Wireless Hotspot Information and FAQ:

Creating and printing tickets

Tickets are created and printed through the hotspot administration web site hosted at Hitech Support.

Printing is handled by a Crystal Reports Print object that will be automatically downloaded and installed to the web browser the first time printing is used. This requires local administrator rights on the computer just for the initial installation. Once installed, it is available for any user on that computer, even if they are an unprivileged user.

As this is a hosted service, no application software is required to be installed, and the administration web site can be accessed using any computer.

Wireless Access Points

Any existing sonicpoint access points are re-configured to run in 'stand alone' mode, meaning they operate as a standard access point and are used simply for accepting any wireless connections. This allows the hotspot controller to manage and authenticate hotspot connections.

A single open SSID is broadcast from the sonicpoints for the hotspot users to connect to.

Hotspot controller

Once hotspot users are connected, the hotspot controller performs the initial redirection to a login page for unauthenticated users, and enforces login polices for hotspot users – such as download and time limits. It also stops any connectivity to the internet until users are authenticated by a ticket.

The hotspot controller physically sits between the wireless access points and the Sonicwall firewall. Once users are authenticated, the Sonicwall firewall takes care of segmenting the traffic away from the rest of the network.

Sonicwall firewall

Any wireless traffic is physically segmented from the rest of the network via interface assignment and VLANs.

The wireless access point is also assigned as an 'unsecured' zone, and as a result, it only allowed to reach the Internet. It is not allowed to reach LAN or DMZ zones.

Wireless traffic is then subjected to the same security measures as WAN traffic, such as stateful inspection, deep packet inspection, reassembly-free fragmented packet handling.

Other security features such as layer 7 applications filtering, anti-virus and anti-spyware are also available, but are subscription based features.

Wireless Internet Access For Libraries – FAQ

Q: How does it work? I assume people have to come in and log on with user ID and a password.

A: We setup a Wireless Access Point (small wireless radio device) in the vicinity of where the public users will be able to sit at a desk with their laptops. This Wireless Access Point is connected back into the Sonicwall firewall and hotspot controller. The wireless access point then allows public users to connect to your existing NSW.net internet service.

The users simply turn on their laptops and turn on their wireless network card. Their laptop should then locate the broadcasted Wireless Access Point automatically and they can browse and connect to it.

There are two ways that we can setup the user logins:

1. We can leave it open to any users who are in the vicinity which means that they can connect without having to put in a username and password. The advantages of this is that it is simple and straight forward but then does not allow the library to control access to the facility. Hence the facility can be abused by a single user sitting somewhere outside of the library. Downloading large files can saturate the link for the whole day eg. Downloading of movies.

2. The second way is to setup the Wireless Hotspot to request a username and password when someone connects to it and tries to access the Internet. The tickets can allow a specific amount of browsing time and download amount. Eg. 1 or 2 hours, 200Mb, and they will also have an expiry date and time. The users are prompted to go to a service desk and request a ticket. This can be provided to restrict access to only library members. Once the time period expires the username and password becomes obsolete and cannot be used again. You can also issue a ticket to users after they have read and agreed to your internet usage policy.

Q: Who issues user IDs and passwords and how long are they valid for?

A: See section 2. above

Q: Can users give their passwords to their friends?

A: Users can give the ticket with the username and password to a friend who can use the remaining time but the system will not allow two devices to log in simultaneously with the same username and password.

Q: Is there a limit on how long they can use the Internet?

A: See section 2. The tickets can allow a specific amount of browsing time. E.g. 1 or 2 hours, and they will also have an expiry date and time and download limit. Bandwidth limiting on a per-user basis is also implemented.

Q: I guess what we really want to know is what security measures do we need to implement in order to make sure that people and especially young people, do not access inappropriate websites.

At the moment we at least have an Internet policy that customers have to accept before using the Internet, and for young people under the age of 16 we require signed parental permission. We are not sure how this will work with people coming in with their laptops.

A: There are two methods available to provide this facility. NSW.net may be able to provide access to an Internet based Content Filtering solution called "Internet Sheriff". This is a web based utility which allows the administrator to log in and set rules on what type of content based on categories are allowed to pass in and out of the Internet service. This is limited to setting one policy per library/Internet connection.

The second option is to deploy a separate third party Web Content Filtering facility with the capability of setting multiple policies based on groups of PC's or Users. We can discuss this if the above option cannot be provided or does not meet your requirements.

Q: Are there any libraries already using this technology, and if so can you please send me a few names so we can contact them to find out how this is working out for them.

A: Joyce from NSWnet can provide you with some of these reference sites. We will need to give them a courtesy call prior to providing you with their details.

In addition to your questions we can also provide the following features:

- Bandwidth Management capability to control how much of the available Internet service will be used buy the public access PC's versus the wireless PCs. Hence limit the impact of the Wireless hotspot on the current public network. Bandwidth throttling on a per user basis, so one wireless hotspot user cannot use all the bandwidth from other wireless users.

- We can also throttle the amount of bandwidth that is provided to users who are browsing multimedia sites eg. You tube. This will provide more bandwidth to users who are trying to use the facility for actual research.

- Monthly Reporting on the amount of tickets created, printed, Internet Usage, Bandwidth by Device, Top Web Sites, Top services

- On demand reporting of hotspot bandwidth, tickets generated, tickets used, number of devices using the hotspot, number of tickets used per device, top downloaders by ticket, top downloaders by device.

Installation & Technical Requirements:

- The Access Point (already provided) needs to be mounted in the vicinity where the users will be located to use the facility. The device can provide a service to both inside and outside areas depending on where it is located. Once we enable the Access point then we can move it around the library and test signal strength to cover the desired areas.

- We can also connect multiple Access points to cover more than one area. A switch will be required to connect multiple devices to the nominated WLAN port.

- The Access Point is powered up via a PoE injector hence we only need to run a single Cat 5/6 cable to the location where it will be mounted.

- Internet Explorer 6 or higher.

- We can assist to install the facility remotely with the assistance of one of the Technical guys from the library of Council. This takes about 1 – 2 hours. Otherwise an onsite visit can be scheduled which will incur installation costs.