WPA2ã,¨ãƒ³ã,¿ãƒ¼ãƒ—ãƒ©ã,¤ã,ºï¼ˆEAP-PEAPï¼‰ã•«ã,ˆã,‹è¹•è¨¼ç„¡ç·šLANåŒ–

Category : ã,µãƒ¼ãƒ•ç®¡ç•†æ—¥è¨˜
Published by M-naka on 2012/2/4

freeradius2ã•§EAP-PEAPã•ªè¹•è¨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,Šã€•WPA2ã,¨ãƒ³ã,¿ãƒ¼ãƒ—ãƒ©ã,¤ã,ºã•Œä½¿ã•ˆã,‹ã,ˆã•†ã•«ã•ªã•£ã•¦ã•„ã,‹ã€,ã•,ã•¨ã•¯RADIUSã,µãƒ¼ãƒ•ã•¨ç„¶ã,‹ã•¹ã••è¨-å®šã•Œä½¿ã•ˆã,‹ã€,ã•§ã€•ãƒ•ãƒ£ãƒ¬ãƒ³ã,¸ã•—ã•¦ã•¿ã•Ÿã€,

ï¼‘ï¼Žè¹•è¨¼æ–¹å¼•ã•®é•¸å®š

ã€€EAPã•«ã•¯ã•„ã••ã•¤ã•‹ç¨®é¡žã•Œã•,ã•£ã•¦ã€•ã,»ã,-ãƒ¥ãƒªãƒ†ã,£ã•Œå¼·åŠ›ã•ªã,,ã•®ã•§ã•¯EAP-TLSã€•EAP-PEAPã€•EAP-TTLSã• ã€,
EAP-TLSï¼šã,µãƒ¼ãƒ•ãƒ»ã,¯ãƒ©ã,¤ã,¢ãƒ³ãƒˆç›¸ä°'ã•§é›»å-•è¨¼æ˜Žæ›¸ã•§è¹•è¨¼ã•™ã,‹ã€,ã,»ã,-ãƒ¥ãƒªãƒ†ã,£å¼·å°¦ã•¯æœ€å¼·ã,¯ãƒ©ã,¹ã€,
EAP-TTLSï¼šã,¯ãƒ©ã,¤ã,¢ãƒ³ãƒˆè¨¼æ˜Žæ›¸ã•¯ä¸•è¦•ã•ªã•Œã,‰EAP-TLSã•¨å•Œç-‰ã•®ã,»ã,-ãƒ¥ãƒªãƒ†ã,£å¼·å°¦ã€,ã•Ÿã• Windowsæ¨™æº–ã,µãƒ—ãƒªã,«ãƒ³ãƒˆã•§ã•¯é•žå¯¾å¿œã•§ãˆ¥é€"ã,µãƒ—ãƒªã,«ãƒ³ãƒˆã•Œå¿…è¦•ã€,
EAP-PEAPï¼šã,»ã,-ãƒ¥ãƒªãƒ†ã,£å¼·å°¦ã•¯EAP-TLS/TTLSã•«è-²ã,‹ã•Œã€•Windowsæ¨™æº–ã,µãƒ—ãƒªã,«ãƒ³ãƒˆã•§å¯¾ã¿œã€•ã,µãƒ¼ãƒ•è¹•è¨¼ã•¯é›»å-•è¨¼æ˜Žæ›¸ã€•ã,¯ãƒ©ã,¤ã,¢ãƒ³ãƒˆè¹•è¨¼ã•¯ID ã•¨ãƒ'ã,¹ãƒ¯ãƒ¼ãƒ‰ã€,
ã•¨ã•ªã•£ã•¦ã•„ã,‹ã€,åˆ¥é€"ã,µãƒ—ãƒªã,«ãƒ³ãƒˆã•Œå¿…è¦•ã•ªæ™‚,ç‚¹ã•§EAP-TTLSã•¯å•´ä¸‹ï¼ˆæ±Žç"¨æ€§é‡•è¦–ï¼‰ã€,EAP-TLSã•¯ã,¯ãƒ©ã,¤ã,¢ãƒ³ãƒˆã•«é›»å-•è¨¼æ˜Žæ›¸ã,'ç¹•ã•£è¾¼ã•¾ã••ã,Œã,‹ã•®ã•Œæ€§ã•«å•ˆã,•ã•ª ã•„ã€,æ±Žç"¨æ€§ã•Œé«˜ã••ã€•ã,µãƒ¼ãƒ•å•´ã•®é›»å-•è¨¼æ˜Žæ›¸ã• ã•'ã•,ã,Œã•°OKã•ªEAP-PEAPã•§è¡Œã••ã•"ã•¨ã•«ã•—ã•Ÿã€,ã•¡ã•ªã•¿ã•«ã•†ã•¡ã•®ä¼šç¤¾ã•®ç¤¾å†…ç„¡ç·šLANã,,EAP-PEAPã• ã€,

