Network Security

Securing Network Equipment and Network Users' Environment

Bachelor's Thesis

Mbah Gipson Mbah

Degree Programme In Information Technology

Telecommunications Engineering

Accepted _____._____._____ _____

SAVONIA UNIVERSITY OF APPLIED SCIENCES

Degree programme

Information Technology

Author

Mbah Gipson Mbah

Title of project

Network Security- Securing Network Equipment And Network Users' Environment

Type of project	Date	pages
Final project	23 August 2010	90 + 4

Academic supervisor

Mr. Pekka Vedenpää, Network System Manager

Company

Savonia University of Applied Sciences, School of Engineering

Abstract

The purpose of this final year project is to research on new network security products and implementation techniques in order to enhance the current network security structure of Savonia University of Applied Sciences. This is very important because, it will avoid the university from suffering any major network attack associated with the present network security architecture. At the time this final project was approved, the university network security architecture was optimized but however, with immerging sophisticated threats and network attacks on daily basis there was need to keep researching on best means to protect the network from future attacks.

In this final project research, following security products were uncovered to produce best network security results when implemented in an integrated framework. The products are: Cisco network admission control, Cisco secure access control server, Cisco network assistant and Windows 2008 server. This thesis shows how to implement a robust network security architecture with the uncovered outstanding security products.

Savonia University of Applied Sciences has adopted using Cisco network assistant to securely manage Cisco network switches to minimize configuration errors. Cisco admission control and Windows 2008 server is up for implementation in the near future.

Keywords

Windows 2008 server, Cisco NAC, Cisco secure ACS, Cisco Network assistant

Confidentiality

Public

SAVONIA-AMMATTIKORKEAKOULU TEKNIIKKA KUOPIO

Koulutusohjelma

Tietotekniikan koulutusohjelma

Tekijä

Mbah Gipson Mbah

Työn nimi

Tietoverkon ja sen käyttäjäympäristön tietoturva

Työn laji	Päiväys	Sivumäärä
Insinöörityö	23.8.2010	90 + 4

Työn valvoja	Yrityksen yhdyshenkilö
Verkkoinsinööri Pekka Vedenpää	Verkkoinsinööri Pekka Vedenpää

Yritys

Savonia Ammattikorkeakoulu

Tiivistelmä

Insinöörityössäni tutkitaan uusien tietoturvaratkaisujen käyttöä Savonia-Amk:n tietoverkon tietoturvan parantamiseksi.Vaikka verkko onkin tietoturvapolitiikaltaan ja -suojauksiltaan hyvässä kunnossa, uusien, entistä varmempien menetelmien käyttöönotto on perusteltua tulevien uuden tyyppisten hyökkäysten varalta sekä myös käyttäjäympäristön toimivuuden turvaamiseksi.

Työssäni tutustaan Cisco´n tietoturvaratkaisuihin; Cisco Network Admission Control NAC, Cisco Secure Access Control Server ACS, sekä tietoverkon hallintatyökaluun Cisco Network Assistant.Työssä esitetään ratkaisumalli edellä mainituilla tuotteilla toteutettavaksi tietoverkossa.

Verkossamme Cisco Network Assistant on otettu käyttöön Cisco-verkkolaitteiden turvalliseen hallintaan, mahdollisten konfigurointivirheiden eliminoimiseksi ja verkon tilan entistä paremman seurannan mahdollistamiseksi.

Avainsanat

Windows 2008 server, Cisco NAC, Cisco secure ACS, Cisco Network assistant

Luottamuksellisuus

julkinen

Acknowledgments

The subject of this thesis was approved in April 2009. My intention was to complete the project and graduate in December 2009 but however, because of the car accident I suffered in May 2009 the thesis was delayed.

My immerse gratitude goes to Mr. Pekka Vedenpää, my supervisor who has been of great inspiration in the field of computer networks. Firstly, as an instructor on the Cisco certify network associate course and later as thesis supervisor in network security. Furthermore, I will also like to thank Ms Liisa Paatelainen, who has been of great assistance and support to me through out my time of studies and especially when I suffered two accidents. Lastly, my gratitude goes to my parents, girl friend Loveline suh and Christian friends in Kuopio and Cameroon who have upheld me in their prayers during the time of my studies.

Kuopio _____

…….

Table of Contents

Glossary

LAN	Local area network
DSL	Digital subscriber line
CIA	Confidentiality, integrity and availability
3DES	Data encryption standard
AES	Advanced encryption standard
RSA	Rivest, Shamir and Adleman
MD5	Message digest 5
SHA	Secure hash algorithm
DOS	Denial of service attack
UPS	Uninterruptible power supply
UDP	User datagram protocol)
TCP	Transmission control protocol
ID	Identification
VLANs	Virtual local area networks
DMZ	Demilitarized zone
MAC	Media access control
IP	Internet protocol
IPS	Intrusion prevention system
VPN	Virtual private network
WAN	Wide area network
DDOS	Distributed DOS
ICMP	Internet control message protocol
PDA	Personal digital assistance
CAM	Clean access manager
CAS	Clean access servers
DHCP	Domain host configuration protocol
DNS	Domain name server
ARP	Address resolution protocol
DAI	Dynamic ARP inspection
BPDU	Bridge protocol data unit

UDLD	Unidirectional link detection
STP	Spanning tree protocol
CDP	Cisco discovery protocol
IOS	Internetwork operating system
ACL	Access control list
EIGRP	Enhanced interior gateway routing protocol
OSPF	Open shortest path first
ACS	Access control server
AAA	Authentication, authorization and accounting
TACACS+	Terminal access controller access control
RADIUS	Remote authentication dial in user services
TFTP	Trivial file transport protocol
ISM	Internal service module
Gbps	Gigabits per second
Mbps	Megabits per second
NAT	Network address translation
PAT	Port address translation
SDM	Security device manager
Ntp	Network time protocol
EET	Eastern European time
EEDT	Eastern European summer time
NAC	Network admission control
eth0	Ethernet 0
eth1	Ethernet 1
SSL	Secure Sockets Layer
SW	Switch
L3	Layer 3
L2	Layer 2
CCA	Cisco clean access
HTML	Hypertext markup language
AD SSO	Active directory single sign-on
IPSEC VPN	IP security virtual private network
AV	Antivirus
AS	Anti -spyware

AD	Active directory
GPO	Group policy
OU	Organization unit
FQDN	Fully qualify domain name

1 Introduction

1.1 General

In today's world of ever increasing computer literacy, it will be almost impossible to live without using the computer to accomplish one task or the other. The computer has become part of our society and daily life. Without gainsaying, it will be interesting to note that some aspects of our daily lives that involve using the computer are as follows;

- Purchasing and conducting business transactions online
- Distance learning using the Internet
- Archiving and retrieval of health records in hospitals
- Archiving and retrieval of academic records in schools
- Archiving and retrieval of criminal records by the judiciary and law enforcement officials.

In conducting any of the above aspects that involves using the computer, it is very important to ensure that data in transit should not be accessed, modified or tampered by unauthorized persons. Unauthorized access to data may cause heavy financial damage to an individual or to a company.

A computer that shares an Internet connection through a local area network (LAN) is more vulnerable to network data attacks such as data theft and data manipulations compared to a standalone computer with a dedicated Internet connection such as a digital subscriber line (DSL). The reason for this is that, on a LAN someone can remotely access your local drive or sniff your data packet without physical access to your computer except some good security measures are put in place to prevent such attempt. With a standalone computer, someone must physically have access to the computer to access data stored on it. However, if the basic security requirement for every computer is not provided for on this computer, it is still possible to steal data from the computer remotely from the Internet. This brings into scene the subject of network security; that is, securing network equipment and network user's access which is the focus of this final year project.

The objective of this final year project is to research on new network security products and implementation techniques in order to enhance the current network security structure of Savonia University of Applied Sciences. This project covers how to implement Cisco's major security products such as Cisco NAC (network admission control), Cisco secure ACS (access control server) and Cisco Network assistant in the network to repel network attacks. Furthermore, Windows 2008 server with enhanced security features is used to manage and consolidate all network users' accounts. Cisco network assistant has been implemented in the network to minimize network switch configuration security holes that might expose the network to attacks. Cisco NAC will be implemented in the near future alongside upgrading Windows 2003 server to Windows 2008 server.

1.2 Attributes of Network security

The subject of network security has become increasingly important nowadays as network security experts face challenges to restrict unauthorized persons from accessing, stealing or tampering with network information. Network security is a mechanism of authentication, encryption and hashing geared at protecting network resources from unauthorized persons. This mechanism takes into account the corporate policy, such as who has access to what resources, and who has not. The following is a closer look at network security attributes:

- **Authentication**

  In accessing a network, a user provides username and password to proof acceptance to use the network. This is known as authentication. [1]

- **Confidentiality**

  When data travels across the network, it should be obscured to those who it not intended for. To achieve this, the data is encrypted symmetrically or asymmetrically. Symmetrical encryption uses shared sacred key to encrypt and decrypt data. A long and complex key renders a more secure encryption. 3DES (Data encryption standard) or AES (advanced encryption standard) algorithm could be used for symmetrical encryption. Asymmetrical encryption uses two separate keys, one for encryption and the other for decryption. The public key is used for data encryption and private key for data decryption. Asymmetrical encryption is reserved only for the authentication purpose because it demands a lot of computing power compare to it symmetric counterpart. An example of asymmetric encryption algorithm is RSA (Rivest, Shamir and Adleman). [3]

- **Integrity**

  When data is in transit through the network, the data should be void of any manipulation by intruders or hackers that may tamper the original nature of the information. Data integrity can be performed by hashing the data sent using MD5 (message digest 5) or SHA-1 or SHA- 2 (secure hash) algorithm. When a hash message arrive its destination, a hash of the data is computed and checked against hash sent by the source computer. If the two hashes match, data integrity has been maintained if not data is rejected for reason of modification in transit. With hashing enforce on data, it is difficult to modify data in transit without detection. SHA- 2 is the most secured and recommended because it is difficult to attend two messages that hash to same hash value. [4]

- **Availability**

  The organization network and services should always be available to authorize persons when ever needed. This means 24 hours of a day and 7 days a week; if not, these will cause tremendous lose of human productivity and financial lose to the company. Network availability should be accomplished such that the total down time percentage for the entire year should be less than 1%. Denial of service attack (DOS) could be launch to deny availability to network resources. DOS mitigation techniques should be put in place to thwart attackers. [2]

1.3 Network Threats

Network threats are skilled individuals who are willing to exploit the security weakness of a network in order to inflict costly damage. They can accomplish this by using various attack tools in the market such as **Netcat** or self written scripts. These attackers have various names depending on what they do as shown in the following list.

1. **Hacker** – nowadays, this is a person who attempts to get unauthorized access to network resources with evil intentions. But however, in early days a hacker was known to be a good computer programmer.
2. **Cracker or Blackhat** – This is a person who tries to gain unauthorized access to network resources for malicious intentions.
3. **Spammer** – individual who sends bulk of unsolicited emails of which may content a virus in an attachment intended harm your computer or to steal information from your computer and forward by email to the spammer.
4. **Phishers** – This is someone who by email or other means trick individuals into getting sensitive information such as credit card number or password. They usually disguise as trusted persons. [5]

1.4 Mitigating Physical Threats

Physical threats are also very important in security implementation such that if overlooked, they pose a potential weakness to the network. The following is a list of physical threats that should be considered in network security deployment.

1. Hardware threats can be mitigated by securing sensitive endpoint devices in lock rooms where only authorize persons can have access. Use security cameras to monitor access to devices.
2. Environmental threats such as high temperatures can be avoided by installing air conditioning systems in server rooms and sensor alarms to indicate high temperature when cooling system fails. Other end devices should be installed where there is good air flow to keep devices operating.
3. Electrical threats can be mitigated by installing UPS (uninterruptible power supply) to briefly keep the computer running when power is off. This will necessitate a proper shutdown of computer without crashing the hard drive. Moreover, in addition to UPS, install a standby generator to provide instant power if electrical power is permanently out for some reason. This will assure an uninterruptible business operation of the company. Redundant power supply for critical devices like servers is needed to keep network services running when the primary power fails.
4. Maintenance threat mitigation involves using electrostatic discharge wrist strap band in maintenance procedure, labeling critical cables and stock plenty of spare parts. [5]

1.5 Network Attacks

There are four groups of network attacks namely:

1. Reconnaissance attack
2. Access attack
3. Denial of service attack
4. Malicious code attack

Reconnaissance Attack

This attack type is also known as information gathering. In this process, the attacker uses various tools to gain valuable information about the network and its vulnerabilities. After information gathering such username and password, the attacker can then launch an audacious attack and if successful, havoc on the network is created with possible theft of data. 'Network engineer tools' by Solarwinds is a good kit for reconnaissance attack. It has all necessary tools for reconnaissance attack. Some tools used in reconnaissance attack involve the following:

- Packet sniffers - for capturing and analyzing packets
- Ping sweep - for indentifying running computers on the network
- Port scan - to identify open UDP (user datagram protocol) or TCP (transmission control protocol) ports on target computer
- Internet information queries using **WHOIS** to get information about domain ownership. [3]

Access Attack

In access attack, the attacker uses tools such like hacks tools and scripts to gain access to computers, servers, routers or resources that he is not allowed access. He does this by cracking the user id and password. An Access attack is categorized as password attack, trust exploitation, port redirection or man in the middle attack.

- **Password attack**: this attack can be achieved by using packet sniffers. In a situation where user id and password is transmitted in clear text for example Telnet, the attacker will learn the user ID and password which he could use subsequently to gain unauthorized access to network device and cause havoc. Alternatively, attacker can use tools brute-force attack tools like **Lophtcracker** or **Cain** to gain unauthorized access. Theses tools repeatedly try to login the attacker using different words from dictionary or combination of words and numbers. A long password of at least 8 characters including uppercase, lowercase and numbers, for example FAMIpark1975 is a good way to mitigate brute-force attack. Furthermore, password attacks can be accomplished using stealth **keyloggers** or Trojan horses that steal username and password and make available to attacker. Mitigate stealth keyloggers by having the latest antivirus install on computer.
- **Trust exploitation**: this is accomplished when a host outside the firewall that is trusted by a host behind the firewall is compromised. When the outside host is

compromised, the attacker then uses the trust association to launch attacks on the inside host. To mitigate trust exploitation, private VLANs should be implemented in the DMZ (demilitarized zone). Furthermore, trust between outside host and host behind the firewall should be limited to specific protocol, ports and authenticated by IP address and MAC (media access control)

- **Port Redirection**: This is a type of trust exploitation in which in a compromised host, for example outside the firewall is used to redirect traffic from an external host on the Internet to an internal host behind the firewall. This would not have been possible for an outside host to communicate directly with host behind the firewall if the DMZ host was not compromised. When a DMZ host is compromised, **Netcat** is example software that an attacker can install to redirect traffic to an internal host. However, to mitigate port redirection, host based IPS (intrusion prevention system) must be install on a computer and configure to prevent and log intrusion. Example of host based IPS is F-secure client security 8.0.
- **Man-in-the –middle attack**: In 'man-in-the middle' attack, the attacker position himself between communication devices, for example routers. With a packet sniffer, attacker can have access to lot of information such as username, password and content of transmitted payload if transmitted data is not encrypted. Man- in-the middle attack can be greatly mitigated by using secure shell for managing network devices like switches and routers, encrypting all wireless traffic and VPN (virtual private network) for WAN connections. [3]

Denial of Service (Dos) attack

Dos attack is an attack type that overwhelms the resources of targeted device, for example a router, such that, the router can not render it's require services. DOS attack has various forms as follows:

- **Ping of death**: this form of DOS attack modifies the IP portion of a ping packet header which normally falls between 64-84 bytes to a value of 65535 bytes. This falsely indicates that the IP packet has more data than it actually content. Any computer that receives such a packet will eventually crash. But however, modern computers are resilient to this attack.
- **Syn flood**: In TCP communication, the must be a three- way –handshake to effect any communication. An attacking computer sends multiple TCP Syn request, target computer for example a server response with Syn Ack response but the attacking computer never response with the final acknowledgment to complete the three- way-handshake. This deliberate act by the attacker computer causes the server computer to run out of resources to serve legitimate users.
- **Email bomb**: it is an attack type where by large quantity of emails are sent to persons with aim to exhaust mailbox capacity or overwhelm the mail server capacity where the mail boxes are hosted.
- **DDOS** (distributed DOS) attack: DDOS is a more advanced form of DOS attack. The aim is to saturate communication links and target hosts with illegitimate data. This will cause links or target hosts to drop legitimate data or request due to lack of resources. In DDOS you have the following characters:
    - Client – computer or person who launches attack.

- Handler – compromised computer running attacker programs. A handler can control many agents (zombes)
- Agent - compromised computer running attacker programs and is responsible for generating large amount of traffic towards target computer.

It is important to mention here that, in recent years, 'Botnet' refers to a jargon used to describe a collection of malicious software used to launch DDOS attacks. Some examples of DDOS attacks include: Smurf attack, Stacheldraht, Rustock and MyDoom. DOS and DDOS attacks can be mitigated by implementing anti-spoof and anti-DOS access control list. In addition, the amount of ICMP traffic allowed in a network should be limited since ICMP is used only for management purpose. [*3*][6]

Malicious Code Attack

This is an attack on a computer either by a virus, worm or Trojan horse. The preceding paragraphs look at viruses, worms and Trojan horses.

A worm does not require human intervention to spread from infected an infected host to a new host. When a worm attacks a computer, it copies itself into the computer memory and then launches attack to another vulnerable host. Worms can contribute to slow network response because they consume network bandwidth. Apply necessary operating system updates, patches and host based IPS to mitigate worms.

A virus unlike a worm, attaches itself to a file. It requires human intervention to spread from one host to another. Its payload may include freezing the computer (blue screen) or damaging your file. Mitigation method involves using up to date antivirus or Internet security program.

A Trojan horse masquerade like a legitimate program, for example a download link with title 'Microsoft update patches windows 7' .when link is clicked by computer user to update operating system , the Trojan horse releases its payload which could be formatting the hard disk or erasing the boot partition of the computer. Trojan horse could also be bundle downloaded from the Internet. Download software only from reliable sources such as software company website. Most Internet security programs such as **F-secure, AVG** are a good starting point to mitigate Trojan horse attacks on your computer. These programs protect against most forms of malwares and spywares. Microsoft malware starter kit is free and serves as first aid for your computer. [7]

2 Securing Network Equipment

A Network Switch, Router, firewall and Network based IPS are some examples of network equipments widely used to provide secure network services to end devices such as computers, laptops and PDAs (personal digital assistance). This section examines how a network switch can be protected from attacks that render the network unusable.

2.1 Network Switch

In most network environments, there exist more network switches than any other network equipment. This is because most of the network operations involve switching rather than routing, except in inter-vlan routing or Internet access that routing is required. The routing can be performed by a layer 3 switch or dedicated router. A switch connects network end devices for network access and because of the enormous switching function performed by a switch, a switch stands expose to a lot attacks. Securing a switch is therefore a must against attacks that are launched from within the enterprise by an intruder or angry employee.

2.2 Layer 2 Network Attacks

1. **Mac address flooding**: This is an attack where the intruder exhausts the capacity of CAM (content address memory) table such that traffic from a legitimate host is flooded out all ports of the switch since its MAC address is not found in the CAM. With attacker connected to one of the switch ports, he has access to unauthorized data. **SMAC 2.0** is example software that can be used to overwhelm the CAM. [6]

   Mitigation: In a database environment where all network clients send and retrieve data from the database server, the MAC address of the server could be statically configure in the CAM to avoid aging out. This makes it difficult for the attacker to flood the CAM causing frames meant for the server to be flooded out on all ports. On Cisco catalyst switch connected to the server enter this command syntax;

   ```
   Switch(config)#set cam static MAC-address server-port
   ```

   Where MAC-address is MAC of server and server-port is port on switch associated with server.

2. **Vlan hopping attack**: In vlan hopping attack, the attacker belonging to a different vlan double tag the Vlan ID of his attack packet with the vlan ID of his target host. In this manner the attacker can send and receive packets from different VLANs. This is easily accomplished by attackers if the switch default configurations status such as port dynamic status, port on and default Vlan 1 is used for unused ports.

   Mitigation: In mitigating Vlan hopping the following instruction must be followed.

   - Shutdown all unused ports
   - Move all unused ports to a different vlan, for example vlan 11
   - Configure all non-trunk port to access mode only

   Another form of VLAN attack is that of DMZ VLAN. Here, the attack is intended for hosts within the same VLAN. This is very eminent in public service segment or DMZ of a network where web server, mail server and FTP server are hosted. A possible compromise of the web server can lead to the compromise of the other servers. [6]

   Mitigation: Implement **private VLAN** for Cisco catalyst 6500, 4500 and 3650 series switches and **protected port** for Cisco catalyst 2960 series switches. Ports configure as protected port can not pass traffic between each other except through Layer 3 device

even though they belong to same VLAN and subnet. Here is example configuration commands syntax for protected port.

```
Switch(config)# int fa0/2
Switch(config-if)# switchport protected
Switch(config-if)#end
```

Implementing private VLAN, you have to choose to implement isolated or community secondary VLAN. A primary VLAN acts as a gateway to the isolated or community VLAN. Ports in isolated VLAN can not communicate amongst themselves except with the primary VLAN (promiscuous port). Host in community can only commune with host in same community and primary VLAN. The following steps illustrate how to implement private VLAN with isolated port.

- Change switch VTP (virtual trunking protocol) mode to transparent
- Create primary VLAN, for example vlan 50 and assign dmz_farm as name
- Assign IP address the primary VLAN
- Define the isolated VLAN, for example VLAN 51 and associate it with VLAN 50. Example commands syntax:

```
Switch(config)# vlan 51
Switch(config-vlan)#private vlan isolated
Switch(config-vlan)#end
Switch(config)#vlan 50
Switch(config-vlan)#private-vlan primary
Switch(config-vlan)#private-vlan association 51
```

- Assign switch ports to isolated VLAN. Example commands syntax:

```
Switch(config)#int fa0/2
Switch(config-if)#switchport private-vlan host
association 50,51
Switch(config-if)# end
```

Furthermore, by creating virtual interfaces for VLANs and assigning IP addresses, it is possible to used VLAN access control list to limit traffic flow from one VLAN to the other. [6]

3. **DHCP starvation attack**: This is an attack on the DHCP server where the attacker spoof MAC addresses, that is, attacker constantly changes MAC addresses while requesting IP addresses from the DHCP server. This causes the DHCP server to run out of IP addresses to lease to legitimate users. This leads to denial of service, where legitimate users can not access the network. Gobbler is example DHCP attack tool. Mitigate this attack by implementing port security on all network switches such as limiting the allowable number of MAC addresses on switch port. [6]

4. **DHCP spoofing**: In this type of attack, the attacker introduces a rogue DHCP server possibly in the same segment with the legitimate DHCP server. When a network host makes a DHCP request, the rogue server response with an IP address, DNS address and default gateway. With this information, the host will forward it data to the wrong destination thinking that it obtained network routing information from

legitimate DHCP server. The attacker will now harvest a lot of information from the network which he was not authorized to access. The attacker can later unplug his rogue server restoring services to the legitimate DHCP server, and the organization will not likely know information has been stolen. DHCP spoofing is also regarded as man-in-the- middle attack.

Mitigation: DHCP snooping is a mechanism to mitigate DHCP spoofing. In this mechanism, ports which network host listens to DHCP replies must be configure as trusted ports while other ports are untrusted. With this in place, a rogue server connected to any arbitrary port that is not trusted can not send DHCP replies. Steps to implement DHCP snooping:

1. Enable snooping globally – `command syntax :{ switch(config)#ip dhcp snooping}`
2. Configure trunk ports and DCHP server connected port with ip dhcp snooping trust - `command syntax :{ {switch(config)#ip dhcp snooping trust}`
3. Limit the number of DHCP request rate on ports on access layer switches. `Command syntax- {switch(config-if)#ip dhcp snooping limit rate 20}`
4. Configure VLANs that will used DHCP snooping. `Command syntax - {switch(config)#ip dhcp snooping vlan 20,50}` [6]

5. **ARP spoofing**: In this attack type, a host for example A, intending to communicate with another host B, initiates an ARP request to know the MAC address of host B. At first host B responses to the ARP request with its MAC address. Host A updates its ARP cache with the received MAC. Later on, a rogue device sends and unsolicited ARP reply, binding its MAC address with the IP address of host B. This cause host A to update its ARP cache again with a false MAC. All packets destined to host B will be diverted to the rogue device as soon as host A updates its ARP cache. [6]

   Mitigation: Dynamic ARP inspection is a mechanism to curb ARP spoofing. It works by intercepting ARP packets from untrusted interfaces and verifying to see if its MAC address matches its IP address. If the IP-to- MAC address does not match, the packet is dropped and a log generated. Steps for configuring ARP inspection:

   1. Enable DAI (Dynamic ARP inspection) on a VLAN or range of VLANs - `command syntax :{switch(config)#ip arp inspection vlan 1}`
   2. Enable DAI on an interface and set it as trust - `command syntax: {switch(config-if)#ip arp inspection trust}`
   3. Configure DAI to drop ARP packets when IP address is invalid - `command syntax: {switch(config-if)#ip arp inspection validate IP}`

6. **Spanning tree attack**: This is an attack aim at damaging the spanning tree protocol which prevents data loops occurring in a switch network. In this attack, the attacker disrupts the election of the root bridge by introducing a rogue switch in the network.

This rogue switch sends a fault BPDU (bridge protocol data unit) packet with lower priority ID than that of the legitimate root bridge. This causes all switches in the network to elect the rogue switch as default Root Bridge and hence forward packets through it. The outcome of this will be poor performance or absolute halt of network services.

Loop guard is a spanning tree protection mechanism aim at protecting spanning tree configuration from a rogue switch. Loop guard should only be configured on Root and Alternative ports on access switches.

UDLD (Unidirectional link detection) is another protection mechanism against STP (spanning tree protocol) loops caused by link failure. The outcome of this link failure produces a unidirectional communication, a possible source of loop. This is very common in fiber optics connection when one of the two pair link is damaged. When UDLD detects unidirectional communication on an interface, it shuts down the link to avoid a loop. [6]

Mitigation: In mitigation spanning tree attacks, BPDU guards, BPDU filters, Root guard, loop guard and UDLD should be configured on switch ports connected to end devices. These are ports configured with portfast status and should not receive BPDU. If BPDU guard and filter are configured globally for all interfaces, it should later be disabled on trunks ports. Configuration commands syntax:

- Globally - `{switch(config)#spanning-tree bpduguard default}`
- Globally - `{switch(config)#spanning-tree portfast bpdufilter default}`
- Interface mode on access layer switch - `{switch(config-if)#spanning-tree guard root}`
- Interface mode on access layer switch - `{switch(config-if)#spanning-tree guard loop}`
- Interface mode on fiber link - `{switch(config-if)#udld port}`

7. **Exploitation of CDP** (Cisco discovery protocol) vulnerability: CDP is Cisco proprietary protocol use to share information amongst Cisco inter-connected devices. The information shared include IP address of connected interfaces, IOS version and device platform. This share information is sent in clear text and can easily be captured by packet sniffers for reconnaissance attack. Information gathering aids in major attacks against the network. Disable CDP if not needed to map adjacent network devices. Command syntax: [6]

    - Interface mode - `{switch(config-if)#no cdp enable}`

3 Network Switch Fundamental Defense Configurations

Every switch or router deploy in a network needs first aid defense to prohibit unauthorized persons from getting access into the IOS of the device and tampering with the configuration.

The following steps outline first aid defense that is also applicable to routers, firewalls and IPS. [9][15]

Step 1- configure switch for secure shell management. Install Putty software on management computer to manage switch. Example configuration commands syntax:

```
{Switch(config)# ip domain-name savateku.com}
{Switch(config)# crypto key generate rsa generate-key module
1024}
{Switch(config)# ip ssh timeout 120}
{Switch(config)#ip ssh authentication-retries 4}
{Switch(config-line)# transport input ssh}
{Switch(config-line)#end }
```

Step 2 – Secure the console port with a password. A password with minimum of 8 characters is recommended. It includes uppercase and lowercase letters and numbers. Example configuration commands syntax :

```
{switch(config)#service password encryption}
{switch(config)#line con 0}
{switch(config-line)#password Teku4girlsonly}
{switch(config-line)#login}
```

Step 3 - Secure enable mode. Example configuration command syntax:

```
{switch(config)#enable secret Teku4boysonly}
```

Step 4 - Secure **vty** lines for remote administering of switch. Used only secure shell for **vty** connection since Telnet is not secure. Example configuration commands syntax:

```
{switch(config)#line vty 0 15}
{switch(config-line)#password Teku4boysonly}
{switch(config-line)#login}
{switch(config)#transport input ssh}
```

Step 5 - Secure auxillary port use for remote configuration. Example configuration commands syntax:

```
{switch(config)#line  aux 0}
{switch(config-line)#password Teku4boysonly}
{switch(config-line)#login}
```

Step 6 - Set minimum password length. Example configuration command syntax

```
{switch(config)#security password min-length 8}
```

Step 7 - Create secure local user account on switch with MD5 encryption. Example configuration command syntax:

```
{switch(config)#username Gipson secret 5 Teku4boysonly}
```

Step 8 - Secure the **ROMMON** (read only memory monitor). Securing the **ROMMON** is a good measure to ensure that your network configuration remain intact should in case an attacker breaks the physical security of your device. With **ROMMON** security in place an attacker will not be able to undo the device password and alter network configurations. **ROMMON** configuration command syntax:

```
{switch(config)#no service password-recovery}
```

With this command in place, a valid IOS image and startup configuration file is required to restore the switch if switch password is forgotten.

Step 9 - Configure authentication login failure limit. When limit is exceeded, a sys log message is generated. Example configuration command syntax to limit login failure rate to 5:

```
{switch(config)#security authentication failure rate 5 log}
```

Step 10 - Mitigate dictionary attack by inserting a time delay after 5 unsuccessful login attempts within a define period of 60 seconds. Example command syntax:

```
{switch(config)#login block-for 120 attempts 5 within 60}
```

Step 11 - Configure login quiet mode to allow legitimate network administrator access to switch during blocking period when switch experiences that the limit for login failure is reached. Without quiet mode configure, legitimate network administrator will also be blocked from accessing switch IOS during the block period. To configure quiet mode, first create access control list for the management subnet and then apply ACL to the switch. Example configuration command syntax:

```
{switch(config)#login quiet-mode access-class permitIP}
```

(permitIP should be the name of the access list created for the management subnet).

Step 12 - Configure a login banner message which informs attacker that he will be prosecuted for unauthorized access to network switch or router. Example configuration command syntax:

```
{switch(config)#banner motd #unathorized access is not
allowed and will be prosecuted! #}
```

Step 13 – Install and configure Syslog server. The Syslog server serves as a repository for event logs send by switches and routers in the network. The log messages may just be informational or report of critical events on switch or router such as interface down or a possible attack. These log messages help in network troubleshooting. Enter the following commands syntax on every device that should send syslog messages. The IP address 172.16.33.15 is the address of the syslog server running the Solarwinds Kiwi Syslog server software.

```
{Switch(config)# logging 172.16.33.15}
{Switch(config)# logging trap informational}
{Switch(config)# logging source-interface loopback 0}
{Switch(config)# logging rate-limit 30 except warnings}
{Switch(config)# logging on}
{Switch(config)# end}
```

Step 14 – Configuring routing protocol authentication. In a large network with multiple routers or layer 3 switches, configuring routing protocol authentication is important because it protects the network from rogue devices that may injection false routes into the routing table. This may lead to failure in proper network routing and possibly attacker having access to sensitive information. The following is example configuration commands syntax with EIGRP and OSPF protocols.

- In EIGRP-

```
{Router(config)#key-chain EIGRP_key}
{Router(config-keychain)#key 1}
{Router(config-keychain-key)#key-string Cisco123}
{Router(config-keychain-key)#end}
{Router(config)# int s0/1/0}
```

```
{Router(config-if)#ip authentication mod eigrp 1md5}
{Router(config-if)#ip authentication key-chain eigrp 1
EIGRP_key}
```

(Int s0/1/0 is an arbitrary interface that may differ on different router or switch platforms).

- In OSPF-

```
{Router(config)#int s0/1/0}
{Router(config-if)#ip ospf message-digest-key 1 md5
cisco123}
{Router(config-if)#ip ospf authentication message digest}
{Router(config-if)#exit}
{Router(config)#router ospf 5}
{Router(config-router)#router ospf 5}
{Router(config-router)# area 0 authentication message
digest}
```

4 Device Management with Cisco Secure Access for Windows

In a network environment where there are tens of network devices such as switches, VPN concentrators, Routers and Firewalls for management, it will be a daunting task for an administrator to move from one device to another to change access password if it has been compromised. Furthermore, in a network with multiple administrators having different privilege level accounts, it would be a challenging task to create all the privilege accounts

on individual devices. If for some reason, one of these accounts has been compromised, the password has to be changed on all devices throughout the network.

