Certificate: genuscreen 7.0

Certification Report

1. Product vendor: genua GmbH
2. Evaluation facility: German Federal Office for Information Security
3. Certificate ID: BSI-DSZ-CC-1085-2019
4. Validity: 28-08-2019 to 27-08-2024
5. Compliance: EAL4+

Target of Evaluation

1. The target of evaluation (TOE), genuscreen 7.0, is a distributed stateful packet filtering firewall system with VPN functionality.
2. The TOE consists only of two software components:
    a. the genuscreen software runs on several distributed network nodes which serve as network filters;
    b. the genucenter software functions as a central management systems for the distributed network filters.
3. Supports IPv4 and IPv6.
4. Cryptographic functions:
    a. **Authentication:** 2048-bit RSA SSA PKCS#1 v1.5 using SHA-256 (used in IKEv1 IPsec and SSH-2).
    b. **Key agreement:** 2048-bit Diffie-Hellman group 14 using HMAC-SHA-256 (in IKEv1 IPsec) and poolp256r1 ECDH with SHA-256 (in SSH-2).
    c. **Confidentiality:** AES-192 (by default) in CBC mode (IKEv1) and AES-128 in CTR mode (SSH-2).
    d. **Integrity:** HMAC-SHA-256 with 256-bit key (IKEv1) and UMAC with AES-256 using the ETM extension (SSH-2).
    e. **Trusted channel:** IKEv1, IPsec and SSH v2.0.

Assumed Attacker Model

The following threats were established for the two software components:

1. An attacker might attempt to break into a protected network. (To be countered by the firewall components, genuscreens.)
2. An attacker might sniff sensitive data passing between protected networks. (To be countered by the genuscreens.)
3. An attacker might access the TOE and read, modify or destroy sensitive data, by sending packets or exploiting a weakness in the protocols used. (Countered by both the management system, genucenter, and the genuscreens.)
4. An attacker might send specially crafted data to access resources not allowed by the policy. (Countered by genuscreens.)
5. An attacker might read and modify configuration or audit data passing between the components. (Countered by both.)

6. An attacker might modify sensitive data between protected networks. (Countered by genuscreens.)

The Security Target assumes the following about the environment:

1. All components of the TOE are physically secure.
2. The TOE was initialised exactly according to the documentation.
3. Administrators, users and revisors are non-hostile and follow administrator guidance. They use strong passwords.
4. Information cannot flow between the internal and external network unless it passes through the TOE.
5. The environment provides reliable timestamps.
6. Administrators, users and revisors using the administrative GUI work in a trusted network connected directly to the system.
7. The environment provides a physically separated network for TSF data transfer for the optional high-availability setup.
8. The server for external LDAP authentication of genucenter administrators and revisors is located in a secure network.

Device Scrutinization

1. The TOE configuration consists of software on at least two firewall components that work as network filters.
2. Another machine to manage this network of firewall components is called management system which is a central component.
3. The firewall components are initialised on a secure network from the management system.
4. After initialisation, the firewall components can be distributed to the locations of the networks they are protecting.
5. The genuscreen firewall components filter incoming and outgoing traffic for multiple networks and can thus enforce a given security policy on the data flow. They can work as bridges or routers and can be used in an optional high availability (HA) setup where the firewall components synchronize their internal states.
6. At the same time, the firewall components can provide confidentiality and integrity for data traffic passing between the networks. This Virtual Private Network function is achieved by IPsec connections.
7. The connection between genucenter and genuscreen is encrypted with SSH.

The product was scrutinized on three fronts: tests performed by the vendor, tests by the independent evaluator and penetration testing by the evaluator.

1. The vendor tests their product regularly as part of their development process on a system consisting of the TOE installed on five devices. Test procedures are scripts written in Ruby, Perl or shell. Their results are collected automatically and are compared with expected results. These tests cover all the specified security functions

and they're performed against the TOE design. All real test results are equal to the expected results.

