WPA2ã‚¨ãƒ³ã‚¿ãƒ¼ãƒ—ãƒ©ã‚¤ã‚ºï¼ˆEAP-PEAPï¼‰ã‚«ã‚ˆã‚‹èªè¨¼ç„¡ç·šLANåŒ–

Category : ã‚µãƒ¼ãƒ•ç®¡ç†æ—¥è¨˜

Published by [M-naka](#) on 2012/2/4

freeradius2ã•§EAP-PEAPã‚ªèªè¨¼ç„¡ç·šLANã‚’æ§‹ç‰ã•—ã•Ÿã€‚

è‡ªå®…ã•§ä½¿ã£ã•¦ã„ã‚‹WHR-HP-GNã•¯DD-WRTåŒ–ã—ã•—ã•¦ã„ã‚Šã€WPA2ã‚¨ãƒ³ã‚¿ãƒ¼ãƒ—ãƒ©ã‚¤ã‚ºã•Œä½¿ã•ˆã‚‹ã•†ã•«ã•ªã£ã•¦ã„ã‚‹ã€‚ã•¨ã•„ã•†ã•¯RADIUSã‚µãƒ¼ãƒ•ã‚’ç¶ã‚•ã••è¨å®šã•Œä½¿ã•ˆã‚‹ã€‚ã•§ã€•ãƒ•ãƒ£ãƒ¬ãƒ³ã‚¸ã—ã•¦ã¿ã•Ÿã€‚

ï¼‘ï¼Žèªè¨¼æ–¹å¼ã•®é¸å®š

ã€€EAPã‚«ã•¯ã„ã•ã•¤ã•‹ç¨®é¡žã•Œã•£ã•¦ã€ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£å¼·åŠ›ã•ªã‚ã®ã•§ã•¯EAP-TLSã€EAP-PEAPã€EAP-TTLSã• ã€‚
EAP-TLSï¼šã‚µãƒ¼ãƒ•ã‚»ãƒ©ã‚¤ã‚¢ãƒ³ãƒˆçŸ¬äºã•§é›»åèªè¨¼ã•™ã€ã‚»ãƒ¥ãƒªãƒ†ã‚£å¼·åº¦ã•¯æœ€å¼·ã€ãƒ©ã‚¹ã€‚
EAP-TTLSï¼šã¯ã‚¤ã‚¢ãƒ³ãƒˆè¨¼æ˜Žæ›¸ã•¯ä¸•è¦•ã•ã•ŒãŠEAP-TLSã•¨åŒç-‰ã•®ã‚»ãƒ¥ãƒªãƒ†ã‚£å¼·åº¦ã•Ÿã•Ÿ Windowsæ¨™æº–ã‚µãƒ—ãƒã‚«ãƒ³ãƒˆã•§ã•¯é•žå¾ã¿œã•ãƒ¥é€œã‚µãƒ—ãƒª ã‚¤ãƒ³ãƒˆã•Œå…¥ã‚‹ã€‚
EAP-PEAPï¼šã‚»ãƒ¥ãƒªãƒ†ã‚£å¼·åº¦ã•¯EAP-TLS/TTLSã•«è²ºã‚‹ã•ŒWindowsæ¨™æº–ã‚µãƒ—ãƒã‚«ãƒ³ãƒˆã•§å¾ã¿œã€ã‚µãƒ¼ãƒ•èªè¨¼ã•é›»åèªè¨¼æ›¸ã€ã€ã‚µãƒ©ã‚¤ã‚¢ãƒ³ãƒˆèªè¨¼ã•¯ID ã•¨ãƒ‘ã‚¹ãƒ¯ãƒ¼ãƒ‰ã€‚
ã•¨ã•ªã£ã•¦ã„ã‚‹ã€å¼·é€"ã‚µãƒ—ãƒªã‚«ãƒ³ãƒˆã•Œå…¥ã‚ªæ™‚ç‚¹ã•§EAP-TTLSã•¯å•„ä›ï¼ˆæ±Žç""æ§é‡è¦–ï¼‰ã€EAP-TLSã•¯ã€ãƒ©ã‚¤ã‚¢ãƒ³ãƒˆã•«é›»åèªè¨¼æ›¸ã‚’ç°ªã•£è¾¾¼è³¾ªã•ãŒã‚ªã€ã•®ã•Œæ€ã•«å•ˆã•ªã•ã€æ±Žç"""æ§ã•Œé«˜ã•ã•ã€ã‚µãƒ¼ãƒ•å•ã•®é›»åèªè¨¼æ›¸ã• ã•'ã‚ã€ã•ªã°OKã•ªEAP-PEAPã•§è¡Œã••ã•"ã•¨ã•«ã•—ã•Ÿã€‚ã•¡ã•ªã¿ã•«ã•†ã¡ã•®ä¼šç¤¾ã•®ç¾å†…ç„¡ç·šLANã„EAP-PEAPã• ã€‚

