FUTURIOM
THE FUTURE OF TECH

Application Networking Trends

HIGHLIGHTS OF ASN SURVEY RESULTS

- The Futuriom Applications Specific Networking (ASN) Survey collected detailed feedback from 200 enterprise technology end users on the topic of networking cloud applications.
- End users are seeking more robust software-based solutions for networking cloud applications in a secure fashion.
- 63.5% of users cited issues with VPN performance.
- 47.5% cited issues with VPN security.
- 75% of VPN users said they are seeking a better solution for cloud networks.
- Key features such as Zero Trust architectures and hardware root of trust are desired for cloud networking security.
- Application Specific Networking (ASN) is emerging as a viable solution to networking cloud applications.

SPONSORED BY NETFOUNDRY™
SPIN UP YOUR NETWORK

EXECUTIVE SUMMARY

The massive shift of applications from on-premises software to hybrid-cloud application environments has posed many challenges to IT and networking managers looking to efficiently and securely connect applications.

To gain insight to these challenges, Futuriom surveyed 200 enterprise IT managers in application development, networking, security and DevOps and reached some major conclusions in a new report. The research, based on survey data and primary research with enterprise end users, shows that cloud IT professionals are looking to evolve their approach to networking and securing cloud applications. These new approaches can fill gaps in existing technologies such as Virtual Private Networks (VPNs).

VPNs are seen as having significant security and performance drawbacks for use in networking cloud applications. High-level conclusions of our research, based on survey data and primary research with end users, include the following:

- 75% of VPN users said they are seeking a better solution for cloud networks.
- VPNs are seen as having significant security and performance drawbacks for use in networking cloud applications:
  - 63.5% of users survey cited issues with VPN performance.
  - 47.5% cited issues with VPN security.
- Users don’t see private lines or MPLS as fully secure networking solutions for cloud applications. Most use an additional security overlay.
- SD-WAN may be appropriate for branch connectivity, but the technology is not seen as suited to Industrial IoT devices. 43.5% of users survey said they agree that SD-WAN is not an ideal solution for networking Industrial IoT devices, while only 33.5% disagreed. 23% said they don’t know.
- The majority of end users are seeking Zero Trust networks and hardware root of trust for network security. 74.5% said they see hardware root-of-trust as a significant security feature.
- When asked if Zero Trust network architectures are a significant improvement in networking security, 55.5% agreed this was true, while only 15% disagreed. 29.5% said they don’t know.

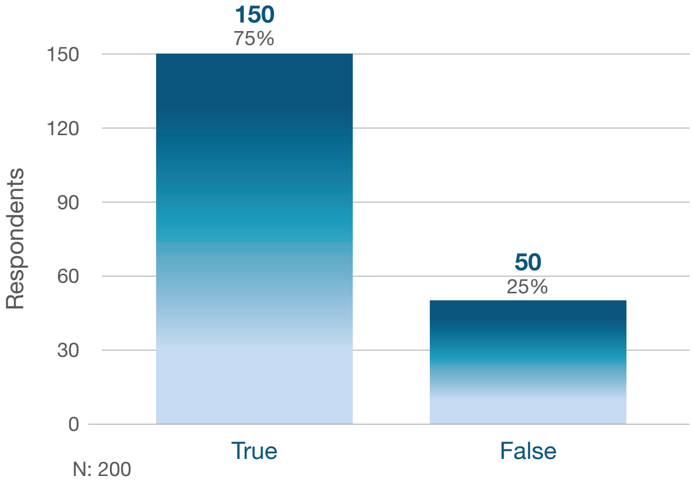
This primary research reflects the fact that cloud-based applications and virtualization has shifted networking needs away from devices and boxes and toward native applications-based networking solutions. The data shows that IT departments are looking for a way to build automated networking functionality directly into applications.

WHAT COMES AFTER VPNS

One of the important themes addressed by the survey is how IT staff view the use of VPNs in cloud networks and how secure networking is likely to evolve. Users expressed serious concerns about the use of VPNs, especially in use cases such as B2B and Internet of Things (IoT).

Data gathered indicates that while many respondents use VPNs for extranets, B2B networks, and connected supply chain, 75% of them are seeking a better solution.

