Zero Phishing

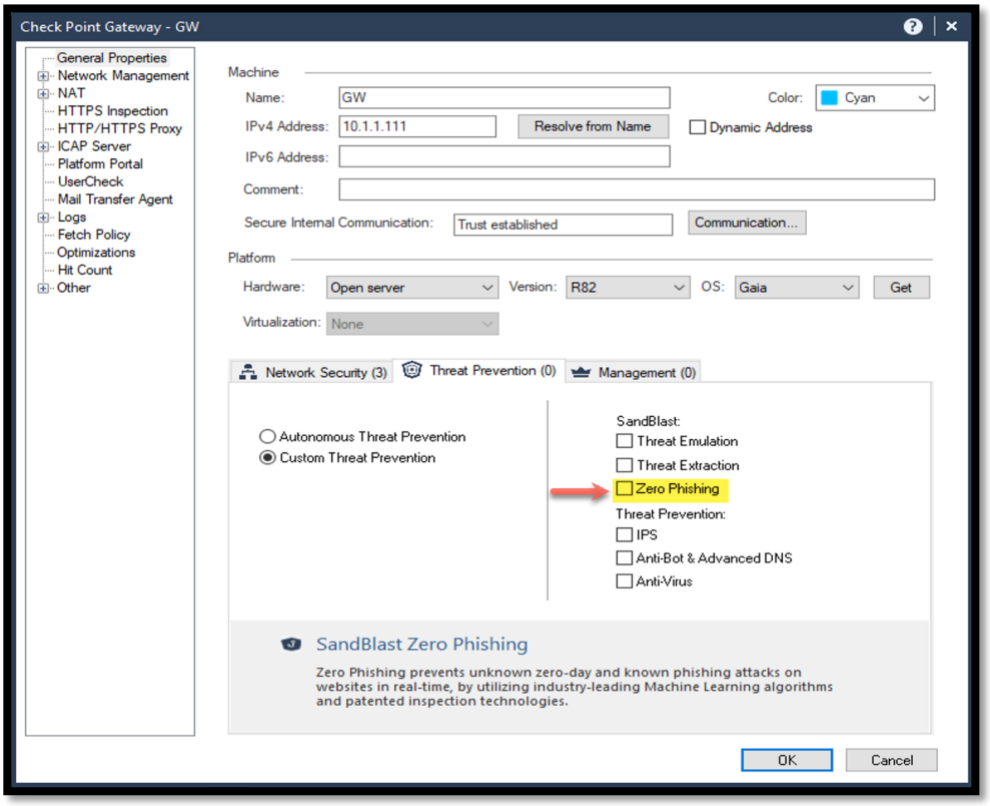
Introduction

The Check Point Zero Phishing prevents unknown zero-day and known phishing attacks on websites in real-time, by utilizing industry leading Machine-Learning algorithms and patented inspection technologies.

Exercise 1: Onboarding

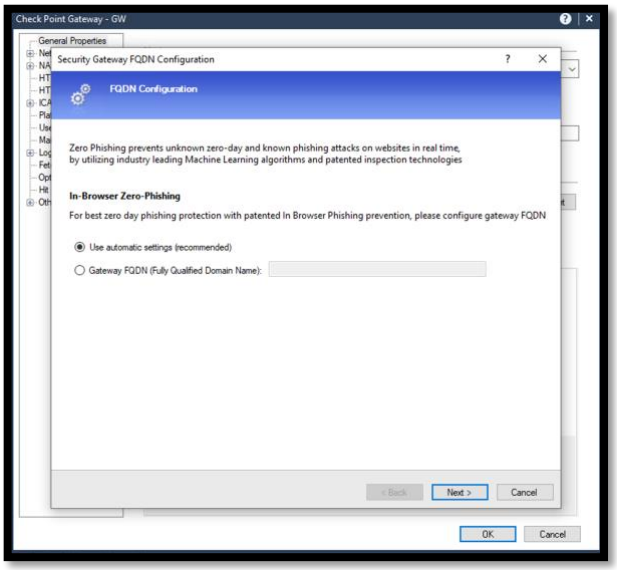
In this exercise, we will enable the Zero Phishing blade and test its capabilities.

