EANTC Test Report
Secucloud ECS² Advanced Suite
Solution Performance Test

INTRODUCTION

EANTC was commissioned by Secucloud GmbH to verify the performance of Secucloud's Elastic Cloud Security System (ECS²) Advanced Suite solution.

Secucloud ECS² Advanced Suite is designed to provide mass market network security protection for mobile (OnNet and OffNet/WiFi) and fixed line telecommunication subscribers. The product has been developed as a cloud based solution that runs in virtualized environments within data centers of telecommunication companies. Telecommunication market customers can integrate the solution within their existing data center infrastructure.

Secucloud's software platform is modular and offers varying suites of protection. EANTC tested the DNS Shield module of ECS² Advanced Suite which is intended to protect telecommunication subscribers from malicious destinations on the internet by providing real time DNS and content filtering.

Secucloud's ECS² Advanced Suite realizes its security functionality by receiving all DNS requests from the subscribers and either delivering the original answer from upstream DNS servers or by injecting the IP of a different component for further inspection within the platform.

Test Highlights

- **4 DNS Shield VMs in a single compute node supports nearly 0.5 million DNS Qps[a]**
- **Up to 130,000 DNS Qps with 1VM**
- **Supports DNS queries for IPv4 & IPv6**
- **Measured 3ms of average DNS response time**

a. Qps: Queries per second

EXECUTIVE SUMMARY

The main scope of the test was to measure the DNS performance of the ECS² Advanced Suite solution. Security features were not in the scope of this test.

EANTC verified that ECS² Advanced Suite solution can handle up to 500,000 DNS queries per second using a single compute server. EANTC evaluated the performance after all DNS records were cached in DNS Shield. Based on DNS statistic inputs collected from service providers and vendors, an average DNS query rate per user is in the range of 0.015 - 0.030 DNS queries per second. Considering these inputs, Secucloud's Advanced Suite solution is theoretically capable of handling a range of 17 - 33 million subscribers per compute node.

Since ECS² Advanced Suite solution has no interdependency between compute nodes, the performance can be scaled linearly by deploying the solution in multiple compute nodes. For example four compute nodes in one or more Data Centers, integrated into the network using IP anycast for the DNS resolver, could theoretically handle a range of 68 - 132 million subscribers in total.

SECUCLOUD ECS² ADVANCED SUITE PLATFORM INTEGRATION

In our tests, the ECS² Advanced Suite platform integration within an existing network was not in scope. However, Secucloud explained a typical ECS² Advanced Suite platform integration which can be used in an ISP environment.

Traffic Flow and Platform Distribution

Secucloud ECS² Advanced Suite platform is deployed to the regional data centers of the operator. Network integration is performed by using IP anycast for the DNS resolver. Secucloud's platform announces its IP anycast address via the BGP routing protocol.

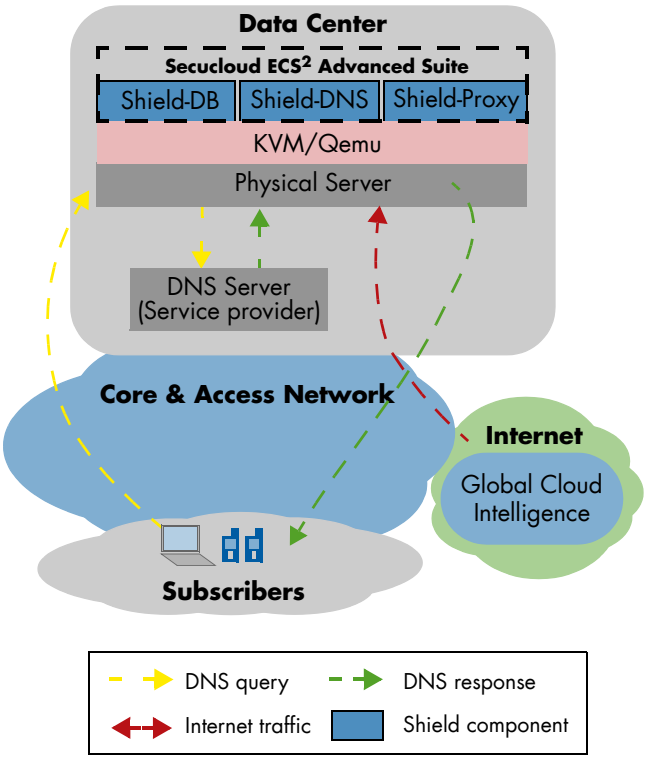


Figure 1: ECS² Advanced Suite Platform

This leads to intra-regional routing of DNS requests from the end-customer devices using the shortest path (or other applicable policy) to the Secucloud platform within the operator's environment.

This DNS implementation with IP anycast via BGP is the common deployment without the need for further equipment or mechanisms in the operators' networks. It integrates into the Secucloud platform in the operators' environments by using standard protocols.