ï¼’ï¼Žé›»åèªè¨¼æ›¸ã®å–å¾—

ã€€RADIUSã‚µãƒ¼ãƒ•ã‚’è¤å–å•ã•ã•®gungnir.mythril.ne.jpã•§é•‹ç""ã•™ã‚‹ã•®ã•¯ãƒªã‚¹ã¯•Œã•ã€ã‚•
ã•®ã‚§ã•å†…å•ã•ã•®mjolnir.mythril.ne.jpã•§é•‹ç""ã•™ã‚‹ã€ã•ã€ã•®é–¢ä¿ã€ã•§ã€é›»åèªè¨¼æ›¸ã•¯
www.mythril.ne.jp
ã•®ã€ã•®ã®æµç""ã•Œã•ã•ã•ªã•ã€ä»Šæ´è‡ªå·±ç½²å••è¨¼æ›¸ï¼ˆã•ã€ã•ã†ã‚€Žã€ªãƒ¬ã‚ªãƒ¬è¨¼æ›¸ã€ï¼‰ã•§ç‰ã•™ã€ã•®ã•"è«—å¤ã• ã€è¶…å††é˜ãã•®ã•§ã€ã•†ä›€æžšèª²•†ã•ã€¦å€æ€ã•ã•£ã•Ÿã•®ã• ã•Œã€è²ã•ã¶•ã€ã•"
ã€€[StartSSL](#)
ã•§ç„¡æ–™å¾—ã•§ã•ã€ã•"ã•"ã•Œå¤æ›Žã€ã•"ã€Œã•§è¡Œã•ã•"ã•«ã•—ã•Ÿã€å•–å¾—æ‰‹é †ã•«ã•¤ã•ã•¯ã–œ«–ã•ã€‰å¤–ã€Œã‚ã•®ã•§çœ•ç•¥ã€FQDNã‚’secgw.mythril.ne.jpã•«ã•—ã•å•–å¾—ã€ä¸€é–"è¨¼æ›¸ã•Œå…¥ã‚Šã•ã•"ã€ã•Šä¿ã€Œã•ªã•ã€‚

（１）freeradius2ã•®ã‚¤ãƒ³ã‚¹ãƒˆãƒ¼ãƒ«ã•è¨å®š

ã€€ã‚¤ãƒ³ã‚¹ãƒˆãƒ¼ãƒ«ã•ã€Œyum install freeradius2
freeradius2-utilsã€•ã•§å®Œäº†ã€‚è¨å®šã•ä»¥ä¸‹ã€‚

ã€€ï¼'ï¼‰radius.conf
ã€€ã€€ã€€å®Ÿã•ãƒ‡ãƒ•ã‚©ãƒ«ãƒˆã•®ã•¾ã•¾ã•§OKã• ã•£ã•Ÿã‚Šã•™ã‚‹ã€‚

