



STARTER KIT

Infoblox DNS Firewall for FireEye

Introduction

Infoblox DNS Firewall integration with FireEye Malware Protection System delivers a unique and powerful defense against Advanced Persistent Threats (APT) for business networks. This solution combines the power of FireEye APT detection and Infoblox DNS level blocking and device fingerprinting -- to detect and disrupt APT malware communication and help pinpoint infected devices attempting to access malicious domains. This is the first and only solution in the marketplace that invokes powerful DNS level control upon FireEye APT detection events. The joint solution enables customers to **detect** APT's, leverage DNS to **disrupt malware communication** and **pinpoint** infected devices for improved response time and faster remediation.

Customers who have Infoblox DNS infrastructure and FireEye appliance can avail these benefits with a license upgrade.

Customers who do not have Infoblox DNS servers and do have the FireEye appliance can configure their existing DNS servers to forward traffic over to Infoblox server with the DNS Firewall-FireEye Adapter. The FireEye appliance will be configured to provide an APT alert feed to the Infoblox server with DNS Firewall -FireEye Adapter. The purpose of this document is to provide configuration steps.

Infoblox's FireEye Starter Kit allows network administrators to integrate the existing DNS infrastructure with the FireEye appliance. The starter kit consists of:

- Infoblox TrinziC 1420 Network Services Appliance or Infoblox TrinziC 2220 Network Services Appliance
- DNS Firewall software
- FireEye Adapter software

The Infoblox DNS Firewall-FireEye Adapter:

- Automatically blocks detected APTs (Advanced Persistent Threats) based upon updates from the FireEye appliance
- Provides flexible policy enforcement for APT-malware-based DNS queries
- Identify infected devices by IP address, MAC address, DHCP fingerprint, and host name (if configured)
- Reporting of malicious domains and IP addresses via Infoblox Reporting server.

This feature saves time and money in safeguarding the customer's network and confidential information.

The following is the flow of this document:

- Background
- Audience
- Description of a network with the FireEye appliance and DNS server or DNS server farm
- Description of a network with a FireEye appliance communicating with the Infoblox TrinziC Network Services Appliance that is running the DNS Firewall-FireEye Adapter.
- Steps and screens shots to show how to configure the Infoblox appliance, Microsoft DNS server, and FireEye appliance to communicate with each other.



- Verification of the configuration on the Infoblox DNS Firewall-FireEye Adapter, the FireEye appliance, and Microsoft DNS server.
- Reporting of FireEye events
- Ordering Information
- Conclusion

After reading this document, the customer will be able to successfully implement the Infoblox/FireEye APT mitigation solution.

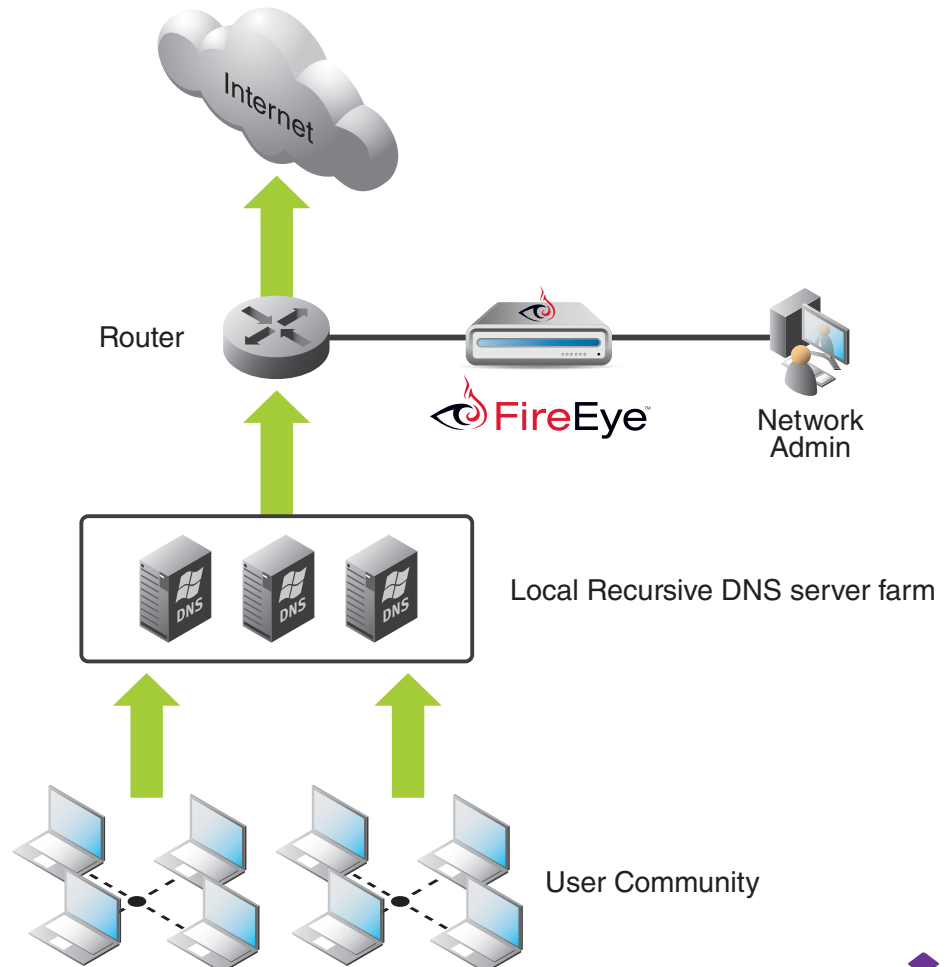
Background

Customers that have the FireEye solution installed find that it is a fine product for detecting APT (advanced persistent threats). When detection is recognized, the person monitoring the FireEye appliance will work on creating and implementing a rule on their firewall to block the APT. This workflow helps in safeguarding the customer's network and confidential information.