Service Integration Into ISP's Environment

Secucloud's DNS resolvers, as part of the Secucloud ECS² Advanced Suite solution, are deployed to the data center infrastructure of the operator's network. They use the existing operator's DNS servers as forwarders for all end-customer requests.

This means that existing filters (e.g. governmental blacklists) on the operator's DNS servers are still effective. Furthermore, the platform is located inside the existing security infrastructure of the operator.

The components listed below were used in Secucloud's ECS² Advanced Suite solution during the test.

SHIELD-DB

The Shield-DB is a management level component which holds security and redirect policies for individual clients or configured subnets. Furthermore, it collects statistics and triggers events (which may alter corresponding policies). The SHIELD-DB component is essentially the core of the Secucloud ECS² platform.

SHIELD-DNS

This security filtering component is a customer facing DNS instance which applies DNS-based filter policies on a per-user level. Depending on the configuration, DNS queries to malicious sites will either be blocked or redirected to another ECS² component, the SHIELD-Proxy, for further inspection. The SHIELD-DNS component accepts DNS queries from the network and acts from the client perspective as a normal resolver per RFC 1035 (Domain Implementation and Specification). Behind the scenes it filters queries according to security and redirect policies from the SHIELD-DB component, thus allowing the system to block or redirect requests if required.

SHIELD-Proxy

The Shield-proxy component is also a security filtering component which is used as an HTTP/HTTPS destination for intercepted DNS requests. It replies either with an HTTP redirect, pointing to an informational page (hosted as the Customer-WEB component) or by directly delivering the content. The main functions are Inline URL Filtering, interception and decryption of HTTPS Flows and AV Scan of HTTP Responses. EANTC did not test functionality of Shield-proxy component.

TEST SETUP

The solution under test (SUT) was Secucloud´s ECS² Advanced Suite solution. Secucloud deployed their solution on a compute node using KVM/QEMU as the virtualization platform. Four Shield VMs were instantiated as VNFs inside a compute node. Each Shield VM was reserved with 4 vCPUs and 8 GiB memory resources. The Shield VMs consisted of 3

virtual bridge type (Virtio model) interfaces for traffic ingress, egress and one port for the management and internet connection. The interfaces were connected with a router as VNF.

In the test setup all DNS Shield VMs were configured as stand alone VMs, i.e there was no inter communication or load sharing between the Shield VMs.

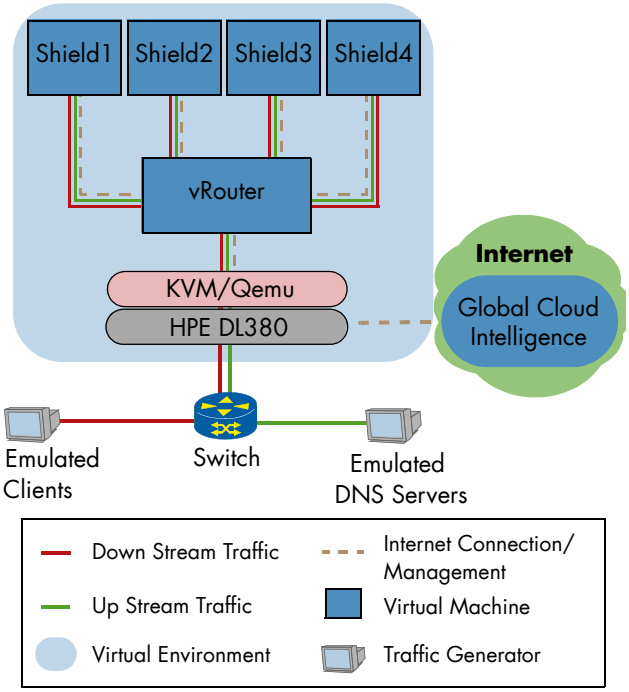


Figure 2: Logical Topology

We used a Spirent C100 appliance with Avalanche commander application as traffic generator to emulate the DNS clients and servers. The SUT and the traffic generator were connected using a physical switch. In the test scenario we emulated IPv4 and IPv6 DNS clients in a ratio of 50:50 to initiate A and AAAA queries. On the other end, we emulated four DNS servers containing 50,000 A type and 12,500 AAAA type unique records in total. Each Shield VM was mapped with one DNS server. In this test we configured 325,636 client IP addresses and 4 DNS server IP addresses.

Traffic Flow

Once a client DNS query is received by the SUT, it is processed based on the configured rules and policies. Typically this includes classifying the domain based on its content. If the domain is new to the SUT (i.e. not present in any of the caches), the classification is done by performing an API call towards the global ECS^2 Cloud Intelligence module which is reachable over the internet. Once a domain has been classified, the result is cached for a configurable duration. In this test, the classification cache TTL was set to eight hours. Additionally, Secucloud configured a default security policy, which included category filtering of malicious and / or high risk websites

We configured the traffic generator to increase the DNS query rate automatically until the target performance was achieved. When transaction errors occurred, the query rate was decreased until a stable rate was reached. The emulated clients were configured for no query reattempts.