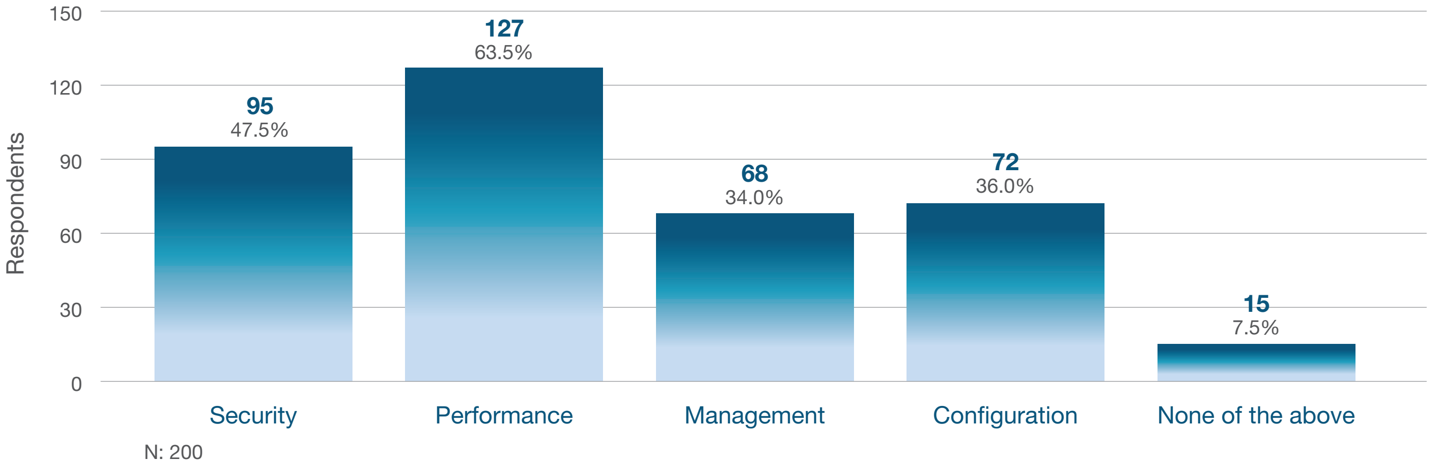
Q: True or False: I use VPNs for extranets, B2B or connect supply-chain use cases, but I am seeking a better solution.



This may lead you to ask: What exactly are the problems with VPNs for cloud networks? Futuriom has conducted primary research in addition to the survey results, to gain additional insight. Comments from IT professionals indicate that VPNs often generate network and/or processing overhead as users connect to VPN servers. In some cases, this can generate significant latency and delays for networking resources. Additionally, VPNs introduce management complexity because they typically require their own servers with authentication.

Survey backs these issues up. The following chart ranks the issues that are mostly commonly faced when using VPNs for cloud connections.

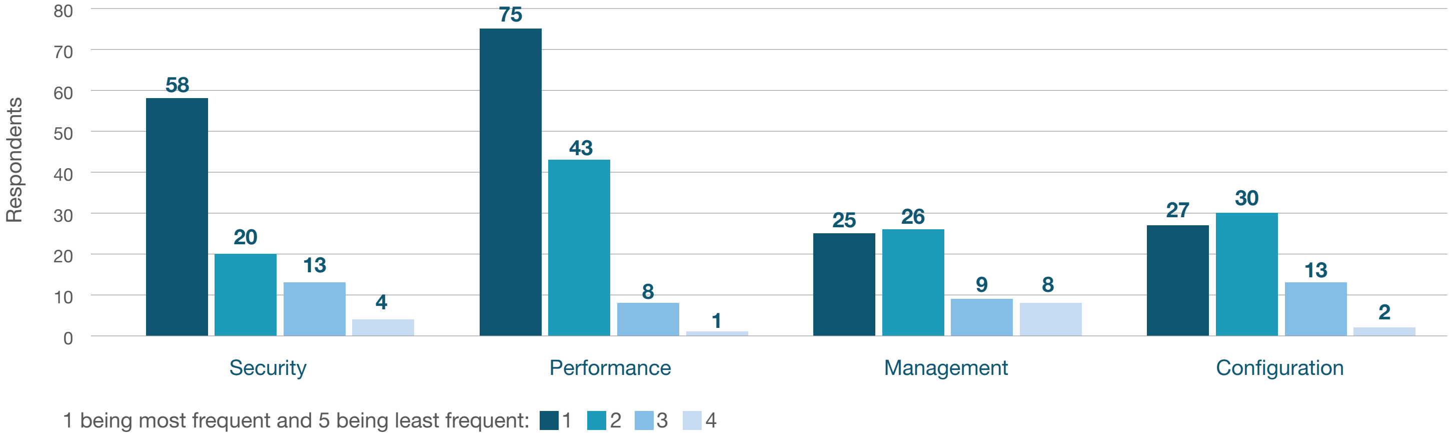
Q: *When using VPNs for cloud connections, which issues do you face? Select all that supply*



Another way to adjust the same question was to ask users to rank which issues they had most frequently. In a ranking hierarchy, performance and security were most often ranked as the top issues.

