Filter Network Traffic, Mitigation M1037 - Enterprise

Archived: 2026-04-02 12:45:31 UTC

Enterprise T1557 Adversary-in-the-Middle

Use network appliances and host-based security software to block network traffic that is not necessary within the environment, such as legacy protocols that may be leveraged for AiTM conditions.

.001 LLMNR/NBT-NS Poisoning and SMB Relay

Use host-based security software to block LLMNR/NetBIOS traffic. Enabling SMB Signing can stop NTLMv2 relay attacks.[1][2][3]

.002 ARP Cache Poisoning

Consider enabling DHCP Snooping and Dynamic ARP Inspection on switches to create mappings between IP addresses requested via DHCP and ARP tables and tie the values to a port on the switch that may block bogus traffic.[4][5]

.003 DHCP Spoofing

Consider filtering DHCP traffic on ports 67 and 68 to/from unknown or untrusted DHCP servers. Additionally, port security may also be enabled on layer switches. Furthermore, consider enabling DHCP snooping on layer 2 switches as it will prevent DHCP spoofing attacks and starvation attacks. Consider tracking available IP addresses through a script or a tool.

Additionally, block DHCPv6 traffic and incoming router advertisements, especially if IPv6 is not commonly used in the network.[6]

Enterprise T1071 Application Layer Protocol

Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic.

.001 Web Protocols

Restrict and monitor outbound web traffic (HTTP/HTTPS) from critical servers to only approved destinations. Limiting the ability to initiate outbound HTTP/HTTPS connections, especially from public-facing servers, can prevent attackers from using tools like curl or wget to communicate with external C2 servers or download malicious payloads.

.002 File Transfer Protocols

Filter outbound FTP/SFTP traffic from sensitive systems, allowing file transfers only to trusted internal or known IP addresses. This measure can prevent attackers from transferring data or payloads via FTP/SFTP channels to or

from unauthorized external systems.

.003 Mail Protocols

Limit the ability of servers and critical systems to initiate outbound email communications. Filtering SMTP/IMAP/POP3 traffic to only trusted mail servers reduces the risk of attackers using compromised systems to exfiltrate data via email or to receive commands from attacker-controlled email accounts.

.004 DNS

Consider filtering DNS requests to unknown, untrusted, or known bad domains and resources. Resolving DNS requests with on-premise/proxy servers may also disrupt adversary attempts to conceal data within DNS packets.

.005 Publish/Subscribe Protocols

Consider filtering publish/subscribe protocol requests to untrusted or known bad resources over irregular ports (e.g. MQTT's standard ports are 1883 or 8883).

Enterprise T1197 BITS Jobs

Modify network and/or host firewall rules, as well as other network controls, to only allow legitimate BITS traffic.

Enterprise T1530 Data from Cloud Storage

Cloud service providers support IP-based restrictions when accessing cloud resources. Consider using IP allowlisting along with user account management to ensure that data access is restricted not only to valid users but only from expected IP ranges to mitigate the use of stolen credentials to access data.

Enterprise T1602 Data from Configuration Repository

Apply extended ACLs to block unauthorized protocols outside the trusted network.[7]

.001 SNMP (MIB Dump)

Apply extended ACLs to block unauthorized protocols outside the trusted network.[7]

.002 Network Device Configuration Dump

Apply extended ACLs to block unauthorized protocols outside the trusted network.[7]

Enterprise T1499 Endpoint Denial of Service

Leverage services provided by Content Delivery Networks (CDN) or providers specializing in DoS mitigations to filter traffic upstream from services.[8] Filter boundary traffic by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport. To defend against SYN floods, enable SYN Cookies.

.001 OS Exhaustion Flood

Leverage services provided by Content Delivery Networks (CDN) or providers specializing in DoS mitigations to filter traffic upstream from services.[8] Filter boundary traffic by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport. To defend against SYN floods, enable SYN Cookies.

