



LAN Inbound / Outbound default Configuration

Mode 1 – User Authentication / Authorization OFF

- All traffic from WAN to LAN is blocked
- Allow LAN to WAN (trusted local network)
- Allow access to local services

Mode 2 – User Authentication / Authorization ON

- Block WAN to LAN traffic
- Block LAN to WAN traffic
- Deny Access to local services**

** except traffic to special services like captive portal

- If User Authentication is enabled, http traffic to port 80 is redirected to Authentication gateway service. User is presented with a web login page. If the user has a successful authentication, the firewall applies the associated user access profile to all traffic to and from this user.

When using 802.1x authentication with a supported switch or wireless AP for SSO, the authentication process will be done transparently and the user will not be presented with the web login page.
- All traffic with origin on LAN and destination local services running on the gateway. Global access to Services running on the gateway can be configured in Security->Firewall->General->Services->Internal. Administrator can globally disable access to a given service even if a specific user access profile allows it.
- User traffic with origin on LAN and destination local services running on the gateway. At this level, the access control is dependent on the access profile enforced on the user. This can be configured in NAC->Access Profiles->"profile name"->Service Access. Please note that the global access control to services in 2, takes precedence, ie: if ftp service is blocked in 2, enabling it in the user access profile does not allow the traffic to get through.
- By default**, access to http services (port 80) on the Internet is transparently redirected through the proxy cache service. A bypass IP address list is available in case there is a need to disable proxy access to certain destination http servers. This can be configured in Router->Proxy Cache->Bypass List.
- Access to destinations on WAN can be filtered in NAC->Access Profiles->"profile name"->Internet Access->Outgoing. Please note that by default access is allowed from LAN to WAN. This option allows the administrator to deny access from LAN to specific destinations on the WAN, for this profile only.

- This is an inbound blacklist access control. IP addresses configured on this list are unconditionally blocked access to LAN and/or local services running on the gateway. See Security->Firewall->Blacklist.
- Traffic with origin on WAN and destination local services running on the gateway. Global access to services running on the gateway can be configured in Security->Firewall->General->Services->External. For a fully stealth firewall, uncheck all services in this list, uncheck option "WebAdmin Access->WAN" and uncheck "Enable Wan Ping Response".
- Access to destinations on LAN can be filtered in NAC->Access Profiles->"profile name"->Internet Access->Incoming. Please note that by default access is blocked from WAN to LAN. This option allows the administrator to allow access from specific origins on the WAN to destinations on the LAN, for this profile only. This option is normally used when the gateway is used in routing mode (ie: NAT disabled).
- Access Control based on content filtering. This is a global configuration and affects all** outbound http (port 80) traffic. Filtering can be based on domain names and words in URLs. See Security->Content Filtering.
- Inter-vlan access control can be configured in NAC->Access Profiles->"profile name"->VLAN->Vlan Access Policies. By default inter-vlan routing is blocked. This option allows the administrator to configure the allowed network destinations for traffic coming from the VLAN where the user is located. If User Authentication is disabled, inter-vlan access control can be configured in the special *default* profile. This special profile allows configuration of VLAN rules based on source and destination network addresses.

*** this does not affect access profiles configured with outbound premium qos pipes. QoS premium pipes are considered EF traffic and as such are not affected by the proxy cache mechanism.