

DEPLOYMENT GUIDE

Advanced DNS Protection

Initial Deployment of PT (Physical) and Software ADP (Physical/Virtual) Appliances, Upgrade of Software ADP (Physical/Virtual) capable Appliances

NIOS 8.4

Table of Contents

Prerequisites for Grid Deployment	
Prerequisites for Standalone Deployment	4
Limitations and Cautions	4
Cautions	5
Stateful Firewalls	5
Low performance network elements (PPS)	5
Best Practices	5
Use of MGMT, LAN1, and LAN2	5
ADP Profiles	6
ADP Rules	6
Reporting	6
System alerts	6
SIEM	6
Unresponsive Servers	6
ADP Appliances	7
PT Appliances	7
Software ADP Appliances	7
Licensing	8
Supported Hypervisors	8
Deployment Architecture	8
Deploying ADP	8
Adding member information in the Grid	9
Making the member Join the Grid from Console	13
Enabling DNS resolver	18
Enabling Services on Software ADP appliance	20
Viewing all Advanced DNS Protection appliances	22
Rules supported by Advanced DNS Protection	23
System Rules	23
Auto Rules	23
Custom Rules	23
Adding Threat Protection Ruleset	
Proxy Setting on the Grid	24
Automatic Download	
Creating Custom Ruleset	29

Creating Profiles	31
Making changes to rules in Profile	34
Switching between ADP Profiles	36
Verifying the Infoblox ADP appliance is working correctly	38
SNMP Support	39
Review the Security Dashboard for Threat Protection Information	39
Security Status for Grid	39
Security Status for All Members	39
Threat Protection Status for Grid	40
Threat Protection Status for Member	42
Auto Refresh	44
Viewing Reports	45
Threat Protection Event Count by Category	45
Threat Protection Event Count by Member	45
Threat Protection Event Count by Rule	46
Threat Protection Event Count by Severity Trend	47
Threat Protection Top Rules Logged	47
Threat Protection Top Rules Logged by Source	48
Threat Protection Event Count by Member Trend	49
Threat Protection Top Rules Logged by Source	49
Logging	50
Troubleshooting & FAQ	54
Unable to download Threat Protection Rules	54
Trouble joining the Grid	54
Different rulesets for different ADP appliances	54
Question	54
Answer	54
Trouble Starting Threat Protection Service	54
Understanding a CEF Log message	54
Outbound API	55

Introduction

The Infoblox Advanced DNS Protection solution employs threat protection rules to detect, report upon, and stop DoS (Denial of Service), DDoS (Distributed Denial of Service) and other network attacks targeting DNS authoritative and recursive applications. Infoblox Advanced DNS Protection helps minimize "false positives" and ensures that your mission-critical DNS services continue to function even when under attack.

You can deploy the Advanced DNS Protection solution on hardware-accelerated appliances (physical appliances only) as well as software-based appliances (both physical and virtual) in the Grid. Depending on the appliances you deploy, you must install applicable hardware-based licenses, software subscription licenses or IB-FLEX capacity-based licensing.

This document is specifically for Software Based Advanced DNS Protection, though some recent NIOS features like profiles, and ruleset extensions also apply to hardware accelerated solutions.

Note: When referring to ADP, it should be implied the document is discussing appliances with Software ADP licenses, IB-FLEX, or Physical PT appliances.

Prerequisites for Grid Deployment

- A separate Infoblox Grid Master with Grid license.
- DNS, Threat Protection and Threat Protection Update licenses from Infoblox for the ADP appliance (Customer can use temp licenses for 60 days)
- Grid master should be able to access https://ts.infoblox.com (resolve and reach) for the Threat Protection rulesets.

Prerequisites for Standalone Deployment

- DNS, Threat Protection and Threat Protection Update licenses from Infoblox for the ADP appliance (Customer can use temp licenses for 60 days)
- The appliance should be able to access https://ts.infoblox.com (resolve and reach) for the Threat Protection rulesets.

Limitations and Cautions

- Grid Masters in Grid deployments cannot run the Threat Protection service. They are only responsible for updating rulesets.
- Standalone deployment does not support Infoblox HA (VRRP-based High Availability).
- Protected interfaces (LAN1 and LAN2) are limited to DNS and DHCP traffic, protocols in support of DNS anycast (BGP and OSPF) and the standard IP protocols such as ICMP, as well as connections to NTP servers.
- The MGMT interface is used for other traffic, such as Grid, SSH, SNMP, NTP, and it will not be protected by ADP.
- You cannot run other services, such as FTP, TFTP, and HTTP, on the advanced appliance.
 - The appliance terminates TCP connections for incoming DNS requests after handling the initial request through each TCP connection. The exception for this default Grid setting is for an SOA query sent by a client that is accepted in the allow-transfer ACL. In the case of an SOA query, the TCP connection remains open for subsequent DNS requests. This exception also covers the case in which an AXFR query follows the SOA query through the same TCP connection.

Cautions

Stateful Firewalls

Under volumetric (high PPS), stateful firewalls need to be sized appropriately. Some types of UDP DNS attacks may not have responses, which may lead to resource starvation in the firewall. Consider that 1GbE ~ 1.4 Mpps, and 10GbE ~ 14 Mpps. To prevent issues with firewalls, the LAN1/LAN2 interfaces of ADP servers should be in front of any stateful firewalls so that as ADP is not affected by these issues. This can also affect the recursion path.

Low performance network elements (PPS)

DNS is a UDP protocol whose typical query packet size is 80-90 bytes. When faced by a line-rate volumetric attack with these DNS packets, some firewalls/switches/routers are unable to cope and may reset or provide substandard performance.

Best Practices

When deploying ADP:

- ADP should not be deployed on the same Layer 2 as Clients, or where DHCP requests are broadcast. For example, in production, we're running our ADP in a /29, or /126 for IPv6
- Clients generate a lot of broadcast, especially port 5353, and other traffic which results in spurious/useless messages. DHCP broadcasts also create unnecessary noise.
- If you are running DHCP, then the expectation is that you use DHCP relay to the ADP.
- If you are not running DHCP, then the reason for the messages need to be understood and resolved. In a Lab environment, just disable the rules (set EPS to 0).
- In situations where a volumetric attack may be experienced against recursive servers, it is best to use LAN2 exclusively for recursion and to also make use of ANYcast.
- Make sure the Grid is using reliable NTP sources, a minimum of 3, and is fully synchronized.

Use of MGMT, LAN1, and LAN2

Whilst it is now possible (as of 8.1) to use LAN1 for management, it is considered a poor design choice since under volumetric attack, you may lose access to the ADP member, and the customer must accept any/all possible repercussions including loss of reporting data, logging data, disconnection from Grid, failure of Threat Protection Updates, failure to upgrade et al.

When you disable **Enable VPN on MGMT Port** setting, upon saving the following pop up is going to appear. This is a warning to be taken seriously.



ADP Profiles

It is a best practice, especially for PoC's, to utilize Profiles for all members. You can then leave the Grid version of the rules unaltered, and hence you can revert to the default rule settings for individual rules, or entire categories at any time. The only time you will need to change the Grid level rules is when you add custom rules.

ADP Rules

- With the exception of the DHCP system rules in general, and the TCP/UDP rules DNS query without Recursion Desired, all system rules should be enabled.
- When viewing the rulesets, sort by Order. The Order is the evaluation order of the rules which can prove useful for debugging and understanding rule deployment.
- Events Per Second (EPS) should either be 0 or 1 so as to reduce the chance of death by syslog. Values greater than 1 should only be used for short debug sessions. EPS limits the number of syslog entries per rule per client that can be generated.
- Setting EPS to 0 will prevent syslog messages, but the counts will still be available on the reporting server.
- Whitelisting should never be used, unless you have total and immediate control over the whitelisted client, and the reason is to give you a chance to formulate an appropriate remediation.
- Remember that like with a firewall ruleset, the last rule drops all. There must be an explicit pass somewhere (i.e. don't disable every rule).

Reporting

- It is recommended to have a Reporting member in the Grid.
- If you have not purchased a Reporting Member, you can consider deploying the free version.
- Remember to enable the security index.

System alerts

A Grid Master is able to generate SNMP and email alerts. Since these are real time, they should be configured for the categories that matter.

- System CPU/Memory/NIC usage
- Cache hit ratio
- NXDOMAIN hits
- Any issues with the status of services (DNS/DHCP/NTP/...)
- Notifications on threat protection dropped traffic and threat protection total traffic

SIEM

Use of any SIEM (Security Information and Event Management tool) is highly recommended since a great deal of Syslog information can be generated.

Unresponsive Servers

Recursive servers that aren't responding tie up resources on members.

In the Security tab in the Grid DNS Properties, it is recommended to turn on the following two options:

- Limit recursive queries per server
- Limit recursive queries per zone

C Toggle Basic Mode	Basic
General	
Forwarders	NON-RESPONSIVE SERVERS
Updates	Recursive servers that aren't responding tie up resources on members. These unresponsive servers are often the side
Queries	effect of a DNS attack, for example, a phantom-domain attack.
Zone Transfers	
Root Name Servers	Enable holddown for non-responsive servers
Sort List	
Blackhole	*Minimum timeout 1000 milliseconds
Logging	*Timeouts to trigger 5
Host Naming	
GSS-TSIG	*Holddown duration 60 seconds
DNSSEC	
Blacklist	Limit recursive queries per server
NXDOMAIN	Maximum fatabas par
DNS64	server
RRset Order	Ouota recalculation 200 fetches
Query Rewrite	interval
Restart	
Security	✓ Limit recursive queries per zone
DNS Scavenging	*Maximum fetches per 200
Traffic Control	zone

ADP Appliances

PT Appliances

The Advanced DNS Protection Appliances are high performance Infoblox network appliances that support the Infoblox ADP solution. With valid licenses installed, these appliances provide a hardware-accelerated solution to DNS threats targeting DNS caching and authoritative applications.

Currently, Infoblox offers the IB-4030 physical appliance for Advanced DNS protection and DNS Cache Acceleration.

Infoblox supports PT-1405, PT-2205, PT-4000, and IB-4030-10G.

Software ADP Appliances

When deploying Advanced DNS Protection solution, you can now install software-based subscription licenses on supported appliances (physical and virtual), in addition to the hardware-based Advanced (PT) appliances.

The Threat Protection licenses for software ADP are currently limited to following virtual and physical appliances:

TE-815, TE-825, TE-1415, TE-1425, TE-2215, TE-2225, TE-4015, TE-4025 IB-V815, IB-V825, IB-V1415, IB-V1425, IB-V2215, IB-V2225, IB-V4015, IB-V4025, IB- FLEX And we continue to support Threat Protection license for TE-1410, TE-1420, TE-2210, TE-2220 and TE-v1410, TE-v1420, TE-v2210, TE-v2220

Note: refer to the release notes for your version of NIOS for the most up to date information.

Licensing

- Threat Protection (Software add-on) A new license feature, which enables the software add-on and is licensed on a per-appliance basis for appropriate Trinzic appliances.
- Supports the Threat Protection Update license for ADP rule feed.
- Threat Protection (Software add-on) licenses are subscription-based. If the license expires, the service will continue to work but a license expiry warning will be displayed.
- The following licenses are not supported if the Threat Protection (Software add-on) license is installed on the same member:
 - Multi-Grid Management
 - o Microsoft Management
- For IB-FLEX appliances, the Threat Protection service and Threat Protection rule feed will be enabled via the Flex Grid Activation license but licensed via the appropriate SPLA ADP license. Please contact your Infoblox Sales Representative if you have any questions.

Supported Hypervisors

Software ADP appliances are supported for the following hypervisor environments:

- VMware ESXi 6.5 or later
- OpenStack (KVM) check the NIOS release notes for the latest information of supported versions
- KVM check the NIOS release notes for the latest information of supported versions

Deployment Architecture

Threat Protection appliances support standalone or grid member deployments. The Threat Protection feature is not supported on the Grid Master (GM) or Grid Master Candidate (GMC) servers. Threat Protection Appliances should always be deployed using out of band management and typically would use anycast for availability and redundancy. The intent is that any attack traffic should be contained to the network that the LAN1 interface is connected to.

If reporting is enabled, reporting traffic must be configured to use the management interface.

No extra configuration is needed if the ADP member's management interface and Reporting member's LAN1 interface share the same subnet. However, a route needs to be added in the ADP members network configuration to enable connectivity to the Reporting server if the two are on different subnets.

Deploying ADP

In this deployment guide we are using a Software ADP appliance. The ADP appliance is going to be configured so that it joins the Grid via its management interface as discussed in the deployment architecture section.

The following sections depict how to accomplish that:

Adding member information in the Grid

Before joining the ADP appliance to the Grid we must add member information in the Grid using the Infoblox Web UI.

Log in to the Grid using super-user privileges.

