# Overview

Introduced first in PAN-OS 8.0, the ***Dynamic IP Address and Tag Registration*** feature makes a significant step forward in the automation of operational, administrative, and, most importantly, security processes on Palo Alto Networks devices. This may become an important aspect to consider when facing the challenges of scaling, such as in dynamic provisioning of servers and clients in cloud environments, or in third-party platform integrations through XML API.

Among a few tools available in PAN-OS which enable dynamic IP and tag registration, one of particular interest is *Auto-Tagging* with logs. Because Auto-Tagging is a function of the operating system and not of hardware or VM hypervisor, firewall engineers and network security designers will hardly experience any limitation when deploying this feature, architecturally or otherwise. One limitation to keep in mind, however, is the storage capacity of each firewall model.

# Objective

Auto-Tagging refers to the system's ability to register and un-register IP addresses and tags dynamically. Firewall administrators can configure the firewall to execute automatic addition of address objects to address groups, once certain events have occurred. If the firewall generates a threat log for example, the firewall will tag the source or the destination IP address in the log, and then add that same IP address to a predefined address group. Correspondingly, the firewall can automatically remove tags on the source or destination IP addresses from the logs. Since address group objects can be applied to security rules, this means that the firewall will be taking action on traffic coming from tagged IP addresses without an external input, or a need to commit.

In order to explore this functionality further, we are going to consider a common real-world scenario. We will assume an infected host on the trust side of the network and then learn how to configure the firewall to quarantine the compromised host dynamically. This method is particularly effective in zero-trust security models, where East-West, internal- and micro-segmentation designs have been properly architected and deployed. Not only will the infected host be blocked from communicating out to the Internet, it will also be cut off from lateral communication as well.

One of the most concerning network security risks involves an employee's machine getting infected with a zero-day malware. While the infection can occur in several different ways, in our case we will presume that the user has downloaded a file which is later determined to be a zero-day exploit. We will also presume that the network environment is properly secured with a Palo Alto Networks firewall. The zero-day exploit will not trigger signature defense while traversing the firewall southbound (while being downloaded), because the file is about to be observed in 'the Wild' for the first time, and so there is no existing signature for it yet. The firewall will forward the payload to the WildFire, which will then examine the file, reach a malicious verdict, generate a log on the firewall, and eventually inform the firewall administrator about the incident. A timely response to the threat in this situation is critically important. Auto-Tagging can significantly expedite the incident response time, and that is the core concept we will be exploring in this exercise.

# The Information You Need and Prerequisites

- ✓ PAN Firewall with current and up-to-date licensing, running PAN-OS 8.0 or later, and preconfigured in VWire, L2, or L3 mode to pass traffic in production.
- ✓ Web browser and access to the Internet.

# Lab Configuration Steps

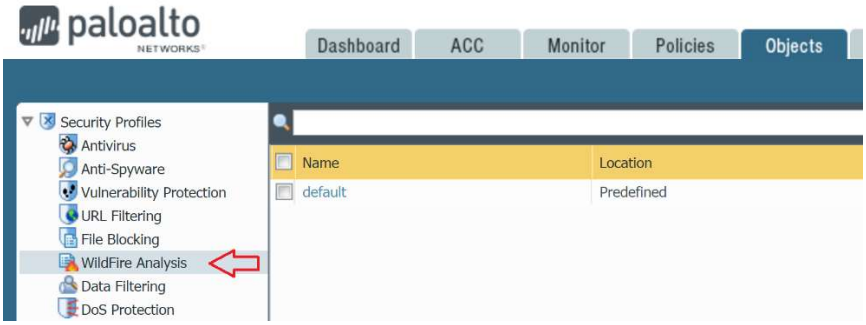
## 1. Configure WildFire Security Profile

### a. Purpose

WildFire security profile is responsible for forwarding previously unseen files to the WildFire engine for inspection. When user attempts to download a file from the Internet, the firewall will compute the file's hash, compare it against the database, and upload it to WildFire if the file is unknown. WildFire profile must be attached to appropriate security rules for this action to happen.

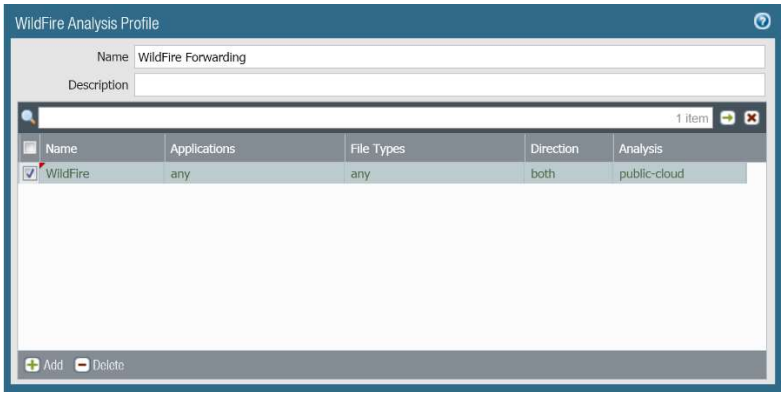
### b. Location

WildFire profile is configured in the Objects tab under Security Profiles in the menu on the left.




### c. Building WildFire Profiles

i. Click on ***Objects*** > ***WildFire Analysis***, then on ***Add*** button at the bottom
ii. Type “WildFire Forwarding” in the ***Name*** field, then on ***Add*** button again to create a profile policy. Name the policy " WildFire" and leave all other fields unchanged.
iii. Before you click on OK button, make sure that the profile you just created looks like in the screenshot below, then click on ***OK*** button to close the window:




## 2. Configure Log Forwarding Profile

### a. Purpose

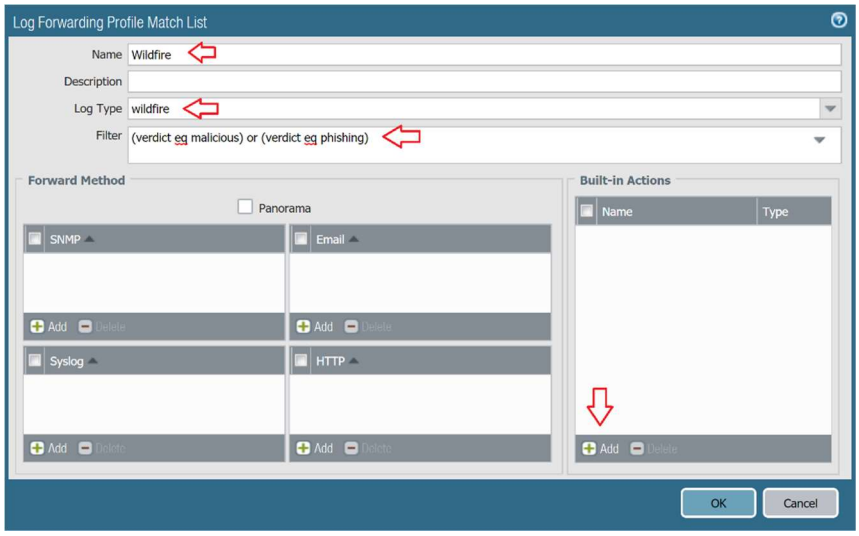
Log Forwarding profile is the key element in the Auto-Tagging implementation. This is where we define the ***dynamic tagging action*** the firewall executes upon detecting a malicious activity. Log forwarding profile has to be applied to appropriate security rules for this action to happen.