Cisco secure ACS (access control server) for windows provides a secure and centralized management of network devices from one location. With Cisco secure ACS, the passwords for all administrators can be modified from a single location and then push for enforcement on the actual devices. With Cisco secure ACS one password can be used to access all devices. [10]

4.1 Preparing Devices to Use Cisco Secure ACS

In this section, Cisco secure ACS would be the AAA (authentication, authorization and accounting) server. Steps involve in preparing device for Cisco secure ACS are as follows:

1. Install Cisco secure access server on a computer running windows 2003 or 2008 server operating system. Have the computer connected to the network and can be accessed via IP address from any network device.
2. On every device that would be accessed by authentication through Cisco secure ACS, the commands that would be outlined later must be executed, the commands take in to account two AAA server for redundancy. When these commands have been executed, access to Aux, Console and Vty lines would be controlled by Cisco secure ACS. These commands take into consideration that, if some reason, the AAA server is not available, access to any device would be granted using the 'enable' password. This prevents an administrator from being denied access to a device because the AAA server is not available. To provide some constant availability of the AAA server, two AAA servers can be deployed to ensure that if one is unavailable, the other is available to authenticate users.
   TACACS+ (Terminal access controller access control) protocol will be used as the main protocol for communication between AAA server and controlled network devices. TACACS+ Cisco proprietary protocol is preferred over RADIUS (remote authentication dial in user services) open standard protocol because of inherent security features that RADIUS does not support some of which include encrypting password and data payload. TACACS+ is suited for an environment where there are only Cisco network devices. Example configuration commands syntax:
   - Authentication commands-
     ```
     {Router (config)# aaa new-model}
     {Router (config)# aaa authentication login default
     group tacacs+ enable}
     {Router (config)# aaa authentication enable default
     group tacacs+ enable}
     {Router (config)# tacacs-server host 172.16.1.2
     key Teku4girls}
     {Router (config)# tacacs-server host 172.16.1.3
     key Teku4girls}
     ```
   - Authorization command syntax (what login user is allowed to do). This is a continuation of authentication commands.
     ```
     {Router (config)# aaa authorization exec default
     group  tacacs+ enable}
     ```
   - Accounting command syntax (what an authorized user did during login period). This is a continuation of authorization.
     ```
     {Router (config)# aaa accounting exec default
     ```

```
start-stop group tacacs+}
```

3. On computer running Cisco secure ACS for windows, launch the program. Figure 1 shows picture of running Cisco secure ACS for windows. Within ACS window, first create an admin account on the server by clicking on the 'Administrator control' tab on the left navigation pane. Next, click 'Add administrator' button. Within the 'Add administrator' window, fill in the necessary information; click 'grant all' button to grant all privileges to the admin. Finally click 'submit' to create account. Furthermore, within 'Administrator control' window, allow default setting for 'Access policy' because AAA server would be access locally. Click the 'Session policy' button and uncheck 'Allow automatic login'; click submit. Allow default settings for 'Audit policy'.

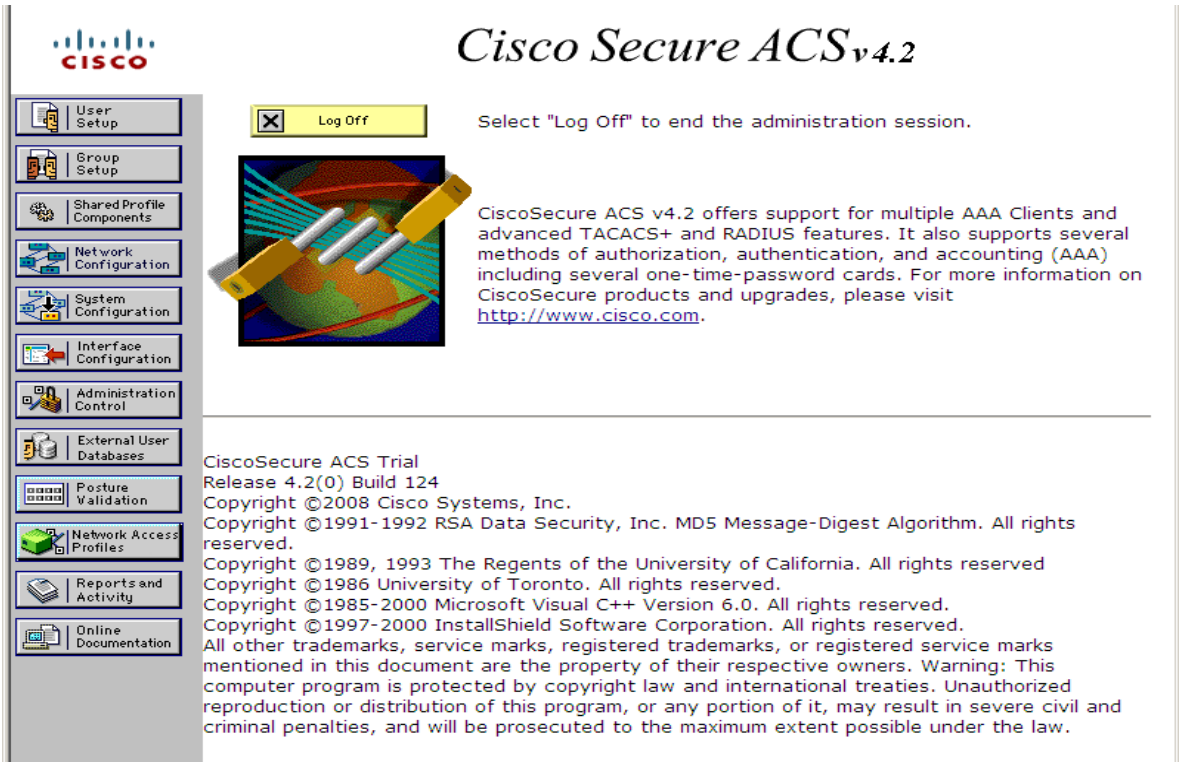


Figure 1.Cisco secure access for windows home page

4. Adding AAA- clients/ servers; that is, all devices that would be monitored by AAA-server. Instruction step:

   Step 1- From within the ACS server home page, click on 'Network configuration' tab. Within the 'Network configuration' window, Under the AAA client section click 'Add entry' and fill the host name, IP address and TACACS+ for authentication protocol. The secret key is same for all devices, that is, 'Teku4girls'. Check 'log update/watchdog packets from client AAA client'. Figure 2 shows ACS form for adding AAA client devices. Since two AAA servers were configured on router for redundancy purpose, within the AAA server section, click 'Add entry' button to add the second AAA server. Enter the hostname, IP address, secret key (Teku4girls) and Cisco secure ACS for AAA server type; also check 'log update/watchdog packets from this remote AAA server'.

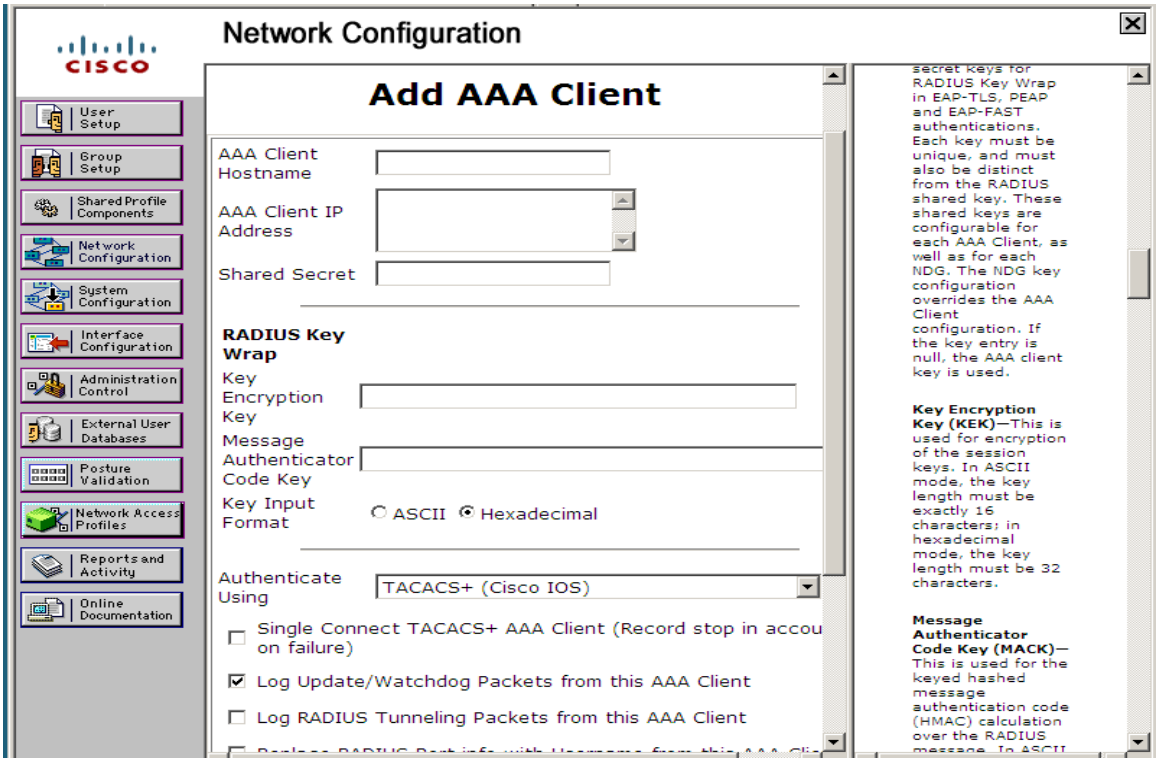


Figure 2. Form for adding AAA client ACS

4.2 Adding Administrative users to Cisco Secure ACS

The follow steps illustrate how to add administrative accounts to manage switches on Cisco secure ACS.

Step 1 – First, configure groups by clicking on the 'Group setup' tab in AAA server home page in Figure 1, rename an existing group with appropriate name. For example rename group 1 as administrator and group 2 as helpdesk. Submit the configuration.

Step 2- Select the administrator group and click on 'Editor Settings'. At the top of administrator group window, select TACACS+ from the 'jump to drop down' menu. Scroll down to the 'shell command authorization set' feature area and accept default option. Select

'per group command authorization option', and under 'Unmatched Cisco IOS commands' select 'Permit' (this allow an administrator to use all IOS commands).

Step 3 - For the helpdesk group, configuration steps are the same as with the administrator group except for the fact that, with 'Unmatched Cisco IOS commands' select 'Deny' instead of 'Permit '. Next, check the 'command check box' and type in the commands that are allowed for the helpdesk group. Check 'Permit unmatched argument' to allow commands with arguments to be used; for example 'show IP route'. Finally click 'submit' to effect the configuration.

Step 4 - Create users' account using the 'User setup' tab as shown in Figure 1. Within the user setup window, type user's name and click 'Add/Edit' button to add a new user. Go to Add/Edit new user window, allow default settings as shown in Figure 3. Type the password 'Teku4girls' and associate user with the administrator group. This will cause the user to adopt admin privileges.

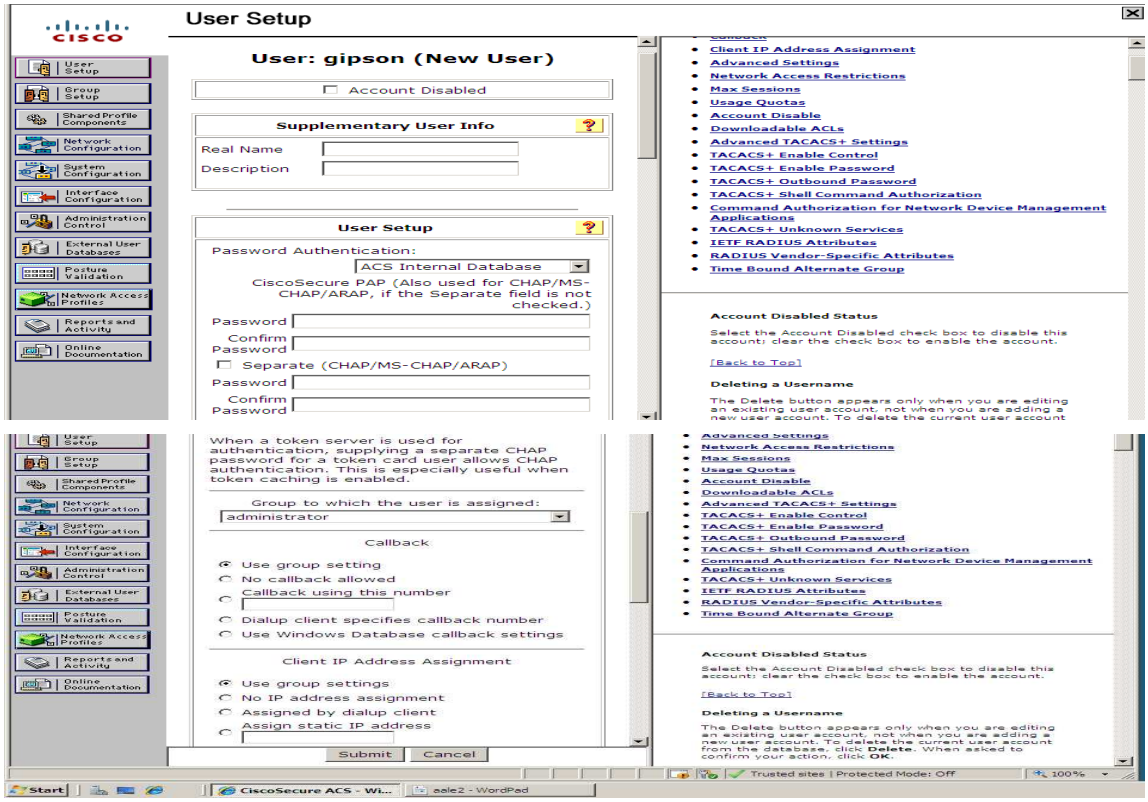


Figure 3.ACS form for creating administrative accounts

To configure auditing, click the 'Report and activity' tab on ACS server home page as shown in Figure 1. Within this window, click on 'TACACS+ accounting' →TACACS+ accounting active. Csv file to view reports generated by ACS server. These reports are administrative activities on network devices. Figure 4 shows accounting report activity window.

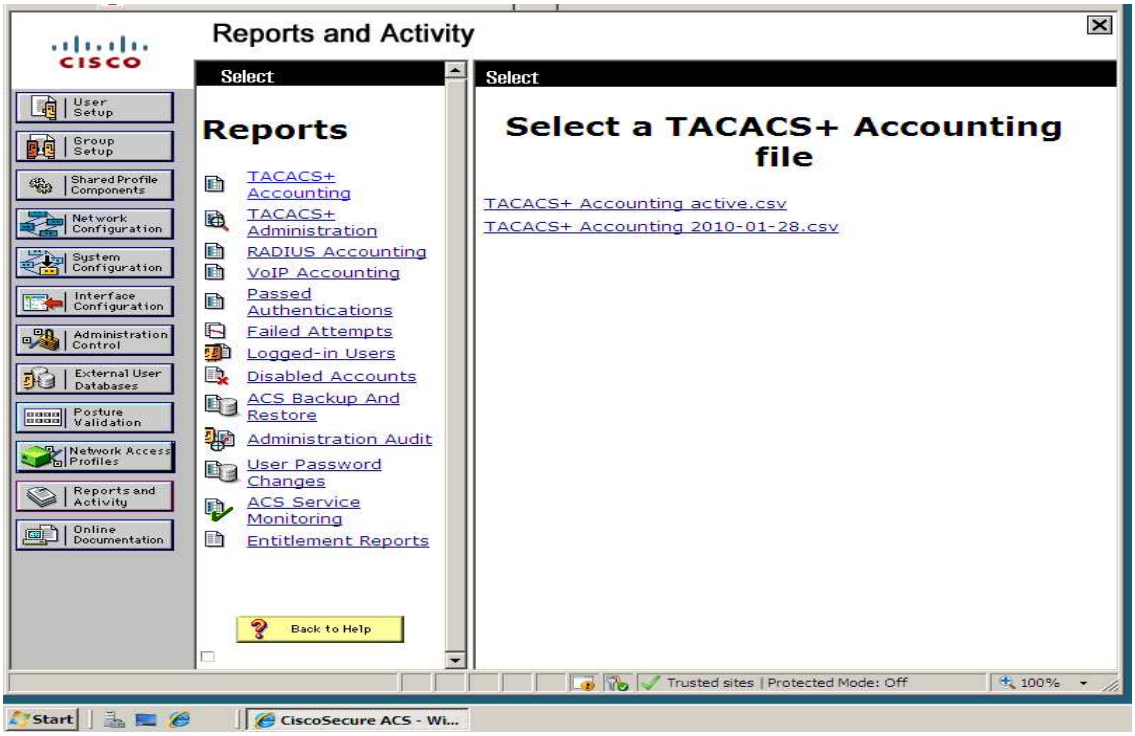


Figure 4.ACS report accounting window

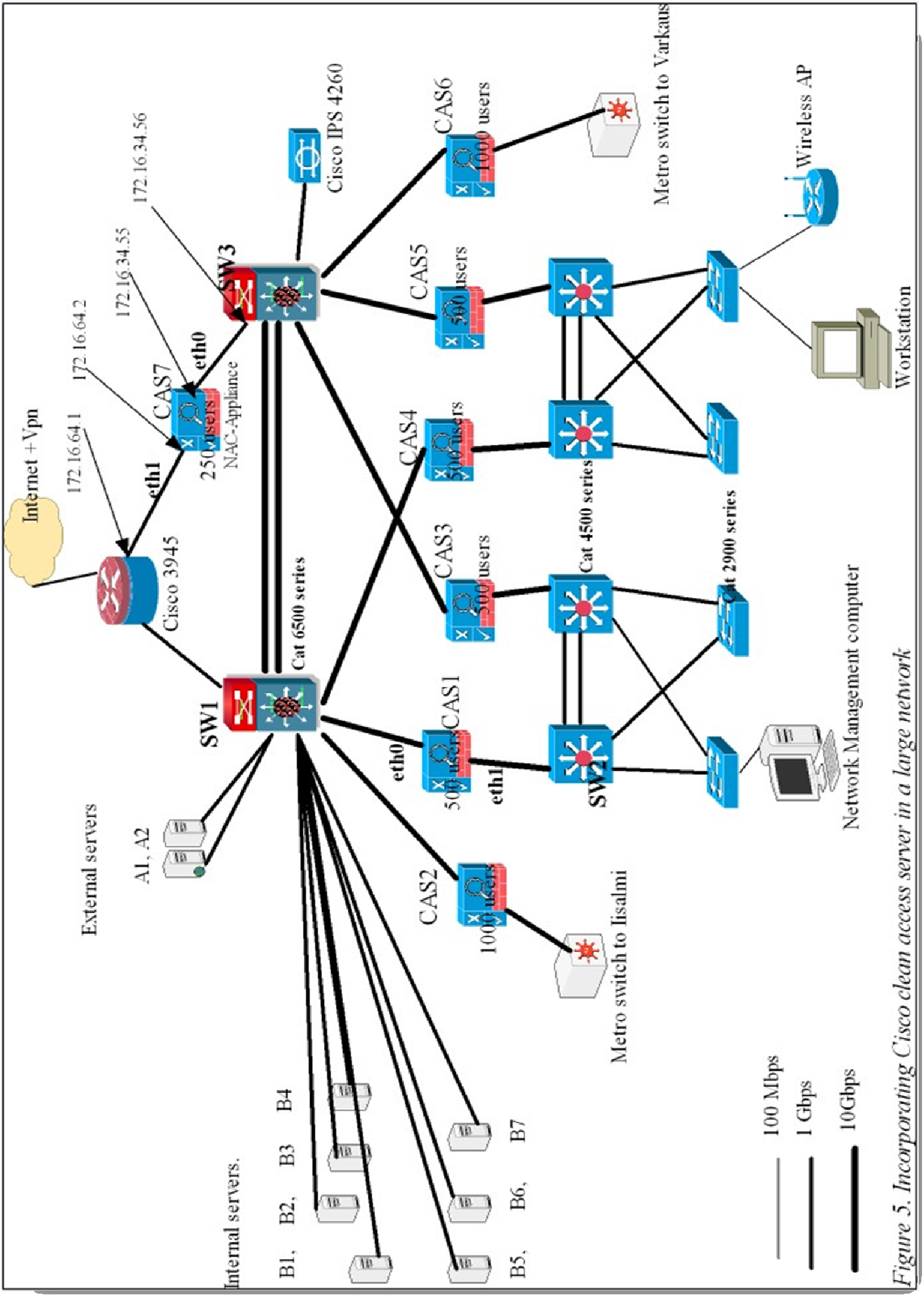


Figure 5. Incorporating Cisco clean access server in a large network

5 Network Security Design Model

Table 1. Internal servers role description

CODE	SERVER DESCRIPTION	IP ADDRESS
B1	Windows 2008 server (AD service and DNS)	172.16.33.10
B2	CAM (clean access manager)	172.16.33.2
B3	Cisco secure access server	172.16.33.4
B4	TFTP server	172.16.33.5
B5	Syslog server	172.16.33.3
B6	Database server	172.16.33.6
B7	Others	172.16.33.7

5.1 Cisco 3945 Firewall Router

The Cisco 3945 integrated service router featuring in Figure 5 is upgraded with Cisco recommended components to boost its performance to support medium and large business enterprises. This device supports 3 Gigabits Ethernet ports by default. Description of ports connection is shown in Table 1.

Cisco ISM (internal service module) is installed as upgrade component to push the overall throughput of the firewall-router to aggregate value of 4 Gbps towards route processor and 2 Gbps towards other slot modules. The default throughput is 150 Mbps without hardware upgrade. The Cisco 3945 also contains and in build IPS module which will be configured later. [11, 12]

Table 2. Cisco 3945 router ports connection description

GigabitEthernet 0/0	Connected to Internet
GigabitEthernet 0/1	Connected to internal network
GigabitEthernet 0/2	Connected to clean access server

In configuring the Cisco 3945 firewall, the following points are considered:

- Static NAT (network address translation) fort the Web server, mail server and VPN server
- Dynamic NAT pool for internal host to access the Internet
- PAT (port address translation) if dynamic NAT runs out of addresses
- DMZ servers can not access internal hosts except for a specific assigned internal server with a protocol port number.
- External host on the Internet cannot access internal network hosts except hosts on the DMZ.
- Internal hosts can access external hosts on the Internet and DMZ hosts.
- DMZ servers are connected by implementing private VLAN to mitigate VLAN hopping attacks.

5.2 Configuring Cisco 3945 Router

Cisco configuration professional is proprietary network management software which is used to configure Cisco 3945 router. Cisco 2800 series router is used to simulate Cisco 3945 router. For this reason, the following interfaces Gig0/0, Gig0/1 and Gig0/2 found on Cisco 3945 will be replaced by Serial0/1/0, Fastethernet0/1 and Fastethernet0/0 respectively. The following steps outline the procedure to configure Cisco 3945: [13, 14]

1. Enter the following command through console connection to prepare the Cisco 3945 for management with Cisco configuration professional.

```
{FW_router(config)# username Teku4boys privilege 15
secret Teku4boys75}
{FW_router(config)# ip http secure-server}
{FW_router(config)# ip http server}
{FW_router(config)# ip authentication local}
{FW_router(config)# line con 0}
{FW_router(config-line)#password ciscosdm }
{FW_router(config-line)#login }
{FW_router(config-line)#transport input ssh}
{FW_router(config-line)# exit}
{FW_router(config)#int Gig0/1}
{FW_router(config-if)#no shutdown}
{FW_router(config-subif)#int Gig0/1.32}
{FW_router(config-subif)#encapsulation dot1q 32 native}
{FW_router(config-subif)#ip address 172.16.32.1
255.255.255.0}
{FW_router(config-subif)#no shutdown}
{FW_router(config-subif)#end}
{FW_router#write}
```

2. Install Cisco configuration professional on management computer. Management computer is configured with IP address in the 172.16.32.0 subnet. Launch Cisco configuration professional program. Within its home window, click ‘Application’ follow by ‘manage community’ from the menu bar. Next, within the manage community window, enter the IP address 172.16.32.1 and hostname for the Cisco 3945 router. Enter username ‘Teku4boys’ and password ‘Teku4boys75’. Check ‘connect securely’ option to enable secure connection to the router. Click okay to

access router. Router's outside interface is assigned IP address 172.16.70.48 255.255.240.0; Table 1-2 displays VLANs and IP address space used in the Firewall configuration.

Table 3.VLANs and their respective subnet IP block

VLAN ID	VLAN NAME	IP SUBNET ADDRESS
2	Isolated_vlan	No ip address
3	DMZ_primary_vlan	172.16.3.0/24
32	Mgt_vlan	172.16.32.0/24
33	Intservers_vlan	172.16.33.0/24
34	NAS_mgt_vlan	172.16.34.0/24
36	Staff_vlan	172.16.36.0/22
48	Student_vlan	172.16.48.0/20

3. Within Cisco configuration professional main window, click the configuration tab below menu bar. On the left navigation window click 'router folder', 'overview', to view current settings on router. Figure 6 shows current router settings.

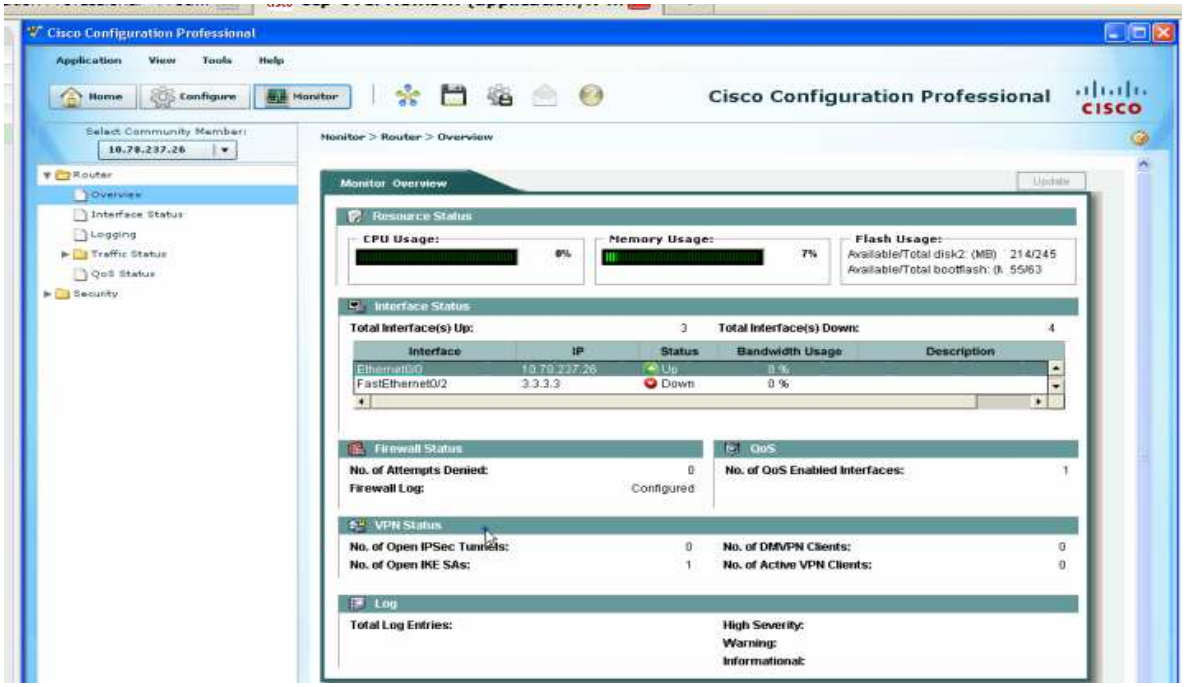


Figure 6. Display window for routers current settings

5.3 Configuring Firewall Sub Module

To configure the firewall, on the left navigation window, click ‘security’, ‘Firewall and ACL’. Next, on the right pane click ‘Advanced firewall’ follow by ‘launch the selected task’. Figure 7 shows firewall configuration start page. The steps involve in configuring advanced firewall using Cisco configuration professional are much the same as using Cisco SDM (security device manager). This involves selecting the inside, outside and DMZ interfaces as shown in Figure 8 and clicking next to proceed. Next, specify two IP addresses 172.16.3.2 TCP port 80 for the webserver and 172.16.3.3 TCP port 25 for mail server. Click next and accept the default security level to be high. Enter two DNS server IP addresses, for example 8.8.8.8 and 8.8.4.4(Google free DNS servers), click next to proceed. Click finish to complete firewall configuration, Figure 9 displays advanced firewall configuration summary. Finally click on deliver button to deliver configuration to router. Figure 10 shows firewall delivery status. [13, 14]

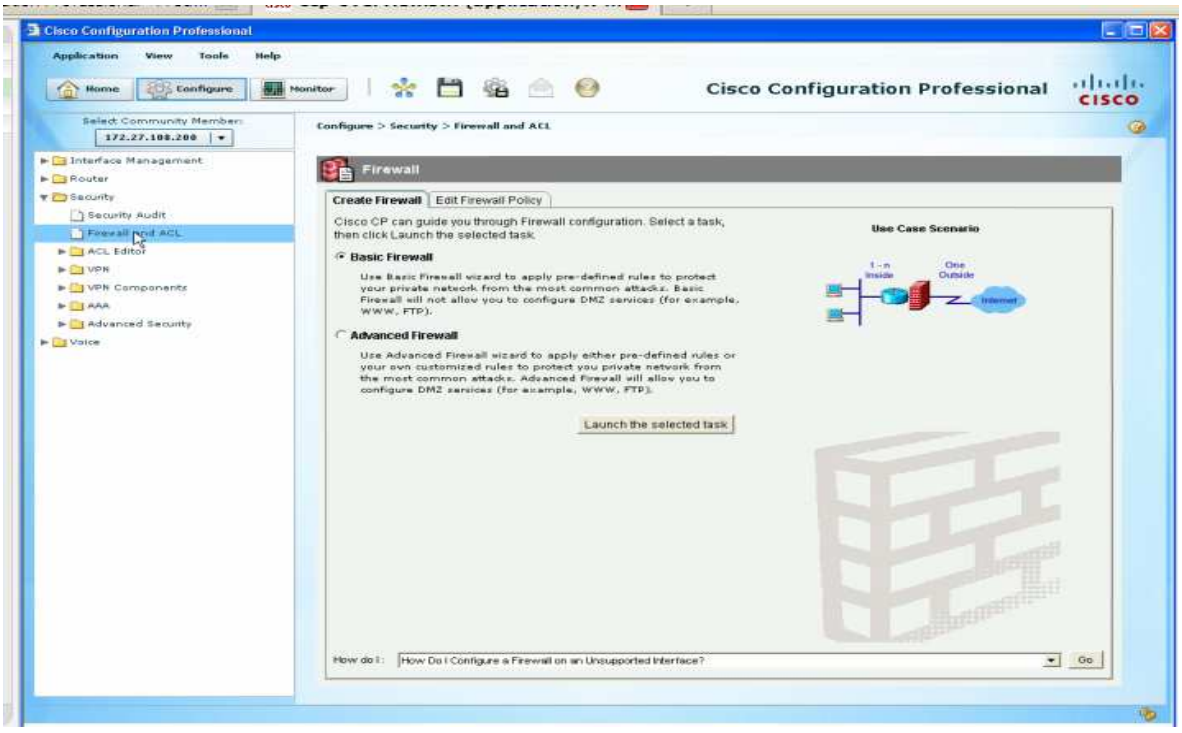


Figure 7. Firewall module configuration start page

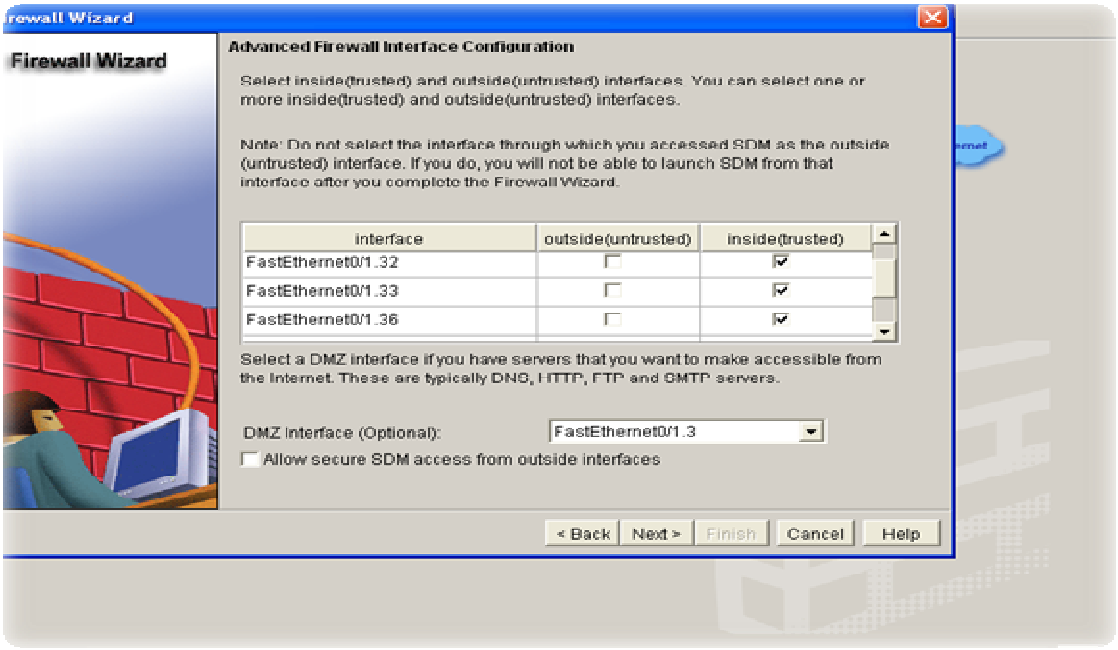


Figure 8. Selecting firewall interfaces

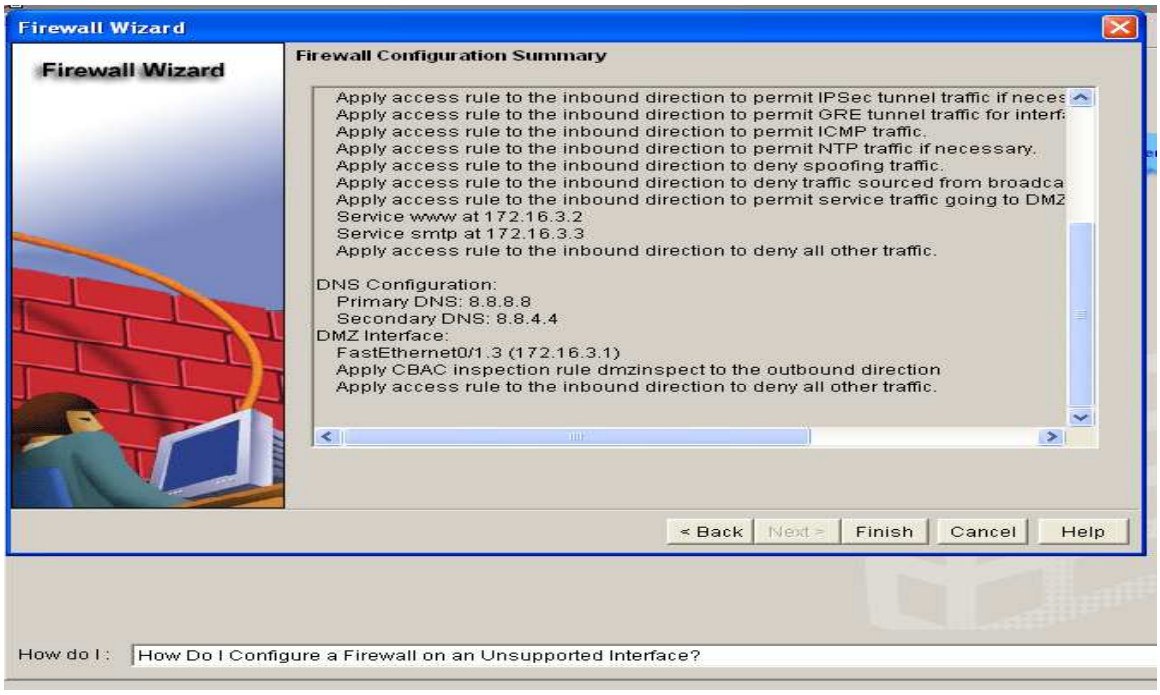


Figure 9. Firewall configuration summary page

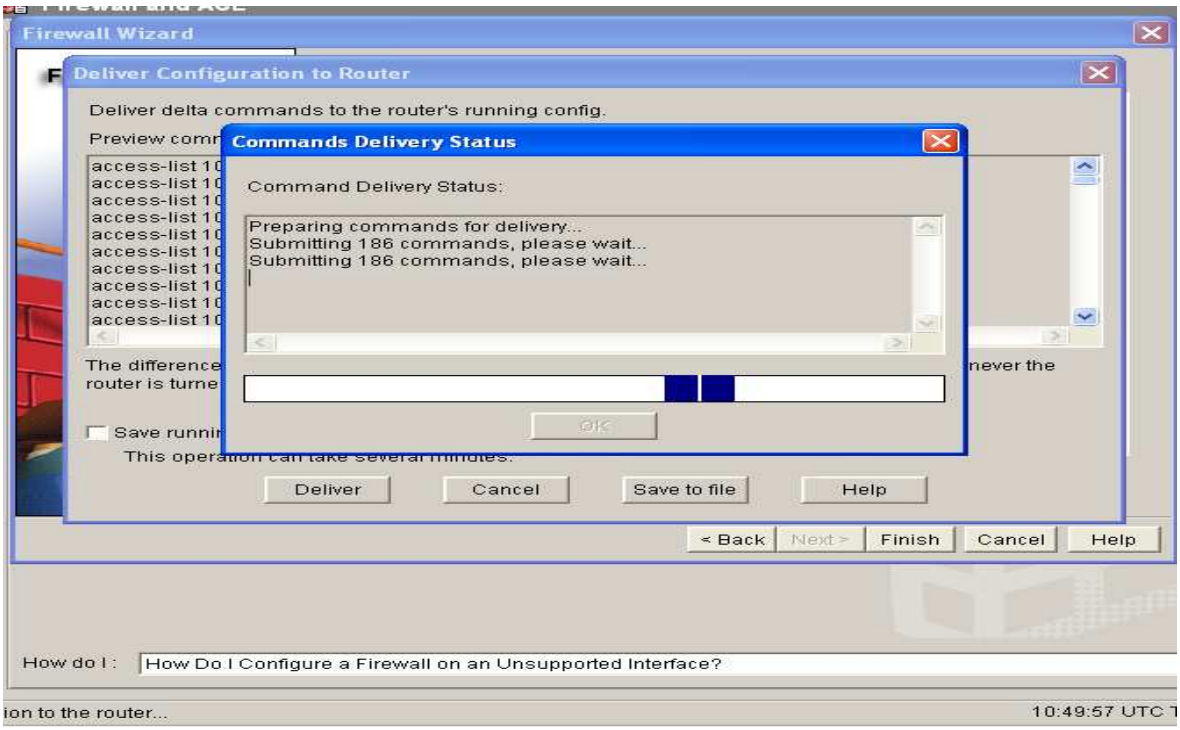


Figure 10. Firewall configuration delivery status

5.4 Configuring NAT Module

To configure NAT- Select NAT option under Router folder in the left navigation pane. Choose ‘Advanced NAT’ on the right pane. Click ‘launch the selected task’ to launch the NAT configuration wizard. Additional options to specify in configuring NAT are follows: [13, 14]

- Choose interface connected to Internet, for example Gig0/0. Enter public IP addresses for the web server, mail server and any internal server by clicking ‘add’ button. For simulation purpose, 180.32.44.44, 180.32.44.45 and 180.32.44.46 were used as public IP addresses.
- Select internal networks that require Internet access as shown in Figure 11.
- Specify private IP address for an internal server, for example 172.16.33.4 and the corresponding public IP address (180.32.44.46) use to access the internal server. Enter TCP port 80 for original port and TCP port 80 for translated port. Click next to proceed.
- Select ‘modify the ACL to work with NAT’ option and click next, okay and finish.
- View configuration summary and click on ‘deliver’ to deliver changes to the firewall-router.
- Access the ‘firewall and ACL’ tab, click on ‘edit firewall policy/ACL’ to view firewall configurations after Advanced NAT has been applied. Figure 12 shows firewall configuration after NAT.

