Cisco and Sonicwall Experience VPN Vulnerabilities Increasing Interest in ZTNA

VPN technology used by remote workers everywhere is 20 years old and easily hacked. Companies are moving to a Zero Trust Network Architecture (ZTNA).

WhiteStar Communications

DURHAM, NC, UNITED STATES, October 13, 2025 /EINPresswire.com/ -- The last 30 days have seen a series of cyber vulnerabilities exploited impacting large enterprise customers using Cisco VPN technology, as well as small/medium businesses who rely on SonicWall VPN devices. What has happened that has put VPNs under such attack? Billy Moon, CTO of WhiteStar Communications and former Distinguished Engineer for Cisco Systems and Extreme Networks with over 300 cellular and internet patents to his name sums up the issue, "Companies are moving away from 20-year-old VPN technology to protect their enterprise. ZTNA is part of that. However, not all ZTNA solutions are the same."

ZTNA, which stands for Zero Trust Network Architecture, is being touted from vendors ranging from HP, to Cato Networks, to WhiteStar Communications, to Tailscale. VPN technology authenticates that the network you are accessing truly belongs to the company that you think you are accessing. However, this authentication typically using certificates builds only half of the "trust" that a ZTNA architecture provides.

With ZTNA, the user who is accessing the servers that host applications for an enterprise via their networks, is also verified. To address the verification of the user, a ZTNA architecture uses either third-party or first-party authentication of the user.

Third party authentication relies on Google or Microsoft or Facebook to verify that you are who you say you are. This inherently violates the concept of "zero trust" by outsourcing the authentication to a third party. Yet many companies are relying on these big companies for

> Companies are moving away from 20-year-old VPN technology to protect their enterprise. ZTNA is part of that. However, not all ZTNA solutions are the same."
>
> *Billy Moon, CTO and Founder of WhiteStar with 300 patents to his name.*

third-party verification.

Moon points out, "Yeah, they're big companies, but they are also giant targets. Think about this for a moment. If you are a thief, are you going to spend time trying to break into someone's house and look under the mattress to find one gold coin or are you going to try to break into a place that has $5 trillion worth of gold coins?" He continues, explaining, "That why you see a data breach practically every month from large companies you recognize. That is also why first-party zero trust authentication is so important."

First-party Zero Trust Authentication is where the person who wants to have access provides their information directly, typically via a coordinated e-mail exchange, to the site they want to access. This ensures that the site you are accessing knows who you are in addition to you knowing that the site is who you think they are.

Is there anything in addition to first-party vs. third-party verification that makes a ZTNA work more effectively than current VPN technology? Marc Fath, VP of Engineering for WhiteStar Communications indicates that there is. "The short answer is that there are a lot of things but not all providers of ZTNA offer them. For example, end to end encryption along the entire path of the communication or whether you use old and vulnerable cryptographic protocols, such as SSL or IKE, or TLS."

Encryption is a topic unto itself. However, most people understand that the National Institute of Standards (NIST) has several types of encryption that have been properly vetted and tested to withstand increasing levels of attack. Generally, this includes an algorithm and the length of a "key". Therefore, in the Advanced Encryption Standard, AES-256 uses the same encryption algorithm, but keys that are twice as long as, the more common AES-128.

"It doesn't stop with just the encryption algorithm, but also includes the protocol used in other cryptographic functions such as distributing keys." Billly Moon explains this further, "Take for example, TLS, which is Transport Layer Security protocol. Normally TLS never rolls keys [meaning change the keys to the encryption]." Moon explains why this occurs. "The reason is that there is a well-known security threat that if you use the TLS protocol, there is a way for a hacker to trigger a new key exchange and insert a key they know. So, everybody turns off the ability for TLS to roll keys. Instead, they just keep using the same key for lots and lots and lots of data which ultimately makes breaking the encryption that uses that key much easier to do."

Yet the Cisco VPN technology issue wasn't authentication, per se, or encryption, but "buffer overflow". Does ZTNA protect against that attack vector? Moon explains, "There is a

fundamental trade off that every network equipment provider makes, which is whether they want their product to be fast or secure. Those that want it to be fast typically write their code using C or C++. Those that want it to be secure choose JAVA."

One of the differences between C, C++ and JAVA is stack management. C and C++ do not manage their memory buffers. While Java does stack management and therefore prohibits buffer overflows. Simply speaking the attack used successfully against Cisco's equipment was to send a message that places more information onto the stack than can be handled. The message causes an error condition of "buffer overflow". This allows root access for the box to be achieved which is even a greater risk than inserting harmful code. Moon exclaims, "Buffer overflows have been with us for thirty years. JAVA is the first and maybe the only language that was written to live on the internet where one's code is constantly being attacked. With today's processor speeds on edge devices, there is no need to risk using C or C++."

Twenty-year old VPN technology is vulnerable. Moving to ZTNA is a strategy being used by many companies to address cyber threats. Not all ZTNA solutions are the same or provide the same depth of security. Some are written using C or C++ while others are written using more secure JAVA. In addition to zero trust authentication of the user, features such as end-to-end communication, surface area, encryption, and cryptographic protocols need to be considered to address the threats facing enterprises today.

James Massa
WhiteStar Communications
+1 919-267-1916
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X
