Tempered

Primer on Host Identity Protocol

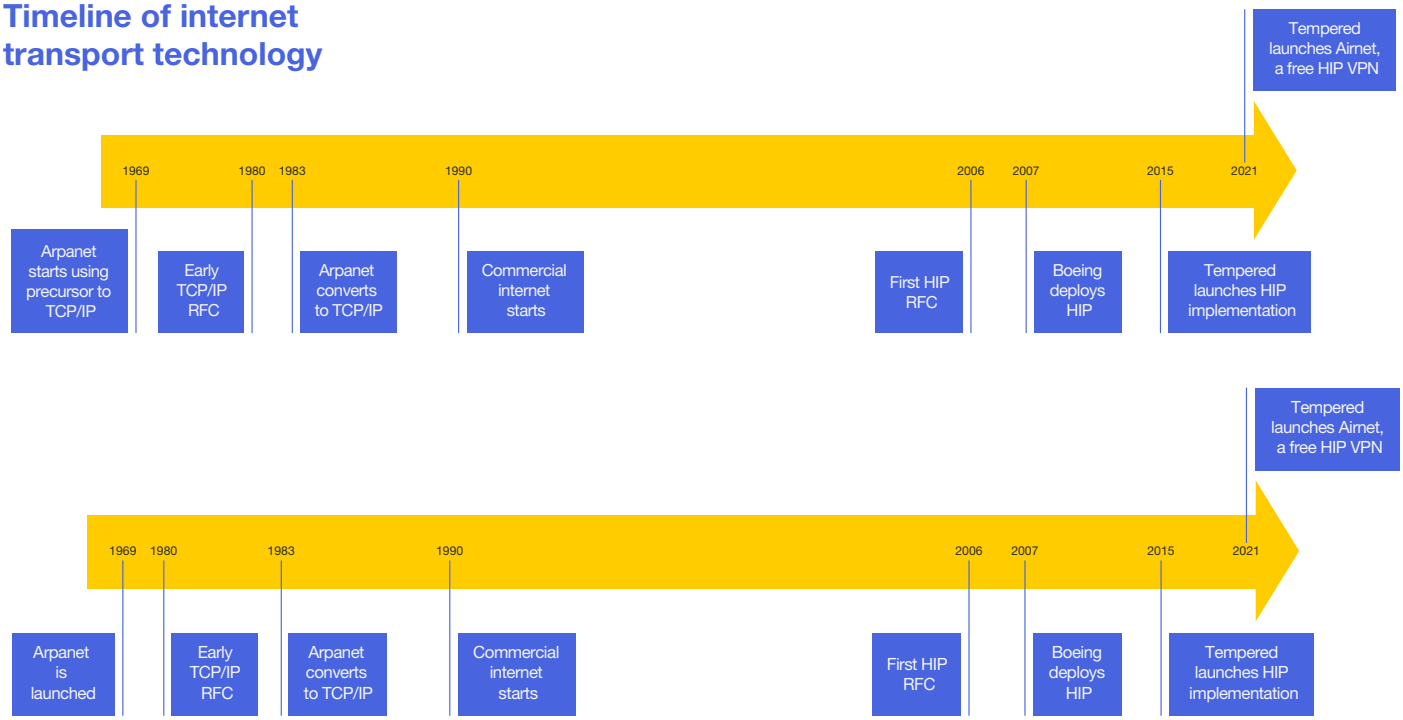
A simpler, more secure approach to IP communications

Creating a new standard for network security

Host Identity Protocol (HIP) is an open standards-based network security protocol, approved by the leading Internet standards organization, the Internet Engineering Task Force, in 2015. That event crowned over 15 years of HIP development, testing and deployment in coordination with several large companies (such as Boeing, Ericsson, Nokia, Verizon, TeliaSonera) and standard bodies (Trusted Computing Group, IEEE 802).

Recognized by the Internet Engineering Task Force (IETF) community as a fundamental improvement in secure IP architecture, HIP was first deployed within the defense and aerospace industry as a cost-efficient and scalable solution to address growing threat environments and the complexity of security policy management. The protocol has been in use for over 10 years in mission-critical environments of all scale and complexity, including applications where downtime costs exceeds $1 million per hour, and nation-state cyber-attacks occur on a regular basis.

