ESG Lab Review

Identity-Defined Networking from Tempered Networks

Date: July 2017 Author**:** Kerry Dolan and Tony Palmer, Senior Validation Analysts

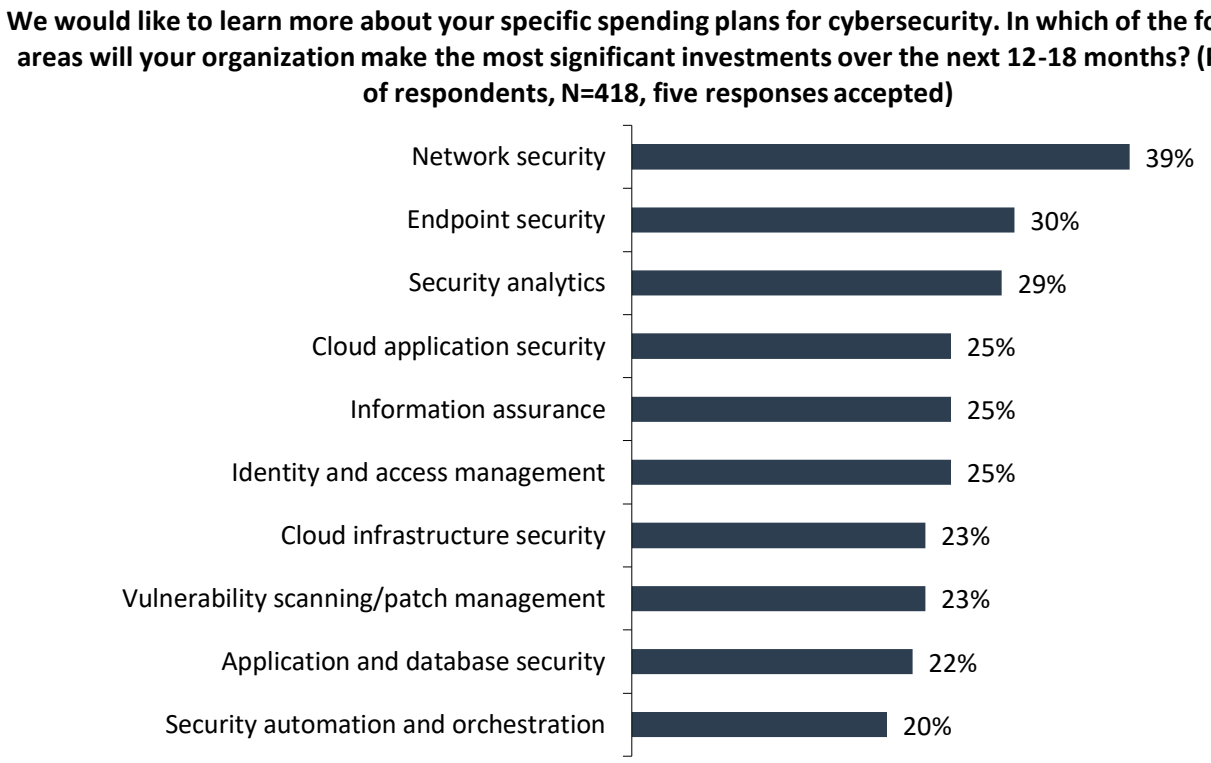
Abstract

This ESG Lab report documents hands-on testing of the Tempered Networks Identity-Defined Networking (IDN) solution. Testing focused on validating how Tempered's identity-first approach to networking can create private, segmented, and secure communications while dramatically simplifying connectivity between systems regardless of environment, network type, or location.

