TEMPERED NETWORKS®

Highly Available. Radically Secure. Remarkably Simple.

Use Case

Instantly Revoke Employee or Vendor Machine Access From Your Network

Identity-Defined Networking: Instant Overlay Networking

Complexity Adds Risk

Internal or 3rd party threats top the list of security challenges for many organizations. Giving access to machines on your network is time-consuming and often involves multiple complex tools and technologies that need to be configured correctly. But what happens when access needs to be revoked? (hint: it takes too long)

Simple Access Revocation

With our IDN solution, it's now incredibly easy to revoke device access to any IDN overlay segment, with a click of a button. Even if the users' credentials are still valid, the device cannot access anything within the IDN fabric unless whitelisted based on its unique cryptographic identity. Whether your CEO's laptop was stolen, or you no longer work with a particular supplier, you can quickly revoke access from IDN overlays. With little, to no, modification to the existing switching and routing infrastructure, you can now provision, revoke, and remediate networked resources 97% faster.

Significantly Reduce Your Risk

- Add, disable, and revoke users' machines—with one mouse click
- Minimize internal threats with verifiable segmented access
- Grant access to only authenticated, authorized, and accountable (AAA) machines
- Eliminate certificate revocation per individual VPN/FW

Decrease IT CapEx and OpEx costs as much as:

50%

Reduce networking & resource provisioning time up to:

97%

Reduce attack surface by up to:

90%

To learn more or schedule a no obligation demo, email: info@temperednetworks.com or visit www.temperednetworks.com

 |