Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0218-2003

for

Internet Security and Acceleration Server 2000 - Standard Edition - SP1 with FP1

from

Microsoft Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49 228 9582-0, Infoline +49 228 9582-111, Telefax +49 228 9582-455

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0218-2003

Common Criteria Arrangement

Internet Security and Acceleration Server 2000 - Standard Edition - SP1 with FP1

from

Microsoft Corporation

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Part 1 Version 0.6*, *Part 2 Version 1.0* for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)*.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria Part 2 conformant**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL2**

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

IT Security Certified

SOGIS-MRA

Bonn, 8. September 2003

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon (0228) 9582-0 - Telefax (0228) 9582-455 - Infoline (0228) 9582-111

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2)

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.
Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)

---

[2] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Federal Office for Information Security (BSI-Kostenverordnung, BSI-KostV) of 29th October 1992, Bundesgesetzblatt I p. 1838

[5] Proclamation of the Bundesministerium des Innern of 22nd September 2000 in the Bundesanzeiger p. 19445

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates based on the ITSEC was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Internet Security and Acceleration Server 2000 - Standard Edition - Service Pack 1 with Feature Pack 1 has undergone the certification procedure at BSI.

The evaluation of the product Internet Security and Acceleration Server 2000 - Standard Edition - SP1 with FP1 was conducted by TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit (ITSEF)[6]. The TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit is an evaluation facility recognised by BSI.

The sponsor and vendor and distributor is Microsoft Corporation.

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 8. September 2003.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-20.

The product Internet Security and Acceleration Server 2000 - Standard Edition - SP1 with FP1 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://www.bsi.bund.de). Further information can be obtained from BSI-Infoline 0228/9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] Microsoft Corporation, 1 Microsoft Way, Redmond WA 98052, USA

B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1 Executive Summary

The Target of Evaluation (TOE) and subject of the Security Target (ST) [5] is the Firewall product Internet Security and Acceleration Server 2000 - Standard Edition - Service Pack 1 with Feature Pack 1 (also named ISA Server in short).

ISA Server is a dedicated firewall that acts as the secure gateway to the Internet for internal computers. ISA Server protects all communication between internal computers and the Internet and runs on a Windows 2000 Server operating system.

The basic functions of the ISA Server are:

- Identification and Authentication: ISA Server 2000 supports a range of authentication methods, whereof basic authentication as the standard method of authentication for Hypertext Transfer Protocol (HTTP) transmissions comprises the scope of the evaluated configuration.
- Filtering (Packet and Application level filtering): Packet filters, Server publishing, Web publishing and Application filters
- Generation of audit records

The ISA Server is intended to be used as a multi-layered firewall. IP packet filtering provides security by inspecting individual packets passing through the firewall. Application level filtering allows ISA Server to inspect and secure popular protocols.

Graphical taskpads and wizards do not belong to the TOE but are implemented in the environment , they shall simplify navigation and configuration for common tasks.

The operating system Windows 2000 maintains security attributes for all administrators. The operating system Windows 2000 stores the identification and authentication data for all known administrators and maintains a method of associating human users with the authorized administrator role.

The TOE itself offers no additional identification and authentication methods for firewall administrators.

The TOE Security Functional Requirements (SFR) used in the Security Target are Common Criteria Part 2 conformant. The ISA Server was evaluated by TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit. The evaluation was completed on 3. September 2003. The TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit (ITSEF)[8] is an evaluation facility recognised by BSI.

The sponsor and vendor and distributor is Microsoft Corporation.

[8] Information Technology Security Evaluation Facility

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C of this report, or [1], part 3 for details).

The TOE meets the assurance requirements of assurance level EAL2 (Evaluation Assurance Level 2).

1.2 Functionality

The TOE provides following functionality:

SFR	Name
Audit Generation	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_STG.3	Action in case of possible audit data loss
Identification and Authentication	
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UID.2	User identification before any action
FIA_UAU.2	User authentication before any action
Information Flow Control	
FDP_IFC.1 (1)	Subset information flow control (1) - UNAUTHENTICATED SFP
FDP_IFC.1 (2)	Subset information flow control (2) - UNAUTHENTICATED_APPL SFP
FDP_IFC.1 (3)	Subset information flow control (3) - AUTHENTICATED SFP
FDP_IFF.1 (1)	Simple security attributes (1) - UNAUTHENTICATED SFP
FDP_IFF.1 (2)	Simple security attributes (2) - UNAUTHENTICATED_APPL SFP
FDP_IFF.1 (3)	Simple security attributes (3) - AUTHENTICATED SFP
FDP_RIP.1	Subset residual information protection
FMT_MSA.3	Static attribute initialization
FPT_RVM.1	Non-bypassability of the TSP

