Suggested Actions

on WebSAMS

Suggested Actions

- Keep Latest Windows Security Update
- Check Windows Hardening Status
- Check Antivirus Protection Status
- Ensure System Backup In Order
- Keep Best Practice in System Operation
- Keep Latest HTTP Server Patch Update

Keep Latest Windows Update

Go to “Control Panel” >“Windows Update” then select:

- Check for Updates

  (Select all updates except “Service Pack” / “Major Version Upgrade”)

- View Update History

- Change Settings

  (“Check for updates but let me choose whether to download and install them”)

Check Windows Hardening Status

- **Refer to**

"Installation Guidelines for WebSAMS 3.0"

➢ *"Appendix 7 : Windows Server 2012 R2 – OS Hardening Guide"*

http://www.websams.edb.gov.hk/files/newschool/Doc%2033%20Installation%20Guidelines%20for%20WebSAMS%203.0%20V1.3.3.pdf

for Checking the Windows Hardening Status including:

- Local Security Policy
- Windows Firewall
- Screen Saver Timeout

  (On resume, display logon screen)
- Remote Desktop with Network Level Authentication

  (In normal operation, the remote desktop should be disabled)

Check Antivirus Protection Status

- ☑ Ensure the Antivirus Software is in latest version
- ☑ Ensure the Online Protection is enabled
- ☑ Ensure the Virus Pattern is up-to-date

Ensure System Backup In Order

- Ensure the following kinds of backup are included:
  - Windows Server (Regular System Backup)
  - WebSAMS Program and Data (Daily, Weekly and Monthly Backup)
- Ensure encryption of backup image
- Check the Backup Log timely
- Check the status of Backup Media timely including:
  - On-line media (NAS)
  - Off-line media

Keep Best Practice on System Operation

- DO NOT share the disk storage of WebSAMS Server as network drive
- Only install WebSAMS related software
- DO NOT enable remote desktop service or install similar software
- DO NOT visit any suspected / unknown website or download files from questionable source in WebSAMS Server

Keep Latest HTTP Server Patch Update

- **Run the following command every month:**

  starthsp

Reference Material

- **Security Guides & Checklist for WebSAMS:**

  http://cdr.websams.edb.gov.hk *>主頁 > 參考資料 > 保安及處理敏感數據指引*

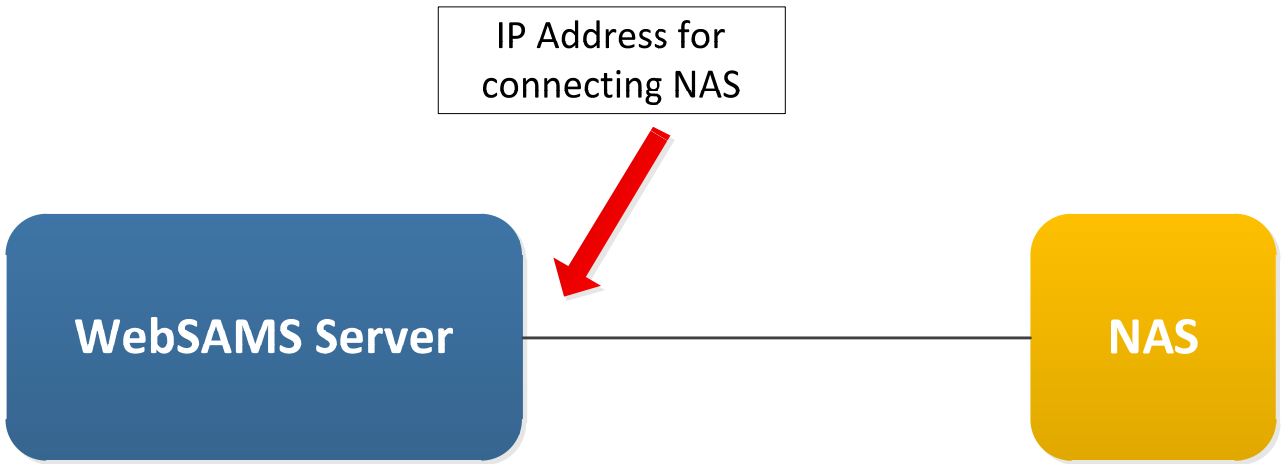
Reference Material (Cont'd)

- **Security Check for WebSAMS:**

  系統保安 > 保安檢查

Reference Material (Cont'd)