ã€€ï¼'ï¼‰client.conf
ã€€ã€€ã€€radiusã¯ãƒ©ã‚¤ã‚¢ãƒ³ãƒˆã•ã•ªã‚‹ç„¡ç·šLANãƒ«ãƒ¼ã‚¿ã•®IPã‚¢ãƒ‰ãƒ¬ã‚¹ã•å…±æœ‰ã‚·ãƒ¼ã‚¯ãƒ¬ãƒƒãƒˆã•shortnameã‚'è¿½è¨˜ã•™ã‚‹ã€‚å…±æœ‰ã‚·ãƒ¼ã‚¯ãƒ¬ãƒƒãƒˆã•¨shortnameã•ä»»æ„•ã•æ–‡å——å̂—ã•§OKã€‚
ã€€ã€€ã€€>ã€€ã€€ã€€ client
ã€€ã€€ã€€>ã€€ã€€ã€€ã€€ require_message_authenticator = yes
ã€€ã€€ã€€>ã€€ã€€ã€€ ã€€secretã€€ã€€ã€€ã€€= xxxxxxxxxxxxxxxx
ã€€ã€€ã€€>ã€€ã€€ã€€ ã€€shortnameã€€ã€€ = xxxxxxxxxxxxxxx
ã€€ã€€ã€€> }

ã€€ï¼"ï¼‰users
ã€€ã€€ã€€radiusçš„ã•«ã•¯UNIXãƒ¦ãƒ¼ã‚¶ï¼ˆ/etc/passewdï¼‰ã„MySQLï¼‹OpenLDAPã•§ã•®èª•è¨¼ã•§ã‚'è¡Œã•ˆã‚‹ã•ã•†ã• ã•Œã€•ä»Šå›žã•ãƒ©ã‚¤ãƒˆã•«radiusç''ã•®ãƒ¦ãƒ¼ã‚¶ãƒ•ã‚¡ãƒ«ã•§ç®¡ç•†ã•™ã‚‹ã•ã•«ã•—ã•Ÿã€‚ä»¥ä¸‹ã‚'è¿½è¨˜ã€‚
ã€€ã€€ã€€>ã€€leartext-Password := ""
ã€€ã€€ã€€> ã€€ã€€ã€€ã€€ã€€ã€€ã€€ã€€ã€€Service-Type = Framed-User,
ã€€ã€€ã€€> ã€€ã€€ã€€ã€€ã€€ã€€ã€€ã€€ã€€Framed-Protocol = PPP

ã€€ï¼"ï¼‰eap.conf
ã€€ã€€ã€€å¤šå›žㅿ̃å±±å ´ã€‚
ã€€ã€€ã€€ã€€ãƒ»default_eap_typeã•peapã•«ã•™ã‚‹ã€‚
ã€€ã€€ã€€ã€€ãƒ»PrivateKeyã•¨Certificateã•ãƒ•ã‚¡ãƒ¼ã•«æŒ‡å®šã•™ã‚‹ã•Œã•°OKã€/etc/pki/tlsä»¥ä¸‹ã•®ã‚·ãƒ³ãƒœãƒªãƒƒã‚¯ãƒªãƒ³ã‚¯ã•§ã‚‚å•ã€‚
ã€€ã€€ã€€ã€€ãƒ»StartSSLã•¨ä¸-é–"è¨¼æ˜Žæ›¸ã¿…ˆã• ã•Œã€•freeradiusçš„ã•«ã•¯CAã•å•¨ä¸€ãƒ•ã‚¡ã‚¤ãƒ«ã•—ã•æŒ‡å®šã•§ã••ã•ªã•ã€•ã•®ã•§ã••
ã€€ã€€ã€€ã€€ã€€ã€€cat CA.pem ä¸-é–"è¨¼æ˜Žæ›¸.pem > çµ•å•̂ã•—ã•Ÿè¨¼æ˜Žæ›¸.pem
ã€€ã€€ã€€ã€€ã€€ã€€ã•§ã••ã•å¸ ̃å•ãƒ•ã‚¡ãƒ«ã•åŒ–ã•™ã‚‹ã€‚StartSSLã•®ãƒ«ãƒˆè¨¼æ˜Žæ›¸ã€•ä¸-é–"è¨¼æ˜Žæ›¸ã•<ins>ã•"ã•"</ins>ã€‚pemå½¢å¼•ã•§ã€‚
ã€€ã€€ã€€ã€€ã€€ãƒrandomãƒ•ã‚¡ã‚¤ãƒ«ã•¯/dev/urandamã‚'æŒ‡å®šã•™ã‚‹ã€‚

