



FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

SEMESTER 1 2017/18

WORKSHOP 2 (BITU 3923)

BITC&BITZ

FINAL REPORT

PROJECT TITLE: DOMAIN NAME SERVICE (DNS)

GROUP NUMBER: 1

PREPARED BY:

TAN SEOW WEI	B031510091
MOHD FITRI AMRI BIN JAAFER	B031510035
SITI ZULAIHA BINTI KHASNAN	B031510018
NOOR AINI BINTI SHAHINE	B031510191
NUR SYAHIRAH BINTI MOHAMAD RAFEE	B031510220
CHAI ROU YIH	B031510137
MOHAMAD ASHRAF FIRDAUS BIN MAT ZAIN	B031510163
MUHAMMAD SYUKUR BIN SHARIFF	B031310460

PREPARED FOR:

SUPERVISOR: DR. MOHD FAIZAL ABDULLAH (M)  
DR. WAHIDAH MD SHAH (C)

EVALUATOR: DR. NAZRULAZHAR BAHAM

## **ACKNOWLEDGEMENT**

First and foremost, we would like to thank our supervisor of this project, Prof Madya Dr Faizal Bin Abdollah for his valuable guidance and advice. He inspired us greatly to work in this project. His willingness to motivate us contributed tremendously to our project. We also would like to thank him for showing us some examples that are related to the services in our project which helped us understand our project better. This helped us complete our project on time. We would also like to thank our evaluator for this workshop, Dr Nazrulazhar Bahaman for taking the time to evaluate us. This evaluation gave us a deeper understanding of our services and network infrastructure.

Besides that, we would like to thank the authority of Technical Malaysia University (UTeM) for providing us with a good environment and facilities to complete this project. Finally, an honorable mention goes to our families and friends for their understandings and supports on us in completing this project. With the help of the particulars that mentioned above, we completed our project successfully on time.

## **ABSTRACT**

The main objectives for this Workshop 2 are designing a secured network infrastructure by using the available equipment, implementing designated secured network services and configuration into the network infrastructure, installing and integrating network infrastructure, services and configuration based on the requirement of secured network environment, and managing the secured network infrastructure, services and configuration. Our group consists of 8 students, 5 students from BITC and 3 students from BITZ. Each of us is required to configure both networking and security services rather than just focus on our own major course's services. This had provided us a great opportunity to understand about other course's services well which may be useful in the future. A project manager has been assigned from the group to lead the group members throughout the workshop. We have been provided with the equipment which are three servers, 1 Cisco 1941 router, one Cisco 2960 manageable switch, 15 meters UTP cable, 12 pieces of RJ-45, one access-point and one set crimping tool. The operating system used in servers are Windows Server 2008 R2 and Ubuntu 16.04. After setting up all the network configuration, infrastructure and services, several tests will be done to ensure they are working properly. At the end of workshop II, we are required to demonstrate our work to supervisors and evaluator. We are also required to produce poster and video for exhibition based on our title which is Domain Name Server.

## **ABSTRAK**

Objektif utama untuk Bengkel 2 adalah mereka bentuk infrastruktur rangkaian yang selamat dengan menggunakan peralatan yang sedia ada, menggunakan servis dan konfigurasi reka bentuk rangkaian selamat ke dalam infrastruktur rangkaian. memasang dan mengintegrasikan infrastruktur rangkaian, servis dan konfigurasi berdasarkan keperluan persekitaran rangkaian yang selamat dan mengurus infrastruktur rangkaian, servis dan konfigurasi. Kumpulan kami terdiri daripada 8 orang pelajar, 5 orang pelajar dari BITC dan 3 orang pelajar dari BITZ. Setiap ahli kumpulan dikehendaki konfigurasi kedua-dua jenis servis iaitu servis rangkaian dan servis keselamatan. Hal ini telah membekalkan kesempatan kepada kami untuk memahami servis kursus lain tanpa hanya fokus servis kursus sendiri. Seorang dari ahli kumpulan telah dilantik menjadi pengurus projek untuk Bengkel 2 ini. Kami dibekalkan dengan peralatan-peralatan seperti server, 1 Cisco 1941 router, 1 Cisco 2960 switch, 15 meter wayar UTP, 12 unit RJ-45, satu akses point dan satu set alat krimping. Sistem operasi yang digunakan adalah Windows Server 2008 R2 dan Ubuntu 16.04. Selepas menyediakan semua konfigurasi rangkaian, infrastruktur dan servis-servis, beberapa ujian akan dijalankan untuk memastikan ia berjalan lancar. Pada akhir Bengkel 2 ini, kami hendaklah menunjuk dan menjalankan servis-servis kami kepada penyelia dan juga penilai. Kami juga hendaklah menghasilkan poster dan video untuk pameran berdasarkan tajuk kami iaitu Domain Name Server (DNS).

## TABLE OF CONTENT

### Contents

ACKNOWLEDGEMENT .....	i
ABSTRACT .....	ii
ABSTRAK .....	iii
LIST OF FIGURES .....	xi
CHAPTER 1: INTRODUCTION .....	1
1.1 INTRODUCTION.....	1
1.2 OBJECTIVE.....	2
1.3 PROJECT PLAN .....	3
1.4 CONCLUSION.....	4
CHAPTER 2: PROJECT REQUIREMENT.....	5
2.1 INTRODUCTION .....	5
2.2 TYPES OF OPERATING SYSTEM.....	5
2.3 OPERATING SYSTEM BACKGROUND .....	5
2.3.1 WINDOWS SERVER 2008 R2.....	5
2.3.2 UBUNTU 16.04.....	6
2.4 OPERATING SYSTEM JUSTIFICATION .....	6
2.4.1 WINDOWS SRVER 2008 R2 .....	6
2.4.2 UBUNTU 16.04.....	7
2.5 HARDWARE REQUIREMENT.....	8
2.6 HARDWARE JUSTIFICATION .....	8
2.6.1 WINDOWS SERVER .....	8
2.6.2 UBUNTU SERVER.....	9
2.6.3 ROUTER.....	10
2.6.4 SWITCH .....	11
2.6.5 UTP CABLE.....	12

2.6.6 RJ-45 .....	12
2.6.7 CRIMPING TOOL .....	13
2.6.8 LINKSYS ACCESS-POINT (WRT1900AC-ME).....	13
2.7 CONCLUSION.....	14
CHAPTER 3: DESIGN.....	15
3.1 INTRODUCTION .....	15
3.3 PHYSICAL DESIGN.....	20
3.4 LOGICAL DESIGN (INCLUDING SECURITY DESIGN).....	21
3.5 CONCLUSION.....	22
CHAPTER 4: SERVICES .....	23
4.1 INTRODUCTION.....	23
4.2 LIST OF SERVICES .....	23
4.3 BRIEF OVERVIEW FOR SERVICES .....	25
4.3.1 DOMAIN NAME SERVER (DNS) .....	25
4.3.2 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP).....	25
4.3.3 ROUTING & NETWORK ADDRESS TRANSLATION (NAT) .....	26
4.3.4 VIRTUAL LOCAL AREA NETWORK (VLAN) .....	28
4.3.5 IPV6 TRANSITION MECHANISM.....	28
4.3.6 WEB, SECURE SOCKETS LAYER (SSL) & VIRTUAL HOSITNG .....	29
4.3.7 IPV6 WEB .....	30
4.3.8 SECURE FILE TRANSFER PROTOCOL (SFTP) .....	30
4.3.9 SAMBA .....	30
4.3.10 PROXY SERVER.....	31
4.3.11 RADIUS SERVER FOR NETWORK ACCOUNTING .....	32
4.3.12 LINUX EMAIL SERVER .....	33
4.3.13 NETWORK MANAGEMENT SYSTEM.....	33
4.3.14 ACCESS CONTROL LIST (ACL) .....	34

4.3.15 SECURITY HARDENING .....	34
4.3.16 AUTHENTICATION USING RADIUS SERVER.....	35
4.3.17 USER AUTHENTICATION AND AUTHORIZATION .....	35
4.3.18 FIREWALL FOR ROUTER.....	36
4.3.19 REMOTE LOGIN USING SSH .....	36
4.3.20 HARDENING LINUX SERVER.....	36
4.3.21 HARDENING WINDOWS SERVER.....	37
4.3.22 HARDENING WEB SERVER.....	37
4.3.23 AUTHENTICATION USER BY INTEGRATING ACTIVE DIRECTORY WITH LINUX .....	38
4.3.24 INTRUSION DETECTION SYSTEM (PORT MIRROR) .....	39
4.3.25 IPSEC BETWEEN SERVER AND USER .....	40
4.3.26 SAMBA SECURITY SERVICES .....	40
4.3.27 PORT SECURITY .....	41
4.3.28 SPANNING TREE PROTOCOL (STP) SECURITY .....	41
4.3.29 VLAN SECURITY .....	42
4.3.30 NETWORK TIME PROTOCOL (NTP) .....	43
4.3.31 SYSLOG .....	44
4.3.32 WIRELESS AUTHENTICATION USING RADIUS SERVER .....	44
4.3 CONCLUSION .....	46
CHAPTER 5: INSTALLATION AND CONFIGURATION.....	47
5.1 INTRODUCTION .....	47
5.2 SERVICES AND CORRESPONDING PERSON-IN CHARGE.....	47
5.3 SERVICE INSTALLATION AND CONFIGURATION .....	50
5.3.1 DOMAIN NAME SERVER (DNS) .....	50
5.3.2 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP).....	71
5.3.3 ROUTING & NETWORK ADDRESS TRANSLATION (NAT) .....	77

5.3.4 VIRTUAL LOCAL AREA NETWORK (VLAN) .....	80
5.3.5 IPV6 TRANSITION MECHANISM.....	83
5.3.6 WEB, SECURE SOCKETS LAYER (SSL) & VIRTUAL HOSTING .....	84
5.3.7 IPV6 WEB .....	87
5.3.8 SECURE FILE TRANSFER PROTOCOL (SFTP) .....	90
5.3.9 SAMBA .....	100
5.3.10 PROXY SERVER.....	104
5.3.11 RADIUS SERVER FOR NETWORK ACCOUNTING .....	107
5.3.12 LINUX EMAIL SERVER .....	125
5.3.13 NETWORK MANAGEMENT SYSTEM.....	132
5.3.14 ACCESS CONTROL LIST (ACL) .....	139
5.3.15 SECURITY HARDENING .....	139
5.3.16 AUTHENTICATION USING RADIUS SERVER.....	145
5.3.17 USER AUTHENTICATION AND AUTHORIZATION .....	162
5.3.18 FIREWALL FOR ROUTER.....	180
5.3.19 REMOTE LOGIN USING SSH .....	181
5.3.20 HARDENING LINUX SERVER .....	187
5.3.21 HARDENING WINDOWS SERVER.....	196
5.3.22 HARDENING WEB SERVER.....	232
5.3.23 AUTHENTICATION USER BY INTEGRATING ACTIVE DIRECTORY WITH LINUX .....	244
5.3.24 INTRUSION DETECTION SYSTEM (PORT MIRROR) .....	248
5.3.25 IPSEC BETWEEN SERVER AND USER .....	263
5.3.26 SAMBA SECURITY SERVICES .....	277
5.3.27 PORT SECURITY .....	279
5.3.28 SPANNING TREE PROTOCOL (STP) SECURITY .....	280
5.3.29 VLAN SECURITY .....	282

5.3.30 NETWORK TIME PROTOCOL (NTP) .....	283
5.3.31 SYSLOG .....	287
5.3.32 WIRELESS AUTHENTICATION USING RADIUS SERVER .....	294
5.3.33 ACTIVE DIRECTORY .....	320
5.4 CONCLUSION .....	337
CHAPTER 6: TESTING.....	338
6.1 INTRODUCTION.....	338
6.2 SERVICE TESTING .....	338
6.2.1 DOMAIN NAME SERVER (DNS) .....	338
6.2.2 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP).....	340
6.2.3 ROUTING & NETWORK ADDRESS TRANSLATION (NAT) .....	341
6.2.4 VIRTUAL LOCAL AREA NETWORK (VLAN) .....	342
6.2.5 IPV6 TRANSITION MECHANISM.....	344
6.2.6 WEB, SECURE SOCKETS LAYER (SSL) & VIRTUAL HOSITNG .....	345
6.2.7 IPV6 WEB .....	347
6.2.8 SECURE FILE TRANSFER PROTOCOL (SFTP) .....	349
6.2.9 SAMBA .....	352
6.2.10 PROXY SERVER.....	354
6.2.11 RADIUS SERVER FOR NETWORK ACCOUNTING .....	355
6.2.12 LINUX EMAIL SERVER .....	357
6.2.13 NETWORK MANAGEMENT SYSTEM.....	359
6.2.14 ACCESS CONTROL LIST (ACL) .....	360
6.2.15 SECURITY HARDENING .....	362
6.2.16 AUTHENTICATION USING RADIUS SERVER.....	365
6.2.17 USER AUTHENTICATION AND AUTHORIZATION .....	366
6.2.18 FIREWALL FOR ROUTER.....	367
6.2.19 REMOTE LOGIN USING SSH .....	367

6.2.20 HARDENING LINUX SERVER .....	374
6.2.21 HARDENING WINDOWS SERVER.....	376
6.2.22 HARDENING WEB SERVER.....	381
6.2.23 AUTHENTICATION USER BY INTEGRATING ACTIVE DIRECTORY WITH LINUX .....	382
6.2.24 INTRUSION DETECTION SYSTEM (PORT MIRROR) .....	384
6.2.25 IPSEC BETWEEN SERVER AND USER .....	386
6.2.26 SAMBA SECURITY SERVICES .....	387
6.2.27 PORT SECURITY .....	388
6.2.28 SPANNING TREE PROTOCOL (STP) SECURITY .....	391
6.2.29 VLAN SECURITY .....	392
6.2.30 NETWORK TIME PROTOCOL (NTP) .....	393
6.2.31 SYSLOG .....	394
6.2.32 WIRELESS AUTHENTICATION USING RADIUS SERVER .....	395
6.2.33 ACTIVE DIRECTORY .....	395
6.3 CONCLUSION.....	398
CHAPTER 7: CONCLUSION .....	399
7.1    INTRODUCTION.....	399
7.2 PROJECT ADVANTAGES .....	399
7.3 PROJECT DISADVANTAGES .....	400
7.4 PROJECT LIMITATION .....	400
7.5 CONCLUSION .....	401
BIBLIOGRAPHX.....	402
APPENDIXES .....	404

## LIST OF FIGURES

Figure 2. 1: Cisco 1941 Router .....	11
Figure 2. 2: Cisco Catalyst 2960 Switch.....	11
Figure 2. 3: UTP cable .....	12
Figure 2. 4: RJ-45 Connector.....	12
Figure 2. 5: Linksys access point .....	13
Figure 3. 1: Physical design .....	20
Figure 3. 2: Logical design .....	21
Figure 5. 1: Server Manager .....	50
Figure 5. 2: Add Roles .....	51
Figure 5. 3: Open Start Manager.....	52
Figure 5. 4: Select Roles .....	53
Figure 5. 5: DNS manager .....	54
Figure 5. 6: New Zone Wizard .....	55
Figure 5. 7: Zone type.....	56
Figure 5. 8: Zone Name .....	57
Figure 5. 9: Zone File.....	57
Figure 5. 10: Dynamic Update.....	58
Figure 5. 11: Completing New Wizard.....	58
Figure 5. 12: Zone Type.....	59
Figure 5. 13: Active Directory Zone Replication Scope.....	60
Figure 5. 14: Reverse Lookup Zone Name .....	60
Figure 5. 15: Reverse Lookup Zone Name .....	61
Figure 5. 16: Completing the New Zone Wizard.....	61
Figure 5. 17: Alias name .....	62
Figure 5. 18: Browse group1 .....	62
Figure 5. 19: FQDN target host .....	63
Figure 5. 20: Successful add .....	63
Figure 5. 21: Properties.....	64
Figure 5. 22: Internet Protocol Version 6 (TCP/IPv6).....	64

Figure 5. 23: Enter the IPv6 Address.....	65
Figure 5. 24: New Zone .....	65
Figure 5. 25: Zone Type.....	66
Figure 5. 26: IPv6 Reverse Lookup Zone .....	66
Figure 5. 27: IPv6 Address Profile .....	67
Figure 5. 28: Dynamic Update.....	68
Figure 5. 29: Completing the new Zone Wizard.....	68
Figure 5. 30: New Pointer (PTR) .....	69
Figure 5. 31: Enter the Host IP Address and Host name .....	69
Figure 5. 32: Browse.....	70
Figure 5. 33: Insert the IPv6 address and host name .....	70
Figure 5. 34: Add Roles Wizard .....	71
Figure 5. 35: Select Server Roles Wizard.....	72
Figure 5. 36: Select Network Connection Bindings .....	73
Figure 5. 37: Specify IPv4 DNS Server Settings .....	73
Figure 5. 38: Specify IPv4 WINS Server Settings.....	74
Figure 5. 39: Add Scope .....	75
Figure 5. 40: Configure DHCPv6 Stateless Mode.....	75
Figure 5. 41: Specify IPv6 DNS Server Settings .....	76
Figure 5. 42: Confirm Installation Selection.....	76
Figure 5. 43: Routing Command .....	78
Figure 5. 44: Add NAT inside source static .....	78
Figure 5. 45: Setup access list and permit ip address .....	78
Figure 5. 46: Set g0/1 interface as public IP address using overload function .....	79
Figure 5. 47: Setup g0/1 as outside interface.....	79
Figure 5. 48: Setup g0/0 as inside.....	80
Figure 5. 52: IPv6 Tunnelling Configuration .....	84
Figure 5. 53: Browse to DNS.....	84
Figure 5. 54: Browse to group1.com .....	85
Figure 5. 55: Browse to Foward Lookup Zones .....	85
Figure 5. 56: Browse to GROUP1 .....	86
Figure 5. 57: Alias (CNAME) .....	86
Figure 5. 58: Open browser and enter www.virtual.group1.com .....	87
Figure 5. 59: Add Web Site .....	88

Figure 5. 60: Fill the requirement .....	88
Figure 5. 61: Directory Browsing .....	89
Figure 5. 62:File in wwwroot.....	89
Figure 5. 63: Installing vsftpd and updating ubuntu .....	90
Figure 5. 64: Installing openssh-server.....	90
Figure 5. 65: Uncommenting anonymous_enable, local_enable and write_enable.....	91
Figure 5. 66: Uncommenting use_localtime and adding local_root .....	91
Figure 5. 67: Uncommenting ascii_upload_enable and ascii_download_enable .....	92
Figure 5. 68: Uncommenting chroot_local_user and chroot_list_enable .....	92
Figure 5. 69: Uncommenting ls_recurse_enable .....	93
Figure 5. 70: Adding pam_service_name=ftp .....	93
Figure 5. 71: Opening ssh/sshd_config file .....	94
Figure 5. 72: Uncomment PermitEmptyPasswords no .....	94
Figure 5. 73: Commenting Subsystem sftp /usr/lib/openssh/sftp-server .....	95
Figure 5. 74: Adding lines the /etc/shh/sshd_config.....	95
Figure 5. 75: Creating new group .....	96
Figure 5. 76: Creating new user.....	96
Figure 5. 77: Entering password for user.....	97
Figure 5. 78: Creating directory for user .....	97
Figure 5. 79: Creating /etc/vsftpd_chroot.list file.....	98
Figure 5. 80: Adding user in the /etc/vsftpd_chroot.list .....	98
Figure 5. 81: Adding ftpuser in /etc/ftpusers .....	99
Figure 5. 82: Opening /etc/pam.d/vsftpd file .....	99
Figure 5. 83: Specifying directory for the user .....	100
Figure 5. 84: Checking directory for the user .....	100
Figure 5. 85: sudo apt-get install samba .....	101
Figure 5. 86: Add New User & restart samba.....	101
Figure 5. 87: sudo netstat -tulpn   grep smbd.....	102
Figure 5. 88: nano /etc/samba/smb.conf .....	102
Figure 5. 89: Samba Configuration.....	102
Figure 5. 90: Create Shared Folder .....	103
Figure 5. 91: 3Folder Sharing from Linux1 Server to Windows Server .....	103
Figure 5. 92: Install squid package .....	104
Figure 5. 93: Check squid status .....	104

Figure 5. 94: Enter squid configuration file.....	104
Figure 5. 95: Edit ACL command on squid configuration file .....	105
Figure 5. 96: Change http access .....	106
Figure 5. 97: Restart squid service.....	106
Figure 5. 98: Network proxy settings .....	107
Figure 5. 99: Fill in the details on proxy manual settings.....	107
Figure 5. 100: Add Roles .....	108
Figure 5. 101: Before You Begin.....	108
Figure 5. 102: Select Server Roles.....	109
Figure 5. 103: Network Policy and Access Services .....	109
Figure 5. 104: Select Role Services. ....	110
Figure 5. 105: Confirm Installation Selections. ....	110
Figure 5. 106: Installation Progress. ....	111
Figure 5. 107: Installation Progress. ....	111
Figure 5. 108: Open NPS .....	112
Figure 5. 109: Go to Network Policy Server .....	112
Figure 5. 110: Click OK.....	113
Figure 5. 111: New RADIUS Client.....	113
Figure 5. 112: RADIUS Client. ....	114
Figure 5. 113: Policy Name and Connection Type.....	115
Figure 5. 114: Specify Conditions. ....	115
Figure 5. 115: Add User Groups.....	115
Figure 5. 116: Add Groups. ....	116
Figure 5. 117: Domain Users.....	116
Figure 5. 118: Select Group.....	117
Figure 5. 119: User Groups.....	117
Figure 5. 120: Specify Conditions. ....	118
Figure 5. 121: Specify Access Permission > Access Granted. ....	118
Figure 5. 122: Configure Authentication Methods .....	119
Figure 5. 123: Set Idle Timeout .....	119
Figure 5. 124: Remove Attributes.....	120
Figure 5. 125: Standard.....	120
Figure 5. 126: Vendor Specific.....	121
Figure 5. 127: Encryption .....	121

Figure 5. 128: IP Settings.....	122
Figure 5. 129: Completing New Network Policy .....	122
Figure 5. 130: Done created.....	123
Figure 5. 131: Open Putty .....	123
Figure 5. 132: Login .....	124
Figure 5. 133: Configuration of AAA model.....	125
Figure 5. 134: Command to install postfix .....	125
Figure 5. 135: Command to install apache2 .....	125
Figure 5. 136: Apache 2 web page.....	126
Figure 5. 137: Postfix configuration .....	127
Figure 5. 138: Command to install squirrelmail .....	127
Figure 5. 139: Edit configuration file .....	128
Figure 5. 140: Edit IMAP servers .....	128
Figure 5. 141: Select IMAP servers .....	129
Figure 5. 142: Edit Server Settings .....	129
Figure 5. 143: Select domain name.....	130
Figure 5. 144: /var/www directory.....	130
Figure 5. 145: Edit configuration file .....	130
Figure 5. 146: edit /etc/apache2/sites-available .....	131
Figure 5. 147: Command to install Mailutils .....	131
Figure 5. 148: Add user for mail server .....	132
Figure 5. 149: Set up APT to talk to the OpenNMS repository.....	132
Figure 5. 150: Install OpenNMS.....	132
Figure 5. 151: Update to get the latest packages .....	133
Figure 5. 152: Show a number of OpenNMS packages.....	133
Figure 5. 153: Install PostgreSQL .....	134
Figure 5. 154: Check PostgreSQL version .....	134
Figure 5. 155: Change option.....	134
Figure 5. 156: Change entries .....	134
Figure 5. 157: Restart database .....	135
Figure 5. 158: Add private packages .....	135
Figure 5. 159: Install Oracle Java8 .....	135
Figure 5. 160: Set up Oracle Java8 to be default .....	136
Figure 5. 161: Verify Java version.....	136

Figure 5. 162: Install OpenNMS.....	136
Figure 5. 163: Auto-detect JRE .....	136
Figure 5. 164: To configure to use specific JRE binary .....	137
Figure 5. 165: Create and configure OpenNMS database .....	137
Figure 5. 166: Install IPLIKE .....	137
Figure 5. 167: Verify connectivity.....	137
Figure 5. 168: Open OpenNMS web .....	138
Figure 5. 169: Scan devices .....	138
Figure 5. 170: Interface appeared .....	138
Figure 5. 171: Configuring ACL .....	139
Figure 5. 172: Login Banner for Switch .....	140
Figure 5. 173: Login Banner for Router .....	140
Figure 5. 174: Disable IP finger.....	141
Figure 5. 175: Password Encryption.....	142
Figure 5. 176: Password min length .....	142
Figure 5. 177: Failure rate enable by the devices .....	143
Figure 5. 178: Failure rate enable .....	143
Figure 5. 179: Disable unused port .....	144
Figure 5. 180: Add Roles .....	145
Figure 5. 181: Before You Begin.....	145
Figure 5. 182: Select Server Roles.....	146
Figure 5. 183: Network Policy and Access Services .....	146
Figure 5. 184: Select Role Services. ....	147
Figure 5. 185: Confirm Installation Selections.....	147
Figure 5. 186: Installation Progress. ....	148
Figure 5. 187: Installation Progress. ....	148
Figure 5. 188: Installation results.....	149
Figure 5. 189: Go to Network Policy Server .....	149
Figure 5. 190: Click Ok .....	150
Figure 5. 191: New RADIUS Client.....	150
Figure 5. 192: RADIUS Client. ....	151
Figure 5. 193: New Network Policies.....	151
Figure 5. 194: Policy Name and Connection Type.....	152
Figure 5. 195: Specify Conditions. ....	152

Figure 5. 196: Add User Groups.....	153
Figure 5. 197: Add Groups. ....	153
Figure 5. 198: Domain Users.....	154
Figure 5. 199: Select Group.....	154
Figure 5. 200: User Groups.....	155
Figure 5. 201: Specify Conditions. ....	155
Figure 5. 202: Specify Access Permission > Access Granted. ....	156
Figure 5. 203: Configure Authentication Methods .....	156
Figure 5. 204: Idle Timeout .....	157
Figure 5. 205: Remove Attributes.....	157
Figure 5. 206: Standard.....	158
Figure 5. 207: Vendor Specific.....	158
Figure 5. 208: Encryption .....	159
Figure 5. 209: IP Settings.....	159
Figure 5. 210: Completing New Network Policy .....	160
Figure 5. 211: Done created.....	160
Figure 5. 212: Login using Serial .....	161
Figure 5. 213: Login Router.....	162
Figure 5. 214: AAA command for Router .....	162
Figure 5. 215: Go to Active Directory Users and Computers.....	163
Figure 5. 216: Add New User .....	163
Figure 5. 217: New Object - User .....	164
Figure 5. 218: Insert Password.....	164
Figure 5. 219: Confirmation Information of User .....	165
Figure 5. 220: Add New Group .....	165
Figure 5. 221: New Object - Group .....	166
Figure 5. 222: Add user into group .....	166
Figure 5. 223: Select Groups .....	167
Figure 5. 224: Multiple Names Found .....	167
Figure 5. 225: Click ok button .....	168
Figure 5. 226: Add User into Print Operation Group .....	168
Figure 5. 227: Go to Network Policy Server .....	168
Figure 5. 228: Add New Network Policy .....	169
Figure 5. 229: Specify Network Policy Name and Connection Type.....	169

Figure 5. 230: Select Conditions.....	170
Figure 5. 231: Select User Groups .....	170
Figure 5. 232: Add Groups .....	171
Figure 5. 233: Insert the Group Name .....	171
Figure 5. 234: Click Ok button .....	172
Figure 5. 235: Click Ok button after confirmed the groups is inserted correct .....	172
Figure 5. 236: Click Next.....	172
Figure 5. 237: Specify Access Permission.....	173
Figure 5. 238: Configure Authentication Methods .....	174
Figure 5. 239: Connection Request Policy .....	174
Figure 5. 240: Configure Constraints.....	174
Figure 5. 241: Configure Settings .....	175
Figure 5. 242: Attribute Information .....	175
Figure 5. 243: Configure Settings at Vendor Specific.....	176
Figure 5. 244: Add Vendor Specific Attribute.....	176
Figure 5. 245: Click Add button .....	177
Figure 5. 246: Set User Privilege .....	177
Figure 5. 247: Click Close button .....	178
Figure 5. 248: The Information will Display in This Box .....	178
Figure 5. 249: Configure Settings At Encryption .....	179
Figure 5. 250: Confirmation policy before Click Finish button .....	179
Figure 5. 251: Policy Done Created.....	180
Figure 5. 252: Extended Access List CLIENT .....	180
Figure 5. 253: SSH configuration on Router .....	182
Figure 5. 254: freeSSHd Setup .....	182
Figure 5. 255: Select Destination Location.....	183
Figure 5. 256: Select Components .....	183
Figure 5. 257: Select Start Menu Folder.....	184
Figure 5. 258: Ready to Install.....	184
Figure 5. 259: Authentication .....	185
Figure 5. 260: Encryption .....	186
Figure 5. 261: Tunnelling .....	186
Figure 5. 262: Server Status.....	187
Figure 5. 263: Change Updates.....	187

Figure 5. 264: Ubuntu Software Centre .....	188
Figure 5. 265: Password status.....	188
Figure 5. 266: Installing libpam-cracklib and opening pam.d/common-password file .....	189
Figure 5. 267: Changing password characteristics .....	189
Figure 5. 268: Port scanned using Nmap .....	190
Figure 5. 269: Disabling cups .....	190
Figure 5. 270: Testing and upgrading Bash .....	191
Figure 5. 271: Opening irq balance.....	191
Figure 5. 272: Changing Enabled .....	192
Figure 5. 273: Opening rc.local file .....	192
Figure 5. 274: Disabling Bluetooth.....	192
Figure 5. 275: Opening bluetooth/main.conf.....	192
Figure 5. 276: Setting Initially Powered .....	193
Figure 5. 277: Opening network/interfaces file .....	193
Figure 5. 278: File Disabling wireless .....	193
Figure 5. 279: Opening security/limits.conf .....	194
Figure 5. 280: Setting security limits .....	194
Figure 5. 281: mysql port is open .....	195
Figure 5. 282: Deleting package file in mysql .....	195
Figure 5. 283: Remove leftover file in the mysql package file.....	196
Figure 5. 284: Security Configuration Wizard .....	197
Figure 5. 285: Creating new security policy .....	197
Figure 5. 286: Naming server .....	197
Figure 5. 287: Processing Security Configuration Database .....	198
Figure 5. 288: Role-Based Service Configuration .....	198
Figure 5. 289: Selecting Server Roles (1) .....	199
Figure 5. 290: Selecting Server Roles (2) .....	199
Figure 5. 291: Selecting Server Roles (3).....	200
Figure 5. 292: Selecting Client Features (1) .....	200
Figure 5. 293: Selecting Client Features (2) .....	201
Figure 5. 294: Selecting Administration and Other Options (1).....	201
Figure 5. 295: Selecting Administration and Other Options (2).....	202
Figure 5. 296: Selecting Administration and Other Options(3).....	202

Figure 5. 297: Selecting Administration and Other Options(4).....	203
Figure 5. 298: Selecting Additional Services (1).....	203
Figure 5. 299: Selecting Additional Services (2).....	204
Figure 5. 300: Handling Unspecified Service.....	204
Figure 5. 301: Confirming Service Changes.....	205
Figure 5. 302: Network Security.....	205
Figure 5. 303: Selecting Network Security Rules.....	206
Figure 5. 304: Registry Settings.....	206
Figure 5. 305: Rewire SMB Security Signatures.....	207
Figure 5. 306: Require LDAP Signing .....	207
Figure 5. 307: Outbound Authentication Methods .....	208
Figure 5. 308: Outbound Authentication using Domain Accounts.....	208
Figure 5. 309: Registry Settings Summary .....	209
Figure 5. 310: Audit Policy.....	209
Figure 5. 311: System Audit Policy .....	210
Figure 5. 312: Audit Policy Summary .....	210
Figure 5. 313: Save Security Policy.....	211
Figure 5. 314: Security Policy File Name.....	211
Figure 5. 315: Apply Security Policy .....	212
Figure 5. 316: Applying Security Policy .....	212
Figure 5. 317: Server Manager .....	213
Figure 5. 318: Disabling Guest Account.....	213
Figure 5. 319: Guest Account Disabled .....	214
Figure 5. 320: Local Security Policy .....	214
Figure 5. 321: Audit Policy.....	215
Figure 5. 322: Opening Audit account logon events properties .....	215
Figure 5. 323: Audit account logon events properties .....	216
Figure 5. 324: Audit account management properties .....	216
Figure 5. 325: Audit directory services access properties .....	217
Figure 5. 326: Audit logon events properties.....	217
Figure 5. 327: Audit object access properties.....	218
Figure 5. 328: Audit policy change properties.....	218
Figure 5. 329: Audit privilege use properties .....	219
Figure 5. 330: Audit process tracking properties .....	219

Figure 5. 331: Audit system events properties.....	220
Figure 5. 332: Check all the audits .....	220
Figure 5. 333: Change settings in Windows Updates .....	221
Figure 5. 334: Updates that are available.....	221
Figure 5. 335: Choosing updates to be installed .....	222
Figure 5. 336: Choosing updates to be installed(2) .....	222
Figure 5. 337: Choosing updates to be installed(3) .....	223
Figure 5. 338: Accepting the license terms.....	223
Figure 5. 339: Opening Features in Server Manager.....	224
Figure 5. 340: Add Features Wizard.....	224
Figure 5. 341: Confirm Installation Selection.....	225
Figure 5. 342: Clicking Check Firewall Status.....	225
Figure 5. 343: Customize Settings in Windows Firewall .....	226
Figure 5. 344: Status of Windows Firewall .....	226
Figure 5. 345: Windows Firewall with Advance Security.....	227
Figure 5. 346: Print Spooler Properties.....	227
Figure 5. 347: Distributed Transaction Coordinator Properties.....	228
Figure 5. 348: KtmRm for Distributed Transaction Coordinator Properties .....	229
Figure 5. 349: Certificate Propagation Properties.....	229
Figure 5. 350: Netlogon Properties .....	230
Figure 5. 351: Special Administration Console Helper Properties .....	231
Figure 5. 352: Secure Socket Tunneling Protocol Service Properties .....	232
Figure 5. 353: Windows Error Reporting Service Properties .....	232
Figure 5. 354: Open the web.conf.....	233
Figure 5. 355: Edit web.conf.....	233
Figure 5. 356: Adding <trace> part .....	234
Figure 5. 357: Adding <remove> part .....	234
Figure 5. 358: Adding https .....	235
Figure 5. 359: Allowed only port 80 and 443 .....	236
Figure 5. 360: Allowed IPsec.....	236
Figure 5. 361: Run Group Policy Management .....	237
Figure 5. 362: Edit Default Domain Policy .....	237
Figure 5. 363: Click computer configuration.....	238
Figure 5. 364: Click Windows Setting.....	238

Figure 5. 365: Select Security Setting.....	238
Figure 5. 366: Select Local Policies .....	239
Figure 5. 367: Select Audit Policy .....	239
Figure 5. 368: Select Audit account logon event .....	239
Figure 5. 369: Define the policy settings .....	240
Figure 5. 370: Update User Policy.....	240
Figure 5. 371: Setting Authentication.....	240
Figure 5. 372: Open Services.....	241
Figure 5. 373: Disabled Startup Type .....	241
Figure 5. 374: Update Windows .....	242
Figure 5. 375: Select version for .NET Framework.....	242
Figure 5. 376: Scan open port.....	243
Figure 5. 377: Add a new rule to block specific port.....	243
Figure 5. 378: New rule created.....	244
Figure 5. 380: Beyond Trust .....	244
Figure 5. 381: List of all files and directories.....	245
Figure 5. 382: Go to root.....	245
Figure 5. 383: Directory .deb appears in CLI .....	245
Figure 5. 384: Directory .deb appears in GUI .....	246
Figure 5. 385: Installing pbis-open-8.5.0.153.....	247
Figure 5. 386: Done installing. ....	247
Figure 5. 387: domainjoin-cli .....	247
Figure 5. 388: Successfully joined the Active Directory domain.....	248
Figure 5. 389: Install all tools .....	249
Figure 5. 390: Install all snort pre-requisites .....	249
Figure 5. 391: Install a few pre-requisites of Snort DAQ.....	249
Figure 5. 392: Create folder .....	249
Figure 5. 393: Change Directory .....	250
Figure 5. 394: Install DAQ .....	250
Figure 5. 395: Change directory to DAQ.....	250
Figure 5. 396: Check everything needed .....	251
Figure 5. 397: Modules being configured.....	251
Figure 5. 398: Executable of this specific application created .....	251
Figure 5. 399: Make install in API.....	251

Figure 5. 400: Install additional pre-requisites .....	252
Figure 5. 401: Install libnghhttp2-14 .....	252
Figure 5. 402: Change Directory .....	253
Figure 5. 403: Install DAQ .....	253
Figure 5. 404: Change Directory .....	253
Figure 5. 405: Enables sourcesfire.....	253
Figure 5. 406: Executable of this specific application created .....	254
Figure 5. 407: Make install in API.....	254
Figure 5. 408: Update shared libraries.....	254
Figure 5. 409: Place to /usr/bin .....	254
Figure 5. 410: Test snort .....	255
Figure 5. 411: Create snort group .....	255
Figure 5. 412: Create snort user .....	255
Figure 5. 413: Create /etc/snort.....	255
Figure 5. 414: Create /etc/snort/rules.....	256
Figure 5. 415: Create /etc/snort/rules/iplists .....	256
Figure 5. 416: Create /etc/snort/preproc_rules.....	256
Figure 5. 417: Create /usr/local/lib/snort_dynamicrules.....	256
Figure 5. 418: Create /etc/snort/so_rules .....	256
Figure 5. 419: Create file to store rules.....	256
Figure 5. 420: Create logging directory .....	256
Figure 5. 421: Adjust permission.....	257
Figure 5. 422: Adjust permission.....	257
Figure 5. 423: Change owner.....	257
Figure 5. 424: Copy configuration files .....	258
Figure 5. 425: Comment out all rulesets in snort.conf file .....	258
Figure 5. 426: Change setting .....	259
Figure 5. 427: Change line.....	259
Figure 5. 428: Edit snort.conf .....	260
Figure 5. 429: Enable local.rules files .....	260
Figure 5. 430: Check PC's interface .....	261
Figure 5. 431: Verify snort.....	261
Figure 5. 432: Check verification .....	261
Figure 5. 433: Edit /etc/snort/rules/local.rules .....	262

Figure 5. 434: Insert line .....	262
Figure 5. 435: Ensure banyard2 knows the rules .....	262
Figure 5. 436: Add line .....	263
Figure 5. 437: Insert port mirror .....	263
Figure 5. 438: Install SoftEther VPN Manager .....	264
Figure 5. 439: Select SoftEther VPN Server .....	264
Figure 5. 440: Select first radio button C:\Program Files\SoftEther VPN Server .....	265
Figure 5. 441: Select Edit Setting .....	266
Figure 5. 442: Change VPN Server Hostname localhost to IP Address 192.168.11.34 .....	266
Figure 5. 443: Change Administrator Password .....	267
Figure 5. 444: SoftEther VPN Server/Bridge East Setup .....	267
Figure 5. 445: Easy Setup – Decide the Virtual Hub Name .....	268
Figure 5. 446: SoftEther VPN Server/Bridge Easy Setup .....	268
Figure 5. 447: Select Virtual Hub .....	269
Figure 5. 448: Manage of Virtual Hub “VPN” .....	269
Figure 5. 449: Create New User .....	270
Figure 5. 450: Manage Users .....	270
Figure 5. 451: VirtualNAT and Vitrual DHCP Function (SecureNAT) Setting .....	271
Figure 5. 452: SoftEther VPN Server Manager .....	271
Figure 5. 453: Open Network and Sharing Center .....	272
Figure 5. 454: Set Up a Connection or Network .....	272
Figure 5. 455: Create a VPN connection .....	273
Figure 5. 456: Connect to a Workplace .....	273
Figure 5. 457: Type your user name and password .....	274
Figure 5. 458: The connection is ready to use .....	274
Figure 5. 459: General tab .....	275
Figure 5. 460: Security tab.....	275
Figure 5. 461: Advanced Properties.....	276
Figure 5. 462: Connect VPN Connection .....	276
Figure 5. 463: add group.....	277
Figure 5. 464: add a new folder .....	277
Figure 5. 465: Add File to workshop .....	277
Figure 5. 466: edit config file .....	278

Figure 5. 467: Add content to [workshop].....	278
Figure 5. 468: Add new user, assign to groups & set password .....	278
Figure 5. 469: Restart Samba Services .....	278
Figure 5. 470: Port Security at port fa0/3 .....	279
Figure 5. 471: Port Security at port fa0/7 .....	279
Figure 5. 472: Port security at port fa0/11 .....	279
Figure 5. 473: Port Security at port fa0/15 .....	280
Figure 5. 474: Enable the spanning-tree portfast and spanning-tree bpduguard .....	281
Figure 5. 475: Enable the spanning-tree guard root.....	282
Figure 5. 476: switchport nonegotiate .....	282
Figure 5. 477: show vlan.....	282
Figure 5. 478: Create VLAN 15 named unusedPort.....	283
Figure 5. 479: Suspend VLAN 15 .....	283
Figure 5. 480: Assign all unused port into VLAN 15.....	283
Figure 5. 481: Assign all usable VLANs into trunk port.....	283
Figure 5. 482: Install service.....	284
Figure 5. 483: Edit config file.....	284
Figure 5. 484: Adding following command.....	284
Figure 5. 485: Restart and check the status of service.....	285
Figure 5. 486: check the date .....	285
Figure 5. 487: List the time zones.....	285
Figure 5. 488: Set the time zone .....	285
Figure 5. 489: Show the setup.....	285
Figure 5. 490: check the condition of the service .....	286
Figure 5. 491: NTP condition .....	286
Figure 5. 492: Alternative command .....	286
Figure 5. 493: Install syslog on linux .....	287
Figure 5. 494: Check syslog version.....	287
Figure 5. 495: Enables syslog receive log .....	287
Figure 5. 496: Uncomment TCP and UDP .....	288
Figure 5. 497: Restart service .....	288
Figure 5. 498: Start service syslog .....	288
Figure 5. 499: Set destination host.....	289
Figure 5. 500: Restart service syslog .....	289

Figure 5. 501: Putty Terminal .....	290
Figure 5. 502: AD username login.....	290
Figure 5. 503: Global configuration.....	291
Figure 5. 504: Insert command in router .....	291
Figure 5. 505: Putty Terminal.....	292
Figure 5. 506: Switch login admin.....	292
Figure 5. 507: Global configuration.....	293
Figure 5. 508: Switch configuration .....	293
Figure 5. 509: Add Roles .....	294
Figure 5. 510: Before You Begin.....	294
Figure 5. 511: Select Server Roles.....	295
Figure 5. 512: Select Role services.....	295
Figure 5. 513: Select Setup Types .....	296
Figure 5. 514: Select CA Type .....	296
Figure 5. 515: Select Private Key .....	297
Figure 5. 516: Configure cryptography .....	297
Figure 5. 517: Configure CA Name.....	298
Figure 5. 518: Configure Validity Period .....	299
Figure 5. 519: Certification Databse .....	299
Figure 5. 520: Installation Page .....	300
Figure 5. 521: Installation Succeeded.....	300
Figure 5. 522: Console.....	301
Figure 5. 523: Certificates snap-in.....	301
Figure 5. 524: Certificates Local Computer .....	302
Figure 5. 525: Add or Remove Snap-ins .....	303
Figure 5. 526: Duplicate Computer Certificates .....	303
Figure 5. 527: Duplicate Template .....	304
Figure 5. 528: Properties of New Template.....	304
Figure 5. 529: Properties of New Template.....	305
Figure 5. 530: Security New Template .....	306
Figure 5. 531: Security New Template .....	306
Figure 5. 532: Certification Authority .....	307
Figure 5. 533: Enable Certification Template.....	307
Figure 5. 534: Request New Certificate.....	308

Figure 5. 535: Cetification Enrollement .....	308
Figure 5. 536: Radius Authentication .....	309
Figure 5. 537: Certification Properties.....	309
Figure 5. 538: Installation Page .....	310
Figure 5. 539: Configure Wireless Radius.....	310
Figure 5. 540: Configure 802.1X .....	311
Figure 5. 541: New Radius Client.....	312
Figure 5. 542: Configure Authentication Method.....	312
Figure 5. 543: EAP properties .....	313
Figure 5. 544: Select Group.....	313
Figure 5. 545: Installation Page .....	314
Figure 5. 546: Putty Terminal.....	314
Figure 5. 547: AD username login.....	315
Figure 5. 548: Global configuration.....	315
Figure 5. 549: Create VLAN 60 .....	316
Figure 5. 550: Putty Terminal.....	316
Figure 5. 551: Switch login admin.....	317
Figure 5. 552: Global configuration.....	317
Figure 5. 553: Configure Vlan 60 .....	318
Figure 5. 554: Access Router sign in .....	319
Figure 5. 555: Connectivity Setting .....	319
Figure 5. 556: Setup the DHCP server.....	320
Figure 5. 557: Server Roles Selection.....	321
Figure 5. 558: Select Next .....	322
Figure 5. 559: Confirmation before installation AD.....	322
Figure 5. 560: AD installation status .....	323
Figure 5. 561: Select Next .....	323
Figure 5. 562: Deployment configuration.....	324
Figure 5. 563: Naming the forest root domain.....	324
Figure 5. 564: Setting forest functional level.....	325
Figure 5. 565: Additional domain controller options.....	326
Figure 5. 566: Select Yes for confirmation.....	326
Figure 5. 567: Configuration location for Database, Log files and SYSVOL.....	326
Figure 5. 568: Setup of Directory Services Restore Mode Administrator Password	327

Figure 5. 569: Summary for dcpromo.exe .....	327
Figure 5. 570: ADDS Installation Wizard .....	328
Figure 5. 571: Open Active Directory Users and Computer .....	329
Figure 5. 572: Add new user for AD .....	329
Figure 5. 573: Set the user information with details .....	330
Figure 5. 574: Enter the password and tick on the Password never expires option...331	331
Figure 5. 575: Detail of the user that has been configured. ....	331
Figure 5. 576: Add new group for AD.....	332
Figure 5. 577: Create windowsTeam.....	332
Figure 5. 578: Create linux1Team .....	333
Figure 5. 579: Create linux2Team .....	333
Figure 5. 580: Add some name members in windowsTeam.....	334
Figure 5. 581: Successfully add members in group .....	334
Figure 5. 582: Select all names .....	335
Figure 5. 583: Add in Print Operator group.....	335
Figure 5. 584: Successfully add in group.....	336
Figure 6. 1: Testing on server and client.....	339
Figure 6. 2: IPv4 and IPv6 Shown in Command Prompt .....	340
Figure 6. 3: DHCP Information Is Shown at Window Server .....	340
Figure 6. 4: Routing Testing .....	341
Figure 6. 5: NAT Testing.....	342
Figure 6. 6: Show VLAN.....	342
Figure 6. 7: Show Interface.....	343
Figure 6. 8: Show Interfaces .....	344
Figure 6. 9: IPv6 web of group2 .....	345
Figure 6. 10: www.group1.com .....	345
Figure 6. 11: https://www.group1.com .....	346
Figure 6. 12: www.grou1ipv6.com .....	346
Figure 6. 13: www.virtual.group1.com.....	347
Figure 6. 14: Testing ipv6 web using domain.....	348
Figure 6. 15: Testing ipv6 web using ip address .....	348
Figure 6. 16: Testing ipv6 web domain at linux server .....	349

Figure 6. 17: Connecting to server compute .....	350
Figure 6. 18: Transferring file to the server.....	350
Figure 6. 19: Using FileZilla to test sftp.....	351
Figure 6. 20: Command asking password.....	351
Figure 6. 21: Using browser to test sftp.....	352
Figure 6. 22: Run \\192.168.11.42 .....	352
Figure 6. 23: Access to 192.168.11.42.....	353
Figure 6. 24: Shared file.....	353
Figure 6. 25: View shared file.....	353
Figure 6. 26: Error message when search “Ask.com” .....	354
Figure 6. 27: Error message when search “Yahoo.com” .....	354
Figure 6. 28: Login with AD.....	355
Figure 6. 29: Check for the log file location .....	355
Figure 6. 30: Log file location .....	356
Figure 6. 31: Details of log file .....	356
Figure 6. 32: Login to SquirrelMail .....	357
Figure 6. 33: Sending email using SquirrelMail .....	357
Figure 6. 34: Delivered message.....	358
Figure 6. 35: Replied email.....	358
Figure 6. 36: Delivered message.....	359
Figure 6. 37: Shows SSH services .....	359
Figure 6. 38: Alarm appeared .....	359
Figure 6. 39: Alert about the problem.....	360
Figure 6. 40: Testing ACL using port 80 .....	360
Figure 6. 41: Testing ACL using port 443 .....	361
Figure 6. 42: Testing ACL by ping .....	361
Figure 6. 43: Login banner.....	362
Figure 6. 44: Login banner.....	362
Figure 6. 45: Disable IP finger.....	363
Figure 6. 46: Password encryption.....	363
Figure 6. 47: Password min length .....	364
Figure 6. 48: Failure rate enable by the devices .....	364
Figure 6. 49: Disable unused port .....	364
Figure 6. 50: Open serial.....	366

Figure 6. 51: Login with AD user .....	366
Figure 6. 52: User Login in Router .....	367
Figure 6. 53: Show ip access-list .....	367
Figure 6. 54: Login to linux1 .....	368
Figure 6. 55: Successfully login to linux1 terminal .....	368
Figure 6. 56: Login to linux2 .....	369
Figure 6. 57: Successfully login to linux2 terminal .....	369
Figure 6. 58: Login to switch.....	369
Figure 6. 59: Successfully login to switch .....	369
Figure 6. 60: Login to router.....	370
Figure 6. 61: Successfully login to router .....	370
Figure 6. 62: Successfully login to linux1 terminal .....	371
Figure 6. 63: Insert IP address of switch.....	371
Figure 6. 64: Successfully login to switch .....	372
Figure 6. 65: Insert the IP address of router.....	372
Figure 6. 66: Successfully login to router .....	373
Figure 6. 67: Ports opened before hardening .....	374
Figure 6. 68: Ipp service is gone from the opened ports.....	374
Figure 6. 69: mysql is available at open ports .....	375
Figure 6. 70: mysql is gone from open ports .....	375
Figure 6. 71: Testing password after hardening.....	376
Figure 6. 72: Nmap Output before hardening .....	376
Figure 6. 73: Ports/Hosts before hardening (1).....	377
Figure 6. 74: Ports/Hosts before hardening (2).....	377
Figure 6. 75: Host Details before hardening .....	378
Figure 6. 76: Topology .....	378
Figure 6. 77: Nmap Output after hardening.....	379
Figure 6. 78: Ports/Hosts after hardening (1).....	379
Figure 6. 79: Ports/Hosts after hardening (2).....	380
Figure 6. 80: Host Details after hardening .....	380
Figure 6. 81: Testing on IP address and Domain Restrictions.....	381
Figure 6. 82: Testing on SSL certificate .....	381
Figure 6. 83: Testing on authentication .....	382
Figure 6. 84: Using ls -l command to view list.....	383

Figure 6. 85: Command to enter and edit the file content. ....	383
Figure 6. 86: Adding a new configuration into the file.....	383
Figure 6. 87: Verify installation.....	384
Figure 6. 88: Test configuration file using IDS interface .....	384
Figure 6. 89: Ping other servers .....	385
Figure 6. 90: An alert appeared.....	385
Figure 6. 91: Testing configuration file using port mirror interface.....	386
Figure 6. 92: Ping other servers .....	386
Figure 6. 93: Log File (Ping from Linux to Windows).....	386
Figure 6. 94: Monitor ESP protocol.....	387
Figure 6. 95: Secured shared.....	387
Figure 6. 96: Authentication required.....	388
Figure 6. 97: Insert username & password .....	388
Figure 6. 98: show port-security .....	389
Figure 6. 99: show port-security address .....	389
Figure 6. 100: Ipconfig /all .....	390
Figure 6. 101: MAC Address Is Shown .....	390
Figure 6. 102: show int status .....	391
Figure 6. 103: Ipconfig .....	391
Figure 6. 104: Show STP summary .....	392
Figure 6. 105: show vlan.....	392
Figure 6. 106: Ipconfig .....	393
Figure 6. 107: show interface trunk .....	393
Figure 6. 108: Testing to sync.....	394
Figure 6. 109: Syslog Server log.....	395
Figure 6. 110: Group1 Wireless Connection .....	395
Figure 6. 111: Right click the computer and select Properties .....	396
Figure 6. 112: Click on the advanced system settings option .....	396
Figure 6. 113: Click on the Change button .....	397
Figure 6. 114: Change the domain to the “group1.com” .....	397
Figure 6. 115: Enter login username and password .....	398
Figure 6. 116: The Welcome notification will be pop out when login success. ....	398

**LIST OF TABLES**

Table 2. 1: Windows Server requirement .....	7
Table 2. 2: Ubuntu Server Requirement .....	8
Table 2. 3: Windows Specification .....	9
Table 2. 4: Ubuntu server specification .....	10

## CHAPTER 1: INTRODUCTION

### 1.1 INTRODUCTION

This Workshop II (BITU 3923) is introduced to all third year Bachelor Degree students as a platform to prepare students before undergone their Final Year Project and Industrial Training. During the workshop, students will work in group and they are required to develop a project based on their majoring. Workshop II provides an opportunity to students to practice their knowledge and experience gained from previous subjects learned before. This project required the student to prepare, analyze, design, built, manage, maintain and test the network. It will also train students to work in a group and solve the problems that arise together similar to the actual environment in industry which emphasize on being a good team and practice critical thinking.

The main objectives for this Workshop 2 are, student should be able to design the network infrastructure by using the available tools and be able to implement designated network services also to install and integrate network services infrastructure to suit the network environment while maintaining and controlling the network services infrastructure. The group for the Workshop 2 consists of 8 students, 5 students from BITC and 3 students from BITZ. We have been provided with the equipment which are 3 servers, 1 NIC, 1 router, 1 manageable switch, 15 meters UTP cable, 12 pieces of RJ-45, 1 access-point and 1 set of crimping tools.

14 network services and 16 security services are required to be implemented in the network infrastructure. Three operating systems are used in the servers which are Microsoft Windows Server 2008 and Ubuntu Server 16.04. After the network is up to service, we need to ensure our domain can communicate with others group's domain.

## **1.2 OBJECTIVE**

1. To develop and configured the network with more than 30 services including 14 services of network infrastructure and 16 services on security services which are necessary.
2. To drafts Security Policy for security purposes and also maintain the network services infrastructures.
3. To utilize different kind of Operating System (OS) such as Windows, Linux or others that suit in the network environment.

### 1.3 PROJECT PLAN

In week 1 and week 2, we will be assigned to the respective supervisors. Then, we borrow the equipment needed such as router, switch and servers from the faculty. We will prepare the project proposal that includes the details of the project such as the executive summary, logical and physical network design to show the network topology, Gantt chart is developed to show the timeline of the project and project distribution where the project manager will distribute the tasks to all the members accordingly. We will submit the finalized proposal by the end of week 2. After the submission of the project proposal, we will proceed to set up the services needed for this project. There are 5 services that we plan to install during this period. The services include VLAN, IPv6, DNS, DHCP and the service for video. We will prepare the Progress Report I that will consists of the details of the setup and installation of the services. Then, we will submit the finalized Progress Report I that has been approved by the end of week 5.

From week 6 to week 10, we plan to proceed to set up the 25 other services. The examples are setting up IPsec between server and user, proxy server, install Samba Security services, set up web, SSL and virtual hosting and radius server for network accounting. We will prepare the Progress Report II that consists of the setup details of the 25 services. Then, we will submit the finalized Progress Report II that has been approved by the end of week 10.

During week 11 to week 12, we will proceed towards completing the setup of the whole network and setup of all services required. At the same time, we will prepare a video and a poster based on our project title Domain Name Server. After the completion of the network setup, we will demonstrate our respective task individually to the supervisor and evaluator.

At week 13, the final report and individual log book will be revised if there is any error and improved. At week 14, the video and poster produced during week 11 to week 12 will be used in the video and poster exhibition. The completed video and poster will be evaluated by the supervisors and evaluator. The finalized final report and individual log book will be submitted during study week which is equivalent to week 15.

#### **1.4 CONCLUSION**

Upon the completion of workshop II, we are able to install, configure, set up, monitor and maintain a complete network given the necessary network equipment and services. We are also exposed to different operating system environment. We should be able to design our own network and maintain a good network environment. Moreover, we will learn to build up a crucial security system to secure and protect the network from being attacked and compromised. Besides, we will be able to apply teamwork and project management skills in the future. All of these are the basic requirements that prepare us for the real working environment. In addition, we can apply our knowledge we gained in class through practical and find out our weaknesses and improve them. Finally, we can gain extra knowledge, experience and confidence to face the future challenges in final year project and industrial training.

## CHAPTER 2: PROJECT REQUIREMENT

### 2.1 INTRODUCTION

In this workshop, we have been provided with the equipment which are three servers, 1 Cisco 1941 router, one Cisco 2960 manageable switch, 15 meters UTP cable, 12 pieces of RJ45, one access-point and one set crimping tool.

By using the equipment above, we are required to design, set up, maintain and monitor a network environment with basic server applications and fundamental services. 14 network services and 16 security services are required to implement in the network infrastructure.

We are also required to use different operating system for servers. The operating systems used in the servers are Windows Server 2008 R2 and Ubuntu Server 16.04. We will explain our selection in next section.

### 2.2 TYPES OF OPERATING SYSTEM

We choose the most popular operating system in the industry to get ourselves familiar for future career. Among these OSs, the most popular ones are Windows and UNIX. (W3Tech, 2015) Therefore, we choose Windows Server 2008 R2 and Ubuntu 16.04.

### 2.3 OPERATING SYSTEM BACKGROUND

#### 2.3.1 WINDOWS SERVER 2008 R2

Windows Server 2008 is a release of Microsoft Windows server line of operating system in 2008. It is the successor to Windows Server 2003. Like

Windows Vista, Windows Server 2008 is built on the Windows NT 6.0 kernel. The main features of Windows Server 2008 including server core, active directory roles, Windows Power Shell (Command Line Shell) and terminal services and so on.

### **2.3.2 UBUNTU 16.04**

Ubuntu is a Debian-based Linux operating system for personal computers, tablets and smartphones, where Ubuntu Touch edition is used; and also runs network servers, usually with the Ubuntu Server edition, either on physical or virtual servers. Ubuntu 16.04 runs on all major architectures – x86, x86-64, ARM v7, ARM64, POWER8 and IBM System z mainframes via LinuxONE. (Ubuntu.com, 2016)

## **2.4 OPERATING SYSTEM JUSTIFICATION**

### **2.4.1 WINDOWS SRVER 2008 R2**

In Workshop II, we decided to use Windows Server 2008. This is because this edition supplies all the features and tools provided by the standard edition such as:

- Full-function server operating system. It automatically comes with most of the technical, security, management and administrative features such as the rewritten networking stack (native IPv6, native wireless, security improvements and speed). It improved image-based installation, deployment and recovery and also improved reporting tools, monitoring, event logging and diagnostic. Have new security features such as Bit Locker and ASLR.

- Improved Windows Firewall with secure default configuration, Windows Workflow Foundation and the core kernel, memory and file system improvements.

Requirement	
Processor	Minimum: 1GHz (x86 processor) or 1.4GHz (x64 processor)  Recommended: 2GHz or faster
Memory	Minimum: 512MB RAM  Recommended: 2GHz or faster  Maximum: 2TB
Disk Space	Minimum: 10GB  Recommended: 40GB or greater
Drive	DVD-ROM drive

Table 2. 1: Windows Server requirement

#### 2.4.2 UBUNTU 16.04

We use Ubuntu 16.04 because is an open source operating system software for computers. It is one of the distribution systems of Linux, and is based on the Debian architecture. It is usually run on network servers, usually running the Ubuntu server variant, with enterprise-class features. Ubuntu operates under the GNU General Public License (GPL) and all of the application software installed by the default is free software.

Requirement	
Processor	Minimum: 1GHz Recommended: Faster
Memory	Minimum: 1GB RAM Recommended: Faster Maximum: 2TB
Disk Space	Minimum: 10GB Recommended: 40GB or greater
Drive	CD and DVD-ROM drive

Table 2. 2: Ubuntu Server Requirement

## 2.5 HARDWARE REQUIREMENT

In this workshop, we have been provided with the equipment which are three servers, one Cisco 1941 router, one Cisco 2960 manageable switch, 15 meters UTP cable, 12 pieces of RJ45, one access-point and one set crimping tool. These hardware are required to complete the workshop. Because the equipment are not new, therefore several preparations have been taken before we start the configuration. For servers, we format the hard drive. Meanwhile for router and switch, we erase the configuration.

## 2.6 HARDWARE JUSTIFICATION

### 2.6.1 WINDOWS SERVER

The hardware specification of Windows Server is shown as table below.

Brand	Dell Optiplex 7010
CPU	Intel Core i7-4790 @3.60GHz
RAM	32GB 1600MHz DDR3 SDRAM
HDD	1TB 7200rpm HDD
Display adapter	Intel HD Graphics 4000 Dynamic Video Memory Technology 5.0

Table 2. 3: Windows Specification

This computer has the best hardware specification among all computers. We reserve this for Windows Server as Windows Server 2008 requires more processing power than Linux OS.

### 2.6.2 UBUNTU SERVER

The hardware specification of Ubuntu Server is shown as table below.

Brand	Dell Optiplex 7010
CPU	Intel Core i5-3470 @3.20GHz
RAM	4GB 1600MHz DDR3 SDRAM
HDD	160GB 7200rpm HDD

Display adapter	Intel HD Graphics 4000 Dynamic Video Memory Technology 5.0
-----------------	--

Table 2. 4: Ubuntu server specification

This computer has decent CPU, more-than-enough amount of RAM but limited HDD capacity. Thus, we select this computer to be used as Ubuntu Server because it will run heavy programs such as email server, network management system and intrusion detection system.

### **2.6.3 ROUTER**

The Cisco 1941 Integrated Services Router (ISR) delivers highly secure data, mobility, and application services. Key features include:

- 2 integrated 10/100/1000 Ethernet port
- 2 enhanced High-Speed WAN Interface Card slots that can host 2 single wide or 1 double wide and 1 single wide (e)HWIC
- 1 Internal Services Module slot
- Fully integrated power distribution to modules supporting 802.3af Power over Ethernet (PoE) and Cisco Enhanced PoE

#### Security

- Embedded hardware-accelerated VPN encryption
- Secure collaborative communications with Group Encrypted Transport VPN, Dynamic Multipoint VPN, or Enhanced Easy VPN

- Integrated threat control using Cisco IOS Firewall, Cisco IOS Zone-Based Firewall, Cisco IOS IPS, and Cisco IOS Content Filtering
- Identity management that uses authentication, authorization, and accounting (AAA), and public key infrastructure



Figure 2. 1: Cisco 1941 Router

#### 2.6.4 SWITCH

Cisco Catalyst 2960 Series Intelligent Ethernet switches are a new family of fixed-configuration standalone devices that provide desktop 10/100 Fast Ethernet and 10/100/1000 Gigabit Ethernet connectivity, enabling enhanced LAN services for entry-level enterprise, mid-market, and branch office networks. The Cisco Catalyst 2960 Series offers integrated security, including network admission control (NAC), advanced quality of service (QoS), and resiliency to deliver intelligent services for the network edge.



Figure 2. 2: Cisco Catalyst 2960 Switch

### 2.6.5 UTP CABLE

15 meters of UTP cable is provided to allow us connected all the network peripherals. Some calculation should be made in order to estimate the length of each cable, and also to prevent insufficiency happens.



Figure 2. 3: UTP cable

### 2.6.6 RJ-45

12 pieces of RJ45 is given in this workshop. RJ45 is an 8-pin plug commonly used to connect computers onto Ethernet-based local area networks (LAN).



Figure 2. 4: RJ-45 Connector

## 2.6.7 CRIMPING TOOL

A crimping tool is a device used to affixing a connector to the end of a cable.

When crimping the cable, we have to decide which cable type we should use: straight through or crossover. When the cable is used to connect two devices at different network layer e.g. switch to router, we should use straight through cable. When we connect two devices at same network layer, e.g. switch to switch, we should use crossover cable.

A cable tester is also provided to ensure the cable is functional.

## 2.6.8 LINKSYS ACCESS-POINT (WRT1900AC-ME)

The new Linksys WRT1900AC has a design that is clearly meant to evoke the WRT54G, but it's a whole new beast. It had 16 megs of RAM and 4 megs of Flash. Compare that to the WRT1900AC with its dual-core 1.2Ghz ARM processor with 256 megs of DDR3.



Figure 2. 5: Linksys access point

## 2.7 CONCLUSION

As the conclusion, before installing Operating System, one should ensure that the computer meet the requirements. It can be complicated to integrate three different types of Operating System with more than 30 different services and configuration in a network infrastructure. We have to consider the compatibility and performance of the server and decide which service belong to which server. We also have to minimize the effect to the network if one of the hardware is down. After all these consideration, we would expect a secured network infrastructure with good performance and minimum downtime.

## CHAPTER 3: DESIGN

### 3.1 INTRODUCTION

In this chapter, we will explain about the design of security policy, physical network and logical network. Design phase is very crucial in the development process. If we proceed to implementation phase and only found that the design does not meet the requirement, our progress will be behind the schedule. Therefore, a good design must not only be organized, artful, more importantly it had to be possible to achieve and meet the requirement.

Every group need to implement their own network design which is needed to be applied in real device. Our group already designs the networks that have two clients that are from internal and external. We have been supplied with RJ-45, UTP cable, console cable and a set of crimping tools. We also required using different operating system to set the network environment. The NOS we choose to install into HP platform is Window Server 2008 R2 and Ubuntu 16.04 LTS.

### **3.2 SECURITY POLICY**

#### **3.2.1 Password Protection Policy**

##### **3.2.1.1 Password Creation**

- All user-level and system-level password must conform to the Password Construction Guideline.
- Password of administrator and client must not be same.
- Build strong password which include character, symbols numbers and contain more or equal 8 characters.

##### **3.2.1.2 Password Protection**

- Password must not be inserted into email message or other forms of electronic communication.
- Password must not be revealed over the phone to anyone.
- Do not reveal or share group password with anyone, including administrative assistant, secretaries, managers, co-workers and family members.
- Do not reveal a password on questionnaire or security forms.
- Do not write password down and store them in a file on a computer system or mobile devices or anywhere without encryption.
- Do not use the “Remember Password” feature of application.
- Any user that suspect may have been compromised his/her must report the incident and change all password.

#### **3.2.2 Server Security Policy**

##### **3.2.2.1 General Requirement**

- All internal servers deployed at Group 13 must be owned by an operational group that is responsible for system administration.
- Approved server configuration must be established and maintained by each operational group.
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management producers.
- Compliance and maintenance purpose, authorized personnel may monitor and audit equipment, systems, processes and network traffic.
- Firewalls will used to filter and block unauthorized access while permitting outward communication.

### 3.2.2.2 Configuration Requirement

- Services and applications that will not be used must be disabled where practical.
- Always use standard security principles of least required access to perform a function.
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.
- Installing the most updated security patches as soon as practically that only exception being immediate application would interfere with business requirements.

### 3.2.3 Physical Security

#### 3.2.3.1 Computer

- Each unit of computer must be inventoried before being put into service.

Inventory list shall be available to all System Administrator

- Computer shall be distinctly and uniquely identified on all visible sides.

Machines shall be housed in secured facilities (caged or locked)

#### 3.2.3.2 Media

- Provisioning where storage media (disk drives, tapes and removable media are inventoried upon acquisition and tracked in their use).
- New storage media whether disk or removable shall be secured erased and formatted before use.

#### 3.2.3.3 Physical Access

- At least two authorized persons for access must be on site at the same time for physical access for granted based the principle of dual control.
- Access Logging (All physical accesses are logged and reported to all).
- Access Authorization (Access to physical equipment must be authorized).

### 3.2.4 Network Security

#### 3.2.4.1 Router and Switch Security Policy

- All routing updates shall be done using secure routing updates.
- Enabling password must be kept in a secure encrypted form. The router or switch must have enable password set to the current production router or switch password from device's support organization.

- No local user accounts are configured on the router. Only administrator can access to the router.
- The enable secret password on the router must be kept in a secure encrypted form.
- Intrusion detection system will used to monitor suspicious packet.

### 3.2.5 Application Security

#### 3.2.5.1 File System Permission

- The server access governed by firewall appliances and software.

### 3.3 PHYSICAL DESIGN

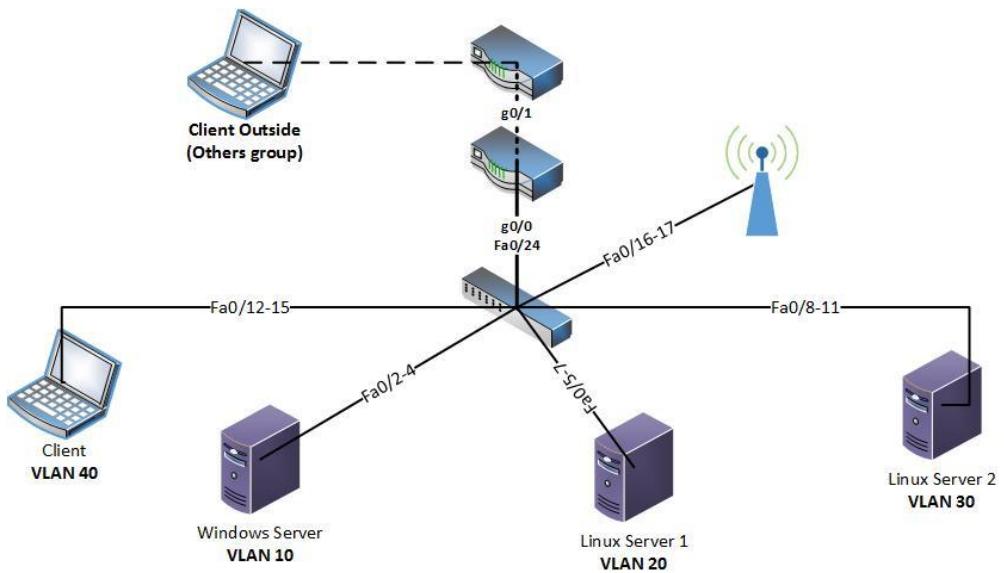


Figure 3. 1: Physical design

### 3.4 LOGICAL DESIGN (INCLUDING SECURITY DESIGN)

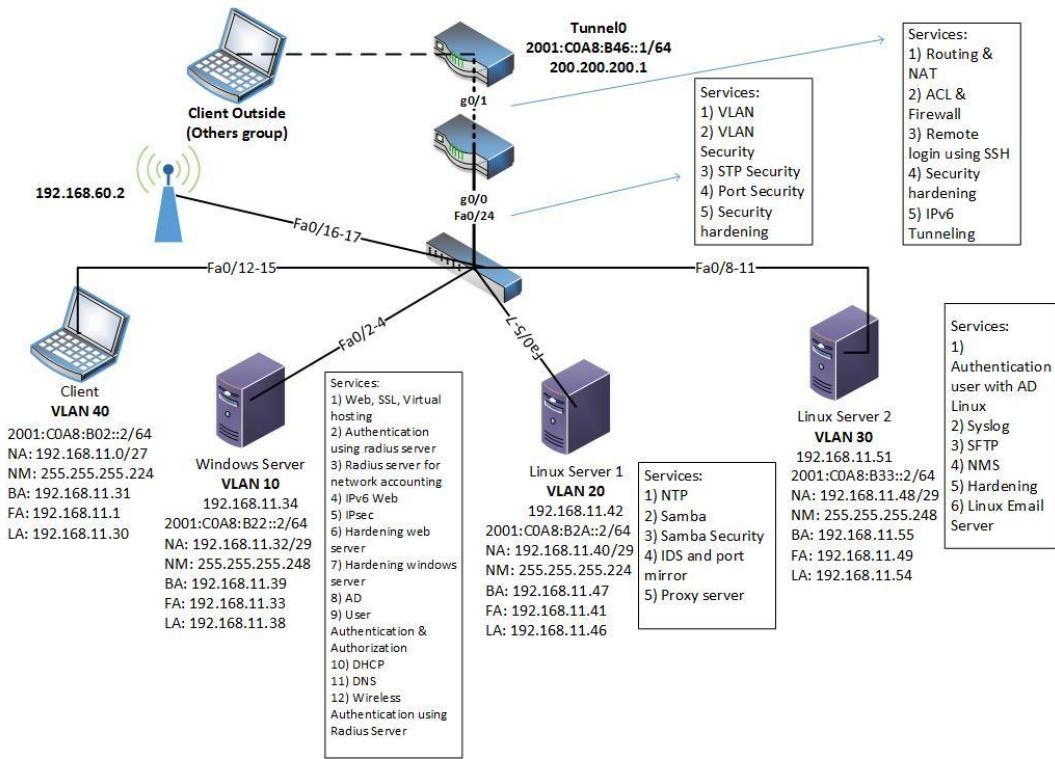


Figure 3. 2: Logical design

### **3.5 CONCLUSION**

These designs have been approved by supervisor to ensure it meets the requirements. A lot of concerns have been considered during the design such as IP addressing, VLAN segregation. Advice from reliable sources such as lecturers helped us a lot in making decision. We will proceed to next phase with our designs.

## CHAPTER 4: SERVICES

### 4.1 INTRODUCTION

In this chapter, we will provide a list of services we are going to implement.

Also, we will describe a brief overview for each service.

### 4.2 LIST OF SERVICES

1. Domain Name Service (DNS)
2. Dynamic Host Configuration Protocol (DHCP)
3. Routing & Network Address Translation (NAT)
4. Virtual LAN (VLAN)
5. IPv6 Transition Mechanism
6. Web, Secure Socket Layer (SSL), Virtual Hosting
7. IPv6 Web
8. Secure File Transfer Protocol
9. Samba
10. Proxy Server
11. RADIUS Server for Network Accounting
12. Linux Email Server
13. Network Management System
14. Access Control List (ACL)
15. Security Hardening
16. Authentication Using RADIUS Server
17. User Authentication and Authorization1
18. Firewall for Router

19. Remote Login Using SSH
20. Hardening Linux Server
21. Hardening Windows Server
22. Hardening Web Server
23. Authentication User by Integrating Active Directory with Linux
24. Intrusion Detection System with Port Mirroring
25. IPSec Between Server and User
26. Samba Security Services
27. Port Security
28. Spanning Tree Protocol (STP) Security
29. VLAN Security
30. Network Time Protocol (NTP)
31. Syslog
32. Wireless Authentication Using Radius Server
33. Active Directory

## 4.3 BRIEF OVERVIEW FOR SERVICES

### 4.3.1 DOMAIN NAME SERVER (DNS)

Domain Name Servers (DNS) is a hierarchical decentralized naming system for computers, services, or any resource connected to the private network. It maintains a directory of domain names and translates them to Internet Protocol (IP) addresses. This is necessary because, although domain names are easy for people to remember, computers or machines, access websites based on IP addresses. Information from all the domain name servers across the Internet are gathered together and housed at the Central Registry. Host companies and Internet Service Providers interact with the Central Registry on a regular schedule to get updated DNS information. It serves as the phone book for the Internet by translating human-friendly computer hostname into IP addresses. For example, the domain name translates to the addresses 192.168.12.34 (IPv4) – group12.com and 2001:a::2 (ipv6) – group12.ipv6.com. DNS can be quickly updated, allowing a service's location on the network to change without affecting the end users, who continue to use the same host name. Users take advantage of this when they use meaningful Uniform Resource Locations (URLs) and e-mail address without having to know how the computer locates the services.

### 4.3.2 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. RFCs 2131 and 2132 define DHCP as an Internet Engineering Task Force (IETF)

standard based on Bootstrap Protocol (BOOTP), a protocol with which DHCP shares many implementation details. DHCP allows hosts to obtain required TCP/IP configuration information from a DHCP server.

Benefit of DHCP:

- Reliable IP address configuration. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.
- Reduced network administration. DHCP includes the following features to reduce network administration:
  - Centralized and automated TCP/IP configuration.
  - The ability to define TCP/IP configurations from a central location.
  - The ability to assign a full range of additional TCP/IP configuration values by means of DHCP options.
- The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable computers that move to different locations on a wireless network.
- The forwarding of initial DHCP messages by using a DHCP relay agent, which eliminates the need for a DHCP server on every subnet.

#### **4.3.3 ROUTING & NETWORK ADDRESS TRANSLATION (NAT)**

##### **Routing**

In internetworking, routing means the process of moving a packet of data from source to destination that is usually performed by a dedicated device called a router. Routing is the process of selecting paths in a network along which to send network traffic. Routing is performed for many kinds of networks. In packet switching networks, routing directs packet forwarding, the transit of logically addressed packets from their source toward their ultimate destination through intermediate nodes. The routing process directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations. Routing is a key feature of the Internet because it enables messages to pass from one computer to another and eventually reach the target machine. Each intermediary computer performs routing by passing along the message to the next computer. Part of this process involves analyzing a routing table to determine the best path.

## NAT

A NAT (Network Address Translation or Network Address Translator) is the virtualization of Internet Protocol (IP) addresses. NAT helps improve security and decrease the number of IP addresses an organization needs. NAT translates the internal IP address of the client to an external address. To outside users, all traffic coming to and going from the network has the same IP address or is from the same pool of addresses. The most common form of network translation involves a large private network using addresses in a private range (10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, or 192.168.0.0 to 192.168.255.255). The private addressing scheme works well for computers that only have to access resources inside the network, like workstations needing access to file servers and printers. Routers inside the private network can route

traffic between private addresses with no trouble. However, to access resources outside the network, like the Internet, these computers have to have a public address in order for responses to their requests to return to them. This is where NAT comes into play.

#### **4.3.4 VIRTUAL LOCAL AREA NETWORK (VLAN)**

VLAN, Virtual Local Area Network or Virtual LAN is concept of partitioning a physical network. VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. VLANs allow network administrators to partition their networks to match the functional and security requirements of their systems without having to run new cables or make major changes in their current network infrastructure. By default, systems on one VLAN don't see the traffic associated with systems on other VLANs on the same network

#### **4.3.5 IPV6 TRANSITION MECHANISM**

Currently, the Internet consists of native IPv4 (IPv4-only), native IPv6, and IPv4/IPv6 dual networks. Unfortunately, IPv4 and IPv6 are incompatible protocols. When both IP versions are available and the users of Internet want to connect without any restrictions, a transition mechanism is required. During the time of migration from IPv4 to IPv6 networks, a number of transition mechanisms have been proposed by IETF to ensure smooth, stepwise and independent changeover

IPv6 Transition Mechanism is a technology that facilitates the transitioning of the Internet from the Internet Protocol version 4 (IPv4) to the successor addressing and routing system of Internet Protocol Version 6 (IPv6). As IPv4 and IPv6 networks are not directly interoperable, transition technologies are designed to permit hosts on either network type to communicate with any other host.

#### **4.3.6 WEB, SECURE SOCKETS LAYER (SSL) & VIRTUAL HOSTING**

Web server is a computer that delivers (serves up) Web pages. A Web server is also known as an Internet server. A Web server is a system that delivers content or services to end users over the Internet. A Web server consists of a physical server, server operating system (OS) and software used to facilitate HTTP communication.

SSL (Secure Sockets Layer) is a standard security technology for establishing an encrypted link between a server and a client that are typically a web server (website) and a browser, or a mail server and a mail client. Normally, data sent between browsers and web servers is sent in plain text. SSL is a security protocol that describes how algorithms should be used.

Virtual Hosting is a method that servers such as web servers use to host more than one domain name on the same computer, sometimes on the same IP address. Virtual hosting is the act of using a remote hosting service provider to host websites, data, applications and/or services. These services will be installed in Windows Server.

#### **4.3.7 IPV6 WEB**

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP). The most obvious improvement in IPv6 is that IP addresses are lengthened from 32 bits to 128 bits. The main purpose of the IPv6 is as a backup plan when there are no IPv4 left available to be used by a device.

The tool used for this service is Internet Information services (IIS) Manager.

#### **4.3.8 SECURE FILE TRANSFER PROTOCOL (SFTP)**

SFTP is a secure version of file transfer protocol. The SFTP functionally similar as FTP but it can provide secure for data access and files transfer or other data over a network connection by using the Secure Shell (SSH) protocol. SFTP need the client should be authenticated first by the server, then the data transfer must take place over a SSH protocol. Normally SFTP may authenticate them using the form of a username and password and it will hides and encrypt the data for secure transmission. SFTP will ensure all data will be encrypt before them being sent through a network. Tool suggested: FileZilla 3.14.

#### **4.3.9 SAMBA**

Samba is an Open Source suite of Unix applications that consist of 2 key programs which is smbd and nmbd to implement the CIFS services including the file and print services, authentication and authorization, name resolution and service announcement. Samba is freely available under the GNU

General Public License. Samba runs on Unix platforms, but speaks to Windows clients like a native. It allows a Unix system to move into a Windows “Network Neighborhood” without causing a stir. Windows users can happily access file and print services without knowing or caring that those services are being offered by a Unix host. All of this is managed through a protocol suite which is currently known as the “Common Internet File System” or CIFS. Samba speak using Server Message Block (SMB) protocol for Microsoft Windows Operating system perform client server networking for file and printer sharing.

Tool: samba version 3.0.11.

#### **4.3.10 PROXY SERVER**

A proxy server is a computer that offers a computer network service to allow clients to make indirect network connections to other network services. A client connects to the proxy server, then requests a connection, file, or other resource available on a different server. The proxy provides the resource either by connecting to the specified server or by serving it from a cache. In some cases, the proxy may alter the client's request or the server's response for various purposes. The tool suggested for this service is Squid 3.

Type of proxy server:

- Transparent Proxy
  - This type of proxy server identifies itself as a proxy server and also makes the original IP address available through the http headers.

These are generally used for their ability to cache websites and do not effectively provide any anonymity to those who use them.

- Anonymous Proxy
  - This type of proxy server identifies itself as a proxy server, but does not make the original IP address available. This type of proxy server is detectable, but provides reasonable anonymity for most users.
- Distorting Proxy
  - This type of proxy server identifies itself as a proxy server, but make an incorrect original IP address available through the http headers.
- High Anonymity Proxy

This type of proxy server does not identify itself as a proxy server and does not make available the original IP address.

#### **4.3.11 RADIUS SERVER FOR NETWORK ACCOUNTING**

- Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.
- The accounting function in RADIUS allows data to be sent at the start and end of the sessions, showing the amount of resources used during the session.
- An Internet Service Provider may use RADIUS access control and accounting software to meet special security and billing needs, statistical purposes and general network monitoring.
- Tool used: NPS

#### **4.3.12 LINUX EMAIL SERVER**

Message transfer agent software that transfers electronic mail messages from one computer to another using client–server application architecture. An MTA implements both the client (sending) and server (receiving) portions of the Simple Mail Transfer Protocol. There are many tools can be used for this service: Postfix, Dovecot, Thunderbird, Outlook 2010/2013.

The major functions of an MTA are:

- Accepting messages originating from the user agent and forwarding them to their destination (other user agents)
- Receiving all messages that are transmitted from other user agents for further transmission
- Keeping track of each and every activity and analyzing and storing the recipient list to perform future routing functions
- Sending auto-responses about non-delivery when a message does not reach its intended destination

#### **4.3.13 NETWORK MANAGEMENT SYSTEM**

Network management is the process of administering and managing the computer networks of one or many organizations. Various services provided by network managers include fault analysis, performance management, provisioning of network and network devices, maintaining the quality of service etc. Software that enables network managers to perform their functions is called network management software. Tool: Nagios Core.

It is responsible to:

- Ensure that the user of a network receive the information technology services with the quality of service than they expect.
- Strategic and tactical planning of the engineering, operations and maintenance of a network and network services.
- Help network engineer to deal with the complexity of a data network and to make sure that data can go across it with maximum efficiency and transparency to the user.

#### **4.3.14 ACCESS CONTROL LIST (ACL)**

ACL is used to prevent certain traffic from entering a network. ACL is a list of flexible permission attached to a system object such as file directory or individual file. The list specifies who is allowed to get access the object and operation are able to be performed on the object. Each system user ability to ability to read a file, to write to the file or files, and to execute the file. At the same time, ACL may able to increase network performance.

#### **4.3.15 SECURITY HARDENING**

The security of all network peripherals is hardened by the following approaches:

- set up password to prevent unauthorized access;
- Disable unused port in switch;

- Enable firewall service on servers.

#### **4.3.16 AUTHENTICATION USING RADIUS SERVER**

Remote Authentication Dial-In Server (RADIUS) is a protocol that uses a centralized Authentication, Authorization and Accounting (AAA) which is used to authenticate remote-access users. The RADIUS server runs on the application layer and uses UDP to transport data. When a user wants to enter the network, he must first authenticate in the RADIUS server. The client device will send a message to the RADIUS server and if the device has been configured as a client by the server, it will send a message whether it accepts or reject the device based on the authentication.

#### **4.3.17 USER AUTHENTICATION AND AUTHORIZATION**

- a. User authentication is a process of verifying that the user is who they claim to be by obtaining some sort of credentials.
- b. User authorization is the process of validating that the user can only perform certain specified actions.
- c. User authentication allows the server to know who exactly is accessing its resources. The user is commonly asked for a username and password during the authentication process. Authentication always proceeds to authorization process.
- d. User authorization allows the server to determine if the user has permission to use access a resource or perform a specific task. Its helps to control the access right by granting or denying specific permission to an authenticated user.

- e. User authentication and authorization protects the server from unwanted third party from accessing or tampering its resource.

#### **4.3.18 FIREWALL FOR ROUTER**

Type of firewall that we have been used is Access Control List(ACLs).

ACLs are widely used in computer networking and in network security for mitigating network attacks and controlling network traffic. Administrators can use ACLs to define and control classes of traffic on networking devices to meet a given set of security requirements.

#### **4.3.19 REMOTE LOGIN USING SSH**

SSH is a stand for secure socket shell. SSH is a network protocol for make secure access to a remote machine over unsecure network. SSH client and server are widely available for most operating system. SSH also provide authentication and secure encrypted data communication between two connected devices over an untrusted network. The encryption may provide confidentiality and integrity of data.

#### **4.3.20 HARDENING LINUX SERVER**

Ubuntu Server may have some security flaw that can be manipulate by intruder to steal information. By applying hardening, it will improve the server security and make the server more secure. Hardened servers make it more

resistant to security issues and threats. Keeping software updated, disable unnecessary service are some of the methods to harden Ubuntu Server.

#### **4.3.21 HARDENING WINDOWS SERVER**

The purpose of hardening is eliminated as many security risks as possible. Techniques to harden systems are protecting accounts with passwords, disabling unnecessary accounts, disabling unnecessary services and protecting management interfaces and application. Hardening the Microsoft Windows Server 2008 R2 operating system reduces the attack surface by disabling functionality that is not required while maintaining the minimum functionality that is required.

#### **4.3.22 HARDENING WEB SERVER**

Security is an essential part of a web application and should be taken into consideration from the first stage of the development process. IIS is responsible for processing requests received on specific ports. For this motive, WWW services run on the machine, which handle and process requests received on various TCP/IP ports, where port 80 is normally assigned to HTTP. First, we harden web server by restrict IP Address on specific address. Then, we secured the web server by activating the authentication.

##### **IP Restriction**

IP restriction enables us to selectively allow or deny access to the files, folder, and website and web server. Custom rules can be built in context of a particular client, or DNS lookup to provision their restriction. When a client who is not permitted access requests a resource, a ‘Forbidden: IP address of the client has been rejected (403.6)’ or ‘DNS name of the client is rejected (403.8)’ HTTP status will be reflected and logged. Moreover, there are two terms introduced by IIS in this scenario which is IP and Domain Restriction.

### **Authentication**

Authentication enables us to selectively allow or deny Windows authentication and anonymous authentication. Whenever the web being accessed, there will be a pop up of authentication box that needed to authenticate by user before having permission to access the website

#### **4.3.23 AUTHENTICATION USER BY INTEGRATING ACTIVE DIRECTORY WITH LINUX**

Active Directory serves as a central location for network administration and security. It is a directory service created by Microsoft for Windows domain. It is responsible for authenticating and authorizing all users and computers within a network of Windows domain type, assigning and enforcing security policies for all computers in a network and installing or updating software on network computers. Server computer that runs Active Directory are called domain controller

For an example, a user login into a computer that has been a part of a Windows domain, then the Active Directory will verifies user's password and specifies whether the users is a system administrator (admin) or normal user(others). Then the AD will lead the user to the specific interface of the windows based on the type of user. Tool suggested: pbis-open-8.3.0.3287.

#### **4.3.24 INTRUSION DETECTION SYSTEM (PORT MIRROR)**

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations to produce report to a Management Station. IDS detect a potential security breach, logs the info and signals an alert on the console and owner.

To ensure that IDS analyses the required or specific data, we mirror the traffic of a switch port or VLAN. For this, we will use the "port mirroring" mechanism which the switch duplicates the traffic on the chosen interface or VLAN and send it to Snort.

Besides, on the IDS system, need at least one network interface to listen to the traffic, but if we can have two network ports, this will be much better as we will able to dedicate one of both for the IDS management and the other one will be configured without IP address just to receive the mirrored (or spanned) traffic. In this case, the IDS management data will not "pollute" the mirrored traffic.

The IDS manager provides a graphical interface for managing security across a distributed network. The IDS module performs network sensing. The

IDS module searches for patterns of misuse by examining either the data portion and/or the header portion of network packets. Content-based attacks derive from the data portion, and context-based attacks derive from the header portion.

#### **4.3.25 IPSEC BETWEEN SERVER AND USER**

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. The purpose of this method is to fulfil security requirements, or simply enhance the security of your application. It allows you to add IP restrictions, and TCP/UDP level encryption to applications which may not otherwise support it. The tool used for this service is: Softener.

#### **4.3.26 SAMBA SECURITY SERVICES**

In Samba, there are two major security modes which are User-level and Share-level. The default setting for the security service is the User-level security where the user can mount multiple shares if the server accepts the user authentication. The client manages multiple authentication by using a UID for each time the user logon.

The Share-level security of the Samba server is where the server only accepts a password without a username. Multiple clients can access the server just by knowing the password and it is very discouraged by the developers of Samba to use share-level security.

Tool: samba version 3.0.11

#### **4.3.27 PORT SECURITY**

Port security is a traffic control service on Cisco switches where the administrator can configure a specified number of MAC addresses that can be used in a single port. The use of port security is to avoid the addition of dumb switches by users who wants to illegally extends the network reach. Port security can be configured with dynamically learned or static MAC addresses to restrict any ingress traffic into the ports. When a registered MAC address connects to the port, the device will have the full bandwidth of the port it is registered to.

#### **4.3.28 SPANNING TREE PROTOCOL (STP) SECURITY**

Spanning Tree Protocol (STP) resolves redundant topologies into loop-free, treelike topologies. When switches are interconnected via multiple paths, STP prevents loops from being formed. An STP loop (or forwarding loops) can occur when the entire network fails because of a hardware failure, a configuration issue, or a network attack. STP loops can be costly, causing

major network outages. The spanning tree protocol prevents the condition known as a bridge loop.

The spanning tree algorithm determines the network (which computer hosts are in which segment) and this data is exchanged using Bridge Protocol Data Units.

#### **4.3.29 VLAN SECURITY**

A virtual LAN (VLAN) is any broadcast domain and isolated in a computer network at the data link layer of OSI model. LAN is an abbreviation of local area network.

To subdivide a network into virtual LANs, one configures a network switch or router. Simpler network device can partition only per physical port (if at all), in which case each VLAN is connected with a dedicated network cable (and VLAN connectivity is limited by the number of hardware ports available). More sophisticated devices can mark packets through IEEE 802.1Q, so that a single interconnect trunking may be used to transport data for multiple VLANs. Since VLANs share bandwidth, a VLAN trunk can use link aggregation and/or quality of service prioritization to route data efficiently.

VLANs allow network administrator to group hosts together even if the hosts are not on the same network switch. This can greatly simplify network design and deployment, because VLAN membership can be configured through software. Without VLANs, grouping hosts according to their resource

needs necessitates the labor of relocating Node (networking) or rewiring data link.

#### **4.3.30 NETWORK TIME PROTOCOL (NTP)**

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

NTP is intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC). It uses the intersection algorithm to select accurate time servers and is designed to mitigate the effects of variable network latency. NTP can usually maintain time to within tens of milliseconds over the public Internet, and can achieve better than one millisecond accuracy in local area networks under ideal conditions. Asymmetric routes and network congestion can cause errors of 100ms or more.

The protocol is usually described in terms of a client-server model, but can as easily be used in peer-to-peer relationships where both peers consider the other to be a potential time source. Implementations send and receive timestamps using the User Datagram Protocol (UDP) on port number 123. They can also use broadcasting or multicasting, where clients passively listen to time updates after an initial round-trip calibrating exchange.

#### **4.3.31 SYSLOG**

In computing, syslog is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity label.

Computer system designers may use syslog for system management and security auditing as well as general informational, analysis, and debugging messages. A wide variety of devices, such as printers, routers, and message receivers across many platforms use the syslog standard. This permits the consolidation of logging data from different types of systems in a central repository. Implementations of syslog exist for many operating systems.

#### **4.3.32 WIRELESS AUTHENTICATION USING RADIUS SERVER**

Wireless connectivity offers users a high degree of mobility and provides another networking option when traditional wired networks are impractical. The Windows Server® 2008 operating system provides the networking services needed to deploy a secure and manageable wireless local area network (WLAN) infrastructure within networks ranging from small business to an enterprise environment. This guide provides comprehensive guidance to deploy an 802.1X authenticated wireless access solution.

Wireless networks can provide the following benefits:

- A cost-efficient network deployment alternative. Installing a wireless network can be easier, less time consuming, and is frequently less expensive to install than a wired network because it eliminates the need to run Ethernet cable through walls and ceilings.
- A means to scale your client access resources with agility. Compared to a wired network, it is relatively easy to expand or decrease the size of a wireless network by adding or removing wireless APs. By contrast, to expand service in a wired network typically requires the installation of additional network switches or hubs as well as installing cable.
- The elimination of recurring telecommunications charges. To connect the networks in two buildings separated by a physical, legal, or financial obstacle, you can either use a link provided by a telecommunications vendor (for a fixed installation cost and ongoing recurring costs), or you can create a point-to-point wireless link by using WLAN technology (for a fixed installation cost but no recurring costs).
- The availability of network resources without the constraints associated with connecting client computers directly to the wired network. Some kinds of buildings, such as historical buildings, might be governed by building codes that prohibit the use of wiring, making wireless networking an important alternative. Additionally, a WLAN lets you extend your network into areas that cannot be easily included in the wired network; examples include courtyards and cafeterias.

### **4.3 CONCLUSION**

Through this chapter, we understand about the services we are going to implement. It allows us to get a clearer picture on each service. These services are common in industry. Thus, it will be helpful for us to have some basic knowledge and understanding before going to industrial training.

## **CHAPTER 5: INSTALLATION AND CONFIGURATION**

### **5.1 INTRODUCTION**

In this chapter, we introduce the list of person-in-charge and their corresponding services. Also, the service installation and configuration will be explained in detail.

### **5.2 SERVICES AND CORRESPONDING PERSON-IN CHARGE**

Our group consists of 8 members. Every member has been assigned different part of services from the 33 services provided. Project manager of our group, Tan Seow Wei is responsible to divide the task among the 8 members. Table below shows the task division:

<b>NAME</b>	<b>SERVICES</b>
MOHD FITRI AMRI BIN  JAAFAR	PROXY SERVER
	LINUX EMAIL SERVER
	IPV6 WEB
	ROUTING & NAT
CHAI ROU YIH	DHCP
	PORT SECURITY
	USER AUTHENTICATION & AUTHORIZATION
	VLAN SECURITY

MOHAMAD ASHRAF FIRDAUS CIN MAT ZAIN	WEB, SSL & VIRTUAL HOSTING
	SAMBA SECURITY SERVICE
	REMOTE LOGIN USING SSH
	SAMBA
TAN SEOW WEI	HARDENING WEB SERVER
	RADIUS SERVER FOR NETWORK ACCOUNTING
	VLAN, IPV6 TRANSITION MECHANISM
	NTP
NOOR AINI BINTI SHAHINE	NMS
	STP SECURITY
	AUTHENTICATION USER BY INTEGRATING AD WITH LINUX
	IDS & PORT MIRROR
SITI ZULAIHA BINTI KHASNAN	DNS
	IPSEC BETWEEN SERVER AND USER
	ACTIVE DIRECTORY
	SFTP

NUR SYAHIRAH BINTI MOHAMAD RAFEE	ACL
	HARDENING LINUX SERVER
	HARDENING WINDOWS SERVER
MUHAMMAD SYUKUR BIN SHARIFF	AUTHENTICATION USING RADIUS SERVER
	SECURITY HARDENING
	SYSLOG
	WIRELESS AUTHENTICATION USING RADIUS SERVER

## 5.3 SERVICE INSTALLATION AND CONFIGURATION

### 5.3.1 DOMAIN NAME SERVER (DNS)

Step 1: Click Start and click Server Manager

The Server Manager main window lets us view a detailed snapshot of the server's identity information, selected security configuration options, and installed roles and features.

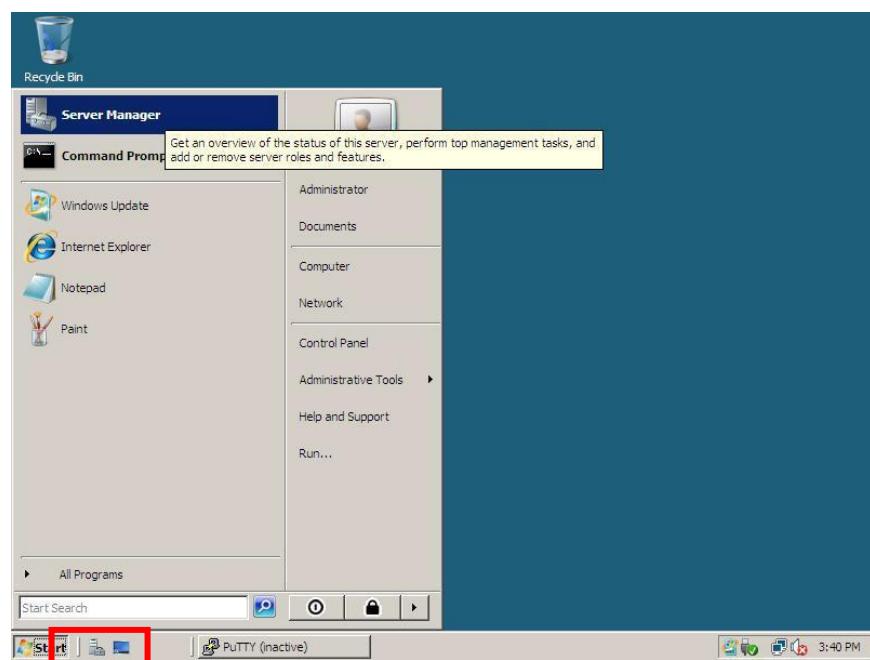


Figure 5. 1: Server Manager

Step 2: Right click on Roles and click Add Roles.

The Roles Summary area of the Server Manager main window shows a list of all roles that are installed on the computer. The names of roles installed on the computer are displayed.

To install additional roles, or remove existing roles, click the appropriate command in the right's side margin of the Roles Summary area.

In the Roles Summary or Features Summary areas of the Server Manager main window, click either Add Roles or Add Features, depending on the software that we want to install.

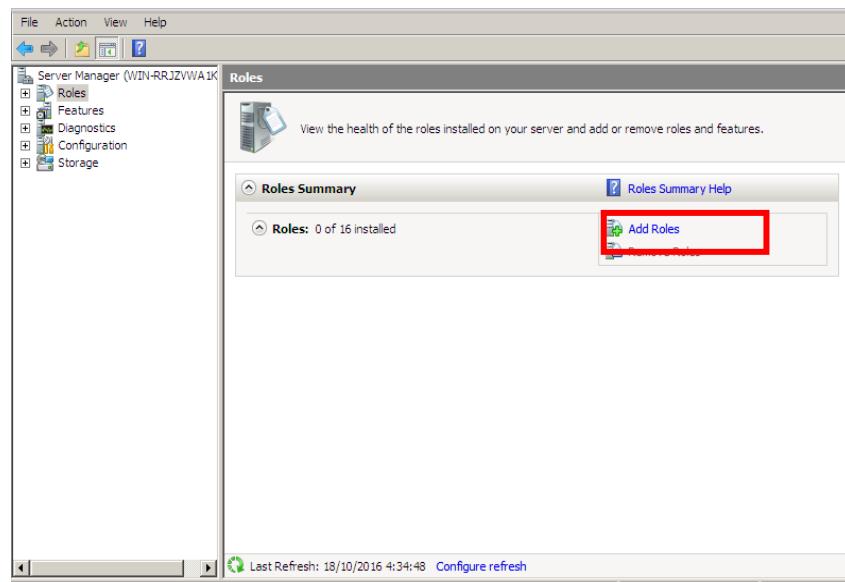


Figure 5. 2: Add Roles

Step 3: In the Add Roles Wizard, if the page Before You Begin appears, click next.

On the Before you begin page, verify that our destination server and network environment are prepared for the role and feature we want to install. Then, click Next.

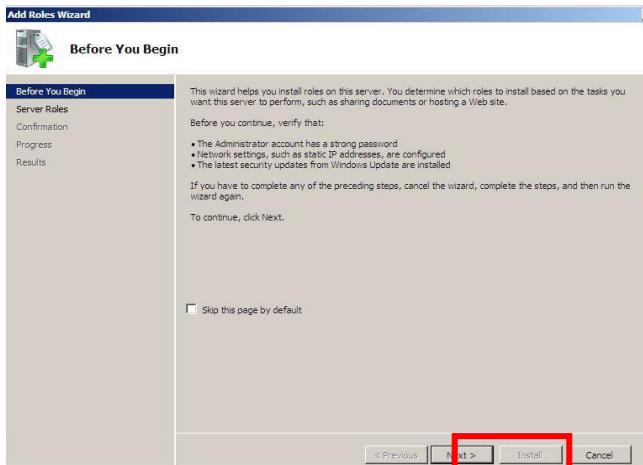


Figure 5. 3: Open Start Manager

Step 4: In the Roles list, click DNS Server, and then click next.

By using the Domain Name System (DNS) server role, we can provide a primary name resolution process for users on our network. The name resolution process enables users to locate computers on the network by querying for a user-friendly computer name instead of an IP address.

We can also integrate the DNS server role with Active Directory Domain Services (AD DS) to store and replicate DNS zones. This makes multimaster replication possible, along with more secure transmission of DNS data.

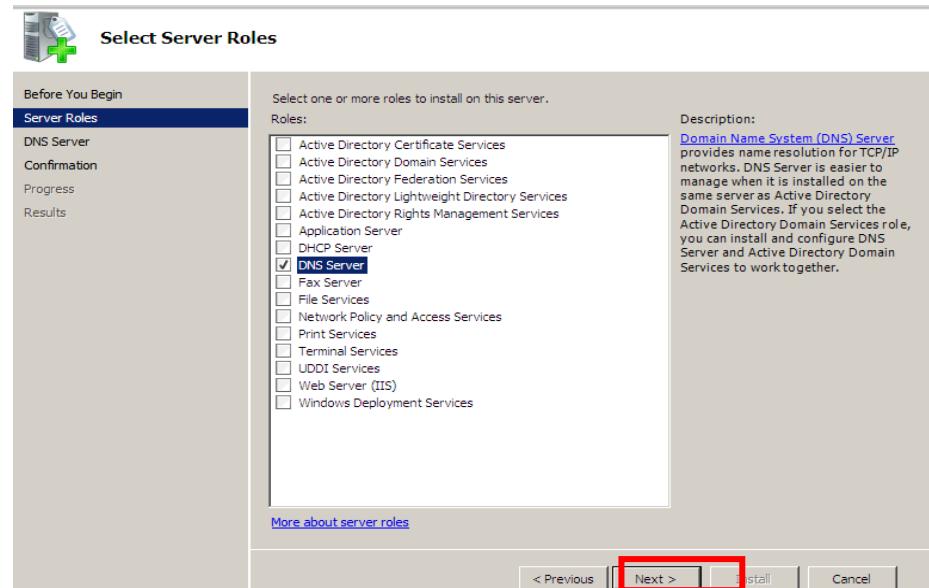


Figure 5. 4: Select Roles

Step 5: Read the information on the DNS Server page, and then click next.

Step 6: On the Confirmation Installation Options page, verify that the DNS Server role will be installed, and then click Install.

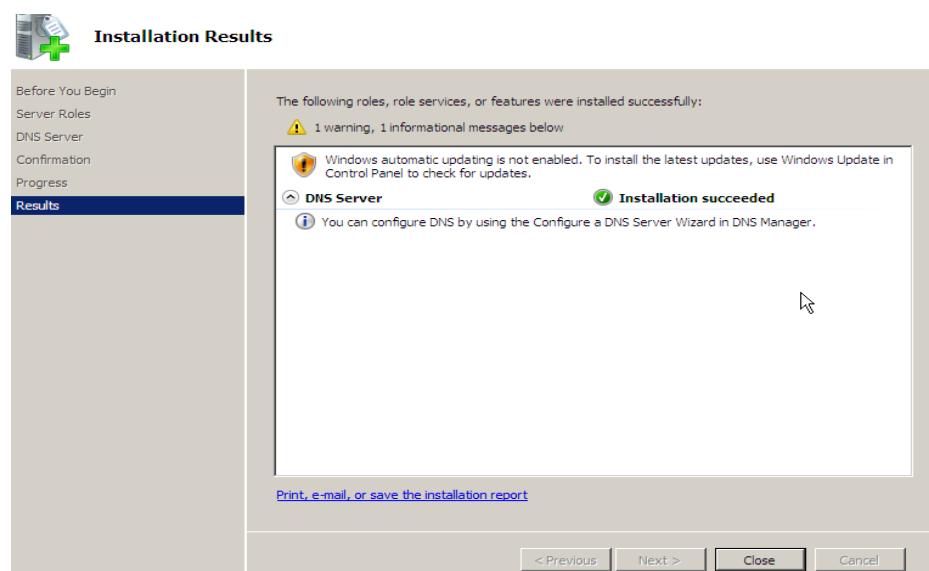


Figure 1 Installation succeeded

Step 7: Choose to add a forward lookup zone. Right click on Forward Lookup Zone and click New Zone. Click next.

Forward lookup zone is using an Internet domain name to find an IP address (convert domain name to IP address). When we enter the address for a web site at our browser (URL), the address is transmitted to router which does a Forward lookup zone to locate the IP address.

We create Forward lookup zone because mostly users can remember domain names rather than IP addresses. However, occasionally you may see a Web page with a URL in which the domain name part is expressed as an IP address (sometimes called a dot address) and want to be able to see its domain name.

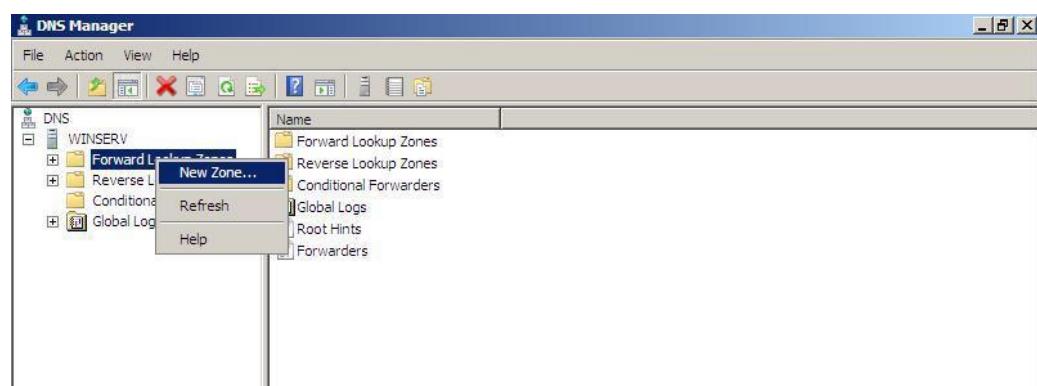


Figure 5. 5: DNS manager

Step 8: In Welcome to the New Zone Wizard page, click next.



Figure 5. 6: New Zone Wizard

Step 9: The new forward lookup zone we choose for Primary Zone and then click next.

The DNS Server service provides for three types of zones:

- Primary zone
- Secondary zone
- Stub zone

We choose primary zone because a primary zone is the only zone type that can be edited or updated because the data in the zone is the original source of the data for all domains in the zone. Updates made to the primary zone are made by the DNS server that is authoritative for the specific primary zone. Users can also back up data from a primary zone to a secondary zone.

A zone contains the resource records for all of the names within the particular zone. Zone files are used if DNS data is not integrated with Active Directory. The zone files contain the DNS database resource records that define the zone.

If DNS and Active Directory are integrated, then DNS data is stored in Active Directory.

When a zone that this DNS server hosts is a primary zone, the DNS server is the primary source for information about this zone, and it stores the master copy of zone data in a local file or in AD DS. When the zone is stored in a file, by default the primary zone file is named group1.com and it is located in the %windir%\System32\DNS folder on the server.

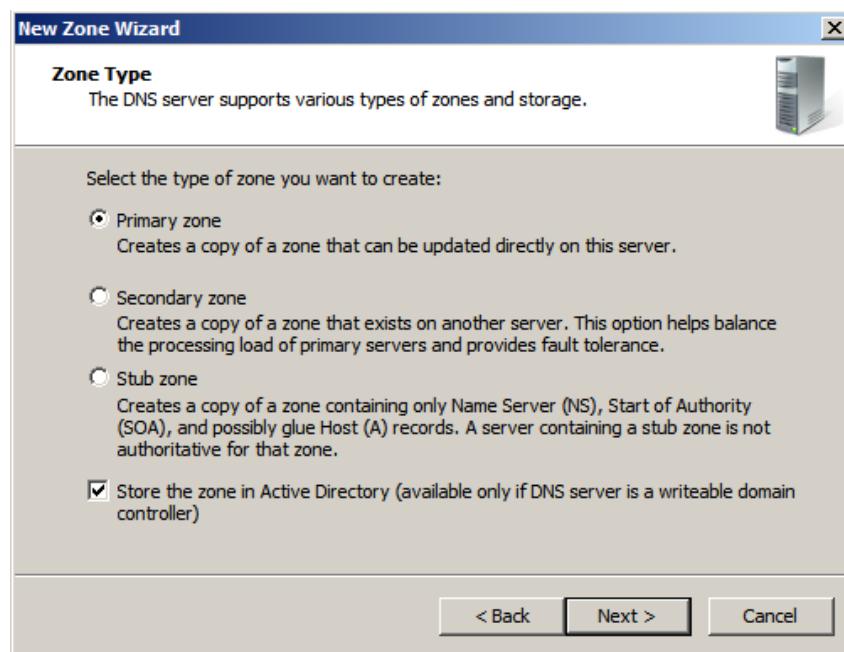


Figure 5. 7: Zone type

Step 10: In Zone Name just type name group1.com.

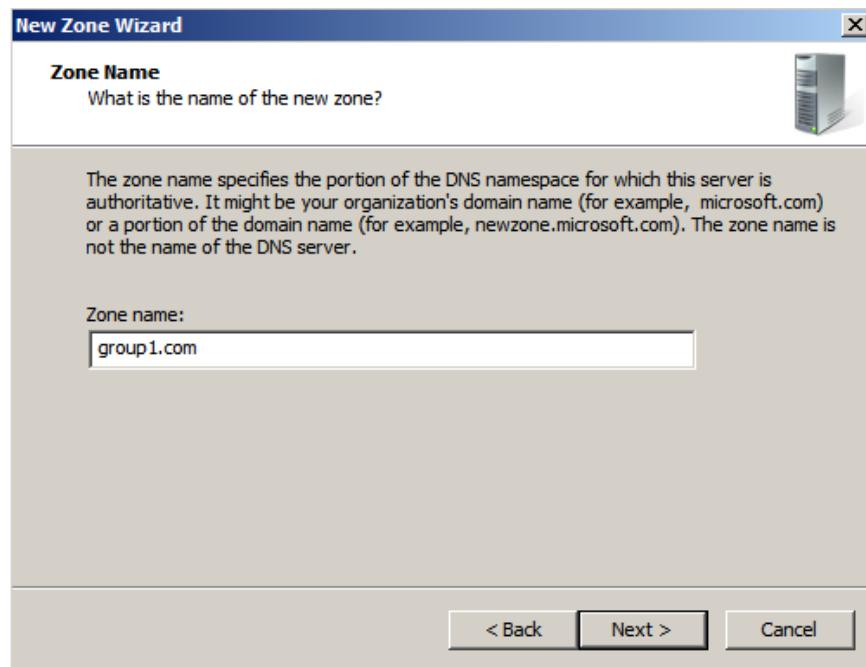


Figure 5. 8: Zone Name

Step 11: In Zone File page, we choose Create a new file with this file name and click next.

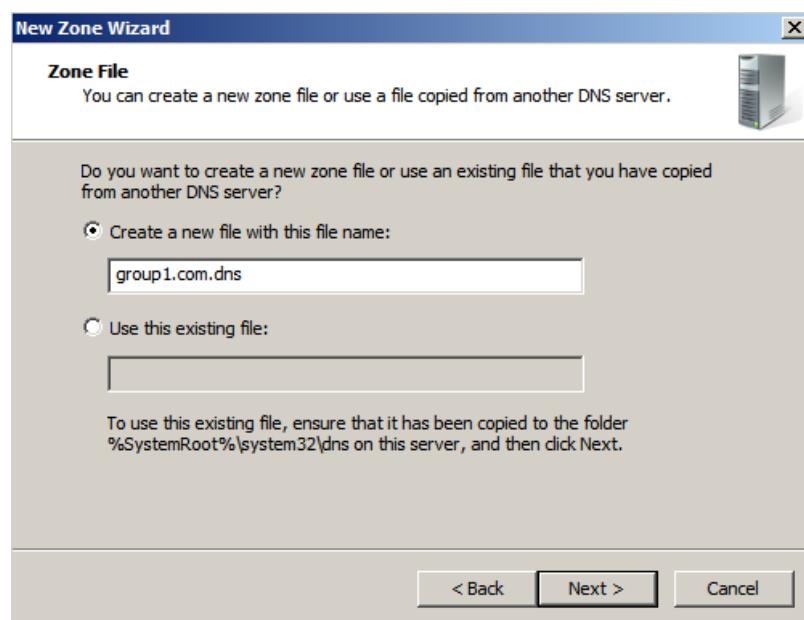


Figure 5. 9: Zone File

Step 12: For Dynamic Update we just choose do not allow dynamic updates and click next.

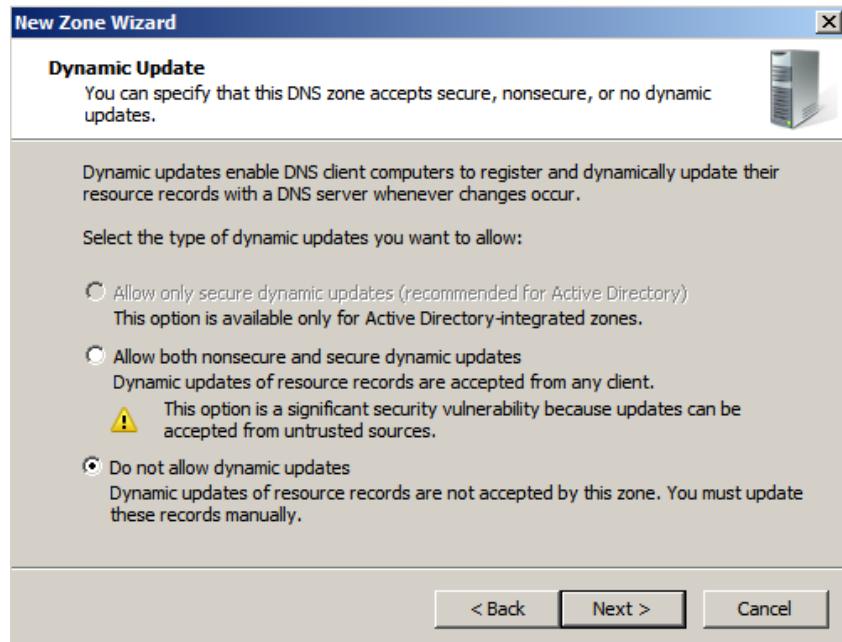


Figure 5. 10: Dynamic Update

Step 13: Then it will show our name, type and lookup type for our zone. Then, click Finish.



Figure 5. 11: Completing New Wizard

Step 14: Next, we will add new zone for reverse lookup. Right click on Reverse Lookup Zone and click New Zone. Then, click next.

Step 15: We choose for Primary Zone also and click next.

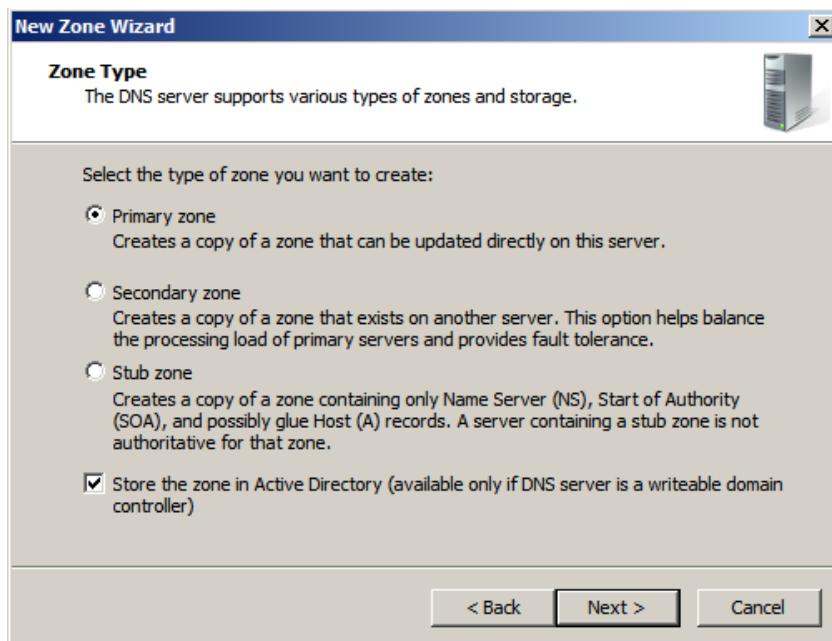


Figure 5. 12: Zone Type

Step 16: In Active Directory Zone Replication Scope choose the radio button To all DNS servers running on domain controllers in this domain: group1.com. this because we already add roles for AD first.

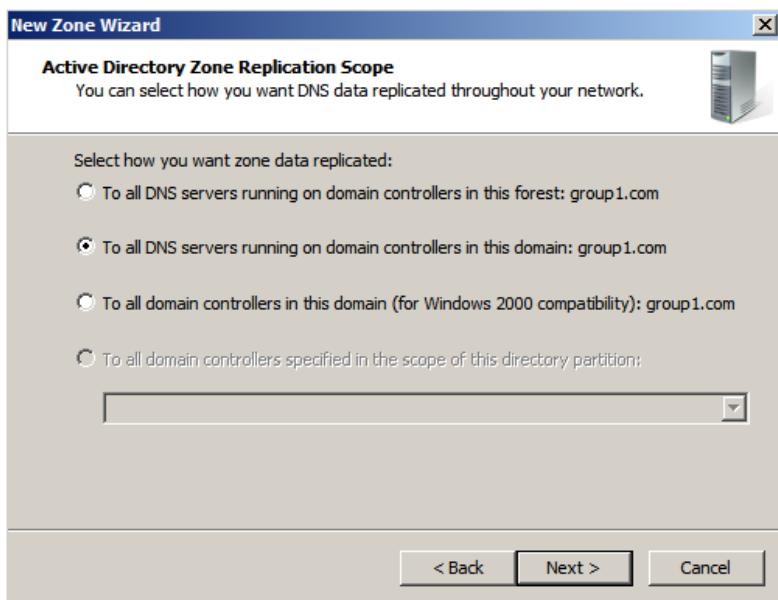


Figure 5. 13: Active Directory Zone Replication Scope

Step 17: For Reverse Lookup Zone Name choose IPv4 Reverse Lookup Zone

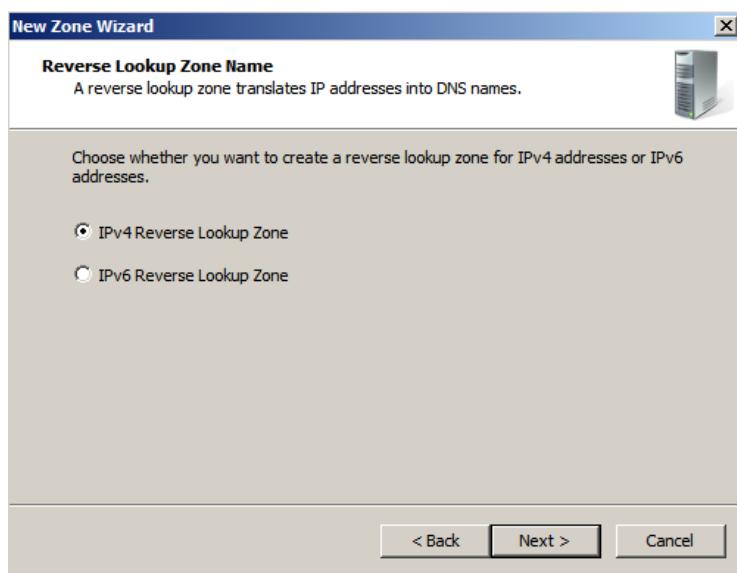


Figure 5. 14: Reverse Lookup Zone Name

Step 18: Then, we choose Network ID. Our group use 192.168.11 as network ID. Proceed to Next.

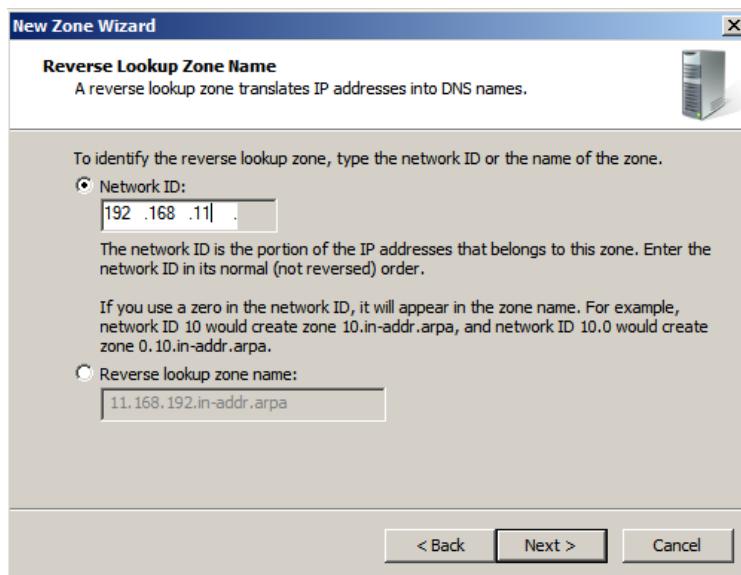


Figure 5. 15: Reverse Lookup Zone Name

Step 19: We choose Create new file with this name 11.168.192.in-addr.arpa.dns. Click Next.

Step 20: Then it will display the name, type and lookup type of the zone. Click Finish.

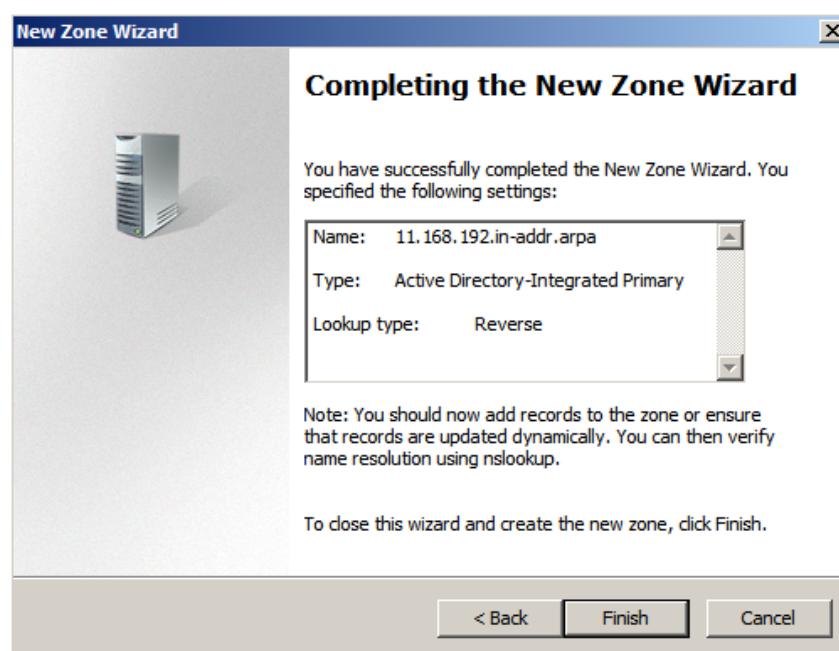


Figure 5. 16: Completing the New Zone Wizard

Step 21: After that, right click on group1.com and click Alias (CNAME) to add www as cname of group1.com.

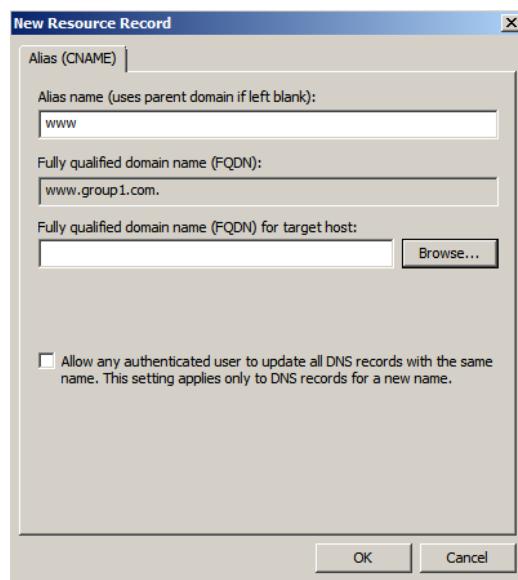


Figure 5. 17: Alias name

Step 22: On the Browse on FQDN to search group1 and click OK

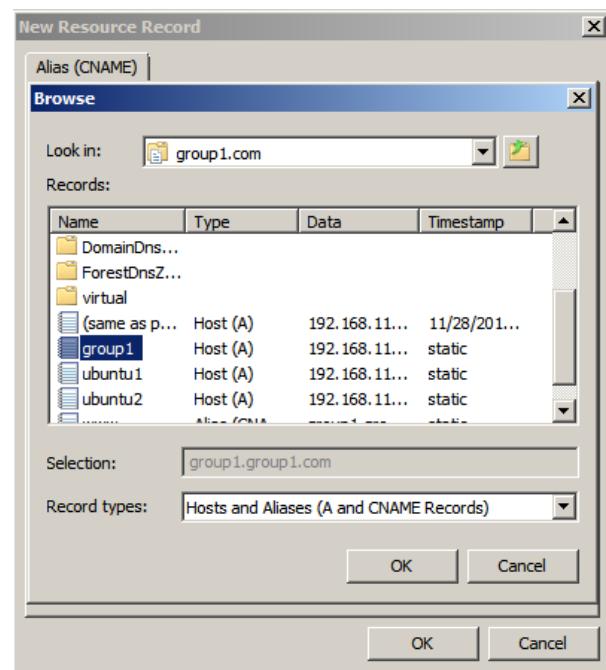


Figure 5. 18: Browse group1

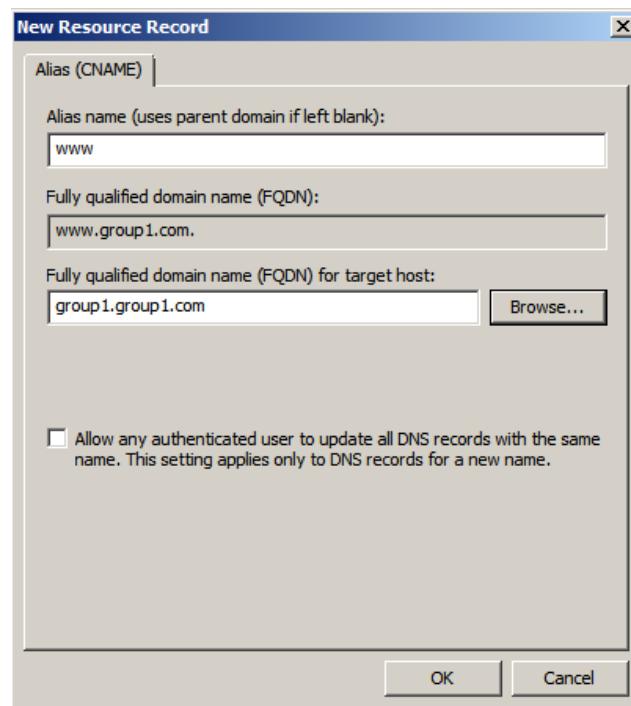


Figure 5. 19: FQDN target host

Step 23: www cname of group 1 successfully added.

Name	Type	Data
_msdcs	(same as parent folder)	Start of Authority (SOA) [211], group1.group1.com., hostmaster.group1.co...
_sites	(same as parent folder)	Name Server (NS) group1.group1.com.
_tcp	(same as parent folder)	Host (A) 192.168.11.34
_udp	(same as parent folder)	IPv6 Host (AAAA) 2001:c0a8:0b22:0000:0000:0000:0000:0002
DomainDnsZones	(same as parent folder)	IPv6 Host (AAAA) 2001:c0a8:0b22:0000:cdc:5655:b052:5dc...
ForestDnsZones	(same as parent folder)	IPv6 Host (AAAA) 2001:c0a8:0b22:0000:0cdc:5655:b052:5dc...
virtual	(same as parent folder)	IPv6 Host (AAAA) 2001:c0a8:0b22:0000:0000:0000:0000:0002
group1	Host (A)	192.168.11.34
group1	IPv6 Host (AAAA)	2001:c0a8:0b22:0000:0cdc:5655:b052:5dc...
group1	IPv6 Host (AAAA)	2001:c0a8:0b22:0000:0000:0000:0000:0002
ubuntu1	Host (A)	192.168.11.42
ubuntu2	Host (A)	192.168.11.51
ubuntu6	Host (A)	192.168.11.51
www	Alias (CNAME)	group1.group1.com.

Figure 5. 20: Successful add

Step 24: Open Local Area Connection and click Properties

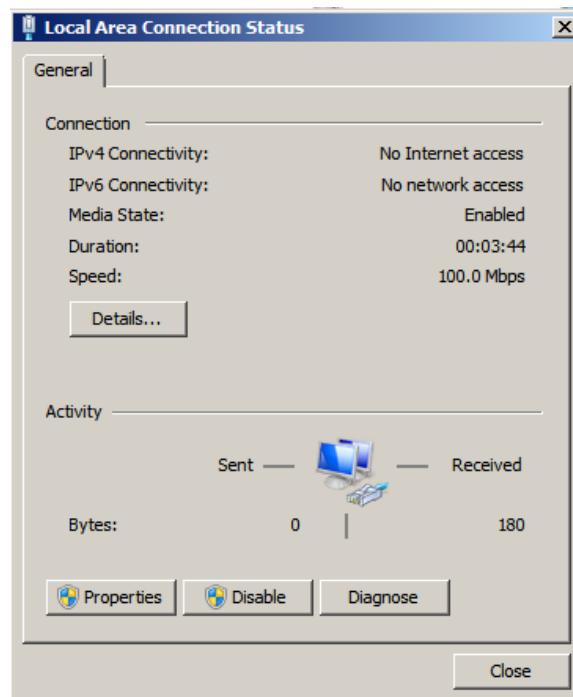


Figure 5. 21: Properties

Step 25: Click on Internet Protocol Version 6 (TCP/IPv6) and select Properties

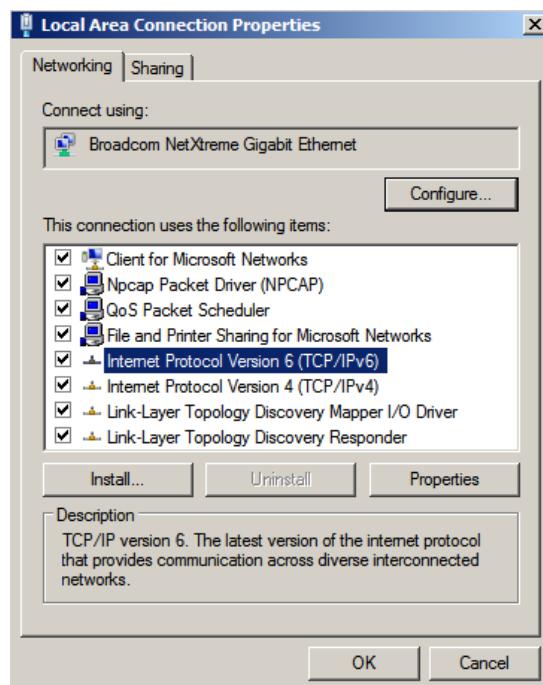


Figure 5. 22: Internet Protocol Version 6 (TCP/IPv6)

Step 26: Then enter the IPv6 Address. We use 2001:c0a8:b22::2/64 and gateway 2001:c0a8:b22::1. The DNS Server we used 2001:c0a8:b22::2. Then click OK and Close.

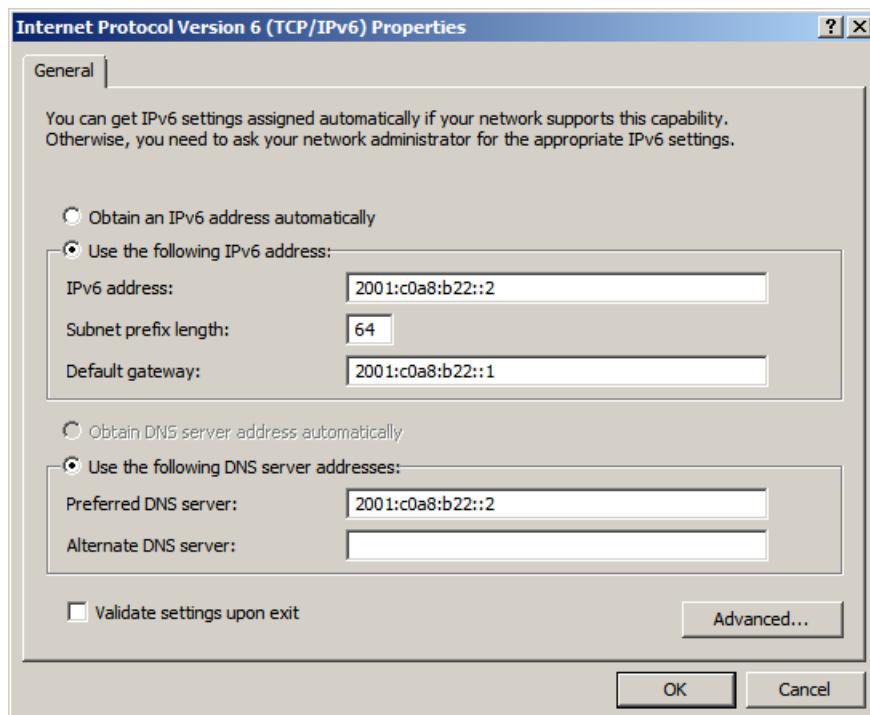


Figure 5. 23: Enter the IPv6 Address

Step 27: On Server Manager, select DNS. Right click on Reverse Lookup Zones and click New Zone.

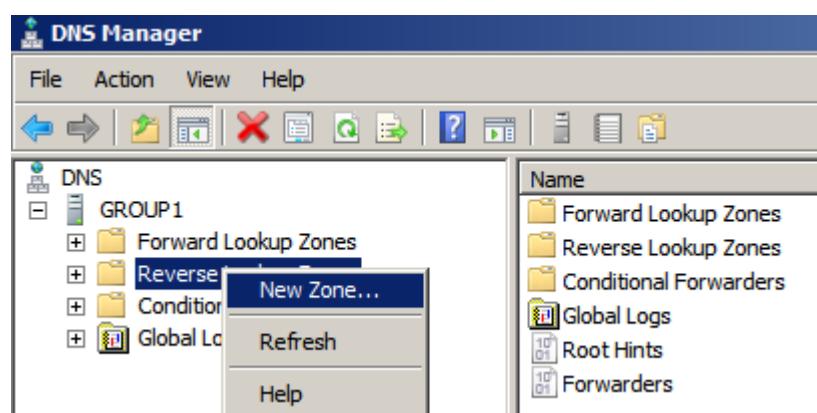


Figure 5. 24: New Zone

Step 28: On page Welcome to New Wizard click next. Then choose Primary zone. Untick on Store the zone in active AD. Then click next.

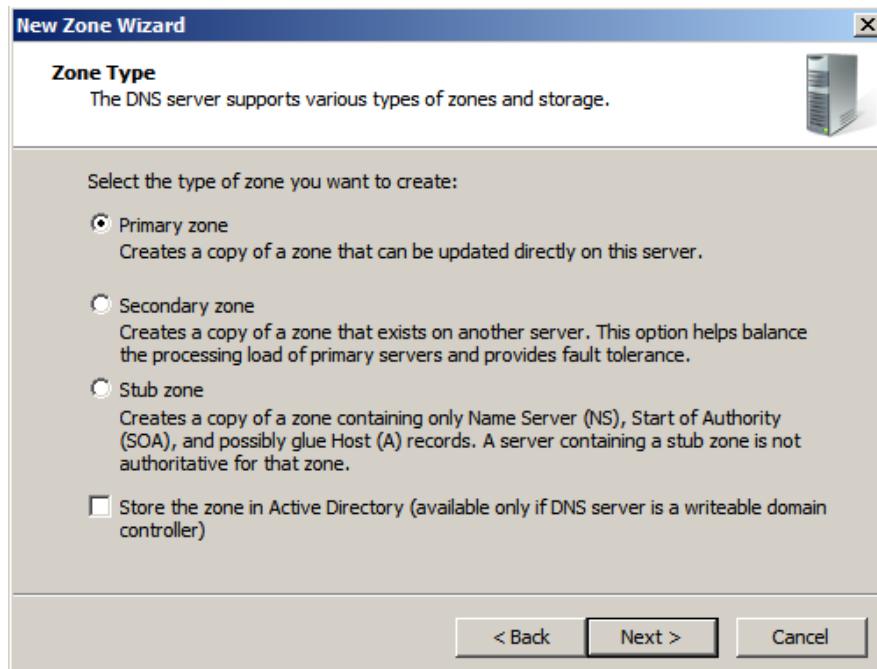


Figure 5. 25: Zone Type

Step 29: Then choose IPv6 Reverse Lookup Zone. Click next.

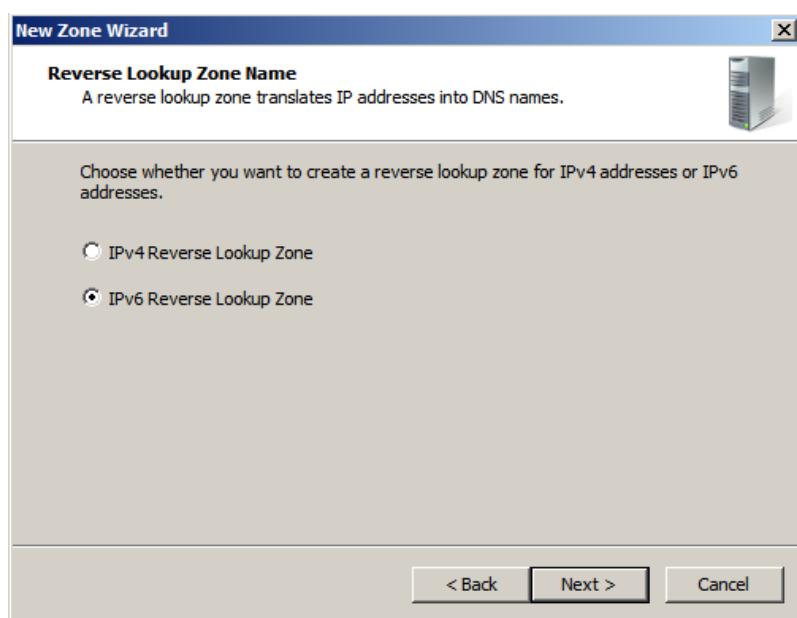


Figure 5. 26: IPv6 Reverse Lookup Zone

Step 30: In IPv6 Address Prefix, we enter 2001:c0a8:b22::/64 and Reverse Lookup Zones will automatically create. Then click next.