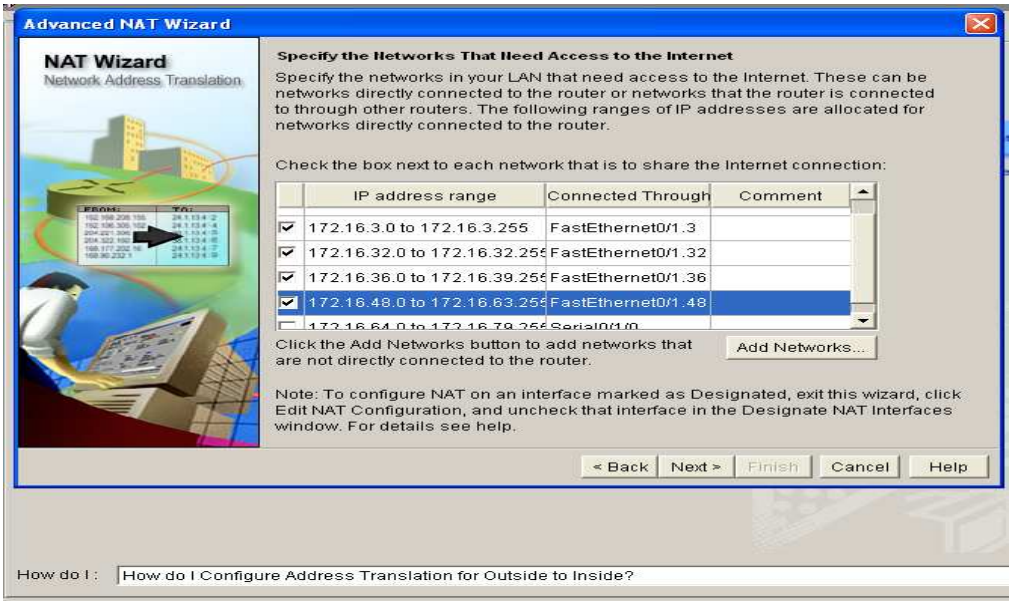


Figure 11. Internal network requiring Internet access

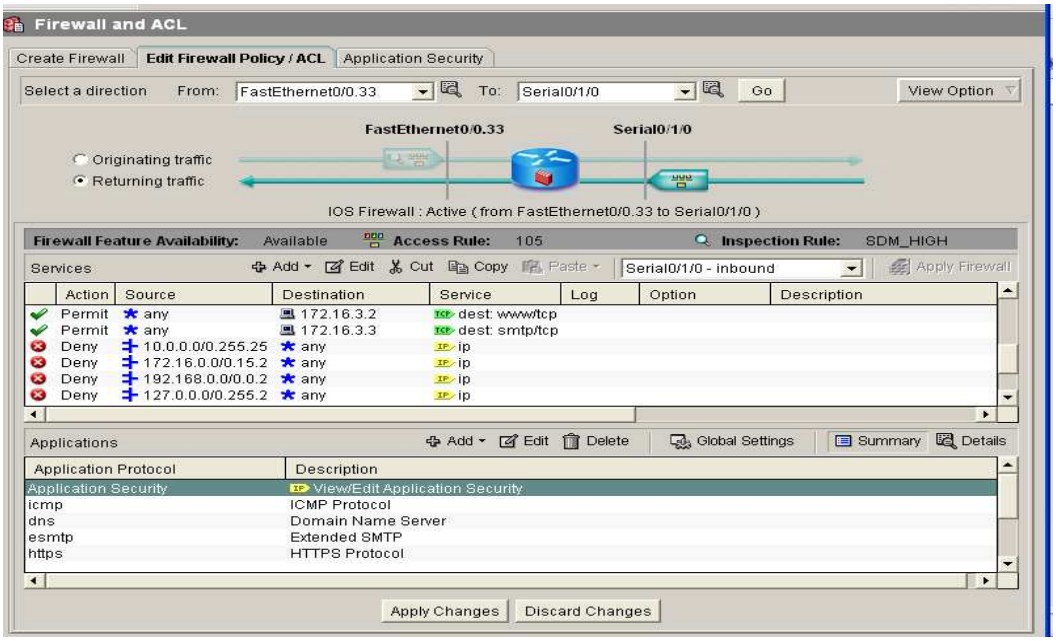


Figure 12. Firewall configuration after NAT implementation

5.5 Configuring IPS sub module

The IPS module is an integrated part of Cisco 3945 router. The following steps outline the procedures in configuring the IPS (Intrusion prevention system).

- Within the configuration tab window in Cisco configuration professional as shown in Figure 6, click ‘advanced security’ folder in the left navigation pane follow by a click on intrusion prevention.
- Click ‘launch IPS Rule wizard’ follow by OK , OK and Next to proceed.
- Select inbound and outbound interfaces as shown in Figure 13 and click next button.
- Click ‘add’ button to specify location of signature definition file (SDF) bought from Cisco corporation or check ‘use build in signature (as backup)’ to use default SDF. Click next to proceed.
- Click finish. Next, click deliver button as shown in Figure 14 to deliver configuration to router IPS module.
- Figure 15 shows a list of signature files included in the IPS configuration

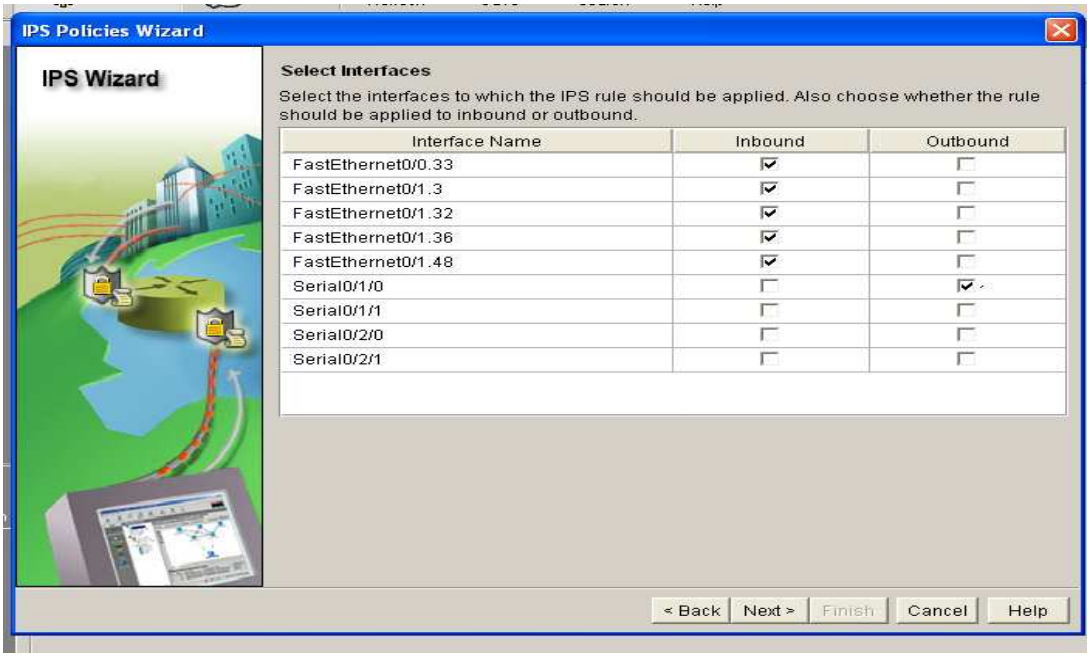


Figure 13.selecting IPS inbound and outbound interfaces

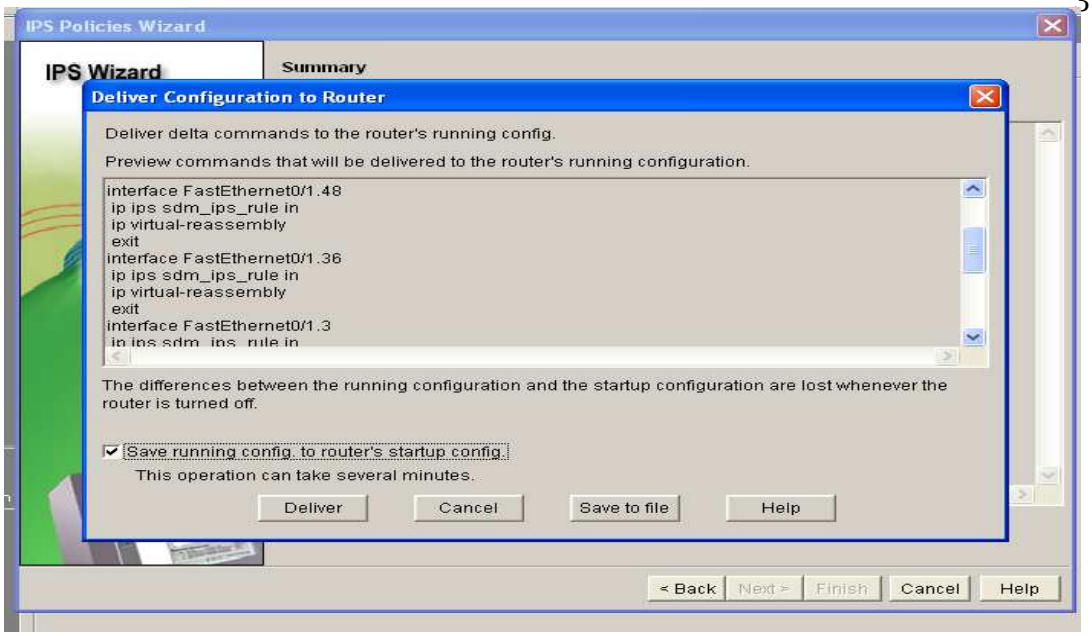


Figure 14.Delivering IPS configuration settings

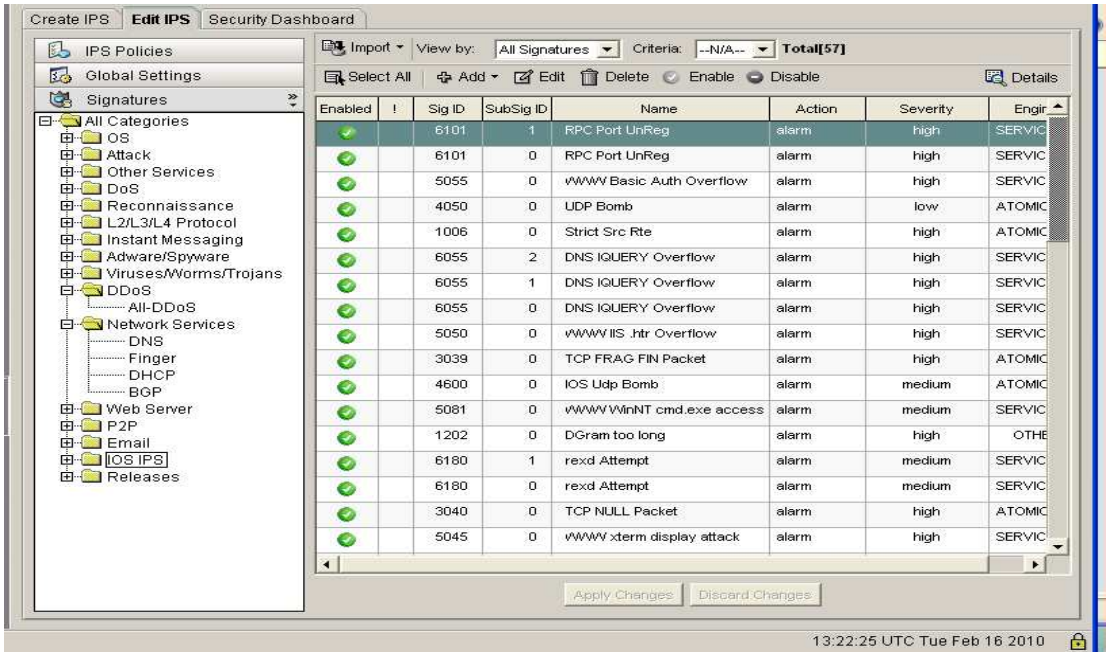


Figure 15.IPS signature files

6 Installing Tftp Server

TFTP server is an important element in network security implementation. This is because TFTP server serves as a repository for backup copies of IOS image and startup configuration files for switches, routers and firewalls in a network environment. If for some reason, one of the network device IOS is deleted, restoration of a new IOS image can be performed without much delay serving network down time. Upgrading of the device IOS image is also much easier with the TFTP server. Steps involve in implementing TFTP server are as follows: [5]

1. Install Solarwinds TFTP server on server computer.
2. Assign IP address on server that can be reached from any host on the network. For example 172.16.33.14 255.255.255.0
3. Install F-secure client security 8.0 or 9.0 or any other Internet security suit on the server computer and enable host based IPS.
4. Launch the TFTP software program.

Backing up IOS Image and Running Configuration

1. To backup IOS image file from Switch to TFTP server, type the following command syntax in privilege enable mode follow by enter key. Accept IOS image file, enter IP address of TFTP server follow by enter key.
   `{Switch#copy flash:TFTP:}`
2. To backup running-configuration file to TFTP server, enter the following command syntax:
   `{Switch#copy running-config tftp://172.16.33.14/configs/back_swconfig}`
   where, 172.16.33.14 is the IP address of the TFTP server. Configs is main configuration files directory and back_swconfig is the switch configuration file name. [5]

Restoring IOS Image and Running Configuration

1. To restore or upgrade IOS image from TFTP server, enter the following command syntax in privilege enable mode follow by carriage return. Next, specify the IP address of the TFTP server and the IOS image file to restore. Press ‘enter key’ after each specification.
   `{Switch#copy TFTP: flash:}`
2. Restoring backup running configuration from TFTP server. Enter command syntax in privilege enable mode.
   `{Switch#copy TFTP: running-config}`
   specify the IP address of TFTP server and backup file to be restored. When file is successfully transfer to switch, enter this command:
   `{Switch#write}`

However, if TFTP server can not be accessed remotely to restore IOS image file to Switch due to network failure, the following steps can help to restore IOS image locally.

1. Copy desire IOS image to a laptop.
2. Connect laptop to switch using console cable
3. Boot switch to rommon mode (rommon>)

4. Type this command example:
   {rommon>xmodem –c c1841-ipbase-mz.123-14-TZ.bin}
   where, c1841-ipbase-mz.123-14-TZ.bin is the IOS image file.
5. Open windows Hyperterminal program. Within the hyperterminal program, from the transfer menu, select 'send file'. From within the 'send file' dialog box, specify the location of the IOS image by clicking browse and choose 'xmodem' transfer protocol. Click send to transfer image file to switch.[5]

6.1 NTP Configuration

Ntp (network time protocol) is very crucial in network security because it is very important to know accurately when an event such as an attack occurred. Furthermore, in order to accurately analyze traffic patterns for network to ensure proper network tuning, it is important to have NTP configure on all network devices for proper time synchronization. In an NTP environment, all devices synchronize to the same time. With NTP, summer and winter time adjustment is automatic. The following steps outline how to configure NTP. [15]

Step 1- Taking care of daylight saving time and device internal calendar, enter following commands syntax:

```
{Router(config)#clock timezone EET +2}
{Router(config)#clock summer-time EEDT recurring 2 Sun Mar
2:00 1 sun Nov 2:00}
{Router(config)#clock summer-time recurring}
{Router(config)#ntp update-calendar}
{Router(config)#end}
```

Step 2 – Configuring Cisco 3945 router to synchronize with stratum 2 free NTP servers on the Internet for accurate time. Commands syntax;

```
{Router(config)#ntp server 194.137.39.68 version 3}
{Router(config)#ntp server 194.137.39.67 version 3}
{Router(config)#int range Gig0/1- 0/2}
{Router(config-if)#ntp broadcast}
```

Stratum 2 NTP servers 194.137.39.68 and 194.137.39.67 belong to 'tock.keso.fi' and 'tick.keso.fi' respectively.

Step 3 – Configuring switches and internal routers that will rely on Cisco 3945 for accurate time synchronization. The following commands syntax is entered on all internal network switches.

```
{switch(config)#ntp broadcastdelay 4}
```

Step 4- Configuring all trunk ports on switches to listen to broadcast. Example commands syntax:

```
{Switch(config)#int Gig0/1}
{Switch(config-if)#ntp broadcast client}
```

7 Secure Switch Management with Network Assistant

To securely manage network switches with Cisco network assistant, all switches in the management domain are assigned an IP address within the mgt_vlan subnet; that is, 172.16.32.0/24. Some switches with old IOS versions will not support network assistant. A complete list of supported devices is available on Cisco website. Cisco catalyst 3560 series switches were used in lab simulation. The following procedures are necessary to manage a switch with Cisco Network assistant. [16, 17]

1. Apply the following configuration commands on every switch that would be managed by network assistant. Only alter the fourth octet value of IP address. Example configuration commands syntax:

```
{switch(config)# username Teku4boys privilege 15 secret
Teku4boys75}
{switch(config)# ip domain-name savoteku.com}
{switch(config)# ip http server}
{switch(config)# ip http max-connections 16}
{switch(config)# ip http timeout-policy idle 180 life
180 request 25}
{switch(config)# int vlan 32}
{switch(config-if)#ip address 172.16.32.2 255.255.255.0
}
{switch(config-if)# no shutdown}
{switch(config-if)#end }
```

2. Install Cisco network assistant on the management computer and assign the computer IP address within the mgt_vlan subnet.

- Assign the switch port (int fa0/7) connected to the management computer to native vlan 32. This can be accomplished by entering the following commands on switch connected to management computer.

```
{switch(config)#int fa0/7}
{switch(config-if)#switchport mode access}
{switch(config-if)#switchport access vlan 32}
{switch(config-if)#no shutdown}
{switch(config-if)#end}
```

- Launch network assistant program on management computer. From within the program startup window, select create community follow by ok.
- Leave the default settings in ‘Advanced’ tab. Enter community name in the ‘name’ text field and tekucompany in the ‘company name’ field. From ‘discover’ drop down menu select ‘devices in an IP address range’ as shown in Figure 16. Enter start and end IP address range, click start follow by ok.

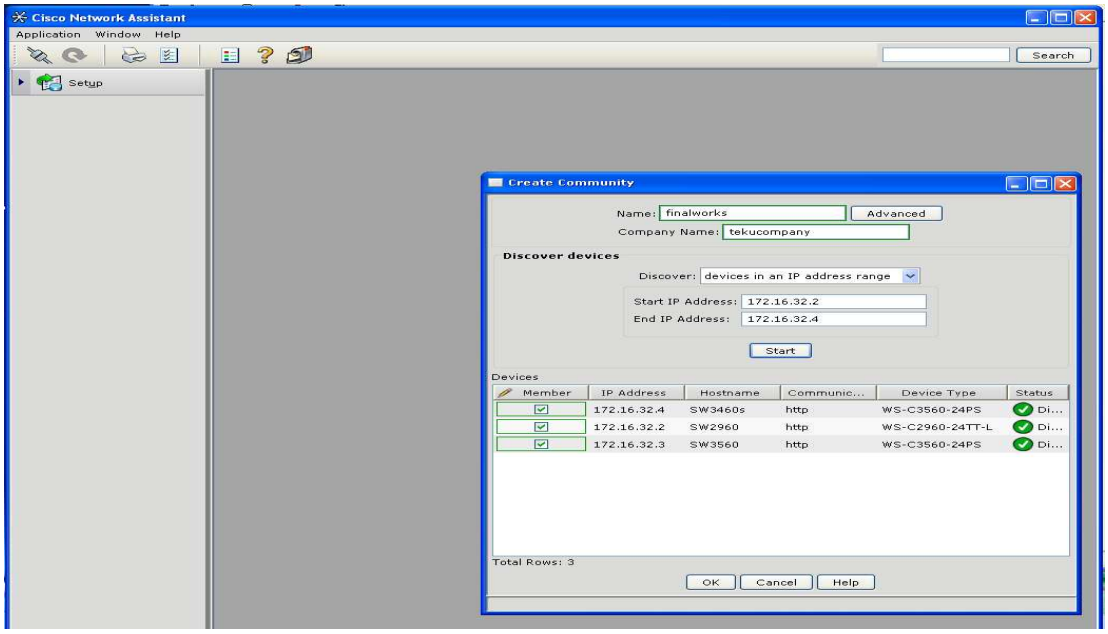


Figure 16. Entering IP address range for manage switches

3. Click on the 'front panel' view button located on the tool bar to see a front view of selected switches. The front view of three simulated switches is shown in Figure 17.

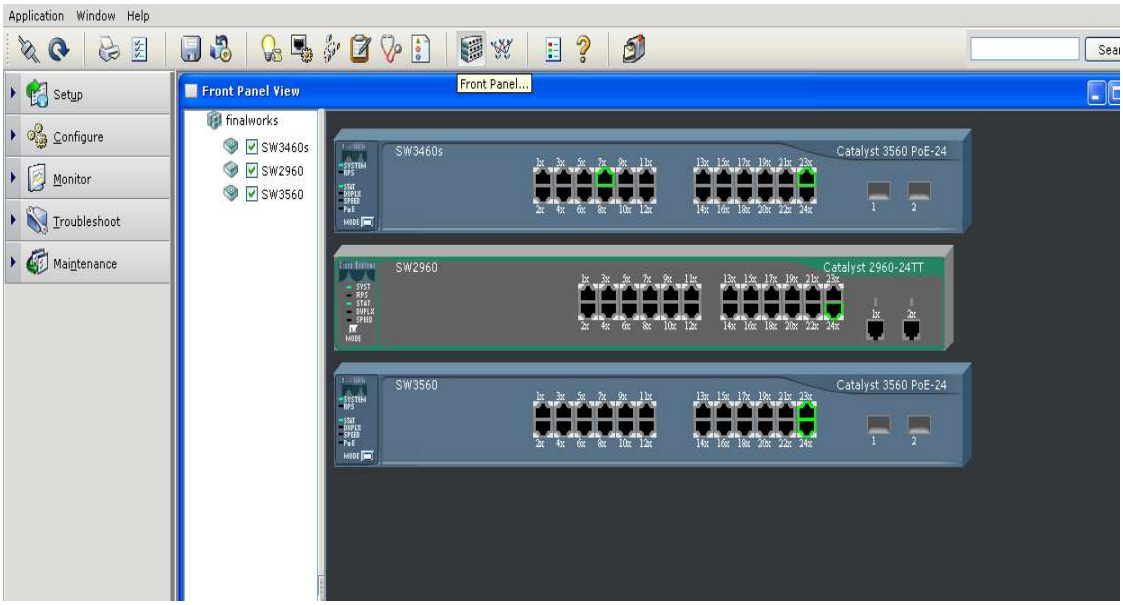


Figure 17. Front panel of simulated switches

7.1 Using Smart Port to Configure Switch Ports

On the left navigation pane in Figure 17, click on ‘configure’ tab and ‘smart ports’ to open the smart ports configuration window. Select ports on the switch you wish to configure by clicking and dragging the mouse over them; next click on modify button. In the modify dialog box, select the role of the port by clicking the role drop down button. If the selected ports are connected to access points, select access point from the ‘role’ drop down menu. Select native vlan, for example management (32) as shown in Figure 18. Click OK and Apply. Click on save configuration on the left navigation bar to push configuration to switch. [16]

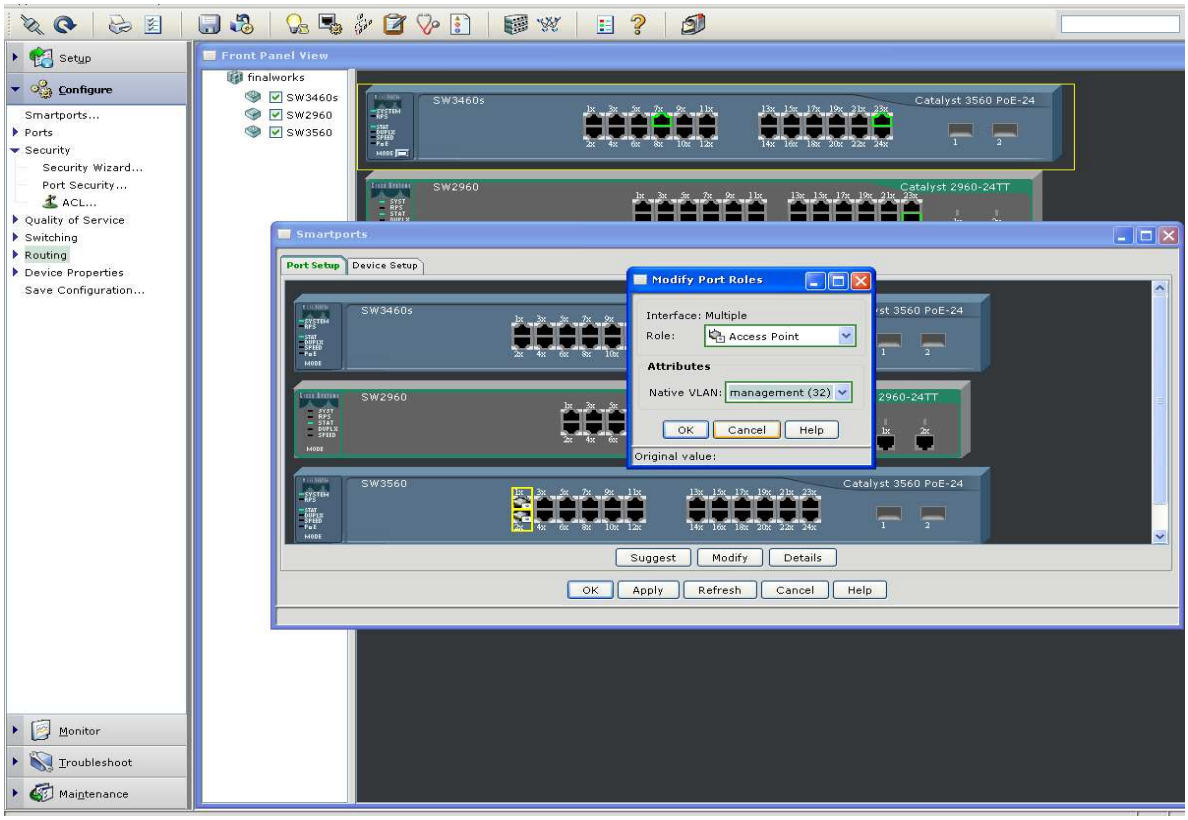


Figure 18. Using smart port to configure switch port

7.2 **Configuring Application Filtering**

To configure application restriction, within the ‘configuration’ tab, select ‘security’ follow by security wizard. In the security wizard window, select ‘restrict applications’ and click next. Select applications to filter from switch access ports, for example telnet and secure shell as shown in Figure 19 and click next. Select the switch to apply filtering and click next. Manually select ports to apply filtering, click next, next and finish. [16]

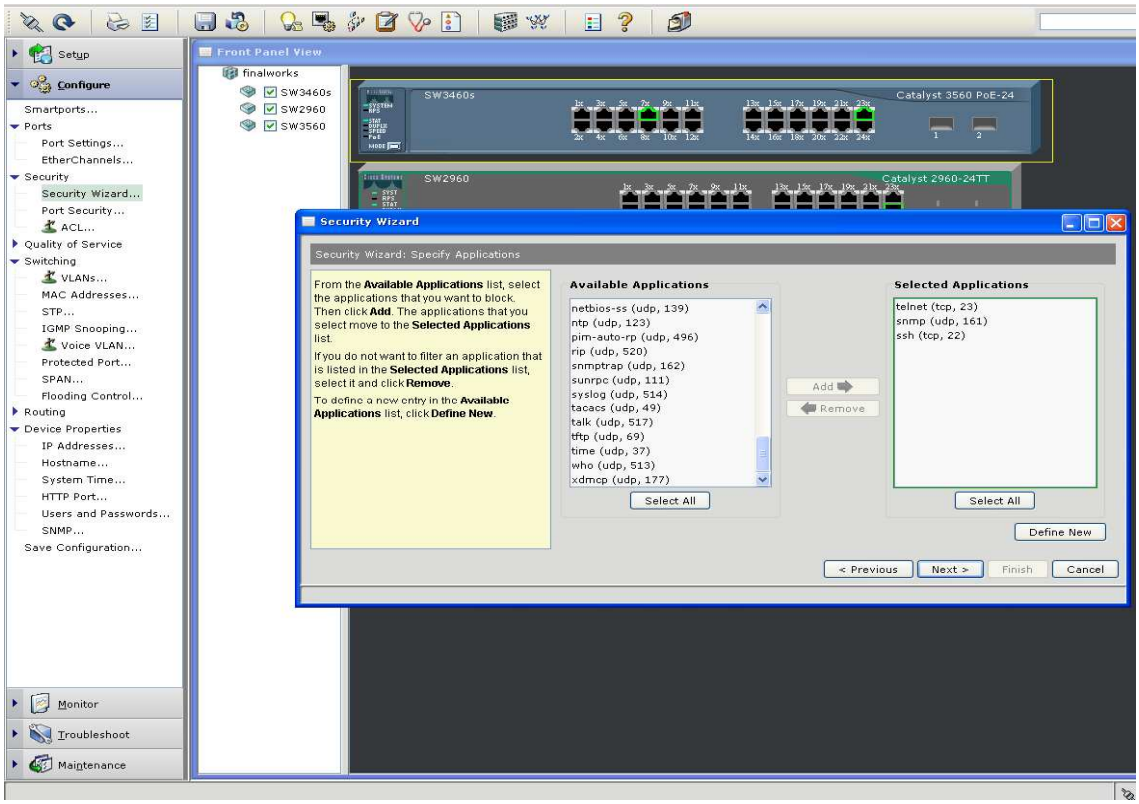


Figure 19. Application filtering

7.3 Configuring Port Security

To configure port security, within the ‘security’ category in the left navigation bar, select ‘port security’. Within port security window, select the desire switch from hostname dropdown menu. Select desire port, for example fa0/5, follow by a click on modify button as shown in Figure 20. In the ‘modify’ dialog box, enable ‘sticky behavior’ and violation action as ‘shutdown’. Click ok and apply. Click ‘save configuration’ to save configuration. [16]

