**CCDC Palo Alto FW Configuration Steps**

1. **(Optional?) Type command “sudo screen /dev/ttyUSB0 9600,cs8,-ixon,ixoff”**
2. **(Optional) Start up PAFW and go to maintenance mode and factory reset system.**

* **Type: “maint” to access maintenance mode**

1. **Restart PAFW and input default admin credentials:**

* **Username: admin**
* **Password: admin**

1. **Change default Password:**

* **Type “configure” to enter configuration mode**
* **Type “set mgt-confg users admin password <new password>**
* **Set password to:**

1. **Turn of management interface TEMPORARILY**

* **Type “set deviceconfig system permitted-ip 127.0.01**
* **# ”commit”**

1. **Turn off external data Interface TEMPORARILY**

* **Type “set network interface ethernet ethernet1/x link-state down**
* **# “commit”**

1. **Review System Information**

* **IN OPERATIONS MODE**
* **Type “show system info”**
* **Document important info**

1. **(Optional?) Change Management Interface IP**

* **Type “set deviceconfig system ip-address x.x.x.x netmask x.x.x.x default-gateway x.x.x.x dns-setting servers primary x.x.x.x”**
* **# commit**

1. **Only allow Secure Protocols to connect:**

* **Type “set deviceconfig system service disable-https no**
* **# commit**

1. **Check to make sure there are no malicious admin accounts:**

* **IN OPERATIONS MODE**
* **Type “show admins all”**
* **# delete mgt-config users xxxxx**
* **# commit**

1. **Turn Data Interfaces / Management Interface back on IF OFF:**

* **IN CONFIGURATION MODE**
* **Type “set network interface ethernet ethernet1/x link-state up”**
* **# commit**
* **Type “set deviceconfig system permitted-ip x.x.x.x”**

1. **License the PAFW**

* **Once logged into GUI, go to “Device” tab**
* **Open “Licenses”**
* **Under “Licensing Management” click “Retrieve license keys”**
* **Reboot the FW**
* **Log back into GUI and go back to “Device” to see if it worked**

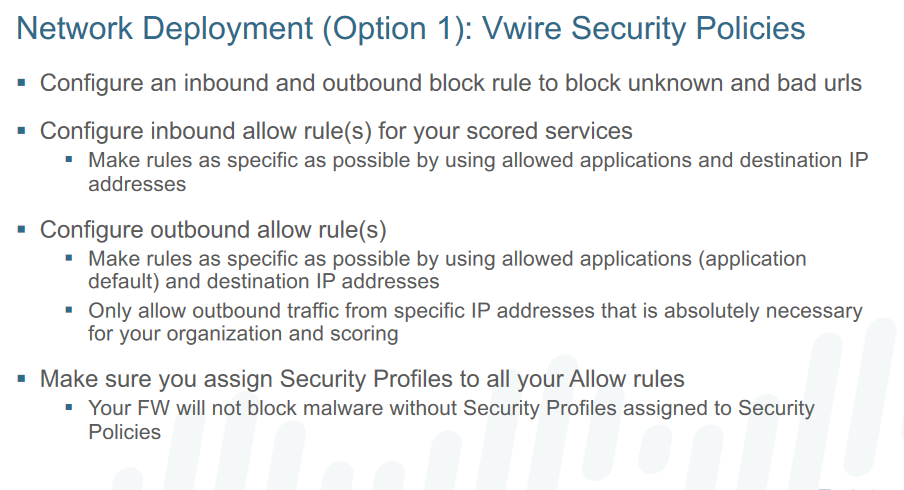
1. **Update Signatures**

* **Go to “Device”**
* **Click on “Dynamic updates”**
* **Click “Check now” and proceed to install all necessary updates**

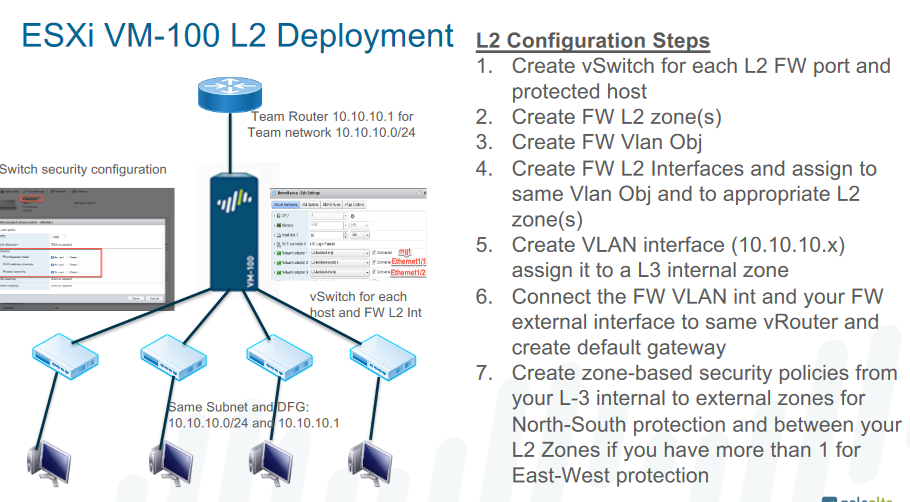
1. **Determine and Configure Network Deployment (layer 3, Layer 2, V-Wire)**