ï¼'ï¼Žé›»å-•è¨¼æ˜Žæ›¸ã•®å•–å¾—

ã€€RADIUSã,µãƒ¼ãƒ•ã,'å¤–å•'ã••ã•®gungnir.mythril.ne.jpã•§é•‹ç"¨ã•™ã,‹ã•®ã•¯ãƒªã,¹ã,¯ã•Œã•,ã,‹ã•®ã•§ã€•å†…å•'ã••ã•®mjolnir.mythril.ne.jpã•§é•‹ç"¨ã•™ã,‹ã€,ã•"ã•®é–¢ä¿,ã•§ã€•é›»å-•è¨¼æ˜Žæ›¸ã•¯ www.mythril.ne.jp
ã•®ã,,ã•®ã•®æµ•ç"¨ã•Œã•§ã••ã•ªã•„ã€,ä»Šæ›´è‡ªå·±ç½²å••è¨¼æ˜Žæ›¸ï¼ˆã•„ã,•ã,†ã,‹ã€Žã,ªãƒ¬ã,ªãƒ¬è¨¼æ˜Žæ›¸ã€•ï¼‰ã•§æ§‹ç¯‰ã•™ã,‹ã•®ã•¯è«–å¤–ã• ã€,è¶…å††é«˜ã•ªã•®ã•§ã,,ã•†ä¸€æžšè²·ã•†ã•‹â€¦â€¦ã•¨æ€•ã•£ã•Ÿã•®ã• ã•Œã€•èª¿ã•¹ã•¦ã•¿ã,‹ã•¨
ã€€StartSSL
ã•§ç„¡æ–™å•–å¾—ã•§ã••ã,‹ã•"ã•¨ã•Œåˆ¤æ˜Žã€,ã•"ã,Œã•§è¡Œã••ã•"ã•¨ã•«ã•—ã•Ÿã€,å•–å¾—æ‰‹é †ã•«ã•¤ã•„ã•¦ã•¯æœ¬è«–ã•‹ã,‰å¤–ã,Œã,‹ã•®ã•§çœ•ç•¥ã€,FQDNã,'secgw.mythril.ne.jpã•«ã•—ã•¦å•–å¾—ã€,ä¸-é–"è¨¼æ˜Žæ›¸ã•Œå¿…è¦•ã•ªã•"ã•¨ã,'ã•Šå¿˜ã,Œã•ªã••ã€,

ï¼“ï¼Žfreeradius2ã•®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-—åˆ—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€€ã€€= xxxxxxxxxxxxxxxxx
ã€€ã€€ã€€>ã€€ã€€ã€€ ã€€shortnameã€€ã€€ã€€ = xxxxxxxxxxxxxxxxx
ã€€ã€€ã€€> }

