# The HIPrelay

## Breaking Barriers, Securing Borders

### SOLUTION OVERVIEW AND OUTCOMES

The HIPrelay, an identity-based router, secures porous networking borders and overcomes the barriers of network complexity to connect all systems, even non-routable IP resources, across any network instantly. Simply. Securely.

An integral component of the Identity-Defined Network (IDN) platform, HIPrelay routing is based on cryptographic identity, so any connected thing, whether it's client, server, virtual machine, cloud, or IoT communications can be securely routed to another without constraint. The HIPrelay routes encrypted traffic between any identity-enabled host to another across any public, private, cellular or cloud network, while maintaining isolation and proper containment of all IP resources.

A key component of the IDN platform, HIPrelay was designed as a seamless and non-disruptive overlay to existing network infrastructure that easily traverses traditional switching and routing infrastructure across both LAN and WAN environments. Unlike SDN and SD-WAN solutions, HIPrelay and IDN effortlessly integrates and can bridge L2 and L3 networks simultaneously. With HIPrelay and IDN orchestration,

instant network connectivity and revocation is now not only possible, but quick and easy to manage. Organizations can reduce errors and the need for complex networking and security point solutions, which support only a few environments, to fully eliminate network provisioning barriers and firmly secure porous borders.

IDN solutions that includes HIPrelay create unbreakable network segments that eliminate up to 90% of attack vectors, while reducing provisioning and mitigation time by 97%, and IT costs by as much as 25%. Network and security teams can now become more agile while significantly reducing business risk.

### ENABLING CRYPTOGRAPHIC MICRO-PERIMETERS

Within the IDN fabric, the security and networking perimeter is easily moved from the network edge to the host, creating secure micro-perimeters that have the flexibility to connect to any other host across any network without sacrificing security. Only authenticated and authorized hosts can communicate within an Identity-Defined Overlay (IDO), providing a level of isolation and containment previously unattainable. This not only hardens the interior, isolating and segmenting lateral movement to only authorized machines; it also simplifies and improves security by reducing an over-reliance on complicated and potentially porous inbound firewall rules.

### GLOBAL IP FLEXIBILITY AND ELASTICITY WITHOUT BORDERS

The HIPrelay supports a Host Identity Namespace (HIN) that overcomes IP address-based provisioning barriers, including VLANs, Network Address Translation (NAT), L3 ACLs and rules, because connectivity is

based on cryptographic identity, not addresses.  If a host's IP address changes, IDN policies don't need to change because the cryptographic identity is bound to the host, not to the IP address, whether static or dynamic. Because policy, routing, and enforcement is based on provable identity, not ephemeral IP, global IP flexibility and mobility becomes a simple, efficient reality.

Using HIPrelay's revolutionary routing technology, organizations can overcome previously impassable barriers beyond their control, such as service provider Carrier Grade NAT environments. Collectively, these barriers have made cost-effective and secure end-to-end mobile networking impossible to achieve – until now.

## 100% NETWORK, SYSTEM, AND ENVIRONMENT AGNOSTIC

Unlike SDN and SD-WAN solutions, HIPrelay bridges and seamlessly integrates Layer 2 and 3 networks without requiring modification to an existing network's switching and routing infrastructure. The HIPrelay does not use Layer 3 rule sets or traditional routing protocols for routing decisions. Instead, encrypted communications are routed within the overlay based on cryptographic identities and simply leverage existing infrastructure as any encrypted traffic would. This simpler, more secure, and flexible architecture reduces over-reliance on imprecise, porous, and difficult to maintain Layer 3 and 4 rule sets, while enabling connectivity across traditionally impassible borders.

## HORIZONTAL SCALE, AVAILABILITY, AND COMPLIANCE ACROSS ANY REGION - FLEXIBILITY ON YOUR TERMS

The HIPrelay puts customers in complete control of how they Internetwork systems, by controlling traffic isolation across regions to achieve optimal performance, security, and even compliance, without disrupting the underlying infrastructure. HIPrelay can be deployed in clusters and distributed across the Internet, whether on-premises or in the public cloud, facilitating an identity-based horizontal scaling, availability, and compliance architecture.