### b. Location

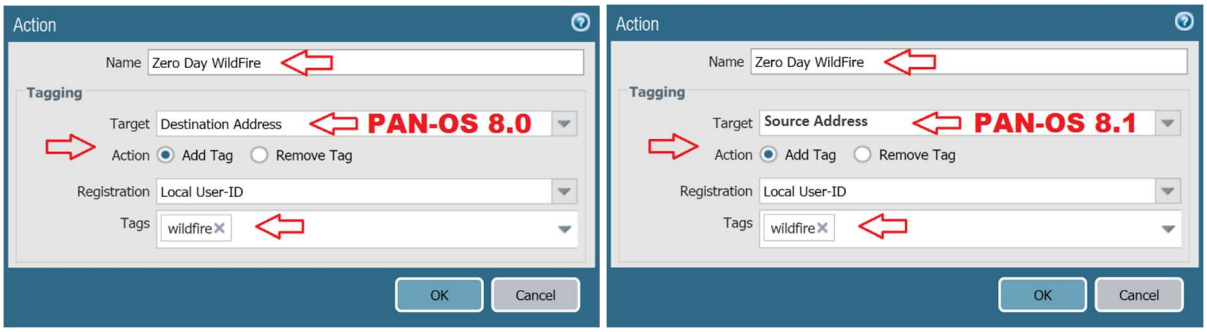
Log Forwarding profile is configured in the Objects tab under Log Forwarding in the menu on the left.

### c. Building Log Forwarding Profiles

i. Click on ***Objects > Log Forwarding***, then click on ***Add*** button at the bottom
ii. Type “Auto-Tag” in the ***Name*** field, then click on ***Add*** button again toward the bottom to create a profile policy. Name the policy "WildFire" and change the ***Log Type*** to WildFire. Under ***Filter*** type '(verdict eq malicious) or (verdict eq phishing)'
iii. Under ***Built-In Actions*** click on ***Add***.



iv. Type " Zero Day WildFire" under the ***Name*** field. Under ***Target***, specify "Destination ***or*** Source Address" (depending on whether you work in 8.0 or 8.1 code). Make sure the ***Action*** field defines "Add Tag" action. Under ***Tags***, type "wildfire". Remember that this filed is case sensitive.




v. Click on ***OK*** three times to close all open dialog boxes.

*Note:* PAN firewall acts as a stateful inspection device, and for that reason we only need an outbound security rule. The client on the internal network will initiate a session with the server on the Internet, and then download a zero-day exploit. The firewall sees the client as the session initiator (source). From the security perspective, however, the client will be the receiver of zero-day binaries, and the firewall will associate the client's IP address with the ***destination IP*** (victim) in the WildFire logs. This is why in PAN-OS 8.0 we need to define ***Target*** *as 'Destination Address*' in the **2-C-iv** step above. Beginning PAN-OS 8.1 WilDFire logging has changed in a way that is similar to traffic logs. The client on the inside will be identified as the ***source***, and the server will be labeled as ***destination***. This affects our log forwarding profile, forcing us to switch the ***Target*** *to 'Source Address*' in the step **2-C-iv**. Below screenshots were taken on two production firewalls running 8.0 & 8.1 to demonstrate the difference. In either case our end goal is tagging the client's IP address.


## 3. Create Outbound Security Rule

### a. Purpose

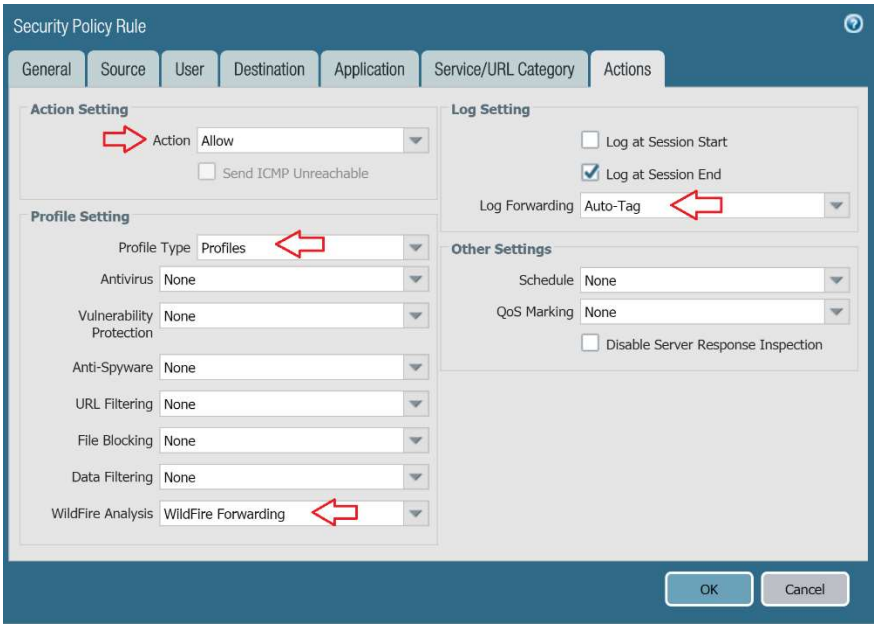
WildFire and Log Forwarding profiles created in prior steps must be assigned to security rules. On firewalls which are already deployed in production, the two profiles would be attached to existing rules. For the purpose of this exercise, we are going to generate a single outbound security policy to allow any traffic originating on the trust side of the network.

### b. Location

Security rules are defined under ***Policies > Security***.

