Setting up BYOD with Ruckus, Smoothwall and HP Switch

I have used the following for my setup:

HP 4204vl as the core switch – 172.16.24.24 255.255.248.0
HP 6108 as an edge switch
Smoothwall UTM 1000 (default gateway) – Port 1 connected to the network - 172.16.24.8 255.255.248.0
Ruckus 1100 Controller
Ruckus 7363 Access point
XP Laptop and Android Phone - DHCP

The network is split up into 5:

VLAN1: Main Domain = 172.16.24.1 – 172.16.31.254 | 255.255.248.0
VLAN2: BYOD-Staff = 192.168.12.1 – 192.168.15.254 | 255.255.252.0
VLAN3: BYOD-Student/ BYOD-Post16 = 192.168.16.1 – 192.168.20.254 | 255.255.248.0
VLAN4: Guest = 192.168.24.1 – 192.168.24.254 | 255.255.255.0
VLAN5: BYOD-Post16=192.168.25.1 – 192.168.25.254 | 255.255.255.0

The Core Switch Config

On the Core switch I have the following configured:

```
hostname "ProCurve Switch 4204vl"
snmp-server contact
snmp-server location
max-vlans 256
module 1 type J8768A
module 2 type J9033A
module 3 type J9033A
module 4 type J9033A
ip default-gateway 172.16.24.8
ip routing
snmp-server community "public" Unrestricted
vlan 1
   name "DEFAULT_VLAN"
   untagged A1,A3-A24,B1-B24,C1-C24,D1-D24
   ip address 172.16.24.24 255.255.248.0
   ip helper-address 172.16.24.4
   no untagged A2
   ip igmp
   exit
vlan 2
   name "Staff-BYOD"
   untagged A2
   no ip address
```

```
  tagged A1,A3-A4,A9,A11,A14
  exit
vlan 3
  name "Stu-BYOD"
  no ip address
  tagged A1,A3-A4,A9,A11,A14
  exit
vlan 4
  name "Guests_BYOD"
  no ip address
  tagged A1,A3-A4,A9,A11,A14
  exit
vlan 5
  name "Post16-BYOD"
  no ip address
  tagged A1,A3-A4,A9,A11,A14
  exit
ip route 0.0.0.0 0.0.0.0 172.16.24.8
spanning-tree
```

Ruckus Configuration

5 SSIDs which are:

BYOD-Staff – set to access VLAN 2 – Authenticated against AD via membership
BYOD-Students - set to access VLAN 3 – Authenticated against AD via membership
BYOD-Post16 – set to access VLAN 5 – Authenticated against AD via membership
MainDomainNetwork – set to access VLAN1
Guests – Set to access VLAN4 – Ticket given out.

Creating the AAA Servers

Configure >> AAA Servers

1. Create the AD AAA server
    a. Give it a Name
    b. Type = Active Directory
    c. Global Catalog = Unticked
    d. Encryption = Unticked
    e. IP Adrress = {IP of a Domain Controller}
    f. Port = 389
    g. Windows Domain name = {your domain name}

2. Create the Smoothwall Radius Accounting AAA Server
    a. Give it a name {Smoothwall Radius ACCT}
    b. Type = RADIUS Accounting
    c. Encryption = unticked

d. Backup RADIUS = unticked
e. IP address = {the smoothwall IP Address}
f. Port = 1813
g. Shared Secret = {give it a password}
h. Confirm Secret = {type the password again}
   Retry Policy
i. Request timeout = 3 seconds
j. Max number of tries = 2 times

Creating the Hotspot Service for the Man In The Middle Certificate

Configure >> HotSpot Services > Create New

1. Give it a name {BYOD-Portal}
   Redirection
2. WISPr Smart Cliient Support = None
3. Login Page – Redirect unauthenticated user to = This needs to be an internal web server where you will host a BYOD page so users can download a certificate.
4. Start page = Redirect to the URL that the user intends to visit
   User Session
5. Session Timeout = Specify your own user session termination
6. Grace Period = Specify your own reconnect without re-authentication
   Authentication/Accounting Servers
7. Authentication Server = **Your AD** settings from AAA Servers
8. Accounting Server = **Smoothwall Radius ACCT** from AAA Servers. Send interim Update every **5** mins.
   Walled Garden
9. I have the following in here:
   IP address of internal webserver
   The IP address of the Zone Director
   School Website

Creating Guest Access

Within **Guest Access >> Restricted Subnet Access** I have had to add the BYOD and Guest Subnets, so i have added:

1. BYOD-Staff | Allow | 192.168.12.1/32
2. BYOD-Students/Post16 | Allow | 192.168.16.1/32
3. Guest | Allow | 192.168.24.1/32
4. BYOD-Post16 | Allow | 192.168.25.1/32

