Identity-Defined Network (IDN) Architecture

UNIFIED, SECURE NETWORKING MADE SIMPLE

ABSTRACT

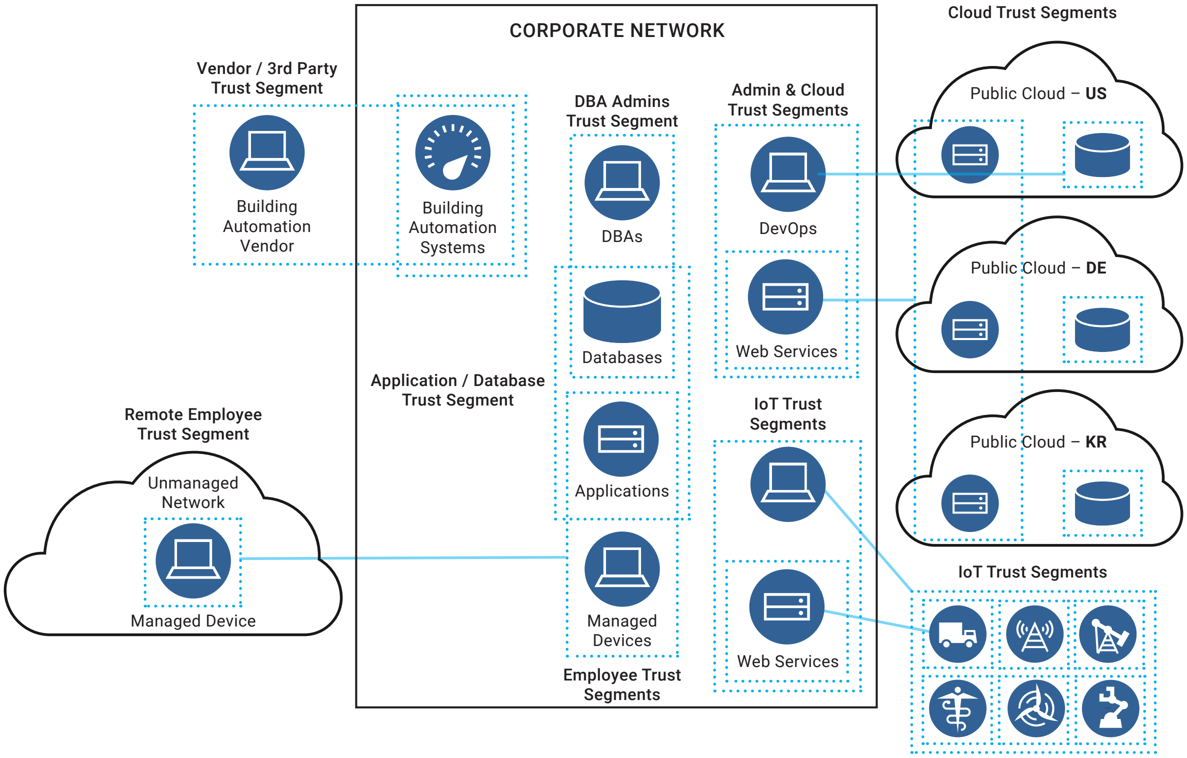
This white paper explains a newer, simpler approach to securely network, segment, move, or revoke any IP resource – anytime, anywhere. The outcome of deploying an IDN overlay is the ability to connect, protect, move, failover, and disconnect any resource globally, instantly. While enabling instant provisioning and revocation for any connected system within the overlay fabric, up to 90% of an organization's attack surface can be reduced, significantly lowering business risk. The result is an architecture that can save an IT organization up to 25% of their IT budget by eliminating unnecessary CapEx and OpEx, accelerating the time to provision networking and security services, and reducing the cost of compliance and audits. Coupled with the lowest TCO on the market, Tempered Networks has begun a secure networking revolution.

EXECUTIVE OVERVIEW

Tempered Networks' Identity-Defined Network (IDN) is a unified, secure networking architecture that significantly reduces IT complexity, is simple to orchestrate, and enables the instant provisioning and revocation of networking and security services with minimal, if any, modification to the underlying network, applications, or infrastructure. A significant reduction, if not elimination of complex firewall rules, VPN policies, keys, ACLs, and VLAN management are no longer required for unified and secure networking. Tempered Networks' IDN is built with an "orchestration and manageability first" mindset, enabling controlled, predictable, and verifiable self-service by authorized technical teams.

The outcome of a Tempered Networks IDN deployment is up to a 90% percent reduction in the overall network and system attack surface through device cloaking and simple trust-based segmentation, which isolates the reach of an attacker even if a device were compromised (Figure 1). The IDN also removes the frequent constraints associated with IP mobility, migration, and failover because an IP address no longer serves the dual purpose of identifier and locator. IDN benefits are achieved through better containment and segmentation, device cloaking, a Host Identity Namespace, simplified multi-homing, and instant failover, all within a unified encrypted fabric. The IDN's Software-Defined Segmentation provides effortless and verifiable micro, macro, and cross-boundary segmentation, which is uniquely enforced by device-based cryptographic identities (CIDs) based on the Host Identity Protocol standard (HIP RFC's 5401, 7401, and 7402). Devices are natively cloaked and invisible to hacker reconnaissance, and protected against DDOS, MiTM attacks, IP spoofing and other types of network and transport layer attacks.