### c. Building Outbound Security Rule

i. Click on ***Policies > Security***, then click on ***Add*** button at the bottom.
ii. Type “Allow All Outbound Traffic” in the ***Name*** field, then switch to the ***Source*** tab.
iii. Under ***Source Zone*** click on ***Add*** and select 'inside' zone (note that the naming convention may differ on your firewall). Leave ***Source Address*** field empty.
iv. Switch to ***Destination*** tab > ***Destination Zone***. select 'outside' zone (note that the naming convention may differ on your firewall). Leave ***Destination Address*** field empty.
v. Switch to ***Actions*** tab and confirm that the ***Action*** field is set to 'Allow'. Under ***Profile Setting*** select 'Profiles' for ***Profile Type***. In the dialog box that opens, select 'WildFire Forwarding' profile which we created earlier. Under ***Log Forwarding*** select previously created profile 'Auto-Tag'.




vi. Click ***OK*** and validate that the security rule looks like in the screenshot:

| | Name | Source Zone | Source Address | Source User | Destination Zone | Destination Address | Application | Service | Action | Profile | Options |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Allow All Outbound Traffic | inside | any | any | outside | any | any | any | Allow | | |
| 2 | intrazone-default | any | any | any | (intrazone) | any | any | any | Allow | none | none |
| 3 | interzone-default | any | any | any | any | any | any | any | Deny | none | |

## 4. Create Dynamic Address Group

### a. Purpose

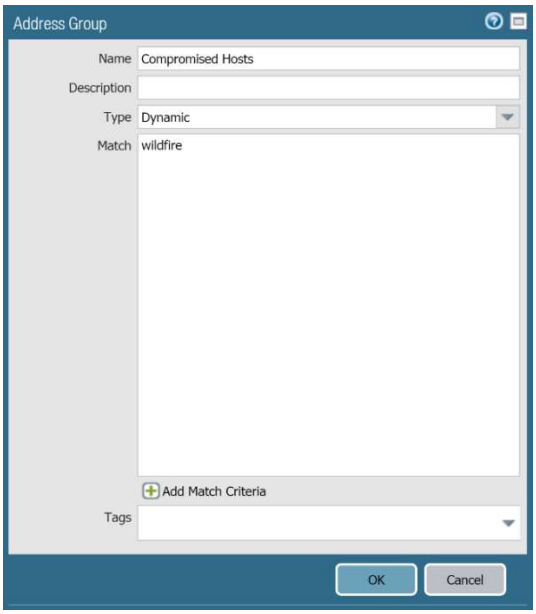
The 'Allow All Outbound Traffic' security rule created in the previous step will be responsible for tagging internal hosts who initiated the downloads of zero-day binaries. We also need to define another security rule which will be responsible for quarantining those hosts. Before we do that, we are going to create a ***dynamic address group*** where all tagged IP addresses will be stored. We will then attach this dynamic address group to the blocking security rule in the ***Source Address*** field.

### b. Location

Address Groups are defined under ***Objects > Address Groups***.

### c. Building Dynamic Address Group

i. Click on ***Objects > Address Groups***, then click on ***Add*** at the bottom.
ii. Type “Compromised Hosts” in the ***Name*** field, then change ***Type*** to 'dynamic'.
iii. Under ***Match*** type 'wildfire' (this value must be the exact match of the ***Tags*** filter we defined in the step **2-C-iv** above).
iv. Validate that the values look like in the screenshot below, then click on ***OK*** button.



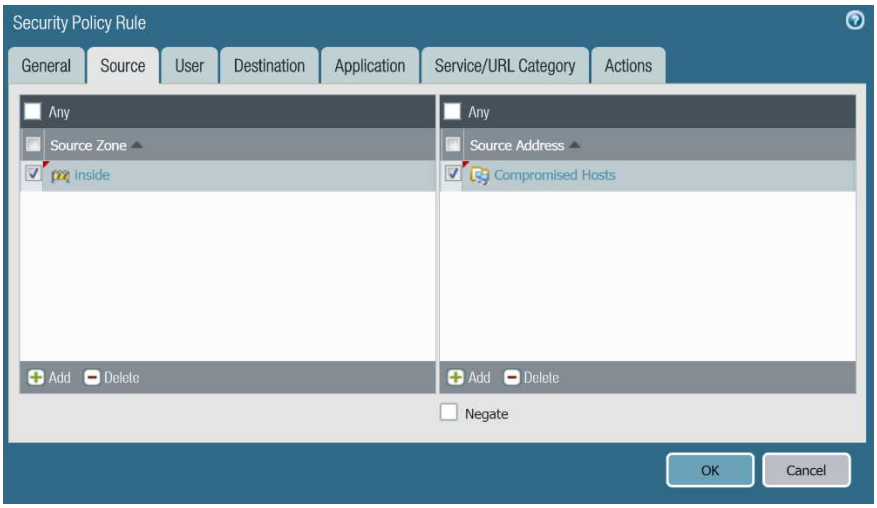
## 5. Create Blocking Security Rule

### a. Purpose

This rule will be responsible for isolating compromised hosts from the rest of the network based on the content of the dynamic address group defined in the previous step. This rule has to be placed above the 'Allow All Outbound Traffic' security rule.

### b. Building Blocking Security Rule

i. Click on ***Policies > Security***, then click on ***Add*** button at the bottom.
ii. Type “Block Compromised Hosts” in the ***Name*** field, then switch to the ***Source*** tab.
iii. Under ***Source Zone*** select 'inside' (note that the naming convention may differ on your firewall). Select 'Compromised Hosts' address group under ***Source Address*** field.




iv. Switch to ***Destination*** tab and select ***any*** destination zone from the menu
v. Under ***Service/URL Category*** change 'application-default' to 'Any'.
vi. Switch to ***Actions*** tab. Change ***Action*** to 'Deny', then click on OK.
vii. Move “Block Compromised Hosts” rule to the top and confirm that security policy looks like as shown on the screenshot:

| | | Source | | | Destination | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Name | Zone | Address | User | Zone | Address | Application | Service | Action | Profile | Options |
| 1 | Block Compromised Hosts | inside | Compromised Hosts | any | any | any | any | any | Deny | none | |
| 2 | Allow All Outbound Traffic | inside | any | any | outside | any | any | any | Allow | | |
| 3 | intrazone-default | any | any | any | (intrazone) | any | any | any | Allow | none | none |
| 4 | interzone-default | any | any | any | any | any | any | any | Deny | none | |

viii. Commit the configuration.

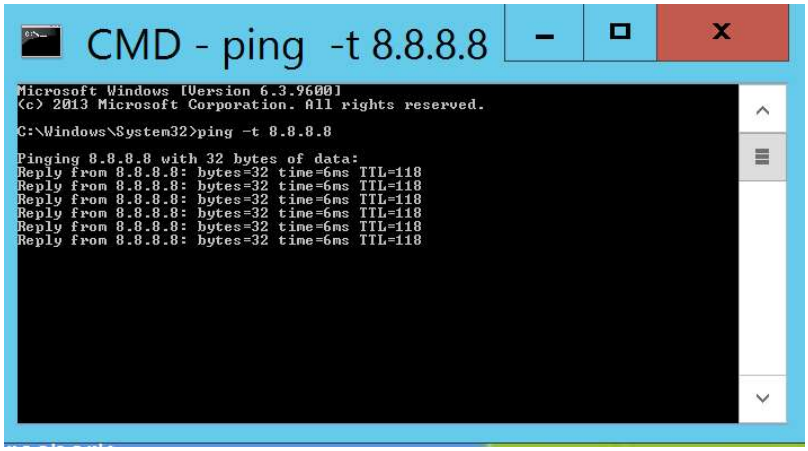
# 6. Test Blocking Security Rule

## a. Purpose

To test whether internal host isolation works as designed, we need to simulate a download of a zero-day vulnerability. Once we obtain the WildFire sample malware file from http://wildfire.paloaltonetworks.com/publicapi/test/apk, the firewall will upload the file to the cloud for analysis, and then generate a WildFire submission log a few minutes later. As soon as the log gets generated on the firewall, the client's IP will be added to the "Compromised Hosts" dynamic address group. At that point all traffic coming from the client will get dropped, based on the "Block Compromised Hosts" security rule.