Go to Grid > Grid Manager > Members tab

Dashboard	is C	ata Manag	ement Cl	oud	Smart	Folders	Grid
Grid Mana	ger	Upgrade	Licenses	HSP	M Group	Micro	soft Servers
Infoblo	x 🔳 🥖					_	
DHCP	DNS	TFTP	HTTP (File	Dist)	FTP	NTP	bloxTools
Members	Se	rvices					

Under Toolbar, Click Add > Grid Member

Toolbar	>>>
🕂 Add	-
Grid Member	

Pick the appropriate Member Type. In our example, it is virtual NIOS (select **Infobiox** for a physical appliance and **Virtual NIOS** for all virtual appliance types). In **Step 1 of 3** of the **Add Grid Member** wizard, select the correct **Member Type**. Type any name of your choice in **Host Name** field. In our example, it is **software-adp.localdomain**. Click **Next**.

Add Grid Member	> Step 1 of 3		E
Member Type	Virtual NIOS 💠		1
*Host Name	software-adp.localdomair	lust be a fully qualified domain name	
Time Zone	(UTC - 8:00) Pacific Tim		Override
Comment			
Master Candidate	0		
Cancel		Previous	Save & Close -

In step 2 of 3, keep the default value for Type of Member as Standalone Member.

Set the appropriate IP address, subnet mask and Gateway information for the member's LAN1 interface.

ad Grid Wen	nber > Step 2 of	3				
ype of Network onnectivity	IPv4	\$				
TYPE OF MEMBE	ER					- 1
 Standalone M High Availabil 	tember lity Pair					
LEGUINED FUR	15 AND ADDRESSES					_
			1			
INTERFACE LAN1 (IPv4)	ADDRESS 10.61.19.55	SUBNET MASK (IPV4) OR PREFIX LENGTH (I 255.255.255.0	GATEWAY 10.61.19.1	VLAN TAG	PORT SETTINGS Automatic	
INTERFACE LAN1 (IPv4)	ADDRESS 10.61.19.55	SUBNET MASK (IPV4) OR PREFIX LENGTH (L 255.255.255.0	GATEWAY 10.61.19.1	VLAN TAG 3019	PORT SETTINGS Automatic	

Click Save & Close.

Note: The newly added member will show as **offline** in the **Grid Manager > Members** Tab.

Grid Manager	Upgrade	Licenses	HSM Group	Micros	oft Servers	Ecosystem		
Infoblox =	× R							
DHCP DN	S TFTP	HTTP (File Dis	t) FTP	NTP	bloxTools	Captive Portal	Reporting	Thre
Members	Services							
Quick Filter Nor	ne	• Off Filt	er On	Show Filter	Off Rep	blication Status Vie	<u>w</u>	
Group Rest	ults Grou	up By Choose o		v		+		
+ 2 8		8 1 - 8						
	NAME		STATUS -	-			IPV4 ADDRESS	IP
	software-a	adp.localdomain	Offline				10.61.19.55	

Click on the Properties icon next to the newly added member software-adp.localdomain.



Click Edit.

Click Toggle Advanced Mode in not already selected.



Go to the Network tab.

Scroll down in Basic Tab to Additional Ports and Addresses section.

Click + > MGMT (IPV4) (Please select the appropriate IP version- v4 or v6).

+	- 💼	3 Backup
POR	MGMT (IPv4)	
	MGMT (IPv6)	
	Additional Address	(loopback) (IPv4)

Set the appropriate IP Address, subnet mask and gateway information for the management interface of the software ADP member.

software-adp.localdomain (Grid Member Properties Editor)								
Basic Adva	nced							
ADDITIONAL PORTS A	AND ADDRESSES			+ - ā				
INTERFACE	ADDRESS	SUBNET MASK (IPV4) OR PREFIX LENGTH (I	GATEWAY	/LAN TAG PORT SETTINGS				
MGMT (IPv4)	10.60.18.126	255.255.255.0	10.60.18.1	Automatic				
	ain (Grid Member Pro Basic Adva ADDITIONAL PORTS A INTERFACE MGMT (IPv4)	Ann (Grid Member Properties Editor) Basic Advanced ADDITIONAL PORTS AND ADDRESSES INTERFACE ADDRESS MGMT (IPv4) 10.60.18.126	ain (Grid Member Properties Editor) Basic Advanced ADDITIONAL PORTS AND ADDRESSES INTERFACE ADDRESS INTERFACE ADDRESS SUBNET MASK (IPV4) OR PREFix LENGTH (L V MGMT (IPv4) 10.60.18.126 255.255.255.0	ain (Grid Member Properties Editor) Basic Advanced ADDITIONAL PORTS AND ADDRESSES INTERFACE ADDRESS INTERFACE ADDRESS SUBNET MASK (IPV4) OR PREFIX LENGTH (I GATEWAY V MGMT (IPv4) 10.60.18.126 255.255.255.0 10.60.18.1				

Switch to the Network -> Advanced tab.

Check the box next to Enable VPN on MGMT Port.



Click Save & Close.

Click **Yes** to confirm at the warning message.

Enable Management IPv4 Address column in the Grid Manager GUI:

Hover over a button in the header row and click on the downwards facing arrow that appears. Expand the **Columns** menu item and select **Edit Columns**.

NAME	•	STATUS 🚽	
software-adp.localdomain		Sort Ascending Sort Descending	
ol-18-121.tme.infoblox.com		Columns 🕨	Edit Columns
Sol-18-122.tme.infoblox.com		Pupping	

Check the box under the Visible column for Management IPv4 Address.

Edit Columns			×
COLUMN	WIDTH	SORT	VISIBLE
Name	171	Yes	
НА	54	Yes	V
Status	250	Yes	
IPv4 Address	100	Yes	✓
IPv6 Address	100	Yes	
Management IPV4 Address	100	Yes	

Click Apply.

You can now view the Management IP address for your server in the general display:

Mem	bers	Services							
Quick	Quick Filter None Filter On Show Filter Off Replication Status View								
	Group Res	ults Group By Choose one	v	+					
+1	2 8	🖂 🎟 🖿 🗘 - 🔒							
		NAME	STATUS 🖵		IPV4 ADDRESS	IPV6 ADDRESS	MANAGEMENT IP		
V	≡	🚸 software-adp.localdomain	Offline		10.61.19.55		10.60.18.126		
	_		-		10 00 10 101				

Making the member Join the Grid from Console

This section describes the steps to add mandatory licenses and networking information on the new Software ADP member through the use of its console and then making the member join the Grid.

Connect to the console of the new member.

Login using the default login (admin/infoblox)

Apply the appropriate license using either the **set license** or **set temp_license** command.

In this guide, we are using temporary licenses. Example:

set temp_license

	type 'help' for more information
Infol	blox > set temm license
	10/ / 000 00mp_1100100
1.	DNSone (DNS, DHCP)
2.	DNSone with Grid (DNS, DHCP, Grid)
З.	Network Services for Voice (DHCP, Grid)
4.	Add NIOS License
5.	Add DNS Server license
6.	Add DHCP Server license
7.	Add Grid license
8.	Add Microsoft management license
9.	Add Multi-Grid Management license
10.	Add Query Redirection license
11.	Add Response Policy Zones license
12.	Add FireEye license
13.	Add DNS Traffic Control license
14.	Add Cloud Network Automation license
15.	Add Security Ecosystem license
16.	Add Flex Grid Activation license
17.	Add Flex Grid Activation for Managed Services license
Seler	t license (1-17) or a to auit:

Select option 4.

```
Add
          Cloud Network Automation license
15. Add Security Ecosystem license
16. Add Flex Grid Activation license
 17. Add Flex Grid Activation for Managed Services license
Select license (1-17) or q to quit: 4
  1. IB-V805
2. CP-V805
  3. IB-V815
  4. IB-V825
5. IB-V1405
  6. CP-V1405
  7. IB-V1415
8. IB-V1425
  9. IB-V2205
 10. CP-V2205
     IB-V2215
 12. IB-V2225
 13. IB-V4005
 14.
     IB-V4015
 15. IB-V4025
 16. IB-V5005
Enter a number corresponding to a NIOS model (1 - 16) or q to quit:
```

In our example we are deploying IB-V825. So, select option 4.

Note: Please choose the option for the model you are going to deploy. For IB-FLEX, see https://docs.infoblox.com/display/nios84/About+IB-FLEX

The appliance will restart shortly after the NIOS license is applied. Once the server completes the restart process, add appropriate licenses using set license command. In our example here, we use the **set temp_licenses** command multiple times to apply the required licenses:

Infoblo	x > set temp_license
1. DN	Sone (DNS, DHCP)
2. DN	Sone with Grid (DNS, DHCP, Grid)
3. Ne	twork Services for Voice (DHCP, Grid)
4. Ad	d NIOS License
5. Ad	d DNS Server license
6. Ad	d DHCP Server license
7. Ad	d Grid license
8. Ad	d Microsoft management license
9. Ad	d Multi-Grid Management license
10. Ad	d Query Redirection license
11. Ad	d Threat Protection (Software add-on) license
12. Ad	d Threat Protection Update license
13. Ad	d Response Policy Zones license
14. Ad	d FireEye license
15. Ad	d DNS Traffic Control license
16. Ad	d Cloud Network Automation license
17. Ad	d Security Ecosystem license
18. Ad	d Flex Grid Activation license
19. Ad	d Flex Grid Activation for Managed Services license
Select	license (1-19) or a to auit:

Select option 5 (DNS Server license).

Select license (1-19) or q to quit: 5

This action will generate a temporary 60-day Add DNS Server license. Are you sure you want to do this? (y or n): _

Select option 7 (Add Grid license).

Select license (1-19) or q to quit: 7

This action will generate a temporary 60-day Add Grid license. Are you sure you want to do this? (y or n): _

Select option 11 (Add Threat Protection (Software add-on) license).

Select license (1-19) or q to quit: 11 Adding license(s) requires a product restart. Are you sure you want to proceed? (y or n): _

After Adding Threat Protection (Software add-on) License, the appliance will restart. Log back in once the restart completes.

Apply the appropriate license to enable the **threat protection** feature via the **set temp_license** command.

Select option 10 (Add Threat Protection Update license).

```
Select license (1-17) or q to quit: 10
This action will generate a temporary 60-day Threat Protection Update license.
Are you sure you want to do this? (y or n): y_
```

If not already configured, issue the following command to configure the LAN1 interface:

set network

Note: This IP address must match the IP address configured for the server in the grid that you will be joining it to. At the **Become grid member** prompt, enter 'n' at this time. You will join it to your Grid using the **set membership** command further down in the steps provided here.

Infoblox >	
Infoblox > set network	
NOTICE: All HA configura	tion is performed from the GUI. This interface is
used only to cor	figure a standalone node or to join a Grid.
Enter IP address: 10.61.	19.55
Enter netmask [Default:	255.255.255.01:
Enter gateway address []	efault: 10.61.19.1]:
Enter VLAN tag [Default:	Untagged]:
Configure IPv6 network s	ettings? (y or n): n
Become grid member? (y c	rn): n
New Network Settings:	
IPv4 address:	10.61.19.55
IPv4 Netmask:	255.255.255.0
IPv4 Gateway address:	10.61.19.1
IPv4 VLAN tag:	Untagged
Old IPv4 Network Settin	gs:
IPv4 address:	192.168.1.2
IPv4 Netmask:	255.255.255.0
IPv4 Gateway address:	192.168.1.1
IPv4 VLAN tag:	Untagged
Is this correct?	(y or n): y
Are you sure? (y	or n):

The appliance will restart in order to reload its network interfaces. Once complete, log back in and configure the server's management interface by issuing the following command:

set interface mgmt

Enter y when asked to enable the management interface.

Then enter the appropriate IP address info for the management port (which again must match what has been set in the Grid which this server will be joining).

In our example we are not using IPv6 addressing. Hence we will not configure it.

Select n for the option Configure Management IPv6 network settings?

Select n for the option Restrict Support and remote console access to MGMT port?

Select y at the confirmation prompts. The management interface is now enabled.

Infoblox >
Infoblox >
Infoblox > set interface mgmt
Enable Management port? (y or n): y
Enter Management IP address: 10.60.18.126
Enter Management netmask [Default: 255.255.255.0]:
Enter Management gateway address [Default: 10.60.18.1]:
Configure Management IPv6 network settings? (y or n): n
Restrict Support and remote console access to MGMT port? (y or n): n
Management IPv4 address: 10.60.18.126
Management IPv4 netmask: 255.255.255.0
Management IPv4 Gateway address: 10.60.18.1
Restrict Support and remote console access to MGMT port: false
Is this correct? (y or n): y
Are you sure? (y or n): y
The management port settings have been updated
Infoblox >

In this step, the server is joined to your Grid by executing the following command in the console:

Set membership

Enter the appropriate IP address of the Grid Master LAN1 interface, along with Grid name and Grid Shared Secret. By default, the Grid name is **Infobiox** and the shared secret is **test**. These are case sensitive.

