Infoblox®
NEXT LEVEL NETWORKING

BloxOne^{TM} Threat Defense Architecture Guide

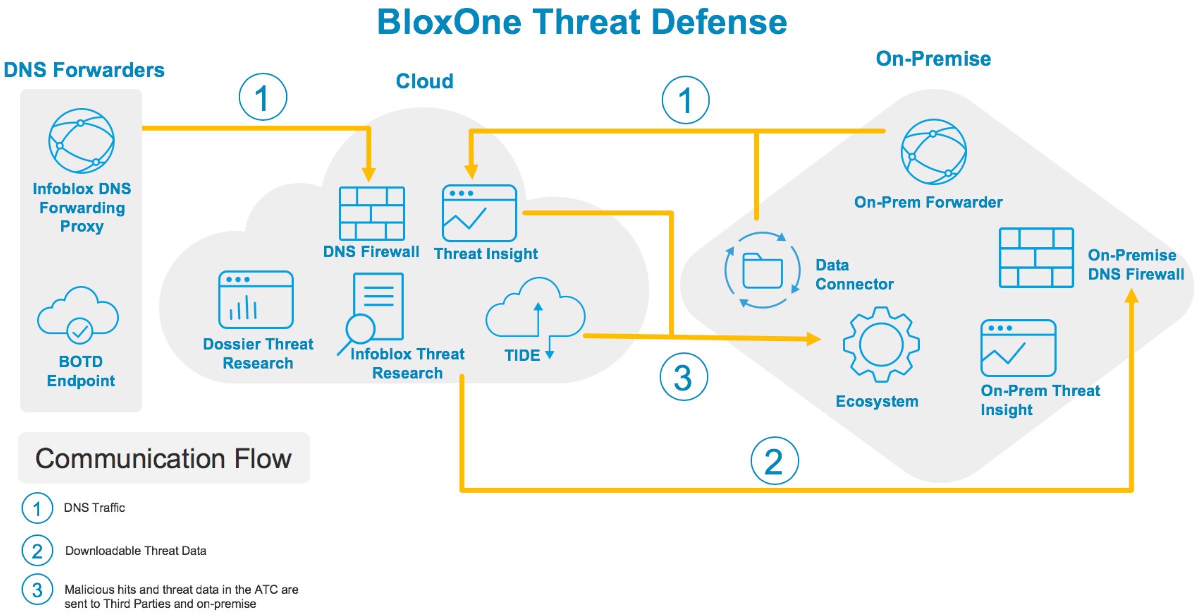
BloxOne Threat Defense

TABLE OF CONTENTS

Introduction

This guide documents the information needed to effectively understand the architecture and integration of different solutions offered by Infoblox in order to give guidance on the design of the system to be deployed. This architecture guide is made for all organizations who will deploy Threat Insight in the cloud and on-premise, BloxOne Threat Defense Cloud (BOTDC) for remote users and Infoblox Ecosystem.

Infoblox BloxOne Threat Defense (BOTD) is the first integrated, cloud managed, hybrid DNS security solution that protects users and devices anywhere – on the enterprise network, while roaming or in a remote office - from cyberattacks. The solution blocks DNS based data exfiltration, stops malware communications with command-and-control servers, automatically prevents access to content not in compliance with policy, and shares intelligence and IoCs with existing security infrastructure for orchestration and faster remediation. BloxOne Threat Defense turns DNS from a security blind spot into a powerful, and pervasive core network security asset, allowing organizations to elevate their security to the next level.



BloxOne Threat Defense comprises of 7 major pieces:

Endpoints: Lightweight mobile agent that redirects DNS traffic from remote devices to the BloxOne Threat Defense Cloud. It allows organizations to apply applicable security policies to roaming end users in remote sites and branch offices. This solution embeds client IP before forwarding to Infoblox Cloud.

DNS Forwarding Proxy: Virtual appliance that redirects DNS traffic from remote devices when installing an endpoint agent is not desirable or possible (on internal networks or IoT devices). This solution enables an agentless deployment that embeds client IP and MAC into DNS queries before forwarding to Infoblox Cloud.

TIDE: Highly accurate machine-readable threat intelligence data via a flexible Threat Intelligence Data Exchange (TIDE) used to aggregate, curate, and enable distribution of data across a broad range of infrastructure. TIDE enables organizations to ease easily consume threat intelligence from various internal and external sources, and to effectively defend against and quickly respond to cyber threats.

TIDE is backed by the Infoblox Cyber intelligence Unit (CIU) that normalizes and refines high-quality threat intelligence data feeds.

Dossier: Threat investigation tool providing immediate contextual information on threats from a dozen sources (including TIDE) simultaneously. This allows threat analysts to save precious time in taking action against any identified threats. By using Dossier, accurate decisions are made more quickly and with greater confidence, shortening the threat's attack window. Infoblox Dossier threat indicator investigation provides rich threat context to prioritize incidents and respond quickly.

Threat Insight: Provides built-in statistics of the DNS infrastructure to detect and block data exfiltration via DNS. In addition, Infoblox enables organizations to effectively stop data theft through the DNS with no need for additional endpoint software, security appliances, or network infrastructure.

DNS Firewall: Uses and Provides threat intelligence feeds with indicators of compromise (IoC) which provides organizations with the ability to protect users anywhere. This is part of a complete DNS, DHCP and IP Address Management (DDI) solution with integrated security, deep visibility and network context of an organization's on-premises and cloud infrastructure. Detected malware events blocked by DNS Firewall are signaled to the organization's other network security technologies.