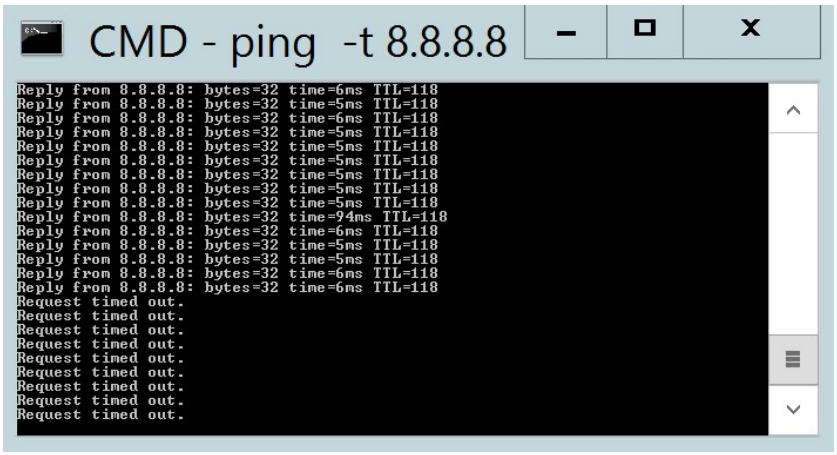
## b. Run Continuous Ping

i. From the client's desktop start a continuous ping sessions to 8.8.8.8, or some other IP address on the Internet.

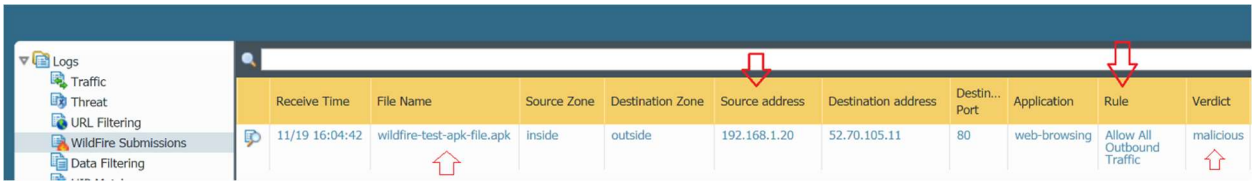


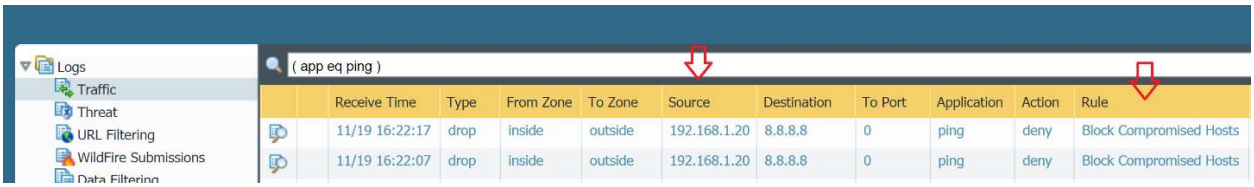

## c. Download Sample Malware File

i. Open a web browser and navigate to http://wildfire.paloaltonetworks.com/publicapi/test/apk
ii. The download will start automatically. Do not open the file. WildFire analysis will take several minutes to complete.
iii. Observe the ongoing ping session. In a few minutes the firewall will start dropping packets.

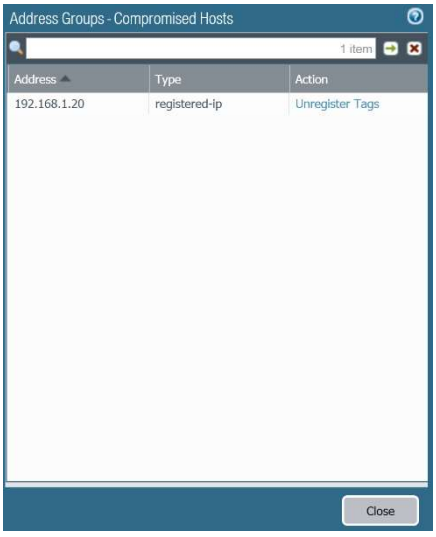



iv. Observe ***WildFire Submissions*** and ***Traffic*** logs. Notice the client's IP in the ***source address*** field, and security rules responsible for tagging and blocking the traffic.



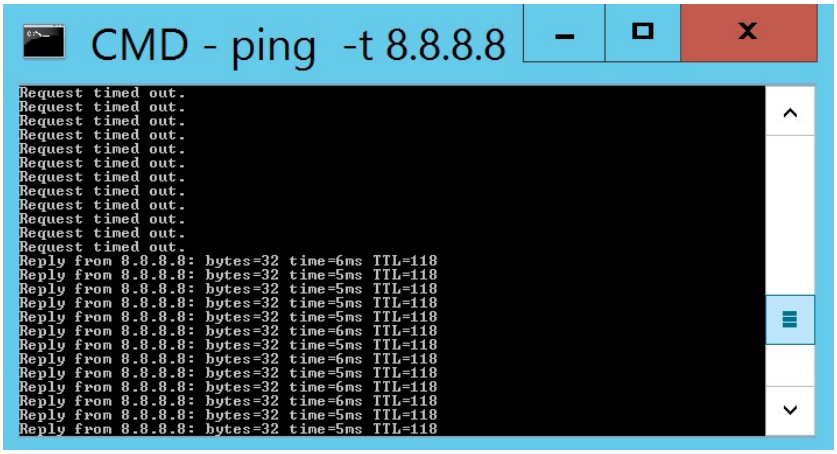




v. Click on ***Objects*** > ***Address Groups***, then locate 'more...' on the right hand side and click on it. Notice that the group membership includes the client's private IP address.



vi. Click on ***Unregister Tags***. A new window opens. Click on ***Add***. In ***Tags*** drop menu select 'wildfire'.


vii. Click ***OK*** three times to close all open dialog boxes.
viii. After a few seconds the ping session resumes.



