Network Boundary Bridging: Network Address Translation Traversal, Sub-technique T1599.001 - Enterprise

Archived: 2026-04-05 13:52:36 UTC

Adversaries may bridge network boundaries by modifying a network device's Network Address Translation (NAT) configuration. Malicious modifications to NAT may enable an adversary to bypass restrictions on traffic routing that otherwise separate trusted and untrusted networks.

Network devices such as routers and firewalls that connect multiple networks together may implement NAT during the process of passing packets between networks. When performing NAT, the network device will rewrite the source and/or destination addresses of the IP address header. Some network designs require NAT for the packets to cross the border device. A typical example of this is environments where internal networks make use of non-Internet routable addresses.[1]

When an adversary gains control of a network boundary device, they may modify NAT configurations to send traffic between two separated networks, or to obscure their activities. In network designs that require NAT to function, such modifications enable the adversary to overcome inherent routing limitations that would normally prevent them from accessing protected systems behind the border device. In network designs that do not require NAT, adversaries may use address translation to further obscure their activities, as changing the addresses of packets that traverse a network boundary device can make monitoring data transmissions more challenging for defenders.

Adversaries may use Patch System Image to change the operating system of a network device, implementing their own custom NAT mechanisms to further obscure their activities.

Source: https://attack.mitre.org/techniques/T1599/001