What the Heck is a Domain Name Registry Doing in Cybersecurity?

Presented by: Sarah Brimacombe

cira

BUILDING A BETTER ONLINE CANADA

.CA

2.7 million .CA domains with 100% uptime.

Cybersecurity Services

100,000 new cybersecurity threats blocked daily by D-Zone Firewall.

Registry Services

Robust top-level domain products and services.

We support initiatives that enhance Canadians' internet experience:

Global Internet Leadership	• Support internet governance and standards through global organizations such as ICANN and CENTR
Canadian Initiatives	• **11** Internet Exchange Points nation-wide • **280,000+** internet performance tests conducted last year
Community Initiatives	• More than **$4.2 million** in grants to **102** projects through our Community Investment Program

.ca CANADA'S DOMAIN

choose CANADA

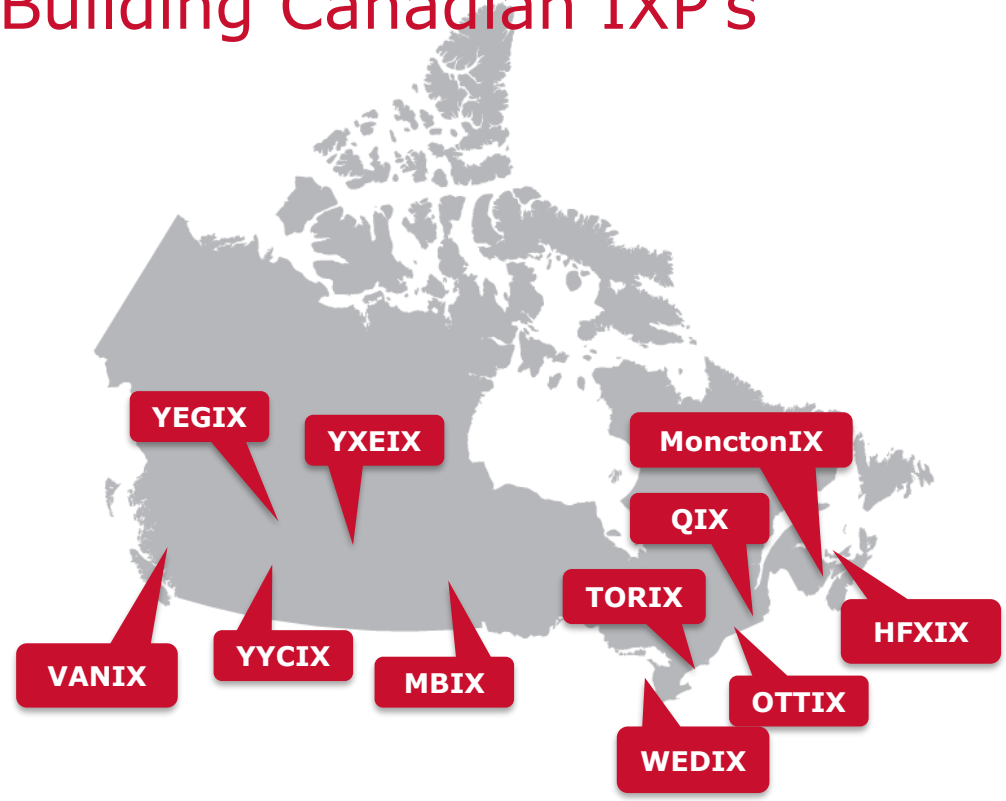
CIRA Building Canadian IXP's

- Help support a cross-country network of Internet Exchange Points

✓ Faster

✓ More Reliable

✓ Sovereign



Community Investment Program

Providing funding for technology based projects and research

- North Island College Centre for Applied Research Technology and Innovation
- Digital Literacy grant
- Youth summer bot camps to expose up to 200 students to programming robotics

- The International Cybercrime Research Centre at Simon Fraser University
- Develop a custom web-crawler to automatically locate websites hosting child exploitation content

- The University of Victoria's Indigenous Law Research Unit
- Produce a video series to provoke and support more complex conversations about Indigenous law and legal issues including, gender, power, sexuality, fairness, community relations, inclusion, safety, change and adaptation and accessibility

Bridging the gap to secure your DNS

DNS IS MISSION CRITICAL

DNS is a mission critical service that requires 100% uptime and low latency

- During a DNS outage websites, web applications, and email are down
- DNS outages result in brand damage and/or lost revenue
- DNS lookups contribute to website performance

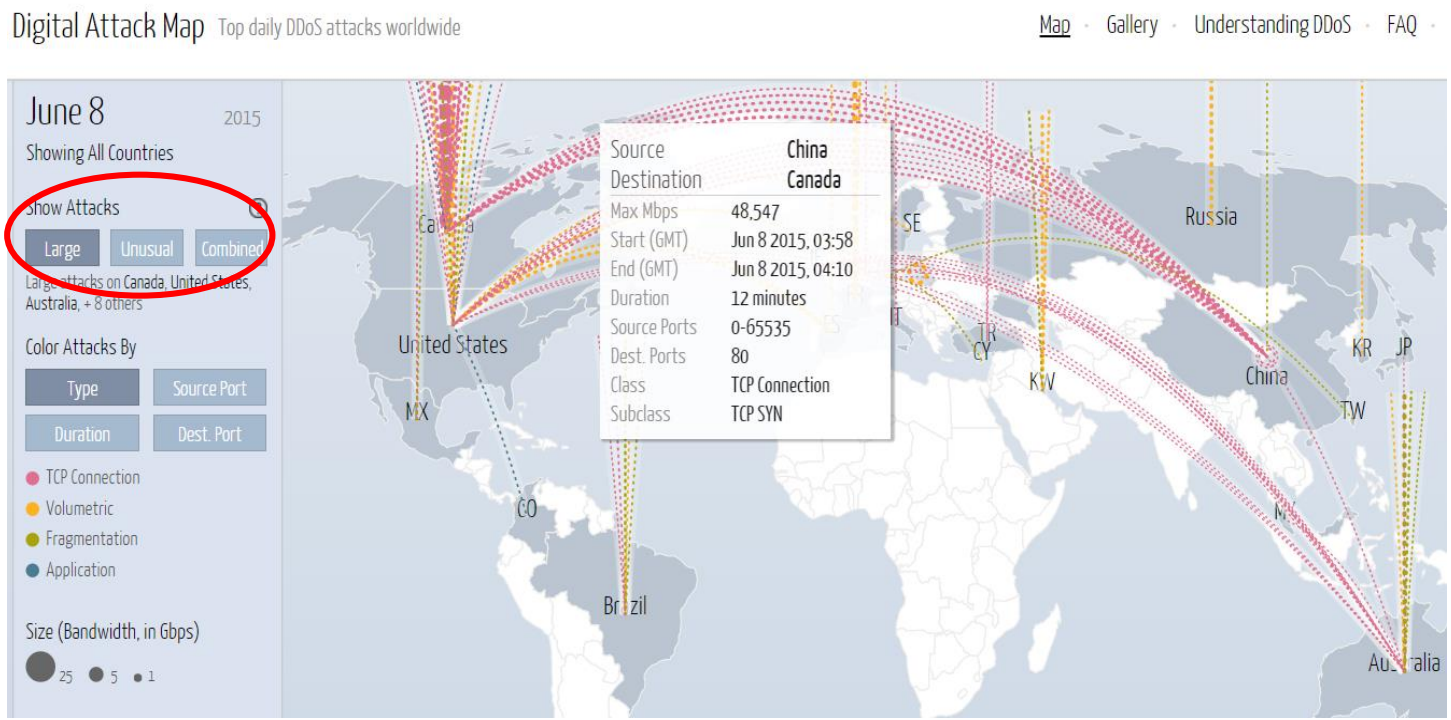
DNS IS VULNERABLE

DNS is vulnerable to failures and attack

- Numerous Failure Mechanisms
  - Equipment failure
  - Network outages
  - Natural disasters
  - Need diversity

- DNS based DDOS Attacks account for 30% of all attacks
  - DNS as the target
  - DNS as the attack vector
  - DNS attacks are easy to generate and hard to defend

DDOS Attacks continue to grow as a major threat to online initiatives



D-Zone anycast global secondary DNS

- Launched 3.5 years ago
- Specifically architected to support Canadians
- Supports all domains; .ca, .com, .net, .org, etc…

BCNET has partnered with CIRA and purchased D-Zone anycast secondary DNS on behalf of all of their members

D-Zone supporting over 160 Canadian schools

THOMPSON RIVERS
UNIVERSITY

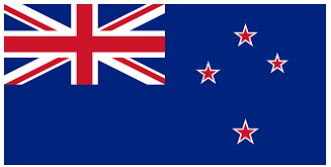
uOttawa

MountAllison
UNIVERSITY

Queen's University

Aruba .AW, Canada .CA, Cayman Islands .KY, Costa Rica .CR, Denmark .DK, Netherlands .NL, New Zealand .NZ, Niue .NU, Portugal .PT, Saint Martin .SX, Sweden .SE











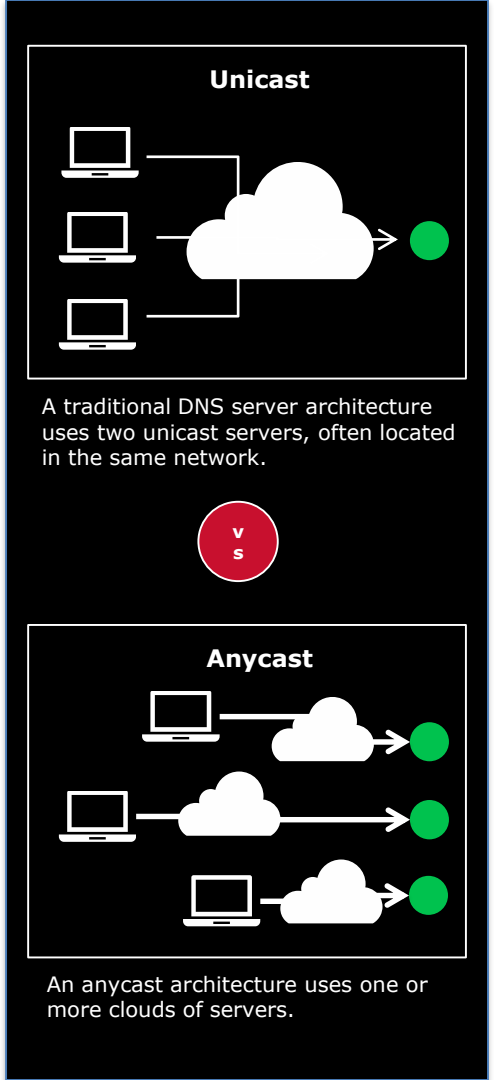

ANYCAST DNS VS UNICAST

Unicast – Traditional DNS deployments

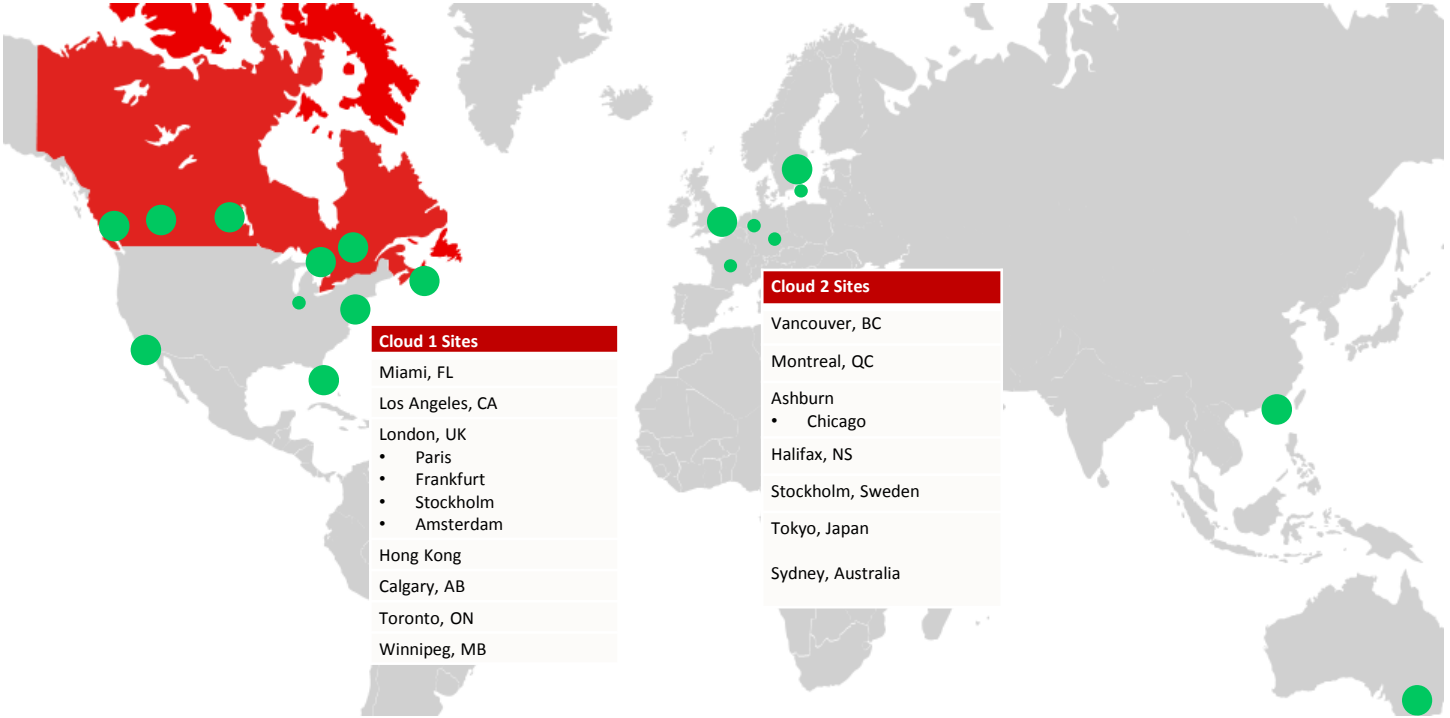
- Nameservers are implemented on single nodes, each with a unique IP address

Anycast – Adding resiliency to your DNS

- Nameservers are implemented on a multiple geographically distributed nodes that share a single IP address
- Layer 3 routing sends packets to the geographically nearest nameserver
- Built in redundancy, failover and load distribution
- Resiliency to DDOS attacks
- Redundancy and fault tolerance
- Enhanced web performance



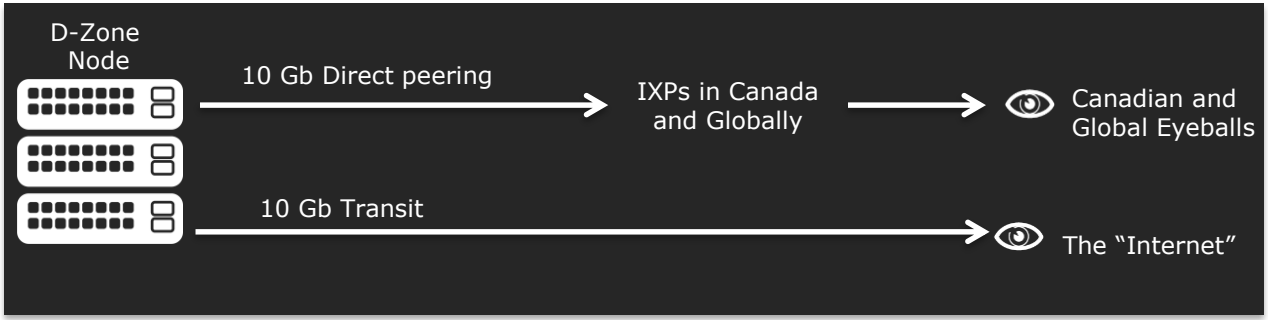
A GLOBAL ANYCAST DNS SERVICE THAT PUTS CANADA AND CANADIAN TRAFFIC FIRST



24 globally distributed nodes with a coast-to-coast Canadian footprint

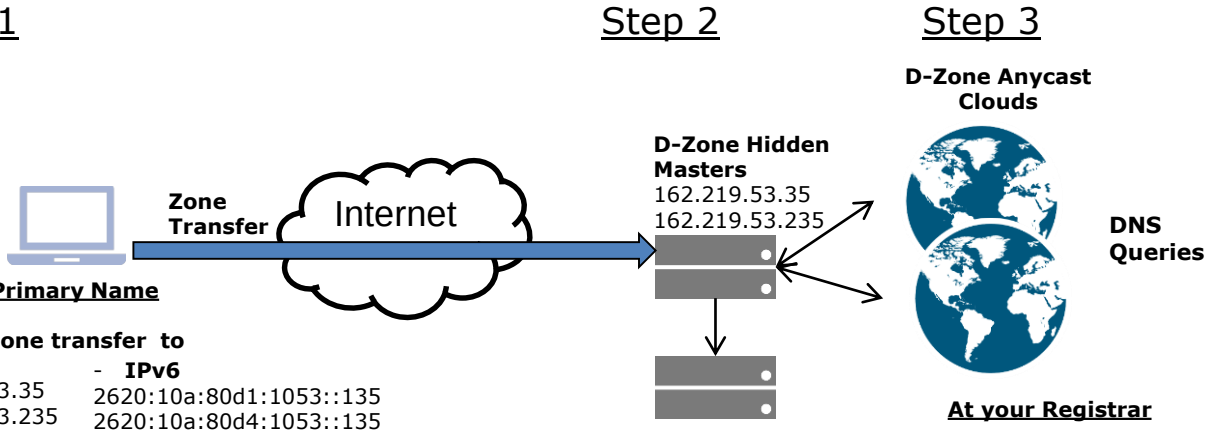
D-Zone Anycast Architecture Highlights

- 2 Anycast Clouds
- 2 diverse transit providers
  - Hurricane Electric
  - GTT
- **3,000 peering relationships globally**
- Diverse management transit
- 2 load shared DNS servers at each site
- Out of band reporting and data collection

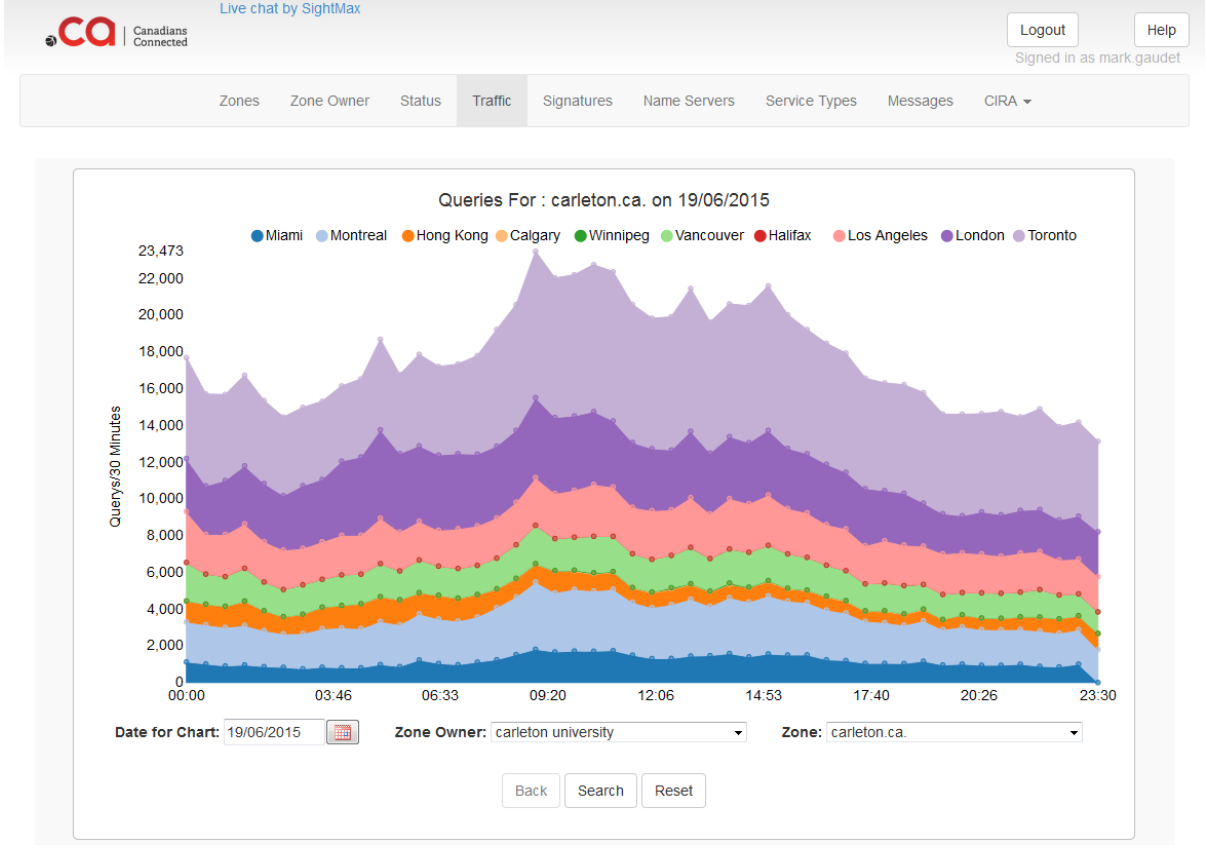


How D-Zone Anycast Works…

D-Zone anycast DNS – operational flow



Example of DNS Traffic Via D-Zone Web Portal



D-Zone anycast includes unlimited queries and 24/7 premium tech support

Contacting Support:

- Email address: Support@d-zone.ca
- Email address: Dnsfirewall@d-zone.ca
- Phone: 1 (844) 863-9663
- Live chat: available at portal.d-zone.ca
- Emergency off-hours support: (613) 237-0324

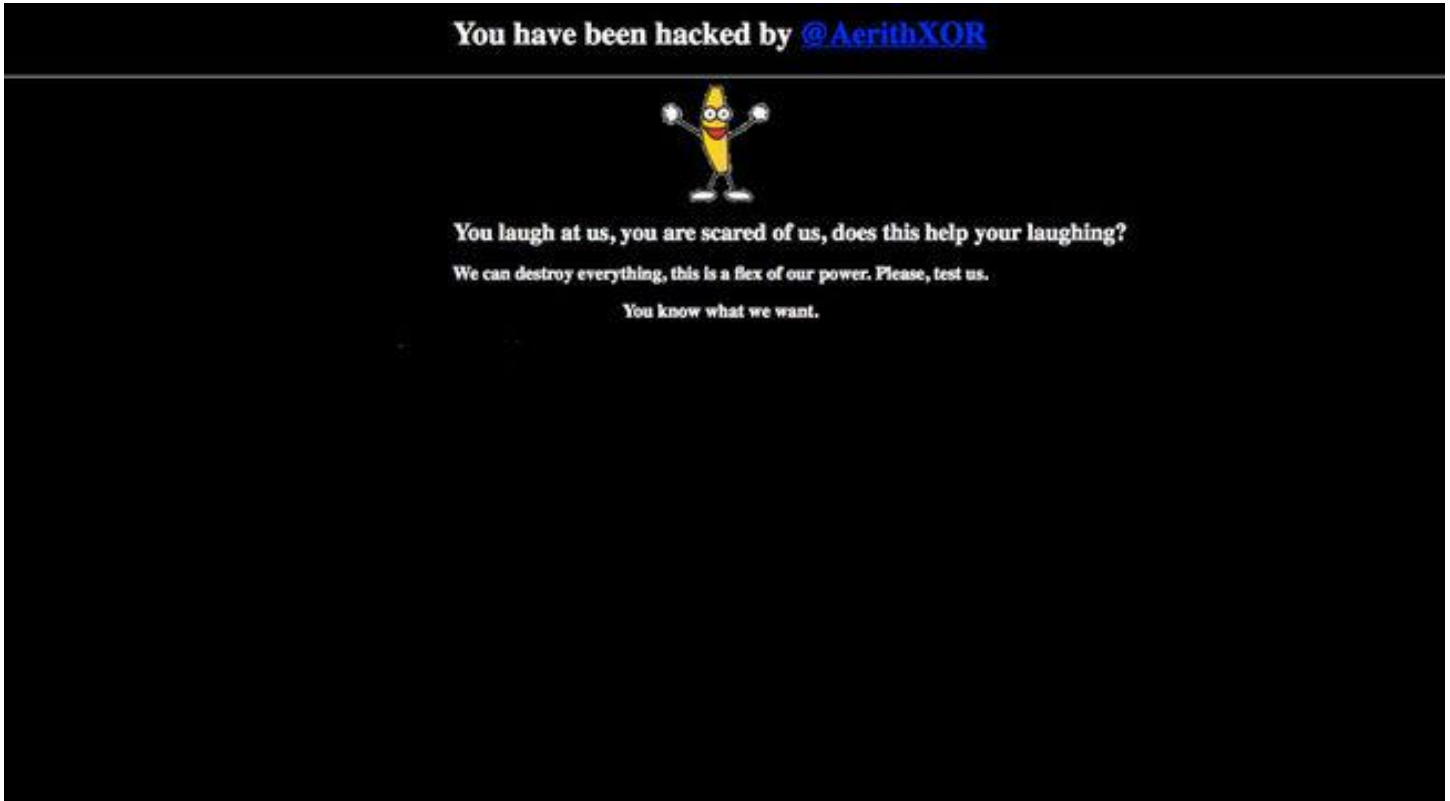
Steps to implementing

- Complete the service agreement (no cost)
- Schedule a 30 minute technical call
- We’ll walk you through the portal and live provision your zones with you

…moving forward

DOMAIN LOCK

It looks like this hack on Canadian city…



…or maybe it was “Hammer Time” affecting one of our provincial governments

Domain Hijacking

Domain hijacking can be done in several ways, by exploiting a vulnerability in the registration process when accessing the domain record at the registrar through social engineering.

- *Hijacking can be executed through;*
  - Social engineering
  - Security breach at the registrar
  - Malicious act from within your organization

- *Risks Include:*
  - Theft of valuable client login information
  - Complete domain theft
  - Email takeover – send and receive your emails

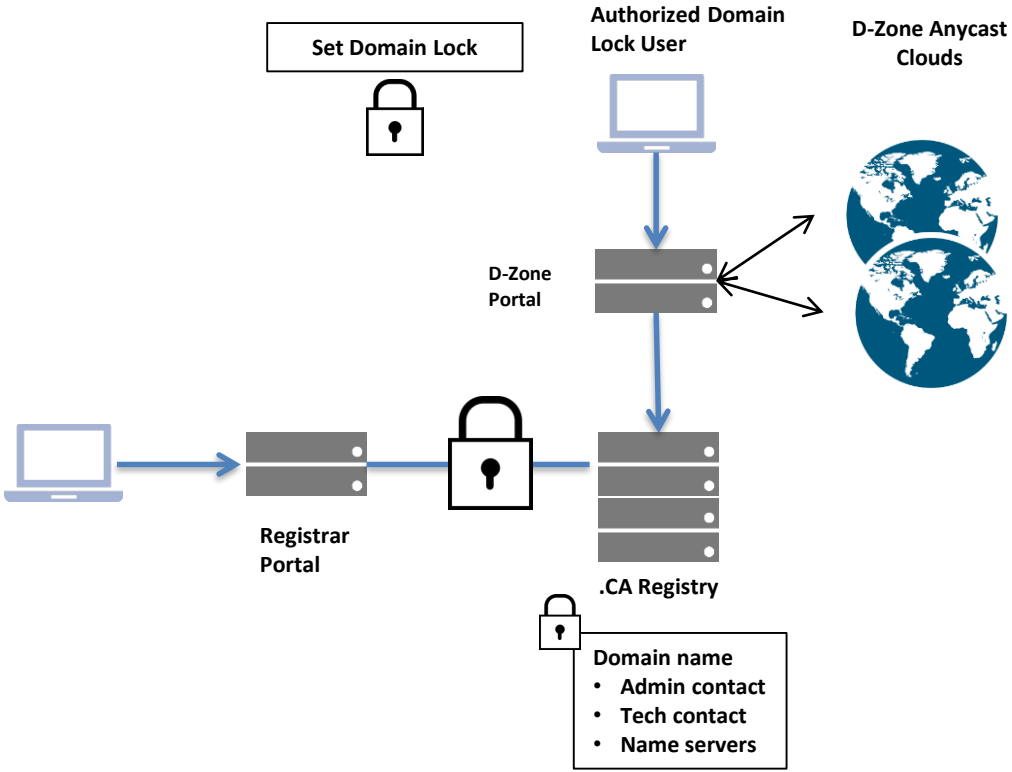
Preventing Domain Hijacking

Domain Lock fully protects from hijacking

- Applies security lock at the registry level
  - Prevents any changes to domain name information
  - Protects from compromise of your registrar account
  - Protects from registrar security breach

- *It is easy to fully protect your domains*
  - Only the owner and admin of the domain can make changes
  - Two factor authentication mandatory as a guard against spoofing

D-Zone Domain Lock operational flow



…and we keep moving forward

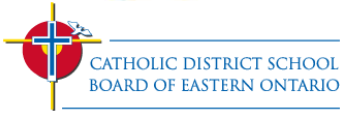
Common problems our base is facing now

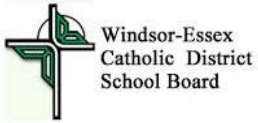
- ISP DNS recursive server outages
- Inefficient routing to CDN content
- Web content filtering scaling with bandwidth
- Protection from malware and ransomware
- Requirement: Affordable secure and highly available recursive DNS service

Malware Protection with Built-in Content Filtering

Keep malware off the network and block communication to command and control with the D-Zone DNS Firewall

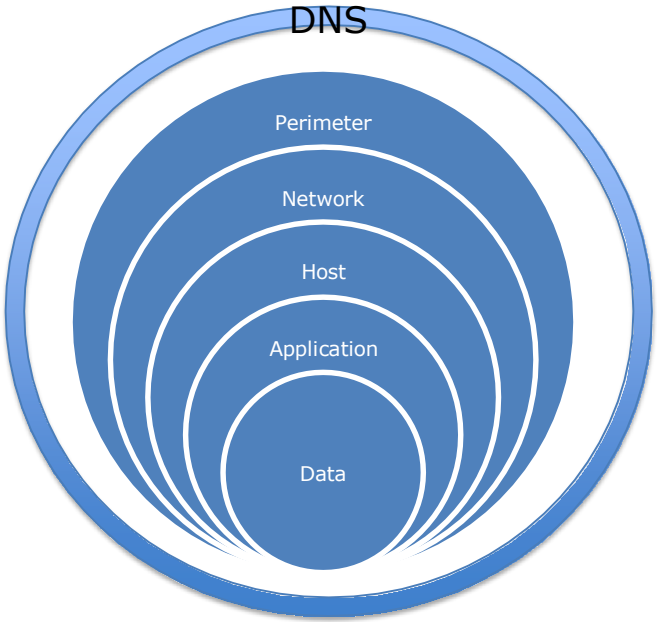
D-Zone firewall protecting Canadian education



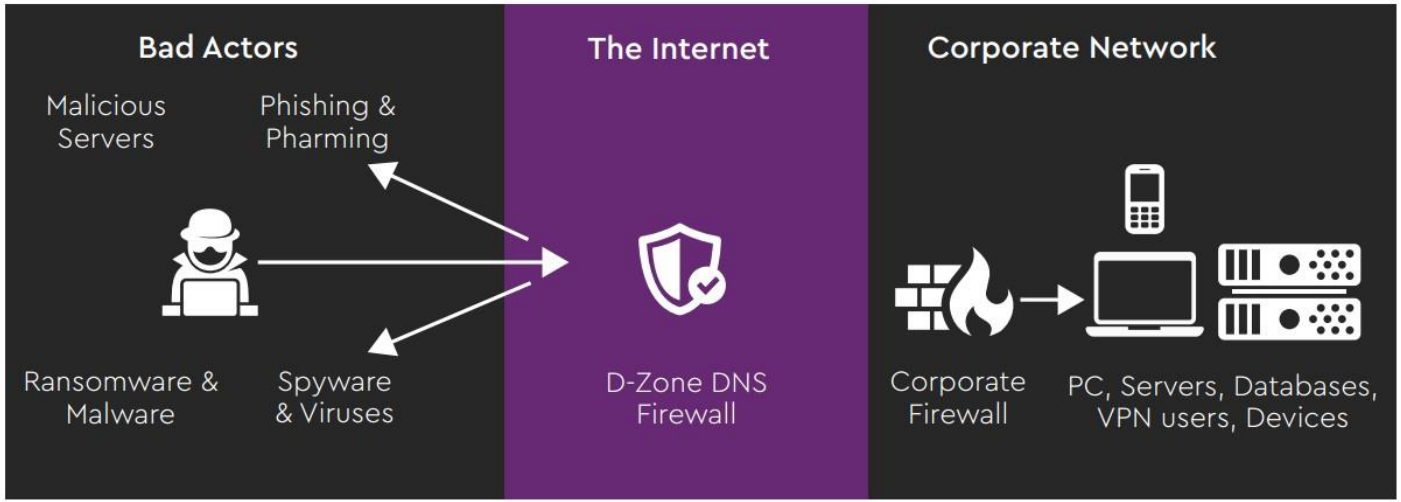


DNS IS THE FABRIC OF THE INTERNET

- DNS is part of a multi-layer defence in depth approach
  - 91.3% of malware uses DNS
  - DNS is used for command and control
  - Endpoint protection
- is limited
  - IoT
  - BYOD



D-ZONE FIREWALL RECURSIVE DNS DIAGRAM



Detect
Real time and analysis of global DNS data to detect threats

Feed
Policy enabled recursive DNS servers are updated with threat feeds

Enforce
Servers examine DNS transactions and block domain and IP security threats

Report
Malicious activity is identified and reported

Mitigate
IT managers can located and quarantine infected devices

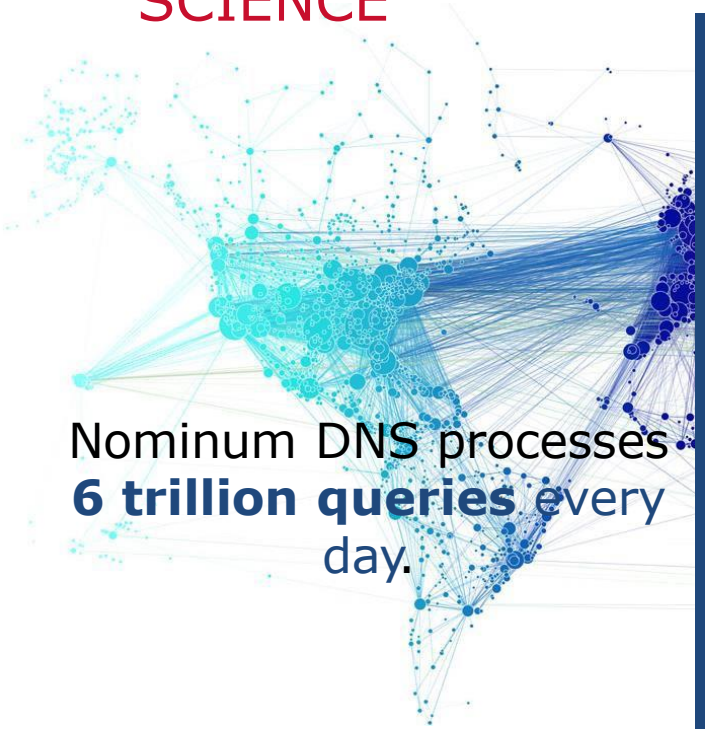
To make this amazing we found an amazing partner!

Leader in DNS – AKAMAI

100+ **providers**
40+ **countries**

sourced from Nominum

COMPETITIVE ADVANTAGE IS DATA SCIENCE



Nominum DNS processes **6 trillion queries** every day.

More than 400x the combined daily volume of Tweets, Facebook likes, and Google searches.

Detect - identify global threats

- Global Intelligence Exchange (GIX) analyzes;
  - 100 billion global DNS queries daily
  - Real-time analysis
    - Rapidly classify anomalous activity
    - Rigorously validate suspected threats

FEED - PROACTIVE REAL TIME SECURITY FEEDS

- Block lists are constantly updated and fed to DNS servers real time
  - Combination of lists from
    - 3rd party external lists
  - Lists generated from DNS data
    - 20 minutes from detection to block list
    - 95,000 domains added daily

ENFORCE

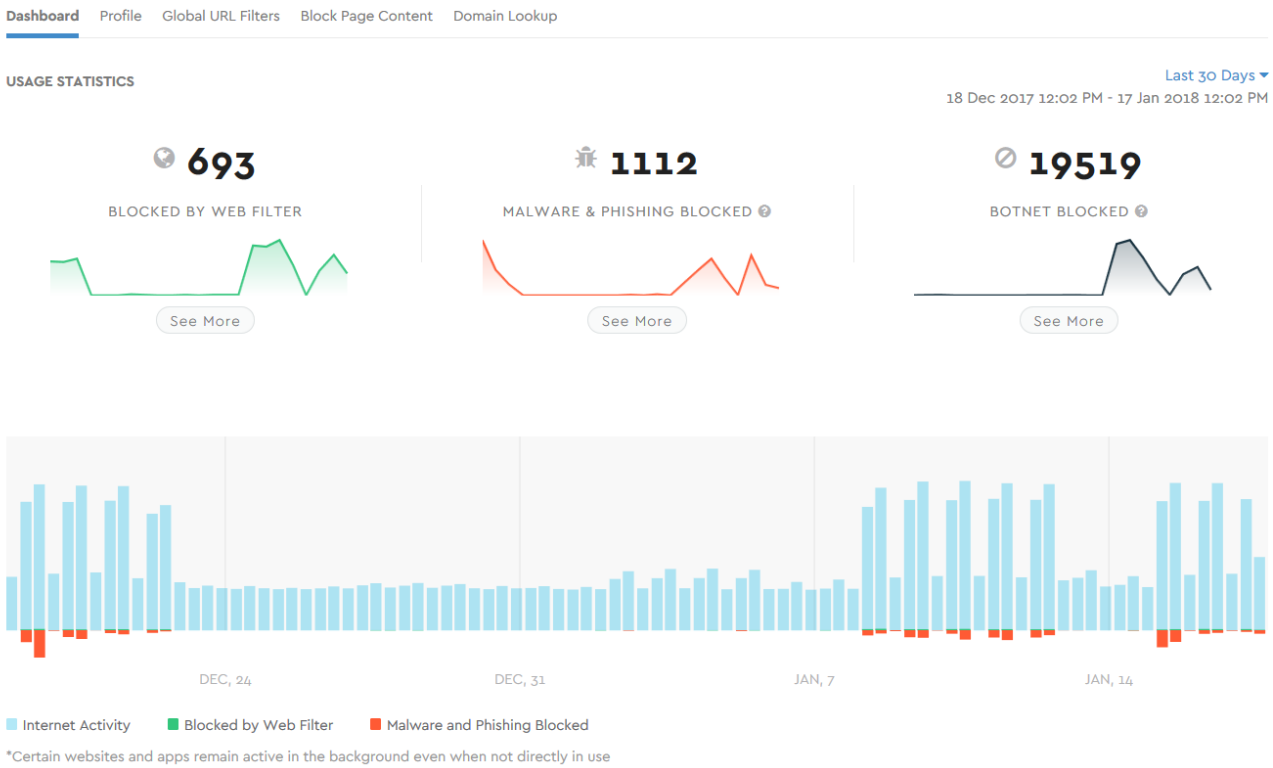
- Policy enabled caching recursive DNS servers
  - Compare incoming DNS queries against lists
  - Blocked queries are redirected to a web page
  - Real time updated lists

REPORT AND MITIGATE

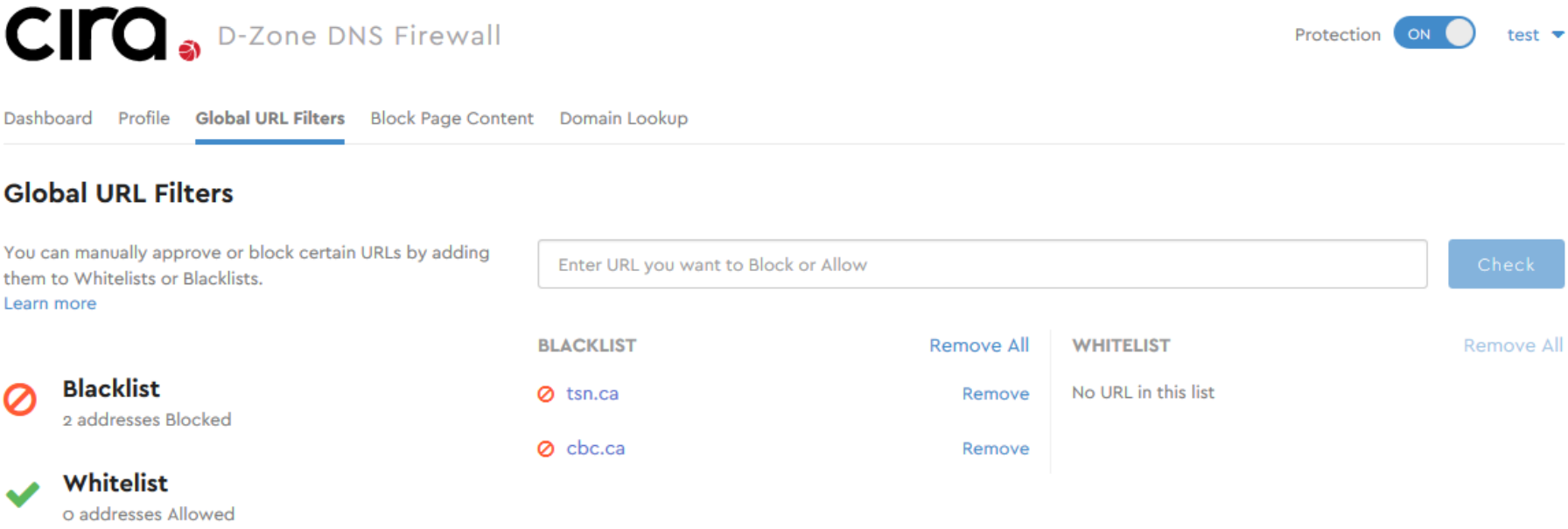
- DNS query traffic

- Detect and report malware
  - What queries were blocked
  - What threats were they associated with

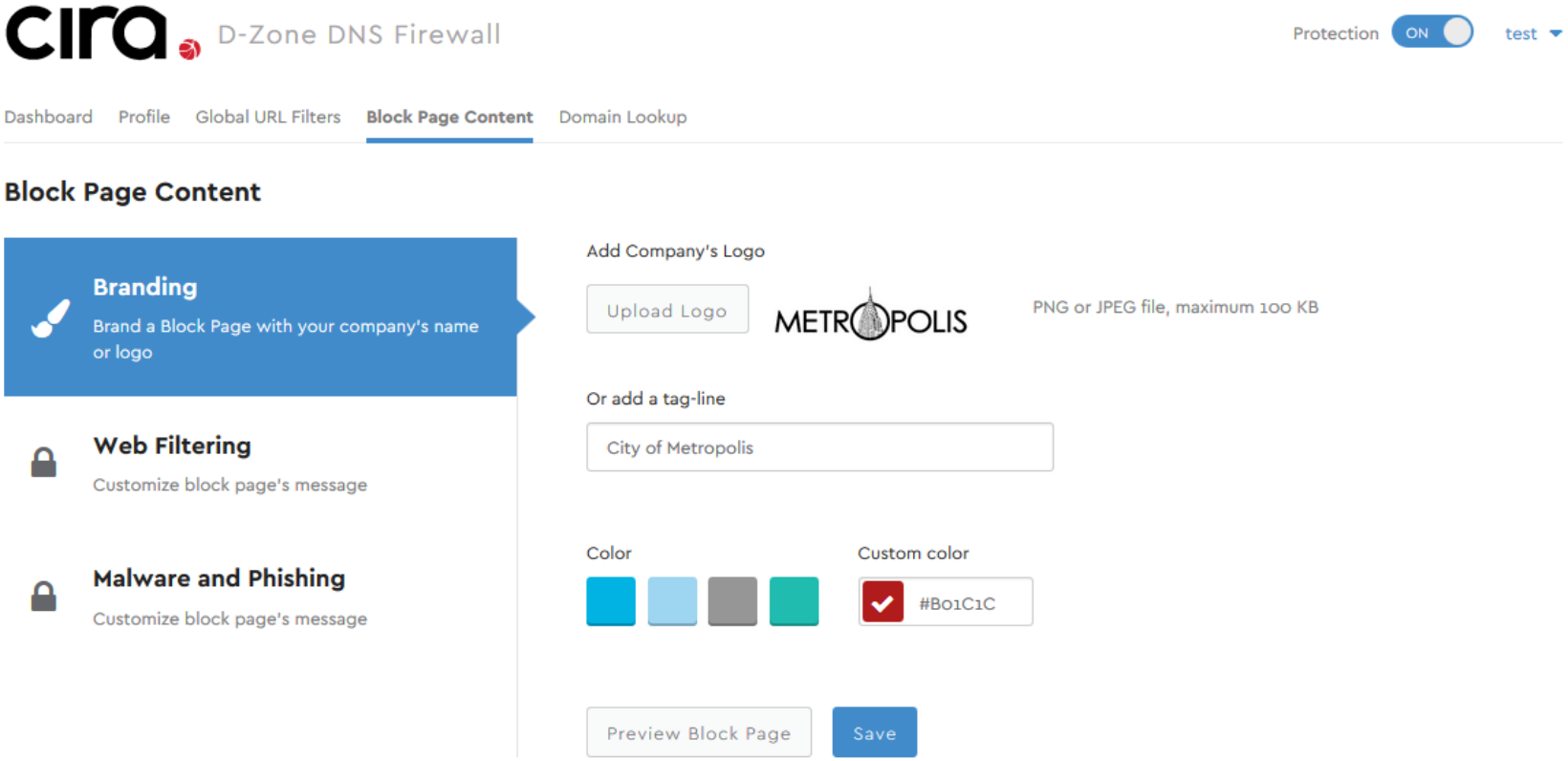
D-Zone blocking malware and ransomware



Total control over content filtering options



CUSTOMIZE YOUR BLOCK PAGES



D-Zone firewall recursive DNS deploying across Canada
*connecting to local IXP's

- Help support a cross-country network of Internet Exchange Points

✓ Faster

✓ More Reliable

✓ Sovereign

Configuring D-Zone Firewall = 4 Steps

Step 1. Provide me the IP address from which your DNS queries will be routed. In addition we need the IP address for all possible egress points from your network.

Step 2. Log in to the D-Zone Firewall portal to perform the following:

a. Configure your web filters

b. Enable Google Safe Search

c. Enable Malware and Phishing Protection

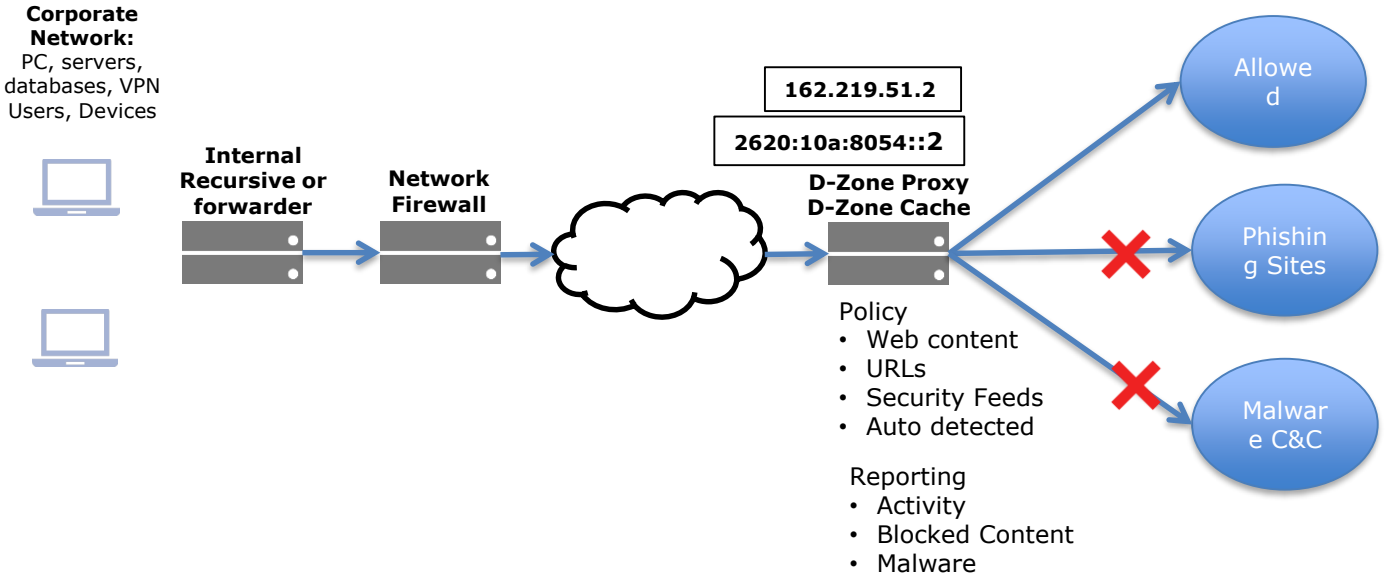
Step 3. Save your settings

Step 4. Direct your DNS queries to D-Zone using the following IP anycast addresses:

IPv4 162.219.51.2

IPv6 2620:10a:8054::2

D-Zone firewall operational flow – step 4



D-ZONE RECURSIVE DNS FIREWALL & CONTENT FILTERING

- ✓ Cloud based - easy to implement with no hardware or software install
- ✓ Automatically updated block lists protect from new threats that appear globally within minutes
- ✓ Cost effective for Canadian higher education
- ✓ Based in Canadian IXPs
- ✓ You're all welcome to an evaluation – we'd love to hear your feedback

Wendy Blake from Thompson Rivers University

THANK YOU!