Data Connector: Collects DNS query and response data from the Infoblox appliances that are answering queries, and then forwards this data to the NIOS reporting server and third-party indexers, such as a SIEM, through the SCP protocol. Similarly, it collects RPZ Hits, DHCP Leasing Information and IPAM User Info data if available, from Infoblox appliances, generates parquet files and sends the parquet files to the Infoblox BloxOne Threat Defense Cloud destination via HTTP requests.

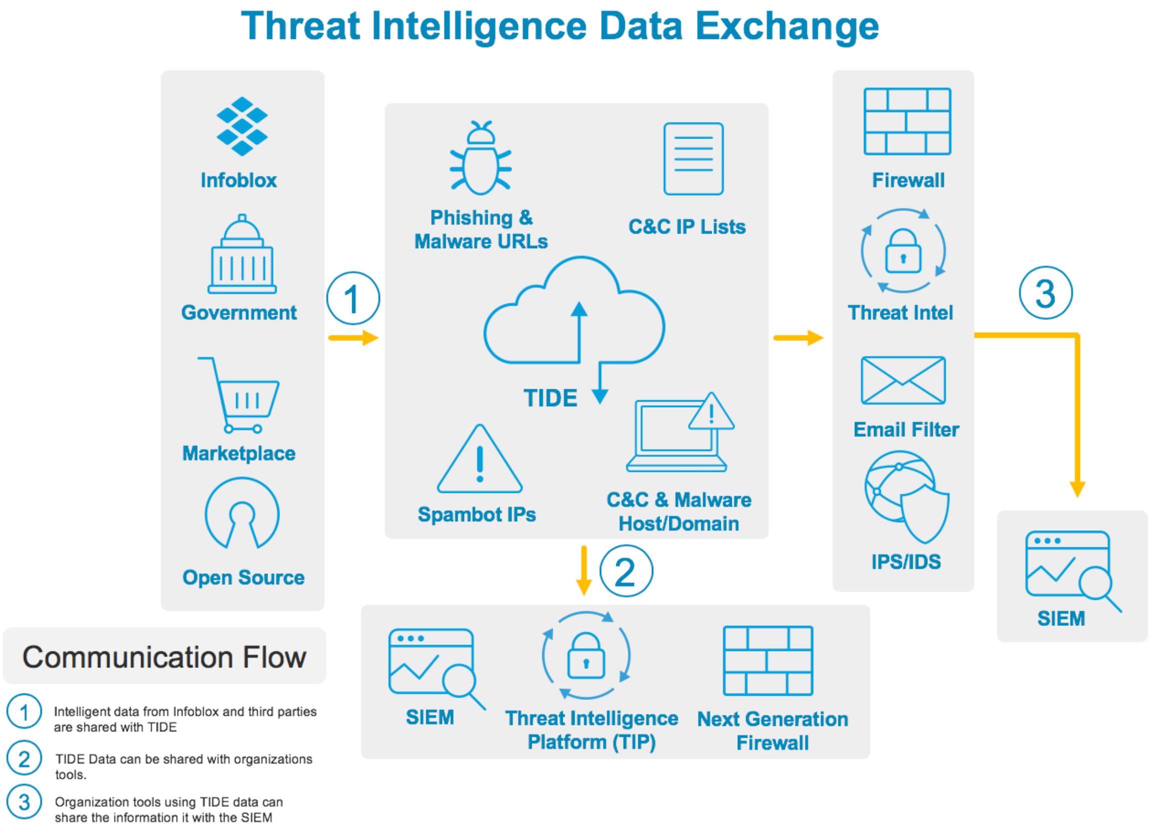
Architecture:

Scalable Threat Intelligence

General Overview

Threat Intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging threat or hazard. Threat Intelligence can be used to inform decisions regarding the subject's response to threats or hazards. TIDE uses highly accurate machine-readable threat intelligence data via a flexible and open Threat Intelligence Data Exchange (TIDE) platform to aggregate, curate, and enable distribution of data across a broad range of infrastructures. TIDE enables organizations to easily consume threat intelligence from Infoblox research and third-party intelligence providers and to effectively defend against and quickly respond to threats.

Structure


Threat Intelligence Data Exchange

Communication Flow

1 Intelligent data from Infoblox and third parties are shared with TIDE

2 TIDE Data can be shared with organizations tools.

3 Organization tools using TIDE data can share the information it with the SIEM

Infoblox designed TIDE to keep security systems such as Infoblox BloxOne Threat Defense and its cybersecurity ecosystem updated in near real time on new and evolving malicious Internet destinations. TIDE uses over 300 distinct classifications and over 20 properties to help prioritize by providing context and insight on threats.

TIDE provides data based on observed malicious Internet destinations with which devices have attempted to communicate, and detailed threat information around those endpoints to enable security teams to quickly understand the nature of the threats they are experiencing. The sources of threat intelligence are reviewed, the data correlated, and whitelists applied to significantly minimize false positives. This work is handled by the Infoblox Cyber Intelligence Unit(CIU) . TIDE was originally formed in 1997 by the CTI after receiving requests from leading financial institutions for this kind of service.

The CIU also have a team looking at very large DNS query and response data sets to find new behavioral and heuristic patterns. Because of our deep experience with the DNS protocol we've also applied that experience to how we approach our threat hunting, large scale spam-traps, reverse-engineering and passive DNS analysis. The TIDE platform is also used to build out a multi-sourced RPZ marketplace for robust DNS security. More sources represent a broader view. More focus brings a more timely, accurate and clean stream of data. We are advancing on both fronts.