The Challenges

A major challenge to network security is its foundation in IP-based network addresses. IP addresses essentially changed the world—from communication to commerce—but they were designed only to identify location and enable reliable connectivity. They were not built to establish identity or deliver security. As a result, in this age of limitless hacking and cyber-attacks, IT organizations must turn themselves inside out with complex solutions—combinations of firewalls, VPNs, routing policies, ACLs, VLANs, etc.—to try to make ubiquitous networked devices secure. Simple configuration errors and IP address changes break the traditional model, leaving you vulnerable. It's no surprise, then, that in ESG research, network and endpoint security topped the cybersecurity priority list.[1]

Figure 1. 2017 Top Ten Cybersecurity Spending Priorities



Source: Enterprise Strategy Group, 2017

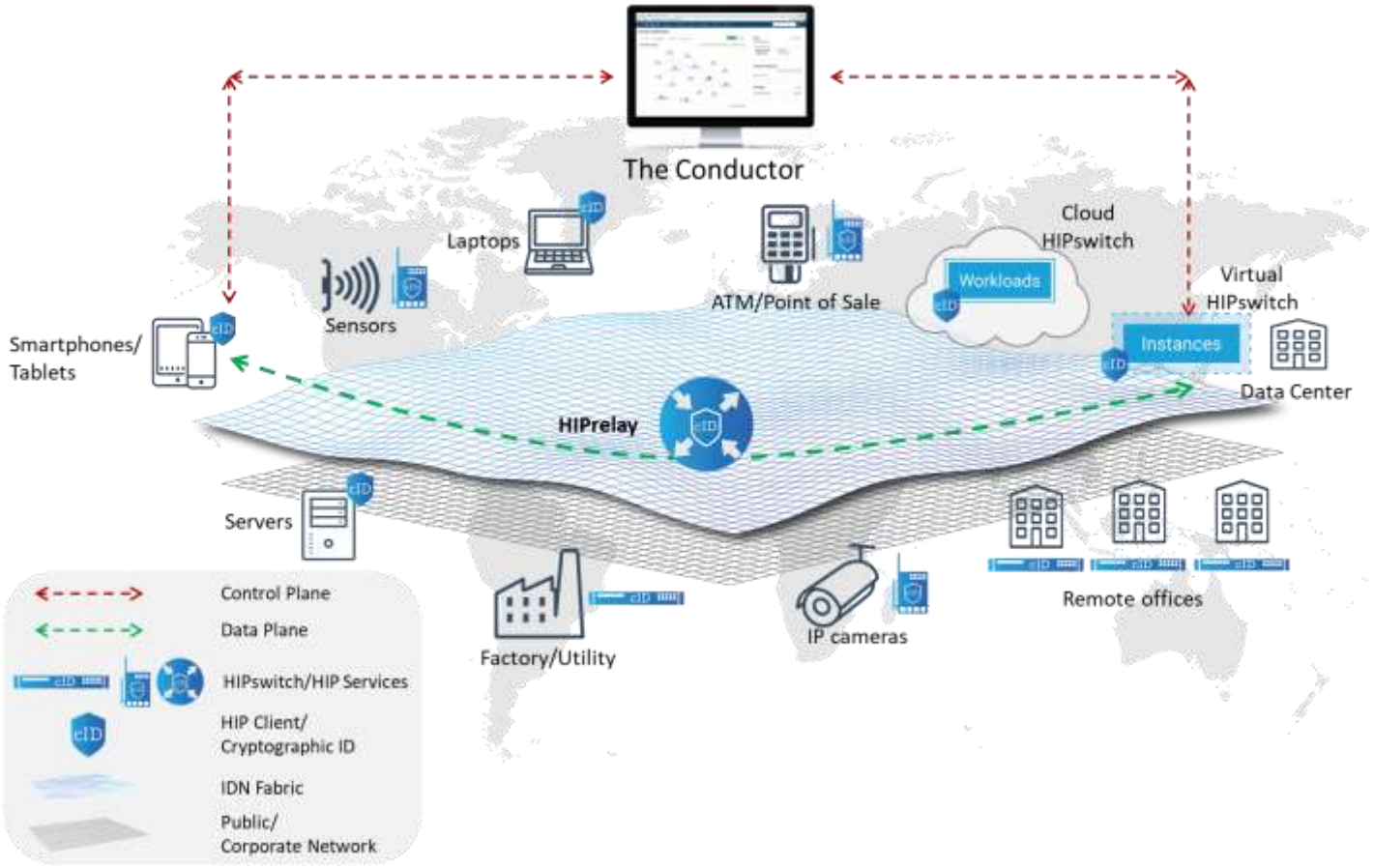
[1] Source: ESG Brief, *2017 Cybersecurity Spending Trends*, March 2017.

