# Gather Victim Network Information: Network Security Appliances, Sub-technique T1590.006 - Enterprise

Archived: 2026-04-05 12:59:05 UTC

Adversaries may gather information about the victim's network security appliances that can be used during targeting. Information about network security appliances may include a variety of details, such as the existence and specifics of deployed firewalls, content filters, and proxies/bastion hosts. Adversaries may also target information about victim network-based intrusion detection systems (NIDS) or other appliances related to defensive cybersecurity operations.

Adversaries may gather this information in various ways, such as direct collection actions via Active Scanning or Phishing for Information.[1] Information about network security appliances may also be exposed to adversaries via online or other accessible data sets (ex: Search Victim-Owned Websites). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: Search Open Technical Databases or Search Open Websites/Domains), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: External Remote Services).

---

Source: https://attack.mitre.org/techniques/T1590/006