ã€€ï¼“ï¼‰users
ã€€ã€€ã€€radiusçš„ã•«ã•¯UNIXãƒ¦ãƒ¼ã,¶ï¼^/etc/passewdï¼‰ã„MySQLï¼‹OpenLDAPã•§ã•®èª•è¨¼ã•§ã„è¡Œã•‘ã,‹ã••ã•†ã• ã•Œã€•ä»Šå›žã•¯ãƒ©ã,¤ãƒˆã•«radiusç"¨ã•®ãƒ¦ãƒ¼ã,¶ãƒ•ã,¡ã,¤ãƒ«ã•§ç®¡ç•†ã•™ã,‹ã•“ã•¨ã•«ã•—ã•Ÿã€,ä»¥ä¸‹ã,'è¿½è¨˜ã€,
ã€€ã€€ã€€>ã€€ Cleartext-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€€**ä»Šå›žã•®å±±å ´ã€,**
ã€€ã€€ã€€ã€€ãƒ»default_eap_typeã•¯peapã•«ã•™ã,‹ã€,
ã€€ã€€ã€€ã€€ãƒ»PrivateKeyã•¨Certificateã•¯ãƒ•ãƒ„ãƒ¼ã•«æŒ‡å®šã•™ã,Œã•°OKã€,/etc/pki/tlsä»¥ä¸‹ã•¸ã•®ã,·ãƒ³ãƒœãƒªãƒƒã,¯ãƒªãƒ³ã,¯ã•§ã„å•¯ã€,
ã€€ã€€ã€€ã€€ãƒ»StartSSLã•¯ä¸-é–“è¨¼æ˜Žæ›¸å¿…é 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€€cat CA.pem ä¸-é–“è¨¼æ˜Žæ›¸.pem > çµ•å•ˆã•—ã•Ÿè¨¼æ˜Žæ›¸.pem
ã€€ã€€ã€€ã€€ã€€ã•§ã€•å•˜ä¸€ãƒ•ã,¡ã,¤ãƒ«åŒ–ã•™ã,‹ã€,StartSSLã•®ãƒ«ãƒˆè¨¼æ˜Žæ›¸ã€•ä¸-é–“è¨¼æ˜Žæ›¸ã•¯ã•“ã•“ã€,pemå½¢å¼•ã•§ã€,
ã€€ã€€ã€€ã€€ãƒ»randomãƒ•ã,¡ã,¤ãƒ«ã•¯/dev/urandamã,'æŒ‡å®šã•™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•‹ã,‰ä½œã,Šã•“ã,“ã• randomãƒ•ã,¡ã,¤ãƒ«ã,'è¨-å®šã•§æƒ³å®šã•—ã•¦ã•„ã,‹ã•Œã€•/dev/randomã•¨/dev/urandomã•‹ã,‰ä½œã,Šã•“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‰è‡µå‹•ã••ã•›ã€•ã,¯ãƒ©ã,¤ã,¢ãƒ³ãƒˆã•‹ã,‰ã•®æŽ¥ç¶šã,'è©¦ã•¿ã,‹ã€,

ï¼”ï¼‰Windows7ã•§è¨-å®šã€•æŽ¥ç¶š

ã€€Windows7å•´ã•®è¨-å®šã•¯ã•“ã,“ã•ªæ„Ÿã•˜ã€,

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€•èª•è¨¼ã•®ç¨®é¡žã•¯ã€ŒMicrosoft:ä¿•è-·ã••ã,Œã•ŸEAPï¼ˆPEAPï¼‰ã€•ã,'ã••ã,Œã•žã,Œé•¸æŠžã€,çµ,ã,•ã•£ã•Ÿã,‰ã€Œè©³ç´°è¨-å®šã€•ã,'æŠ¼ã•™ã€,

ã€€èª•è¨¼ãƒ¢ãƒ¼ãƒ‰ã•¯ã€Œãƒ¦ãƒ¼ã,¶ãƒ¼èª•è¨¼ã€•ã•§æŒ‡å®šã€,ä»Šå›žã•¯Windowsãƒ¦ãƒ¼ã,¶ãƒ¼/ãƒ'ã,¹ãƒ¯ãƒ¼ãƒ‰ã•§èª•è¨¼ã•™ã,‹ä»•çµ„ã•¿ã•«ã•—ã•¦ã•,ã,‹ã•®ã•§ã€•ã,·ãƒ³ã,°ãƒ«ã,µã,¤ãƒ³ã,ªãƒ³ã,'æœ‰åŠ¹ã•«ã•—ã•¦ã•Šã••ã€,å¿…é ˆã•§ã•¯ã•ªã•„ã•Œç„¡ç·šLANã•¸ã•®æŽ¥ç¶šã•ŒWindowsãƒ-ã,°ã,ªãƒ³ã•¨ã,·ãƒ¼ãƒ ãƒ¬ã,¹ã•«ã•ªã,‹ã€,