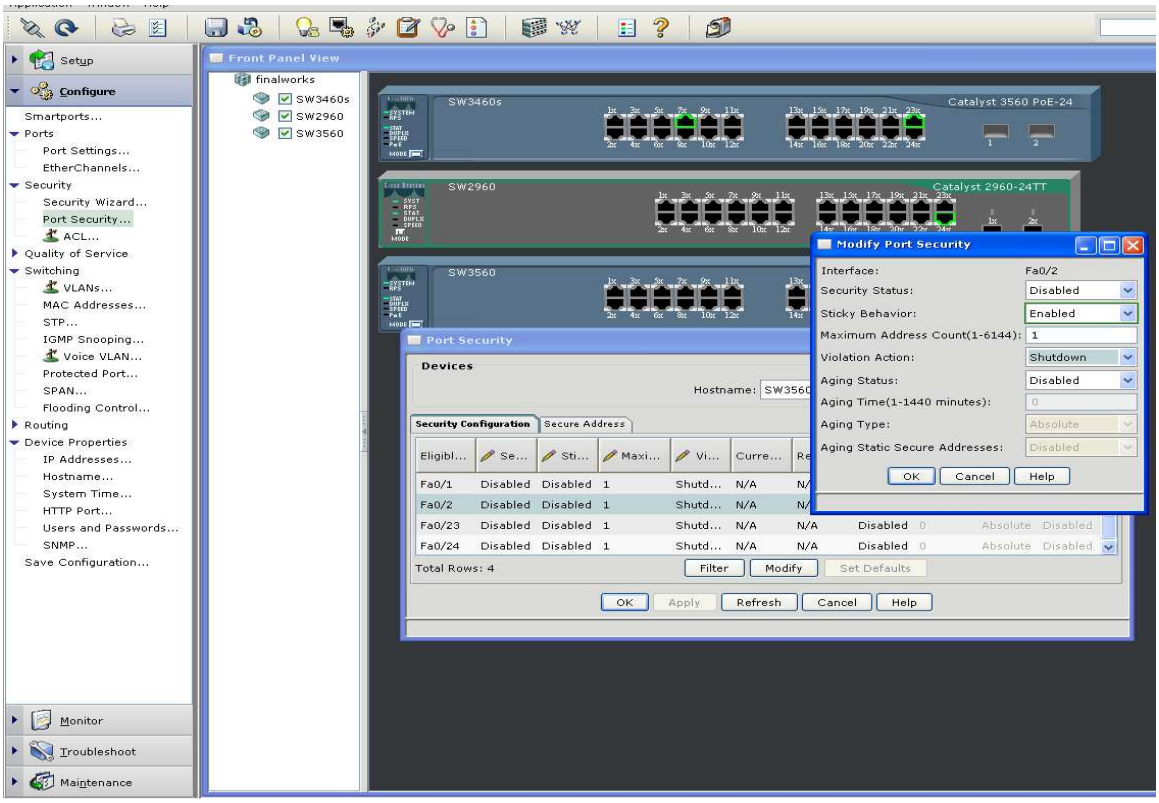
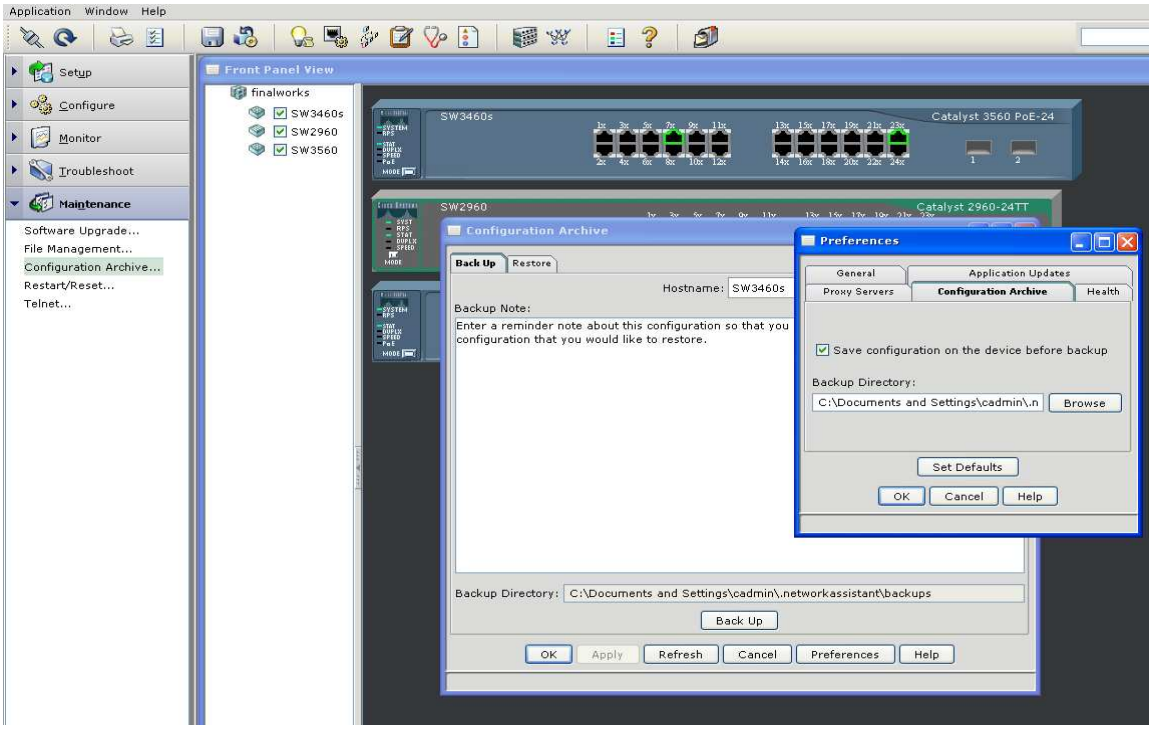


Figure 20. Configuring port security

7.4 Backing and Restoring Files to TFTP Server

To backup and restore configuration files to the TTFTP server, go to ‘maintenance’ tab and click ‘configuration archive’. Within the configuration archive window, ‘select backup tab’, select switch. Click ‘preferences’ to specify location of TFTP server as shown in Figure 21. Click browse to locate TFTP server on the network. Click ok to backup configuration file.



[16]

Figure 21. Backing up configurations to TFTP server

8 Enforcing Endpoint Security Control with Cisco NAC

Cisco NAC (network admission control) formally known as Cisco clean access, is a network security solution aim at providing and enforcing network security policies on all devices requesting access to network. Some of these policies involve checking if computer requesting network access has up-to-date operating system patches, up-to-date antivirus/spyware signature files; If not, the computer is quarantine and user asked to comply with network security policy before network access is granted.
Cisco NAC appliance has three user roles which are as follows:

1. Unauthenticated role is created by default and can not be edited. Both web and agent login users are placed into unauthenticated role when they initiate network access.
2. Client posture assessment role (agent temporary and quarantine role). Agent user is put into temporary role while system checks are performed. A user is put in quarantine role when system checks fail to comply with network security policies. Quarantine and temporary role are created by default and require just configuration.
3. Normal role – network user is placed into normal role after successful login. Normal role must be created and associated with traffic polices.

A network running Cisco NAC along side other security frame work implementation has the ability to reply major network attacks that may ground the network. In implementing Cisco NAC, many factors must be taken into account. These include the number of CAS (clean access servers) needed in the deployment, the maximum number of concurrent connection per CAS and a CAM (clean access manager) for managing CAS. Cisco requires that a license be purchased for every CAS (based on the number of maximum concurrent connection) and CAM (based on the maximum number of manage CAS). In Figure 5, seven CASs are deployed, that is including CAS for Iisalmi and Varkaus campuses. The design in Figure 5, where by routing is performed at the network core instead of distribution layer as recommended by Cisco, is necessary because it reduces the number of CAS needed in the deployment. But however, when performance is a priority over cost of CAS, then routing will be performed at the distribution layer. This means the number of CASs will increase from 7 to a minimum of 17 and will drive up cost. [18][19][20]

8.1 Installation of CAS

To install CAS, it is required that the server computer must support two network cards (eth0 and eth1). In this deployment example, Dell PowerEdge 1950 is used to install CAS software; Dell powerEdge 950 is also compatible. A detail list of hardware server appliances that support CAS software is available on Cisco website. The two GigabitEthernet network cards (eth0 and eth1) in CAS server should be replaced with Dell Intel Pro/10GbE SR 10Gigabit network cards to eliminate bandwidth mismatch bottle neck between the distribution and core layer. Layer 2 virtual gateway inband mode (IB-mode) is used in CAS installation example with exemption of CAS 7 which is deployed as layer 3 real IP gateway. In Cisco NAC terminology, eth0 is referred as trusted and eth1 as untrusted interface. The necessary steps to install CAS are as follows: [19]

Step 1 - insert the ISO bootable image disc of CAS software into Dell powerEdge1950 and allow the server to boot from the disc. Select ‘install clean access server’ by hitting the

return key. Enter information available in Table 5 when prompted in the installation process.

Table 5. CAS installation data

Eth0 IP address	172.16.34.4 255.255.255.0
Default gateway	172.16.34.1 (this is switch virtual interface)
Vlan ID- passthrough	Yes
Management Vlan tagging	Yes , value =989
Eth1 IP address	172.16.34.4/24
Default gateway	172.16.34.1
Vlan ID –passthrough	Yes
Management Vlan tagging	Yes, value =990
Hostname	CAS1
IP address of Name server	172.16.33.10
Shared secret	Gipson123
Time	Enter correct time
Fully qualify Name for SSL	172.16.34.4
Organization unit name	Teku
Organization name	Savonia university
City name	Kuopio
State code	Ps
Country code	Fi
Root password	Gipson123
Web console admin password	Gipson123

When all the information in Table 5 is entered in the installation process, CAS would have been successfully installed. At the root prompt `([root@cas1-]#) type 'service perfigo reboot'` to reboot the CAS. When the reboot process is completed, use `'service perfigo config ',` at the root prompt at any time to make CAS configuration changes.

8.2 Installation of CAM

On the computer dedicated for CAM, insert the bootable image disc of the CAM software into the disc drive of the server computer and allow the server to boot from disc drive. Select 'install CAM' from the boot option menu by hitting the return key. Enter information found in Table 6.The CAM uses only one Ethernet card (eth0); eth1 is left unused. [20]

Table 6. CAM installation data

Eth0 IP address	172.16.33.2 255.255.255.0
Default gateway	172.16.33.1 (this is switch virtual interface)
Hostname	CAM
IP address of Name server	172.16.33.10
Shared secret	Gipson123

Time	Enter correct time
Fully qualify Name for SSL	172.16.32.2
Organization unit name	Teku
Organization name	Savonia university
City name	Kuopio
State code	Ps
Country code	Fi
Root password	Gipson123
Web console admin password	Gipson123

When CAM software installation is completed, reboot the server with ‘service perfigo reboot’ command. To login into CAM or CAS when it has rebooted, use ‘root’ as username and Gipson123 as password. Table 7 shows example commands syntax for configuring SW1 and SW2 connected to CAS1. VLAN 989 and 990 are dummy VLANs and are not allow to be used anywhere else in the network; they should not have switch virtual interfaces.

Table 7.SW1and SW2 example commands syntax to support CAS1

```
SW1(config)#ip routing
SW1(config)#vtp mode transparent
SW1(config)#vlan 2
SW1(config-vlan)#name isolated_vlan
SW1(config-vlan)#vlan 3
SW1(config-vlan)#name DMZ_primary_vlan
SW1(config-vlan)#vlan 32
SW1(config-vlan)#name mgt_vlan
SW1(config-vlan)#vlan 33
SW1(config-vlan)#name Inteservers_vlan
SW1(config-vlan)#vlan 34
SW1(config-vlan)#name NAS_mgt_vlan
SW1(config-vlan)#vlan 36
SW1(config-vlan)#name staff_vlan
SW1(config-vlan)#vlan 48
SW1(config-vlan)#name student_vlan
.
.
SW1(config)# int vlan 3
SW1(config-if)#ip address 172.16.3.2 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#int vlan 32
SW1(config-if)#ip address 172.16.32.2 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#int vlan 33
SW1(config-if)#ip address 172.16.33.2 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#int vlan 34
SW1(config-if)#ip address 172.16.34.2 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#int vlan 36
SW1(config-if)#ip address 172.16.36.2 255.255.252.0
SW1(config-if)#no shutdown
SW1(config-if)#int vlan 48
```

```
SW1(config-if)#ip address 172.16.48.2 255.255.240.0
SW1(config-if)#no shutdown

 'Trunk link between SW1 and CAS 1 '

SW1(config)#hw-module uplink select tengigabitethernet
SW1(config)#int tengig 1/2
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport  trunk native vlan 989
SW1(config-if)#switchport trunk allow vlan
3,32,33,34,36,48
SW1(config-if)#no shutdown

 'Trunk link between SW2 and CAS 1 '

SW2(config)#hw-module uplink select tengigabitethernet
SW2(config-if)# int tengig 1/2
SW2(config-if)#switchport trunk encapsulation dot1q
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport  trunk native vlan 990
SW2(config-if)#switchport trunk allow vlan
3,32,33,34,36,48
SW2(config-if)#no shutdown
```

8.3 Adding CAS to CAM

To be able to enforce network access polices through CAS, all CASs in the network environment must be added to the CAM. The following outline steps to add CAS to CAM. [20]

Step 1 – From the network management computer, open a web browser and enter the IP address of the CAM (https://172.16.33.2). Accept the untrusted certificate warning. Enter username 'admin' and password 'Gipson123' to login into CAM. Figure 22 shows CAM login window.

Figure 22. CAM login window

Step 2 – Submit CAM license file obtained from Cisco by clicking browse button and locating the file. This file contains the MAC address of eth0 of the CAM server computer. Click on 'install license' button to install license as shown in Figure 23.

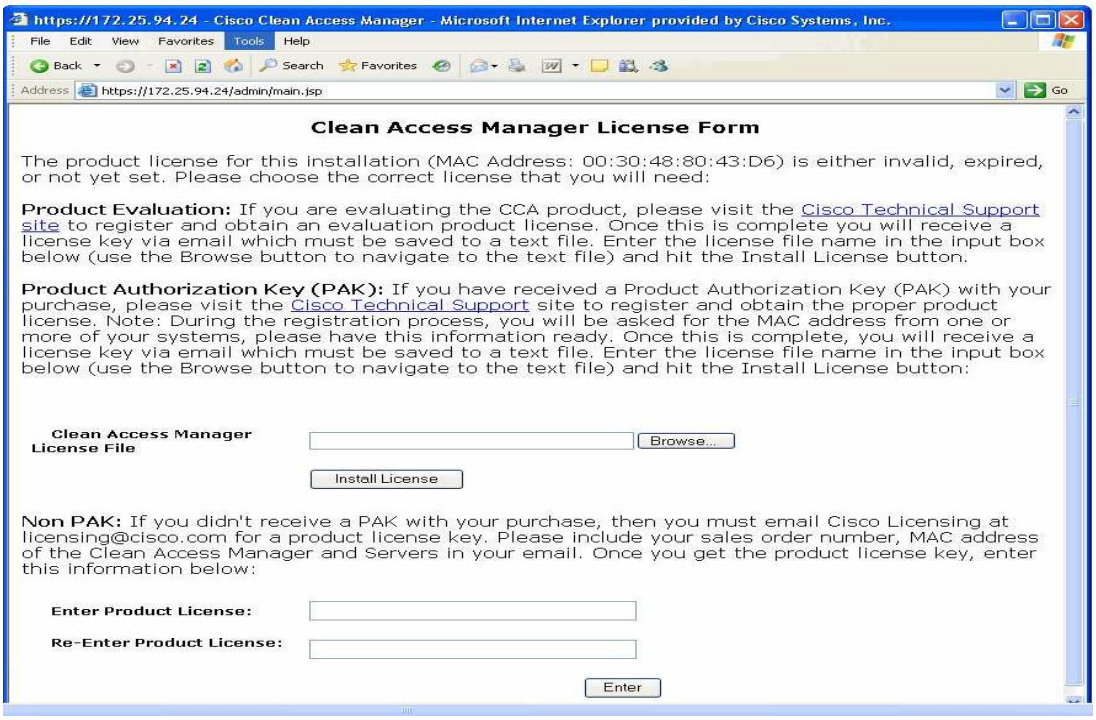


Figure 23. CAM license installation window

Step 3 – Within the CAM manger home page, click CCA Server follow by new server from the left navigation pane to add a new CAS server to CAM. Enter CAS IP address, location information and 'virtual gateway' for server type as shown in Figure 24. Click 'add access server' button to add CAS server. When many servers are added, a list of available servers can be viewed by clicking on the 'list of server' tab in the CCA server window. Click the authorization tab and check 'enable CCA server authorization' and 'test CCA server authorization'; Type CAS1.savoteku.local and click update.
To add CAS 7 to the CAM server select 'real IP gateway' as server type. Next, go to Device management, 'CCA server', 'manage (CAS_IP)', 'network', IP. Enable L3 (layer 3) support and L3 strict mode as shown in Figure 25. These options will allow VPN clients to authenticate through CAS 7 to access the network. The trusted interface (eth0) is connected to SW3 and untrusted (eth1) connected to Cisco 3945 router. Each interface is on a separate subnet.

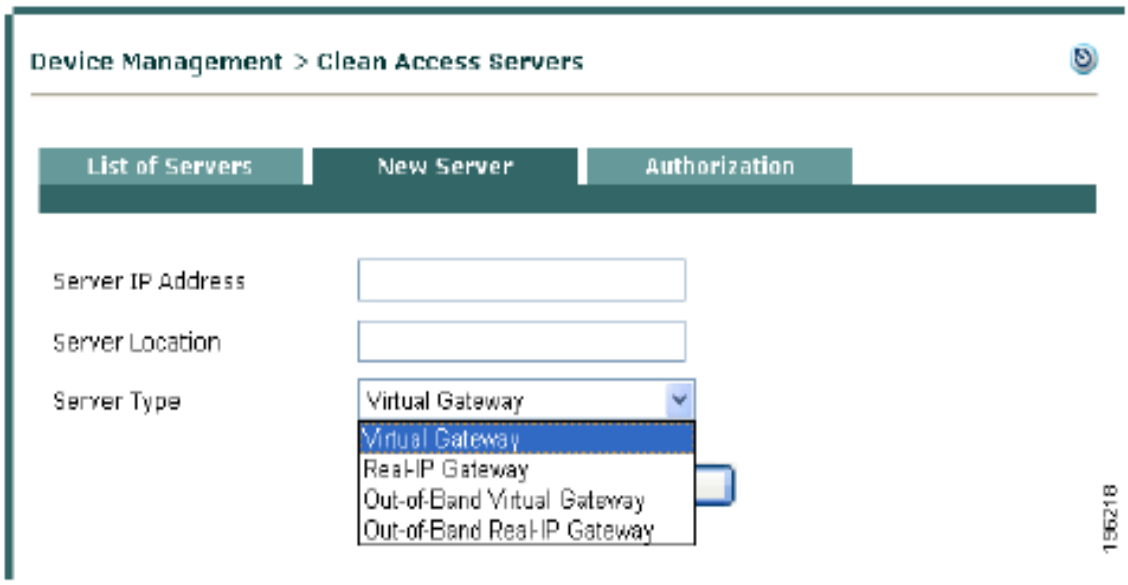


Figure 24. Selecting 'virtual gateway' for CAS server type

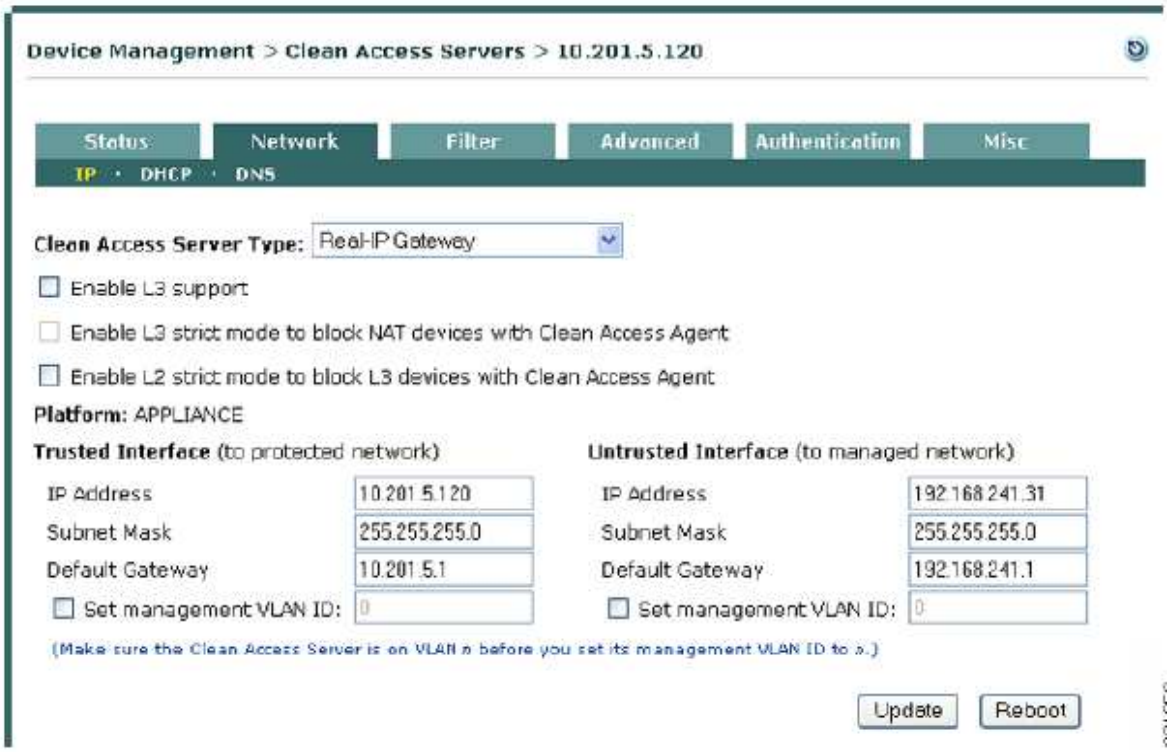


Figure 25. Selecting 'real-IP gateway' for CAS7 server type

Step 4 – After installing the license for CAM, it is required to install additional licenses for the CAS that will be managed by the CAM. To accomplish this, after successfully logging into the CAM, click on 'CCA manager' follow by 'licensing' as shown in Figure 26. Browse to the CAS license file and click 'install license' to install individual licensed for the CAS. A list of successful install CAS with licenses will be seen in the licensing window. Figure 26 displays ten inband and ten outband servers installed.

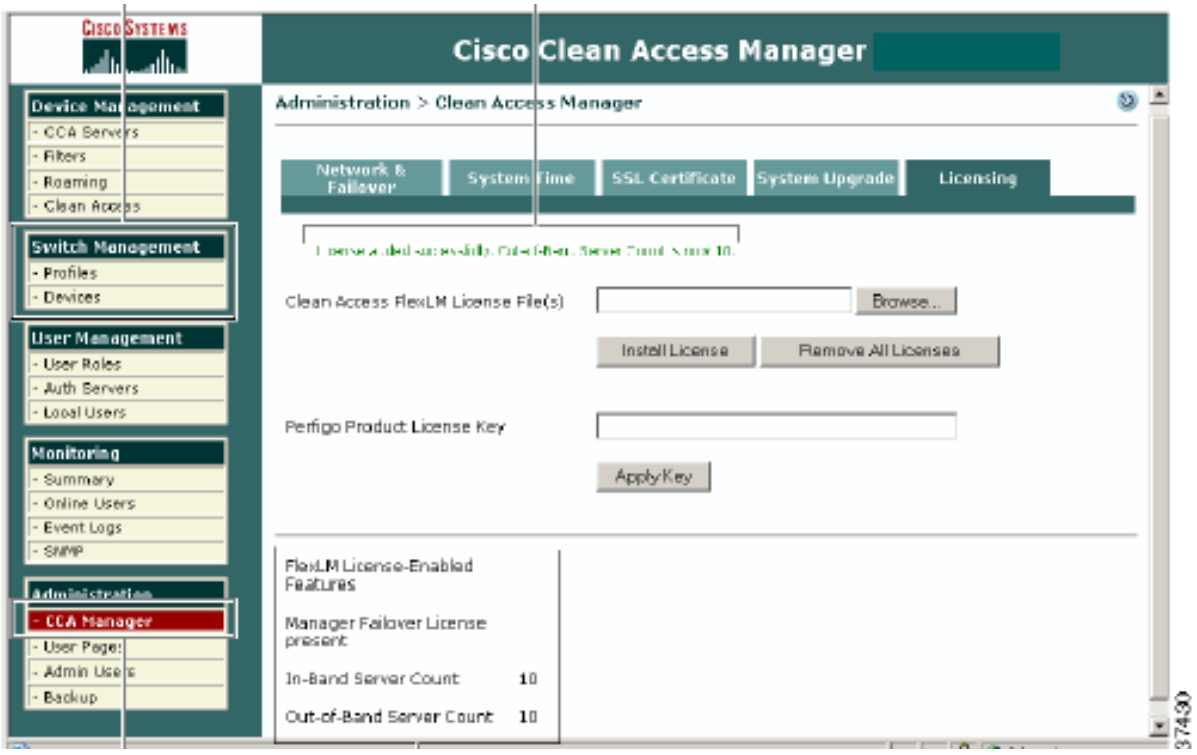


Figure 26. Installing licenses for CAS servers

8.4 Configuring Global Filters

Global filters apply to all CAS in the CAM management domain. Subnet filter allows for authentication specification and access filter to be applied to an entire subnet. All devices accessing the network on a subnet are subject to a filter rule. Steps involve in configuring global filters are as follows: [20]

Step 1- Go to device management, 'filters' and 'subnets' as shown in Figure 27

Step 2- Enter IP address of subnet, description and 'unauthenticated role' as user role. choose 'allow' as access type as shown in Figure 27. The subnet IP address refers to the entire IP address block for the internal networks represented by the VLANs.
Step 3 – click 'add' to save policy.

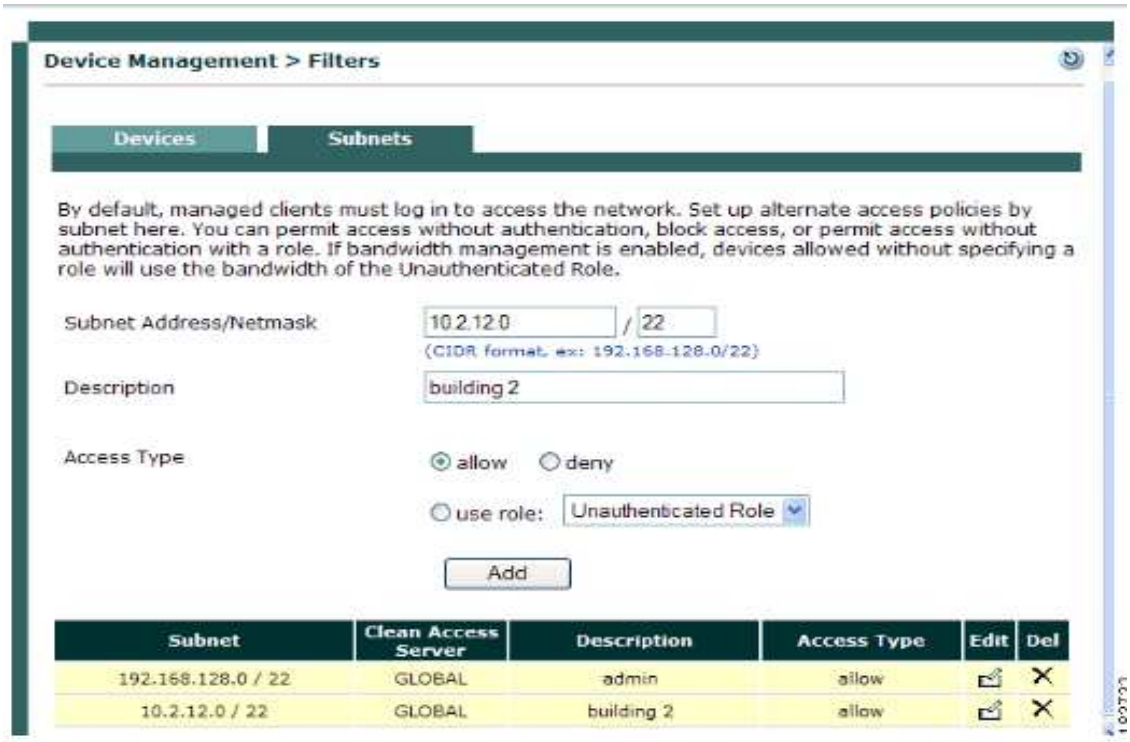


Figure 27. Configuring global filters

8.5 Configuring User Roles

To configure user role, go to ‘user management’, ‘user roles’ and ‘new role’ as shown in Figure 28. Next, follow the following outline steps: [20]

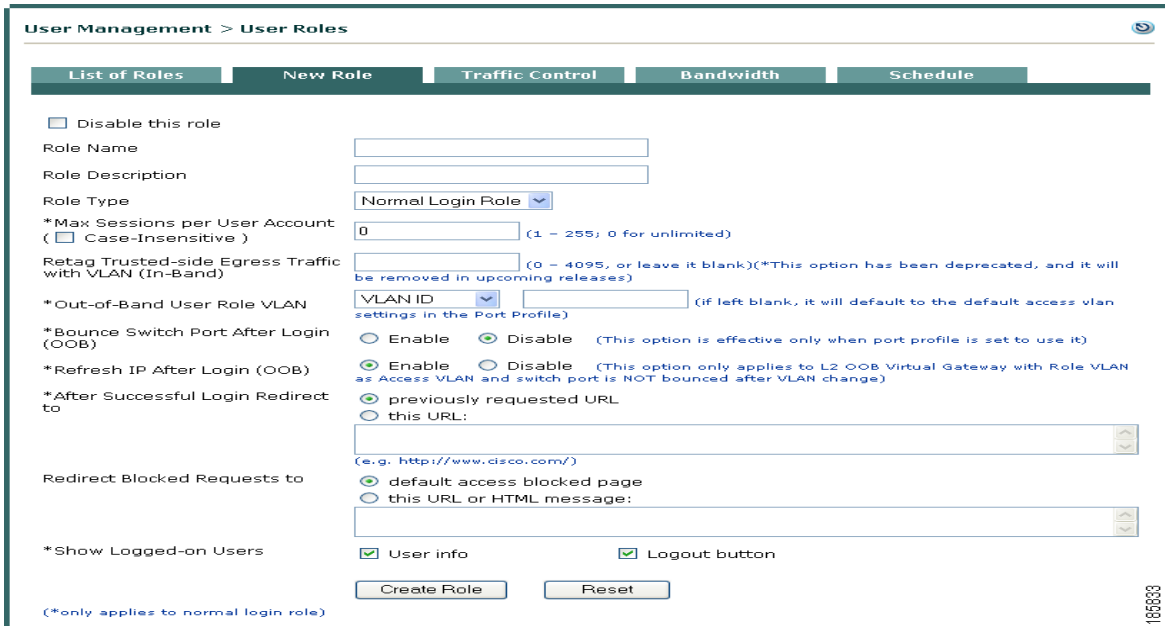


Figure 28. Creating new user role

Step 1- Enter role name and description
Step 2- Enter role type as 'normal login role'
Step 3- Select URL option. Enter www.savonia.fi in 'after successful login redirect to' field.
Step 4- Disable 'refresh IP after login (OOB)'
Step 5- allow other options untouched as shown in Figure 28. Click on 'create role'
Step 6- Go to 'user management', 'user roles', 'list of role' to access the new role created. Here it is possible to edit traffic policies and bandwidth for created roles as shown in Figure 29. The traffic policy for CAS7 is created locally and given a higher priority over global traffic policy. This is because CAS7 is deployed in L3 mode while other CASs in the network are in L2 mode. Local traffic policy for CAS7 is created by going to device management, 'CCA servers' 'manage (CAS_IP)', 'filter' and role.
Step 7 - Click the edit icon in Figure 29 to open window for editing desired user role.

Step 8 – Click on traffic control tab in Figure 29 to configure policies associated with different roles. The traffic control policy configured in this network is 'IP based' as shown in Figure 30. Individual roles can be configured by clicking on 'add policy' link or on 'add policy for all roles' to configure all roles in bulk.

