TEMPERED NETWORKS

Identity-Based Software-Defined Networking Brings Control and Simplicity

The Identity-Defined Networking phenomena is taking hold because businesses can't afford to wait.

The concept of Identity-Defined Networking, which enables the creation of instant overlay networks that are inherently secure and mobile—with no changes to the existing underlay network—appeals to 98% of survey participants

HOW COMPLEX ARE TODAY'S NETWORKS? Very. But nothing compared to what we will see by the end of this decade.

Just connecting business users who routinely switch between three or more devices, such as laptops, tablets, and servers, is no small task. Accelerated deployment of hybrid and multi-cloud architectures leaves organizations struggling to connect, provision, and secure their networks as workloads shift from on-premises to cloud. Then there's the OT (Operational Technologies) and Internet of Things (IoT) trend, which IDC projects will connect 30 billion industrial and consumer devices by 2020 .

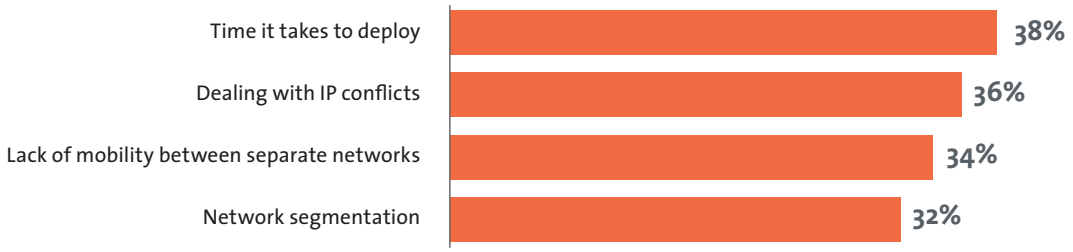
In a recent survey, 74% of IT decision makers conceded that securing network access and control is already a challenge. IDG Research Services partnered with Tempered Networks to survey director-level and higher executives in IT roles at companies of 500 or more to assess the pain points organizations are dealing with as they expand enterprise networks to the cloud.

Reflecting pent-up frustration with the complexities and vulnerabilities of traditional IP-based networking and security, virtually all respondents identified with the appeal of an alternative networking architecture based on identity rather than IP addresses. The concept of Identity-Defined Networking (IDN), which enables organizations to create instant overlay networks that are inherently secure and mobile—with no changes to the existing underlay network—is appealing to 98% of survey participants; the other 2% indicate it is somewhat appealing.

Verifiable, point-and-click

IDN overlays are based on verifiable machine identities, managed through a point-and-click orchestration engine that is incredibly easy. While VPNs and other security products can take days or weeks to set up, IDN overlays can be created in minutes. With private workgroups, it's as simple as sending an email invitation to end users in finance, for example, who with a one-click install, can join a secure finance overlay.

Figure 1. **Biggest Pain Points in Network Operations When Managing a Network**



With IDN, organizations can ensure that IoT device traffic is only visible to devices and applications that are necessary, rendering those devices invisible to anyone or anything else, no matter where they are.

Compare that to traditional provisioning, connecting, and securing processes, which 44% of survey respondents cite as their biggest pain point. Other challenges they are currently dealing with include managing distributed network policies, dealing with IP conflicts, and VPN and firewall complexity. The growth in network complexity is exposing an expanding attack surface that is difficult to manage and secure. Meanwhile, the effort to patch and more tightly control systems is driving up IT costs, according to 62% of survey participants.

IDN overlays, on the other hand, simplify network and security management while *improving* overall network performance, since traffic from machines that are not part of the overlay won't even be seen by the network connection. IDN has the added benefit of being able to traverse multi-cloud environments, enabling simple, secure connections between on-premises and cloud endpoints regardless of ISP, cloud provider, or existing network underlay.

Networking only provable machine identities

Sophisticated hackers can take advantage of a fundamental flaw of the TCP/IP protocol on which internet addressing is based. TCP/IP uses a connected device's IP address for both the identity of the device and its location on the network. As a result, devices are highly visible to hackers and the addresses can be spoofed from anywhere in the world.

IDN does not rely on IP addresses, but instead creates a namespace that works seamlessly with IP and DNS, stripping away the complexity of existing addressing and instead utilizing unique crypto identities that can be anywhere in the fabric. It no longer matters where a device is, it only matters *what* that device is.

