

Requirement:

He is using Web Authentication and URL black/white-listing on it. It works 100%. Now he needs the following Groups set up with a schedule to be applied to each group, and I'm not sure how to proceed.

1. Managers - must have unrestricted internet access.
2. Employees - must have some privileges (black/white-list). Schedule must be unrestricted internet between 06-08h00, 13-14h00 and 17-19h00. the rest of the time the black and white-list must be active.
3. Other users must have only restricted internet access from 06-08h00, 13-14h00 and 17-19h00. Other time in between must be blocked completely.

Login information:

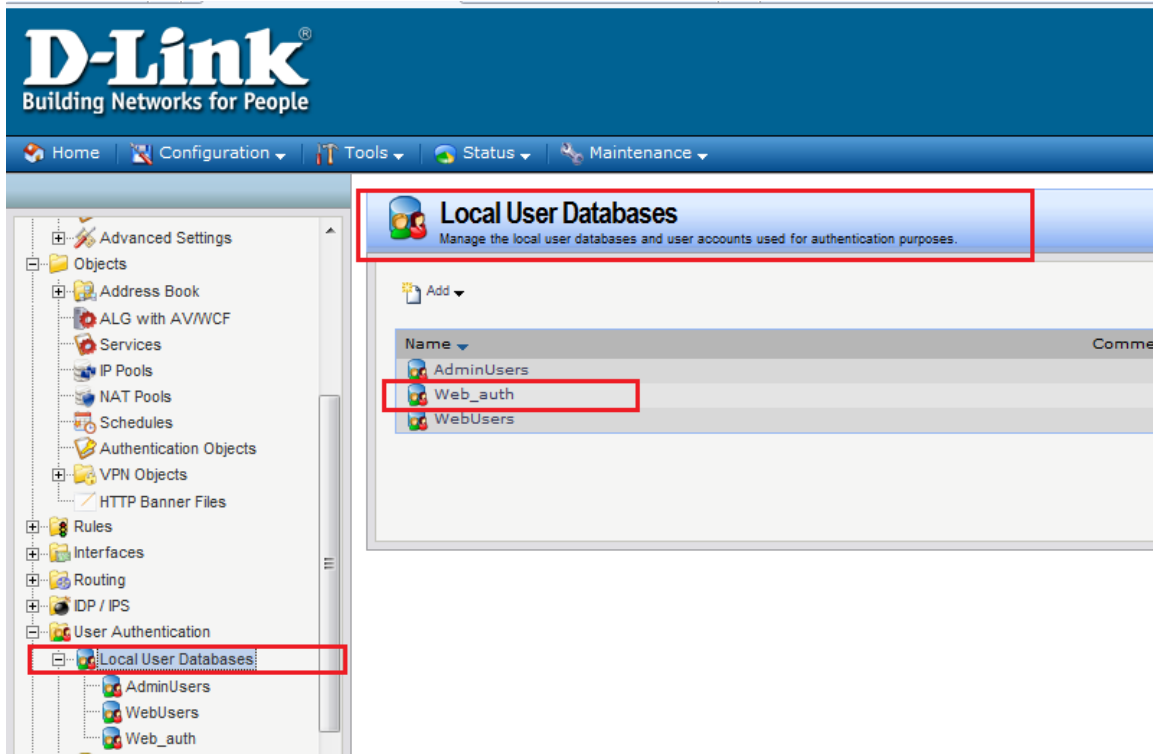
User admin
Password bj1107
router ip 172.16.1.1
netmask 255.255.255.0

Configuration:

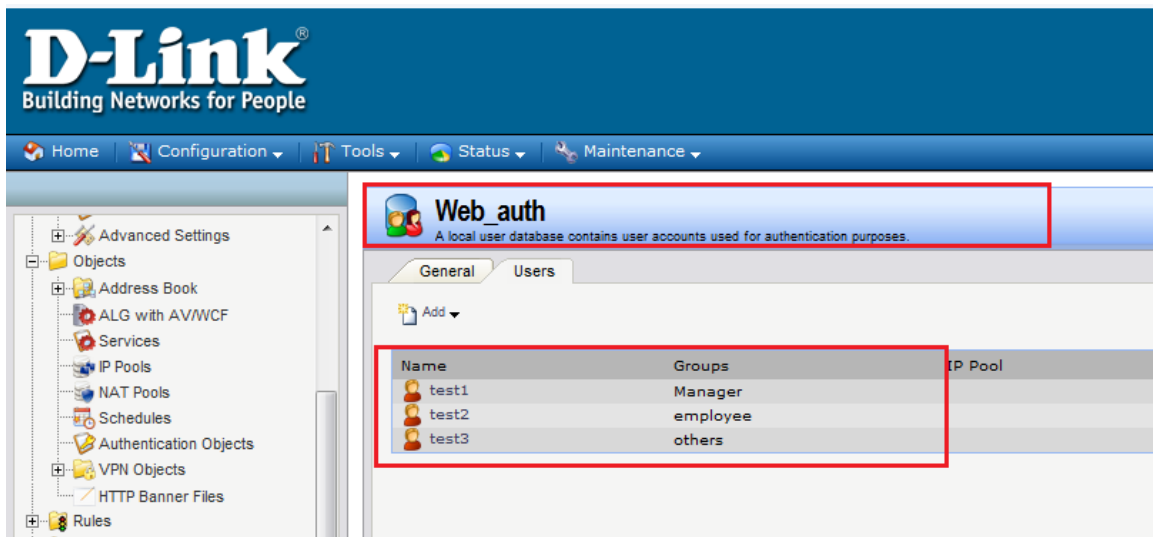
User's configuration and with some modification.