SOLUTION OVERVIEW



A unified secure networking fabric is now possible spanning any IP resource, location and link medium with little to no modification of the network and security underlay or applications. Policies are distributed by the Conductor and enforced by HIP Services endpoints. Devices can be automatically or manually segmented, migrated, failed over or revoked within the encrypted overlay.

The IDN architecture incorporates a fully encrypted fabric that is orchestrated through an intuitive, visually-driven management and orchestration engine. Unlike traditional IP networking and SDN approaches, Tempered Networks' solution requires few, if any, changes to the underlying network or security infrastructure, significantly reducing complexity and cost, and increasing organizational responsiveness.

Tempered Networks' IDN design objective is based on the principle that it must be simple to connect, disconnect, segment, move, failover, or revoke any resource or network instantly. The result is an approach that can enable self-service by business units, yet satisfy corporate IT's requirement to control and verify policy enforcement (Figure 1).

The flexibility of the IDN allows for securely networking local and remote resources to services, regardless of where a device, host or network is located; whether the resource is corporate managed, a 3rd party vendor, external web services, or part of an organization's supply chain. Because IDN security policy is based on a unique, long-lived CryptoID (CID), rather than on a short-lived IP address, whose ephemeral nature is constrained within classic IT infrastructure, the IDN can deliver secured on-demand network provisioning for any resource – anywhere, at any time.

De-coupling the identifier and locator functions of an IP address restores its original purpose as a resource locator, and using unique CryptoIDs are what makes the unified secure IDN approach not only resilient but practical. Unlike SDN technologies, networking and security policy orchestration is made to be so simple that authorized business teams can easily make their own policy changes without involving other teams or risk exposing corporate networks and other connected resources.

As a result, organizations now have a common unified architecture that significantly reduces attack vectors and configuration errors while improving network and operational efficiency. Network and resource provisioning is simplified and can now be done in minutes. Failover is faster, predictable, and easily verifiable. Dependencies on complex firewall rules, VPN policies and key management overhead, ACLs, and VLAN configuration is greatly reduced. Managing a simple IP address change, migration, addition of a new network, office, or kiosk, or providing temporary and controlled 3rd party access no longer requires significant time and expertise. The complexity of network and security provisioning will no longer constrain an organization's ability to quickly adapt regardless of where a resource is located and whether it's coming from a managed or unmanaged network.

PRODUCT PLATFORM OVERVIEW

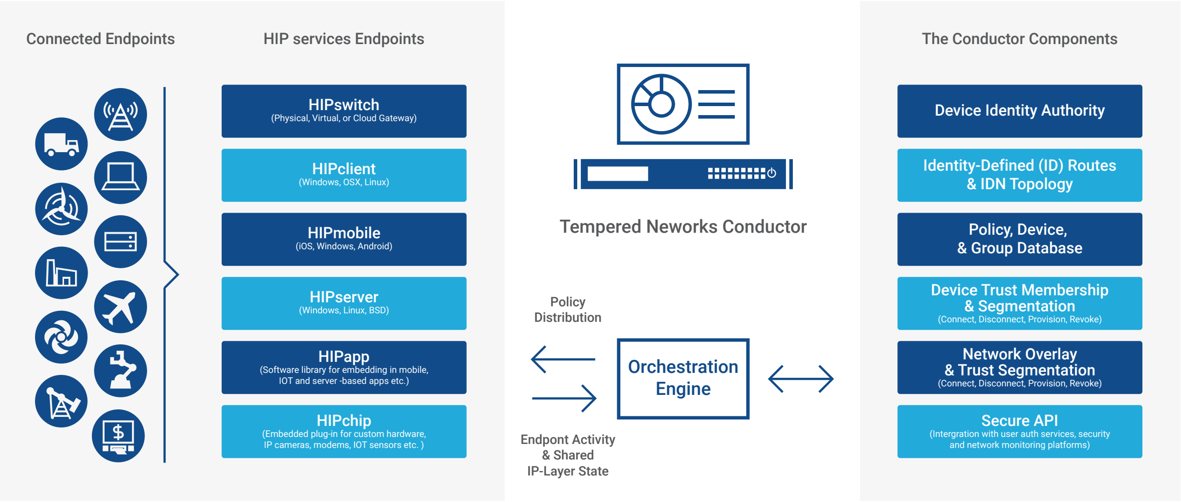

Connected Endpoints
HIP services Endpoints
HIPswitch
(Physical, Virtual, or Cloud Gateway)
HIPclient
(Windows, OSX, Linux)
HIPmobile
(iOS, Windows, Android)
HIPserver
(Windows, Linux, BSD)
HIPapp
(Software library for embedding in mobile, IOT and server -based apps etc.)
HIPchip
(Embedded plug-in for custom hardware, IP cameras, modems, IOT sensors etc.)
Tempered Neworks Conductor
Policy Distribution
Orchestration Engine
Endpont Activity & Shared IP-Layer State
The Conductor Components
Device Identity Authority
Identity-Defined (ID) Routes & IDN Topology
Policy, Device, & Group Database
Device Trust Membership & Segmentation
(Connect, Disconnect, Provision, Revoke)
Network Overlay & Trust Segmentation
(Connect, Disconnect, Provision, Revoke)
Secure API
(Intergration with user auth services, security and network monitoring platforms)

