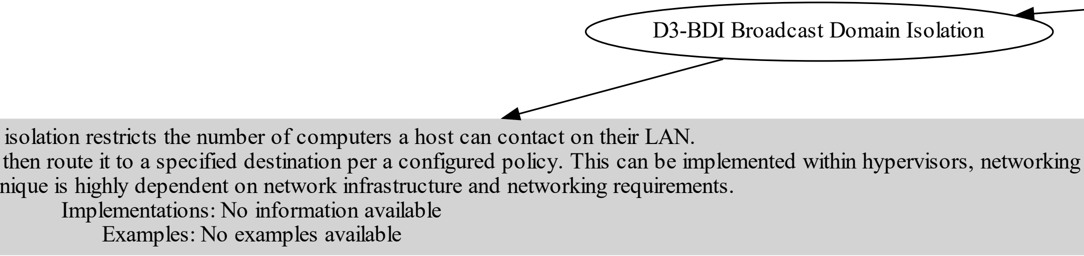
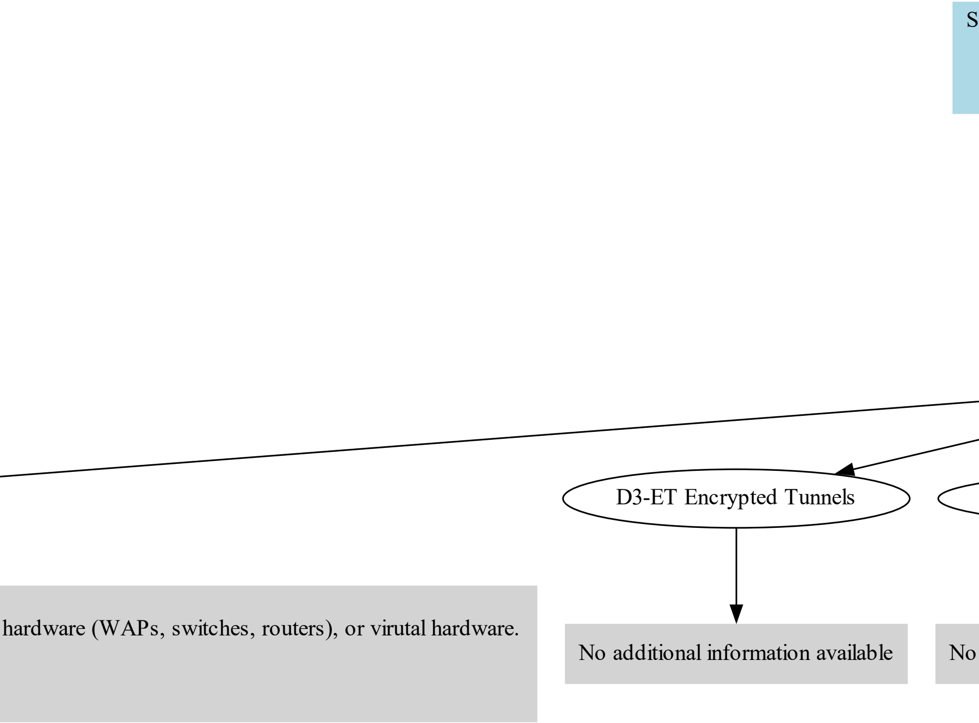
Definition: Broadcast