Modification:

- 1.Create 3 groups: manager, employee, and others.**



We create a user and assign the user to the group:



Home Configuration Tools Status Maintenance

test1
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

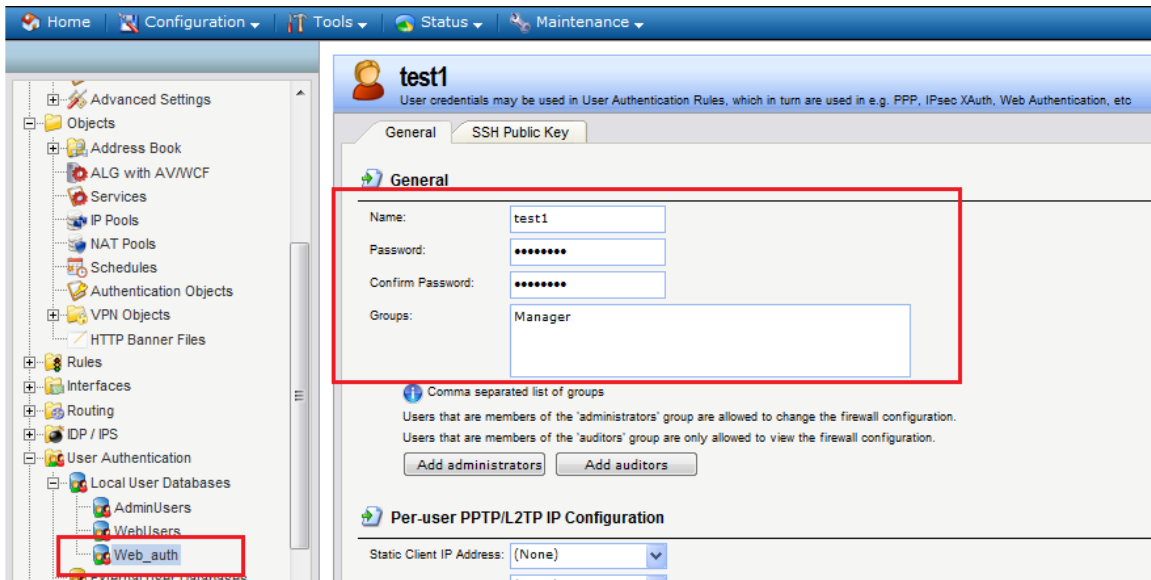
Name: test1
Password:
Confirm Password:
Groups: Manager

Comma separated list of groups
Users that are members of the 'administrators' group are allowed to change the firewall configuration.
Users that are members of the 'auditors' group are only allowed to view the firewall configuration.

Add administrators Add auditors

Per-user PPTP/L2TP IP Configuration

Static Client IP Address: (None)



test2
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

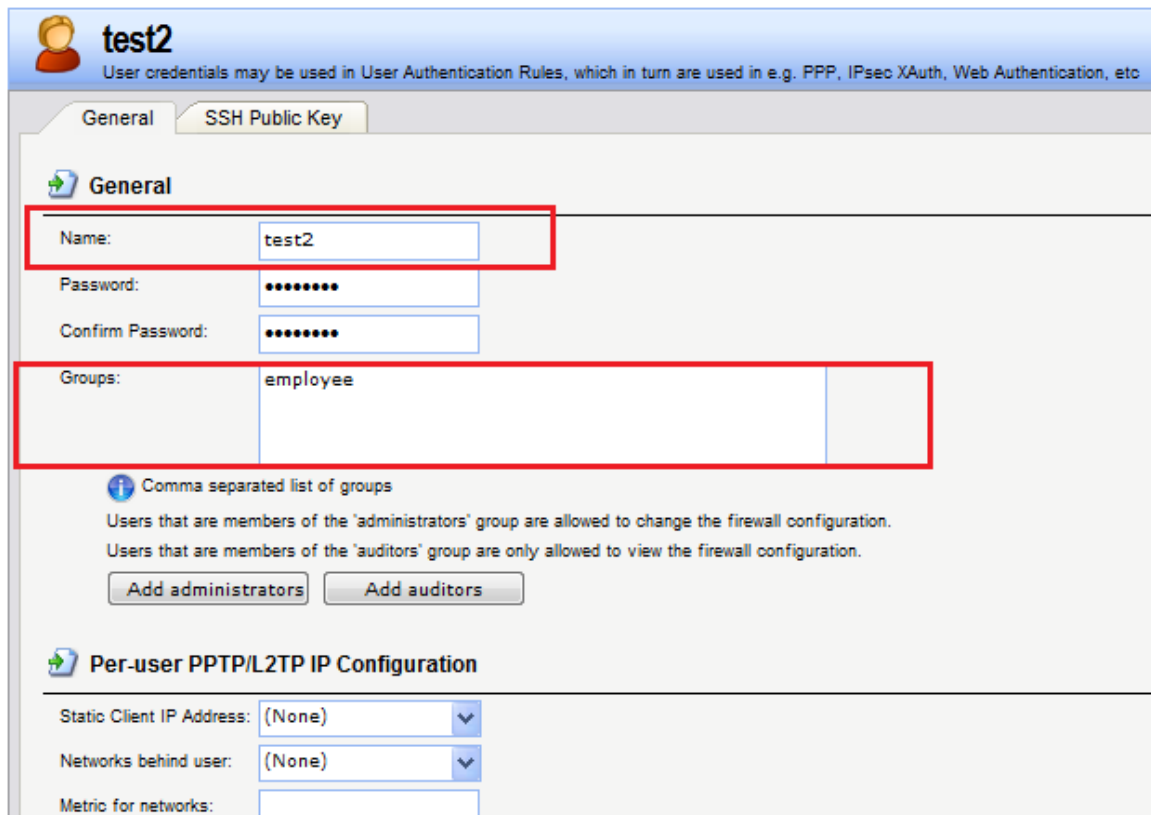
Name: test2
Password:
Confirm Password:
Groups: employee


Comma separated list of groups
Users that are members of the 'administrators' group are allowed to change the firewall configuration.
Users that are members of the 'auditors' group are only allowed to view the firewall configuration.