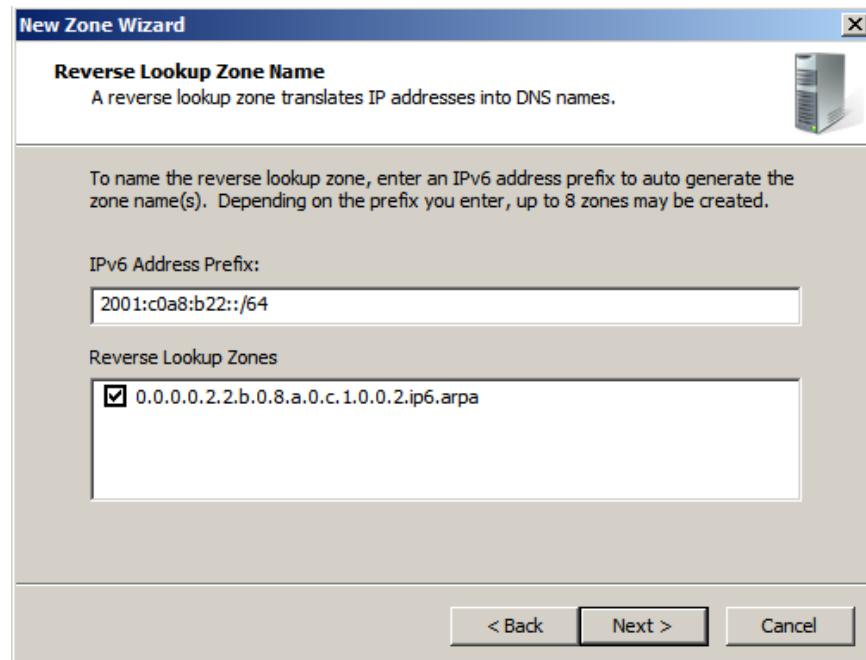


Figure 5. 27: IPv6 Address Profile

Step 31: On Dynamic Update page, select Allow only secure dynamic updates and proceed to next.

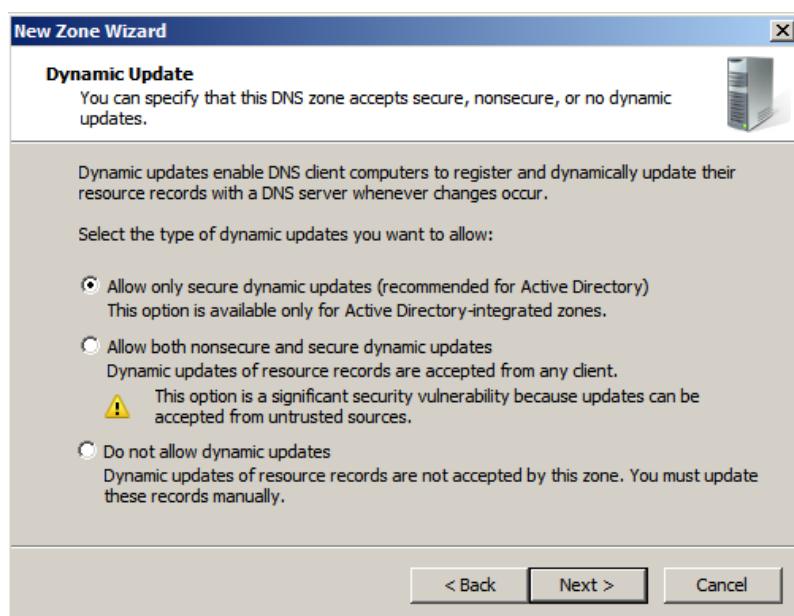


Figure 5. 28: Dynamic Update

Step 32: In Completing the New Zone Wizard page, it will display the zone name, type and lookup type. Click Finish.

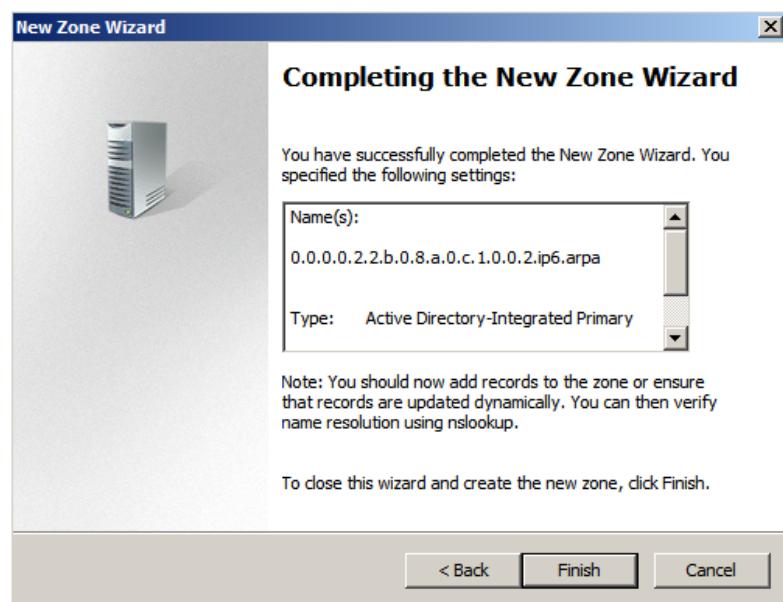


Figure 5. 29: Completing the new Zone Wizard

Step 33: Right click on IPv6 in Reverse Lookup Zones and click New Pointer (PTR).

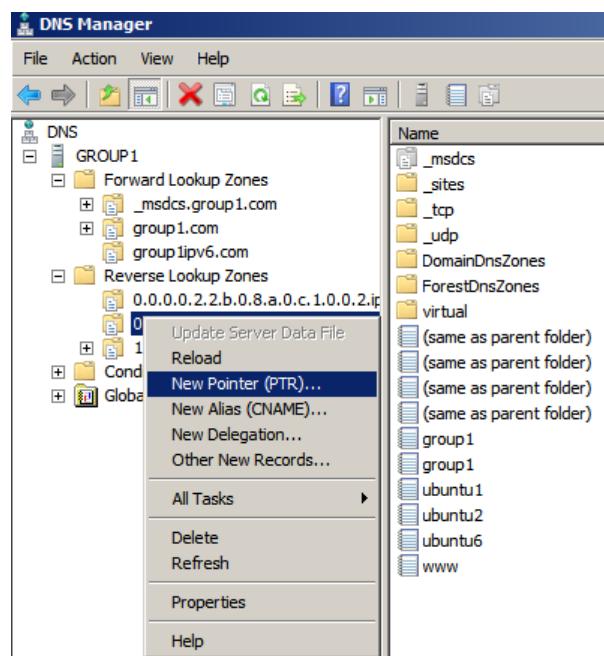


Figure 5. 30: New Pointer (PTR)

Step 34: Enter the Host IP Address and host name.

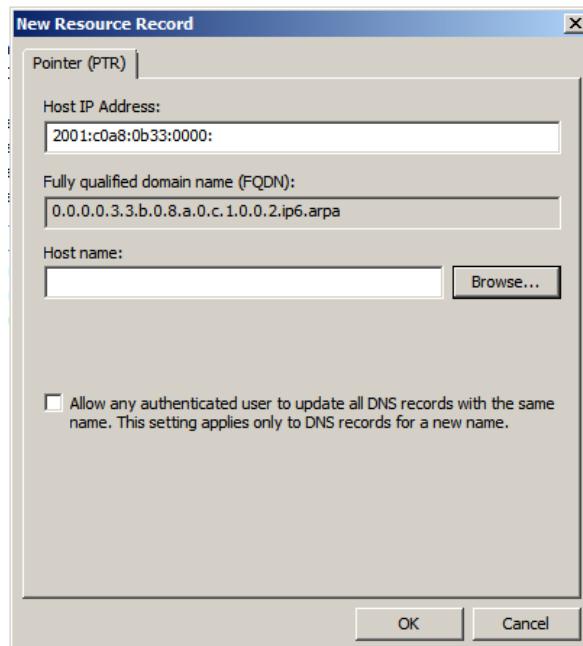


Figure 5. 31: Enter the Host IP Address and Host name

Step 35: Click Browse and choose ubuntu6.group1.com

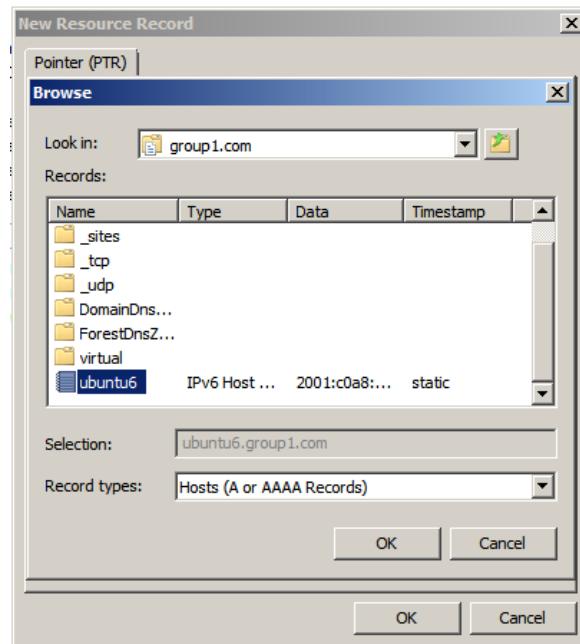


Figure 5. 32: Browse

Step 36: Click OK

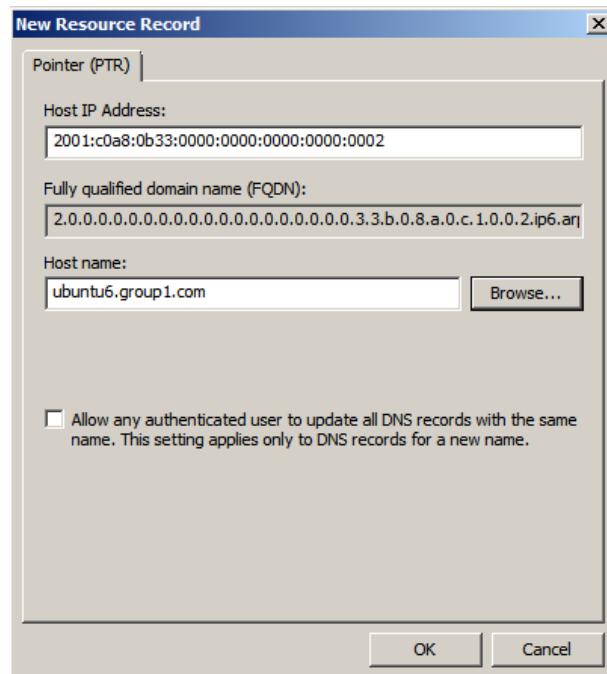


Figure 5. 33: Insert the IPv6 address and host name

## Problems

Some user complaining that they are confused with the IP of the server as they want to use the service on the server. They asked for naming the service so that it would be easier for them to recognize the service they want to use.

## Solution

We install DNS Server in Windows Server 2008. We added hostname for each service so that it is easier for the user to recognize and use the services.

### 5.3.2 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Step 1: Go to Start > Administrative Tools > Server Manager.

Step 2: Expand and click on Roles > Add Roles.

Step 3: Click Next on the Add Roles Wizard box.

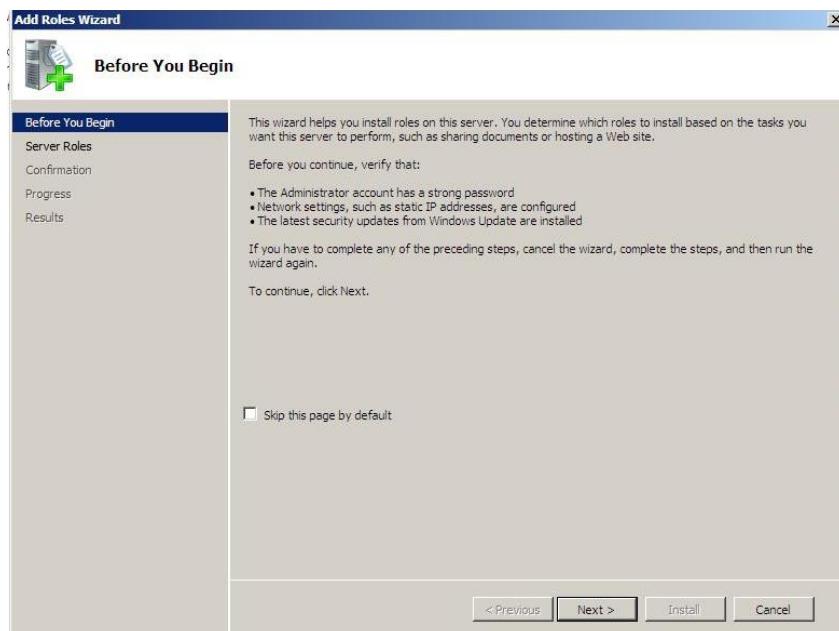


Figure 5. 34: Add Roles Wizard

Step 4: Choose Add Roles and follow the wizard by selecting the DHCP role and click next button.

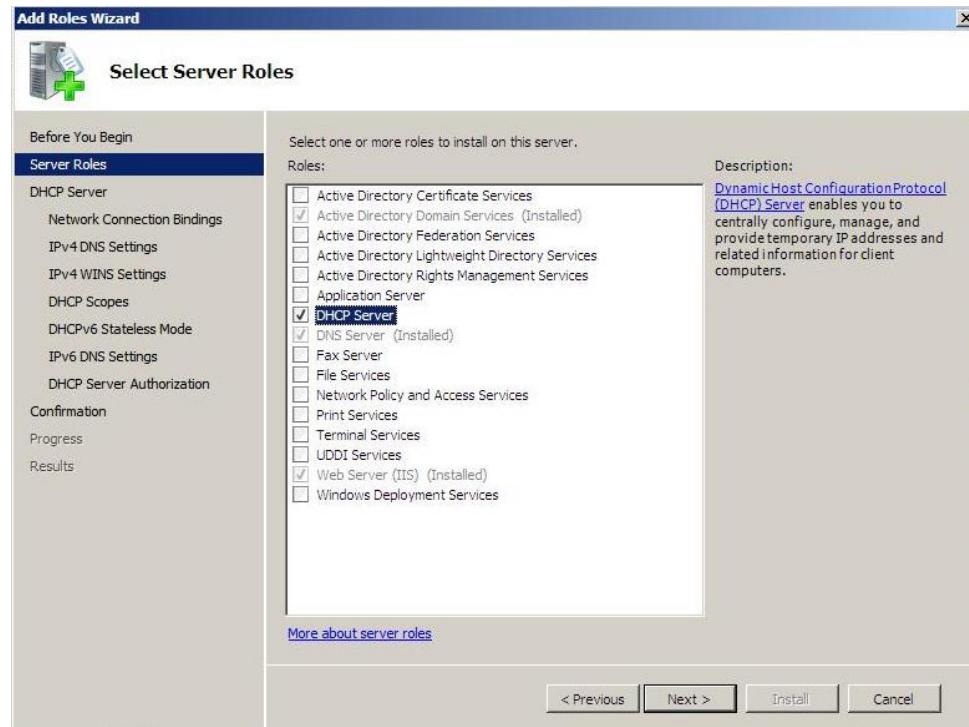


Figure 5. 35: Select Server Roles Wizard

Step 5: Network card and static IP addresses are automatically detected. It will try to check the server whether it is static IP address or not. Click next button if it display the correct IP address.

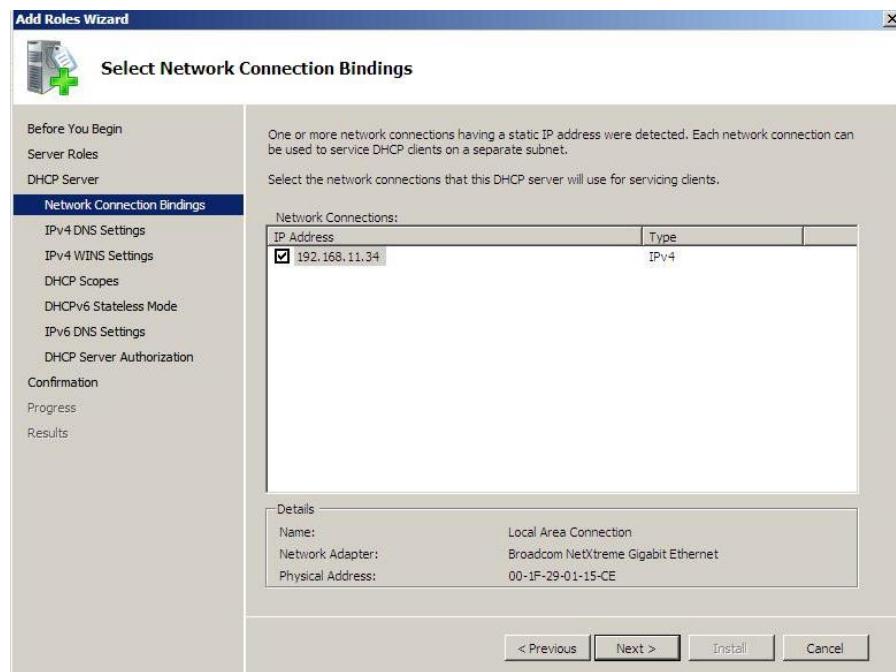


Figure 5. 36: Select Network Connection Bindings

Step 6: Specify the applicable DNS server to be used with DHCP when an address is assigned. Enter the domain name and validate the DNS server IPv4 address before click next button.

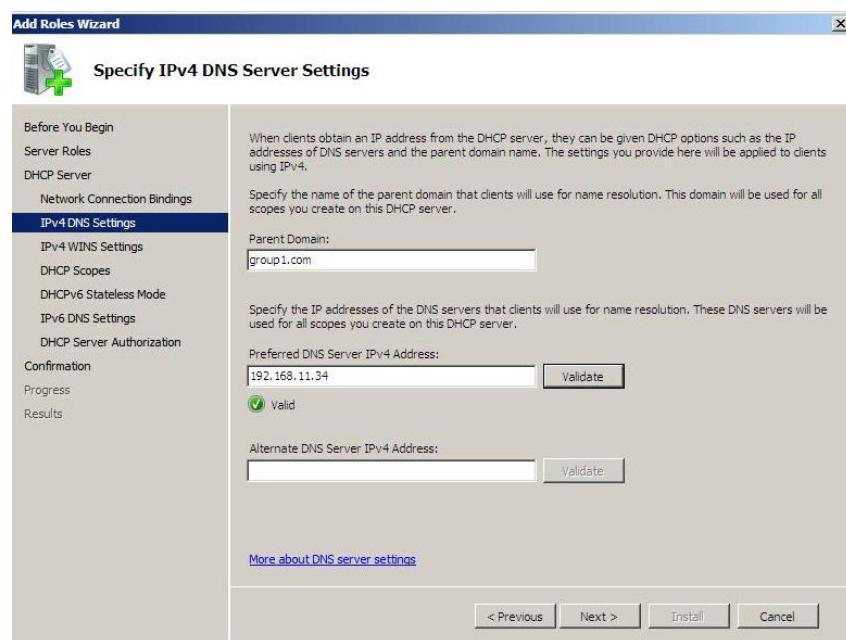


Figure 5. 37: Specify IPv4 DNS Server Settings

Step 7: Specify IPv4 WINS server setting. If have WINS server, enter the details here otherwise select first option and click next.

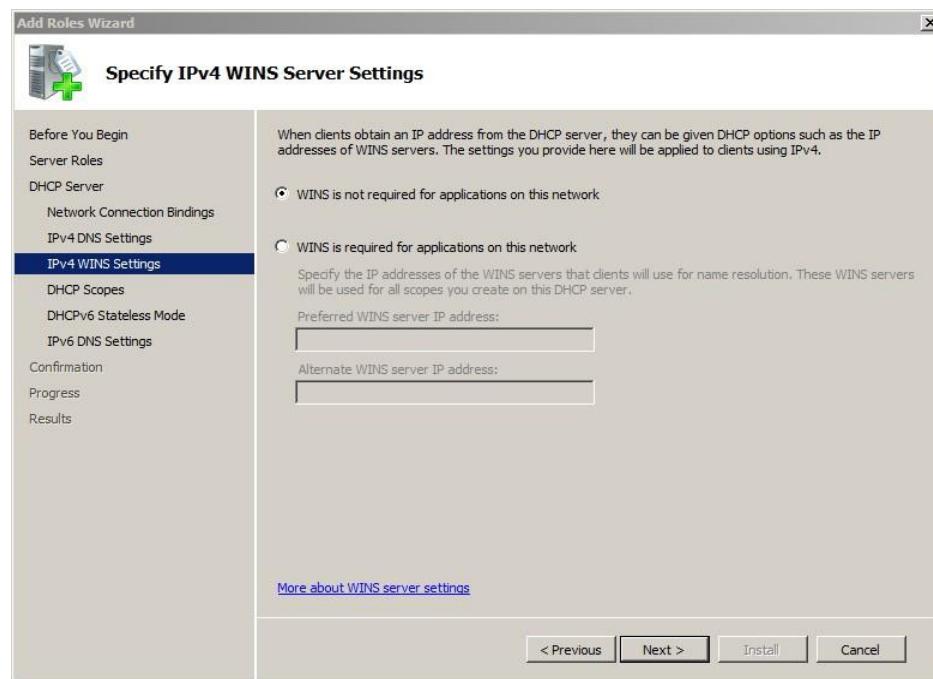


Figure 5. 38: Specify IPv4 WINS Server Settings

Step 8: The next window will ask to enter the range of addresses that the scope will distribute across the network and the subnet mask for the IP address. Enter the scope detail and click ok button.

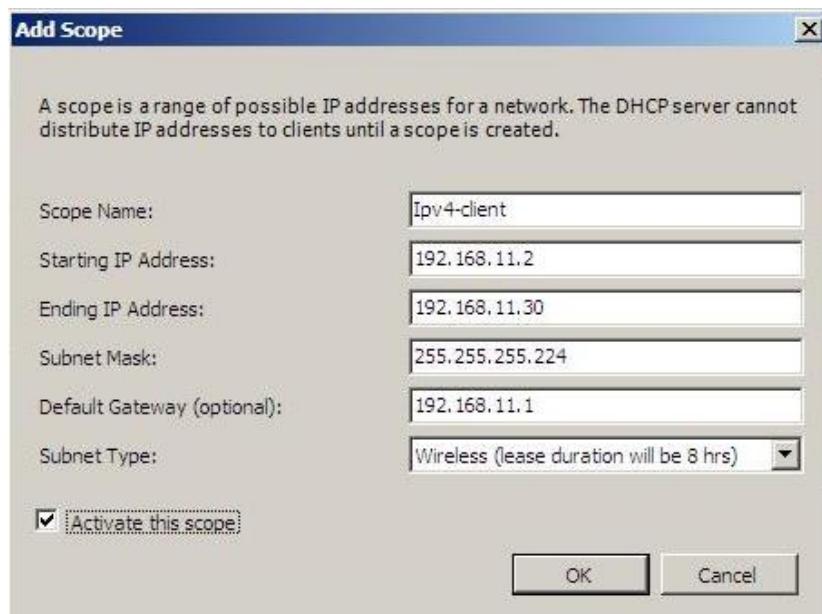


Figure 5. 39: Add Scope

Step 9: Click on Enable DHCPv6 stateless mode and click next button.

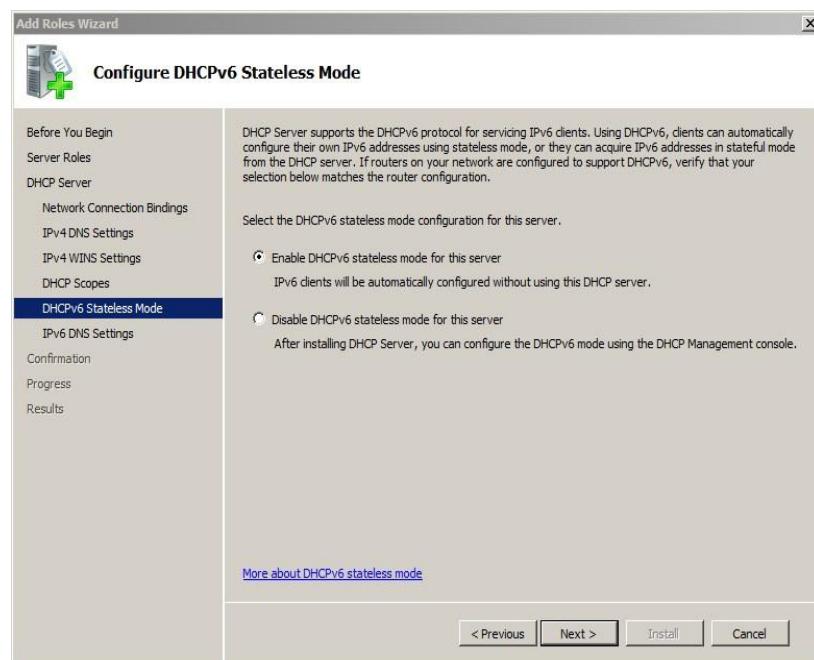


Figure 5. 40: Configure DHCPv6 Stateless Mode

Step 10: Specify the applicable DNS server to be used with DHCP when an address is assigned. Enter the domain name and validate the DNS server IPv6 address before click next.



Figure 5. 41: Specify IPv6 DNS Server Settings

Step 11: After confirming all the installation selections, click Install button.

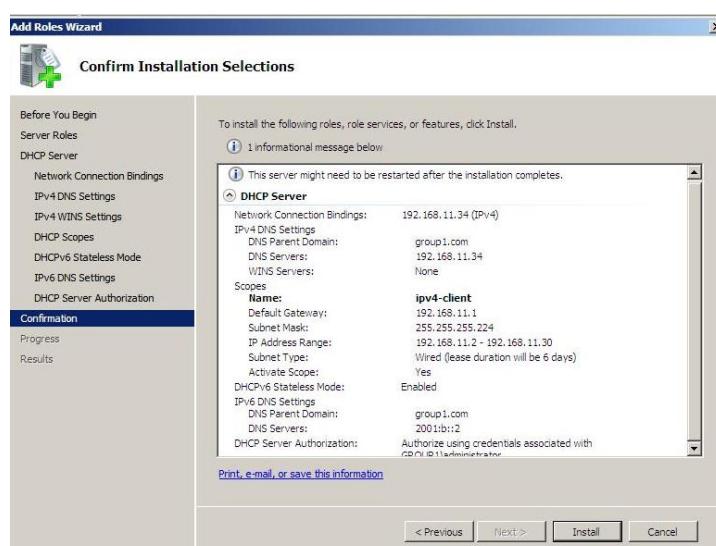


Figure 5. 42: Confirm Installation Selection

Configuring DHCPv6 statefull in router.

Router #conf t

Router(config) #ipv6 dhcp pool DHCPV6

Router(config-dhcpv6) #address prefix 2001:c0a8:b02::/64

Router(config-dhcpv6) #dns-server 2001:c0a8:b22::2

Router(config-dhcpv6) #domain-name group1.com

Router(config-dhcpv6) #end

Router #conf t

Router(config) #int g0/0.40

Router(config-subif) #ipv6 dhcp srver DHCPV6

Router(config-subif) #ipv6 nd managed-config-flag

Router(config-subif) #ipv6 nd prefix 2001:c0a8:b02::/64 14400 14400 no-autocfg

Router(config-subif) #end

Router #copy run start

### **5.3.3 ROUTING & NETWORK ADDRESS TRANSLATION (NAT)**

#### **Routing**

Step1: Enter the command as below using OSPF Protocol

```
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.11.0 0.0.0.255 area 1
Router(config-router)#network 200.200.200.0 0.0.0.255 area 1
Router(config-router)#ex
```

Figure 5.43: Routing Command

## Installation and Configuration NAT

Step1: Add NAT inside source static

Figure 5.44: Add NAT inside source static

ACL

Step1: Setup access-list and permit IP address

```
Router(config)# access-list 1 permit 192.168.11.0 0.0.0.31  
Router(config)#
```

Figure 5.45: Setup access list and permit ip address

## PAT NAT overload

Step1: Set g0/1 interface as public IP address using overload function

```
[OK]
R1(config)#ip nat inside source list 1 interface g0/1 overload
R1(config)#do copy run start
Destination filename [startup-config]?
Building configuration...

[OK]
R1(config)#exit
R1#
```

Figure 5. 46: Set g0/1 interface as public IP address using overload  
function

### Outside Interface

Step1: Setup g0/1 interface as outside interface

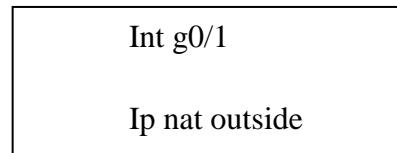


Figure 5. 47: Setup g0/1 as outside interface

### Inside Interface

Step1: Setup g0/0 sub-interface as NAT inside

```
R1#
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g0/0.5
R1(config-subif)#ip nat inside
R1(config-subif)#ex
R1(config)#int g0/0.10
R1(config-subif)#ip nat inside
R1(config-subif)#ex
R1(config)#int g0/0.20
R1(config-subif)#ip nat inside
R1(config-subif)#ex
R1(config)#int g0/0.20
R1(config-subif)#ip nat inside
R1(config-subif)#ex
R1(config)#int g0/0.30
R1(config-subif)#ip nat inside
R1(config-subif)#ex
R1(config)#int g0/0.40
R1(config-subif)#ip nat inside
R1(config-subif)#ex
R1(config)#do copy run start
Destination filename [startup-config]?
Building configuration...

[OK]
```

Figure 5. 48: Setup g0/0 as inside

### 5.3.4 VIRTUAL LOCAL AREA NETWORK (VLAN)

Step 1: Create VLAN and assign port number.

```
Switch(config)#vlan 5 name trunk
```

```
Switch(config-vlan)#vlan 10 name windows
```

```
Switch(config-vlan)#vlan 20 Linux1
```

```
Switch(config-vlan)#vlan 30 Linux2
```

```
Switch(config-vlan)#vlan 40 Client
```

```
Switch(config-vlan)#exit
```

```
Switch(config)#int range fa0/2-4
```

```
Switch(config-if-range)#switchport mode access
```

```
Switch(config-if-range)#switchport access vlan 10
```

```
Switch(config-if-range)#int range fa0/5-7
```

```
Switch(config-if-range)#switchport mode access
```

```
Switch(config-if-range)#switchport access vlan 20
```

```
Switch(config-if-range)#int range fa0/8-11
```

```
Switch(config-if-range)#switchport mode access
```

```
Switch(config-if-range)#switchport access vlan 30
```

```
Switch(config-if-range)#int range fa0/12-15
```

```
Switch(config-if-range)#switchport mode access
```

```
Switch(config-if-range)#switchport access vlan 40
```

Step 2: Assign trunking in VLAN 5

```
Switch(config)#int fa0/24
```

```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)#switchport trunk native vlan 5
```

```
Switch(config-if)#exit
```

Step 3: Assign gateway address and ipv6 address on the router.

```
R1 (config)#int g0/0.5
```

```
R1(config-subif)#encapsulation dot1q 5
```

```
R1 (config-subif)#ip address 192.168.11.65 255.255.255.252
```

```
R1 (config-subif)#ipv6 address 2001:C0A8:B41::1/64
```

```
R1 (config-subif)#ipv6 address 2001:C0A8:B41::1/64 eui-64
```

```
R1 (config-subif)#ipv6 enable
```

```
R1 (config-subif)#ipv6 ospf 1 area 1
```

```
R1 (config-subif)#no shut
```

```
R1 (config-subif)#int g0/0.10
```

```
R1 (config-subif)#encapsulation dot1q 10
```

```
R1 (config-subif)#ip address 192.168.11.33 255.255.255.248
```

```
R1 (config-subif)#ipv6 address 2001:C0A8:B22::1/64
```

```
R1 (config-subif)#ipv6 address 2001:C0A8:B22::1/64 eui-64
```

```
R1 (config-subif)#ipv6 enable
```

```
R1 (config-subif)#ipv6 ospf 1 area 1
```

```
R1 (config-subif)#no shut
```

```
R1 (config-subif)#int g0/0.20
```

```
R1 (config-subif)#encapsulation dot1q 20
```

```
R1 (config-subif)#ip address 192.168.11.41 255.255.255.248
```

```
R1 (config-subif)#ipv6 address 2001:C0A8:B2A::1/64
```

```
R1 (config-subif)#ipv6 address 2001:C0A8:B2A::1/64 eui-64
```

```
R1 (config-subif)#ipv6 enable
```

```
R1 (config-subif)#ipv6 ospf 1 area 1
```

```
R1 (config-subif)#no shut
```

```
R1 (config-subif)#int g0/0.30
```

```
R1 (config-subif)#encapsulation dot1q 30
```

```
R1 (config-subif)#ip address 192.168.11.49 255.255.255.248
```

```
R1 (config-subif)#ipv6 address 2001:C0A8:B33::1/64
```

```
R1 (config-subif)#ipv6 address 2001:C0A8:B33::1/64 eui-64
```

```
R1 (config-subif)#ipv6 enable
```

```
R1 (config-subif)#ipv6 ospf 1 area 1
```

```
R1 (config-subif)#no shut
```

```
R1 (config-subif)#int g0/0.40
```

```
R1 (config-subif)#encapsulation dot1q 40
```

```
R1 (config-subif)#ip address 192.168.11.1 255.255.255.224
```

```
R1 (config-subif)#ipv6 address 2001:C0A8:B02::1/64
```

```
R1 (config-subif)#ipv6 address 2001:C0A8:B02::1/64 eui-64
```

```
R1 (config-subif)#ipv6 enable
```

```
R1 (config-subif)#ipv6 ospf 1 area 1
```

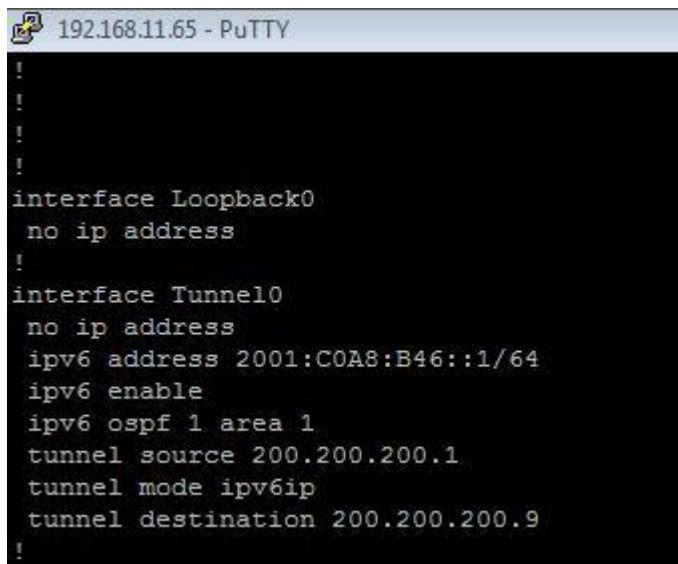
```
R1 (config-subif)#no shut
```

```
R1 (config-subif)#exit
```

```
R1(config)#end
```

### **5.3.5 IPV6 TRANSITION MECHANISM**

We manually configure IPv6 Tunnel in router by defining the source and destination IP address. This allow us to send IPv6 packets over the networks.



```
! interface Loopback0
no ip address
!
interface Tunnel0
no ip address
ipv6 address 2001:COA8:B46::1/64
ipv6 enable
ipv6 ospf 1 area 1
tunnel source 200.200.200.1
tunnel mode ipv6ip
tunnel destination 200.200.200.9
!
```

Figure 5. 49: IPv6 Tunnelling Configuration

### 5.3.6 WEB, SECURE SOCKETS LAYER (SSL) & VIRTUAL HOSTING

domain name (FQDN) > browse...

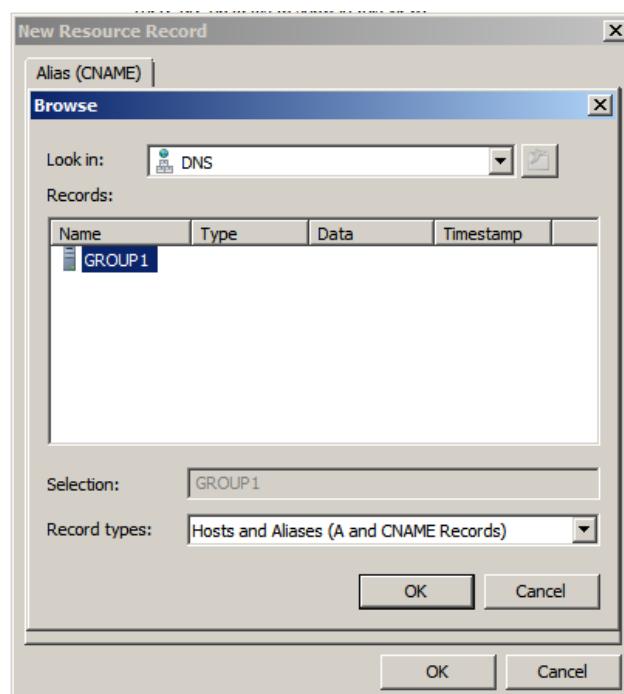


Figure 5. 50: Browse to DNS

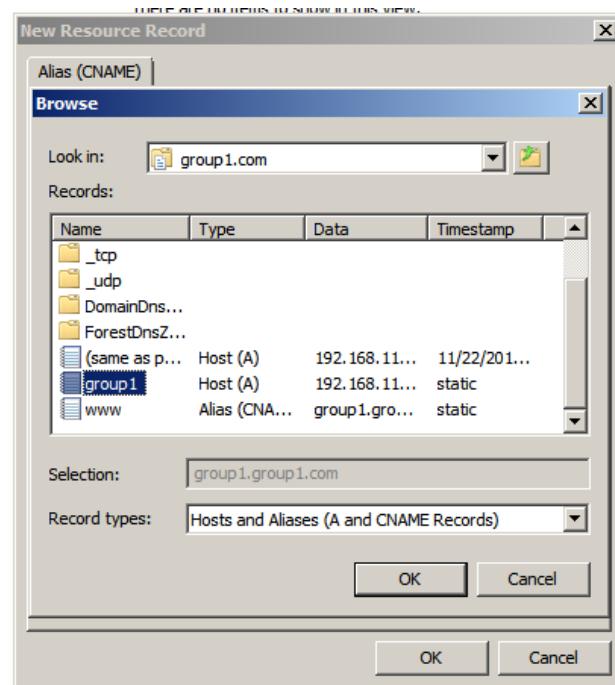


Figure 5. 51: Browse to group1.com

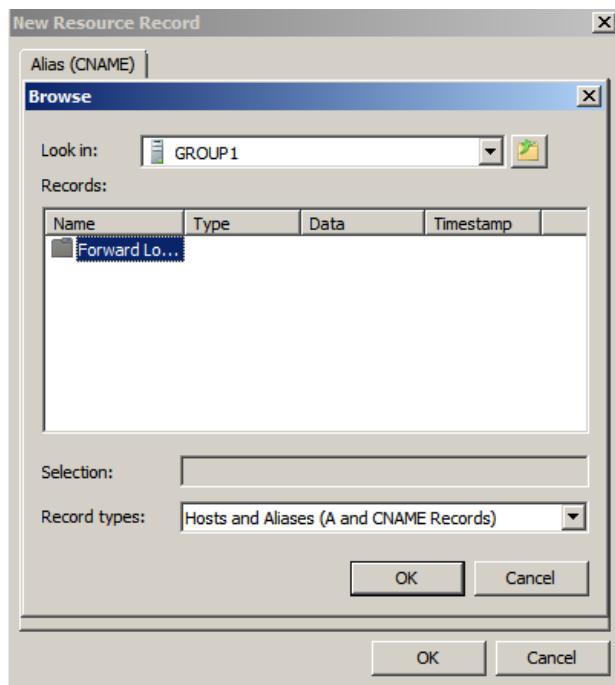


Figure 5. 52: Browse to Foward Lookup Zones

Step 3: Select group1 for the FQDN

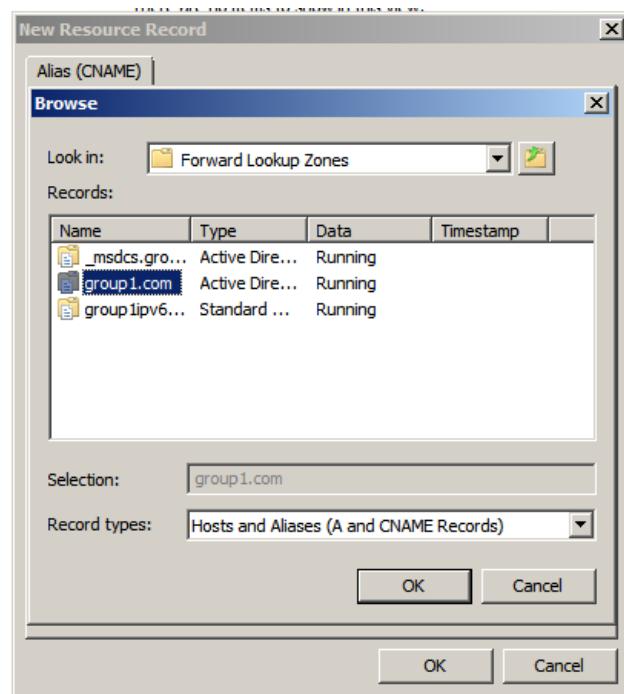


Figure 5. 53: Browse to GROUP1

Step 4: Completed as shown below.

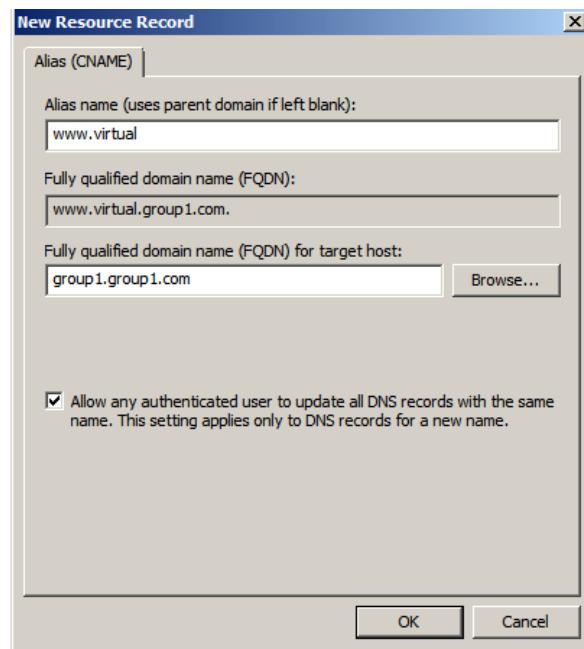


Figure 5. 54: Alias (CNAME)

Step 5: Testing the virtual hosting of <http://www.virtual.group1.com/>



Figure 5. 55: Open browser and enter [www.virtual.group1.com](http://www.virtual.group1.com/)

### 5.3.7 IPV6 WEB

Step1: At ISS manager> Right click “Sites” and click “Add Web Site”.

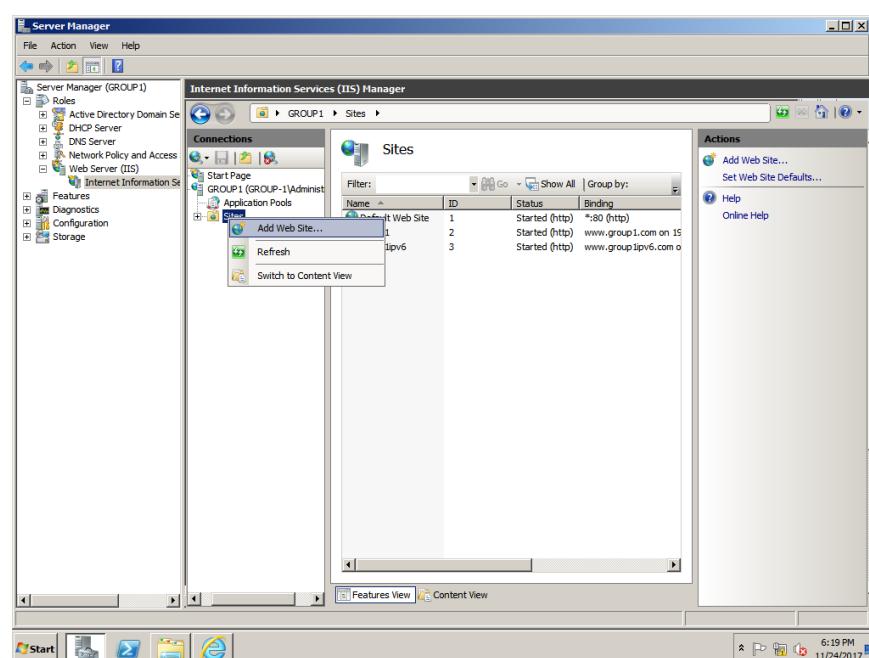


Figure 5. 56: Add Web Site

Step2: Fill the requirement needed.

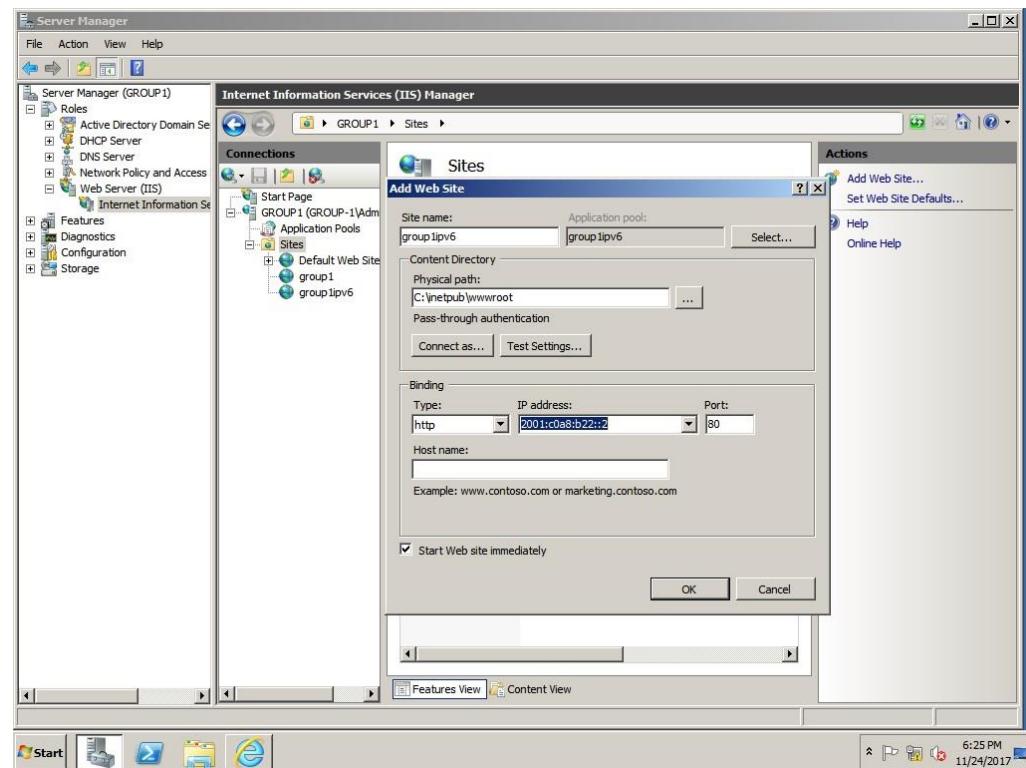


Figure 5. 57: Fill the requirement

Step3: Go to the “Directory Browsing” and click “Explore”

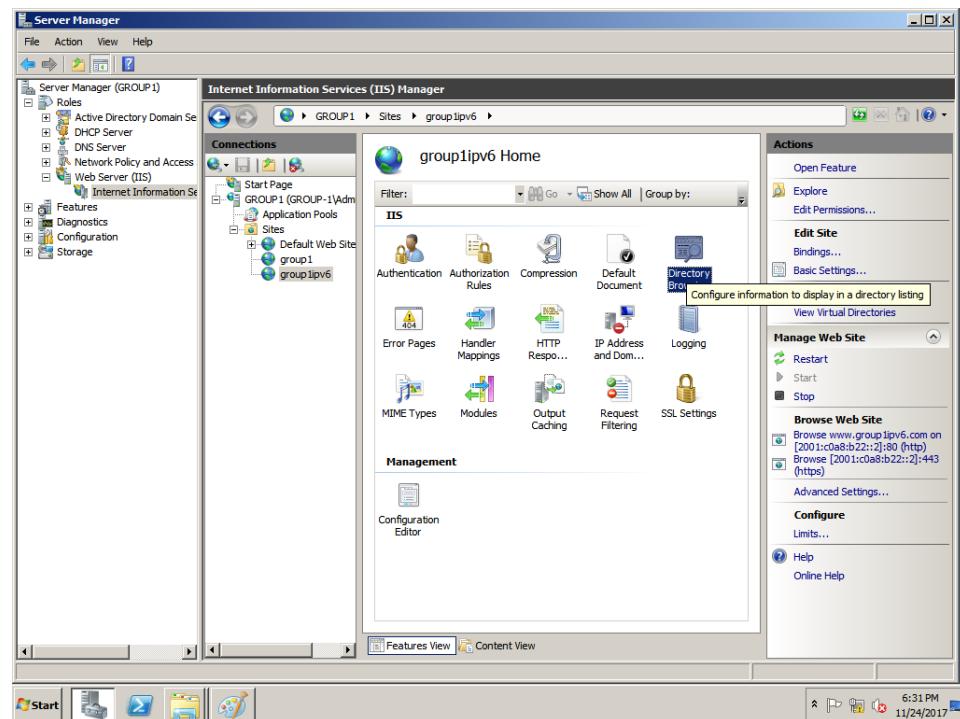


Figure 5. 58: Directory Browsing

Step4: Create a html document in the “wwwroot”

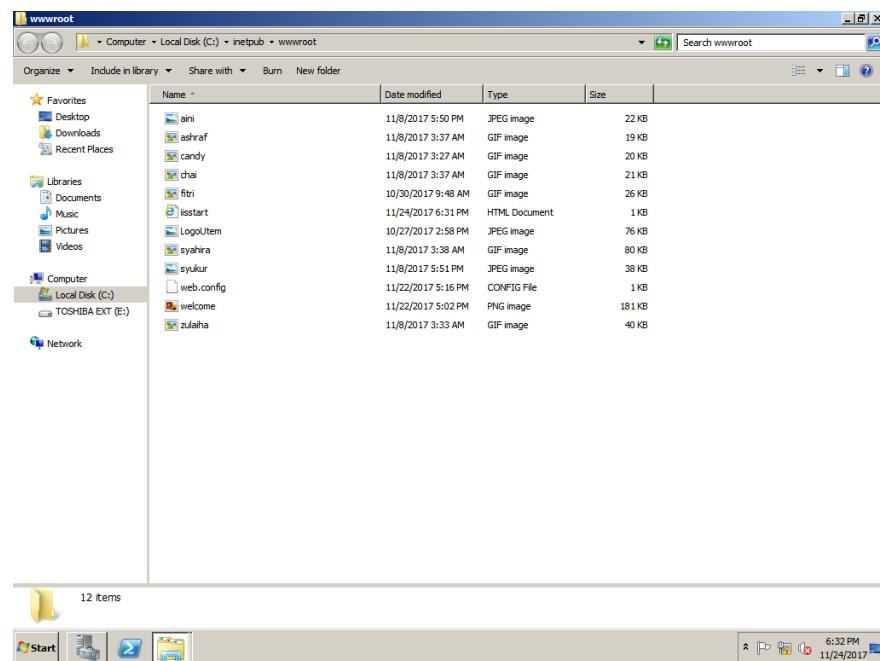
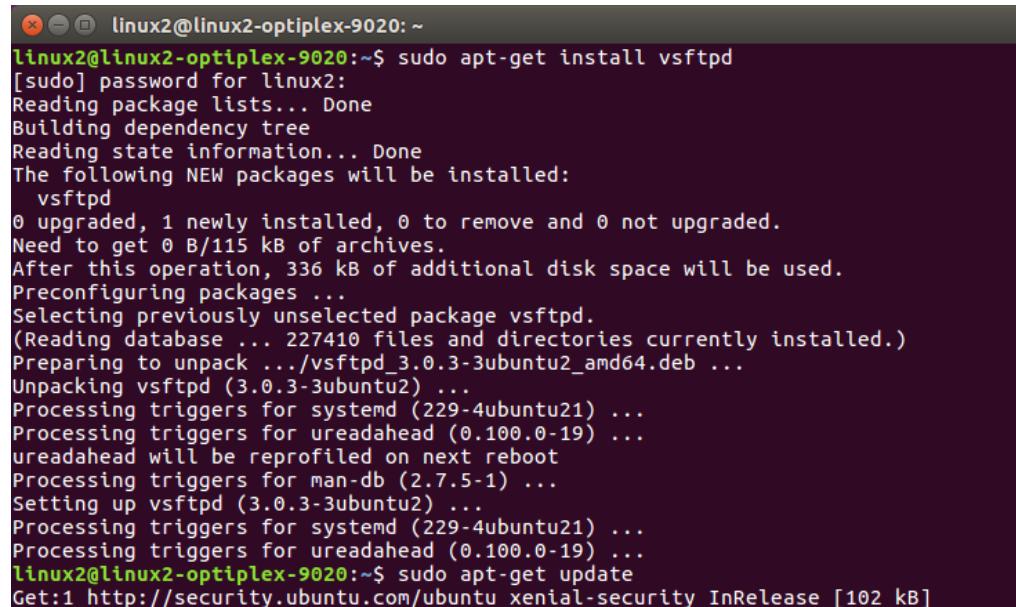


Figure 5. 59:File in wwwroot

### 5.3.8 SECURE FILE TRANSFER PROTOCOL (SFTP)

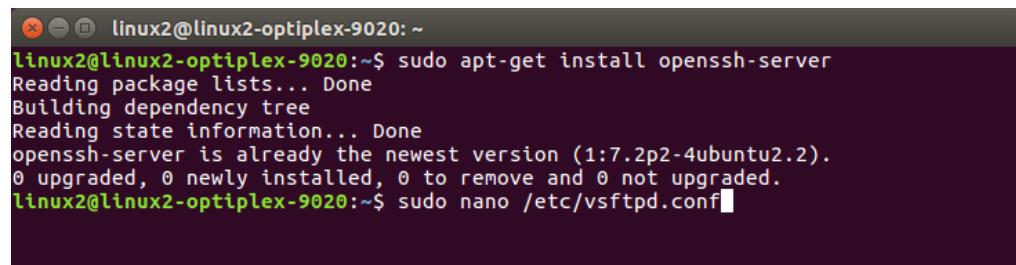
1. In linux2, install vsftpd by entering the command “sudo apt-get install vsftpd”and then update the Ubuntu by entering the command “sudo apt-get update”.



```
linux2@linux2-optiplex-9020:~$ sudo apt-get install vsftpd
[sudo] password for linux2:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/115 kB of archives.
After this operation, 336 kB of additional disk space will be used.
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 227410 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-3ubuntu2_amd64.deb ...
Unpacking vsftpd (3.0.3-3ubuntu2) ...
Processing triggers for systemd (229-4ubuntu21) ...
Processing triggers for ureadahead (0.100.0-19) ...
ureadahead will be reprofiled on next reboot
Processing triggers for man-db (2.7.5-1) ...
Setting up vsftpd (3.0.3-3ubuntu2) ...
Processing triggers for systemd (229-4ubuntu21) ...
Processing triggers for ureadahead (0.100.0-19) ...
linux2@linux2-optiplex-9020:~$ sudo apt-get update
Get:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [102 kB]
```

Figure 5. 60: Installing vsftpd and updating ubuntu

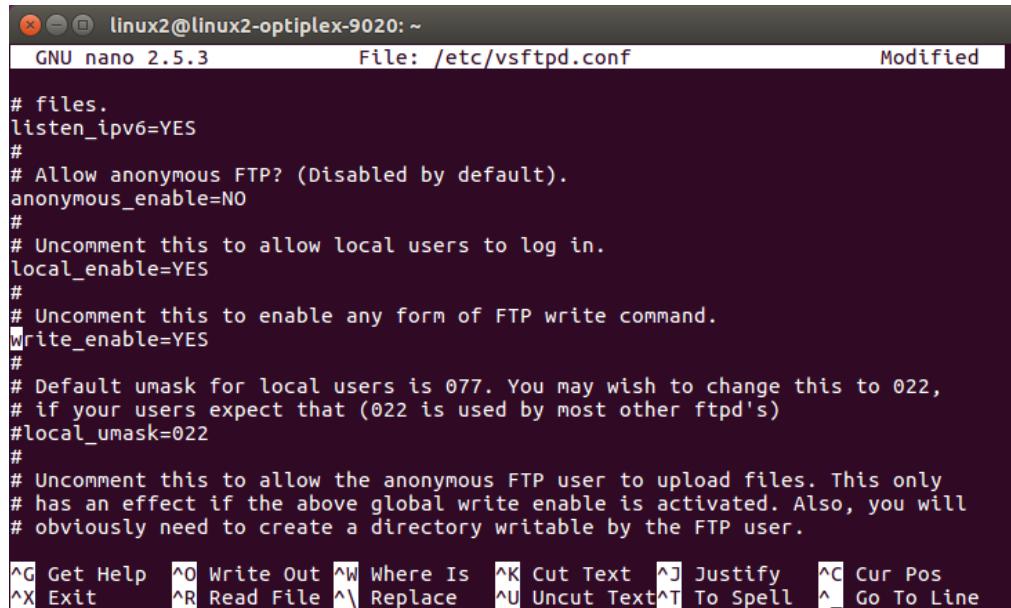
2. Install OpenSSH server by entering the command of “sudo apt-get install openssh-server”. Then, open the vsftpd.conf file by entering “sudo nano /etc/vsftpd.conf”.



```
linux2@linux2-optiplex-9020:~$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
openSSH-server is already the newest version (1:7.2p2-4ubuntu2.2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
linux2@linux2-optiplex-9020:~$ sudo nano /etc/vsftpd.conf
```

Figure 5. 61: Installing openssh-server

3. Uncomment the “anonymous\_enable=NO”, “local\_enable=YES” and “write\_enable=YES”.



```
linux2@linux2-optiplex-9020: ~
GNU nano 2.5.3           File: /etc/vsftpd.conf           Modified

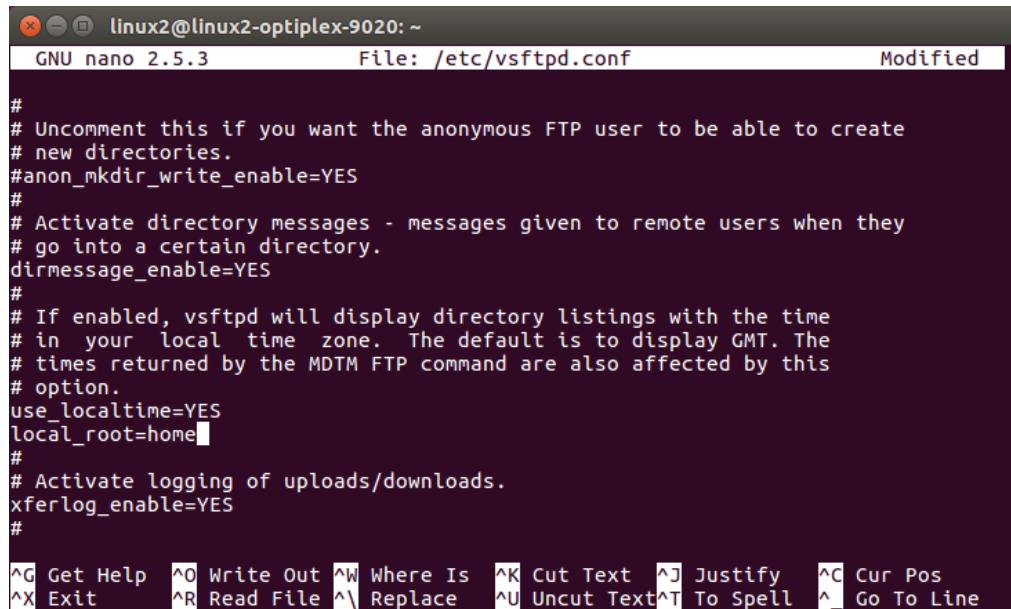
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^L Replace   ^U Uncut Text^T To Spell ^_ Go To Line
```

Figure 5. 62: Uncommenting anonymous\_enable, local\_enable and  
write\_enable

4. Uncomment “use\_localtime=YES” and add the following line;

“local\_root=home”

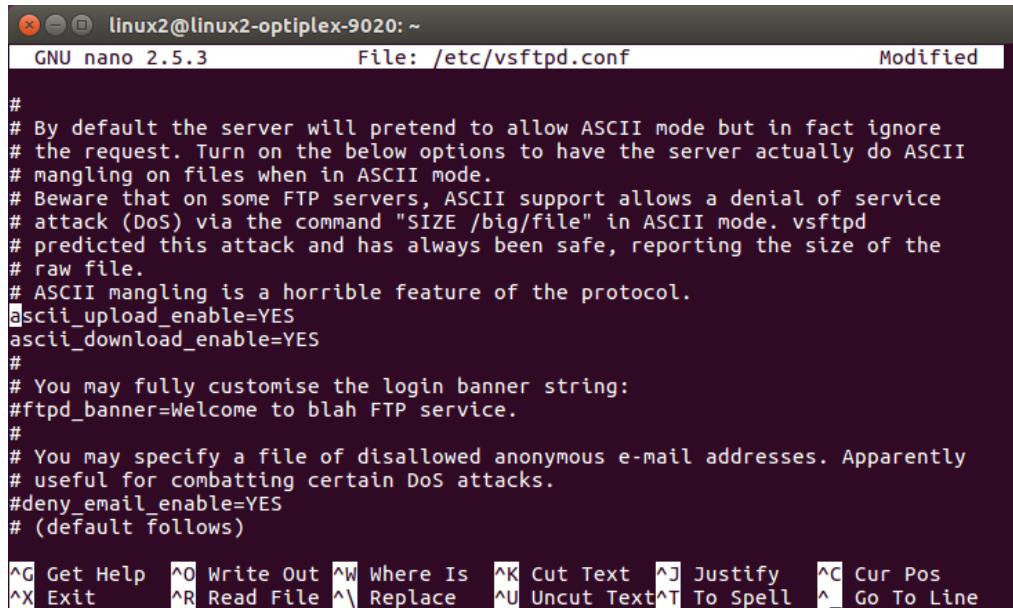


```
linux2@linux2-optiplex-9020: ~
GNU nano 2.5.3           File: /etc/vsftpd.conf           Modified

#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# If enabled, vsftpd will display directory listings with the time
# in your local time zone. The default is to display GMT. The
# times returned by the MDTM FTP command are also affected by this
# option.
use_localtime=YES
local_root=home
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^L Replace   ^U Uncut Text^T To Spell ^_ Go To Line
```

Figure 5. 63: Uncommenting use\_localtime and adding local\_root

5. Uncomment “asci\_upload\_enable=YES” and “asci\_download\_enable=YES”.



```

linux2@linux2-optiplex-9020: ~
GNU nano 2.5.3           File: /etc/vsftpd.conf           Modified

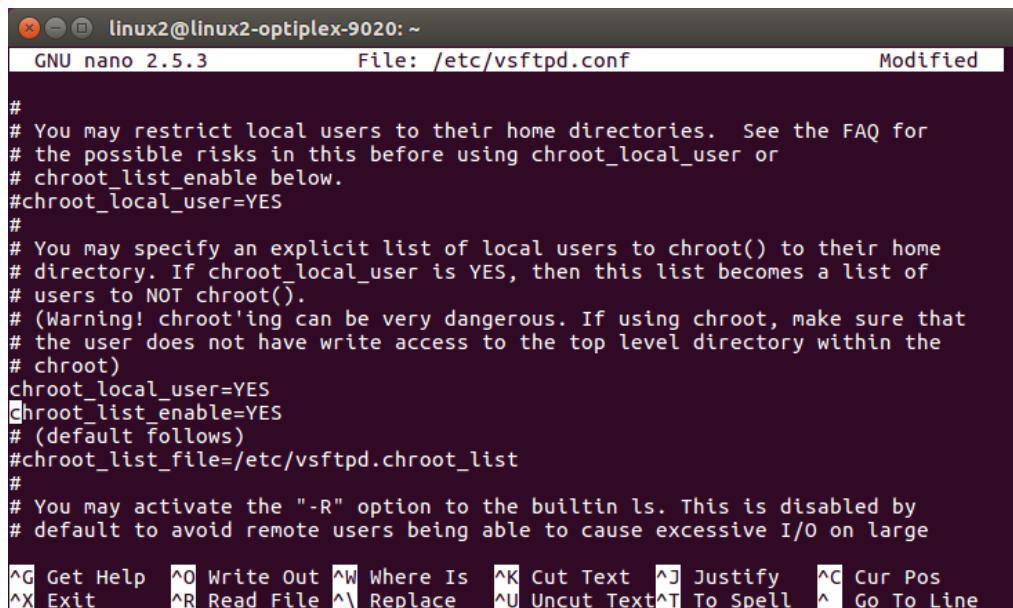
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode.
# Beware that on some FTP servers, ASCII support allows a denial of service
# attack (DoS) via the command "SIZE /big/file" in ASCII mode. vsftpd
# predicted this attack and has always been safe, reporting the size of the
# raw file.
# ASCII mangling is a horrible feature of the protocol.
ascii_upload_enable=YES
ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell ^L Go To Line

```

Figure 5. 64: Uncommenting ascii\_upload\_enable and  
ascii\_download\_enable

6. Uncomment “chroot\_list\_enable=YES” and “chroot\_local\_user=YES”.



```

linux2@linux2-optiplex-9020: ~
GNU nano 2.5.3           File: /etc/vsftpd.conf           Modified

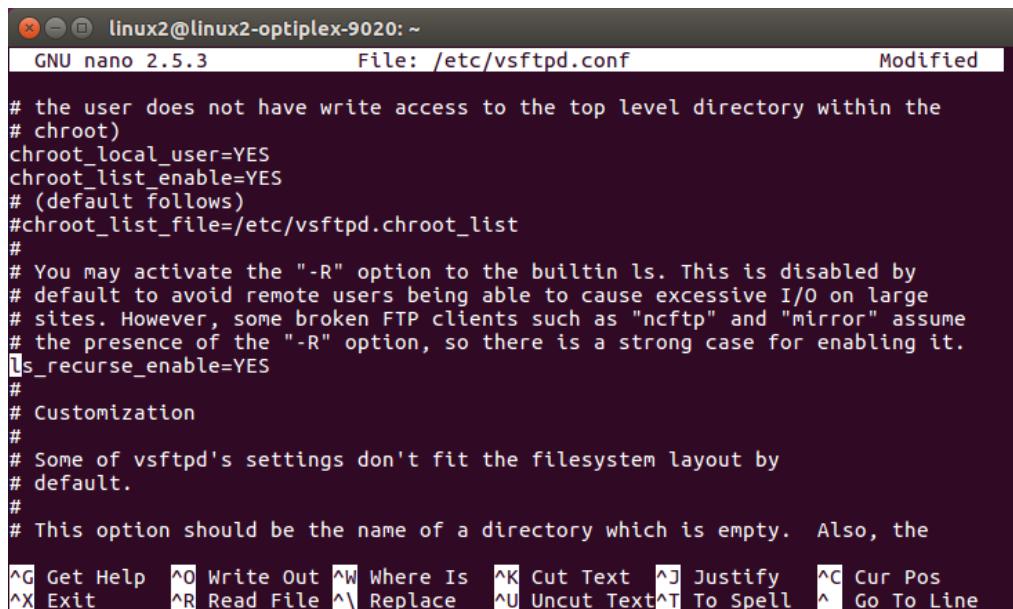
#
# You may restrict local users to their home directories. See the FAQ for
# the possible risks in this before using chroot_local_user or
# chroot_list_enable below.
#chroot_local_user=YES
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd.chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell ^L Go To Line

```

Figure 5. 65: Uncommenting chroot\_local\_user and  
chroot\_list\_enable

7. Uncomment “ls\_recurse\_enable=YES”.



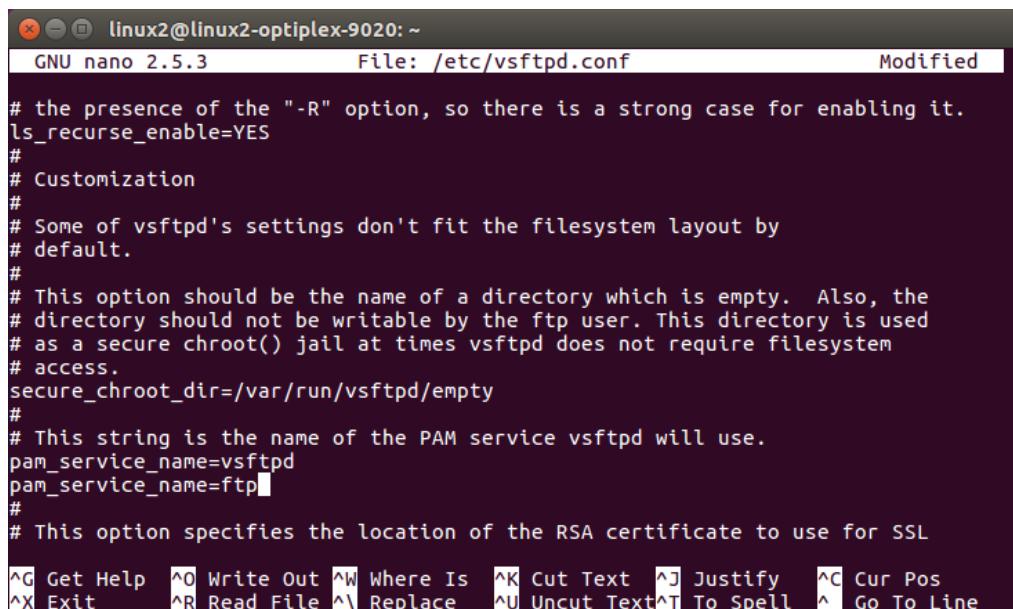
```
linux2@linux2-optiplex-9020: ~
GNU nano 2.5.3          File: /etc/vsftpd.conf          Modified

# the user does not have write access to the top level directory within the
# chroot)
chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd.chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
ls_recurse_enable=YES
#
# Customization
#
# Some of vsftpd's settings don't fit the filesystem layout by
# default.
#
# This option should be the name of a directory which is empty. Also, the

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^L Replace   ^U Uncut Text^T To Spell ^_ Go To Line
```

Figure 5. 66: Uncommenting ls\_recurse\_enable

8. Add the line “pam\_service\_name=ftp” under “pam\_service\_name=vsftpd”.



```
linux2@linux2-optiplex-9020: ~
GNU nano 2.5.3          File: /etc/vsftpd.conf          Modified

# the presence of the "-R" option, so there is a strong case for enabling it.
ls_recurse_enable=YES
#
# Customization
#
# Some of vsftpd's settings don't fit the filesystem layout by
# default.
#
# This option should be the name of a directory which is empty. Also, the
# directory should not be writable by the ftp user. This directory is used
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
pam_service_name=ftp#
#
# This option specifies the location of the RSA certificate to use for SSL

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^L Replace   ^U Uncut Text^T To Spell ^_ Go To Line
```

Figure 5. 67: Adding pam\_service\_name=ftp

9. Open the sshd.config file by entering the command “sudo nano etc/ssh/sshd\_config”.

```
linux2@linux2-optiplex-9020:~$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
openSSH-server is already the newest version (1:7.2p2-4ubuntu2.2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
linux2@linux2-optiplex-9020:~$ sudo nano /etc/ssh/sshd_config
linux2@linux2-optiplex-9020:~$ nano /etc/ssh/sshd_config
[sudo] password for linux2:
linux2@linux2-optiplex-9020:~$
```

Figure 5. 68: Opening ssh/sshd\_config file

10. Uncomment “PermitEmptyPasswords no” in the configuration file.

```
RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile      %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
#IgnoreUserKnownHosts yes

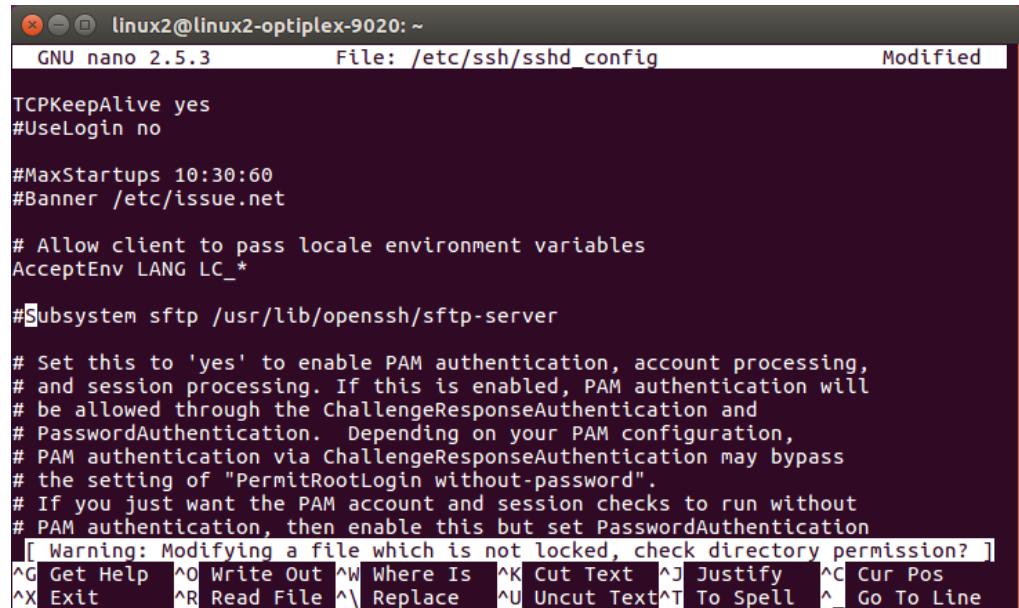
# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
#Overwritten by lwidentity: ChallengeResponseAuthentication no

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^L Replace   ^U Uncut Text^T To Spell  ^G Go To Line
```

Figure 5. 69: Uncomment PermitEmptyPasswords no

11. Add the # in the line “Subsystem sftp /usr/lib/openssh/sftp-server”.



```
linux2@linux2-optiplex-9020: ~
GNU nano 2.5.3           File: /etc/ssh/sshd_config           Modified

TCPKeepAlive yes
#UseLogin no

#MaxStartups 10:30:60
#Banner /etc/issue.net

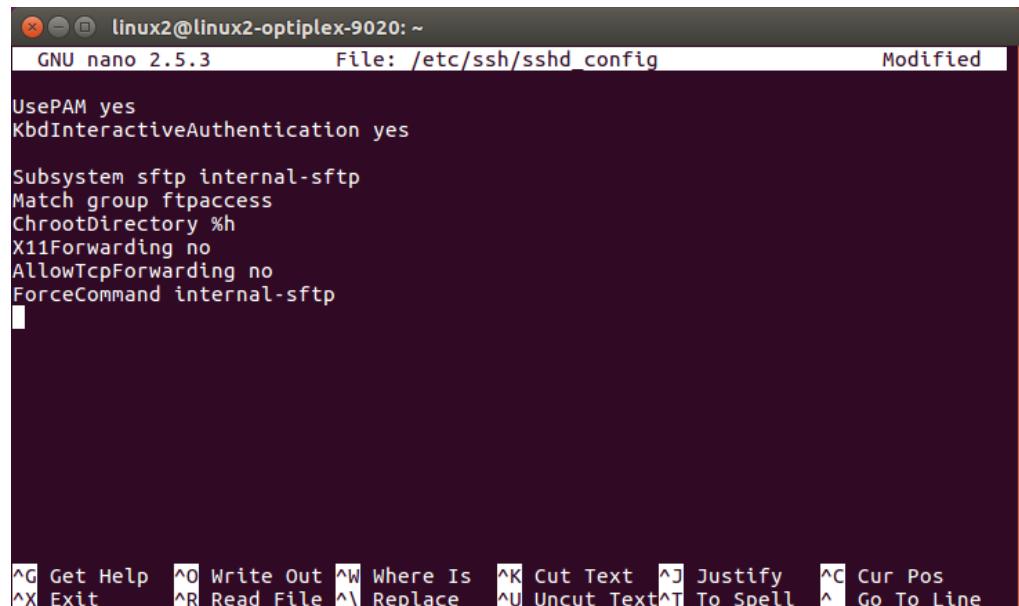
# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

#Subsystem sftp /usr/lib/openssh/sftp-server

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
[ Warning: Modifying a file which is not locked, check directory permission? ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell ^L Go To Line
```

Figure 5. 70: Commenting Subsystem sftp /usr/lib/openssh/sftp-server

12. Add the “Subsystem sftp internal-sftp”, “Match group ftpaccess”, “ChrootDirectory %h”, X11Forwarding no”, “AllowTcpForwarding no” and “ForceCommand internal-sftp” at the bottom of the file. Exit and save the changes.



```
linux2@linux2-optiplex-9020: ~
GNU nano 2.5.3           File: /etc/ssh/sshd_config           Modified

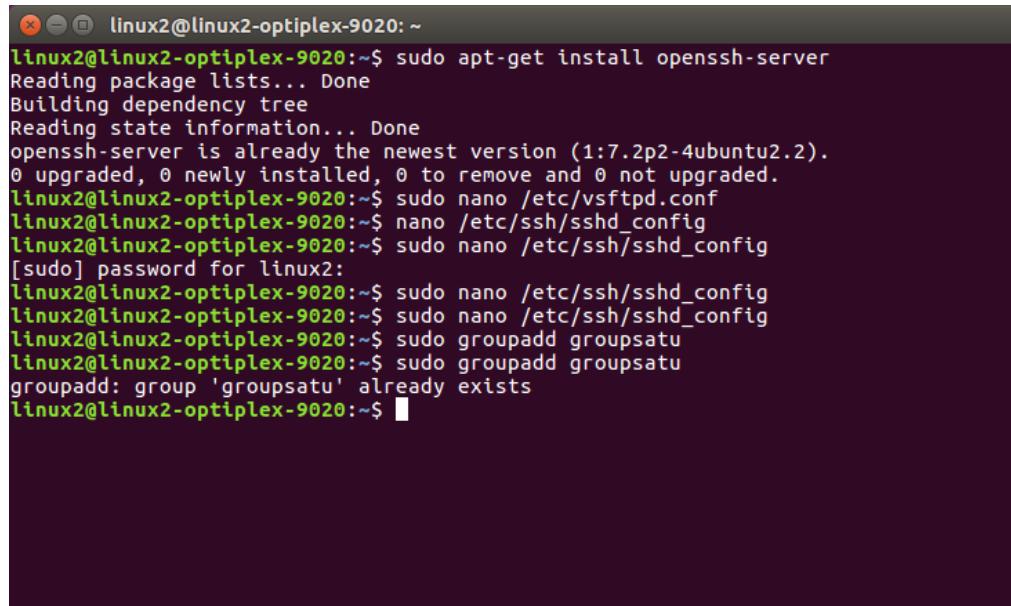
UsePAM yes
KbdInteractiveAuthentication yes

Subsystem sftp internal-sftp
Match group ftpaccess
ChrootDirectory %h
X11Forwarding no
AllowTcpForwarding no
ForceCommand internal-sftp

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell ^L Go To Line
```

Figure 5. 71: Adding lines the /etc/shh/sshd\_config

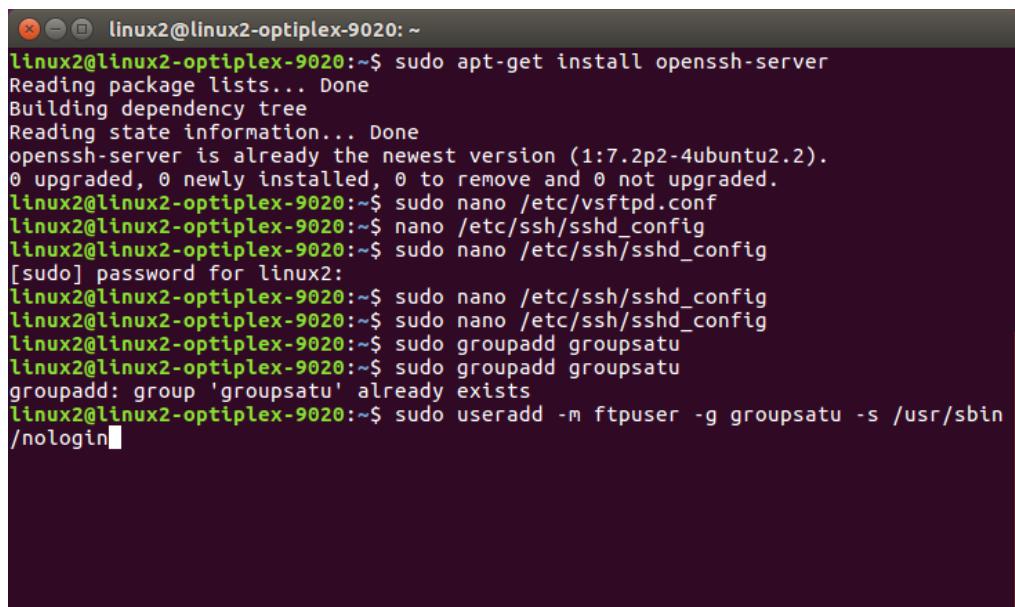
13. Create a group called groupsatu.



```
linux2@linux2-optiplex-9020:~$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-server is already the newest version (1:7.2p2-4ubuntu2.2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
linux2@linux2-optiplex-9020:~$ sudo nano /etc/vsftpd.conf
linux2@linux2-optiplex-9020:~$ nano /etc/ssh/sshd_config
linux2@linux2-optiplex-9020:~$ sudo nano /etc/ssh/sshd_config
[sudo] password for linux2:
linux2@linux2-optiplex-9020:~$ sudo nano /etc/ssh/sshd_config
linux2@linux2-optiplex-9020:~$ sudo nano /etc/ssh/sshd_config
linux2@linux2-optiplex-9020:~$ sudo groupadd groupsatu
linux2@linux2-optiplex-9020:~$ sudo groupadd groupsatu
groupadd: group 'groupsatu' already exists
linux2@linux2-optiplex-9020:~$
```

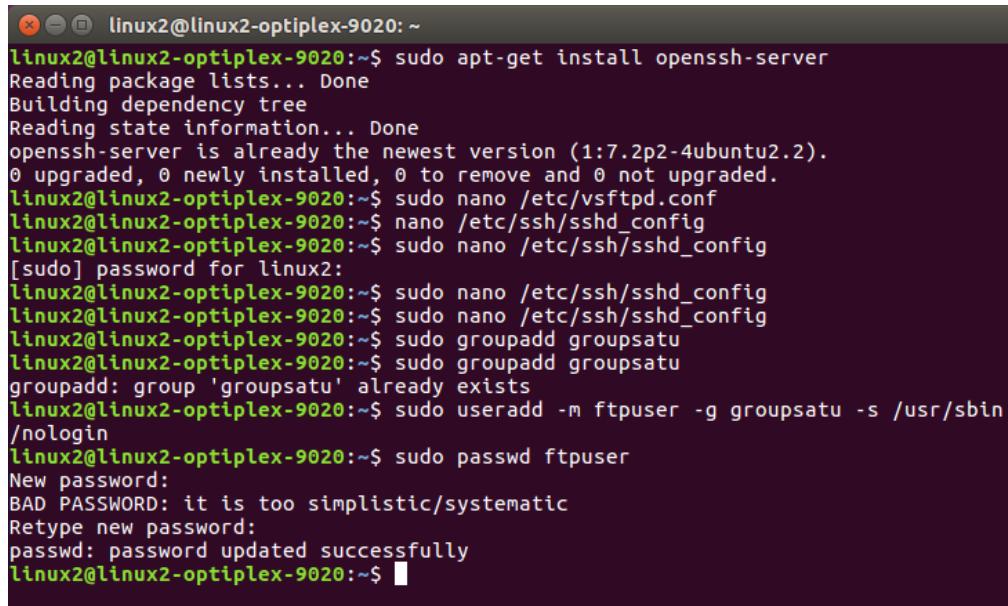
Figure 5. 72: Creating new group

14. Create a user called ftpuser and add the user in the groupsatu group.



```
linux2@linux2-optiplex-9020:~$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-server is already the newest version (1:7.2p2-4ubuntu2.2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
linux2@linux2-optiplex-9020:~$ sudo nano /etc/vsftpd.conf
linux2@linux2-optiplex-9020:~$ nano /etc/ssh/sshd_config
linux2@linux2-optiplex-9020:~$ sudo nano /etc/ssh/sshd_config
[sudo] password for linux2:
linux2@linux2-optiplex-9020:~$ sudo nano /etc/ssh/sshd_config
linux2@linux2-optiplex-9020:~$ sudo nano /etc/ssh/sshd_config
linux2@linux2-optiplex-9020:~$ sudo groupadd groupsatu
linux2@linux2-optiplex-9020:~$ sudo groupadd groupsatu
groupadd: group 'groupsatu' already exists
linux2@linux2-optiplex-9020:~$ sudo useradd -m ftpuser -g groupsatu -s /usr/sbin/nologin
```

Figure 5. 73: Creating new user

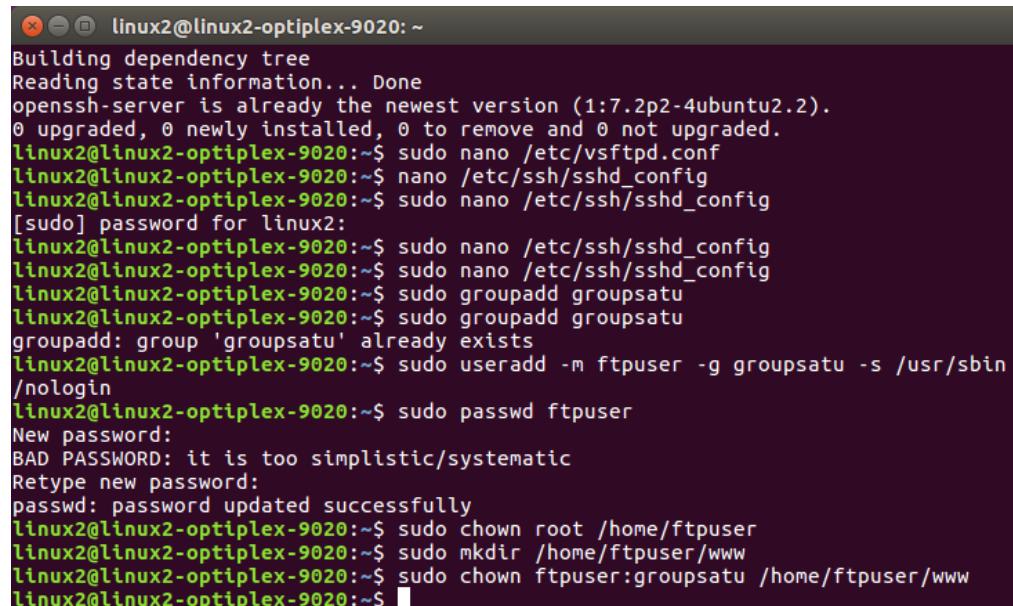


```

linux2@linux2-optiplex-9020:~$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-server is already the newest version (1:7.2p2-4ubuntu2.2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
linux2@linux2-optiplex-9020:~$ sudo nano /etc/vsftpd.conf
linux2@linux2-optiplex-9020:~$ nano /etc/ssh/sshd_config
linux2@linux2-optiplex-9020:~$ sudo nano /etc/ssh/sshd_config
[sudo] password for linux2:
linux2@linux2-optiplex-9020:~$ sudo nano /etc/ssh/sshd_config
linux2@linux2-optiplex-9020:~$ sudo nano /etc/ssh/sshd_config
linux2@linux2-optiplex-9020:~$ sudo groupadd groupsatu
linux2@linux2-optiplex-9020:~$ sudo groupadd groupsatu
groupadd: group 'groupsatu' already exists
linux2@linux2-optiplex-9020:~$ sudo useradd -m ftpuser -g groupsatu -s /usr/sbin/nologin
linux2@linux2-optiplex-9020:~$ sudo passwd ftpuser
New password:
BAD PASSWORD: it is too simplistic/systematic
Retype new password:
passwd: password updated successfully
linux2@linux2-optiplex-9020:~$ 
```

Figure 5. 74: Entering password for user

15. Create a directory for the “ftpaccess” user to access.

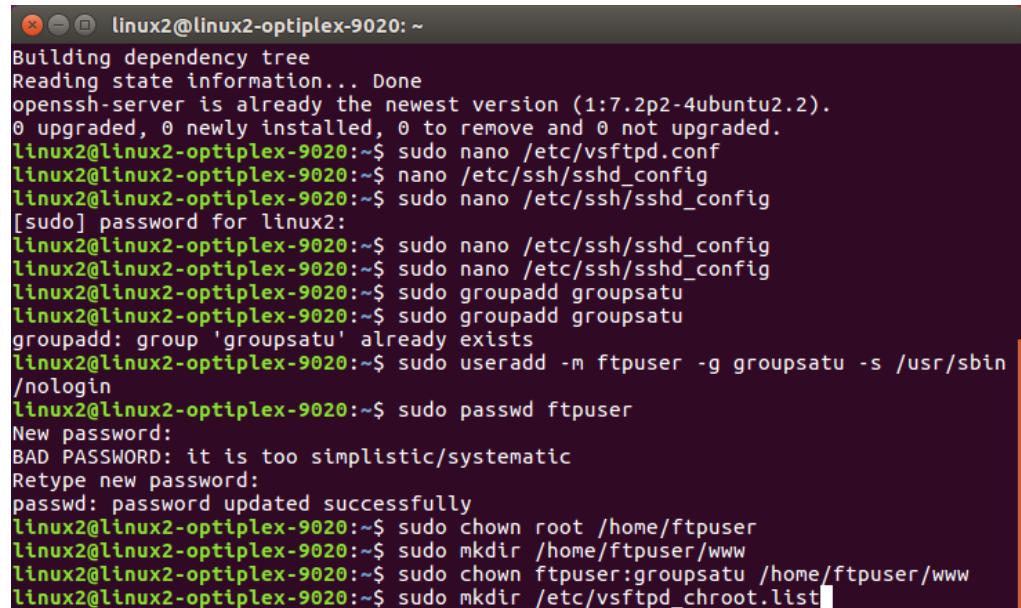


```

Building dependency tree
Reading state information... Done
openssh-server is already the newest version (1:7.2p2-4ubuntu2.2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
linux2@linux2-optiplex-9020:~$ sudo nano /etc/vsftpd.conf
linux2@linux2-optiplex-9020:~$ nano /etc/ssh/sshd_config
linux2@linux2-optiplex-9020:~$ sudo nano /etc/ssh/sshd_config
[sudo] password for linux2:
linux2@linux2-optiplex-9020:~$ sudo nano /etc/ssh/sshd_config
linux2@linux2-optiplex-9020:~$ sudo nano /etc/ssh/sshd_config
linux2@linux2-optiplex-9020:~$ sudo groupadd groupsatu
linux2@linux2-optiplex-9020:~$ sudo groupadd groupsatu
groupadd: group 'groupsatu' already exists
linux2@linux2-optiplex-9020:~$ sudo useradd -m ftpuser -g groupsatu -s /usr/sbin/nologin
linux2@linux2-optiplex-9020:~$ sudo passwd ftpuser
New password:
BAD PASSWORD: it is too simplistic/systematic
Retype new password:
passwd: password updated successfully
linux2@linux2-optiplex-9020:~$ sudo chown root /home/ftpuser
linux2@linux2-optiplex-9020:~$ sudo mkdir /home/ftpuser/www
linux2@linux2-optiplex-9020:~$ sudo chown ftpuser:groupsatu /home/ftpuser/www
linux2@linux2-optiplex-9020:~$ 
```

Figure 5. 75: Creating directory for user

16. Create vsftpd\_chroot.list by typing “sudo mkdir /etc/vsftpd\_chroot.list



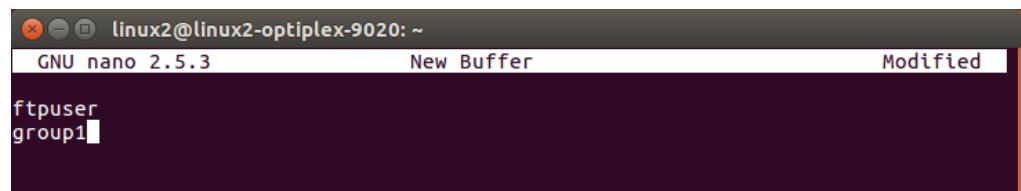
```

linux2@linux2-optiplex-9020: ~
Building dependency tree
Reading state information... Done
openSSH-server is already the newest version (1:7.2p2-4ubuntu2.2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
linux2@linux2-optiplex-9020:~$ sudo nano /etc/vsftpd.conf
linux2@linux2-optiplex-9020:~$ nano /etc/ssh/sshd_config
linux2@linux2-optiplex-9020:~$ sudo nano /etc/ssh/sshd_config
[sudo] password for linux2:
linux2@linux2-optiplex-9020:~$ sudo nano /etc/ssh/sshd_config
linux2@linux2-optiplex-9020:~$ sudo nano /etc/ssh/sshd_config
linux2@linux2-optiplex-9020:~$ sudo groupadd groupsatu
linux2@linux2-optiplex-9020:~$ sudo groupadd groupsatu
groupadd: group 'groupsatu' already exists
linux2@linux2-optiplex-9020:~$ sudo useradd -m ftpuser -g groupsatu -s /usr/sbin/nologin
linux2@linux2-optiplex-9020:~$ sudo passwd ftpuser
New password:
BAD PASSWORD: it is too simplistic/systematic
Retype new password:
passwd: password updated successfully
linux2@linux2-optiplex-9020:~$ sudo chown root /home/ftpuser
linux2@linux2-optiplex-9020:~$ sudo mkdir /home/ftpuser/www
linux2@linux2-optiplex-9020:~$ sudo chown ftpuser:groupsatu /home/ftpuser/www
linux2@linux2-optiplex-9020:~$ sudo mkdir /etc/vsftpd_chroot.list

```

Figure 5. 76: Creating /etc/vsftpd\_chroot.list file

17. Add “ftpuser” in the /etc/vsftpd\_chroot.list.



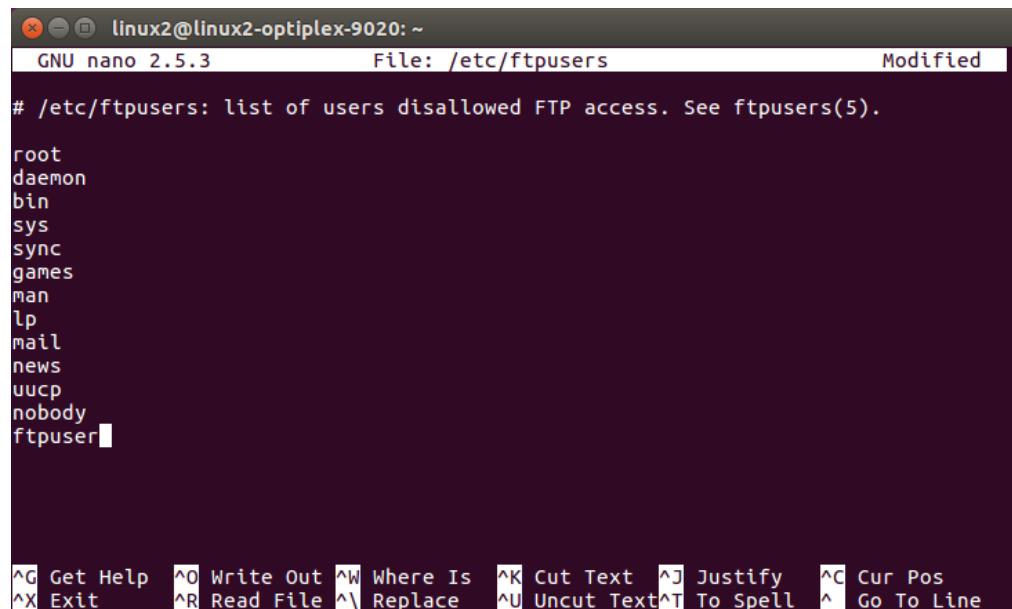
```

linux2@linux2-optiplex-9020: ~
GNU nano 2.5.3          New Buffer          Modified
ftpuser
group1

```

Figure 5. 77: Adding user in the /etc/vsftpd\_chroot.list

18. Go to /etc/ftpusers file and add the “ftpuser” in it.



```
linux2@linux2-optiplex-9020: ~
GNU nano 2.5.3           File: /etc/ftpusers          Modified

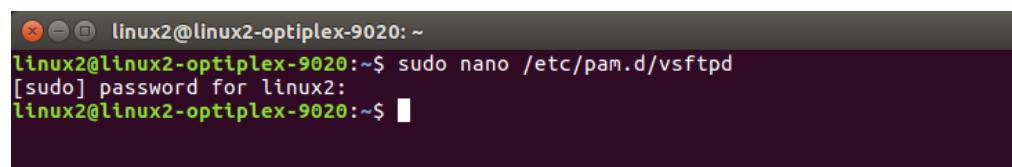
# /etc/ftpusers: list of users disallowed FTP access. See ftpusers(5).

root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
nobody
ftpuser

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text^T To Spell  ^L Go To Line
```

Figure 5. 78: Adding ftpuser in /etc/ftpusers

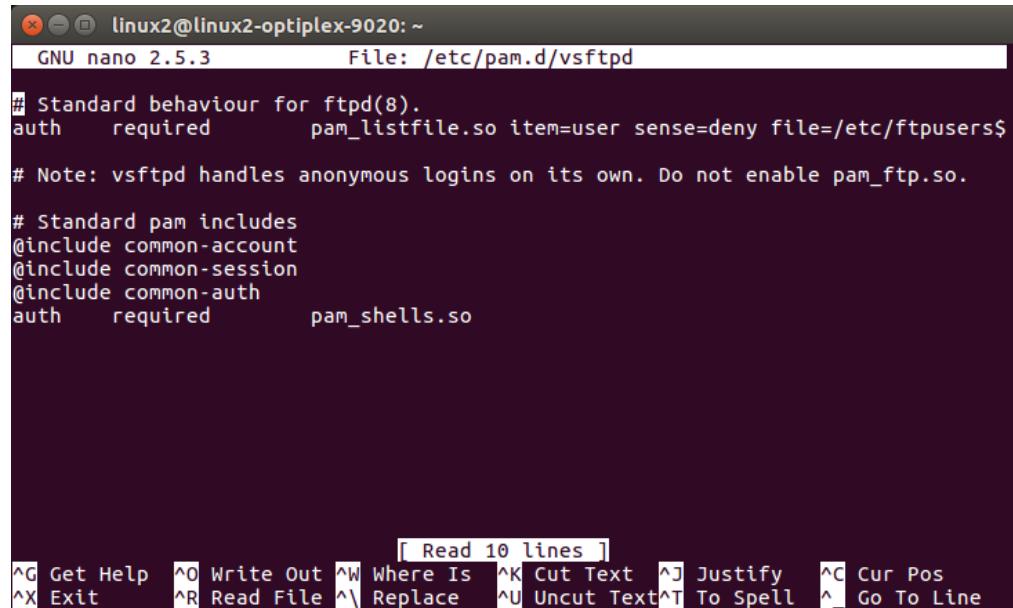
19. Open the pam.d/vsftpd file by entering the command “sudo nano /etc/pam.d/vsftpd”.



```
linux2@linux2-optiplex-9020: ~
linux2@linux2-optiplex-9020:~$ sudo nano /etc/pam.d/vsftpd
[sudo] password for linux2:
linux2@linux2-optiplex-9020:~$
```

Figure 5. 79: Opening /etc/pam.d/vsftpd file

20. Specify the directory for “ftpuser” at the “file=”.



```

linux2@linux2-optiplex-9020: ~
GNU nano 2.5.3           File: /etc/pam.d/vsftpd

# Standard behaviour for ftpd(8).
auth    required      pam_listfile.so item=user sense=deny file=/etc/ftpusers$ 

# Note: vsftpd handles anonymous logins on its own. Do not enable pam_ftp.so.

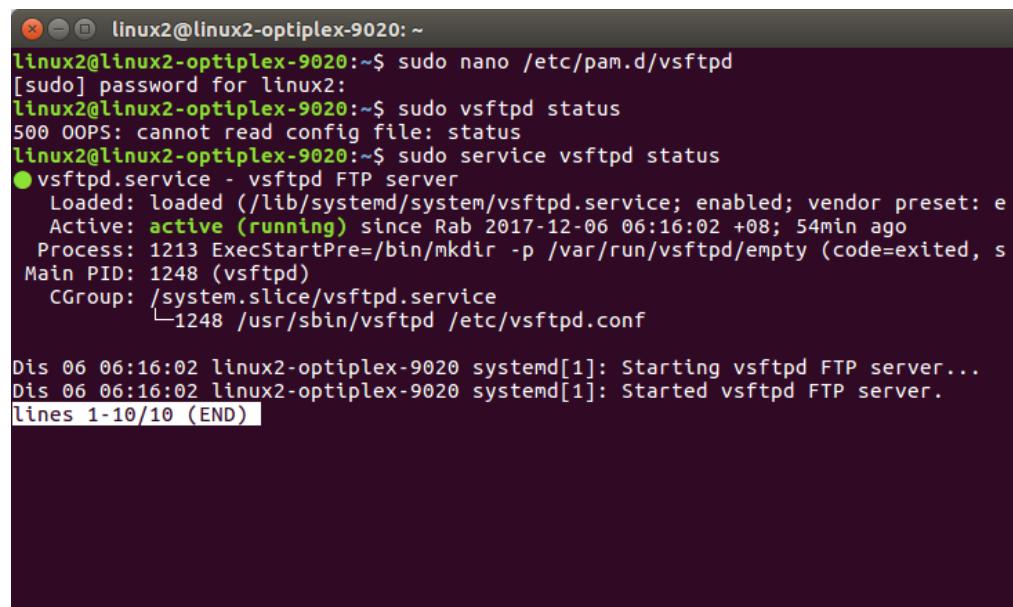
# Standard pam includes
@include common-account
@include common-session
@include common-auth
auth    required      pam_shells.so

[ Read 10 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^L Replace   ^U Uncut Text^T To Spell ^A Go To Line

```

Figure 5. 80: Specifying directory for the user

21. Then, check the status of vsftpd by entering “sudo vsftpd status”.



```

linux2@linux2-optiplex-9020: ~
linux2@linux2-optiplex-9020:~$ sudo nano /etc/pam.d/vsftpd
[sudo] password for linux2:
linux2@linux2-optiplex-9020:~$ sudo vsftpd status
500 OOPS: cannot read config file: status
linux2@linux2-optiplex-9020:~$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: e
   Active: active (running) since Rab 2017-12-06 06:16:02 +08; 54min ago
     Process: 1213 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, s
Main PID: 1248 (vsftpd)
   CGroup: /system.slice/vsftpd.service
           └─1248 /usr/sbin/vsftpd /etc/vsftpd.conf

Dis 06 06:16:02 linux2-optiplex-9020 systemd[1]: Starting vsftpd FTP server...
Dis 06 06:16:02 linux2-optiplex-9020 systemd[1]: Started vsftpd FTP server.
lines 1-10/10 (END)

```

Figure 5. 81: Checking directory for the user

### 5.3.9 SAMBA

Step 1: Open terminal.

Step 2: To install samba, enter sudo apt install samba.

Step 3: Enter sudo apt-get update to update repositories

```
linux1@linux1-HP-xw6600-Workstation:~$ sudo apt install samba
[sudo] password for linux1:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  attr python-crypto python-dnspython python-ldb python-samba python-tdb
    samba-common samba-common-bin samba-dsdb-modules samba-vfs-modules tdb-tools
Suggested packages:
  python-crypto-dbg python-crypto-doc bind9 bind9utils ctdb ldb-tools ntp
    smbldap-tools winbind heimdal-clients
The following NEW packages will be installed:
  attr python-crypto python-dnspython python-ldb python-samba python-tdb samba
    samba-common samba-common-bin samba-dsdb-modules samba-vfs-modules tdb-tools
0 upgraded, 12 newly installed, 0 to remove and 20 not upgraded.
Need to get 3,439 kB of archives.
After this operation, 25.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Figure 5. 82: sudo apt-get install samba

Step 4: Enter sudo smbpasswd -a group1 to add new user.

Step 5: Enter /etc/init.d/samba restart to restart samba.

```
linux1@linux1-HP-xw6600-Workstation:~$ sudo adduser group1
[sudo] password for linux1:
adduser: The user `group1' already exists.
linux1@linux1-HP-xw6600-Workstation:~$ sudo smbpasswd -a group1
New SMB password:
Retype new SMB password:
linux1@linux1-HP-xw6600-Workstation:~$ /etc/init.d/samba restart
[ ok ] Restarting nmbd (via systemctl): nmbd.service.
[ ok ] Restarting smbd (via systemctl): smbd.service.
[ ok ] Restarting samba-ad-dc (via systemctl): samba-ad-dc.service.
linux1@linux1-HP-xw6600-Workstation:~$ systemctl status samba
● samba.service
  Loaded: masked (/dev/null; bad)
  Active: inactive (dead)
linux1@linux1-HP-xw6600-Workstation:~$ █
```

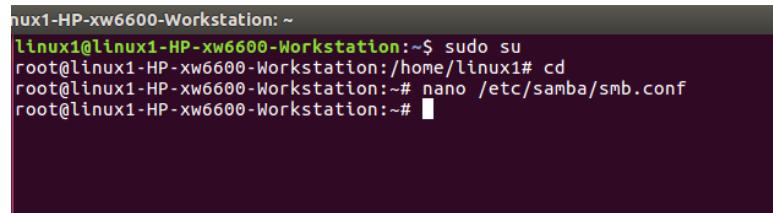
Figure 5. 83: Add New User & restart samba

Step 6: Enter sudo netstat -tulpn | grep smbd to view samba active port.

```
linux1@linux1-hp-xw6600-workstation:~$ sudo netstat -tulpn | grep smbd
tcp        0      0 0.0.0.0:445          0.0.0.0:*              LISTEN
8287/smbd
tcp        0      0 0.0.0.0:139          0.0.0.0:*              LISTEN
8287/smbd
tcp6       0      0 :::445               :::*                  LISTEN
8287/smbd
tcp6       0      0 :::139               :::*                  LISTEN
8287/smbd
linux1@linux1-hp-xw6600-workstation:~$ █
```

Figure 5. 84: sudo netstat -tulpn | grep smbd

Step 7: enter sudo vim /etc/samba/smb.conf to edit samba configuration

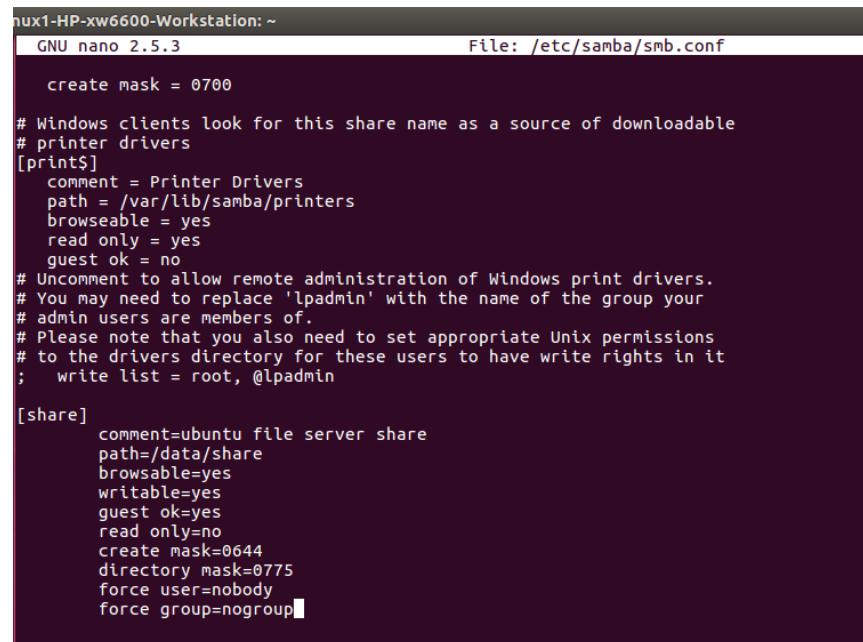


```
linux1@linux1-HP-xw6600-Workstation: ~
linux1@linux1-HP-xw6600-Workstation:~$ sudo su
root@linux1-HP-xw6600-Workstation:/home/linux1# cd
root@linux1-HP-xw6600-Workstation:~/# nano /etc/samba/smb.conf
root@linux1-HP-xw6600-Workstation:~/#
```

Figure 5. 85: nano /etc/samba/smb.conf

Step 8: To create shared folder for group 1

```
# sudo su
# mkdir -p /data/share
# cd /data/share
# touch group1.txt
```



```
linux1@linux1-HP-xw6600-Workstation: ~
GNU nano 2.5.3                                     File: /etc/samba/smb.conf

create mask = 0700

# Windows clients look for this share name as a source of downloadable
# printer drivers
[print$]
    comment = Printer Drivers
    path = /var/lib/samba/printers
    browsable = yes
    read only = yes
    guest ok = no
# Uncomment to allow remote administration of Windows print drivers.
# You may need to replace 'lpadmin' with the name of the group your
# admin users are members of.
# Please note that you also need to set appropriate Unix permissions
# to the drivers directory for these users to have write rights in it
;   write list = root, @lpadmin

[share]
    comment=ubuntu file server share
    path=/data/share
    browsable=yes
    writable=yes
    guest ok=yes
    read only=no
    create mask=0644
    directory mask=0775
    force user=nobody
    force group=nogroup
```

Figure 5. 86: Samba Configuration

```

linux1@linux1-HP-xw6600-Workstation: /data/share
linux1@linux1-HP-xw6600-Workstation:~$ sudo su
root@linux1-HP-xw6600-Workstation:/home/linux1# cd
root@linux1-HP-xw6600-Workstation:~# nano /etc/samba/smb.conf
root@linux1-HP-xw6600-Workstation:~#
root@linux1-HP-xw6600-Workstation:~# mkdir -p /data/share
root@linux1-HP-xw6600-Workstation:~# cd /data/share
root@linux1-HP-xw6600-Workstation:/data/share# touch group1.txt
root@linux1-HP-xw6600-Workstation:/data/share# ls
group1.txt
root@linux1-HP-xw6600-Workstation:/data/share# ll
total 8
drwxr-xr-x 2 root root 4096 Okt  9 02:47 .
drwxr-xr-x 3 root root 4096 Okt  9 02:47 ../
-rw-r--r-- 1 root root   0 Okt  9 02:47 group1.txt
root@linux1-HP-xw6600-Workstation:/data/share# cd ..
root@linux1-HP-xw6600-Workstation:/data# chown nobody.nogroup /data/share/group1.txt
root@linux1-HP-xw6600-Workstation:/data# cd /data/share
root@linux1-HP-xw6600-Workstation:/data/share# ll
total 8
drwxr-xr-x 2 root  root 4096 Okt  9 02:47 .
drwxr-xr-x 3 root  root 4096 Okt  9 02:47 ../
-rw-r--r-- 1 nobody nogroup   0 Okt  9 02:47 group1.txt
root@linux1-HP-xw6600-Workstation:/data/share# █

```

Figure 5. 87: Create Shared Folder

Step 9: To make file sharing between Ubuntu and Window:

1. Click on Home> Document> data
2. Right click on data and choose properties.
3. Click on Local Network Share > write ‘public’ as Share Name > tick on ‘Allow other to create and delete file on this folder’ and ‘Guest access (for people without a user account)’.

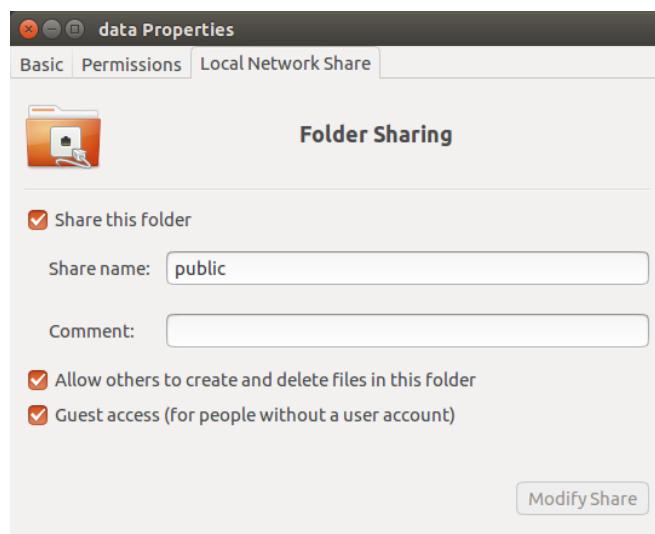
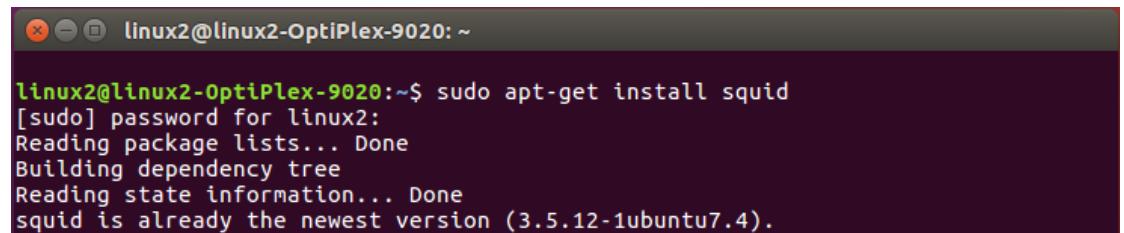


Figure 5. 88: 3Folder Sharing from Linux1 Server to Windows Server

### 5.3.10 PROXY SERVER

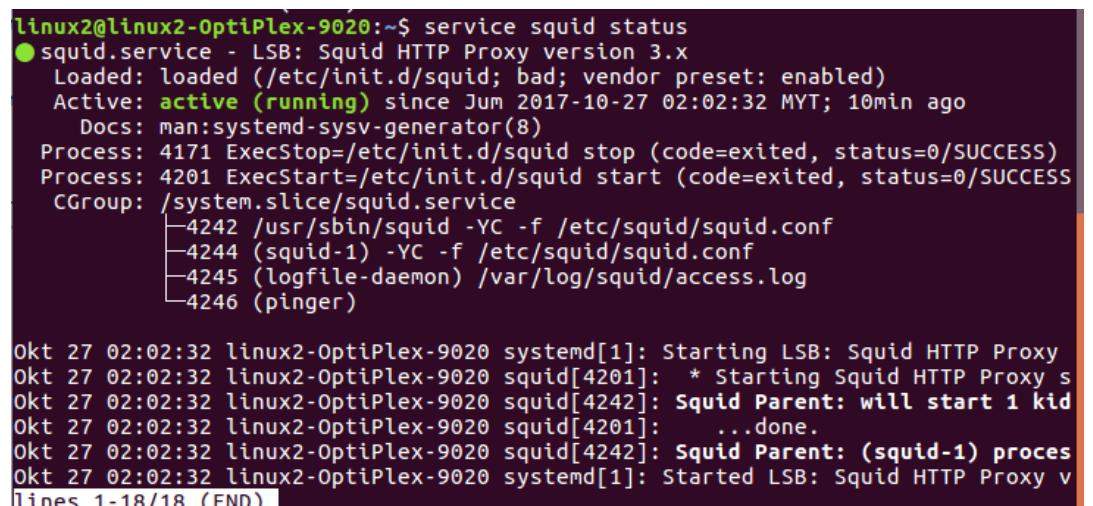
Step1: Install squid package



```
linux2@linux2-OptiPlex-9020:~$ sudo apt-get install squid
[sudo] password for linux2:
Reading package lists... Done
Building dependency tree
Reading state information... Done
squid is already the newest version (3.5.12-1ubuntu7.4).
```

Figure 5. 89: Install squid package

Step2: Check squid status

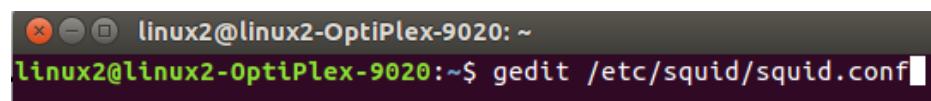


```
linux2@linux2-OptiPlex-9020:~$ service squid status
● squid.service - LSB: Squid HTTP Proxy version 3.x
  Loaded: loaded (/etc/init.d/squid; bad; vendor preset: enabled)
  Active: active (running) since Jun 2017-10-27 02:02:32 MYT; 10min ago
    Docs: man:systemd-sysv-generator(8)
  Process: 4171 ExecStop=/etc/init.d/squid stop (code=exited, status=0/SUCCESS)
  Process: 4201 ExecStart=/etc/init.d/squid start (code=exited, status=0/SUCCESS)
  CGroup: /system.slice/squid.service
          └─4242 /usr/sbin/squid -YC -f /etc/squid/squid.conf
              ├─4244 (squid-1) -YC -f /etc/squid/squid.conf
              ├─4245 (logfile-daemon) /var/log/squid/access.log
              ├─4246 (pinger)

okt 27 02:02:32 linux2-OptiPlex-9020 systemd[1]: Starting LSB: Squid HTTP Proxy
okt 27 02:02:32 linux2-OptiPlex-9020 squid[4201]: * Starting Squid HTTP Proxy s
okt 27 02:02:32 linux2-OptiPlex-9020 squid[4242]: Squid Parent: will start 1 kid
okt 27 02:02:32 linux2-OptiPlex-9020 squid[4201]: ...done.
okt 27 02:02:32 linux2-OptiPlex-9020 squid[4242]: Squid Parent: (squid-1) proces
okt 27 02:02:32 linux2-OptiPlex-9020 systemd[1]: Started LSB: Squid HTTP Proxy v
|lines 1-18/18 (END)|
```

Figure 5. 90: Check squid status

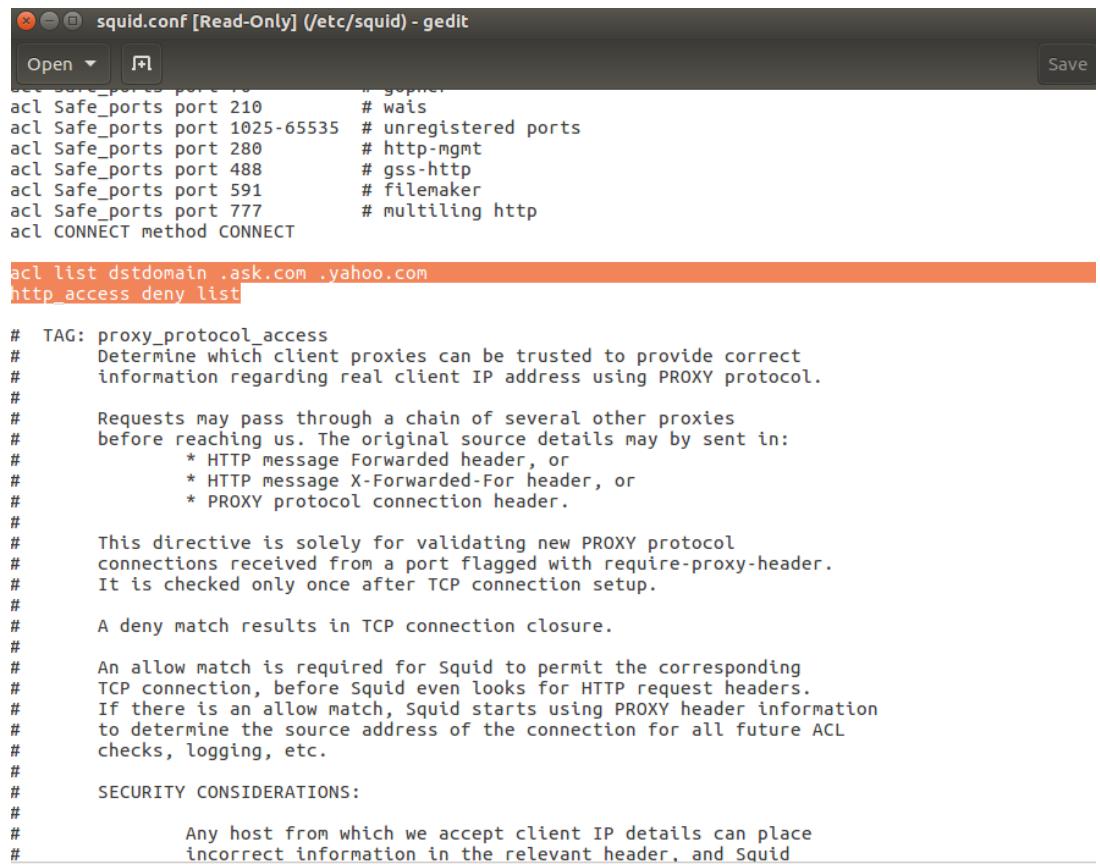
Step3: Enter squid configuration file



```
linux2@linux2-OptiPlex-9020:~$ gedit /etc/squid/squid.conf
```

Figure 5. 91: Enter squid configuration file

Step4: Edit squid configuration file



```

acl Safe_ports port 1024-65535 "gopher"
acl Safe_ports port 210      # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280      # http-mgmt
acl Safe_ports port 488      # gss-http
acl Safe_ports port 591      # filemaker
acl Safe_ports port 777      # multiling http
acl CONNECT method CONNECT

acl list dstdomain .ask.com .yahoo.com
http_access deny list

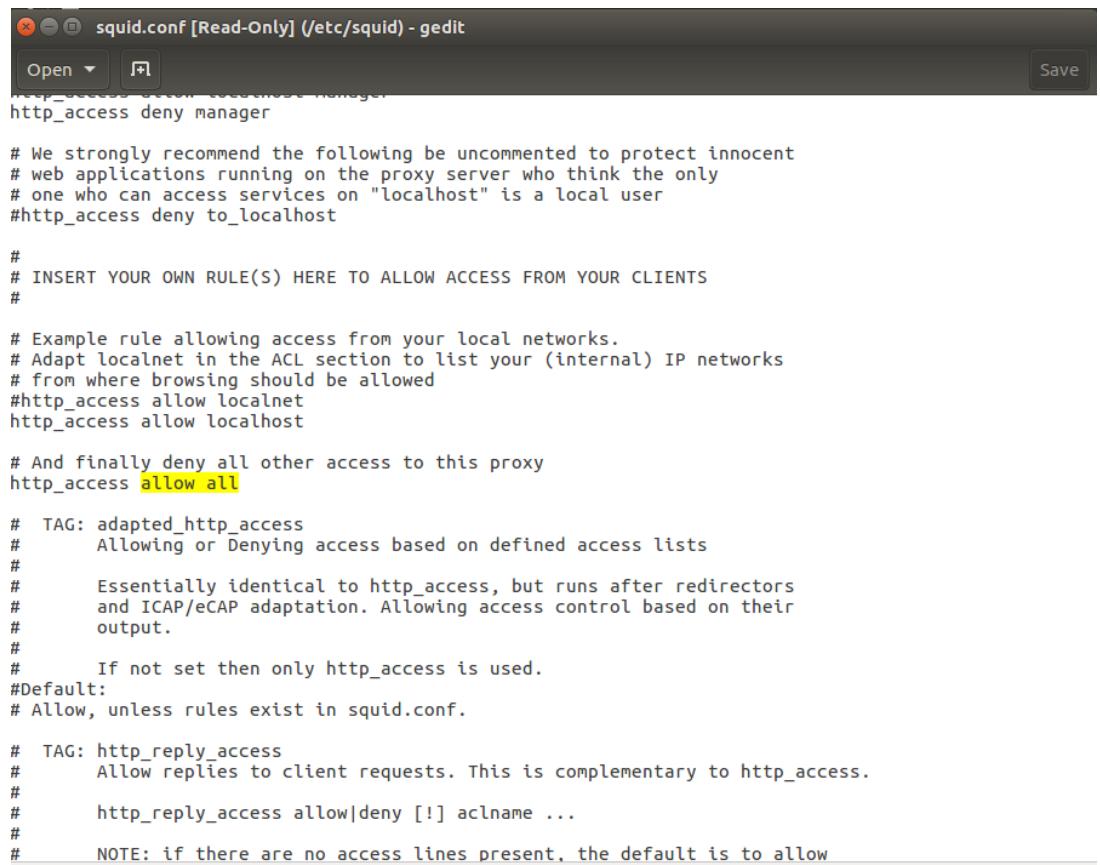
# TAG: proxy_protocol_access
# Determine which client proxies can be trusted to provide correct
# information regarding real client IP address using PROXY protocol.
#
# Requests may pass through a chain of several other proxies
# before reaching us. The original source details may be sent in:
#   * HTTP message Forwarded header, or
#   * HTTP message X-Forwarded-For header, or
#   * PROXY protocol connection header.

# This directive is solely for validating new PROXY protocol
# connections received from a port flagged with require-proxy-header.
# It is checked only once after TCP connection setup.
#
# A deny match results in TCP connection closure.
#
# An allow match is required for Squid to permit the corresponding
# TCP connection, before Squid even looks for HTTP request headers.
# If there is an allow match, Squid starts using PROXY header information
# to determine the source address of the connection for all future ACL
# checks, logging, etc.
#
# SECURITY CONSIDERATIONS:
#
# Any host from which we accept client IP details can place
# incorrect information in the relevant header, and Squid

```

Figure 5. 92: Edit ACL command on squid configuration file

Step5: Change ‘deny’ all to ‘allow’ all.



```

squid.conf [Read-Only] (/etc/squid) - gedit
Open Save
http_access deny manager
# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access allow all

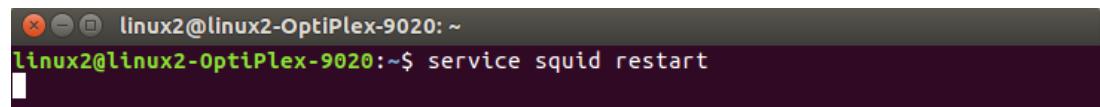
# TAG: adapted_http_access
#     Allowing or Denying access based on defined access lists
#
#     Essentially identical to http_access, but runs after redirectors
#     and ICAP/eCAP adaptation. Allowing access control based on their
#     output.
#
#     If not set then only http_access is used.
#Default:
# Allow, unless rules exist in squid.conf.

