TEMPERED NETWORKS®

Secure Networking Made Simple.

Product Datasheet

HIPrelay: Identity-Based Router

Instantly create a highly resilient, cloaked, and encrypted WAN across any public or private network.

Provision Your Own Private WAN in Seconds

Instant Peer-to-Peer Encrypted WAN Connectivity Without Constraints

It's now possible for network and DevOps teams to create a wide-area overlay network that directly connects any privately-addressed endpoints on separate networks with others—No modifying the underlay network. No having to re-IP the endpoints. Our customers can add new resources on their WAN 97% faster with greater predictability than any other alternative. Device revocation is instant, no endpoint needs to be exposed to the public Internet, and routing access is determined by verifiable machine identities, not IP addresses.

Unlike SDN and SD-WAN solutions, the HIPrelay easily integrates with and can bridge L2 and L3 networks simultaneously. And it easily traverses traditional switching and routing infrastructure across both LAN and WAN environments. Instant network connectivity and revocation is not only possible, but quick and easy to manage. Organizations can reduce errors and the need for complex networking and security point solutions, eliminating network provisioning barriers, and porous or spoofable ACL borders. Our customers have seen a 70% increase in productivity and a 90% reduction in attack vectors.

On-Demand WAN Micro-Segmentation

Using the HIPrelay, the security and networking perimeter is moved from the network edge to the host, creating secure micro-perimeters that have the ability to connect to any other host across any network without sacrificing security. HIPrelay routing and forwarding is based on verifiable cryptographic machine identities, so any connected thing, whether it's client, server, virtual machine, cloud, or IoT communications can be securely routed to another—overcoming NAT, CGNAT, and APN routing barriers. The HIPrelay routes and forwards encrypted traffic between any HIP-enabled clients, servers, or gateways to others across any public, private, cellular, or cloud network. 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 traffic flows to only authorized machines, it also simplifies security by reducing an over-reliance on complicated and potentially error-prone inbound firewall rules.

Features and Benefits

- Deploy and activate secure peer-to-peer networking in as little as 15 minutes with no changes to underlay network
- Securely connect resources within an identity micro segment to others regardless of location or network,using the Conductor's simple policy orchestration
- Reduce reliance on IP addresses to route and punch through impassable barriers like multi-NAT and Carrier Grade NAT
- Overcome previously costly and impassable network barriers and borders across the LAN and WAN
- Move the security and networking perimeter from the network edge to the hosts or machines themselves with the HIPrelay, along with HIP Services
- Instantly connect and revoke resources quickly and predictably, with the ability to directly connect non-routable IP's
- Get unbreakable WAN micro-segmentation that prevents and eliminates command and control exploits with end-to-end encryption (AES 256) and cloaking

 |