Table 1: TOE security functional requirements

These Security Functional Requirements are implemented by the following TOE Security Functions:

Security function
SF1: Identification and Authentication
SF2: Information Flow Control
SF3: Audit Generation

Table 2: TOE security functions

Note: Only the titles of the Security Functional Requirements and of the TOE Security Functions are provided. For more details please refer to the Security Target [5], chapter 5 and 6.

1.3 Strength of Function

The TOE's strength of function is claimed SOF-basic for the chosen basic authentication method within the security function "Identification and Authentication".

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The following list of threats is defined in the Security Target [5], chapter 3.3:

T.NOAUTH

An attacker may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

T.ASPOOF

An attacker may carry out spoofing in information flows mediated by the TOE between clients and servers located on internal and external networks governed by the TOE, by using a spoofed source address to hide his identity.

T.MEDIAT

An attacker may send impermissible information through the TOE, which results in the exploitation of resources on the internal network and gathering of information he is not authorized for.

T.OLDINF

Because of a flaw in the TOE functioning, an attacker may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.

T.AUDFUL

An attacker may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.

There is one Security policy to be fulfilled by the TOE, please refer to the Security Target [5], chapter 3.2:

P.AUDACC

Persons must be accountable for the actions that they conduct. Therefore audit records must contain sufficient information to prevent an attacker to escape detection.

1.5 Special configuration requirements

There are two versions of ISA Server available: Standard Edition (single machine support only) and Enterprise Edition (can be member of a firewall cluster). The Standard Edition with local administration and without Active Directory integration comprises the TOE.

ISA Server Standard Edition is intended for small businesses, workgroups, and departmental environments. Standard Edition provides local policy only, and supports up to four processors. Scalability is not part of the evaluation. For the Standard Edition security policy configuration data is stored in the local Windows registry, however, the storage of policy configuration data is not part of the evaluation as Windows Registry and Active Directory are outside the scope of the TOE.

ISA Server can be installed in one out of three modes: firewall, cache, or integrated. For evaluation the firewall mode without cache is chosen. The caching functionality does not include any security related features.

The evaluated TOE is uniquely named as "Microsoft Internet Security and Acceleration Server 2000 - Standard Edition" and its software version is Microsoft ISA 2000 Service Pack 1 with Feature Pack 1.

The ISA Server software and the Administrator and User Guidance as parts of the evaluated version for the TOE are provided as a boxed product that is delivered to the sales channels. The required Service Pack 1 and Feature Pack 1 are distributed to users using both physical distribution and electronic distribution via the web in a secure way. Subject of evaluation was the secure distribution via the web. The AGD Addendum of the guidance documentation is delivered via the web only.

The Administrator and User Guidance is also available on the internet, however, relevant for the evaluated version of the TOE is the Administrator and User Guidance that is delivered together with the software on CD-ROM [7]. The AGD Addendum [8] is also part of the evaluated version of the TOE. It is only available as a pdf document via a secure channel on the vendors TOE-internet-homepage.

The TOE is running on a Windows 2000 operating system with service pack 3, installed on an HP/Compaq ProLiant ML330 G2 as the server hardware.

1.6 Assumptions about the operating environment

The following constraints concerning the operating environment are made in the Security Target, please refer to the Security Target [5], chapter 3.1:

A.PHYSEC

The TOE is physically secure. Only authorized personal has physical access to the TOE.

A.GENPUR

The TOE stores and executes security-relevant applications only. It stores only data required for its secure operation.

A.NOEVIL

Authorized administrators are non-hostile and follow all administrator guidance.

A.SINGEN

Information can not flow among the internal and external networks unless it passes through the TOE.

A.DIRECT

The TOE is available to authorized administrators only. Personal who has physical access to the TOE and can log in the operating system is assumed to act as an authorized TOE administrator.

A.SECINST

Required certificates and user identities are installed using a confidential path.

A.OS

The operating system implements following functions which are used by the TOE security functions: reliable time stamp (log file audit), file protection (for log file access protection), tools for audit review, and administration access control.

The ISA Server is running on a Windows 2000 operating system with service pack 3 and is installed on an HP/Compaq ProLiant ML330 G2 hardware.

