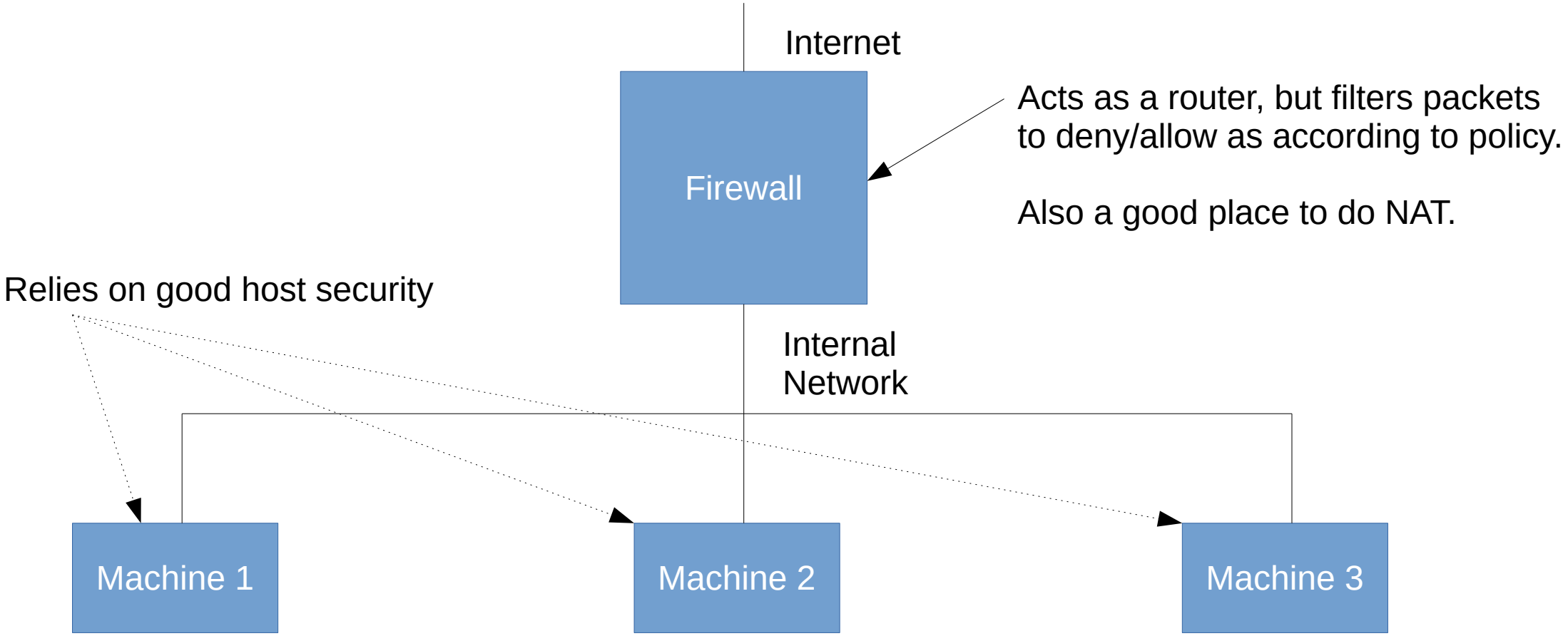
Firewalls

Peter Chapin

Vermont State University

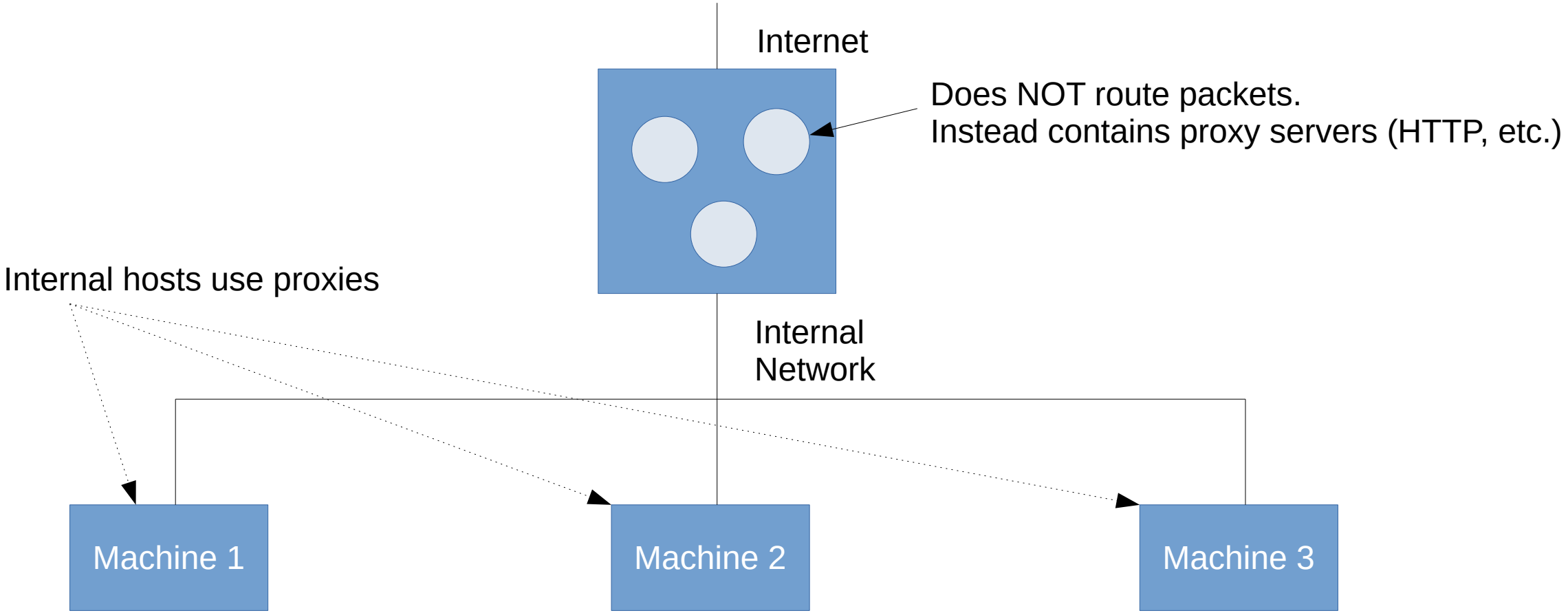
Screening Router



Zero Trust?

- Traditionally, those on the internal network were implicitly trusted
  - This causes problems when an internal host or employee is compromised.
- *Zero Trust* is a security stance that says the internal network isn't trusted
  - Use local firewalls and host-based firewalls to partition the network into micro-segments
  - Require explicit authentication and MFA for internal users when accessing internal resources.
  - Use encrypted network protocols even for traffic across the internal network.
  - etc.