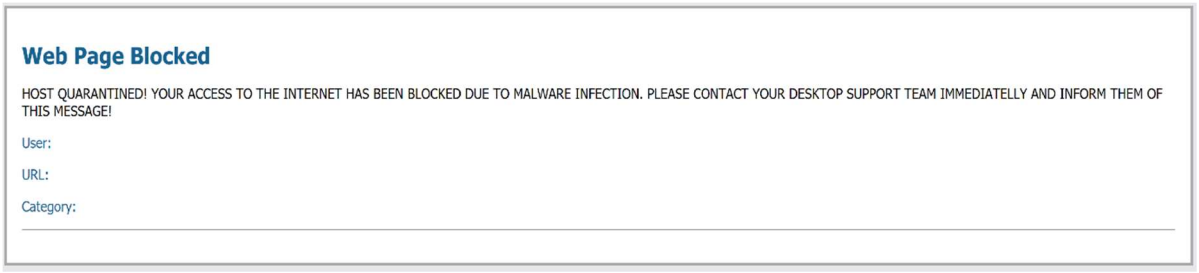

## 7. Notify Affected users

### a. Purpose

Although optional, this step makes a good deployment practice. Users will be notified when their systems have been put in isolation, prompting them to reach out to the IT Support team for assistance. When a user (whose IP address has been tagged by the firewall) opens a web browser to get access to the internet, he/she will receive a response page notifying them about the incident.

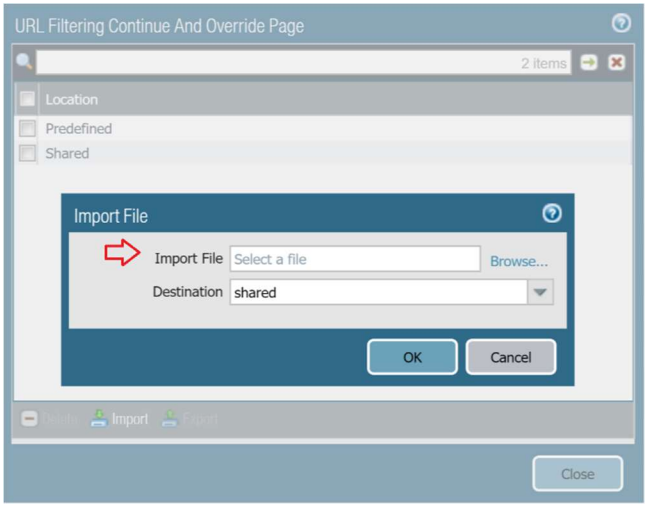
### b. Create a Response Page

Firewall administrator needs to generate a response page to be presented to the users, and upload it onto the firewall. The firewall accepts html and txt file formats. A sample message is shown on the screenshot below:



### c. Upload Custom Response Page to Firewall

Click on ***Device > Response Pages***. Locate 'URL Filtering Continue and Override Page' and click on it. Select 'Import' and upload the custom response page created in the previous step.

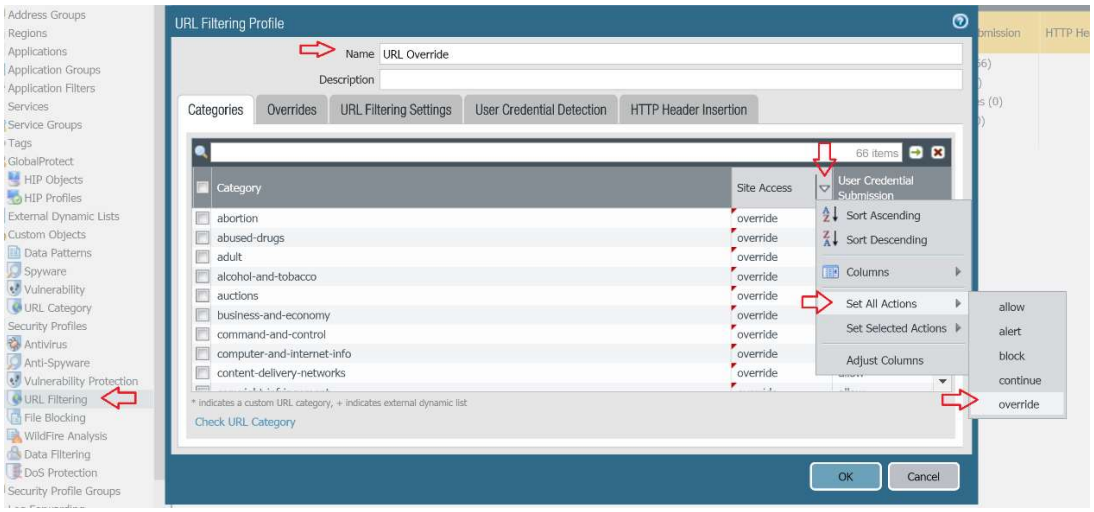



Click OK twice to close both open dialog boxes.

### d. Creating Override URL Filtering Profile

We need a third security rule, an URL filtering profile, and another log forwarding profile. The URL filtering profile will be responsible for triggering the custom response page generated in the previous step.

i. Click on ***Objects > Security Profiles > URL Filtering***, then click on ***Add*** button at the bottom. In the ***Name*** field type ' URL Override', then under ***Site Access > Set All Actions*** select 'Override'.

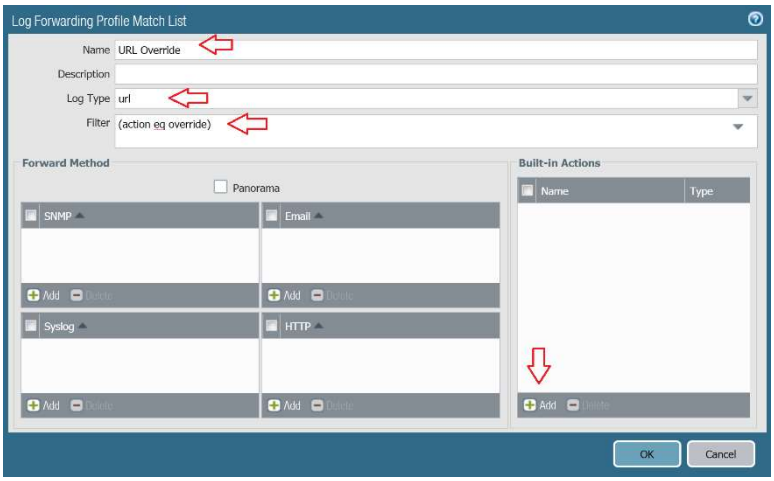



ii. Click on ***OK*** to close the dialog box.