1. Edit the **GW** object, and under Threat Prevention, Enable the Zero Phishing blade.

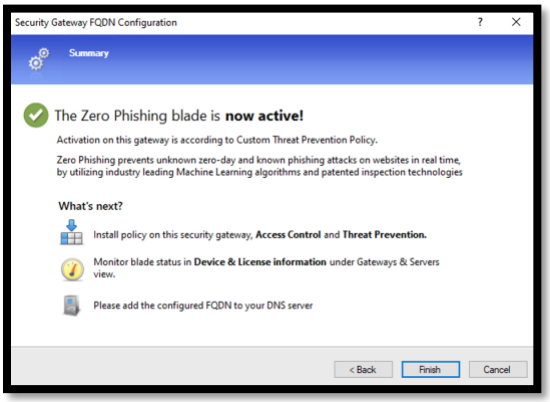


- You can disable other Threat Prevention blades as the functionality of Zero Phishing does not require any other blade activated.
- The procedure to activate the blade depends on whether HTTPS Inspection is enabled. In this lab, we have HTTPS Inspection from previous labs.

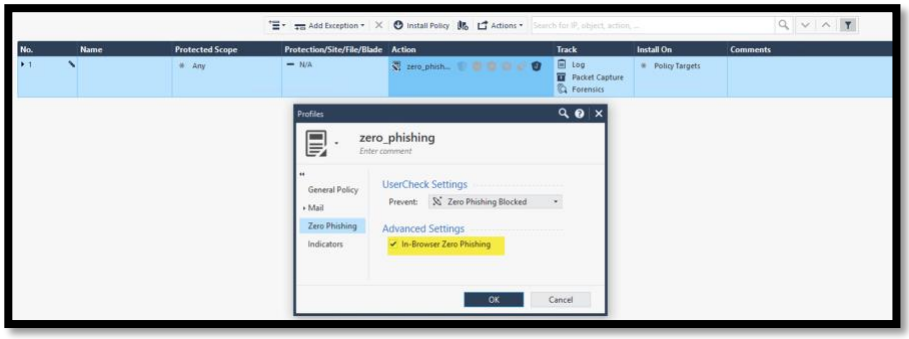
2. Leave the default recommended selection for In-Browser Zero-Phishing. This step was simplified in R82.



3. The Zero Phishing blade is now active. Save the changes



4. Under the Threat Prevention Policy, use a profile that has Zero Phishing activated. Confirm that In-Browser Zero Phishing is activated.