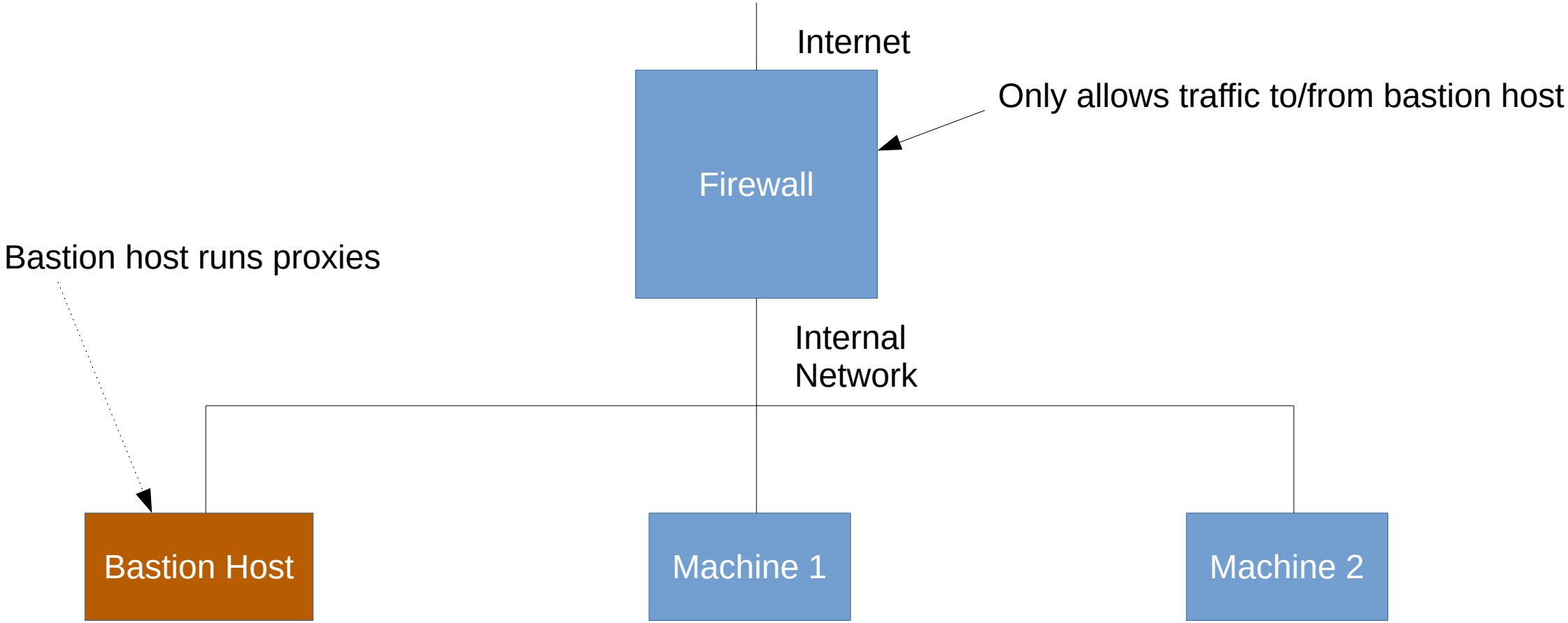
Dual Homed Host



Proxies?

- A proxy server provides a service for an internal user using external servers.
  - HTTP supports proxies. User configures web browser to connect to the proxy.
  - Every web access is sent to the proxy; the proxy makes the request on behalf of the user.
  - Users don’t connect to external web servers directly.
- Advantages…
  - Proxy can cache responses across multiple users
  - Proxy has access to the Internet; users have no direct internet access
  - Proxy can block access to certain websites using a centrally located policy
- HTTP, SMTP are natural for proxies because their standards support the feature directly.