Figure 2: Tempered Networks IDN Architecture and Orchestration Model

Building an IDN fabric requires that two or more HIP Service endpoints be deployed symmetrically either in a hub and spoke topology, mesh, or both (Figure 2). Every HIP endpoint within the fabric knows the IP-layer state of its peers, and every peer maintains Identity-Based Routing (IDR) tables.
Here are a few of the high-level functions that the IDN platform delivers:

- Device cloaking and automatic AES-256 encryption tunnels between all IDN endpoints
- Secured VLAN isolation and micro, macro, and cross-boundary segmentation
- A default zero trust model with one-click trust establishment based on unique device CIDs
- Transparent mobility of secured devices and services within the fabric
- Connectivity for secure Layer 2 or Layer 3 networks across any link medium
- Network transparency, resiliency, and instant failover
- Rapid provisioning, revocation, and instant verifiable quarantine
- Visual Trust Map to assist with proving PCI and other compliance requirements
- Flexible gateway deployments supporting physical, virtual, and cloud appliances
- Extensibility down to clients, servers, applications, and even embedded hardware

In the near future, Tempered Networks will be able to realize the objective of a self-healing optimized mesh of HIP Services that can route around problems within an underlay network further overcoming the complexity of managing IP networking infrastructure and resilience.

The Conductor

Policy-Based Orchestration

Tempered Networks' Conductor is the orchestration engine and intelligence behind an IDN. As shown in Figure 2, the Conductor drives simple configuration of policy and issues unique Cryptographic IDs (CIDs) to the IDN endpoints that enforce explicit trust relationships through device-based whitelisting. The Conductor is the engine that ensures all HIP Services are up-to-date and synchronized and collects metrics as well as active state information from the HIP Service endpoints within the IDN fabric. It also provides the secure API that enables integration and automation with other security and networking services like directory services, SIEMs, and monitoring tools. Instant quarantine or failover can now be automated based on events detected by these systems.

HIP Services

Secure Networking Enforcement Points

HIP Services (Figure 2) or IDN endpoints are software products delivered in different form factors to support Tempered Networks' design vision of secure and mobile networking for any device, anywhere. They provide cloaking, secure connectivity, identity-based routing, IP mobility, and micro, macro, as well as cross-boundary segmentation enforcement all within the military-grade encrypted fabric. They enforce the Conductor's provisioning, de-provisioning, and revocation of trust of any managed IP resource behind a HIP Service. HIP Services follow the Host Identity Protocol standard, which initiates trust before transport communication is established and any data is exchanged between the HIP Service and other authorized HIP Service endpoints. Tempered Networks' Conductor orchestrates policies across HIP Service endpoints that are distributed throughout the IDN fabric where the Conductor maintains state but does not require persistence for HIP Services to function.

HIP Services enable functionality that is independent from and can separate business traffic flows from normal network forwarding logic. Networking and security teams can now innovate and move as fast as DevOps, but with a high degree of control, predictability, and verifiability in response to new business needs.

These IDN endpoints make IP mobility not only possible, but extremely simple and practical. Using the cryptographic identity, HIP services enable the mobility and migration of an IP resource anywhere within the fabric without requiring changes to the networking or security underlay. This decoupling overcomes many of the addressing, routing, mobility, and failover challenges associated with traditional IP networking and SDN technologies.

HIP Services (Figure 2) or IDN endpoints are software products delivered in different form factors to support Tempered Networks' design vision of secure and mobile networking for any device, anywhere. They provide cloaking, secure connectivity, identity-based routing, IP mobility, and micro, macro, as

well as cross-boundary segmentation enforcement all within the military-grade encrypted fabric. They enforce the Conductor's provisioning, de-provisioning, and revocation of trust of any managed IP resource behind a HIP Service. HIP Services follow the Host Identity Protocol standard, which initiates trust before transport communication is established and any data is exchanged between the HIP Service and other authorized HIP Service endpoints. Tempered Networks' Conductor orchestrates policies across HIP Service endpoints that are distributed throughout the IDN fabric where the Conductor maintains state but does not require persistence for HIP Services to function.

HIP Services enable functionality that is independent from and can separate business traffic flows from normal network forwarding logic. Networking and security teams can now innovate and move as fast as DevOps, but with a high degree of control, predictability, and verifiability in response to new business needs.