1.7 Disclaimers

The Certification Results only apply to the version of the product indicated in the Certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product

by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation is called:

Microsoft Internet Security and Acceleration Server 2000 - Standard Edition with Service Pack 1 and Feature Pack 1

The following table summarises the TOE components and defines the evaluated configuration of the TOE:

Deliverables	Version	Comment
Box	3.0.1200.50	CD-ROM ISA Server 2000 Standard Edition without SP1 and FP1 including the Administrator and User Guidance on CD-ROM [7]
Service Pack 1	3.0.1200.166	Direct download page for English language version: http://www.microsoft.com/isaserver/downloads/ENGsp1.asp File to download: isasp1.exe
Feature Pack 1	3.0.1200.235	Direct download page for English language version: http://www.microsoft.com/downloads/details.aspx?FamilyID=2f92b02c-ac49-44df-af6c-5be084b345f9&DisplayLang=en File to download: isafp1.exe
AGD Addendum (of the Administrator and User Guidance)	1.0	Guidance evaluation addendum [8], downloaded from: https://s.microsoft.com/isaserver/code/commoncriteria/msisa_agd_usr.pdf The end-user gets the location of the Common Criteria documentation from the ISA Server homepage http://www.microsoft.com/isaserver/ via "Technical Resources" to "Deployment".

Table 3: Identification of the TOE

Note: Although administration and management tools (e. g. for reporting and alerting, cache, monitoring, logging, remote management) are delivered together with the TOE, they are all excluded from the TOE and are considered part of the environment. Graphical taskpads and wizards that simplify navigation and configuration for common tasks do not belong to the TOE because they are embedded in the Microsoft Management Console (MMC - a configuration management tool that is supplied with the operating system Windows 2000). The TOE is the ISA Server running in firewall mode and with basic authentication only.

The TOE environment also includes applications that are not delivered with the ISA Server, but are used functionality of the underlying operating system Windows 2000 (e. g. File System, Event Log File, Registry, Network Interface, Cryptographic Support Interface, User Account Database).

3 Security Policy

The security policy of the TOE is to provide controlled and audited access to services, both from inside and outside an organisation's network, by allowing, denying, and/or redirecting the flow of data through the firewall.

The TOE allows or denies a set of computers or a group of users to access specific servers. If a rule is defined specifically to users, the TOE checks how the user should be authenticated. The evaluated TOE supports basic authentication as the standard method of authentication for Hypertext Transfer Protocol (HTTP) transmissions.

The TOE controls the flow of incoming and outgoing IP packets and controls information flow on protocol level. Information flow control is subdivided into IP packet filters, Protocol rules, Site and content rules, Server- and Web publishing, and Application filters.

The TOE also features the generation of security and access logs.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

Based on the personnel assumptions, the following usage conditions exist. Please refer to the Security Target [5], chapter 3.1 for more detail:

- Authorized administrators are non-hostile and follow all administrator guidance (A.NOEVIL).
- Personal who has physical access to the TOE and can log in the operating system is assumed to act as an authorized TOE administrator. That means that the TOE is available to authorized administrators only (A.DIRECT).

4.2 Environmental assumptions

The following assumptions about physical and connectivity aspects defined by the Security Target have to be met (refer to Security Target [5], chapter 3.1):

- Only authorized personal has physical access to the TOE because the TOE is physically secured (A.PHYSEC).
- The TOE stores and executes security-relevant applications only. It stores only data required for its secure operation (A.GENPUR).
- Information can not flow among the internal and external networks unless it passes through the TOE (A.SINGEN).
- Required certificates and user identities are installed using a confidential path (A.SECINST).
- The operating system implements the functions which are used by the TOE security functions. These functions are: reliable time stamp for log file audit, file protection for log file access protection, tools for audit review, and administration access control (A.OS).

Furthermore, the Security Target [5], chapter 3.2 defines an Organisational Security Policy (P.AUDACC) that states that audit records must contain sufficient information to prevent an attacker to escape detection in order to make persons accountable for the actions they conduct.

4.3 Clarification of scope

Additional threats that are not countered by the TOE and its evaluated security functions were not addressed by this product evaluation.

5 Architectural Information

The Target of Evaluation (TOE) and subject of the Security Target (ST) [5] is the Firewall product Internet Security and Acceleration Server 2000 - Standard Edition - SP1 with FP1.