The Solution: Identity-Defined Networks from Tempered Networks

Tempered Networks offers a new network architecture that creates provable host identities for all networked devices—including servers, laptops, mobile phones, IP cameras, ATMs, machine sensors, and other IoT devices—so that each endpoint is defined by a cryptographic identity instead of an unsecure IP address. Once devices are proven and identifiable, a secure, encrypted communication tunnel is created among whitelisted devices only. Devices in this trusted layer are cloaked so they cannot be detected via the underlying network. Because they cannot be seen, they cannot be hacked.

The Tempered Networks solution can include Ethernet, cellular, wireless, radio, and serial over IP networks and can be deployed without operational disruption. Tempered Networks touts the ease of installation and management that contribute to the solution's cost efficiency.

Figure 2. Tempered Networks IDN



Source: Enterprise Strategy Group, 2017

Host Identity Protocol (HIP)

The solution is based on the Host Identity Protocol (HIP), an open standard ratified in 2015 by the IETF. HIP has been in production for more than a decade at a large aerospace company and in custom deployments, primarily in federal agencies. Only recently was HIP commercialized for the general market. HIP enables separation of the identifier and locator roles of IP addresses, replacing the identifier with a public key identifier (PKI) from a Host Identity namespace for mutual peer authentication. With built-in encryption and authentication, it is resistant to denial-of-service and man-in-the-middle attacks. With HIP-enabled solutions, IP addresses are used only to locate hosts, not to identify them, enhancing mobility.

Primary Components

The Tempered Networks solution comprises two primary components:

- The Conductor—Available as a physical or virtual appliance or in the AWS cloud, the Conductor is Tempered Networks' centralized orchestration and intelligence engine that connects, protects, and disconnects any resource globally. No traffic goes through the Conductor; it only defines and enforces policies for HIP Services. HIPswitches deployed on the network automatically register with the Conductor using their cryptographic identity.

- HIP Services— HIP Services provide software-based policy enforcement, enabling secure connectivity among IDN-protected devices, as well as cloaking, segmentation, identity-based routing, and IP mobility.
    - These services are delivered as client-side software for laptops or servers, and by HIPswitches, which can be physical, virtual—supporting VMware ESXi and Microsoft Hyper-V—and cloud-based, supporting Amazon Web Services (AWS). HIP Services can also be embedded in custom hardware or applications. HIPswitches have no TCP or UDP service ports that can be listened in on, and can only be configured through the Conductor.
    - Placing HIPswitches in front of any connected device renders the device HIP-enabled and immediately micro-segments the traffic, isolating inbound and outbound traffic from the underlying network.
    - HIPrelay is a product add-on to certain HIPswitch models.
        - HIPrelay works in conjunction with Tempered Networks' HIP Service-enabled endpoints to network and encrypt communications between distributed, *non-routable* hosts or systems from any location.
        - The HIPrelay does not use Layer 3 or 4 rule sets or traditional routing protocols; instead, encrypted communications are routed and connected based on provable cryptographic identities traversing existing infrastructure as any encrypted traffic would.
        - HIPrelay can be deployed in clusters and distributed across the Internet whether on-premises or in the public cloud.

Unlike SDN and SD-WAN solutions, IDN enables the bridging and seamless integration of Layer 2 and 3 networks without requiring modification to an existing network's switching and routing infrastructure across the LAN and WAN.

Tempered Networks solutions deliver fast, flexible, scalable protection for devices across the globe, immediately reducing risk by reducing the attack surface. They are extremely easy to deploy and manage, and enable fast provisioning and revocation of devices and security services.

