NTS version 5.2.1 firmware update

Available Model

NTS 1134F / NTS 1136F / NTS 1154FR / NTS 3356FR / NTS 3372FR / NTS5572FT

Available firmware version

5.2.0.4

Attention

1 The system will be rebooted in 3-5 minutes after upgraded the new version.

2 .The system will be rebooted without update process. If the version is not 5.2.0.x (5.2.0.4).

Upgraded items:

==

##Homepage

-Add the hint at login and homepage if there's new firmware could be updated.

##Configuration > System

-Add [System Backup to USB].

##Configuration > Notification

-Modify the notification which is excluding the last log which was sent yesterday.

##Configuration > Report

-Modify the maximum range to 99 days at Report query interval.

-Modify the issue to remove “NO_” at System report and safety factor.

##Configuration > AP management

-Modify AP management,if deliver multiple NWA1100-NH,only one of the device will be delivered successfully.

##Network > Interface

-Modify the multiple subnet which can't be added in T-bridging mode at DMZ.

-Modify WAN Alive Detection.

-Modify the setting problem in T-bridging mode at DMZ.

-Modify the system error problem when the LAN is saved.

##Policy

-Modify the realtime traffic which can't be displayed.

-Modify the WAN which can't be selected at policy of IPv6.

-Modify NAT or Routing which are disconnected at LAN to WAN.

-Modify the policy, the packets which won't be dropped when select application control and set action as drop.

-Modify IPv6 policy,if designation network is disconnected,the policy will be ignored and compare to the next policy.

-Modify IPv6 loading which determines the interface is disconnected or not.

-Modify Max. Quota which is loaded error after the device rebooted.

-Modify the resolution which is more than 1600*900 will be shown abnormally.

##Objects > Address Table

-Modify partial ARP Table which can't be cleared.

##Objects > Service Table

-Add ICMP protocol at Service Group.

##Objects > Application Control

-Modify the Google service which can't be used after block BT.

-Add OneDrive （ Version 2015:17.3.6390.0509 , Version 2016:17.3.6743.1212）

-Modify the DHCP which is blocked accidentally after block BT.

##Objects > URL Filter

-Modify the block error issue when URL Whitelist is same with Domain Whitelist.

-Adjust the issue to remove the check process which is about checking the domain is exist or not at URL Filter and Objects > Address Table > WAN Group >User Define Domain.

##Objects > Authentication

-Modify the Page setting which displays [CMD Error] after saved.

-Modify one of the servers which is timed out when set multiple PoP3 servers at .

-Add Content Block and Background Block at Page setting.

##Objects > Bulletin Board

-Modify the redirect error issue when the URL with slash (/) in the browser.

##Objects > Radius

-Add Radius at Objects.

-Modify the authentication which can't be authenticated automatically after AP login and set client address as segment at client list.

##Network Service > DHCP

-Modify the service error when enable DHCP at DMZ without binding IP at DMZ.

##Network Service > DNS Server

-Add SRV record.

-Add IPv6 at Reverse DNS domain address.

-Add AAAA DNS Backup.

##Network Service > FTP Server

-Modify the lost issue when loading is too high.

##Network Service > Anti-Virus Engine

-Modify

-Modify the Kaspersky which can't be enabled.

-Modify the Clear Log which is invalid at Kaspersky.

##Network Service > High Availability

-Modify the related error when HA is processing.

##Advanced Protection > Anomaly IP Analysis

-Modify the invalid detection issue.

##Advanced Protection > Switch

-Modify the system operation which displays error when edit bind list.

-Modify the sequence of the column issue when double click at port information at Switch status.

-Modify the updated time issue when sort the data and double click at port information at Switch status.

-Modify the resolution invalid issue when the VLAN range is continuous number (e.g. 1~5) at DHCP Snooping.

-Add the bind port which could set any at IP Source Guard > bind list.

-Modify the IP source Guard which is disabled accidentally when delete bind list.

##Advanced Protection > Intranet Protect

-Adjust the IP collision mode.

-Adjust Detection Interface which should be NAT mode at Spoofing Setup.

-Add dump switch port at Automatically Block by Switch.

-Modify MAC collision log which displays 169.254.0.0/16.

##Mail Security > Filter & Log

-Adjust the synchronization issue at AD Valid Account Setting.

-Modify the mail issue.

-Add Link Filter at Anti-Spam.

-Add Rspamd at Filter & Log.

**The action is irreversible if Rspamd replaces SpamAssassin,and the learning database of SpamAssassin will be cleared.

-Add [Add file extension to infected mail] and [Subject of Infected Mail] at PoP3 virus mail.

-Modify the disconnected issue when enable mail log in DMZ-bridge mode.

##Mail Security > Mail Log

-Modify the error message when download deleted mail.

##SSL VPN > SSL VPN setting

-Modify the local account which couldn't access SSL VPN after the account is expired.

-Modify the password which supports particular string.

-Add Software Download Page Setting.

##VPN > IPSec Tunnel

-Add the issue to support multiple subnet.

-Modify the connection error issue.

##VPN > L2TP

-Add L2TP

##Other

-Modify the device which could use other WAN1 IP access the UI in DMZ bridging mode