**Option 1 (V-Wire) – Most Recommended because easiest to set up but lacks some protection**

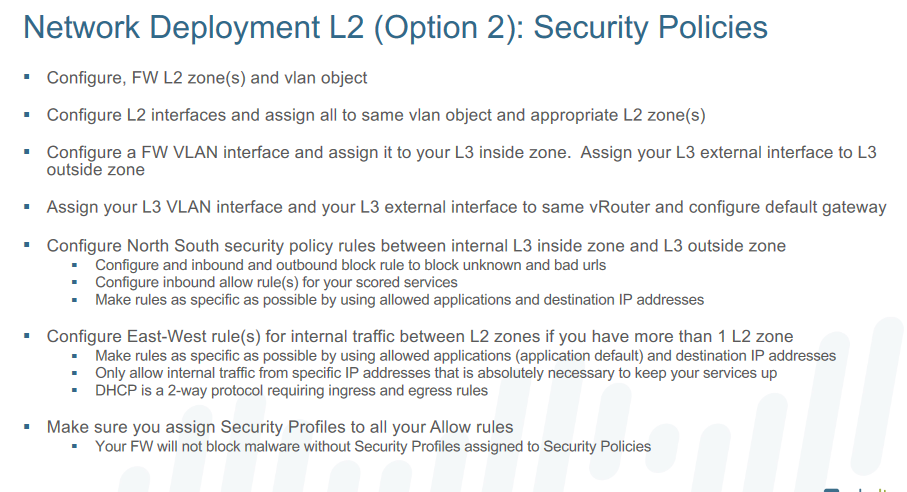
* **Go to “Policies” tab – “Security” – Block all inbound unknown URLs**
* **Under “Profile” – click the action you wish to take**

****

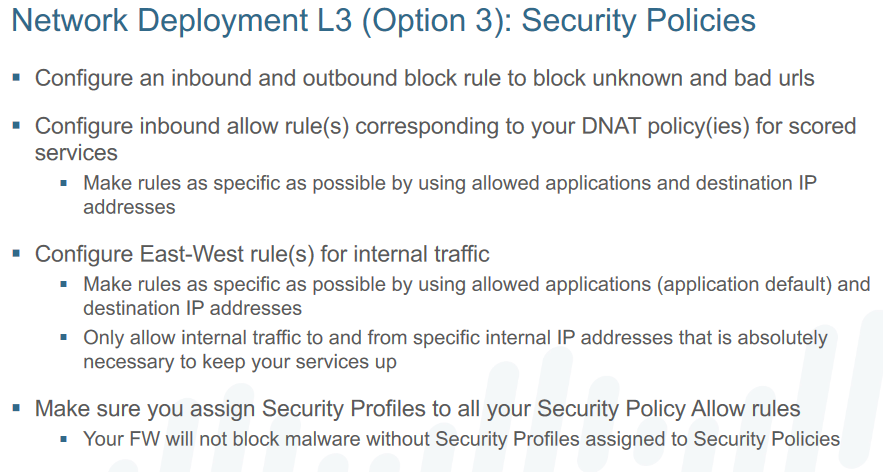
**Option 2 (L2) – Most applicable if we only have 1 Subnet, 1 Switch and no router**

****

**L2 Security Policies:**

****

**Option 3 (L3) – Most secure but hardest to configure properly – REPLACES ROUTER**

****

**How to configure L3 Deployment**

1. **Go to “Application Filter” Click “Add”**

* **Click “file sharing” Click “peer-to-peer”**
* **Name it “Peer-to-Peer”**
* **OK**

1. **Go to “Policies” tab Click “Add”**

* **Name p2p**
* **Source = trust**
* **Destination = untrust**
* **Application – Type “Peer-to-Peer”**
* **Action – Set to “Deny”**
* **Move p2p above all other rules**

1. **In Policies, Click on “rule1”**

* **Actions – profile type change to “Profiles”**
* **And set all underneath to “default”**
* **After this is done, Connect router to untrust /2 and switch to trust /x**

1. **Go to “Network” tab ‘zones’ and change trust/untrust type to “Layer 3”**

* **Go to ‘interfaces’ Change /1 to Layer 3 and set virtual router to “default”**
* **Change IPv4 to what you need**
* **Change /2 to Layer 3 and set virtual router to default**
* **Set zone to trust and change Ipv4 to private “Default gateway” config**