# TTP Detail – T1599

## TTP Information

Name: Network Boundary Bridging

Description: Adversaries may bridge network boundaries by compromising perimeter network devices or internal devices responsible for network segmentation. Breaching these devices may enable an adversary to bypass restrictions on traffic routing that otherwise separate trusted and untrusted networks.  
  
Devices such as routers and firewalls can be used to create boundaries between trusted and untrusted networks. They achieve this by restricting traffic types to enforce organizational policy in an attempt to reduce the risk inherent in such connections. Restriction of traffic can be achieved by prohibiting IP addresses, layer 4 protocol ports, or through deep packet inspection to identify applications. To participate with the rest of the network, these devices can be directly addressable or transparent, but their mode of operation has no bearing on how the adversary can bypass them when compromised.  
  
When an adversary takes control of such a boundary device, they can bypass its policy enforcement to pass normally prohibited traffic across the trust boundary between the two separated networks without hinderance. By achieving sufficient rights on the device, an adversary can reconfigure the device to allow the traffic they want, allowing them to then further achieve goals such as command and control via [Multi-hop Proxy](https://attack.mitre.org/techniques/T1090/003) or exfiltration of data via [Traffic Duplication](https://attack.mitre.org/techniques/T1020/001). Adversaries may also target internal devices responsible for network segmentation and abuse these in conjunction with [Internal Proxy](https://attack.mitre.org/techniques/T1090/001) to achieve the same goals.(Citation: Kaspersky ThreatNeedle Feb 2021) In the cases where a border device separates two separate organizations, the adversary can also facilitate lateral movement into new victim environments.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## APTs (Intrusion Sets)

* APT41