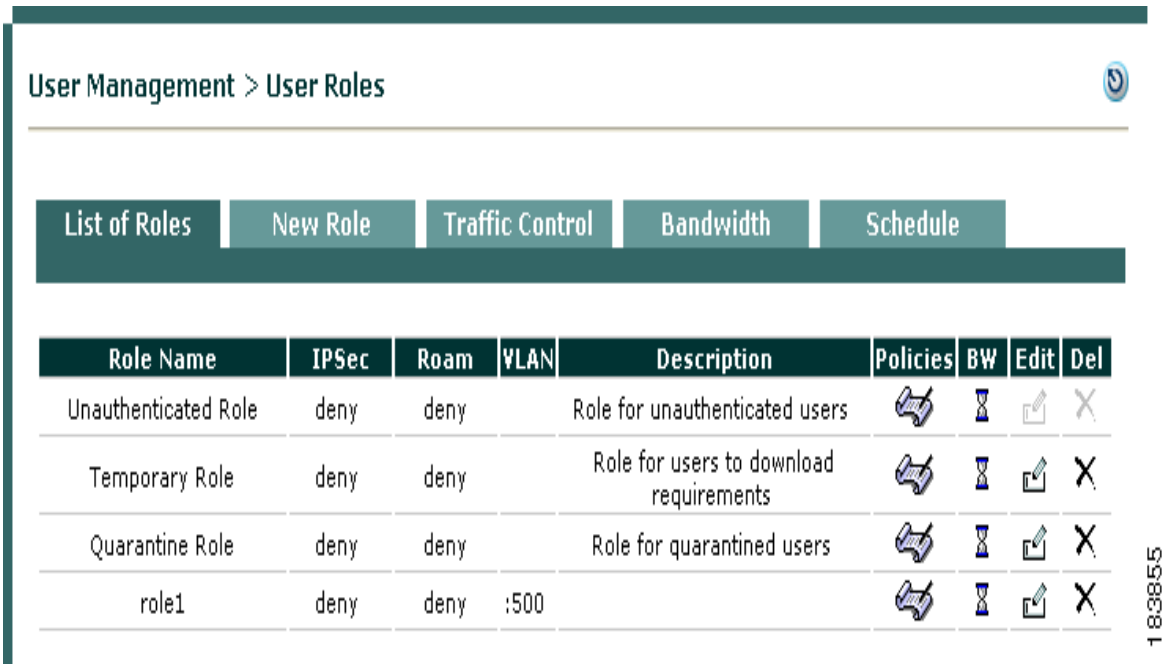


Figure 29. A list of created user roles

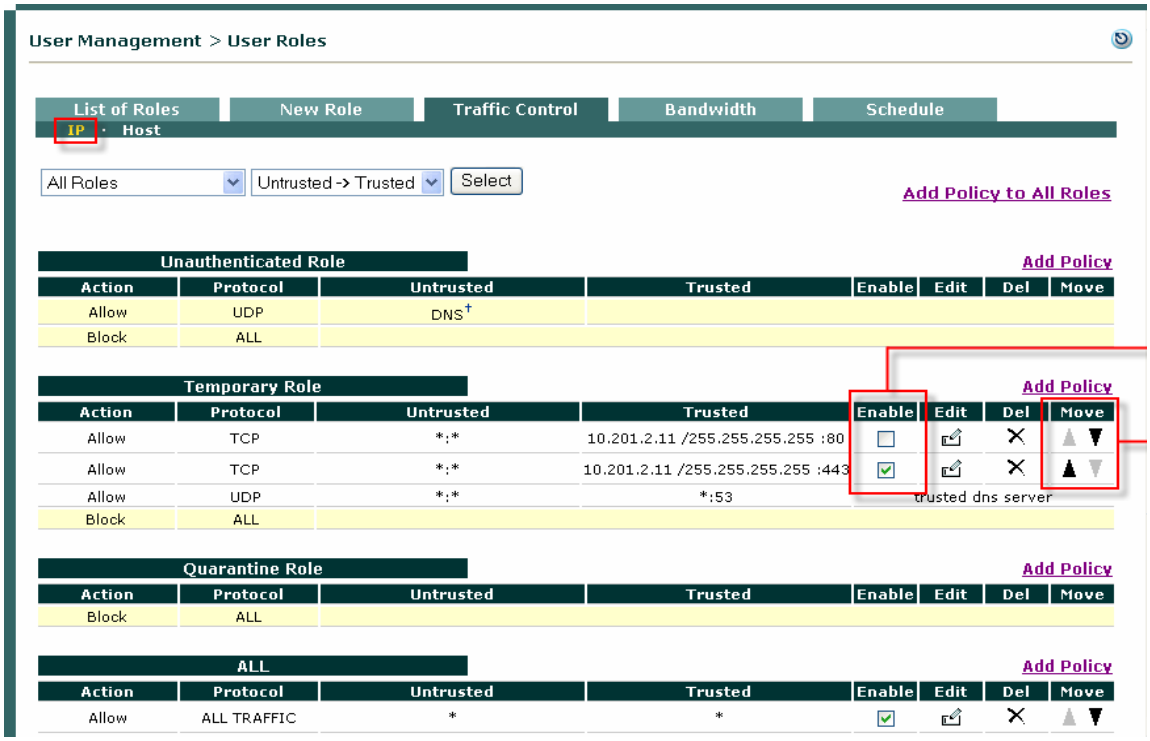


Figure 30. IP based traffic policy window

Step 9 – Select an existing role created, for example role1in Figure 29 and click on 'add policy'. Within the add IP policy window in Figure 31, in the protocol field choose 'TCP' as the allow protocol to be used by unauthenticated users. Enter IP address/subnet and ports for the untrusted network (connected to eth1). Enter also IP address/subnet and ports for trusted network (connected to eth0). The IP address for the untrusted network is the IP address block for all internal networks represented by VLANs in Table 3. It is possible to create separate roles for each VLAN if a single IP address block is not possible. Allow other options untouched as shown in Figure 31. Click on 'add policy' button to implement policy.

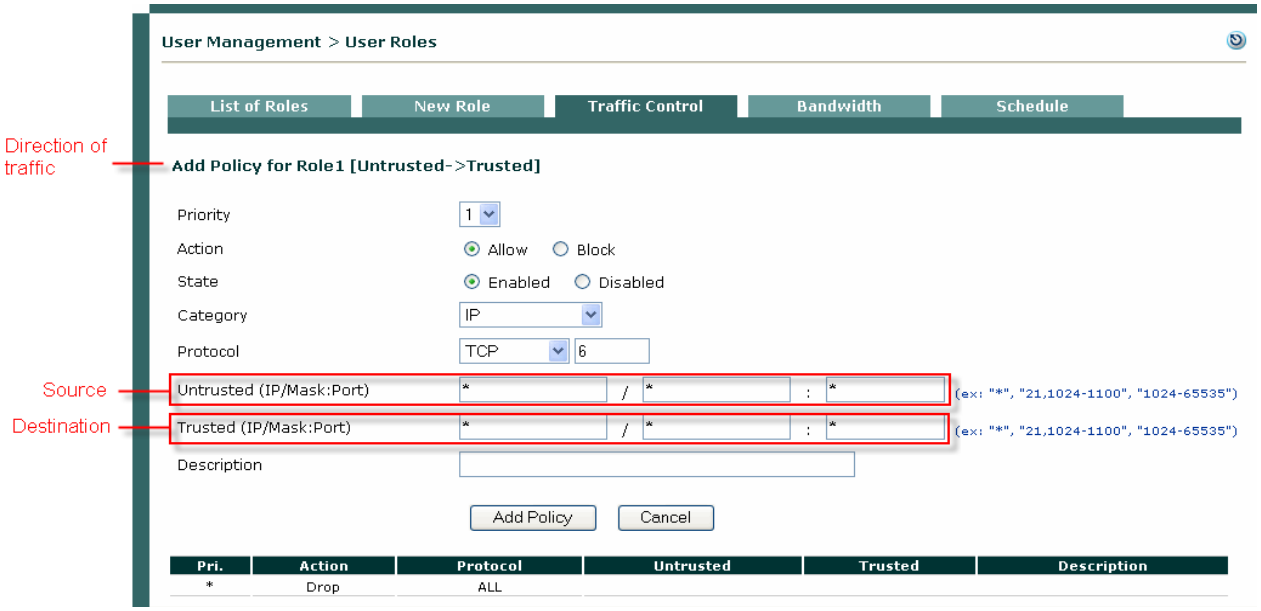


Figure 31. Configuring IP based traffic policy for Role1

8.6 Configuring Bandwidth Control

In a network environment where bandwidth availability and how it is being used is very important, Cisco NAC appliance can help regulate bandwidth by user role. First on the CAS connected to bandwidth sensitive network segment, enable bandwidth management and click on update button. To accomplish this, go to device management, 'CCA servers', 'manage (CAS_IP)', 'filters', 'roles' and 'bandwidth'. Next, from the 'user management', click 'user roles' follow by 'bandwidth'. Click edit button next to the role you want to configure bandwidth limits. The bandwidth window form opens as shown in Figure 32. Enter desire bandwidth information. Choose 'all users share the specify bandwidth' for share mode and click on save button. Session time out for each role can be configured by going to 'schedule' and 'session timers' but however, default session time out is 4 minutes. [19, 20]

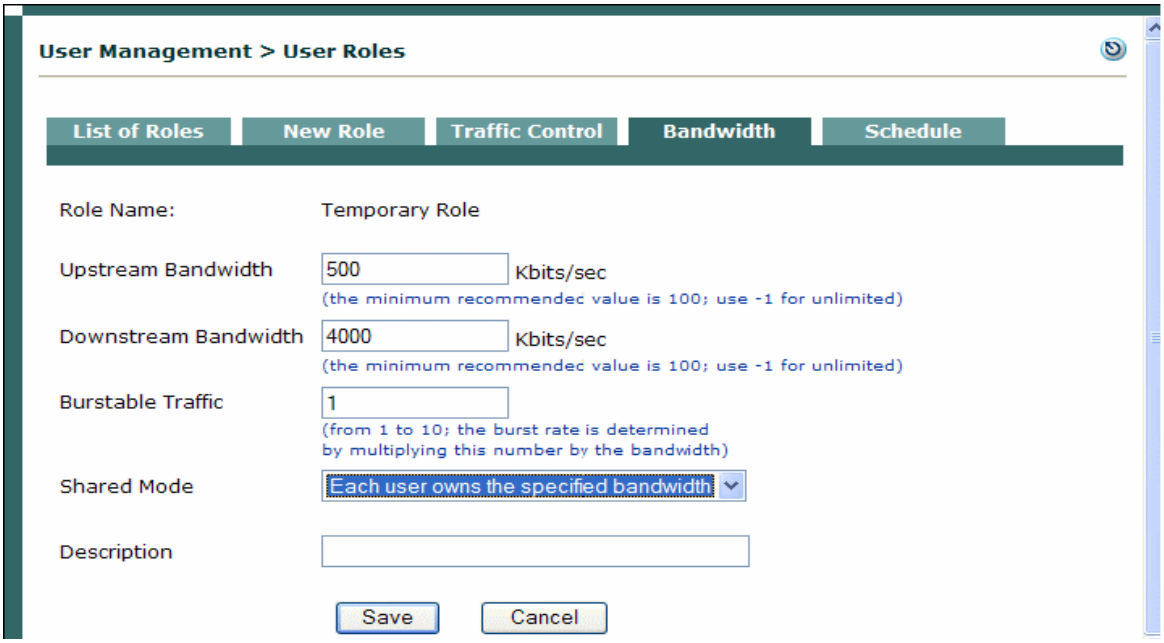


Figure 32. Configuring bandwidth for temporary role

8.7 Configuring Temporary Role

The temporary role is used to place users requesting network access while their computers are being checked for any vulnerability. Select temporary role by going to ‘user management’, ‘user role’ and ‘traffic control’ as shown Figure 33. Click on ‘add policy’ link to configure temporary role. A temporary role window like the one in Figure 31 will appear. In the trusted (IP/mask:port) field enter the IP address of the CAM and port 80. This will allow temporary role users only access to CAM server when system check is on. [19, 20]

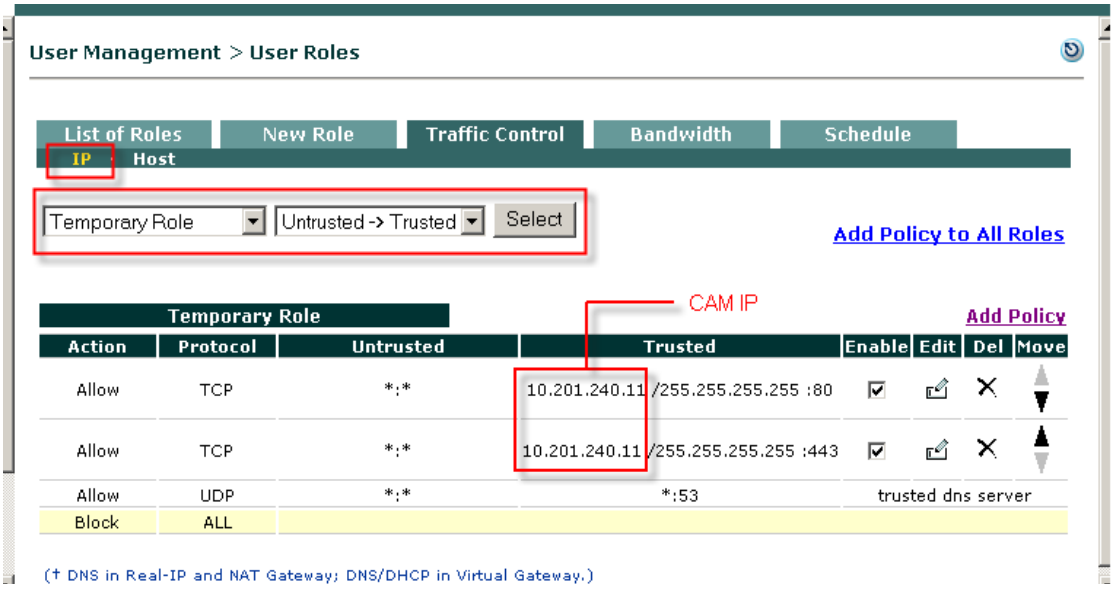


Figure 33. Configuring temporary role

8.8 Configuring Quarantine Role

In configuring the quarantine role, select quarantine role in Figure 29 and click on ‘add policy ‘. In Figure 34, fill in the IP address block for all VLANs in the untrusted text field along with allowed communication ports (for example port 80 and 443). In the trusted text field, enter only the IP address of the CAM and port 80,443. [19, 20]

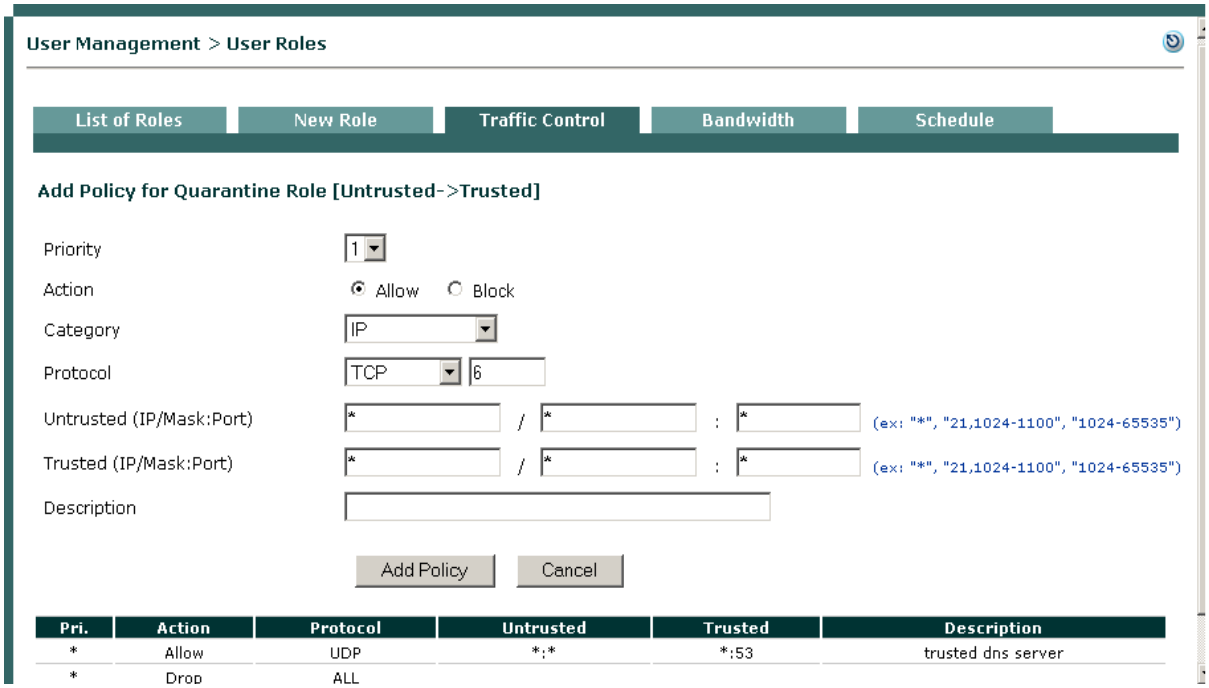


Figure 34. Configuring quarantine role

8.9 Configuring Network Scanning

Cisco NAC appliance uses Nessus plugin to perform network vulnerability assessment. Cisco NAC only support Nessus version 2.2 and can be downloaded from Nessus website. Nessus plugin is loaded to the CAM and the CAM then distributes it to all CAS in CAM domain. Figure 35 shows how to upload Nessus plugin file to the CAM. The file could be a bundle with .tar.gz extension or individual downloaded files from Nessus website with .nasl extension. To upload plugin files, go to Device management, 'clean access', 'network scanners' and plugin updates. To view a list of uploaded plugins, go to, Device management, 'clean access', 'network scanners', 'scan setup' and 'plugins. Within the plugin window, click 'show plugin' dropdown menu. [19, 20]

Nessus scanning can be associated with the temporary role. This is very useful because Nessus plugin checks computer for any vulnerability while in temporary role before full access to network is granted. To associate Nessus scanning with temporary role, follow these steps:

Step 1 - Go to device management, 'clean access', 'network scanner', 'scan setup' and plugins.
Step 2 - Select 'temporary role' from user role and select windows for operating system.
Step 3 - Select desired plugin or 'all' from show plugins dropdown menu as shown in Figure 36.
Step 4 - Check 'enable scanning with selected plugin' and click update button.

Figure 35.Uploading Nessus plugin

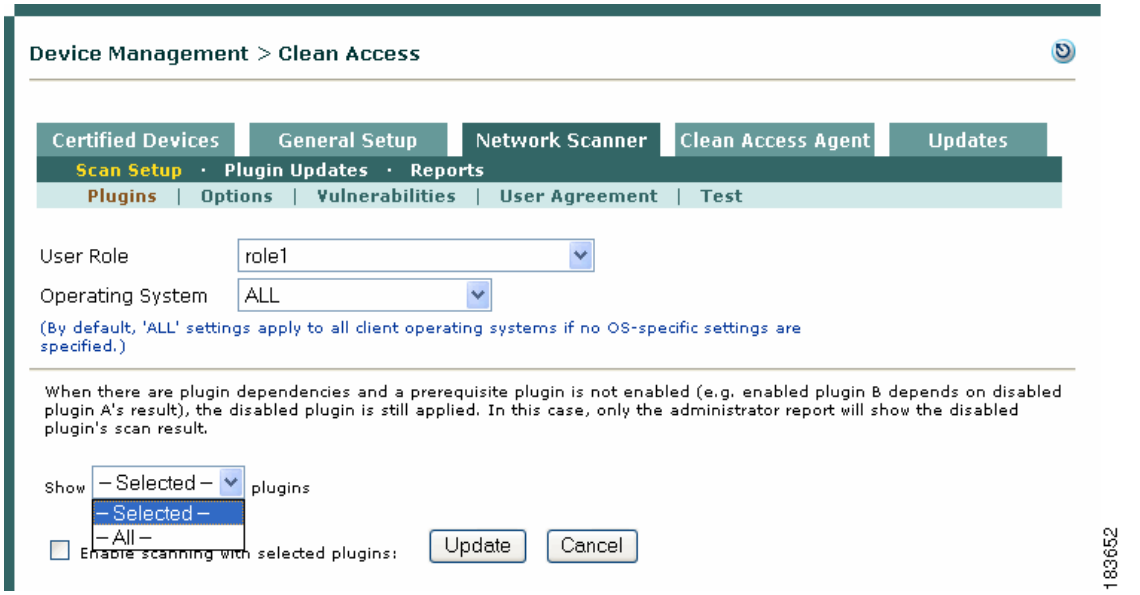


Figure 36. Associating Nessus plugin with temporary role

8.10 Configuring Vulnerability

The vulnerability feature ensures how the end user who wants to access network will respond when vulnerability is found on his or her computer. Access the vulnerability configuration form by going to Device management, ‘clean access’ ‘network scanner’, ‘scan setup’ and vulnerabilities. Within this form, select ‘temporary role’ for user role and ‘windows_all’ for operating system. Next, select the Nessus plugin ID, name and vulnerable if option. The ‘vulnerable if’ is an option that specifies what action will be taken if a scan match is found. In Figure 37 an example of vulnerability configuration is shown. It is recommend to select ‘HOLE’ for the vulnerable if option. This is because all computers in the network are running F-secure client security or any other antivirus software with personal firewall. With ‘HOLE’ option, a computer is put to quarantine role if a vulnerability match is found after scanning. To edit a plugin ID, click on the edit icon associated with the plugin; an edit plugin form appears as shown in Figure 38. Within this form, it is recommended to type in the ‘link’ text field the web address to redirect users to go and solve the vulnerability problems on their computers. [20]

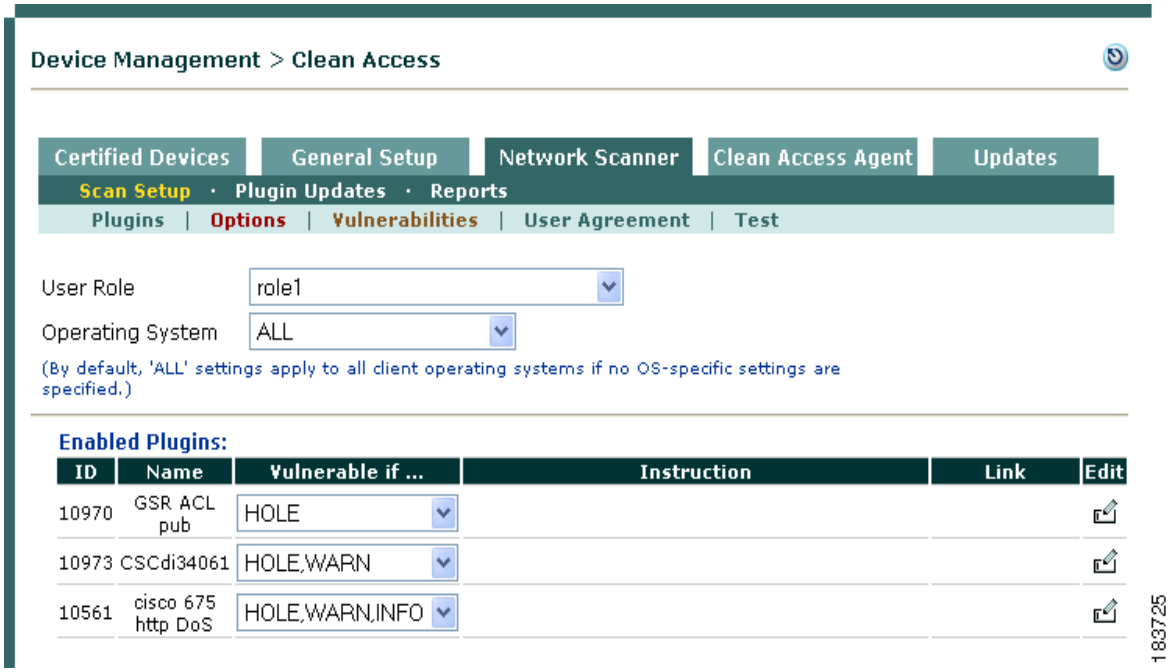


Figure 37. Configuring vulnerability for temporary role

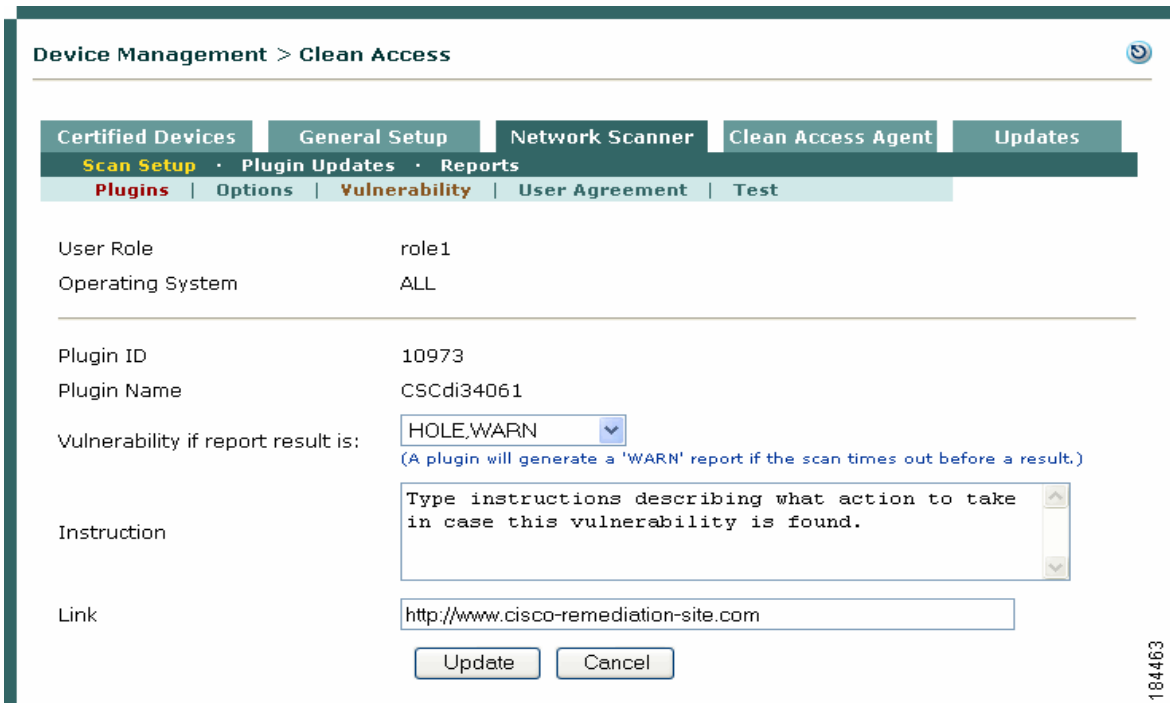


Figure 38. Editing plugin ID

8.11 Configuring User Agreement Page

The user agreement page is a page that appears when user initiates login and network scanning has been performed on user's computer. When no vulnerability is found after scanning, the agreement page appears with 'accept' and 'decline' buttons. However, if vulnerability is found, the page appears only with 'report' and 'logout' buttons. Figure 39 show user agreement configuration form. Steps to configure user agreement are as follows: [19, 20]

Step 1 - For user role, select 'temporary role' and select 'windows_all' for operating system
Step 2 – In the 'information page message' field, enter the HTML file that conveys a message about company security policy to end user.
Step 3 – Allow other options on Figure 39 untouched and click update button.
Step 4 – Follow step 1-3 to create user agreement for quarantine role. Select quarantine role as user role; for operating system choose windows.

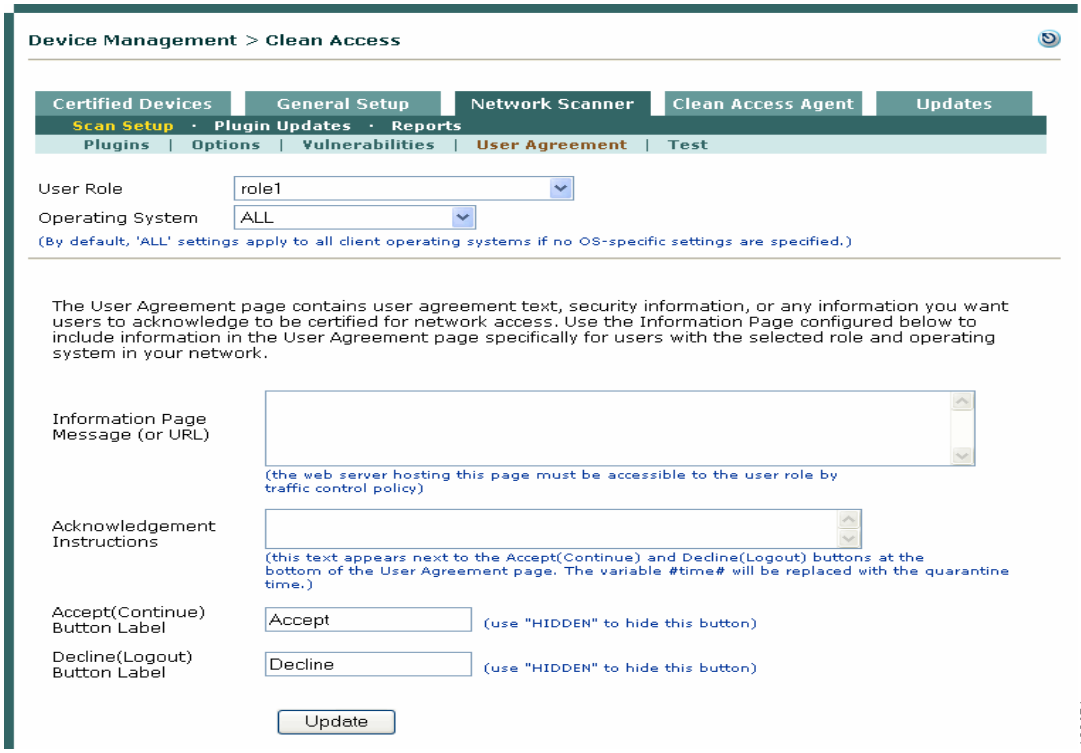


Figure 39. Configuring user agreement for temporary role

8.12 Configuring CAM Updates

Configuring CAM update is necessary when a company is required to be up-to date with recent version of CAM software. Follow these steps to configure CAM updates. [20]
Step 1- Go to Device management, ‘clean access’ and updates
Step 2 – Within the update form shown in Figure 40, the time for CAM to automatically check for updates should be same as that configure for windows update on every end computer. This is very useful because, at every given time, windows update patch files will be current and network users will not be quarantine because of vulnerability in their operating system.
Step 3 – Uncheck ‘check for Macintosh clean access agent updates’ and ‘check for Cisco NAC web agent’ because it not needed in this project.
Step 4 – click update button.

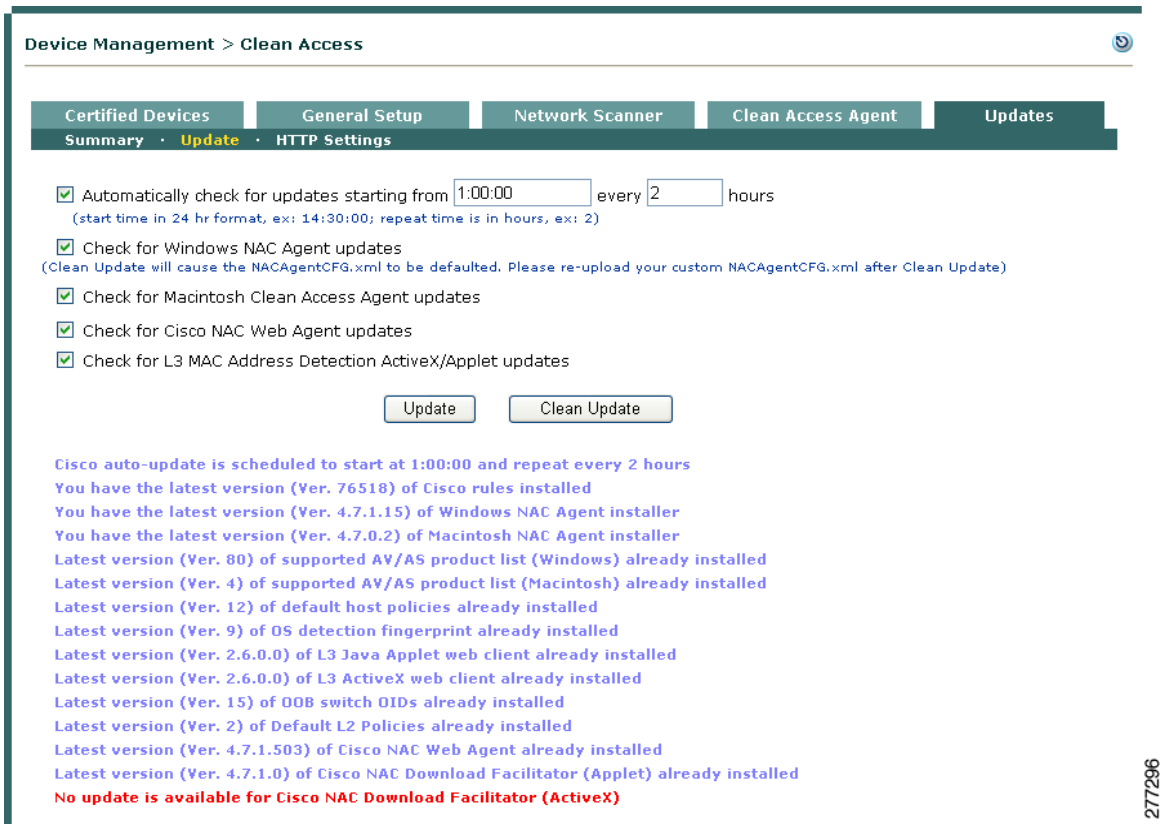


Figure 40. Configuring CAM updates

8.13 Configuring Cisco NAC Agent Distribution

Cisco NAC agent software has to be distributed to all computers in the network that will need network access. Agent software will not be used to login into the network but will run in the background of Active directory single sign-on to communicate computer posture to the CAS sever. To distributing Cisco NAC agent software, the followings steps are necessary: [20]

Step 1- Go to Device management, ‘clean access’, ‘clean access agent’ and distribution as shown in Figure 41. Browse and upload current version of NAC agent software and click on update button.
Step 2 – Click ‘installation’ from the menu bar, fill information as shown in Figure 42 and click on update button. The ‘discovery host’ IP address is automatically generated; it is the IP address of the CAM. For this project it should be 172.16.33.2
Step 3 – When an AD SSO (Active directory single sign-on) domain user initiate login for the first time and launches a web browser, the user is directed to Figure 43 to download and install Cisco NAC agent on computer in order to have full network access.