Audience

This document is written for customers with the FireEye appliance and non-Infoblox DNS servers.

Existing Malware Detection/Mitigation Environment

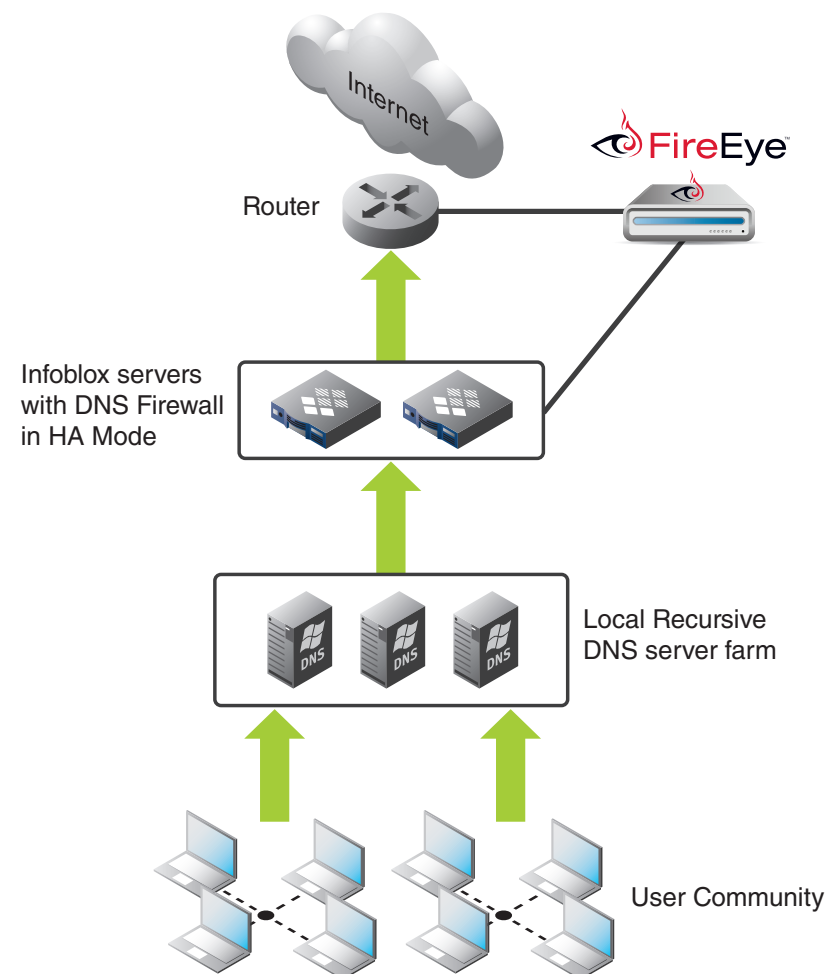


The existing network shows packet flow and workflow as it pertains to APT detection/mitigation:

- An infected device is brought into the office. Upon connection, the malware sends traffic onto the network.
- Customer has Microsoft DNS server or other DNS server vendor with the FireEye appliance in the network.
- Malware infected and non-infected clients send requests to the Microsoft DNS server for DNS resolution.
- A network engineer monitors the FireEye appliance.
- When an APT alert is posted and recognized by the network engineer, the network engineer will create a firewall rule to block the intrusion.

In this scenario, too much time is lost between the detection and mitigation of the APT.

New Malware Detection/Mitigation Environment



This new network shows the packet flow and workflow as it pertains to APT detection/mitigation:

- The malware-infected and non-infected clients will continue to send DNS requests to the current DNS server.
- The current DNS server will send requests to the Infoblox DNS Firewall-FireEye Adapter if it is unable to resolve the DNS name.

- The Infoblox DNS Firewall server will have FireEye Adapter services enabled with a special FireEye RPZ (response policy zone) configured.
- The FireEye appliance will send periodic updates to the Infoblox FireEye Adapter.
- The Infoblox DNS Firewall appliance will add each update as a policy/rule.
- When the DNS Firewall receives a DNS response, the response will be manipulated according to the settings (ex. None, passthru, block (no data), block (no such domain), or substitute domain).
- When an event is marked as an APT from FireEye, the Infoblox DNS Firewall server will block the DNS response if configured accordingly.

Best Practices for FireEye Integrated RPZs

Before you configure a FireEye integrated RPZ, consider the following:

- FireEye integrated RPZs inherit default values from local RPZs. You can create, edit and delete rules using the GUI, PAPI, and RESTful API.
- To avoid false positives, Infoblox recommends that you create a whitelist of allowed zones using a local RPZ that is sorted above the FireEye RPZ. This list should contain popular domains, such as Alexa 250, and other desired domains.
- When a new FireEye alert is mapped to an RPZ rule, it increases the object count in the database, which might have an impact on the storage capacity. Note that the processing of alerts will consume a few CPU cycles, which will have some impact on the system.
- You must properly configure the settings on a FireEye appliance. NIOS supports only Per Event delivery mechanism and JSON Normal message format. To ensure that the NIOS appliance process alerts properly, configure the FireEye appliance accordingly. For more information about alerts, refer to the Infoblox NIOS Administrator guide.
- You cannot add a FireEye integrated RPZ during a scheduled full upgrade.
- The rules created due to insertion of alerts will be visible through the FireEye RPZ viewer. Infoblox recommends that you do not modify any internal objects. For more information, refer to the Infoblox NIOS Administrator guide.
- You must verify the following after you configure the FireEye and NIOS appliances:
 - The URL configured on the FireEye appliance matches the URL in the FireEye integrated RPZ on NIOS.
 - Verify the username and password for FireEye admin on the FireEye appliance.
 - Ensure that the settings are properly configured on the FireEye appliance.
 - Verify the state of the FireEye appliance. For more information about configuring the FireEye appliance to send alerts to the NIOS appliance, refer to the Infoblox NIOS Administrator guide.
 - Note that the frequency of alerts received from FireEye can be minimal. A very small number of alerts are generated on a weekly basis. For example, the FireEye appliance may generate only tens of alerts per day.
- Infoblox recommends purchasing and configuring two Infoblox DNS Firewall appliances in HA (high availability) mode. Refer to the Infoblox NIOS Administrator Guide for more information.