These IDN endpoints make IP mobility not only possible, but extremely simple and practical. Using the cryptographic identity, HIP services enable the mobility and migration of an IP resource anywhere within the fabric without requiring changes to the networking or security underlay. This decoupling overcomes many of the addressing, routing, mobility, and failover challenges associated with traditional IP networking and SDN technologies (see Use Cases below).
Tempered Networks HIP Services can effectively function as a router and/or bridge, eliminating or reducing the need to maintain VPNs, complex firewall rule sets, VLAN segmentation, routing convergence and DNS for failover, and ACLs in attempt to accomplish secure connectivity, access, availability, and segmentation.

To allow for a flexible deployment model that is elastic and can span nearly any type of resource, location, or environment, Tempered Networks provides HIP Service endpoints as physical, virtual, or cloud appliances; as software installed directly on a client or server, as an SDK and library for embedding in an application or as firmware for custom hardware. This capability of easily extending a secure networking overlay as broadly or deeply as an organization may choose across any environment cannot be matched by any other SDN, SD-WAN, traditional networking or security vendor.

Our objective is to enable rapid orchestration of HIP services everywhere in order to realize the bold vision of a secure, mobile, and private Internet that is as flexible as it is impenetrable. Figure 3 shows a foundational aspect of Tempered Networks' unique value proposition and our vision of providing simplified and secure Identity-Based Networking services that will cover the full OSI stack – from the Link Layer to the Application Layer.

We believe that eventually every connected thing should have the Host Identity Protocol embedded or running natively to create an encrypted and explicit trust-based perimeter of one. Because the foundational flaw in TCP/IP, the identifier – locator split problem, is now solved we can begin to control and overcome most of the severe networking and security limitations that have continued to place all Internet users, industries, governments, and countries at extreme risk. To our knowledge, only Tempered Networks has approached the problem from this perspective leveraging the brilliant research and development that came before us.

Tempered's IDN Endpoint Vision - unified secure networking coverage across the OSI stack

OSI Model	HIPswitch	HIPclient HIPmobile HIPserver	HIPapp	HIPchip
Physical - Layer 1				
Data Link - Layer 2				
Network - Layer 3				
Transport - layer 4				
Session - Layer 5				
Presentation - Layer 6				
Application - Layer 7				

Figure 3

HIPswitch

HIPswitches are typically deployed in front of devices or hosts that cannot protect themselves, like legacy systems and machines, or when customers are unable to install either a HIPclient, HIPserver, or embed a HIPapp. HIPswitches can be deployed as a physical, virtual, or cloud-based appliance.

Tempered Networks' physical appliances have built-in Ethernet, Wi-Fi, Cellular (2G, 3G, 4G LTE modems), as well as Serial-over IP for the most flexible link connectivity options found in the industry. The physical appliances can fail to wire, Wi-Fi, and/or cell and can be configured for high availability depending on customer need. The physical HIPswitches will often replace existing cellular modems, access points, VPNs, and internal firewalls for significant CapEx and OpEx savings while providing a level of networking flexibility, speed, and security previously beyond the reach of most organizations.

Our virtual and cloud appliances function in the same manner as our physical HIPswitches. For the first time, an organization can instantly connect, protect, segment, move, failover, and disconnect any private or public cloud-based workloads anywhere in the world with unprecedented speed and simplicity. Unlike SDN or traditional networking and security technologies, organizations no longer need to deploy and maintain different networking and security policies for their on-premises resources and another set for their cloud-based resources. The result is consistency and predictability while lowering costs and the overall attack surface.

Our approach makes it easy to deploy and extend a unified, trust-based, and encrypted networking fabric that for the first time enables micro, macro, and cross-region segmentation as well as global IP mobility. Deploying and maintaining intra-cloud (region-to-region), cloud-to-cloud, and cloud-to-datacenter cryptographic trust-based communications with non-traversal segmentation becomes a simple three-click operation that is verifiable and nearly hack-proof.

HIPclient

The HIPclient is a software client installed on Windows and Mac laptops and PCs and will soon be available on Linux PCs as well.

The HIPclient enables customers to give managed computers a trusted and verifiable identity, which opens up a broad array of end-user secure access, networking, mobility, and segmentation use cases. Trust-based client segmentation, granular access control, encryption everywhere, and auditing is now possible in both static and dynamic IP environments.

For the first time, user authentication can be easily integrated with device-based authentication, overcoming much of the complexity associated with attempts to extend directory services to include device-based trust. Unlike traditional VPN technologies, The HIPclient would allow an organization to explicitly allow or deny any client to not only securely connect to a network, but easily segment access by explicitly defining resources that a HIPclient or group of HIPclients can and cannot access. The HIPclient also overcomes the typical session constraints of legacy VPNs. The HIPclient is not restricted by the number of concurrent client to resource encrypted sessions. A HIPclient can theoretically have an unlimited number of simultaneous encrypted sessions, to discrete HIP Service endpoints.

With the HIPclient, revocation of trust is a one-click operation that even a non-technical employee can implement. Because of the HIPclient’s unique 2048-bit CID, that device is revoked access permanently regardless of the status of their user credentials or the distributed nature of corporate networks and resources.

