NTS version 5.2.0.3 Firmware Update

Available Model

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

Available firmware version

5.2.0.2

Attention

01 The system will be rebooted (twice) in 35
minutes after upgraded the new version.

02 Minimum Version：V5.2.0.2. Otherwise the system will be rebooted without updating.

Upgraded items:

==========

##Configuration > Notification

-Modify WAN Disconnection which displays incorrect.

-Modify the partial items which could set scheduling time.

##Configuration > System > Schedule Backup

-Modify the restoration which is not allowed in small version.

##Configuration > AP Management

Modify
the update function of Client. The original function is to update AP2 after AP1 is updated. From now on AP1 and AP2 could be updated simultaneously.

-Modify the issue when add AP and click Connection Test at SNMP Write Community which is no reaction.

-Add NWA5123-NI

-Modify AP Management which can't connect to NWA1100-NH which has “@” in the password.

##Network > Interface

-Modify WAN in DHCP mode issue,the interface will take twice to enable DHCP's Client service and delete the second time's log,leading the interface without IP apparently.

##Network > 802.1Q

-Modify the invalid issue when LAN bind multiple ports.

##Policy

-Add Multiple Subnet in drop-down selection of source and destination

##Objects > QoS

-Add Qos which supports multiple ports detail setting.

##Objects > Application Control

-Add Youtube
-Modify freegate which blocks iCloud Mail accidentally.
-Modify BT which blocks Teamviewer accidentally when blocking BT is enabled.
-Add QQ_xf.
Test Version 4.8
-Add Wechat
Android test version 6.3.13
IOS test version 6.3.13
PC test version 2.0.0.37
-Add WhatsApp
Android test version 2.12.510
IOS test version 2.12.15
##Objects > URL Filter
-Modify the error message in PHP5's array function and URL filter > List Setting.
-Modify Domain Blacklist which is invalid in bridge mode.
##Objects > Virtual Server
-Modify virtual server which displays “specific reason,the action is denied“ when WAN is by PPPOE.
##Objects > Authentication
-Modify password which has add particular character transcoding in connection test in POP3 and Radius.
-Modify the AD account which should conform the uppercase and lowercase to login, switching to customize the request.
-Modify connection test which is successfully connected by POP3 Server but displays login fail in SSL VPN authentication.
-Modify the login issue if the password with particular symbols (e. g.$) in Radius will login fail.
##Objects > Bulletin Board
-Modify the error message when select Unselected group at Image-text Template > Group Management.
-Modify the following issue:
1. Schedule and Service Group should be considered when applying Bulletin Board.
2.If the source is by Select MAC Address Group in Address Table in Policy which can't apply Bulletin Board.
3.LAN,IP,MASK which are applied when the source is Inside_Any in Policy,switching to LAN_IP_MASK,SSL_VPN_MASK,and PPTP_REMOTE_IP could be applied in Bulletin Board.

4.If the source is Inside_DHCP or DMZ_DHCP in Policy which can't apply Bulletin Board.

-Modify Authentication issue:

1.Login with authentication may display “Internet Auth error,Please contact administrator “ if applied schedule in mode 2 in policy.

##Network Services > DHCP

-Modify the setting which will be cleared after disabled 802.1Q in DHCP.

-Modify the DHCP service which is off because of the repeated IP. (Add foolproof mechanism to prevent this situation.)

##Network Services > Skype Serivce

-Modify the error message voiceHelp.exe in Skype client.

-Modify the counter which unlimited increases,leading the memory crushed.

-Modify the log which didn't load the log in UI,but export the former log.

##Network Services > AntiVirus Engine

-Modify the database which can't be updated because of the connection test which can't socket to database.clamav.net.

-Modify ClamAV's monit which is enabled in the device without ClamAV.

-Modify the ClamAV which can't be updated.

##Network Services > High Availability

-Modify VLAN which doesn't enable when HA switches to Slave.(VLAN has bind multiple ports.)

-Modify VLAN DHCP which is disabled when HA switches to Slave.