ESG Lab Tested

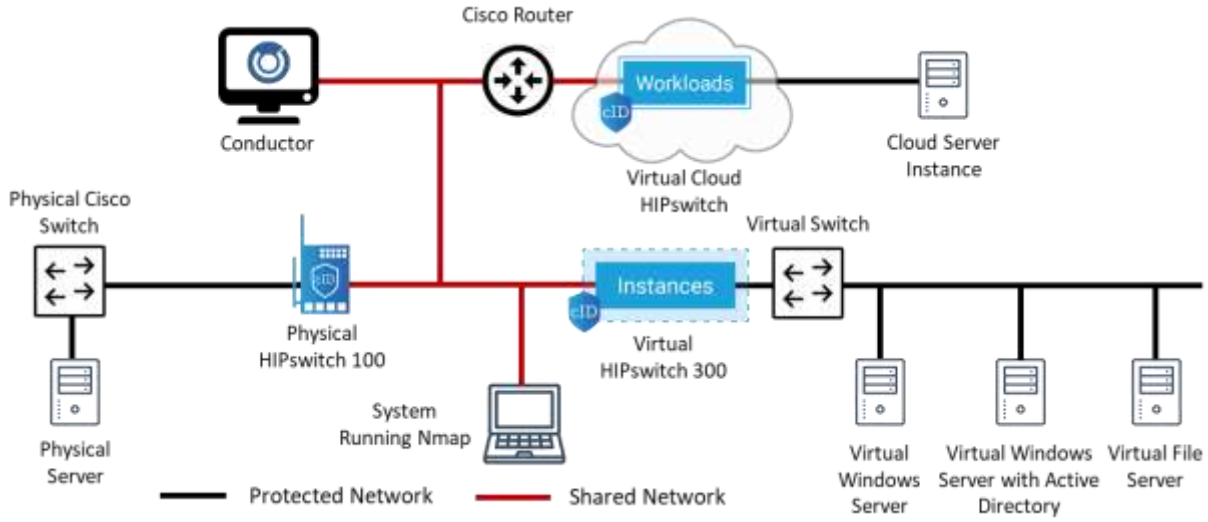
ESG Lab created a test environment connecting multiple industry-standard systems running Windows server and workstation operating systems and Apple Macintosh systems over a standard wired Ethernet network constructed using common switches, routers, and other network devices. Physical, virtual, and cloud-based HIPswitches were utilized as well as HIPclients for Windows and Mac. It's important to note that this subset of available HIP Services was chosen for these tests to demonstrate IDN fabric functionality for on-premises, remote site, and cloud-based workloads as well as a variety of remote access clients. HIP Services come in a variety of virtual, physical, cloud, software, and embedded flavors. Tempered can also provide embedded software to third-party providers and manufacturers to realize their vision of enabling HIP and the orchestration of secure networking for any connected thing.

Stopping Hackers with Identity-based Micro-segmentation

First, ESG Lab examined how identity-based micro-segmentation stops lateral hacker reconnaissance. Two servers running Windows Server 2016 were installed on an open, shared network segment, as illustrated in Figure 3, with one server running Active Directory. ESG Lab remotely logged into one of the servers and attempted to connect to the other one using the nMap open source utility for network discovery and security auditing. nMap was run against the Windows server before

and after deployment of the Tempered Networks IDN platform. This test was designed to mimic what a hacker who has penetrated an internal network could or could not discover and fingerprint. Hackers will often do stealthy reconnaissance by executing randomly timed and infrequent scans of an internal network to discover and identify high-value targets.

Figure 3. The ESG Lab Test Bed



It took less than five seconds for the Windows Server running Active Directory to have all its listening ports scanned and identified, as seen in Figure 4. In this situation, hackers would easily recognize that they could start targeting this Active Directory server with a number of exploits.

Figure 4. nMap Results on an Open, Shared Subnet

```
$ nmap -Pn 10.11.1.120

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-05 10:03 PDT
Nmap scan report for 10.11.1.120
Host is up (0.011s latency).
Not shown: 982 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open http
88/tcp   open kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
443/tcp  open  https
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open ldapssl
3268/tcp open globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
49154/tcp open  unknown
49155/tcp open  unknown
49159/tcp open  unknown
49160/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.55 seconds
```

Next, ESG Lab added the Windows Server running Active Directory to a trusted micro-segment. When nMap was run again, it was unable to discover any listening ports; the system was effectively cloaked and invisible. The host is reported as "up" because the nMap command ignores ICMP failures and assumes the host is up but not responding to ICMP.