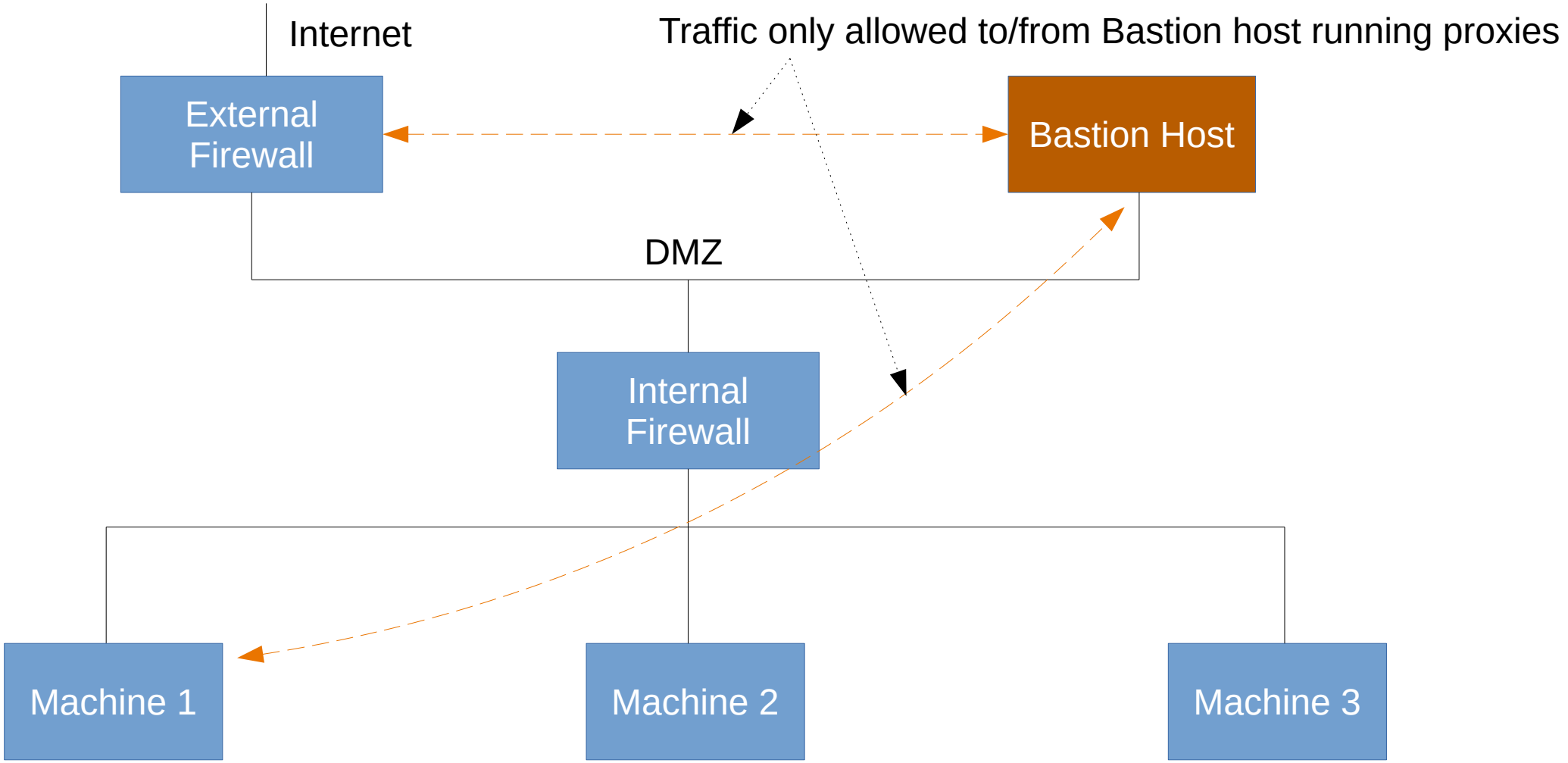
Screened Host



Bastion Host?

- A *hardened host* that connects to the external network. Location for externally facing servers.
  - Minimal software configuration
  - Aggressive security patching
  - Very limited access (typically just administrators)
  - Extensive monitor/auditing

