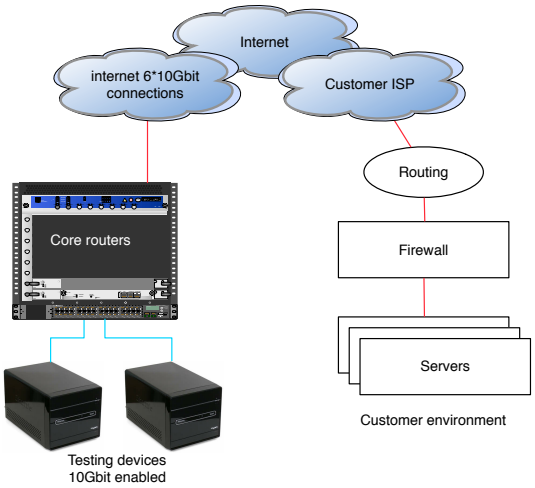
DDoS Testing Services



DOES YOUR BUSINESS HAVE AN OPTIMISED DDOS PROTECTION STRATEGY

Our DDoS testing service exercises your infrastructure and allows a complete review of your infrastructure, organisational readiness with the highest degree of transparency. We can perform DDoS testing remotely across the internet or on-site with optimised testing devices providing more than 10Gbit full wirespeed with small packets from each testing device.

Using highly optimised hacking tools and packet generators we can help pinpoint devices and bottlenecks in your infrastructure. Resulting output will allowing for a well planned strategy to improve your over-all protection against DDoS attacks.

Scenarios covered include popular attacks like TCP-Syn, ICMP and UDP Flooding and more exotic packet types.

Features at a glance

- Full portscan and host discovery using best current security testing
- Controlled DDoS testing from 50.000 packets per second to millions of pps.
- Bandwidth testing from 100Mbit to multiple 10Gbit with ICMP, UDP and TCP
- Detailed listing of scenarios which have impact on infrastructure with parameters for reproducing tests
- Suitable for any firewall type and IDS/IDP
- Reporting in english containing both Management Summary and technical recommendations for each scenario

Easy testing

We will do the test to your specifications and have a strong team to test your network with the least inconvenience to your production.

We will be available online during the testing period for questions and will contact your staff immediately if systems are behaving erratically during testing.

In the worst case we can also postpone activities or even halt the entire testing procedure in case you experience high impact to servers.

Coordinated and proven

We believe in active testing to verify your infrastructure as well as the organisation.

After testing has finished and reporting is done we will work with your staff to help remedy the problems identified in your infrastructure. Experience show that we often see security will have improved radically after testing and recommendations are implemented.

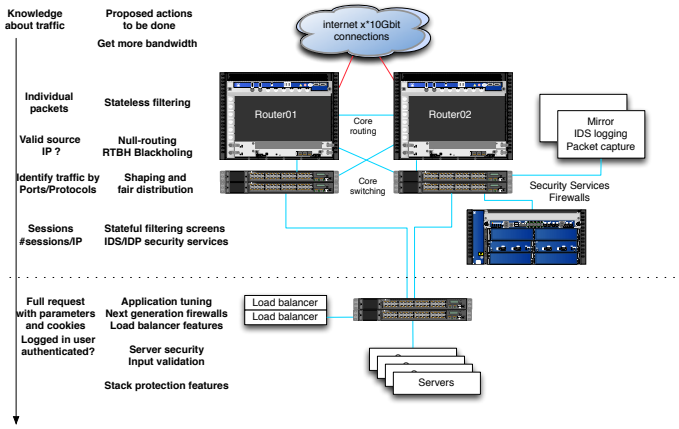
The goal is a commitment to providing you with an efficient tools to help you design and implement secure internet services.

Productive

Our remote testing is performed from high capacity setup in Denmark simulating DDoS attacks using the same tools and methods as real attackers. We focus initially on network layer testing, but can expand to higher level protocols as needed.

DDoS Testing Services

Recommendations for generic DDoS protection



We have the following generic recommendations with regards to creating a robust infrastructure to protect against DDoS attacks:

- Create a multilayered defensive infrastructure
- Identify which services the organization provides to the Internet
- Identify which providers are critical for the services provided, for example your ISP
- Deploy Network Security Monitoring, for example IDS
- Deploy Network usage monitoring, for example interface graphs and Netflow
- Analyze the features and settings available in the existing infrastructure devices
- Appropriately configure the features and settings, disable the features that are not needed
- Prepare filtering configurations before the attacks occur (ACL and router filters that are

quickly deployable)

Discard packets early – using stateless methods:

- from protocols not used
- to IP addresses not in use
- to ports and services which are not in use
- clearly attacks – TCP SYN+PUSH illegal combinations
- pretending to be from inside the network, ingress/egress filtering
- sending packets with spoofed addresses, ingress/egress filtering and BCP38

Discard packets arriving from un-routable sources, employ Reverse Path Forwarding

Restrict protocols needed to acceptable levels using shaping and quality of service

DDoS Testing Services

Deploy components that have more resources available than needed

Restrict usage by source IP and by destination IP to a limited number of sessions

Buy more bandwidth than needed

Create a procedure to evaluate what level of DDoS attacks your organization is likely to receive

Make sure the web servers are configured for the specific use-cases – disable unnecessary features and enable time-out of lingering sessions (slowloris attack types)

Regarding applications, application servers and languages used, make sure to use updated software, disable features that are not used and configure everything in a hardened internet configuration, as recommended by vendor

Databases should be configured to match success – including enough sessions for a high number of concurrent users in the application; this includes the use of database session pool etc.

Databases should be optimized to ensure that all searches, lookups and functions resulting from customer and internet users are working as efficient as possible; adding indexes and reducing the number of concurrent searches from the web site might be required

Ensure that devices, applications and database systems can efficiently log and have enough storage for high load

Ensure that security logging is done and being monitored; including successful and failed logins

Ensure devices and servers are monitored for high usage and resource shortage, including CPU, Memory and disk I/O

Include DOS tests in web-application testing or as a separate test