# TAG: http_reply_access
#     Allow replies to client requests. This is complementary to http_access.
#
#     http_reply_access allow|deny [!] aclname ...
#
#     NOTE: if there are no access lines present, the default is to allow

```

Figure 5. 93: Change http access

Step6: Restart squid service



```

linux2@linux2-OptiPlex-9020: ~
linus2@linus2-OptiPlex-9020:~$ service squid restart

```

Figure 5. 94: Restart squid service

Step7: Open your web browser

Step8: At the top right bar, click and select “Preferences” option

Step9: In “Network Proxy” select Settings option

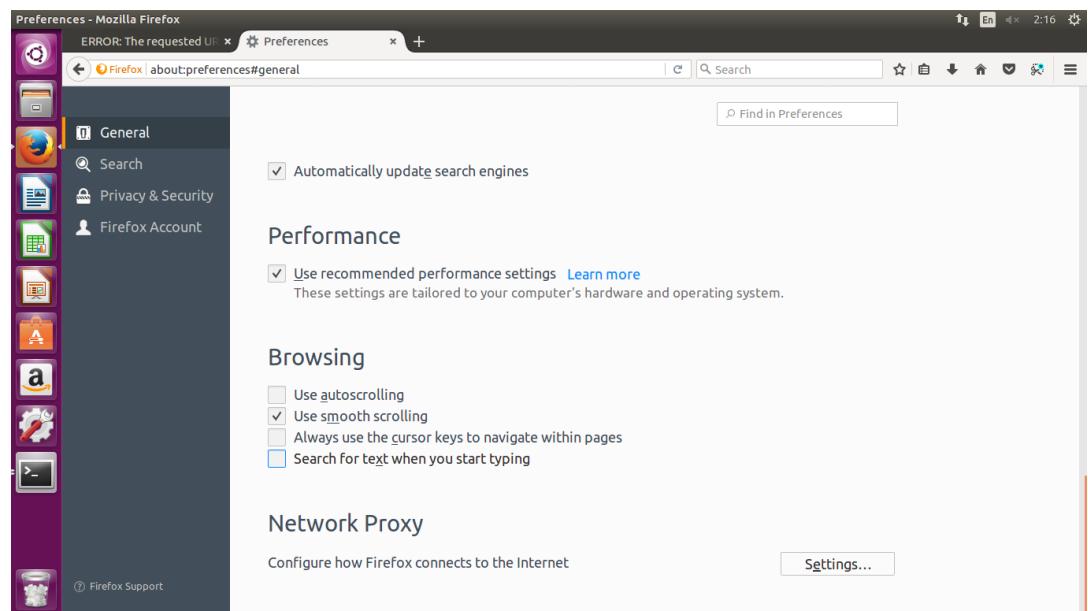


Figure 5. 95: Network proxy settings

Step10: Select “Manual proxy configuration” and fill in as below

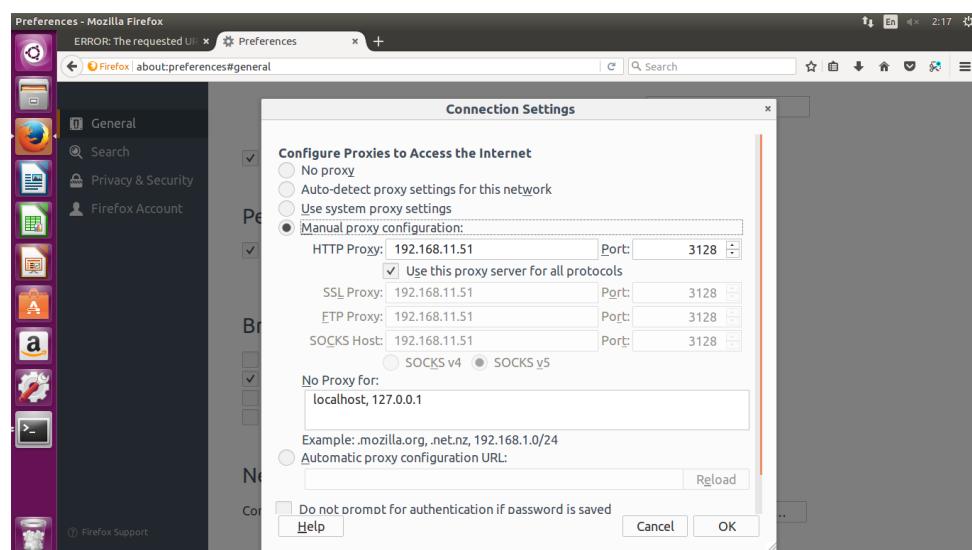


Figure 5. 96: Fill in the details on proxy manual settings

### 5.3.11 RADIUS SERVER FOR NETWORK ACCOUNTING

Step 1: Click on Server Manager > Roles > Add Roles.

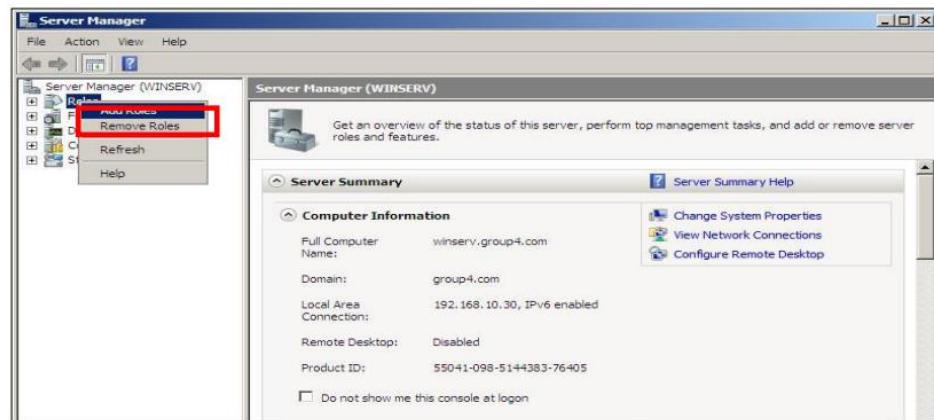


Figure 5. 97: Add Roles

Step 2: Then, in Before You Begin, after read the information, click Next.

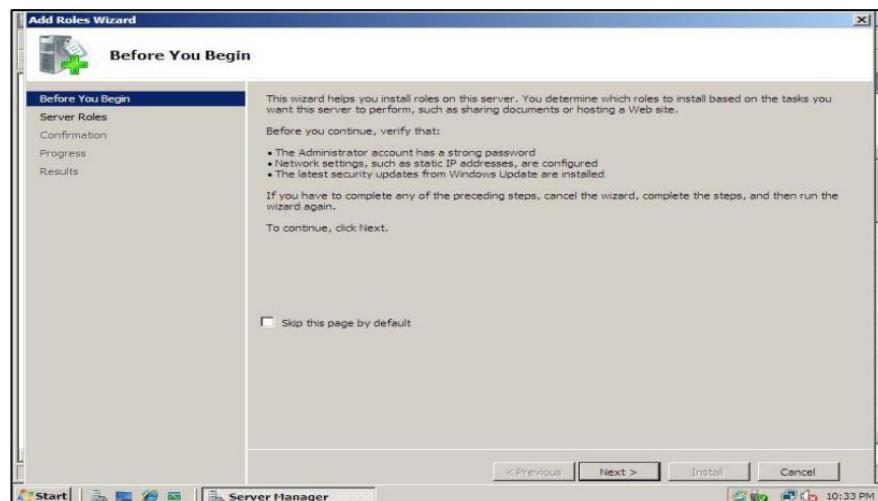


Figure 5. 98: Before You Begin

Step 3: In Add Roles Wizard, tick on Network Policy and Access Services.

Then click Next.

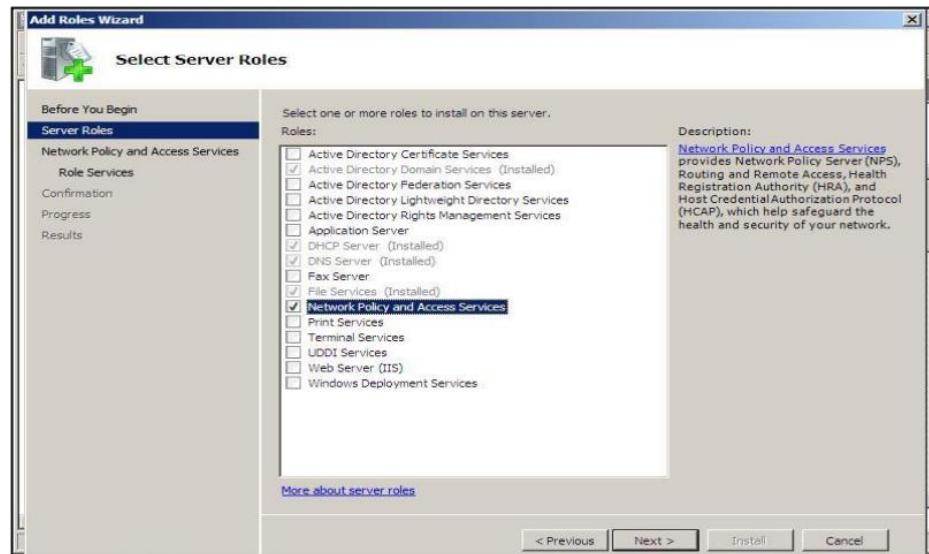


Figure 5. 99: Select Server Roles

Step 4: Read the information in Network Policy and Access Services then click Next.



Figure 5. 100: Network Policy and Access Services

Step 5: In Select Role Services, tick on Network Policy Server. Then, click Next.

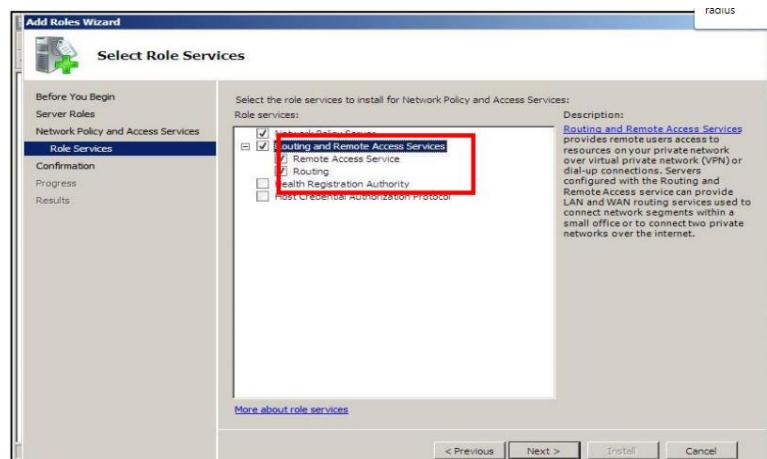


Figure 5. 101: Select Role Services.

Step 6: In Confirm Installation Selections page, click Install.

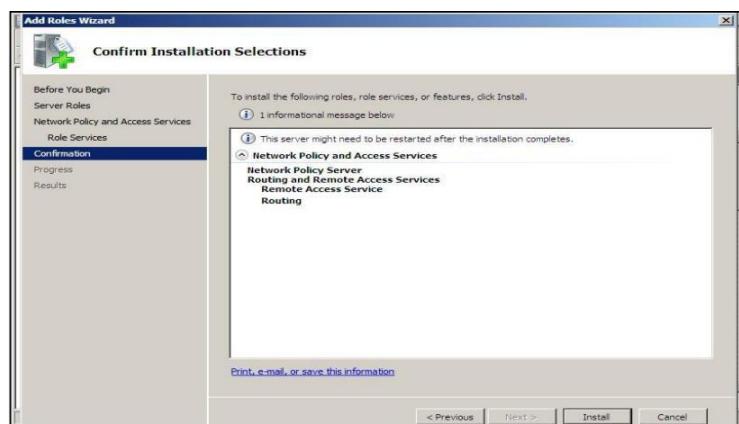


Figure 5. 102: Confirm Installation Selections.

Step 7: Installation Progress page.

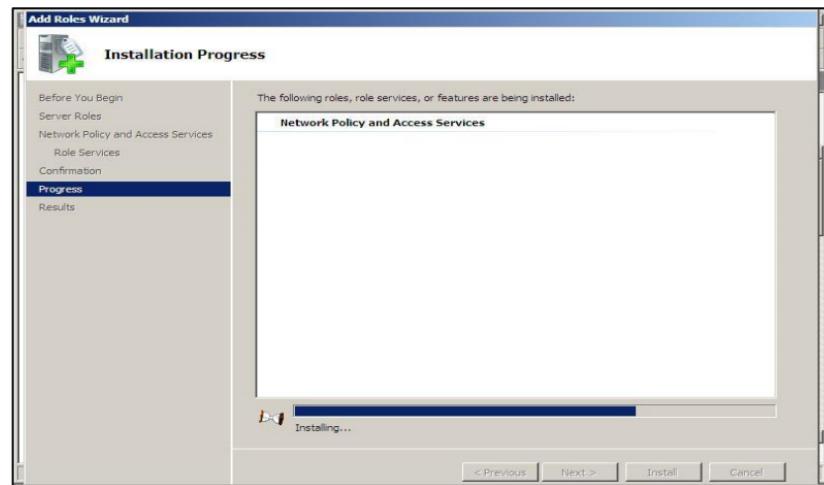


Figure 5. 103: Installation Progress.

Step 8: In Installation Results page show Installation succeeded. Then, click Close.

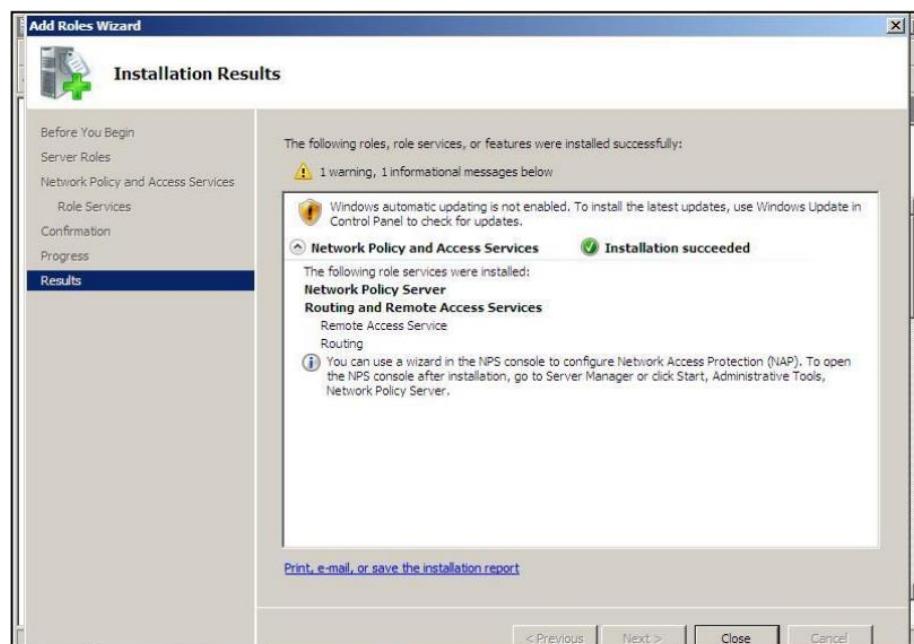


Figure 5. 104: Installation Progress.

Step 9: Click on Start > All Programs > Administrative Tools > Network Policy Server.

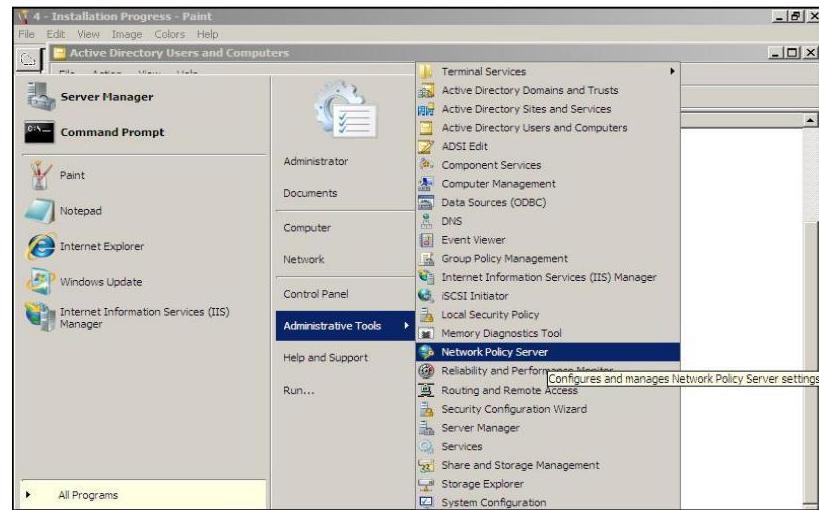


Figure 5. 105: Open NPS

Step 10: Right click on NPS (Local) > Register server in Active Directory.

Then popup windows, click OK.

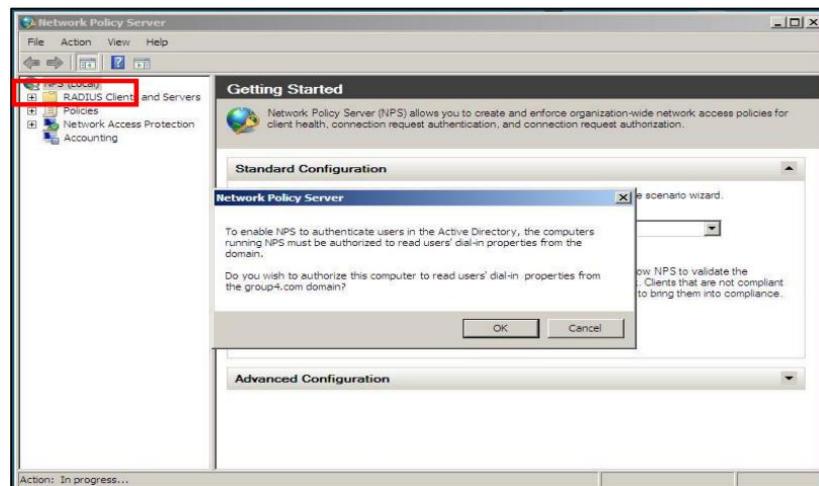


Figure 5. 106: Go to Network Policy Server

Step 11: Next, popup windows click OK.

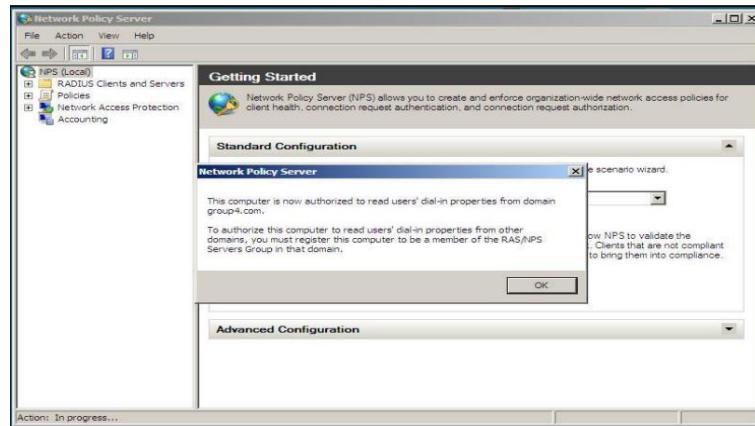


Figure 5. 107: Click OK

Step 12: Expand RADIUS Clients and Servers, right click on RADIUS Clients, and choose New RADIUS Client.

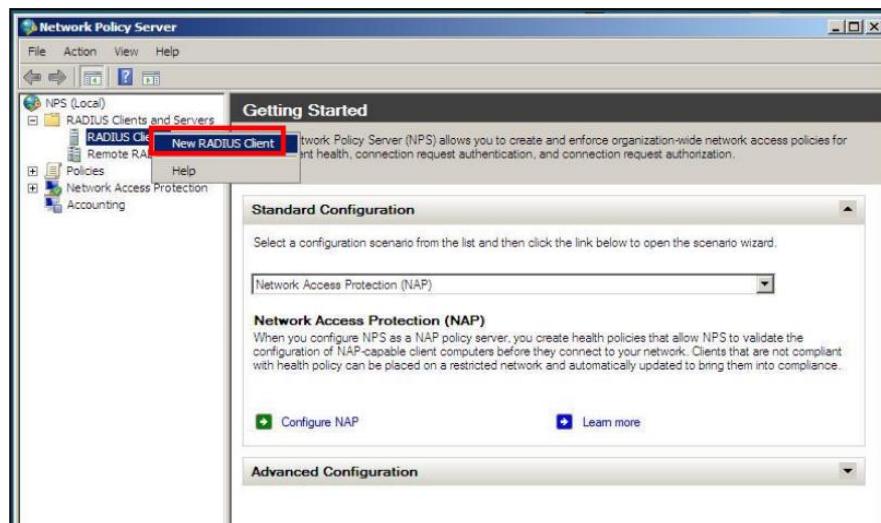


Figure 5. 108: New RADIUS Client.

Step 13: Enter Friendly Name and Address. Tick Manual shared secret and enter the Shared secret. Then, click OK.

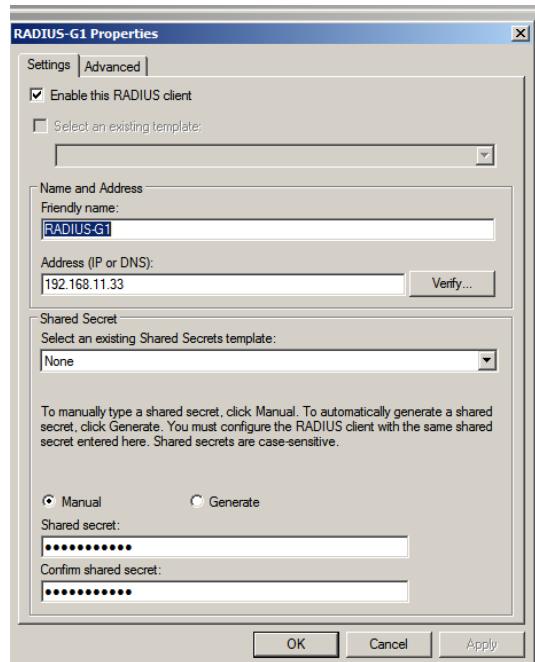


Figure 5. 109: RADIUS Client.

Step 14: Create a connection request policy. Expand the Policies, right click on Connection Request Policies and choose New.

Step 15: Enter the Policy Name and click Next.

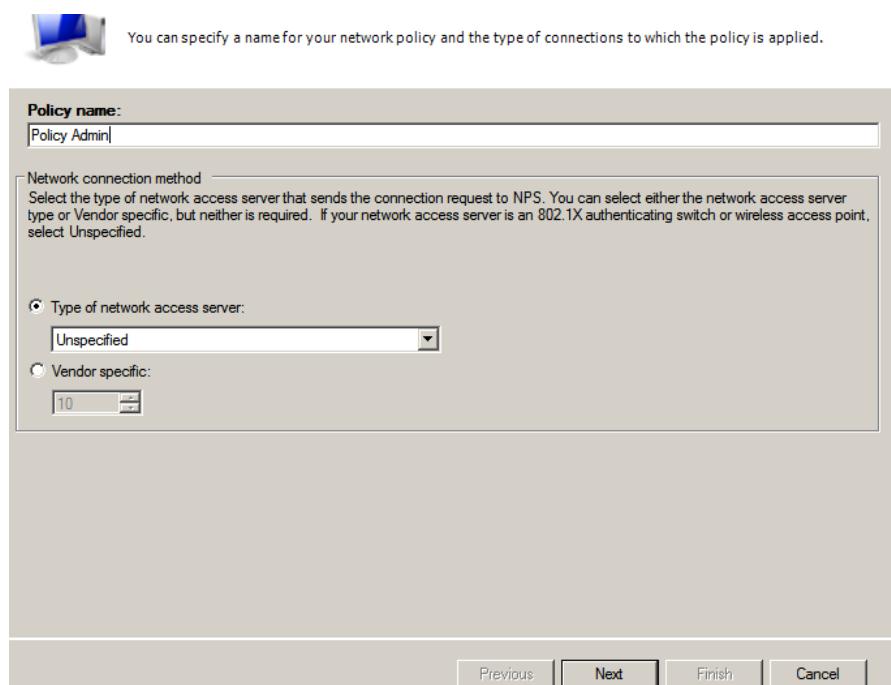


Figure 5. 110: Policy Name and Connection Type.

Step 16: On Specify Conditions page, click Add.



Figure 5. 111: Specify Conditions.

Step 17: Select the condition > User Groups, then click Add.

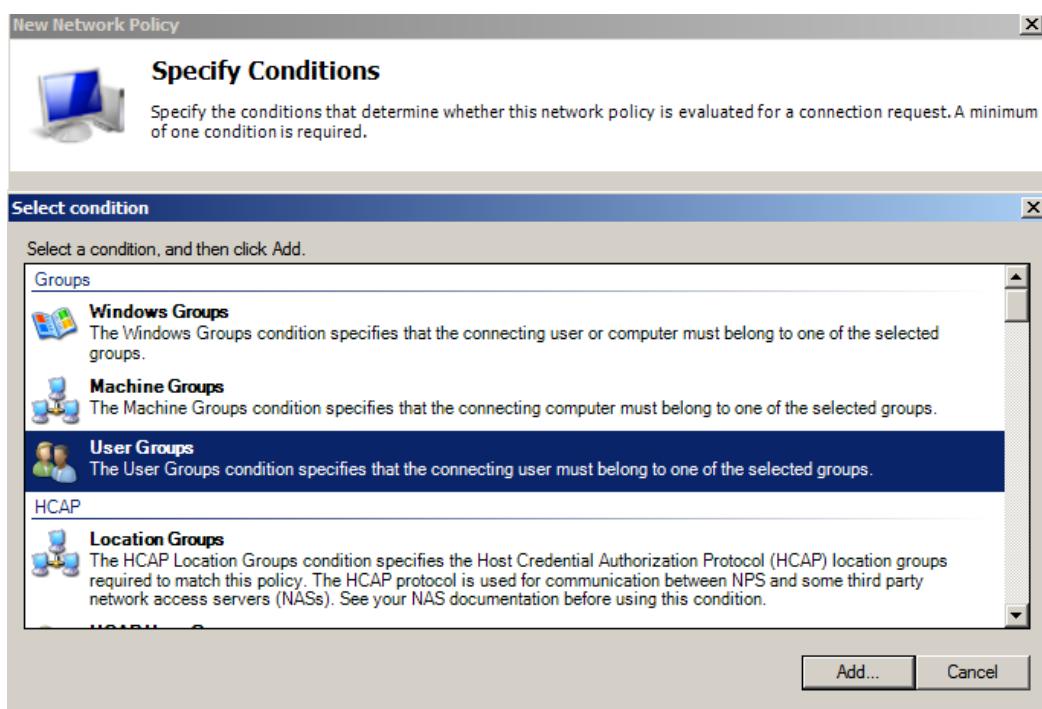


Figure 5. 112: Add User Groups

Step 18: In User Groups page, click Add Groups.

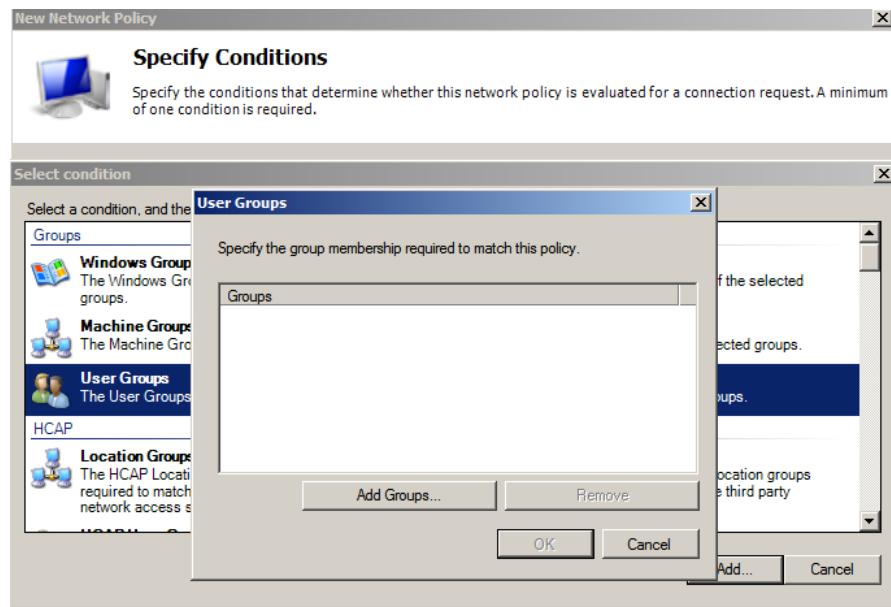


Figure 5. 113: Add Groups.

Step 19: Enter the object name to select > dom > Check Names. Then, choose Domain Users and click OK.

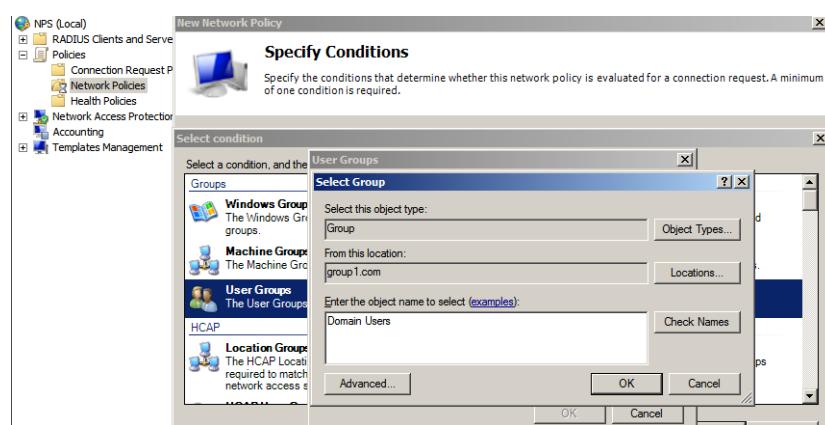


Figure 5. 114: Domain Users.

Step 20: Then, click OK.

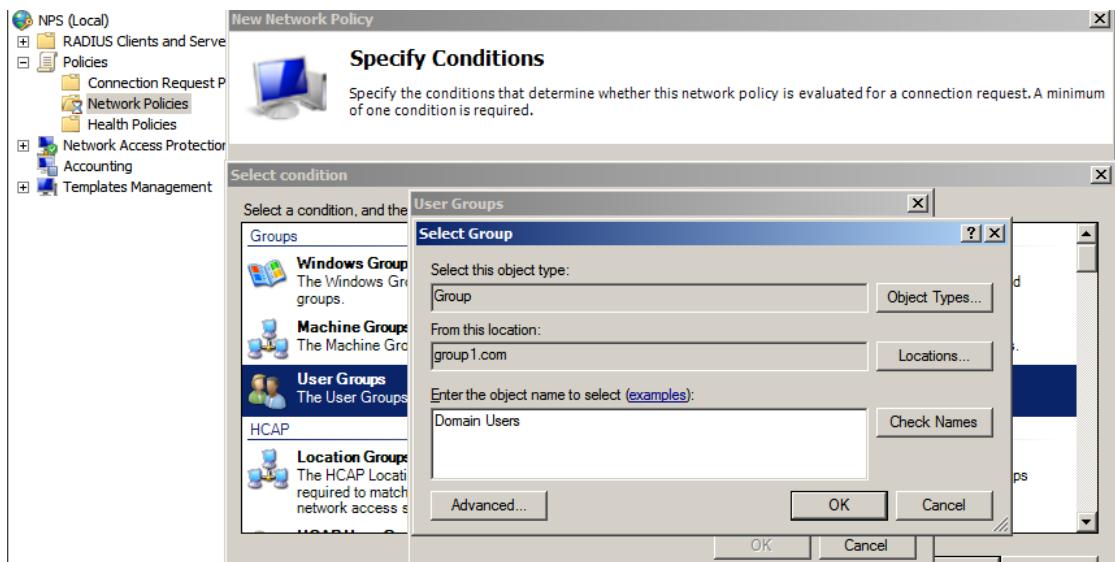


Figure 5. 115: Select Group.

Step 21: Proceed to OK.

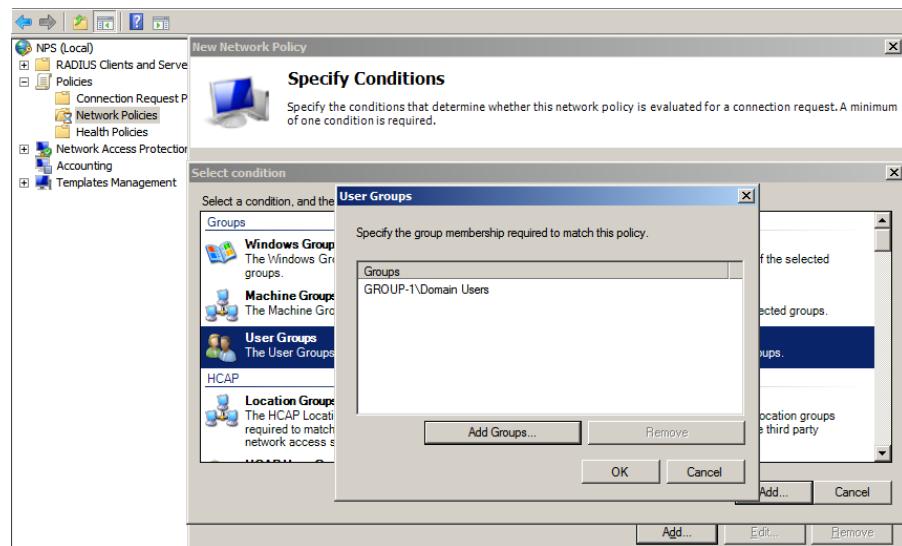


Figure 5. 116: User Groups.

Step 22: In Specify Conditions page, proceed to Next.

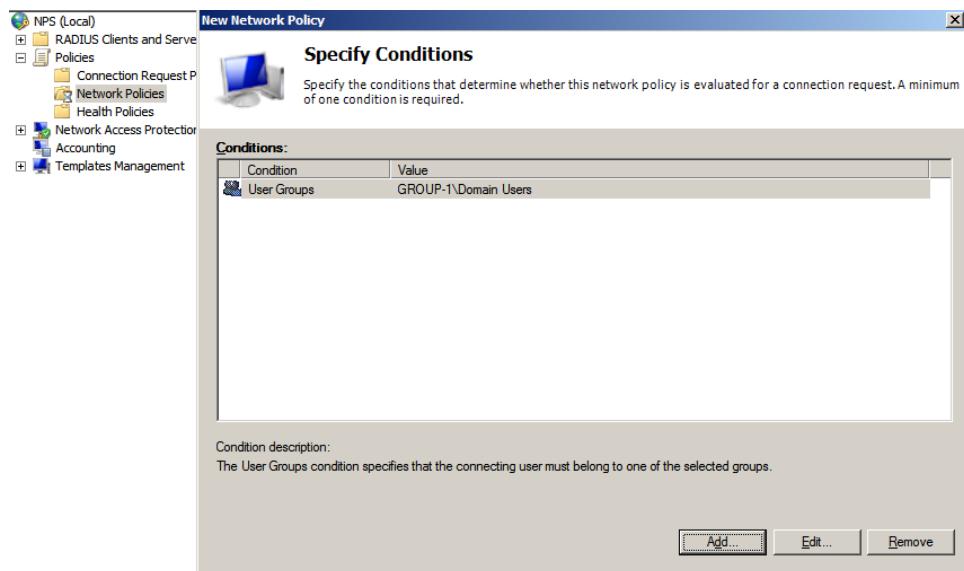


Figure 5. 117: Specify Conditions.

Step 23: In Specify Access Permission, tick Access granted. Proceed to Next.

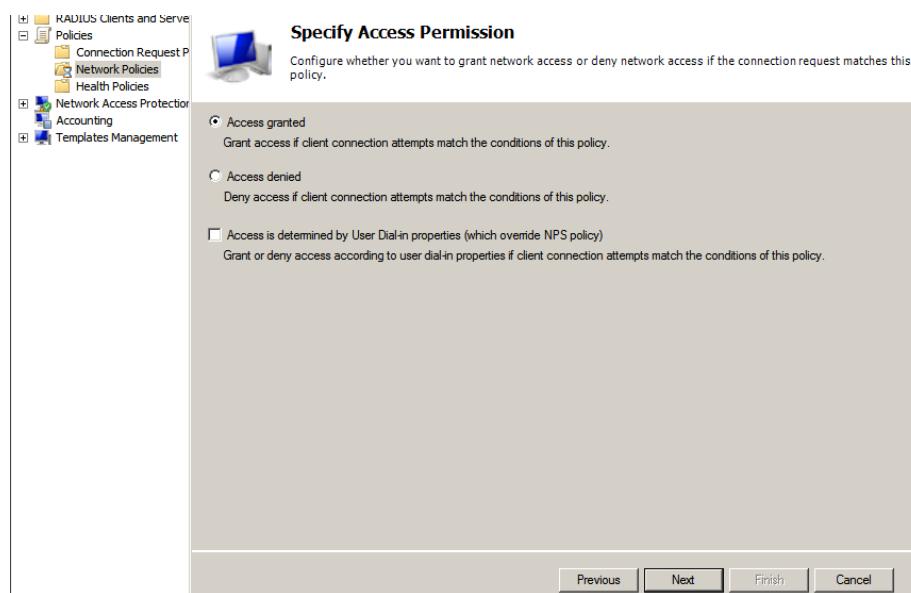


Figure 5. 118: Specify Access Permission > Access Granted.

Step 24: On Configuration Authentication Methods, tick on Unencrypted authentication (PAP, SPAP). Proceed to Next. When Connection request policy windows appear, click No.

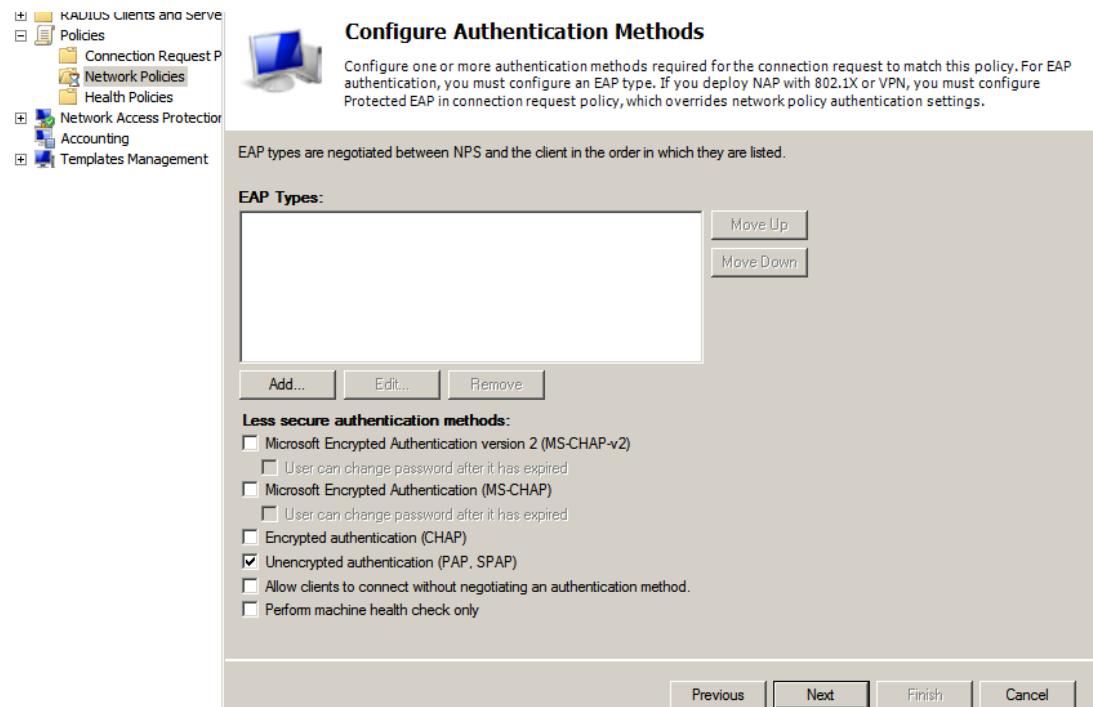


Figure 5. 119: Configure Authentication Methods

Step 25: Configure Constraints page, proceed to Next.

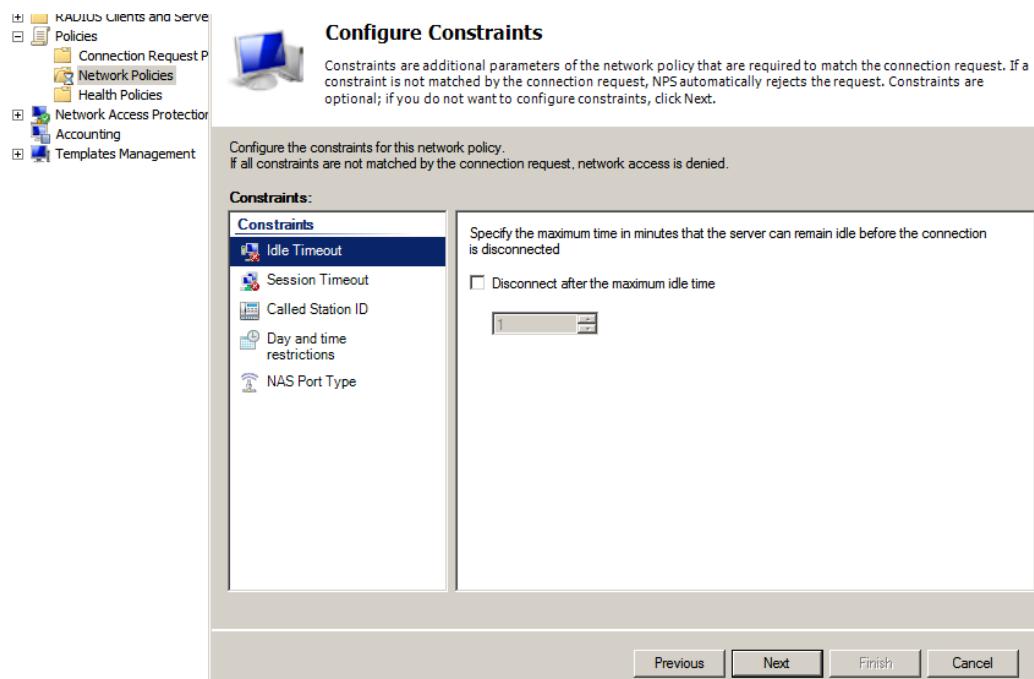


Figure 5. 120: Set Idle Timeout

Step 26: In Standard, remove Framed-Protocol and Service-Type attributes.

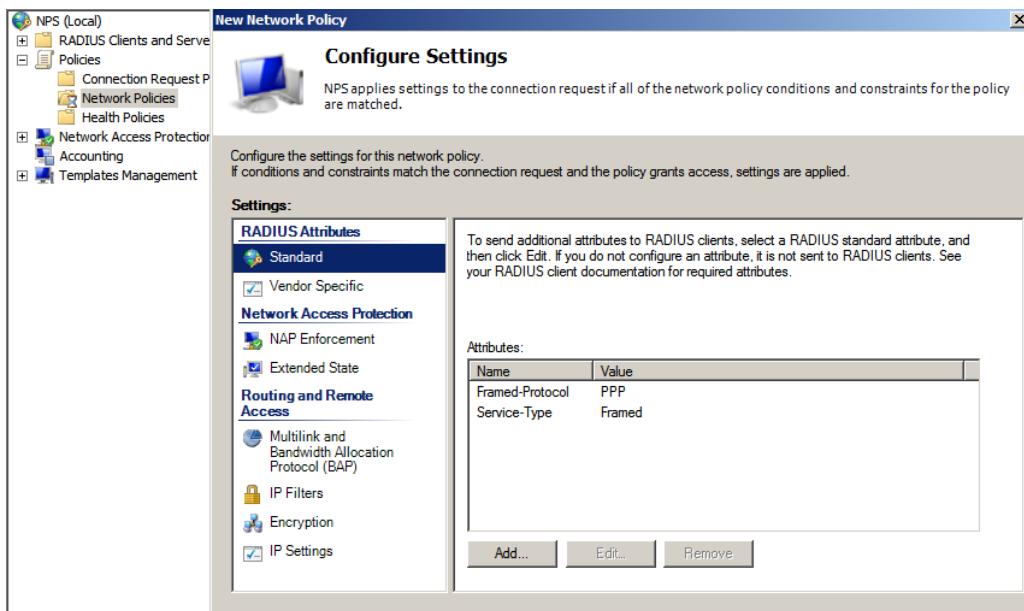


Figure 5. 121: Remove Attributes.

Step 27: Click Add to add attributes, set the name as Service-Type and value as Login.

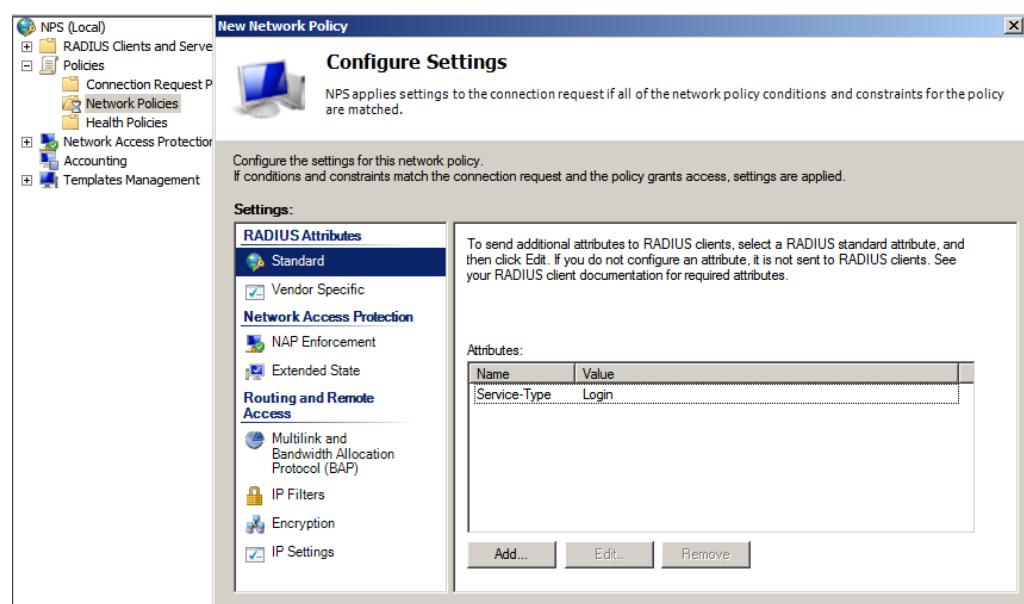


Figure 5. 122: Standard.

Step 28: In Vendor Specific, add attributes name Cisco-AV-Pair, vendor Cisco and value shell:priv-lvl=15.

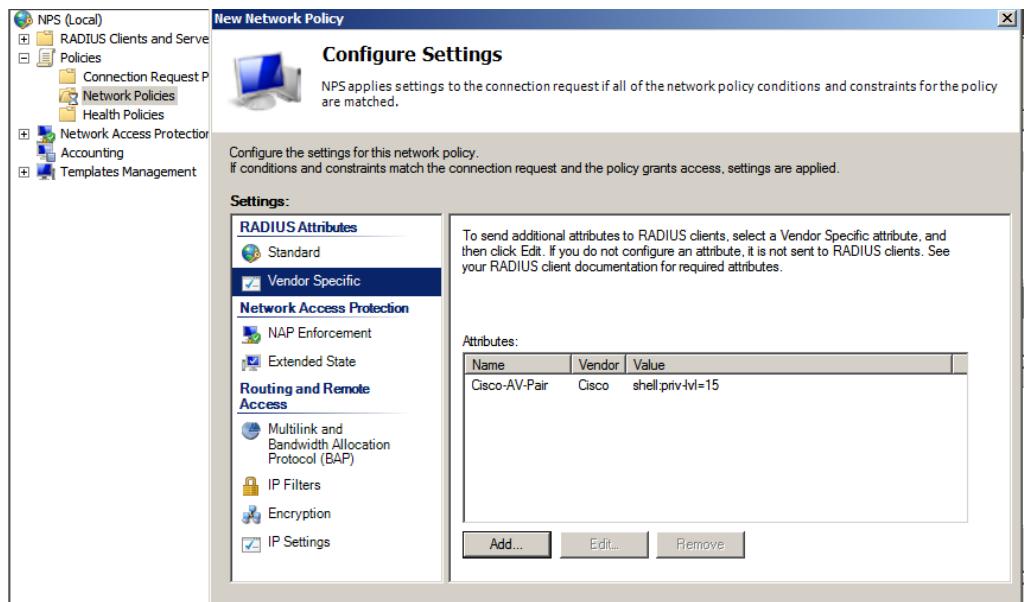


Figure 5. 123: Vendor Specific.

Step 29: In Encryption, tick on the No encryption. Then, click Next.

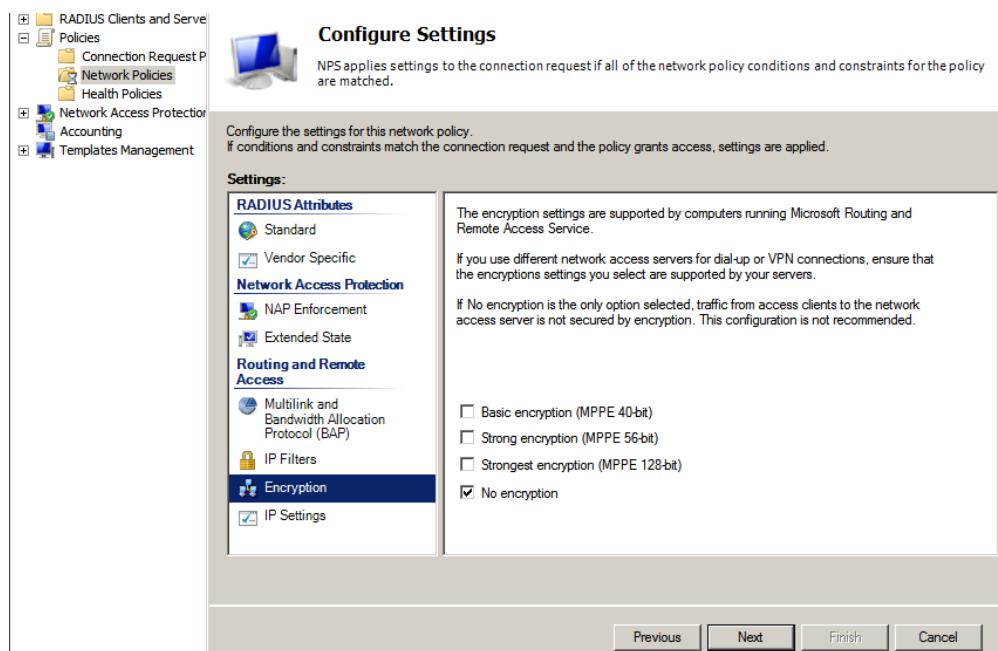


Figure 5. 124: Encryption

Step 30: On IP Settings, tick on the Server settings determines IP address assignment.

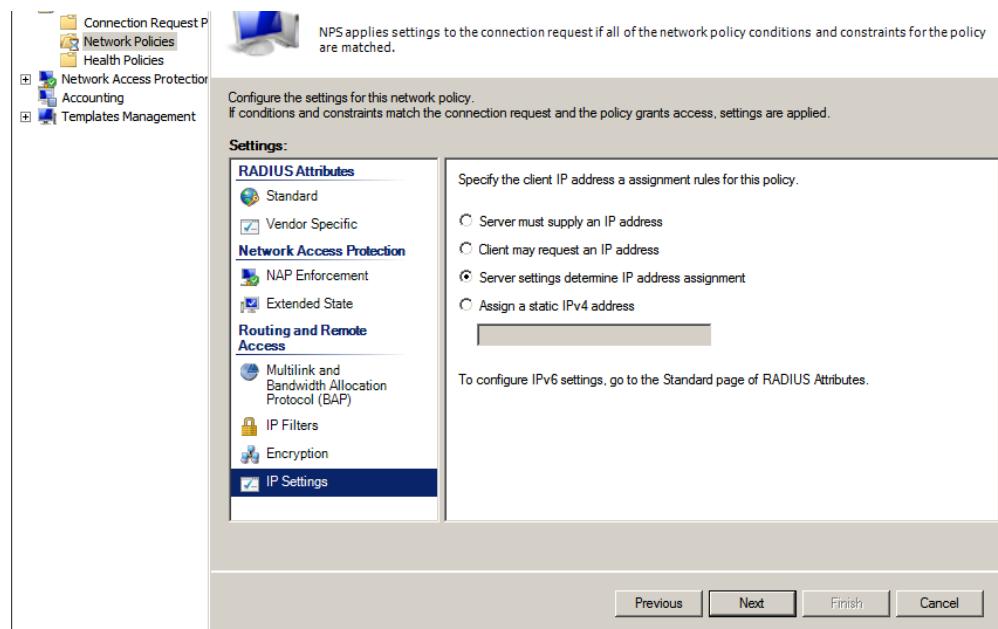


Figure 5. 125: IP Settings

Step 31: In Completing New Network Policy, it will displays that successfully created the network policy. Click Finish.

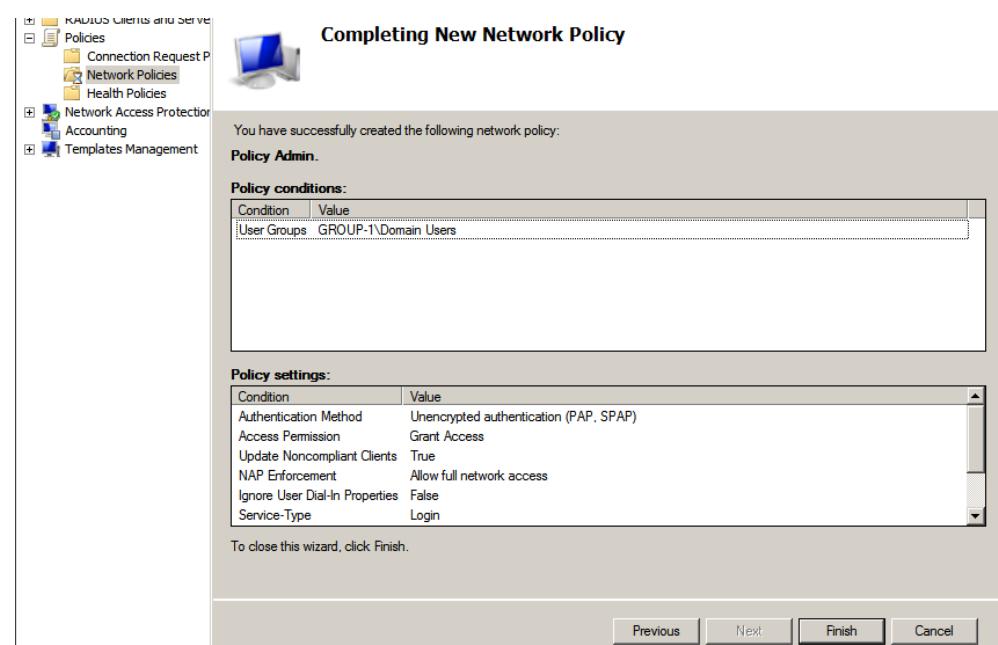


Figure 5. 126: Completing New Network Policy

Step 32: Network policy that had been created.

The screenshot shows the Windows Network Policy Service interface. On the left, a tree view shows 'NPS (Local)', 'RADIUS Clients and Servers', 'Policies' (which is expanded to show 'Connection Request Policy', 'Network Policies', and 'Health Policies'), 'Network Access Protection', 'Accounting', and 'Templates Management'. The main window is titled 'Network Policies' and contains a table of policies:

Policy Name	Status	Processing Order	Access Type	Source
Secure Wireless Connections	Enabled	1	Grant Access	Unspecified
Policy Admin	Enabled	2	Grant Access	Unspecified
Policy User	Enabled	3	Grant Access	Unspecified
Connections to Microsoft Routing and Remote Access server	Enabled	4	Deny Access	Unspecified
Connections to other access servers	Enabled	5	Deny Access	Unspecified

Below the table, there are two sections: 'Conditions - If the following conditions are met:' and 'Settings - Then the following settings are applied:'. The 'Conditions' section shows a table with one row: 'User Groups' set to 'GROUP-1\Domain Users'. The 'Settings' section shows a table with three rows:

Setting	Value
Cisco-AV-Pair	shell.priv-lvl=15
Extended State	<Blank>
Access Permission	Grant Access

Figure 5. 127: Done created

Step 33: Open putty. Select Serial and click Open.

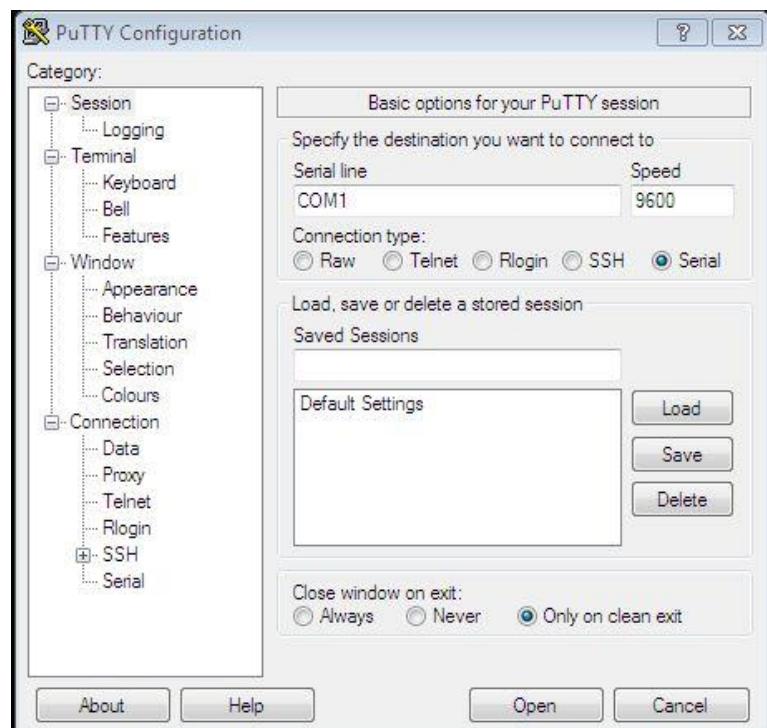
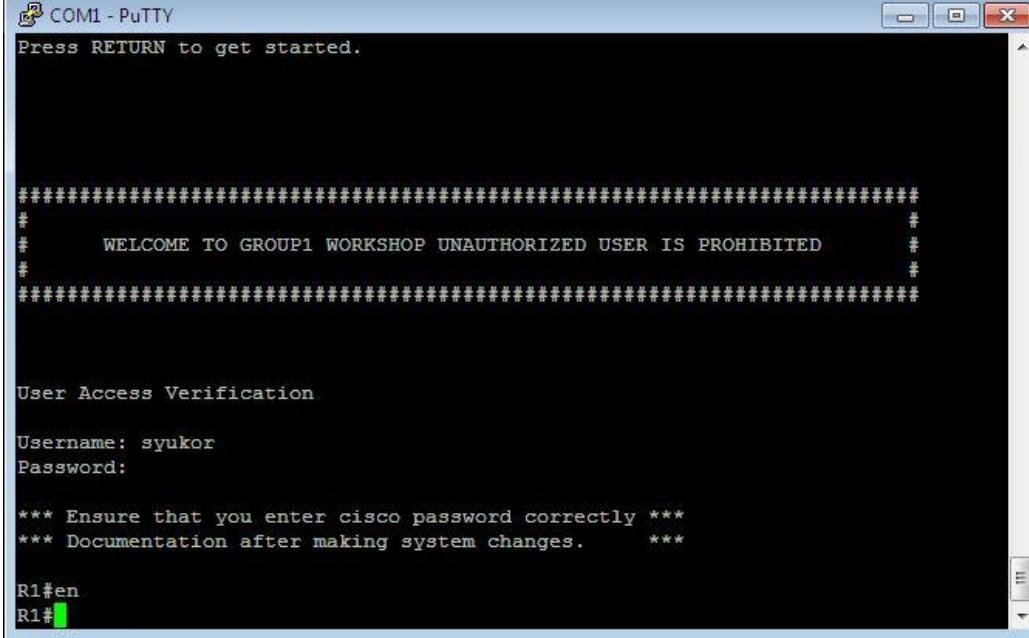


Figure 5. 128: Open Putty

Step 34: User Access Verification will display. Enter the username (Any AD users) and password. Enter enable (en).

Step 35: Enter global configuration mode using command configure terminal.



```
COM1 - PuTTY
Press RETURN to get started.

#####
#          WELCOME TO GROUP1 WORKSHOP UNAUTHORIZED USER IS PROHIBITED
#
#####

User Access Verification

Username: syukor
Password:

*** Ensure that you enter cisco password correctly ***
*** Documentation after making system changes.      ***

R1#en
R1#
```

Figure 5. 129: Login

Step 36: Setup AAA global configuration in the putty terminal

```

R1(config)#aaa new-model
R1(config)#aaa group server radius RADIUS-G1
R1(config-sg-radius)#$8.11.33 auth-port 1812 acct-port 1813 key RADIUS-G1
Translating "private"...domain server (255.255.255.255)

server private 192.168.11.33 auth-port 1812 acct-port 1813 key RADIUS-G1
^
* Invalid input detected at '^' marker.

R1(config-sg-radius)#$8.11.33 auth-port 1812 acct-port 1813 key Abc12345
R1(config-sg-radius)#aaa authentication login default group RADIUS-G1 local
R1(config)#$zation exec default group RADIUS-G1 local if-authenticated
R1(config)#aaa authorization console
R1(config)#exit
R1#
*Nov 17 04:04:41.235: %SYS-5-CONFIG_I: Configured from console by group1 on cons
ole
R1#copy run start
Destination filename [startup-config]?
Building configuration...

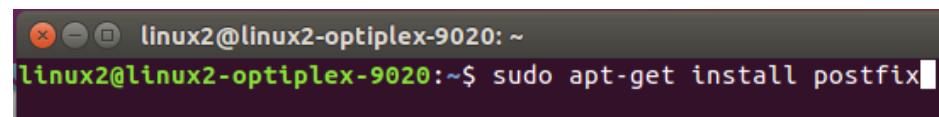
[OK]
R1#

```

Figure 5. 130: Configuration of AAA model

### 5.3.12 LINUX EMAIL SERVER

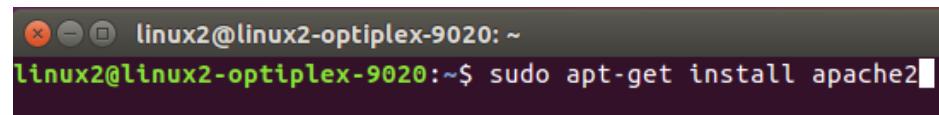
Step1: Enter terminal and install postfix services in Ubuntu 16.04 for Mail Transfer Agent(MTA)



A screenshot of a terminal window titled 'linux2@linux2-optiplex-9020: ~'. The window shows the command 'sudo apt-get install postfix' being typed into the terminal.

Figure 5. 131: Command to install postfix

Step2: Install apache 2 services



A screenshot of a terminal window titled 'linux2@linux2-optiplex-9020: ~'. The window shows the command 'sudo apt-get install apache2' being typed into the terminal.

Figure 5. 132: Command to install apache2

Step3: Type your IP address in web browser to see check apache2 correctly installed or not.

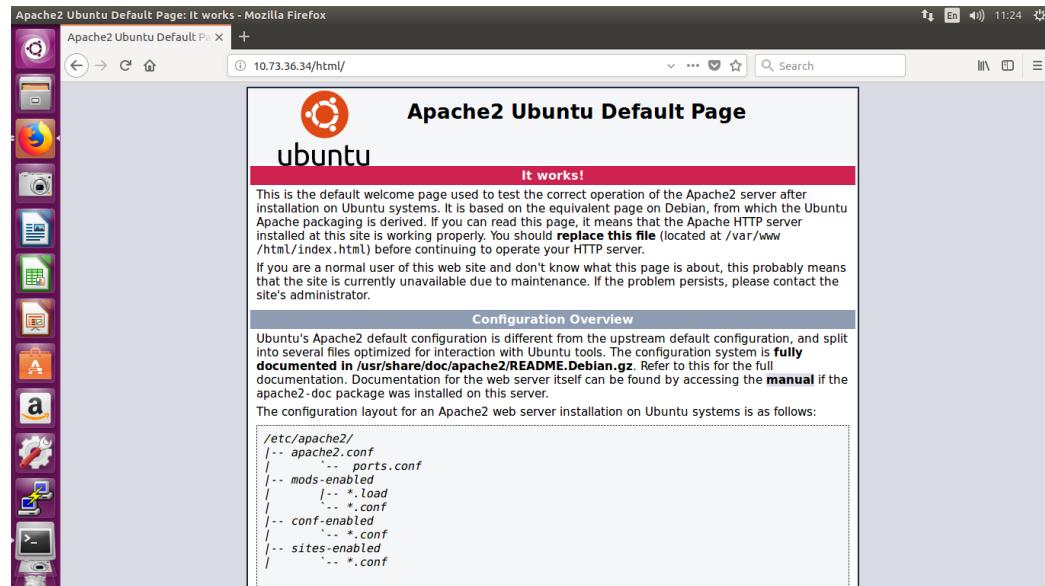


Figure 5. 133: Apache 2 web page

Step4: Enter “sudo vim /etc/postfix/main.cf” to enter postfix configuration then at “inet\_protocols” change to “= ipv4” and type “home\_mailbox = Maildir/”.

```

x - linux2@linux2-optiplex-9020: ~
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = linux2-OptiPlex-9020.lan
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname,group1.com, linux2-OptiPlex-9020, localhost.localdomain, localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 10240000
recipient_delimiter =
inet_interfaces = all
inet_protocols = ipv4
home_mailbox = Maildir/

```

Figure 5. 134: Postfix configuration

Step5: Install Dovecot service for Mail Delivery Agent(MDA)

```
sudo apt-get install dovecot-imapd
```

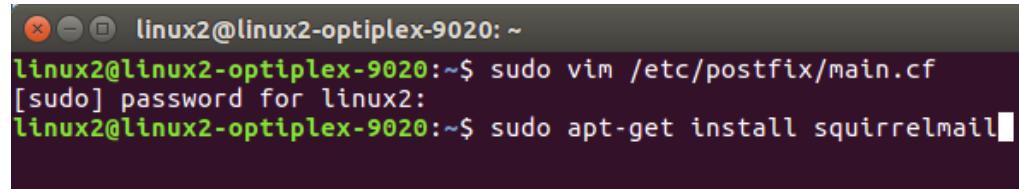
Step6: Configure Dovecot

```
sudo vim /etc/dovecot.dovecot.conf
```

Add Below command:

- protocols = imap pop3
- #disable\_plaintext\_auth = no
- mail\_location = mbox:~/mail:INBOX=/var/mail/%
- mail\_location = maildir:~/Maildir

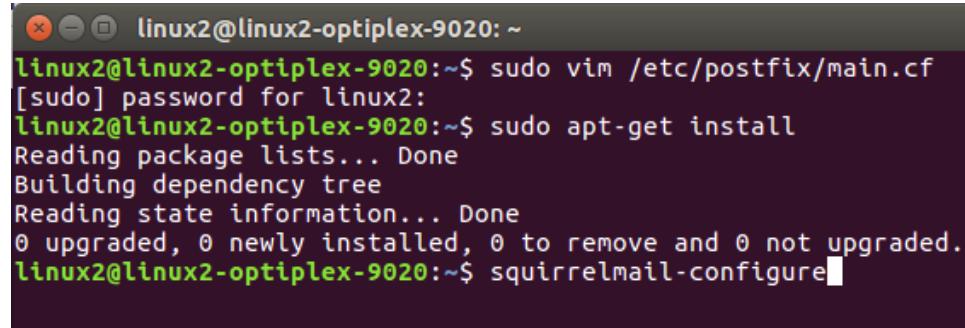
Step7: Install squirrelmail services for Mail User Agent(MUA)



```
linux2@linux2-optiplex-9020: ~
linux2@linux2-optiplex-9020:~$ sudo vim /etc/postfix/main.cf
[sudo] password for linux2:
linux2@linux2-optiplex-9020:~$ sudo apt-get install squirrelmail
```

Figure 5. 135: Command to install squirrelmail

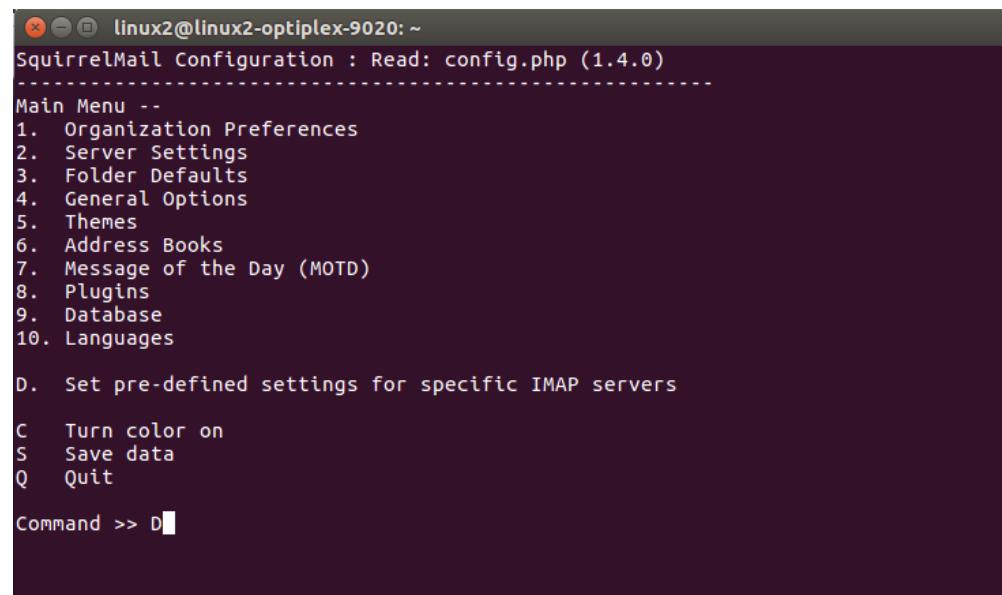
Step8: Enter command “squirrelmail-configure” to edit configuration file



```
linux2@linux2-optiplex-9020:~$ sudo vim /etc/postfix/main.cf
[sudo] password for linux2:
linux2@linux2-optiplex-9020:~$ sudo apt-get install
Reading package lists... Done
Building dependency tree
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
linux2@linux2-optiplex-9020:~$ squirrelmail-configure
```

Figure 5. 136: Edit configuration file

Step9: Type “D” to set IMAP servers



```
linux2@linux2-optiplex-9020:~$ SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Main Menu --
1. Organization Preferences
2. Server Settings
3. Folder Defaults
4. General Options
5. Themes
6. Address Books
7. Message of the Day (MOTD)
8. Plugins
9. Database
10. Languages

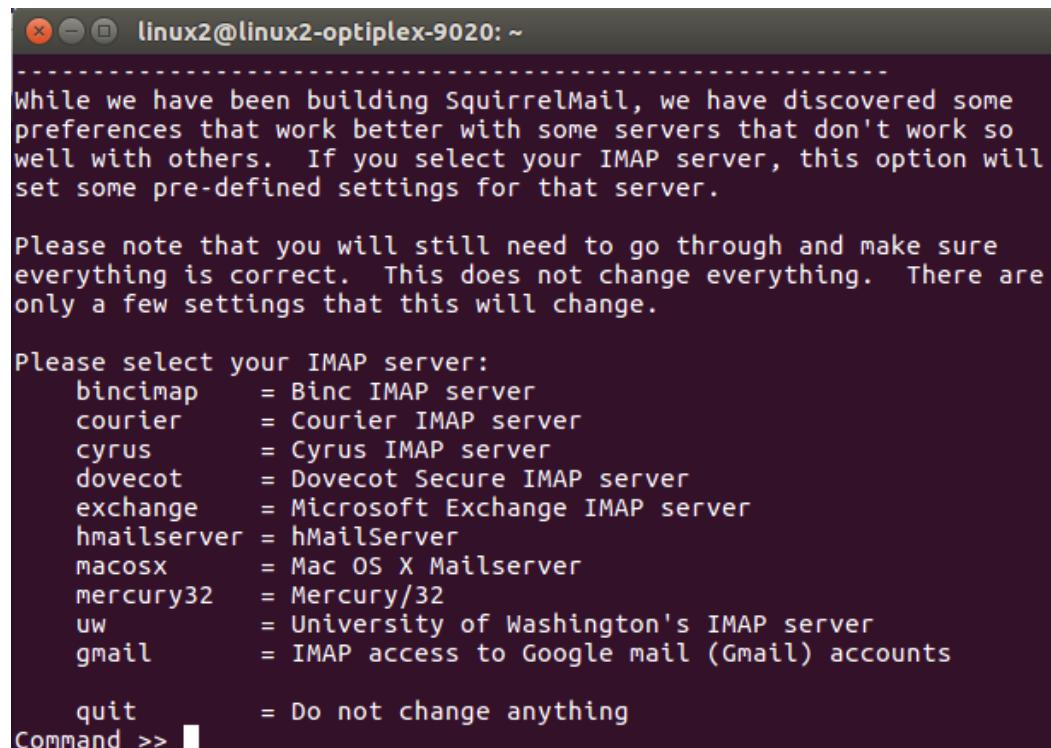
D. Set pre-defined settings for specific IMAP servers

C Turn color on
S Save data
Q Quit

Command >> D
```

Figure 5. 137: Edit IMAP servers

Step10: Type “dovecot” for IMAP server



```
linux2@linux2-optiplex-9020: ~
-----
While we have been building SquirrelMail, we have discovered some
preferences that work better with some servers that don't work so
well with others. If you select your IMAP server, this option will
set some pre-defined settings for that server.

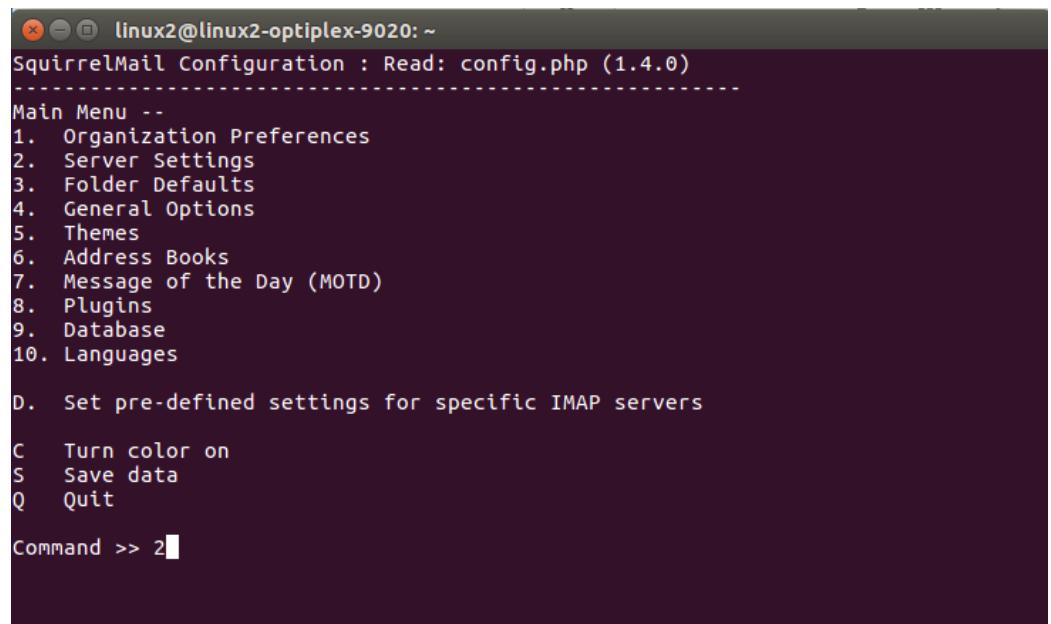
Please note that you will still need to go through and make sure
everything is correct. This does not change everything. There are
only a few settings that this will change.

Please select your IMAP server:
  bincimap      = Binc IMAP server
  courier       = Courier IMAP server
  cyrus         = Cyrus IMAP server
  dovecot       = Dovecot Secure IMAP server
  exchange      = Microsoft Exchange IMAP server
  hmailserver   = hMailServer
  macosx        = Mac OS X Mailserver
  mercury32     = Mercury/32
  uw            = University of Washington's IMAP server
  gmail          = IMAP access to Google mail (Gmail) accounts

  quit          = Do not change anything
Command >> 2
```

Figure 5. 138: Select IMAP servers

Step11: Type “2” to edit Server settings



```
linux2@linux2-optiplex-9020: ~
SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Main Menu --
1. Organization Preferences
2. Server Settings
3. Folder Defaults
4. General Options
5. Themes
6. Address Books
7. Message of the Day (MOTD)
8. Plugins
9. Database
10. Languages

D. Set pre-defined settings for specific IMAP servers

C Turn color on
S Save data
Q Quit

Command >> 2
```

Figure 5. 139: Edit Server Settings

Step12: In server settings, type “1” to change domain to group1.com

```

linux2@linux2-optiplex-9020: ~
SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Server Settings
General
-----
1. Domain : group1.com
2. Invert Time : false
3. Sendmail or SMTP : SMTP
A. Update IMAP Settings : localhost:143 (dovecot)
B. Update SMTP Settings : localhost:25
R  Return to Main Menu
C  Turn color on
S  Save data
Q  Quit
Command >> 1

```

Figure 5. 140: Select domain name

Step13: Change directory to /var/www then type below command

```

linux2@linux2-optiplex-9020: /var/www
linx2@linx2-optiplex-9020:~$ cd /var/www
linx2@linx2-optiplex-9020:/var/www$ ln -s /usr/share/squirrelmail webmail

```

Figure 5. 141: /var/www directory

Step14: Change directory to /etc/apache2/sites-available then enter command

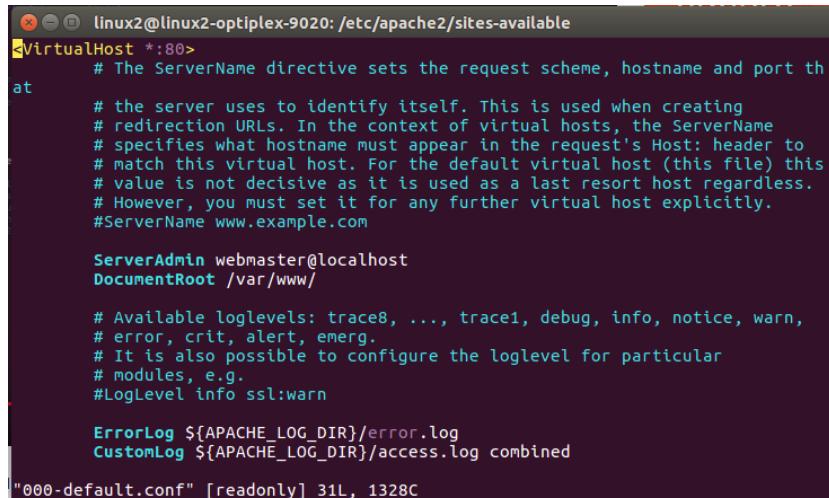
below to edit apache 2 configuration file

```

linux2@linux2-optiplex-9020: /etc/apache2/sites-available
linx2@linx2-optiplex-9020:~$ cd /var/www
linx2@linx2-optiplex-9020:/var/www$ cd ..
linx2@linx2-optiplex-9020:/var$ cd ..
linx2@linx2-optiplex-9020:/$ cd /etc/apache2/sites-available
linx2@linx2-optiplex-9020:/etc/apache2/sites-available$ vim 000-default.conf

```

Figure 5. 142: Edit configuration file



```

linux2@linux2-optiplex-9020: /etc/apache2/sites-available
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port th
at
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

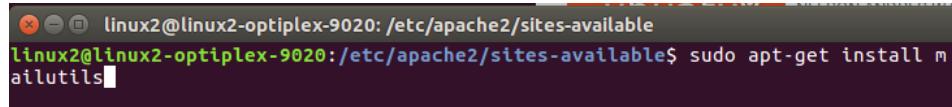
"000-default.conf" [readonly] 31L, 1328C

```

Figure 5. 143: edit /etc/apache2/sites-available

Step15: At DocumentRoot, change to /var/www/

Step16: Install Mailutils services



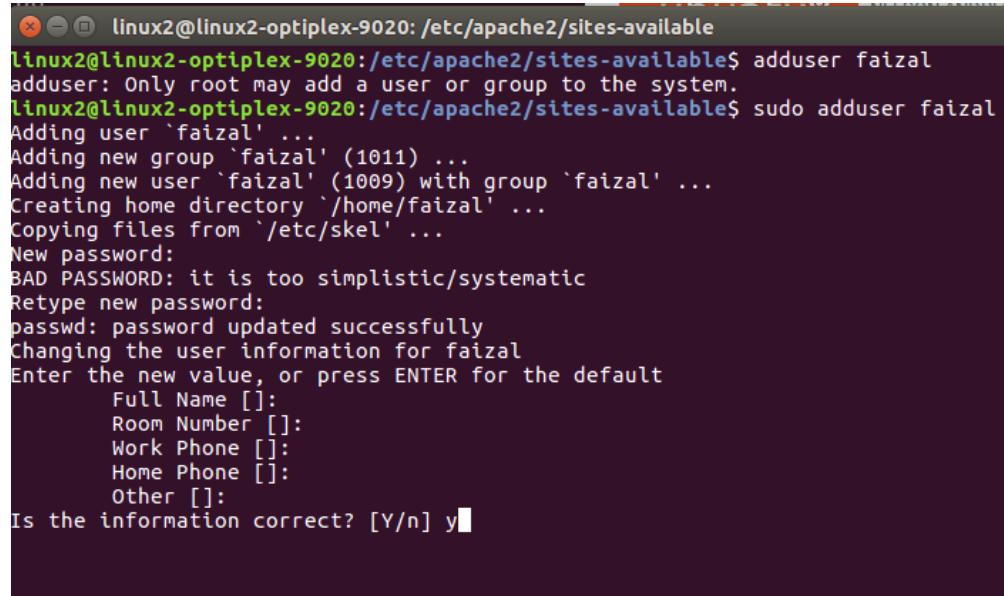
```

linux2@linux2-optiplex-9020: /etc/apache2/sites-available
linux2@linux2-optiplex-9020:/etc/apache2/sites-available$ sudo apt-get install m
ailutils

```

Figure 5. 144: Command to install Mailutils

Step17: Enter command below to add user for mail server



```

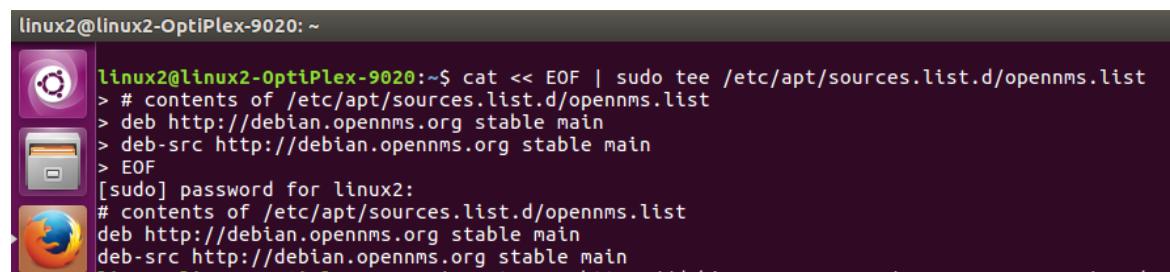
linux2@linux2-optiplex-9020: /etc/apache2/sites-available
linux2@linux2-optiplex-9020:/etc/apache2/sites-available$ adduser faizal
adduser: Only root may add a user or group to the system.
linux2@linux2-optiplex-9020:/etc/apache2/sites-available$ sudo adduser faizal
Adding user `faizal' ...
Adding new group `faizal' (1011) ...
Adding new user `faizal' (1009) with group `faizal' ...
Creating home directory `/home/faizal' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: it is too simplistic/systematic
Retype new password:
passwd: password updated successfully
Changing the user information for faizal
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y

```

Figure 5. 145: Add user for mail server

### 5.3.13 NETWORK MANAGEMENT SYSTEM

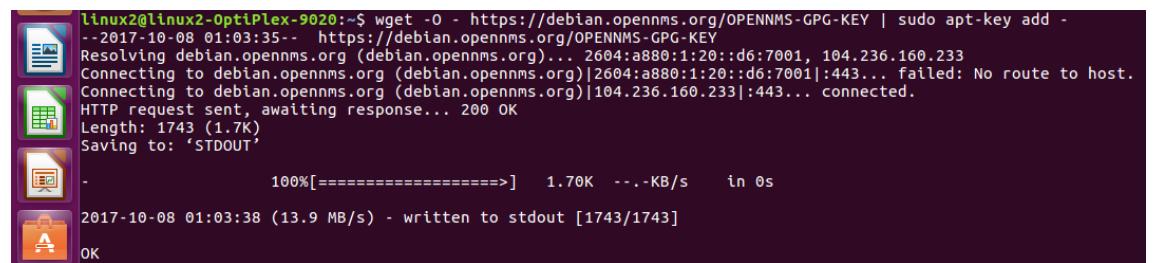
Step 1: To set up APT to talk to the OpenNMS repository, the following commands are applied.



```
linux2@linux2-OptiPlex-9020: ~
linux2@linux2-OptiPlex-9020:~$ cat << EOF | sudo tee /etc/apt/sources.list.d/opennms.list
> # contents of /etc/apt/sources.list.d/opennms.list
> deb http://debian.opennms.org stable main
> deb-src http://debian.opennms.org stable main
> EOF
[sudo] password for linux2:
# contents of /etc/apt/sources.list.d/opennms.list
deb http://debian.opennms.org stable main
deb-src http://debian.opennms.org stable main
```

Figure 5. 146: Set up APT to talk to the OpenNMS repository

Step 2: To install the OpenNMS GPG key into your system, type the following at a command prompt.



```
linux2@linux2-OptiPlex-9020:~$ wget -O - https://debian.opennms.org/OPENNMS-GPG-KEY | sudo apt-key add -
--2017-10-08 01:03:35-- https://debian.opennms.org/OPENNMS-GPG-KEY
Resolving debian.opennms.org (debian.opennms.org)... 2604:a880:1:20::d6:7001, 104.236.160.233
Connecting to debian.opennms.org (debian.opennms.org)|2604:a880:1:20::d6:7001|:443... failed: No route to host.
Connecting to debian.opennms.org (debian.opennms.org)|104.236.160.233|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1743 (1.7K)
Saving to: 'STDOUT'

[  0% [=====]  1.70K  ---KB/s   in 0s
2017-10-08 01:03:38 (13.9 MB/s) - written to stdout [1743/1743]
```

Figure 5. 147: Install OpenNMS

Step 3: Run sudo apt-get update to get the latest list of packages in APT repositories, including those in the OpenNMS repository.

```
linux2@linux2-OptiPlex-9020:~$ sudo apt-get update
Ign:1 http://debian.opennms.org stable InRelease
Get:2 http://debian.opennms.org stable Release [7,187 B]
Get:3 http://debian.opennms.org stable Release.gpg [181 B]
Get:4 http://debian.opennms.org stable/main Sources [5,694 B]
Get:5 http://debian.opennms.org stable/main amd64 Packages [40.7 kB]
Get:6 http://debian.opennms.org stable/main i386 Packages [45.2 kB]
Hit:7 http://my.archive.ubuntu.com/ubuntu xenial InRelease
Get:8 http://my.archive.ubuntu.com/ubuntu xenial-updates InRelease [102 kB]
Get:9 http://my.archive.ubuntu.com/ubuntu xenial-backports InRelease [102 kB]
Get:10 http://my.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [636 kB]
Get:11 http://my.archive.ubuntu.com/ubuntu xenial-updates/main i386 Packages [606 kB]
Get:12 http://my.archive.ubuntu.com/ubuntu xenial-updates/main amd64 DEP-11 Metadata [305 kB]
Get:13 http://my.archive.ubuntu.com/ubuntu xenial-updates/main DEP-11 64x64 Icons [213 kB]
Get:14 http://my.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 Packages [538 kB]
Get:15 http://my.archive.ubuntu.com/ubuntu xenial-updates/universe i386 Packages [515 kB]
Get:16 http://my.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 DEP-11 Metadata [172 kB]
Get:17 http://my.archive.ubuntu.com/ubuntu xenial-updates/universe DEP-11 64x64 Icons [234 kB]
Get:18 http://my.archive.ubuntu.com/ubuntu xenial-updates/multiverse amd64 DEP-11 Metadata [5,888 B]
```

Figure 5. 148: Update to get the latest packages

Step 4: After configured APT for the release of your choice, a query of the APT database should show a number of OpenNMS packages as available install options when you run “apt-cache show opennms”.

Figure 5. 149: Show a number of OpenNMS packages

Step 5: Before installing OpenNMS, you need to install PostgreSQL and make sure PostgreSQL is working properly.



```
linux2@linux2-OptiPlex-9020:~$ sudo apt-get install postgresql
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libpq5 postgresql-9.5 postgresql-client-9.5 postgresql-client-common
  postgresql-common postgresql-contrib-9.5 sysstat
Suggested packages:
  postgresql-doc locales-all postgresql-doc-9.5 libdbd-pg-perl isag
The following NEW packages will be installed:
  libpq5 postgresql postgresql-9.5 postgresql-client-9.5
  postgresql-client-common postgresql-common postgresql-contrib-9.5 sysstat
0 upgraded, 8 newly installed, 0 to remove and 20 not upgraded.
Need to get 4,801 kB of archives.
After this operation, 19.4 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://my.archive.ubuntu.com/ubuntu xenial-updates/main amd64 libpq5 amd64 9.5.9-0ubuntu0.16.04 [78.8 kB]
Get:2 http://my.archive.ubuntu.com/ubuntu xenial/main amd64 postgresql-client-common all 173 [28.3 kB]
```

Figure 5. 150: Install PostgreSQL

Step 6: To see the version of PostgreSQL installed, put this command.



```
linux2@linux2-OptiPlex-9020:~$ PGVERSION='pg_lsclusters -h | head -n 1 | cut -d' ' -f1'
linux2@linux2-OptiPlex-9020:~$ echo $PGVERSION
```

Figure 5. 151: Check PostgreSQL version

Step 7: To allow connections as the PostgreSQL user to authenticate without a password, you must change the option first in the pg\_hba.conf file.

```
linux2@linux2-OptiPlex-9020:~$ sudo vi /etc/postgresql/9.5/main/pg_hba.conf
```

Figure 5. 152: Change option

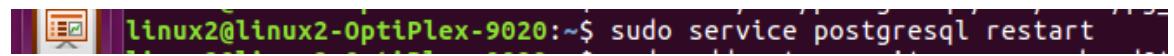
Step 8: Change these entries to replace the default authentication methods with the method “trust”.



```
# Database administrative login by Unix domain socket
local  all      postgres                                peer
# TYPE  DATABASE        USER        ADDRESS            METHOD
# "local" is for Unix domain socket connections only
local  all      all                                     trust # the default method is peer
# IPv4 local connections:
host   all      all          127.0.0.1/32         trust # the default method is md5
# IPv6 local connections:
host   all      all          ::1/128              trust # the default method is md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
#local  replication  postgres                                peer
#host   replication  postgres      127.0.0.1/32         md5
#host   replication  postgres      ::1/128              md5
```

Figure 5. 153: Change entries

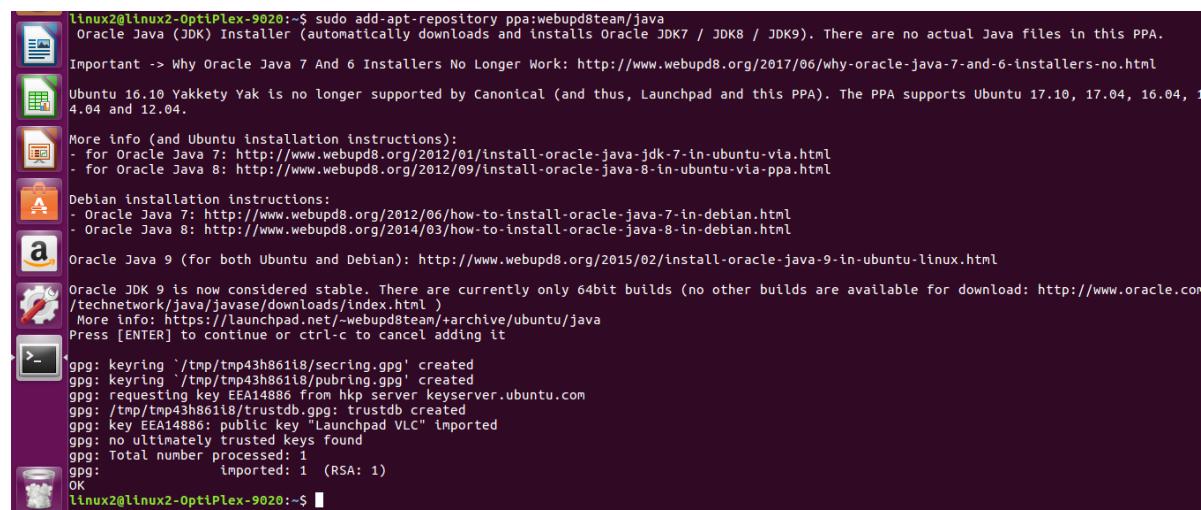
Step 9: After finish making changes, restart the database (as root).



```
linux2@linux2-OptiPlex-9020:~$ sudo service postgresql restart
```

Figure 5. 154: Restart database

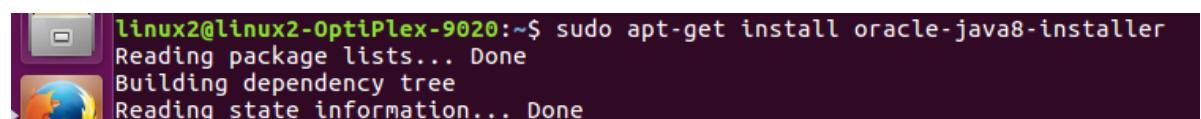
Step 10: To install Java, first we need to add the private package archive webupd8team/java.



```
linux2@linux2-OptiPlex-9020:~$ sudo add-apt-repository ppa:webupd8team/java
Oracle Java (JDK) Installer (automatically downloads and installs Oracle JDK7 / JDK8 / JDK9). There are no actual Java files in this PPA.
Important -> Why Oracle Java 7 And 6 Installers No Longer Work: http://www.webupd8.org/2017/06/why-oracle-java-7-and-6-installers-no.html
Ubuntu 16.10 Yakkety Yak is no longer supported by Canonical (and thus, Launchpad and this PPA). The PPA supports Ubuntu 17.10, 17.04, 16.04, 14.04 and 12.04.
More info (and Ubuntu installation instructions):
- for Oracle Java 7: http://www.webupd8.org/2012/01/install-oracle-java-jdk-7-in-ubuntu-via.html
- for Oracle Java 8: http://www.webupd8.org/2012/09/install-oracle-java-8-in-ubuntu-via-ppa.html
Debian installation instructions:
- Oracle Java 7: http://www.webupd8.org/2012/06/how-to-install-oracle-java-7-in-debian.html
- Oracle Java 8: http://www.webupd8.org/2014/03/how-to-install-oracle-java-8-in-debian.html
Oracle Java 9 (for both Ubuntu and Debian): http://www.webupd8.org/2015/02/install-oracle-java-9-in-ubuntu-linux.html
Oracle JDK 9 is now considered stable. There are currently only 64bit builds (no other builds are available for download: http://www.oracle.com/technetwork/java/javase/downloads/index.html )
More info: https://launchpad.net/~webupd8team/+archive/ubuntu/java
Press [ENTER] to continue or ctrl-c to cancel adding it
gpg: keyring '/tmp/tmp43h88i18/secring.gpg' created
gpg: keyring '/tmp/tmp43h88i18/pubring.gpg' created
gpg: requesting key EEA14886 from hkp server keyserver.ubuntu.com
gpg: /tmp/tmp43h88i18/trustdb.gpg: trustdb created
gpg: key EEA14886: public key "Launchpad VLC" imported
gpg: no ultimately trusted keys found
gpg: Total number processed: 1
gpg:           imported: 1  (RSA: 1)
OK
linux2@linux2-OptiPlex-9020:~$
```

Figure 5. 155: Add private packages

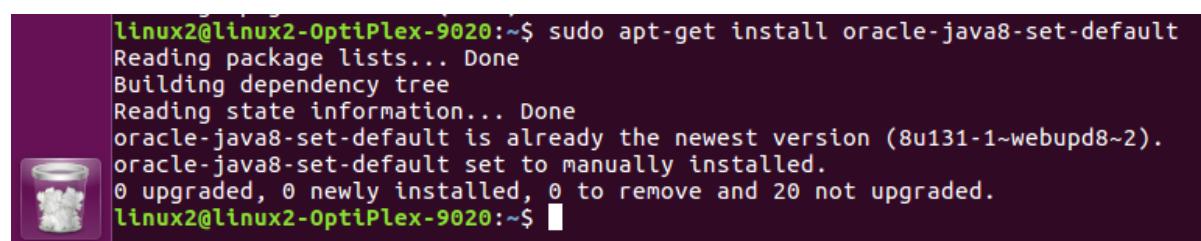
Step 11: Install Oracle Java8.



```
linux2@linux2-OptiPlex-9020:~$ sudo apt-get install oracle-java8-installer
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Figure 5. 156: Install Oracle Java8

Step 12: Setup Oracle Java8 to be the default Java VM.



```
linux2@linux2-OptiPlex-9020:~$ sudo apt-get install oracle-java8-set-default
Reading package lists... Done
Building dependency tree
Reading state information... Done
oracle-java8-set-default is already the newest version (8u131-1~webupd8~2).
oracle-java8-set-default set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 20 not upgraded.
linux2@linux2-OptiPlex-9020:~$
```

Figure 5. 157: Set up Oracle Java8 to be default

Step 13: To verify Java version.



```
linux2@linux2-OptiPlex-9020:~$ sudo apt-get install oracle-java8-set-default
Reading package lists... Done
Building dependency tree
Reading state information... Done
oracle-java8-set-default is already the newest version (8u131-1~webupd8~2).
oracle-java8-set-default set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 20 not upgraded.
```

Figure 5. 158: Verify Java version

Step 14: To install OpenNMS.



```
linux2@linux2-OptiPlex-9020:~$ sudo apt-get install opennms
Reading package lists... Done
```

Figure 5. 159: Install OpenNMS

Step 15: To tell OpenNMS which Java to use, first we need to have OpenNMS

search for and auto-detect the JRE.



```
linux2@linux2-OptiPlex-9020:~$ sudo /usr/share/opennms/bin/runjava -S
runjava: Looking for an appropriate JRE...
runjava: Checking for an appropriate JRE in JAVA_HOME...
runjava: skipping... JAVA_HOME not set
runjava: Checking JRE in user's path: "/usr/bin/java"...
runjava: found an appropriate JRE in user's path: "/usr/bin/java"
runjava: value of "/usr/bin/java" stored in configuration file
linux2@linux2-OptiPlex-9020:~$
```

Figure 5. 160: Auto-detect JRE

Step 16: To configure OpenNMS to use a specific JRE binary, use the ‘-S’ with

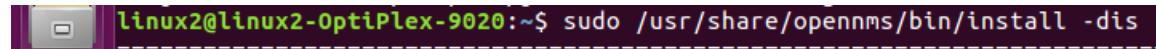
the path to the desired binary.



```
linux2@linux2-OptiPlex-9020:~$ sudo /usr/share/opennms/bin/runjava -S /usr/bin/java
runjava: checking specified JRE: "/usr/bin/java"...
runjava: specified JRE is good.
runjava: value of "/usr/bin/java" stored in configuration file
linux2@linux2-OptiPlex-9020:~$
```

Figure 5. 161: To configure to use specific JRE binary

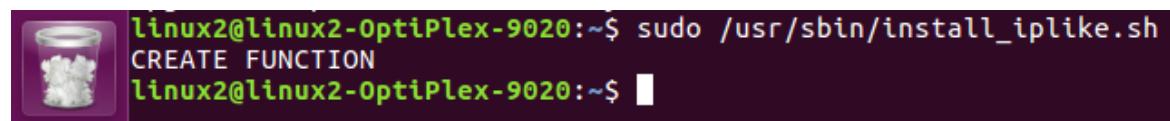
Step 17: To create and configure the OpenNMS database.



```
linux2@linux2-OptiPlex-9020:~$ sudo /usr/share/opennms/bin/install -dis
```

Figure 5. 162: Create and configure OpenNMS database

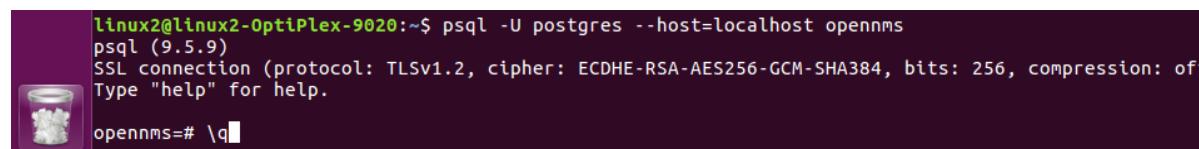
Step 18: To install IPLIKE database stored procedure



```
linux2@linux2-OptiPlex-9020:~$ sudo /usr/sbin/install_iplike.sh
CREATE FUNCTION
linux2@linux2-OptiPlex-9020:~$
```

Figure 5. 163: Install IPLIKE

Step 19: To verify connectivity to the OpenNMS database



```
linux2@linux2-OptiPlex-9020:~$ psql -U postgres --host=localhost opennms
psql (9.5.9)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
Type "help" for help.

opennms=# \q
```

Figure 5. 164: Verify connectivity

Step 20: Enter command sudo service opennms start to start OpenNMS.

Step 21: Go to “<http://192.168.11.51:8980/opennms/>” in browser and we will see the OpenNMS web UI. The default username and password are both “admin”.

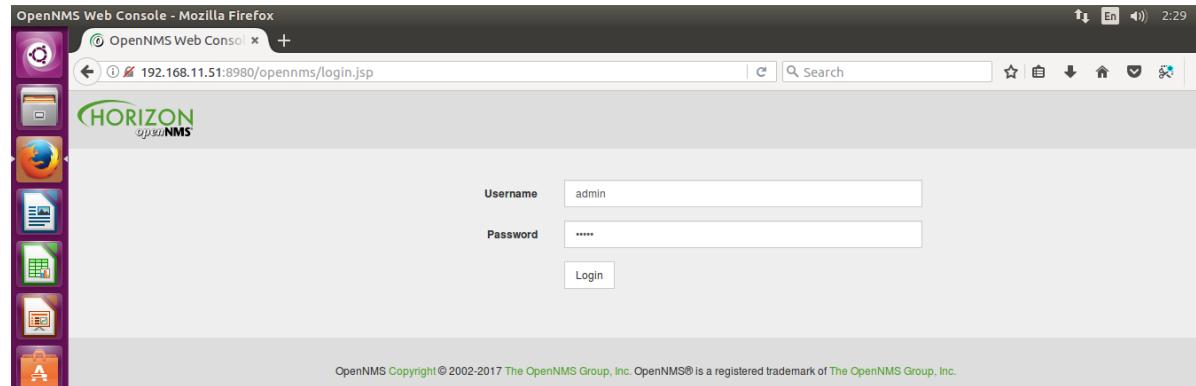


Figure 5. 165: Open OpenNMS web

Step 22: To scan device, use the send-event.pl script below. Replace the IP address with the device you wish to scan.

```
linux2@linux2-OptiPlex-9020:~$ perl /usr/share/opennms/bin/send-event.pl --interface 192.168.11.51 uei.opennms.org/internal/discovery/newSuspect
linux2@linux2-OptiPlex-9020:~$ perl /usr/share/opennms/bin/send-event.pl --interface 192.168.11.42 uei.opennms.org/internal/discovery/newSuspect
linux2@linux2-OptiPlex-9020:~$ perl /usr/share/opennms/bin/send-event.pl --interface www.group1.com uei.opennms.org/internal/discovery/newSuspect
*** "www.group1.com" does not appear to be a valid IP address
Usage: /usr/share/opennms/bin/send-event.pl <UEI> [host] [options]
```

Figure 5. 166: Scan devices

Step 23: The device will be added into OpenNMS once it is found.

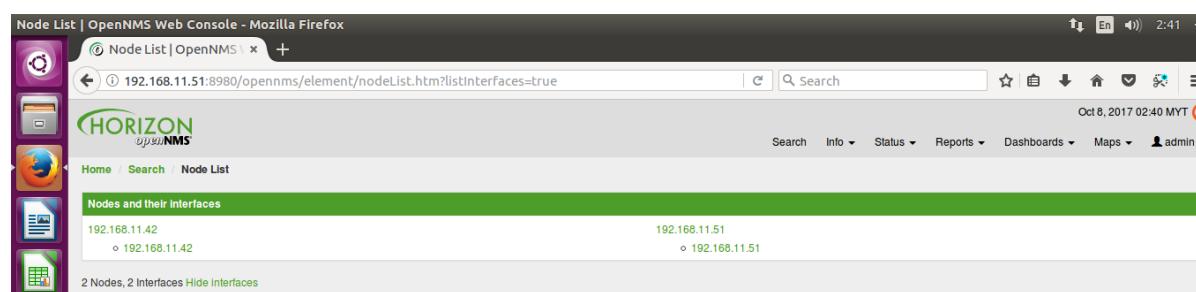


Figure 5. 167: Interface appeared

### 5.3.14 ACCESS CONTROL LIST (ACL)

Step 1: Add access-list extended to block specific port from outside client accessing to our network.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 1 permit 192.168.11.0 0.0.0.255
R1(config)#access-list 100 deny tcp any host 200.200.200.2 eq 80
R1(config)#access-list 100 deny tcp any host 200.200.200.4 eq 21
R1(config)#access-list 100 deny tcp any any eq 22
R1(config)#access-list 100 deny icmp any any
R1(config)#access-list 100 permit ip any any
R1(config)#int g0/1
R1(config-if)#ip access-group 100 in
R1(config-if)#

```

Figure 5. 168: Configuring ACL

- We are denying access to 200.200.200.2 (Windows) to access our web page.
- We are denying access to 200.200.200.4 (Ubuntu) to do file transfer protocol to that server.
- We are denying access to do ssh(port 22) to our network.
- We are denying access to ping to our network.

### 5.3.15 SECURITY HARDDENING

#### Create banner on Switch

Step 1: Enter switch terminal

Step 2: Enter Global Configuration mode using command “configure terminal”

Step 3: Enter command Banner login ^C

```
User Access Verification

Username: admin
Password:
Switch>ena
Password:
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#banner exec ^c
Enter TEXT message. End with the character '^'.
^c
Switch(config)#banner login ^c
Enter TEXT message. End with the character '^'.
#####
#
# THIS SYSTEM IS PROVIDED FOR THE USE BY AUTHORIZED USER ONLY. THANK YOU!
#
#####
^c
Switch(config)#exit
Switch#exit
```

Figure 5. 169: Login Banner for Switch

### Create banner on Router

Step 1: Enter router terminal

Step 2: Enter global configuration mode using command “configure terminal”

Step 3: Enter command Banner login ^C

```
banner exec ^C
*** Ensure that you enter cisco password correctly ***
*** Documentation after making system changes. ***
^C
banner motd ^C
#####
#
#      WELCOME TO GROUP1 WORKSHOP UNAUTHORIZED USER IS PROHIBITED
#
#####

^C
```

Figure 5. 170: Login Banner for Router

### Disable IP finger service

Step 1: Enter terminal

Step 2: Enter global configuration mode using command “configure terminal”

Step 3: Enter command “no service finger”

```
User Access Verification

Username: admin
Password:
Switch>ena
Password:
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#banner exec ^c
Enter TEXT message. End with the character '^'.
^c
Switch(config)#banner login ^c
Enter TEXT message. End with the character '^'.
#####
#
# THIS SYSTEM IS PROVIDED FOR THE USE BY AUTHORIZED USER ONLY. THANK YOU!
#
#####
^c
Switch(config)#exit
Switch#exit
```

Figure 5. 171: Disable IP finger

Notes: Any network devices that have services finger have to disable or protected by firewall if not use to protect against Denial of Service attacks.

### **Password encryption**

Step 1: Enter terminal

Step 2: Enter global configuration mode using command “configure terminal”

Step 3: Enter command “service password-encryption”

```

Building configuration...

[OK]
R1#
R1#
R1#
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#service password-encryption
R1(config)#exit
R1#co
*Nov 14 07:42:03.804: %SYS-5-CONFIG_I: Configured from console by group1 on cons
ole
R1#copy run start
Destination filename [startup-config]?
Building configuration...

[OK]
R1#

```

Figure 5. 172: Password Encryption

Note: Every network devices must have password protected to secure the devices and prevent unauthorized use. The password need to be encrypted by in the devices.

### **Password minimal length**

Step 1: Enter terminal

Step 2: Enter global configuration mode using command “configure terminal”

Step 3: Enter command “service min-length 10 “

```

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#security passwords min-length 10
R1(config)#

```

Figure 5. 173: Password min length

Notes: Password that too short will make the devices easily to guest and will be crack by the hacker. The device is configured to set the password length more than 10 make the devices more secure.

## Login failure

Step 1: Enter terminal

Step 2: Enter global configuration mode using command “configure terminal”

Step 3: Enter command “security authentication failure rate 3 log “

```
R1(config)#
R1(config)#security authentication failure rate 3 log
R1(config)#exit
R1#
*Nov 16 04:30:42.619: %SYS-5-CONFIG_I: Configured from console by group1 on console
R1#copy run start
Destination filename [startup-config]?
Building configuration...

[OK]
R1#
```

Figure 5. 174: Failure rate enable by the devices

Note: Security authentication failure rate is use configure the number of allowable unsuccessful login attempts. The failure rate attempts by the devices is 3 times.

```
#####
#      WELCOME TO GROUP1 WORKSHOP UNAUTHORIZED USER IS PROHIBITED
#
#####
User Access Verification
Username: group1
Password:
Nov 28 04:39:21.812 UTC: %LOGIN-3-TOOMANY_AUTHFAILS: Too many Login Authentication failures have occurred in the last one minute on the line 0.
% Authentication failed
Username: 
```

Figure 5. 175: Failure rate enable

## Disable unused port on switch

Step 1: Enter terminal

Step 2: Enter global configuration mode using command “configure terminal”

Step 3: Enter terminal configuration interface by using command: interface range fa0/13-23

Step 4: Shut down the unused port by using command “shutdown” and exit

```

Switch(config)#interface range fa0/13-23
Switch(config-if-range)#shutdown
Switch(config-if-range)#exit
Switch(config)#
*Mar 6 07:37:45.152: %LINK-5-CHANGED: Interface FastEthernet0/13, changed state
to administratively down
*Mar 6 07:37:45.161: %LINK-5-CHANGED: Interface FastEthernet0/14, changed state
to administratively down
*Mar 6 07:37:45.161: %LINK-5-CHANGED: Interface FastEthernet0/15, changed state
to administratively down
*Mar 6 07:37:45.161: %LINK-5-CHANGED: Interface FastEthernet0/16, changed state
to administratively down
*Mar 6 07:37:45.161: %LINK-5-CHANGED: Interface FastEthernet0/17, changed state

Switch(config)#to administratively down
*Mar 6 07:37:45.169: %LINK-5-CHANGED: Interface FastEthernet0/18, changed state
to administratively down
*Mar 6 07:37:45.169: %LINK-5-CHANGED: Interface FastEthernet0/19, changed state
to administratively down
*Mar 6 07:37:45.169: %LINK-5-CHANGED: Interface FastEthernet0/20, changed state
to administratively down
*Mar 6 07:37:45.169: %LINK-5-CHANGED: Interface FastEthernet0/21, changed state
to administratively down
*Mar 6 07:37:45.169: %LINK-5-CHANGED: Interface FastEthe
Switch(config)#rnet0/22, changed state to administratively down
*Mar 6 07:37:45.178: %LINK-5-CHANGED: Interface FastEthernet0/23, changed state
to administratively down
*Mar 6 07:37:46.176: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/22, changed state to down
Switch(config)#exit
Switch#co
*Mar 6 07:37:52.065: %SYS-5-CONFIG_I: Configured from console by admin on conso
le
Switch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]

```

Figure 5. 176: Disable unused port

Notes: Disabling unused port is the efficient way to secure the cisco devices to prevent unauthorized user from access the devices. Futhermore, there is no traffic flow between the unused ports

### 5.3.16 AUTHENTICATION USING RADIUS SERVER

Step 1: Click on Server Manager > Roles > Add Roles.

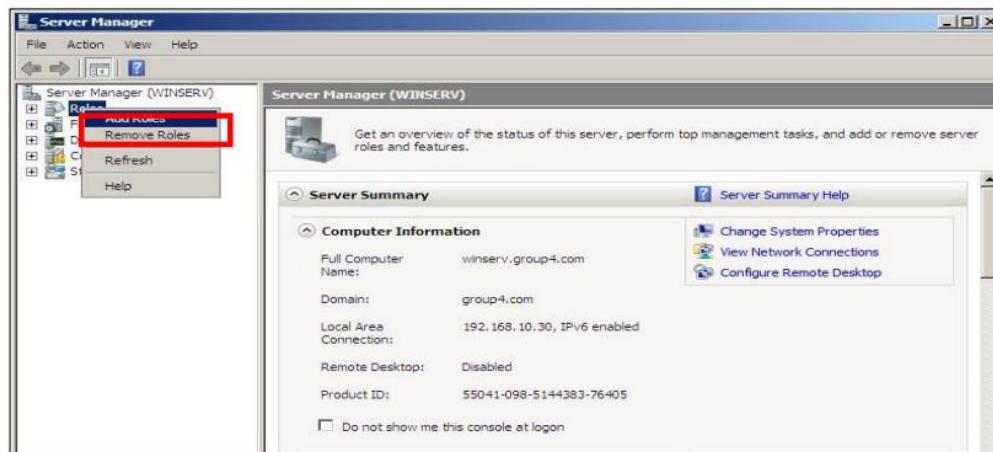


Figure 5. 177: Add Roles

Step 2: Then, in Before You Begin, after read the information, click Next.

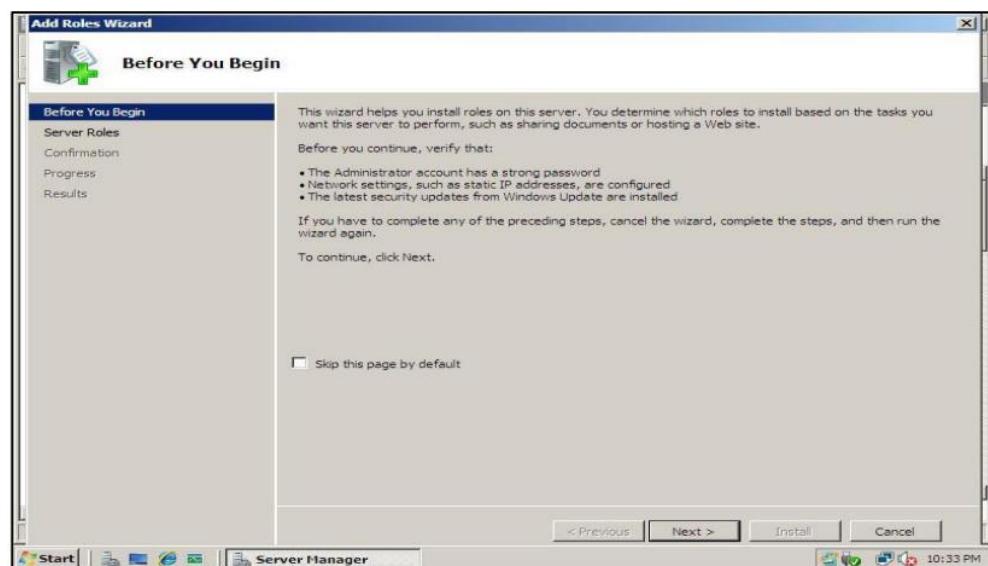


Figure 5. 178: Before You Begin

Step 3: In Add Roles Wizard, tick on Network Policy and Access Services.

Then click Next.

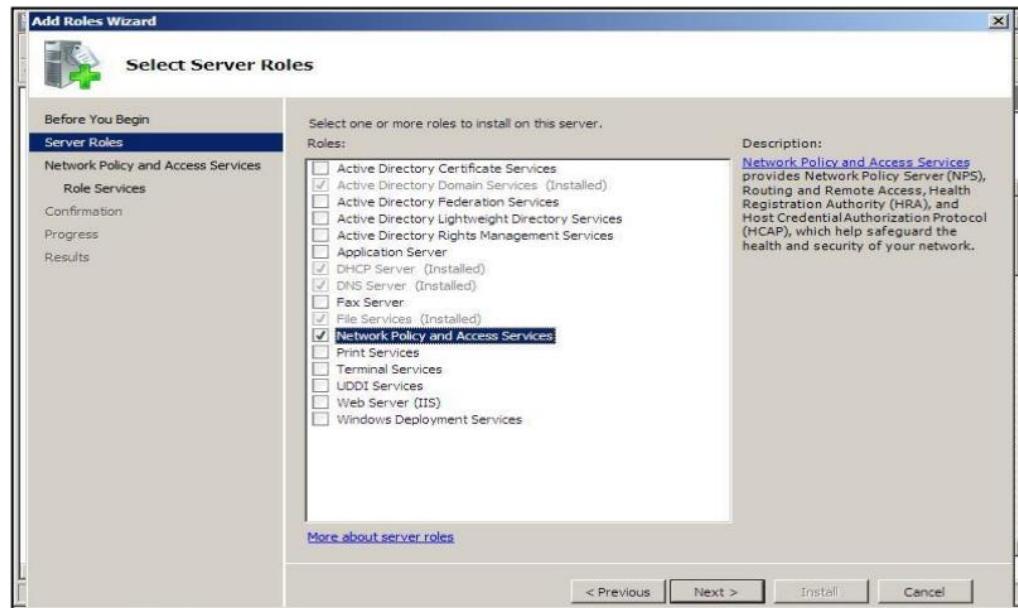


Figure 5. 179: Select Server Roles

Step 4: Read the information in Network Policy and Access Services then click Next.



Figure 5. 180: Network Policy and Access Services

Step 5: In Select Role Services, tick on Network Policy Server. Then, click Next.

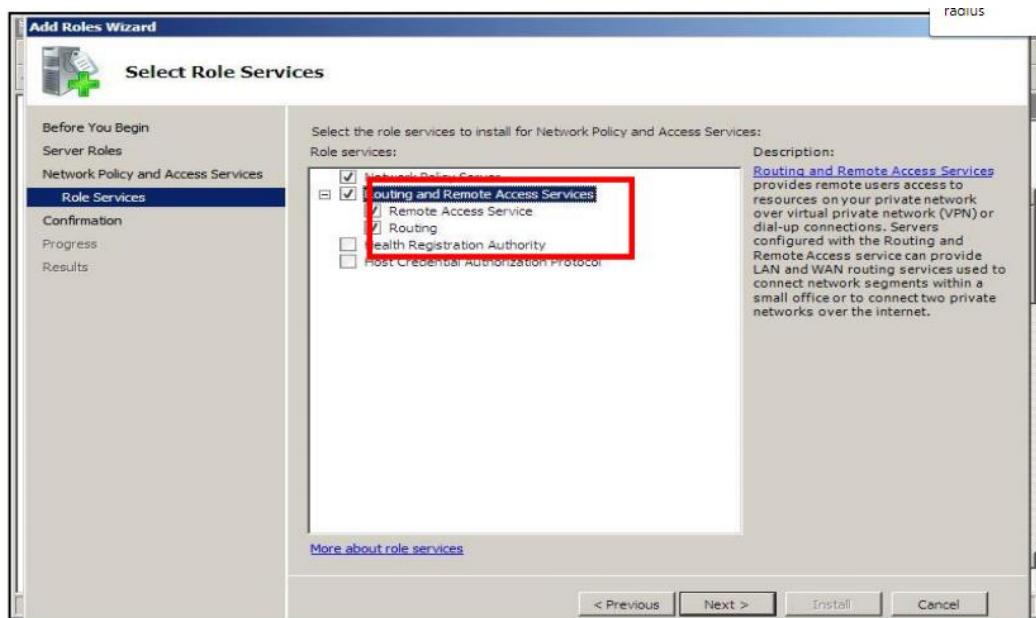


Figure 5. 181: Select Role Services.

Step 6: In Confirm Installation Selections page, click Install.

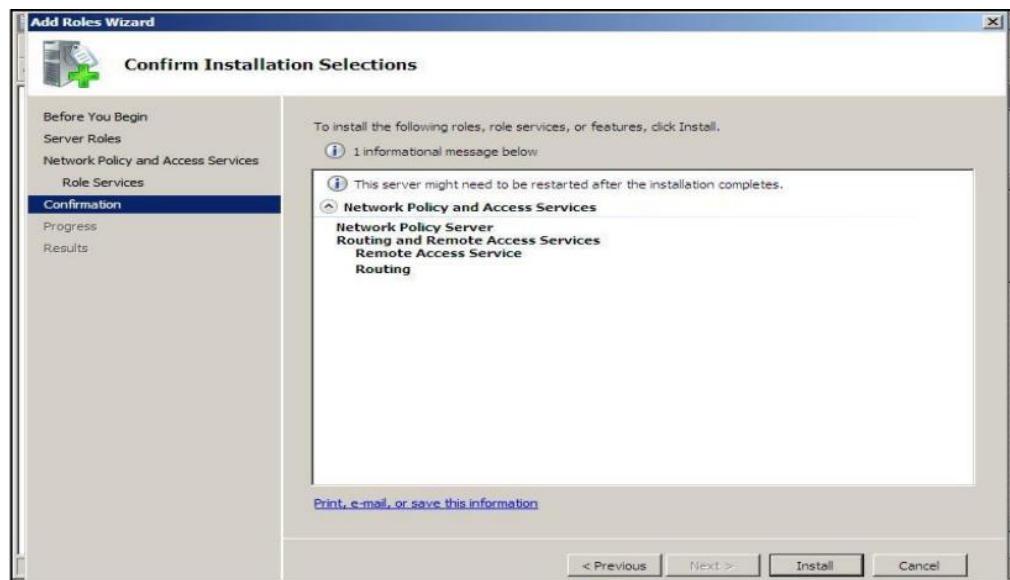


Figure 5. 182: Confirm Installation Selections.

Step 7: Installation Progress page.

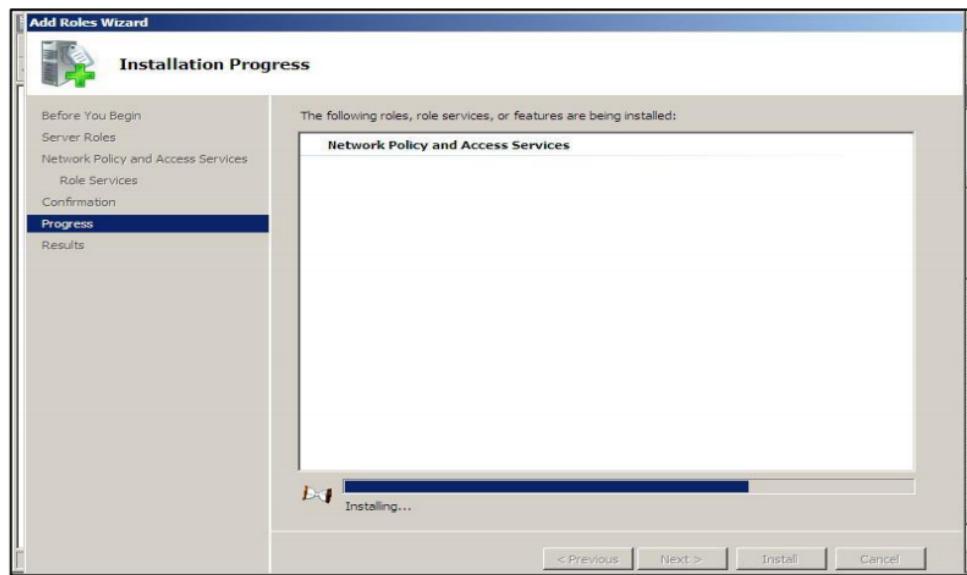


Figure 5. 183: Installation Progress.

Step 8: In Installation Results page show Installation succeeded. Then, click Close.

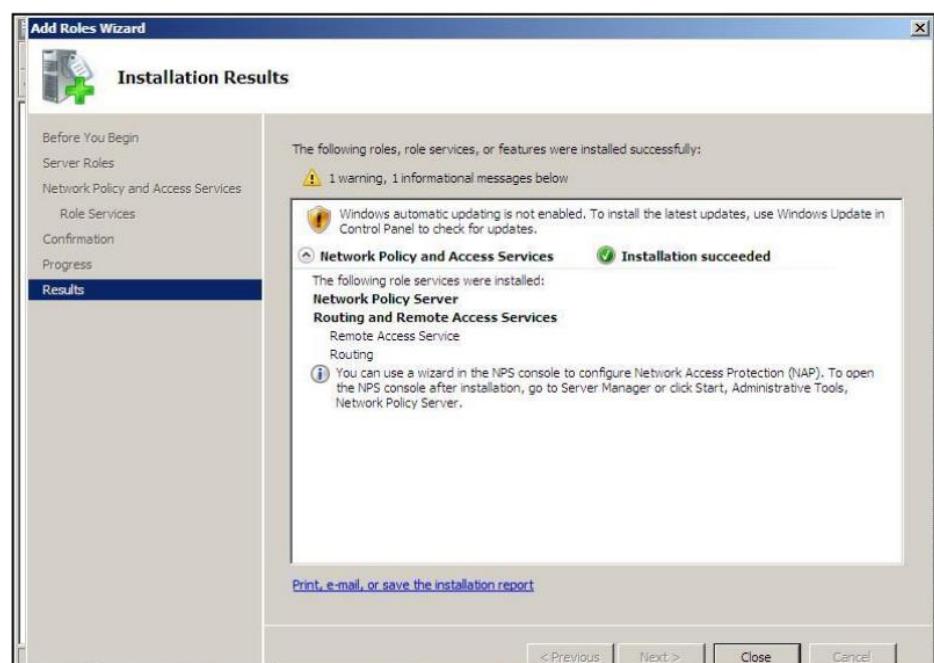


Figure 5. 184: Installation Progress.

Step 9: Click on Start > All Programs > Administrative Tools > Network Policy Server.

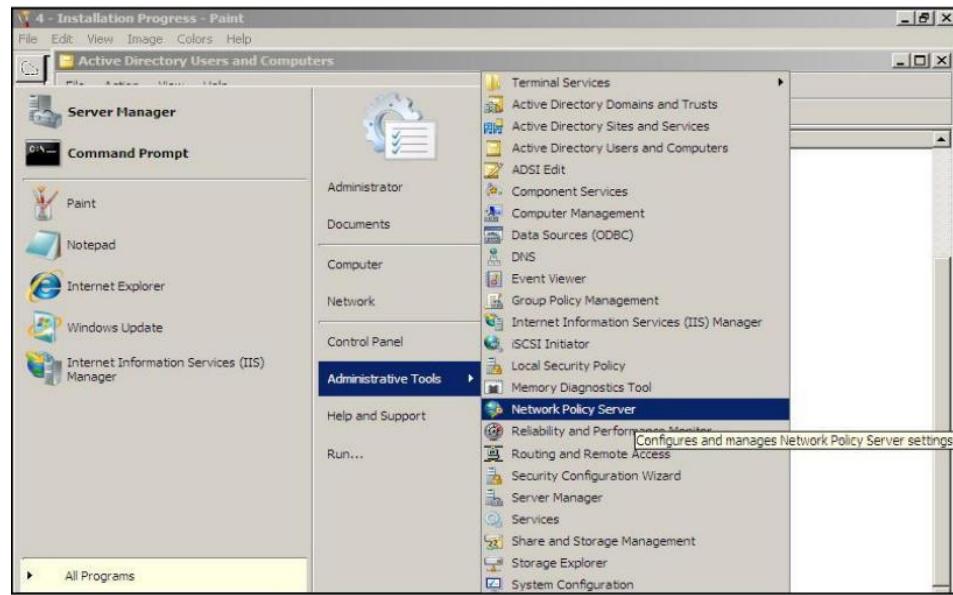


Figure 5. 185: Installation results.

Step 10: Right click on NPS (Local) > Register server in Active Directory.

Then popup windows, click OK.

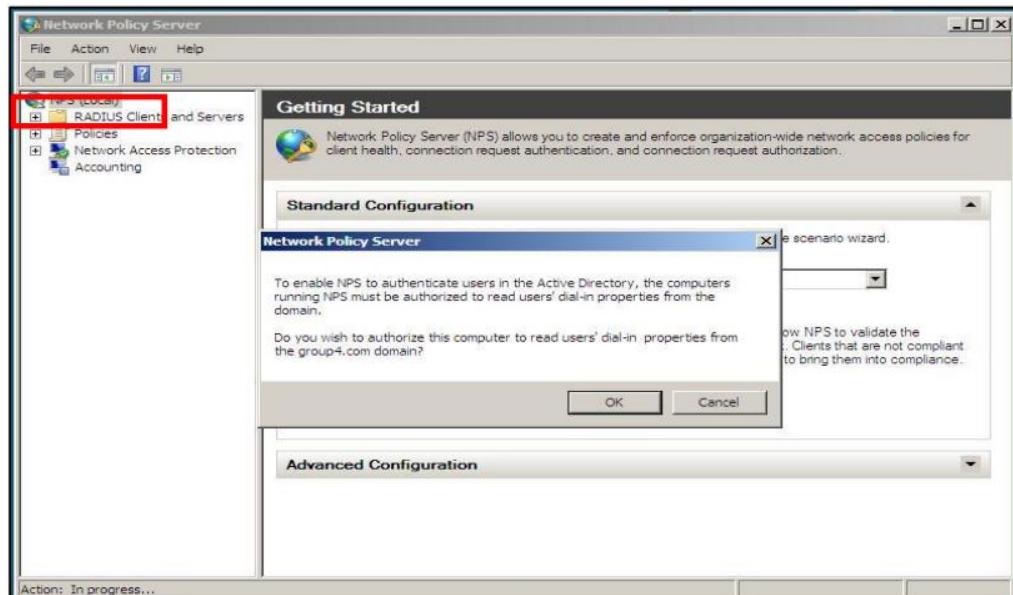


Figure 5. 186: Go to Network Policy Server

Step 11: Next, popup windows click OK.

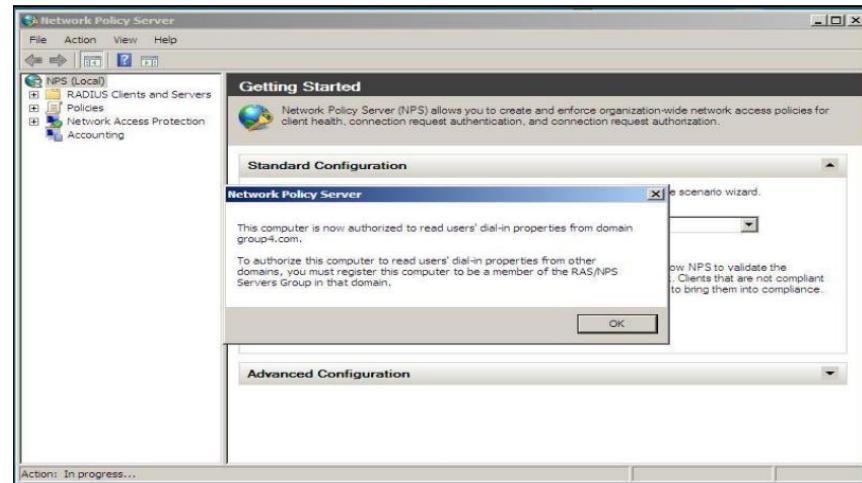


Figure 5. 187: Click Ok

Step 12: Expand RADIUS Clients and Servers, right click on RADIUS Clients, and choose New RADIUS Client.

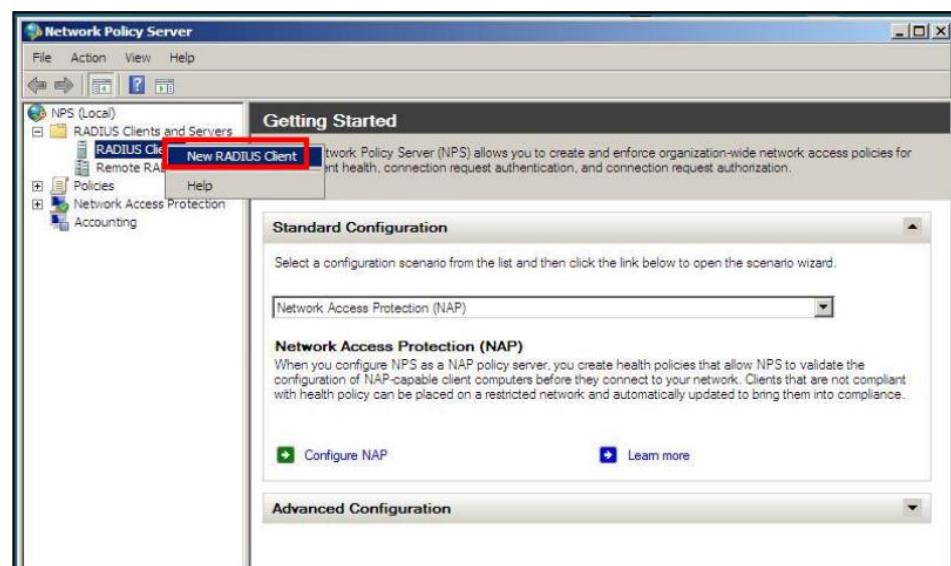


Figure 5. 188: New RADIUS Client.

Step 13: Enter Friendly Name and Address. Tick Manual shared secret and enter the Shared secret. Then, click OK.

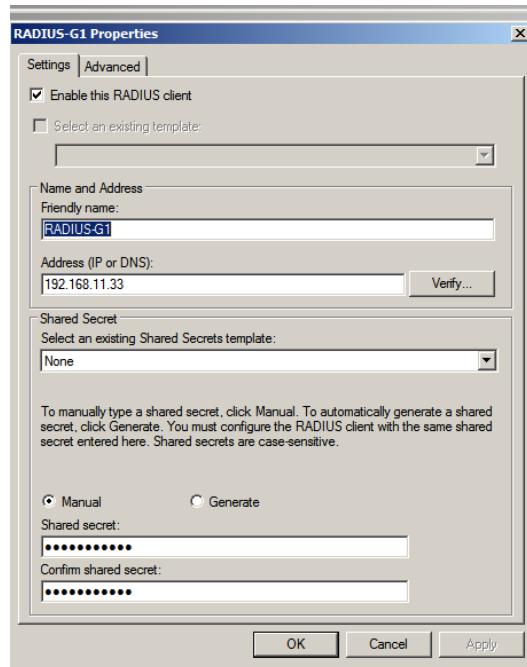


Figure 5. 189: RADIUS Client.

Step 14: Create a connection request policy. Expand the Policies, right click on Connection Request Policies and choose New.

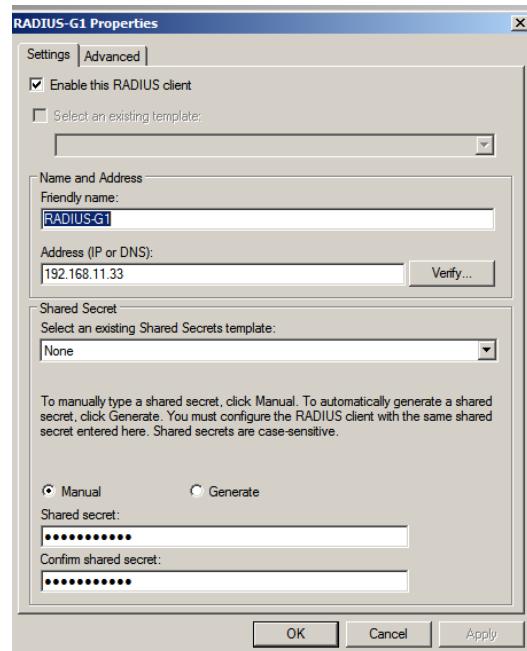


Figure 5. 190: New Network Policies.

Step 15: Enter the Policy Name and click Next.

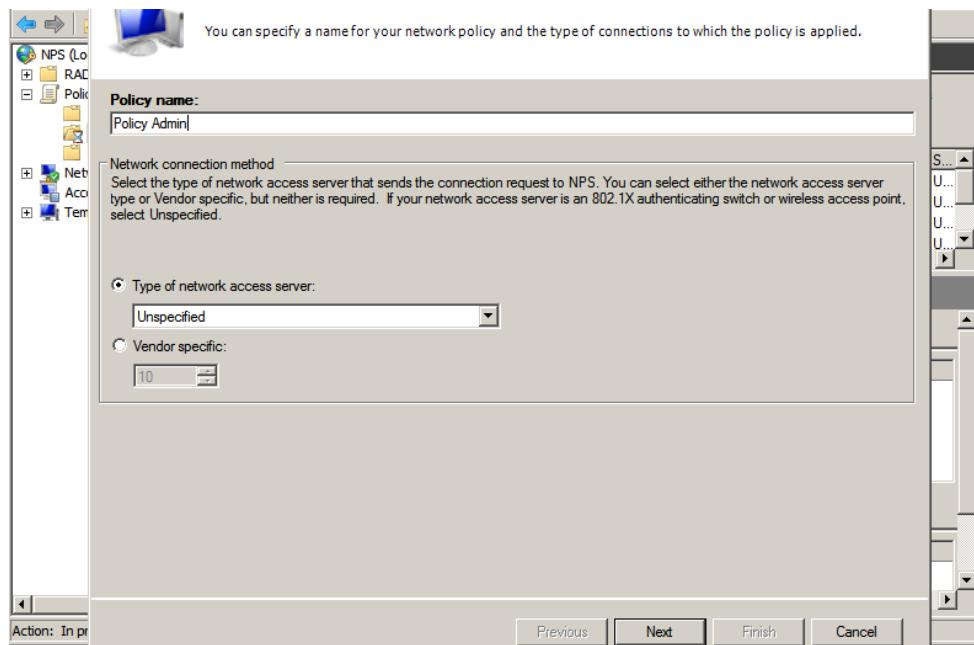


Figure 5. 191: Policy Name and Connection Type.

Step 16: On Specify Conditions page, click Add.

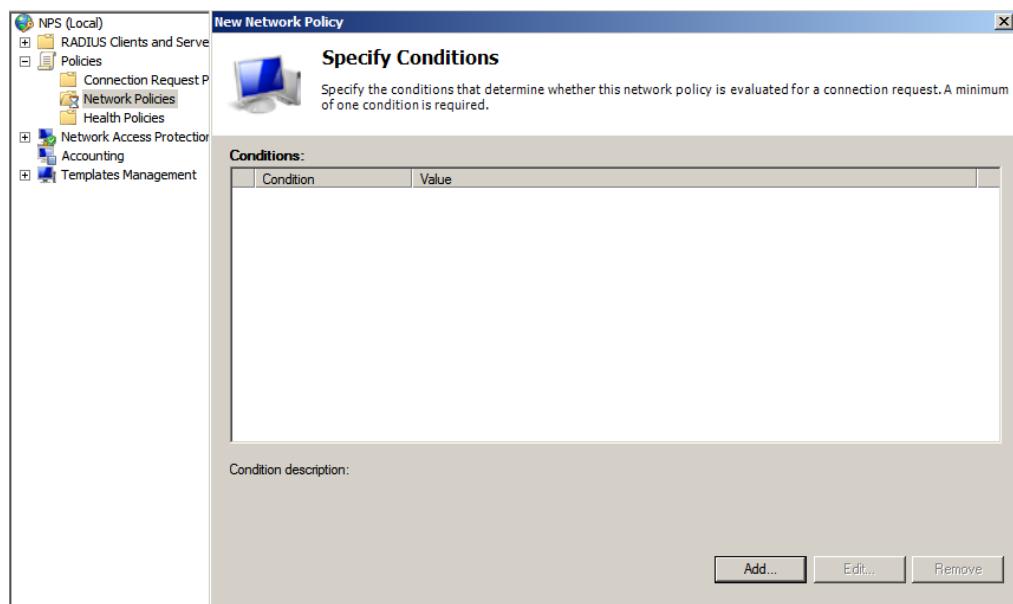


Figure 5. 192: Specify Conditions.

Step 17: Select the condition > User Groups, then click Add.

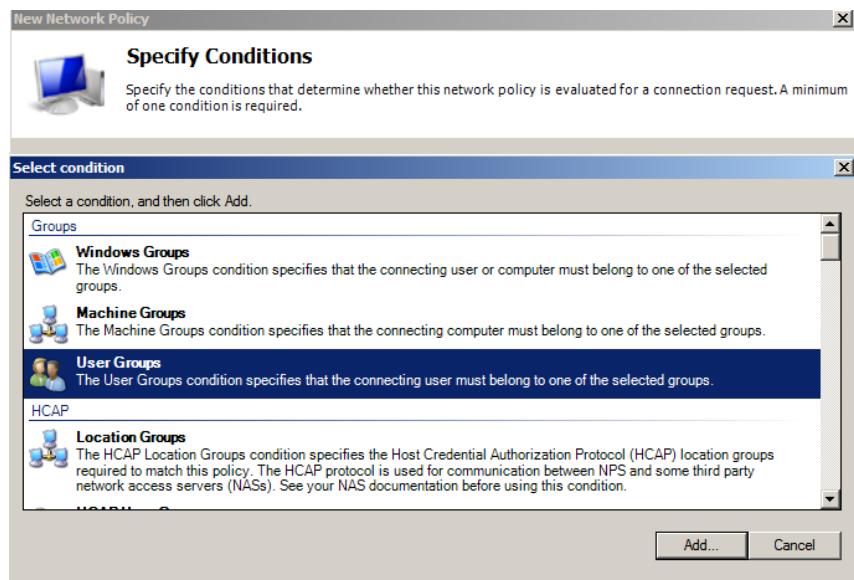


Figure 5. 193: Add User Groups.

Step 18: In User Groups page, click Add Groups.

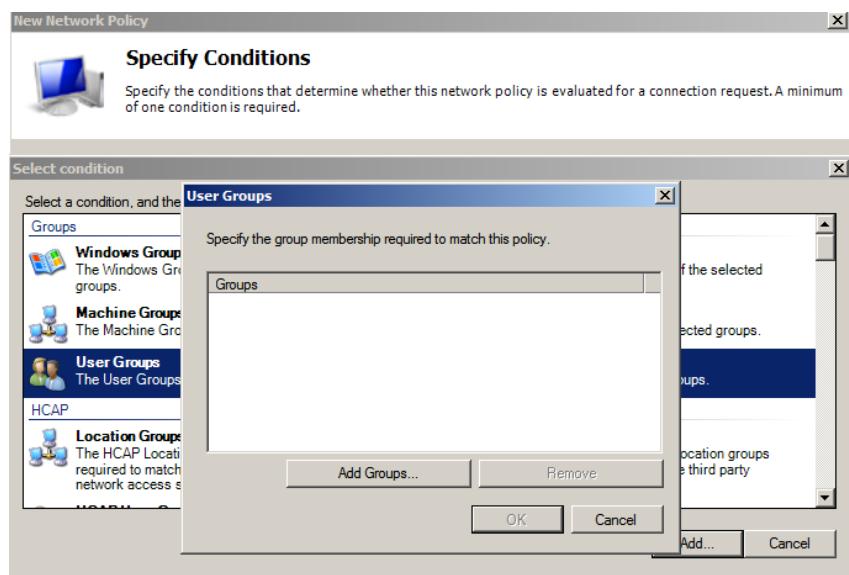


Figure 5. 194: Add Groups.

Step 19: Enter the object name to select > dom > Check Names. Then, choose Domain Users and click OK.

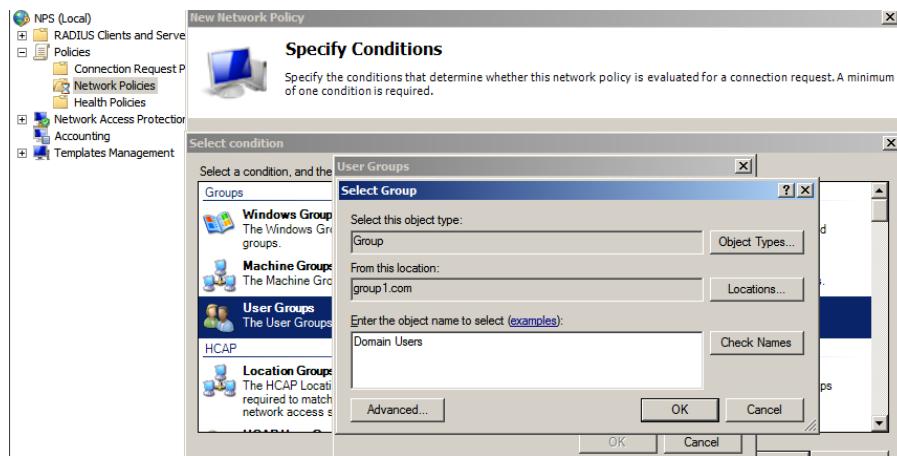


Figure 5. 195: Domain Users.

Step 20: Then, click OK.

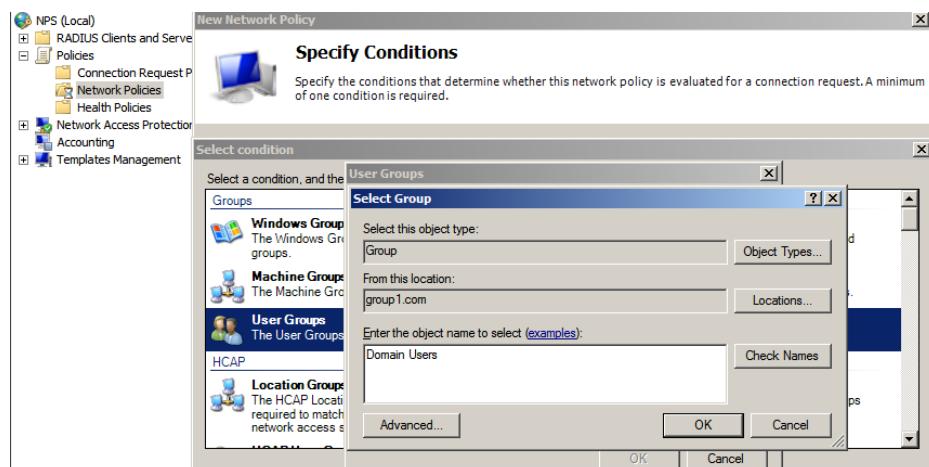


Figure 5. 196: Select Group.

Step 21: Proceed to OK.

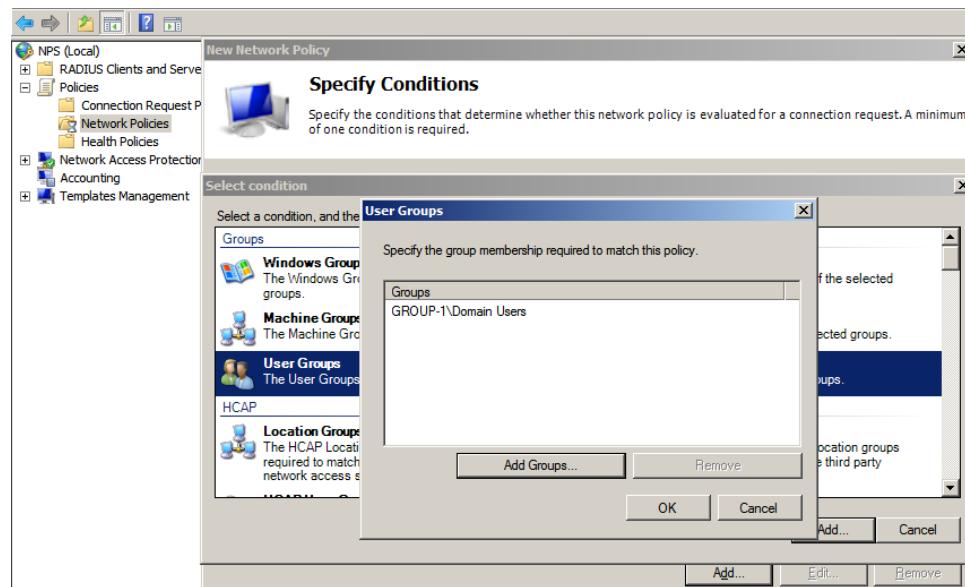


Figure 5. 197: User Groups.

Step 22: In Specify Conditions page, proceed to Next.

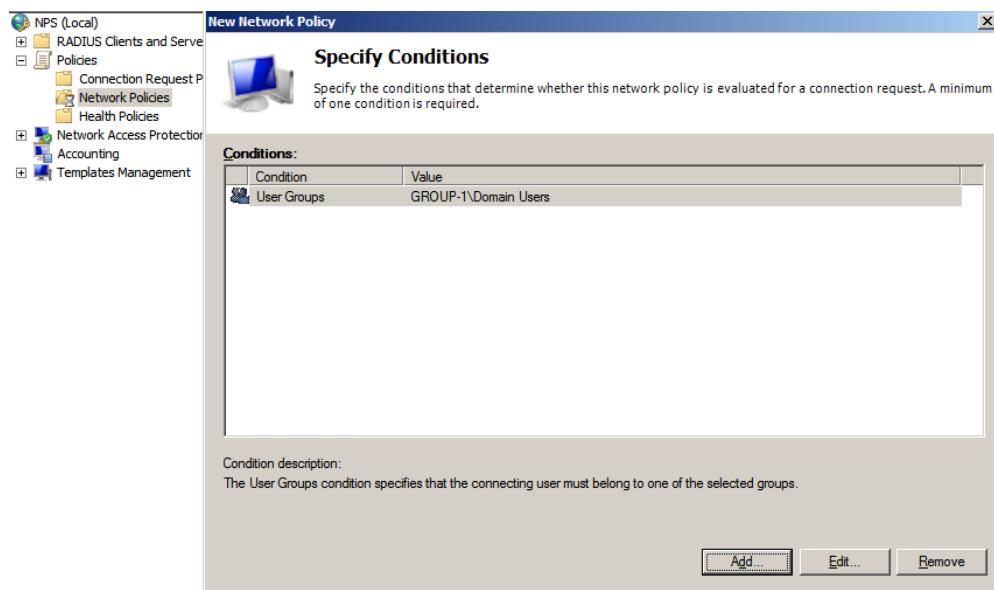


Figure 5. 198: Specify Conditions.

Step 23: In Specify Access Permission, tick Access granted. Proceed to Next.

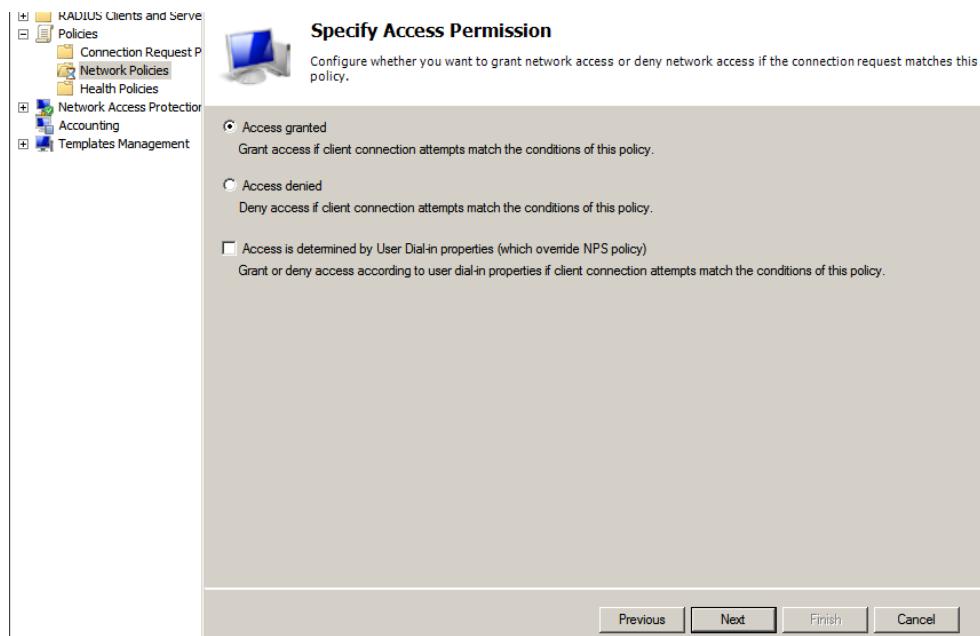


Figure 5. 199: Specify Access Permission > Access Granted.

Step 24: On Configuration Authentication Methods, tick on Unencrypted authentication (PAP, SPAP). Proceed to Next. When Connection request policy windows appear, click No.

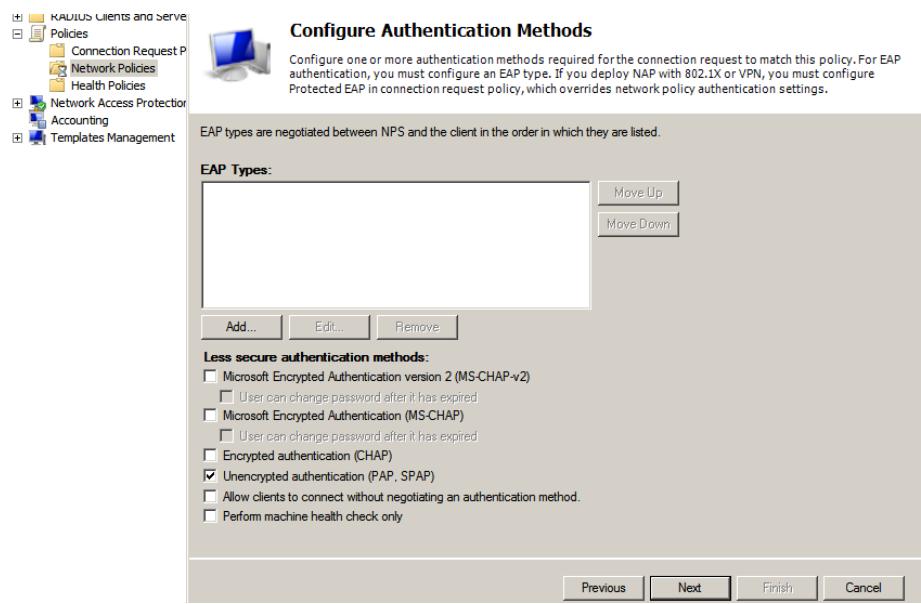


Figure 5. 200: Configure Authentication Methods

Step 25: Configure Constraints page, proceed to Next.

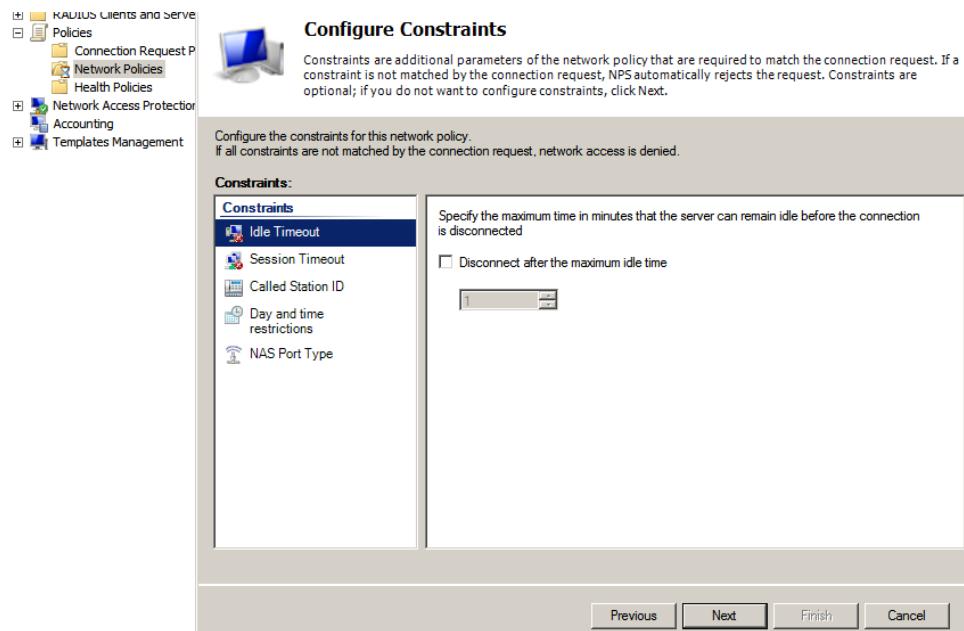


Figure 5. 201: Idle Timeout

Step 26: In Standard, remove Framed-Protocol and Service-Type attributes.

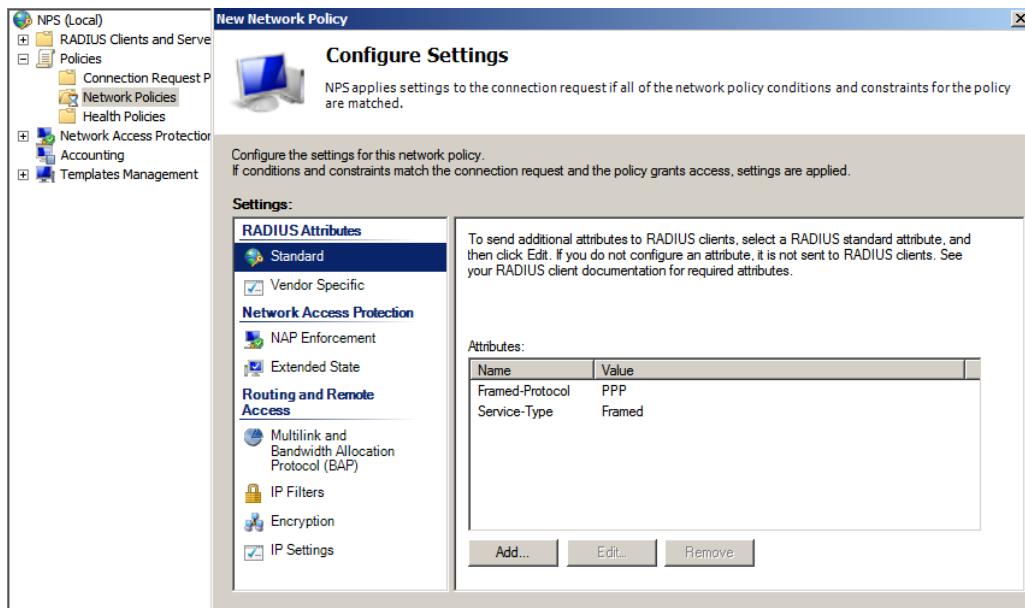


Figure 5. 202: Remove Attributes.

Step 27: Click Add to add attributes, set the name as Service-Type and value as Login.

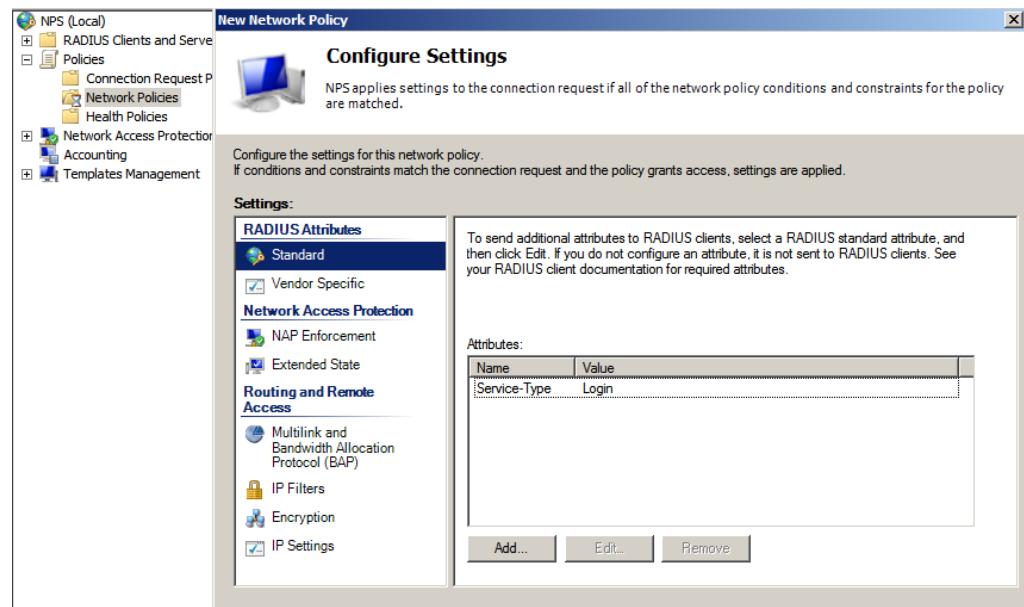


Figure 5. 203: Standard.

Step 28: In Vendor Specific, add attributes name Cisco-AV-Pair, vendor Cisco and value shell:priv-lvl=15.

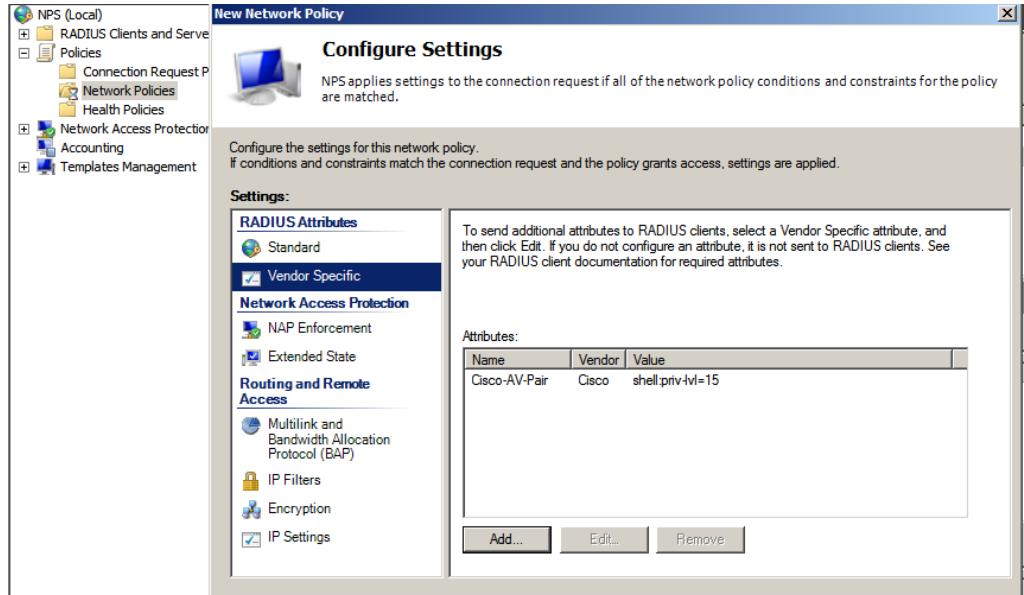


Figure 5. 204: Vendor Specific.

Step 29: In Encryption, tick on the No encryption. Then, click Next.

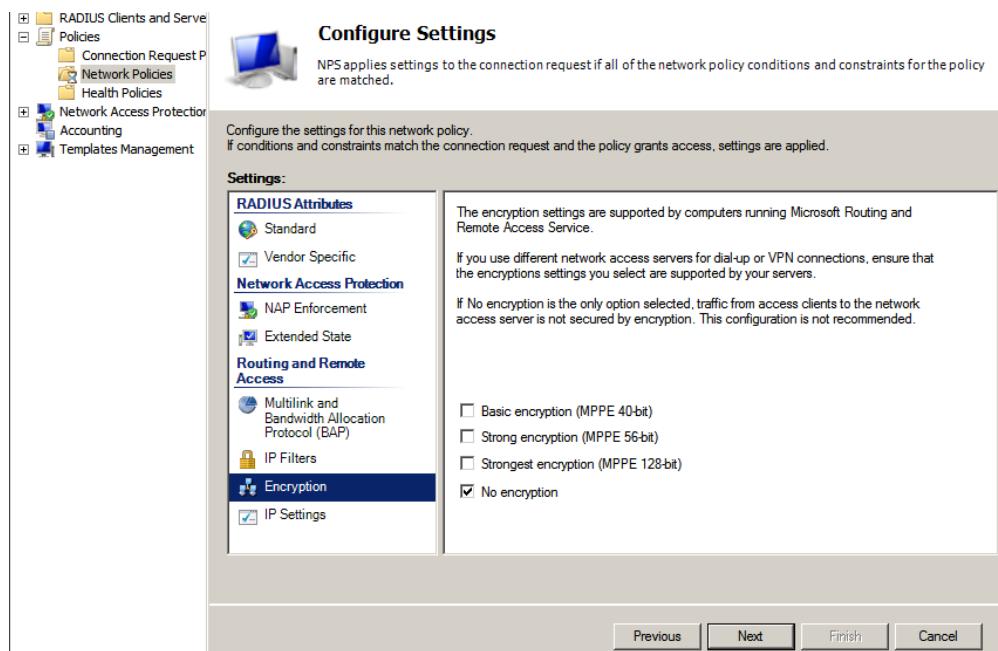


Figure 5. 205: Encryption

Step 30: On IP Settings, tick on the Server settings determines IP address assignment.

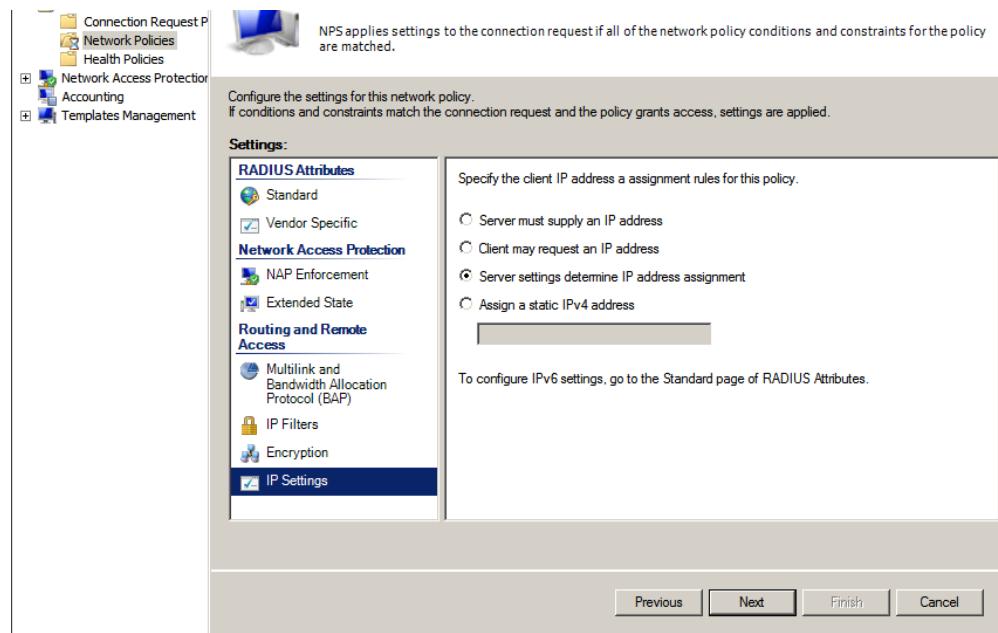


Figure 5. 206: IP Settings

Step 31: In Completing New Network Policy, it will displays that successfully created the network policy. Click Finish.

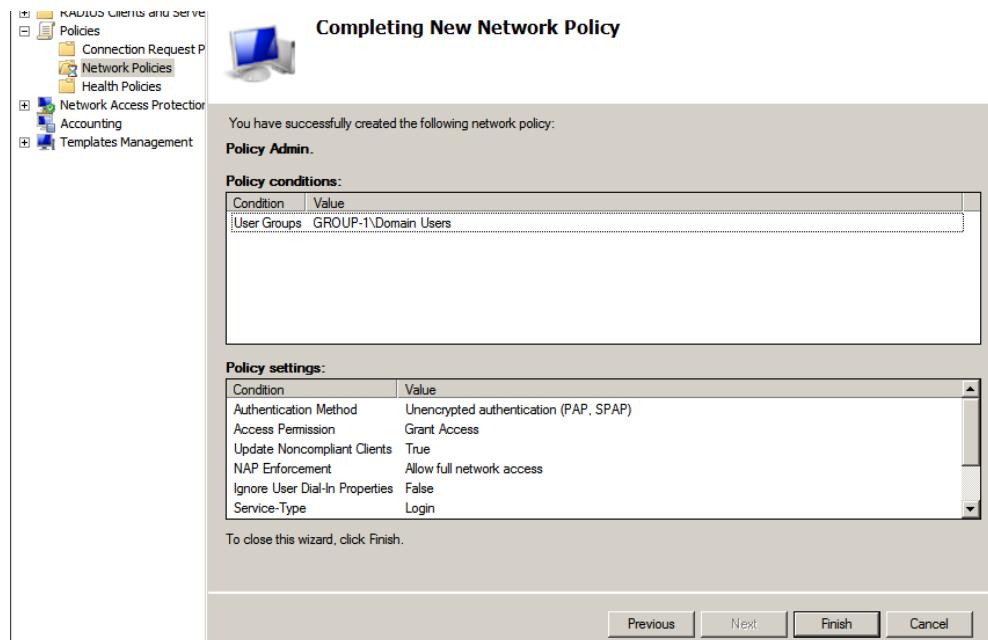


Figure 5. 207: Completing New Network Policy

Step 32: Network policy that had been created.

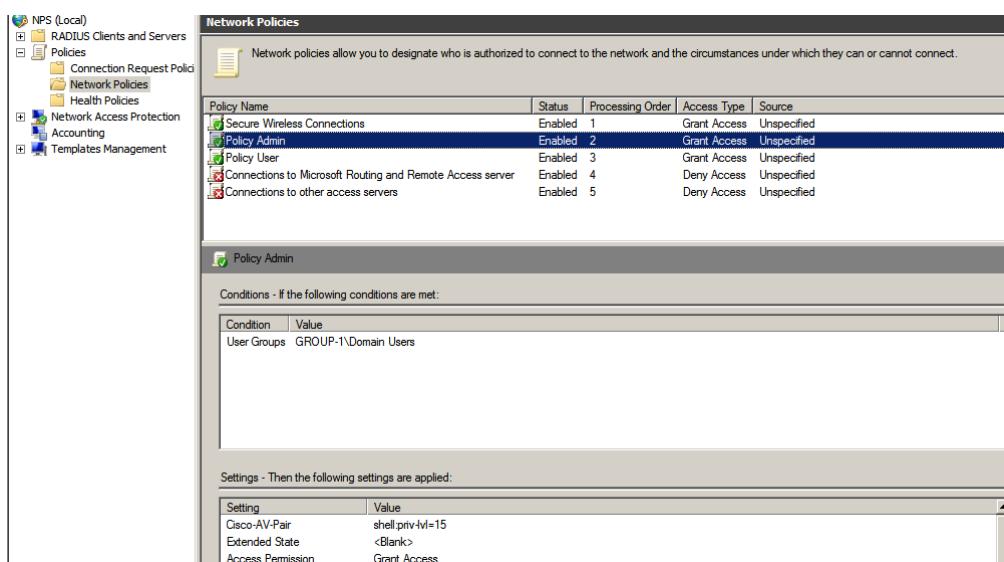


Figure 5. 208: Done created

Step 33: Open putty. Select Serial and click Open.

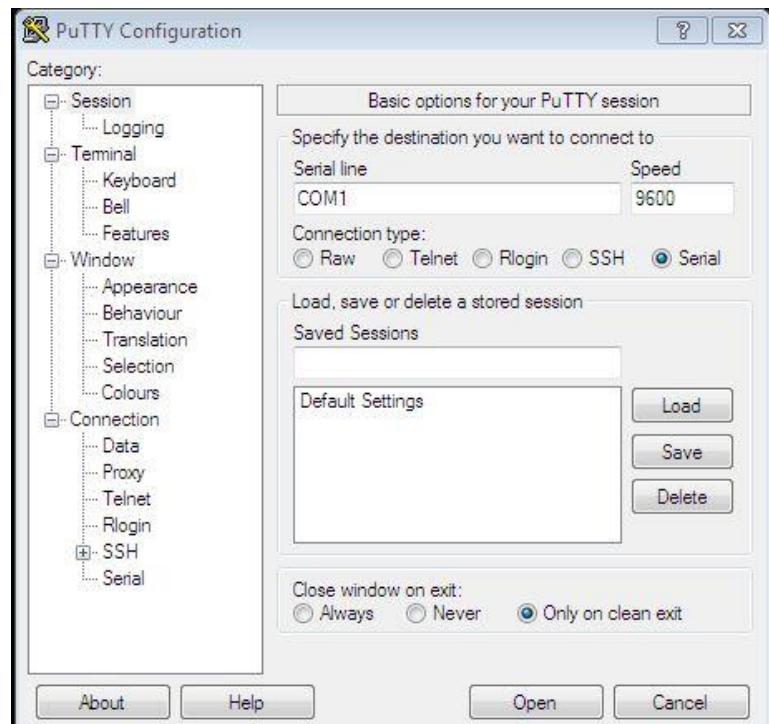


Figure 5. 209: Login using Serial

Step 34: User Access Verification will display. Enter the username (Any AD users) and password. Enter enable (en).

Step 35: Enter global configuration mode using command configure terminal.