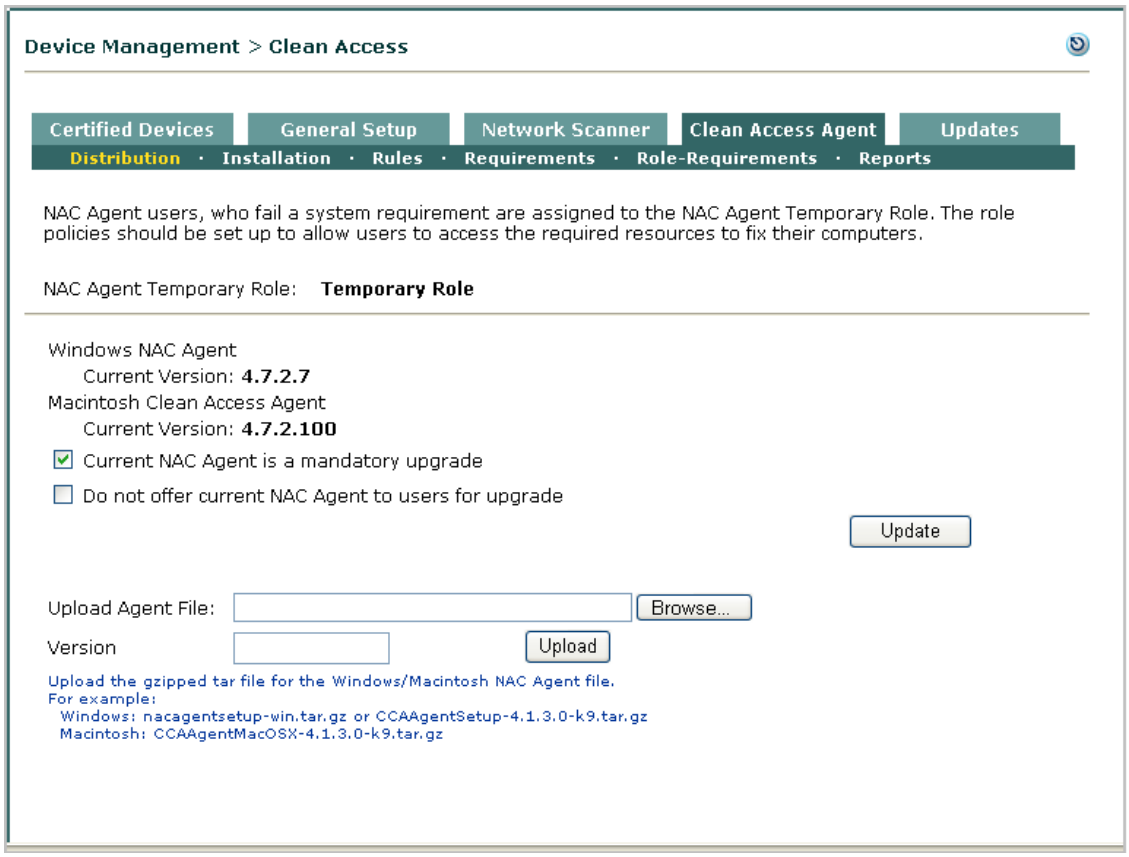


Figure 41.Configuring NAC agent distribution

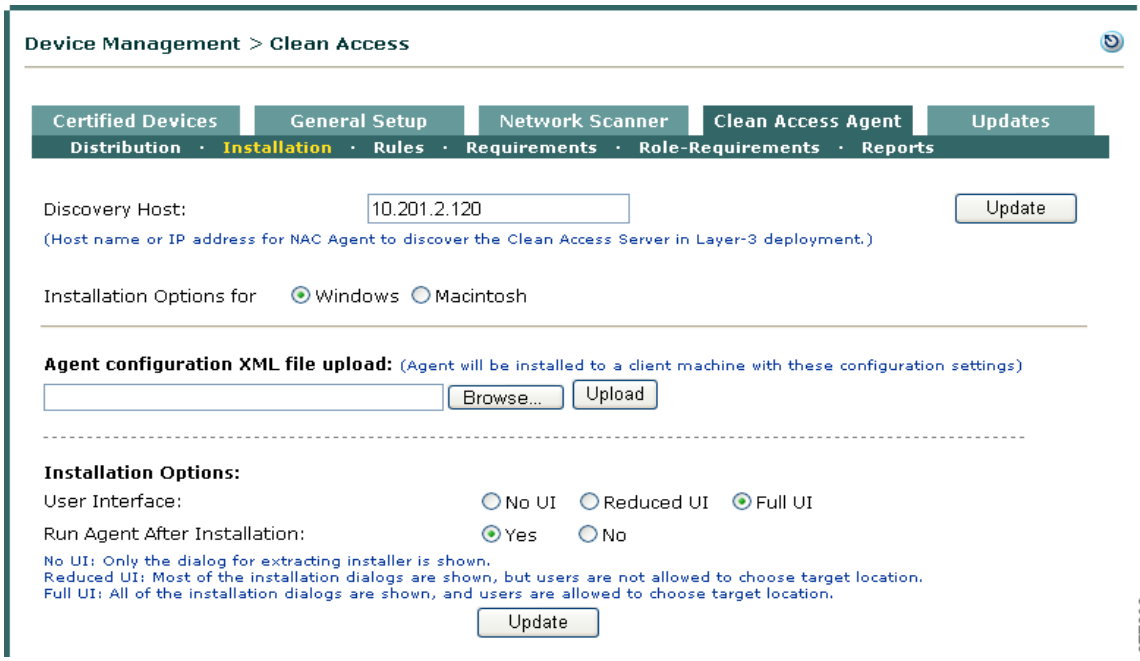


Figure 42. Configuring NAC agent installation

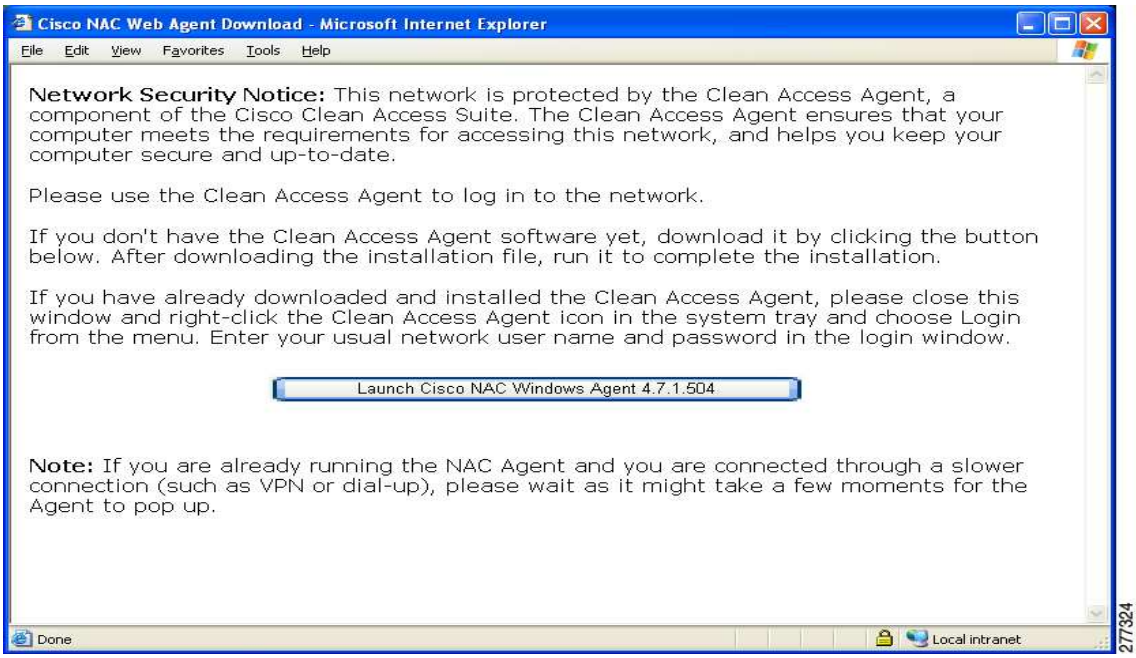


Figure 43.Information page to download and install Agent software

8.14 Configuring DNS Server for CAS

All CAS in the CAM domain must be configured to synchronize with the DNS server. To accomplish this, go to Device management, ‘CCA server’,’ manage (CAS_IP)’, ‘Network’ and ‘DNS’. Enter 172.16.33.10 for DNS server, ‘savoteku.local’ for host domain as shown in Figure 44 and click update button. [20]

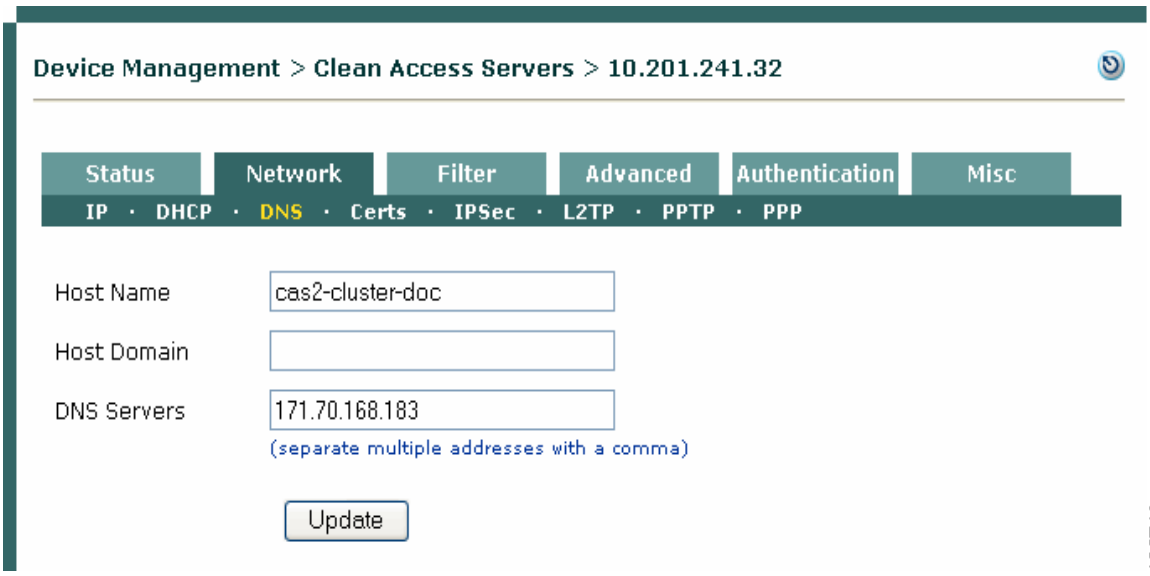


Figure 44. Synchronizing CAS with DNS server

8.15 Configuring Manage Subnet and Static Route for CAS

All CAS in the CAM domain except for CAS7 are configured with ‘managed subnet’. This is because these CAS are configured for L2 deployment. This ‘managed subnet’ are subnets represented by VLANs in Table 3. The VLANs subnets can be added individually. To configure managed subnet, go to device management, ‘CCA server’, ‘manage (CAS_IP)’, ‘advanced’ and managed subnet as shown in Figure 45. Add the individual VLANs and check ‘enable subnet-based vlan-retag’. [19]

CAS7 is configured with static route because it is deployed in L3 mode. It is also placed behind vpn concentrator which is integrated in Cisco 3945 router. To configure static route for CAS7, click on ‘static routes’ tab within ‘advanced’ tab of managed CAS7.Enter network connected to eth1 and default gateway. Network connected to eth1 is found in Figure 5. [19]

To configure IPSEC VPN (IP security virtual private network) for CAS7, go to, ‘Device management’, ‘CCA server’, ‘manage (CAS_IP)’, ‘Network’ and ‘IPSEC’. Within the IPSEC form as shown in Figure 46, choose ‘enforce’ from ‘vpn policy for clean access server’ dropdown menu. Enter preshared key, for example ciscokey. Leave other options in default and click on update. [19]

Configuring ARP entry for CAS7 enables Internet vpn clients to have smooth connection to the internal network. To configure ARP entry for CAS7, click on ARP tab as shown in Figure 47 for managed CAS7. Enter network connected to eth0, eth1 as shown in Figure 5 and click on ‘add ARP entry’ button. [19]

Adding VPN concentrator to CAS7- the VPN concentrator must be added to the CAS to enable VPN client traffic to pass through the CAS for posture assessment. To accomplish adding VPN concentrator to CAS7, go to, Device management, ‘CCA server’, ‘list of servers’ ‘manage (CAS_IP)’, ‘authentication’, ‘vpn auth’ and ‘vpn concentrators’. Within the add VPN concentrator form in 48, enter concentrator name, IP address and the share secret between CAS7 and concentrator. [19]

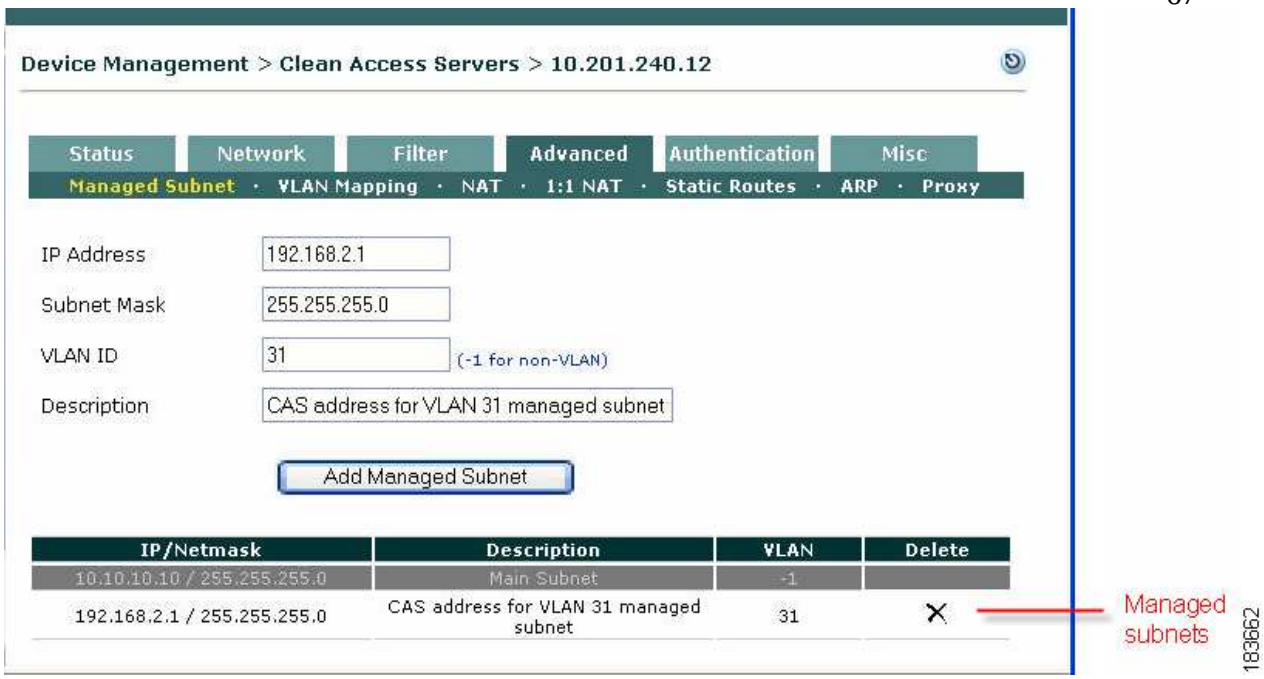


Figure 45. Configuring managed subnet

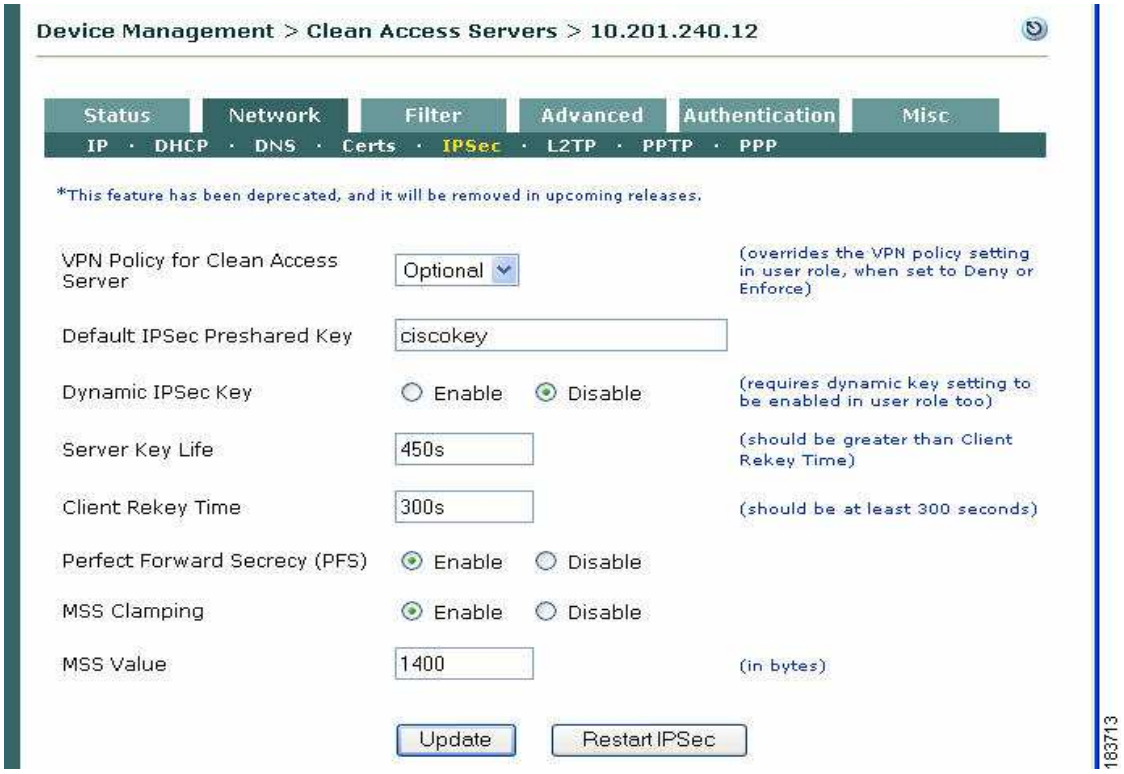


Figure 46. Configuring IPSEC

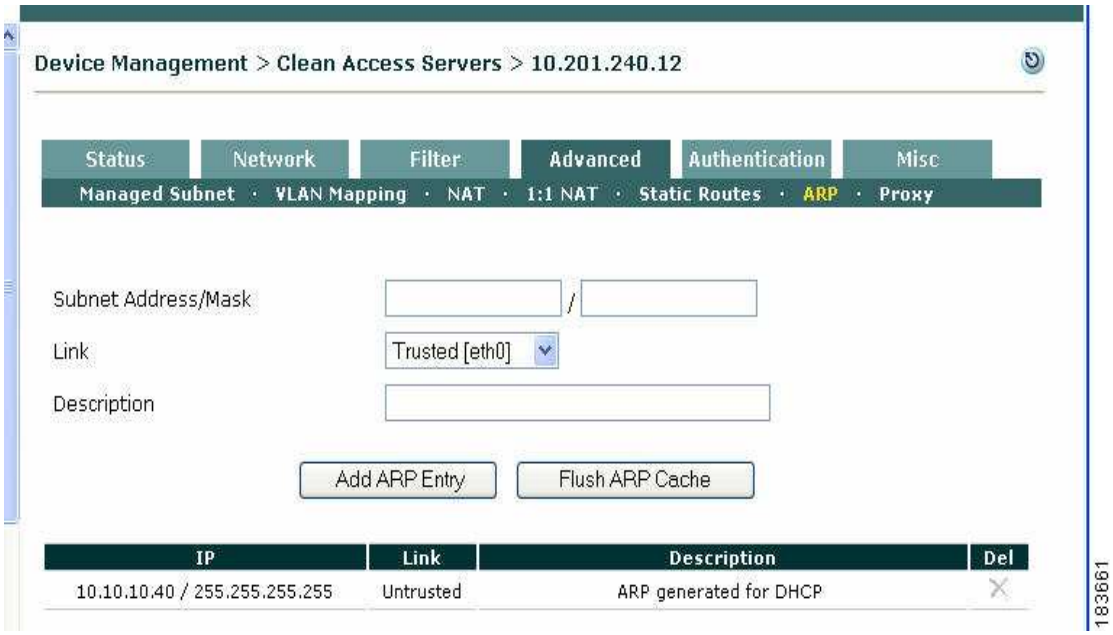


Figure 47. Configuring ARP entry

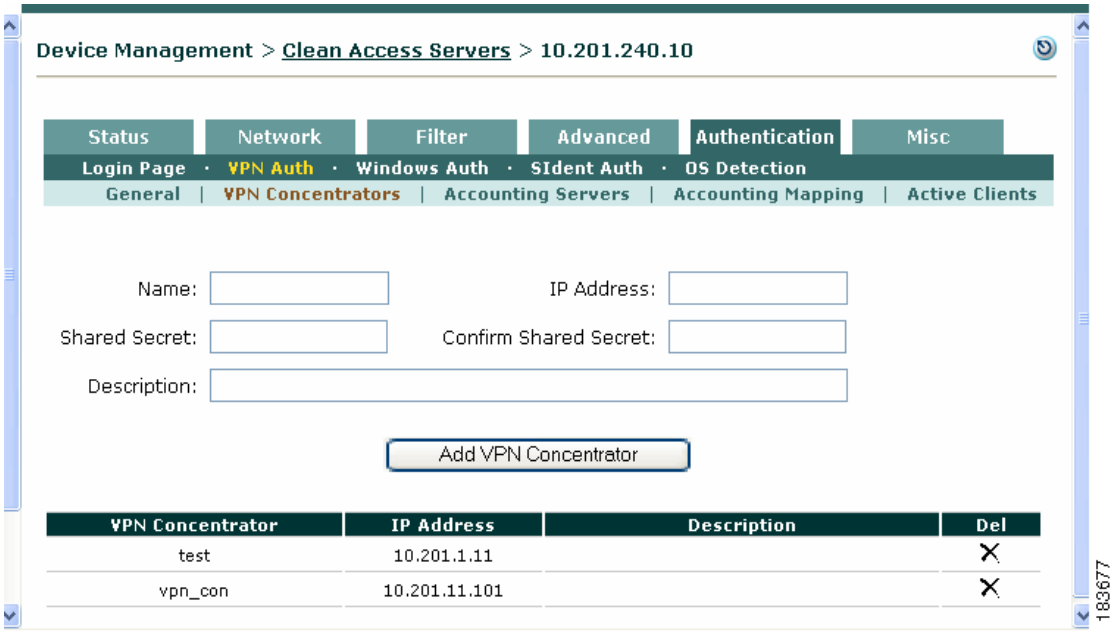


Figure 48. Adding VPN concentrator to CAS7

8.16 Configuring Active Directory Single Sign-On

AD SSO enables windows domain users to logon to windows domain without using Cisco NAC agent software. But however, Agent software must be installed on end user computer to facilitate in posture assessment when ever user wants to access the network. To configure AD SSO in a network environment, the following steps are outlined: [19, 21]

Step 1-install windows 2008 server on a dedicated server computer. Use 'add roles' to install active directory domain services as shown in Figure 49. After adding AD domain services role, go to start, 'run' and type 'dcpromo' and click ok. In the proceeding wizard, select 'create new domain in new forest' option and enter 'savoteku.local' as FQDN. Select windows 2003 forest and domain functional level. Accept installation of DNS integrated with AD.

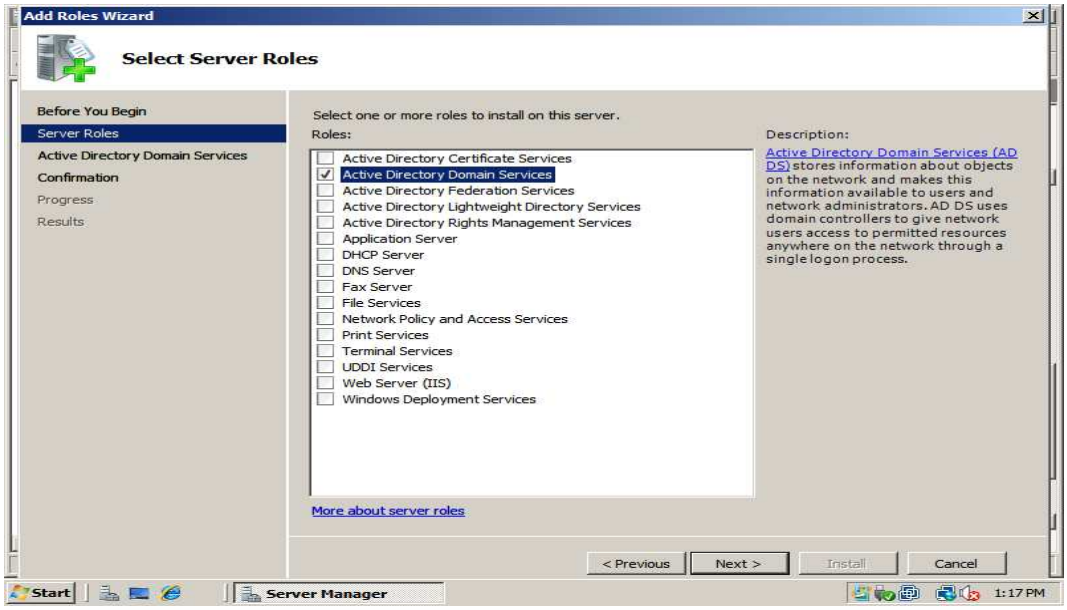


Figure 49. Adding AD domain service

Step 2- Creating network users accounts on windows 2008 server AD. In this example, three users' accounts are created, one for the network administrator, one for student and one for the purpose of synchronizing AD SSO. The account to synchronize AD SSO will not be assigned to any end user to the network. To create user account, go to start, 'programs', 'administrative tools', 'server manager'. Within the server manager window, click on 'Roles', 'AD domain services' and 'savoteku.local'. Right click on 'users' icon and choose new and 'user' as shown in Figure 50. In the new user form, enter information as shown in Figure 51. Click next, enter password and check 'password never expire'. Click next and 'finish'. Figure 52 shows highlighted user account called 'gipson mbah'. The network administrator and student user accounts are created with the same approach used to create the user account 'gipson mbah' . The option 'password never expires' should not be checked for these other accounts. Allow the default option, 'user must change password at next logon '. Six additional user CAS accounts have to be created for the purpose of synchronizing additional CASs in the network for AD SSO.

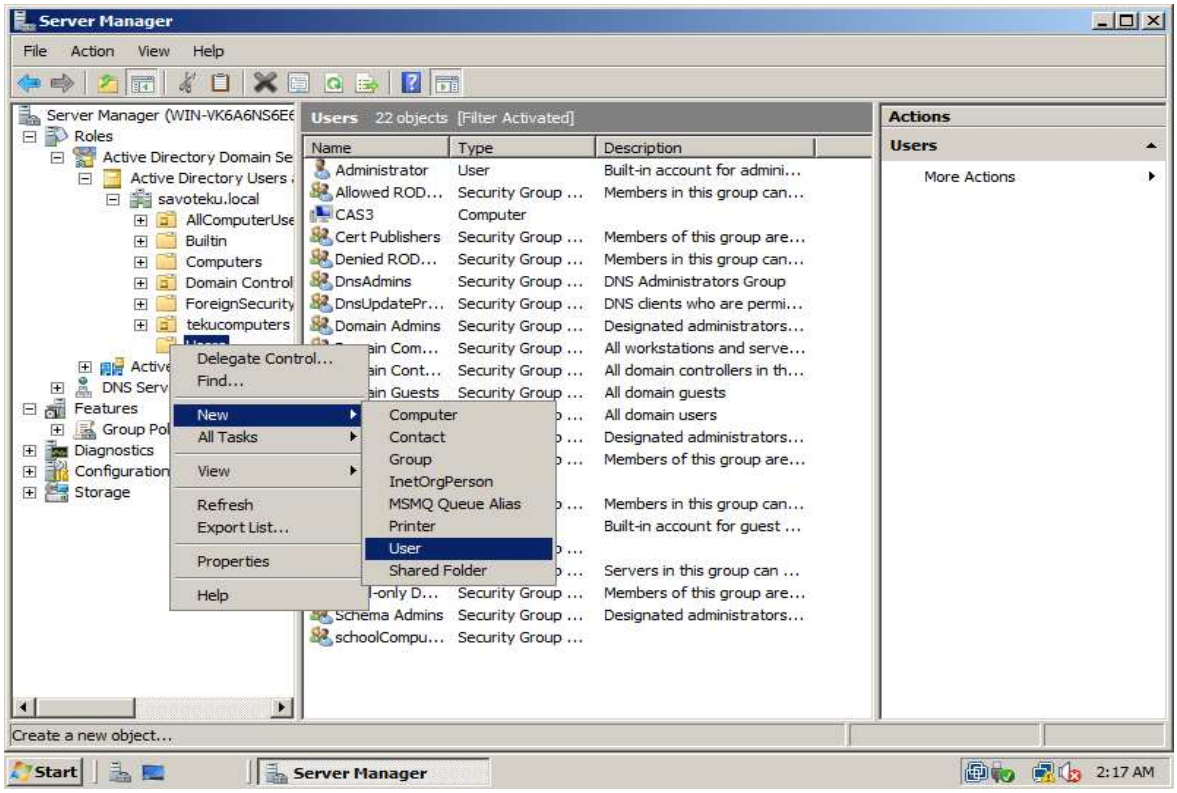


Figure 50. Configuring user account

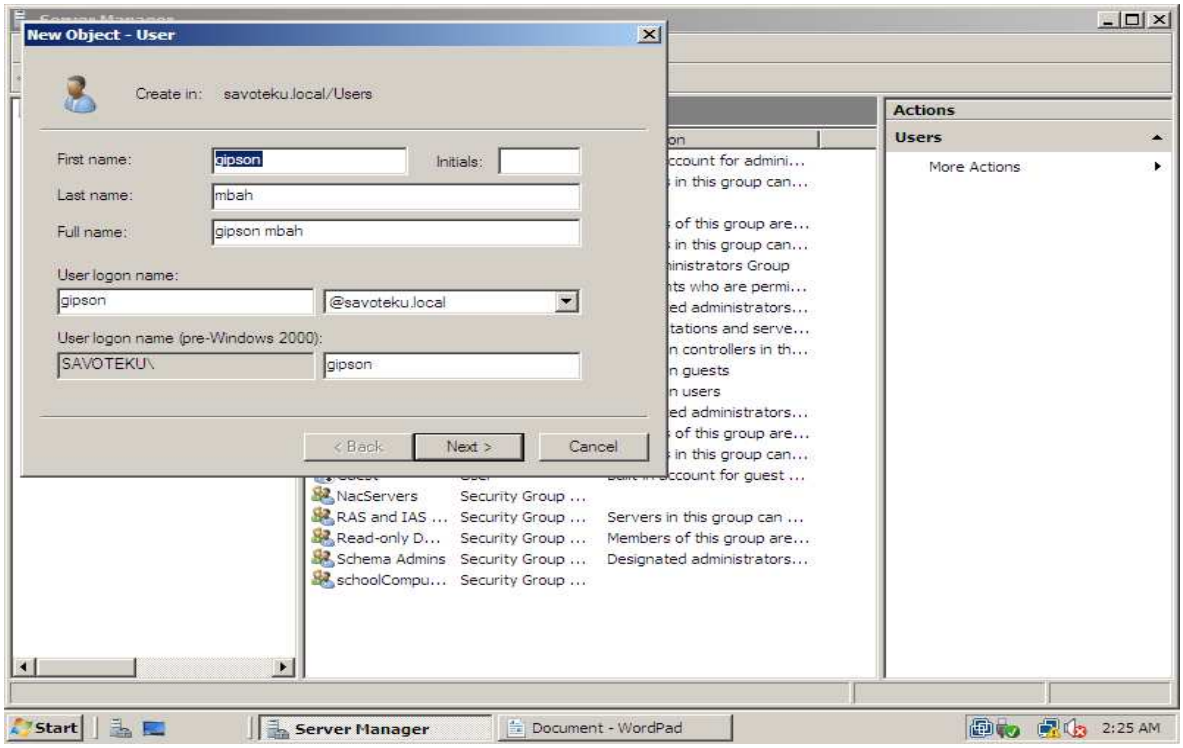


Figure 51. New user account form

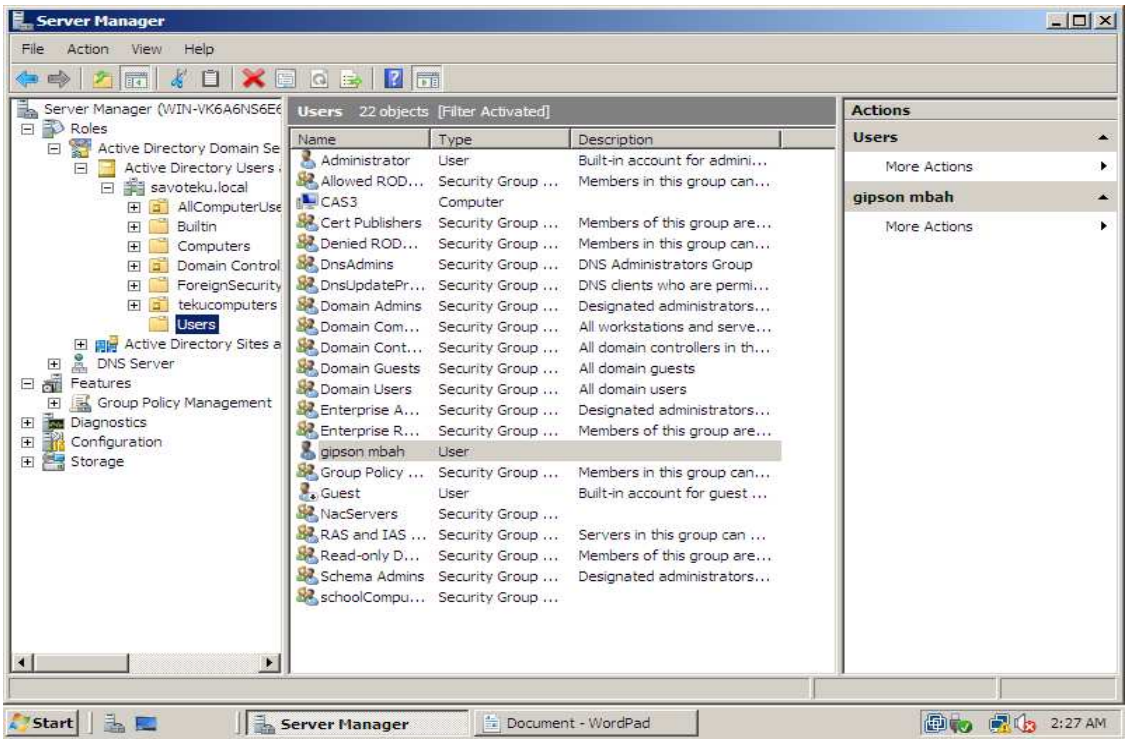


Figure 52.created user account

Step 3-Create computer accounts for clean access servers and network computers on AD. To create computer accounts, right click on ‘computers’, ‘new’ and computer in Figure 52. Within the new computer form, enter ‘hostname’ for the computer to be added to AD, for example CAS1 (clean access server one). To view a list of created computer and CASs accounts, double click on ‘Domain computers’ as shown in Figure 53. Domain computers and Domain users are default group accounts for computer accounts and user accounts respectively on AD.