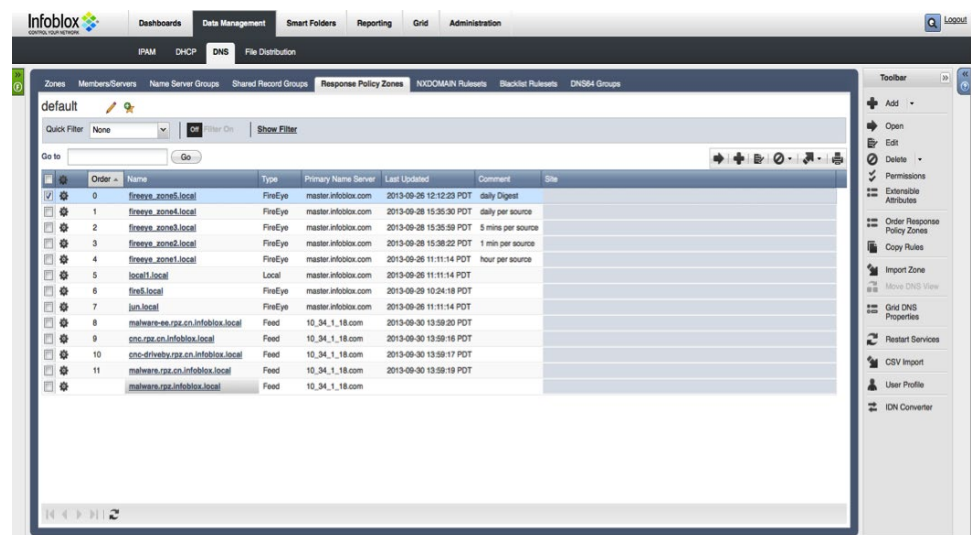


Configuration steps for Infoblox DNS Firewall-FireEye Adapter and FireEye appliance

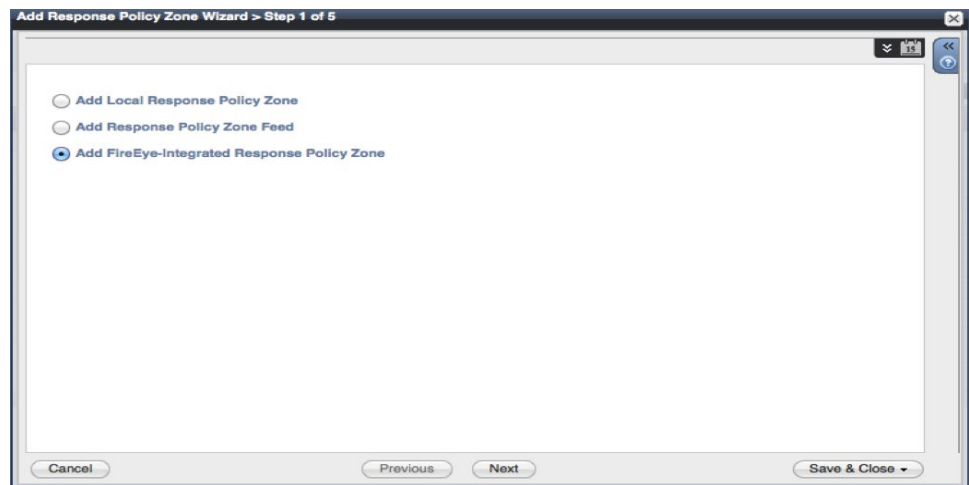
Summary of Configuration Steps

- Install a valid RPZ license. Refer to the Infoblox NIOS administrators guide for more information.
- Enable recursive queries for a DNS view, member, or Grid. Refer to the Infoblox NIOS administrator guide for more information.
- Configure RPZ logging to ensure all matching and disabled rules for all queries are logged in the syslog. Refer to the Infoblox NIOS administrator guide for more information.
- Configure DNS Firewall-FireEye Adapter.
- Configure username and password for FireEye group.
- Configure FireEye appliance.

Configure DNS Firewall-FireEye Adapter



After logging into the Infoblox appliance, click on Data Management tab -> DNS tab -> Response Policy Zone tab. Click on the + icon in the Response Policy Zone section to add a FireEye Response Policy Zone. A Response Policy Zone wizard will appear. This is the zone that will be used to communicate with the FireEye appliance.



Click on the bottom button to add a FireEye-Integrated Response Policy Zone. Click on the Next button.

Input a name for this RPZ. This name is meant for documentation purposes. Input the Policy Override: Select a value from the drop-down list. You can override the policy actions that are specified in the rule level.

- Log only. If a response comes through the DNS Firewall-FireEye Adapter, the response is logged. This setting is good for initial testing to determine if the DNS Firewall-FireEye Adapter is configured correctly. Usually no policies have been entered into the response policy zone.
- None. If a response comes through the DNS Firewall-FireEye Adapter and there is a match, then the policy setting is enforced. Otherwise the response is then tested against any subsequent RPZs.
- Block (no data). If a response is matched, then the response is blocked regardless of the policy setting. A response with no data is sent. Otherwise, the response is tested against any subsequent RPZs.
- Block (no such domain). If a response is matched, then a DNS response is blocked and a response is sent that indicates no domain. All policy actions are replaced with a NXDOMAIN block. Otherwise, the response is tested against any subsequent RPZs.