Add administrators Add auditors


Per-user PPTP/L2TP IP Configuration

Static Client IP Address: (None)
Networks behind user: (None)
Metric for networks:



 **test3**
 User credentials may be used in User Authentication Rules, which in turn are used in e.g. PPP, IPsec XAuth, Web Authent

General **SSH Public Key**


 **General**

Name:


Password:

Confirm Password:

Groups:

 Comma separated list of groups

Users that are members of the 'administrators' group are allowed to change the firewall configuration.
 Users that are members of the 'auditors' group are only allowed to view the firewall configuration.

 **Per-user PPTP/L2TP IP Configuration**


Static Client IP Address:

Networks behind user:

Metric for networks:


User Authentication Rule:

Home Configuration Tools Status Maintenance Logout

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

Add

#	Name	Authentication agent	Authentication source	Interface	Comments
1	web_auth	HTTP	Local	lan	
2	lan_http_auth	HTTP	Local	lan	

 Right-click on a row for additional actions

Navigation tree:
 Advanced Settings
 Objects
 Address Book
 ALG with AVWCF
 Services
 IP Pools
 NAT Pools
 Schedules
 Authentication Objects
 VPN Objects
 HTTP Banner Files
 Rules
 Interfaces
 Routing
 OP / IPS
 User Authentication
 Local User Databases
 External User Databases
 Accounting Servers
User Authentication Rules
 Authentication Settings
 Traffic Management

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

General Log Settings Authentication Options Accounting Agent Options Restrictions

General

Name: web_auth

Authentication agent: HTTP

Authentication Source: Local

Interface: lan

Originator IP: lannet

Terminator IP: (None)

For XAuth and PPP, this is the tunnel originator IP.

Comments

Comments:

Home Configuration Tools Status Maintenance

DFL-210

- System
 - Date and Time
 - DNS
 - Remote Management
 - Log and Event Receivers
 - DHCP
 - Misc. Clients
 - Hardware Monitoring
 - Whitelist
 - Advanced Settings
- Objects
 - Address Book
 - ALG with AV/WCF
 - Services
 - IP Pools
 - NAT Pools
 - Schedules
 - Authentication Objects
 - VPN Objects
 - HTTP Banner Files
- Rules

LDAP servers

Available Selected

RADIUS Method: Unencrypted password (PAP)

Local User DB: Web_auth

Create 3 network address for each user auth group:

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
dmz_ip	172.17.100.254		IPAddress of interface dmz
dmznet	172.17.100.0/24		The network on interface dmz
Employee	172.16.1.0/24	Employee	
lan-auth	172.16.1.0/24	webuser	
lan_ip	172.16.1.1		IPAddress of interface lan
lannet	172.16.1.0/24		The network on interface lan
Manager_net	172.16.1.0/24	Manager	
Others	172.16.1.0/24	Others	
wan_dns1	0.0.0.0		Primary DNS server for interface wan.
wan_dns2	0.0.0.0		Secondary DNS server for interface wan
wan_ip	0.0.0.0		IPAddress of interface wan
wan_phys_ip	0.0.0.0		IP address of interface wan_phys
wan_physnet	0.0.0.0		Network on interface wan_phys
wannet	0.0.0.0		The network on interface wan

Manager_net
Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General User Authentication

General

Name:

Address:

Comments

Comments:

Manager_net
Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General User Authentication

General

Groups and user names that belong to this network object. Objects that filter on credentials can only be used as source nets and destination nets in the Rules section.

Comma separated list of user names and groups:

No defined credentials

Checking this box specifies that this network object requires user authentication, but that it has no credentials (user names or groups) defined. This means that the network object only requires that a user is authenticating, but ignores any kind of group membership.

Employee

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General User Authentication

General

Name:

Address:

Comments

Comments:

Employee

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General User Authentication

General

Groups and user names that belong to this network object. Objects that filter on credentials can only be used as source nets and destination nets in the Rules section.

Comma-separated list of user names and groups:

No defined credentials

i Checking this box specifies that this network object requires user authentication, but that it has no credentials (user names or groups) defined. This means that the network object only ignores any kind of group membership.

Others

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General User Authentication

General

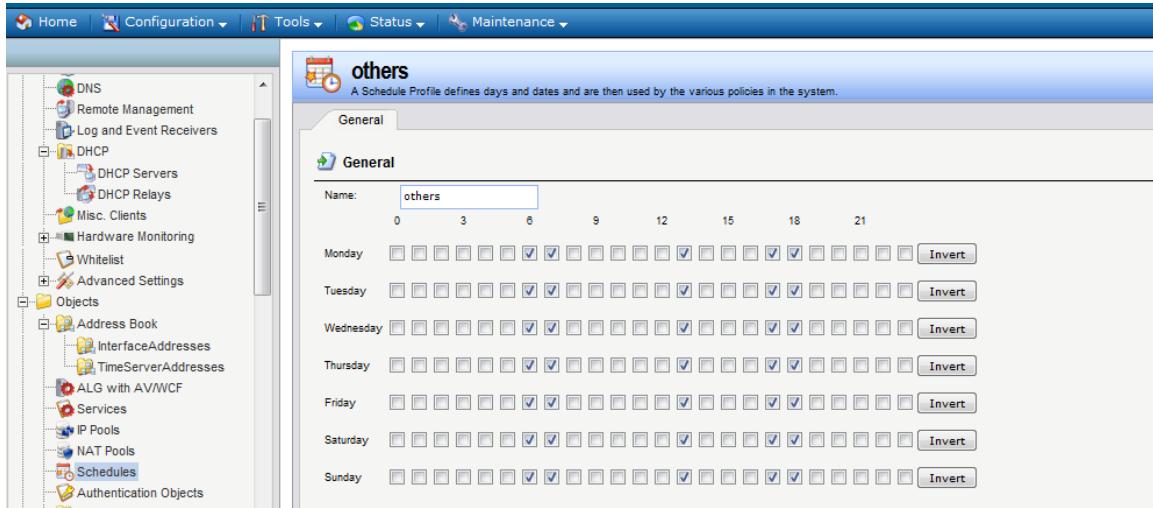
Name:

