What is SSH tunneling?

SSH tunneling uses an SSH connection as a carrier for other network traffic, so a service that is only reachable from the SSH server becomes reachable from elsewhere. The three flags are `-L` (local forward), `-R` (remote forward), and `-D` (dynamic, a SOCKS proxy). It is the most common manual pivoting method: an attacker who has SSH to a compromised host tunnels through it to reach the internal network. It is also legitimate administration, so detection looks for the pattern, not the protocol.

HOW IT WORKS

01 How it works and payload

With SSH access to a pivot, the attacker sets up the forward they need:

- Local (reach an internal web app): `ssh -L 8080:10.10.0.20:80 user@PIVOT` then open `http://localhost:8080`.
- Remote (expose your handler on the pivot): `ssh -R 4444:127.0.0.1:4444 user@PIVOT`.
- Dynamic (SOCKS for the whole subnet): `ssh -D 1080 user@PIVOT` then run tools through the proxy (with proxychains).

Documented techniques shown for defenders.

> REMEMBER THE FLAGS
>
> *-L brings a remote service to you. -R pushes a local service to the far side. -D is a SOCKS proxy for everything. These three cover almost all SSH pivoting.*

HOW TO DEFEND

- Restrict SSH on internet-facing and sensitive hosts (who can connect, from where).
- Disable forwarding where not needed (`AllowTcpForwarding no`, `PermitTunnel no` in sshd_config).
- Segment and restrict egress so a tunnel cannot reach much or call out.
- Monitor for long-lived SSH sessions with forwarding and for SOCKS proxy patterns.
- Limit tooling on servers so an attacker has fewer ways to tunnel.

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-ssh-tunneling

Open online