-Modify SSL VPN which doesn't enable when HA switches to Slave.

-Add Manage IP and remote IP which could be original LAN IP when detect HA port.

-Modify connection interface which is connected by network cable. Master will take over when link down.

-Modify Skype record which is invalid when HA switches to backup.

-Modify HA which doesn't synchronize the certification of SSL VPN.

-Add HA port setting. (Network > Zone Setting)

-Add Network Services > High Availability > Interface LAN | HA

##Advanced Protection > Switch

-Add POE function.

-Modify the supported model GS-2210 which switches to GS2210-24HP and GS2210-24.

-Modify the port which can't be edited if the switch has bind or set POE.

-Modify Advanced Protection > Switch > Switch Setup

-Add the foolproof prompt which login account and login password can't be null in Codefense mode when edit or add the switch.

-Modify SNMP Read Community and SNMP Write Community which are public/public as default setting in ZyXEL's device.
-Modify the issue to clear /HDD/switch/xxx_stratum completely when delete switch.
-Modify the issue to fill the related setting automatically when search and add ZyXEL's switch.
-Add IP source guard in GS-2210 and XGS-3700.
-Modify SnmpNetworkClass.php get_ethinfo() .
-Add the issue to distinguish bind mode when edit or add switch.
-Modify bind mode's operation log.
-Modify the config of bind mode which should be null if switch type is SNMP.
-Modify the issue when edit switch's IP, the previous IP is cleared incompletely.
-Modify the switch model which can't be searched in Search Switch.
-Modify the issue to enable or disable the port by click.
-Modify the UI which displays Warning: fmod() expects parameter 1 to be double, string given in /PDATA/apache/class/Telnet.php on line 237 in new connection function in GS-2200, XGS-3700.
-Add XGS-3700. (Switch Type: Co-defense)
##Advanced Protection > Intranet protect > Spoofing Setup
-Modify Detection Interface which was LAN,DMZ, switching to LAN,DMZ which are equal to Advanced Protection > Switch > Add/Edit > Interface.
-Modify MAC > Router MAC and True Address in Collision Detection was shown normally but True Address's mac shown Router mac after refresh the page.
-Modify MAC Address Collision Detection N times / hour in operation log.
-Modify the issue to exclude the language in operation log.
-Modify the issue to hide Router MAC column if router mac is null.
##Mail Security
-Modify the PHP error message at Spam Mail Notice.
##SSL VPN
-Modify local account with Account Expiration Date may display login fail when download SSL VPN.
##VPN > VPN Policy
-Modify IPSec's policy which displays the first data when edit the policy in Internal to VPN.
##Tools > Connection Test
-Modify IP route which displays blank.
##Logs > System Operation
-Modify Logs_Sys.lang, Logs_Sys_AW5.lang, Logs_Sys_AW5R.lang.

-Modify the language in Japanese.
-Modify the issue to delete the repeated language ID.
-Modify the sequence of languages ID which are by Big5.
-Modify operation log
1.[Add]
(1)Column of Switch Type which doesn't display language.
(2)Column of Switch Model which displays incorrectly in Co-defense mode.
2.[Edit]
(1) Column of Switch Type which doesn't switch the language automatically after system switched the language.
##Other
-Modify User Group at Authentication,Service Group at Service Table,Setting at Application Control,URL Filter which can't enter Chinese character.
-Add the issue to check whether GET POST REQUEST include HTML tag or not.
-Modify DHCP interface which can't display correctly if VLAN bind multiple ports.
-Modify “LAN1” which switches to “LAN” in UI.
-Modify the setting which is related to the interface may display the ports which are set in UI.
-Modify the loophole issue which is mentioned by Hitcom.
-Modify frox version update 1.5
1.Modify FTP Server which is still working without setting Max. size of scanned files (KB) when downloading files.
2.Add SNAT in By pass and transparent bridge mode.
-Modify the time zone incorrect issue by PHP5.
-Disable HTTP Trace to prevent the loophole attack.