https://www.vanillaplus.com/2018/10/01/42333-users-failed-vpns-security-performance-sd-wans-no-option-industrial-iot-next/

Users failed by VPN security and performance, but SD-WANs no option for industrial IoT. So where next?

01/10/18

Scott Raynovich opens the Application Networking session at #NetEvents18

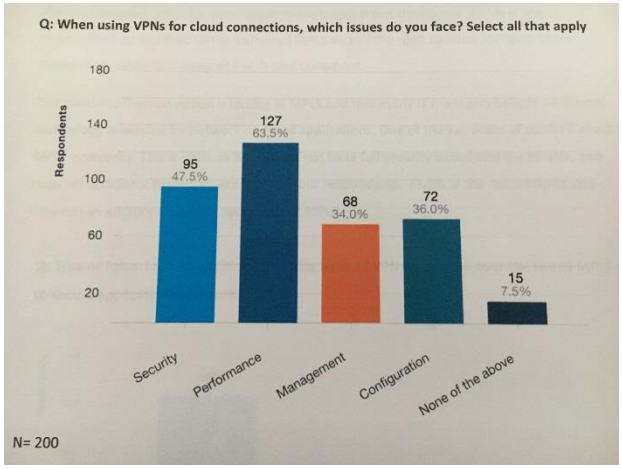
Virtual Private Networks (VPNs) have significant security and performance drawbacks for use in networking cloud applications. This was the start-point for a recent survey and primary research by industry analysts, **Futuriom**, that (spoiler alert) leads the firm to conclude that Application Specific Networking (ASN) may be a way forward.

As *Jeremy Cowan* reports from the *NetEvents' Press & Analyst Spotlight* (#NetEvents18) in Albufeira, Portugal (September 27-28th, 2018) Futuriom's research, sponsored by **NetFoundry**, has shown that IT managers want more flexible, secure, software-based networking solutions for the cloud.

Is it ASNs to the rescue?

Scott Raynovich, Futuriom's founder and chief analyst, led the survey of 200 enterprise technology users, comprising managers with roles in application development, networking, security, and DevOps. He was looking for insight into the features that IT staff are looking for in cloud networking security. He also wanted to know why ASNs – which connect

distributed applications in Software-, Infrastructure-, and Platforms-as-a-Service – are emerging as a viable solution to networking cloud applications.



Performance tops the issues faced by IT managers when using VPNs for cloud connections

An Application Specific Network is a software-only network that connects applications without requiring management of hardware devices, operating systems, or servers. Unlike VPNs, they can be provisioned automatically by the applications in the cloud.

Raynovich sums up ASNs' key features:

- ASNs offer secure networking, tied to applications not devices
- They are easy to set up and tear down with software,
- No "box management" is needed to create a network,
- Networking and security features are targeted at DevOps and software development staff (not networking specialists),
- They can employ a native Zero Trust security architecture as well as hardware root-of-trust on demand with high performance, and
- ASNs are generally transparent to the end user.

Raynovich tells us: "ASNs' design incorporates a new architectural design of creating logical networks across the internet an WAN to connect applications – called AppWANs. The AppWANs are the glue that can securely connect parts of a distributed application, which often includes connecting applications programming interfaces (APIs) and workloads that may run across clouds.

"It appears IT managers are looking for a more flexible and secure software-based networking solution for the loud. ASNs are likely to serve that person to connect distributed applications in SaaS, IaaS, and PaaS environments, whether it's single cloud, hybrid cloud, and multi-cloud environments."

Secure connections

What Futuriom's research also found was that hardware root of trust and Zero Trust security architectures are gaining traction. Raynovich tells the conference "the massive shift … from

on-premises applications to hybrid cloud environments has posed many challenges to IT and network managers looking to efficiently and securely connect applications."

No fewer than 63.5% of those surveyed cited issues with VPN performance and almost half (47.5%) pointed to security problems, with the result that 75% of Virtual Private Network users said they are looking for a better solution for cloud networks. Users don't see private lines or MPLS (Multi-Protocol Label Switching) as fully secure solutions and most use an additional security layer.

No good for IIoT

Although SD-WANs (Software-Defined Wide Area Networks) can be appropriate for connecting branch networks, the technology cannot support applications beyond the network. This includes industrial Internet of Things (IIoT) devices, for which 43.5% of respondents to the survey said SD-WAN is not an ideal IIoT solution (*33.5% disagreed and 23% said they did not know. Ed.*).

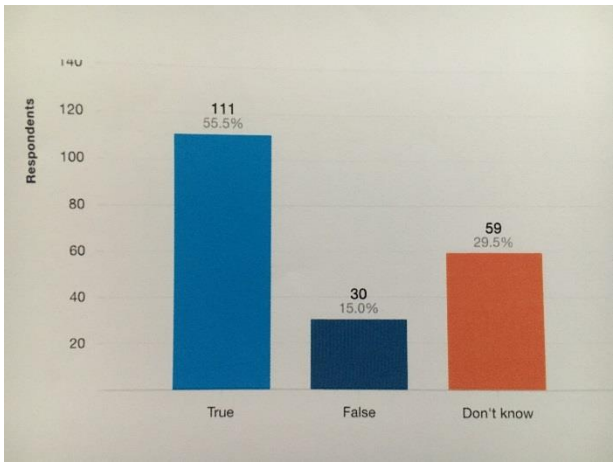
Instead, the majority of end users are looking for zero-trust networks and hardware root of trust for their security. In all, 74.5% declared they see hardware root-of-trust as a significant security feature.

Scott Raynovich, principal analyst at Futuriom

Raynovich says: "Cloud-based applications and virtualisation have shifted networking needs away from devices and boxes and toward native applications-based networking solutions. The data shows that IT departments are looking for a way to build automated networking functionality directly into applications."

VPNs, the survey shows, are used for extranets, business-to-business (B2B) or connected supply chains. Additional research indicates that end users find VPNs often generate network and processing overheads. In some cases, this can also generate significant latency and delays

for networking resources. Furthermore, they can introduce complexity for managers because they often require their own servers with authentication.



Surveyed companies mostly agree that Zero Trust network architectures are a significant improvement in network security.

It will come as no surprise that NetFoundry has skin in the AppWAN game. The company has recently worked with **Microsoft** to ensure simple, integrated provisioning between Azure Virtual WAN and NetFoundry AppWANs. As a result, says Philip Griffiths, head of EMEA Partnerships, NetFoundry AppWANs "provide enterprise-grade security, improve performance and simplify network management."

Jeremy Cowan

NetFoundry AppWANS are described by the company as an "integrated on-ramp to Microsoft Azure", claiming cloud-native agility, instant connectivity, simple deployment and scalability. NetFoundry reportedly enables ASNs by allowing customers to use its global network control platform to spin up connectivity instantly for IoT deployments, virtual WANs, and custom secure application connectivity between organisations, partners and end users.

The author is Jeremy Cowan, editorial director of IoT Now, IoT Global Network, and VanillaPlus.