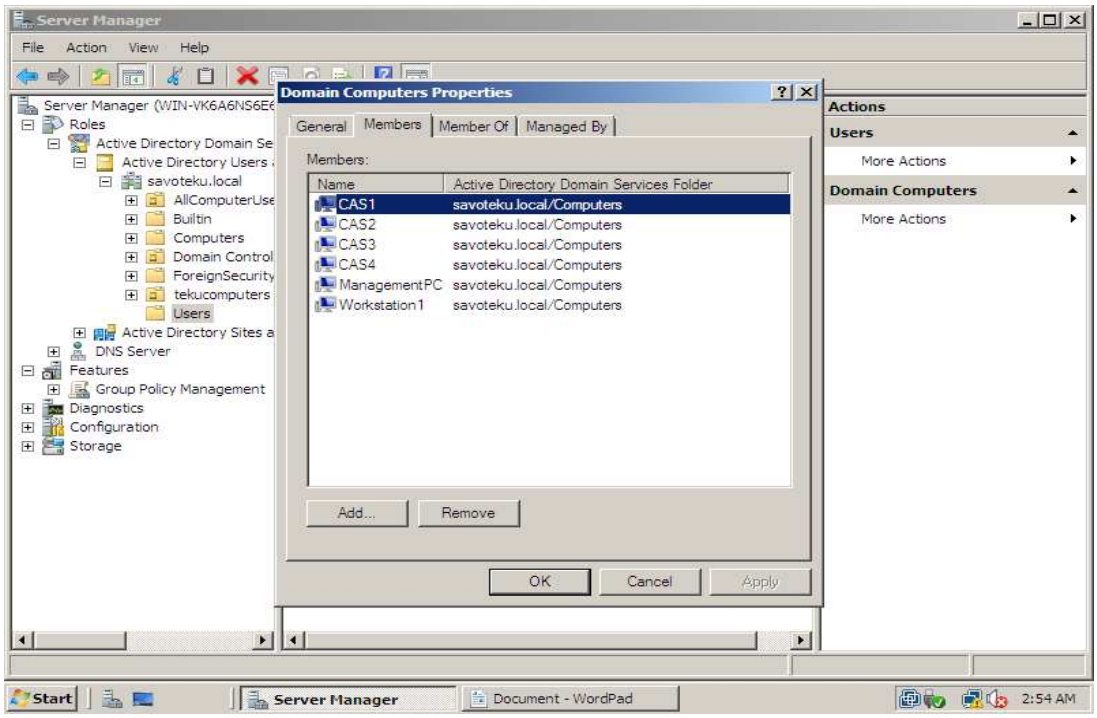


Figure 53.List of CAS and computer accounts

Step 4- Creating group accounts to accommodate for users, computers and CASs accounts created earlier. To create users group account, right click on 'users' icon and select new and 'group'. Enter group name and click ok button. To create computers group account, right click on 'computers' icon and select new and 'group'. Enter group name and click ok button. For simulation purpose, the following group accounts are created:

- CASPCgroup- to accommodate all CASs on the network
- schoolComputers- to accommodate all computers in teku campus
- StudentUsergroup- to accommodate all student user accounts
- StaffUsergroup- to accommodate all staff user accounts
- Enterprise Admin group account created by default will be used to accommodate network administrator user account.

To add computers or users to a group, double click the group and click on 'members' tab. Within the 'members' tab window, click on 'add' button and select group members as shown in Figure 54.

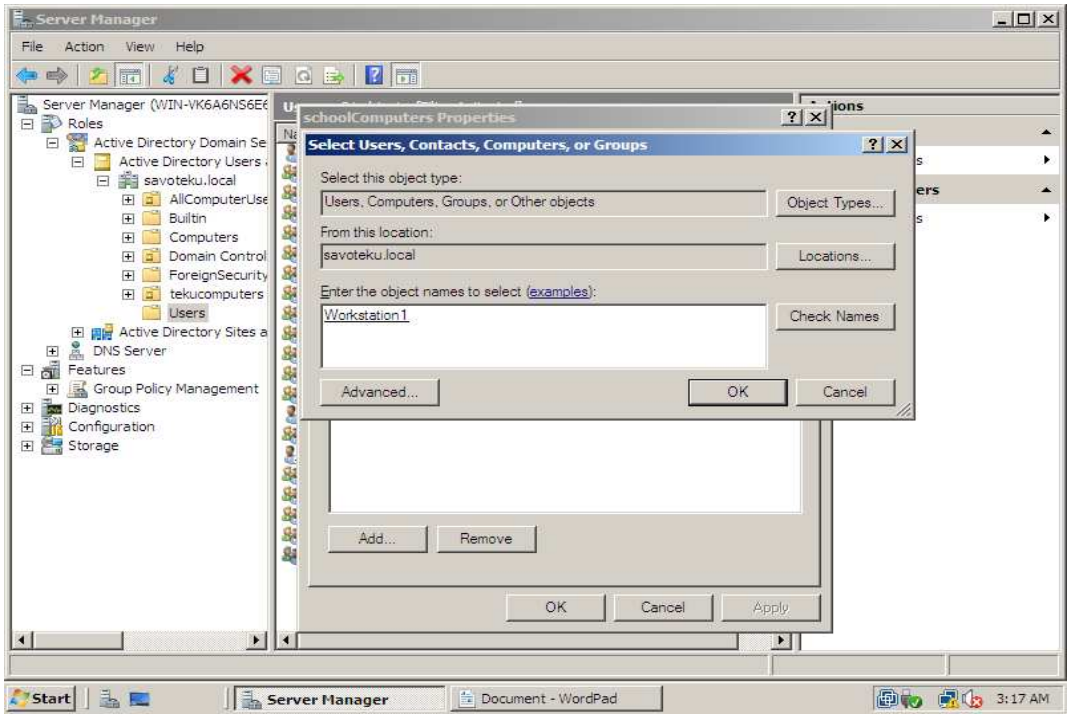


Figure 54.Adding computers to schoolComputers group

Step 5- Creating an OU (organization unit). An OU facilitate the assigning of group policies to user and computer groups. It also helps in software distribution over the network. Before a group policy can be applied to an OU, an OU must be created. Users, groups, computers and printers can later be placed in the OU. The structure of the OU depends on the company's needs. To create an OU, within the server manager, click 'features' follow by 'savoteku.local'. Right click on 'savoteku.local' and choose 'new organization unit' and enter name for OU. For simulation purpose, the following OUs are created as shown in Figure 55.

- AllcomputerUsers – this is a parent OU and contains three sub OUs, namely
  -savoniaAdmins, to accommodate network administators.
  -staff, to accommodate teachers.
  -students, to accommodate students
- savoniaComputers – this a parent OU and contain three sub OUs,namely
  -adminComputers, to accommodate network administrator computers.
  -tekuComputers, to accommodate computers for teku campus.
  -technopolisComputers, to accommodate computers at technopolis campus.

After creating OUs, computer groups and user groups have to be move into appropriate OUs in order to inherit the group security policy associate with the OU. To move a group into an OU, right click the group and choose move. Within the move dialog box, select the OU to add group and click ok. Figure 56 shows how to add computer group called 'schoolComputers' to 'tekuComputers' OU.

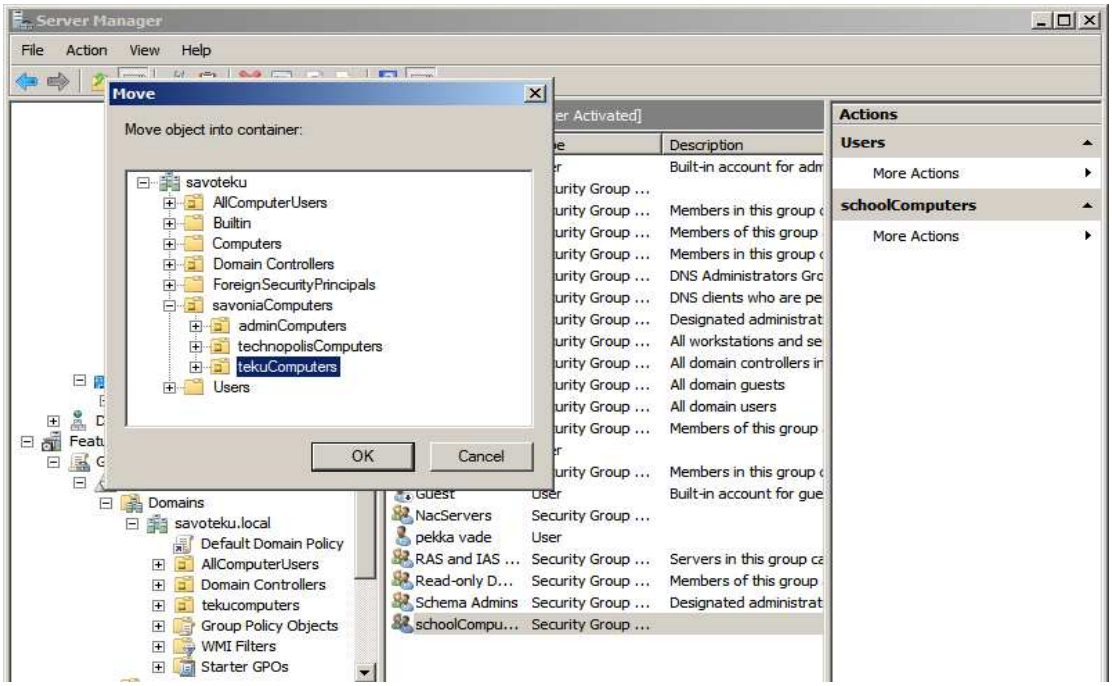


Figure 55. List of OUs created

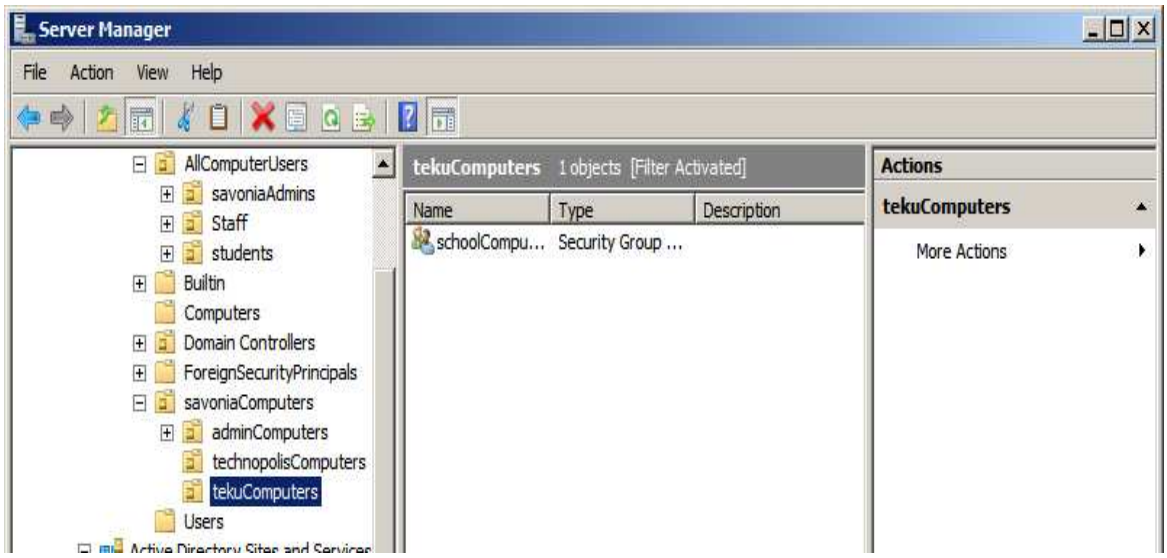


Figure 56. Adding computer group to tekuComputers OU

Step 6- Creating GPO (group policy). A GPO contains security settings which when associated with an OU, groups, users or computers placed into the OU inherit the security settings. In this example, one GPO is created for the student OU. The procedure for creating GPOs for other OUs is the same but however, the security settings must reflect the needs of the OU. The OU 'savoniaAdmin' must be granted limitless network privileges since it is administrators OU. To create a GPO for the students OU, within server manager, go to, 'features', 'savoteku.local', 'AllcomputerUsers' and 'students'. Right click on students and

choose ‘create a GPO in this domain, and link it here…’ Enter GPO name as ‘studentsGPO’ and click ok. Go to, ‘group policy objects’, right click on ‘studentsGPO’ created earlier and choose edit. The GPO management editor window opens as shown in Figure 57.

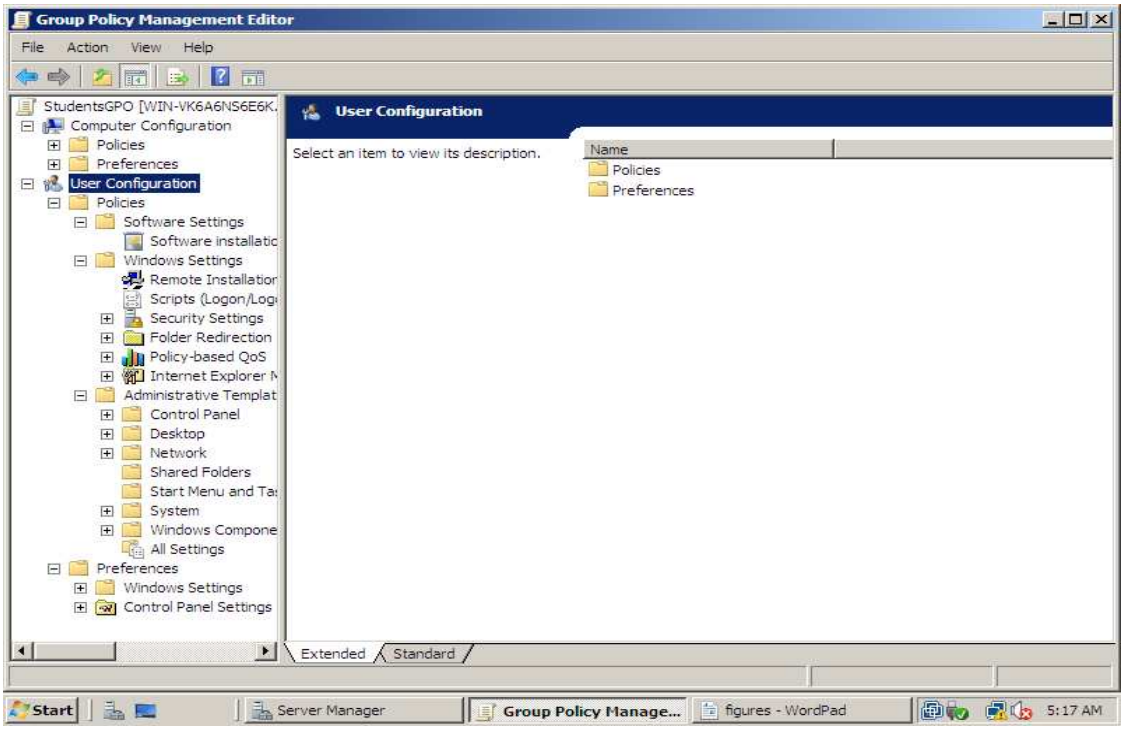


Figure 57. ‘studentsGPO’ group policy management editor

Within GPO management editor, on the left navigation bar, computer configuration is used to configure computer security settings regardless of who logs on to it. ‘user configuration’ is used to configure users’ security settings that move with users as they roam through out the savoteku.local domain; regardless of which computer user is logon. The following example outlines security settings configured for ‘studentsGPO’ organization unit and how to configure the settings:

1. Prohibit access to control panel: Go to, ‘user configuration’, ‘policies’, ‘administrative templates’ and ‘control panel’. Double click ‘prohibit control panel’ icon and choose enable follow by ok.
2. Prevent deleting/adding of printers: Go to, ‘user configuration’, ‘policies’, ‘administrative templates’, ‘control panel’ and ‘printers’. Double click ‘prevent addition and deleting of printers’ icons. Choose enable follow by ok.
3. Prevent access to windows connection wizards: Go to, ‘user configuration’, ‘policies’, ‘administrative templates’, ‘network’ and windows connection. Double click ‘prohibit access of windows connection wizards’ choose enable follow by ok.
4. Securing network critical options. The following item represented by numbers, 1,2,3,4,6,7,10,12,13,15,16,17,21 and 22, starting at the top of the page and found in the network connections windows must be enable. To accomplish this, go to, ‘user configuration’, ‘policies’, ‘administrative templates’, ‘network’ and network connections. Double click each item, choose enable follow by ok.

5. Securing sharing critical security features: Go to, ‘‘user configuration’’, ‘policies’, ‘administrative templates’ and ‘shared folders’. Within shared folder, double click items 1 and 2, follow by disable and ok.
6. Securing start menu features: Go to, ‘user configuration’ ‘policies’, ‘administrative templates’ and ‘start menu and task bar’. Enable items 58, 59, 61, 62 in the list by double clicking on each item, follow by enable and ok.
7. Securing system critical features: Go to, ‘user configuration’, ‘policies’, ‘administrative templates’ and ‘system’. Enable items 14, 15, 20, 23 in the list.
8. Securing Crtl+Alt+Del options: Go to, ‘user configuration’, ‘policies’, ‘administrative templates’, ‘system’ and ‘Crtl+Alt+Del options’. Enable the first item and disable all other items in list.
9. Securing system power management: Go to, ‘user configuration’, ‘policies’, ‘administrative templates’ and ‘system power management’. Enable the only available item.
10. Controlling user’s profile size: Go to, ‘user configuration’ ‘policies’, ‘administrative templates’, ‘system’ and ‘user profiles’. Enable fourth item on the list.
11. Configuring windows logon notification alert. This alert comes up when AD is not available to authenticate the end user. Go to, ‘user configuration’, ‘policies’, ‘administrative templates’, ‘windows components’, and ‘windows logon option’. Enable third item on the list.
12. Setting password policy: Go to, computer configuration, ‘policies’, ‘windows settings’, ‘security settings’, ‘account policies’ and ‘password policy’. Within the password policy window, double click each item and enter information as shown in Figure 58.

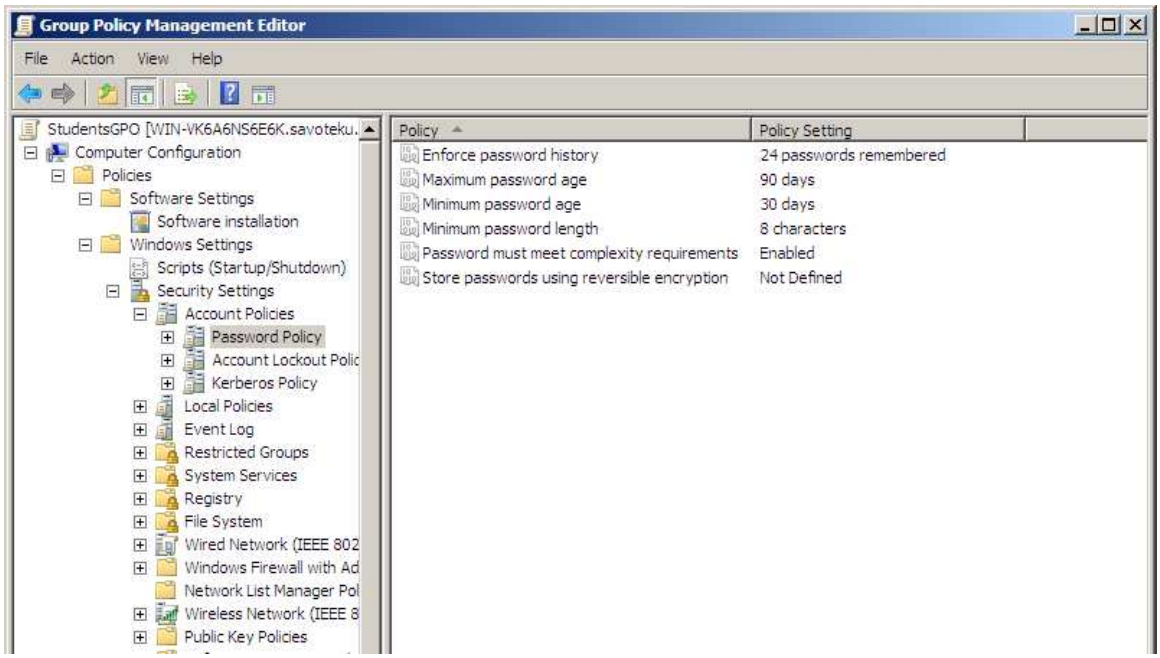


Figure 58. Configuring password policy

13. Configuring account lockout policy: Go to, ‘computer configuration’, ‘policies’, ‘windows settings’, ‘security settings’, ‘account policies’ and ‘account lockout policy’. Within account lockout policy window, double click item and enter information as shown in Figure 59.

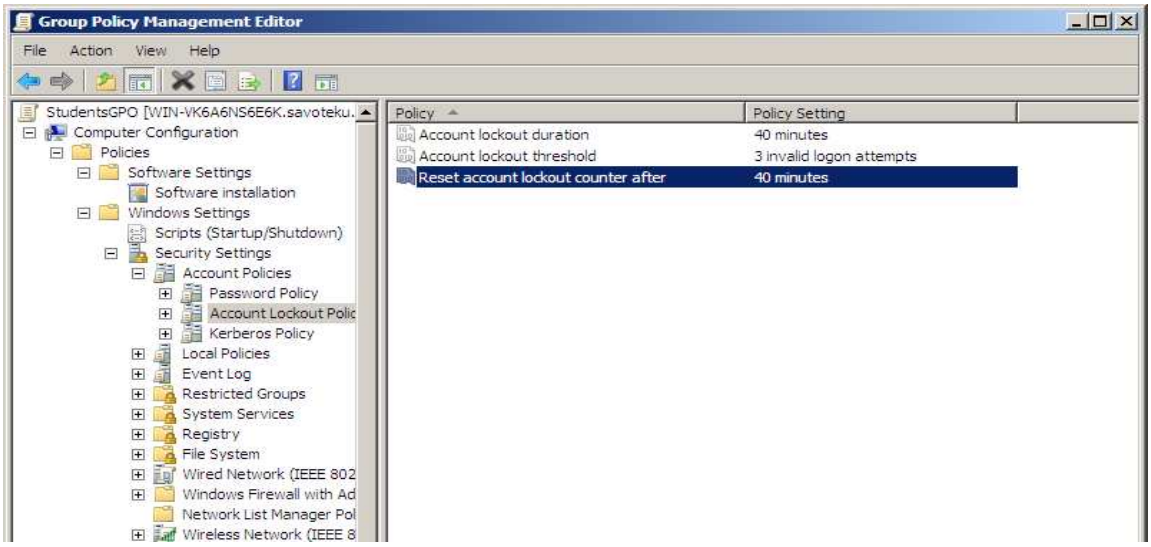


Figure 59. Configuring account lockout policy

14. Configuring Kerberos authentication feature : Go to, ‘computer configuration’, ‘policies’, ‘windows settings’, ‘security settings’ ‘account policies’ and ‘Kerberos policy’. Within Kerberos policy window, double click each item and enter formation as show in Figure 60.

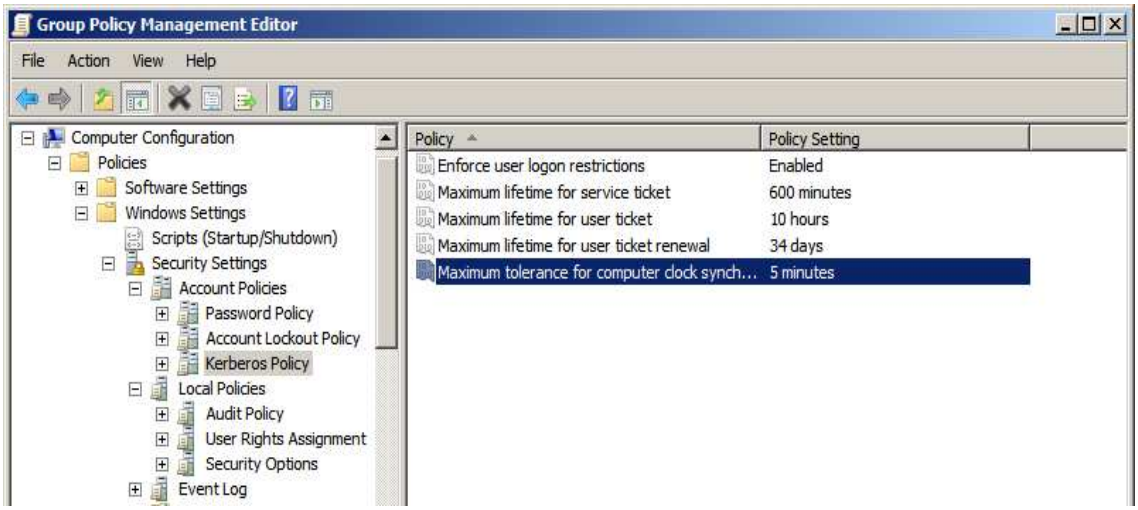


Figure 60. Configuring Kerberos policy

15. Configuring AD audit policy for ‘studentUsergroup’ group. Go to, start, ‘programs’, ‘administrative tools’ and ‘active directory users and computers’. Access the view menu and click ‘advanced features ‘. Right click on ‘users’ icon follow by properties. Within the properties window, select ‘security’ follow by ‘advanced’ option. In the advanced security settings form for users, click ‘add’ and choose ‘studentUsergroup’ group for AD auditing as shown in Figure 61. Click ok and return to the ‘user properties’ dialog box. Select ‘object’ tab and check ‘protect to accidental deletion’. Click ok.

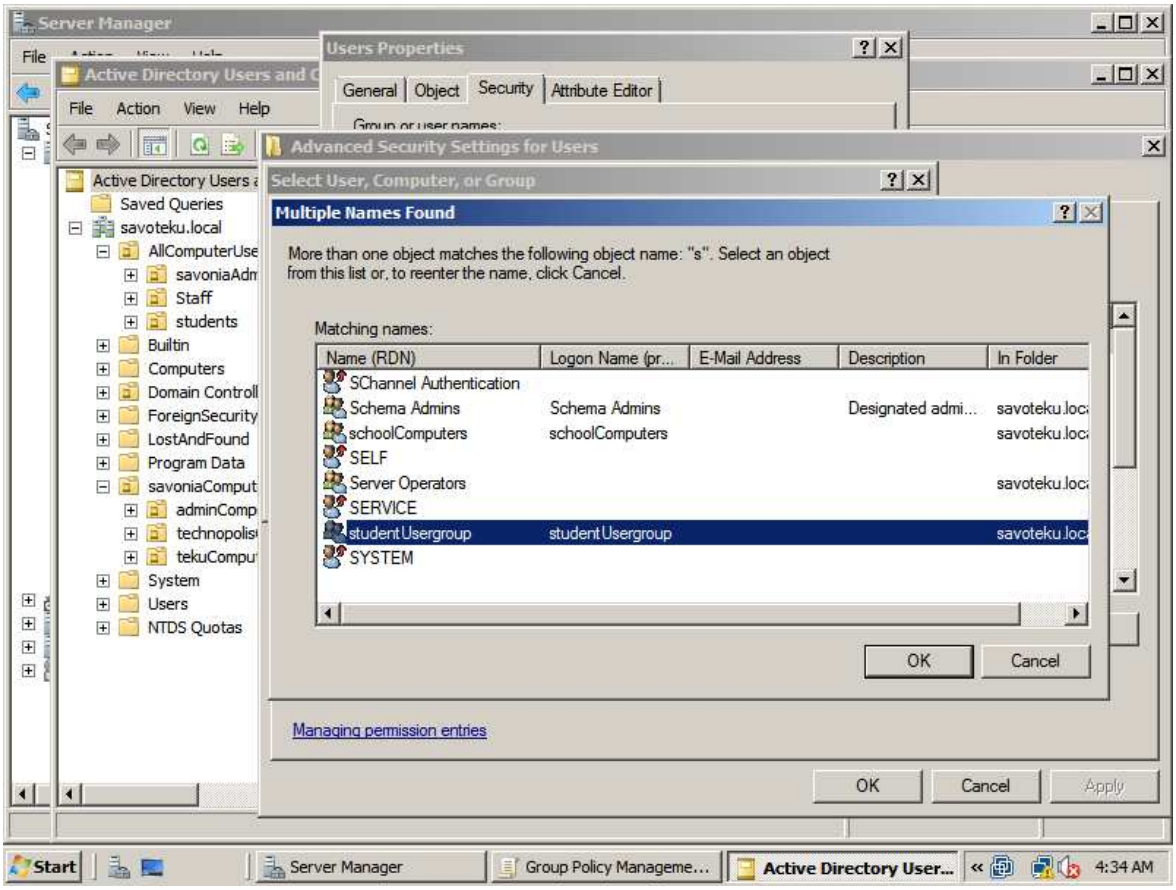


Figure 61. Configuring AD auditing for ‘studentUsergroup’ group

Step 7 – Creating DNS forward and reverse lookup zones. The DNS forward and reverse lookup zones are necessary for proper host to IP address resolving and vice versa. To configure forward lookup zones, within server manager, click on DNS server follow by DNS. Right click on ‘forward lookup zones’, ‘new zone’ and next. Within the new zone wizard form, choose primary zone follow by clicking next. Enter savoteku.local for forward DNS. Click next, ‘next’ and finish.
To create reverse lookup zone, right click on ‘reverse lookup zones’ and ‘new zone’. Click on next, accept ‘primary zone’; click next, ‘next’ and ‘next’. Enter 172.16 for the network ID portion. Click next and finish.

Step 8- Configuring CAM to support AD SSO. To accomplish this, go to ‘‘user management’’, ‘auth servers’ and ‘new’. Enter information as shown in Figure 62.

Step 9- Configuring traffic policy for CAS on active directory server. To accomplish this, go to, 'user management', 'user roles', 'list of roles' and policies (unauthenticated role) as shown in Figure 63. In the trusted (IP/mask: port), enter the IP address of the Active directory server, port numbers 88, 135, 389, 1025 and 1026 for supported ports. Allow other options on default and click on 'add policy' button.

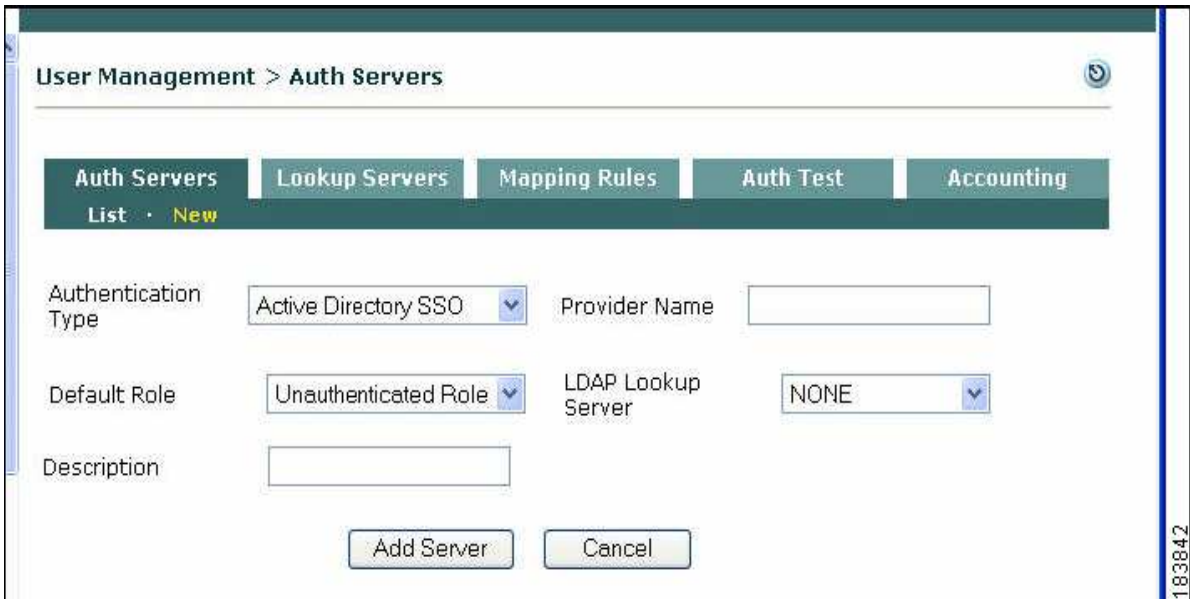


Figure 62. Configuring CAM for SSO

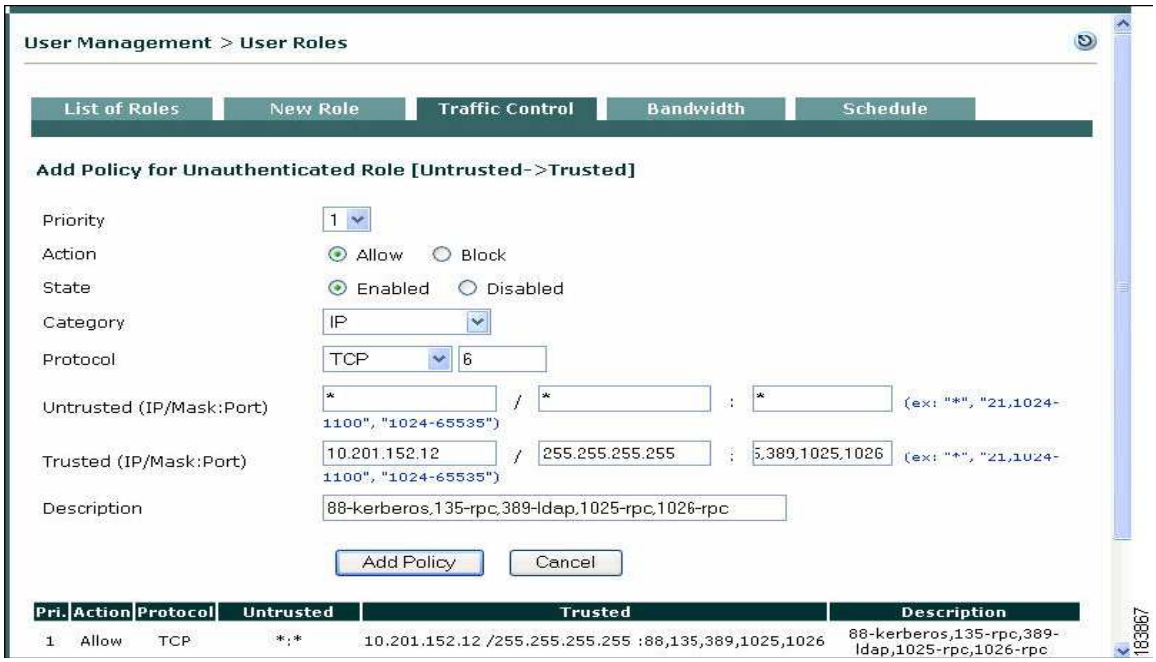


Figure 63. Configuring traffic policy for CAS

Step 10- Configuring all CAS to support AD SSO. To accomplish this, go to, Device management, 'CCA server', 'manage (CAS_IP)', 'authentication', 'windows auth' and 'active directory sso' as shown in Figure 64. Within the AD SSO form, do not check 'enable agent based windows single sign-on with active directory (Kerberos)' if active directory is running on windows 2003 server. It will be enabled later after configuration of active directory and executing KTPass in step 11. Next, choose 'single active directory sever' option, enter 'savotuku.local' for active directory domain and **ActiPC.savoteku.local** for FQDN. Where, ActiPC is the computer name for the AD server. Enter the CAS active directory user account name in 'account name of CAS' field and password in 'account password for CAS' field. In the 'active directory SSO auth server' filed, choose the name given to 'provider name' field in Figure 62. Click update.