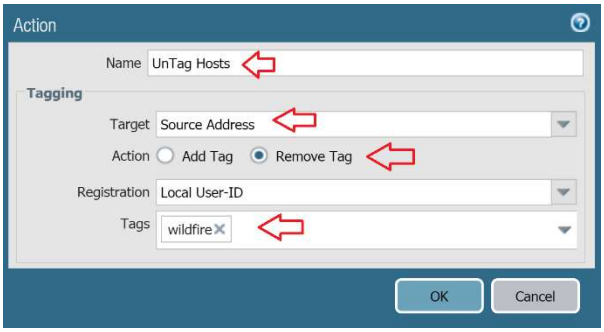
### e. Building Log Forwarding Profile

The log forwarding profile will be responsible for untagging internal hosts and restoring their network access. Both profiles (URL and log forwarding) will be attached to the security rule which we are going to generate in the next step.

i. Click on ***Objects > Log Forwarding***, then click on ***Add*** button at the bottom
ii. Type “UnTag Hosts” in the ***Name*** field, then click on ***Add*** button again toward the bottom to create a profile policy. Name the policy "URL Override" and change the ***Log Type*** to URL. Under ***Filter*** type '(action eq override)'
iii. Under ***Built-In Actions*** click on ***Add***.




iv. Type "UnTag Hosts" under the ***Name*** field. Under ***Target***, specify "Source Address". Make sure the ***Action*** field defines "Remove Tag" action. Under ***Tags***, type 'wildfire' (this value must be the exact match of the ***Tags*** filter we defined in the step **2-C-iv**).

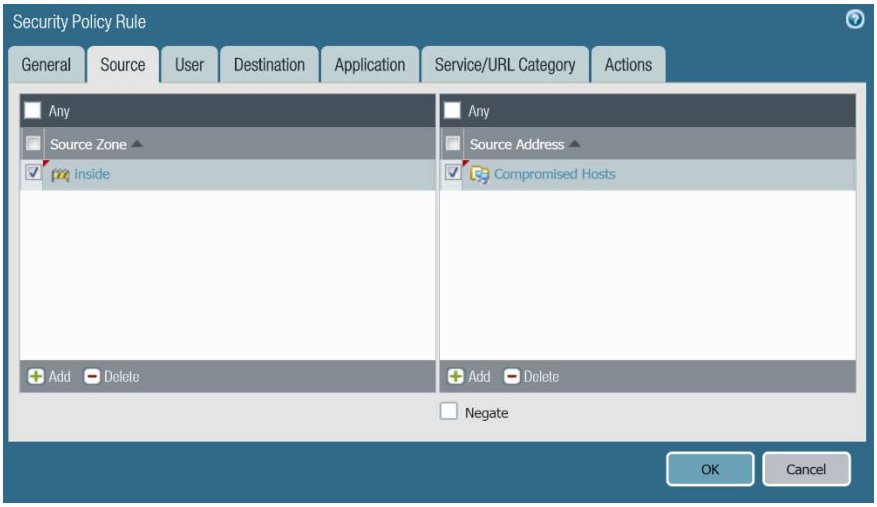



v. Click on ***OK*** three times to close all open dialog boxes.

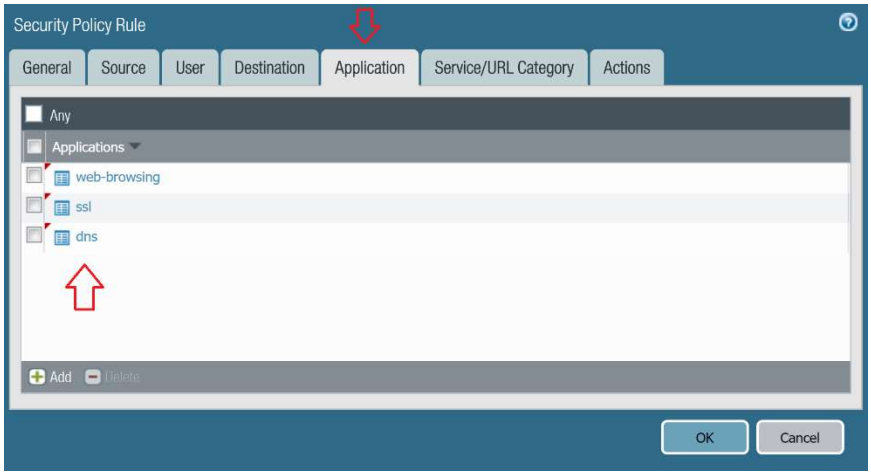
**f. Create Unblocking Security Rule**

The URL Filtering and Log Forwarding profiles defined in the previous two steps need to be attached to a new security rule. This rule will serve a dual purpose: a) inform the user that his/her computer has been quarantined, and b) allow firewall administrators to unblock the compromised IP address once the machine has been cleaned from infection. To do so, the firewall administrators will have to use a unique password known only to them.

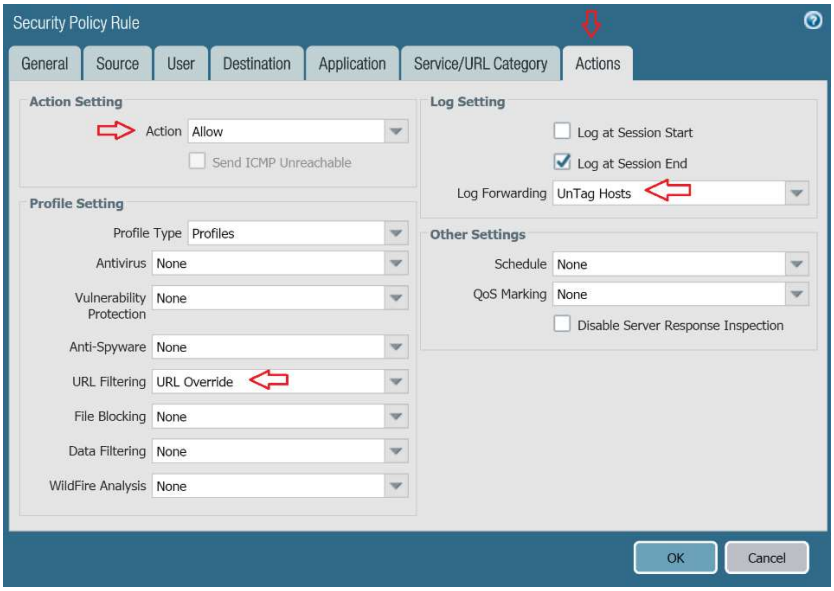
i. Click on ***Policies > Security***, then click on ***Add*** button at the bottom.
ii. Type “Block Override” in the ***Name*** field, then switch to the ***Source*** tab.
iii. Under ***Source Zone*** select 'inside' (note that the naming convention may differ on your firewall). Specify 'Compromised Hosts' address group under ***Source Address*** field. Set ***Destination*** zone to ***any***.




iv. Under ***Application*** tab select three signatures, 'web-browsing', 'ssl' and 'dns'.



v. Switch to ***Actions*** tab. make sure the ***Action*** field says 'Allow'.
vi. Under ***Profile Settings > Profile Type*** select 'Profiles'.
vii. Under ***URL Filtering*** select 'URL Override' profile which we created in the step ***7-d***.
viii. Under ***Log Settings > Log Forwarding*** select 'UnTag Hosts' profile which we created in the step ***7-e***. Click OK to close dialog box.