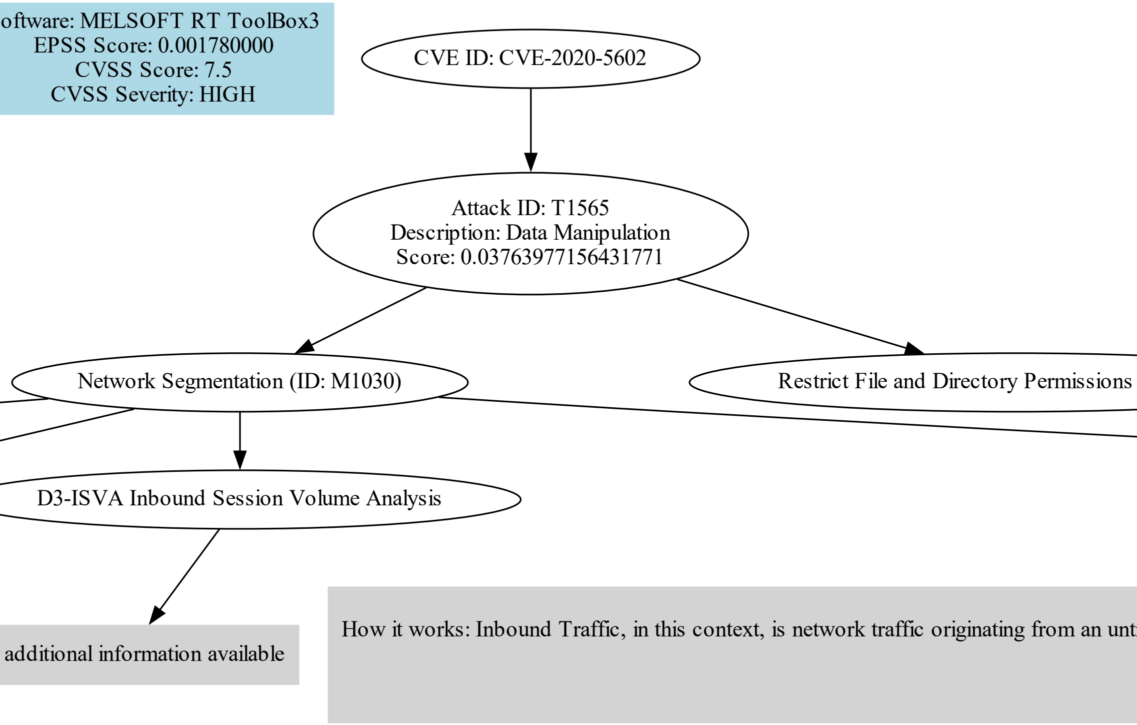
How it works: Software Defined Networking, or other network encapsulation technologies intercept host broadcast traffic