TEST BED SPECIFICATIONS

The following table summarizes the specifications of the hardware and software used in our test bed to run the Secucloud ECS^2 Advanced Suite solution.

Compute Node	
Hardware	Hewlett-Packard HPE DL380 Gen9
CPU	2x Intel(R) Xeon(R) CPU E5-2699 v3 @ 2.30GHz x 18 cores (used 17 vCPUs from one socket only)
Memory	DDR4 512GB (used 36GB)
NICs	Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01) (used 2x NICs) Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet PCIe (rev 01) (used for management & cloud intelligence)
Hardware Configuration	
CPU pinning on each VM, CPU Governor: Performance, HyperThreading: disabled	
Host Software Details	
OS	Ubuntu 16.04.2, kernel version 4.4.0-62
Hypervisor	QEMU v2.5.0; API: QEMU 1.3.1
Shield VM	
OS	Ubuntu Linux 16.04.2 x86_64
Software	1.1.5
Test Equipment	
Spirent C100 appliance Avalanche commander 4.75	

TEST RESULTS

Performance with 4 DNS Shield VMs

We configured the traffic generator to initiate DNS queries for all 62,500 unique domains sequentially.

During the initial period of the first test run with four Shield VMs, there were no DNS records classified and cached in the solution. As expected, during the caching period, the solution could handle a lower number of DNS queries.

We measured an average rate of 90,000 queries per second for a duration of 15 minutes. After which, the SUT reached the target performance. The DNS caching period was not part of the test.

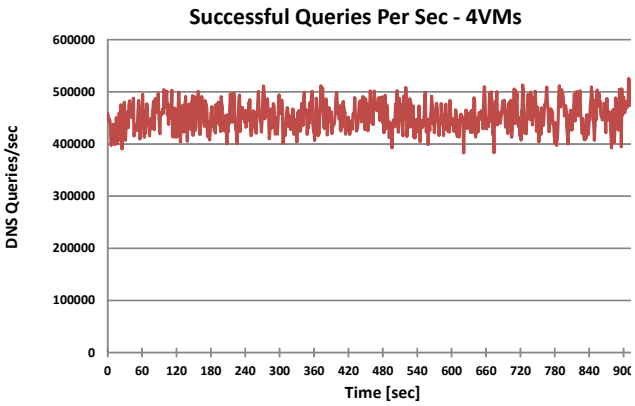


Figure 3: DNS Performance with 4 VMs

Once the SUT classified and cached all DNS records, it responded to the queries at a rate of between 420,000 and 510,000 queries per second. As shown in Figure 3, the average successful DNS query rate supported by the SUT was 490,000 queries per second. We measured 3ms as an average DNS response time.

Performance with Single DNS Shield VM

Figure 4 shows the performance of a single DNS Shield VM setup. As observed, the DNS performance was between 100,000 to 140,000 queries per second and the average was 129,000 queries per second. We measured 3ms as an average DNS response time.

During the tests, we additionally simulated some DNS queries from the emulated clients to some domains classified as "malicious". As expected, the SUT responded to these queries with the redirection IP address. This confirms that the DNS filtering feature was active during the performance test.

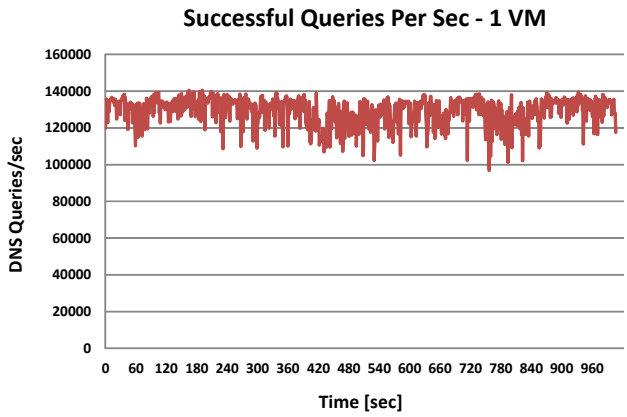
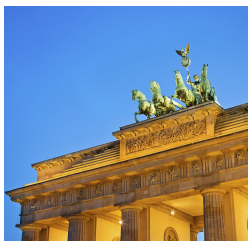


Figure 4: DNS Performance of 1 VM

ABOUT EANTC



The European Advanced Networking Test Center (EANTC) is internationally recognized as one of the world's leading independent test centers for telecommunication technologies. Based in Berlin, Germany, the company offers vendor-neutral consultancy and realistic, reproducible high-quality testing services since 1991. Customers include leading network equipment manufacturers, tier-1 service providers, large enterprises and governments worldwide. EANTC's proof of concept, acceptance tests and network audits cover established and next-generation fixed and mobile network technologies. http://www.eantc.com

EANTC AG, Salzufer 14, 10587 Berlin, Germany
info@eantc.com, http://www.eantc.com/