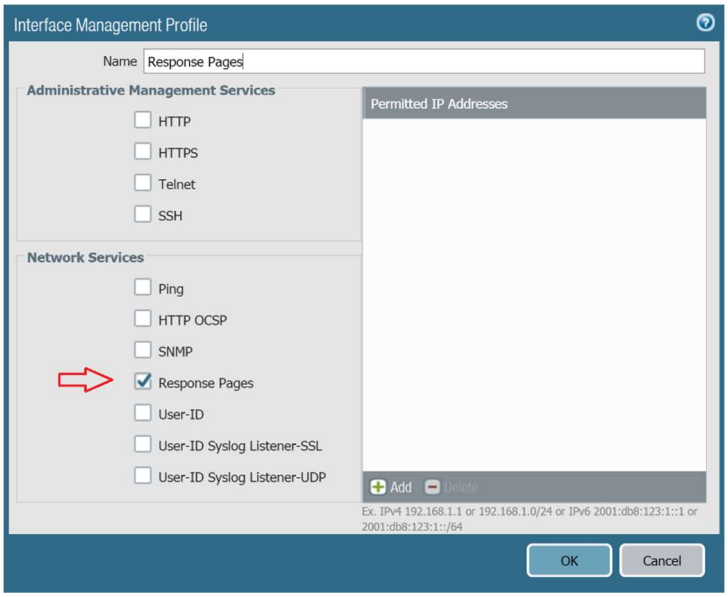

ix. Move the newly created “Block Override” rule to the top and confirm that security policy looks like as shown on the screenshot:

| | | Source | | | Destination | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Name | Zone | Address | User | Zone | Address | Application | Service | Action | Profile | Options |
| 1 | Block Override | inside | Compromised Hosts | any | any | any | dns<br>ssl<br>web-browsing | application-default | Allow | | |
| 2 | Block Compromised Hosts | inside | Compromised Hosts | any | any | any | any | any | Deny | none | |
| 3 | Allow All Outbound Traffic | inside | any | any | outside | any | any | any | Allow | | |
| 4 | intrazone-default | any | any | any | (intrazone) | any | any | any | Allow | none | none |
| 5 | interzone-default | any | any | any | any | any | any | any | Deny | none | |

**g. Create Interface Management Profile**

As mentioned earlier, the firewall will intercept http requests from quarantined clients and present them with the response page which was generated and uploaded onto the firewall in steps ***7-b*** & ***7-c***. To enable this intercepting action, we need to create an Interface Management Profile with ***Response Pages*** action set to 'enable', and attach it to an interface on the firewall. In most cases this will be the client-facing L3 firewall interface.

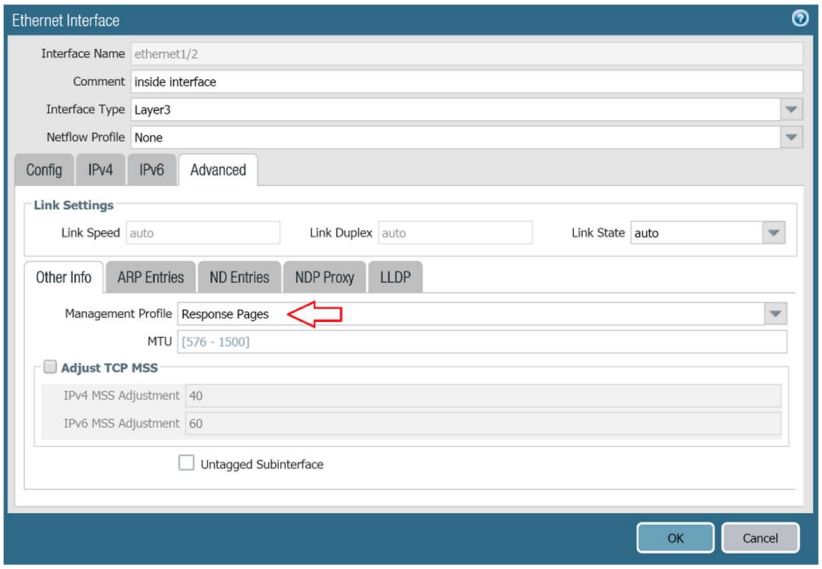
i. Click on ***Network > Interface Mgmt***, and click on ***Add*** to create a new profile.
ii. Name the profile 'Response Pages', and make sure that ***Response pages*** option is selected. Click OK to close the dialog box.




**h. Attach Interface Management Profile to an Interface**

We will use the firewall's interface assigned to the 'inside' security zone to attach the profile created in the previous step to (note that the nomenclature may differ on your firewall).

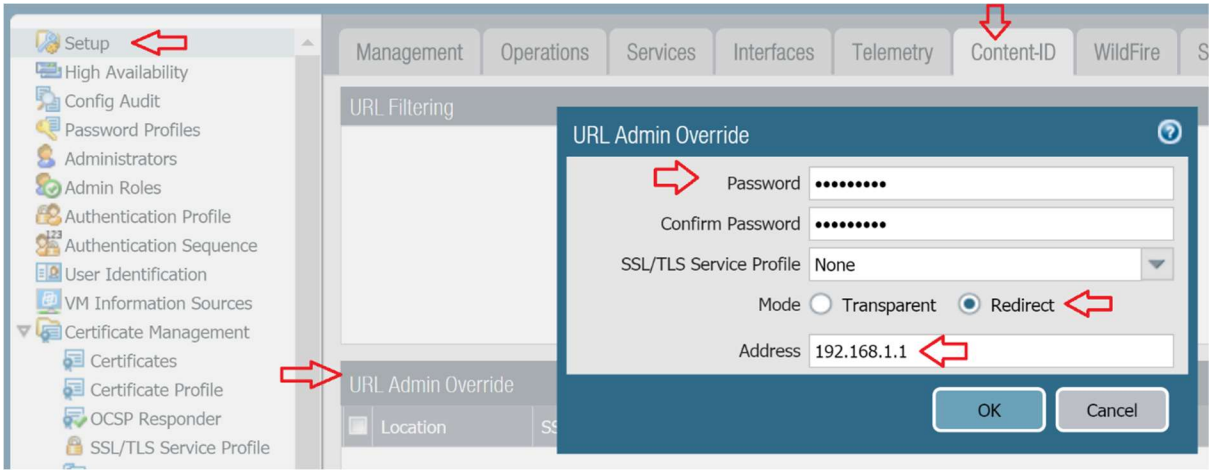
i. Click on ***Network > Interfaces***, and click on ***ethernet1/2***.
ii. Under ***Advanced > Management Profile*** select 'Response Pages'. Click on ***OK*** to close the interface dialog box.