Configure Local Users to create guest tickets

Configure >> Users >> Create New

Username: [give it a username]
Full Name/Password : [Fill these details in]
Role: Select the role you just created, in this case its Guest Access

Creating WLANs

Configure >> WLANs >> Create New

Creating the Domain SSID

1. Name/ESSID = Name of wireless for domain machines
2. ESSID = Name of your SSID
3. Description = Give the WLAN a bit of a description
   WLAN Usages
4. Type = Standard usage
   Authentication Options
5. Method = Open
6. Fast BBS Transition = Unticked
   Encryption Options
7. Method = WPA2
8. Algorithm = AES
9. Passphrase = {Give it a passphrase}
   Options
10. Priority = High
    Advanced options
11. Access VLAN = State which VLAN your SSID is to be part of.
12. 802.11d = Ticked
13. Client Fingerprinting = Ticked
    Any other options that you would like to enable can be enabled here.

Creating the BYOD SSIDs

1. Name/ESSID = Name of your SSID {BYOD-Staff,BYOD-Post16,BYOD-Students}
2. ESSID = Name of wireless for domain machines
3. Description = Give the WLAN a bit of a description
   WLAN Usages
4. Type = Hotspot Service (WISPr)
   Authentication Options
5. Method = Open
6. Fast BBS Transition = Unticked
   Encryption Options
7. Method = None
   Options
8. Hotspot services = {BYOD-Portal}
9. Priority = High
   Advanced options
10. Rate Limit = Uplink {1 Mbps} Downlink {2 Mbps}
11. Access VLAN = State which VLAN your SSID is to be part of.
12. 802.11d = Ticked
13. Client Fingerprinting = Ticked

Any other options that you would like to enable can be enabled here.

Creating the Guest SSID

1. Name/ESSID = Name of your SSID {Guests}
2. ESSID = Name of wireless for domain machines
3. Description = Give the WLAN a bit of a description
   WLAN Usages
4. Type = Guest Access
   Authentication Options
5. Method = Open
6. Fast BBS Transition = Unticked
   Encryption Options
7. Method = None
   Options
8. Guest Access Service = {Name of created guest service}
14. Wireless Client Isolation = Ticked Isolate Wireless Client traffic from other client on the same AP.
15. Priority = High
    Advanced options
16. Rate Limiting = Uplink {I set mine to 2 Mbps} Downlink {2 Mbps}
17. Access VLAN = State which VLAN your SSID is to be part of.
18. 802.11d = Ticked
19. Client Fingerprinting = Ticked
    Any other options that you would like to enable can be enabled here.

Creating Roles so Staff access STAFF SSID and Post16 access POST16 SSID

Configure >> Roles >> Create New

Name: [Give it a name]
Policies: Tick the relevant WLAN you want your guests to have access to. I ticked only the Guest WLAN.
Guest Pass: Tick

This will add a local user to local database on Ruckus so your receptionist etc can create guest logins.

Smoothwall

Add new virtual interfaces

On port 1 (which is my port to the network) on the smoothwall; **Networking >> Configuration >> Interfaces**

Click **Add new Interface**

Configure Virtual Ports

Virtual Port 1a	Virtual Port 1b	Virtual Port 1c	Virtual Port 1d
Name: Port 1-1_BYOD-Staff **Parent Interface:** Port 1 Main Network **VLAN Tag:** 2 **Use as:** Basic Interface **Default IP addresses:** Leave this blank for now	Name: Port 1-2_BYOD-Students **Parent Interface:** Port 1 Main Network **VLAN Tag**: 3 Internal: Ticked **Default IP addresses:** Leave this blank for now	Name: Port 1-3_Guests **Parent Interface:** Port 1 Main Network **VLAN Tag:** 4 **Use as:** Basic Interface **Default IP addresses:** Leave this blank for now	Name: Port 1-4_Post16 **Parent Interface:** Port 1 Main Network **VLAN Tag**: 5 Internal: Ticked **Default IP addresses:** Leave this blank for now

Find each of the newly created Virtual Ports and Click on **Edit** and then **Add New Address**.

Status = Tick Enabled
Type = Static IPv4
IP Address = The Starting IP Address of the BYOD VLAN {192.168.12.1 | 192.168.16.1 | 192.168.24.1 | 192.168.25.1}
Subnet Mask = The subnet mask of the BYOD VLAN {255.255.252.0 | 255.255.248.0 | 255.255.255.0 | 255.255.255.0}
Gateway = None

Setup clients to access the SSL login page (Possibly not needed when using RADIUS but will set up anyway)

