NTS Version 5.2.1.1 Firmware Update

Available Model

NTS 1134F 1136F 1154FR 3356FR 3372FR 5572FR

Available firmware version

5.2.1.1 (d4c3bf5b152980201e83e77b6d035b3f4e0db38d)

Attention

01 The system will be rebooted for twice in 3 to 5 minutes after upgrading the new version.

02 MD5 : 9c81a9405ed14d90a335d135d6d92217

Updated items:

==========

Configuration > Administration > System

●Modify an issue that the policy does not work if the policy is not point to WAN1 or the WAN Group does not include WAN1 in Transparent Bridging. (users does not select Outbound load balance of t-bridging.)

Configuration > System > Firmware Message

●Modify a display of update issue that small version may not display on the screen.

Configuration > AP Management

●Add a new model: NWA1123-ACv2 in AP Management.

Configuration > Backup and Mount

●Modify an issue that there is no content when accessing the external storage.

Configuration > Report

●Modify a display issue that there is no display of device interface flow and internet interface flow in the report.

●Modify an error which is scheduling may have probability for sending mail unsuccessfully.

●Modify a searching date error when searching report logs.

Signature update

●Modify an issue that URL Blacklist Database have been updated but Domain Blacklist does not update.

Network > Interface

●Modify an error that users choose a value in Speed and Duplex Mode but the value change to auto after the system restarting.

●Modify an issue that users can set bandwidth value in Network > Interface.

Network > Routing

●Modify an issue which cause double gateway when users setting another default gateway.

●Modify Routing table in Network > Routing.

●Modify an error that users can not change routing interface.

Policy

●Modify a display error that users add or edit “Service Port or Group” does not show the other languages.

●Modify an issue that policy support many service port groups.

1.Only changed in LAN and DMZ policy.

2.User defined can only choose the options at most 10 in the “Service Port or Group”.

●Modify an issue that users can assign a range for blocking “Source Port”.

●Modify a packet direction error in WAN policy > [incoming policy (IPV6)].

●Modify an issue that realtime traffic flow chart display unsteadily in the policy.

Object > Qos

●Modify an error that users can not restrict the flow of Qos list and recording.

●Modify an issue that users can select “per source ip based” bandwidth mode to restrict Qos of each network interface.

Object > Virtual Server

●Modify an issue that users can not modify the same network segment ip for WAN when setting WAN IP in the Virtual Server.

Object > Bulletin Board

●Modify an issue that users can not modify the format of “waiting for 10 seconds” character string in English after reading bulletin board.

Object > URL Filter

Object > URL Filter > Default Blacklist > URL Test

1.Modify an comparison issue for Default Blacklist database.

2.Modify an error message when Domain IP collate the Default Blacklist in Domain testing.

●Modify an issue that users can do domain searching in the URL Filter > Log.

●Add URL Blacklist database storage.

1. The system will check the database when booting the system every time.

2. Add update messages on the home page and Object > URL Filter > List setting for users to update URL Blacklist database.

3. Modify some URL device which does not have hard disk but the system still have web virus logs. Any URL device without hard disk is not supposed to have web virus logs.

Object > Address table

●Modify a display issue when deleting the address table, there will be a messages window show that address table link to policy will be deleted or not. The “confirm key” is outside the message window.

●Modify an issue that users set the same ip in WAN IP address, but the system do not

alert users to avoid it.

●Modify an issue when users delete address table group and policy, address table group and policy are still remaining.

Object > Application Control

●Modify an error for blocking file name(.exe) function failure in Application control.

●Modify an error that Application Control logs may not able to write in the DB.

Object > RADIUS

●Modify an issue that users start using radius from UI and it will occupy apache port.

●Modify an setting in Object > RADIUS > Client list

* Group change to authentication method.

+ supporting 3 kind of authentication method.

1. Local Authentication.

2. External Authentication.

3. Local + External Authentication.

Object > RADIUS

1. Add POP3 authentication method, but users should use EAP-TTLS + PAP authentication method.

1.1PC should install SecureW2.exe(for more detail please refer to http://dp.tsh.ttu.edu.tw/tshweblog/post/328/9569)

1.2 Android should set up EAP-TTLS + PAP.

2. If users select filter out REALM in connecting test, the system will filter out realm from the account which is created by users.

3. Radacct、radpostauth saving engine changed from INNODB to MyISAM.

Object > Authentication

●Modify an error that users adding or editing local user account will show php error message in object > authentication.