Address:

Comments

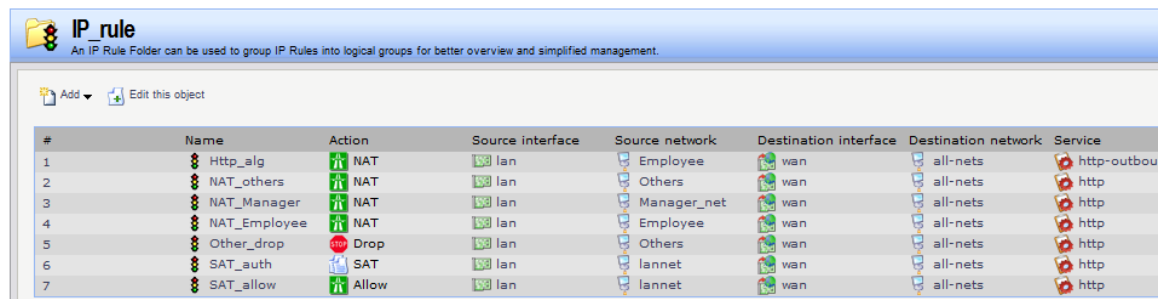
Comments:

The above setting is the rule will apply on the time except 6:00~7:59,13:00~13:59,and 17:00~18:59.

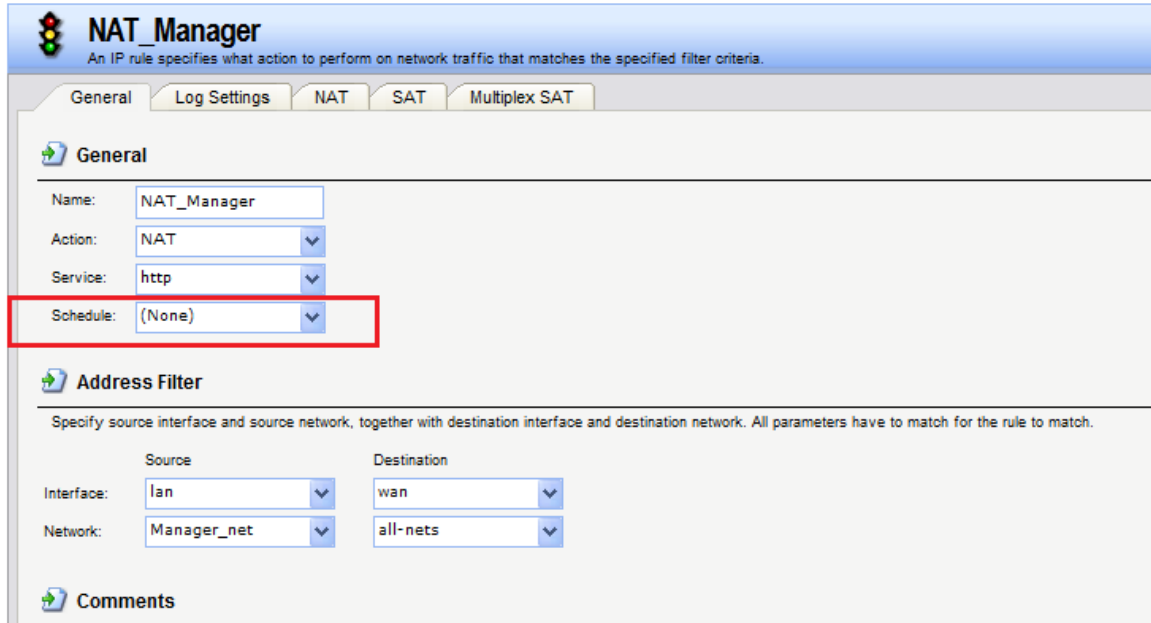


The above setting is the rule will apply on the time 6:00~7:59,13:00~13:59,and 17:00~18:59.

Set the IP rule:



Since the manager group doesn't have any restriction, we can have the following setting:



NAT Manager
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General | Log Settings | NAT | SAT | Multiplex SAT

General

Name: NAT_Manager
Action: NAT
Service: http
Schedule: (None)