System >> Administration >> External Access

Add the ports of the BYOD VLANs

Interface: Port 1-1_BYOD-Staff Source IP: 192.168.12.0/22 Service: Web based on HTTP (80) Enabled: Ticked	Interface: Port 1-1_BYOD-Staff Source IP: 192.168.12.0/22 Service: Web based on HTTPs (442) Enabled: Ticked	Interface: Port 1-1_BYOD-Staff Source IP: 192.168.12.0/22 Service: RADIUS accounting (1813) Enabled: Ticked
Interface: Port 1-2_BYOD-Student Source IP: 192.168.16.0/21 Service: Web based on HTTP (80) Enabled: Ticked	Interface: Port 1-2_BYOD-Student Source IP: 192.168.16.0/21 Service: Web based on HTTPs (442) Enabled: Ticked	Interface: Port 1-2_BYOD-Student Source IP: 192.168.16.0/21 Service: RADIUS accounting (1813) Enabled: Ticked
Interface: Port 1-3_Guests Source IP: 192.168.24.0/24 Service: Web based on HTTP (80) Enabled: Ticked	Interface: Port 1-3_Guests Source IP: 192.168.24.0/24 Service: Web based on HTTPs (442) Enabled: Ticked	Interface: Port 1-3_Guests Source IP: 192.168.24.0/24 Service: RADIUS accounting (1813) Enabled: Ticked
Interface: Port 1-4_Post16 Source IP: 192.168.25.0/24 Service: Web based on HTTP (80) Enabled: Ticked	Interface: Port 1-4_BYOD-Post16 Source IP: 192.168.25.0/24 Service: Web based on HTTPs (442) Enabled: Ticked	Interface: Port 1-4_BYOD-Post16 Source IP: 192.168.25.0/24 Service: RADIUS accounting (1813) Enabled: Ticked

Please note, the end column might have been added automatically. On my Smoothwall, it was added automatically by Update 82.

Set Up DHCP

Services >> DHCP >> Global

Global Settings: Enabled: Ticked
Server: Selected
Enable Logging: Ticked

Interfaces:

Select all the appropriate interfaces. Here I selected the 3 virtual ports. I left *port 1 – Main Network Domain* unticked as I was already giving out DHCP addresses via my windows server to all the clients on the main domain.

Services >> DHCP >> DHCP Server

Select a DHCP Subnet from the drop down menu and click select. I created 3 and changed the names to:

BYOD-Staff, BYOD-Students, Guests, BYOD-Post16

And setup the network details.

In each of the DHCP subnets, I set up the network addresses:

BYOD-Staff:
Network: 192.168.12.0 Netmask: 255.255.252.0
Primary DNS: 192.168.12.1 Secondary DNS:
Default Gateway: 192.168.12.1 Enabled: Ticked

Scroll down to bottom of page and click Save.

BYOD-Students:
Network: 192.168.16.0 Netmask: 255.255.248.0
Primary DNS: 192.168.16.1 Secondary DNS:
Default Gateway: 192.168.16.1 Enabled: Ticked

Scroll down to bottom of page and click Save.

Guests:
Network: 192.168.24.0 Netmask: 255.255.255.0
Primary DNS: 192.168.24.1 Secondary DNS:
Default Gateway: 192.168.24.1 Enabled: Ticked

Scroll down to bottom of page and click Save.

Post16:
Network: 192.168.25.0 Netmask: 255.255.255.0
Primary DNS: 192.168.25.1 Secondary DNS:
Default Gateway: 192.168.25.1 Enabled: Ticked

Scroll down to bottom of page and click Save

Once the networks were setup, I had to setup the address ranges, so I first selected BYOD-Staff and filled in the following:

Add a new dynamic range:
192.168.12.21 – 192.168.15.254
Comment: BYOD-Staff Range
Enabled: Ticked

Click Add dynamic Range

Then selected BYOD-Students, filled in the ranges:

Add a new dynamic range:
192.168.16.21 – 192.168.20.254
Comment: BYOD-Students
Enabled: Ticked

Click Add dynamic Range

Then selected BYOD-Guests, filled in the ranges:

Add a new dynamic range:
192.168.24.21 – 192.168.24.254
Comment: BYOD-Guest Range
Enabled: Ticked

Click Add dynamic Range

Then selected BYOD-Post16, filled in the ranges:

Add a new dynamic range:
192.168.25.21 – 192.168.25.254
Comment: BYOD-Post16
Enabled: Ticked

Click Add dynamic Range

Once I had set all this up, I needed to click Restart from the top of the page.

Set Location Blocking

Guardian >> Web Filter >> location blocking

I had to make sure all the entries in here were set to allow

Check the SSL Login

Services >> Authentication >> SSL Login

I originally had SSL login set for transparent proxies. Since changing this to Core Authentication I no longer have the option to tick the SSL Login Redirection in SSL Login.

