ASUS Internet Security Router SL500/SL1000 Release Note

Version 1.1.11b.410

2004/5/25

Bug Fixes

The following lists bugs fixed for each release.

Bug Report Clarification – why these are not bugs

- Packets w/ source port = UDP No. 7 are blocked.
  - Explanation: After the firewall detects a uninitiated inbound UDP echo reply packet (i.e. UDP No. 7), the DoS module in the firewall will drop the invalid packets.
- Regarding the VPN configuration, as choose "ALL" in "Encryption/Authentication" of IKE, router negotiates "Life time" for ISAKMP SA with both time and data.
  - ASUS has done some research on this and according to our understanding that there is no differentiation between ISAKMP SA policy and ESP/AH SA policy. They are together referred as IPSEC SA policy.

    RFC 2407 is not very clear if the ISAKMP policy need only to have the Lifetime as TIME.

    The "ALL" is mainly used to make sure that VPN interoperability is smooth. For VPN interoperability and backward compatibility issues, ASUS finds it best that in "ALL" IKE negotiation, we should use lifetime in both time and data.

    ASUS has tested VPN interoperability with multiple VPN devices and never faced a problem. With Netscreen when AR260S initiates a IKE with Lifetime in both data and time, Netsceen replies back with both the values. However, when Netscreen initiates the IKE with lifetime only as time, AR260S correctly replies back with the lifetime as only Time.
- In VPN Aggressive mode, router re-transmits Quick(2) for IKE re-key.
  - Explanation: From the captured traces, it is found that the retransmission occurs after about 0.5 sec. Our code configures the time out dynamically. The time out is a complex calculation based on round trip time and also takes into consideration the time that might be needed to decode the DH or RCA encoding. We think that the behavior is normal as this is a UDP packet and retransmission is needed if it takes more than 0.5 seconds. Hence this is not a BUG.
- Router re-transmit ARP request though ARP negotiation is resolved.
  - Explanation: It is the bottom-half function in the OS kernel sending out another ARP request to update its neighbor table. This is done only once if the MAC address in the incoming packet is not yet in the ARP table. For example, a host pings the AR260S, and the MAC address of the host is not in the ARP table of the AR260S, then AR260S will send another ARP request out to update its neighbor table. If the MAC address of the host is in the ARP table, then AR260S will not send another ARP request to its neighbors.

Release 1.1.11b.410

- Removed un-used VPN statistics counters – Partial Packets, Packets Currently Reassembled and Non-First Fragments Currently in the Engine.
- Incorrect "Life Time(IKE or IPsec)" parameter if "Day" is used as the life time units. Its value will drop to 1/4 of the actual life time, e.g. 1 day = 21600 seconds instead of 86400 seconds.

Release 1.1.09b.410

- Default system is changed from 1/1/1970 to 1/1/2000 00:00:00 to avoid integer overflow due to
- Router reboots after enabling MAC cloning when click on the “Apply” button in WAN configuration in “dynamic” mode.
- Count down display is missing when system is reset via GUI Reset page.

Release 1.1.08.410

- WAN
  - Dynamic (i.e. DHCP client) connection mode
    - Bug fix for problem encountered when MAC cloning is enabled and disabled consecutively for many times.
- SL-500 specific
  - Fix ASP error when the 6th VPN policy is added.