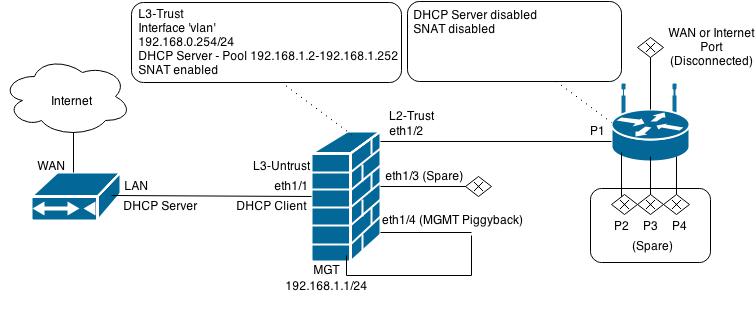
Setting up the PA-220 for Home and Small Office (SOHO)



**Purpose:** We intent to configure the PA-220 for home and small office use. This will be the most beneficial in a majority of situations and will give us more practice configuring SOHO environment firewalls.

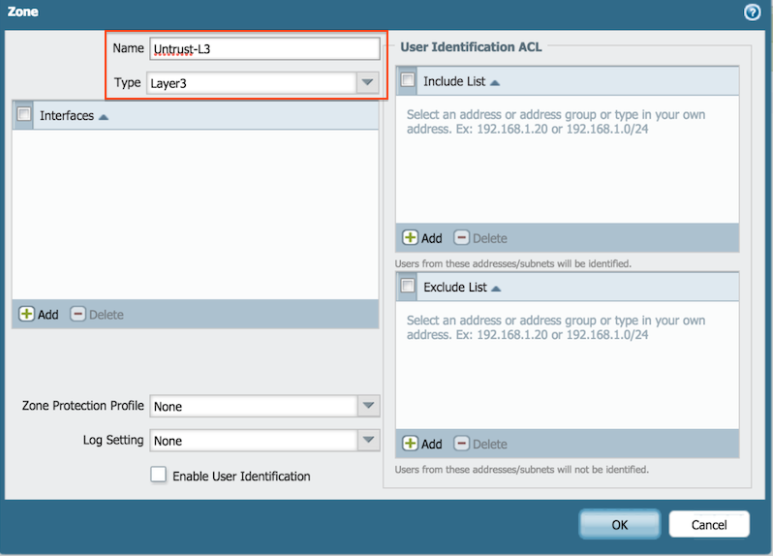
**Background information on Lab;** Palo Alto`s PA 220 firewall is a portable platform that enables safety for applications, users and content within the SOHO network. The firewall works in networking, security, content inspection and many other areas to keep your network safe. The web interface is simple to use and quite intuitive.

**Lab Summary:**   
Our first step is getting access to the PA-220 web interface. To do this we will need to connect an ethernet cable from the computer to the Palo Alto management port. After connecting the cable, we will configure our computer to have an IP of 192.168.1.2 and a subnet mask of 255.255.255.0 Then we will open a web browser and go to <https://192.168.1.1>. This is the default IP address of the PA-220 and we will use the default credentials admin, admin to login.

Once we have access to the web interface, we can begin to configure the PA-220 for a SOHO environment.

Create Security Zones,

Once in the web interface we go to Network, and then Zones and click add,



We then must add 3 security zones

Untrust L3, which is type; Layer 3

Trust L3, which is a type; Layer 3

Trust-L2, which is a type; Layer 2

Now we must configure the ethernet Interfaces to do so we must go to Network, Interfaces and configure ethernet 1/1



Under Ethernet 1/1 we need to set the virtual router to default and the security zone to Untrust L-3

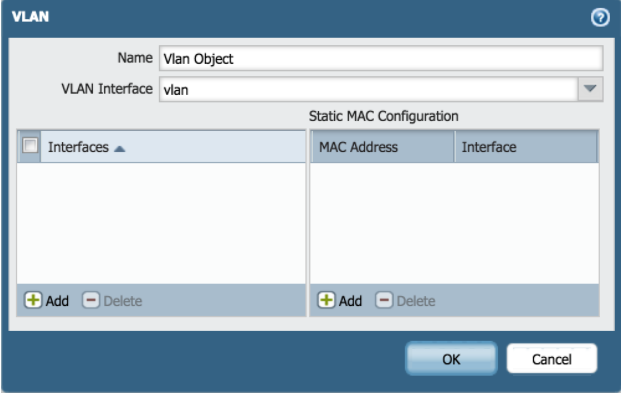
We then go to the IPv4 tab and enable it as a DHCP client