When prompted for **Enable grid services on the Management port?**, select **y**. This will enable the server to join your Grid using its mgmt interface, instead of LAN1 as is done by default. Enter **y** at the confirmation prompts.

Infoblox > Infoblox > Infoblox > set membership Join status: No previous attempt to join a grid. Enter New Grid Master VIP: 10.60.18.121 Enter Grid Name [Default Infoblox]: Enter Grid Shared Secret: test Enable grid services on the Management port? (y or n): y Join grid as member using the Managment port with attributes: Grid Master VIP: 10.60.18.121 Grid Mame: Infoblox Grid Shared Secret: test WARNING: Joining a grid will replace all the data on this node! Is this correct? (y or n): y_

The server will now attempt to contact Grid Master and synchronize database. Multiple restarts are expected during this process.

Good Bye
Disconnect NOW if you have not been expressly authorized to use this system.
login: [2019/08/06_17:46:38.340] System restart
[2019/08/06 17:47:06.320] Infoblox system initializing
[2019/08/06 17:47:07.966] MGMT port ÍPv4 10.60.18.126, netmask 255.255.255.0, ga
teway 10.60.18.1
[2019/08/06 17:47:07.968] LAN port IPv4 10.61.19.55, netmask 255.255.255.0, gate
way 10.61.19.1
[2019/08/06 17:47:39.542] Contacting the grid master at 10.60.18.121
[2019/08/06 17:47:44.193] Synchronizing database with the grid master
[2019/08/06 17:47:53.593] System restart: config change

Once the server has completed the join process to your grid, it will show as online and running when viewing its status in your Grid Manager GUI.

Dashb	oards	Data Management Smart F	olders Reporting Grid	Administration						
Grid N	lanager	Upgrade Licenses HS	SM Group Microsoft Servers	Ecosystem						
Infol	blox 💻	/ R								
DHC	P DN	S TFTP HTTP (File Dist)	FTP NTP bloxTools	Captive Portal R	Reporting T	hreat Protection	Subscriber Collection	Threat Analytics	TAX	
Mam	hara	Samilaaa								
wern	ibers	Services								
Quick	Filter No	ne v Off Filter	On Show Filter Off Re	plication Status View						
	Group Res	ults Group By Choose one		+						
+1	1	🖂 🎫 🖽 🕹 - 😝					Go to		••••]	Go
		NAME	STATUS	IPV4	ADDRESS	IPV6 ADDRESS	MANAGEMENT IPV4	HARDWARE TYPE 👻	DNS	THREAT
	=	ol-18-19.tme.infoblox.com	Running	10.6	61.19.53	fc00:10:61:19::53	10.60.18.19	PT-4000-10GE	•	
		ol-18-18.tme.infoblox.com	Running	10.6	61.21.53	fc00:10:61:21::53	10.60.18.18	PT-2200		
		pt1400-123.tme.infoblox.com	Running	10.6	61.13.123	fc00:10:61:13::123	10.60.18.123	PT-1400	•	
		l-18-121.tme.infoblox.com	Running	10.6	60.18.121			IB-VNIOS		
	\equiv	al-18-122.tme.infoblox.com	Running	10.6	60.18.122			IB-VNIOS		
		software-adp.localdomain	Running	10.6	61.19.55		10.60.18.126	IB-V825	-	-
	Ξ	v1415-124.tme.infoblox.com	Running	10.6	61.13.124	fc00:10:61:13::124	10.60.18.124	IB-V1415	•	
	=	ol-18-123.tme.infoblox.com	Running	10.6	51.19.54		10.60.18.125	IB-FLEX		

Enabling DNS resolver

To add an appropriate DNS resolver to the Grid, if not already configured, please follow the steps listed below.

Note: If this ADP is part of a Subscriber Services Site, the DNS resolver should not be inherited from the Grid. Please review release notes and documentation on Subscriber Services

Go to Grid > Grid Manager > Members

Dashboards	s Di	ata Manage	ement Sr	mart Fo	iders	Reportir	ng Grid
Grid Manag	er	Jpgrade	Licenses	s HSM Group		Micros	soft Servers
Infoblox	- /	R				_	
DHCP	DNS	TFTP	HTTP (File	Dist)	FTP	NTP	bloxTools
Members	Sen	vices					

From Toolbar, Click Grid Properties

Тоо	lbar	>>
+	Add	
ď	Edit	
Ē	Delete	
ž	Permissions	
=	Extensible Attributes	
۶	License	
C	Restart Services	
۵	Control	
=	Grid	ř.
	Properties	

Click **DNS Resolver** tab in **Grid Properties Editor**. Click **Enable DNS Resolver**.

Click +

Add the IP address(es) to be used for the DNS resolver.

C Toggle Basic Mode	Basic	
General	Enable DNS Resolver	
Security		
Password		+1 m
Proxy Settings	NAME SERVERS	
DNS Resolver Aonitoring	10.61.0.2	-
Syslog Backup		
SNMP		

Click Save & Close.

Enabling Services on Software ADP appliance

After the new server has joined the grid, it's time to start the DNS and Threat Protection services.

To start DNS Service, Go to the Grid > Grid Manager > DNS > Services tab.

Select the appropriate ADP member for which the DNS services need to be turned on.

Dashboards	Data Manage	ement Sn	nart Folders	Reporting	Grid	Administrati	on
Grid Manager	Upgrade	Licenses	HSM Group	Microso	ft Servers	Ecosystem	
Infoblox =	/ R						
DHCP DI	IS TFTP	HTTP (File	Dist) FTP	NTP	bloxTools	Captive Portal	Reporting
Members	Services						
DNS 📕 🧪							
Quick Filter	None	¢ Of	Filter On	Show Filte	er Toggle	Restart Groups	View
Group Res	sults Gro	up By Choos		×		+	
	12-18						
NAME		SE			IPV4 AD	DRESS CON	IMENT
software	e-adp.localdoma	in No	ot Running		10.61.1	9.55	
🔲 🚸 ol-18-12	21.tme.infoblox.c	com DI	NS Service is wo	orking	10.60.1	8.121	

Click Start from Toolbar.

Toolbar	>>
+ Add	-
C Restart Services	
🗹 Edit	-
Start	
Stop	

Click Yes when prompted for Start Member DNS Service.



To verify if the DNS service started, check the **Services Status column.** It will report "**DNS Service is working**" once it has finished starting. Click on the Refresh button as necessary (the page does not automatically refresh).

-	software-adp.localdomain	DNS Service is working

To start Threat Protection Service, Go to the Grid > Grid Manager > Threat Protection > Services tab.

Select the appropriate ADP member for which the Threat Protection service needs to be turned on.

Dashboards	Data Manager	ment Sn	nart Folders	Reporting	Grid	Administra	tion	
Grid Manager	Upgrade	Licenses	HSM Group	Microsoft S	ervers	Ecosystem		
Infoblox	S TFTP	HTTP (File I	Dist)	NTP blo	xTools	Captive Porta	l Reporting	Threat Protection
Members Threat Protectio	Services							
Quick Filter	lone	t) Off	Filter On	Show Filter				
Group Res	ults Grou	p By Choos		Y		+		
	1 B							
NAME		SE			IPV4 AD	DRESS CO	OMMENT	SITE
🔽 🐟 software	-adp.localdomai	n No	ot Running		10.61.1	9.55		

Click Start from Toolbar.

Toolbar	>>
🕂 Add	-
C Publish Changes	
C Edit	-
Start	

Click Yes at the Start Member Threat Protection Service prompt.



Click Restart (the prompt for Restart Services will appear twice).

To verify if the Threat Protection service started successfully, check the **Services Status column.** It must say, "**Threat Protection Service is working**". Click on the refresh button until this updates, as the page is not refreshed automatically.

🔲 🚸 software-adp.localdomain	Threat Protection Service is working	10.61.19.55
P.54341 8323		

Viewing all Advanced DNS Protection appliances

All Infoblox Active DNS appliances that are part of a Grid can be viewed from a single location, by going to **Data Management > Security > Members**.

Dashboards	Data Management	Smart Folders	Reporting	Grid	Administration
PAM V	LANs Super Host	DHCP DNS	File Distribution	on Se	curity Threat Analyti
Threat Prot	ection Rules Member	s Profiles			
Quick Filter	None	Off Filter On	Show Filter		
→ 🗷	1 B				
	NAME		STATUS	VERSION	COMMENT
	ol-18-123.tme.infoblo	x.com	Running	2019072	25-9
	software-adp.localdo	main	Running	2019072	25-9

The other place where we can view only the ADP appliances under one location is by going to

Grid > Grid Manager > Threat Protection > Services.

Dashboards	Data Manage	ment Sr	mart Folders	Reporting	Grid	Administration			
Grid Manager	Upgrade	Licenses	HSM Group	Microsoft S	ervers	Ecosystem			
DHCP DN:	Services	HTTP (File	Dist) FTP	NTP bk	IX Tools	Captive Portal	Reporting	Threat Prot	ection
Ouick Filter	n 📕 💉	t) of	Filter On	Show Filter					
Group Rest	ults Grou	ip By Choose		~		+			
	18								
NAME	tme.infoblox.co	m Ti	ERVICE STATUS	Service is workir	ıg	10.61.2	21.53	COMMENT	SITI
software	-adp.localdomai	in T	hreat Protection S	Service is workir	ıg	10.61.1	19.55		

Rules supported by Advanced DNS Protection

Infoblox ADP supports system rules, auto-generated rules, and custom rules. New system rules are added through rule updates.

System Rules

System rules are predefined threat protection rules that are built into ADP. You can enable an entire category of system rules, as well as individual rules. Although you cannot add or delete system rules, you can change some parameters, enable and disable. For most system rules, you can also modify the Action and Log Severity.

Auto Rules

Auto rules are firewall rules that are automatically defined by NIOS for blocking traffic for disabled services and ports. These rules can be grouped into different rule categories and are enabled or disabled automatically. You cannot enable or disable autogenerated rules, however, you may be able to set the log severity and control logging for some of these rules. Autogenerated rules are automatically enabled or disabled and are reconfigured based on the current running services and the configuration of the appliance.

Custom Rules

Based on your security needs, you can define custom rules using predefined rule templates. Custom rules are typically whitelisting and blacklisting rules that utilize rate limiting to detect suspicious UDP and TCP traffic. You can create up to 500 custom rules for each rule template offered by ADP. The appliance logs a syslog message if there are more than 500 rules for a specific rule category. You can remove some rules in order to create new ones for that category.

You can add or delete custom rules at the Grid level only. While you cannot add or delete custom rules for Grid Members and/or profiles, you can enable, disable, and modify some rule parameters at the appropriate place, which is recommended to be in Profiles.

Adding Threat Protection Ruleset

The Threat Protection Ruleset can be added manually or automatically. In this guide, we demonstrate the automatic Ruleset deployment as it is considered a best practice to use automatic downloads for Threat Protection Rulesets.

Proxy Setting on the Grid

Complete the following steps if you are using proxy server for web connections; otherwise skip this section and go to next section titled "Automatic Download".

Go to Grid > Grid Manager > Members.

Dashboards	Di	ata Manago	ement	Smart Fo	Iders	Reporti	ng Grid	Administratio
Grid Manage	er l	Upgrade	License	es HSM	d Group	Micro	soft Servers	Ecosystem
Infoblox	- /	A				_		

Click Grid Properties From Toolbar.

Тоо	lbar	>>
+	Add	•
Z	Edit	
	Delete	
žΞ	Permissions	
	Extensible Attributes	
۶	License	
C	Restart Services	
۵	Control	•
=	Grid Properties	•

From Toggle Advanced Mode, click **Proxy Settings**.

Click Use Proxy Server.

C Toggle Basic Mode	Basic	
General Security	Once enabled, the proxy server is used for downloading threat protection rulesets, threat analytics bundle	s, and other applicable information.
Password Proxy Settings DNS Resolver Monitoring Syslog Backup SNMP SNMP Threshold Notification	Use Proxy Server Name or IP Address Port HTTPS Proxy Content Inspection None Credentials for Proxy Server (if configured at proxy server) Use username and password to connect to proxy server if configured Username Password	
Email LOM	Members INTERFACE	+- % 8
NAT Groups	Grid Master Any	•
Object Change Tracking ActiveTrust Cloud Integration Microsoft Integration Extensible Attribute Inheritance		

Add the appropriate Name or IP Address of the Proxy Server and the appropriate port number.

Add All Members in the Grid in Members Section by clicking + and then select Add Member.



Select all members in the Member Selector dialogue.

Apple Mac OS Devices							
Conflicts	Find		Go				\rightarrow
Gaming Console Device		IPV4 ADDRESS		IPV6 ADDRESS	COMMENT	SITE	
Bouter and Wireless Ac	ol-18-122.tme.infob	10.60.18.122					
Smartphone, PDA, Tabl	ol-18-123.tme.infob	10.61.19.54					
Unmanaged	ol-18-18.tme.infoble	10.61.21.53		fc00:10:61:21::53			
	ol-18-19.tme.infoble	10.61.19.53		fc00:10:61:19::53			
	pt1400-123.tme.inft	10.61.13.123		fc00:10:61:13::123			
	software-adp.locald	10.61.19.55					
	v1415-124.tme.info	10.61.13.124		fc00:10:61:13::124	5		
		a					

Click OK.

