BLOX FEST

Infoblox

Hardening DNS: How to Configure Your DNS Infrastructure to Defend Itself

Hardening DNS: How to Configure Your DNS Infrastructure to Defend Itself

- Panel **Moderator:**
  Srikrupa Srivatsan, Senior Product Marketing Manager, Infoblox

- Panel:
  Victor Mejia, Bestel
  Wayne Dake, Fidelity National Information Services

  Philip Parker, Senior Technical Marketing Engineer, Infoblox

The Volumetric Challenge to DNS Infrastructure

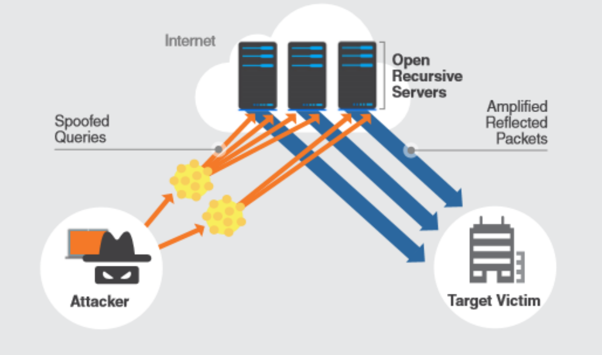
DNS attacks

78%	The most common service targeted by application layer attacks is now, for the first time, DNS [1]
84%	Of reflection/ amplification attacks use DNS [1]
>$500	Per minute cost of internet downtime due to DDoS attack [1]
$1.5M	Average total cost per year to deal with denial of service attacks [2]

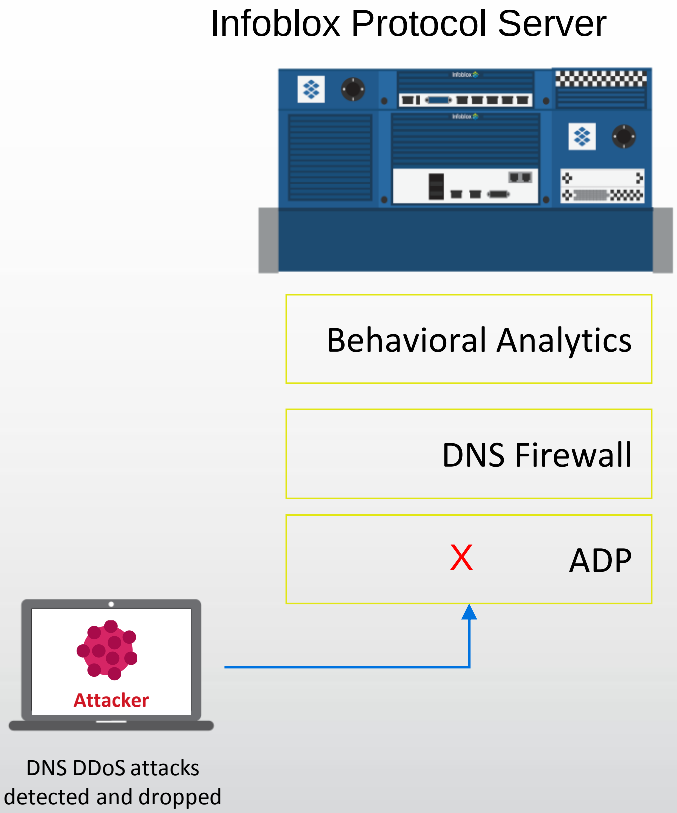
Sources:
1.Arbor WISR2016 report
2. Ponemon Institute Study – The cost of denial-of-services attacks, March 2015

How a DNS attack works

A distributed reflection attack uses third-party open resolvers on the Internet to unwittingly participate in attacks against a target. These types of attacks use reflection and amplification techniques to spoof their identity and increase the magnitude and effectiveness of an attack. Authoritative name servers can also be used for this attack. Attackers send their spoofed queries to multiple open recursive servers—sometimes thousands of servers at a time. Each query is designed to elicit a large response and send an overwhelming amount of data to the victim’s IP address. When a victim is hit by the attack, it can cause slow performance or site outages that can shut down important business processes.



Advanced DNS Protection - DDoS and Attack Mitigation



Infoblox Protocol Server

DNS DDoS attacks detected and dropped

- Purpose-built deep packet inspection hardware examines each protocol query
  - All protocols, including OSPF and BGP for anycast
- Detects malformed “packets of death” and other exploits
- Sophisticated rate limiting algorithms detect and discard DDoS attack traffic
- No impact on appliance, regardless of attack volume, up to line rate.
- Successfully stops volumetric DNS tunnels designed to bypass paywalls, and ISP enforced data caps.

Infoblox ADP Appliances

- The following hardware Appliances have the ADP feature set.
  - PT-1400, PT-2200, PT-4000
  - IB-4030
- These appliance are particular suited to survive volumetric attacks

ADP Deployments

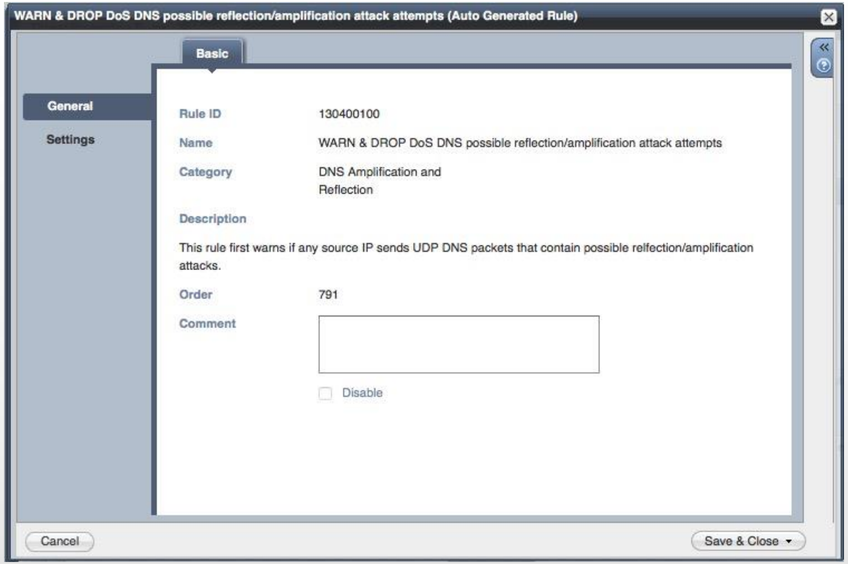
- Multiple Infoblox appliance deployment methods within
  - Enterprise internal recursive
  - Enterprise external authoritative environments
  - Service Provider recursive
  - Service Provider authoritative (MSSP)

  - Mixed use case – look at a Hospital System
    - Internal Authoritative/Recursive for Staff
    - Internal Authoritative/Recursive for Equipment
    - Authoritative/Recursive for Patients and Guests

ADP Rule Categories

- BGP
- BLACKLIST DROP TCP IP prior to rate limiting
- BLACKLIST DROP UDP IP prior to rate limiting
- BLACKLIST TCP FQDN lookup
- BLACKLIST UDP FQDN lookup
- DHCP
- DNS Amplification and Reflection
- DNS Cache Poisoning
- DNS DDoS
- DNS Malware
- DNS Message Types
- DNS Protocol Anomalies
- DNS Tunneling
- Default Pass/Drop
- General DDoS
- HA Support
- ICMP
- NTP
- OSPF
- Potential DDoS related Domains
- RATE LIMITED TCP FQDN lookup
- RATE LIMITED TCP IP
- RATE LIMITED UDP IP
- Reconnaissance
- **TCP/UDP Floods**
- WHITELIST PASS TCP IP prior to rate limiting
- WHITELIST PASS UDP IP prior to rate limiting
- WHITELIST TCP domain
  WHITELIST UDP domain

WARN & DROP DoS DNS possible reflection/amplification attack attempts


WARN & DROP DoS DNS possible reflection/amplification attack attempts (Auto Generated Rule)

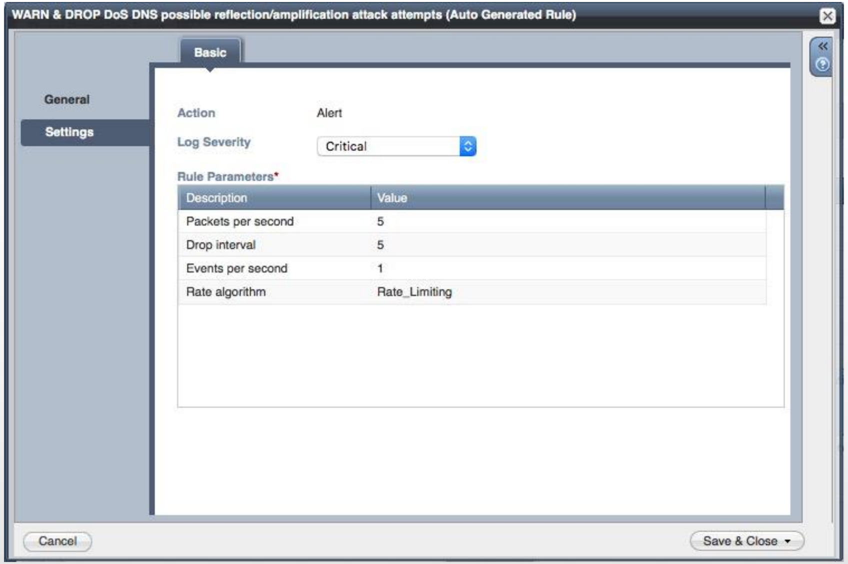
Rule ID	130400100
Name	WARN & DROP DoS DNS possible reflection/amplification attack attempts
Category	DNS Amplification and Reflection

Description

This rule first warns if any source IP sends UDP DNS packets that contain possible relfection/amplification attacks.

Order	791
Comment	

□ Disable

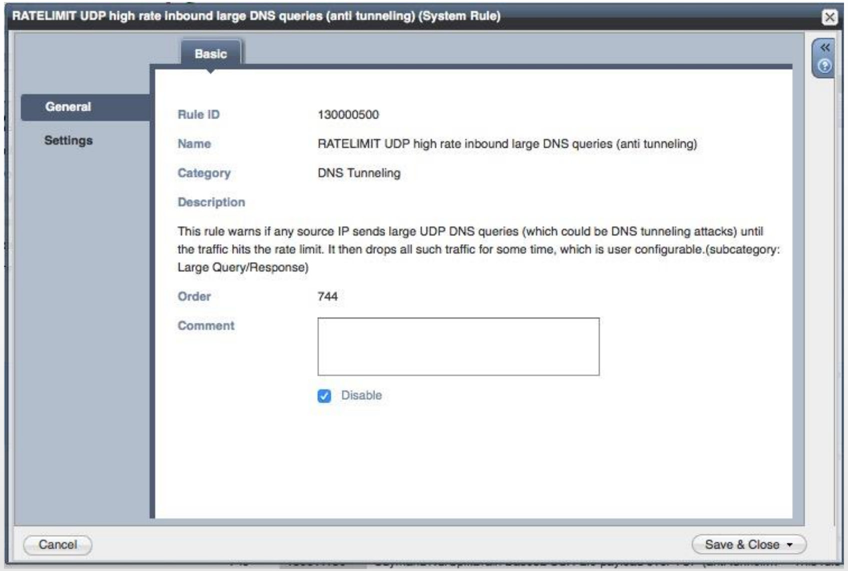

WARN & DROP DoS DNS possible reflection/amplification attack attempts (Auto Generated Rule)

Action	Alert
Log Severity	Critical

Rule Parameters*

Description	Value
Packets per second	5
Drop interval	5
Events per second	1
Rate algorithm	Rate_Limiting

RATELIMIT UDP high rate inbound large DNS queries (anti tunneling)



RATELIMIT UDP high rate inbound large DNS queries (anti tunneling) (System Rule)

Rule ID	130000500
Name	RATELIMIT UDP high rate inbound large DNS queries (anti tunneling)
Category	DNS Tunneling

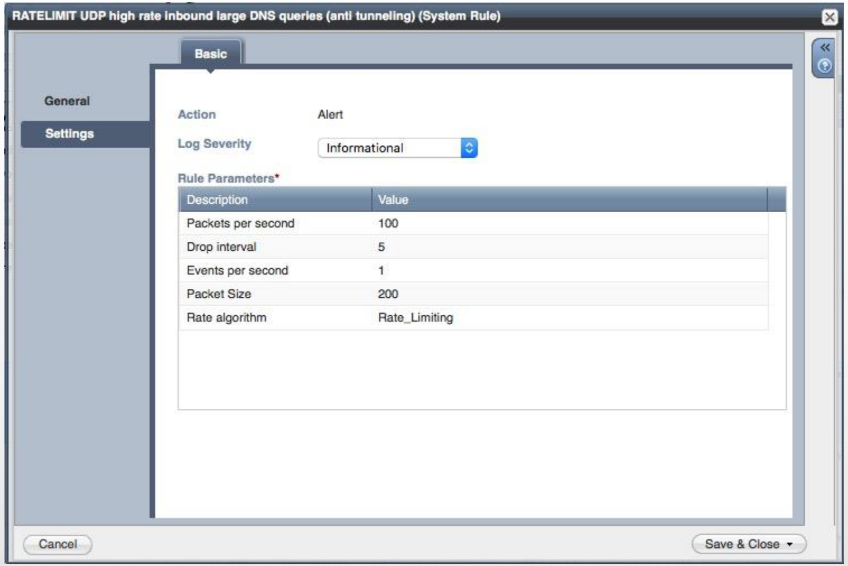
Description

This rule warns if any source IP sends large UDP DNS queries (which could be DNS tunneling attacks) until the traffic hits the rate limit. It then drops all such traffic for some time, which is user configurable.(subcategory: Large Query/Response)

Order 744

Comment

☑ Disable



RATELIMIT UDP high rate inbound large DNS queries (anti tunneling) (System Rule)

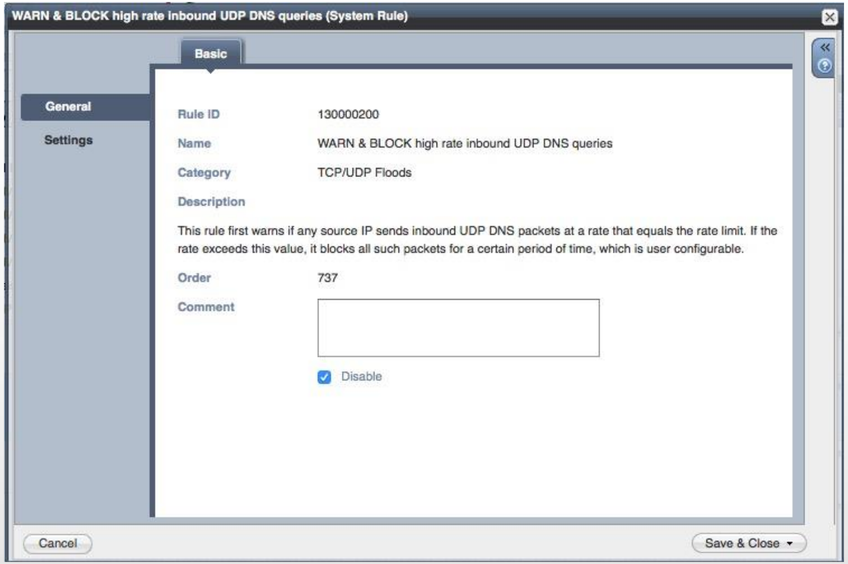
Action Alert

Log Severity Informational

Rule Parameters*

Description	Value
Packets per second	100
Drop interval	5
Events per second	1
Packet Size	200
Rate algorithm	Rate_Limiting

WARN & BLOCK high rate inbound UDP DNS queries



WARN & BLOCK high rate inbound UDP DNS queries (System Rule)

Rule ID 130000200

Name WARN & BLOCK high rate inbound UDP DNS queries

Category TCP/UDP Floods

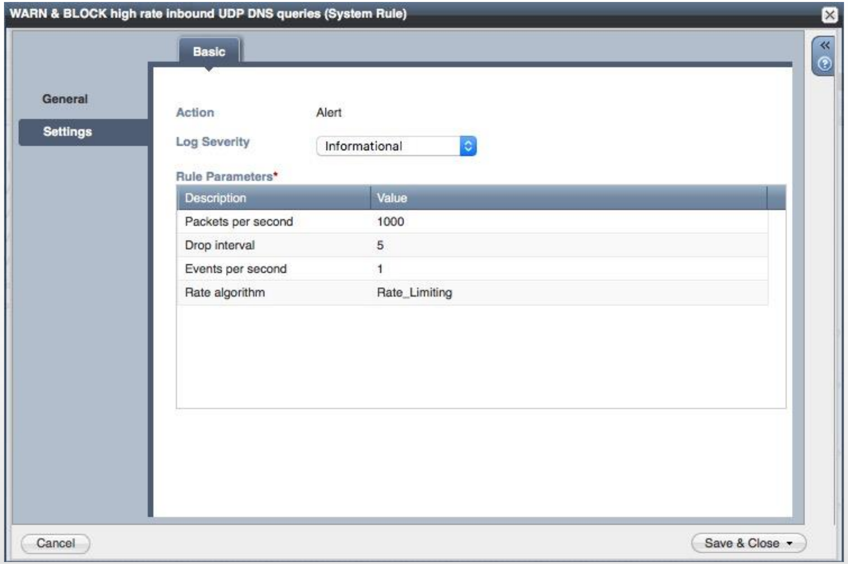
Description

This rule first warns if any source IP sends inbound UDP DNS packets at a rate that equals the rate limit. If the rate exceeds this value, it blocks all such packets for a certain period of time, which is user configurable.

Order 737

Comment

☑ Disable



WARN & BLOCK high rate inbound UDP DNS queries (System Rule)

Action Alert

Log Severity Informational

Rule Parameters*

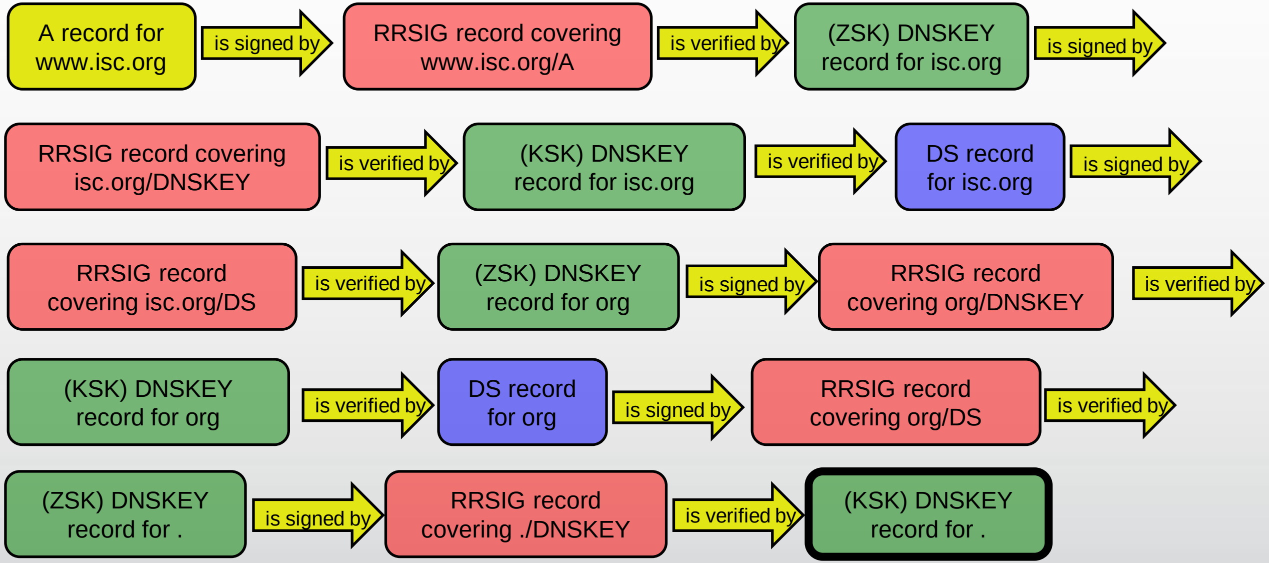
Description	Value
Packets per second	1000
Drop interval	5
Events per second	1
Rate algorithm	Rate_Limiting

DNSSEC

- The DNS Security Extensions, or DNSSEC, use asymmetric cryptography to “digitally sign” DNS zone data
- This provides
  - Authentication of DNS data (“Was this data signed by the administrator of the zone?”)
  - Integrity checking of DNS data (“Is this the same data that was signed by the administrator of the zone?”)
- This protects against Cache Poisoning …
- But … anything else

DNSSEC Validation

- In DNSSEC validation, a recursive name server verifies all of the signatures from the answer back to the closest *trust anchor* (a public key it knows and trusts)
  - When DNSSEC is fully deployed, the only trust anchor necessary will be the root’s public key
  - Validation can take a lot of steps, assuming a cold cache, www.isc.org



A record for www.isc.org → is signed by → RRSIG record covering www.isc.org/A → is verified by → (ZSK) DNSKEY record for isc.org → is signed by →

RRSIG record covering isc.org/DNSKEY → is verified by → (KSK) DNSKEY record for isc.org → is verified by → DS record for isc.org → is signed by →

RRSIG record covering isc.org/DS → is verified by → (ZSK) DNSKEY record for org → is signed by → RRSIG record covering org/DNSKEY → is verified by →

(KSK) DNSKEY record for org → is verified by → DS record for org → is signed by → RRSIG record covering org/DS → is verified by →

(ZSK) DNSKEY record for . → is signed by → RRSIG record covering ./DNSKEY → is verified by → (KSK) DNSKEY record for .

BLOX FEST

Infoblox