IDN starts with zero trust and is based on the open Host Identity Protocol (HIP), which only allows networking of devices with provable host identities, creating a cloaked and unbreakable network segment. HIP was implemented at Boeing in 2004 to secure industrial control systems and has only recently been commercialized for the general market.

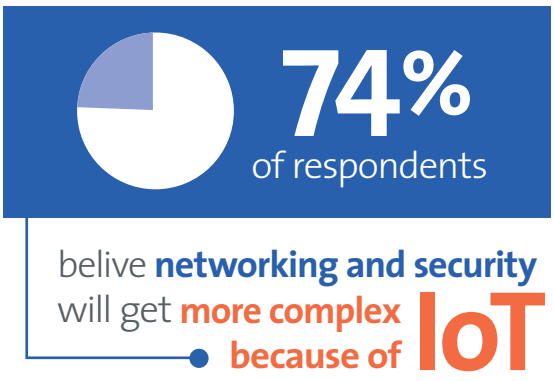
With HIP-based IDN, "only endpoints that are authenticated and authorized can communicate within an overlay segment, creating a fully isolated, hardened network zone that is operationally much simpler because there is no reason to use things such as NAT/PAT, VLANs, layer 3 VPNs and static routes," writes Zeus Kerravala, founder and principal analyst with ZK Research.

Line-of-business users can set up their own instant, elastic, private networks in minutes.

Only devices on a trusted whitelist can view, query, or detect HIP-based appliances. Meanwhile, users can be invited via email to download a HIP token, or can be provisioned with a HIP-embedded device that, when activated, automatically joins them to the HIP network. This enables a bring-your-own-network (BYON) approach in which line-of-business users can set up their own instant, elastic, private networks in minutes. Marketing, financial, and development teams can each create their own private networks, thus securing valuable information, protecting systems from malware, and improving overall network performance.

The IoT tsunami

The rapid proliferation of IoT represents a virtual tsunami of connectivity that threatens



With each device reliant on the TCP/IP location flaw, IoT provides criminals and other bad actors with literally billions of points of attack to try and exploit.

to drown enterprise networks. With a big push to put systems and machines on a common network for sharing data and streamlining operations, security is often an afterthought. In the IDG Research survey, 74% of respondents believe networking and security are going to get more complex because of IoT.

It takes weeks on average to provision a new resource on a network, using traditional networking solutions. How can organizations connect, secure, and manage thousands of devices, including endpoints that cannot protect themselves? IoT devices have already been exploited for Distributed Denial of Service (DDoS) attacks. With each device reliant on the TCP/IP location flaw, IoT provides criminals and other bad actors with literally billions of attack vectors to try and exploit.

IDN has the added benefit of being able to traverse multi-cloud environments, enabling simple, secure connections between on-premises and cloud endpoints regardless of ISP, cloud provider, or existing network underlay.

With IDN, organizations can ensure that IoT device traffic is only visible to devices and applications that are necessary, rendering those devices invisible to anyone or anything else, no matter where they are. Organizations can embed provable identities from the start for any IoT or machine-to-machine (M2M) device to eliminate the need to purchase multiple security and connectivity appliances to achieve secure connectivity over any existing IP network.

Why make a move now?

Tempered Networks pioneered IDN to make end-to-end privacy, security, and IP mobility possible by relying on provable machine identity that is simple, reliable, and ubiquitous. In the course of the past 30 years, we've gone from a world of manageable internet connections to one in which virtually any electronic device can be connected. For all the benefits, there have also been challenges, including security shortfalls as well as constantly increasing network complexity and costs, all surrounding an inherent TCP/IP defect—using an IP address as a device identity, a role for which it was never designed.

Tempered Networks uses HIP to provide products and services that comprise an encrypted IDN fabric. This fabric protects every connected resource with a unique crypto identity, instead of a spoofable IP address, so enterprises can cloak any IP or serial-enabled endpoint, machine, or network—with no IP modifications. This standards-based architecture supports all legacy and modern resources regardless of environment, allowing businesses of all sizes to reduce errors, minimize address-based rule sets, and reduce the need for complex point solutions such as VPNs, internal firewalls, and switches.

Now, your organization can instantly connect, cloak, encrypt, micro-segment, move, revoke, or failover for any networked resource, anytime, anywhere. It's a simple, cost-effective, and safe solution that guards against hackers and human error.

To learn more about Identity-Defined Networking, please contact Tempered Networks or visit their website.