Infoblox (Grid Properties	Editor)	×
C Toggle Basic Mode	Basic	0
General Security Password • Proxy Settings DNS Resolver Monitoring Syslog Backup SNMP • SNMP Threshold	Once enabled, the proxy server is used for downloading threat protection rulesets, threat analytics bundles, and other applica Use Proxy Server Name or IP Address Port HTTPS Proxy Content Inspection None Credentials for Proxy Server (if configured at proxy server) Use username and password to connect to proxy server if configured	whe information.
Notification Email LOM	Members + -	1 📲 1 🗰
Customer Improvement NAT Groups	name interpace ol-18-19.tme.infoblox.com Any pt1400-123.tme.infoblox.com Any	•
Object Change Tracking ActiveTrust Cloud Integration Microsoft Integration	software-adp.localdomain Any v1415-124.tme.infoblox.com Any	
Extensible Attribute Inheritance		Save & Close 🔻

Click Save & Close. Automatic Download

This section describes the method to enable automatic download of the Threat Protection Ruleset.

Go to Data Management > Security > Members.



Click Grid Security Properties from Toolbar.

Toolbar	>>
→ Open	
🗹 Edit	
E Permissions	
Start	
Stop	
so Merge	-
Grid Security Properties	
C Publish Changes	
L CSV Import	
差 CSV Job Manager	
≓ IDN Converter	

Select option **Enable Automatic Ruleset Downloads** and Click **Test Connection** to verify connectivity to the Ruleset portal.

Note: This will contact ts.infoblox.com directly from the Grid Master. If you need to use a proxy server for this connection, refer to the previous section titled "**Proxy Setting**".

A light blue banner displaying the message "Download members test connectivity overall status Success" will appear if this connection is successful.

Infoblox (Grid Securit	y Properties)		×
Download members test co	nnectivity overall status Success		Close
C Toggle Basic Mode	Basic Advanced		C
Threat Protection NAT Mappings	THREAT PROTECTION RULESE	T VERSION	
Ecosystem	*Active Ruleset Version 201	90725-9 💠	- 1
	Active Ruleset Comment		
	THREAT PROTECTION RULESE	I UPDATES	
	Latest Available Ruleset	20190725-9	
	Last Checked For Updates	2019-08-06 11:20:32 PDT	
	Rule Update Policy	Automatic \$	
	 Enable Automatic Ruleset Downloads 	Test Connection Download Rules Now	
Cancel			Save & Close 🔹

Click Download Rules Now.

Wait for the download to complete.

Infoblox (Grid Securit	y Properties)		X
Download members test co	nnectivity overall status Success	Cio	se
Toggle Basic Mode Threat Protection NAT Mappings Ecosystem	Basic Advanced THREAT PROTECTION RULESE	TVERSION	() () () ()
	Active Ruleset Comment	190725-9 \$ Loading ET UPDATES	
	Latest Available Ruleset Last Checked For Updates Rule Update Policy	20190725-9 2019-08-06 11:20:32 PDT Automatic ‡	
Cancel	Enable Automatic Ruleset Downloads	Test Connection Download Rules Now	-

Click Save & Close.

Once the download is complete you are going to see the ruleset downloaded under;

Data Management > Security > Threat Protection Rules

Dashboa	rds Data Manaç	gement Smart Folders	Reporting Grid	Administration		
IPAM	VLANs Super	Host DHCP DNS	File Distribution Sec	curity Threat Analytics		
Threat	Protection Rules	Members Profiles				
Grid T	hreat Rulese	ts				
→ +	• 🗭 🏛 🔽	0				
		ACTIVE ON	DO NOT DELET	TE ADDED ON	ADD TYPE	COMMENT
	20190725-9	Grid	No	2019-08-06 11:20:37 PDT	Automatic	

Click on the ruleset to view its content,

Dashboards Date Management Smart Folders Reporting	Grid Administrati	on				
IPAM VLANs Super Host DHCP DNS File Distribu	tion Security Thre	at Analytics				
Threat Protection Rules Members Profiles						
Threat Protection Rules Home						1
Version 20190725-9 Threat Ruleset 💉 📮						
Quick Filter None Giff Filter On Show Filter	Toggle Flat View					
+ 🖒 💼 🕹 🕀				Go to	Go	
	ORDER 🔺	RULE ID	RULE PARAMETERS	RULE NAME	ТҮРЕ С	
■ ▶ = BFD						
BGP BGP						
BLACKLIST DROP TCP IP prior to rate limiting						
BLACKLIST DROP UDP IP prior to rate limiting						
BLACKLIST TCP FQDN lookup for DNS Message Type						
BLACKLIST TCP FQDN lookup						
■ ► BLACKLIST UDP FQDN lookup for DNS Message Type						
BLACKLIST UDP FQDN lookup						
DHCP						
DNS Amplification and Reflection						
DNS Cache Poisoning						
DNS DDoS						
DNS Malware						
DNS Message Types						
N A P N I B						

Creating Custom Ruleset

Infoblox Advanced DNS Protection supports a custom rule templates from which you create new custom rules. Note that when you use a specific rule template to create custom rules, the new rules reside in their respective rule categories.

For each rule you create, you can define the Events per second value to determine the number of events per second that will be logged for the rule. In our example we are creating a custom rule that will block UDP DNS queries for domain foo.foo.foo.

To create this custom rule:

Go to Data Management > Security > Threat Protection Rules tab



Click +

Threat Protection Rules Home	
Version 20190725-9) т
Quick Filter None	•
+ 2 = 1 8	
Add Custom Rule	

From the drop-down list, select the appropriate template. In our example we select **BLACKLIST UDP FQDN lookup**

Add Custom Ru	ule > Step 1 of 2	×
*Template	BLACKLIST UDP FQDN lookup	G «
Description	A custom rule template that you use to allow blacklisting FQDN lookups on UDP.	
Comment		
	Disable	
Cancel	Previous Next	Save & Close 🔹

Click Next

Select appropriate Log Severity. We leave it at default value, which is Major.

Add foo.foo in the Value field for Blacklisted FQDN

escription ction	A custom rule template that you use to allow blacklisting FQDN lookups on UDP. Drop	- P
og Severity	Major 🗘	- 1
*RULE PARAMETER	5	
DESCRIPTION	VALUE	
Events per second	1	
Blacklisted FQDN	foo.foo	

Click Save & Close

Click **Publish** to bring up pop-up window

Publish change to apply change	Publish	
Infoblox 📚 📃 🖻	ashboards	Data Management

Click Publish to apply changes

To verify the custom rule configuration, send a DNS query (**dig @<LAN1-IP> foo.foo**) to the LAN1 IP address of the ADP appliance. The query is not going to be resolved as expected and a log message confirms the query is dropped.

CEF:0IInfobloxINIOS ThreatI8.4.0-381062I120303001IBlacklist:foo.foo.fooI7Isrc=10.61.19.13 spt=58289 dst=10.61.19.55 dpt=53 act="DROP" cat="BLACKLIST UDP FQDN lookup" nat=0 nfpt=0 nlpt=0 fqdn=foo.foo.foo hit_count=1

Creating Profiles

The ADP Profiles enables groups of members to have the same tuned ADP rulesets. Previously it was managed either as a Grid wide ruleset or every single member had to be individually managed. The cloning of profiles can be used to enable testing of ruleset tuning changes, which allow a rapid and accurate reversion, as well as implementing change control. Multiple profiles also allow you to match rulesets with customer profile. For example NATed Enterprise vs subscriber vs customer ISP.

To create a profile,

Go to Data Management > Security > Profiles

Dashboards	Data Ma	inagement	Smart	Folders	Reporting	Grid A	dministration
ipam VL	ANs Su	per Host	DHCP	DNS	File Distribution	Securit	y Threat Analytics
Threat Prote	ction Rules	Members	Prof	iles			

Click Add from Toolbar

Toolbar	>>
+ Add	
-> Open	
🗹 Edit	
Delete	
Extensible Attributes	
🍾 Merge	
Grid Security Properties	

Enter an appropriate name for the profile.

Add Threat Protection	Profile Wizard > Step 1 of 2	E
Name	ADP-Test	
Comment		
To manually apply ruleset (pdates, you must override and select the Active Ruleset Version to use for this profile.	
Active Ruleset Version	20190725-9 \$	
Active Ruleset Comment Inherited from Grid Infoblox		
*Events per Second per Rule	1 Override	
Inherited from Grid Infoblox		
Causes BIND to terminate th client matches the allow-tran	e TCP session following the sending of a response unless the query is for an SOA record and the fer ACL. Recommended for added security when using Advanced DNS Protection.	
Disable multiple DNS real Inherited from Grid Infoblox	uests via single TCP session Override	
Cancel	Previous	Save & Close

Select a ruleset from Active Ruleset Version drop down menu

By default, this field has value inherited from the Grid setting.

To select a different ruleset, Click Override

Active Ruleset Version	1	Choose One
		20190725-9
Active Ruleset Comment	-	

Select the appropriate ruleset from the list.

By default, **Events per Second per Rule** is set to **1**, to change this you can **Click Override** and configure the appropriate value.

Click Save & Close

Click Properties icon next to the newly created profile in order to assign a member to it,



Click Edit

Click Member Assignment

	Basic	
ieneral Iember Assignment	MEMBERS ASSIGNED TO THIS PROFILE	+1 =
Extensible Attributes	NAME	
	No data	

Click +

All Threat Protection Men	off Filter On	Show Filter					1
Reple Mac OS Devices	Find		Go			÷	
Gaming Console Device		IP ADDRESS	IPV6 ADDRESS	PROFILE	COMMENT		
Router and Wireless Ac	ol-18-123.tme.infob	10.61.19.54					
😭 Smartphone, PDA, Tabl	ol-18-18.tme.infoble	10.61.21.53	fc00:10:61:21::53	POC-ADP			
Unmanaged	ol-18-19.tme.infobk	10.61.19.53	fc00:10:61:19::53	POC-ADP			
	pt1400-123.tme.infc	10.61.13.123	fc00:10:61:13::123	Factory			
	software-adp.locald	10.61.19.55		ADP-Test			
	v1415-124.tme.info	10.61.13.124	fc00:10:61:13::124	POC-ADP			
	N A P PI	3					

Select the member you want to this profile be assigned to,

	Basic	
General Member Assignment	MEMBERS ASSIGNED TO THIS PROFILE	+1 🖮
Extensible Attributes	NAME software-adp.localdomain	

Click Save & Close

Click **Publish** to apply changes



Click Publish

Making changes to rules in Profile

One advantage of Profile is to use it to tune rules. In this section we are going to enable a rule that is by default disabled on the Grid.

Click on the profile link under Name column

Dashboar	ds Data Managem	ent Smart Folders	Reporting G	Grid Administration		
IPAM	VLANs Super Hos	t DHCP DNS	File Distribution	Security	Threat Analytics	
Threat P	rotection Rules Mer	nbers Profiles				
Quick Filt	None	✓ Off Filter On	Show Filter			
+ →	🗹 💼 🕹 - (₽				
		VERSION	MEMBERS			

Click on Quick Filter drop down menu



Click on All Disabled Rules

Dashboard	s Data Management S	mart Folders Rej	porting Grid	Administration				
IPAM	VLANs Super Host DHC	CP DNS File	Distribution Sec	urity Threat Analytics				
Threat Pr	otection Rules Members	Profiles						
Profiles Hor	ne							
Quick Filte	r [S] - All Disabled Rt V	Filter Off Show	Filter 🗮 <u>Toggle</u>	Flat View				
Z 1	8					Go	to	Go
	CATEGORY		RULE ID	RULE NAME	TYPE	DISABLED	RULE PARAMETERS	
	HA Support	1	10000055	PASS VRRP over UDP	Auto	Yes		
	Default Pass/Drop	3	10000070	PASS UDP VPN traffic on LAN1 interface	Auto	Yes		1
	DNS Message Types	4	10000080	EARLY PASS UDP QUIC response traffic	Auto	Yes	Rate algorithm	Rate_Limiting
	DNS Protocol Anomalies	41	110100860	EARLY DROP UDP DNS query without Recursion Desired	System	Yes	Events per second	1
	DNS Protocol Anomalies	43	110101000	EARLY DROP TCP DNS query without Recursion Desired	System	Yes	Events per second	1
	TCP/UDP Floods	2437	130000100	WARN about high rate inbound UDP DNS queries	System	Yes	Packets per second Events per second Rate algorithm	40 1 Rate_Limiting
	TCP/UDP Floods	2439	130000300	WARN about high rate inbound TCP DNS queries	System	Yes	Packets per second Events per second Rate algorithm	5 1 Rate_Limiting

Click on Properties icon next to category TCP/UDP Floods

Disable tocol Anomalies	43	110101000
Tinherit:Grid Rule Settings Edit	2437	130000100

The rule is disabled. Click **Disable** to enable it



Click Yes

Click Publish Switching between ADP Profiles

It is easy to move member assignments from one ADP profile to another ADP profile. In our example, the member is assigned to Profile named ADP-Test. If the need is to have member use a different ADP Profile, for example POC-ADP, then:

Go to Data Management > Security > Members

ashboards	Data Management	Smart Folders	Reporting	Grid Admi	inistration	
PAM VI	LANs Super Host	DHCP DNS	File Distribution	Security	Threat Analytics	
Threat Prote	ection Rules Member	s Profiles				
Quick Filter	None	Off Filter On	Show Filter			
Quick Filter	None	Off Filter On	Show Filter			
Quick Filter	None 🗸	Off Filter On	Show Filter STATUS	VERSION	COMMENT	PROFILE .