Figure 5. nMap Results After Server Added to Trusted Micro-segment

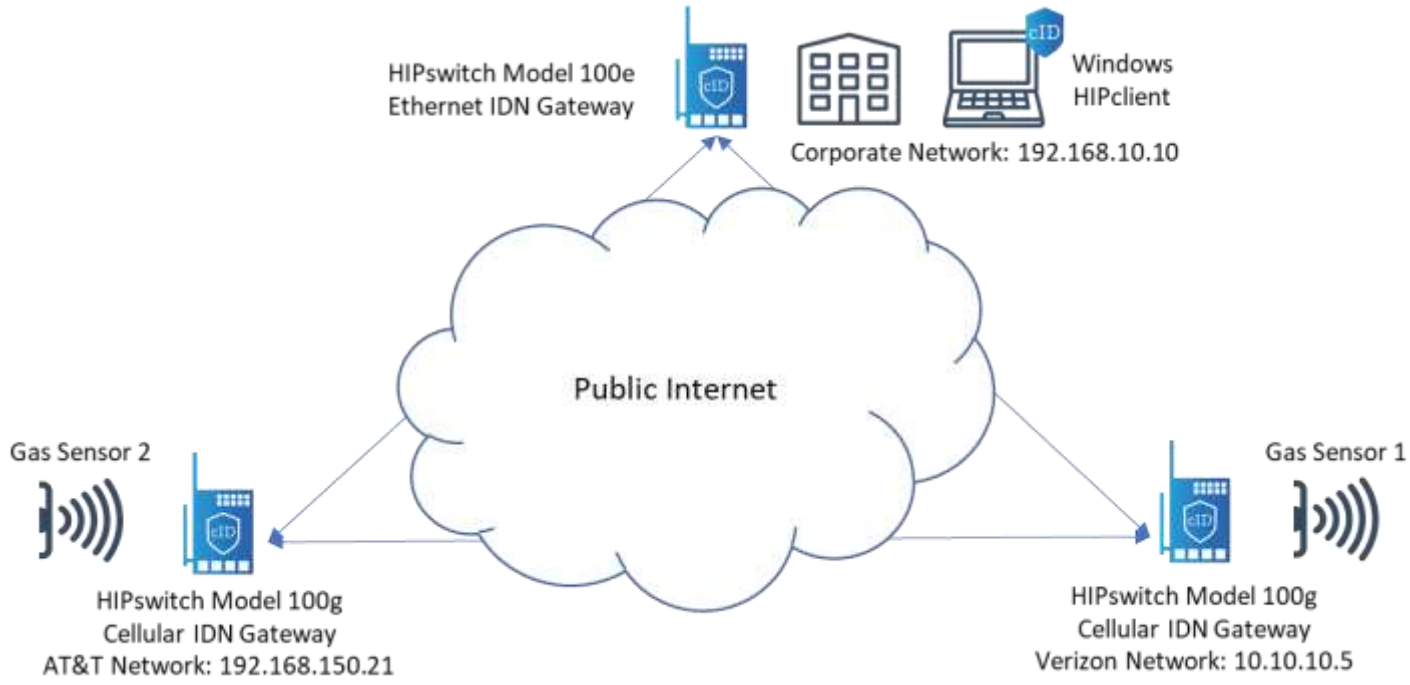
```
$ nmap -Pn 10.11.1.120

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-05 09:49 PDT
Nmap scan report for 10.11.1.120
Host is up.
All 1000 scanned ports on 10.11.1.120 are filtered

Nmap done: 1 IP address (1 host up) scanned in 201.78 seconds
```

This is the same result obtained when nMap was run against the same server with its network interface disconnected from the network. Finally, ESG Lab assigned trust to the Windows server from which we were running nMap in the same micro-segment and ran nMap again. Once trust was established, we obtained the same result as seen in Figure 4. This series of tests validated that all services were available to trusted machines within the micro-segment, but they are not visible or reachable to any untrusted machines. No changes to the underlay network were required and there was no disruption of services.