ISA Server is a dedicated firewall that acts as the secure gateway to the Internet for internal computers. ISA Server protects all communication between internal computers and the Internet and runs on a Windows 2000 Server operating system. As a multi-layered firewall, the TOE provides security at different levels. IP packet filtering provides security by inspecting individual packets passing through the firewall. Application-level filtering allows ISA Server to inspect and secure popular protocols. The TOE has the possibility to create filters that allow or deny traffic on the packet layer and with data-aware filters to determine if packets should be accepted, rejected, redirected, or modified. The identification and authentication capabilities can be configured separately for incoming and outgoing requests. The TOE also includes the generation of security and access logs. The log files can be configured and enabled for

packet and application filters. They are human readable and can be reviewed with additional tools that belong to the TOE environment.

The operating system Windows 2000 maintains security attributes for all administrators. Windows 2000 stores the identification and authentication data for all known administrators and maintains a method of associating human users with the authorized administrator role. The TOE itself offers no additional identification and authentication methods for firewall administrators.

Figure 1 shows the TOE boundaries of the TOE, whereas the arrows indicate the interfaces between the TOE and the operating system Windows 2000.

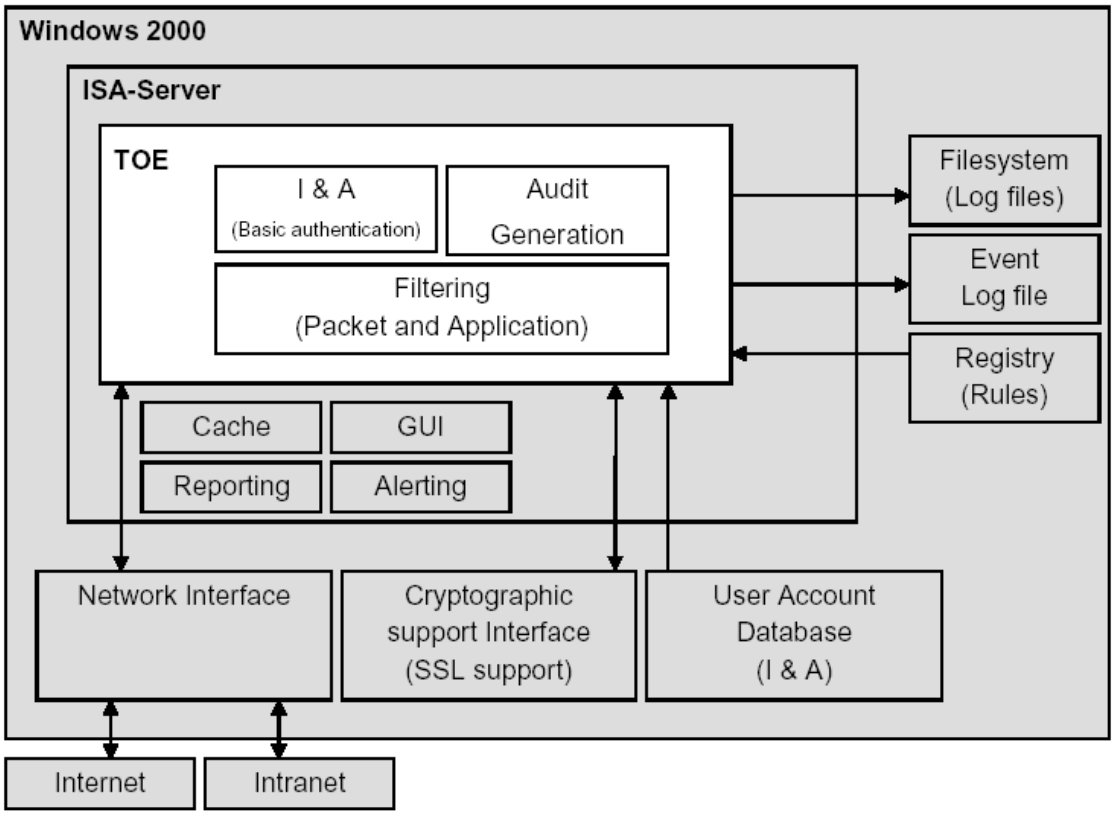

Figure 1: Identification of the TOE

The three main security functionality of the TOE are:

- Identification and Authentication:

  The scope of the evaluation is basic authentication. Basic authentication is the standard method of authentication for Hypertext Transfer Protocol (HTTP) transmissions for incoming and outgoing requests. Basic authentication sends and receives user information as text characters. No encryption is used with basic authentication, however, an optional SSL channel can be used but is not part of the evaluation.