●Modify program file code: UTF8-BOM → UTF8-NO BOM

●Modify an issue that users can customize background color for login page in authentication, but the web pages have different color between https and http web pages.

●Modify an issue that User Group can sorting automatically and add searching function in Object > Authentication.

●Add sorting function in Mail Security > Filter and Log > Valid Account Setting > Exchange Server List > View List.

●Modify an error that authentication account was removed usually and the log showed Login Timeout when users enter 0 in “Re-login after user has logged in for” setting.

Object > Authentication > Local User:

●Modify an issue that users can add account over the amount of limit.

●Modify an issue that the system shows over amount of limit when user adding account ; however, numbers of account does not reach to the limit.
●Modify an issue that users does not select “Login with domain” in Object > Authentication > POP3, RADIUS User > POP3 Server, when SSL VPN client download the authentication and then enter account number without domain, the downloading will fail and the system keep showing login fail message window.
●Modify some part of functions in Authentication.
1.The system will not sent a new notification in Configuration > Notification > Authentication Expiring notice and Authentication Maturity delete notification.
2.Modify an issue that list page would not go to the last page after users add user group in Object > Authentication would not
Network Services > DHCP Services
●Modify an error that [DHCP Server] page and [MAC location in DHCP blacklist] page will missing when users use interface of LAN2 to 4.
●Add a function that UTM DHCP Server can support blacklist MAC.
Network Services > FTP Services
●Modify update of Service version.
Network Services > Anti-Virus Engine
●Modify an error that Kaspersky updating will be failed when Kaspersky’s key is expired.
●Modify an error that Anti-Virus does not update automatically after downloading Kaspersky engine.
Mail Security
●Modify an issue that the result of searching block IP logs in mail audit will be error.
●Modify an issue if subject is null but the system still can compare to the subject of mail.
●Add a fool-proofing function that system will automatically check graylist IP is IP or not.(The processing will not be executed if users enter domain in graylist IP.)
●Modify an issue that the filter will start to block as long as users set null in mail audit.
●Modify an issue that synchronization list does not appear when Valid Account Setting (Exchange Server) synchronize successfully.
●Modify an issue for release the mail.
●Modify an error that users enter 0 into the personal information comparison proportion.
●Modify a display error for learning logs in URL learning function.
●Modify an issue of isolation letter when users releasing and downloading mail.
●Add a new function for graylist and trusted list in order to supporting users to enter domain list.

●Modify an issue in Mail Audit > Mail capacity
1. Modify the judgement of mail capacity.
2. Add a reverse function for mail capacity audit.
●Modify an issue in Mail Security > Anti-Spam.
1.Supporting to add item of setting update automatically and the default adding setting will be selected.
2.Modify an issue that users would not see the Link Filter label form the spam mail notice.
●Modify an issue for adding * character to compare completely in mail audit.
1. Add a new way of completely comparison.
Completely comparison way is to enter ^ symbol in the beginning of ip address.
EX: If enter ^192.168. It means that starting with ip address 192.168 which would meet the requirement, on the other hand , 10.50.192.168 would not meet the requirement.
2. Add a character * for any kind of using.
●Modify an issue in Mail Security > Filter & Log > Valid Account Setting > Valid Account Setting AD list.
●When users select to add to ignore, the setting still have not added into the ignore setting of AD.
●Modify an issue of mail.
1. Improve mail searching.
2. The content of mail may not audit for CP850 mail code.
3. Modify download files when deleting them in the system, download files will be removed including isolation and backup files. ⇒ Mails will not be released and downloaded.
4. Modify an issue when using SMTP to send mail, it may cause sending repeatedly.
●Modify an error that mail isolation list does not work when clicking release.
The original timeout default value change from 10 seconds to 30 seconds.
●Modify a way for mails to open a larger capacity file.(larger than 15M)
●Modify an language error for filter conditions prompt in mail audit setting.
●Modify an issue that the system’ s file folder have over 3 million files and it will cause the system high loading when searching the file.
●Modify an issue in Mail Security > Mail Audit > Audit Advanced Setting
Releasing IP for blocking display of UI.
1. The setting changed. It will show up a window which shows all of the blocking ip in the window after users click IP blocking list.
2. Users can release all directly.
3. Add a function for searching IP to IP blocking log.
VPN
●Modify an error in the VPN policy, if we choose IPSec Tunnel as source or destination

ip and it have more than two network segments in the same time, the system will show up a error message.