Click on Properties icon for the appropriate member,

Quick Filter	None v Off Filter C	Dn
→ œ	1 B	
	Open	
	Edit	
	Permissions	
	Cope to pere profile nobiox.com	

Click Edit

On **Basic** Tab under **Threat Protection**, you can select a specific ruleset or specific profile.

C Toggle Basic Mode	Basic Advanced	
Threat Protection NAT Mappings	Use ruleset Use profile ADP-Test Select Profile	
Ecosystem Permissions	*Active Ruleset Version 20190725-9 \$	Override
	Active Ruleset Comment Inherited from Grid Infobiox	
	*Events per Second per 1 Rule	Override
	Inherited from Grid Infoblox	

Click on Select Profile

hreat Protection Prof	Off Filter On	Show Filter	
onflicts	Find		Go
ing Console Device		COMMENT	SITE
osoft Windows Dev ter and Wireless Ac	ADP-Test		
tphone, PDA, Tabl	Factory		
anaged	POC-ADP		

Select the appropriate Profile from Threat Protection Profile Selector

Click OK, then Save & Close

Click Publish

Publish change to apply change	Publish	
Infoblox 📚 📃 🗖	ashboards	Data Management

Click Publish to apply changes

Click Save & Close

Verifying the Infoblox ADP appliance is working correctly

As a last step in the deployment, we can send a query to the ADP appliance to make sure it's configured as expected. Make sure rule 110100200 is not disabled. To do that, send the following query from a terminal that can reach the ADP appliance,

dig -t txt -c chaos VERSION.BIND @<LAN1-IP-Address>

The expected output is that the server is not going to be reached and the command is going to show the following output upon execution,

dig -t txt -c chaos VERSION.BIND @<LAN1-IP-Address>

; <<>> DiG 9.8.3-P1 <<>> -t txt -c chaos VERSION.BIND @<LAN1-IP-Address>

- ;; global options: +cmd
- ;; connection timed out; no servers could be reached

If you are using nslookup instead of dig, then use the following command,

nslookup -q=txt -class=CHAOS version.bind. <LAN1-IP-Address>

Now go to the Administration > Logs > Syslog

Select the ADP appliance to which the query is sent in Member field.

Dashboards	Data Management	Smart Folde	ers Reportir	ng Grid Admini	stration					
Administrators	s RIR Workflow	Logs	Network Views	Extensible Attributes	Authentication Server Groups	Named ACLs	Reporting			
Audit Log	Syslog Microsoft Log	9								
SysLog	Log Viewer Membe	r software	-adp.localdom	R						
Quick Filter	None \$	Off Filter O	n Show F	ilter 🔚 Toggle multi-li	ne view					
C 1 12	1111010									٩
	TIMESTAMP -	FACILITY	LEVEL	SERVER	MESSAGE					
	2019-08-07 15:49:51 PDT	daemon	CRITICAL	threat-protect-log[9682]	CEF:0linfobloxINIOS Threati8.4. spt=48921 dst=10.61.19.55 dpt=	0-381062111010020 53 act="DROP" cat	00IEARLY DROP UD ="Reconnaissance" r	P DNS named version nat=0 nfpt=0 nlpt=0 f	on attemptsl8lsrc=10.61.1 (qdn=version.bind hit_cour	19.13 nt=1
	2019-08-07 15:49:46 PDT	daemon	CRITICAL	threat-protect-log[9682]	CEF:0IInfobloxINIOS Threatl8.4. spt=48921 dst=10.61.19.55 dpt=	0-381062111010020 53 act="DROP" cat	00IEARLY DROP UD ="Reconnaissance" r	P DNS named version nat=0 nfpt=0 nlpt=0 fe	on attemptsl8lsrc=10.61.1 fqdn=version.bind hit_court	19.13 nt=1

The following log message confirms that query was received and dropped by design and it verified the correct configuration of the Infoblox ADP appliance. You can see it in context above, and the message details below.

CEF:0IInfobloxINIOS Threatl8.4.0-381062I110100200IEARLY DROP UDP DNS named version attemptsl8Isrc=10.61.19.13 spt=48921 dst=10.61.19.55 dpt=53 act="DROP" cat="Reconnaissance" nat=0 nfpt=0 nlpt=0 fqdn=version.bind hit_count=1

SNMP Support

Software ADP supports:

- Existing SNMP threshold traps for software-based ADP platforms
 - Threat Protection Dropped Traffic
 - o Threat Protection Total Traffic
 - Flood Threats
 - Alert Rate
 - Drop Rate
- SNMP trap for rule publish failure for software-based ADP platforms

Review the Security Dashboard for Threat Protection Information

The Security Dashboard is appropriately populated whenever Threat Protection, RPZ, and Threat Analytics services are enabled. The dashboard shows data for last thirty minutes. If data more than 30 minutes is required then go to Reports for that. To review, and explore this dashboard,

Go to Dashboards > Status > Security

Dashboar	ds	Da	ita Ma	inag	emen
Tasks	Statu	s	¢ -		
Default			Secur	ity 🖠	2 -

Security Status for Grid

This widget displays the overall security status for the Grid. The **Security Status for Grid** widget shows the Critical, Major, Warning and Informational events for different security services enabled in the Grid, such as Threat Protection, RPZ and Threat Analytics. Grid manager displays this widget only when at least one member in the Grid has the Threat Protection, RPZ or Threat Analytics license installed.

Da	shboards	Data Management	Smart Folders	Reporting	Grid A	dministration	
Tas	sks Status	¢ -					
C	efault	Security 😂 🗸	SOC Dig				
	Warning Sec	urity Status for Gri	d				
	Data for the pa	st 30 minutes.					
		Status	Events from 7 of 7 se	curity capable m	nembers	Definitions/Rules	Configuration Status
	Threat Protect	Warning	3 Critical 2 Major	0 Warning	50 Informationa	4 hour(s) old	×
	RPZ	ОК	0 Blocked hits 0 Su	ubstituted hits	0 Passthru hits	No Infoblox-specific subscription.	~

Security Status for All Members

The widget Security Status for All Members shows the information about the status of all the Grid members that support ADP and Threat Analytics. At least one member in the Grid must have Threat Protection, RPZ or Threat Analytics licenses for this widget to be present. The green status means no security incident occurred for last 30 minutes.

Overall Status columns shows current overall Status of the members that support Infobiox ADP. The status can be **OK**, **Warning**, **Critical** or **Unknown**.

Go to:	Response Policy Zo	nes Threat Protection	Threat Analytic	cs Members	
=	OVERALL STATUS	MEMBER -	IPV4 ADDRESS	IPV6 ADDRESS	THREAT PROTECTION STATUS
\equiv	OK	v1415-124.tme.infoblox.c	10.61.13.124	fc00:10:61:13::1	ОК
\equiv	ОК	software-adp.localdomai	10.61.19.55		ОК
\equiv	OK	pt1400-123.tme.infoblox.	10.61.13.123	fc00:10:61:13::1	ОК
=	OK	ol-18-19.tme.infoblox.cor	10.61.19.53	fc00:10:61:19::53	ОК
=	OK	ol-18-18.tme.infoblox.cor	10.61.21.53	fc00:10:61:21::53	ОК

Threat Protection Status for Grid

The Threat Protection Status for Grid widget displays the statistical information about the threat protection events triggered on all the members in the Grid that support ADP and Threat Analytics.

To see more detailed view of threat protection status, the **Threat Protection Status for Grid** widget is the place to go. It shows information such as,

- Top 10 Rules hit.
- Top 10 attackers
- Number of events over time broken down to Critical, Major, Warning and Informational
- Top 10 Grid members reporting the events
- Total events by severity

The example screenshots are as follows:









Threat Protection Status for Member

To view the Threat Protection Status for a particular member, go to the Widget **Threat Protection Status for Member.** You can select the Gear Icon, and edit the configuration, and select member.

Critical Threat Protec	tion Status for	Member > s	oftware-adp.lo	caldomain			¢ 🗖 🖂	
Select Member							Configu	ire
Traffic being dropped	O Dial	o Bar						
Traffic being received	🔘 Dial	o Bar						
NIC Settings: LAN1	\$							
Events Over Time:	Critical	🕑 Major	🕑 Warning	🕑 Informati	onal			
				5	Auto Refresh Pe	eriod 20 s	seconds	

Select the member for which you need status on.

The widget now shows the percentage of traffic being received and dropped on LAN1 and LAN2 interfaces and interfaces usage. In addition, it also shows the Security events over time, top 10 rules being hit and the top 10 attackers handled by the appliance.

Critical Threat Protection S	tatus for Member > software-adp	localdomain	◙ጵ₿¢◘⊠
Select Member			
Traffic being dropped	Dial 🧿 Bar		
Traffic being received	Dial 🔿 Bar		
NIC Settings: LAN1	+		
Events Over Time:	Critical 🕑 Major 🕑 Warni	ng 🗹 Informational	esh Period 20 seconds
Summary Events Over Tir	ne Top 10 Rules Top 10 Clients	Interface Usage (LAN1)	
		20 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	20 0 0 100 100
0%	0%	0%	0%
	0 /0	0 /0	0 /0
Traffic being dropped: LAN1	Traffic being dropped: LAN2	Traffic being received: LAN1	Traffic being received: LAN2



Auto Refresh

All widgets mentioned above support auto-refresh. Click the configure icon and select the **Auto Refresh Period** check box in the lower right corner. There you can specify the refresh period in seconds. The default auto refresh period is 30 seconds, the minimum is 5. Click the Configure icon again to hide the configuration panel.

OK Threat Protection	Status for Me	mber > softw	are-adp.localdo	main	ø≈∂¢≧⊠
Select Member					
Traffic being dropped	🔘 Dial	💿 Bar			
Traffic being received	o Dial	🔘 Bar			
NIC Settings: LAN1	\$				
Events Over Time:	Critical	✓ Major	✓ Warning	✓ Informational	
			Z	Auto Refresh Period	a 20 seconds

Viewing Reports

Various reports are available for Threat Protection service, examples below:

Threat Protection Event Count by Category

This report presents event counts based upon category for the selected time period.