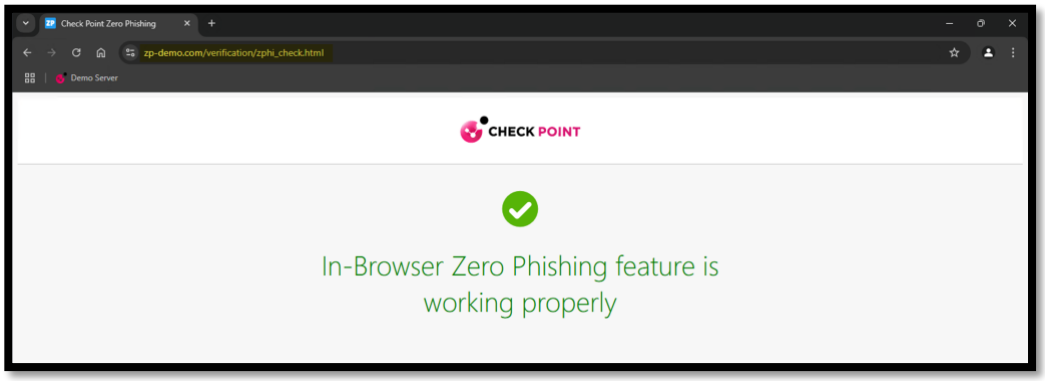


5. Install the Access Control and Threat Prevention Policy.

Exercise 2: Zero Phishing Engines

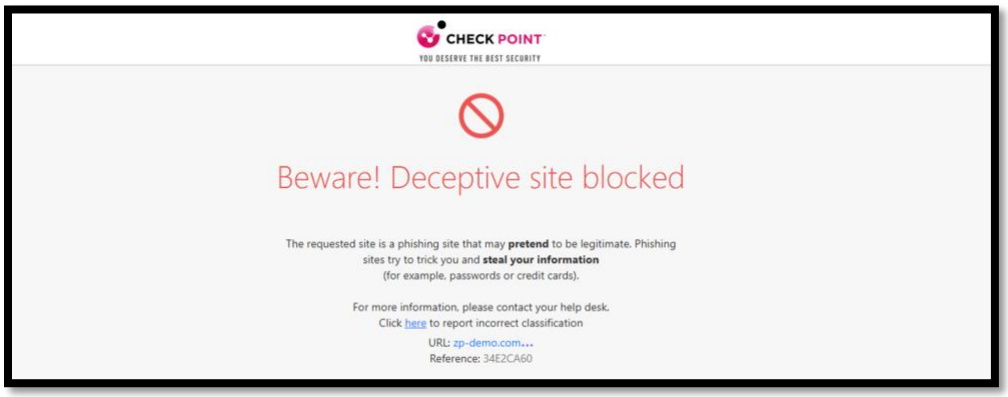
In this exercise, we will enable demonstrate how Zero Phishing engines can block phishing attacks. It is possible to block accessing phishing sites, and the blade is also capable of actively scan web sites field and prevent phishing attack.

1. To confirm that the Zero phishing works properly, login to win_client and use a web browser to reach the test site https://zp-demo.com/verification/zphi_check.html



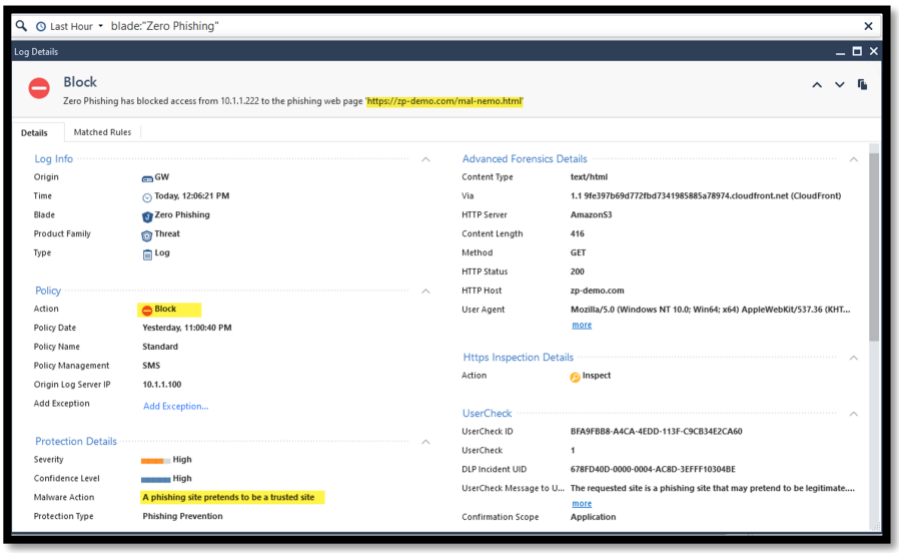
   - In the first test, we will review how the Zero Phishing blade can prevent accessing known phishing sites. The classification is done by the Threat Cloud

2. Try reaching the test URL https://zp-demo.com/mal_nemo.html. Notice that a block message was returned to the user instead of loading the phishing site.

