

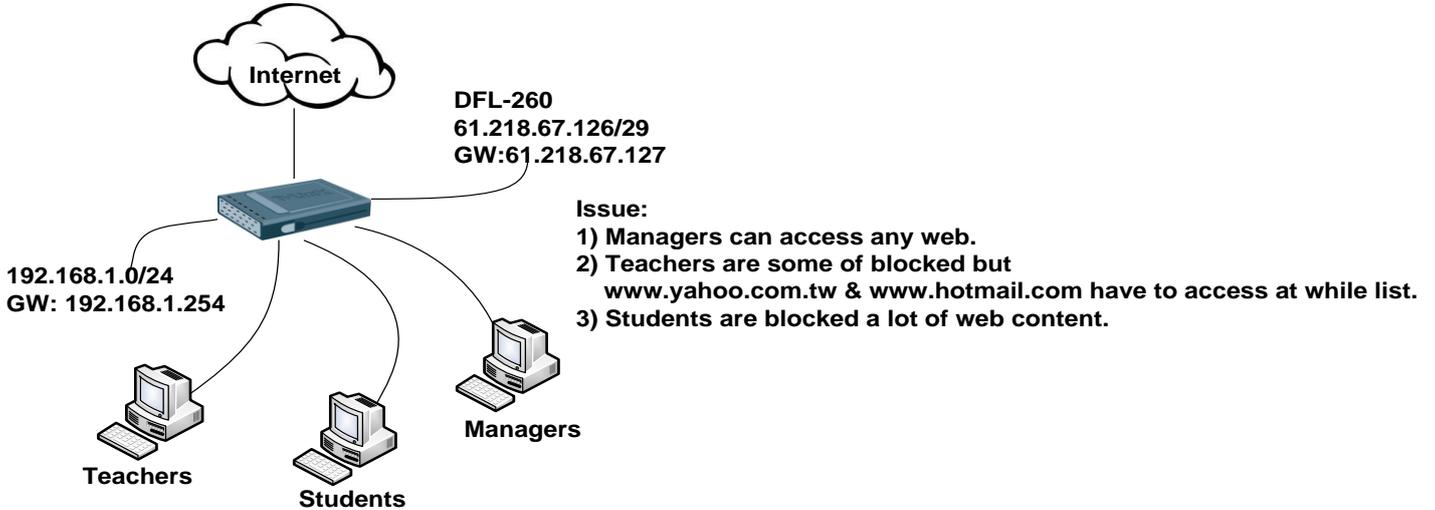
How to set up WCF with allow SSH web page

[Foreword]

1) ALG with WCF is not direct support SSH port in firewall object.

(www.hotmail.com is Redirection to https site)

[Topology]



Issue:

- 1) Managers can access any web.
- 2) Teachers are some of blocked but www.yahoo.com.tw & www.hotmail.com have to access at while list.
- 3) Students are blocked a lot of web content.

[Setting]

1. Setting WAN IP on wan port interface.

#	Name	IP address	Network	Default Gateway	Enable DHCP Client	Comments
1	wan	wan_ip	wannet	wan_gw	No	
2	dmz	Address: 61.218.67.126	Address: 61.218.67.120/29	Address: 61.218.67.121		
3	lan					

2. Create Students and Teachers WCF Objects

Objects > ALG with AV/WCF

The image shows two screenshots of the WCF configuration interface. The top screenshot is for 'http-Students-wcf' and the bottom is for 'http-Teachers-wcf'. Both screenshots show the 'General' tab with the name of the object. The 'http-Students-wcf' screenshot shows the 'Active Content Handling' tab with checkboxes for 'Strip ActiveX objects (including Flash)', 'Strip Java applets', 'Strip Javascript/VBScript', and 'Block Cookies'. The 'http-Teachers-wcf' screenshot shows the 'Web Content Filtering' tab with 'Mode' set to 'Enabled' and a list of 'Blocked' categories including 'Adult content', 'Dating sites', 'Games sites', and 'Spam'. The 'URL Filter' tab is also visible at the bottom of the 'http-Teachers-wcf' screenshot, showing a list of 'Whitelist' entries for '*.yahoo.com/*' and '*.hotmail.com*'.