- Filtering (Packet and Application level filtering):

  The TOE controls the flow of incoming and outgoing IP packets and controls information flow on protocol level. This control has to be active before any information can be transmitted through the TOE. Information flow control is subdivided into IP packet filters, Protocol rules, Site and content rules, Server- and Web publishing, and Application filters.

- Audit Generation:

  The TOE allows the generation of security and access logs. Logging information can be stored in Packet filter log files, Firewall service log file, Web proxy service log files, and Windows application event log files, outside the TOE.

6 Documentation

The following documentation is provided with the product by the developer to the customer:

[7] Microsoft Internet Security & Acceleration Server 2000 - Standard Edition manual, CD-ROM file: isa\chmbook\isa.chm; Date: 2000-12-15; size: 716.128 Bytes

[8] Microsoft Internet Security & Acceleration Server 2000 - Standard Edition - Evaluation addendum manual; Version 1.0; Date: 2003-08-22

7 IT Product Testing

Developer Tests

Test Configuration

The TOE has been tested within a configuration that consists of three networks. The TOE as the centre of the configuration has been connected to the three networks which are:

- a local network,
- the internet,
- and the DMZ.

Test Approach

The developer's tests were conducted to confirm that the TOE meets the security functions. The developer's strategy was to test the TOE against the specification of all security functions detailed in the developer’s functional specification.

The tests cover all security functions defined in the Security Target [5]. The amount of developer tests ensures that the TSF behave as specified in the Security Target [5] and as detailed in the developer’s functional specification.

The majority of tests were performed as automated testing using a proprietary automated test tool named Xcite.

Test Results

The developer specified, conducted and documented suitable functional tests for each security function. The test results obtained for all of the performed tests turned out to be as expected. In a few cases retraceable aberrance to the expected results could be described entirely due to configuration problems and could be resolved in a second test run.

No errors or other flaws occurred with regard to the security functionality defined in the Security Target [5]. Consequently, the test results demonstrate that the behaviour of the security functions are as specified.

All security functions could be tested successfully. The manufacturer was able to demonstrate that all security functions behave as specified in the Security Target [5] and as detailed in the developer’s functional specification.

Independent Evaluator Tests

Test Configuration

Basis of all test configurations is an installed TOE as identified in the Security Target [5]. For the testing, ISA Server has been installed on HP/Compaq ProLiant ML330 hardware.

For ITSEF’s independent testing as well as for the penetration testing, four different test configurations have been used including the same configuration as for the developer tests.

The evaluator tests have been performed both at the ITSEF facility in Essen, Germany and at Microsoft in Munich/München, Germany.

Test Approach:

The evaluation facility included all security functions in its test activities.

When choosing a sample of tests, the ITSEF accompanied all developer tests. All test cases and tests that were already conducted by the developer were taken into consideration, automated tests as well as manual tests. All TSFIs were tested.

Additionally, independent tests according to each TOE security function and other miscellaneous tests were conducted by the ITSEF. The objective was to test the functionality of the TOE and to verify the developer's test results.

To verify and reject possible vulnerabilities, the ITSEF performed penetration tests. Additionally, the TOE has been scanned with the Internet Security Scanner (ISS), a tool that can identify about 1200 possible vulnerabilities, including possible vulnerabiolities for the TOE and for the operating system. Because of the very different kind of created packets and scans this is also a stress test for the TOE.

Test Results

The independent tests as well as the repeated manufacturer tests confirmed that the TOE's security functions behave as specified in the Security Target [5] and as detailed in the developer's functional specification.

The penetration tests showed that the TOE does not feature obvious security vulnerabilities that can be exploited in its intended environment.

8 Evaluated Configuration

The TOE configuration consists of the software package "Microsoft Internet Security and Acceleration Server 2000 - Standard Edition" with Service Pack 1 and Feature Pack 1 installed, running on a single machine in firewall mode without cache and with basic authentication.

The ISA Server software and the Administrator and User Guidance as parts of the evaluated version for the TOE are delivered on CD-ROM through the sales channels. The required Service Pack 1 and Feature Pack 1 are distributed to users using both physical distribution and electronic distribution via the web. Part of the evaluation was the web distribution of Service Pack 1 and Feature Pack 1. The Guidance documentation [7] that is used for the evaluation is present on the distributed CD-ROM. The AGD Addendum [8] of the guidance documentation is delivered via the web only.