●Modify an error in VPN > IPSec Tunnel

IPSec Tunnel will fail if users set the different preshare key between IPSec tunnel and L2TP and also the user use L2TP, ike v1 mode and both of local ID and remote ID are domain name.

●Modify an formate issue and application in pptp log.

●Add regular checking for status of dialing in VPN > PPTP Client.

●Modify an issue that the system will do a simple connection test before the user set up a connection in VPN > PPTP Client.

●Modify an issue in ipsec scheduling and add application execution monitoring.

●Modify an issue that VPN > PPTP server > PPTP server still using after resetting to default setting.

●Modify some IPsec service changes. openswan→ strongswan. The setting which will be affected are below the following:

1. VPN > IPSec Tunnel (a) add a mode which is multiple tunnel.

(b) users can assign v1 or v2 for IKE.

(c) add a option which is ipsec tunnel compatible with L2TP.

2. VPN > L2TP

→Modify an issue that Logs will be filled up if ipsec is attacked by ddos.

Others

●Modify an issue that if users save line detections as ICMP in IP tunnel, UI will show a error message.(two items are as follow:)

-Network > Interface > WAN interface.

-Object > Qos > Qos Setting.

●Modify an issue when system detecting virus block for encrypted web, the block page will show a line of text.

→Add a import function into URL blacklist database in Object > URL Filter > List Setting > add/edit default blacklist.

-Import file must belong to (zip files, files can judge password for encryption file and md5)

→When importing successfully, URL blacklist database version will change according to the version in the file.

→Add software interrupted and default average distribution.

→Modify an issue that console keep showing error message: /bin/cat: /PDATA/DEV/WAN*_v6: No such file or directory

●Modify IP Tunnel:

→Add a new setting location: Network > Interface > WAN interface > IP tunnel

setting

→ Model have IP Tunnel: NTS 1134F 1136F 1154FR 3356FR 3372FR 5572FR

→ IP Tunnel use dynamic distribution, and the order of distribution is eth7、eth6、eth5、eth4、eth2

→The maximum setting of WAN+IP Tunnel for users to use is 6.

●Modify an issue that users use 802.1Q DHCP service, but server service for DHCP Service in the home page would show

●Modify an issue in HTTPS Web logs and URL Filter.

1.Automatically checking the application is exist or not when booting, if not exist, the system will try to download from auto-update.

2. Network Service > WEB Service > WEB

-Use SSL Sniffer or not.

-Import Sniffer application by manual.

3. Add https URL list in Object > URL Filter.

4. Add https logs in Content Record > Web log.

5. Add Backup & Mount for https logs in Configuration > Web Log Backup & Mount.

6. Add HTTPS logs remove in WEB logs.

●Add a new searching which is Quota for users to search.

●Modify some database saving location for model without hard disk(NTS 1134F 1136F).

Advanced Protection

●Modify an issue that system provide a new function for Sorting the data in Advanced > Anomaly IP Analysis > Block List

●Modify an issue in [Advanced Protection > Intranet protect > Spoofing setup >

ARP Spoofing Alert Value > True Address.

● [Advanced Protection > Intranet protect > Arp Log] still have trust address logs after setting ip address.

SSL VPN

●Add “Last connection time” into SSL VPN account display.

●Modify some errors in SSL VPN > SSL VPN log

→[no searching result] would not show on the window.

→[currently connection time] change to [last connection time]

●Modify a debug of SSLVPN logging in checking which fill up with messages logs.

●Modify an issue that SSL VPN will occur an connection error if the default is not [C:\windows\system] in windows system.

version update 1.5.0.3

support --win-sys env

Skype

●Modify an issue in Network > Skype Service
1.Server IP would not reset when the user rest to default setting.
- use LAN IP as Server IP.
2. Add language for download page of setting item.
3. Users can not change Server port, the limit of transfer files record, the limit of voice record if users doesn't use skype service.
● Modify an issue in Network Service > Skype Service
→Users can not select DMZ IP in Server IP.
VPN Policy
●Modify an issue which is WAN interface information will show up in the VPN policy logs.
●Modify an issue that packet tracking in the VPN policy will show up a source ip which is belong to multiple subnet network segment.
●Modify an issue that users can restrict source IP in PPTP SERVER.
Log > System Operation
●Modify an issue that Logs will display error if users customize too many data of logs in Address Group.
●Modify an issue that the system can not display the information of IPV6 completely.
Status > Connection Status
●Modify an issue that computer list will show up an IP which beginning of ip address is 169, and it can not delete.
●Modify an issue that there is no keeping days for user to set in the wireless computer list.