Setting up anonymous web access for guest devices - “Bring Your Own Device”

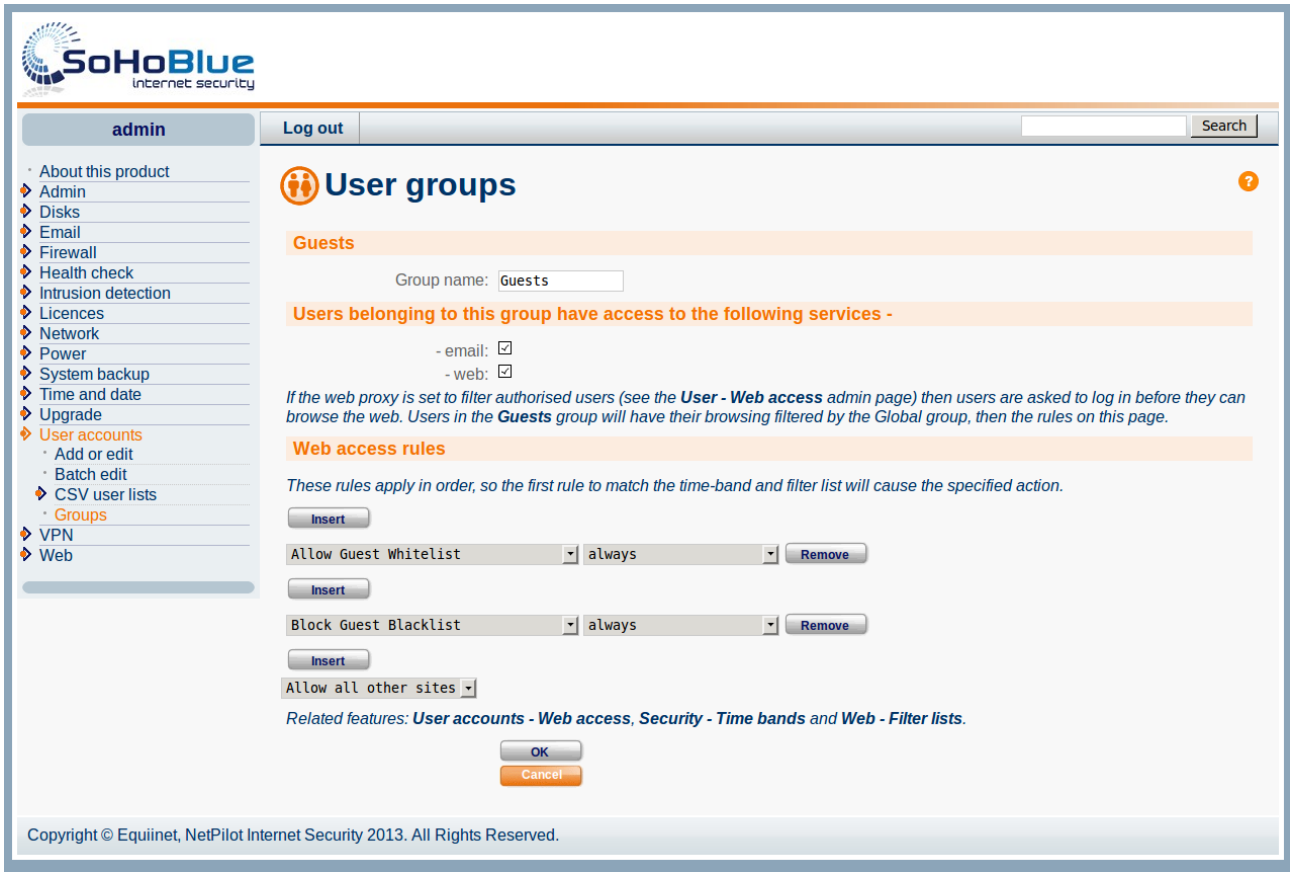
The typical scenario is that you are using Active Directory authentication on your network. (However this applies to NetPilot or LDAP authentication modes also.) You wish to introduce guest devices which are not part of the Active Directory domain, and you don't want your guest users to be prompted for a username and password when they browse the internet.

There are several ways to implement this, depending on the degree of separation between the fixed devices and the guest devices.

Scenario A. The guest devices are in a dedicated IP address range.

This is the most straightforward to set up and is the recommended configuration for new deployments.

1. Go to Web>Filtering>Site lists and create a whitelist called “Guest Whitelist” and a blacklist called “Guest Blacklist”. In these lists, tick site categories to be allowed and blocked as required.
2. Go to Users>Groups and create a group called “Guests” for the guest devices. Attach “Guest Whitelist” and “Guest Blacklist” to this group, as shown below:-



3. Go to Web>Filtering>IP Address Groups.
4. Create a new address group called “Guests”. Enter the network address and network mask of the guest network, and set the group to “Guests”.
5. If you have multiple guest networks, repeat step 4 for each additional network.

Scenario B. The guest devices and the fixed devices are in the same address range

There are two methods, based on whether you need to give your guest users access to HTTPS (secure) sites and you also wish to filter access to HTTPS sites.