- Passthru. If a query is matched, then the actual response is pass through without any modification. All policy actions in the RPZ are replaced with a passthru action. Otherwise, the response is tested against any subsequent RPZs.
- Substitute (Domain Name)—Select this if you want to replace all the policy actions in an RPZ with the specified substitution action. Otherwise, the response is tested against any subsequent RPZs.
 - Domain Name: This appears only when you select Substitute (Domain Name) from the Policy Override list. Enter the domain name that you want the client to receive instead of the actual domain name, which is malicious or unauthorized.

Click on the Next button

Copy/paste this URL into the Server URL field when setting up notifications on the FireEye appliance.

Server URL: `https://10.34.35.2/alert/feye/default/default/Thomas+FireEye+Test`

FireEye Alert Type	Policy
Domain Match	Substitute (Domain Name)
Infection Events	Block (No Such Domain)
Callback Events	Passthru
Malware Object	Passthru
Web Infection	Passthru

Override rule mapping for APT events: No Override

Substituted Domain Name*

Buttons: Cancel, Previous, Next, Save & Close

For each FireEye Alert type, select the Policy from each drop down menu:

- Server URL: The appliance displays the URL that you use when configuring the FireEye appliance. This URL is used to handle alerts, which are sent by the FireEye appliance. It handles alerts based on the standard authentication. The URL generated by the Infoblox DNS Firewall-FireEye Adapter consists of the Grid Manager IP address, network view, and DNS view of the FireEye zone. If you change the IP address, network view, zone or DNS view after you have configured a FireEye RPZ, then the URL will change accordingly. Thus FireEye will not be able to send alerts to the updated URL. You must update the URL in the FireEye appliance to send alerts to the NIOS appliance. The Server URL is in this format: `https://<host address>/alert/feye/<network view>/<dns view>/<zone>`.
- Rule Mapping: You can map a FireEye alert type with an RPZ policy. Select an RPZ policy type from the drop-down list. Note that the FireEye alert type is read-only. The Infoblox DNS Firewall-FireEye Adapter applies corresponding RPZ policy type when the FireEye appliance sends an alert to the Infoblox DNS Firewall-FireEye Adapter. If you change the rule mapping(s) later, then any subsequent updates will be reflected in the change, but previous rules will have the previous rule mapping.

The following lists the FireEye alerts and RPZ policy types that can be mapped with the alert:

- Domain Match
- Infection Events
- Callback Events
- Malware Object
- Web Infection
- The RPZ policy types are:
 - None
 - Passthru (this is the default)
 - Block (No such domain)
 - Block (No data)
 - Substitute (Domain name)
- Override rule mapping for APT events: Select a value from the drop-down list to override rule mapping for Advanced Persistent Threats (APT). Events that are marked as APT events by FireEye overrides rules that are set for other event types. The values in the drop-down list are:
 - No Override—Select this if you want to use the policy from the rule level and do not want to override the rule mapping settings. This value is displayed in the drop-down list, by default.
 - Passthru—Select this if you want the user to see the actual response without modification. All the policy actions in an RPZ are replaced with the passthru action.
 - Block (No Such Domain)—Select this if you want the user to receive a NXDOMAIN as the DNS response. All the policy actions in an RPZ are replaced with a NXDOMAIN block. **This setting would be a best practice for handling APTs.**
 - Block (No Data)—Select this if you want the user to receive a response that indicates that there is no data. **This setting would be a best practice for handling APTs.**
 - Substitute (Domain Name)—Select this if you want to replace all the policy actions in an RPZ with the substitution action that is specified. **This setting would be a best practice for handling APTs.**
 - Substituted Domain Name: This appears only when you select Substitute (Domain Name) from the Policy Override list either for APT events or for FireEye alerts. Enter the domain name that you want the client to receive instead of the actual domain name, which is malicious or unauthorized.

Click on the Next button.



Add Response Policy Zone Wizard > Step 4 of 5

☐ None
☒ Use this name server group all
☐ Use this set of name servers

Name	IPv4 Address	IPv6 Address	Type	TSIG
No data				

Cancel Previous Next Save & Close

Associate the FireEye integrated RPZ with at least one primary name server:

- Define the name servers for the FireEye integrated RPZ. A Grid name server must be recursive when primary Grid name server is used as an RPZ source. A FireEye integrated RPZ may or may not have a recursive server. For example, there could be a Grid that has only primary Grid name server for a FireEye integrated RPZ to act as an RPZ source for an external set of name servers. A FireEye integrated RPZ must have only one primary Grid name server and it can have one or more secondary Grid name servers. When you select All Recursive Name Servers from the list, all the recursive name servers in the Grid are added as secondary servers for the zone.

Click on the Next button.

Add Response Policy Zone Wizard > Step 5 of 5

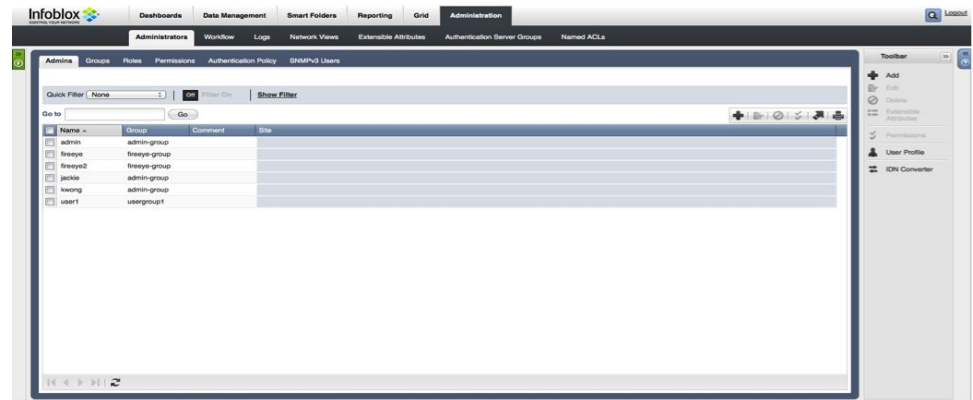
Extensible Attributes

Attribute Name	Value	Required
No data		

Cancel Previous Next Save & Close

Optionally add extensible attributes and click on Save & Close to complete the process. For more information on extensible attributes, please refer to the Infoblox NIOS Administrator Guide. Click on the Save & Close button.

