ServersMan @ VPSã•¨ã•®OpenVPNæŽ¥ç¶š

Category : ã‚µãƒ¼ãƒ•ç®¡ç†æ—¥è¨˜
Published by M-naka **on 2011/7/17**

ServersMan@VPSã•§tunãƒ‡ãƒ•ã‚¤ã‚Œä½¿ã•ˆã•ªã•ã•£ã•Ÿã•®ã•Œ

ã€æ š«ã••å‰•ã•®æ©Ÿè½å¼•å€ã•è¨£¶ã€OpenVPNã•Œä½¿ã•ˆã‚ˆã†ã•ªã•£ã•Ÿã€ã•
ã‚Œã•§ServersMan@VPSã•®ä»®æ³ã‚µãƒ¼ãƒ•ã•¨ã‚™æ™VPNã•§ç¹‹ã•ã‚‰ã•Œã•"ã•¨ã•ã•ªã‚ã€‚

ServersMan@VPS
ã•ç¨¼å‹•ä¸ã•®ä»®æ³ã‚µãƒ¼ãƒ•ã€Gramr.mythril.jpã€å•´ã'192.168.2.0/24ã•®ã‚»ã‚°ãƒ¡ãƒ³ãƒˆã•
¨ã•—ã€è‡ªå®…å•´ã•®192.168.1.0/24ã•¨ã•é–"ã'OpenVPNãƒ«ãƒ¼ãƒ†ã‚£ãƒ³ã‚°ãƒ¢ãƒ¼ãƒ‰ã•§LA
Né–"æŽ¥ç¶šVPNã‚’æ§‹ç¯‰ã•—ã•Ÿã€è‡ªå®…å•´ã•®VPNã‚²ãƒ¼ãƒ•ã‚¦ã‚¤ã•å¯å®¶ã•¨ã•®LANé
–"æŽ¥ç¶šVPNã•«ä½¿ã•£ã•¦ã•"ã‚‹Mjolnir.mythril.ne.jpã‚’ä½¿ã•†ã€‚

ã"ã•£ã•Ÿã•"ã•¨ã•¯ä»¥ä¸‹ã€‚

1.ServersMan@VPSå•´ã•§ä»®æƒ³NICã‚’è¿½åŠ ã•™ã‚‹

ã€/etc/sysconfig/network-scripts/ã•«ã•ã‚‹ifcfg-venet0:0ã•§ã‚ƒ-ãƒ¼ãƒ•ãƒ«IPã‚¢ãƒ‰ãƒ¬ã‚¹ã•Œè¨å
®šã••ã‚Œã•¦ã•¦ã•ã‚‹ã€ã•ã‚Œã‚'ã‚³ãƒ"ãƒ¼ã•—ä»®æƒ³NICã•§ã•ã‚‹ifcfg-venet0:1ã‚'ä½œã‚Šã€ã••ã••ã€
ã‚Œã'æ›¸ã••æ›ã•ˆ¦venet0:1ã•«192.168.2.0/24ã•IPã‚¢ãƒ‰ãƒ¬ã‚¹ã‚'å‰²ã‚Šå½"ã•¦ã‚‹ã€ä»Šå›žã•19
2.168.2.1ã•¨ã•—ã•Ÿã€ã••ã•®å¾Œ/etc/init.d/networkã‚'å†•èµ·å•‹ã•™ã‚Œã•°ã€ä»®æƒ³NICã•Œ192.1
68.2.1/24ã•§èµ·å•‹ã•™ã‚‹ã€‚

2.Mjolnir.mythril.ne.jpã•§OpenVPNè¨å®šã•¨iptablesè¨å®šã‚’è¿½åŠ ã•™ã‚‹

ã€ã‚ã•ã‚‰ã‚¨Mjolnir.mythril.ne.jpï¼ˆ192.168.1.165/24ï¼‰ã•§ã•¯è‡ªå®…â^å®¶ã•®é–"ã•®LANé–"
æŽ¥ç¶šVPNã•Œèµ·å•‹ã•—ã•¦ã•ã‚‹ã€ä¸Šå›žã•"ã•Œã‚'æ¡å¼µã•™ã‚‹å½¢ã•§ã‚³ãƒ³ãƒ•ã‚£ã‚°ã‚’è¿
½åŠ ã•—ã•Ÿã€å…¬½"çš"ã•«ã•¯

