

## Anti-Bot and DNS Security

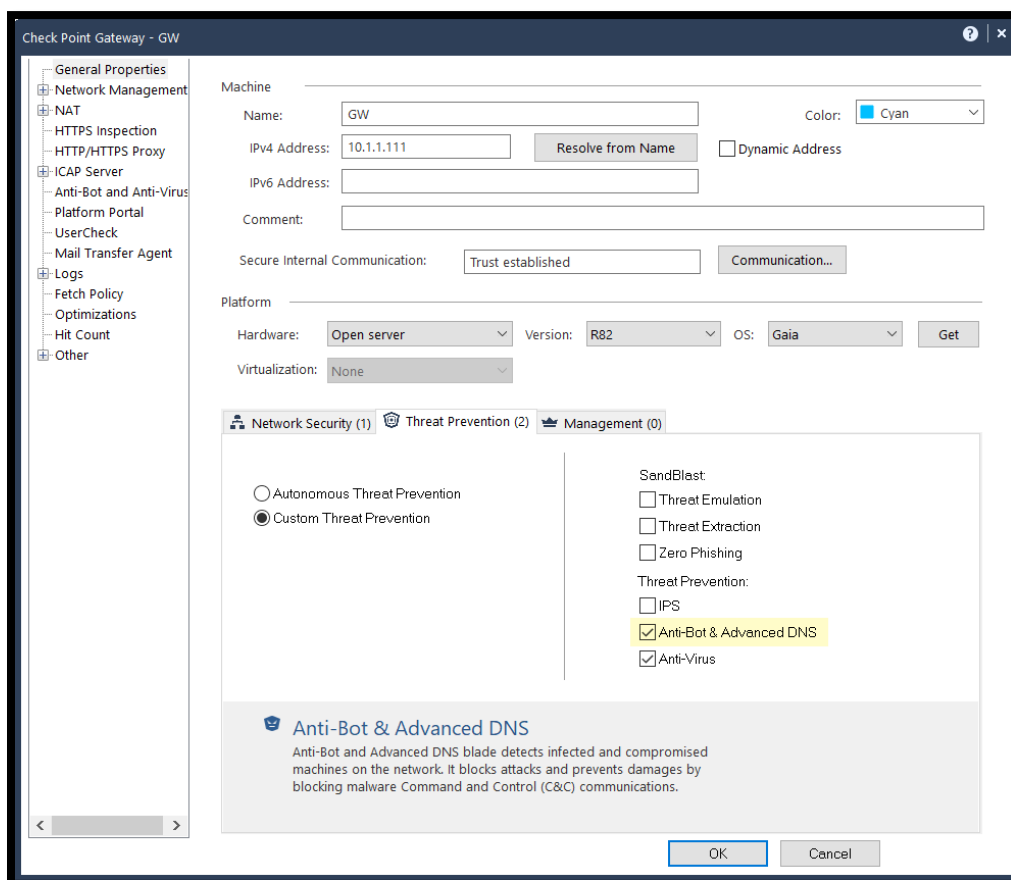
### Introduction

Anti-Bot detects and prevents bot activity while you are in the organizational network or outside of it. A bot is malicious software that neutralizes Anti-Virus defenses, connects to a Command-and-Control center for instructions from cyber criminals, and carries out the instructions.

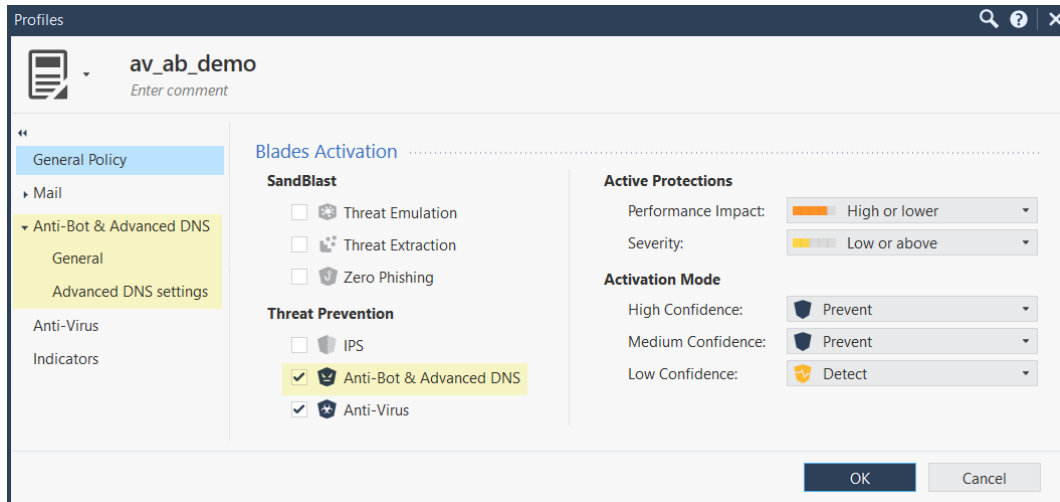
### Exercise 1: Onboarding

In this exercise, we will enable and test the protections provided by the Anti-Bot blade.

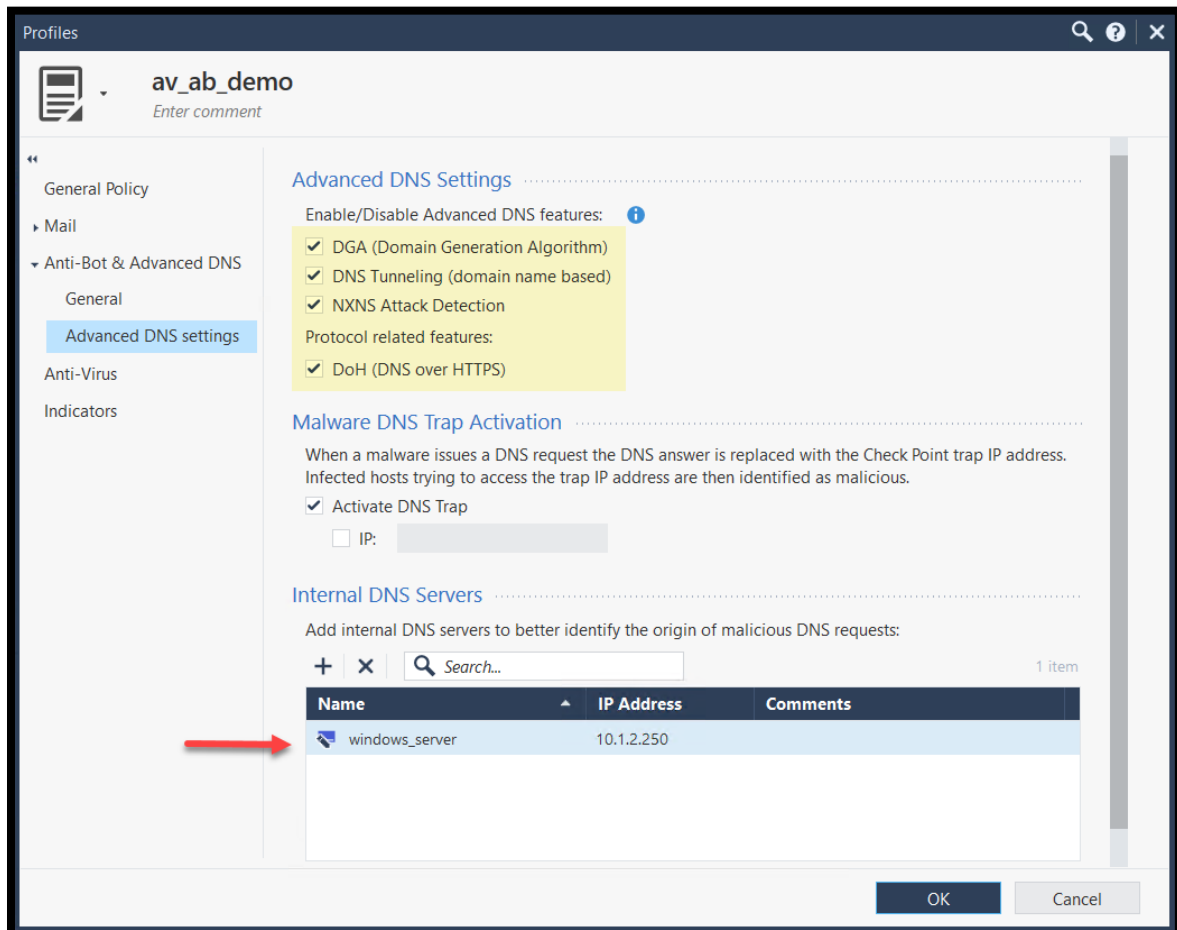
1. Edit the GW object and enable the **Anti-Bot & Advanced DNS** blade. Save the changes.



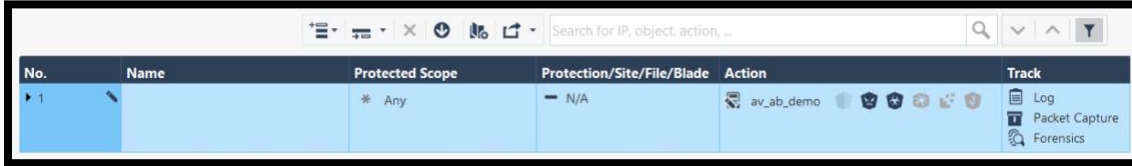
2. Edit the custom profile and enabled the Anti-Bot & Advanced DNS.



3. Review the default settings under Advanced DNS settings tab. Add the internal DNS Server object **win\_server** to the list of internal DNS servers and save the changes.



- Confirm the correct profile is assigned to the Threat Prevention default rule and install the Access and Threat Prevention Policies.

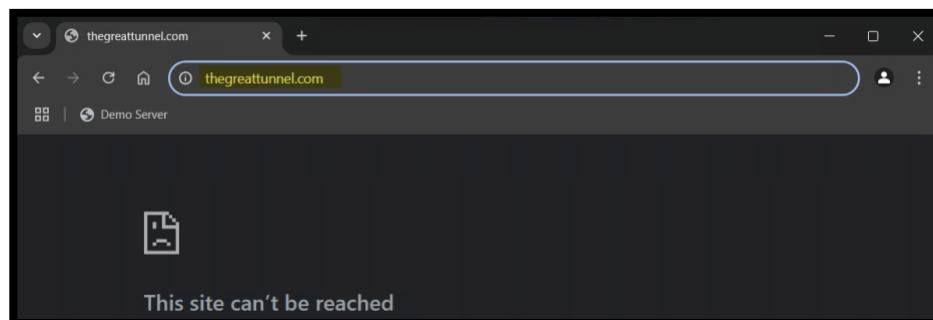


No.	Name	Protected Scope	Protection/Site/File/Blade	Action	Track
1		* Any	N/A	av_ab_demo	Log Packet Capture Forensics

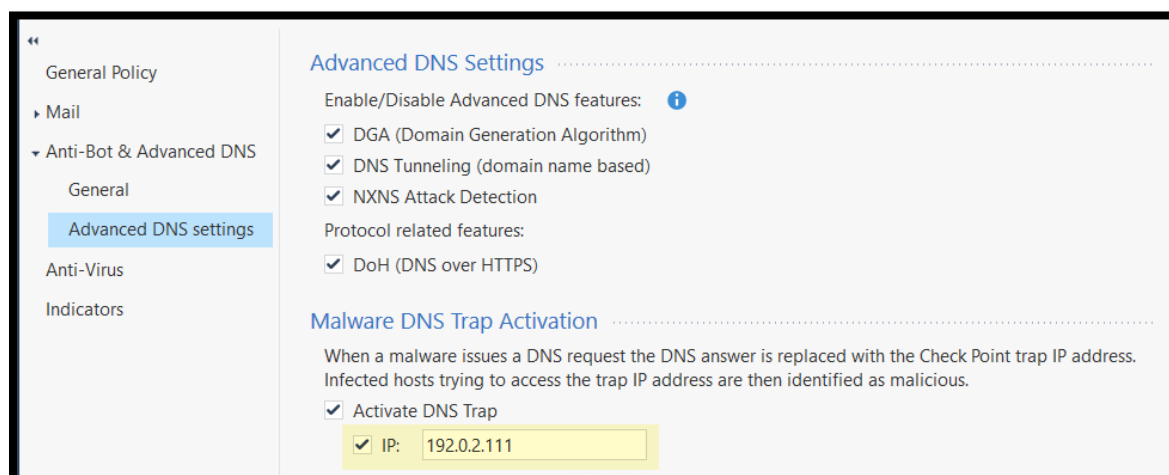
## Exercise 2: DNS Security

In this exercise, we will test the DNS protections, enabled by default on the profile.

- From the windows client host, browse to <http://thegreattunnel.com>. This site is used to test DNS Tunneling protections.



- The malware DNS trap feature replaces the DNS address of the malicious site with a bogus address. Customize the profile and assign a random local address such as 192.0.2.111.

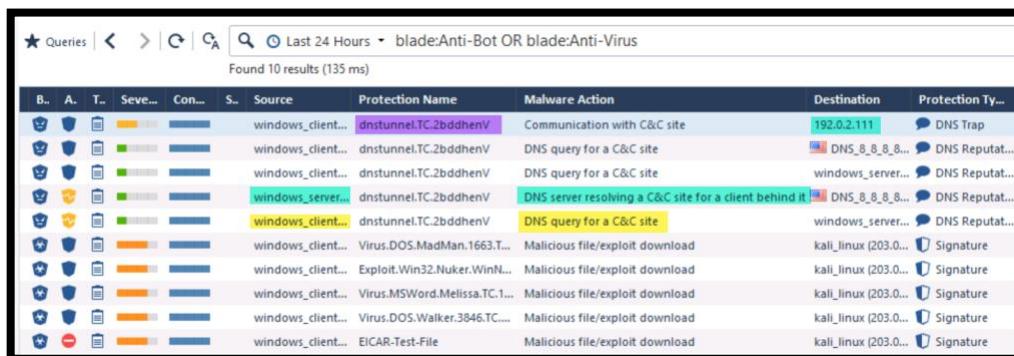


- Test DNS resolution from the windows client with the command `nslookup thegreattunnel.com`

```
C:\Users\admin>nslookup thegreattunnel.com
Server: UnKnown
Address: 10.1.2.250

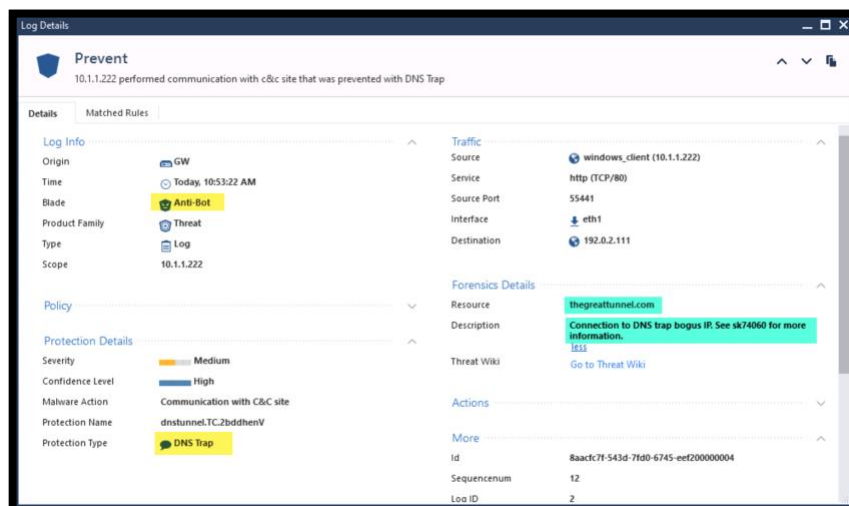
Non-authoritative answer:
DNS request timed out.
    timeout was 2 seconds.
Name:   thegreattunnel.com
Address: 192.0.2.111
```

- Filter the logs to show Anti-Bot logs. Notice that the same DNS Tunneling protections is associated with different actions.
  - The attempt to reach the C&C associated with DNS tunneling was identified by multiple protection types.



B.	A.	T.	Seve...	Con...	S.	Source	Protection Name	Malware Action	Destination	Protection Ty...
						windows_client...	dnstunnel.TC.2bddhenV	Communication with C&C site	192.0.2.111	DNS Trap
						windows_client...	dnstunnel.TC.2bddhenV	DNS query for a C&C site	DNS_8_8_8...	DNS Reputat...
						windows_client...	dnstunnel.TC.2bddhenV	DNS query for a C&C site	windows_server...	DNS Reputat...
						windows_server...	dnstunnel.TC.2bddhenV	DNS server resolving a C&C site for a client behind it	DNS_8_8_8...	DNS Reputat...
						windows_client...	dnstunnel.TC.2bddhenV	DNS query for a C&C site	windows_server...	DNS Reputat...
						windows_client...	Virus.DOS.MadMan.1663.T...	Malicious file/exploit download	kali_linux (203.0...	Signature
						windows_client...	Exploit.Win32.Nuker.WinN...	Malicious file/exploit download	kali_linux (203.0...	Signature
						windows_client...	Virus.MSWord.Melissa.TC.1...	Malicious file/exploit download	kali_linux (203.0...	Signature
						windows_client...	Virus.DOS.Walker.3846.TC...	Malicious file/exploit download	kali_linux (203.0...	Signature
						windows_client...	EICAR-Test-File	Malicious file/exploit download	kali_linux (203.0...	Signature

- Review the log generated by the DNS Trap. In this case, the windows client initiated the request to the DNS on Windows Server. The windows server does not know the IP address and makes a request to the public forwarder 8.8.8.8. The GW can identify which original host made the request.



**Log Details**

Prevent  
10.1.1.222 performed communication with c&c site that was prevented with DNS Trap

Details | Matched Rules

**Log Info**

- Origin: GW
- Time: Today, 10:53:22 AM
- Blade: Anti-Bot
- Product Family: Threat
- Type: Log
- Scope: 10.1.1.222

**Policy**

**Protection Details**

- Severity: Medium
- Confidence Level: High
- Malware Action: Communication with C&C site
- Protection Name: dnstunnel.TC.2bddhenV
- Protection Type: DNS Trap

**Traffic**

- Source: windows\_client (10.1.1.222)
- Service: http (TCP/80)
- Source Port: 55441
- Interface: eth1
- Destination: 192.0.2.111

**Forensics Details**

- Resource: thegreattunnel.com
- Description: Connection to DNS trap bogus IP. See sk74060 for more information.
- Threat Wiki: Go to Threat Wiki

**Actions**

**More**

- Id: 8aac7f1543d-7f60-6745-ee220000004
- Sequencenum: 12
- Log ID: 2

## Exercise 3: IoC Feeds

Like Anti-Virus, the Check Point Anti-Bot blade can enforce external IoC feed. We will enforce the block of specific domains and IP addresses.

1. Review the IoC feed file and notice that we configured the IP address 4.2.2.1 to be blocked by the Anti-Bot blade.

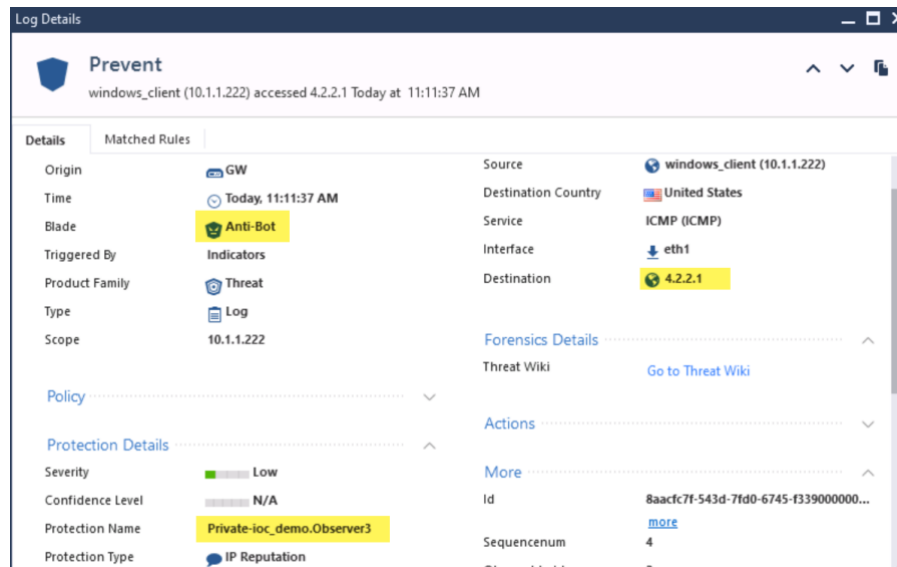
#! DESCRIPTION = IoC Demo							
#! REFERENCE = SBT							
# All lines beginning "#" are comments							
# All lines beginning "!" are metadata read by the SW							
# UNIQ-NAME,VALUE,TYPE,CONFIDENCE,SEVERITY,PRODUCT,COMMENT							
block_md5	20b2ca0d0694fdc37e3fb3f55754bdd4	MD5	high	high	AV		ioc_test_md5
block_url	http://example.com	URL	high	high	AV		ioc_test_url
block_domain	stamdomain.com	domain	high	high	AB		ioc_test_domain
block_ip	4.2.2.1	IP	high	medium	AB		ioc_block_ip

2. From windows client, try to ping the IP address 4.2.2.1.

```
C:\Users\admin>ping 4.2.2.1

Pinging 4.2.2.1 with 32 bytes of data:
Control-C
```

3. Review the logs and notice that the traffic was prevented based on the IoC feed configurations.



**Log Details**

**Prevent**  
windows\_client (10.1.1.222) accessed 4.2.2.1 Today at 11:11:37 AM

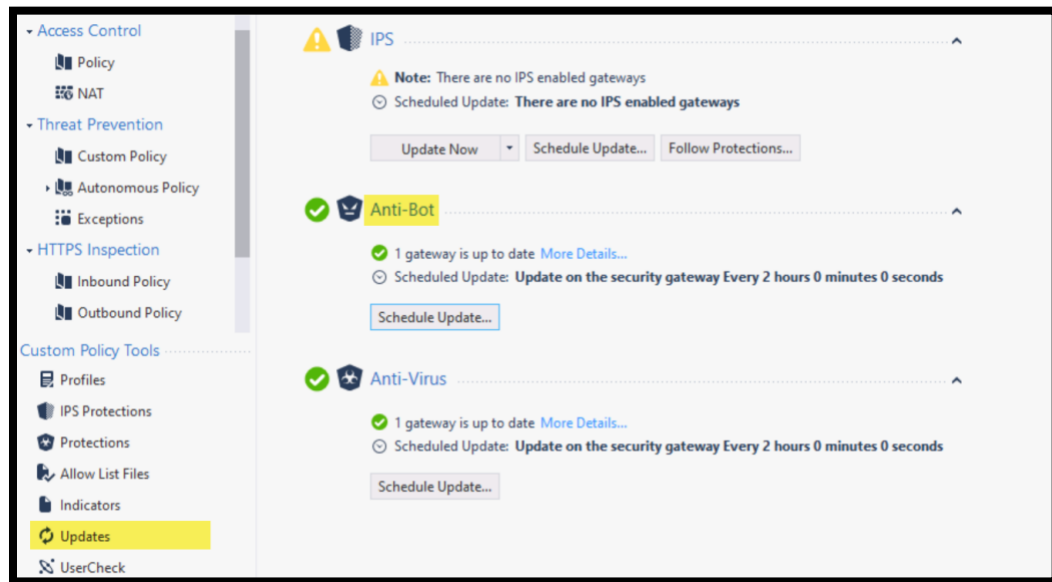
Details		Matched Rules	
Origin	GW	Source	windows_client (10.1.1.222)
Time	Today, 11:11:37 AM	Destination Country	United States
Blade	Anti-Bot	Service	ICMP (ICMP)
Triggered By	Indicators	Interface	eth1
Product Family	Threat	Destination	4.2.2.1
Type	Log	Forensics Details	
Scope	10.1.1.222	Threat Wiki: <a href="#">Go to Threat Wiki</a>	
Policy		Actions	
Protection Details		More	
Severity	Low	Id	8aacfc7f-543d-7fd0-6745-f339000000...
Confidence Level	N/A	Sequencenum	4
Protection Name	Private-ioc_demo.Observer3		
Protection Type	IP Reputation		

4. Public lists are available from different vendors. Attempt adding different IoC lists.

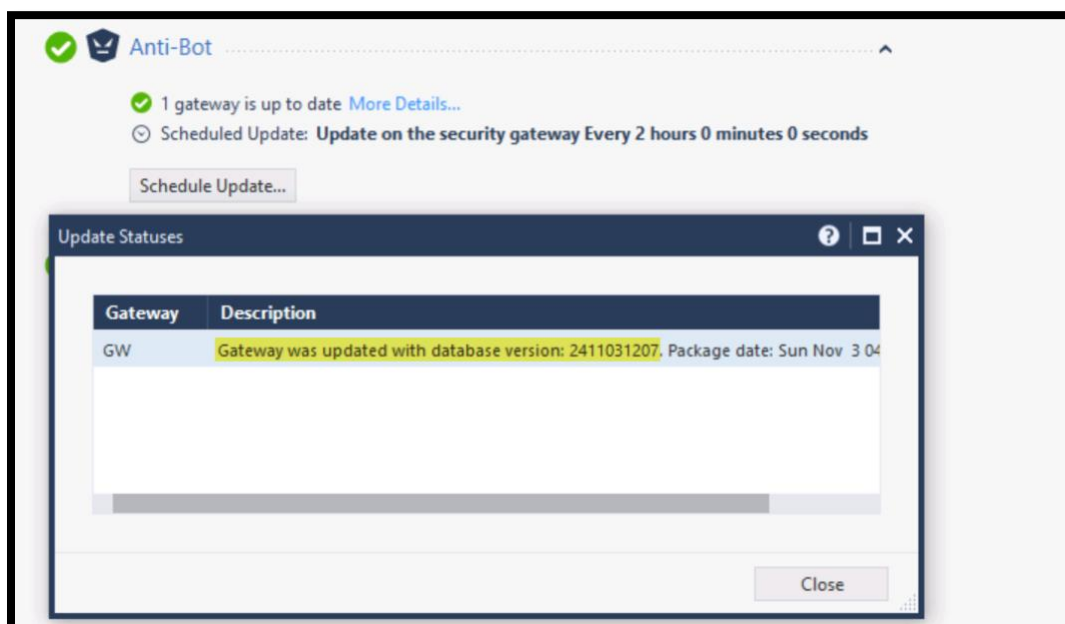
## Exercise 4: Updates

Like Anti-Virus, Anti-Bot depends on intelligence feed and updates from the Threat Cloud. By default, the GW will try to fetch updates every 2 hours.

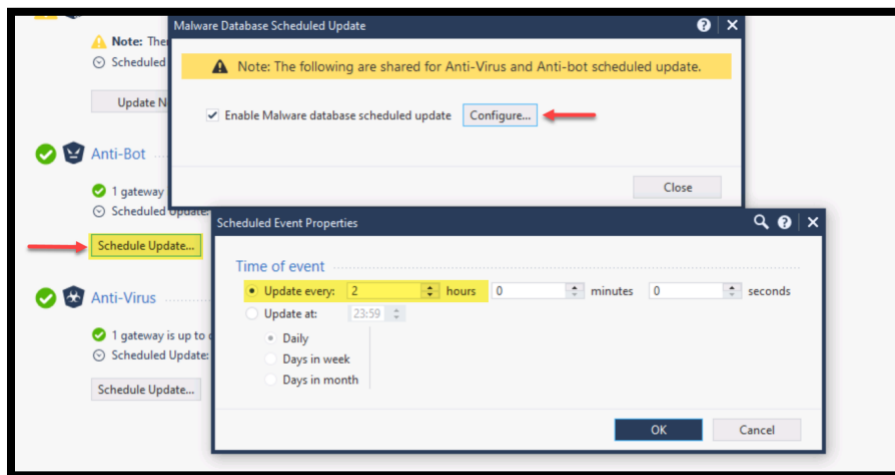
1. Navigate to the update section under the threat prevention policy.



2. Click More Details to see the update status per gateway.



3. View the default configurations under schedule Update. It is possible to disable the automatic updates.



End of Lab 7