```
COM1 - PuTTY
Press RETURN to get started.

#####
#          WELCOME TO GROUP1 WORKSHOP UNAUTHORIZED USER IS PROHIBITED
#
#####
User Access Verification
Username: syukor
Password:

*** Ensure that you enter cisco password correctly ***
*** Documentation after making system changes.      ***

R1#en
R1#
```

Figure 5. 210: Login Router

Step 36: Setup AAA global configuration in the putty terminal

```
R1(config)#aaa new-model
R1(config)#aaa group server radius RADIUS-G1
R1(config-sg-radius)##$8.11.33 auth-port 1812 acct-port 1813 key RADIUS-G1
Translating "private"...domain server (255.255.255.255)

server private 192.168.11.33 auth-port 1812 acct-port 1813 key RADIUS-G1
^
% Invalid input detected at '^' marker.

R1(config-sg-radius)##$8.11.33 auth-port 1812 acct-port 1813 key Abc12345
R1(config-sg-radius)##aaa authentication login default group RADIUS-G1 local
R1(config)##$zation exec default group RADIUS-G1 local if-authenticated
R1(config)##aaa authorization console
R1(config)##exit
R1#
*Nov 17 04:04:41.235: %SYS-5-CONFIG_I: Configured from console by group1 on cons
ole
R1#copy run start
Destination filename [startup-config]?
Building configuration...

[OK]
R1#
```

Figure 5. 211: AAA command for Router

**Problem:** Some users want to secure the router with AAA. Moreover, they also want to know who login into the router.

**Solution:** We install Network Policy Server inside Windows Server 2008 and configure router as radius client. Each user must authenticate using AD before he/she can login into router console or remotely. All the action is recorded in log files.

### 5.3.17 USER AUTHENTICATION AND AUTHORIZATION

Step 1: Go to Start > Administrative Tools > Active Directory Users and Computers.

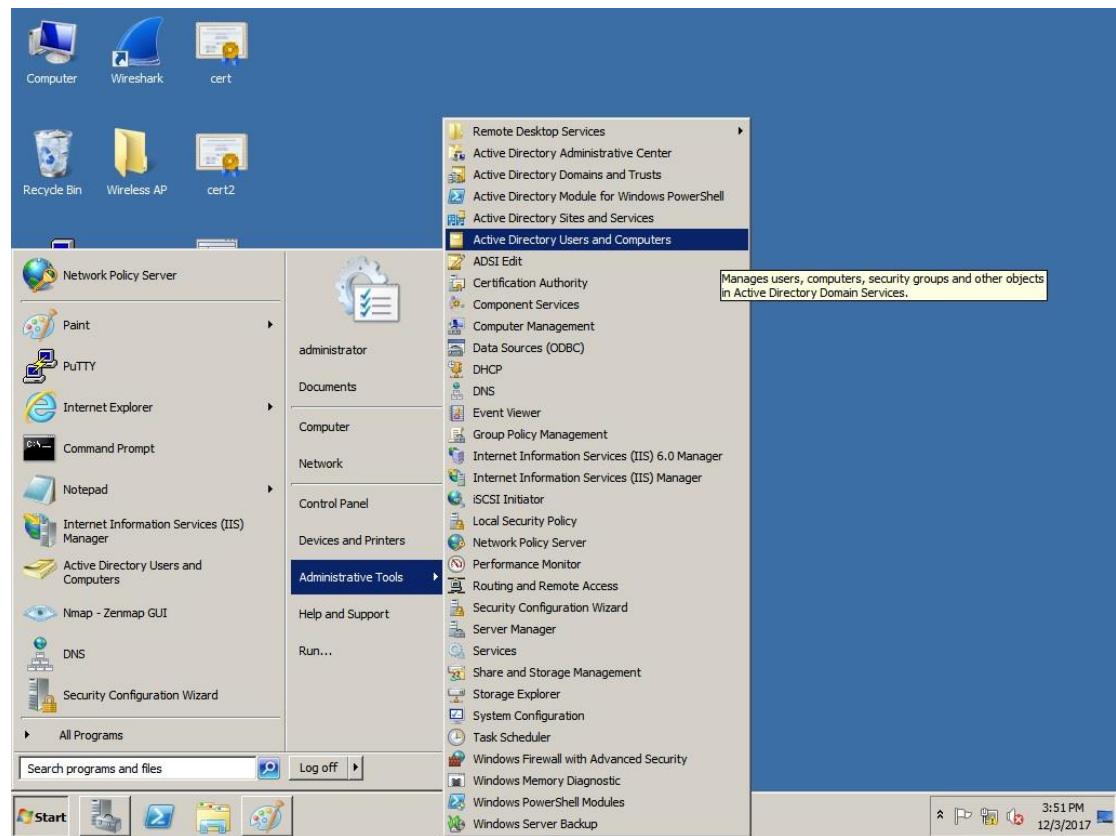


Figure 5. 212: Go to Active Directory Users and Computers

Step 2: Create a new user for RADIUS server user. Right click the User folder > New > User.

Name	Type
abu	User
Administrator	User
Aduser	Security Group - Global
ahmad	User
aini	User
Allowed RODC Password Replication G...	Security Group - Domain Local
ara	User
ashley	User
ashraf	User

Figure 5. 213: Add New User

Step 3: Insert the user information.



Figure 5. 214: New Object - User

Step 4: Insert the password and tick the Password never expires box.



Figure 5. 215: Insert Password

Step 5: Click Finish after confirmed the user information.

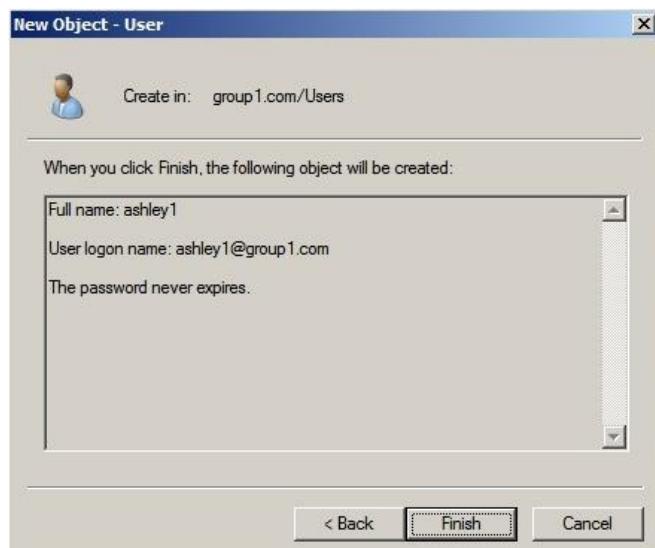


Figure 5. 216: Confirmation Information of User

Step 6: Create a user group for RADIUS server. Right click User folder > New > Group.

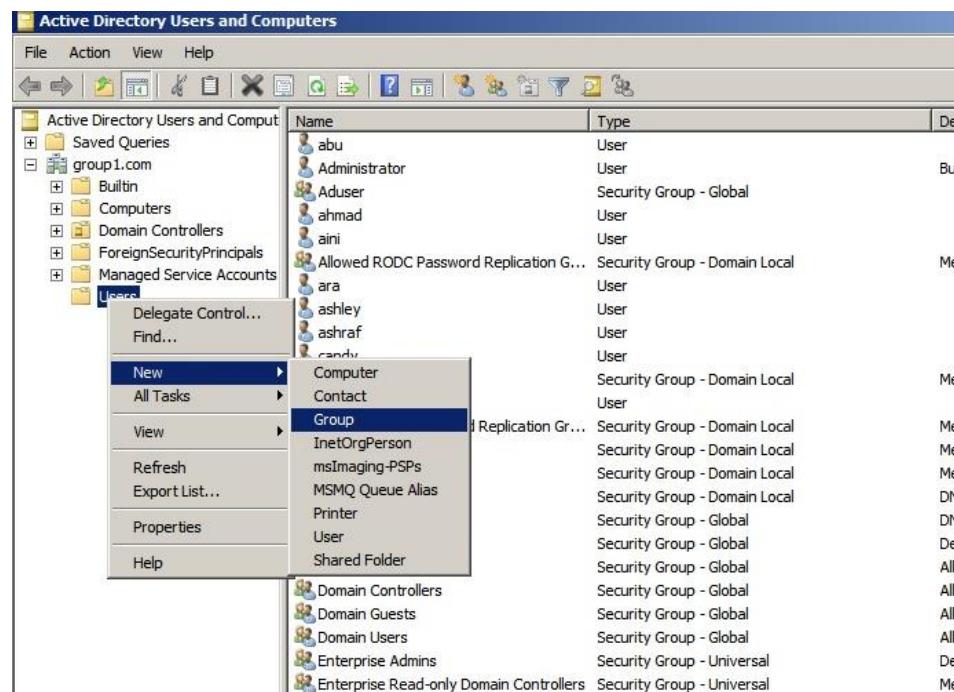


Figure 5. 217: Add New Group

Step 7: Insert a name for user group. Tick the Global box and Security box.

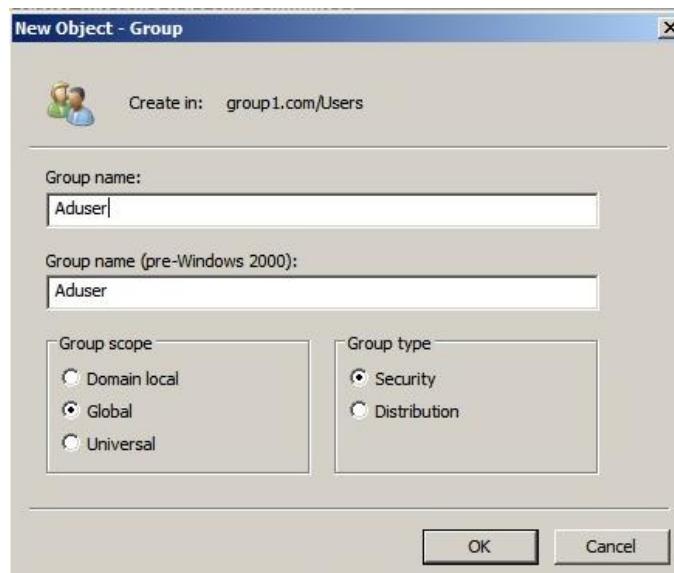


Figure 5. 218: New Object - Group

Step 8: Right click the RADIUS server user and click the Add to a group.

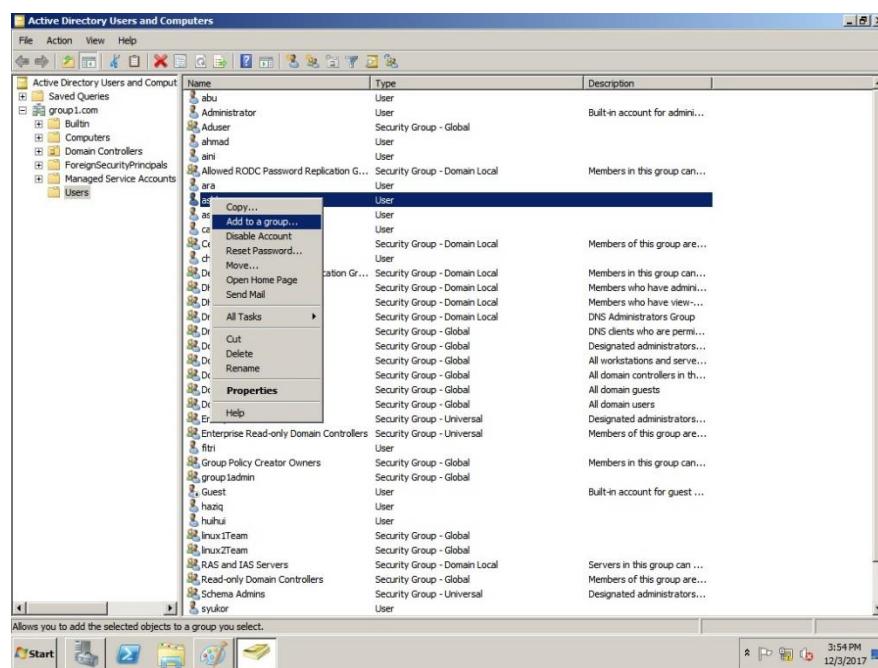


Figure 5. 219: Add user into group

Step 9: Enter the name of the RADIUS server user group. Check the name by click the Check name box.

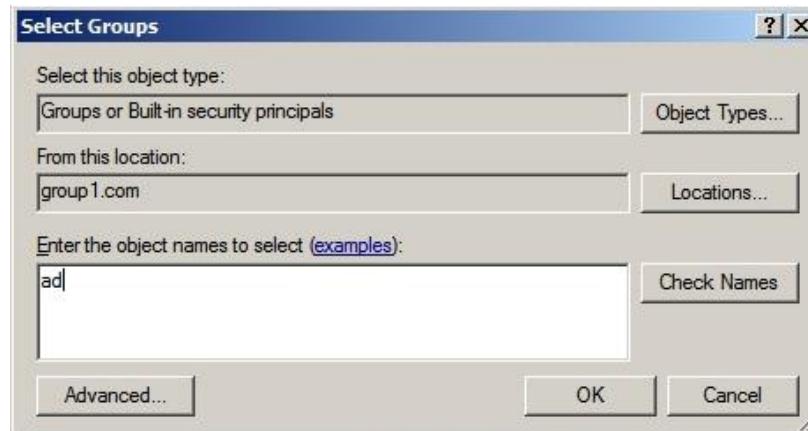


Figure 5. 220: Select Groups

Step 10: Select the name of RADIUS server user group.

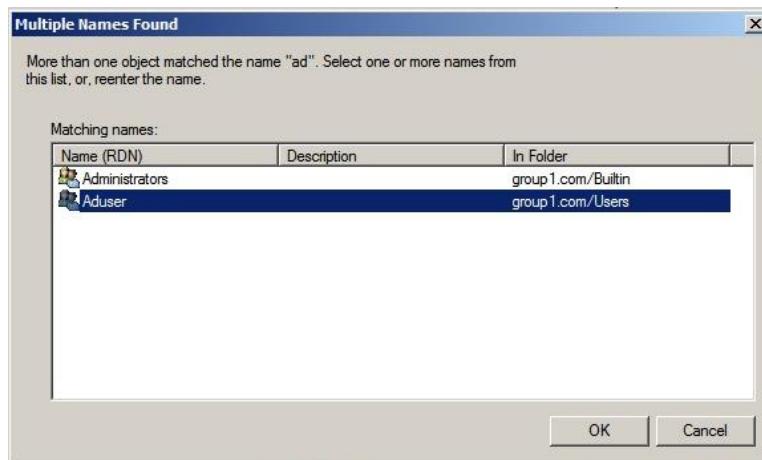


Figure 5. 221: Multiple Names Found

Step 11: Click OK button after confirmed all the information.

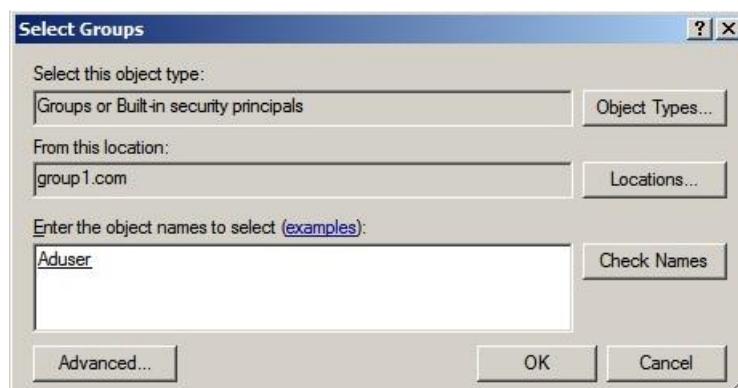


Figure 5. 222: Click ok button

Step 12: Insert the same user into Print Operation group.

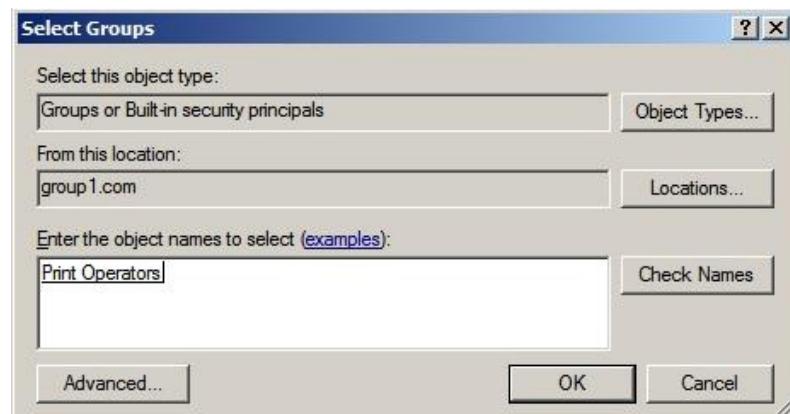


Figure 5. 223: Add User into Print Operation Group

Step 13: Go to Start > Administrative Tools > Network Policy Server.

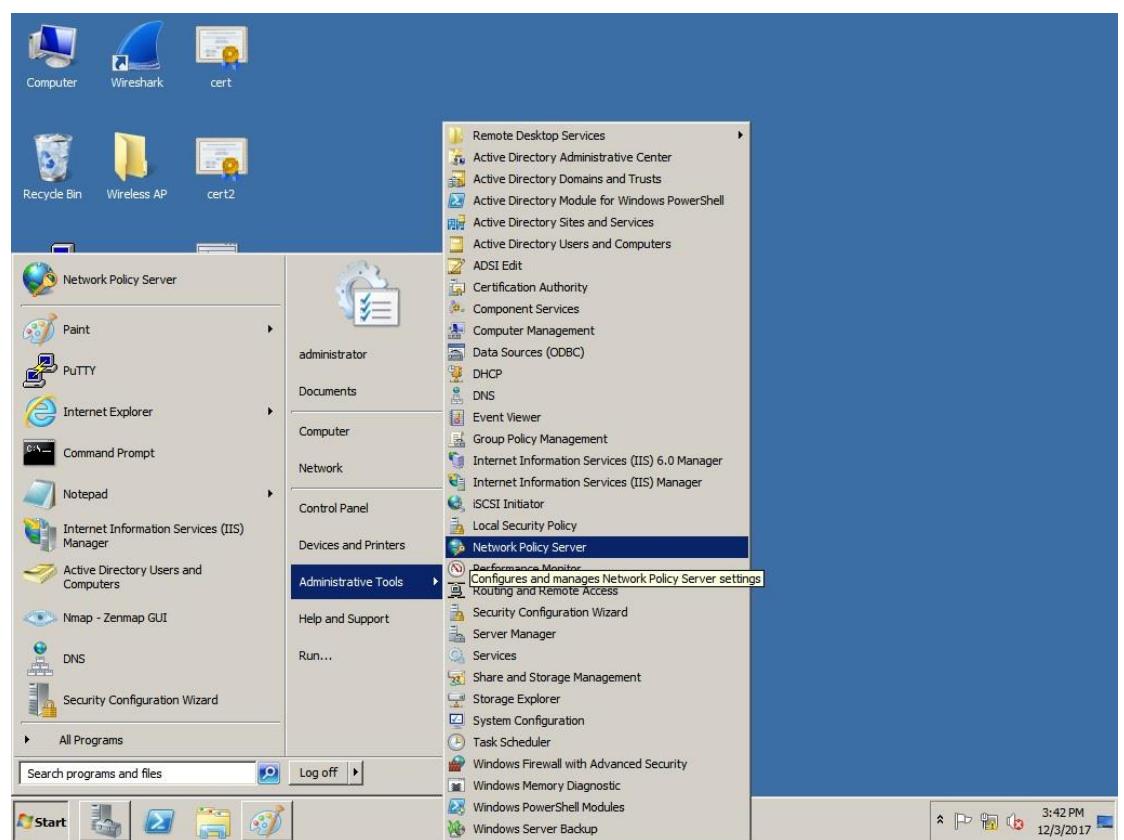


Figure 5. 224: Go to Network Policy Server

Step 14: Expand the Policies. Right click on Network Policies and click New to add new policy.

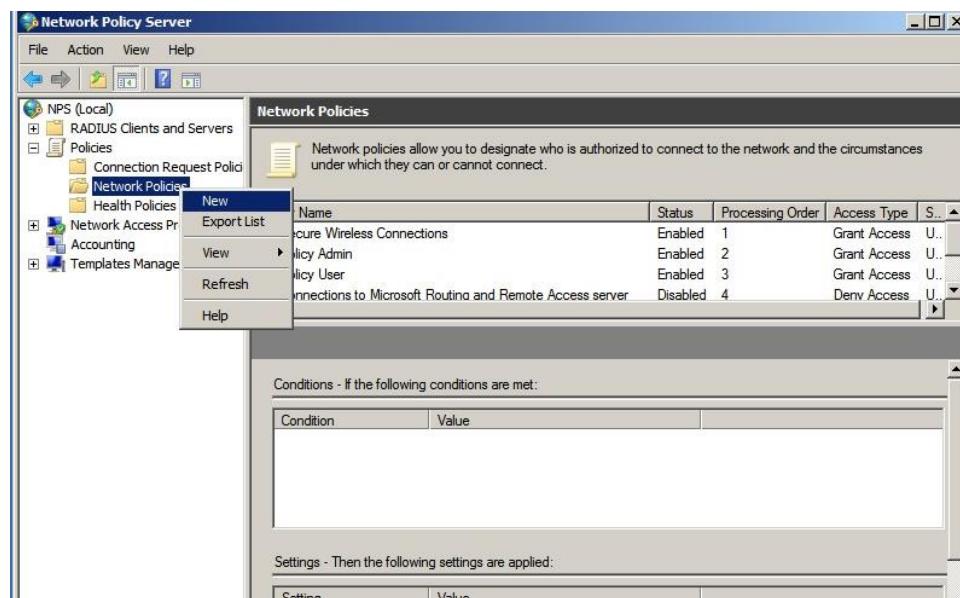


Figure 5. 225: Add New Network Policy

Step 15: Name the policy and the type of network access server is unspecified.

Then, click Next.

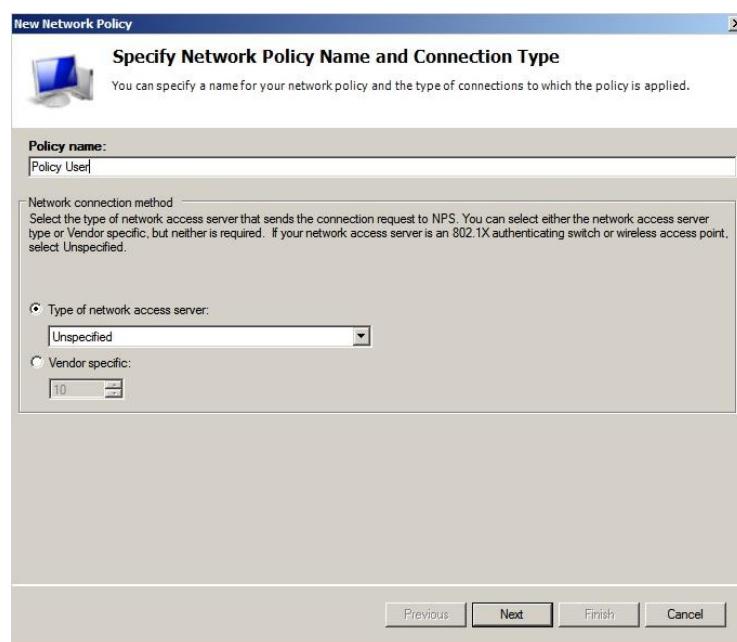


Figure 5. 226: Specify Network Policy Name and Connection Type

Step 16: Click the Add button.

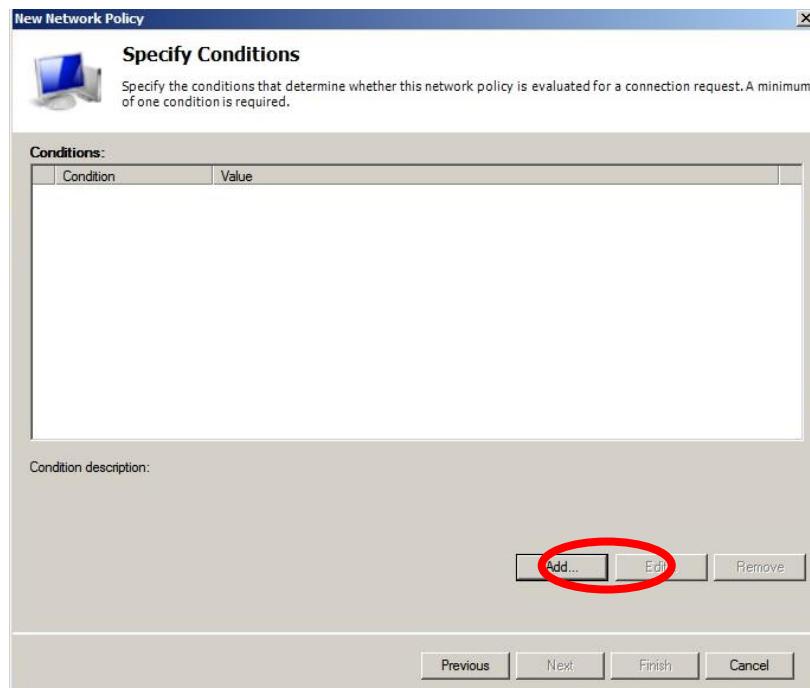


Figure 5. 227: Select Conditions

Step 17: Select the User Groups and click Add button.

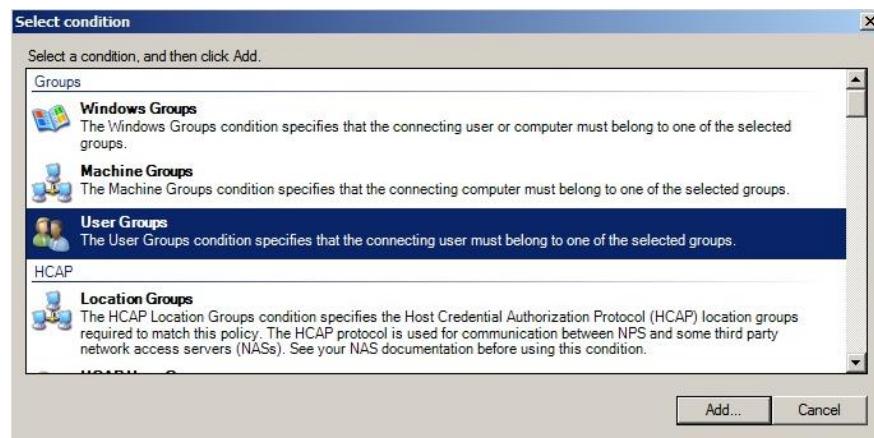


Figure 5. 228: Select User Groups

Step 18: Click Add Groups.



Figure 5. 229: Add Groups

Step 19: Insert the name of RADIUS server user group and click OK.

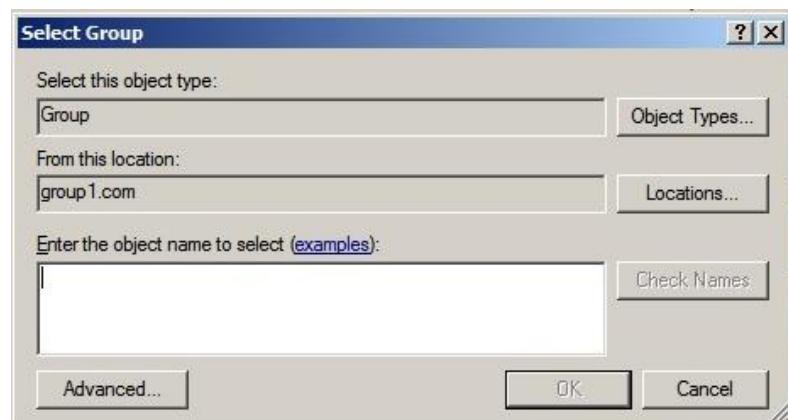


Figure 5. 230: Insert the Group Name

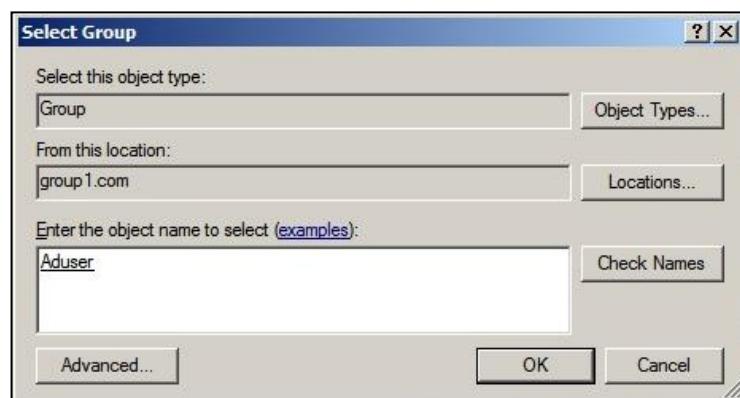


Figure 5. 231: Click Ok button

Step 20: Click OK.



Figure 5. 232: Click Ok button after confirmed the groups is inserted  
correct

Step 21: The name of User Groups is shown in this box and click Next.

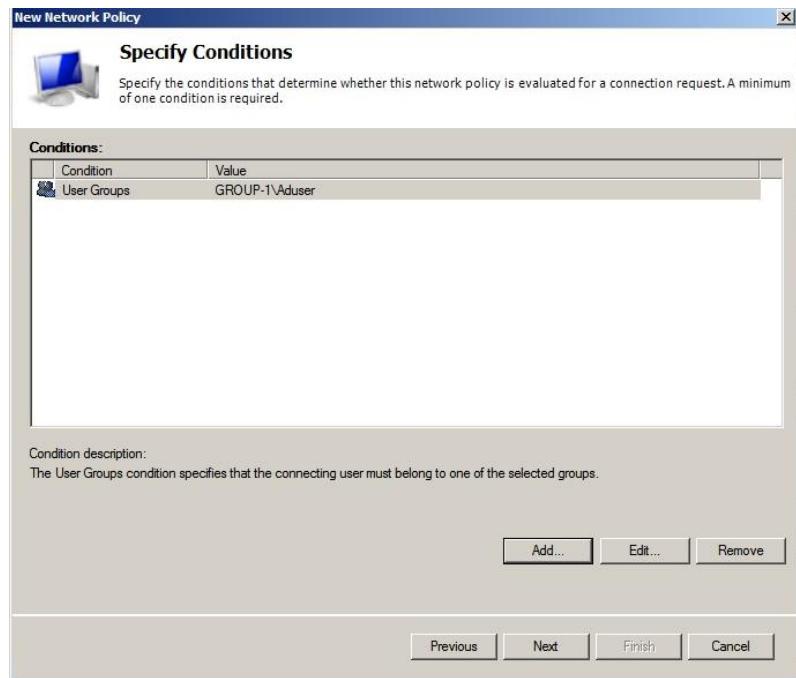


Figure 5. 233: Click Next

Step 22: Select the Access granted and click Next.

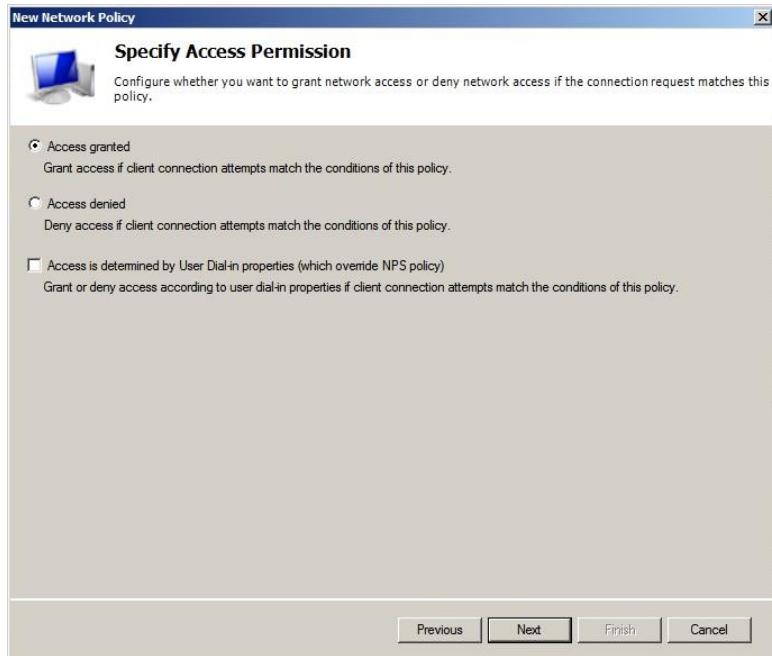


Figure 5. 234: Specify Access Permission

Step 23: Configure the Authentication Method by tick Unencrypted authentication (PAP, SPAP) box and click Next.

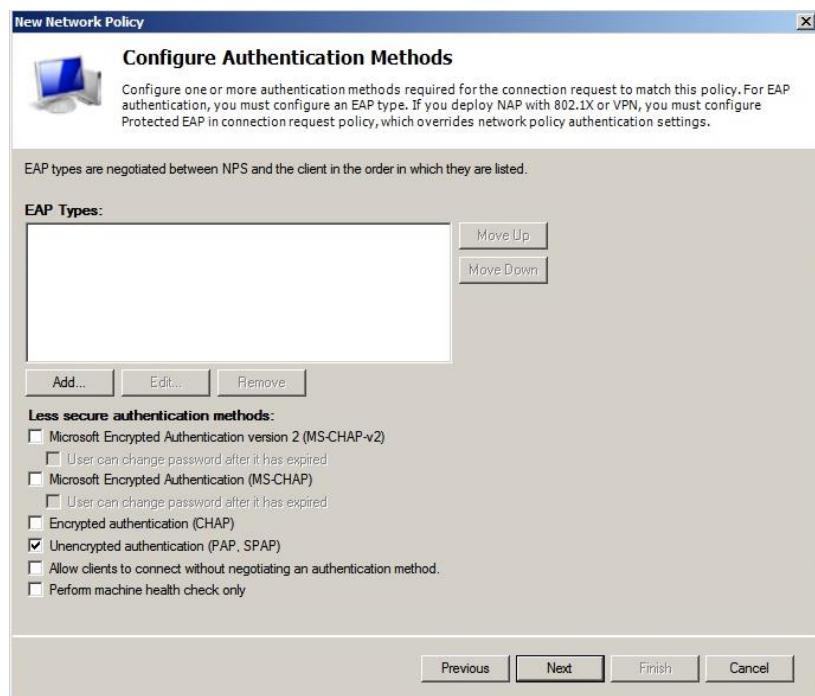


Figure 5. 235: Configure Authentication Methods

Step 24: Click No.



Figure 5. 236: Connection Request Policy

Step 25: For configure constraints, click Next.

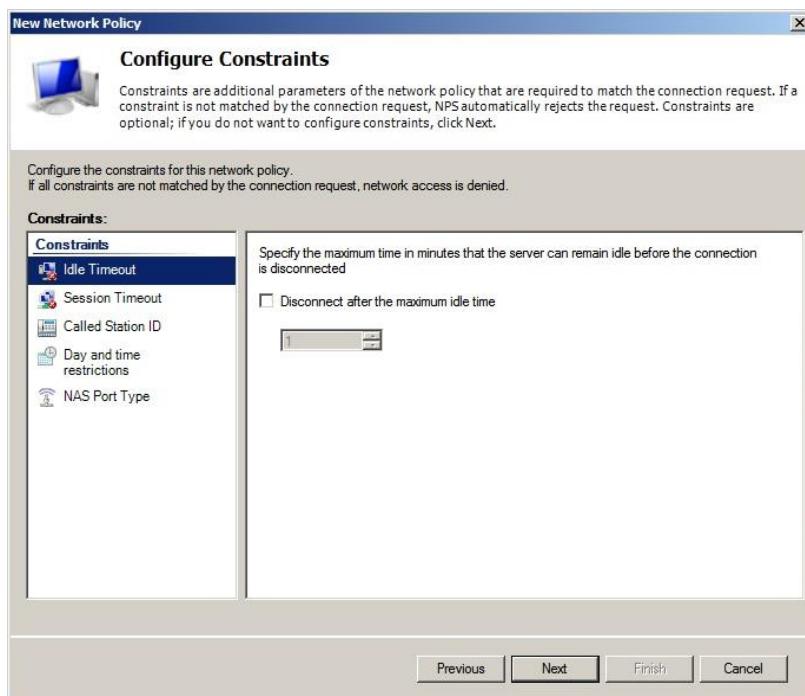


Figure 5. 237: Configure Constraints

Step 26: In Standard tab, remove the Frame-protocol (PPP). Edit the Service-Type by click the Edit button.

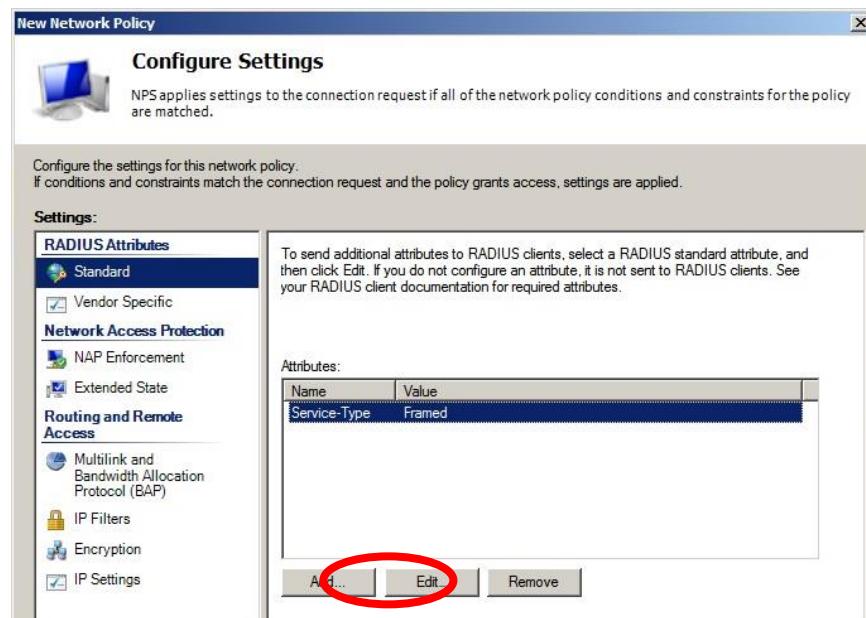


Figure 5. 238: Configure Settings

Step 27: Select the Others and then select Login. Then, click OK.



Figure 5. 239: Attribute Information

Step 28: In the Vendor Specific tab, click Add.

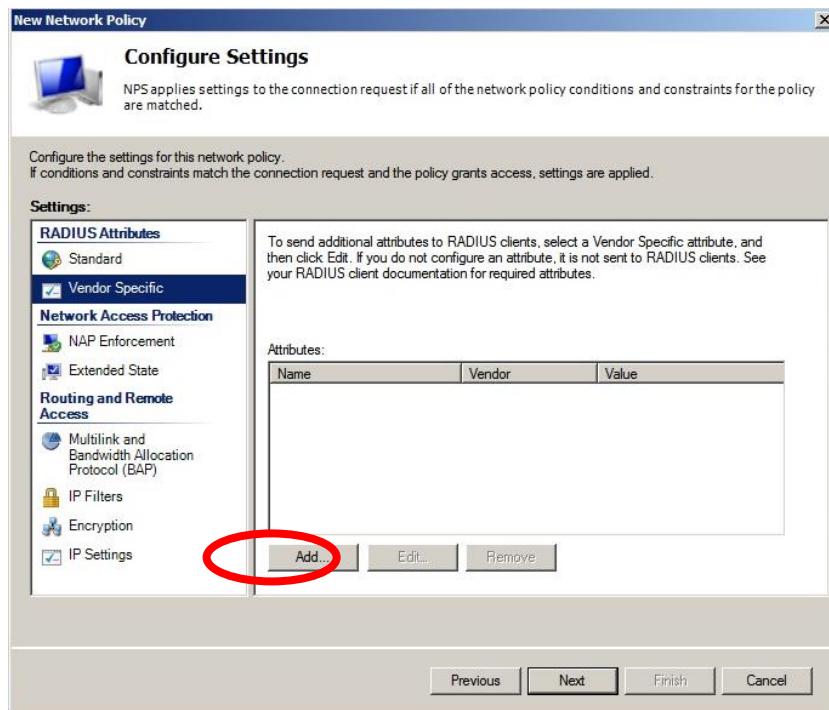


Figure 5. 240: Configure Settings at Vendor Specific

Step 29: In the Vendor site, select Cisco and click Cisco AV-Pair. Then, click Add.

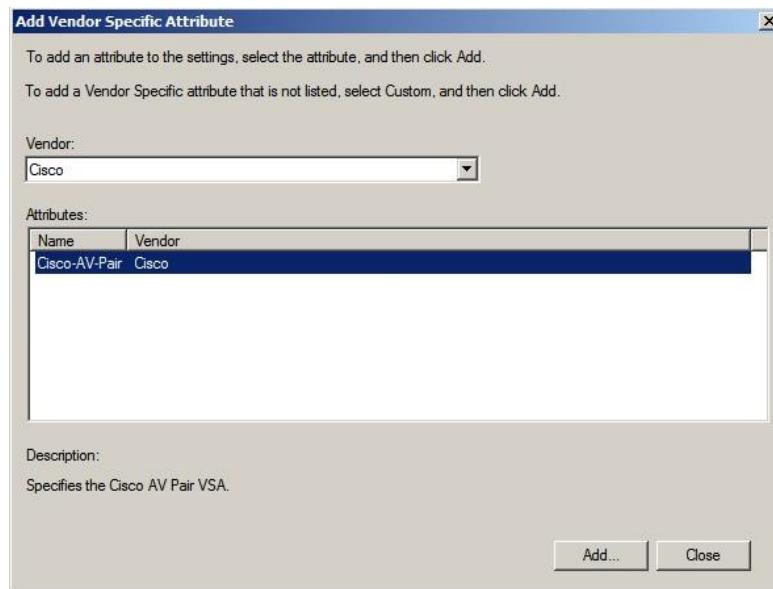


Figure 5. 241: Add Vendor Specific Attribute

Step 30: Click Add.

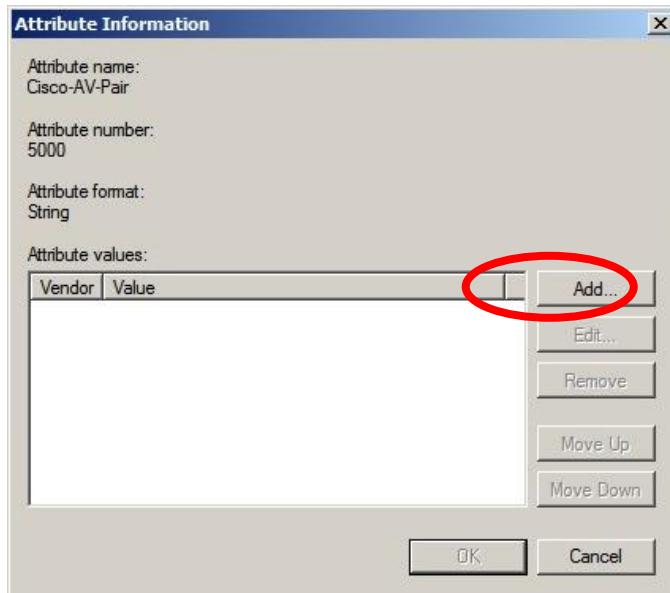


Figure 5. 242: Click Add button

Step 31: Set the privilege level to 1 using command “shell:priv-lvl=1” and click OK.

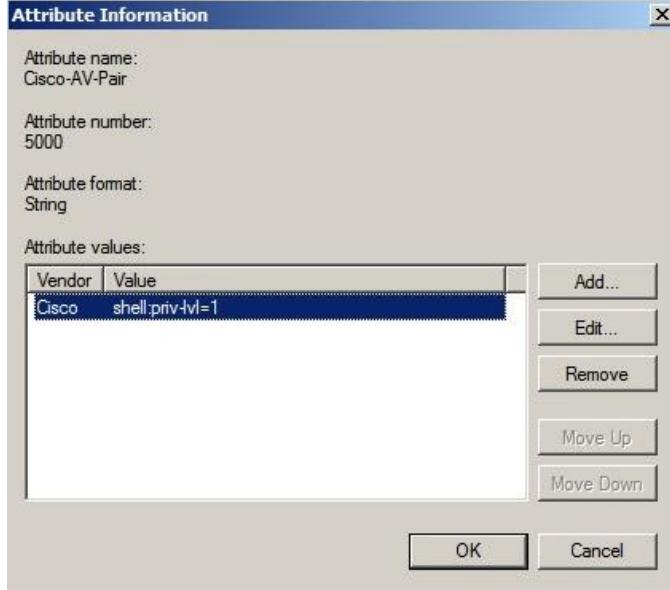


Figure 5. 243: Set User Privilege

Step 32: Click Close.

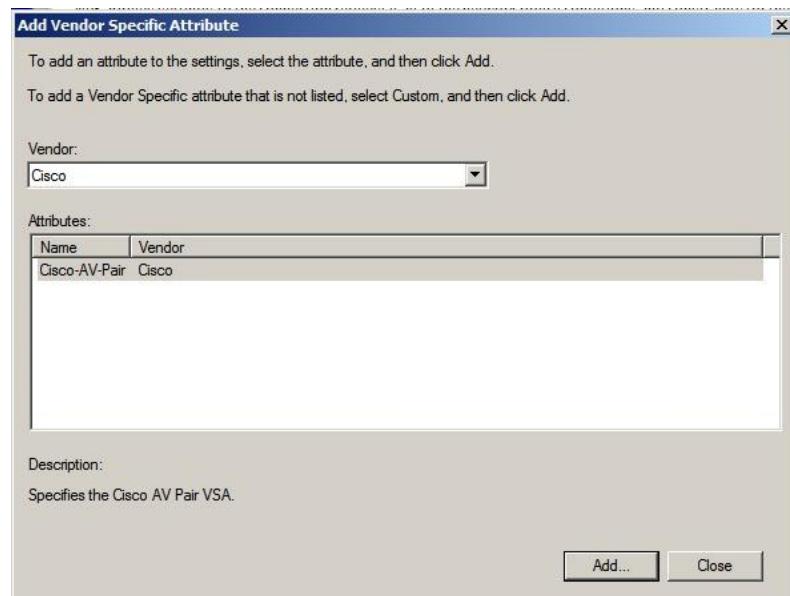


Figure 5. 244: Click Close button

Step 33: The information is shown in this box.

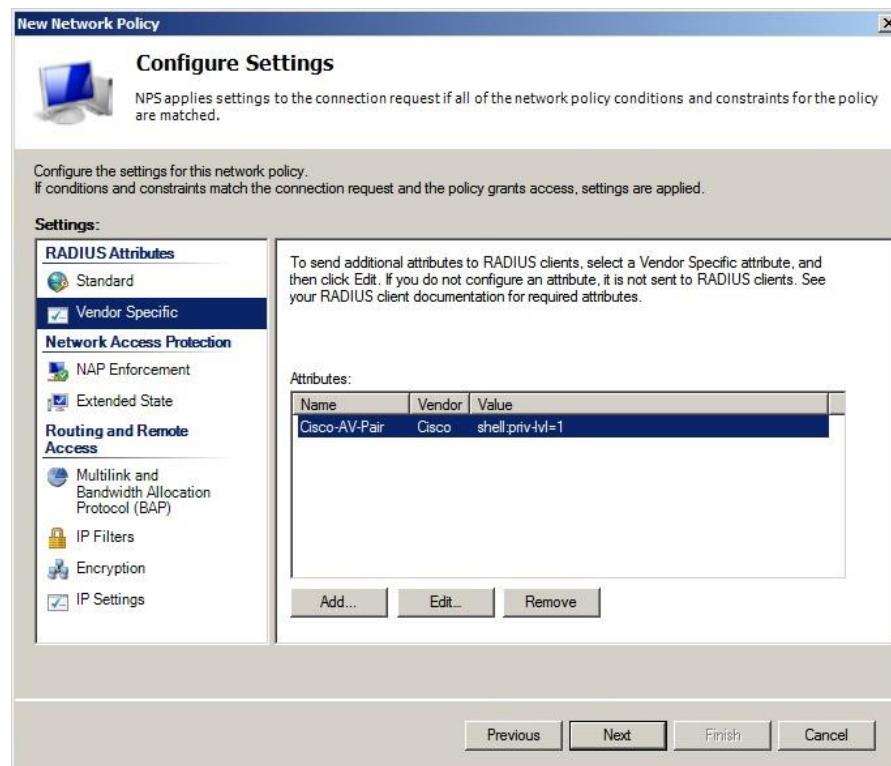


Figure 5. 245: The Information will Display in This Box

Step 34: In the Encryption tab, select all the box and click Next.

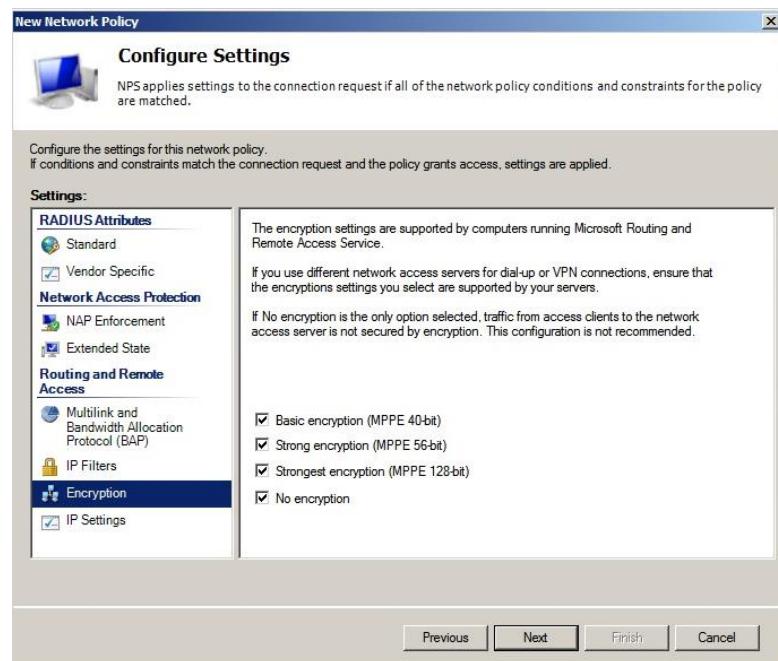


Figure 5. 246: Configure Settings At Encryption

Step 35: Click Finish after confirmed the policy.

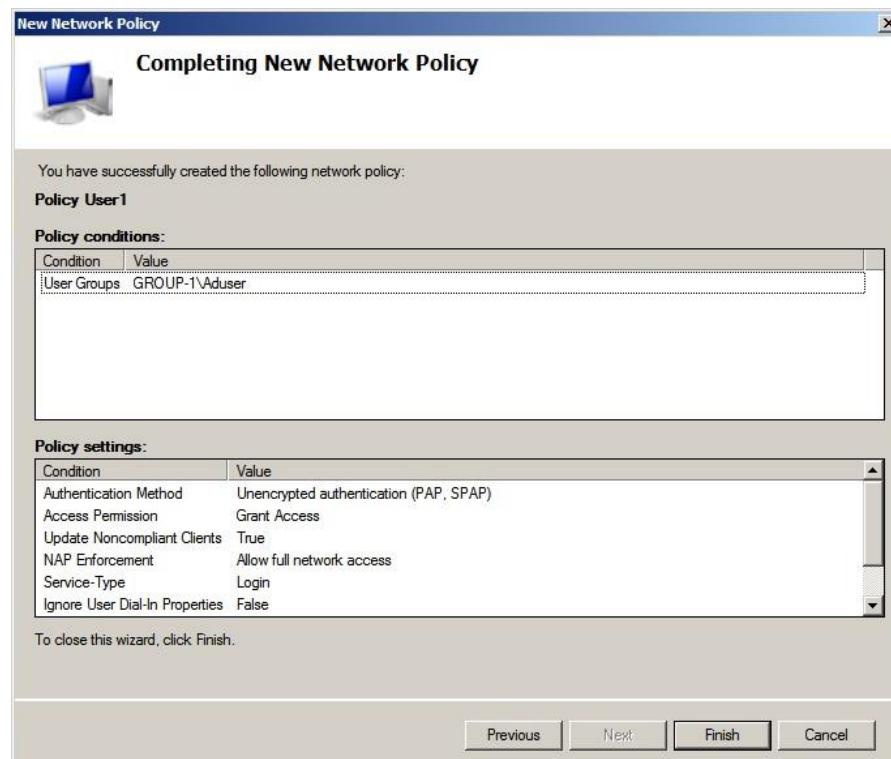


Figure 5. 247: Confirmation policy before Click Finish button

Step 36: The policy is done created.

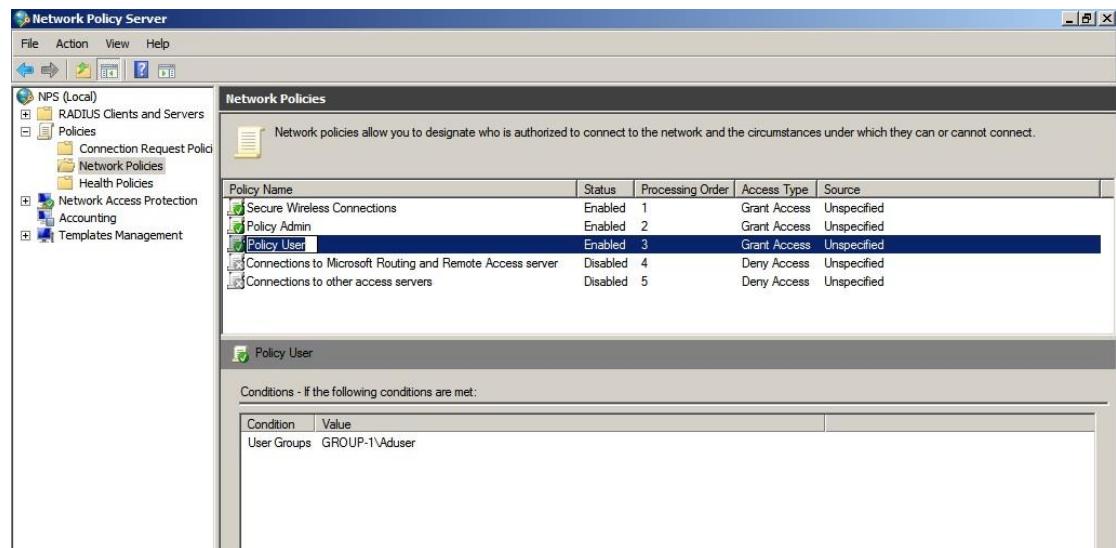


Figure 5. 248: Policy Done Created

### 5.3.18 FIREWALL FOR ROUTER

This ACL is applied in Client VLAN and served for several purposes:

- To prevent client directly access to web server
- To force client to use proxy server
- To prevent client from pinging to other devices
- To prevent client to use FTP service

Step 1: Create an extended access list and add rules into it.

```
ip access-list extended CLIENT
deny  tcp any any eq www
deny  tcp any any eq 443
deny  icmp any any
deny  tcp any any eq ftp-data
deny  tcp any any eq ftp
permit ip any any
```

Figure 5. 249: Extended Access List CLIENT

Step 2: Apply the ACL into interface g0/0.40

```
R1(config)# int g0/0.40
```

```
R1(config-subif)# ip access-group CLIENT in
```

```
R1(config-subif)# ip access-group CLIENT out
```

```
R1(config-subif)# no shut
```

### 5.3.19 REMOTE LOGIN USING SSH

1. SSH configuration for router:

```
# conf t
# ip domain-name group1.com
# crypto key generate rsa general-keys modulus 1024
# line vty 0 5
# transport input ssh
# login aut default
# username group1 privilege 3 secret P@ssw0rd888
# exit
# conf t
# line vty 0 5
# privilege exec all alevel 3 shw running-config
# exit
```

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip domain-name group1.com
R1(config)#crypto key generate rsa general-keys modulus 1024
% You already have RSA keys defined named R1.group1.com.
% They will be replaced.

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable..
*Nov 16 05:12:10.919: %SSH-5-DISABLED: SSH 2.0 has been disabled
[OK] (elapsed time was 2 seconds)

R1(config)#
*Nov 16 05:12:12.487: %SSH-5-ENABLED: SSH 2.0 has been enabled
R1(config)#line vty 0 5
R1(config-line)#transport input ssh
R1(config-line)#login aut default
R1(config-line)#username group1 privilege 3 secret Abc12345
% Invalid Password length - must contain 10 to 25 characters. Password configuration failed
R1(config)#username group1 privilege 3 secret P@ssw0rd888
R1(config)#exit
R1#c
*Nov 16 05:13:18.775: %SYS-5-CONFIG_I: Configured from console by group1 on console
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#line vty 0 5
R1(config-line)#privilege exec all level 3 show running-config
R1(config)#show running-conf view full
^
% Invalid input detected at '^' marker.

R1(config)#exit
```

Figure 5. 250: SSH configuration on Router

## 2. Configuration OpenSSH at Linux Server

Ubuntu Server: \$ sudo apt-get install openssh-server

## 3. Installation of freeSSHd.exe at Windows server

Step 1: Click on Next button to proceed the installation of freesshd.exe



Figure 5. 251: freeSSHd Setup

Step 2: Select destination location to save



Figure 5. 252: Select Destination Location

Step 3: Install SSH as a full installation and click on Next button.

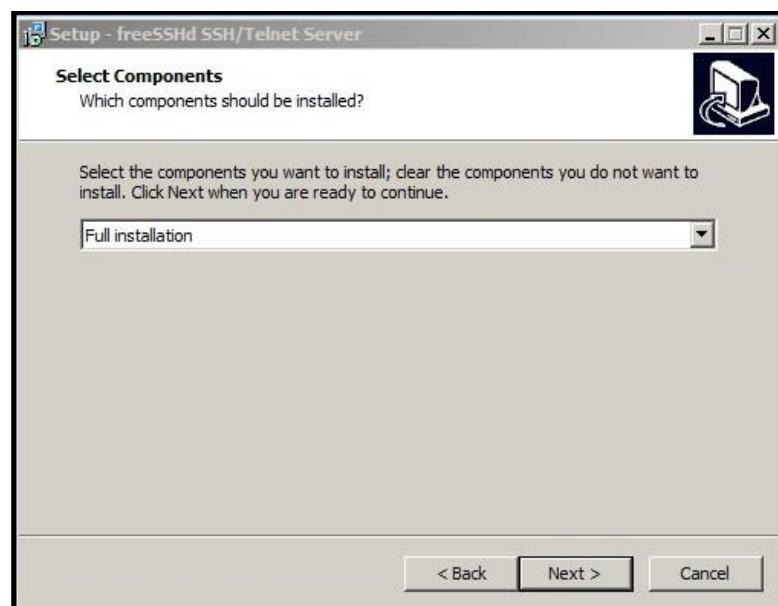


Figure 5. 253: Select Components

Step 4: Select start menu folder

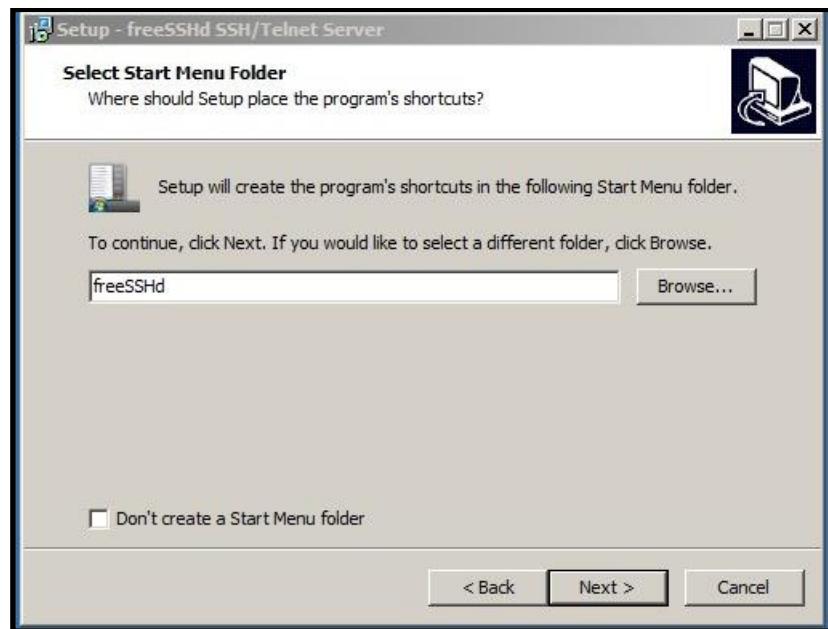


Figure 5. 254: Select Start Menu Folder

#### Step 5: Ready to install



Figure 5. 255: Ready to Install

#### Step 6: Put administrator as login name and password Abc12345

Step 7: Set listen address as Windows IP address 192.168.11.34 and port 22 as SSH port

Step 8: Click password authentication as required and public key as allowed

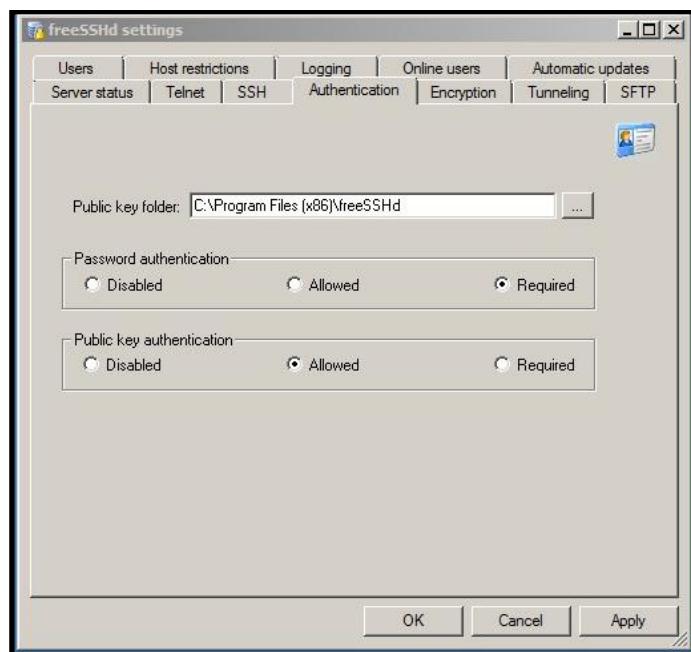


Figure 5. 256: Authentication

Step 9: Click on Encryption and click AES256

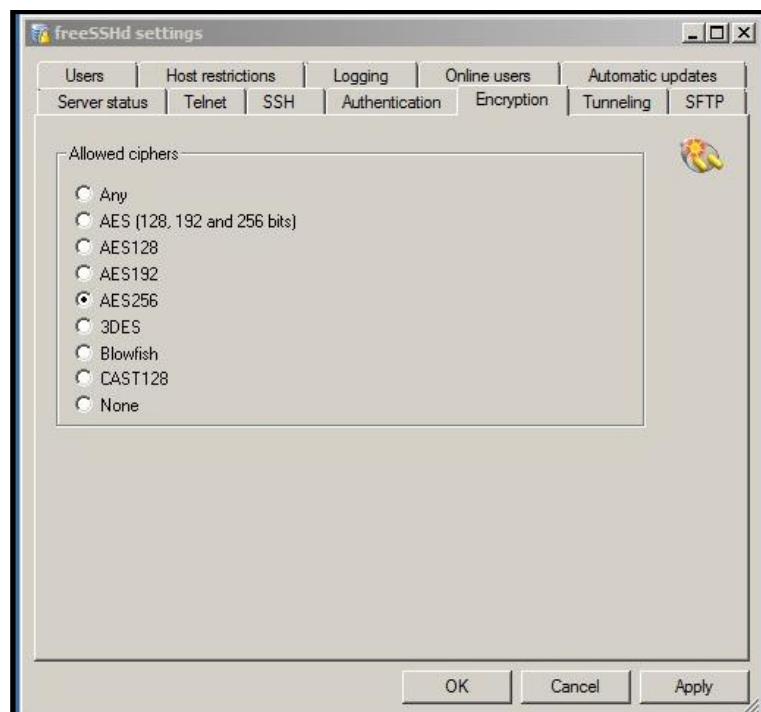


Figure 5. 257: Encryption

Step 10: Go to Tunnelling and allow local and remote port forwarding

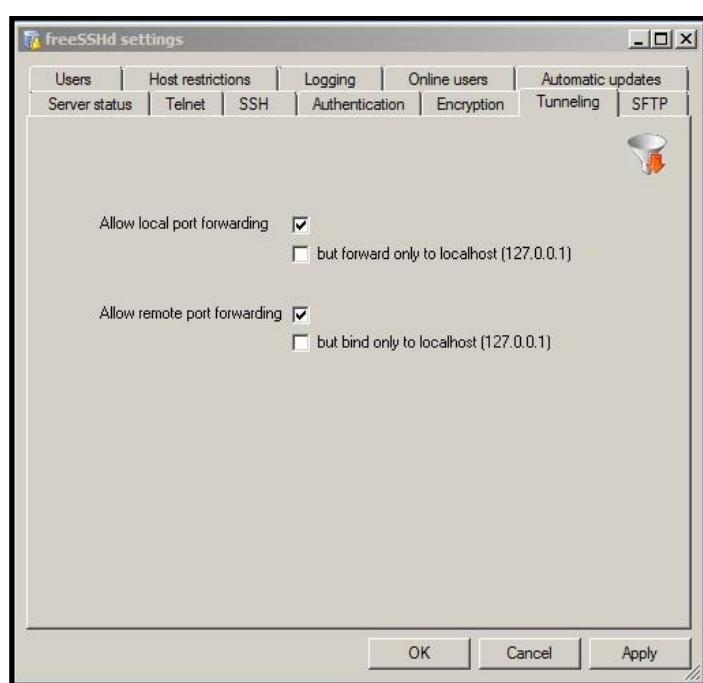


Figure 5. 258: Tunnelling

Step 11: Check server status. Make sure SSH is running.

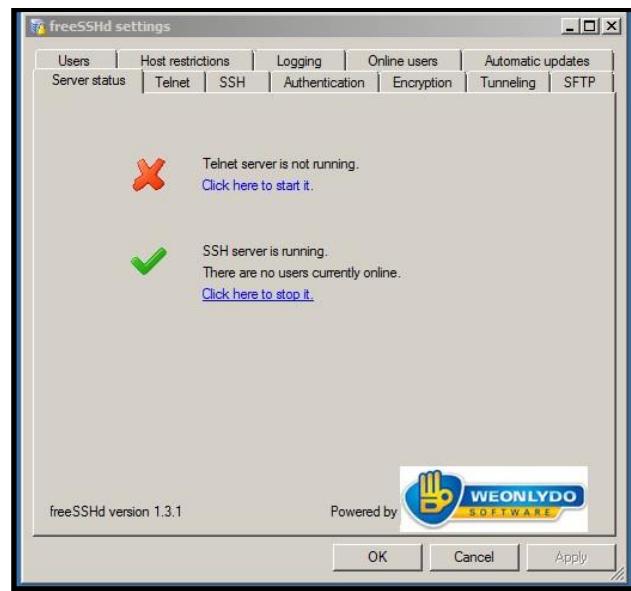


Figure 5. 259: Server Status

### 5.3.20 HARDENING LINUX SERVER

1. Set daily update: Go to Software and Updates. Then click Updates bar. Then make changes to it.

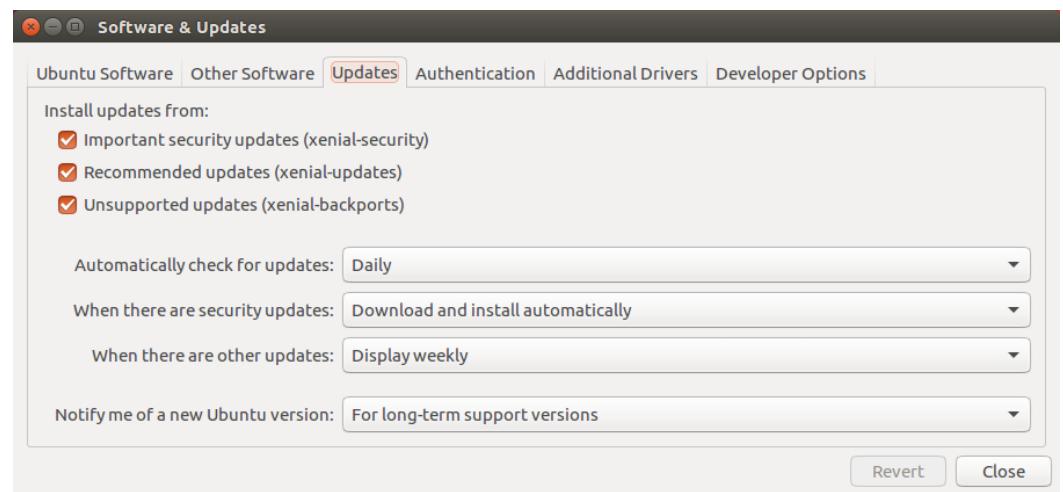


Figure 5. 260: Change Updates

2. Check Ubuntu Software Centre that can used to monitor or check the software updates.

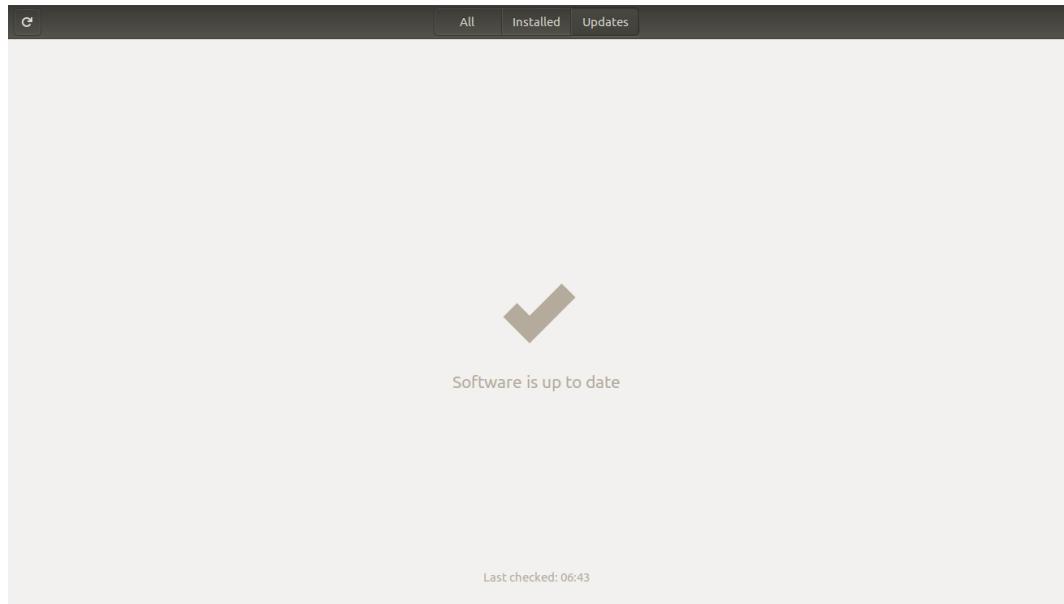


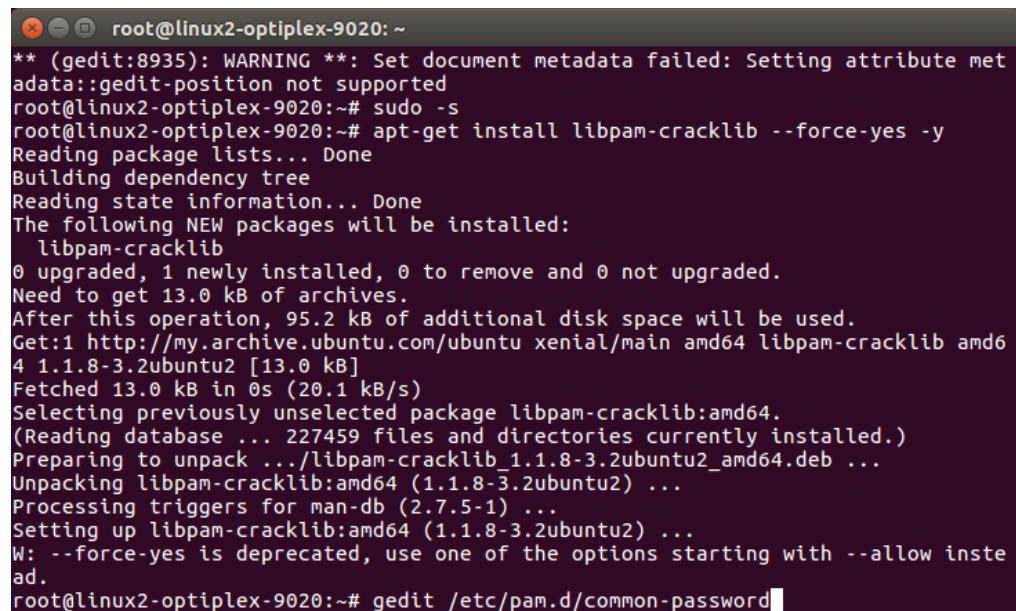
Figure 5. 261: Ubuntu Software Centre

3. Change the minimum and maximum password age.

```
linux2@linux2-optiplex-9020:~$ sudo chage -l linux2
[sudo] password for linux2:
Last password change : Nov 15, 2017
Password expires     : Feb 13, 2018
Password inactive    : Mac 15, 2018
Account expires      : Jan 01, 2018
Minimum number of days between password change : 5
Maximum number of days between password change : 90
Number of days of warning before password expires : 14
linux2@linux2-optiplex-9020:~$ sudo chage -M 180 -I 60 -W 14 linux2
linux2@linux2-optiplex-9020:~$ sudo chage -l linux2
Last password change : Nov 15, 2017
Password expires     : Mei 14, 2018
Password inactive    : Jul 13, 2018
Account expires      : Jan 01, 2018
Minimum number of days between password change : 5
Maximum number of days between password change : 180
Number of days of warning before password expires : 14
linux2@linux2-optiplex-9020:~$
```

Figure 5. 262: Password status

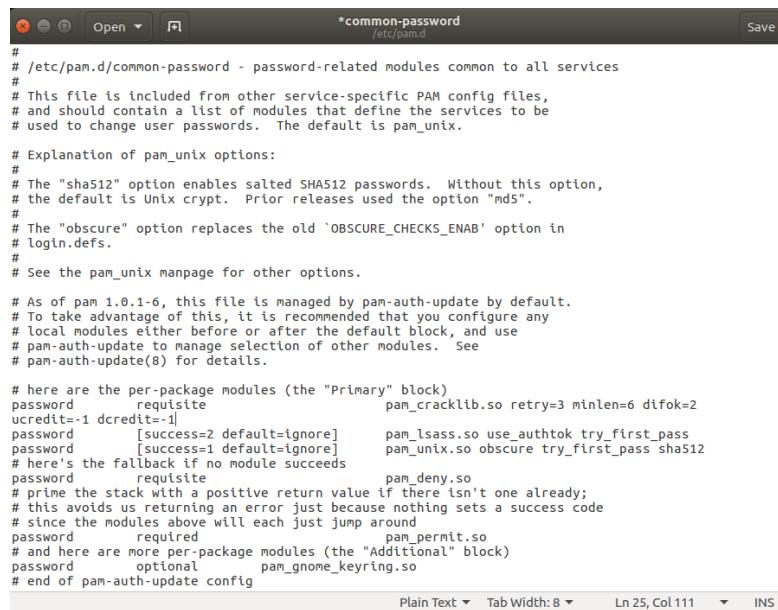
4. Install libpam-cracklib to enable us to set the settings of the password. Then, type “gedit /etc/pam.d/common-password” to open the pam.d/common-password.



```
root@linux2-optiplex-9020: ~
** (gedit:8935): WARNING **: Set document metadata failed: Setting attribute met
adata::gedit-position not supported
root@linux2-optiplex-9020:~# sudo -s
root@linux2-optiplex-9020:~# apt-get install libpam-cracklib --force-yes -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  libpam-cracklib
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 13.0 kB of archives.
After this operation, 95.2 kB of additional disk space will be used.
Get:1 http://my.archive.ubuntu.com/ubuntu xenial/main amd64 libpam-cracklib amd6
4 1.1.8-3.2ubuntu2 [13.0 kB]
Fetched 13.0 kB in 0s (20.1 kB/s)
Selecting previously unselected package libpam-cracklib:amd64.
(Reading database ... 227459 files and directories currently installed.)
Preparing to unpack .../libpam-cracklib_1.1.8-3.2ubuntu2_amd64.deb ...
Unpacking libpam-cracklib:amd64 (1.1.8-3.2ubuntu2) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up libpam-cracklib:amd64 (1.1.8-3.2ubuntu2) ...
W: --force-yes is deprecated, use one of the options starting with --allow inste
ad.
root@linux2-optiplex-9020:~# gedit /etc/pam.d/common-password
```

Figure 5. 263: Installing libpam-cracklib and opening pam.d/common-password file

## 5. Change the characteristics of the password that are safe for the Ubuntu.



```
*common-password
/etc/pam.d
Save

#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.

# Explanation of pam_unix options:
#
# The "sha512" option enables salted SHA512 passwords. Without this option,
# the default is Unix crypt. Prior releases used the option "md5".
#
# The "obscure" option replaces the old 'OBSCURE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password      requisite          pam_cracklib.so retry=3 minlen=6 difok=2
ucred=-1 dcredit=-1]
password      [success=2 default=ignore]    pam_lsass.so use_authtok try_first_pass
password      [success=1 default=ignore]    pam_unix.so obscure try_first_pass sha512
# here's the fallback if no module succeeds
password      requisite          pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password      required           pam_permit.so
# and here are more per-package modules (the "Additional" block)
password      optional           pam_gnome_keyring.so
# end of pam-auth-update config
```

Figure 5. 264: Changing password characteristics

## 6. Scan ports using Nmap by typing command “sudo nmap -v -sT localhost”.

```

linux2@linux2-optiplex-9020: ~
Completed SYN Stealth Scan at 09:55, 1.56s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000070s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
514/tcp   open  shell
631/tcp   open  ipp
1099/tcp  open  rmiregistry
1199/tcp  open  dmidi
3128/tcp  open  squid-http
5432/tcp  open  postgresql

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
  Raw packets sent: 1063 (46.772KB) | Rcvd: 2141 (89.952KB)
linux2@linux2-optiplex-9020:~$ █

```

Figure 5. 265: Port scanned using Nmap

7. Disable 631/tcp port as it is not important. We can do that by typing “echo manual > /etc/init/cups.override”, “sudo service cups stop”.

```

root@linux2-optiplex-9020: ~
root@linux2-optiplex-9020:~$ sudo -i
root@linux2-optiplex-9020:~# echo "manual" > /etc/init/cups.override
root@linux2-optiplex-9020:~# sudo service cups stop
root@linux2-optiplex-9020:~# █

```

Figure 5. 266: Disabling cups

8. The Shellshock vulnerabilities affect Bash, a program that various Unix-based system use to execute command lines and command scripts. It is often installed as the system's default command-line interface.

Test shellshock bash by typing “env VAR='() {;echo hohoho!}' bash –c “echo Bash Test”. Then upgrade the Bash to stop any kind of vulnerability.

```

root@linux2-optiplex-9020:~#
root@linux2-optiplex-9020:~# env VAR = '()' {;echo hohoho!' bash -c "echo Bash Test"
env: 'VAR': No such file or directory
root@linux2-optiplex-9020:~# env VAR ='() {;echo hohoho!' bash -c "echo Bash Test"
env: 'VAR': No such file or directory
root@linux2-optiplex-9020:~# env VAR='()' {;echo hohoho!' bash -c "echo Bash Test"
Bash Test
root@linux2-optiplex-9020:~# sudo apt-get update && sudo apt-get install -only-upgrade bash

```

Figure 5. 267: Testing and upgrading Bash

9. IRQ balance is distributed hardware interrupts across processors on a multiprocessor system in order to increase performance. Turning off IRQ Balance, will optimize the balance between power savings and performance through distribution of hardware interrupts across multiple processors.

Open the /etc/default/irqbalance file by typing “sudo nano /etc/default/irqbalance”.

```

root@linux2-optiplex-9020:~#
root@linux2-optiplex-9020:~# sudo nano /etc/default/irqbalance
root@linux2-optiplex-9020:~#

```

Figure 5. 268: Opening irq balance

10. Change the ENABLED to “0”.

```

root@linux2-optiplex-9020:~#
GNU nano 2.5.3           File: /etc/default/irqbalance

#Configuration for the irqbalance daemon

#Should irqbalance be enabled?
ENABLED="0"
#Balance the IRQs only once?
ONEShot="0"

```

Figure 5. 269: Changing Enabled

11. Disable the Bluetooth service as we not going to use it. First type “sudo nano /etc/rc.local”

```
root@linux2-optiplex-9020: ~
root@linux2-optiplex-9020:~# sudo nano /etc/rc.local
root@linux2-optiplex-9020:~#
```

Figure 5. 270: Opening rc.local file

12. Add the line “rfkill block bluetooth” before “exit 0”.

```
root@linux2-optiplex-9020: ~
GNU nano 2.5.3                               File: /etc/rc.local

#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

rfkill block bluetooth
exit 0
```

[ Read 15 lines ]

**^G** Get Help **^O** Write Out **^W** Where Is **^K** Cut Text **^J** Justify **^C** Cur Pos  
**^X** Exit **^R** Read File **^V** Replace **^U** Uncut Text **^T** To Linter **^A** Go To Line

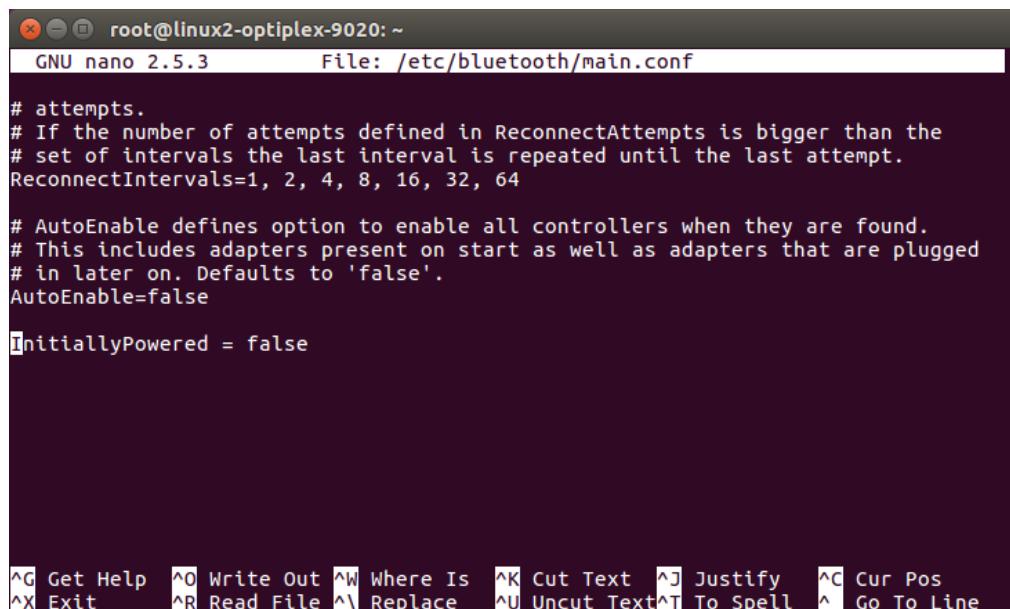
Figure 5. 271: Disabling Bluetooth

13. Open the file Bluetooth/main.conf by typing “sudo nano /etc/bluetooth/main.conf”.

```
root@linux2-optiplex-9020: ~
root@linux2-optiplex-9020:~# sudo nano /etc/rc.local
root@linux2-optiplex-9020:~# sudo nano /etc/rc.local
root@linux2-optiplex-9020:~# sudo nano /etc/bluetooth/main.conf
root@linux2-optiplex-9020:~#
```

Figure 5. 272: Opening bluetooth/main.conf

14. Set the “InitiallyPowered = false”.



```
root@linux2-optiplex-9020:~#
GNU nano 2.5.3           File: /etc/bluetooth/main.conf

# attempts.
# If the number of attempts defined in ReconnectAttempts is bigger than the
# set of intervals the last interval is repeated until the last attempt.
ReconnectIntervals=1, 2, 4, 8, 16, 32, 64

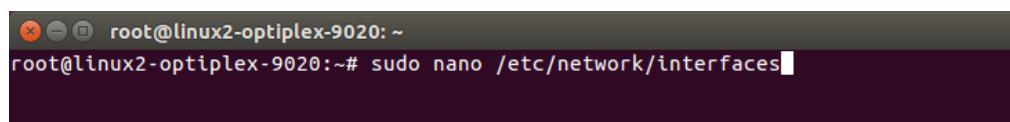
# AutoEnable defines option to enable all controllers when they are found.
# This includes adapters present on start as well as adapters that are plugged
# in later on. Defaults to 'false'.
AutoEnable=false

InitiallyPowered = false

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^Y Replace   ^U Uncut Text^T To Spell  ^L Go To Line
```

Figure 5. 273: Setting Initially Powered

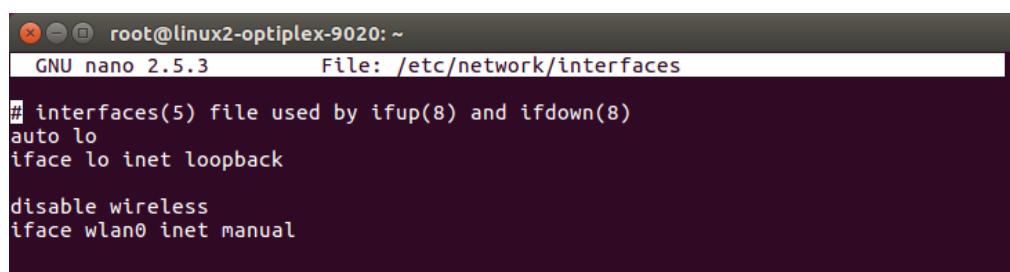
15. Then, we disabled wireless as we not going to use them. First we do that by opening network/interfaces file.



```
root@linux2-optiplex-9020:~#
root@linux2-optiplex-9020:~# sudo nano /etc/network/interfaces
```

Figure 5. 274: Opening network/interfaces file

16. Then, add line “disable wireless” and “iface wlan0 inet manual” at the bottom of the file. Then, restart the network manager.



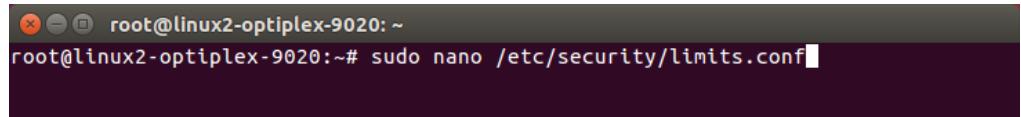
```
root@linux2-optiplex-9020:~#
GNU nano 2.5.3           File: /etc/network/interfaces

# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

disable wireless
iface wlan0 inet manual
```

Figure 5. 275: File Disabling wireless

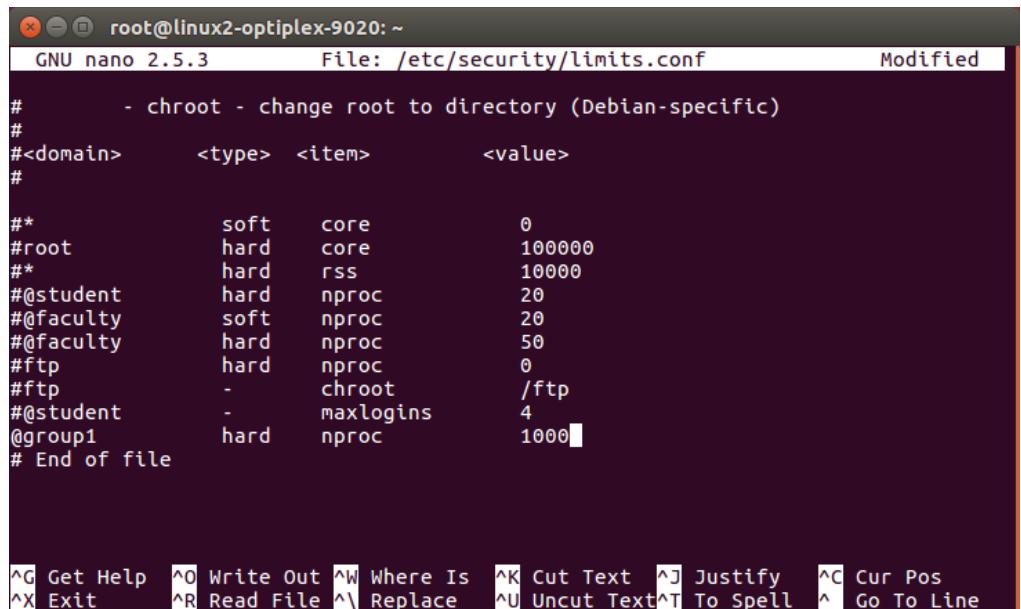
17. Set the security limits for the user in the Ubuntu. First, open the security/limits.conf file.



```
root@linux2-optiplex-9020:~# sudo nano /etc/security/limits.conf
```

Figure 5. 276: Opening security/limits.conf

18. Set the security limits for the user.



```
#      - chroot - change root to directory (Debian-specific)
#
#<domain>      <type>  <item>          <value>
#
#*          soft   core        0
#root      hard   core    100000
#*          hard   rss       10000
#@student    hard   nproc      20
#@faculty    soft   nproc      20
#@faculty    hard   nproc      50
#ftp        hard   nproc       0
#ftp        -      chroot    /ftp
#@student    -      maxlogins   4
@group1     hard   nproc    1000
# End of file

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text^T To Spell  ^L Go To Line
```

Figure 5. 277: Setting security limits

19. After that, we delete the mysql service as we do not use them.

```
linux1@linux1-hp-xw6600-workstation:~$ nmap -p- localhost
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 139/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 9090/tcp on 127.0.0.1
Discovered open port 3128/tcp on 127.0.0.1
Completed Connect Scan at 04:51, 0.03s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00018s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3128/tcp  open  squid-http
3306/tcp  open  mysql
9090/tcp  open  zeus-admin

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
linux1@linux1-hp-xw6600-workstation:~$
```

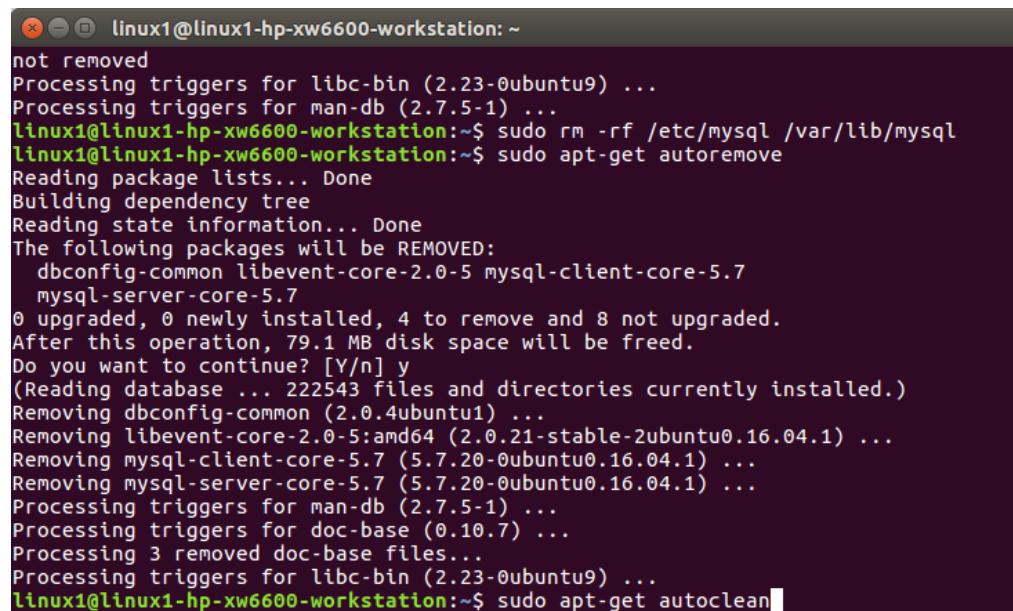
Figure 5. 278: mysql port is open

20. Clean the msyql file by typing “`sudo apt-get purge mysql-server mysql-client mysql-common mysql-server-core-5.5 mysql-client-core-5.5`”.

```
linux1@linux1-hp-xw6600-workstation:~$ sudo apt-get purge mysql-server mysql-client mysql-common mysql-server-core-5.5 mysql-client-core-5.5
[sudo] password for linux1:
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package 'mysql-server-core-5.5' is not installed, so not removed
Package 'mysql-client-core-5.5' is not installed, so not removed
Package 'mysql-client' is not installed, so not removed
The following packages were automatically installed and are no longer required:
  dbconfig-common libevent-core-2.0-5 mysql-client-core-5.7
  mysql-server-core-5.7
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  libmysqlclient20* mysql-client-5.7* mysql-common* mysql-server*
  mysql-server-5.7* rsyslog-mysql*
0 upgraded, 0 newly installed, 6 to remove and 8 not upgraded.
After this operation, 87.1 MB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 222697 files and directories currently installed.)
Removing rsyslog-mysql (8.16.0-1ubuntu3) ...
Determining localhost credentials from /etc/mysql/debian.cnf: succeeded.
Purging configuration files for rsyslog-mysql (8.16.0-1ubuntu3) ...
```

Figure 5. 279: Deleting package file in mysql

21. Then, type “`sudo rm -rf /etc/mysql /var/lib/mysql`”, “`sudo apt-get autoremove`” and “`sudo apt-get autoclean`” to remove any leftover file in the package.



```

linux1@linux1-hp-xw6600-workstation: ~
not removed
Processing triggers for libc-bin (2.23-0ubuntu9) ...
Processing triggers for man-db (2.7.5-1) ...
linux1@linux1-hp-xw6600-workstation:~$ sudo rm -rf /etc/mysql /var/lib/mysql
linux1@linux1-hp-xw6600-workstation:~$ sudo apt-get autoremove
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  dbconfig-common libevent-core-2.0-5 mysql-client-core-5.7
  mysql-server-core-5.7
0 upgraded, 0 newly installed, 4 to remove and 8 not upgraded.
After this operation, 79.1 MB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 222543 files and directories currently installed.)
Removing dbconfig-common (2.0.4ubuntu1) ...
Removing libevent-core-2.0-5:amd64 (2.0.21-stable-2ubuntu0.16.04.1) ...
Removing mysql-client-core-5.7 (5.7.20-0ubuntu0.16.04.1) ...
Removing mysql-server-core-5.7 (5.7.20-0ubuntu0.16.04.1) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for doc-base (0.10.7) ...
Processing 3 removed doc-base files...
Processing triggers for libc-bin (2.23-0ubuntu9) ...
linux1@linux1-hp-xw6600-workstation:~$ sudo apt-get autoclean

```

Figure 5. 280: Remove leftover file in the mysql package file

### 5.3.21 HARDENING WINDOWS SERVER

1. Install Nmap in the Windows Server.
2. Open Security Configuration Wizard.

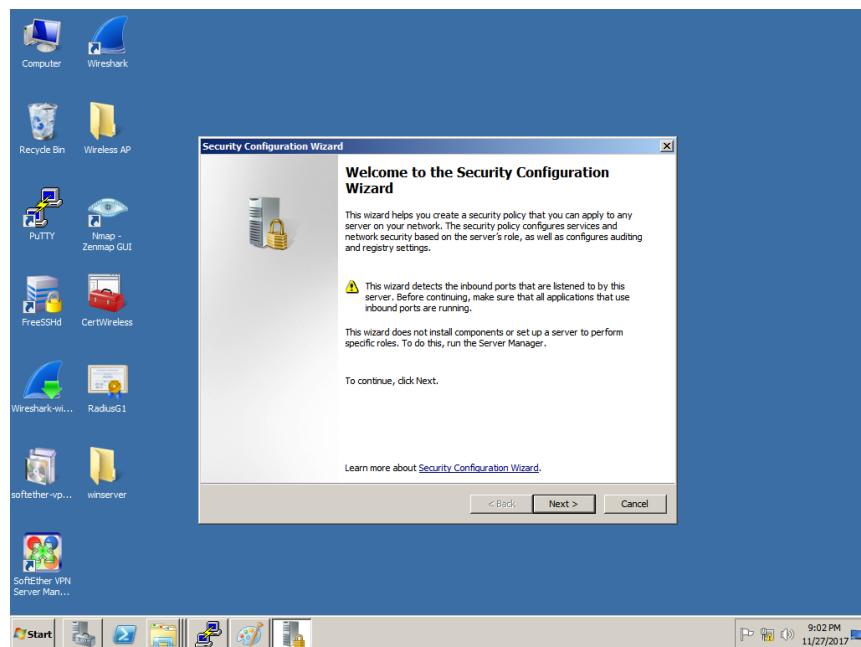


Figure 5. 281: Security Configuration Wizard

3. Create a new security policy.

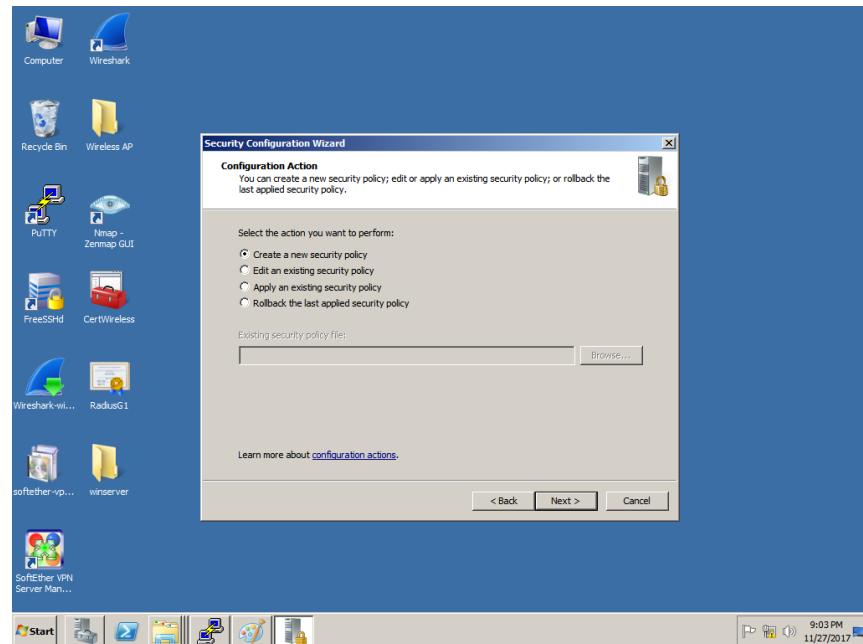


Figure 5. 282: Creating new security policy

4. Name the server.

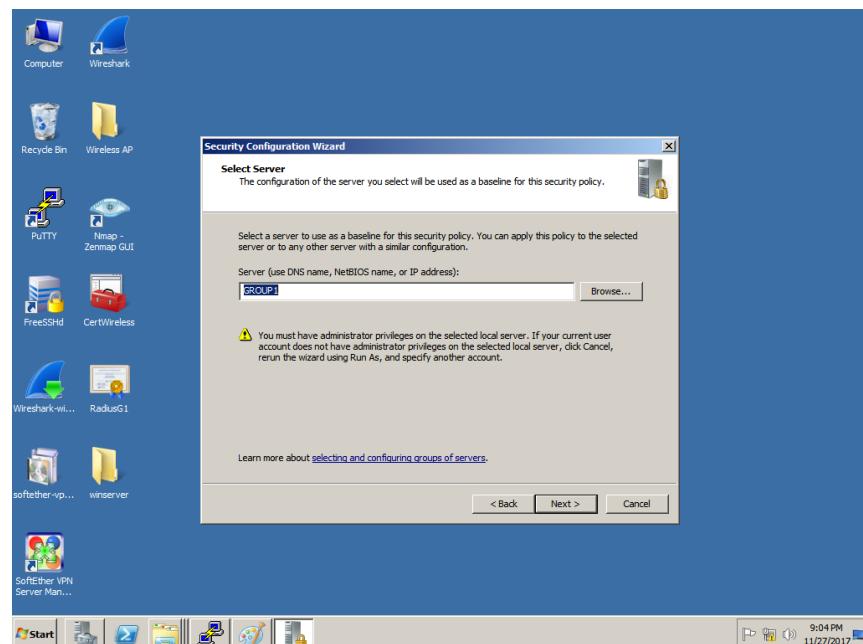


Figure 5. 283: Naming server

5. Click next at the Processing Security Configuration Database after the processing completed.

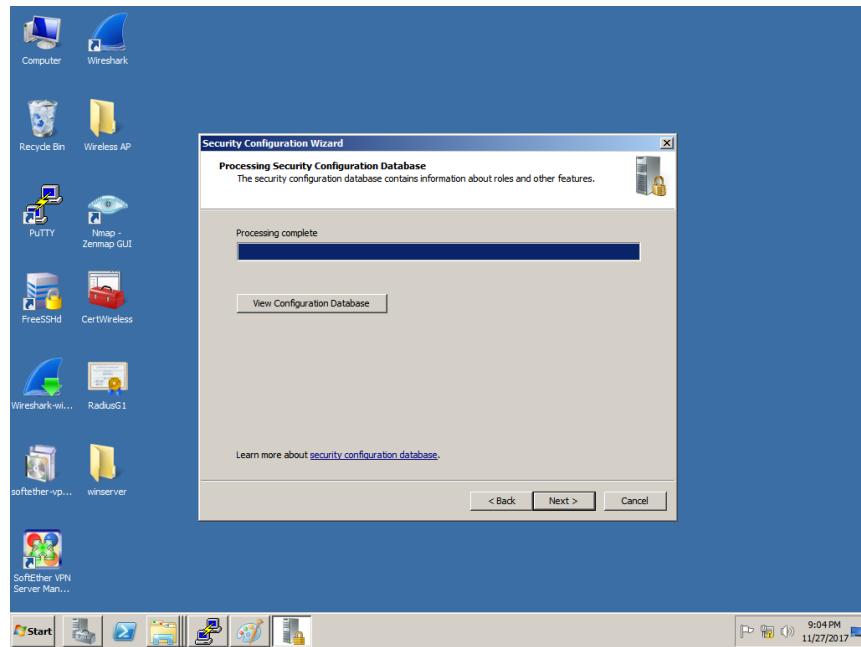


Figure 5. 284: Processing Security Configuration Database

6. Click next at the Role-Based Service Configuration.

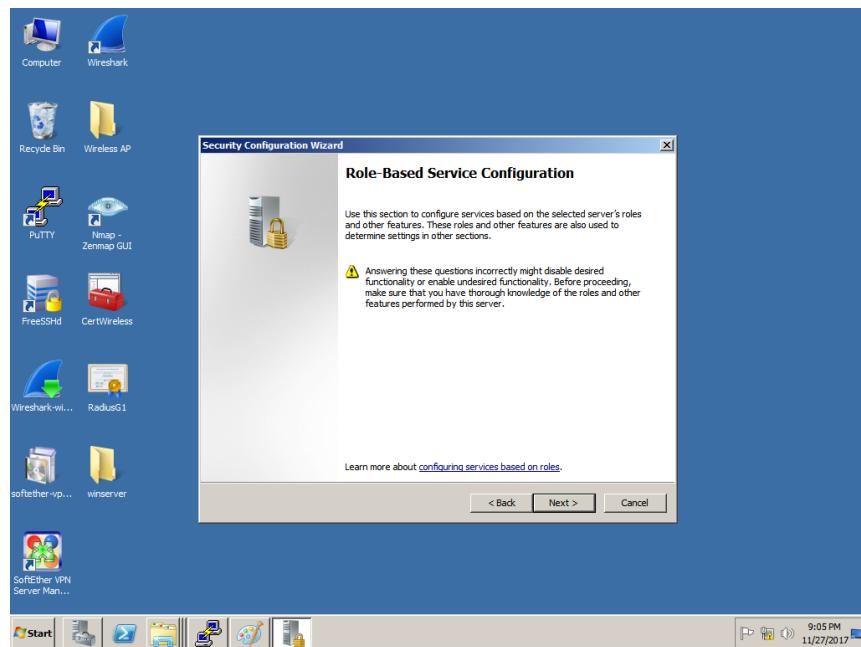


Figure 5. 285: Role-Based Service Configuration

## 7. Select the server roles.

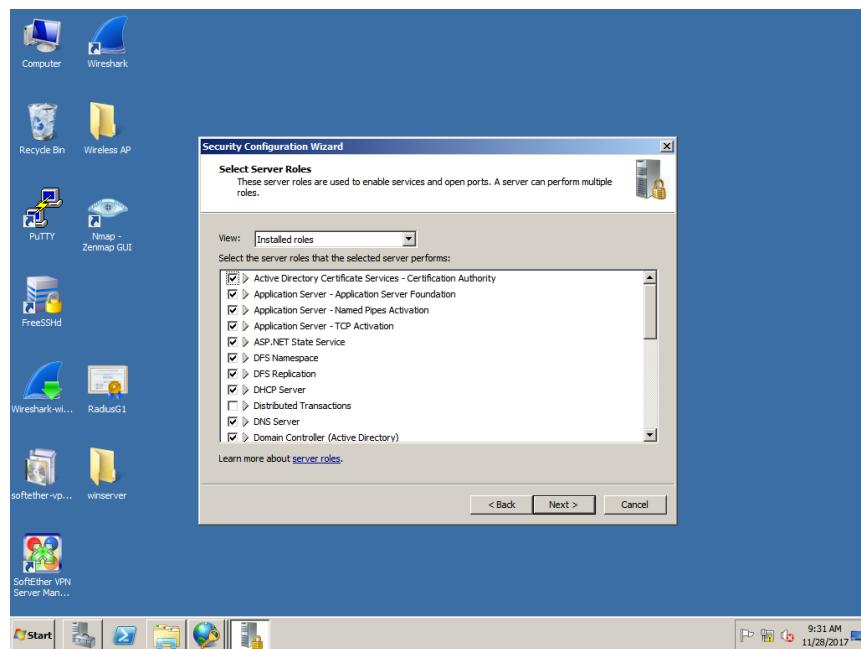


Figure 5. 286: Selecting Server Roles (1)

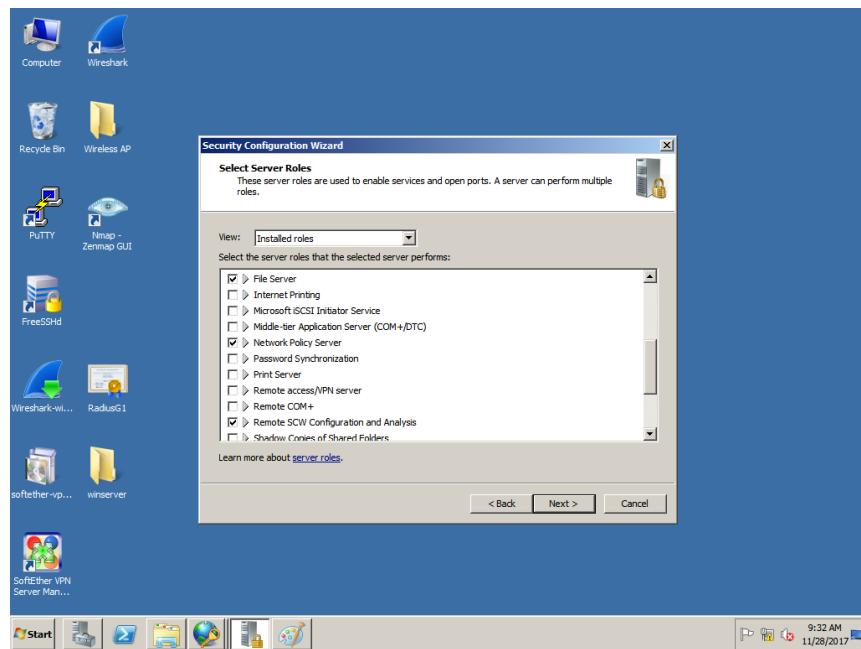


Figure 5. 287: Selecting Server Roles (2)

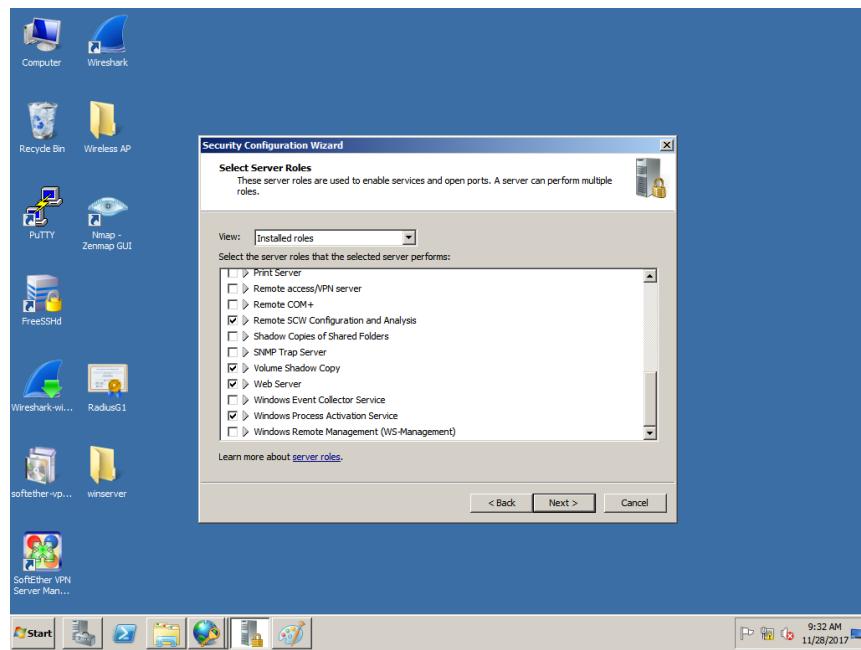


Figure 5. 288: Selecting Server Roles (3)

### 8. Select the client features.

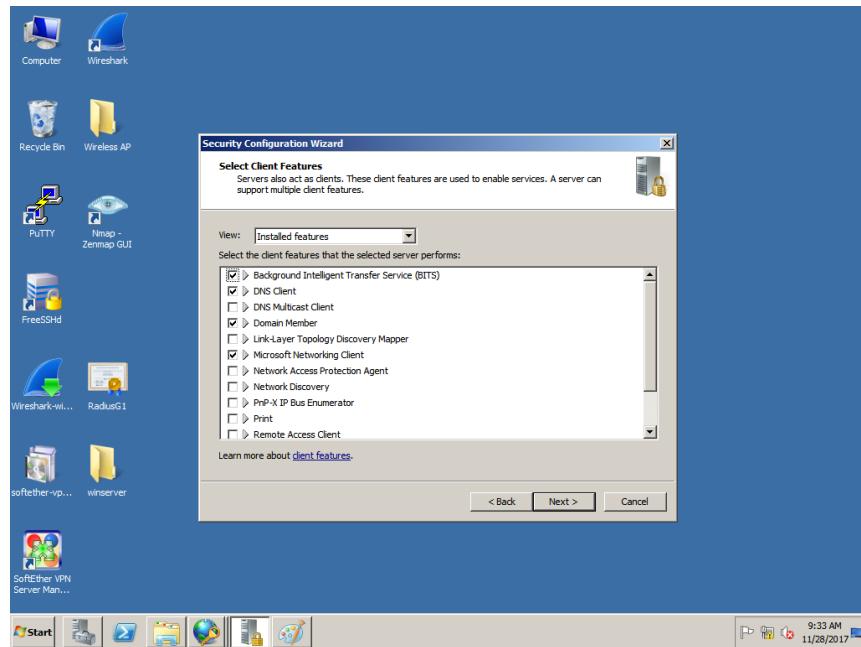


Figure 5. 289: Selecting Client Features (1)

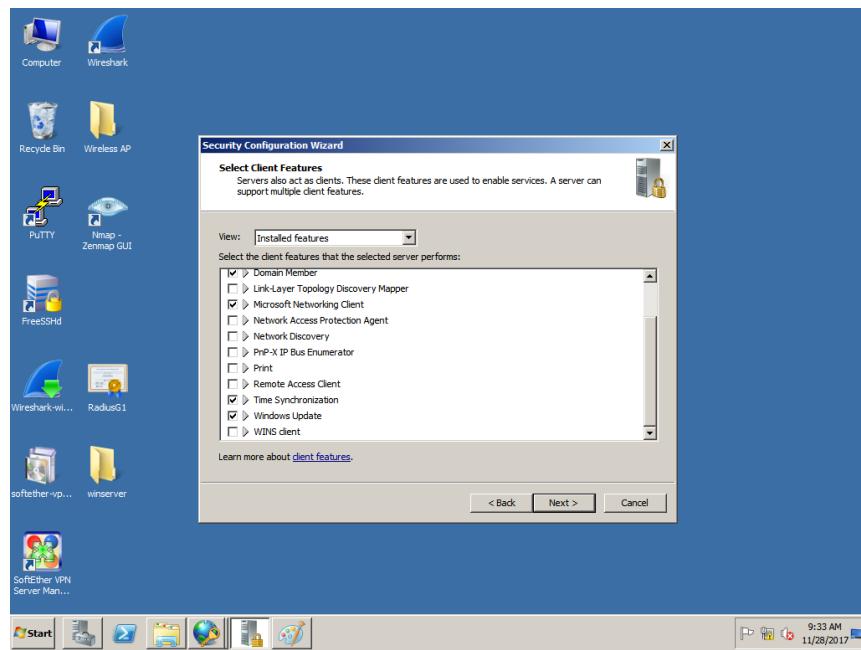


Figure 5. 290: Selecting Client Features (2)

## 9. Select the Administration and Other Options.

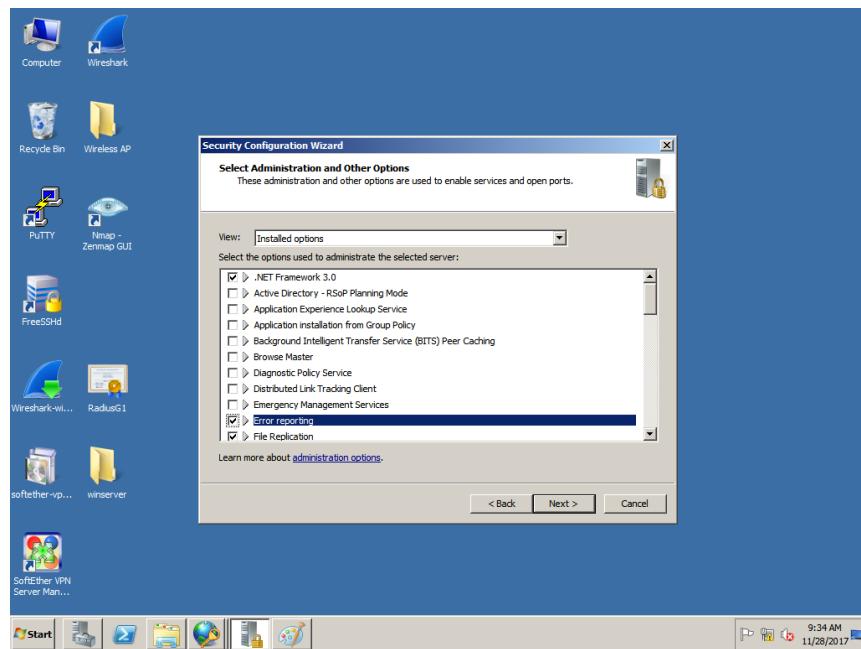


Figure 5. 291: Selecting Administration and Other Options (1)

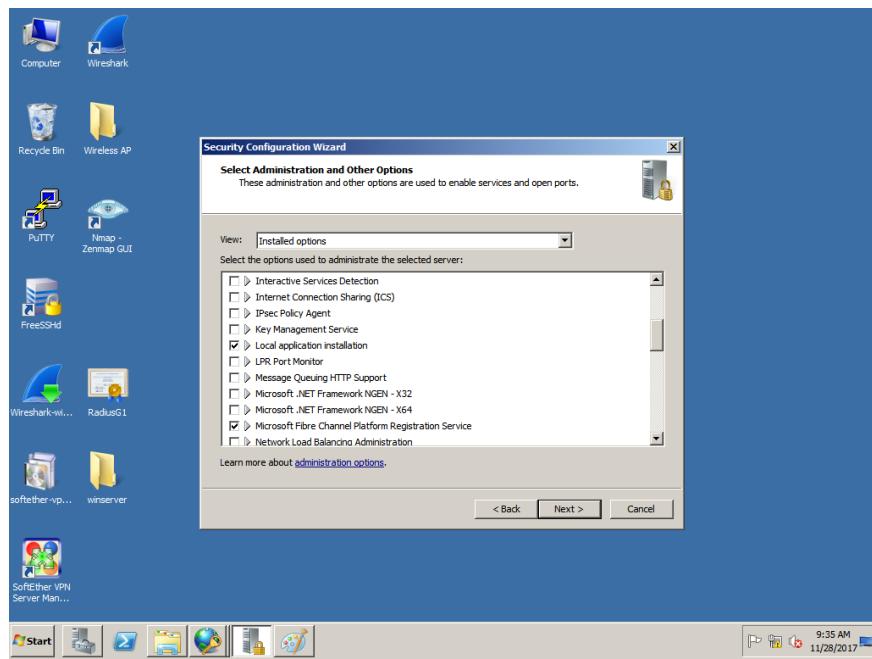


Figure 5. 292: Selecting Administration and Other Options (2)

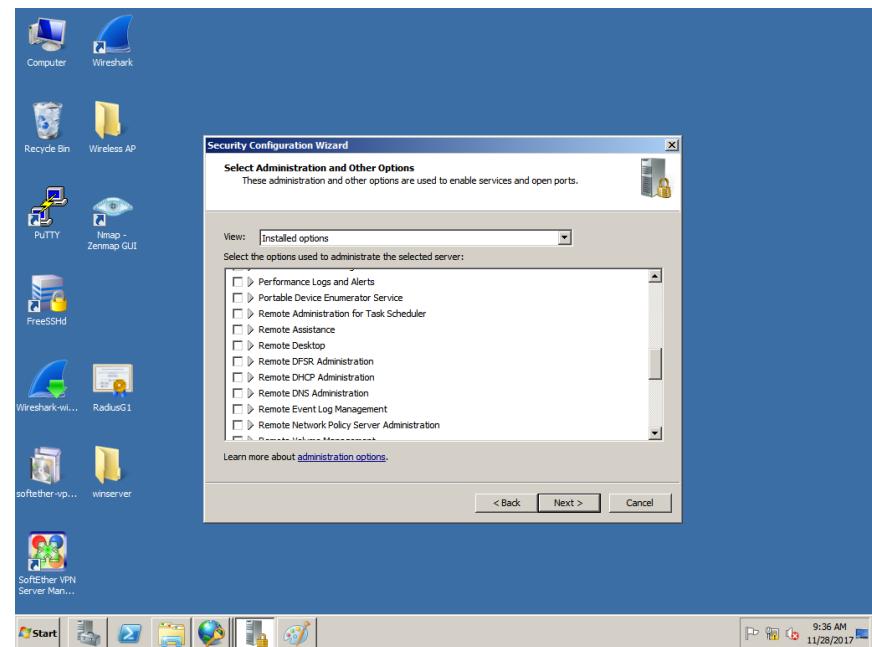


Figure 5. 293: Selecting Administration and Other Options(3)

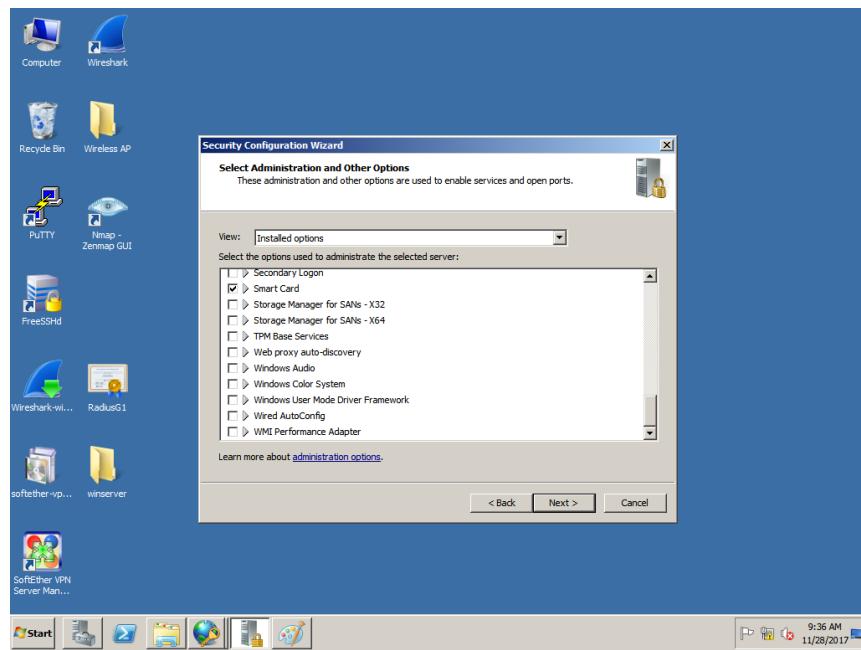


Figure 5. 294: Selecting Administration and Other Options(4)

#### 10. Select the Additional Services for the server.

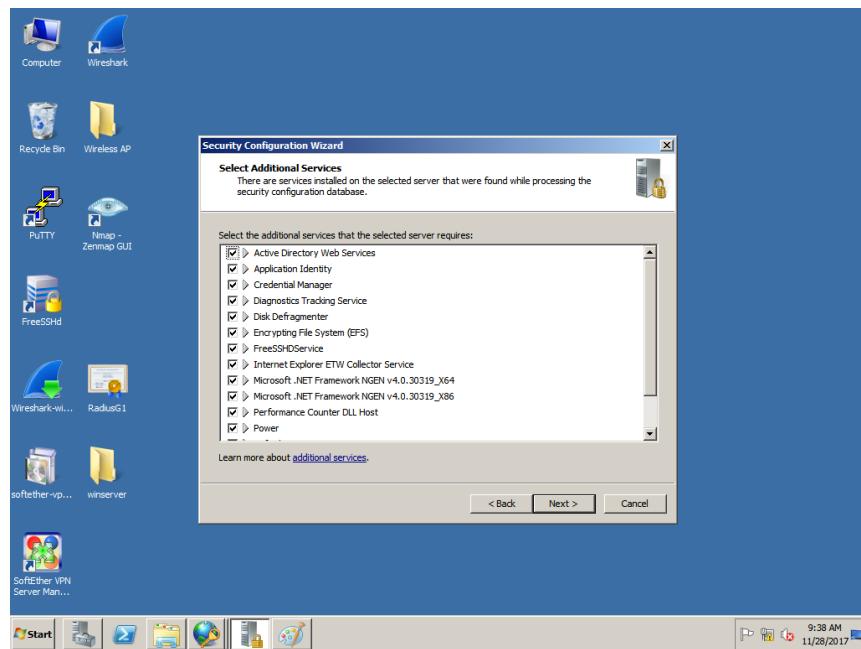


Figure 5. 295: Selecting Additional Services (1)

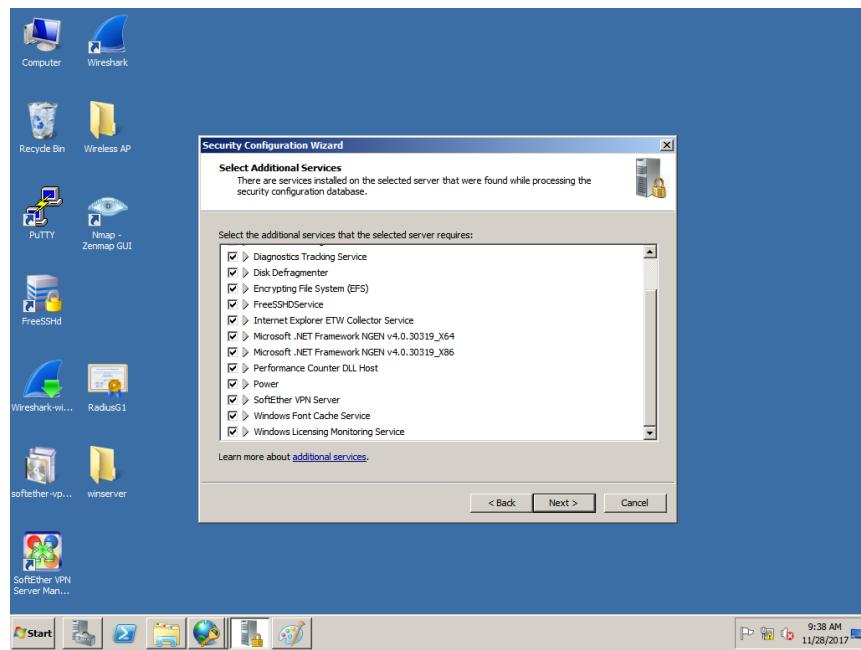


Figure 5. 296: Selecting Additional Services (2)

11. Select “Do not change the startup mode of the service” on Handling Unspecified Service.

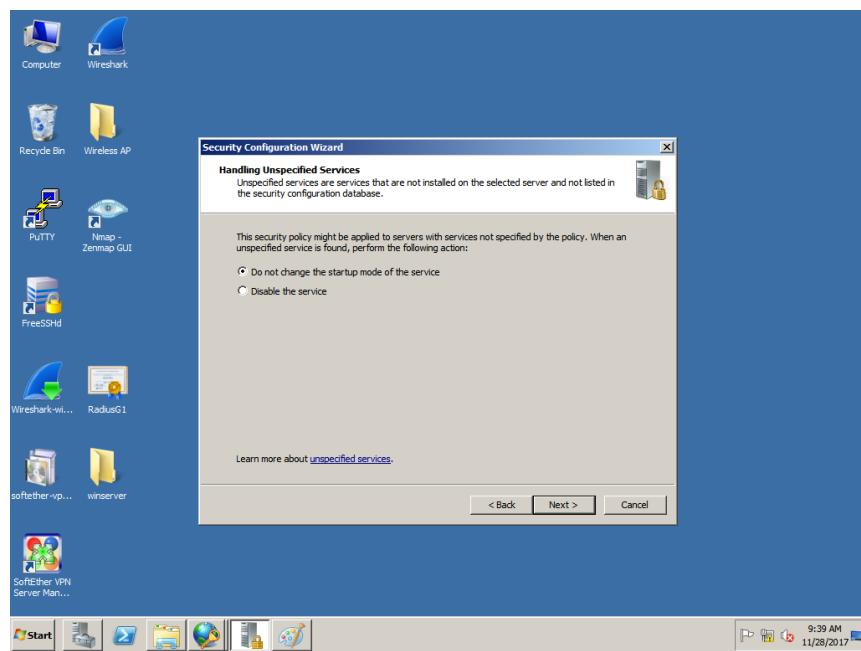


Figure 5. 297: Handling Unspecified Service

12. Confirm the Service Changes.

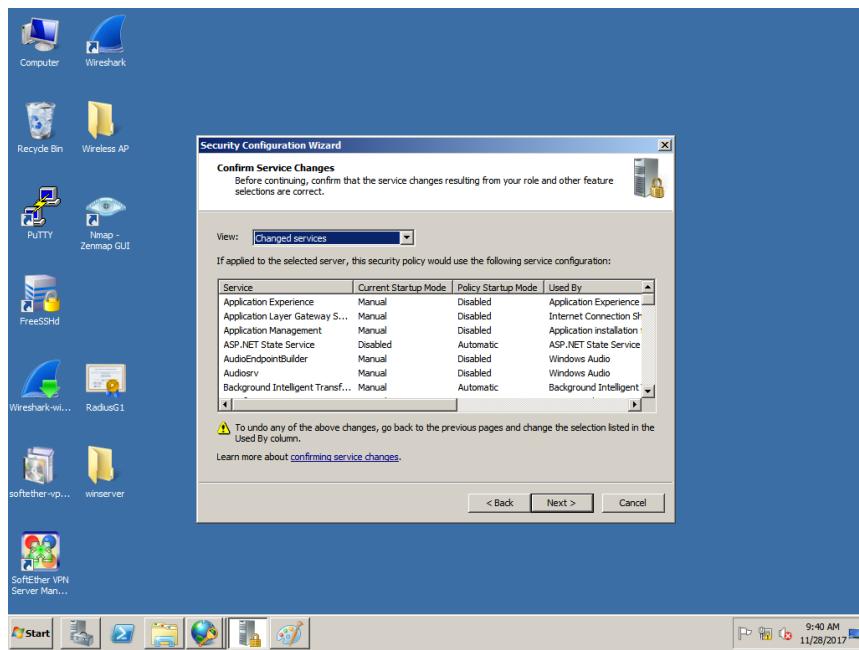


Figure 5. 298: Confirming Service Changes

13. Click next at the Network Security.

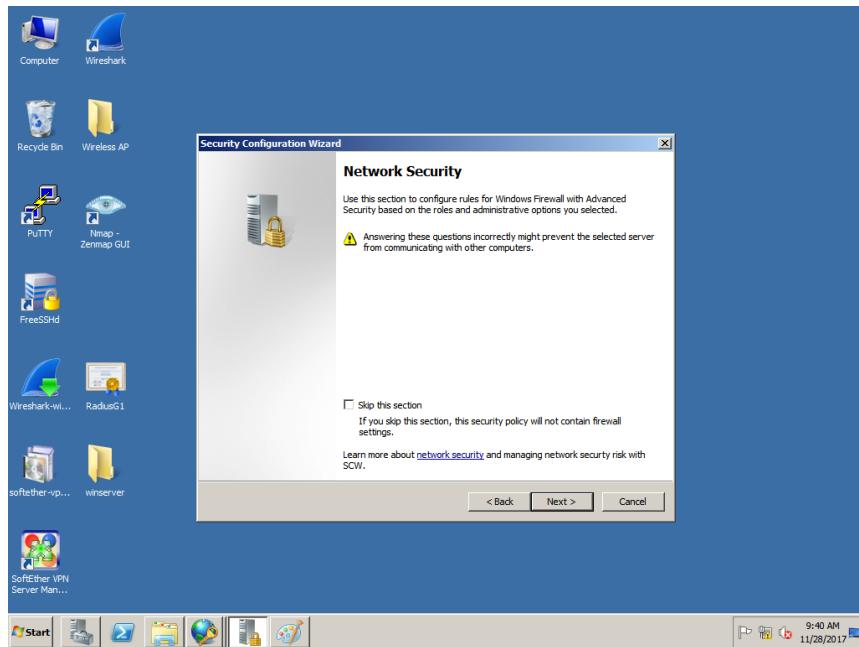


Figure 5. 299: Network Security

14. Select the network security rules.

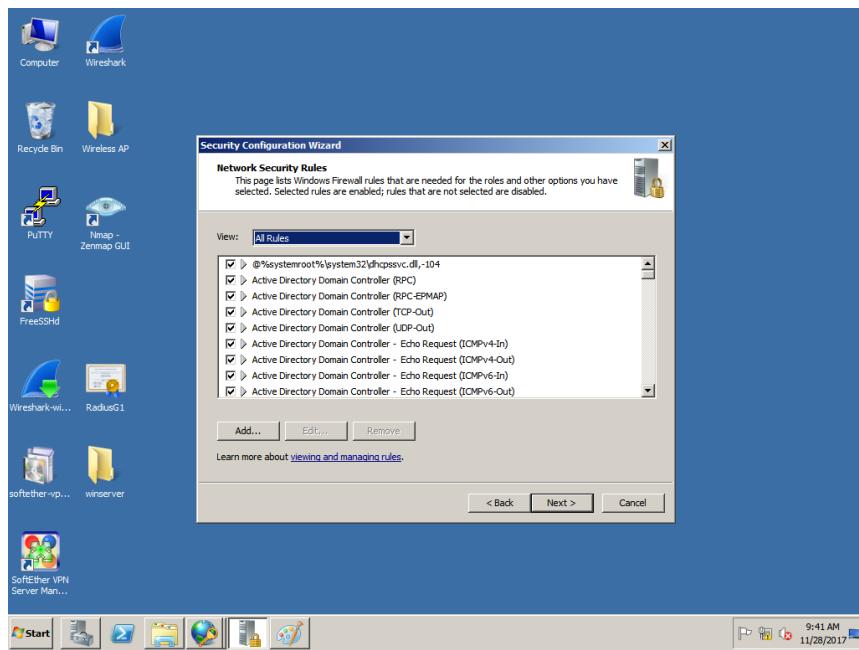


Figure 5. 300: Selecting Network Security Rules

15. Click next at the Registry Settings.

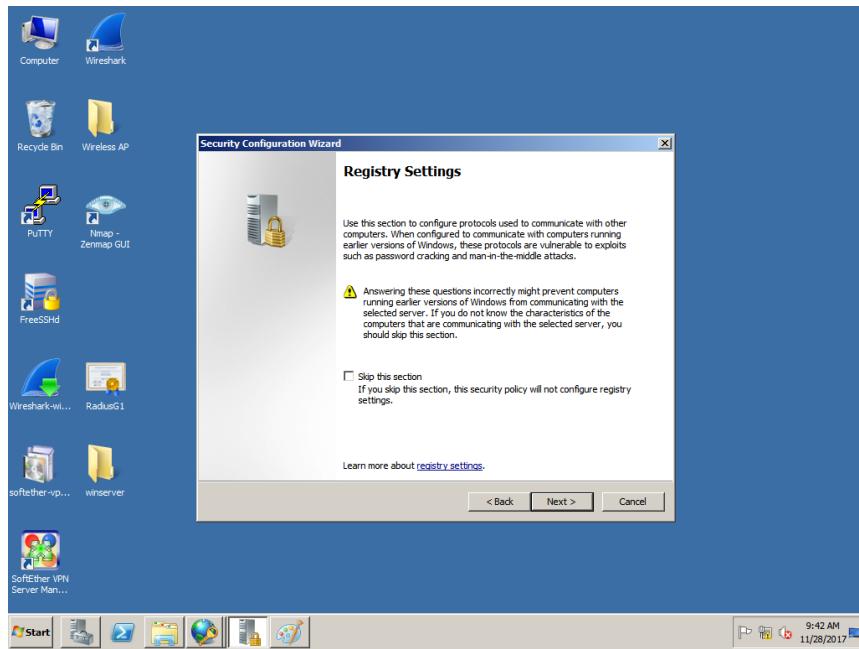


Figure 5. 301: Registry Settings

16. Select the server attributes at the Require SMB Security Signatures.

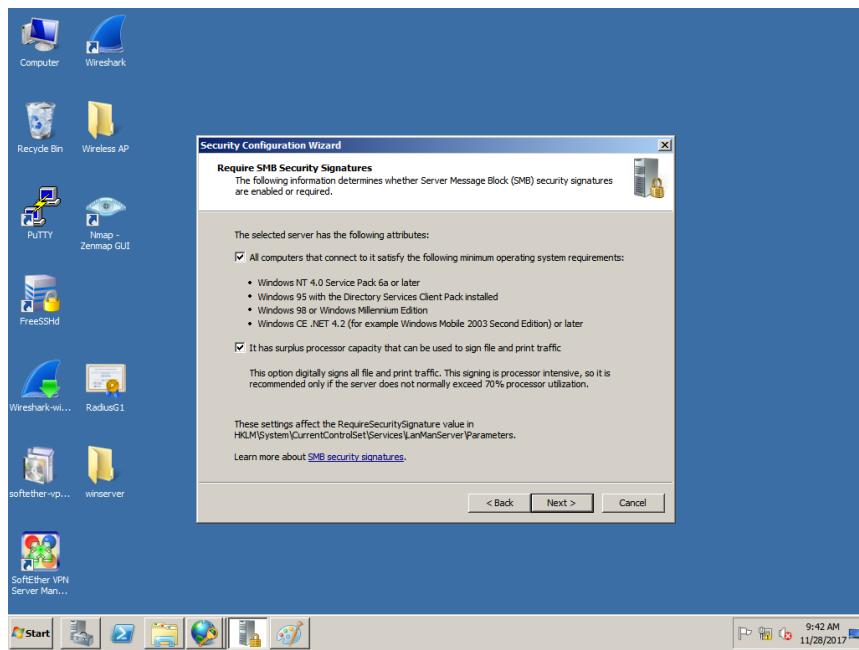


Figure 5. 302: Rewuire SMB Security Signatures

17. Click the checkbox unchecked at the Required LDAP Signing.

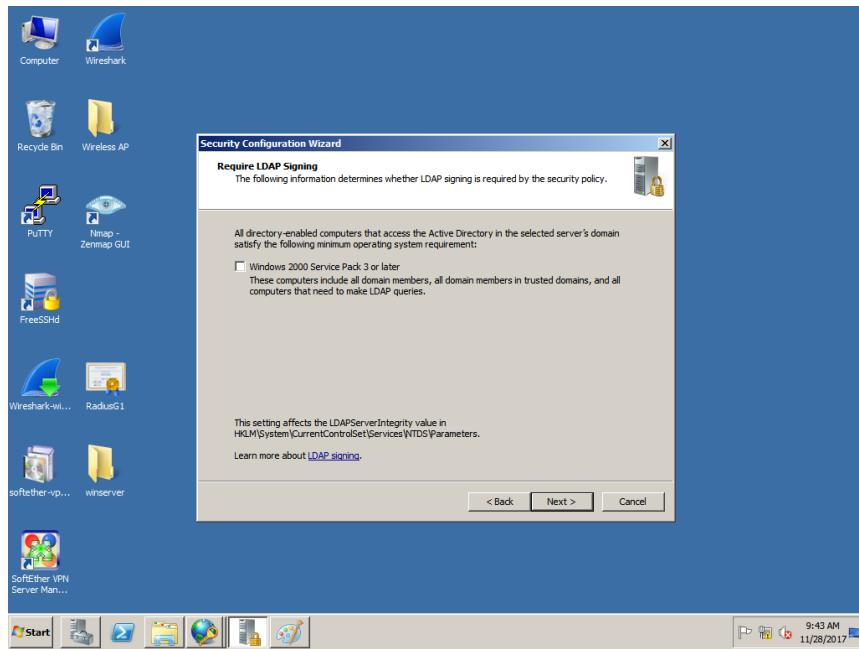


Figure 5. 303: Require LDAP Signing

18. Click “Domain Accounts” checkbox at the Outbound Authentication Methods.

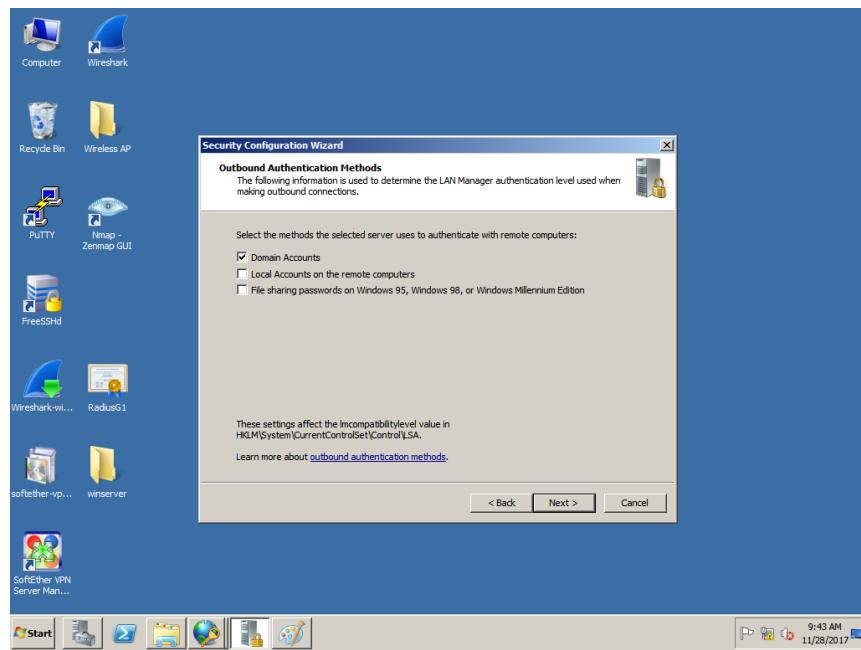


Figure 5. 304: Outbound Authentication Methods

19. Click “Windows NT 4.0 Service Pack 6a or later operating systems” checkbox at the Outbound Authentication using Domain Accounts.