Following enabling the DHCP client we will connect to the wireless router

First we need to create a VLAN object

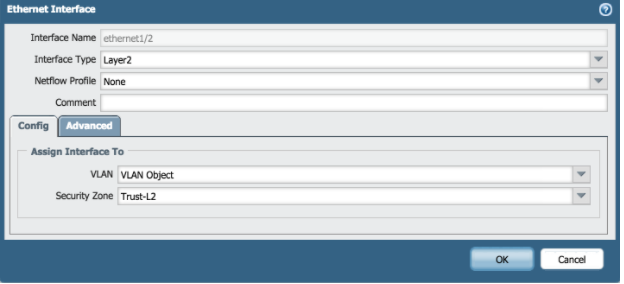
1. Go to network, VLAN`s and click add
2. Enter a name and select “vlan” for the VLAN interface



Now to configure the Layer2 ports and the VLAN object

1. Go to network, Interfaces, ethernet
2. Edit the following settings for the ethernet ½, ethernet 1/3, ethernet ¼ etc.
3. All of these interfaces ethernet ½ -> ethernet 1/8 need

* Interface type; layer 2
* Netflow profile; None
* VLAN; VLAN object
* Security Zone; Trust-L2



\*Repeat for all interfaces 2-8

To configure the VLAN interface, we must go to Network-> Interfaces-> VLAN and edit the following settings

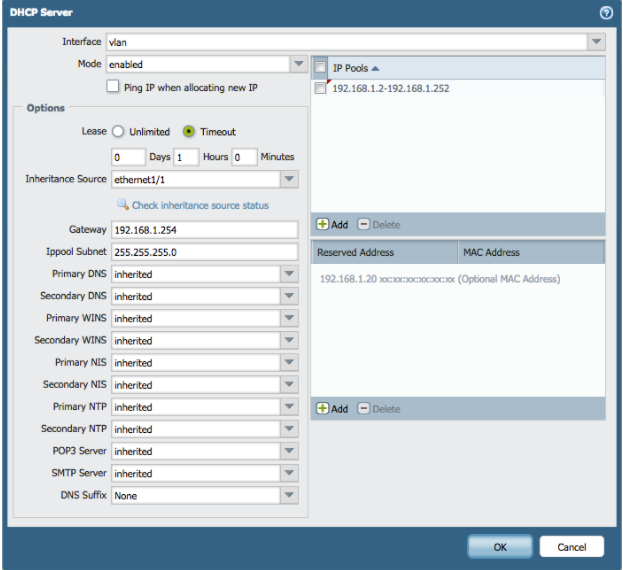
* VLAN; VLAN Object
* Virtual Router; default
* Security Zone; Trust-L3

Then under the IPv4 tab

Add a IPv4 address with the address 192.168.1.254 with a subnet mask of 255.255.255.0

Configure the DHCP server

1. Go to Network > DHCP > DHCP Server
2. Click Add
3. Edit the DHCP server settings as shown



Configure the DHCP server with these settings and add DNS servers

Any public DNS server such as google works for this, but Open DNS is the most reliable DNS server

The Open DNS primary server IP`s

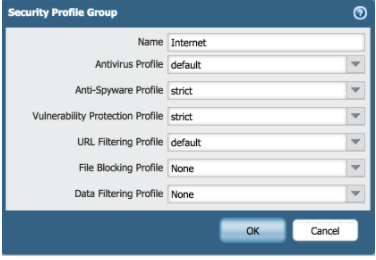
*208.67. 222.222*

And the secondary DNS server is

*208.67. 220.220*

Now we need to set up a Security Profile Group

1. Go to objects > Security profile groups and click add.
2. Edit the following Security Profile Group settings as desired



These are the default settings, but you should customize them to your liking according to your SOHO environment

Now we must configure the outbound internet security policy,

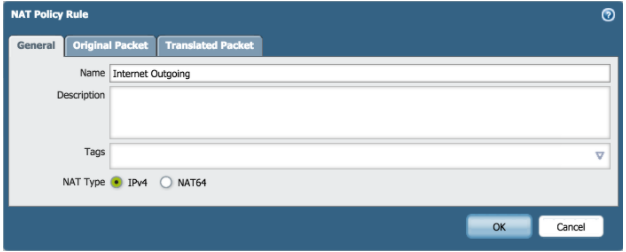
1. Go to policies > Security and Click Add
2. Enter Name and Description