Setup the locations

Guardian >> Policy Objects >> Locations

Name: BYOD-Staff
Addresses: 192.168.12.1-192.168.15.254
Click: Save

Name: BYOD-Student
Addresses: 192.168.16.1-192.168.20.254
Click: Save

Name: BYOD-Guests
Addresses: 192.168.24.1-192.168.24.254
Click: Save

Name: BYOD-Post16
Addresses: 192.168.25.1-192.168.25.254
Click: Save

Setting up Transparent Proxies

Web Proxy >> Authentication >> Manage Policies

Create a new transparent proxy

BYOD-Staff
Step 1 - What:
Type = Transparent
Method = ~~Redirect users to SSL Login Page (with session cookie)~~ Core Authentication
Interface = {Select relevant interface} so I selected Port 1-1_BYOD-Staff
Port = 80
HTTPS = Ticked
Step2 - Where:
Select BYOD-Staff
Step 3 - Options for unauthenticated requests:
Select Unauthenticated IPs
Enabled: Ticked
Click: Confirm then at the summary screen click Save

BYOD-Students
Step 1 - What:
Type = Transparent
Method = ~~Redirect users to SSL Login Page (with session cookie)~~ Core Authentication
Interface = Port 1-2_BYOD-Students
Port = 80
HTTPS = Ticked
Step 2 - Where:

Select BYOD-Students
Step 3 - Options for unauthenticated requests:
Select Unauthenticated IPs
Enabled: Ticked
Click: Confirm then at the summary screen click Save

BYOD-Guests
Step 1What:
Type = Transparent
Method = Identification by location
Interface = Port 1-3_BYOD-Guests
Port = 80
HTTPS = Ticked
Step 2 - Where:
Select BYOD-Guests
Step 3 - Options for unauthenticated requests:
Select Unauthenticated IPs
Enabled: Ticked
Click: Confirm then at the summary screen click Save

BYOD-Post16
Step 1What:
Type = Transparent
Method = ~~Redirect users to SSL Login Page (with session cookie)~~ Core Authentication
Interface = {Select relevant interface} so I selected Port 1-4_BYOD-Post16
Port = 80
HTTPS = Ticked
Step 2 - Where:
Select BYOD-Post16
Step 3 - Options for unauthenticated requests:
Select Unauthenticated IPs
Enabled: Ticked
Click: Confirm then at the summary screen click Save

Note: A mistake which I found out and thanks to users of Edugeek was the windows XP and IE don't like HTTPS so I have told my users if they are using XP as their OS, they really need to be using Firefox or Chrome.

~~Check the DNS Proxy~~

~~Services >> DNS >> DNS Proxy~~

~~Interfaces: All interfaces are to be Selected / Ticked~~
~~Advanced: Forward SRN & SOA records: Not Ticked~~

Setting the RADIUS connection between Ruckus and Smoothwall

Services >> Authentication >> BYOD

Here you need to add the Zone Director(s) to the Authorized RADIUS clients. Click **Add new RADIUS client** >>

Status = Enabled
Name = Give it a name
IP Address = IP Address of your Zone Director(s) (only 1 at a time if you have more than 1)
Shared Secret = The password you used when you set up the AAA Server Smoothwall RADIUS ACCT
Confirm the shared secret
Give it a comment if you wish to do so.
Click Add

Download the Man In The Middle Certificate

Now that Google services have started to use HTTPS, we need to download and push the Smoothwall Man In The Middle (MITM) certificate out to clients.

Web Proxy >> Global Proxy >> Settings

Make sure Client Certificates is selected next to Proxy Security and Download the Client Certificate to your machine. This certificate needs to sit on the webserver in where the unauthenticated users will be directed to before they login to the wireless network. This enables their local accounts / devices to use the MITM certificate before they join the WLAN. If they don't download and install the certificate, they will end up seeing the HTTPS insecure message on HTTPS sites.

The BYOD unauthenticated landing page

This landing page is just a basic landing page which unauthenticated devices will hit before signing in to the WLAN. It has a bit of an explanation about downloading and installing the certificate, a link to download the certificate, help pages incase users don't know what to do, a link to continue logging in to the WLAN which points to https://{IPAddressOf ZoneDirector_or_DNSName/user/user_login_auth.jsp and most importantly, a disclaimer about the certificate (as Googles Android OS KitKat 4.4 and later has some security issues) which states:

Please note: *If you are installing the certificate on an Android device which is running version KitKat 4.4 or later, you will get a "Network will be monitored by an unknown third party" warning message. This warning can be daunting but it is displayed due to a flaw with Google's security policy.*

We issue a user/device certificate that Google does not trust however you don't need to worry as the school does trust this certificate and keeps you & your device safe whilst on the school WiFi so any warnings your device provides can be disregarded (open the notification bar (swipe down from the top) and swipe it off) – Please do not remove the certificate otherwise your user credentials will become vulnerable.

These Security issues can be found here: https://code.google.com/p/android/issues/detail?id=62644. The other way to remove this warning is to ask the user to root their device and add the certificate manually into the android device.