	Infoblox 💲 🛛 Dashboards 🛛 Data Manag	gement Smart Folders Reporting	Grid Administration			Q Search admin 👻
Inter Database Report Report <th< th=""><th>App: Infoblox Reporting & Analytics \vee</th><th></th><th></th><th>infoblox-admin</th><th>Messages \lor Settings \lor Activity \lor</th><th>Help 🗸 🛛 Find</th></th<>	App: Infoblox Reporting & Analytics \vee			infoblox-admin	Messages \lor Settings \lor Activity \lor	Help 🗸 🛛 Find
	Home Dashboard Dashboards Reports Alerts	Search Pivot Administration	Reporting Help Quick filter 🗸		Infol	blox Reporting & Analytics
710 emers (MV19 1020000 MV b 19/19 1020000 MV) UN	Threat Protection Event Count b System-created report: Please clone before editing. Last 24 hours ~	by Category			Edit 🗸	More Info 🗸 Add to Dashboard
A00.000 Image: Control Description Image: Control Des	710 events (8/8/19 1:00:00.000 PM to 8/9/19 1:08:24.000 PP	PM)				Job 🗸 🔲 🔲 O 🛓 🖨
1000000 0 </td <td>4,000,000</td> <td></td> <td></td> <td></td> <td></td> <td></td>	4,000,000					
Construction Disk of the construction <thdisk construc<="" of="" td="" the=""><td>3,000,000</td><td></td><td></td><td></td><td></td><td>Critical Event Count Major Event Count Warning Event Count</td></thdisk>	3,000,000					Critical Event Count Major Event Count Warning Event Count
Category °Citical Event CourtsMajor Event CourtsMaring Event CourtsInformational Event CourtsTotal Event CourtsGeneral DDoS <td< th=""><th>1,000,000 DNS Coning Defaul/Drop TCP/U_loads Recons</th><th>nora DHCP BLACK due Botest miles</th><th>THE B. allow MAR. APR</th><th></th><th></th><th>Total Event Count</th></td<>	1,000,000 DNS Coning Defaul/Drop TCP/U_loads Recons	nora DHCP BLACK due Botest miles	THE B. allow MAR. APR			Total Event Count
General DDoS 4 0 0 4 DNS Message Types 0 8 0 0 8 Subscriber Services 0 0 0 14 14 BGP 0 0 0 14 14 BGP 0 0 0 16 16 DNS Amplification and Reflection 36 0 0 38 38 DFD 38 0 0 0 38 38 39 38 39 38 39 39 38 39 38 39 38 39 39 38 39 38 39 <	17 results 20 per page ➤	ande onter softeneordy roteneordand	Category	BFD DNS Malware DNS Action	BCP Subscrvices DNS Mypes Gener.	DDes
DNS Message Types08008Subscriber Services000016BGP00001616DNS Amplification and Reflection3600036DNS Makare38000036DNS Makare3800036DNS Makare3800036DNS Makare3800036DNS Protecol Anomales57400036DNS Protecol Anomales300006697DNS Protecol Anomales00006697DNS Protecol Anomales00000BLACKLIST UDP FROM000000DPCPF Floods0000000DPCPF Floods0000000Default PascDoph0000000Default PascDoph0000000	17 results 20 per page ∽ Category ≎	Critical Event Count 0	Category Major Event Count 0	BPD UNS Malware UNS Action	BCP Subscr., vices DNS M., ypes Cener.	Doos Total Event Count *
Subscriber Services0001414BP0000000DNS Malware38000038DNS Malware38000038BFD0000076NTP0000054DNS Nationalities3800065DNS Nationalities0006574DNS Nationalities3800065DNS Nationalities000669700DNS Nationalities00006697DNS Nationalities000000DNS Nationalities000000DNS Nationalities000000DNS Nationalities000000DNS Nationalities000000DNS Nationalities000000DNS Nationalities0000000DNS Nationalities0000000DNS Nationalities00000000DNS Nationalities0000000000DNS Nationalities<	17 results 20 per page ∽ Category ≎ General DDoS	Critical Event Count 0	Category Major Event Count ©	BPD DNS Malware DNS Acoon Warning Event Count 0	BCP Subscrvices DNS Mypes Cener.	Total Event Count ^
BGP001616DNS Amplification and Reflection3600066DNS Amplification and Reflection3600038DNS Amplification and Reflection3800038DRS Protection000076NTP0000251251DNS Protecci Anomalies432000974DNS Protecci Anomalies0009607767Drector LDD SP Created Domains0009607767Drector LDD SP Created Domains0009607767Drector LDD SP Created Domains00096079607Drector LDD SP Created Domains00096079607Drector LDD SP Created Domains00096079607Drector LDD SP Created Domains0009607Drector LDD SP Create Domains0009607Drector LDD SP Create Domains0009607Drector LDD SP Create Domains000<	17 results 20 per page ∽ Category © General DDoS DNS Message Types	Critical Event Count 0	Category Major Event Count © 0 8	IFD Drs Maiware Drs Adon Warning Event Count 0 0 0	BCP Subscvices Dids M_ypes Cener.	Total Event Count * 4 8
DNS Amplification and Reflection360038DNS Malware3800088BFD000088BFD000067NTP000025ICMP57400094DNS Protoci Anomalies433200006832Potential DDoS related Domains055000006847DKCKLIST UDP FQDN lookup066970006843268432Reconnaissance1039000010344Default PasoDop00010344010344Default PasoDop00015380571538057	17 results 20 per page ~ Category © General DDoS DNS Message Types Subscriber Services	Critical Event Count 0	Category Major Event Count 0 0 8 0	IFD Dris Malakara Dris Adon Warning Event Count 0 0 0 0	BCP Subscrvices Did Mypes Cener.	Total Event Count ^ 4 8 14
DNS Malware 38 0 0 0 38 FP 0 0 0 67 67 NTP 0 0 0 25 25 IGMP 574 0 0 25 25 IGMP 574 0 0 0 482 Potential DDoS related Domains 0 0 0 4822 Potential DDOS related Domains 0 0 0 6697 BLACKLIST UDP FQDN lookup 0 0 0 6697 0 0 6697 DHCP 0 0 0 0 6697 0 0 6697 DFQPD FROOD 0 0 0 0 6697	17 results 20 per page ✓ Category ≎ General DDoS DNS Message Types Subscriber Services BGP	Critical Event Count 2 4 0 0 0	Major Event Count 0 0 8 0 0	IFD Dro Mainaire Dro ACon Warning Event Count 0 0 0 0 0	BCP Subscriccs DIG M_ypes Cener. Informational Event Count © 0 14 16	Total Event Count ^ 4 8 14 16
BFD 0 0 6 6 NTP 0 0 0 25 25 ICMP 574 0 0 0 25 25 DNS Protocol Annales 674 0 0 67 25 DNS Protocol Annales 0 0 0 68 26 27 DNS Protocol Annales 0 0 0 0 68 26 26 27 DNS Protocol Annales 0 0 0 0 0 68 26 <th26< th=""> <th26< th=""> <th26< th=""> <t< td=""><td>17 results 20 per page ∨ Category ≎ General DDoS DNS Message Types Subscriber Services BGP DNS Amplification and Reflection</td><td>Critical Event Count © 4 0 0 36</td><td>Major Event Count o Major Event Count o 0 0 0 0 0 0</td><td>BPD DRS Mainster DRS AClon Warning Event Count 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td><td>BCP Subsrics DIG M_ypes Cener.</td><td>Total Event Count * 4 8 14 16 36</td></t<></th26<></th26<></th26<>	17 results 20 per page ∨ Category ≎ General DDoS DNS Message Types Subscriber Services BGP DNS Amplification and Reflection	Critical Event Count © 4 0 0 36	Major Event Count o Major Event Count o 0 0 0 0 0 0	BPD DRS Mainster DRS AClon Warning Event Count 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	BCP Subsrics DIG M_ypes Cener.	Total Event Count * 4 8 14 16 36
NTP 0 0 251 251 ICMP 574 0 0 574 DNS Protocid Annales 432 0 0 674 DNS related Domains 432 0 0 6832 Potential DOS related Domains 0 6697 0 0 6697 DLCP 0 6697 0 0 6832 6832 Potential DOS related Domains 0 0 0 697 69	17 results 20 per page ✓ Category ≎ General DDoS DNS Message Types Subscriber Services BGP DNS Amplification and Reflection DNS Majiware	Critical Event Count © 4 0 0 36 38	Major Event Count o 0 Major Event Count o 0 0 0 0 0 0	BPD DRS Mainster DRS Aclon Warning Event Count ○ 0 0 0 0 0 0 0 0 0 0	BCP Subscriccs DNS.Mpes Gener. Informational Event Count ○ 0 14 16 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Total Event Count * 4 8 14 16 36 38
ICMP 574 0 0 0 574 DNS Protocol Anomalies 4322 0 0 0 4322 Potential DDoS related Domains 0 5001 0 0 6001 6001 0 6001	17 results 20 per page ✓ Category ≎ General DDoS DNS Message Types Subscriber Services BGP DNS Malware BFD	Critical Event Count © 4 0 0 36 38 0 0	Major Event Count 0 Major Event Count 0 0 0 0 0 0 0 0 0 0	IPD Dris Maiware Dris Aclon	BCP Subscvices DNS M_ypes Cener. Informational Event Count 0 0 14 16 0 0 67	Total Event Count * 4 8 14 16 36 38 67
DNS Protocol Anomalies 4332 0 0 4832 Potential DDoS related Domains 0 5001 0 0 5001 BLACKLIST UDP FQDN lookup 0 6697 0 0 6697 DHCP 0 0 0 6832 68393 Preconnaissance 1039 0 0 10399 TOP/UDP FRods 0 0 101494 Default Pass/Drop 0 0 1538067	17 results 20 per page ✓ Category ≎ General DDoS DNS Message Types Subscriber Services BGP DNS Amplification and Reflection DNS Malware BFD NTP	Critical Event Count 5 4 0 0 36 38 0 0 0	Major Event Count o Major Event Count o 0 0 0 0 0 0 0 0 0	IPD Dris Maiware Dris Adon Warning Event Count 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	80P Subsrvices Dids Kpes Cener. Informational Event Count ≎ 0 14 16 0 0 0 14 16 0 0 0 251	Total Event Count * 4 8 14 16 36 38 67 251
Potential DboS related Domains 0 5001 0 0 5001 BLACKLISTUDP FQDN lookup 0 6697 0 0 6697 0 0 6697 0 0 6697 0 0 6697 0 0 6697 0 0 6697 0 0 6697 0 0 6697 0 0 6697 0 0 6697 0 0 6697 0 0 6697 0 0 6697 0 0 6697 0 0 6697 0 0 6697 0 0 6697 0 0 0 6697 0	17 results 20 per page ✓ Category ≎ General DDoS DNS Message Types Subscriber Services BBOP DNS Amplification and Reflection DNS Malware BFD NTP ICMP	Critical Event Count 2 4 0 0 0 36 38 0 0 574	Major Event Count o Category	BPD DRS Mainster DRS Aclon Warning Event Count 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	80P Subscstos Di8 Kypes Cener. Informational Event Count © 0 0 14 16 0 0 0 67 251 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Total Event Count * 4 8 14 16 16 36 38 67 251 574
BLACKLIST UDP FQDN lookup 0 6697 0 0 6697 DHCP 0 0 0 8432 8432 Reconnaissance 10389 0 0 0 0389 TDY/UDP Floods 0 0 0 10149 Default Paso/Dop 0 0 1538067 1538067	17 results 20 per page ✓ Category © General DDoS DNS Message Types Subscriber Services BGP DNS Amplification and Reflection DNS Mailware BFD NTP ICMP DNS Protocol Anomalies	Critical Event Count © 4 0 0 36 38 0 0 0 574 4832	Major Event Count o Category Major Event Count o 0 0 0 0 0 0 0 0 0	BPD DRS Mainster BRS Aclon Warning Event Count 0 0 0 0 0 0 0 0 0 0 0 0 0	80 ⁰ Subsrics Diskpes Gener. Informational Event Count ○ 0 0 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0	Total Event Count * 4 8 1 1 1 1 5 6 7 2 5 1 6 7 4 4 8 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
DHCP 0 0 8432 8432 Reconnaissance 10389 0 0 0 10389 TCP/UDP Floods 0 0 100149 0 100149 Default Pass/Drop 0 0 0 1538067 1538067	17 results 20 per page ✓ Category ≎ General DDoS DNS Message Types Subscriber Services BGP DNS Amplification and Reflection DNS Malware BFD NTP ICMP DNS Protocol Anomalies Potential DDoS related Oomains	Critical Event Count © 4 0 0 36 38 0 0 574 4332 0 0	Major Event Count o Category	■PD DNS Mainstar DNS Aclon Warning Event Count 0 0 0 0 0 0 0 0 0 0 0 0 0	80 ^P Subsricis Diskpes Gener. Informational Event Count ○ 0 14 16 0 0 0 14 16 0 0 0 0 0 0 0 0 0 0 0 0 0	Total Event Count ↑ 4 8 14 16 36 38 67 251 574 4832 5001
Reconnaissance 10389 0 0 10389 TCP/UDP Floods 0 0 100149 0 100149 Default Pass/Drop 0 0 0 1538067 1538067	17 results 20 per page ∨ Category © General DDoS DNS Message Types Subscriber Services BGP DNS Amplification and Reflection DNS Malware BFD NTP ICMP ICMP DNS Protocol Anomalies Potential DDoS related Domains BLACKLIST UDP FGON lookup	Critical Event Count 5 4 0 0 0 0 36 38 0 0 574 4332 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Ansream Surger Category Category 0 Category	BPD DNS Mainsairs DNS Adoen Warning Event Count ○ 0 0 0 0 0 0 0 0 0 0 0 0 0	80 ^P Subsrics Di8Kpes Gener. Informational Event Count ≎ 0 14 14 16 0 0 0 0 0 0 0 0 0 0 0 0 0	Total Event Count ▲ 4 8 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
TCP/UDP Floods 0 100149 0 100149 Default Pass/Drop 0 0 0 1538067 1538067	17 results 20 per page ✓ Category ≎ General DDoS DNS Message Types Subscriber Services BBOP DNS Amplification and Reflection DNS Malware BFD NTP ICMP ICMP DNS Protocol Anomalies Potential DDoS related Comains BLACKLIST UOP FQON lookup DHCP	Critical Event Count 5 4 0 0 0 0 36 38 0 0 574 4332 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Category Cat	IFO DRS Addedse Warning Event Count ○ 0	BCP Subscrstors DNB M_uppes Cener. Informational Event Count 0 0 0 0 0 0 0 0 14 16 0	Total Event Count * 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5
Default Pass/Drop 0 0 0 1538067 1538067	17 results 20 per page ✓ Category ≎ General DDoS DNS Message Types Subscriber Services BBOP DNS Amplification and Reflection DNS Mailware BFD NTP ICKMP DNS Protocol Anomalies Potential DDoS related Domains BLACKLIST UDP FQDN lookup DHCP Reconnaissance	Critical Event Count 2 4 4 0 0 36 38 0 0 38 0 0 574 4832 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Major Event Count 0 Category Major Event Count 0 0 0 0 0 0 0 0 0 0 0 0 0 0	IPD DNS Mainstrat DNS Aclon Warning Event Count 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	80 ⁹ Subsrics Di8Kpes Gener. Informational Event Count ○ 0 0 0 0 0 0 0 0 0 0 0 0 0	Total Event Count * 4 4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5
	17 results 20 per page ✓ Category C General DDoS DNS Message Types Subscriber Services BGP DNS Amplification and Reflection DNS Mailware BFD NTP ICMP DNS Protool Anomalies Potential DDoS related Domains BLACKLIST UDP FQON lookup DHCP Reconnaisance TCP/UDP Floods	Critical Event Count © 4 0 0 0 38 38 0 0 574 4832 0 0 0 0 0 0 0 0 0 0 0 0 0	Ans room of the second se	IPD DNS Mainster DNS Aclon Warning Event Count 0 0 0	80 ⁹ Subsrics Diskpps Cener. Informational Event Count ○ 0 0 1 1 1 1 0 0 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0	Total Event Count ↑ 4 8 14 16 95 38 67 251 574 4832 5001 6697 8432 10389 100149
DNS Cache Poisoning 0 0 3313960 0 3313960	17 results 20 per page ∨ Category © General DDoS DNS Message Types Subscriber Services BGP DNS Amplification and Reflection DNS Malware BFD NTP ICMP DNS Protocol Anomalies Potential DDoS related Domains BLACKLIST UDP FOON lookup DHCP Reconnaissance TCP/UDP Floods	Critical Event Count 5 4 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Ansreams American and Americ American and American and Am	IPD DNS Aussurg DNS ACon 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	80 ⁹ Subsrics Diskps Cener. Informational Event Court € 0 1 1 1 1 1 1 1 1 1 1 1 1 1	Total Event Count ▲ 4 8 14 16 36 38 67 251 574 482 5001 6697 8832 10389 109149 1538067