Configure Username and Password for FireEye Group



From the Administration tab, select Administrators, and then click Admins. Click on the + icon to bring up the Add Administrator Wizard. This is the username and password that the FireEye appliance is going to use to send updates to the Infoblox DNS Firewall-FireEye Adapter.

The screenshot shows the 'Add Administrator Wizard - Step 1 of 2' dialog. The fields are filled as follows:

- Login: fireeye3
- Password: (masked with dots)
- Confirm Password: (masked with dots)
- Email Address: (empty)
- Admin Group: fireeye-group (selected)
- Comment: (empty)
- Disable: ☐

A yellow dashed box highlights the Password and Confirm Password fields with the message: "Password must contain at least 4 characters." The 'Next' button is visible at the bottom right.

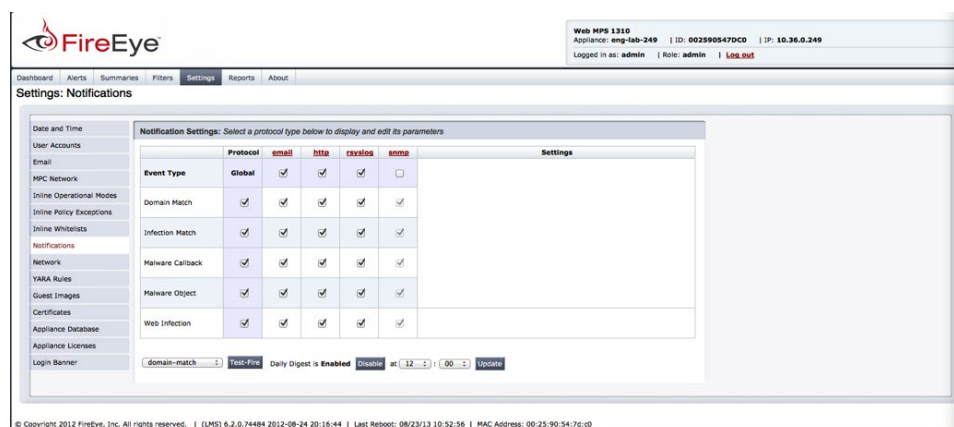
Input the username in the login box and password in the password boxes. Select fireeye-group for the admin group and click Next.

The screenshot shows the 'Add Administrator Wizard - Step 2 of 2' dialog. The 'Extensible Attributes' section is empty, showing a table with columns 'Attribute Name' and 'Value'. The 'Save & Close' button is visible at the bottom right.

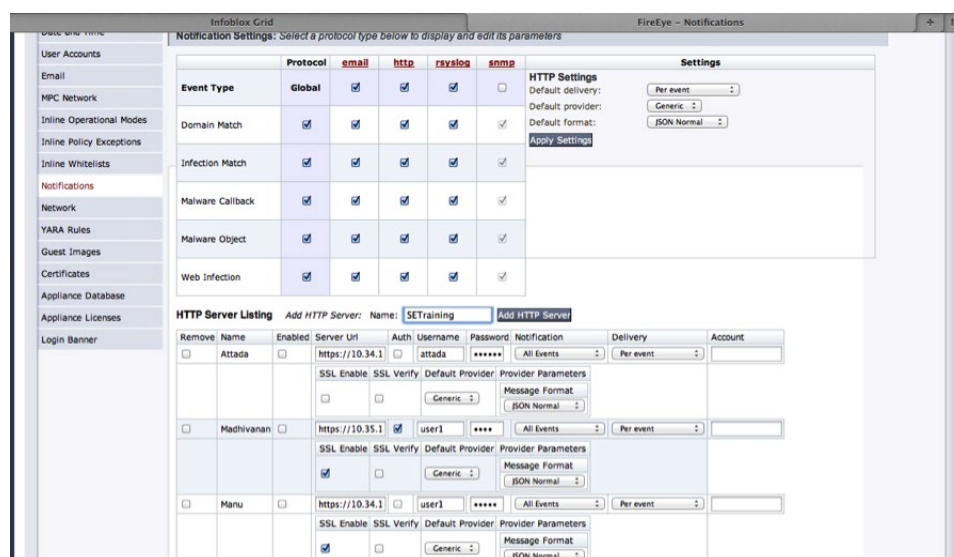
Optionally, add extensible attributes and then click on the Save & Close button to save the usernames and passwords.



Configure FireEye Appliance



Login to the FireEye appliance with your username and password. In the FireEye GUI, click on the Settings tab and then click on the Notifications tab on the left panel.



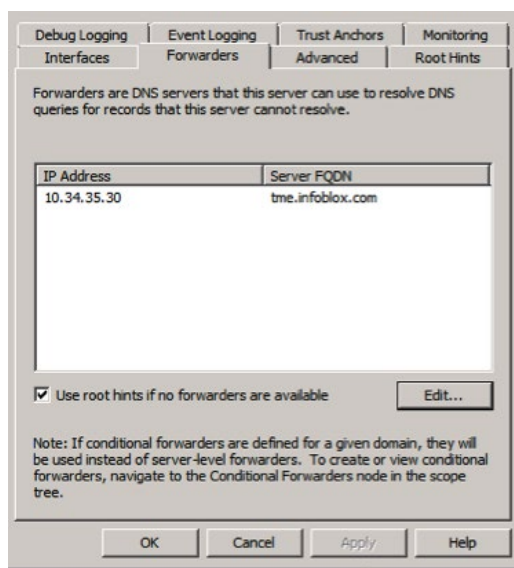
In the Notification Settings page, click on the HTTP link and then enter the name of the HTTP server you want to add.