Because of the Conductor’s ability to immediately orchestrate and update distributed policies to all IDN endpoints, the rest of the IDN fabric knows that device and its CID have been revoked. No IDN endpoint will respond to any request, anywhere, even if the revoked employee knew the hostnames, IP addresses, and user credentials to those resources. Granting and revoking guest Wi-Fi access instantly and in a manner that is easily verifiable is a oneclick operation as well. The same is true when an organization needs to grant temporary segmented access to a 3rd a party vendor or contractor where the segmentation is explicit and instantly revocable. With the HIPclient, the IDN becomes the first place to enable and revoke user access, even before performing revocation in a directory service. The reason is that once device-based trust and authentication have been revoked, even active user credentials will no longer work because the user cannot access any resource from an untrusted device.

HIPserver

The HIPserver supports Windows Server today and will soon be available for Linux and BSD-based servers. HIPserver behaves much like the HIPclient but is also built to allow an organization to choose whether they want to completely cloak the server itself so only authenticated and authorized endpoints can discover and communicate with it. Using the explicit IDN trust model, cloaking, software-defined segmentation, and encryption are driven down to the server level, effectively enforcing a perimeter of one. Simplified and consistent global IP mobility and migration become a reality across the IDN’s Host Identity Namespace for those applications and servers running the HIPserver as an IDN endpoint.

HIPapp

The HIPapp will be a complete software library that will enable HIP to be embedded into nearly any application or service, making it easy for developers to incorporate unified, secure networking directly into an application or service. Encrypted, authenticated, and authorized access based on that application's device, VM, or container's cryptographic identities bypasses traditional networking complexity and enables that application to have explicit trust orchestrated by the Conductor. Accelerating the time to provision and revoke discrete application connectivity, while allowing for simpler and faster migration and failover methods is the main objective of the HIPapp. Embedding that application's device, VM, or container's cryptographic identities bypasses traditional networking complexity and enables that application to have explicit trust orchestrated by the Conductor.

Accelerating the time to provision and revoke discrete application connectivity, while allowing for simpler and faster migration and failover methods is the main objective of the HIPapp. Embedding HIPapp as a HIP Service endpoint will also protect a user or organization if user credentials are stolen. Stolen user credentials will not work without the cryptographically trusted device. Mobile SMS "smishing" and other SMS attacks can now be prevented.

Any type of application—mobile, web-based, and even fat client applications—can now embed devicebased trust into the applications and clients themselves, providing the same degree of simplified networking flexibility, mobility, instant failover, encryption, and granular cross-boundary segmentation without the traditional overhead found with today's technologies.

HIPmobile

HIPmobile is a complete mobile phone client similar to the HIPclient for laptops and PCs. Working versions for iOS, Android, and Windows are in development and are being designed to support both phones and tablets. The same functionality described above for the HIPclient applies to HIPmobile devices as well.

HIPchip

The HIPchip is Tempered Networks' firmware designed specifically to run on custom hardware for almost any type of connected device. Point of Sale (PoS) systems, IP cameras, webcams, cable modems and routers, industrial control systems (ICS), POE switches, as well as IoT sensors can now function as an IDN endpoint and be easily managed as any other IP resource within the IDN fabric. The minimum hardware requirement to run the HIPchip firmware is a 500 MHz RISC or x86 processor and 64 MB of RAM. The application of the HIPchip is to give any Operational Technology (OT) or Information Technology (IT) system the ability to join and be orchestrated by the IDN's encrypted and authenticated fabric as easily as having a Mac client or a Windows server managed within the fabric. The deployment diversity of HIP Services is a key component of an IDN and the orchestration of policy across all endpoints makes it simple, fast, and easily verifiable. For the first time in the industry, a unified secure networking architecture spanning both Operations and Information Technologies (OT and IT convergence) is now possible which Gartner has cited as a critical competitive advantage for any organization.

FOUNDATIONAL CONCEPTS OF IDENTITY-DEFINED NETWORKING

Host Identity Protocol
(HIP RFC 5201, 7401, 7402, and VPLS 4665)

The concepts behind Tempered Networks' Identity-Defined Networking (IDN) fabric were first proposed by Robert Moskovitz in 1999 as an individual IETF submission when the Host Identity Protocol (HIP) was conceived as a solution to overcome the fundamental flaw in TCP/IP networking - which has made networking and security the complex Rubik it is today. HIP was not only developed by leading academics and Global 2000 companies but was put into production before formal ratification by the IETF in April 2015.

HIP has been used in production since 2006 for everything from secure field communications by the military to accelerating manufacturing operations at Boeing by securing and enabling network mobility of their tooling infrastructure. HIP is the foundation of an IDN. The cornerstone of HIP is the idea of separating a host's identity from its present topological location in the Internet," for the sole purpose of "enabling a secure and mobile Internet. One of the most important principles is that HIP is both backward and forward compatible with any IP-based network, application, or resource. HIP separates the end-point identifier and locator roles of IP addresses, introducing a more flexible networking and secure Host Identity Namespace.

Identify-Defined Networks (IDN)

HIP is an open standard. But to realize the vision of host identity enabled on every IP-based device, a new management paradigm was needed. It required scale, policy-based orchestration, and compatibility of HIP Services for any O/S, Hypervisor, Container, or hardware platform in order to realize the vision of HIP Services everywhere for creating "a secure and mobile Internet."