## VPC TO VPC, REGIONAL, AND MULTI-CLOUD PEERING MADE SIMPLE

For the first time, DevOps can eliminate cloud networking complexity, access control, and peering limitations within and between cloud providers, creating a unified architecture. With the HIPrelay and cloud-based HIP Services, the IDN functions as a secure broadcast domain, eliminating IPv6 and IPv4 conflicts, overcoming restrictions on the number of peering connections and relationships, and making cross-regional peering possible.

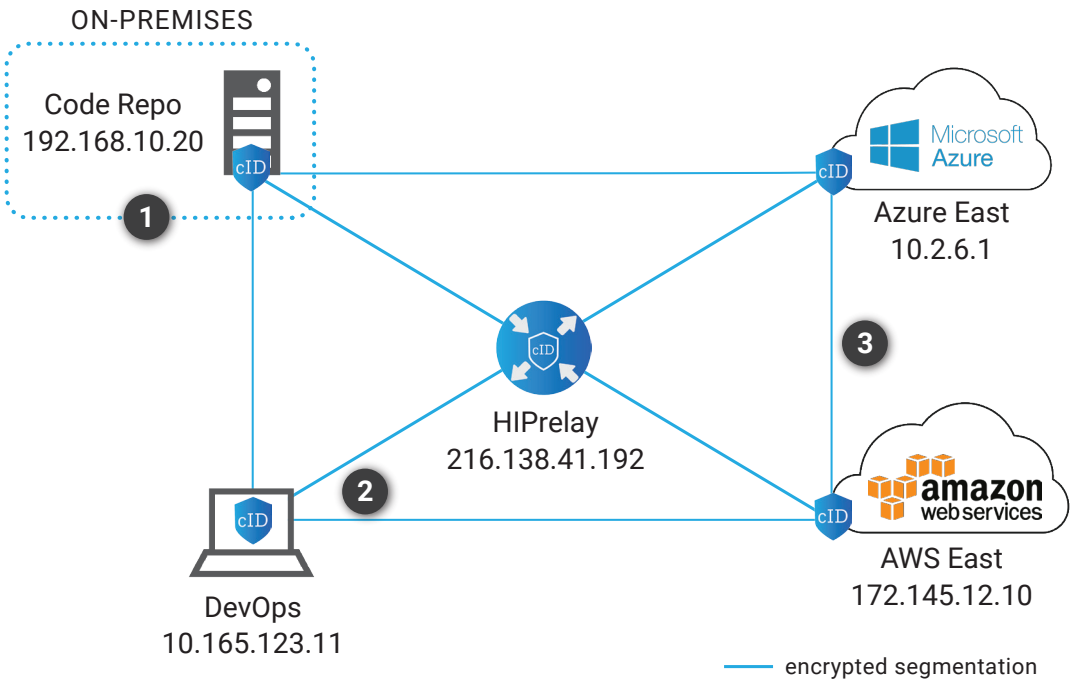
Instead of 150+ complex configuration steps just to peer between AWS' and Azure's network edge, a HIP-enabled peering architecture can be done in 5 simple steps. It even goes further by creating direct instance-to-instance peering to span both AWS and Azure without modification to functions like security groups.


© 2017 Tempered Networks. All rights reserved.

Secure code updates, micro-service connectivity, macro- and micro failover, as well as workload migration are now possible, extremely simple, and efficient. In addition, DevOps no longer has to use insecure SSH and shared keys or maintain disparate and complex VPNs for secure remote access that may or may not work depending upon DevOps' location. Instead, users can now have secured direct access to any VPC instance based on authenticated, authorized, and provable machine identities in conjunction with their user credentials from anywhere in the world.

HIPrelay and IDN – Self-secured networks without borders.

## Example HIPrelay DevOps Deployment




1. Code Repo is located deep inside HQ network and has explicit segmented and encrypted trust to directly connect to any instances in the cloud. Simple, secure, and auditable code targeted code updates are now possible regardless of IP schema.

2. DevOps has encrypted and auditable direct client-to-instance access from anywhere. Instant direct connectivity, revocation, and remediation is now possible.

3. Instances in Azure East and AWS West both use different IP namespaces. Instances with private IP addresses, whether static or dynamic, can still be peered.

HIPrelay – makes routing of non-routable private IP addresses wthin the Host Identity Namespace easy and fast.

HIPservices – whether deployed as a lightweight client, server, or cloud gateway binds provable crypto-identity to an IP address securely overcoming traditional barriers and borders.


© 2017 Tempered Networks. All rights reserved.