TEMPERED NETWORKS®

HIPswitch for Public & Private Cloud

Zero Trust Identity Defined Networking (IDN) for 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**

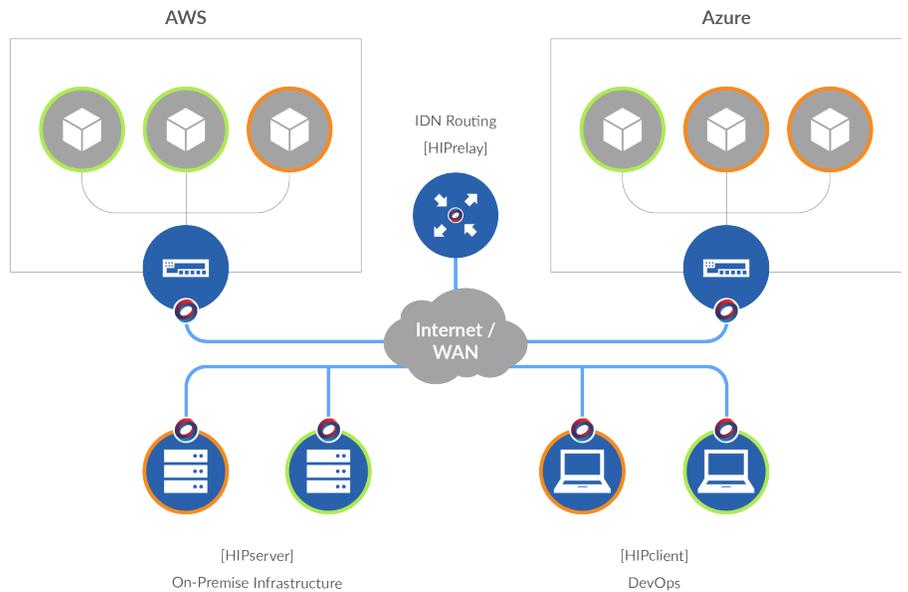## HIPswitch Virtual and Cloud Overview

The HIPswitch for Virtual and Cloud is a software-based enforcement point that serves as an IDN gateway for connecting and protecting workloads and containers. Our customers can now rapidly join all workloads, containers, and micro-services to a private and segmented overlay network in minutes, and unlike traditional alternatives, IDN requires little to no changes to existing infrastructure. As an IDN enforcement point, all workloads behind a HIPswitch are cloaked and can't be discovered or reached by unauthorized endpoints, eliminating the network attack surface.

Because the HIPswitch serves as the network boundary and security perimeter for its protected workloads and containers, the complexity associated with traditional network and security methods is eliminated. Now peering and micro-segmenting private instances between AWS VPCs, Azure VNETs, Google Cloud, VMware, and on premises-environments is point-and-click simple. Using IDN, our customers easily orchestrate secure DevOps access, workload migration, data backup, and micro-services integration with a level of security and predictability that was previously impractical. The result is universal connectivity and segmentation across all networks that is simple, fast, and extremely cost-effective.

FEATURES	BENEFITS
Zero Trust Policy Enforcement	The HIPswitch enforces whitelisted network and security policy for trusted and protected devices in the IDN overlay, making it simple to connect and protect any IP-enabled device. Revocation of device access is instant.
Plug and Play Deployment	Deploy overlay networks in under 15 minutes and accelerate release cycles with greater predictability, segmentation, and security. Add, disable, move, or revoke cloud workloads and containers in one click.
Software Defined Perimeter	As a software defined gateway for protected devices, the HIPswitch becomes both the network boundary and security perimeter eliminating the complex, error-prone, and ineffective network and security controls of traditional IT solutions.
Cloaking	Cloaked endpoints and networks have no visible TCP/IP footprint and are invisible to the underlying network and any untrusted devices or systems, meaning attackers cannot discover or hack protected endpoints.
Universal Connectivity and Peer-to-Peer Encryption	IDN delivers private wide-area overlay networks that makes it simple to connect privately-addressed devices on separate Layer 2 and Layer 3 networks. AES-256 encryption for all sessions is on by default.
Network Resiliency and Availability	Traffic flows between distributed HIP Services can easily be moved instantly without disrupting application sessions to enable fast and predictable failover, disaster recovery, and quarantine.
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.
Autonomous Operation	Ensuring the highest level of security, the HIPswitch is managed only by Conductor with no local administration. It does not need to persist to Conductor allowing for autonomous and continuous operation.

Deployment

- Enable simple orchestration of connectivity and segmentation to all IDN enforcement points within a unified overlay architecture that's network, platform, and transport agnostic.

- Simplify 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 Cloud environments.

- Central policy orchestration is non-persistent, so all enforcement points can run autonomously for superior network resiliency and availability

- Simple and cost-effective to acquire, deploy, and maintain to save time, money, and personnel resources.

AWS

Azure

IDN Routing
[HIPrelay]

Internet /
WAN

[HIPserver]
On-Premise Infrastructure

[HIPclient]
DevOps

"With HIPswitch for AWS I create instantly secured WAN micro-segments that span on premises, VPCs across regions, and my DevOps team. I now have a well-encapsulated and private network overlay that's simple, resilient, and secure. It's my cloud control plane."

**Director of DevOps,
Energy Services Company**

PRODUCT	SUPPORTED PLATFORMS	RECOMMENDED REQUIREMENTS
CLOUD	Amazon Web Services (AWS)	T2.Medium
	Microsoft Azure	Standard_A2_v2
	Google Cloud Platform (GCP)	n1-highcpu-2
VIRTUAL	VMware ESXi	5.0 and above
	Microsoft Hyper-V	2012 R2

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 to learn more.