



Product Datasheet

The Conductor

Zero Trust Policy Orchestration for Identity Defined Networks (IDN)

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**

Conductor Overview

The Conductor manages zero trust policy orchestration for all distributed HIP Services, which serve as the enforcement points for Conductor-created network and security policies. With instant policy distribution, our customers enable fast network provisioning, micro-segmentation, and secure overlay connectivity based on cryptographic device identities, not spoofable addresses.

The simple point-and-click user interface (UI) enables our customers to easily scale IDN deployments to thousands of devices, without requiring advanced technical training or adding new headcount. They can now add, move, and revoke endpoints 97% faster than traditional IT solutions. In addition, non-persistent policy orchestration allows all HIP Services to run autonomously with last known policy, until a change is made.

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

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.
Trust Based Whitelisting	Whitelisted HIP Services and their protected devices mutually authenticate and authorize based on their unique cryptographic identities before data transport, after which encrypted (AES-256) peer-to-peer connections are created.
Smart Device Groups	Automate overlay network device membership for fast provisioning and policy enforcement. Overlay group membership can be based on combinations of device attributes like CIDR, HIP Service location, MAC prefix, and other metadata.
Network Automation with HIP Invite	Provide email addresses and create a workgroup in under five minutes. As users download and add their devices, they're automatically added to the dedicated network segment, simplifying the time-consuming process of getting people access to resources on the network.
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	Simple segmentation down to the device or workload level secures north-south and east-west traffic in any environment - physical, virtual, and cloud - across Wi-Fi, cellular, radio, and Ethernet networks, without complex network changes.
Zero Trust Routing	WAN connectivity made simple. Identity-based routing technology that doesn't rely on traditional layer 3 rule sets or routing protocols to securely connect privately-addressed and previously unroutable endpoints across separate networks.
Monitoring and API Integration	Get visibility into performance data like connection rates, device availability, and cell network quality. Automate workflows and resource provisioning/revocation by integrating IDN with security and networking services like SIEMs or other monitoring tools.

Deployment

- Unlike the many complex, fragile, and time-consuming steps associated with traditional IT solutions, our customers eliminate human error through simple point-and-click policy orchestration.
- 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 Internet environments.
- Central policy orchestration is non-persistent so that all enforcement points can run autonomously for superior network resiliency and availability
- High Availability (HA) and backup services for the Conductor are included at no additional cost.



“Tempered Networks gave us a simple way to achieve end-to-end private networking for our Building Automation network that’s resilient, scalable, and secure. In less than 20 minutes, we were able to deploy our first cloaked overlay network without having to modify systems or involve IT”

Tom Walker
Facility Automation Services,
Penn State University

Trust	Device name	Overlay IP	MAC address	HIPService
	Infusion Pump Group	12		
	Master Server_Infusion Pumps	192.168.45.11	67:92:3e:ce:32:17	HIPswitch 3
	Nurse Group	9		
	VDI Server	10.0.2.17	52:c4:bb:c0:00:00	VDI Server

Trusted end-to-end connectivity with point-and-click simplicity to add, disable, and revoke devices

The Visual Trust Map verifies creation and revocation of connectivity and segmentation between endpoints.

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.