Name, Internet Outgoing, Description, All traffic to internet

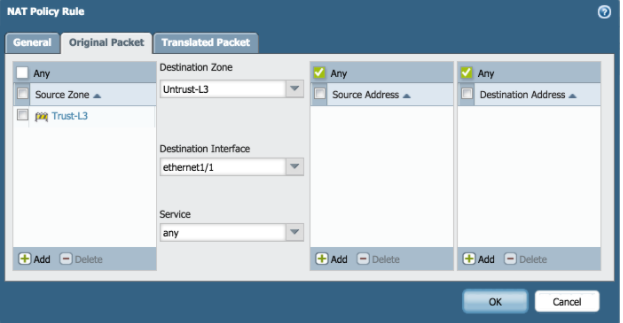
1. Add the Source Zone, Trust- L3 under the tab Source
2. Add the Destination Zone, Untrust L3 under the tab Destination
3. Specify the action Setting as allow under the Actions Tab

Configure Outbound Internet NAT Policy

1. Go to Policies >NAT and click Add
2. Enter a Name and check IPV4 for NAT type



On Original Packet, specify the Source, Destination zone and Destination interface

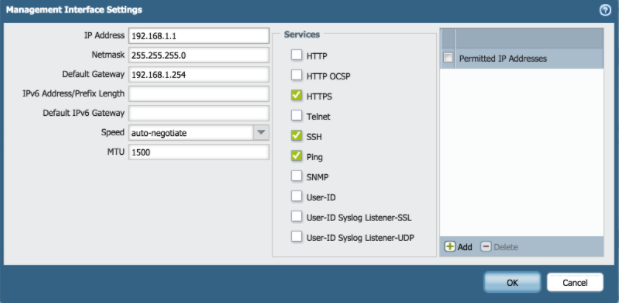


On Translated Packet, set:

* Translation Type: Dynamic IP And Port
* Address Type: Interface Address
* Interface: ethernet1/1

Configure the Management IP

Go to device > setup > Management and specify the following management Interface Settings



Under Services, Enter the DNS server IP`s. Mine was OpenDNS therefore my primary DNS Server was

208.67.222.222

And my secondary DNS server was

208.67.222.222

Commit the Changes and enjoy your SOHO configuration

COMMANDS

    ip-address 192.168.1.1;

    netmask 255.255.255.0;

    update-server updates.paloaltonetworks.com;

    update-schedule {

      threats {

        recurring {

          weekly {

            day-of-week wednesday;

            at 01:02;

            action download-only;

    timezone US/Pacific;

    service {

      disable-telnet yes;

      disable-http yes;

    hostname PA-220;

    type {

      static;

    default-gateway 192.168.1.254;

    dns-setting {

      servers {

        primary 208.67.222.222;

        secondary 208.67.220.220;

            neighbor-discovery {

              router-advertisement {

                enable no;

          ndp-proxy {

            enabled no;

          lldp {

            enable no;

          dhcp-client;

      ethernet1/2 {

        layer2 {

          lldp {

            enable no;

      ethernet1/3 {

        layer2 {

          lldp {

            enable no;

      ethernet1/4 {

        layer2 {

          lldp {

            enable no;

      ethernet1/5 {

        layer2 {

          lldp {

            enable no;

    loopback {

      units;

    vlan {

      ipv6 {

        neighbor-discovery {

          router-advertisement {

            enable no;

      ndp-proxy {

        enabled no;

      adjust-tcp-mss {

        enable no;

      ip {

        192.168.1.254/24;

    tunnel {

      units;

        vlan {

    "Vlan Object" {

      virtual-interface {

        interface vlan;

            interface [ ethernet1/2 ethernet1/3 ethernet1/4 ethernet1/5];

        virtual-wire;

  profiles {

    monitor-profile {

      default {

        interval 3;

        threshold 5;

        action wait-recover;

          ike {

    crypto-profiles {

      ike-crypto-profiles {

        default {

          encryption [ aes-128-cbc 3des];

          hash sha1;

          dh-group group2;

          lifetime {

            hours 8;

        Suite-B-GCM-128 {

          encryption aes-128-cbc;

          hash sha256;

          dh-group group19;

          lifetime {

            hours 8;

                          Suite-B-GCM-256 {

          encryption aes-256-cbc;

          hash sha384;

          dh-group group20;

          lifetime {

            hours 8;

      ipsec-crypto-profiles {

        default {

          esp {

            encryption [ aes-128-cbc 3des];

            authentication sha1;

          dh-group group2;

          lifetime {

            hours 1;