The TOE is running on a Windows 2000 operating system with service pack 3 installed and on a HP/Compaq ProLiant ML330 G2 hardware as the server hardware. The Standard Edition of the ISA Server with local administration and without Active Directory integration comprises the TOE.

9 Results of the Evaluation

The Evaluation Technical Report (ETR) [6] was provided by the ITSEF according to the Common Criteria [1], the Common Evaluation Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The verdicts for the CC, Part 3 assurance components (according to EAL2 and the Security Target evaluation) are summarised in the following table:

Assurance Classes and Components		**Verdict**
Security Target	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Configuration items	ACM_CAP.2	PASS
Delivery and Operation	CC Class ADO	PASS
Delivery Procedures	ADO_DEL.1	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC class ADV	PASS
Informal functional specification	ADV_FSP.1	PASS
Descriptive high-level design	ADV_HLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Tests	CC Class ATE	PASS
Evidence of coverage	ATE_COV.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Developer vulnerability analysis	AVA_VLA.1	PASS

Table 4: Verdicts for the assurance components

The evaluation has shown that the TOE fulfils the claimed strength of function (SOF-basic) for the authentication function using passwords.

The results of the evaluation are only applicable to the product ISA Server in the configuration as defined in the Security Target and summarised in this report (refer to the Security Target [5] and the chapters 2, 4 and 8 of this report). The

validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, and if the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The User Guidance documentation (refer to chapter 6 of this report) contains necessary information about the secure usage of the TOE. Additionally, for secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [5] and the Security Target as a whole has to be taken into account. Therefore a user/administrator has to follow the guidance in these documents.

The user of the TOE has to be aware of the existence and purpose of the AGD Addendum [8]. Therefore, the TOE's Internet product homepage has to provide information about the existence of the document and describe how to access the document. The reference has to be unambiguous and permanent.

11 Annexes

none

12 Security Target

For the purpose of publishing, the security target [5] of the target of evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

AGD Guidance Documentation (according to the CC assurance class " Guidance Documentation")

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security

DMZ Originally an abbreviation for demilitarised zone. In firewall terms a DMZ separates the internal network from the hostile forces of the Internet.

CC Common Criteria for IT Security Evaluation

EAL Evaluation Assurance Level

FP Feature Pack

http	Hypertext Transfer Protocol
ISA-Server	Internet Security and Acceleration Server
IT	Information Technology
MMC	Microsoft Management Console, a configuration management tool supplied with Windows 2000 that can be extended with plugins
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
SP	Service Pack
SSL	Secure Sockets Layer, a protocol that supplies secure data communication.
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.

[5] ISA Common Criteria Evaluation - Security Target, BSI-DSZ-CC-0218-2003, Version 1.2, Date 2003-08-12, Microsoft Corporation

[6] Evaluation Technical Report, BSI-DSZ-CC-0218-2003, Version 2, Datum 2003-09-02, TÜV Informationstechnik GmbH (confidential document)

[7] Microsoft Internet Security & Acceleration Server 2000 - Standard Edition manual, CD-ROM file: isa\chmbook\i sa.chm; Date: 2000-12-15; size: 716.128 Bytes

[8] Microsoft Internet Security & Acceleration Server 2000 - Standard Edition - Evaluation addendum manual; Version 1.0; Date: 2003-08-22

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / **Final Interpretation 008**

The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

***Package name* Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

***PP* Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.

CC Part 3:

Assurance categorisation (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class ADV: Development	Functional specification	ADV_FSP
	High-level design	ADV_HLD
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Low-level design	ADV_LLD
	Representation correspondence	ADV_RCR
	Security policy modeling	ADV_SPM
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 2.1 -Assurance family breakdown and mapping“

Evaluation assurance levels (chapter 6)

„The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.

Evaluation assurance level (EAL) overview (chapter 6.1)

Table 6.1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation“ allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component“ is not recognised by the CC as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6.1 - Evaluation assurance level summary“

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

„Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.“

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 6.2.2)

„Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.“

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 6.2.3)

„Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.“

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 6.2.4)

„Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous,

do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.“

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 6.2.5)

„Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.“

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 6.2.6)

„Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.“

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 6.2.7)

„Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 14.3)

AVA_SOF Strength of TOE security functions

„Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.“

Vulnerability analysis (AVA_VLA) (chapter 14.4)

AVA_VLA Vulnerability analysis

„Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.“

„Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.“

„Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“