

Product Datasheet

# HIPrelay for Public & Private Cloud

Zero Trust Routing for IoT, Virtual, and Cloud Workloads

## IDN Overview

IDN eliminates the complexity, cost, and exposure of traditional IP networks. With IDN, our customers accelerate resource provisioning and eliminate the network attack surface by enabling peer-to-peer, zero trust overlay networks that are remarkably simple to deploy and maintain.

All devices in an IDN overlay transparently authenticate and authorize network connections before data transport, making the network invisible and inaccessible by any unauthorized devices. Segmentation is made simple, and administrators can easily connect, encrypt, failover, and disconnect device communications across any network without disrupting or changing existing infrastructure.

 **50% Lower CapEx and OpEx**

 **97% Faster Resource Provisioning Time**

 **90% Reduced Attack Surface**

## HIPrelay Overview

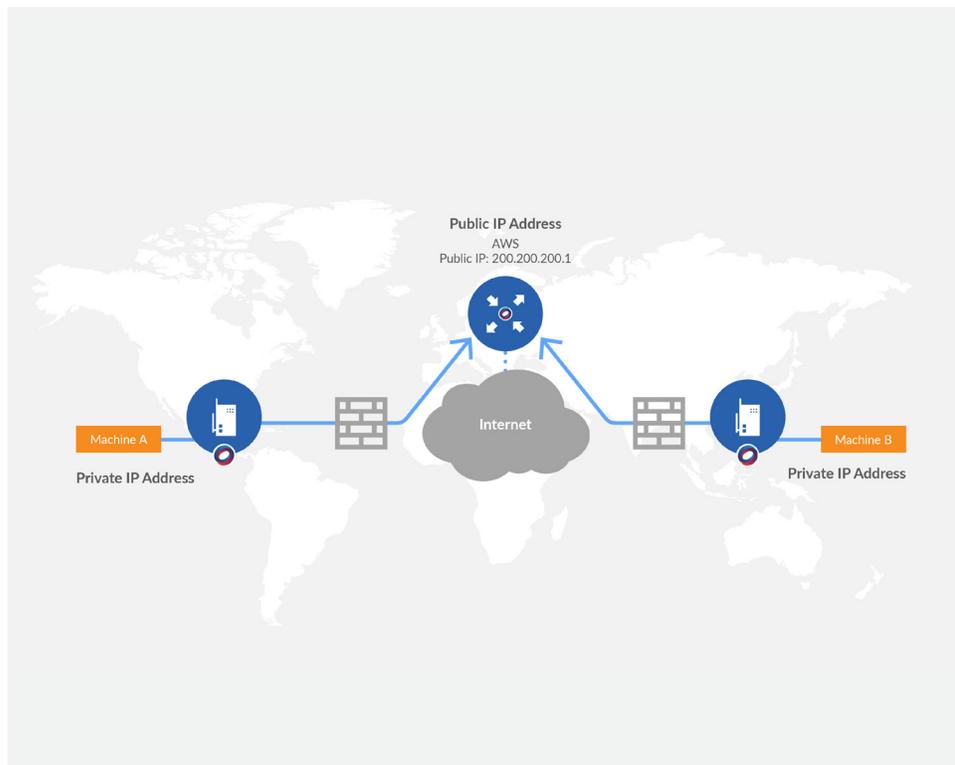
The HIPrelay is the world's first identity based router that delivers isolated wide-area overlay networks with distributed high availability, horizontal scaling, and direct peer-to-peer networking. Our customers can now connect privately-addressed and previously non-routable endpoints on separate Layer 2 and Layer 3 networks, with little to no changes to existing networking infrastructure. IDN routing and access control is determined by verifiable identities, not ephemeral IP addresses. Because of this, IDN overcomes traditional networking barriers like NAT, CGNAT, IP conflicts, or having to provision private APNs to use cellular networks.

The HIPrelay can make the WAN look and behave like one local broadcast domain, eliminating the need for complex networking and security solutions like SDN, FW/VPNs, remote access servers, jump boxes, and routing updates to securely connect distributed devices. It brokers only authenticated and authorized session, without decrypting the sessions. With IDN, secure peer-to-peer connectivity and segmentation across both LAN and WAN environments is not only possible, but simple.