Communications between Non-routable Devices

The next tests were designed to evaluate two scenarios involving communication between non-routable devices. The test illustrated in Figure 6 emulated an IoT application: A public utility might deploy sensors in the field and connect them to the Internet using different cellular carriers based on availability at each location. In this test case, the monitoring and analytics software at the corporate site required bidirectional communication with all sensor locations, which required communication between themselves as well.

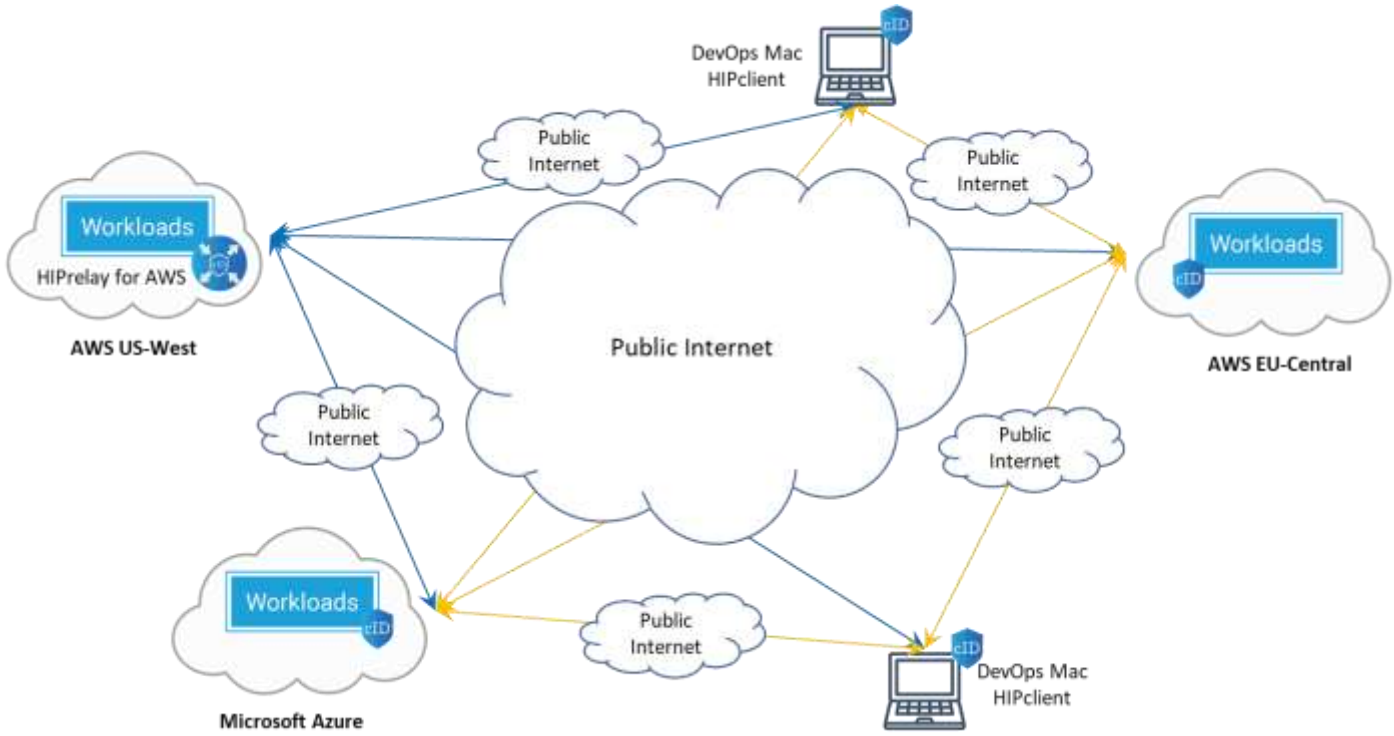
Figure 6. Routing Between Two Different Cellular Networks



Using the HIPswitch Model 100g Cellular IDN gateways, ESG Lab created a trust relationship between both sensors and the Windows system on the corporate network in seconds. All devices were able to communicate bidirectionally with one another with no reconfiguration of the underlying networks.

