



# Secutec Secure DNS

## Outsmart malware and bad URL's through DNS

DNS (*Domain Name System*) is a fast protocol that is used to protect your company against malicious host names.

More than 91% of all malware uses DNS to communicate with your server, to steal data or redirect traffic to malicious sites. Today, the dangers are very often hidden in innocent applications, documents and websites. Invisible to firewalls and other security solutions.

### What is Secure DNS?

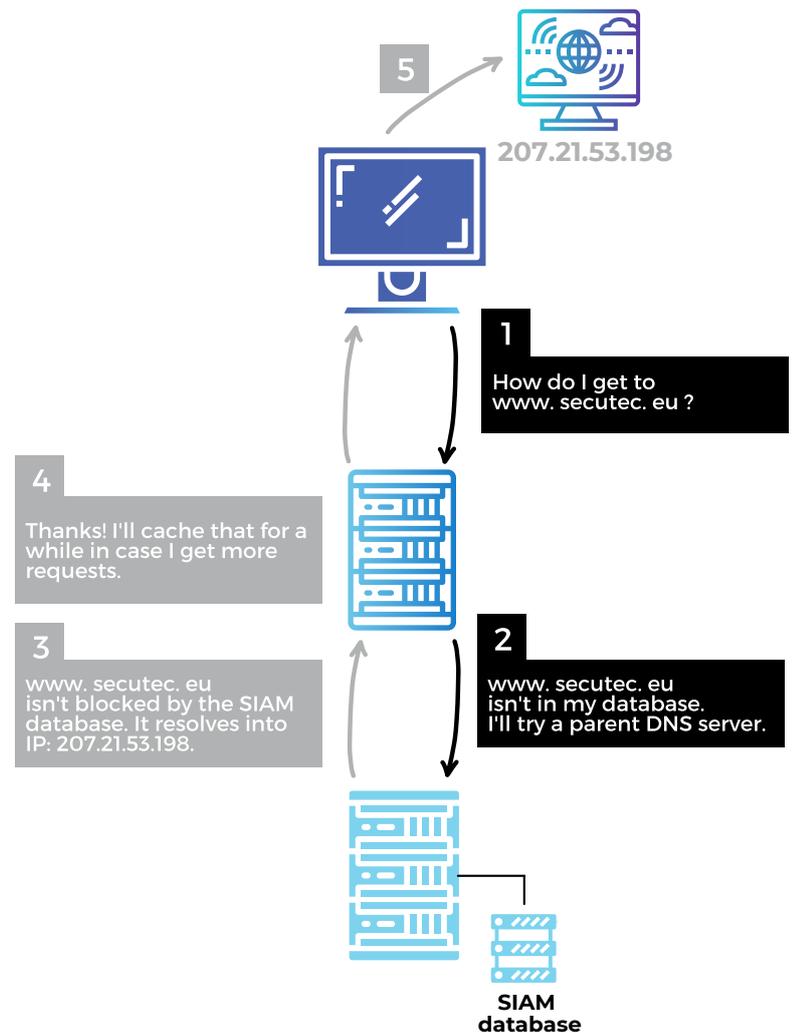
Security through DNS protects you against new threats that your current antispam, firewall and proxies are not yet aware of. DNS is one of the most fundamental instruments of Internet and for network. DNS is the phonebook of the Internet. A user access information online through domain names, because that's something they can remember, like [www.secutec.eu](http://www.secutec.eu). Web browsers interact through IP addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

By setting your DNS forwarder to send DNS queries to our [Secutec Secure DNS Server](#) the domain reputation will be checked.

### How does it work?

All known malicious domains are actively blocked as most of the phishing and ransomware domains have a low lifetime. If a user browses to a domain that has been blocked, they will be presented with a default blocking page. If the domain is whitelisted or if it is not known as "bad" the user will be able to access the domain.

By blocking through DNS, we are not only blocking the web traffic that should go through your web proxies, but also the traffic that is bypassing the proxy. Secutec Secure DNS Service works with any IT, network or security setup within your corporation.



## SIAM, a unique Secutec service

### Secutec Integrated Advanced Malware

Secutec Secure DNS receives feeds from the Secutec SIAM database that gives information on which domain should be whitelisted or blacklisted.

- **Whitelist category:** All domains which are known as secure.
- **Blacklist category:** All malicious and untrusted domains.
- **Others:** All domains not known as 'bad'.

The SIAM database gathers information from Secutec Honeypots, sensors, security feeds and other sources on the internet.

## No downtime, service interruptions or server reboots needed.

Secutec has developed Secure DNS to get an overview of the outgoing traffic through DNS and to block malicious domains. There are no infrastructure changes needed to install our Secure DNS service and compatible with any endpoint solution.





## Your KEY advantages

### PRO ACTIVE BLOCKING ON NOT YET CATEGORISED DOMAINS

Newly seen domains (domains that were seen for the first time in the previous 24h) will automatically be blocked, because more than 22% of all new created domains will be used for Malware, Phishing, Ransomware, ... After 24 hours they will be removed from that category.

### NO INFRASTRUCTURE CHANGES

No downtime, service interruption, or server reboots are needed. The implementation can be done in less than 15 minutes. The service will work straight away.

### VISIBILITY ACROSS DEVICES

In order to keep track of your performance, we provide you with a detailed report on what has been blocked. The reporting and alerting system can be customized.

"We are very satisfied about the response time of the detection and the extra protection layer on top of our firewall and antivirus."

**KURT DEBERSAQUES – RENSON**



Get in touch

**Wondering what Security through DNS could do for you?**

We are ready to help you.

Secutec by  
Boomssesteenweg 41/11  
2630 Aartselaar

+32(0)3 877 82 93

info@secutec.be