What is port forwarding?

Port forwarding relays traffic for a single port from one machine to another, commonly through a compromised pivot host so an attacker can reach an internal service they cannot connect to directly. There are three directions: local (open a port on your side that maps to an internal service), remote (open a port on the pivot that maps back to you), and dynamic (a SOCKS proxy for any destination). It is the basic building block of network pivoting.

HOW IT WORKS

01 How it works and payload

SSH is the most common way to set up each direction (see SSH tunneling):

- Local: `ssh -L 8080:10.10.0.20:80 user@PIVOT` then browse `localhost:8080` to reach the internal web server.
- Remote: `ssh -R 9001:127.0.0.1:9001 user@PIVOT` to expose your service on the pivot.
- Dynamic (SOCKS): `ssh -D 1080 user@PIVOT` then point tools through the proxy.

Dedicated tools like chisel and ligolo-ng do the same without SSH. Documented techniques shown for defenders.

> THREE DIRECTIONS
>
> *Local brings an internal port to you. Remote pushes a port to the far side. Dynamic opens a SOCKS proxy for everything. Knowing which one is in use tells you which way traffic is flowing.*

HOW TO DEFEND

- Segment the internal network so a single pivot cannot reach sensitive services in the first place.
- Restrict egress so a compromised host cannot tunnel out to the attacker.
- Monitor for long-lived connections and tunneling patterns, especially from servers that should not initiate them.
- Limit SSH and tooling available on servers that face the internet.
- Detect SOCKS proxy and forwarded-port behaviour on the network.

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-port-forwarding

Open online