Considerations: This tech

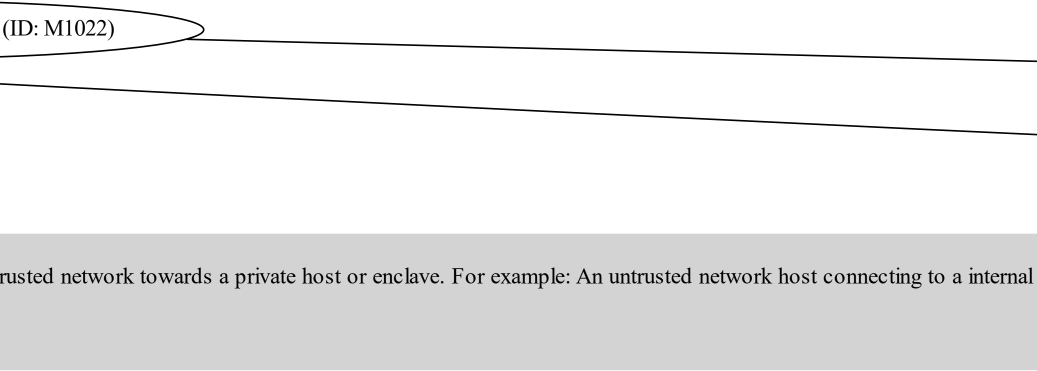

D3-BDI Broadcast Domain Isolation

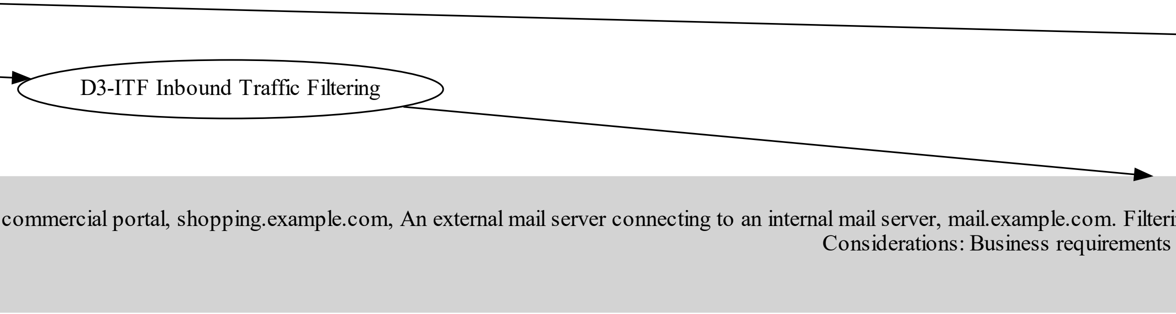
isolation restricts the number of computers a host can contact on their LAN.
then route it to a specified destination per a configured policy. This can be implemented within hypervisors, networking
nique is highly dependent on network infrastructure and networking requirements.
Implementations: No information available
Examples: No examples available


S
D3-ET Encrypted Tunnels
hardware (WAPs, switches, routers), or virutal hardware.
No additional information available
No


oftware: MELSOFT RT ToolBox3
EPSS Score: 0.001780000
CVSS Score: 7.5
CVSS Severity: HIGH
CVE ID: CVE-2020-5602
Attack ID: T1565
Description: Data Manipulation
Score: 0.03763977156431771
Network Segmentation (ID: M1030)
Restrict File and Directory Permissions
D3-ISVA Inbound Session Volume Analysis
additional information available

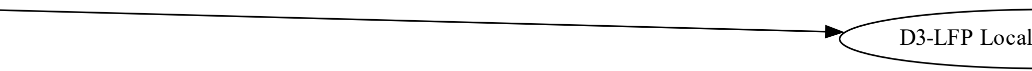
How it works: Inbound Traffic, in this context, is network traffic originating from an unt


(ID: M1022)
rusted network towards a private host or enclave. For example: An untrusted network host connecting to a internal

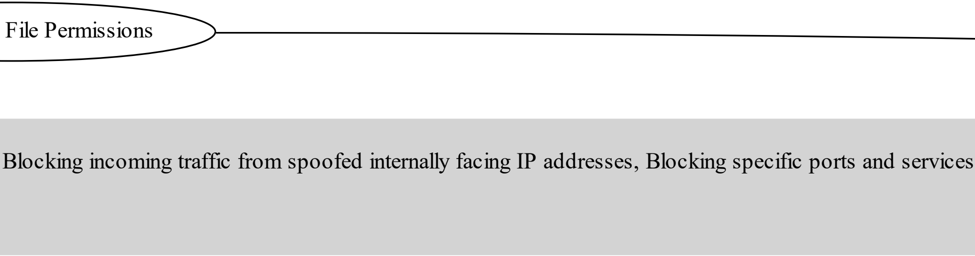

D3-ITF Inbound Traffic Filtering

commercial portal, shopping.example.com, An external mail server connecting to an internal mail server, mail.example.com. Filteri
Considerations: Business requirements

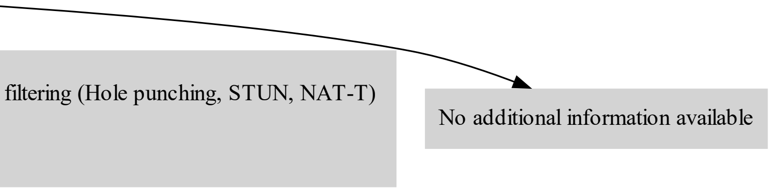
Definition: Restricting network traffic originating from untrusted networks destined towards a
ng policies are developed by administrators to meet business requirements and limit connectivity. These policies
typically drive the development of filtering rulesets. Protocols using non-standard ports may circumvent filtering
Implementations: OpenWRT, Netfilter (Linux), Windows Firewall
Examples: No examples available


D3-LFP Local

private host or enclave.
are implemented on edge devices such as firewalls, routers, and intrusion prevention systems. Examples of filters:
technology, which does not detect application protocol based on traffic Content


File Permissions
Blocking incoming traffic from spoofed internally facing IP addresses, Blocking specific ports and services

from establishing Connections, Limiting specific IP ranges from connecting to the network, Dynamic inbound


filtering (Hole punching, STUN, NAT-T)
No additional information available