Timeline of internet transport technology



Tempered Networks now offers the leading, field-proven HIP implementation. Tempered's real-world solution layers on simplified management, various end-point protection features and scalability. It is in use in a variety of use cases and network environments worldwide, and includes gateway technology allowing HIP networks to protect the traffic of any device, even if it can't or doesn't run HIP natively.

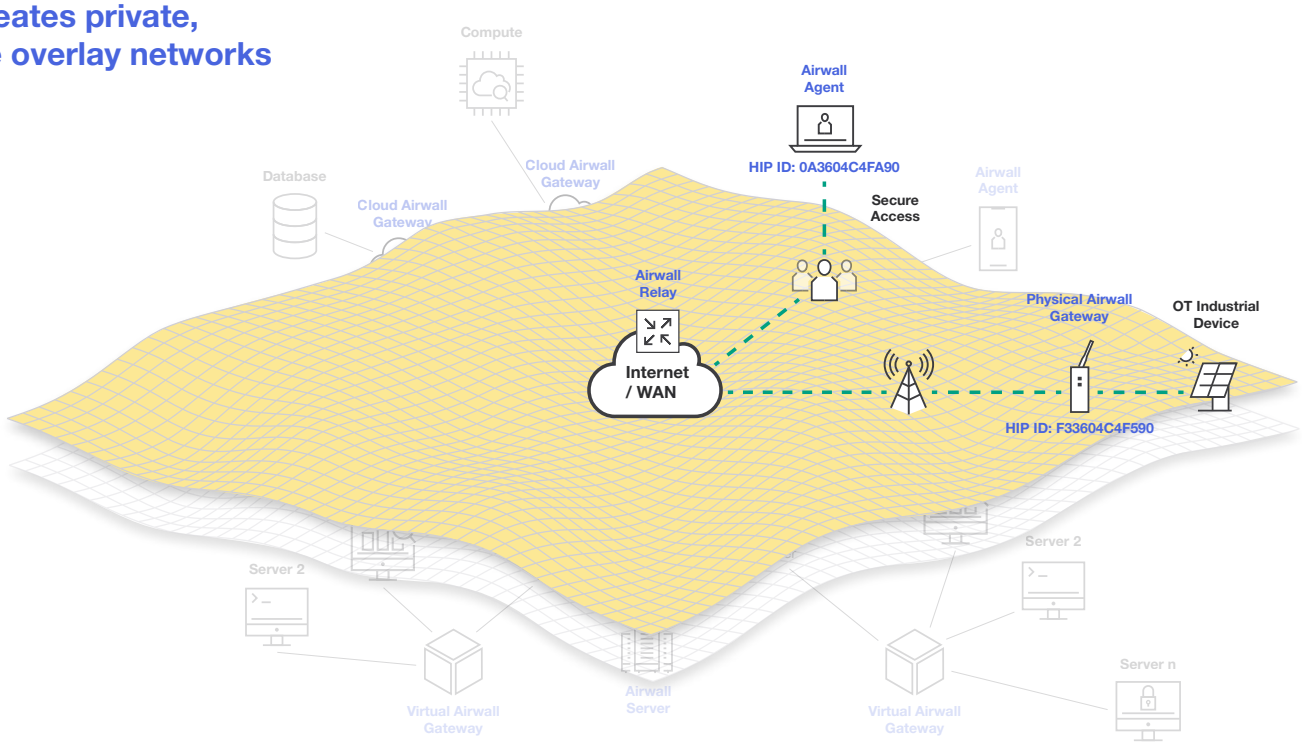
This paper gives a brief technical overview of some of the advantages of running HIP, and how these advantages create a fundamentally safer internet. These advantages include:

- Separation of the location (IP address) and identity of the devices. This makes security policy much easier in a mobile world where addresses are entirely ephemeral
- Completely eliminates the need for "VPN" solutions – devices can have the exact same network access policies regardless of where they are or how they are accessing the internet
- "Cloaking" of devices, which makes attacks from outside impossible
- All links between HIP systems are always encrypted at the network level, without need for the application to worry about data-ion-motion security
- DDoS attacks against HIP are nearly impossible because of its unique connection establishment protocols
- The cryptographically unique device identity makes man-in-the-middle attacks impossible

Secure by design

HIP creates a secure overlay fabric over existing network infrastructures. These private networks can typically traverse nearly any firewall and move between private, public, and mobile networks. The only requirement is that two ports – TCP 8096 and UDP 10500 – be open *outbound*. No inbound ports are required. This network is fully private, encrypted, and cannot be seen from the outside.

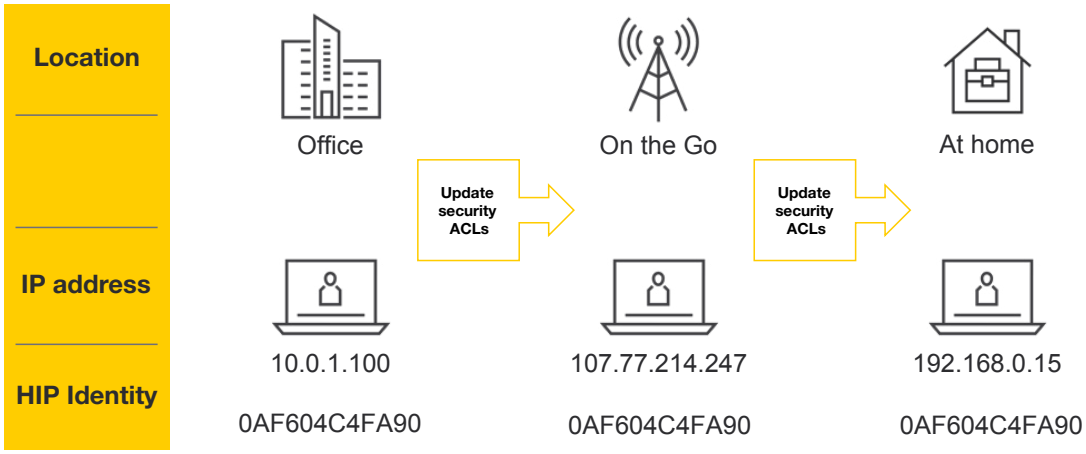
HIP creates private, secure overlay networks



HIP also introduces a new cryptographic host identifier separate from the usual IP address. The fact that IP addresses include both routing/location information and host IDs has complicated security policy management for decades. This new HIP ID allows for simplified, centralized management of end-point access control policies – without the need to change all the access control lists each time a device moves from one location to another.

The creation of a secure overlay network and the encrypted identifier renders hosts completely invisible to unauthorized users and potential attacks. HIP hosts are identified using strong cryptographic identities in the form of 2048-bit RSA public keys. Rather than probing an IP device for vulnerabilities, attackers will never know of the existence of the host on the network. To them, the device is completely cloaked.