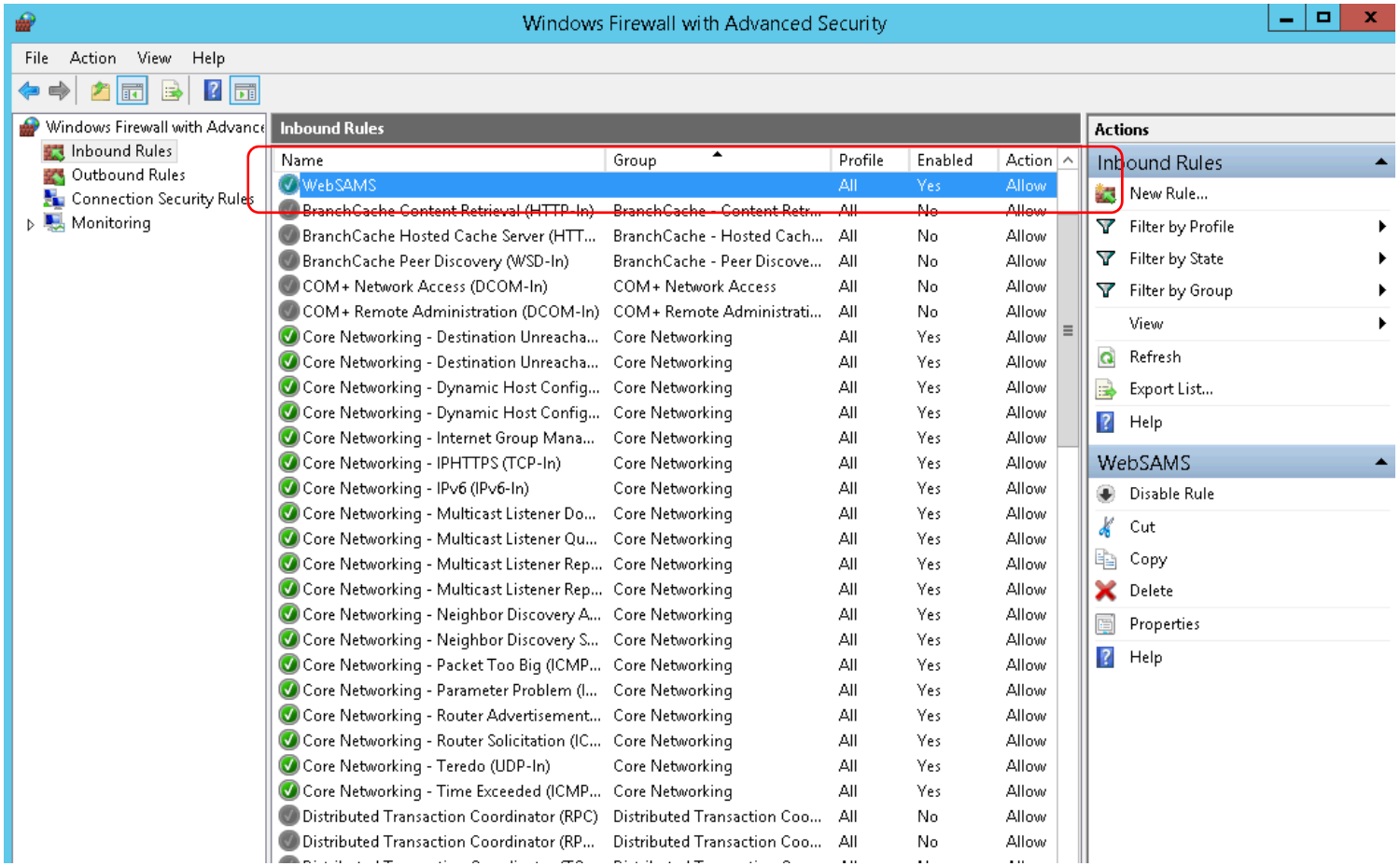
- **IP Address for connecting NAS:**



Reference Material (Cont'd)

- **Windows Firewall Settings:**

  Control Panel > Windows Firewall > Advanced Settings



Reference Material (cont'd)

- **WebSAMS Version Upgrade release note:**

  http://www.websams.edb.gov.hk > Version Upgrade for 3.0 > Major Upgrade

- **IT Security in Schools – Recommended Practice:**

  http://www.edb.gov.hk/attachment/en/edu-system/primary-secondary/applicable-to-primary-secondary/it-in-edu/WiFi900/IT_SecurityinSchools_RecommendedPractice_Aug2016.pdf

Reference Material (cont'd)

- Regularly visit the Information Security website of HKSAR for the update information of IT security

  http://www.infosec.gov.hk

- Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)

  https://www.hkcert.org

Reference Material (cont'd)

For enquiries:

- **Technical support:**
  - WebSAMS Helpdesk 3125 8510
- **Other enquiries:**
  - School Liaison Officer of the WebSAMS Team

http://cdr.websams.edb.gov.hk/Files/Doc/WebSAMS%20School%20Liaison%20Officer%20list.xls

The End