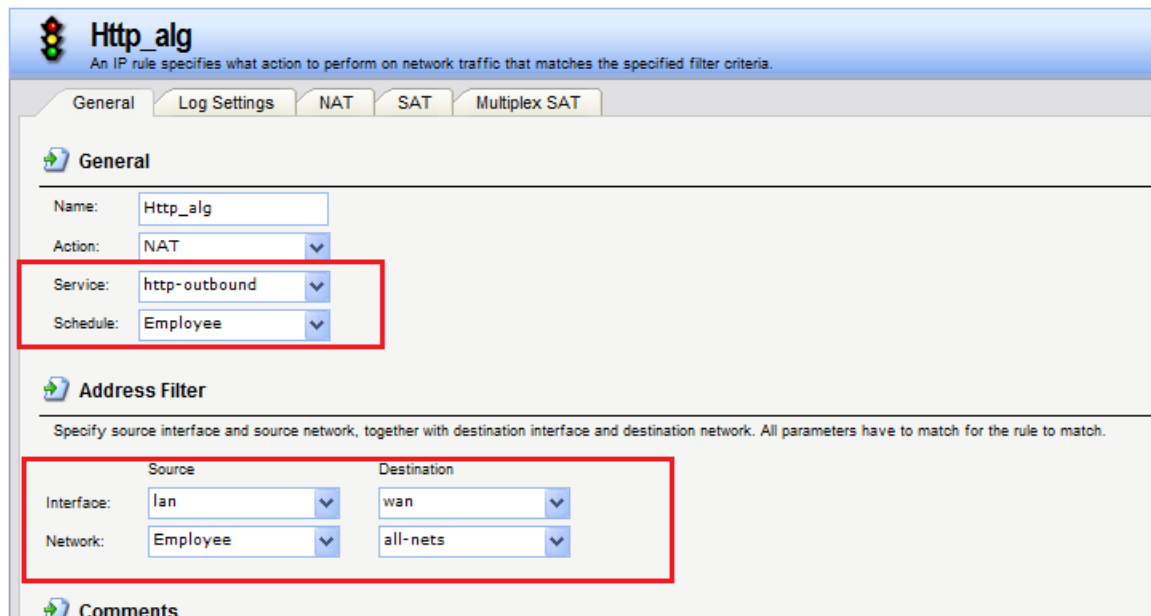
Address Filter
Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

Source: Interface: lan, Network: Manager_net
Destination: Interface: wan, Network: all-nets

Comments

For the employee, we have set the following two rules:

In the following schedule period, this rule will be applied



Http_alg
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General | Log Settings | NAT | SAT | Multiplex SAT

General

Name: Http_alg
Action: NAT
Service: http-outbound
Schedule: Employee

Address Filter
Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

Source: Interface: lan, Network: Employee
Destination: Interface: wan, Network: all-nets

Comments

Other time will be used the following rule (please notice the priority):

NAT_Employee

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General Log Settings NAT SAT Multiplex SAT

General

Name: NAT_Employee
Action: NAT
Service: http
Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Source	Destination
Interface:	lan	wan
Network:	Employee	all-nets

For others:

NAT_others

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General Log Settings NAT SAT Multiplex SAT

General

Name: NAT_others
Action: NAT
Service: http
Schedule: others

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Source	Destination
Interface:	lan	wan
Network:	Others	all-nets

Comments

Other_drop

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General Log Settings NAT SAT Multiplex SAT

General

Name: Other_drop
Action: Drop
Service: http
Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Source	Destination
Interface:	lan	wan
Network:	Others	all-nets

Comments

SAT_auth

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General Log Settings NAT SAT Multiplex SAT

General

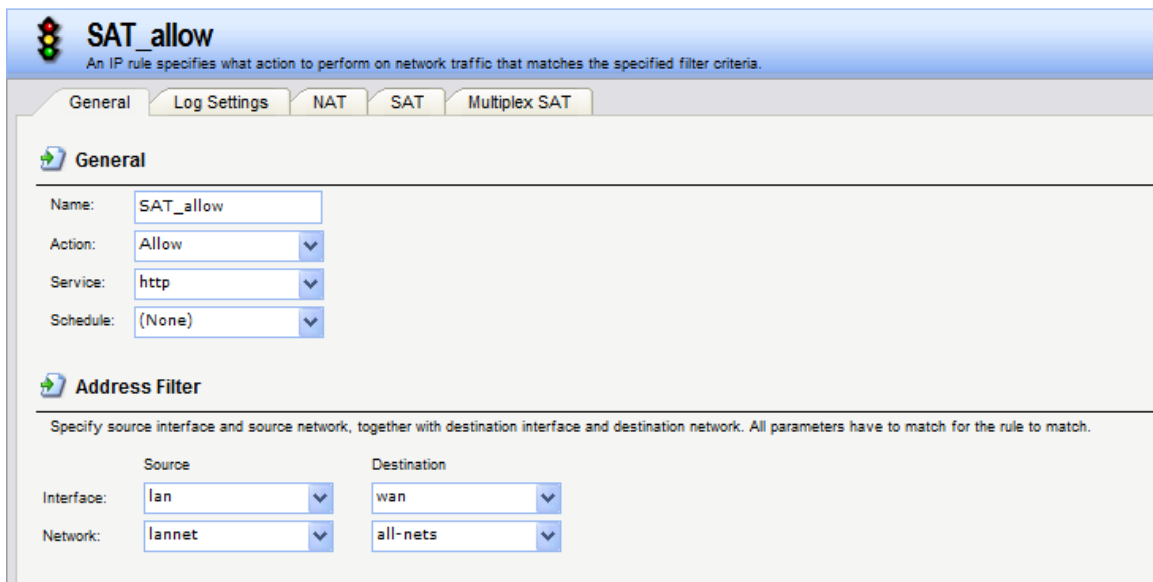
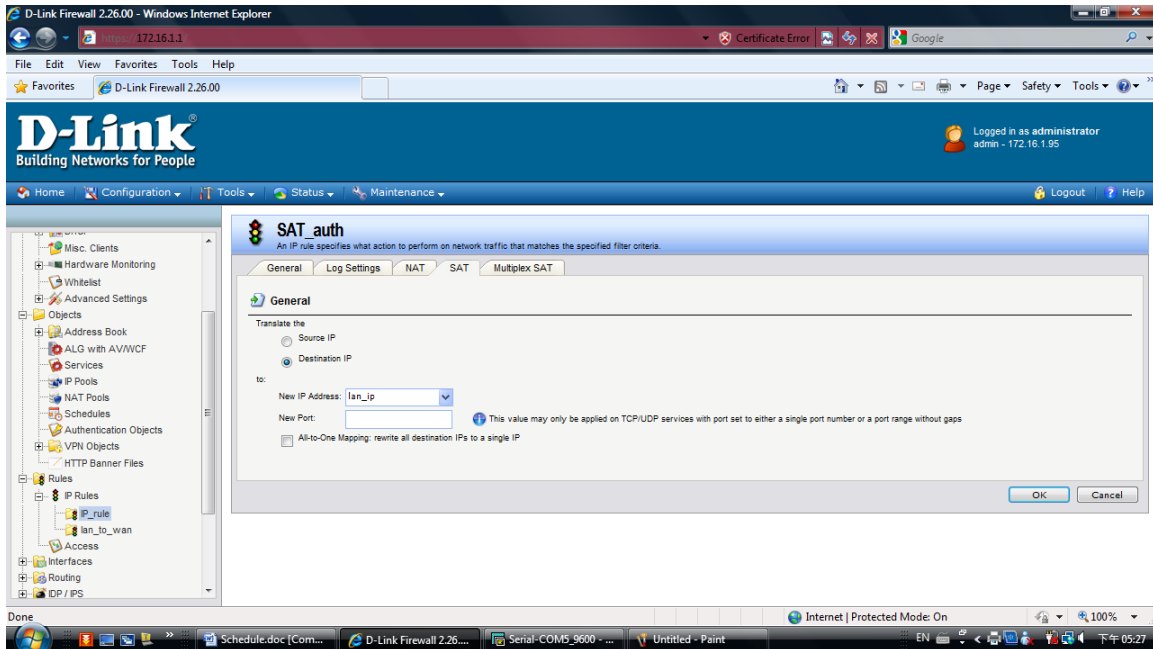
Name: SAT_auth
Action: SAT
Service: http
Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Source	Destination
Interface:	lan	wan
Network:	lannet	all-nets