ã€€RADIUSã,µãƒ¼ãƒ•ã•®èª•è¨¼ã,'ã•™ã,‹ã•®ã•§è¨-å®šã•¯ã•“ã,“ã•ªæ„Ÿã•˜ã€,CAã•¯StartSSLã•®ãƒ«ãƒ¼ãƒˆã•§ã•,ã,‹StartComã•«ãƒ•ã,§ãƒƒã,¯ã,'å…¥ã,Œã,‹ã€,èª•è¨¼æ–¹å¼•ã•¯EAP-MSCHAPv2ã,'é•¸æŠžã€,çµ,ã,•ã•£ã•Ÿã,‰ã€Œæ§‹æˆ•ã€•ã,'æŠ¼ã•™ã€,

ã€€ãƒ‡ãƒ•ã,©ãƒ«ãƒˆã• ã•¨ã•“ã•“ã•«ãƒ•ã,§ãƒƒã,¯ã•Œå…¥ã•£ã•¦ã•„ã,‹ã•®ã•§å¤–ã•™ã€,ã•“ã,Œã,'ãƒ•ã,§ãƒƒã,¯ã,'å…¥ã,Œã•Ÿã•¾ã•¾ã•«ã•—ã•¦ã•Šã••ã•¨ã€•PCå••ãƒ¦ãƒ¼ã,¶ãƒ¼å••ã•§RADIUSèª•è¨¼ã•Œå®Ÿè¡Œã••ã,Œã•¦ã•—ã•¾ã•„ã€•ã•†ã•¡ã•®ç'°å¢ƒã•§ã•¯ä¸Šæ‰‹ã••ã•ª è¨-å®šã•«ä¾•å-˜ã•™ã,‹ã,ˆã•†ã• ã•Œã€•å‰•æ®µã•®ã,·ãƒ³ã,°ãƒ«ã,µã,¤ãƒ³ã,ªãƒ³ã,'è¡Œã•†ã•“ã•¨ã,„ã•,ã,Šã€•ã•“ã•“ã•¯ä¸•è¦•ã€,

ã€€ã•“ã•“ã•¾ã•§ã,„ã•£ã•¦ã€•ã,ˆã•†ã,„ã••æˆ•åŠŸã€,
ã€€ã••ã••ã•£ã•¨æ›¸ã•„ã•¦ã•„ã,‹ã•Œã€•å¤§ä½“ãºŒãƒ¶æœˆã••ã,‰ã•„ã•¡ã•³ã•¡ã•³ã,„ã•£ã•¦ã•®çµ•æžœã•§ã•,ã,‹ã€,

ã€€èª•è¨¼ç„¡ç·šLANã•¨ã•„ã•†ã•“ã•¨ã•§ã€•ã,»ã,-ãƒ¥ãƒªãƒ†ã,£ãƒ¬ãƒ™ãƒ«ã•Œä¸Šã•Œã•£ã•Ÿã•“ã•¨ã•«ã•ªã,‹ã€,
ã€€DD-WRTã•¨ä»®æƒ³ã,µãƒ¼ãƒ•ã•¨ã•„ã•†ã,¤ãƒ³ãƒ•ãƒ©ã•§ã€•è‡ªå®…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€,

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

ã€€ãƒ»ServersMan@VPSã,'ãƒ•ãƒƒã,¯ã,¢ãƒƒãƒ—RADIUSã,µãƒ¼ãƒ•åŒ–
ã€€ãƒ»OpenVPNã•®RADIUSèª•è¨¼å°Žå…¥
ã€€ãƒ»MySQLï¼‹OpenLDAPèª•è¨¼åŒ–

ã•,ã•Ÿã,Šã,'è¿½ã€…ã„ã•£ã•¦ã•¿ã,‹ã•¤ã„,ã,Šã€,