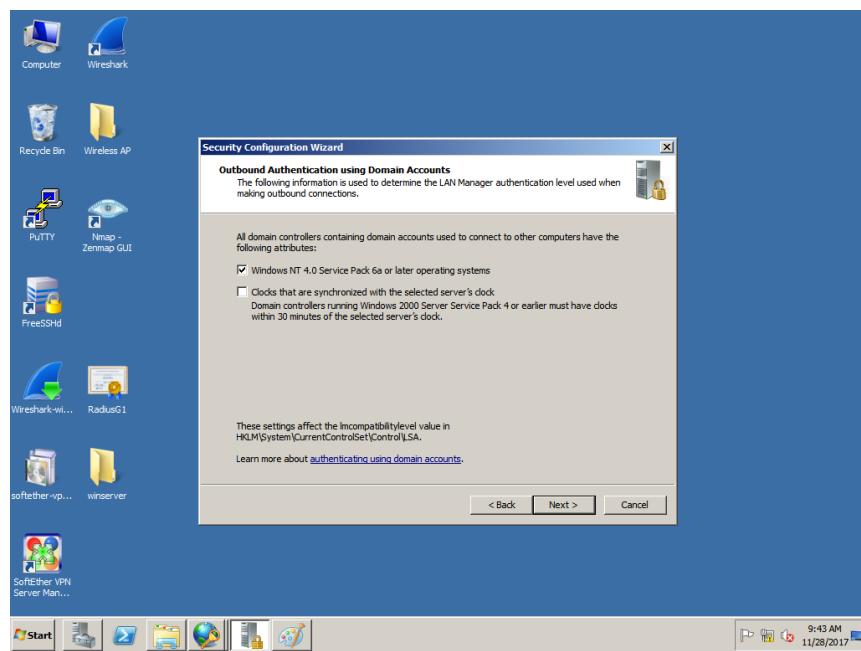


Figure 5. 305: Outbound Authentication using Domain Accounts

20. Confirm the registry settings at the Registry Settings Summary by clicking next.

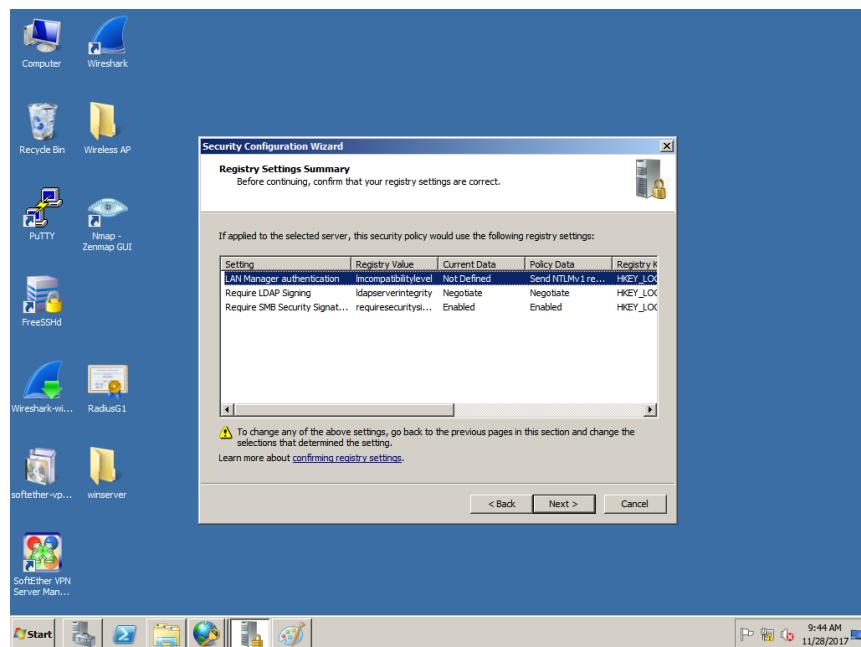


Figure 5. 306: Registry Settings Summary

21. Click next at the Audit Policy.

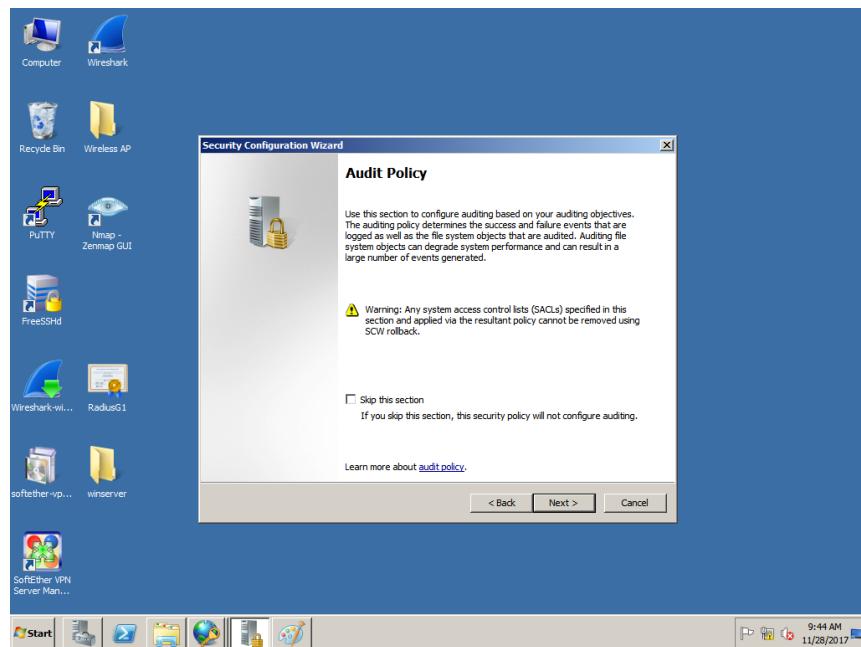


Figure 5. 307: Audit Policy

22. Click the “Audit successful and unsuccessful activities” checkbox at the System Audit Policy.

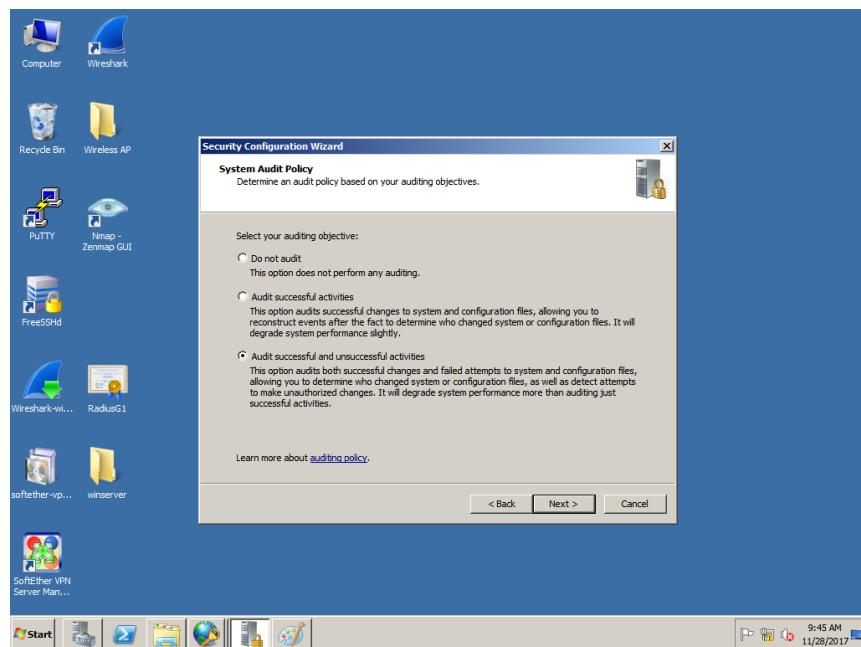


Figure 5. 308: System Audit Policy

23. Confirm auditing selections by clicking next at the Audit Policy Summary.

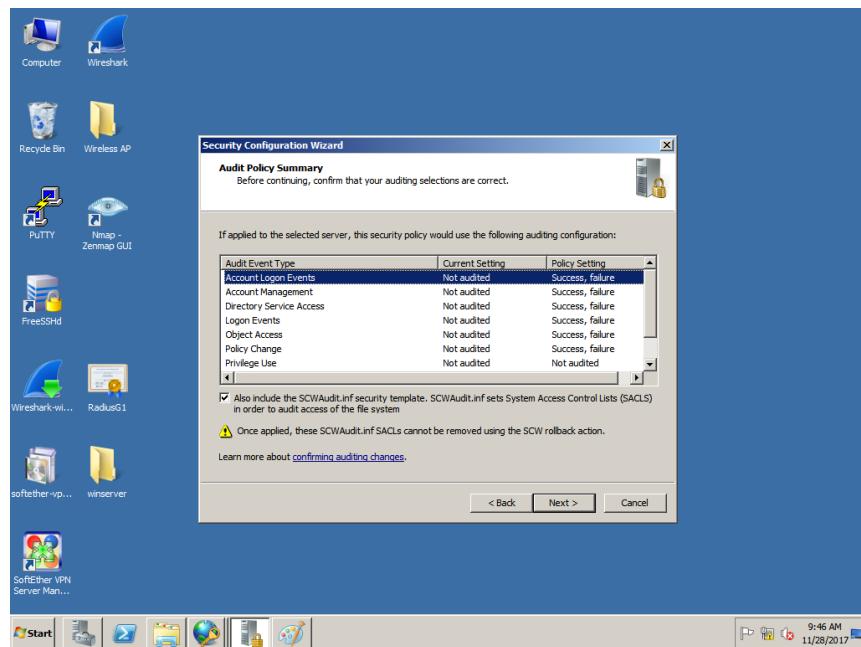


Figure 5. 309: Audit Policy Summary

24. Save the Security Policy by clicking next.

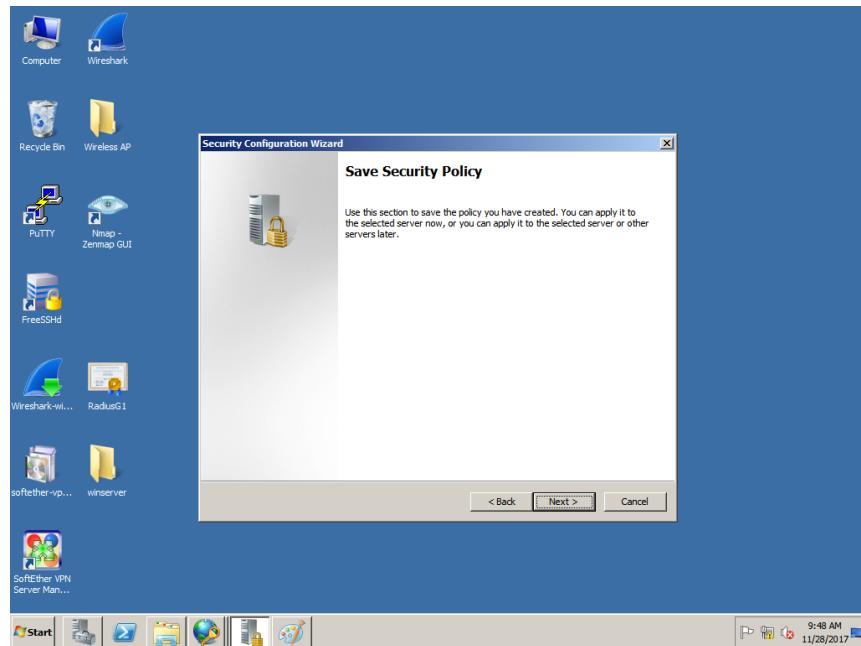


Figure 5. 310: Save Security Policy

25. Name the security policy and click next.

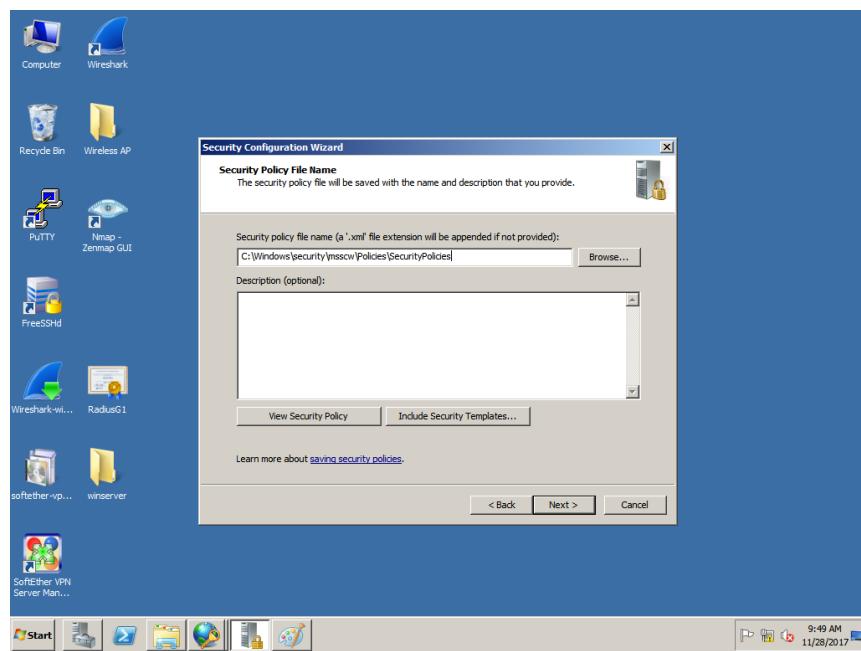


Figure 5. 311: Security Policy File Name

26. Click “Apply now” checkbox at the Apply Security Policy.

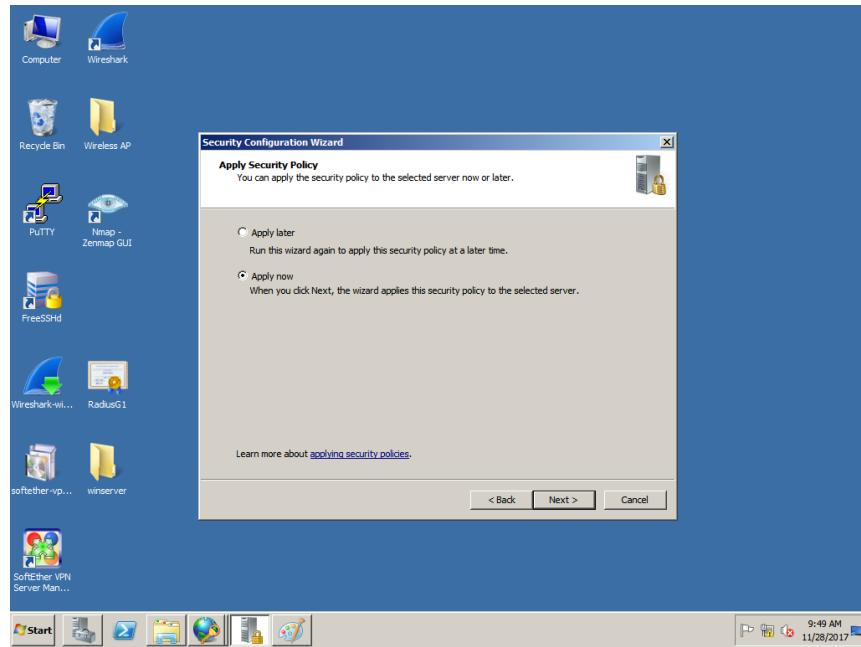


Figure 5. 312: Apply Security Policy

27. Click next at the Applying Security Policy after the application completed.

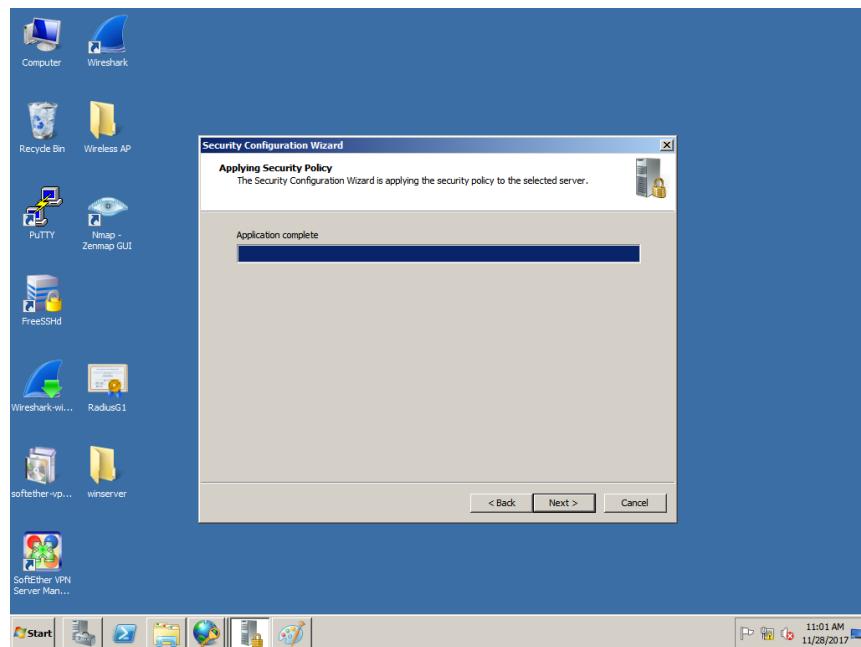


Figure 5. 313: Applying Security Policy

28. Open Server Manager.

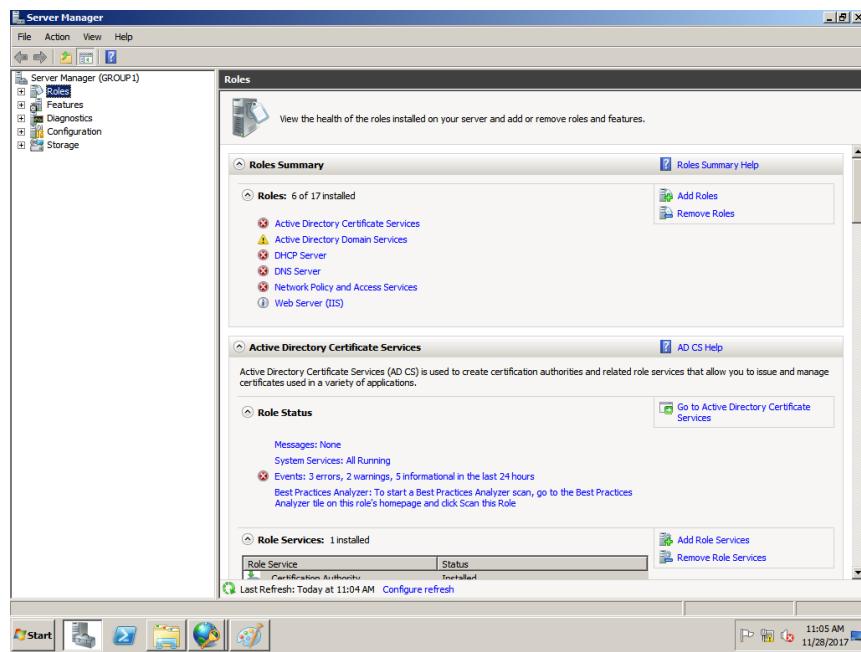


Figure 5. 314: Server Manager

29. At the Users, right click at the Guest and click Disable Account.

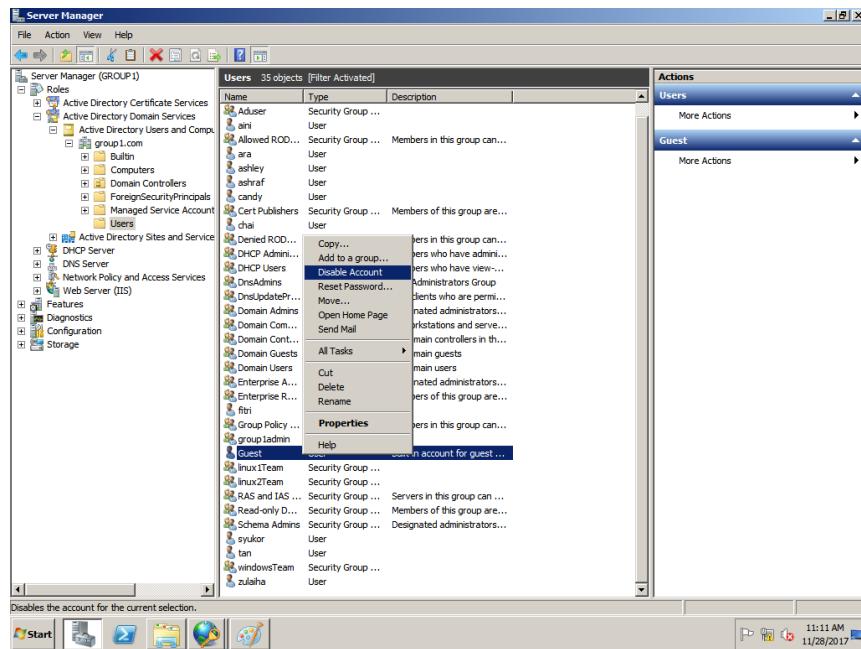


Figure 5. 315: Disabling Guest Account

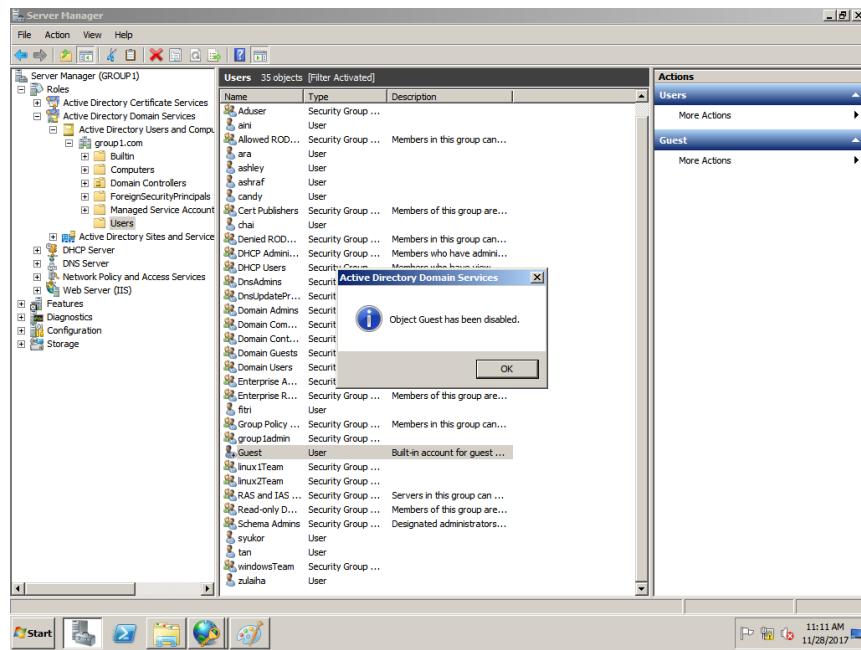


Figure 5. 316: Guest Account Disabled

### 30. Open the Local Security Policy.

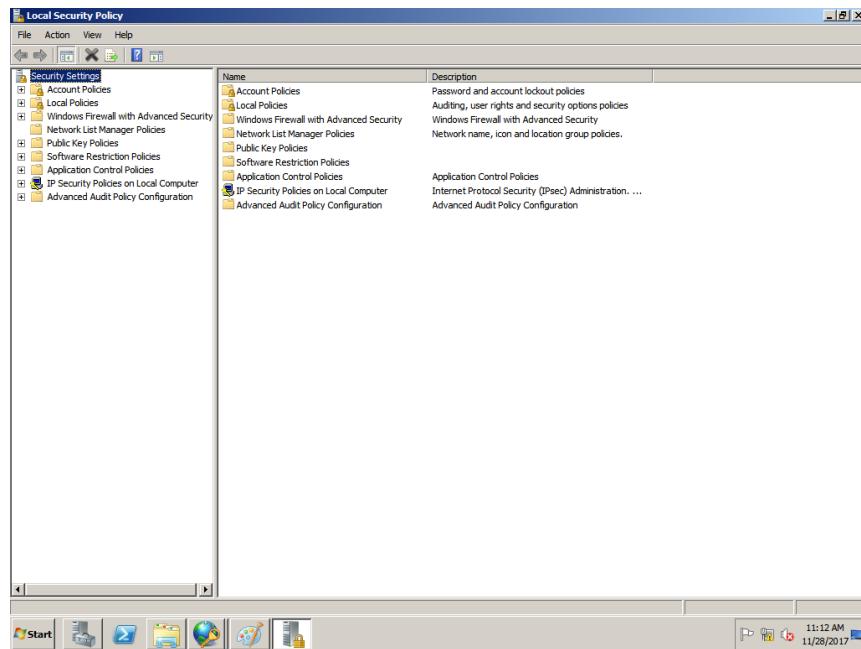


Figure 5. 317: Local Security Policy

### 31. Open Audit Policy under Local Policies.

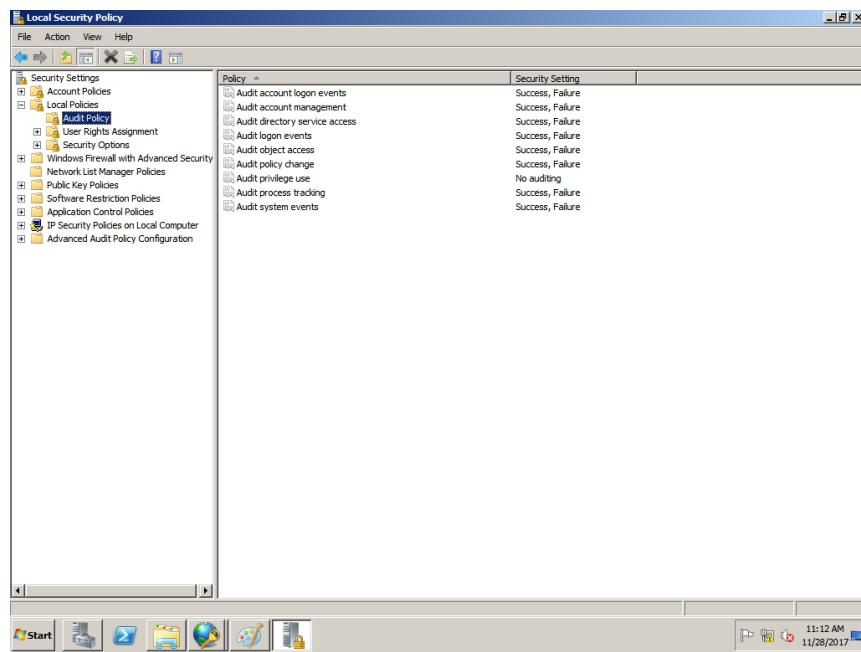


Figure 5. 318: Audit Policy

32. Right click on the Audit account logon events and click properties.

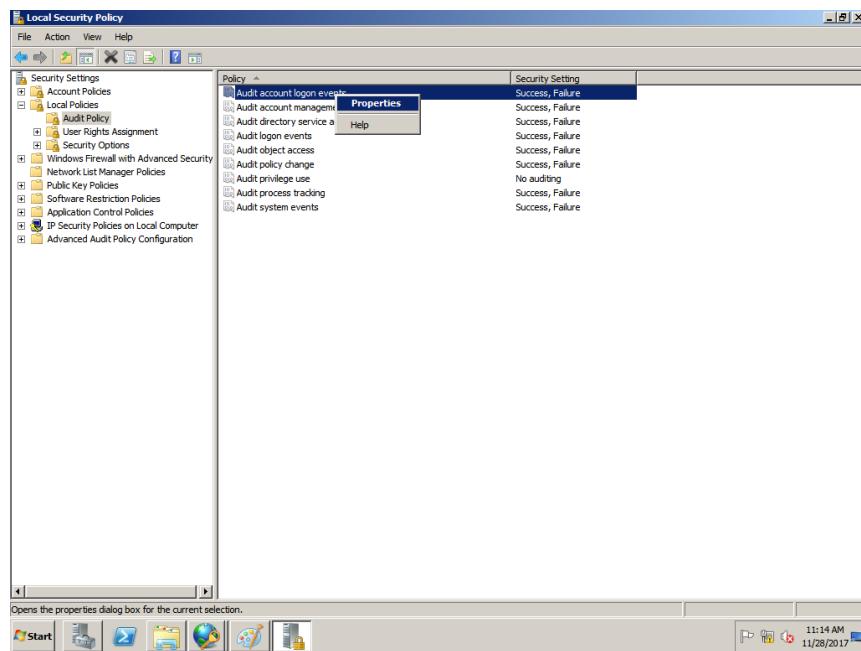


Figure 5. 319: Opening Audit account logon events properties

33. Check both “Success” and “Failure” at the Audit account logon events properties and click OK.

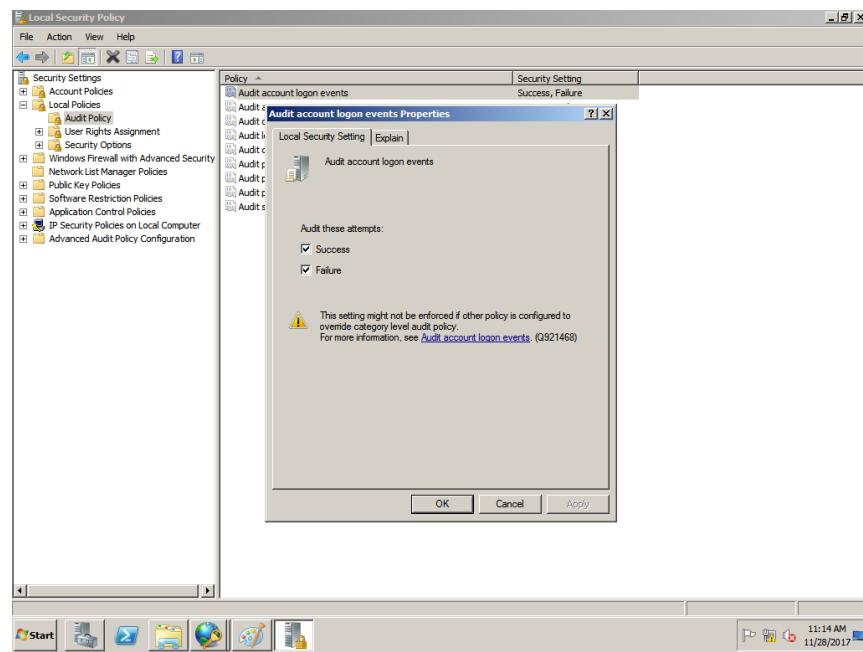


Figure 5. 320: Audit account logon events properties

34. Check both “Success” and “Failure” at the Audit account management properties and click OK.

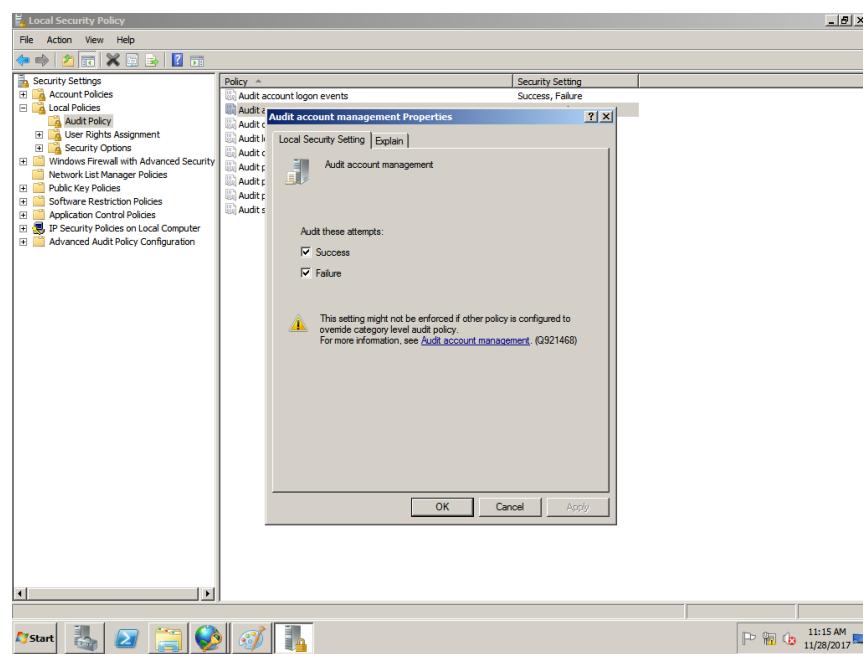


Figure 5. 321: Audit account management properties

35. Check both “Success” and “Failure” at the Audit directory services access properties and click OK.

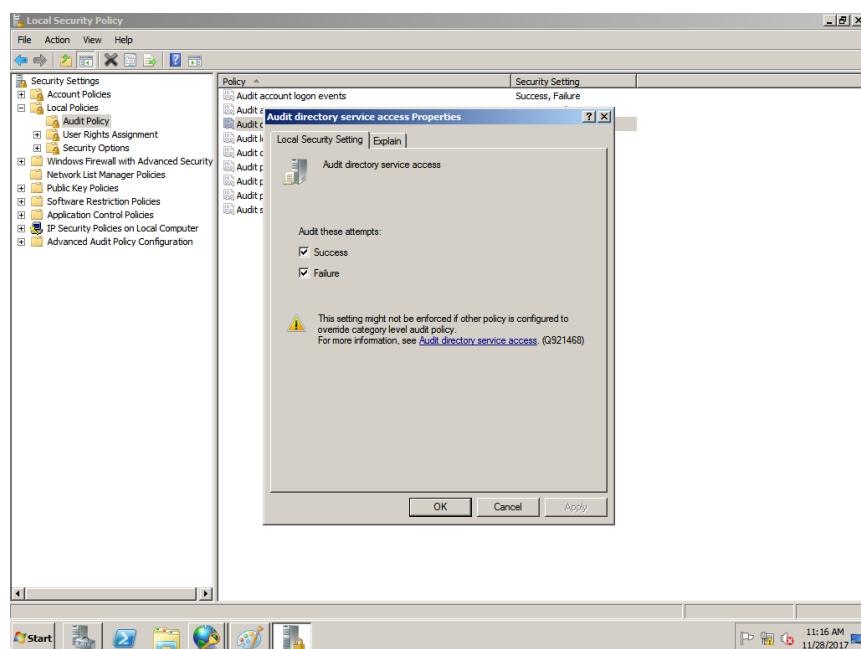


Figure 5. 322: Audit directory services access properties

36. Check both “Success” and “Failure” at the Audit logon events properties and click OK.

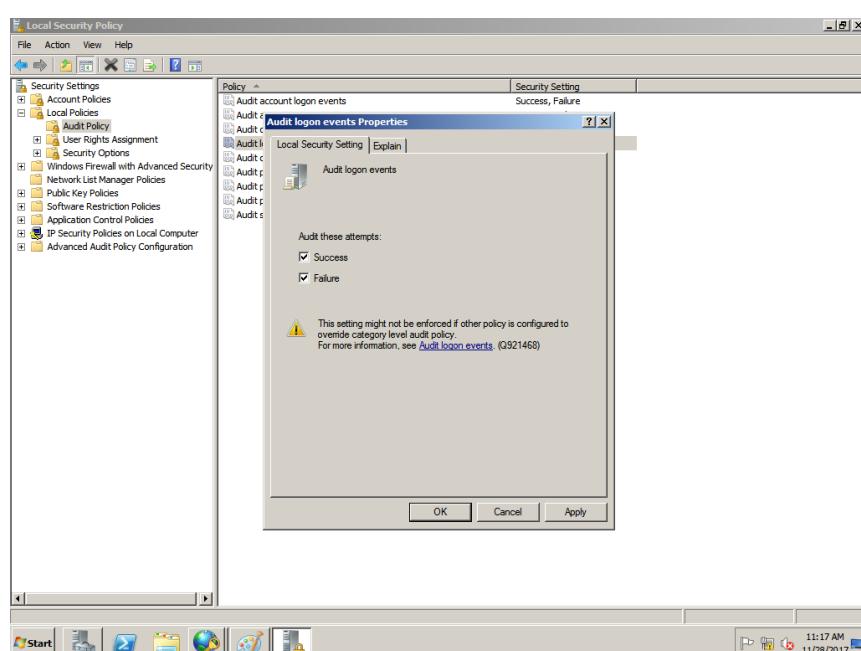


Figure 5. 323: Audit logon events properties

37. Check both “Success” and “Failure” at the Audit object access properties and click OK.

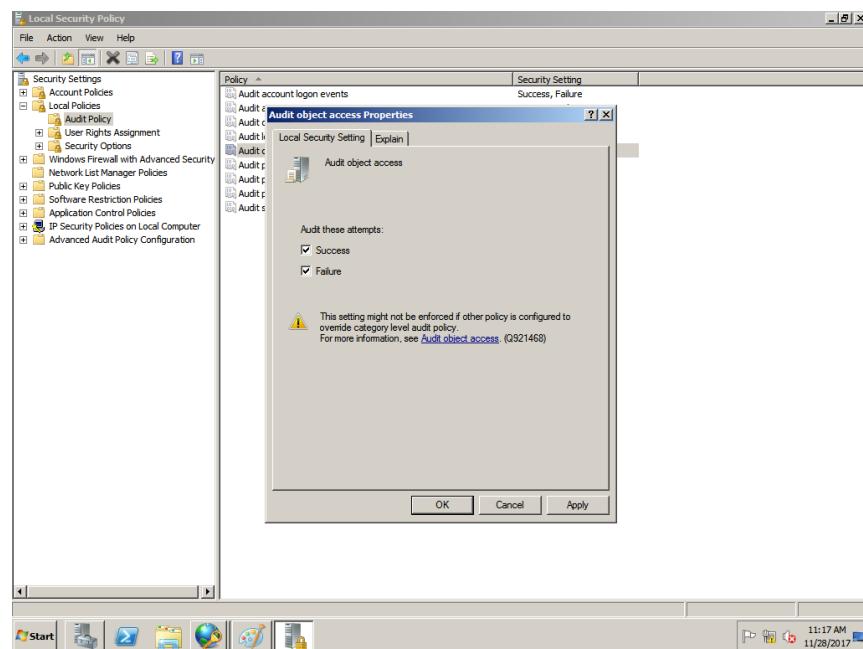


Figure 5. 324: Audit object access properties

38. Check both “Success” and “Failure” at the Audit policy change properties and click OK.

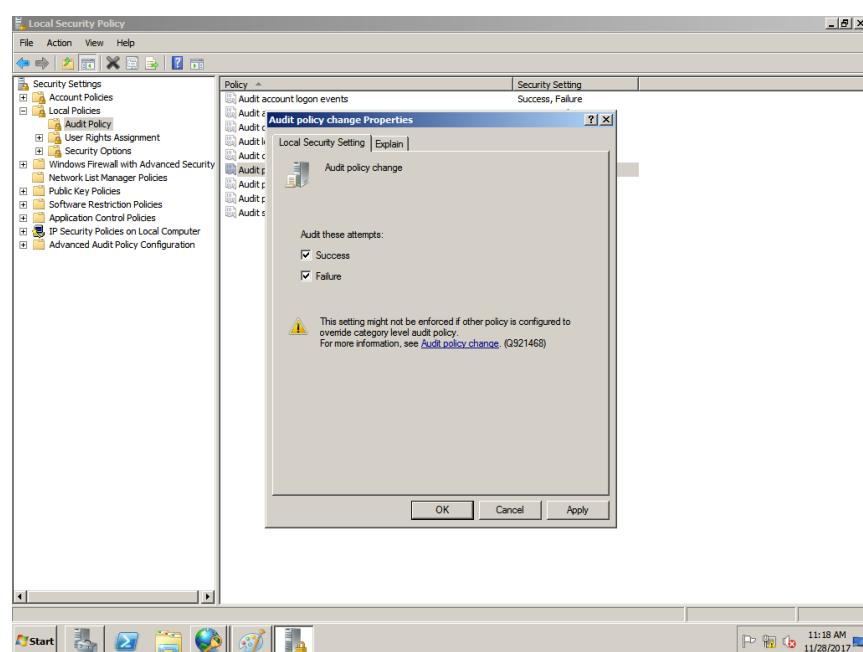


Figure 5. 325: Audit policy change properties

39. Check both “Success” and “Failure” at the Audit privilege use properties and click OK.

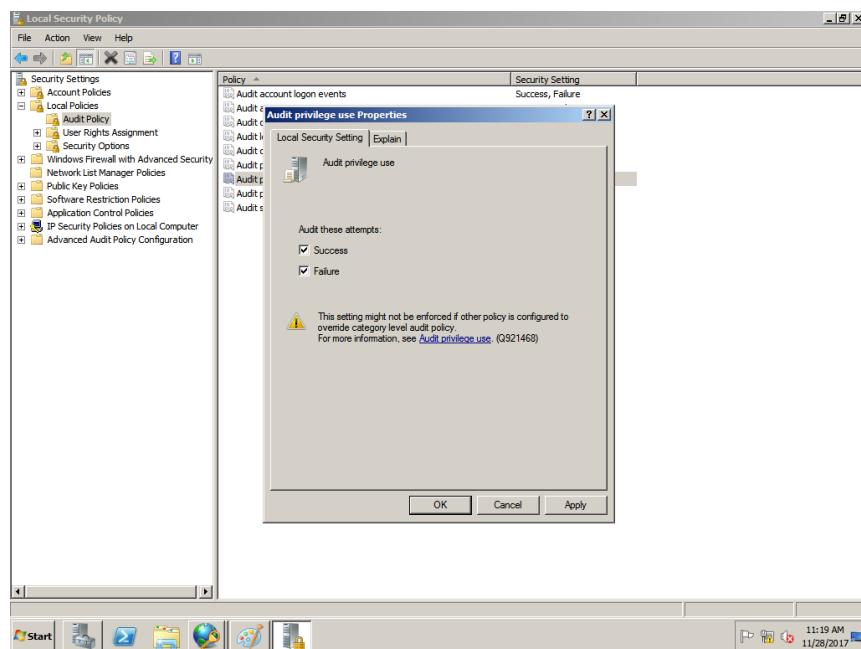


Figure 5. 326: Audit privilege use properties

40. Check both “Success” and “Failure” at the Audit process tracking properties and click OK.

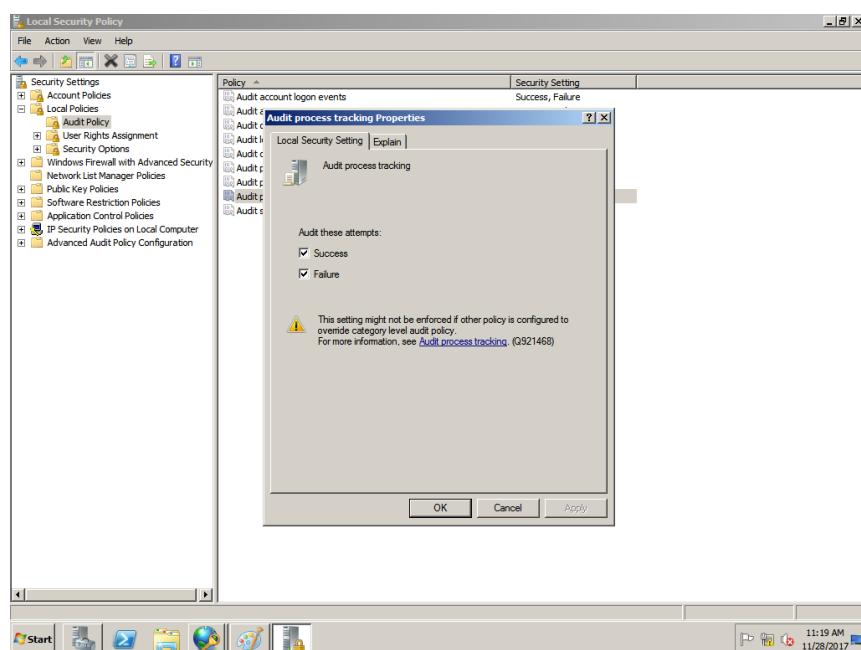


Figure 5. 327: Audit process tracking properties

41. Check both “Success” and “Failure” at the Audit system events properties and click OK.

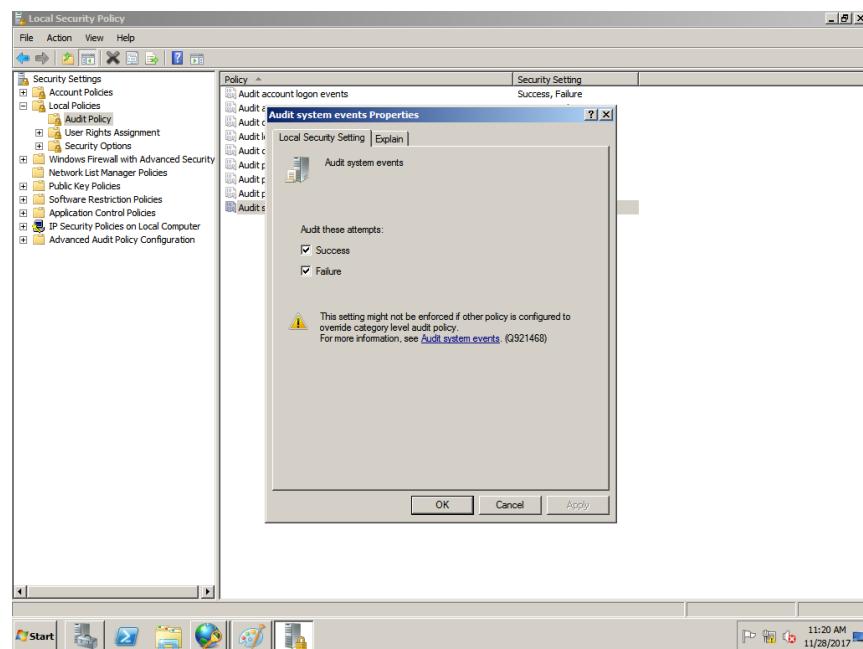


Figure 5. 328: Audit system events properties

42. Check the security changes after changing all the properties.

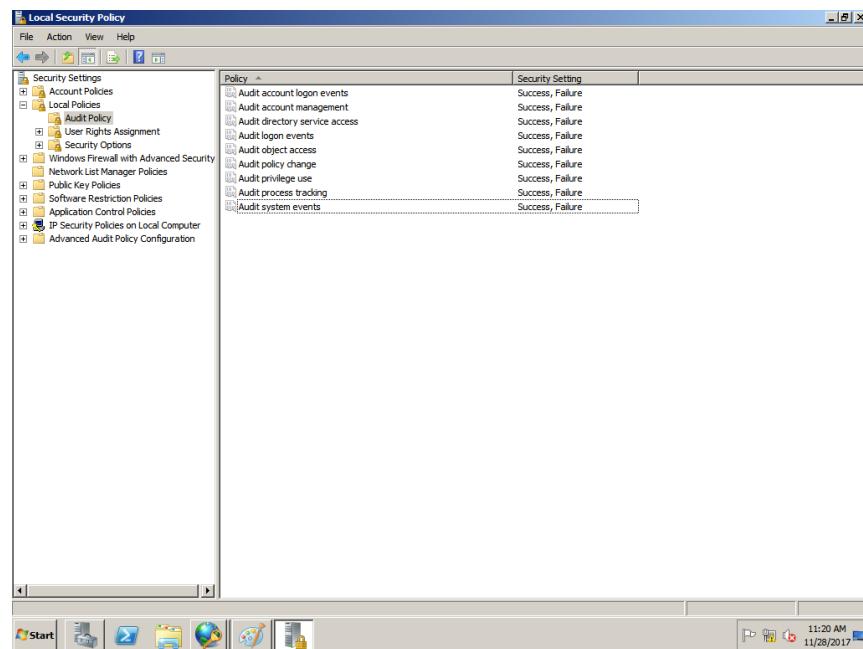


Figure 5. 329: Check all the audits

43. Open the Change settings in Windows Update. Make the updates to be installed automatically and make them every day.

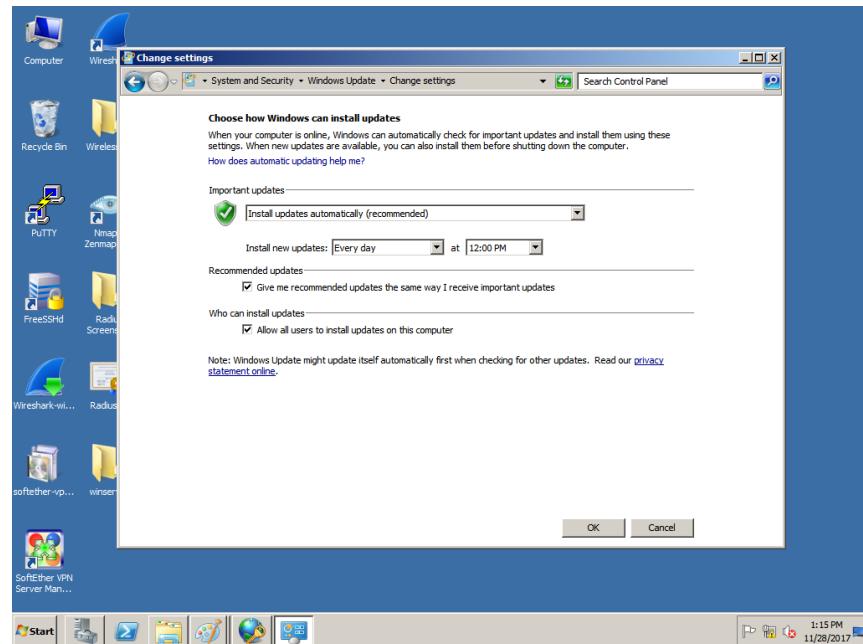


Figure 5. 330: Change settings in Windows Updates

44. Check for updates and click on the important updates.

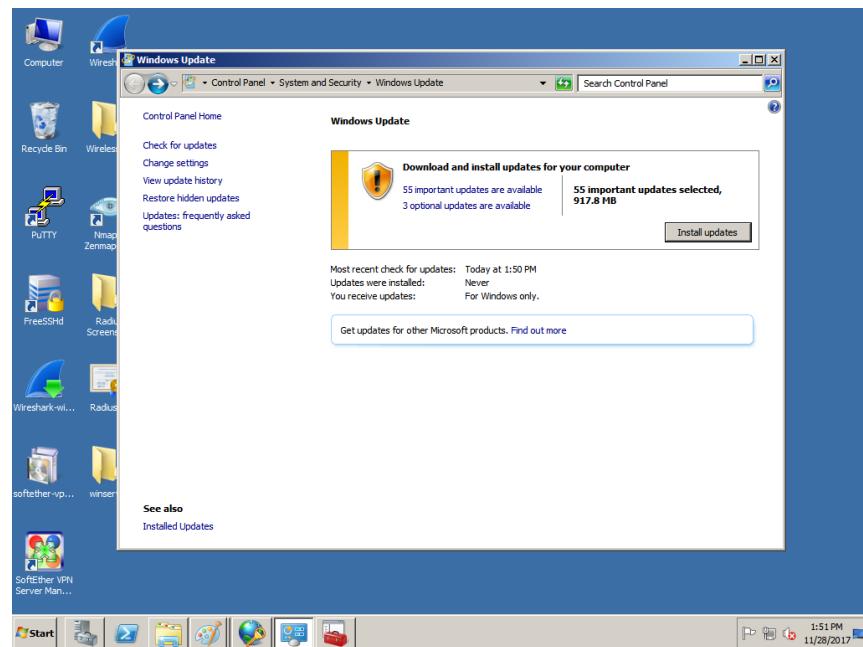


Figure 5. 331: Updates that are available

45. Choose the updates to be installed.

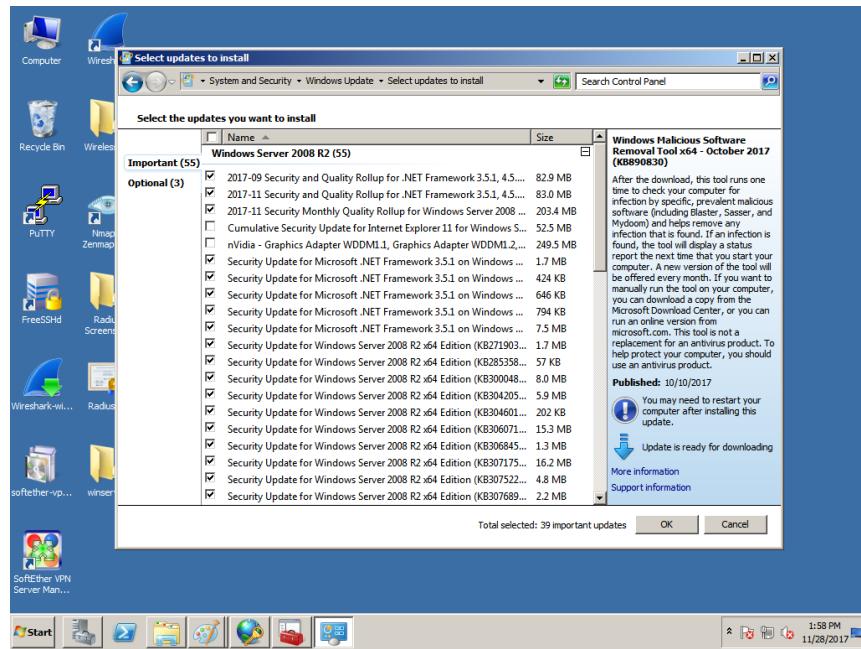


Figure 5. 332: Choosing updates to be installed

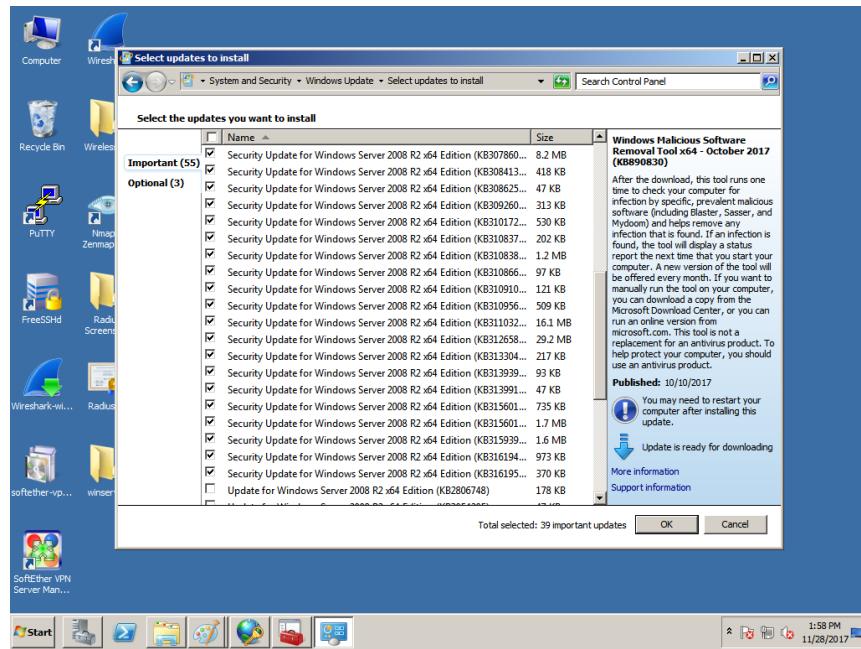


Figure 5. 333: Choosing updates to be installed(2)

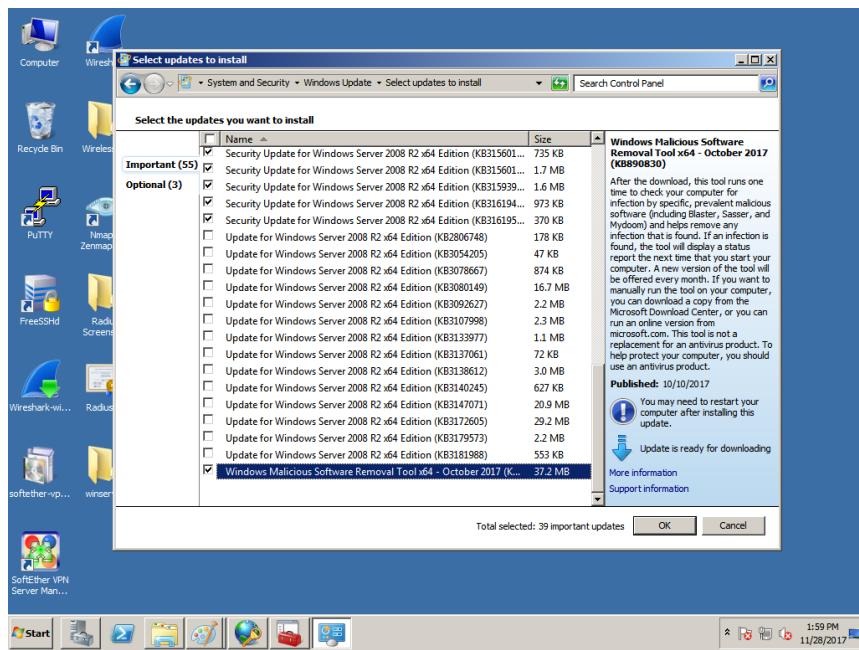


Figure 5. 334: Choosing updates to be installed(3)

46. Click “I accept the license terms” and click Finish.

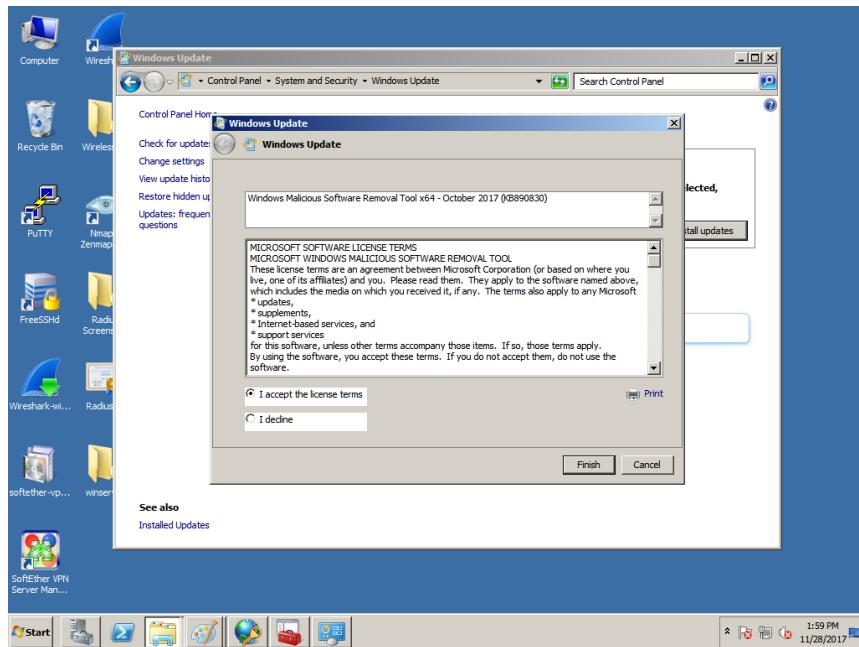


Figure 5. 335: Accepting the license terms

47. Open Server Manager and click Features.

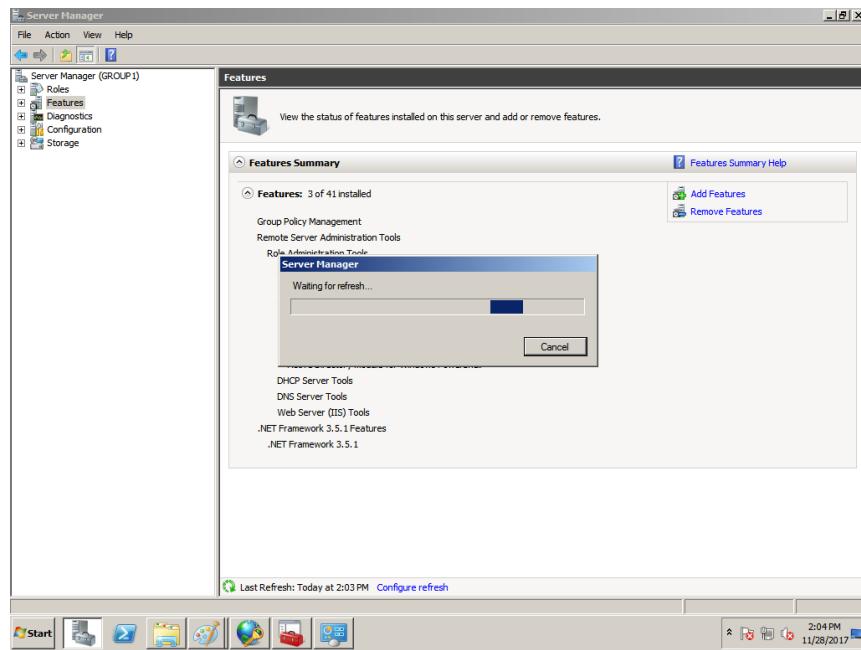


Figure 5. 336: Opening Features in Server Manager

48. Check BitLocker Drive Encryption checkbox and click Next.

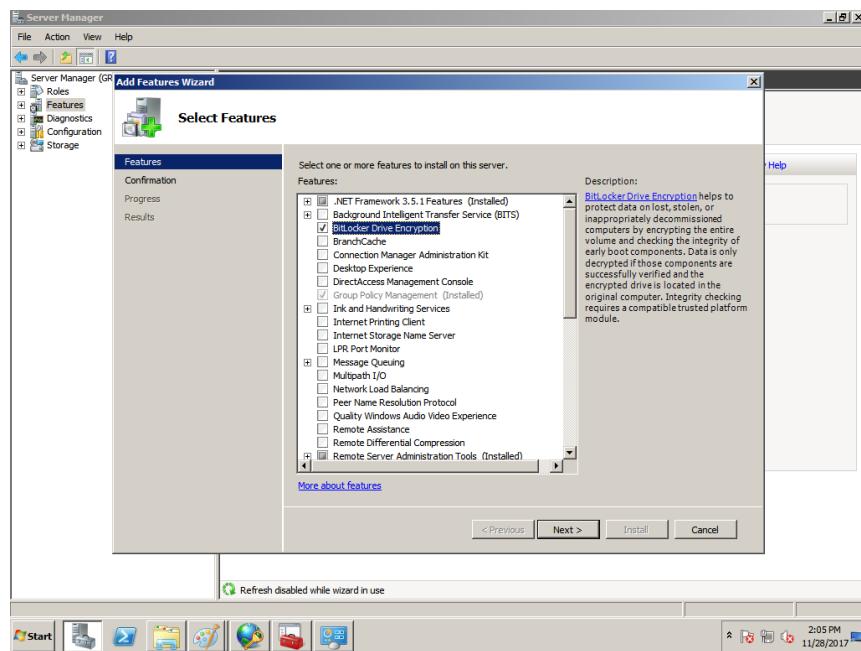


Figure 5. 337: Add Features Wizard

49. Click Install at the Confirm Installation Selection. Then, restart Windows Server.

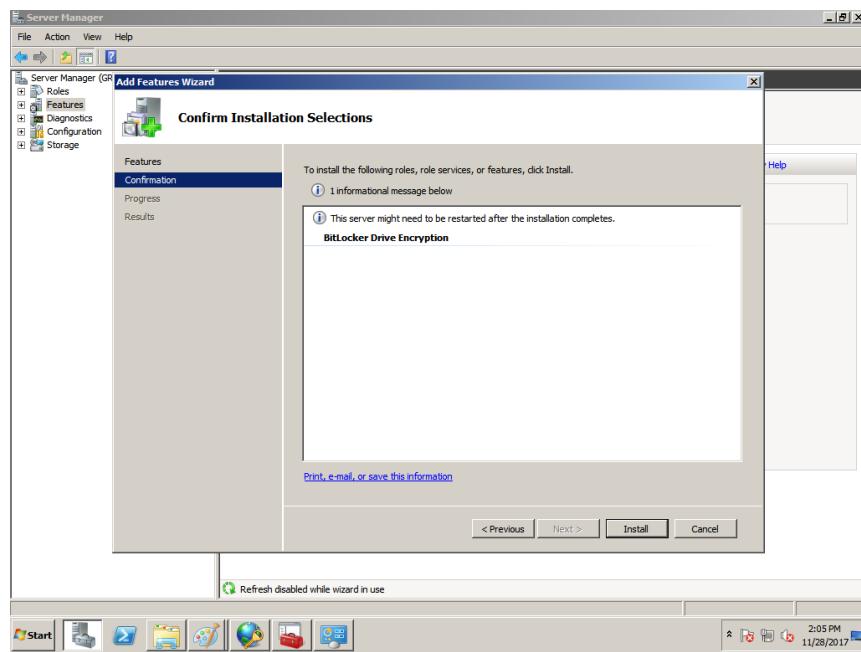


Figure 5. 338: Confirm Installation Selection

50. Open Control Panel and click Check firewall status.

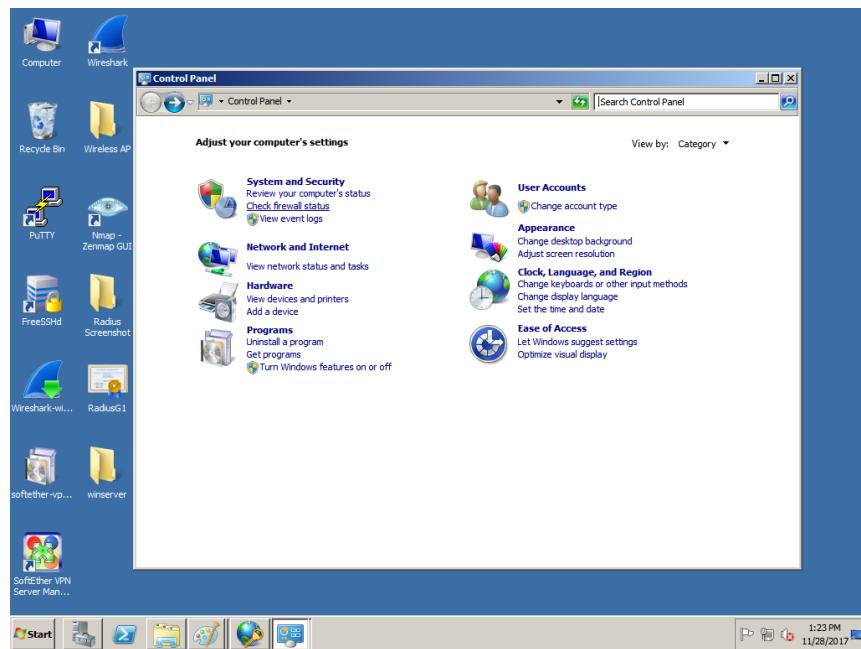


Figure 5. 339: Clicking Check Firewall Status

51. Turn on Windows Firewall in all the location settings.

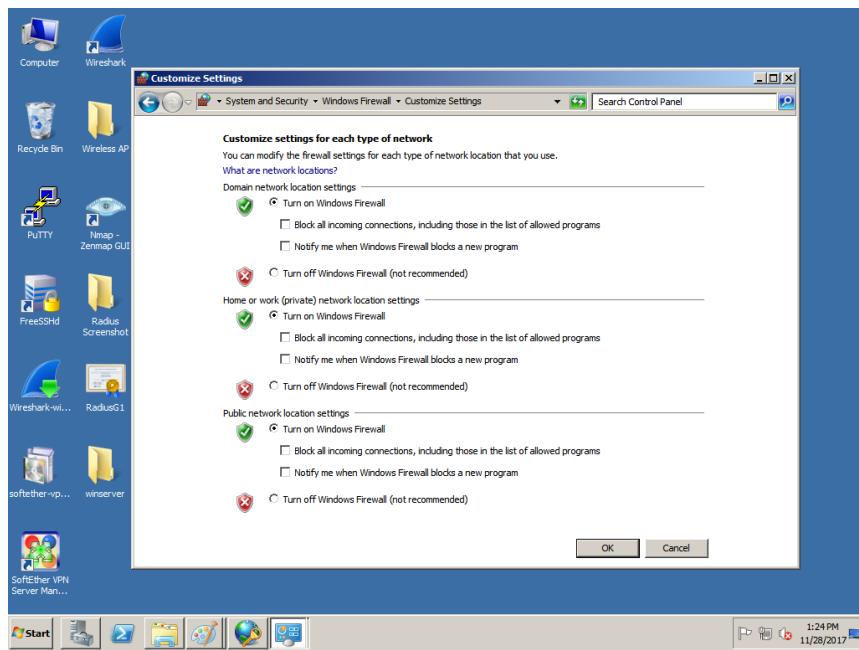


Figure 5. 340: Customize Settings in Windows Firewall

## 52. Check the status of Windows Firewall.

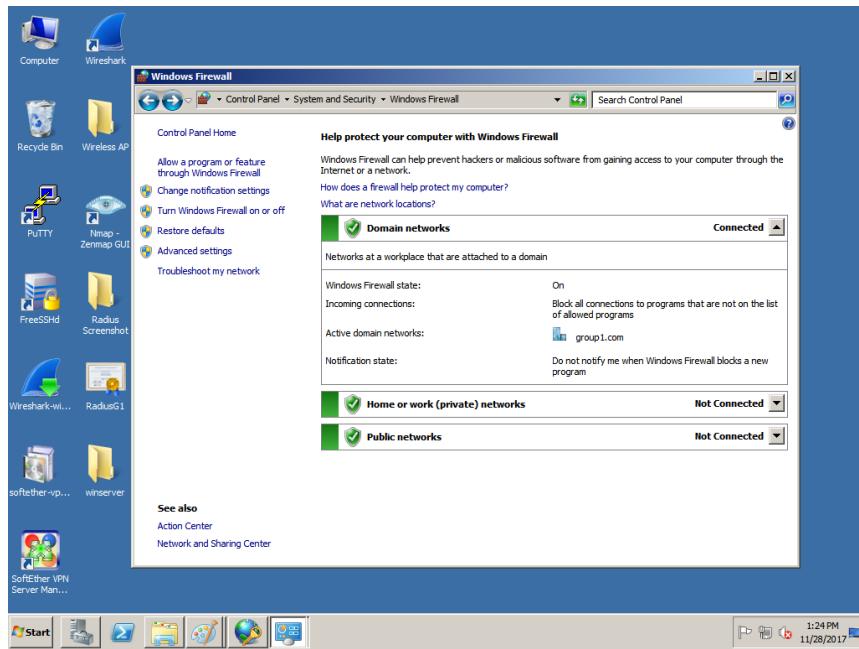


Figure 5. 341: Status of Windows Firewall

## 53. Open Windows Firewall with Advanced Security. Check the Firewall to see if it is enabled.

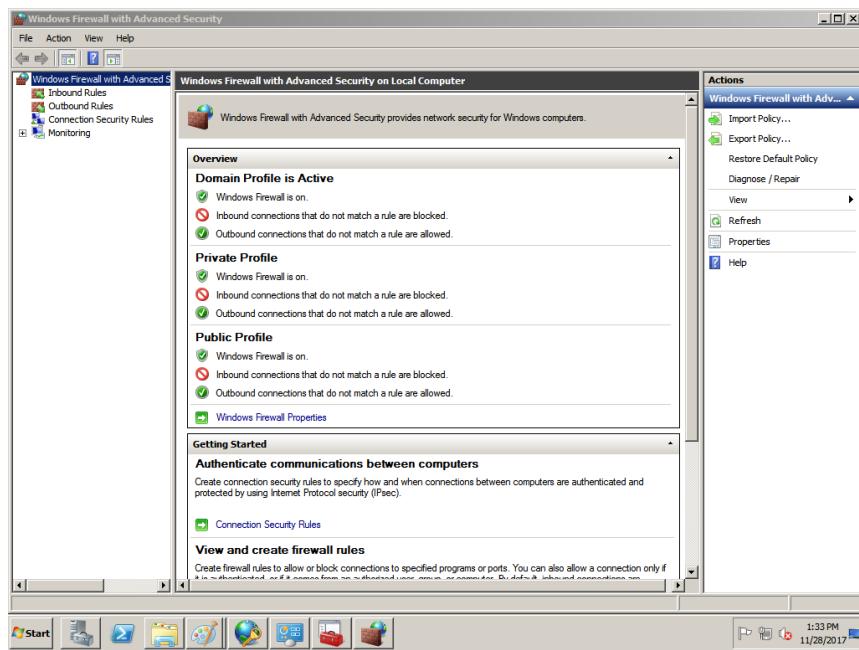


Figure 5. 342: Windows Firewall with Advance Security

54. Run services.msc. Check the list of the services. Double click the Print Spooler service. We are not using this service as it is for printing so change the Startup from Automatic to Disabled. Then, click Apply.

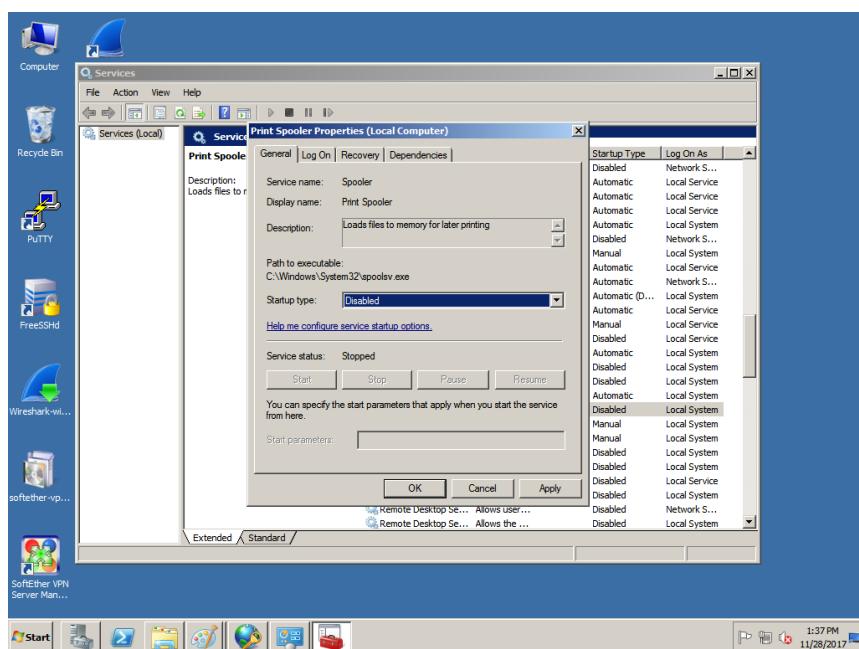


Figure 5. 343: Print Spooler Properties

55. Double click Distributed Transaction Coordination service. The Distributed Transaction Coordinator service is responsible for coordinating transactions that span multiple resource managers, such as databases, message queues, and file systems. Windows server is not used as a SQL server so we change startup type from Automatic to Disable.

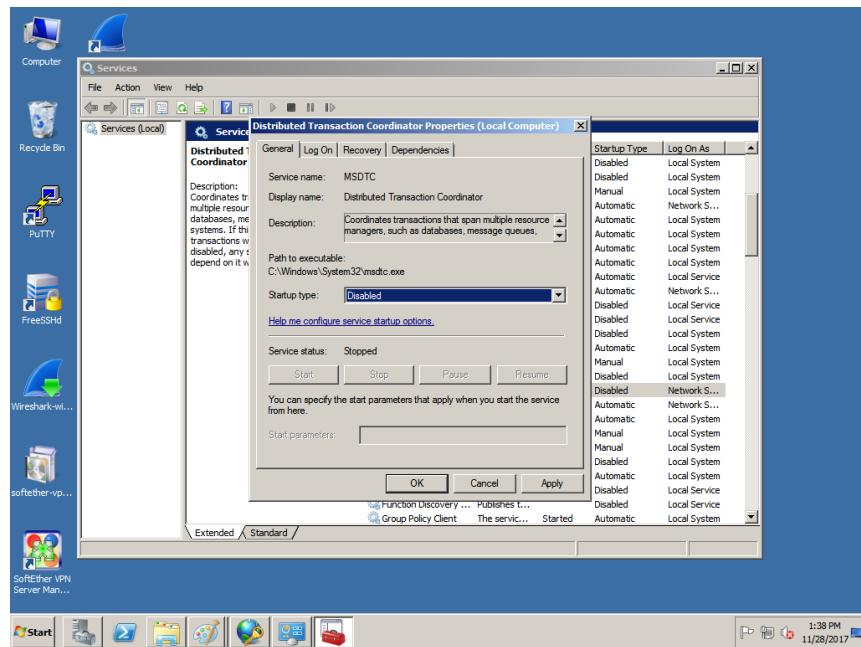


Figure 5. 344: Distributed Transaction Coordinator Properties

56. Double click KtmRm for Distributed Transaction Coordinator service. This is used to coordinate transactions between the Distributed Transaction Coordinator (DTC) and the Kernel Transaction Manager (KTM). Since DTC is disabled, this service is not needed so we change startup type from Automatic to Disable.

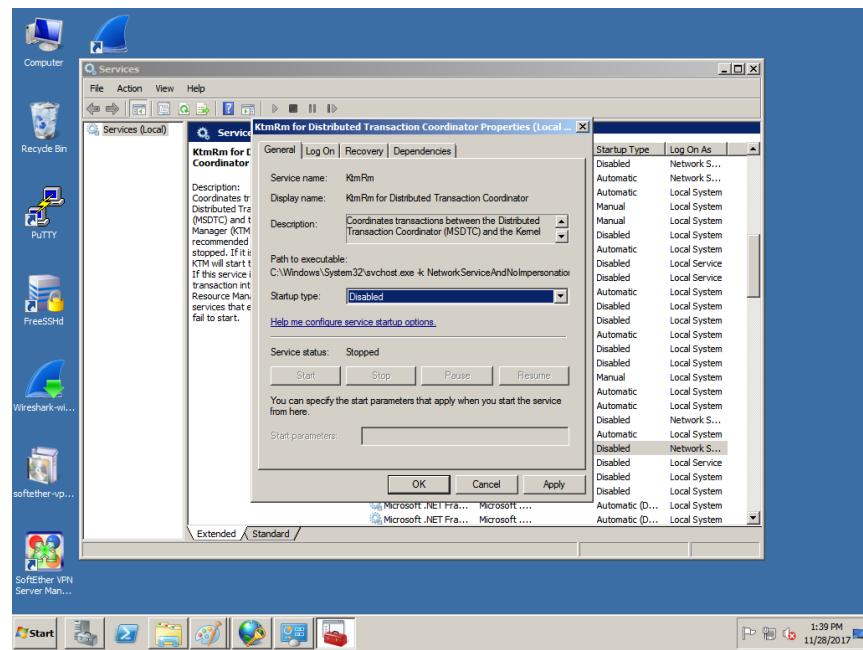


Figure 5. 345: KtmRm for Distributed Transaction Coordinator Properties

57. Double click Certificate Propagation services. It is used for Smart Card certificate handling. Smart-cards are used sometimes for log in instead of a password. Change the Startup type to Automatic and click Start.

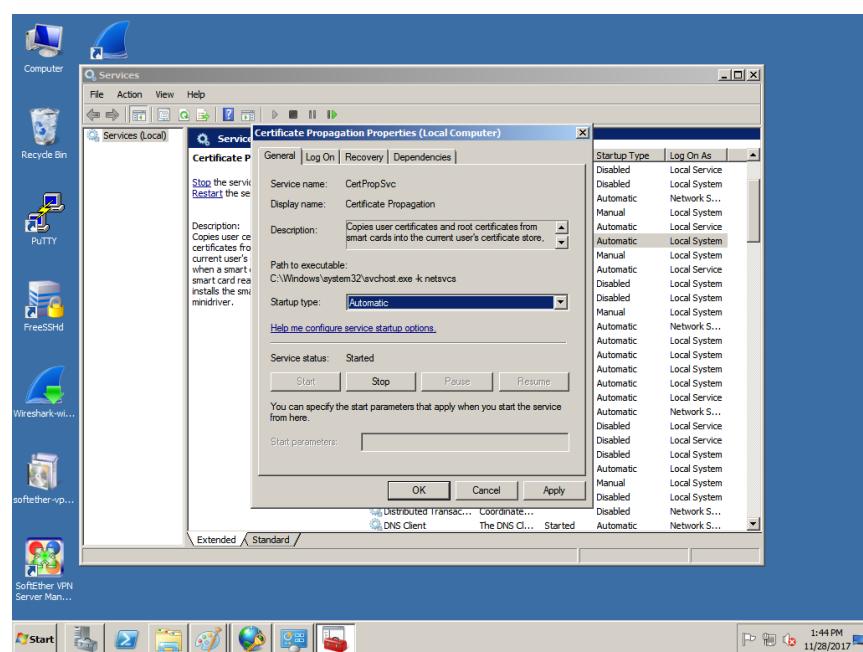


Figure 5. 346: Certificate Propagation Properties

58. Double click Netlogon Properties. NetLogon maintains a channel between computer and domain controller. The Netlogon sub-key stores information for the Net Log-on service. The Net Log on service verifies log-on requests, and it registers, authenticates, and locates domain controllers. Make the Startup type to Automatic and click Start.

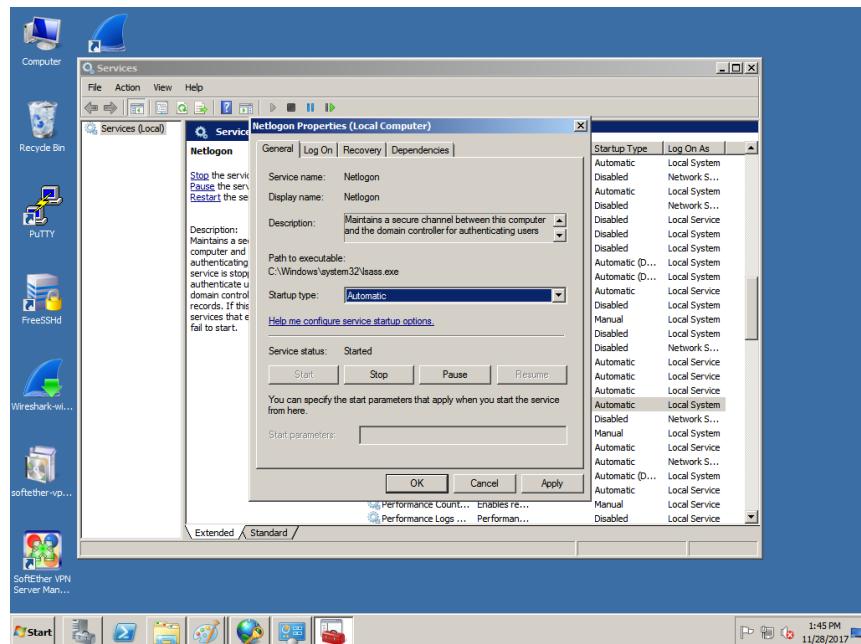


Figure 5. 347: Netlogon Properties

59. Double click on the Special Administration Console Helper. It allows the administrators to remotely the command prompt. The Special Administration Console (SAC) can connect to a machine where this service is running. SAC can perform remote management tasks in case the machine stop functioning due to a Stop error message. Make the Startup type to Automatic and click start.

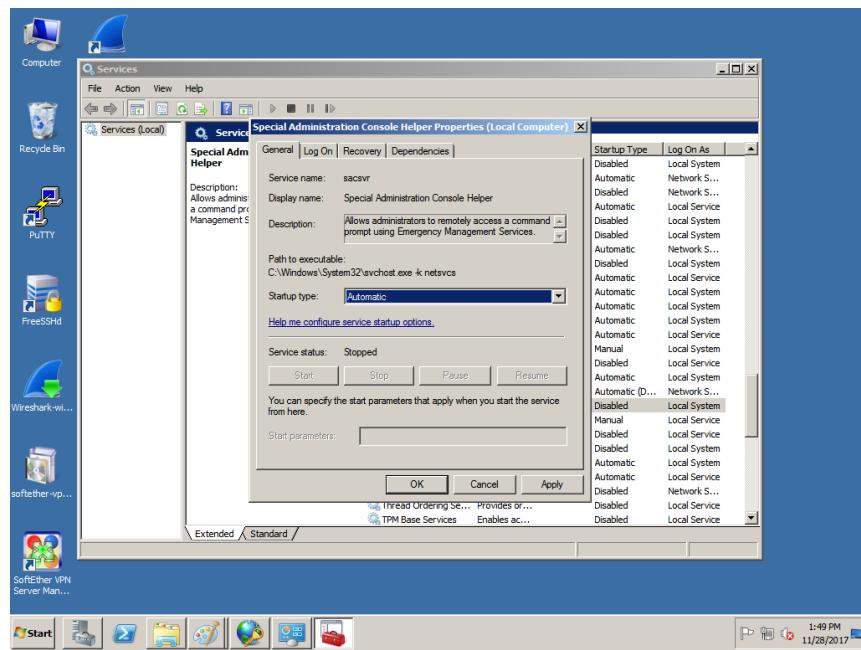


Figure 5. 348: Special Administration Console Helper Properties

60. Double click on the Secure Socket Tunneling Protocol Service. Secure Socket Tunneling Protocol (SSTP) is a form of VPN tunnel that provides a mechanism to transport PPP or L2TP traffic through an SSL 3.0 channel. SSL provides transport-level security with key-negotiation, encryption and traffic integrity checking so make the Startup type to Automatic and click Start.

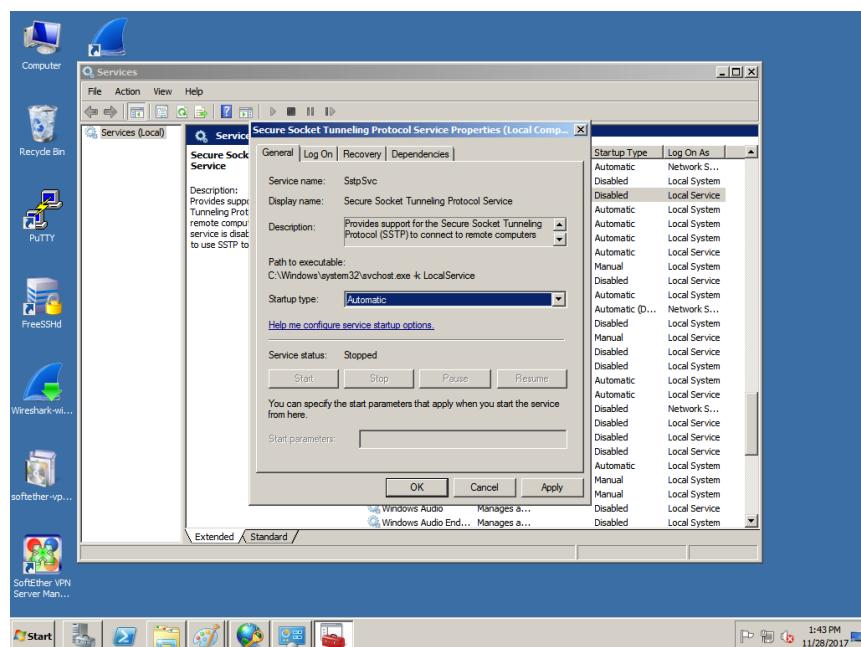


Figure 5. 349: Secure Socket Tunneling Protocol Service Properties

61. Double click on the Windows Error Reporting Service. Windows Error Reporting is a set of Windows technologies that capture software crash data and support end-user reporting of crash information. Change the Startup type to Automatic and start the service.

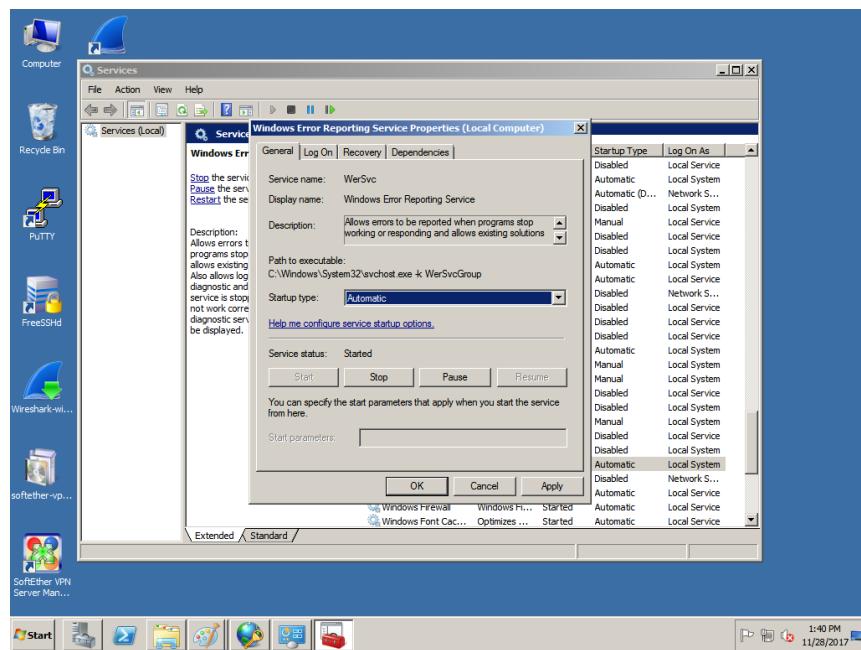


Figure 5. 350: Windows Error Reporting Service Properties

### 5.3.22 HARDENING WEB SERVER

Step 1: Navigate to Windows> Microsoft.NET> Framework> v2.0.50727> CONFIG> Double Click web.conf

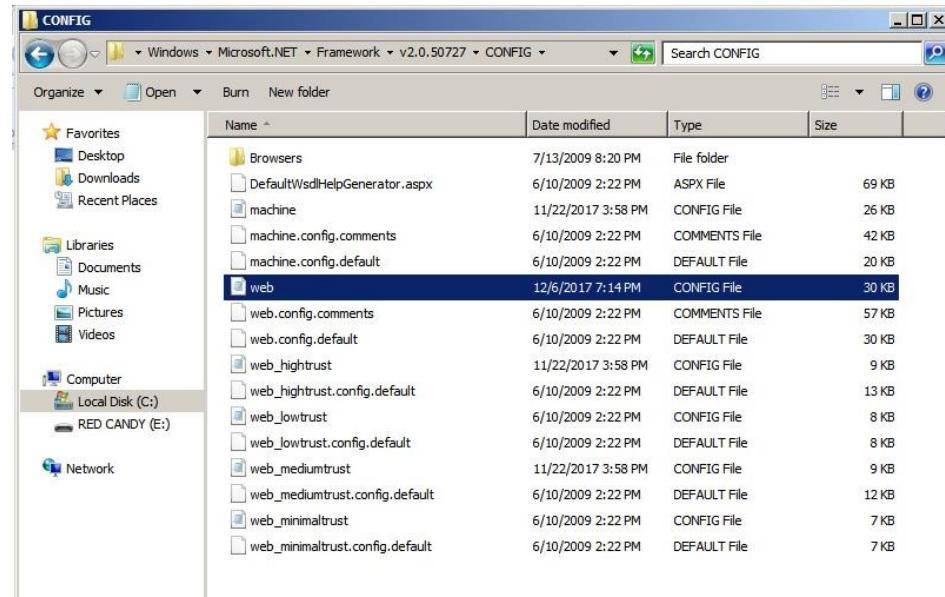


Figure 5. 351: Open the web.conf

### Step 2: Adding debug="false" in compilation

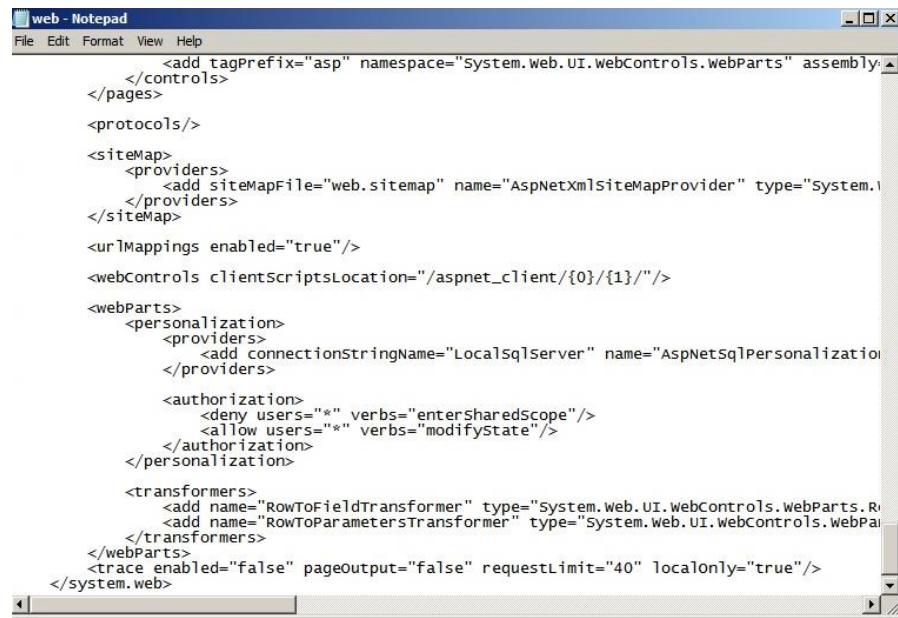
```

<result type="System.Web.Mobile.MobileCapabilities, System.web.Mobile, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
</browserCaps>
<clientTarget>
<add alias="ie5" userAgent="Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 4.0)"/>
<add alias="ie4" userAgent="Mozilla/4.0 (compatible; MSIE 4.0; Windows NT 4.0)"/>
<add alias="uplevel" userAgent="Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)"/>
<add alias="downlevel" userAgent="Generic Downlevel"/>
</clientTarget>
<compilation debug='false'>
<assemblies>
<add assembly="mscorlib"/>
<add assembly="System, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
<add assembly="System.Configuration, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
<add assembly="System.web, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
<add assembly="System.Data, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
<add assembly="System.web.Services, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
<add assembly="System.xml, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
<add assembly="System.Drawing, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
<add assembly="System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
<add assembly="System.web.Mobile, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
<add assembly="*"/>
<add assembly="System.Runtime.Serialization, Version=3.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
<add assembly="System.IdentityModel, Version=3.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
<add assembly="System.ServiceModel, Version=3.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
<add assembly="System.ServiceModel.web, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
<add assembly="System.WorkflowServices, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
</assemblies>
<buildProviders>
<add extension=".aspx" type="System.Web.Compilation.PageBuildProvider"/>
<add extension=".ascx" type="System.Web.Compilation.UserControlBuildProvider"/>
<add extension=".master" type="System.Web.Compilation.MasterPageBuildProvider"/>
<add extension=".asmx" type="System.Web.Compilation.webServiceBuildProvider"/>
<add extension=".ashx" type="System.Web.Compilation.webHandlerBuildProvider"/>
</buildProviders>

```

Figure 5. 352: Edit web.conf

### Step 3: Adding <trace enabled="false">



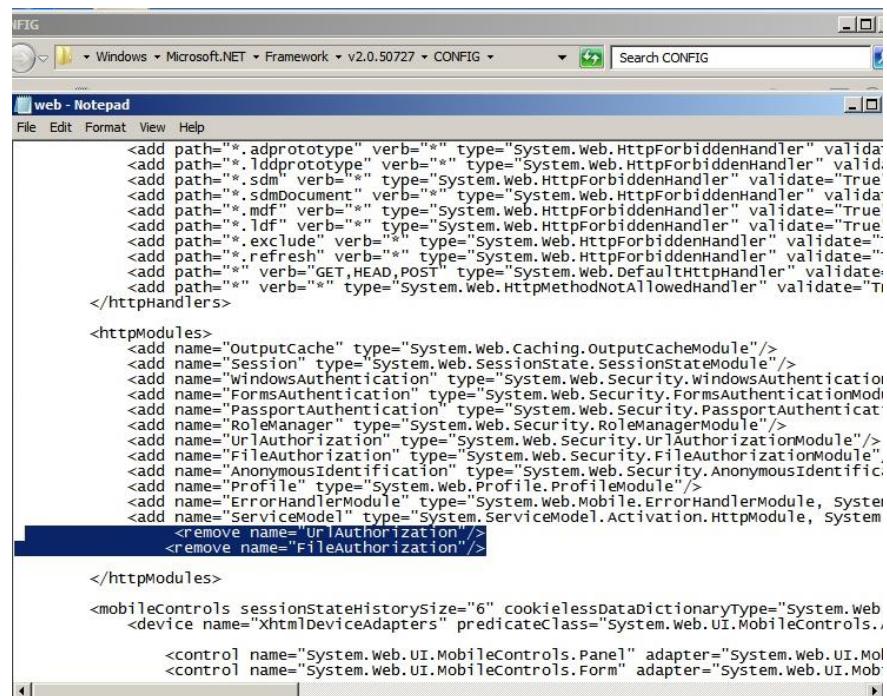
```

<!-->
</controls>
</pages>
<protocols/>
<siteMap>
    <providers>
        <add siteMapFile="web.sitemap" name="AspNetXmlSiteMapProvider" type="System.Web.SitemapProvider" />
    </providers>
</siteMap>
<urlMappings enabled="true"/>
<webControls clientscriptsLocation="/aspnet_client/{0}/{1}"/>
<webParts>
    <personalization>
        <providers>
            <add connectionstringName="LocalSqlServer" name="AspNetSqlPersonalizationProvider" />
        </providers>
        <authorization>
            <deny users="*" verbs="entersharedscope" />
            <allow users="*" verbs="modifystate" />
        </authorization>
    </personalization>
    <transformers>
        <add name="RowToFieldTransformer" type="System.Web.UI.WebControls.WebParts.RowToFieldTransformer" />
        <add name="RowToParametersTransformer" type="System.Web.UI.WebControls.WebParts.RowToParametersTransformer" />
    </transformers>
</webParts>
<trace enabled="false" pageoutput="false" requestLimit="40" localonly="true"/>
</system.web>

```

Figure 5. 353: Adding &lt;trace&gt; part

Step 4: Adding <remove name=“urlAuthorization”/> and <remove name=“FileAuthorization”/>



```

<!-->
</httpHandlers>
<httpModules>
    <add name="OutputCache" type="System.Web.Caching.OutputCacheModule" />
    <add name="Session" type="System.Web.SessionState.SessionStateModule" />
    <add name="WindowsAuthentication" type="System.Web.Security.WindowsAuthenticationModule" />
    <add name="FormsAuthentication" type="System.Web.Security.FormsAuthenticationModule" />
    <add name="PassportAuthentication" type="System.Web.Security.PassportAuthenticationModule" />
    <add name="RoleManager" type="System.Web.Security.RoleManagerModule" />
    <add name="UrlAuthorization" type="System.Web.Security.UrlAuthorizationModule" />
    <add name="FileAuthorization" type="System.Web.Security.FileAuthorizationModule" />
    <add name="AnonymousIdentification" type="System.Web.Security.AnonymousIdentificationModule" />
    <add name="Profile" type="System.Web.Profile.ProfileModule" />
    <add name="ErrorHandlerModule" type="System.Web.Mobile.ErrorHandlerModule" />
    <add name="ServiceModel" type="System.ServiceModel.Activation.HttpModule" />
    <remove name="UrlAuthorization" />
    <remove name="FileAuthorization" />
</httpModules>
<mobileControls sessionStateHistorySize="6" cookielessDataDictionaryType="System.Web.Mobile.CookielessDataDictionary" />
<device name="XhtmlDeviceAdapters" predicateClass="System.Web.UI.MobileControls.DeviceAdapters" />
<control name="System.Web.UI.MobileControls.Panel" adapter="System.Web.UI.MobileControls.Adapters" />
<control name="System.Web.UI.MobileControls.Form" adapter="System.Web.UI.MobileControls.Adapters" />

```

Figure 5. 354: Adding &lt;remove&gt; part

Step 5: Binding site https to www.group1.com

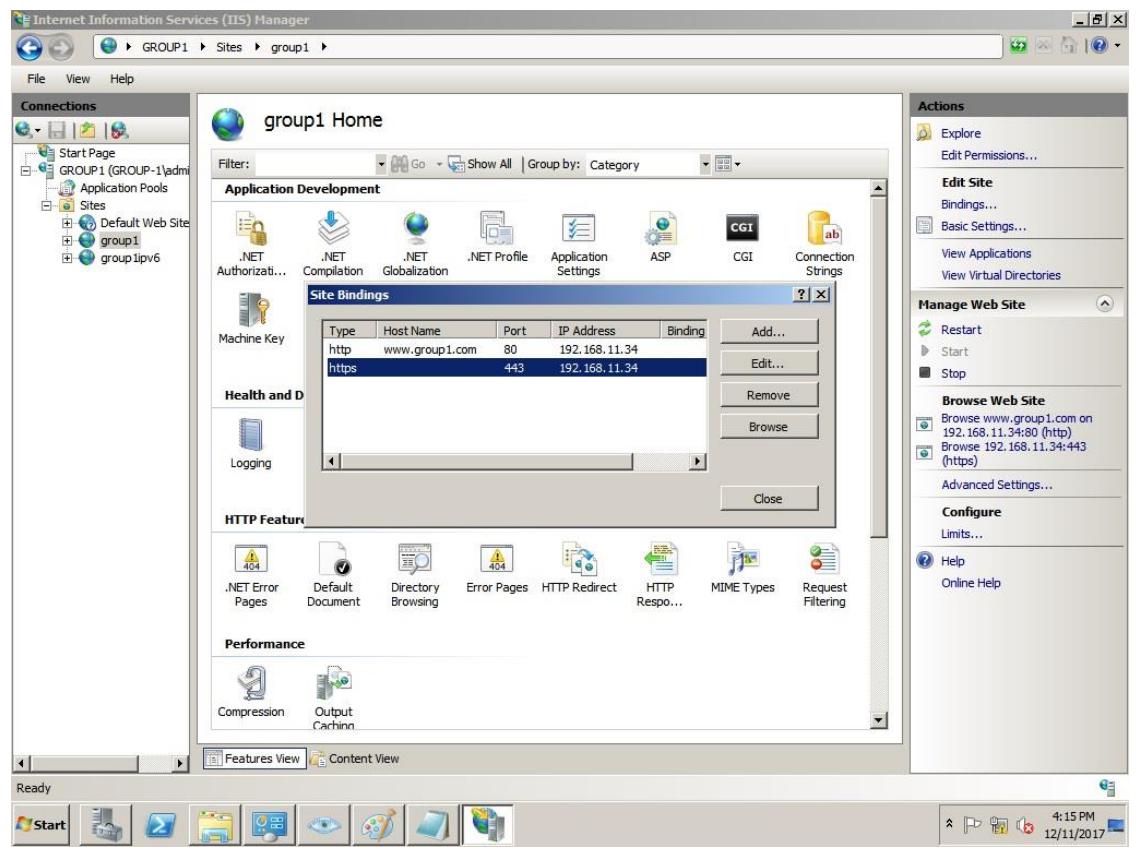


Figure 5. 355: Adding https

Step 6: Make sure that only port 80 and 443 are allowed for web.

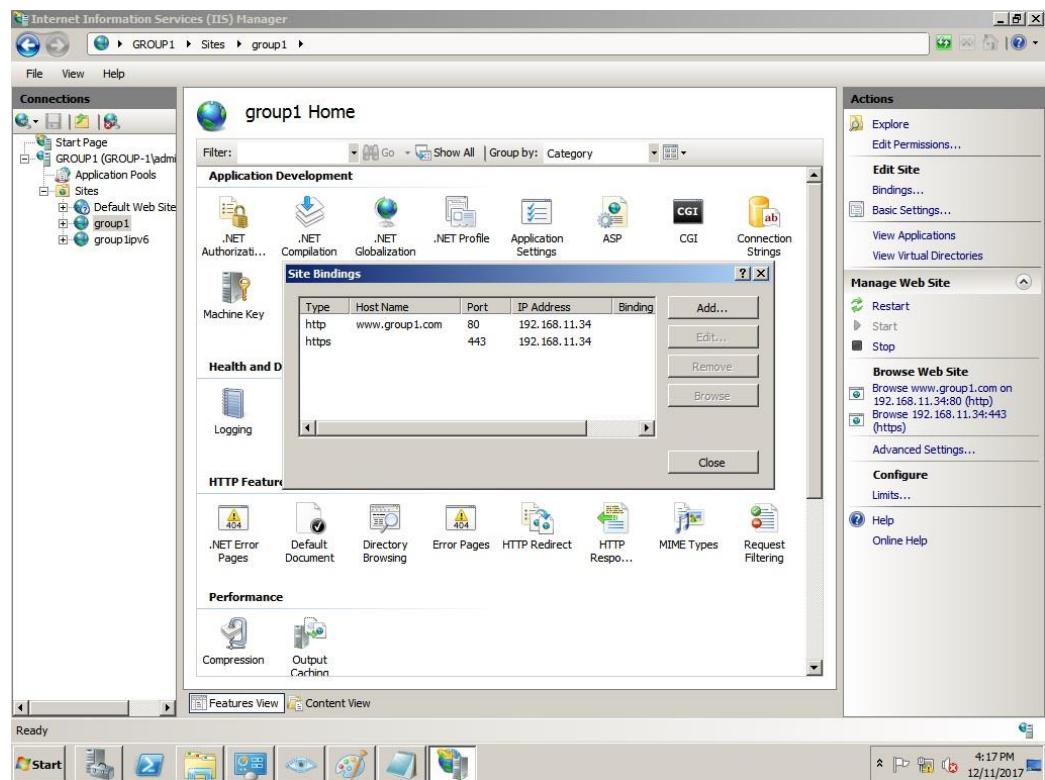


Figure 5. 356: Allowed only port 80 and 443

Step 7: Ensure that IPsecs is formed in the network.

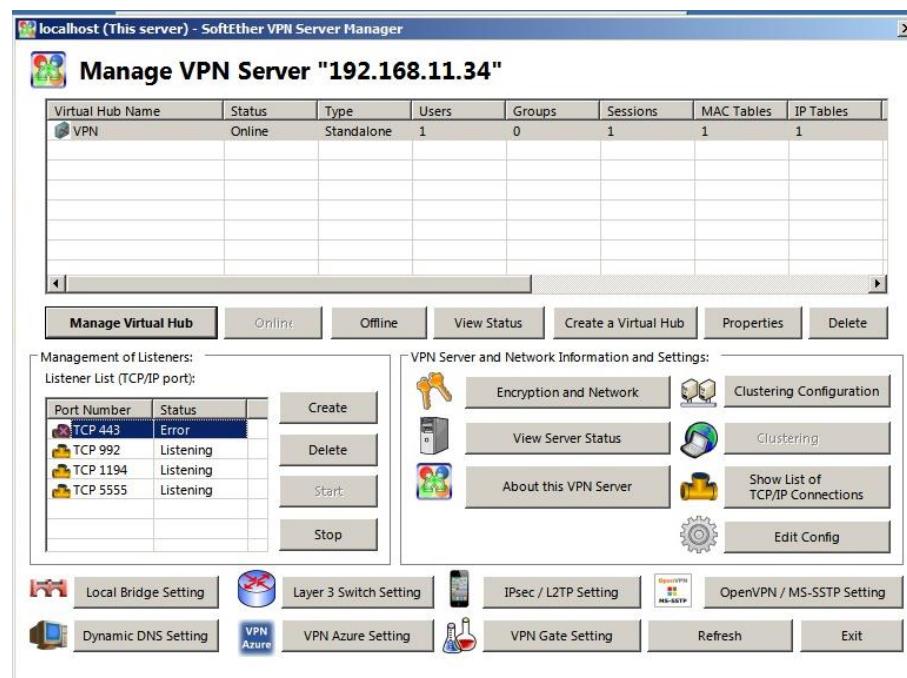


Figure 5. 357: Allowed IPsec

Step 8: Click on Start> Run> Type gpmc.msc

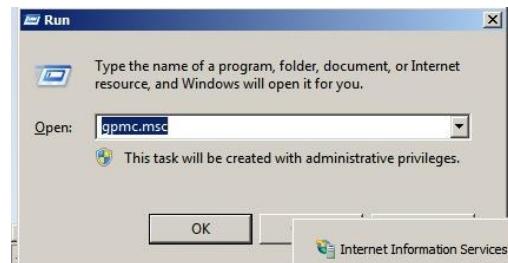


Figure 5. 358: Run Group Policy Management

Step 9: Right Click to edit Default Domain Policy

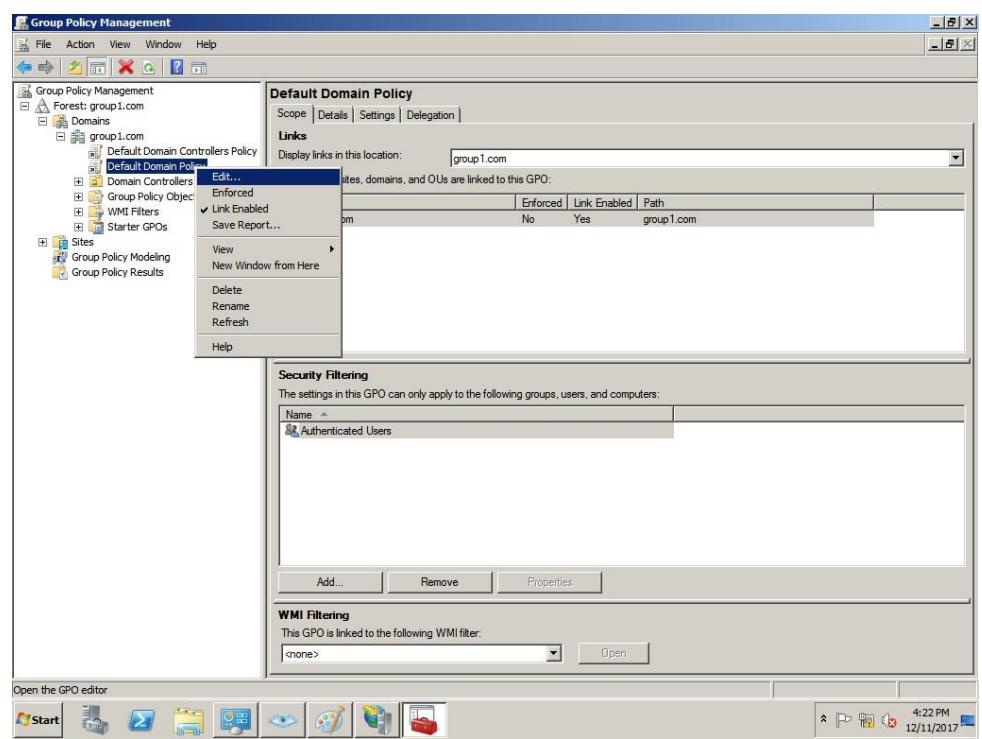


Figure 5. 359: Edit Default Domain Policy

Step 10: Click computer configuration

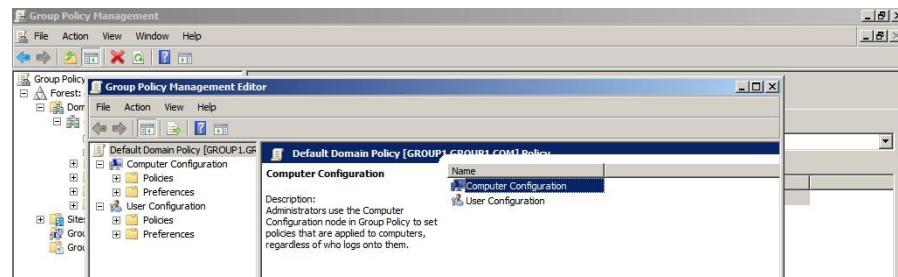


Figure 5. 360: Click computer configuration

Step 11: Click Windows Setting



Figure 5. 361: Click Windows Setting

Step 12: Select security setting

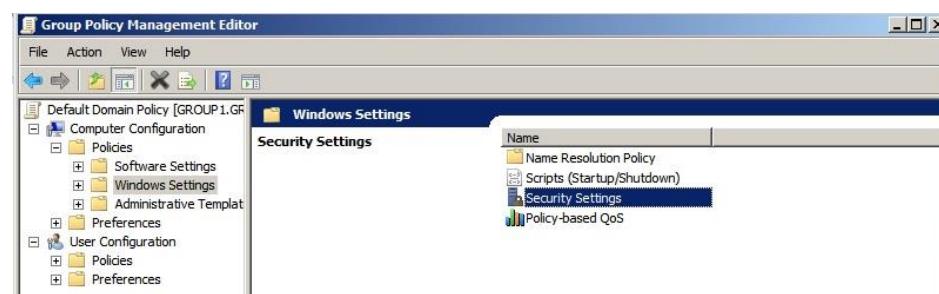


Figure 5. 362: Select Security Setting

Step 13: Select Local Policies



Figure 5. 363: Select Local Policies

#### Step 14: Select Audit Policy

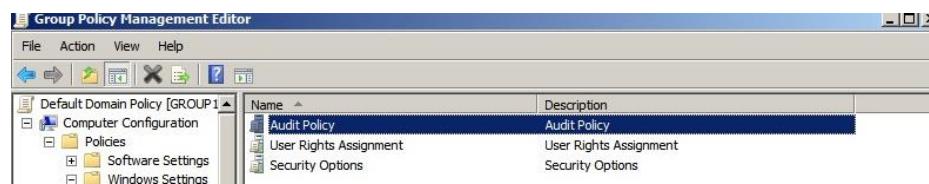


Figure 5. 364: Select Audit Policy

#### Step 15: Select Audit account logon events



Figure 5. 365: Select Audit account logon event

#### Step 16: Tick on both Success and Failure.

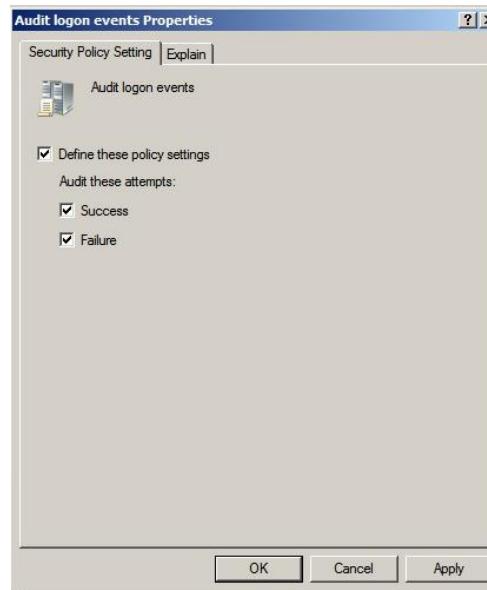


Figure 5. 366: Define the policy settings

Step 17: Update user policy by typing gpupdate/force in command prompt.

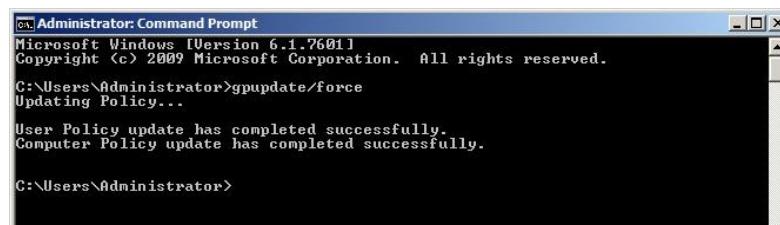


Figure 5. 367: Update User Policy

Step 18: Ensure anonymous logon is disabled.

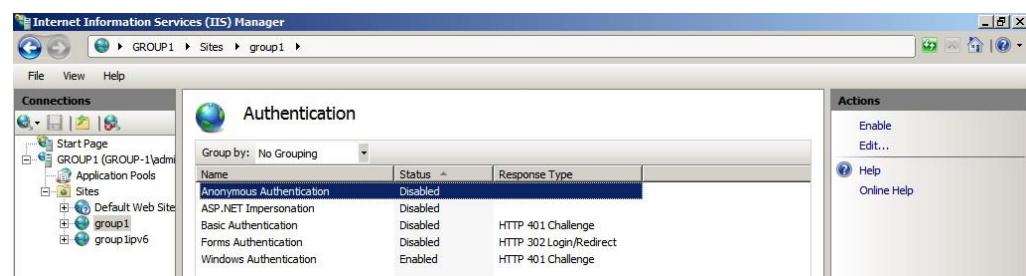


Figure 5. 368: Setting Authentication

Step 19: Open Administrative Tools> Services

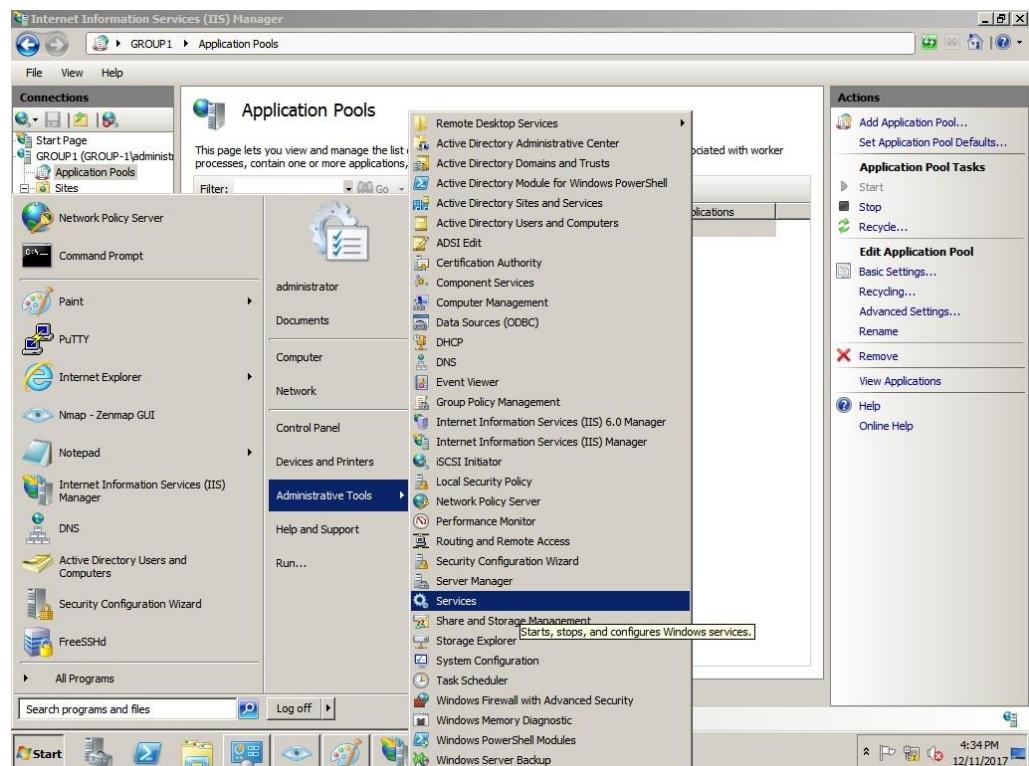


Figure 5. 369: Open Services

Step 20: Confirm ASP.NET state service is disabled.



Figure 5. 370: Disabled Startup Type

Step 21: Ensure Windows is updated.



Figure 5. 371: Update Windows

Step 22: Ensure .NET Framework is updated.

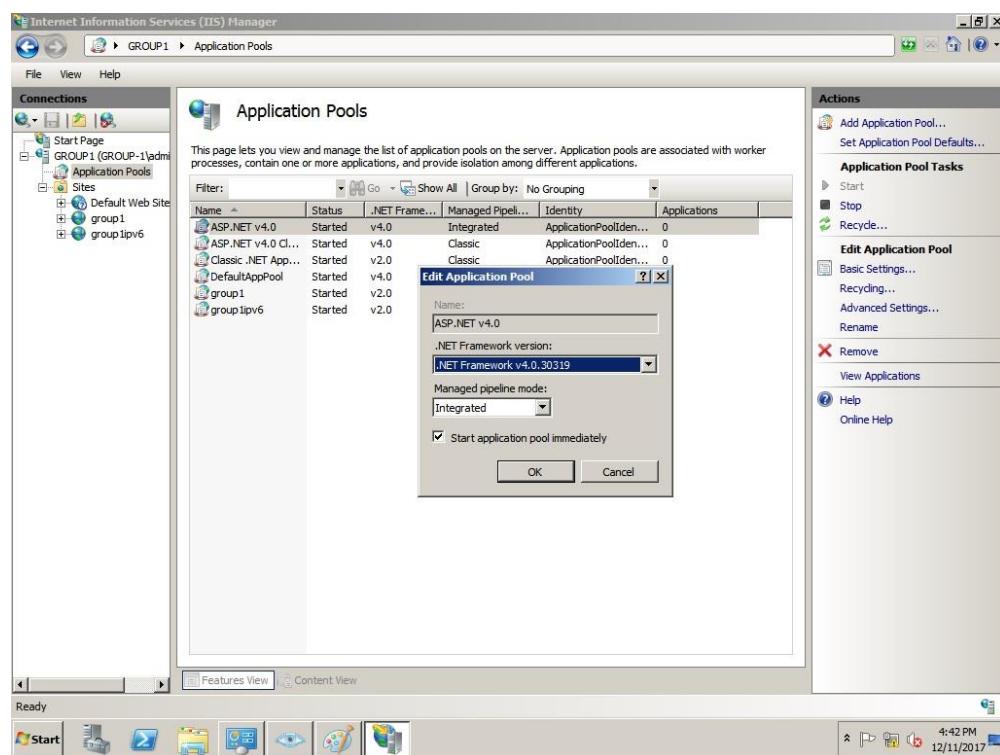


Figure 5. 372: Select version for .NET Framework

Step 23: Scan the port using Nmap.