2. The vendor provided the evaluator with several different hardware components for testing. All the components were installed on physical hardware in a separate administrator network in accordance with the configuration in the Security Target. A complex configuration of all security features was tested, with a focus on the SIP relay, the management system, cryptograpic functions, random number generation and its entropy source (part of the OpenBSD kernel). The actual test results were consistent with the expected results.
3. Additional vulnerability tests were designed by the evaluator. Additionally, the source code was analysed for vulnerabilities, as well. No attack with at least moderate attack potential was successful in the environment defined in the Security Target.

Security Assurance Requirements (SARs)

1. Development
    1. Security architecture description
    2. Complete functional specification
    3. Implementation representation of the TSF
    4. Basic modular design
2. Guidance
    1. Operation user guidance
    2. Preparative procedures
3. Life-cycle
    1. Production support, acceptance procedures and automation
    2. Problem tracking CM coverage
    3. Delivery procedures
    4. Identification of security measures
    5. Flaw reporting procedures
    6. Developer defined life-cycle model
4. Security target
    1. Conformance claims
    2. Extended components definition
    3. ST introduction
    4. Security objectives
    5. Derived security requirements

6. Security problem definition
7. TOE summary specification with architectural design summary

5. Tests
    1. Analysis of coverage
    2. Testing: basic design
    3. Functional testing
    4. Independent testing – sample
6. Vulnerability
    1. Methodical vulnerability analysis

Security Functional Requirements (SFRs)

1. **Firewall SFP:** Requirements for the firewall components to enforce the security policies defined by the administrators. Protects against unauthorised access. Addressed by the SF_PF Packet Filter and SF_ADM functionalities.
2. **Network Separation SFP:** Network separation using routing domains. Addressed by the SF_NS Network Separation and SF_ADM functionalities.
3. **IPSEC:** Requirements relating to VPN connections between firewall components – OS kernel part. Addressed by the SF_IPSEC Ipsec Filtering functionality.
4. **IKE-SFP:** Requirements relating to key management of VPN connections between firewall components – userspace part. Addressed by the SF_IPSEC IPsec Filtering and SF_ADM functionalities.
5. **SSH-SFP:** Requirements for communication between the management system and firewall components. Addressed by the SF_SSH SSH Channel and SF_ADM functionalities.
6. **SIP Relay:** Requirements for access control by the SIP relay. Addressed by the SF_SIP SIP Relay and SF_ADM functionalities.
7. **Administration:** Requirements related to the administration of the TOE. Addressed by the SF_ADM Administration and SF_IA functionalities.
8. **Identification and authentication:** Identification and authentication of administrators, users and revisors. Addressed by the SF_IA Identification and Authentication functionality.
9. **Audit:** Requirements on the audit capabilities of the TOE. Addressed by the SF_AU Audit functionality.
10. **General management facilities.** Addressed by the SF_GEN General Management Facilities functionality.

11. **Random number generation:** The internal state of the RNG must have at least 64 bits of entropy after initialization and it should provide forward secrecy. Addressed by the SF_IPSEC and SF_SSH functionalities.

What seems interesting to me is that the system applies numerous "self-protection measures against interference and logical tampering" or imposes such measures on the environment, such as the use of LibreSSL instead of OpenSSL, using the functions `str|cat` and `str|cpy` which don't overwrite allocated memory and employing stack and memory protection mechanisms provided by compilers.

Out of Scope

- Any hardware components are out of scope.
- Running the central management software (genucenter) is out of scope of the TOE.
- Usage of a cryptocard for performing cryptographic operations is out of scope.
- Third-party VPN connections as well as L2TP VPN are out of scope and must not be used.
- The use IKEv2/MOBIKE is not considered as part of the TOE.
- IPVv4 dynamic routing using OSPF is out of scope.
- While high-availability (HA) setup for genuscreens is part of the TOE, HA setup for genucenter is out of scope.
- Remote maintenance feature is out of scope.
- genucenter's REST API is out of scope and must not be used.

Critical Evaluation and Conclusions

Would you buy the product? What you were missing? Are you convinced by eval. laboratory testing?

It looks all right from a quick read. They seem to consider a wide range of functionality, definitely enough for a decent firewall. I like that they rely on OpenBSD and LibreSSL as opposed to the usual configuration GNU/Linux+OpenSSL or GnuTLS. I'd most likely consider it as one of the products to buy if I were in the position to decide.