What is network pivoting?

Network pivoting is using a compromised host as a relay to reach systems the attacker cannot connect to directly, typically an internal network segment behind the first machine. It is built from port forwarding, SOCKS proxies, and tunneling tools (SSH, chisel, ligolo-ng) that route the attacker's traffic through the foothold. Pivoting turns a single compromised, internet-facing box into a doorway onto the whole internal network, which is why segmentation and egress control matter.

HOW IT WORKS

01 How it works: forwarding, proxies, tunnels

Pivoting is assembled from a few building blocks, each with its own page:

- Port forwarding: relay one port from the attacker, through the pivot, to one internal service.
- SSH tunneling: local, remote, and dynamic forwards over SSH, the most common manual method.
- SOCKS proxies and proxychains: route any tool through the pivot, not just one port.
- chisel and ligolo-ng: purpose-built tunneling tools for pivoting over HTTP or a virtual interface.

02 Why it matters

A single exposed host with weak internal segmentation can expose the entire internal network. Pivoting is what converts "they popped one server" into "they can reach the database, the file shares, and the domain."

It also helps attackers evade controls: traffic to internal systems originates from a trusted internal host, not a suspicious external IP.

> SEGMENTATION IS THE ANSWER
>
> *Pivoting works because the compromised host can reach internal systems. Network segmentation and strict egress filtering shrink what a single pivot can touch, which is the most effective defence.*

SOURCES

[1] MITRE ATT&CK: Lateral Movement (TA0008)

[2] NIST SP 800-115 Technical Guide to Security Testing

[3] Linux man-pages: ssh(1)

Find the lateral-movement paths before an attacker does.

securelayer7.net/learn/lateral-movement/what-is-network-pivoting

Open online