ã€€ã€€ã‚·ã‚¹ãƒ†ãƒ çš„ã•«ã•¯ãƒ©ãƒ³ãƒ€ãƒ ãƒ‡ãƒ•ã‚¤ã‚¹ã•¯/dev/randomã•¨/dev/urandomã•®2ã•¤ã•ã‚Šã€•eap.confçš„ã•«ã•¯ã•"ã•<ã‚‰ä½•œã‚Šã•"ã•"ã• randomãƒ•ã‚¡ã‚¤ãƒ«ã‚'è¨å®šã•§æŒ‡å®šã•—ã•¦ã•‚ã‚‹ã•Œã•/dev/randomã•¨/dev/urandomã•ã‚‰ä½•œã‚‹ã•"ã•"ã• ãƒ•ã‚¡ã‚¤ãƒ«ã•§ã•radiusdã•Œèµ·å‹•ã‚‹ã•šã€•/dev/urandomã‚'ç›´æŽ¥æŒ‡å®šã•™ã‚‹ã•ã•"ã•§è§£æ±ºã•—ã•Ÿã€‚

ã€€ã•ã•"ã•freeradiusã‚'/usr/sbin/radiusd
-Xã•§ãƒ‡ãƒ•ãƒƒã‚°ãƒ¢ãƒ¼ãƒ‰èµ·å‹•ã••ã•›ã€•ã¯ãƒ©ã‚¤ã‚¢ãƒ³ãƒˆã•‹ã‚‰ã•®æŽ¥ç¶šã‚'è©¦ã•¿ã‚‹ã€‚

（２）Windows7ã•§è¨å®šã•æŽ¥ç¶š

Windows7å•´ã•®è¨å®šã•¯ã•“ã‚“ãªæ„Ÿã•˜ã€‚

　ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£ã•®ç¨®é¡žã•¯ã€ŒWPA2ã¨ãƒ³ã‚¿ãƒ¼ãƒ—ãƒ©ã‚¤ã‚ºã€•ã•æš—å•·åŒ–ã•®ç¨®é¡žã•¯ã€ŒAESã€•ã•è¬•è¨¼ã•®ç¨®é¡žã•¯ã€ŒMicrosoft:ä¿•è·ã••ã‚ŒãŸEAPï¼ˆPEAPï¼‰ã€•ã•’ã••ã•Œã•žã€é•¸æŠžã€çµ•ã•£ãŸã‚‰ã€Œè©³ç´°è¨å®šã•’æŠ¼ã•™ã€‚

　è¬•è¨¼ãƒ¢ãƒ¼ãƒ‰ã•¯ã€Œãƒ¦ãƒ¼ã‚¶ãƒ¼è¬•è¨¼ã€•ã•§æœ‡å®šã•ä»Šå›žã•¯Windowsãƒ¦ãƒ¼ã‚¶ãƒ¼/ãƒ‘ã‚¹ãƒ¯ãƒ¼ãƒ‰ã•è¬•è¨¼ã•™ã•ä»•çµ•ã•¿ã•—ã•Ÿã•—ã•®ã•§ã€ã•·ãƒ³ã‚°ãƒ«ã‚µã‚¤ãƒ³ã‚ªãƒ³ã•’æœ‰åŠ¹ã•—ã•—ã•Šã••ã€å¿…é ˆã•§ã•ã•ªã•ã€ç„¡ç•šLANã•ã•®æŽ¥ç¶šã•Windowsãƒã‚°ã‚ªãƒ³ã•ã•ƒ¼ãƒ¬ã‚¹ã•ã•ã€‚