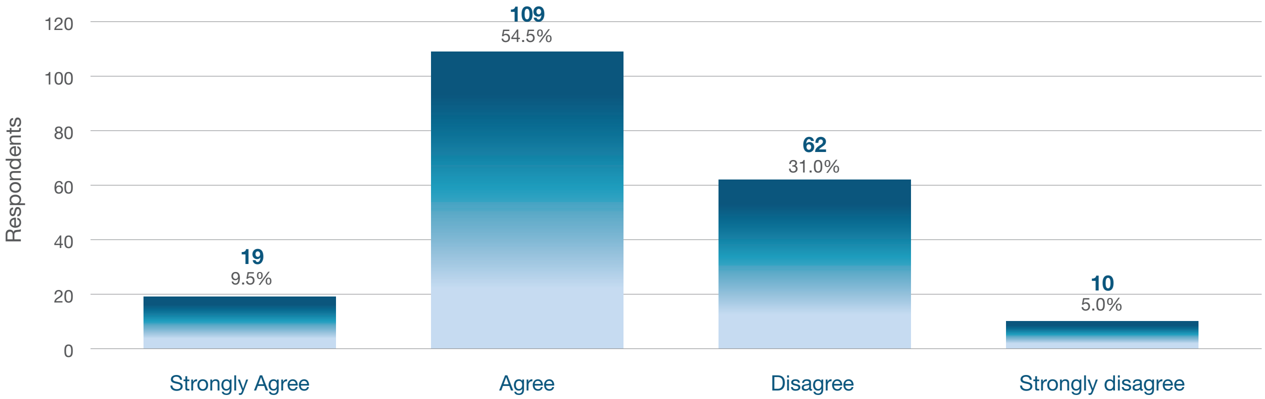
The follow question asked the users surveyed to rank performance issues.

Q: *Rank the top VPN issues you have faced when using VPNs for cloud connections. (1 = most frequent; 4 = lease frequent)*



Users also expressed reservations about using traditional VPNs in the Industrial IoT environment.

Q: Please select your level of agreement with the following statement: I believe that traditional VPNs are not the best solution for Industrial IoT device connectivity.



The majority of those surveyed agreed that VPNs are not the best solution in such cases.

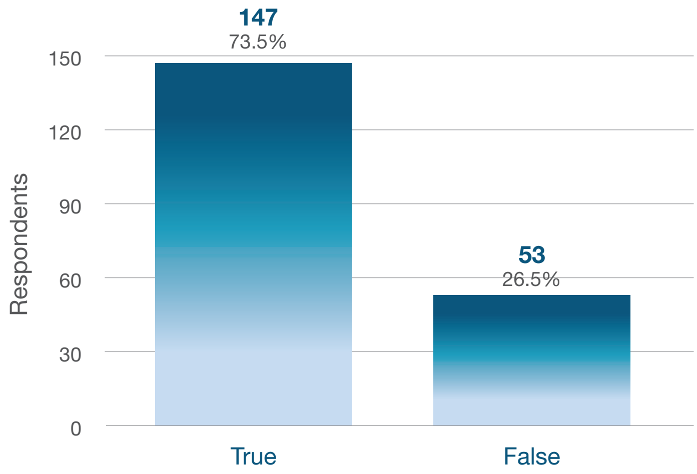
VIEWS ON MPLS AND SD-WAN

It's important to understand the relationship among legacy networks using private circuits such as MPLS, the next-generation architecture known as SD-WAN, VPNs, and additional potential solutions for cloud network. While some respondents believe that MPLS and SD-WAN can be used to network cloud applications, it's clear that there is the desire for additional layers of security and virtualization in applications such as IoT and cloud.

The view on using MPLS for cloud applications is split down the middle. 45.5% of the respondents agreed that carrier-delivered MPLS wasn't the right solution for cloud-based networking, while 46% disagreed with that statement.

This indicates that conviction is lacking in MPLS and that many IT managers believe additional technology is needed for networking cloud applications. One of the key areas of concern about MPLS is security. This is because MPLS does not have full security baked into the service, and requires additional measures, according to our respondents. 73.5% of the respondents said they run an additional layer of security over MPLS.