.002 Service Exhaustion Flood

Leverage services provided by Content Delivery Networks (CDN) or providers specializing in DoS mitigations to filter traffic upstream from services.[8] Filter boundary traffic by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport.

.003 Application Exhaustion Flood

Leverage services provided by Content Delivery Networks (CDN) or providers specializing in DoS mitigations to filter traffic upstream from services.[8] Filter boundary traffic by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport.

.004 Application or System Exploitation

Leverage services provided by Content Delivery Networks (CDN) or providers specializing in DoS mitigations to filter traffic upstream from services.[8] Filter boundary traffic by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport.

Enterprise T1048 Exfiltration Over Alternative Protocol

Enforce proxies and use dedicated servers for services such as DNS and only allow those systems to communicate over respective ports/protocols, instead of all systems within a network. Cloud service providers support IP-based restrictions when accessing cloud resources. Consider using IP allowlisting along with user account management to ensure that data access is restricted not only to valid users but only from expected IP ranges to mitigate the use of stolen credentials to access data.

.001 Exfiltration Over Symmetric Encrypted Non-C2 Protocol

Enforce proxies and use dedicated servers for services such as DNS and only allow those systems to communicate over respective ports/protocols, instead of all systems within a network.

.002 Exfiltration Over Asymmetric Encrypted Non-C2 Protocol

Enforce proxies and use dedicated servers for services such as DNS and only allow those systems to communicate over respective ports/protocols, instead of all systems within a network.

.003 Exfiltration Over Unencrypted Non-C2 Protocol

Enforce proxies and use dedicated servers for services such as DNS and only allow those systems to communicate over respective ports/protocols, instead of all systems within a network.

Enterprise T1190 Exploit Public-Facing Application

Restrict outbound network traffic from public-facing servers to prevent unauthorized connections from initiating communications with attacker-controlled infrastructure. While this may not prevent the initial exploitation, it limits the attacker's ability to verify and control the compromised server post-exploit, reducing the overall impact of the attack.

Enterprise T1187 Forced Authentication

Block SMB traffic from exiting an enterprise network with egress filtering or by blocking TCP ports 139, 445 and UDP port 137. Filter or block WebDAV protocol traffic from exiting the network. If access to external resources over SMB and WebDAV is necessary, then traffic should be tightly limited with allowlisting. [9] [10]

Enterprise T1105 Ingress Tool Transfer

Use network filtering to block outbound traffic from compromised systems to unapproved external destinations. Restricting access to known, trusted IP addresses and protocols can prevent attackers from downloading malicious tools or payloads onto compromised servers after gaining initial access.

Enterprise T1570 Lateral Tool Transfer

Consider using the host firewall to restrict file sharing communications such as SMB. [11]

Enterprise T1599 Network Boundary Bridging

Upon identifying a compromised network device being used to bridge a network boundary, block the malicious packets using an unaffected network device in path, such as a firewall or a router that has not been compromised. Continue to monitor for additional activity and to ensure that the blocks are indeed effective.

.001 Network Address Translation Traversal

Block Traffic Upon identifying a compromised network device being used to bridge a network boundary, block the malicious packets using an unaffected network device in path, such as a firewall or a router that has not been compromised. Continue to monitor for additional activity and to ensure that the blocks are indeed effective.

Enterprise T1498 Network Denial of Service

When flood volumes exceed the capacity of the network connection being targeted, it is typically necessary to intercept the incoming traffic upstream to filter out the attack traffic from the legitimate traffic. Such defenses can be provided by the hosting Internet Service Provider (ISP) or by a 3rd party such as a Content Delivery Network (CDN) or providers specializing in DoS mitigations.[8]

Depending on flood volume, on-premises filtering may be possible by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport.[8]

As immediate response may require rapid engagement of 3rd parties, analyze the risk associated to critical resources being affected by Network DoS attacks and create a disaster recovery plan/business continuity plan to respond to incidents.[8]