Finally, ESG Lab looked at Virtual Private Cloud (VPC) peering between VPCs in different regions—or across different clouds—a use case that has been described as impossible. In fact, AWS documentation states explicitly: *You cannot create a VPC peering connection between VPCs in different regions.*[2] A VPC peering connection can help organizations peer VPCs across multiple accounts to create a file sharing network, or to allow VPCs to access resources in other VPCs for availability.

Figure 7. Multi-cloud Peering for DevOps



As seen in Figure 7, Tempered Networks HIPrelay and HIPswitches enabled ESG Lab to create a multi-region and multi-cloud peering configuration. DevOps resources were shared between the Amazon EU-Central and US-West regions as well as between Amazon US-West and Microsoft Azure.

Why This Matters

Security is top of mind in every organization today, for good reason—just a look at the news will remind you that threats abound. However, the dependence on networks to conduct business creates vulnerabilities that are exacerbated by complex security technologies and processes. That dependence is here to stay, as businesses run on many devices and locations that must connect, so making those connections secure is of paramount importance.

The Tempered Networks solution uses cryptographic host identities to improve security beyond the traditional IP network. ESG Lab validated the ability to quickly and easily create secure, encrypted communications channels that are isolated from other network traffic. ESG Lab also enabled secure communications between non-routable devices and secure peering across different cloud regions and providers. These tasks were simple to execute, took only minutes, and did not require changes to the existing infrastructure. This can save organizations time and money while improving their security profile.

[2] http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/vpc-peering-basics.html#vpc-peering-limitations

Customer Interview

ESG Lab spoke with the chief infrastructure architect of a large company with more than 500 buildings across the world, and tens of billions of dollars in annual revenue. The company must comply with regulations in 135 countries, including the stringent privacy and security regulations of the European Union, as well as Sarbanes-Oxley accounting regulations, PCI Data Security Standards for credit cards, and HIPAA for healthcare.

This company deployed the Tempered Networks solution in less than a day. The organization uses numerous mission-critical applications that do not use DNS, and were written for only a single desitination IP address, leading to serious availability problems and creating a ripple effect across locations. If the destination server went offline, the distributed pieces of equipment could not function until IT created a new server using the same IP address and security tokens in the same data center. But if the whole data center went offline, this not only required bringing up a new server with the same IP address in another data center, but required routing updates across their global MPLS network, which took longer than an hour and was error-prone. Thus, it didn't meet their availability requirements but was also extremely difficult to upgrade the software. The Tempered Networks solution solved these problems. As the chief architect commented, "This [Tempered Networks] product allows us to move that reality of where that software runs based on business needs, and not based on the network team reconfiguring something. [It] allows us to move traffic flows from one physical server to another, so we can deal with software upgrades, version differences, and availability."

Another key application included built-in protection for server authentication, but not for client authentication—leaving it vulnerable to spoofing. The company installed an add-on security product to authenticate users, but that solution also assumed a single IP address. With the Tempered Networks solution that uses device cryptographic identity for networking and access control, they can now move that service where they need it within the IDN fabric and eliminate the additional client security solution.

In addition, some equipment in several locations is used on a timeshare basis using IP addresses and ACLs for segmentation and access control. The company can now base local and wide-area micro-segmentation on provable host identities where every machine authenticates and authorizes before a TCP session can be established. They can now also fail that service over automatically between data centers without impacting firewalls or routing processes. This eliminates the typical network operations process of waiting for someone to report the problem and then forcing a route change. "Real-time, application-aware traffic routing is another significant feature that we are getting out of this," said the chief architect.

This company has big plans for its Tempered Networks solution in the coming years. The team expects to roll it out to 100+ locations and three data centers, using a mix of physical and virtual HIPswitches as well as application and client downloads. In addition, they plan to use the Tempered Networks' HIPclient on more than 60,000 employee mobile devices that must be able to travel from cellular to Wi-Fi networks without losing application connections while providing device-based access control.