This comprehensive intelligence of indicators can also be leveraged at the DNS control plane (via automatic updates to its Response Policy Zone (RPZ) policy) to enforce policies set by the user to block unwanted IP communications. The threat intelligence is also easily deployable via the Infoblox TIDE platform via an API in various formats (CEF, CSV, XML, STIX and JSON) on security infrastructure such as next-generation firewalls, email gateways, web proxies, SIEMs and others.

Guides

TIDE Solutions:
https://community.infoblox.com/t5/Infoblox-TIDE-Solution/gp-p/TidePartners

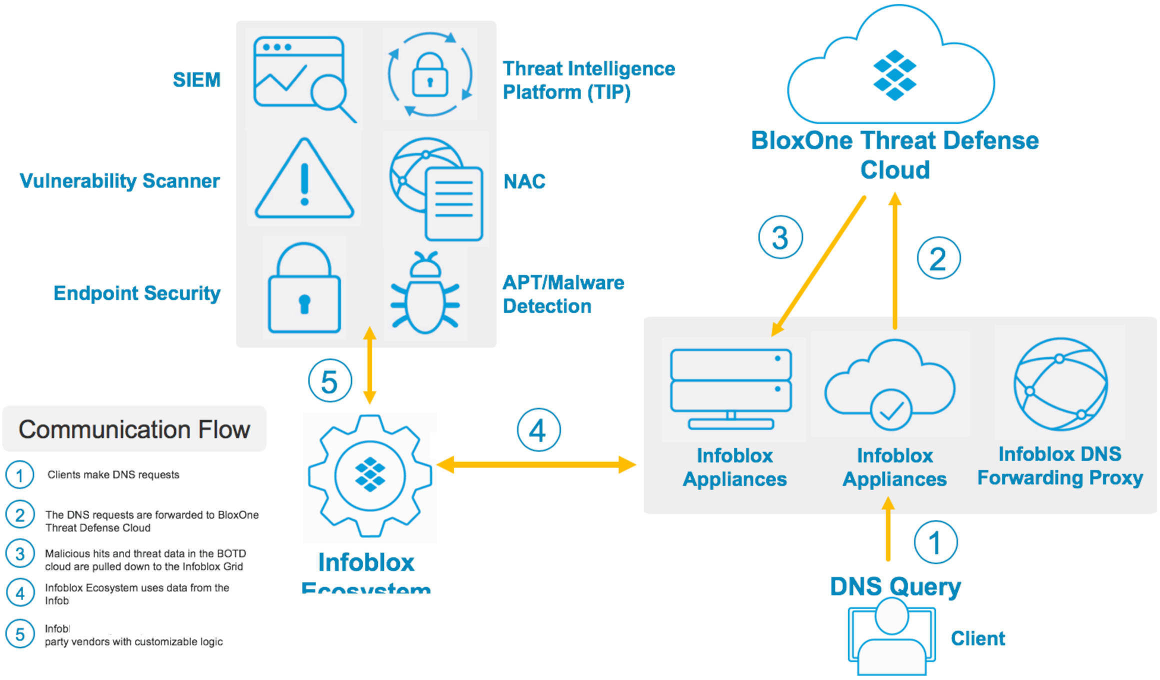
TIDE Quick Start Guide:
https://community.infoblox.com/t5/Infoblox-TIDE-Solution/Infoblox-Dossier-TIDE-Quick-Start-Guide/gpm-p/11868

Infoblox Ecosystem

General Overview

Infoblox BOTD has many different types of integrations and ability to share its data with numerous different third-party vendors. Outbound notification integration (enabled by the on-premise ecosystem license) provides the ability to send data to other systems from the BOTD about blocked DNS-based data exfiltration, malware communications and prevention of access to content not in compliance with policy. The signaling and data sharing between security ecosystem elements results in faster threat response, uninhibited remediation and reduced risk from cyberattacks via DNS with data from BOTD.

Structure


SIEM
Threat Intelligence Platform (TIP)
Vulnerability Scanner
NAC
Endpoint Security
APT/Malware Detection
BloxOne Threat Defense Cloud
3
2
5
4
Infoblox Appliances
Infoblox Appliances
Infoblox DNS Forwarding Proxy
Communication Flow
1 Clients make DNS requests
2 The DNS requests are forwarded to BloxOne Threat Defense Cloud
3 Malicious hits and threat data in the BOTD cloud are pulled down to the Infoblox Grid
4 Infoblox Ecosystem uses data from the Infob
5 Infobl party vendors with customizable logic
Infoblox Ecosystem
1
DNS Query
Client

When pushing data to other systems there are three things that must be uploaded and configured:

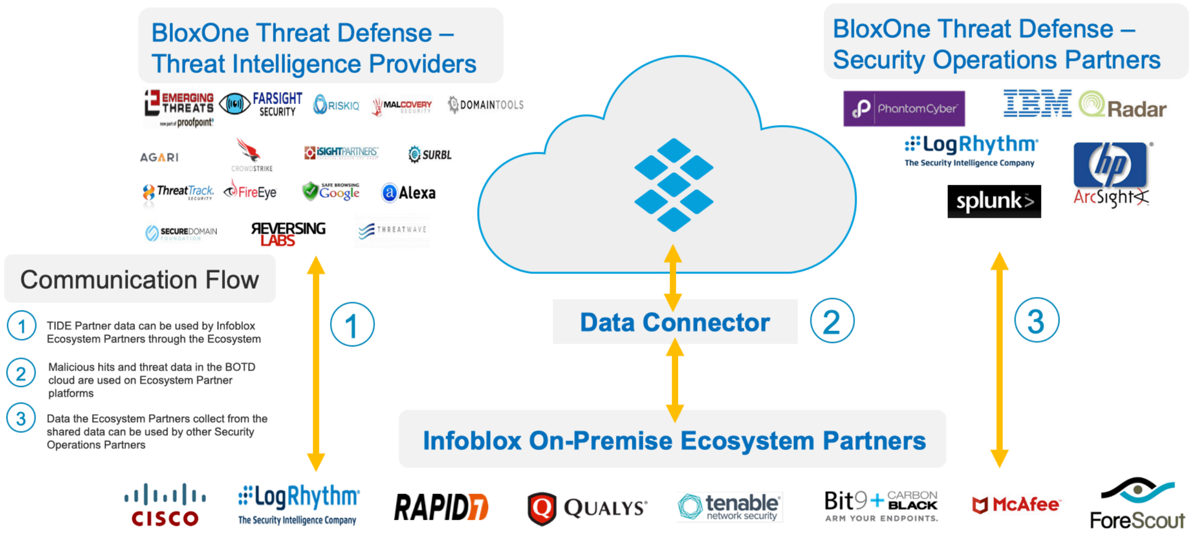
Templates: Provides the logic through a simple JSON file that enables organizations to manipulate the BOTD events into RESTful API. Using supported variables in the templates, organizations can get respective events and define actions they want to take for the BOTD events.

Outbound Endpoint: There are many different third parties that Infoblox works with and as such the outbound endpoint provides the third party to send the BOTD events to.

Notification Rules: BOTD has many different events, with notification rules organizations can decide which events they want to use and which endpoints they want to send events to.

Infoblox Ecosystem is a system wide license that requires on-premises physical or virtual Infoblox infrastructure. Infoblox's appliance will pull data from the BOTD and push the data to third party vendors. The data that is pushed to third party vendors can be manipulated with logic found inside templates, which is part of Infoblox's Ecosystem. Additionally, Outbound API is required to share TIDE data with third party vendors.

Cybersecurity Ecosystem



1. TIDE Partner data can be used by Infoblox Ecosystem Partners through the Ecosystem
2. Malicious hits and threat data in the BOTD cloud are used on Ecosystem Partner platforms
3. Data the Ecosystem Partners collect from the shared data can be used by other Security Operations Partners

Guides

BOTD Integration with Infoblox Outbound Notifications:
https://community.infoblox.com/cixhp49439/attachments/cixhp49439/security/1675/3/ActiveTrust%20Cloud%20Outbound%20Notifications%20QSG.pdf

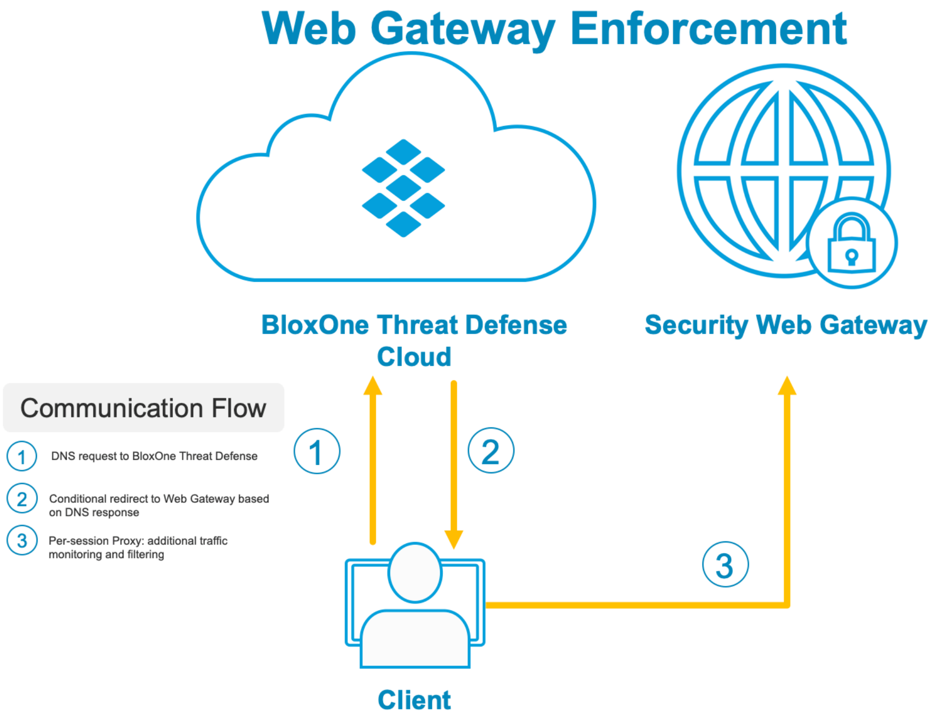
Third-party integrations:
https://community.infoblox.com

Web Gateway Enforcement

General Overview

The DNS policy engine of BOTD can be used in conjunction with Security Web Gateway (SWG) and Cloud Access Security Broker (CASB) solutions in order to enforce security policy-based routing and offload the security infrastructure from substantial CPU intensive level 7 analysis.

Structure


Web Gateway Enforcement
BloxOne Threat Defense Cloud
Security Web Gateway
Communication Flow
1 DNS request to BloxOne Threat Defense
2 Conditional redirect to Web Gateway based on DNS response
3 Per-session Proxy: additional traffic monitoring and filtering
1
2
3
Client

The ability to redirect traffic from BloxOne Threat Defense allows for Offloading of whitelists and being able to return actual applications IPs at the DNS level for things such as organization cloud direct access, corporate SaaS solutions, Alexa top domains, Office 365 and more. BloxOne threat defense has the ability to Redirecting to a SWG or a CASB a FQDN or IP for authentication, decryption and additional security policy enforcements such as shadow IT, file sharing, remote control of applications and more. This also provides Organizations the ability to redirect to a proxy or block the DNS requests. Additionally, Organizations are given the ability to redirect to honeypot FQDN or IPs.