Click Add HTTP Server and complete the following:

- **Name:** When you click Add HTTP Server, the HTTP server name that you specified gets listed in the Name column.
- **Enabled:** Select the check box to enable alerts and notifications for the HTTP server.
- **Server URL:** Enter the URL you received on the Infoblox DNS Firewall-FireEye Adapter. The alerts and notifications are sent using this URL by the FireEye appliance.
- **Auth:** Select this check box if authentication is required for the server.
- **Username and Password:** Enter the Username and Password of the user that you have configured for the fireeye-group on the Infoblox DNS Firewall-FireEye Adapter.
- **Notification:** Select a notification from the drop-down list. You can choose to include notifications for all events or only events of a selected type. The FireEye appliance will send an alert to the NIOS appliance only when selected event is encountered. When you select All Events, alerts are sent when the FireEye appliance encounters each event.

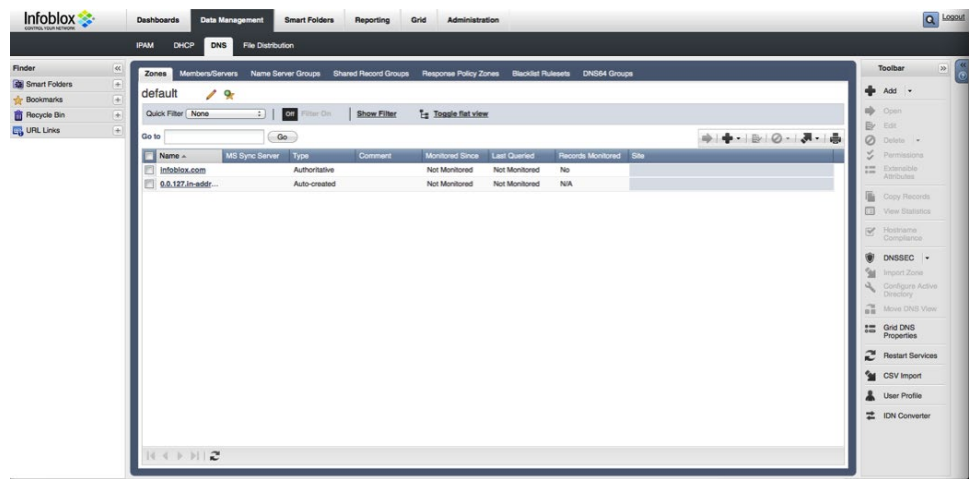
- **Delivery:** Select Per Event from the drop-down list. Note that the NIOS appliance supports only Per Event selection. The FireEye appliance sends an alert each time it encounters an event.
- **Account:** You can specify a user account name for this notification.
- **SSL Enable:** Select this check box to enable SSL for secure transmission of alerts.
- **SSL Verify:** Select this check box to implement SSL verification.
- **Default Provider:** Select a default provider from the list.
- **Message Format:** Select JSON Normal from the drop-down list. Note that the NIOS appliance supports only this message format.
- Click Update at the bottom of the page.

Steps to Configure Microsoft DNS Server to Communicate with the Infoblox DNS Firewall-FireEye Adapter as a Forwarder

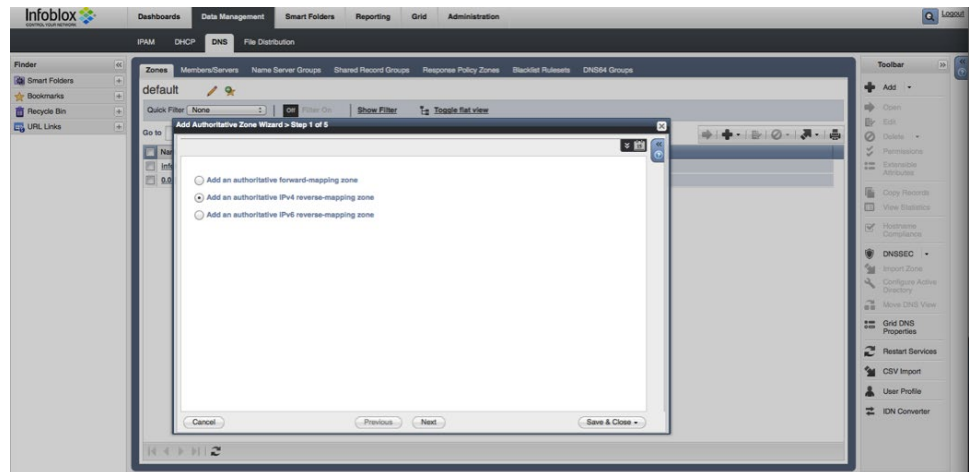


- Bring up the DNS application on the Microsoft DNS server.
- Select the DNS server name.
- Right click on the DNS server name and scroll down to properties.
- Select the Forwarders tab.
- Press the 'Edit' button to add the IP address of the Infoblox DNS Firewall-FireEye Adapter.
- Click OK.