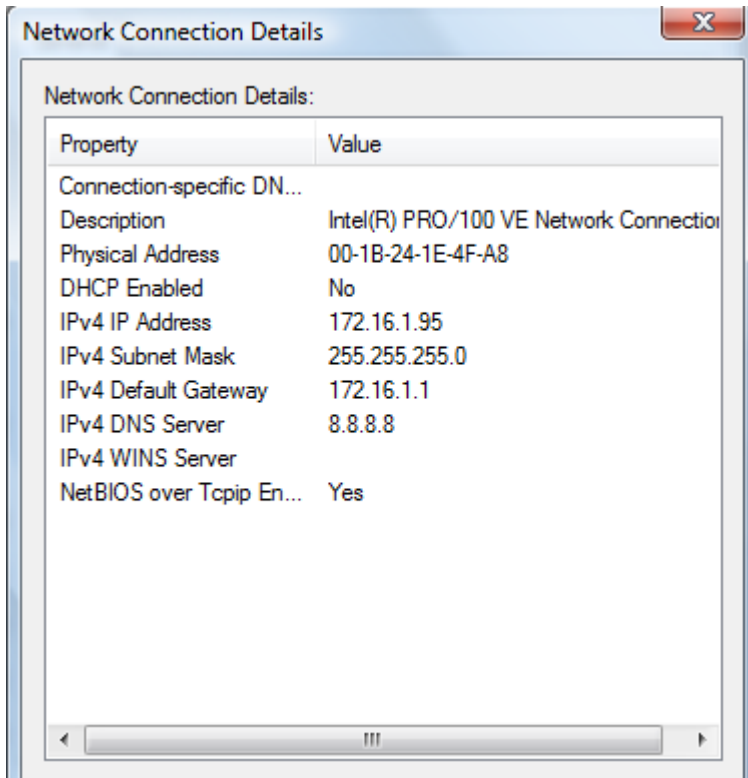
Comments



Testing procedure:

[Topology]:

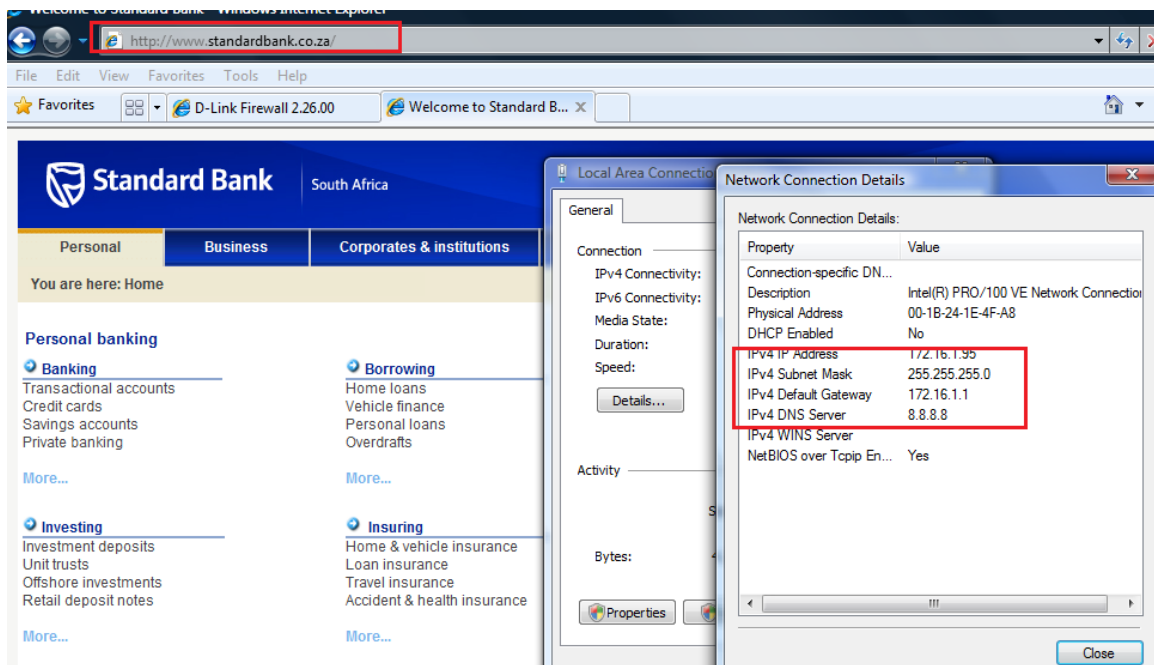
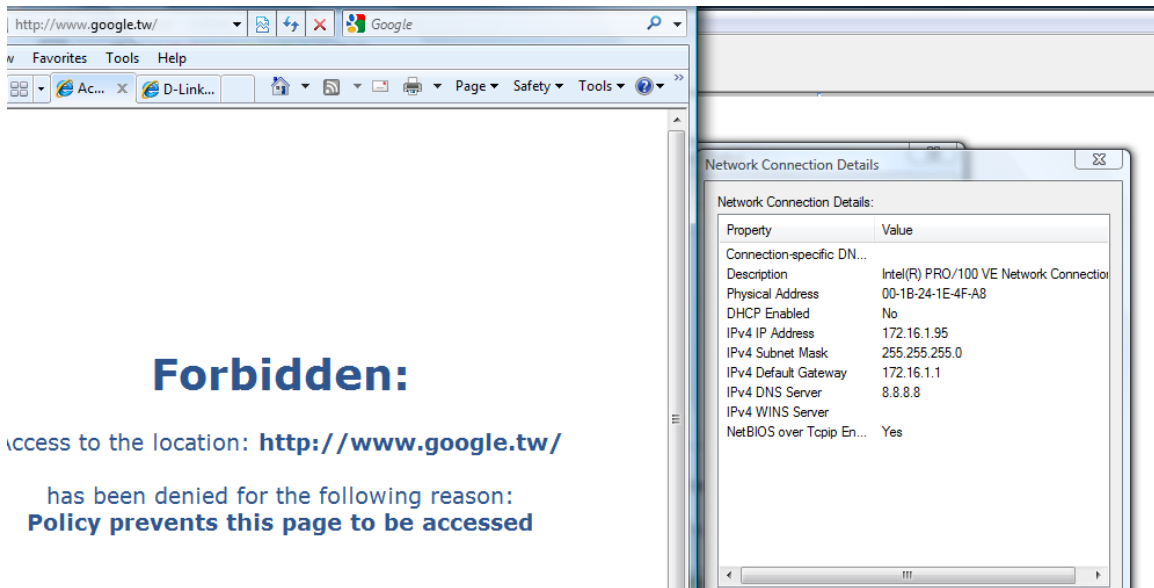
PC(172.16.1.1/24)----LAN(172.16.1.1)DFL-210(WAN)



Testing result:

Login with the test2 account which is employee group.

```
DFL-210:~> time
System time is 2010-01-21 20:43:45 (UTC+02:00)
DFL-210:~> userauth -list
Currently authenticated users:
-----
Login          IP Address    Source        Ses/Idle      Privileges
-----
test2         172.16.1.95  lan          none/27m     Employee
DFL-210:~>
```

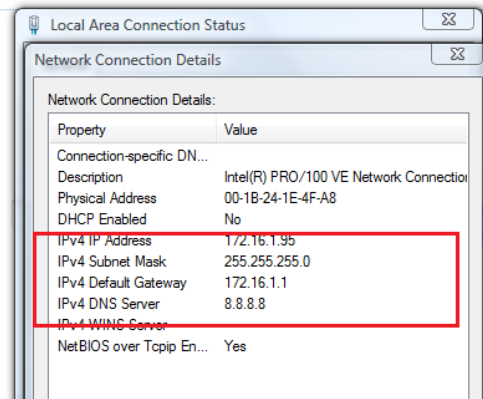
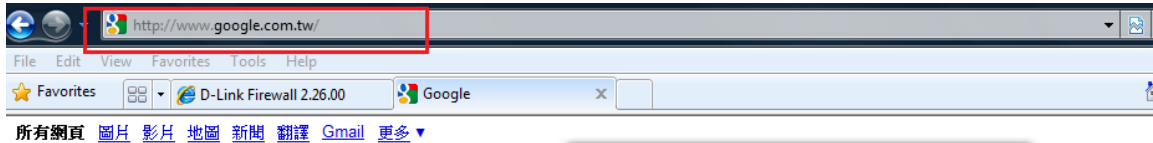


To test the time between the 17:00~18:59 and we set the firewall time as follows and test the above website again:

```
DFL-210:/> time
System time is 2010-01-21 17:53:39 (UTC+02:00)
DFL-210:/> userauth
Valid options: -list, -privilege, -remove, -user, <enter>
DFL-210:/> userauth -list
Currently authenticated users:
```

Login	IP Address	Source Interface	Ses/Idle Timeouts	Privileges
test1	172.16.1.102	lan	none/26m	Manager
test2	172.16.1.95	lan	none/28m	Employee