Tempered Networks is the only software vendor that has now accomplished this feat creating an IDN that is simple to orchestrate and manage allowing any organization to create their own secure, private, and mobile Internet—one that even non-IT personnel can manage. An IDN is comprised of one or more Identity-Defined Overlays (IDO) made up of Virtual Trust Segments (VTS) based on every HIP Service or IDN endpoint possessing its own unique 2048-bit Cryptographic ID (CID) following the HIP RFCs. The result is an elastic military-grade encrypted fabric that can span nearly any device, network, or environment.

Identify-Defined Overlay (IDO)

Unlike existing SDN technologies, the IDO is a true overlay requiring little to no modification of the underlying network or security infrastructure. The IDO is a simple policy-based configuration of devices or groups of devices that are explicitly trusted within the IDN as an overlay network based on whitelisting. This trust, based on unique CIDs, determines what systems or machines can initiate and establish communication before any data is exchanged. A device or group of devices can belong to multiple IDOs. An IDO can span multiple existing VLANs, subnets, and easily span networking boundaries – across datacenters, public clouds, campus networks, remote locations, and even unmanaged networks, allowing for a unified secure networking fabric that is elastic and can be connected or disconnected in seconds without disturbing the networking and security underlay infrastructure.

The main design principle behind this simple yet powerful concept is that organizations can now have a consistent and predictable trust-based enforcement model that spans any environment and is easily verified for compliance purposes. Unlike other segmentation technologies today that are domain specific with very different architectures and functions, the IDN enables a common, unified, and secure networking architecture which reduces complexity and creates consistency in the application of policy across all connected systems and devices regardless of their network, location, type, or connectivity medium. If it's an IP-based resource, it can join and be managed by and within the secure fabric.

The IDO allows for simple, explicit, and completely enforceable macro, micro, and cross-boundary segmentation. An IDO addresses the fundamental provisioning, management overhead, and errors associated with using complex firewall rules, VPN policies, policy-based routing, access control lists (ACLs), and VLANs to connect, secure, and segment traffic.

Virtual Trust Segments (VTS)

A virtual trust segment is defined by an explicit trust relationship between one IDN endpoint (HIPserver, HIPclient, HIPswitch, etc.) and another. A VTS is created when an IDN administrator explicitly allows one IP resource (network, device, application, or machine) to communicate with another one or a group of IP resources via an IDN endpoint. A VTS can span subnets, networks, locations, and can even act as a temporary secure, segmented, and encrypted bridge between business partners or vendors without having to change any of the underlying networking or security infrastructure. Micro, macro, and cross-boundary segmentation is not only possible now but it requires only a few clicks of a mouse to create a VTS between any IDN endpoints. In addition to eliminating a hacker's ability to do reconnaissance and fingerprinting of an IP resource, a hacker's ability to move laterally in a network, even if a device were to become compromised, is contained within a VTS, significantly reducing an organizations overall attack surface. Any resource behind a HIP Service can effectively be cloaked. There are no TCP nor UDP listeners enabled, unless otherwise allowed, and if the correct 2048-bit cryptographic identity is not presented on initiation for access to that resource, the HIP Service simply doesn't respond.

For example, an Application Server Trust Segment could be rapidly provisioned where only application servers are allowed to talk to a database cluster. For any other machine in the network, the database cluster would be cloaked and unreachable regardless of existing network rights or topologies. But the database cluster may also require administrator access, so another VTS could be created called the Database Administrator VTS where only designated administrative machines are allowed to communicate with the database cluster. Authorized database administrators' machines would be allowed to communicate with the databases, but these DBA's machines would not have direct access to communicate with the application servers. The application servers would be cloaked and unreachable by the DBAs.

This removes a significant part of the overall attack surface for the database cluster. If malware or a hacker were able to penetrate parts of the network that was not yet part of the IDN, any type of lateral movement to discover the database cluster would not be possible. The only way the database cluster could now be compromised would be directly through the application servers or the DBA's own devices, significantly reducing the available attack surface. If an application server or DBA's machine was found to be compromised, putting that machine in quarantine or revoking it immediately is a simple one-click operation or secure API call.

The IDN's new approach to provisioning, hardened and non-traversable segmentation, and instant revocation allows an organization to streamline and focus their security efforts much more effectively by eliminating much of the overall attack surface, saving significant time and money.

Host Identity Namespace (HIN)

The Host Identity Namespace is complementary to the current IP and DNS Namespaces. The HIN is what provides global IP mobility and migration, overcoming many of the fragile and costly challenges associated with basing networking and security policies on public and private IP addresses. Within the IDN fabric, the identity of an IP resource is now a unique CID, not the IP address itself. This secure abstraction allows tremendous flexibility in IP resource and networking mobility. For the first time, an IP resource can move within the fabric and still be found, authenticated and authorized whether it's movement is in a static or dynamic IP environment. Mobility and migration between campus, datacenter, remote offices, intra and inter-cloud mobility, segmentation, automatic encrypted communication, and explicit trust becomes not only possible, but simple and practical.