Why This Matters

For a large global company, agility is essential and downtime can be expensive. For this organization, the Tempered Networks solution is solving fundamental problems with legacy applications and networks without having to change the network topology. It has not only increased security, but also minimized business disruption, enhanced application mobility, improved application availability, and reduced management. Critical systems can be routed according to real-time needs without taking systems down.

The Tempered Networks solution also empowers the business units to create the data environments they need, which is often difficult, especially as business needs change. "The other amazing thing this gives us is the fact that the business units determine the rules of how the product works – so a change in business policy doesn't require configuration changes on the network," commented the chief architect.

The Bigger Truth

Organizations today demand flexible and dynamic connectivity across global deployments to compete in today's business landscape. Most data centers are on the road to becoming hybrid with a mix of on-premises and cloud-based services as well as mobile devices, and many are adopting IoT devices such as IP cameras and machine sensors. Unfortunately, cloud and IoT adoption increase risk—particularly as control systems come online for critical infrastructure such as water supplies, power plants, etc. Perimeter-based security is not sufficient—risks come not just from a cybercriminal trying to access personal information for financial gain, but from state-sponsored threats that can be devastating. Improving security and explicit access control is of paramount importance, and remains the top IT priority for most organizations.

Today, organizations use a complex mix of networking and security solutions and technologies that are too easily compromised—for instance, a simple misconfiguration or change of IP address can break the security paradigm, leaving you vulnerable as well as requiring significant administrative time and cost to fix. Organizations work hard to create flexible, agile environments to keep up with the competition—but if they are not secure, none of that matters.

Tempered Networks Identity-Defined Networking changes the network architecture from connectivity and policy enforcement based on IP addresses to an architecture based on cryptographic identities. It creates a trusted network architecture that solves networking and security problems that traditional IT architectures cannot. And it does so while reducing costs and dramatically simplifying deployment and management, without disrupting operations. Customers gain simpler connectivity, better security with less complexity, and without having to separate networking and security policies and technologies across their global environment—including on-premises, cloud, IoT, etc.

IDN creates a unique cryptographic identity for every endpoint, instead of using the IP address as an identifier. This enables organizations to instantly connect, cloak, and segment devices, as well as to instantly revoke permission, move workloads, and failover. If a hacker steals a user's credentials and attempts to use them from another machine, the breach will fail because security is based on the device identity only. The attack surface is reduced—should a breach occur, it cannot spread laterally; in contrast, while a VLAN would prevent a breach from spreading to the full network, it cannot prevent infiltration across that VLAN. IDN also reduces the effort to remediate after a breach—IT can focus on the breached endpoint, not on patching vulnerabilities across the entire network.

ESG Lab validated that with Tempered Networks IDN, organizations can—in a few clicks—segment networks, cloak devices to prevent hacking, and segment third-party access with instant provisioning and revocation. Any IP resource can be easily moved across networks, subnets, or the cloud, and organizations can deliver secure remote connectivity, instant DR/failover, and secure machine-to-machine communications. Deployment and provisioning are extremely simple and fast, and the Conductor delivers simple, non-disruptive, policy-based orchestration that scales easily.

The benefits of Tempered Networks IDN are sometimes difficult for prospects to believe. Because it uses a host-identity-based security foundation instead of a traditional IP-based one, IDN can make your network secure by default, drastically simplify provisioning and management, reduce the attack surface, and make IT teams more productive. This all translates to lower OpEx, while the improved connectivity, access, and encryption with segmentation reduce the hardware requirements and therefore CapEx.

ESG Lab was very impressed with the Tempered Networks IDN solution. There are some features on the roadmap that will improve it, particularly expanding beyond only Windows devices; the addition of Linux and iOS endpoints will be a good start. IDN is worth a close look for organizations that want to make networking simpler and upgrade security while reducing costs. In addition, we believe it's a smart idea for organizations to investigate the Host Identity Protocol (HIP) and begin thinking of its application in transforming their networks of connected things.