.001 Direct Network Flood

When flood volumes exceed the capacity of the network connection being targeted, it is typically necessary to intercept the incoming traffic upstream to filter out the attack traffic from the legitimate traffic. Such defenses can be provided by the hosting Internet Service Provider (ISP) or by a 3rd party such as a Content Delivery Network (CDN) or providers specializing in DoS mitigations.[8]

Depending on flood volume, on-premises filtering may be possible by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport.[8]

As immediate response may require rapid engagement of 3rd parties, analyze the risk associated to critical resources being affected by Network DoS attacks and create a disaster recovery plan/business continuity plan to respond to incidents.[8]

.002 Reflection Amplification

When flood volumes exceed the capacity of the network connection being targeted, it is typically necessary to intercept the incoming traffic upstream to filter out the attack traffic from the legitimate traffic. Such defenses can be provided by the hosting Internet Service Provider (ISP) or by a 3rd party such as a Content Delivery Network (CDN) or providers specializing in DoS mitigations.[8]

Depending on flood volume, on-premises filtering may be possible by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport.[8]

As immediate response may require rapid engagement of 3rd parties, analyze the risk associated to critical resources being affected by Network DoS attacks and create a disaster recovery plan/business continuity plan to respond to incidents.[8]

Enterprise T1095 Non-Application Layer Protocol

Filter network traffic to prevent use of protocols across the network boundary that are unnecessary. If VMCI is not required in ESXi environments, consider restricting guest virtual machines from accessing VMCI services.[12]

Enterprise T1572 Protocol Tunneling

Consider filtering network traffic to untrusted or known bad domains and resources.

Enterprise T1090 Proxy

Traffic to known anonymity networks and C2 infrastructure can be blocked through the use of network allow and block lists. It should be noted that this kind of blocking may be circumvented by other techniques like Domain Fronting.

.003 Multi-hop Proxy

Traffic to known anonymity networks and C2 infrastructure can be blocked through the use of network allow and block lists. It should be noted that this kind of blocking may be circumvented by other techniques like Domain

Fronting.

Enterprise T1219 Remote Access Tools

Properly configure firewalls, application firewalls, and proxies to limit outgoing traffic to sites and services used by remote access software.

.002 Remote Desktop Software

Properly configure firewalls, application firewalls, and proxies to limit outgoing traffic to sites and services used by remote access software.

Enterprise T1021 .002 Remote Services: SMB/Windows Admin Shares

Consider using the host firewall to restrict file sharing communications such as SMB. [11]

.005 Remote Services: VNC

VNC defaults to TCP ports 5900 for the server, 5800 for browser access, and 5500 for a viewer in listening mode. Filtering or blocking these ports will inhibit VNC traffic utilizing default ports.

Enterprise T1218 System Binary Proxy Execution

Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic.

.012 Verclsid

Consider modifying host firewall rules to prevent egress traffic from verclsid.exe.

Enterprise T1205 Traffic Signaling

Mitigation of some variants of this technique could be achieved through the use of stateful firewalls, depending upon how it is implemented.

.001 Port Knocking

Mitigation of some variants of this technique could be achieved through the use of stateful firewalls, depending upon how it is implemented.

.002 Socket Filters

Mitigation of some variants of this technique could be achieved through the use of stateful firewalls, depending upon how it is implemented.

Enterprise T1537 Transfer Data to Cloud Account

Implement network-based filtering restrictions to prohibit data transfers to untrusted VPCs.

Enterprise T1552 Unsecured Credentials

Limit access to the Instance Metadata API. A properly configured Web Application Firewall (WAF) may help prevent external adversaries from exploiting Server-side Request Forgery (SSRF) attacks that allow access to the Cloud Instance Metadata API.[13]

.005 Cloud Instance Metadata API

Limit access to the Instance Metadata API. A properly configured Web Application Firewall (WAF) may help prevent external adversaries from exploiting Server-side Request Forgery (SSRF) attacks that allow access to the Cloud Instance Metadata API.[13]

Source: https://attack.mitre.org/mitigations/M1037