### i. Create Password Override

Our final step involves defining an override password for the firewall administrators' use. When quarantined clients attempt to browse the web and are presented with the response page instructing them to reach out to the support team for assistance, the only way their network access can be restored is to supply the override password. The firewall administrator will type this password in once the infected machine has been reimaged.

i. Click on ***Device > Setup > Content-ID > URL Admin Override***, and click on ***Add*** button on the bottom.
ii. Type 'Password!' in the ***Password*** field, and switch ***Mode*** to 'Redirect'.
iii. In the Address field put the IP of the ethernet1/2 interface which was edited in the ***7-h-2*** step above (note that the nomenclature may differ on your firewall). In our case the ethernet1/2 interface IP address is 192.168.1.1. Click ***OK*** to close the dialog box.

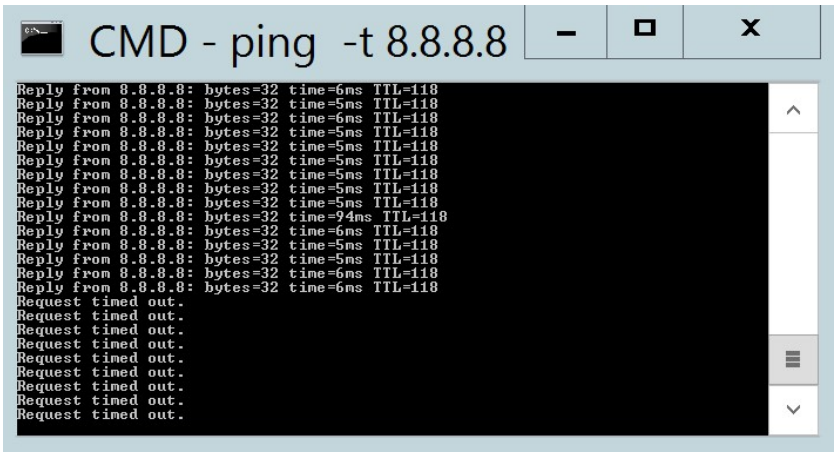



iv. Commit the configuration.

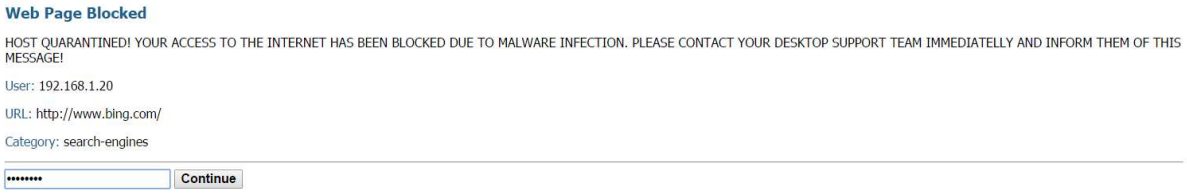
## 8. Test Configuration

### a. Download Sample Malware File

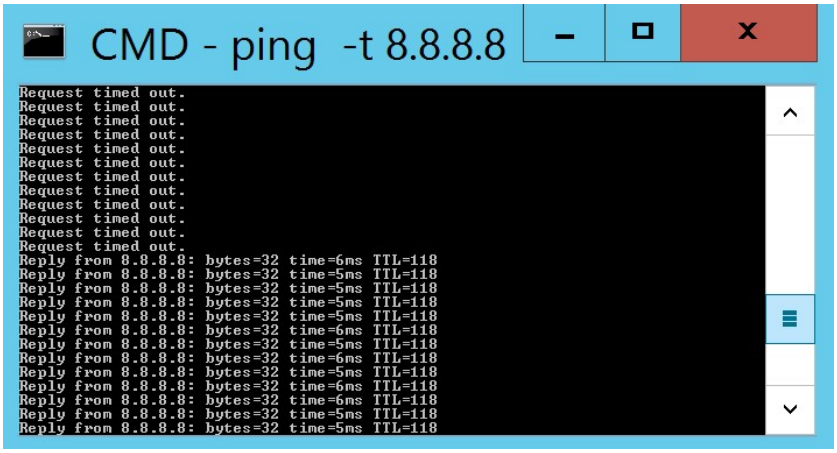
i. With the continuous ping session to 8.8.8.8 still running, open a web browser and navigate to the same page as before to download another instance of a sample malware binary: http://wildfire.paloaltonetworks.com/publicapi/test/apk
ii. The download will start automatically. Do not open the file. WildFire analysis will take several minutes to complete.
iii. Observe the ongoing ping session. In a few minutes the firewall will start dropping packets.




iv. Wait until ping sessions time out, then open another web browser instance and navigate to a web site, such as www.bing.com. Ignore the certificate warning (this is expected behavior since the firewall is redirecting traffic to the eth1/2 interface). The firewall then presents the response page to the user:




v. Type in Password!, as defined in the step ***7-i-ii*** and click on ***Continue***.
vi. The browser then redirects the user to www.bing.com, and the continuous ping session resumes.



## Next Steps

If you want to test this on your own and do not have access to a lab environment to do so, you have a couple options:

**a.** Contact your Sun Management Account Rep to get pricing on a lab bundle. The newly released PA-220 and VM-50 appliances are excellent platforms for testing things such as this and there are specific part numbers for lab equipment that are more heavily discounted than the same appliance for use in production.

If you are unsure who your Account Rep is or do not have one yet, you can reach out to **sales@sunmanagement.net** for assistance.

**b.** Reach out through the free Fuel Users Group (www.fuelusersgroup.org) which at the time this lab is being written is offering limited free access to a virtual lab environment, which they refer to as their "Virtual Test Lab," in which you can practice the steps outlined above. (Note: The Fuel Users Group may alter or discontinue offering their "Virtual Test Lab" at any time)

**c.** For access to live Palo Alto Networks boxes for lab practice purposes please go to: **https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab**. This is a no charge service provided by Palo Alto Networks.

*If you feel Sun Management brings value to you and your organization with these labs, please keep us in mind for other network and network security related requirements. We are here to help you. Thank you for your business.*

*Please direct any questions/comments/feedback on this lab exercise to:*
***education@sunmanagement.net***

*Lab Author:* *Bob Pesakovic*
*Palo Alto Networks Instructor & Sr. Network Security Engineer, PCNSE, PCNSI*

*Last Modified:* *December 28, 2018*