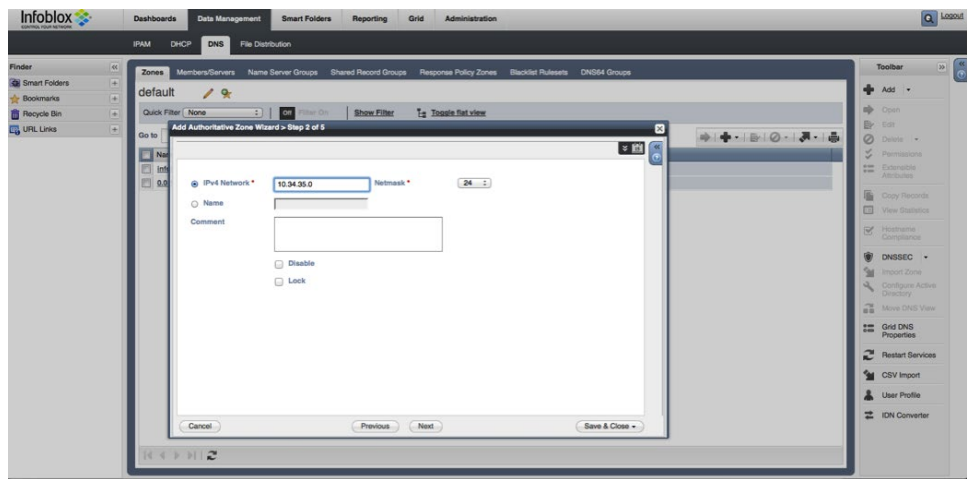
Note: If you are using another DNS server vendor, configure that DNS server to forward requests to the Infoblox Trinetic Network Services Appliance. Refer to the vendor's user guide on configuring DNS forwarding.



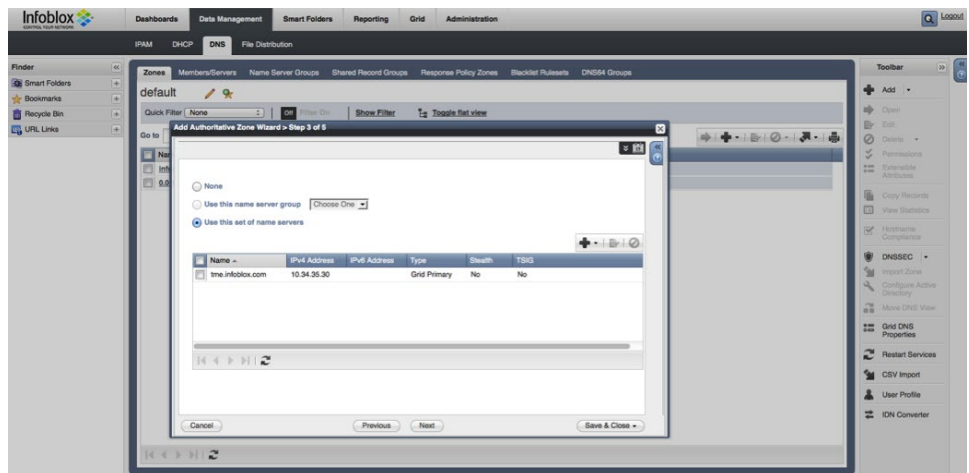
- Log into the Infoblox DNS Firewall-FireEye Adapter.
- Click on Data Management.
- Click on DNS.
- Click on Zones.



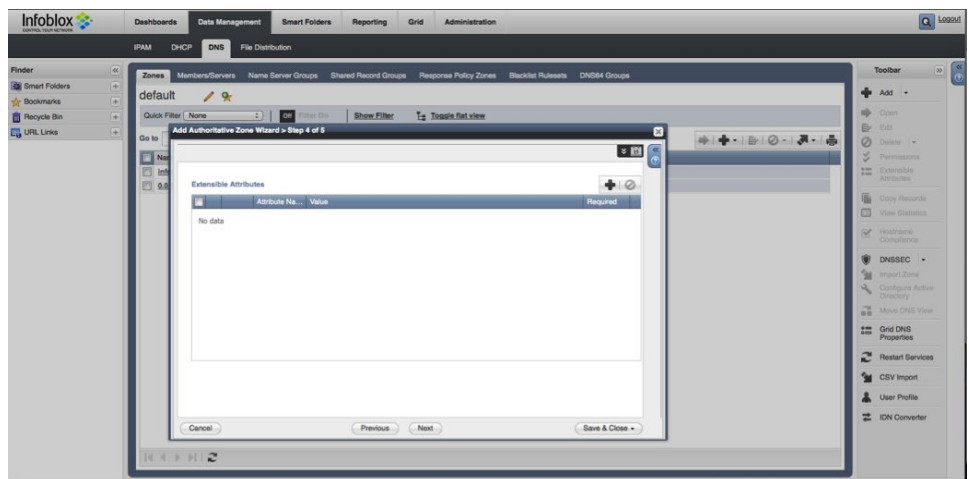
- Click on the + icon to bring up the Authoritative Zone Wizard.
- Click on the button for the Authoritative IPv4 reverse mapping zone in the Add Authoritative Zone Wizard.
- Click on the Next Button.



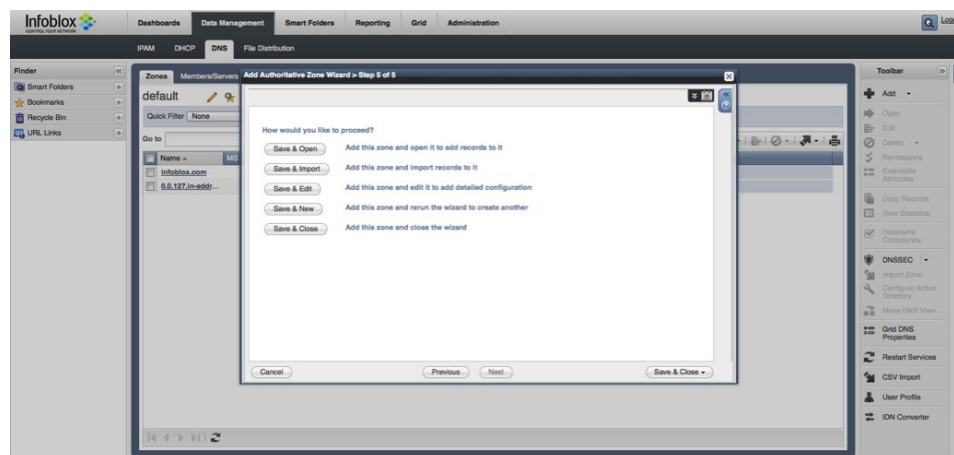
Add the IP address of the zone. This would be the subnet of the Microsoft DNS server. Click on the Next button.



