

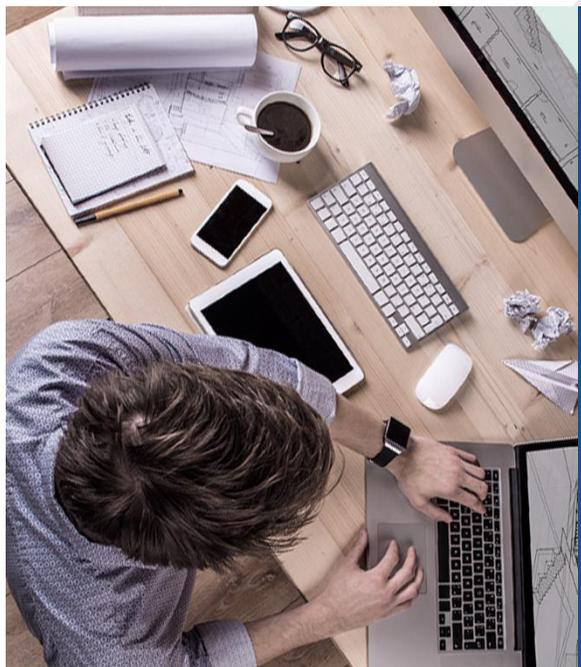


SANGFOR

SANGFOR_NGAF_V8.0.6_Professional

APT Protection





1 APT

2 APT Protection Test

3 APT Misjudgment Troubleshooting

1. APT



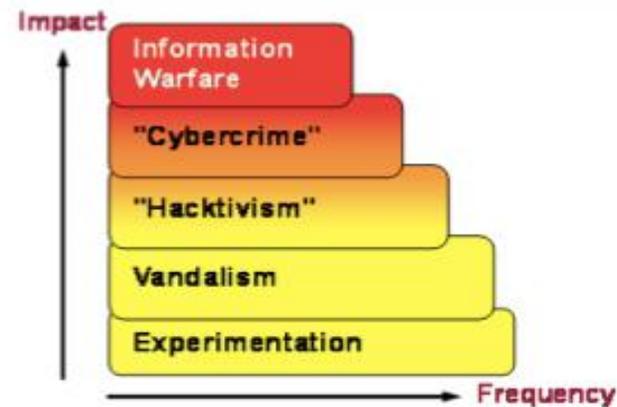
What is APT

Gartner: Defining Advanced Persistent Threats

Defining the "Advanced Persistent Threat" (aka. Advanced Targeted Attack)



Internet Threat Hierarchy



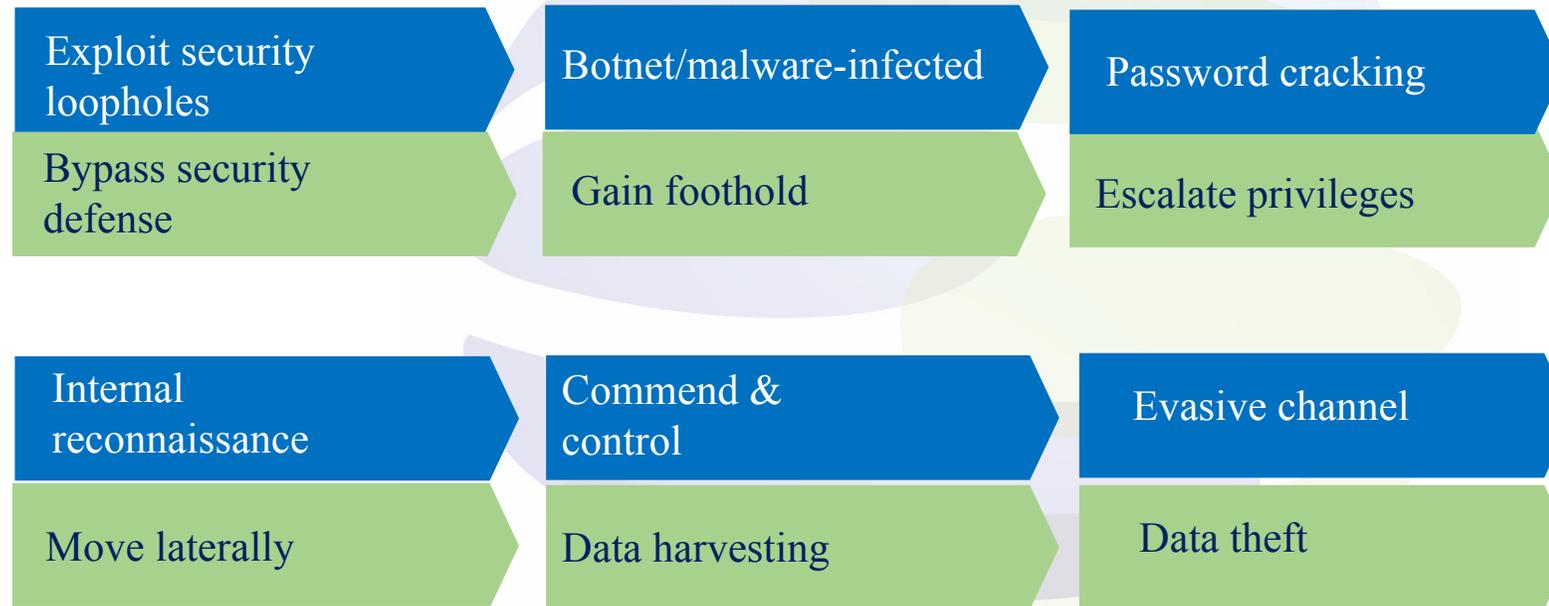
© 2013 Gartner, Inc. and/or its affiliates. All rights reserved.

Source: Gartner (August 2013)

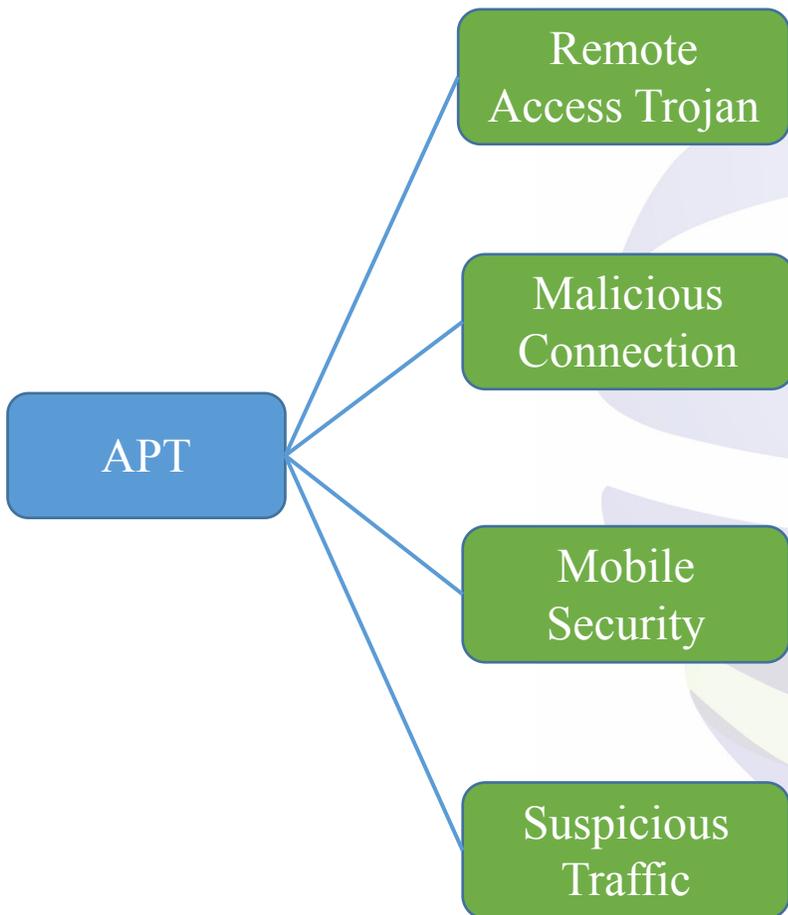
Gartner

What is APT

SANGFOR: APT is Not An Attack, But a Continuous Process



APT Protection



Security Options

- Remote Access Trojan
- Malicious Link(Cloud-Based Sandbox)
- Mobile Security(Cloud-Based Sandbox)
- Suspicious Traffic [Settings](#) ⓘ

Select Anomaly Traffic Detection Rule

<input checked="" type="checkbox"/>	Rule Name	Description
<input checked="" type="checkbox"/>	Port 3389 anomaly	The protocol running on port 3389 is not RDP.
<input checked="" type="checkbox"/>	RDP anomaly	RDP protocol is running on port rather than port 3389.
<input checked="" type="checkbox"/>	Port 53 anomaly	The protocol running on port 53 is not DNS.
<input checked="" type="checkbox"/>	Port 80/8080 anomaly	An unknown application runs on port 80 or 8080.
<input checked="" type="checkbox"/>	Port 21 anomaly	The protocol running on port 21 is not FTP.
<input checked="" type="checkbox"/>	Port 69 anomaly	The protocol running on port 69 is not TFTP.
<input checked="" type="checkbox"/>	Port 443 anomaly	An unknown application runs on port 443.
<input checked="" type="checkbox"/>	Port 25 anomaly	The protocol running on port 25 is not SMTP.
<input checked="" type="checkbox"/>	Port 110 anomaly	The protocol running on port 110 is not POP3.
<input checked="" type="checkbox"/>	Port 143 anomaly	The protocol running on port 143 is not IMAP.
<input checked="" type="checkbox"/>	ICMP anomaly	Size of ICMP packet is greater than 64 Bytes.
<input checked="" type="checkbox"/>	Port 22 anomaly	The protocol running on port 22 is not SSH.
<input checked="" type="checkbox"/>	SSH protocol anomaly	SSH is used to connect to an internal server on a port ra...
<input checked="" type="checkbox"/>	Suspicious Outgoing Traffic Settings	Check if Trojan exists by detecting outgoing traffic anom...

OK Cancel

APT Protection

Remote Access Trojan

- Detection based on database for Trojan.
- Path: Objects > Threat Signature Database > Predefined Database



- Detection based on endpoint behavior. (For example, endpoint will send the heartbeat packet to server to keep connection after it was infected.)

APT Protection

Malicious Link

- Detect the URL that may lead to the threat, such as webpage linked to horse, virus download link.
- Malicious link matching process:
 1. Match the white list (allow after matching);
 2. Match the blacklist (built-in database), executing action according to the policy configuration;
 3. Black and white list are not matched, then NGAF reported to the Neural X analysis. If detected the malicious behavior, the cloud sent to the AF action in accordance with the policy;
 4. Cloud update the blacklist to the new version of malicious link database;
- Whitelist is the domain in the Alexa Ranking List, such as google.com

APT Protection

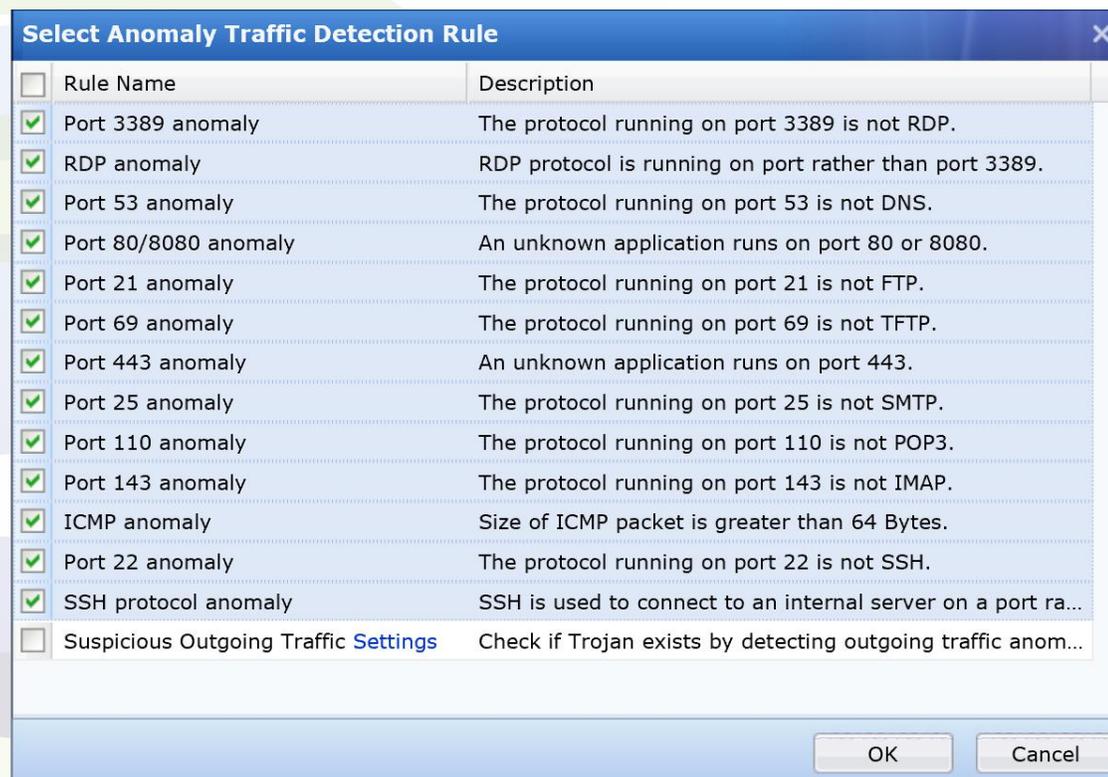
Mobile Security

- Mobile security contains two sub-functions: anti-virus of apk file and mobile botnet detection, to generate two types of log: mobile anti-viruses and mobile botnet.
- In addition to the regular detail logs, the mobile anti-virus contains a behavior analysis report, the NGAF reports the virus to the cloud sandbox, and the cloud sandbox generates a report and sends the report to the NGAF.
- If the NGAF can not access the Internet, the mobile virus behavior analysis report will not be generated.

APT Protection

Suspicious Traffic

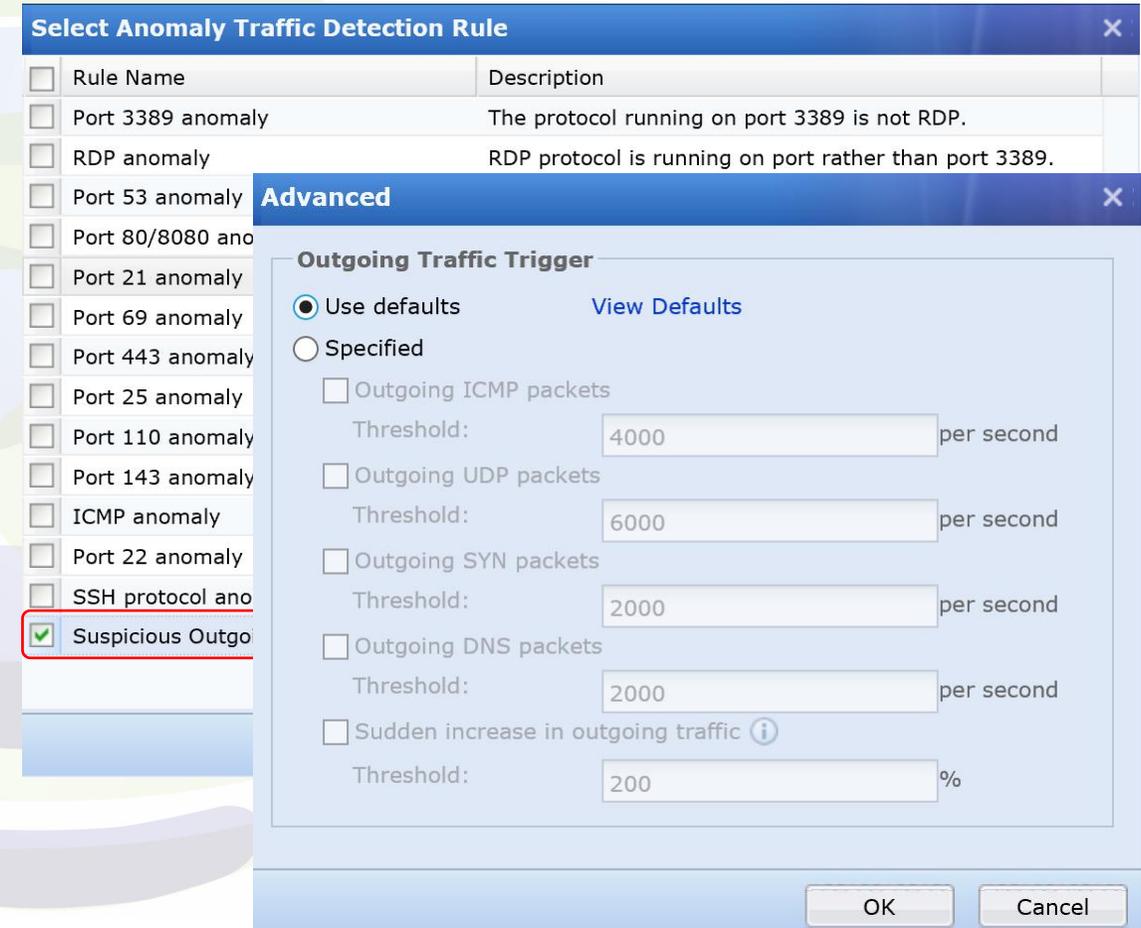
- Abnormal traffic is two-way identification, log suspicious traffic only and do not deny;
- Abnormal traffic can only identify SSH and RDP reverse shell, other protocols can not identify the reverse shell;
- IPs in the exclude IP list of APT still identify reverse shell of SSH and RDP;



APT Protection

Suspicious Traffic

- Suspicious outgoing traffic is a heuristic dos attack detection, it can detect the unchanged source IP SYN flood, ICMP flood, DNS flood and UDP flood attacks, does not support syn+ack flood and ack flood.
- Suspicious outgoing traffic features is that when the specific protocol packet outgoing pps exceeds the configured threshold, to judge whether is suspicious by detecting whether the packet is a one-way traffic, whether there is a normal response or other ways, then capture around 5 minutes packets to analyse the conclusion.



The screenshot displays two overlapping windows from a Sangfor security management interface. The top window, titled "Select Anomaly Traffic Detection Rule", contains a table of rules. The bottom window, titled "Advanced", shows configuration options for the "Suspicious Outgoing Traffic" rule.

Rule Name	Description
<input type="checkbox"/> Port 3389 anomaly	The protocol running on port 3389 is not RDP.
<input type="checkbox"/> RDP anomaly	RDP protocol is running on port rather than port 3389.
<input type="checkbox"/> Port 53 anomaly	
<input type="checkbox"/> Port 80/8080 ano	
<input type="checkbox"/> Port 21 anomaly	
<input type="checkbox"/> Port 69 anomaly	
<input type="checkbox"/> Port 443 anomaly	
<input type="checkbox"/> Port 25 anomaly	
<input type="checkbox"/> Port 110 anomaly	
<input type="checkbox"/> Port 143 anomaly	
<input type="checkbox"/> ICMP anomaly	
<input type="checkbox"/> Port 22 anomaly	
<input type="checkbox"/> SSH protocol ano	
<input checked="" type="checkbox"/> Suspicious Outgo	

Advanced

Outgoing Traffic Trigger

Use defaults [View Defaults](#)

Specified

Outgoing ICMP packets
Threshold: 4000 per second

Outgoing UDP packets
Threshold: 6000 per second

Outgoing SYN packets
Threshold: 2000 per second

Outgoing DNS packets
Threshold: 2000 per second

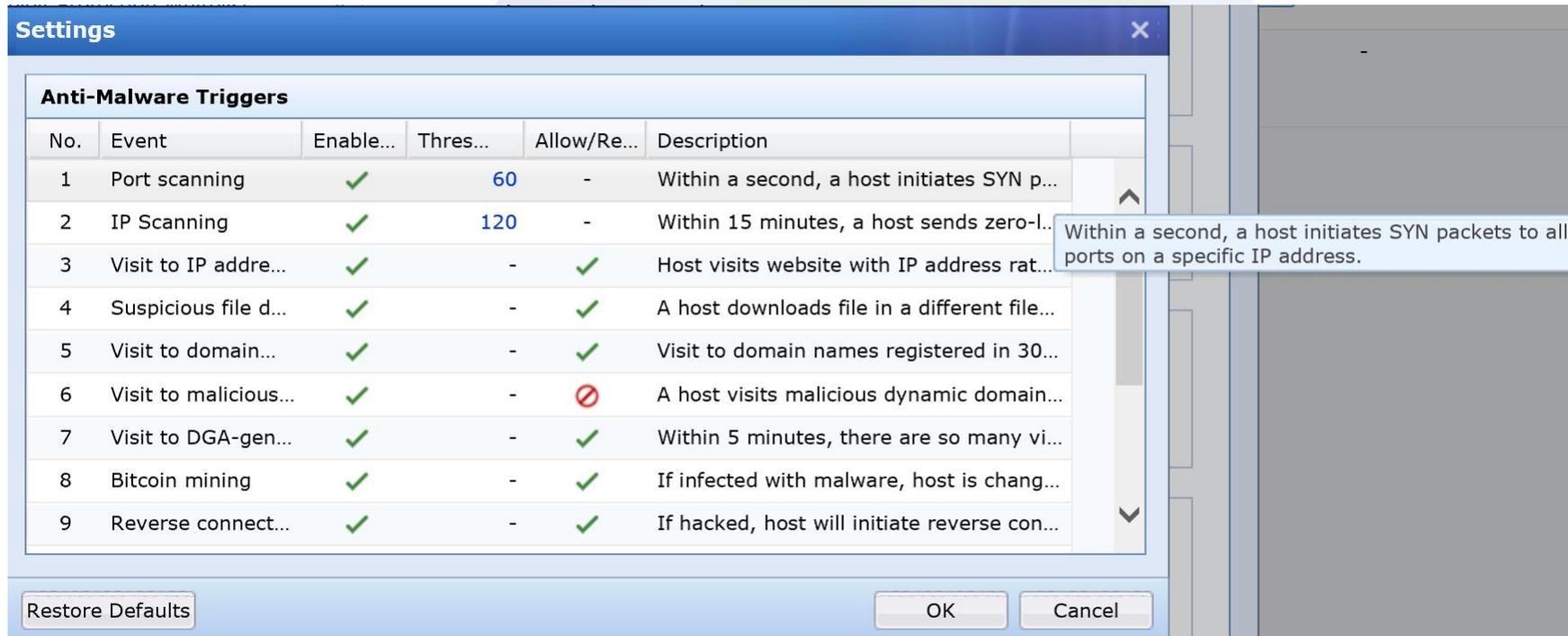
Sudden increase in outgoing traffic ⓘ
Threshold: 200 %

OK Cancel

APT Protection

Auxiliary functions: Malware detection

By detecting for suspicious behaviors, it locates the possible bot-infected hosts and logs the events.



Settings

Anti-Malware Triggers

No.	Event	Enable...	Thres...	Allow/Re...	Description
1	Port scanning	✓	60	-	Within a second, a host initiates SYN p...
2	IP Scanning	✓	120	-	Within 15 minutes, a host sends zero-l...
3	Visit to IP addre...	✓	-	✓	Host visits website with IP address rat...
4	Suspicious file d...	✓	-	✓	A host downloads file in a different file...
5	Visit to domain...	✓	-	✓	Visit to domain names registered in 30...
6	Visit to malicious...	✓	-	⊘	A host visits malicious dynamic domain...
7	Visit to DGA-gen...	✓	-	✓	Within 5 minutes, there are so many vi...
8	Bitcoin mining	✓	-	✓	If infected with malware, host is chang...
9	Reverse connect...	✓	-	✓	If hacked, host will initiate reverse con...

Restore Defaults OK Cancel

Log only, does not deny.

APT Protection

Auxiliary functions: DNS redirections of malware URLs

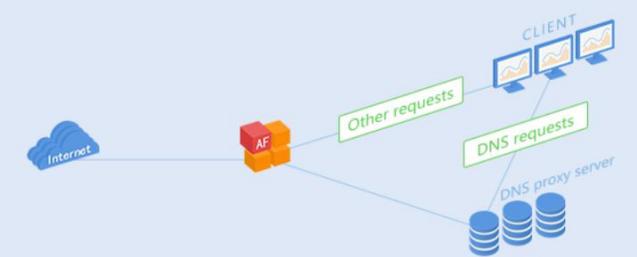
It is also called DNS sinkhole used in scenario with DNS proxy server to find the true IP address of bot-infected internal host.

Settings

The IP address to a malicious URL will be redirected to the following honeypot IP address upon access, so as to find the true IP address of the bot-infected host by listening to the accesses to that honeypot IP address.

This is recommended only for the following situation:

1. The NGAF appliance is not deployed in Mirror mode.
2. A DNS server is deployed in the network, as shown in the figure below:



Honeypot Address

Use Sangfor online honeypot address (recommended)

Specified

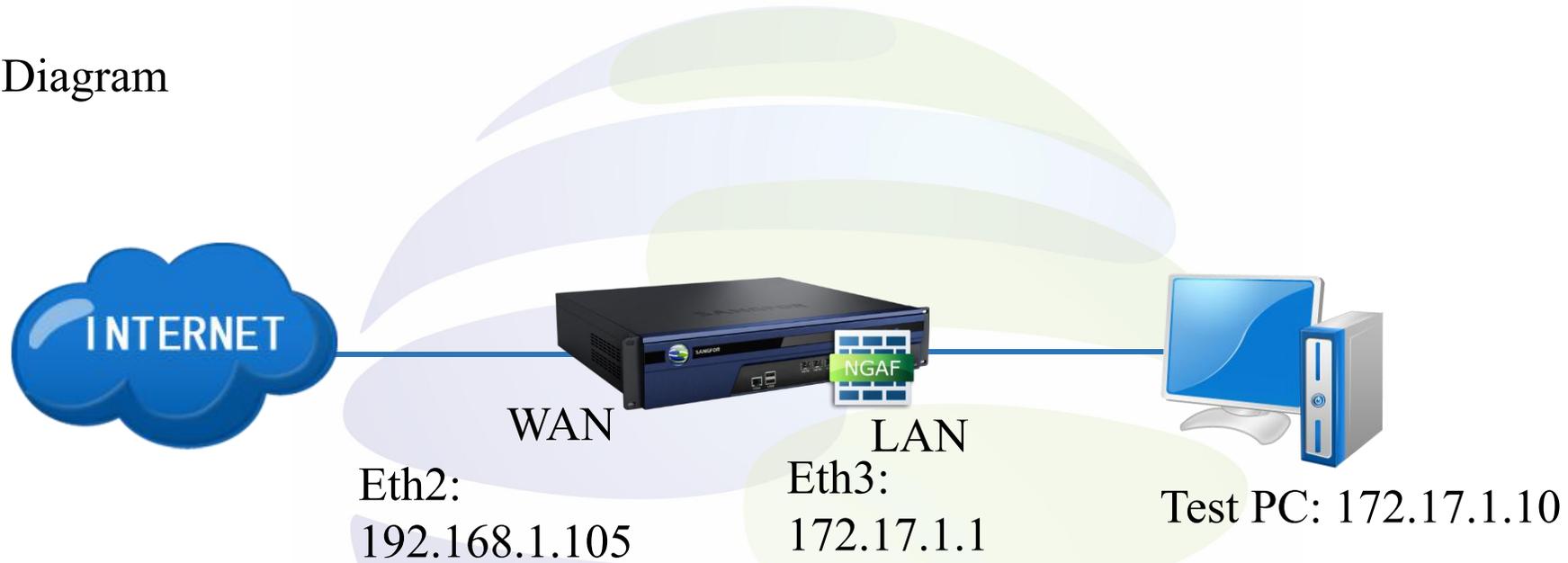
(make sure internal hosts have access to this address)

2. APT Protection Test



APT Protection Test

Network Diagram



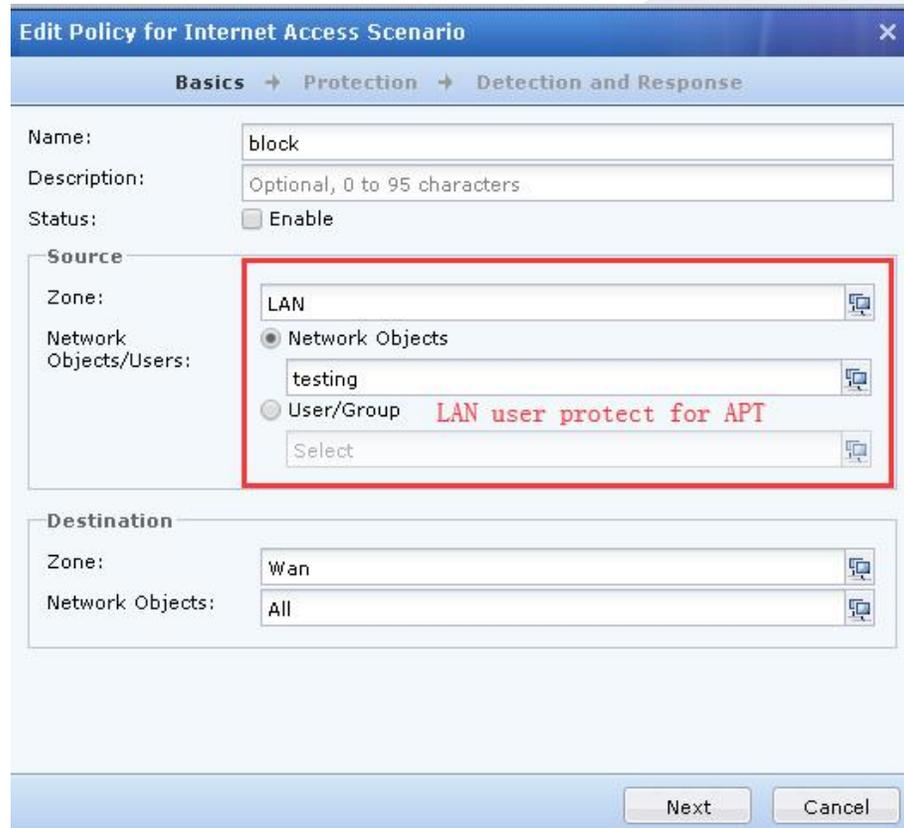
NGAF deploy as route mode, test PC simulate as an botnet infected client and access the internet via NGAF.

(Network setting, application control policy and NAT are omitted.)

APT Protection Test

Policy settings

Path: Policies > Network Security > Policies



Edit Policy for Internet Access Scenario

Basics → Protection → Detection and Response

Name: block

Description: Optional, 0 to 95 characters

Status: Enable

Source

Zone: LAN

Network Objects/Users:

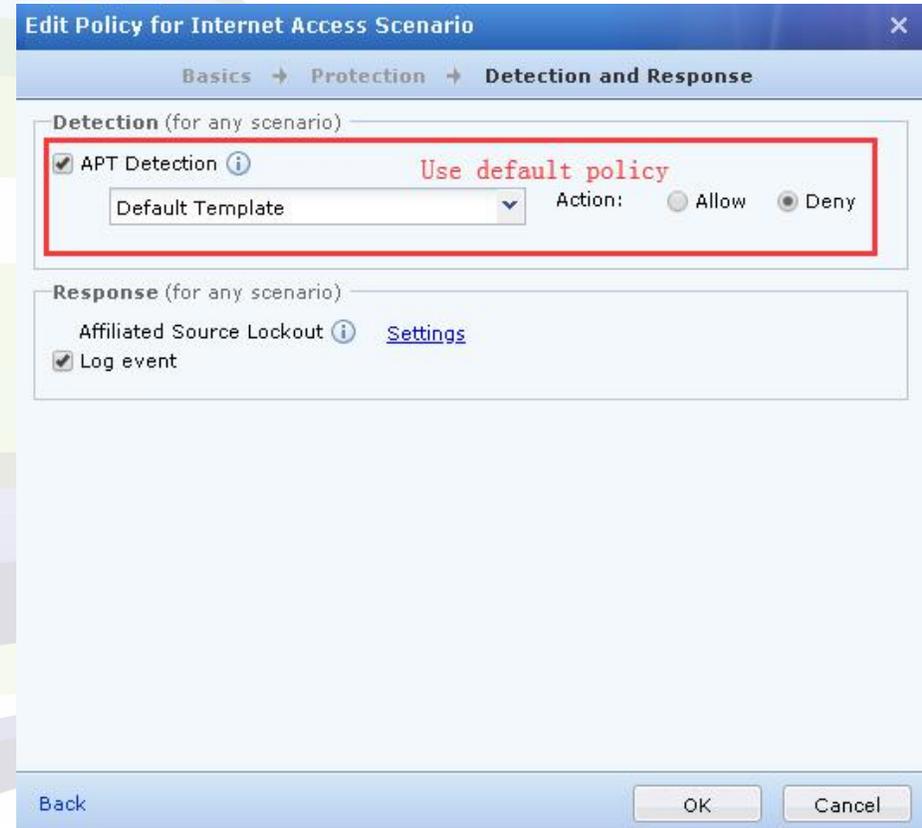
- Network Objects
- testing
- User/Group LAN user protect for APT
- Select

Destination

Zone: Wan

Network Objects: All

Next Cancel



Edit Policy for Internet Access Scenario

Basics → Protection → Detection and Response

Detection (for any scenario)

APT Detection Use default policy

Default Template Action: Allow Deny

Response (for any scenario)

Affiliated Source Lockout Settings

Log event

Back OK Cancel

APT Protection Test

Login to NGAF internal report center to check logs after PC accessed some malicious links

APT

Filter | Export Logs

Filter: Period (2017-12-17 00:00~2017-12-17 23:59) | Src zone (All) | Src IP/user (All) | Dst zone (All) | ID(All) | Type (All) | Threat level (High,Medium,Low,Info) | Action (Allow,Deny)

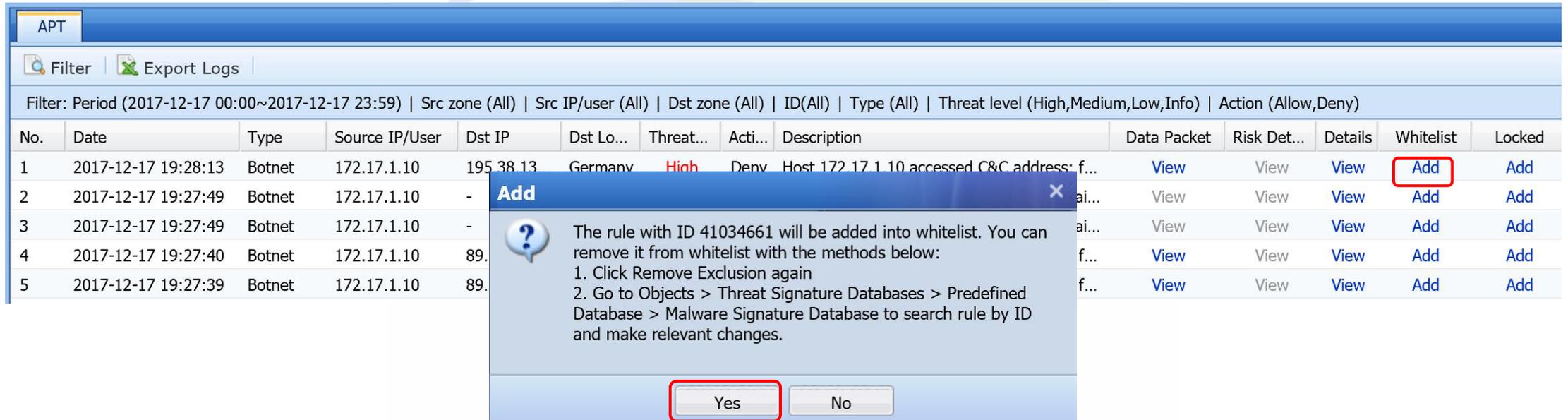
No.	Date	Type	Source IP/User	Dst IP	Dst Lo...	Threat...	Acti...	Description	Data Packet	Risk Det...	Details	Whitelist	Locked
1	2017-12-17 19:28:13	Botnet	172.17.1.10	195.38.13...	Germany	High	Deny	Host 172.17.1.10 accessed C&C address: f...	View	View	View	Add	Add
2	2017-12-17 19:27:49	Botnet	172.17.1.10	-	-	High	Deny	Sangfor security engir					
3	2017-12-17 19:27:49	Botnet	172.17.1.10	-	-	High	Deny	Sangfor security engir					
4	2017-12-17 19:27:40	Botnet	172.17.1.10	89.185.44...	France	High	Deny	Host 172.17.1.10 acce					
5	2017-12-17 19:27:39	Botnet	172.17.1.10	89.185.44...	France	High	Deny	Host 172.17.1.10 acce					
6	2017-12-17 19:23:08	Botnet	172.17.1.10	195.38.13...	Germany	High	Deny	Host 172.17.1.10 acce					
7	2017-12-17 19:23:07	Botnet	172.17.1.10	195.38.13...	Germany	High	Deny	Host 172.17.1.10 acce					
8	2017-12-17 19:16:24	Botnet	172.17.1.10	89.223.10...	Russia	High	Deny	Sangfor security engir					
9	2017-12-17 19:14:54	Botnet	172.17.1.10	115.231.1...	China	High	Deny	Sangfor security engir					
10	2017-12-17 19:14:40	Botnet	172.17.1.10	-	-	High	Deny	Sangfor security engir					
11	2017-12-17 19:11:19	Botnet	172.17.1.10	89.223.10...	Russia	High	Deny	Sangfor security engir					
12	2017-12-17 19:11:18	Botnet	172.17.1.10	89.223.10...	Russia	High	Deny	Sangfor security engir					
13	2017-12-17 19:09:49	Botnet	172.17.1.10	115.231.1...	China	High	Deny	Sangfor security engir					
14	2017-12-17 19:09:49	Botnet	172.17.1.10	115.231.1...	China	High	Deny	Sangfor security engir					
15	2017-12-17 19:09:35	Botnet	172.17.1.10	-	-	High	Deny	Sangfor security engir					
16	2017-12-17 19:09:34	Botnet	172.17.1.10	-	-	High	Deny	Sangfor security engir					

No. 1	
Date:	2017-12-17 19:28:13
Type:	Botnet
Protocol:	TCP
URL/Directory:	futureinterest.org/
Src Zone:	LAN
Source IP/User:	172.17.1.10
Group:	-
Src Port:	55304
Dst Zone:	WAN
Dst IP:	195.38.137.100
Dst Location:	Germany
Dst Port:	80
Rule ID:	41034661
Policy Name:	APT
Threat Level:	High
Action:	Deny
Description:	Host 172.17.1.10 accessed C&C address: futureinterest.org/, which is proved by virustotal. Host may be infected with virus botnet.malware.

APT Protection Excluded List

There are two ways to exclude IP/domain of NGAF APT protection if there is misjudgment:

- If the traffic of a terminal is misjudged by NGAF database, you can find the logs to click ‘Add’ of whitelist button to exclude this IP/domain



The screenshot shows the NGAF APT Protection interface. At the top, there is a tab labeled 'APT'. Below it, there are buttons for 'Filter' and 'Export Logs'. A filter bar shows the following settings: Period (2017-12-17 00:00~2017-12-17 23:59) | Src zone (All) | Src IP/user (All) | Dst zone (All) | ID(All) | Type (All) | Threat level (High,Medium,Low,Info) | Action (Allow,Deny).

No.	Date	Type	Source IP/User	Dst IP	Dst Lo...	Threat...	Acti...	Description	Data Packet	Risk Det...	Details	Whitelist	Locked
1	2017-12-17 19:28:13	Botnet	172.17.1.10	195.38.13	Germany	High	Deny	Host 172.17.1.10 accessed C&C address: f...	View	View	View	Add	Add
2	2017-12-17 19:27:49	Botnet	172.17.1.10	-				ai...	View	View	View	Add	Add
3	2017-12-17 19:27:49	Botnet	172.17.1.10	-				ai...	View	View	View	Add	Add
4	2017-12-17 19:27:40	Botnet	172.17.1.10	89.				f...	View	View	View	Add	Add
5	2017-12-17 19:27:39	Botnet	172.17.1.10	89.				f...	View	View	View	Add	Add

A dialog box titled 'Add' is overlaid on the table. It contains the following text:

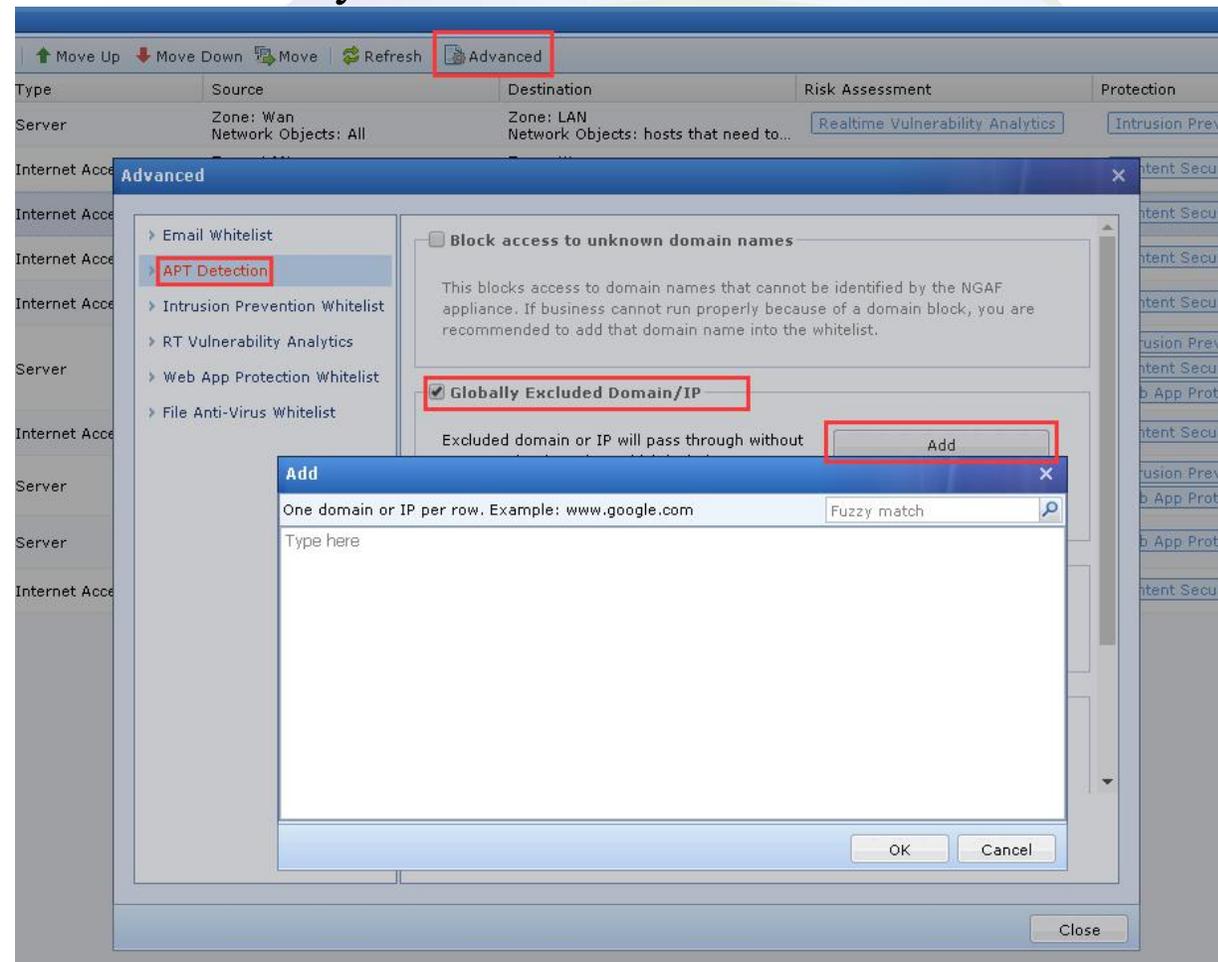
The rule with ID 41034661 will be added into whitelist. You can remove it from whitelist with the methods below:

1. Click Remove Exclusion again
2. Go to Objects > Threat Signature Databases > Predefined Database > Malware Signature Database to search rule by ID and make relevant changes.

At the bottom of the dialog box, there are two buttons: 'Yes' and 'No'. The 'Yes' button is highlighted with a red box.

APT Protection Test

- You can exclude the specified IP under the APT module, then this IP will not be intercepted by the APT policy.
- Path: Policies > Network Security > Policies > Advance

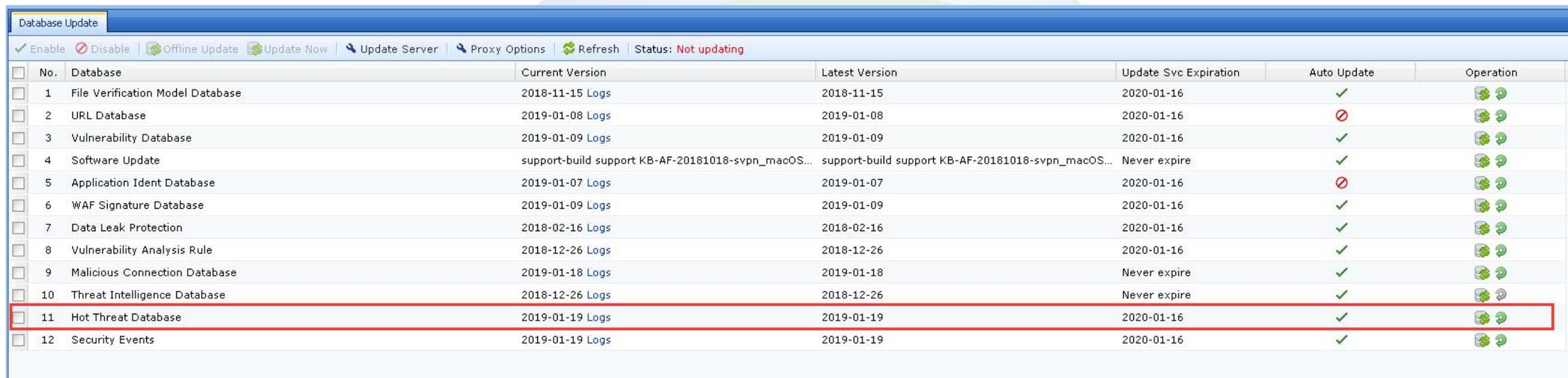


3. APT Misjudgment Troubleshooting



APT Misjudgment Troubleshooting

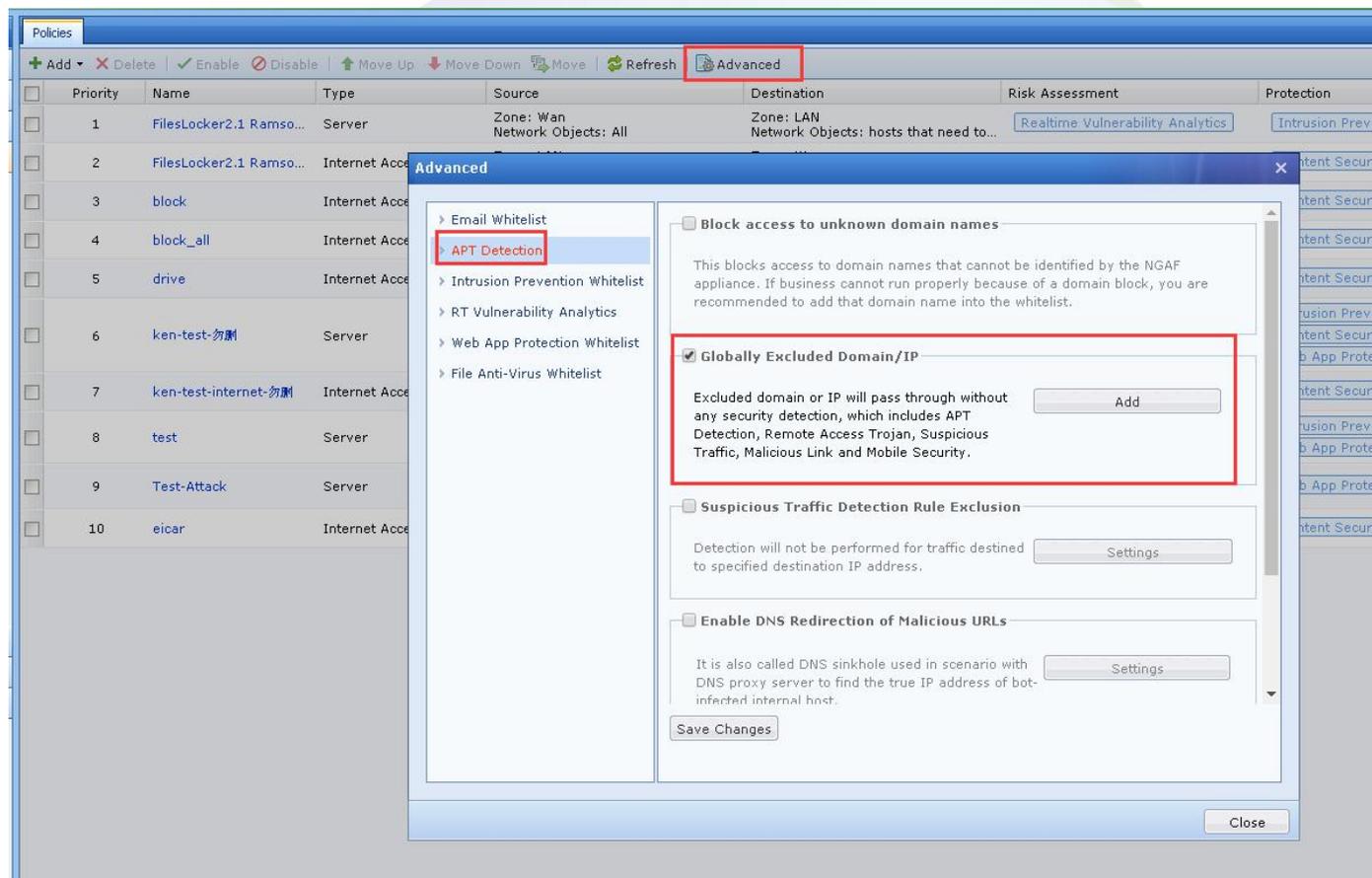
- Check the Hot Threat Database version is upgraded to latest version
- Path: System > Maintenance > Update > Database Update



No.	Database	Current Version	Latest Version	Update Svc Expiration	Auto Update	Operation
1	File Verification Model Database	2018-11-15 Logs	2018-11-15	2020-01-16	✓	 
2	URL Database	2019-01-08 Logs	2019-01-08	2020-01-16	✗	 
3	Vulnerability Database	2019-01-09 Logs	2019-01-09	2020-01-16	✓	 
4	Software Update	support-build support KB-AF-20181018-svnpn_macOS...	support-build support KB-AF-20181018-svnpn_macOS...	Never expire	✓	 
5	Application Ident Database	2019-01-07 Logs	2019-01-07	2020-01-16	✗	 
6	WAF Signature Database	2019-01-09 Logs	2019-01-09	2020-01-16	✓	 
7	Data Leak Protection	2018-02-16 Logs	2018-02-16	2020-01-16	✓	 
8	Vulnerability Analysis Rule	2018-12-26 Logs	2018-12-26	2020-01-16	✓	 
9	Malicious Connection Database	2019-01-18 Logs	2019-01-18	Never expire	✓	 
10	Threat Intelligence Database	2018-12-26 Logs	2018-12-26	Never expire	✓	 
11	Hot Threat Database	2019-01-19 Logs	2019-01-19	2020-01-16	✓	 
12	Security Events	2019-01-19 Logs	2019-01-19	2020-01-16	✓	 

APT Misjudgment Troubleshooting

- Add those misjudgment domain to whitelist
- Path: Policies > Network Security > Policies



Thank you !

tech.support@sangfor.com

community.sangfor.com

Sangfor Technologies (Headquarters)

Block A1, Nanshan iPark, No.1001

Xueyuan Road, Nanshan District,

Shenzhen, Guangdong Province,

P. R. China (518055)