Threat Insight

General Overview

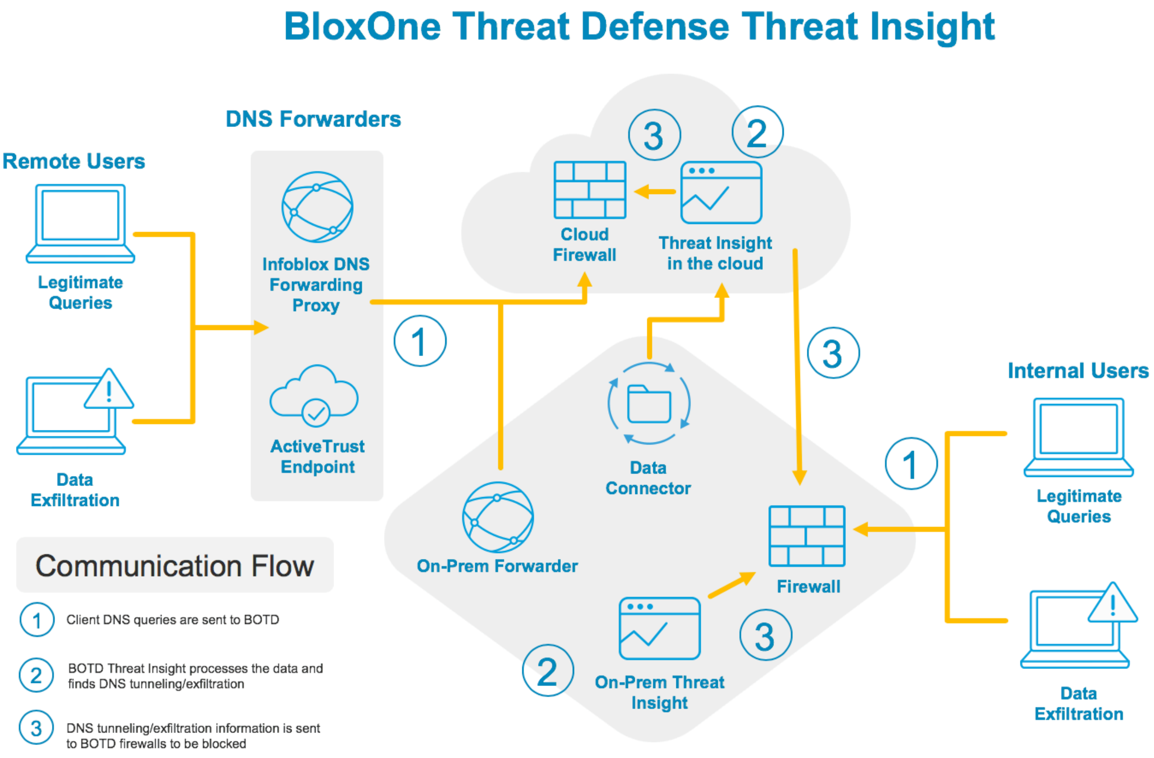
Threat Insight (TI) and Threat Insight in the Cloud (TI in the Cloud) protects DNS infrastructure from being used for data exfiltration, data infiltration and DNS tunneling.

Hackers exploit the DNS protocol as a pathway for data exfiltration through DNS tunneling attacks. DNS tunneling involves tunneling another protocol through port 53 by means of malware-infected devices. This malicious DNS tunneling activity mostly goes undetected, even by the next-generation firewalls. The purpose of these attacks is to steal sensitive information such as credit card numbers and company financials. This is achieved either by establishing a DNS tunnel from within the network or by encrypting and embedding chunks of that data in DNS queries/responses. Data is decrypted at the other end and put back together so valuable information can be stolen and misused by malicious attackers.

DNS tunneling is a two-way protocol exchange occurring over DNS. Data exfiltration/infiltration via DNS does not necessary imply DNS tunneling even though some methods may be similar. In this document when we specify any of these data transfers over DNS methods, all are applicable.

A major differentiator between Threat Insight and TI in the Cloud is that TI in the Cloud, although slower, blocking of malicious DNS traffic is more advanced and has a greater processing capability to deal with a wider range of threats. For example, it can protect against DGA and Fast Flux activity and deal with “lower and slower” exfiltration attempts, while Threat Insight on-premise is faster it can’t protect against DGA and Fast Flux.

Structure


BloxOne Threat Defense Threat Insight
DNS Forwarders
Remote Users
Legitimate Queries
Data Exfiltration
Infoblox DNS Forwarding Proxy
ActiveTrust Endpoint
3
2
Cloud Firewall
Threat Insight in the cloud
1
3
Data Connector
Internal Users
1
Legitimate Queries
On-Prem Forwarder
Firewall
2
On-Prem Threat Insight
3
Data Exfiltration
Communication Flow
1 Client DNS queries are sent to BOTD
2 BOTD Threat Insight processes the data and finds DNS tunneling/exfiltration
3 DNS tunneling/exfiltration information is sent to BOTD firewalls to be blocked

How Threat Insight Defends Against Threat Actors.

Threat Insight is a zero-day approach where the threat is unknown by blacklists beforehand and through the use of sophisticated algorithms new threats are caught and stopped in their tracks. These algorithms leverage AI via machine learning and neural networks. Multiple benchmarks are taken into account across a sequence of requests to determine malicious activity; anomaly scoring is used to ensure maximum accuracy.