Add the Infoblox DNS Firewall-FireEye Adapter as Grid Primary, Grid Secondary, External Primary, External Secondary, or All Recursive Name Servers. Refer to the Infoblox NIOS Administrator guide for further information. Click on the Next button.



Optionally, add extensible attributes. Click on the Next button.



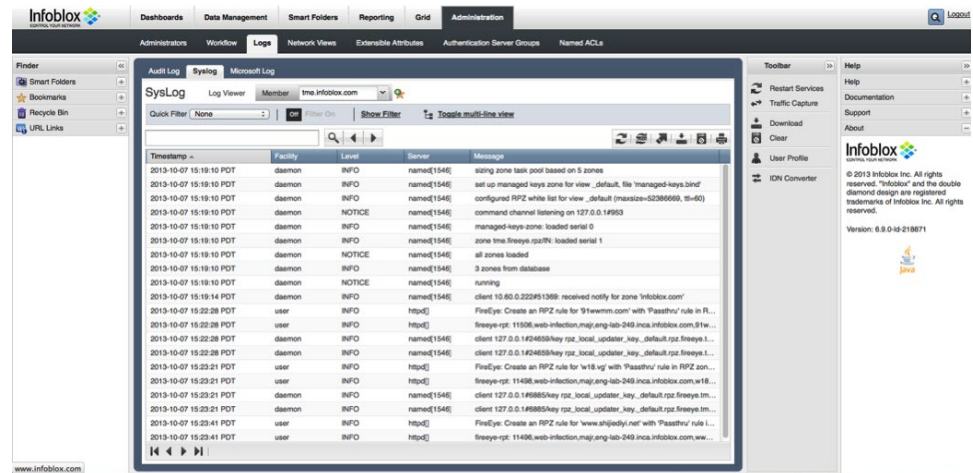
Click on Save and Open to add records to the reverse authoritative zone. At this point, the FQDN on the Microsoft DNS Server Forwarder screen should be resolved.

Verify FireEye Configuration



To test the communication between the FireEye appliance and the Infoblox DNS Firewall-FireEye, you can select the criteria and then hit the Test-Fire button. Domain-match is checked by default. If the configuration is successful, FireEye sends a confirmation message to the NIOS appliance and the NIOS appliance logs this message in the syslog. It generally takes a few seconds for the NIOS appliance to receive alerts. You must verify the configuration, if there is no entry in the syslog. On the network level, FireEye uses port 443 to communicate with the Infoblox DNS Firewall-FireEye Adapter.

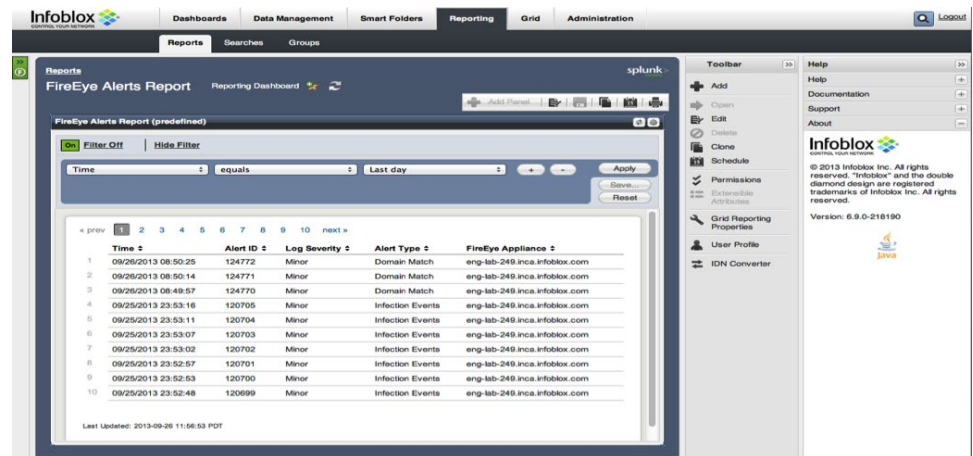
Verify RPZ Configuration



After you have set up and configured RPZs and RPZ rules, you can verify whether the RPZ zone transfers are functioning properly by doing the following:

- View the syslog for zone transfer confirmation.
- Verify the last RPZ updates.

Reports



Click on the Reporting tab -> Reports tab -> FireEye Alerts to view a report on FireEye events. This report can be exported into a PDF file for operational reporting as well as compliance reporting.

Conclusion

The FireEye/Infoblox DNS Firewall-FireEye Adapter integration will allow the customer to:

- Detect the APT with the FireEye appliance.
- Disrupt the malware attack by installing a rule into the Infoblox DNS Firewall-FireEye Adapter by the FireEye appliance.
- Pinpointing the source of the malware attack with the use of Infoblox reporting, DHCP server (DHCP fingerprinting), and IP address management.
- Save time and money in detecting and mitigating the APTs.
- Safeguard confidential information.
- Enhance network and computer system uptime.



CORPORATE HEADQUARTERS:

+1.408.986.4000

+1.866.463.6256

(toll-free, U.S. and Canada)

info@infoblox.com

www.infoblox.com

EMEA HEADQUARTERS:

+32.3.259.04.30

info-emea@infoblox.com

APAC HEADQUARTERS:

+852.3793.3428

sales-apac@infoblox.com