Identity-Based Routing (IDR)

Identity-Based Routing (IDR) is a policy-based approach to IDN that enables all IDN endpoints to know and maintain knowledge of where resources within and across networks are located and what IDN endpoint or HIP Service is in front of a single resource or many resources. This allows the fabric and IDN endpoints to establish the most direct route to that resource within the IDN. Every IDN endpoint has the equivalent of a policy-based IDR table that is instantly updated via the Conductor's policy-based orchestration engine any time an administrator or an automated secure API call makes a change. The IDR policies maintain state within the fabric via the Conductor, but do not require persistence, ensuring only authorized resources are in fact communicating only with others that have been explicitly allowed.

Software-Defined Segmentation (SDS)

Software-Defined Segmentation is the process for which Virtual Trust Segments get defined. SDS can be performed manually by an administrator or automated via our secure API. Any type of segmentation whether micro, macro, or cross-boundary segmentation can now be instantly provisioned or revoked with little effort. Within the IDN, segmentation and access controls move from complex and fragile underlay network configurations (firewalls, VPNs, routers, and switches), to the IDN's device-based trust model that is simple to orchestrate. SDS shifts control from the perimeter or traditional network to the device and its CID. What makes SDS so powerful is that it is based on the most common denominator that every organization has – the unique identity of a connected device. As mentioned above, this function protects against the lateral movement of threats, dramatically reducing an organizations overall attack surface.

USE CASES AND THE APPLICATION OF IDENTITY-DEFINED NETWORKING

Because of the breadth and depth of how and where the Tempered Networks' IDN endpoints can be deployed, the use cases that can be supported are broad.

An organization could add the HIPclient or HIPserver to their standard OS or embed the HIPapp as part of an application. They can deploy a cellular enabled modem HIPswitch to protect remote critical infrastructure that can't reliably connect or protect itself. Consider these additional real-world use cases of Tempered Network's IDN:

Instantly Provision or Revoke Vendor, 3rd Party, or Supply Chain Access

Some of the most common attack vectors today are 3rd party systems that are either permanently or temporarily connected to a corporate network. HVAC systems, building automation, web services to credit bureaus or supply chain vendors, vending machines, vendor technicians, PoS systems, and even guest Wi-Fi all increase an organization's attack vector.

Pinholes are opened in firewalls and then frequently forgotten. Configuring temporary VPN access is laborious, slow, and cannot be easily segmented down to a specific resource. Permanent connections for things like building automation are difficult to properly segment and maintain over time. Using VLANs or ACLs are not sustainable nor should they be considered proper or hardened segmentation that cannot be traversed by a bad actor. With an IDN, not only can temporary or permanent access be provisioned instantly, but can also be segmented by explicit trust that cannot be traversed, is immediately verifiable, and can be instantly revoked regardless of user credentials.

Instant Connectivity, Encryption, and Failover Across Managed and Unmanaged Networks

Failover can be for any connected "resource" for anything as broad as a datacenter or as specific as one service. For example, even a commercial airplane (the most mobile resource imaginable) can land anywhere in the world and an airline could still securely communicate with the plane on any network where the plane has access even if a plane were configured with only one destination IP address, as is the case with some models of Airbus aircraft. Plane connectivity, secure communication, and instant failover for uploading and downloading that airplane's manifest data between datacenters is now possible in as little as 1 millisecond. This overcomes the complexity of attempting to use slow and fragile routing convergence for failover within a global MPLS network and overcomes the problems typically associated with using DNS for failover. An airline can now easily maintain instant failover assuring timely landing and takeoff schedules.

On-Demand Secure Network Provisioning and PCI Compliance

Point of Sale (PoS) systems, kiosks, or pop-up stores can be provisioned on a network in seconds, cloaked, segmented, and moved out of scope for PCI compliance over any network. Shared and unmanaged networks become a non-issue because software-defined segmentation and containment prevents hackers from using those temporal or permanently connected systems on a corporate network as an attack vector. In addition, all communication is automatically AES 256 encrypted.

MPLS Replacement, Remote Office Security, and Instant Failover

Costly MPLS networks can be replaced with Tempered Networks' IDN and commercial broadband from service providers, saving connectivity costs for distributed remote sites while providing better security, faster provisioning, and much simpler management.

At each site, an inexpensive HIPswitch can be deployed, creating a cloaked, secure, and private corporate WAN. Adding a new link to the overall IDN fabric requires just a few clicks in the Conductor to establish cryptographically assigned trust between that IDN endpoint and others within the mesh. Devices behind the IDN endpoint can also be assigned trust within the mesh, providing unique cross-network trust and segmentation. Remote office exposure to Man in the Middle (MiTM) attacks is prevented because hackers are unable to find and fingerprint devices in order to execute attacks. And if a link fails, the HIPswitch will immediately failover between links, ensuring high availability.