Once Infoblox starts forwarding its traffic to the cloud or sends its traffic via Infoblox's data connector, the TI in the Cloud starts analyzing incoming DNS data and applying the algorithms to detect security threats that have the same or similar behavior as known malicious data. Once security threats are detected, the appliance blacklists the domains and transfers them to the designated mitigation response policy zone and traffic from the offending domains are blocked preventing DNS lookups for these domains.

Infoblox Threat Insight also includes a whitelist that contains trusted domains for which DNS traffic is allowed. These are known good domains that carry legitimate DNS tunneling traffic such as Amazon AWS, Sophos, McAfee, Spotify and various others. The whitelist is extensible, so new whitelisted domains can be added and rolled out accordingly. Organizations can also add custom whitelisted domains or move blacklisted domains to the whitelist.

Guides

Deployment Guide:
https://www.infoblox.com/wp-content/uploads/infoblox-deployment-guide-threat-insight-in-the-cloud.pdf

Threat Insight in the Cloud set up:
https://docs.infoblox.com/display/IDCUG/Configuring+Threat+Insight+for+Cloud+Destination

On-Premise Survivability

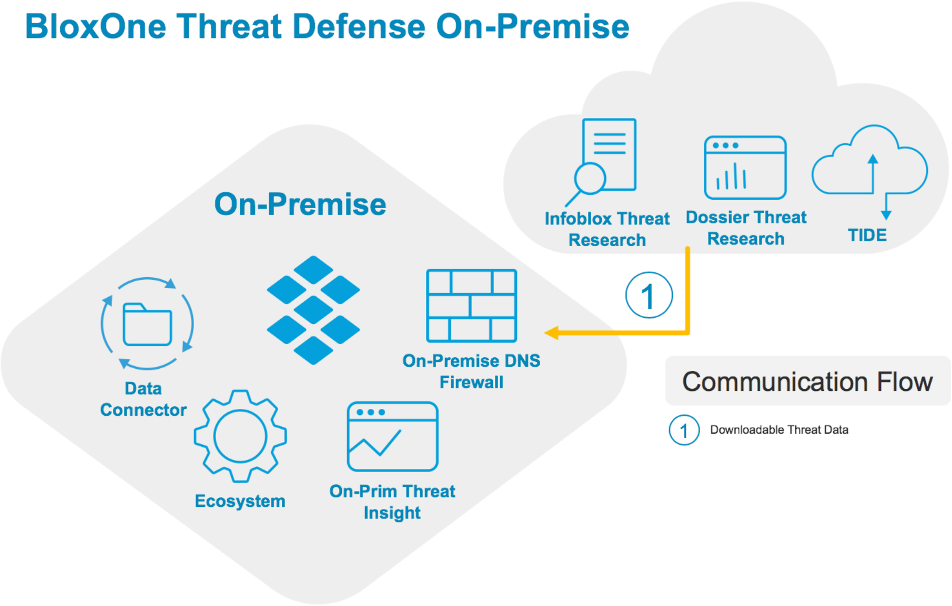
General Overview

BOTD provides protection from the cloud and on-premise where most can only protect from the cloud or on-premise alone. This hybrid approach allows organizations to separate critical assets from less-sensitive assets by allowing organizations to keep full control of their data on-premise while pushing data that isn't so sensitive to the cloud. This includes protection from frequent influx of DNS traffic by controlling what data goes to the cloud for scalability while protecting crucial resources. If speed is of upmost importance, then organizations won't find a quicker query response then an on-premise DNS security solution which cloud security solutions won't be able to offer due to the time it takes to transfer the data.

The hybrid approach allows for organizations to decide in the future to move from on-prime to cloud and back without trouble and decide what blend is best for the individual organization based on their resources. This means organizations using a hybrid approach can move incrementally to the cloud and choose the speed that is right for them included pushing traffic to the cloud to prevent overflow of traffic from on premise and prevent network outages that may occur.

While connection to the outside internet can go down at any time, the internal network will continue to work with a hybrid approach and can continue to service assets within the network so that there is complete internal network accessibility, while the external network is unavailable.

Structure



The advantage of using a hybrid approach is to allow for all remote and local users to be completely protected. If the cloud service was unavailable for any reason, the internal network will continue to service clients and provide protection.

Guides

Forward DNS to BOTD cloud:
https://docs.infoblox.com/display/BloxOneThreatDefense/Forwarding+DNS+Traffic+to+BloxOne+Threat+Defense+Cloud

Component Deployment Options:

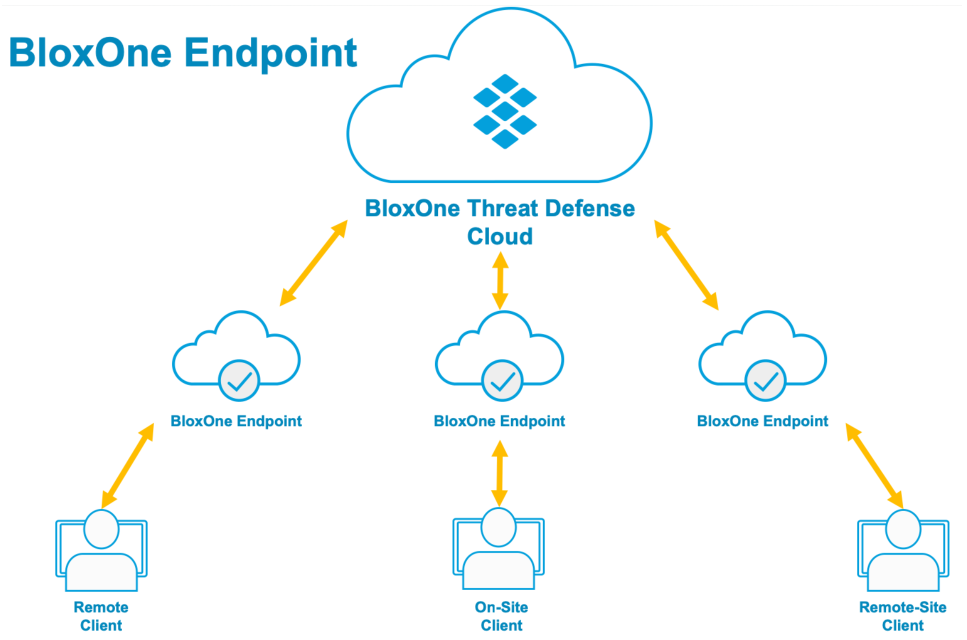
BloxOne Endpoint

General Overview

The popularity and convenience of mobile devices mixed with increasing cybercrime have caused security challenges for most companies that are losing control over when and where employees use their devices. In ideal situations a company can implement enterprise security policies and content categorization that always apply regardless of users' actions. That's what we do at Infoblox. Our approach is to protect devices anywhere, whether on premises, roaming or in remote or branch offices, without requiring any user authentication or action.

Infoblox Endpoint is a lightweight mobile agent that redirects DNS traffic from remote devices to the BloxOne Threat Defense Cloud. It allows organizations to apply applicable security policies to their roaming end users in remote sites and branch offices. For the devices that are off premises, BloxOne Endpoint sends device name and MAC address with each DNS request. In addition, the solution's Cloud Service Portal provides a single pane of glass for all security events.

Structure



The client enforces security policies that are applied to remote networks, regardless of where end users are located, and to which networks they are connected. BloxOne Endpoint listens on port 53 of the device. If other software listens on the same port, DNS traffic cannot be redirected to BloxOne Threat Defense Cloud, and the device will not be protected by BloxOne Endpoint.

When using BloxOne Endpoint, DNS queries are sent to BloxOne Threat Defense Cloud directly except for:

1. queries that target the bypassed domains and
2. internal domains collected through the DHCP server.

If organizations have internal domains that are served by their local DNS servers and they want to reach them without interruptions, consider adding the internal domains to the bypassed internal domains list so that DNS queries for these internal domains are sent to the local DNS servers instead of BloxOne Threat Defense Cloud.

BloxOne Endpoint supports dual-stack IPv4 and IPv6 DNS configurations, thereby protecting all devices regardless of their network environments. BloxOne Endpoint in a dual-stack environment can proxy IPv6 DNS queries and forward them to BloxOne Threat Defense Cloud over IPv4.

Guides

Download Endpoint:
https://docs.infoblox.com/display/BloxOneThreatDefense/Downloading+Endpoint

Standalone Deployment:
https://docs.infoblox.com/display/BloxOneThreatDefense/Standalone+Deployment

Windows Mass Deployment:
https://docs.infoblox.com/display/BloxOneThreatDefense/Windows+Mass+Deployment

Mac OS X Mass Deployment:
https://docs.infoblox.com/display/BloxOneThreatDefense/Mac+OS+X+Mass+Deployment

McAfee ePO Deployment:
https://docs.infoblox.com/display/BloxOneThreatDefense/McAfee+ePO+Deployment

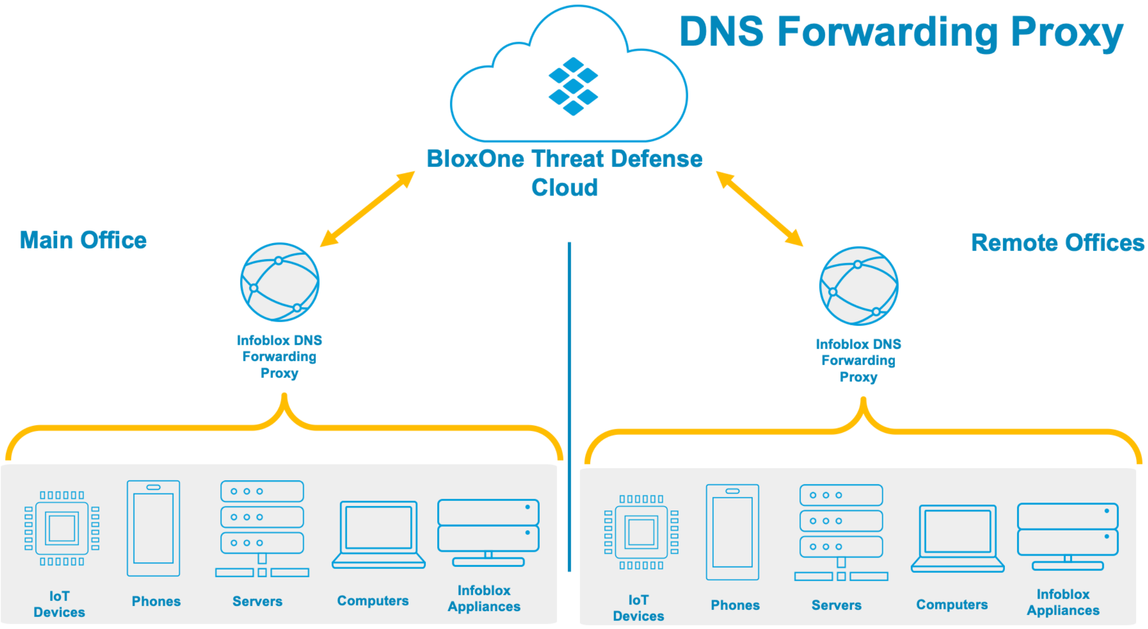
DNS Forwarding Proxy

General Overview

For remote office deployments or in cases where installing an endpoint agent is not desirable or possible, it’s best to use the DNS Forwarding Proxy. It is a software that runs on bare-metal, VM infrastructures, or Infoblox NIOS appliances; and it embeds the client IPs in DNS queries before forwarding them to BloxOne Threat Defense Cloud. The communications are encrypted, and client visibility is maintained. The DNS Forwarding Proxy also provides DNS resolution to local DNS zones when organizations configure local resolvers. Once organizations set up an DNS Forwarding Proxy, it becomes the main DNS server for the organizations remote site. It will also cache responses to speed resolution of future queries.

By implementing the DNS Forwarding Proxy, organizations can rest assured that BloxOne Threat Defense Cloud effectively enforces DNS client-based security policies at organizations remote sites. On-premises devices that send DNS queries reveal their actual client IP addresses (instead of their NAT IP address), which allows BloxOne Threat Defense Cloud to apply the security policies applicable to the respective endpoints and identify infected clients.

Structure



Infoblox BloxOne Threat Defense Cloud is a SaaS offering designed to provide protection to devices on and off-premises, including roaming, remote, and branch offices. It provides visibility into infected and compromised devices, prevents DNS-based data exfiltration, and automatically stops device communications with command-and-control servers (C&Cs) and botnets, in addition to providing recursive DNS services in the cloud. organizations can access the services by deploying the DNS forwarding proxy.

Guides

Deploying DNS Forwarding Proxy:
https://docs.infoblox.com/display/BloxOneThreatDefense/Deploying+DNS+Forwarding+Proxies

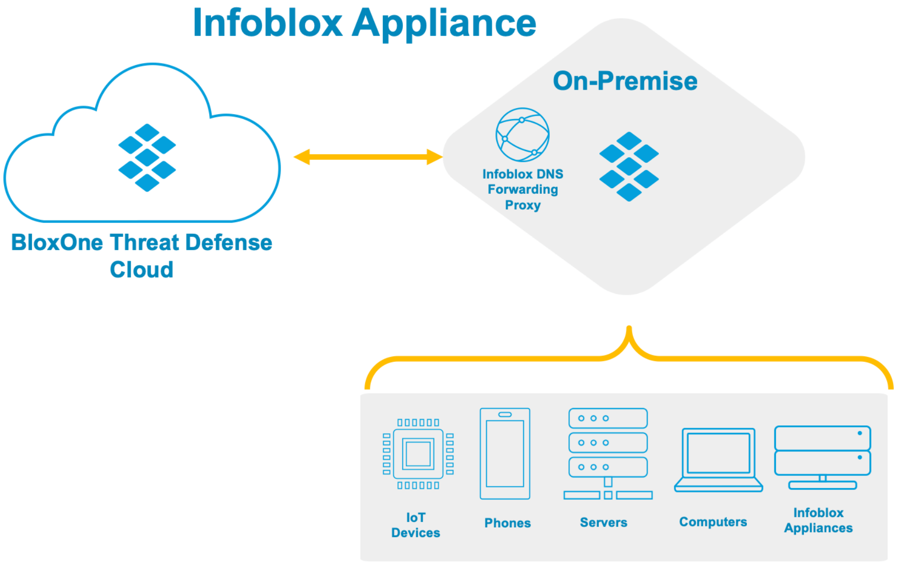
Infoblox Appliance

General Overview

If the organizations network infrastructure consists of an On-Prem Infoblox Grid, they can select any Grid member to function as a DNS forwarder. This gives the ability to configure the firewall to allow Infoblox appliances to communicate with external DNS servers and enable DNS recursion on the member. organizations can define a list of forwarders for all appliances, individual appliances, or individual groups inside the appliance.

By implementing the Infoblox DNS Forwarding Proxy on the Infoblox appliance, organizations can rest assured that BloxOne Threat Defense Cloud effectively enforces DNS client-based security policies at their remote sites. On-premises devices that send DNS queries reveal their actual client IP addresses (instead of their NAT IP address), which allows BloxOne Threat Defense Cloud to apply the security policies applicable to the respective endpoints and identify infected clients.

Structure



Infoblox BloxOne Threat Defense Cloud is a SaaS offering designed to provide protection to devices on and off-premises, including roaming, remote, and branch offices. It provides visibility into infected and compromised devices, prevents DNS-based data exfiltration, and automatically stops device communications with command-and-control servers (C&Cs) and botnets, in addition to providing recursive DNS services in the cloud.

For remote office deployments, or in cases where installing an endpoint agent is not desirable or possible and the organization is currently using Infoblox for DNS, using the DNS Forwarding Proxy on the Infoblox appliances the best option. It is a software application that runs on the Infoblox NIOS appliances and embeds the client IPs in DNS queries before forwarding them to BloxOne Threat Defense Cloud. The communications are encrypted, and client visibility is maintained. The proxy also provides DNS resolution to local DNS zones when organizations configure local resolvers. Once organizations set up a DNS forwarding proxy, it becomes the main DNS server for their sites. It will also cache responses to speed resolution of future queries.

Guides

Configuring BloxOne Threat Defense Cloud Destination:
https://docs.infoblox.com/display/IDCUG/Configuring+ActiveTrust+Cloud+Destination

Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to cloud and hybrid systems, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com