

Software: RSLogix  
EPSS Score: 0.820820000  
CVSS Score: N/A  
CVSS Severity: N/A

CVE ID: CVE-2012-0221

Attack ID: T1071  
Description: Application Layer Protocol  
Score: 0.10365885890717234

Network Intrusion Prevention (ID: M1031)

Filter Network Traffic (ID: M1037)

D3-ITF Inbound Traffic Filtering

D3-NTA Network Traffic Analysis

D3-OTF Outbound Traffic Filtering

D3-NI Network Isolation

No additional information available

No additional information available

No additional information available

Definition: Restricting network traffic originating from untrusted networks destined towards a private host or enclave.  
How it works: Inbound Traffic, in this context, is network traffic originating from an untrusted network towards a private host or enclave. For example: An untrusted network host connecting to a internal commercial portal, shopping.example.com, An external mail server connecting to an internal mail server, mail.example.com. Filtering policies are developed by administrators to meet business requirements and limit connectivity. These policies are implemented on edge devices such as firewalls, routers, and intrusion prevention systems. Examples of filters: 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)  
Considerations: Business requirements typically drive the development of filtering rulesets. Protocols using non-standard ports may circumvent filtering technology, which does not detect application protocol based on traffic Content  
Implementations: OpenWRT, Netfilter (Linux), Windows Firewall  
Examples: No examples available