Critical Infrastructure Protection, Rapid Provisioning, and Cost-Effective Remote Support

Secure networks for critical infrastructure can now be provisioned instantly with one-click by adding any type of distributed IP-enabled device or group of devices to an Identity-Defined Overlay (IDO).

Oil and gas pipelines, electrical substations, smart meter systems, and unprotected healthcare devices can now be automatically networked, cloaked, and secured. These devices can now be remotely secured and managed from anywhere in the world without the traditional cost and complexity of attempting to deploy and maintain separate routers, firewalls, and VPNs. Because IDN access is based on cryptographically signed, authenticated and authorized devices, the business risk resulting from the common practice of using shared administrator credentials is eliminated.

An industrial, business, or healthcare enterprise can significantly reduce the exposure, expense, and productivity loss of leaving these systems unprotected or having to send field technicians to remote locations for maintenance. The complexity and cost of additional networking and security infrastructure, that would still prove to be ineffective to hacks, is no longer necessary.

Secure and Segmented User, Vendor, and Application Access Control

- Unlike traditional VPN technologies, a client or server can now have many concurrent encrypted virtual trust segments (VTS) or tunnels to specific applications, services, or other IDN endpoints without requiring a gateway. Building automation vendors can deploy OT systems at customer locations and provide encrypted and verifiably segmented access to those systems for faster and less expensive maintenance without their customers fearing those systems as a potential attack vector. Those vendor responsible systems can be verifiably segmented and cannot communicate with any other system on the corporate network because they only have a trust relationship with the vendor's network. All other systems on the corporate network can be cloaked and will not respond to any communication with those systems unless it is explicitly allowed.

- Secure internal and remote access for employees anywhere in the world becomes much more practical and cost-effective than traditional VPN and firewall technologies, eliminating failover, key management, and networking problems associated with client gateway access and mobility. Clients and servers can now connect directly or through HIPswitches without the concern of opaque and complex legacy network constraints.

- Organizations can embed Tempered Networks' HIPapp into mobile or web applications providing customers a much higher degree of security and segmentation. Application access can now easily include device-based authentication and authorization. HIPapp is not a replacement for user credentials but adds another layer for hardened access control by including a device's unique CID as a policy foundation for secure networking. Even if a user's credentials were stolen for a HIPapp enabled application, a hacker would not be able to gain access unless they possessed the authorized device as well. Access policy could be easily tiered for user convenience. If the user had the correct user credentials, but was accessing from an unauthorized device, a policy could be created limiting their access to a subset of their account information only as an example. Only if the user has both the correct user credentials and the authorized device would they be allowed to access the whole application. It's the equivalent of having multi-factor authentication built-into the application and device itself.

Secure and Segmented Machine-to-Machine Communication

Secure machine-to-machine communication without requiring an IDN gateway is now possible, freeing networking and application services from the constraints of the network.

Servers running the HIPserver can bind a unique IDN IP address that is only known and available to other IDN devices. The unique IDN IP address frees the application server from the constraints of the hosted network, allowing it to freely move from network segment to network segment and even to a public cloud within the IDN fabric without losing its IDN IP address. Only whitelisted IDN devices will be able to locate the HIPserver's enabled service by its IDN CID and its unique IDN IP address. The benefits for mobility, as well as consistent monitoring across all connected things, become not only possible but simple.

CONCLUSION

Tempered Networks' Identity Defined Network (IDN) is the only scalable, multi-use solution that creates a common secure networking architecture able to span and adapt for any connected resource – anytime, anywhere.

The simplicity, cost-effectiveness, and secure design of the IDN architecture is expected to enable fast and scalable network and security operations, global IP mobility and instant failover, a dramatic reduction of cost by reducing if not eliminating security and networking complexity while significantly reducing an organization's overall attack surface. Achieving this while keeping it simple and easily orchestrated is what Tempered Networks has uniquely pioneered and why we believe the concept of an IDN is not just evolutionary, but revolutionary.

Unlike either physical and virtual networking or security alternatives, Tempered Networks' approach is unrestricted in its use – it works regardless of where, what, or for whom it is deployed. And unlike other approaches, Tempered Networks' deployment and implementation requires little to no modification of existing security, network, or application infrastructure. The IDN fabric establishes explicit device-based cryptographic trust, and can cloak resources from the start while automatically encrypting all communication within the fabric. The speed and ease in connecting, protecting, moving, and disconnecting any resource – anywhere – while providing instant failover is unprecedented.

All of these benefits could be accomplished using a variety of different technologies from different vendors but the additional cost and complexity is what has made fast and effective secure networking the elusive objective it is today. Tempered Networks' approach is not only a fraction of the cost of alternatives, but is the only simple approach focused on making the vision of a secure mobile Internet a reality. It's simply never been possible before – until now.

Additional Resources

https://tools.ietf.org/html/rfc7401

https://tools.ietf.org/html/rfc7402

http://www.cs.helsinki.fi/u/gurtov/papers/hip_survey.pdf

https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity_framework_bsi_2015-04-08.pdf

http://www.temperednetworks.com/wp-content/uploads/2015/09/Host-Identity-Protocol-Andrei-Gurtov.pdf