　RADIUSã‚µãƒ¼ãƒ•ã•®è¬•è¨¼ã•’ã•™ã•ã•è¨å®šã•¯ã•“ã‚“ãªæ„Ÿã•˜ã€‚CAã•¯StartSSLã•®ãƒ«ãƒ¼ãƒ^ã•§ã‚‹StartComã•«ãƒ•ã‚§ãƒƒã‚¯ã‚’å…¥ã‚Œã‚ã€è¬•è¨¼æ–¹å¼•ã•¯EAP-MSCHAPv2ã‚’é•¸æŠžã€çµ•ã•£ãŸã‚‰ã€Œæ§‹æ•ˆã•’æŠ¼ã•™ã€‚

　ãƒ‡ãƒ•ã‚©ãƒ«ãƒˆã•¯ã•“ã•“ã•«ãƒ•ã‚§ãƒƒã‚¯ã•Œå…¥ã•£ã•¦ã„ã•ã•®ã•å¤–ã•™ã€ã•“ã€ã•’ãƒ•ã‚§ãƒƒã‚¯ã•å…¥ã•Œã•¾ã•¾ã•ã•—ã•¦ã•—ã•¾ã•ã•PCå••ãƒ¦ãƒ¼ã‚¶ãƒ¼••ã•§RADIUSè¬•è¨¼ã•Œå®Ÿè¡Œã••ã•Œã•¦ã•—ã•—ã•—ã•†ã•¦ã•®ç•°å¢ƒã•§ã•ä¸Šæ‰‹ã••ã•è¬•è¨¼ã•§ã••ã•ªã•ã€ã•“ã•“ã•¯freeradiuså•´ã•®ãƒãƒ«ãƒ è¨å®šã•ä¾•å˜ã•™ã•ã•‹ã•†ã•Œã€å‰•æ®µã•®ã•·ãƒ³ã‚°ãƒ«ã‚µã‚¤ãƒ³ãƒ³ã‚’è¡Œã•†ã•ã•ã•ã•Šã•ã•ã•ä•è¦•ã€‚

　ã•ã•ã•¾ã•§ã„ã•£ã•ã•ã€ã•ã•†ã„••æ•˜åŸã€‚
　ã••ã•ã•ã•£ã•æ›´ã€ã„ã•ã•ã€ã•Œã€å§ä½•"äºŒãƒ¶æœ‡ã••ã•‰ã•ã•¡ã•³ã•³ã€ã•ã•£ã•ã•®çµ•æž•œ•§ã•ã•ã€‚

　è¬•è¨¼ç„¡ç•šLANã•ã•ã•†ã•ã•ã•§ã•ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£ãƒ¬ãƒ™ãƒ«ã•Œä•Šã•Œã•£ã•Ÿã•ŸãŸã•ã€ã•ªã•ã€‚
　DD-WRTã•ä»•æƒ³ã‚µãƒ¼ãƒ•ã•ã•ã•†ã•¤ãƒ³ãƒ•ãƒ©ã•§ã•è‡•å®…ã•å®‰ä¾•ã•«é«˜ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£ã•ªç„¡ç•šLANã•Œçµ•ã•ã€ã•®ã•¯ç•´ æ™´ã‚‰ã•—ã„ã€‚

　freeradiusã€ä»–ã•«ã„æ´•ç"¨ã•®ç"¨é€"ã•¯ã€ã•®ã•§•

　ãƒ»ServersMan@VPSã‚’ãƒ•ãƒƒã‚¯ã‚¢ãƒƒãƒ—RADIUSã‚µãƒ¼ãƒ•åŒ–
　ãƒ»OpenVPNã•®RADIUSè¬•è¨¼å°Žå…¥
　ãƒ»MySQLï¼‹OpenLDAPè¬•è¨¼åŒ–

　ã•ã•Ÿã‚Šã‚’è¿´ã€…ã„ã•£ã•¦ã•¿ã‚‹ã•¤ã€ã•Šã€‚