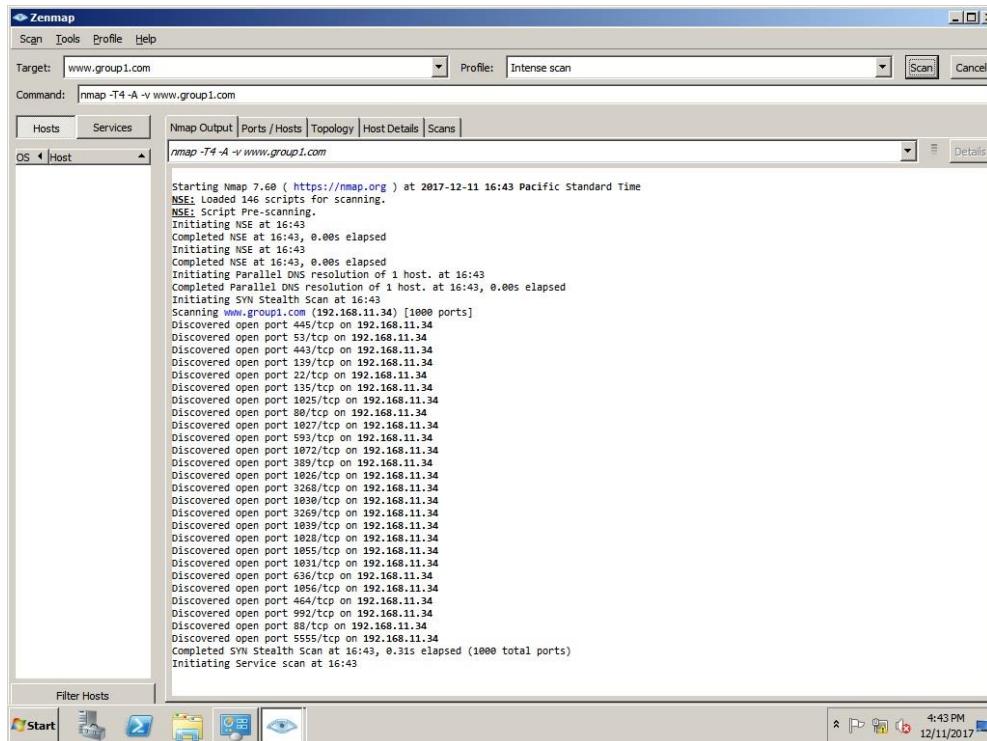


Figure 5. 373: Scan open port

Step 23: Go to Windows Firewall> Advance Setting> Add New Rule to block

specific port that are not in used.

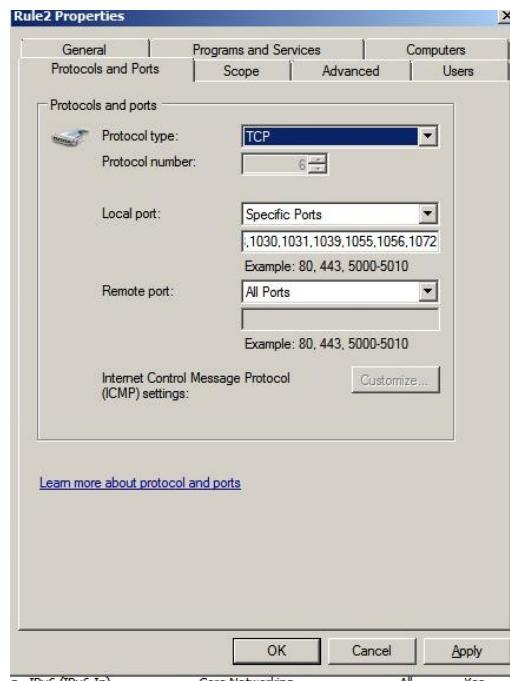


Figure 5. 374: Add a new rule to block specific port

Step 24: Rule 2 is created.

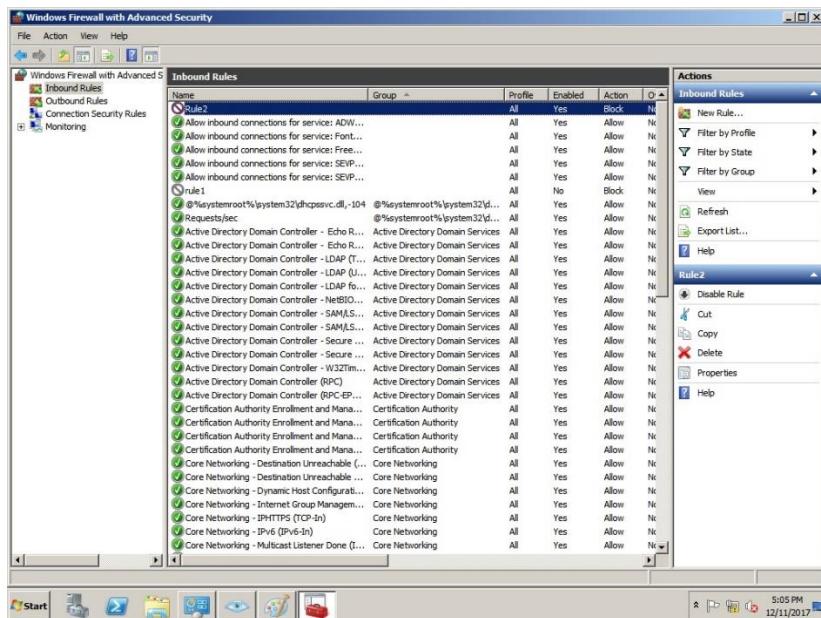


Figure 5. 375: New rule created

### 5.3.23 AUTHENTICATION USER BY INTEGRATING ACTIVE DIRECTORY WITH LINUX

Step 1: Open browser, search for Beyond Trust. Choose the PBIS Open-8.3 – Stable Releases, Linux Download Packages. Download the Linux 2.4/2/6 kernel 64-bit DEB. Click Download.

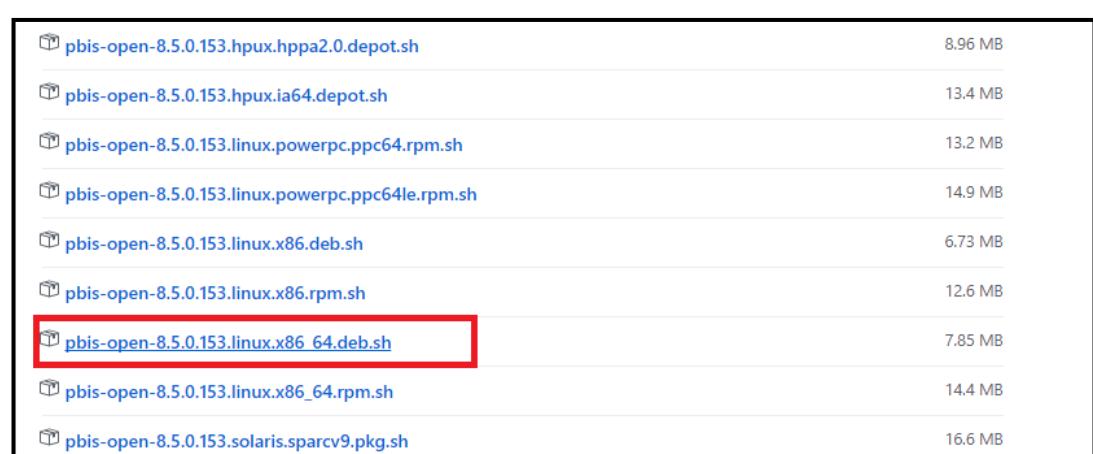
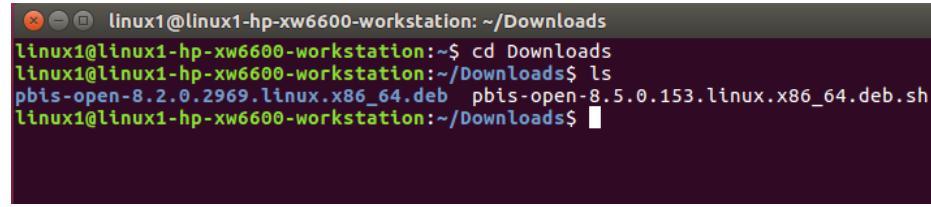


Figure 5. 376: Beyond Trust

Step 2: Press Ctrl+Alt+T to open Terminal. Then, open Downloads folder by entering the cd Downloads command. To list all the files and directories in this folder, type in the ls command.

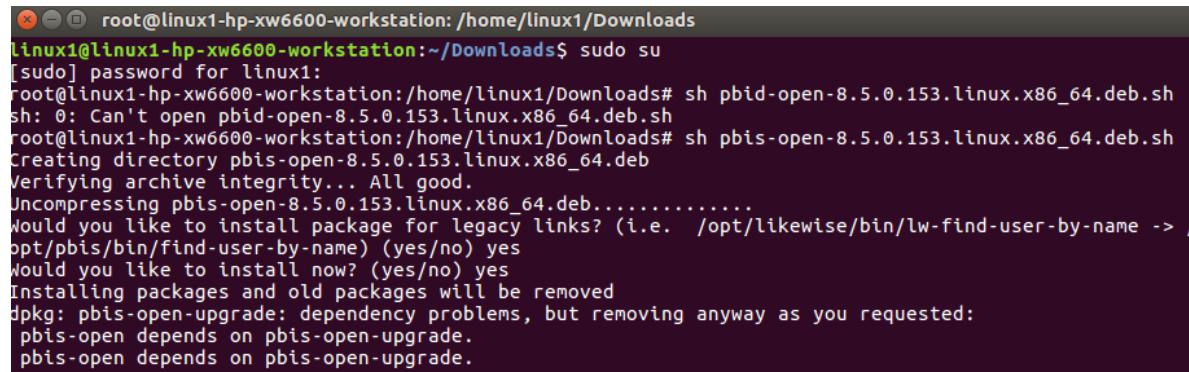


```
linux1@linux1-hp-xw6600-workstation:~/Downloads
linux1@linux1-hp-xw6600-workstation:~$ cd Downloads
linux1@linux1-hp-xw6600-workstation:~/Downloads$ ls
pbis-open-8.2.0.2969.linux.x86_64.deb  pbis-open-8.5.0.153.linux.x86_64.deb.sh
linux1@linux1-hp-xw6600-workstation:~/Downloads$
```

Figure 5. 377: List of all files and directories.

Step 3: To install the .deb file, go to root and the folder that contains .deb files.

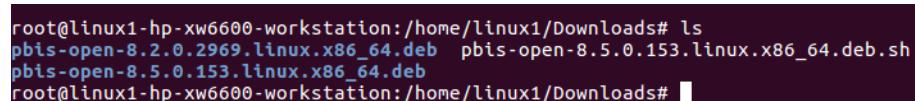
Enter the sh <file name.deb> command.



```
root@linux1-hp-xw6600-workstation:/home/linux1/Downloads
root@linux1-hp-xw6600-workstation:~/Downloads$ sudo su
[sudo] password for linux1:
root@linux1-hp-xw6600-workstation:/home/linux1/Downloads# sh pbid-open-8.5.0.153.linux.x86_64.deb.sh
sh: 0: Can't open pbid-open-8.5.0.153.linux.x86_64.deb.sh
root@linux1-hp-xw6600-workstation:/home/linux1/Downloads# sh pbis-open-8.5.0.153.linux.x86_64.deb.sh
Creating directory pbis-open-8.5.0.153.linux.x86_64.deb
Verifying archive integrity... All good.
Uncompressing pbis-open-8.5.0.153.linux.x86_64.deb.....
Would you like to install package for legacy links? (i.e. /opt/likewise/bin/lw-find-user-by-name -> /opt/pbis/bin/find-user-by-name) (yes/no) yes
Would you like to install now? (yes/no) yes
Installing packages and old packages will be removed
dpkg: pbis-open-upgrade: dependency problems, but removing anyway as you requested:
  pbis-open depends on pbis-open-upgrade.
  pbis-open depends on pbis-open-upgrade.
```

Figure 5. 378: Go to root

Step 4: After the installing is successful, the directory .deb will appear.



```
root@linux1-hp-xw6600-workstation:/home/linux1/Downloads# ls
pbis-open-8.2.0.2969.linux.x86_64.deb  pbis-open-8.5.0.153.linux.x86_64.deb.sh
root@linux1-hp-xw6600-workstation:/home/linux1/Downloads#
```

Figure 5. 379: Directory .deb appears in CLI

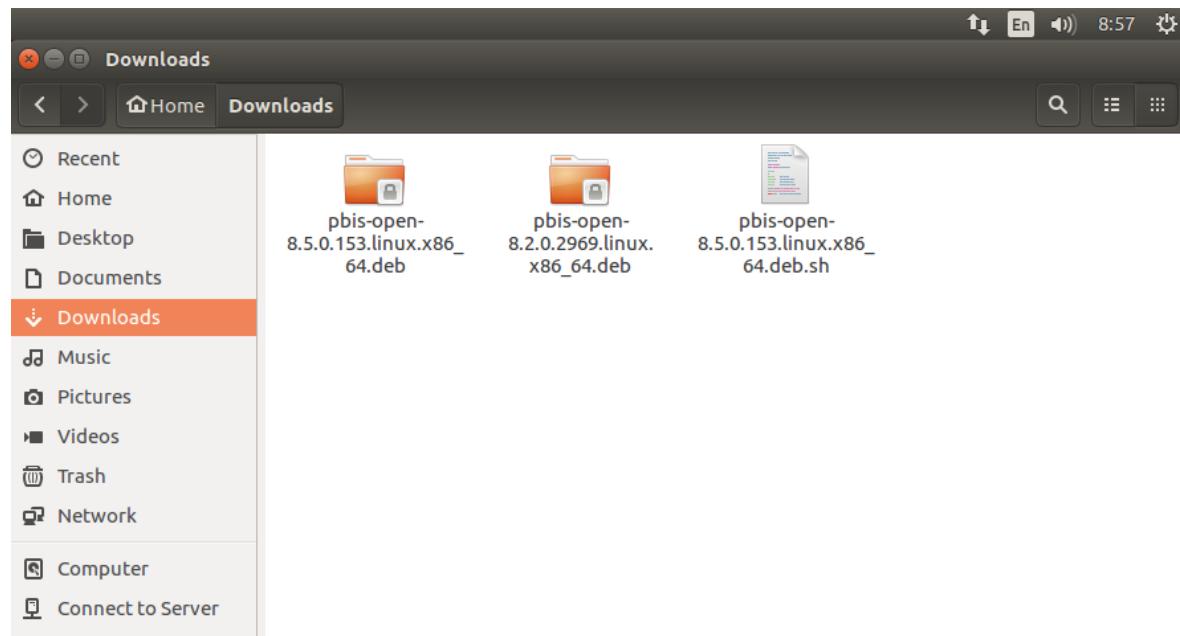


Figure 5. 380: Directory .deb appears in GUI

Step 5: Go to root by typing the sudo su- command. Drag the install.sh file which is located in the pbis-open-8.5.0.153.linux.x86\_64.deb folder into the Terminal.

Step 6: After dragging the install.sh file into the Terminal, add the install command at the back of the line.

```
root@linux1-hp-xw6600-workstation:/home/linux1/Downloads
root@linux1-hp-xw6600-workstation:/home/linux1/Downloads# '/home/linux1/Downloads/pbis-open-8.5.0.153.linux.x86_64.deb/install.sh' install
Installing packages and old packages will be removed
dpkg: pbis-open-upgrade: dependency problems, but removing anyway as you requested:
 pbis-open depends on pbis-open-upgrade.
 pbis-open depends on pbis-open-upgrade.

(Reading database ... 216650 files and directories currently installed.)
Removing pbis-open-upgrade (8.5.0.153) ...
Selecting previously unselected package pbis-open-upgrade.
(Reading database ... 216650 files and directories currently installed.)
Preparing to unpack .../pbis-open-upgrade_8.5.0.153_amd64.deb ...
Unpacking pbis-open-upgrade (8.5.0.153) ...
Setting up pbis-open-upgrade (8.5.0.153) ...
(Reading database ... 216650 files and directories currently installed.)
Removing pbis-open-legacy (8.5.0.153) ...
Removing pbis-open-gui (8.5.0.153) ...
Removing pbis-open (8.5.0.153) ...
Processing triggers for libc-bin (2.23-0ubuntu9) ...
Selecting previously unselected package pbis-open.
(Reading database ... 216247 files and directories currently installed.)
Preparing to unpack .../pbis-open_8.5.0.153_amd64.deb ...
Unpacking pbis-open (8.5.0.153) ...
"selected (36.4 kB)
```

Figure 5. 381: Installing pbis-open-8.5.0.153.

```

root@linux1-hp-xw6600-workstation: /home/linux1/Downloads
Setting up pbis-open-upgrade (8.5.0.153) ...
(Reading database ... 216650 files and directories currently installed.)
Removing pbis-open-legacy (8.5.0.153) ...
Removing pbis-open-gui (8.5.0.153) ...
Removing pbis-open (8.5.0.153) ...
Processing triggers for libc-bin (2.23-0ubuntu9) ...
Selecting previously unselected package pbis-open.
(Reading database ... 216247 files and directories currently installed.)
Preparing to unpack .../pbis-open_8.5.0.153_amd64.deb ...
Unpacking pbis-open (8.5.0.153) ...
Setting up pbis-open (8.5.0.153) ...
Importing registry...

Selecting previously unselected package pbis-open-gui.
(Reading database ... 216598 files and directories currently installed.)
Preparing to unpack .../pbis-open-gui_8.5.0.153_amd64.deb ...
Unpacking pbis-open-gui (8.5.0.153) ...
Setting up pbis-open-gui (8.5.0.153) ...
Installing Packages was successful

New libraries and configurations have been installed for PAM and NSS.
Please reboot so that all processes pick up the new versions.

As root, run domainjoin-gui or domainjoin-cli to join a domain so you can log on
with Active Directory credentials. Example:
domainjoin-cli join MYDOMAIN.COM MyJoinAccount

root@linux1-hp-xw6600-workstation:/home/linux1/Downloads# 
```

Figure 5. 382: Done installing.

Step 7: From root, go to directory /opt/pbis/bin by using the cd /opt/pbis/bin command. It will list all the domain files and directories.

```

root@linux1-hp-xw6600-workstation: /opt/pbis/bin
root@linux1-hp-xw6600-workstation:/home/linux1/Downloads# cd /opt/pbis/bin
root@linux1-hp-xw6600-workstation:/opt/pbis/bin# ls domain*
domainjoin-cli domainjoin-gui
root@linux1-hp-xw6600-workstation:/opt/pbis/bin# 
```

Figure 5. 383: domainjoin-cli

Step 8: to join domain by using command line interface, open the domainjoin-cli by entering these commands:

- cd /opt/pbis/bin/
- sudo domainjoin-cli join DOMAIN\_NAME USER

Where DOMAIN\_NAME is the name of the Windows domain that wants to join and USER is the user to authenticate with.

EXAMPLE: sudo domainjoin-cli join group1.com Administrator

Step 9: When prompted for the user's password, type in the appropriate credentials. Upon the successful authentication, a SUCSES message will appear at the end of console. Therefore, the joining of Ubuntu client to Windows domain is successful.

```
root@linux1-hp-xw6600-workstation:/opt/pbis/bin# sudo domainjoin-cli join group1.com Administrator
Joining to AD Domain: group1.com
With Computer DNS Name: linux1-hp-xw6600-workstation.group1.com

Administrator@GROUP1.COM's password:
Warning: System restart required
Your system has been configured to authenticate to Active Directory for the first time. It is
recommended that you restart your system to ensure that all applications recognize the new settings.

SUCCESS
```

Figure 5. 384: Successfully joined the Active Directory domain.

Step 10: After joining the domain, it is a must to restart the machines to make sure a number of daemons restart in a specific sequence.

Step 11: Once the Ubuntu machine has successfully joined the Active Directory domain, now we can login using any valid AD user on the local machine.

The domainjoin-cli utility can also be used to leave the domain. For example:

```
#sudo domainjoin-cli leave
```

### **5.3.24 INTRUSION DETECTION SYSTEM (PORT MIRROR)**

#### **Installing the Snort Pre-Requisites**

First, we need to install all the tools required for building software.

```
linux1@linux1-hp-xw6600-workstation:~$ sudo apt-get install -y build-essential
Reading package lists... Done
Building dependency tree
Reading state information... Done
build-essential is already the newest version (12.1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 22 not upgraded.
linux1@linux1-hp-xw6600-workstation:~$
```

Figure 5. 385: Install all tools

Install all Snort pre-requisites that are available from the Ubuntu repositories.

```
linux1@linux1-hp-xw6600-workstation:~$ sudo apt-get install -y libpcap-dev libpcre3-dev libdumbnet-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
libdumbnet-dev is already the newest version (1.12-7).
libpcap-dev is already the newest version (1.7.4-2).
libpcre3-dev is already the newest version (2:8.38-3.1).
0 upgraded, 0 newly installed, 0 to remove and 22 not upgraded.
linux1@linux1-hp-xw6600-workstation:~$
```

Figure 5. 386: Install all snort pre-requisites

Install a few pre-requisites of the Snort DAQ (Data AcQuisition library) that are needed.

```
linux1@linux1-hp-xw6600-workstation:~$ sudo apt-get install -y bison flex
Reading package lists... Done
Building dependency tree
Reading state information... Done
bison is already the newest version (2:3.0.4.dfsg-1).
flex is already the newest version (2.6.0-11).
0 upgraded, 0 newly installed, 0 to remove and 22 not upgraded.
linux1@linux1-hp-xw6600-workstation:~$
```

Figure 5. 387: Install a few pre-requisites of Snort DAQ

Create a folder called snort\_src to keep them all in one place

```
linux1@linux1-hp-xw6600-workstation:~$ mkdir ~/snort_src
mkdir: cannot create directory '/home/linux1/snort_src': File exists
linux1@linux1-hp-xw6600-workstation:~$
```

Figure 5. 388: Create folder

Change the directory to snort\_src folder

```
linux1@linux1-hp-xw6600-workstation: ~/snort_src
linux1@linux1-hp-xw6600-workstation:~$ cd ~/snort_src
```

Figure 5. 389: Change Directory

Download and install the latest version of DAQ from the snort website. Browse this link <https://snort.org/downloads/snort/daq-2.0.6.tar.gz> and drag the downloaded file into the terminal.

```
linux1@linux1-hp-xw6600-workstation: ~/snort_src/daq-2.0.6
linux1@linux1-hp-xw6600-workstation:~/snort_src$ tar -xvzf '/home/linux1/Downloads/daq-2.0.6.tar.gz'
daq-2.0.6/
daq-2.0.6/ChangeLog
daq-2.0.6/missing
daq-2.0.6/daq.dsp
```

Figure 5. 390: Install DAQ

After finish installing, change directory to daq-2.0.6.tar.gz.

```
linux1@linux1-hp-xw6600-workstation: ~/snort_src/daq-2.0.6
linux1@linux1-hp-xw6600-workstation:~/snort_src$ cd daq-2.0.6
linux1@linux1-hp-xw6600-workstation:~/snort_src/daq-2.0.6$ ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
```

Figure 5. 391: Change directory to DAQ

Check if everything needed is already exist. Then, insert command “make”. After this step, the executable of this specific application you are trying to install will be created. Moves all the needed for the application files to the appropriate system directories.

```
linux1@linux1-hp-xw6600-workstation:~/snort_src/daq-2.0.6$ ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
```

Figure 5. 392: Check everything needed

You should see the following output that shows which modules are being configured and which will be available when you compile DAQ:

```
Build AFPacket DAQ module.. : yes
Build Dump DAQ module..... : yes
Build IPFW DAQ module..... : yes
Build IPQ DAQ module..... : no
Build NFQ DAQ module..... : no
Build PCAP DAQ module..... : yes
Build netmap DAQ module.... : no
```

Figure 5. 393: Modules being configured

```
linux1@linux1-hp-xw6600-workstation:~/snort_src/daq-2.0.6$ make
make all-recurisve
make[1]: Entering directory '/home/linux1/snort_src/daq-2.0.6'
Making all in api
make[2]: Entering directory '/home/linux1/snort_src/daq-2.0.6/api'
/bin/bash ..../libtool --tag=CC --mode=compile gcc -DHAVE_CONFIG_H -I. -I.. -I/usr/include -g -O2 -fvisibility=hidden -Wall -Wwrite-strings -Wsign-compare -Wcast-align -Wextra -Wformat -Wformat-security -Wno-unused-parameter -fno-strict-aliasing -fdiagnostics-show-option -pedantic -std=c99 -D_GNU_SOURCE -MT daq_base.lo -MD -MP -MF .deps/daq_base.Tpo -c -o daq_base.lo daq_base.c
```

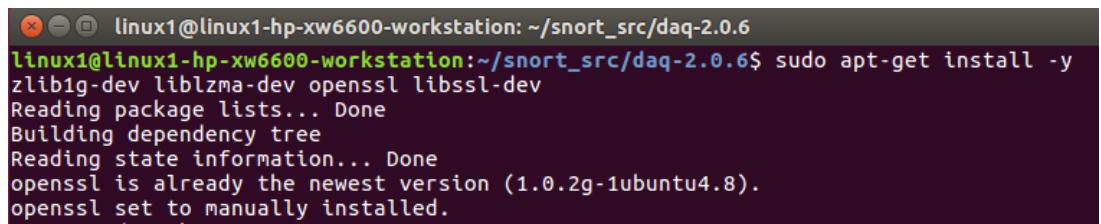
Figure 5. 394: Executable of this specific application created

```
linux1@linux1-hp-xw6600-workstation:~/snort_src/daq-2.0.6$ sudo make install
[sudo] password for linux1:
Access denied
Access denied
Making install in api
make[1]: Entering directory '/home/linux1/snort_src/daq-2.0.6/api'
make[2]: Entering directory '/home/linux1/snort_src/daq-2.0.6/api'
/bin/mkdir -p '/usr/local/lib'
/bin/bash ..../libtool --mode=install /usr/bin/install -c libdaq.la libdaq_statis.la '/usr/local/lib'
libtool: install: /usr/bin/install -c .libs/libdaq.so.2.0.4 /usr/local/lib/libdaq.so.2.0.4
libtool: install: (cd /usr/local/lib && { ln -s -f libdaq.so.2.0.4 libdaq.so.2 } || {
```

Figure 5. 395: Make install in API

## Installing snort

To install Snort on Ubuntu, there is one additional required pre-requisite that needs to be installed that is not mentioned in the documentation: zlib which is a compression library. There are four optional libraries that improves functionality: liblzma-dev three of which provide decompression of swf files (adobe flash), openssl, and libssl-dev which both provide SHA and MD5 file signatures:



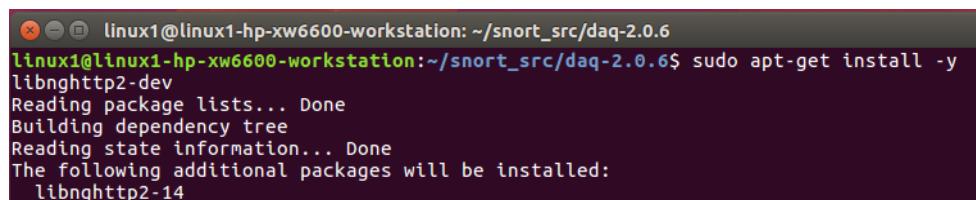
```
linux1@linux1-hp-xw6600-workstation: ~/snort_src/daq-2.0.6
linux1@linux1-hp-xw6600-workstation:~/snort_src/daq-2.0.6$ sudo apt-get install -y
zlib1g-dev liblzma-dev openssl libssl-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssl is already the newest version (1.0.2g-1ubuntu4.8).
openssl set to manually installed.
```

Figure 5. 396: Install additional pre-requisites

Finally, we need the development libraries for Nghttp2: a HTTP/2 C Library which implements the HPAC header compression algorithm. In Ubuntu 16 the install is easy:

# Ubuntu 16 only (not Ubuntu 14)

sudo apt-get install -y libnghttp2-dev



```
linux1@linux1-hp-xw6600-workstation: ~/snort_src/daq-2.0.6
linux1@linux1-hp-xw6600-workstation:~/snort_src/daq-2.0.6$ sudo apt-get install -y
libnghttp2-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
libnghttp2-14
```

Figure 5. 397: Install libnghttp2-14

Once all pre-requisites are installed, we are ready to download the Snort source tarball, compile, and then install. The --enable-sourcefire option gives Packet Performance Monitoring (PPM)<sup>4</sup> <sup>5</sup>, which lets us do performance monitoring

for rules and pre-processors, and builds Snort the same way that the Snort team does:

```
linux1@linux1-hp-xw6600-workstation:~/snort_src/daq-2.0.6$ cd ~/snort_src
linux1@linux1-hp-xw6600-workstation:~/snort_src$
```

Figure 5. 398: Change Directory

Download and install the latest version of DAQ from the snort website. Browse this link <https://snort.org/downloads/snort/snort-2.9.9.0.tar.gz> and drag the downloaded file into the terminal.

```
linux1@linux1-hp-xw6600-workstation:~/snort_src$ tar -xvzf '/home/linux1/Downloads/snort-2.9.9.0.tar.gz'
snort-2.9.9.0/
snort-2.9.9.0/depcomp
snort-2.9.9.0/tools/
snort-2.9.9.0/tools/u2streamer/
snort-2.9.9.0/tools/u2streamer/sf_error.h
snort-2.9.9.0/tools/u2streamer/sf_error.c
snort-2.9.9.0/tools/u2streamer/UnifiedLog.h
snort-2.9.9.0/tools/u2streamer/UnifiedLog.c
snort-2.9.9.0/tools/u2streamer/TimestampedFile.h
```

Figure 5. 399: Install DAQ

```
linux1@linux1-hp-xw6600-workstation:~/snort_src$ cd snort-2.9.9.0
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0$
```

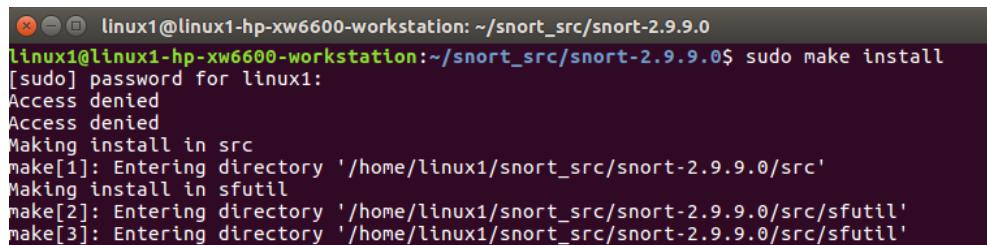
Figure 5. 400: Change Directory

```
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0$ ./configure --enable-sourcefire
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... no
checking for mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
```

Figure 5. 401: Enables sourcesfire

```
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0$ make
make all-recursive
make[1]: Entering directory '/home/linux1/snort_src/snort-2.9.9.0'
Making all in src
make[2]: Entering directory '/home/linux1/snort_src/snort-2.9.9.0/src'
Making all in sfutil
```

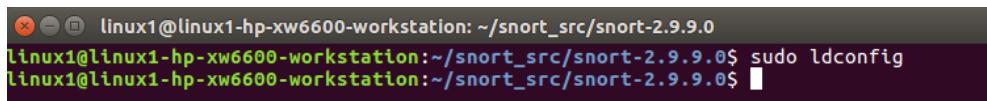
Figure 5. 402: Executable of this specific application created



```
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0$ sudo make install
[sudo] password for linux1:
Access denied
Access denied
Making install in src
make[1]: Entering directory '/home/linux1/snort_src/snort-2.9.9.0/src'
Making install in sfutil
make[2]: Entering directory '/home/linux1/snort_src/snort-2.9.9.0/src/sfutil'
make[3]: Entering directory '/home/linux1/snort_src/snort-2.9.9.0/src/sfutil'
```

Figure 5. 403: Make install in API

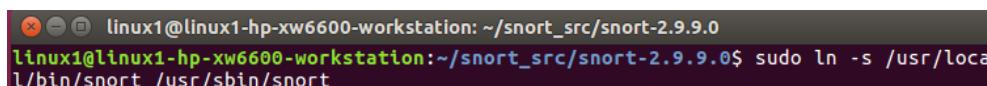
Run the following command to update shared libraries (you'll get an error when you try to run Snort if you skip this step):



```
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0$ sudo ldconfig
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0$
```

Figure 5. 404: Update shared libraries

Place a symlink to the Snort binary in /usr/sbin:



```
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0$ sudo ln -s /usr/local/bin/snort /usr/sbin/snort
```

Figure 5. 405: Place to /usr/bin

Test Snort by running the binary as a regular user, passing it the -V flag (which tells Snort to verify itself and any configuration files passed to it). You should see output similar to what is shown below (although exact version numbers may be slightly different):

```
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0$ snort -V
      _*-> Snort! <*-
o'`_)~ Version 2.9.9.0 GRE (Build 56)
     By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
     Copyright (C) 2014-2016 Cisco and/or its affiliates. All rights reserved

     Copyright (C) 1998-2013 Sourcefire, Inc., et al.
     Using libpcap version 1.7.4
     Using PCRE version: 8.38 2015-11-23
     Using ZLIB version: 1.2.8

linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0$
```

Figure 5. 406: Test snort

Since we don't want Snort to run as root, we need to create an unprivileged account and group for the daemon to run under (snort:snort). We will also create a number of files and directories required by Snort, and set permissions on those files. Snort will have the following directories: Configurations and rule files in /etc/snort Alerts will be written to /var/log/snort Compiled rules (.so rules) will be stored in /usr/local/lib/snort dynamicrules

Create the snort user and group:

```
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0$ sudo groupadd snort
```

Figure 5. 407: Create snort group

```
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0$ sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort
```

Figure 5. 408: Create snort user

Create the Snort directories:

```
linux1@linux1-hp-xw6600-workstation:~$ sudo mkdir /etc/snort
[sudo] password for linux1:
```

Figure 5. 409: Create /etc/snort

```
linux1@linux1-hp-xw6600-workstation:~$ sudo mkdir /etc/snort/rules
```

Figure 5. 410: Create /etc/snort/rules

```
linux1@linux1-hp-xw6600-workstation:~$ sudo mkdir /etc/snort/rules/iplists
```

Figure 5. 411: Create /etc/snort/rules/iplists

```
linux1@linux1-hp-xw6600-workstation:~$ sudo mkdir /etc/snort/preproc_rules
```

Figure 5. 412: Create /etc/snort/preproc\_rules

```
linux1@linux1-hp-xw6600-workstation:~$ sudo mkdir /usr/local/lib/snort_dynamicrules
```

Figure 5. 413: Create /usr/local/lib/snort\_dynamicrules

```
linux1@linux1-hp-xw6600-workstation:~$ sudo mkdir /etc/snort/so_rules
```

Figure 5. 414: Create /etc/snort/so\_rules

Create some files that stores rules and IP lists:

```
linux1@linux1-hp-xw6600-workstation:~$ sudo touch /etc/snort/rules/blklist.rules
linux1@linux1-hp-xw6600-workstation:~$ sudo touch /etc/snort/rules/wlalist.rules
linux1@linux1-hp-xw6600-workstation:~$ sudo touch /etc/snort/rules/local.rules
linux1@linux1-hp-xw6600-workstation:~$ sudo touch /etc/snort/sid-msg.map
linux1@linux1-hp-xw6600-workstation:~$
```

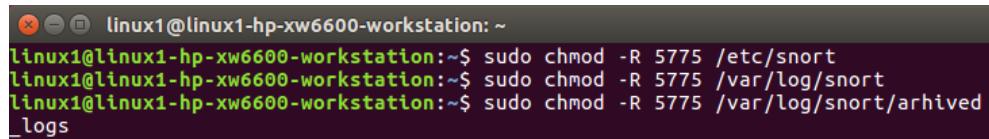
Figure 5. 415: Create file to store rules

Create our logging directories:

```
linux1@linux1-hp-xw6600-workstation:~$ sudo mkdir /var/log/snort
mkdir: cannot create directory '/var/log/snort': File exists
linux1@linux1-hp-xw6600-workstation:~$ sudo mkdir /var/log/snort/archived_logs
linux1@linux1-hp-xw6600-workstation:~$
```

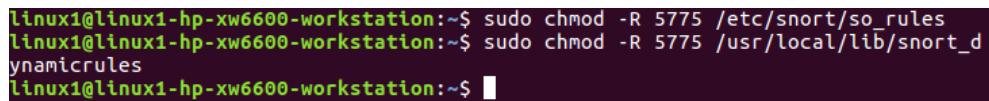
Figure 5. 416: Create logging directory

Adjust permissions:



```
linux1@linux1-hp-xw6600-workstation:~$ sudo chmod -R 5775 /etc/snort
linux1@linux1-hp-xw6600-workstation:~$ sudo chmod -R 5775 /var/log/snort
linux1@linux1-hp-xw6600-workstation:~$ sudo chmod -R 5775 /var/log/snort/archived_logs
```

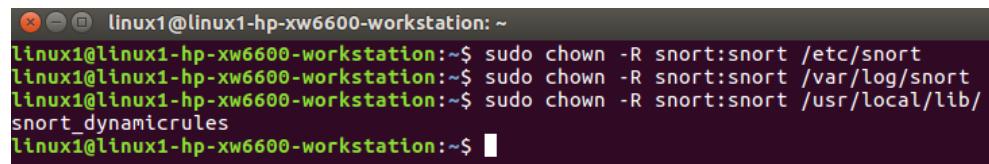
Figure 5. 417: Adjust permission



```
linux1@linux1-hp-xw6600-workstation:~$ sudo chmod -R 5775 /etc/snort/so_rules
linux1@linux1-hp-xw6600-workstation:~$ sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
linux1@linux1-hp-xw6600-workstation:~$ 
```

Figure 5. 418: Adjust permission

We want to change ownership of the files we created above as well to make sure Snort can access the files it uses



```
linux1@linux1-hp-xw6600-workstation:~$ sudo chown -R snort:snort /etc/snort
linux1@linux1-hp-xw6600-workstation:~$ sudo chown -R snort:snort /var/log/snort
linux1@linux1-hp-xw6600-workstation:~$ sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules
linux1@linux1-hp-xw6600-workstation:~$ 
```

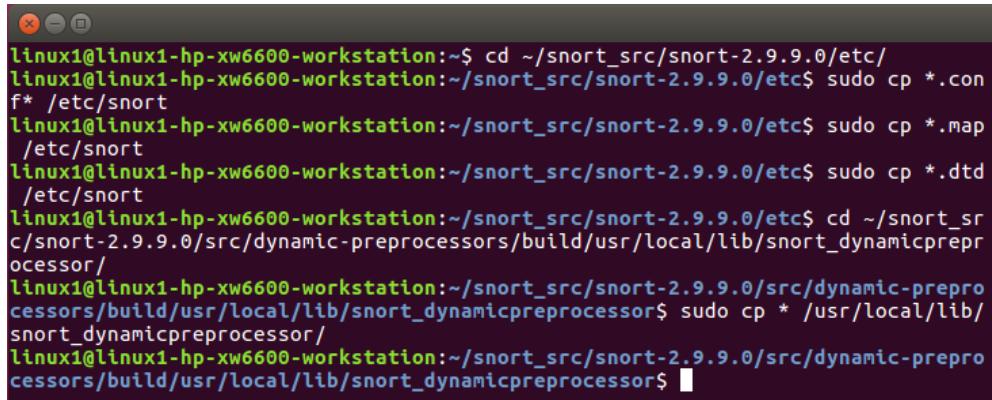
Figure 5. 419: Change owner

Snort needs some configuration files and the dynamic preprocessors copied from the Snort source tarball into the /etc/snort folder. The configuration files are:

- classification.config
- file magic.conf
- reference.config
- snort.conf
- threshold.conf
- attribute table.dtd

- gen-msg.map
- unicode.map

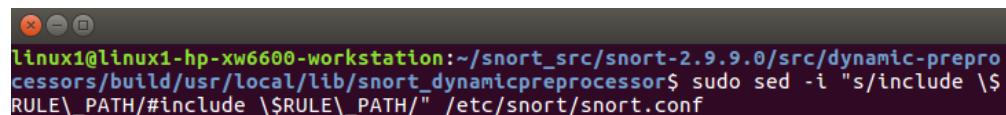
To copy the configuration files and the dynamic preprocessors, run the following commands



```
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0/etc$ cd ~/snort_src/snort-2.9.9.0/etc/
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0/etc$ sudo cp *.conf /etc/snort
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0/etc$ sudo cp *.map /etc/snort
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0/etc$ sudo cp *.dtd /etc/snort
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0/etc$ cd ~/snort_src/snort-2.9.9.0/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicprocessor/
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicprocessor$ sudo cp * /usr/local/lib/snort_dynamicprocessor/
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicprocessor$
```

Figure 5. 420: Copy configuration files

We now need to edit Snort's main configuration file, /etc/snort/snort.conf. When we run Snort with this file as an argument, it tells Snort to run in NIDS mode. We need to comment out all of the individual rule files that are referenced in the Snort configuration file, since instead of downloading each file individually, we will use PulledPork to manage our rulesets, which combines all the rules into a single file. The following line will comment out all rulesets in our snort.conf file (there are about 100 lines to comment out, beginning at line 540):



```
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicprocessor$ sudo sed -i "s/include \$RULE_PATH/#include \$RULE_PATH/" /etc/snort/snort.conf
```

Figure 5. 421: Comment out all rulesets in snort.conf file

We will now manually change some settings in the snort.conf file, using your favourite editor:

```
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor$ sudo vim /etc/snort/snort.conf
```

Figure 5. 422: Change setting

Change the following lines to meet your environment: Line 45, HOME NET should match your internal (friendly) network. In the below example our HOME NET is 192.168.11.0 with a 24-bit subnet mask (255.255.255.0)

```
root@linux1-hp-xw6600-workstation: /etc/snort/rules
# 9) Customize shared object rule set
#####
##### Step #1: Set the network variables. For more information, see README.variables
#####
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.11.0/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

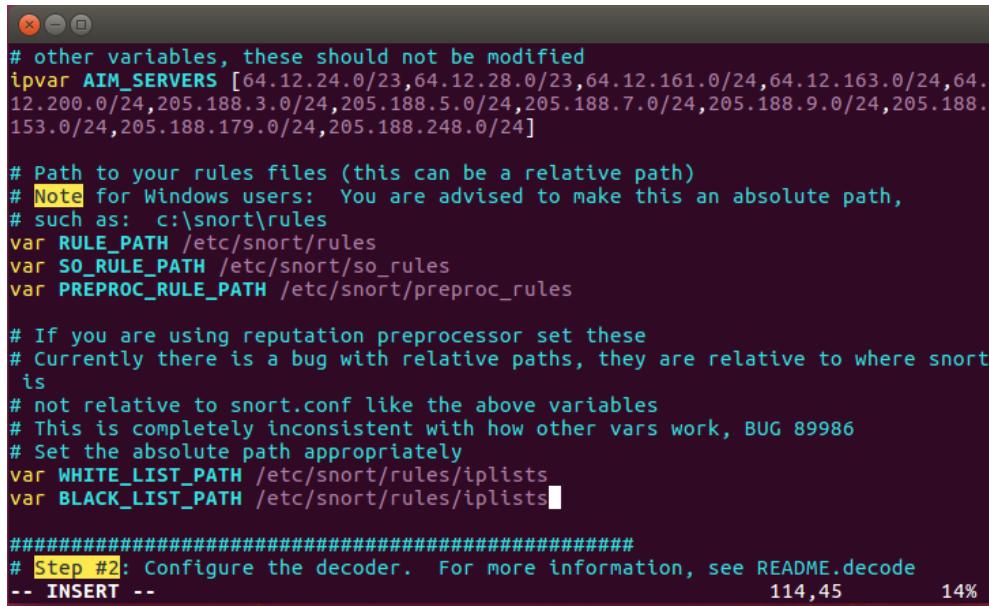
# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET
```

60,1                    5%

Figure 5. 423: Change line

Set the following file paths in snort.conf, beginning at line 104



```

# other variables, these should not be modified
ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.
12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.
153.0/24,205.188.179.0/24,205.188.248.0/24]

# Path to your rules files (this can be a relative path)
# Note for Windows users: You are advised to make this an absolute path,
# such as: c:\snort\rules
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

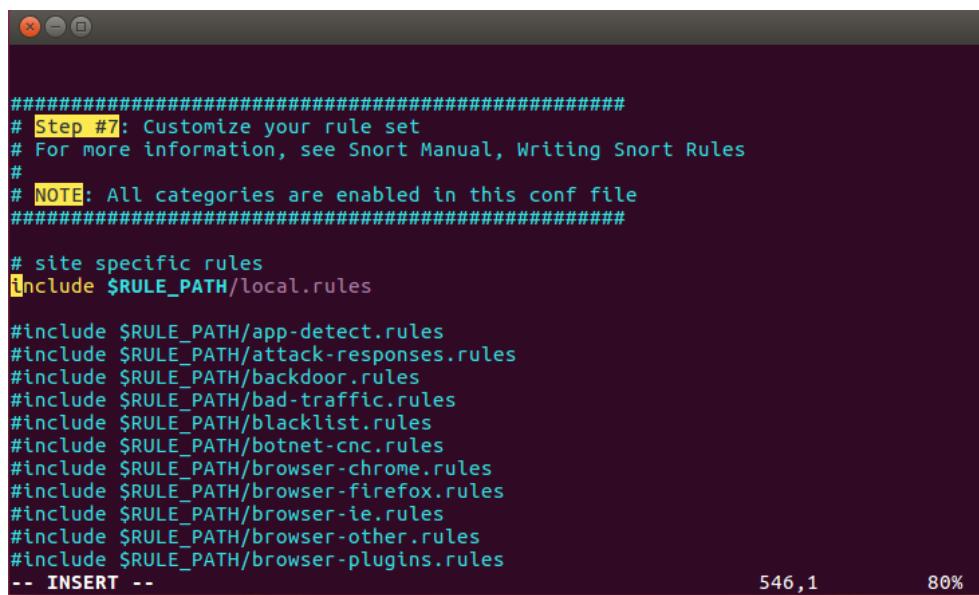
# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort
# is
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules/iplists
var BLACK_LIST_PATH /etc/snort/rules/iplists

#####
# Step #2: Configure the decoder. For more information, see README.decode
-- INSERT --           114,45      14%

```

Figure 5. 424: Edit snort.conf

In order to make testing Snort easy, we want to enable the local.rules file, where we can add rules that Snort can alert on. Un-comment (remove the hash symbol) from line 546 so it looks like this:



```

#####
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
#####

# site specific rules
#include $RULE_PATH/local.rules

#include $RULE_PATH/app-detect.rules
#include $RULE_PATH/attack-responses.rules
#include $RULE_PATH/backdoor.rules
#include $RULE_PATH/bad-traffic.rules
#include $RULE_PATH/blacklist.rules
#include $RULE_PATH/botnet-cnc.rules
#include $RULE_PATH/browser-chrome.rules
#include $RULE_PATH/browser-firefox.rules
#include $RULE_PATH/browser-ie.rules
#include $RULE_PATH/browser-other.rules
#include $RULE_PATH/browser-plugins.rules
-- INSERT --           546,1      80%

```

Figure 5. 425: Enable local.rules files

Do this following command to know our PC's interface

```
linux1@linux1-hp-xw6600-workstation:~$ ifconfig
enp14s0    Link encap:Ethernet HWaddr 00:1f:29:01:15:9e
            inet addr:192.168.11.42 Bcast:192.168.11.47 Mask:255.255.255.248
            inet6 addr: 2001:d::2/48 Scope:Global
              inet6 addr: fe80::4fa:6dc1:be23:cb05/64 Scope:Link
                UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                RX packets:2691058 errors:0 dropped:0 overruns:0 frame:0
                TX packets:22410 errors:0 dropped:0 overruns:0 carrier:0
                collisions:0 txqueuelen:1000
                RX bytes:283164647 (283.1 MB) TX bytes:2472630 (2.4 MB)
                Interrupt:16

lo         Link encap:Local Loopback
            inet addr:127.0.0.1 Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
              UP LOOPBACK RUNNING MTU:65536 Metric:1
              RX packets:8491 errors:0 dropped:0 overruns:0 frame:0
              TX packets:8491 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1
              RX bytes:636795 (636.7 KB) TX bytes:636795 (636.7 KB)

linux1@linux1-hp-xw6600-workstation:~$
```

Figure 5. 426: Check PC's interface

Once the configuration file is ready, we will have Snort verify that it is a valid file, and all necessary files it references are correct. We use the -T flag to test the configuration file, the -c flag to tell Snort which configuration file to use, and -i to specify the interface that Snort will listen on (this is a new requirement beginning with the 2.9.8.x version of Snort when active response is enabled).

Run sudo snort -T -c /etc/snort/snort.conf -i eth0. Run this command as shown below and look for the following output.

```
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor$ sudo snort -T -i enp14s0
-c /etc/snort/snort.conf
[sudo] password for linux1:
Running in Test mode

==== Initializing Snort ===-
```

Figure 5. 427: Verify snort

```
Snort successfully validated the configuration!
Snort exiting
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor$
```

Figure 5. 428: Check verification

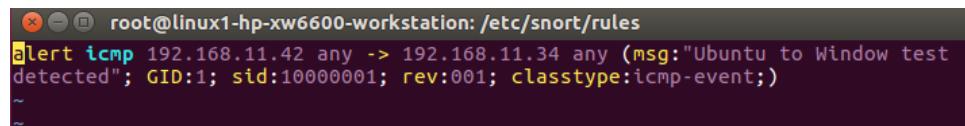
At this stage, Snort does not have any rules loaded (our rule files referenced in snort.conf are empty). To test Snort's detection abilities, let's create a simple rule that will cause Snort to generate an alert whenever Snort sees an ICMP "Echo request" or "Echo reply" message, which is easy to generate with the ubiquitous ping utility.



```
root@linux1-hp-xw6600-workstation: /etc/snort/rules
root@linux1-hp-xw6600-workstation:/etc/snort/rules# vim /etc/snort/rules/local.rules
```

Figure 5. 429: Edit /etc/snort/rules/local.rules

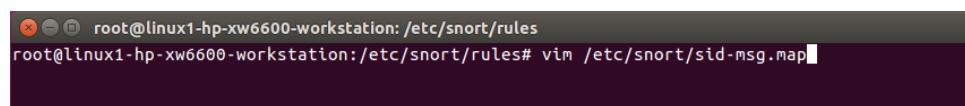
Paste the following single line into the empty local rules file: /etc/snort/rules/local.rules.



```
root@linux1-hp-xw6600-workstation: /etc/snort/rules
alert icmp 192.168.11.42 any -> 192.168.11.34 any (msg:"Ubuntu to Window test
detected"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)
```

Figure 5. 430: Insert line

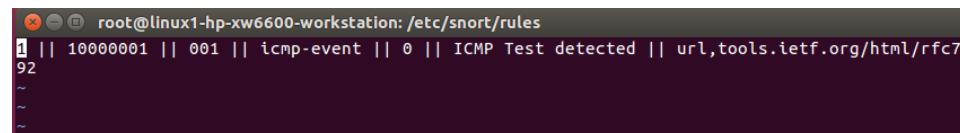
Barnyard2 doesn't read meta-information about alerts from the local.rules file. To make sure that barnyard2 knows that the rule we created with unique identifier 10000001 has the message "ICMP Test Detected", as well as some other information



```
root@linux1-hp-xw6600-workstation: /etc/snort/rules
root@linux1-hp-xw6600-workstation:/etc/snort/rules# vim /etc/snort/sid-msg.map
```

Figure 5. 431: Ensure barnyard2 knows the rules

We add the following line to the /etc/snort/sid-msg.map file:

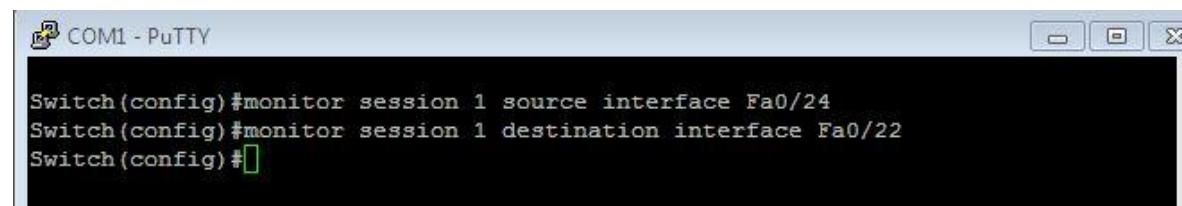


```
root@linux1-hp-xw6600-workstation: /etc/snort/rules
1 || 10000001 || 001 || icmp-event || 0 || ICMP Test detected || url.tools.ietf.org/html/rfc792
~
```

Figure 5. 432: Add line

Port Mirror Configuration in Switch:

Connect to switch and insert this command to insert the port mirror



```
Switch(config)#monitor session 1 source interface Fa0/24
Switch(config)#monitor session 1 destination interface Fa0/22
Switch(config)#[
```

Figure 5. 433: Insert port mirror

### 5.3.25 IPSEC BETWEEN SERVER AND USER

1. On the server

Step 1: Install SoftEther VPN Manager

- a) Run SoftEther VPN Manager and edit setting change localhost to IP address 192.168.11.34

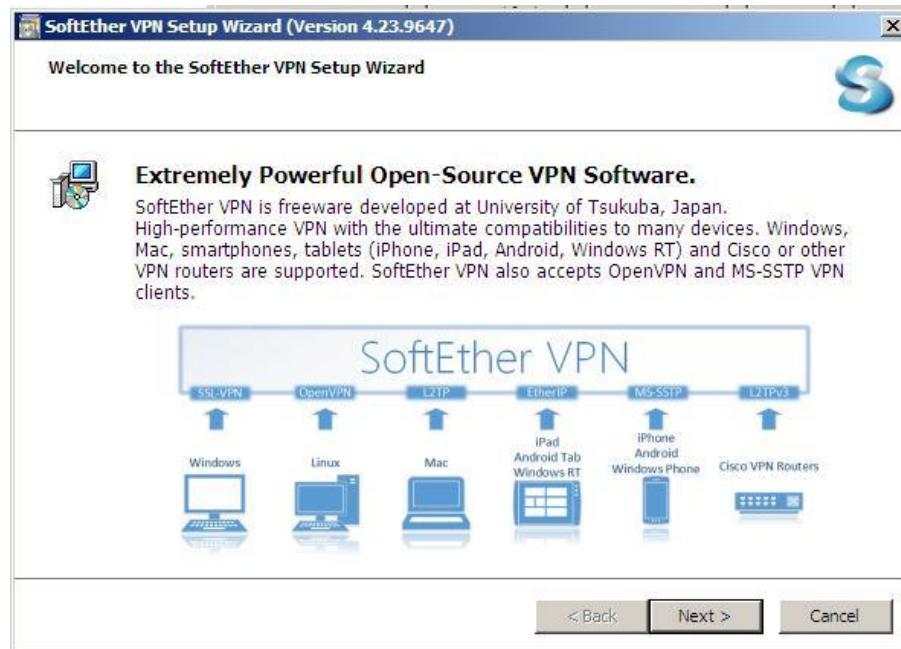


Figure 5. 434: Install SoftEther VPN Manager

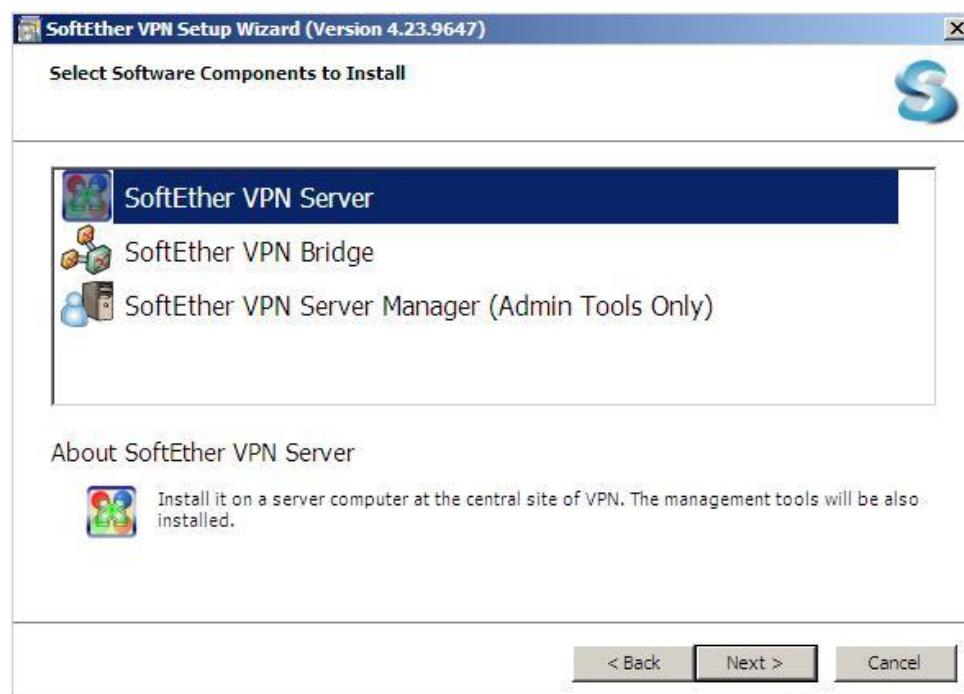


Figure 5. 435: Select SoftEther VPN Server

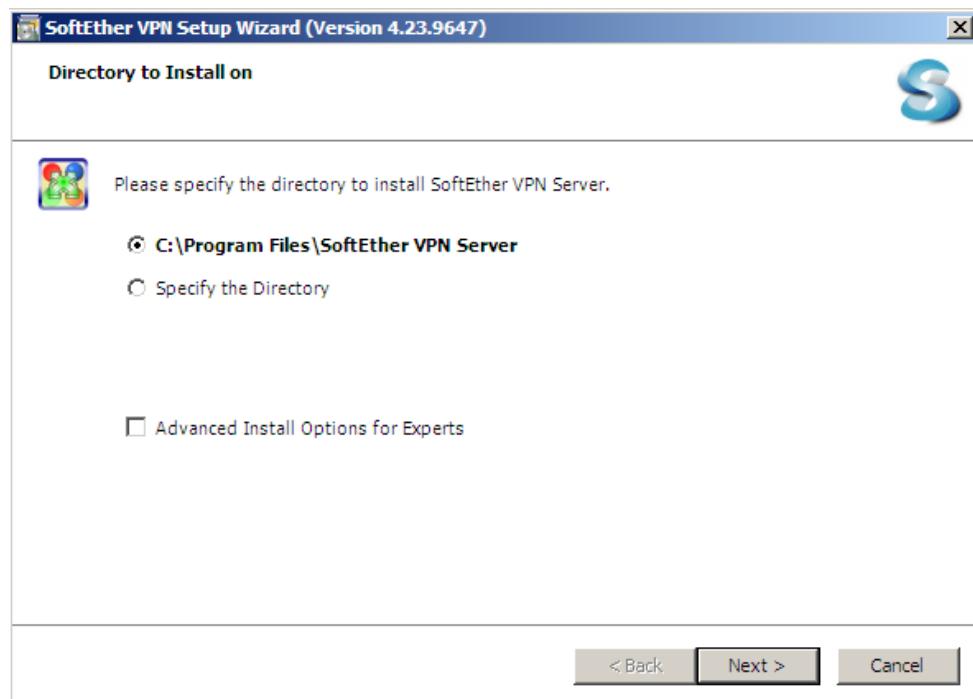


Figure 5. 436: Select first radio button C:\Program Files\SoftEther  
VPN Server

Step 2: Configure the SoftEther VPN Manager



Figure 5. 437: Select Edit Setting

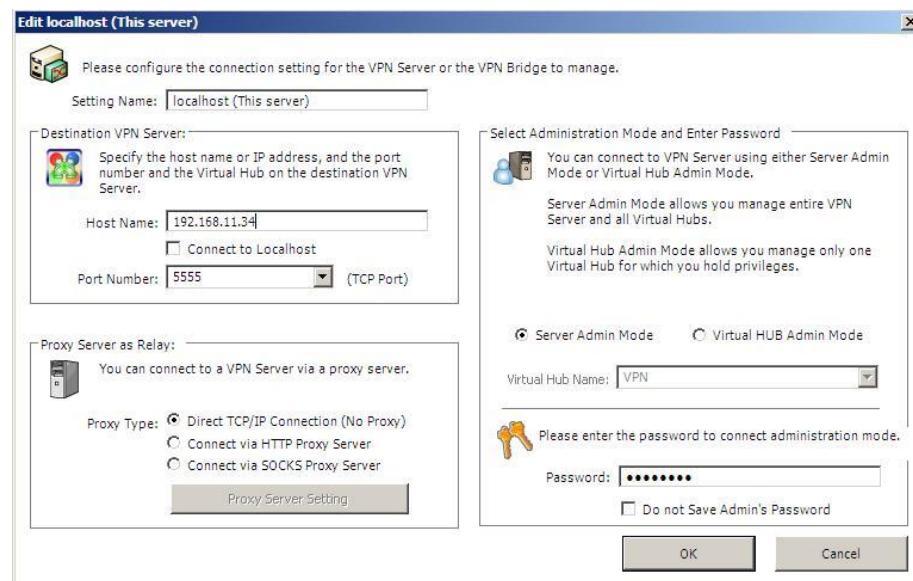


Figure 5. 438: Change VPN Server Hostname localhost to IP Address

192.168.11.34

- a) Change Administrator Password Abc12345 to connect VPN



Figure 5. 439: Change Administrator Password

- b) Click Next to configuration

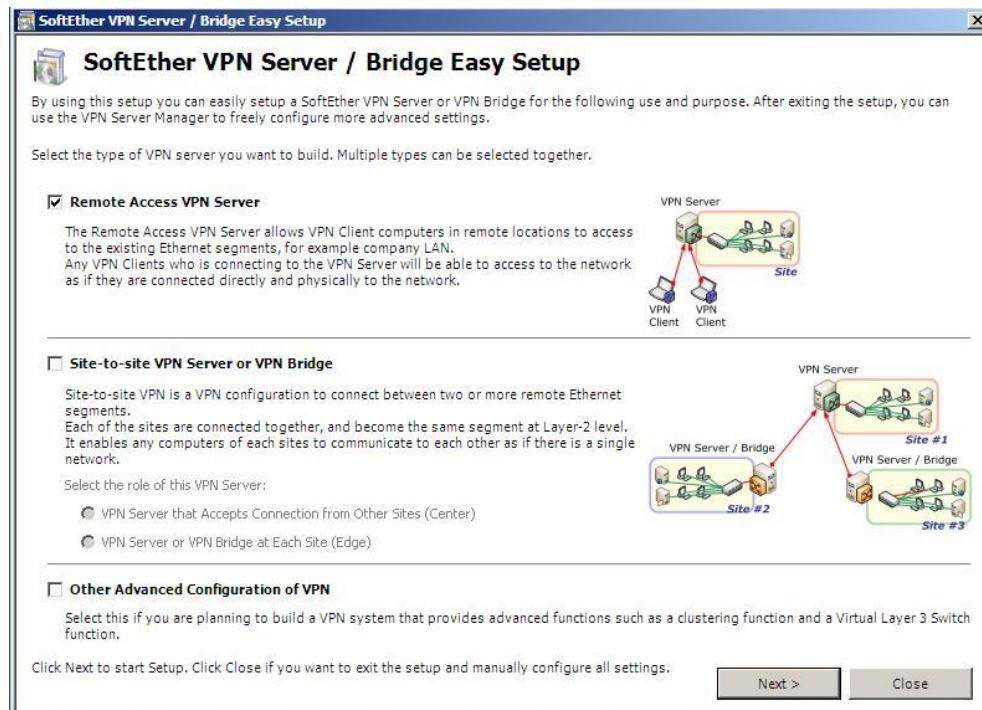


Figure 5. 440: SoftEther VPN Server/Bridge East Setup

- c) Popup Easy Setup shows the default Virtual Hub Name is VPN



Figure 5. 441: Easy Setup – Decide the Virtual Hub Name

- d) Click right on the box Remote Access VPN Server, Site-to-site VPN Server or VPN Bridge and select the role of this VPN Server VPN Server that Accepts Connection from Other Sites (Center)

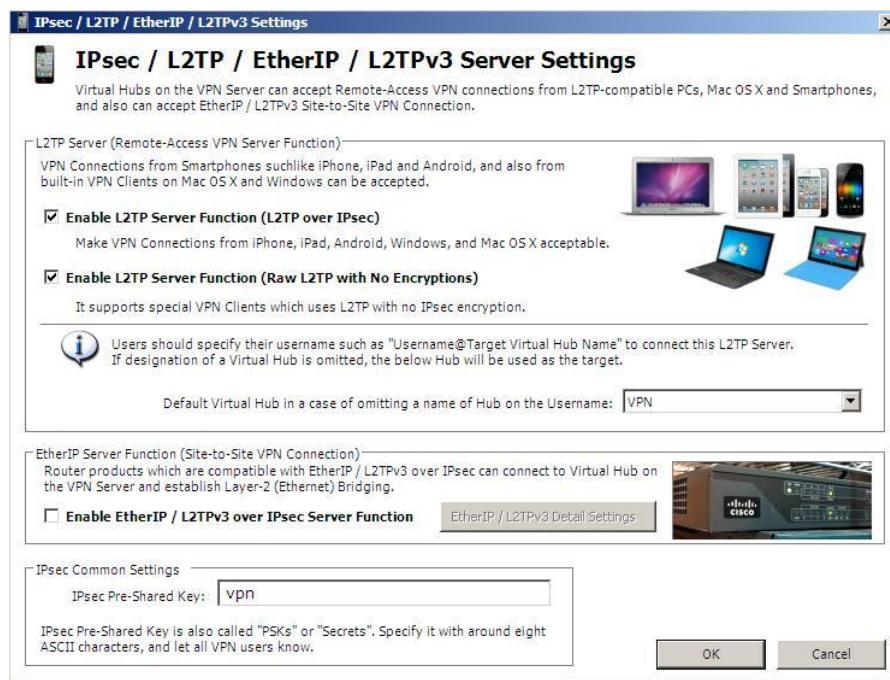


Figure 5. 442: SoftEther VPN Server/Bridge Easy Setup

### Step 3: Create a user to Accept VPN Connection

- a) Select Manager Virtual Hub to add user

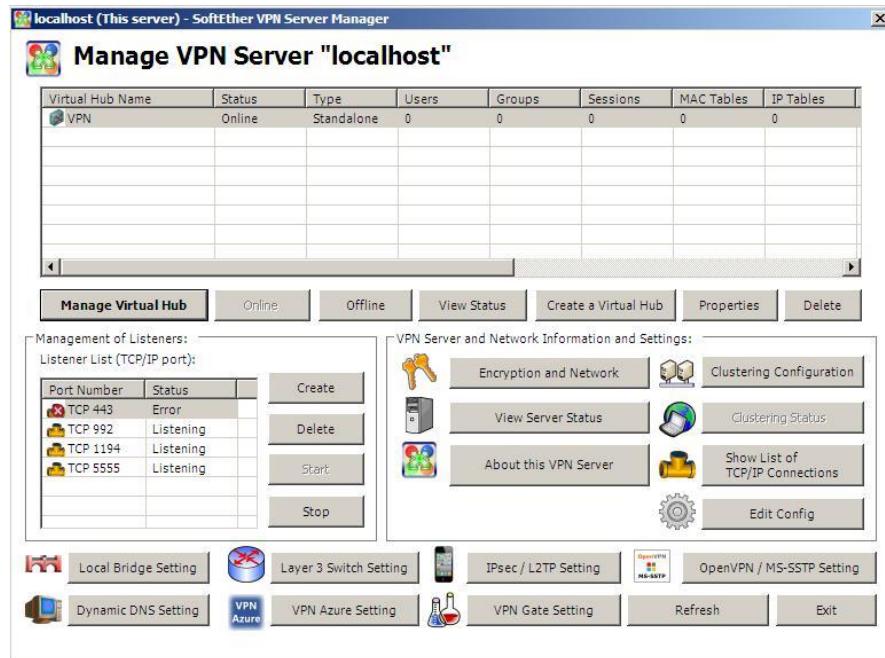


Figure 5. 443: Select Virtual Hub

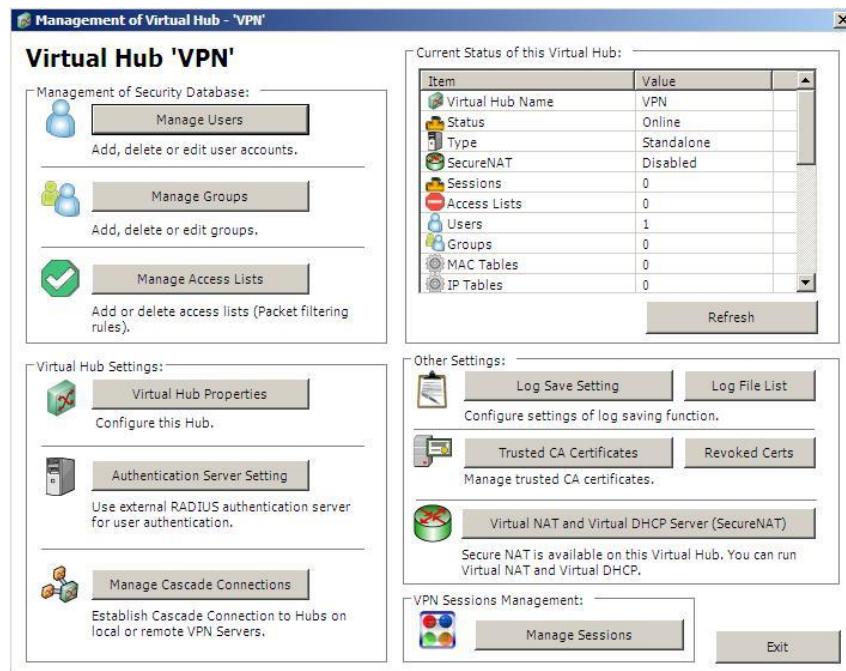


Figure 5. 444: Manage of Virtual Hub “VPN”

- Fill the username group1 and password Abc12345 and click OK

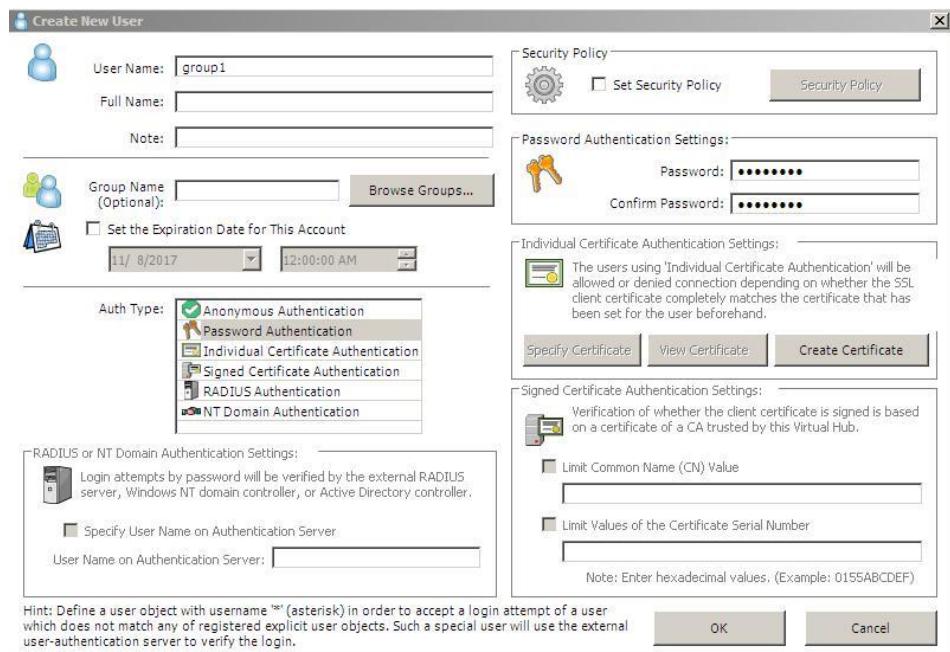


Figure 5. 445: Create New User

b) Successfully adding a user

User Name	Full Name	Group Name	Description	Auth Method	Num Logins	Last Login
group1		-		Password Auth...	0	(None)
<hr/>						

At the bottom, there are buttons for 'New', 'Edit', 'View User Info', 'Remove', 'Refresh', and 'Exit'.

Figure 5. 446: Manage Users

Step 4: Enable SecureNAT.

a) Click on secureNAT tab

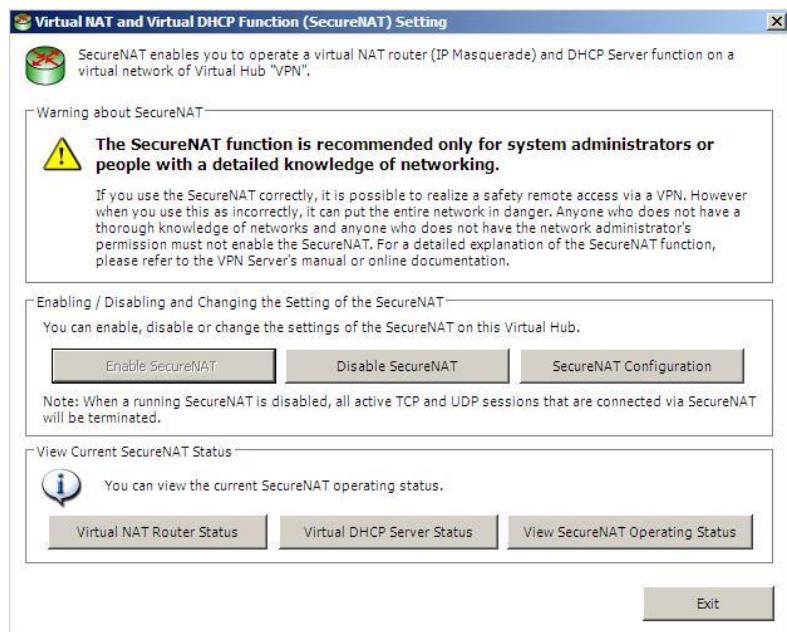


Figure 5. 447: VirtualNAT and Vitrual DHCP Function (SecureNAT)

### Setting

#### b) Confirm to enable the SecureNAT



Figure 5. 448: SoftEther VPN Server Manager

## 2. Configure VPN Connection on Client

### Step 1: Create VPN Connection

- a) Open Network and Sharing Center → Setup a new connection or network

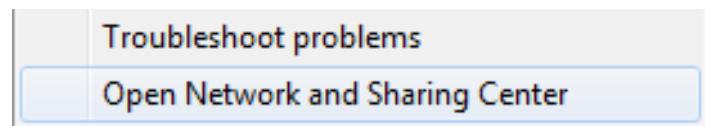


Figure 5. 449: Open Network and Sharing Center

- b) Select Connect to a workplace

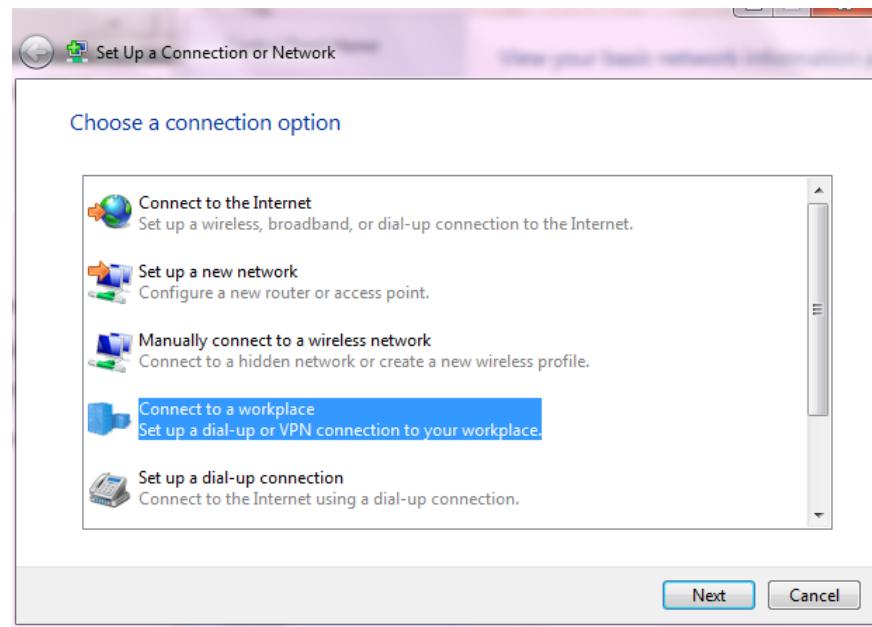


Figure 5. 450: Set Up a Connection or Network

- c) Select I'll set up an Internet connection later

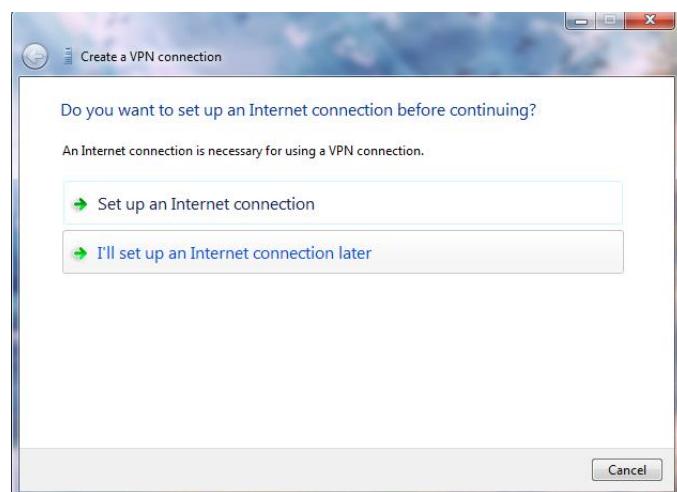


Figure 5. 451: Create a VPN connection

- d) Fill up the public IP Address of Windows Server and tick Allow other people to use this connection.

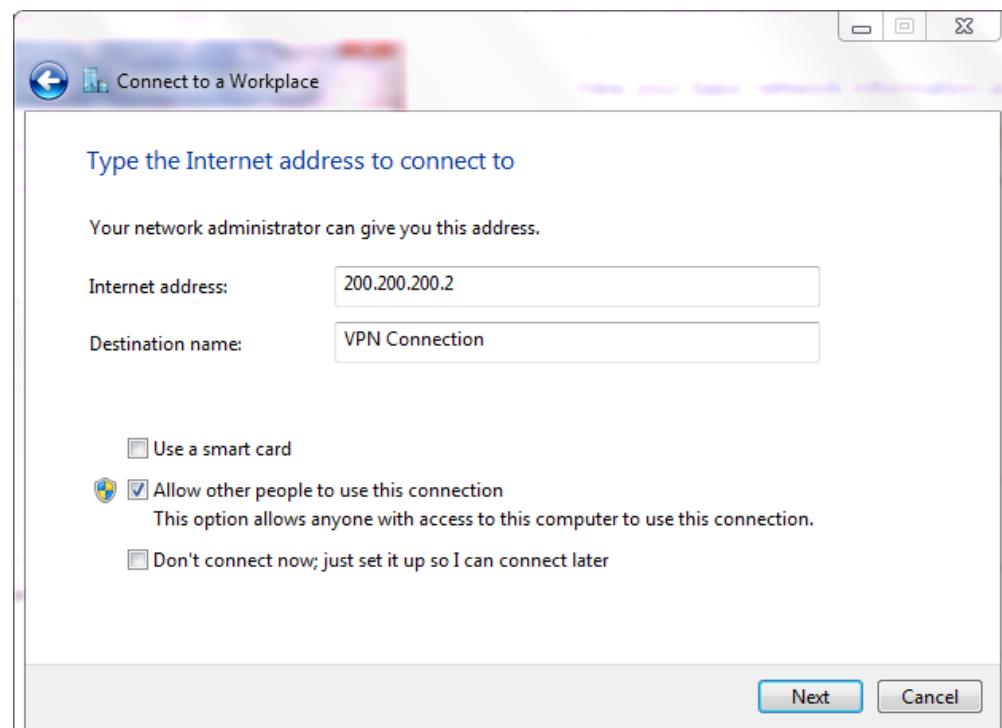


Figure 5. 452: Connect to a Workplace

- e) Fill up the username group1 and password Abc12345

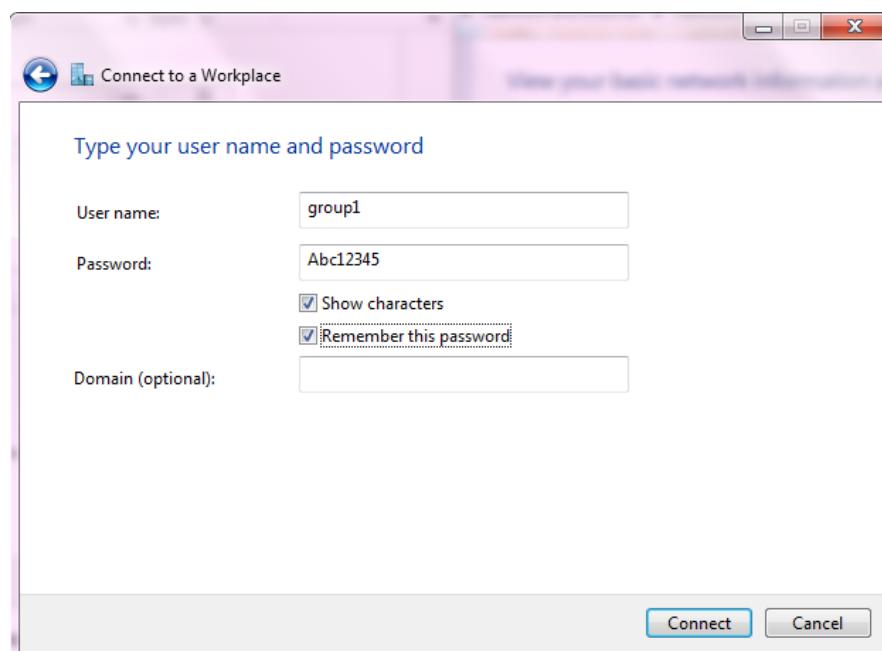


Figure 5. 453: Type your user name and password

f) Click close

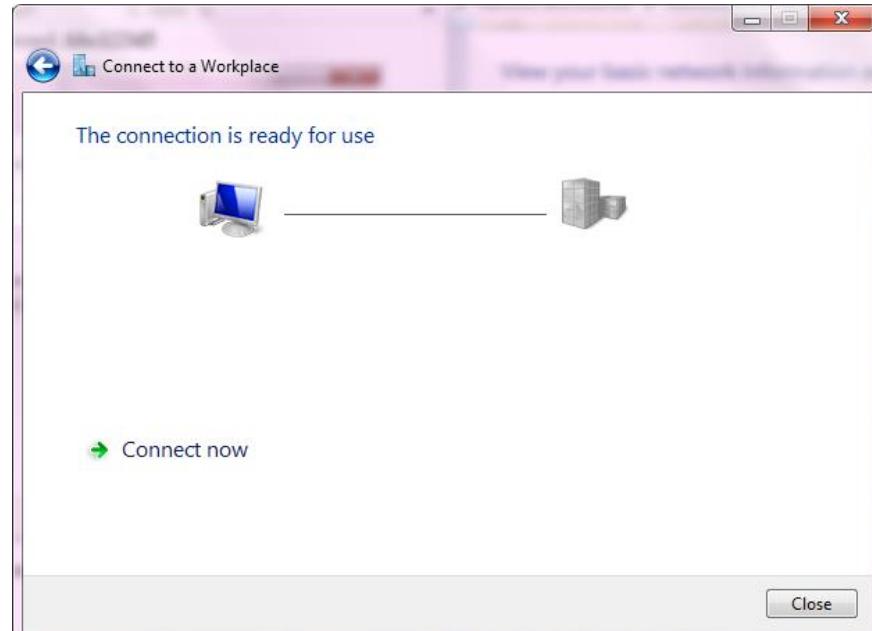


Figure 5. 454: The connection is ready to use

## Step 2: Connect VPN Connection

a) Right click on VPN Connection → Properties

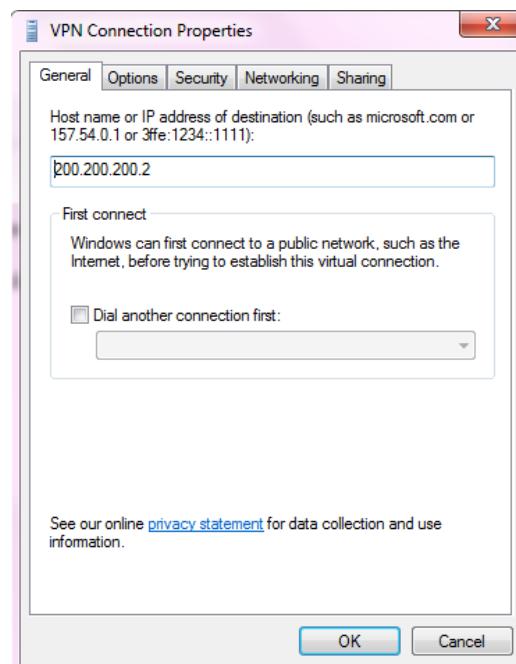


Figure 5. 455: General tab

- b) Select Security tab and choose Layer 2 Tunneling Protocol IPsec (L2TP/IPSec)

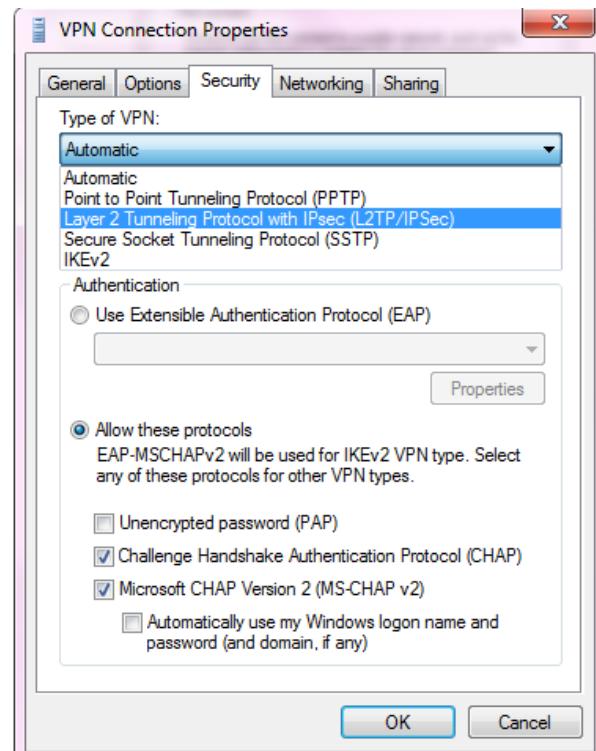


Figure 5. 456: Security tab

- c) Select Advance on Security tab and click radio button Use preshared key for authentication and fill the preshared key is vpn.

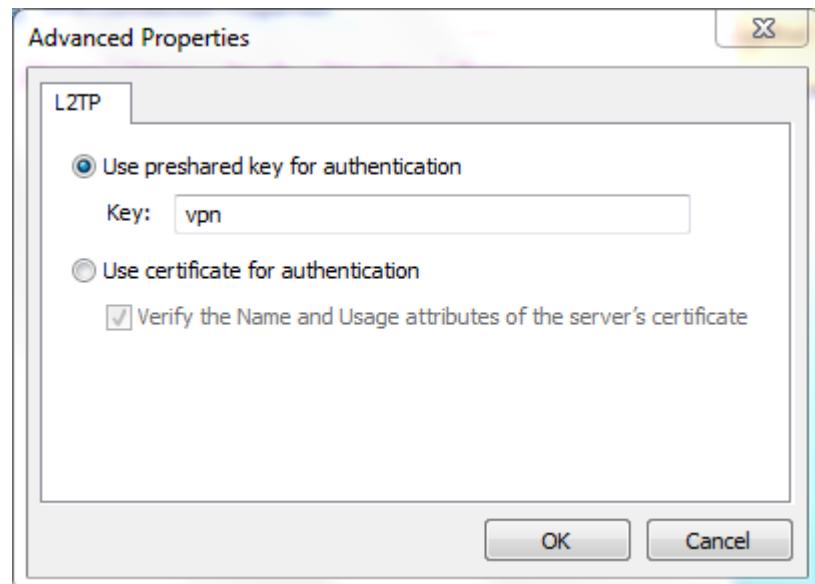


Figure 5. 457: Advanced Properties

- d) Lastly, Open Network and Sharing Center → Change Adapter Setting → VPN Connection → Connect
- e) Fill up the username and password



Figure 5. 458: Connect VPN Connection

## Problem

We want to ensure private and secure communications over Internet Protocol (IP) networks between our network and our neighbour network.

## Solution

We used IPsec policy by installing VPN software on our server. IPsec use of cryptographic security services to private and secure the communication. Because IPsec is integrated at the Internet layer (layer 3), it provides security for almost all protocols in the TCP/IP suite.

### 5.3.26 SAMBA SECURITY SERVICES

Step 1: Adding new group > create folder secured, workshop > change directory to workshop > Add a text file in the workshop folder

```
root@linux1-HP-xw6600-Workstation:~# addgroup sambag1
Adding group `sambag1' (GID 1006) ...
Done.
```

Figure 5. 459: add group

```
root@linux1-HP-xw6600-Workstation:~# mkdir -p /secured/workshop
```

Figure 5. 460: add a new folder

```
root@linux1-HP-xw6600-Workstation:~# cd /secured/workshop
root@linux1-HP-xw6600-Workstation:/secured/workshop# touch securedf.txt
root@linux1-HP-xw6600-Workstation:/secured/workshop# ls
securedf.txt
root@linux1-HP-xw6600-Workstation:/secured/workshop# ll
total 8
drwxr-xr-x 2 root root 4096 Okt  9 02:57 .
drwxr-xr-x 3 root root 4096 Okt  9 02:51 ..
-rw-r--r-- 1 root root    0 Okt  9 02:57 securedf.txt
```

Figure 5. 461: Add File to workshop

Step 2: Edit samba configuration by type a command nano  
 /etc/samba/smb.conf

```
root@linux1-HP-xw6600-Workstation:~# nano /etc/samba/smb.conf
```

Figure 5. 462: edit config file

Step 3: Add the following in the smb.conf

```
[workshop]
comment=secured share
path=/secured/workshop
browsable=yes
writable=yes
guest ok=no
valid users=@sambag1]
```

Figure 5. 463: Add content to [workshop]

Step 4: Adding new user > assign new user to group sambag1 > set the password

```
root@linux1-HP-xw6600-Workstation:/secured/workshop# cd
root@linux1-HP-xw6600-Workstation:~# useradd chai -s /usr/bin/nologin -G sambag1
root@linux1-HP-xw6600-Workstation:~# smbpasswd -a Group1
New SMB password:
Retype new SMB password:
root@linux1-HP-xw6600-Workstation:~# smbpasswd -a chai
New SMB password:
Retype new SMB password:
Added user chai.
```

Figure 5. 464: Add new user, assign to groups & set password

Step 5: Restart samba services

```
root@linux1-HP-xw6600-Workstation:~# service smbd restart
root@linux1-HP-xw6600-Workstation:~# service nmbd restart
```

Figure 5. 465: Restart Samba Services

### 5.3.27 PORT SECURITY

Use command below to secure port fa0/3, port fa0/7, port fa0/11 by using command switchport port-security mac-address sticky.

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/3
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#end
Switch#
*Mar 2 04:23:03.652: %SYS-5-CONFIG_I: Configured from console by admin on consol
e
Switch#
```

Figure 5. 466: Port Security at port fa0/3

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/7
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#end
Switch#
*Mar 2 04:23:55.142: %SYS-5-CONFIG_I: Configured from console by admin on consol
e
Switch#
```

Figure 5. 467: Port Security at port fa0/7

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/11
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#end
Switch#
*Mar 2 04:24:46.941: %SYS-5-CONFIG_I: Configured from console by admin on consol
e
Switch#
```

Figure 5. 468: Port security at port fa0/11

Use command below to secure port by using command switchport port-security mac-address [static].

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/15
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address D4-81-D7-6A-6C-71
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#end
Switch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

Figure 5. 469: Port Security at port fa0/15

### 5.3.28 SPANNING TREE PROTOCOL (STP) SECURITY

Step 1: Enable the spanning-tree portfast and spanning-tree bpduguard in every interface range

```

Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int range fa0/2-4
Switch(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast will be configured in 3 interfaces due to the range command
but will only have effect when the interfaces are in a non-trunking mode.
Switch(config-if-range)#spanning-tree bpduguard enable
Switch(config-if-range)#int range fa0/5-7
Switch(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast will be configured in 3 interfaces due to the range command
but will only have effect when the interfaces are in a non-trunking mode.
Switch(config-if-range)#spanning-tree bpduguard enable
Switch(config-if-range)#int range fa0/8-11
Switch(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast will be configured in 4 interfaces due to the range command
but will only have effect when the interfaces are in a non-trunking mode.
Switch(config-if-range)#spanning-tree bpduguard enable
Switch(config-if-range)#int range fa0/12-23
Switch(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast will be configured in 12 interfaces due to the range command
but will only have effect when the interfaces are in a non-trunking mode.
Switch(config-if-range)#spanning-tree bpduguard enable
Switch(config-if-range)#

```

Figure 5. 470: Enable the spanning-tree portfast and spanning-tree

bpduguard

Step 2: Enable the spanning-tree guard root in the trunking interface which is  
interface Fa0/24

```

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int range fa0/24
Switch(config-if-range)#spanning-tree guard root
Switch(config-if-range)#
*Mar  2 03:36:00.416: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root guard enabled on
port FastEthernet0/24.
Switch(config-if-range)#

```

Figure 5. 471: Enable the spanning-tree guard root

### 5.3.29 VLAN SECURITY

Step 1: To prevent switch spoofing, disable DTP by using command switchport nonegotiate on fa0/24.

```

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/24
Switch(config-if)#switchport nonegotiate
Switch(config-if)#end
Switch#

```

Figure 5. 472: switchport nonegotiate

Step 2: To prevent double tagging, do not put any host on native VLAN 5.

VLAN	Name	Status	Ports
1	default	active	
5	Trunk	active	
10	WindowsServer	active	Fa0/2, Fa0/3, Fa0/4
15	unusedPort	suspended	Fa0/1, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/23, Gi0/1, Gi0/2
20	LinuxServer1	active	Fa0/5, Fa0/6, Fa0/7
30	LinuxServer2	active	Fa0/8, Fa0/9, Fa0/10, Fa0/11
40	Client	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15
50	Management	active	
60	wireless	active	Fa0/16, Fa0/17

Figure 5. 473: show vlan

Step 3: Create a VLAN 15 to place all unused ports and suspend it so that there is no communication between VLAN 15 and other VLANs.

```
Switch(vlan)#vlan 15 name unusedPort
VLAN 15 modified:
    Name: unusedPort
```

Figure 5. 474: Create VLAN 15 named unusedPort

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 15
Switch(config-vlan)#state suspend
Switch(config-vlan)#end
```

Figure 5. 475: Suspend VLAN 15

Step 4: Put all unused port into VLAN 15.

```
Switch(config)#int range fa0/1,fa0/18,fa0/19,fa0/20,fa0/21
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 15
Switch(config-if-range)#int range fa0/23,g0/1,g0/2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 15
Switch(config-if-range)#end
```

Figure 5. 476: Assign all unused port into VLAN 15

Step 5: Assign used vlans into trunk port.

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 1,5,10,20,30,40,50,60
Switch(config-if)#end
Switch#
```

Figure 5. 477: Assign all usable VLANs into trunk port

### 5.3.30 NETWORK TIME PROTOCOL (NTP)

Step 1: Install NTP service in the server using command sudo apt-get install

ntp

```
linux2@mail:~$ sudo apt-get install ntp
```

Figure 5. 478: Install service

Step 2: Allow port 123 by using command sudo ufw allow 123/udp. Then, edit ntp.conf.

```
linux2@mail:~$ sudo ufw allow 123/udp
Skipping adding existing rule
Skipping adding existing rule (v6)
linux2@mail:~$ sudo nano /etc/ntp.conf
```

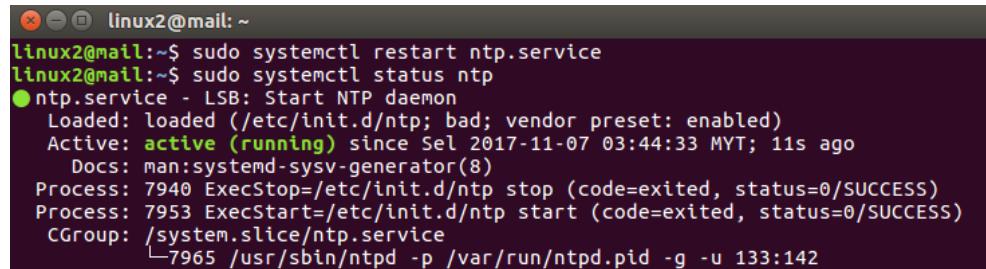
Figure 5. 479: Edit config file

Step 3: Adding the following command in the config file.

```
filegen clockstats file clockstats type day enable
# Specify one or more NTP servers.
# Use servers from the NTP Pool Project. Approved by Ubuntu Technical Board
# on 2011-02-08 (LP: #104525). See http://www.pool.ntp.org/join.html for
# more information.
Server 0.my.pool.ntp.org iburst
server 1.my.pool.ntp.org
server 2.my.pool.ntp.org
server 3.my.pool.ntp.org
server 127.127.1.0
fudge 127.127.1.0 stratum 10
# Use Ubuntu's ntp server as a fallback.
server ntp.ubuntu.com
```

Figure 5. 480: Adding following command

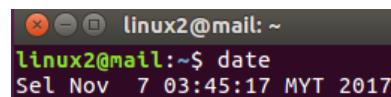
Step 4: Restart NTP service by issuing command sudo systemctl restart ntp.service. Then, check the status of the service by sudo systemctl status ntp.



```
linux2@mail:~$ sudo systemctl restart ntp.service
linux2@mail:~$ sudo systemctl status ntp
● ntp.service - LSB: Start NTP daemon
  Loaded: loaded (/etc/init.d/ntp; bad; vendor preset: enabled)
  Active: active (running) since Sel 2017-11-07 03:44:33 MYT; 11s ago
    Docs: man:systemd-sysv-generator(8)
 Process: 7940 ExecStop=/etc/init.d/ntp stop (code=exited, status=0/SUCCESS)
 Process: 7953 ExecStart=/etc/init.d/ntp start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/ntp.service
           └─7965 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 133:142
```

Figure 5. 481: Restart and check the status of service

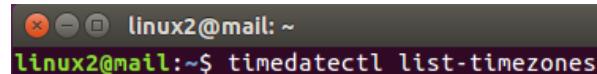
Step 5: Check date of the server.



```
linux2@mail:~$ date
Sel Nov  7 03:45:17 MYT 2017
```

Figure 5. 482: check the date

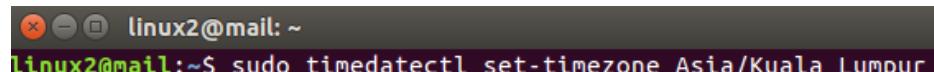
Step 6: List the time zones by using command timedatectl list-timezones.



```
linux2@mail:~$ timedatectl list-timezones
```

Figure 5. 483: List the time zones

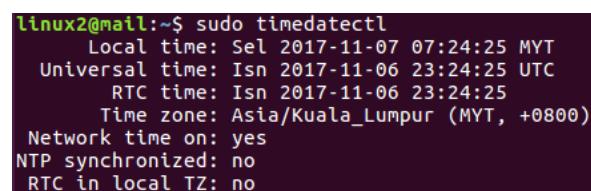
Step 7: Select the time zone.



```
linux2@mail:~$ sudo timedatectl set-timezone Asia/Kuala_Lumpur
```

Figure 5. 484: Set the time zone

Step 8: sudo timedatectl to show the time set.



```
linux2@mail:~$ sudo timedatectl
      Local time: Sel 2017-11-07 07:24:25 MYT
      Universal time: Isn 2017-11-06 23:24:25 UTC
            RTC time: Isn 2017-11-06 23:24:25
             Time zone: Asia/Kuala_Lumpur (MYT, +0800)
        Network time on: yes
     NTP synchronized: no
      RTC in local TZ: no
```

Figure 5. 485: Show the setup

Step 9: Check the peer and association condition of NTP using watch ntpq -cpe -cas.

```
linux2@mail:~$ watch ntpq -cpe -cas
```

Figure 5. 486: check the condition of the service

Step 10: While the condition showing sys.peer, means that the service had been up successfully.

remote	refid	st	t	when	poll	reach	delay	offset	jitter
*LOCAL(0)	.LOCL.	10	l	21	64	377	0.000	0.000	0.000
ind assid	status	conf	reach	auth	condition	last_event	cnt		
1 65173	963a	yes	yes	none	sys.peer	sys_peer	3		

Figure 5. 487: NTP condition

Step 11: The second command that can also be used to show the condition of NTP service.

remote	refid	st	t	when	poll	reach	delay	offset	jitter
*LOCAL(0)	.LOCL.	10	l	23	64	77	0.000	0.000	0.000
ind assid	status	conf	reach	auth	condition	last_event	cnt		
1 65173	963a	yes	yes	none	sys.peer	sys_peer	3		

Figure 5. 488: Alternative command

### 5.3.31 SYSLOG

#### Part A: Configure syslog server and client

##### Syslog Server

Step 1: Enter Linux II terminal

Step 2: Download syslog by using command “sudo apt-get install rsyslog”

```
other options.
linux2@linux2-optiplex-9020:~$ sudo apt-get install rsyslog
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Figure 5. 489: Install syslog on linux

Step 3: Verify syslog is already installed on the devices by using command “rsyslogd -N1”

```
linux2@linux2-optiplex-9020:~$ rsyslogd -N1
rsyslogd: version 8.16.0, config validation run (level 1), master config /etc/rsyslog.conf
```

Figure 5. 490: Check syslog version

Step 4: Enter sudo su and enter password “abc123”

Step 5: Enter syslog configuration file by entering command “sudo nano /etc/rsyslog.conf”

Step 6: Uncomment TCP and UDP reception to enable the syslog to listen any syslog from external sources with port 514

```
# Provides UDP syslog reception
#$ModLoad imudp
#$UDPServerRun 514

# Provides TCP syslog reception
#$ModLoad imtcp
#$InputTCPServerRun 514
```

Figure 5. 491: Enables syslog receive log

```
# For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html
# If you experience problems, see http://www.rsyslog.com/doc/troubleshoot.html

##### MODULES #####
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imklog   # provides kernel logging support (previously done by rklogd)
#$ModLoad immark  # provides --MARK-- message capability

$SystemLogRateLimitInterval 1
$SystemLogRateLimitBurst 50000

# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
```

Figure 5. 492: Uncomment TCP and UDP

Step 7: Restart the syslog by using the command “sudo service rsyslog restart”

```
linux2@linux2-optiplex-9020:~$ sudo service rsyslog restart
linux2@linux2-optiplex-9020:~$ █
```

Figure 5. 493: Restart service

## Syslog Client

Step 1: Enter Linux I terminal

Step 2: Download syslog by using command “sudo apt-get install rsyslog”

```
Linux1@linux1-hp-xw6600-workstation:~$ sudo apt-get install rsyslog
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Figure 5. 494: Start service syslog

Step 3: Verify syslog is already installed on the devices by using command

“rsyslogd –N1”

Step 4: Enter “sudo su” and enter password “abc123”

Step 5: Enter syslog configuration file by entering command “sudo nano/etc/rsyslog.conf”

Step 6: Set host IP 192.168.11.51 to send log to syslog server with syslog protocol

```
# Save boot messages also to boot.log
local7.*                                     /var/log/boot.log

# ### begin forwarding rule #####
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#■
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$WorkDirectory /var/lib/rsyslog # where to place spool files
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList  # run asynchronously
#$ActionResumeRetryCount -1    # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
*. * @192.168.11.51:514
# ### end of the forwarding rule #####
#■
```

Figure 5. 495: Set destination host

Step 7: Restart the syslog by using the command “sudo service rsyslog restart”

```
linux1@linux1-hp-xw6600-workstation:~$ sudo service rsyslog restart
[sudo] password for linux1:
linux1@linux1-hp-xw6600-workstation:~$ ■
```

Figure 5. 496: Restart service syslog

## Part B: Syslog on router and switch

### Syslog on router

Step 1: Open putty. Select Serial and click Open.

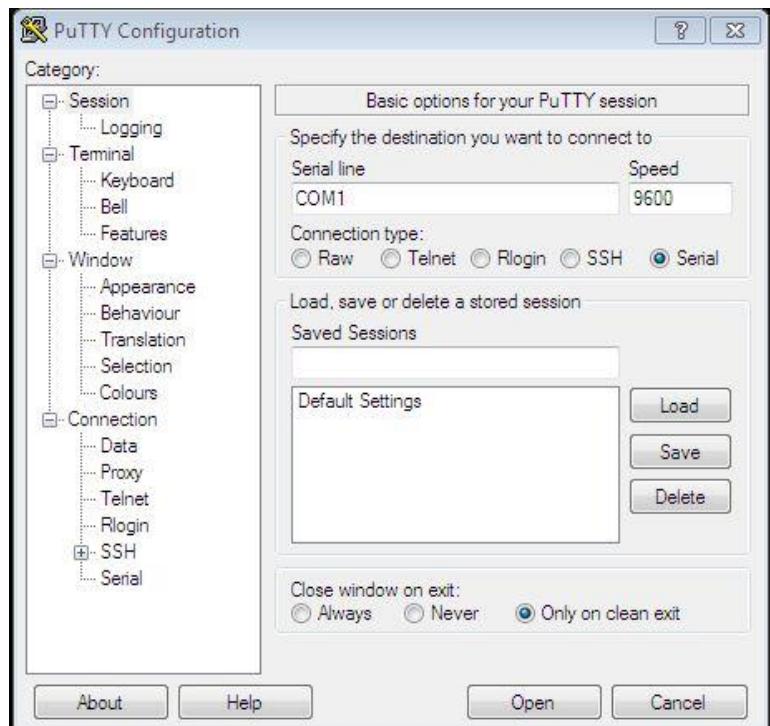


Figure 5. 497: Putty Terminal

Step 2: User Access Verification will display. Enter the username (Any AD users) and password. Enter

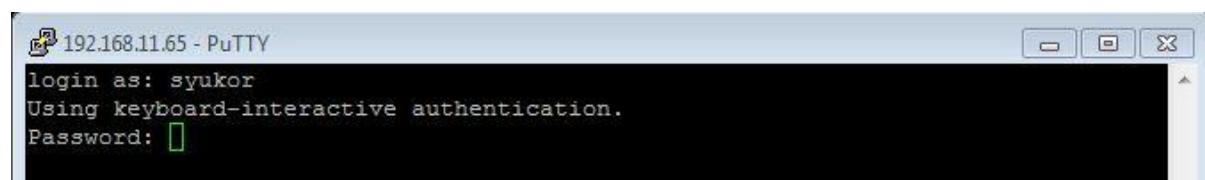


Figure 5. 498: AD username login

Step 3: Enter global configuration mode using command configure terminal.

```

192.168.11.65 - PuTTY
login as: syukor
Using keyboard-interactive authentication.
Password:

#####
#      WELCOME TO GROUP1 WORKSHOP UNAUTHORIZED USER IS PROHIBITED
#
#####

*** Ensure that you enter cisco password correctly ***
*** Documentation after making system changes. ***

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#

```

Figure 5. 499: Global configuration

Step 4: Setup syslog command in the putty terminal

```

192.168.11.65 - PuTTY
login as: syukor
Using keyboard-interactive authentication.
Password:

#####
#      WELCOME TO GROUP1 WORKSHOP UNAUTHORIZED USER IS PROHIBITED
#
#####

*** Ensure that you enter cisco password correctly ***
*** Documentation after making system changes. ***

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#logging trap debugging
R1(config)#logging facility local0
R1(config)#logging source-interface Loopback0
R1(config)#logging host 192.168.11.51 transport tcp port 514
R1(config)#logging host 192.168.11.51 transport udp [port 514]

```

Figure 5. 500: Insert command in router

## Syslog on switch

Step 1: Open putty. Select Serial and click Open.

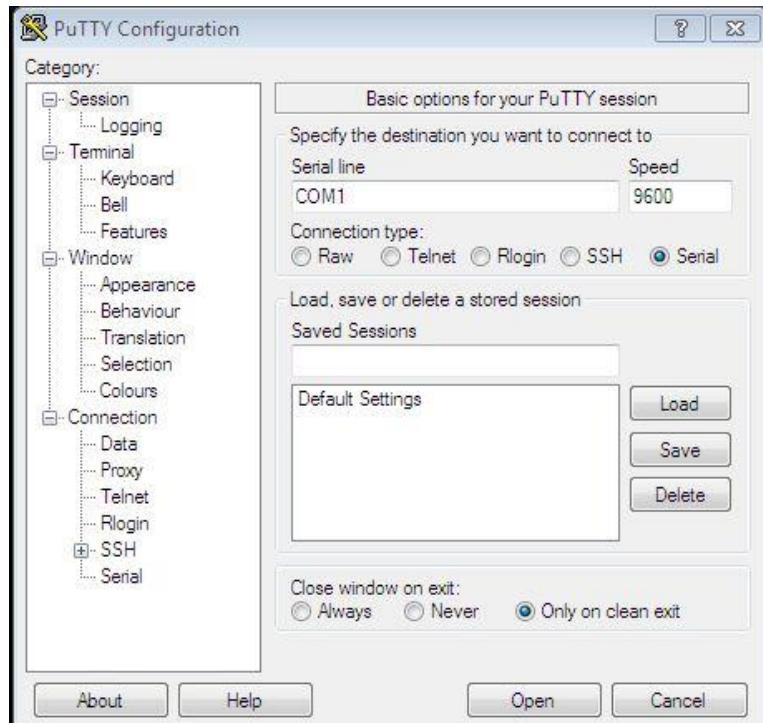


Figure 5. 501: Putty Terminal

Step 2: User Access Verification will display. Enter the username admin and password admin01. Enter

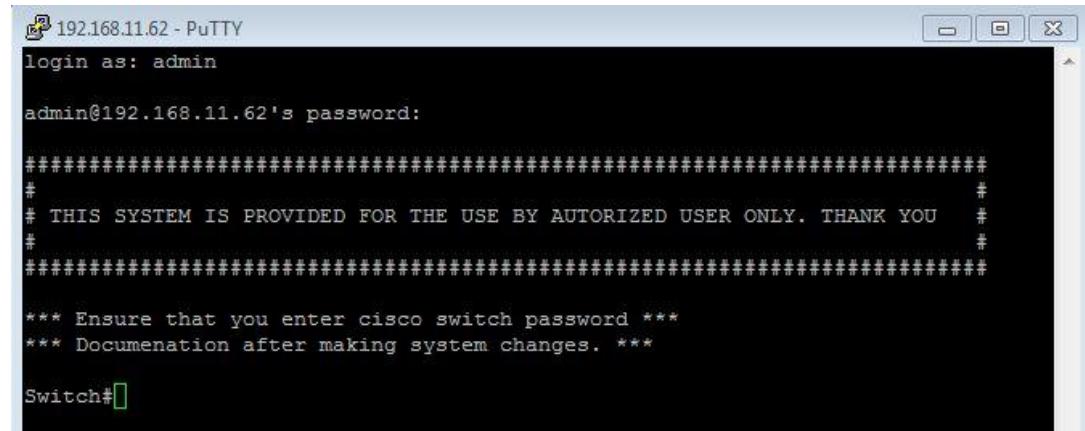
```

192.168.11.62 - PuTTY
login as: admin
admin@192.168.11.62's password:
#####
# THIS SYSTEM IS PROVIDED FOR THE USE BY AUTHORIZED USER ONLY. THANK YOU #
#####
*** Ensure that you enter cisco switch password ***
*** Documentation after making system changes. ***
Switch#

```

Figure 5. 502: Switch login admin

Step 3: Enter global configuration mode using command configure terminal.



```
192.168.11.62 - PuTTY
login as: admin

admin@192.168.11.62's password:

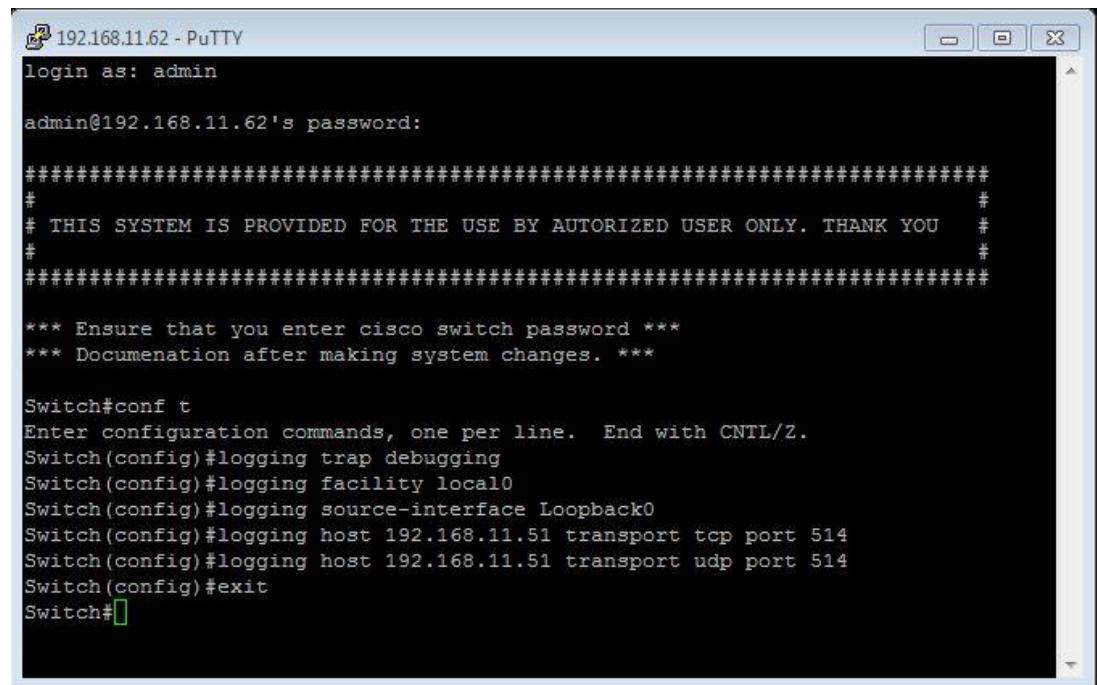
#####
#
# THIS SYSTEM IS PROVIDED FOR THE USE BY AUTHORIZED USER ONLY. THANK YOU
#
#####

*** Ensure that you enter cisco switch password ***
*** Documentation after making system changes. ***

Switch#
```

Figure 5. 503: Global configuration

Step 4: Setup syslog command in the putty terminal



```
192.168.11.62 - PuTTY
login as: admin

admin@192.168.11.62's password:

#####
#
# THIS SYSTEM IS PROVIDED FOR THE USE BY AUTHORIZED USER ONLY. THANK YOU
#
#####

*** Ensure that you enter cisco switch password ***
*** Documentation after making system changes. ***

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#logging trap debugging
Switch(config)#logging facility local0
Switch(config)#logging source-interface Loopback0
Switch(config)#logging host 192.168.11.51 transport tcp port 514
Switch(config)#logging host 192.168.11.51 transport udp port 514
Switch(config)#exit
Switch#
```

Figure 5. 504: Switch configuration

**Problem:** For network administrator it is important to have centralized logging server to view log messages from another device. It's hard to monitor log messages from every device include cisco device which takes time.

**Solution:** We install rsyslog and configure Linux as syslog server. Every log messages from client syslog, router and switch will be sent to syslog server. All the action is recorded in log files.

### 5.3.32 WIRELESS AUTHENTICATION USING RADIUS SERVER

Step 1: Click on Server Manager > Roles > Add Roles.

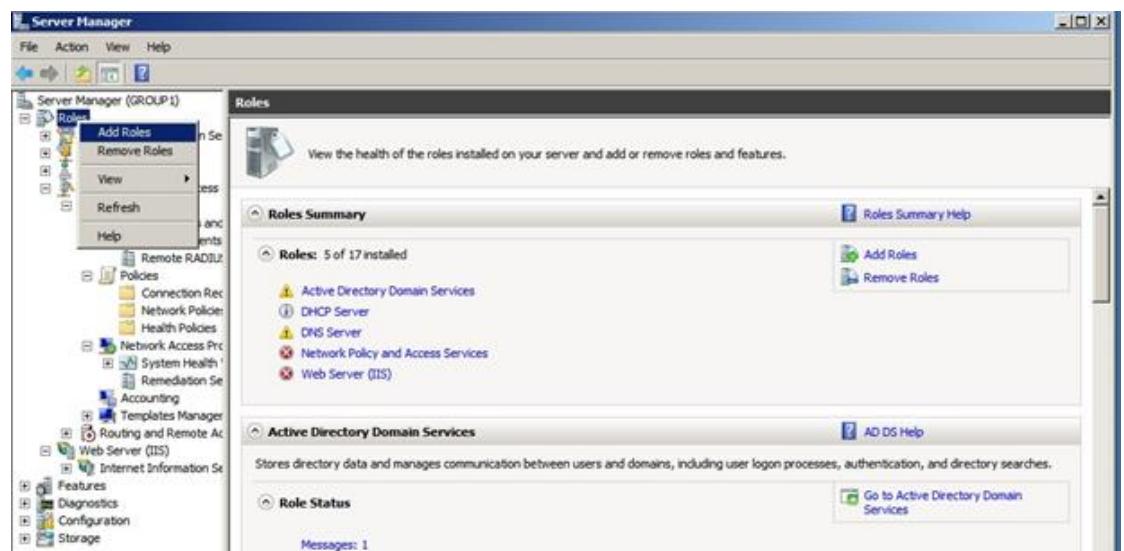


Figure 5. 505: Add Roles

Step 2: Then, in Before You Begin, after read the information, click Next.

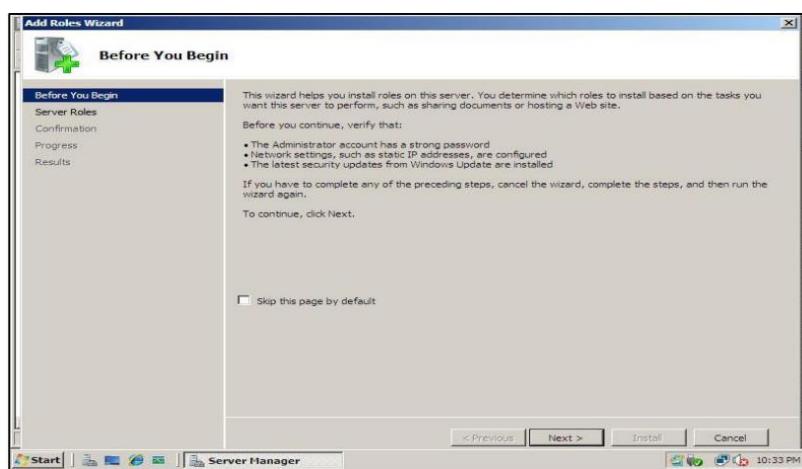


Figure 5. 506: Before You Begin

Step 3: In Add Roles Wizard, tick on Active Directory Certificate Services.

Then click Next.

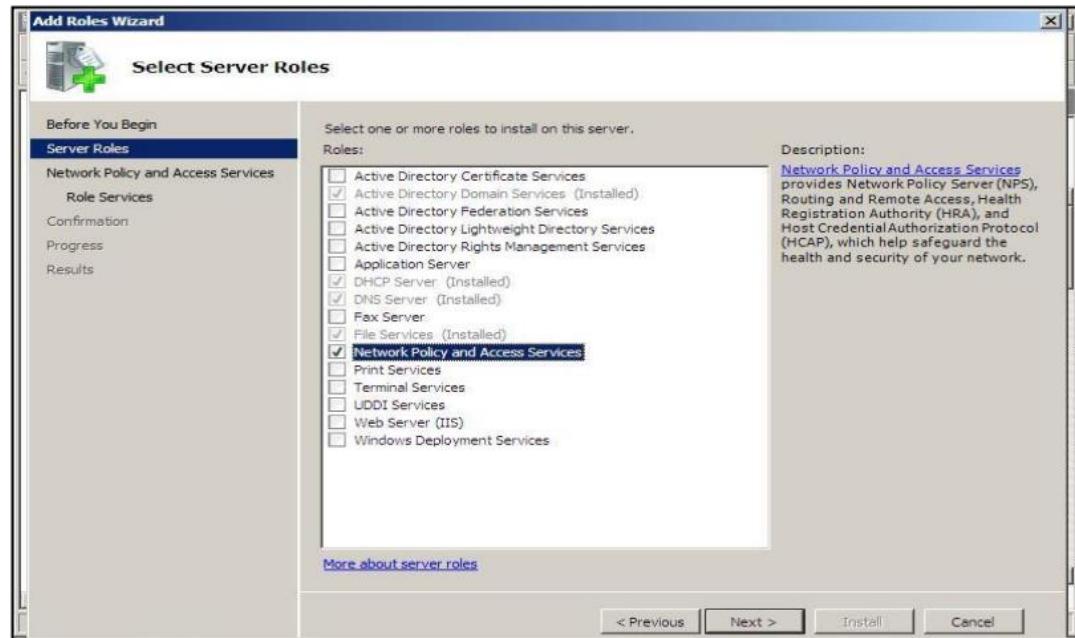


Figure 5. 507: Select Server Roles

Step 4: In Select Role Services, tick on Certification Authority. Then, click Next.

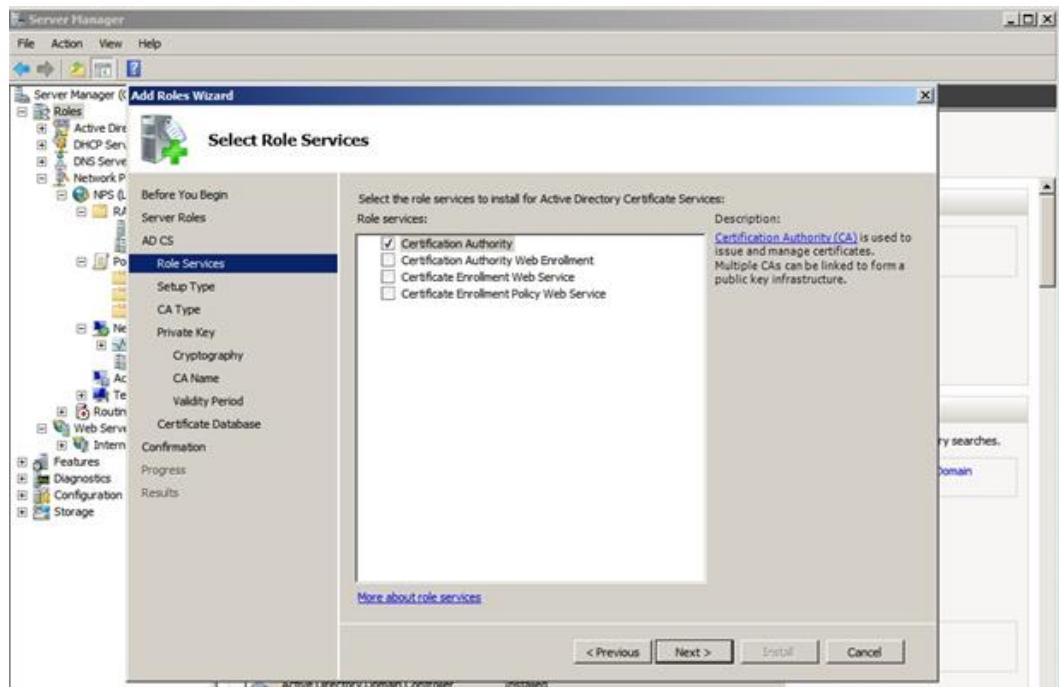


Figure 5. 508: Select Role services

Step 5: In Select Setup Type, tick on Enterprise. Then, click Next.

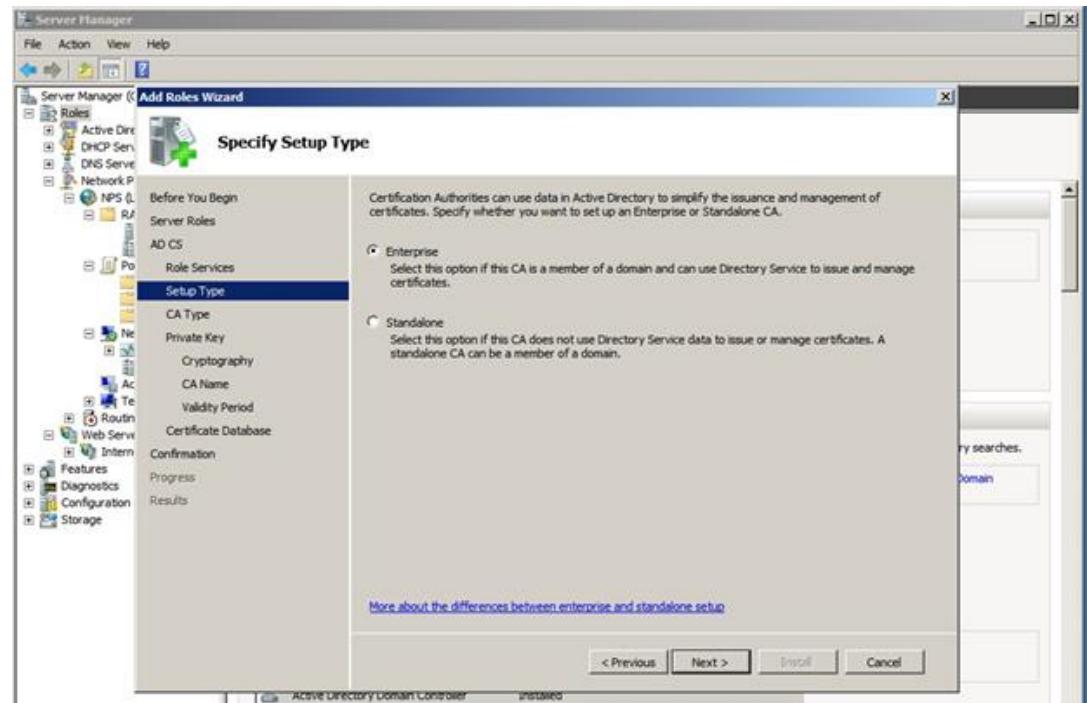


Figure 5. 509: Select Setup Types

Step 6: In Select CA Type, tick on Root CA. Then, click Next.

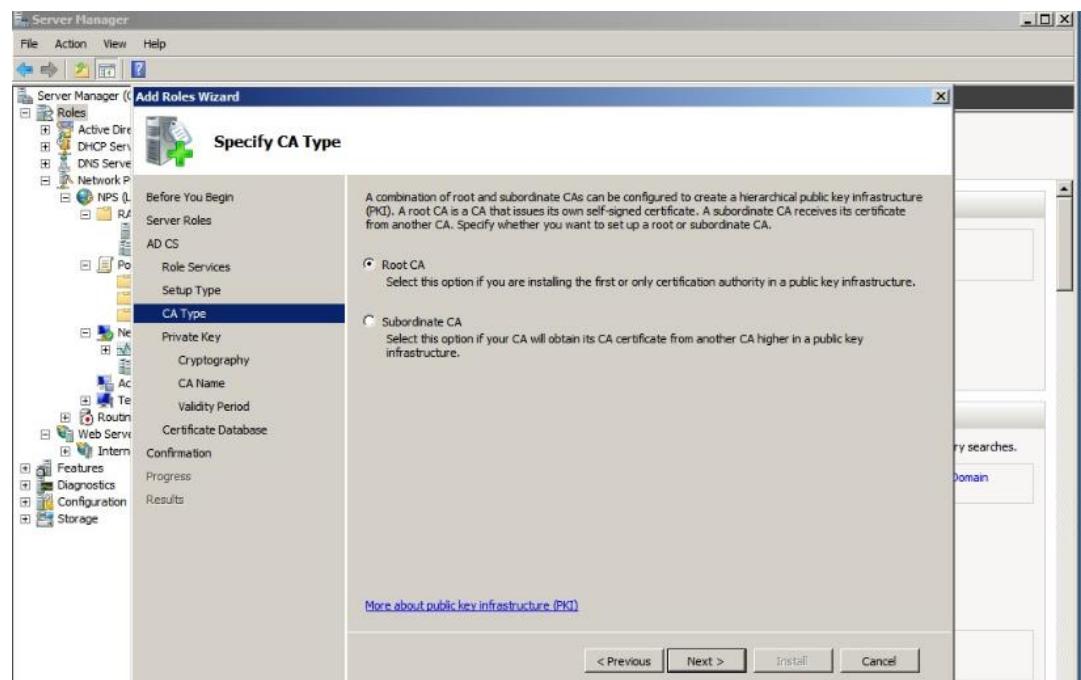


Figure 5. 510: Select CA Type

Step 7: In Select Private Key, tick on Create a new private. Then, click Next.

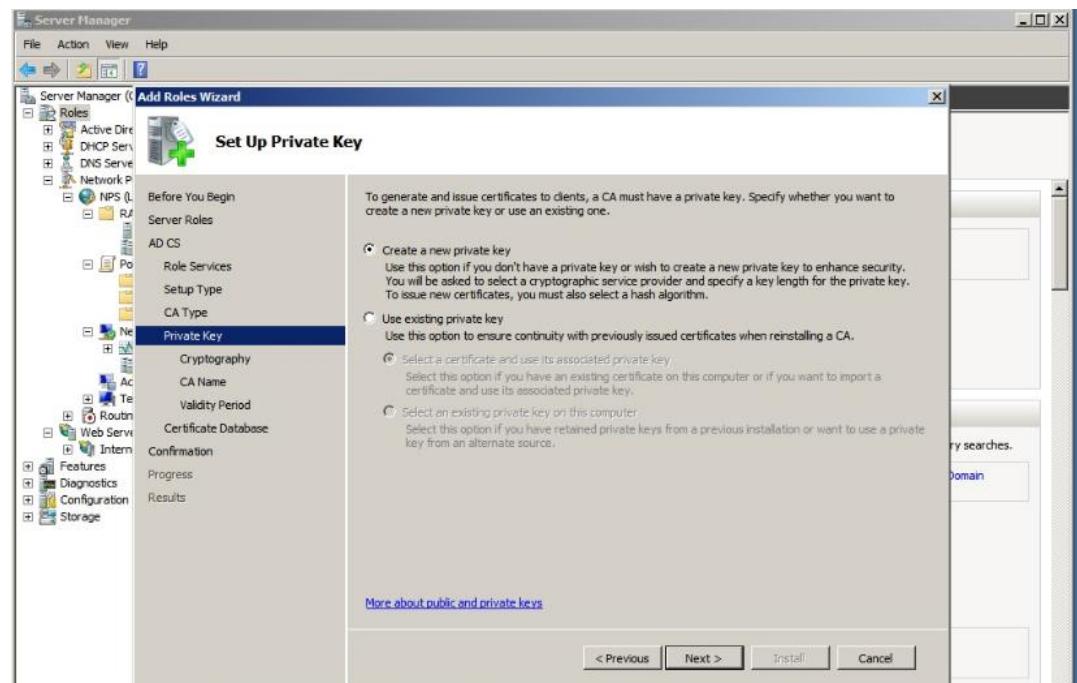


Figure 5. 511: Select Private Key

Step 8: Click on Private Key > Crptography, select hash algorithm SHA256 and key character length 2048. Then, click Next.

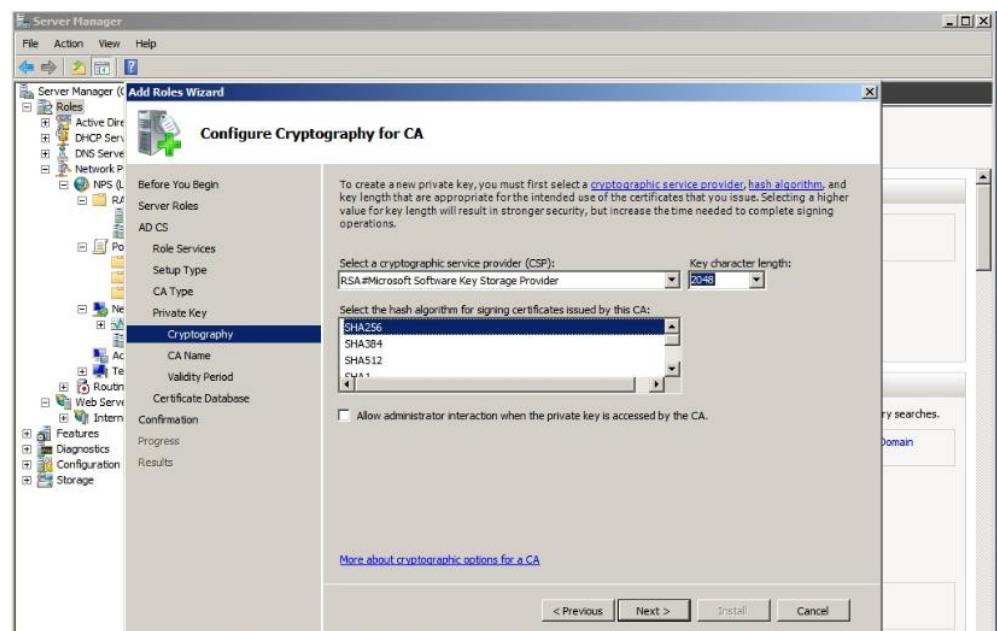


Figure 5. 512: Configure cryptography

Step 9: Click on Private Key > CA Name, Enter value for common name for this CA: group1-GROUP1-CA. Enter value for distinguished name suffix: DC=group1, DC=com.

Next, Enter value for preview of distinguished name: CN=group1-GROUP1-CA, DC=group1, DC=com. Then, click Next.

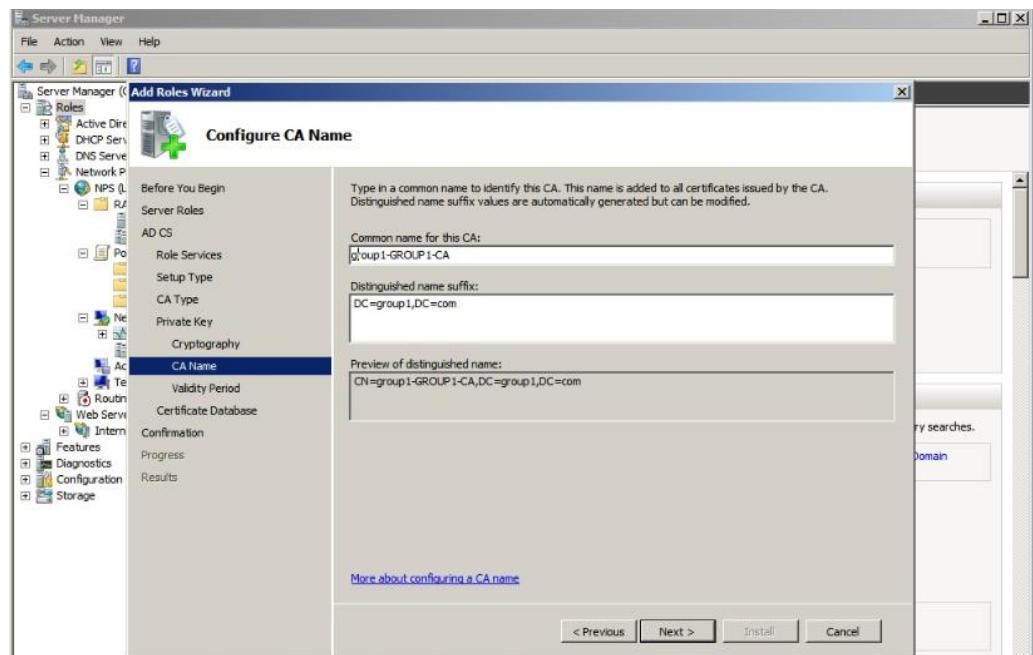


Figure 5. 513: Configure CA Name

Step 10: Click on Private Key > Validity Period, in select validity period for certification generated for this CA enter value 5. Then, click Next.

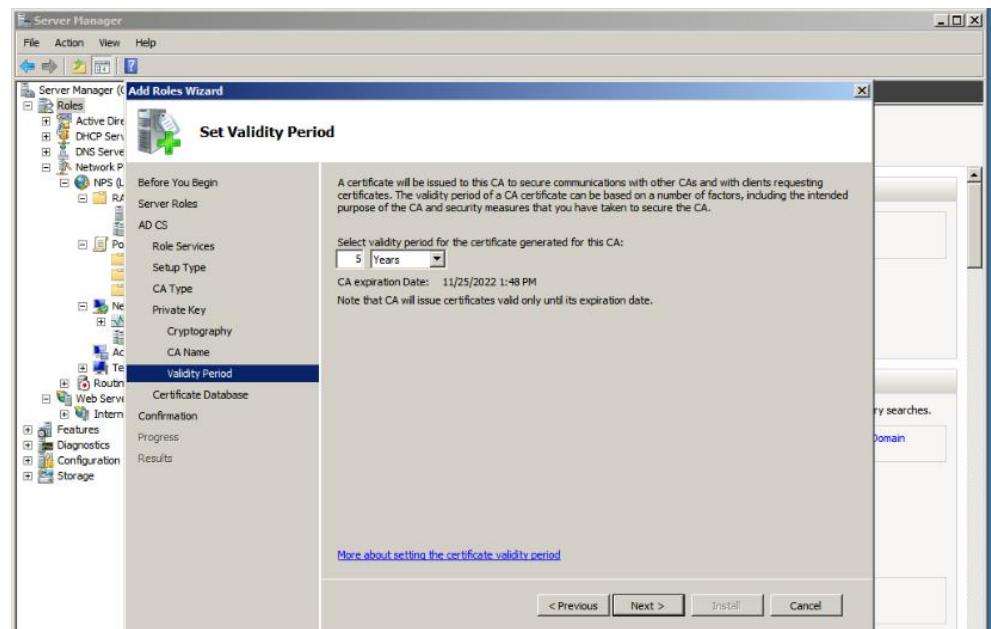


Figure 5. 514: Configure Validity Period

Step 11: In Select Certification Database, Enter the location for certification database and certification database log in C:\Windows\system32\Certlog. Then, click Next.

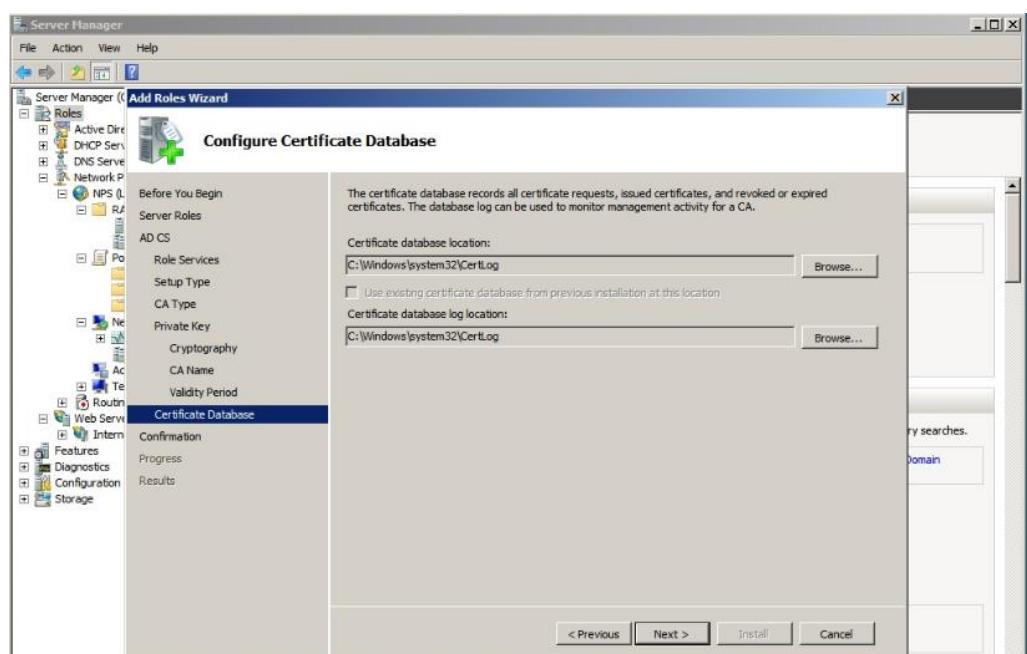


Figure 5. 515: Certification Database

Step 12: In Confirm Installation Selections page, click Install.

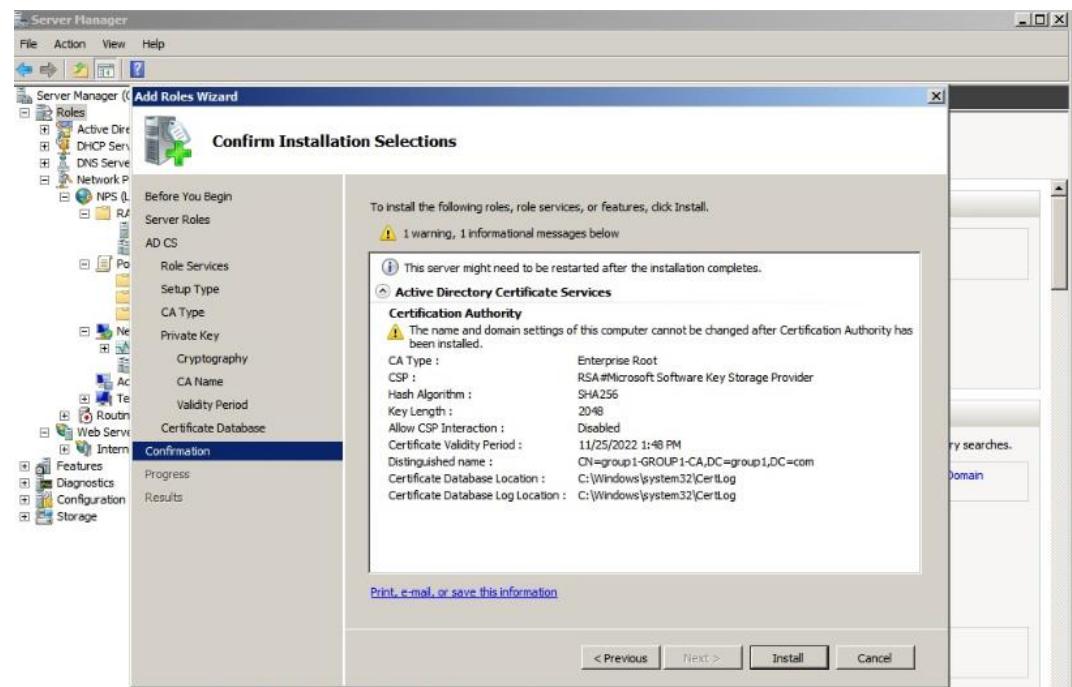


Figure 5. 516: Installation Page

Step 13: In Installation Results page show Installation succeeded. Then, click Close.

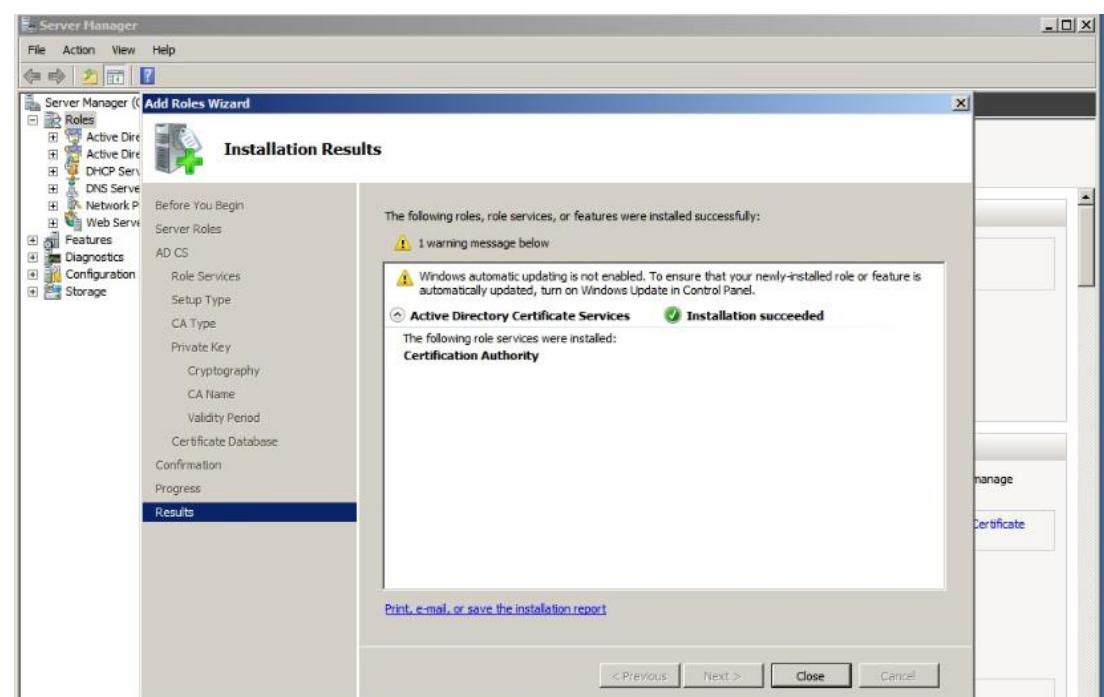


Figure 5. 517: Installation Succeeded

Step 14: Open Console1, click on Files > Add/Remove Snap-in.

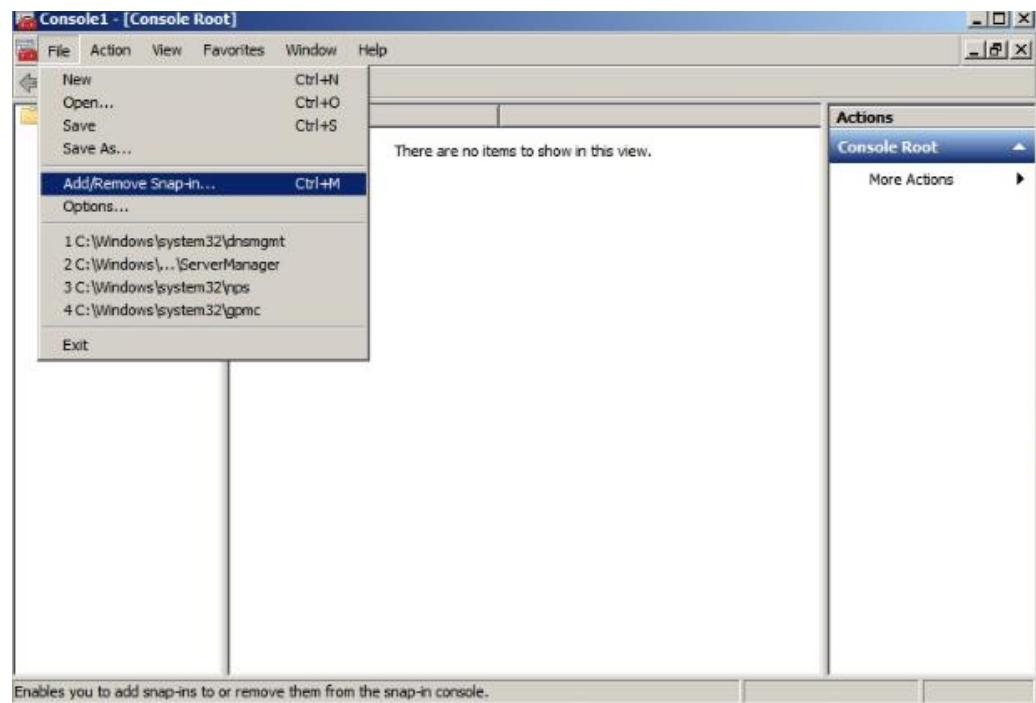


Figure 5. 518: Console

Step 15: In console Add or remove Snaps-ins, expand Certificates and click on Computer account. Then, click Next.

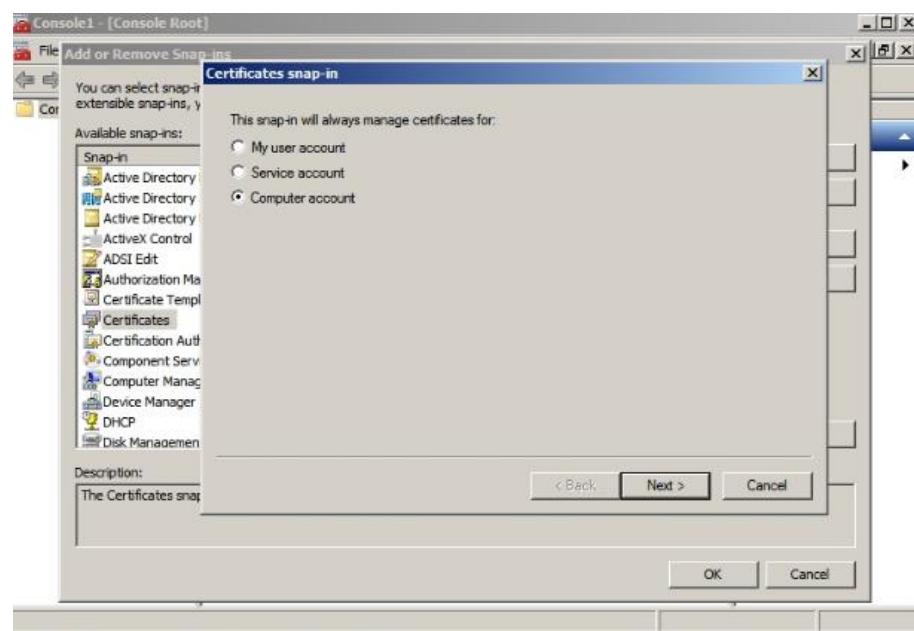


Figure 5. 519: Certificates snap-in

Step 16: Tick on Local computer (the computer this computer is running on).

Then, click Finish.

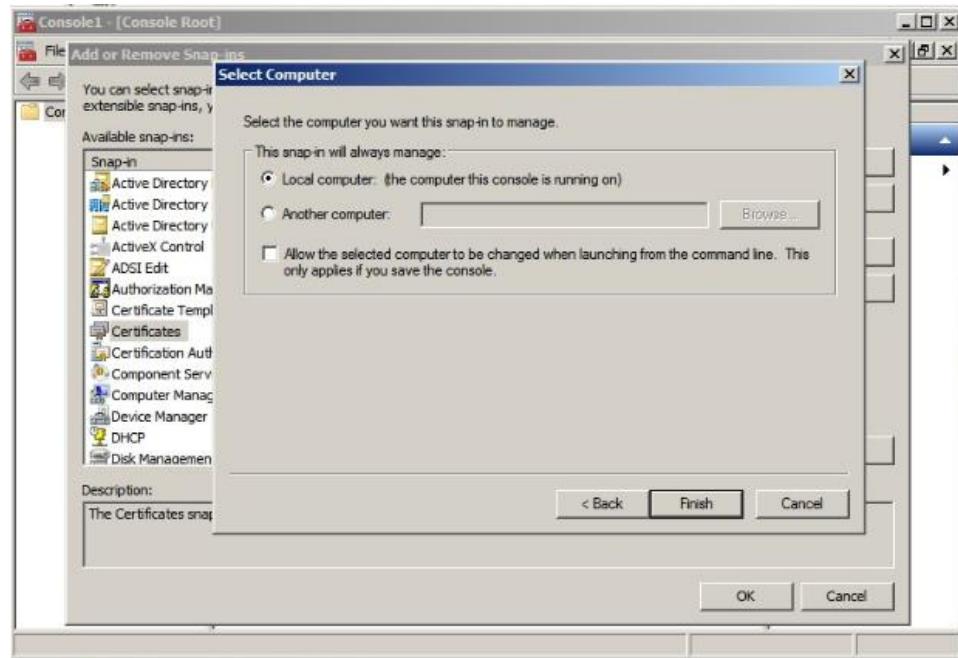


Figure 5. 520: Certificates Local Computer

Step 17: In selected snap-ins box, expand Console Root. Then, Add Certificates Templates and Certification Authority (Local).

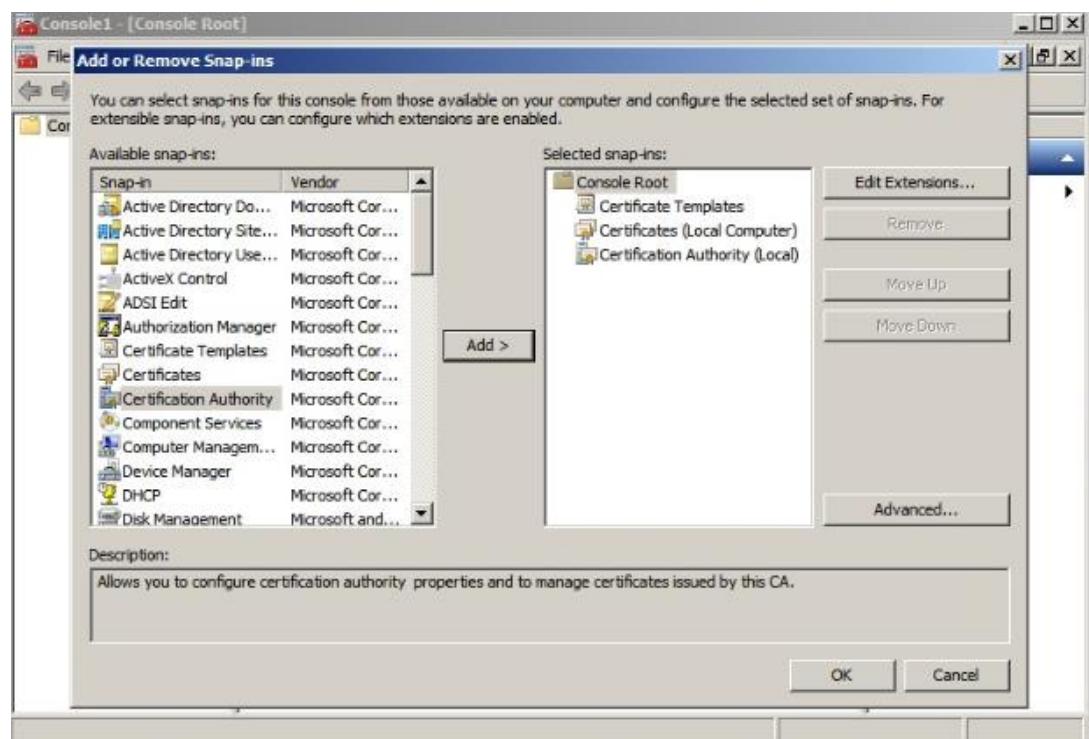


Figure 5. 521: Add or Remove Snap-ins

Step 18: In Certification Templates, expand Computer and click on duplicate computer.

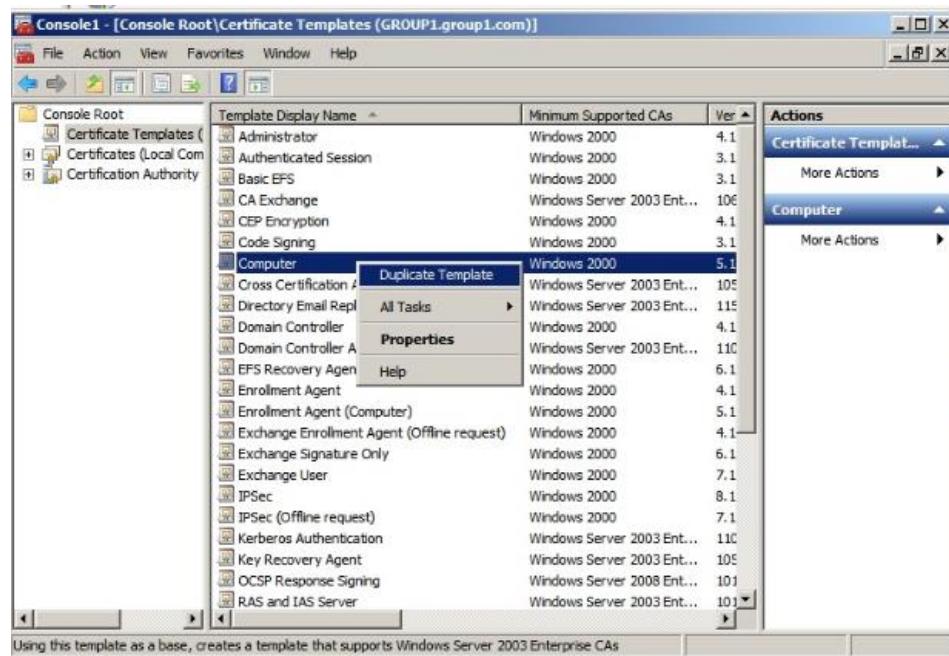


Figure 5. 522: Duplicate Computer Certificates

Step 19: After Duplicate Template pops up, tick Windows Server 2008 Enterprise. Then, click OK

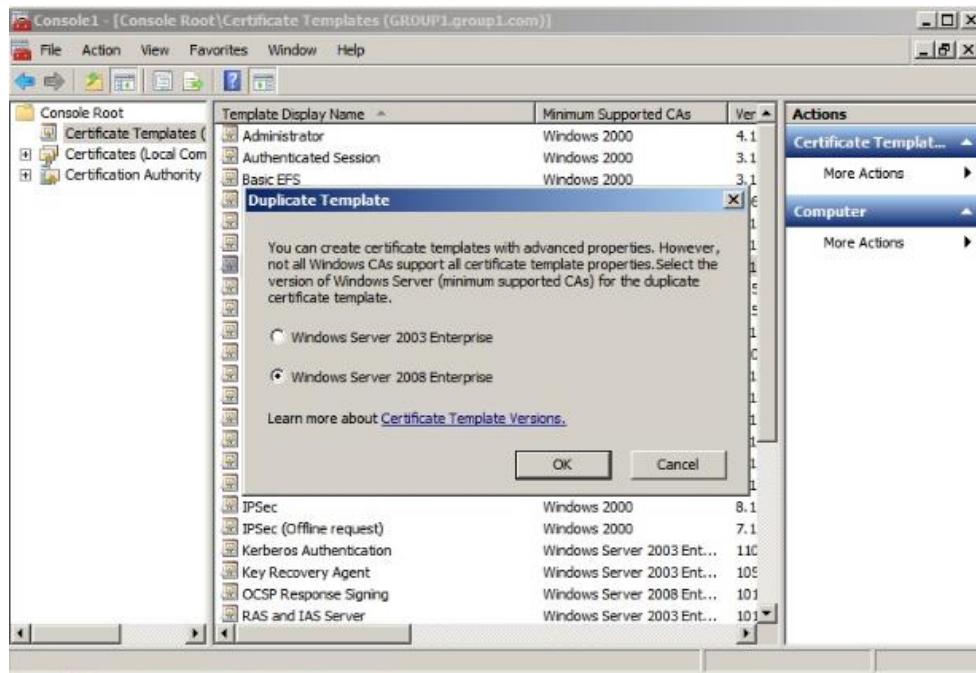


Figure 5. 523: Duplicate Template

Step 20: In Properties of New Template click on General attributes box enter Template display name: Radius Authentication. Then, Click OK.

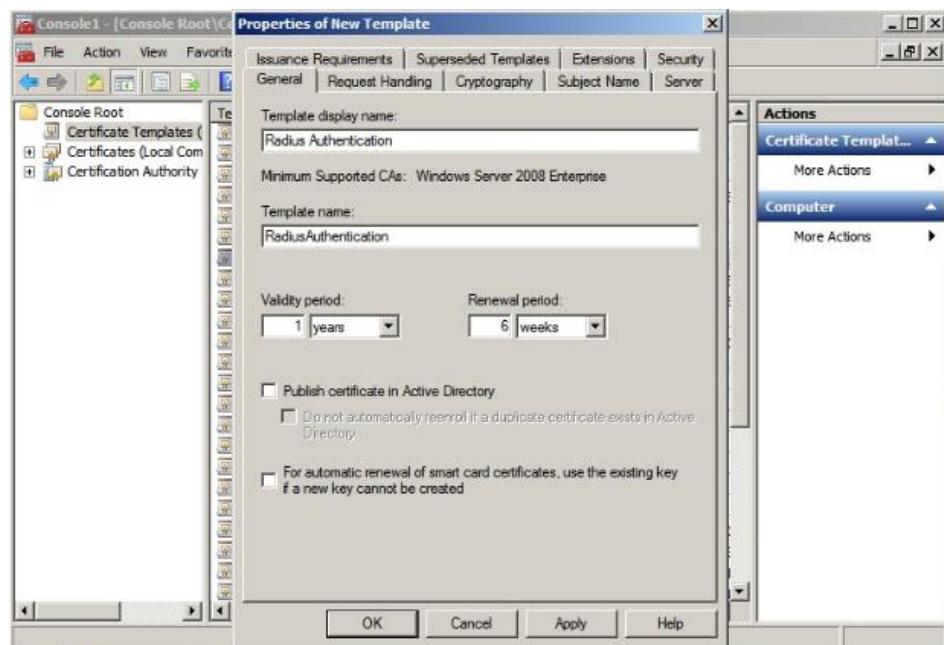


Figure 5. 524: Properties of New Template

Step 21: In Properties of New Template click on Subject Name attributes box tick on Build from this Active Directory information and select Fully distinguished name. Then, Click OK.

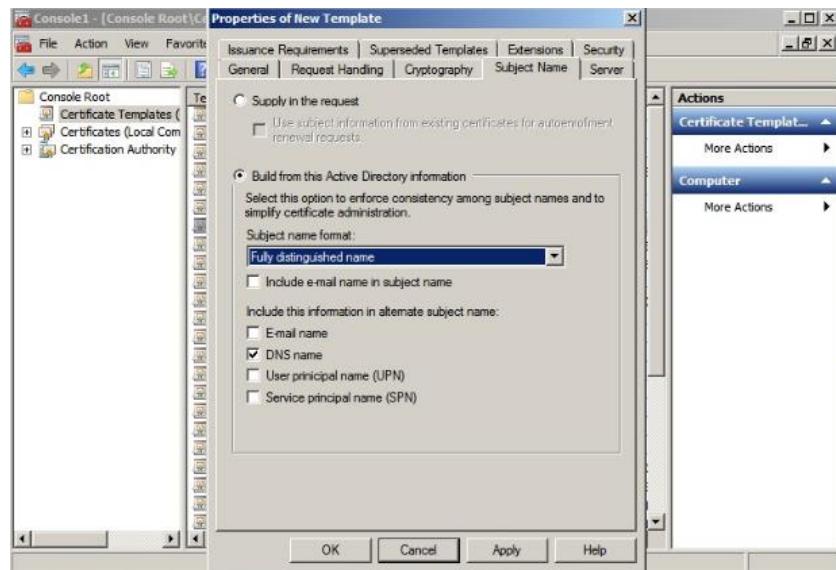


Figure 5. 525: Properties of New Template

Step 22: In Properties of New Template click on Security attributes box on Authenticated User tick on Read, Enroll and Autoenroll.

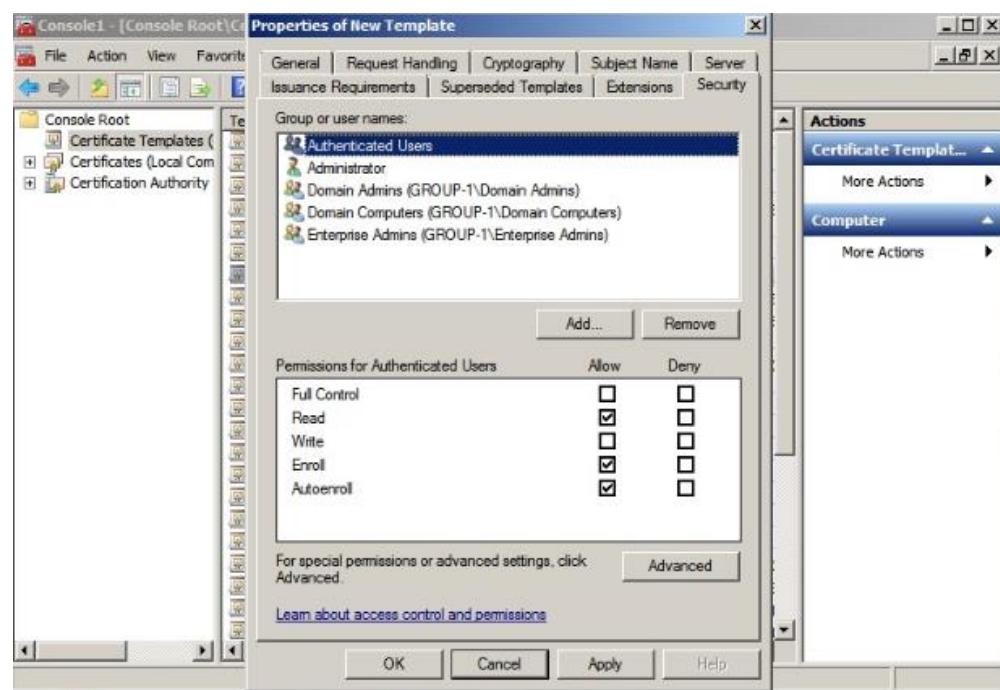


Figure 5. 526: Security New Template

Step 23: In Properties of New Template click on Security attributes box on Domain Computers (GROUP-1\Domain Computers) tick on Read and Autoenroll. Then, Click OK.

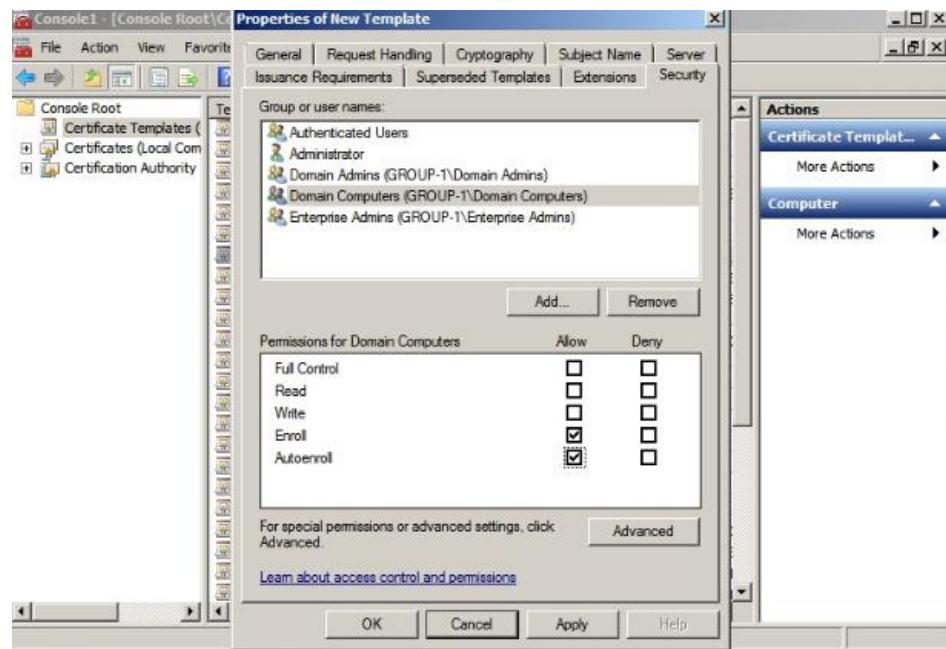


Figure 5. 527: Security New Template

Step 24: Go to Certification Authority, expand and select Certificate Templates. Right click and select New> Certificate Template to issue.

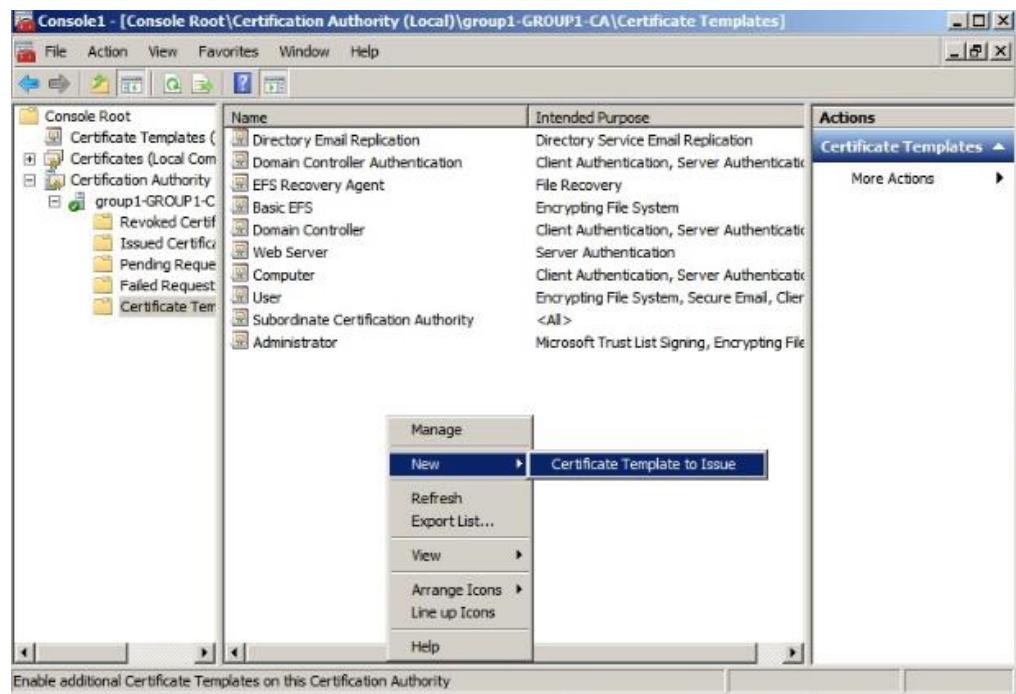


Figure 5. 528: Certification Authority

Step 25: Enable Certificate Template box will pop up, tick on Radius Authentication. Then click OK.

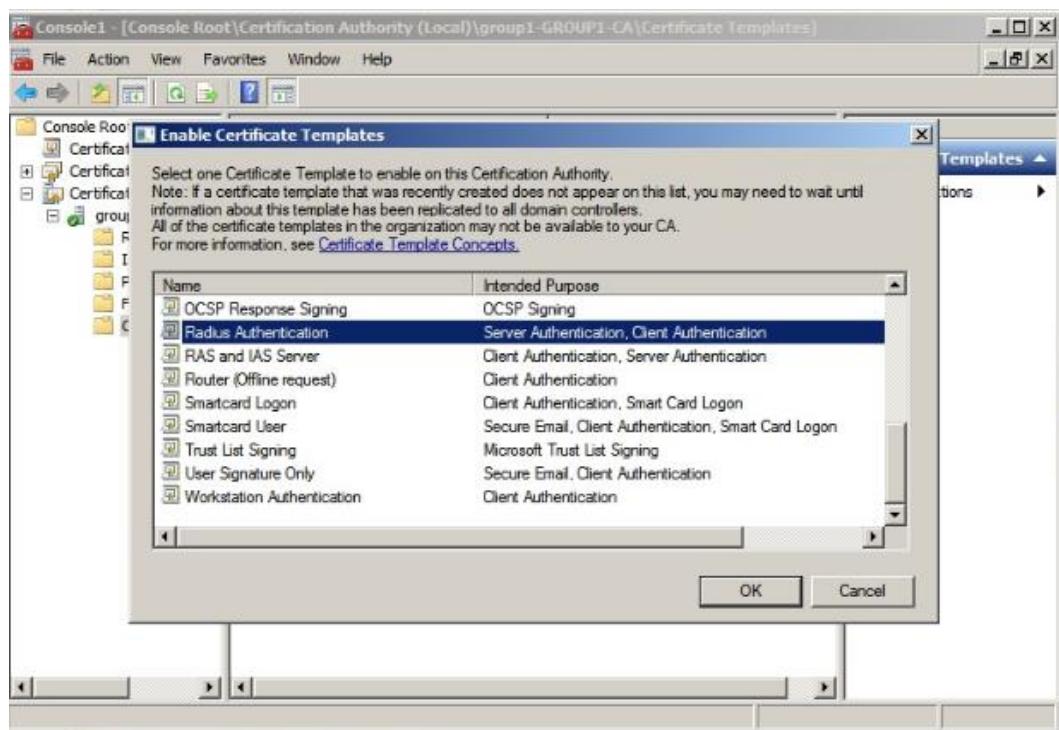


Figure 5. 529: Enable Certification Template

Step 26: Click on Certificates (Local Computer) > Personal > Certificates, Right-click mouse and select All Tasks > Request New Certificate.

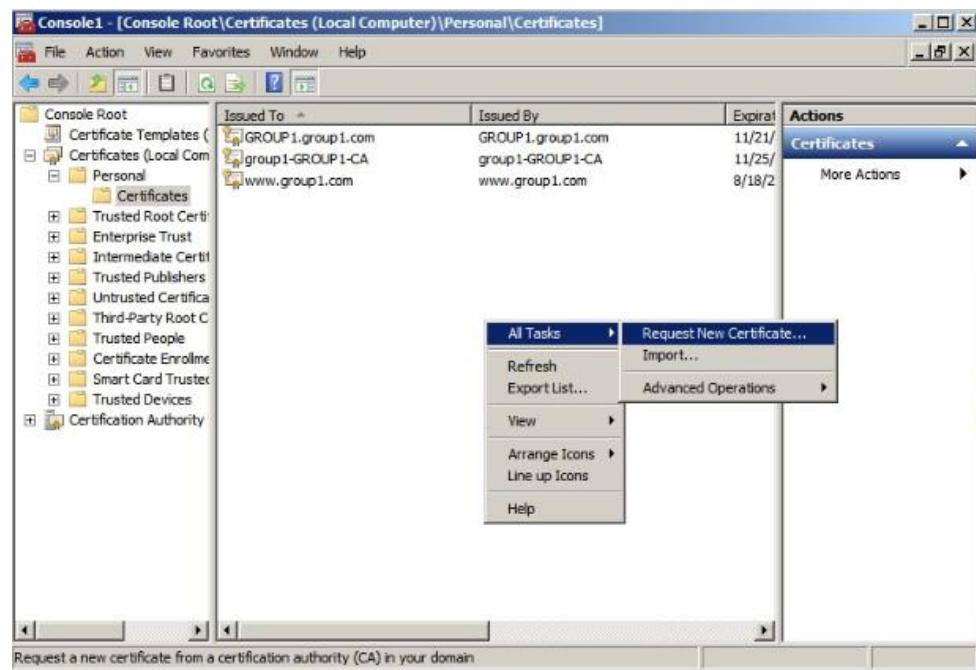


Figure 5. 530: Request New Certificate

Step 27: Certificate Enrollment box will pop up, tick on Radius Authentication.

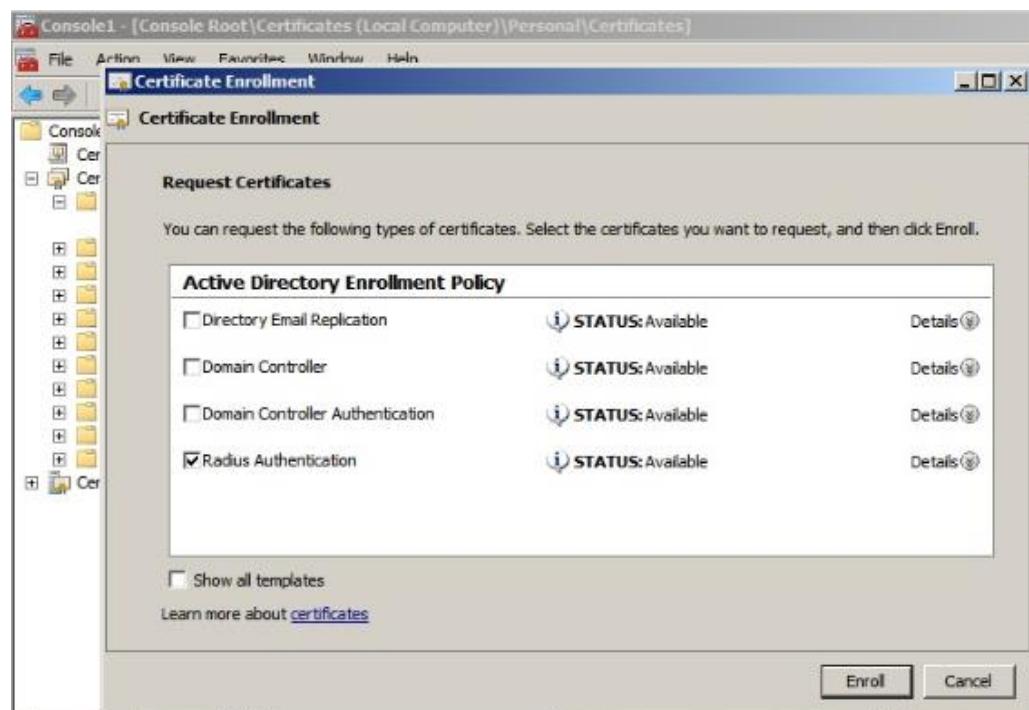


Figure 5. 531: Cetification Enrollement

Step 28: Select Radius Authentication, click on Details.

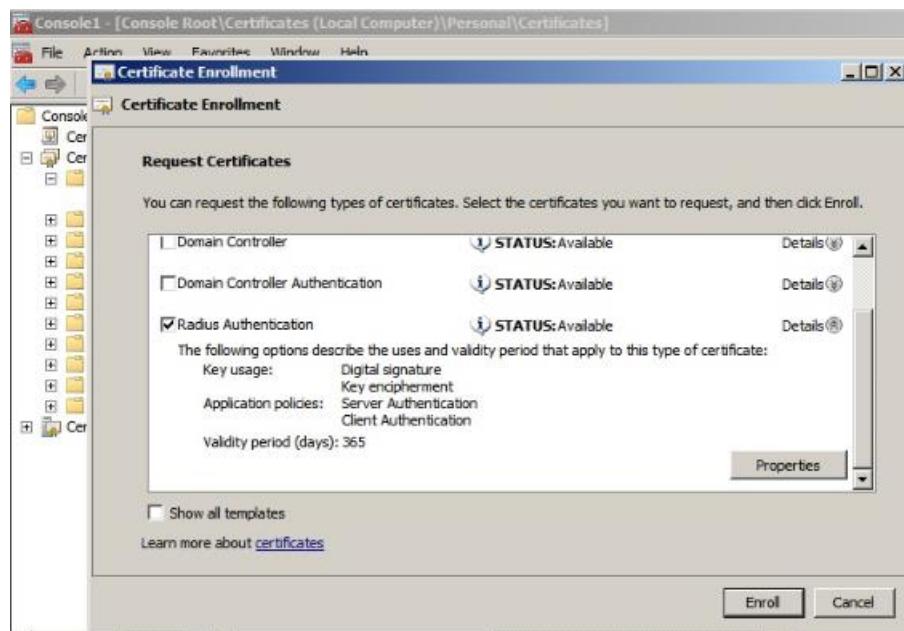


Figure 5. 532: Radius Authentication

Step 29: Click Properties, tick on Enable this extension. Then Click OK.

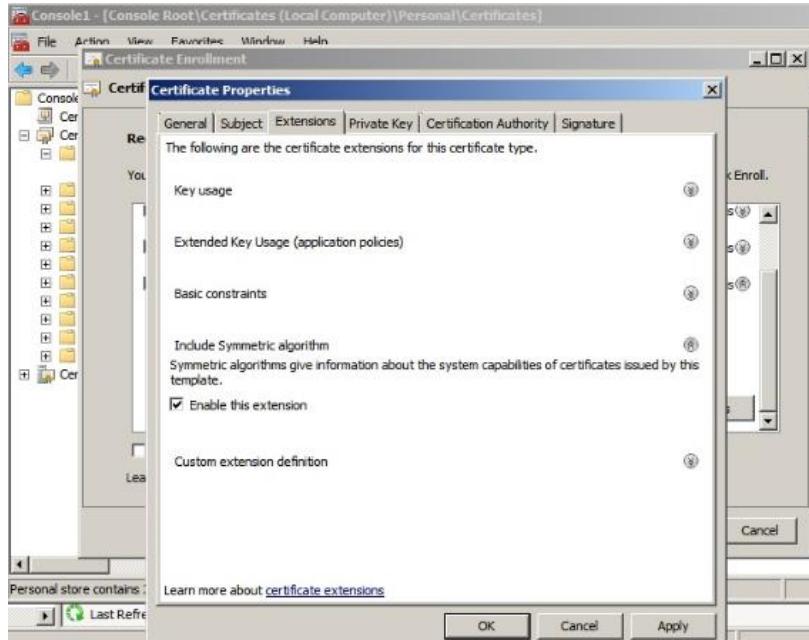


Figure 5. 533: Certification Properties

Step 30: In Certification Installation Results page show Status: succeeded. Then, click Finish.

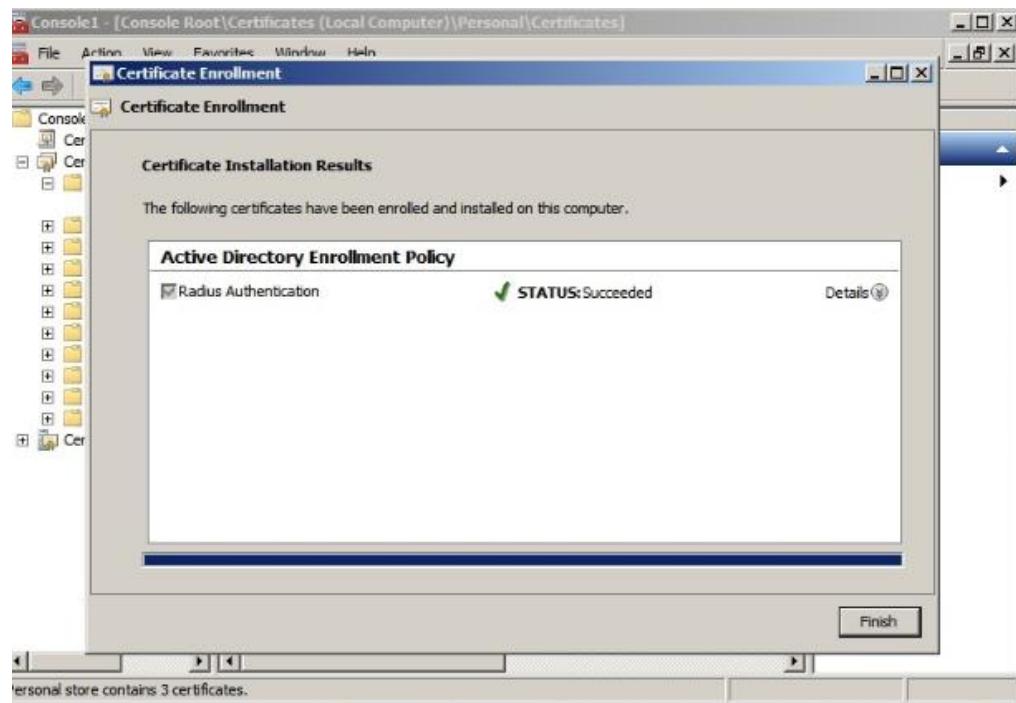


Figure 5. 534: Installation Page

Step 31: Go to Network Policy Server, select radio Radius server for 802.1X Wireless or Wired Connection. Then, click Configure 802.1X.



Figure 5. 535: Configure Wireless Radius

Step 32: Next, popup windows tick Secure Wireless Connections, enter Name:

Secure Wireless Connections.

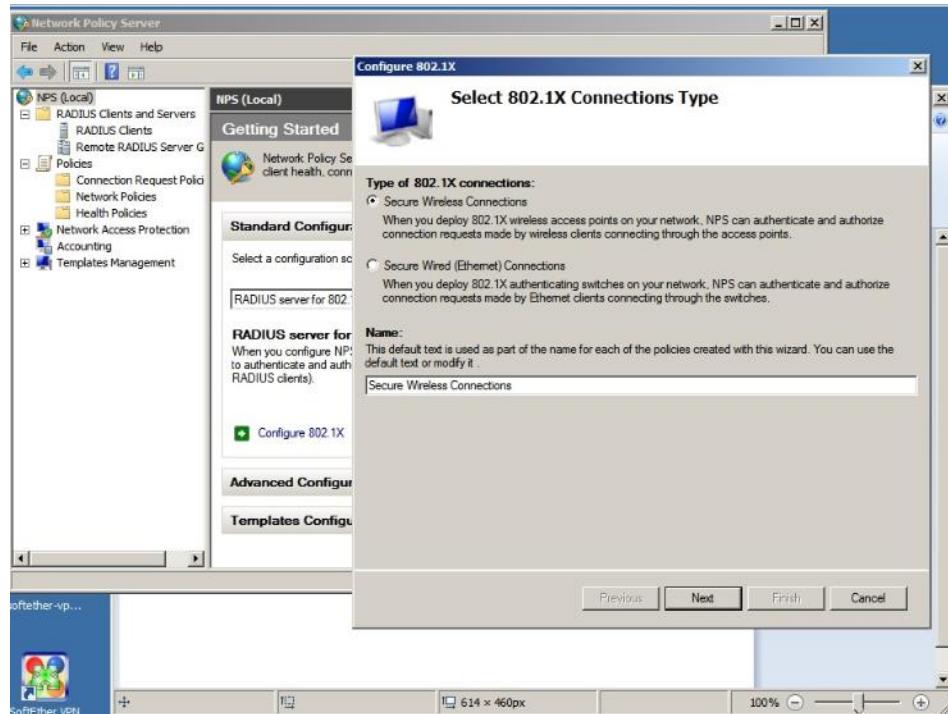


Figure 5. 536: Configure 802.1X

Step 33: On New Radius Client box, enter Friendly name: Wireless Radius IP

address 192.168.11.34 and Shared Secret: Abc12345. Then click OK.

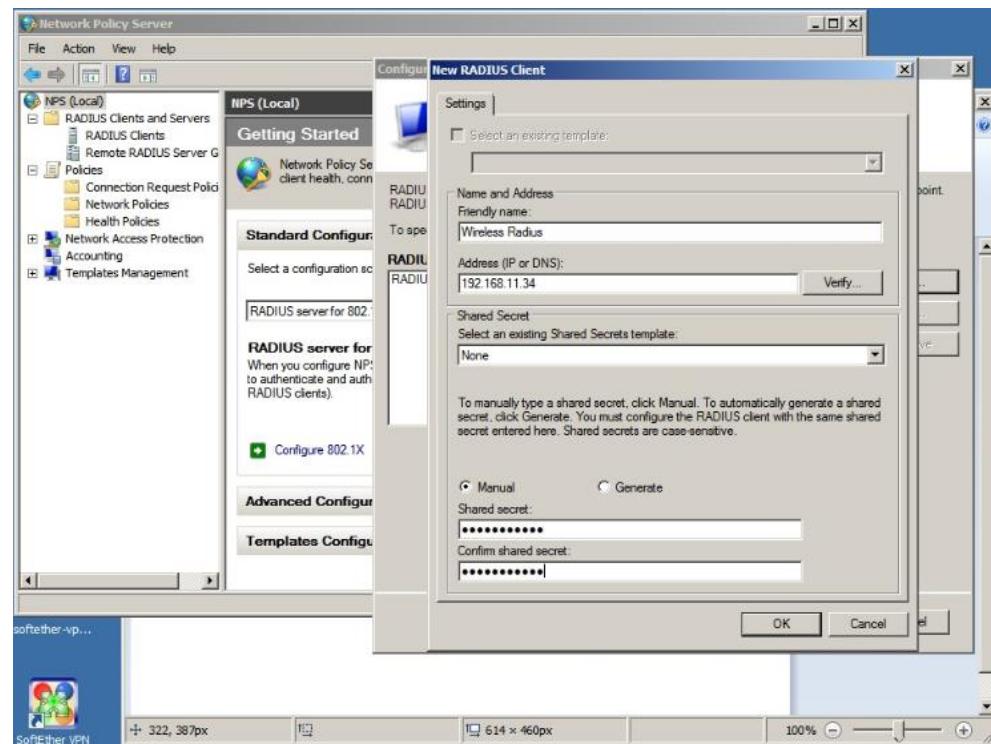


Figure 5. 537: New Radius Client

Step 34: On Configure an Authentication Method, select Microsoft Protected EAP (PEAP). Then, Click Configure.

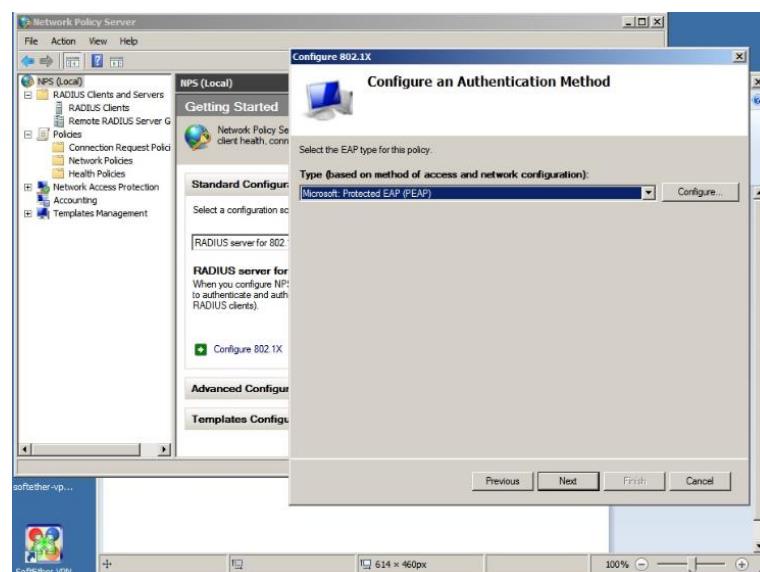


Figure 5. 538: Configure Authentication Method

Step 35: On Edit Protected EAP Properties box, enter value 5 for Number of authentication retries.

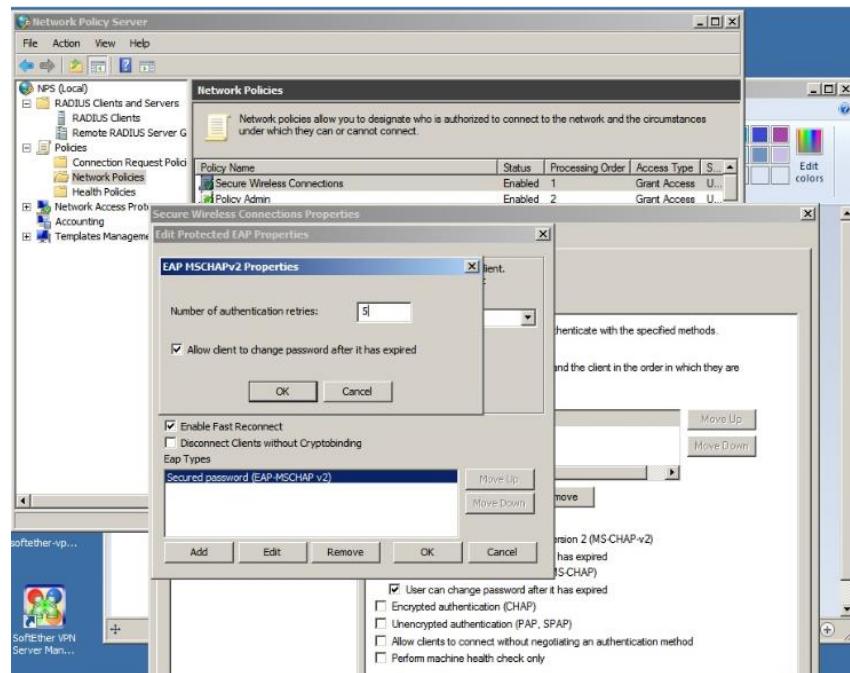


Figure 5. 539: EAP properties

Step 36: On Select Group box, Enter value object type: Group1, From this location: group1.com, object names: Domain Users.

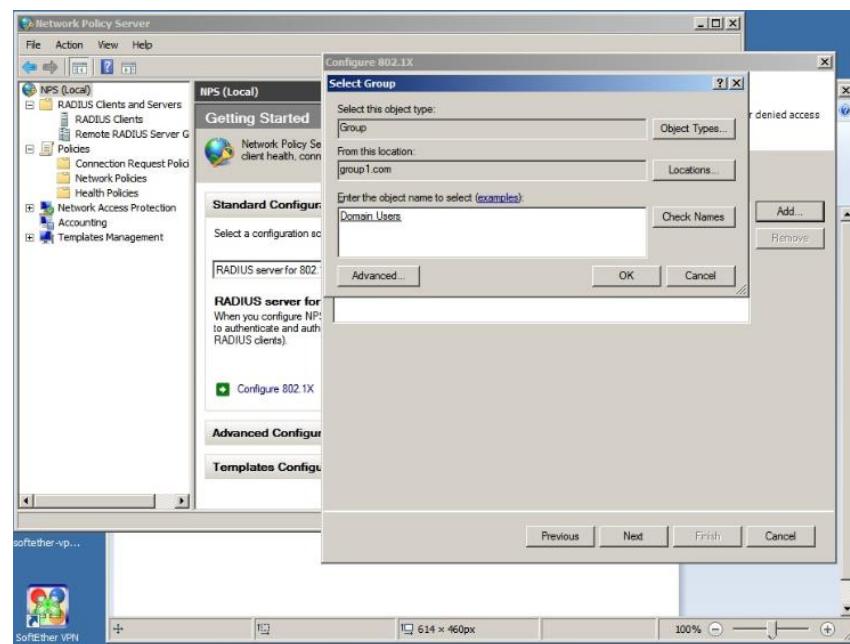


Figure 5. 540: Select Group

Step 37: In Completing New IEEE 802.1X Wired and Wireless Connection and Radius, it will display that successfully created the Radius Client. Click Finish.

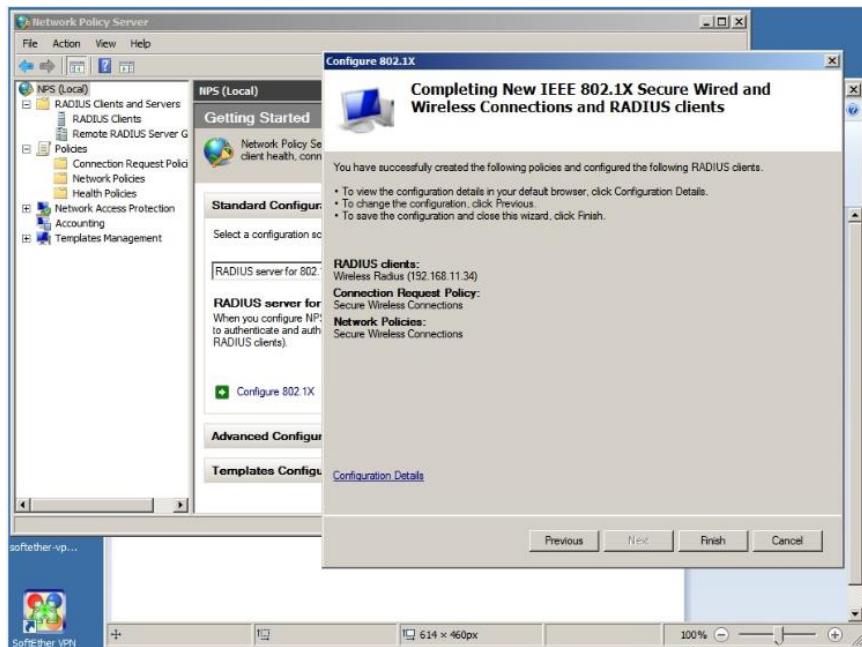


Figure 5. 541: Installation Page

Step 38: Open putty. Select Serial and click Open.

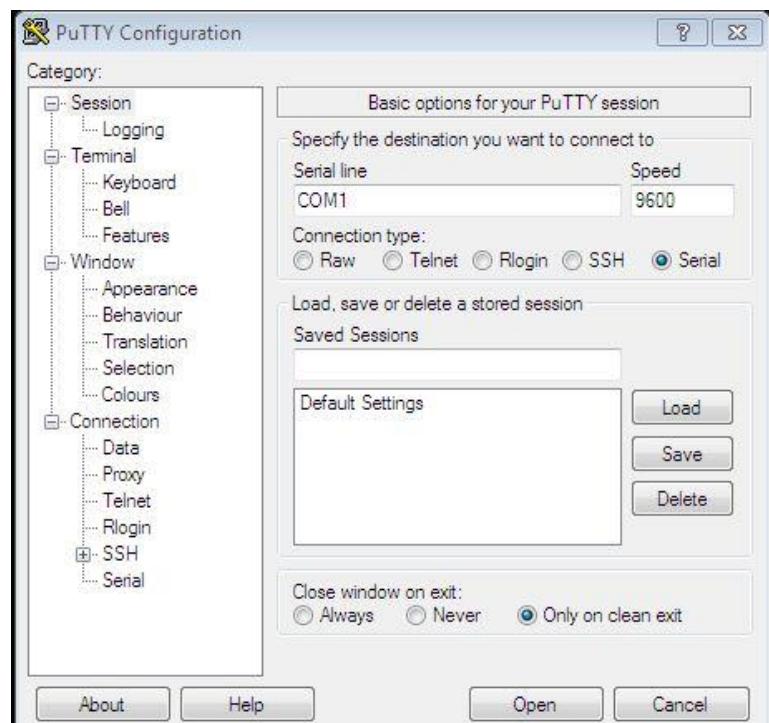


Figure 5. 542: Putty Terminal

Step 39: User Access Verification will display. Enter the username (Any AD users) and password. Enter

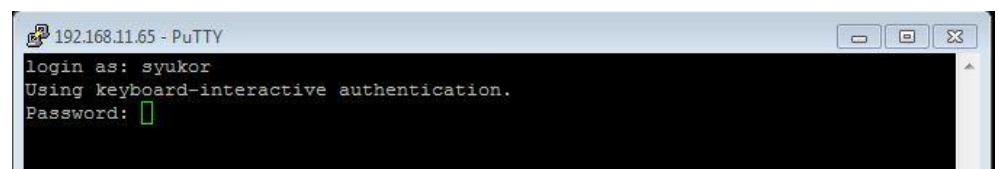


Figure 5. 543: AD username login

Step 40: Enter global configuration mode using command configure terminal.

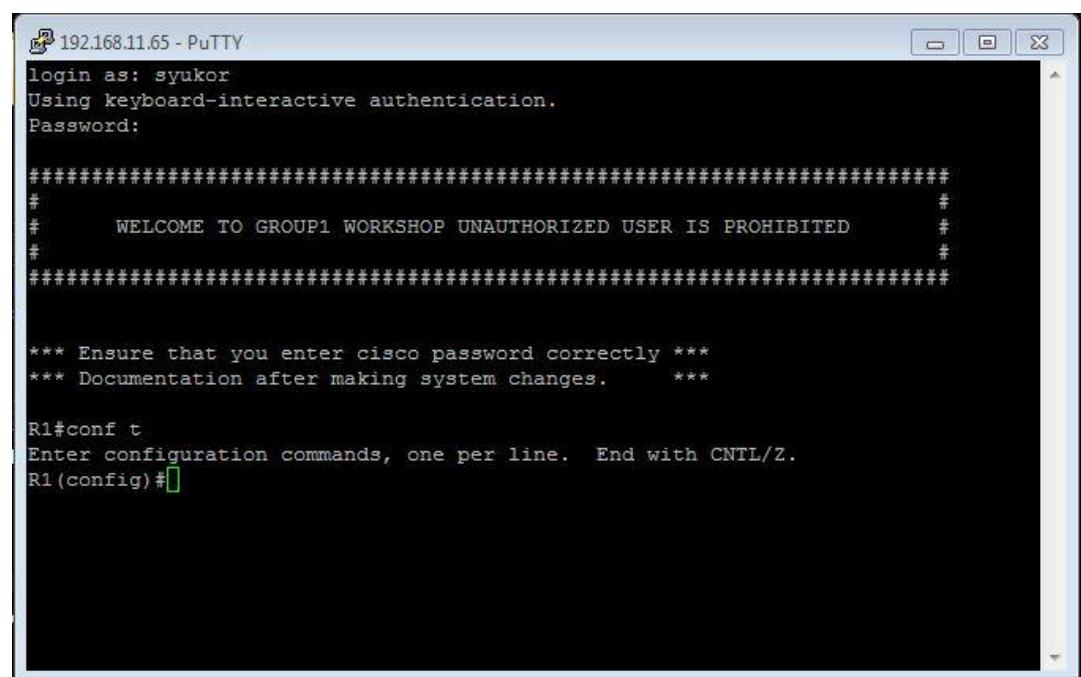


Figure 5. 544: Global configuration

Step 41: Setup Vlan 60 for wireless Radius in the putty terminal

```

COM1 - PuTTY
Username: syukor
Password:

*** Ensure that you enter cisco password correctly ***
*** Documentation after making system changes. ***

R1#
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0.60
R1(config-subif)#encap dot1q 60
R1(config-subif)#ip add 192.168.60.1 255.255.255.0
R1(config-subif)#exit
R1(config)#end
R1#c
Nov 28 20:15:52.223 UTC: %SYS-5-CONFIG_I: Configured from console by syukor on c
onsole
R1#copy r s
Destination filename [startup-config]?
Building configuration...

[OK]
R1#

```

Figure 5. 545: Create VLAN 60

Step 42: Open putty. Select Serial and click Open.

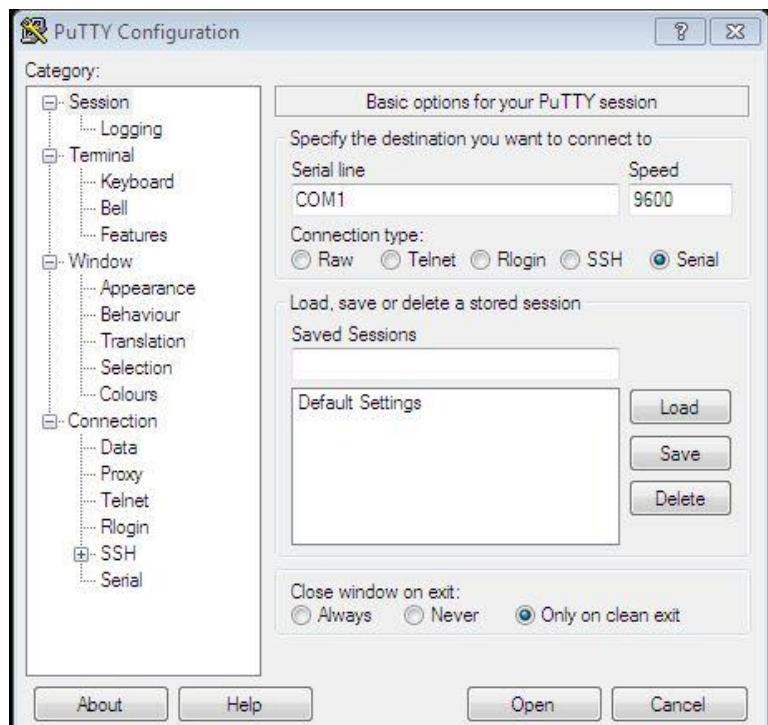
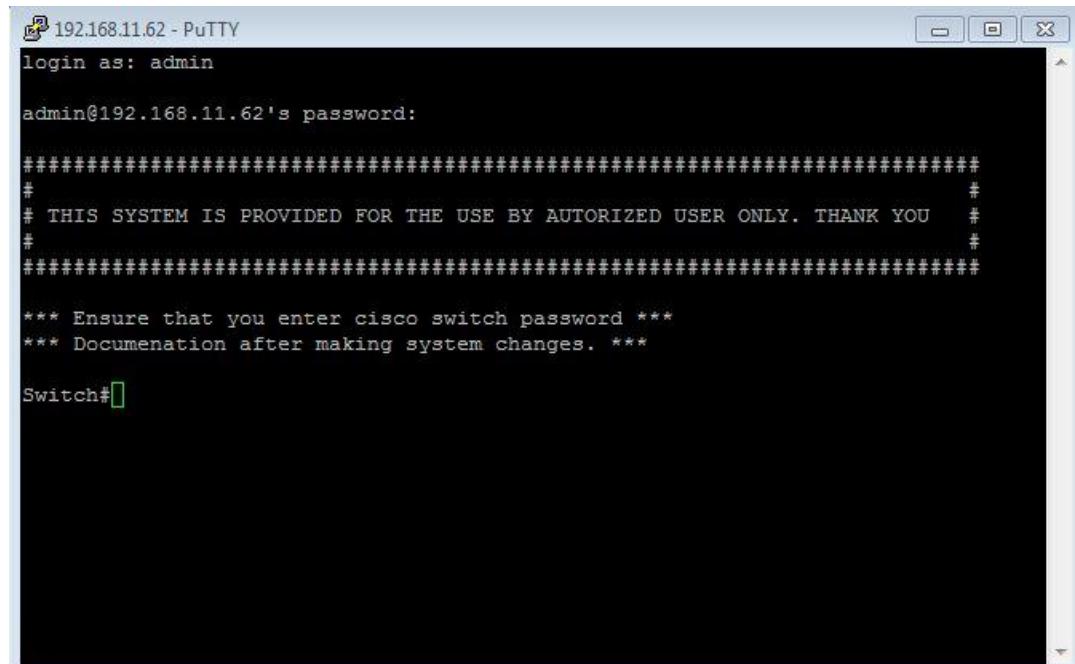


Figure 5. 546: Putty Terminal

Step 43: User Access Verification will display. Enter the username admin and password admin01. Enter



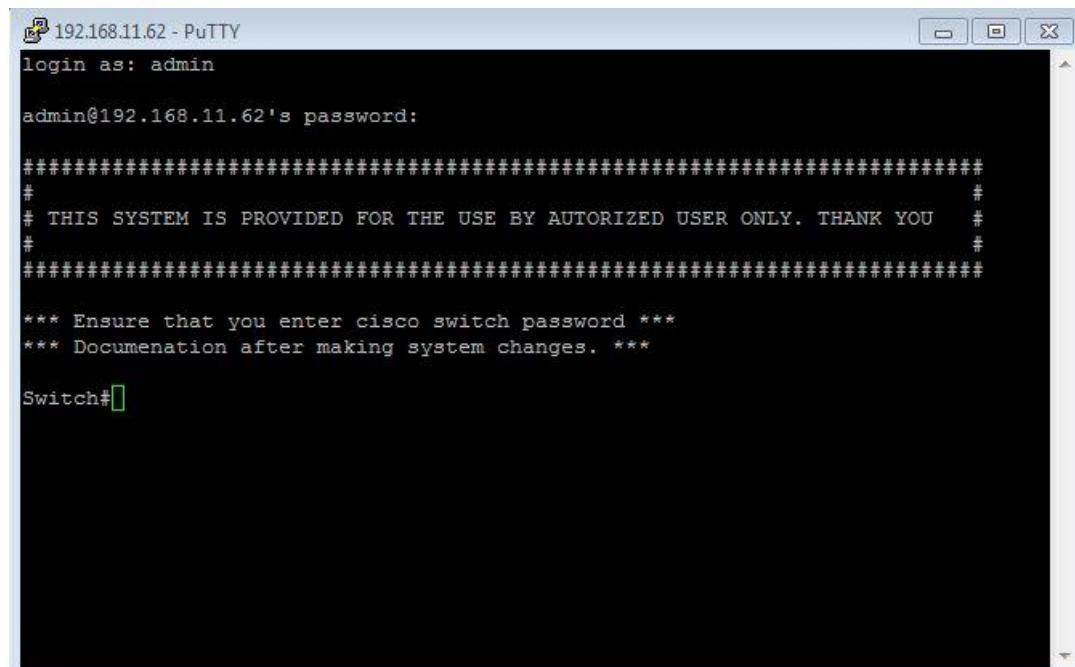
A screenshot of a PuTTY terminal window titled "192.168.11.62 - PuTTY". The session is logged in as "admin". The password prompt "admin@192.168.11.62's password:" has been entered, followed by several lines of system documentation. The command "Switch# [ ]" is displayed at the bottom.

```
192.168.11.62 - PuTTY
login as: admin
admin@192.168.11.62's password:
#####
#
# THIS SYSTEM IS PROVIDED FOR THE USE BY AUTORIZED USER ONLY. THANK YOU
#
#####
*** Ensure that you enter cisco switch password ***
*** Documentation after making system changes. ***

Switch# [ ]
```

Figure 5. 547: Switch login admin

Step 44: Enter global configuration mode using command configure terminal.



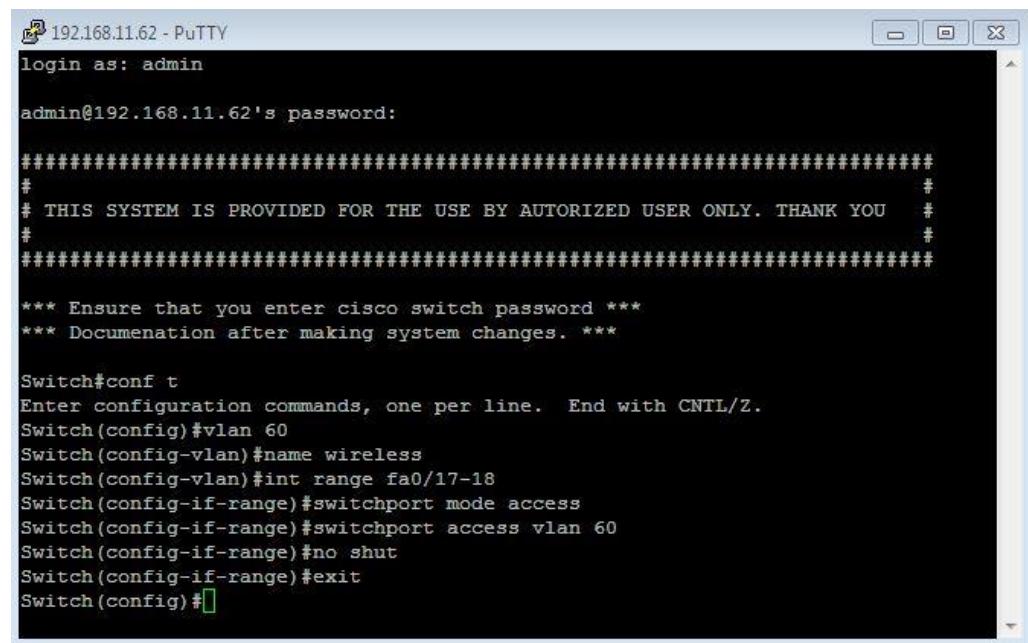
A screenshot of a PuTTY terminal window titled "192.168.11.62 - PuTTY". The session is logged in as "admin". The password prompt "admin@192.168.11.62's password:" has been entered, followed by several lines of system documentation. The command "Switch# [ ]" is displayed at the bottom.

```
192.168.11.62 - PuTTY
login as: admin
admin@192.168.11.62's password:
#####
#
# THIS SYSTEM IS PROVIDED FOR THE USE BY AUTORIZED USER ONLY. THANK YOU
#
#####
*** Ensure that you enter cisco switch password ***
*** Documentation after making system changes. ***

Switch# [ ]
```

Figure 5. 548: Global configuration

Step 45: Setup Vlan 60 in switch in the putty terminal



```

192.168.11.62 - PuTTY
login as: admin
admin@192.168.11.62's password:
#####
#
# THIS SYSTEM IS PROVIDED FOR THE USE BY AUTORIZED USER ONLY. THANK YOU
#
#####
*** Ensure that you enter cisco switch password ***
*** Documentation after making system changes. ***

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 60
Switch(config-vlan)#name wireless
Switch(config-vlan)#int range fa0/17-18
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 60
Switch(config-if-range)#no shut
Switch(config-if-range)#exit
Switch(config)#

```

Figure 5. 549: Configure Vlan 60

Step 46: Switch on Cisco Access Point Device

Step 47: Open web browser and type IP Address 192.168.60.3, The page will browse to Access Router sign-in, Enter password Abc12345. Then, Click Sign in.

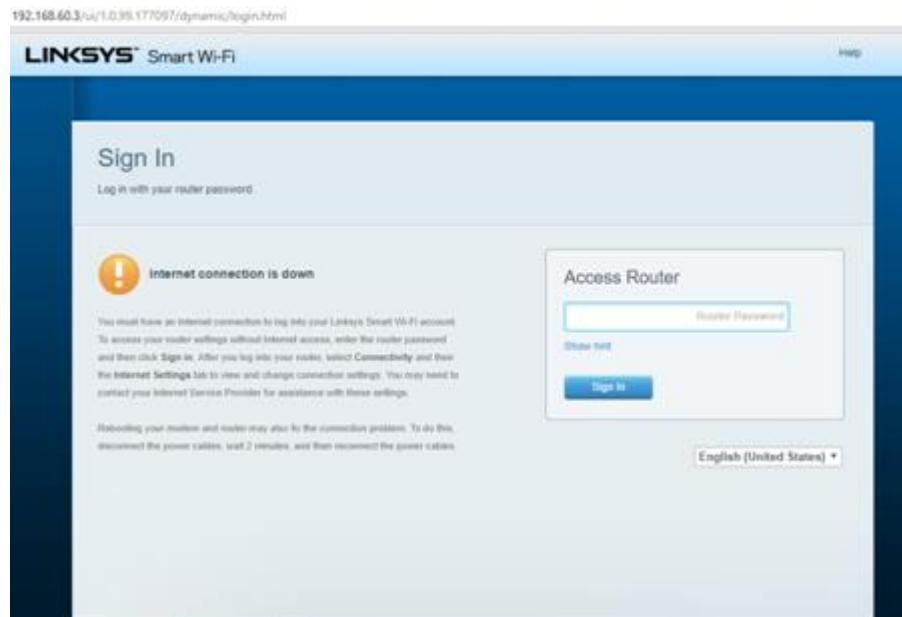


Figure 5. 550: Access Router sign in

Step 48: In Connectivity, go to Internet Setting, edit type of connection: Static IP, Internet IPv4 address 192.168.60.3 Subnet mask 255.255.255.248 Default gateway 192.168.60.1 DNS 192.168.11.34.

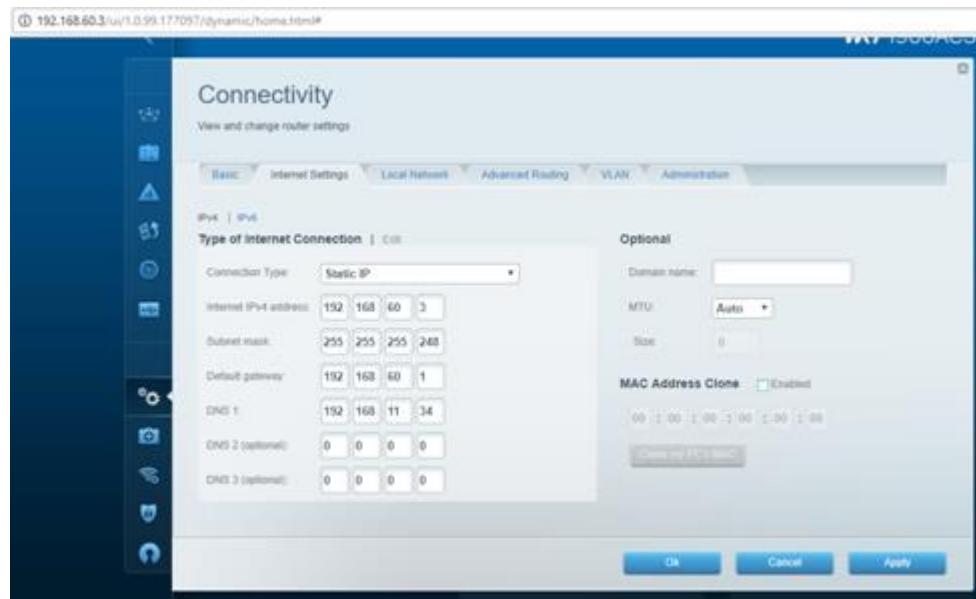


Figure 5. 551: Connectivity Setting

Step 49: In Connectivity, go to Local Network, tick DHCP server enabled and set Static IP address 192.168.1.100, Maximum number of users: 100 Static DNS 192.168.11.34.

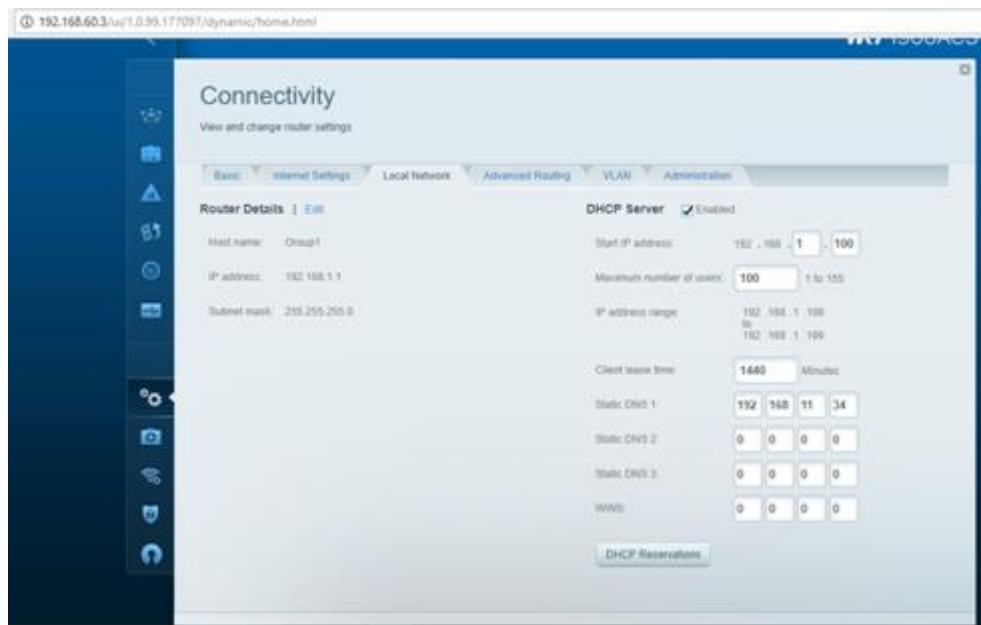


Figure 5. 552: Setup the DHCP server

**Problem:** Some users want a secure the wireless network access, If the wireless connection is not protected. The network can easily penetrate by unauthorized user.

**Solution:** We install Network Policy Server inside Windows Server 2008 and configure access point as wireless radius client. Each user wants to connect with access point must authenticate using AD before he/she can login into the network. This enhanced more secure network and better network authentication and authorization.

### 5.3.33 ACTIVE DIRECTORY

Install Active Directory Domain Services on Windows Server 2008 is use the server to become a domain controller. It is install by using dcpromo.exe. It

provides authentication and authorization mechanisms as a framework within which other related services can be deployed.

## I. Installation in Windows Server

Step 1: Install Active Directory Domain Services in Windows Server.

- a) Open Server Manager → Roles → Add Roles → Ticks Active Directory Domain Services → Next → Install → Close

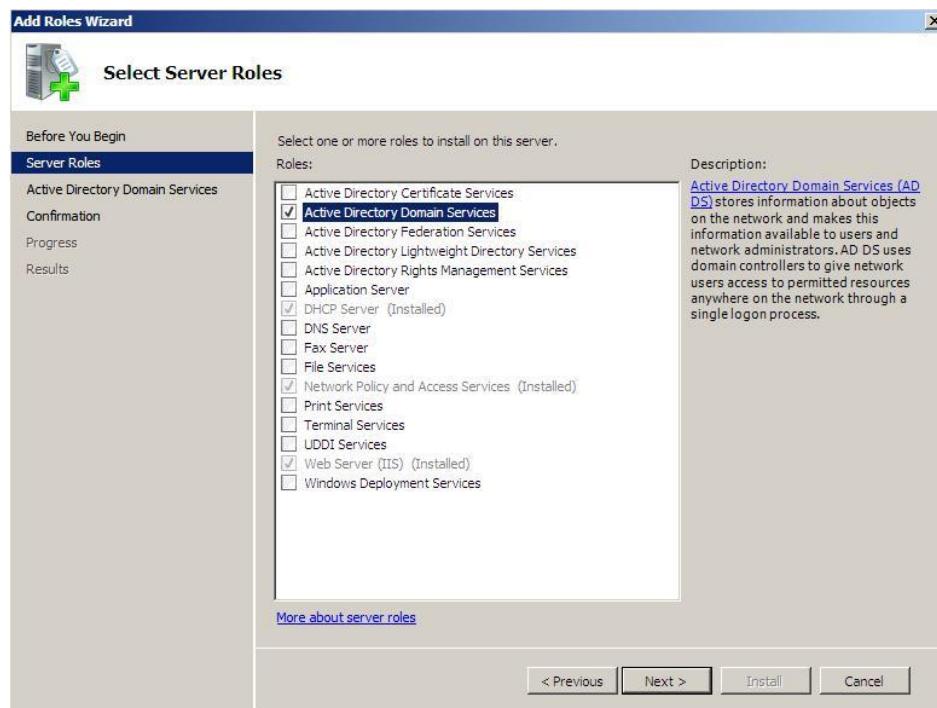


Figure 5. 553: Server Roles Selection

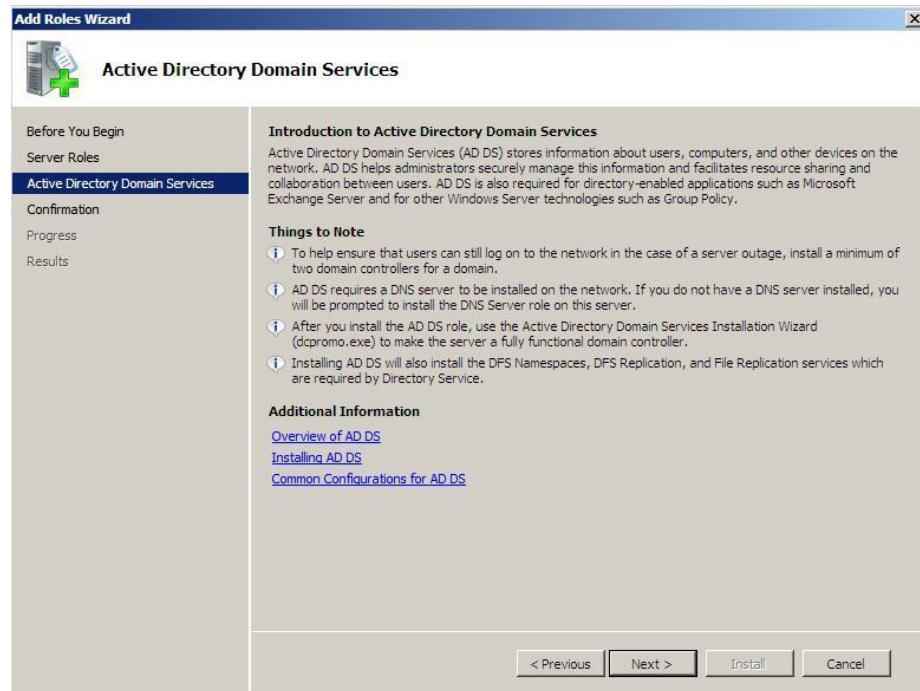


Figure 5. 554: Select Next

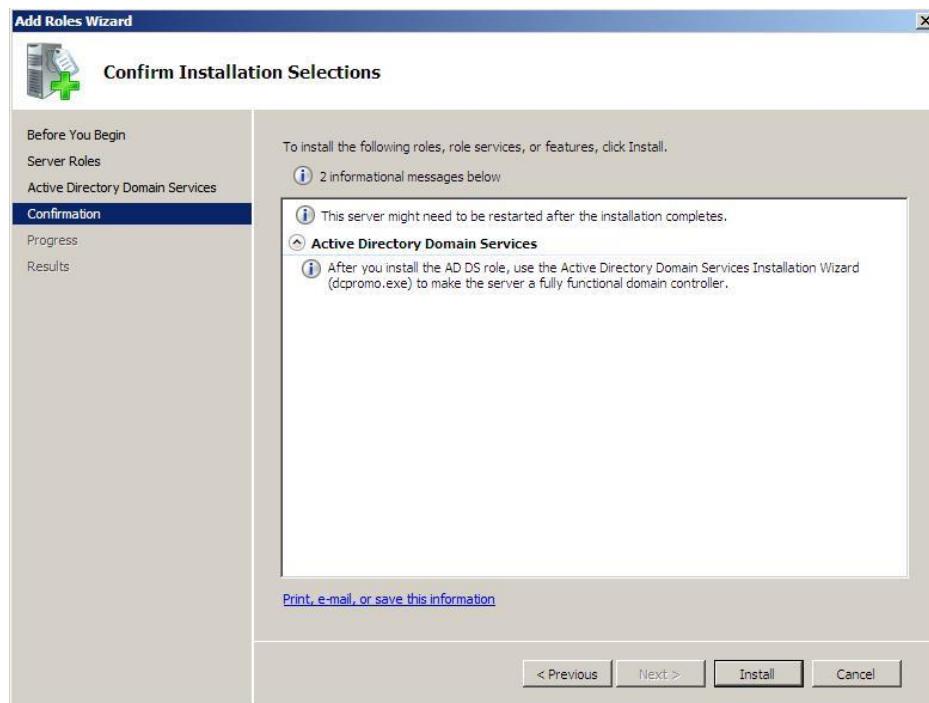


Figure 5. 555: Confirmation before installation AD.

b) The result of installation of Active Directory Domain Services

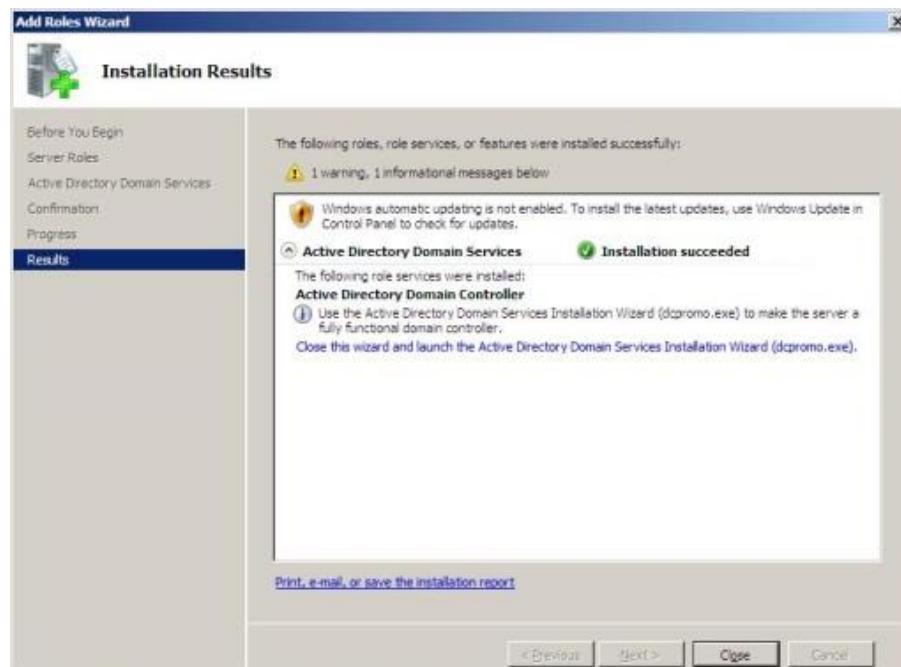


Figure 5. 556: AD installation status

- c) Start menu → type dcromo.exe → Enter
- d) Next → Click second radio button, Create new domain in a new forest →  
Next → Name the forest root name as group1.com



Figure 5. 557: Select Next

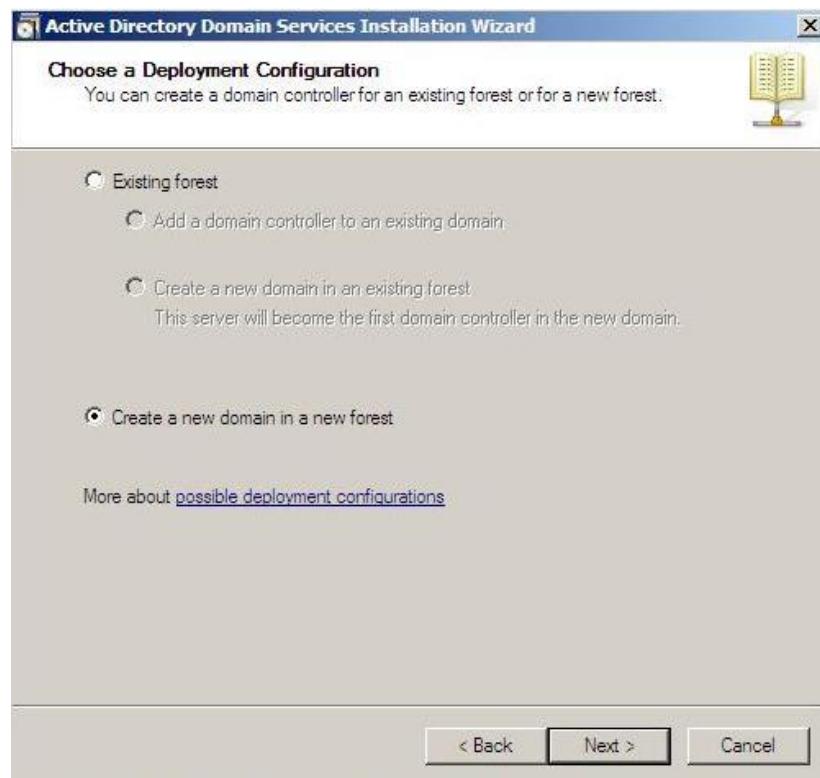


Figure 5. 558: Deployment configuration

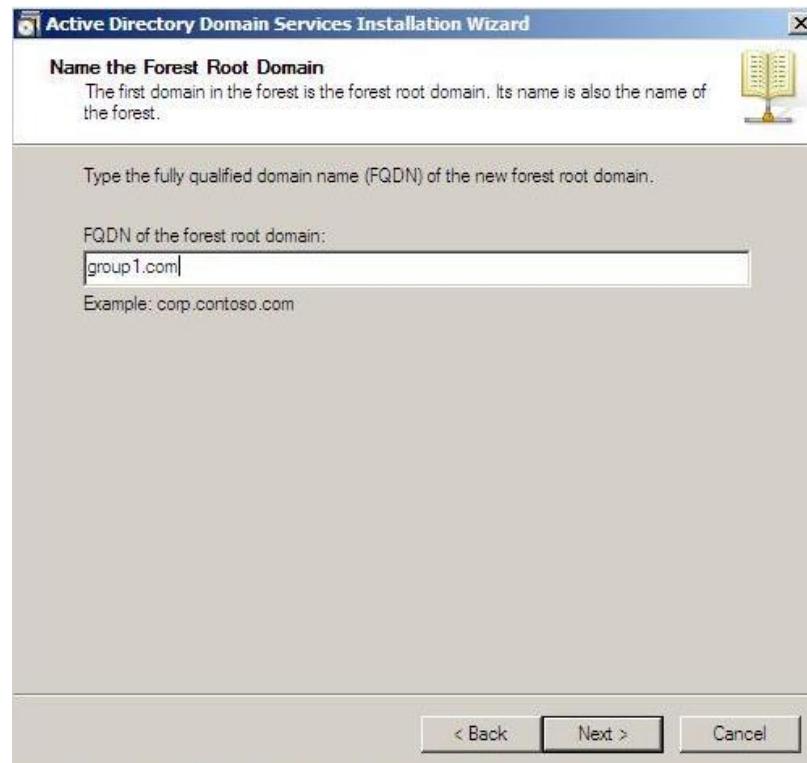


Figure 5. 559: Naming the forest root domain

- e) Choose Windows Server 2008 → Next → tick DNS Server → Next → Next  
→ Enter password → Next → summary review → Next → Next → Finish

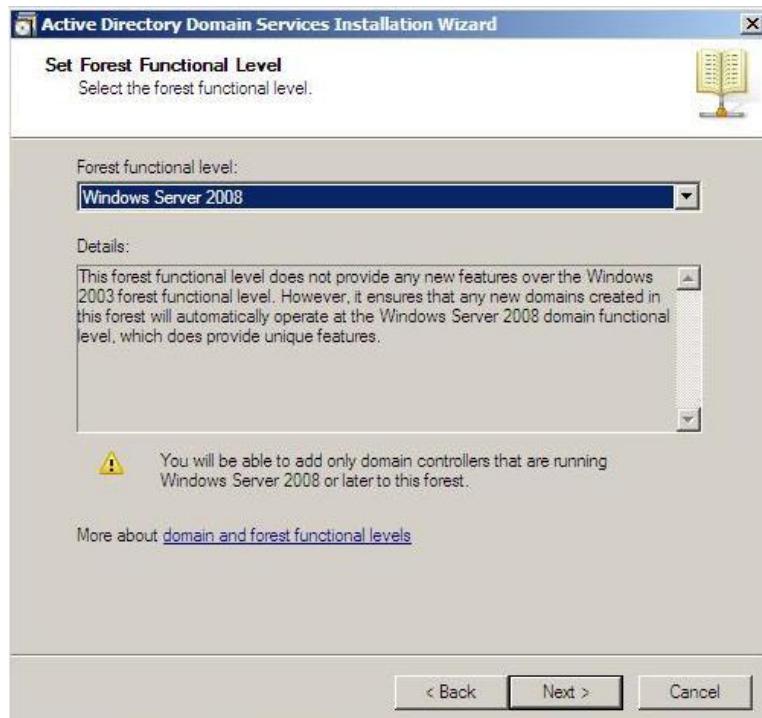


Figure 5. 560: Setting forest functional level

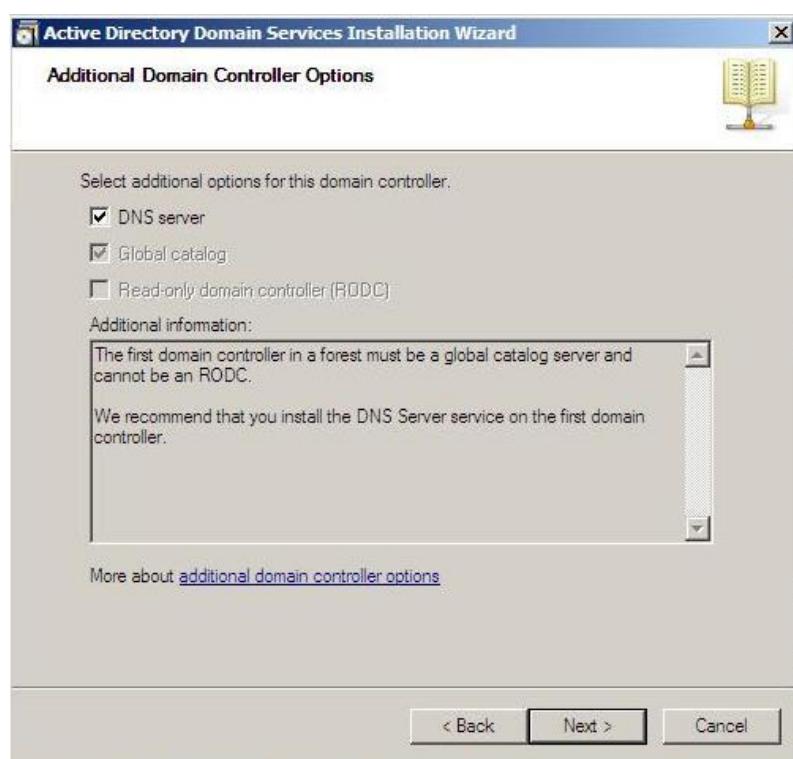


Figure 5. 561: Additional domain controller options



Figure 5. 562: Select Yes for confirmation

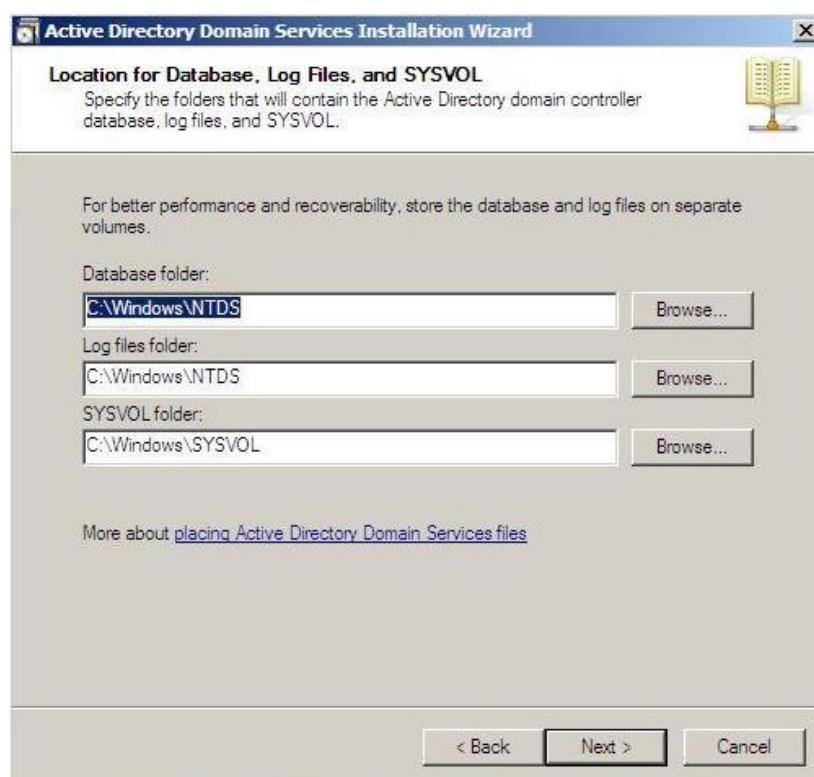


Figure 5. 563: Configuration location for Database, Log files and  
SYSVOL



Figure 5. 564: Setup of Directory Services Restore Mode  
Administrator Password

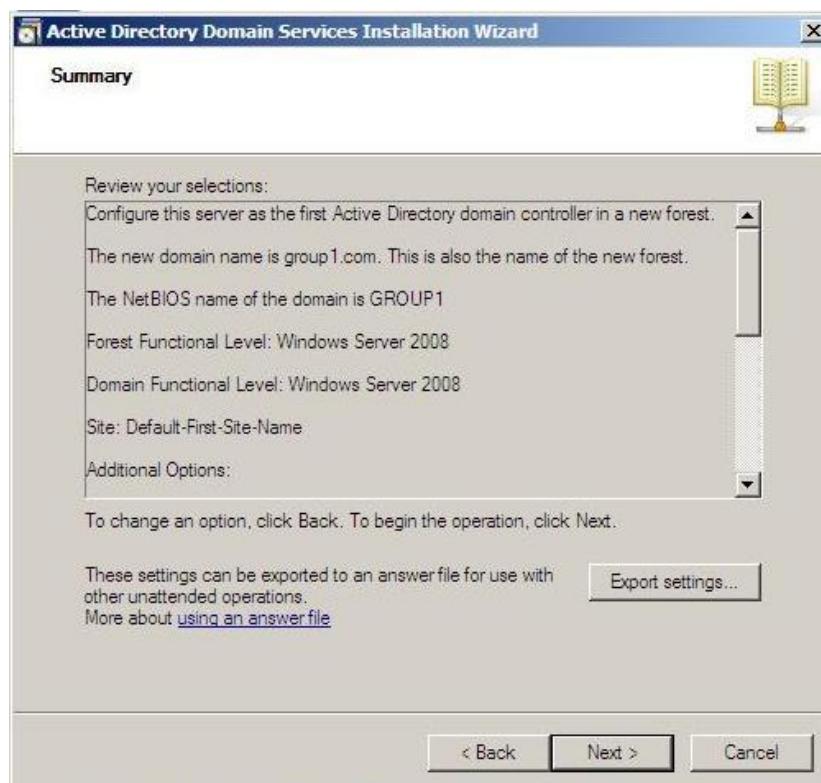


Figure 5. 565: Summary for dcpromo.exe

- f) Reboot the computer on completion of installation.



Figure 5. 566: ADDS Installation Wizard

### Step 2: Configure User in the Active Directory

User accounts are used to authenticate, authorize or deny access to resources for, and audit the activity of individual users on your network. A group account is a collection of user accounts that you can use to assign a set of permissions and rights to multiple users simultaneously. A group can also contain contacts, computers, and other groups. The user created is assigned to the group created.

- a) Go to Start → Administrative Tools → Active Directory Users and Computers to configure

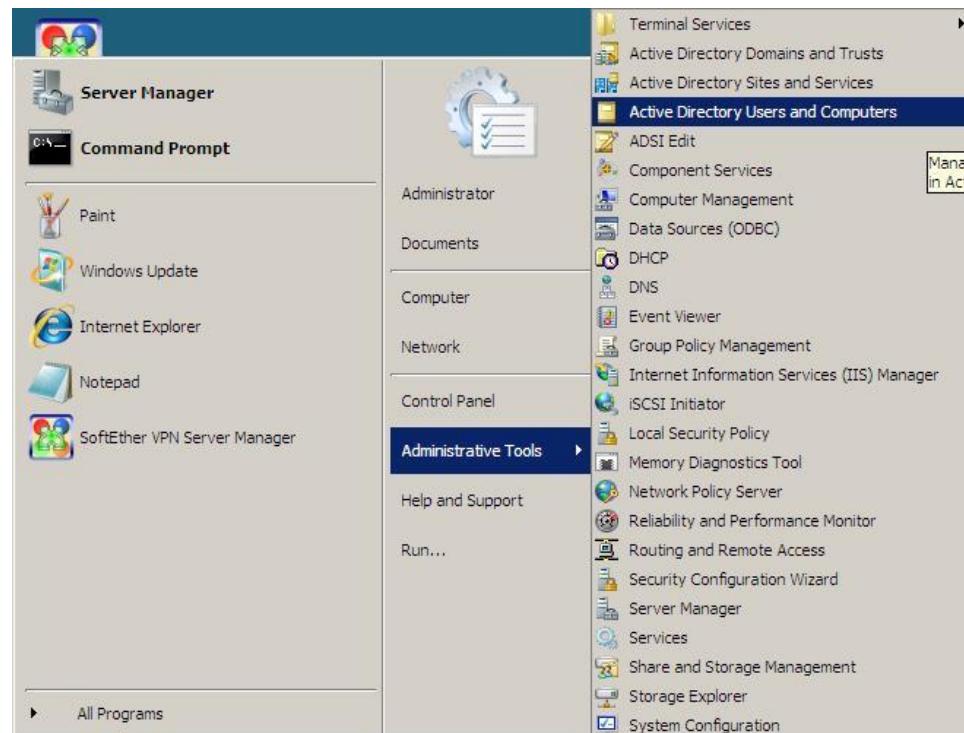


Figure 5. 567: Open Active Directory Users and Computer

- b) On User Organization Unit and Right click on it and select New → User in order to add a new user for Active Directory

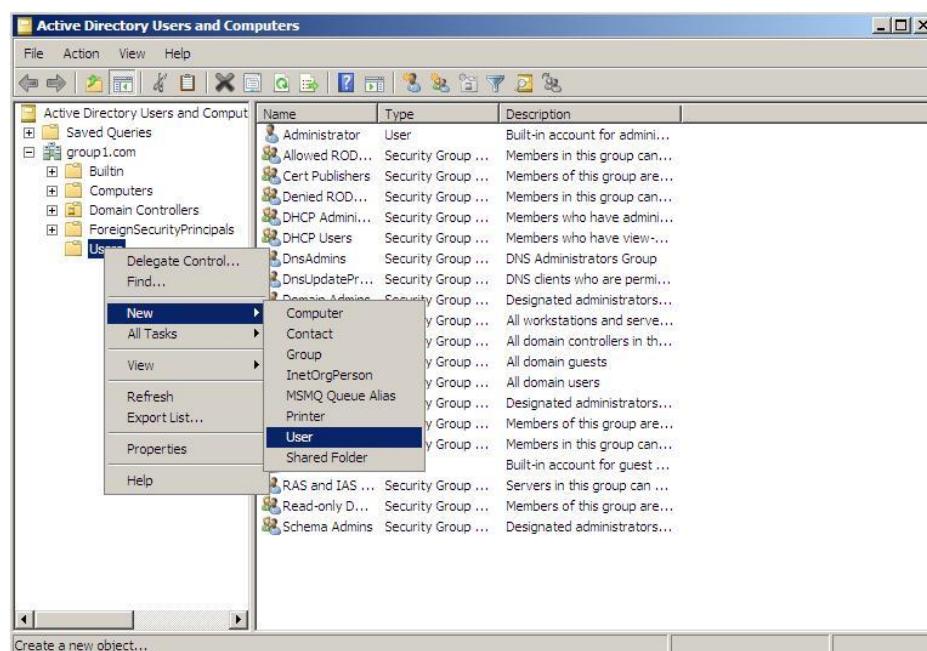


Figure 5. 568: Add new user for AD

- c) Configure the new user by enter the First Name and Full name, and also user login name of the user, click next when done.

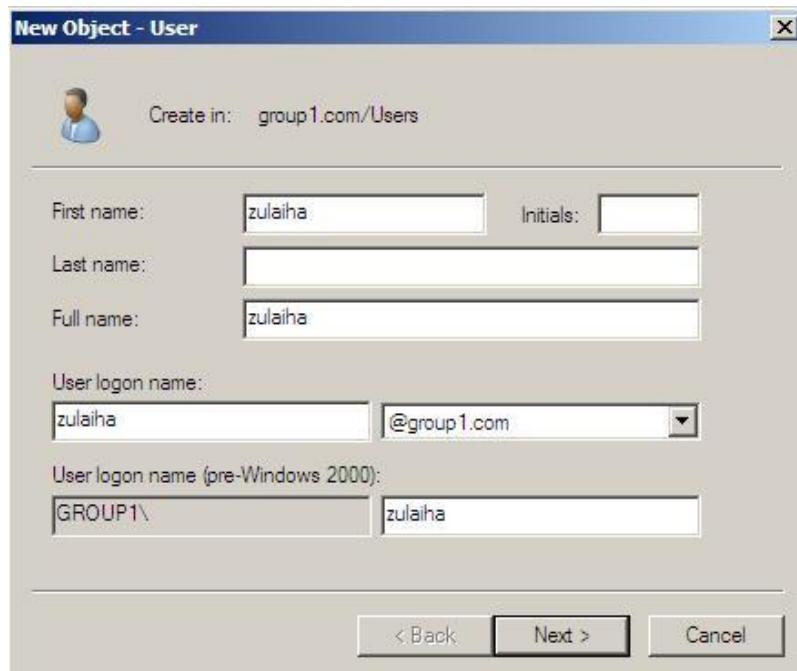


Figure 5. 569: Set the user information with details

- d) Configure the user by enter the password and set the password to never expired option.



Figure 5. 570: Enter the password and tick on the Password never expires option

- e) The user had been successfully created.

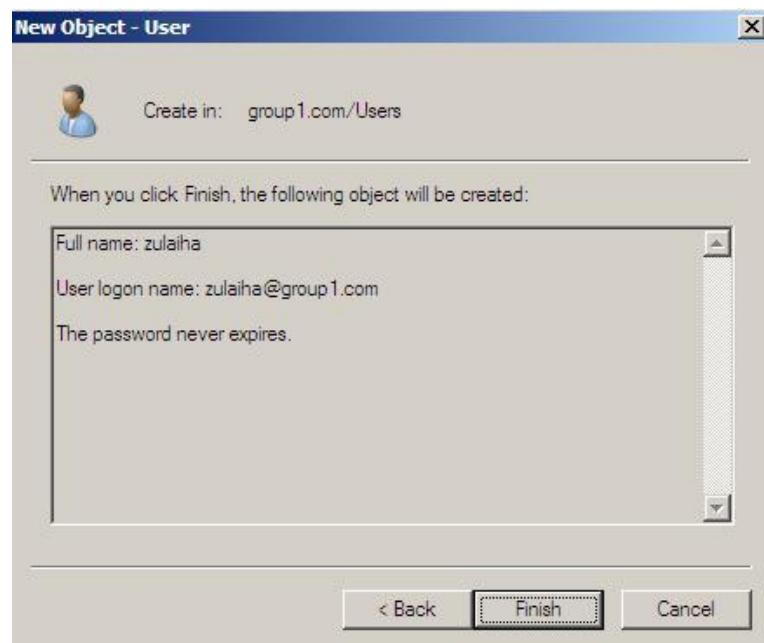


Figure 5. 571: Detail of the user that has been configured.

- f) Repeat the step from b – e in order to add user: tan, fitri, ashraf, chai, aini, ara, and syukor.
- g) Right click on User and select New → Group in order to add a new group for Active Directory

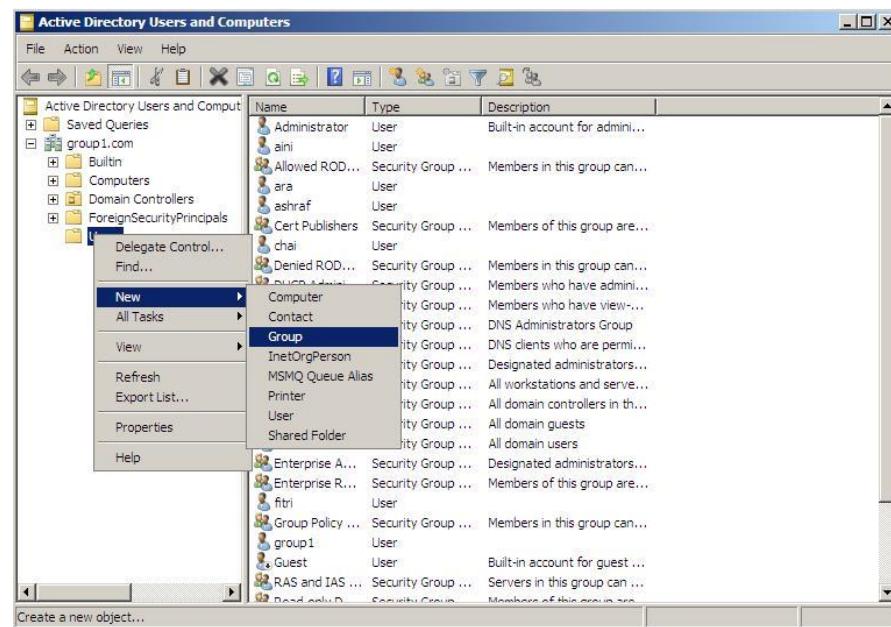


Figure 5. 572: Add new group for AD

- h) Create a new windowsTeam, linux1Team, linux2Team in AD and press OK

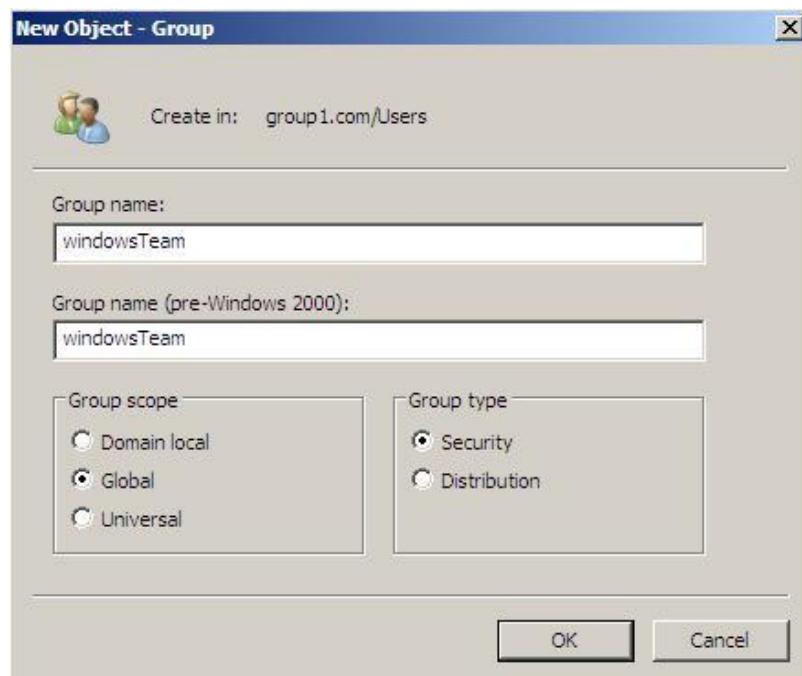


Figure 5. 573: Create windowsTeam

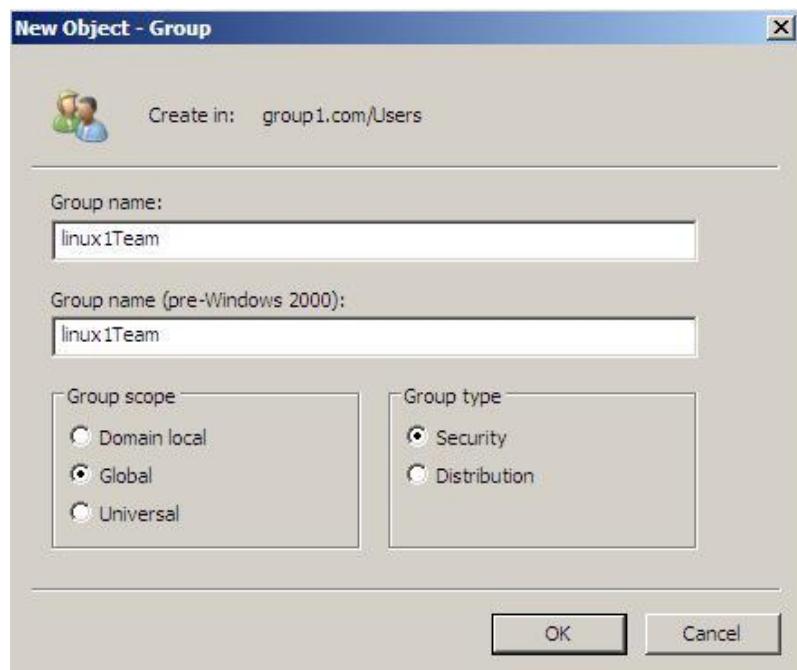


Figure 5. 574: Create linux1Team

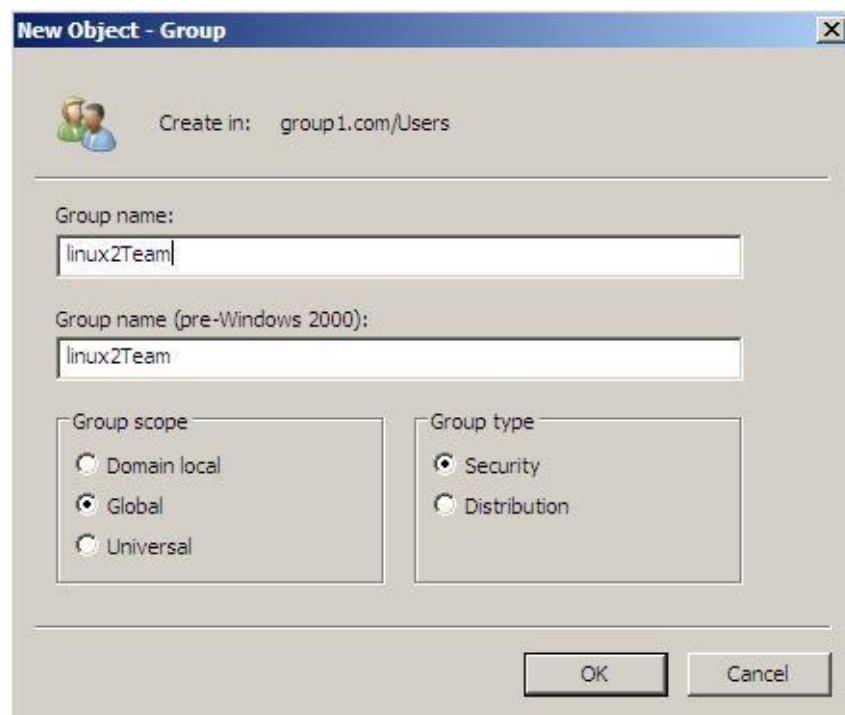


Figure 5. 575: Create linux2Team

- i) Right click at every name that we have created and add to group and put the group that we want to add it.

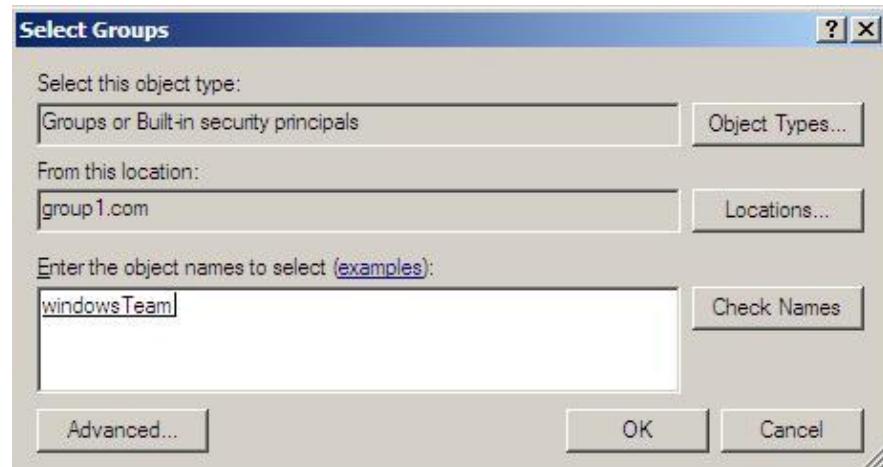


Figure 5. 576: Add some name members in windowsTeam.

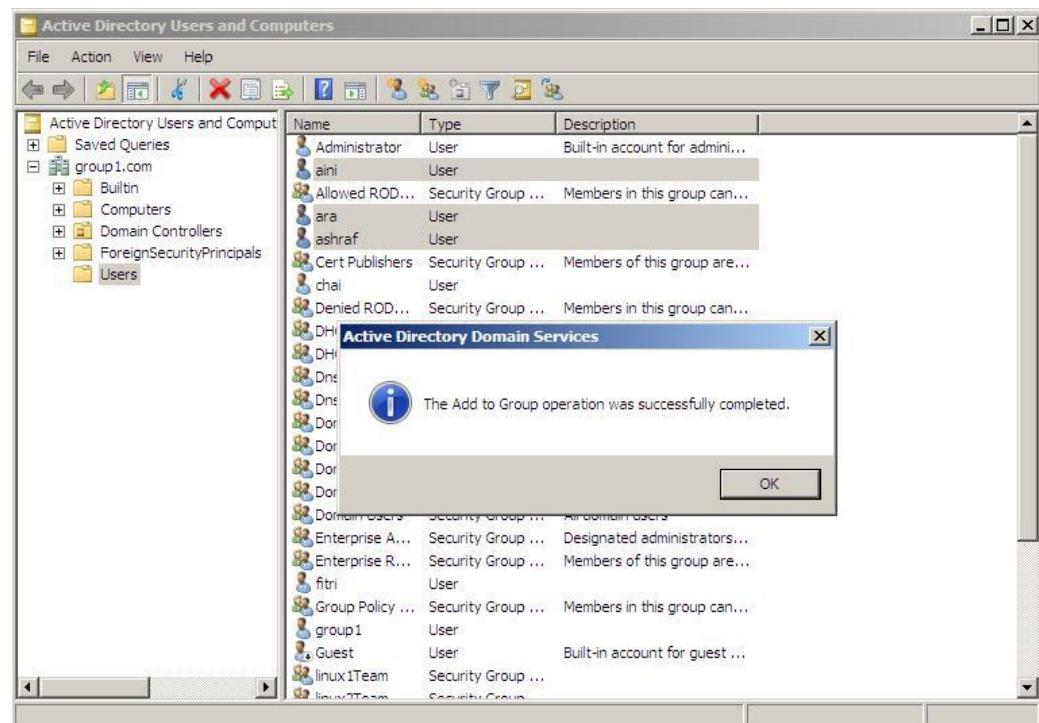


Figure 5. 577: Successfully add members in group

- j) Right click all names member and add to Print Operator group.

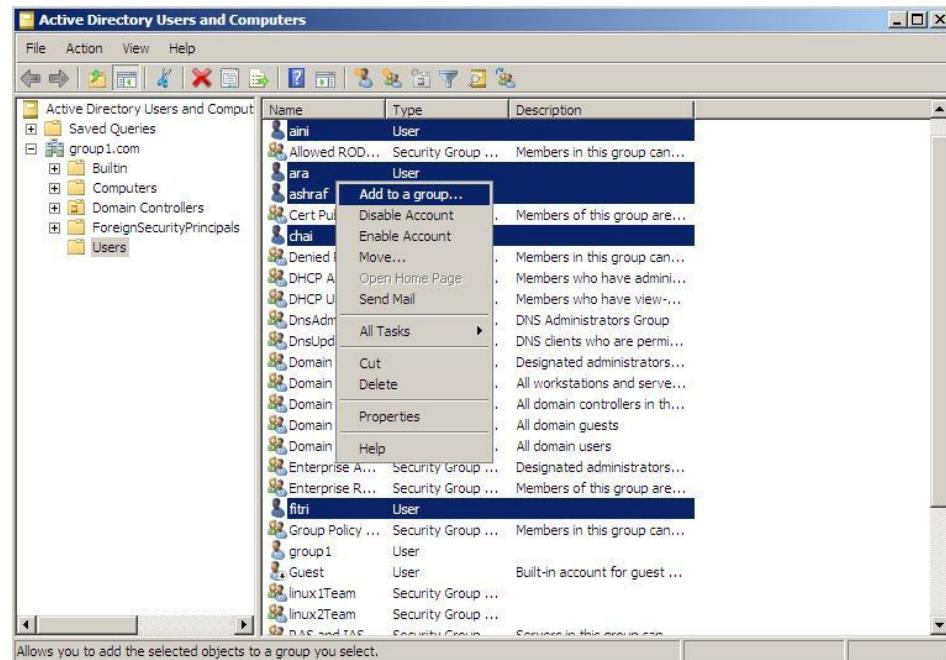


Figure 5. 578: Select all names

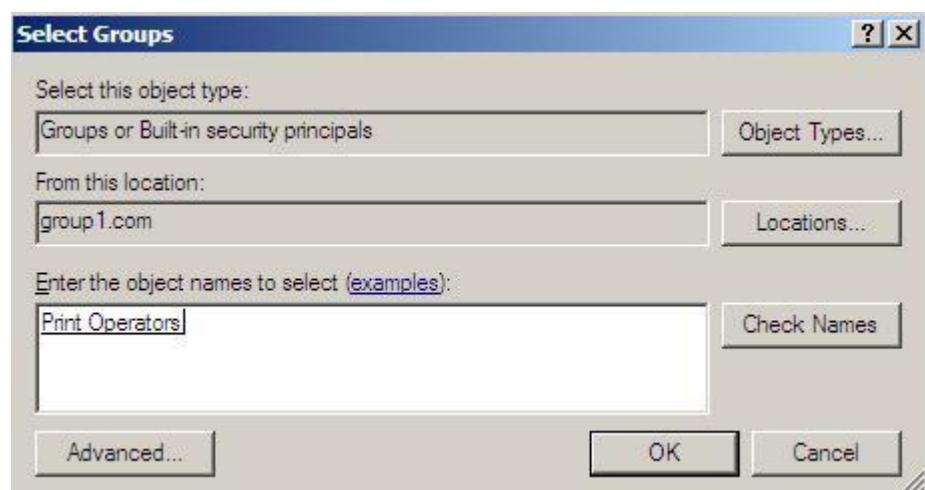


Figure 5. 579: Add in Print Operator group

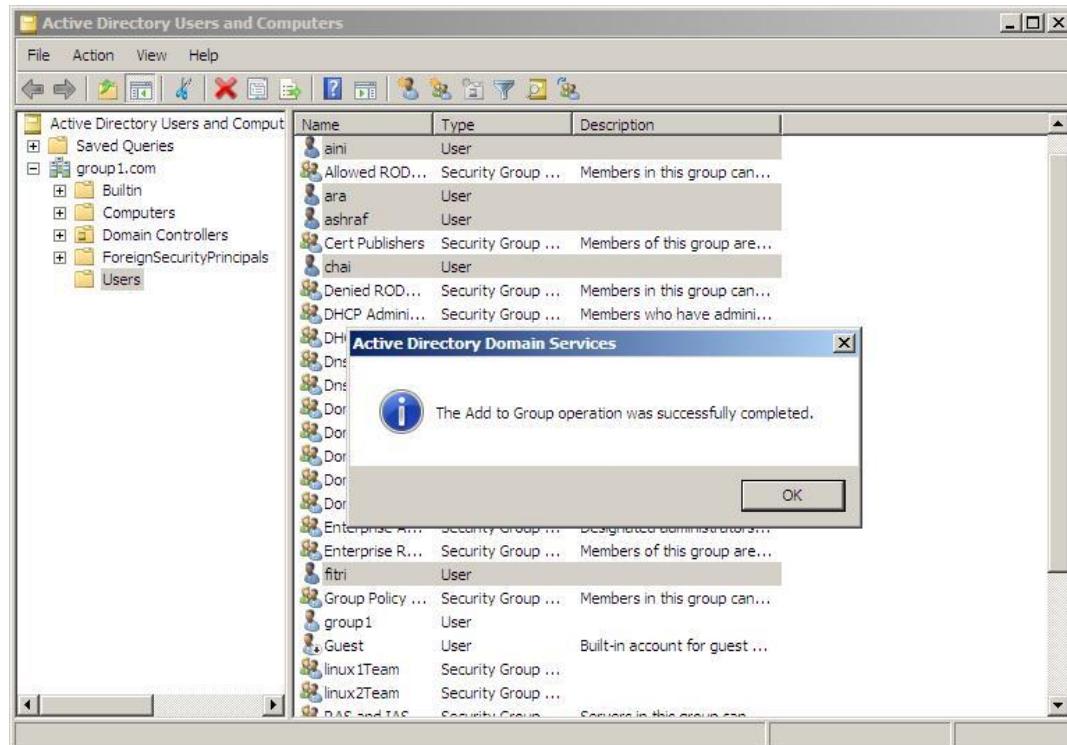


Figure 5. 580: Successfully add in group

### **Problem**

The network places did not show under the computer when successfully connected by using client and can't integrate with Linux Server.

### **Solution**

After created the Active Directory (AD) it make easier to connect with Linux Server, router and switch after create Radius with only use AD in Windows Server.

### **Security Enhancement**

Active Directory provides a flexible, secure authentication and authorization for each user that created inside the operating platform which in our case is the Windows Platform. Flexible and secure authentication and authorization

services provide protection for data while minimizing barriers to doing business over the Internet. Active Directory supports multiple authentication protocols, such as the Kerberos V5 protocol, Secure Sockets Layer (SSL) v3, and Transport Layer Security (TLS) using X.509 v3 certificates, and security groups that span domains efficiently.

(Source: TechNet, Microsoft).

#### **5.4 CONCLUSION**

During the service installation and configuration phase, we have referred to many online tutorials. Yet, we still faced a lot of problems. This is due to the unclear and missing instruction from the tutorials. To solve these problems, we spent a lot of time troubleshooting. Through this process, we found that service configuration is not about clicking “next” buttons. It involves extensive knowledge of computer, operating system and network theory and analytical thinking. We have gained experience and exposure towards service configuration which will help us in future career.

## CHAPTER 6: TESTING

### 6.1 INTRODUCTION

In this chapter, the testing approach and result for each service will be explained. There might be different approach to test the services, but we only focus on one as our goal is to ensure the service is up and correctly configured.

### 6.2 SERVICE TESTING

#### 6.2.1 DOMAIN NAME SERVER (DNS)

To verify the DNS servers are functioning is by using command “nslookup”. Nslookup is a network utility program used to obtain information about Internet servers. The utility finds name server information for domains by queuing DNS (Bradley Mitchell, 2014).

Step 1: Type nslookup. Enter the IP address of the server.



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt - nslookup". The command entered is "nslookup". The output displays various DNS lookups for hosts within the "group1" domain, including "group1", "ubuntu1", "ubuntu2", and "www". It also shows the default server being used and the IP addresses of the hosts.

```
C:\>Administrator: Command Prompt - nslookup
C:\Users\Administrator>nslookup
Default Server: www.group1.ipv6.com
Address: 2001:c0a8:b22::2

> server group1.group1.com
Default Server: group1.group1.com
Addresses: 2001:c0a8:b22::2
          2001:c0a8:b22:0:cdc:5655:b052:5dcd
          192.168.11.34

> 192.168.11.34
Server: group1.group1.com
Addresses: 2001:c0a8:b22::2
          2001:c0a8:b22:0:cdc:5655:b052:5dcd
          192.168.11.34

Name: group1.group1.com
Address: 192.168.11.34

> 192.168.11.42
Server: group1.group1.com
Addresses: 2001:c0a8:b22::2
          2001:c0a8:b22:0:cdc:5655:b052:5dcd
          192.168.11.34

Name: ubuntu1.group1.com
Address: 192.168.11.42

> 192.168.11.51
Server: group1.group1.com
Addresses: 2001:c0a8:b22::2
          2001:c0a8:b22:0:cdc:5655:b052:5dcd
          192.168.11.34

Name: ubuntu2.group1.com
Address: 192.168.11.51

> www.group1.com
Server: group1.group1.com
Addresses: 2001:c0a8:b22::2
          2001:c0a8:b22:0:cdc:5655:b052:5dcd
          192.168.11.34

Name: group1.group1.com
Addresses: 2001:c0a8:b22:0:cdc:5655:b052:5dcd
          2001:c0a8:b22::2
          192.168.11.34
Aliases: www.group1.com

> -
```

Figure 6. 1: Testing on server and client

## 6.2.2 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Step 1: Use command ipconfig to check the DHCP in client's computer.

```

Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . : group1.com
  IPv6 Address . . . . . : 2001:c0a8:b02:0:d58a:b013:9a0e:92ae
  Link-local IPv6 Address . . . . . : fe80::a5b6:185f:b49:727ax11
  IPv4 Address . . . . . : 192.168.11.2
  Subnet Mask . . . . . : 255.255.255.224
  Default Gateway . . . . . : fe80::281:c4ff:fe38:c9a0x11
                                         192.168.11.1

Tunnel adapter isatap.{5DC21EE6-CBCD-41B4-A589-AA30248E9B74}:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : group1.com

Tunnel adapter isatap.group1.com:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : group1.com

C:\Users\Group1>

```

Figure 6. 2: IPv4 and IPv6 Shown in Command Prompt

Step 2: Open DHCP and it will display all the user that get the DHCP IPv4.

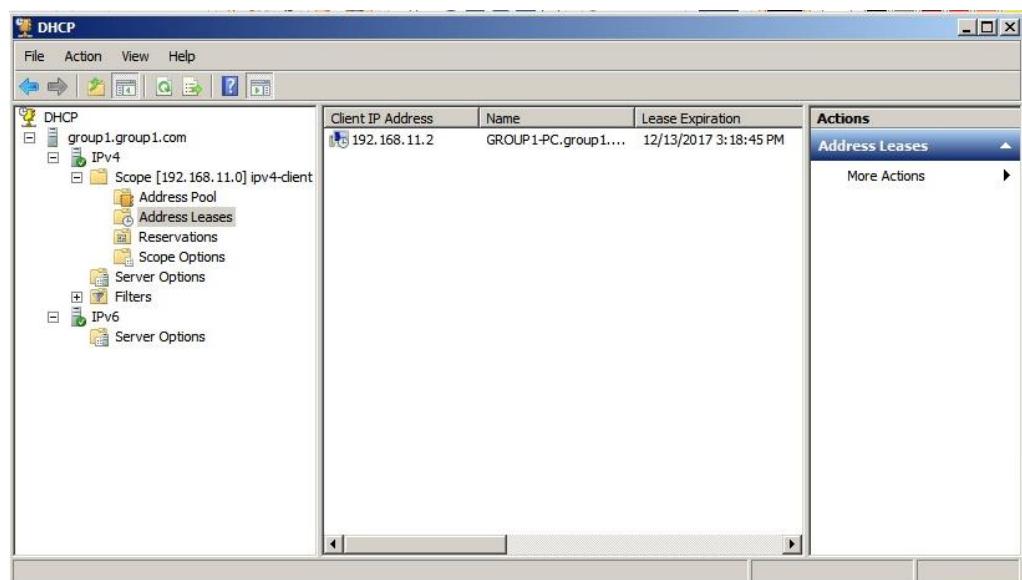


Figure 6. 3: DHCP Information Is Shown at Window Server

### 6.2.3 ROUTING & NETWORK ADDRESS TRANSLATION (NAT)

#### Routing

Enter the router and use “sh ip route” command to see the routing that has been configured.

```

login as: fitri
Using keyboard-interactive authentication.
Password:

#####
#          WELCOME TO GROUP1 WORKSHOP UNAUTHORIZED USER IS PROHIBITED      #
#
#####

*** Ensure that you enter cisco password correctly ***
*** Documentation after making system changes.      ***

R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, 1 - LIS
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      192.168.11.0/24 is variably subnetted, 12 subnets, 4 masks
C        192.168.11.0/27 is directly connected, GigabitEthernet0/0.40
L        192.168.11.1/32 is directly connected, GigabitEthernet0/0.40
C        192.168.11.32/29 is directly connected, GigabitEthernet0/0.10
L        192.168.11.33/32 is directly connected, GigabitEthernet0/0.10
C        192.168.11.40/29 is directly connected, GigabitEthernet0/0.20
L        192.168.11.41/32 is directly connected, GigabitEthernet0/0.20
C        192.168.11.48/29 is directly connected, GigabitEthernet0/0.30
L        192.168.11.49/32 is directly connected, GigabitEthernet0/0.30
C        192.168.11.56/29 is directly connected, GigabitEthernet0/0.50
L        192.168.11.61/32 is directly connected, GigabitEthernet0/0.50

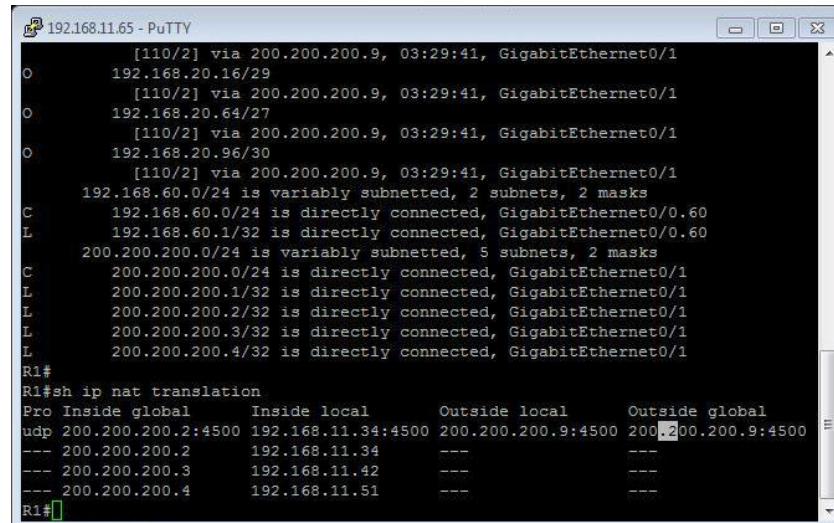
R1#

```

Figure 6. 4: Routing Testing

#### NAT

Inside router enter the command “sh ip nat translation” to see the translation of private IP to public IP and vice-versa.



```

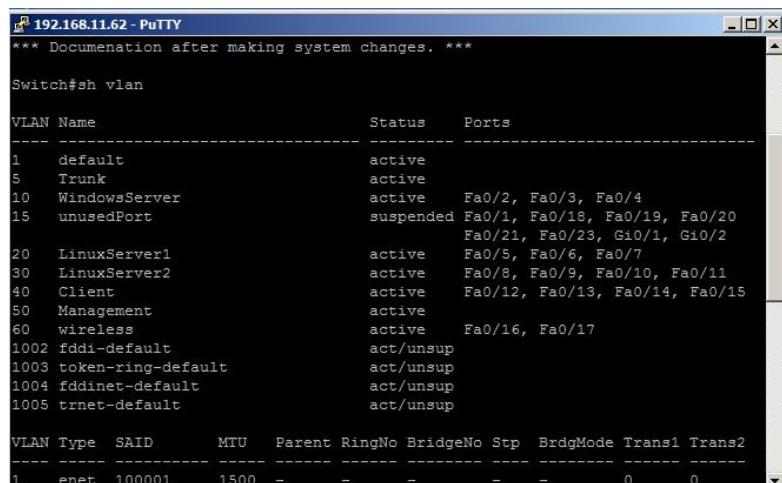
192.168.11.65 - PuTTY
[110/2] via 200.200.200.9, 03:29:41, GigabitEthernet0/1
O 192.168.20.16/29
[110/2] via 200.200.200.9, 03:29:41, GigabitEthernet0/1
O 192.168.20.64/27
[110/2] via 200.200.200.9, 03:29:41, GigabitEthernet0/1
O 192.168.20.96/30
[110/2] via 200.200.200.9, 03:29:41, GigabitEthernet0/1
192.168.60.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.60.0/24 is directly connected, GigabitEthernet0/0.60
L 192.168.60.1/32 is directly connected, GigabitEthernet0/0.60
200.200.200.0/24 is variably subnetted, 5 subnets, 2 masks
C 200.200.200.0/24 is directly connected, GigabitEthernet0/1
L 200.200.200.1/32 is directly connected, GigabitEthernet0/1
L 200.200.200.2/32 is directly connected, GigabitEthernet0/1
L 200.200.200.3/32 is directly connected, GigabitEthernet0/1
L 200.200.200.4/32 is directly connected, GigabitEthernet0/1
R1#
R1#sh ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
udp 200.200.200.2:4500 192.168.11.34:4500 200.200.200.9:4500 200.200.200.9:4500
--- 200.200.200.2      192.168.11.34      ---              ---
--- 200.200.200.3      192.168.11.42      ---              ---
--- 200.200.200.4      192.168.11.51      ---              ---
R1#

```

Figure 6. 5: NAT Testing

#### 6.2.4 VIRTUAL LOCAL AREA NETWORK (VLAN)

Step 1: Insert command sh vlan on switch



```

192.168.11.62 - PuTTY
*** Documentation after making system changes. ***
Switch#sh vlan

VLAN Name          Status    Ports
---- --
1    default        active
5    Trunk          active
10   WindowsServer  active    Fa0/2, Fa0/3, Fa0/4
15   unusedPort     suspended Fa0/1, Fa0/18, Fa0/19, Fa0/20
                           Fa0/21, Fa0/23, Gi0/1, Gi0/2
20   LinuxServer1   active    Fa0/5, Fa0/6, Fa0/7
30   LinuxServer2   active    Fa0/8, Fa0/9, Fa0/10, Fa0/11
40   Client          active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
50   Management     active
60   wireless        active    Fa0/16, Fa0/17
1002 fddi-default  act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default  act/unsup
1005 trnet-default   act/unsup

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- --
1    enet  100001    1500   -      -      -      -      0      0

```

Figure 6. 6: Show VLAN

Step 2: Insert command sh run on router and check on the interfaces configured.