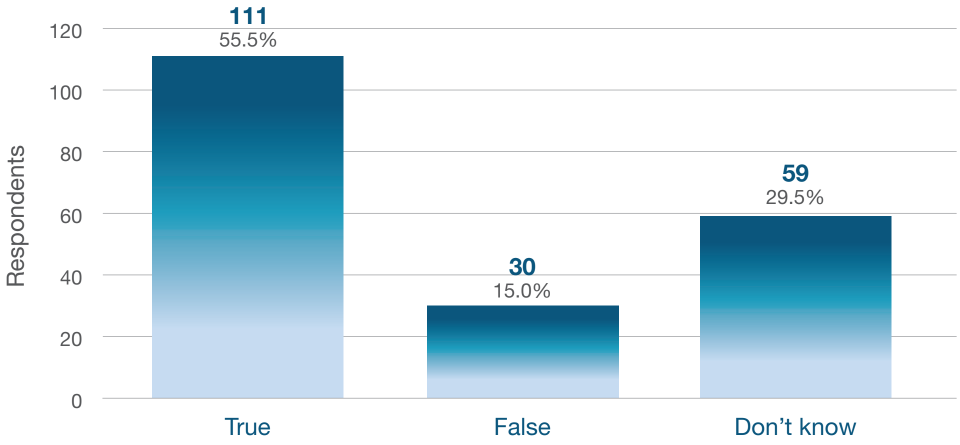
Q: True or False: I run an additional security layer of VPN encryption over the top of MPLS services to secure applications and data.



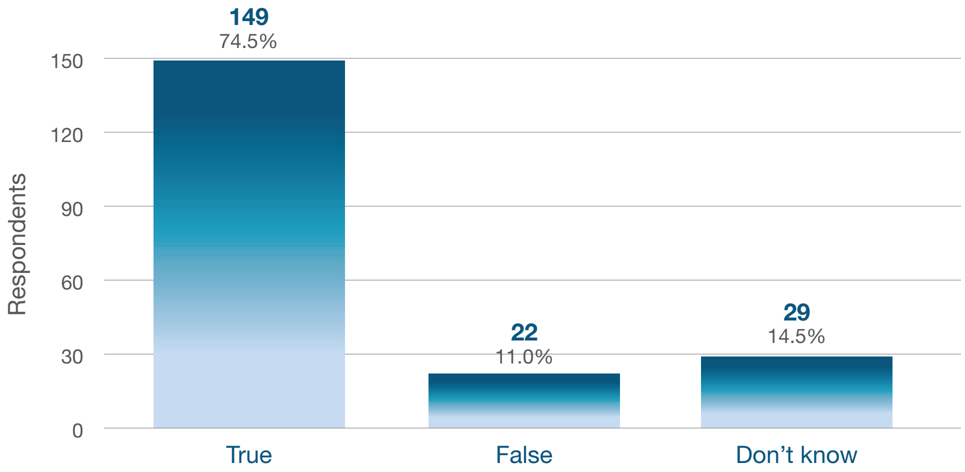
SEEKING ZERO TRUST NETWORKS AND HARDWARE ROOT OF TRUST

End-user research, including survey data and end-user interviews, indicates that more robust networking security features are desired for networking cloud applications. A majority of those surveyed indicated that both Zero Trust network architectures and hardware root of trust offer improvements to network security.

Q: I believe Zero Trust network architectures are a significant improvement in network security.



Q: True or False: I believe that hardware root of trust is a significant security feature for networking.



CONCLUSION: APPLICATION SPECIFIC NETWORKS (ASNS) COULD IMPROVE CLOUD NETWORKING AND SECURITY

Futuriom believes that the results of the Application Networking Survey show that IT staff, including networking, applications development, security, and networking professionals, are not satisfied with existing solutions for networking cloud applications, including the use of legacy VPN technology.

End users are seeking more flexible, software-based security and networking technologies that are native to the cloud and can be built into applications. This approach is used through the emerging networking technology known as ASNs.

ASNs are used to build software-only networks that can connect applications without requiring management of hardware devices, operating systems, or servers. Unlike VPNs, ASNs can be provisioned automatically by the applications in the cloud. This architectural design creates logical networks across the Internet and WAN to connect applications — an approach that NetFoundry refers to as AppWANs. These 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. An AppWAN can connect an endpoint or resource in the cloud that need to be connected securely and efficiently. It can be used to replace legacy technologies like VPNs and MPLS, which are tied to specific hardware devices but aren't nearly as flexible.