â—†OpenVPN
ã€ã‚³ãƒ³ãƒ•ã‚£ã‚°ãƒ•ã‚¡ã¤ãƒ«ã•è‡ªå®…â^å®¶ã•®é–"ç"¨ã‚'openvpn00.confã€è‡ªå®…â^Gramrç""
ã‚'openvpn01.confã•¨2ã•¤ã•ã€ã•¾ã•Ÿäºˆå‰•å…±æ‰ˆé•µãƒ•ã‚¡ã¤ãƒ«ã‚'ã€œ00.keyã•¨ã€œ01.ke
yã•¨å¥ã€…ã•«ã•—ã•Ÿã€openvpn00.confã•"openvpn01.confã•¯æŽ¥ç¶šå…^ã€UDPãƒ•ãƒ¼ãƒˆã€ro
uteè¨å®šã•Œç•°ã•ªã‚‹ã••ã‚‰ã•§åŸºæœ¬è¨å®šã•¯å•Œä¸€ã•§ã•ã‚‹ã€OpenVPNã•¯ã‚³ãƒ³ãƒ•ã‚£ã‚°
ãƒ•ã‚¡ã¤ãƒ«ã•æ ¼ç•ãƒ‡ã‚£ãƒ¬ã‚¯ãƒˆãƒªã•«ã‚ã‚‹*.confã•®æ•°ã• ã•‘ã‚µãƒ¼ãƒ"ã‚¹èµ·å•‹ã•™ã‚‹ã•®ã
•§ã•ã•"ã€ã•§èµ·å®…â^å®¶ã•®é–"ç""ã•¨è‡ªå®…â^Gramrç""ã•Œä¸¡æ–¹èµ·å•‹ã•™ã‚‹ã•ã•†ã•«ã•ªã
‚ã€‚

â—†iptables
ã€æ—¢å˜è¨å®šã•æ¡¼ã•,IPmasqueradeè¨å®šã•è‡ªå®…â^Gramrç""VPNã•§ä½¿ã•†UDPãƒ
•ãƒ¼ãƒˆã•®INPUTãƒ•ã‚£ã‚¤ãƒ³ã‚'å¢—ã•—ã•—ã•Ÿã• ã•‘ã€‚

ã€ã•ã‚Œã•§Mjolnir.mythril.ne.jpã•¯3ã•¤ã•®LANï¼ˆè‡ªå®…LANã€å¯å®¶LANã€
ServersMan@VPS

ï¼‰æ•Ÿã•-ã‹VPNã'å—ã'æŒ•ã•¤VPN-Hubã®å½¹å‰²ã'è² ã†ã•"ã•ã•«ã•ªã‹ã€,

3.Gramr.mythril.jpã•§OpenVPNè¨å®šã'è¡Œã†

ã€€Mjolnir.mythril.ne.jpã•¨å¯¾å•'ã•«ã•ªã‹OpenVPNè¨å®šã'Gramr.mythril.jpã•«è¡Œã†ã€,åŸ°æœ¬ã•¯Mjolnir.mythril.ne.jpã•«ä»•è¼ƒã"ã• openvpn01.confã®å¯¾å•'ç‰ˆã€,ä»Šå›žã•æŽ¥ç¶šã‚¹ã,-ãƒ¼ãƒ ã•¯LANé–"æŽ¥ç¶šVPNã• ã•Œã€•192.168.2.0/24å€•ã•¤å•¾ã‚ŠServersMan@VPS å•'ã•¯Gramræœ¬ä½"ã•®ã•¿ç¹'ã•Œã€,Œã•°è‰•ã•'ã•Ÿã•ã€Gramrå•'ã•§ã®iptablesè¨å®šï¼ˆIPmasquerade ã•"INPUTãƒ•ã‚§ã‚¤ãƒ³ã•®è¿½åŠ ï¼‰ã•¯ä¸•å‰•ã•§ã"æ§‹ã•ã•ªã„ã€,

4.è‡ªå®…LANãƒ«ãƒ¼ã‚¿ã®è¨èº«½åŠ

ã€€ä½¿ç"¨ã•™ã‹udpãƒ•ãƒ¼ãƒˆã‚'ã‚ªãƒ¼ãƒ—ãƒ³ã•Mjolnir.mythril.ne.jpã•«ãƒ•ãƒ¼ãƒˆãƒ•ã,©ãƒ¯ãƒ¼ãƒ‰ã•™ã‹è¨å®šã•ã€•192.168.2.0/24å®›ãƒ'ã,±ãƒƒãƒˆã‚'Mjolnir.mythril.jpã•«å•'ã•'ã‹é™™çš„ãƒ«ãƒ¼ãƒˆã,£ãƒ³ã‚°è¨å®šã'ä»•è¼ƒã‚‹ã€,ã•"ã,Œã,æ—¢å-˜è¨ã•®æ¡å¼µã€,

5.DNSç™»éŒ²

ã€€192.168.2.1ã'Gramr.mythril.ne.jpã•§æ-£å¼•ã••ã•§ã••ã‚‹ã,ˆã•†ã•«DNSç™»éŒ²ã'è¡Œã£ã•Ÿã€,ã•"ã,Œã•§LANã•‹ã‚‰ã•¯Gramr.mythril.ne.jpã•¸ã•®ã,¢ã,¯ã,»ã,¹ã•ŒVPNçµŒç"±ã•§è¡Œã•ã,Œã‚‹ã,ˆã•†ã•«ã•ªã‹ã€,