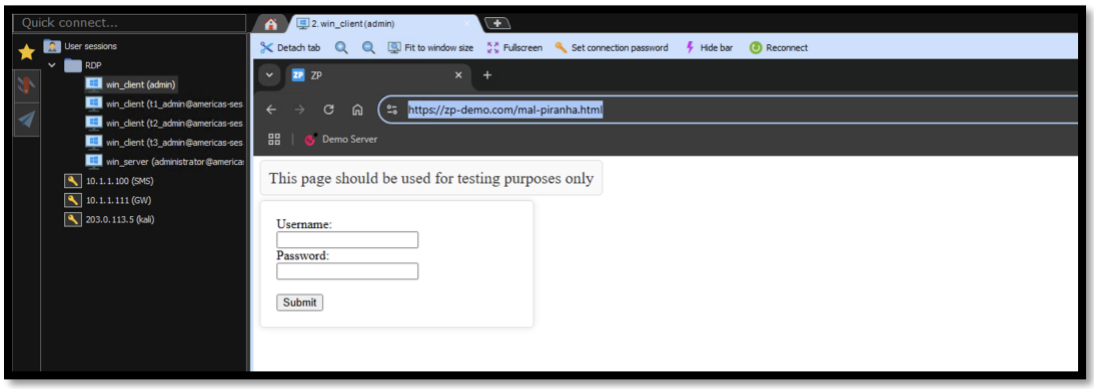


3. Check the related logs in SmartConsole. Use the filter below to see the Zero Phishing logs:

   Blade: “Zero Phishing”

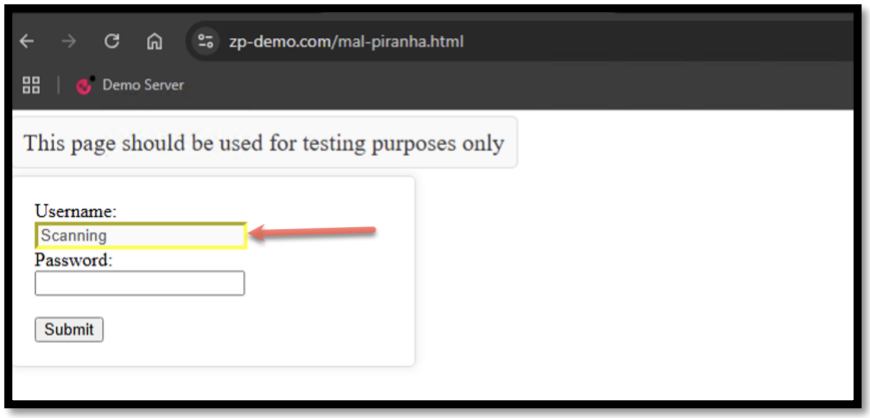


4. Back from win_client, try reaching the site https://zp-demo.com/mal-piranha.html

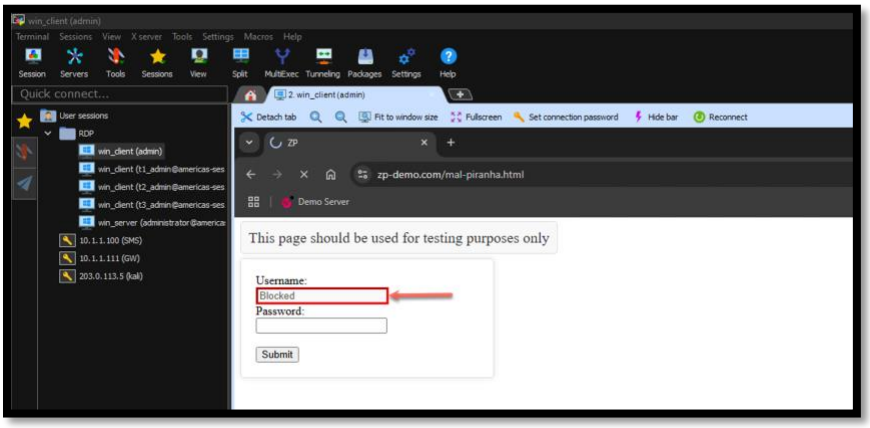


- Notice that the site is accessible. This is only indication that the site itself was not categorized as a phishing site.

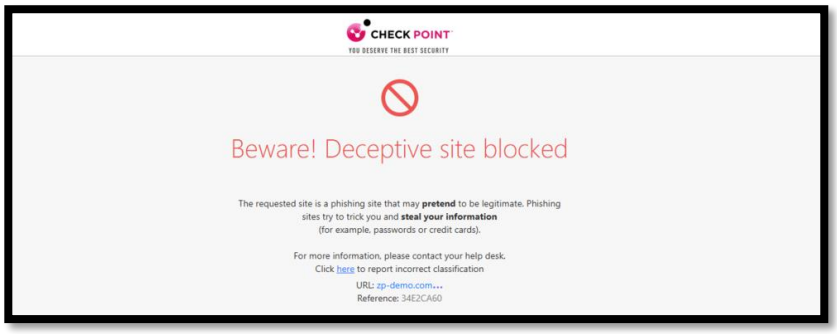
5. Click inside the **Username** field, notice that it is being scanned.