FEATURES	BENEFITS
Zero Trust Policy Orchestration	Create, deploy, and disconnect overlay networks in seconds based on verifiable trust. The simple UI requires no advanced training and eliminates the complexity, conflicts, and dependencies caused by traditional IP network and security products.
Trusted and Universal WAN Connectivity	All HIP Service enforcement points and their protected devices can remain privately addressed and only need outbound access to the Internet to reach publicly addressed HIPrelays. Encrypted (AES-256) peer-to-peer WAN connections keep communications private across any networks.
HIPrelay Rules	HIPrelay rules are point-and-click simple. In the Conductor, simply select an endpoint or group of endpoints to connect, and then specify the HIPrelays you want those endpoints to use for instant WAN networking.
High Availability and Horizontal Scaling	Groups of HIPrelays can be distributed geographically. Distributed HIP Services will use the fastest response to determine which HIPrelay to use for that session, ensuring high-availability and scale.
Secure Mobile Workloads	Remove the limitations of IP-based networking and overcome common connectivity barriers like NAT and CGNAT. Within an IDN, all workloads behave as one private and micro-segmented broadcast domain, allowing you to easily move and replicate workloads across on-premises and clouds.
LAN and WAN Micro-Segmentation	Secures north-south and east-west traffic in any environment - physical, virtual, and cloud - across Wi-Fi, cellular, and Ethernet networks. Provides authenticated and verifiable device-level access control that can't be spoofed or violated.
Simple Compliance	It's now simple to define an in-country cluster of HIPrelays where devices will always use their country-specific HIPrelay, even when they're out of the country. This ensures all encrypted data communications remain within that country's IDN fabric for compliance purposes.

## Deployment

- HIPrelay delivers simple connectivity between IDN enforcement points with unified overlay architecture that's network, platform, and transport agnostic.
- Our customers increase security, reduce complexity and break through NAT, CGNAT, and APN connectivity barriers.
- Simplifies your network. Organizations use IDN for secure peer-to-peer connectivity and segmentation that traverses existing switching and routing infrastructure across all LAN WAN, and Internet environments.
- Can be deployed in distributed clusters, providing superior availability, network performance, and an effective data governance architecture.



“The HIPrelay is a miracle in simplicity for secure WAN connectivity. My DevOps team can instantly create private peering between on-premises workloads and our multi-cloud environment, with no changes to our existing infrastructure. With Tempered, I can do the work it would take 10 – 15 people to accomplish.”

Director DevOps  
Energy Services Company

ENVIRONMENT	PLATFORM OPTIONS	MINIMUM REQUIREMENTS
CLOUD	Amazon Web Services	T2.Medium
	Microsoft Azure	Standard_A2_v2
	Google Cloud	n1-highcpu-2
VIRTUAL	VMware ESXi	5.0 and above
	Microsoft Hyper-V	2012 R2
HARDWARE	1U Platform	Conductor 500

## Value Licensing

- Uniform software pricing regardless of platform or environment creates predictability
- No-charge software portability delivers agility to adapt to changing requirements
- HIPswitch throughput ‘bursting’ without penalty eliminates surprise costs
- High Availability: No charge for HA software subscriptions

## Summary

IDN enables borderless, zero trust overlay networks with point-and-click simplicity. It's now simple to create segmented and private networks spanning on-premises, remote, and cloud environments, with granular access control for each connected resource. With IDN's unique overlay technology, our customers can start small and quickly scale and automate their segmentation architecture, without having to change their existing networking infrastructure. The results? Provision, segment, and revoke endpoints 97% faster than alternatives, while reducing the attack surface by up to 90%. With simple segmentation, built-in peer-to-peer encryption, cloaking, and universal connectivity and mobility, IDN delivers a more resilient, flexible, and extremely secure architecture.



Contact us at [sales@temperednetworks.com](mailto:sales@temperednetworks.com) to learn more.