        Suite-B-GCM-128 {

          esp {

            encryption aes-128-gcm;

            authentication none;

          dh-group group19;

          lifetime {

            hours 1;

        Suite-B-GCM-256 {

          esp {

            encryption aes-256-gcm;

            authentication none;

          dh-group group20;

          lifetime {

            hours 1;

      global-protect-app-crypto-profiles {

        default {

          encryption aes-128-cbc;

          authentication sha1;

  qos {

    profile {

      default {

        class-bandwidth-type {

          mbps {

            class {

              class1 {

                priority real-time;

              class2 {

                priority high;

              class3 {

                priority high;

              class4 {

                priority medium;

              class5 {

                priority medium;

              class6 {

                priority low;

              class7 {

                priority low;

              class8 {

                priority low;

  virtual-router {

    default {

      protocol {

        bgp {

          enable no;

          dampening-profile {

            default {

              cutoff 1.25;

              reuse 0.5;

              max-hold-time 900;

              decay-half-life-reachable 300;

              decay-half-life-unreachable 900;

              enable yes;

      interface [ ethernet1/1 vlan];

  dhcp {

    interface {

      vlan {

        server {

          option {

            dns {

              primary inherited;

              secondary inherited;

            wins {

              primary inherited;

              secondary inherited;

            nis {

              primary inherited;

              secondary inherited;

            ntp {

              primary inherited;

              secondary inherited;

            lease {

              timeout 60;

            pop3-server inherited;

            smtp-server inherited;

            gateway 192.168.1.254;

            subnet-mask 255.255.255.0;

            inheritance {

              source ethernet1/1;

          mode enabled;

          ip-pool 192.168.1.2-192.168.1.252;

shared {

  application;

  application-group;

  service;

  service-group;

  botnet {

    configuration {

      http {

        dynamic-dns {

          enabled yes;

          threshold 5;

        malware-sites {

          enabled yes;

          threshold 5;

        recent-domains {

          enabled yes;

          threshold 5;

        ip-domains {

          enabled yes;

          threshold 10;

        executables-from-unknown-sites {

          enabled yes;

          threshold 5;

      other-applications {

        irc yes;

      unknown-applications {

        unknown-tcp {

          destinations-per-hour 10;

          sessions-per-hour 10;

          session-length {

            maximum-bytes 100;

            minimum-bytes 50;

        unknown-udp {

          destinations-per-hour 10;

          sessions-per-hour 10;

          session-length {

            maximum-bytes 100;

            minimum-bytes 50;

    report {

      topn 100;

      scheduled yes;

zone {

  trust {

    network {

      layer3;

  untrust {

    network {

      layer3;

  Untrust-L3 {

    network {

      layer3 ethernet1/1;

  Trust-L3 {

    network {

      layer3 vlan;

  Trust-L2 {

    network {

      layer2 [ ethernet1/2 ethernet1/3 ethernet1/4 ethernet1/5];

service-group;

service;

schedule;

rulebase {

  security {

    rules {

      rule1 {

        from trust;

        to untrust;

        source any;

        destination any;

        service any;

        application any;

        action allow;

        log-end yes;

      "Internet Outgoing" {

        profile-setting {

          group Internet;

        to Untrust-L3;

        from Trust-L3;

        source any;

        destination any;

        source-user any;

        category any;

        application any;

        service application-default;

        hip-profiles any;

        action allow;

        description "All traffic to the internet";

  nat {

    rules {

      "Internet Outgoing" {

        source-translation {

          dynamic-ip-and-port {

            interface-address {

              interface ethernet1/1;

        to Untrust-L3;

        from Trust-L3;

        source any;

        destination any;

        service any;

        to-interface ethernet1/1;

profile-group {

  Internet {

    virus default;

    spyware default;

    vulnerability default;

    url-filtering default;

import {

  network {

    interface [ ethernet1/1 ethernet1/2 ethernet1/3 ethernet1/4 ethernet1/5 vlan];

application-group;

application;

mgt-config {

  users {

    admin {

      phash $1$ckoofbbn$PWKcUVCtFbpJ0k1FSzTEi0;

      permissions {

        role-based {

          superuser yes;

**Problems:** I made a few mistakes in entering commands or creating zones. When I tried to commit changes, I was unable to and had to backtrack to resolve these issues. Outside of these problems committing the changes the lab was straightforward.

**Conclusion,** the web interface is very easy to manage and quite intuitive. There are a lot of settings that are difficult to navigate through but once you find them it is straight forward. The SOHO configuration was relatively easy to setup.