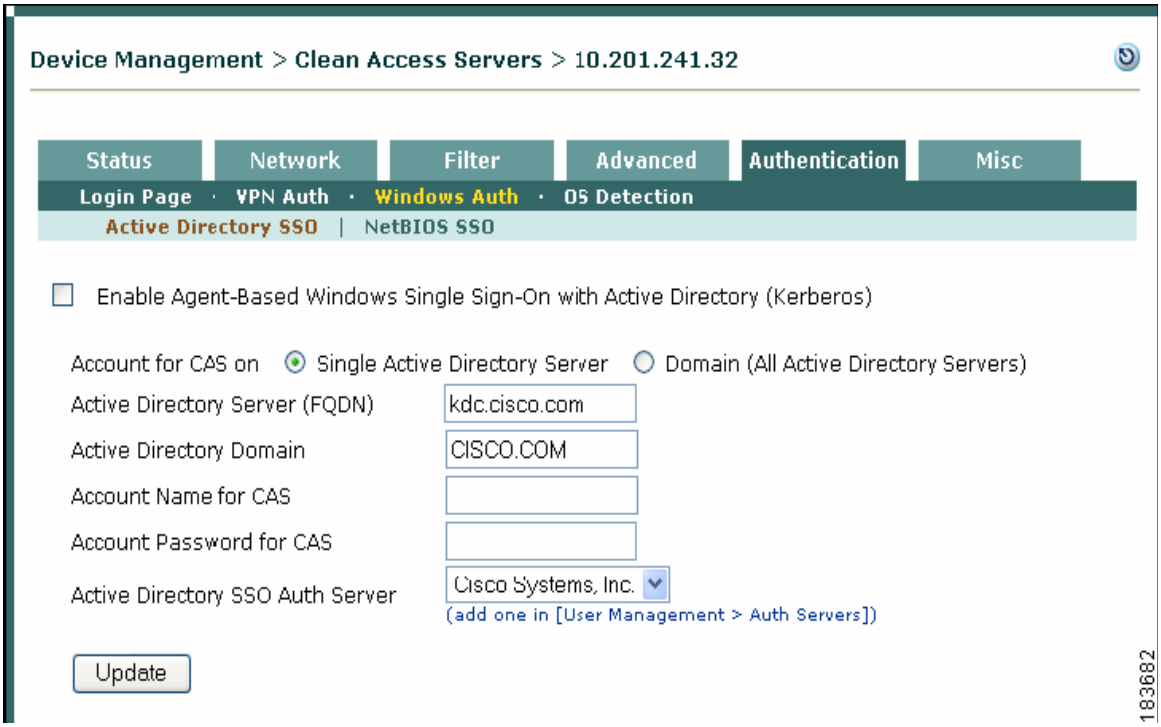


Figure 64. Configuring CAS to support AD SSO

Step 11- Download KTpass.exe tool version 5.2.3790.0 or higher version from Microsoft support site. Install KTpass program on windows 2003 server. Install KTpass.exe in C:\programs files\support tools folder. It is not allowed double click KTpass.exe in the support tools folder. After installation is completed at the command prompt `type,-ktpass.exe -princ gipson/ ActiPC.savoteku.local @ SAVOTEKU.LOCAL -mapuser gipson -pass Cisco123 -out c:\gipson.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly.`
In this command syntax, gipson refers to the name of CAS user account on AD, Cisco123 is the password, ActiPC.savoteku.local is the AD server FQDN and SAVOTEKU.LOCAL is the domain name entered in Figure 64. The general command syntax is however thus:

```
ktpass.exe -princ
<CAS_username>/<AD_DomainServer>@<AD_DOMAIN> -mapuser
<CAS_username> -pass <CAS_password> -out
c:\<CAS_username>.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly.
```

When this command is executed properly, a message "account Gipson has been set for DES-only encryption" is displayed at the command prompt.

With AD directory configured and KTpass executed, go to Figure 64, check 'enable agent based windows single sign-on with active directory (Kerberos)' option and click update. Go to 'device management', 'CCA server', 'manage (CAS_IP)' and 'status' as shown in Figure 65 to verify if Active directory SSO is started.

Figure 65. Verifying AD SSO status on CAS

8.17 Configuring Agent Based Posture Assessment

In order for Cisco NAC agent software that is running on network computers to effectively report the status of the computers, it is required to specify on the CAM, the AV (antivirus) and AS (anti- spyware) product that the network computer is to be validated against. The agent software periodically scans the host computer and report the status to the CAM. The status is checked against the configured AV/AS and their latest definition files. If the host computer is not in compliance, the computer is quarantined while providing a link option to remediate the computer. It is recommended that Cisco NAC and agent software should be version 4.5 or higher. The following steps are involved to configure AV/AS for computer posture check. [20]

Step 1- Create a rule for AV. This is accomplished by clicking on 'device management', 'clean access', 'clean access agent', 'rules' and 'new AV rule'. Within the new AV rule shown in Figure 66, enter 'rule name' and choose desired 'AV vendor'. Allow all other options as shown in Figure 66. Click on 'add rule' button.

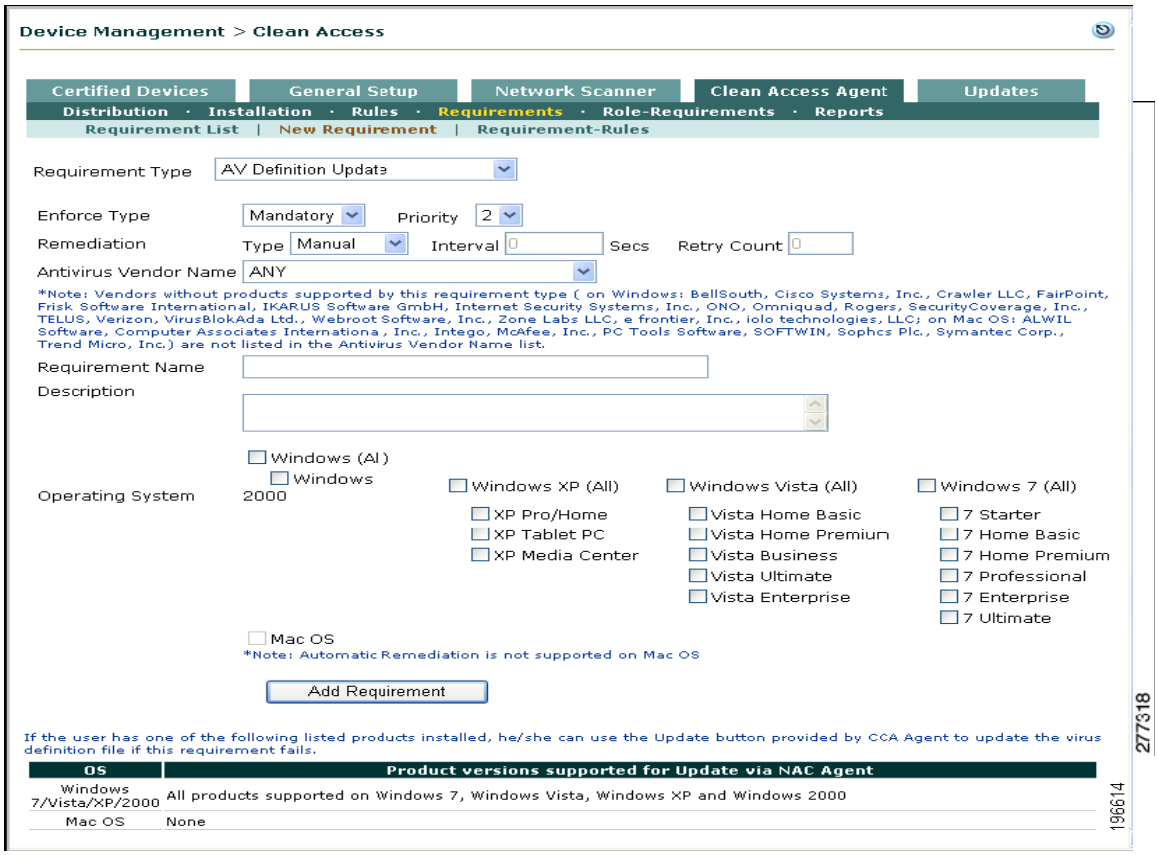


Figure 66. AV rule configuration window

Step 2- Create AV update as a mandatory requirement. To accomplish this task, click on 'requirements' tab and 'new requirement' as shown in Figure 66. in the 'new requirement' window in Figure 67, enter 'remediation type' as 'automatic', choose 'AV vendor' name as F-secure, check ' windows(all) for all windows operating systems. In the 'description field', enter instructor for computer user to click on 'update/remediate' button to remediate computer if remediation method was configured as 'manual'. Allow all other options as shown in Figure 67. Click on 'add requirement' button.
Figure 67. AV update configuration window

Step 3- Create a rule for AS. To create a rule for AS, go to 'device management', 'clean access', 'clean access agent', 'rules', 'new AS rule'. With the 'new AS rule' window, enter 'rule name' and 'AS vendor'. Allow all other options in window as in Figure 66.

Step 4- Create AS update requirement to be mandatory. To accomplish this task, click on 'new requirement' tab as shown in Figure 67, within the 'requirement type' field, select 'AS definition update'. Allow all other options as illustrated in step 2. Click 'add requirement' button.

Step 5- Map exiting AV/AS update requirements to the AV/AS rules created in steps 1 and step 3. To accomplish this task, click on the 'requirement-rules' tab shown in Figure 67. In the 'requirement-rules' window, select 'AV definition update' for the 'requirement name' field and ' windows(all)' for 'operating system'. Select the AV/AS vendor chosen in step 1 and step 3. Allow all other options as shown in Figure 68. Click on 'update' button.

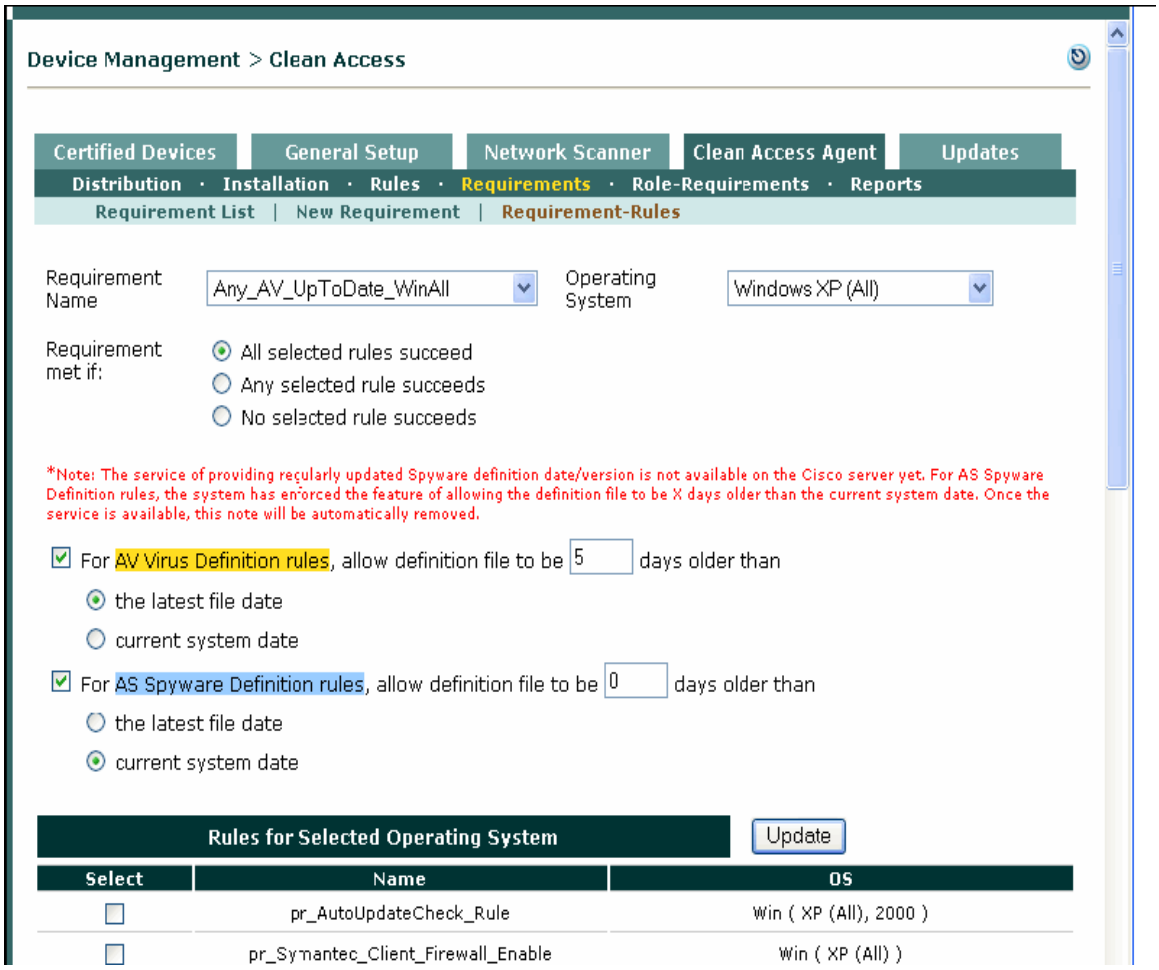


Figure 68. Mapping update requirement to rules

Step 6- Applying configured requirements in step 5 to user roles. This can be accomplished as follows; click on ‘roles-requirement’ tab in Figure 68. in the ‘role-requirement’ window, select ‘normal login role’ as ‘ role type’ and ‘role 1’ as ‘user role’. ‘Role 1’ is the name given to normal login role in Figure 28. Below the ‘select requirement to associate with the role’ sub section, select the specified AV/AS vendor configured in step1 and step 3. Click on ‘update’ button.

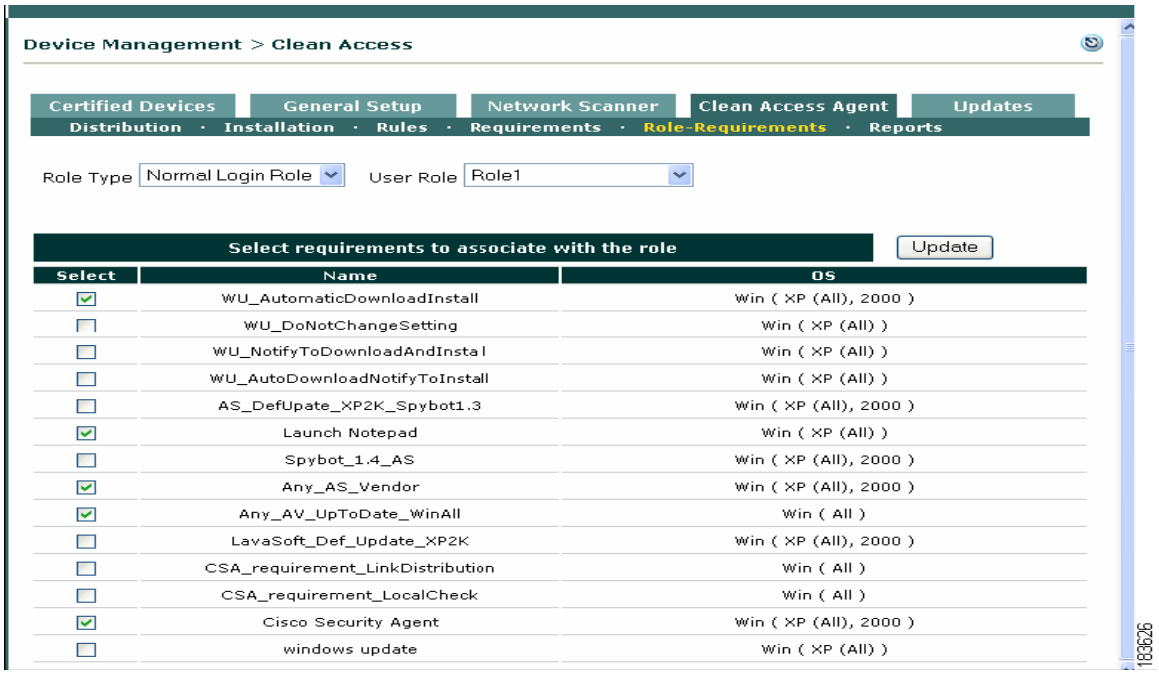


Figure 69. Applying configured requirement to user role

8.18 Joining Computers to Domain with Netdom

In a network environment with hundreds of computers authenticated by AD, it will be a daunting task to join each of these computers to a domain if one has to move from one computer to another in order to join them. Netdom is a windows 2003 and 2008 server active directory tool that enables network administrators to join computers to a domain from a single seating point. First, it is recommended to create an OU for computers, create and assigned GPO to the OU and then join computers to the AD OU. This enables computers to inherit the security settings assigned to the OU. When Netdom join command is used to join a computer to a domain prior to creating the computer account in AD, Netdom join command creates the computer account and joins it to the domain. In the proceeding example for Netdom join command, the following information is used:

- Savoteku.local- used as domain name
- Peketun- used as administrator's user account name
- Cisco123- used as administrator's password
- TekR3002wk1- used as hostname for the computer to join domain
- savoniaComputers- used as parent OU
- tekuComputers- used as child OU

To join a computer a domain using 'Netdom join' command, click windows 'start' menu , right click 'command prompt' and choose run as administrator. Within the elevated command prompt, enter this command syntax: [22]

```
Netdom join
TekR3002wk1/d:savoteku.local/ou:ou=savoniaComputers,ou=tekuCo
mputers,DC=Microsoft,DC=com/ud:peketun/pd:cisc0123
```

9 Conclusion

With ever increasing network attacks and attack tools created on daily basis, a network that was robust against network attacks yesterday might not be robust against new attacks today. It is for this reason that, once a network is properly secured based on the company's security policy, it needs to be monitored to ensure network security continuity using any available network audit tool. Next, the network should be test for any new vulnerability using **Satan or Nessus** software programs on weekly basis. If any new vulnerability is found on the network, an improvement on the company's security policy is required; and network security settings made to address the new security vulnerability.

With Cisco network assistant already in implementation on Savonia University of Applied sciences network; configuration security holes for L2 and L3 devices that might be exposed to attacks have been minimized. It is, however, recommended that Cisco NAC and Windows 2008 server be deployed without much delay. This will enable the school network to enjoy the advanced security features available in these products. Furthermore, the school network will enjoy the ability of being robust against any imaging network attack that may render the network unable.

References

1. Wikipedia Free encyclopedia, 13 February, 2010 [Online]
http://en.wikipedia.org/wiki/Network_security

2. Yusuf, B.(2008*).Network Security Technologies and Solutions*. Cisco press.

3. Implementing secure converged Wide-area networks v5.0, 13 February, 2010 [Online].CCNP- Cisco networking academy program
http://netacad.savonia.fi

4. James, J. (2008).*Network Security:* Know It All. Morgan Kaufmann

5. CCNA exploration- Accessing the WAN v4.0, 23 February, 2010 [Online]. Cisco networking academy program
http://netacad.savonia.fi

6. Wikipedia Free encyclopedia, 25 February, 2010 [Online]
http://en.wikipedia.org/wiki/Botnet

7. Computer security "Help prevent computer viruses" and "how to prevent computer worms",8th March, 2010 [Online]. Microsoft security.
http://www.microsoft.com/security/default.aspx

8. Building multilayer switched networks v5.0, 8 March, 2010 [Online]. CCNP- Cisco networking academy program
http://netacad.savonia.fi

9. Joe, H. (2002). *Cisco Network Security Little Black Book*. Paraglyph Press.

10. Configuration Guide for Cisco Secure ACS 4.2, 10 March, 2010 [Online]
http://www.cisco.com

11. Cisco 3945 Integrated Services Router specifications, 10 March, 2010 [Online]
http://www.cisco.com/en/US/products/ps10541/index.html

12. Cisco 3900 series integrated services routers, 14 March, 2010 [Online].
http://www.cisco.com/en/US/prod/collateral/routers/ps10536/
data_sheet_c78_553924.html

13. Cisco Configuration Professional Features, 14 March, 2010 [Online].
https://www.cisco.com/en/US/products/ps9422/index.html

14. Cisco configuration professional quick start guide, 17 March 2010 [Online].
http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/

guides/CiscoCPqsg.html

15. Kevin, D. and Ian, B. (2006).*Cisco IOS Cookbook*. O'Reilly Media.

16. Cisco network assistant quick tips, 20 March, 2010 [Online]. http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps5931/prod_white_paper0900aecd802d1b95.html

17. Cisco network assistant configuration guide to Catalyst 4500 switch, 20 March, 2010 [Online] http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sg/configuration/guide/netasist.pdf

18. Introduction to network admission control, 21 March, 2010 [Online]. http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html

19. Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide-Release 4.1(1) February 2008, 23 March, 2010 [Online]. http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/411/cam/m_auth.html

20. Cisco NAC Appliance - Clean Access Manager Configuration Guide-Release 4.7(2) February 2010, 24 March, 2010 [Online]. http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/47cam-book.html

21. *70-640, Package: Windows Server 2008 Active Directory Configuration (Microsoft Official Academic Course Series).* (2008).Wiley.

22. Netdom commands-Microsoft windows server techcenter, 27 March, 2010 [Online]. http://technet.microsoft.com/en-us/library/cc772217%28WS.10%29.aspx

Appendix 1

Table 4.Configuration file of Cisco 3945 router

```
FW_router#show run
Building configuration...

Current configuration : 10565 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname FW_router
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
resource policy
!
ip cef
!
ip name-server 8.8.8.8
ip name-server 8.8.4.4
ip inspect log drop-pkt
ip inspect name SDM_HIGH appfw SDM_HIGH
ip inspect name SDM_HIGH icmp
ip inspect name SDM_HIGH dns
ip inspect name SDM_HIGH esmtp
ip inspect name SDM_HIGH https
ip inspect name SDM_HIGH imap reset
ip inspect name SDM_HIGH pop3 reset
ip inspect name SDM_HIGH tcp
ip inspect name SDM_HIGH udp
ip inspect name dmzinspect tcp
ip inspect name dmzinspect udp
ip ips notify SDEE
ip ips name sdm_ips_rule
!
appfw policy-name SDM_HIGH
  application im aol
```

```
    service default action reset alarm
    service text-chat action reset alarm
    server deny name login.oscar.aol.com
    server deny name toc.oscar.aol.com
    server deny name oam-d09a.blue.aol.com
    audit-trail on
  application im msn
    service default action reset alarm
    service text-chat action reset alarm
    server deny name messenger.hotmail.com
    server deny name gateway.messenger.hotmail.com
    server deny name webmessenger.msn.com
    audit-trail on
  application http
    strict-http action reset alarm
    port-misuse im action reset alarm
    port-misuse p2p action reset alarm
    port-misuse tunneling action reset alarm
  application im yahoo
    service default action reset alarm
    service text-chat action reset alarm
    server deny name scs.msg.yahoo.com
    server deny name scsa.msg.yahoo.com
    server deny name scsb.msg.yahoo.com
    server deny name scsc.msg.yahoo.com
    server deny name scsd.msg.yahoo.com
    server deny name cs16.msg.dcn.yahoo.com
    server deny name cs19.msg.dcn.yahoo.com
    server deny name cs42.msg.dcn.yahoo.com
    server deny name cs53.msg.dcn.yahoo.com
    server deny name cs54.msg.dcn.yahoo.com
    server deny name ads1.vip.scd.yahoo.com
    server deny name radio1.launch.vip.dal.yahoo.com
    server deny name in1.msg.vip.re2.yahoo.com
    server deny name data1.my.vip.sc5.yahoo.com
    server deny name address1.pim.vip.mud.yahoo.com
    server deny name edit.messenger.yahoo.com
    server deny name messenger.yahoo.com
    server deny name http.pager.yahoo.com
    server deny name privacy.yahoo.com
    server deny name csa.yahoo.com
    server deny name csb.yahoo.com
    server deny name csc.yahoo.com
    audit-trail on
!
voice-card 0
!
crypto pki trustpoint TP-self-signed-3537330086
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3537330086
```

```
 revocation-check none
 rsakeypair TP-self-signed-3537330086
!
crypto pki certificate chain TP-self-signed-3537330086
 certificate self-signed 01
  30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33353337 33333030 3836301E 170D3130 30323136 31323134
  35355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 35333733
  33303038 3630819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100E20A 777C8D1C 099A54E6 92B123A1 B7B597A5 B61EE330 56D9CE99
920D4FB2
  F78F3754 2966C02F 77A86432 6C404914 A021B8D4 7407B235 184769A9
D6138CC5
  8D2AB3BF FA18AA12 CECD54C7 31464CB0 2F76DDC7 8B182B9E 354291F3
DE7CF9BC
  CCE16E8C 9615FF51 20ED6DE5 27C4887C 54DD79DA 60E4247B D1C75B86
DC8947AB
  72130203 010001A3 69306730 0F060355 1D130101 FF040530 030101FF 30140603
  551D1104 0D300B82 0946575F 726F7574 6572301F 0603551D 23041830 168014A3
  80181B93 D07C9895 A76C61BB 46631C24 F5BA4D30 1D060355 1D0E0416
0414A380
  181B93D0 7C9895A7 6C61BB46 631C24F5 BA4D300D 06092A86 4886F70D
01010405
  00038181 0044436A 31701286 DA0F2C32 3887F3E8 A34CFC04 1EC7C7BB
95651761
  310814A4 9901825B 910EFD19 21DE2AFB 25FB13C2 DE57C0A6 DD058E85
AA85CCBD
  E96EF34A AD3C5F29 B258E98C 65577E3C FFA2D7C3 1D666D07 EC8D99F5
7B6C3D5D
  F1E3E041 895AEF8D 4DDD3A93 22B9746E 8B956C9F 37856519 64F12109
610E1A38
  8F5F9F9C D7
  quit
username teku4boys privilege 15 secret 5 $1$.bhS$xNLJpkcDSJ7RCasAVE/vz0
!
class-map match-any sdm_p2p_kazaa
 match protocol fasttrack
 match protocol kazaa2
class-map match-any sdm_p2p_edonkey
 match protocol edonkey
class-map match-any sdm_p2p_gnutella
 match protocol gnutella
class-map match-any sdm_p2p_bittorrent
 match protocol bittorrent
!
policy-map sdmappfwp2p_SDM_HIGH
 class sdm_p2p_edonkey
   drop
```

```
 class sdm_p2p_gnutella
   drop
 class sdm_p2p_kazaa
   drop
 class sdm_p2p_bittorrent
   drop
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.33
 description $FW_INSIDE$
 encapsulation dot1Q 33
 ip address 172.16.33.1 255.255.255.0
 ip access-group 100 in
 ip nat inside
 ip inspect SDM_HIGH in
 ip ips sdm_ips_rule in
 ip virtual-reassembly
 no snmp trap link-status
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.3
 description $FW_DMZ$
 encapsulation dot1Q 3
 ip address 172.16.3.1 255.255.255.0
 ip access-group 104 in
 ip nat inside
 ip inspect dmzinspect out
 ip ips sdm_ips_rule in
 ip virtual-reassembly
 no snmp trap link-status
!
interface FastEthernet0/1.32
 description $FW_INSIDE$
 encapsulation dot1Q 32 native
 ip address 172.16.32.1 255.255.255.0
 ip access-group 101 in
 ip nat inside
 ip inspect SDM_HIGH in
 ip ips sdm_ips_rule in
 ip virtual-reassembly
 no snmp trap link-status
!
```

```
interface FastEthernet0/1.36
 description $FW_INSIDE$
 encapsulation dot1Q 36
 ip address 172.16.36.1 255.255.252.0
 ip access-group 102 in
 ip nat inside
 ip inspect SDM_HIGH in
 ip ips sdm_ips_rule in
 ip virtual-reassembly
 no snmp trap link-status
!
interface FastEthernet0/1.48
 description $FW_INSIDE$
 encapsulation dot1Q 48
 ip address 172.16.48.1 255.255.240.0
 ip access-group 103 in
 ip nat inside
 ip inspect SDM_HIGH in
 ip ips sdm_ips_rule in
 ip virtual-reassembly
 no snmp trap link-status
!
interface Serial0/1/0
 description $FW_OUTSIDE$
 ip address 172.16.70.48 255.255.240.0
 ip access-group 105 in
 ip verify unicast reverse-path
 ip nat outside
 ip ips sdm_ips_rule out
 ip virtual-reassembly
 clock rate 125000
 service-policy input sdmappfwp2p_SDM_HIGH
 service-policy output sdmappfwp2p_SDM_HIGH
!
ip http server
ip http authentication local
ip http secure-server
ip nat inside source list 1 interface Serial0/1/0 overload
ip nat inside source static tcp 172.16.33.4 80 180.32.44.46 80 extendable
!
access-list 1 remark SDM_ACL Category=2
access-list 1 permit 172.16.3.0 0.0.0.255
access-list 1 permit 172.16.33.0 0.0.0.255
access-list 1 permit 172.16.32.0 0.0.0.255
access-list 1 permit 172.16.36.0 0.0.3.255
access-list 1 permit 172.16.48.0 0.0.15.255
access-list 100 remark auto generated by SDM firewall configuration
access-list 100 remark SDM_ACL Category=1
access-list 100 deny   ip 172.16.48.0 0.0.15.255 any
access-list 100 deny   ip 172.16.36.0 0.0.3.255 any
```

```
access-list 100 deny   ip 172.16.32.0 0.0.0.255 any
access-list 100 deny   ip 172.16.3.0 0.0.0.255 any
access-list 100 deny   ip 172.16.64.0 0.0.15.255 any
access-list 100 deny   ip host 255.255.255.255 any
access-list 100 deny   ip 127.0.0.0 0.255.255.255 any
access-list 100 permit ip any any
access-list 101 remark auto generated by SDM firewall configuration
access-list 101 remark SDM_ACL Category=1
access-list 101 deny   ip 172.16.48.0 0.0.15.255 any
access-list 101 deny   ip 172.16.36.0 0.0.3.255 any
access-list 101 deny   ip 172.16.33.0 0.0.0.255 any
access-list 101 deny   ip 172.16.3.0 0.0.0.255 any
access-list 101 deny   ip 172.16.64.0 0.0.15.255 any
access-list 101 deny   ip host 255.255.255.255 any
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any
access-list 101 permit ip any any
access-list 102 remark auto generated by SDM firewall configuration
access-list 102 remark SDM_ACL Category=1
access-list 102 deny   ip 172.16.48.0 0.0.15.255 any
access-list 102 deny   ip 172.16.32.0 0.0.0.255 any
access-list 102 deny   ip 172.16.33.0 0.0.0.255 any
access-list 102 deny   ip 172.16.3.0 0.0.0.255 any
access-list 102 deny   ip 172.16.64.0 0.0.15.255 any
access-list 102 deny   ip host 255.255.255.255 any
access-list 102 deny   ip 127.0.0.0 0.255.255.255 any
access-list 102 permit ip any any
access-list 103 remark auto generated by SDM firewall configuration
access-list 103 remark SDM_ACL Category=1
access-list 103 deny   ip 172.16.36.0 0.0.3.255 any
access-list 103 deny   ip 172.16.32.0 0.0.0.255 any
access-list 103 deny   ip 172.16.33.0 0.0.0.255 any
access-list 103 deny   ip 172.16.3.0 0.0.0.255 any
access-list 103 deny   ip 172.16.64.0 0.0.15.255 any
access-list 103 deny   ip host 255.255.255.255 any
access-list 103 deny   ip 127.0.0.0 0.255.255.255 any
access-list 103 permit ip any any
access-list 104 remark auto generated by SDM firewall configuration
access-list 104 remark SDM_ACL Category=1
access-list 104 deny   ip any any log
access-list 105 remark auto generated by SDM firewall configuration
access-list 105 remark SDM_ACL Category=1
access-list 105 permit tcp any host 180.32.44.46 eq www
access-list 105 deny   ip 172.16.48.0 0.0.15.255 any
access-list 105 deny   ip 172.16.36.0 0.0.3.255 any
access-list 105 deny   ip 172.16.32.0 0.0.0.255 any
access-list 105 deny   ip 172.16.33.0 0.0.0.255 any
access-list 105 deny   ip 172.16.3.0 0.0.0.255 any
access-list 105 permit icmp any host 172.16.70.48 echo-reply
access-list 105 permit icmp any host 172.16.70.48 time-exceeded
access-list 105 permit icmp any host 172.16.70.48 unreachable
```

```
access-list 105 permit tcp any host 172.16.3.2 eq www
access-list 105 permit tcp any host 172.16.3.3 eq smtp
access-list 105 deny   ip 10.0.0.0 0.255.255.255 any
access-list 105 deny   ip 172.16.0.0 0.15.255.255 any
access-list 105 deny   ip 192.168.0.0 0.0.255.255 any
access-list 105 deny   ip 127.0.0.0 0.255.255.255 any
access-list 105 deny   ip host 255.255.255.255 any
access-list 105 deny   ip host 0.0.0.0 any
access-list 105 deny   ip any any log
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
 transport input ssh
!
scheduler allocate 20000 1000
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
End
```