3. Create Students and Teachers Services Objects

Objects > Services

Services					
Services are pre-defined or user-defined objects representing various IP protocols, such as HTTP, FTP and Telnet.					
94	 http-Students-wcf	TCP	80	http-Students-wcf - WCF:Enabled	
95	 http-Teachers-wcf	TCP	80	http-Teachers-wcf - WCF:Enabled	

http-Teachers-wcf

A TCP/UDP Service is a definition of an TCP or UDP protocol with specific parameters.

General

General

Name:

Type:

Source:

Destination:

Enter port numbers and/or port ranges separated by commas. For example: 137-139,445

Pass returned ICMP error messages from destination

SYN flood protection (SYN Relay)

Application Layer Gateway

An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for this service.

ALG:

Max Sessions: Specifies how many concurrent sessions that are permitted using this service.

http-Students-wcf

A TCP/UDP Service is a definition of an TCP or UDP protocol with specific parameters.

General

General

Name:

Type:

Source:

Destination:

Enter port numbers and/or port ranges separated by commas. For example: 137-139,445

Pass returned ICMP error messages from destination

SYN flood protection (SYN Relay)

Application Layer Gateway

An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for this service.

ALG:

Max Sessions: Specifies how many concurrent sessions that are permitted using this service.

4. Create each of monitor group permission in authentication DB.

User Authentication > Local User Databases

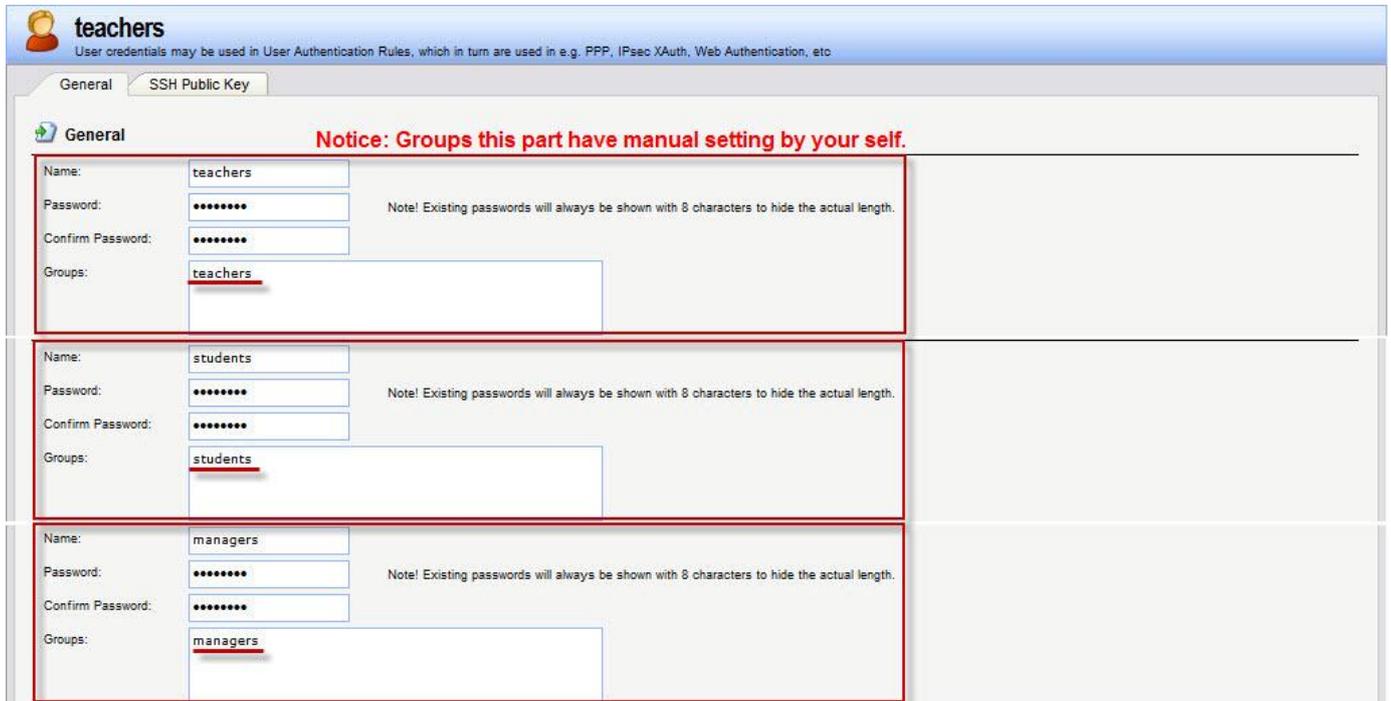


WCF_AuthDB
A local user database contains user accounts used for authentication purposes.