Threat Protection Event Count by Member

This report shows the event count by member based upon severity.

Infobiox 📚 🛛 Dashboard	is Data Management Sn	nart Folders Reporting	Grid Administration		Q Search admin 👻
App: Infoblox Reporting & Analytics \vee			infoblox-admin Messages 🗸	Settings \sim Activity \sim Help \sim	Find
Home Dashboard Dashboards R	eports Alerts Search	Pivot Administration	Reporting Help 🛛 Quick filter 🗸	r Infoblox F	eporting & Analytics
Threat Protection Eve System-created report: Please clone before Last 7 days ~ < 4,210 events (8/2/19 1:00:00.000 PM to 6,000,000	nt Count by Mem editing. 8/9/19 1:16:43.000 PM)	iber		Edit V More Ir Job V	II = O ± Č
4,000,000 2,000,000 software-adp.localdomain 5 results 20 per page ~	ol-18-18.tme.infobiox.com	pt1400–123.tme.infoblo Member	x.com ol-18-19.tme.infoblox.com	ol-18-123.tme.infoblox.com	Critical Event Count Major Event Count Warning Event Count Informational Event Count Total Event Count
Member 0	Critical Event Count	Major Event Count	Warning Event Count 0	Informational Event Count 0	Total Event Count 0
software-adp.localdomain	15914	11769	3143369	1801722	4972774
ol-18-18.tme.infoblox.com	25	0	270741	8	270774
pt1400-123.tme.infoblox.com	0	0	0	108751	108751
ol-18-19.tme.infoblox.com	0	6	0	14	20
ol-18-123.tme.infoblox.com	7	3	0	0	10

Threat Protection Event Count by Rule

The report displays the event rule hits sorted by the total event count.

App: Infoblox I	Reporting & Analytics \smallsetminus			- W	infoblox-admin	Messages \vee	Settings \vee	Activity \vee	Help \sim	Find	
Home Dasht	board Dashboards	Reports Alerts	Search Pivo	t Administration	Reporting Hel	p Quick fi	lter 🗸	Inf	foblox Re	eporting 8	& Analytics
Threat System-crea	t Protection Ev ated report: Please clone be ainutes ~	rent Count b	y Rule					Edit 🗸	More Info	o√ Add	o Dashboard
✓ 16 events	(8/9/19 1:06:23.000 PM to	8/9/19 1:21:23.000 PM)						Job 🗸 🛛 🛛	0	¥ .
00,000											
										E	ent Name
0 results	40000600 13090600 20 per page ~	1 ' 120303001 '	130400100 1	30800800 ['] 2000 SID	01100 11010	0900 11	0100600	130910100	1309061		ent Name ert Count op Count otal Event Cou
0 results	40000600 13090600 20 per page ~	1 120303001	130400100 1	30800800 2000 SID	01100 11010	0900 11	0100600	130910100	Alert	Drop Count	Total Even
00,000 14 0 results SID 0 140000600	40000600 13090600 20 per page ~ Category © Default Pass/Drop	1 120303001 Log Severity © INFORMATIONAL	130400100 1 Event Name © DROP UDP unexpr This rule drops all	30800800 2000 SID	01100 11010	0900 11	0100600	130910100	13090610 Alert Count ≎ 0	D1	Total Even Count otal Event Cou
14 0 results SID 0 140000600 130906001	40000600 13090600 20 per page ✓ Category ≎ Default Pass/Drop DHCP	1 120303001 Log Severity © INFORMATIONAL	130400100 1 Event Name © DROP UDP unexpr This rule drops all DROP IPv4 DHCP This rule drops an	30800800 2000 SID intered unexpected UDP pack unexpected IPV4 DHI	01100 ¹ 11010 ets. CP packets when II	0900 ['] 11	0100600 '	130910100	13090610 Alert Count ≎ 0 0	D1	Total Even 277334
00,000 14 0 results SID 0 140000600 130906001 120303001	40000600 13090600 20 per page ~ Category © Default Pass/Drop DHCP BLACKLIST UDP FQDN lookup	1 120303001 Log Severity © INFORMATIONAL INFORMATIONAL MAJOR	130400100 1 Event Name © DROP UDP unexp This rule drops all DROP IPv4 DHCP This rule drops an Blacklistfoo.foo.fo A custom rule tem	30800800 2000 SID cted unexpected UDP pack unexpected r unexpected IPv4 DHI io plate that you use to a	01100 11010 ets. CP packets when II	224 DHCP is d	0100600	130910100	13090610 Alert Count ○ 0 0 0 0	D1 Drop Count © 270334 77 43	Total Even Count Total Even Count 27033 77 4
00,000 14 0 results SID © 140000600 130906001 120303001 130400100	40000600 13090600 20 per page ~ Category © Default Pass/Drop DHCP BLACKLIST UDP FQDN lookup DNS Amplification and Reflection	1 120303001 Log Severity 0 INFORMATIONAL INFORMATIONAL MAJOR CRITICAL	130400100 1 Event Name © DROP UDP unexp This rule drops all DROP IPv4 DHCP This rule drops all Blacklistfoot of of A custom rule tem WARN & DROP DO This rule first war reflection/amplific	30800800 2000 SID cted unexpected UDP pack unexpected IPv4 DHI io plate that you use to a S DNS possible reflect s if any source IP sen ation attacks.	01100 11010 ets. CP packets when II llow blacklisting Fri tion/amplification a ds UDP DNS packet	20900 11	0100600 isabled. n UDP. s possible	130910100	13090610 Alert Count ≎ 0 0 0 4	Drop Count 0 270334 77 43 25	Total Even Count Total Even Count 27033 77 42 21

Threat Protection Event Count by Severity Trend

The report displays the number of threat protection events broken down by severity.



Threat Protection Top Rules Logged

The report is based on frequently hit rules and while displaying the top sources IP address.



Threat Protection Top Rules Logged by Source

The source IP addresses with the highest logged event count are presented with the top rules that the address has hit.

Infoblox 📚	Dashb	oards Da	ata Manageme	ont Sma	rt Folders	Reporting	Grid	Administ	ration							Q Search	ad	imin 🤜
App: Infoblox Reportin	g & Analytics \vee					-85	infoblox-adr	nin M	essages 🗸	Settings <	- Ac	tivity \sim	Help \sim	E	nd			
Home Dashboard	Dashboards	Reports	Alerts	Search	Pivot	Administration	Reporti	ng Help	Quick fil	ter 🗸		Int	foblox	Repo	orting	& Ana	lytic	s
Threat Pro System-created repo Custom time ~	tection To rt: Please clone be	op Rule efore editing.	es Logo	ged by	Sourc	ce					3	Edit 🗸	More	Info 🗸	Ad	d to Dashi	ooard	
2,307 events (8/2/	19 1:27:40.000 PN	A to 8/9/19 1	:27:40.000 PM	A)									Job 🗸	Ш	• •	9	L e	5
60,000 40,000 20,000 10 results 20 per	, 10.61.19.13:[0- page ∽	-0] ⁺ 10.61.21.	13:[0-0] / 131.1	17697:[0-0]	¹ 79.199.2¢	4:[0-0] [↑] 94.33.88. Source	192:[0-0] ^{-'} fe80:	:be173:[0-0] 101.184	37.[0-0] 10	13.231	91:[0-0] 10	94.17611	:[0-0]	Lo To La	gged Eve p Rules st Active	nt Co	ount
Source 0			Logged Eve	ent Count 0	Top Rule	s ¢								Last	Active			
0.0.0.0:[0-0]				50314	1309060 DROP IP	00 /4 DHCP unexpe	cted							08/09	9/2019	13:18:51		
10.61.19.13:[0-0]				3441	Blacklist: EARLY DI Potential	foo.foo.foo ROP UDP DNS n DDoS related do	amed version omain: ontrees	attempts .com	5					08/09	9/2019	13:09:44		
10.61.21.13:[0-0]				37	EARLY DI EARLY DI EARLY P/	ROP UDP DNS n ROP UDP DNS n ASS UDP respon	amed author amed version se traffic	attempts attempts	5					08/08	8/2019	15:53:09		

Threat Protection Event Count by Member Trend

This report displays number of threat protection events by each ADP member.

Infoblox 📚	Dashboards	Data Management	Smart Folders Report	ng Grid Administration		Q Search admin
App: Infoblox Reportin	g & Analytics 🗸			infoblox-admin Messages	✓ Settings ✓ Activity ✓ He	lp ~ Find
Home Dashboard	Dashboards Rep	orts Alerts Se	earch Pivot Administr	ation Reporting Help Quic	rfilter ∽ Infob	lox Reporting & Analytics
Threat Pro System-created repo Last 2 months ~	tection Even rt: Please clone before e	t Count by N diting.	Nember Trend		Edit 🗸	More Info 🗸 Add to Dashboard
√ 49,761 events (6/1	/19 12:00:00.000 AM to	8/9/19 2:08:24.000 PM)		Jo	b∨ II III O ⊥ 🖷
4,000,000 2,000,000 Sat Jun 1 2019			Tue jul 23 time		Tue Aug 6	ol-18-18.tme.infoblox.com ol-18-19.tme.infoblox.com pt1400-123.tme.infoblox.com software-adp.localdomain v1415-124.tme.infoblox.com
			_time			
32 results 20 per	page 🗸					<prev 1="" 2="" next=""></prev>
_time 🗸	ol-18-18	3.tme.infoblox.com 0	ol-18-19.tme.infoblox.com	pt1400-123.tme.infoblox.com	 software-adp.localdomain 	v1415-124.tme.infoblox.com 0
2019-08-09				26.	93 39026.21	
2019-08-08		67691.5		26.	96 28358.74	
2019-08-07		8.0	6.6	26.	84 4.8	
2019-08-06				20	5.8	

Threat Protection Top Rules Logged by Source

This shows the IP addresses that have the highest number of rule hits.

