes for more information and refer to vendors for appropriate updates when available. The DHS/CERT warning follows a previous notice from Carnegie Mellon on a CERT that VPNs deployed by some of the world's largest and most well-regarded vendors that authentication or session cookies were insecurely available in memory or log files.

The problem is that any exploit based on extracting keys or cookies and transferring them to another machine means that the VPN implementation on the gateway side does lack some additional countermeasures that should have been implemented. But which countermeasures or additional security measures should the victims have put into place? What is proposed by industry experts is a cloud-based solution that follows the user and their devices wherever they are, rather than a solution relying on traditional VPN infrastructure at the office or data center.

Until more effective, identity-based remote access solutions such as software-defined perimeters (SDPs) are commonly deployed, below are five of the most typical types of security threats that VPNs are no longer well-equipped to protect against.

Threat 1: MITM Attacks

In a security breach known as "man in the middle" or MITM, a cyberthief enters a communication channel between an application and a user. The hacker may pretend to be the other party or may "listen in" to the conversation without permission. The user may have no idea that anything untoward is happening, since the MITM can make

it appear to be a normal information exchange. While a VPN can offer some shelter from this type of subterfuge through encryption, what often happens is that the VPN sends traffic out via a split encrypted tunnel in the name of cost savings, which means endpoints are left unprotected. SDPs avoid this problem by securing open endpoints, which can protect web traffic while safeguarding network access.

Threat 2: Domain Name System (DNS) Hijacking

Many remote workers rely on public WIFI to get business done—but security is a huge issue on these open networks when using a VPN solution, in particular through the possibility of DNS hijacking. In this type of attack, perpetrators infiltrate the Domain Name System and reroute victims away from the site they wanted, directing them into a malicious site instead. If a hacker gets his or her hooks into the DNS, this can cause ongoing trouble as the hacker directs users to pages with ads or malware. SDPs, on the other hand, are structured as Network-as-a-Service to prevent DNS hijackers from having their way.

Threat 3: Worms

Worm exploits often grab headlines for their ability to spread and self-replicate in a worm-like way, going from computer to computer wreaking havoc. It’s simple for machines to become infected: all it takes is a user joining a worm-infected network via their device. This is why traditional endpoint security platforms can’t add protection. Since such exploitations occur on a network, a VPN solution is rarely prepared to defend against these worm attacks. The best way to prevent a worm exploit from succeeding is via an SDP solution, which allows users finely grained access through a unique identity as well as micro-segmentation to the specific resources required—and not to any others. This means that a single infected smartphone or laptop won’t contaminate the entire network and puts an effective stop to this type of havoc.

Threat 4: Repeated Login Attempts

Much like a Distributed Denial of Service Attack (DDOS)—which is yet another threat whereby an app is overloaded with requests and thus made unavailable—repeated login attacks can trip up VPN solutions. In this type of hack, also called a “brute force attack,” the perpetrator may end up accessing a company’s network by trying repeatedly to determine the password and log in. The advantage of an SDP solution in the face of a brute force attack is that it is designed to flag failed attempts to log in. Additionally, SDP will deny access to someone if it detects:

- Suspicious login locations
- Odd times of day for login attempts
- Changes to posture of device
- Endpoint has no active antivirus

Threat 5: Legacy apps

Security is an issue in legacy applications, since many of these older apps were never designed with Internet accessibility in mind. Modern SDP solutions mitigate this security risk by limiting access to legacy applications, separating the application from the network or Internet while adding adaptive controls for risk reduction.

In defense of organizational security, one approach to stopping such threats is to build networks around a zero-trust security framework, which puts greater control in the hands of IT to secure employee or contractor access. This is done by identifying those logging in and extending privileges based on their employee profile. In such a zero-trust network environment, legitimate network users do not have to be concerned about dealing with network-security issues because the zero-trust network

orchestrates all of the security and access rules on their behalf.

With their ability to secure gateways at the application layer rather than the network layer, software-defined perimeters are a much more effective alternative to modern enterprise security threats than VPNs, since SDP solutions are designed to confront these threats head-on. By replacing broad network access with granular, identity-based access, the SDP's zero-trust approach to remote access is what enterprises need for reliable protection from a wide range of threats and attacks that can otherwise compromise the enterprise network. In today's evolving, remote-work-based environment, the SDP is therefore an increasingly popular approach to leveraging zero-trust access.