General Users

Add

Name	Groups	IP Pool	Networks	Comments
managers	managers			Password:managers
students	students			Password:students
teachers	teachers			Password:teachers



teachers
User credentials may be used in User Authentication Rules, which in turn are used in e.g. PPP, IPsec XAuth, Web Authentication, etc

General SSH Public Key

General **Notice: Groups this part have manual setting by your self.**

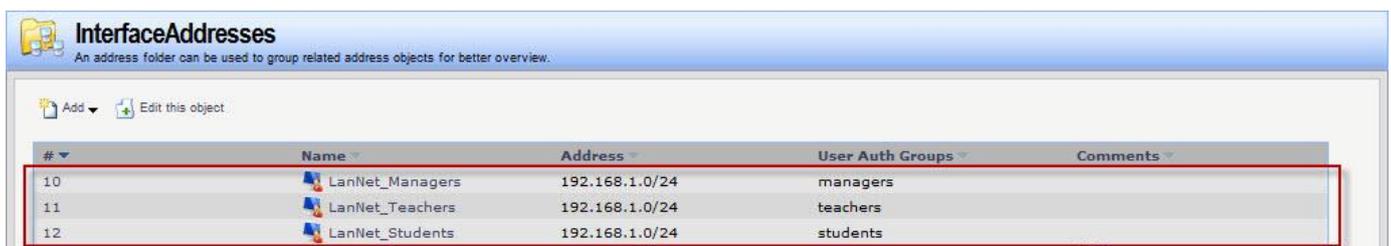
Name: teachers
Password: Note! Existing passwords will always be shown with 8 characters to hide the actual length.
Confirm Password:
Groups: teachers

Name: students
Password: Note! Existing passwords will always be shown with 8 characters to hide the actual length.
Confirm Password:
Groups: students

Name: managers
Password: Note! Existing passwords will always be shown with 8 characters to hide the actual length.
Confirm Password:
Groups: managers

5. Create InterfaceAddresses include user permission.

Objects > Address Book > InterfaceAddresses



InterfaceAddresses
An address folder can be used to group related address objects for better overview.

Add Edit this object

#	Name	Address	User Auth Groups	Comments
10	LanNet_Managers	192.168.1.0/24	managers	
11	LanNet_Teachers	192.168.1.0/24	teachers	
12	LanNet_Students	192.168.1.0/24	students	

6. Create an authentication rule for authentication DB.

User Authentication > Local User Databases > User Authentication Rules

User Authentication Rules
The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

#	Name	Authentication agent	Authentication source	Interface	Comments
1	Auth_Rule	HTTP	Local	lan	

General

Name: Auth_Rule
 Authentication agent: HTTP
 Authentication Source: Local
 Interface: lan
 Originator IP: lannet
 Terminator IP: (None)

Authentication Options

RADIUS Method: Unencrypted password (PAP)
 Local User DB: WCF_AuthDB

7. Create IP Rules

One of rule for teacher's https policy. This IP rule must high than other WCF rules.

LAN-To-WAN
An IP Rule Folder can be used to group IP Rules into logical groups for better overview and simplified management.

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
2	https-nat	NAT	lan	LanNet_Teachers	wan	all-nets	https

LAN-To-WAN
An IP Rule Folder can be used to group IP Rules into logical groups for better overview and simplified management.

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	DNS-NAT	NAT	lan	lannet	wan	all-nets	dns-all
2	https-nat	NAT	lan	LanNet_Teachers	wan	all-nets	https
3	http2fw	Allow	lan	lannet	core	lan_ip	http-all
4	NAT_Managers	NAT	lan	LanNet_Managers	wan	all-nets	http-all
5	NAT-Teachers	NAT	lan	LanNet_Teachers	wan	all-nets	http-Teachers-wcf
6	NAT-Students	NAT	lan	LanNet_Students	wan	all-nets	http-Students-wcf
7	Auth-Sat	SAT	lan	lannet	wan	all-nets	http-all
8	Allow	Allow	lan	lannet	wan	all-nets	http-all
9	Ping	Allow	lan	lannet	any	all-nets	ping-outbound

END