ã•"ã,Œã•§çµ,äº†ã•,è‡ªå®…LANå•´ã•‹ã‚‰ã•¯ã•¤ãƒ³ã,¿ãƒ¼ãƒ•ã‚§ãƒ¼ã,Šã•®ã,µãƒ¼ãƒ•ã•§ã,‹Gramr.mythril.jpã•Œã€•ã€Œéš£ã•®LANã,»ã,°ãƒ¡ãƒ³ãƒˆã•«ã,ã,ã,µãƒ¼ãƒ•ã€•ã•§ã,‹Gramr.mythril.ne.jpã•¨ã•—ã•¦è¦‹ã•ˆã‚‹ã€,192.168.2.0/24ã•ç"¼å•ã•—ã¦ã,ã‚fžã,·ãƒ³ã•¯Gramr.mythril.jp1å•°ã• ã•'ã• ã•Œã€•è¦‹ã•¯ã‚²ãƒ¼ã‚,¦ã•§ã‚¤ãƒžã,·ãƒ³ã•®ã,¿ç¹'ã•Œã•£ã•¦ã„ã,‹Š¶æ…•ã•ªã®ã•§ã€LANé–"æŽ¥ç¶šVPNã'ä½¿ã†ä¸Šã•®å••é¡Œã,ªªã„ã€,

ã•ã•¨ã€ServersMan@VPS ã•§ã®SSHãƒ•ãƒ¼ãƒˆã•¯ãƒ‡ãƒ•ã‚©ãƒ«ãƒˆ3843/tcpã•«ã•ªã£ã•¦ã„ã,‹ã•®ã•§ã€æŽ¥ç¶šã•®éf½åº°ãƒ•ãƒ¼ãƒˆã'å…¥åŠ›ã•—ã•ªã•ã€ã•°ã„ã•ã‚‹ã•®ã•Œé¢å€•ã• ã•£ã•Ÿã€,VPNçµŒç"±ã•®ã•ã•®ã•¿ã€22/tcpã•§ã•®æŽ¥ç¶šã•Œã•§ã•ã‚‹ã,ˆã•†ã•«ã•—ã•Ÿã€,

ã€€â€ sshd_configã•«ã€ŒPort 22ã€•ã'è¿½åŠ ã€,
ã€€â€ iptablesã•§22/tcpã•®æŽ¥ç¶šã•¯VPNçµŒç"±ã€•ã•¤ã•¾ã,Šãƒ-ãƒ¼ã,«ãƒ«ã,¢ãƒ‰ãƒ¬ã,¹ã•‹ã,‰ã•®ã•¿ACCEPTã•™ã‹ã,ˆã•†ã•«
ã€€ã€INPUTãƒ•ã‚§ã‚¤ãƒ³ã'è¿½æ•ˆ•ã€,

ãƒ‡ãƒ•ã,©ãƒ«ãƒˆã•®3843/tcpã'22/tcpã•«å¤‰æ›´ã•—ã•ã€è‰•ã•ã•®ã• ã•Œã€åŸ°æœ¬çš„ã•«ãƒ-ãƒ¼ã,«ãƒ«ã•ã,‰tcp/22ã•«SSHæŽ¥ç¶šã•§ã••ã,Œã•°è‰•ã••ã•ã•¾ã•Ÿ3843/tcpã•«ã•ªã£ã•¦ã„ã,‹ã•®ã•¯æ"»æ'f対å¾—ã•ªã•®ã•§ã€å¤–å•'ã••ã•«ã•¯3843/tcpã€å†…å•'ã••ã•«ã•¯22/tcpã•"ã,ã•†ã†ã•"ã•ã•§è¦‹Œã••ã•'ã•"ã•«ã•—ã•Ÿã€,

å¸¸æ™,VPNæŽ¥ç¶šã•Œã•§ã••ã•¦ã„ã,‹ã•¦â€¦•ã•¦ã•ªã‚‰ã•¯ã,•ã•"ã•ã•"ã•ã•ç""é€"ã•Œåºfã•Œã,ã€,è‡ªå•Œæ™ã,ªãƒ³ãƒ©ã,¤ãƒ³ã,¹ãƒ'ãƒ¬ãƒ¼ã,ã€•ã,ªãƒ«ãƒ•ã,ºãƒ³ãƒ©ã,¤ãƒ³ãƒ•ã,ãƒ•ã•ãƒ¯ã€Webã,µãƒ¼ãƒ•/Mailã,µãƒ¼ãƒ•ã•®å†—é•·æ€§å¯¾å¿œ—ã€…å¶ã€…ç-‰ã€…ã€å¤æã•Œåºfã•Œã,Šã•"ã••ã•ªæ„Ÿã•ã€,