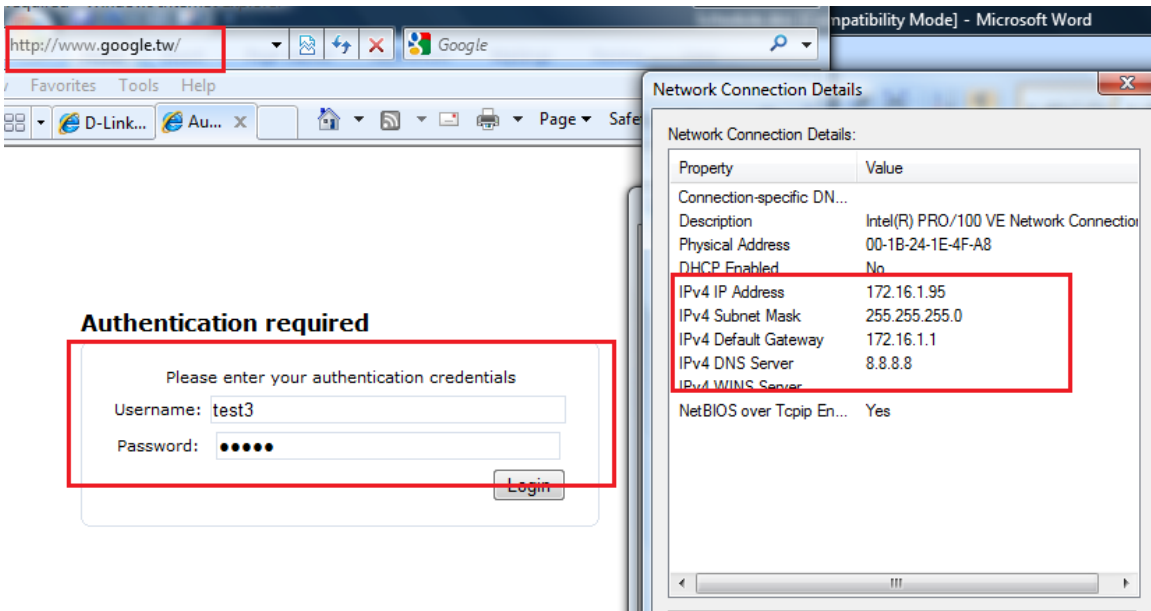
```
DFL-210:/>
Ready
```



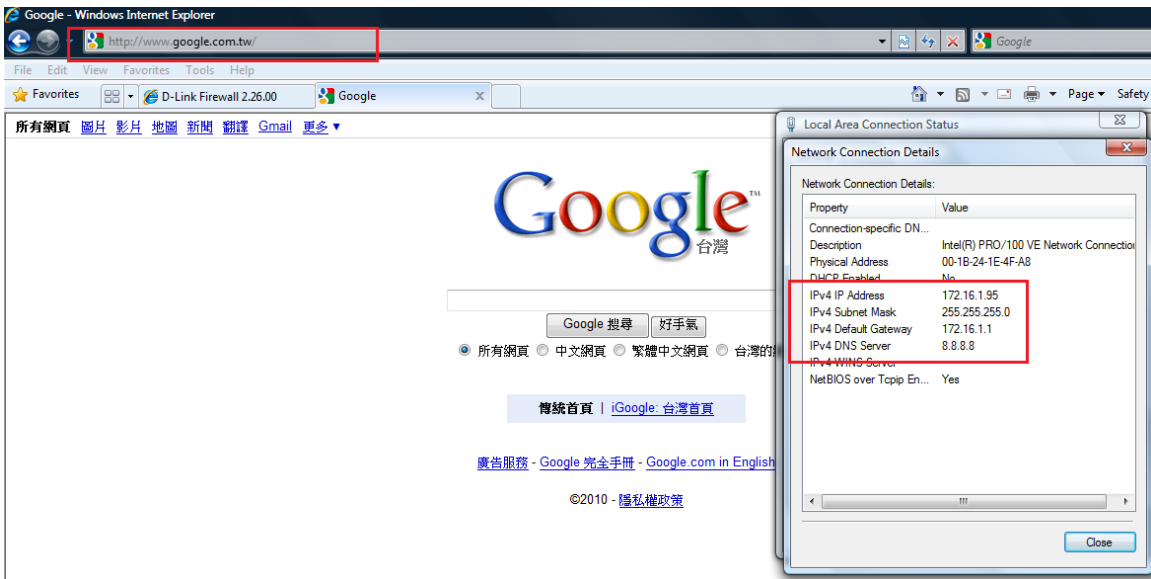
階搜尋
言選項

Test the other groups:

```
DFL-210:/> userauth -list
No authenticated users
DFL-210:/> time
System time is 2010-01-21 18:16:23 (UTC+02:00)
```

```
DFL-210:~# userauth -list
Currently authenticated users:
Login          IP Address      Source          Ses/Idle
-----
test3          172.16.1.95    lan             none/29m     others
DFL-210:~# time
System time is 2010-01-21 18:21:01 (UTC+02:00)
```



```
DFL-210:/>
DFL-210:/> time
System time is 2010-01-21 20:33:42 (UTC+02:00)
DFL-210:/> userauth -list
Currently authenticated users:
```

Login	IP Address	Source Interface	Ses/Idle Timeouts	Privileges
test3	172.16.1.95	lan	none/21m	others

```
DFL-210:/>
```

The screenshot shows a Windows Internet Explorer browser window with the address bar containing `http://dtrack.dlink.com.tw/`. The main content area displays the error message "Internet Explorer cannot display the webpage". A "Local Area Connection Status" window is open, showing "Network Connection Details" for the Intel(R) PRO/100 VE Network Connection. The details include:

Property	Value
Connection-specific DN...	
Description	Intel(R) PRO/100 VE Network Connection
Physical Address	00-1B-24-1E-4F-A8
DHCP Enabled	No
IPv4 IP Address	172.16.1.95
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	172.16.1.1
IPv4 DNS Server	8.8.8.8
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes