

Switch DNS Firewall

First layer of protection

More security with the Switch DNS Firewall

The Switch DNS Firewall allows specific DNS information to be overwritten. This makes it possible to generate alternative responses to DNS queries and to protect all devices effectively before a connection is established to any malicious systems.



Prevention

Blocking access to infected sites can prevent further infection.



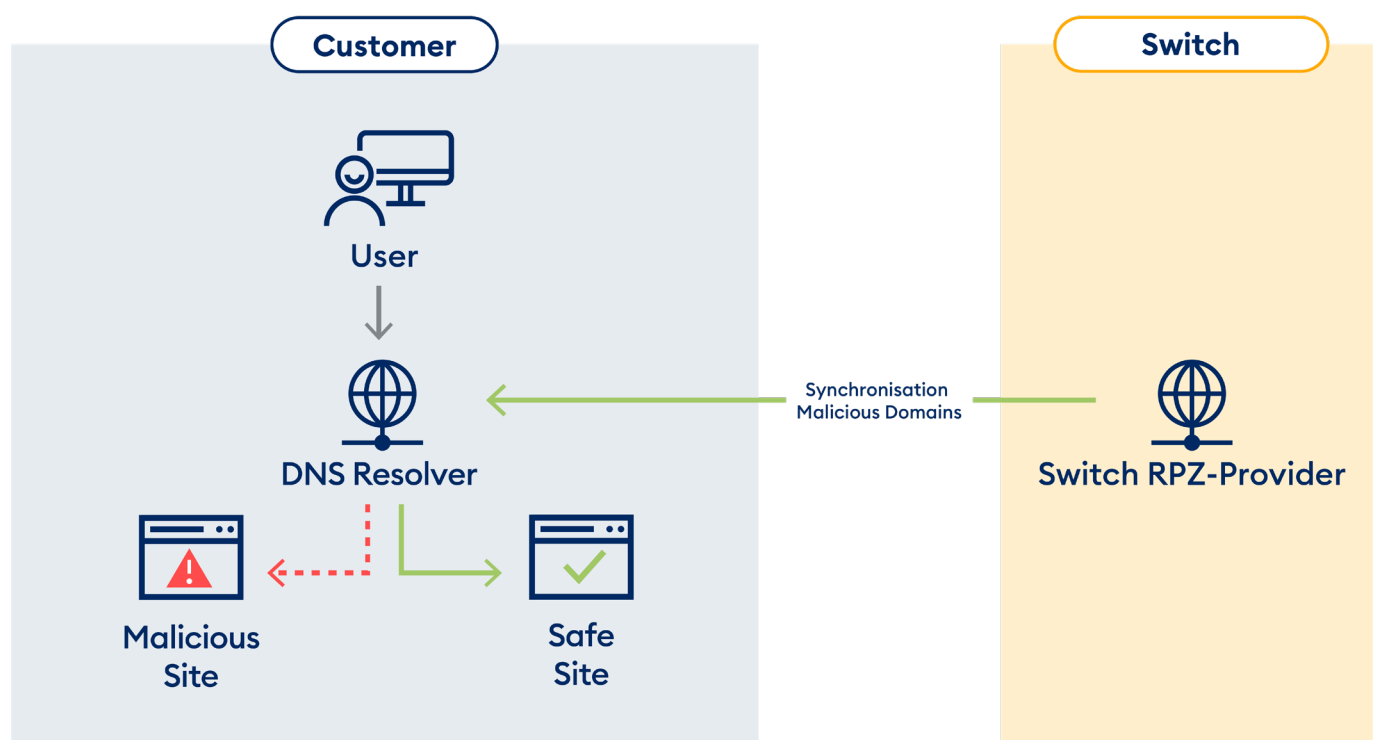
Detection

Systems that have already been infected can be detected by Switch. Customers are promptly notified of any such infections via security reports.



Information

When accessing a malicious domain name, users are redirected to a secure landing page.





Malicious Website blocked

The website you've tried to visit is marked as malicious.

A visit might infect your computer and cause potential damage to your data. To protect you from getting infected, your organisation is using a filter that redirects requests to malicious websites to this landing page.

The website is NOT malicious? If you think a request to a website is wrongfully restricted, click [here](#)

For additional information and help, please contact the support of your organization:

dnsfirewall@switch.ch

Technical Information

Client	1.2.3.4
Queried domain	landingpage.mw.rpz.switch.ch
Queried port	443
URL	https://landingpage.mw.rpz.switch.ch

Switch landing page (Screenshot)

Technical requirements

Integrating the DNS Firewall service is easy: DNS RPZ must be enabled on the resolver which allows you to subscribe to the desired DNS RPZ feeds. This requires a DNS appliance or DNS service software that supports DNS RPZ.

Switch offers its customers wide-ranging expertise in the connection and integration of RPZ technology.

DNS Software

- BIND
- PowerDNS Recursor
- Knot Resolver
- Unbound

DNS Appliance

- Infoblox
- BlueCat
- EfficientIP
- Nokia VitalQIP

Testimonial

«Jisc has worked and collaborated closely with Switch for over 5 years, helping shape and support Jisc's Janet Network Resolver Service, a protective DNS service which supports over 300 Higher and Further Education organisations in the UK, representing over 2.7 million users.

Switch's DNS Firewall data feeds have proved an effective tool in trying to prevent common attack vectors such as phishing and ransomware aimed at the UK education community. We look forward to continuing our close partnership with Switch in tackling a common threat.»

Andrew Davis

Jisc, Infrastructure and Critical Services Manager (Cyber security)

Switch DNS Firewall modules

The following modules can be freely combined:

RPZ Feed

Harmful or infected domains identified by Switch are sent to your organisation's DNS system. This allows it to recognise and block threatening domains. Switch RPZs are not tied to any specific provider and are supported by all common DNS appliances and server software.

Landing Page

Malicious requests are redirected to a specific landing page. This provides end users with information about blocked access attempts. In addition to HTTP/HTTPS, other protocols and their respective ports are also covered to fully inform users.

Notification of Infected Systems

As a customer, we promptly inform you of attempted accesses to infected systems through security reports. The reports are based on the DNS RPZ log data sent from your organisation to Switch. This gives you a comprehensive overview of the current threat landscape within your organisation.

With our redundant system architecture, we guarantee high system availability. Thanks to anycast implementation, latency is also minimised.

Our team is ready to support you with extensive expertise in finding the right solution and integrating the DNS Firewall.

Testimonial

«CERN is using the Switch's DNS Firewall since Q4 2015 for pro-actively preventing our user community accessing malicious domain names and phishing web-sites. Using the Switch DNS Firewall, unfortunate users are redirected to an internal web-page informing them about the risks of browsing the WWW. So far, we have made great experience with it, also thanks to the quick response of Switch to our queries and input, and observed no false positives nor mayor issues.»

Stefan Lüders

Computer Security Officer, CERN, The European Organisation for Nuclear Research, 3,000 users



About Switch

Switch was established in 1987 as a private foundation by the Swiss Confederation and the eight university cantons that existed at the time. The core aspects of the foundation's mission are to enable, maintain and promote a secure and networked research and education infrastructure in Switzerland. With more than 160 employees from 17 countries, we are committed to the purpose of our foundation.

Switch CERT – a leading national centre of expertise

Your trusted partner for cyber security

The Switch Computer Emergency Response Team (CERT) is a leading independent centre of expertise for information security. It was set up in 1994 and was one of the first CERTs in Switzerland to receive international certification in 1996. Its aim is to support Swiss universities in combating cyber threats.

Today, the team provides services as a multi-sector CERT for universities, the domain registry, banks, industry and logistics, and the energy sector. Our areas of expertise include incident response, threat intelligence, detection and trusted community building. We are part of a global network for exchanging alerts and knowledge about cyber threats and work closely with the federal government's National Cyber Security Centre (NCSC). Switch CERT is one of two national CERTs and is considered part of Switzerland's critical infrastructure by the Federal Office for Civil Protection (FOCP)

Independence and transparency

Switch has been responsible for a secure internet for over 25 years and works without any conflicts of interest with manufacturers or suppliers.

Threat information sharing

Comprehensive threat information from the monitoring of university networks and various sectors in Switzerland, supplemented by international partners.

National and international networking

Switch has been cooperating with national and international players from various areas of cyber security since 1994.

Interdisciplinary security expertise

Switch offers comprehensive IT security expertise, including incident response, threat hunting, domain security, malware analysis and more.

Unique synergie

By monitoring and working with different sectors, Switch CERT creates synergies in the fight against cybercrime.

Critical infrastructure protection

Switch operates important infrastructures for Switzerland, such as the.ch registry and national research networks.

Contact us

- Switch DNS Firewall **no-obligation 60-day trial**
- Consulting services for DNS RPZ implementation
- Further information on the Switch DNS Firewall

DNS Firewall Contact:

Switch Security: +41 44 268 15 40

Email: dnsfirewall@switch.ch

Web: <https://dnsfirewall.ch>

Zürich

Werdstrasse 2

8004 Zurich

switch.ch

info@switch.ch

Lausanne

Werdstrasse 2

1001 Lausanne

switch.ch

info@switch.ch

 LinkedIn

 Website

 Newsletter