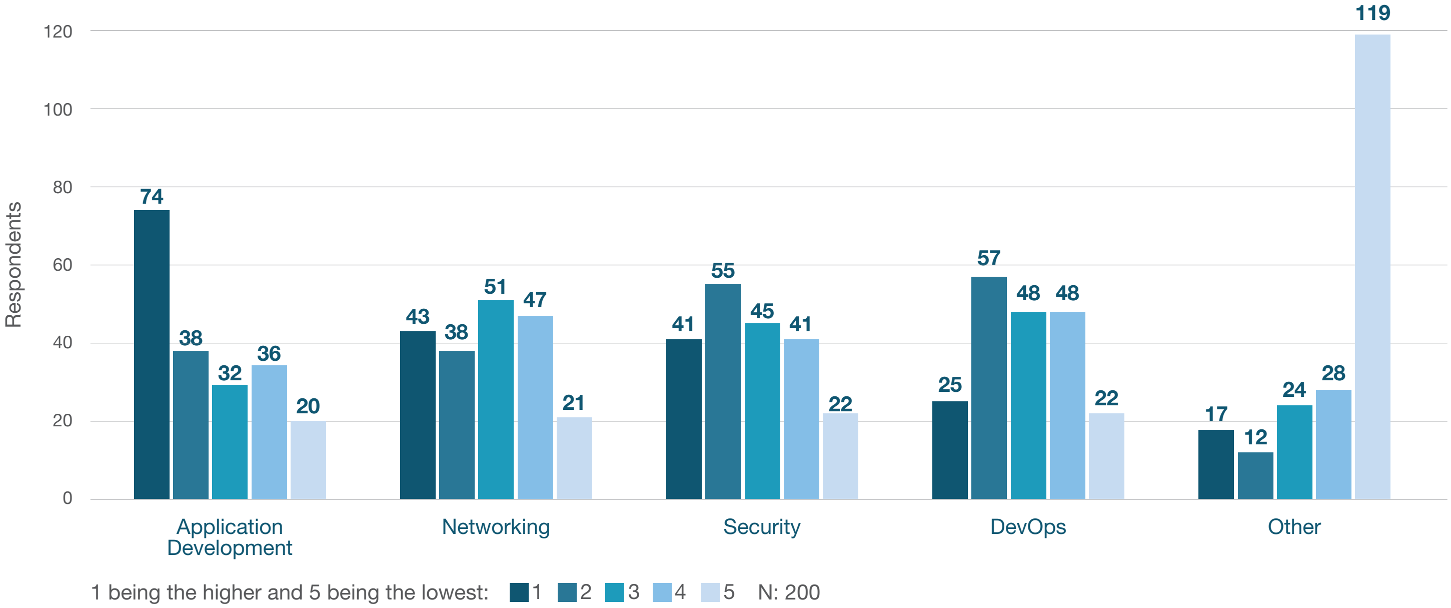
The key features of ASNs and AppWANs include:

- Secure networking tied to applications, not devices.
- Applications-based networking that is easy to set up and tear down with software.
- No "box management" necessary to instantiate a network.
- Networking and security features targeted at DevOps and software development staff rather than networking specialists.
- Capability to employ a native, Zero Trust security architecture as well as hardware root-of-trust on demand with high performance.

- Generally transparent to the end user ASNs are likely to serve to connect distributed applications in SaaS, IaaS, and PaaS environments, whether it's single cloud, hybrid cloud, or multi-cloud environments.

BACKGROUND ON THE SURVEY RESPONDENTS AND METHODOLOGY

Futuriom used an online survey tool to reach 200 IT staff balanced over applications development, networking, security, and DevOps functions. The survey used screening questions to assure that only the results from IT staff at management level and above were included in the data. The survey also asked the respondents to rank their responsibilities, as shown below. (1 being the higher and 5 being the lowest.)



NETFOUNDRY™
SPIN UP YOUR NETWORK

ABOUT THE SPONSOR: NETFOUNDRY

NetFoundry is the leader in Application Specific Networking, enabling businesses to instantly connect distributed applications in any cloud, on any device, anywhere with unprecedented simplicity. The NetFoundry platform enables businesses to securely and reliably connect applications without the constraints of VPNs, custom hardware and private circuits. NetFoundry is headquartered in Charlotte, North Carolina, with offices in San Francisco, New York, London, Bangalore and Singapore.