```
interface GigabitEthernet0/0.5
encapsulation dot1Q 5
ip address 192.168.11.65 255.255.255.252
ip nat inside
ip virtual-reassembly in
ipv6 address 2001:COA8:B41::1/64
ipv6 address 2001:COA8:B41::/64 eui-64
ipv6 enable
ipv6 ospf 1 area 1
!
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.11.33 255.255.255.248
ip nat inside
ip virtual-reassembly in
ipv6 address 2001:COA8:B22::1/64
ipv6 address 2001:COA8:B22::/64 eui-64
ipv6 enable
ipv6 ospf 1 area 1
!
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.11.41 255.255.255.248
ip nat inside
ip virtual-reassembly in
ipv6 address 2001:COA8:B2A::1/64
ipv6 address 2001:COA8:B2A::/64 eui-64
ipv6 enable
ipv6 ospf 1 area 1
!
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.11.49 255.255.255.248
ip nat inside
ip virtual-reassembly in
ipv6 address 2001:COA8:B33::1/64
ipv6 address 2001:COA8:B33::/64 eui-64
ipv6 enable
ipv6 ospf 1 area 1
!
```

Figure 6. 7: Show Interface

```
interface GigabitEthernet0/0.40
encapsulation dot1Q 40
ip address 192.168.11.1 255.255.255.224
ip access-group CLIENT in
ip access-group CLIENT out
ip helper-address 192.168.11.34
ip nat inside
ip virtual-reassembly in
ipv6 address 2001:COA8:B02::1/64
ipv6 address 2001:COA8:B02::/64 eui-64
ipv6 enable
ipv6 nd prefix 2001:COA8:B02::/64 14400 14400 no-autoconfig
ipv6 nd managed-config-flag
ipv6 dhcp server DHCPV6
ipv6 ospf 1 area 1
!
interface GigabitEthernet0/0.50
encapsulation dot1Q 50
ip address 192.168.11.61 255.255.255.248
ip nat inside
ip virtual-reassembly in
!
interface GigabitEthernet0/0.60
encapsulation dot1Q 60
ip address 192.168.60.1 255.255.255.0
!
interface GigabitEthernet0/0.400
!
interface GigabitEthernet0/1
ip address 200.200.200.1 255.255.255.0
ip access-group 100 in
ip nat outside
ip virtual-reassembly in
duplex auto
speed auto
!
```

Figure 6. 8: Show Interfaces

### 6.2.5 IPV6 TRANSITION MECHANISM

Step 1: Browse IPv6 web of **GROUP 2** by using IPv6 address.

Step 2: Browse **[2001:c0a8:140a::2]** (IPv6 website's address of GROUP 2).

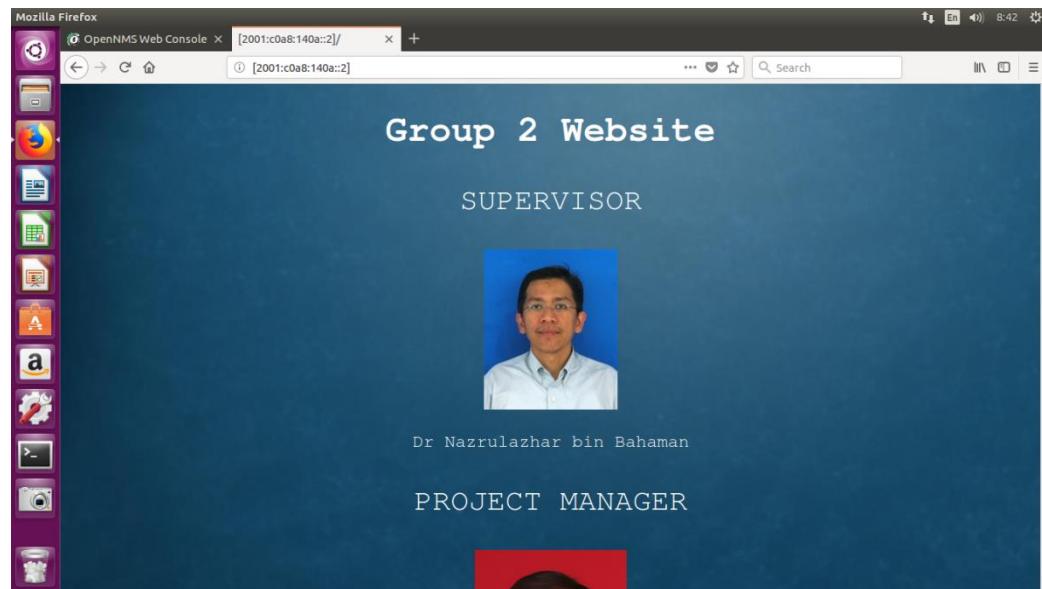


Figure 6. 9: IPv6 web of group2

## 6.2.6 WEB, SECURE SOCKETS LAYER (SSL) & VIRTUAL HOSITNG

### IPv4 Web

Open Web browser > enter [www.group1.com](http://www.group1.com)



Figure 6. 10: [www.group1.com](http://www.group1.com)

### SSL (Secure Sockets Layer)

Open Web browser -> type <https://www.group1.com>



Figure 6. 11: <https://www.group1.com>

## IPv6

Open Web browser -> type <https://www.group1ipv6.com>



Figure 6. 12: [www.group1ipv6.com](https://www.group1ipv6.com)

Open Web browser -> type [www.virtual.group1.com](http://www.virtual.group1.com)



Figure 6. 13: [www.virtual.group1.com](http://www.virtual.group1.com)

### 6.2.7 IPV6 WEB

Step1: Open IE then type <http://www.group1ipv6.com> then the website will appear.



Figure 6. 14: Testing ipv6 web using domain

Step2: Browse using ipv6 address



Figure 6. 15: Testing ipv6 web using ip address

Step3: Browse ipv6 web domain at linux server



Figure 6. 16: Testing ipv6 web domain at linux server

Step4: Browse ipv6 web IP address at linux server



Figure4: Testing ipv6 web ip address at linux server

### **6.2.8 SECURE FILE TRANSFER PROTOCOL (SFTP)**

1. Testing using command prompt in client computer.
  - i. Enter FTP (IP address of ftp server) in the command prompt. Enter the user name and the password. Then make the www to become the directory. Try to get the “test.txt” that was created in the directory.

```

C:\ Command Prompt - ftp 192.168.11.51
Microsoft Windows [Version 6.1.7600]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\Group1>ftp 192.168.11.51
Connected to 192.168.11.51.
220 <vsFTPd 3.0.3>
User <192.168.11.51:<none>>: ftpuser
331 Please specify the password.
Password:
230 Login successful.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
examples.desktop
www
226 Directory send OK.
ftp: 23 bytes received in 0.00Seconds 23000.00Kbytes/sec.
ftp> cd www
250 Directory successfully changed.
ftp> get test.txt
200 PORT command successful. Consider using PASV.
150 Opening ASCII mode data connection for test.txt (6 bytes).
226 Transfer complete.
ftp: 8 bytes received in 0.00Seconds 8000.00Kbytes/sec.
ftp>

```

Figure 6. 17: Connecting to server compute

- ii. Put the “test.txt” into “upload.txt” to the server computer.

```

C:\ Command Prompt - ftp 192.168.11.51
220 <vsFTPd 3.0.3>
User <192.168.11.51:<none>>: ftpuser
331 Please specify the password.
Password:
230 Login successful.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
examples.desktop
www
226 Directory send OK.
ftp: 23 bytes received in 0.00Seconds 23000.00Kbytes/sec.
ftp> cd www
250 Directory successfully changed.
ftp> get test.txt
200 PORT command successful. Consider using PASV.
150 Opening ASCII mode data connection for test.txt (6 bytes).
226 Transfer complete.
ftp: 8 bytes received in 0.00Seconds 8000.00Kbytes/sec.
ftp> put test.txt upload.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp: 8 bytes sent in 0.00Seconds 8000.00Kbytes/sec.
ftp>

```

Figure 6. 18: Transferring file to the server

2. Testing using FileZilla.

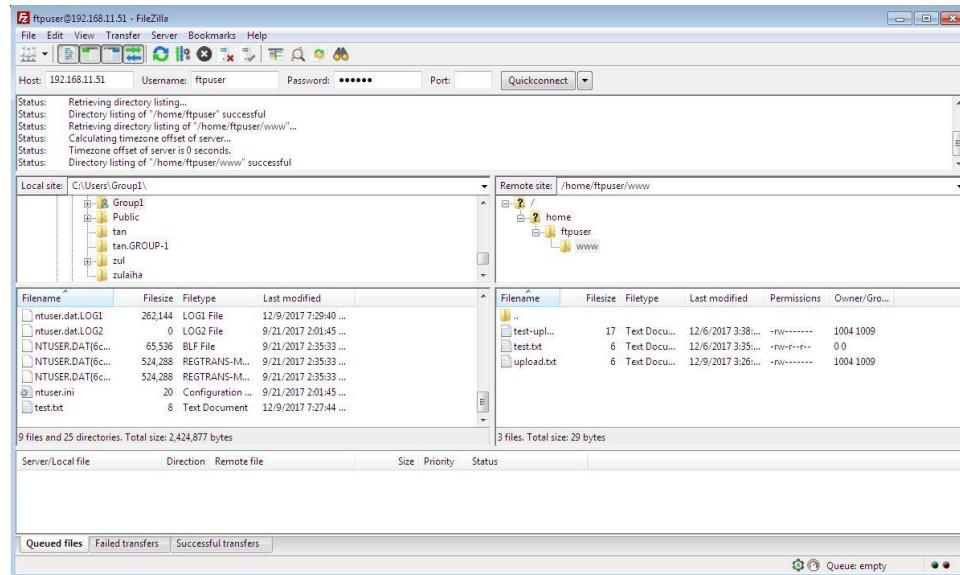


Figure 6. 19: Using FileZilla to test sftp

### 3. Testing using browser.

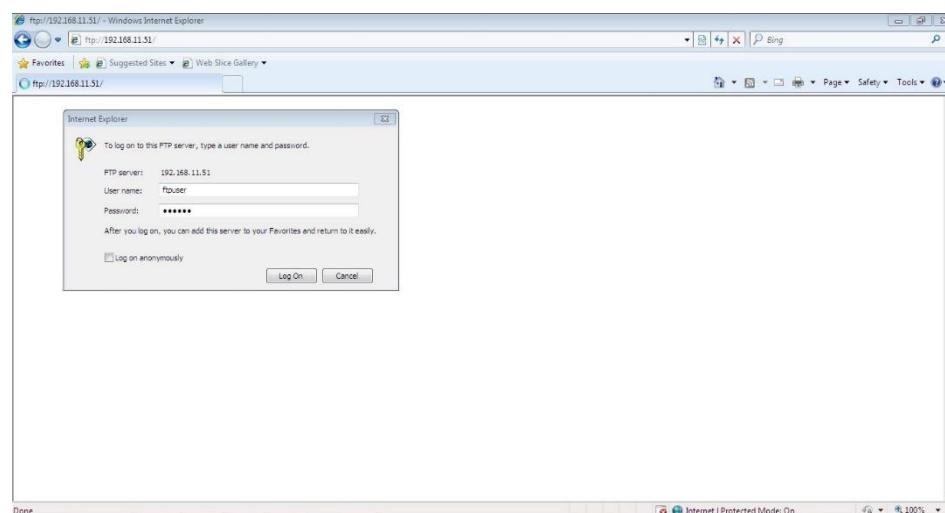


Figure 6. 20: Command asking password

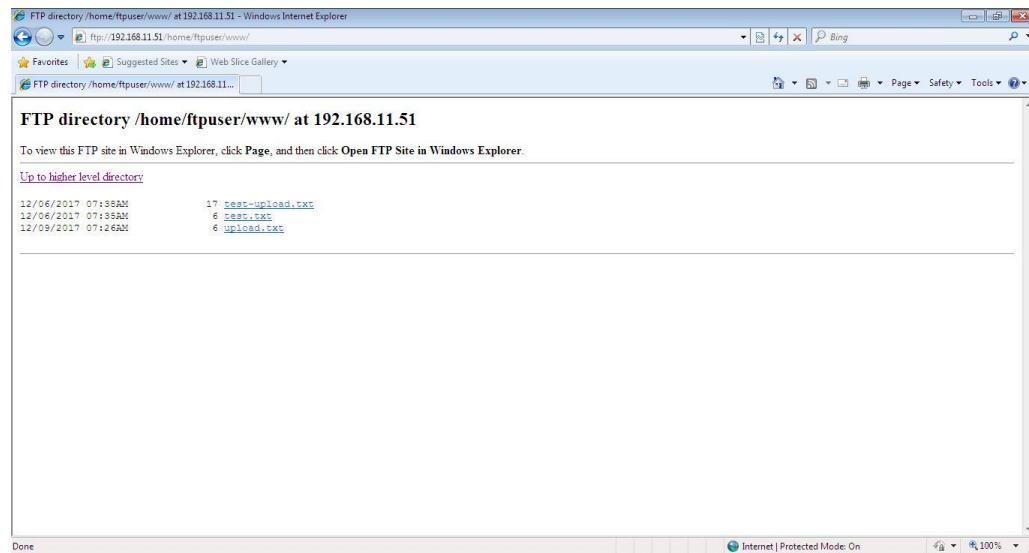


Figure 6. 21: Using browser to test sftp

### 6.2.9 SAMBA

Step 1: Run \\192.168.13.42 on windows client server and click OK.

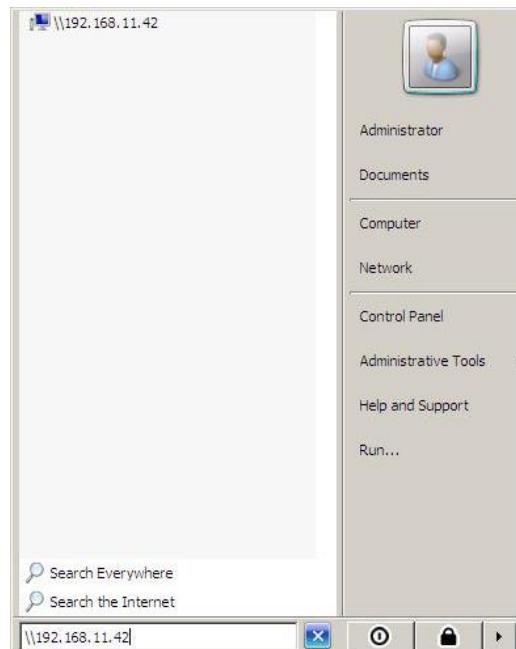


Figure 6. 22: Run \\192.168.11.42

Step 2: The files is successfully shared

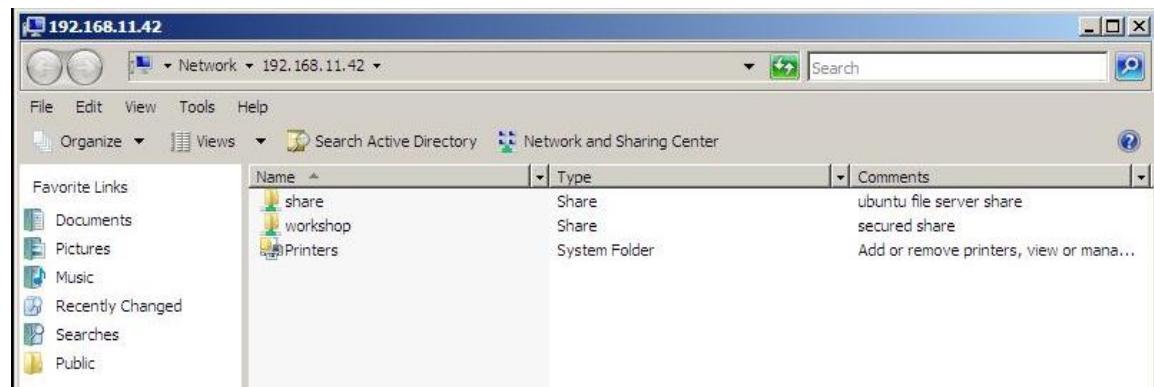


Figure 6. 23: Access to 192.168.11.42

Step 3: Click on the share folder

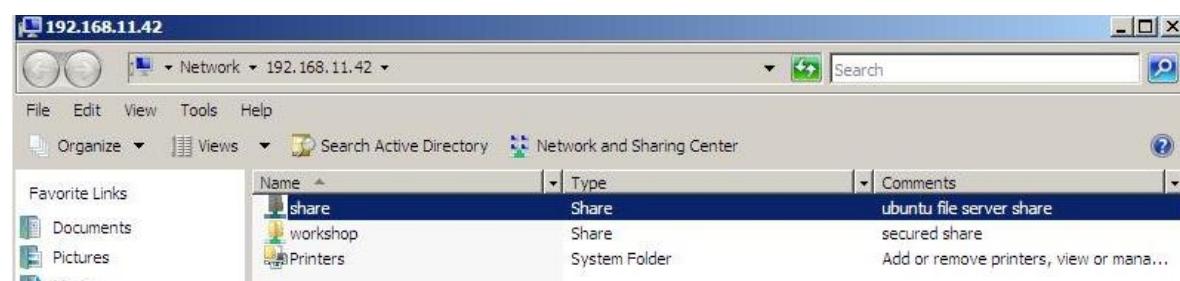


Figure 6. 24: Shared file

Step 4: View the shared file

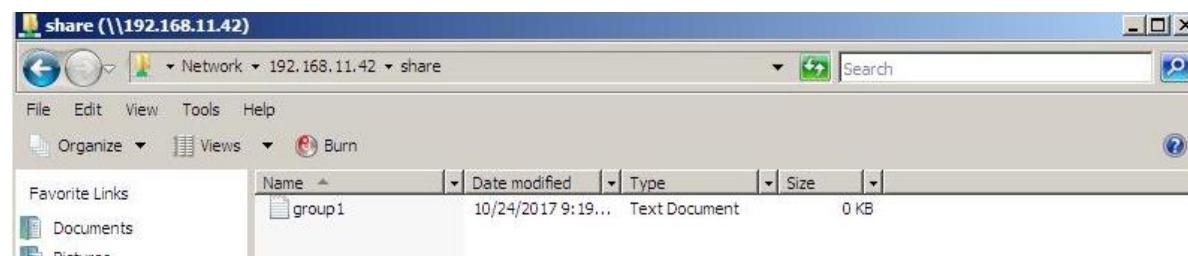


Figure 6. 25: View shared file

### 6.2.10 PROXY SERVER

Step 1: Open Your Web Browser

Step 2: Search blocked website which is Yahoo.com and Ask.com

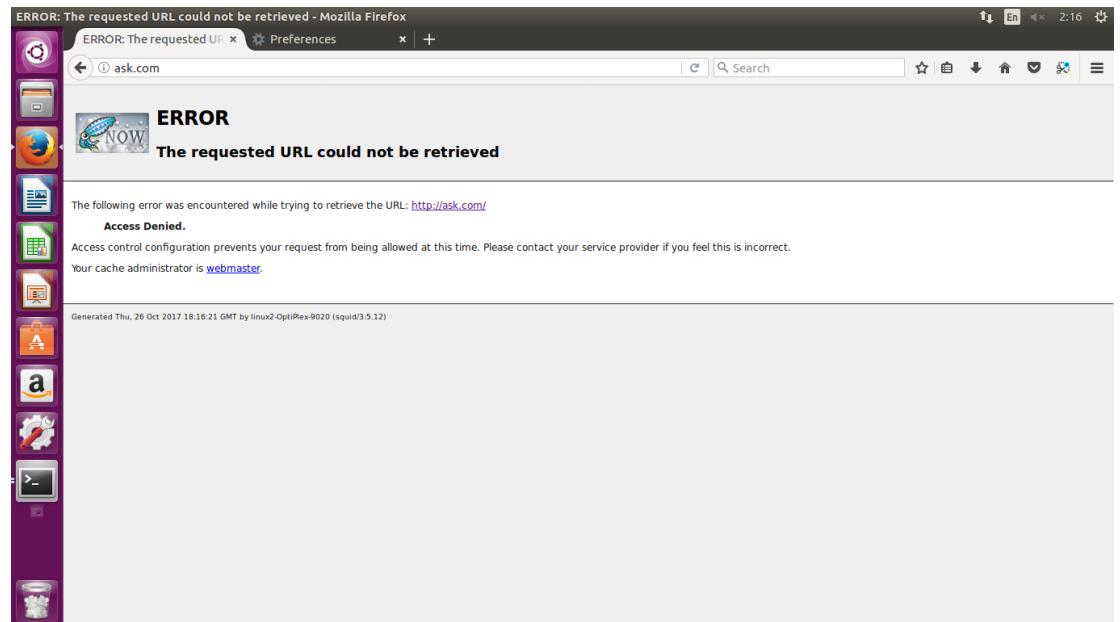


Figure 6. 26: Error message when search “Ask.com”

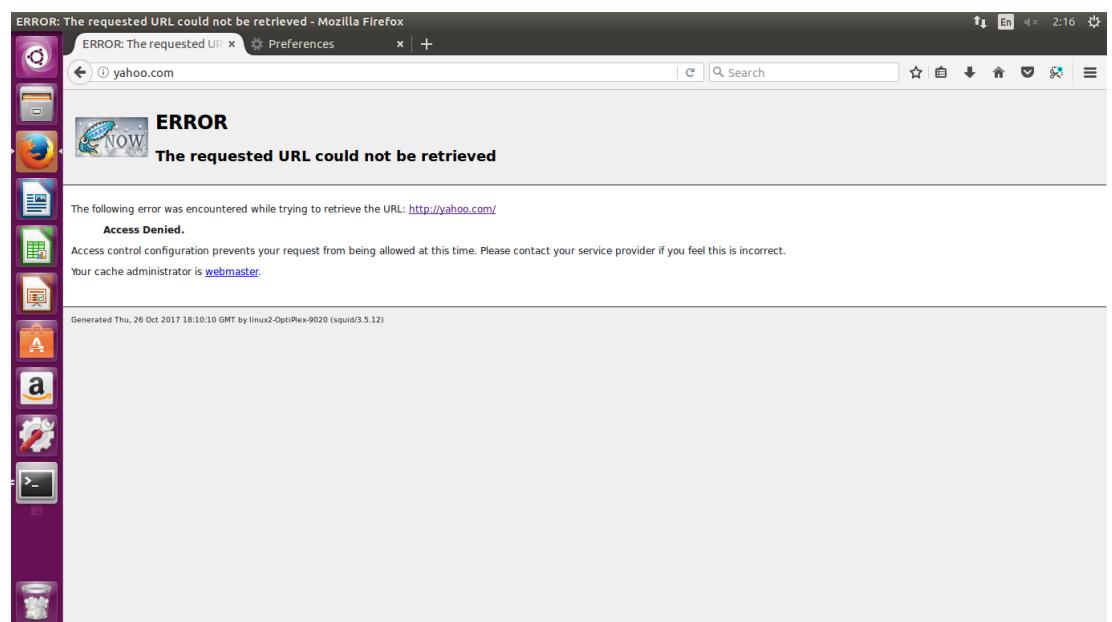


Figure 6. 27: Error message when search “Yahoo.com”

### 6.2.11 RADIUS SERVER FOR NETWORK ACCOUNTING

Try to login router with AD username

```
192.168.11.65 - PuTTY
login as: syukor
Using keyboard-interactive authentication.
Password:

#####
#      WELCOME TO GROUP1 WORKSHOP UNAUTHORIZED USER IS PROHIBITED
#
#####

*** Ensure that you enter cisco password correctly ***
*** Documentation after making system changes.      ***

R1#en
R1#
```

Figure 6. 28: Login with AD

In Accounting panel, navigate to the Log File location.

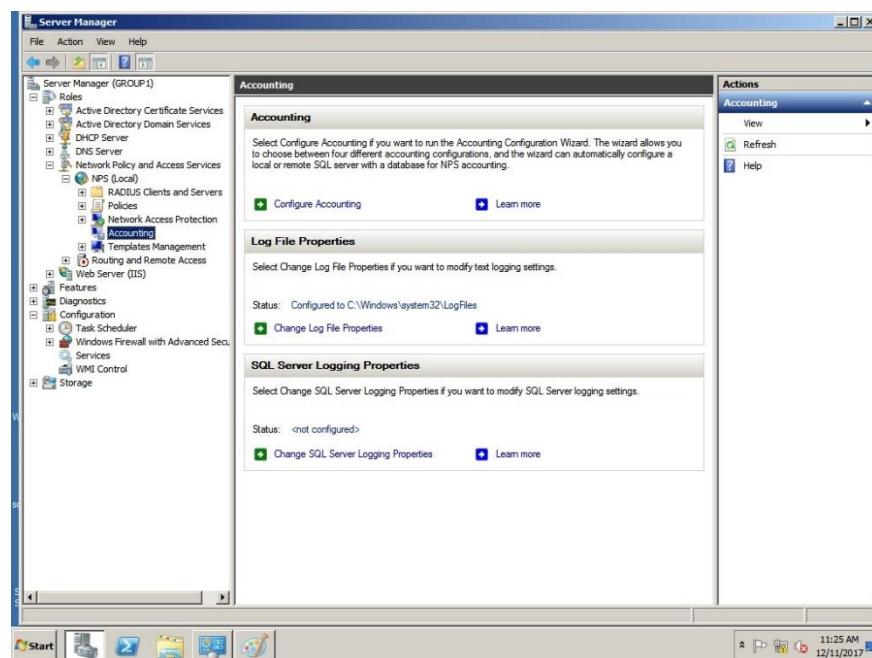


Figure 6. 29: Check for the log file location

Double click on the INI.txt to view the log information.

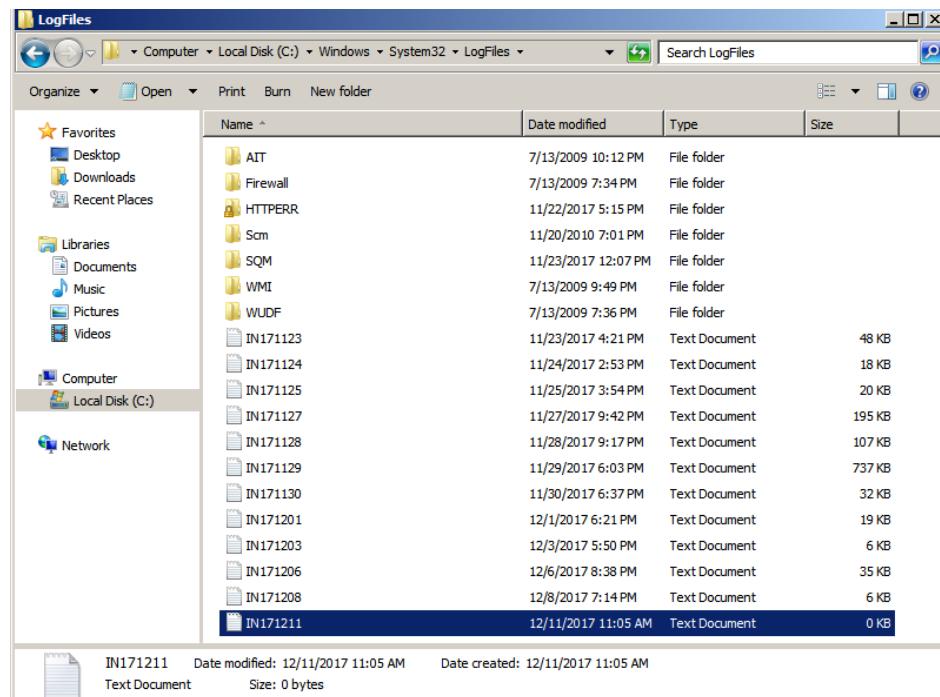


Figure 6. 30: Log file location

```

<Event-Source data_type="1">IAS</Event-Source><User-Name data_type="1">candy4</User-Name>
<MS-Quarantine-State data_type="0">0</MS-Quarantine-State><Fully-Qualified-User-Name data_type="1">group1
<Event-Source data_type="1">IAS</Event-Source><Class data_type="1">311_1_192.168.11.34
<Quarantine-Update-Non-Compliant><Service-Type data_type="0">1</Service-Type><MS-Link-utiliza

```

Figure 6. 31: Details of log file

### 6.2.12 LINUX EMAIL SERVER

Step1: Open SquirrelMail homepage and login using name and password that has been set.

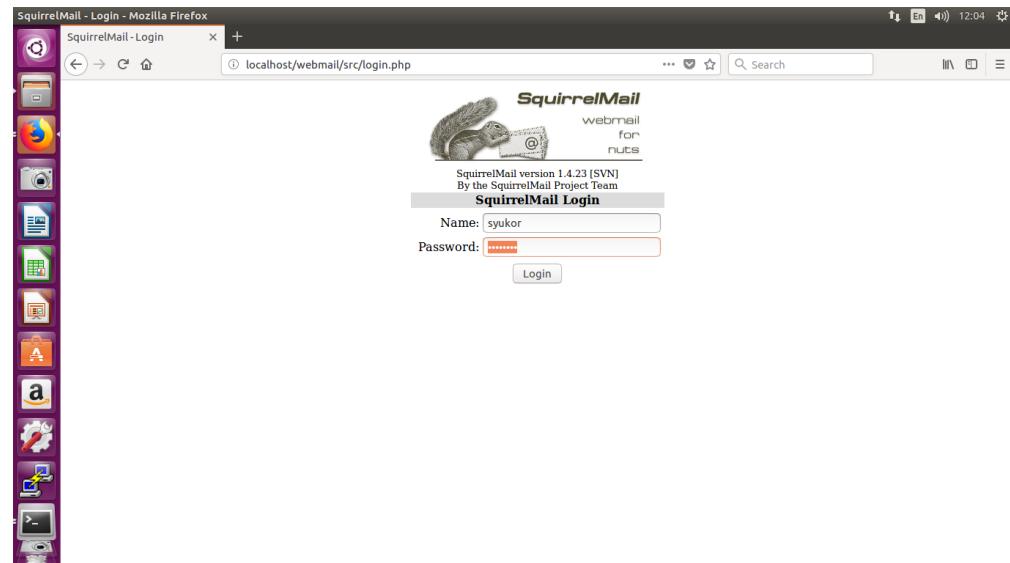


Figure 6. 32: Login to SquirrelMail

Step2: Username Syukor try to send email to username Faizal

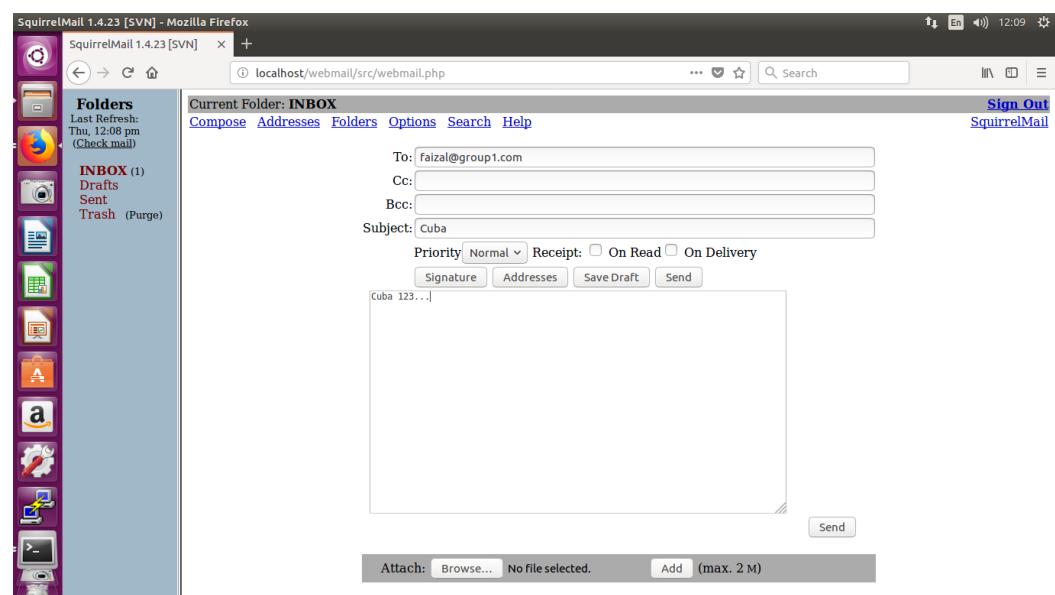


Figure 6. 33: Sending email using SquirrelMail

Step3: The message is delivered to username Faizal

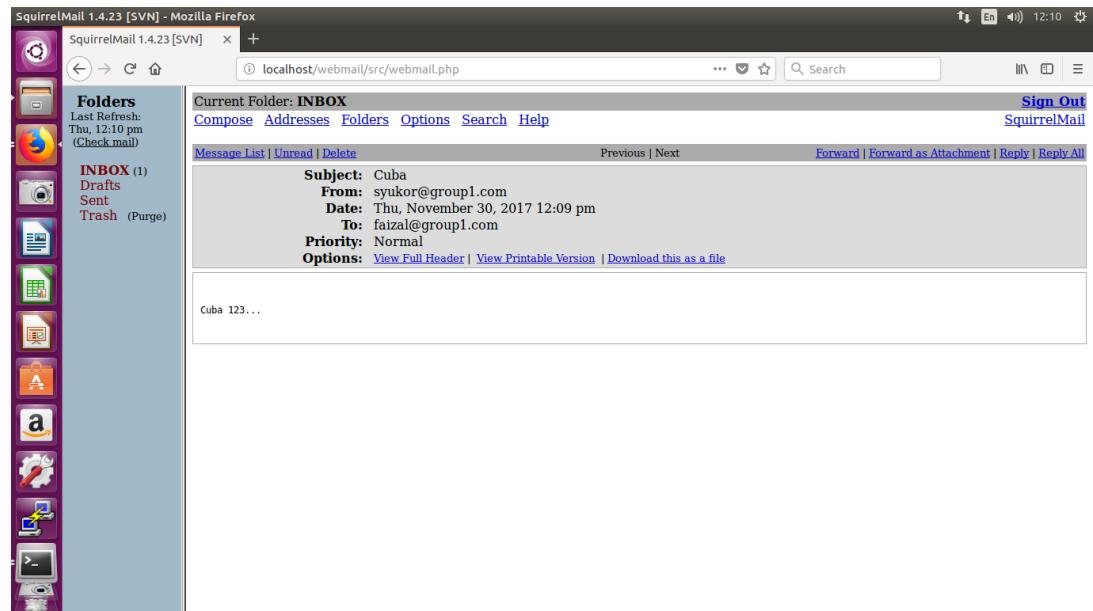


Figure 6. 34: Delivered message

Step4: Replied email to username Syukor

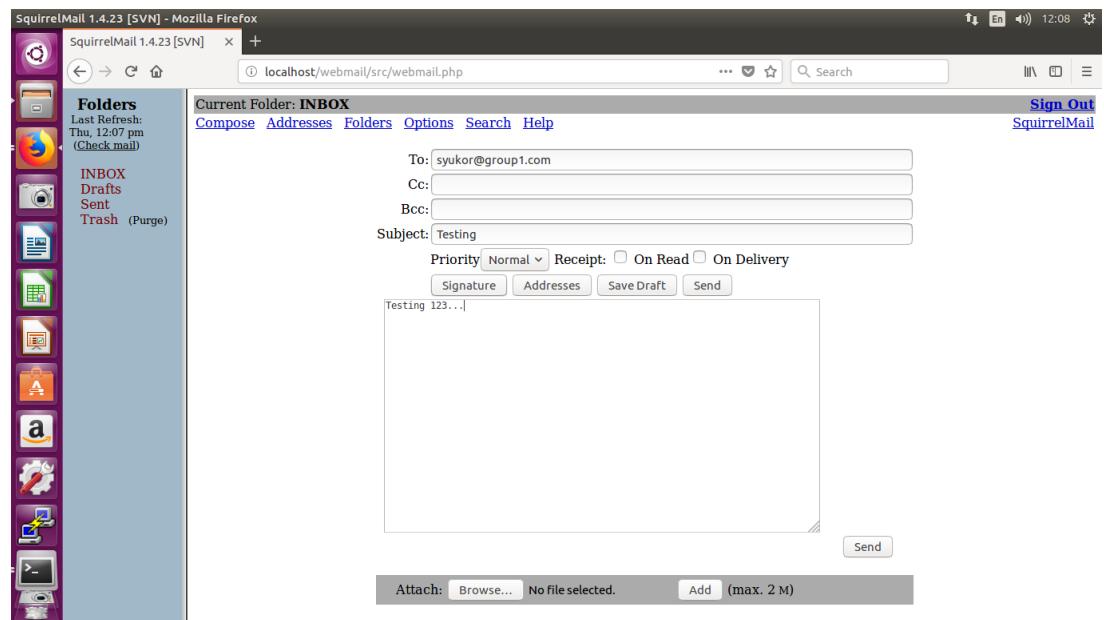


Figure 6. 35: Replied email

Step5: The message is delivered to username Syukor

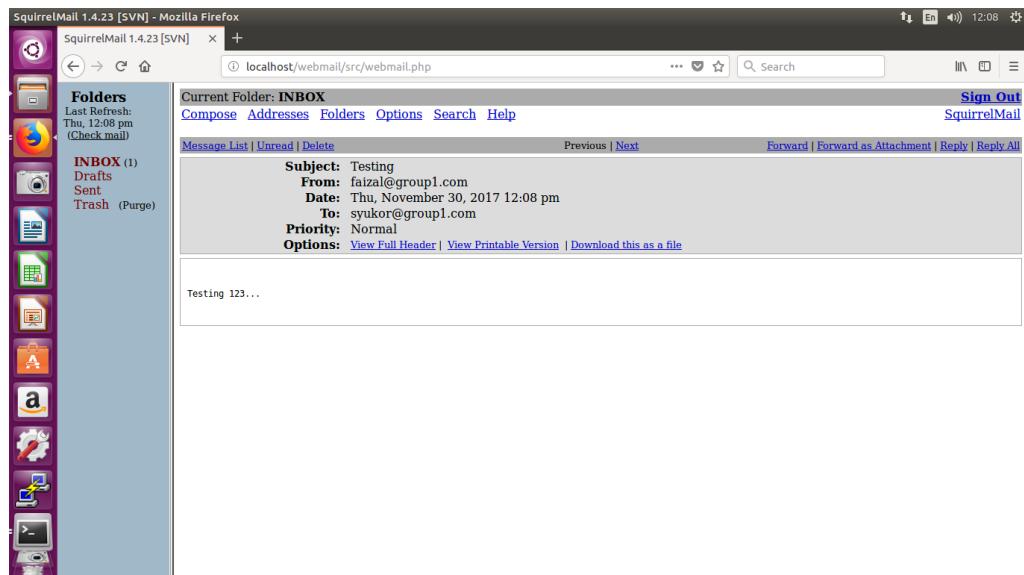


Figure 6. 36: Delivered message

### **6.2.13 NETWORK MANAGEMENT SYSTEM**

Step 1: No problem were found.

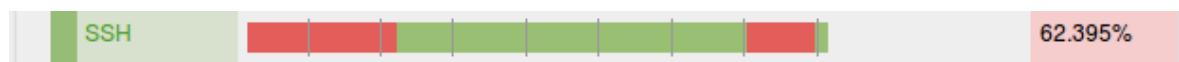


Figure 6. 37: Shows SSH services

Step 2: Stop services in Linux 1 (192.168.11.42) by using this command,  
`service sshd stop`

Step 3: New alarm appear in the nms web to notify admin about the problem occurred

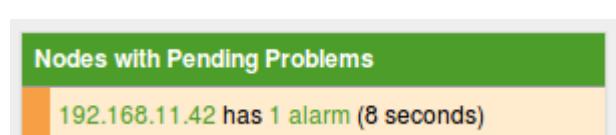


Figure 6.38: Alarm appeared

Step 4: SSH services problem appeared.

Ack	ID	Severity	Node	Count	Last	Log Msg
<input type="checkbox"/>	197	Minor	192.168.11.42	1	Nov 28, 2017 5:32:59 AM	SSH outage identified on interface 192.168.11.42.

Figure 6. 39: Alert about the problem

#### 6.2.14 ACCESS CONTROL LIST (ACL)

1. We have denied the http website to login to (server name). Now we can try from other group to test whether can login http website or not.



This page can't be displayed

- Make sure the web address is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

[Fix connection problems](#)



Figure 6. 40: Testing ACL using port 80

2. We do not deny the https website to login to (server name). When we are testing from other groups, we can login to the https website.



Figure 6. 41: Testing ACL using port 443

3. We also denied other group servers from pinging to our network.

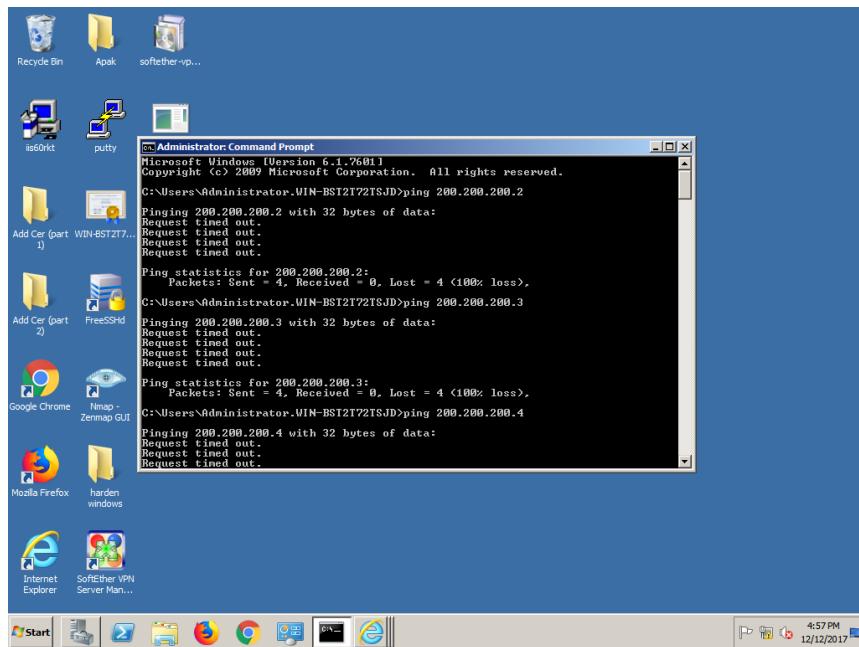


Figure 6. 42: Testing ACL by ping

### 6.2.15 SECURITY HARDENING

Create banner on Switch:

```
User Access Verification

Username: admin
Password:
Switch>ena
Password:
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#banner exec ^c
Enter TEXT message. End with the character '^'.
^c
Switch(config)#banner login ^c
Enter TEXT message. End with the character '^'.
#####
#
# THIS SYSTEM IS PROVIDED FOR THE USE BY AUTHORIZED USER ONLY. THANK YOU! #
#
#####
^c
Switch(config)#exit
Switch#exit
```

Figure 6. 43: Login banner

Create banner on Router:

```
banner exec ^C
*** Ensure that you enter cisco password correctly ***
*** Documentation after making system changes. ***
^C
banner motd ^C
#####
#
#      WELCOME TO GROUP1 WORKSHOP UNAUTHORIZED USER IS PROHIBITED
#
#####

^C
```

Figure 6. 44: Login banner

Disable IP finger service:

```
User Access Verification

Username: admin
Password:
Switch>ena
Password:
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#banner exec ^c
Enter TEXT message. End with the character '^'.
^c
Switch(config)#banner login ^c
Enter TEXT message. End with the character '^'.
#####
#
# THIS SYSTEM IS PROVIDED FOR THE USE BY AUTHORIZED USER ONLY. THANK YOU!
#
#####
^c
Switch(config)#exit
Switch#exit
```

Figure 6. 45: Disable IP finger

Password encryption:

```
Building configuration...

[OK]
R1#
R1#
R1#
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#service password-encryption
R1(config)#exit
R1#co
*Nov 14 07:42:03.804: %SYS-5-CONFIG_I: Configured from console by group1 on con
ole
R1#copy run start
Destination filename [startup-config]?
Building configuration...

[OK]
R1#
```

Figure 6. 46: Password encryption

Password minimal length:

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#security passwords min-length 10
R1(config)#[
```

Figure 6. 47: Password min length

Login failure:

```
R1(config)#
R1(config)#security authentication failure rate 3 log
R1(config)#exit
R1#
*Nov 16 04:30:42.619: %SYS-5-CONFIG_I: Configured from console by group1 on console
R1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R1#[
```

Figure 6. 48: Failure rate enable by the devices

Disable unused port on switch:

```
Switch(config)#interface range fa0/13-23
Switch(config-if-range)#shutdown
Switch(config-if-range)#exit
Switch(config)#
*Mar 6 07:37:45.152: %LINK-5-CHANGED: Interface FastEthernet0/13, changed state
to administratively down
*Mar 6 07:37:45.161: %LINK-5-CHANGED: Interface FastEthernet0/14, changed state
to administratively down
*Mar 6 07:37:45.161: %LINK-5-CHANGED: Interface FastEthernet0/15, changed state
to administratively down
*Mar 6 07:37:45.161: %LINK-5-CHANGED: Interface FastEthernet0/16, changed state
to administratively down
*Mar 6 07:37:45.161: %LINK-5-CHANGED: Interface FastEthernet0/17, changed state

Switch(config)#to administratively down
*Mar 6 07:37:45.169: %LINK-5-CHANGED: Interface FastEthernet0/18, changed state
to administratively down
*Mar 6 07:37:45.169: %LINK-5-CHANGED: Interface FastEthernet0/19, changed state
to administratively down
*Mar 6 07:37:45.169: %LINK-5-CHANGED: Interface FastEthernet0/20, changed state
to administratively down
*Mar 6 07:37:45.169: %LINK-5-CHANGED: Interface FastEthernet0/21, changed state
to administratively down
*Mar 6 07:37:45.169: %LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
*Mar 6 07:37:45.178: %LINK-5-CHANGED: Interface FastEthernet0/23, changed state
to administratively down
*Mar 6 07:37:46.176: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/22, changed state to down
Switch(config)#exit
Switch#co
*Mar 6 07:37:52.065: %SYS-5-CONFIG_I: Configured from console by admin on console
Switch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

Figure 6. 49: Disable unused port

### 6.2.16 AUTHENTICATION USING RADIUS SERVER

The main purpose we use Radius is to enable remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. In order to test the Radius Server working or not, we can connect by using telnet or SSH at the client side and try connecting to the radius client (in our case, router is our Radius client). After the client successfully logs in to the user access verification in the router, this will meet the policy that has been setup and all the detail record will be recorded at the directory C:>Windows> System32>LogFiles by default. Another way to test whether the Radius Server is working or not, we can view the log activity which is located inside the Network Policy and Access at the Server Manager.

Step 1: Open putty. Select Serial and click Open.

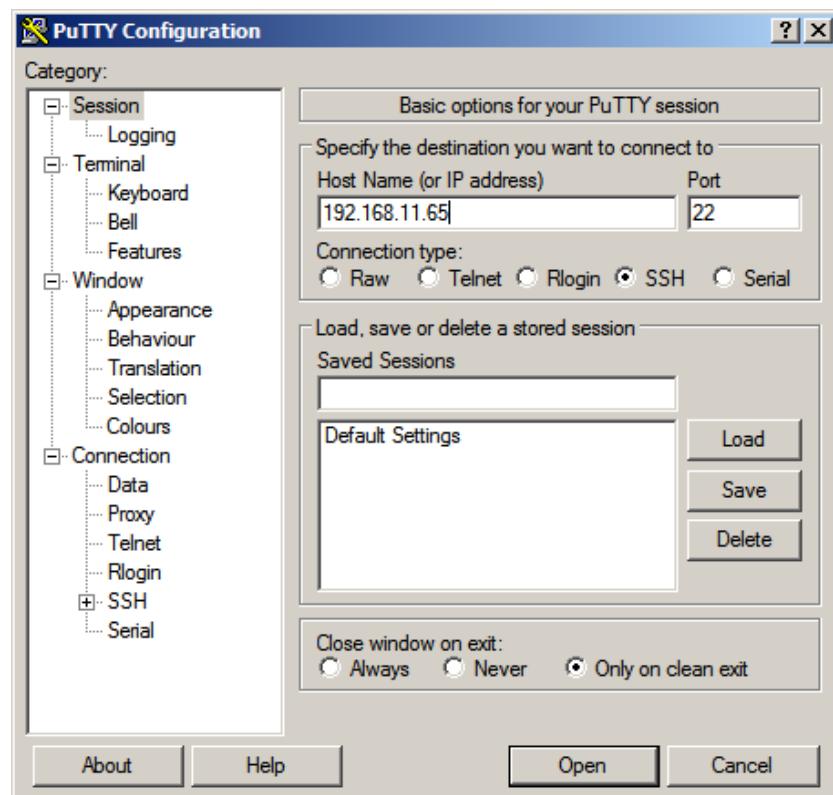


Figure 6. 50: Open serial

Step 2: User Access Verification will display. Enter the username (Any AD users) and password. Enter enable (en).

```

192.168.11.65 - PuTTY
login as: syukor
Using keyboard-interactive authentication.
Password:

#####
# WELCOME TO GROUP1 WORKSHOP UNAUTHORIZED USER IS PROHIBITED #
#
#####

*** Ensure that you enter cisco password correctly ***
*** Documentation after making system changes. ***

R1>en
R1>

```

Figure 6. 51: Login with AD user

### 6.2.17 USER AUTHENTICATION AND AUTHORIZATION

Step 1: Open putty.

Step 2: Test the user login to router. User unable to configure the router due to their privilege level is 1 although user is successfully login.

```

login as: ashley
Using keyboard-interactive authentication.
Password:

#####
# WELCOME TO GROUP1 WORKSHOP UNAUTHORIZED USER IS PROHIBITED #
#
#####

*** Ensure that you enter cisco password correctly ***
*** Documentation after making system changes. ***

R1>en
% Error in authentication.

R1>sh run
^
% Invalid input detected at '^' marker.

R1>conf t
^
% Invalid input detected at '^' marker.

R1>

```

Figure 6. 52: User Login in Router

### **6.2.18 FIREWALL FOR ROUTER**

Firewall ACL testing is done using the command show ip access-list in the router. This will show the output of how many matches found through the denied and permitted port. This then confirms that ACL is successfully configured.

Step 1: Access to web server from Client VLAN without using proxy server.

Step 2: There are 21 matches shows there are http packets were denied by the ACL.

```
Extended IP access list CLIENT
 10 deny tcp any any eq www (21 matches)
 20 deny tcp any any eq 443
 30 deny icmp any any
 40 deny tcp any any eq ftp-data
 50 deny tcp any any eq ftp
 60 permit ip any any (20691 matches)
```

Figure 6. 53: Show ip access-list

### **6.2.19 REMOTE LOGIN USING SSH**

#### **Testing SSH Login from the Windows Server**

Step 1: Open putty > insert ip address > click SSH > Open

SSH login to Linux 1:

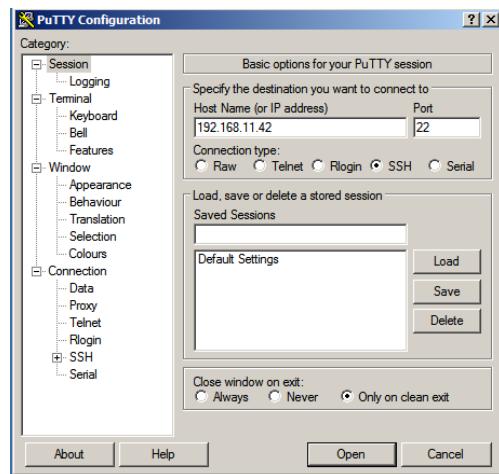


Figure 6. 54: Login to linux1

```
linux1@linux1-hp-xw6600-workstation: ~
login as: linux1
Using keyboard-interactive authentication.
Password:
Access denied
Access denied
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-98-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

12 packages can be updated.
12 updates are security updates.

Last login: Fri Nov 24 06:16:50 2017 from 192.168.11.34
linux1@linux1-hp-xw6600-workstation:~$
```

Figure 6. 55: Successfully login to linux1 terminal

SSH Login to Linux 2:

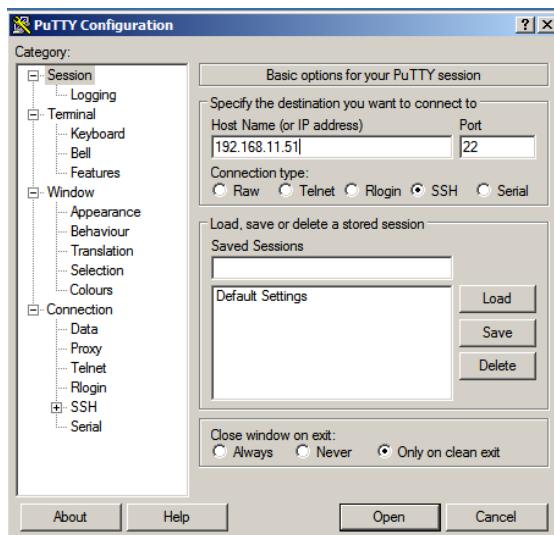


Figure 6. 56: Login to linux2

```
linux2@linux2-optiplex-9020: ~
login as: linux2
Using keyboard-interactive authentication.
Password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-101-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Wed Nov 22 13:05:46 2017 from 192.168.11.2
linux2@linux2-optiplex-9020:~$
```

Figure 6. 57: Successfully login to linux2 terminal

SSH Login to Switch:

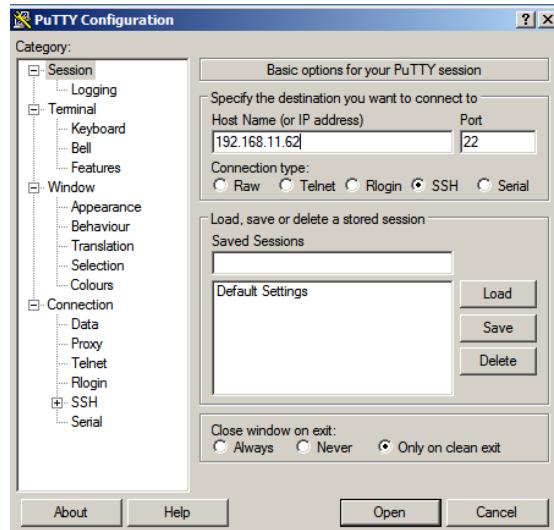


Figure 6. 58: Login to switch

```
192.168.11.62 - PuTTY
login as: admin
admin@192.168.11.62's password:
#####
# THIS SYSTEM IS PROVIDED FOR THE USE BY AUTORIZED USER ONLY. THANK YOU #
#
#####
*** Ensure that you enter cisco switch password ***
*** Documentation after making system changes. ***

Switch#
```

Figure 6. 59: Successfully login to switch

### SSH Login to Router:

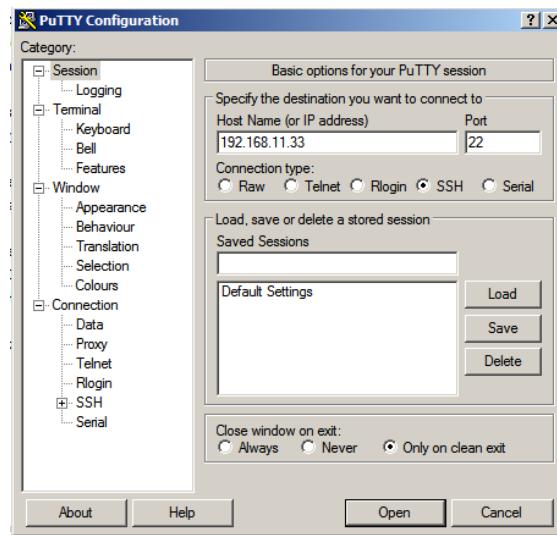


Figure 6. 60: Login to router

```
192.168.11.33 - PuTTY
login as: administrator
Using keyboard-interactive authentication.
Password:

#####
#          WELCOME TO GROUP1 WORKSHOP UNAUTHORIZED USER IS PROHIBITED      #
#
*** Ensure that you enter cisco password correctly ***
*** Documentation after making system changes.      **

R1:*
```

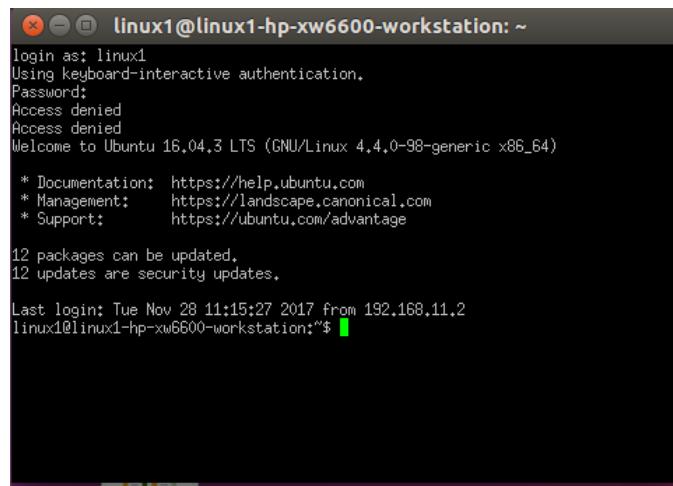
A screenshot of a terminal window titled '192.168.11.33 - PuTTY'. It shows a successful SSH login for the user 'administrator'. The terminal displays a welcome message from 'GROUP1 WORKSHOP' and some instructions at the bottom. The prompt 'R1:' is visible at the bottom.

Figure 6. 61: Successfully login to router

### Testing SSH Login from Linux 2 Ubuntu Server

Step 1: Open Putty > Insert IP Address > Choose SSH > Open

### SSH Login to Linux 1:



```
linux1@linux1-hp-xw6600-workstation: ~
login as: linux1
Using keyboard-interactive authentication.
Password:
Access denied
Access denied
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-98-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

12 packages can be updated,
12 updates are security updates.

Last login: Tue Nov 28 11:15:27 2017 from 192.168.11.2
linux1@linux1-hp-xw6600-workstation:~$
```

Figure 6. 62: Successfully login to linux1 terminal

### SSH Login to Switch:

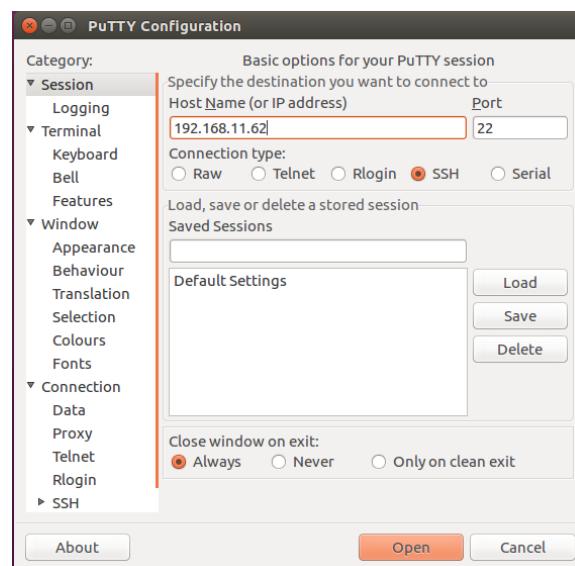
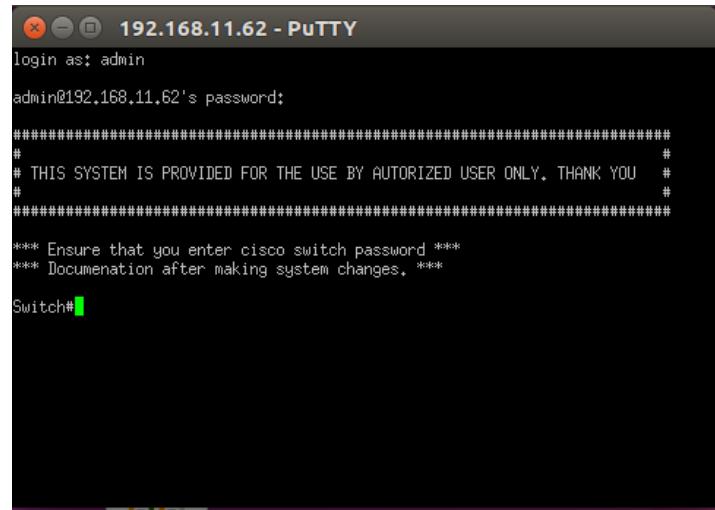


Figure 6. 63: Insert IP address of switch



```
192.168.11.62 - PuTTY
login as: admin
admin@192.168.11.62's password:
#####
# THIS SYSTEM IS PROVIDED FOR THE USE BY AUTORIZED USER ONLY. THANK YOU #
#
#####
*** Ensure that you enter cisco switch password ***
*** Documentation after making system changes. ***

Switch#
```

Figure 6. 64: Successfully login to switch

### SSH Login to Router:

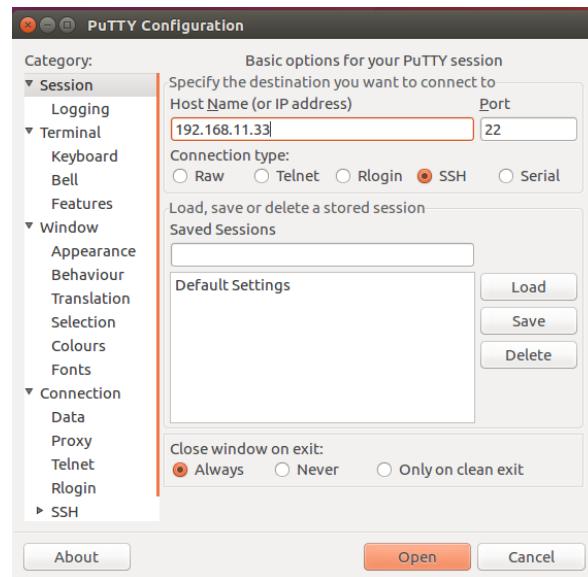
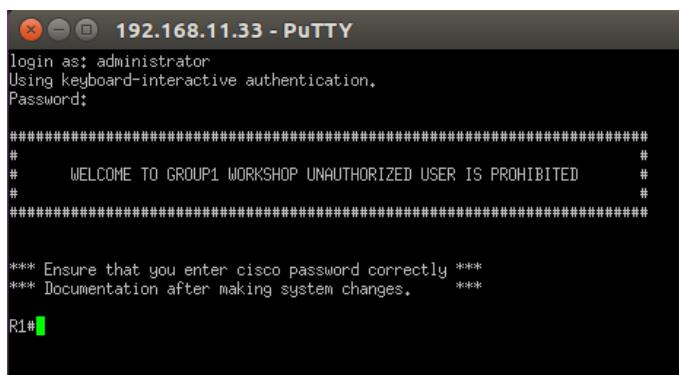


Figure 6. 65: Insert the IP address of router



The screenshot shows a PuTTY terminal window with the title "192.168.11.33 - PuTTY". The session details indicate "login as: administrator" and "Using keyboard-interactive authentication.". A password prompt follows. The terminal then displays a multi-line banner message:

```
#####
#      WELCOME TO GROUP1 WORKSHOP UNAUTHORIZED USER IS PROHIBITED      #
######
*** Ensure that you enter cisco password correctly ***
*** Documentation after making system changes. ***
```

Finally, the prompt "R1#" is visible at the bottom left, indicating a successful login.

Figure 6. 66: Successfully login to router

### 6.2.20 HARDENING LINUX SERVER

1. Before hardening:

```
linux2@linux2-optiplex-9020: ~
Completed SYN Stealth Scan at 09:55, 1.56s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000070s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
514/tcp   open  shell
631/tcp   open  ipp
1099/tcp  open  rmiregistry
1199/tcp  open  dmidi
3128/tcp  open  squid-http
5432/tcp  open  postgresql

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
  Raw packets sent: 1063 (46.772KB) | Rcvd: 2141 (89.952KB)
linux2@linux2-optiplex-9020:~$
```

Figure 6. 67: Ports opened before hardening

2. After removing ipp:

```
root@linux2-optiplex-9020: ~
Discovered open port 514/tcp on 127.0.0.1
Completed Connect Scan at 10:35, 0.01s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000044s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
514/tcp   open  shell
1099/tcp  open  rmiregistry
1199/tcp  open  dmidi
3128/tcp  open  squid-http
5432/tcp  open  postgresql

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
  Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
root@linux2-optiplex-9020:~#
```

Figure 6. 68: Ipp service is gone from the opened ports

3. Before removing mysql:

```

linux1@linux1-hp-xw6600-workstation: ~
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 139/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 9090/tcp on 127.0.0.1
Discovered open port 3128/tcp on 127.0.0.1
Completed Connect Scan at 04:51, 0.03s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00018s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3128/tcp  open  squid-http
3306/tcp  open  mysql
9090/tcp  open  zeus-admin

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
linux1@linux1-hp-xw6600-workstation:~$ 

```

Figure 6. 69: mysql is available at open ports

#### 4. After removing mysql:

```

linux1@linux1-hp-xw6600-workstation: ~
Try using --system-dns or specify valid servers with --dns-servers
Initiating Connect Scan at 06:49
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 139/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 9090/tcp on 127.0.0.1
Discovered open port 3128/tcp on 127.0.0.1
Completed Connect Scan at 06:49, 0.03s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00018s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3128/tcp  open  squid-http
9090/tcp  open  zeus-admin

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
linux1@linux1-hp-xw6600-workstation:~$ 

```

Figure 6. 70: mysql is gone from open ports

#### 5. Testing password:

```
x - root@linux2-optiplex-9020: ~
root@linux2-optiplex-9020:~# sudo passwd group1
New password:
BAD PASSWORD: it is WAY too short
BAD PASSWORD: is a palindrome
Retype new password: [REDACTED]
```

Figure 6. 71: Testing password after hardening

### **6.2.21 HARDENING WINDOWS SERVER**

Penetration Test Using Nmap before Hardening Window Server 2008

1. Enter the IP address of Windows Server at the target.
  2. Click Intense scan, all TCP ports at the Profile.

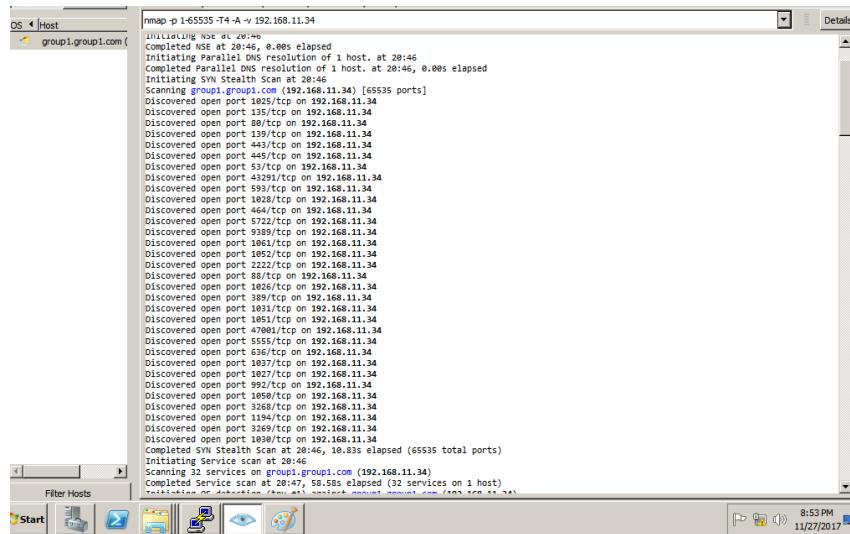


Figure 6. 72: Nmap Output before hardening

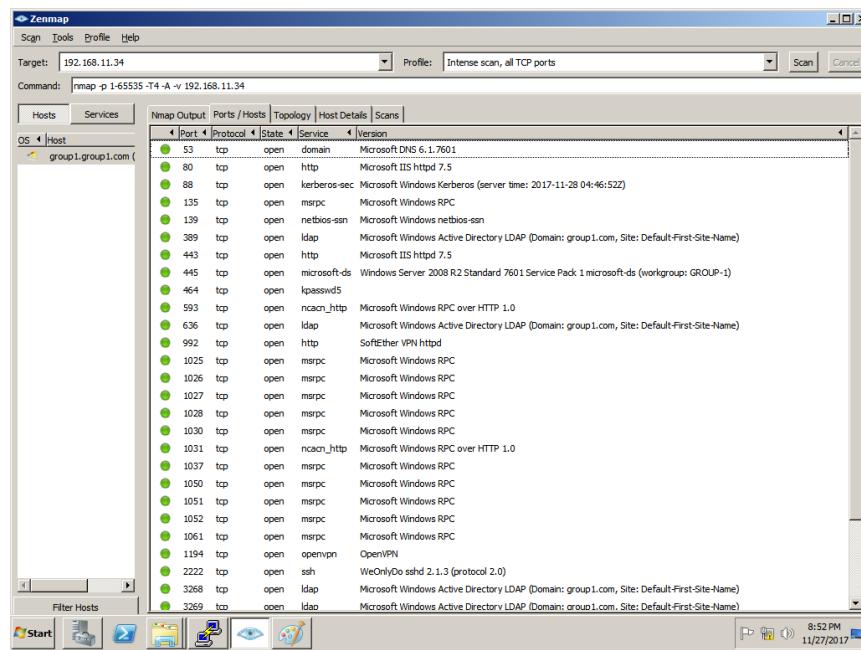


Figure 6. 73: Ports/Hosts before hardening (1)

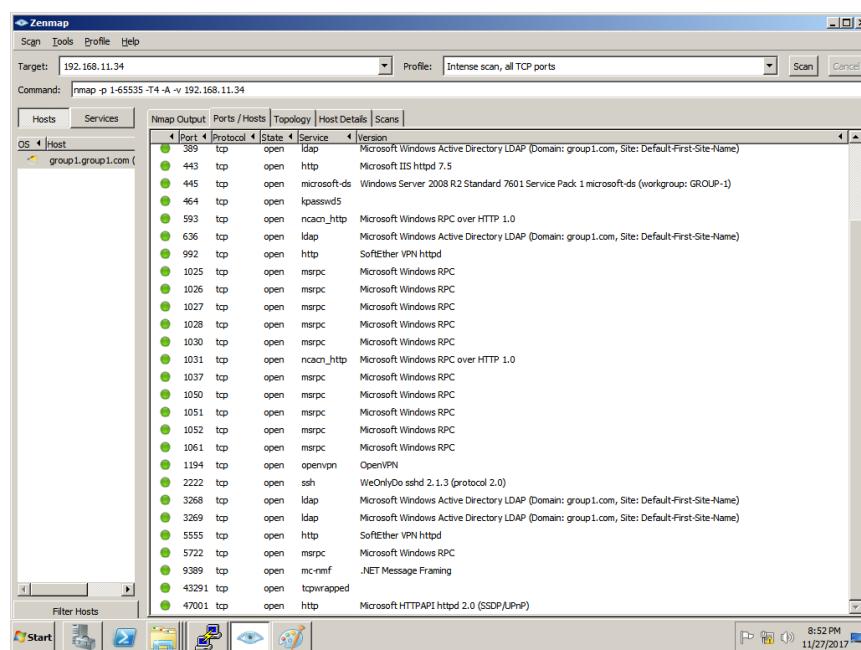


Figure 6. 74: Ports/Hosts before hardening (2)

There is a total of 32 ports opened before Hardening.

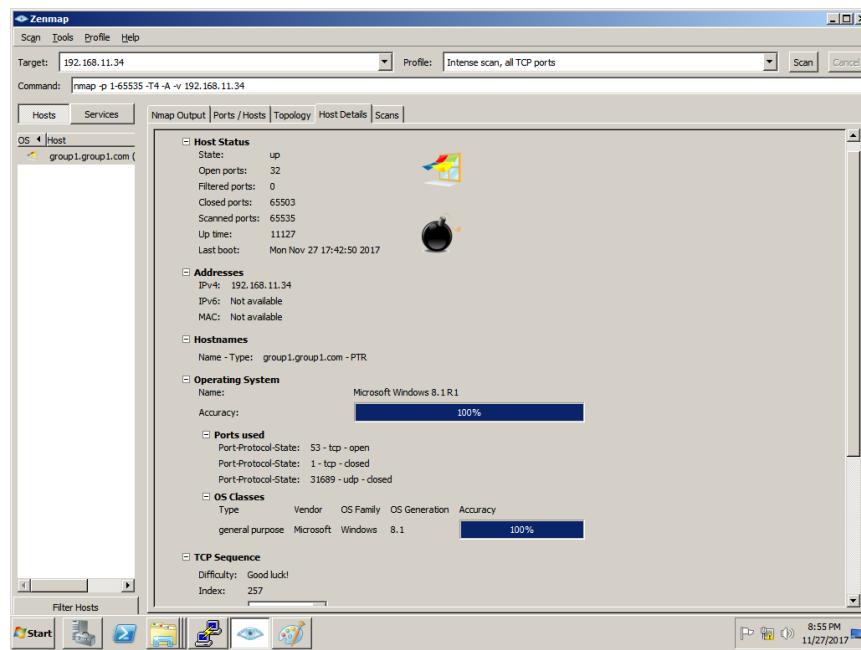


Figure 6. 75: Host Details before hardening

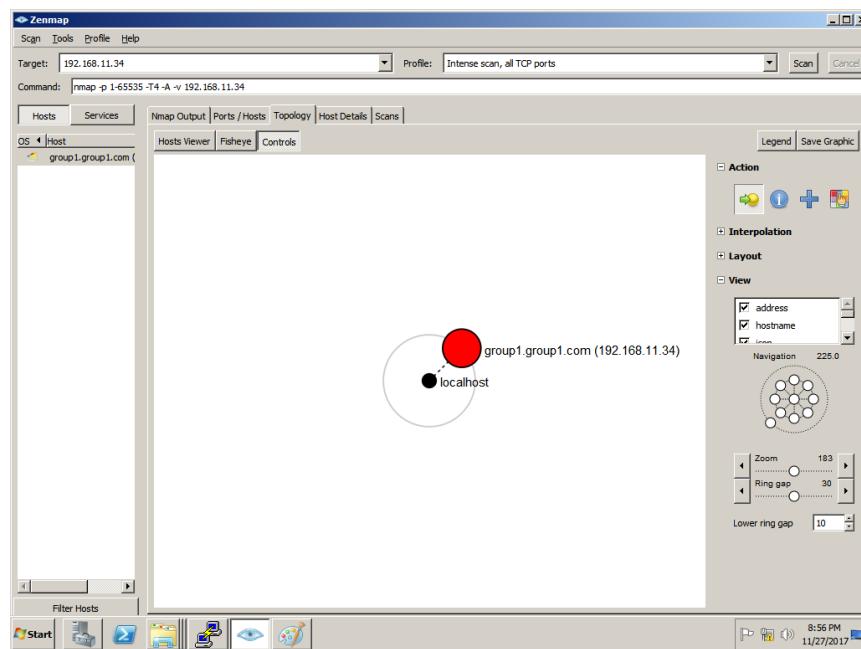


Figure 6. 76: Topology

Penetration Test Using Nmap after Hardening Window Server 2008

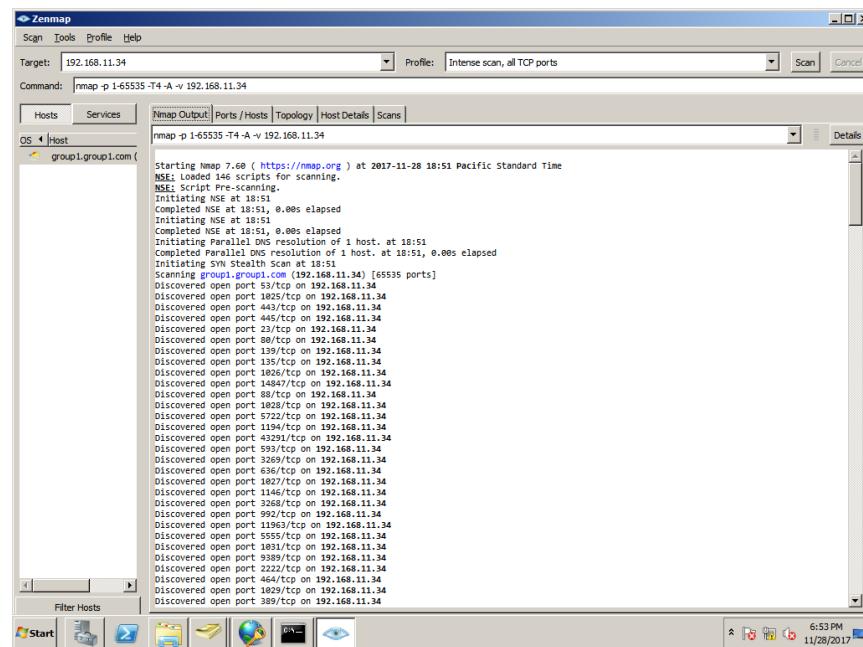


Figure 6. 77: Nmap Output after hardening

Port	Protocol	State	Service	Version
23	tcp	open	telnet	freeSSHd telnetd
53	tcp	open	domain	Microsoft DNS 6.1.7601
80	tcp	open	http	Microsoft IIS httpd 7.5
88	tcp	open	kerberos-sec	Microsoft Windows Kerberos (server time: 2017-11-29 02:51:24Z)
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
389	tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: group1.com, Site: Default-First-Site-Name)
443	tcp	open	http	Microsoft IIS httpd 7.5
445	tcp	open	microsoft-ds	Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds (workgroup: GROUP-1)
464	tcp	open	kpasswd5	
593	tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636	tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: group1.com, Site: Default-First-Site-Name)
992	tcp	open	http	SoftEther VPN httpd
1025	tcp	open	msrpc	Microsoft Windows RPC
1026	tcp	open	msrpc	Microsoft Windows RPC
1027	tcp	open	msrpc	Microsoft Windows RPC
1028	tcp	open	msrpc	Microsoft Windows RPC
1029	tcp	open	msrpc	Microsoft Windows RPC
1031	tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1057	tcp	open	msrpc	Microsoft Windows RPC
1146	tcp	open	msrpc	Microsoft Windows RPC
1194	tcp	open	openvpn	OpenVPN
2222	tcp	open	ssh	WeOnlyDo sshd 2.1.3 (protocol 2.0)
3268	tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: group1.com, Site: Default-First-Site-Name)
3269	tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: group1.com, Site: Default-First-Site-Name)
5555	tcp	open	http	SoftEther VPN httpd
5722	tcp	open	msrpc	Microsoft Windows RPC

Figure 6. 78: Ports/Hosts after hardening (1)

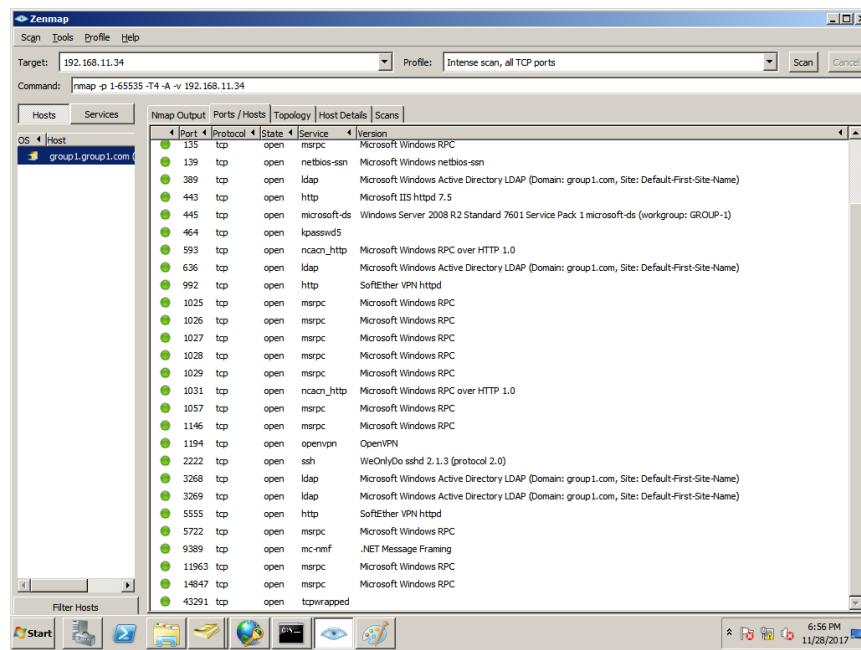


Figure 6. 79: Ports/Hosts after hardening (2)

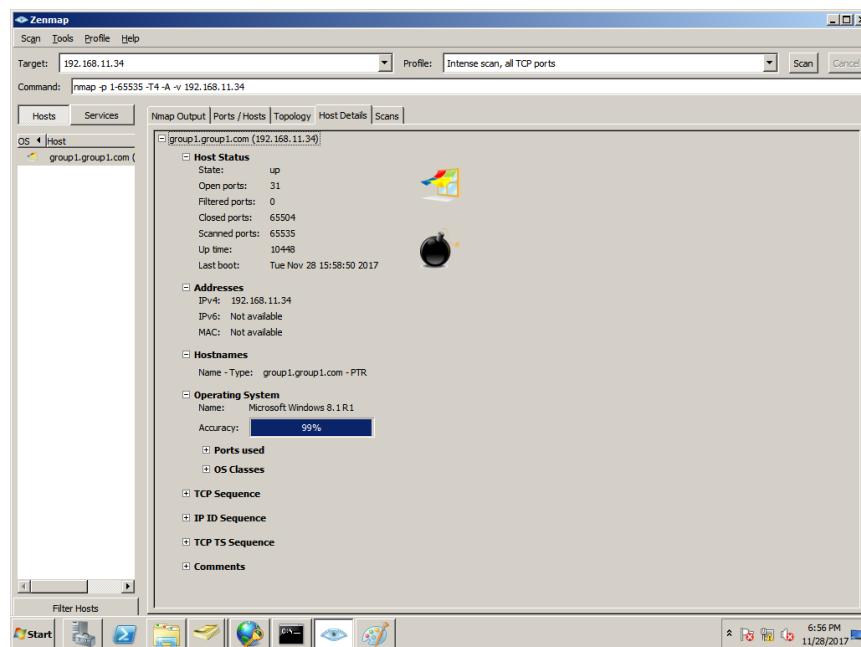


Figure 6. 80: Host Details after hardening

### 6.2.22 HARDENING WEB SERVER

When trying to open [www.group1.com](http://www.group1.com) from Linux1, the following result appear since 192.168.11.42 had been deny.

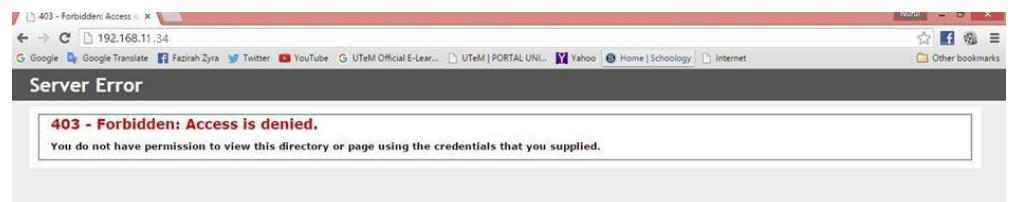


Figure 6. 81: Testing on IP address and Domain Restrictions

SSL certificate is located for https address.



Figure 6. 82: Testing on SSL certificate

We make an authentication required on the web server in order to restrict only users have permission to access the website. This is to make sure that the website is more secured.



Figure 6. 83: Testing on authentication

### **6.2.23 AUTHENTICATION USER BY INTEGRATING ACTIVE DIRECTORY WITH LINUX**

Step 1: First press **Ctrl+Alt+T** to open the Terminal. Then, type in the **cd /usr/share/lightdm/lightdm/conf.d/** command and press enter button. After that type the **ls -l** command to view a list.

```
linux2@linux2-optiplex-9020: /usr/share/lightdm/lightdm.conf.d
linux2@linux2-optiplex-9020:/usr/share/lightdm/lightdm.conf.d$ ls -l
total 24
-rw-r--r-- 1 root root 76 Apr  1 2017 50-disable-log-backup.conf
-rw-r--r-- 1 root root 66 Apr  1 2017 50-greeter-wrapper.conf
-rw-r--r-- 1 root root 62 Apr  1 2017 50-guest-wrapper.conf
-rw-r--r-- 1 root root 29 Ogos 14 2016 50-ubuntu.conf
-rw-r--r-- 1 root root 39 Mei  20 2015 50-unity-greeter.conf
-rw-r--r-- 1 root root 45 Apr  1 2017 50-xserver-command.conf
linux2@linux2-optiplex-9020:/usr/share/lightdm/lightdm.conf.d$
```

Figure 6. 84: Using ls –l command to view list.

Step 2: Then, type the sudo nano 50-ubuntu.conf command to edit the configuration in the file.

```
linux2@linux2-optiplex-9020: /usr/share/lightdm/lightdm.conf.d
linux2@linux2-optiplex-9020:/usr/share/lightdm/lightdm.conf.d$ sudo nano 50-ubuntu.conf
[sudo] password for linux2:
```

Figure 6. 85: Command to enter and edit the file content.

Step 3: After entering the file, add the line “allow-guest=false” and “greeter-show-manual-login=true” and then Save the configuration.

```
linux2@linux2-optiplex-9020: /usr/share/lightdm/lightdm.conf.d
GNU nano 2.5.3          File: 50-ubuntu.conf

[Seat:*]
user-session=ubuntu
allow-guest=false
greeter-show-manual-login=true
```

Figure 6. 86: Adding a new configuration into the file.

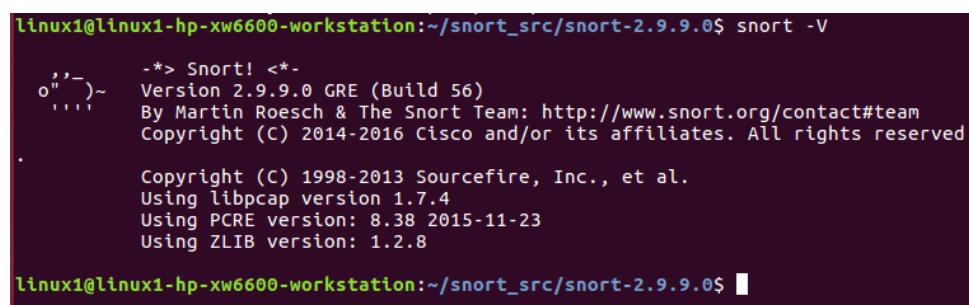
Step 4: After doing all of the above steps, make sure to Reboot the machine.

Step 5: Then, at first interface after the Reboot process there will be a new Login area. To login, type in the DOMAIN NAME\USERNAME and password that have been created during the AD service configuration earlier.

#### 6.2.24 INTRUSION DETECTION SYSTEM (PORT MIRROR)

##### Verify Snort Installation:

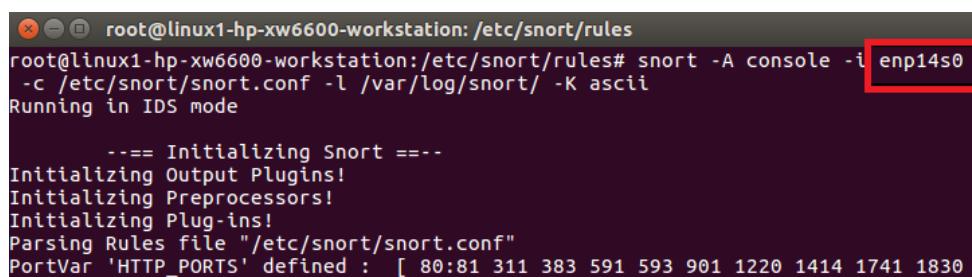
Enter the command: \$ snort -V



```
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0$ snort -V
o'''~  -*> Snort! <*-.
      Version 2.9.9.0 GRE (Build 56)
      By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014-2016 Cisco and/or its affiliates. All rights reserved
.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using libpcap version 1.7.4
      Using PCRE version: 8.38 2015-11-23
      Using ZLIB version: 1.2.8
linux1@linux1-hp-xw6600-workstation:~/snort_src/snort-2.9.9.0$
```

Figure 6. 87: Verify installation

Test the configuration file: \$ sudo snort -A console -i enp14s0 -c /etc/snort/snort.conf -l /var/log/snort/ -K ascii

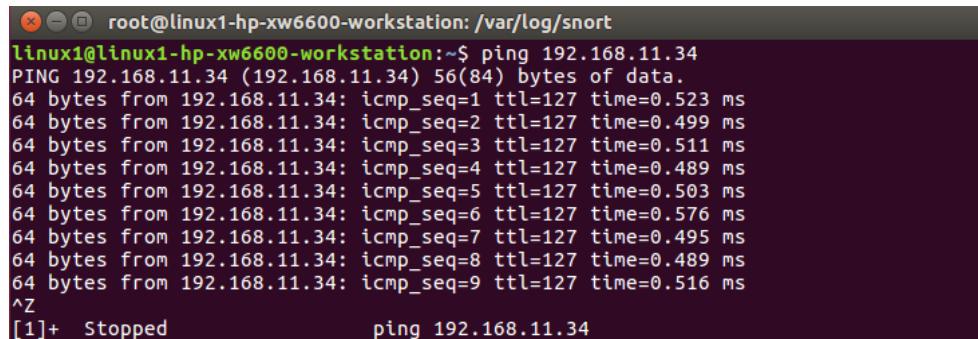


```
root@linux1-hp-xw6600-workstation:/etc/snort/rules
root@linux1-hp-xw6600-workstation:/etc/snort/rules# snort -A console -i enp14s0
-c /etc/snort/snort.conf -l /var/log/snort/ -K ascii
Running in IDS mode

     === Initializing Snort ===
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830
```

Figure 6. 88: Test configuration file using IDS interface

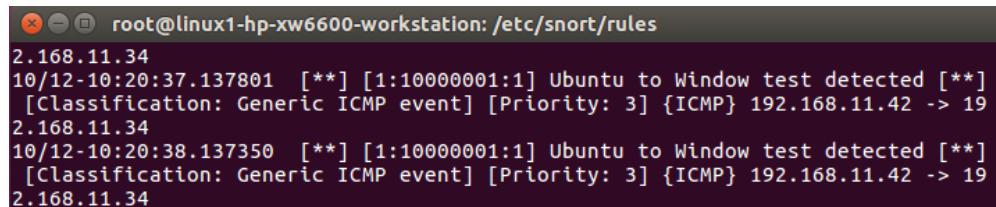
Now that Snort is running and listening on enp14s0, let's ping from Ubuntu Server (192.168.11.42) to Window server (192.169.11.34) by using the command above.



```
root@linux1-hp-xw6600-workstation: /var/log/snort
linux1@linux1-hp-xw6600-workstation:~$ ping 192.168.11.34
PING 192.168.11.34 (192.168.11.34) 56(84) bytes of data.
64 bytes from 192.168.11.34: icmp_seq=1 ttl=127 time=0.523 ms
64 bytes from 192.168.11.34: icmp_seq=2 ttl=127 time=0.499 ms
64 bytes from 192.168.11.34: icmp_seq=3 ttl=127 time=0.511 ms
64 bytes from 192.168.11.34: icmp_seq=4 ttl=127 time=0.489 ms
64 bytes from 192.168.11.34: icmp_seq=5 ttl=127 time=0.503 ms
64 bytes from 192.168.11.34: icmp_seq=6 ttl=127 time=0.576 ms
64 bytes from 192.168.11.34: icmp_seq=7 ttl=127 time=0.495 ms
64 bytes from 192.168.11.34: icmp_seq=8 ttl=127 time=0.489 ms
64 bytes from 192.168.11.34: icmp_seq=9 ttl=127 time=0.516 ms
^Z
[1]+  Stopped                  ping 192.168.11.34
```

Figure 6. 89: Ping other servers

Now you can see that there is and alert appeared.



```
root@linux1-hp-xw6600-workstation: /etc/snort/rules
2.168.11.34
10/12-10:20:37.137801  [**] [1:10000001:1] Ubuntu to Window test detected [**]
[Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.11.42 -> 19
2.168.11.34
10/12-10:20:38.137350  [**] [1:10000001:1] Ubuntu to Window test detected [**]
[Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.11.42 -> 19
2.168.11.34
```

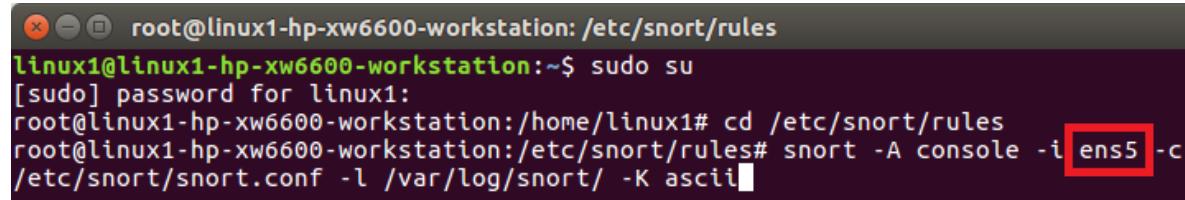
Figure 6. 90: An alert appeared

### **Port Mirror Testing:**

Ensure you in root user

Change the interface into port mirror.

```
$ sudo snort -A console -i ens5 -c /etc/snort/snort.conf -l /var/log/snort/ -K ascii
```

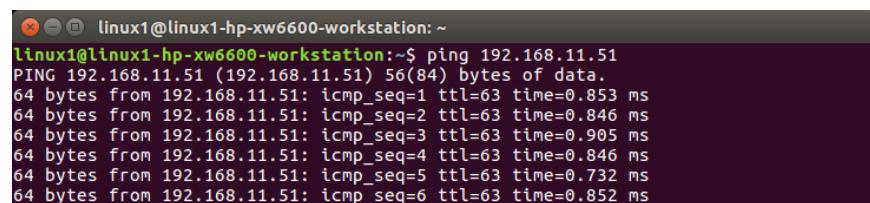


```
root@linux1-hp-xw6600-workstation: /etc/snort/rules
linux1@linux1-hp-xw6600-workstation:~$ sudo su
[sudo] password for linux1:
root@linux1-hp-xw6600-workstation:/home/linux1# cd /etc/snort/rules
root@linux1-hp-xw6600-workstation:/etc/snort/rules# snort -A console -i ens5 -c /etc/snort/snort.conf -l /var/log/snort/ -K ascii
```

Figure 6. 91: Testing configuration file using port mirror interface

Open new terminal,

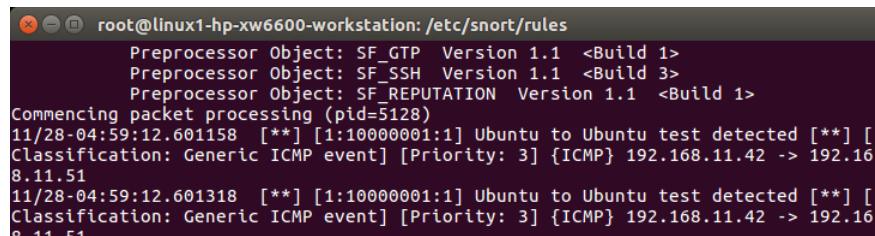
Ping from Linux Server (192.16.11.42) to Windows Server (192.168.11.34)



```
linux1@linux1-hp-xw6600-workstation: ~
linux1@linux1-hp-xw6600-workstation:~$ ping 192.168.11.51
PING 192.168.11.51 (192.168.11.51) 56(84) bytes of data.
64 bytes from 192.168.11.51: icmp_seq=1 ttl=63 time=0.853 ms
64 bytes from 192.168.11.51: icmp_seq=2 ttl=63 time=0.846 ms
64 bytes from 192.168.11.51: icmp_seq=3 ttl=63 time=0.905 ms
64 bytes from 192.168.11.51: icmp_seq=4 ttl=63 time=0.846 ms
64 bytes from 192.168.11.51: icmp_seq=5 ttl=63 time=0.732 ms
64 bytes from 192.168.11.51: icmp_seq=6 ttl=63 time=0.852 ms
```

Figure 6. 92: Ping other servers

Log file shown.



```
root@linux1-hp-xw6600-workstation: /etc/snort/rules
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Commencing packet processing (pid=5128)
11/28-04:59:12.601158 [**] [1:10000001:1] Ubuntu to Ubuntu test detected [**] [
Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.11.42 -> 192.16
8.11.51
11/28-04:59:12.601318 [**] [1:10000001:1] Ubuntu to Ubuntu test detected [**] [
Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.11.42 -> 192.16
8.11.51
```

Figure 6. 93: Log File (Ping from Linux to Windows)

## 6.2.25 IPSEC BETWEEN SERVER AND USER

Step 1: Monitor IPsec VPN protocol which is ESP protocol on Wireshark

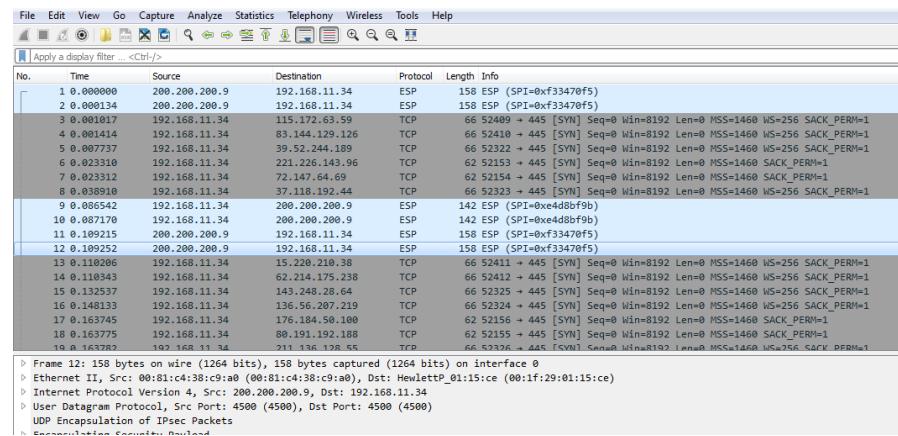


Figure 6. 94: Monitor ESP protocol

This because if connect the IPsec VPN, Wireshark only monitor the ESP protocol and another protocol cannot be monitor.

### 6.2.26 SAMBA SECURITY SERVICES

Samba security provided authentication security in order to give only authorized person to access the file or folder.

Step 1: Go to the workshop folder that been created.

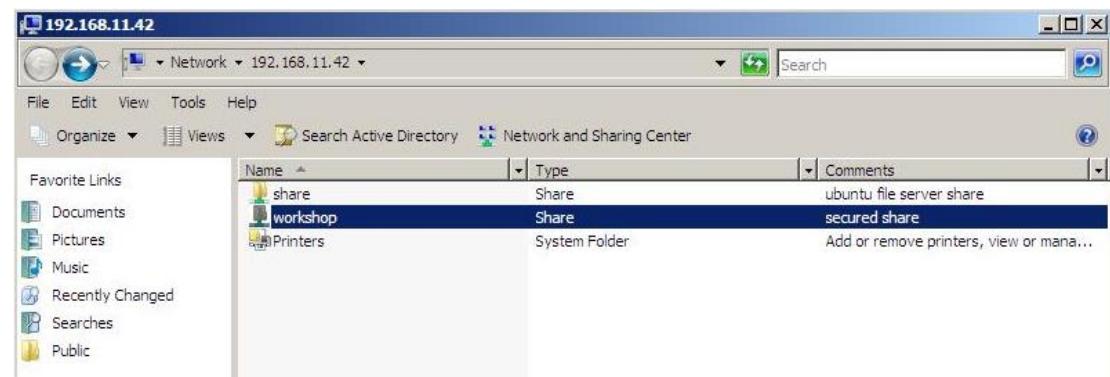


Figure 6. 95: Secured shared

Step 2: A window will appear to be fill with username and password

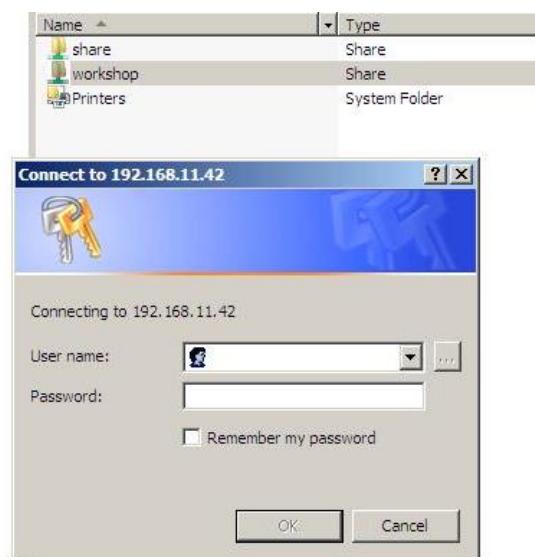


Figure 6. 96: Authentication required



Figure 6. 97: Insert username & password

### 6.2.27 PORT SECURITY

To check port security, use command show port-security.

```

Switch#sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
          (Count)        (Count)        (Count)
-----
Fa0/3           1            0            0      Shutdown
Fa0/7           1            0            0      Shutdown
Fa0/11          1            0            0      Shutdown
Fa0/15          1            1            1      Shutdown

Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8192
Switch#

```

Figure 6. 98: show port-security

To check port security address, use command show port-security address.

```

Switch#sh port-security address
      Secure Mac Address Table

-----+-----+-----+-----+-----+
Vlan   Mac Address       Type      Ports      Remaining Age
          (mins)
-----+-----+-----+-----+-----+
  60    d481.d76a.6c71  SecureConfigured  Fa0/15      -
-----+-----+-----+-----+-----+
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8192
Switch#

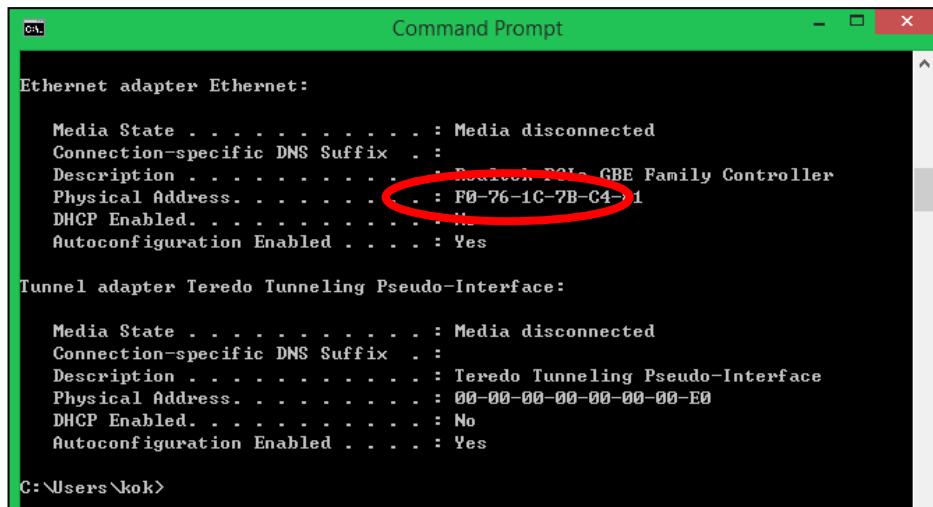
```

Figure 6. 99: show port-security address

### To test port security:

Step 1: Connect a PC or laptop which never connect to the switch.

Step 2: Record PC or laptop Ethernet interface physical address. To show the physical address of PC or laptop, use command ipconfig /all.



```

C:\> Command Prompt
Ethernet adapter Ethernet:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :
  Description . . . . . : Intel PRO GBE Family Controller
  Physical Address . . . . . : F0-76-1C-7B-C4-1
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes

Tunnel adapter Teredo Tunneling Pseudo-Interface:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :
  Description . . . . . : Teredo Tunneling Pseudo-Interface
  Physical Address . . . . . : 00-00-00-00-00-00-E0
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes

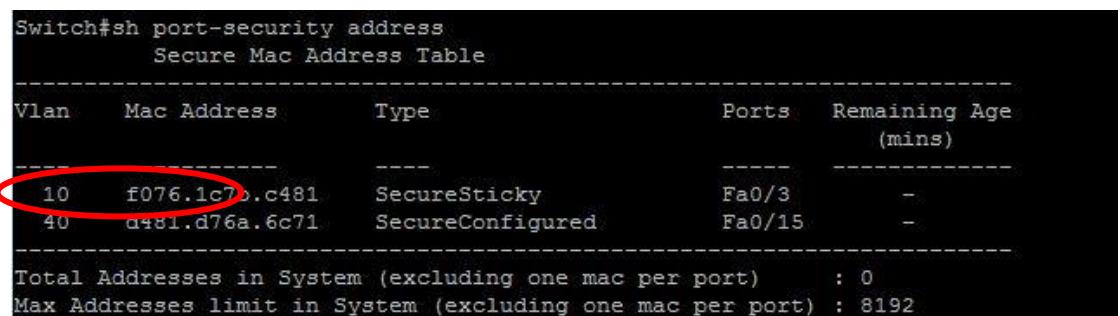
C:\Users\kok>

```

Figure 6. 100: Ipconfig /all

Step 3: Connect the PC or laptop into switch port.

Step 4: Check switch configuration. It shows that the MAC address is recorded in interface fa0/3.



Secure Mac Address Table					
Vlan	Mac Address	Type	Ports	Remaining Age (mins)	
10	f076.1c7b.c481	SecureSticky	Fa0/3	-	
40	a481.d76a.6c71	SecureConfigured	Fa0/15	-	
Total Addresses in System (excluding one mac per port) : 0					
Max Addresses limit in System (excluding one mac per port) : 8192					

Figure 6. 101: MAC Address Is Shown

Step 5: Connect the PC or laptop into other port. PC or laptop unable to connect to switch.

Step 6: Check status of switch port fa0/15 by using command show int status. It will show the port is down (err-disable).

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1		disabled	15	auto	auto	10/100BaseTX
Fa0/2		connected	10	a-full	a-100	10/100BaseTX
Fa0/3		notconnect	10	auto	auto	10/100BaseTX
Fa0/4		notconnect	10	auto	auto	10/100BaseTX
Fa0/5		connected	20	a-full	a-100	10/100BaseTX
Fa0/6		disabled	20	auto	auto	10/100BaseTX
Fa0/7		disabled	20	auto	auto	10/100BaseTX
Fa0/8		connected	30	a-full	a-100	10/100BaseTX
Fa0/9		disabled	30	auto	auto	10/100BaseTX
Fa0/10		disabled	30	auto	auto	10/100BaseTX
Fa0/11		disabled	30	auto	auto	10/100BaseTX
Fa0/12		connected	40	a-full	a-100	10/100BaseTX
Fa0/13		notconnect	40	auto	auto	10/100BaseTX
Fa0/14		disabled	40	auto	auto	10/100BaseTX
Fa0/15		err-disabled	40	auto	auto	10/100BaseTX
Fa0/16		notconnect	60	auto	auto	10/100BaseTX
Fa0/17		notconnect	60	auto	auto	10/100BaseTX

Figure 6. 102: show int status

Step 7: Check the status of switch port fa0/15 by connecting the PC or laptop

MAC address that we assigned. It will get an IPv4 address from DHCP.

```

Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . : group1.com
  IPv6 Address . . . . . : 2001:c0a8:b02:0:d58a:b013:9a0e:92ae
  Link-local IPv6 Address . . . . . : fe00::a5b6:185f:b49:727a%11
  IPv4 Address . . . . . : 192.168.11.2
  Subnet Mask . . . . . : 255.255.255.224
  Default Gateway . . . . . : fe80::281:c4ff:fe38:c9a0%11
                                         192.168.11.1

Tunnel adapter isatap.<5DC21EE6-CBCD-41B4-A589-AA30248E9B74>:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : group1.com

Tunnel adapter isatap.group1.com:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : group1.com

C:\Users\Group1>

```

Figure 6. 103: Ipconfig

## 6.2.28 SPANNING TREE PROTOCOL (STP) SECURITY

Show the STP summary by using command below:

```

Switch#sh spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN0001, VLAN0005, VLAN0010, VLAN0020, VLAN0030, VLAN0040
  VLAN0101
Extended system ID      is enabled
Portfast Default        is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default       is disabled
EtherChannel misconfig guard is enabled
UplinkFast              is disabled
BackboneFast             is disabled
Configured Pathcost method used is short

          Blocking Listening Learning Forwarding STP Active
-----+-----+-----+-----+-----+-----+
VLAN0001           0       0       0       1       1
VLAN0005           0       0       0       1       1
VLAN0010           0       0       0       2       2
VLAN0020           0       0       0       2       2
VLAN0030           0       0       0       2       2
VLAN0040           0       0       0       2       2
VLAN0101           0       0       0       1       1
-----+-----+-----+-----+-----+-----+
          Blocking Listening Learning Forwarding STP Active
-----+-----+-----+-----+-----+
7 vlans            0       0       0      11      11
Switch# █

```

Figure 6. 104: Show STP summary

### 6.2.29 VLAN SECURITY

By using command show vlan on switch, we can know that fa0/1, fa0/18, fa0/19, fa0/20, fa0/21, fa0/23, gi0/1, and gi0/2 are in VLAN unusedPort which is suspended.

VLAN	Name	Status	Ports
1	default	active	
5	Trunk	active	
10	WindowsServer	active	Fa0/2, Fa0/3, Fa0/4
15	unusedPort	suspended	Fa0/1, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/23, Gi0/1, Gi0/2
20	LinuxServer1	active	Fa0/5, Fa0/6, Fa0/7
30	LinuxServer2	active	Fa0/8, Fa0/9, Fa0/10, Fa0/11
40	Client	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15
50	Management	active	
60	wireless	active	Fa0/16, Fa0/17
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdtnet-default	act/unsup	
1005	trnet-default	act/unsup	

Figure 6. 105: show vlan

We try to connect a PC or laptop into fa0/18, the connection cannot be made.

To check the status, use command ipconfig.

```
C:\Users\kok>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

C:\Users\kok>
```

Figure 6. 106: Ipconfig

To check VLAN trunk, use command show interface trunk.

```
Switch#sh int trunk

Port      Mode          Encapsulation  Status        Native vlan
Fa0/24    on           802.1q         trunking    5

Port      Vlans allowed on trunk
Fa0/24    5,10,20,30,40,50,60

Port      Vlans allowed and active in management domain
Fa0/24    5,10,20,30,40,50,60

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/24    5,10,20,30,40,50,60
Switch#
```

Figure 6. 107: show interface trunk

### 6.2.30 NETWORK TIME PROTOCOL (NTP)

On Client:

Step 1: Open Date and Time Setting> Internet time> Change time setting.

Step 2: Tick on “Synchronize with an internet time server”.

Step 3: Insert the IP address of NTP server> Click Update now.

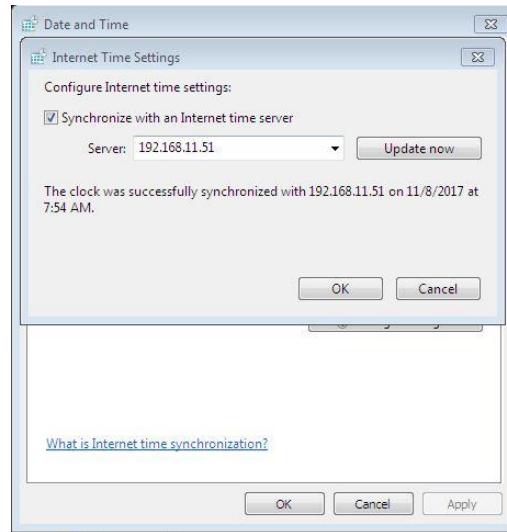


Figure 6. 108: Testing to sync

### 6.2.31 SYSLOG

Step 1: Open system log and view syslog server on Linux 2

```

Nov 29 14:11:02 linux2-optiplex-9020 postfix/qmgr[7190]: 84B661122B6E: from=<syukor@ubuntu2.group1.com>, size=707, nrcpt=1 (queue active)
Nov 29 14:11:02 linux2-optiplex-9020 postfix/smtpd[11392]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5
Nov 29 14:11:02 linux2-optiplex-9020 dovecot: imap-login: Login: user=<syukor>, method=PLAIN, rip=127.0.0.1, lpid=11406, secured, session=<YWcFABlfNqp/AAAB>
Nov 29 14:11:02 linux2-optiplex-9020 postfix/smtp[11398]: 84B661122B6E: to=<ara@ubuntu2.group1.com>, relay=none, delay=0.19, delays=0.18/0/0/0, dsn=4.4.3, status=deferred (1)
Nov 29 14:11:02 linux2-optiplex-9020 dovecot: imap-login: Logged out in=587 out=564
Nov 29 14:11:02 linux2-optiplex-9020 dovecot: imap-login: Login: user=<syukor>, method=PLAIN, rip=127.0.0.1, lpid=11408, secured, session=<GtQIABlfOKp/AAAB>
Nov 29 14:11:02 linux2-optiplex-9020 dovecot: imap-login: Logged out in=117 out=1526
Nov 29 14:11:03 linux2-optiplex-9020 dovecot: imap-login: Login: user=<syukor>, method=PLAIN, rip=127.0.0.1, lpid=11408, secured, session=<GtQIABlfOKp/AAAB>
Nov 29 14:11:06 linux2-optiplex-9020 dovecot: imap-login: Login: user=<syukor>, method=PLAIN, rip=127.0.0.1, lpid=11412, secured, session=<q4BAbLfOqp/AAAB>
Nov 29 14:11:06 linux2-optiplex-9020 dovecot: imap-login: Logged out in=289 out=2027
Nov 29 14:11:20 linux2-optiplex-9020 dovecot: imap-login: Login: user=<ara>, method=PLAIN, rip=127.0.0.1, lpid=11415, secured, session=<IzQARlfPqp/AAAB>
Nov 29 14:11:20 linux2-optiplex-9020 dovecot: imap(ara): Logged out in=44 out=831
Nov 29 14:11:20 linux2-optiplex-9020 dovecot: imap-login: Login: user=<ara>, method=PLAIN, rip=127.0.0.1, lpid=11417, secured, session=<OsQARlfqqp/AAAB>
Nov 29 14:11:20 linux2-optiplex-9020 dovecot: imap(ara): Logged out in=261 out=1883
Nov 29 14:11:20 linux2-optiplex-9020 dovecot: imap-login: Login: user=<ara>, method=PLAIN, rip=127.0.0.1, lpid=11419, secured, session=<Z0ERARlfRkp/AAAB>
Nov 29 14:11:30 linux2-optiplex-9020 dovecot: imap(ara): Logged out in=117 out=1526
Nov 29 14:11:30 linux2-optiplex-9020 dovecot: imap-login: Login: user=<ara>, method=PLAIN, rip=127.0.0.1, lpid=11421, secured, session=<bh6nArLfsKp/AAAB>
Nov 29 14:11:30 linux2-optiplex-9020 dovecot: imap(ara): Logged out in=269 out=2026
Nov 29 14:12:09 linux2-optiplex-9020 postfix/smtpd[11392]: connect from localhost[127.0.0.1]
Nov 29 14:12:09 linux2-optiplex-9020 postfix/smtpd[11392]: client=[localhost[127.0.0.1]]
Nov 29 14:12:09 linux2-optiplex-9020 postfix/cleanup[11397]: DABAB1123613: message-id=<19d5e68413effdb9f92a1bd83f71e5f0.squirrel@localhost>
Nov 29 14:12:09 linux2-optiplex-9020 postfix/smtpd[11392]: disconnect from localhost[127.0.0.1] ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5
Nov 29 14:12:09 linux2-optiplex-9020 postfix/smtpd[11398]: 25C401123741: to=<syukor@ubuntu2.group1.com>, relay=none, delay=0.08, delays=0.08/0/0/0, dsn=4.4.3, status=deferred (1)
Nov 29 14:12:10 linux2-optiplex-9020 postfix/smtp[11398]: 25C401123741: from=<ara@ubuntu2.group1.com>, size=705, nrcpt=1 (queue active)
Nov 29 14:12:10 linux2-optiplex-9020 dovecot: imap-login: Login: user=<ara>, method=PLAIN, rip=127.0.0.1, lpid=11433, secured, session=<voMHBBlfUkp/AAAB>
Nov 29 14:12:10 linux2-optiplex-9020 dovecot: imap(ara): Logged out in=588 out=566
Nov 29 14:12:10 linux2-optiplex-9020 dovecot: imap-login: Login: user=<ara>, method=PLAIN, rip=127.0.0.1, lpid=11447, secured, session=<pfsJB8lfXqp/AAAB>
Nov 29 14:12:10 linux2-optiplex-9020 dovecot: imap(ara): Logged out in=291 out=2419
Nov 29 14:12:21 linux2-optiplex-9020 dovecot: imap-login: Login: user=<syukor>, method=PLAIN, rip=127.0.0.1, lpid=11452, secured, session=</m2B8B1fakp/AAAB>
Nov 29 14:12:21 linux2-optiplex-9020 dovecot: imap(lyukor): Logged out in=44 out=831
Nov 29 14:12:22 linux2-optiplex-9020 dovecot: imap-login: Login: user=<syukor>, method=PLAIN, rip=127.0.0.1, lpid=11454, secured, session=<9A23B8B1fkp/AAAB>
Nov 29 14:12:22 linux2-optiplex-9020 dovecot: imap(lyukor): Logged out in=261 out=1883
Nov 29 14:12:22 linux2-optiplex-9020 dovecot: imap-login: Login: user=<syukor>, method=PLAIN, rip=127.0.0.1, lpid=11456, secured, session=<FNq4BBlfbqp/AAAB>
Nov 29 14:12:22 linux2-optiplex-9020 dovecot: imap(lyukor): Logged out in=117 out=1526
Nov 29 14:12:25 linux2-optiplex-9020 dovecot: imap-login: Login: user=<syukor>, method=PLAIN, rip=127.0.0.1, lpid=11458, secured, session=<ZyP7B8lfCkp/AAAB>
Nov 29 14:12:25 linux2-optiplex-9020 dovecot: imap(lyukor): Logged out in=289 out=2027
Nov 29 14:12:28 linux2-optiplex-9020 dovecot: imap-login: Login: user=<syukor>, method=PLAIN, rip=127.0.0.1, lpid=11460, secured, session=<gEs0B8lfcp/AAAB>
Nov 29 14:12:47 linux2-optiplex-9020 dovecot: imap-login: Login: user=<syukor>, method=PLAIN, rip=127.0.0.1, lpid=11465, secured, session=<en8+Bhlfdqp/AAAB>
Nov 29 14:12:52 linux2-optiplex-9020 dovecot: imap-login: Login: user=<syukor>, method=PLAIN, rip=127.0.0.1, lpid=11468, secured, session=<8a1BhlfeKp/AAAB>
Nov 29 14:13:06 linux2-optiplex-9020 dovecot: imap-login: Aborted Login (auth failed, 1 attempts in 5 secs): user=<fitri>, method=PLAIN, rip=127.0.0.1, lpid=127.0.0.1, secured
Nov 29 14:13:38 linux2-optiplex-9020 netlogon: [netlogon] Failed ldap search on 2001:c0a8:b22:0:0:0:0:2 error=40290
Nov 29 14:13:38 linux2-optiplex-9020 lsass: [lsass] Failed to sync system time [error code: 9502]
Nov 29 14:14:08 linux2-optiplex-9020 org.gnome.evolution.dataserver.Sources[2898]: ** (evolution-source-registry:3157): WARNING **: secret_service_search_sync: must specify
Nov 29 14:14:08 linux2-optiplex-9020 org.gnome.evolution.dataserver.Sources[2898]: where=[1935]: [14:14:08.226444] reached: https://apps.ubuntu.com
Nov 29 14:15:01 linux2-optiplex-9020 CRON[11728]: (root) CMD (command) /usr/sbin/ntpdate -u null && debian-sa 1 1
Nov 29 14:16:36 linux2-optiplex-9020 postfix/qmgr[7190]: 84B661122B6E: from=<ara@ubuntu2.group1.com>, size=705, nrcpt=1 (queue active)
Nov 29 14:16:36 linux2-optiplex-9020 postfix/smtp[7190]: 84B661122B6E: from=<ara@ubuntu2.group1.com>, size=705, nrcpt=1 (queue active)
Nov 29 14:16:36 linux2-optiplex-9020 postfix/smtpd[11766]: 25C401123741: to=<fitri@ubuntu2.group1.com>, relay=none, delay=569, delays=569/0.01/0/0, dsn=4.4.3, status=deferred (1)

```

Figure 6. 109: Syslog Server log

### 6.2.32 WIRELESS AUTHENTICATION USING RADIUS SERVER

Step 1: Restart Cisco Access Point Device

Step 2: Open Wireless Network Connection and Click Group 1

Step 3: Wireless Connection will display. Enter the username (Any AD users) and password. Click OK

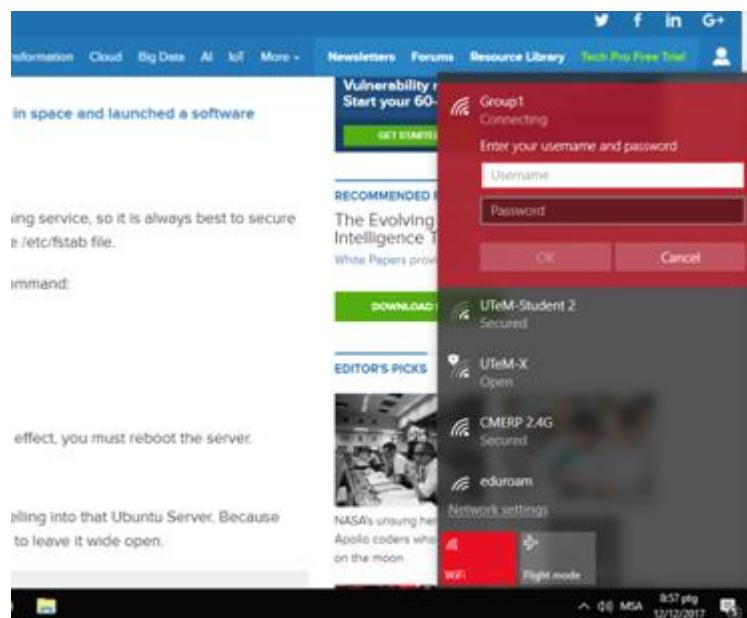


Figure 6. 110: Group1 Wireless Connection

### 6.2.33 ACTIVE DIRECTORY

Step 1: With using computer client to login the active directory user. Go to the Computer and right click Properties.



Figure 6. 111: Right click the computer and select Properties

Step 2: Then, click on the advanced system settings.

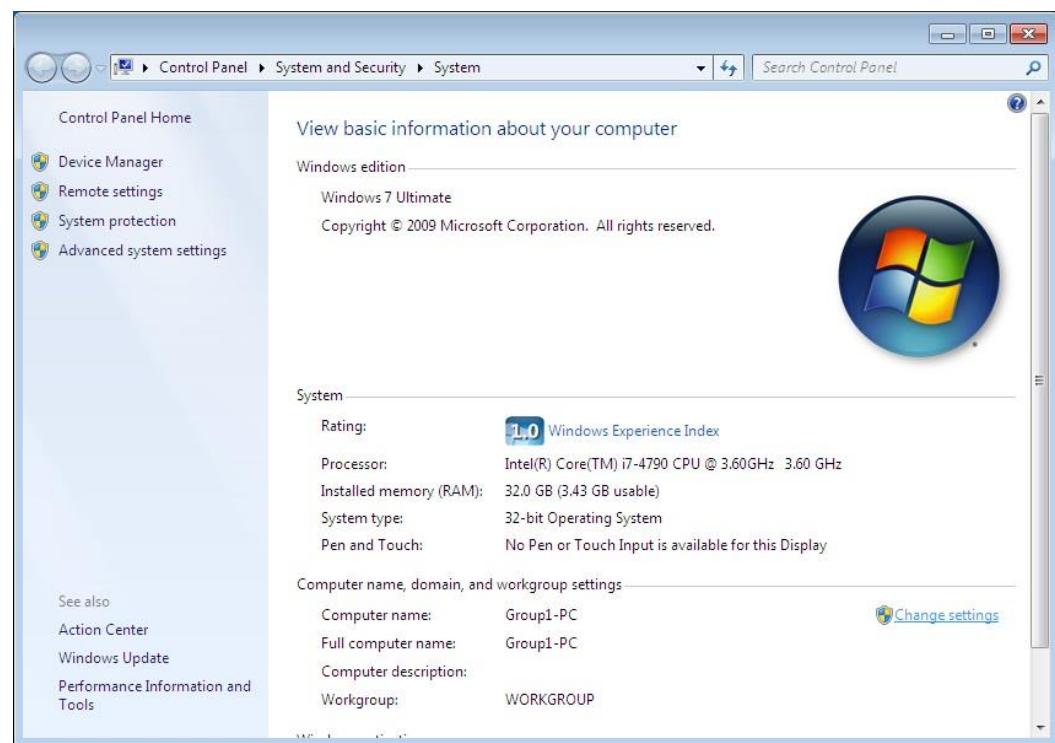


Figure 6. 112: Click on the advanced system settings option

Step 3: To connect to the domain (group1.com), click on the Change button

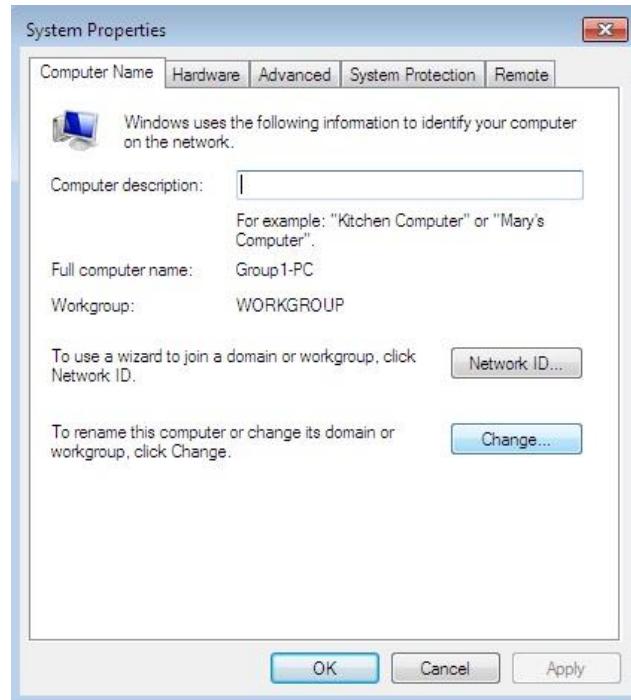


Figure 6. 113: Click on the Change button

Step 4: Click on the domain radio button, and change the name to the “group1.com”. Click OK when done.

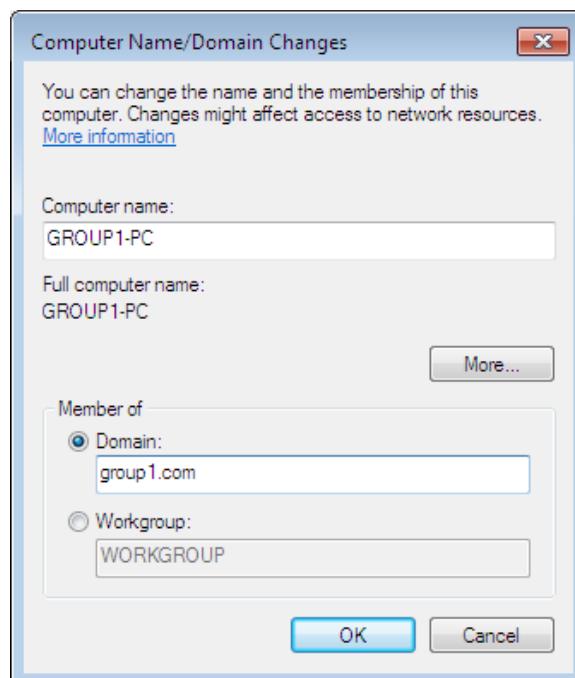


Figure 6. 114: Change the domain to the “group1.com”

Step 5: A window security will pop out. Use one of the AD users to login to the domain.

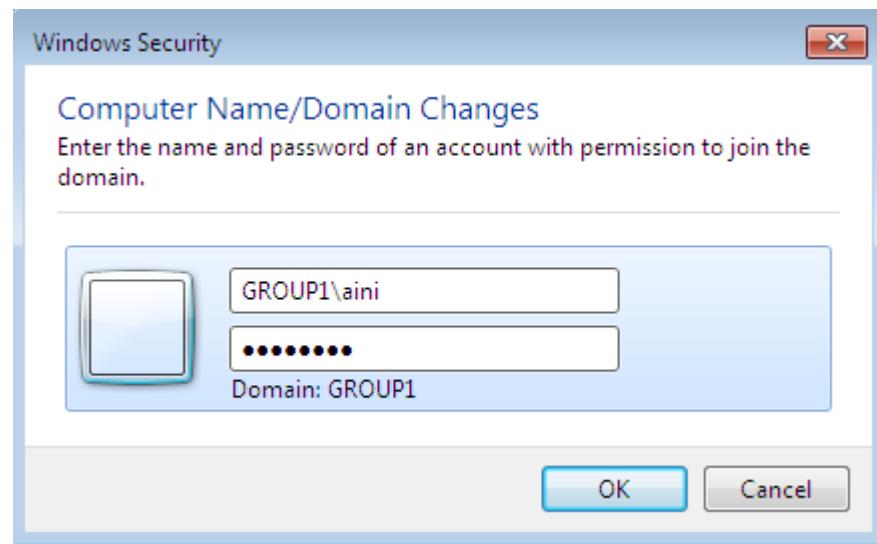


Figure 6. 115: Enter login username and password

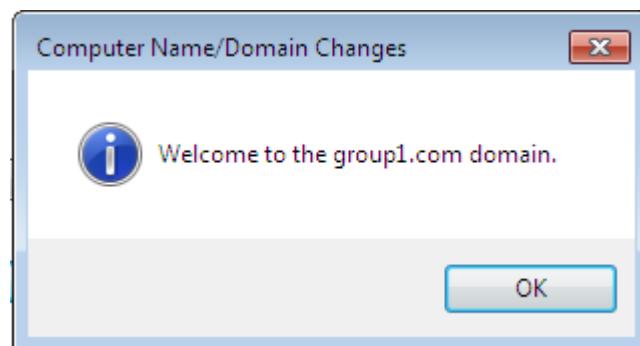


Figure 6. 116: The Welcome notification will be pop out when login success.

### 6.3 CONCLUSION

During the testing phase, we found that some services were not working. To troubleshoot it, we check the log file and configuration file. Also, we check on the dependencies and firewall to ensure the required port is open.

## CHAPTER 7: CONCLUSION

### 7.1 INTRODUCTION

Through these weeks in workshop, a lot of networking stuff have been studied and experienced. With limited knowledge and experience, we successfully managed to set up, configure, maintain, and troubleshoot a complete network infrastructure. We also understand the basic concept of the services in this workshop. All the hard work that been put into this project are considered as a preparation for us to attend industrial training. The overall performance for this workshop is quite satisfying. Although there were certain difficulties arisen while completing the workshop, we successfully done it before due date. It is very important in managing every task to prevent any problems and error from occurring. This network infrastructure that we developed is suitable for Small and Medium Enterprise Business since it is in small scale and is easy to manage and implement. Furthermore, it includes all the basic service (such as DNS, DHCP, Email, SFTP and etc.) that needs to run the business. After going through all the obstacles and challenges in completing the tasks, we are grateful to gain all these knowledge and experience.

### 7.2 PROJECT ADVANTAGES

This project provides us a great opportunity to implement a real network environment that are useful in the industrial. We had learnt to configure and maintain various of network services by using the equipment provided by UTeM. Without this workshop, we probably just understand the theory and have no experience in configuring and troubleshooting network devices at all. This can be a big problem when we are working in the future because an employer would expect a networking

graduate know how to manage the servers and routers. Therefore, this is a golden opportunity for us to learn how to be a professional network engineer.

On the other hands, we also learnt to troubleshoot and overcome the problems that we faced during implementing the services in the servers with different operating system. Others important benefit that we get is we had gained experience on how to work in a group and tolerate between each other to complete this project.

### **7.3 PROJECT DISADVANTAGES**

However, there are always pros and cons in a project. The disadvantages that we found in this project are the servers' PC are too old and not in good condition. This caused the servers corrupted and not working as expected. Besides, most of the services we have no idea on what are they and how to configure them. So, it became flurry when we faced problems during configuration. We suggest that faculty could include some basic server configuration hands on before we are taking this workshop.

### **7.4 PROJECT LIMITATION**

There are some limitations of this workshop:

1. The group members are stand from BITC and BITZ students. It makes the discussion harder as the timetable of everyone is required to be in the consideration.
2. Lack of current industrial technique. Most of the enterprises are implementing switch stacking, load balancing, and server failover

technique. Faculty is suggested to introduce these techniques into workshop as it will be useful for students in future working environment.

3. The equipment provided is not in good condition as expected. Some of the servers' PC will restart several times when turn on due to low battery and RAM problems. These had slowed down our progress and unable to accomplish this project on scheduled.

## **7.5 CONCLUSION**

Upon the completion of Workshop 2, we are expected to be able to install, configure, monitor and maintain our network infrastructure. In this workshop, we had used heterogenous operating system for different servers such as Microsoft Windows Server 2008 R2 and Ubuntu 16.04. We are also designed our own network by assigning the appropriate IP address and VLANs for maintaining a good network environment.

Furthermore, we have learned to build up crucial security system to secure and protect the network from being unauthorized access. With the project planning and cooperation from everyone in the team, we able to finish the project on schedule.

We become more knowledgeable as we make use of all the skills that we have learned and apply them in Workshop 2. This is a good opportunity for us to gain experience and knowledge that can be used in the future. Finally, this project is a very good network environment exposure to us. Thanks to every support and helping hands, we completed all the given tasks successfully.

## **BIBLIOGRAPHX**

Book:

1. L.L. Peterson and B.S. Davie (2000), Computer Networks: A System Approach. Morgan Kaufman Publisher.
2. R. Caceres, F. Douglis, A. Feldmann, G. Glass, M. Rabinovich (1998). Web proxy caching: the devil is in the details. Workshop on Internet Server Performance held with SIGMETRICS.
3. Carl Taylor, Alistair McDonald (2005). Linux Email: Setup and Run a Small Office Email Server Using Postfix, Courier, Procmail, Squirrelmail, Clamav and Spamassassin. Packt Publishing.
4. Paul Mueller. John (2007). "IIS 7 Implemntation and Administration".

Website:

1. "Usage of operating systems for websites". W3Techs. 7 March 2015.
2. "What's new in 16.04 LTS". Ubuntu.com. Canonical Ltd. 2016. Retrieved 13 June 2016.
3. Dr. Thomas W. Shinder (2009, June 10th). Overview of the Windows Server 2008 Firewall with Advanced Security Part 2: Inbound and Outbound Firewall Rules. Retrieved from <http://www.windowsecurity.com/articles/Windows-Server-2008-Firewall-Advanced-Security-Part2.html>
4. David Davis (2008, Dec.9th). How to Install and Configure Windows Server 2008 DHCP Server. Retrieved from [http://www.windowsnetworking.com/articles\\_tutorials/How-to-Install-ConfigureWindows-Server-2008-DHCP-Server.html](http://www.windowsnetworking.com/articles_tutorials/How-to-Install-ConfigureWindows-Server-2008-DHCP-Server.html)

5. Linode (March 24th, 2014) Troubleshooting Problems with Postfix, Dovecot, and MySQL from

<https://www.linode.com/docs/email/postfix/troubleshootingproblems-with-postfix-dovecot-and-mysql#dovecot>.

6. Cisco IOS IPv6 Configuration Guide (2009, March 5th). Retrieved from  
[http://www.cisco.com/c/en/us/td/docs/ios/ipv6/configuration/guide/12\\_4t/ipv\\_12\\_4t\\_book/ip6-tunnel.html](http://www.cisco.com/c/en/us/td/docs/ios/ipv6/configuration/guide/12_4t/ipv_12_4t_book/ip6-tunnel.html)

Cisco Manual Configuration Guidelines:

1. CCNA Exploration LAN Switching and Wireless: VLANs

2. Configuring Port Security, Cisco IOS Software Configuration Guide, Release 12.2S

3. CCNA Security 2.0 Instructor Lab Manual

4. CCNA Exploration 4.0.5.0 Routing Protocols and Concepts Student Lab Manual

5. Cisco Guide to Harden Cisco IOS Devices Contributed by Shashank Singh, Cisco TAC Engineer, Jun 03, 2014

6. Configuring RADIUS, Cisco IOS Security Configuration Guide, Release 12.2

7. Cisco IOS Software Configuration Guide for Cisco Aironet Access Points Cisco IOS Releases 12.4(10b) JA and 12.3(8) JEC

## APPENDIXES

### APPENDIX A: Web Server IIS 6.0 Security Checklist

<b>Security Specifications</b>	<b>Before</b>	<b>After</b>
<b>Machine Configuration File</b>		
Ensure DEBUG is turned off in WEB.CONFIG file	<b>X</b>	/
Ensure TRACE is set to false or disabled	<b>X</b>	/
Ensure unnecessary HTTP Modules are removed	<b>X</b>	/
<b>Secure Communication</b>		
Ensure HTTPS is enabled	<b>X</b>	/
Ensure Server Certificates are updated and issued by a trusted organization	<b>X</b>	<b>X</b>
Ensure Certificates have not withdrawn	<b>X</b>	<b>X</b>
Ensure communication happens through only port 80 or 443	<b>X</b>	/
Ensure that IPSec is formed in the network for secure communication	<b>X</b>	/
<b>Logging and Audit</b>		
Ensure Failed Logon Attempts are regularly inspected	<b>X</b>	/
<b>Server Accounts</b>		

Ensure anonymous logon is disabled	X	/
Ensure administrator account is properly hardened by strong password scheme	X	/
<b>System Configuration</b>		
Confirm ASP .NET state service is disabled	X	/
Ensure IIS is not installed on domain controller(x)	/	<b>X</b>
Confirm FTP and SMTP services are disabled(x)	/	/
Ensure IDS is installed in the network perimeter	X	/
<b>Server Updates</b>		
Ensure Windows Operating System is updated	X	/
Ensure .NET Framework is Updated	X	/

Referring to: <http://resources.infosecinstitute.com/securing-iis-server-checklists-2/#gref>

## **APPENDIX B: Windows Server 2008 Security Checklist**

Tasks	Before	After
<b>Preparation and Installation</b>		
Install Nmap	X	/
Using Nmap for penetration test (before)	X	/
Using Security Configuration Wizard to harden the server	X	/
Create new policy	X	/
<b>Role-Based Service Configuration</b>		
Selecting server roles	X	/
Selecting client features	X	/
Selecting Administration and Other option	X	/
Check error option in administration and other option	X	/
Select additional services	X	/
<b>Handling Unspecified Service</b>		

Do not change the startup mode of the services when unspecified services is found	X	/
Confirm service changes	X	/
<b>Network Security</b>		
View network security rules	X	/
<b>Registry Settings</b>		
Require SMB Security Signatures  -check both of the attributes	X	/
Outbound Authentication Methods  -check Domain Accounts	X	/
Outbound Authentication using Domain Accounts -check Windows NT 4.0 Service Pack 6a or later operating systems	X	/
Confirm registry settings in Registry  Setting Summary	X	/
<b>Audit Policy</b>		

Select Audit successful and unsuccessful activities in System Audit Policy	X	/
Check Audit Policy Summary	X	/
<b>Save Security Policy</b>		
Rename security policy	X	/
Apply now to the security policy	X	/
<b>Server Manager</b>		
Open server manager	X	/
Disabled guest account in users	X	/
<b>Local Security Policy</b>		
Open audit policies	X	/
Make sure all the audits have the success and failure checked and applied in the properties	X	/
<b>Windows Update</b>		
Open windows update	X	/
Change the setting of updates to install update automatically for every day	X	/

Check for updates	X	/
Select updates to be installed	X	/
Install updates	X	/
<b>Server Manager</b>		
Install BitLocker Drive Encryption	X	/
<b>Windows Firewall</b>		
Turn on Windows Firewall	/	/
<b>Disable Automatic Services</b>		
Open services by typing services.msc in run	X	/
Disable Print Spooler Properties	X	/
Disable Distributed Transaction Coordinator Properties	X	/
Disable KtmRm for Distributed Transaction Coordinator Properties	X	/
Change startup type from disable to automatic in Windows Error Reporting Service Properties and start the services	X	/

Change startup type to automatic in Secure Socket Tunneling Protocol Service Properties and start the services	X	/
Change startup type to automatic in Certificate Propagation Properties and start the services	X	/
Change startup type to automatic in Netlogon Properties and start the services	X	/
Change startup type to automatic in Special Administration Console Helper Properties	X	/
<b>Penetration Test (After)</b>		
Do penetration test using Nmap after all the steps	X	/

## **APPENDIX C: Linux Server Security Checklist**

Task	Before	After
<b>Software and Updates</b>		
Click Updates in Ubuntu Search Bar	X	/
Change from weekly to daily in automatically in automatically check for updates bar	X	/
Change from download automatically to download and install automatically in when there are security updates bar	X	/
Check for updates	X	/
<b>Terminal</b>		
Check password expiration with sudo chage -l (username)	X	/
Change password expiration with sudo chage -M (max days) -I (days inactive) -W (days for warning) (username)	X	/

Open gedit /etc/pam.d/common-password-change min length of the password	X	/
Install Nmap	X	
Scan ports with Nmap (Penetration test before)	X	/
Disable CUPS service (for printing)	X	/
Upgrade Bash	X	/
Disable IRQ balance (for optimization of power savings and performance)	X	/
Disable Bluetooth	X	/
Disable Wireless	X	/
Set security limits	X	/
Remove mysql	X	/
Scan ports with Nmap (Penetration test after)	X	/