If 'no' :-

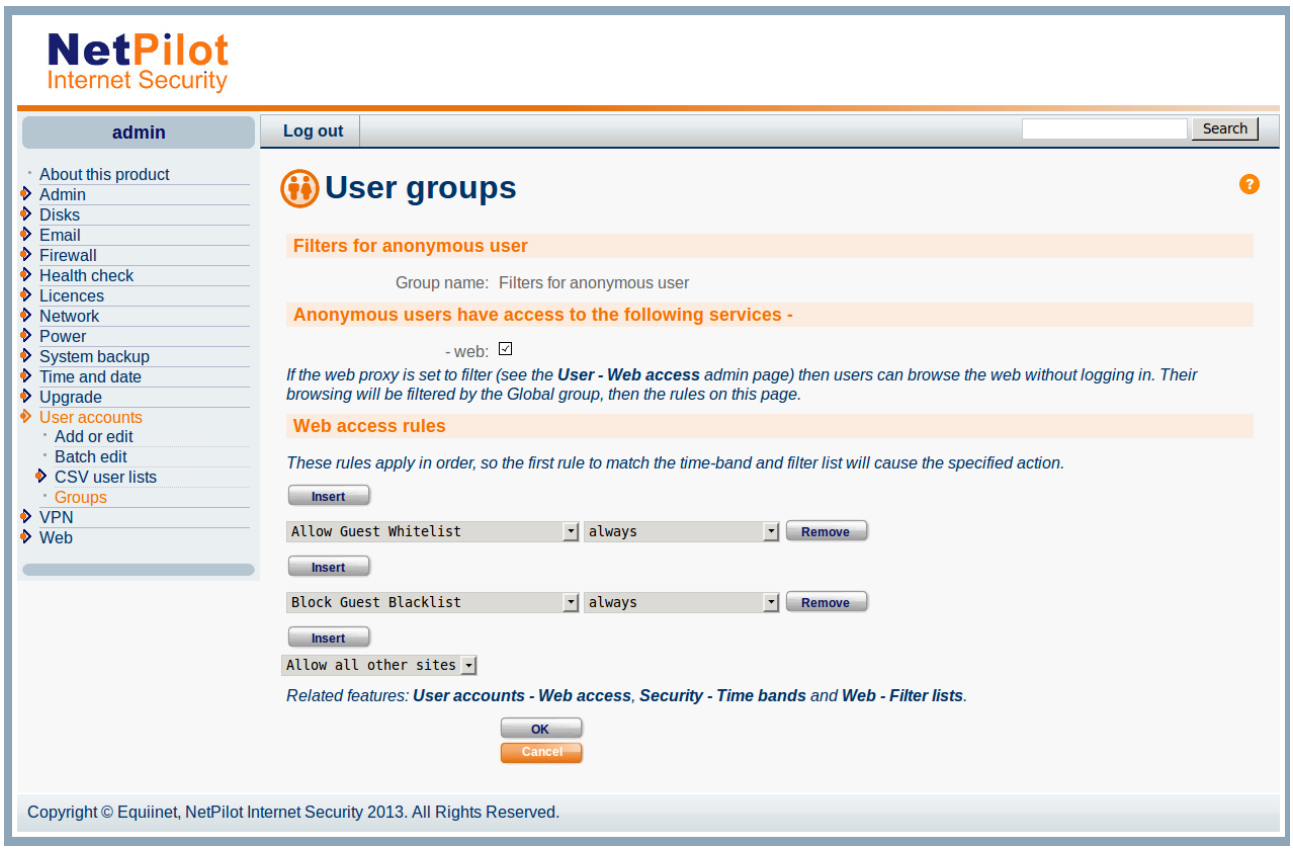
Configure transparent filtering for guest devices on the Trusted/Internet firewall, by following the instructions below.

1. Go to Firewall>Firewall Overview>Trusted/Internet.
2. Set 'web' to 'accept: url-filter'.
3. Set 'secure web' to 'accept' or 'reject', depending on whether guest devices should have access to HTTPS sites or not.

If 'yes' :-

All devices will need to access the NetPilot's proxy server for their web access. To minimise configuration on the guest devices, we'll create a PAC (Proxy Auto Configuration) file which directs guest devices to a dedicated proxy port. Follow the instructions below:-

1. Go to Firewall>Firewall Overview>Trusted/Local.
2. Tick the box to go into Advanced mode.
3. Add a new service: “web proxy url-filter”.
4. Set the action on “web proxy url-filter” to “accept”.
5. Go to Users>Groups, and edit the “Filters for anonymous user” group. Ensure that there is a whitelist and blacklist associated with this group. If not, go to Web>Filtering>Site lists, and create a “Guest Whitelist” and “Guest Blacklist”. Tick site categories to be allowed and blocked as required. Then attach the guest whitelist and guest blacklist to the “Filters for anonymous user” group as shown below:-



6. Open the supplied example file “wpad.dat” in a text editor such as Wordpad. Edit the IP address in this file to match the LAN1 IP address of the NetPilot unit. The wpad.dat file should read as follows:-

```
function FindProxyForURL(url, host)
{
        return "PROXY 10.0.0.1:8106"
}
```

The port number should be 8106, and the IP address should be changed to match the LAN1 IP address of the NetPilot.
7. Upload your edited version of wpad.dat to the webadmin fileshare of the NetPilot unit. You can do this via the Windows file browser or via FTP. In both cases the username is 'webadmin' and the password is the same as the admin password which you use to log in to the admin interface.
8. Restart guest devices so that they pick up the new proxy settings. If a device continues to give an authentication prompt, check the browser settings and ensure that proxy auto-detect is enabled.
9. Permanently connected devices should have their proxy address and proxy port configured manually in the browser settings. The proxy address is the NetPilot's LAN1 IP address, and the port is 8000.