Infoblox 📚	Dashbo	oards D	ata Manageme	ent Smai	rt Folders	Reporting	Grid	Administr	ration						Q Search	admin
App: Infoblox Reportin	ng & Analytics 🗸						infoblox-a	dmin M	essages ~	Settings	Activity	/~ Не	elp ~ [Find		
Home Dashboard	Dashboards	Reports	Alerts	Search	Pivot	Administration	Repor	ting Help	Quick fi	ter 🗸		Infob	lox Re	portin	g & Ana	llytics
Threat Pro System-created report Last 1 week ~	tection To ort: Please clone be	op Rule	es Log <u>o</u>	ged by	Sourc	ce					E	dit 🗸	More Info	~ A	dd to Dash	board
✓ 2,307 events (8/2/	/19 2:38:37.000 PM	1 to 8/9/19 2	:38:37.000 PM	A)								Jo	b~ II	-	0.	¥ ð
60,000																
40,000 - 20,	10.61.19.13:(0-	0] 10.61.21	13:[0-0] 131.3	17697.[0-0]	79.199.20	4:[0-0] 94.33.88.1 Source	192:[0-0] ['] fe8	0::be173:[(0-0] 101.184	37:[0-0] ¹ 10	3.23191:[0-	0] 104.17	′611:[0-0	L T L	ogged Eve Top Rules ast Active	ent Count
Source 0			Logged Eve	ent Count 0	Top Rules	s ¢							La	st Active	0	
0.0.0.0:[0-0]				50314	13090600 DROP IPv	00 /4 DHCP unexpe	cted						08	/09/201	9 14:28:44	
10.61.19.13:[0-0]				3441	Blacklist: EARLY DF Potential	foo.foo.foo ROP UDP DNS na DDoS related do	amed versio main: ontre	n attempts es.com					08	/09/201	9 13:09:44	
10.61.21.13:[0-0]				37	EARLY DE EARLY DE EARLY PA	ROP UDP DNS na ROP UDP DNS na ASS UDP respons	amed autho amed versic se traffic	r attempts n attempts					08	/08/201	9 15:53:09	
131.176.108.97:[0-0]				34	DROP BF	D packets when	BFD is disa	bled					08	/09/201	9 13:09:44	
79.199.229.104:[0-0]				30	EARLY DE	ROP UDP query i ROP UDP query r	nvalid ques nultiple que	tion count stions or n	on query op	eration code			08	/09/201	9 13:09:44	

Logging

By default, when a DNS attack is detected against an enabled rule, the appliance generates a log message. These threat protection messages are displayed in CEF (Common Event Format).

The number of log messages generated is based on the 'Event per Second' setting in each rule. For example, if the setting is 5, the appliance generates maximum of five log messages of the same event per second per client when a rule is hit within the time duration. Following is a sample CEF log message for a ADP rule hit event,

2019-08-09 12:46:35 PDT daemon ERROR threat-protect-log[6524] CEF:0|Infoblox|NIOS Threat|8.4.4-386831|120601966|Potential DDoS related domain: ontrees.com|7|src=10.61.19.13 spt=51460 dst=10.61.19.55 dpt=53 act="DROP" cat="Potential DDoS related Domains" nat=0 nfpt=0 nlpt=0 fqdn=ontrees.com hit_count=4981

This log contains the following information:

- The timestamp when the event happened in yyyy-mm-ddThh:mm:ss+00:00 format.
- Infoblox/NIOS Threat/x.x.x: Indicates the Infoblox product, and x.x.x represents the NIOS version.
- The number following the NIOS version is the rule ID. In this example, it is 120601966.
- Following the rule ID is the rule name specified in the rule. In this example it is "Potential DDoS related domain: ontrees.com"
- The number following the rule ID is the log severity. The following numbers indicate the severity levels:
 - 8 = Critical

- 7 = Major
- \circ 6 = Warning
- 4 = Informational
- src: Source IP address
- spt: Source port.

•

- dst: Destination IP address.
- dpt: Destination port.
- act: The rule action, which can be ALERT, DROP, or PASS, depending on the rule configuration.
- cat: The rule category to which the rule belongs. In this example, the rule category is "Potential DDoS related Domains
- nat: Indicates if the syslog event is logged for a NAT'ed client. In this example, nat=0 means that it's not a NAT'ed client.
- nfpt: Indicates the first port in the port block if syslog is for NAT'ed client.
- nlpt: Indicates the last port in the port block if syslog is for NAT'ed client.
- fqdn: Indicates the FQDN that was queried by the client
- hit_count: Indicates the number of rule hits

The logs for Infoblox Advanced DNS Protection appliance can be viewed by going to;

Administration > Logs > Syslog

Select the appropriate member from the **Member** drop down menu.

Dashboards	Data Ma	nagement	Smart Fo	iders Reporting	Grid	Administ	tration			
Administrators	RIR	Workflow	Logs	Network Views	Extensible	Attributes	Authen	tication Server Groups	Named ACLs	Reporting
Audit Log	Syslog	Microsoft Log)							
SysLog	Log View	ver Membe	r softw	are-adp.localdom	R					

To view Threat Protection logs, click on Show filter

SysLog	Log Viewer	Member	software-adp	localdom 🚩	A	
Quick Filter	[S] - Threat Deter	st 🛊 🛛 💽	Filter Off	Show Filt	er	Toggle single line view
C 1 12 1		•				

Select the values of the filter fields as "Server equals Threat Protection" shown in the screenshot below,

SysLog Log Viewer Member softwa	re-adp.localdom 🗡 🚦		
Quick Filter None	Off Hide Filter 🔚 Toggle single line view		
Server ÷	equais 🛟	Threat Protection \$	+ Apply Save Reset
C' ⇔ ≰ ≦ ⊠ ⊖			Q 4

To only view CEF messages logged for Threat Protection Rules hit,

select **Threat Detection Event Logs** from Quick Filter drop down menu, after selecting the appropriate member in Syslog,

riddit Log	Syslog	Microsoft Log					
SysLog	None [S] - RPZ Inc [S] - Threat / [S] - Threat I	cident Logs Analytics Module Rule Update Eve	e Update Events ents	s Logs	R		
Quick Filt	[S] - Threat [[S] - DNS In [S] - DNS T	Detection Event tegrity Check Di	Logs screpancy Logs	pw F	Filter 🗮 T	oggle single line vi	ew
C 17	[S] - All Outb [G] - Cleane	bound API Logs					
	TIMESTAMP V	r	FACILITY	LEVEL	SERVER	N	IESSAGE
Audit Log SysLog	Syslog Log View	Microsoft Log ver Member	software-ad	ip.localdom	R		
Audit Log SysLog Quick Filter	Syslog Log View	Microsoft Log ver Member Detect 🗘 📔	software-ad	ip.localdom ¥	IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	oggle single line vie	w

Click Apply

The filters can be used to view different levels of log messages, such as CRITICAL, ALERT, INFO etc.

The critical messages can be viewed by setting the filter settings as shown in the screenshot below,

Audit Log	Syslog Microsoft Log	1				
SysLog	Log Viewer Member	r software	-adp.localdom	* ¤		
Quick Filte	er None 🛟	On Filter Of	f Hide F	ilter 🔚 Toggle single line	view	
Server	÷		equ	uals 🛟	CRITICAL ¢	+ - Apply Save + - Reset
C 12	11100					Q 4 +
	TIMESTAMP 👻	FACILITY	LEVEL	SERVER	MESSAGE	
	2019-08-09 13:10:00 PDT	daemon	CRITICAL	threat-protect-log[6524]	CEF:0IInfobloxINIOS Threatl8.4.4-386831110100600IEARLY DROP UDP que dst=10.61.19.55 dpt=53 act="DROP" cat="DNS Protocol Anomalies" nat=0 nfp	ry invalid question countl8Isrc=6.28.226.249 spt=14887

A DNS amplification attack is a reflection-based distributed denial of service (DDoS) attack.

The attacker spoofs client requests to DNS servers to hide the true source of the attacker and direct the response to the client. Using various techniques, small DNS queries may be turned into a much larger payload directed at the target network. The following log message has rule id of 130400100. This rule first warns if any source IP sends UDP DNS packets that contain possible reflection/amplification attacks.

2019-08-09 15:05:45 PDT daemon CRITICAL threat-protect-log[6524]

CEF:0IInfobloxINIOS Threatl8.4.4-3868311130400100IWARN & DROP DoS DNS possible reflection/amplification attack attemptsI8Isrc=10.61.19.13 spt=33921 dst=10.61.19.55 dpt=53 act="DROP" cat="DNS Amplification and Reflection" nat=0 nfpt=0 nlpt=0 fqdn=www.whitehouse.gov hit_count=33

In order to view the rule that is being hit to generate the above log message,

Go to Data Management > Security > Threat Protection Rules

Click on the Active ruleset for the Grid and in Go to field type the rule id 130400100. Click Go

Dashb	oards	Data Management	Smart Folders	Reporting	Grid Adm	inistration			
IPAM	VLAN	ls Super Host	DHCP DNS	File Distributio	n Security	Threat Analytics			
Threa	at Protecti	on Rules Members	Profiles						
Threat Vers	Protection	n Rules Home 190731-9 Thr	reat Ruleset 💉 🚦	1					
Quick	Filter No	ne 💌	off Filter On	Show Filter	Toggle Flat Vie	w			
+1	c	11 B						Go to 130400	100 Go
	Ξ			0	RDER 🔺	RULE ID	RULE PARAMETERS		RULE NAME
	=	BLACKLIST UDP FQD	IN lookup for DNS Me	essage Type					
	Ξ	DHCP							
-	=	DNS Amplification and	Reflection						
	=			24	493	130400100	Packets per second Drop interval Events per second Rate algorithm	5 5 1 Rate_Limiting	WARN & DROP DoS DN
	Ξ			24	497	130400500	Packets per second Drop interval Events per second Rate algorithm	500 5 1 Rate_Limiting	RATELIMIT PASS UDP [
	Ξ			24	498	130400600	Packets per second Drop interval Events per second Rate algorithm	500 5 1 Rate_Limiting	RATELIMIT PASS UDP (

The following log message is generated when ADP receives large ICMP ping packet.

2019-08-09 09:39:00 PDT	daemon	CRITICAL	threat-protect-log[9682]	CEF:0IInfobloxINIOS Threatl8.4.0-381062I130400200IDROP ICMP large packetsl8Isrc=10.61.19.13 spt=8 dst=10.61.19.55 dpt=0 act="DROP" cat="ICMP" nat=0 nfpt=0 nlpt=0 fqdn=(null) hit_count=3
-------------------------	--------	----------	--------------------------	---

The following log message is generated when ADP receive drops request to a malicious domain.

2019-08-09 09:38:24 PDT daemon	CRITICAL	threat-protect-log[9682]	CEF:0IInfobloxINIOS Threatl8.4.0-381062I130300400IDROP MALWARE possible Hilotii8Isrc=10.61.19.13 spt=60334 dst=10.61.19.55 dpt=53 act="DROP" cat="DNS Malware" nat=0 nfpt=0 nlpt=0 fqdn=9charname.cmd_exe hit_count=6
--------------------------------	----------	--------------------------	---

Troubleshooting & FAQ

Some common issues and their resolution are discussed in this section.

Unable to download Threat Protection Rules

You may encounter a situation where the ADP appliance is not able to download threat protection rules from ts.infoblox.com. The troubleshooting steps are as follows,

- Make sure the Grid can resolve the hostname ts.infoblox.com.
 - A Resolver must be configured for the Grid so that any member involved can resolve the hostname. (Please see **Enabling DNS resolver** section)
- Make sure the Grid can reach the server ts.infoblox.com.
 - Check to see if any firewall rule is blocking the path to https.
 - Check the proxy setting if applicable.

Trouble joining the Grid

If you are having trouble joining a member to the Grid, here are things to look at;

- Member type (Make sure the right member type is selected)
 - Infoblox for physical PT Appliances, and TE Appliances for Software ADP.
 - Virtual NIOS for Virtual TE-Appliances for Software ADP.
- Enable VPN on MGMT Port has been checked in Grid Member Properties Editor > Network > Advanced
- Make sure the member can ping the Grid Master and verify the firewall is not restricting any access. For reference, check the NIOS Administration Guide.
- Make sure that you have enable MGMT on the member to join and that MGMT IPs match on member local configuration & grid provisioned member configuration.

Different rulesets for different ADP appliances

Question

How can I create two rulesets in ADP? one for external ADP appliances and the other for internal ADP appliances? Both sets need to be tuned differently so I need to apply different tuning to different appliances.

Answer

Best practice is to use ADP Profiles.

Trouble Starting Threat Protection Service

- The Member cannot be a Grid-Master unless it is a Grid of one.
- The Threat Protection Service may not start.

Understanding a CEF Log message

Please see Logging section in this deployment guide to be able to read the contents of a CEF log message.

Outbound API

The Infoblox Outbound API can send outbound notifications to Syslog, DXL (Data Exchange Layer), and REST API endpoints. The ADP *event_type* can trigger on events like: Hits Count, Member IP, Member Name, Query FQDN, Rule Action, Rule Category, Rule Severity, SID, and Source IP. This will notify any solution that will accept indicators that can be acted upon.

These notifications can do a myriad number of things, like triggering client remediation with endpoint security solutions, integration with SOAR solutions, create SOC events, trigger DDoS mitigations, and even opening Service Now tickets. These notifications are vendor neutral.

To use the Outbound API, a Security Ecosystem License is required

Please defer to the NIOS 8.4 Documentation for details on the Infoblox Outbound API. At https://docs.infoblox.com, search for "Outbound Notification Overview"



in

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054 +1.408.986.4000 | info@infoblox.com | www.infoblox.com

© 2019 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).