serverfault

How do captive portal network connections work?

Asked 11 years, 11 months ago Modified 4 years, 11 months ago Viewed 14k times

11

Internet access at hotels, airports cafes is often gated by a captive portal which forces you to a particular web page on first use, for example a payment page or some page to accept a terms of service or an authentication/authorization page. You see this with both wireless and wired connections.

How does this work?

internet captive-portal wifi

Share Improve this question Follow

edited Mar 12, 2012 at 1:12

asked Mar 12, 2012 at 0:26

Howiecamp
495 3 9 17

2 Kinda like this, but not done for evil. ex-parrot.com/~pete/upside-down-ternet.html – Zoredache Mar 12, 2012 at 7:49

3 Answers

Sorted by: Highest score (default)

19

It certainly varies by vendor of the wireless product but in my experience it usually works something like this:

1. Your laptop makes a wireless connection to an intelligent access point, which may be connected to a centralized management station.
2. Your first web request is intercepted and replied to with a `Location:` header that redirects you to a login/policy page (e.g. http://hotelwireless.net/login). This might live directly on the intelligent access point, or on a central management station.
3. Once you've completed authentication, your MAC address is added to a list of allowed clients causing future requests to be correctly routed to the Internet, or accessible Intranet resources.

With regards to what to call it, I've heard it referred to as a "captive portal" or "wireless access portal" most frequently.

Share Improve this answer Follow

answered Mar 12, 2012 at 0:49

Kyle Smith
9,743 1 31 32

2 I have also seen it using dns, so the first dns query will be resolved to the login/policy page. – Niko S P Mar 12, 2012 at 1:19

1 Are you looking to set one up? There are some quick, easy and secure linux distros like pfSense that you can deploy in less than an hour. – G Koe Mar 12, 2012 at 2:39

2 How does the client side work? Windows 10, upon getting such a wifi connection, will launch default browser to go to the portal. Android 5 phones will launch a `Sign-in to Network` app (not the default browser) which basically just show that portal page. Is there a new protocol involved? What are its specifications? – Old Geezer Jan 4, 2016 at 14:49

I know it's an old post, but how do you intercept juts the first web request (or rather web requests until the user has authenticated by some means like clicking a button) ? – Dominik Feb 11, 2016 at 0:57

6

First for achieving the redirection, you need an inline authenticator (access controller). In context of your topic, you will need a Wireless lan controller if you opt for central management of AP. OR you can also place a captive portal type of network access controller with Wall garden features.

NAS monitors the traffic entering the downlink (client side) through promiscuous mode raw socket and when the browser initiated traffic for a unauthenticated client is detected a HTTP redirection is given to it as response. So browser on receiving gets redirected to our CAPTIVE portal homepage, which can be hosted inline on authenticator or out of box at some external web server.

The sole work of this page is to provide user a UI to enter credentials. the credentials entered are forwarded back to the authenticator Daemon like chilli in case of coova chilli, futher these credentials are passed as radius request to the RADIUS server or may be checked locally. Upon successful authentication the state of the client at authenticator is marked authorized and client is granted access.

How Redirection is achieved

The most widely used approach is to intercept the HTTP request initiated by user and 302 code as response to client. In chilli it is done via below function

```
http_redirect2() {

cat < <  EOF
HTTP/1.1 302 Redirect

Location: $1

Set-Cookie: PORTAL_SESSIONID=$PORTAL_SESSIONID

Set-Cookie: COOVA_USERURL=$COOVA_USERURL

Connection: close

EOF
    exit

}
```

This redirection can be easily achieved pragmatically controlled tun tap interface to client side interface which intercepts client traffic. Further redirection can be achieved via DNS poisoning too but may sometimes cause problem if responses got cached at client browser. Further things can be done more specifically according to the problem domain. I can help you with that if you want.

Share Improve this answer Follow

edited Oct 20, 2016 at 1:54
Weaver
1,962 12 13

answered Oct 17, 2016 at 10:50
Arjun sharma
625 4 9

6

There is a great description of this at https://www.arubanetworks.com/vrd/GuestAccessAppNote/wwhelp/wwhimpl/js/html/wwhelp.htm.

Here's part of it:

> Captive Portal Authentication Process
>
> Captive portal is a Layer 3 authentication, which requires that the devices connect to the network and obtain an IP address and related DNS information before authenticating through the captive portal. The following steps explain the entire captive portal process when the native ArubaOS is used for captive portal authentication:
>
> 1. The device that is associating to the guest SSID is assigned an initial role (guest-logon role in the example configuration). This initial role allows DHCP, so the user gets an IP address.
>
> 2. The user opens a browser and makes an HTTP (or HTTPS) request to some destination (for example, www.bbc.com).
>
> 3. The resolver in the device sends a DNS request to resolve the www.bbc.com. The initial role (guest-logon role) permits DNS services, so the resolver can communicate with the DNS server.
>
> 4. The DNS server replies with the correct address to www.bbc.com.
>
> 5. The resolver tells the browser which IP address to use based on the DNS reply.
>
> 6. The browser initiates a TCP connection to port 80 of the www.bbc.com address.
>
> 7. The controller intercepts the connection and spoofs the initial TCP handshakes of the HTTP process. At this moment, the client browser thinks it is communicating with the bbc.com server.
>
> 8. When the browser sends the HTTP GET request for the web page, the controller replies saying that bbc.com has “temporarily moved” to .
>
> 9. The browser closes the connection.
>
> 10. The browser attempts to connect with , but it first needs to send a DNS request for the address.
>
> 11. The actual DNS server responds that it cannot resolve https://securelogin.arubanetworks.com, but the controller intercepts that reply and changes the packet to say that securelogin.arubanetworks.com is at the IP address of the controller itself. Remember that

it is critical that the DNS server sends back a reply to the query. It is only then that the controller can spoof the reply back from the DNS server. Sending a DNS request without receiving a reply is not sufficient, since without a reply the controller will never help the client resolve securelogin.arubanetworks.com.

12. The browser initiates an HTTPS connection to address of controller, which responds with the captive portal login page, where the guest authenticates.

13. After successful authentication, the user is assigned the post authentication role (auth-guest role in the example configuration). This is the default role in the captive portal profile.

14. After authentication, the browser is redirected to bbc.com at the address originally resolved by the DNS. Alternatively, if a welcome page is configured, the browser is redirected to the welcome page.

15. To successfully redirect to the original web page the controller spoofs a reply from bbc.com to tell the client that bbc.com has "permanently moved" to bbc.com. This step corrects the "temporary relocation" that occurred as part of the captive portal login.

16. This causes the client to re-query DNS for the address of www.bbc.com.

17. The browser starts to communicate with the actual bbc.com server.

Share Improve this answer Follow

answered Apr 6, 2019 at 14:46

dǝɥɔS ʇoıllƎ

165 1 6