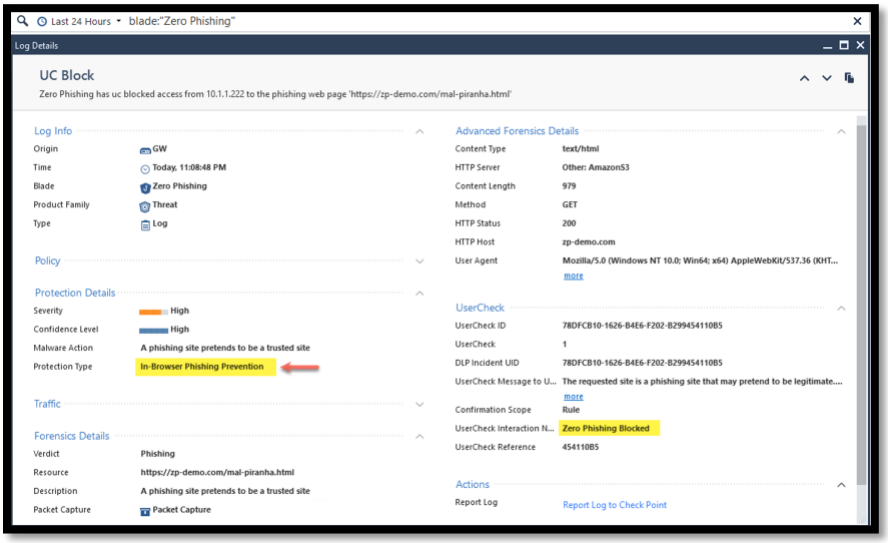
6. The Zero Phishing engine returned a verdict indicating a phishing behavior. You can see a block message in the field.



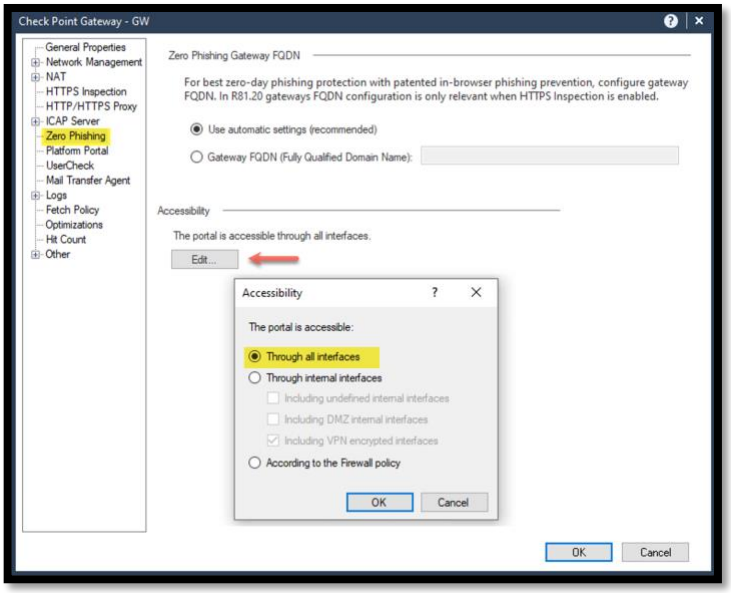
7. The user will be directed to the User Check block message.



8. Review the logs from SmartConsole and notice that the action was decided by the In-Browser protection.



- Notice that the two steps above are happening quick and might be hard to notice sometimes.
- The scan can be done in the browser without any extension.
- This is done by a script that is injected into the web page.
- It is essential to make sure the UserCheck is configured and is accessible correctly.
- The blade configuration on the GW object also has accessibility settings. Confirm this is configured correctly.



End of Lab 11