IP Address is a poor policy tool

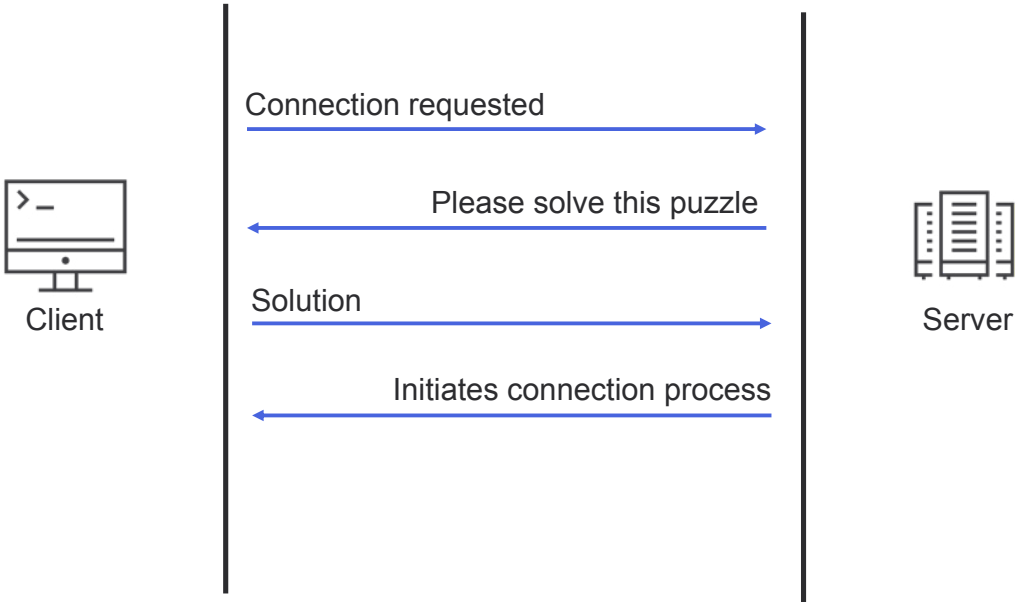


HIP provides end-to-end encryption for every network flow, including a key exchange protocol for creating secure encrypted tunnels. This enables transparent and legacy-compatible security for *all* TCP/IP applications without modification. Since HIP also introduces the concept of an identifier-locator split (separating the role of IP addresses as host identity and topological location in the Internet), with the unique cryptographic identity provided by HIP, the device can change locations and not require a new tunnel be built or require a policy update. Hosts can change their physical location, but retain their strong cryptographic identity. HIP remains compatible with IPv4 and IPv6 applications, utilizing a customized IPsec tunnel mode for confidentiality, authentication, and integrity of the network applications.

Since hosts and network devices can use the cryptographic ID for identification rather than dynamic IP addresses, features and use cases such as host and network mobility, single sign-on, and multihoming are easily implemented.

Furthermore, in contrast to TCP, HIP was designed from the start to be robust against the Denial-of-Service (DoS) and Man-in-the-Middle (MiTM) attacks plaguing the internet by deploying a clever cryptographic puzzle mechanism based on the Diffie-Hellman key exchange. The server keeps no state until the client completes a computationally expensive “puzzle”. Only after the client returns the answer to the puzzle (which the server already knew the answer to and doesn’t need to compute in real-time) does the server establish state and begin to negotiate a key exchange with the client. This puzzle essentially makes DDoS attacks too expensive for the attacker to implement.

Puzzle challenge makes DDoS Expensive



A radically different approach

The internet today remains a playground for hackers and state-backed groups engaging in cyber warfare. Instead of being an asset to the security community, today's networking standards are a big part of the problem. The complete lack of accountability and trust created by the ease of spoofing IP and MAC addresses, as well as the never-ending vulnerabilities that enable access to network perimeters create ripe targets. And our increasingly mobile and remote workforces have significantly increased the available threat surface.

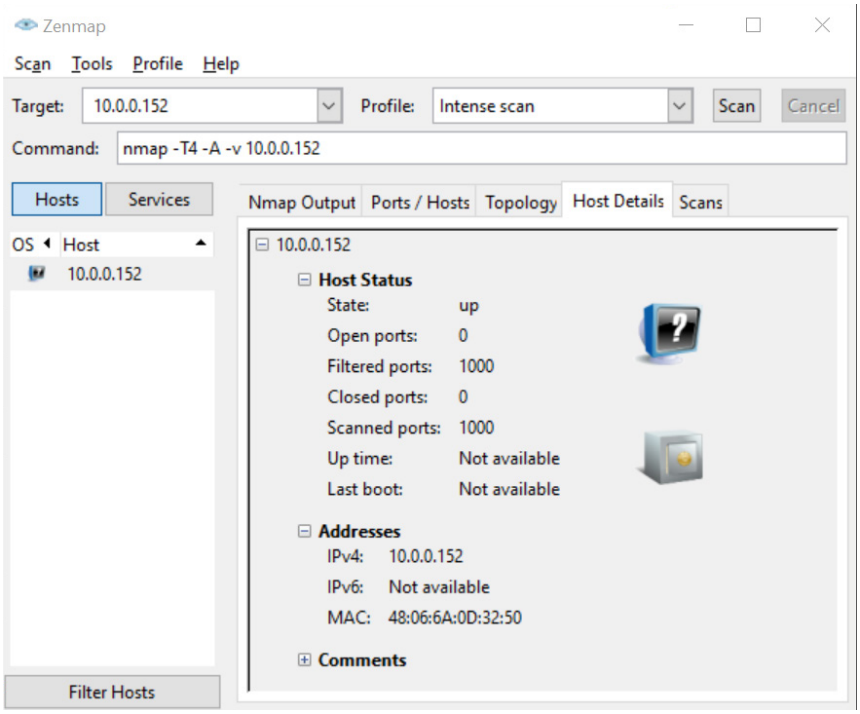
Today, most enterprises attempt to stop this using traditional tools such as firewalls and intrusion detection systems (IDS) – relying on traffic analysis and easily spoofed identifiers such as TCP ports, IP or MAC addresses – making for a fragile foundation that is tedious and costly to manage.

Tempered takes a radically different approach, addressing one of the root causes of internet attacks – the lack of robust host identities and open availability of exploitable systems. The cryptographic host identity becomes the primary operational unit in host access control and network traffic filtering. Recognizing the difficulty of patching legacy Internet devices, such as printers or industrial equipment, Tempered introduces gatekeepers known as Airwall Gateways in front of any IP-connected device, which require no changes to the underlying network.

In contrast to traditional firewalls with static traffic filtering rules, or IPsec gateways that encapsulate all traffic through tunnels, Airwall Gateways use a stronger approach. They establish secure tunnels over public internet to deliver vulnerable user data privately and securely. Airwall Gateways employ a positive security model that white-lists which hosts (cryptographic identities) are allowed to establish encrypted tunnels, thereby protecting against unauthenticated malicious traffic.

By partitioning and isolating the network into trusted micro-segments, Tempered completely cloaks vulnerable infrastructure from outside users, without the difficulty of having to individually update each connected device. Devices that are cloaked are undetectable from the underlying network. Combined with a powerful and scalable management interface, this provides an amazingly easy and highly efficient protection of internet communication.

Though multiple companies have attempted to benefit from using HIP, none have been as successful in productizing the various components into an extremely reliable and easy to deploy and manage solution as Tempered Networks. Two key Tempered innovations have made HIP operational and scalable for industry. Policy Orchestration and Traffic Relaying. HIP only specificies host-to-host communications. Tempered has created a uniquely effective policy creation and orchestration engine that works with HIP clients, and is intuitively represented in the Conductor user interface. Tempered's Relay provides the routing and transport needed for HIP traffic to find its destination on a non-local network, i.e. to cross complex network segments, VLANs, firewall and NAT boundaries.



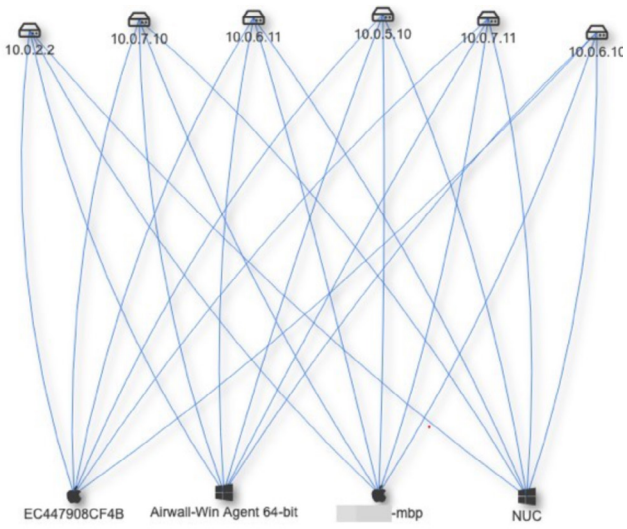
1. Zenmap scan of a Tempered Gateway

Compared to VPN solutions relying on layer-4 security, such as SSL, the use of HIP enables network security deep in the network protocol stack, alleviating known application-level attacks. As such, SSL operates on top of the TCP transport protocol, which itself is highly insecure and vulnerable to attacks such as SYN flooding or reset attacks. A malicious user can interrupt a secure session employing TCP-level weaknesses. Furthermore, relying on public authorities for approving SSL level certificates was shown to be unreliable with compromised root CAs. Exploits in the SSL/TLS protocol enabled attackers to not only compromise the confidentiality and integrity of communication, but also leverage DDoS attacks.

How Tempered productizes HIP

Even though HIP provides the highest level of network security, it initially introduced some deployment overhead. One of the key challenges had been the difficulty of configuring the rules in the HIP controller or policy management devices, which involved manual editing of XML files and the synchronization among multiple devices. Without an investment in usability, the HIP protocol was just another tool for experts and narrow, academic use cases.

Tempered's HIP investment has created an easy-to-use centralized graphical management console, which enables adding or removing user devices from a trusted list with a few clicks. Modern policy objects have been added, enabling real-world management of groups of users and network assets. There is a full API, allowing teams to fully automate all aspects of network configuration and user provisioning. And, of course, a fully auditable configuration history. Tempered's HIP implementation is, essentially, a realization of the promise of a fully software defined network.



2. Visualizing trust in Tempered's HIP Conductor

The Tempered solution has been successfully deployed in mission-critical industrial domains such as aircraft manufacturing, utilities sector, oil and gas, and electricity generation, as well as enterprise domains such as isolating ticketing machines running out-of-support systems and networking corporate laptops. The unique distinction of the Tempered platform is that it enables network engineers to securely connect anything that they would connect over the inherently insecure TCP/IP protocol. New use cases are realized everyday.

HIP raises the bar on network security with protection against most of today's known threats. In fact, one of the Boeing architects and security experts in the OpenGroup, Richard Paine, wrote a book about HIP deployments: *"Beyond HIP: The End to Hacking as We Know It."* Providing strong cryptographic host identities enables HIPswitches to robustly filter out all unauthorized traffic, eliminating the danger of DoS or impersonation attacks. Combined with military-grade AES-256 encryption and SHA-256 authentication of data packets, the bridged HIP traffic presents an insurmountable obstacle even for the most capable attacker on the internet.

While security of physical systems and devices is a primary driver of Tempered's HIP technology, Tempered's HIP implementation also solves many of today's enterprise secure networking challenges. Tempered is working with enterprises to unlock new ways of doing business in today's challenging times, including remote access solutions like alternatives to traditional VPNs, internal security challenges such as network segmentation, and API-driven approaches to secure cloud management.

Dr. Andrei Gurtov, Aalto University, Finland

Andrei Gurtov received his M.Sc (2000) and Ph.D. (2004) degrees in Computer Science from the University of Helsinki, Finland. He is presently a Principal Scientist at the Helsinki Institute for Information Technology HIIT, and a senior member of IEEE and ACM.

He is also adjunct professor at Aalto University, University of Helsinki and University of Oulu, and was a Professor at University of Oulu in the area of Wireless Internet in 2010-12. Previously, he worked at TeliaSonera, Ericsson NomadicLab, and University of Helsinki, and was a visiting scholar at the International Computer Science Institute (ICSI), Berkeley in 2003, 2005 and 2013.

Dr. Gurtov is a co-author of over 150 publications including three books, research papers, patents, and five IETF RFCs. He has contributed to HIP standardization at the IETF, where he co-led the HIP Research Group at the Internet Research Task Force (IRTF), co-authoring RFC 6538 summarizing experiences of early HIP experiments and deployments. His book on HIP was placed on IEEE “Best Readings” list in Communications and Information Systems Security (CIS).

Richard Langston, Tempered Networks

Richard Langston runs product management at Tempered, and has been building networks as both a practitioner and product designer for over two decades. He got his start building university Arpanet networks and was also a network architect at Cisco Systems before building products for Cisco, Extreme Networks, Juniper, and others.

Leverage Host Identity Protocol to secure your business.

Schedule a meeting with our experts to learn more.

experts@tempered.io | +1 206.452.5500