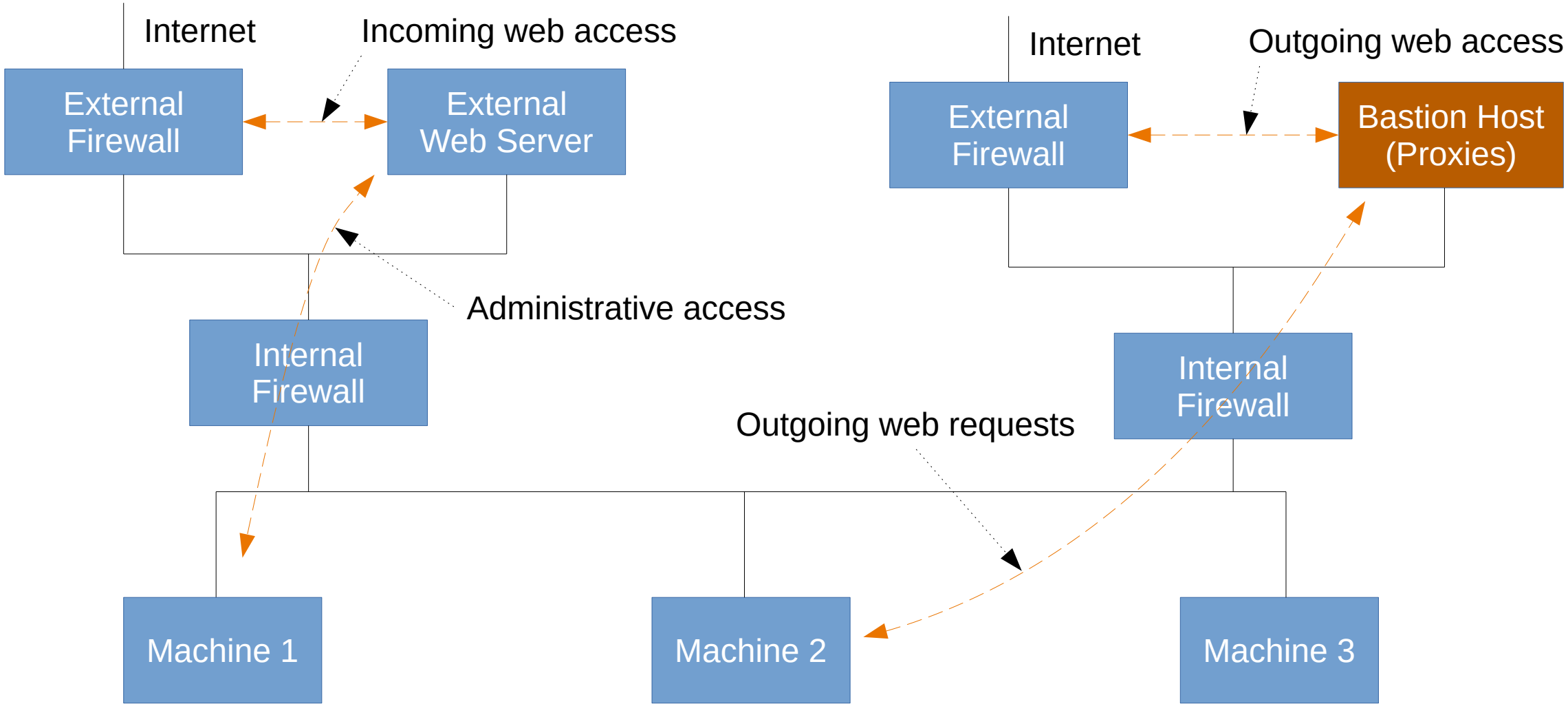
Screened Subnetwork



DMZ?

- *Demilitarized Zone* (DMZ): A network segment that separates the internal network from the external network.
- In a *two-firewall* solution, the DMZ is the network between the firewalls.
  - If the bastion host is compromised, the internal firewall protects the internal network.
- In an alternative configuration, the DMZ might be connected to a dedicated interface on the router/firewall.

Split DMZs


Internet
Incoming web access
External Firewall
External Web Server
Administrative access
Internal Firewall
Internet
Outgoing web access
External Firewall
Bastion Host (Proxies)
Internal Firewall
Outgoing web requests
Machine 1
Machine 2
Machine 3

Notes

- Multiple bastion hosts okay (even good)
- Okay to merge bastion host & external router
- Dangerous to merge bastion host & internal router
  - If bastion host compromised, internal network is exposed
- Dangerous to use multiple interior routers
  - Internal traffic may accidentally pass over the perimeter network
- Okay to use multiple exterior routers
- Dangerous to use both screened subnets and screen hosts
  - Hard to manage